Content Gateway Manager ヘルプ

Websense® Content Gateway

v7.8.x

Websense Content Gateway オンライン ヘルプ

February 2014

R250214782

目次

1 概要

Help | Content Gateway | バージョン 7.8.x

Websense® Content Gateway は、Websense Web Security Gateway および Web Security Gateway Anywhere の Web プロキシ コンポーネントです。

Content Gateway は、Websense Web Security と組み合せて使用することによって、コンテンツがプロキシを通過するときに、必要に応じて、詳細なコンテンツ分析を正確に実行し、分析結果に基づき適切な Web Security ポリシーを適用することによって、不正で望ましくないコンテンツからユーザーおよびネットワークを保護します。このオンデマンドの分析は、ユーザーとネットワークを保護すると同時にそれをすばやく変更し、*Web 2.0* サイトを組織およびユーザーにとって安全にします。Content Gateway の設定に応じて、高度な分析が HTTP、HTTPS、および FTP チャネルに適用されます。

高度な分析の正確な適用は、各 Web Security Gateway (Anywhere) 環境の管理者によって設定されます。

Content Gateway はまた、頻繁にアクセスされる情報をネットワークの端でキャッシュする高性能の Web プロキシ キャッシュとして機能するように構成することもできます。これによってコンテンツは物理的にエンド ユーザーの近くに置かれ、迅速に配信でき、帯域幅の使用を減らすことができます。

Content Gateway は、下記のいずれかとして配備できます。

- *SSL 検査*
- *Web プロキシ キャッシュとして*
- *キャッシュ階層の中で*
- *管理されたクラスタの中で*
- *DNS プロキシ キャッシュとして*

Content Gateway は、下記のように設定することもできます。

- クライアントがコンテンツにアクセスする前に、必ず認証が行われるようにする。Content Gateway は、統合 Windows 認証、レガシー NTLM (NTLMSSP)、LDAP、および RADIUS をサポートします。*Content Gateway ユーザー認証*、216 ページを参照してください。
- プロキシへのクライアント アクセスを制御する。*プロキシへのクライアント アクセスの制御*、200 ページを参照してください。
- プロキシが名前解決するべきホストがファイア ウォールの内側か外側かによって、異なる DNS サーバーを使用する。これによって、社内ネットワーク構成を保護し、同時にインターネット上の外部サイトへの透過的アクセスを提供します。*Split DNS オプションの使用*、215 ページを参照してください。
- インストールされている Data Security ポリシー エンジンまたは ICAP インターフェースを使用して、Websense Data Security を使用するサイトが Web ポスティングなどのアウトバウンド マテリアルを検査し、企業のポリシーに基づいてブロックまたは許可できるようにする。*Websense Data Security の使用*、147 ページを参照してください。
- 下記のどちらかの方法で Content Gateway manager へのアクセスを制御する。
  - 暗号化され、認証されたアクセスの場合は、SSL (Websense Data Security) 保護
  - ユーザー アカウントによって、どのユーザーがマネージャにアクセスできるか、およびそれらのユーザーがどのアクティビティ（例、[統計の表示のみ]、[統計の表示と Content Gateway の設定]）を実行できるかを指定する。
- ユーザーのファイアウォールに統合し、SOCKS サーバーを通じてトラフィックを制御する。

  セキュリティ、199 ページを参照してください。

関連項目：

- *配備のオプション*、3 ページ
- *コンポーネント*、5 ページ
- *プロキシ トラフィック分析の機能*、9 ページ
- *オンライン ヘルプ*、10 ページ
- *テクニカル サポート*、11 ページ

配備のオプション

Help | Content Gateway | バージョン 7.8.x

SSL 検査

HTTPS が有効化されている場合、HTTPS トラフィックは復号化され、検査され、次に、クライアントとオリジン サーバーの間で転送される時に再-暗号化されます。

Content Gateway は、認証処理機能の完全なセットを含んでいます。*暗号化データの使用*、159 ページを参照してください。

注意

Content Gateway は HTTPS コンテンツをキャッシュしません。

重要

HTTPS が有効化されて**いない**場合でも、Content Gateway は、HTTPS URL フィルタリングを実行します。つまり、各 HTTPS 要求に対して、URL ルックアップが実行され、ポリシーが適用されます。

明示的プロキシ モードでは、HTTPS が無効化されたとき、Content Gateway は 要求内のホスト名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、Content Gateway はブロック ページを提供します。一部のブラウザは、ブロック ページの表示をサポートしません。この機能を無効にするには、クライアントがプロキシに HTTPS 要求を送信しないように設定します。

透過的プロキシ モードでは、HTTPS が無効化されたとき、要求内に SNI がある場合は、Content Gateway は、SNI からホスト名を取得し、そのホスト名に基づき URL フィルタリングを実行します。そうでない場合は、Content Gateway は配信先サーバーの証明書で指定されている共通名を使用します。しかし、共通名がワイルドカード（*）を含んでいる場合は、宛先 IP アドレスの検索が実行されます。サイトがブロックされている場合、クライアントとの接続が失われます。ブロック ページは提供されません。WCCP と共に使用しているときこの機能を無効にするには、HTTPS のサービス グループを作成しないでおきます。

Web プロキシ キャッシュとして

Content Gateway が Web プロキシ キャッシュとして配備されているとき、ユーザーによる Web コンテンツ要求は、宛先 Web サーバー（オリジン サーバー）への転送の途中で Content Gateway を通過します。Content Gateway キャッシュが要求されたコンテンツを含んでいる場合は、Content Gateway はそのコンテンツを直接に提供します。Content Gateway キャッシュが要求されたコンテンツを含んでいない場合は、Content Gateway はプロキシとして動作し、ユーザーのためにオリジン サーバーからコンテンツを取得し、将来の要求に対応できるようにコピーを保持します。

Content Gateway は、一般的には、下記のどちらかの方法でクライアントの要求を受信するように配備されます。

- *明示的プロキシ*として。この場合、ユーザーのブラウザまたはクライアント ソフトウェアは要求を直接に Content Gateway に送信するように設定されます。*明示的プロキシ、49 ページ*を参照してください。
- *透過的プロキシ*として。この場合、ユーザーの要求は、宛先サーバーへの転送の途中で、透過的に Content Gateway にルーティングされます。ユーザーのクライアント ソフトウェア（一般的にはブラウザ）は、プロキシと通信していることを認識しません。*透過的プロキシと ARM、61 ページ*を参照してください。

キャッシュ階層の中で

Websense Content Gateway を柔軟なキャッシュ階層に組み込むことができます。そこでは、あるキャッシュで処理されなかったインターネット要求を、他のリージョナル キャッシュにルーティングでき、そのキャッシュのコンテンツと、要求元からの近接性を活用することができます。プロキシ サーバー階層内では、Content Gateway は、他の Content Gateway サーバーまたは他のキャッシング サーバーの親または子として機能することができます。*階層キャッシング、111 ページ*を参照してください。

管理されたクラスタの中で

Websense Content Gateway は、単一ノードから複数ノードに拡張でき、管理されたクラスタを形成することによって、システムの容量、パフォーマンス、および信頼性を高めます。

- 管理されたクラスタは、ノードの追加および削除を検出します。
- クラスタ ノードは、自動的に設定情報を共有し、それによってクラスタのメンバーをすべて同時に管理できます。

仮想 IP フェールオーバー オプションが有効化されている場合、Content Gateway はクラスタのノードに割り当てる仮想 IP アドレスのプールを維持します。Content Gateway は、ノードの故障（電源または CPU 障害など）を検出し、故障したノードの IP アドレスを正常なノードに再割り当てします。詳細については、*仮想IP フェールオーバー、108 ページ*を参照してください。

Content Gateway が WCCP を備えた透過的プロキシとして構成されている場合、フェールオーバーは WCCP によって処理され、仮想 IP フェールオーバーは使用できません。*WCCP の負荷配分、68 ページ*を参照してください。

詳細については、*クラスタ、101 ページ*を参照してください。

DNS プロキシ キャッシュとして

DNS プロキシ キャッシュとして、Content Gateway はクライアントの DNS 要求を解決できます。これによって、リモート DNS サーバーの負荷を減らし、DNS ルックアップの応答時間を短縮します。*DNS プロキシ キャッシング、123 ページ*を参照してください。

コンポーネント

Help | Content Gateway | バージョン 7.8.x

キャッシュ

キャッシュは、オブジェクト ストアと呼ばれる高速オブジェクト データベースから成ります。オブジェクト ストアは、URL および関連付けられているヘッダに従ってオブジェクトにインデックスを付けます。オブジェクト ストアは、同じオブジェクトの代替バージョン（言語または暗号化タイプが異なる）をキャッシュすることができ、また大小のドキュメントを保存でき、無駄なスペースを最小限にします。キャッシュがいっぱいになったとき、プロキシは陳腐化したデータを削除し、頻繁に要求されるオブジェクトが最新の状態であるようにします。

Content Gateway は、キャッシュ ディスク上のディスク障害を許容します。ディスクが完全に壊れた場合、Content Gateway はそのディスクに [破損] を表すマークを付け、残りのディスクを引き続き使用します。すべてのキャッシュ ディスクが機能しなくなった場合、Content Gateway はプロキシ専用モードに移行します。

キャッシュをパーティションで区切って、ディスク スペースを特定のプロトコルおよびオリジン サーバーのデータの保存用に予約することができます。*キャッシュの構成、113 ページ*を参照してください。

RAM キャッシュ

Content Gateway は、非常によくアクセスされるオブジェクトの小さな RAM メモリ キャッシュを保持します。この RAM キャッシュは、最もよくアクセスされるオブジェクトをすばやく提供し、ディスクの負荷を減らします（特にトラフィック ピーク時に）。RAM キャッシュ サイズは設定可能です。*RAM キャッシュのサイズ変更*、122 ページを参照してください。

Adaptive Redirection Module

Adaptive Redirection Module (ARM) は、いくつかの重要な機能を提供します。1 つは、クラスタ通信インターフェース フェールオーバーのデバイス通知を送信する機能です。もう 1 つは、着信パケットを、IP レイヤーがそれを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更する機能です。

ARM は常にアクティブです。

ユーザーの要求をプロキシにリダイレクトするために、ARM は着信パケットのアドレスを変更します。パケットの配信先 IP アドレスはプロキシの IP アドレスに変更され、パケットの配信先ポートは使用されているプロトコルに応じて変更されます。たとえば、HTTP の場合、パケットの配信先ポートはプロキシの HTTP ポート（通常は 8080）に変更されます。

ARM は、プロキシを通じて適切に転送できないサイトの自動バイパスをサポートします。

ARM はまた、クライアント要求の過負荷を防止します。クライアント接続の数が指定されている限度を超えたとき、ARM は着信した要求を直接にオリジン サーバーに転送します。*接続負荷の軽減*、92 ページを参照してください。

ホスト データベース

ホスト データベースは、プロキシが接続するオリジン サーバーの Domain Name Server (DNS) エントリを保存します。ホスト データベースは特に、以下の情報を追跡します。

- DNS 情報（ホスト名を IP アドレスにすばやく変換するため）
- 各 ホストの HTTP バージョン（最新のプロトコル機能を、種々のサーバーを実行しているホストで使用できるようにするため）
- ホストの信頼性および可用性情報（機能していないサーバーからの応答待ちを避けるため）

DNS リゾルバ

透過的プロキシ環境では、プロキシは非同期 DNS リゾルバを含み、それによってホスト名の IP アドレスへの変換を簡素化します。Content Gateway は、DNS リゾルバをそのまま実装し、リゾルバのライブラリを利用せずに直接に DNS コマンド パケットを発行します。多くの DNS クエリーを同時に発行でき、また、高速 DNS キャッシュはよく使用するバインドをメモリに保持し、DNS トラフィックを削減します。

重要

Linux システムの DNS サーバの設定を変更した場合 (/etc/resolv.conf)、Content Gateway を再起動する必要があります。

プロセス

Help | Content Gateway | バージョン 7.8.x

Content Gateway には 4 つの基本的なプロセスがあります。

プロセス名	説明
content_gateway	接続を受け入れ、プロトコル要求を処理し、キャッシュまたはオリジン サーバーからのドキュメントを提供します。
content_manager	**content_gateway** プロセスを開始、モニタ、および設定します。 **content_manager** プロセスはまた、Content Gateway manager のユーザー インターフェース、プロキシ自動設定ポート、統計インターフェース、クラスタ管理、仮想 IP フェールオーバーを処理します。 **content_manager** プロセスは、**content_gateway** プロセスの失敗を検出した場合、このプロセスを再起動し、また、すべての着信要求の接続キューを保持します。サーバーが再起動するまでの数秒間に着信した着信接続は接続キューに保存され、順に処理されます。この接続キューは、ユーザーをサーバーの再起動によるダウンタイムから保護します。

プロセス名	説明
content_cop	**content_gateway** および **content_manager** の状態をモニタします。 **content_cop** プロセスは、定期的に（1 分に数回）**content_gateway** および **content_manager** の状態を問い合わせるために、ハートビート要求を発行して合成 Web ページを取得します。タイムアウト時間内に応答を受け取らなかった場合、または不適切な応答を受け取った場合、**content_cop** は、**content_manager** および **content_gateway** を再起動します。
analytics_server	Content Classification Analytics のために発行された要求および生成されたプロセスを管理します。

管理ツール

Help | Content Gateway | バージョン 7.8.x

Content Gateway の主要な設定および管理ツールは、ユーザーのブラウザを通じてアクセスできる Web ベースのグラフィカル ユーザー インターフェースです。Content Gateway manager は、Content Gateway クラスタ全体に対して、パスワード保護され、SSL 暗号化された、シングルポイント管理を提供します。Content Gateway manager は、Content Gateway のパフォーマンスとネットワーク トラフィックをモニタするためのグラフおよび統計表示、およびプロキシの設定と微調整のためのオプションを備えています。

Content Gateway コマンドライン インタフェ- スを使用するのが便利または必要な場合があります。個別のコマンドを実行するか、またはシェルの中に一連のコマンドを記述することができます。この方法は、Content Gateway が Websense アプライアンス上にインストールされているときには、部分的にのみ利用できます。その場合には、代わりに Content Gateway manager と Appliance manager の **[Command Line Utility]** を使用します。

コマンド ライン インターフェースと同様に、Content Gateway 設定ファイルで設定変更を行うのが便利または必要な場合があります。これはファイル編集およびシグナル処理インターフェースを通じて管理をサポートします。Content Gateway manager またはコマンドライン インターフェースを通じて行った変更は自動的に設定ファイルに反映されます。

下記を参照してください :

Content Gateway manager、127 ページ

コマンドライン インターフェース、129 ページ

設定ファイル、129 ページ

プロキシ トラフィック分析の機能

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、ネットワーク トラフィック分析およびモニタのための下記のオプションを提供します。

- *Manager 統計およびグラフ*は、ネットワークトラフィック情報を表示します。Content Gateway manager からのグラフおよび統計を表示するか、またはコマンドライン インターフェースを使用して統計を収集し、処理します。
- 種々の*パフォーマンス グラフ*は、仮想メモリ使用量、クライアント接続、ドキュメントのヒット率などに関する履歴情報を示します。*パフォーマンス グラフ*を Content Gateway manager に表示します。
- *Manager のアラーム*は、Content Gateway manager に表示されます。Content Gateway は、検出したエラー条件に関するアラームを生成します。アラームが発生したときサポート担当者に電子メールまたはページを送信するように Content Gateway を設定できます。

  Content Gateway はまた、いくつかのアラームを Web Security マネージャに送信します。そこではそれらは**アラート**と呼ばれます。要約アラート メッセージは、Web Security **[Status（ステータス）] > [Today（本日）]** ページに表示されます。完全なアラート メッセージは、**[Alerts（アラート）]** ページに表示されます。Web Security 管理者は、Content Gateway がどのような状態でアラート メッセージを生成するか、およびどのような方法でアラートを送信するか（電子メールまたは SNMP）を設定できます。
- *トランザクション ロギング*によって、プロキシが受け取る各要求およびプロキシが検出する各エラーに関してログ ファイルに情報を記録できます。ログを使用して、何人のユーザーがプロキシを使用し、各ユーザーがどのぐらいの量の情報を要求したか、また、どのページが最も人気があるかを判断します。トランザクションでエラーが発生した理由と、その時点でのプロキシ キャッシュの状態を確認できます。たとえば、Content Gateway が再起動したこと、またはクラスタ通信がタイムアウトになったことを確認できます。

  Content Gateway はいくつかの標準ログ ファイル フォーマット（例、Squid、Netscape）および独自のカスタム フォーマットをサポートします。標準フォーマットのログ ファイルを既製の分析パッケージを使って分析できます。ログ ファイルを分割して、プロトコルまたはホストに固有の情報を含むようにしておくと、ログ ファイルの分析が容易になります。

トラフィック分析のオプションについては、*トラフィックのモニタリング*、133 ページを参照してください。ロギングのオプションについては、*ログ ファイルの使用*、271 ページを参照してください。

オンライン ヘルプ

Help | Content Gateway | バージョン 7.8.x

Content Gateway manager のどのページからでも、**[Get Help!（ヘルプを表示 !）]** をクリックすると、製品の使用に関する詳細な情報が表示されます。

重要

Microsoft Internet Explorer のデフォルト設定によって、ヘルプ システムの操作がブロックされている場合があります。セキュリティ アラートが表示された場合、[Help（ヘルプ）] を表示するには、**[Allow Blocked Content（ブロックされているコンテンツを許可）]** を選択します。

組織のセキュリティ標準によって許可されている場合、**[Tools（ツール）] > [Internet Options（インターネット オプション）]** インターフェースの [Advanced（詳細設定）] タブで警告メッセージを永久に無効にすることができます（ [Security（セキュリティ）] オプションの下の **[Allow active content to run in files on My Computer（マイコンピュータのファイルでのアクティブ コンテンツの実行を許可する）]** をオンにします ）。

オンライン ヘルプの PDF バージョンにアクセスするか、またはリリース ノート、インストールおよび配備情報、FAQ、ヒント、および他の技術情報にアクセスするには、Websense Technical Library にアクセスします。

テクニカル サポート

Help | Content Gateway | バージョン 7.8.x

Websense 製品に関する技術情報は、1 日 24 時間、下記のオンラインで入手できます：

http://support.websense.com

サポート サイトでは下記の情報を参照できます。

- ヒント
- カスタマ フォーラム
- 最新のリリース情報
- 検索可能な Websense Knowledge Base
- 最新のホットフィックスおよびパッチ
- [show-me] チュートリアルとビデオ
- 製品マニュアル
- テクニカル ライブラリ
- よくある質問に対する回答
- 詳細な技術ペーパー
- 月別サポート ウェビナー
- テクニカル アラート
- 最も一般的なソリューション

Websense Support サイトは、Service Request ポータルを通じた [ケースの開始] を含む、すべてのテクニカル リソースへのアクセスを提供します。

2 使用開始にあたって

Help | Content Gateway | バージョン 7.8.x

Content Gateway をシステムまたはクラスタ内のすべてのノードにインストールした後、プロキシは使用できる状態になります。

使用を開始するには下記の手順を参照してください。

Content Gateway manager へのアクセス

Help | Content Gateway | バージョン 7.8.x

Web ブラウザベースの Content Gateway manager は、Content Gateway の管理コンソールです。

Content Gateway manager は、下記のブラウザでサポートされています。

- Microsoft Internet Explorer 8、9、および 10
- Mozilla Firefox バージョン 5 以上
- Google Chrome 13 以上、同じ拡張子を持つ Chrome（アドオン）を使用すると予期しない動作を引き起こすことがあります。

他のブラウザおよびバージョンを使用すると予期しない動作を引き起こすことがあります。

Java および JavaScript は、ご使用のブラウザで有効化する必要があります。Java および JavaScript の有効化に関する詳細は、ご使用のブラウザのマニュアルを参照してください。

Content Gateway manager にアクセスするには下記の 3 つの方法があります。

- Web Security manager の [Content Gateway] ボタンから。* Web Security manager からのアクセスの設定については、Web Security Help を参照してください。
- ブラウザで Content Gateway ホスト システムの IP アドレスおよびポートを入力する。下記を参照。
- Content Gateway が Websense アプライアンスのモジュールである場合、アプライアンス Logon ポータルを開き、[Content Gateway] ボタンをクリックします。

*TRITON Unified Security Center で二要素認証（証明書認証または RSA SecurID）が設定されている場合、唯一の方法は、Web Security manager を通じて Content Gateway manager にアクセスすることです。*Content Gateway を二要素認証として設定する、16 ページ*を参照してください。

> **注意**
> シングル サインオンを使用しているとき、Content Gateway IP アドレス上にポップ-アップできるようにブラウザを設定する必要があります。

Content Gateway manager に直接にアクセスするには、下記の手順を実行します。

1. Web ブラウザを開き、下記の URL を入力します。

   `https://nodename:adminport`

   ここで、*nodename* は IP アドレス、*adminport* は Content Gateway Manager に割り当てられたポート番号です（デフォルト：8081）。

   Content Gateway Manager を起動するための HTTPS の使用方法の詳細については、*セキュアな管理のための SSL の使用、203 ページ*を参照してください。
2. 管理者 ID（デフォルト：admin）およびパスワード、またはユーザー アカウントを使用して Content Gateway manager にログオンします。

   Content Gateway manager のパスワードはインストール時に設定されます。

   ID およびパスワードを変更でき、またユーザー アカウントも作成および変更できます。*Content Gateway Manager へのアクセスの制御、200 ページ*を参照してください。

Content Gateway manager は、**[Monitor（モニタ）] > [My Proxy（マイ プロキシ）] > [Summary（要約）]** ページに開きます。このページは、サブスクリプションの機能および Content Gateway システムの詳細に関する情報を表示します。[Monitor（モニタ）] タブの詳細については、*統計の表示、133 ページ*を参照してください。また Content Gateway manager の設定オプションの詳細については、*システムの構成、127 ページ*を参照してください。

セキュリティ証明書アラート

Content Gateway managerとのセキュアなブラウザ ベースの通信のために、SSL 接続 が使用されます。この接続は、Websense, Inc. が発行するセキュリティ証明書を使用します。対応しているブラウザは Websense, Inc. を既知の Certificate Authority として認識しないので、新しいブラウザから Content Gateway manager を最初に起動するとき証明書エラーが表示されます。このエラーを避けるためには、ブラウザ内にその証明書をインストールするか、またはその証明書を [今後も受け入れる] ように設定します。詳細についてはご使用のブラウザのマニュアルを参照してください。

注意

Internet Explorer を使用している場合、その証明書を受け入れてからも証明書エラーが表示されます。このエラー メッセージを消去するには、ブラウザをいったん閉じて、再度開きます。

Windows 7 の考慮事項

Windows 7 を使用している場合、ActiveX コントロールを許可するためには管理者としてブラウザを開く必要があります。

1. ブラウザ アプリケーションを右クリックし、**[Run as administrator（管理者として実行）]** を選択します。
2. Content Gateway managerにログオンし、上記の説明のようにセキュリティ証明書を受け入れます。

マネージャのログオフ

Content Gateway manager にログオンする方法は、ログオフ動作に影響します。

シングル サイン オンを使って Web Security manager から Content Gateway manager にログオンした場合は、Content Gateway manager をログオフしたとき、セッションが閉じられます。

しかし、Content Gateway manager に直接にログオンした場合は、**[Log Off（ログ オフ）]** ボタンをクリックしたとき、すべての開いているブラウザ ウィンドウを閉じるまで、セッションは閉じられません。

Content Gateway を二要素認証として設定する

Help | Content Gateway | バージョン 7.8.x

二要素（証明書）認証：

- TRITON Unified Security Center ログオンにのみ設定および適用されます。
- 管理者にログオン時に 2 つの形式の ID を提供することを要求します。
- 管理者が Content Gateway manager にアクセスする前に TRITON Unified Security Center にログオンするよう強制することによって、Content Gateway manager に適用することができます。
- Content Gateway managerへのアクセスを許可された管理者に対してシングル サインオンを設定することを要求します。
- **Content Gateway でパスワード ログオン機能を無効化することを要求します**（下記を参照）。それによって、シングル サインオンが設定されていない管理者が Content Gateway manager にアクセスするのを防止します。Content Gateway をアプライアンスに配備している場合、パスワード アクセスはアプライアンス マネージャ コマンドを使って無効化されます。V-シリーズまたは X- シリーズ マネージャ ヘルプを参照してください。

二要素認証の設定の詳細については、TRITON コンソール ヘルプの [証明書認証の設定] を参照してください。

Content Gateway パスワード ログオンの無効化および有効化

Content Gateway manager パスワード ログオンを無効化することによって TRITON コンソールからの二要素認証またはシングル サインオン アクセスのみを許可することができます。

> **重要**
> Content Gateway が Websense アプライアンス 上にインストールされている場合は、詳細については Appliance Manager を参照してください。

アプライアンスのパスワード ログオンを無効化するには、下記の手順を実行します。

1. Web Security manager でシングル サインオンを設定します。
2. 二要素認証を使用する場合は、TRITON コンソールで二要素認証を設定します。
3. Content Gateway ホスト システムにログオンし、ルート権限を取得します。
4. ディレクトリを [/etc] に変更し、[websense] サブディレクトリがあるかどうか確認します。ない場合は、[websense] サブディレクトリ（[mkdir websense]）を作成します。

5. ディレクトリを [websense]（パスは現在 [/etc/websense]）に変更し、ファイル [password-logon.conf] があるかどうか確認します。
6. ない場合は、そのファイル（[touch password-logon.conf]）を作成します。
7. [password-logon.conf] を編集します。
8. 行を追加するか、または既存の行を下記の通りに変更します。

   ```
   password-logon=disabled
   ```

9. ファイルを保存し、終了します。

変更はすぐに有効になります。Content Gateway を再起動する必要はありません。

すべての管理者のパスワード ログオンを再有効化するには、下記の手順を実行します。

1. Content Gateway ホスト システムにログオンし、ルート権限を取得します。
2. ディレクトリを [/etc/websense] に変更します。
3. [password-logon.conf] を編集し、下記の通りに変更します。

   ```
   password-logon=disabled
   ```

   を下記のように変更します。

   ```
   password-logon=enabled
   ```

4. ファイルを保存し、終了します。

変更はすぐに有効になります。Content Gateway を再起動する必要はありません。

マスタ管理者パスワードを忘れた場合の Content Gateway manager へのアクセスの方法

Help | Content Gateway | バージョン 7.8.x

注意

下記の手順を Content Gateway スタンドアロン（ソフトウェア）のインストールに適用します。

Content Gateway が Websense アプライアンスで実行している場合は、Appliance マネージャの **[Administration（管理）] > [Account Management（アカウント管理）]** ページでパスワードがリセットされます。

インストール時に、管理者パスワードを指定することができます。インストーラは自動的にパスワードを暗号化し、暗号化されたパスワードを **records.config** ファイルに保存します。Content Gateway manager のパスワードを変更する度に、Content Gateway は、**records.config** ファイルを更新します。

管理者パスワードを忘れ、Content Gateway manager にアクセスできない場合、**records.config** ファイルで現在のパスワードをクリア（設定変数の値を NULL に設定します）し、Content Gateway manager で新しいパスワードを入力します。パスワードの変数にはパスワードの暗号化または値 NULL のみを含めることができますから、**records.config** ファイルでパスワードを設定できません。

1. **/opt/WCG/config** の **records.config** ファイルを開きます。
2. 変数 **proxy.config.admin.admin_password** を NULL にせ手値し、パスワードを空白のままにしておきます。

   注意
   語 NULL の後ろにスペースがないことを確認します。

3. ファイルを保存して、閉じます。
4. Content Gateway **bin** ディレクトリ **(/opt/WCG/bin)** から **./content_line -x** を実行して変更を適用します。
5. Content Gateway manager にログ オンします。ユーザー名とパスワードの入力を要求されたとき、管理者 ID を入力し、パスワードの欄は空白のままにしておきます。

   records.config ファイルでパスワードをクリアしていた場合は、管理者としてログオンするためにパスワードは入力する必要はありません。
6. **[Configure（設定）] > [My Proxy（マイ プロキシ）] > [UI Setup（UI のセットアップ）] > [Login（ログイン）]** タブを順に選択します。
7. **[Administrator（管理者）]** セクションで [Old Password] フィールドを空白のままにしておきます。**[New Password（新しいパスワード）]** フィールドに新しいパスワードを入力し、次に **[New Password (Retype)（新しいパスワード（再入力））]** フィールドに新しいパスワードを再入力します。
8. **[Apply]** をクリックします。

   Content Gateway manager に次回アクセスするとき、この新しいパスワードを使用する必要があります。

サブスクリプション キーの入力

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *システム情報の設定、20 ページ*

Content Gateway が Web Security Gateway または Web Security Gateway Anywhere と共に配備されている場合、Content Gateway manager でサブスクリプション キーを入力する必要はありません。キーは、Web Securit y で指定されたとき自動的に共有されます。

注意

使用される Web Security インスタンスは、設定される Policy Server によって決められます。設定された Policy Server IP アドレスは、Content Gateway manager の **[More Details（詳細）]** ビューが選択されたとき、**[Monitor（モニタ）] > [My Proxy（マイ プロキシ）] > [Summary（要約）]** ページに表示されます。

Policy Server を設定するには、下記の手順を実行します。

- V- シリーズ または X シリーズ マネージャで **[Configuration（設定）] > [Web Security Components（Web Security コンポーネント）]** に移動します。
- ソフトウェアのインストール時に、**/opt/WCG/websense.ini** を編集し、**PolicyServerIP** の値を設定します。次に Content Gateway の処理を下記の通り一旦停止し、開始します。

```
/opt/WCG/WCGAdmin stop
/opt/WCG/WCGAdmin start
```

Content Gateway が Websense Data Security のみと共に配備されている場合は、Content Gateway manager でサブスクリプション キーを入力する必要があります。

1. **[Configure] > [My Proxy] > [Subscription（サブスクリプション）] > [Subscription Management（サブスクリプション管理）]** タブで Websense によって提供されているサブスクリプション キーを入力します。
2. **[Apply]** をクリックします。
3. **[Configure] > [My Proxy] >[Basic（基本）] > [General（一般）]** ページで **[Restart（再起動）]** をクリックします。

システム情報の設定

Help | Content Gateway | バージョン 7.8.x

Content Gateway が Web Security Gateway または Web Security Gateway Anywhere のプロキシ統合である場合、Policy Server IP アドレスおよびポートはインストール時に指定されています。

Policy Server および Filtering Service タイムアウトの条件および動作（トラフィックを許可またはブロック）の設定を完了するには、下記の手順を実行します。

1. **[Configure] > [My Proxy] > [Subscription] > [Scanning（スキャン）]** タブに移動します。Filtering Service の IP アドレスおよびポートを確認します。これは、Web Security をインストールしたとき入力した情報です。
2. **[Communication Timeout（通信タイムアウト）]** の設定値を確認します。これは Content Gateway が Policy Server または Filtering Service との通信で待機する時間（ミリ秒）です。この時間を過ぎると、設定されている **[Action for Communication Errors（通信エラーに対する処置）]** がトリガされます。

   デフォルトのタイムアウト値は、5000 ms（5 秒）です。値を変更した場合、Content Gateway を再起動する必要があります。
3. 通信タイムアウト条件が発生した場合、**[Action for Communication Errors]** セクションで、トラフィックを許可またはブロックすることを選択する必要があります。タイムアウトが発生した場合、Content Gateway はその設定値を適用し、サービスに戻ることを検出するためにサービスを定期的にポーリングします。
4. **[Apply]** をクリックします。

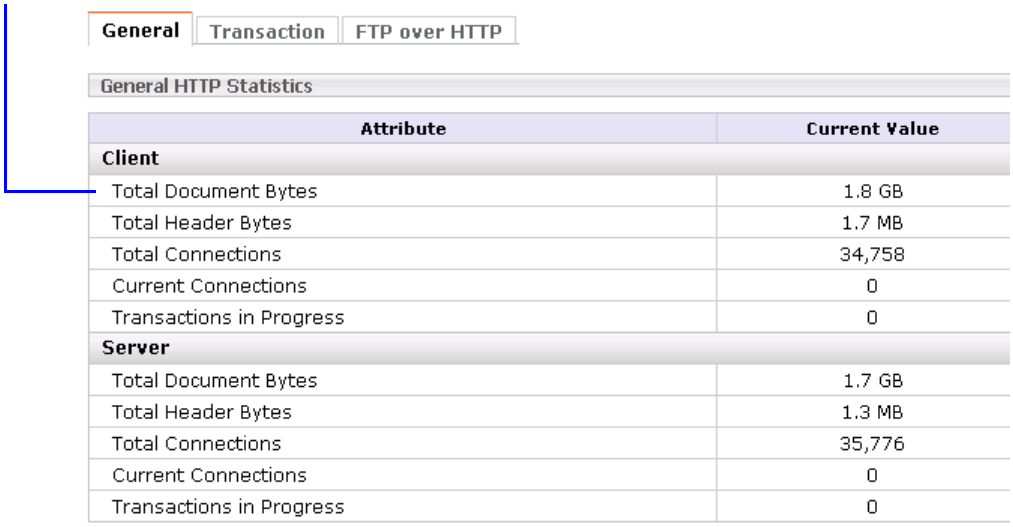
プロキシがインターネット要求を処理していることの確認

Help | Content Gateway | バージョン 7.8.x

プロキシをインストールした後、プロキシが Web コンテンツの要求を処理していることを確認します。

1. Content Gateway manager を開きます。*Content Gateway manager へのアクセス、13 ページ*を参照してください。
2. **[Monitor] > [My Proxy] > [Summary]** ページに移動し、ライセンス契約の詳細、データ ファイルのスキャンニング ステータス、および使用されているオブジェクトの数、ヒット率、他の基本プロキシ サービス情報を含むノードの詳細を確認します。
3. **[Monitor] > [Protocol（プロトコル）] > [HTTP] > [General]** に移動して、[General HTTP Statistics（一般的な HTTP 統計）] テーブルを表示します。
4. テーブルの **[Client（クライアント）]** セクションの中の現在の **[Total Document Bytes（合計のドキュメント バイト）]** 統計を確認します。

この統計の値を調べます。



General | Transaction | FTP over HTTP

General HTTP Statistics

Attribute	Current Value
Client	
Total Document Bytes	1.8 GB
Total Header Bytes	1.7 MB
Total Connections	34,758
Current Connections	0
Transactions in Progress	0
Server	
Total Document Bytes	1.7 GB
Total Header Bytes	1.3 MB
Total Connections	35,776
Current Connections	0
Transactions in Progress	0

5. ブラウザをプロキシ ポートに設定します。
6. インターネットを参照します。
7. 再度 **[Total Document Bytes]** 統計を調べます。
   この値は プロキシが HTTP 要求を処理する際に大きくなります。

コマンドライン インターフェースの使用

Help | Content Gateway | バージョン 7.8.x

ブラウザへのアクセス権がない場合、または UNIX シェルのようなコマンド インターフェースを使用したい場合、コマンドライン インターフェースはプロキシ統計の確認および Content Gateway の設定を行うためのすばやい方法を提供します。

> **注意**
> コマンドライン インタフェースは、Content Gateway が Websense アプライアンス上にインストールされている場合は、利用できません。代わりに、Content Gateway manager と V シリーズまたは X シリーズ マネージャのコマンドライン ユーティリティを使用します。

個別のコマンドを実行するか、またはシェルの中に複数のコマンドを記述することができます。*Websense Content Gateway のコマンド*、329 ページを参照してください。

1. root に移動します。

   ```
   su
   ```

2. Content Gateway の **bin** ディレクトリ (/opt/WCG/bin) に変更します。このディレクトリから Content Gateway のコマンドを実行します。

   コマンドは下記の形式です。

   ```
   content_line - コマンド引数
   ```

3. **content_line** コマンドのリストで、下記の通り入力します。

   ```
   content_line -h
   ```

> **注意**
> Content Gateway **bin** ディレクトリがパスにない場合、コマンドの先頭に ./ が付きます。/
>
> 例：
>
> ```
> ./content_line -h
> ```

コマンド ラインでの Content Gateway の起動および停止

Help | Content Gateway | バージョン 7.8.x

コマンド ラインから Content Gateway を停止または起動するには、下記の手順を実行します。

1. root に移動します。

   ```
   su
   ```

2. Content Gateway のインストール ディレクトリ（/opt/WCG）に変更します。

プロキシを起動するには、下記の通り入力します。

```
./WCGAdmin start
```

プロキシを停止するには、下記の通り入力します。

```
./WCGAdmin stop
```

プロキシを再起動するには、下記の通り入力します。

```
./WCGAdmin restart
```

Content Gateway サービスが何を実行しているか確認するには、下記の通り入力します。

```
./WCGAdmin status
```

Content Gateway をインストールした後、Content Gateway manager（管理インターフェース）を開き、プロキシが実行していることを確認します。*Content Gateway manager へのアクセス*、13 ページおよび*プロキシがインターネット要求を処理していることの確認*、21 ページを参照してください。

no_cop ファイル

ファイル **/opt/WCG/config/internal/no_cop** は、**content_cop** プロセスが **content_manager** を起動したり、何らかのヘルス チェックを実行することなく、すぐに終了するよう指示する管理制御として機能します。**no_cop** ファイルは、プロキシが **./WCGAdmin stop** コマンドによって停止された時に自動的に開始するのを防ぎます。

そのような静的制御がなくても、Content Gateway はシステムの再起動時に自動的に再起動します。**no_cop** 制御は、Content Gateway が **./WCGAdmin start** コマンドによって再起動されるまでオフにしておきます。

no_cop ファイルが Content Gateway の起動を禁止しているとき、システム ログ ファイルに下記のメッセージが記録されます。

```
content_cop[16056]: encountered "config/internal/no_cop"
file...exiting
```

3 Web プロキシ キャッシング

Help | Content Gateway | バージョン 7.8.x

Web プロキシ キャッシングは、頻繁にアクセスされる Web オブジェクト（ドキュメント、イメージ、記事など）のコピーをユーザーに近い場所に保存し、この情報をユーザーに提供します。インターネット ユーザーはそれらの情報をより速く取得でき、インターネット帯域幅を他のタスクのために解放することができます。

インターネット ユーザーは、インターネット上のあらゆる場所の Web サーバーに要求を送信します。キャッシング サーバーがそれらの要求を処理するためには、Web プロキシ サーバーとして機能する必要があります。Web プロキシ サーバーは、Web オブジェクトに対するユーザーの要求を受け取り、それらの要求を処理するか、またはそれらの要求を**オリジン サーバー**（要求された情報のオリジナルのコピーを含んでいる Web サーバー）に転送します。

Content Gateway は、**透過的プロキシ環境**（ユーザーのクライアント ソフトウェア（一般的にはブラウザ）はプロキシと通信していることを認識しません）、と**明示的プロキシ環境**（ユーザーのクライアント ソフトウェアは要求を直接にプロキシに送信するように設定されています）の両方をサポートします。

キャッシュ要求

関連項目：

- *キャッシュされたオブジェクトの最新性の確認、27 ページ*
- *ローカル キャッシュ コンテンツへの更新のスケジュール設定、34 ページ*
- *キャッシュ内のコンテンツのピンニング、36 ページ*
- *キャッシュするか否か?、38 ページ*
- *HTTP オブジェクトのキャッシング、38 ページ*
- *オブジェクト キャッシングの強制、45 ページ*
- *HTTP の代替のキャッシング、45 ページ*
- *FTP オブジェクトのキャッシング、47 ページ*

以下の概要は、Content Gateway がユーザー要求を処理する方法を示しています。

1. Content Gateway は、Web オブジェクトに対するユーザーの要求を受け取ります。
2. プロキシは、Web アドレスを使用して、そのオブジェクト ストア（キャッシュ）の中で要求されたオブジェクトを探します。
3. オブジェクトがキャッシュ内にある場合、プロキシは、オブジェクトが十分に新しいバージョンであるかどうかを確認します。（*キャッシュされたオブジェクトの最新性の確認、27 ページ*を参照）。オブジェクトが新しい場合、プロキシは、それをユーザーに**キャッシュ ヒット***として提供します。*
4. キャッシュ内のデータが古くなっている場合、プロキシはオリジン サーバーに接続し、オブジェクトがまだ最新であるかどうかを照会します（再確認）。オブジェクトがまだ最新である場合、プロキシは、キャッシュされているコピーをユーザーに送信します。
5. オブジェクトがキャッシュ内にない場合（キャッシュ ミス）、またはキャッシュされているコピーがもはや有効でない場合、プロキシはオリジン サーバーからオブジェクトを取得し、それをユーザーに送信し、同時にキャッシュに保存します。それ以降のそのオブジェクトに対する要求は、より速く処理されます。なぜならオブジェクトはキャッシュから直接に取得されるからです。

Content Gateway は、**Java アプレット**、**JavaScript** プログラム、**VBScripts** および他の実行可能なオブジェクトを、HTTP オブジェクトの最新性およびキャッシュ可能性のルールに従って、キャッシュに保存し、そのキャッシュから提供することができます。Content Gateway は、アプレット、スクリプト、またはプログラムを実行しません。これらのオブジェクトは、要求を送信したクライアント システムがこれらのオブジェクトをロードしたときのみ実行します。

Content Gateway は、部分的なドキュメントをキャッシュに保存しません。 HTTP または FTP ダウンロードが進行中にクライアントが切断した場合は、Content Gateway は、切断の後、最大 10 秒間ダウンロードを継続します。転送が正常に完了した場合は、Content Gateway は、オブジェクトをキャッシュに保存します。ダウンロードが完了しなかった場合は、Content Gateway はオリジン サーバーとの接続を解除し、キャッシュからオブジェクトを削除します。

キャッシュされたオブジェクトの最新性の確認

Help | Content Gateway | バージョン 7.8.x

Content Gateway は Web オブジェクトに対する要求を受け取ったとき、そのキャッシュ内で要求されたオブジェクトを探します。オブジェクトがキャッシュ内にある場合、プロキシは、オブジェクトが十分に新しいバージョンであるかどうかを確認します。

プロキシがキャッシュ内のオブジェクトの最新性を判断する方法はプロトコルによって異なります。

- HTTP オブジェクトは、作成者が指定した有効期限をサポートします。プロキシはこれらの有効期限に従います。そのような有効期限がない場合、プロキシはオブジェクトが変更される頻度と、管理者が選択した最新性のガイドラインに基づいて有効期間を選択します。さらに、オブジェクトがまだ最新であるかどうかをオリジン サーバーで確認することによって、オブジェクトを再確認できます。*HTTP オブジェクトの最新性、28 ページ*を参照してください。
- FTP オブジェクトは、指定された期間キャッシュ内に留まります。*FTP オブジェクトの最新性、33 ページ*を参照してください。

HTTP オブジェクトの最新性

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、キャッシュ内の HTTP オブジェクトが新しいかどうかを以下の方法によって判断します。

- **Expires** または **max-age** ヘッダーをチェックする

  一部の HTTP オブジェクトは、オブジェクトをキャッシュできる期間を指定する **Expires** ヘッダーまたは **max-age** ヘッダーを含んでいます。現在の時刻と期限切れ時刻を比較することによって、プロキシにオブジェクトが新しいかどうかを知らせます。

- **Last-Modified / Date** ヘッダーの確認

  HTTP オブジェクトに **Expires** ヘッダーまたは **max-age** ヘッダーがない場合、プロキシは下記の式を使用して最新性の限界値を計算できます。

  ```
  freshness_limit =(date - last_modified) * 0.10
  ```

  ここで、*date* はオブジェクトのサーバー応答ヘッダーの日付、*last_modified* は **Last-Modified** ヘッダーの日付です。**Last-Modified** ヘッダーがない場合は、プロキシはオブジェクトがキャッシュに書き込まれた日付を使用します。値を 0.10（10 パーセント）増減できます。*最新性計算のエージング係数の変更、28 ページ*を参照してください。

  計算による最新性の限界値は、最小および最大境界によって設定されます。*絶対最新性限界値の設定、29 ページ*を参照してください。

- 絶対最新性限界値の確認

  HTTP オブジェクトに **Expires** ヘッダーがないか、または **Last-Modified** と **Date** の両方のヘッダーがない場合は、プロキシは最大および最小最新性限界値を使用します。*絶対最新性限界値の設定、29 ページ*を参照してください。

- **cache.config** ファイル内の再確認ルールの確認

  再確認ルールは、特定の HTTP オブジェクトに最新性限界値を適用します。たとえば、特定のドメインまたは IP アドレスから発信するオブジェクト、指定された正規表現を含む URL をもつオブジェクト、および特定のクライアントによって要求されたオブジェクトに対して最新性限界値を設定できます。*cache.config、450 ページ*を参照してください。

最新性計算のエージング係数の変更

Help | Content Gateway | バージョン 7.8.x

オブジェクトに期限切れ情報が含まれていない場合、Content Gateway は、**Last-Modified** および **Date** ヘッダーからその最新性を推定できます。デフォルトでは、プロキシは、オブジェクトを最後に変更されてから経過した時間の 10 % の間保存します。この比率を増減できます。

1. Content Gateway **config** ディレクトリにある **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
proxy.config.http.cache.heuristic_lm_factor	最新性計算のためのエージング係数を指定します。 デフォルト値は 0.10（10 パーセント）です。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway **bin** ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

絶対最新性限界値の設定

Help | Content Gateway | バージョン 7.8.x

一部のオブジェクトには **Expires** ヘッダーがないか、または **Last-Modified** および **Date** の両方のヘッダーがありません。絶対最新性限界値を指定することによって、キャッシュ内でこれらのオブジェクトが最新であるとみなされる時間を制御できます。寿命時間が長いほど、オブジェクトはキャッシュ内に長く保持されます。ページをネットワークから検索する代わりにキャッシュから取得することによってパフォーマンスが向上します。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** タブに移動します。
2. **[Freshness（最新性）]** セクションの **[Minimum Heuristic Lifetime（最小ヒューリスティック寿命）]** 領域で、有効期限がない HTTP オブジェクトがキャッシュ内で最新とみなされる最小時間を指定します。この時間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、3600 秒（1 時間）です。
3. **[Maximum Heuristic Lifetime（最小ヒューリスティック寿命）]** フィールドで、有効期限がない HTTP オブジェクトがキャッシュ内で最新とみなされる最大時間を指定します。この時間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、86400 秒（1 日）です。
4. **[Apply]** をクリックします。

ヘッダー要件の指定

Help | Content Gateway | バージョン 7.8.x

キャッシュ内のオブジェクトの最新性を確保するために、Content Gateway が指定したヘッダーを持つオブジェクトだけをキャッシュするように設定します。

> **警告**
> デフォルトでは、プロキシはすべてのオブジェクト（ヘッダーのないオブジェクトを含む）をキャッシュします。Websense では、プロキシの特別の事情がない限りデフォルト設定を変更しないことを推奨します。プロキシが **Expires** または **max-age** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするように設定されている場合、キュッシュ ヒット率が大幅に下がります（明示的な期限切れ情報があるオブジェクトはごく少数です）。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** タブに移動します。
2. **[Behavior（動作）]** セクションの **[Required Headers（必要なヘッダー）]** 領域で、下記のいずれかを指定します。
   - **Expires** ヘッダーまたは **Cache-Control** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、**[An Explicit Lifetime Header（明示的寿命ヘッダー）]** を指定します。
   - **Expires** ヘッダーまたは **Last-Modified** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、**[A Last-Modified Header（最後に変更したヘッダー）]** を指定します。
   - すべての HTTP オブジェクトをキャッシュする（特定のヘッダーを必要としない）には、**[No Required Headers（ヘッダーを必要としない）]** を指定します。これは、デフォルトです。
3. **[Apply]** をクリックします。

Cache-Control ヘッダー

Help | Content Gateway | バージョン 7.8.x

キャッシュ内でオブジェクトが最新であると見なされる場合でも、クライアントまたはサーバーにはキャッシュからのオブジェクトの取得を禁止する制約が設定されていることがあります。たとえば、クライアントはオブジェクトがキャッシュから取得されたものでない、またはキャッシュから取得された場合にはオブジェクトを 10 秒以上キャッシュしないことを要求する場合があります。

Content Gateway は、キャッシュされたオブジェクトの可用性を **Cache-Control** ヘッダーを基に判断します。**Cache-Control** ヘッダーをクライアントの要求とサーバーの応答の両方に含めることができます。

下記の **Cache-Control** ヘッダーはオブジェクトがキャッシュから提供されるかどうかに影響を与えます。

- クライアントによって送信される **no-cache** ヘッダーは、プロキシに、オブジェクトをキャッシュから直接に*提供しない*こと、つまり常にオリジン サーバーからオブジェクトを取得することを指示します。クライアントの **no-cache** ヘッダーを無視するようにプロキシを設定できます（*クライアントの no-cache ヘッダーを無視するようにプロキシを設定する、39 ページ*を参照）。
- サーバーによって送信される **max-age** ヘッダーは、オブジェクトの経過時間と比較されます。経過時間の値が **max-age** よりも小さい場合、オブジェクトは最新であり、提供できます。
- クライアントによって送信される **min-fresh** ヘッダーは、*許容可能な最新性の許容値*です。クライアントは、オブジェクトの最新性がこの値以上であることを求めます。キャッシュされたオブジェクトが将来、少なくともこの期間最新性を保たない場合、そのオブジェクトは再確認されます。
- クライアントによって送信される **max-stale** ヘッダーは、プロキシが少し古くなったオブジェクトを提供することを許可します。一部のブラウザは、パフォーマンスの向上と引き換えに、少し古いオブジェクトを受け入れます（特に、インターネットの可用性に制約がある期間に）。

プロキシは、HTTP 最新性基準の*後に* Cache-Control 可用性基準を適用します。たとえば、オブジェクトが最新と見なされる場合でも、その経過時間がその `max-age` よりも大きい場合、提供されません。

HTTP オブジェクトの再確認

Help | Content Gateway | バージョン 7.8.x

クライアントがキャッシュ内の古くなった HTTP オブジェクトを要求した場合、Content Gateway はそのオブジェクトを再確認し、オブジェクトが変更されていないかどうかをオリジン サーバーに問い合わせます。再確認の結果は、以下のいずれかになります。

- オブジェクトがまだ最新である場合は、プロキシはその最新性限界値をリセットして、そのオブジェクトを提供します。
- オブジェクトの新しいコピーが利用できる場合は、プロキシは新しいオブジェクトをキャッシュし、古くなったコピーと置き換え、同時にユーザーにオブジェクトを提供します。

- オブジェクトがオリジン サーバーにない場合、プロキシはキャッシュされたコピーを提供しません。
- オリジン サーバーが再確認の問い合わせに応答しない場合、プロキシは確認を実行せず、キャッシュからの古くなったオブジェクトを提供します。

デフォルトでは、プロキシは、キャッシュ内の要求された HTTP オブジェクトが古くなっていると判断した場合、そのオブジェクトを再確認します。プロキシは、オブジェクトの最新性を*HTTP オブジェクトの最新性、28 ページ*に記載している方法で評価します。プロキシが HTTP オブジェクトを再確認する頻度を設定できます。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** タブに移動します。
2. **[Behavior]** セクションの **[When to Revalidate（再確認する時期）]** 領域で下記のいずれかを選択します。
   - **Never Revalidate（再確認しない）**。要求された HTTP オブジェクトの最新性をオリジン サーバーに照会しない場合。
   - **Always Revalidate（常に再確認する）**。要求された HTTP オブジェクトの最新性を常にオリジン サーバーに照会する場合。
   - **Revalidate if Heuristic Expiration（ヒューリスティック期限切れで再確認）**。要求された HTTP オブジェクトの最新性について、そのオブジェクトに **Expires** ヘッダーまたは **Cache-Control** ヘッダーがない場合にオリジン サーバーに照会する場合。Content Gateway は、**Expires** ヘッダーまたは **Cache-Control** ヘッダーのないすべての HTTP オブジェクトを陳腐化していると見なします。
   - **Use Cache Directive or Heuristic（キャッシュ ディレクティブまたはヒューリスティックを使用）**。Content Gateway がキャッシュ内のオブジェクトを陳腐化していると見なす場合に、要求された HTTP オブジェクトの最新性をオリジン サーバーに照会する場合。これは、デフォルトです。
3. **[Apply]** をクリックします。

> **注意**
>
> また、**cache.config** ファイルで特定の再確認ルールを設定できます。*cache.config、450 ページ*を参照してください。

FTP オブジェクトの最新性

Help | Content Gateway | バージョン 7.8.x

FTP オブジェクトにはタイム スタンプや日付情報がなく、指定した期間（15 分 ～ 2 週間）、キャッシュ内で最新であるとみなされます。この期間が過ぎると陳腐化していると見なされます。

FTP オブジェクトは、HTTP クライアント（ブラウザなど）から、または FTP クライアント（WS_FTP など）から要求することができます。Content Gateway は HTTP クライアントから要求された FTP オブジェクトのみをキャッシュします。

HTTP クライアントによって要求された FTP オブジェクト

HTTP クライアントによって要求された FTP オブジェクト（HTTP オブジェクト上の FTP）の絶対最新性限界値を設定できます。

> **注意**
> HTTP クライアントによって要求された FTP オブジェクトの絶対最新性限界値のほかに、**cache.config** ファイルで特定の FTP オブジェクトの最新性ルールを設定できます（*cache.config*、450 ページを参照）。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Freshness]** セクションの **[FTP Document Lifetime（FTP ドキュメントの寿命）]** 領域で、HTTP クライアントによって要求された FTP オブジェクトが最新とみなされる期間を指定します。この期間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、259200 秒（3 日間）です。
3. **[Apply]** をクリックします。

ローカル キャッシュ コンテンツへの更新のスケジュール設定

Help | Content Gateway | バージョン 7.8.x

パフォーマンスをさらに向上させ、HTTP および（HTTP クライアントから要求された）FTP オブジェクトがキャッシュ内で最新状態を保つように、[Scheduled Update（スケジュール設定した更新）] オプションを使用して、プロキシがスケジュール設定した時刻に特定のオブジェクトをキャッシュに入れるように設定することができます。

[Scheduled Update] オプションを使用するには、以下の手順を実行します。

- 更新をスケジュール設定するオブジェクトを含む URL のリスト、更新を行う時刻、および URL の再帰の深さを指定します。
- Scheduled Update オプションを有効化し、オプションの再試行設定を設定します。

詳細は、*スケジュール設定した更新オプションの設定、35 ページ*を参照してください。

Content Gateway は、ユーザーが指定した情報を使用して、処理する URL を決定し、各 URL について（該当する場合）すべての再帰的 URL を導出します。次に一意な URL リストを生成します。プロキシは、このリストを使用して、未アクセスの各 URL に対して HTTP **GET** を開始し、それがどの時点においても HTTP の同時性についてのユーザー指定の限度内にあるようにします。

> **注意**
> システムは、すべての HTTP **GET** 処理の完了をログに記録し、この機能のパフォーマンスをモニタできるようにします。

[Force Immediate Update（直ちに更新を強制）] オプションは、指定された更新時刻を待たずに、URL を更新できるようにします。このオプションを使用して、スケジュール設定した更新の設定をテストできます。*即時更新の強制、36 ページ*を参照してください。

スケジュール設定した更新オプションの設定

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Protocols] > [HTTP Scheduled Update（HTTP スケジュール設定した更新）] > [Update URLs（URL を更新）]** に移動します。
2. **[Scheduled Object Update]** 領域で、**[Edit File（ファイルを編集）]** をクリックして、**update.config** ファイルの設定ファイルの編集エディタを開きます。
3. 下記の情報を入力します。
   - **[URL]** フィールドに、更新のスケジュールを設定する URL を入力します。
   - *オプション*。**[Request Headers（ヘッダーを要求）]** フィールドに、各 **GET** 要求で渡されたヘッダーのセミコロン区切りのリストを入力します。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。
   - **[Offset Hour（オフセット時間）]** フィールドに、更新時間を導出するために使用する基準時間を入力します。00 から 23 までの値を指定できます。
   - **[Interval（間隔）]** フィールドに、更新が行われる（オフセット時間からの）間隔（秒）を入力します。
   - **[Recursion Depth（再帰の深さ）]** フィールドに、参照されている URL が再帰的に更新される（指定した URL からの）深さを入力します。たとえば、再帰の深さが 1 であれば、指定した URL と、元の URL からのリンクによって直接に参照されるすべての URL が更新されます。
4. **[Add]** をクリックし、次に **[Apply]** をクリックします。
5. **[Close]** をクリックします。
6. **[General（一般）]** タブをクリックします。
7. **[Scheduled Update]** を有効化します。
8. **[Maximum Concurrent Updates（最大同時更新）]** フィールドに、スケジュール設定した更新処理によってホストに過大な負荷をかけないようにするために、許容する同時更新要求の最大数を入力します。デフォルトは 100 です。
9. **[Retry on Update Error（更新エラー時の再試行）]** セクションの **[Count（カウント）]** フィールドに、失敗した場合に URL のスケジュール設定した更新を再試行する回数を入力します。デフォルト値は 10 です。
10. **[Retry on Update Error]** セクションの **[Interval]** フィールドに、失敗した場合に URL のスケジュール設定した更新の各再試行間の間隔を秒単位で入力します。デフォルト値は 2 です。
11. **[Apply]** をクリックします。

即時更新の強制

Help | Content Gateway | バージョン 7.8.x

[Force Immediate Update] オプションによって、**update.config** ファイルにリストされている URL を直ちに確認できます。このオプションは、**update.config** ファイルに含まれているオフセット時間および間隔設定を無視して、リストされている URL を更新します。

> **重要**
>
> Force Immediate Update オプションを有効化した場合、このオプションを無効化するまで、プロキシは、**update.config** ファイルで指定した URL を更新し続けます。

1. **[Configure] > [Protocols] > [HTTP Scheduled Update] > [General]** に移動します。
2. **Scheduled Update** が有効化されていることを確認します。
3. **[Update URLs]** タブをクリックします。
4. **[Force Immediate Update]** を有効化します。
5. **[Apply]** をクリックします。

キャッシュ内のコンテンツのピンニング

Help | Content Gateway | バージョン 7.8.x

キャッシュ ピンニング オプションは、Content Gateway が特定の HTTP オブジェクト（および HTTP クライアントから要求された FTP オブジェクト）を指定した時間、キャッシュ内に保持するように設定します。このオプションを使用して、最もよくアクセスされるオブジェクトが必要なときにキャッシュにあり、プロキシが重要なオブジェクトをキャッシュから削除しないようにします。

> **注意**
>
> プロキシは、Cache-Control ヘッダーを監視し、オブジェクトがキャッシュ可能である場合にだけ、キャッシュ内でそのオブジェクトをピンニングします。

キャッシュ ピンニングを使用するために、下記のタスクを実行します。

- **cache.config** ファイルでキャッシュ ピンニング ルールを設定します。*キャッシュ ピンニング ルールの設定、37 ページ*を参照してください。
- キャッシュ ピンニング オプションを有効化します。*キャッシュ ピンニングの有効化、37 ページ*を参照してください。

キャッシュ ピンニング ルールの設定

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. ページの終わりで **[Edit File]** をクリックして、**cache.config** ファイルの設定ファイル エディタを表示します。
3. 表示されたフィールドに、下記の情報を指定します。
   - **[Rule Type（ルール タイプ）]** ドロップダウン ボックスから、**pin-in-cache** を選択します。
   - **[Primary Destination Type]** ドロップダウン ボックスから、**url_regex** を選択します。
   - **[Primary Destination Value（一次宛先値）]** フィールドに、キャッシュでピンニングする URL を指定します。
   - **[Time Period（時間）]** フィールドに、キャッシュに含まれているプロキシがオブジェクトをピンニングする時間を指定します。

     さらに、二次指定子（例、**Prefix**、**Suffix**）をルールに追加できます。すべてのフィールドは *HTTP、350 ページ*で説明しています。
4. **[Add]** をクリックして、ルールをリストに追加し、**[Apply]** をクリックします。
5. **[Close]** をクリックします。

キャッシュ ピンニングの有効化

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Subsystems（サブシステム）] > [Cache（キャッシュ）] > [General]** で、**[Allow Pinning（ピンニングを許可）]** を有効化します。
2. **[Apply]** をクリックします。

キャッシュするか否か？

Help | Content Gateway | バージョン 7.8.x

Content Gateway がキャッシュに含まれていない Web オブジェクトの要求を受け取ったとき、オリジン サーバーから Web オブジェクトを取得し、それをクライアントに提供します。同時に、プロキシは、そのオブジェクトがキャッシュ可能かどうか調べてから、将来の要求に対応するためにそれをキャッシュ内に保存します。

Content Gateway は、オブジェクトがキャッシュ可能かどうかを、プロトコルをもとに判断します。

- HTTP オブジェクトの場合、プロキシは、クライアントおよびオリジン サーバーからのキャッシング指令に対応します。また、プロキシが特定のオブジェクトをキャッシュしないように設定できます。*HTTP オブジェクトのキャッシング、38 ページ*を参照してください。
- FTP オブジェクトの場合、プロキシは、ユーザーが設定オプションおよびファイルを通じて指定するキャッシング指令に対応します。*FTP オブジェクトのキャッシング、47 ページ*を参照してください。

HTTP オブジェクトのキャッシング

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、クライアントおよびオリジン サーバーからのキャッシング指令に対応し、またユーザーが設定オプションおよびファイルを通じて指定するキャッシング指令にも対応します。

この項は、下記のトピックについて解説します。

クライアントの指令

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、下記の要求ヘッダーが付いたオブジェクトをキャッシュ *しません*。

- **Cache-Control: no-store**
- **Cache-Control: no-cache**

> **注意**
> プロキシが **Cache-Control: no-cache** ヘッダーを無視するようにプロキシを設定できます。*クライアントの no-cache ヘッダーを無視するようにプロキシを設定する*、39 ページを参照してください。

- **Cookie:**（テキスト オブジェクトの場合）

  デフォルトでは、プロキシはオブジェクトがテキストでない限り、クッキーを含む要求に対応して提供されたオブジェクトをキャッシュします。プロキシがどのタイプのクッキーを含むコンテンツもキャッシュしない、または、クッキーを含むコンテンツをすべてキャッシュする、もしくはイメージ タイプのクッキーを含むコンテンツのみをキャッシュするように設定できます。*クッキーを含むオブジェクトのキャッシング*、44 ページを参照してください。
- **Authorization:**

> **注意**
> HTTP クライアントから要求された FTP オブジェクトはまた、**Cache-Control: no-store**、**Cache-Control: no-cache**、または **Authorization** ヘッダーを含むことができます。HTTP クライアントから要求された FTP オブジェクトがそのようなヘッダーを含む場合、プロキシは明示的にキャッシュするように設定されていない限り、そのオブジェクトをキャッシュしません。

クライアントの no-cache ヘッダーを無視するようにプロキシを設定する

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、クライアントの **Cache Control:no-cache** 指令を監視します。要求されたオブジェクトが **no-cache** ヘッダーを含む場合、プロキシは、そのオブジェクトがキャッシュ内の新しいコピーであっても、その要求をオリジン サーバーに転送します。

クライアントの **no-cache** 指令を無視するようにプロキシを設定できます。この場合、プロキシは、クライアント要求から **no-cache** ヘッダーを無視し、そのオブジェクトをそのキャッシュから提供します。

重要

no-cache 指令の監視のデフォルトの動作は、ほとんどの場合適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみクライアントの **no-cache** 指令を無視するように Content Gateway を設定します。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Behavior]** セクションで **[Ignore “no-cache” in Client Requests（クライアントの要求内の “no-cache” を無視する）]** オプションを有効化します。
3. **[Apply]** をクリックします。

注意

Microsoft Internet Explorer の一部のバージョンは、ユーザーがブラウザの **[Refresh（リフレッシュ）]** ボタンを押した場合、透過的キャッシュからのキャッシュ再ロードを要求しません。それによって、コンテンツがオリジン サーバーから直接にロードされるのを防止します。Content Gateway が Microsoft Internet Explorer の要求をより慎重に処理するように設定できます。その場合、提供するコンテンツの最新性を向上させることができますが、キャッシュから提供できるドキュメントの数が少なくなります。Content Gateway manager（**[Configure] > [Protocols] > [HTTP] > [Cacheability]** タブの **[Behavior]** セクション）で、プロキシが Microsoft Internet Explorer からの要求に対して **no-cache** ヘッダーを追加するように設定できます。

オリジン サーバーの指令

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、下記の要求ヘッダーが付いたオブジェクトをキャッシュしません。

- **Cache-Control: no-store**
- **Cache-Control: private**
- **WWW-Authenticate:**

注意

WWW-Authenticate ヘッダーを無視するようにプロキシを設定できます。*WWW-Authenticate ヘッダーを無視するようにプロキシを設定する*、42 ページを参照してください。

- **Set-Cookie:**
- **Cache-Control: no-cache**

注意

no-cache ヘッダーを無視するようにプロキシを設定できます。*サーバーの no-cache ヘッダーを無視するようにプロキシを設定する*、41 ページを参照してください。

- **Expires:** 0（ゼロ）の値または過去の日付の付いたヘッダー

サーバーの no-cache ヘッダーを無視するようにプロキシを設定する

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、**Cache Control:no-cache** 指令を監視します。**no-cache** ヘッダーが付いたオリジン サーバーからの応答は、キャッシュ内に保存されず、キャッシュに含まれているオブジェクトの以前のすべてのコピーが削除されます。

重要

no-cache ヘッダーを無視するようにプロキシを設定した場合、プロキシは、**no-store** ヘッダーも無視します。

重要

no-cache 指令の監視のデフォルトの動作は、ほとんどの場合適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみオリジン サーバーの **no-cache** 指令を無視するようにプロキシを設定します。

オリジン サーバー の **no-cache** ヘッダーを無視するようにプロキシを設定できます。

1. Content Gateway **config** ディレクトリにある **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
proxy.config.http.cache.ignore_server_no_cache	サーバーの指令を無視してキャッシュをバイパスするには 1 に設定します。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway **bin** ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

WWW-Authenticate ヘッダーを無視するようにプロキシを設定する

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、**WWW-Authenticate** 応答ヘッダーが含まれているオブジェクトをキャッシュしません。**WWW-Authenticate** ヘッダーは、認証チャレンジ応答をオリジン サーバーと比較するときクライアントが使用する認証パラメータを含んでいます。

重要

デフォルトの動作、つまり **WWW-Authenticate** ヘッダーが付いたオブジェクトをキャッシュしないという設定は、ほとんどの場合に適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみサーバーの **WWW-Authenticate** ヘッダーを無視するようにプロキシを設定します。

オリジン サーバーの **WWW-Authenticate** ヘッダーを無視するようにプロキシを設定できます。その場合 **WWW-Authenticate** ヘッダーの付いたオブジェクトは今後の要求に対応するためにキャッシュに保存されます。

1. Content Gateway **config** ディレクトリにある **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
proxy.config.http.cache.ignore_ authentication	**WWW-Authenticate** ヘッダーの付いたオブジェクトをキャッシュするには 1 に設定します。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway **bin** ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

設定の指令

Help | Content Gateway | バージョン 7.8.x

クライアントおよびオリジン サーバーの指令のほかに、Content Gateway は、ユーザーが設定オプションおよびファイルを通じて指定する指令に対応します。

プロキシを下記のいずれかに設定できます。

- どの HTTP オブジェクトもキャッシュ*しない*。*HTTP オブジェクト キャッシングの無効化、43 ページ*を参照してください。
- ダイナミック コンテンツをキャッシュする（疑問符 (?)、セミコロン (;)、cgi を含むまたは .asp で終了する URL を含むオブジェクト）*ダイナミック コンテンツのキャッシング、44 ページ*を参照してください。
- **Cookie:** ヘッダーに対応して提供したオブジェクトをキャッシュする*クッキーを含むオブジェクトのキャッシング、44 ページ*を参照してください。
- **cache.config** ファイルに含まれている never-cache ルールを監視します。*cache.config、450 ページ*を参照してください。

HTTP オブジェクト キャッシングの無効化

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、**cache.config** ファイルで never-cache ルールを設定した HTTP オブジェクトを除くすべての HTTP オブジェクトをキャッシュします。HTTP オブジェクトのキャッシングを無効化できます。それによってすべての HTTP オブジェクトはオリジン サーバーから提供され、キャッシュされません。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** タブに移動します。
2. **HTTP キャッシング**を無効化します。
3. **[Apply]** をクリックします。

ダイナミック コンテンツのキャッシング

Help | Content Gateway | バージョン 7.8.x

URL が疑問符 (?)、セミコロン (;)、cgi を含むか、または .asp で終了する場合、その URL はダイナミックと見なされます。デフォルトでは、Content Gateway は、ダイナミック コンテンツをキャッシュ*しません*。しかし、このコンテンツをキャッシュするようにプロキシを設定できます。

> **警告**
> 専用のプロキシが割り当てられている場合にのみ、プロキシがダイナミック コンテンツをキャッシュするように設定することを推奨します。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Dynamic Caching（ダイナミック キャッシング）]** セクションで、**[Caching Documents with Dynamic URLs（ダイナミック URL を含むドキュメントのキャッシュ）]** を有効化します。
3. **[Apply]** をクリックします。

クッキーを含むオブジェクトのキャッシング

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は、オブジェクトがテキスト *でない限り*、クッキーを含む要求に対応して提供されたオブジェクトをキャッシュします。プロキシはクッキーを含むテキスト コンテンツをキャッシュしません。なぜならオブジェクトとともにオブジェクト ヘッダーも保存され、パーソナライズされたクッキー ヘッダー値がオブジェクトとともに保存される可能性があるからです。

テキストでないオブジェクトの場合、パーソナライズされたヘッダーが配信されたり使用されたりする可能性はありません。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Dynamic Caching]** セクションの **[Caching Response to Cookies（クッキーへの応答のキャッシング）]** 領域で、下記のいずれかのキャッシング オプションを選択します。
   - テキストであるコンテンツを除くすべてのクッキーを含むコンテンツをキャッシュするには、**[Cache All but Text（テキストを除くすべてをキャッシュ）]** を選択します（これはデフォルト設定です）。
   - イメージであるクッキーを含むコンテンツをキャッシュするには、**[Cache Only Image Types（イメージ タイプのみキャッシュ）]** を選択します。

- すべてのタイプのクッキーを含むコンテンツをキャッシュするには、**[Cache Any Content Type（すべてのコンテンツ タイプをキャッシュ）]** を選択します。
- どのタイプのクッキーを含むコンテンツもキャッシュ*しない*場合は、**[No Cache on Cookies（クッキーをキャッシュしない）]** を選択します。

3. **[Apply]** をクリックします。

オブジェクト キャッシングの強制

Help | Content Gateway | バージョン 7.8.x

特定の URL（ダイナミック URL を含む）を指定した期間、**Cache-Control** 応答ヘッダーとは無関係にキャッシュするように Content Gateway を強制できます。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. ページの終わりで **[Edit File]** をクリックして、**cache.config** ファイルの設定ファイル エディタを表示します。
3. 表示されたフィールドに、下記の情報を指定します。
   - **[Rule Type]** ドロップダウン ボックスから、**ttl-in-cache** を選択します。
   - **[Primary Destination Type]** ドロップダウン ボックスから、**url_regex** を選択します。
   - **[Primary Destination Value]** フィールドに、キャッシュを強制する URL を指定します。
   - **[Time Period]** フィールドに、プロキシがキャッシュから URL を処理できる時間を指定します。

     さらに、二次指定子（例、**Prefix**、**Suffix**）をルールに追加できます。すべてのフィールドは*HTTP*、350 ページで説明しています。
4. **[Add]** をクリックし、次に **[Apply]** をクリックします。
5. **[Close]** をクリックします。

HTTP の代替のキャッシング

Help | Content Gateway | バージョン 7.8.x

一部のオリジン サーバーは、種々のオブジェクトが含まれている同一の URL への要求に応答します。これらのオブジェクトのコンテンツは、サーバーが種々の言語のコンテンツを配信するか、種々のプレゼンテーション スタイルを持つ種々のブラウザを対象としているか、または種々のドキュメント フォーマット（HTML、PDF）を提供するかどうかによって異なります。同一のオブジェクトの種々のバージョンを*代替*と言い、**Vary** 応答ヘッダーに基づいて Content Gateway によってキャッシュされます。

Content Gateway が代替をキャッシュする方法の設定

プロキシがキャッシングの代替として識別する特定のコンテンツ タイプに追加的な要求および応答ヘッダーを指定できます。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Vary Based on Content Type（コンテンツ タイプに基づいて変動）]** セクションで、**[Enabled（有効化）]** をクリックして **[Vary]** ヘッダーを含んでいない HTTP ドキュメントの代替バージョンをキャッシュします。
3. プロキシ サーバーが識別する追加的な要求および応答ヘッダーを指定します。
   - **[Vary by Default on Text（テキストの場合にデフォルトで変動）]** フィールドに、テキスト（例、HTML ドキュメント）の要求の場合に変動させる HTTP ヘッダー フィールドを入力します。
   - **[Vary by Default on Images（イメージの場合にデフォルトで変動）]** フィールドに、イメージ（例、**.gif** ファイル）の要求である場合に変動させる HTTP ヘッダー フィールドを入力します。
   - **[Vary by Default on Other Document Types（他のドキュメント タイプの場合にデフォルトで変動）]** フィールドに、テキストまたはイメージ以外の要求の場合に変動させる HTTP ヘッダー フィールドを入力します。

   注意
   上記のフィールドで変動させるヘッダー フィールドとして **[Cookie（クッキー）]** を指定した場合、**[Dynamic Caching]** セクションの **[Caching Response to Cookies]** 領域で適切なオプションが有効化されていることを確認します。たとえば、**[Caching Response to Cookies]** 領域で **[Cache Only Image Types]** オプションを有効化し、**[Vary Based on Content Type]** セクションで **[Vary by Default on Text]** オプションを有効化した場合、クッキーを使用する代替はテキストに適用されません。

4. **[Apply]** をクリックします。

オブジェクトの代替の数の制限

Content Gateway がオブジェクトごとにキャッシュできる代替の数を制限できます。代替のデフォルト数は、3 です。

> **注意**
> 代替の数が大きくなると、すべての代替が同一の URL をもちますからプロキシのパフォーマンスに影響を与える場合があります。Content Gateway は、インデックスに含まれている URL を非常にすばやく検索しますが、オブジェクト ストアに含まれている利用可能な代替を順にスキャンする必要があります。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Maximum Alternates（代替の最大数）]** フィールドに、プロキシがキャッシュするオブジェクトの代替バージョンの最大数を入力します。デフォルト値は 3 です。
3. **[Apply]** をクリックします。

FTP オブジェクトのキャッシング

Help | Content Gateway | バージョン 7.8.x

FTP オブジェクトは、HTTP クライアント（ブラウザなど）から、または FTP クライアント（WS_FTP など）から要求することができます。

HTTP クライアントから要求された FTP オブジェクト（HTTP 上の FTP）の場合、プロキシが何をキャッシュに保存するかを決定するために、下記の設定を実行します。

- HTTP 上の FTP のキャッシングを無効化し、プロキシが HTTP クライアントから要求されたすべての FTP オブジェクトをキャッシュしないようにします（*HTTP 上の FTP キャッシングの無効化*、48 ページを参照）。
- **cache.config** ファイルで never cache ルールを設定します（*cache.config*、450 ページを参照）。
- クライアントの **Cache-Control: no-store** または **Cache-Control: no-cache** ヘッダーを無視するようにプロキシを設定します（*クライアントの no-cache ヘッダーを無視するようにプロキシを設定する*、39 ページを参照）。

FTP クライアントから要求された FTP オブジェクトの場合、キャッシングは、サポートされていません。

HTTP 上の FTP キャッシングの無効化

Help | Content Gateway | バージョン 7.8.x

HTTP 上の FTP オプションを無効化することによって、HTTP クライアントから要求されたすべての FTP オブジェクトをキャッシュしないように Content Gateway を設定できます。プロキシは要求を FTP サーバーに転送することによってそれらの要求を処理しますが、要求されたすべてのオブジェクトをキャッシュしません。

1. **[Configure] > [Protocols] > [HTTP] > [Cacheability]** に移動します。
2. **[Caching]** セクションで、**[FTP over HTTP Caching（HTTP 上の FTP のキャッシング）]** を無効化します。
3. **[Apply]** をクリックします。

4 明示的プロキシ

Help | Content Gateway | バージョン 7.8.x

インターネット要求が透過的に Layer 4 スイッチまたはルータを経由して Content Gateway へとルーティングされていない場合（*透過的プロキシと ARM*、61 ページを参照）、クライアントのインターネット ブラウザを設定することによってトラフィックを Content Gateway に**明示的に**ルーティングする必要があります（これを*明示的プロキシ環境*と言います）。

クライアントは下記の 3 つのいずれかの方法で Web ブラウザを設定できます。

- ブラウザが直接にプロキシに要求を送信するように、ブラウザを直接に設定する。*手動でのブラウザの設定*、50 ページを参照してください。
- ブラウザが PAC (Proxy Auto-Config) ファイルからプロキシ設定の指示をダウンロードするように設定する。*PAC ファイルの使用*、51 ページを参照してください。
- WPAD (Web Proxy Auto-Discovery Protocol) を使用して、WPAD サーバーからプロキシ設定の指示をダウンロードするようにする（Microsoft Internet Explorer のみ）。*WPAD の使用*、53 ページを参照してください。

また、Content Gateway が FTP トラフィックをプロキシに転送するように設定されている場合、FileZilla や WS_FTP などの FTP クライアント アプリケーションは、明示的にプロキシに要求を送信するように設定されている必要があります。*明示的プロキシ環境での FTP クライアントの設定*、54 ページを参照してください。

手動でのブラウザの設定

Help | Content Gateway | バージョン 7.8.x

ブラウザが Content Gateway に要求を送信するように設定するには、クライアントは、プロキシによる処理を希望する各プロトコルついて以下の情報を提供する必要があります。

- プロキシのホスト名または IP アドレス。

  重要

  ユーザー認証のために統合 Windows 認証が設定されている場合、Fully Qualified Domain Name（完全修飾ドメイン名）を使用する必要があります。IP アドレスを指定すると、認証が失敗します。*統合 Windows 認証*、225 ページを参照してください。

- プロキシ サーバー ポート。Content Gateway のデフォルトのサーバー ポートは 8080 です。

  重要

  Content Gateway プロキシの IP アドレスを仮想 IP アドレスに設定してはいけません。

  Content Gateway Manager は仮想 IP アドレスの入力を禁じていませんが、VIP を使用した場合プロキシは適切に機能しません。

また、クライアントは特定のサイトに対してはプロキシを使用しないように指定できます。リストされたサイトへの要求は直接にオリジン サーバーに送信されます。

Microsoft Internet Explorer バージョン 7.0 以上の場合、プロキシ設定は **[Tools] > [Internet Options（インターネット オプション）] > [Connections（接続）] > [LAN Settings（LAN の設定）]** に含まれています。デフォルトでは Microsoft Internet Explorer は、すべてのプロトコルを同じプロキシ サーバーに設定します。各プロトコルを別々に設定するには、**[LAN Settings]** セクションに含まれている **[Advanced（詳細設定）]** をクリックします。プロキシ設定の手順の詳細については、ブラウザのマニュアルを参照してください。

Mozilla Firefox 4.0 以上の場合、プロキシ設定は、**[Tools] > [Options] > [Advanced] > [Network] > [Settings（設定）] > [Connection Settings（接続設定）] > [Manual Proxy Configuration（手動のプロキシ設定）]** に含まれています。デフォルトでは、各プロトコルを個別に設定する必要がありあます。しかし、**[Use this proxy server for all protocols（このプロキシ サーバーをすべてのプロトコルに使用）]** を選択することによって、すべてのプロトコルを同じサーバーに設定できます。

手動で設定したブラウザからの要求を受け入れるために、プロキシで設定オプションを設定する必要はありません。

PAC ファイルの使用

Help | Content Gateway | バージョン 7.8.x

PAC ファイルは、ブラウザが要求を処理する方法を決定するために呼び出す JavaScript 関数定義です。クライアントは自分のブラウザ設定の中で、PAC ファイルをロードする URL を指定する必要があります。

PAC ファイルをプロキシに保存し、このファイルの URL をクライアントに提供できます。**proxy.pac** ファイルがある場合は、それを Content Gateway の **config** ディレクトリにコピーします。

> **注意**
>
> PAC ファイルはネットワーク内のどのサーバーにも常駐できます。
>
> HTTPS プロトコル オプションを有効化している場合、HTTPS トラフィックに使用する PAC ファイルの詳細について、*明示的プロキシ モードでの実行*、161 ページを参照してください。

1. 既存の **wpad.dat** ファイルがある場合、Content Gateway の **config** ディレクトリに含まれている **wpad.dat** ファイルを既存のファイルに置き換えます。
2. **[Configure]** > **[Content Routing（コンテンツ ルーティング）]** > **[Browser Auto-Config（ブラウザ自動設定）]** > **[PAC]** タブに移動します。
3. **[Auto-Configuration Port（ポートの自動設定）]** フィールドで、Content Gateway が PAC ファイルを提供するために使用するポートを指定します。デフォルト ポートは 8083 です。

4. [PAC Settings（PAC 設定）] 領域に **proxy.pac** ファイルが表示されます。
   - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーした場合、**proxy.pac** ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
   - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーしていない場合は、[PAC Settings] 領域は空です。プロキシ サーバーの設定を提供するスクリプトを入力します。サンプルのスクリプトを*サンプルの PAC ファイル、52 ページ*に示しています。Websense Technical Library の [PAC File Best Practices] という表題の記事も参照してください。
5. **[Apply]** をクリックします。
6. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。
7. ユーザーに、ブラウザがこの PAC ファイルを選択するように設定するよう指示します。

   たとえば、PAC ファイルが置かれているプロキシ サーバーのホスト名が **proxy1** であり、Content Gateway がデフォルト ポート 8083 を使用してファイルを提供する場合、ユーザーはプロキシ設定で下記の URL を指定する必要があります。

   ```
   http://proxy1.company.com:8083/proxy.pac
   ```

PAC ファイルの場所の指定の手順はブラウザによって異なります。たとえば、Microsoft Internet Explorer の場合、**[Tools] > [Internet Options] > [Connections] > [LAN Settings]** から **[Use automatic configuration script（自動設定スクリプトを使用）]** で PAC ファイルの場所を設定します。Mozilla Firefox の場合、プロキシの設定は、**[Tools] > [Options] > [Advanced] > [Network] > [Settings] > [Connection Settings] > [Automatic proxy configuration URL（手動のプロキシ設定 URL）]** に含まれています。詳細についてはご使用のブラウザのマニュアルを参照してください。

サンプルの PAC ファイル

Help | Content Gateway | バージョン 7.8.x

以下のサンプル PAC ファイルは、ブラウザに対して、完全に修飾されたドメイン名のないすべてのホスト、およびローカル ドメインに含まれているすべてのホストに直接に接続するよう指示します。他のすべての要求は、**myproxy.company.com** という名前のプロキシ サーバーに送られます。

```
function FindProxyForURL(url, host)
{
if (isPlainHostName(host) || dnsDomainIs(host,
".company.com"))
return "DIRECT";
else
return "PROXY myproxy.company.com:8080; DIRECT";
}
```

WPAD の使用

Help | Content Gateway | バージョン 7.8.x

Internet Explorer バージョン 7 以上で WPAD を使用すると、プロキシ サーバーの設定を提供するサーバーを自動的に検出できます。クライアントは、ブラウザがプロキシ サーバに要求を送信するように設定する必要はありません。1 つのサーバーがネットワーク上のすべてのクライアントに設定を提供します。

> **注意**
> WPAD は、透過的プロキシ環境に適合します。

Internet Explorer バージョン 7 以上のブラウザは、起動時に、プロキシ サーバーの設定を提供する WPAD サーバーを検索します。このサーバーの現在の完全修飾ドメイン名の前にホスト名 WPAD を付けます。たとえば、**x.y.company.com** に含まれるクライアントは **wpad.x.y.company.com** にある WPAD サーバーを検索します。検索が失敗した場合、ブラウザは最下位のドメインを削除し、再度検索を試みます。たとえば **wpad.y.company.com** で検索します。ブラウザは、WPAD サーバーを検出したとき、または 3 番目のレベルのドメイン **wpad.company.com** に達したとき、検索を中止します。このアルゴリズムは 3 番目のレベルで停止しますから、ブラウザは現在のネットワークの外側を検索しません。

> **注意**
> デフォルトでは、Microsoft Internet Explorer バージョン 7 以上は自動的に WPAD サーバーを検出するように設定されています。しかし、ブラウザ ユーザーはこの設定を無効化することができます。

Content Gateway を WPAD サーバーとして使用するように設定できます。

1. 既存の **wpad.dat** ファイルがある場合、Content Gateway の **config** ディレクトリに含まれている **wpad.dat** ファイルを既存のファイルに置き換えます。
2. Content Gateway Manager にログオンし、**[Configure] > [Content Routing] > [Browser Auto-Config] > [WPAD]** に移動し、**wpad.dat** ファイルを表示します。
3. [WPAD Settings（WPAD の設定] 領域に **wpad.dat** ファイルが表示されます。
   - 既存の **wpad.dat** ファイルを Content Gateway の **config** ディレクトリにコピーした場合、ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
   - 既存の **wpad.dat** ファイルを Content Gateway の **config** ディレクトリ (/opt/WCG/config) にコピーしていない場合は、[WPAD Settings] 領域は空です。プロキシ サーバーの設定を提供するスクリプトを入力しま

す。サンプル スクリプトを*サンプルの PAC ファイル、52 ページ*に示しています（**wpad.dat** ファイルは **proxy.pac** ファイルと同じスクリプトを含むことができます）。

4. **[Apply]** をクリックします。
5. **[Configure]** > **[Networking]** > **[ARM]** に移動します。
6. **[Network Address Translation (NAT)（ネットワーク アドレス変換）]** セクションで **[Edit File（ファイルを編集）]** をクリックし、**ipnat.conf** ファイルに特別のリマップ ルールを追加します。
7. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。
   - **[Ethernet Interface（イーサネット インターフェース）]** フィールドに、ブラウザからの WPAD 要求を受け取るネットワーク インターフェース（例、hme0 or eth0）を入力します。
   - **[Connection Type]** ドロップダウン リストから **tcp** を選択します。
   - **[Destination IP]** フィールドに Content Gateway サーバーの IP アドレスを入力します。この IP アドレスは、ローカル名前サーバーの後に /32 を付けることによって WPAD サーバー名に解決されます。123.456.7.8/32。
   - **[Destination Port]** フィールドに、**80** と入力します。
   - **[Redirected Destination IP（リダイレクト宛先 IP）]** フィールドに **[Destination IP]** フィールドで入力した同じ IP アドレスを、/32 を省いて入力します。
   - **[Redirected Destination Port（リダイレクト宛先ポート）]** フィールドに **8083** と入力します。
8. **[Add]** をクリックします。
9. 左側の矢印キーを使用して新しい規則をファイルの最初の行に移動します。
10. **[Apply]** をクリックし、次に **[Close]** をクリックします。
11. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** を順に選択して、**[Restart]** をクリックします。

明示的プロキシ環境での FTP クライアントの設定

Help | Content Gateway | バージョン 7.8.x

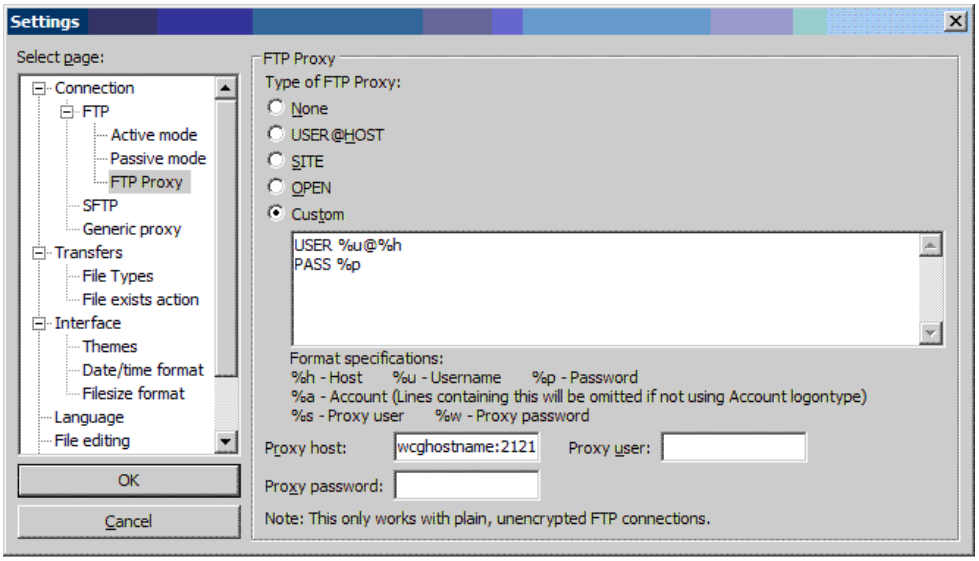
Content Gateway が FTP トラフィックをプロキシに転送するように設定されている場合（*FTP、367 ページ*を参照）、FileZilla や WS_FTP などの FTP クライアント アプリケーションは、明示的にプロキシに要求を送信するように設定されている必要があります。そのように設定した場合、FTP クライアント アプリケーションをプロキシが存在しないかのように使用できます。

FTP サーバーに接続するには、通常、下記の 4 つの情報が必要です。これらの情報は、下記のようにマップされます。

マップ元：	マップ先：
FTP サーバー ホスト名	FTP **プロキシ** ホスト名
FTP サーバー ポート番号	FTP **プロキシ** ポート番号（デフォルトは 2121）
FTP サーバー ユーザー名	FTP_server_username@FTP_server_hostname 例：anon@ftp.abc.com
FTP サーバー パスワード	FTP サーバー パスワード

一部の FTP クライアント アプリケーションには、FTP プロキシ情報を指定するための設定ページがあります。これらの設定を Content Gateway FTP プロキシを指定するように更新します。ご使用の FTP クライアント アプリケーションのマニュアルを参照してください。

これは FileZilla の最新のバージョンを使った設定の例です。



[FTP Proxy] 領域で下記の手順を実行します。

1. **[FTP Proxy]** を **[Custom（カスタム）]** に設定し、上記のように USER および PASS を指定します。
2. **[Proxy host（Proxy ホスト）]** を Content Gateway の FTP プロキシ ホスト名およびポート番号に設定します。
3. **[OK]** をクリックして設定を適用します。

次に、通常の、プロキシが存在しない場合と同様の方法で FTP 接続情報を入力します。例：

Host: ftp.example.com

Username: anon

Password: 123abc

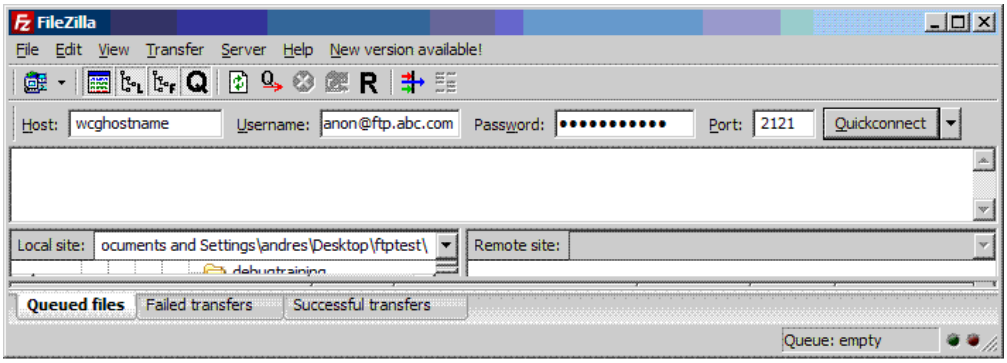
FTP クライアント アプリケーションが設定されて**いない**場合、下記のように FTP 要求を入力する必要があります。

Host: Content Gateway の プロキシ ホスト名

Username: anon@ftp.example.com

Password: 123abc

Port: 2121



IPv6 のサポート

Help | Content Gateway | バージョン 7.8.x

TRITON Enterprise のバージョン 7.7（Content Gateway プロキシ コンポーネントを含む）は、IP v 6 の増分サポートを提供します。

重要

サポートは、明示的プロキシ環境の場合のみ提供されます。

Content Gateway による IPv6 のサポートは、下記を含みます。

- デュアル IP スタック イーサネット インタフェース上の IPv6
- 次のプロトコルをサポートします：HTTP、HTTPS、FTP、DNS
- インターネット、クライアント、および PAC ファイル サーバーへの IPv6 トラフィック
- IPv6 仮想 IP アドレス (vaddrs.config)
- クライアント IPv6 アドレス範囲に基づく認証ルール
- プロキシへのアクセスを許可または禁止するクライアント IPv6 アドレスおよびアドレス範囲 (ip_allow.config)
- Content Gateway Manager へのアクセスを許可または禁止するクライアント IPv6 アドレスおよびアドレス範囲 (mgmt_allow.config)
- プロキシ フィルタリング ルール (filter.config)、キャッシュ ルール (cache.config)、およびチェーンの中の親プロキシ サーバー (parent.config) に含まれる IPv6 一次宛先値および送信元 IP 値
- SSL Incident List（インシデント リスト） に含まれる IPv6 アドレス
- IPv6 データに対する SNMP トラップおよびカウンタ

制限と制約：

- IPv6 専用の内部ネットワークはサポートされません。
- Content Gateway クラスタの他のメンバーを含むすべての TRITON コンポーネント間の通信には、IPv4 を使用する必要があります（マルチキャスト アドレス）。

> **注意**
> Content Gateway Manager に組み込まれている記述テキストとは異なり、**マルチキャスト グループ アドレス**は IPv4 でなければなりません（**[Configure] > [My Proxy] > [Basic] > [Clustering（クラスタ化）]**）。

- すべてのユーザー認証で、Domain Controller が IPv4 アドレスでアクセスできなければなりません。
- ARM は IPv6 アドレスをサポートしません。これはリダイレト ルール (ipnat.config) および静的バイパス ルール (bypass.config) においてもです。
- チェーンの中の親プロキシが IPv6 であってはなりません。
- IP スプーフィングはサポートされていません。
- SOCKS プロキシはサポートされていません。

警告

オペレーティング システムが Red Hat Enterprise Linux 6 アップデート 3、または CentOS 6 アップデート 3 である場合は、/etc/resolv.conf に IPv6 ネームサーバーを指定してはいけません。エントリが含まれている場合、Content Gateway は起動を試みるごとにリセットします。ユーザーの環境が IP v 6 ネームサーバーを必要とする場合、オペレーティング システムを Red Hat Enterprise Linux 6 アップデート 4、または CentOS 6 アップデート 4 にアップグレードします。

IPv6 プロキシの統計：

Content Gateway は IPv6 トラフィックを追跡します。**[Monitor] > [Networking] > [System]** ページを順に選択すると統計が表示されます。

IPv6 のイベント ログへの影響

IPv6 を有効化した場合、イベント ログの入力項目が IPv6 フォーマットに標準化されます。たとえば、[10.10.41.200] は、[::ffff:10.10.41.200] とログされます。

カスタム ログの [10.10.41.200] でクライアントをフィルタリングするには、下記のフィルタが必要です。

```
<LogFilter>
   <Name = "IPv6_Test_Machine"/>
   <Condition = "chi MATCH ::ffff:10.10.41.200"/>
   <Action = "ACCEPT"/>
</LogFilter>
```

IPv6 設定のまとめ

IPv6 サポートはデフォルトでは無効化されています。

Content Gateway が Websense Appliance に配備されている場合、最初に Appliance Manager **[Configuration] > [Network Interfaces] > [IPv6]** タブで IPv6 を有効化します。

IPv6 は、Content Gateway Manager の **[Configure] > [My Proxy] > [Basic]** ページの **[Network]** セクションで有効化されます。有効化されたとき、前の項で列挙したすべての機能領域のサポートが有効化されます。

IPv6 アドレスを受け入れるフィールドでは、アドレスを標準に適合する任意の形式で入力できます。例：

- 16 ビット値の中の先頭の 0 を省略できます
- 連続する 0 の 1 つのグループをダブル コロンに置換できます

IPv6 を無効化すると、IPv6 エントリ フィールドは非表示にされ、IPv6 値が設定ファイルから削除されます。

DNS Resolver を使用している場合、**[Configure] > [Network] > [DNS Resolver]** ページに移動し、IPv4 または IPv6 の優先設定を設定します。IPv4 がデフォルトです。

5 透過的プロキシと ARM

Help | Content Gateway | バージョン 7.8.x

透過的プロキシ オプションによって Content Gateway は、クライアントのインターネット要求に対して、ユーザーにブラウザの再構成を要求することなしに応答できます。そのために、トラフィックが遮断された - 多くの場合、レイヤー 4（L4）のスイッチまたはルーターによって - 後で要求のフローをプロキシへ、リダイレクトします。

透過的プロキシ環境

1. プロキシはスイッチまたはルーターによってクライアントからオリジン サーバーへの要求を遮断します。*透過的遮断戦略*、63 ページを参照してください。
2. Adaptive Redirection Module (ARM) は、着信パケットの宛先 IP アドレスをプロキシの IP アドレスに変更し、宛先ポートをプロキシ ポートに変更します（もし異なる場合）。（ARM は常に有効化されます。）
3. プロキシは遮断されたクライアント要求を受信し、処理を開始します。要求がキャッシュ ヒットである場合、プロキシは要求されたオブジェクトを提供します。要求がヒットしない場合、プロキシはオリジン サーバーからオブジェクトを取得し、クライアントに対してそれを提供します。
4. クライアントへの応答では、ARM は送信元 IP アドレスをオリジン サーバーの IP アドレスに変更し、送信元のポートをオリジン サーバーのポートに変更します。

重要

複数のインターフェースまたはゲートウェイがある透過的プロキシ構成では、Content Gateway はオペレーティング システムのルーティング テーブルにクライアントおよびインターネットへの適切なルートを確保していなければなりません。

HTTP では、プロキシは問題があるクライアントおよびサーバーを識別でき、ARM はそのようなクライアントおよびサーバーの遮断を無効化し、そのトラフィックを直接にオリジン サーバーへ渡します。また、クライアントおよびサーバーをプロキシへのリダイレクトから除外するための ARM 静的バイパス ルールを作成することもできます。*遮断の迂回、88 ページ*を参照してください。

関連項目：

- *透過的遮断戦略、63 ページ*
- *遮断の迂回、88 ページ*
- *接続負荷の軽減、92 ページ*
- *DNS ルックアップの削減、92 ページ*
- *IP スプーフィング、94 ページ*

ARM

Help | Content Gateway | バージョン 7.8.x

Content Gateway ARM は着信パケットを、IP レイヤーがそれを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更します。

ARM は着信パケット アドレスに 2 つの変更を行うことができます。その宛先 IP アドレスと宛先ポートを変更できます。たとえば、HTTP パケットの宛先 IP アドレスがプロキシの IP アドレスにアドレス変更され、宛先 HTTP ポートが Content Gateway HTTP プロキシ ポート（通常はポート 8080）にアドレス変更されます。

クライアントへの応答では、ARM は送信元 IP アドレスをオリジン サーバーの IP アドレスに変更し、送信元のポートをオリジン サーバーのポートに変更します。

ARM コンポーネントはいくつかのファイルと 1 つのカーネル モジュールから成り、製品インストール時にインストールされます。インストール プログラムはまた、プロキシ コンピュータの IP アドレスとデフォルトのポート割り当てを使って、パケットのアドレス変更を行うリダイレクト ルールを作成することができます。ARM は常にアクティブです。

プロキシが HTTP、HTTPS、FTP、または DNS 要求を透過的に処理するためには、**ipnat.conf** ファイルの中のリダイレクト ルールを確認し、必要に応じて変更する必要があります。WCCP を使って透過的な遮断を行う場合、すべてのアクティブ サービス グループですべてのポートに対してリダイレクト ルールが設定されていなければなりません。デフォルトでは、標準ポートに対するルールが設定されています。ARM リダイレクト ルールを表示し、処理するには、以下の手順を実行します。

1. Content Gateway Manager にログオンし、**[Configure（設定）] > [Networking（ネットワーキング）] > [ARM] > [General（一般）]** タブへ移動します。

   [Network Address Translation (NAT)（ネットワーク アドレス変換 (NAT)）] セクションに **ipnat.conf** ファイルの中のリダイレクト ルールが表示されます。リダイレクト ルールを確認し、必要な変更を行います。

   a. リダイレクト ルールを変更するには、**[Edit File（ファイルの編集）]** をクリックして、**ipnat.conf** ファイルの編集のための設定ファイル エディタを開きます。

   b. 編集するルールを選択し、変更対象のフィールドを編集および変更します。**[Set（設定）]** をクリックし、次に **[Apply（適用）]** をクリックして変更を適用します。設定ファイル エディタを終了するためには、**[Close（閉じる）]** をクリックします。

   すべてのフィールドは *ARM、411 ページ*で説明されています。

2. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

透過的遮断戦略

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は、以下の透過的遮断ソリューションをサポートします。

- レイヤー 4 スイッチ。*レイヤー 4 スイッチによる透過的遮断、64 ページ*を参照してください。
- WCCP v2 をサポートするルーターとスイッチ。Cisco IOS ベースのルーターが最も一般的です。*WCCP v2 デバイスによる透過的遮断、65 ページ*を参照してください。
- ポリシー ベースのルーティング*透過的遮断とマルチキャスト モード、84 ページ*を参照してください。
- ソフトウェア ルーティング *ソフトウェア ベースのルーティングによる透過的遮断、86 ページ*を参照してください。

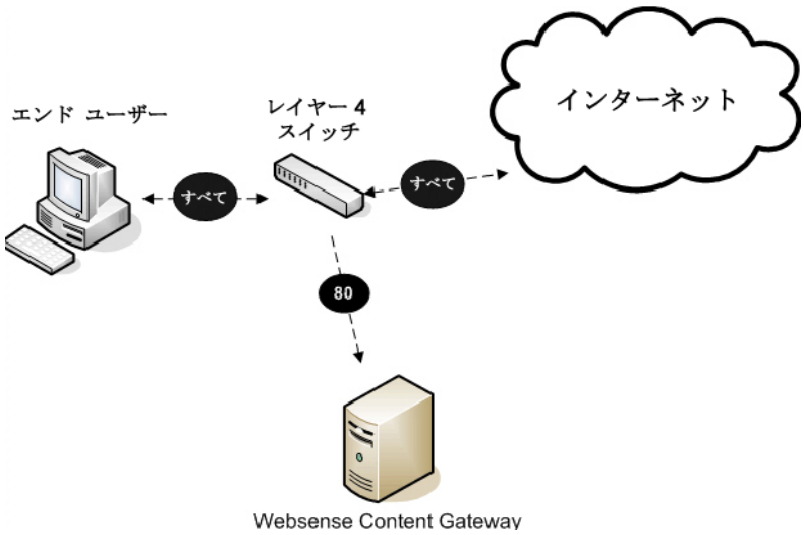
クライアント要求がプロキシに到達する経路はネットワーク トポロジーに依存します。複合的なネットワークでは、どのクライアントを透過的に処理するかを決定し、そのネットワーク デバイスとプロキシがその要求を遮断するように配置されていることを確認する必要があります。Content Gateway または Content Gateway に接続しているルーターまたはスイッチは多くの場合、インターネットへの幹線または集約パイプ上に配置されています。

透過的トラフィックのみを処理するように Content Gateway を設定する方法については、*Content Gateway が透過的要求のみ処理するように設定する、87 ページ*を参照してください。

レイヤー 4 スイッチによる透過的遮断

Help | Content Gateway | バージョン 7.8.x

レイヤー 4 スイッチはサポートされているプロトコルをプロキシにリダイレクトし、他のすべてのインターネット トラフィックをその宛先に直接に渡します（HTTP について、下図に示しています）。



レイヤー 4 スイッチは、スイッチのタイプに応じて、以下の機能を提供します。

- ネットワーク上の停止しているホストを検知し、トラフィックをリダイレクトできるレイヤー 4 スイッチは、信頼性を向上させます。
- 1 つのレイヤー 4 スイッチが複数のプロキシ サーバーに接続している場合、スイッチは Content Gateway ノードの間でのロード バランシングを処理します。スイッチの種類によってロード バランシングの方法（ラウンドロビン、ハッシュなど）が異なります。ノードが使用不可能になった場合、スイッチは負荷を再配分します。ノードが復旧したとき、いくつかのスイッチがノードを元の作業負荷に戻しますから、ノード キャッシュを再ポピュレートする必要はありません。この機能を*キャッシュ アフィニティー*と言います。

> **注意**
> クラスタ構成でスイッチがロード バランシングを提供している時は、Content Gateway の仮想 IP フェールオーバーを**有効化しない**ことを推奨します。

WCCP v2 デバイスによる透過的遮断

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *WCCP の負荷配分、68 ページ*
- *WCCP v2 ルーターの構成、70 ページ*
- *Content Gateway で WCCP v2 を有効化します、76 ページ*
- *ARM 迂回と WCCP、68 ページ*

Content Gateway は、WCCP v2 対応のルーターおよびスイッチによる透過的遮断をサポートします。

HTTP、HTTPS、FTP、および DNS プロトコルがサポートされています。標準ポートには HTTP、HTTPS、および FTP のためのデフォルトの ARM リダイレクト ルールが含まれています。

セットアップの概要の後に、*WCCP v2 でサポートされている機能*のリストを示しています。

重要

ネットワーク クライアント、Content Gateway プロキシ サーバー、宛先 Web サーバー（デフォルト ゲートウェイ）は別々のサブネット上に常駐していなければなりません。

以下は WCCP v2 のセットアップの概要です。

1. WCCP v2 デバイスをインストールし、システム設定します。
   各 WCCP v2 デバイスに対して、以下のことを行います。
   - サービス グループを設定します。
   - 必要なら、パスワード セキュリティを設定します。
   - 必要なら、マルチキャスト通信を設定します。

   *WCCP v2 ルーターの構成、70 ページ*を参照してください。

2. Content Gateway を WCCP デバイスとともに使用できるように設定します。
   - 対応するサービス グループを定義します。

     ネットワーク インターフェース、プロトコル、ポート、認証（使用する場合）、およびマルチキャスト通信（使用する場合）のほかに、下記を設定します。
     - WCCP v2 デバイスの IP アドレス。
     - Packet Forward Method（パケット転送方法）と Packet Return Method（パケット返送方法）。
     - Content Gateway がクラスタ内に配備されている場合（必要な場合）、**assignment method（割り当て方法）**による負荷の配分
   - 非標準ポートのための ARM NAT ルールを作成します。

   *Content Gateway で WCCP v2 を有効化します、76 ページ*および *ARM、62 ページ*を参照してください。
3. テスト トラフィックを使って構成を検証します。

WCCP v2 でサポートされている機能

Content Gateway は、以下の WCCP v2 機能をサポートします。

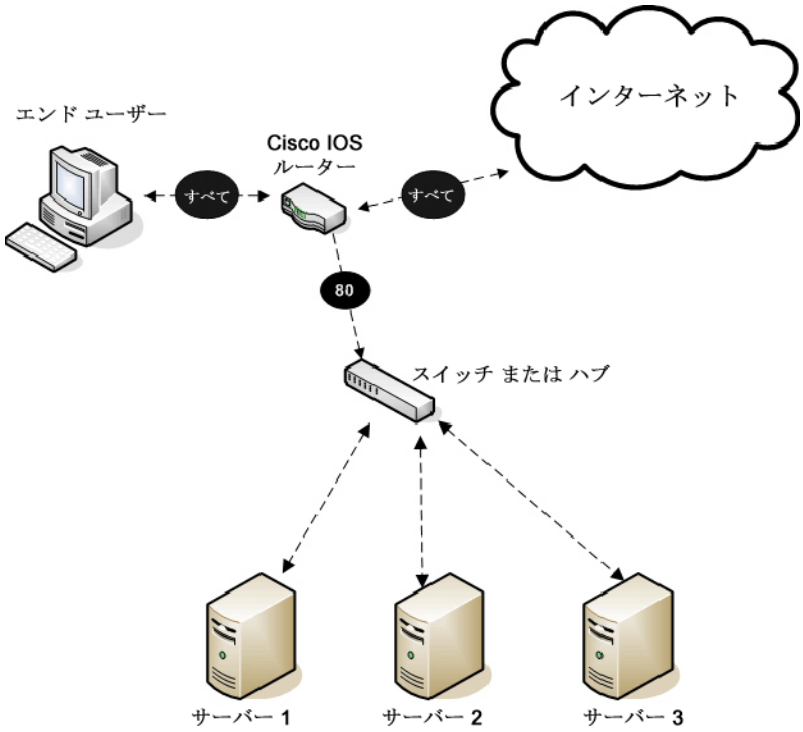
- 1 つのプロキシ クラスタ内の複数のルーター
- 1 つのサービス グループに複数のポート
- 1 つのプロトコルに複数のサービス グループ異なる WCCP デバイスに異なるサービス グループを割り当てる必要がある、またはそうすることが便利である場合があります。たとえば、Cisco ASA ファイアウォールでは、ネットワーク内の WCCP デバイスごとに異なるサービス グループが必要とされます。
- **assignment method** HASH または MASK によるクラスタ内の動的負荷配分。*WCCP の負荷配分、68 ページ*を参照してください。
- Packet Return Method および Packet Forward Method ネゴシエーション
- サービス グループごとの MD5 パスワード セキュリティ
- マルチキャスト モード

Content Gateway クラスタでは、WCCP 環境で仮想 IP フェールオーバーを**有効化しない**ことを推奨します。WCCP v2 および Content Gateway の設定は、ノードの障害および再起動を処理します。（*WCCP の負荷配分、68 ページ*および *仮想 IP フェールオーバー、108 ページ*を参照。）

Content Gateway はまた、キャッシュ アフィニティをサポートします。ノードが使用不可能になり、その後復旧したとき、ノード キャッシュを再ポピュレートする必要はありません。

WCCP v2 遮断の仕組み

1. WCCP v2 デバイスは、サービス グループの設定に従って、プロキシ サーバーまたはサーバーのクラスタに HTTP、HTTPS、FTP および DNS トラフィックを送信します。
2. ARM はトラフィックのアドレスを変更します。たとえば、ポート 80 上の HTTP トラフィックは、Content Gateway ポート 8080 にアドレス変更されます。
3. プロキシは通常通りに要求を処理し、クライアントに応答を返送します。
4. ARM は応答ヘッダの中のプロキシ ポートをポート 80 にアドレス変更します（プロキシへの転送の際に行ったアドレス変更を元に戻す）。その結果、ユーザーには、応答があたかもオリジン サーバーから直接に送信されたかのように示されます。



ARM 迂回と WCCP

Help | Content Gateway | バージョン 7.8.x

Content Gateway に ARM 迂回ルール（*遮断の迂回*、88 ページを参照）がある場合、Content Gateway は特定のクライアント要求を直接にオリジン サーバーに転送します。

ARM は迂回された要求を変更せず、クライアントの送信元 IP アドレスはそのまま保持されます。

WCCP v2 では、特定のルーター インターフェースをリダイレクトから除外することができます。**Content Gateway ARM バイパス ルールは、Content Gateway が接続されているルーター インターフェースを WCCP リダイレクトから除外している場合にのみ機能します**。そのためには、Content Gateway に接続しているインターフェースを選択し、ルーター設定コマンド **ip wccp redirect exclude in** を発行します。これによってルーターは指定したインターフェース上での着信トラフィックをすべてのリダイレクト ルールから除外します。

WCCP の負荷配分

Help | Content Gateway | バージョン 7.8.x

WCCP プロトコルはクラスタ内の動的対称および非対称負荷配分の **assignment method** を提供します。WCCP は、ノードの障害を検出し、Content Gateway によって通知された設定をもとに再配分を実行します。

- 負荷配分は Content Gateway Manager で設定され、WCCP デバイスにプッシュされます。
- 負荷配分は**サービス グループごとに**設定されます。

  各サービス グループで、以下のように設定します。
  - 関係するクラスタ メンバーは、サービス グループに登録されていなければなりません。（WCCP デバイスはロード バランシングについて何も決定しません。）
  - assignment method として HASH または MASK を選択します。HASH は一般的には GRE forward/return method と共に使用し、MASK は L2 forward/return method と共に使用します。

> **重要**
>
> MASK は Cisco Catalyst シリーズ スイッチのために特に開発されており、これらのプラットフォーム上のハードウェアで WCCP 遮断の適切な実行を可能にする主要な特性の 1 つです。これはサポートが文書化されているデバイスでのみ使用します。

- 1 つ以上の**配分属性**を選択します。一般的には、宛先の IP アドレスを使用します。
- 負荷を異なるクラスタ メンバーに異なる割合で配分する場合は、各クラスタ メンバーに **weight** の値を設定します。この値は、それぞれのメンバーが受け取る要求の割合を、他のメンバーのそれに対する相対的な値で指定します。このオプションは **Synchronize in the Cluster** オプションが無効化されている場合のみ有効です。*Content Gateway Manager でのサービス グループの設定、77 ページ*を参照してください。

  weight の値を使用する非対称的負荷配分は、次のような場合に便利です。

  - 処理能力が異なる複数の Content Gateway サーバー（例、V シリーズ V10000 G2 と V10000 G3）を使用する。
  - 特定のオリジン サーバー（および宛先 IP アドレス）を優先するために、インターネット トラフィック プロファイルが均等な配分に適さない。

動的再配分の仕組み

WCCP デバイスがクラスタ メンバーがオフラインであることを検出した時に、動的再配分が実行されます。このとき、WCCP デバイスは自動的に、負荷配分の設定をもとに、残りのクラスタ メンバーに負荷を再配分します。クラスタ メンバーが復旧し、WCCP デバイスによって検出されたとき、再び、その設定をもとに負荷配分が自動的に再調整されます。

設定の手順については*Content Gateway Manager でのサービス グループの設定、77 ページ*を参照してください。

weight 値による非対称負荷配分の仕組み

> **重要**
>
> **Weight** は、**Synchronize in the Cluster** オプションが**無効化**されている場合のみ有効です。*Content Gateway Manager でのサービス グループの設定、77 ページ*を参照してください。

weight 値は、各サービス グループおよびノードに固有です。weight 値はクラスター全体に適用されるのではなく、クラスタ内の各ノードに対して個別に設定する必要があります。

weight の値は、他のクラスタ メンバーに対する設定に対する相対的な値であり、WCCP がそのノードに転送するトラフィックの割合を決定します。

デフォルトでは、weight は 0 に設定されています。この場合、トラフィックはすべてのクラスタ メンバーに均等に配分されます。

非対称負荷配分を実行するためには、weight 値をクラスタ内の他のメンバーの値に対する相対的値として設定します。たとえば、クラスタに 3 つのノードが含まれるとします。

Node（ノード）	weight 値	負荷配分
Node1	50	50%
Node2	25	25%
Node3	25	25%

Node1 がオフラインになった場合、Node2 と Node3 が同じ量のトラフィックを受け取ります。Node3 がオフラインになった場合、Node1 はトラフィックの 3 分の 2 を受け取り、Node2 はトラフィックの 3 分の 1 を受け取ります。

weight 値は他のクラスタ ノードに設定されている値に対する相対的な値ですから、weight 値がそれぞれ 10、5、5 でも同じ配分が得られます（weight 値の範囲は 0-255 です）。

weight をデフォルト値の 0 から変更する場合、クラスタ内のすべてのノードに対して weight 値を設定する必要があります。

WCCP v2 ルーターの構成

Help | Content Gateway | バージョン 7.8.x

WCCP v2 の構成と処理能力に関する情報について、マニュアルおよび製造業者のサポート サイトを参照することを強く推奨します。

大部分のデバイスを、ハードウェア ベースのリダイレクトを最大限に活用するように構成する必要があります。

Cisco デバイスでは、通常は IOS の最新バージョンが最も適切です。

WCCP v2 デバイスをプロキシとともに使用するように準備するには、以下のことを行います。

1. 使用するプロトコルに対して、1 つ以上のサービス グループを設定します。1 つのサービス グループは 1 つ以上のプロトコルを処理できます。*WCCP デバイス上のサービス グループを設定します、71 ページ*を参照してください。
2. これらのサービス グループに対する WCCP 処理を可能にするようにルーターを設定します。*サービス グループに対する WCCP 処理の有効化、72 ページ*を参照してください。
3. 任意に、ルーターのセキュリティを有効化します。Content Gateway 内のサービス グループに対してもルーターのセキュリティを有効化しなければなりません。*ルーター上での WCCP v2 セキュリティの有効化、75 ページ*を参照してください。

> **注意**
> 使用しているルーターの構成に関する指示は、ハードウェア ベンダーによるマニュアルを参照してください。Cisco ルーターについては http://www.cisco.com/cisco/web/psa/default.html?mode=prod を参照し、ご使用の IOS およびデバイスのバージョンを検索してください（例、IOS 12.4）。

4. ルーターの構成が完了したとき、Content Gateway Manager で WCCP を設定し、有効化しなければなりません。*Content Gateway Manager での WCCP v2 の有効化、77 ページ*を参照してください。

WCCP デバイス上のサービス グループを設定します

Help | Content Gateway | バージョン 7.8.x

WCCP は、**サービス グループ**を使って、Content Gateway（および他のデバイス）にリダイレクトするトラフィックを指定します。

サービス グループは、

- 1 つ以上のポート上で、
- 1 つ以上のプロトコルを遮断できます。

サービス グループには 0 ～ 255 の範囲の固有の整数の識別子 (ID) が割り当てられます。

サービス グループ ID はユーザー定義であり、デフォルトのポートまたはトラフィック タイプはありません。

下の表は、ネットワーク内でよく使用されるサービス グループ定義のセットを示しています。IP スプーフィングを設定する場合、*IP スプーフィング、94 ページ*の表に示している、よく使用されるリバース サービス グループ ID を参照してください。

サービス ID	ポート	トラフィック タイプ
0	80	HTTP
5	21	FTP
70	443	HTTPS（HTTPS サポートが有効化されている場合）

サービス グループは、ルーター上、および Content Gateway 内で設定しなければなりません。

最善の方法は、ルーターを先に設定し、次に Content Gateway を設定することです。

詳細についてはルーターのマニュアルに従ってください。一般的には、下記のように行います。

1. ルーターで WCCP に対して何が設定されているかを確認するために、次のように入力します。

   ```
   show running-config | include wccp
   ```

2. WCCP v2 を有効にするために、次のように入力します。

   ```
   ip wccp version 2
   ```

3. ルーターで、Content Gateway の前に別のプロキシ キャッシュを使用した場合、前に使用したサービス ID を無効化します。たとえば、Cisco ルーターを使用している場合、下記のコマンドを発行することによってサービス ID **web-cache** を無効化します。

   ```
   no ip wccp web-cache
   ```

4. Content Gateway で使用するサービス グループ ID を指定します。使用するコマンドについては、ルーターのマニュアルを参照してください。

   ルーターによってサポートされている各サービス グループを個別に設定しなければなりません。ルーターを一括で設定することはできません。

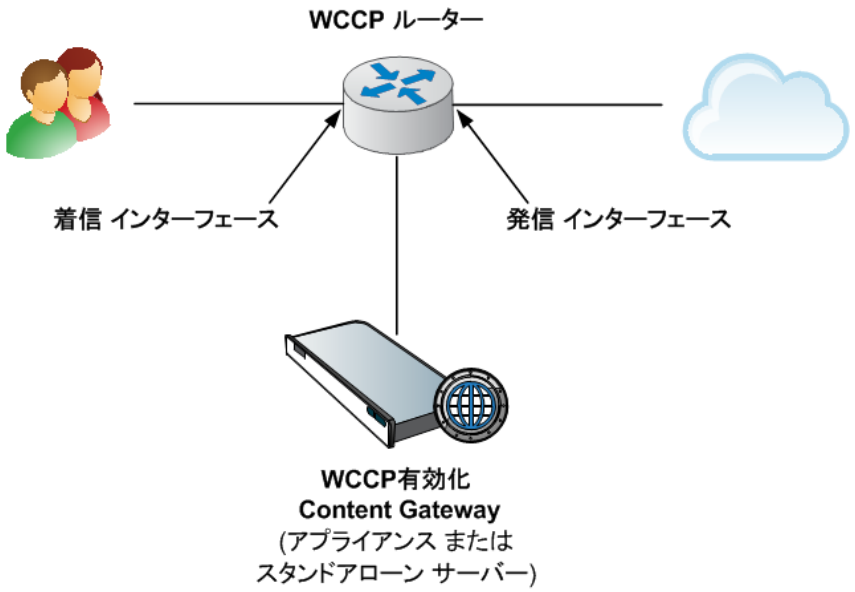
サービス グループに対する WCCP 処理の有効化

Help | Content Gateway | バージョン 7.8.x

設定するそれぞれの WCCP v2 サービス グループに対して、WCCP 処理を有効化しなければなりません。

WCCP v2 ルーターは、下記のような複数のネットワーク インターフェースを含んでいます。

- 着信 (ingress) クライアント トラフィックを受信する 1 つ以上のインターフェース
- Content Gateway に接続している 1 つ以上のインターフェース
- インターネットに向けた発信 (egress) トラフィックのための専用のインターフェース



以下は、ルーター上のサービス グループのための WCCP 処理を有効化するためのいくつかのガイドラインです。詳細についてはルーターのマニュアルの手順を参照してください。

1. WCCP 機能をオンにします。

   ```
   ip wccp <service group ID> password [0-7] <passwd>
   ```

2. ルーターまたはスイッチ インターフェース上で、着信 (ingress) パケットまたは発信 (egress) パケットのリダイレクトを有効化します。

> **注意**
> ハードウェアおよびネットワーク トポロジによってサポートされている場合、ingress インタフェース上でリダイレクトを実行する（[redirect in] コマンドを使用）ことを推奨します。

以下は例です。必ずルーター上で指定したサービス グループ ID に置換してください。

はじめに、設定するインターフェースを選択します。

```
interface <type> <number>
```

次に、リダイレクト ルールを設定します。

```
ip wccp <service group ID> redirect in
```

着信リダイレクトの例

以下のコマンドは、サポートする各プロトコルに対して、**ただし、着信 (ingress) トラフィック**専用のインターフェース上でのみ実行します。

たとえば、HTTP 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 0 redirect in
```

HTTPS 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 70 redirect in
```

FTP 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 5 redirect in
```

HTTP 送信元ポート トラフィックのリダイレクトをオンにする - IP スプーフィングのために必須 - には、下記のように入力します。

```
ip wccp 20 redirect in
```

発信 **(egress) リダイレクト**の例：

以下のコマンドは、サポートする各プロトコルに対して、**ただし、発信 (egress) トラフィック**専用のインターフェース上でのみ実行します。

はじめに、設定するインターフェースを選択します。

```
interface <type> <number>
```

次に、リダイレクト ルールを設定します。

```
ip wccp <service group ID> redirect out
```

たとえば、HTTP のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 0 redirect out
```

HTTPS のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 70 redirect out
```

FTP のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 5 redirect out
```

3. **重要：ARM 動的または静的迂回が有効化されているか IP スプーフィングが有効化されていて、着信 (egress) インターフェース上のリダイレクトがオンになっている時、**Content Gateway の egress トラフィックを処理するルーター インターフェース上での Content Gateway の発信パケットのリダイレクトを除外します。下の図を参照してください。

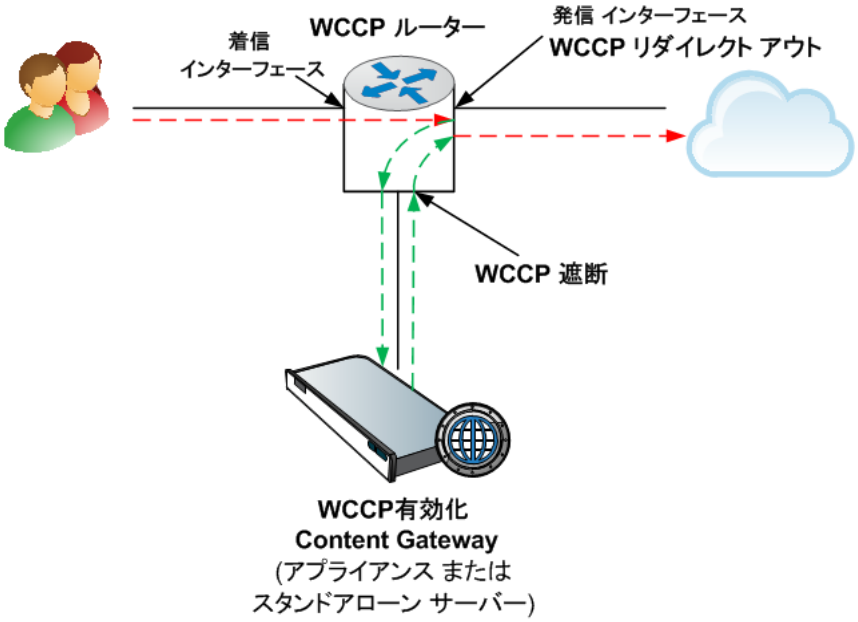
   a. Content Gateway の egress トラフィックを処理するインターフェースを選択します。

      ```
      interface <type> <number>
      ```

   b. このインターフェース上の Content Gateway 発信トラフィックを、ルーター上のすべてのリダイレクト ルールから除外します。

```
ip wccp redirect exclude in
```

ARM 迂回が行われた時、または IP スプーフィングが有効化されている時、プロキシは元の送信元の IP アドレスでトラフィックをインターネットに送信します。[redirect exclude in] コマンドは、ルーターがトラフィックをループに入れて、Content Gateway に戻すのを防止します。



サービス グループに対する WCCP 処理の無効化

Help | Content Gateway | バージョン 7.8.x

何らかの理由で WCCP 処理を無効化する必要がある場合、このコマンドを発行して WCCP 機能をオフにします。

```
no ip wccp <service group ID> password [0-7] <passwd>
```

ルーター上での WCCP v2 セキュリティの有効化

Help | Content Gateway | バージョン 7.8.x

WCCP v2 を実行している場合、Content Gateway ノード上でセキュリティを有効化して、プロキシとルーターが相互に認証できるようにすることができます。ルーターによってサポートされている各サービス グループに対して個別にセキュリティを有効化しなければなりません。Content Gateway の場合とは違って、ルーターを一括で設定することはできません。

セキュリティ オプションの有効化と認証パスワードの提供は、Content Gateway Manager で行います。

遮断する各サービス グループについて、指定する認証パスワードとルーター上で設定されている認証パスワードが一致しなければなりません。以下の手順は、異なるサービス グループに認証パスワードを設定する方法の例です。

1. Telnet でルーターに接続し、Enable モードに切り換えます。
2. プロンプトに対して、下記のコマンドを入力して、端末からルーターを設定します。

   ```
   configure terminal
   ```

3. ルーター上で WCCP を有効化した時にパスワードを定義した場合は、ステップ 4 に進みます。そうでない場合は、ルーターが遮断する各サービス グループに対して、下記のコマンドを入力します。

   ```
   hostname(config)# ip wccp service_group password password
   ```

   ここで、*hostname* は設定しているルーターのホスト名、*service_group* はサービス グループ ID（たとえば、HTTP の場合は 0）、*password* は Content Gateway を認証するために使用するパスワードです。このパスワードは、このサービス グループに対して Content Gateway 設定の中で指定したパスワードに一致ししなければなりません。

4. ルーター設定を終了し、保存します。

Content Gateway で WCCP v2 を有効化します

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *WCCP v2 ルーターの構成、70 ページ*
- *WCCP デバイス上のサービス グループを設定します*
- *サービス グループに対する WCCP 処理の有効化*
- *ルーター上での WCCP v2 セキュリティの有効化、75 ページ*

WCCP v2 ルーターの設定が完了した後、以下の手順が残っています。

1. *Content Gateway Manager での WCCP v2 の有効化*
2. *Content Gateway Manager でのサービス グループの設定*

3. Content Gateway の再起動

> **重要**
>
> Content Gateway を再起動する前に、設定が以下の要件を満たしていることを確認してください。
>
> - Cisco IOS デバイスが IOS のごく最近のバージョンを実行しており、すべての関連するパッチが適用されている。
> - WCCP ルーターに適切なサービス グループおよび他の機能がプログラミングされている。

Content Gateway Manager での WCCP v2 の有効化

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [My Proxy] > [Basic] > [General]** の順に選択します。
2. **[Features（フィーチャ）]** テーブルの **[Networking（ネットワーキング）]** のセクションで **WCCP** を見つけ、**[On]** をクリックし、**[Apply]** をクリックします。Content Gateway を再起動しては**いけません**。

Content Gateway Manager でのサービス グループの設定

Help | Content Gateway | バージョン 7.8.x

トラフィックを Content Gateway プロキシへリダイレクトするすべての WCCP サービス グループは、Content Gateway サーバーまたはクラスタでそれに対応するサービス グループが定義されていなければなりません。

サービス グループを定義するには、**[Configure] > [Networking] > [WCCP]** を順に選択します。

a. **Service Groups** テーブルは、設定されているサービス グループのリストと、そのシステム設定のサブセットを表示します。

   このエントリは、**wccp.config** ファイルに保存されます。

   [Refresh（リフレッシュ）] ボタンをクリックすると、**wccp.config** が再読み込みされ、テーブルがリフレッシュされます。

   サービス グループを追加、編集、削除、順序変更するには、**[Edit File（ファイルの編集）]** をクリックします。

b. **Synchronize in the Cluster:** クラスタで Content Gateway が設定されている場合は、**Synchronize in the Cluster** オプションを有効化（デフォルト）、または無効化します。（このオプションの値は、クラスタ内で常に同期化されます）。

このオプションが有効化されているとき、WCCP 設定（**wccp.config** に保存されている）がクラスタ内で同期化され、設定の変更はクラスタ内のどのノード上でも行うことができます。

このオプションが無効化されているとき、WCCP 設定はクラスタ内で同期化されず、WCCP 設定の変更は各ノードで個別に行う必要があります。一般的な使用例として、各ノードでどのサービス グループを有効化 / 無効化するかを制御するため、および（または）**weight** を使って負荷の比例配分を行うためにこのオプションを使用できます。

このオプションが無効化された後に有効化された場合、管理者がこのオプションを有効化したノードにおける設定が、クラスタの最初の同期化に使用されます。

警告：Synchronize in the Cluster が**無効化**されている場合、ユーザーの WCCP 設定を調べ、保守するためにクラスタ内の各ノードにアクセスする必要があります。それによって WCCP のトラブルシューティングがより困難になることがあります。

サービス グループの設定（wccp.config の編集）

1. **[Configure] > [Networking] > [WCCP]** で **[Edit File]** をクリックし、エディタで **wccp.config** を開きます。

   このページの上部に、定義済みのサービス グループの一覧が表示されます。

   リストの中のエントリをクリックすると、その詳細が表示され、編集または順序変更を行うことができます。

   エントリが選択されている時、その左側の上および下向き矢印を使ってそのエントリのリスト内での位置を変更できます。

   選択したエントリを削除するには、[X] をクリックします。

2. **Service Group Information（サービス グループの情報）**

   a. **サービス グループのステータス**：サービス グループを有効化するには、**[Enabled（有効化）]** を選択します。サービス グループを定義し、非アクティブにしておくことができます。

   b. **サービス グループの名前**：固有のサービス グループ名を指定します。サービス グループ名は管理に役立ちます。

   c. **サービス グループの ID**：WCCP サービス グループの識別番号を 0 ～ 255 の範囲で指定します。この ID は、ルーターで設定されている対応するサービス グループ番号と一致していなければなりません。*WCCP デバイス上のサービス グループを設定します*を参照してください。

   d. **プロトコル**：サービス グループに適用されるネットワーク プロトコルを指定します（TCP または UDP）。

   e. **ポート**：このサービス グループが使用するポートを指定します。カンマ区切り形式のリストで最大 8 つのポートを選択できます。

> **重要**
> サービス グループ内の各ポートには、トラフィックを Content Gateway にリダイレクトするために、対応する ARM NAT が指定されていなければなりません。*ARM* を参照してください。

f. **ネットワーク インターフェース：**ドロップダウン リストから、このサービス グループが使用する Content Gateway ホスト システム上のネットワーク インターフェースを選択します。

3. **Mode Negotiation（モードのネゴシエーション）**

Packet Forward Method は、トラフィックを WCCP ルーターからプロキシへ送信する方法を決定します。

Packet Return Method は、トラフィックを WCCP ルーターへ返送する方法を決定します。

一般的には、ルーターは 1 つの方法だけをサポートします。

一般的にはパケット転送方法とパケット返送方法は一致しています。

a. トラフィックが Cisco ASA ファイアウォールによってプロキシへルーティングされている場合、**[Special Device Profile（特殊デバイス プロファイル）]** ドロップダウン ボックスで **[ASA Firewall]** を選択します。このオプションを選択すると、**[Packet Forward Method（パケット転送方法）]** および **[Packet Return Method（パケット返送方法）]** の両方に **GRE** が自動的に選択されます。この設定は変更できません。

b. トラフィックがルータまたはスイッチによってプロキシへルーティングされている場合、ルータまたはスイッチの能力および位置に対応する **Packet Forward Method** および **Packet Return Method** を選択します。

Content Gateway がルーターによってサポートされていない Forward/Return 方法を使用するように設定されている場合、プロキシはルーターによってサポートされている方法を折衝します。

Packet Forward Method: L2 または GRE を選択します。

L2 を選択した場合、返送方法としては L2 が自動的に選択されます（GRE は選択できません）。

> **重要**
> L2 を選択するには、ルーターとスイッチが Content Gateway と Layer 2-adjacent（同じサブセットにある）であることが必要です。

GRE を選択している場合、[WCCP Routers] セクションでサービス グループ内の各ルーターに対して、一意な Content Gateway トンネル エンドポイント IP アドレスを指定する必要があります（下の **[ルーター情報]** を参照してください）。

Packet Forward Method: L2 または GRE を選択します。

> **重要**
> GRE は WCCP マルチキャスト モードでは使用できません。

> **重要**
> WCCP デバイスとのアクティブな接続があるときに forward/return 方法の設定を変更した場合、その方法を再折衝するために、現在の接続の中断を強制する必要があります。通常は、そのために WCCP デバイス上のサービス グループを 60 秒間オフにします。WCCP デバイスのマニュアルを参照してください。

4. **Advanced Settings（拡張設定）**
   a. **割り当て方法**：遮断されたトラフィックをクラスタ内の複数のノードで配分するために使用するパラメータを指定します。WCCP 負荷配分機能の詳細については、*WCCP の負荷配分、68 ページ*を参照してください。

   HASH は選択した配分属性にハッシュ演算を適用します。

   - HASH では、2 つ以上の配分属性を選択できます。
   - ハッシュ演算の結果によって、トラフィックを受信するクラスタ メンバーが決まります。

   MASK は選択した配分属性にマスク演算を適用します。

   - 1 つの配分属性（通常は IP アドレス）だけを選択できます。
   - マスク演算の結果によって、トラフィックを受信するクラスタ メンバーが決まります。

   次の配分属性を選択することができます。

   - Destination IP address（宛先 IP アドレス）
   - Destination Port（宛先ポート）
   - Source IP address（送信元 IP アドレス）
   - Source Port（ソース ポート）

   MASK 値は最大 6 つの有効ビットまで適用されます（1 つのクラスタで、合計 64 個の bucket が作成されます）。割り当て方法 HASH および MASK 演算の詳細については WCCP のマニュアルを参照してください。ご使用のデバイスに、製造業者のマニュアルで推奨されている値を使用してください。

b. **Weight: Synchronize in the Cluster** が無効化されているときのみ有効です。

比例的負荷配分のために、0 ～ 255 の範囲の値を指定します。値はクラスタ内のサーバー間での比例的負荷配分を決定します。

デフォルトではすべてのクラスタ メンバーに値 0 が割り当てられています。この設定では、トラフィックは均等に配分されます。weight が 1 以上の値に設定されている場合、この値はノード間の比例的配分の基準となります。たとえば、クラスタ内に 3 つのノードがあり、Proxy1 の weight が 20、Proxy2 の weight が 10、Proxy3 の weight が 10 である場合、Proxy1 がトラフィックの半分を処理し、Proxy2 と Proxy3 がそれぞれトラフィックの 4 分の 1 を処理します。

重要

クラスタのいずれかのメンバーに対して 0 より大きい **weight** 値が設定されている時、weight 値が 0 のクラスタ メンバーにはトラフィックは**転送されません**。weight を使用する場合、必ずクラスタの各メンバーに weight を設定してください。

注意

Weight は **Synchronize in the Cluster** が無効化されているときのみ有効です。

負荷配分の詳細については、*WCCP の負荷配分、68 ページ*を参照してください。

c. **リバース サービス グループ ID** IP スプーフィングリバース サービス グループ ID を指定できます。

IP スプーフィングが有効化されている時、それぞれの HTTP および HTTPS フォーワード サービス グループにリバース サービス グループを定義しなければなりません。

注意

IP スプーフィングでは、HTTP および HTTPS のみがサポートされます。

Content Gateway は、指定された ID を使用して、フォーワード サービス グループのミラーであるリバース サービス グループを作成します。たとえば、フォーワード サービス グループの割り当て方法が宛先 IP アドレスを基準にしている場合、リバース サービス グループでは割り当て方法は送信元 IP アドレスを基準にします。

注意

IP スプーフィングは、宛先および送信元の両方の属性に対してハッシュ割り当て方法を使用するサービス グループに対してはサポートされません。そのようなサービス グループに対して IP スプーフィングを有効化すると、アラームが生成され、IP スプーフィングは無効化されます。

5. **ルーター情報**

注意

新しいプロキシ サーバーがサービス グループに追加されたとき、ルーターがそれを報告するまでに最大で 1 分かかります。

a. **セキュリティ**：オプションの WCCP 認証を使用するには、**[Enabled]** を選択し、ルーター上のサービス グループ認証に使用するのと同じパスワードを入力します。*ルーター上での WCCP v2 セキュリティの有効化、75 ページ*を参照してください。

b. **マルチキャスト**：マルチキャスト モードで実行するには、**[Enabled]** を選択し、マルチキャスト IP アドレスを入力します。マルチキャスト IP アドレスは、ルーター上で指定されているマルチキャスト IP アドレスと一致していなければなりません。*透過的遮断とマルチキャスト モード、84 ページ*を参照してください。

重要

GRE パケットの Forward/Return 方法はマルチキャスト モードでは使用できません。

c. **WCCP ルーター**：最大 10 個の **ルーター IP アドレス**を指定します。これらのルーターは、対応するサービス グループと合わせて構成しなければなりません。

GRE が **[Packet Forward Method]** として指定されている場合は、各ルーターについて一意な **ローカル GRE トンネル エンドポイント IP アドレス** を指定し（ASA ファイアウォールの場合には必要ありません）、オプションで **GRE トンネル ネクスト ホップ ルーター IP アドレス** を指定します。

ローカル GRE トンネル エンドポイント IP アドレス は、関連する **ルーター IP アドレス** の Content Gateway トンネル エンドポイントです。

ローカル GRE トンネル エンドポイント IP アドレス：

- IP v 4 でなければなりません
- 一意で、どのデバイスにも割り当てられていないアドレスでなければなりません
- ルーティング可能な IP アドレスでなければなりません
- プロキシと同じサブネット上である必要があります。そうでない場合は、そのサブネットへのルートを定義する必要があります。
- クライアント側プロキシ IP アドレスとして使用してはいけません
- サービス グループに指定した物理インターフェースにバインドされます（V-シリーズ アプライアンス上で、eth0 = P1、eth1 = P2）

[GRE Packet Return Method] が設定され、Content Gateway に WCCP ルーターへのルート バックがない場合、**[GRE Tunnel Next Hop Router IP Address]** を指定します。

ping を使用してルーターへの接続をテストできます。

- Content Gateway から、サービス グループ内で（[Router IP Address] フィールドで）定義されている各ルーターを ping します。
- ping が応答を返さない場合は、そのルーターへの **[GRE Tunnel Next Hop（GRE トンネル ネクスト ホップ）]** を指定する必要があります。介在するルーターには、WCCP またはネクスト ホップへのルートがなければなりません。

注意

複数のインターフェースをもつ WCCP ルーターは最も大きい値の IP アドレスをもつインターフェースに**ルーター ID** を割り当てます。Content Gateway は方法を折衝するためにルーター ID に接続できなければなりません。接続を確認するため、およびルーター ID が意図しない時に変更されないようにするために、ルーター ループバック アドレスを最も高い IP アドレス値にしておくことを推奨します。また、そうしておけば **[Monitor] > [Networking] > [WCCP]** ページに報告されるトラフィックおよび統計は必ず既知のルーター ID に対して報告されます。

6. **[Add]** をクリックして新しいエントリを追加するか、または **[Set]** をクリックして選択したエントリへの変更を保存します。
7. **[Apply]** をクリックし、次に **[Close]** をクリックし、エディタを閉じます。**[Apply]** をクリックする前に別のページへ移動すると、すべての変更が失われます。

8. プロキシを再起動して変更を有効にします。**[Configure] > [My Proxy] > [Basic] > [General]** の順に選択して、**[Restart]** をクリックします。

> **注意**
> ルーターがプロキシにトラフィックを送信していることを確認するために、Content Gateway Manager の **[Monitor]** ペインで統計を調べます。たとえば、**[My Proxy] > [Summary]** セクションの **[Objects Served（処理されたオブジェクト）]** の統計値が増えていることを確認します。

透過的遮断とマルチキャスト モード

Help | Content Gateway | バージョン 7.8.x

Content Gateway がマルチキャスト モードで実行するように設定するには、マルチキャスト モードを有効化し、Content Gateway Manager でマルチキャスト IP アドレスを指定します。

> **重要**
> GRE パケットの Forward/Return 方法はマルチキャスト モードでは使用できません。

さらに、ルーター上で、遮断する各サービス グループ（HTTP、FTP、DNS、SOCKS）に対してマルチキャスト アドレスを設定しなければなりません。以下の手順は、WCCP v2 対応のルーター上で異なるサービス グループにマルチキャスト アドレスを設定する方法の例です。

1. Telnet でルーターに接続し、Enable モードに切り換えます。
2. プロンプトに対して、下記のコマンドを入力して、端末からルーターを設定します。

   ```
   configure terminal
   ```

3. プロンプトが表示された時に、ルーターが遮断する各サービス グループに対して下記のコマンドを入力します。

   ```
   hostname(config)# ip wccp service_group group-address
   multicast_address
   ```

   ここで *hostname* は設定しているルーターのホスト名、*service_group* はサービス グループ ID（たとえば、HTTP の場合は 0）、*multicast_address* は IP マルチキャスト アドレスです。

4. プロンプトに対して、下記のコマンドを入力して、ネットワーク インターフェースを設定します。

   ```
   interface interface_name
   ```

   ここで *interface_name* は、ルーター上の、遮断されリダイレクトされるネットワーク インターフェースです。

5. プロンプトが表示された時に、ルーターが遮断する各サービス グループに対して下記のコマンドを入力します。

   ```
   hostname(config-if)# ip wccp service_group group-listen
   ```

6. ルーター設定を終了し、保存します。

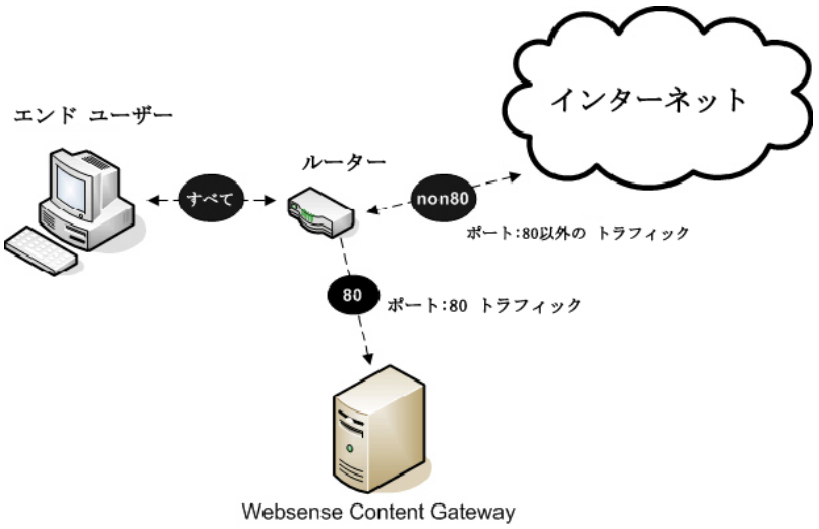
ポリシー ベースのルーティングによる透過的遮断

Help | Content Gateway | バージョン 7.8.x

WCCP プロトコルの代わりに、ルーターのポリシー ルーティング機能を使用して Content Gateway へトラフィックを送信することができます。一般的には、この設定には WCCP またはレイヤー 4 スイッチを使用するのが適切です。なぜなら、ポリシー ベースのルーティングはルーターの処理能力に影響を及ぼし、また、ポリシー ベースのルーティングはロードバランシングやハートビート メッセージングをサポートしないからです。

- クライアントのすべてのインターネット トラフィックは、Content Gateway に接続しているルーターに送信されます。
- ルーターはポート 80 (HTTP) トラフィックをプロキシに送信し、残りのトラフィックを次のホップ ルーターに送信します。
- ARM は、遮断された要求を Content Gateway 要求に変換します。
- 変換された要求はプロキシへ送信されます。
- 透過的に処理する Web オブジェクトは、ARM によって、クライアントへの返送パス上でアドレス変更されます。それによってドキュメントはオリジン サーバーから送信されたように見えます。

仮想 IP フェールオーバー機能を持つ Content Gateway クラスタは、信頼性を高めます。一方のノードが停止したとき、他方のノードがその透過要求を引き受けます。*仮想 IP フェールオーバー、108 ページ*を参照してください。



ソフトウェア ベースのルーティングによる透過的遮断

Help | Content Gateway | バージョン 7.8.x

Content Gateway ノード上でルーティング ソフトウェアを使用することによって、ルーターまたはスイッチを追加することなしに Content Gateway を配備できます。この場合、Content Gateway はソフトウェア ルーターで、すべてのトラフィックをプロキシ コンピュータを通じて転送します。このソリューションは、プロキシ コンピュータをルーターとして使用した場合の処理能力への影響がそれほど大きくないような低トラフィック環境で便利です。

Linux システムでは、**routed** および **gated** デーモンをソフトウェア ベースのルーティング ソリューションとして使用できます。**routed** デーモンは、通常のすべての Linux 配布のバンドルされている部分です。**gated** デーモンは、Merit GateD Consortium からの包括的な商業用ソフトウェア パッケージです。

ルーティング ソフトウェアを Content Gateway と合わせて使用すると、下記のようになります。

- すべてのインターネット トラフィックは、ネットワーク内の Content Gateway の背後にあるコンピュータから Content Gateway を通過します。
- ルーティング ソフトウェアは、すべての非透過的要求をインターネットにルーティングします。このソフトウェアはポート 80 HTTP 要求をプロキシ キャッシュにルーティングします。
- ARM は、遮断された要求をプロキシ要求に変換します。
- 変換された要求はプロキシへ送信されます。
- 透過的に処理する Web オブジェクトは、ARM によって、クライアントへの返送パス上でアドレス変更されます。それによってオブジェクトはオリジン サーバーから送信されたように見えます。

注意

Content Gateway コンピュータはルーターとして機能しますが、明示的にルーターとして設計されているわけではありません。信頼性を高めるために、Content Gateway クラスタと仮想 IP フェールオーバー オプションを合わせて使用することができます。一方のノードが停止した場合に、他方のクラスタ ノードが代替します。*仮想 IP フェールオーバー、108 ページ*を参照してください。）Content Gateway クラスタのフェールオーバーのメカニズムは Hot Standby Router Protocol (HSRP) と似ています。

Content Gateway が透過的要求のみ処理するように設定する

Help | Content Gateway | バージョン 7.8.x

下記の方法で、Content Gateway が透過的要求のみを処理し、明示的プロキシ要求を処理しないように構成できます。

- プロキシへの接続を許可される IP アドレスの範囲を指定することによって、Content Gateway へのクライアント アクセスを制御できます。Content Gateway は、この範囲にリストされていない IP アドレスから要求を受け取った場合、その要求を破棄します。*プロキシへのクライアント アクセスの制御、200 ページ*を参照してください。
- Content Gateway へのアクセスを許可されているクライアント IP アドレスの範囲がわからない場合は、Layer 4 スイッチまたは WCCP ルータによってリダイレクトされた要求のみがプロキシ ポートに受信されるようにするルールを **ipnat.conf** ファイルに追加できます **([Configure] > [Networking] > [ARM] > [General])**。

  透過専用の Content Gateway をサーバーを作成するには、**ipnat.conf** ファイルの通常のリダイレクト サービスのルールの前に、明示的プロキシ トラフィックをリスンしているサービスがないポートにリダイレクトするルールを追加します。たとえば、Content Gateway が明示の HTTP 要求を無視するようにするには、**ipnat.conf** ファイルの通常の HTTP リダイレクト ルールの前に、下記のようなルールを追加します（ここで、*ipaddress* はご使用の Content Gateway システムの IP アドレス、*port_number* はリスンしているサービスがないポート番号です）。

  rdr hme0 *ipaddress* port 80 -> *ipaddress* port *port_number* tcp

  rdr hme0 *ipaddress* port 8080 -> *ipaddress* port *port_number* tcp

  rdr hme0 0.0.0.0/0 port 80 -> *ipaddress* port 8080 tcp

  処理対象の各プロトコル サービス ポートまたは個別のネットワーク インターフェースについて、同様のルールを **ipnat.conf** ファイルに追加します。**ipnat.conf** ファイルに変更を行った後、プロキシを再起動する必要があります。

- Content Gateway システムに複数のネットワーク インターフェースがある場合、または Content Gateway オペレーティング システムが仮想 IP アドレスを使用するように設定する場合、Content Gateway に 2 つの IP アドレスを割り当てることができます。1つのアドレスは、プロキシがオリジン サーバーと通信するために使用する実際のアドレス、もう一方のアドレスは、WCCP またはスイッチ リダイレクションに使用するプライベート IP アドレス（例、10.0.0.1）でなければなりません。IP アドレスを設定した後、**records.config** ファイルの終わりに下記の変数を追加しなければなりません。**private_ipaddress** を WCCP またはスイッチ リダイレクションに使用されるプライベート IP アドレスに置き換え **real_ipaddress** をプロキシがオリジン サーバーと通信するために使用する IP アドレスに置き換えます。

  ```
  LOCAL proxy.local.incoming_ip_to_bind STRING
  private_ipaddress
  LOCAL proxy.local.outgoing_ip_to_bind STRING
  real_ipaddress
  ```

遮断の迂回

Help | Content Gateway | バージョン 7.8.x

一部のクライアントおよびサーバーは Web プロキシを使用する時に正しく機能しません。この問題の原因として以下のことが考えられます。

- クライアント ソフトウェアが通常のソフトウェアでない（カスタマイズされている、非商業用ブラウザ）。
- サーバー ソフトウェアが通常のソフトウェアでない。
- アプリケーションがセキュリティ上の制限を回避する方法として、HTTP ポート上で非 HTTP トラフィックを送信する。
- サーバー IP アドレスの認証（オリジン サーバーがアクセスを一部のクライアント IP アドレスに制限しているが、Content Gateway IP アドレスが異なるために、そのクライアント IP アドレスがサーバーにアクセスできない）。この方法は頻繁には用いられていません。なぜなら、多くの ISP はクライアントの IP ダイヤルアップ アドレスを動的に割り当てており、現在ではもっと安全な暗号化プロトコルが、より一般的に使用されるようになっているからです。

Web プロキシは企業ネットワークやインターネットでは非常に一般的に使用されていますから、相互運用性の問題は稀です。しかし、Content Gateway は、透過的プロキシ処理によって起こる相互運用性の問題を認識し、オペレーターの介入なしにトラフィックが自動的にプロキシ サーバーを迂回するようにする適応学習モジュールを備えています。

Content Gateway は 2 つのタイプのバイパス ルールに従います。

- *動的*（[適応型] とも言います）バイパス ルールは、Content Gateway がポート 80 で 非 HTTP トラフィックを検出した、または何らかの HTTP エラーが発生した時にキャッシュを迂回するように設定している場合に、動的に生成されます。*動的バイパス ルール*、89 ページを参照してください。
- *静的*バイパス ルールは、**bypass.config** ファイルで手動で設定しなければなりません。*静的バイパス ルール*、91 ページを参照してください。

> **注意**
>
> ARM バイパス ルールとクライアント アクセス制御リストを混同しないでください。バイパス ルールは、相互運用性の問題に対応するために作成されます。クライアント アクセス制御は、*プロキシへのクライアント アクセスの制御*、200 ページで説明しているように、単にプロキシにアクセスできるクライアントの IP アドレスを制限するだけです。

動的バイパス ルール

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *動的バイパス ルールの設定*、90 ページ
- *動的バイパス統計の表示*、91 ページ

プロキシは、プロトコルの相互運用性のエラーを監視します（そうするように設定されている場合）。プロキシはエラーを検出したとき、ARM がエラーの原因となったクライアントとサーバーに対してプロキシを迂回するように設定します。

これによって、プロキシで正常に処理されない一部のクライアントまたはサーバーが自動的に検出され、プロキシ キャッシング サーバーを迂回するようになり、継続的に機能できるようになります（ただしキャッシュに入れることはできません）。

下記のいずれかのエラーが発生した時にプロキシが動的に自分を迂回するように設定することができます。

エラー コード	説明
N/A	ポート 80 上の非 HTTP トラフィック
400	不適切な要求

エラー コード	説明
401	無許可
403	禁止（認証に失敗）
405	メソッドが許可されていない
406	許可されない（アクセス）
408	要求の時間切れ
500	内部サーバー エラー

たとえば、Content Gateway が認証失敗 **(403 Forbidden)** 時に迂回するように設定されている場合、オリジン サーバーへのいずれかの要求が 403 エラーを返した時、Content Gateway はオリジン サーバーの IP アドレスに対する宛先バイパス ルールを生成します。プロキシを再起動するまで、そのオリジン サーバーへのすべての要求は迂回されます。

もう 1 つの例として、クライアントがポート 80 上で特定のオリジン サーバーへの非 HTTP 要求を送信している時、Content Gateway は送信元 / 宛先ルールを生成します。そのクライアントからオリジン サーバーへのすべての要求は迂回され、他のクライアントからの要求は迂回されません。

動的に生成されたバイパス ルールは、Content Gateway が再起動したときにパージされます。動的に生成されたルールを残しておきたい場合は、現在のバイパス ルールのセットのスナップショットを保存することができます。*現在のバイパス ルールのセットの表示、92 ページ*を参照してください。

Content Gateway が特定の IP アドレスを動的に迂回しないようにするために、**bypass.config** ファイルで動的バイパス拒否ルールを設定することができます。バイパス拒否ルールは、プロキシが自分を迂回することを禁止できます。動的バイパス拒否ルールの設定の詳細については、*bypass.config、447 ページ*を参照してください。

動的バイパス ルールの設定

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway は HTTP エラーが発生した場合や、ポート 80 上で非 HTTP トラフィックが検出された場合に、自分を迂回するようには設定されていません。適当なオプションを設定することによって動的バイパス ルールを有効化しなければなりません。

1. **[Configure] > [Networking] > [ARM] > [Dynamic Bypass（動的バイパス）]** を順に選択します。
2. **[Dynamic Bypass]** ボタンを有効化します。
3. **[Behavior（動作）]** のセクションで、使用する動的バイパス ルールを選択します。

4. **[Apply]** をクリックします。
5. **[Configure] > [My Proxy] > [Basic] > [General]** タブで **[Restart]** をクリックします。

動的バイパス統計の表示

Help | Content Gateway | バージョン 7.8.x

Content Gateway は動的バイパスのトリガーの種類別に、迂回された要求を集計します。たとえば、Content Gateway は 401 エラーに対応して迂回されたすべての要求をカウントします。

- **[Monitor] > [Networking] > [ARM]** の順に選択します。

この統計はテーブルの **[HTTP Bypass Statistics（HTTP バイパス統計）]** のセクションに表示されます。

静的バイパス ルール

Help | Content Gateway | バージョン 7.8.x

特定のクライアントからの要求や、特定のオリジン サーバーへの要求を、プロキシを迂回して転送するためのルールを設定できます。動的バイパス ルールはプロキシを再起動したときにパージされますが、静的バイパス ルールは設定ファイルに保存されます。

3 つのタイプの静的バイパス ルールを設定できます。

- 送信元バイパス。Content Gateway は特定の送信元 IP アドレスまたは IP アドレスの範囲を迂回します。たとえば、このソリューションを使って、キャッシュ ソリューションを回避したいクライアントを迂回することができます。
- 宛先バイパス。Content Gateway は特定の宛先 IP アドレスまたは IP アドレスの範囲を迂回します。たとえば、クライアントの実際の IP アドレスを基に IP 認証を使用するオリジン サーバーを迂回できます。宛先バイパス ルールは Content Gateway がサイト全体をキャッシュするのを防止します。迂回したサイトが人気のあるサイトである場合、ヒット率への影響が顕著に表れます。
- 送信元/宛先ペアのバイパスでは、Content Gateway は指定した送信元から指定した宛先への要求を迂回します。たとえば、IP 認証が破られた、または帯域外の HTTP トラフィックの問題があるクライアント / サーバー ペアを迂回することができます。

  送信元 / 宛先バイパス ルールは、宛先サーバーを、問題が発生した特定のユーザーに対してのみブロックしますから、宛先バイパス ルールよりも適切です。

静止バイパス ルールを設定するには、**bypass.config** ファイルを編集します（*bypass.config*、447 ページを参照）。

現在のバイパス ルールのセットの表示

Help | Content Gateway | バージョン 7.8.x

ARM **print_bypass** という名前のサポート ユーティリティがあり、それによって現在の動的および静的バイパス ルールを表示することができます。

現在のすべての動的および静的バイパス ルールを表示します。

1. Content Gateway ノードにログオンし、次に、ディレクトリを Content Gateway **bin** directory（/opt/WCG/bin）に変更します。
2. プロンプトに対して下記のコマンドを入力し、**[Return]** をクリックします。

   ```
   ./print_bypass
   ```

   現在のすべての静的および動的バイパス ルールが画面に表示されます。ルールは IP アドレスによってソートされています。**print_bypass** の出力をファイルに転送して、保存することができます。

接続負荷の軽減

Help | Content Gateway | バージョン 7.8.x

負荷軽減機能は、クライアント要求の過負荷を防止します。クライアント接続の数が指定されている限度を超えたとき、ARM は着信した要求を直接にオリジン サーバーに転送します。デフォルトのクライアント接続の数は 100 万件です。

1. **[Configure] > [Networking] > [Connection Management（接続管理）] > [Load Shedding（負荷の削減）]** の順に選択します。
2. **[Maximum Connections（最大接続）]** フィールドで、許可されるクライアント接続の最大数を指定します。この数を超えると ARM は要求を直接にオリジン サーバーに転送しはじめます。
3. **[Apply]** をクリックします。
4. **[Configure] > [My Proxy] > [Basic] > [General]** の順に選択し、**[Restart]** をクリックします。

DNS ルックアップの削減

Help | Content Gateway | バージョン 7.8.x

Content Gateway を透過的プロキシ モードで実行している場合、**[Always Query Destination（常に宛先を照会する）]** オプションを有効化することによって DNS ルックアップの数を減らし、応答時間を改善することができます。Always Query Destination オプションが有効化されている時、プロキシは常に ARM から着信する要求の元の宛先 IP アドレスを取得するように設定さ

れます。この場合、Content Gateway は、要求のホスト名について DNS ルックアップを実行するのではなく、その IP アドレスを使ってオリジン サーバーを判別します。クライアントがすでに DNS ルックアップを実行していますから、Content Gateway は DNS ルックアップを実行する必要はありません。

重要

Content Gateway が明示および透過の両方のプロキシ モードで実行している場合、Always Query Destination オプションを有効化しないことを推奨します。明示のプロキシ モードでは、クライアントはオリジン サーバーのホスト名について DNS ルックアップを実行しませんから、プロキシが DNS ルックアップを実行しなければなりません。

また、カテゴリー ルックアップは IP アドレスを基に実行されます。これは常に URL ベースのルックアップと同等に正確であるとは限りません。

また、Web Security トランザクション ログ で IP アドレスではなくドメイン名を検索する場合は、Always Query Destination オプションを有効化してはいけません。

Always Query Destination を有効化するには、下記の手順を実行します。

1. Content Gateway の **config** ディレクトリ (**/opt/WCG/config)** の **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
proxy.config.arm.always_query_dest	Always Query Destination オプションを無効化するには、0 に設定します。ドメイン名がキャプチャーされます。 Always Query Destination オプションを有効化するには、1 に設定します。IP アドレスがキャプチャーされます。ドメイン名はキャプチャーされません。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway **bin** ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

IP スプーフィング

Help | Content Gateway | バージョン 7.8.x

通常、Content Gateway はクライアントへの要求をプロキシへ転送するとき、クライアント の IP アドレスの代わりに自分の IP アドレスを使用してオリジン サーバーと通信します。これは、フォワード プロキシの標準動作です。

IP スプーフィングは、下記のどちらかを使用するためにプロキシを設定します。

- オリジン サーバーと通信するときのクライアントの IP アドレス（基本的なスプーフィング）、または
- オリジン サーバーと通信するときに指定した IP アドレス（*範囲ベースの IP スプーフィング*）

IP スプーフィングは、クライアント IP アドレスまたは特定の IP アドレスを要求するアップストリーム アクティビティをサポートするために使用することもあります。その結果、オリジン サーバーはプロキシ IP アドレスではなくクライアントまたは指定した IP アドレスを受け取ることになります（ただし、プロキシ IP アドレスが指定した IP アドレスと同じであることもあります。詳細は下記を参照）。

IP スプーフィングの機能と制限：

- IP スプーフィングは、透過的プロキシ要求に対してのみサポートされています。
- IP スプーフィングは、HTTP および HTTPS トラフィックに対してのみサポートされています。
- IP スプーフィングが有効化されているとき、HTTP と HTTPS の両方に適用されます。1 つのプロトコルのみに設定することはできません。
- HTTPS トラフィックは、SSL サポートが有効化されているか否かにかかわらずスプーフィングされます。
- IP スプーフィングには ARM が必要です。
- IP スプーフィングは、Cisco ASA または PIX ファイアウォールなどのエッジ デバイスではサポート**されていません**。これを試みた場合、Content Gateway がクライアント IP アドレスを使って行った要求は Content Gateway にループバックされます。
- IP スプーフィングは IPv6 をサポートしません。

警告

IP スプーフィングを配備するためには、ネットワーク上のルーティング パスを正確に制御する必要があり、TCP ポート 80 および 443 上で実行する通常のルーティング プロセスを無効にする必要があります。

IP スプーフィングを有効化している時、従来のデバッグ ツール（例、**traceroute**、**ping**）の用途は限られます。

重要

プロキシ カーネル ルーティング テーブルが透過的プロキシ環境に及ぼす影響については、Solution Center に掲載されている [Web sites in the Static or Dynamic bypass list fail to connect（静的または動的バイパス リストに含まれる web サイトに接続できない）] というタイトルの記事を参照してください。

範囲ベースの IP スプーフィング

範囲ベースの IP スプーフィングは、指定された IP アドレスにマッピングされるクライアントのグルーピング（IP アドレスおよび IP アドレス範囲）をサポートします。

他のユーザーの間で、範囲ベースの IP スプーフィングによって下記のことが可能になります。

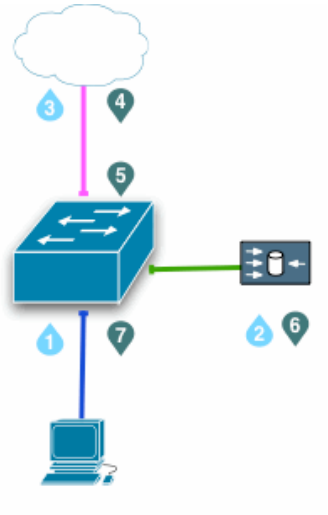
- 識別がソース IP アドレスによって行われる場合に、Web ホスト サービスの配信。たとえば、web-ホストされたサービスを受け取るために、組織は既知の IP アドレスを通じてサービスにメンバーシップを登録することを求められる場合があります。
- 1 つの固有の IP アドレスがユーザーのグループを代表する場合に、外部サービスに対する IP アドレス ベースの認証。
- 一部のクライアントに従来の IP スプーフィング（どのグループにもマッチングしないソース IP アドレスがそれらの固有の IP アドレスによってスプーフィングされる）、一部のクライアントに範囲ベースの IP スプーフィング、一部のクライアントに標準プロキシ IP アドレス代替を設定する。後の設定はプロキシ IP アドレスを指定するグループを作成することによって行われます。

重要

範囲ベースの IP スプーフィングは、Cisco IOS ファームウェアの多くの旧バージョンではサポートされていません。問題を回避するために、使用している Cisco デバイスを最新のファームウェアに更新してください。

IP スプーフィングとトラフィックのフロー

以下は、WCCP で IP スプーフィングを使用している時の HTTP および HTTPS トラフィックのフローを説明しています。ポリシー ベースのルーティングを導入することによって同じ結果を得ることもできます。図の中の番号は、番号付きのリストで説明している動作に対応しています。



1. クライアント要求が、経路指定されているポート、または、宛先ポートが HTTP (80) または HTTPS (443) であるトラフィックを探している Switched Virtual Interface (SVI) に到達します。
2. スイッチは、クライアント要求を Content Gateway にリダイレクトします。

   必要な場合、プロキシは、クライアント IP アドレス または指定した IP アドレス（範囲ベースの IP スプーフィング）を使用してオリジン サーバーへの接続を作成します。
3. 要求はスイッチ、NAT、および（または）ファイアウォールを通じてオリジン サーバーへ送信されます。

4. オリジン サーバーの応答が返されたとき、IP パケットには代替の IP アドレス（クライアントまたは指定した IP アドレス）が宛先として使用されています。
5. オリジン サーバーの応答が、経路指定されているポート、または、送信元ポートが HTTP (80) または HTTPS (443) であるトラフィックを探している Switched Virtual Interface (SVI) に到達します。下の注記を参照してください。
6. スイッチはオリジン サーバーの応答をプロキシにリダイレクトし、プロキシから オリジン サーバーへの TCP 接続を完了します。
7. クライアントへのプロキシ応答が生成され、プロキシからクライアントへの TCP 接続を通じてクライアントへ返されます。

> **注意**
> IP スプーフィングが有効化されている時、プロキシはそれぞれの有効化されている WCCP サービスに対して、リバース サービス グループを公告します。リバース サービス グループは、プロキシのリターン パスに適用されなければなりません。

WCCP サービス グループ ID はユーザー定義の ID であり、WCCP デバイス上、および Content Gateway 内でプログラミングされていなければなりません（*WCCP デバイス上のサービス グループを設定します*および *Content Gateway Manager でのサービス グループの設定*を参照）。

以下は推奨する定義のセットです。

サービス ID	ポート	トラフィック タイプ
0	宛先ポート 80	HTTP
20	送信元ポート 80	HTTP
70	宛先ポート 443	HTTPS（HTTPS サポートを有効化しなければなりません）
90	送信元ポート 443	HTTPS

ポリシー ベースのルーティング (PBR) は、アクセス制御リスト (ACL) を使ってフローを識別し、リダイレクトします。PBR 環境では、すべてのシステム設定はルーター上で行われ、対応する Content Gateway 側の設定はありません。PBR 環境は、オリジン サーバーのポート 80 および 443 から返されるトラフィックを Content Gateway にリダイレクトしなければなりません。

IP スプーフィングの設定

基本 IP スプーフィング

1. **[Configure] > [Networking] > [ARM] > [General]** の順に選択します。
2. **[IP Spoofing（IP スプーフィング）]** で **[Enabled（有効化）]** を選択します。
3. **[Apply]** をクリックします。
4. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

警告

ARM は Content Gateway の不可欠のコンポーネントであり、無効化してはいけません。IP スプーフィングを有効化している時に ARM が無効化されている場合、クライアント要求は [Cannot display Web page（web ページを表示できない）] エラーを受け取り、エラー メッセージが /var/log/messages に記録されます。

WCCP ルーターの設定については、*WCCP v2 ルーターの構成*、70 ページを参照してください。

範囲ベースの IP スプーフィング

- クライアント IP アドレスおよびそれらに対応するスプーフィングされた IP アドレスは 1 つのテーブルに指定されます。
- テーブルは上下にトラバースされます。最初のマッチが適用されます。
- テーブル内の IP アドレスにマッチングしないクライアントからの要求は、自身の IP アドレスによってスプーフィングされます（基本 IP スプーフィング）。
- 一連の IP アドレスがプロキシから送信されているように見せる（通常のフォワード プロキシ要求処理と同様に）エントリを作成するには、希望するクライアント IP アドレス範囲を指定し、次に **[Spoofed IP Address（スプーフィング対象の IP アドレス）]** フィールドで、プロキシのインターネット側 IP アドレスを指定します。
- 必要を満たす最小のリストを作成することを推奨します。各接続要求に対してリストがトラバースされます。リストが非常に大きいと遅延が発生することがあります。プロキシ パフォーマンスをモニタするには、パフォーマンス チャート（**[Monitor] > [Performance（パフォーマンス）]**）を使用します。

範囲ベースの IP スプーフィング テーブルを作成するには、下記の手順を実行します。

1. **[Configure] > [Networking] > [ARM] > [General]** の順に選択します。
2. **[IP Spoofing]** で **[Enabled]** を選択します。範囲ベースの IP スプーフィングを有効化するためには基本 IP スプーフィングを有効化する必要があります。
3. **[Range Based IP Spoofing（範囲ベースの IP スプーフィング）]** で **[Enabled]** を選択します。
4. **[Client IP Addresses]** フィールドで個別の IP アドレスおよび（または）IP アドレス範囲のカンマ区切りリストを入力します。

   範囲では、最初の IP アドレスは、最後からハイフンで区切られます。例：10.100.100.0-10.100.100.254

   CIDR 表記法を使用できます。スペースは使用できません。
5. **[Specified IP Address]** フィールドに、1 つの IP アドレスを入力します。
6. **[Apply]** をクリックして、エントリをテーブルに追加します。

   警告：いずれかのフォーマティングが無効な場合、その行にあるデータのすべてがクリアされます。
7. テーブルに新しい行を追加するには **[Add Row（行を追加）]** をクリックします。
8. 新しいエントリを有効にするには、**[Apply]** をクリックし、次に Content Gateway を再起動します。

IP スプーフィング テーブルからエントリーを削除するには、下記の手順を実行します。

1. 削除対象の行のすべての値をクリアします。
2. **[Apply]** をクリックします。
3. 変更を有効にするために、Content Gateway を再起動します。

6 クラスタ

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *クラスタ構成の変更*、103 ページ
- *クラスタへのノードの追加*、105 ページ
- *クラスタからのノードの削除*、107 ページ
- *仮想 IP フェールオーバー*、108 ページ

Websense Content Gateway は 1 つのノードから 2 つ以上のノードのクラスタまで拡張可能であり、迅速に容量を拡大し、システムの処理能力と信頼性を向上させることができます。

- Content Gateway はクラスタ内のノードの追加および削除を検出し、ノードが停止した時にそれを検出できます。
- いつでもクラスタ内のノードを追加または削除できます。
- ノードをクラスタから除去したとき、Content Gateway は除去したノードへのすべての参照を除去します。
- クラスタ内の 1 つのノードを再起動すると、クラスタ内のすべてのノードが再起動します。
- *仮想 IP フェールオーバー*機能が有効化されている時、クラスタ内のアクティブなノードが、停止しているノードのトラフィックを引き受けることができます。
- クラスタ内のノードは自動的に設定情報を共有します。

注意

Filtering Service および Policy Service の IP アドレスはクラスタ全体には適用されません。

WCCP での透過的プロキシ環境では、サービス グループの有効 / 無効状態はクラスタ全体には適用されません。*WCCP v2 デバイスによる透過的遮断、65 ページ*を参照してください。

SSL サポートが有効化されている時、ダイナミック インシデント リストはクラスタ全体に適用されません。

Content Gateway はクラスタ化のための専用プロトコルを使用します。これはノード検出用にはマルチキャストされ、クラスタ内のすべてのデータ交換用にはユニキャストされます。

重要

Content Gateway クラスタ通信には専用のネットワーク インターフェースを使用することを推奨しますが、**例外として**、ホストが V シリーズ アプライアンスである場合には P1（eth0）インターフェースを推奨します。

重要

プロキシの階層の中で、クラスタ内のノードに HTTP の親と子が混在することはできません。

管理クラスタ化

Help | Content Gateway | バージョン 7.8.x

管理クラスタ化モードでは、すべての Content Gateway ノードを同時に管理することができます。なぜなら、クラスタ ノードは構成情報を共有するからです。

注意

クラスタ内のノードの数は 2 つ以上です。

配備環境の拡張については、Websense のアカウント担当者にご相談ください。

- Content Gateway は、クラスタ内のすべてのノードについて 1 つのシステム イメージを維持するために、マルチキャスト管理プロトコルを使用します。
- クラスタのメンバー、構成、例外に関する情報は、すべてのノードで共有されます。
- **content_manager** プロセスは、構成変更をクラスタ内のノードに適用します。
- HTTPS オプションが有効化されている時（SSL サポート）、その設定値も、ダイナミック インシデント リスト以外を除いてクラスタ全体に適用されます。

クラスタ構成の変更

Help | Content Gateway | バージョン 7.8.x

クラスタ化は通常、プロキシをインストールする時に設定されます。しかし、あとで、いつでも、Content Gateway manager でクラスタ化を設定できます。

1. Content Gateway manager で、**[Configure] > [My Proxy] > [Basic] > [Clustering（クラスタ化）]** を順に選択します。
2. **[Cluster Type（クラスタ タイプ）]** 領域で、クラスタ化モードを選択します。
   - このプロキシをクラスタに含める場合は、**[Management Clustering（管理クラスタ化）]** を選択します。
   - このプロキシをクラスタに含めない場合は、**[Single Node（単一ノード）]** を選択します。
3. **[Interface（インターフェース）]** 領域に、ネットワーク インターフェースの名前を入力します。これは Content Gateway がクラスタ内の他のノード（例、eth1）との通信に使用するインターフェースです。

   専用のセカンダリー インターフェースを使用することを推奨します。

   ノード構成情報は、プレーン テキストで、同じサブネット中の他の Content Gateway ノードにマルチキャストされます。したがって、Websense は、クライアントを Content Gateway ノードから独立したサブネット上に配置することを推奨します（クラスタ化のためのマルチキャスト通信はルーティングされません）。

   V シリーズ アプライアンス上では、P1 (eth0) が推奨インターフェースです。しかし、クラスタ管理トラフィックを隔離したい場合には、P2 (eth1) を使用してもかまいません。

4. **[Cluster Multicast Group Address（クラスタ マルチキャスト グループ アドレス）]** 領域で、クラスタの全メンバーが共有するマルチキャスト グループ アドレスを入力します。デフォルトは 224.0.1.37 です。

警告

マルチキャスト IP アドレスが他のアプリケーションまたはサービスが使用している同じアドレスと競合していないことを確認します。

競合がある場合に Content Gateway ノードの再起動が許可されると、インターフェースを初期化できず、Content Gateway インスタンスがシャットダウンします。状態を確認するためには、**/var/log/messages** を調べ、下記のようなメッセージを探します。

[LocalManager::initCCom] Unable to find network interface eth2.#011 Exiting

問題を是正するには、クラスタの全メンバーに対して有効な一意なマルチキャスト IP アドレスを指定し、

Content Gateway がアプライアンス上にある場合：

- appliance manager にログオンし、**[Administration] > [Toolbox]** を順に選択し、**[Command Line Utility]** を開きます。
- **[Websense Content Gateway Module]** を選択し、次にコマンド [**content-line -s**] を選択します。
- **[Variable Name]** に **proxy.config.cluster.mc_group_addr** を指定し、**[Value]** にマルチキャスト IP アドレスを指定します。
- クラスタの各メンバーをチェックし、全メンバーが同じマルチキャスト IP アドレスを使用していることを確認します。
- ノードを再起動します。

Content Gateway が別のサーバーにインストールされている場合：

- Linux ホストにログオンし、**/opt/WCG/config** にアクセスします。
- (vi) **records.config** を編集し、**proxy.config.cluster.mc_group_addr** を見つけ、それにマルチキャスト IP アドレスの値を割り当てます。
- クラスタの各メンバーをチェックし、全メンバーが同じマルチキャスト IP アドレスを使用していることを確認します。
- ノードを再起動します。

5. **[Apply]** をクリックします。
6. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

> **重要**
> Content Gateway はクラスタ化モードの変更を、クラスタ内のすべてのノードには適用しません。各ノードのクラスタ化モードを個別に変更しなければなりません。

クラスタへのノードの追加

Help | Content Gateway | バージョン 7.8.x

Content Gateway はネットワーク上で新しい Content Gateway ノードを検出し、それをクラスタに追加し、新しいクラスタ メンバーに最新の構成情報を適用します。これによって新しいコンピュータのブートストラップを簡単に行うことができます。

ノードを Content Gateway クラスタに接続するための操作は、新しいノード上に Content Gateway ソフトウェアをインストールすることだけです。この時、クラスタ名とポート割り当てが既存のクラスタのそれと同じであることを確認してください。これによって Content Gateway は自動的に新しいノードを認識します。

> **重要**
> クラスタ内のノードは均質でなければなりません。つまり、各ノードは同じハードウェア プラットフォーム上にあり、オペレーティング システムの同じバージョンを使用しており、Content Gateway が同じディレクトリ (/opt/WCG) にインストールされていなければなりません。

1. 適切なハードウェアをインストールし、それをネットワークに接続します。
2. クラスタ ノードをインストールするための適当な手順を使用して Content Gateway ソフトウェアをインストールします。Deployment and Installation Center の Content Gateway のインストールの手順を参照してください。

3. インストール手順の中で、以下の条件が満たされていることを確認してください。
   - 新しいノードに割り当てるクラスタ名が、既存のノードのクラスタ名と同じである。
   - 新しいノードのポート割り当てが、他のノードで使用するポート割り当てと同じである。
   - マルチキャスト アドレスとマルチキャスト経路設定を追加した。
4. Content Gateway を再起動してください。*コマンド ラインでの Content Gateway の起動および停止、23 ページ*を参照してください。

既存の Content Gateway インストールをクラスタに追加するには、下記の手順を実行します。

1. In the Content Gateway manager で **[Configure] > [My Proxy] > [Basic] > [General]** を順に選択し、**[Proxy Name]** をクラスタの名前に設定します。
2. **[Configure] > [My Proxy] > [Basic] > [Clustering]** の順に選択します。
3. **[Interface]** をクラスタが使用するインターフェースに設定します。すべてのメンバーが、同じインターフェースを使用しなければなりません。
4. **[Multicast Group Address（マルチキャスト グループ アドレス）]** をクラスタが使用するアドレスに設定します。
5. **[Type]** 領域で、**[Management Clustering（管理クラスタ化）]** を選択します。
6. **[Apply]** をクリックします。
7. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

また、追加対象のノードの **record.config** ファイルの変数値を編集することによってノードを追加することもできます。

1. クラスタに追加するノード上で、**/opt/WCG/config** の中の **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
proxy.local.cluster.type	クラスタ モードを指定します。 2 = 管理モード 3 = クラスタ化しない
proxy.config.proxy_name	Content Gateway クラスタの名前を指定します。クラスタ内のすべてのノードは同じ名前を使用しなければなりません。

変数	説明
proxy.config.cluster.mc_group_addr	クラスタ通信のためのマルチキャスト アドレスを指定します。クラスタ内のすべてのノードは同じマルチキャスト アドレスを使用しなければなりません。
proxy.config.cluster.rsport	信頼できるサービス ポートを指定します。信頼できるサービス ポートはクラスタ内のノード間でデータを送信するために使用します。クラスタ内のすべてのノードは同じ信頼できるサービス ポートを使用しなければなりません。デフォルト値は 8087 です。
proxy.config.cluster.mcport	マルチキャスト ポートを指定します。マルチキャスト ポートは、ノードの識別のために使用します。クラスタ内のすべてのノードは同じマルチキャスト ポートを使用しなければなりません。デフォルト ポートは 8088 です。
proxy.config.cluster.ethernet_interface	クラスタ トラフィックのためのネットワーク インターフェースを指定します。クラスタ内のすべてのノードは同じネットワーク インターフェースを使用しなければなりません。

3. ファイルを保存して、閉じます。
4. Content Gateway を再起動します (**/opt/WCG/WCGAdmin restart**)。

クラスタからのノードの削除

Help | Content Gateway | バージョン 7.8.x

クラスタから除去するノードで、以下の手順を実行します。

1. **[Configure] > [My Proxy] > [Basic] > [Clustering]** の順に選択します。
2. **[Cluster Type]** 領域で、**[Single Node]** を選択します。
3. **[Apply]** をクリックします。

4. クラスタからノードを永久に削除する場合、プロキシ名をクラスタ名以外の名前に変更するのが最良の方法です。

   [Configure] > [My Proxy] > [Basic] > [General] を順に選択し、**[Proxy Name（プロキシ名）]** をシステム ホスト名またはその他の意味のある値に変更します。
5. プロキシを再起動します。

仮想 IP フェールオーバー

Help | Content Gateway | バージョン 7.8.x

仮想 IP フェールオーバー機能によって、Content Gateway は必要に応じてクラスタ内のノードに割り当てる仮想 IP アドレスのプールを維持します。これらのアドレスは仮想です。つまり、特定のコンピュータに関連付けられているわけではありません。Content Gateway はそれを任意のノードに割り当てることができます。クラスタの外に対しては、これらの仮想 IP アドレスは Content Gateway サーバーのアドレスです。

仮想 IP フェールオーバーによって、クラスタ内の 1 つのノードが停止しても、他のノードが停止したノードの役割を引き受けることができます。Content Gateway は仮想 IP フェールオーバーを以下の方法で処理します。

- **content_manager** プロセスはクラスタ通信を維持します。ノードは自動的に、マルチキャスト通信を通じて統計情報および構成情報を交換します。いずれかのクラスタ ノードからマルチキャスト ハートビートが受信されない場合、他のノードはそのノードが使用不能であると認識します。
- **content_manager** プロセスは、約 30 秒以内に、停止しているノードの IP アドレスを残りのアクティブなノードに再割り当てし、それによってサービスが中断なしに継続できるようにします。
- IP アドレスが新しいネットワーク インターフェースに割り当てられ、新しい割り当てがローカル ネットワークにブロードキャストされます。IP アドレスの再割り当ては **ARP リバインド**と呼ばれる処理を通じて行われます。

仮想 IP アドレスとは？

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *仮想 IP アドレス指定の有効化と無効化、109 ページ*
- *仮想 IP インターフェースの追加と編集、110 ページ*

仮想 IP アドレスは、特定のコンピューターに結合されていない IP アドレスです。したがって、これらのアドレスは Content Gateway クラスタ内のノード間で持ち回りで使用できます。

1 台のコンピュータが同じサブネット上の複数の IP アドレスを持つことは、よくあることです。このコンピュータは、そのインターフェース カードに関連付けられているプライマリー、または実 IP アドレスを持ち、また、多くの仮想アドレスに対応できます。

ユーザー ベースが、Content Gateway コンピュータの実 IP アドレスを使用するのではなく、仮想 IP アドレスへの DNS ラウンドロビン ポインティングを使用するようにセットアップすることができます。

仮想 IP アドレスは特定のコンピュータに結合されていませんから、Content Gateway クラスタは、非アクティブのノードからアドレスを取り上げ、それを残りのアクティブなノードの間で配分することができます。

専用の管理プロトコルを使って Content Gateway ノードはそのステータスを、ピアのノードに通知することができます。ノードが停止したとき、そのピアのノードはそれを認識し、残りのノードのうちのどれが、停止したノードの仮想インターフェースを引き継ぐことによって障害をマスクするかを折衝します。

仮想 IP アドレス指定の有効化と無効化

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [My Proxy] > [Basic] > [General]** の順に選択します。
2. [Features（機能）] テーブルの [Networking（ネットワーキング）] セクションで、**[Virtual IP（仮想 IP）]** に対して **[On]** または **[Off]** を選択して仮想 IP を有効化または無効化します。
3. **[Apply]** をクリックします。

仮想 IP インターフェースの追加と編集

Help | Content Gateway | バージョン 7.8.x

仮想 IP アドレスは、他のすべての IP と同様に、Content Gateway に割り当てる前に事前予約されていなければなりません。

> **警告**
> 不適切な IP アドレス指定の結果、システムが使用不能になることがあります。必ず、仮想 IP アドレスを変更する前に、仮想 IP アドレスの仕組みを理解しておいてください。

1. **[Configure] > [Networking] > [Virtual IP]** の順に選択します。

   [Virtual IP Addresses] 領域は、Content Gateway によって管理される仮想 IP アドレスを表示します。

   > **注意**
   > [Virtual IP] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** の [Features] テーブルで [Virtual IP] オプションを有効化した場合にだけ表示されます。

2. 新しい仮想 IP アドレスを追加するか、既存の仮想 IP アドレスを編集するために、**[Edit File（ファイルの編集）]** をクリックします。
3. 仮想 IP アドレスを編集するには、ページ上部のテーブルからそれを選択し、表示されたフィールドを編集し、**[Set（設定）]** をクリックします。

   選択した IP アドレスを削除するには、**[Clear Fields（フィールドの消去）]** をクリックします。

   仮想 IP アドレスを追加するには、表示されたフィールドに仮想 IP アドレス、イーサネット インターフェース、およびサブインターフェースを指定し、**[Add（追加）]** をクリックします。
4. **[Apply]** をクリックし、次に **[Close]** をクリックします。

7 階層キャッシング

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway を *HTTP キャッシュ階層、111 ページ*に組み込むことができます。そこでは、あるキャッシュで処理されなかったインターネット要求を他のリージョナル キャッシュにルーティングでき、そのキャッシュのコンテンツと要求元からの近接性を活用することができます。

キャッシュ階層は、相互に交信する複数のレベルのキャッシュによって成り立っています。Content Gateway は、いくつかのタイプのキャッシュ階層をサポートしています。すべてのキャッシュ階層は*親*と*子*という概念を認識します。親キャッシュは階層の上位のキャッシュであり、プロキシはこれに対して要求を転送することができます。子キャッシュは、プロキシを親とするキャッシュです。

HTTP キャッシュ階層

Help | Content Gateway | バージョン 7.8.x

HTTP キャッシュ階層では、Content Gateway ノードが要求されたオブジェクトを自分のキャッシュで見出せないとき、そのオブジェクトをオリジン サーバーから取得する前に親キャッシュで探すことができ、またこの親キャッシュは他のキャッシュで探すことができます。

1 つ以上の HTTP 親キャッシュを使用するように Content Gateway ノードを構成し、ある親が利用できないとき、別の親が要求に対応できるようにすることができます。これは親フェイルオーバーといい、その説明は*親フェールオーバー、112 ページ*にあります。

注意

すべての要求が親キャッシュに向かうのを避けるために、**parent.config** 構成ファイル（*parent.config、470 ページ*参照）で親プロキシ ルールを設定することにより、プロキシが特定の要求（特定の URL を含む要求など）をオリジン サーバーに直接にルーティングするように構成することができます。

注意

要求されたコンテンツが親キャッシュでキャッシュされていない場合、親はそのコンテンツをオリジンサーバー（または、親の構成によっては、別のキャッシュ）から取得します。親はコンテンツをキャッシュし、次にコピーをプロキシ（その子）に送り、この送り先でそれはキャッシュされ、クライアントに提供されます。

親フェールオーバー

Help | Content Gateway | バージョン 7.8.x

プロキシが複数の親キャッシュを使用するように構成されているとき、プロキシは、ある親が利用できないことを検出すると、処理されなかった要求を別の親キャッシュに送ります。3 つ以上の親キャッシュが指定されているとき、それらの親キャッシュが問い合わせを受ける順序は親の設定ファイル中で構成されている親プロキシ ルール（*parent.config*、470 ページ参照）によって異なります。デフォルトでは、親キャッシュに対する問い合わせは親の設定ファイルでそれらがリストされている順序に従って行われます。

HTTP 親キャッシュを使用する Content Gateway の構成

Help | Content Gateway | バージョン 7.8.x

1. **[Configure（構成）] > [Content Routing（コンテンツ ルーティング）] > [Hierarchies（階層）] > [Parenting（親）]** ページで **[Parent Proxy（親プロキシ）]** を有効にします。
2. **[Edit File（ファイルの編集）]** をクリックして、*parent.config* ファイルの編集のために設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは *Hierarchies（階層）*、368 ページで説明しています。
4. **[Apply]** をクリックし、次に **[Close]** をクリックします。
5. **[Parenting]** タブで **[Apply]** をクリックして、設定ファイルを保存します。

重要

子プロキシ上でこの手順を実行します。親について、いかなる変更もしないでください。

8 キャッシュの構成

Help | Content Gateway | バージョン 7.8.x

キャッシュは、**オブジェクト ストア**と呼ばれる高速オブジェクト データベースから成ります。オブジェクト ストアは、URL および関連付けられているヘッダに従ってオブジェクトのインデックスを作成し、Websense Content Gateway が Web ページおよび Web ページの一部を保存、取得、および提供できるようにし、最適な帯域幅の節約を可能にします。オブジェクト ストアは、オブジェクト管理を使用して、同じオブジェクトの代替バージョン（言語または暗号化タイプが異なる）をキャッシュすることができ、また大小のドキュメントを保存でき、無駄なスペースを最小限にします。キャッシュがいっぱいになると、Content Gateway は陳腐化したデータを除去します。

フォールト トレランス：Content Gateway は、キャッシュ ディスク上のディスク障害を許容します。ディスク ドライブが 5 回連続で IO 動作に失敗した場合、Content Gateway は、そのディスクを故障とマーク付けし、キャッシュからドライブを削除し、ディスクが機能しなくなったことを示すアラーム メッセージを Content Gateway manager に送信します。残りのキャッシュ ディスクでは正常なキャッシュ処理が続行します。すべてのキャッシュ ディスクが機能しなくなった場合、Content Gateway はプロキシ専用モードに移行します。

下記のようなキャッシュ構成設定タスクを行なうことができます：

- インストール後にキャッシュ ディスクを追加する。*インストール後のキャッシュ ディスクの追加*、114 ページを参照してください。
- キャッシュに割り当てられているディスク スペースの総容量を変更する。*キャッシュ容量の変更*、115 ページを参照してください。
- キャッシュ ディスク スペースを特定のプロトコル、オリジン サーバー、ドメインなどに予約して、キャッシュをパーティションに区分する。*キャッシュのパーティション区分*、118 ページを参照してください。
- キャッシュで許容されるオブジェクトのサイズの限度を指定する。*キャッシュ オブジェクトのサイズ制限*、121 ページを参照してください。
- キャッシュ中のすべてのデータを削除する。*キャッシュのクリア*、121 ページを参照してください。
- RAM キャッシュのサイズを変更する。*RAM キャッシュのサイズ変更*、122 ページを参照してください。

RAM キャッシュ

Content Gateway には、非常によくアクセスされるオブジェクトの小さな RAM キャッシュがあります。この RAM キャッシュは最もよくアクセスされるオブジェクトをすばやく提供し、特にトラフィック ピーク時にディスクの負荷を軽減します。RAM キャッシュ サイズは設定可能です。*RAM キャッシュのサイズ変更、122 ページ*を参照してください。

インストール後のキャッシュ ディスクの追加

Help | Content Gateway | バージョン 7.8.x

キャッシュ ディスクを追加するには、下記のものが必要です：

- 未フォーマットの物理ディスク デバイス（OS インストールによって作成されます）。サイズ（バイト数）を書き留めておきます。
- raw キャラクタ デバイス（mknod によって作成されます）

デバイスを追加するには、物理ディスクを raw キャラクタ デバイスにマッピングしなければなりません。

以下の例では、ほとんどの場合、HP DL360 とその RAID コントローラのコマンドを扱っています。（すべてのディスクは RAID 0 です。）

1. raw デバイスをセットアップし、パーミッションを変更します：

   ```
   mknod /etc/udev/devices/raw c 162 0
   chmod 600 /etc/udev/devices/raw
   ```

2. キャッシュ ディスク物理デバイス名を確認し、サイズ（バイト数）を書き留めておきます（後で使用します）：

   ```
   fdisk -l | grep "^Disk"
   Disk /dev/cciss/c0d1:146.7 GB, 146778685440 bytes
   ```

3. ノードを作成し、そのノードの所有者を変更し、その raw ノードを物理ディスクにマッピングします。追加されるディスクごとに最後の引数が 1 だけインクリメントすることに注意してください：

   `mknod /etc/udev/devices/raw_c0d1 c 162 1` デバイス名を `fdisk -l` コマンドによって返されたデバイス名に変えることができます。

   `chown Websense /etc/udev/devices/raw_c0d1 mknod` ステートメントで使用したデバイス名を使用します。

   `/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1 mknod` ステートメントで使用したデバイス名を使用します。

4. 再起動によって変更を有効にし、同じ /usr/bin/raw コマンドを **/etc/init.d/content_gateway** の 6 行目に追加します：

   ```
   ...
   case "$1" in
   ```

```
'start')
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
mknod ステートメントで使用したデバイス名を使用します。
...
```

5. **fdisk -l** によって戻された raw ノードとサイズ（ブロック数）を使用して、デバイスを **/opt/WCG/config/storage.conf** に追加します：

   ```
   /etc/udev/devices/raw_c0d1 146778685440
   mknod ステートメントで使用したデバイス名を使用します。
   ```

6. キャッシングが有効になっていることを確認します。インストール時にキャッシュ ディスクがセットアップされていないと、キャッシングは無効になります：
   a. Content Manager で **[Configure] > [Protocols] > [HTTP]** へ進み、**[Cacheability（キャッシュ機能）]** タブをクリックします。
   b. **[HTTP Caching（HTTP キャッシング）]** で **[Enabled（有効）]** を選択します。
   c. **[Apply]** をクリックし、Content Gateway を再起動します。

キャッシュ容量の変更

Help | Content Gateway | バージョン 7.8.x

全体のディスク キャッシュの最大サイズは 147 GB です。このサイズはシステム リソースの最大限の活用を実現し、またエンドユーザーに快適な環境を提供します。

ディスク キャッシュの最小サイズは 2 GB です。

関連項目：

- *キャッシュ サイズの確認*、115 ページ
- *キャッシュ容量の増加*、116 ページ
- *キャッシュ容量の削減*、117 ページ

キャッシュ サイズの確認

Help | Content Gateway | バージョン 7.8.x

構成されている全体のキャッシュ サイズを調べるには、Content Manager を開き、**[Monitor（モニタ）] > [Subsystems（サブシステム）] > [Cache（キャッシュ）]** に進みます。**[Cache Size（キャッシュ サイズ）]** フィールドの **[Current Value（現在の値）]** 列で、キャッシュ サイズ（バイト数）を確認できます。

あるいは、Content Gateway の **bin** ディレクトリ **(/opt/WCG/bin)** から下記のコマンドを実行して、キャッシュ サイズを表示します：

```
content_line -r proxy.process.cache.bytes_total
```

キャッシュ容量の増加

Help | Content Gateway | バージョン 7.8.x

既存のディスク上でキャッシュに割り当てられている総ディスク スペースを増加するか、または Content Gateway ノードに新しいディスクを追加するには、下記の手順を実行します：

1. Content Gateway を停止します。*コマンド ラインでの Content Gateway の起動および停止、23 ページ*を参照してください。
2. 必要であれば、ハードウェアを追加します。
   a. raw デバイスをセットアップし、パーミッションを変更します：例：

      ```
      mknod /etc/udev/devices/raw c 162 0
      chmod 600 /etc/udev/devices/raw
      ```

   b. キャッシュ ディスク物理デバイス名を確認し、サイズ（バイト数）を書き留めておきます（後で使用します）：例：

      ```
      fdisk -l | grep "^Disk"

      Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
      ```

   c. 実際のディスクの 1 つ 1 つについて、それぞれノードを作成し、そのノードの所有者を変更し、その raw ノードを物理ディスクにマッピングします。追加されるディスクごとに最後の引数が 1 だけインクリメントすることに注意してください：

      ノードを作成するには、次のコマンドを実行します：

      ```
      mknod /etc/udev/devices/raw_c0d1 c 162 1
      ```

      デバイス名を、ステップ b で **fdisk -l** コマンドから戻された名前に変更することができます。

      所有者を変更するには、次のコマンドを実行します：

      ```
      chown Websense /etc/udev/devices/raw_c0d1
      ```

      所有者はインストール ユーザーです（デフォルトは Websense です）。mknod ステートメントで使用されているデバイス名を使用します。

      raw ノードを物理ディスクにマッピングするには、次のコマンドを実行します：

      ```
      /usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
      ```

      mknod ステートメントで使用されているデバイス名を使用します。

d. 同じ **/usr/bin/raw** コマンドを **/etc/init.d/content_gateway** ファイルに追加し、変更が再起動により有効になるようにします。例えば、6 行目において下記の追加を行います：

```
...
case "$1" in
'start')
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

3. Content Gateway **config** ディレクトリ **(/opt/WCG/config)** 中の **storage.config** ファイルを編集し、既存のディスク上のキャッシュに割り当てられているディスク スペースの容量を増加するか、または新しいディスク デバイスを追加します。*storage.config*、559 ページを参照してください。
4. Content Gateway を再起動してください。

キャッシュ容量の削減

Help | Content Gateway | バージョン 7.8.x

既存のディスク上のキャッシュに割り当てられているディスク スペースの総容量を削減するか、または Content Gateway ノードからディスクを除去することができます。

1. Content Gateway を停止します。
2. 必要であれば、ハードウェアを除去します。
3. **storage.config** ファイルを編集して、既存のディスク上のキャッシュに割り当てられているディスク スペースの容量を削減するか、または除去しようとするハードウェアへの参照を削除します。*storage.config*、559 ページを参照してください。
4. ディスクを除去する場合は、**/etc/rc.d/init.d/content_gateway** ファイルを編集して、そのディスクの raw ディスク バインドを除去しなければなりません。
5. Content Gateway を再起動してください。

重要

storage.config ファイル中で、フォーマット済みディスクまたは raw ディスクは少なくとも 2 GB でなければなりません。

キャッシュのパーティション区分

Help | Content Gateway | バージョン 7.8.x

個々のプロトコルに対応する異なるサイズのキャッシュ パーティションを作成することによって、キャッシュ スペースを効率的に管理し、ディスクの使用状況を改善することができます。特定のオリジン サーバーやドメインからのデータを保存するためのパーティションを構成することもできます。

重要

パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

HTTP がサポートされている唯一のプロトコルです。

プロトコルに対応するキャッシュ パーティションの作成

Help | Content Gateway | バージョン 7.8.x

個々のプロトコルに基づいてコンテンツを保存する個別のパーティションをキャッシュで作成することができます。この構成によって、特定のプロトコルのために一定のディスク スペースを確保できるようになります。

重要

HTTP がサポートされている唯一のプロトコルです。

Content Gateway Manager で下記の手順を実行します：

1. **[Configure] > [Subsystems] > [Cache] > [Partition（パーティション）]** を順に選択します。
2. **[Cache Partition（キャッシュ パーティション）]** エリアで **[Edit File（ファイルの編集）]** をクリックして、**partition.config** ファイルのための設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは *キャッシュ、400 ページ*で説明しています。
4. **[Apply（適用）]** をクリックして情報を保存し、次に **[Close（閉じる）]** をクリックします。

パーティション サイズとプロトコルの変更

Help | Content Gateway | バージョン 7.8.x

プロトコルに基づくキャッシュ パーティションを作成したら、その構成をいつでも変更できます。変更する前に、下記のことに注意してください：

- キャッシュ サイズとプロトコル割り当てを変更する前に、Content Gateway を停止しなければなりません。
- パーティションのサイズを大きくするとき、パーティションのコンテンツは**削除されません**。しかし、パーティションのサイズを小さくするとき、パーティションのコンテンツが**削除されます**。
- パーティション番号を変更するとき、サイズとプロトコル タイプに変更がなくても、パーティションは削除され、つづいて再作成されます。
- 新しいディスクを Content Gateway ノードに追加するとき、パーセンテージで指定されているパーティション サイズは比例的に大きくなります。
- パーティション サイズを何度も変更するとディスクが断片化し、そのためパフォーマンスとヒット率に影響します。キャッシュ パーティションのサイズを何度も変更する前に、キャッシュをクリアすることを推奨します（*キャッシュのクリア*、121 ページを参照してください）。

オリジン サーバーまたはドメインに基づくキャッシュのパーティション区分

Help | Content Gateway | バージョン 7.8.x

サイズとプロトコルに基づいてキャッシュをパーティションに区分したら、それらのパーティションを特定のオリジン サーバーとドメインに割り当てることができます。

1 つのパーティションを単一または複数のオリジン サーバーに割り当てることができます。しかし、1 つのパーティションを複数のオリジン サーバーに割り当てると、そのキャッシュで各オリジン サーバーが利用できるスペースについて問題が発生するかもしれません。コンテンツは使用頻度に基づいてパーティションに保存されます。

特定のオリジン サーバーとドメインにパーティションを割り当てるだけでなく、リストされないすべてのオリジン サーバーとドメインからのコンテンツを保存するための汎用パーティションを割り当てなければなりません。この汎用パーティションは、特定のオリジン サーバーまたはドメインのためのパーティションが破損した場合にも使用されます。

重要

汎用パーティションを割り当てないと、Content Gateway プロキシ専用モードで動作します。

> **注意**
> 特定のホストまたはドメインにパーティションを割り当てる前に Content Gateway を停止する必要は**ありません**。しかし、この種の構成タスクはメモリの使用状況にスパイクをもたらす可能性があり、その作業は時間がかかります。パーティション割り当ての構成タスクはトラフィックが少ないときに行うべきでしょう。

ホスト名とドメインに基づくキャッシュのパーティション区分は Content Gateway manager で行なうことができます。

Content Gateway Manager で下記の手順を実行します：

1. *partition.config*、472 ページの説明に従って、サイズとプロトコルに基づくキャッシュ パーティションを構成します。

   各ホストおよびドメインについてプロトコル（HTTP のみ）に基づく個別のパーティションと、それらのオリジン サーバーまたはドメインに属しないコンテンツで使用される汎用パーティションを作成しなければなりません。例えば、2 つの異なるオリジン サーバーからそれぞれ別個のコンテンツが必要であると、少なくとも 3 つの異なるパーティションを作成しなければなりません : 各オリジン サーバーのためのそれぞれ 1 つの HTTP ベース パーティションと他のすべてのオリジン サーバーのための汎用パーティション（これらのパーティションは同じサイズでなくても結構です）。
2. **[Configure]** タブで **[Subsystems]** をクリックし、次に **[Cache]** をクリックします。
3. **[Hosting（ホスティング）]** タブをクリックし、**[Cache Hosting（キャッシュ ホスティング）]** エリアで **[Edit File]** をクリックして、**hosting.config** ファイルのための設定ファイル編集エディタを開きます。
4. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは *キャッシュ*、400 ページで説明しています。
5. **[Apply]** をクリックし、次に **[Close]** をクリックします。

キャッシュ オブジェクトのサイズ制限

Help | Content Gateway | バージョン 7.8.x

デフォルトでは、Content Gateway はキャッシュであらユサイズのオブジェクトを許容します。このデフォルト動作を変更し、キャッシュ中のオブジェクトについてサイズの制限を指定することができます。

1. **[Configure] > [Subsystems] > [Cache] > [General]** を順に選択します。
2. **[Maximum Object Size（最大オブジェクト サイズ）]** フィールドで、キャッシュで許容されるオブジェクトの最大サイズ（バイト数）を入力します。サイズ制限を設けない場合は、0（ゼロ）を入力します。
3. **[Apply]** をクリックします。

オブジェクトがサイズ制限を超えた時、下記のメッセージがシステム ログ ファイルに記入されます。

```
WARNING: Maximum document size exceeded
```

キャッシュのクリア

Help | Content Gateway | バージョン 7.8.x

キャッシュをクリアすると、ホスト データベースのデータを含めて、すべてのデータがキャッシュ全体から除去されます。パーティション区分のようなキャッシュ構成タスクを行う前に、キャッシュをクリアします。

注意

Content Gateway が動作していると、キャッシュのクリアはできません。

1. Content Gateway を停止します。*コマンド ラインでの Content Gateway の起動および停止、23 ページ*を参照してください。
2. 次のコマンドを入力して、キャッシュをクリアします :

```
content_gateway -Cclear
```

警告

clear コマンドは、オブジェクト ストアとホスト データベースのすべてのデータを削除します。Content Gateway は削除の確認を**求めません**。

3. Content Gateway を再起動してください。

RAM キャッシュのサイズ変更

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、頻繁に使用される小さなオブジェクトの迅速な取得のために専用の RAM キャッシュを用意しています。デフォルトの RAM キャッシュ サイズは、すでに構成されているパーティションの数とサイズに基づいて算出されます。RAM キャッシュのサイズを大きくすることによって、キャッシュのヒット パフォーマンスを改善することができます。

警告

RAM キャッシュのサイズを大きくして、Content Gateway パフォーマンスの低下（遅延の増大など）が認められる場合、オペレーティング システムがネットワーク リソースのためにメモリの増大を必要としている可能性があります。RAM キャッシュ サイズを以前の大きさに戻します。

注意

プロトコルまたはホストに基づいてキャッシュがパーティションに区分されている場合、各パーティションに対応する RAM キャッシュのサイズはそのパーティションのサイズと比例します。

1. **[Configure] > [Subsystems] > [Cache] > [General]** を順に選択します。
2. **[Ram Cache Size（RAM キャッシュ サイズ）]** フィールドで、RAM キャッシュに割り当てようとするスペースの容量（メガバイト）を入力します。ユーザー インターフェースは大きな値を受け入れますが、**512 MB を上まわらないようにしてください。**

   デフォルトのサイズは 104857600 (100 MB) です。

   注意

   値 [-1] は、Content Gateway に RAM キャッシュのサイズを自動的にディスク キャッシュの 1 GB につき約 1 MB にするように指示します。

3. **[Apply]** をクリックします。
4. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

9 DNS プロキシ キャッシング

Help | Content Gateway | バージョン 7.8.x

通常、クライアントは DNS 要求を DNS サーバーに送り、ホスト名を解決しようとします。しかし、DNS サーバーがしばしば過負荷状態になったり、またクライアントから遠く離れている場合があり、そのために DNS ルックアップが遅くなったり、要求の達成にとってボトルネックになることがあります。

DNS プロキシ キャッシング オプションにより、Content Gateway がクライアントに代わって DNS 要求を解決することができます。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。

重要

DNS プロキシ キャッシング オプションは、レイヤー 4 (L4) スイッチ、または WCCP v2 を実行している Cisco ルータでだけを利用できます。

以下の概要は、Content Gateway が DNS 要求を処理する方式を示しています。

1. クライアントが DNS 要求を出します。この要求は、ポート 53 上のすべての DNS トラフィックを Content Gateway にリダイレクトするように構成されているルータまたは L4 スイッチによって捕捉されます。
2. ARM がその DNS パケットを調べます。DNS 要求が**タイプ A**（応答）であると、ARM はその要求を Content Gateway に転送します。ARM は、**タイプ A** でないすべての DNS 要求を DNS サーバーに転送します。
3. **タイプ A** 要求の場合は、Content Gateway はその DNS キャッシュをチェックし、当該 DSN についてホスト名 /IP アドレスのマッピングがあるかどうかについて調べます。そのマッピングが DNS キャッシュにあると、Content Gateway はその IP アドレスをクライアントに送ります。マッピングが DNS キャッシュにないと、Content Gateway はホスト名を解決するために DNS サーバーと交信します。Content Gateway が DNS サーバーから応答を受け取ると、ホスト名 /IP アドレス マッピングをキャッシングし、その IP アドレスをクライアントに送ります。ラウンドロビンが使用されていると、Content Gateway は IP アドレス マッピングのリスト全体をクライアントに送り、ラウンドロビンの順序が厳格に守られます。

> **注意**
> ホスト名 /IP アドレス マッピングが DNS キャッシュにないと、Content Gateway は **/etc/resolv.conf** ファイルで指定されている DNS サーバーと交信します。resolv.conf の最初のエントリのみが使用されます。このサーバーは、当初において DNS 要求で予定されていた DNS サーバーとは異なるものになるでしょう。

DNS キャッシュはメモリで維持され、ディスクでバックアップされます。Content Gateway はディスク上のデータを 60 秒ごとに更新します。TTL（残り寿命）は、あらゆるホスト名 /IP アドレス マッピングで厳格に守られます。

DNS プロキシ キャッシングの構成

Help | Content Gateway | バージョン 7.8.x

Content Gateway を DNS プロキシ キャッシュとして構成するには、下記の手順を実行します：

- **ipnat.conf** ファイルに remap ルールを追加します。
- DNS プロキシ オプションを有効にし、Content Gateway が DNS プロキシ トラフィックで使用するポートを指定します。
- ポート 53 上の　DNS トラフィックを Content Gateway に送信するようにレイヤ 4 スイッチまたは WCCP ルータを設定します。

> **重要**
> DNS プロキシ キャッシング オプションは、レイヤー 4 (L4) スイッチ、または WCCP v2 を実行している Cisco ルータでだけを利用できます。

Content Gateway Manager で下記の手順を実行します :

1. **[Configure] > [Networking] > [ARM] > [General]** の順に選択します。
2. **[Network Address Translation（ネットワーク アドレス変換 : NAT）]** セクションで **[Edit File]** をクリックして、**ipnat.conf** ファイルのためにファイル エディタを開きます。

3. 表示される各フィールドで情報を入力します：
   - **[Ethernet Interface（イーサネット インターフェース）]** フィールドで、クライアント DNS 要求がルーティングされる Content Gateway イーサネット インターフェースを入力します。例、eth0。
   - **[Connection Type（接続のタイプ）]** ドロップダウン リストで **udp** を選択します。
   - **[Destination IP（宛先 IP）]** フィールドで **0.0.0.0** と入力し、すべてのクライアントからの DNS 要求を受け入れます。
   - **[Destination CIDR（宛先 CIDR）]** フィールド（オプション）で CIDR マスク値を入力します。[Destination IP] フィールドで 0.0.0.0 を指定している場合は、ここに [0] を入力します。
   - **[Destination Port（宛先ポート）]** フィールドで、DNS 要求が Content Gateway に送られるとき使用されるポートを入力します。デフォルト ポートは 53 です。
   - **[Redirected Destination IP（リダイレクトされた宛先 IP）]** フィールドで Content Gateway の IP アドレスを入力します。
   - **[Redirected Destination Port（リダイレクトされた宛先ポート）]** フィールドで、Content Gateway が DNS サーバーとの通信で使用するポートを入力します。デフォルト ポートは 5353 です。
   - **[User Protocol（ユーザー プロトコル）]** ドロップダウン リストで **dns** を選択します。
4. **[Add]** をクリックし、次に **[Apply]** をクリックし、さらに **[Close]** をクリックします。要求される再起動は、ステップ 8 が終わってから行います。
5. **[My Proxy] > [Basic]** に移り、**[Features（機能）]** テーブルで **[Networking]** セクションの **[DNS Proxy]** を有効にして、**[Apply]** をクリックします。要求される再起動は、ステップ 8 が終わってから行います。
6. **[Networking] > [DNS Proxy]** に移ります。
7. **[DNS Proxy Port（DNS プロキシ ポート）]** フィールドで DNS プロキシ ポートを入力します。デフォルト ポートは 5353 です。
8. **[Apply]** をクリックし、Content Gateway を再起動します。
9. DNS トラフィックを Content Gateway の DNS ポートに送信するようにレイヤ 4 スイッチまたは WCCP v2 ルータを設定します（デフォルト：53）。

10 システムの構成

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は、システムを構成するための複数のオプションを提供します。

- *Content Gateway manager*、127 ページ
- *コマンドライン インターフェース*、129 ページ
- *設定ファイル*、129 ページ
- *構成の保存と復元*、130 ページ

多くの設定変更は、Content Gateway の再起動を必要とします。Content Gateway manager でそのような変更が行われた時、再起動が必要であることを知らせるメッセージが表示されます。コマンド ラインまたは設定ファイルでそのような変更が行われた場合は、通知はありません。再起動が必要か否か確認するには、Content Gateway のマニュアルを参照することを推奨します。

Content Gateway manager

Help | Content Gateway | バージョン 7.8.x

Content Gateway manager は、Content Gateway Web プロキシを構成するための Web ベースのユーザー インターフェースを提供します。

> **注意**
>
> 一部のオプションは、**records.config** ファイルで、またはコマンドライン インターフェースから設定変数の編集によってのみ変更できます。*コマンドライン インターフェース*、129 ページおよび*設定ファイル*、129 ページを参照してください。

Content Gateway manager へのログ オンの手順については、*Content Gateway manager へのアクセス*、13 ページを参照してください。

設定モードの使用

デフォルトでは、Content Gateway manager は、モニタ モードで開きます。

設定モードのボタンを表示するには、**[Configure（設定）]** タブをクリックします。

設定モードでは、Content Gateway manager は、一連のボタンを表示します。各ボタンは、設定オプションのグループを表します。

設定モードで利用可能なすべての設定オプションについては、*設定のオプション*で説明しています。

コマンドライン インターフェース

Help | Content Gateway | バージョン 7.8.x

Content Gateway manager の代わりに、コマンドライン インターフェースを使用して、Content Gateway の設定を表示および変更できます。

1. Content Gateway ノードに root としてログオンし、次に、ディレクトリを変更 ('cd') して Content Gateway **bin** ディレクトリ (/opt/WCG/bin) に移動します。
2. 構成の設定値を表示するには、下記のコマンドを入力します。

   ```
   ./content_line -r var
   ```

   ここで、*var* は、設定オプションに関連する変数です（変数のリストについては、*設定変数、475 ページ*を参照）。
3. 構成の設定値を変更するために、下記のコマンドを入力します。

   ```
   ./content_line -s var -v value
   ```

   ここで、*var* は、設定オプションに関連する変数であり、また *value* は、使用する値です。

   たとえば、FTP 非アクティブ タイムアウト オプションを 200 秒に変更するには、プロンプトに対して下記のコマンドを入力し、[Return（戻る）] を押します。

   ```
   ./content_line -s
   proxy.config.ftp.control_connection_timeout -v 200
   ```

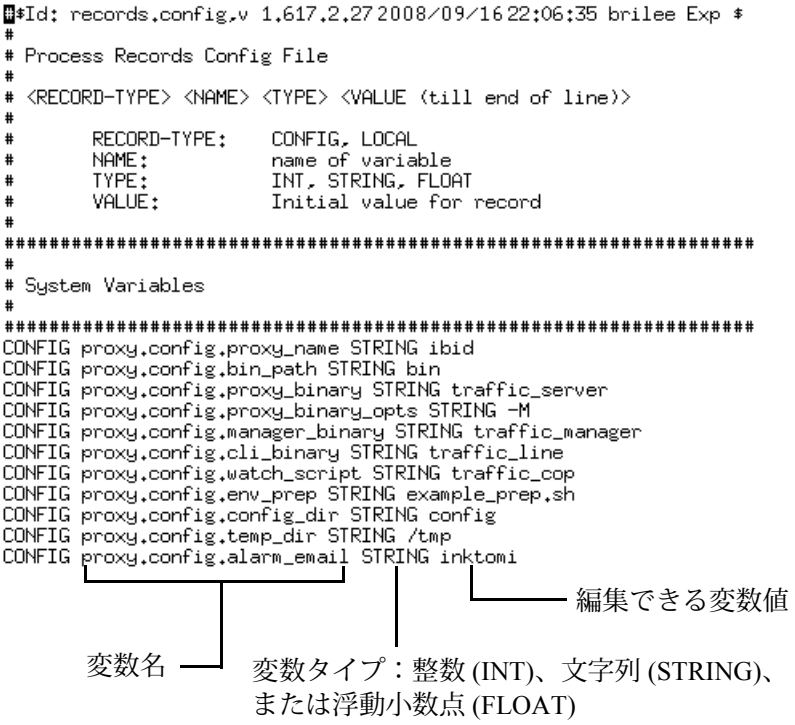
設定ファイル

Help | Content Gateway | バージョン 7.8.x

/opt/WCG/config にある **records.config** ファイルの特定の変数を編集することによって、Content Gateway の一部の設定オプションを変更できます。テキスト エディタ（**vi**、**emacs** など）でファイルを開き、変数の値を変更します。

> **注意**
>
> **records.config** ファイルを変更した後、Content Gateway はその設定ファイルを再読み込みする必要があります。それには、Content Gateway **bin** ディレクトリ **(/opt/WCG/bin)** から、下記のコマンドを入力します。
>
> ```
> ./content_line -x
> ```
>
> 場合によっては、プロキシを再起動し、変更を適用する必要があります。

下記の数字は、**records.config** ファイルのサンプルの部分を示しています。



Content Gateway は、特定の機能を設定するために使用するその他の設定ファイルを提供します。すべて設定ファイルは*設定ファイル*、441 ページで説明しています。

構成の保存と復元

Help | Content Gateway | バージョン 7.8.x

構成スナップショット機能を使用して、現在のすべての構成の設定値を保存し、必要に応じてそれらを復元できます。Content Gateway は、構成のスナップショットをそれらが撮られるノード、FTP サーバー、およびポータブル メディア上に保存できます。Content Gateway は、クラスタ内のすべてのノード上で構成のスナップショットを復元します。

注意

構成のスナップショットを撮ってから、システム保守を実行したり、システム パフォーマンスを微調整することを推奨します。構成のスナップショットを撮るにはほんの数秒ですみます。

このセクションでは、下記のタスクを実行する方法について説明しています。

- 現在の構成のスナップショットを撮る。*構成のスナップショットを撮る、131 ページ*を参照してください。
- 以前に撮った構成のスナップショットを復元する。*構成のスナップショットの復元、132 ページ*を参照してください。
- Content Gateway ノード上に保存されている構成のスナップショットを削除する。*構成のスナップショットの削除、132 ページ*を参照してください。

構成のスナップショットを撮る

Help | Content Gateway | バージョン 7.8.x

現在のすべての構成の設定値を Content Gateway manager の機能を使用して Content Gateway システムに保存できます。

構成のスナップショットを撮り、それをローカル システムに保存するには、下記の手順を実行します

1. **[Configure] > [Snapshots] > [File System]** を順に選択します。
2. **[Change Snapshot Directory（スナップショット ディレクトリを変更）]** フィールドに、Content Gateway が構成のスナップショットを保存するディレクトリの名前が表示されます。デフォルトの場所は、Content Gateway **config/snapshots** ディレクトリです。ディレクトリを変更するには、**[Change Snapshot Directory]** フィールドに絶対パスを入力します。相対パスを入力した場合は、Content Gateway は、そのディレクトリが **config** ディレクトリにあると想定します。
3. **[Save Snapshot]** フィールドに現在の構成に使用する名前を入力します。
4. **[Apply]** をクリックします。

構成のスナップショットを撮り、それを FTP サーバーに保存するには、下記の手順を実行します

1. **[Configure] > [Snapshots] > [FTP Server]** を順に選択します。
2. 表示されたフィールドに、FTP サーバー名、ログイン およびパスワード、および FTP サーバーが構成のスナップショットを保存するリモート ディレクトリを入力します。
3. **[Apply]** をクリックします。

   FTP サーバーに正常にログ オンした後、**[FTP Server]** ページに追加のフィールドが表示されます。
4. **[Save Snapshot to FTP Server（FTP サーバーにスナップショットを保存）]** フィールドに、撮る構成のスナップショットの名前を入力します。
5. **[Apply]** をクリックします。

構成のスナップショットの復元

Help | Content Gateway | バージョン 7.8.x

Content Gateway サーバーのクラスタを実行している場合、構成はそのクラスタ内のすべてのノードに復元されます。

ローカルノード上に保存されている構成のスナップショットを復元するには、下記の手順を実行します

1. **[Configure] > [Snapshots] > [File System]** タブを順に選択します。
2. **[Restore（復元）] > [Delete Snapshot（スナップショットを削除）]** ドロップダウン リストから、復元する構成のスナップショットを選択します。
3. **[Restore Snapshot from “directory_name” Directory（ [directory_name] ディレクトリからスナップショットを復元）]** ボックスをクリックします。
4. **[Apply]** をクリックします。

   Content Gateway システムまたはクラスタは、復元された構成を使用します。

FTP サーバーから構成のスナップショットを復元するには、下記の手順を実行します

1. **[Configure] > [Snapshots] > [FTP Server]** を順に選択します。
2. 表示されたフィールドに、FTP サーバー名、ログイン およびパスワード、および FTP サーバーが構成のスナップショットを保存するリモートディレクトリを入力します。
3. **[Apply]** をクリックします。

   FTP サーバーに正常にログ オンした後、**[FTP Server]** タブにに追加のフィールドが表示されます。
4. **[Delete Snapshot（スナップショットを削除）]** ドロップダウン リストで、復元する構成のスナップショットを選択します。
5. **[Apply]** をクリックします。

   Content Gateway システムまたはクラスタは、復元された構成を使用します。

構成のスナップショットの削除

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Snapshots] > [File System]** を順に選択します。
2. **[Restore] > [Delete Snapshot）]** ドロップダウン リストから、削除する構成のスナップショットを選択します。
3. **[Delete Snapshot from “directory_name” directory（ [directory_name] ディレクトリからスナップショットを削除）]** ボックスをクリックします。
4. **[Apply]** をクリックします。

   構成のスナップショットが削除されます。

11 トラフィックのモニタリング

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は、システム パフォーマンスをモニタし、ネットワーク トラフィックを分析するために下記のツールを提供します。

- Content Gateway のパフォーマンスとネットワーク トラフィック情報を示す統計。*統計の表示*、133 ページを参照してください。コマンドライン インターフェースは、この情報を表示するための代わりの方法を提供します。*コマンドラインからの統計の表示*、138 ページを参照してください。
- 検出したエラー条件を知らせるアラーム。*アラームの処理*、139 ページを参照してください。
- Content Gateway のパフォーマンスとネットワーク トラフィックの履歴情報を示すパフォーマンス グラフ。*パフォーマンス グラフの使用*、140 ページを参照してください。
- 認証機関およびインシデントのステータスを含む SSL トラフィックのレポート。*SSL 関連レポートの作成*、142 ページを参照してください。

統計の表示

Help | Content Gateway | バージョン 7.8.x

Content Gateway manager を使用して、Content Gateway のパフォーマンスおよび Web トラフィックに関する統計を収集し、解釈します。モニタ モードを使用して統計を表示します。

Content Gateway manager へのログ オンの手順については、*Content Gateway manager へのアクセス*、13 ページを参照してください。

モニタ モードの使用

モニタ モードの場合、Content Gateway manager は、ディスプレイの左側に一連のボタンを表示します。統計を表示するには、ボタンをクリックします。

モニタ モードで表示されるすべての統計の詳細については、*統計*、301 ページを参照してください。

My Proxy（マイプロキシ）

Content Gateway に関する統計を表示するには、**[My Proxy（マイ プロキシ）]** をクリックします。

- Content Gateway システムの簡潔なビューを表示するには、**[Summary（要約）]** をクリックします。ページの上部は、有効期限を含む、Websense Web Security Gateway サブスクリプションの機能に関する情報を表示します。ページの中間部分は、使用中のスキャンニング エンジンとそれに関連するデータ ファイルに関する情報を表示します。ページの下部は、プロキシ ノードに関する統計を含み、名前別にすべてのクラスタ ノードを表示し、各ノードの必須の統計を追跡します。クラスタ内の特定のノードに関する詳細情報を表示する場合、[Summary] テーブルでノードの名前をクリックし、次に **[Monitor（モニタ）]** タブ上の別のいずれかのボタンをクリックします。
- 選択したノードに関する情報を表示するには、**[Node（ノード）]** をクリックします。ノードがアクティブか非アクティブかを確認でき、また **content_gateway** プロセスが開始された日付および時刻、キャッシュのパフォーマンス情報（ドキュメント ヒット率、帯域幅の節約量、現在のキャッシュの空き容量の割合 (%)）、現在開いているクライアントとサーバーの接続の数、および現在進捗中の転送の数を確認できます。また、ホスト データベースのヒット率および秒あたりの DNS ルックアップの数など、名前解決情報を確認できます。

  注意
  ノードがクラスタの一部である場合は、次の 2 組の統計が表示されます。シングル ノードに関する情報とクラスタ内のすべてのノードの平均値を示す情報です。グラフ形式で情報を表示するには、統計の名前をクリックします。

- **[Node（ノード）]** ページに表示される同じ統計（キャッシュのパフォーマンス、現在の接続および転送、ネットワーク、および名前解決）をグラフ形式で表示するには、**[Graphs（グラフ）]** をクリックします。1 つのグラフに複数の統計を表示できます。

特定の統計をグラフ形式で表示するには、グラフの名前の隣のボックスをクリックし、次に **[Graph]** をクリックします。1 つのグラフに複数の統計を表示するには、表示する各グラフの名前の隣のボックスをクリックし、次に **[Graph]** をクリックします。

> **重要**
> グラフは Java アプレットを使用しているブラウザに表示されます。使用する PC に Java の最新のバージョン（バージョン 1.7 以上）がインストールされている必要があります。Content Gateway 統計へのユーザーのアクセス権を検証するために、Content Gateway ログオン資格情報の入力が求められます。

- Content Gateway が生成したアラームを表示するには、**[Alarms（アラーム）]** をクリックします。*アラームの処理*、139 ページを参照してください。

Protocols（プロトコル）

Protocols ボタンは、HTTP および FTP のトランザクションに関する情報を提供します。

- HTTP のトランザクションおよび速度（キャッシュ ミス、キャッシュ ヒット、接続エラー、中断されたトランザクションなど）に関する情報、およびクライアントとサーバーの接続情報を確認するには、**[HTTP]** をクリックします。また、開いている FTP サーバー接続の数、成功および失敗した PASV と PORT 接続の数、キャッシュのルックアップ、ヒット、およびミスの数など HTTP クライアントからの FTP 要求に関する情報を確認できます。
- FTP クライアントからの FTP 要求に関する情報を確認するには、**[FTP]** をクリックします。

> **注意**
> **[FTP]** ボタンは、**[Configure] > [My Proxy] > [Basic]** タブの **[Features]** テーブルで FTP 処理を有効化している場合にだけ表示されます。

Security（セキュリティ）

Security ボタンは、下記に示すようにプロキシ認証、および SOCKS サーバー接続に関する情報を提供します。

- LDAP キャッシュ ヒットおよびミスの数、および LDAP 認証サーバー エラーの数と失敗した認証の試行回数を確認するには、**[LDAP]** をクリックします。[LDAP] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [LDAP] オプションを有効化した場合だけ表示されます。
- NTLM キャッシュ ヒットおよびミスの数、および NTLM 認証サーバー エラーの数と失敗した認証の試行回数を確認するには、**[NTLM]** をクリックします。[NTLM] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [NTLM] オプションを有効化した場合だけ表示されます。
- 折衝済み要求のカウンタ、HTLM 要求カウンタ、および基本認証要求カウンタを確認するには、**[Integrated Windows Authentication（統合 Windows 認証）]** (IWA) をクリックします。[IWA] タブは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [IWA] オプションを有効化した場合だけ表示されます。
- SOCKS サーバーへの接続の成功回数と失敗回数、および現在進捗中の接続の数を確認するには **[SOCKS]** をクリックします。[SOCKS] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [SOCKS] オプションを有効化した場合だけ表示されます。

Subsystems（サブシステム）

Subsystems ボタンは、下記のようなプロキシ キャッシュ、クラスタ、イベント ロギングに関する情報を提供します。

- プロキシ キャッシュに関する情報を確認するには、**[Cache（キャッシュ）]** をクリックします。現在使用中のキャッシュの空き容量、キャッシュのギガバイト単位の合計サイズ、RAM キャッシュのバイト単位の合計サイズ、RAM キャッシュのヒットおよびミスの数、キャッシュ ルックアップ、オブジェクトの読み込み、書き込み、更新、および削除の数を示します。
- クラスタ内のノードの数、クラスタ操作の合計の数、クラスタ内のすべてのノードへのバイト読み取りおよび読み込みの数、およびクラスタ内のオープン接続の現在の数を確認するには、**[Clustering]** をクリックします。
- 現在開いているログ ファイルの数、ログ ファイルに現在使用中のスペースの量、ログされたアクセス イベントとエラー イベントの数、スキップされたアクセス イベントの数を確認するには、**[Logging（ロギング）]** をクリックします。

Networking（ネットワーク）

Networking ボタンは、システム ネットワーク構成、ARM ルーター、WCCP ルーター、DNS プロキシ、ドメイン名解決、仮想 IP アドレス指定に関する情報を提供します。

- プロキシ コンピュータおよびデフォルト ゲートウェイに割り当てられたホスト名、検索ドメイン、プロキシ コンピュータが使用する DNS サーバーを含むシステム ネットワーク構成を確認するには、**[System（システム）]** をクリックします。
- Network Address Translation（ネットワーク アドレス変換）および動的バイパスに関する情報を確認するには、**[ARM]** をクリックします。
- WCCP v2 フラグメント化の統計、Content Gateway ノードで有効にされている各 WCCP サービス グループの構成を確認するには、**[WCCP]** をクリックします。[WCCP] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで WCCP を有効化した場合だけ表示されます。
- Content Gateway によって処理された DNS 要求の合計数、およびキャッシュのヒットとミスの数を確認するには、**[DNS Prox（DNS プロキシ）]** をクリックします。[DNS Proxy] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [DNS Proxy] オプションを有効化している場合だけ表示されます。
- ホスト データベース内のルックアップとヒットの合計数、および DNS サーバーでの平均ルックアップ時間、ルックアップの合計数、成功したルックアップの数を確認するには、**[DNS Resolver（DNS リゾルバ）]** をクリックします。
- 現在の仮想 IP アドレス マッピングを確認するには、**[Virtual IP Address（仮想 IP アドレス）]** をクリックします。[Virtual IP Address] ボタンは、**[Configure] > [My Proxy] > [Basic] > [General]** の [Features] テーブルで [Virtual IP] オプションを有効化した場合にだけ表示されます。
- 現在の接続のクライアント接続の合計、最後の再起動以降の一意なクライアントの数、接続制限を超えたクライアントの数、および接続が閉じたクライアントの数を表示するには、**[Client Connections（クライアント接続）]** をクリックします。

パフォーマンス

Performance ボタンは、パフォーマンスの履歴的グラフを表示します。*パフォーマンス グラフの使用*、140 ページを参照してください。

SSL

[SSL] ボタンは、SSL キー データ、証明書取り消し、CCSP カウント、および SSL ログに関する情報および統計を提供します。

- SSL サービス ヘルス（動作中）、接続統計、および SSL セッション キャッシュのヒットとミスに関する情報を確認するには、**[SSL Key Data（SSL キー データ）]** ボタンをクリックします。

CRL および OCSP の統計を確認するには、**[CRL Statistics（CRL の統計）]** をクリックします。

Certificate Authority レポートおよびインシデント レポートを生成するには、[Reports（レポート）] をクリックします。

コマンドラインからの統計の表示

Help | Content Gateway | バージョン 7.8.x

コマンドライン インターフェースを使用して Content Gateway のパフォーマンスおよび Web トラフィックに関する統計を表示できます。

またコマンドラインから Content Gateway を構成、停止、再起動することもできます。*コマンドライン インターフェース*、129 ページおよび *Websense Content Gateway の変数*、330 ページを参照してください。

Content Gateway のノードまたはクラスタに関する特定の情報を表示するには、下記の手順を実行し、表示対象の統計に対応する変数を指定します。

1. root に移動します。

   ```
   su
   ```

2. Content Gateway ノードにログオンします。
3. Content Gateway **bin** ディレクトリ (/opt/WCG/bin) から、下記のコマンドを入力します。

   ```
   ./content_line -r variable
   ```

   ここで **variable** は、表示対象の情報を表す変数です。指定できる変数のリストについては、*Websense Content Gateway の変数*、330 ページを参照してください。

   たとえば、下記のコマンドは、ノードのドキュメント ヒット率を表示します。

   ```
   content_line -r proxy.node.http.cache_hit_ratio
   ```

アラームの処理

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、問題を検出したとき、例えばイベント ログに割り当てられたスペースがいっぱいになった場合、または設定ファイルに書き込みできない場合に、アラームを生成します。

すべてのアラームが重要というわけではありません。一部のアラームは、一時的な状況を報告します。たとえば、インタネット接続での一時的な中断によって **Content Gateway subscription download failed: error connecting** アラームが生成されることがあります。

下記に示すような現在のアラームのリストを表示するには、**[Monitor（モニタ）] > [My Proxy] > [Alarms（アラーム）]** に移動します。

注意

Content Gateway はまた、いくつかの選択したアラームを Web Security manager に送信します。そこではそれらは**アラート**と呼ばれます。要約アラート メッセージは、Web Security **[Status（ステータス）] > [Today（本日）]** ページに表示されます。Web Security 管理者は、Content Gateway がどのような状態でアラート メッセージを生成するか、およびどのような方法でアラートを送信するか（電子メールまたは SNMP）を、**[Sttomgs] > [Alerts]** ページで設定できます。

アラームの解除

アラーム メッセージを読み取った後、アラームを除去するには、アラーム メッセージ ウィンドウの **[Clear（クリア）]** をクリックします。アラーム メッセージ、566 ページに、Content Gateway が生成するいくつかのアラーム メッセージの説明を示しています。

> **重要**
>
> **[Clear]** をクリックするとアラーム メッセージを除去するだけです。アラームの原因を解決しません。

同じアラーム状況が 2 度発生した場合、最初のアラームが解除されなかった場合は 2 度目のアラームはログされません。

アラーム メッセージを電子メール送信するように Content Gateway を構成する

1. **[Configure] > [My Proxy] > [Basic] > [General]** タブの順に選択します。
2. **[Alarm eMai（アラーム電子メール）]** フィールドに、アラームの送信先の電子メール アドレスを入力します。下記の例のような @ 記号を含む完全な電子メール アドレスを必ず使用してください。

   ```
   receivername@example.com
   ```

3. **[Apply]** をクリックします。

アラームのスクリプト ファイルの使用

アラーム メッセージは、Content Gateway に組み込まれています。それらを変更できません。しかし、アラームが生成されたとき特定のアクションを実行するようにスクリプト ファイルに書き込むことができます。

example_alarm_bin.sh という名前のサンプルのスクリプト ファイルが **/opt/WCG/bin** にあります。このファイルを変更できます。

パフォーマンス グラフの使用

Help | Content Gateway | バージョン 7.8.x

パフォーマンス グラフ表示ツール (Multi Router Traffic Grapher) を使って Content Gateway のパフォーマンスをモニタし、ネットワーク トラフィックを分析できます。パフォーマンス グラフは、仮想メモリ使用量、クライアント接続、キャッシュのヒット率およびミス率などに関する情報を示します。表示された情報は、Content Gateway が起動した時刻から記録されます。統計は、5 分間隔で収集されます。

パフォーマンス グラフにアクセスするには、**[Monitor] > [Performance]** を順に選択します。

> **重要**
> Multi Router Traffic Grapher（パフォーマンス グラフ表示ツール）を実行するには、Content Gateway システム上に Perl v5.005 以上をインストールしている必要があります。

1. Content Gateway ノードがクラスタに含まれている場合は、**[Monitor] > [My Proxy] > [Summary（要約）]** ディスプレイから表示する統計のノードを選択します。
2. **[Monitor]** タブで **[Performance（パフォーマンス）]** をクリックします。
3. 利用可能なグラフのサブセットを表示するには、**[Overview（概要）]** をクリックします。

   本日の統計を表示するには、**[Daily（毎日）]** をクリックします。

   今週の統計を表示するには、**[Weekly（毎週）]** をクリックします。

   今月の統計を表示するには、**[Monthly（毎月）]** をクリックします。

   今年の統計を表示するには、**[Yearly（毎年）]** をクリックします。
4. Content Gateway の起動の後、少なくとも 15 分間待機してからグラフを見ます。ツールは 5 分間のサンプルをいくつか処理してから統計を初期化します。

Multi Router Traffic Grapher（MRTG）を構成していない場合、システムは、それが利用できないことを示すメッセージを表示します。ツールを構成するには、以下の手順を行います。

1. システムに Perl 5.005 がインストールされていることを確認します。
2. コマンド プロンプトで下記のように入力します。

   ```
   perl ./pathfix.pl 'which perl'
   ```

   これによって perl バイナリが PATH にあることを確認します。
3. Content Gateway の **bin** ディレクトリ (/opt/WCG/bin) に変更します。
4. コマンド プロンプトで下記のように入力して MRTG 更新の間隔を変更します。

   ```
   ./update_mrtg;sleep 5;./update_mrtg;sleep 5;
   ```

   デフォルトでは MRTG 更新の間隔は 15 分に設定されています。このコマンドは、更新を 5 分に設定します。
5. 下記のコマンドを入力して MRTG cron 更新を開始します。

   ```
   ./mrtgcron start
   ```
6. 約 15 分間待ってから、Content Gateway manager からパフォーマンス グラフにアクセスします。

注意

MRTG cron 更新を停止するには、下記のコマンドを入力します。

```
./mrtgcron stop
```

SSL 関連レポートの作成

Help | Content Gateway | バージョン 7.8.x

認証機関のステータスを詳述するレポート（*認証機関*、142 ページを参照）、またはインシデントのリストを示すレポート（*Incidents（インシデント）*、144 ページを参照）を要求できます。

レポートは、HTML 形式か、カンマ区切り形式にできます。カンマ区切りのレポートは、Excel スプレッドシートとして表示されます。

認証機関

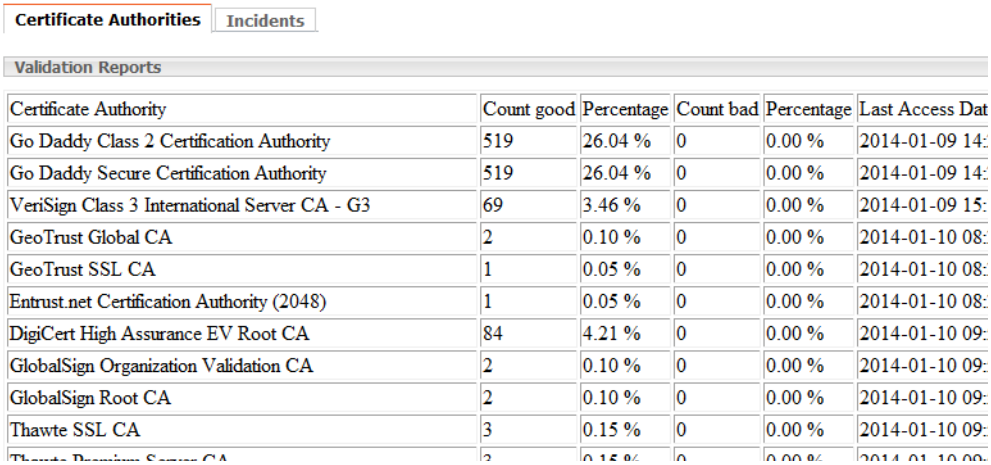
Help | Content Gateway | バージョン 7.8.x

1. **[Monitor] > [SSL] > [Reports] > [Certificate Authorities（認証機関）]** タブを順に選択します。
2. レポートの形式を選択します。
   a. HTML
   b. Comma-separated values (CSV)

      CSV を選択した場合、レポートは Excel スプレッドシートとして作成されます。
3. レポートが対象とする期間を指定します。
   a. 日数
   b. 現在に及ぶ開始日
   c. ログ内のすべてのレコード
4. レポートのソート順序を指定します。
   a. 日付別に機関をリストする
   b. OCSP 適切な応答を最初にリストする
   c. OCSP 不良な応答を最初にリストする

   最新の取り消し情報を保持する、186 ページ を参照してください。
5. レポートを生成するには、**[Generate Report]** をクリックします。

HTML 出力は下記のように示されます。

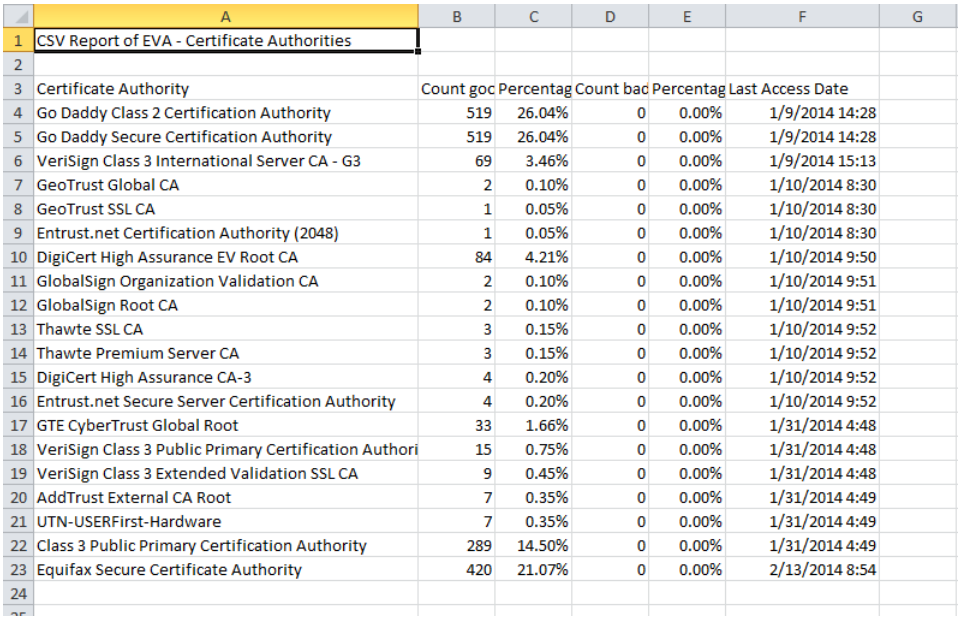


Certificate Authorities | Incidents

Validation Reports

Certificate Authority	Count good	Percentage	Count bad	Percentage	Last Access Dat
Go Daddy Class 2 Certification Authority	519	26.04 %	0	0.00 %	2014-01-09 14:
Go Daddy Secure Certification Authority	519	26.04 %	0	0.00 %	2014-01-09 14:
VeriSign Class 3 International Server CA - G3	69	3.46 %	0	0.00 %	2014-01-09 15:
GeoTrust Global CA	2	0.10 %	0	0.00 %	2014-01-10 08:
GeoTrust SSL CA	1	0.05 %	0	0.00 %	2014-01-10 08:
Entrust.net Certification Authority (2048)	1	0.05 %	0	0.00 %	2014-01-10 08:
DigiCert High Assurance EV Root CA	84	4.21 %	0	0.00 %	2014-01-10 09:
GlobalSign Organization Validation CA	2	0.10 %	0	0.00 %	2014-01-10 09:
GlobalSign Root CA	2	0.10 %	0	0.00 %	2014-01-10 09:
Thawte SSL CA	3	0.15 %	0	0.00 %	2014-01-10 09:

カンマ区切りの形式の同じレポートは、下記のように表示されます。



	A	B	C	D	E	F	G
1	CSV Report of EVA - Certificate Authorities						
2							
3	Certificate Authority	Count goc	Percentag	Count bad	Percentag	Last Access Date	
4	Go Daddy Class 2 Certification Authority	519	26.04%	0	0.00%	1/9/2014 14:28	
5	Go Daddy Secure Certification Authority	519	26.04%	0	0.00%	1/9/2014 14:28	
6	VeriSign Class 3 International Server CA - G3	69	3.46%	0	0.00%	1/9/2014 15:13	
7	GeoTrust Global CA	2	0.10%	0	0.00%	1/10/2014 8:30	
8	GeoTrust SSL CA	1	0.05%	0	0.00%	1/10/2014 8:30	
9	Entrust.net Certification Authority (2048)	1	0.05%	0	0.00%	1/10/2014 8:30	
10	DigiCert High Assurance EV Root CA	84	4.21%	0	0.00%	1/10/2014 9:50	
11	GlobalSign Organization Validation CA	2	0.10%	0	0.00%	1/10/2014 9:51	
12	GlobalSign Root CA	2	0.10%	0	0.00%	1/10/2014 9:51	
13	Thawte SSL CA	3	0.15%	0	0.00%	1/10/2014 9:52	
14	Thawte Premium Server CA	3	0.15%	0	0.00%	1/10/2014 9:52	
15	DigiCert High Assurance CA-3	4	0.20%	0	0.00%	1/10/2014 9:52	
16	Entrust.net Secure Server Certification Authority	4	0.20%	0	0.00%	1/10/2014 9:52	
17	GTE CyberTrust Global Root	33	1.66%	0	0.00%	1/31/2014 4:48	
18	VeriSign Class 3 Public Primary Certification Authori	15	0.75%	0	0.00%	1/31/2014 4:48	
19	VeriSign Class 3 Extended Validation SSL CA	9	0.45%	0	0.00%	1/31/2014 4:48	
20	AddTrust External CA Root	7	0.35%	0	0.00%	1/31/2014 4:49	
21	UTN-USERFirst-Hardware	7	0.35%	0	0.00%	1/31/2014 4:49	
22	Class 3 Public Primary Certification Authority	289	14.50%	0	0.00%	1/31/2014 4:49	
23	Equifax Secure Certificate Authority	420	21.07%	0	0.00%	2/13/2014 8:54	
24							

注意

収集した SSL ログ データを削除するには、**[Reset all collected data]** をクリックします。

Incidents（インシデント）

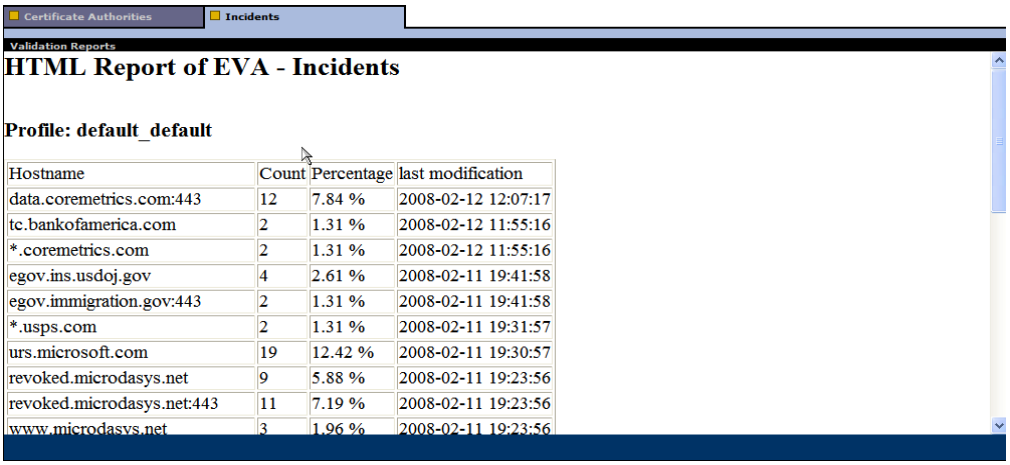
Help | Content Gateway | バージョン 7.8.x

SSL インシデントのレポートを作成するには、下記の手順を実行します。

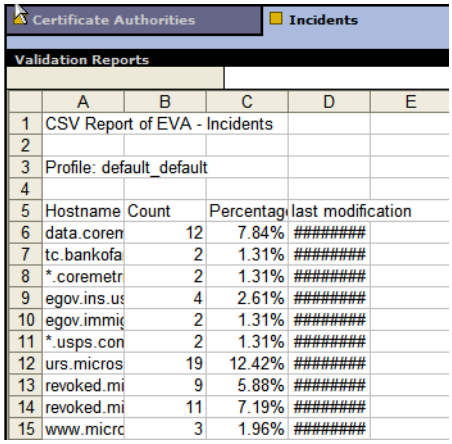
1. **[Monitor] > [SSL] > [Reports] > [Incidents（インシデント）]** タブを順に選択します。
2. HTML 形式、またはカンマ区切り形式を選択します。カンマ区切り形式を選択場合、レポートは Excel スプレッドシートとして作成されます。
3. レポートが対象とする期間を指定します。下記のいずれかを指定できます。
   a. 日数
   b. 日付範囲
   c. SSL サポートが有効化されて以降の期間
4. レポートのソート順序を指定します。
   a. 日付別にインシデントをリストする
   b. URL 別にインシデントをリストする
   c. 各インシデントが発生した回数をリストする

   HTTPS Web サイトのアクセスの管理、188 ページを参照してください。
5. レポートを生成するには、**[Generate Report]** をクリックします。

HTML 出力は下記のように示されます。



カンマ区切りの形式の同じレポートは、下記のように表示されます。


Certificate Authorities
Incidents
Validation Reports

	A	B	C	D	E
1	CSV Report of EVA - Incidents				
2					
3	Profile: default_default				
4					
5	Hostname	Count	Percentag	last modification	
6	data.coren	12	7.84%	########	
7	tc.bankofa	2	1.31%	########	
8	*.coremetr	2	1.31%	########	
9	egov.ins.us	4	2.61%	########	
10	egov.immig	2	1.31%	########	
11	*.usps.con	2	1.31%	########	
12	urs.micros	19	12.42%	########	
13	revoked.mi	9	5.88%	########	
14	revoked.mi	11	7.19%	########	
15	www.micrc	3	1.96%	########	

注意

収集した SSL ログ データを削除するには、**[Reset all collected data]** をクリックします。

12 Websense Data Security の使用

関連項目：

- *Data Security の登録と構成*、150 ページ
- *ICAP クライアントの構成*、154 ページ
- *ICAP フェールオーバーとロード バランシング*、156 ページ

Websense Content Gateway は、Websense Data Security コンポーネントと共に、下記の機能をサポートします。

- Web Security Gateway を使用する場合の Threats ダッシュボード
- Web Security Gateway Anywhere を使用する場合の Web データ 損失防止 (DLP) および Threats ダッシュボード

Web Security Gateway を使用する場合の Threats ダッシュボード

Content Gateway と Web Security Gateway を合わせて配備している場合、Content Gateway および TRITON 管理サーバー上にいくつかの Data Security コンポーネントがインストールされ、Web Security Threats ダッシュボードをサポートします（Web Security Help を参照）。これらのコンポーネントには、Data Security Policy Engine（Content Gateway コンピュータ上）、および TRITON 管理サーバー上の Data Security Forensics Repository が含まれます。

Content Gateway は最初に構成されたときこれらのコンポーネントに登録し、それ以降は、再起動時に登録ステータスをチェックし、必要に応じて自動的に再登録します。

Web Security Gateway Anywhere を使用する場合の Web DLP および Threats ダッシュボード

Content Gateway が Web Security Gateway Anywhere（または Web Security Gateway およびフル Data Security サブスクリプション）と合わせて配備されているとき、Threats ダッシュボード内のフォレンシック データ、および HTTPS、FTP、FTP over HTTP などの Web チャネル上でのデータ損失防止（DLP）などの機能がサポートされます。（フル Data Security 環境は、Web DLP がモバイル デバイス、リムーバブル メディア、プリンタなどのチャネルを含むように拡張できます。Websense Data Security の詳細については、www.websense.com の Data Security 製品のページを参照してください。

Web DLP、および拡張 Data Security 構成では、Data Security と他の Data Security のコンポーネントを別々にインストールする必要があります。Content Gateway を Data Security と合わせて使用するように構成する場合、Websense Technical Library で提供している配備およびインストール情報を参照してください。

Content Gateway を Data Security と合わせて使用する 2 つの方法があります。

- 推奨：Data Security のコンポーネントを Content Gateway と合わせてインストールする。
- ICAP 上で、別のホスト上にある Data Security のコンポーネントを使用する。Data Security Suite バージョン 7.1 以前で使用する場合。

2 つの方法を同時に使用することはできません。

Web DLP のしくみ

下記で説明している Web DLP データ フローのほかに、特別な解析エンジンを有効化するとアウトバウンド トラフィックを解析してデータ脅威をチェックすることができます。Web Security manager で、**[Scanning（スキャン）] > [Scanning Options（スキャンのオプション）]** を順に選択し、**[Outbound security（アウトバウンド セキュリティ）]** を参照してください。

Web DLP データ フローは下記のように機能します。

1. プロキシは、アウトバウンド コンテンツを傍受し、そのコンテンツを Data Security に提供します。
2. Data Security は、そのコンテンツを分析して、Web 転送または FTP アップロードを許可するか、またはブロックするかを決定します。
   - この決定は、Data Security Web DLP ポリシーに基づいて行われます。
   - ディスポジションは、プロキシに伝達されます。
   - Data Security は、トランザクションをログに記録します。

3. プロキシは、Data Security の決定に影響を与えます。
   a. コンテンツがブロックされた場合、そのコンテンツはリモート ホストに送信されず、Data Security は送信者にブロック ページを返します。
   b. コンテンツが許可された場合、コンテンツはその宛先に転送されます。

> **注意**
>
> 要求がブロックされ、DLP サーバーが応答でブロック ページを送信するとき、下記の事柄が行われます。
>
> - Content Gateway は、ブロック ページを 403 Forbidden メッセージの形式で送信者に転送します。
> - ブロック ページは 512 キロバイト以上であるか、または一部のユーザー エージェント（例、Internet Explorer）は一般的なエラー メッセージに置き換えます。
> - ブロック ページをカスタマイズできます。Modifying Data Endpoint Confirm And Block Messages を参照してください。

HTTP、HTTPS、FTP、および FTP over HTTP を使用するトランザクションが検査されることがあります。

トランザクションの詳細情報は、Data Security によってその構成ごとにログに記録されます。

Content Gateway と共にインストールされた Data Security コンポーネント

Content Gateway をインストールした場合、いくつかの Data Security コンポーネントが同じコンピュータにインストールされます。Content Gateway は最初に構成されたときこれらのコンポーネントに登録し、それ以降は再起動時に常に登録ステータスをチェックし、必要の応じて自動的に再登録します。Data Security の登録の詳細については、*Data Security の登録と構成*、150 ページを参照してください。

Data セキュリティ マネージャでポリシーが作成され、配備された後、Content Gateway は、分析およびポリシーの実施のために、転送やアップロードなどのコンテンツを Data Security に送信します。

Content Gateway は、以下のよう Data Security のトランザクションの統計を収集し、表示します。

- 転送の合計数
- 分析した転送の合計数

- 分析した FTP アップロードの数
- ブロックした要求の数
- 等々

これらの統計を Content Gateway manager で表示するには、**[Monitor] > [Security] > [Data Security]** を順に選択します。統計の完全なリストについては、*Data Security*、314 ページを参照してください。

ICAP を使用する Data Security

Data Security ポリシー エンジンが別のホストにあるとき、Content Gateway は、ICAP v1.0 準拠の Data Security と通信できます。構成の詳細については*ICAP クライアントの構成*、154 ページを参照してください。推奨する配備は、オンボックス コンポーネントとの統合です。

Data Security の登録と構成

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *ICAP クライアントの構成*、154 ページ

Websense Data Security の概要については、*Websense Data Security の使用*、147 ページを参照してください。

登録と構成の要約：

- コンピュータにインストールされている Data Security コンポーネントへの登録は自動的に行われます。構成は不要です。

  Threat ダッシュボードのフォレンシック データは、Websense Web Security によって自動的に収集されます。

  登録が失敗した場合、アラームが表示されます。

- オフボックス Data Security Management Server への登録は、**[Configure] > [My Proxy] > [Basic] > [Data Security] > [Integrated on-box（コンピュータに統合済み）]** が有効化され、Content Gateway が再起動さた後自動的に行われます。

  Content Gateway は、Data Security Management Server の存在を TRITON コンソールに問い合わせます。

重要

Content Gateway と Data Security Management Server のシステム時間は差が数分以内になるように同期化する必要があります。

Content Gateway が起動されるたびに、登録が検査され、必要に応じて再登録されます。

自動登録が失敗した場合、アラームが表示されます。

重要

Data Security と Content Gateway は、下記のように複数のポートを通じて通信します。IPTable が Content Gateway ホスト システムに構成されている場合、これらの ポートを IPTables で開く必要があります。下記の Technical Library の関連記事を参照してください。Content Gateway Ports、および Configuring IPTables for Websense Content Gateway。

- Web DLP ポリシーは、**System Modules** セクションの Data Security manager で構成されます。Data Security ポリシーを有効にするために、それらのポリシーを**配備**する必要があります。詳細については、Data Security Help を参照してください。
- **[More Detail（詳細）]** をクリックし、**[Subscription Details（サブスクリプションの詳細）]** セクションの下部のリストをチェックすることによって、**[Monitor] > [Summary]** ページで Content Gateway manager の登録ステータスを表示します。
- 登録の成功および失敗の情報は下記のファイルにログ記録されます。/opt/WCG/logs/dss_registration.log

登録と構成の詳細

Web Security Gateway を配備する場合でも Web Security Gateway Anywhere を配備する場合でも、Forensics Repository への登録は自動的に行われます。追加の構成はありません。

Web DLP を使用するために Web Security Gateway Anywhere を配備する場合は、下記の手順で Content Gateway manager で Data Security の統合を有効にする必要があります。

- **[Configure] > [My Proxy] > [Basic]** を順に選択し、**[Data Security > Integrated on-box（コンピュータに統合された Data Security）]** を有効にします。このオプションが有効に**されなかった**場合、登録は Forensics Repository にのみ行われます。

重要

[Data Security >Integrated on-box] を有効化する前に、Content Gateway コンピュータと Data Security Management Server コンピュータが実行しておりアクセス可能であること、またそれらのシステム クロックが数分以内で同期化していることを確認します。

[Data Security > Integrated on-box] が有効化された後、**Data Security Management Server** への登録は自動的に行われ、Content Gateway が起動するたびに必要に応じて実行されます。登録を実行するために、Content Gateway は、IP アドレスやクラスタ ID を含む必要な情報について Websense Web Security Policy Broker に問い合わせます。

[More Detail] をクリックし、**[Subscription Details]** セクションの下部のリストをチェックすることによって、**[Monitor] > [Summary]** ページで Content Gateway Manager の登録ステータスを表示できます。

登録が完了した後、Content Gateway は、マルウェア検出のために Web DLP ポリシー エンジンを使用します。Data Security manager に移動し、Web DLP のポリシーを構成し、配備します。Data Security manager で Web DLP を配備する必要があります。

自動登録が失敗した場合、アラームが表示されます。

手動登録

[Data Security > Integrated on-box] を有効にした後、Content Gateway を再起動した場合、**[Configure] > [Security] > [Data Security]** を順に選択することによって手動登録を行うことができます（下記を参照）。

Content Gateway の再起動によって常に登録ステータスがチェックされ、必要に応じて、自動-再登録が開始されます。

登録の成功および失敗の情報は下記のファイルにログ記録されます。/opt/WCG/logs/dss_registration.log

重要

Content Gateway が V シリーズ アプライアンス上に**ない**場合、登録のために Content Gateway ホストシステムが eth0 ネットワーク インターフェースに割り当てられた IPv4 アドレスを取得していることを**必要**とします。登録の後、IP アドレスはシステム上の他のネットワーク インターフェースに移動してもかまいません。しかし、その IP アドレスは Data Security の構成配備に使用され、2 つのモジュールが登録されている間は利用可能でなければなりません。

Data Security Management Server への手動登録：

1. Content Gateway システムと Data Security Management Server システムが実行しておりアクセス可能であること、またそれらのシステム クロックが数分以内で同期化していることを確認します。
2. **[Data Security > Integrated on-box]** が有効化されていることを確認します。Content Gateway manager で、**[Configure] > [Basic] > [General]** を順に選択します。**Networking** にある **[Features（フィーチャ）]** のリストで、**[Data Security]** を見つけ、**[On（オン）]** を選択し、次に **[Integrated on-box（コンピュータに統合済み）]** を選択し、**[Apply]** をクリックします。
3. **[Integrated on-box]** の隣の **[Not registered（未登録）]** リンクをクリックします。それによって、**[Configure] > [Security] > [Data Security]** 登録画面が開きます。
4. **[Data Security Management Server]** の IP アドレスを入力します。
5. Data Security manager にログ オンするためにユーザー名およびパスワードを入力します。ユーザーは、配備設定の権限をもつ Data Security 管理者である必要があります。
6. **[Register（登録）]** をクリックします。登録が成功した場合、結果を確認するメッセージが示され、Content Gateway を再起動するように要求されます。

   登録が失敗した場合、失敗の原因を示すエラー メッセージが表示されます。問題を訂正し、登録プロセスをもう一度実行します。

設定のオプション

登録が成功したとき、**[Configure] > [Security] > [Data Security]** ページで下記のオプションを設定します。

1. **Analyze FTP Uploads（FTP アップロードを分析）**：分析とポリシーの実施のために、FTP アップロードを Data Security に送信するには、このオプションを選択します。
2. **Analyze HTTPS Content（HTTPS コンテンツを分析）**：分析とポリシーの実施のために、復号化した HTTPS ポストを Data Security に送信するには、このオプションを選択します。HTTPS プロトコル オプションを Content Gateway で有効化する必要があります。参照

   注意
   これらのオプションを有効にするために、Content Gateway をプロキシ FTP および HTTPS トラフィックに構成する必要があります。

3. **[Apply]** をクリックして設定を保存し、次に Content Gateway を再起動します。

4. Data Security manager に移動し、Data Security Content Gateway モジュールを構成します。*Data Security Manager Help* の [Configuring the Web Content Gateway module] を参照してください。

Data Security と Content Gateway は、下記のように複数のポートを通じて通信します。IPTable が Content Gateway ホスト システムに構成されている場合、これらの ポートを IPTables で開く必要があります。下記の Technical Library の関連記事を参照してください。Content Gateway Ports、および Configuring IPTables for Websense Content Gateway。

注意

Content Gateway manager のアラームは、下記の場合に生成されます。

- コンピュータにインストールされている Data Security が有効化されているが、登録されていない
- コンピュータにインストールされている Data Security が有効化され登録されているが、Data Security manager に構成されていない

ICAP クライアントの構成

Help | Content Gateway | バージョン 7.8.x

ICAP は、Websense Data Security のすべてのバージョンと共に使用できますが、しかし、**ポリシー エンジンが Content Gateway と同じコンピュータにインストールされている場合は、ダイレクト インターフェースを使用することを推奨します。***Data Security の登録と構成*、150 ページを参照してください。

Data Security Suite バージョン 7.1 以前と相互運用する場合は、ICAP を使用する**必要があります。**

注意

プライマリ サーバーが故障した場合のフェールオーバーとして、セカンダリ ICAP サーバーを指定できます。

プライマリ サーバーとセカンダリ サーバーをロード バランシングを実行するように構成できます。

下記の *ICAP フェールオーバーとロード バランシング*を参照。

ICP との統合を構成するには、Content Gateway manager にログ オンし、**[Configure] > [My Proxy] > [Basic] > [General]** ページを順に選択します。

1. [Features] テーブルの **[Networking]** セクションで、Data Security の **[On（オン）]** を選択します。
2. **[Apply]** をクリックし、次に **[Restart（再起動）]** をクリックします。
3. **[Configure] > [Networking] > [ICAP] > [General]** を順に選択します。
4. **[ICAP Service URI（ICAP サービス URI）]** フィールドに、一次 ICAP サービスの Uniform Resource Identifier (URI) を入力し、次にカンマ（スペースなし）を入力し、二次 ICAP サービスの URI を入力します。セカンダリ ICAP サービスは任意です。

   URI は URL と似ていますが、URI は、ページではなくディレクトリで終了します。Websense Data Security Suite 管理者から識別子を取得してください。URI を下記の形式で入力します。

   `icap://hostname:port/path`

   hostname として、Websense Data Security Suite Protector アプライアンスの IP アドレスまたはホスト名を入力します。

   デフォルトの ICAP ポートは 1344 です。

   Path は、ホスト コンピュータ上の ICAP サービスのパスです。

   例：

   `icap://ICAP_machine:1344/REQMOD`

   デフォルトの ICAP ポート 1344 を使用している場合はポートを指定する必要はありません。たとえば、デフォルト ポートでなくても上記の URI を入力できます。

   `icap://ICAP_machine/REQMOD`

5. **[Analyze HTTPS Content（HTTPS コンテンツを分析）]** で、復号化したトラフィックを分析のために Websense Data Security に送信するか、または宛先の直接に送信するかを指定します。Data Security にトラフィックを送信するために HTTPS プロトコル オプションを有効化する必要があります。*暗号化データの使用、159 ページ*を参照してください。
6. **[Analyze FTP Uploads（FTP アップロードを分析）]** で、FTP アップロード要求を分析のために Websense Data Security Suite に送信するかどうかを指定します。FTP トラフィックを Websense Data Security に送信するには、FTP プロキシ機能を有効化する必要があります。*FTP、367 ページ*を参照してください。
7. **[Action for Communication Errors（通信エラーの場合の処置）]** で、Data Security Suite との通信中に Content Gateway にエラーが発生した場合に、トラフィックを許可するか、またはブロック ページを送信するかを選択します。

8. **[Action for Large Files（大きなファイルの場合の処置）]** で、Data Security Suite で指定されたサイズの上限より大きいファイルが送信される場合に、トラフィックを許可するか、またはブロック ページを送信するかを選択します。Data Security Suite バージョン 7.0 以前のデフォルトのサイズの上限は、12 MB です。
9. **[Apply]** をクリックします。

> **注意**
> URI を変更した場合、Content Gateway を再起動する必要があります。他の変更では、再起動は不要です。

ICAP フェールオーバーとロード バランシング

Help | Content Gateway | バージョン 7.8.x

アクティブな ICAP サーバーが障害を起こした場合、バックアップ ICAP サーバーにフェイルオーバーするように Content Gateway を構成できます。プロキシは、エラー条件を検出し、トラフィックをセカンダリ サーバーに送信します。セカンダリ サーバーが応答しなくなった場合、プロキシはプライマリ サーバーを使用します。どちらの ICAP サーバーも利用できない場合、プロキシはフェールオープンします。

2 つの ICAP サーバー間のロード バランシングも任意です。

フェールオーバーまでの時間

Content Gateway では、実際に故障が発生した時からプロキシが障害を起こしたサーバーを [故障] とマークする時までの間に、一時的に要求と処理の間の遅延が発生する場合があります。障害を起こしたサーバーが [故障] とマークされた後、新しい要求はすべて、セカンダリ ICAP サーバーに送信されます。フェールオーバーまでの時間は、主に接続タイムアウトの設定によって制限されています。

フェールオーバーの原因になるエラー条件

- レイヤー 3 の障害によって ICAP 要求が失敗した（同じ要求に対して 2 回）
- 指定された時間内にポートに接続できなかった
- 要求を送信できなかった（サーバーによる接続のリセットなど）

除外される失敗条件

Content Gateway は、応答がない、無効、または遅いことを失敗とはみなしません。

しかし、Content Gateway は、ICAP OPTIONS 要求への応答を検証することによって ICAP サーバーが起動時に有効であったことを確認します。

復旧の条件

障害を起こしたサーバーが [故障] とマークされた後、新しい要求はセカンダリ サーバーに送信されます。下記の復旧条件に基づいて、サーバーが再びアクティブであることが検出されるまで、障害を起こしたサーバーには新しい ICAP 要求は送信されません。

Content Gateway は、指定された間隔で、故障した各 ICAP サーバーの復旧条件についてテストします。ロード バランシングが無効化されている場合は、プライマリ ICAP サーバーがオンラインに復帰するまで、要求は引き続き セカンダリ ICAP サーバーに送信されます。ロード バランシングが有効化されている場合は、Content Gateway は、サーバー（ラウンドロビン）が [稼働中] とマークされるとすぐに、そのサーバーに要求の送信を開始します。

- TCP 接続が成功した
- OPTIONS 要求が正常に送信された
- OPTIONS 要求への有効な応答が正常に受信された

復旧の処置

サーバーの復旧時（サーバーがオンラインに復帰し、[稼働中] とマークされる）

- ロード バランシングがオンのとき : 要求は、新しく稼働中になったサーバー（ラウンドロビン）に配信され始めます。
- ロード バランシングがオフのとき：プライマリ サーバーが復旧した場合は、すべての要求はプライマリ サーバーに送信され始めます。セカンダリ サーバーが復旧した場合は、プライマリ サーバーがダウンするまで、トラフィックは引き続きプライマリ サーバーに送信されます。

フェイル オープン

すべての ICAP サーバーが停止した場合は、構成オプションによってフェール オープンまたはフェール クローズの動作が可能になります。すべての ICAP サーバーが停止した場合、バックグラウンド スレッドは、引き続き各サーバーとの新しい接続の再確立を試みます。

構成の設定

下記の ICAP フェールオーバー パラメータは、*records.config* ファイルで設定されています（デフォルト値を示しています）。

設定変数	データタイプ	デフォルト値	説明
proxy.config.icap.ICAPUri	STRING	（空白）	ICAP URI のカンマ区切り形式のリスト。例： icap://1.2.3.4:1344/reqmod, icap://4.3.2.1:1344/reqmod
proxy.config.icap.ActiveTimeout	INT	5	読み込み / 応答タイムアウト（秒単位）。タイムアウトを超過した場合、アクティビティは失敗と見なされます。
proxy.config.icap.RetryTime	INT	5	停止したサーバーが復旧したかどうかをテストするための復旧時間（秒）。
proxy.config.icap.FailOpen	INT	1	設定： • ICAP サーバーがダウン状態にあるとき、トラフィックを許可する場合は 1 に設定 • サーバーがダウン状態にあるとき、ブロック ページを送信する場合は 0 に設定
proxy.config.icap.LoadBalance	INT	1	設定： • すべての利用可能なサーバーに要求を配信する場合は 1 に設定 • プライマリ サーバーにだけ要求を配信する場合は、0 に設定。

13 暗号化データの使用

関連項目：

- *明示的プロキシ モードでの実行*、161 ページ
- *最初の SSL 設定の作業*、165 ページ
- *SSL サポートの有効化*、163 ページ
- *証明書*、166 ページ
- *内部ルート CA*、166 ページ
- *証明書の管理*、175 ページ
- *インバウンド トラフィックの場合の SSL 構成の設定*、178 ページ
- *アウトバウンド トラフィックの場合の SSL 構成の設定*、180 ページ
- *証明書の検証*、182 ページ
- *HTTPS Web サイトのアクセスの管理*、188 ページ
- *クライアント証明書*、194 ページ
- *SSL 接続エラー メッセージのカスタム化*、196 ページ

SSL (Secure Sockets Layer) および TLS (Transport Layer Security) は、インターネット上のセキュアなデータ転送のための業界標準です。これらは、データ暗号化と、認証機関により発行されクライアントおよびサーバーにより承認されている承認機関 (CA) によって発行された信頼される証明書のシステムに依拠します。ブラウザで行われた SSL/TLS 要求は、URL の先頭の文字列 [https] によって簡単に識別されます。

後のトピックでは、わかりやすく、簡潔にするために、SSL/TSL を単に SSL と表記します。

SSL 接続を確立するために、クライアントはサーバーに SSL 接続要求を送信します。サーバーが同意した場合、クライアントとサーバーは、標準ハンドシェークを使用して SSL 接続を折衝します。

Content Gateway は、HTTPS トラフィックに 2 種類のサポートを提供します。両方を同時に使用することはできません。

- 単純な接続管理 - Content Gateway は URL フィルタリングを実行し、その後、クライアントがサーバーとの接続を行うことを許可します。
- 高度な接続管理 - Content Gateway は下記のことを行います。
  - 要求をプロキシへ転送する
  - コンテンツを復号化し、リアルタイム コンテンツおよびセキュリティ分析を実行する
  - クライアントまたはオリジン サーバーに配信するためにコンテンツを再暗号化する

高度なプロキシ サポートを単にクライアント HTTPS サポートまたは SSL サポートと言います。その機能の方法および設定方法については、以下のセクションで説明しています。

Content Gateway manager では、SSL サポートは **[Configure] > [My Proxy] > [Basic] > [General]** ページの **[Protocols]** エリアで **[HTTPS]** オプションを選択することによって有効化されます。

重要

HTTPS サポートが**有効化されておらず**、HTTPS が復号化されていないときでも、Content Gateway は URL フィルタリングを実行します。つまり、クライアントから受信した各 HTTPS 要求に対して、URL ルックアップが実行され、ポリシーが適用されます。

明示的プロキシ モードでは、HTTPS のサポートが無効化されたとき、Content Gateway は 要求内のホスト名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、Content Gateway はブロック ページを提供します。一部のブラウザは、ブロック ページの表示をサポートしません。この機能を無効にするには、クライアントがプロキシに HTTPS 要求を送信しないように設定します。

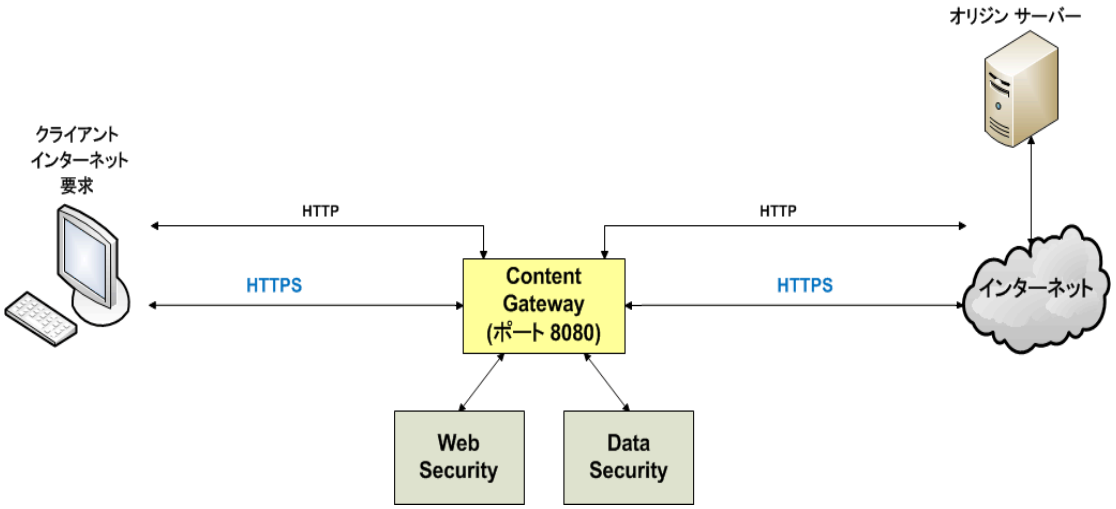
透過的プロキシ モードでは、HTTPS が無効化されたとき、要求内に SNI がある場合は、Content Gateway は、SNI からホスト名を取得し、そのホスト名に基づき URL フィルタリングを実行します。SNI がない場合は、Content Gateway は、配信先サーバーの証明書にある共通名を使用します。しかし、共通名がワイルドカード（*）を含んでいる場合は、宛先 IP アドレスの検索が実行されます。サイトがブロックされている場合、クライアントとの接続が失われます。ブロック ページは提供されません。WCCP と共に使用しているときこの機能を無効にするには、HTTPS のサービス グループを作成しないでおきます。

> **注意**
> **Content Gateway は HTTPS コンテンツをキャッシュしません。**

HTTPS が有効化された時、各 HTTPS 要求は、下記の 2 つの別個のセッションで構成されます。

- 1 つは クライアント ブラウザから Content Gateway へのセッションです。これは、**インバウンド**接続です。
- もうひとつは、SContent Gateway からセキュアなデータを受信するオリジン サーバーへのセッションです。これは、**アウトバウンド**接続です。

各セッションのために種々の証明書が必要です。



SSL、TLS、および SSL/TLS 証明書の詳細については、インターネットで検索するか、または市販の入手可能な書籍を参照してください。

明示的プロキシ モードでの実行

Help | Content Gateway | バージョン 7.8.x

既存の PAC ファイルがある場合は、Content Gateway **config** ディレクトリ（デフォルトの場所は **/opt/WCG/config**）にある **proxy.pac** を既存のファイルに置き換えます。PAC ファイルがない場合は、カスタム PAC ファイルの作成の基礎として使用できるスクリプトについて下記のステップ 4 を参照してください。

1. **[Configure] > [My Proxy] > [Basic] > [General（一般）]** タブで、HTTPS が有効化されていることを確認します。無効化されている場合は、HTTPS を **[On（オン）]** に設定し、**[Apply（適用）]** をクリックし、Content Gateway の **[Restart（再起動）]** をクリックします。
2. **[Configure] > [Content Routing（コンテンツ ルーティング）] > [Browser Auto-Config（ブラウザ自動設定）] > [PAC]** タブを順に選択します。
3. **[Auto-Configuration Port（ポートの自動設定）]** フィールドで、プロキシが PAC ファイルを提供するために使用するポートを指定します。デフォルト ポートは 8083 です。
4. [PAC Settings（PAC 設定）] 領域に **proxy.pac** ファイルが表示されます。
   - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーした場合、**proxy.pac** ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
   - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーしていない場合は、**proxy.pac** ファイルは空です。PAC の設定として下記のスクリプトをコピー & ペーストします。プロキシ ドメイン名または IP アドレスを入力する必要があります。このテンプレートは、基本的なテストのみを目的としています。組織のすべてのニーズに対応するようにこのファイルをさらに変更してください。

```
function FindProxyForURL(url, host)
{
  url = url.toLowerCase();
  host = host.toLowerCase();
  if (url.substring(0, 5)== "http:"){
    return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
  }
  else if (url.substring(0, 4)== "ftp:"){
    return "PROXY WCG_DOMAIN_NAME_or_IP_Address:2121";
  }
  else if (url.substring(0, 6)== "https:"){
    return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
  }
  else{
    return "DIRECT";
  }
}
```

5. **[Apply]** をクリックします。
6. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

新しい PAC 情報を配置した後、ユーザーにブラウザで PAC ファイルを設定するよう指示しなければなりません。たとえば、PAC ファイルが置かれているプロキシ サーバーのホスト名が **proxy1** であり、Content Gateway がデフォルト ポート 8083 を使用してファイルを提供する場合、ユーザーはプロキシ設定で下記の URL を指定する必要があります。

```
http://proxy1.company.com:8083/proxy.pac
```

PAC ファイルの場所の指定の手順はブラウザによって異なります。

Microsoft Internet Explorer バージョン 7.0 以上の場合：

1. **[Tools（ツール）] > [Internet Options（インターネット オプション）] > [Connections（接続）] > [LAN Settings（LAN の設定）]** を順に選択します。
2. **[Use automatic configuration script（自動構成スクリプトを使用）]** フィールドを選択し、**[Address]** フィールドに下記の URL を入力します。

   `http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac`
3. **[OK]** をクリックします。

Mozilla Firefox 2.0 以上の場合：

1. **[Tools] > [Options（オプション）] > [Advanced（詳細設定）] > [Network（ネットワーク）] > [Connection] > [Settings（設定）]** を順に選択します。
2. **[Automatic proxy configuration URL（自動プロキシ構成 URL）]** フィールドを選択し、下記の URL を入力します。

   `http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac`
3. **[Reload（再ロード）]** をクリックし、**[OK]** をクリックします。

詳細についてはご使用のブラウザのマニュアルを参照してください。

SSL サポートの有効化

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [My Proxy] > [Basic] > [General]** を順に選択し、HTTPS の **[On]** をクリックします。

> **注意**
>
> HTTPS トラフィックを検査する他の Websense の製品、たとえば、Data Security などと共に実行している場合は、ここで HTTPS を有効化しなければなりません。

2. **[Apply]** をクリックし、次に **[Restart]** をクリックします。
3. SSL 証明書ファイルの名前を入力します。*下位 CA の作成*、169 ページを参照してください。

[Configure] > [Protocols] > [HTTPS] ページを使用して、下記の事柄を指定します。

- HTTPS サポート（デフォルトは 8080）
- Skype トンネリング（明示的プロキシのみ）
- 要求が **Unknown protocol（未知のプロトコル）**エラーを返した時のトンネリング

1. **HTTPS Proxy Server Port** は、Content Gateway 接続の際にクライアントに使用するポートです。デフォルトは 8080 です。トラフィックが 443 で透過する場合、デフォルト ARM NAT ルールは、要求を 8080 にアドレス変更します。**[Configure] > [Networking] > [ARM: Network Address Translation（ARM：ネットワーク アドレス変換）]** を参照してください。
2. Content Gateway が**明示的プロキシ**であり、Skype トラフィックを許可する場合は、**[Tunnel Skype（Skype をトンネリング）]** オプションを有効化します。このオプションが必要です。なぜなら、Skype は SSL ハンドシェークを提示しますが、Skype のデータ フローは SSL 標準に準拠しないからです。トラフィックがトネリングされない限り、接続が失われます。

   設定を完了するには、Web Security manager で Skype のユーザーに適用するフィルタリング ポリシーが [インターネット電話] を許可することを確認します。HTTPS サポートを有効化するか否かを指定することは、Skype のユーザーにとって必須です。

   また、禁止されなかった場合、最初のハンドシェークの後、Skype は非 HTTP ポートを使ってトラフィックをルーティングします。Content Gateway を経由するように Skype トラフィックを強制するには、『Skype IT Administrators Guide』 に記載されている通り、GPO を使用します。

   重要

   HTTPS が有効化されていない場合は、このオプションを設定する必要はありません。

   このオプションは Content Gateway が透過的プロキシである場合は、有効ではなく、無効です。

3. SSL ハンドシェークが未知のプロトコル エラーになった時、HTTPS 要求をトンネリングするには、**[Tunnel Unknown Protocols（未知のプロトコルをトンネリング）]** を有効化します。

警告

トンネリングされた接続は、復号化または検査をされません。

また、7.8.1 の場合のみ、このオプションの設定は **[Configure] > [My Proxy] > [Basic] > [General]** で HTTPS 機能が無効にされている場合でも保持されます。このページは HTTPS が有効化されている場合にのみ表示されるので、HTTPS を無効化する場合はその前にこのオプションを無効化する必要があります。

Web Security の動作は、プロキシ環境のタイプに基づいて異なります。

- Content Gateway が**明示的プロキシ**である場合、ポリシーを適用する前に URL ルックアップが実行され、SSL 接続要求が行われます。トランザクションは通常通りログ記録されます。
- Content Gateway が**透過的プロキシ**であるとき、要求に SNI がある場合は、Content Gateway は、SNI からホスト名を取得し、そのホスト名に基づき URL フィルタリングを実行します。そうでない場合は、Content Gateway がサーバーに接続を送信したとき、未知のプロトコル エラーが検出されると要求がトンネリングされ、プロキシはそれを関知しません。トランザクションはログに記録されません。

最初の SSL 設定の作業

Help | Content Gateway | バージョン 7.8.x

インバウンド（クライアントから Content Gateway へ）トラフィックの場合、Content Gateway を通過する HTTP トラフィックのサポートを準備するために、下記の手順を実行します。

1. 内部ルート CA（認証機関）を作成します。SSL トラフィックにサインするために、Content Gateway は、SSL 証明書を署名する能力をもつ内部 SSL Certificate Authority を必要とします。これは、ブラウザと Content Gateway の間のトラフィックを対象としています。*内部ルート CA*、166 ページを参照してください。
2. この CA を証明書ツリーに追加します。宛先サーバーなどのサーバーは、このツリーをチェックして、ユーザーがここにリストされている機関からの証明書があるのでそれらのサーバーがユーザーを信用できることを確認します。証明書ツリーにリストされている証明書は、個別の Web サイトの妥当性を検証する権限（信用）を与える認証機関です。証明書ツリー内の認証機関によって署名されていて、[許可] ステータスをもつすべてのサイトは、Content Gateway を通過することを許可されます。*証明書の管理*、175 ページを参照してください。

3. ブラウザのユーザーが閲覧するページをカスタマイズします。*SSL 接続エラー メッセージのカスタム化、196 ページ*を参照してください。カスタマイズできるページは、接続失敗および証明書検証失敗ページです。

証明書

Help | Content Gateway | バージョン 7.8.x

HTTPS セキュリティでは、証明書が中心的な役割を果たします。証明書は、下記の 3 つの基準を満たさなければなりません。

- 現在の証明書であること（有効期限切れになっていたり、取り消されていないこと）。*証明書の検証、182 ページ*を参照してください。
- 信頼のある CA（認証機関）によって発行されていること。*証明書の管理、175 ページ*を参照してください。
- URL と証明書の所有者が一致すること。*検証設定値の設定、183 ページ*を参照してください。

クライアント ブラウザと Content Gateway の間の HTTPS 接続は、内部 CA によって発行された証明書を必要とします。*内部ルート CA、166 ページ*を参照してください。

Content Gateway とオリジン サーバーの間の接続は、**[Configure] > [SSL] > [Certificates（証明書）] > [Certificate Authorities（認証機関）]** タブの Certificate Authority Tree（認証機関ツリー）にリストされている証明書署名機関の 1 つによって署名された証明書を必要とします。*証明書の管理、175 ページ*を参照してください。

内部ルート CA

Help | Content Gateway | バージョン 7.8.x

内部ルート CA は、クライアント ブラウザと Content Gateway の間で使用されるすべての証明書を動的に生成します。

- インバウンド接続を完了するために、内部ルート CA を持つ必要があります。
- 内部ルート CA をインポートするか、または作成できます。
- 内部ルート CA は SSL 設定データベースに保存されます。

重要

既存の内部ルート CA のバックアップを作成してから、新しい内部ルート CA をインポートまたは作成してください。それによって、必要な場合に以前のバージョンに戻ることができるようになります。詳細については、*内部ルート CA のバックアップの作成、175 ページ*を参照してください。

一度に 1 つの内部ルート CA だけをアクティブにできます。

重要

Content Gateway に含まれているデフォルトの内部ルート CA は一意な内部ルート CA ではありませんから、製造環境では使用しないでください。

デフォルトの内部ルート CA を組織のルート CA に置き換えるかまたは新しいルート CA を作成します。後の項を参照してください。

内部ルート CA を作成するための下記の 3 つのオプションがあります。

- 既存の企業 CA を活用し、それを Content Gateway にインポートする。*ルート CA のインポート、167 ページ*を参照してください。
- 新しいルート CA を作成し、その CA をブラウザが利用できるようにする。*新しいルート CA の作成、168 ページ*を参照してください。
- 下位 CA を作成する。これは企業 CA を活用します。しかし企業 CA によって取り消すこともできます。*下位 CA の作成、169 ページ*を参照してください。

ルート CA のインポート

Help | Content Gateway | バージョン 7.8.x

組織がルート CA を所有している場合は、それをインポートできます。この証明書は、組織内のすべてのブラウザによって信頼を得なければなりません。インポートした新しい内部ルート CA のバックアップを必ず作成してください。詳細については、*内部ルート CA のバックアップの作成、175 ページ*を参照してください。

1. **[Configure] > [SSL] > [Internal Root CA] > [Import Root CA（ルート CA をインポート）]** を順に選択します。
2. 参照して証明書を選択します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。

3. 参照してプライベート キーを選択します。プライベート キーは、ステップ 2 で選択した証明書と一致しなければなりません。

> **重要**
>
> 証明書とプライベート キー フォーマットは一致しなければなりません。
>
> さらに、プライベート キー フォーマットは、インポート側のノードが要求するフォーマットと一致しなければなりません（暗号化または復号化）。
>
> 証明書およびプライベート キー フォーマットを確認するために、テキスト エディタでファイルを参照します。データベースから CA をエクスポートするには、**[Backup Root CA（ルート CA のバックアップを作成）]** を使用します。
>
> プライベート キー フォーマットの変換の詳細については、下記の項目を参照してください。
>
> - 内部ルート CA を FIPS 140-2 有効化ノードにインポートするための準備
> - RSA キー タイプの PKCS#8 キー タイプへの変換
> - 暗号化されたプライベート キーの RSA キーへの変換

4. パスフレーズを入力し、確認します
5. **[Import Root CA]** をクリックします。インポートされたルート CAは SSL 設定データベースに保存されます。

新しいルート CA の作成

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *下位 CA の作成*、169 ページ

またルート CA がない場合は、このタブのフィールドに記入して、ルート CA を作成します。

このプロセスは、**openssl pkcs#8** を使用します。

作成した新しいルート CA のバックアップを必ず作成してください。詳細については、*内部ルート CA のバックアップの作成、175 ページ*を参照してください。

このページのアスタリスク (*) は、必須のフィールドを示しています。

1. **[Configure] > [SSL] > [Internal Root CA]** を順に選択し、次に **[Create Root CA（ルート CA を作成）]** を選択します。
2. 要求された情報、特に下記の情報をフィールドに入力します。
   - フィールド **[Organization（組織）]**、**[Organizational Unit（組織単位）]**、および **[Common Name（共通名）]** が 1 つの**識別名**で構成されています。
     - **[Organization]** に、自社名を入力します。
     - **[Common Name]** に、自社内認証機関の名前を入力します。
   - コメントは証明書の一部になります。入力する最初の行はエンド ユーザーが閲覧できます。
   - パスフレーズを入力し、確認します（パスフレーズはパスワードに似ています。しかし通常は、より大きなセキュリティを実現するためにパスフレーズのほうが長いです）。数字、文字、および大文字と小文字の組み合せた、強いパスフレーズを使用することを推奨します。
3. **[Generate and Deploy Certificate（証明書を生成し配備）]** をクリックして、証明書を Content Gateway サーバーに配備します。

下位 CA の作成

Help | Content Gateway | バージョン 7.8.x

下位認証機関（下位 CA）を作成することによって、ルート CA の既存のすべての情報を利用することができます。しかし、ルート CA はいつでも下位 CA を取り消すことができます。

OpenSSL および Microsoft Windows の認証サービスを使用して下位 CA を作成するには、下記の手順を実行します。

準備

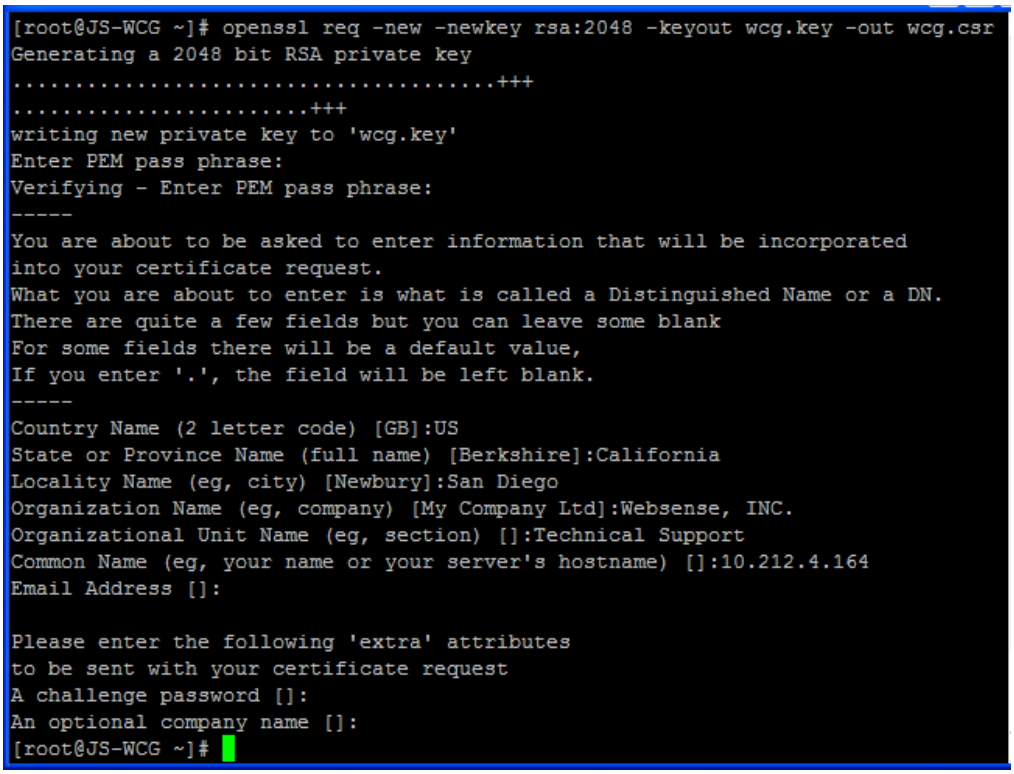
- **企業ドメイン管理者でない場合は、その管理者と協力して下位 CA を作成するための正しいドメイン許可を得る必要があります。**
- IWindows コンピュータまたは Linux コンピュータに **OpenSSL 1.0.1e** ツールキット（www.openssl.org）をインストールします。

証明書署名要求 (CSR) の作成

1. OpenSSL を使用して CSR を作成します。

   Windows Command Prompt 画面でまたは Linux コマンド ラインで、下記の **openssl** コマンドを使って CSR を作成します。

   ```
   openssl req -new -newkey rsa:2048 -keyout wcg.key -out
   wcg.csr
   ```



2. 一連の質問があります。各質問に回答し、チャレンジ パスワードをメモします。これは後のプロセスで必要になります。

   openssl コマンドは 下記の 2 つのファイルを生成します。

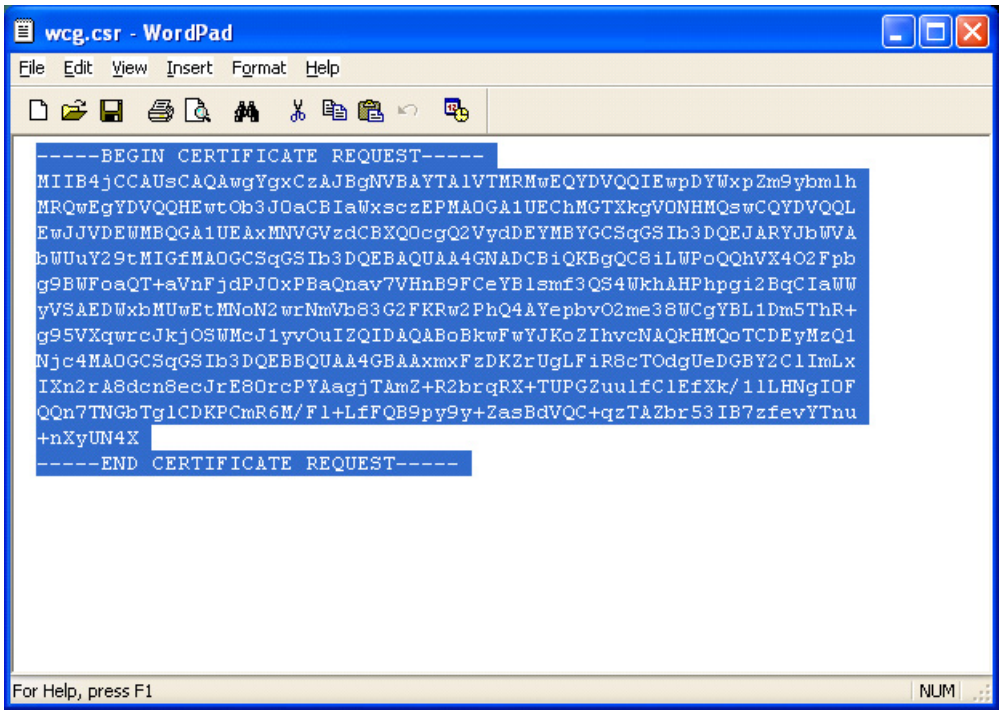
   - **wcg.csr** — 最終の証明書を作成するため認証機関によって署名される CSR
   - **wcg.key** — プライベート キー

3. Linux システムで CSR を作成した場合は、WinSCP または他のファイル転送ユーティリティを使用して作成した CSR を Windows ホストにコピーします。

要求の署名

要求を Microsoft Certificate Services を使用して署名する必要があります。

1. **WordPad** で **wcg.csr** を開き（フォーマットを保持するため）、コンテンツをクリップボードにコピーします（[Edit（編集）] > [Select all、Edit（すべて選択； 編集）] > [Copy（コピー）] ）。

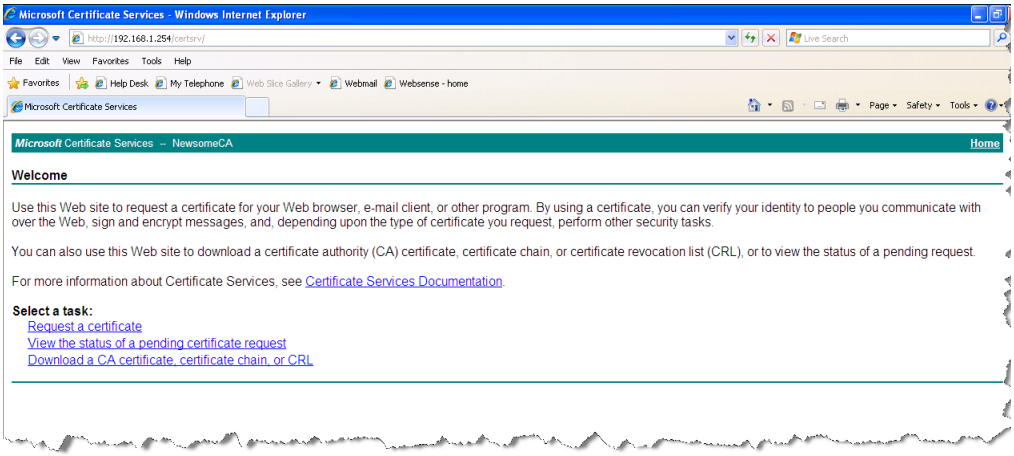


2. **Internet Explorer** で、**Microsoft CA server**（**Microsoft CA** サーバー）に移動します。

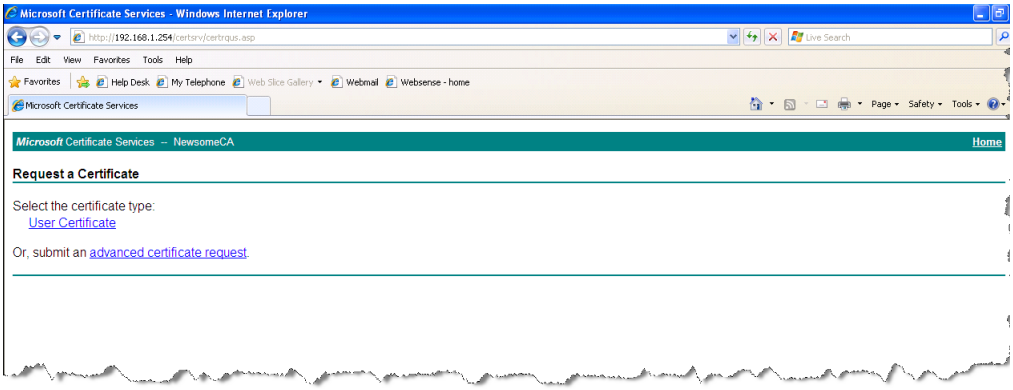
   下記の URL を入力します。

   http://<CA_server_IP_address>/certsrv

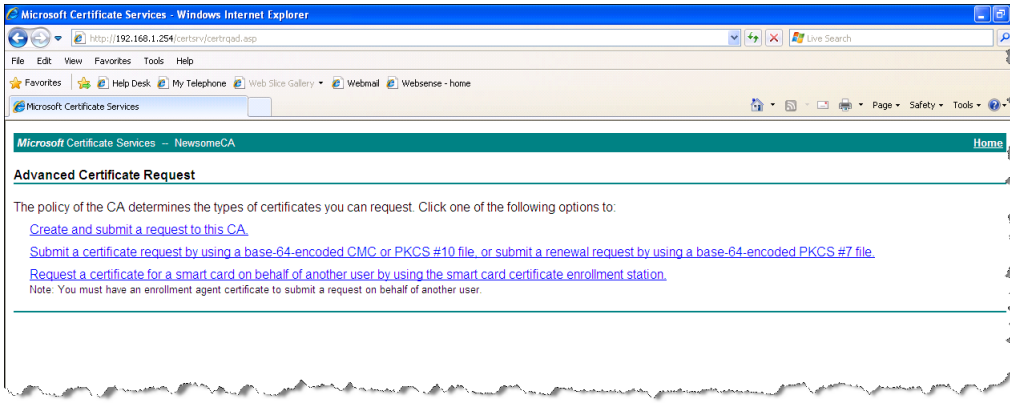
   Certificate Services（認証サービス）アプレットが起動します。



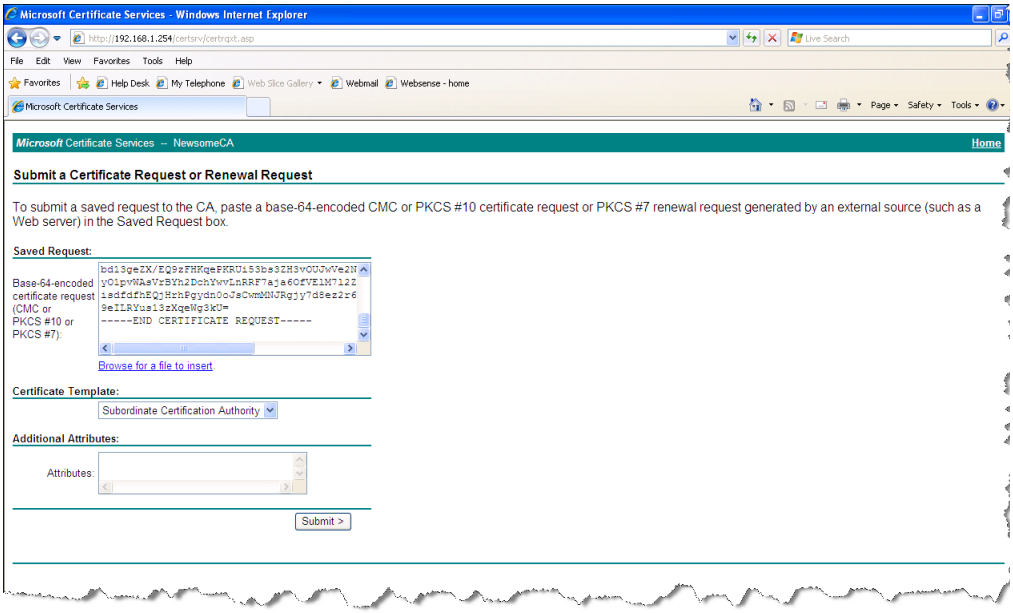
3. **[Welcome（ようこそ）]** 画面の見出し **[Select a task（タスクを選択）]** の下から **[Request a certificate（証明書を要求）]** を選択します。**[Request a certificate（証明書を要求）]** ページが表示されます。



4. **advanced certificate request（最新の証明書要求）**を送信するように選択します。

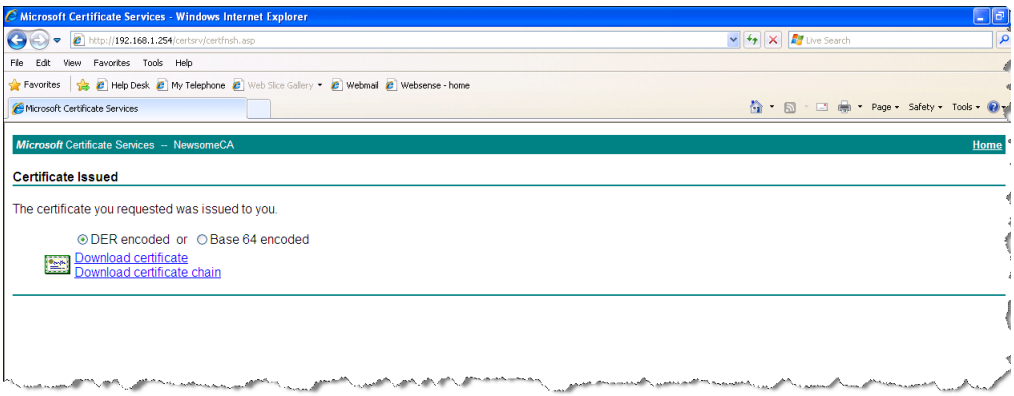


5. **[Advanced Certificate Request（拡張証明書要求）]** 画面で、**[Submit a certificate request by using a base-64-encoded CMC（base64 エンコード CMAC を使用して証明書要求を送信）]** を選択します。**[Submit a Certificate Request or Renewal Request（証明書要求または更新要求を送信）]** 画面が表示されます。



6. **[Submit a Certificate Request or Renewal Request]** 画面で、**[Certificate Template（証明書テンプレート）]** ドロップ ダウン ウィンドウ に **wcg.csr** ファイル（前にクリップボードに置かれていた）のコンテンツを張付け、**[Submit（送信）]** をクリックします。

   証明書が発行され、**[Certificate Issued（証明書発行済み）]** 画面が表示されます。代わりに、**[Certificate Pending（証明書保留中）]** 画面が表示されて場合は、下位 CA を作成するための十分な権限がないことを表します。企業ドメイン管理者に問い合わせて証明書作成プロセスを完了してから、次にステップ 7 に進んでください。

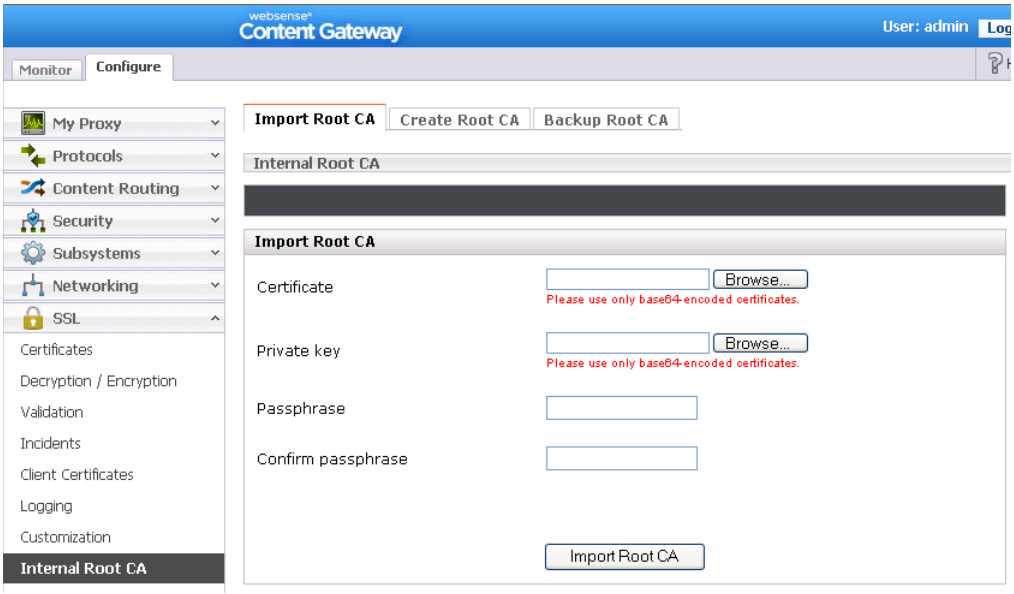


7. **[Base 64 encoded（Base 64 エンコード方式）]** ラジオ ボタンを選択し、次に **[Download certificate（証明書をダウンロード）]** を選択します。証明書をデスクトップに保存します。後で、その証明書を Content Gateway にインポートします。

デスクトップ上の base 64 エンコード方式の証明書は、CSR 生成プロセス中に作成されたプライベート キーと共に Content Gateway にインポートできる状態になっています。

下位 CA を Content Gateway にインポート

1. Content Gateway manager を開き、**[Configure] > [SSL] > [Internal Root CA] > [Import Root CA（ルート CA をインポート）]** を順に選択します。



2. **参照**して証明書を選択します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。
3. **参照**してプライベート キーを選択します。プライベート キーは、ステップ 2 で選択した証明書と一致しなければなりません。
4. パスフレーズを入力し、確認します
5. **[Import Root CA]** をクリックします。
6. Content Gateway を再起動してください。

内部ルート CA のバックアップの作成

Help | Content Gateway | バージョン 7.8.x

常に、内部ルート CA のパブリック キーとプライベート キーのバックアップを作成してから、新しい内部ルート CA をインポートまたは作成してください。それによって、必要な場合に証明書の以前のバージョンに戻ることができるようになります。さらにインポートしたまたは作成した新しいルート CA のバックアップを作成します。

1. **[Configure] > [SSL] > [Internal Root CA] > [Backup Root CA（ルート CA のバックアップを作成）]** を順に選択します。
2. **[Save Public CA Key（パブリック CA キーを保存）]** をクリックして、パブリック CA キーを確認するか、または保存します。このパブリック キーは、ユーザーの Web ブラウザによって信頼を得なければなりません。このキーがない場合は、ネットワーク管理者に問い合わせてください。
3. **[Save Private CA Key（プライベート CA キーを保存）]** をクリックして、プライベート CA キーを確認するか、または保存します。このキーがない場合は、ネットワーク管理者に問い合わせてください。

証明書の管理

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *新しい認証機関の追加*、177 ページ
- *証明書のバックアップの作成*、177 ページ
- *証明書の復元*、178 ページ

Content Gateway は、最初に Certificate Authority Tree（認証機関ツリー）（信頼される証明書ストア）と Mozilla for Firefox によって認定されたリストを表示します（この mozilla.org page を参照）。CA ツリーは、**[Configure] > [SSL] > [Certificates] > [Certificate Authorities]** タブを順に選択するとリストされます。Content Gateway は、これらの証明書を提供するオリジン サーバーを信頼します。

リストでは、CRL（証明書取り消しリスト）または OCSP（オンライン証明書ステータス プロトコル）を通じて検証できる証明書の名前の前に、小文字の [i] が示されることがあります。証明書の取り消しステータスのチェックの方法については、*最新の取り消し情報を保持する*、186 ページを参照してください。Content Gateway は、インバウンド トラフィックとアウトバンド トラフィックの両方に使用される証明書の取り消しステータスをチェックします。

下記の動作を実行するために、証明書の名前をクリックします。

- *証明書を確認、176 ページ*
- *証明書を削除、176 ページ*
- *証明書の許可 / 拒否ステータスの変更、176 ページ*

証明書を確認

1. **[Configure] > [SSL] > [Certificates]** > **[Certificate Authorities]** を順に選択します。
2. 確認するステータスの機関の名前を選択します。
3. ポップアップ ウィンドウで、**[Click to view certificate（クリックして証明書を確認）]** を選択します。
4. Opening（オープニング）ウィンドウの指示に従い、ファイルを開くか、保存します。

証明書を削除

1. **[Configure] > [SSL] > [Certificates]** > **[Certificate Authorities]** を順に選択します。
2. 削除する認証機関の名前を入力します。
3. ポップアップ ウィンドウで、**[Click to delete certificate（クリックして証明書を削除）]** を選択します。
4. 証明書を削除することを確認するか、または否定します。
5. 証明書を削除することを確認する場合は、**[Configure] > [SSL] > [Certificates] > [Certificate Authorities]** を順に選択し、証明書がリストされていないことを確認します。

証明書の許可 / 拒否ステータスの変更

1. **[Configure] > [SSL] > [Certificates] > [Certificate Authorities]** を順に選択します。
2. 変更するステータスの機関の名前を選択します。
3. ポップアップ ウィンドウで、**[Click to change status to（クリックしてステータスを変更）]** を選択します。証明書のステータスに応じて、**[allow（許可）]** または **[deny（拒否）]** を選択します。ステータスを拒否に変更した場合は、認証機関ツリーの認証機関の名前の隣に赤い X が表示されます。ステータスを許可に変更した場合は、認証機関の名前の隣に緑の円が表示されます。

新しい認証機関の追加

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *証明書のバックアップの作成、177 ページ*
- *証明書の復元、178 ページ*

手動で追加の認証機関をインポートするには、**[Configure] > [SSL] > [Certificates] > [Add Root CA（ルート CA を追加）]** のページを順に選択します。手動でインポートする証明書は、デフォルトのステータス **allow** にされています。

重要

現在の証明書のバックアップを作成してから、証明書の追加や削除などの変更を行うことを推奨します。*証明書のバックアップの作成、177 ページ*を参照してください。Content Gateway の構成全体のバックアップを作成する場合は、*構成の保存と復元、130 ページ*を参照してください。

1. **[Browse（参照）]** をクリックし、ディレクトリ構造を検索して、証明書を見つけます。[.cer] 拡張子のあるファイルを探します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。
2. **[Add Certificate Authority（認証機関を追加）]** をクリックします。
3. インポートが正常に完了した場合は、**[Configure] > [SSL] > [Certificates] > [Certificate Authorities]** を順に選択し、そこに新しい証明書がリストされていることを確認します。

新しい CA は、ユーザーがその認証機関によって署名されたサイトを閲覧したときにも追加されます。これらの証明書を**許可**または**拒否**できます。詳細は *証明書の許可 / 拒否ステータスの変更、176 ページ*を参照してください。

証明書のバックアップの作成

Help | Content Gateway | バージョン 7.8.x

用心のために、証明書の追加や削除などの変更を行う場合は常に、CA 証明書を含んでいるデータベースのバックアップを作成することを推奨します。そうすることによって、それらのデータベースを後日復元できます。

証明書のバックアップを作成するには、**[Configure] > [SSL] > [Certificates] > [Backup Certificates]** ページを順に選択します。

- **[Back Up Configuration to Database（構成のバックアップをデータベースに作成）]** をクリックします。

Content Gateway の構成全体のバックアップを作成するには、*構成の保存と復元*、130 ページを参照してください。

証明書の復元

Help | Content Gateway | バージョン 7.8.x

証明書を復元するには、**[Configure] > [SSL] > [Certificates] > [Restore Certificates（証明書を復元）]** を順に選択します。証明書データベースはクラスタ全体に適用されます。

1. **[Browse]** をクリックして、バックアップ証明書データベースの場所に移動します。
2. **[Restore（復元）]** をクリックします。復元が正常に完了したことを伝え、以前の証明書データベースのバックアップが作成された場所を示すメッセージを受け取ります。

複数のプロキシを実行している場合、この復元機能を使用して、すべてのプロキシが同じ構成にされていることを確認します。

復号化と暗号化

Help | Content Gateway | バージョン 7.8.x

インバウンド トラフィックの場合の SSL 構成の設定、178 ページ

アウトバウンド トラフィックの場合の SSL 構成の設定、180 ページ

インバウンド トラフィックの場合の SSL 構成の設定

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *アウトバウンド トラフィックの場合の SSL 構成の設定*、180 ページ

インバウンド トラフィックとして SSL および TLS の設定値および暗号を設定するには、**[Configure] > [SSL] > [Decryption / Encryption]** > **[Inbound（インバウンド）]** を順に選択します。

1. **[Protocol Settings（プロトコルの設定）]** で、Content Gateway がサポートするプロトコルを指定します。サポートされているプロトコルは下記のとおりです。
   - SSLv2
   - SSLv3（デフォルトでは有効化）
   - TLSv1（デフォルトでは有効化）

   注意

   TLSv1.1 および TLSv1.2 もサポートされています。

   両方のプロトコルは、デフォルトではインバウンド接続の場合は有効化されますが（宛先サーバーへの）アウトバウンド 接続の場合は有効化されません。

   各プロトコルは、下記の変数 **records.config** によって有効化 / 無効化されます。

   proxy.config.ssl.client.TLSv11 INT 1 —（0 = 無効化）

   proxy.config.ssl.client.TLSv12 INT 1 —（0 = 無効化）

   Content Gateway が Websense アプライアンス上にあるとき、値を設定するには、Appliance manager Toolbox Command Line Utility を使用します。

   Content Gateway がソフトウェアとしてインストールされているとき、値を設定するには、Linux コマンド ラインで [content_line -s] を使用します。

   組織のセキュリティ ポリシーが適用されており、ブラウザがサポートするプロトコルを選択します。

   少なくとも 1 つのプロトコルを選択しなければなりません。

   これらの設定は、ユーザーのブラウザでのプロトコルの設定を上書きします。

   アウトバウンド トラフィックとは異なるプロトコルを選択できます。
2. 暗号リストは、利用可能なアルゴリズムと、クライアントと Content Gateway の間の暗号化のレベルを示します。

デフォルトの設定は、eNULL、ADH、および EXP スーツを**除く**利用可能なすべての暗号を使用するように指示します。

最強の暗号（高レベルの暗号化を提供）が最初に適用されます。アウトバウンド トラフィックとは異なるレベルの暗号化に設定できます。

追加の暗号の設定値は下記の通りです。

- **High（高）**暗号化暗号セット：128 ビットより長いキーを持つ暗号セット、および 128 ビットのキーをもつ一部の暗号セット。
- **Medium（中）**暗号化暗号セット：128 ビット暗号化を使用する暗号セット
- **Low（低）**暗号化暗号セット：64 ビットまたは 56 ビットの暗号化アルゴリズムを使用するが、エクスポート暗号セットを除く暗号セット。

インバウンド要求（Content Gateway へのクライアントの接続）の場合、パフォーマンスを向上させるために Low 暗号化を使用することを検討してください。

暗号の詳細については、www.openssl.org/docs を参照してください。

3. **[Apply]** をクリックします。
4. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

アウトバウンド トラフィックの場合の SSL 構成の設定

Help | Content Gateway | バージョン 7.8.x

アウトバウンド トラフィック（Content Gateway からオリジン サーバーへ）として SSL および TLS の設定値、セッション キャッシュ、暗号を設定するには、**[Configure] > [SSL] > [Decryption / Encryption]** > **[Outbound（アウトバウンド）]** を順に選択します。

1. **[Protocol Settings（プロトコルの設定）]** で、Content Gateway がサポートするプロトコルを指定します。サポートされているプロトコルは下記のとおりです。
   - SSLv2
   - SSLv3（デフォルトでは有効化）
   - TLSv1（デフォルトでは有効化）

注意

TLSv1.1 および TLSv1.2 もサポートされています。

両方のプロトコルはアウトバウンド接続の場合はデフォルトでは無効化されています。

それらのプロトコルは、下記の変数 records.config によって有効化 / 無効化されます。

proxy.config.ssl.client.TLSv11 INT 0 —（0 = 無効化）

proxy.config.ssl.client.TLSv12 INT 0 —（0 = 無効化）

Content Gateway が Websense アプライアンス上にあるとき、値を設定するには、Appliance manager Toolbox Command Line Utility を使用します。

Content Gateway がソフトウェアとしてインストールされているとき、値を設定するには、Linux コマンド ラインで [content_line -s] を使用します。

組織のセキュリティ ポリシーが適用されているプロトコルを選択します。

少なくとも 1 つのプロトコルを選択しなければなりません。

インバウンド トラフィックの場合、種々のプロトコルを選択できます。

2. **[Session Cache Timeout（セッション キャッシュ タイムアウト）]** で指定した時間が終了するまで、キーをキャッシュする場合は、**[Session Cache（セッション キャッシュ）]** を選択します。これによって、パフォーマンスを改善できます。キーがキャッシュされなかった場合、各要求はもう一度折衝されます。

   [Session Cache Timout] を 0 に設定すると、セッション キャッシュ機能が無効化されます。

3. キーがキャッシュに保持される時間（単位、秒）を指定します。デフォルトは 300 秒（5 分）です。
4. 暗号リストは、利用可能なアルゴリズムと、Content Gateway とオリジン サーバーの間の暗号化のレベルを示します。

   デフォルトの設定は、eNULL、ADH、および EXP スーツを**除く**利用可能なすべての暗号を使用するように指示します。

   最強の暗号（高レベルの暗号化を提供）が最初に適用されます。インバウンド トラフィックとは異なるレベルの暗号化に設定できます。

追加の暗号の設定は下記の通りです。

- **High（高）**暗号化暗号セット：128 ビットより長いキーを持つ暗号セット、および 128 ビットのキーをもつ一部の暗号セット。
- **Medium（中）**暗号化暗号セット：128 ビット暗号化を使用する暗号セット
- **Low（低）**暗号化暗号セット：64 ビットまたは 56 ビットの暗号化アルゴリズムを使用するが、エクスポート暗号セットを除く暗号セット。

アウトバウンド要求の場合、セキュリティを向上させるために、より高度な暗号化レベルを使用することを検討してください。

暗号の詳細については、www.openssl.org/docs を参照してください。

5. **[Apply]** をクリックします。
6. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

証明書の検証

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *検証のバイパス、186 ページ*
- *最新の取り消し情報を保持する、186 ページ*

SSL 証明書の検証は、SSL セキュリティの重要な構成要素の 1 つです。クライアント（この場合は、Content Gateway） とオリジン サーバーは、証明書の交換と検証を通じて、相互の身元を確認します。

Content Gateway は、証明書検証エンジン（CVE）によってこのタスクを実行します。

CVE を有効化し、設定するには、**[Configure] > [My Proxy] > [SSL] > [Validation（検証）]** のタブを順に選択します。

検証が失敗したが、そのサイトを信用する場合のオプションの詳細については、*検証のバイパス、186 ページ*を参照してください。

CVE の使用法および最善の方法の包括的な説明については、『SSL Certificate Verification Engine v7.8』を参照してください。

検証設定値の設定

1. **[Configure] > [SSL] > [Validation] > [General]** の順に選択します。
2. **Enable the certificate verification engine（証明書検証エンジンを有効化）：** このオプションは、証明書検証エンジンを有効化および無効化します。

   デフォルトでは、証明書検証は**無効化**されています。それによって、HTTP が（**[Configuration] > [My Proxy] > [Basics > [General]** ページで）最初に有効化されたとき、証明書検証の結果によって、Content Gateway 管理者およびネットワーク ユーザーが不意をつかれないようにします。

   このオプションを選択しなかった場合は、証明書検証はおこなわれません。

   > **重要**
   > CVE を無効化した場合、下記のページにのみ設定値を指定する必要があります。
   >
   > - [Configure] > [SSL] > [Decryption / Encryption] > [Inbound]
   > - [Configure] > [SSL] > [Decryption / Encryption] > [Outbound]
   > - [Configure] > [SSL] > [Customization（カスタム化）] > [Connection Error（接続エラー）]

3. **Deny certificates where the common name does not match the URL（共通名が URL と一致しない場合に証明書を拒否する）**：このオプションを有効化した場合、下記の 2 つのチェックが行われます。
   - 最初に、証明書の共通名について宛先 URL と正確に一致しているかチェックします。
   - 最初のチェックが失敗した場合、証明書の Subject Alternative Name (SAN) リストをチェックして、宛先 URL と正確に一致する名前がないか調べます。

   チェックは、大文字と小文字を**区別します**。

   正確な一致が要求されるため、共通名に些細な違いがあったり、SAN で一致するバリエーションがないときに、ブロックされる場合があります。

   たとえば、[https://cia.gov] を使用して [https://www.cia.gov] にアクセスしようとすると、ブロックされてしまうことがあります。さらに、IP アドレスを使ってサイトにアクセス使用としたときもブロックされることがあります。
4. **Allow wildcard certificates（ワイルドカードの証明書を許可）**：これは、**When Deny Certificates where the common name does not match the URL（共通名が URL と一致しない場合に証明書を拒否する）**のサブオプションです。このオプションを有効化したとき、それによって、名前に [*]（ワイルドカード）文字を含む共通名との一致を許可します。

一部の HTTPS サーバーは、共通名にワイルドカードを使用しますから、それによって単一の証明書がドメイン全体を対象とすることができます。例：[*.example.com] は、[email.example.com] および [stream.example.com] などを対象とします。

ワイルドカードの使用は、ドメイン内部の個々のサーバーが検証されないことを意味します。それらはワイルドカードの結果として含まれます。

ワイルドカードの証明書を許可することは、共通名の一致が必要とされるとき厳格なマッチングの負担を軽減します。また、google.com や yahoo.com などの複数のサブドメインをもつドメインの場合に役立ちます。またドメインの詐欺的なまたは望ましくないバリエーションがブロックされずまかり通るというある種のリスクをもたらします。

5. **No expired or not yet valid certificates（期限切れまたはまだ有効でない証明書なし）**：このオプションを有効化したとき、期限切れの証明書またはまだ有効でない証明書を提供するサイトへのアクセスを拒否します。これは重要な基本のチェックです。なぜなら多くの不正なサイトが期限切れ証明書を使って運営しているからです。このオプションを選択しなかった場合、これらのサイトへのアクセスが許可されます。

   注意
   自己署名証明（公的認証機関の発行でない証明書）は、無効と見なされ、このカテゴリに属します。

6. **Verify entire certificate chain（証明書チェーン全体を検証）**：このオプションを有効化したとき、サイト証明書と証明書の証明書パスでルートとして指定されたルート認証機関との間のすべての証明書の期限切れステータスと取り消しステータスを検証します。これは、重量なチェックです。

7. **Check certificate revocation by CRL（CRL による証明書取り消しをチェック）**：証明書取り消しリスト（CRL）は、証明書の取り消しステータスをチェックするために使用されます。CRL は、CA によって発行され、その後取り消された証明書をリストします。

   取り消しステータスの検証は、非常に重要な基本チェックです。なせなら、証明書は、CA によって、それらが不適切に発効された、信用できなかった、偽の ID を持っている、またはポリシー違反と指定されたとき、取り消されるからです。

   このオプションを有効化する場合は、CRL の日別更新機能が有効化されていることを確認することを推奨します。**[Revocation Settings]** タブを選択し、**[CRL Settings（CRL の設定値）]** のチェック ボックスを有効化します。

   このオプションを**使用しない**場合は、CRL の日別更新機能を無効化することを推奨します。**[Revocation Settings]** タブを選択し、**[CRL Settings]** のチェック ボックスを無効化します。

8. **Check certificate revocation by OCSP（OCSP による証明書取り消しをチェック）**：Online Certificate Status Protocol（OCSP）は、証明書の取り消しステータスをチェックするもう一つの方法です。OCSP は役立ちますが、CRL ほど広範に使用されておらず、したがってそれほど信頼できません。また、これはリアルタイムのインターネットがホストするチェックであり、要求処理の遅延をもたらすことがあります。

   注意

   CRL の代わりではなく、CRL に加えて OCSP を使用することを推奨します。CRL と OCSP の詳細については、*最新の取り消し情報を保持する*、186 ページを参照してください。

9. **Block certificates with Unknown OCSP state（未知の OCSP 状態がある証明書をブロック）**：OCSP 取り消しチェックを有効にしたとき、[Unknown（未知）] ステータスを返す証明書をブロックするためにこのオプションを有効化します。
10. **Preferred method for revocation check（取り消しチェックの優先する方法）**：CRL と OCSP の両方の取り消しチェックを有効にしたとき、最初にどの方法を適用するか指示するためにこのオプションを使用します。デフォルト設定は CRL です。
11. **Block certificates with no CRL URI and with no OCSP URI（CRL URI がない証明書、および OCSP URI がない証明書をブロック）**：CRL チェック、OCSP チェック、または両方のチェックを有効にしたとき、想定した関連する URI がない証明書をブロックするには、このオプションを使用します。たとえば、CRL チェックだけを有効化し、証明書に CRL URI がない場合、このオプションが有効化した場合は、接続がブロックされます。CRL と OCSP の両方のチェックを有効化した場合、CRL と OCSP の両方に URI がない場合だけ、接続がブロックされます。

    ブラウザで証明書を確認することを選択した場合、証明書内の URI 情報を確認できます。詳細については、*証明書を確認*、176 ページを参照してください。

    多くの証明書は、CRL 情報や OCSP 情報を含んでいませんから、このオプションを使用すると検証失敗の数が多くなる可能性があります。多くの場合、失敗は、[Unknown revocation state（未知の取り消し状態）] エラーとして報告されます。

    これは、多くのアクセス拒否がある高い制限付きポリシーになる可能性があります。

    すべての検証の失敗と同様に、インシデント リスト使用して例外を許可できます。*HTTPS Web サイトのアクセスの管理*、188 ページを参照してください。

検証のバイパス

Help | Content Gateway | バージョン 7.8.x

証明書の検証が失敗したときにユーザーがサイトを閲覧するのを許可するには **[Configure] > [SSL] > [Validation] > [Verification Bypass（検証のバイパス）]** ページを使用します。

1. ユーザにサイトが無効の証明書があることを知らされた後、ユーザーがサイトに進むことができるようにするには、**[Permit users to visit sites with certificate failure after confirmation（証明書の認証が失敗した場合に、ユーザーに対して、確認後にサイトの閲覧を許可する）]** を選択します。これは、**検証のバイパス**と言います。このチェック ボックスを選択していなかった場合は、ユーザーにはサイトを参照するオプションがありません。
2. 検証のバイパスを有効化している場合は、ユーザーが特定のサイトをバイパスできる時間を秒単位で指定できます。この時間を超えると、再度警告に対して一連のクリックを行うことが必要になります。**[Time before the user is notified again for the site（サイトについて次に通知されるまでの時間）]** 入力フィールドを指定します。デフォルトは 6 分です。
3. バイパスした証明書に関する情報をキャッシュに保存し、切速を再利用するには、**[Enable the SSL session cache for bypassed certificates（バイパスした証明書の SSL セッション キャッシュを有効化）]** を選択します。
   - このオプションを選択した場合は、パフォーマンスは向上しますが、一部のユーザーには検証に失敗したサイトにアクセスしようとしていることが通知されません。
   - このオプションを選択しなかった場合は、すべてのユーザーは、有効な証明書がないサイトについて通知されますが、パフォーマンスはそれほど向上しません。

最初にバイパス検証を有効化しておくことを推奨します。次にインシデント レートの変更の場合と同様に、[Incident List] を使用してポリシーを適用できます。*HTTPS Web サイトのアクセスの管理*、188 ページを参照してください。

最新の取り消し情報を保持する

Help | Content Gateway | バージョン 7.8.x

サイトが証明書を受け入れる前に、証明書が取り消されていないことを確認するために証明書のステータスをチェックすることを推奨します。このチェックを行うための下記の 2 つの方法があります。CRL を通じて（*証明書取り消しのリスト [しょうめいしょとりけしのりすと]*、187 ページを参照）と OCSP を通じて（*Online certification status protocol（オンライン証明書ステータス プロトコル）(OCSP)*、187 ページを参照）。

証明書取り消しのリスト [しょうめいしょとりけしのりすと]

Content Gateway が最新の取り消し情報を保持する方法を設定するには、**[Configure] > [SSL] > [Validation] > [Revocation Settings]** ページを順に選択します。デフォルトでは、Content Gateway は毎日 CRL をダウンロードします。

1. CRL を毎日ダウンロードするには、**[Download the CRL at（指定時に CRL をダウンロード）]** を選択し、CRL ダウンロードを行う時刻を選択します。
2. **[Apply]** をクリックします。

すぐに CRL を更新する必要がある場合もこのページを使用します。

1. 指定した時刻以外の時刻に CRL をダウンロードするには、**[Update CRL Now（CRL をすぐにダウンロード）]** をクリックします。

> **注意**
> CRL ファイルは、たくさんの証明書を含むことがあり、そのため CRL のダウンロードには時間がかかり、CPU リソースを消費することがあります。システム上のインターネット トラフィックの量が少ない時に、CRL をダウンロードすることを推奨します。

2. 更新のステータスを確認するには、**[View CRL Update Progress（CRL 更新の進捗状況を表示）]** をクリックします。

証明書取り消しリストの詳細については、RFC 3280 を参照してください。

Online certification status protocol（オンライン証明書ステータス プロトコル）(OCSP)

OCSP は、要求 / 応答に基づき機能するプロトコルです。つまり、サイトが証明書の取り消しステータスを確認するために待機しているとき、サイトは CA に証明書のステータスに関する要求を送信します。それによって CA が応答し、証明書の有効性（または取り消し）を確認します。

CRL をダウンロードするのではなく、OCSP を使用すると、要求を処理するので、パフォーマンスの向上が実現できます。しかし、一部の CA は応答を提供せず、そのため CRL を使用する方がより多くの証明書のステータスに関する情報を得ることができます。

Content Gateway は、証明書の取り消しステータスに関する OCSP 情報をキャッシュできるようにします。応答のキャッシュ処理は、SSL トラヒック量が多く、帯域幅の節約が重要な環境では便利なことがあります。

Content Gateway が最新の取り消し情報を保持する方法を設定するには、**[Configure] > [SSL] > [Validation] > [Revocation Settings]** ページを順に選択します。

1. OCSP データがキャッシュされる期間（日数）を指定します。OCSP データをキャッシュしない場合は、**[0]** と入力します。最大の日数は 1000 日です。
2. **[Apply]** をクリックします。

OCSP の詳細については、RFC 2560 を参照してください。

HTTPS Web サイトのアクセスの管理

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *インシデントの表示*、189 ページ
- *インシデントのステータスの変更*、191 ページ
- *インシデントの削除*、191 ページ
- *メッセージのテキストの変更*、191 ページ
- *インシデントの詳細の表示*、192 ページ
- *Incident List への Web サイトの追加*、192 ページ

一連のタブは、Web サイトへのアクセスを管理するのに役立ち、またアクセス問題のトラブルシューティングの際に HelpDesk を支援します。

Web サイトがセキュリティ ポリシーに準拠しなかったのでクライアントがアクセス拒否メッセージを受け取った場合、Content Gateway は、*インシデント*を生成します。*インシデントの表示*、189 ページを参照してください。

Content Gateway が特定のサイトを処理する方法を指定する場合、そのことを Incident List にも追加できます。*Incident List への Web サイトの追加*、192 ページを参照してください。

トラブルシューティングの追加情報については、SSL Certificate Verification Engine v7.8 を参照してください。

インシデントの表示

Help | Content Gateway | バージョン 7.8.x

クライアントがアクセス拒否メッセージを受け取った事象のレポートを表示するには、**[Configure] > [SSL] > [Incidents（インシデント）] > [Incident List（インシデント リスト）]** ページを順に選択します。

クラスタ内の各ノードに別々の Incident List が維持されます。管理者によって追加または変更されたインシデントは、クラスタ全体にコピー（同期化）されます。デフォルトでアクセス拒否メッセージを生成する予期しないインシデントは、クラスタ内で同期化されません。

このレポートのフィールドを使用して、今後 Content Gateway がサイトへ要求されたアクセスを処理する方法を指定することができます。

- ローカル リストの特定のインシデントを表示するには、ID 番号または URL を入力し、**[Search Node（ノードを検索）]** をクリックします。

  ノードがクラスタの一部であり、ID または URL のすべてのインスタンスを参照する場合は、すべてのリストで **[Search Cluster（クラスタを検索）]** をクリックします。
- 検索を表示した後、完全なローカル リストを復元するには、**[Show All in Node（ノード内のすべてを表示）]** をクリックします。

  リストが非常に大きい場合は、**[Show All]** は、最初の 2,500 ～ 3,000 個のレコードを表示します。リストをスクロールするには、スクロール バーを使用します。次のページまたは前のページを表示するには、[>] および [<] ボタンを使用します。

インシデント レポート

列見出しの隣の小さな三角形をクリックしてどの列でもソートできます。

インシデント レポートは、下記のフィールドを含んでいます。

フィールド	説明
Node（ノード）	リスト エントリがある Content Gateway ノードの名前。
ID	システムにより割り当てられます。これはインシデント ID 番号であり、Ticket ID（チケット ID） とも言います。HelpDesk はエラー メッセージでユーザーに Ticket ID を尋ね、それを URL インシデント リストからすばやく取得します。 エンド ユーザーには、Ticket ID と拒否メッセージが表示されます。

フィールド	説明
Status （ステータス）	Content Gateway が今後この Web サイトを処理する方法を指定します。下記の 4 つの条件が可能です。 • Allow（許可） ユーザは証明書が有効でない場合でもそのサイトにアクセスできます。トラフィックが復号化され、証明書チェック機能が無効にさます。 • Blacklisted（ブラックリストに載せる） そのサイトは完全にブロックされます。Verification Bypass（検証のバイパス）が設定されてい場合でも、ユーザーはこのサイトにアクセスできません。 • Block（ブロック） 証明書検証が失敗した場合、Verification Bypass が設定されていない限り その Web サイトへのアクセスはブロックされます。Verification Bypass が設定されている場合は、ブロックページに [Visit site anyway（それでもサイトを閲覧する）] ボタンが表示されます。*検証のバイパス、186 ページ*を参照してください。 • Tunnel このサイトはトネリングされます。トラフィックは復号化されず、Content Gateway は証明書をチェックしません。トネリングは、信用のあるサイトの検査のバイパスとパフォーマンスの向上のために使用します。 **ご注意 :** Tunnel by URL（URL に基づくトンネル）は、すべての透過的プロキシ トラフィックでは使用できるわけではありません。*Incident List への Web サイトの追加、192 ページ*を参照してください。 [Action（アクション）] 列のドロップダウン ボックスからサイトのステータスを変更できます。
Type （タイプ）	サイトがその URL またはその証明書のどちらに基づいて追加されたかを指定します。サイトを証明書に基づく Incident List に追加することを推奨します。*Incident List への Web サイトの追加、192 ページ*を参照してください。
URL	証明書が有効でなかったサイトの URL。
Message （メッセージ）	エラー メッセージの編集を有効化します。エラー メッセージのカスタム化の詳細については、*メッセージのテキストの変更、191 ページ*を参照してください。ペンシルと虫メガネは、それぞれリンクを表します。これらのリンクの詳細については、*インシデントの詳細の表示、192 ページ*を参照してください。
Action （アクション）	インシデントのステータスの変更を有効化します。またインシデントを削除できるようにします。*インシデントの削除、191 ページ*を参照してください。

インシデントのステータスの変更

Help | Content Gateway | バージョン 7.8.x

インシデントのステータスを変更するとき、Content Gateway が今後リストされている URL を処理する方法を変更します。

1. **[Configure] > [SSL] > [Incidents]** > **[Incident List]** を順に選択します。
2. [Action] 列のドロップダウン リストから下記のいずれかのオプションを選択します。これらのオプションの詳細については、*インシデント レポート、189 ページ*を参照してください。
   - Tunnel（トンネル）
   - Block（ブロック）
   - Blacklist（ブロックリスト）
   - Allow（許可）
3. **[OK]** をクリックします。[Status（ステータス）] 列のアイコンは新しいステータスを反映するように変わります。

インシデントの削除

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [SSL] > [Incidents]** > **[Incident List]** を順に選択します。
2. 削除するインシデントを選択します。インシデントが表示されない場合、ID を使って検索できます。*インシデントの表示、189 ページ*を参照してください。
3. [Action] 列の Action ドロップダウン リストから **[Delete（削除）]** を選択し、次に **[OK]** をクリックします。

Incident List リスト全体を削除するのが必要また便利な場合、下記の sqlite3 コマンドを使用します。

```
sqlite3 /opt/WCG/config/new_scip3.db "delete from certificate_acl;"
```

メッセージのテキストの変更

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [SSL] > [Incidents]** > **[Incident List]** を順に選択します。
2. さらに詳しく検査するインシデントを見つけます。*インシデントの表示、189 ページ*を参照してください。
3. ペンシルをクリックしてウィンドウを開き、そこでこのエラー メッセージのテキストを変更します。たとえば、HelpDesk は、エラー メッセージにより詳細な情報を追加できます。
4. 新しいテキストを記入したときは、**[Submit（送信）]** をクリックし、変更を行わない場合は、**[Close Window（ウィンドウを閉じる）]** をクリックします。

インシデントの詳細の表示

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [SSL] > [Incidents]** > **[Incident List]** を順に選択します。
2. さらに詳しく検査するインシデントを見つけます。*インシデントの表示*、189 ページを参照してください。
3. 虫メガネをクリックし、下記のようなインシデントに関する追加の詳細情報を確認します。
   - **Description** — インシデント リストに表示されるメッセージ
   - **Created** — インシデントが作成された時刻
   - **Modified** — インシデントが変更された時刻
   - **Access attempts** — ユーザーがこのサイトにアクセスを試みた回数

Incident List への Web サイトの追加

Help | Content Gateway | バージョン 7.8.x

許可する、ブラックリストに載せる、またはトネリングするサイトを指定するには、**[Configure] > [SSL] > [Incidents] > [Add Website（Web サイトを追加）]** を順に選択します。手動で追加されたサイトには、時系列順の Ticket ID が割り当てられます。これらのサイトは、Incident List に表示されます。*インシデントの表示*、189 ページを参照してください。

1. インシデント リストに追加するサイトの URL を入力します。

   注意
   IPv6 アドレスを指定する場合は、アドレスを角括弧 ([]) で囲んでは**いけません**。

2. **[By Certificate（証明書に基づく）]** または **[By URL（URL に基づく）]** を選択します。
   - **[By Certificate]** は、より高度のセキュリティを提供します。証明書に基づきサイトを追加した場合、クライアントは、URL ではなく IP アドレスを使うことによってポリシーをバイパスすることはできません。[By Certificate] を選択した場合、Content Gateway はサーバー証明書を取得し、サイトを Incident List に追加します。*インシデントの表示*、189 ページを参照してください。

     サイトが証明書によってブロックされている場合、ワイルドカードの証明書は、共通名が認識されている場合でも受け入れられません。
   - サイトをトネリングする、許可する、またはブラックリストに載せるには、**[By URL]** を選択します。

3. [Action] ドロップダウン リストでサイトを **[Tunnel]**、**[Allow]**、または **[Blacklist]** のどのステータスで追加するかを指定します。詳細については、*インシデント レポート*、189 ページを参照してください。

   - **Tunnel**：（**[By URL]** の場合のみ有効）このサイトはトネリングされます。トラフィックは復号化されず、Content Gateway は証明書をチェックしません。

     重要

     Tunnel by URL（URL に基づくトンネル）は、すべての透過的プロキシ トラフィックで使用できるわけではありません。

     それは下記の条件で機能します。

     - クライアント アプリケーションが TLS を使用し、SNI（サーバー名識別）を含む場合は、Content Gateway は SIN のホスト名についてインシデント リストをチェックします。
     - SNI がない場合は、Content Gateway はオリジン サーバーに接続し、証明書を取得します。共通名が一意な FQDN である場合、Content Gateway はそれをインシデント リストで検索します。共通名が [*]（ワイルドカード）を含むか、または一意な FQDN でない場合は、Content Gateway は、インシデント リストで IP アドレスを検索します。

     代わりに、ARM *静的バイパス ルール*を使用します。

   - **Allow**：ユーザは証明書が有効でない場合でもそのサイトにアクセスできます。トラフィックが復号化され、証明書チェック機能が無効にさます。
   - **Blacklist**：そのサイトは完全にブロックされます。Verification Bypass（検証のバイパス）が設定されてい場合でも、ユーザーはこのサイトにアクセスできません。

4. **[Apply]** をクリックします。

CVE を無効化し一定の時間ネットワーク トラフィックをモニタした後、サイトを手動で Incident List に追加することを推奨します。（*検証設定値の設定*、183 ページを参照してください）。それにより、信頼のあるサイトをトネリングし、アクセスすべきでないと分かっているサイトをブロックすることによって、パフォーマンスを向上させます。トネリングなどステータスをサイトおよびインシデントに割り当てる方法については、*インシデント レポート*、189 ページを参照してください。

クライアント証明書

Help | Content Gateway | バージョン 7.8.x

セキュリティのために、宛先サーバーはクライアント証明書を要求することがあります。

関連項目：

- *クライアント証明書のインポート、194 ページ*
- *クライアント証明書が常に要求された場合：ホストリスト、195 ページ*
- *クライアント証明書の削除、195 ページ*

クライアント証明書が要求された場合

1. **[Cnfigure] > [SSL] > [Client Certificates（クライアント証明書）] > [Gneral]** を順に選択します。
2. Content Gateway がその証明書およびサイトを処理する方法を指定するには、**[Tunnel]** または **[Create incident（インシデントを作成）]** を選択します。トンネル以外の処理（ホワイト リストに入れる）を使用する場合は、**[Create incident]** を選択しなければなりません。ホワイト リスト機能は、常にサーバーに証明書を提供します。可能な処理のリストについては、*インシデント レポート、189 ページ*を参照してください。
3. **[Apply]** をクリックします。

クライアント証明書のインポート

Help | Content Gateway | バージョン 7.8.x

クライアントが代表する組織から証明書をインポートするには、**[Configure] > [SSL] > [Client Certificates] > [Import（インポート）]** を順に選択します。

重要

X.509 形式の、base64 エンコード方式の証明書のみを使用してください。

1. クライアント証明書の名前を入力します。
2. 証明書のパブリック キーを入力します。キーについてネットワーク管理者に問い合わせる必要があります。

3. 証明書のプライベート キーを入力します。キーについてネットワーク管理者に問い合わせる必要があります。
4. パスフレーズを入力し、確認します数字、文字、および大文字と小文字の組み合せた、強いパスフレーズを使用することを推奨します。パスフレーズについてネットワーク管理者に問い合わせる必要があります。
5. **[Import（インポート）]** をクリックします。

クライアント証明書が常に要求された場合：ホストリスト

Help | Content Gateway | バージョン 7.8.x

クライアント証明書が常に要求される宛先サーバーをリストするには、**[Configure] > [SSL] > [Client Certificates]** > **[Hostlist（ホストリスト）]** を順に選択します。必ず、証明書をインポートしてから、それを [Hostlist] に追加してください。*クライアント証明書のインポート、194 ページ*を参照してください。

1. クライアント証明書を必要とする宛先サーバーの URL を入力します。
2. **[Client Certificate（クライアント証明書）]** ドロップダウン リストからクライアント証明書の名前を選択します。このリストには、インポート済みの証明書だけが表示されます。
3. **[Add]** をクリックします。

> **重要**
>
> Server Name Indicator (SNI) を送信しないブラウザの場合、たとえば Internet Explorer バージョン 8 以前では、宛先 IP アドレスとホスト名の両方のエントリを作成します。

クライアント証明書の削除

Help | Content Gateway | バージョン 7.8.x

インポートしたクライアント証明書を削除するには、**[Configure] > [SSL] > [Client Certificates] > [Manage Certificates（クライアントを管理）]** を順に選択します。

1. 削除するクライアントを選択します。
2. **[Delete]** をクリックします。

SSL 接続エラー メッセージのカスタム化

Help | Content Gateway | バージョン 7.8.x

下記の場合に、ユーザーが受け取るメッセージをカスタマイズできます。

- ユーザーが無効の証明書があるサイトに接続しようとしている。*証明書検証フィールド*、196 ページを参照してください。
- 接続エラーがある。*SSL 接続エラー*、197 ページを参照してください。

メッセージ テンプレートの中で下記の変数を利用できます。

%P	プロトコル（HTTP または HTTPS）
%h	メッセージを生成したプロキシのホストの IP アドレスおよびポート
%o	メッセージを生成したプロキシのホストの IP アドレス
%H	要求のリモート ホスト名
%t	時刻
%s	Content Gateway サーバーの名前
%u	完全な URL
$$DETAILS	詳細なエラー メッセージ
$$TICKET_ID	インシデントの ID 番号

証明書検証フィールド

Help | Content Gateway | バージョン 7.8.x

証明書検証が失敗したときにユーザーが受け取るメッセージをカスタマイズするには、**[Configure] > [SSL] > [Customization] > [Certificate Failure（証明書エラー）]** を順に選択します。

注意

[Preview] をクリックすると、デフォルトのメッセージがどのように表示されるか確認できます。

Internet Explorer 10 の既知の問題によって、誤ったブロック ページが表示されることがあります。この問題を回避するには、正しいページが表示されるまで [Preview] を繰り返しクリックするか、または Internet Explorer 10 の TLS 1.0 を無効化します。

1. ウィンドウの HTML コードを編集してメッセージを反映させるようにします。メッセージで利用できる変数のリストについては、*SSL 接続エラー メッセージのカスタム化、196 ページ*を参照してください。
2. **[Preview]** をクリックして変更を確認します。
3. メッセージが適切に表示されるまで、ステップ 1 と 2 を繰り返します。
4. 編集を確認するには、**[Apply]** をクリックし、また元のメッセージに戻るには **[Cancel]** をクリックします。

SSL 接続エラー

Help | Content Gateway | バージョン 7.8.x

Content Gateway が宛先 Web サーバーに接続できなかったときに、ユーザーが受け取るメッセージをカスタマイズするには、**[Configure] > [SSL] > [Customization] > [Connect Error（接続エラー）]** を順にクリックします。

> **注意**
>
> **[Preview]** をクリックすると、デフォルトのメッセージがどのように表示されるか確認できます。
>
> Internet Explorer 10 には誤ったブロック ページが表示されてしまう k ことがある既知の問題があります。この問題を回避するには、正しいページが表示されるまで [Preview] を繰り返しクリックするか、または Internet Explorer 10 の TLS 1.0 を無効化します。

1. ウィンドウのテキストを編集してメッセージを反映させるようにします。メッセージで利用できる変数のリストについては、*SSL 接続エラー メッセージのカスタム化、196 ページ*を参照してください。
2. **[Preview]** をクリックして変更を確認します。
3. メッセージが適切に表示されるまで、ステップ 1 と 2 を繰り返します。
4. 編集を確認するには、**[Apply]** をクリックし、また元のメッセージに戻るには **[Cancel]** をクリックします。

14 セキュリティ

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway によって、プロキシとネットワーク上の他のコンピュータの間のセキュアな通信を確立できます。以下のことが可能です。

- プロキシへのクライアント アクセスを制御する。*プロキシへのクライアント アクセスの制御*、200 ページを参照してください。
- 下記のどちらかの方法で Content Gateway Manager へのアクセスを制御する。
  - 管理者アカウント（*管理者 ID およびパスワードの設定*、201 ページおよび*ユーザー アカウントのリストの作成*、202 ページを参照）。
  - 暗号化され、認証されたアクセスの場合の SSL (Secure Sockets Layer) 保護（*セキュアな管理のための SSL の使用*、203 ページを参照）。
- インターネットへのアクセスを制御し、特別の認証要件を指定し、プロキシを経由する他のトラフィックを制御するフィルタリング ルールを作成する。*フィルタリング ルール*、206 ページを参照してください。
- Content Gateway をユーザーのファイアウォールに統合し、1 つ以上の SOCKS サーバーを通じてトラフィックを制御する。*SOCKS ファイアウォール統合の設定*、211 ページを参照してください。
- Content Gateway がサイトのセキュリティ設定に対応するために複数の DNS サーバーを使用するように構成する。*Split DNS オプションの使用*、215 ページを参照してください。
- Content Gateway がユーザー認証を実行するように設定する。プロキシは、統合 Windows 認証（Kerberos を使用）、レガシー NTLM (NTLMSSP)、LDAP、および RADIUS ユーザー認証をサポートします。このほかに、複数の認証領域で複数の認証方法をサポートします。*Content Gateway ユーザー認証*、216 ページを参照してください。

プロキシへのクライアント アクセスの制御

Help | Content Gateway | バージョン 7.8.x

Content Gateway が特定のクライアントにだけプロキシの使用を許可するように設定できます。

アクセスを許可するには、**ip_allow.config** でクライアントの IP アドレスと IP アドレス範囲を指定します。

アクセスを拒否するには、そのクライアントの IP アドレスをこのファイルに含めないようにします。

1. **[Configure（設定）] > [Security（セキュリティ）] > [Connection Control（接続の制御）] > [Proxy Access（プロキシ アクセス）]** ページへ移動します。
2. **[Edit File（ファイルの編集）]** をクリックして、**ip_allow.config** ファイルの編集のための設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。各フィールドについては*設定のオプション*で説明しています。
4. **[Apply（適用）]** をクリックして情報を保存し、次に **[Close（閉じる）]** をクリックします。

> **注意**
> 許可されていないクライアントが Content Gateway へのアクセスを試みた場合、要求されたコンテンツを取得できないことを知らせるメッセージがブラウザに表示されます。

Content Gateway Manager へのアクセスの制御

Help | Content Gateway | バージョン 7.8.x

Content Gateway Manager へのアクセスを制限して、許可されているユーザーだけが設定オプションを変更し、パフォーマンスおよびネットワーク トラフィック統計を表示できるようにできます。

以下のことが可能です。

- 管理者 ID およびパスワードを設定する。管理者 ID で Content Gateway Manager にログオンしたユーザーは、Content Gateway Manager のすべてのアクティビティにアクセスできます。*管理者 ID およびパスワードの設定、201 ページ*を参照してください。

- Content Gateway Manager にログオンできるユーザーと、そのユーザーが実行できるアクティビティを決定するユーザー アカウントのリストを作成し、保守する。*ユーザー アカウントのリストの作成*、202 ページを参照してください。
- どのコンピューターが Content Gateway Manager にアクセスできるかを定義する IP アドレス アクセス制御リストを作成する。*Content Gateway Manager へのホスト アクセスの制御*、203 ページを参照してください。
- セキュアな管理のために SSL を使用する。*セキュアな管理のための SSL の使用*、203 ページを参照してください。
- 管理者に二要素認証を使用して、または使用せずに TRITON Unified Security Center にログオンし、次に、[Web Security manager Content Gateway access（Web Security manager Content Gateway アクセス）] ページを使用して Content Gateway Manager にログオンすることを要求する。*Content Gateway manager へのアクセス*、13 ページを参照してください。

管理者 ID およびパスワードの設定

Help | Content Gateway | バージョン 7.8.x

インストール時に、Content Gateway Manager への管理アクセスを制御するパスワードを割り当てます。正しい ID とパスワードを使用して Content Gateway Manager にログオンしたユーザーは、[Monitor（モニター）] タブのすべての統計を表示でき、また、[Configure（設定）] タブの任意の設定オプションを変更できます。

管理者 ID とパスワードは随時変更できます。

1. **[Configure] > [My Proxy] > [UI Setup（UI のセットアップ）] > [Login（ログイン）]** タブに移動します。
2. **[Basic Authentication]** が有効になっていることを確認します。

   Basic Authentication が無効化されている場合は、アクセスを拒否する IP アドレスのリスト（*Content Gateway Manager へのホスト アクセスの制御*、203 ページを参照）をセットアップしていない限り、すべてのユーザーが Content Gateway Manager にアクセスできます。
3. 現在の管理者 ID を変更するには、**[Administrator（管理者）]** セクションの **[Login（ログイン）]** フィールドに新しい ID を入力します。
4. 現在のパスワードを変更するには、[Old Password（古いパスワード）] フィールドに現在のパスワードを入力します。[New Password] フィールドに新しいパスワードを入力し、次に [New Password（Retype）（新しいパスワード（再入力））] フィールドに新しいパスワードを再入力します。

   現在の管理者パスワードを忘れた場合、*マスタ管理者パスワードを忘れた場合の Content Gateway manager へのアクセスの方法*、17 ページをご覧ください。
5. **[Apply]** をクリックします。

ユーザー アカウントのリストの作成

Help | Content Gateway | バージョン 7.8.x

Content Gateway Manager のために 1 つの管理者 ID とパスワードを設定するだけではニーズに対応する十分なセキュリティを確保できない場合、Content Gateway Manager にアクセスできるユーザーと、そのユーザーが実行できるアクティビティを定義するユーザー アカウントのリストを作成することができます。

1. **[Configure] > [My Proxy] > [UI Setup] > [Login（ログイン）]** に移動します。
2. Content Gateway Manager へのアクセスを許可するユーザーの名前を入力します。
3. そのユーザーのパスワードを入力し、次に [New Password (Retype)] フィールドにそのパスワードを再入力します。
4. **[Apply]** をクリックします。
5. ユーザー テーブルの **[Access（アクセス）]** ドロップダウン リストで、ユーザーが実行できる Content Gateway Manager アクティビティを選択します。
   - ユーザーによる Content Gateway Manager へのアクセスを無効化するには、**[No Access（アクセス禁止）]** を選択します。
   - ユーザーに [Monitor] タブでの統計の表示のみを許可する場合は **[Monitor Only（モニターのみ）]** を選択します。
   - ユーザーに [Monitor] タブでの統計の表示と [Configure] タブでの設定オプションの表示を許可する場合は **[Monitor and View Configuration（モニターおよび設定の表示）]** を選択します。
   - ユーザーに **[Monitor]** タブでの統計の表示と [Configure] タブでの設定オプションの変更を許可する場合は **[Monitor and Modify Configuration（モニターおよび設定の変更）]** を選択します。
6. **[Apply]** をクリックします。
7. Content Gateway Manager へのアクセスを許可する各ユーザーについて、ステップ 2 ～ ステップ 6 の手順を繰り返します。
8. **[Basic Authentication]** が有効になっていることを確認します。

   Content Gateway は、このオプションが有効化されている場合にのみ、ユーザー名とパスワードをチェックします。

Content Gateway Manager へのホスト アクセスの制御

Help | Content Gateway | バージョン 7.8.x

管理者 ID とユーザー アカウントの使用のほかに、どのホストが Content Gateway Manager にアクセスできるかを管理することができます。

1. **[Configure] > [My Proxy] > [UI Setup Access（UI セットアップ アクセス）]** へ移動します。
2. [Access Control（アクセス制御）] 領域で、**[Edit File]** をクリックして、**mgmt_allow.config** ファイルの編集のための設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは *UI セットアップ*、343 ページで説明しています。
4. **[Apply]** をクリックし、次に **[Close]** をクリックします。

セキュアな管理のための SSL の使用

Help | Content Gateway | バージョン 7.8.x

Websense は、Content Gateway Manager によるリモート管理モニタリングおよび設定を保護するために Secure Sockets Layer protocol (SSL) をサポートします。SSL セキュリティは、証明書を使用してネットワーク接続の両端の認証を提供し、暗号化を使用してプライバシーを提供します。

SSL を使用するには、以下の準備が必要です。

- SSL 証明書を取得する
- Content Gateway Manager SSL オプションを有効化する

SSL 証明書の取得

Help | Content Gateway | バージョン 7.8.x

SSL 証明書は、承認された認証機関から取得できます（例、VeriSign）。証明書を Content Gateway の **config** ディレクトリ（**/opt/WCG/bin**）にインストールします。証明書ファイルの名前をデフォルトのファイル名 **private_key.pem** に変更するか、または Content Gateway Manager を使用して証明書の名前を指定します（*SSL の有効化*、204 ページの手順に従います）。

SSL の有効化

Help | Content Gateway | バージョン 7.8.x

SSL 証明書を取得した後、SSL を有効化することができます。

1. **[Configure] > [My Proxy] > [UI Setup] > [General]** タブに移動します。
2. **HTTPS** オプションを有効化します。
3. [Certificate File（証明書ファイル）] フィールドで、SSL 証明書のファイル名を指定します。

   ファイル名の変更が必要になるのは、証明書ファイルがデフォルトのファイル名 **private_key.pem** を使用しない場合だけです。
4. **[Apply]** をクリックします。

FIPS 140-2 モード

Help | Content Gateway | バージョン 7.8.x

FIPS (Federal Information Processing Standard) 140-2 は、米国政府のハードウェアおよびソフトウェア暗号化モジュールに関するセキュリティ標準です。この標準に基づいて検証されているモジュールは、政府および他のユーザーに対して、システムで使用する暗号が基準に適合していることを保証します。

Websense Web Security Gateway (Anywhere) のバージョン 7.8 で使用している暗号ライブラリは、Content Gateway のコンポーネントを含めて、FIPS 140-2 の確認が完了しています。確認のリストを参照するには、[Validated FIPS 140 1 and FIPS 140-2 Cryptographic Modules] の 2012 年のリストにアクセスし、[Websense] を検索します。NIST FIPS 140-2 プログラムの詳細については、Cryptographic Module Validation Program (CMVP) 確認ページを参照してください。

デフォルトでは、Content Gateway は FIPS 140-2 モードでは機能しません。Content Gateway はまだ FIPS で確認されたライブラリを使用しますが、FIPS 140-2 標準でサポートされない暗号アルゴリズムも許可します。

Content Gateway を HTTPS 接続上で FIPS 140-2 を有効化するように構成することができます。

FIPS 暗号化が有効化されている時、

- HTTPS 接続は TLSv1 を使用します
- HTTPS 接続は FIPS 140-2 で承認されているアルゴリズムを使用します
- Content Gateway はオリジン サーバー証明書要求への応答として、SHA-256 証明書を生成します。

警告

FIPS 140-2 オプションが有効化された後、Content Gateway の完全な再インストールなしにそれを無効化することはできません。Content Gateway がアプライアンス上にある場合、アプライアンスを再構成しなければなりません。

重要

Web Security Gateway がいずれかの TRITON Enterprise コンポーネントと接続する時、FIPS 140-2 境界の問題が起こることがあります。これには下記の問題が含まれます。

- Web Security Gateway Anywhere で、クラウドを経由するトラフィックが FIPS 140-2 を使用しない。
- ThreatScope トラフィックが FIPS 140-2 を使用しない。
- Websense Data Security が FIPS 140-2 を使用しない。
- TRITON Mobile Security が FIPS 140-2 を使用しない。
- TRITON コンソール ログオンのために RSA SecurID が設定されている場合、RSA SecurID が FIPS 140-2 でない。

重要

システムの制限のため、FIPS 140-2 モードは、IWA の NTLM またはレガシー NTLM ユーザー認証へのフォールバックには使用できません。

HTTPS 接続上で FIPS 140-2 を有効化するには、以下の手順を実行します。

1. Content Gateway Manager で、**[Configure] > [Security] > [FIPS Security（FIPS セキュリティ）]** に進みます。
2. 警告を確認し、**[Enabled]** を選択し、**[Apply]** をクリックします。
3. FIPS を有効化する場合は、Content Gateway を再起動します。
4. FIPS を有効化しない場合は、**[Disable]** を選択して、**[Apply]** をクリックします。

注意

FIPS 140-2 モードが有効化された後でも、デフォルトで、TRITON 管理コンソールへのログオンのために SHA-1 証明書が引き続き使用されます。より強い SHA 認証書を作成およびインストールする方法については、[How do I create a stronger SHA certificate for Websense management consoles?（Websense 管理コンソール用の強い SHA 認証書を作成する方法）] を参照してください。

フィルタリング ルール

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、要求のいくつかのパラメータを検査して、条件に一致する場合に指定した処置を提供するためのルールを作成する機能をサポートします。以下のようなルールを作成できます。

- URL 要求を拒否または許可する
- カスタム ヘッダを挿入する
- 指定したアプリケーション、または指定した Web サイトの要求が認証をバイパスすることを許可する
- クライアント要求のヘッダー情報を保持または削除する
- 指定したアプリケーションがプロキシを通過することを禁止する

注意

IWA、NTLM および LDAP ユーザー認証のルールを作成する方法については、*ルール ベースの認証*、239 ページを参照してください。Content Gateway ユーザー認証オプションの使用を開始する方法については、*Content Gateway ユーザー認証*、216 ページを参照してください。

フィルタリング ルールの作成および変更は、**[Configure] > [Security] > [Access Control] > [Filtering]** タブ上で行います。ルールは **filter.config** ファイルに保存されます。

ルールはリストの上から順に適用されます。最初に条件に一致したルールだけが適用されます。条件に一致するルールがない場合、要求は処理されます。

二次指定子は任意です。ルールの中で 2 つ以上の二次指定子を使用できます。ただし、1 つの二次指定子を繰り返すことはできません。

デフォルトでは 3 つのフィルタリング ルールが設定されます。最初のルールは、すべてのアクセス先に対してポート 25 上のトラフィックを拒否します。2 番目と 3 番目のルールは、ThreatScope の 2 つの アクセス先に対してユーザー認証をバイパスします。

ルールを追加、削除または変更した後、Content Gateway を再起動します。

保存されているルールの構成に関する詳細は、*filter.config* を参照してください。

フィルタリング ルールの作成

1. **[Configure] > [Security] > [Access Control] > [Filtering]** タブに移動し、**[Edit File]** をクリックして、ファイル エディタで *filter.config* を開きます。
2. ドロップダウンリストから **[Rule Type（ルール タイプ）]** を選択します。ルール タイプは、ルールが適用する処置を指定します。下記のオプションがサポートされています。

   [allow（許可）] — 特定の URL 要求が認証をバイパスすることを許可します。プロキシは要求されたコンテンツをキャッシュに入れ、提供します。

   [deny（拒否）] — 特定の宛先からのオブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。

   [keep_hdr] — どのクライアント要求ヘッダ情報を保持するかを指定します。

   [strip_hdr] — どのクライアント要求ヘッダ情報を削除するかを指定します。

   [add_hdr] — カスタムのヘッダと値のペアを挿入します。**カスタム ヘッダ**と**ヘッダ値**が指定されている必要があります。特定のヘッダと値のペアを要求する宛先ポストをサポートします。具体例を下の *Google enterprise gmail を許可する add_hdr ルールの作成*に示しています。

   > **注意**
   > [radius] ルール タイプは**サポートされていません**。

3. **[Primary Destination Type（一次宛先タイプ）]** を選択し、次に **[Primary Destination Value（一次宛先値）]** フィールドに対応する値を入力します。一次宛先タイプには、下記のタイプが含まれます。

   dest_domain — 要求されたドメイン名。対応する値はドメイン名です。

   dest_host — 要求されたホスト名。対応する値はホスト名です。

   dest_ip — 要求された IP アドレス。対応する値は IP アドレスです。

   url_regex — URL に含まれる正規表現。対応する値は正規表現です。

4. 一次宛先タイプが **keep_hdr** または **strip_hdr** である場合、**[Header Type（ヘッダー タイプ）]** ドロップダウン リストから保持または削除する情報のタイプを選択します。以下のオプションがあります。
   - **date（日付）**
   - **host（ホスト）**
   - **クッキー**
   - **client_ip**
5. ルールが特定のポート上のインバウンド トラフィックにのみ適用される場合、**プロキシ ポート**の値を入力します。
6. ルール タイプが **add_hdr** である場合、**カスタム ヘッダ**および**ヘッダ値**を指定します。**カスタム ヘッダ**と**ヘッダ値**は、宛先ホストが想定している値でなければなりません。下の Google Business Gmail の例を参照してください。
7. 要求または想定されている二**次指定子**の値を提供します。以下の二次指定子があります。

   Time（時間）— 時間範囲（例、08:00-14:00）を指定します。

   Prefix（接頭辞）— URL のパス部分の接頭辞を指定します。

   Suffix（接尾辞）— URL のファイル接尾辞を指定します。

   Source IP address（ソース IP アドレス）— 1 つのクライアント IP アドレス、またはクライアントの IP アドレスの範囲を指定します。

   Port（ポート）— 要求された URL の中のポートを指定します。

   Method（メソッド）— 要求された URL メソッドを指定します。
   - get
   - post
   - put
   - trace

   Scheme（スキーム）— 要求された URL のプロトコルを指定します。以下のオプションがあります。
   - HTTP
   - HTTPS
   - FTP（FTP over HTTP の場合のみ）

   User-Agent（ユーザー - エージェント）— 要求ヘッダのユーザー - エージェントの値を指定します。これは正規表現（regex）です。

   [User-Agent] フィールドを使用して、下記のような処置を行うアプリケーション フィルタリング ルールを作成できます。
   - 認証の要求を適切に処理しないアプリケーションが認証をバイパスすることを許可する
   - 特定のクライアント ベースのアプリケーションからのインターネットのアクセスを禁止する

より詳しい説明といくつかの例が、Websense Knowledge Base の『When authentication prevents devices, browsers, and custom applications from working with the proxy』というタイトルの記事に収録されています。

8. ルールの定義が完了したとき、**[Add]** をクリックしてルールを追加し、次に、**[Apply]** をクリックしてルールを保存します。
9. ルールの追加が完了したとき、**[Apply]** をクリックしてすべての変更を保存し、次に、**[Close]** をクリックして編集ウィンドウを閉じます。
10. 新しいルールを有効にするには、[Content Gateway Manager] ウィンドウを選択し、Content Gateway を再起動します。

ルールの編集

1. **[Configure] > [Security] > [Access Control] > [Filtering]** に進み、**[Edit File]** をクリックしてファイル エディタで *filter.config* を開きます。
2. リストの中の変更するルールを選択し、希望する値に変更します。
3. **[Set（設定）]** をクリックしてルールを更新し、**[Apply]** をクリックしてルールを保存します。
4. **[Close]** をクリックして編集ウィンドウを閉じます。
5. 変更を有効にするには、[Content Gateway Manager] ウィンドウを選択し、Content Gateway を再起動します。

Google enterprise gmail を許可する add_hdr ルールの作成

Google は要求の中のカスタム ヘッダの形で、Google が enterprise gmail および他の Google Apps for Business へのアクセスを認識し、許可またはブロックするメカニズムを提供しています。

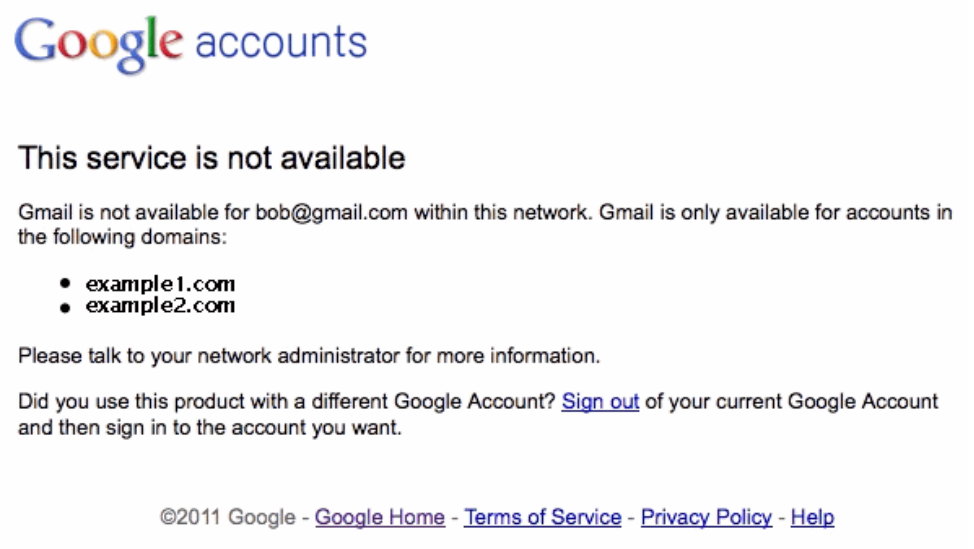
Google のソルーションを enterprise gmail で使用できるようにするには、

1. Web Security manager で、Web Security カテゴリ **[Internet Communication] > [General Email]** を許可します。
2. Content Gateway Manager で **HTTPS**（SSL 暗号化）を有効化します。サイトでまだ SSL サポートを使っていない場合は、この機能をよく理解してから有効化してください。
3. Content Gateway Manager の **[Configure] > [Security] > [Access Control]** ページで **filter.config** を開き、**add_hdr** ルールを作成します。

> **注意**
>
> **add_hdr** ルール タイプは、カスタム ヘッダ-値のペアを使用して特殊な処理を実施する任意のサイトに使用できます。

a. **add_hdr** を選択します。
b. **[Primary Destination Type]** には **dest_domain** を選択します。
c. **[Primary Destination Value]** には、mail.google.com を指定します。
d. **[Custom Header]** フィールドで、[X-GoogApps-Allowed-Domains] を指定します。
e. **[Header Value]** フィールドで、自分のドメイン、またはドメインのリスト（カンマで区切る）を指定します。例：www.example1.com,www.example2.com
f. オプションとして、**[Source IP]** フィールドでこのルールを適用する送信元 IP アドレスまたは送信元 IP アドレスの範囲を指定します。例：10.10.20.30 または 10.10.1.1-10.30.40.50
g. **[Add]** をクリックしてルールを追加します。
h. **[Apply]** をクリックしてすべての変更を保存し、次に、**[Close]** をクリックして編集ウィンドウを閉じます。
i. 新しいルールを有効にするために、Content Gateway を再起動します。

ユーザーが許可されていないアカウントから Google サービスにアクセスしようとしたとき、Google は下のようなブロック ページを表示します。



Google のフィルタリング ソリューションについての Google による説明は、『Block access to consumer accounts and services while allowing access to Google Apps for your organization』に掲載されています。

SOCKS ファイアウォール統合の設定

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *SOCKS サーバーの設定*、212 ページ
- *SOCKS プロキシ オプションの設定*、214 ページ
- *SOCKS サーバー バイパスの設定*、215 ページ

SOCKS はネットワーク ファイアウォールとしてよく使われており、SOCKS サーバーの後方のホストがインターネットへの完全なアクセスを取得することを許可し、同時に、インターネットからファイアウォールの内側のホストへの無許可のアクセスを禁止します。

Content Gateway はキャッシュに保存されていないコンテンツへの要求を受け取ったとき、オリジン サーバーにそのコンテンツを要求しなければなりません。SOCKS 設定では、プロキシはオリジン サーバーに直接にアクセスする代わりに、SOCKS サーバーを経由してアクセスします。SOCKS サーバーはプロキシとオリジン サーバーの間の通信を許可し、データをオリジン サーバーに中継します。次に、オリジン サーバーは SOCKS サーバーを経由してプロキシにコンテンツを返送します。キャッシュが有効化されている場合、Content Gateway はコンテンツをキャッシュに入れてからクライアントに送信します。

- Content Gateway は SOCKS クライアントとして動作でき、SOCKS クライアントとして HTTP または FTP 要求を通常通りに受信および提供します。
- Content Gateway は SOCKS プロキシとして動作でき、SOCKS サーバーとの間での要求のやりとり（通常はポート 1080 上）を中継します。
- Content Gateway は、V-シリーズ アプライアンス上にインストールされている時、SOCKS サーバーとして動作でき、SOCKS サーバーのすべてのサービスを提供します。（Content Gateway は、アプライアンス上に**インストールされていない**時、SOCKS サーバーとして動作できません）。

注意

Content Gateway は、クライアントによる認証を実行しません。しかし、Content Gateway は SOCKS バージョン 5 を実行している SOCKS サーバーによるユーザー名およびパスワードの認証を実行します。

SOCKS サーバーの設定

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、ネットワーク内の 1 つ以上の SOCKS サーバーを処理するように設定できます。Content Gateway が V-シリーズ アプライアンス上にインストールされている時、SOCKS サーバーはそのモジュールに含まれています。

> **注意**
> Content Gateway が V-シリーズ アプライアンス上に**インストールされていない**時、Content Gateway に SOCKS サーバーは提供されません。

SOCKS サーバーを設定するには、下記の手順を実行します。

1. SOCKS 機能を有効化します。
   a. **[Configure] > [My Proxy] > [Basic] > [General]** の順に選択します。
   b. **[Features（フィーチャ）]** テーブルの **[Security]** セクションで、**[SOCKS On]** をクリックし、次に、**[Apply]** をクリックします。
   c. Content Gateway を再起動してください。
2. SOCKS のバージョンを指定します。
   a. **[Configure] >[Security] >[SOCKS] >[General]** の順に選択します。
   b. SOCKS サーバー上で実行している SOCKS のバージョンを選択し、**[Apply]** をクリックします。
3. アプライアンス上の V-シリーズ SOCKS を設定するには、以下の手順を実行します。
   a. **[Server（サーバー）]** タブを選択します。
   b. **[On-Appliance SOCKS Server（アプライアンス上の SOCKS サーバー）]** 領域で、**[Enabled（有効）]** を選択し、**[Apply]** をクリックします。

      socks_server.config ファイルにサーバーのエントリが作成されます。
   c. デフォルト エントリを変更するには、**[SOCKS Server]** 領域で **[Edit File]** を選択します。エディタで **[On-Appliance-SOCKS-Server]** ルールを選択します。

      ポートを変更することができ、それがデフォルトの SOCKS サーバーであるかどうか、およびサーバー認証が適用されるかどうかの設定を変更できます。

      サーバー名または IP アドレスは変更できません。これは常にループバック アドレスです。

      必要な変更を行った後、**[Set]** をクリックします。

4. ネットワーク内での他の SOCKS サーバーの使用を設定するには、以下の手順を実行します。
   a. **[Server]** タブを選択し、**[SOCKS Server]** 領域で **[Edit File]** をクリックします。
   b. SOCKS サーバー名を入力します。
   c. SOCKS サーバーの IP アドレス、またはネットワーク内の DNS サーバーによって解決できるドメイン名を入力します。
   d. これをデフォルトの SOCKS サーバーとして指定するかどうかを選択します。
   e. 認証を使用する場合、SOCKS ユーザー名とパスワードを指定します。
   f. **[Set]** をクリックして、サーバーをリストに追加します。

      いつでもエディタに戻って、ルールを選択し、変更を行い、**[Set]** をクリックしてそれを保存することができます。
5. 複数の SOCKS サーバーがある場合、それらを追加した後、または追加中に、それらを優先順に編成することができます。そのためには、エントリを選択して上向きおよび下向き矢印を使って、リスト内でそのエントリを上または下に移動します。
6. **[Apply]** をクリックしてすべての変更を確認し、次に、**[Close]** をクリックしてエディタを閉じます。
7. **[SOCKS Server Rules（SOCKS サーバー ルール）]** 領域で、宛先 IP アドレスによって特定のルーティングまたはバイパスを指定するルールを作成できます。*SOCKS サーバー バイパスの設定、215 ページ*を参照してください。
8. すべての SOCKS サーバーに適用する設定オプションを検討するには、**[Options]** タブを選択します。
   a. **[Server Connection Timeout（サーバー接続タイムアウト）]** の値を検討し、調整します。これは Content Gateway が SOCKS サーバーへの接続を試みて待機する時間（秒）を指定します。この時間を過ぎるとタイムアウトになります。
   b. **[Connection Attempts Per Server（サーバーあたりの接続試行回数）]** の値を検討し、調整します。これは Content Gateway が特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、サーバーに [接続不能] というマークが付けられます。
   c. **[Server Pool Connection Attempts（サーバー プール接続試行回数）]** の値を検討し、調整します。これは Content Gateway がプール内の特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、試行を中止します。
9. SOCKS サーバー設定が完了したとき、**[Apply]** をクリックし、次に、**[Configure] > [My Proxy] > [General]** を選択して Content Gateway を再起動します。

リストからサーバーを削除するには、以下の手順を実行します。

1. **[SOCKS Server]** 領域で **[Edit File]** をクリックします。
2. リストの中で、削除するエントリを選択し、リストの左側の **X** をクリックします。
3. **[Apply]** をクリックし、次に、エディタを終了する準備ができたとき、**[Close]** をクリックします。
4. 設定が完了したとき、**[Configure] > [My Proxy] > [General]** を選択して Content Gateway を再起動します。

SOCKS プロキシ オプションの設定

Help | Content Gateway | バージョン 7.8.x

Content Gateway を SOCKS プロキシとして設定するには、SOCKS プロキシ オプションを有効化し、Content Gateway が SOCKS クライアントからの SOCKS トラフィックを受け付けるポートを指定します。

SOCKS プロキシとして、Content Gateway はクライアントからの SOCKS パケットを受信し（通常はポート 1080 上で）、要求を SOCKS サーバーへ直接に転送することができます。

> **注意**
> SOCKS オプションを有効化し、*SOCKS サーバーの設定、212 ページ*に示している SOCKS サーバー情報を指定するだけでなく、SOCKS プロキシ オプションを設定しなければなりません。

1. **[Configure] > [Security] > [SOCKS] > [Proxy]** の順に選択します。
2. **SOCKS プロキシ**を有効化します。
3. Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。デフォルト ポートは 1080 です。
4. **[Apply]** をクリックします。
5. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

SOCKS サーバー バイパスの設定

Help | Content Gateway | バージョン 7.8.x

Content Gateway が SOCKS サーバーをバイパスし、特定のオリジン サーバーに直接にアクセスするように設定することができます。

1. **[Configure] > [Security] > [SOCKS] > [Server]** の順にクリックします。**[SOCKS Server Rules（SOCKS Server ルール）]** 領域で、**[Edit File]** を選択して **socks.config** を開きます。
2. 既存のルールを変更するには、リストからルールを選択し、変更を行い、**[Set]** をクリックします。
3. 新しいルールを作成するには、パラメータを指定して **[Add（追加）]** をクリックします。
   a. **ルール タイプ**を選択します。
      SOCKS サーバーを通過する
      SOCKS サーバーを通過しない
   b. 宛先 IP アドレスまたはアドレスの範囲を指定します。[すべてのネットワーク ブロードキャスト アドレス] (255.255.255.255) を指定してはいけません。
   c. トラフィックに使用する SOCKS サーバーを選択します。
   d. トラフィックを指定された SOCKS サーバーにラウンド ロビン方式で配分するかどうかを指定します。
   e. **[Add]** をクリックしてルールを追加します。
4. **[Apply]** をクリックし、次に **[Close]** をクリックします。
5. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

Split DNS オプションの使用

Help | Content Gateway | バージョン 7.8.x

セキュリティ要件に応じて、Content Gateway が複数の DNS サーバーを使用するように設定できます。たとえば、Content Gateway が 1 つの DNS サーバーのセットを使って社内ネットワーク上のホスト名を解決し、ファイアウォールの外側の DNS サーバーがインターネット上のホストを解決するように設定することができます。これによってイントラネットのセキュリティを維持し、同時に組織外のサイトへの直接のアクセスを提供します。

[Split DNS（分割 DNS）] を設定するためには、次のタスクを実行しなければなりません。

- 宛先ドメイン、宛先ホスト、または URL 正規表現を基に DNS サーバー選択を実行するためにルールを指定します。
- [Split DNS] オプションを有効化する。

Content Gateway Manager で下記の手順を実行します :

1. **[Configure] > [Networking] > [DNS Resolver] > [Split DNS]** タブを選択します。
2. **[Split DNS]** オプションを有効化する。
3. **[Default Domain（デフォルト ドメイン）]** フィールドで、分割 DNS 要求のデフォルト ドメインを入力します。Content Gateway は、自動的にこの値を、使用する DNS サーバーを決定する前の、ドメインを含まないホスト名に付加します。
4. **[DNS Servers Specification（DNS サーバー指定）]** 領域で、**[Edit File]** をクリックして、*splitdns.config* ファイルの編集のための設定ファイル エディタを開きます。
5. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは *splitdns.config* で説明しています。
6. **[Apply]** をクリックし、次に **[Close]** をクリックします。.
7. **[Split DNS]** タブで、**[Apply]** をクリックして設定を保存します。
8. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

Content Gateway ユーザー認証

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *ブラウザの制約*、219 ページ
- *グローバル認証オプション*、220 ページ
- *統合 Windows 認証*、225 ページ
- *レガシー NTLM 認証*、230 ページ
- *LDAP 認証*、233 ページ
- *RADIUS 認証*、236 ページ
- *ルール ベースの認証*、239 ページ
- *Mac および iPhone/iPad 認証*、263 ページ

Content Gateway は、ユーザーの要求の処理を許可する前にユーザー認証を行うためのいくつかの方法をサポートします。これらの方法と Websense Web Security ユーザー認証 (XID) 機能を合わせて使用することによって、ユーザー認証が失敗した場合や利用できなくなった場合のフォールバックを提供できます。

明示および透過プロキシ モードの両方で、Content Gateway は、下記の方法によるユーザー認証をサポートします。

- *統合 Windows 認証* (Kerberos with SPNEGO to NTLM)
- *レガシー NTLM 認証* (NTLMSSP)
- *LDAP 認証*
- *RADIUS 認証*

Content Gateway はまた、下記を使用した統合 Windows 認証 (IWA)、レガシー NTLM、および LDAP をサポートします。

- *ルール ベースの認証、239 ページ*

ルール ベースの認証サマリ

ルール ベースの認証は、順序が指定された認証ルールのリストです。要求を処理する時、リストが上から順に検討され、最初に一致したルールが適用されます。

ルールは下記を指定します：

1. クライアントの一致基準。

   基準

   - IP アドレス
   - インバウンド プロキシ ポート（明示のプロキシのみ）
   - User-Agent 値
   - 上記の組み合わせ
2. 認証の基準となるドメイン、またはドメインの順序が指定されたリスト

   リストの中で、最初に認証に成功したドメインが記憶され、そのユーザーの以降の認証に使用されます。

複数レルムのネットワーク ルール ベースの認証は複数レルムのネットワーク構造、つまり、Windows Active Directory ドメインに相互の信頼関係がないため、各ドメイン メンバーがそのドメイン内でドメイン コントローラによって認証される必要があるようなネットワーク構造をサポートします。この環境では、下記を指定するルールが作成されます。

1. IP アドレスまたはプロキシ ポートを基準とするレルム（信頼されないドメイン）メンバー
2. そのメンバーが属すレルム（ドメイン）

ドメインのメンバーシップが不明の場合の認証 組織によっては、ユーザーがどのドメインに属しているかを常時把握していないことがあります。たとえば、組織が新規事業を迅速に取得している場合に、そのような問題が起こります。ドメインのメンバーシップが不明であるという問題は、ルール ベースの認証では、IP アドレスのリストまたは範囲に対して、認証の基準として使用するドメインの順序を指定したリストを指定するルールを作成することによって対処できます。最初に認証に成功したドメインが記憶され、以降の認証に使用されます。

User-Agent 値をベースとする認証。認証ルールで 1 つ以上の User-Agent 値を指定できます。多くの場合、これはブラウザのリストです。User-Agent 値がルールと一致する場合、指定されたドメインを基準に認証が実行されます。User-Agent 値がどのルールとも一致せず、他の値をベースとして一致するルールも存在しない場合、認証は実行されません（どんな場合でも、一致するルールがなければ認証は実行されません）。

認証方法の選択

認証モードは Content Gateway Manager の **[Configure] > [My Proxy] > [Basic]** ページの **[Authentication]** セクションで選択します。ルール ベースの認証のための認証の設定では、最初に **[Rule-Based Authentication（ルール ベースの認証）]** を選択します。

サポートされているドメイン コントローラとディレクトリ

- Windows NT ドメイン コントローラ
- Windows 2003、2008、2012 Active Directory
- Novell eDirectory 8.7 および 8.8（LDAP のみ）
- Oracle DSEE 11g、Sun Java 7 および 6.2（LDAP のみ）

Windows Active Directory を使用する時の最善の方法

1 つの Active Directory ドメインだけが存在するか、またはすべての Active Directory ドメインがインバウンドおよびアウトバウンドの信頼関係を共有している場合の最善の方法は、統合 Windows 認証を配備することです。ただし、User-Agent 値をベースとして認証を管理する場合は、ルール ベースの認証を使用しなければなりません。

複数のドメインまたはレルムが存在し、ユーザー認証が必要である場合、ルール ベースの認証を使用しなければなりません。詳細については、*ルール ベースの認証*、239 ページを参照してください。

ユーザー識別だけで十分である場合、Web Security ユーザー識別オプションの 1 つを使用することができます。『*User Identification* in Web Security Help』というタイトルのセクションを参照してください。

バックアップ ドメイン コントローラ

統合 Windows 認証およびレガシー NTLM に対して、Content Gateway はフェールオーバー用のバックアップ ドメイン コントローラの指定をサポートします。プライマリ ドメイン コントローラ (DC) がプロキシ要求に応答しない場合、Content Gateway はリストの中の次の DC（バックアップ ドメイン コントローラ）にコンタクトします。次の要求に対して、プロキシは再びプライマリ DC へのコンタクトを試み、接続が失敗した場合、バックアップ DC にコンタクトします。

透過的ユーザー認証

Content Gateway は透過的認証（シングル サインオン）と対話形式（プロンプト形式）の認証の両方をサポートします。透過的認証は統合 Windows 認証およびレガシー NTLM によってサポートされます。一部のブラウザは、限定的なサポートのみを提供します。*ブラウザの制約、219 ページ*を参照してください。

Windows ネットワークで、シングル サインオンを設定している時、ユーザーは一度だけサインオンすれば、すべての許可されているネットワーク リソースに透過的にアクセスできます。したがって、ユーザーがすでに Windows ネットワークに正常にログオンしている場合、Windows ログオン時に指定された証明書がプロキシ認証に使用され、ユーザーは再びユーザー名とパスワードの入力を求められることはありません。

[対話形式の認証は、シングル サインオンに設定されていないネットワークで、また。シングル サインオンをサポートしないブラウザで使用するためにサポートされます。対話形式の認証では、ユーザーは Content Gateway を通じてコンテンツにアクセスできるようになる前に、資格情報の入力を要求されます。

ブラウザの制約

Help | Content Gateway | バージョン 7.8.x

すべての Web ブラウザが透過的ユーザー認証をサポートするわけではありません。

注意
最も完全で最新の情報については、『version 7.8 Content Gateway Release Notes』を参照してください。

下のテーブルは、統合 Windows 認証（IWA）が構成されている時に、ブラウザが認証要求に対応する方法を示しています。

ブラウザ / OS	Internet Explorer（v9 および 10 でテスト済み）	Firefox	Chrome	Opera（v12.02 でテスト済み）	Safari（v6.02 でテスト済み）
Windows	透過的認証を実行	透過的認証を実行（v21 でテスト済み）	透過的認証を実行（v26 および 27 でテスト済み）	NTLM にフォールバックして資格情報を要求	NTLM にフォールバックして資格情報を要求
Mac OS X	対応しない	透過的認証を実行（v21 でテスト済み）	透過的認証を実行（v23 でテスト済み）	テスト未実行	透過的認証を実行
Red Hat Enterprise Linux, update 6	対応しない	透過的認証を実行 （v11 でテスト済み）	明示的プロキシ：透過的認証を実行。 透過的プロキシ：NTLM にフォールバックして資格情報を要求。 （v27 でテスト済み）	テスト未実行	対応しない

グローバル認証オプション

Help | Content Gateway | バージョン 7.8.x

[Configuration] > [Security] > [Access Control] > [Global Authentication Options（グローバル認証オプション）] ページを使用して、下記を設定します。

- ユーザー認証 *Fail Open*/fail closed の動作
- *資格情報キャッシング*オプション
- *リダイレクト ホスト名*（透過的プロキシ配備のために必要）

これらの設定はすべてのプロキシ ユーザー認証設定に対して、下記の各オプションで記述されているパラメータの範囲内で適用されます。

これらの設定のいずれかを変更した時は、必ず **[Apply]** をクリックして変更を保存し、次にプロキシを再起動して、変更を有効化してください。

Fail Open

Fail Open は、ユーザー認証が失敗した場合に、要求の Web Security での処理を許可するかどうかを指定します。

Fail Open が有効化されていて、Web Security XID エージェントが設定されているとき、認証が失敗し、クライアントが XID エージェントによって識別される場合、ユーザー ベースのポリシーが適用されます。ユーザーを識別できず、クライアントの IP アドレスにポリシーが割り当てられている場合、そのポリシーが適用されます。そうでない場合は、デフォルトのポリシーが適用されます。

重要

[Fail Open（フェイル オープン）] の設定は、IWA が認証方法であり、ドメインコントローラ (DC) の停止によってクライアントが DC から kerberos チケットを取得できない場合には適用しません。

IWA が NTLM にフォールバックしたときには、[Fail Open] の設定は IWA に適用されます。

以下のオプションがあります。

- **[Disabled（無効）]** — 認証が失敗した時に要求を処理しないことを指定します。
- **[Enabled only for critical service failures（クリティカルなサービスの障害の場合にのみ有効）]**（デフォルト）— 下記の原因で認証が失敗した場合にのみ要求を処理することを指定します。
  - ドメイン コントローラからの応答がない
  - クライアントが送信しているメッセージのフォーマットが不適切である
- **[Enabled for all authentication failures, including incorrect password（パスワードの間違いを含むすべての認証失敗で有効）]** — パスワードの間違いを含むすべての認証失敗で要求を処理することを指定します。

重要

ユーザー認証がルール ベースで、ドメイン リストを使用する時、

- **[Enabled only for critical service failures]** を選択している場合は、クリティカルなサービスの障害が発生した時、フェイル オープンは**適用されません**。エラーが発生した場合は常にフェイル クローズになります。
- **[Enabled for all authentication failures, including incorrect password]** を選択している場合は、リスト内のすべてのドメインで基本資格情報を試した後、フェイル オープンが適用されます。

資格情報キャッシング

資格情報キャッシングには次のようなオプションがあります。

- キャッシング方法
- キャッシュ継続時間 (TTL)（分単位）
- LDAP 固有の設定

資格情報キャッシングは、Content Gateway が明示のプロキシか透過的プロキシかに関わりなく、すべてのクライアントに適用されます。

資格情報キャッシングは下記に適用されます。

- Content Gateway が透過的プロキシの場合、すべての認証方法に
- Content Gateway が明示的プロキシの場合
  - Integrated Windows Authentication (IWA) が NTLM にフォールバックするか NTLM を折衝するとき、NTLM に
  - レガシーNTLM

IWA が Kerberos を使用して認証する時、Kerberos はチケット（資格情報）キャッシングを使用します。

キャッシング方法のオプション

[**Cache using IP address only（キャッシュに IP アドレスのみを使用）**] — すべての資格情報が IP アドレスの代替を使ってキャッシングされることを指定します。これはすべてのクライアントが固有の IP アドレスを持っている場合に推奨される方法です。

[**Cache using Cookies only（キャッシュに Cookie のみを使用）**] — すべての資格情報が cookie の代替を使ってキャッシングされることを指定します。これはすべてのクライアントが IP アドレスを共有している場合 — たとえば、Citrix サーバーのようなマルチ ホスト サーバーを使用している場合 — や、トラフィックが Content Gateway へトラフィックを転送するデバイスによってネットワーク アドレス変換される場合に推奨される方法です。

[**Cache using both IP addresses and Cookies（キャッシュに IP アドレスと Cookie の両方を使用）**] — cookie キャッシング リストにリストされている IP アドレスには cookie の代替を使用し、他のすべての IP アドレスには IP アドレスの代替を使用することを指定します。これは、ネットワークに固有の IP アドレスを持つクライアントと、マルチ ユーザー ホストを使用するかネットワーク アドレス変換されるクライアントの両方が含まれる場合に推奨される方法です。

代替資格情報については、*代替資格情報*を参照してください。

重要

Cookie モードのキャッシング

- Cookie モードのキャッシングは cookie をサポートしないアプリケーションや、または cookie のサポートが無効化されているブラウザでは使用できません。
- ブラウザが Internet Explorer である場合、ローカル イントラネット領域に完全なプロキシ ホスト名（“http://host.domain.com” の形式）が追加されなければなりません。
- ブラウザが Chrome である場合、サードパーティーの cookie を許可するように設定するか、またはプロキシ ホスト名からの cookie（“host.domain.com” の形式）を許可するための例外を設定しなければなりません。
- cookie モードとして IP アドレスが設定されていて、要求方法が CONNECT である場合、キャッシングは実行されません。
- FTP 要求には cookie モードのキャッシングは実行されません。

注意

明示的プロキシに対する NTLM キャッシュを無効にするためのユーザー インターフェース設定が削除されました。**proxy.config.ntlm.cache.enabled** の値を **0**（ゼロ）に設定することによって、records.config 内の明示的プロキシ トラフィックに対するキャッシュを無効化することができます（ただし、この方法は推奨されません）。

キャッシュ継続時間

[**Cache Time-To-Live**] (TTL) は、キャッシュ内のエントリが保持される時間（分単位）を指定します。TTL を過ぎるとエントリは消去され、ユーザーが次に要求を送信した時、認証を要求されます。認証が成功した場合、エントリがキャッシュに保存されます。

TTL のデフォルトは 15 分です。有効な値の範囲は 5 - 1440 秒です。

LDAP 固有の設定

[**Purge LDAP cache on authentication failure（認証失敗時に LDAP キャッシュをパージ）**] を有効にすると、LDAP ユーザー認証が失敗した時にプロキシはそのクライアントの認証レコードを LDAP キャップから削除します。

リダイレクト ホスト名

[Redirect Hostname（リダイレクト ホスト名）] は、プロキシの代替ホスト名を指定します。

> **注意**
> 統合 Windows 認証ではリダイレクト ホスト名は使用されません。

デフォルトでは、認証を行っているクライアントは、Content Gateway コンピュータのホスト名へリダイレクトされます。クライアントが DNS によってそのホスト名を解決できない場合、またはプロキシに代替の DNS 名が定義されている場合、**[Redirect Hostname]** フィールドでそのホスト名を指定しなければなりません。

> **注意**
> 透過的プロキシのユーザー認証が透過的に（つまり、ユーザーに資格情報を要求することなしに）行われるようにするには、リダイレクト ホスト名がブラウザの**イントラネット ゾーン**に含まれるようにブラウザを設定しなければなりません。そのためには、一般的には、リダイレクト ホスト名がブラウザを実行しているコンピュータと同じドメインに含まれるようにします。たとえば、クライアントが **workstation.example.com** で、リダイレクト ホスト名が **proxyhostname.example.com** である場合、ブラウザは認証が透過的に行われる（ユーザーに認証を要求しない）ことを許可します。ご使用のブラウザのマニュアルを参照してください。

> **注意**
> Content Gateway は WCCP 負荷配分を使用するプロキシ クラスタでの透過的認証をサポートします。ただし、**割り当てメソッドの配分属性**はソース IP アドレスでなければなりません。詳細については、*WCCP の負荷配分、68 ページ*を参照してください。

代替資格情報

代替資格情報は、最初の認証成功の後に資格情報キャッシュに保存されるエントリです。

- IP アドレス代替は資格情報と IP アドレスを結合します。これはその IP アドレスがどの時点においても 1 人のユーザーによってのみ使用されることを想定します。
- cookie 代替はクライアントのシステム上に置かれている cookie と結合します。これはクライアントのアプリケーションが cookie をサポートすることに依存します。この方法は、クライアントの IP アドレスが同時に 2 人以上のユーザーによって共有される場合 - たとえば Citrix サーバーなどのマルチユーザー ホストを使用する場合 - に必要となります。

最初の認証成功以降は、Content Gateway はその後のユーザーの認証要求に対して代替資格情報を使用して応答し、それによって遅延を減らし、ドメイン コントローラおよびディレクトリ サービスへの負荷を軽減します。TTL が過ぎると資格情報代替エントリは消去されます。

統合 Windows 認証

Help | Content Gateway | バージョン 7.8.x

統合 Windows 認証 (IWA) は、共有の信頼関係がある Windows ドメイン（1 つまたは複数）に属している複数のユーザーを認証するための堅牢な手段です。

統合 Windows 認証は、

- Kerberos および SPNEGO を使用する
- 明示および透過的プロキシ モードで NTLM をサポートする
- NTLMv2 with Session Security および NTLMv1 with Session Security をサポートする
- Windows Active Directory 2003、2008 および 2012 をサポートする
- ルール ベースの認証と合わせて使用できる
- Internet Explorer 7 以上、Firefox 4 以上、Google Chrome 6 以上、Windows Safari 4 以上、iPad iOS4 上の Safari 4 以上、Opera 10 以上をサポートする
- UTF-8 形式のユーザー名をサポートする
- 要求された認証（プロンプト形式）へのフォールバックをサポートする

必要条件

- クライアントがドメインに結合されている
- クライアントのブラウザが Content Gateway の完全修飾ドメイン名 (FQDN) をイントラネット サイトまたは信頼できるサイトとして指定している
- 明示的プロキシ環境では、ブラウザは Content Gateway の FQDN を指定しなければならない

IWA でルール ベースの認証を使用している場合の設定の手順は*ルール ベースの認証、239 ページ*を参照してください。

統合 Windows 認証：設定のまとめ

IWA をユーザーの Content Gateway 配備のユーザー認証方法として設定するには、以下の手順を実行します。

- Content Gateway Manager の **[Configure] > [My Proxy] > [Basic]** ページで [**Integrated Windows Authentication**] を有効化し、**[Apply]** をクリックします。
- *グローバル認証オプション*を設定します。
- Content Gateway を Windows ドメインに結合します。要求される条件のリストは、*統合 Windows 認証の設定*に掲載しています。

統合 Windows 認証の設定

1. **[Configure] > [My Proxy] >[Basic] >[General]** の順に選択します。**[Authentication**（認証）**]** セクションで [Integrated Windows Authentication] をクリックして **[On]** にして、**[Apply]** をクリックします。
2. *グローバル認証オプション*の設定
3. Windows ドメインを結合します。

   ドメインを結合するには、以下の条件が満たされていなければなりません。

   - Content Gateway がドメイン名を解決できなければなりません。
   - Content Gateway のシステム時刻がドメイン コントローラの時刻と ±1 分以内の誤差で同期化されていなければなりません。
   - 正しいドメイン管理者名とパスワードを指定しなければなりません。
   - ドメイン コントローラ（ポート 88、389、445）に対する TCP/UDP 接続が確立されていなければなりません。
   - バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center (KDC) サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。

   a. **[Domain Name**（ドメイン名）**]** フィールドに完全修飾名を入力します。
   b. **[Administrator Name]** フィールドに Windows Administrator のユーザー名を入力します。
   c. **[Administrator Password]** フィールドに Windows Administrator のパスワードを入力します。

      名前とパスワードは結合時にのみ使用し、保存されません。
   d. ドメイン コントローラを見つける方法を選択します。
      - **DNS による自動検出**
      - **DC 名と IP アドレス**

ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。

e. **[Content Gateway Hostname（Content Gateway ホスト名）]** フィールドで、ホスト名が正しいホスト名で、15 文字以内（V-シリーズ アプライアンスでは 11 文字以内）であることを確認します。文字数がそれより多ければ、IWA を使用する場合は短くしなければなりません。長さの制限は、NetBIOS ホスト名の長さの制限（15 文字）によるものです。

警告

ドメインを結合した後でホスト名を変更してはいけません。ホスト名が変更された場合、IWA はただちに作業を中止し、ドメインの結合を解除して、新しいホスト名で再結合するまで機能しません。

f. **[Join Domain]** をクリックします。エラーがある場合、上記の条件が満たされていることを確認してから、*ドメインを結合できない*を参照してください。

重要

認証対象のすべてのクライアントがドメインに結合されていなければなりません。

ブラウザと他のプロキシ クライアントが Content Gateway の FQDN をイントラネット サイトまたは信頼できるサイトとして指定するように設定されていなければなりません。

g. Content Gateway を再起動し、プロキシを通じていくつかのテスト トラフィックを実行して、認証が想定通りに機能していることを確認します。問題がある場合は、*統合 Windows 認証のトラブルシューティング*を参照してください。

現在のドメインの結合を解除し、新しいドメインを結合するには

1. **[Configure] > [Security] > [Access Control] > [Integrated Windows Authentication]** タブに移動し、**[Unjoin（結合を解除）]** をクリックします。
2. 新しいドメインを結合するには、**[Domain Name]** フィールドに完全修飾ドメイン名を入力します。
3. **[Administrator Name]** フィールドに Windows Administrator のユーザー名を入力します。

4. **[Administrator Password]** フィールドに Windows Administrator のパスワードを入力します。名前とパスワードは結合時にのみ使用し、保存されません。
5. ドメイン コントローラを見つける方法を選択します。
   - **DNS による自動検出**
   - **DC 名と IP アドレス**

     ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
6. **[Join Domain]** をクリックします。

ドメイン コントローラを見つける方法を変更するには、以下の手順を実行します

1. **[Configure] > [Security] > [Access Control] > [Integrated Windows Authentication]** タブに移動します。
2. **[Domain Controller]** のセクションで、ドメイン コントローラを見つける方法を選択します。
   - **DNS による自動検出**
   - **DC 名と IP アドレス**

     ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
3. **[Apply]** をクリックします。

統合 Windows 認証のトラブルシューティング

Help | Content Gateway | バージョン 7.8.x

この項では、よく起こる 2 つの問題を説明しています。

- *ドメインを結合できない*
- *クライアントを認証できない*

ドメインを結合できない

Content Gateway がドメインを結合するには、以下の条件が必要です。

- Content Gateway がドメイン名を解決できなければなりません。
- Content Gateway のシステム時刻がドメイン コントローラの時刻と±1 分以内の誤差で同期化されていなければなりません。
- 正しいドメイン管理者名とパスワードを指定しなければなりません。
- ドメイン コントローラ（ポート 88、389、445）に対する TCP/UDP 接続が確立されていなければなりません。

- バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center（KDC）サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。
- Active Directory が複数サイトで設定されている場合、Content Gateway が置かれているサブネットがそれらのサイトのいずれかに追加されることを確認してください。

トラブルシューティング

- 結合処理中に発生したエラーは画面の上部（ [Integrated Windows Authentication] タブ）に報告されます。
- 通常、エラー メッセージには、詳細情報が記載されている障害ログへのリンクが含まれています。
- 結合の障害は **/opt/WCG/logs/smbadmin.join.log** に記録されます。
- ほとんどの場合、ログ内の障害メッセージは標準 Samba および Kerberos エラー メッセージであり、インターネット検索によって容易に参照できます。

クライアントを認証できない

クライアントを認証するには、以下の条件が必要です。

- Content Gateway クライアントは、Content Gateway によって結合されるクライアントと同じドメインのメンバーでなければなりません。
- クライアント のシステム時刻がドメイン コントローラおよび Content Gateway の時刻と ±1 分以内の誤差で同期化されていなければなりません。
- 明示のプロキシ クライアントが Content Gateway の IP アドレスに要求を送信するように**設定されていない**こと。クライアントは Content Gateway の完全修飾ドメイン名（FQDN）を使用しなければなりません。IP アドレスを使用している場合、常に NTLM 認証が実行されます。
- Content Gateway FQDN が DNS の中にあり、すべてのプロキシ クライアントがそれを解決できなければなりません。
- ブラウザと他のクライアント アプリケーションが Content Gateway の FQDN をイントラネット サイトまたは信頼できるサイトとして指定しなければなりません。
- Active Directory が複数サイトで設定されている時、Content Gateway が置かれているサブネットがそれらのサイトのいずれかに追加されなければなりません。そうでない場合、Content Gateway を再開した時に下記のアラームが生成されることがあります。

  `Windows domain [domain name] unreachable or bad membership status`（`Windows` トメイン ［ドメイン名］ が見つからないか、メンバーシップの状態が不適切です）

トラブルシューティング

Content Gateway Manager の **[Monitor] > [Security] > [Integrated Windows Authentication]** タブで **[Diagnostic Test（診断テスト）]** 機能を選択します。このモニター ページは認証要求の統計を表示し、診断テスト機能を提供します。

[**Diagnostic Test**] 機能は接続性および認証テストを実行し、エラーを報告します。また、ドメイン コントローラの TCP ポート接続性および遅延を示します。

エラーおよびメッセージは、下記のファイルにログ記録されます。

- /var/log/messages
- content_gateway.out
- /opt/WCG/logs/smbadmin.log
- /opt/WCG/logs/smbadmin.join.log

パフォーマンスの問題

- **IWA (Kerberos):** 認証のパフォーマンスは CPU によって制約されます。Kerberos 認証では、ドメイン コントローラとの通信は行われません。
- **NTLM および基本 :** ドメイン コントローラの応答性がパフォーマンスに影響を及ぼします。**[Monitor] > [Security] > [Integrated Windows Authentication]** ページは、平均応答時間を示します。

レガシー NTLM 認証

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、Windows ネットワークのユーザーがインターネットへのアクセスを許可される前に認証されることを保証する方法として、NTLM (NT LAN Manager) 認証プロトコルをサポートしています。

> **重要**
> この NTLM サポートの実装（レガシー NTLM）は NTLMSSP プロトコルのみを使用します。これは本セクションに記載されている通りに信頼できるパフォーマンスを提供しますが、この方式の代わりに *統合 Windows 認証*モードを使用することを強く推奨します。後者は NTLM に対する、より堅牢で、安全なサポートを提供します。

重要

ルール ベースの認証を使用する場合、*ルール ベースの認証*オプションで Legacy NTLM 認証を設定します。

しかし、このセクションを読んで、Legacy NTLM の機能および制限に習熟してください。

レガシー NTLM オプションが有効化されている時、プロキシはコンテンツを要求するユーザーに対して資格情報の証明を要求します。次に、プロキシはユーザーの資格情報の証明を直接に Windows ドメイン コントローラに送信して確認を求めます。資格情報が有効であれば、プロキシは要求されている内容を提供し、その資格情報を将来の使用のために NTLM キャッシュに保存します。資格情報が有効でない場合、プロキシは *authentication failed（認証失敗）*メッセージを送信します。

制約

1. **WINS 解決**はサポートされていません。ドメイン コントローラのホスト名は DNS サーバーが解決できる名前でなければなりません。
2. **拡張セキュリティ**はサポートされておらず、ドメイン コントローラ上で有効化できません。
3. **NTLM2 セッション セキュリティ**はサポートされておらず、クライアント上で有効化できません。Windows OS の [Security Settings（セキュリティ設定）] の領域で、**[Network Security: Minimum session security（ネットワーク セキュリティ: 最小限のセッション セキュリティ）]** の設定を調べます。
4. **NTLMv2** は Active Directory 2008 ではサポートされていません。**要求される [Network Security: LAN Manager Authentication（ネットワーク セキュリティ：LAN マネージャ認証）]** の設定については、下の *[NTLM プロキシ認証の設定]* のステップ 5 で示しています。
5. すべてのブラウザが透過的 NTLM 認証をサポートするわけではありません。*ブラウザの制約*、219 ページを参照してください。

Legacy NTLM でルール ベースの認証を使用している場合の設定の手順は*ルール ベースの認証*、239 ページを参照してください。

レガシー NTLM 認証の設定

1. **[Configure] > [My Proxy] >[Basic] >[General]** の順に選択します。
2. **[Authentication（認証）]** セクションで Legacy NTLM をクリックして **[On]** にし、**[Apply]** をクリックします。
3. *グローバル認証オプション*の設定
4. **[Configure] > [Security] > [Access Control] > [Legacy NTLM]** へ進みます。

5. **[Domain Controller Hostnames]** フィールドにプライマリ ドメイン コントローラのホスト名を入力し、次に、任意に、バックアップ ドメイン コントローラのカンマ区切り形式のリストを入力します。ホスト名の形式は下記のいずれかでなければなりません。

   ```
   host_name[:port][%netbios_name]
   ```

   または

   ```
   IP_address[:port][%netbios_name]
   ```

   注意

   Active Directory 2008 を使用している場合、netbios_name を含めるか、SMB ポート 445 を使用しなければなりません。ポート 445 を**使用しない**場合、Active Directory サーバー上で Windows Network File Sharing サービスが実行していることを確認しなければなりません。詳細についてはご使用の Windows Server 2008 のマニュアルを参照してください。

   注意

   Active Directory 2008 を使用押している場合、Windows の **[Network Security（ネットワーク セキュリティ）]** 設定で、**[LAN Manager Authentication level（LAN マネージャ認証レベル）]** を **[Send NTLM response only（NTLM 応答の送信のみ）]** に設定しなければなりません。詳細についてはご使用の Windows Server 2008 のマニュアルを参照してください。

6. 複数のドメイン コントローラに認証要求を送信するときにプロキシがロードバランスを利用するようにするには、**[Load Balancing（ロード バランス）]** を有効化します。

   注意

   複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。

7. **[Apply]** をクリックし、Content Gateway を再起動します **([configure] > [My Proxy] > [Basic] > [General])**。

オプションとして、Content Gateway が特定のクライアントに対して、NTLM サーバーによる認証を求められることなしにインターネット上の特定のサイトにアクセスすることを許可するように設定することができます（*Access Control（アクセス制御）*、378 ページを参照）。

LDAP 認証

Help | Content Gateway | バージョン 7.8.x

Content Gateway は LDAP オプションをサポートします。このオプションは、ユーザーがプロキシを通じてコンテンツにアクセスする前に LDAP サーバーによって認証されることを保証します。

> **重要**
> ルール ベースの認証を使用する場合、*ルール ベースの認証*オプションで LDAP 認証を設定します。しかし、このセクションを読んで、LDAP の機能および制限に習熟してください。

LDAP が有効化されている時、

- Content Gateway は LDAP クライアントとして機能し、コンテンツを要求するユーザーに直接にユーザー名およびパスワードを要求します。
- ユーザー名とパスワードを受け取った後、Content Gateway は LDAP サーバーにコンタクトして、その資格情報が正しいかどうかを確認します。
- LDAP サーバーがユーザー名とパスワードを受け入れた場合、プロキシはクライアントに要求されたコンテンツを提供し、そのユーザー名とパスワードを資格情報キャッシュに保存します。
- その後のそのユーザーについての認証要求は、キャッシュ エントリの継続期間（TTL 値）が過ぎるまで、キャッシュ情報によって処理されます。
- LDAP サーバーがそのユーザー名とパスワードを拒否した場合、ユーザーのブラウザは認証が失敗したことを知らせるメッセージを表示し、再びユーザー名とパスワードの入力を要求します。

LDAP 認証は単純バインドと匿名バインドの両方をサポートします。

Content Gateway が LDAP クライアントとして機能するように設定する

1. **[Configure] > [My Proxy] >[Basic] >[General]** の順に選択します。
2. **[Authentication（認証）]** セクションで LDAP をクリックして **[On]** にし、**[Apply]** をクリックします。
3. *グローバル認証オプション*の設定
4. **[Configure] > [Security] > [Access Control] > [LDAP]** へ進みます。
5. LDAP サーバーのホスト名を入力します。
6. Content Gateway が LDAP サーバーとの通信に使用するポートを入力します。デフォルト ポートは 389 です。

   注意

   LDAP ディレクトリ サービスが Active Directory である時、グローバル カタログのベース ドメインの外のユーザーからの要求は認証に失敗します。これは LDAP のデフォルト ポートが 389 であり、389 へ送信された要求がグローバル カタログのベース ドメイン内でのみオブジェクトを検索するからです。ベース ドメインの外のユーザーを認証するには、LDAP ポートを 3268 に変更します。3268 へ送信された要求は、フォレスト全体でオブジェクトを検索します。

7. プロキシが LDAP サーバーとの間でセキュアな通信を使用するようにするには、**Secure LDAP** を有効化します。セキュアな通信はポート 636 または 3269 上で実行されます。必要に応じて、前のフィールドでポートの値を変更できます。
8. 検索のためのフィルタを設定するために、ディレクトリ サービスのタイプを選択します。
   - **[Microsoft Active Directory]** を選択すると、タイプが **sAMAccountName**（デフォルト）に設定されます。
   - **[Other]** を選択すると、eDirectory またはその他のディレクトリ サービスでは、タイプが **uid** に設定されます。
9. LDAP ベースのディレクトリ サービスのユーザーの**バインド識別名**（完全修飾名）を入力します。例：

   ```
   CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
   ```

   このフィールドには最大 128 文字まで入力できます。

   このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
10. 前のステップで指定したユーザーのパスワードを入力します。
11. **ベース識別名** (DN) を入力します。この値は LDAP 管理者から取得します。

12. **[Apply]** をクリックします。
13. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

任意に、以下の手順を実行できます。

- LDAP キャッシュ オプションを変更します。*LDAP キャッシュ オプションの設定*、235 ページを参照してください。
- Content Gateway が特定のクライアントに対して、LDAP サーバーによる認証を求められることなしにインターネット上の特定のサイトにアクセスすることを許可するように設定する。（*Access Control（アクセス制御）*、378 ページを参照してください）。

LDAP キャッシュ オプションの設定

デフォルトでは、LDAP キャッシュは 5000 個のエントリを保存するように設定されており、各エントリは 3000 分の間、最新であると想定されます。これらのオプションを変更するには **records.config** ファイルを編集します。

1. **/opt/WCG/config** の **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
`proxy.config.ldap.cache.size`	LDAP キャッシュに保存できるエントリの数を指定します。 デフォルト値は 5000 で、最小値は 256 です。
`proxy.config.ldap.auth.ttl_value`	Content Gateway がユーザー名およびパスワード エントリを LDAP キャッシュに保存できる期間（分）を指定します。
`proxy.config.ldap.cache.storage_size`	LDAP キャッシュが使用できるディスク スペースの量（バイト数）の最大値を指定します。 この値を変更する時、それに比例して **proxy.config.ldap.cache.size** の値も更新しなければなりません。たとえば、キャッシュ サイズを 2 倍にした場合は、キャッシュ ストレージ サイズも 2 倍にします。 この変数を変更して **proxy.config.ldap.cache.size** を変更しなかった場合、LDAP サブシステムは機能停止します。

3. ファイルを保存して、閉じます。
4. Content Gateway の **bin** ディレクトリ **(/opt/WCG/bin)** から、**content_line -L** を実行してローカル ノード上でプロキシを再起動するか、または **content_line -M** を実行してクラスタ内のすべてのノード上でプロキシを再起動します。

セキュアな LDAP の設定

デフォルトでは、LDAP トラフィックはセキュアでない状態で送信されます。Secure Sockets Layer (SSL) / Transport Layer Security (TLS) テクノロジを使用して LDAP トラフィックを機密のセキュアな通信にすることができます。LDAP over SSL (LDAPS) を有効化するには、Microsoft 認証機関 (CA) または Microsoft 以外の CA から適切な形式の証明書をインストールします。

Content Gateway で LDAPS を使用には、以下の手順を実行します。

1. **/opt/WCG/config** の **records.config** ファイルを開きます。
2. **records.config** に下記のエントリを追加します。

   ```
   CONFIG proxy.config.ldap.secure.bind.enabled INT 1
   ```

3. **[Configure] > [Security] > [Access Control] > [LDAP]** へ移動し、ポートを 3269 に変更します。

> **注意**
>
> Directory Service は LDAPS 認証をサポートするように設定されていなければなりません。その方法については、ディレクトリ サービスのプロバイダによって提供されるマニュアルを参照してください。

RADIUS 認証

Help | Content Gateway | バージョン 7.8.x

Content Gateway は RADIUS オプションをサポートします。このオプションは、ユーザーがプロキシを通じてコンテンツにアクセスする前に RADIUS サーバーによって認証されることを保証します。

RADIUS が有効になると、下記のようになります。

- Content Gateway は RADIUS クライアントとして機能し、コンテンツを要求するユーザーに直接にユーザー名およびパスワードを要求します。
- ユーザー名とパスワードを受け取った後、Content Gateway は RADIUS サーバーにコンタクトして、その資格情報が正しいかどうかを確認します。

- RADIUS サーバーがそのユーザー名とパスワードを受け入れた場合、プロキシは要求されたコンテンツをクライアントに提供し、そのユーザー名とパスワードを RADIUS キャッシュに保存します。そのユーザーに関する将来のすべての認証要求は、そのエントリが時間切れになるまで、RADIUS キャッシュから処理されます。
- RADIUS サーバーがそのユーザー名とパスワードを拒否した場合、ユーザーのブラウザは認証が失敗したことを知らせるメッセージを表示し、再びユーザー名とパスワードの入力を要求します。

Content Gateway は、フェールオーバー用にプライマリ RADIUS サーバーとセカンダリ RADIUS サーバーをサポートします。プライマリ サーバーが指定した時間（デフォルトでは 60 秒）内にプロキシ要求に応答しない場合、Content Gateway は再びユーザー名とパスワードのチェックを試みます。最大再試行回数（デフォルトでは 10 回）までにプライマリ RADIUS サーバーからの応答がない場合、プロキシはセカンダリ RADIUS サーバーにコンタクトします。Content Gateway がセカンダリ RADIUS サーバーにコンタクトできない場合、ユーザーは再びユーザー名とパスワードの入力を要求されます。

RADIUS のキャッシュはメモリに保持され、ディスク上に保存されます。Content Gateway はディスク上のデータを 60 秒ごとに更新します。また、Content Gateway は RADIUS のキャッシュのユーザー名およびパスワード エントリを 60 秒ごとに保存します。RADIUS キャッシュ内のパスワードおよびユーザー名エントリが期限切れになっている場合、Content Gateway はユーザー名およびパスワードを承認または拒否するために RADIUS サーバーにコンタクトします。

Content Gateway が RADIUS クライアントとして機能するように設定するには、以下の手順を実行します。

- RADIUS オプションを有効化します。
- プライマリおよびセカンダリ（任意）RADIUS サーバーのホスト名または IP アドレスと、Content Gateway が RADIUS サーバーと通信するために使用するポートおよび共有キーを指定します。

Content Gateway が RADIUS クライアントとして機能するように設定する、237 ページを参照してください。

Content Gateway が RADIUS クライアントとして機能するように設定する

1. **[Configure] > [My Proxy] >[Basic] >[General]** の順に選択します。
2. [Authentication] セクションで、[Radius] をクリックして **[On]** にして、**[Apply]** をクリックします。
3. **[Configure] > [Security] > [Access Control] > [Radius]** へ移動します。
4. プライマリ RADIUS サーバーのホスト名を入力します。
5. Content Gateway がプライマリ RADIUS サーバーとの通信に使用するポートの番号を入力します。

6. 暗号化に使用するキーを入力します。
7. セカンダリ RADIUS サーバーを使用している場合、**[Secondary Radius Server（Optional）]** 領域の該当するフィールドにホスト名、ポート、共有キーを入力します。
8. **[Apply]** をクリックします。
9. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

> **注意**
> これらの手順を実行するほかに、Content Gateway コンピュータをプライマリおよびセカンダリ RADIUS サーバー上の信頼できるクライアントとして追加し、Content Gateway コンピュータに使用する共有キーを指定しなければなりません（共有キーは下記の手順で使用するものと同じでなければなりません）。RADIUS サーバーのマニュアルを参照してください。

RADIUS キャッシュおよびサーバー タイムアウト オプションの設定

デフォルトでは、RADIUS キャッシュおよび RADIUS サーバー タイムアウト オプションは下記のように設定されます。

- RADIUS キャッシュは 1,000 個のエントリを保存するように設定されており、各エントリは 60 分の間、最新であると想定されます。
- 接続が 10 秒間アイドル状態である場合、Content Gateway は RADIUS サーバーへの接続の再確立を試みることができ、接続の再試行は 10 回まで可能です。

これらのデフォルト値を変更するには **records.config** ファイルを編集します。

1. **/opt/WCG/config** の **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
`proxy.config.radius.auth.min_timeout`	Content Gateway から RADIUS サーバーへの接続がアイドル状態に維持される時間を指定します。この時間を過ぎると Content Gateway の接続が失われます。
`proxy.config.radius.auth.max_retries`	Content Gateway が RADIUS サーバーへの接続を試みる最大回数を指定します。

変数	説明
proxy.config.radius.cache.size	RADIUS キャッシュに保存できるエントリの数を指定します。 最小値は 256 です。256 より小さい値を入力した場合、Content Gateway は SEGV を生成します。
proxy.config.radius.auth.ttl_value	Content Gateway がユーザー名およびパスワード エントリを RADIUS キャッシュに保存できる期間（分）を指定します。
proxy.config.radius.cache.storage_size	RADIUS キャッシュが使用できるディスク スペースの量の最大値を指定します。 この値はエントリの数の 100 倍以上でなければなりません。可能な最大量のディスク スペースを割り当てることを推奨します。

3. ファイルを保存して、閉じます。
4. Content Gateway の **bin** ディレクトリ **(/opt/WCG/bin)** から **content_line -L** を実行してローカル ノード上で Content Gateway を再起動するか、**content_line -M** を実行してクラスタ内のすべてのノード上で WCG を再起動します。

ルール ベースの認証

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *グローバル認証オプション、220 ページ*
- *ルール ベース認証のドメイン リスト、245 ページ*
- *LDAP ルールの作成、251 ページ*
- *既存の認証ルールの使用、254 ページ*
- *ルール ベースの認証の使用例、255 ページ*
- *User-Agent をベースとする認証、258 ページ*
- *認証ルールのトラブルシューティング、260 ページ*

ルール ベースの認証は、順序が指定された認証ルールのリストを使用して、複数レルム、複数ドメイン、および他の特殊な認証を要件をサポートします。要求を処理する時、リスト リストの上から順に検討され、最初に一致したルールが適用されます。

ルールは下記を指定します：

1. ユーザーの一致基準。

   基準

   - IP アドレス
   - インバウンド プロキシ ポート（明示のプロキシのみ）
   - User-Agent 値
   - 上記の組み合わせ

2. 認証の基準となるドメイン、またはドメインの順序が指定されたリスト

   ドメインのリストの中で、最初に認証に成功したドメインがキャッシュされ、以降の認証に使用されます。IP アドレス キャッシングが設定されている場合、IP アドレスがキャッシュされます。Cookie Mode が設定されている場合、クッキー（ユーザー）がキャッシュされます。

ルール ベースの認証では、最初に一致したルールだけが試行されます。認証が失敗した場合、それ以上の認証の試みは行われません。

ルール ベースの認証は、これらの特殊な要件を満たすために考案されました。

- **複数レルムのネットワーク** ルール ベースの認証は複数レルムのネットワーク、つまり、ドメインが信頼関係を共有していないため、各ドメイン のメンバーがそのドメイン内でドメイン コントローラによって認証される必要があるようなネットワークをサポートします。この環境では、下記を指定するルールが作成されます。
  - IP アドレスまたはプロキシ ポートを基準とするレルム（信頼されないドメイン）メンバー
  - そのメンバーが属すレルム（ドメイン）

注意

v7.7.x 以前の Multiple Realm Authentication を使用しているユーザーは、ルール ベースの認証を次のように考えることができます。

- Multiple Realm Authentication 機能の名称を変更し、機能を拡張した
- ドメインの順序が指定されたリストをサポートする
- ルールで使用するドメインを指定する方法を再編し、簡素化した
- 資格情報キャッシュの方法を簡素化した（*グローバル認証オプション*、220 ページを参照）

詳しい説明は、このセクションの以下の部分をお読みください。

- **ドメインのメンバーシップが不明の場合の認証**組織によっては、ユーザーがどのドメインに属しているかを常時把握していないことがあります。たとえば、組織が新規事業を迅速に取得している場合や、ディレクトリ サービスのマッピングまたは集約が行われていない場合に、そのような問題が起こります。ドメインのメンバーシップが不明であるという問題は、ルール ベースの認証では、IP アドレスのリストまたは範囲に対して、認証の基準として使用するドメインの順序を指定したリストを指定するルールを作成することによって対処できます。最初に認証に成功したドメインが記憶され、以降の認証に使用されます。認証が失敗した場合や、ブラウザがタイムアウトになった場合、認証は実行されません。
- **User-Agent 値をベースとする認証**。認証ルールで 1 つ以上の User-Agent 値を指定できます。多くの場合、これはブラウザのリストです。User-Agent 値がルールと一致する場合、指定されたドメインを基準に認証が実行されます。User-Agent 値がどのルールとも一致せず、他の値をベースとして一致するルールも存在しない場合、認証は実行されません（ルール ベースの認証では、どんな場合でも、一致するルールがなければ認証は実行されません）。

使用例は、*ルール ベースの認証の使用例、255 ページ*を参照してください。

> **注意**
> ネットワーク内のすべてのユーザーが、信頼関係を共有しているドメイン コントローラによって認証できる場合、ルール ベースの認証は必要ありません。
>
> しかし、このオプションは IP アドレス、インバウンド プロキシ ポート（明示のプロキシ）、および（または）User-Agent 値をベースとする複数のルールを活用できる単一ドメイン環境に適しています。

ルール ベースの認証の構造とロジック

構造

- ドメインのリストが作成および保守されます。

  ドメインをリストに追加する時、認証方法が指定されます。IWA、レガシー NTLM、LDAP のいずれかです。RADIUS はサポートされません。

  認証ルールでは、ドメイン リスト上のドメインだけが指定可能です。

  ドメイン リストの作成および保守は、**[Configure] > [Security] > [Access] [Control] > [Domains（ドメイン）]** タブ上で行います。ドメイン リストは **auth_domains.config** ファイルに保存されます。
- 認証ルールはユーザー（クライアント）を IP アドレス、インバウンド プロキシ ポート（明示のプロキシのみ）、および（または）User-Agent 値によって識別し、ユーザーを指定したドメインまたはドメインのリストに対して認証しようとします。

認証ルールは **[Configure] > [Security] > [Access Control] > [Authentication Rules（認証ルール）]** タブ上で定義されます。ルールは **auth_rules.config** ファイルに保存されます。

> **注意**
> 資格情報キャッシングは **[Configure] > [Security] > [Access Control] > [Global Configuration Options（グローバル設定オプション）]** タブ上で実行されます。このページで IP アドレス キャッシング、cookie キャッシング、またはその両方を指定します。この設定は透過的プロキシと明示的プロキシの両方のトラフィックに適用されます。IP アドレス キャッシングと cookie キャッシングの両方を指定している時、cookie キャッシングを適用する IP アドレスを指定しなければなりません。

ロジック

- クライアントおよびドメインに対して 1 つ以上のルールが定義されます **[Configure] > [Security] > [Access Control] > [Authentication Rules（認証ルール）]**
- web コンテンツ要求を受信した時、
  - リストが上から順にチェックされます
  - 最初に一致したルールが適用されます
  - ルールがドメインのリストを含んでいる場合、認証は下記のように行われます。
    - プロキシは最初のドメインを、そのドメインのために設定されている方法を使用して認証しようとします。たとえば、最初のドメインが IWA である場合、Content Gateway は透過的に資格情報（407 または 401）についてブラウザと折衝します。
    - 認証が失敗し、Content Gateway がまだ資格情報を要求（入力要求）していない場合、Content Gateway は資格情報の入力を要求します。

      例外：Content Gateway が明示的プロキシであり、最初および 2 番目のドメインが IWA である場合、基本資格情報は要求されません。代わりに、Content Gateway はクライアントによって提供された Kerberos チケットを使用して 2 番目のドメインの認証を試みます。この試みが失敗し、NTLM 認証へのフォールバックが失敗した場合、ユーザーは資格情報の入力を要求されます。

      Content Gateway が透過的プロキシである場合、標準動作が適用されます。これは、ユーザーが最初のドメインのメンバーでない場合、Kerberos チケットの要求は失敗します。これはクライアントがこの要求と共に送信された FQDN を信頼しないためです。NTLM 認証へのフォールバックも失敗し、ユーザーは資格情報の入力を要求されます。

- 次に Content Gateway は、2 番目のドメインから順に、認証が成功するまで、またはリストの終わりまで各ドメインに対して基本資格情報を使用して認証を試みます。
- 次に Content Gateway は基本資格情報を使用して、もう一度、最初のドメインに対して認証を試みます。
- すべてのドメインに対して認証が失敗した場合、**[Fail Open]**（**[Configuration] > [Security] > [Access Control] > [Global Authentication Options]**）の設定に応じて、下記のどちらかが行われます。

  [Enabled only for critical service failures（クリティカルなサービスの障害の場合にのみ有効）] に設定されている場合、プロキシはユーザーが入力した資格情報が間違っていると判断して、もう一度基本資格情報の入力を要求し、リストに対して順に認証を試みます。

  [Enabled for all authentication failures, including incorrect password（パスワードの間違いを含むすべての認証失敗の場合に有効）] に設定されている場合、フェイル オープンが適用されます。

  - 条件に一致するルールがない場合、認証の試みは行われません。

- トランザクションは、Filtering Service で使用するユーザー名を使ってログに記録されます。
- プロキシの認証統計が収集され、認証方法別に報告されます。*セキュリティ、309 ページ*（[統計] のセクション）を参照してください。

> **重要**
>
> Content Gateway には、各レルムについて IWA 認証で使用する Content Gateway の完全修飾ドメイン名 (FQDN) を解決できる DNS サーバーが組み込まれていなければなりません。そうでない場合、IWA は機能しません。DNS サーバーの設定方法はネットワーク管理者が決定します。1 つのオプションとして、Content Gateway のプライマリ DNS サーバーと各認証レルム（隔離されたドメイン）の DNS サーバーの間に DNS トランスファー ゾーン（サブ ゾーン）を構成するという方法があります。

ルール ベース認証の設定の要約

1. Content Gateway が明示のプロキシで、複数ポート上でトラフィックを受信したい場合、**[Configure] > [Protocol] > [HTTP]** タブでポートを指定します。

重要

また、クライアントが正しいポートを使用するように設定しなければなりません。

2. *グローバル認証オプション、220 ページ*を設定します（**[Configure] > [Security] > [Access Control] > [Global Authentication Options（グローバル認証オプション）]**）。
3. ドメイン リストを作成します **([Configure] > [Security] > [Access Control] > [Domains])**。
   - ルール内でドメインを指定するためには、そのドメインがドメイン リストのメンバーでなければなりません。
   - IWA で使用する Active Directory ドメインは結合されていなければなりません。

   未知のユーザーの処理

重要

ルール ベースの認証では、Content Gateway は Web Security に知られていない（User Services プライマリ ドメインの外の）ユーザーを認証することがあります。この場合に Content Gateway が Web Security に知られている [別名] のユーザー名を送信するように設定できます。デフォルト ポリシーを適用する、つまり名前を送信しないように設定することもできます。ドメイン リスト内の各ドメインに対して、この指定を行うことができます。

詳細情報は、下の*未知のユーザーと [別名] オプション*を参照してください。

4. 認証ルールを作成します（**[Configure] > [Security] > [Access Control] > [Authentication Rules（認証ルール）]**）。
5. Content Gateway を再起動して、新しいルールを有効にします。

ルール ベース認証の最善の方法

- ルールが必要でない場合は、ルール ベースの認証を使用しない。単一の認証方法を配備すると最高のパフォーマンスが得られる。
- 要求を満たすために必要な最小限の数のルールを使用する。
- 必要でない場合は、ルール内でドメイン リストを使用しない。

ドメイン リストを使用する時

- IWA または NTLM ドメインがある場合は、それをリストの先頭にする。
- IWA または NTLM ドメインが 2 つ以上ある場合は、アクティブ メンバーの数が最も多いドメインをリストの先頭にする。つまり、最も頻繁にユーザーを認証するドメインを最初のドメインにする。
- IWA ドメインがリストの先頭になっていて、ユーザーがそのドメインに結合していない場合、そのユーザーは資格情報の入力を要求されます。
- リストの最初のドメインが LDAP である場合、ルールに一致するすべてのユーザーは資格情報の入力を要求されます。提供された資格情報がその後の各ドメインに提供されます。

未知のユーザーと [別名] オプション

ルール ベースの認証では、Content Gateway が認証したユーザーが、Web Security に転送された時に、その名前が User Services ディレクトリにないために認識されないことがあります。

認証されたユーザー名が Web Security にない場合、**デフォルト** ポリシーが適用されます。この問題を解決するには、いくつかの方法があります。

- Web Security User Services の設定を変更し、その名前を検出してそのディレクトリに追加できるようにする。
- 認識されない名前を Web Security のプライマリ ドメインに追加する。名前は正確に一致しなければなりません。新しい名前に対するポリシーを定義します。
- 特定の認証ルールに一致するユーザーについて、別名を Web Security に転送し、別名を Web Security のプライマリ ドメインに追加する。名前は正確に一致しなければなりません。別名に対するポリシーを定義します。
- 既存の Web Security のデフォルト ポリシーで十分な場合は、何もしないか、または特定のルールに一致する各ユーザーに対して、そのルールの中で空白の別名を使用することを選択します。

*ルール ベースの認証の使用例*にいくつかの具体例を示しています。

ルール ベース認証のドメイン リスト

Help | Content Gateway | バージョン 7.8.x

ルール ベースの認証を使用するには、**ドメイン リスト**を作成および保守しなければなりません。認証ルールを定義する前に、リストに少なくとも 1 つのドメインがなければなりません。

ドメインをリストに追加する時、認証方法が指定されます。

ルールを定義する時、ドメイン リストから 1 つまたは複数のドメインが選択されます。

サポートされるドメインには、下記のタイプが含まれます。

- IWA で使用する Active Directory (AD) ドメインこれらのドメインには Content Gateway、およびそのメンバー（ユーザー）が結合されていなければなりません。
- レガシー NTLM で使用する Domain Controllers (DC)
- LDAP で使用する AD および uid ドメイン コントローラおよびディレクトリ サービス

ドメイン指定の設定の要約

1. ルール ベース認証を有効にしなければなりません **([Configure] > [My Proxy] > [General])**。
2. **[Configure] > [Security] > [Access Control] [Domains] > タブで、**[New Domain（新規ドメイン）] **をクリックします。**
3. 認証方法の選択
4. ドメインとその目的がわかるような固有の名前を指定します。
5. 任意に、**Aliasing（別名）**オプションを設定します。
6. ドメインの設定を指定します。これは認証方法によって異なります。

下記を参照してください :

- *IWA で使用する Active Directory ドメインの追加*
- *レガシー NTLM で使用する NTLM ドメインの追加*
- *LDAP で使用するドメイン（ディレクトリ サービス）の追加*

IWA で使用する Active Directory ドメインの追加

IWA で使用する Active Directory (AD) ドメインには Content Gateway とディレクトリ メンバー（クライアント）の両方が結合されていなければなりません。

ドメインを結合するには、以下の手順を実行します。

- Content Gateway がドメイン名を解決できなければなりません。
- Content Gateway のシステム時刻がドメイン コントローラの時刻と ±1 分以内の誤差で同期化されていなければなりません。
- 正しいドメイン管理者名とパスワードを指定しなければなりません。
- ドメイン コントローラ（ポート 88、389、445）に対する TCP/UDP 接続が確立されていなければなりません。
- バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center (KDC) サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。

ドメインを指定し、結合するには、以下の手順を実行します。

1. **[Configure] > [Security] > [Access Control] [Domains] > タブで、**[New Domain（新規ドメイン）] **をクリックします。**
2. **[Authentication Method（認証方法）]** ドロップダウン ボックスから **[Integrated Windows Authentication]** を選択します。
3. **[Domain Identifier（ドメイン識別子）]** フィールドにドメインとその目的がわかるような固有の名前を入力します。
4. 任意に、**[Aliasing（別名）]** オプションを設定します。詳細については、*未知のユーザーと [別名] オプション、245 ページ*を参照してください。
5. **[Domain Name（ドメイン名）]** フィールドに完全修飾名を入力します。例、ad1.example.com。
6. **[Administrator Name]** フィールドに Windows Administrator のユーザー名を入力します。
7. **[Administrator Password]** フィールドに Windows Administrator のパスワードを入力します。

   名前とパスワードは結合時にのみ使用し、保存されません。
8. **ドメイン コントローラ**を見つける方法を選択します。
   - **DNS による自動検出**
   - **DC 名と IP アドレス**

     ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
9. **Content Gateway のホスト名**を確認します。

警告

ドメインを結合した後でホスト名を変更してはいけません。変更した場合、IWA はただちに作業を中止し、ドメインの結合を解除して、新しいホスト名で再結合するまで機能しません。

10. **[Join Domain]** をクリックします。

[Monitor（モニター）] > [Security（セキュリティ）] > [Integrated Windows Authentication] ページの **[Joined Domain Connections（結合したドメイン接続）]** セクションは、結合されたドメインおよび接続のリストを表示し、診断テスト機能を提供します。

トラブルシューティングのヒントは*ドメインを結合できない*に示しています。

ドメイン コントローラを見つける方法、および他の属性を変更するには、以下の手順を実行します

1. **[Domains]** ページのリストで変更するドメインを選択し、**[Edit]** をクリックします。
2. **[IWA Domain Details（IWA ドメイン詳細）]** のセクションで、ドメイン コントローラを見つける方法を選択します。
   - **DNS による自動検出**
   - **DC 名と IP アドレス**

     ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
3. **[Aliasing]** の設定を変更することもできます。*未知のユーザーと [別名] オプション*、245 ページを参照してください。
4. **[Apply]** をクリックします。

レガシー NTLM で使用する NTLM ドメインの追加

レガシー NTLM のサポートには以下の制限があります。

- **WINS 解決**はサポートされていません。ドメイン コントローラのホスト名は DNS サーバーが解決できる名前でなければなりません。
- **拡張セキュリティ**はサポートされておらず、ドメイン コントローラ上で有効化できません。
- **NTLM2 セッション セキュリティ**はサポートされておらず、クライアント上で有効化できません。Windows OS の [Security Settings（セキュリティ設定）] の領域で、**[Network Security: Minimum session security（ネットワーク セキュリティ：最小限のセッション セキュリティ）]** の設定を調べます。
- **NTLMv2** は Active Directory 2008 ではサポートされていません。
- すべてのブラウザが透過的 NTLM 認証をサポートするわけではありません。*ブラウザの制約*、219 ページを参照してください。

レガシー NTLM のサポートについての詳細な説明は、*レガシー NTLM 認証*、230 ページを参照してください。

ルール ベースの認証で使用する NTLM ドメインを追加するには、以下の手順を実行します。

1. **[Configure] > [Security] > [Access Control] [Domains] > タブで、**[New Domain（新規ドメイン）] **をクリックします。**
2. **[Authentication Method（認証方法）]** ドロップダウン ボックスから **[Legacy NTLM]** を選択します。

3. **[Domain Identifier（ドメイン識別子）]** フィールドにドメインとその目的がわかるような固有の名前を入力します。ドメインを追加した後、ドメイン名は変更できません。
4. 任意に、**[Aliasing（別名）]** オプションを設定します。詳細については、下記の項を参照してください。*未知のユーザーと [別名] オプション*、245 ページ。
5. **[Legacy NTLM Domain Details（レガシー NTLM ドメインの詳細）]** セクションで、
   a. **[Domain Controller（ドメイン コントローラ）]** 入力フィールドにプライマリ ドメイン コントローラの IP アドレスとポート番号を入力します。ポートが指定されていない場合、Content Gateway はポート 139 を使用します。

      カンマ区切り形式のリストでセカンダリ ドメイン コントローラを指定できます。下記の形式がサポートされています。

      host_name[:port][%netbios_name]

      IP_address[:port][%netbios_name]

      netbios_name は Active Directory 2008 では必須です。
   b. 複数 DC 間でロード バランシングを適用するかどうかを指定します。

> **注意**
> ロード バランスが**選択されていない**場合でも、複数のドメイン コントローラが指定されていて、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。

6. **[Add Domain（ドメインを追加）]** をクリックします。

LDAP で使用するドメイン（ディレクトリ サービス）の追加

LDAP を使用している時、

- Content Gateway は LDAP クライアントとして機能し、コンテンツを要求するユーザーに直接にユーザー名およびパスワードを要求します。
- ユーザー名とパスワードを受け取った後、Content Gateway は LDAP サーバーにコンタクトして、その資格情報が正しいかどうかを確認します。
- LDAP サーバーがユーザー名とパスワードを受け入れた場合、プロキシはクライアントに要求されたコンテンツを提供し、そのユーザー名とパスワードを資格情報キャッシュに保存します。

- その後のそのユーザーについての認証要求は、キャッシュ エントリの継続期間（TTL 値）が過ぎるまで、キャッシュ情報によって処理されます。
- LDAP サーバーがそのユーザー名とパスワードを拒否した場合、ユーザーのブラウザは認証が失敗したことを知らせるメッセージを表示し、再びユーザー名とパスワードの入力を要求します。

LDAP 認証は単純バインドと匿名バインドの両方をサポートします。

Domains リストに LDAP ドメインを追加するには、下記の手順を実行します。

1. **[Configure] > [Security] > [Access Control] [Domains] > タブで、**[New Domain（新規ドメイン）] **をクリックします。**
2. **[Authentication Method]** ドロップダウン リストから **[LDAP]** を選択します。
3. **[Domain Identifier（ドメイン識別子）]** フィールドにドメインとその目的がわかるような固有の名前を入力します。ドメインを追加した後、ドメイン名は変更できません。
4. 任意に、**[Aliasing（別名）]** オプションを設定します。詳細については、下記の項を参照してください。*未知のユーザーと [別名] オプション*、245 ページ。
5. **[LDAP Domain Details（LDAP ドメインの詳細）]** セクションで、
   a. **[LDAP Server Name（LDAP サーバー名）]** フィールドに LDAP サーバーの完全修飾ドメイン名または IP アドレスを入力します。
   b. LDAP サーバー ポートがデフォルト（389）以外のポートである場合、**[LDAP Server Port（LDAP サーバー ポート）]** フィールドに LDAP サーバー ポートを入力します。
   c. **LDAP ベース識別名**を入力します。この値は LDAP 管理者から取得します。
   d. ドロップダウン リストから **[LDAP Server Type（LDAP サーバー タイプ）]** を選択します。
      - Active Directory の **sAMAccountName** を選択します。
      - 他のディレクトリ サービスでは、**uid** を選択します。
   e. **[Bind Domain Name（バインド ドメイン名）]** フィールドにバインド識別名を入力します。これは LDAP ディレクトリ サービスのユーザーの完全識別名でなければなりません。例：

      CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM

   f. **[Bind Password（バインド パスワード）]** フィールドに **[Bind Domain Name]** フィールドで指定した名前に対応するパスワードを入力します。
   g. Content Gateway が LDAP サーバーとの間でセキュアな通信を使用するようにするには、**[Secure LDAP]** を有効にします。有効にした場合、LDAP ポードは 636 または 3269 に設定されます。
6. **[Add Domain（ドメインを追加）]** をクリックします。

ドメインの結合を解除する、またはドメインを Domain リストから削除するには、以下の手順を実行します

[Domains] ページのリストでドメインを選択し、**[Unjoin（結合解除）]** または **[Delete]** をクリックします。

確認ダイアログが表示されます。ドメインをリストから削除することを確認します。

警告

ドメインが削除されると、そのドメインはそれを指定している認証ルールからも削除されます。

それがルールで指定されている唯一のドメインである場合、ドメインが削除された時、ルールは無効となり、削除されます。

LDAP ルールの作成

Help | Content Gateway | バージョン 7.8.x

認証ルールを作成する前に、下記の処理を行う必要があります。

- **[Configure] > [My Proxy] > [Basic] > [General]** で **[Rule-Based Authentication（ルール ベースの認証）]** を有効にします。
- *グローバル認証オプション、220 ページ*を設定します。
- *ルール ベース認証のドメイン リスト、245 ページ*を作成します。

また、次の情報が必要です。

- ルールで指定するドメイン（1 つまたは複数）の名前これはドメインをドメイン リストに追加した時に指定された固有の名前です。
- ユーザーの一致基準。

  基準

  - IP アドレス — 個別のアドレス、またはアドレスの範囲を指定できます。
  - インバウンド プロキシ ポート（明示のプロキシのみ）
  - User-Agent 値
  - 上記の組み合わせ

ルールを作成するには、以下の手順を実行します。

> **注意**
> ルール エディタですべての指定子を入力した後、**[Add]** をクリックしてから **[Apply]** をクリックします。先に [Apply] をクリックした場合や、編集ウィンドウが閉じている場合は、すべてのエントリ フィールドが消去されます。
>
> ルールのサイズは 512 文字以内でなければなりません。

1. **[Configure] > [Security] > [Access Control]** に進み、**[Global Authentication Options（グローバル認証オプション）]** および **Domains** リストを検討および調整します。
2. IWA で AD ドメインを使用する場合、**[Monitor] > [Security] > [Integrated Windows Authentication]** へ進み、IWA ドメインが結合されていて、接続が確立していることを確認します。
3. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブに移動します。既存の認証 ルールのリストがページ上部に表示されます。
4. **[Edit File]** をクリックしてルール エディタを開きます。
5. すでにいくつかのルールが定義されている場合、ページの上部のリストでルールの順番を確認してください。

> **重要**
> ルールの順序が重要です。ルールの一致の検討は上から下へ順に行われます。最初に条件に一致したルールだけが適用されます。

6. ルールを追加し、Content Gateway を起動した後でルールをアクティブにするには、**[Status] [Enabled]** を選択します。
7. 一意な**ルール名**を入力します（必須）。短い、説明的な名前を指定すると、ルールとその目的を知るのに便利です。名前は 50 文字を超えないようにしてください。
8. ルールを特定の IP アドレスに適用する場合は、**[Source IP Addresses（ソース IP アドレス）]** フィールドに個別の IP アドレスおよび（または）IP アドレス範囲のカンマ区切り形式のリストを入力します。スペースは使用できません。例：

   10.4.1.1,10.12.1.1-10.12.254.254

   ソース IP アドレスの範囲に重なりがあってもかまいません。範囲の重なりは、大きなプールの中のサブグループをすばやく識別する手段として便利です。範囲の重なりの中では、最初の一致だけが使用されます。

   このフィールドが空白（未定義）である場合は、すべての IP アドレスが一致します。

9. ルールを特定のポート上の着信トラフィックに適用する場合、ドロップ ダウン リストからそのプロキシ ポートを選択します。このオプションは明示的プロキシの場合にのみ有効です。

   着信ポートは **[Configure] > [My Proxy] > [Protocols] > [HTTP] > [General]** ページの **[Secondary HTTP Proxy Server Ports（セカンダリ HTTP プロキシ サーバー ポート）]** フィールドで指定されます。要求を希望するポートへ送信するようにクライアント アプリケーションを設定しておかなければなりません。

   定義されていない場合は、すべてのポートが一致します。透過的プロキシ配備では、このフィールドを未定義にしておく必要があります。

10. ルールを特定の **User-Agent** 値に適用するには、希望する値に一致する POSIX 適合の正規表現 (regex) を入力します。共通ブラウザ タイプを指定するには、ドロップ ダウンリストから**定義済み**の regex を選択し、**[Include（含める）]** をクリックします。

    定義されていない場合は、すべての User-Agents が一致します。

    このフィールドを直接に編集できます。

    複数の regex を区切るために、“|” 文字（論理和）を使用します。

    regex の演算子 “^” はサポートされません。

    regex の検証はルールが設定ファイルへ提出された時（**[Add]** または **[Set]** をクリックしてから **[Apply] をクリックした後**）に行われます。**regex が有効でない場合、ルールは削除され、有効な regex を使って再作成しなければなりません。**

    詳しい説明と具体例を *User-Agent をベースとする認証*、258 ページに示しています。

11. 認証の基準となるドメインを指定します。

    a. **[Domains]** ドロップダウン リストからアプリケーション ドメインを選択し、**[Include]** をクリックします。**Domains** リストに追加されているドメインのみが利用可能です（リストへの追加には **[Configure] > [Security] > [Access] [Control] > [Domains]** タブを使用します）。

    b. 順序を指定したドメインのリストを使用する場合、各ドメインを 1 つずつ選択して **[Include]** をクリックします。次にリストでドメインを選択し、上 / 下矢印を使用して順序を変更します。

    > **重要**
    >
    > [*Fail Open*/fail closed（フェイル オープン / フェイル クローズ）] の設定はリスト内のすべてのドメインを調べた後で適用されます。

12. **[Add]** をクリックしてルールを追加します。

13. ページ上部で、ルール リストの中でのそのルールの位置をチェックし、調整します。最初に条件に一致したルールが適用されます。

14. **Apply** をクリックしてから、ルールを有効にするために Content Gateway を再起動します。

> **警告**
> ルールに無効な値がある場合、無効なルールを示した警告メッセージが表示されます。ルールはファイルには書き込まれません。

既存の認証ルールの使用

Help | Content Gateway | バージョン 7.8.x

Content Gateway manager のルール エディタを使用します。auth_rules.config を直接に編集しないでください。

ルールの編集

1. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで、**[Edit File]** をクリックします。
2. ルールのテーブルで、変更するルールをクリックします。その値が定義領域のフィールドに入力されます。
3. 変更を行った後、**[Set]** をクリックし、次に **[Apply]** をクリックします。

> **重要**
> フィールドの値が有効でない場合、ルールは提出されず、ルール エントリは廃棄されます。ルールを再作成する手間を少なくするために、フィールド値を別途に記録しておくと、不適切なフィールド値を訂正するだけで簡単にルールを再作成できます。

4. **[Close]** をクリックして **[Authentication Rules]** タブに戻り、**[Refresh（更新）]** をクリックして更新されたリストを表示します。
5. 変更を有効にするために、Content Gateway を**再起動**します。

ルールのリストの順序変更

認証ルールはリストの中の上から順にマッチングされます。最初に条件に一致したルールだけが適用されます。

1. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで、**[Edit File]** をクリックします。
2. ルールのテーブルで、位置を変更するルールをクリックし、次に左側の下向きまたは上向き矢印をクリックすることによってこのルールの位置を変更します。
3. ルールが希望する位置に置かれたとき、**[Apply]** をクリックします。

4. **[Close]** をクリックして **[Authentication Rules]** タブに戻り、**[Refresh（更新）]** をクリックして更新されたリストを表示します。
5. 変更を有効にするために、Content Gateway を**再起動**します。

ルールの削除

1. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで、**[Edit File]** をクリックします。
2. ルールのテーブルで、削除するルールをクリックして、左側の "X" ボタンをクリックします。
3. ルールの削除を完了したとき、**[Apply]** をクリックします。
4. **[Close]** をクリックして **[Authentication Rules]** タブに戻り、**[Refresh（更新）]** をクリックして更新されたリストを表示します。
5. 変更を有効にするために、Content Gateway を**再起動**します。

ルール ベースの認証の使用例

Help | Content Gateway | バージョン 7.8.x

複数レルムの使用例 1：ドメイン取得済み、明示的プロキシ、255 ページ

複数レルムの使用例 2：内部ドメイン追加、明示的プロキシ、256 ページ

複数レルムの使用例 3：一時ドメイン追加、透過的プロキシ、257 ページ

User-Agent をベースとする認証、258 ページ

複数レルムの使用例 1：ドメイン取得済み、明示的プロキシ

この例では、既存の単一ドメイン環境にもう 1 つのドメインが追加されます。Content Gateway は明示のプロキシで、クライアントは PAC ファイルを使用します。

ある組織 — [Quality Corp] という名前であると仮定します - は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (QCORP) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

Quality Corp は New Corp を取得しました。New Corp は独自のドメイン (NCORP) とドメイン コントローラを持っています。New Corp は LDAP を使用してユーザーを認証します。

Quality Corp は両者の従業員を 1 つのドメインで管理したいと考えていますが、インフラストラクチャーの変更を行う用意はありません。その用意が整うまで、New Corp ユーザーには別の使用ポリシーを適用する（つまり、QCORP ドメインの [デフォルト] ユーザーを使用しない）ことを希望しています。

ルール ベース認証によってそれが可能になります。

この解決策を設定するために、Quality Corp は次のことを行います。

1. ルール ベースの認証を有効にします。
2. 2 番目の、デフォルト以外の HTTP ポートを追加します (**[Configure] > [Protocols] > [HTTP] > General**)。このポートは NCORP のすべてのメンバーが使用します。
3. NCORP のメンバーが新しい、2 番目のポートを通じて Content Gateway に接続するようにする PAC ファイルを作成します。
4. 認証ルールを、QCORP ドメインと NCORP ドメインのそれぞれのために 1 つずつ作成します。
   a. **[Configure] > [Security] > [Access Control] > [Domains]** タブで、Domains リストに QCORP および NCORP ドメインを追加します。
      - **NCORP を追加する時、[Aliasing] オプションを使用してポリシーの決定に使用する [NCorpUser] を指定します。**
   b. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで、2 番目のポート上の接続のための NCORP ルールを作成します。New Corp ユーザーの IP アドレス / 範囲がわかっている必要があり、また、NCORP ドメインを指定しなければなりません。
   c. 他のすべての接続を処理する QCORP ルールを定義します。
5. Web Security manager で [NCorpUser] を QCORP ドメインに有効なユーザーとして追加し、そのユーザーのためのポリシーを作成します。

これによって、NCORP から Content Gateway に接続するすべてのユーザーが NCORP ドメイン コントローラに対して認証され、NCorpUser に関連付けられているグループ ポリシーを適用されます。このシナリオでは、個別ユーザー ベースのポリシーまたは機能（例、割り当て時間）は処理できません。トランザクションは NCorpUser としてログ記録されます。これはすべて、QCORP ドメインのユーザーの認証、ポリシー、ログ記録にはどんな影響も及ぼしません。

複数レルムの使用例 2：内部ドメイン追加、明示的プロキシ

この例では、既存の単一ドメイン環境にもう 1 つのドメインが追加されます。Content Gateway は明示のプロキシで、クライアントは PAC ファイルを使用します。

ある組織 — [BigStars] という名前であると仮定します - は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (BIG) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

会社内の 1 つのグループが Apple コンピュータに切り替えますが、Apple コンピュータは NTLM では認証できません。IT グループは LDAP サーバーをインストールし、Apple ユーザーのために新しいドメイン [BIGAPL] を作成します。

このユーザーのグループは以前に存在しており、プライマリ ドメイン (BIG) 上で管理されていましたから、IT 部では、ユーザー ベースのポリシーとログ記録の両方が依然として適用されると想定しています。

ルール ベースの認証の機能によってそれが可能になります。

この解決策を設定するために、BigStars は次のことを行います。

1. BIGAPL のすべてのユーザーが BIG にも存在し、正確に同じユーザー名を割り当てられていることを確認します。
2. ルール ベースの認証を有効にします。
3. 2 番目の、デフォルト以外の HTTP ポートを追加します **([Configure] > [Protocols] > [HTTP])**。このポートは BIGAPL のすべてのメンバーが使用します。
4. BIGAPL のメンバーが新しい、2 番目のポートを通じて Content Gateway に接続するようにする PAC ファイルを作成します。
5. 認証ルールを、BIGAPL ドメインと BIG ドメインのそれぞれのために 1 つずつ作成します。
   a. **[Configure] > [Security] > [Access Control] > [Domains]** タブで、Domains リストに BIGAPL および BIG ドメインを追加します。
   b. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで、2 番目のポート上の接続のための BIGAPL ルールを作成します。
   c. 他のすべての接続を処理する BIG ルールを定義します。

これによって、BIGAPL のすべてのメンバーは LDAP によって認証されますが、それらの既存の NTLM ID によって指定されている個別のポリシーが引き続き適用されます。ログおよびレポートもその同じユーザーを参照します。

複数レルムの使用例 3：一時ドメイン追加、透過的プロキシ

この例では、既存の単一ドメイン環境にもう 1 つの、特別の目的を持つドメインが追加されます。Content Gateway は WCCP v2 を使用する透過的プロキシです。

ある組織 — [Creative Corp] という名前であると仮定します - は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (CCORP) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

Creative Corp は、新製品を発売し、躍進を遂げたいと考えています。この会社はキオスク、デモンストレーション、プレゼンターを揃えたオープン ハウスを設立することを決定しました。キオスクは、新製品の適切なデモンストレーションのために、デフォルトのインターネット ポリシーのみを必要としています。IT マネージャはキオスク ネットワークを可能な限り社内イントラネットから隔離したいと考えています。このシナリオでは、個別ユーザーのログ記録は必須要件ではありません。

ルール ベースの認証の機能によってそれが可能になります。

この解決策を設定するために、Creative Corp は次のことを行います。

1. 独自のドメイン コントローラを備えた新しい、一時的なネットワークを構築します。これを [CTEMP] ドメインと名付けます。
2. CTEMP に 1 人または複数のユーザーを追加します。これらのユーザーはプライマリ ドメイン上の既存のユーザーと 1 対 1 で対応させるか、または、プレゼンターが使用する 1 つ以上の一般ユーザーとして指定することができます。
3. CTEMP 上のトラフィックを WCCP v2 が使用されている Content Gateway へリダイレクトします。
4. ルール ベースの認証を有効にします。
5. 認証ルールを、CTEMP ドメインと CCORP ドメインのそれぞれのために 1 つずつ作成します。
    a. **[Configure] > [Security] > [Access Control] > [Domains]** タブで、CTEMP ドメインを追加し、Aliasing を有効にし、名前フィールドを空白にしておきます。これによってデフォルト ポリシーが CTEMP のすべてのユーザーに適用されます。
    b. CCORP ドメインをドメイン リストに追加します。
    c. **[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブで CTEMP ドメインに割り当てられている IP アドレス範囲から着信するすべての接続に適用する CTEMP ルールを定義します。
    d. 他のすべての接続を処理する CCORP ルールを定義します。

これによって、いずれかのキオスク上でインターネットを使用しているユーザーは CTEMP ネットワークに対して認証され、要求に対してデフォルト ポリシーが適用されます。

User-Agent をベースとする認証

認証ルールの中で、要求ヘッダの User-Agent 値を使用して、ユーザー認証を実行するかどうかを決定できます。これは既知のクライアント アプリケーションのセット - 通常はブラウザ - を使用するユーザーの認証を実行し、他のアプリケーション - 多くの場合、認証をサポートしないアプリケーションのセット - には認証なしに続行を許可する場合に便利です。また、このようなルールでは IP アドレスと（Content Gateway が明示的プロキシである場合）着信プロキシ ポートを指定することもできます。

他のすべての認証ルールと同様に、最初に一致したルールが適用されます。（ルール ベースの認証の詳細は、*ルール ベースの認証*、239 ページを参照してください）。

[User-Agent] フィールドを使用する時、クリティカルな要素はマッチングを実行する正規表現 (regex) です。

- regex は POSIX に適合している必要があります。
  - regex の演算子 “^” はサポートされません。
- 一般的に使用される大部分のブラウザには、定義済みの regex が提供されます。
- このフィールドが空白である場合は、すべての User-Agent 値が一致します。
- このフィールドを直接に編集することによってカスタム regex を作成できます。
- 複数の regex を使用できます。それらは “|”（‘or’ 演算子）で区切る必要があります。

[Apply] をクリックしたとき（[Add] または [Set] の後で）、regex が解析および検証されます。**regex が有効でない場合、ルールは削除され、有効な regex を使って再作成しなければなりません**。

以下はカスタム regex の例です。

Microsoft Internet Explorer 8、9、または 9

```
MSIE ([7-9]{1}[\.0-9]{0})
```

User-Agent 文字列の例

```
Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)
```

Microsoft Internet Explorer Mobile（全バージョン）

```
IEMobile
```

User-Agent 文字列の例

```
Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5;
Trident/5.0; IEMobile/9.0)
```

Apple iPhone（全バージョン）

```
(iPhone)OS (\d+)_(\d+)(?:_(\d+))?
```

User-Agent 文字列の例

```
Mozilla/5.0 (iPod; U; CPU iPhone OS 4_3_3 like Mac OS X;
ja-jp)AppleWebKit/533.17.9 (KHTML, like Gecko) Version/
5.0.2 Mobile/8J2 Safari/6533.18.5
```

Apple iPad（全バージョン）

```
(iPad).+ OS (\d+)_(\d+)(?:_(\d+))?
```

User-Agent 文字列の例

```
Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/
536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5355d
Safari/8536.25
```

User-Agent 文字列のリスト、正規表現の例、regex チェッカーおよび関連リソースはインターネットで検索してください。

使用例

この例では、単一ドメイン環境の組織が一般的に使用されている 2 つの web ブラウザからの要求を認証する方法を示します。この組織はまた、認証をサポートしない web アプリケーションの認証をバイパスすることを希望しています。

ある組織 — [Best Corp] という名前であると仮定します — は Content Gateway を使用しています。この組織には 1 つのドメイン (BCORP) と 1 つのドメイン コントローラがあります。この組織は IWA を使用してユーザーを認証します。

Best Corp は下記のような構成を希望しています。

- 一般的に使用されている web ブラウザからの要求を認証する。どの web ブラウザが組織のコンピュータ上で許可されるかを管理できる。
- 認証をサポートしない web アプリケーションが認証をバイパスする。

ルール ベースの認証の User-Agent 機能によってそれが可能になります。

この解決策を構成するために、Best Corp は次のことを行います。

1. ルール ベースの認証を有効にします。
2. BCORP ドメインをドメイン リストに追加します。
3. 下記の IWA ルールを作成します。
   a. オプションとして、サポートされるクライアント IP アドレス範囲を指定する。
   b. User-Agent 値によって、認証する web ブラウザを指定する。

      [User-Agent] フィールドで、**事前定義済みの**ドロップ ダウン リストを使用して Internet Explorer および Firefox を選択し、**追加**します。regex は次のようになります。

      ```
      MSIE*|Firefox*
      ```

これで完了です。この構成では、組織のコンピュータ上にインストールできるブラウザは Internet Explorer と Firefox の 2 つだけであり、それらはユーザー認証の対象となります。他のすべての要求 - 特に web アプリケーション — は認証をバイパスします。この構成をさらにカスタマイズするために、Best Corp は他の認証ルールを作成したり、プロキシ フィルタリング ルールを追加する (filter.config) ことによって User-Agent に基づいて特定のアプリケーションを拒否またはバイパスすることもできます。

認証ルールのトラブルシューティング

Help | Content Gateway | バージョン 7.8.x

ルール ベースの認証では、下記のような問題がしばしば発生します。

- ユーザーに対して認証を要求するべき時に、資格情報の入力が*要求されない*。
- ユーザーに対して認証を要求する必要がない時に、資格情報の入力が*要求される*。

- ユーザー認証が間違ったドメインに対して行われる。

これらの問題は、ユーザー認証プロセスの下記のいずれかの段階において発生します。

- 一般的なユーザー認証ロジック（下記を参照）
- ルールの定義と照合
- ユーザー認証プロトコル処理（IWA、NTLM、LDAP、IWA のトラブルシューティングについては*統合 Windows 認証のトラブルシューティング*を参照）

ルール ベース認証のロジック

ルール ベースの認証は、以下のロジックを適用します。

1. **filter.config** 内のルールがチェックされ、適用されます。このアクションは、すべてのタイプの Content Gateway ユーザー認証の最初のステップとして行われます。適合するフィルタリング ルールが見つかった場合、そのルールが適用され、ユーザー認証プロセスは終了します。*フィルタリング ルール、206 ページ*を参照してください。
2. 適合するフィルタリング ルールが見つからない場合、ユーザー認証ルールの照合が実行されます。
   a. 要求の IP アドレスが、ルール セットに対して、上から順に照合されます。
   b. IP アドレスに適合するルールが見つかった場合、ソース ポートがチェックされます。
   c. IP アドレスに適合するルールが見つかった場合、User-Agent 値がチェックされます。
   d. 最初に条件に一致したルールが適用されます。**条件に一致するルールがない場合、認証の試みは行われません。**
3. 適合するルールが見つかった場合、指定されたドメインに対して指定された認証プロトコルが適用されます。すべてのルール設定の詳細が適用されます。
4. ユーザーが認証された場合、要求は処理されるか、または Web Security ポリシーによって拒否されます。
5. このトランザクションはログに記録されます。

ロジックが実行環境にどのように適用されるかを調べるために、一時的にユーザー認証デバッグ出力を有効化することができます。デバッグ出力は、特に、ルールの解析と照合の詳細を示します。*ユーザー認証デバッグ出力の有効化と無効化*を参照してください。

トラブルシューティング

ルール ベースの認証が所期の結果をもたらさない場合、以下の順序でトラブルシューティングを実行することを推奨します。

1. **ネットワーク アドレス変換 (NAT) をチェックする**

   想定外の IP アドレスの NAT が行われていないことを確認します。ネットワーク アドレス変換を行うと、ユーザー認証が実行される前に元のソース IP アドレスが別のアドレスに変更されます。Content Gateway Manager で **[Configure] > [Networking] > [ARM] > [General]** を選択し、**ipnat.config** の中のルールを調べます。ネットワーク内の他のデバイス、たとえばダウンストリームのプロキシやファイアウォールによってアドレスのネットワーク アドレス変換が行われることもあります。

2. **filter.config 内のルールのチェック**

   想定外の **filter.config** ルールとの一致がないことを確認します。filter.config ルールは、特に、ユーザー認証を迂回するために使用することができます。*フィルタリング ルール*を参照してください。

3. **ルールの一致のチェック**

   想定に反して認証が要求された、または認証が要求されなかったユーザーの IP アドレスを使用して、各ルールを上から順に調べ、その設定が条件に一致している最初のものを見つけます。この分析は、細部まで慎重に行ってください。よくある問題は、その IP アドレスを含む IP アドレス範囲が広すぎることです。

   ルールが別名を使用している場合、その別名がプライマリ ドメイン コントローラの User Service の中にあることを確認します。

   特定のポートにトラフィックを送信するように設定されている明示のクライアントについては、クライアントのブラウザのルールと設定の両方をチェックします。

4. **ドメインのチェック**

   想定している一致するドメインが見つかった場合、そのドメインがアクセス可能であり、そのユーザーがそのドメインのメンバーであることを確認します。それが確認された場合、認証プロトコル レベルの問題のトラブルシューティングを行います。IWA については*統合 Windows 認証のトラブルシューティング*を参照してください。

5. **Content Gateway がプロキシ チェーンの中にある場合**

   Content Gateway がプロキシ チェーンのメンバーである場合、[X-Forwarded-For] ヘッダーがダウンストリーム プロキシによって送信され、Content Gateway によって読み取られることを確認します。

   - パケット スニファーを使ってダウンストリームのプロキシからのインバウンド パケットを検査します。適切な形式の [X-Forwarded-For] ヘッダーを探します。
   - Content Gateway Manager で、**[Configure] > [My Proxy] > [Basic]** を選択し、ページの最下部までスクロールし、**[Read authentication from child proxy（子プロキシからの認証の読み取り）]** を有効化します。有効化されていない場合は **[On]** を選択し、**[Apply]** をクリックし、次に Content Gateway を再起動します。

ユーザー認証デバッグ出力の有効化と無効化

警告
デバッグ出力を有効化したままにしてはいけません。デバッグ出力はプロキシのパフォーマンスを低下させ、ファイル システムをログ出力でいっぱいにしてしまいます。

デバッグ ログ情報は下記のファイルに書き込まれます。**/opt/WCG/logs/content_gateway.out**

ユーザー認証デバッグ情報を有効化するには、下記のファイルを編集します。**/opt/WCG/config/records.config**

```
(root)# vi /opt/WCG/config/records.config
```

以下のパラメータを見つけ、変更して、下記のように値を割り当てます。

```
CONFIG proxy.config.diags.debug.enabled INT 1
CONFIG proxy.config.diags.debug.tags STRING
   http_xauth.* | auth_* | winauth.* | ldap.* | ntlm.*
```

ファイルを保存して、閉じます。下記のコマンドによって、Content Gateway がファイルを再読み込みするように指示します。

```
(root)# /opt/WCG/bin/content_line -x
```

tail -f コマンドによってデバッグ情報のフローを追跡します。

```
(root)# tail -f /opt/WCG/logs/content_gateway.out
```

Ctrl+C を使用してコマンドを終了します。

必要なデバッグ出力の収集が完了したとき（1 つ以上のユーザー認証プロセスを完了した後）、**records.config** を編集して、パラメータ値を下記のように変更することによってデバッグ出力を無効化します。

```
(root)# CONFIG proxy.config.diags.debug.enabled INT 0
```

ファイルを保存して、閉じます。下記のコマンドによって、Content Gateway がファイルを再読み込みするように指示します。

```
(root)# /opt/WCG/bin/content_line -x
```

Mac および iPhone/iPad 認証

Websense Web Security ソリューションは、ユーザーまたはグループ ベースのフィルタリングで Mac および iPhone/iPad ユーザーを認証または識別することができます。

Mac コンピュータについては、下記を参照してください。

- *Mac コンピュータの認証*
  - *DC Agent による Mac ユーザーの透過的識別の有効化*
  - *Content Gateway による Mac ユーザーの認証*
    - *Mac を Active Directory ドメインに結合するための一般的なステップ*

iPhone/iPad については、下記を参照してください。

- *iPhone および iPad の認証*

Mac および iPhone/iPad 認証について、よく尋ねられる質問のリストを How do I use Websense Web Security solutions to authenticate or identify Mac users for user- or group-based filtering?（Websense Web Security ソリューションを使用して、ユーザーまたはグループ ベースのフィルタリングで Mac ユーザーを認証または識別する方法）に示しています。

Mac コンピュータの認証

Web Security ソリューションは、ユーザーまたはグループ ベースのフィルタリングで Mac ユーザーを認証または識別することができます。以下の制限が適用されます。

- 認証および識別のためには、ユーザーが Active Directory に属している必要があります。
- プロトコル ブロック メッセージは Mac コンピュータでは表示されません。
- Mac OS X システム上では Websense Remote Filtering Client および Web Endpoint はサポートされません。

ユーザーの組織が透過的ユーザー識別のために DC Agent を使用している場合、*DC Agent による Mac ユーザーの透過的識別の有効化*を参照してください。

ユーザーの組織がユーザー認証のために Content Gateway を使用している場合、*Content Gateway による Mac ユーザーの認証*を参照してください。

Mac ユーザーのユーザーおよびグループ ベースのフィルタリングを可能にするために手動の（プロンプト方式の）認証を使用することもできます。

DC Agent による Mac ユーザーの透過的識別の有効化

DC Agent が Mac ワークステーション上でユーザーを識別するためには、Mac はドメイン コントローラ上でファイル共有をマウントしなければなりません。そのためには、Mac がドメイン コントローラ マシン上のファイル共有をユーザーのホーム ディレクトリとして使用するように構成するか、またはドメイン コントローラとの間で別の共有をマウントします。

> **注意**
> Mac がドメインにログするだけで、ファイル共有をマウントしない場合、DC Agent には認識されません。

設定のまとめ

- 関係する各 Mac ユーザーが共通の Active Directory のメンバーであることを確認します。Active Directory のマニュアルを参照してください。
- 各 Mac ユーザーのホーム フォルダを作成し、それがユーザーからアクセス可能であることを確認します。このセクションの最初の段落を参照してください。

ユーザーが適切に構成された Mac OS X システムにログオンすると、Mac はネットワーク ディレクトリをユーザーのホーム ディレクトリとしてマウントし、DC Agent のユーザー マップにデータが入力され、ユーザー要求に対してユーザーおよびグループ ベースのポリシーを適用できるようになります。要求がブロックされた時、通常通りにブラウザ ベースのブロック ページが表示されます。

Content Gateway による Mac ユーザーの認証

Mac ユーザーが Active Directory ドメインのメンバーであり、Mac コンピュータが Active Directory ドメインに結合されている場合、Content Gateway の Integrated Windows Authentication (IWA) 機能を使用してこのユーザーを透過的に認証することができます。詳細については、*統合 Windows 認証*を参照してください。

設定のまとめ

- 各 Mac コンピュータが Active Directory ドメインに結合していることを確認します。*Mac を Active Directory ドメインに結合するための一般的なステップ*を参照してください。
- 関係する各 Mac ユーザーが共通の Active Directory のメンバーであることを確認します。Active Directory のマニュアルを参照してください。
- Content Gateway が Active Directory ドメインに結合していることを確認します。
  - Content Gateway が IWA 用に構成されていない場合、*統合 Windows 認証*を参照し、構成についての指示に従ってください。
  - Content Gateway がすでに IWA 用に構成されていて、Mac ユーザーが現在の結合されているドメインに属している場合、何もすることはありません。
  - Content Gateway がすでに IWA 用に構成されていて、Mac ユーザーが異なる Active Directory ドメインに属している場合、ルールベースの認証の機能を使用します。*ルール ベースの認証*を参照して、構成についての指示に従ってください。

- Content Gateway が明示的プロキシである場合、関係する Mac システムおよびブラウザが Content Gateway の Fully Qualified Domain Name (FQDN) に HTTP、HTTPS および FTP 要求を送信するように構成します。または、NTLM で十分である場合は、Content Gateway の IP アドレスを指定します。

  Content Gateway が透過的プロキシである場合、Mac システムまたはブラウザの追加的設定は必要ありません。

重要

Safari ユーザーは、初めてブラウザを開いた時、資格情報の入力を求められることがあります。ユーザーは自分の資格情報を入力し、[Remember password in keychain（キーチェインにパスワードを記憶する）] チェックボックスをオンにする必要があります。

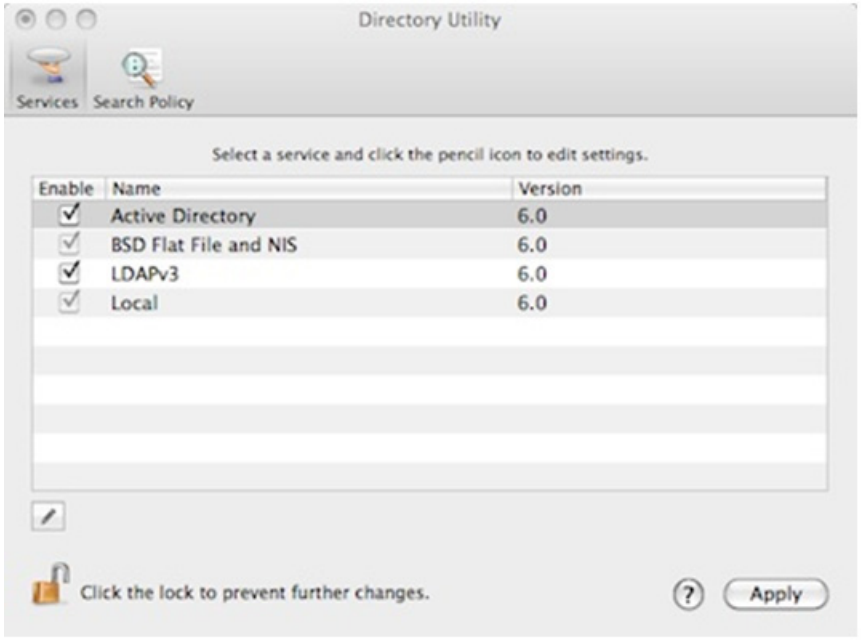
FireFox ユーザーに [Proxy Authentication Required（プロキシ認証が要求されます）] というエラー メッセージが表示される場合があります。これは FireFox (http://support.mozilla.org/en-US/questions/926378) の既知の問題であり、ブラウザの設定変更によって簡単に是正されます。**[About:Config]** で、下記のオプションを **false** に設定します。

- network.automatic-ntlm-auth.allow-proxies
- network.negotiate-auth.allow-proxies

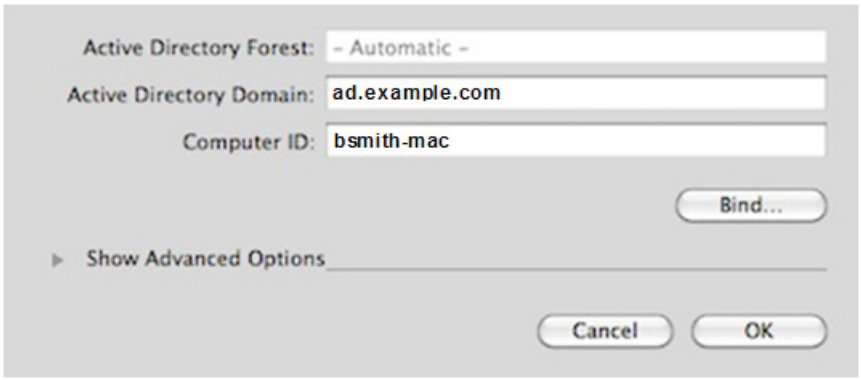
Mac を Active Directory ドメインに結合するための一般的なステップ

1. Administrator 権限を持つアカウントを使用して、Active Directory に結合する Mac コンピュータにログオンします。
2. **Directory Utility** を開きます。OS X 10.6 (Snow Leopard) 上で、下記へ進みます。

   /System/Library/CoreServices
3. 必要な場合、錠のアイコンをクリックし、パスワードを入力して Directory Utility のロックを解除します。
4. **[Active Directory]** の横のボックスを選択して、Active Directory のサポートを有効にします。



5. Active Directory をハイライト表示し、ペンシル アイコンをクリックして Active Directory 接続を構成します。
6. **[Domain]** の下に完全修飾ドメイン名 (FQDN) を入力します。
7. **[Computer ID]** の下にコンピュータ名を入力します。



8. [Bind（バインド）] をクリックします。ネットワーク資格情報とコンピュータ OU の入力を要求されます。OU 管理者アカウントとパスワード、およびコンピュータ OU の場所を入力します。例：

   ou=computers,ou=orgunits,dc=ad,dc=example,dc=com

   ユーザーのコンピュータが指定した Active Directory に結合されます。
9. Directory Utility で **[Apply]** をクリックして変更を保存し、次にコンピュータを再起動します。

iPhone および iPad の認証

プロキシ ベースのユーザー認証が Web Security Gateway および Web Security Gateway Anywhere の Content Gateway（proxy）コンポーネントによってサポートされており、それによってユーザーまたはグループ ベースのフィルタリングが行われます。

DC Agent によるユーザー識別はサポートされていませんから、Web Filter または Web Security ではユーザーまたはグループ ベースのフィルタリングのソリューションはありません。これらのデバイスには、フィルタリングは IP アドレスまたはネットワーク範囲をベースに提供できます。

Content Gateway のユーザー認証には、以下の機能と制限があります。

- Content Gateway で設定された認証方法を使用できます。ユーザーは関連付けられているユーザー ディレクトリに属している必要があります。
- Safari ブラウザをサポートします。他のブラウザは期待通りに機能しないことがあります。
- 透過的認証はサポートされていません。ユーザーは常に資格情報を求められます。
- 透過的および明示的 Content Gateway 配備で機能します。
- 多くの iPhone および iPad アプリケーションは Content Gateway（および他の Web プロキシ）で適切に機能しません。なぜなら、プロキシ ユーザー認証を処理するように適切にプログラムされていないからです。

明示的プロキシ設定は、iOS のネットワーク設定エリアで設定できます。


AT&T
4:08 PM
Not Charging
Settings
Airplane Mode
OFF
Wi-Fi
Websense
Location Services
On
Cellular Data
Brightness & Wallpaper
Picture Frame
General
Mail, Contacts, Calendars
Safari
iPod
Video
Photos
Notes
Store
Wi-Fi Networks
Websense
Forget this Network
IP Address
DHCP
BootP
Static
IP Address
10.64.143.154
Subnet Mask
255.255.255.0
Router
10.64.143.254
DNS
10.8.0.85, 10.8.0.84
Search Domains
websense.com
Client ID
Renew Lease
HTTP Proxy
Off
Manual
Auto
Server
10.203.136.21
Port
8080
Authentication
ON
Username
chris-wcgdev\administrator
Password

15 ログ ファイルの使用

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *イベント ログ ファイル*、272 ページ
- *イベント ログ ファイルの管理*、274 ページ
- *イベント ログ ファイルのフォーマット*、276 ページ
- *イベント ログ ファイルの取り込み*、284 ページ
- *イベント ログ ファイルの分割*、287 ページ
- *イベント ログ ファイルの照合*、289 ページ
- *ログ記録統計情報の表示*、293 ページ
- *ログ ファイルの表示*、294 ページ
- *イベント ログ ファイル エントリの例*、295 ページ

Websense Content Gateway には 3 種類のログ ファイルがあります：

- *システム ログ ファイル*はシステム情報を記録しますが、これは Content Gateway の状態に関するメッセージと Content Gateway によって出されたエラーや警告を含んでいます。この情報には、イベント ログ ファイルが取り込まれたというメッセージ、クラスタ通信がタイムアウトになったという警告、および Content Gateway が再起動されたことを示すエラーが含まれます。（Content Gateway は、エラー状態に関するアラームを Content Gateway manager に転送します。詳細については、*アラームの処理*、139 ページを参照してください。）

  すべてのシステム情報メッセージは、デーモン機能のもとでシステム全体のログ機能 **syslog** によってログ記録されます。**syslog.conf** 設定ファイル（**/etc** directory に保存されています）で、これらのメッセージがログ記録される場所が指定されます。通常の場所は **/var/log/messages** です。

  syslog プロセスはシステム全体を対象にして動作するので、このプロセスはすべての Content Gateway プロセス（これは **content_gateway**、**content_manager**、および **content_cop** を含みます）によるメッセージを記録する単一のレポジトリになっています。

ログ中の各ログ エントリは、エラーがログ記録された日時、エラーをレポートしたプロキシ サーバーのホストネーム、およびエラーまたは警告の説明についての情報を保持しています。

Content Gateway によってログ記録されるシステム情報メッセージのリストについては、*Websense Content Gateway のエラー メッセージ*、563 ページを参照してください。

- *エラー ログ ファイル*は、トランザクションがエラーになった理由に関する情報も記録します。
- *イベント ログ ファイル*（*アクセス ログ ファイル*ともいいます）は、Content Gateway が処理した各トランザクションの状態に関する情報を記録します。

Content Gateway はエラーおよびイベントの両ログ ファイルを作成し、システム情報をシステム ログ ファイルに記録します。イベント ログ記録とエラー ログ記録の両方またはいずれか一方を無効にすることができます。ピーク時にはエラーのログ記録だけにするか、またはログ記録を無効にすることをお勧めします。

▶ **[Configure（設定）] > [Subsystems（サブシステム）] > [Logging（ログ記録）]** タブで、次のようなオプションのいずれかを選択します：**[Log Transactions and Errors（トランザクションとエラーのログ記録）]**、**[Log Transactions Only（トランザクションだけのログ記録）]**、**[Log Errors Only（エラーだけのログ記録）]**、または **[Disabled（無効）]**。

イベント ログ ファイル

Help | Content Gateway | バージョン 7.8.x

イベント ログ ファイルは、Websense Content Gateway が処理するあらゆる要求についての情報を記録します。ログ ファイルを分析することによって、プロキシを利用しているユーザーの数、各ユーザーが要求している情報量、非常に人気があるページ、等々について調べることができます。

Content Gateway はいくつかの標準ログ ファイル フォーマット（例、Squid、Netscape）とユーザー定義カスタム フォーマットをサポートしています。標準フォーマットのログ ファイルを既製の分析パッケージを使って分析できます。ログ ファイルを分割し、各ファイルがプロトコルまたはホスト固有の情報を含むようにしておくと、ログ ファイルの分析が容易になります。また、ログ ファイルを特定の時間間隔で自動的に取り出すように Content Gateway を構成することもできます。

以下の各セクションでログ ファイルの取り扱いについて説明しています：

- イベント ログ ファイルの管理

  ログ ファイルを保存する集中的場所、ログ ファイルのためのディスク スペース、およびログ ファイルを取り出す回数と時刻について設定することができます。*イベント ログ ファイルの管理*、274 ページを参照してください。

- 種々のイベント ログ ファイル フォーマットの選択

  トラフィック分析で使用する標準ログ ファイル フォーマットを選択できます（例、Squid、Netscape）。あるいは、XML ベースの Content Gateway カスタム フォーマットを使用すると、ログ ファイルで記録する情報の種類をより細かに管理することができます。*イベント ログ ファイルのフォーマット*、276 ページを参照してください。

- イベント ログ ファイルの自動的な取り出し

  1 日のうち特定の時間間隔でイベント ログ ファイルを自動的に取り出すように Content Gateway を構成することができ、これによってアクティブでないログ ファイルを取り扱えるようになります。*イベント ログ ファイルの取り込み*、284 ページを参照してください。

- ホストごとの個別のログ ファイル

  異なるプロトコルの個別のログファイルをホスト ベースに作成するようにプロキシを構成することができます。*イベント ログ ファイルの分割*、287 ページを参照してください。

- 異なるノードのログ ファイルの照合

  ネットワーク上の 1 つ以上のノードをログ照合サーバーとして機能するように指定することができます。これらのサーバーはスタンドアローンまたは Content Gateway の一部のどちらでもよく、照合サーバーによってすべてのログ記録情報を適切に定義された場所で保存することできます。*イベント ログ ファイルの照合*、289 ページを参照してください。

- ログ記録システムに関する統計情報の表示

  Content Gateway はログ記録システムに関する統計情報を提供します。Content Gateway manager またはコマンド ライン インターフェースにより、この統計情報にアクセスできます。*ログ記録統計情報の表示*、293 ページを参照してください。

- ログ ファイルの表示

  Content Gateway が作成するシステム、イベント、およびエラーの各ログ ファイルを表示できます。ログ ファイルの全体、ログ ファイル末尾の指定行数、または指定文字列を含むすべての行を表示することができます。

- 標準ログ ファイル フォーマットのログ ファイル エントリの解釈。*イベント ログ ファイル エントリの例*、295 ページを参照してください。

イベント ログ ファイルの管理

Help | Content Gateway | バージョン 7.8.x

イベント ログ ファイルを管理し、ログ ファイルの保存場所、ログ ファイルが使用できるスペースの容量、およびログ記録ディレクトリのディスク スペースが小さくなったときの対応について設定することができます。

ログ記録ディレクトリの選択

デフォルトにより、Content Gateway はすべてのイベント ログ ファイルを **logs** ディレクトリに書き込みますが、これは Content Gateway がインストールされているディレクトリにあります。別のディレクトリを使用する場合は、*ログ ファイル管理オプションの設定、275 ページ*を参照してください。

ログ記録スペースの管理

ログ記録ディレクトリが使用できるディスク スペースの大きさを管理することができます。これにより、システムは指定のスペースの枠内で長期にわたってスムーズに作動することができます。

スペース限界が設定されたら、Content Gateway はログ記録ディレクトリのスペースを継続してモニタします。空きスペースが減少してヘッドルーム限界に近づくと（*ログ ファイル管理オプションの設定、275 ページ*参照）、Content Gateway は小スペース状態になり、以下のような処置を行います：

- 自動削除オプション（*イベント ログ ファイルの取り込み、284 ページ*参照）が*有効化*されていると、Content Gateway は以前に取り込まれたログ ファイル（**.old** 拡張子付きログ ファイル）を特定し、それらを古いものから削除しはじめ、小スペース状態から抜け出すまで続けます。Content Gateway は、それが削除するすべてのファイルの記録をシステム エラー ログ中に残します。
- 自動削除オプションが*無効*であるか、またはシステムが小スペース状態から抜け出すのに十分な古いログ ファイルがない場合は、Content Gateway は警告を出し、スペースがなくなるまでログ記録を継続します。小スペース状態から抜け出すのに十分なスペースが利用できるようになると、Content Gateway はイベント ログ記録を再開します。ログ記録ディレクトリからファイルを消去するか、またはログ記録スペース限界を増大することによって、利用可能なスペースをつくることができます。

cron スクリプトを Content Gateway と連携して実行させることによって、Content Gateway が小スペース状態になる前にログ記録ディレクトリから古いファイルを自動的に除去し、それらを一時パーティションに移すことができます。古いファイルを移動したら、これらのファイルについてログ分析スクリプトを実行することができ、次にこれらを圧縮してアーカイブ場所に移すか、または削除することができます。

ログ ファイル管理オプションの設定

1. **[Configure（構成）] > [Subsystems（サブシステム）] > [Logging（ログ記録）]** に移ります。
2. **[Log Directory（ログ ディレクトリ）]** フィールドで、イベント ログ ファイルを保存しようとするディレクトリのパスを入力します。これは絶対パスでもよいし、または Content Gateway がインストールされているディレクトリに対する相対パスでも結構です。デフォルトのディレクトリは、Content Gateway インストール ディレクトリ中の **logs** です。

   注意
   指定されるディレクトリはすでに存在していなくてはなりません。

   Websense ユーザーは、ログ ファイルを保存するディレクトリについて読み取り / 書き込み許可を保持していなければなりません。

3. **[Log Space（ログ スペース）]** エリアの **[Limit（限界）]** フィールドで、ログ記録ディレクトリに割り当てるスペースの最大容量を入力します。

   Content Gateway が V シリーズ アプライアンス上である場合は、そのサイズは 5120 (5 GB) に設定され、これを変更することはできません。

   Content Gateway がスタンドアローン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。

   注意
   ログ記録ディレクトリ中のすべてのファイルは、ログ ファイルでないものも含めて、なんらかのスペースを使用します。

4. **[Headroom（ヘッドルーム）]** フィールドで、ログ記録スペース限界の許容値を入力します。デフォルト値は 100 MB です。

   [Log Rolling（ログ取り込み）] セクションで **[Auto-Delete Rolled Files（取り込みファイルの自動削除）]** オプションが有効になっている場合、ログ記録ディレクトリで利用できる空きスペースがヘッドルームより小さくなると、自動削除がトリガされます。ログ ファイルの取り込みについては、*イベント ログ ファイルの取り込み*、284 ページを参照してください。

5. **[Apply]** をクリックします。

イベント ログ ファイルのフォーマット

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は下記のログ ファイル フォーマットをサポートします：

- *標準フォーマット*：Squid や Netscape など（*標準フォーマットの使用*、277 ページを参照してください）
- Content Gateway *カスタム フォーマット*（*カスタム フォーマット*、277 ページを参照してください）

標準およびカスタム ログ ファイル フォーマットのほかに、ログ ファイルを *バイナリ*または *ASCII* のどちらで保存するかについて選択しなければなりません。*バイナリまたは ASCII の選択*、281 ページを参照してください。

重要

イベント ログ ファイルは大量のディスク スペースを消費します。同時に複数のフォーマットでログ エントリを作成すると、ディスク リソースを速やかに消費し、プロキシ パフォーマンスに影響することがあります。

重要

IPv6 を有効化した場合、イベント ログの入力項目が IPv6 フォーマットに標準化されます。

たとえば、[10.10.41.200] は、[::ffff:10.10.41.200] とログ記録されます。

カスタム ログ中で [10.10.41.200] のクライアントをフィルタリングするには、下記のフィルタが必要です。

```
<LogFilter>
   <Name = "IPv6_Test_Machine"/>
   <Condition =
       "chi MATCH ::ffff:10.10.41.200"/>
   <Action = "ACCEPT"/>
</LogFilter>
```

標準フォーマットの使用

Help | Content Gateway | バージョン 7.8.x

標準ログ ファイル フォーマットには、Squid、Netscape Common、Netscape Extended、および Netscape Extended-2 があります。

標準ログ ファイル フォーマットは、各種の既製分析パッケージによって分析することができます。標準フォーマットで対応できない情報を必要としないかぎり、いずれかの標準イベント ログ フォーマットを使用すべきです。*カスタム フォーマット、277 ページ*を参照してください。

デフォルトでは、Content Gateway は Netscape Extended ログ ファイル フォーマットだけを使用するように構成されています。

標準ログ ファイル フォーマット オプションの設定

1. **[Configure] > [Subsystems] > [Logging] > [Formats（フォーマット）]** に移ります。
2. 使用するフォーマットを有効にします。
3. ログ ファイルの種類（**ASCII** または**バイナリ**）を選択します。
4. **[Filename（ファイルネーム）]** フィールドで、イベント ログ ファイルで使用する名前を入力します。
5. **[Header（ヘッダー）]** フィールドで、イベント ログ ファイルの最上部で表示されるテキスト ヘッダーを入力します。テキスト ヘッダーを使用しない場合は、このフィールドを空白のままにします。
6. **[Apply]** をクリックします。
7. **[Configure] > [My Proxy] > [Basic] > [General]** で **[Restart]** をクリックします。

カスタム フォーマット

Help | Content Gateway | バージョン 7.8.x

XML ベースのカスタム ログ フォーマットは標準ログ ファイル フォーマットよりも柔軟であり、ログ ファイル中の情報の種類をよりよく管理できるようになります。標準フォーマットで対応できないデータ分析を必要とする場合は、カスタム ログ フォーマットを作成します。各 Content Gateway トランザクションで記録すべき情報を確定し、ログ記録すべきトランザクションを定義するフィルタを作成します。

カスタム ログ記録機能の中心は XML ベースのログ記録構成ファイル **(logs_xml.config)** であり、これによりログ記録オブジェクトのモジュラ記述を作成することができます。**logs_xml.config** ファイルは、カスタム ログ ファイルを作成するために下記の 3 種類のオブジェクトを使用します：

- **LogFormat** は、printf スタイル フォーマットの文字列によってログ ファイルのコンテンツを定義します。
- **LogFilter** は、ログファイルに特定の情報を含めたり、そこから特定の情報を除外したりするフィルタを定義します。
- **LogObject** は、ログ ファイルの生成のために必要なすべての情報を指定します。例：
  - ログ ファイルの名前（必須）。
  - 使用するフォーマット（必須）。これは、標準フォーマット（Squid あるいは Netscape）または事前に定義されているカスタム フォーマット（事前定義の **LogFormat** オブジェクト）のどちらかです。
  - ファイル モード（ASCII、Binary（バイナリ）、または ASCII_PIPE）。デフォルトは ASCII です。

    ASCII_PIPE モードは、UNIX 名前付きパイプ（メモリ中のバッファ）にログ エントリを書き込みます。他のプロセスが標準 I/O 機能によりデータを読めるようになります。このオプションの利点は、Content Gateway によるハードディスク書き込みが不要になり、ディスク スペースと帯域幅が他のタスクのために解放されることです。

    注意

    バッファが一杯であると、Content Gateway はログ エントリをドロップし、抜け落ちたエントリの数を明示するエラー メッセージを出します。Content Gateway は完全なログ エントリだけをパイプに書き込むので、抜け落ちるのは完全なレコードだけです。

  - 使用する任意のフィルタ（事前定義の **LogFilter** オブジェクト）。
  - ログ ファイルを受け取る照合サーバー。
  - ログ記録しようとするプロトコル（プロトコル タグが使用されていると、Content Gateway はリストされているプロトコルからのトランザクションだけをログ記録します。そうでない場合は、すべてのプロトコルについてすべてのトランザクションがログ記録されます）。
  - ログ記録しようとするオリジン サーバー（サーバー タグが使用されていると、Content Gateway はリストされているオリジン サーバーのトランザクションだけをログ記録します。そうでない場合は、すべてのオリジン サーバーについてすべてのトランザクションがログ記録されます）。

- ログ ファイルに含めるヘッダー テキスト。ヘッダ テキストは、ログ ファイルの冒頭で最初のレコードの直前に表示されます。
- ログ ファイル取り込みオプション。

> **注意**
> カスタム ログ フォーマットを生成するには、少なくとも 1 つの **LogObject** 定義を指定しなければなりません。各 **LogObject** 定義ごとに 1 つのログ ファイルがつくられます。カスタム ログ フォーマットを作成するには、Content Gateway manager を使用するか、または構成ファイルを編集します。

1. **[Configure] > [Subsystems] > [Logging] > [Custom（カスタム）]** で、**[Custom Logging（カスタム ログ記録）]** オプションを有効にします。
2. **[Custom Log File Definitions（カスタム ログ ファイル定義）]** エリアで **logs_xml.config** ファイルが表示されます。**[LogFormat]**、**[LogFilter]**、および **[LogObject]** 定義を構成ファイルに追加します。

   logs_xml.config ファイルおよび関連するオブジェクト定義の詳細については、*logs_xml.config*、461 ページを参照してください。
3. **[Apply]** をクリックします。

要約ログ ファイルの作成

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、毎秒、数百のオペレーションを実行するので、イベント ログ ファイルは非常に大きくなります。SQL 式の集計演算子を使用して、特定の期間にわたるログ エントリのセットをまとめた要約ログ ファイルを作成するように Content Gateway を構成することができます。このことによって、生成されるログ ファイルのサイズを縮小することができます。

XML ベースのログ記録構成ファイル **(logs_xml.config)** で **LogFormat** オブジェクトを作成することによって要約ログファイルを生成するには、下記の SQL 式集計演算子を利用します：

- **COUNT**
- **SUM**
- **AVERAGE**
- **FIRST**
- **LAST**

これらの演算子をそれぞれ特定のフィールドに適用し、指定間隔にわたって作動するように要求することができます。

要約ログ ファイルは利便性と情報の精細性とのトレードオフを表しています。ただ 1 つのレコードが生成される時間間隔を指定しなければならないので、これにより情報が失われるかもしれません。要約ログの利便性と通常のログ ファイルの詳細性の両方を必要とする場合は、2 つのカスタム ログ フォーマットを作成し、有効化して、一方が集計演算子を使用し、他方が集計演算子を使用しないようにすることを検討してください。

要約ログ ファイル フォーマットを作成するには、下記の手順に従います：

1. **[Configure] > [Subsystems] > [Logging] > [Custom]**に移り、**logs_xml.config** ファイルを表示します。
2. 下記に従ってログ ファイルのフォーマットを定義します：

```
<LogFormat>
   <Name = "summary"/>
   <Format = "%<operator(field)> : %<operator(field)>"/>
   <Interval = "n"/>
</Format>
```

ここで：

operator は、5 つの演算子（**COUNT**、**SUM**、**AVERAGE**、**FIRST**、**LAST**）の 1 つです。フォーマット行で 2 つ以上の演算子を指定できます。

field は、集計しようとするログ記録フィールドです。

n は、要約ログ エントリ間の秒単位の間隔です。

詳細については、*logs_xml.config*、461 ページを参照してください。

例えば、下記のフォーマットは 10 秒ごとに 1 つのエントリを生成し、各エントリでは当該エントリの最新のエントリのタイム スタンプ、10 秒間隔内に認められたエントリ数のカウント、およびクライアントに送信されたすべてのバイト数の合計が要約されます：

```
<LogFormat>
   <Name = "summary"/>
   <Format = "%<LAST(cqts)> : %<COUNT(*)> :
   %<SUM(psql)>"/>
   <Interval = "10"/>
</Format>
```

重要

集計演算子と標準フィールドの両方を含むフォーマット定義を作成することはできません。例えば、下記の定義を無効です：

```
<Format = "%<LAST(cqts)> : %<COUNT(*)> :
%<SUM(psql)> : %<cqu>"/>
```

3. このフォーマットを使用する **LogObject** を定義します。
4. **[Apply]** をクリックします。

クラスタ内のすべてのノードへの logs_xml.config ファイルの変更の適用

Help | Content Gateway | バージョン 7.8.x

1 つの Content Gateway ノードで **logs_xml.config** ファイルを変更した後、Content Gateway **bin** ディレクトリ **(/opt/WCG/bin)** から下記のコマンドを入力します。

```
content_line -x
```

Content Gateway は、変更をクラスタ内のすべてのノードに適用します。変更はすぐに有効になります。

バイナリまたは ASCII の選択

Help | Content Gateway | バージョン 7.8.x

下記のどちらかのイベント ログ ファイルを作成する Content Gateway を構成することができます：

- **ASCII**：この種類のファイルは、既製の標準的分析ツールによって処理できます。しかし、Content Gateway は ASCII でファイルを作成するために追加的処理を実行しなければならず、その結果、オーバヘッドが大きくなります。また ASCII ファイルは、同等なバイナリ ファイルよりも大きくなりがちです。ASCII ログ ファイルの拡張子はデフォルトで **.log** となります。
- **Binary（バイナリ）**：この種類のファイルはシステムにとってオーバヘッドが小さく、また、ログ記録される情報のタイプにもよりますが、一般にディスクの使用 スペースが少なくてすみます。しかし、標準ツールによってこの種のファイルを読んだり、分析する前に、変換アプリケーションを使用しなければなりません。バイナリ ログ ファイルの拡張子はデフォルトで **.blog** となります。

バイナリ ログ ファイルでは、ディスク スペースの使用は一般に少なくなるのですが、常でそうであるとはいえません。例えば、0（ゼロ）値は、ASCII で保存する場合は 1 バイトにすぎませんが、バイナリ整数として保存する場合は 4 バイトになります。IP アドレスをログ記録するカスタム フォーマットを定義するとき、バイナリ ログ ファイルでは 32 ビット アドレスごとに 4 バイトの記憶容量を必要とするにすぎません。しかし、同じ IP アドレスをドット表記法で保存すると、ASCII ログ ファイルでは約 15 文字（バイト）が必要になります。

標準ログ フォーマットでは、Content Gateway manager の **[Configure] > [Subsystems] > [Logging] > [Formats]** タブで **[Binary]** または **[ASCII]** を選択します。*標準ログ ファイル フォーマット オプションの設定、277 ページ*を参照してください。カスタム ログ フォーマットでは、**LogObject** で ASCII または Binary モードを指定します。*カスタム フォーマット、277 ページ*を参照してください。

> **注意**
>
> カスタム ログ ファイルでは、ASCII および Binary オプションの他に、UNIX 名前付きパイプ（メモリ中のバッファ）にログ エントリを書き込むことができます。他のプロセスが標準 I/O 機能によりデータを読めるようになります。このオプションの利点は、Content Gateway によるハードディスク書き込みが不要になり、ディスク スペースと帯域幅が他のタスクのために解放されることです。また、UNIX 名前付きパイプはディスク スペースを使用しないので、ログ記録スペースが使い尽くされても、パイプへの書き込みは中断しません。ASCII_PIPE オプションの詳細については、*logs_xml.config、461 ページ*を参照してください。

ログ ファイルで ASCII またはバイナリ モードを選択する前に、ログ記録するデータのタイプについて検討してください。別々の日にそれぞれ ASCII およびバイナリ モードでログ記録をとってみてください。両日の要求数がほぼ同じであるものとすると、大ざっぱに両フォーマットを数量的に比較することができます。

logcat によるバイナリ ログから ASCII ログへの変換

Help | Content Gateway | バージョン 7.8.x

バイナリ ログ ファイルを ASCII ファイルに変換して、標準ツールで分析できるようしなければなりません。

1. バイナリ ログ ファイルを保存しているディレクトリに移ります。
2. **logcat** ユーティリティのパスが有効であることを確認してください。
3. 次のコマンドを入力します：

```
logcat options input_filename...
```

下記の表はコマンド行オプションについての説明です。

オプション	説明
-o output_file	コマンドの出力先を指定します。

-a	入力ファイルネームに基づいて出力ファイルネームを自動的に生成します。入力が **stdin** からであると、このオプションは無視されます。
	例：
	`logcat -a squid-1.blog squid-2.blog squid-3.blog`
	により、下記のファイルを生成されます：
	`squid-1.log, squid-2.log, squid-3.log`

-S	可能であれば、入力を Squid フォーマットに変換しようとします。
-C	可能であれば、入力を Netscape Common フォーマットに変換しようとします。
-E	可能であれば、入力を Netscape Extended フォーマットに変換しようとします。
-2	可能であれば、入力を Netscape Extended-2 フォーマットに変換しようとします。

注意

下記のオプションのうち、どれか 1 つだけを使用するようにしてください：**-S**、**-C**、**-E**、または **-2**。

入力ファイルが指定されていないと、**logcat** は標準入力 **(stdin)** から読み込みます。出力ファイルが指定されていないと、**logcat** は標準出力 **(stdout)** に書き出します。

例えば、バイナリ ログ ファイルを ASCII ファイルに変換するには、下記のオプションどちらかで **logcat** コマンドを使用します。

```
logcat binary_file > ascii_file
logcat -o ascii_file binary_file
```

バイナリ ログ ファイルは、このコマンドによって変更されません。

イベント ログ ファイルの取り込み

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は自動ログ ファイル取り込み機能を提供します。すなわち、Content Gateway は 1 日のうち特定の間隔で現在のセットのログ ファイルを閉じ、新しいログ ファイルを開きます。

ログ ファイル取り込みには、下記のような便益があります：

- これは、ログ分析を実行できる時間間隔を定義します。
- これは単一のログ ファイルが過大になるのを防止し、指定されている限界のスペースでのログ記録システムの動作を支援します。
- これは、使用されなくなっているファイルを特定して、自動化スクリプトによるログ記録ディレクトリのクリーンアップとログ分析プログラムの実行を容易にします。

1 日に数回、ログ ファイルを取り込むべきです。6 時間ごの取り込みが好ましいガイドラインになるでしょう。

取り込みログ ファイルネーム フォーマット

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は、取り込まれたログ ファイルの特定を容易にする整合的なネーム フォーマットを提供します。

Content Gateway がログ ファイルを取り込むとき、古いファイルを保存して閉じ、新しいファイルを開始します。Content Gateway は古いファイルをリネームして、下記の情報を含めます：

- ファイルのフォーマット（例、**squid.log**）。
- ログ ファイルを生成した Content Gateway サーバーのホストネーム。
- ハイフン（-）で区切られた 2 つのタイムスタンプ。最初のタイムスタンプは、ログ ファイル中の最初のレコードのタイムスタンプの下限です。この下限は、ログ レコードのために新しいバッファが作成されるときの時刻です。低負荷のもとでは、ファイルネーム中の最初のタイムスタンプは最初のエントリのタイムスタンプと異なることがあります。標準負荷のもとでは、ファイルネーム中の最初のタイムスタンプと最初のエントリのタイムスタンプは近似します。

  二番目のタイムスタンプは、ログ ファイル中の最後のレコードのタイムスタンプの上限です（これは、通常、取り込み時刻です）。
- 接尾辞の **.old** — これは自動化スクリプトによる取り込みログ ファイルの検出を容易にします。

タイムスタンプは次のようなフォーマットになっています：

```
%Y%M%D.%Hh%Mm%Ss-%Y%M%D.%Hh%Mm%Ss
```

以下の表でフォーマットについて説明しています：

コード	定義	例
%Y	4 桁表記の年	2000
%M	2 桁表記の月、01-12	07
%D	2 桁表記の日、01-31	19
%H	2 桁表記の時、00-23	21
%M	2 桁表記の分、00-59	52
%S	2 桁表記の秒、00-59	36

下記は取り込みログ ファイルネームの例です：

```
squid.log.mymachine.20000912.12h00m00s-
20000913.12h00m00s.old
```

この例では、ファイルは squid ログ フォーマットであり、そのホスト コンピュータは mymachine です。最初のタイムスタンプは、2000 年、9 月、12 日、正午 12 時 00 分という日時を示しています。二番目のタイムスタンプは、2000 年、9 月、13 日、正午 12 時 00 分という日時を示しています。ファイルネームの終りに接尾辞の .old があります。

ログ記録システムは、ログ レコードをディスクに書き込む前に、それらをバッファします。ログ ファイルが取り込まれるとき、ログ バッファはかなり一杯になっているかもしれません。そのような場合、新しいログ ファイルの最初のエントリのタイムスタンプは取り込み時刻よりも前になるでしょう。新しいログ ファイルが取り込まれると、その最初のタイムスタンプが最初のエントリのタイムスタンプの下限になります。例えば、ログ記録が 3 時間毎に取り込まれるものとし、最初の取り込みログ ファイルが下記のものであるとします：

```
squid.log.mymachine.19980912.12h00m00s-
19980912.03h00m00s.old
```

3:00:00 の時点のログ バッファの最初のエントリの下限が 2:59:47 であると、次のログ ファイルが取り込まれると、そのタイムスタンプは下記のようになります：

```
squid.log.mymachine.19980912.02h59m47s-
19980912.06h00m00s.old
```

ログ ファイルのコンテンツは、常に、これら 2 つのタイムスタンプの間のものです。連続するタイムスタンプが重複しているようであっても、ログ ファイルには重複するエントリはありません。

取り込み間隔

Help | Content Gateway | バージョン 7.8.x

ログ ファイルは、1 日の所定時刻を基準として特定の間隔で取り込まれます。下記の 2 つのオプションによって、ログ ファイルが取り込まれる時点が管理されます：

- オフセット時刻 — これは 0 時（真夜中）から 23 時までのいずれかの正時です。
- 取り込み間隔

オフセット時刻と取り込み間隔の両方によって、ログ ファイルの取り込みが始まる時点が決まります。取り込みは、取り込み間隔毎*および*オフセット時刻に行われます。

例えば、取り込み間隔が 6 時間で、オフセット時刻が 0（真夜中）であると、ログ記録の取り込みは、毎日、真夜中 (00:00)、06:00、12:00、および 18:00 に行われます。取り込み間隔が 12 時間で、オフセット時刻が 3 であると、ログ記録の取り込みは、毎日、03:00 および 15:00 に行われます。

ログ ファイル取り込みオプションの設定

1. **[Configure] > [Subsystems] > [Logging] > [General]** を順に選択します。
2. **[Log Rolling（ログ取り込み）]** セクションで **[Log Rolling]** オプションが有効になっていることを確かめます（デフォルトは有効です）。
3. **[Offset Hour（オフセット時刻）]** フィールドで、毎日、ログ ファイル取り込みが行われるべき時刻を入力します。Content Gateway は、毎日、オフセット時刻にログ ファイルの取り込みを行わせます。

   0（真夜中）から 23 までの任意の正時を入力できます。
4. **[Interval（間隔）]** フィールドで、次回の取り込みまで Content Gateway がログ ファイルにデータを書き込む時間の長さを入力します。

   最小値は 300 秒（5 分）です。最大値は 86400 秒（1 日）です。

   > **注意**
   > 次の取り込み時刻の数分以内に Content Gateway を起動すると、ログ ファイル取り込みはその次の取り込み時刻からになるでしょう。

5. **[Auto-Delete Rolled Files（取り込みファイルの自動削除）]** オプションが有効であることを確かめてください（デフォルトは有効です）。これにより、ログ ディレクトリで利用できるスペースが少なくなると、取り込みログ ファイルが自動的に削除されます。

ログ ディレクトリで利用できる空きスペースがヘッドルーム未満になると、自動削除がトリガされます。

6. **[Apply]** をクリックします。

> **注意**
>
> **logs_xml.config** ファイルの **LogObject** 定義でカスタム ログ ファイルの取り込み設定を微調整することができます。カスタム ログ ファイルはその **LogObject** を取り込み設定として使用しますが、これは Content Gateway manager または前述の **records.config** ファイルで指定されているデフォルト設定よりも優先します。

イベント ログ ファイルの分割

Help | Content Gateway | バージョン 7.8.x

デフォルトで、Websense Content Gateway は標準ログ フォーマットを使用し、同じファイルに HTTP および FTP トランザクションを含むログ ファイルを生成します。しかし、異なるオリジン サーバーのトランザクションを個別のログ ファイルにログ記録することが望ましい場合、ホスト ログ分割を有効にすることができます。

HTTP ホスト ログ分割

Help | Content Gateway | バージョン 7.8.x

HTTP ホスト ログ分割によって、異なるオリジン サーバーの HTTP および FTP トランザクションを個別のログ ファイルに記録することができます。HTTP ホスト ログ分割が有効であると、Content Gateway は **log_hosts.config** ファイルにリストされている各オリジン サーバーごとに個別のログ ファイルを作成します（*log_hosts.config ファイルの編集、288 ページ*を参照してください）。

HTTP ホスト ログ分割が有効であるとき、Content Gateway は HTTP/FTP トランザクションについて、オリジン サーバー別のログ ファイルを作成します。

例えば、**log_hosts.config** ファイルが 2 つのオリジン サーバー — **uni.edu** と **company.com** — を含んでいて、かつ Squid フォーマットが有効であると、Content Gateway は下記のようなログ ファイルを生成します：

ログ ファイルネーム	説明
squid-uni.edu.log	**uni.edu** のすべての HTTP および FTP トランザクション
squid-company.com.log	**company.com** のすべての HTTP および FTP トランザクション
squid.log	他のホストのすべての HTTP および FTP トランザクション

Content Gateway では、プロトコルおよびホスト名に基づいてログ ファイルの生成を詳細に管理することを可能にする XML ベースのログ フォーマットを作成することもできます。*カスタム フォーマット、277 ページ*を参照してください。

ログ分割オプションの設定

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Subsystems] > [Logging] > [Splitting（分割）]** を順に選択します。
2. **[Split Host Logs（ホスト ログの分割）]** オプションを有効にして、**log_hosts.config** ファイルにリストされている各オリジン サーバーのすべての HTTP および FTP トランザクションをそれぞれ個別のログ ファイルに記録します。**[Split Host Logs（ホスト ログの分割）]** オプションを無効にして、**log_hosts.config** ファイルにリストされている各オリジン サーバーのすべての HTTP および FTP トランザクションを同一のログ ファイルに記録します。
3. **[Apply]** をクリックします。

log_hosts.config ファイルの編集

Help | Content Gateway | バージョン 7.8.x

デフォルトの **log_hosts.config** ファイルは **/opt/WCG/config** にあります。異なるオリジン サーバーの HTTP および FTP トランザクションを個別のログ ファイルに記録するには、log_hosts.config ファイルの個別の行で各オリジン サーバーのホストネームを指定しなければなりません。

注意

log_hosts.config ファイルでキーワードを指定し、そのキーワードをホストネームに含むオリジン サーバーのすべてのトランザクションを別個のログ ファイルに記録することができます。例えば、キーワードとして **sports** を指定すると、Content Gateway は **sports.yahoo.com** および **www.foxsports.com** からのすべての HTTP および FTP トランザクションを **squid-sports.log** というログ ファイルに記録します（Squid フォーマットが有効である場合）。

注意

Content Gateway がクラスタ化されていて、ログ ファイル照合が有効である場合は、クラスタ中のあらゆるノードで同じ **log_hosts.config** ファイルを使用すべきでしょう。

1. **/opt/WCG/config** にある **log_hosts.config** ファイルを開きます。
2. このファイルで、各オリジン サーバーのホストネームをそれぞれ別個の行に入力します。例：

   ```
   webserver1
   webserver2
   webserver3
   ```

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway の **bin** ディレクトリ **(/opt/WCG/bin)** から下記のコマンドを実行します：

   ```
   ./content_line -x
   ```

イベント ログ ファイルの照合

Help | Content Gateway | バージョン 7.8.x

ログ ファイル照合機能を使用して、ログ記録されたすべての情報を一箇所で保存することができます。このことにより、個別のノードとしてではなく、全体としての Content Gateway を分析し、クラスタ中の特定のノードに存在している大容量ディスクを利用することができます。

Content Gateway は、1 つ以上のノードをログ照合サーバにし、他のすべてのノードをログ照合クライアントにして、ログ ファイルの照合を行います。ノードがイベント ログ エントリのバッファを生成するとき、そのノードは自らが照合サーバーと照合クライアントのどちらであるかについて判断します。照合サーバー ノードは、あたかもログ照合が有効になっていないかのように、すべてのログ バッファをそのローカル ディスクに書き込みます。

照合クライアント ノードは、そのログ バッファをネットワークを介する転送に向けて準備し、それらのバッファをログ照合サーバーに送ります。ログ照合サーバーがログ バッファをクライアントから受け取ると、サーバー ノードはそのバッファをあたかもローカルに生成されたものであるかのように自己のログ ファイルに書き込みます。ログ クライアントがそのログ照合サーバーと通信できない場合、クライアント ノードはそのログ バッファを自己のローカル ディスクで *orphan*（オーファン）ログ ファイルに書き込みます。オーファン ログ ファイルは、手動による照合を必要とします。ログ照合サーバーはスタンドアローンでもよいし、または Content Gateway を作動させているノードの一部であってもかまいません。

注意

ログ照合はネットワークのパフォーマンスに影響することがあります。なぜならば、すべてのノードがそれぞれログ データを単一の照合サーバーに転送するので、ネットワーク中の単一のノードに送られるデータの量がそのノードによる迅速なデータ処理能力を上まわり、ボトルネックがネットワークで発生するかもしれないからです。

注意

照合ログ ファイルは各エントリのタイムスタンプ情報を含んでいますが、ファイル中のエントリは厳密に時系列順になっているのではありません。分析する前に照合ログ ファイルをソートすることができます。

照合サーバーにするための Content Gateway の構成

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Subsystems] > [Logging] > [Collation（照合）]** を順に選択します。
2. **[Collation Mode（照合モード）]** セクションで、**[Be A Collation Server（照合サーバーになる）]** オプションを有効にします。
3. **[Log Collation Port（ログ照合ポート）]** フィールドで、照合クライアントとの通信で使用されるポート番号を入力します。デフォルトのポート番号は 8085 です。

4. **[Log Collation Secret（ログ照合秘密）]** フィールドで、ログ記録データを検証し、恣意的情報の交換を防止するために使用されるパスワードを入力します。

> **注意**
> すべての照合クライアントは、この同じ秘密を使用しなければなりません。

5. **[Apply]** をクリックします。

> **重要**
> 照合サーバーと照合クライアントとの接続が確立した後で照合ポートまたは秘密を変更した場合、Content Gateway を再起動しなければなりません。

照合クライアントにするための Content Gateway の構成

Help | Content Gateway | バージョン 7.8.x

1. **[Configure] > [Subsystems] > [Logging] > [Collation]** を順に選択します。
2. **[Collation Mode]** セクションで、**[Be a Collation Client（照合クライアントになる）]** オプションを有効にして、Content Gateway ノードを照合クライアントに設定し、アクティブな標準フォーマット ログ エントリ（Squid や Netscape など）をログ照合サーバーに送ります。

> **注意**
> XML ベース フォーマットの ログ エントリを照合サーバーに送るためには、**logs_xml.config** ファイルにログ オブジェクト定義を追加しなければなりません。*カスタム フォーマット、277 ページ*を参照してください。

3. **[To Collation Server（宛先照合サーバー）]** フィールドで、照合サーバーのホストネームを入力します。これは、Content Gateway 照合サーバーまたはスタンドアローン照合サーバーのどちらでもかまいません。
4. **[Log Collation Port（ログ照合ポート）]** フィールドで、照合サーバーとの通信で使用されるポート番号を入力します。デフォルトのポート番号は 8085 です。
5. **[Log Collation Secret（ログ照合秘密）]** フィールドで、ログ記録データを検証し、恣意的情報の交換を防止するために使用されるパスワードを入力します。これは、照合サーバーで設定されるのと同じ秘密でなければなりません。

6. 照合ログ ファイルでログ エントリのオリジンを維持する場合は、**[Log Collation Host Tagged（照合ホストをタグ付きでログ記録する）]** オプションを有効にします。
7. **[Log Collation Orphan Space（ログ照合オーファン スペース）]** フィールドで、照合クライアントのログ記録ディレクトリでオーファン ログ ファイルを保存するために割り当てるスペースの最大容量（メガバイト単位）を入力します。（ログ照合サーバーと通信できない場合、オーファン ログ ファイルが作成されます。）デフォルト値は 25 MB です。
8. **[Apply]** をクリックします。

> **重要**
> 照合サーバーと照合クライアントとの接続が確立した後で照合ポートまたは秘密を変更した場合、Content Gateway を再起動しなければなりません。

スタンドアローン照合サーバー

Help | Content Gateway | バージョン 7.8.x

ログ照合サーバーを Content Gateway ノードにしたくない場合は、ログ ファイルの収集、処理、および書き込みにほぼ集中するスタンドアローン照合サーバー (SAC) をインストールおよび構成することができます。

> **注意**
> スタンドアローン照合サーバーを利用できるのは、現在、Linux プラットフォームだけです。

1. Content Gateway ノードをログ照合クライアントとして構成します。*照合クライアントにするための Content Gateway の構成*、291 ページを参照してください。
2. **sac** バイナリを Content Gateway の **bin** ディレクトリ **(/opt/WCG/bin)** からスタンドアローン照合サーバーになるコンピュータにコピーします。
3. **sac** バイナリを保持するディレクトリ中に **config** というディレクトリを作成します。
4. ステップ 3 で作成した **config** ディレクトリ中に **internal** というディレクトリを作成します。このディレクトリは、スタンドアローン照合サーバーによってロック ファイルを保存するために内部的に使用されます。
5. ログ照合クライアントとして構成されている Content Gateway ノードから **records.config** ファイル **(/opt/WCG/config)** をステップ 3 でスタンドアローン照合サーバーで作成した **config** ディレクトリにコピーします。

records.config ファイルは、照合クライアントになるノードの構成時に指定されたログ照合秘密およびポートを含んでいます。照合ポートおよび秘密はすべての照合クライアントおよびサーバーで同一でなければなりません。

6. スタンドアローン照合サーバー上で **records.config** ファイルを開き、下記の変数を編集します：

変数	説明
proxy.config.log2.logfile_dir	ログ ファイルを保存すべきディレクトリを指定します。このディレクトリへの絶対パスをしてもよいし、または **sac** バイナリが実行されるディレクトリとの相対パスでもかまいません。 ご注意：このディレクトリは、スタンドアローン照合サーバーになるコンピュータ上ですでに存在していなければなりません。

7. ファイルを保存して、閉じます。
8. 次のコマンドを入力します：

```
sac -c config
```

ログ記録統計情報の表示

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、下記のような情報の確認を支援するログ記録システム統計情報を生成します：

- 現在、書き込まれているログ ファイル（フォーマット）の数。
- すべてのイベントおよびエラー ログを保持するログ記録ディレクトリによって使用されている現在のスペースの容量。
- Content Gateway インストール以降、ログ ファイルに書き込まれたアクセス イベントの数。このカウンタは 1 つのファイルに 1 つのエントリを表します。複数のフォーマットが書き込まれると、単一のイベントによって複数のイベント ログ エントリが作成されます。
- Content Gateway インストール以降、フィルタリングによって撥ねられたためにスキップされたアクセス イベントの数。
- Content Gateway インストール以降、イベント エラー ログに書き込まれたアクセス イベントの数。

Content Gateway manager の [Monitor（モニタ）] タブからこの統計情報を表示でき、またコマンドライン インターフェースによりこの統計情報を取得することもできます。*トラフィックのモニタリング、133 ページ*を参照してください。

ログ ファイルの表示

Help | Content Gateway | バージョン 7.8.x

関連項目：

- *Squid フォーマット*、296 ページ
- *Netscape の例*、297 ページ

Content Gateway が作成するシステム、イベント、およびエラーのログ ファイルを Content Gateway manager で表示することができます。ログ ファイルの全体、ログ ファイル末尾の指定行数、または指定文字列を含むすべての行を表示することができます。

またログ ファイルを削除したり、それをローカル システムへコピーすることもできます。

注意

ログ ファイルのコピーと削除には、正しいユーザー許可が必要です。

注意

Content Gateway はログ ファイルの最初の 1 MB だけを表示します。1 MB を超えるログ ファイルが選択されると、Content Gateway はファイルを切り詰め、ファイルが大きすぎるという警告メッセージを表示します。

Content Gateway manager によりログ ファイルにアクセスできるようになりました。

1. **[Configure] > [My Proxy（マイ プロキシ）] > [Logs] > [System]** を順に選択します。
2. システム ログ ファイルを表示、コピー、または削除する場合は、ステップ 3 へ進みます。

   イベントまたはエラー ログ ファイルを表示、コピー、または削除するには、**[Access（アクセス）]** タブを選択します。
3. **[Log File]** ドロップダウン リストで、表示、コピー、または削除するログ ファイルを選択します。

   Content Gateway は、システム全体のログ記録機能である **syslog** がデーモン機能のもとで記録したシステム ログ ファイル をリストアップします。

Content Gateway はイベント ログ ファイルをリストアップしますが、これらのファイルは **[Configure] > [Subsystems] > [Logging] > [General]** タブの **[Logging Directory]** フィールドで指定されているか、または **records.config** ファイルの **proxy.config.log2.logfile_dir** 構成変数によって指定されているディレクトリに保存されています。デフォルトのディレクトリは、Content Gateway インストール ディレクトリの **logs** です。

4. **[Action（アクション）]** エリアで、下記のオプションのどれかを選択します：
   - **Display the selected log file（選択ログ ファイルの表示）** — ログ ファイル全体を表示します。ファイルが 1 MB 超であると、最初の 1MB のデータだけが表示されます。
   - **Display last lines of the selected file（選択ファイルの末尾部分の表示）** — ログ ファイルの末尾部分を表示します。表示させる行数を用意されているフィールドで指定します。
   - **Display lines that match in the selected log file（選択ログ ファイル中の一致する行の表示）** — ログ ファイル中で特定の文字列と一致する行を表示します。文字列を用意されているフィールドで入力します。
   - **Remove the selected log file（選択ログ ファイルの削除）** — 選択されているログ ファイルを Content Gateway システムから削除します。
   - **Save the selected log file in local filesystem（選択ログ ファイルをローカル ファイルシステムへ保存）** — 選択されているログ ファイルのコピーをローカル システム上で保存します。
5. **[Apply]** をクリックします。

   ログ ファイルの表示を選択していると、Content Gateway はファイルをページの最後で表示します。

   ログ ファイルの削除を選択していると、Content Gateway はファイルを削除します。削除の確認は求められません。

   ログ ファイルの保存を選択していると、ローカル システム上でファイルを保存すべき場所の指定を求められます。

イベント ログ ファイル エントリの例

Help | Content Gateway | バージョン 7.8.x

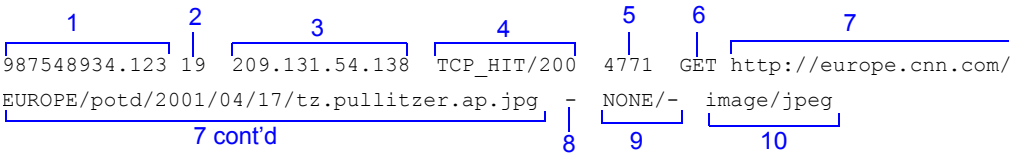
このセクションでは、Content Gateway でサポートされている各標準ログ フォーマットのログ ファイル エントリの例を紹介します：

- *Squid フォーマット*、296 ページ
- *Netscape の例*、297 ページ
- *Netscape Extended フォーマット*、297 ページ
- *Netscape Extended-2 フォーマット*、297 ページ

Squid フォーマット

Help | Content Gateway | バージョン 7.8.x

次の図は、**squid.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。



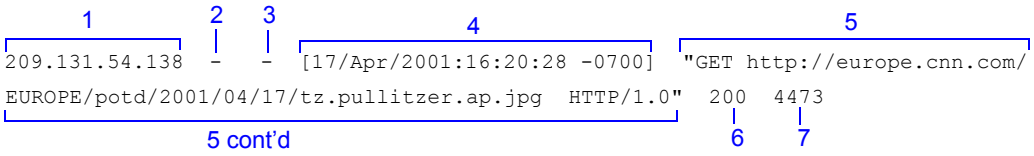
フィールド	説明
1	Squid フォーマットのクライアント要求タイムスタンプ、1970 年 1 月 1 日 (UTC) からの秒数で示されるクライアント要求の時刻（精度：ミリ秒）。
2	プロキシがクライアントの要求の処理で費やした時間、クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までのミリ秒数。
3	クライアントのホスト コンピュータの IP アドレス。
4	キャッシュ戻り値、要求に対するキャッシュの応答を示します：HIT（ヒット）、MISS（ミス）、等々。キャッシュ戻り値については、*Squid 形式および Netscape 形式のログ ファイル内のキャッシュ戻り値、299 ページ*で説明しています。 プロキシ ステータス コード（Content Gateway からクライアントへの HTTP 応答ステータス コード）。
5	クライアントに対する Content Gateway の応答の長さ（バイト数）で、これはヘッダとコンテンツを含みます。
6	クライアント要求方式：GET、POST、等々。
7	クライアント要求の標準 URL、ログ分析ツールで解析できないブランクやその他の特殊文字はエスケープ シーケンスによって置き換えられます。エスケープ シーケンスは、パーセント記号とそれに後続する置換された文字の ASCII コード番号（16 進表記）です。
8	認証されたクライアントのユーザー名。ハイフン（-）は、認証が不要であったことを示しています。
9	プロキシ階層ルート、Content Gateway がオブジェクトの取得のために使用したルート。プロキシ要求サーバー名、要求を実現したサーバーの名前。要求がキャッシュ ヒットであった場合、このフィールドにはハイフン（-）があります。
10	プロキシ応答のコンテンツ タイプ、Content Gateway 応答 ヘッダから取られたオブジェクト コンテンツ タイプ。

Netscape の例

Help | Content Gateway | バージョン 7.8.x

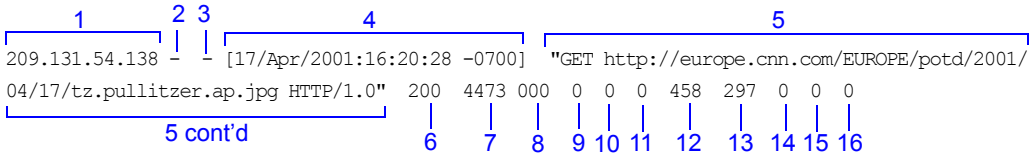
Netscape Common フォーマット

次の図は、**common.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。



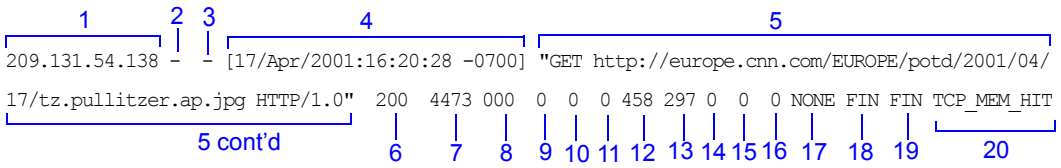
Netscape Extended フォーマット

次の図は、**extended.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。



Netscape Extended-2 フォーマット

次の図は、**extended2.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。



フィールド	説明
	Netscape Common
1	クライアントのホスト コンピュータの IP アドレス。
2	Netscape ログ エントリでは、このハイフン（-）は常に存在します。
3	認証されたクライアントのユーザー名。ハイフン（-）は、認証が不要であったことを示しています。

フィールド	説明
4	クライアントの要求の日付と時刻 - 括弧で囲まれています。
5	要求行 - 引用符で囲まれています。
6	プロキシ応答ステータス コード（HTTP 応答コード）。
7	クライアントに対する Content Gateway 応答の長さ（バイト数）。
	Netscape Extended
8	オリジン サーバーの応答ステータス コード。
9	サーバー応答転送の長さ、プロキシに対するオリジン サーバー応答本文の長さ（バイト数）。
10	クライアント要求転送の長さ、プロキシに対するクライアントの要求本文の長さ（バイト数）。
11	プロキシ要求転送の長さ、オリジン サーバーに対するプロキシ要求本文の長さ。
12	クライアント要求ヘッダの長さ、プロキシに対するクライアントの要求ヘッダの長さ。
13	プロキシ応答ヘッダの長さ、クライアントに対するプロキシ応答ヘッダの長さ。
14	プロキシ要求ヘッダの長さ、オリジン サーバーに対するプロキシ要求ヘッダの長さ。
15	サーバー応答ヘッダの長さ、プロキシに対するオリジン サーバー応答ヘッダの長さ。
16	Content Gateway がクライアントの要求の処理で費やした時間、クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までの秒数。
	Netscape Extended-2
17	プロキシ階層ルート、Content Gateway がオブジェクトの取得のために使用したルート。
18	クライアント終了ステータス コード：FIN（クライアント要求が正常に完了した場合）または INTR（クライアント要求が中断された場合）。
19	プロキシ終了ステータス コード：FIN（オリジン サーバーに対する Content Gateway 要求が正常に完了した場合）または INTR（その要求が中断された場合）。
20	キャッシュ戻り値、要求に対する Content Gateway キャッシュの応答：HIT（ヒット）、MISS（ミス）、等々。キャッシュ戻り値については、*Squid 形式および Netscape 形式のログ ファイル内のキャッシュ戻り値*、299 ページで説明しています。

Squid 形式および Netscape 形式のログ ファイル内のキャッシュ戻り値

Squid および Netscape ログ ファイル内のキャッシュ戻り値：

キャッシュ戻り値	説明
TCP_HIT	要求されたオブジェクトの有効なコピーがキャッシュに入れられたこと、およびプロキシがオブジェクトをクライアントに送信したことを示します。
TCP_MISS	要求されたオブジェクトがキャッシュに入れられなかったこと、およびプロキシがオリジン サーバーまたは親プロキシからオブジェクトを取得し、それをクリアントに送信したことを示します。
TCP_REFRESH_HIT	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、`if-modified-since` 要求をオリジン サーバーに行い、オリジン サーバーが `304 not-modified` 応答を送信したことを示します。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。
TCP_REF_FAIL_HIT	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、`if-modified-since` 要求をオリジン サーバーに行いましたが、そのサーバーは応答しませんでした。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。
TCP_REFRESH_MISS	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、`if-modified-since` 要求をオリジン サーバーに行い、そのサーバーは新しいオブジェクトを返しました。プロキシは、新しいオブジェクトをクライアントに送信しました。
TCP_CLIENT_REFRESH	クライアントが `no-cache` ヘッダーの付いた要求を発行したことを示します。プロキシは要求されたオブジェクトをオリジン サーバーから取得し、コピーをクライアントに送信します。Content Gateway は、キャッシュからオブジェクトの以前のすべてのコピーを削除します。

キャッシュ戻り値	説明
TCP_IMS_HIT	クライアントが `if-modified-since` 要求を発行し、オブジェクトがキャッシュに入っていて IMS の日付より新しいこと、またはオリジン サーバーへの `if-modified-since` でそのキャッシュ オブジェクトが新しいことが確認されたことを示します。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。
TCP_IMS_MISS	クライアントが `if-modified-since` 要求を発行したこと、およびオブジェクトがキャッシュにいれられていなか、またはキャッシュ内で陳腐化していることを示します。プロキシは、`if-modified-since` 要求をオリジン サーバーに行い、新しいオブジェクトを受信しました。プロキシは、更新されたオブジェクトをクライアントに送信しました。
TCP_SWAPFAIL	オブジェクトがキャッシュに入れられたが、アクセスできなかったことを示します。クライアントはオブジェクトを受信しませんでした。
ERR_CLIENT_ABORT	完全なオブジェクトが送信される前にクライアントが切断されたことを示します。
ERR_CONNECT_FAIL	Content Gateway がオリジン サーバーにアクセスできなかったことを示します。
ERR_DNS_FAIL	Domain Name Server がオリジン サーバー名を解決できなかったこと、または Domain Name Server がアクセスできなかったことを示します。
ERR_INVALID_REQ	クライアント HTTP 要求が無効であったことを示します。Content Gateway は未知の方法で要求をオリジン サーバーに転送します。
ERR_READ_TIMEOUT	タイムアウト間隔以内にオリジン サーバーが Content Gateway の要求に応答しなかったことを示します。
ERR_PROXY_DENIED	クライアント サービスがアクセス制御設定によって拒否されたことを示します。
ERR_UNKNOWN	クライアントは接続しましたが、その後要求を送信せずに切断されたことを示します。

A 統計

Help | Content Gateway | バージョン 7.8.x

本章では、Content Gateway Manager の **Monitor** タブの下記の統計について説明しています。

My Proxy

Help | Content Gateway | バージョン 7.8.x

My Proxy 統計は下記のカテゴリに分けられます。

Summary（要約）

Help | Content Gateway | バージョン 7.8.x

統計情報 / フィールド	説明
	Subscription Details（サブスクリプション詳細）
Feature（機能）	スキャン オプション、Data Security、ThreatScope など利用可能な機能をリストします。
Purchased Status（購入ステータス）	機能が購入されたかどうか示します。
Expiration Date（有効期限）	機能が購入されている場合、サブスクリプションの有効期限を表示します。
	More Detail（より詳細）
Subscription key（サブスクリプション キー）	サブスクリプション キーを表示します。*サブスクリプション キーの入力、19 ページ*を参照してください。
Last successful subscription download time（最終サブスクリプション ダウンロード成功 時間）	サブスクリプション キーの最終確認時間を表示します。このチェックは 1 日に 1 回行われます。
Connection status（接続ステータス）	Content Gateway の Policy Server、Policy Broker、および Filtering Service への接続状態を表示します。
Registration status（登録ステータス）	Forensics Repository の Content Gateway 登録ステータスを表示します。
	Scanning Data Files（スキャンニング データ ファイル）
Engine Name（エンジン名）	各スキャンニング エンジン名を表示します。
Engine Version（エンジン バージョン）	スキャンニング エンジンのバージョン番号を表示します。
Data File Version（データファイル バージョン）	スキャンニング エンジンで現在使用されているデータ ファイルのバージョン番号を表示します。
Last update（最終更新）	Content Gateway が、分析データ ファイル、設定、およびポリシーを最後にロードした日時を表示します。
Last time Content Gateway loaded data（Content Gateway 最終データ ロード 時間）	Content Gateway が、分析データファイル、設定、およびポリシーを最後にロードした日時を表示します。

統計情報 / フィールド	説明
Last time Content Gateway checked for updates（Content Gateway 最終更新確認時間）	Content Gateway が、データ ファイルの更新を確認するために、Websense ダウンロード サーバーと最後に通信した日時を表示します。
	Node Details（ノード詳細）
Node（ノード）	Content Gateway ノードまたはクラスタ名
On/Off（オン / オフ）	プロキシおよびマネージャ サービスが実行中であるかどうかを示します。
Objects Served（処理されたオブジェクト）	ノードによって使用されたオブジェクトの合計数
Ops/Sec（処理数 / 秒）	ノードによって処理された 1 秒あたりの処理数。
Hit Rate（ヒット率）	キャッシュから処理された HTTP 要求パーセンテージ（過去 10 秒間の平均）。
Throughput (Mbit/sec)（スループット）	ノード（およびクラスタ）の 1 秒あたりの通過量 (Mbit)。 プロキシは、オブジェクト全体を転送した後、スループット統計を更新します。サイズが大きなファイルの場合、転送の終わりの時点でバイト カウントが急に大きくなります。転送されるバイトの完全な数は、最後の 10 秒間の結果であると考えられます。ただしオブジェクトを転送するのに数分かかることがあります。 この一時的な不正確さは、負荷が小さい場合に、より顕著になります。
HTTP Hit (ms)（HTTP ヒット）	キャッシュ内に最新のものが存在する HTTP オブジェクトをクライアントに出力するために要した時間。
HTTP Miss (ms)（HTTP ミス）	キャッシュ内に存在しない または 陳腐化した HTTP オブジェクトを クライアントに出力するために要した時間。
	More Detail（より詳細）
cache hit rate（キャッシュ ヒット率）	キャッシュから処理された HTTP 要求パーセンテージ（過去 10 秒間の平均）。この値は 10 秒毎に更新されます。
errors（エラー率）	障害により終了した要求のパーセンテージ。
aborts（中断率）	中断され要求のパーセンテージ。
active clients（アクティブなクライアント）	クライアント接続の現在のオープン数。
active servers（アクティブな サーバー）	オリジン サーバー接続の現在のオープン数。
node IP address（ノード IP アドレス）	ノードに割り当てられた IP アドレス。仮想 IP アドレス指定が有効化されている場合、複数の仮想 IP アドレスをこのノードに割り当てることができます。

統計情報 / フィールド	説明
cache free space（キャッシュ空容量）	キャッシュの空き容量。
HostDB hit rate（ホスト DB ヒット率）	ホスト データベース ルックアップの合計に対するホスト データベース ヒットの比率（10 秒間の平均）。

ノード

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Node Summary（ノード要約）
Status（ステータス）	Content Gateway が このノード上で実行しているかを示します（active または inactive）。
Up Since（起動日時）	Content Gateway が起動した日時。
Clustering（クラスタ化）	このノード上でのクラスタ化のオン / オフ状態を示します。
	キャッシュ
Document Hit Rate（ドキュメント ヒット率）	全キャッシュ要求に対するキャッシュ ヒットの割合（10 秒間の平均値 ）。この値は 10 秒毎に更新されます。
Bandwidth Savings（帯域幅の節約）	全要求バイトに対するキャッシュから提供されたバイト数の割合（10 秒間の平均値 ）。この値は 10 秒毎に更新されます。
Cache Percent Free（キャッシュの空き容量の割合）	全キャッシュ容量に対するキャッシュ空き容量の割合。
	In Progress（処理中）
Open Server Connections（サーバー接続のオープン数）	オリジン サーバー接続の現在のオープン数。
Open Client Connections（クライアント接続のオープン数）	クライアント接続の現在のオープン数。
Cache Transfers in Progress（処理中のキャッシュ転送）	処理中のキャッシュ転送（キャッシュ読み込み / 書き込み）数。
	Network（ネットワーク）
Client Throughput（Mbit/Sec）（クライアント スループット）	ノード（およびクラスタ）の通過量 (Mbit/sec)。

統計情報	説明
Transactions per Second（秒当たりのトランザクション）	秒当たりの HTTP トランザクション数。
	Name Resolution（名前解決）
Host Database Hit Rate（ホスト データベースのヒット率）	ホスト データベース ルックアップの合計に対するホスト データベース ヒットの割合（10 秒間の平均値）。この値は 10 秒毎に更新されます。
DNS Lookups per Second（秒当たりの DNS ルックアップ）	秒当たりの DNS ルックアップ数。

グラフ

Help | Content Gateway | バージョン 7.8.x

グラフィックページには、*ノード*ページと同じ統計（キャッシュ パフォーマンス、現在の接続と転送量、ネットワーク、およびネーム レゾルーション）がグラフィック形式で表示されます。グラフに表示する統計を選択することができます。*統計の表示*、133 ページを参照してください。

重要

グラフは Java アプレットを使用しているブラウザに表示されます。使用する PC に Java の最新のバージョン（バージョン 1.7 以上）がインストールされている必要があります。Content Gateway 統計へのユーザーのアクセス権を検証するために、Content Gateway ログオン資格情報の入力が求められます。

アラーム

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway が問題（たとえば、イベント ログに割り当てられた容量が満杯の場合や、Content Gateway が設定ファイルに書き込めない場合）を検出した時、アラームを発生させ、アラーム メッセージ ウィンドウにアラームの説明を表示します。さらに、Content Gateway Manager 上部の **Alarm! [pending]** バーに、アラームがいつ検出されたか、存在するアラームの数を表示します。

アラーム メッセージを読んだ後、アラーム メッセージ ウィンドウ内の **[Clear（クリア）]** をクリックすると、アラームは削除されます。**[Clear]** をクリックするとアラーム メッセージを除去するだけです。アラームの原因を実際には解決しません。

アラームに関する情報は、*アラームの処理*、139 ページを参照してください。

プロトコル

Help | Content Gateway | バージョン 7.8.x

Protocol 統計は次のカテゴリに分けられます。

- *HTTP*、306 ページ
- *FTP*、308 ページ

SSL の統計情報については、[Monitor] タブの下部の [SSL] ボタンをクリックします。

HTTP

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	General（一般）
Client（クライアント）	
Total Document Bytes（ドキュメントの合計バイト）	インストール以降クライアントに提供された HTTP データの合計数。
Total Header Bytes（ヘッダーの合計バイト）	インストール以降クライアントに提供された HTTP ヘッダーの合計数。
Total Connections（接続の合計）	インストール以降の HTTP クライアント接続の合計数。
Current Connections（現在の接続）	HTTP クライアント接続の現在の数。
Transactions in Progress（処理中のトランザクション）	処理中の HTTP クライアント トランザクションの数。
Server（ サーバー）	
Total Document Bytes（ドキュメントの合計バイト）	インストール以降のオリジン サーバーから受信した HTTP データの合計数。
Total Header Bytes（ヘッダーの合計バイト）	インストール以降のオリジン サーバーから受信した HTTP ヘッダー データの合計数。
Total Connections（接続の合計）	インストール以降の HTTP サーバー接続の合計数。
Current Connections（現在の接続）	HTTP サーバー接続の現在の数。

統計情報	説明
Transactions in Progress（処理中のトランザクション）	進行中の HTTP サーバー接続の合計数。
	Transaction（トランザクション）
Hits（ヒット数）	
Fresh（最新性）	最新性ヒットのパーセンテージと平均処理時間。
Stale Revalidated（再確認され陳腐化）	陳腐化し、再確認され、最新となり、提供されているヒットのパーセンテージと平均処理時間。
Misses（ミス数）	
Now Cached（現在キャッシュ）	キャッシュ内に存在しなかった（現在は存在）ドキュメント要求のパーセンテージとその平均処理時間。
Server No Cache（サーバーキャッシュなし）	キャッシュ内に存在しないが、サーバーの no-cache ヘッダー（キャッシュ不可）を含む HTTP オブジェクト要求のパーセンテージとその平均処理時間。
Stale Reloaded（再ロードされ陳腐化）	再確認され、変更され、再ロードされて処理されたミスのパーセンテージとその平均処理時間。
Client No Cache（クライアント キャッシュなし）	クライアント no-cache ヘッダーを含むミスのパーセンテージとその平均処理時間。
Errors（エラー）	
Connection Failures（接続エラー）	接続エラーのパーセンテージとその平均処理時間。
Other Errors（その他のエラー）	その他のエラーのパーセンテージとその平均処理時間。
Aborted Transactions（トランザクション中断）	
Client Aborts（クライアントによる中断）	クライアントによる中断処理のパーセンテージとその平均処理時間。
Questionable Client Aborts（クライアントによると思われる中断）	クライアントが中断した可能性がある処理のパーセンテージとその平均処理時間。
Partial Request Hangups（部分要求ハングアップ）	部分要求後の初期ハングアップのパーセンテージとその平均処理時間。
Pre-Request Hangups（要求前ハングアップ）	Pre-Request ハングアップのパーセンテージとその平均処理時間。
Pre-Connect Hangups（接続前ハングアップ）	Pre-Connect ハングアップのパーセンテージとその平均処理時間。
Other Transactions（その他のトランザクション）	
Unclassified（未分類）	未分類処理のパーセンテージとその平均処理時間。

統計情報	説明
	HTTP 上の FTP
Connections（接続）	
Open Server Connections（サーバー接続のオープン数）	FTP サーバー接続をオープンした回数。
Successful PASV Connections（PASV 接続の成功数）	インストール以降 PASV 接続に成功した回数。
Failed PASV Connections（PASV 接続の失敗数）	インストール以降 PASV 接続に失敗した回数。
Successful PORT Connections（PORT 接続の成功数）	インストール以降 PORT 接続に成功した回数。
Failed PORT Connections（PORT 接続の失敗数）	インストール以降 PORT 接続に失敗した回数。
Cache Statistics（キャッシュ統計）	
Hits（ヒット数）	キャッシュから提供された FTP オブジェクトの HTTP 要求数。
Misses（ミス数）	オブジェクトがキャッシュ内に存在しないか無効のために、オリジン サーバーに直接転送された FTP オブジェクトの HTTP 要求の数。
Lookups（ルックアップ）	Content Gateway が、キャッシュ内の FTP オブジェクトの HTTP 要求をルックアップした回数。

FTP

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Client（クライアント）
Open Connections（接続オープン数）	現在オープンされているクライアント接続の数。
Bytes Read（読み込みバイト数）	インストール以降、読み込まれたクライアント要求のバイト数。
Bytes Written（書き込みバイト数）	インストール以降、書き込まれたクライアント要求のバイト数。
	Server（サーバー）
Open Connections（接続オープン数）	現在オープンされている FTP サーバー接続の数。

統計情報	説明
Bytes Read （読み込みバイト数）	インストール以降、FTP サーバーから読み込まれたバイト数。
Bytes Written （書き込みバイト数）	インストール以降、キャッシュに書き込まれたバイト数。

セキュリティ

Help | Content Gateway | バージョン 7.8.x

セキュリティ 統計は次のカテゴリに分けられます。

- *統合 Windows 認証*、309 ページ
- *LDAP*、312 ページ
- *レガシー NTLM*、313 ページ
- *SOCKS*、313 ページ
- *Data Security*、314 ページ

> **注意**
> 複数の認証ルール使用している場合でも、Content Gateway は、各認証方法（IWA、LDAP、Legacy NTLM）の認証統計を個別にレポートします。

統合 Windows 認証

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Diagnostic Test（診断テスト） この機能は、選択されたドメインに対してケルベロス接続を行う場合に診断テストを実行します。結果は、画面上と /opt/WCG/logs/content_gateway.out および /opt/WCG/logs/smbadmin.log に書き込まれます。
Domain ドロップダウンボックス	接続されているドメインを選択します。ルール ベースの認証が設定されていない限り、接続されているドメインは 1 つのみです。
Run Test ボタン	クリックするとテストを開始します。

統計情報	説明
	Active Directory Joined Domains（Active Directory 結合済みドメイン）リスト 結合済みのすべての AD ドメインをリストします。 **Content Gateway Hostname DNS（Content Gateway ホスト名 DNS）**は、クライアントが Kerberos 認証を行うためにブラウザ プロキシ設定で指定しなければならない名前です。
	Kerberos request counters（Kerberos 要求カウンタ）
Total Kerberos requests（Kerberos 要求の合計数）	Kerberos 認証要求の合計数。
Authentication succeeded（認証成功数）	認証に成功した Kerberos 認証要求の数。
Authentication failed（認証失敗数）	認証に失敗した Kerberos 認証要求の数。
Kerberos errors（Kerberos エラー数）	Kerberos プロセス エラーの数。
	NTLM request counters（NTLM 要求カウンタ）
Total NTLM requests（NTLM 要求の合計数）	NTLM 認証要求の合計数。
Authentication succeeded（認証成功数）	認証に成功した NTLM 認証要求の数。
Authentication failed（認証失敗数）	認証に失敗した NTLM 認証要求の数。
NTLM request errors（NTLM 要求エラーの数）	NTLM プロセス エラーの数。
NTLM within negotiate requests（ネゴシエーション要求内の NTLM 要求）	ネゴシエーション要求内にカプセル化された NTLM 要求の数。
	Basic authentication request counters（Basic 認証要求カウンタ）
Total basic authentication requests（Basic 認証要求の合計数）	Basic 認証要求の合計数。
Authentication succeeded（認証成功数）	認証に成功した Basic 認証要求の数。
Authentication failed（認証失敗数）	認証に失敗した Basic 認証要求の数。
Basic authentication request errors（Basic 認証要求エラー）	Basic 認証処理エラーの数。

統計情報	説明
	Performance counters（パフォーマンス カウンタ）
Kerberos - Average time per transaction（Kerberos トランザクション平均時間）	Kerberos トランザクションを完了するまでの平均時間（単位ミリ秒）。
NTLM - Average time per transaction（NTLM トランザクション平均時間）	NTLM トランザクションを完了するまでの平均時間（単位ミリ秒）。
Basic - Average time per transaction（Basic トランザクション平均時間）	Basic トランザクションを完了するまでの平均時間（単位ミリ秒）。
Average helper latency per transaction（ヘルパー遅延トランザクション平均時間）	Samba の認証要求を処理する平均時間。
Time authentication spent offline（認証オフィライン時間）	サービスまたは接続性の障害のために、Content Gateway が NTLM 認証を実行できなかった時間（単位秒）。（DC と通信する必要がないため、この測定は Kerberos に適用されません。） Global Fail Open オプションが有効化されている（*グローバル認証オプション*）場合、プロキシ要求は認証なしに続行されます。 障害の後、接続が再確立した時に、カウンタは増加します。
Number of times authentication servers or services went offline（認証サーバーまたはサービスがオフラインになった回数）	認証サーバーまたはサービスとの接続性が失われた回数。
	上位リスト カウンタ これらのユーザー認証リストは、最もアクティブな User-Agent 値およびクライアント IP アドレスの一覧を表示します。4 つのカウンタは、ユーザー認証に合格または失敗した回数が最も多い 20 の User-Agent とクライアント IP アドレスを集計します。
ボタン：Reset Top Lists to Zero（上位リストを 0 にリセット）	すべての上位リストのカウンタを 0 にリセットします。
Top User-Agents passing authentication（認証に合格した上位 User-Agent）	合格した認証の試みの回数が最も多い 20 の User-Agent マッチングをリストします。
Top User-Agents failing authentication（認証に失敗した上位 User-Agent）	失敗した認証の試みの回数が最も多い 20 の User-Agent マッチングをリストします。

統計情報	説明
Top Client IP addresses passing authentication（認証に合格した上位 クライアント IP アドレス）	合格した認証の試みの回数が最も多い 20 の IP アドレスをリストします。
Top Client IP addresses failing authentication（認証に失敗した上位 クライアント IP アドレス）	失敗した認証の試みの回数が最も多い 20 の IP アドレスをリストします。

LDAP

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Cache（キャッシュ）
Hits（ヒット数）	LDAP キャッシュのヒット回数。
Misses（ミス数）	LDAP キャッシュのミス回数。
	Errors（エラー）
Server（ サーバー）	LDAP サーバーエラーの回数。
	認証成功（7.8.2）
Authentication succeeded（認証成功数）	認証が成功した回数。
	Unsuccessful Authentications（認証失敗回数）
Authentication Denied（認証拒否数）	LDAP サーバーが認証を拒否した回数。
Authentication Timeouts（認証タイムアウト）	認証がタイムアウトになった回数。
Authentication Cancelled（認証キャンセル回数）	LDAP 認証を開始し完了する前に、終了してしまった回数。 **ご注意：**クライアントが資格情報を要求するダイアログボックス内の [Cancel] をクリックして、認証をキャンセルした場合は、ここではカウント**されません**。

レガシー NTLM

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Cache（キャッシュ）
Hits（ヒット数）	NTLM キャッシュのヒット回数。
Misses（ミス数）	NTLM キャッシュのミスの回数。
	Errors（エラー）
Server（ サーバー）	NTLM サーバーエラーの回数。
	認証成功（7.8.2）
Authentication succeeded（認証成功数）	認証が成功した回数。
	Unsuccessful Authentications（認証失敗回数）
Authentication Denied（認証拒否数）	NTLM サーバーが認証を拒否した回数。
Authentication Cancelled（認証キャンセル回数）	認証がキャンセルされた回数。
Authentication Rejected（認証リジェクト回数）	キューが満杯のために認証が失敗した回数。
	Queue Size（キューのサイズ）
Authentication Queued（キューに入っている認証数）	すべてのドメイン コントローラがビジーのため、現在キューに入れられている要求の数。

SOCKS

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
On-Appliance SOCKS Server（V シリーズ アプライアンス上に Content Gateway が存在する場合）	アプライアンス上の SOCKS サーバーがオン（有効化）かオフ（無効化）かを示します。
Unsuccessful Connections（接続失敗回数）	Content Gateway を起動して以降、SOCKS サーバーとの接続に失敗した回数。
Successful Cconnections（接続成功回数）	Content Gateway を起動して以降、SOCKS サーバーとの接続に成功した回数。
Connections in Progress（現在の接続数）	現在の SOCKS サーバー接続の数。

Data Security

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
Total Posts （転送の合計数）	Data Security への転送の合計数。
Total Analyzed （分析の合計数）	Data Security で分析した転送の合計数。
FTP Analyzed （FTP 分析の合計数）	Data Security で分析した FTP 要求の合計数。
Blocked Requests （ブロックされた要求数）	分析およびポリシーの実施後に、ブロックされた要求の合計数。
Allowed Requests （許可された要求数）	分析およびポリシーの実施後に、許可された要求の合計数。
Failed Requests （失敗した要求数）	Data Security へ送信され、タイムアウトまたはその他の原因で完了しなかった転送の合計数。
Huge Requests （超過要求数）	最大 トランザクション サイズを超過した要求の合計数。
Tiny Requests （不足要求数）	最小トランザクション サイズより小さい要求の合計数。
Decrypted Requests （復号化要求数）	復号化され、Data Security に送信された SSL 要求の合計数。
Total Bytes Scanned （スキャン合計バイト数）	Data Security でスキャンされた合計バイト数。
Average Response Time （平均応答時間）	Content Gateway が最後に起動して以降の、Data Security がスキャンを完了するまでに必要とした平均時間。

Subsystems（サブシステム）

Help | Content Gateway | バージョン 7.8.x

サブシステム統計は下記のカテゴリに分けられます。

- *キャッシュ*、315 ページ
- *Clustering（クラスタ化）*、316 ページ
- *Logging（ログ記録）*、316 ページ

キャッシュ

Help | Content Gateway | バージョン 7.8.x

> **注意**
> Content Gateway に送信されたすべてのコンテンツがキャッシュ不可の場合でも、キャッシュ統計 はゼロではない場合があります。クライアントが no-cache ヘッダーを送信した場合でも、Content Gateway はキャッシュ読み込みを実行します。

統計情報	説明
	General（一般）
Bytes Used（使用バイト数）	現在キャッシュに使用されているバイト数。
Cache Size（キャッシュサイズ）	キャッシュに割り当てられているバイト数。
	Ram Cache（RAM キャッシュ）
Bytes（バイト数）	RAM キャッシュの合計サイズ（バイト単位）。
Hits（ヒット数）	RAM キャッシュにヒットしたドキュメント数。
Misses（ミス数）	RAM キャッシュにヒットしなかったキュメント数。ドキュメントは キャッシュ ディスクにヒットすることがあります。
	Reads（読み込み）
In Progress（処理中）	現在読み込み中のキャッシュの数（HTTP および FTP）。
Hits（ヒット数）	Content Gateway が起動して以降、キャッシュ読み込みを完了した回数（HTTP および FTP）。
Misses（ミス数）	Content Gateway が起動して以降、キャッシュ読み込みをミスした回数（HTTP および FTP）。
	Writes（書き込み）
In Progress（処理中）	現在書き込み中のキャッシュ数（HTTP および FTP）。
Successes（成功回数）	Content Gateway が起動して以降の、キャッシュ書き込み成功回数（HTTP および FTP）。
Failures（失敗回数）	Content Gateway が起動して以降の、キャッシュ書き込み失敗回数（HTTP および FTP）。

統計情報	説明
	Updates（更新）
In Progress（処理中）	現在更新中の HTTP ドキュメントの数。Content Gateway がオブジェクトを再確認し、最新であることを検出し、オブジェクト ヘッダーを更新した時に、更新が発生します。
Successes（成功回数）	Content Gateway が起動して以降、HTTP キャッシュ更新に成功した回数。
Failures（失敗回数）	Content Gateway が起動して以降、HTTP キャッシュ更新に失敗した回数。
	Removes（削除）
In Progress（処理中）	現在削除中のドキュメントの数。Content Gateway がドキュメントを再確認し、オリジン サーバー上で削除するドキュメントを発見し、キャッシュ から削除（HTTP および FTP を含む）した時に、削除が発生します。
Successes（成功回数）	Content Gateway が起動して以降、キャッシュの削除に成功した回数。
Failures（失敗回数）	Content Gateway が起動して以降、キャッシュの削除に失敗した回数（HTTP および FTP を含む）。

Clustering（クラスタ化）

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
Clustering Nodes（クラスタリング ノード数）	クラスタリング ノードの数。

Logging（ログ記録）

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
Currently Open Log Files（現在オープン中のログ ファイル数）	現在書き込み中の event log ファイル（フォーマット）の数。
Space Used for Log Files（ログ ファイル使用容量）	ログ記録ディレクトリ（すべてのイベント、およびエラー ログを保持）に使用されている現在の容量。

統計情報	説明
Number of Access Events Logged（アクセス イベントのログ数）	Content Gateway インストール以降、ログ ファイルに書き込まれたアクセス イベントの数。このカウンタは 1 つのファイルに 1 つのエントリを表します。複数のフォーマットが書き込まれると、単一のイベントによって複数のイベント ログ エントリが作成されます。
Number of Access Events Skipped（アクセス イベントのスキップ数）	Content Gateway インストール以降、（フィルタリングによって撥ねられたために）スキップされたアクセス イベントの数。
Number of Error Events Logged（イベント エラーのログ数）	Content Gateway インストール以降、イベント エラー ログに書き込まれたアクセス イベントの数。

ネットワーク

Help | Content Gateway | バージョン 7.8.x

ネットワーク統計は次のカテゴリに分けられます。

- *システム*、317 ページ
- *ARM*、318 ページ
- *ICAP*、320 ページ
- *WCCP*、320 ページ
- *DNS リゾルバ*、322 ページ
- *仮想 IP*、322 ページ

システム

Help | Content Gateway | バージョン 7.8.x

統計情報 / フィールド	説明
	General（一般）
Hostname（ホスト名）	Content Gateway コンピュータに割り当てられたホスト名。
Search Domain（検索ドメイン）	Content Gateway コンピュータが使用する検索ドメイン。
IPv4 または IPv6	

統計情報 / フィールド	説明
Default Gateway（デフォルト ゲートウェイ）	Content Gateway コンピュータから、他のネットワークまたはサブネットに、パケット転送を行うために使用するデフォルト ゲートウェイの IP アドレス。
Primary DNS（一次 DNS）	Content Gateway コンピュータが、ホスト名の解決に使用する一次 DNS サーバーの IP アドレス。
Secondary DNS（二次 DNS）	Content Gateway コンピュータが、ホスト名の解決に使用する二次 DNS サーバーの IP アドレス。
Tertiary DNS（三次 DNS）	Content Gateway コンピュータが、ホスト名の解決に使用する三次 DNS サーバーの IP アドレス。
	NIC <*interface_name*>
Status（ステータス）	NIC が動作中か停止中かを示します。
Start on Boot（起動時開始）	NIC が起動時に開始するよう設定されているかを示します。
IPv4 または IPv6	
IP アドレス	NIC に割り当てられた IP アドレス。
Netmask（ネットマスク）	IP アドレスのネットマスク。
Gateway（ゲートウェイ）	NIC に設定されたデフォルト ゲートウェイの IP アドレス。

ARM

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	Network Address Translation (NAT) Statistics（ネットワーク アドレス変換（NAT）統計）
Client Connections Natted（変換されたクライアント接続数）	ARM によって透過的にリダイレクトされたクライアント接続の数。
Client Connections in Progress（処理中の接続数）	ARM によって現在処理中のクライアント接続数。
Total Packets Natted（変換されたパケットの合計数）	ARM によって変換されたパケットの数。

統計情報	説明
DNS Packets Natted（変換された DNS パケットの合計数）	ARM によって変換された DNS パケットの数。
	Bypass Statistics（バイパス統計）
Total Connections Bypassed（バイパスされた接続の合計数）	ARM によってバイパスされた接続の合計数。
Connections Dynamically Bypassed（動的にバイパスされた接続の合計数）	動的にバイパスされた接続の合計数。*動的バイパス ルール、89 ページ*を参照してください。
DNS Packets Bypassed（バイパスされた DNS パケットの合計数）	ARM によってバイパスされた DNS パケットの数。
Connections Shed（放棄された接続の合計数）	放棄された接続の合計数。*接続負荷の軽減、92 ページ*を参照してください。
	HTTP Bypass Statistics（HTTP バイパス統計）
Bypass on Bad Client Request（不正クライアント要求によるバイパス）	Content Gateway が ポート 80 上で非 HTTP トラフィックを検出したために、直接オリジン サーバーに転送された要求の数。
Bypass on 400	オリジン サーバーが 400 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 401	オリジン サーバーが 401 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 403	オリジン サーバーが 403 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 405	オリジン サーバーが 405 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 406	オリジン サーバーが 406 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 408	オリジン サーバーが 408 エラーを返したために、オリジン サーバーに直接転送された要求の数。
Bypass on 500	オリジン サーバーが 500 エラーを返したために、オリジン サーバーに直接転送された要求の数。

ICAP

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
Total Posts（転送の合計数）	Data Security への転送の合計数。
Total Analyzed（分析の合計数）	Data Security で分析した転送の合計数。
FTP Analyzed（FTP 分析の合計数）	Data Security で分析した FTP 要求の合計数。
Blocked Requests（ブロックされた要求数）	分析およびポリシーの実施後に、ブロックされた要求の合計数。
Allowed Requests（許可された要求数）	分析およびポリシーの実施後に、許可された要求の合計数。
Failed Requests（失敗した要求数）	Data Security へ送信され、タイムアウトまたはその他の原因で完了しなかった転送の合計数。
Huge Requests（超過要求数）	最大 トランザクション サイズを超過した要求の合計数。
Decrypted Requests（復号化要求数）	復号化され、Data Security に送信された SSL 要求の合計数。

WCCP

Help | Content Gateway | バージョン 7.8.x

WCCP バージョン v2 が有効化されている場合にのみ、WCCP v2 統計が表示されます。

統計情報 / フィールド	説明
	WCCP v2.0 Statistics（WCCP v2.0 統計）
WCCP Fragmentation（WCCP フラグメント）	
Total Fragments（フラグメントの合計数）	WCCP フラグメントの合計数。
Fragmentation Table Entries（フラグメント テーブルのエントリ数）	フラグメント テーブル内のエントリ数。

統計情報 / フィールド	説明
Out of Order Fragments（順番に並んでいないフラグメントの数）	順番に並んでいないフラグメントの数。
Matches（フラグメント一致数）	フラグメント テーブル内のフラグメントと一致しているフラグメントの数。
Service group name（サービス グループの名前）	
Service Group ID（サービス グループの ID）	サービスが提供されているプロトコルのサービス グループの ID
Configured mode（設定モード）	転送、返送、割り当ての設定。
IP Address（IP アドレス）	ルーターが トラフィックを送信している IP アドレス。
Leader's IP Address（リーダーの IP アドレス）	WCCP キャッシュ ファームのリーダーの IP アドレス。
Number of Buckets Assigned（割り当てられたバケット数）	Content Gateway ノードに割り当てられているバケット数。Weight 値と現在のアクティブ ノードによって決定されます。
Number of Caches（キャッシュ数）	WCCP キャッシュ ファームに存在するキャッシュの数。
Number of Routers（ルーター数）	Content Gateway ノードにトラフィックを送信しているルーターの数。
Router IP Address（IP アドレス）	Content Gateway ノードにトラフィックを送信している WCCP ルーターの IP アドレス。 **ご注意：**WCCP ルーターに複数の IP アドレスが設定されている場合 — たとえばルーターが複数の VLAN をサポートするように設定されている時、**[Monitor] > [Networking] > [WCCP]** の統計で報告される IP アドレスが、ここで設定される IP アドレスと異なる場合があります。これは、ルーターが常に最も高いアクティブ IP アドレスにおけるトラフィックを報告するからです。 ルーターが常に同じ IP アドレスを報告するようにする 1 つの方法は、ルーターのループバック アドレスをルーターの最も高い IP アドレスよりも高い値に設定することです。それによってループバック アドレスが常にルーターの IP アドレスとして報告されるようになります。この設定を使用することを推奨します。
Router ID Received（ルーター ID 受信回数）	Content Gateway が、ルーターから WCCP プロトコル メッセージを受信した回数。
Router Negotiated mode（ルーター ネゴシエーション モード）	ルーターとネゴシエーションされた転送、返送、割り当てモード。

DNS プロキシ

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
Total Requests（要求の合計数）	クライアントから受信した DNS 要求の合計数。
Hits（ヒット数）	DNS キャッシュ ヒットの数。
Misses（ミス数）	DNS キャッシュ ミスの数。

DNS リゾルバ

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	DNS Resolver（DNS リゾルバ）
Total Lookups（ルックアップの合計数）	インストール以降の DNS ルックアップ（DNS ネームサーバーへのクエリー）の合計数。
Successes（成功回数）	インストール以降の DNS ルックアップ成功の合計回数。
Average Lookup Time (ms)（平均ルックアップ時間）	DNS ルックアップの平均時間。
	Host Database（ホスト データベース）
Total Lookups（ルックアップの合計数）	インストール以降、Content Gateway ホスト データベースをルックアップ した合計回数。
Total Hits（ヒット合計回数）	インストール以降、ホスト データベースにヒットした合計回数。
Average TTL (min)（平均 TTL）	平均継続時間（分単位）。

仮想 IP

Help | Content Gateway | バージョン 7.8.x

仮想 IP テーブルは、クラスタ内のプロキシによって管理されている仮想 IP アドレスを表示します。

クライアント接続の状態

Help | Content Gateway | バージョン 7.8.x

統計情報	説明
	クライアント接続
Current Unique Clients Connected（現在接続中の一意なクライアントの数）	
Total Unique Clients that have Connected（接続が完了した一意なクライアントの合計数）	Content Gateway が最後に起動して以降の合計数。
Total Clients that have Exceeded the Limits（制限を超えたクライアントの合計数）	Content Gateway が最後に起動して以降の接続制限を超えたクライアントの合計数。[Configure] > [Connection Management（接続管理）] > [Client Connection Control（クライアント接続の制御）] を参照。
Total Clients for which Connections were Closed（接続が閉じたクライアントの合計数）	Content Gateway が最後に起動して以降の合計数。

パフォーマンス

Help | Content Gateway | バージョン 7.8.x

パフォーマンス グラフによって、Websense Content Gateway のパフォーマンスをモニタし、ネットワーク トラフィックを分析することができます。また、パフォーマンス グラフは、仮想メモリ使用量、クライアント接続、ドキュメント ヒット率などに関する情報を示します。パフォーマンス グラフは、Multi Router Traffic Grapher ツール（MRTG）によって作成されます。MRTG は、5 分間隔で 統計情報を累積します。

パフォーマンス グラフは、次の情報を提供します。

統計情報	説明
Overview（概要）	利用可能なグラフのサブセットを表示します。
Daily（毎日）	現在の日付の履歴情報を示すクラフを表示します。
Weekly（毎週）	現在の週の履歴情報を示すクラフを表示します。
Monthly（毎月）	現在の月の履歴情報を示すクラフを表示します。
Yearly（毎年）	現在の年の履歴情報を示すクラフを表示します。

重要

Multi Router Traffic Grapher（パフォーマンス グラフ表示ツール）を実行するには、Content Gateway システム上に Perl バージョン 5.005 以上をインストールしている必要があります。

グラフの横に説明が表示されます。1 つの画面で、毎日、毎週、毎月、毎年を表示するには、グラフをクリックします。

下記のグラフが利用可能です（アルファベット順にソートされます）。

- Active Client Connections（アクティブなクライアントの接続の数）
- Active Native FTP Client Connections（アクティブなネーティブ FTP クライアントの接続の数）
- Active Origin Server Connections（アクティブなオリジン サーバーの接続の数）
- Active Parent Proxy Connections（アクティブな親プロキシの接続の数）
- Bandwidth Savings（帯域幅の節約）
- Cache Read（キャッシュ読み込みの数）
- Cache Reads Per Second（1 秒あたりのキャッシュ読み込みの回数）
- Cache Writes（キャッシュ書き込みの数）
- Cache Writes Per Second（1 秒あたりのキャッシュ書き込みの回数）
- 1 秒あたりの完了したクライアント トランザクションの数
- Content Gateway Manager Memory Usage（Content Gateway manager のメモリの使用状況）
- Content Gateway Uptime（Content Gateway の稼働時間）
- CPU Available（CPU 利用可能状況）
- CPU Busy（CPU ビジー）
- Data Security Module Memory Usage（Data Security モジュール メモリの使用状況）
- Disk Cache Usage（ディスク キャッシュの使用状況）
- DNS Cache Usage（DNS キャッシュの使用状況）
- DNS Lookup Latency（DNS ルックアップ遅延）
- HTTP Abort Latency（HTTP 中断遅延）
- HTTP and HTTPS Transactions Per Second（秒あたりの HTTP および HTTPS トランザクションの数）
- HTTP Cache Hit Latency（HTTP キャッシュ ヒットの遅延）
- HTTP Cache Miss Latency（HTTP キャッシュ ミスの遅延）
- HTTP Connection Errors & Aborts (Count)（HTTP 接続エラーおよび中断（回数））

- HTTP Connection Errors & Aborts (Percentage)（HTTP 接続エラーおよび中断（パーセンテージ））
- HTTP Document Hit Rate（HTTP ドキュメント ヒット率）
- HTTP Error Latency（HTTP エラー遅延）
- HTTP Hits & Misses (Count)（HTTP ヒットおよびミス（回数））
- HTTP Hits & Misses (Percentage)（HTTP ヒットおよびミス（パーセンテージ））
- HTTP POST and FTP PUT Transactions Per Second（秒あたりの HTTP POST および FTP PUT トランザクションの数）
- Microsoft Internet Explorer Browser Requests (Percentage)（Microsoft Internet Explorer のブラウザの要求（パーセンテージ））
- MRTG Runtime（MRTG 実行時間）
- Network Reads（ネットワークの読み込みの数）
- Network Writes（ネットワーク書き込みの数）
- RAM Cache Read I/O Hit Rate（RAM キャッシュ読み込み I/O ヒット率）
- RAM Cache Usage（RAM キャッシュの使用状況）
- TCP CLOSE_WAIT Connections（TCP CLOSE_WAIT の接続回数）
- TCP Connect Rate（TCP 接続速度）
- TCP ESTABLISHED Connections（確立された TCP 接続の数）
- TCP FIN_WAIT_1 Connections（TCP FIN_WAIT_1 接続の数）
- TCP FIN_WAIT_2 Connections（TCP FIN_WAIT_2 接続の数）
- TCP LAST_ACK Connections（TCP LAST_ACK 接続の数）
- TCP Segments Transmitted（送信された TCP セグメントの数）
- TCP Throughput（TCP スループット）
- TCP TIME_WAIT Connections（TCP TIME_WAIT 接続の数）
- Transaction Buffer Memory Usage（トランザクション バッファ メモリの使用状況）
- WCCP Exceptional Input Fragments（WCCP 例外入力フラグメントの数）
- WCCP Fragment Table Size（WCCP フラグメント テーブルのサイズ）
- WCCP Input Fragments（WCCP 入力フラグメントの数）
- Web Security Scanned Transactions（Percentage）（Web Security スキャン済みトランザクションの数（パーセンテージ））
- Web Security Slow Scanned Transactions（Web Security 低速スキャンされたトランザクションの数）
- Web Security Slow Transactions（Web Security 低速トランザクションの数）
- Websense Content Gateway Memory Usage（Websense Content Gateway メモリの使用状況）

SSL

Help | Content Gateway | バージョン 7.8.x

下記のタブは、SSL トラフィックをモニタし、レポートします。

SSL Key Data（SSL キー データ）、326 ページ

CRL Statistics（CRL 統計）、327 ページ

レポート、327 ページ

SSL Key Data（SSL キー データ）

Help | Content Gateway | バージョン 7.8.x

下記のフィールドは SSL 接続およびアクティビティに関する情報を提供します。

統計情報 / フィールド	説明
	SSL Inbound Key Data（SSL インバウンド キー データ）
Is alive（動作中）	Online は SSL サポートが有効化されていることを示します。
Current SSL connections（現在の SSL 接続の数）	（ブラウザから Content Gateway への）アクティブなインバウンド SSL 要求の数。
Total SSL server connections（SSL サーバー接続の合計数）	ブラウザ要求の数。
Total finished SSL server connections（完了した SS L サーバー接続の合計数）	復号化されたブラウザ要求の数。
Total SSL server renegotiation requests（SSL サーバー ネゴシエーションの合計数）	ブラウザと Content Gateway 間のハンドシェークが失敗、または証明書が無効のために、再ネゴシエーションされたブラウザ要求の数。
	SSL Outbound Key Data（SSL アウトバウンド キー データ）
Is alive（動作中）	Online は SSL サポートが有効化されていることを示します。
Current SSL connections（現在の SSL 接続の数）	（Content Gateway からオリジン サーバーへの）アクティブなアウトバウンド SSL 要求の数。
Total SSL client connections（SSL クライアント接続の合計数）	オリジン サーバへの Content Gateway の要求の数

統計情報 / フィールド	説明
Total finished SSL client connections（完了した SSL クライアント接続の合計数）	Content Gateway からオリジン サーバーにデータが送信された要求の数
Total SSL client renegotiation requests（SSL クライアント ネゴシエーションの合計数）	Content Gateway とオリジン サーバー間のハンドシェークが失敗、または証明書が無効のために、再ネゴシエーションされた要求の数。
Total SSL session cache hits（SSL セッション キャッシュ ヒット回数）	セッション キャッシュ内のキーによって、要求が検証された回数。
Total SSL session cache misses（SSL セッション キャッシュ ミス回数）	セッション キャッシュ内のキーによって、要求が検証できなかった回数。
Total SSL session cache misses（SSL セッション タイムアウト回数）	タイムアウト時間が切れために、キーがセッション キャッシュから削除された回数。

CRL Statistics（CRL 統計）

Help | Content Gateway | バージョン 7.8.x

下記のフィールドは証明書のステータスについての情報を提供します。

統計情報 / フィールド	説明
	CRL Statistics（CRL 統計）
CRL list count（CRL リスト数）	証明書取り消しリストの証明書の数。このリストは毎晩ダウンロードされます。*最新の取り消し情報を保持する、186 ページを参照してください。*
	OCSP Statistics（OCSP 統計）
OCSP good count（OCSP 有効数）	証明書が有効である応答の数。
OCSP unknown count（OCSP 未知の数）	証明書が認証されなかった OCSP 応答の数。
OCSP revoked count（OCSP 取り消し 数）	取り消されたことがわかった証明書の数。

レポート

Help | Content Gateway | バージョン 7.8.x

認証機関またはインシデントのレポートを作成するための情報は、*SSL 関連レポートの作成、142 ページ*を参照してください。

B コマンドと変数

Websense Content Gateway のコマンド

個別のコマンドを実行するか、シェルの中に複数のコマンドを記述するときに、コマンドラインを使用します。

コマンドを実行するために、root に移動します：

```
su
```

Content Gateway **bin** ディレクトリから、Content Gateway のコマンドを実行します。

> **注意**
>
> Content Gateway **bin** ディレクトリがパスにない場合、コマンドの先頭に下記の記号を追加します：
>
> ```
> ./
> ```
>
> 例：
>
> ```
> ./content_line -p
> ```

コマンド	説明
`WCGAdmin start`	Content Gateway サービスを起動します。
`WCGAdmin stop`	Content Gateway サービスを停止します。
`WCGAdmin restart`	Content Gateway サービスを停止し、その後再起動します。
`WCGAdmin status`	次の Content Gateway サービスのステータス（実行中または停止中）を表示します。Content Cop、Content Gateway、Content Gateway Manager、および Analytics Server。
`WCGAdmin help`	WCGAdmin コマンドのリストを表示します。
`content_line -h`	Content Gateway コマンドのリストを表示します。

コマンド	説明
`content_line -p socket_path`	Content Gateway コマンド ラインと Content Gateway マネージャの通信で使用するファイルの位置（ディレクトリとパス）を指定します。デフォルト パスは **install_dir/config/cli** です。
`content_line -r variable`	指定されたパフォーマンス統計または現在の設定値を表示します。指定できる変数のリストについては、*Websense Content Gateway の変数*、330 ページを参照してください。
`content_line -s variable -v value`	設定変数を設定します。*variable* は、変更する設定変数であり、*value* は設定する値です。指定できる設定変数のリストについては、*records.config*、474 ページを参照してください。
`content_line -x`	Content Gateway 設定ファイルの再読み込みを開始します。このコマンドを実行することは、Content Gateway マネージャの **[Apply（適用）]** をクリックすること似ています。
`content_line -y`	キャッシュおよび SSL sqlite データベースから Websense の動的署名証明書を消去します。
`content_line db_clear -y`	Content Gateway が次に停止または再起動するとき、SSL sqlite データベースから Websense の動的署名証明書を消去します。
`content_line -M`	クラスタ内のすべてのノード上の **content_manager** プロセスと **content_gateway** プロセスを再起動します。
`content_line -L`	ローカル ノード上の **content_manager** プロセスと **content_gateway** プロセスを再起動します。
`content_line -S`	ローカル ノード上の Content Gateway を停止します。
`content_line -U`	ローカル ノード上の Content Gateway を起動します。
`content_line -B`	Content Gateway をクラスタ全体に渡って再起動します。ノード毎に Content Gateway を停止し即座にプロキシを再起動します。
`content_line -b`	ローカルノード上の Content Gateway を再起動します。ローカルノード上で Content Gateway を停止し即座にプロキシを再起動します。

Websense Content Gateway の変数

Help | Content Gateway | バージョン 7.8.x

content_line -s コマンドを使用して、コマンド ライン上で指定の構成変数の値を変更することができます。設定できる変数については、*records.config*、474 ページを参照してください。

content_line -r コマンドを使用して、コマンド ライン上で指定の変数に関連する統計を表示することができます。変数のリストは、下記を参照してください。

また、*コマンドラインからの統計の表示*、138 ページおよび*コマンドライン インターフェース*、129 ページを参照してください。

統計情報

Help | Content Gateway | バージョン 7.8.x

次の表は、個々の統計を表示させるために、コマンド ライン上で指定できる変数をリストしています。詳細は*統計*、301 ページを参照してください。

統計を表示させるためには、プロンプトで次のように入力します：

```
content_line -r variable
```

統計情報	変数
	Summary（要約）
Node name（ノード名）	*proxy.node.hostname*
Objects served（処理されたオブジェクト）	*proxy.node.user_agents_total_documents_served*
Transactions per second（秒あたりのトランザクションの数）	*proxy.node.user_agent_xacts_per_second*
	Node（ノード）
Document hit rate（ドキュメント ヒット率）	*proxy.node.cache_hit_ratio_avg_10s* *proxy.cluster.cache_hit_ratio_avg_10s*
Bandwidth savings（帯域幅の節約）	*proxy.node.bandwidth_hit_ratio_avg_10s* *proxy.cluster.bandwidth_hit_ratio_avg_10s*
Cache percent free（キャッシュの空き容量の割合）	*proxy.node.cache.percent_free* *proxy.cluster.cache.percent_free*
Open origin server connections（オープンなオリジン サーバー接続の数）	*proxy.node.current_server_connections* *proxy.cluster.current_server_connections*
Open client connections（オープンなクライアント接続の数）	*proxy.node.current_client_connections* *proxy.cluster.current_client_connections*
Cache transfers in progress（進行中のキャッシュ転送 ）	*proxy.node.current_cache_connections* *proxy.cluster.current_cache_connections*

統計情報	変数
Client throughput (Mbits/sec)（クライアント スループット (Mbits/sec)）	*proxy.node.client_throughput_out* *proxy.cluster.client_throughput_out*
Transactions per second（秒あたりのトランザクションの数）	*proxy.node.http.user_agent_xacts_per_second* *proxy.cluster.http.user_agent_xacts_per_second*
DNS lookups per second（秒あたりの DNS ルックアップの数）	*proxy.node.dns.lookups_per_second* *proxy.cluster.dns.lookups_per_second*
Host database hit rate（ホスト データベースのヒット率）	*proxy.node.hostdb.hit_ratio_avg_10s* *proxy.cluster.hostdb.hit_ratio_avg_10s*
	HTTP
Total document bytes from client（クライアントからのドキュメントの合計のバイト数）	*proxy.process.http.* *user_agent_response_document_total_size*
Total document bytes from client（クライアントからのヘッダーの合計バイト数）	*proxy.process.http.* *user_agent_response_header_total_size*
Total response header bytes to client from cache（キャッシュからクライアントへのヘッダーの合計のバイト数）	*proxy.process.http.* *user_agent_response_from_cache_header_total_size*
Total response header bytes to client from cache（キャッシュからクライアントへの応答ヘッダーの合計のバイト数）	*proxy.process.http.user_agent_response_* *from_cache_document_total_size*
Total connections to client（クライアントへの接続の合計数）	*proxy.process.http.current_client_connections*
Current unique clients connected（現在接続中の一意なクライアントの数）	*proxy.process.http.client.unique_clients.active*
Total unique clients that have connected（接続が完了した一意なクライアントの合計数）	*proxy.process.http.client.unique_clients.total*

統計情報	変数
Total clients that exceeded limit（限界数を超過したクライアントの合計数）	*proxy.process.http.client.exceeding_limit*
Total clients for which connections were closed（接続が閉じたクライアントの合計数）	*proxy.process.http.client.closed_connections*
Open HTTP client connections（オープンな HTTP クライアント接続の数）	*proxy.process.http.current_active_http_client_connections*
Open HTTPS client connections（オープンな HTTPS クライアント接続の数）	*proxy.node.process.http.current_active_https_client_connections*
Client Requests (IPv4 +IPv6)（クライアント要求の数 (IPv4 +IPv6)）	*proxy.process.http.real_client_requests*
Client IPv6 Requests（クライアント IPv6 要求の数）	*proxy.process.http.real_client_ipv6_requests*
Client transactions in progress（処理中のクライアントトランザクションの数）	*proxy.process.http.current_client_transactions*
Total document bytes from origin server（オリジンサーバーからのドキュメントの合計バイト数）	*proxy.process.http.origin_server_response_document_total_size*
Total document bytes from origin server（オリジンサーバーからのヘッダーの合計バイト数）	*proxy.process.http.origin_server_response_header_total_size*
Total connections to origin server（オリジン サーバーへの接続の合計数）	*proxy.process.http.current_server_connections*
Origin server transactions in progress（進行中のオリジン サーバートランザクションの数）	*proxy.process.http.current_server_transactions*
	FTP
Currently open FTP connections（現在のオープンな FTP 接続の数）	*proxy.process.ftp.connections_currently_open*

統計情報	変数
Successful PASV connections（PASV 接続の成功の数）	*proxy.process.ftp.connections_successful_pasv*
Unsuccessful PASV connections（PASV 接続の失敗の数）	*proxy.process.ftp.connections_failed_pasv*
Successful PORT connections（ポート接続の成功の数）	*proxy.process.ftp.connections_successful_port*
Unsuccessful PORT connections（ポート接続の失敗の数）	*proxy.process.ftp.connections_failed_port*
	WCCP
Enabled（有効化）	*proxy.config.wccp.enabled*
WCCP interface（WCCP インターフェース）	*proxy.local.wccp2.ethernet_interface*
	Cache（キャッシュ）
Bytes Used（使用バイト数）	*proxy.process.cache.bytes_used*
Cache size（キャッシュ サイズ）	*proxy.process.cache.bytes_total*
Lookups in progress（進行中のルックアップの数）	*proxy.process.cache.lookup.active*
Lookups completed（完了したルックアップの数）	*proxy.process.cache.lookup.success*
Lookup misses（ルックアップ ミスの数）	*proxy.process.cache.lookup.failure*
Reads in progress（進行中の読み込みの数）	*proxy.process.cache.read.active*
Reads completed（完了した読み込みの数）	*proxy.process.cache.read.success*
Read misses（読み込みミスの数）	*proxy.process.cache.read.failure*
Writes in progress（進行中の書き込みの数）	*proxy.process.cache.write.active*
Writes completed（完了した書き込みの数）	*proxy.process.cache.write.success*
Write failures（書き込み失敗の数）	*proxy.process.cache.write.failure*

統計情報	変数
Updates in progress（進行中の更新の数）	*proxy.process.cache.update.active*
Updates completed（完了した更新の数）	*proxy.process.cache.update.success*
Update failures（更新失敗の数）	*proxy.process.cache.update.failure*
Removes in progress（進行中の削除の数）	*proxy.process.cache.remove.active*
Remove successes（削除成功の数）	*proxy.process.cache.remove.success*
Remove failures（削除失敗の数）	*proxy.process.cache.remove.failure*
	Host DB（ホストデータベース）
Total Lookups（ルックアップの合計数）	*proxy.process.hostdb.total_lookups*
Total hits（ヒットの合計）	*proxy.process.hostdb.total_hits*
Time TTL（分）（TTL 時間）	*proxy.process.hostdb.ttl*
	DNS
DNS total lookups（DNS ルックアップの合計）	*proxy.process.dns.total_dns_lookups*
Average lookup time（ミリ秒）（平均ルックアップ時間）	*proxy.process.dns.lookup_avg_time*
DNS successes（DNS 成功の数）	*proxy.process.dns.lookup_successes*
	Cluster（クラスタ）
Bytes read（読み込まれたバイト数）	*proxy.process.cluster.read_bytes*
Bytes written（書き込まれたバイト数）	*proxy.process.cluster.write_bytes*
Connections open（接続オープンの数）	*proxy.process.cluster.connections_open*
Total operations（処理合計数）	*proxy.process.cluster.connections_opened*
Network backups（ネットワーク バックアップの数）	*proxy.process.cluster.net_backup*

統計情報	変数
Clustering nodes（クラスタリング ノードの数）	*proxy.process.cluster.nodes*
	SOCKS
Unsuccessful connections（接続失敗の数）	*proxy.process.socks.connections_unsuccessful*
Successful connections（接続成功の数）	*proxy.process.socks.connections_successful*
Connections in progress（進行中の接続の数）	*proxy.process.socks.connections_currently_open*
	Logging（ログ記録）
Currently open log files（現在開いているログ ファイルの数）	*proxy.process.log2.log_files_open*
Space used for log files（ログ ファイルに使用されているスペース）	*proxy.process.log2.log_files_space_used*
Number of access events logged（ログされたアクセス イベントの数）	*proxy.process.log2.event_log_access*
Number of access events skipped（スキップされたアクセス イベントの数）	*proxy.process.log2.event_log_access_skip*
Number of error events logged（ログされたエラー イベントの数）	*proxy.process.log2.event_log_error*

C 設定のオプション

Help | Content Gateway | バージョン 7.8.x

オプションは、設定ペインのの左側に、次のように分類されています。

My Proxy

Help | Content Gateway | バージョン 7.8.x

My Proxy のオプションは、下記の通りです。

Basic

Help | Content Gateway | バージョン 7.8.x

[Configure] > [My Proxy] > [Basic] > [General]

Restart（再起動）	プロキシおよびマネージャー サービス（**content_gateway** および **content_manager** プロセス）を再起動します。一部の設定オプションを変更した場合、プロキシおよびマネージャー サービスを再起動する必要があります。再起動が必要な時、メッセージがマネージャに表示されます。 **重要**：クラスタ構成の場合、**[Restart]** ボタンを押すとクラスタ内のすべてのノード上のプロキシおよびマネージャー サービスが再起動します。
Proxy Name（プロキシ名）	Content Gateway ノードの名前を指定します。デフォルトは、Content Gateway を実行しているコンピュータのホスト名です。 ノードがクラスタの一部である場合は、このオプションで、Content Gateway クラスタの名前を指定します。クラスタでは、すべてのノードは、同じノード名を共有する必要があります。
Alarm email（アラーム電子メール）	Content Gateway が、アラーム通知を送信する電子メール アドレスを指定します。
Features（機能）	
Protocols（プロトコル）：FTP	このオプションを有効にした場合、Content Gateway は、FTP クライアントからの FTP 要求を受け入れます。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Protocols: HTTPS	Content Gateway HTTPS トラフィック管理およびセキュリティ分析を有効化 / 無効化します。HTTPS の **[On]** を選択した場合、**[Configure] > [Protocols] > [HTTPS]** ページ、および **[Configure] > [SSL]** ページで、追加情報を入力する必要があります。*暗号化データの使用、159 ページ*を参照してください。
Networking（ネットワーク）：WCCP	このオプションを有効にした場合、Content Gateway への透過的なリダイレクトのために、WCCP v2-対応のルーターを使用します。WCCP v1 は、サポートされていません。 *WCCP v2 デバイスによる透過的遮断、65 ページ*を参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

Networking: DNS Proxy（DNS プロキシ）	このオプションを有効にした場合、Content Gateway は、クライアントに代わって、DNS 要求を解決します。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。*DNS プロキシ キャッシング、123 ページ*を参照してください。
Networking: Virtual IP（仮想 IP）	このオプションを有効にした場合、Content Gateway は必要に応じてクラスタ内のノードに割り当てる仮想 IP アドレスのプールを維持します。*仮想IP フェールオーバー、108 ページ*を参照してください。
Networking: IPv6（明示的プロキシのみ）	このオプションを有効にした場合、Content Gateway は、IPv6 に対する限定的なサポートを提供します。 サポートは、明示的プロキシのみ提供されます。 IPv6 アドレスは、クライアントおよび（または）インターネット トラフィックを処理する、すべてのデュアル スタック イーサネット インタフェースで使用することができます。 すべての TRITON コンポーネントとの通信には、IPv4 アドレスを使用する必要があります。 この機能の詳細および重要な制限のリストについては、*IPv6 のサポート、56 ページ*を参照してください。
Networking: Data Security	Websense Data Security との接続を有効化します。下記の 2 つのオプションがあります。 • Data Security Management Server への自動登録（バージョン 7.8.x が必要） • リモート Data Security Suite との ICAP 通信（バージョン 7.1、またはそれ以前） *Websense Data Security の使用、147 ページ*を参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Networking: Data Security: Integrated on-box（コンピュータに統合済み）	コンピュータにインストールされている Data Security コンポーネントと Data Security Management Server への登録を有効にします。*Data Security の登録と構成、150 ページ*を参照してください。
Networking: Data Security: ICAP	Data Security Suite で ICAP を有効にします。*ICAP クライアントの構成、154 ページ*を参照してください。

Security（セキュリティ）：SOCKS	[SOCKS] を有効にした場合、Content Gateway は SOCKS サーバーと通信します。*SOCKS ファイアウォール統合の設定*、211 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication（認証）：None（なし）	Content Gateway は、ユーザー認証のいくつかのタイプをサポートしています。 このオプションを選択した場合、プロキシはユーザー認証を実行しません。これは、デフォルト設定です。
Authentication（認証）：Integrated Windows Authentication（統合 Windows 認証）	[Integrated Windows Authentication (IWA)（統合 Windows 認証 (IWA)）] を有効化した場合、ユーザーがコンテンツへのアクセスを許可される前に、ユーザーは IWA によって認証されます。 *統合 Windows 認証*、225 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication: LDAP	[LDAP] を有効化した場合、コンテンツへのアクセスを許可される前に、ユーザーは LDAP によって認証されます。*LDAP 認証*、233 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication: Radius	[RADIUS] を有効化した場合、コンテンツへのアクセスを許可される前に、ユーザーは RADIUS によって認証されます。*RADIUS 認証*、236 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication: Legacy NTLM（レガシー NTLM）	[legacy NTLM (NTLMSSP)] を有効化した場合、Windows ネットワーク内のユーザーは、コンテンツへのアクセスを許可される前に、ドメイン コントローラによって認証されます。 *レガシー NTLM 認証*、230 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

Authentication: Rule-based Authentication（認証：ルールベースの認証）	[Rule-Based Authentication（ルールベースの認証）] を有効化した場合、ユーザーは一致するルールのパラメータに基づいて認証されます。ルールベースの認証は、複数のレルム、複数ドメイン、および他のユーザー認証のシナリオをサポートします。*ルール ベースの認証*、239 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication: Read authentication from child proxy（子プロキシからの認証の読み取り）	着信要求内の X-Authenticated-User、および X-Forwarded-For ヘッダー値の読み込みを有効化または無効化します。このオプションはデフォルトでは無効化されます。 Content Gateway がチェーンの中の親（アップストリーム）プロキシであり、子（ダウンストリーム）プロキシが認証のために、X-Authenticated-User、および -X-Forwarded-For ヘッダーを送信する場合に、このオプションを有効にします。
Authentication: Send authentication to parent proxy（認証を親プロキシに送信）	送信要求内に、X-Authenticated-User ヘッダーの値を挿入するかどうか指定します。このオプションはデフォルトでは無効化されます。 Content Gateway がチェーンの中の子（ダウンストリーム）プロキシであり、親（アップストリーム）プロキシが認証のために、X-Authenticated-User ヘッダーを必要とする場合に、このオプションを有効にします。

[Configure] > [My Proxy] > [Basic] > [Clustering（クラスタ化）]

Cluster: Type（タイプ）	クラスタ化のモードを指定します。 Content Gateway サーバーを単一モードで実行する場合、**Single Node** を選択します。このノードは、クラスタの一部ではなくなります。 管理クラスタ化モードアクティブにするには、**[Management Clustering（管理クラスタ化）]** を選択します。クラスタ内のノードは設定情報を共有しており、同時にすべてのノードを管理できます。 クラスタ化の詳細については、*クラスタ*、101 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

Cluster: Interface（インターフェース）	Content Gateway が、クラスタ内の他のノードと通信するために、どのインターフェースを使用するかを指定します。例、**eth1**。 専用のセカンダリー インターフェースを使用することを推奨します。 ノード構成情報は、プレーン テキストで、同じサブネット中の他の Content Gateway ノードにマルチキャストされます。したがって、Websense は、クライアントを Content Gateway ノードから独立したサブネット上に配置することを推奨します（クラスタ化のためのマルチキャスト通信はルーティングされません）。 V シリーズ アプライアンス上では、P1 (eth0) が推奨インターフェースです。しかし、クラスタ管理トラフィックを隔離したい場合には、P2 (eth1) を使用してもかまいません。 *クラスタ構成の変更*、103 ページを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Cluster: Multicast Group Address（マルチキャスト グループ アドレス）	Content Gateway が、クラスタ ピアと通信するためのマルチキャスト グループ アドレスを指定します。 *クラスタ構成の変更*、103 ページを参照してください。

サブスクリプション

Help | Content Gateway | バージョン 7.8.x

[Configure] > [My Proxy] > [Subscription（サブスクリプション）] > [Subscription Management（サブスクリプション管理）]

サブスクリプション キー	Websense 社から受け取ったサブスクリプション キーを表示します。 Content Gateway を **Web Security Gateway** または **Web Security Gateway Anywhere** と共に使用する場合は、このキーは Web Security に入力したサブスクリプション キーです。 Content Gateway が **Websense Data Security Suite** とのみ共に配備されている場合は、このフィールドに Content Gateway のサブスクリプション キーを入力する必要があります。

[Configure] > [My Proxy] > [Subscription] > [Scanning（スキャン）]

Policy Server	
IP address（IP アドレス）	Websense Web Security Policy Server の IP アドレス。この値は、Content Gateway がインストールされる時に指定されます。
Port（ポート）	Websense Web Security Policy Server が使用するポート。デフォルト ポートは 55806 です。
Filtering Service	
IP address（IP アドレス）	Websense Web Security Filtering Service の IP アドレスを指定します。この値は、Content Gateway がインストールされる時に指定されます。
Port（ポート）	Websense Web Security Filtering Service が使用するポートを指定します。デフォルト ポートは 15868 です。
Communication Timeout（通信タイムアウト）	Policy Server および Filtering Service による応答のタイムアウト時間を、ミリ秒単位で指定します。この時間を過ぎると通信タイムアウト条件が発生し **[Action for Communication Errors（通信エラーの場合の措置）]** の設定が適用されます。 デフォルトのタイムアウト値は、5000ms（5 秒）です。
Action for Communication Errors（通信エラーの場合の処置）	
Permit traffic（トラフィックを許可）	Policy Server または Filtering Service との通信が失敗した場合に、すべてのトラフィックを許可します。
Block traffic（トラフィックをブロック）	Policy Server または Filtering Service との通信が失敗した場合に、すべてのトラフィックをブロックします。

UI セットアップ

Help | Content Gateway | バージョン 7.8.x

[Configure] > [My Proxy] > [UI Setup（UI セットアップ）] > [General]

UI Port（UI ポート）	ブラウザが Content Gateway Manager との接続に使用できるポートを指定します。デフォルト ポートは 8081 です。 この設定を変更した場合、Content Gateway を再起動する必要があります。

HTTPS: Enable/Disable（有効化 / 無効化）	Content Gateway Manager との SSL 接続のサポートを有効化または無効化します（デフォルトでは有効化されています）。 SSL は、リモート管理モニタリングおよび設定の保護を提供します。Content Gateway マネージャとの接続に SSL を使用するためには、Content Gateway サーバー コンピュータに SSL 証明書をインストールする必要があります。詳細については、*セキュアな管理のための SSL の使用*、203 ページを参照してください。
HTTPS: Certificate File（証明書ファイル）	Content Gateway マネージャにアクセスするユーザーを認証するための、SSL 証明書ファイルを指定します。
Monitor Refresh Rate（モニタ更新頻度）	Content Gateway Manager が **[Monitor]** ペイン上の統計を更新する頻度を指定します。デフォルト値は 30 秒です。
Default Help Language（デフォルトのヘルプ言語）	デフォルト時に Content Gateway Manager Help が表示する言語を指定します。ページがデフォルトの言語で利用できない場合は、他の言語を代用してもかまいません。

[Configure] > [My Proxy] > [UI Setup] > [Login（ログイン）]

Basic Authentication（基本認証）	基本認証を有効化または無効化します。このオプションを有効にした場合、Content Gateway は、ユーザーが Content Gateway マネージャにアクセスする度に、管理者ログインとパスワード、または ユーザー名とパスワード（ユーザー アカウントが設定されている場合）をチェックします。
Administrator（管理者）：Login（ログイン）	管理者ログインを指定します。デフォルトは [admin] です。 管理者ログインは、Content Gateway マネージャの設定モード、およびモニタ モード両方にアクセスできるマスター ログインです。 **ご注意**：基本認証オプションが有効化されている場合にのみ、Content Gateway は管理者ログインをチェックします。

Administrator: Password（パスワード）	Content Gateway マネージャへのアクセスを制御する管理者パスワードを変更します。 **[Old Password（古いパスワード）]** フィールドに現在のパスワードを入力します。**[New Password（新しいパスワード）]** フィールドに新しいパスワードを入力し、次に **[New Password（Retype）（新しいパスワード（再入力））]** フィールドに新しいパスワードを再入力し、その後 **[Apply]** をクリックします。 ご注意：基本認証オプションが有効化されている場合にのみ、Content Gateway は管理者ログインとパスワードをチェックします。 インストール中に管理者パスワードを選択します。インストーラは自動的にパスワードを暗号化し、**records.config** ファイルに暗号を保存します。Content Gateway マネージャでパスワードを変更するたびに、Content Gateway は **records.config** ファイルを更新します。管理者パスワードを忘れてしまい、Content Gateway マネージャにアクセスできない場合、*マスタ管理者パスワードを忘れた場合の Content Gateway manager へのアクセスの方法*、17 ページを参照してください。
Additional Users（追加のユーザー）	現在のユーザーアカウントをリストし、新しいユーザーアカウントを追加できます。ユーザー アカウントは、誰が Content Gateway マネージャにアクセスし、どのアクティビティを実行できるかを決定します。1 つの管理者ログインとパスワードだけではニーズに対応する十分なセキュリティを確保できない場合に、ユーザー アカウントのリストを作成できます。 新しいアカウントを作成するには、**[New User]** フィールドにユーザー ログインを入力し、**[New Password]** フィールドにユーザー パスワードを入力します。**[New Password (Retype)]** フィールドにユーザー パスワードを再入力し、**[Apply]** をクリックします。新しいユーザーの情報が、テーブルに表示されます。テーブルの **[Access]** ドロップダウン リストで、新しいユーザーが実行できるアクティビティを選択します（**[Monitor（モニター）]**、**[Monitor and View Configuration（モニターおよび設定の表示）]**、または **[Monitor and Modify Configuration（モニターおよび設定の変更）]**）。ユーザー アカウントの詳細については、*ユーザー アカウントのリストの作成*、202 ページを参照してください。 ご注意：基本認証オプションが有効化されている場合にのみ、Content Gateway はユーザー ログインとパスワードをチェックします。

[Configure] > [My Proxy] > [UI Setup] > [Access]

Access Control（アクセス制御）	*mgmt_allow.config* ファイルのルールをリストするテーブルを表示します。ルールは、Content Gateway マネージャへのアクセスを許可されるリモート ホストを指定します。このファイルのエントリは、認証されたユーザーだけが設定オプションを変更でき、パフォーマンスおよびネットワーク トラフィック統計を表示できるようにします。 ご注意：デフォルトでは、すべてのリモートホストが Content Gateway マネージャへのアクセスを許可されています。
Refresh（リフレッシュ）	テーブルを更新して、**mgmt_allow.config** ファイルの最新のルールを表示します。
Edit File（ファイルを編集）	**mgmt_allow.config** ファイルを編集し、ルールを追加するために、設定ファイル エディタを開きます。
	mgmt_allow.config Configuration File Editor（mgmt_allow.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	**mgmt_allow.config** ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。Content Gateway は、リストの上から順にルールを適用します。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
IP Action（IP アクション）	追加できるルールのタイプをリストします。 **ip_allow** ルールは、**[Source IP]** フィールドで指定したリモートホストが、Content Gateway マネージャにアクセスすることを許可します。 **ip_deny** ルールは、**[Source IP]** フィールドで指定したリモートホストが、Content Gateway マネージャにアクセスすることを拒否します。
Source IP（送信元 IP）	Content Gateway マネージャにアクセスすることを、許可、または 拒否する IP アドレスを指定します。単一の IP アドレス (111.111.11.1)、または アドレスの範囲 (0.0.0.0-255.255.255.255) を入力できます。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

スナップショット

Help | Content Gateway | バージョン 7.8.x

[Configure] > [My Proxy] > [Snapshots（スナップショット）] > [File System（ファイル システム）]

Change Snapshot Directory（スナップショット ディレクトリを変更）	この Content Gateway ノード上でスナップショットを保存するディレクトリを指定します。
Snapshots（スナップショット）：Save Snapshot（スナップショットを保存）	作成する構成スナップショットの名前を入力します。**[Apply]** をクリックして、ローカルノード上の設定を保存します。Content Gateway は、**[Change Snapshot Directory]** フィールドで指定されたディレクトリに、構成のスナップショットを保存します。 システム保守を実行したりシステム パフォーマンスを微調整する前にスナップショットを作成することを推奨します。スナップショットの作成は数秒かかるだけであり、それによって構成の間違いを修正するための数時間を節約できます。
Snapshots: Restore/Delete Snapshot（スナップショットを復元 / 削除）	ノードに保存されているスナップショットをリストします。ドロップダウン リストから、削除または復元したいスナップショットを選択します。
Snapshots: Restore Snapshot from “directory_name” Directory（[directory_name] ディレクトリからスナップショットを復元）	**[Restore/Delete Snapshot]** ドロップダウン ボックスで選択されたスナップショットを復元します。 クラスタ構成の場合、スナップショットは、クラスタ内のすべてのノード上で復元されます。
Snapshots: Delete Snapshot from “directory_name” Directory（[directory_name] ディレクトリからスナップショットを削除）	**[Restore/Delete Snapshot]** ドロップダウン ボックスで選択されたスナップショットを削除します。

[Configure] > [My Proxy] > [Snapshots] > [FTP server（FTP サーバー）]

FTP Server（FTP サーバー）	構成のスナップショットから復元する、または 構成のスナップショットに保存する FTP サーバー名を指定します。
Login（ログイン）	FTP サーバーへのアクセスに必要なログイン名を指定します。

Password（パスワード）	FTP サーバーへのアクセスに必要なパスワードを指定します。
Remote Directory（リモート ディレクトリ）	構成スナップショットから復元、または 構成スナップショットに保存する FTP サーバーのディレクトリを指定します。
Restore Snapshot（スナップショットを復元）	復元できる FTP サーバーの構成スナップショットがリストされます。 FTP サーバーに正常にログ オンした後、このフィールドが表示されます。
Save Snapshot to FTP Server [FTP サーバーにスナップショットを保存]	撮る構成のスナップショットの名前を入力し、FTP サーバーに保存します。 FTP サーバーに正常にログ オンした後、このフィールドが表示されます。

ログ

Help | Content Gateway | バージョン 7.8.x

[Configure] > [My Proxy] > [Logs（ログ）] > [System（システム）]

Log File（ログ ファイル）	表示できるシステム ログ ファイルがリストされ、削除、またはローカル システムにコピーします。Content Gateway は、システム全体のログ記録機能である **syslog** がデーモン機能のもとで記録したシステム ログ ファイルをリストアップします。
Action: Display the selected log file（選択したログ ファイルを表示）	このオプションを有効にした場合、Content Gateway は、**[Log File]** ドロップダウン リストで選択されたシステム ログ ファイルの最初の 1MB を表示します。 全体のファイルを表示するには、[Save the selected log file in local filesystem（選択したログ ファイルをローカル ファイルシステムに保存）] を選択し、ローカル ビューアで ファイルを表示します。
Action: Display last lines of the selected file（選択したファイルの最後の数行を表示）	このオプションを有効にした場合、Content Gateway は選択したシステム ログ ファイルの最後の、指定された数の行を表示します。
Action: Display lines that match in the selected log file（選択したログ ファイルの中の一致する行を表示）	このオプションを有効にした場合、Content Gateway は、システム ログ ファイル内の、指定した文字列と一致するすべての行を表示します。

Action: Remove the selected log file（選択したログ ファイルを削除）	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを削除します。
Action: Save the selected log file in local filesystem（選択したログ ファイルをローカル ファイルシステムに保存）	このオプションを有効化した場合、Content Gateway は、選択されたログ ファイルを、ローカル システム上の指定された場所に保存します。

[Configure] > [My Proxy] > [Logs] > [Access（アクセス）]

Log File（ログ ファイル）	ローカル システムに表示、削除、またはコピーできるイベント ログ ファイルまたはエラー ログファイルをリストします。Content Gateway はイベント ログ ファイルを、**[Subsystems/Logging（サブシステム / ログ記録）]** の **[Logging Directory（ログ記録）]** フィールドで指定され、かつ **records.config** ファイルの 設定変数 **proxy.config.log2.logfile_dir** によって指定されているディレクトリに保存します。デフォルトのディレクトリは、Content Gateway インストール ディレクトリの **logs** です。
Action: Display the selected log file（選択したログ ファイルを表示）	このオプションを有効にした場合、Content Gateway は、**[Log File]** ドロップダウン リストで選択されたイベントまたはエラー ログ ファイルの最初の 1MB を表示します。 全体のファイルを表示するには、[Save the selected log file in local filesystem（選択したログ ファイルをローカル ファイルシステムに保存）] を選択し、ローカル ビューアで ファイルを表示します。
Action: Display last lines of the selected file（選択したファイルの最後の数行を表示）	このオプションを有効にした場合、Content Gateway は、**[Log File]** ドロップダウン リストで選択されたイベントまたはエラー ログ ファイルの末尾の指定行数を表示します。
Action: Display lines that match in the selected log file（選択したログ ファイルの中の一致する行を表示）	このオプションを有効にした場合、Content Gateway は、指定された文字列と一致するイベントまたはエラー ログ ファイルのすべての行を表示します。

Remove the selected log file（選択したログ ファイルを削除）	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを削除します。
Action: Save the selected log file in local filesystem（選択したログ ファイルをローカル ファイルシステムに保存）	このオプションを有効化した場合、Content Gateway は、選択されたログ ファイルを、ローカル システム上の指定された場所に保存します。

プロトコル

Help | Content Gateway | バージョン 7.8.x

プロトコル設定オプションは、下記のカテゴリに分けられます：

HTTP、350 ページ

HTTP Responses（HTTP 応答）、362 ページ

HTTP Scheduled Update、364 ページ

HTTPS、365 ページ

FTP、367 ページ

HTTP

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Protocols] > [HTTP] > [General]

HTTP Proxy Server Port（HTTP プロキシ サーバー ポート）	Content Gateway が、HTTP トラフィックの Web プロキシ サーバーとして動作する時、または HTTP 要求を透過的に処理する時に使用するポートを指定します。デフォルト ポートは 8080 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary HTTP Proxy Server Port（セカンダリ HTTP プロキシ サーバー ポート）	**明示的プロキシ構成の場合のみ**、Content Gateway が HTTP トラフィックを受信待機する追加のポートを指定します。 **透過的プロキシ構成では、常にすべての HTTP トラフィックをポート 8080 に送信します。**

Unqualified Domain Name Expansion（未修飾のドメイン名の拡張）	**.com** 名拡張を有効化または無効化します。このオプションを有効化した場合、Content Gateway は未修飾のホスト名を解決するために、ホスト名の先頭に **www.**、末尾に **.com** を付加した拡張アドレスにそれをリダイレクトします。たとえば、クライアントが *company* に要求を行うと、Content Gateway は、**www.company.com** に要求をリダイレクトします。 ローカル ドメイン拡張が有効な場合（*DNS リゾルバ*、423 ページを参照）、Content Gateway は **.com** ドメイン拡張の前に、ローカル ドメイン拡張を試みます。Content Gateway は ローカルドメイン拡張が失敗した場合にのみ **.com** ドメイン拡張を試みます。
Send HTTP 1.1 by Default（デフォルトで HTTP 1.1 を送信）	オリジン サーバーへの最初の要求時に HTTP 1.1 の送信を有効化します（デフォルト）。オリジン サーバーが HTTP 1.0 で応答した場合、Content Gateway は HTTP 1.0 に変更します（ほとんどのオリジン サーバーは HTTP 1.1 を使用します）。無効化された場合、オリジン サーバーへの最初の要求に HTTP 1.0 が使用されます。オリジン サーバーが HTTP 1.1 で応答した場合、Content Gateway は HTTP 1.1 に変更します。
Reverse DNS（リバース DNS）	URL に（ホスト名の代わりに）IP アドレスが含まれ、**filter.config**、**cache.config**、または **parent.config** にルールが存在する場合、リバース DNS ルックアップを有効化します。これは、ルールが 宛先ホスト名、および ドメイン名に基づく場合に必要です。
Tunnel Ports（ポートをトンネリング）	Content Gateway が トンネリングを許可するポートを指定します。これは、スペースで区切られたリストで、ホート範囲を指定できます（例、1-65535）。 SSL が有効化されていない場合、指定されたポート宛てのすべてのトラフィックは、オリジン サーバーへのトンネリングを許可されます。 SSL が有効化されている場合、**[HTTPS Ports]** フィールドにリストされているすべてのポートへのトラフィックはトンネリングされず、復号化され、フィルタリング ポリシーが適用されます。

HTTPS ports （HTTPS ポート）	SSL サポートが有効化されている場合は、トラフィックが復号化され、フィルタリング ポリシーが適用されるポートを指定します。Content Gateway は、**[Configure] > [Protocols] > [HTTPS] > [HTTPS Proxy: Server Port（HTTP プロキシ：サーバー ポート）]** で指定されているポートで HTTPS トラフィックを受信します。 SSL サポートが無効化されている場合は、これらのポートへのトラフィックは復号化されません。しかし、フィルタリング ポリシーは、下記のどちらかに基づいて適用されます。 • 明示的プロキシ：CONNECT 要求内のサーバー ホスト名。 • 透過的プロキシ：SNI ホスト名またはサーバーの証明書内のサーバー ホスト名。サーバーの証明書内のホスト名がワイルドカード（*）を含んでいる場合は、宛先 IP アドレスの検索が実行されます。
FTP over HTTP: Anonymous Password （匿名パスワード）	パスワードを要求する FTP サーバー接続に、Content Gateway が 使用する匿名パスワードを指定します。このオプションは、HTTP クライアントからの FTP 要求に適用されます。
FTP over HTTP: Data Connection Mode （データ接続モード）	FTP 転送は、下記の 2 つの接続を必要とします。データの要求を FTP サーバーに通知するコントロール接続と、データを送信するデータ接続。Content Gateway は常に、コントロール接続を開始します。FTP モードは、データ接続を Content Gateway が開始するか、FTP サーバーが開始するかを決定します。 **[PASV then PORT]** を選択すると、Content Gateway は、最初に PASV 接続モードを試みます。PASV モードが失敗した場合、Content Gateway は PORT モードを試み、データ接続を開始します。成功すれば、FTP サーバーはデータ接続を受け入れます。 **[PASV only]** を選択すると、Content Gateway は、FTP サーバーとデータ接続を開始します。このモードは、ファイアウォールに適していますが、いくつかの FTP サーバーはサポートしていません。 **[PORT only（ポートのみ）]** を選択すると、FTP サーバーは データ接続を開始し、Content Gateway は接続を受け入れます。 デフォルト値は、**[PASV then PORT]** です。

[Configure] > [Protocols] > [HTTP] > [Cacheability（キャッシュ機能）]

Caching: HTTP Caching（HTTP キャッシング）	HTTP キャッシングを有効化または無効化します。このオプションを有効化した場合、Content Gateway は HTTP 要求をキャッシュから処理します。このオプションを無効化した場合、Content Gateway はプロキシ サーバーとして動作し、すべての HTTP 要求を直接オリジン サーバーに転送します。 ご注意：HTTPS コンテンツはキャッシングされることはありません。
Caching: FTP over HTTP Caching（FTP over HTTP キャッシング）	FTP over HTTP キャッシングを有効化または無効化します。このオプションを有効化した場合、Content Gateway は、HTTP クライアントからの FTP 要求をキャッシュから処理します。このオプションを無効化した場合、Content Gateway は、プロキシ サーバーとして動作し、HTTP クライアントからのすべての FTP 要求を直接オリジン サーバーに転送します。
Behavior: Required Headers（必須のヘッダー）	HTTP オブジェクトをキャッシュ可能にするために要求される最小限のヘッダー情報を指定します。 **Expires or max-age** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、**[An Explicit Lifetime Header（明示的寿命ヘッダー）]** を選択します。 **last_modified** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、**[A Last-Modified Header（最後に変更したヘッダー）]** を選択します。 **Expires**、**max-age**、または **last-modified** ヘッダーを含まない HTTP オブジェクトをキャッシュするには、**[No Required Headers（ヘッダーを必要としない）]** を選択します。これは、デフォルト オプションです。 **警告**：デフォルトでは、Content Gateway は、すべてのオブジェクト（ヘッダーのないオブジェクトを含む）をキャッシュします。プロキシの特別の事情がない限りデフォルト設定を変更しないことを推奨します。Content Gateway が **Expires** または **max-age** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするように設定されている場合、キャッシュ ヒット率が下がります（明示的な期限切れ情報があるオブジェクトはごく少数です）。

Behavior: When to Revalidate （再確認する時期）	キャッシュ内の HTTP オブジェクトの最新性を評価する方法を指定します。 キャッシュ内の HTTP オブジェクトをオリジン サーバーに再確認しない場合は、**[Never Revalidate（再確認しない）]** を選択します（Content Gateway は、キャッシュ内のすべての HTTP オブジェクトが最新であるとみなします）。 常にキャッシュ内の HTTP オブジェクトをオリジン サーバーに再確認する場合は、**[Always Revalidate（常に再確認する）]** を選択します（Content Gateway は、キャッシュ内のすべての HTTP オブジェクトが古くなったとみなします）。 オブジェクトが **Expires** または **Cache-Control** ヘッダーを含まない場合に、HTTP オブジェクトの最新性をオリジン サーバーに確認する場合は、**[Revalidate if Heuristic Expiration（ヒューリスティック期限切れか否か再確認）]** を選択します。Content Gateway は、**Expires** または **Cache-Control** ヘッダーがないすべての HTTP オブジェクトが [古い] とみなします。 Content Gateway が、オブジェクト ヘッダー、絶対最新性限界値、および（または）**cache.config** ファイル内のルールに基づいて、キャッシュ内のオブジェクトが古くなったと見なしたときに、オリジン サーバーで HTTP オブジェクトの最新性を確認する場合は、**[Use Cache Directive or Heuristic（キャッシュ ディレクティブまたはヒューリスティックを使用）]** を選択します。これは、デフォルト オプションです。 再確認の詳細については、*HTTP オブジェクトの再確認*、31 ページを参照してください。

Behavior: Add “no-cache” to MSIE Requests（MSIE 要求に [no-cache] を追加）	Content Gateway が、Microsoft Internet Explorer からの要求に対して **no-cache** ヘッダー付加する場合に、このオプションを指定します。 Microsoft Internet Explorer の一部のバージョンは、ユーザーがブラウザの **[Refresh（リフレッシュ）]** ボタンを押した場合、透過的キャッシュからのキャッシュ再ロードを要求しません。それによって、コンテンツがオリジン サーバーから直接にロードされるのを防止します。Content Gateway が Microsoft Internet Explorer の要求をより慎重に処理するように設定できます。その場合、提供するコンテンツの最新性を向上させることができますが、キャッシュから提供できるドキュメントの数が少なくなります。 Microsoft Internet Explorer からのすべての要求に、**no-cache** ヘッダー付加する場合、**[To All MSIE Requests（すべての MSIE 要求に対して）]** を選択します。 IMS（If Modified Since）を含む Microsoft Internet Explorer からの要求に **no-cache** ヘッダー付加する場合、**[To IMS MSIE Requests（IMS MSIE 要求に対して）]** を選択します。 Microsoft Internet Explorer からのどの要求に対しても **no-cache** ヘッダーを付加しない場合、[Not to Any MSIE Requests（どの MSIE 要求にも付加しない）] を選択します。
Behavior: Ignore “no-cache” in Client Requests（クライアント要求の [no-cache] を無視する）	このオプションを有効化すると、Content Gateway は クライアント要求の **no-cache** ヘッダーを無視し、キャッシュから要求を処理します。 このオプションを無効化すると、Content Gateway は **no-cache** ヘッダーが設定されている要求をキャッシュから処理せず、オリジン サーバーに転送します。
Freshness: Minimum Heuristic Lifetime（最小ヒューリスティック寿命）	HTTP オブジェクトをキャッシュ内で最新と見なすことができる最小時間を指定します。
Freshness: Maximum Heuristic Lifetime（最大ヒューリスティック寿命）	HTTP オブジェクトをキャッシュ内で最新と見なすことができる最大時間を指定します。
Freshness: FTP Document Lifetime（FTP ドキュメントの寿命）	FTP ファイルをキャッシュ内に保存できる最大時間を指定します。このオプションは、HTTP クライアントからの FTP 要求のみに適用されます。

Maximum Alternates（代替の最大数）	Content Gateway が、キャッシュする HTTP オブジェクトの代替バージョンの最大数を指定します。 **警告：**0（ゼロ）を入力した場合、キャッシュできる代替バージョンの数は無制限です。アクセス数が多い URL に数千の代替がある場合、Content Gateway が各要求に対して数千の代替を検索する時に、キャッシュ ヒット遅延（処理時間）が大きくなることがあります。特に、いくつかの URL は、クッキーによって、多くの代替をもつことがあります。Content Gateway がクッキーによって変化するよう設定されている場合、この問題に遭遇するかもしれません。
Vary Based on Content Type（コンテンツ タイプに基づいて変動）：Enable/Disable（有効化 / 無効化）	**Vary** ヘッダーを含んでいない HTTP ドキュメントの代替バージョンのキャッシングを、有効化 または 無効化します。**Vary** ヘッダーが存在しない場合、Content Gateway はドキュメントのコンテンツ タイプに従って、下記で指定されたヘッダーを変化させます。
Vary by Default on Text（テキストの場合にデフォルトで変化）	テキスト ドキュメントの場合に、Content Gateway が変化させるヘッダー フィールドを指定します。
Vary by Default on Images（イメージの場合にデフォルトで変化）	イメージの場合に、Content Gateway が 変化させるヘッダー フィールドを指定します。
Vary by Default on Other Document Types（他のドキュメント タイプの場合にデフォルトで変化））	テキストとイメージ以外の場合に、Content Gateway が変化させるヘッダー フィールドを指定します。
Dynamic Caching: Caching Documents with Dynamic URLs（ダイナミック URL を含むドキュメントのキャッシング）	このオプションを有効にした場合、Content Gateway は、ダイナミック コンテンツをキャッシュしようとします。コンテンツが疑問符（?）、セミコロン（;）、**cgi** を含むか、または **.asp** で終了する場合、そのコンテンツはダイナミックと見なされます。 **警告：**専用のプロキシが割り当てられている場合にのみ、Content Gateway がダイナミック コンテンツをキャッシュするように設定することを推奨します。

Dynamic Caching: Caching Response to Cookies（クッキーへの応答のキャッシング）	クッキーを含む要求に対する応答がキャッシュされる方法を指定します。 テキスト以外のすべてコンテンツ タイプを含むクッキーをキャッシュする場合、**[Cache All but Text（テキストを除くすべてをキャッシュ）]** を選択します。これは、デフォルトです。 イメージを含む場合にのみ クッキーをキャッシュする場合、**[Cache Only Image Types（イメージ タイプのみをキャッシュ）]** を選択します。 すべてのコンテンツ タイプのクッキーをキャッシュする場合、**[Cache Any Content-Type（すべてのコンテンツ タイプをキャッシュ）]** を選択します。 クッキーをキャッシュしない場合は、**[No Cache on Cookies（クッキーをキャッシュしない）]** を選択します。
Caching Policy/Forcing Document Caching（ポリシーのキャッシング / ドキュメントのキャッシングの強制）	URL の特定のグループをキャッシュするかどうかを指定する **cache.config** ファイル内のルールのテーブルを表示します。このファイルで、指定時間、特定の URL をキャッシュするよう強制できます。
Refresh（リフレッシュ）	**cache.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。設定ファイル エディタで、ルールを追加 または 編集した後は、**[Refresh]** をクリックします。
Edit File（ファイルを編集）	**cache.config** ファイルを編集し、ルールを追加するために、設定ファイル エディタを開きます。
	cache.config Configuration File Editor（cache.config 設定ファイル エディタ）
Rule display box（ルール表示ボックス）	**cache.config** ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。

Rule Type（ルール タイプ）	**cache.config** ファイルに追加できるルールのタイプをリストします。 **never-cache** ルールは、特定のオブジェクトをキャッシュしないように、Content Gateway を設定します。 **ignore-no-cache** ルールは、すべての **Cache-Control: no-cache** ヘッダーを無視するように、Content Gateway を設定します。 **ignore-client-no-cache** ルールは、クライアント要求からの **Cache-Control: no-cache** ヘッダーを無視するように、Content Gateway を設定します。 **ignore-server-no-cache** ルールは、オリジン サーバーの応答から **Cache-Control: no-cache** ヘッダーを無視するように、Content Gateway を設定します。 **pin-in-cache** ルールは、指定時間の間、キャッシュにオブジェクトを残しておくように、Content Gateway を設定します。 **revalidate** ルールは、指定時間の間、キャッシュ内のオブジェクトが最新であると見なすように、Content Gateway を設定します。 **ttl-in-cache** ルールを設定すると、Content Gateway は HTTP 要求および応答ヘッダー内のキャッシング指令に関係なく、**[Time Period（時間）]** フィールドで指定された時間、キャッシュから HTTP オブジェクトを処理します。
Primary Destination Type（一次宛先タイプ）	下記の一次宛先タイプをリストします。 **dest_domain** は 要求されたドメイン名。 **dest_host** は 要求されたホスト名。 **dest_ip** は 要求された IP アドレス。 **url_regex** は URL に含まれる正規表現。
Primary Destination Value（一次宛先値）	一次宛先タイプの値を指定します。たとえば、Primary Destination Type が **dest_ip** の場合、このフィールドに 123.456.78.9 を選択できます。
Additional Specifier（追加の指定子）：Time Period（期間）	**revalidate**、**pin-in-cache**、および **ttl-in-cache** ルール タイプに適用する時間を指定します。次の時間形式で入力できます： **d**：日付（例 2d） **h**：時間（例 10h） **m**：分（例 5m） **s**：秒（例 20s） 単位の組み合わせ（例 1h15m20s）
Secondary Specifiers（二次指定子）：時間	時間範囲（例、08: 00-14: 00）を指定します。

Secondary Specifiers: Prefix（接頭辞）	URL のパス部分の接頭辞を指定します。
Secondary Specifiers: Suffix（接尾辞）	URL のファイル接尾辞を指定します。
Secondary Specifiers: Source IP（送信元 IP）	クライアントの IP アドレスを指定します。
Secondary Specifiers: Port（ポート）	要求された URL の中のポートを指定します。
Secondary Specifiers: Method（メソッド）	要求された URL メソッドを指定します。
Secondary Specifiers: Scheme（スキーム）	要求された URL のプロトコルを指定します。
Secondary Specifiers: User-Agent（ユーザー エージェント）	要求ヘッダーのユーザー エージェントの値を指定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Protocols] > [HTTP] > [Privacy（プライバシー）]

Insert Headers: Client-IP（クライアント IP）	このオプションを有効にすると、クライアント IP アドレスを保持するために、Content Gateway は 送信要求に **Client-IP** ヘッダーを挿入します。 このオプションは、**[Remove Headers: Client-IP（ヘッダーを削除：クライアント IP）]** オプションと相互に排他的です。[Insert Headers: Client-IP] が有効化されると、[Remove Headers: Client-IP] オプションが自動的に無効化されます。 [Insert Headers: Client-IP] と [Remove Headers: Client-IP] の両方のオプションを無効化できます。
Insert Headers: Via	有効にすると、Content Gateway は送信要求に **Via** ヘッダーを挿入します。Via ヘッダーは宛先サーバーに、要求の送信で経由したプロキシを知らせます。
Insert Headers: X-Forwarded-For	このオプションを有効化すると、Content Gateway は送信要求に **X-Forwarded-For** ヘッダーを挿入します。X-Forwarded-For 値は、送信元の IP アドレスを含んでいます。

Remove Headers: Client-IP	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から **Client-IP** ヘッダーを削除します。 このオプションは、**[Insert Headers: Client-IP]** オプションと相互に排他的です。[Remove Headers: Client-IP] が有効化されると、[Insert Headers: Client-IP] オプションが自動的に無効化されます。 [Remove Headers: Client-IP] と [Insert Headers: Client-IP] の両方のオプションを無効化できます。
Remove Headers: Cookie	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は 送信要求から **Cookie** ヘッダーを削除します。**Cookie** ヘッダーは、しばしば要求を行ったユーザーを識別します。
Remove Headers: 開始日	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は 送信要求から **From** ヘッダーを削除します。ヘッダ **From** はクライアントの電子メール アドレスを示します。
Remove Headers: Referer	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は 送信要求から **Referer** ヘッダーを削除します。**Referer** ヘッダーは、クライアントが選択した Web リンクを識別します。
Remove Headers: ユーザー エージェント	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は 送信要求から **User-Agent** ヘッダーを削除します。**User-Agent** ヘッダーは、要求を行ったエージェント（通常はブラウザ）を識別します。
Remove Headers: Remove Others	ユーザーのプライバシーを保護するために、送信要求から削除する、**From**、**Referer**、**User-Agent**、および **Cookie** 以外のヘッダーを指定します。

[Configure] > [Protocols] > [HTTP] > [Timeouts]

HTTP タイムアウト オプションについては、knowledge base のこの記事を参照してください。

キープアライブのタイムアウト Client	トランザクション終了後、後続の要求のために、クライアントとの接続を開きつづける時間（秒単位）を指定します。クライアント要求を受け入れるために Content Gateway が接続をオープンする度に、要求を処理した後、指定されたタイムアウト時間の間、接続を続けます。タイムアウト時間前にクライアントが他の要求を行った場合、Content Gateway は 接続を閉じます。クライアントが他の要求を行った場合、タイムアウト時間は再開始します。 クライアントは いつでも接続を閉じることができます。

Keep-Alive Timeouts: Origin Server	トランザクション終了後、後続のデータ転送のために、オリジン サーバーへの接続を開き続ける時間（秒単位）を指定します。オリジン サーバーからデータをダウンロードするために、Content Gateway が接続をオープンする度に、データをダウンロードした後、指定されたタイムアウト時間の間、接続を続けます。タイムアウト時間前に後続のデータ要求が必要ない場合は、Content Gateway は接続を閉じます。その場合、タイムアウト時間は再開始します。 オリジン サーバーは いつでも接続を閉じることができます。
Inactivity Timeouts（非アクティブ タイムアウト）：Client	トランザクションが停止した場合に、Content Gateway がクライアントとの接続を開き続ける時間を指定します。Content Gateway がデータの受信を停止した場合や、クライアントがデータの読み込みを停止した場合、Content Gateway は、このタイムアウト時間が経過した後、接続を閉じます。 クライアントは いつでも接続を閉じることができます。
Inactivity Timeouts: Origin Server	トランザクションが停止した場合に、Content Gateway がオリジン サーバーとの接続を開き続ける時間を指定します。Content Gateway が、オリジン サーバーからのデータ受信を停止した場合、このタイムアウト時間が経過するまで、接続を閉じません。 オリジン サーバーは いつでも接続を閉じることができます。
Active Timeouts（アクティブ タイムアウト）：Client	Content Gateway が、クライアントと接続されたままになる時間を指定します。このタイムアウト時間の前に、クライアントが 要求（読み込み および 書き込みデータ）を完了していない場合、Content Gateway は接続を閉じます。 デフォルト値の 0 は タイムアウトなしです。 クライアントは いつでも接続を閉じることができます。
Active Timeouts: Origin Server Request（オリジン サーバー要求）	Content Gateway がオリジン サーバーへの接続要求の完了を待つ時間を指定します。 このタイムアウト時間の前に、Content Gateway が オリジン サーバーと接続を確立できなかった場合、Content Gateway は接続を終了します。 デフォルト値の 0 は タイムアウトなしです。 オリジン サーバーは いつでも接続を閉じることができます。

Active Timeouts: Origin Server Response（オリジン サーバー応答）	Content Gateway がオリジン サーバーからの応答を待つ時間を指定します。
FTP Control Connection Timeout（FTP 接続の制御のタイムアウト）	Content Gateway が FTP サーバーからの応答を待つ時間を指定します。指定した時間内に FTP サーバーが応答しない場合、Content Gateway はクライアントのデータ要求を破棄します。このオプションは、HTTP クライアントからの FTP 要求のみに適用されます。 デフォルト値は 300 です。

HTTP Responses（HTTP 応答）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Protocols] > [HTTP Responses] > [General]

Response Suppression Mode（応答抑制モード）	Content Gateway は、特定のクライアント トランザクションで HTTP の問題（利用できないオリジン サーバー、認証要件、プロトコル エラーなど）を検出した場合に、クライアント ブラウザに HTML 応答を送信します。Content Gateway には、HTTP エラーの詳細をクライアントに説明する変更不可のデフォルトの応答ページのセットがあります。 クライアントに HTTP 応答を送信しない場合、**[Always Suppressed]** を選択します。 非透過的なトラフィックのみに HTTP 応答を送信する場合、**[Intercepted Traffic Only]** を選択します。（Content Gateway が透過的に実行されていて、キャッシュの存在を示したくない場合に、このオプションは有用です。） すべてのクライアントに HTTP 応答を送信する場合、**[Never Suppressed]** を選択します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Protocols] > [HTTP Responses] > [Custom]

Custom Responses（カスタム応答）	Content Gateway が クライアントに送信する応答をカスタマイズすることができます。デフォルトでは、カスタマイズ可能な応答は、Content Gateway の **config/body_factory/default** ディレクトリにあります。 **Accept-Language ヘッダー**で指定された言語で、クライアントにカスタマイズされた応答を送信する場合、`[Select Enabled Language-Targeted Response]` を選択します。 デフォルト ディレクトリにあるカスタム応答をクライアントに送信するには、**[Enabled in "default" Directory Only（デフォルト ディレクトリにのみ有効）]** を選択します。 カスタム応答を無効にする場合、**[Disabled]** を選択します。**[Response Suppression Mode]** オプションで、**[Never Suppressed]** または **[Intercepted Traffic Only]** が選択されている場合、Content Gateway は変更不可のデフォルトの応答を送信します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Custom Response Logging（カスタム応答ログ記録）	有効にした場合、カスタム応答が使用 または変更された時に、Content Gateway はエラー ログに メッセージを送信します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Custom Response Template Directory（カスタム応答テンプレート ディレクトリ）	カスタム応答の位置するディレクトリを指定します。デフォルトの場所は、Content Gateway **config/body_factory** ディレクトリです。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

カスタム応答ページへのイメージ、動画 gift、Java アプレットの組み込み

Content Gateway はクライアントへの応答にシングル テキストまたは HTML ドキュメントのみを使用できます。

しかし、カスタム応答ページにイメージ、動画 gift、Java アプレットまたは Web サーバーに置かれているテキスト以外のオブジェクトへのリファレンスを提供できます。

body_factory テンプレート ファイルにリンクを追加する方法は、HTML ドキュメントにイメージを追加するのと同じ方法で、SRC 属性に完全な URL を指定します。

Web サーバーと Content Gateway が同じポート番号を使ってドキュメントを送信しようとするのを防止するために、これらのプログラムを同じシステムで実行しないことを推奨します。

HTTP Scheduled Update

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Protocols] > [HTTP Scheduled Updates] > [General]

Scheduled Update（スケジュール設定した更新）	Scheduled Update オプションを有効化 または 無効化します。このオプションを有効化した場合、Content Gateway は、指定した時間にローカル キャッシュ内の特定のオブジェクトを自動的に更新します。
Maximum Concurrent Updates（最大同時更新）	許容する同時更新要求の最大数を指定します。スケジュール設定した更新が、ホストに過大な負荷をかけないようにするために、このオプションを有効にします。デフォルト値は 100 です。
Retry on Update Error（更新エラー時の再試行）：Count（カウント）	失敗した場合に、URL のスケジュール設定した更新を再試行する回数を指定します。デフォルト値は 10 回です。
Retry on Update Error（更新エラー時の再試行）：Interval（間隔）	失敗した場合に、URL のスケジュール設定した各更新の再試行の間隔を秒単位で指定します。デフォルト値は 2 秒です。

[Configure] > [Protocols] > [HTTP Scheduled Updates] > [Update URLs]

[Force Immediate Update（即時更新を強制する）] を有効化します。	有効にした場合、Content Gateway は すべてのスケジュール設定した更新の期限切れ時刻を上書きし、25 秒毎に更新を開始します。
Scheduled Object Update（スケジュール設定されたオブジェクト更新）	Content Gateway が、指定したローカル キャッシュ コンテンツのスケジュール設定した更新を制御する方法を指定する *update.config* ファイル内のルールのテーブルを表示します。

Refresh（リフレッシュ）	**update.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**update.config** ファイル編集、および ルールを追加するために、設定ファイル エディタを開きます。
	update.config Configuration File Editor（update.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	**update.config** ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
URL	更新する URL を指定します。
Request Headers（オプション）	各 **GET** 要求で渡されたヘッダー（セミコロンで区切り）のリストを指定します。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。デフォルトは、要求ヘッダーなしです。
Offset Hour	更新時間を導出するために使用する基準時間を指定します。範囲は 00-23 時です。
Interval（間隔）	更新が行われる（オフセット時間からの）間隔（秒）。
Recursion Depth（再帰の深さ）]	参照されている URL が再帰的に更新される（指定した URL からの）深さ。たとえば、再帰の深さが 1 であれば、指定した URL と、元の URL からのリンクによって直接に参照されるすべての URL が更新されます。

HTTPS

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Protocols] > [HTTP]

このページは、**[Configure] > [My Proxy] > [Basic] > [General]** で HTTP が有効化されている場合のみ表示されます。

HTTP Proxy Server Port（HTTP プロキシ サーバー ポート）	Content Gateway が、HTTPS トラフィックの Web プロキシ サーバーとして動作する時に使用するポートを指定します。デフォルト値は 8080 です。 *[Configure] > [Protocols] > [HTTP] > [General]* **も参照してください。HTTPS ports（HTTPS ポート）**

Tunnel Skype（Skype のトンネリング）	HTTPS が有効であり、Content Gateway が明示的プロキシである場合に、Skype トラフィックの トンネリングを有効化 / 無効化します。 **設定を完了するには**、Skype の使用を許可されたすべてのユーザーが、**[インターネット電話]** を許可する Web Security フィルタリング ポリシーを使用していることを確認します。HTTPS を有効化して Skype を使用するか否かに関わらず、これは必要です。 また、Skype が禁止されていない場合、ハンドシェークの後、Skype は非 HTTP ポートを使ってトラフィックをルーティングします。Content Gateway を経由するように Skype を強制するには、『Skype IT Administrators Guide』 に記載されている通り、GPO を使用します。 **ご注意：**HTTPS が有効化されていない場合、このオプションは必要ありません。 **ご注意：**Content Gateway が透過的プロキシの場合、このオプションは無効です。
Tunnel Unknown Protocols（未知のプロトコルのトンネリング）	SSL ハンドシェイクで [未知のプロトコル] エラーが発生した時に、HTTPS 要求のトンネリングを有効化および無効化します。 **トンネリングされた接続は、復号化または検査をされません。** Content Gateway が明示的プロキシである場合、サーバーに SSL 接続要求が行われる前に、URL ルックアップが実行され、ポリシーが適用されます。そのため、トンネリングされたトランザクションが Web Security のトランザクション ログに表示されます。 Content Gateway が透過的プロキシであるとき、SNI がある場合は SNI のホスト名に基づき URL ルックアップを実行します。それ以外の場合は URL ルックアップは実行できず、トンネリングされたトランザクションはログに記録されません。これは SSL 証明書から共通名を取得するために最初にサーバーとの接続が要求されるからです。これは URL ルックアップに使用されます。接続ハンドシェイクが失敗し、このオプションが有効にされている場合、プロキシに認識されることなく接続がトンネリングされます。 **重要：**この設定は、HTTP 機能が無効にされた（**[Configure] > [My Proxy] > [Basic] > [General]** で）場合でも保持されます。そのため、HTTPS サポートを無効化する場合は、その前にこのオプションを無効化する必要があります。

FTP

Help | Content Gateway | バージョン 7.8.x

> **注意**
> FTP 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで FTP 処理を有効化した場合だけ、[Configure] ペインに表示されます。

[Configure] > [Protocols] > [FTP] > [General]

FTP Proxy Server Port（FTP プロキシ サーバー ポート）	Content Gateway が、FTP 要求を受け入れるために使用するポートを指定します。デフォルト ポートは 2121 です。
ポート構成のリッスン	データ転送のために FTP が開くリッスン ポートを指定します。 **[Default Settings]** を選択すると、オペレーティング システムが使用可能なポートを選択します。Content Gateway は 0 を送信し、リッスンが成功すれば新しいポート番号を取得します。 **[Listening Port (Max)]** および **[Listening Port (Min)]** フィールドで指定されたポート範囲によってリッスン ポートを決定する場合、**[Specify Range]** を選択します。
Default Data Connection Method（デフォルトのデータ接続方法）	FTP サーバーとのデータ接続設定に使用するデフォルトの方法を指定します。 **[Proxy Sends PASV]** を選択すると、FTP サーバーに PASV を送信し、FTP サーバーはリッスン ポートを開きます。 **[Proxy Sends PORT]** を選択すると、Content Gateway 側に最初の接続のリッスン ポートをセットアップします。
Shared Server Connections（共有サーバー接続）	有効にすると、サーバー コントロール接続が、複数の匿名 FTP クライアントの間で共有されます。

[Configure] > [Protocols] > [FTP] > [Timeouts]

Keep-Alive Timeouts: Server Control（サーバー コントロール）	どの FTP クライアントも FTP サーバー コントロール接続を使用しなくなった時の、タイムアウト値を指定します。デフォルト値は 90 秒です。
Inactivity Timeouts: Client Control（クライアント コントロール）	FTP クライアントコントロール接続のアイドル状態の持続時間を指定します。デフォルト値は 900 秒です。
Inactivity Timeouts: Server Control（サーバー コントロール）	FTP サーバーコントロール接続のアイドル状態の持続時間を指定します。デフォルト値は 120 秒です。
Active Timeouts: Client Control（クライアント コントロール）	FTP クライアントコントロール接続のオープン状態の持続時間を指定します。デフォルト値は 14400 秒です。
Active Timeouts: Server Control（サーバー コントロール）	FTP サーバーコントロール接続のオープン状態の持続時間を指定します。デフォルト値は 14400 秒です。

コンテンツ ルーティング

Help | Content Gateway | バージョン 7.8.x

Content Routing 設定オプションは、次のカテゴリに分けられます：

Hierarchies（階層）、368 ページ

Mapping and Redirection（マッピングおよびリダイレクト）、371 ページ

Browser Auto-Config（ブラウザ自動設定）、374 ページ

Hierarchies（階層）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Content Routing（コンテンツ ルーティング）] > [Hierarchies]

Parent Proxy（親プロキシ）	HTTP 親キャッシング オプションを有効化 または 無効化します。このオプションを有効にした場合、Content Gateway を HTTP キャッシュ階層を組み込むことができます。Content Gateway サーバーを、親ネットワーク キャッシュ（他の Content Gateway サーバー または 別のキャッシング製品）に接続して、クライアント要求実行中に親キャッシュに依存する子キャッシュのキャッシュ階層形成できます。*HTTP キャッシュ階層*、111 ページを参照してください。
No DNS and Just Forward to Parent（DNS ルックアップせず、親に転送）	このオプションを有効にした場合、HTTP 親キャッシュが有効になり、Content Gateway は 要求されたホスト名の DNS ルックアップを行いません。 選択された要求のみが親プロキシに送られるように、**parent.config** ファイルのルールが設定されている場合、Content Gateway は、親プロキシに送られる要求のみ名前解決をスキップします。親プロキシに送られない要求は、通常通りに名前解決が実行されます。親プロキシが停止していて、子プロキシが直接オリジン サーバーを参照できる場合、子プロキシは名前解決を実行します。
Uncacheable Requests Bypass Parent（キャッシュできない要求が親をバイパス）	このオプションが有効で、親キャッシングが有効な場合、Content Gateway は キャッシュできない要求の場合、親プロキシを迂回します。
HTTPS Requests Bypass Parent（HTTPS 要求が親をバイパス）	このオプションが有効にすると、Content Gateway は HTTPS 要求の場合に 親プロキシを迂回します。
Tunnel Requests Bypass Parent（トンネル要求が親をバイパス）	このオプションが有効にすると、Content Gateway は 非 HTTPS トンネル要求の場合に 親プロキシを迂回します。
Parent Proxy Cache Rules（親プロキシ キャッシュ ルール）	HTTP キャッシュ階層で使用される HTTP 親プロキシを指定し、選択された URL 要求が親プロキシを迂回するように設定された *parent.config* ファイルのルールのテーブルを表示します。 ルールはリストの上から順にチェックされ、最初に条件に一致するルールが適用されます。
Refresh（リフレッシュ）	**parent.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**parent.config** ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。

	parent.config Configuration File Editor（parent.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*parent.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Primary Destination Type（一次宛先タイプ）	下記の一次宛先タイプをリストします。 **dest_domain** は 要求されたドメイン名。 **dest_host** は 要求されたホスト名。 **dest_ip** は 要求された IP アドレス。 **url_regex** は URL に含まれる正規表現。
Primary Destination Value（一次宛先値）	一次宛先タイプの値を指定します。 例： 一次宛先が **dest_domain** の場合 このフィールドの値に yahoo.com を選択できます。 一次宛先タイプが **dest_ip** の場合、このフィールドに 123.456.78.9 を選択できます。 一次宛先が **url_regex** の場合 このフィールドの値に politics 選択できます。
Parent Proxy（親プロキシ）	親プロキシの IP アドレス または ホスト名、通信に使用するポート番号を指定します。親プロキシは リスト内で指定された順序に従って問い合わせを受けます。リスト内の最後の親サーバーによって要求が処理されなかった場合、オリジン サーバーにルーティングされます。各エントリはセミコロンで区切ります。例：**parent1: 8080**、**parent2: 8080**
Round Robin（ラウンド ロビン）	プロキシがクライアント IP アドレスに基づいたラウンドロビン内の親キャッシュ リストを経由する場合、**[true]** を選択します。 プロキシが厳格に順番どうりに要求を処理するためには、**[strict]** を選択します。たとえば、コンピュータ proxy1 が最初の要求を処理し、proxy2 が 2 番目の要求を処理するなど。 ラウンド ロビン選択を発生させたくない場合、**[false]** を選択します。
Go direct（直接アクセス）	**[true]** を選択すると、要求が親階層を迂回して、直接オリジン サーバーに向かいます。 要求が親階層を迂回することを望まない場合、**[false]** を選択します。

Secondary Specifiers（二次指定子）：Time（時間）	08: 00-14: 00 等の 24 時間クロックを使用して、時間範囲を指定します。範囲が 午前 0 時をまたぐ場合、2 つのカンマ区切りの範囲を入力します。たとえば、範囲が 午後 6: 00 から午前 8: 00 の場合、次のように入力します： `18: 00 - 23: 59, 0: 00 - 8: 00`
Secondary Specifiers: Prefix（接頭辞）	URL のパス部分の接頭辞を指定します。
Secondary Specifiers: Suffix（接尾辞）	.htm、.gif 等の URL のファイル接尾辞を指定します。
Secondary Specifiers: Source IP（送信元 IP）	クライアントの IP アドレス または IP アドレス範囲を指定します。
Secondary Specifiers: Port（ポート）	要求された URL の中のポートを指定します。

Secondary Specifiers: Method（メソッド）	要求された URL メソッドを指定します。例：
	`get`
	`post`
	`put`
	`trace`

Secondary Specifiers: Scheme（スキーム）	要求された URL のプロトコルを指定します。HTTP か FTP である必要があります。
Secondary Specifiers: User-Agent（ユーザー エージェント）	要求ヘッダーのユーザー エージェントの値を指定します。

Mapping and Redirection（マッピングおよびリダイレクト）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Content Routing（コンテンツ ルーティング）] > [Mapping and Redirection（マッピングとリダイレクト）]

Serve Mapped Hosts Only（マッピングされたホストのみを処理）	**remap.config** ファイルのマッピング ルールにリストされたオリジン サーバーへの要求のみをプロキシに処理させる場合、**[Required]** を選択します。要求が **remap.config** ファイルのルールに一致しない場合、ブラウザはエラーを受け取ります。このオプションは Content Gateway システムのセキュリティを強化します。
Retain Client Host Header（クライアント ホスト ヘッダーを保持）	このオプションが有効な場合、Content Gateway は 要求内のクライアント ホスト ヘッダーを保持します（マッピング変換内のクライアント ホスト ヘッダーは含みません）。

Redirect No-Host Header to URL（非ホスト ヘッダーを URL へリダイレクト）	`Host:` ヘッダーを提供しない旧バージョンのクライアントからの着信要求をリダイレクトする代替 URL を指定します。ヘッダーに対応して提供したオブジェクトをキャッシュする 状態をユーザーに説明し、ブラウザのアップグレードを指示するか、プロキシを迂回するオリジン サーバーへの直接のリンクを提供するページを設定することが推奨されます。代わりに **Host:** ヘッダーのない要求を特定のサーバーにマップするマップ ルールを指定することもできます。
URL Remapping Rules（URL リマップ ルール）	オリジン サーバーに接続せずに、永久的 または 一時的に HTTP 要求をリダイレクトする **remap.config** ファイルのマッピング ルールのテーブルを表示します。 **ご注意：**URL を同じドメインの別の URL にマッピングする場合、**[From Path Prefix]** フィールドに “/” を指定する必要があります。このテーブルの後の例を参照してください。
Refresh（リフレッシュ）	**remap.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**remap.config** ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。
	remap.config Configuration File Editor（remap.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	**remap.config** ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type（ルール タイプ）	remap.config ファイルに追加できるルールのタイプをリストします。 **[redirect]** は、オリジン サーバーに接続せずに、永久的に HTTP 要求をリダイレクトします。永久的リダイレクトは、（HTTP ステータス コード 301 を返すことで）URL 変更をブラウザに通知しますので、ブラウザはブックマークを更新できます。 **[redirect_temporary]** は、オリジン サーバーに接続せずに、一時的に HTTP 要求をリダイレクトします。一時的リダイレクトは、（HTTP ステータス コード 307 を返すことで）現在の要求のみの URL 変更をブラウザに通知します。 **map** および **reverse_map** はサポートされません。

From Scheme（マップ元のスキーム）	マッピング ルールのプロトコルを指定します。**rtsp** および **mms** はサポートされません。 **ご注意：**あるプロトコル（スキーム）の URL を別のプロトコル（スキーム）にマッピングすることは、サポートされていません。
From Host	マップ元の URL のホスト名を指定します。
From Port（オプション）	マップ元の URL のポート番号を指定します。
From Path Prefix（オプション）	マップ元の URL のパス接頭辞を指定します。 URL を同じドメインのサブ ページにリダイレクトしたい場合があります。例、“www.cnn.com” を “www.cnn.com/tech” にリダイレクト . このルールを使用するには [From Path Prefix] フィールドで “/” を指定しなければなりません。もし指定しなければ、再帰的にページ指定子が URL に追加されます。たとえば、[www.example.com/tech] が [www.example.com/tech/tech/tech/tech/tech/tech/tech/tech/...] になります。
From Query（オプション）	マップ元の URL のクエリーを指定します。
To Scheme（マップ先のスキーム）	**From Scheme** と一致しなければなりません。
To Host（マップ先のホスト）	マップ先の URL のホスト名を指定します。
To Port（オプション）	マップ先の URL のポート番号を指定します。
To Path Prefix（オプション）	マップ先の URL のパス接頭辞を指定します。
To Query（オプション）	マップ先の URL のクエリーを指定します。
{undefined}	マッピング ルールのメディア プロトコル タイプを指定します。サポートされていません。

Browser Auto-Config（ブラウザ自動設定）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Content Routing] > [Browser Auto-Config（ブラウザ自動設定）] > [PAC]

Auto-Configuration Port（ポートの自動設定）	Content Gateway が、自動設定ファイルをブラウザにダウンロードするポートを指定します。このポートは 他のすべてのプロセスに割り当てることはできません。デフォルト ポートは 8083 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
PAC Settings（PAC 設定）	PAC ファイル（**proxy.pac**）を編集します。*PAC ファイルの使用*、51 ページを参照してください。

[Configure] > [Content Routing] > [Browser Auto-Config] > [WPAD]

WPAD Settings（WPAD 設定）	**wpad.dat** ファイルを編集します。*WPAD の使用*、53 ページを参照してください。

セキュリティ

Help | Content Gateway | バージョン 7.8.x

Security 設定オプションは、次のカテゴリに分けられます：

Connection Control（接続の制御）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Security] > [Connection Control（接続の制御）]

オプション	説明
	Proxy Access（プロキシ アクセス）
Access Control（アクセス制御）	どのクライアントが Content Gateway にアクセスできるかを制御する *ip_allow.config* ファイルのルールを表示します。 デフォルトでは、すべてのリモートホストはプロキシへのアクセスを許可されています。
Refresh（リフレッシュ）	**ip_allow.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**ip_allow.config** ファイルを編集するために、設定ファイル エディタを開きます。
	ip_allow.config Configuration File Editor（ip_allow.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*ip_allow.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
IP Action（IP アクション）	追加できるルールのタイプをリストします。 **ip_allow** ルールは、[Source IP] フィールドにリストされたクライアントが、プロキシにアクセスすることを許可します。 **ip_deny** ルールは、[Source IP] フィールドにリストされたクライアントが、プロキシにアクセスすることを拒否します。
Source IP（送信元 IP）	クライアントの IP アドレス または IP アドレス範囲を指定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

FIPS Security（FIPS セキュリティ）

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Security] > [FIPS]

このオプションは HTTPS トラフィック および FIPS 140-2 暗号化標準に関連しています。

デフォルトでは、HTTPS トラフィックを処理する場合、Content Gateway は SSLv3 を使用して接続を受け入れます。SSLv3 は FIPS 140-2 に適合していません。

FIPS モードが有効化されている時、

- HTTPS 接続は TLSv1 以上のみを使用します
- HTTPS 接続は FIPS 140-2 で承認されているアルゴリズムを使用します
- Content Gateway はオリジン サーバー証明書要求への応答として、SHA-256 証明書を生成します。

警告
一度有効にすると、Content Gateway を再インストールしないと、FIPS 140-2 モードを無効にできません。Content Gateway がアプライアンス上にある場合、アプライアンスを再構成しなければなりません。

重要
システムの制限のため、FIPS 140-2 モードは、NTLM ユーザー認証（IWA の NTLM またはレガシー NTLM へのフォールバック）には使用できません。

詳細については、*FIPS 140-2 モード*、204 ページを参照してください。

オプション	説明
FIPS Enable/Disable ラジオ ボタン	デフォルトでは、Content Gateway は 非 FIPS 140-2 モードでインストールされます。 FIPS 140-2 モードに切り替えるためには、**[Enabled]** ラジオ ボタンを選択し、**[Apply]** をクリックし、Content Gateway を再起動します。 **警告**：一度有効にすると、Content Gateway を再インストールしないと、FIPS 140-2 モードを無効にできません。Websense アプライアンス インストールの場合、再インストールは システムの再構成を必要とします。

Data Security

Help | Content Gateway | バージョン 7.8.x

> **注意**
> Data Security 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブで Data Security を有効化し、**[Features]** テーブルで **[Integrated on-box（コンピュータに統合済み）]** を選択した場合にだけ、[Configure] メニューに表示されます。

[Configure] > [Security] > [Data Security]

オプション	説明
Data Security IP address [データ セキュリティ IP アドレス]	[Data Security Management Server] の IP アドレスを指定します。これは、Websense Data Security ポリシーの構成と管理が実行される場所です。
Analyze HTTPS Content	復号化したトラフィックを分析のために、Websense Data Security に送信するか、または宛先の直接に送信するかを指定します。
Analyze FTP Uploads	FTP アップロード要求を分析のために、Websense Data Security に送信するかどうかを指定します。FTP プロキシ機能を有効化する必要があります。*FTP*、367 ページを参照してください。

登録画面フィールド：

オプション	説明
Data Security Management server IP（データ セキュリティ管理サーバー IP）	[Data Security Management Server] の IP アドレスを指定します。これは、データ セキュリティ ポリシーの構成と管理が実行される場所です。
Data Security administrator user name（データ セキュリティ管理者のユーザー名）	Websense Data Security 管理者のアカウント名を指定します。管理者には 配備設定権限が必要です。
Data Security administrator password（データ セキュリティ管理者のパスワード）	Websense Data Security 管理者のパスワードを指定します。
[Register] ボタン	登録を開始します。このボタンはすべてのフィールドにデータが入力された後にのみ有効になります。

Access Control（アクセス制御）

Help | Content Gateway | バージョン 7.8.x

[Access Control] タブを次のように使用します：

- カスタム フィルタリング ルールを作成します
- プロキシ ユーザー認証を設定します

[Access Control] ページ上の *フィルタリング*タブは常に使用可能です。

その他のタブは、**[Configure] > [My Proxy] > [Basic]** タブの **[Authentication]** セクションで選択された認証方法に基づいて、動的に変化します。

いずれかの認証方法が有効化されている場合、常に *グローバル設定オプション*タブが表示されます。

[Integrated Windows Authentication（統合 Windows 認証）] が選択されている場合、次のタブが表示されます。

- *Integrated Windows Authentication（統合 Windows 認証）*
- *グローバル設定オプション*

LDAP が選択されている場合、次のタブが表示されます：

- *LDAP*
- *グローバル設定オプション*

Radius が選択されている場合、次のタブが表示されます：

- *Radius*
- *グローバル設定オプション*

NTLM が選択されている場合、次のタブが表示されます：

- *NTLM*
- *グローバル設定オプション*

[Rule-Based Authentication（ルール ベースの認証）] が選択されている場合、次のタブが表示されます。

- **ドメイン**
- **認証ルール**
- *グローバル設定オプション*

下の表は各タブの各フィールドの目的を説明しています。目的のフィールドを見つけるためには、ブラウザの検索機能を使用してください。

Content Gateway ユーザー認証機能の詳細は、*Content Gateway ユーザー認証*、216 ページを参照してください。

[Configure] > [Security] > [Access Control（アクセス制御）] > [Filtering（フィルタリング）]

フィルタリング ルールは以下の処理のために使用することができます：

- URL 要求を拒否または許可する
- カスタム ヘッダを挿入する
- 指定したアプリケーション、または指定した Web サイトの要求が認証をバイパスすることを許可する
- クライアント要求のヘッダー情報を保持または削除する
- 指定したアプリケーションがプロキシを通過することを禁止する

ルールは順序が設定されており、ユーザー認証（構成されている場合）の前にチェックされます。ルールはリストの上から下へ辿り、最初に条件に一致するルールが適用されます。条件に一致するルールがない場合、要求は処理されます。

ルールは *filter.config* に保存されます。

ルールを追加、削除または変更した後、Content Gateway を再起動します。

フィルタリング ルールの詳細については、*フィルタリング ルール、206 ページ*を参照してください。

フィルタリング	フィルタリング ルールの順序指定されたリストを表示します。 デフォルトでは 3 つのフィルタリング ルールが設定されます。最初のルールは、すべてのアクセス先に対してポート 25 上のトラフィックを拒否します。2 番目と 3 番目のルールは、ThreatScope の 2 つの アクセス先に対してユーザー認証をバイパスします。
Refresh（リフレッシュ）	**filter.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**filter.config** ファイルを編集するために、設定ファイル エディタを開きます。
	filter.config Configuration File Editor（filter.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*filter.config* に現在保存されているルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。ルールを選択 または 値を入力した後、[Add] クリックします。

Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type（ルール タイプ）	ルール タイプを指定します。 **[allow]** を選択すると、特定の URL 要求が認証をバイパスすることを許可します。 **[deny]** を選択すると、特定の宛先からのオブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。 どのクライアント要求ヘッダ情報を保持するかを指定するためには、**[keep_hdr]** を選択します。 どのクライアント要求ヘッダ情報を削除するかを指定するためには、**[strip_hdr]** を選択します。 要求にカスタム ヘッダーを追加するには、**[add_hdr]** を選択します。このルールタイプは、**[Custom Header]** および **[Header Value]** で定義された値を必要とします。宛先ドメインの特定の要求に対応するために、カスタム ヘッダーを追加します。*フィルタリング ルール*、206 ページを参照してください。 ルール タイプ **[radius]** はサポートされていません。
Primary Destination Type（一次宛先タイプ）	下記の一次宛先タイプをリストします。 **dest_domain** は 要求されたドメイン名。 **dest_host** は 要求されたホスト名。 **dest_ip** は 要求された IP アドレス。 **url_regex** は URL に含まれる正規表現。
Primary Destination Value（一次宛先値）	一次宛先タイプの値を指定します。たとえば、Primary Destination Type が **dest_ip** の場合、このフィールドに 123.456.78.9 を指定できます。
Additional Specifier（追加の指定子）：Header Type（ヘッダー タイプ）	保持または削除するクライアント要求ヘッダー情報を指定します。 このオプションは、**keep_hdr** または **strip_hdr** ルールタイプにのみ適用されます。
Additional Specifier（追加の指定子）：Realm（オプション）	サポートされていません。
Additional Specifier（追加の指定子）：Proxy Port（プロキシ ポート）（オプション）	このルールに一致するプロキシ ポートを指定します。
Additional Specifier（追加の指定子）：Custom Header（カスタム ヘッダー）（オプション）	ルールタイプが **add_hdr** の場合に使用します。宛先ドメインが要求内で検索するカスタム ヘッダー名を指定します。

Additional Specifier（追加の指定子）：Header Value（ヘッダー値）（オプション）	ルールタイプが **add_hdr** の場合に使用します。宛先ドメインがカスタム ヘッダーと組になるカスタム ヘッダー値を指定します。
Secondary Specifiers: Time（時間）	時間範囲（例、08: 00-14: 00）を指定します。
Secondary Specifiers: Prefix（接頭辞）	URL のパス部分の接頭辞を指定します。
Secondary Specifiers: Suffix（接尾辞）	URL のファイル接尾辞を指定します。
Secondary Specifiers: Source IP（送信元 IP）	クライアントの IP アドレスを指定します。
Secondary Specifiers: Port（ポート）	要求された URL の中のポートを指定します。
Secondary Specifiers: Method（メソッド）	要求の URL メソッドを指定します： • **get** • **post** • **put** • **trace**
Secondary Specifiers: Scheme（スキーム）	要求された URL のプロトコルを指定します。以下のオプションがあります。 • **HTTP** • **HTTPS** • **FTP**（FTP over HTTP の場合のみ） **rtsp** および **mms** はサポートされません。
Secondary Specifiers: User-Agent（ユーザー エージェント）	要求ヘッダーのユーザー エージェントの値を指定します。 このフィールドを、次のアプリケーション フィルタリング ルールを作成するために使用します： • 認証の要求を適切に処理しないアプリケーションが認証をバイパスすることを許可する • 指定のクライアント ベースのアプリケーションからのインターネットのアクセスを禁止する
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Security] > [Access Control] > [Global Configuration Options（グローバル設定オプション）]

このページでは、下記のためのグローバル オプションを指定します。

- ユーザー認証が失敗した場合のフェイル オープン / フェイル クローズ アクション
- 資格情報キャッシング
- 透過的プロキシの場合、ネットワーク上のすべてのクライアントが解決できるプロキシの代替ホスト名必須。

詳細については、*グローバル認証オプション、220 ページ*を参照してください。

注意

明示的プロキシに対する NTLM キャッシュを無効にするためのユーザー インターフェース設定が削除されました。**proxy.config.ntlm.cache.enabled** の値を **0**（ゼロ）に設定することによって、records.config 内の明示的プロキシ トラフィックに対するキャッシュを無効化することができます（ただし、この方法は推奨されません）。

グローバル設定オプション

Fail Open	**[Disabled]** - 認証が失敗した場合に要求がインターネットへ送信されないようにします。 **[Enabled only for critical service failures（クリティカルなサービス障害の場合のみ有効化）]**（デフォルト）- 認証失敗の理由がドメイン コントローラからの応答がないこと、またはクライアントが送信しているメッセージの形式が不適切であることである場合に、要求の処理を許可します。 **[Enabled for all authentication failures（すべての認証失敗の場合に有効化]** - すべての認証失敗（パスワード エラーを含む）の場合に要求の処理を許可します。 フェイル オープンが有効化されていて、Web Security XID エージェントが構成されている場合、要求者を識別し、ユーザー ベースのポリシーを適用する試みが行われます。そうでない場合、クライアントの IP アドレスにポリシーが割り当てられている場合は、そのポリシーが適用されます。それ以外の場合は、デフォルトのポリシーが適用されます。 **重要：**ユーザー認証がルール ベースで、ドメイン リストを使用する時、 • [**Enabled only for critical service failures**] を選択している場合は、クリティカルなサービスの障害が発生した時、フェイル オープンは適用されません。エラーが発生した場合は常にフェイル クローズになります。 • [**Enabled for all authentication failures, including incorrect password**] を選択している場合は、リスト内のすべてのドメインで基本資格情報を試した後、フェイル オープンが適用されます。 **重要：**[Fail Open（フェイル オープン）] の設定は、IWA が認証方法であり、クライアントがドメインコントローラ（DC）がダウンしたために DC から kerberos チケットを取得できない場合には適用しません。[Fail Open] の設定は、IWA が NTLM にフォールバックし、認証が失敗した場合 IWA に適用しません。

資格情報キャッシング キャッシング方法	[**Cache using IP address only（キャッシュに IP アドレスのみを使用）**] - すべての資格情報が IP アドレスの代替を使ってキャッシングされることを指定します。これはすべてのクライアントが固有の IP アドレスを持っている場合に推奨される方法です。 [**Cache using Cookies only（キャッシュに Cookie のみを使用）**] - すべての資格情報が cookie の代替を使ってキャッシングされることを指定します。これはすべてのクライアントが IP アドレスを共有している場合 - たとえば、Citrix サーバーのようなマルチ ホスト サーバーを使用している場合 - や、トラフィックが Content Gateway へトラフィックを転送するデバイスによってネットワーク アドレス変換される場合に推奨される方法です。 [**Cache using both IP addresses and Cookies（キャッシュに IP アドレスと Cookie の両方を使用）**] - cookie キャッシング リストにリストされている IP アドレスには cookie の代替を使用し、他のすべての IP アドレスには IP アドレスの代替を使用することを指定します。これは、ネットワークに固有の IP アドレスを持つクライアントと、マルチ ユーザー ホストを使用するかネットワーク アドレス変換されるクライアントの両方が含まれる場合に推奨される方法です。 代替資格情報については、*代替資格情報*を参照してください。 **重要：** • Cookie モードのキャッシングは cookie をサポートしないアプリケーションや、または cookie のサポートが無効化されているブラウザでは使用できません。 • ブラウザが Internet Explorer である場合、ローカル イントラネット領域に完全なプロキシ ホスト名（“http: //host.domain.com” の形式）が追加されなければなりません。 • ブラウザが Chrome である場合、サードパーティーの cookie を許可するように設定するか、またはプロキシ ホスト名からの cookie（“host.domain.com” の形式）を許可するための例外を設定しなければなりません。 • cookie モードとして IP アドレスが設定されていて、要求方法が CONNECT である場合、キャッシングは実行されません。 • FTP 要求には cookie モードのキャッシングは実行されません。
Credential Caching（資格情報キャッシング）：Time-To-Live（継続時間）	キャッシュ内のエントリが保持される時間（分単位）を指定します。TTL を過ぎるとエントリは消去され、ユーザーが次に要求を送信した時、認証を要求されます。認証が成功した場合、エントリがキャッシュに保存されます。

Purge LDAP cache on authentication failure（認証失敗時に LDAP キャッシュをパージ）	LDAP ユーザー認証が失敗した時に、Content Gateway がそのクライアントの認証記録を LDAP キャッシュから消去することを指定します。
Redirect Hostname（リダイレクト ホスト名）	透過的プロキシの場合、ネットワーク上のすべてのクライアントが解決できるプロキシの代替ホスト名を指定します。必須。 詳細については、*リダイレクト ホスト名、224 ページ*を参照してください。

[Configure] > [Security] > [Access Control]> IWA

統合 Windows 認証（IWA）ページは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで IWA を有効化した場合だけ表示されます。

Windows ドメインと結合するか、または 結合を解除するために、このページを使用します。ドメインが結合されている場合、このページにはドメイン属性の要約と [Unjoin] ボタンが表示されます。

詳細は *統合 Windows 認証、225 ページ*を参照してください。

Integrated Windows Authentication（統合 Windows 認証）

Domain Name	完全修飾 Windows ドメイン名を指定します。
Administrator Name（管理者名）	Windows Administrator のユーザー名を指定します。
Administrator Password	Windows Administrator のパスワード指定します。 **ご注意：**名前とパスワードは結合時にのみ使用し、保存されません。
Domain Controller	ドメイン コントローラを見つける方法を指定します。 • DNS による自動検出 • DC 名と IP アドレス ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式のリストでバックアップ ドメイン コントローラも指定できます。

Content Gateway Hostname（Content Gateway ホスト名）	Content Gateway のホスト名を指定します。 IWA は、Kerberos に登録する時に ホスト名を NetBIOS 名として使用するため、ホスト名長は 15 文字を超えることができません（NetBIOS の制限）。また、V-Series は モジュール (Dom) 間で一意的であることを保障するために、ホスト名に 4 文字付加します。V-Series アプライアンス上では、ホスト名は 11 文字を超えることができません。 **重要**：一度ホスト名と結合されたドメインは変更できません。もしそうした場合、ドメインの結合を解除して、新しいホスト名と再結合するまで、IWA は 即座に動作を停止します。
Join Domain（ドメインの結合）	ドメインを結合するには、[Join Domain] をクリックします。

[Configure] > [Security] > [Access Control] > [LDAP]

LDAP 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで LDAP を有効化た場合だけ、[Configure] ペインに表示されます。

LDAP の設定の詳細は、*LDAP 認証*、233 ページを参照してください。

LDAP	
LDAP Server: Hostname（ホスト名）	LDAP サーバーのホスト名を指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
LDAP Server: Port（ポート）	LDAP 通信に使用するポートを入力します。デフォルトのポート番号は 389 です。 デフォルトの Global Catalog サーバー ポートを使用するには、ポート 3268 を指定します。 Secure LDAP が有効化されている場合、ポート 636 または 3269（セキュア LDAP ポート）を設定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
LDAP Server: Secure LDAP（セキュアな LDAP）	Content Gateway が LDAP サーバーとセキュア通信を行うかどうかを指定します。有効にすると、[LDAP Port] フィールド（上記）が 636 または 3269（セキュアな LDAP ポート）に設定されます。
LDAP Server: Server Type（サーバー タイプ）	検索フィルタを指定します。Microsoft Active Directory または他のディレクトリサービスを指定します。

LDAP Server: Bind Distinguished Name（バインド識別名）	LDAP ベースのディレクトリ サービスのユーザーの完全識別名（完全修飾名）を指定します。例： `CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM` このフィールドには最大 128 文字まで入力できます。 このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
LDAP Server: Password（パスワード）	**[Bind_DN]** フィールドに識別されるユーザーのパスワードを指定します。
LDAP Server: Base Distinguished Name（ベース識別名）	ベース識別名 (DN) を指定します。この値は LDAP 管理者から取得します。 正しいベース識別名 (DN) を指定する必要があります。そうでない場合は、LDAP 認証は機能しません。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Security] > [Access Control] > [Radius]

Radius 構成オプションは、**[Configure] > [[My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [Radius] を有効化した場合だけ、[Configure] ペインに表示されます。

Radius の設定の詳細は、*RADIUS 認証*、236 ページを参照してください。

Radius	
Primary Radius Server（プライマリ RADIUS サーバー）：Hostname（ホスト名）	プライマリ RADIUS 認証サーバーのホスト名または IP アドレスを入力します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Primary Radius Server: Port（ポート）	Content Gateway がプライマリ RADIUS 認証 サーバーとの通信に使用するポートの番号を指定します。デフォルト ポートは 1812 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Primary Radius Server: Shared Key（共有キー）	暗号化に使用するキーを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary Radius Server（（セカンダリ RADIUS サーバー）（オプション）：Hostname（ホスト名）	セカンダリ RADIUS 認証サーバーのホスト名または IP アドレスを入力します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

Secondary Radius Server (optional): Port（ポート）	Content Gateway がセカンダリ RADIUS 認証 サーバーとの通信に使用するポートの番号を指定します。デフォルト ポートは 1812 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary Radius Server (optional): Shared Key（共有キー）	暗号化に使用するキーを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Security] > [Access Control] > [NTLM]

NTLM 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで NTLM を有効化した場合だけ、[Configure] ペインに表示されます。

NTLM の設定の詳細は、*レガシー NTLM 認証、230 ページ*を参照してください。

NTLM	

Domain Controller Hostnames（ドメイン コントローラのホスト名]	カンマ区切り形式のリストで ドメイン コントローラのホスト名を指定できます。形式は下記の通りです。
	`host_name[: port][%netbios_name]`
	または
	`IP_address[: port][%netbios_name]`
	Active Directory 2008 を使用している場合、`netbios_name` を含めるか、SMB ポート 445 を使用しなければなりません。
	このオプションを変更した場合、Content Gateway を再起動する必要があります。

Load Balancing（ロード バランシング）	ロード バランシングを有効化または無効化します。有効にすると、Content Gateway は ドメイン コントローラに認証要求を送信するときにロードバランスを行います。 **ご注意**：複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Security] > [Access Control] > [Domains]

[Configure] > [My Proxy] > [Basic] > [General] タブの [Features] テーブルで **[Rule-Based Authentication]** を有効化した場合だけ、アクセス制御リストに [Domains] タブが表示されます。

認証ルールで指定できるドメインのリストを作成および保持するには、このタブを使用します。認証ルールを定義するには [Authentication Rules（認証ルール）] タブを使用します。必ず、*グローバル認証オプション、220 ページ*を設定してください。

> **重要**
>
> 認証ルールを設定する前に [Domains（ドメイン）] リストを設定する必要があります。
>
> ルールベースの認証を設定していなかった場合は、詳細について、*ルール ベースの認証、239 ページ*を参照してください。

ドメイン

Domain List（ドメイン リスト）	認証ルールで使用するために識別されたドメインの順序が指定されていないリスト。 ドメインと関連付けられている一部の属性を変更するには、**[Edit]** を使用します。 リストからドメインを削除するには、**[Delete]** または **[Unjoin（結合解除）]** をボタンを使用します。 ドメイン リストは auth_domains.config ファイルに保存されます。
Domain list: New Domain button（新規ドメイン ボタン）	ドメイン リストにドメインを追加するには、**[New Domain（新規ドメイン）]** ボタンを使用します。ドメインを指定できるように画面が展開されます。
	[New Domain] アクション
Domain Details（ドメインの詳細）：Domain Identifier（ドメイン識別子）	ドメインの一意な名前を指定します。名前は、Content Gateway によってのみ使用されます。それによって実際のドメインまたはディレクトリのどの属性も変更しません。 **重要：**ドメイン識別子がリストに追加された後、ドメイン識別子を変更できません。名前を変更するには、リストからそのエントリを削除し、新しい名前のドメインを再度追加します。

Domain Details: Authentication Method（認証方法）	認証方法の選択を指定します。IWA、レガシー NTLM、LDAP のいずれかです。RADIUS はサポートされません。 認証方法を選択した時、その方法に固有の設定のオプションがページに追加されます。 **重要：**ドメインがリストに追加された後、認証方法を変更できません。認証方法を変更するには、リストからそのエントリを削除し、新しい名前を指定するドメインを再度追加します。
Domain Details: Aliasing（別名の指定）	このルールに一致したすべてのユーザーについてフィルタリング サービスに送信するときの別名を指定します（オプション）。別名は静的である必要があります。空白（ブランク）にすることができます。別名はプライマリ ドメイン コントローラに存在している必要があります（DC はフィルタリング サービスが認識します）。*未知のユーザーと [別名] オプション、245 ページ*を参照してください。
IWA Domain Details（IWA ドメインの詳細）	これらのオプションは IWA が認証方法として指定された場合に表示されます。
Domain Name（ドメイン名）	完全修飾ドメイン名を指定します。例： corp-domain.example.com
Administrator Name（管理者名）	Windows Active Directory ドメインの管理者ユーザー名を指定します。
Administrator Password（管理者パスワード）	対応するドメイン管理者パスワードを指定します。 **ご注意：**名前とパスワードは結合時にのみ使用し、保存されません。
Domain Controller（ドメイン コントローラ）	ドメイン コントローラを見つける下記のどちらかの方法を指定します。 • DNS による自動検出 • DC 名または IP アドレス ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式のリストでバックアップ ドメイン コントローラも指定できます。

Content Gateway Hostname（Content Gateway ホスト名）	Content Gateway のホスト名を指定します。 IWA は、Kerberos に登録する時に ホスト名を NetBIOS 名として使用するため、ホスト名長は 15 文字を超えることができません（NetBIOS の制限）。また、V-Series は、ホスト名がモジュール（Dom）間で一意的であることを保障するために、ホスト名に 4 文字付加します。V-Series アプライアンス上では、ホスト名は 11 文字を超えることができません。 **警告：**一度ホスト名と結合されたドメインは変更できません。もしそうした場合、ドメインの結合を解除して、新しいホスト名と再結合するまで、IWA は 即座に動作を停止します。
Join Domain（ドメインの結合）	ドメインを結合するには、[Join Domain] をクリックします。
Legacy NTLM Domain Details（レガシー NTLM ドメインの詳細）	
Domain Controller（ドメイン コントローラ）	プライマリ ドメイン コントローラの IP アドレスとポート番号を指定します（ポート番号を指定しない場合、Content Gateway は ポート 139 を使用します）。続けて、カンマ区切り形式のリストで、ロードバランシングおよび フェールオーバーに使用するセカンダリ ドメイン コントローラを指定します。
Load Balancing（ロード バランシング）	複数 の NTLM DC 間でロード バランシングを適用するにはこのチェック ボックスを選択します。 **ご注意：**複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。
LDAP Domain Details（LDAP ドメインの詳細）	
LDAP Server Name（LDAP サーバー名）	LDAP サーバー名を指定します。
LDAP Server Port（LFSP サーバー ポート）	LDAP サーバー ポートを指定します（オプション）。 デフォルトは 389 です。

LDAP Base Distinguished Name（LDAP ベース識別名）	LDAP ベース識別名を指定します。
LDAP Server Type（LDAP サーバー タイプ）	Active Directory の場合、検索フィルタを [sAMAccountName] に指定します。その他のディレクトリ サービスでは、[uid] に指定します。
Bind Domain Name（バインド ドメイン名）	LDAP バインド アカウント識別名を指定します。 例： CN=John Smith,CN=USERS,DC=MYCOMPANY, DC=COM フィールドの長さは、128 文字以内に制限されています。 値が指定されていない場合、Content Gateway は匿名でバインドを試みます。
Bind Password（バインド パスワード）	LDAP バインド アカウントパスワードを指定します。
Secure LDAP（セキュアな LDAP）	Content Gateway が LDAP サーバーとセキュア通信を行うかどうかを指定します。 有効化した場合、LDAP ポートに下記のどちらかのセキュア ポートを設定する必要があります : 636 または 3269。

[Configure] > [Security] > [Access Control] > [Authentication Rules（認証ルール）]

[Configure] > [My Proxy] > [Basic] > [General] タブの [Features] テーブルで **[Rule-Based Authentication（ルールベースの認証）]** を有効化した場合だけ、アクセス制御リストに [Authentication Rules（認証ルール）] タブが表示されます。

認証ルールを作成および保持するには、このタブを使用します。認証ルールで指定できるドメインのリストを作成および保持するには、**[Domains（ドメイン）]** タブを使用します。認証ルールを定義する前に [Domains] リストを設定する必要があります。

必ず、*グローバル認証オプション、220 ページ* を設定してください。

重要

ルールベースの認証を設定していなかった場合は、詳細について、*ルール ベースの認証、239 ページ*を参照してください。

認証ルール

Authentication Rule List（認証ルール リスト）	ユーザー認証に対して定義されているルールの順序指定済みリストのテーブルが表示されます。ルールは、1 つまたは複数の IWA、LDAP、および NTLM ドメインに対して認証されるクライアントのセットに対して定義されます。*ルール ベースの認証*、239 ページを参照してください。
Refresh（リフレッシュ）	**auth_rules.config** ファイルの現在のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	認証ルール エディタを開きます。 **警告：**ルールを直接に設定ファイルで編集してはいけません。
	auth_rules.config Configuration File Editor（auth_rules.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	現在のルール セットを順にリストします。ユーザー認証を実行する時、リストが上から下に順に検討され、最初に一致したルールが適用されます。 編集するルールを選択します。 ボックスの左側の矢印で、選択したルールをリスト内で上下に移動できます。 [X] ボタンは選択したルールを削除します。 ルールを 512 文字以上にすることはできません。
Add（追加）	新しいルールを追加します。
Set（設定）	選択したルールを現在の値によって更新します。
Status（ステータス）	ルールを保存し Content Gateway が再起動された後、ルールを有効化（アクティブ）するか、無効化するかを指定します。 ルールを作成し、ネットワークの他の要素がそのルールをサポートできるまで有効化しないように設定できます。
Rule Name（ルール名）	ルールのわかりやすい一意な名前を指定します。名前は 50 文字を超えないようにしてください。

Source IP（送信元 IP）	このルールの IP アドレス、または IP アドレス範囲を指定します（スペースを含めないでください）。 例：10.1.1.1 または 0.0.0.0-255.255.255.255 または 10.1.1.1,20.2.2.2,3.0.0.0-3.255.255.255
Proxy Port（プロキシポート）	Content Gateway が明示のプロキシとして配備されている時のトラフィックのインバウンドポートを指定します。定義されていない場合は、**[Configure] > [Protocols] > [HTTP] > [General]** で設定されている通り、すべてのポートが一致します。透過的プロキシ配備では、このフィールドを未定義にしておく必要があります。
User-Agent（ユーザーエージェント）	User-Agent 文字列の形式でテキストのマッチングを行う（たとえば、一般的なブラウザのマッチング）ために使用する 1 つ以上の正規表現を指定します。 Regex は POSIX に適合している必要があります。 演算子 [^] はサポートされていません。 このフィールドが空白である場合は、すべての User-Agent 値が一致します。 このフィールドを直接に編集できます。 共通ブラウザとして事前定義された regex を挿入するには、regex をドロップダウン リストから選択し、**[Add]** をクリックします。 複数の regex を指定できます。複数のエントリを区切るために、[|] 文字（論理和）を使用します。 regex の例を含む詳細については、*User-Agent をベースとする認証*、258 ページを参照してください。

Auth Sequence（認証シーケンス）	認証に使用するために 1 つ以上のドメインを指定します。 [Domains] ドロップダウン リスト（[Domains List（ドメインのリスト）] から取り込まれます）からドメインを選択し、その後、**[Include（含める）]** をクリックして、そのドメインをリストに追加します。 2 つ以上のドメインを追加する場合、エントリを選択し、上下の矢印を使って順序を設定できます。[X] ボタンを使用して選択したドメインを削除できます。 **最善の方法：**ユーザーのセットがどのドメインに属するか分かっている場合は、そのグループのルールだけ作成します。 **最善の方法：**既知のドメイン メンバーシップによって認証するユーザーの数が最も多いルールをリストの最上部に置きます。これらが最も早い認証方法です。 **最善の方法：**ユーザーのセットが属しているドメインがどれか分からない場合は、そのセットのユーザーを認証するのに必要な最小数のドメインを指定します。 **最善の方法：**常に対象を絞ったルールを作成することを推奨します。なぜなら大きなドメインのセットに対する認証を試みると、顕著な遅延が発生することがあるからです。 **重要：**ユーザー認証がルール ベースで、ドメイン リストを使用する時、 • ユーザーごとに、最初に成功した認証がキャッシュされ、以降の認証に使用されます。IP アドレス キャッシングが設定されている場合、IP アドレス代替がキャッシュされます。Cookie Mode が設定されている場合、クッキー代替がキャッシュされます。 **Fail Open** の場合： • **[Enabled only for critical service failures（クリティカルなサービス障害の場合のみ有効化）]** を選択した場合は、フェイル オープン設定が適用されません。タイムアウトになるまで、ユーザーは資格情報の入力を要求されつづけます。 • [**Enabled for all authentication failures, including incorrect password**] を選択している場合は、リスト内のすべてのドメインで基本資格情報を試した後、フェイル オープンが適用されます。

Apply（適用）	設定の変更を適用します。 **重要：**ルールが User-Agent として regex を指定した場合、**[Apply]** をクリックした時 regex が検証されます。regex が有効でない場合、ルールは削除され、再作成しなければなりません。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

SOCKS

Help | Content Gateway | バージョン 7.8.x

Content Gateway による SOCKS のサポートの詳細については、*SOCKS ファイアウォール統合の設定、211 ページ*を参照してください。

> **注意**
>
> SOCKS 設定オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで SOCKS を有効化した場合だけ、[Configure] ペインに表示されます。

[Configure] > [Security] > [Access Control] > [SOCKS] > [General]

SOCKS Version（SOCKS バージョン）	SOCKS サーバーに使用する SOCKS のバージョンを指定します。Content Gateway は SOCKS バージョン 4 と バージョン 5 をサポートしています。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Security] > [Access Control] > [SOCKS] > [Proxy]

SOCKS Proxy（SOCKS プロキシ）	SOCKS Proxy オプションを有効化または無効化します。SOCKS プロキシとして、Content Gateway はクライアントからの SOCKS パケットを受信し（通常はポート 1080 上で）、要求を SOCKS サーバーへ直接に転送することができます。 SOCKS Proxy オプションの詳細については、*SOCKS ファイアウォール統合の設定、211 ページ*を参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

SOCKS Proxy Port（SOCKS プロキシ ポート）	Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。通常これは ポート 1080 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Security] > [Access Control] > [SOCKS] > [Server]

On-Appliance SOCKS Server（アプライアンス上の SOCKS サーバー）	このオプションは、Content Gateway が Websense アプライアンス上のある場合のみ表示されます。 アプライアンス上の SOCKS サーバーを有効化または無効化します。 クライアント要求が SOCKS サーバーを経由するためには、SOCKS プロキシ オプションを有効化する必要があります。 **socks_server.config** を編集して、ネットワーク内の他の SOCKS サーバーの使用するように、Content Gateway を設定できます。次のエントリを参照してください。
Socks Servers table（Socks サーバー テーブル）	設定された SOCKS サーバーのテーブルを表示します。SOCKS サーバーの追加および設定については、*SOCKS サーバーの設定*、212 ページを参照してください。
Refresh（リフレッシュ）	**socks_server.config** ファイルの現在のエントリを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**socks_server.config** ファイルを編集するために、設定ファイル エディタを開きます。
	socks_server.config Configuration File Editor（socks_server.config 設定ファイル エディタ）
entry display box（エントリ表示ボックス）	Content Gateway で使用するために設定された SOCKS サーバーをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したエントリを削除、または 上下に移動できます。
Add（追加）	サーバーのリストにエントリを追加します。
Set（設定）	選択されたエントリを更新します。リストからサーバーを選択し、設定を修正し、**[Set]** をクリックしてエントリを更新します。
Clear Fields（フィールドの消去）	選択されたサーバーのすべてのフィールドをクリアします。
SOCKS Server Name（SOCKS サーバー名）	他の SOCKS サーバーと、この SOCKS サーバーを区別するための名前を指定します。
SOCKS Server Host（SOCKS サーバー ホスト）	SOCKS サーバーの IP アドレス、または内部 DN S サーバーによって解決できるホスト名を指定します。

SOCKS Port（SOCKS ポート）	SOCKS サーバーがリッスンするポートを指定します。
Default SOCKS Server（デフォルトの SOCKS サーバー）	この SOCKS サーバーをデフォルトの SOCKS サーバーとして指定する場合、オプションを選択します。
SOCKS User Name（SOCKS ユーザー名）	SOCKS 認証が使用される場合に、認証される SOCKS ユーザー名を指定します。
SOCKS Password（SOCKS パスワード）	SOCKS 認証が使用される場合に、指定したユーザーのパスワードを指定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。
Socks Server Rules（SOCKS サーバーのルール）	Content Gateway が指定したオリジン サーバーにアクセスするために経由しなければならない SOCKS サーバー、および Content Gateway が経由する SOCKS サーバーリストの順序を指定した **socks.config** ファイルのルールを表示します。 また、SOCKS サーバーを経由せずに、プロキシが直接アクセスするオリジン サーバーを指定することもできます。
Refresh（リフレッシュ）	**socks.config** ファイルの現在のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**socks.config** ファイルを編集するために、設定ファイル エディタを開きます。
	socks.config Configuration File Editor（socks.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*socks.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type（ルールタイプ）	プロキシに SOCKS サーバーを経由されるオリジン サーバーを指定するには、**[Route through SOCKS server]** を選択します。 プロキシが SOCKS サーバーを迂回して、直接アクセスするオリジン サーバーを指定するには、**[Do not route through SOCKS server]** を選択します。

Destination IP（宛先 IP）	**[Route through SOCKS server]** を選択した場合、下記の *[SOCKS Servers]* フィールドで指定された Content Gateway が使用する SOCKS サーバーに、オリジン サーバーの 1 つの IP アドレス **または** IP アドレスの範囲を指定します。 **[Do not route through SOCKS server]** を選択した場合、（SOCKS サーバーを経由せずに）プロキシに直接アクセスさせるオリジン サーバーの IP アドレスを指定します。1 つの IP アドレス、IP アドレスの範囲、または IP アドレスのリストを入力できます。リストの各エントリをカンマで区切ります。下記のすべてのネットワーク ブロードキャスト アドレスを指定してはいけません。255.255.255.255.
SOCKS Server（SOCKS サーバー）	**[Route through SOCKS server]** を選択した場合、要求を通過させる SOCKS サーバー を選択します。
Round Robin（ラウンド ロビン）	Content Gateway が厳格にラウンドロビン方式を使用するかどうかを指定します。**[strict]** または **[false]** を選択できます。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Security] > [Access Control] > [SOCKS] > [Options]

Server Connection Timeout（サーバー接続タイムアウト）	Content Gateway が SOCKS サーバーへの接続を試みて待機する時間（秒）を指定します。この時間を過ぎるとタイムアウトになります。
Connection Attempts Per Server（サーバーあたりの接続試行回数）	Content Gateway が特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、サーバーに [接続不能] というマークが付けられます。
Server Pool Connection Attempts（サーバー プール接続試行回数）	Content Gateway がプール内の特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、試行を中止します。

サブシステム

Help | Content Gateway | バージョン 7.8.x

Subsystem の設定オプションは、下記のカテゴリに分けられます。

キャッシュ、400 ページ

ログ記録、403 ページ

ネットワーク、407 ページ

キャッシュ

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Subsystems] > [Cache] > [General]

Allow Pinning（ピンニングを許可）	指定時間の間、キャッシュにオブジェクトを残しておくキャッシュ ピンニング オプションを有効化または無効化します。*cache.config* ファイルでキャッシュ ピンニング ルールを設定します。
Ram Cache Size（RAM キャッシュ サイズ）	RAM キャッシュのサイズをバイト単位で指定します。デフォルトのサイズは 104857600（100 MB）です。 値 [-1] は、Content Gateway に RAM キャッシュのサイズを自動的にディスク キャッシュの 1 GB につき約 1 MB にするように指示します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Maximum Object Size（最大オブジェクト サイズ）	キャッシュで許容されるオブジェクトの最大サイズのを指定します。 値 0（ゼロ）は、サイズ制限がないことを意味します。

[Configure] > [Subsystems] > [Cache] > [Partition]

Cache Partition（キャッシュ パーティション）	キャッシュのパーティション区分を制御する *partition.config* ファイルのルールを示すテーブルを表示します。
Refresh（リフレッシュ）	**partition.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。設定ファイル エディタで、ルールを追加 または 編集した後は、このボタンをクリックします。

Edit File（ファイルを編集）	**partition.config** ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。
	partition.config Configuration File Editor（partition.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*partition.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。このボタンをクリックする前に、表示されるフィールドに情報を入力します。
Set（設定）	このページ上部のルール表示ボックスを更新します。このボタンをクリックする前に、ルールを選択しプロパティを変更します。
Partition Number（パーティション番号）	1 から 255 までのパーティション番号を指定します。
Scheme（スキーム）	パーティションに保存されるコンテンツ タイプを指定します。HTTP のみがサポートされています。
Partition Size（パーティション サイズ）	パーティションに割り当てられるキャッシュ容量を指定します。このサイズは、全キャッシュ容量に対するパーセンテージか、MB 単位の絶対値を指定できます。
Partition Size Format（パーティション サイズ フォーマット）	下記のどちらかのパーティション サイズの形式を指定します。パーセンテージまたは絶対値。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Subsystems] > [Cache] > [Hosting]

Cache Hosting（キャッシュ ホスティング）	指定のオリジン サーバー、および ドメインのキャッシュ パーティションへの割り当てを制御する **hosting.config** ファイルのルールのテーブルを表示します。
Refresh（リフレッシュ）	**hosting.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**hosting.config** ファイルを編集するために、設定ファイル エディタを開きます。 設定ファイル エディタ ページについては後述します。

	hosting.config Configuration File Editor（hosting.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	**hosting.config** ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Primary Destination Type（一次宛先タイプ）	下記のどちらかの条件に基づいて一次宛先タイプを指定します。 ドメインに基づいてキャッシュのパーティション区分を行うの場合、**domain** を選択します。 ホスト名に基づいてキャッシュのパーティション区分を行うの場合、**hostname** を選択します。
Primary Destination Value（一次宛先値）	特定のパーティションに保存するコンテンツのドメイン、またはオリジン サーバー ホスト名を指定します。
Partitions（パーティション）	指定したオリジン サーバー または ドメインに属するコンテンツを保存するパーティションを指定します。各パーティションをカンマで区切ります。 ご注意：パーティションが、既に **partition.config** ファイルに作成されている必要があります。パーティション作成については、*キャッシュのパーティション区分、118 ページ*を参照してください。
Partitions	指定したオリジン サーバー、または ドメインに属するコンテンツを保存するパーティションのカンマ区切り形式のリストを指定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

ログ記録

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Subsystems] > [Logging] > [General]

Logging（ログ記録）	トランザクションをイベント ログ ファイル および / または エラー ログ ファイルに記録する、イベントログ記録を有効化 または 無効化します。 トランザクションを選択したイベント ログ ファイルに、エラーをエラー ログファイルに記録する場合、**[Log Transactions and Errors]** を選択します。 トランザクションのみを選択したイベント ログ ファイルに記録する場合、**[Log Transactions Only]** を選択します。Content Gateway は エラー ログ ファイルにエラーを記録しません。 エラーのみをエラー ログ ファイルに記録する場合、**[Log Errors Only]** を選択します。Content Gateway は トランザクションを選択したイベント ログ ファイルに記録しません。 ログ記録を停止する場合、**[Disabled]** を選択します。
Log Directory（ログ ディレクトリ）	Content Gateway がイベント ログを保存するディレクトリのパスを指定します。ディレクトリのパスは、Content Gateway クラスタのフェイルオーバー グループ内の各ノードで同じである必要があります。デフォルトのパスは下記のとおりです。/opt/WCG/logs
Log Space（ログ スペース）：Limit（制限）	ログ ファイルのログ記録ディレクトリに割り当てられる最大容量（メガバイト単位）を指定します。 Content Gateway が Websense アプライアンス上にある場合は、そのサイズは 5120 (5GB) に設定され、これを変更することはできません。 Content Gateway がスタンドアローン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。 **ご注意：**トランザクション ログは大量のディスク スペースを消費します。この制限が、ログ記録ディレクトリを含むパーティションの使用可能な実容量より、小さいことを確認してください。
Log Space: Headroom（ヘッドルーム）	ログ記録容量限界の許容値を指定します。**[Auto-Delete Rolled Files（取り込みファイルの自動削除）]** オプションが有効になっている場合、ログ記録ディレクトリで利用できる空きスペースがヘッドルームより小さくなると、自動削除がトリガされます。

Log Rolling（ログ取り込み）：Enable/Disable（有効化 / 無効化）	ログ ファイル取り込みを 有効化 または 無効化します。ログ ファイルを処理しやすいサイズに維持するために、定期的に取り出すことができます。*イベント ログ ファイルの取り込み、284 ページ*を参照してください。
Log Rolling: Offset Hour（オフセット時間）	ログ ファイル取り込みが行われる時間を指定します。例えば、オフセット時刻が 0（真夜中）で、取り込み間隔が 6 時間であると、ログ記録の取り込みは、真夜中 (00: 00)、06: 00、12: 00、および 18: 00 に行われます。
Log Rolling: Interval（間隔）	**.old** ファイルへの取り込みまでに、Content Gateway がログ ファイルにデータを書き込む時間の長さを指定します。最小値は 300 秒（5 分）です。デフォルトのタイムアウト値は、21600 秒（6 時間）です。最大値は 86400（1 日）です。
Log Rolling: Auto-Delete Rolled Files（取り込みファイルの自動削除）	ログ ディレクトリで利用できるスペースが少なくなった時の、取り込みログ ファイルの自動的削除を有効化します。ログ ディレクトリの空き容量が **Log Space Headroom** 未満になると、自動削除がトリガされます。
Reverse DNS lookup for Threat Tracking（脅威の追跡のためのリバース DNS ルックアップ）	Web Security Threat ダッシュボード、ログおよびレポートにクライアント ホスト名を含めることを円滑にするために、リバース DNS ルックアップを有効化または無効化します。 **警告**：想定した結果を達成し、想定外のネットワーク動作を回避するために、このオプションを有効化する前に、必ずリバース DNS をネットワークに設定してください。

[Configure] > [Subsystems] > [Logging] > [Formats]

Squid Format（Squid フォーマット）：Enable/Disable（有効化 / 無効化）	Squid ログ フォーマットを有効化または無効化します。
Squid Format: ASCII/Binary	作成されるログ ファイルの種類（**[ASCII]** または **[Binary]**）を選択します。
Squid Format: Filename（ファイル名）	Squid ログ ファイルの名前を指定します。デフォルトのファイル名は **squid.log** です。
Squid Format: Header（ヘッダー）	Squid ログ ファイルに含めるテキスト ヘッダーを指定します。
Netscape Common Format（Netscape Common フォーマット）：Enable/Disable（有効化 / 無効化）	Netscape Common ログ フォーマットを有効化または無効化します。
Netscape Common Format: ASCII/Binary	作成されるログ ファイルの種類（**[ASCII]** または **[Binary]**）を選択します。

Netscape Common Format: Filename（ファイル名）	Netscape Common ログ ファイルの名前を指定します。デフォルトのファイル名は **common.log** です。
Netscape Common Format: Header（ヘッダー）	Netscape Common ログ ファイルに含めるテキスト ヘッダーを指定します。
Netscape Extended Format（Netscape Extended フォーマット）：Enable/Disable（有効化 / 無効化）	Netscape Extended ログ フォーマットを有効化 または 無効化します。
Netscape Extended Format: ASCII/Binary	作成されるログ ファイルの種類（**[ASCII]** または **[Binary]**）を選択します。
Netscape Extended Format: Filename（ファイル名）	Netscape Extended ログ ファイルの名前を指定します。デフォルトのファイル名は **extended.log** です。
Netscape Extended Format: Header（ヘッダー）	Netscape Extended ログ ファイルに含めるテキストヘッダーを指定します。
Netscape Extended 2 Format（Netscape Extended 2 フォーマット）：Enable/Disable（有効化 / 無効化）	Netscape Extended-2 ログ フォーマットを有効化または無効化します。
Netscape Extended 2 Format: ASCII/Binary	作成されるログ ファイルの種類（**[ASCII]** または **[Binary]**）を選択します。
Netscape Extended 2 Format: Filename（ファイル名）	Netscape Extended-2 ログ ファイルの名前を指定します。デフォルトのファイル名は **extended2.log** です。
Netscape Extended 2 Format: Header（ヘッダー）	Netscape Extended-2 ログ ファイルに含めるテキストヘッダーを指定します。

[Configure] > [Subsystems] > [Logging] > [Splitting]

Split ICP Logs（ICP ログの分割）	このオプションを有効化した場合、Content Gateway は ICP トランザクションを別個のログ ファイルに記録します。 このオプションを無効化した場合、Content Gateway は、ICP トランザクションを HTTP および FTP エントリと同じログ ファイルに記録します。
Split Host Logs（ホスト ログの分割）	このオプションを有効化した場合、Content Gateway は、log_hosts.config ファイルにリストされている各ホストについて別個のログ ファイルを作成します。 このオプションを無効化した場合、Content Gateway は、すべてのホストのトランザクションを同じログ ファイルに記録します。

[Configure] > [Subsystems] > [Logging] > [Collation]

Collation Mode（照合モード）	Content Gateway ノードのログ照合モードを指定します。ログ ファイル照合機能を使用して、ログ記録されたすべての情報を一箇所で保存することができます。ログファイル照合については、*イベント ログ ファイルの照合*、289 ページを参照してください。 Content Gateway ノードのログ照合を無効化するには、**[Collation Disabled（照合無効化）]** を選択します。 Content Gateway ノードを照合サーバーにするには、**[Be a Collation Server（照合サーバーにする）]** を選択します。 Content Gateway ノードを照合クライアントにするには、**[Be a Collation Client（照合クライアントにする）]** を選択します。照合クライアントと設定された Content Gateway は、Squid、Netscape Common 等の アクティブな標準ログファイルのみを照合サーバーに送信します。このオプションを選択した場合、**[Log Collation Server（ログ照合サーバー）]** フィールドに、クラスタの照合サーバーのホスト名を指定します。 ご注意：**[Log collation host tagged（照合ホストをタグ付きでログ記録する）]** オプション（後述）を有効化しない限り、ログが照合されるときにログ エントリのソース（オリジンのノード）は失われます。 ログ照合は、1 つのノードにすべてのログエントリ送信する際に、クラスタの帯域幅を消費します。従って、クラスタのパフォーマンスに影響を及ぼします。 照合クライアントの Content Gateway に、カスタム（XML ベースの）ログ ファイルを送信させるためには、`logs_xml.config` ファイルに **LogObject** を指定する必要があります。

Log Collation Server（ログ照合サーバー）	ログ ファイルを送信するログ照合サーバーのホスト名を指定します。
Log Collation Port（ログ照合ポート）	照合サーバーとクライアント間の通信に使用するポートを指定します。ログ照合がアクティブな場合は、どの場合でも、ポート番号を指定する必要があります。デフォルトのポート番号は 8085 です。 ご注意：他のサービスが既に使用しているポートと競合しない限り、ホート番号を変更しないでください。
Log Collation Secret（ログ照合秘密）	クラスタ内のログ照合サーバーと他のノードとのパスワードを指定します。このパスワードは、ログ記録データを検証し、恣意的情報の交換を防止するために使用されます。
Log Collation Host Tagged（照合ホストをタグ付きでログ記録する）	このオプションを有効にした場合、Content Gateway は、照合ログ ファイルの最後にログ エントリを作成したノードのホスト名を追加します。
Log Collation Orphan Space（ログ照合オーファン スペース）	Content Gateway ノード上で、オーファン ログ ファイルを保存するためのログ記録ディレクトリに割り当てられる最大容量（メガバイト単位）を指定します。Content Gateway は、ログ照合サーバーと接続できない場合にオーファン ログ エントリを作成します。

[Configure] > [Subsystems] > [Logging] > [Custom]

Custom Logging（カスタム ログ記録）	カスタム ログ記録を有効化または無効化します。
Custom Log File Definitions（カスタム ログ ファイル定義）	カスタム（XML ベースの）ログ記録オプションを設定するために、*logs_xml.config* ファイルを表示します。

ネットワーク

Help | Content Gateway | バージョン 7.8.x

ネットワーク設定オプションは、下記のカテゴリに分けられます：

接続管理、408 ページ

ARM、411 ページ

WCCP、417 ページ

DNS Proxy（DNS プロキシ）、422 ページ

DNS リゾルバ、423 ページ

ICAP、427 ページ

仮想 IP、428 ページ

URL のヘルス チェック、429 ページ

接続管理

Help | Content Gateway | バージョン 7.8.x

[Connection Management（接続管理）] ページのオプションを使用して、接続スロットル、負荷の軽減、個別のクライアント接続の限度および率、ローメモリ状態への応答方法を含むプロキシ動作のいくつかの重要なプロパティを調整できます。

デフォルトでは、Content Gateway は 45,000 のネットワーク接続を受入ます。クライアントまたはオリジン サーバーの接続が設定された制限値の半分の 90 %（デフォルトでは 20,250）に到達したとき、接続スロットル イベントが発生します。接続スロットル イベントが発生した場合、Content Gateway は既存のすべての接続を処理し続けますが、接続カウントが制限値以下に下がるまで、新しいクライアントの接続要求をキューに入れます。

Content Gateway が接続制限に達したと思われる場合、パフォーマンス グラフをモニタして、コネクション アクティビティの正確な値を把握しておく必要があります。特に **[Active Client Connections（アクティブなクライアントの接続の数）]** および **[TCP ESTABLISHED Connections（TCP 確立済み接続）]** グラフに注目してください。またシステム ログ ファイル、エラー ログ ファイル、またはイベント ログ ファイルでエラー メッセージを調べることもできます。

[Configure] > [Networking] > [Connection Management] > [Throttling]

Throttling Net Connections（ネット接続のスロットル）	Content Gateway が、受け入れるネットワーク接続の最大数を指定します。デフォルト値は 45,000 です。 Content Gateway のスロットル制限は、ボトルネックの発生時のシステムの過負荷防止に役立ちます。ネットワーク接続がこの値に達した場合、Content Gateway は、既存の接続が閉じるまで新しい接続を順番待ちさせます。 この変数を最小値 100 より以下に設定しないようにしてください。

[Configure] > [Networking] > [Connection Management] > [Load Shedding]

Maximum Connections（最大接続数）	ARM が着信要求を直接オリジン サーバーに転送を開始する前に、許可されるクライアント接続の最大数を指定します。デフォルト値は、100 万件の接続です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

[Configure] > [Networking] > [Connection Management] > [Client Connection Control]

下記の事柄を指定します。

- クライアント同時接続限度
- クライアント接続率の限度
- 制限超過時のプロキシ応答
- 限度から除外されるクライアントのリスト

Concurrent Connection Limit（同時接続限度）：Maximum concurrent connections（最大接続数）	クライアントに許可される同時 HTTP/HTTPS 接続数の最大値を指定します。デフォルトは 1000 です。下記の値の範囲が有効です。1 - 45000
Concurrent Connection Limit: Alert when limit exceeded（限度超過時のアラート）	有効化にすると、クライアントが最大同時接続限度を超過した場合に、Content Gateway にアラートを発生させます。 Content Gateway マネージャにアラートを表示する他に、/var/log/messages および content_gateway.out にもログ記録します。
Concurrent Connection Limit: Close excessive connections when limit exceeded（限度超過時に過剰な接続を閉じる）	有効化すると、限度を超過した場合に Content Gateway に過剰な接続を閉じさせます。
Connection Rate Limit（接続率限度）：最大接続率	クライアントが接続可能な秒当たりの最大接続数（1 分間の平均）を指定します。デフォルトは 100 です。下記の値の範囲が有効です。1 - 1000

Connection Rate Limit: Alert when limit exceeded（限度超過時のアラート）	有効化すると、クライアントが最大接続率限度を超過した場合に、Content Gateway にアラートを発生させます。 Content Gateway マネージャにアラートを表示する他に、/var/log/messages および content_gateway.out にもログ記録します。
Connection Rate Limit: Close excessive connections when limit exceeded（限度超過時に過剰な接続を閉じる）	有効化すると、限度を超過した場合に Content Gateway に過剰な接続を閉じさせます。
Exceptions（例外）	接続限度を適用**しない** IP アドレス、または IP アドレスの範囲を指定します。IP アドレスは、IPv4 または IPv6（IPv6 サポートを有効化する必要があります）を指定できます。カンマ区切り形式のリストで、複数の IP アドレス または IP アドレスの範囲を指定できます。

[Configure] > [Networking] > [Connection Management] > [Low Memory Mode]

ホスト システムがロー メモリ状態になった場合に、Content Gateway が Web トラフィックの分析を中断するかどうかを指定します。この状態では、URL フィルタリングは通常通りに適用されます。

Low Memory Mode（ロー メモリ モード）：Enabled/Disabled（有効化 / 無効化）	ロー メモリ状態である場合コンテンツの分析を中断するには、**[Enabled]** を選択します。
Low Memory Mode Duration（ロー メモリ モード時間）	分析が中断される時間の長さを分単位で指定します。 タイマーが切れる前にロー メモリ状態が解決された場合、分析を再開し ロー メモリ トリガーをリセットします。 タイマーが切れた場合、分析を再開しますが、ロー メモリ モード トリガーをリセット**しません**。

ARM

Help | Content Gateway | バージョン 7.8.x

Adaptive Redirection Module（ARM）は、クラスタ通信インターフェース フェールオーバーのデバイス通知を送信する機能、および IP レイヤーが着信パケットを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更する機能を含むいくつかの重要な機能を実行します。

ARM は常にアクティブです。詳細については、*ARM*、62 ページを参照してください。

[Configure] > [Networking] > [ARM] > [General]

Network Address Translation（NAT）Statistics（ネットワーク アドレス変換（NAT）統計）	プロキシが透過的にトラフィックを処理する時に、着信パケットをどのようにアドレス変更するかを指定した *ipnat.conf* ファイルのリダイレクトのルールを表示します。Content Gateway はインストール中にリダイレクトのルールを作成します。これらのルールを変更できます。
Refresh（リフレッシュ）	**ipnat.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**ipnat.config** ファイルを編集するために、設定ファイル エディタを開きます。
	ipnat.conf Configuration File Editor（ipnat.conf 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*ipnat.conf* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Ethernet Interface（イーサネット インターフェース）	Content Gateway コンピュータへアクセスするトラフィックが使用するイーサネットインタフェースを指定します。例 `eth0`（Linux）
Connection Type（接続タイプ）	ルールに適用する接続タイプを指定します：TCP または UDP。
Destination IP（宛先 IP）	トラフィックの送信 IP アドレスを指定します。 0.0.0.0 は すべての IP アドレスにマッチします。
Destination CIDR（宛先 CIDR）	1.1.1.0/24 等の CIDR（Classless Inter-Domain Routing）形式の IP アドレスを指定します。このフィールドへの入力はオプションです。

Destination Port（宛先ポート）	トラフィックの宛先ポートを指定します：例 HTTP トラフィックの場合 80。
Redirected Destination IP（リダイレクトされる宛先 IP）	Content Gateway サーバーの IP アドレスを指定します。
Redirected Destination Port（リダイレクトされる宛先ポート）	プロキシポートを指定します。例 HTTP トラフィックの場合 8080。
User Protocol（ユーザー プロトコル）（オプション）	**dns** を選択した場合、ARM は DNS トラフィックを Content Gateway にリダイレクトします。そうでない場合は、DNS トラフィックはバイパスされます。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は破棄されます。
IP Spoofing（IP スプーフィング）：Enabled/Disabled（有効化 / 無効化）	IP スプーフィング オプションを有効化または無効化します。IP スプーフィング オプションは、Content Gateway の IP アドレスの代わりにクライアント IP アドレスを使用して、オリジン サーバーとの接続を確立するように、Content Gateway を設定します。詳細については、*IP スプーフィング、94 ページ*を参照してください。 **警告**：IP スプーフィングは、ネットワーク上のルーティング パスを正確に制御する必要があり、TCP ポート 80 および 443 上で実行する通常のルーティング プロセスを無効にする必要があります。
Range Based IP Spoofing（範囲ベースの IP スプーフィング）：Enabled/Disabled（有効化 / 無効化）	範囲ベースの IP スプーフィング拡張を有効化または無効化します。この拡張機能は、スプーフィングのために指定された IP アドレスへマッピングされる IP アドレスおよびアドレスの範囲の指定をサポートします。 多数のグループを指定できます。しかし、リストのトラバースが各接続要求の負荷を増やしますから、この機能を多用しないでください。リストが大きくなるほど、オーバーヘッドが大きくなります。 リストは（表示されている）順番でトラバースされます。最初のマッチが適用されます。 グループとマッチングしないクライアントは、独自の IP アドレスによってスプーフィングされます（基本 IP スプーフィング）。 詳細については、*IP スプーフィング、94 ページ*を参照してください。

Range Based IP Spoofing: Address table（アドレス テーブル）	**[Client IP Addresses]** フィールドで個別の IP アドレスおよび（または）IP アドレス範囲のカンマ区切りリストを入力します。スペースは使用できません。 以下を使用できます。 • 123.45.67.8 等の単一の IP アドレス • 1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式 • 1.1.1.1-2.2.2.2 等のダッシュで区切られた IP アドレス範囲 • 1.1.1.0/24,25.25.25.25,123.1.23.1-123.1.23.123 等のカンマで区切られた上記の組み合わせ。 **[Specified IP Address（指定対象の IP アドレス）]** フィールドにクライアントのマッチングで使用する IP アドレスを入力します。これは、スプーフィング対象の IP アドレスです。 テーブルに行を追加するには **[Add Row（行を追加）]** をクリックします。 テーブルから行を削除するには、セルのコンテンツを削除します。**[Apply]** をクリックすると、空の行が削除されます。 テーブルは常に最小 5 行を保持します。 変更を有効にするために、Content Gateway を再起動します。

[Configure] > [Networking] > [ARM] > [Static Bypass]

静的バイパス ルールは、要求をプロキシを通らないように経路指定します（バイパス）。ルールをクライアント（ソース）、オリジン サーバー（宛先）、または両方（ペア）に対して定義できます。*静的バイパス ルール、91 ページ* を参照してください。

> **重要**
> この機能は、透過的プロキシの配備のみを目的としています。

Static Bypass table（静的バイパス テーブル）	設定済みの静的バイパス ルールをリストします。Content Gateway が透過的トラフィックを処理するとき、プロキシは着信クライアント要求をバイパスするか、それらの要求を透過的に処理するかを決定するために、このルールを使用します。 ルールは *bypass.config* に保存されます。
Refresh（リフレッシュ）	**bypass.config** ファイルの最も最新のルールを表示するために、テーブルを更新します。
Edit File（ファイルを編集）	**bypass.config** ファイルを編集するために、設定ファイル エディタを開きます。

	bypass.config Configuration File Editor（bypass.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*bypass.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type（ルール タイプ）	ルール タイプを指定します。 **[bypass]** ルールは、指定された着信要求をバイパスします。 **[deny_dyn_bypass]** ルールは、指定された着信クライアント要求がプロキシをバイパスすることを禁止します（バイパス禁止ルールは、Content Gateway 自身をバイパスすることを禁止できます）。
Source IP（送信元 IP）	プロキシをバイパスするか、または バイパスを禁止する着信要求の送信元 IP アドレスを指定します。IP アドレスは、下記のいずれかの表記が可能です。 123.45.67.8 等の単一の IP アドレス 1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式 1.1.1.1-2.2.2.2 等のダッシュで区切られた IP アドレス範囲 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123 等のカンマで区切られた上記の組み合わせ
Destination IP（宛先 IP）	プロキシをバイパスするか、または バイパスを禁止する着信要求の宛先 IP アドレスを指定します。IP アドレスは、下記のいずれかの表記が可能です。 123.45.67.8 等の単一の IP アドレス 1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式 1.1.1.1-2.2.2.2 等のダッシュで区切られた IP アドレス範囲 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123 等のカンマで区切られた上記の組み合わせ
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Networking] > [ARM] > [Dynamic Bypass]

Dynamic Bypass（動的バイパス）	クライアントまたはサーバーに問題が発生した場合に、プロキシをバイパスし直接オリジン サーバーに向かう動的バイパス オプションを有効化 または 無効化します。Content Gateway を停止した場合、動的バイパス ルールは削除されます。
Behavior（動作）：Non-HTTP, Port 80（非 HTTP、ポート 80）	Content Gateway が ポート 80 上で非 HTTP トラフィックを検出した時に、動的バイパスを有効にするには、**[Enabled]** を選択します。 Content Gateway が ポート 80 上で非 HTTP トラフィックを検出した時に、動的バイパスを無効にするには、**[Disabled]** を選択します。 Content Gateway が ポート 80 上で非 HTTP トラフィックを検出した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、**[Source-Destination]** を選択します。 Content Gateway が ポート 80 上で非 HTTP トラフィックを検出した時に、動的宛先バイパスのみを有効にするには、**[Destination Only]** を選択します。
Behavior: HTTP 400	オリジン サーバーが 400 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 400 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 400 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 400 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。
Behavior: HTTP 401	オリジン サーバーが 401 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 401 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 401 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 401 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。

Behavior: HTTP 403	オリジン サーバーが 403 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 403 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 403 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 403 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。
Behavior: HTTP 405	オリジン サーバーが 405 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 405 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 405 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 405 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。
Behavior: HTTP 406	オリジン サーバーが 406 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 406 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 406 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 406 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。

Behavior: HTTP 408	オリジン サーバーが 408 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 408 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 408 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 408 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。
Behavior: HTTP 500	オリジン サーバーが 500 エラーを返した時に、動的バイパスを有効化するには、**[Eabled]** を選択します。 オリジン サーバーが 500 エラーを返した時に、動的バイパスを無効化するには、**[Disabled]** を選択します。 オリジン サーバーが 500 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効化するには、**[Source-Destination]** を選択します。 オリジン サーバーが 500 エラーを返した時に、動的宛先バイパスのみを有効化するには、**[Destination Only]** を選択します。

WCCP

Help | Content Gateway | バージョン 7.8.x

> **注意**
> WCCP 設定オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで WCCP を有効化た場合だけ、[Configure] ペインに表示されます。

このオプションは、Content Gateway での WCCP の使用を制御する **wccp.config** 設定ファイルに定義されています。エントリは、**[Configure] > [Networking] > [WCCP]** で提供されているエディタを使用して、定義および保守する必要があります。

管理者は、WCCP に関する実用的知識を持っていることが必要になります。

WCCP v2 のみサポートされています。

WCCP v2 の設定と処理能力に関する情報について、マニュアルおよび製造者のサポート サイトを参照することを強く推奨します。大部分のデバイスを、ハードウェア ベースのリダイレクトを最大限に活用するように構成する必要があります。Cisco デバイスでは、通常は IOS の最新バージョンが最も適切です。

アクティブな WCCP サービス グループは、それぞれに対応する ARM NAT ルールが必要です。*ARM*、411 ページを参照してください。

Content Gateway の WCCP v2 サポートの詳細は、*WCCP v2 デバイスによる透過的遮断*、65 ページを参照してください。

オプション	説明
WCCP Service Groups（WCCP サービス グループ）	**wccp.config** ファイルで定義されているサービス グループのテーブルを表示します。WCCP サービス グループの設定は WCCP の動作を定義します。列フィールドは下記の設定エディタ エントリで説明されています。
Refresh（リフレッシュ）	**wccp.config** ファイルの現在の定義を表示するために、テーブルをリフレッシュします。
Edit File（ファイルを編集）	設定ファイル エディタで、**wccp.config** ファイルを開きます。
Synchronize in the Cluster（クラスタ内の同期化）	クラスタ内に複数の Content Gateway ノードがある場合： クラスタ内で WCCP 設定 **(wccp.config)** を同期化させるために、このオプションを有効化します。それによってクラスタ内のどのノードでも設定変更ができるようになります。 クラスタ内で WCCP 設定を同期化**しない**場合は、このオプションを無効にします。この場合、WCCP 設定の変更は各ノードで個別に行う必要があります。一般的な使用例として、各ノードでどのサービス グループを有効化 / 無効化するかを制御するため、および（または）**weight** によって負荷の比例配分を行うためにこのオプションを使用できます。 このオプションが無効化された後に有効化された場合、このオプションを有効化したノードにおける設定が、クラスタの最初の同期化に使用されます。
	wccp.config Configuration File Editor（wccp.config 設定ファイル エディタ）
Service group display box（サービス グループ表示ボックス）	WCCP サービス グループの定義をリストします。 リスト内で編集するエントリを選択します。 選択を削除するには、[X] ボタンを使用します。 リストの順序に意味はありません。そのため、上 / 下矢印ボタンは無視されます。
Add（追加）	新しいサービス グループの定義を追加します。[Add] をクリックすると、ページの上部のボックス内に新しい定義が表示されます。
Set（設定）	選択したサービス グループの定義の変更を適用し、ページの上部のボックス内に新しい値を表示します。

オプション	説明
	Service Group Information（サービス グループの情報）
Service Group Status（サービス グループのステータス）	サービス グループを有効化または無効化します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Service Group Name（サービス グループの名前）	固有のサービス グループ名を指定します。これは管理に役立ちます。
Service Group ID（サービス グループの ID）	0 から 255 までのサービス グループ ID を指定します。この ID は、ルーター上でも設定しなければなりません。 既に使用中の番号を指定した場合は、[Add] または [Set] がクリックされた時にエラーを表示します。
Protocol（プロトコル）	このサービス グループに適用するプロトコル（TCP または UDP）を指定します。
Ports（ポート）	カンマ区切り形式のリストで最大 8 つのポートを指定します。
Network Interface（ネットワーク インターフェース）	このサービス グループに使用する Content Gateway ホスト システム上のネットワーク インターフェースを指定します。V10000 アプライアンスでは、eth0 は P1 にバインドされ、eth1 は P2 にバインドされます。
	Mode Negotiation（モードのネゴシエーション）
Special Device Profile（特別なデバイス プロファイル）	トラフィックが Cisco ASA ファイアウォールによってルーティングされるように指定するために **[ASA Firewall]** を選択します。このオプションが選択されたとき、Packet Forward Method および Packet Return Method として GRE が自動的に選択されます。これらの設定は必須であり、変更できません。
Packet Forward Method（パケット転送方法）	遮断されたトラフィックをプロキシに送信するために、WCCP ルーターによって使用される優先されるカプセル化の方法を指定します。ルーターが GRE および L2 をサポートしている場合、ここで指定された方法を使用します。 **重要：**GRE と Multicast は互換性がありません。 **重要：**WCCP デバイスとのアクティブな接続があるときに forward または return 方法の設定を変更した場合、その方法を再折衝するために、現在の接続の中断を強制する必要があります。通常は、そのために WCCP デバイス上のサービス グループを 60 秒間オフにします。WCCP デバイスのマニュアルを参照してください。

オプション	説明
Packet Return Method（パケット返送方法）	遮断されたトラフィックを WCCP ルーターに返信するために使用される、優先されるパケットカプセル化の方法を指定します。 **ご注意**：Content Gateway がルーターによってサポートされていない Forward/Return 方法を使用するように設定されている場合、プロキシはルーターによってサポートされている方法を折衝しようと試みます。 **ご注意**：L2 を選択するには、ルーターとスイッチが Content Gateway と Layer 2-adjacent（同じサブセットにある）であることが必要です。
	Advanced Settings（拡張設定）
Assignment Method（割り当て方法）	遮断されたトラフィックを複数のプロキシサーバーに配分するために使用する方法を指定します。選択肢は、**[HASH]** と **[MASK]** です。 MASK 値は最大 6 つの有効ビットまで適用されます（1 つのクラスタで、合計 64 個のバケットが作成されます）。 割り当て方法の詳細については WCCP のマニュアルを参照してください。ご使用のデバイスに、製造業者のマニュアルで推奨されている値を使用してください。
Distribution attribute (s)（配分属性）	どの要求がどのプロキシサーバーに配信されるかを決定するために、割り当て方法が使用する属性を指定します。 割り当て方法が HASH の場合、1 つ以上の配分属性を選択します。 割り当て方法が MASK の場合、1 つの配分属性を選択します。
Weight（ウェート）	このオプションは **Synchronize in the Cluster** が**無効化されている**ときのみ有効です。 比例重み付けによる要求のサーバーへの配分を指定します。**weight** をトラフィックの全フローに対する希望する割合の値に設定します。 すべてのクラスタ メンバーが 0（デフォルト）に設定された場合、均等に配分されます。いずれかのメンバーが 0 以外に設定されている時、他のメンバーの重み付けの値との関係に応じて比例的に分配されます。0 の値のままのメンバーはトラフィックを受け取りません。 *WCCP の負荷配分、68 ページ*を参照してください。

オプション	説明
Reverse Service Group ID（リバース サービス グループ ID）	IP スプーフィングが有効化されている場合にのみ使用します。 IP スプーフィングが有効化されている時、プロキシはそれぞれの有効化されている WCCP フォーワード サービス グループに対して、リバース サービス グループを公告します。**リバース サービス グループは、プロキシへのオリジン サーバー応答のリターン パスに適用されなければなりません。**
	Router Information（ルーター情報）
Security（セキュリティ）（オプション）	ルーターと Content Gateway との相互認証を有効化または無効化します。 Content Gateway のセキュリティを有効化した場合、ルーターのセキュリティも有効化する必要があります。ルーターのマニュアルを参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Security: Password（セキュリティ：パスワード）	認証に使用されるパスワードを指定します。パスワードは、ルーターに設定されたパスワードと同じ必要があり、最大 8 文字まで入力できます。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Multicast（マルチキャスト）（オプション）	WCCP マルチキャスト モードを有効化または無効化します。 **重要：**GRE パケットの Forward/Return メソッドでは使用できません。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Multicast: IP Address（IP アドレス）	マルチキャスト IP アドレスを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
WCCP Routers（WCCP ルーター）：Router IP Address（ルーター IP アドレス）	最大 10 個の WCCP v 2-対応ルーターの IP アドレスを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

オプション	説明
WCCP Routers: Local GRE Tunnel Endpoint IP Address（ローカル GRE トンネル エンドポイント IP アドレス）	GRE が [Packet Return Method]] として選択された場合、デバイスが ASA ファイアウォースである場合を**除いて**、[Local GRE Tunnel Endpoint IP Addresses] を指定する必要があります。 関連する [Router IP Addresses] に対応する Content Gateway トンネル エンドポイントがあります。 [Local GRE Tunnel Endpoint IP Address] は下記の条件を満たす必要があります。 • IP v 4 でなければなりません • テーブル内の各ルータについて一意でなければなりません • 他のデバイスに割り当てられいないアドレスにしなければなりません • ルーティング可能な IP アドレスでなければなりません • プロキシと同じサブネット上である必要があります。そうでない場合は、そのサブネットへのルートを定義する必要があります。 • クライアント側プロキシ IP アドレスとして使用してはいけません • サービス グループに指定した物理インターフェースにバインドされます（V シリーズ アプライアンス上で、eth0 = P1、eth1 = P2）
WCCP Routers: GRE Tunnel Next Hop Router IP Address（GRE トンネル ネクスト ホップ ルータ IP アドレス）	[GRE Packet Return Method] が設定され、Content Gateway が WCCP ルーターにルートを返さなかった場合、[GRE Tunnel Next Hop Router IP Address] を指定します。ping を使用してルーターへの接続をテストできます。

DNS Proxy（DNS プロキシ）

Help | Content Gateway | バージョン 7.8.x

注意

DNS Proxy 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで DNS Proxy を有効化した場合だけ、[Configure] ペインに表示されます。

[Configure] > [Networking] > [DNS Proxy]

DNS Proxy Port（DNS プロキシ ポート）	Content Gateway が DNS トラフィックに使用するポートを指定します。デフォルト ポートは 5353 です。

DNS リゾルバ

Help | Content Gateway | バージョン 7.8.x

[Configure] > [Networking] > [DNS Resolver] > [Resolver]

Local Domain Expansion（ローカル ドメイン拡張）	ローカルドメインを拡張することで、不適切なホスト名を解決しようと試みるローカル ドメイン拡張を有効化または無効化します。たとえば、クライアントが不適切なホスト名 `hostx` を要求した時、WCG ローカル ドメインが **y.com** である場合、Content Gateway は ホスト名を **hostx.y.com** に拡張します。
DNS Preference（DNS 優先設定）	Content Gateway IP v 6 サポートが有効化されており、Web サーバーが IP v 4 と IP v 6 の両方をサポートする場合は、IP バージョン優先設定を指定します。 プロキシが IPv4 を選ぶようにするには、IP v 4 を選択します。 プロキシが IPv6 を選ぶようにするには、IP v 6 を選択します。
DNS Preference Exceptions（DNS 優先設定の例外）	特定のオリジン サーバーについて IPv4 / IPv6 優先設定ルールをリストします。
Refresh（リフレッシュ）	最新のルールを表示するためにテーブルを更新します。設定ファイル エディタで、ルールを追加または編集した後、このボタンをクリックします。
Edit File（ファイルを編集）	設定ファイル エディタを開きます。
	dns_prefer_exception.config File Editor（dns_prefer_exception.config ファイル エディタ）
rule display box（ルール表示ボックス）	**dns_prefer_exception.config** ファイル ルールの順序指定済みリストを表示します。 編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	ルール表示ボックスに新しいルールを追加します。このボタンをクリックする前に、表示されているフィールドに情報を入力します。

Set（設定）	選択したルールをエントリ フィールド内の値によって更新します。
Name（名前）	ルールの管理の際に役立つ一意な名前を指定します。
Destination Host（宛先ホスト）	宛先ホストを指定します。
Preferred Format（優先するフォーマット）	優先する IP バージョンとして IP v 4 または IP v 6 を指定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

[Configure] > [Networking] > [DNS Resolver] > [Host Database]

これらの設定は Content Gateway によって実行されたすべての DNS 名前解決（DNS プロキシを含む）に適用します。

DNS Lookup Timeout（DNS ルックアップ タイムアウト）	プロキシが DNS サーバーからのルックアップ応答を待つ最大時間を秒単位で指定します。 最初の DNS 要求に対する応答がない場合に、プロキシが 2 回目の DNS 要求を行う前に待機する時間を秒単位で指定します。値は、[proxy.config.hostdb.lookup_timeout] に保存されます。デフォルト値は、120 秒です。 **重要：**この設定は使用されません。代わりに records.config エントリ [proxy.config.dns.lookup_timeout] が使用されます。デフォルト値は、20 秒です。**proxy.config.dns.lookup_timeout** はプロキシが要求を送信する前に DNS 応答を待つ時間を指定します。

Foreground Timeout（フォアグラウンド タイムアウト）	DNS エントリをホスト データベース内に保持する時間を指定します。この時間を過ぎるとその DNS エントリは古くなったとみなされます。この設定は、[proxy.config.hostdb.ttl_mode] がゼロでない場合のみ使用されます（デフォルト値は 0 です。このとき、DNS サーバーによって設定されている time-to-live (ttl)（保持時間）値を使用します）。*HostDB*、528 ページを参照してください。 たとえば、このタイムアウトが 24 時間で、データベース内に 24 時間以上存在するエントリをクライアントが要求した場合、プロキシはエントリを処理する前にリフレッシュします。 デフォルトは 86400 秒（144 分）です。 **警告：**フォアグラウンド タイムアウトが小さすぎると、応答時間が遅くなります。設定が高すぎると、誤った情報を蓄積する危険性があります。
Failed DNS Timeout（DNS 失敗タイムアウト）	ホスト名が DNS ルックアップ失敗キャッシュに保存される時間を秒単位で指定します（デフォルト = 60）。タイムアウト時間が経過すると、ホスト名はキャッシュから削除され、そのホスト名への次の要求は DNS サーバーへ送信されます。 以下の場合に DNS ルックアップ失敗が起こったとみなされます。 • DNS 応答がない • DNS 応答エラー コード（NXDOMAIN を含む）がある • DNS 応答コードの解析中にエラーが検出された（不適切な形式の応答がある）。 ゼロ (0) は無効な値です。

[Configure] > [Networking] > [DNS Resolver] > [Split DNS]

Split DNS（分割 DNS）	[Split DNS] オプションを有効化または無効化します。有効化すると、セキュリティ要件に応じて、Content Gateway が複数の DNS サーバーを使用できます。たとえば、プロキシが 1 つの DNS サーバーのセットを使って社内ネットワーク上のホスト名を解決し、ファイアウォールの外側の DNS サーバーがインターネット上のホストを解決するように設定することができます。分割 DNS の使用方法使用については、*Split DNS オプションの使用*、215 ページを参照してください。
Default Domain（デフォルト ドメイン）	DNS 要求を分割するために使用するデフォルト ドメインを指定します。ホスト名がドメインを含まない場合、Content Gateway は、使用する DNS サーバーを選択する前に、ホスト名にデフォルト ドメインを付加します。

DNS Servers Specification（DNS サーバー指定）	特定の条件のもとで、プロキシがホストを解決するために使用する DNS サーバーを制御する *splitdns.config* ファイルのルールを表示します。
Refresh（リフレッシュ）	**splitdns.config** ファイルの最新のルールを表示するために、テーブルを更新します。設定ファイル エディタで、ルールを追加または編集した後、このボタンをクリックします。
Edit File（ファイルを編集）	**splitdns.config** ファイルを編集し , ルールを追加するために、設定ファイル エディタを開きます。 設定ファイル エディタ ページについては後述します。
	splitdns.config Configuration File Editor（splitdns.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	*splitdns.config* ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。このボタンをクリックする前に、表示されるフィールドに情報を入力します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。このボタンをクリックする前に、ルールを選択しプロパティを変更します。
Primary Destination Type（一次宛先タイプ）	DNS サーバーが、宛先ドメイン（**dest_domain**）、宛先ホスト（**dest_host**）、または 正規表現（**url_regex**）のいずれかに基づいて選択されるかを指定します。
Primary Destination Value（一次宛先値）	一次宛先の値を指定します。NOT 論理演算子を指定するには、値の最初に記号 [!] を置きます。
DNS Server IP（DNS サーバー IP）	一次宛先指定子に使用する DNS サーバーを指定します。コロン（:）を使用してポートを指定できます。指定しない場合、53 が使用されます。スペースまたはセミコロン（;）で区切ることで、複数の DSN サーバーを指定できます。
Default Domain Name（デフォルト ドメイン名）（オプション）	ホストの解決に使用するデフォルト ドメイン名を指定します。1 つのエントリのみ入力できます。デフォルト ドメインを提供しない場合、システムは **/etc/resolv.conf** からその値を決定します。
Domain Search List（ドメイン検索リスト）（オプション）	ドメイン検索の順序を指定します。スペースまたはセミコロン（;）で区切ることで、複数のドメインを指定できます。検索リストを提供しない場合、システムは **/etc/resolv.conf** からその値を決定します。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

ICAP

Help | Content Gateway | バージョン 7.8.x

> **注意**
> ICAP 構成オプションは、**[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** タブの **[Features]** テーブルで **[ICAP]** を有効化した場合だけ、[Configure] ペインに表示されます。

ICAP は、Websense Data Security、および ICAP 対応のその他のデータ セキュリティ サービスに、代替インターフェースを提供します。プライマリおよびバックアップ URI を指定でき、フェールオーバーおよびロード バランシングを設定できます。*ICAP クライアントの構成*、154 ページおよび *ICAP フェールオーバーとロード バランシング*、156 ページのサブセクションを参照してください。

[Configure] > [Networking] > [ICAP]

ICAP Service URI（ICAP サービス URI）	ICAP サービスの Uniform Resource Identifier を指定します。形式は下記の通りです。
	`icap: //hostname: port/path`
	例：
	`icap: //ICAP_machine: 1344/REQMOD`
	デフォルトの ICAP ポートは 1344 です。デフォルトのポートを使用している場合、URI にポートを指定する必要はありません。
	オプションの第 2 URI サービスは、最初のサービスのすぐ後に、カンマと第 2 サービスをスペースなして付加することで指定できます。

Analyze HTTPS Content（HTTPS コンテンツを分析）	復号化したトラフィックを分析のために、Data Security に送信するか、または直接宛先に送信するかを指定します。
Analyze FTP Uploads（FTP のアップロードを分析）	FTP アップロード要求を分析のために、Websense Data Security に送信するかどうかを指定します。FTP プロキシ機能を有効化する必要があります。*FTP*、367 ページを参照してください。

Action for Communication Errors（通信エラーの場合の処置）	Content Gateway が Websense Data Security との通信中にエラーを受信した場合に、トラフィックを許可するか、ブロック ページを送信するかを指定します。
Action for Large files（大きなファイルの場合の処置）	Data Security で指定されたサイズ制限より大きなファイルが送られた場合に、トラフィックを許可するか、ブロック ページを送信するかを指定します。Data Security のデフォルトのサイズ制限は 12 MB です。

仮想 IP

Help | Content Gateway | バージョン 7.8.x

注意

Virtual IP 構成オプションは、**[Configure] > [My Proxy] > [Basic] > [General]** タブの [Features] テーブルで [Virtual IP（仮想 IP）] を有効化した場合だけ、[Configure] ペインに表示されます。

[Configure] > [Networking] > [Virtual IP]

Virtual IP Addresses（仮想 IP アドレス）	Content Gateway によって管理される仮想 IP アドレスのテーブルを表示します。
Refresh（リフレッシュ）	最新の仮想 IP アドレスを表示するために、テーブルを更新します。設定ファイル エディタで、仮想 IP アドレスを追加または編集した後、このボタンをクリックします。
Edit File（ファイルを編集）	仮想 IP アドレスのリストを編集、および追加するために、設定ファイル エディタを開きます。
	vaddrs.config Configuration File Editor（vaddrs.config 設定ファイル エディタ）
rule display box（ルール表示ボックス）	仮想 IP アドレスをリストします。編集する仮想 IP アドレスを選択します。ボックスの左側のボタンで、選択した仮想 IP アドレスを削除、または上下に移動できます。
Add（追加）	設定ファイル エディタ ページ上部のルール表示ボックスに、新しい仮想 IP アドレスを追加します。
Set（設定）	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Virtual IP Address（仮想 IP アドレス）	Content Gateway によって管理される仮想 IP アドレスを指定します。

Ethernet Interface（イーサネット インターフェース）	仮想 IP アドレスに割り当てられるネットワーク インターフェースを指定します。
Sub-Interface（サブインターフェース）	サブインターフェース ID を指定します。これは、インターフェースがアドレスとして使用する 1 から 255 までの番号です。
Apply（適用）	設定の変更を適用します。
Close（閉じる）	設定ファイル エディタ を終了します。 **[Close]** をクリックする前に、**[Apply]** をクリックします。そうでないと、設定変更は失われます。

URL のヘルス チェック

Help | Content Gateway | バージョン 7.8.x

Content Gateway は、HTTP 応答に含まれているプロキシ ヘルスおよびパフォーマンス情報を返す 3 つの URL を含んでいます。これらの URL は、各プロキシノードのリアルタイムの状態情報を取得し調整することによって、負荷バランサーがパフォーマンスを最適化するのを支援するように設計されています。

URL の ヘルスチェックのためのデフォルト ポートは 8083 です。この値を records.config で変更するには、**proxy.config.admin.autoconf_port** に希望する値を割り当てます。

[Configure] > [Networking] > [Health Check URLs]

Force Health Checks to Report Proxy Down（プロキシ ダウンのレポート時にヘルスチェックを強制）	

Enable/Disable（有効化 / 無効化）	このオプションを有効化した場合、すべての URL のヘルス チェックがこのプロキシ レポート WSDOWN に送信されます。
	URL 応答は下記のようになります。
	`HTTP/1.0 503 Service Unavailable`
	`Server: Content Gateway Manager 7.7.0`
	`Date: Thu, 26 Jul 2012 20: 26: 14 GMT`
	`Cache-Control: no-store`
	`Pragma: no-cache`
	`Content-type: text/plain`
	`Content-length: 6`
	
	`WSDOWN`

Health Check URLs（URL のヘルス チェック）	URL 要求が下記の理由で失敗した場合、ロード バランサーはサービス停止と見なします。 • TCP 接続なし — プロキシ ダウン • 応答が遅すぎる — プロキシがデッドロック状態か、または応答していない • 無効な応答
http: //[Content Manager IP address]: 8083/health.basic	Content Gateway との接続をチェックし、WSUP または WSDOWN によって応答します。
http: //[Content Manager IP address]: 8083/health.app.filtering	Content Gateway 要求に対する Filtering Service 応答のヘルスチェックを行い、WSUP または WSDOWN を報告します。

http: //[Content Manager IP address]: 8083/health.load	health.basic URL が WSDOWN を報告する場合、この URL も WSDOWN を報告します。
	そうでない場合は、health.load は下記の使用状況を返します。
	• CPU 使用状況（オペレーティング システムの負荷平均）
	• 接続使用状況（オープン接続の数）
	• 帯域幅使用状況
	これらの値が計算される方法およびそれらが下記に示すようにカスタム化される方法。
	デフォルトの応答は下記のようになります。
	`HTTP/1.0 200 OK`
	`Server: Content Gateway Manager 7.7.0`
	`Date: Thu, 26 Jul 2012 20: 26: 14 GMT`
	`Cache-Control: no-store`
	`Pragma: no-cache`
	`Content-type: text/plain`
	`Content-length: xx`
	
	`Load=2253`
	`Conns=5150`
	`Mbps=6.42`

フォーマット ファイル **/opt/WCG/config/health.load.template** は、応答フォーマットをカスタム化できます。

フォーマットの指定子は下記のとおりです。

%L = Load (integer)

%C = Connections (integer)

%B = Bandwidth in Mbps (double)

%% = %

デフォルトの **health.load.template** ファイルは下記のとおりです。

Load=%L

Conns=%C

Mbps=%B

ここで **health.load.template** は、xml-like フォーマットによって下記のように応答に変更されます。

<load>

<item name="Load" value="%L" />

<item name="Conns" value="%C" />

<item name="Mbps" value="%B" />

</load>

下記の方法で値が計算されます。

Load（負荷）値、%L は、LINUX システム負荷平均から得られます。コアの数が異なるコンピュータ間の比較のために、この値をシステム上のコアの数で割ります。

計算は下記のとおりです。

```
// load avg values are 0.00 precision
double avgs[3];
// get load averages for 1, 5, and 15 minutes
getloadavg(avgs, 3);
// 5 minute_load_average * 10000 / number_of_cores
Load = avgs[1] * 10000 / get_nprocs();
```

Connection（接続）値、%C は、proxy.process.http.current_server_connections と proxy.process.http.current_client_connections の合計です。

Bandwidth（帯域幅）、%B は、proxy.node.client_throughput_out の値です。

注意

HTTP 接続および帯域幅情報を Content Gateway マネージャの **[Monitor] > [Protocols] > [HTTP]** ページを順に選択して表示できます。

SSL

Help | Content Gateway | バージョン 7.8.x

SSL 設定オプションは、次のカテゴリに分けられます。

- 証明書（*証明書の管理*、175 ページを参照）
- 復号化 / 暗号化（*インバウンド トラフィックの場合の SSL 構成の設定*、178 ページ および *アウトバウンド トラフィックの場合の SSL 構成の設定*、180 ページを参照）
- 検証（*証明書の検証*、182 ページを参照）
- インシデント（*HTTPS Web サイトのアクセスの管理*、188 ページを参照）
- クライアント証明書（*クライアント証明書*、194 ページを参照）
- カスタム化（*SSL 接続エラー メッセージのカスタム化*、196 ページを参照）
- 内部ルート CA（*内部ルート CA*、166 ページを参照）

D イベント ログ記録のフォーマット

Help | Content Gateway | バージョン 7.8.x

カスタム ログ記録フィールド

関連項目：

- *ログ記録フォーマット相互参照*、437 ページ

%<field symbol>	説明
{*HTTP header field name*}cqh	クライアント要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Accept-Language}cqh> はクライアント要求ヘッダー内の **Accept-Language:** フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。
{*HTTP header field name*}cqhua	クライアント要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{User-Agent}cqhua> はクライアント要求ヘッダー内の **User-Agent:** フィールドをログ記録します。
{*HTTP header field name*}pqh	プロキシ要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Authorization}pqh> はプロキシ要求ヘッダー内の **Authorization:** フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。

%<field symbol>	説明
{*HTTP header field name*}psh	プロキシ応答 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{{Retry-After}psh> はプロキシ応答ヘッダー内の **Retry-After:** フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。
{*HTTP header field name*}ssh	サーバー応答 HTT P ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Age}ssh> はサーバー応答ヘッダー内の **Age:** フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。
caun	認証されたクライアントのユーザー名。クライアント ユーザー名の RFC931/ident ルックアップの結果。
cfsc	クライアント終了ステータス コード。プロキシへのクライアント要求が成功（FIN）したか、中断（INTR）したかを示します。
chi	クライアント ホスト IP。クライアントのホスト コンピュータの IP アドレス。
cqbl	クライアント要求転送の長さ。Content Gateway に対するクライアントの要求本文の長さ（バイト数）。
cqhl	クライアント要求ヘッダーの長さ。Content Gateway に対するクライアント要求ヘッダーの長さ。
cqhm	Content Gateway に対するクライアント要求の HTTP メソッド：GET、POST 等（cqtx のサブセット）。
cqhv	クライアントの要求の HTTP バージョン。
cqtd	クライアント要求のタイムスタンプ。*yyyy-mm-dd* の形式のクライアントの要求の日付。ここで、*yyyy* は 4-桁の年、*mm* は 2 桁の月、*dd* は 2 桁日です。
cqtn	クライアント要求のタイムスタンプ。クライアントの要求の日付と時刻（Netscape タイムスタンプ形式）。
cqtq	クライアントの要求のミリ秒精度のタイムスタンプ。
cqts	Squid フォーマットのクライアント要求タイムスタンプ。1970 年 1 月 1 日以降の秒単位で示されるクライアント要求の時刻。

%<field symbol>	説明
cqtt	クライアント要求のタイムスタンプ。*hh:mm:ss* 形式のクライアントの要求の時刻。ここで、*hh* は 24 時間形式の 2 桁の時刻、*mm* は 2 桁の分、*ss* は 2-桁の秒です。例：16:01:19
cqtx	ヘッダーを除いた完全な HTTP クライアント要求テキスト。例：`GET http://www.company.com HTTP/1.0`
cqu	クライアント要求 URI。クライアントから Content Gateway への要求の URI（cqtx のサブセット）。
cquc	クライアント要求の標準 URL。cqu との違いは、ブランク（および、ログ分析ツールで解析できないその他の特殊文字）が、エスケープ シーケンスによって置き換えられていることです。エスケープ シーケンスは、パーセント記号とそれに後続する 16 進表記の ASCII コード番号です。
cqup	クライアント要求の URL パス。URL の引数部分（ホストの後のすべて）を指定します。たとえば、URL が **http://www.company.com/images/x.gif** の場合、このフィールドは **/images/x.gif** と表示します。
cqus	クライアント要求の URL スキーム（HTTP、FTP など）。
crc	キャッシュ戻り値。要求に対するキャッシュの応答を示します（HIT、MISS 等）。
pfsc	プロキシ終了ステータス コード。Content Gateway のオリジンサーバーへの要求が、正常に完了した (FIN) か、中断された (INTR) かどうかを示します。
phn	照合ログ ファイルにログ エントリを生成した Content Gateway サーバーのホストネーム。
phr	プロキシ階層ルート。Content Gateway がオブジェクトの取得のために使用したルート。
pqbl	プロキシ要求転送の長さ。オリジン サーバーに対する Content Gateway 要求本文の長さ。
pqhl	プロキシ要求ヘッダーの長さ。オリジン サーバーに対する Content Gateway 要求ヘッダーの長さ。
pqsi	プロキシ要求サーバーの IP アドレス（0 はキャッシュ ヒット、親プロキシへの要求は 親 IP アドレス）。
pqsn	プロキシ要求サーバー名、要求を実現したサーバーの名前。
pscl	プロキシ応答転送の長さ。クライアントに対する Content Gateway 応答の長さ（バイト数）。

%<field symbol>	説明
psct	プロキシ応答のコンテンツ タイプ。サーバー応答ヘッダー内のドキュメント（例：img/gif）のコンテンツ タイプ。
pshl	プロキシ応答ヘッダーの長さ。クライアントに対する Content Gateway 応答ヘッダーの長さ。
psql	Squid フォーマットのプロキシ応答転送の長さ（ヘッダーとコンテンツの長さを含む）。
pssc	プロキシ応答ステータス コード（Content Gateway からクライアントへの HTTP 応答ステータス コード）。
shi	要求内のホストの DNS 名ルックアップで解決された IP アドレス。複数の IP アドレスをもつホストでは、このフィールドは特定の DNS 名ルックアップで解決された IP アドレスを記録します。これは、キャッシュ ドキュメントのためにミスリードされることがあります。 たとえば、サーバー S の最初の要求はキャッシュ ミスで IP1 から取得し、サーバー S の 2 回目の要求が IP2 と解決され、キャッシュから取得した場合、2 回目の要求のログ エントリは IP2 と表示されます。
shn	オリジン サーバーのホスト名。
sscl	サーバー応答転送の長さ。Content Gateway に対するオリジン サーバーから応答の長さ（バイト数）。
sshl	サーバー応答ヘッダーの長さ。Content Gateway に対するオリジン サーバーの応答ヘッダーの長さ（バイト数）。
sshv	サーバー応答の HTTP バージョン（1.0、1.1 等）。
sssc	サーバー応答ステータス コード。オリジン サーバーから Content Gateway への HTTP 応答ステータス コード。
ttms	Content Gateway がクライアントの要求の処理で費やした時間。クライアントが Content Gateway との接続を確立した時点から Content Gateway がその応答の最後のバイトをクライアントに送り返した時点までのミリ秒。

%<field symbol>	説明
ttmsf	Content Gateway がクライアントの要求の処理で費やした時間（秒の分数）。ミリ秒精度の時間 を示しますが、整数形式（*ttms*）の出力の代わりに、秒の分数を表す浮動小数点形式で表示します。たとえば、時間が 1500 ミリ秒の場合、このフィールドは 1.5 と表示されますが、**ttms** フィールドでは 1500 と表示され、**tts** フィールドでは 1 と表示されます。
tts	Content Gateway がクライアントの要求の処理で費やした時間、クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までの秒数。
wc	スキャンされるデータの URL の事前定義カテゴリまたはカスタム カテゴリ。例：[News and Media]
wct	Web ページのコンテンツ タイプ。例、[text/html、charset=UTF-8]。
wsds	CATEGORY_BLOCKED、PERMIT_ALL、FILTERED_AND_PASSED 等のスキャン フィルタの種類の文字列。
wsr	スキャン推奨ビット（ [true] または [false] ）。URL データベースで、さらに分析すべきデータを識別し、推奨します。使用されているポリシーに依存して、データは更に分析される場合もあり、分析されない場合もあります。
wstms	ダウンロードしたファイルまたはページのスキャンに費やしたスキャン時間（単位ミリ秒）。
wui	クライアント要求のデータをスキャンするポリシーを選択するために使用する認証されたユーザーの ID。

ログ記録フォーマット相互参照

Help | Content Gateway | バージョン 7.8.x

以下のセクションでは、Content Gateway のログ記録フィールドと、Squid および Netscape フォーマットの標準ログ記録フィールドとのやり取りを示しています。

Squid ログ記録フォーマット

Squid	Content Gateway フィールドの記号
time	cqts
elapsed	ttms
client	chi
action/code	crc/pssc
size	psql
method	cqhm
url	cquc
ident	caun
hierarchy/from	phr/pqsn
content	psct

たとえば、最初の 3 つの Squid フィールドを基にして、`short_sq` という名前のカスタム フォーマットを作成する場合、**logs.config** ファイルの下記の行を入力します。

```
format:enabled:1:short_sq:%<cqts> %<ttms>
%<chi>:short_sq:ASCII:none
```

カスタム ログ ファイルの定義の詳細については、*カスタム フォーマット、277 ページ*を参照してください。

Netscape Common ログ記録フォーマット

Netscape Common	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	cqtn
“req”	“cqtx”
s1	pssc
c1	pscl

Netscape Extended ログ記録のフォーマット

Netscape Extended	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtx”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts

Netscape Extended-2 ログ記録のフォーマット

Netscape Extended-2	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtx”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl

Netscape Extended-2	Content Gateway フィールドの記号
h3	pqhl
h4	sshl
xt	tts
route	phr
pfs	cfsc
ss	pfsc
crc	crc

E 設定ファイル

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway には、下記の設定ファイルを含まれ、プロキシをカスタマイズするために編集することができます。

URL 正規表現の指定 (url_regex)

Help | Content Gateway | バージョン 7.8.x

照会を実行する場合の正規表現を使用する設定ファイル内の `url_regex` タイプのエントリ。

下記の表は、有効な `url_regex` を作成する方法を示す例を提供しています。

値	説明
x	文字 x に一致。
.	すべての文字に一致。
^	行の先頭を指定。
$	行の最後を指定。
[xyz]	*文字クラス*。この場合、パターンは x、y、または z のいずれかに一致します。
[abj-oZ]	範囲の *文字クラス*。このパターンは a、b、j から o までのいずれかの文字、または Z に一致します。
[^A-Z]	*否定された文字クラス*。このパターンは クラスの中の文字以外のすべての文字に一致します。
r*	r の 0 回以上の繰り返しに一致します。ここで、r は すべての正規表現です。
r+	r の 1 回以上の繰り返しに一致します。ここで、r は すべての正規表現です。
r?	r の 0 回または 1 回の繰り返しに一致します。ここで、r は すべての正規表現です。
r{2.5}	r の 2 回から 5 回までの繰り返しに一致します。ここで、r は すべての正規表現です。
r{2,}	r の 2 回以上の繰り返しに一致します。ここで、r は すべての正規表現です。
r{4}	r の 4 回丁度の繰り返しに一致します。ここで、r は すべての正規表現です。
"[xyz]\"images"	リテラルの文字列 [xyz]"images"
\X	X が a、b、f、n、r、t、または v の場合、\x の ANSI-C インタープリテーション。そうでない場合は、リテラルの文字 X。これは、* 等のエスケープ演算子に使用されます。
\0	NULL 文字。
\123	8 進数の値 123 の文字。
\x2a	16 進数の値 2a の文字。

値	説明
(r)	r に一致します。ここで、r は すべての正規表現です。優先順位をオーバーライドするために、括弧を使用できます。
rs	正規表現 r の後に正規表現 s が続きます。
r|s	r または s のいずれかに一致します。
#<n>#	到達した時に正規表現マッチングを停止させる *エンドノード*を挿入。値 n が返されます。

例

mydomain.com 内のすべてのホストに一致させるには、`dest_domain=mydomain.com` を指定します。同様に、すべての要求に一致されるには、`dest_domain=.` を指定します。

auth_domains.config

Help | Content Gateway | バージョン 7.8.x

auth_domains.config ファイルは、*ルール ベースの認証*、239 ページで使用するために識別されているドメインのリストを保存します。

ドメインは、Content Gateway マネージャで **[Configure] > [Security] > [Access Control] > [Domains]** タブを順に選択し、インターフェースを使用して特定する（このフィールドに追加する）必要があります。この設定ファイルを編集してはいけません。

フォーマット

auth_domains.config の各行は、一連のタグとそれに続く値で構成されています。例：

type=<auth_method> name=<unique_name> use_alias=<0 or 1> <additional tags>

一連のタグは、選択した認証方法によって異なります。

下記の表は、すべてのタグをリストしています。

タグ	使用できる値
type	認証方法を指定します。IWA、NTLM、LDAP
name	ドメインの一意な名前を指定します。これは実際のドメイン名ではなく、プロキシおよびルールベースの認証に固有の名前です。

タグ	使用できる値
use_alias	認証が成功した場合にフィルタリング サービスに送信するユーザ名を指定します。 • 0 = 実際に認証されたユーザ名を送信（デフォルト）。 • 1 = 空白のユーザ名を送信 • 2 = auth_name_string で指定された文字列を送信
alias	use_alias=2 の場合にのみ有効。このルールを使用して認証に成功したすべてのユーザーのユーザー名として送信される静的文字列を指定します。

下記の表は、IWA 認証で使用される追加のタグをリストしています。

IWA タグ	使用できる値
winauth_realm	ルールで使用する結合 Windows ドメインを指定します。Content Gateway は、このドメイン内で結合されアクティブにされる必要があります。

下記の表は、NTLM ドメインで使用される追加のタグをリストしています。

NTLM タグ	使用できる値
dc_list	プライマリ ドメイン コントローラの IP アドレスとポート番号を指定（ポートが指定されていない場合、Content Gateway は ポート 139 を使用）、続けてカンマ区切り形式のリストで、ロード バランシングとフェールオーバーに使用するとセカンダリ ドメイン コントローラを指定。
dc_load_balance （オプション）	ロード バランシングを使用するかどうかを指定します。 • 0 = 無効化 • 1 = 有効化 **ご注意：**複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。

下記の表は、LDAP 認証で使用される追加のタグをリストしています。

LDAP タグ	使用できる値
server_name	LDAP サーバーの完全修飾ドメイン名を指定します。
server_port（オプション）	LDAP サーバーのポートを指定します。デフォルトは 389 です。 デフォルトの Global Catalog サーバー ポートを使用するには、ポート 3268 を指定します。 Secure LDAP が有効化されている場合、ポート 636 または 3269（セキュア LDAP ポート）を設定します。
base_dn（オプション）	LDAP ベース識別名を指定します。
uid_filter（オプション）	LDAP タブの設定と異なる場合に、サービスのタイプを指定します。Active Directory の場合は **sAMAccountName** と入力し、他のサービスの場合は **uid** を指定します。
bind_dn（オプション）	バインド識別名を指定します。これは LDAP ディレクトリ サービスのユーザーの完全識別名でなければなりません。例： CN=John Smith,CN=USERS,DC=MYCOMPANY, DC=COM
bind_pwd（オプション）	バインド識別名のパスワードを指定。
sec_bind	Content Gateway が LDA P サーバーとセキュア通信を行うかどうかを指定します。 • 0 = 無効化 • 1 = 有効化 有効化されている場合、LDAP ポードは 636 または 3269（セキュア LDAP ポート）に設定されます。

auth_rules.config

Help | Content Gateway | バージョン 7.8.x

auth_rules.config ファイルは、指定された IP アドレスと IP アドレス範囲、および（または）指定された着信ポート上のトラフィック（明示的プロキシのみ）、および（または）マッチする要求ヘッダー User-Agent 値を別々のドメイン コントローラで認証するよう指示するルールを保存します。順序指定されたリストで、1 つ以上のドメイン コントローラを指定できます。この機能は、*ルール ベースの認証、239 ページ* と呼ばれます。

ルールベースのルールは、Content Gateway マネジャの **[Configure]> [Security] > [Access Control] > [Authentication Rules]** タブを順に選択して定義します。この設定ファイルを編集してはいけません。

- ルールベースの認証は、統合 Windows (IWA)、レガシー NTLM、および LDAP 認証のみをサポートしています。
- 各認証ルールは、発信元 IP アドレス、インバウンド ポート（明示的プロキシのみ）、および（または）User-Agent regex を指定できます。
- 各認証ルールは、順序指定されたリストで 1 つ以上のドメインを指定できます。ドメインは、**[Configure] > [Security] > [Access Control] > [Authentication Rules]** タブを順に選択し、特定します。そのプロセスは、認証方法の指定（IWA、レガシー NTLM、LDAP） を含みます。
- ルールが一致した場合、認証が順序指定されたリスト内の 1 つ以上のドメインに対して実行されます。最初に成功した認証がドメイン リストのトラバースを終了し、認証中のドメインが後の使用のためにキャッシュされます。
- 認証ルールはリストの上から順にチェックされ、最初に一致するルールのみが適用されます。一致するルールがない場合、ユーザー認証は行われません。

> **注意**
>
> ネットワーク内のすべてのユーザーが、信頼関係を共有しているドメイン コントローラによって認証できる場合、ルール ベースの認証は必要ありません。
>
> しかし、ルールベースの認証は、IP アドレス、インバウンド プロキシ ポート（明示的プロキシ）、および（または User-Agent）に基づき特別な認証の処理を実行することが必要な環境では役立つことがります。

フォーマット

auth.config の各行は、一連のタグとそれに続く値で構成されている認証ルールを含んでいます。認証ルールは次の形式になります。

rule_name=<name> src_ip=<IP addresses> user_agent=<regex> <additional tags>

下記の表は、すべてのタグをリストしています。

タグ	使用できる値
rule_name	短い、一意な名前。
enabled	ルールがアクティブかどうかを指定します。 • 0 = 無効化 • 1 = 有効化

タグ	使用できる値
src_ip	IP アドレスおよび IP アドレス範囲のカンマ区切りリストを指定します。スペースなしです。このフィールドが空白である場合は、すべての IP アドレスが一致します。
user_agent（オプション）	user-agent 文字列に適用される正規表現を指定します。
proxy_port（オプション）	ポート番号を指定します。明示的プロキシの場合のみ有効です。要求を正しいポートへ送信するためにクライアント アプリケーションを設定しておかなければなりません。
domain_list	ドメインの順序指定されたカンマ区切りのリストで、Content Gateway はこのリストを使ってマッチするユーザーの認証を試みます。

bypass.config

Help | Content Gateway | バージョン 7.8.x

bypass.config ファイルには、Content Gateway が透過プロキシ モードで使用する*静的*バイパス ルールが含まれます。静的バイパス ルールは、Content Gateway に特定の着信クライアント要求をバイパスし、オリジン サーバーによって処理されるよう指示します。

また、**bypass.config** ファイルは *動的*バイパス拒否ルールに対応しています。*動的バイパス拒否ルール、449 ページ*を参照してください。

3 つのタイプの静的バイパス ルールを設定できます。

- *送信元バイパス*ルールは、特定の送信元 IP アドレスまたは IP アドレスの範囲を迂回するようプロキシを設定します。たとえば、キャッシュを使用させたくないクライアントを迂回させることができます。
- *宛先バイパス*ルールは、特定の宛先 IP アドレスまたは IP アドレスの範囲を迂回するようプロキシを設定します。たとえば、クライアントの実際の IP アドレスを基に IP 認証を使用するオリジン サーバーを迂回できます。

重要

宛先バイパス ルールは、プロキシがサイト全体をキャッシュすることを防止します。迂回したサイトが人気のあるサイトである場合、ヒット率への影響が顕著に表れます。

- *送信元/宛先*ペアバイパス ルールは、指定の送信元から指定の宛先へ発信する要求を迂回するようプロキシを設定します。たとえば、IP 認証が破られた、またはキャッシュ時に帯域外の HTTP トラフィックの問題があるクライアント / サーバー ペアを迂回することができます。送信元 / 宛先バイパス ルールは、宛先サーバーを、問題が発生したユーザーに対してのみブロックしますから、宛先バイパス ルールよりも適切です。

フォーマット

バイパス ルールは下記の形式になります。

```
bypass src ipaddress | dst ipaddress | src ipaddress AND dst
ipaddress
```

オプション	説明
src *ipaddress*	プロキシが迂回するべき着信要求内の送信元（クライアント）IP アドレスを指定。 *ipaddress* は 以下のいずれかになります： `123.45.67.8` 等の単一 IP アドレス • `1.1.1.0/24` 等の CIDR (Classless Inter-Domain Routing) 形式 • `1.1.1.1-2.2.2.2` 等のダッシュで区切られたアドレス範囲 • `1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123` 等のコンマで区切られた上記の組み合わせ。
dst *ipaddress*	プロキシが迂回するべき着信要求内の宛先（オリジン サーバー）IP アドレスを指定します。 *ipaddress* は 以下のいずれかになります： `123.45.67.8` 等の単一 IP アドレス • `1.1.1.0/24` 等の CIDR (Classless Inter-Domain Routing) 形式 • `1.1.1.1-2.2.2.2` 等のダッシュで区切られたアドレス範囲 • `1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123` 等のコンマで区切られた上記の組み合わせ。
src *ipaddress* AND dst *ipaddress*	プロキシが迂回するべき送信元 / 宛先 IP アドレスのペアを指定。 *ipaddress* には単一の IP アドレス、IP アドレスの範囲、またはその両方の組み合せ（カンマ区切り）を指定できます。

動的バイパス拒否ルール

静的バイパス ルールに加えて、**bypass.config** ファイルは*動的バイパス拒否*ルールに対応しています。

バイパス拒否ルールは、プロキシに特定の着信クライアント要求が迂回することを動的に禁止させます（バイパス拒否ルールは、プロキシが自分を迂回することを禁止できます）。動的バイパス拒否ルールは、送信元、宛先、送信元 / 宛先を指定でき、次の形式になります：

```
deny_dyn_bypass src ipaddress | dst ipaddress | src
ipaddress AND dst ipaddress
```

オプションの説明は、フォーマット、448 ページの表を参照してください。

注意

動的バイパス拒否ルールを動作させるには、Content Gateway マネージャで **[Dynamic Bypass]** オプションを有効化するか、**records.config** ファイルで、変数 *proxy.config.arm.bypass_dynamic_enabled* を 1 に設定する必要があります。

重要

静的バイパス ルールは 動的バイパス拒否ルールを上書きします。従って、静的バイパス ルールと動的バイパス拒否ルールが同じ IP アドレスを含む場合、動的バイパス拒否ルールは無視されます。

例

下記の例は、送信元、宛先、送信元 / 宛先の*バイパス*ルールを示しています：

```
bypass src 1.1.1.0/24, 25.25.25.25, 128.252.11.11-
128.252.11.255
bypass dst 24.24.24.0/24
bypass src 25.25.25.25 AND dst 24.24.24.0
```

下記の例は、送信元、宛先、送信元 / 宛先の*動的バイパス拒否*ルールを示しています：

```
deny_dyn_bypass src 128.252.11.11-128.252.11.255
deny_dyn_bypass dst 111.111.11.1
deny_dyn_bypass src 111.11.11.1 AND dst 111.11.1.1
```

cache.config

Help | Content Gateway | バージョン 7.8.x

cache.config ファイルは、プロキシが Web オブジェクトをキャッシュする方法を指定します。下記の設定を指定することで、キャッシング ルールを追加できます：

- 特定の IP アドレスのオブジェクトのキャッシュしない
- 特定のオブジェクトをキャッシュ内に留める時間
- キャッシュされたオブジェクトが最新であると見なされる時間
- サーバーからの no-cache 指示を無視するかどうか

重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

cache.config ファイルの各行には、キャッシュ ルールが含まれます。Content Gateway は下記のように 3 つのスペース区切りのタグを認識します。

```
primary_destination=value secondary_specifier=value
action=value
```

下記の表は、使用可能な一次宛先とその値をリストしています。

一次宛先	使用できる値
dest_domain	要求されたドメイン名。
dest_host	要求されたホスト名。
dest_ip	要求された IP アドレス。
url_regex	URL に含まれる正規表現。

cache.config ファイルでは二次指定子は任意です。下記の表は、使用可能な二次指定子とその値をリストしています。

注意

ルールの中で 1 つ以上の二次指定子を使用できます。ただし、1 つの二次指定子を繰り返すことはできません。

二次指定子	使用できる値
port	要求された URL のポート。
scheme	要求 URL のプロトコル。下記のどちらか 1 つ： • HTTP • FTP
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。
method	要求 UR L のメソッド。下記のいずれか 1 つ。 • get • put • trace
time	時間範囲（例、08:00-14:00）。
src_ip	クライアント IP アドレス。
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	値
アクション	下記の値の内の 1 つ。 • nnever-cache は、プロキシが指定したオブジェクトをキャッシュしないよう設定します。 • ignore-no-cache は、プロキシがすべての Cache-Control: no-cache ヘッダーを無視するように設定します。 • ignore-client-no-cache は、プロキシがクライアント要求の Cache-Control: no-cache ヘッダーを無視するように設定します。 • ignore-server-no-cache は、プロキシがオリジン サーバー応答の Cache-Control:no-cache ヘッダーを無視するように設定します。

アクション	値
pin-in-cache	オブジェクトがキャッシュ内に留まる時間。下記の時間形式で入力できます： • *d*：日付（例、2d） • *h*：時間（例、10h） • *m*：分（例、5m） • *s*：秒（例、20s） • 組み合わせ（例、1h15m20s）
revalidate	オブジェクトが、キャッシュ内で最新と見なされる時間。pin-in-cache と同じ時間形式を使用します。
ttl-in-cache	Cache-Control 応答ヘッダーに関係なく、キャッシュ内にオブジェクトを保持する時間。pin-in-cache および revalidate と同じ時間形式を使用します。

例

下記の例は、IP アドレス 112.12.12.12 から要求された FTP ドキュメントをキャッシュしないようにプロキシを設定します。

```
dest_ip=112.12.12.12 scheme=ftp action=never-cache
```

下記の例は、正規表現 politics とパス **prefix/viewpoint** を含む URL のドキュメントを 12 時間の間キャッシュ内に保持するように、プロキシを設定します。

```
url_regex=politics prefix=/viewpoint pin-in-cache=12h
```

下記の例は、ドメイン mydomain.com 内の gif および jpeg オブジェクトを 6 時間毎に再確認し、mydomain.com 内のその他のオブジェクトを 1 時間毎に再確認するように、プロキシを設定します。

```
dest_domain=mydomain.com suffix=gif revalidate=6h
dest_domain=mydomain.com suffix=jpeg revalidate=6h
dest_domain=mydomain.com revalidate=1h
```

注意
ルールはリストされた順に適用されます。

filter.config

Help | Content Gateway | バージョン 7.8.x

filter.config に保存されたフィルタリング ルールで下記のことができます。

- URL 要求を拒否または許可する
- クライアント要求のヘッダー情報を保持または削除する
- カスタム ヘッダを挿入する
- 指定したアプリケーション、または指定した Web サイトの要求が認証をバイパスすることを許可する
- 指定したアプリケーションがプロキシを通過することを禁止する

フィルタリング ルールは、Content Gateway マネージャの **[Configure] > [Security] > [Access Control] > [Filtering]** タブ上で定義されます。*フィルタリング ルールの作成*、207 ページを参照してください。

> **重要**
> このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

デフォルトでは 3 つのフィルタリング ルールが設定されます。最初のルールは、すべてのアクセス先に対してポート 25 上のトラフィックを拒否します。2 番目と 3 番目のルールは、ThreatScope の 2 つの アクセス先に対してユーザー認証をバイパスします。

フォーマット

filter.config の各行がフィルタリング ルールです。Content Gateway は、ファイルの上位から開始し、リストされた順にルールを適用します。条件に一致するルールがない場合、要求は処理されます。

Content Gateway は下記のように 3 つのスペース区切りのタグを認識します。

```
primary_destination=value secondary_specifier=value action=value
```

下記の表は、使用可能な一次宛先タイプをリストしています。

一次宛先タイプ	使用できる値
dest_domain	要求されたドメイン名。
dest_host	要求されたホスト名。
dest_ip	要求された IP アドレス。
url_regex	URL に含まれる正規表現。

二次指定子は任意です。下記の表は、使用可能な二次指定子とその用途をリストしています。

注意

ルールの中で 1 つ以上の二次指定子を使用できます。ただし、1 つの二次指定子を繰り返すことはできません。

二次指定子	使用できる値
time	時間範囲（例、08:00-14:00）。
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。
src_ip	単一のクライアント IP アドレス、またはクライアント IP アドレスの範囲。
port	要求された URL のポート。
method	要求 URL のメソッド。下記のいずれか 1 つ。 • get • post • put • trace
scheme	要求 URL のプロトコル。以下のいずれかを指定できます： • HTTP • HTTPS • FTP（FTP over HTTP の場合のみ）
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	使用できる値
action	下記のいずれか 1 つを指定します。 • **allow** - 特定の URL 要求が認証をバイパスすることを許可します。プロキシは要求されたコンテンツをキャッシュに入れ、提供します。 • **deny** - 特定の宛先からの HTTP または FTP オブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。 • **radius** - サポートされていません。
`keep_hdr`	保持するクライアント要求ヘッダー情報。下記のいずれかのオプションを指定できます： • `date` • `host` • `cookie` • `client_ip`
`strip_hdr`	削除するクライアント要求ヘッダー情報。**keep_hdr** と同じオプションを指定できます。
add_hdr	追加するカスタム ヘッダー値。カスタム ヘッダーとヘッダー値が指定されている必要があります。例： `add_hdr="header_name:header_value"`

例

下記の例は、IP アドレス 112.12.12.12 に対するすべての FTP ドキュメント要求を拒否するように、Content Gateway を設定します。

```
dest_ip=112.12.12.12 scheme=ftp action=deny
```

下記の例は、正規表現 `politics` とパス接頭辞 /viewpoint を含む URL 要求のクライアント IP アドレス ヘッダーを保持するように、Content Gateway を設定します：
/viewpoint:

```
url_regex=politics prefix=/viewpoint keep_hdr=client_ip
```

下記の例は、オリジン サーバー **www.server1.com** 宛てのクライアント要求のすべてのクッキーを削除するように、Content Gateway を設定します：

```
dest_host=www.server1.com strip_hdr=cookie
```

下記の例は、オリジン サーバー**www.server2.com** への **put** を非許可にするように、Content Gateway を設定します：

```
dest_host=www.server2.com method=put action=deny
```

Content Gateway は、ファイルにリストされた順にルールを適用します。たとえば、下記のサンプルの **filter.config** ファイルは、下記の動作をさせるように Content Gateway を設定します：

- server1.com へのアクセスをすべてのユーザーに許可（internal.com へのアクセス試行を除く）
- notthatsite.com へのアクセスをすべてのユーザーに拒否

```
dest_host=server1.com action=allow
dest_host=notthatsite.com action=deny
```

hosting.config

Help | Content Gateway | バージョン 7.8.x

hosting.config ファイルを使用して、キャッシュ パーティションを特定のオリジン サーバーとドメインに割り当てることで、キャッシュ スペースをより効率的に管理し、ディスクの使用を制限することができます。

オリジン サーバーとドメイン別のキャッシュのパーティショニングの手順については、*オリジン サーバーまたはドメインに基づくキャッシュのパーティション区分、119 ページ*を参照してください。

> **注意**
>
> 特定のオリジン サーバーとドメインにキャッシュ パーティションを割り当てる前に、**partition.config** ファイルで、サイズとプロトコルに基づいてキャッシュを分割する必要があります。キャッシュ パーティショニングの詳細については、*キャッシュのパーティション区分、118 ページ*を参照してください。**partition.config** ファイルの説明は、*partition.config、472 ページ*を参照してください。

hosting.config ファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリで **content_line -x** を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は 自動的にクラスタ内のすべてのノードに変更を適用します。

> **重要**
>
> パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

フォーマット

hosting.config ファイルの各行は、下記の形式のいずれかである必要があります：

```
hostname=hostname partition=partition_numbers
domain=domain_name partition=partition_numbers
```

ここで、

hostname は、コンテンツを特定のパーティションに保存させるオリジン サーバーの完全修飾ホスト名です（例、www.myhost.com）。

domain_name は、コンテンツを特定のパーティション保存させるドメイン名です（例、mydomain.com）。

partition_numbers は、リストされたオリジン サーバーまたはドメインのコンテンツを保存させるパーティションのカンマ区切り形式のリストです。パーティション番号は、**partition.config** ファイルにリストされた有効な番号でなければなりません（*partition.config*、472 ページを参照）。

> **注意**
> オリジン サーバーまたはドメインに 1 つ以上のパーティションを割り当てる場合、1 行にカンマ区切り形式のリストでパーティションを入力します。**hosting.config** ファイルに、同じオリジン サーバーまたはドメインの複数のエントリを含めることはできません。

汎用パーティション

hosting.config ファイルの設定時に、どのオリジン サーバーまたはドメインにも属さないコンテンツのために使用する汎用パーティションを割り当てる必要があります。特定のオリジン サーバーのためのすべてのパーティションが破損した場合、Content Gateway はオリジン サーバーのコンテンツを保存するために汎用パーティションを使用します。

汎用パーティションは次の形式にする必要があります。

```
hostname=* partition=partition_numbers
```

ここで、**partition_numbers** は汎用パーティションのカンマ区切り形式のリストです。

例

下記の例は、ドメイン **mydomain.com** のコンテンツを パーティション 1 に、ドメイン **www.myhost.com** のコンテンツをパーティション 2 に保存するようにプロキシを設定します。プロキシはすべてのオリジン サーバーのコンテンツを パーティション 3 と 4 に保存します。

```
domain=mydomain.com partition=1
hostname=www.myhost.com partition=2
hostname=* partition=3,4
```

ip_allow.config

Help | Content Gateway | バージョン 7.8.x

ip_allow.config ファイルは、プロキシに対するクライアント アクセスを制御します。Content Gateway を使用することを許可する IP アドレスの範囲を指定できます。

重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

ip_allow.config ファイルの各行は下記の形式である必要があります：

```
src_ip=ipaddress action=ip_allow | ip_deny
```

ここで、*ipaddress* は プロキシへのアクセスを許可するクライアントの IP アドレスまたは IP アドレス範囲です。

アクション `ip_allow` は、指定したクライアントがプロキシにアクセスすることを許可します。

アクション `ip_deny` は、指定したクライアントがプロキシにアクセスすることを拒否します。

デフォルトでは、**ip_allow.config** ファイルは 次の行を含み、すべてのクライアントにプロキシへアクセスすることを許可します。アクセス制限のルールを追加する前に、この行をコメントとして除くか、削除してください。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

例

下記の例は、すべてのクライアントにプロキシへアクセスすることを許可します。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

下記の例は、特定のサブネット上のすべてのクライアントにプロキシへアクセスすることを許可します。

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

下記の例は、特定のサブネット上のすべてのクライアントにプロキシへアクセスすることを拒否します。

```
src_ip=123.45.6.0-123.45.6.123 action=ip_deny
```

ipnat.conf

Help | Content Gateway | バージョン 7.8.x

ipnat.conf ファイルには、プロキシが透過的にトラフィックを処理するときに、着信パケットのアドレスを変更する方法を指定するリダイレクト ルールが含まれます。Content Gateway はインストール時にリダイレクト ルールを作成します。これらのルールを変更できます。

重要
このファイルを変更したらコンピュータを再起動する必要があります。

フォーマット

ipnat.conf ファイルの各行は 下記の形式である必要があります：

```
rdr interface 0.0.0.0/0 port dest -> ipaddress port proxy
tcp|udp
```

ここで、

interface は、トラフィックが Content Gateway コンピュータにアクセスするために使用するイーサネット インタフェースです（例 Linux 上の場合 `eth0`）。

dest は トラフィックの宛先ポートです（例、HTTP トラフィックの場合 `80`）。

ipaddress は Content Gateway サーバーの IP アドレスです。

proxy は Content Gateway のプロキシ ポート（HTTP トラフィックの場合、通常 `8080`）です。

例

下記の例は、すべての着信 HTTP トラフィックを、Content Gateway の プロキシ ポート（8080）上の Content Gateway IP アドレス（111.111.11.1）へアドレス変更するように、ARM を設定します：

```
rdr hme0 0.0.0.0/0 port 80 -> 111.111.11.1 port 8080 tcp
```

log_hosts.config

Help | Content Gateway | バージョン 7.8.x

異なるオリジン サーバーの HTTP/FTP トランザクションを個別のログ ファイルに記録するには、**llog_hosts.config** ファイルに各オリジン サーバーのホスト名をリストしなければなりません。さらに、HTTP ホスト分割オプションを有効にする必要があります（*HTTP ホスト ログ分割、287 ページ*を参照）。

> **注意**
> クラスタ内の各 Content Gateway ノードで、同じ **log_hosts.config** ファイルを使用することを推奨します。

> **重要**
> このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

log_hosts.config ファイルの各行は下記の形式である必要があります。

```
hostname
```

ここで、*hostname* はオリジン サーバーのホスト名です。

> **注意**
>
> **log_hosts.config** ファイルでキーワードを指定し、そのキーワードをホスト名に含むオリジン サーバーのすべてのトランザクションを別個のログ ファイルに記録することができます。下記の例を参照してください。

例

下記の例は、オリジン サーバー webserver1、webserver2、および webserver3 のすべての HTTP/FTP トランザクションを含む別個のログ ファイルを作成するように、Content Gateway を設定します：

```
webserver1
webserver2
webserver3
```

下記の例は、名前に sports を含むオリジン サーバー（例、`sports.yahoo.com` および www.foxsports.com）からのすべての HTTP および FTP ランザクションを、**squid-sport.log**（Squid フォーマットが有効な場合）という名前のログ ファイルに保存します：

```
sports
```

logs_xml.config

Help | Content Gateway | バージョン 7.8.x

logs_xml.config ファイルは、カスタム ログ ファイル フォーマット、フィルタ、および 処理オプションを定義します。このファイルのフォーマットは、XML（Extensible Markup Language）モデルです。

フォーマット

logs_xml.config は、下記の定義を含みます。

- `LogFormat` は、各プロトコル イベント アクセスから収集されるフィールドを指定します。*LogFormat*、462 ページを参照してください。
- `LogFilter` は、エントリ内の値を基にログ記録される特定のエントリ を含める または 除外するために使用するフィルタを指定します。*LogFilter*、463 ページを参照してください。
- `LogObject` は、特定のフォーマット、ローカル ファイル名、フィルタ、および 照合サーバーを含むオブジェクトを指定します。*LogObject*、464 ページを参照してください。

> **注意**
>
> **logs_xml.config** ファイルは 余分な空白、空白の行、および すべてのコメントを無視します。

LogFormat

下記の表は `LogFormat` の定義をリストしています。

フィールド	使用できる入力値
`<Name = "valid_format_name"/>`	必須。使用できるフォーマットの名前は、squid、common、extended、extended2（事前定義されているフォーマット名）を除くすべての名前です。このタグのデフォルト設定はありません。
`<Format = "valid_format_specification"/>`	必須。使用できるフォーマットの定義は、ASCII 形式出力としてフォーマット化された各ログ エントリを表す `printf` スタイルの文字列です。有効なフィールド名のプレースホルダとして、`'%<field>'` を使用します。詳細については、*カスタム ログ記録フィールド、433 ページ*を参照してください。指定フィールドは 2 つの型を使用できます： 単純な型：例 ,`%<cqu>` HTTP ヘッダーまたは Content Gateway 統計等のコンテナ内のフィールド。この型のフィールドは下記の構文を使用します。`'%<{field}container>'`。
`<Interval = "aggregate_interval_secs"/>`	フォーマットに集計演算子が含まれる場合にこのタグを使用します。 `"aggregate_interval_secs"` は、個々の集計値が作成される秒単位の間隔を表しています。使用できる集計演算子のセットを下記に示します。 • `COUNT` • `SUM` • `AVG` • `FIRST` • `LAST`

LogFilter

下記の表は LogFilter の定義をリストしています。

フィールド	使用できる入力値
<Name = "valid_filter_name"/>	必須。すべてのフィルタは 固有の名前をもつ必要があります。
<Condition = "valid_log_field valid_operator valid_comparison_value"/>	必須。このフィールドには次の要素が含まれます： valid_log_field - 指定された値に対して比較されるフィールド。詳細については、*ログ記録フォーマット相互参照*、437 ページを参照してください。 valid_operator_field - 下記のいずれかになります：MATCH、CASE_INSENSITIVE_MATCH、CONTAIN、CASE_INSENSITIVE_CONTAIN。MATCH は、フィールドと値が同じ場合に true になります（大文字と小文字を区別）。CASE_INSENSITIVE_MATCH は、大文字と小文字を区別しない以外は MATCH と同じです。CONTAIN は、フィールドが値を含む場合に true になります（値はフィールドの部分文字列になります）。CASE_INSENSITIVE_CONTAIN は、CONTAIN の大文字と小文字を区別しないバージョンです。 valid_comparison_value - フィールドタイプに一致する整数または文字列。整数値の場合、演算子はすべて等価演算子で、フィールドが指定された値と等しくなければならないことを意味します。 ご注意：否定比較演算子は存在しません。否定条件を指定したい場合、**Action** フィールドを使用してレコードを拒否します。
<Action = "valid_action_field"/>	必須。ACCEPT または REJECT。これは、フィルタの条件を満足するレコードを受け入れるか、拒否するかを Content Gateway に指示します。

LogObject

下記の表は LogObject の定義をリストしています。

フィールド	使用できる入力値
<Format = "valid_format_name"/>	必須。使用できるフォーマットの名前は、事前定義された次のログ記録フォーマットです：事前定義されたカスタム ログ フォーマットと squid、common、extended、extended2。このタグのデフォルト設定はありません。
<Filename = "file_name"/>	必須。ローカル システムまたはリモート照合サーバー上で書き込まれるログ ファイルのファイル名。このタグを指定し損なった場合、ローカル ログ ファイルは作成されません。すべてのファイル名は、デフォルトログ記録ディレクトリからの相対位置になります。 名前に特定の拡張子（例、squid）が含まれない場合、ASCII 形式のログには 拡張子 .log が、バイナリ形式のログには blog が自動的に付加されます。（下記の <Mode = "valid_logging_mode"/> を参照 .）拡張子を付加したくない場合は、ファイル名の最後をドット（.）で終わります：例、squid.

フィールド	使用できる入力値
<Mode = "valid_logging_mode"/>	使用できるログ記録モードは、ascii、binary、および ascii_pipe です。デフォルトは ascii です。 人が読みとれる形式（プレーン ASCII）でイベント ログ ファイルを作成するには、ascii を使用します。 バイナリ形式のイベント ログ ファイルを作成するには、binary を使用します。バイナリ形式のログ ファイルは、システム オーバヘッドが小さく、ディスク スペースが少なくてすみます（ログ記録される情報に依存します）。バイナリ形式のログ ファイルを ASCII 形式に変換するためには、logcat ユーティリティ を使用する必要があります。 UNIX 名前付きパイプ（ メモリ中のバッファ）にログ エントリを書き込むには、ascii_pipe を使用します。他のプロセスが標準 I/O 機能によりデータを読み込めるようになります。Content Gateway によるハードディスク書き込みが不要になり、ディスク スペースと帯域幅が他のタスクのために解放されます。また、UNIX 名前付きパイプはディスク スペースを使用しないので、ログ記録スペースが使い尽くされても、パイプへの書き込みは中断しません。 ご注意：照合サーバーを使用している場合、ログは照合サーバー上のパイプに書き込まれます。トランザクションが処理される前でも、ローカル パイプは作成されます。従って、Content Gateway 起動直後に パイプを参照できます。ただし、照合サーバー上のパイプは Content Gateway が起動した時に作成 *されます*。
<Filters = "list_of_valid_filter_names"/>	前に定義されたログ フィルタ名のカンマ区切り形式のリスト。1 つ以上のフィルタが指定されている場合、レコードがログ記録されるためには、すべてのフィルタがレコードを受け入れる必要があります。
<Protocols = "list_of_valid_protocols"/>	ログ記録されるべきオブジェクトのプロトコルのカンマ区切り形式のリスト。使用できるプロトコル名は HTTP です。
<ServerHosts = "list_of_valid_servers"/>	ホスト名のカンマ区切り形式のリスト。このタグは、ファイルに含まれる名前付のサーバーのエントリのみを示します。

フィールド	使用できる入力値
<CollationHosts = "list_of_valid_hostnames"/>	（このオブジェクトの）すべてのログ エントリが転送される照合サーバーのカンマ区切り形式のリスト。照合サーバーは、名前または IP アドレスで指定できます。名前の後のコロンで照合ポートを指定します（例、host:port）。
<Header = "header"/>	ログ ファイルに含めるヘッダー テキスト。ヘッダ テキストは、ログ ファイルの冒頭で最初のレコードの直前に表示されます。
<RollingEnabled = "truth value"/>	*LogObject* のログ ファイル取り込みを有効化または無効化します。この設定は、Content Gateway Manager の設定 **[Log Rolling: Enabled/Disabled]** または records.config ファイルの *proxy.config.log2.rolling_enabled* を上書きします。 取り込みを有効化するには、“truth value” を 1 または true に設定します。この特定の *LogObject* の取り込みを無効化するには、0 または false に設定します。
<RollingIntervalSec = "seconds"/>	*LogObject* のログ ファイル取り込みの秒単位の間隔を指定します。この設定は、Content Gateway マネージャの設定 **[Log Rolling: Interval]** または records.config ファイルの *proxy.config.log2.rolling_interval_sec* を上書きします。このオプションで、異なる *LogObjects* に異なる取り込み間隔を指定できます。
<RollingOffsetHr = "hour"/>	取り込みを [整列] させる時間（0 から 23）を指定します。その時間より前に取り込みが開始されることがありますが、取り込みファイルはその時間に作成されます。取り込み間隔が 1 時間より大きい場合にのみ、この設定の影響が重要になります。この設定は、Content Gateway マネージャの設定 **[Log Rolling: Offset Hour]** または records.config ファイルの *proxy.config.log2.rolling_offset_hr* を上書きします。

例

下記は、3 つのカンマ フィールドを使用して情報収集する LogFormat の定義の例です：

```
<LogFormat>
<Name = "minimal"/>
<Format = "%<chi> :%<cqu> :%<pssc>"/>
</LogFormat>
```

下記は、集計演算子を使用した LogFormat の定義の例です。

```
<LogFormat>
<Name = "summary"/>
<Format = "%<LAST(cqts)> :%<COUNT(*)> :%<SUM(psql)>"/>
<Interval = "10"/>
</LogFormat>
```

下記は、REFRESH_HIT エントリのみによりログ記録する LogFilter の定義の例です：

```
<LogFilter>
<Name = "only_refresh_hits"/>
<Action = "ACCEPT"/>
<Condition = "%<pssc> MATCH REFRESH_HIT"/>
</LogFilter>
```

注意

フィルタ条件フィールドを指定する時に、%<> を省略することができます。これは、下記のフィルタが上記同じであることを意味します。

```
<LogFilter>
   <Name = "only_refresh_hits"/>
   <Action = "ACCEPT"/>
   <Condition = "pssc MATCH REFRESH_HIT"/>
</LogFilter>
```

下記は、前に定義した最小限の形式でローカル ログ ファイルを作成する LogObject の定義の例です：これは ASCII ログ ファイル（デフォルト）なので、ログ ファイル名は **minimal.log** になります。

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
</LogObject>
```

下記は、ドメイン company.com のホスト、または 指定のサーバー server.somewhere.com で処理される HTTP 要求のみを含める LogObject の定義の例です：ログ エントリは、照合ホスト logs.company.com のポート 4000 と、照合ホスト 209.131.52.129 のポート 5000 に送信されます。

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
<ServerHosts = "company.com,server.somewhere.com"/>
<Protocols = "http"/>
<CollationHosts =
"logs.company.com:4000,209.131.52.129:5000"/>
</LogObject>
```

WELF (WebTrends Enhanced Log Format)

Content Gateway は、WELF (WebTrends Enhanced Log Format) をサポートしており、WebTrend レポーティング ツールを使用して、Content Gateway のログ ファイルを分析することができます。WELF 互換の定義済みの <LogFormat> は、logs.config ファイルの最後に指定されます（下記参照）。WELF 形式のログ ファイルを作成するためには、この定義済みフォーマットを使用する <LogObject> を作成します。

```
<LogFormat>
<Name = "welf"/>
<Format = "id=firewall time=\"%<cqtd> %<cqtt>\" fw=%<phn>
pri=6 proto=%<cqus> duration=%<ttmsf> sent=%<psql>
rcvd=%<cqhl> src=%<chi> dst=%<shi> dstname=%<shn>
user=%<caun> op=%<cqhm> arg=\"%<cqup>\" result=%<pssc>
ref=\"%<{Referer}cqh>\" agent=\"%<{user-agent}cqh>\"
cache=%<crc>"/>
</LogFormat>
```

mgmt_allow.config

Help | Content Gateway | バージョン 7.8.x

mgmt_allow.config ファイルは、Content Gateway マネージャへのアクセスを許可または拒否するリモート ホストの IP アドレスを指定します。

重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

mgmt_allow.config ファイルの各行は、下記の形式である必要があります：

```
src_ip=ipaddress action=ip_allow|ip_deny
```

ここで、*ipaddress* は、Content Gateway マネージャへのアクセスを許可される IP アドレスまたは IP アドレスの範囲です。

`action` は、Content Gateway マネージャへのアクセスを許可するには `ip_allow` を、アクセスを拒否するには `ip_deny` を指定します。

デフォルトでは、**mgmt_allow.config** は下記の行を含み。それによってすべてのリモート ホストが Content Gateway マネージャにアクセスすることを許可します。アクセス制限のルールを追加する前に、この行をコメントとして除くか、削除してください。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

例

下記の例は、Content Gateway マネージャへのアクセスを一人のユーザーのみに許可するように、Content Gateway を設定します。

```
src_ip=123.12.3.123 action=ip_allow
```

下記の例は、特定の IP アドレス範囲に Content Gateway マネージャへのアクセスを許可するように、Content Gateway を設定します。

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

下記の例は、IP アドレス 123.45.67.8 が Content Gateway マネージャへアクセスするのを拒否するように、Content Gateway を設定します。

```
src_ip=123.45.67.8 action=ip_deny
```

parent.config

Help | Content Gateway | バージョン 7.8.x

parent.config ファイルは、HTTP キャッシュ階層の中で使用される HTTP 親プロキシを指定します。下記の設定を実行するために、このファイルを使用します。

- 複数の親および親フェールオーバーの親キャッシュ階層を設定
- 親プロキシを迂回する URL 要求を設定

ルールはリストの上から順にチェックされ、最初に条件に一致するルールが適用されます。通常、バイパス ルールは 親プロキシ指定ルールの上位に位置します。

HTTP 親キャッシュ オプションが有効化されている場合にのみ、Content Gateway は **parent.config** ファイルを使用します。*HTTP 親キャッシュを使用する Content Gateway の構成*、112 ページを参照してください。

> **重要**
> このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

parent.config ファイルの各行は 親キャッシュのルールを含む必要があります。Content Gateway は下記のように 3 つのスペース区切りのタグを認識します。

```
primary_destination=value secondary_specifier=value
action=value
```

下記の表は、使用可能な一次宛先とその値をリストしています。

一次宛先	使用できる値
`dest_domain`	要求されたドメイン名。
`dest_host`	要求されたホスト名。
`dest_ip`	要求された IP アドレスまたはのダッシュ（-）で区切られた IP アドレスの範囲。
`url_regex`	URL に含まれる正規表現。

parent.config ファイルでは二次指定子は任意です。下記の表は、使用可能な二次指定子とその値をリストしています。

二次指定子	使用できる値
time	08:00-14:00 等の親キャッシュ要求を処理する時間範囲。
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。
src_ip	クライアント IP アドレス。
port	要求された URL のポート。
scheme	要求 URL のプロトコル。下記のどちらか 1 つ： • HTTP • FTP
method	要求 UR L のメソッド。下記のいずれか 1 つ。 • get • post • put • trace
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	使用できる値
parent	親サーバーの順序指定されたリスト。リスト内の最後の親サーバーによって要求が処理されなかった場合、オリジン サーバーにルーティングされます。ホスト名または IP アドレスを指定できます。ポート番号を指定する必要があります。
round_robin	下記の値の内の 1 つ。 • true - Content Gateway はクライアント IP アドレスに基づいたラウンドロビン内の親キャッシュ リストを経由します。 • strict - Content Gateway コ ンピュータは厳格に順番どうりに要求を処理します。たとえば、コンピュータ proxy1 が最初の要求を処理し、proxy2 が 2 番目の要求を処理するなどです。 • false - ラウンド ロビン選択を発生させません。
go_direct	下記の値の内の 1 つ。 • true - 要求は親階層を迂回して、直接オリジン サーバーに向かいます。 • false - 要求は親階層を迂回しません。

例

下記のルールは、Content Gateway（子）と 2 つの親 p1.x.com および p2.x.com で構成される親キャッシュ階層を設定します。round_robin=true であるため、プロキシは、処理できない要求を親サーバー p1.x.com および p2.x.com にラウンド ロビン方式で転送します。

```
dest_domain=. method=get parent="p1.x.com:8080;
p2.y.com:8080" round_robin=true
```

下記のルールは、正規表現 politics とパス **/viewpoint** を含むすべての要求を、（親階層を迂回して）直接オリジン サーバーに送信するように、Content Gateway を設定します：

```
url_regex=politics prefix=/viewpoint go_direct=true
```

下記のルールは、標準的な宛先バイパス ルールです。

```
dest_domain=example.com go_direct=true
```

> **重要**
>
> **parent.config** ファイルの各行は、parent= または go_direct= ディレクティブの**いずれか**を含む必要があります。
>
> parent= **および** go_direct=true を含むバイパス ルールでは、指定された dest_domain は親に送信され、（通常意図されたアクションとは反対に）その他のすべてのドメインはバイパスされます。

partition.config

Help | Content Gateway | バージョン 7.8.x

partition.config ファイルを使用して、異なるサイスのキャッシュ パーティションを作成することで、キャッシュ スペースをより効果的に管理できます。*hosting.config* ファイルで、特定のオリジン サーバーおよびドメインからのデータをこれらのパーティションに保存するように設定することができます。これは、コンテンツか稀にしか変更されない頻繁に訪問するサイトのキャッシングに活用できます。

> **重要**
>
> パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

キャッシュ パーティション サイズを変更する前に、Content Gateway を停止しなければなりません。

フォーマット

作成する各パーティションのために、下記の形式で行を入力します。

```
partition=partition_number scheme=protocol_type
size=partition_size
```

ここで、

partition_number は 1 から 255 までの数字です（パーティションの最大数は 255 です）。

protocol_type は **http** です。

> **注意**
> 現時点では、HTTP のみがサポートされています。ストリーミング メディア コンテンツ **-mixt-** はサポートされていません。

partition_size は パーティションに割り当てられるキャッシュ容量です。値は、全キャッシュ容量に対するパーセンテージか、絶対値のいずれかを指定できます。絶対値は 128 MB の倍数である必要があります。ここで、128 MB は最小値です。パーセンテージを指定した場合、サイズは最も近い 128 MB の倍数に丸められます。各パーティションは、パラレル I/O を実行するために 複数のディスクに分割されます。たとえば、4 つ のディスクがある場合、1 GB のパーティションは、各ディスク上で 256 MB になります（各ディスクが十分な空き容量をもつ場合）。

> **注意**
> キャッシュにすべてのディスクを割り当てない場合、追加ディスク スペースは使用できません。既存のパーティションを削除 / クリアすることなしに、後で新しいパーティションを作成するために、追加スペースを使用できます。

例

下記の例は、キャッシュを均等にパーティション化します。

```
partition=1 scheme=http size=50%
partition=2 scheme=http size=50%
```

records.config

Help | Content Gateway | バージョン 7.8.x

rrecords.config ファイルは、Content Gateway で使用される設定変数のリストです。

ほとんどの値は、Content Gateway マネージャのコントロールを使用して設定されます。いくつかのオプションは、**records.config** ファイル内の変数を編集するだけで設定できます。

警告

確信がない場合、**records.config** の変数を変更しないでください。多くの変数は組になっており、それらは他の変数に影響します。個別に単一の変数を変更することは、Content Gateway に障害を発生させる原因になります。**可能な限り、Content Gateway の設定には Content Gateway マネージャを使用してください。**

重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。

クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

各変数は下記の形式になります。

```
CONFIG variable_name DATATYPE variable_value
```

ここで、*DATATYPE* は `INT`（整数）、`STRING`（文字列）、`FLOAT`（浮動小数点）。

例

下記の例で、変数 **proxy.config.proxy_name** は データタイプ **文字列**であり、その値が **contentserver1** です。つまり、Content Gateway プロキシの名前が **contentserver1** であることを意味します。

```
CONFIG proxy.config.proxy_name STRING contentserver1
```

下記の例で、変数 **proxy.config.winauth.enabled** は、[はい] または [いいえ] のフラグです。0（ゼロ）はこのオプションを無効化します。1 は オプションを有効化します。

```
CONFIG proxy.config.winauth.enabled INT 0
```

下記の例では、クラスタ スタートアップ タイムアウトを 10 秒に設定します。

```
CONFIG proxy.config.cluster.startup_timeout INT 10
```

設定変数

Help | Content Gateway | バージョン 7.8.x

下記の表は、**records.config** ファイル内にリストされる設定変数を説明しています。

システム変数

ローカル マネージャー

仮想 IP マネージャ

アラーム設定

ARM

負荷軽減設定 (ARM)

認証基本レルム

LDAP

RADIUS 認証

NTLM

統合 Windows 認証

透過的認証

HTTP エンジン

親プロキシ設定

キャッシュ コントロール

ヒューリスティック期限

ダイナミック コンテンツおよびコンテンツ ネゴシエーション

匿名 FTP パスワード

キャッシュされた FTP ドキュメントのライフタイム

システム変数

Help | Content Gateway | バージョン 7.8.x

設定変数 データ タイプ	データ タイプ	デフォルト値	説明
proxy.config.proxy_name	STRING		Content Gateway ノードの名前を指定します。
proxy.config.bin_path	STRING	bin	Content Gateway の **bin** ディレクトリの位置を指定します。 これは、インストーラによって Content Gateway のバイナリ ファイルが配置されるディレクトリです。
proxy.config.proxy_ binary	STRING	content_gateway	**content_gateway** プロセスを実行する実行ファイルの名前を指定します。

設定変数 データ タイプ	データ タイプ	デフォルト値	説明
proxy.config.proxy_ binary_opts	STRING	-M	**content_gateway** 起動時のコマンドライン オプションを指定します。
proxy.config.manager_ binary	STRING	content_manager	**content_manager** プロセスを実行する実行ファイルの名前を指定します。
proxy.config.cli_binary	STRING	content_line	**content_line** インターフェースを実行する実行ファイルの名前を指定します。
proxy.config.watch_ script	STRING	content_cop	**content_cop** プロセスを実行する実行ファイルの名前を指定します。
proxy.config.env_prep	STRING	example_prep.sh	**content_manager** プロセスが **content_gateway** プロセスを発行する前に、実行されるスクリプトを指定します。
proxy.config.config_dir	STRING	config	Content Gateway 設定ファイルが含まれるディレクトリ（上記の bin_path からの相対）を指定します。
proxy.config.temp_dir	STRING	/tmp	Content Gateway 一時ファイルに使用するディレクトリを指定します。
proxy.config.alarm_email	STRING	websense	Content Gateway が、アラーム メッセージを送信する電子メール アドレスを指定します。 インストール中に電子メール アドレスを指定できます。そうでない場合は、Content Gateway は、デフォルト値として Content Gateway ユーザー アカウント名を使用します。
proxy.config.syslog_ facility	STRING	LOG_DAEMON	システム ログ ファイルを記録するために使用する機能を指定します。 *ログ ファイルの使用*、271 ページを参照してください。

設定変数 データ タイプ	データ タイプ	デフォルト値	説明
proxy.config.cop.core_signal	INT	3	**content_cop** は、管理するプロセス - **content_manager** および **content_gateway** - に、それらを停止するために送信するシグナルを指定します。 **ご注意：この変数の値を変更しないでください。**
proxy.config.cop.sleep_time	INT	45	**content_manager** および **content_gateway** プロセスの状態をテストするために、**content_cop** によって実行されるハートビート テストの間隔を秒単位で指定します。 **ご注意：この変数の値を変更しないでください。**
proxy.config.cop.linux_min_swapfree_kb	INT	10240	この変数は使用させません。
proxy.config.cop.linux_min_memfree_kb	INT	10240	この変数は使用させません。
proxy.config.output.logfile	STRING	content_gateway.out	Content Gateway プロセスで作成される警告、ステータス、メッセージ、および エラー メッセージを保存するファイルの名前と場所を指定します。 パスが指定されない場合、Content Gateway は このファイルをログ記録ディレクトリに作成します。
proxy.config.output.logfile.log_dir_usage_percent	INT	35	**proxy.config.log2.max_space_mb_for_logs** によって割り当てられるスペースのパーセンテージを指定します。このパーセンテージは、**content_gateway.out** を**除いて** /opt/WCG/logs/ にログ記録するために使用できます。Content_gateway.out はログ ディレクトリ限界まで使用できます。

設定変数 データ タイプ	データ タイプ	デフォルト値	説明
proxy.config. snapshot_dir	STRING	snapshots	Content Gateway が 構成のスナップショットを保存するローカル システム上のディレクトリを指定します。絶対パスを指定しない場合、このディレクトリは Content Gateway **config** ディレクトリに入れられます。
proxy.config. attach_debugger_script	STRING	attach_debugger	この変数は、Websense テクニカル サポートからの指示があった場合にのみ使用する必要があります。 セットすると、**content_gateway** プロセス再起動時に、デバッグ スクリプト（in /opt/WCG/bin）を実行します。
proxy.config.healthcheck _force_offline	INT	0	有効化 (1) すると、プロキシ ダウンのレポート時に URL ヘルスチェックを強制します。 *URL のヘルス チェック*、429 ページを参照してください。

ローカル マネージャー

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.lm.sem_id	INT	11452	ローカル マネージャーのセマフォ ID を指定します。 **ご注意：この変数の値を変更しないでください。**
proxy.local.cluster.type	INT	3	クラスタ モードを指定します。 • 2 = 管理専用モード • 3 = クラスタ化しない

設定変数	データタイプ	デフォルト値	説明
proxy.config.cluster.rsport	INT	8087	信頼できるサービス ポートを指定します。信頼できるサービス ポートはクラスタ内のノード間で設定情報を送信するために使用します。クラスタ内のすべてのノードは同じ信頼できるサービス ポートを使用しなければなりません。
proxy.config.cluster.mcport	INT	8088	マルチキャスト ポートを指定します。マルチキャスト ポートは、ノードの識別のために使用します。クラスタ内のすべてのノードは同じマルチキャスト ポートを使用しなければなりません。
proxy.config.cluster.mc_group_addr	STRING	224.0.1.37	クラスタ通信のためのマルチキャスト アドレスを指定します。クラスタ内のすべてのノードは同じマルチキャスト アドレスを使用しなければなりません。
proxy.config.cluster.mc_ttl	INT	1	クラスタ通信のためのマルチキャスト Time-To-Live を指定します。
proxy.config.cluster.log_bogus_mc_msgs	INT	1	無効なマルチキャスト メッセージのログ記録を有効化 (1) または 無効化 (0) します。
proxy.config.admin.html_doc_root	STRING	ui	Content Gateway マネージャr のドキュメント ルートを指定します。
proxy.config.admin.web_interface_port	INT	8081	Content Gateway マネージャのポートを指定します。
proxy.config.admin.autoconf_port	INT	8083	自動構成ポートを指定します。
proxy.config.admin.overseer_port	INT	-1	統計および設定変数を取得 / 設定するポートを指定します。このポートはデフォルトでは無効化されます。
proxy.config.admin.admin_user	STRING	admin	Content Gateway マネージャへのアクセスを制御する管理者 ID を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.admin.admin_password	STRING		Content Gateway マネージャrへのアクセスを制御する管理者パスワードを指定します。パスワードを編集することはできません。しかし、パスワードをクリアするために NULL を指定することはできます。 *マスタ管理者パスワードを忘れた場合の Content Gateway manager へのアクセスの方法*、17 ページを参照してください。
proxy.config.admin.basic_auth	INT	1	Content Gateway マネージャへのアクセスを制御する基本ユーザー認証を有効化 (1) または無効化 (0) します。 ご注意：基本認証が有効でない場合、Content Gateway をモニターおよび設定するために、すべてのユーザーが Content Gateway マネージャにアクセスできます。
proxy.config.admin.use_ssl	INT	1	リモートホストと Content Gateway マネージャの間でセキュア通信を行うために、Content Gateway マネージャ SSL オプションを有効化します。
proxy.config.admin.ssl_cert_file	STRING	server.pem	リモートホストと Content Gateway マネージャの間でセキュア通信を行うために、Content Gateway システムにインストールされた SSL 証明書のファイル名を指定します。
proxy.config.admin.number_config_bak	INT	3	保持する取り込み設定ファイルのコピーの最大数を指定します。
proxy.config.admin.user_id	STRING	root	Content Gateway に指定される非特権ユーザー アカウントを指定します。
proxy.config.admin.ui_refresh_rate	INT	30	Content Gateway マネージャの [Monitor] ページの統計表示の更新頻度を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.admin.log_mgmt_access	INT	0	すべての Content Gateway マネージャトランザクションを **lm.log** ファイルにログ記録することを、有効化 (1) または無効化 (0) します。
proxy.config.admin.log_resolve_hostname	INT	1	有効化 (1) すると、Content Gateway マネージャに接続しているクライアントのホスト名が、**lm.log** ファイルに記録されます。 無効化 (0) すると、Content Gateway マネージャに接続しているクライアントの IP アドレスが、**lm.log** ファイルに記録されます。
proxy.config.admin.subscription	STRING	NULL	未使用。
proxy.config.admin.supported_cipher_list	STRING	AES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA	Content Gateway マネージャによってサポートされている暗号のカンマ j 区切り形式のリスト（空白を含まない）。 文字列の検証は行われません。
proxy.config.lm.display_reset_alarm	INT	0	有効化 (1) すると、Content Gateway がリセットされた時はいつでも、電子メールが管理者 **(poxy.config.alarm_email)** に送信されます。 デフォルトは 0 です。

プロセス マネージャー

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.process_ manager.mgmt_port	INT	8084	**content_manager** プロセスと **content_gateway** プロセスの間の内部通信に使用するポートを指定します。

仮想 IP マネージャ

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.vmap. enabled	INT	0	仮想 IP オプションを有効化 (1) または 無効化 (0) します。

アラーム設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.alarm.bin	STRING	example_alarm_ bin.sh	アラームが発生した時に特定の動作をさせるスクリプトの名前を指定します。デフォルト ファイルは、**bin** ディレクトリにある **example_alarm_bin.sh** という名前のサンプル スクリプトです。必要に応じてスクリプトを編集する必要があります。
proxy.config.alarm.abs_ path	STRING	NULL	**proxy.config.alarm.bin**（前のエントリ）で指定されたスクリプト ファイルの絶対パスを指定します。

ARM

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.enabled	INT	1	ARM を有効化するか、または無効化するかを指定します。 警告：ARM を無効化してはいけません。すべての環境で、適切なプロキシ機能をサポートするために ARM を実行しなければなりません。
proxy.config.arm.ignore_ifp	INT	1	NAT ルールが適用される場合に、Content Gateway が NAT ルールをトリガしたインタフェースではなく、パケットのクライアントへの返信時に利用可能なインタフェースを使用するように設定します。
proxy.config.arm.always_query_dest	INT	0	有効化 (1) すると、Content Gateway は 常に着信要求の元の宛先 IP アドレスを ARM に問い合わせます。これは、要求のホスト名 DNS ルックアップの代わりに行われます。 有効化した場合、ドメイン名の代わりに IP アドレスがログ記録されます。 無効化した場合、ドメイン名がログ記録されます。詳細は*DNS ルックアップの削減*、92 ページを参照してください。 Content Gateway が 明示的プロキシおよび透過的プロキシモードの*両方*で動作している場合、この変数を有効化しないことを推奨します。明示的プロキシモードでは、クライアントは、オリジン サーバーのホスト名の DNS ルックアップを実行しません。そのため、Content Gateway がそれを行う必要があります。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.use_hostname_for_wisp_and_reporting	INT	0	透過的プロキシ配備のために Always Query Destination が有効化されているとき、（IP アドレスの代わりに）ホスト名をキャプチャする機能を有効化 (1) または無効化 (0) します。前の項目を参照してください。 注意：この変数は config ファイルに手動で追加する必要があり、バージョン 7.8.2 以上で利用できます。
proxy.config.http.outgoing_ip_spoofing_enabled	INT	0	Content Gateway の IP アドレスの代わりにクライアントの IP アドレスを使用して、オリジン サーバーとの接続を確立することを、Content Gateway に許可する IP スプーフィング オプションを有効化 (1) または無効化 (0) します。 *IP スプーフィング、94 ページ*を参照してください。
proxy.config.arm.bypass_dynamic_enabled	INT	0	クライアントまたはサーバーに問題が発生した場合に、プロキシを迂回して直接オリジン サーバーに送信する適応型バイパスオプションを有効化 (1) または無効化 (0) します。 *動的バイパス ルール、89 ページ*を参照してください。
proxy.config.arm.bypass_use_and_rules_bad_client_request	INT	0	ポート 80 上で非 HTTP トラフィックの発生時の動的送信元 / 宛先バイパスを有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_bad_client_request** も有効化する必要があります。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.bypass_use_and_rules_400	INT	0	オリジン サーバーが 400 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_400** も有効化する必要があります。
proxy.config.arm.bypass_use_and_rules_401	INT	0	オリジン サーバーが 401 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_401** も有効化する必要があります。
proxy.config.arm.bypass_use_and_rules_403	INT	0	オリジン サーバーが 403 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_403** も有効化する必要があります。
proxy.config.arm.bypass_use_and_rules_405	INT	0	オリジン サーバーが 405 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_405** も有効化する必要があります。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.bypass_use_and_rules_406	INT	0	オリジン サーバーが 406 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_406** も有効化する必要があります。
proxy.config.arm.bypass_use_and_rules_408	INT	0	オリジン サーバーが 408 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_408** も有効化する必要があります。
proxy.config.arm.bypass_use_and_rules_500	INT	0	オリジン サーバーが 500 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意：このオプションが動作するためには、変数 **proxy.config.arm.bypass_on_500** も有効化する必要があります。
proxy.config.arm.bypass_on_bad_client_request	INT	0	ポート 80 上で非 HTTP トラフィック発生時に、動的宛先バイパスを有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_400	INT	0	オリジン サーバーが 400 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_401	INT	0	オリジン サーバーが 401 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.bypass_on_403	INT	0	オリジン サーバーが 403 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_405	INT	0	オリジン サーバーが 405 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_406	INT	0	オリジン サーバーが 406 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_408	INT	0	オリジン サーバーが 408 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_500	INT	0	オリジン サーバーが 500 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。

負荷軽減設定 (ARM)

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.loadshedding.max_connections	INT	1000000	許可されるクライアント接続の最大数を指定します。この数を超えるとプロキシは要求を直接にオリジン サーバーに転送しはじめます。
proxy.config.http.client.connection_control.enabled	INT	1	1 つのコンピュータからの接続数を制限する機能を有効化 (1) または無効化 (0) します。
proxy.config.http.client.concurrent_connection_control.close.enabled	INT	1	同時接続制限に達した場合に接続を閉じる機能を有効化 (1) または無効化 (0) します。
proxy.config.http.client.concurrent_connection_control.alert.enabled	INT	0	同時接続制限違反の警告を有効化 (1) または無効化 (0) します。
proxy.config.http.client.concurrent_connection_control.max_connections	INT	1000	1 つのクライアント IP アドレスに許可される同時接続数の最大値を指定します。
proxy.config.http.client.connection_rate_control.close.enabled	INT	0	接続率制限に達した場合に接続を閉じる機能を有効化 (1) または無効化 (0) します。
proxy.config.http.client.connection_rate_control.alert.enabled	INT	1	接続率制限超過時の警告を有効化 (1) または無効化 (0) します。
proxy.config.http.client.connection_rate_control.second	INT	100	1 つのクライアント IP アドレスに許可される 1 秒当たりの最大接続数を指定します。
proxy.config.http.client.connection_control.exceptions	STRING	NULL	接続制限を適用しない IP アドレスをカンマ区切りリストで指定します。

認証基本レルム

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.proxy.authenticate.basic.realm	STRING	NULL	認証レルムの名前を指定します。デフォルト値 **NULL** を指定すると、**Content Gateway** が使用されます。
proxy.config.auth_type	INT	0	クライアント認証のタイプを指定します。 • 0 = なし • 1 = LDAP • 2 = RADIUS • 3 = レガシー NTLM • 4 = 統合 Windows 認証 (Integrated Window Authentication) • 5 = ルール ベースの認証
proxy.config.multiauth.enabled	INT	0	LDAP プロキシ認証を有効化 (1) または無効化 (0) します。Content Gateway に auth_rules.config ファイルを使用するように伝えます。

LDAP

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.ldap.auth.enabled	INT	0	LDAP プロキシ認証を有効化 (1) または 無効化 (0) します。*LDAP 認証*、233 ページを参照してください。
proxy.config.ldap.cache.size	INT	5000	LDAP キャッシュに許可されるエントリの最大数を指定します。 この値を変更する時、それに比例して **proxy.config.ldap.cache.size** の値も更新しなければなりません。たとえば、キャッシュ サイズを 2 倍にした場合は、キャッシュ ストレージ サイズも 2 倍にします。
proxy.config.ldap.cache.storage_size	INT	24582912	LDAP キャッシュのサイズをバイト単位で指定します。これは、直接 キャッシュ内のエントリ数に関連します。 この値を変更する時、それに比例して **proxy.config.ldap.cache.size** の値も更新しなければなりません。たとえば、キャッシュ ストレージ サイズを 2 倍にした場合は、キャッシュサイズも 2 倍にします。 **proxy.config.ldap.cache.size** を修正せずにこの変数を修正した場合、LDAP サブシステムの機能停止の原因になることがあります。
proxy.config.ldap.auth.ttl_value	INT	3000	エントリがキャッシュ内で有効である時間を分単位で指定します。
proxy.config.ldap.auth.purge_cache_on_auth_fail	INT	1	有効化 (1) すると、認証が失敗した時に LDAP キャッシュ内のクライアントの認証エントリを削除します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ldap.proc.ldap.server.name	STRING	NULL	LDAP サーバー名を指定します。
proxy.config.ldap.proc.ldap.server.port	INT	389	LDAP サーバーのポートを指定します。
proxy.config.ldap.proc.ldap.base.dn	STRING	NULL	LDAP ベース識別名 (DN) を指定します。この値は LDAP 管理者から取得します。
proxy.config.ldap.proc.ldap.uid_filter	STRING	**sAMAccountName**	LDAP ログイン名 /ID を指定します。これを完全 DN データベースを検索するためのフィルタとして使用します。 eDirectory またはその他のディレクトリ サービスでは、このフィールドに **uid** を入力します。
proxy.config.ldap.secure.bind.enabled	INT	0	有効化 (1) にすると、プロキシが LDAP サーバーとの通信にセキュアな LDAP (LDAPS) を使用するように設定します。通常セキュア通信はポート 636 または 3269 上で実行されます。
proxy.config.ldap.proc.ldap.server.bind_dn	STRING	NULL	LDAP ベースのディレクトリ サービスのユーザーの完全識別名（完全修飾名）を指定します。例： `CN=John Smith,CN=USERS, DC=MYCOMPANY,DC=COM` このフィールドには最大 128 文字まで入力できます。 このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
proxy.config.ldap.proc.ldap.server.bind_pwd	STRING	NULL	**proxy.config.ldap.proc.ldap.server.bind_dn** 変数によって識別されるユーザーのパスワードを指定します。

RADIUS 認証

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.radius.auth.enabled	INT	0	RADIUS プロキシ認証を有効化 (1) または無効化 (0) します。
proxy.config.radius.proc.radius.primary_server.name	STRING	NULL	プライマリ RADIUS 認証サーバーのホスト名または IP アドレスを入力します。
proxy.config.radius.proc.radius.primary_server.auth_port	INT	1812	Content Gateway が RADIUS サーバーとの通信で使用する RADIUS サーバー ポートを指定します。
proxy.config.radius.proc.radius.primary_server.shared_key	STRING	NULL	プライマリ RADIUS 認証サーバーで暗号化に使用するキーを指定します。
proxy.config.radius.proc.radius.secondary_server.name	STRING	NULL	セカンダリ RADIUS 認証サーバーのホスト名または IP アドレスを指定します。
proxy.config.radius.proc.radius.secondary_server.auth_port	INT	1812	プロキシがセカンダリ RADIUS 認証サーバーとの通信に使用するポートを指定します。
proxy.config.radius.proc.radius.secondary_server.shared_key	STRING	NULL	セカンダリ RADIUS 認証サーバーで暗号化に使用するキーを指定します。
proxy.config.radius.auth.min_timeout	INT	10	RADIUS サーバーとの接続がアイドル状態を維持する時間を指定します。この時間を過ぎると Content Gateway は接続を閉じます。
proxy.config.radius.auth.max_retries	INT	10	Content Gateway が RADIUS サーバーへの接続を試みる最大回数を指定します。
proxy.config.radius.cache.size	INT	1000	RADIUS キャッシュに保存できるエントリの数を指定します。 最小値は 256 です。

設定変数	データタイプ	デフォルト値	説明
proxy.config.radius.cache.storage_size	INT	15728640	RADIUS キャッシュが使用できるディスク スペースの量の最大値を指定します。 この値はエントリの数の 100 倍以上でなければなりません。可能な最大量のディスク スペースを割り当てることを推奨します。
proxy.config.radius.auth.ttl_value	INT	60	Content Gateway がユーザー名およびパスワード エントリを RADIUS キャッシュに保存できる期間（分）を指定します。

NTLM

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.ntlm.auth.enabled	INT	0	NTLM プロキシ認証を有効化 (1) または無効化 (0) します。

proxy.config.ntlm.dc.list	STRING	NULL	ドメイン コントローラのホスト名を指定します。各エントリをカンマで区切る必要があります。形式は下記の通りです。
			`host_name[:port] [%netbios_name]`
			または
			`IP_address[:port] [%netbios_name]`
			Active Directory 2008 を使用している場合、**netbios_name** を含めるか、SMB ポート 445 を使用しなければなりません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ntlm.dc.load_balance	INT	0	ロードバランシングを有効化 (1) または無効化 (0) します。有効化すると、Content Gateway は ドメイン コントローラに認証要求を送信するときにロードバランスを行います。 **ご注意：**複数のドメイン コントローラが指定されている時は、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。
proxy.config.ntlm.dc.max_connections	INT	10	Content Gateway がドメイン コントローラをオープンすることができる接続の最大数を指定します。
proxy.config.ntlm.cache.enabled	INT	1	NTLM キャッシュを有効化 (1) または無効化 (0) します。Content Gateway が明示的プロキシの時にのみ適用します。 無効化すると、Content Gateway は 今後の使用に備えて NTLM キャッシュにすべての資格情報を保存しません。Content Gateway は 常に確認のためにドメイン サーバーに資格情報を送信します。
proxy.config.ntlm.cache.ttl_value	INT	900	Content Gateway が NTLM キャッシュにエントリを保存する時間（秒）を指定します。サポートされる値の範囲は 300 - 86400 秒です。
proxy.config.ntlm.cache.size	INT	5000	NTLM キャッシュに保存できるエントリの数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ntlm.cache.storage_size	INT	15728640	NTLM キャッシュが使用できるディスク スペースの量の最大値を指定します。この値は、NTLM キャッシュ内のエントリ数に比例する必要があります。たとえば、NTLM キャッシュ内の各エントリが約 128 バイトで、NTLM キャッシュに許可されるエントリの数が 5000 の場合、キャッシュ ストレージ サイズは 少なくとも 64000 バイト必要です。
proxy.config.ntlm.cache_exception.list	STRING	NULL	キャッシュされない IP アドレスおよび IP アドレスの範囲のリストを保持します。この変数は、Content Gateway マネージャの NTLM Multi-Host の IP アドレス フィールドから値を取得します。
proxy.config.ntlm.fail_open	INT	1	認証が下記の理由で失敗した場合に、要求の処理を続行することを許可する (1) か許可しない (0) かを指定します。 • ドメイン コントローラからの応答がない • クライアントからのメッセージの形式が正しくない • SMB 応答が不適切 **ご注意：**パスワード認証が失敗した場合は、続行されません。

統合 Windows 認証

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.winauth.enabled	INT	0	統合 Windows 認証 (Kerberos) を有効化 (1) または 無効化 (0) します。
proxy.config.winauth.realm	STRING	NULL	Windows Active Directory ドメインの名前を指定します。[*] を入力することで、DNS SRV レコード内で発見されたすべてのドメイン コントローラを使用できます。
proxy.config.winauth.dc.list	STRING	NULL	ドメイン コントローラのカンマ区切り形式のリストを指定します。
proxy.config.winauth.log_denied_requests	INT	1	拒否された認証要求のログ記録を有効化 (1) または無効化 (0) します。

透過的認証

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.transparent_auth_hostname	STRING	NULL	DSN を介してすべてのクライアントが解決できるプロキシの代替ホスト名を指定します。Content Gateway コンピュータの正規ホスト名が、DSN を介してすべてのユーザーに解決されない場合に、これが必要になります。
proxy.config.http.transparent_auth_type	INT	1	下記のどちらかを指定します： • 0 を指定すると、ユーザーセッションが認証された後、セッション ID とユーザー名を関連付けます。プロキシ チェイニングまたはネットワーク アドレス変換等 で 1 つの IP アドレスを共有するユーザーを、一意に識別するためにこの設定が必要になります。 • 1 を指定すると、ユーザーセッションが認証された後、クライアント IP アドレスとユーザー名を関連付けます。 いずれのモードでも、クライアントが再認証する必要かある時間の長さは、**proxy.config.http.transparent_auth_session_time** の値によって決定されます。
proxy.config.http.transparent_auth_session_time	INT	15	ブラウザが再認証を必要とするまでの時間（分）の長さを指定します。IP およびクッキー モード両方で、この値が使用されます。

HTTP エンジン

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.server_port	INT	8080	Content Gateway が Web トラフィック の Web プロキシサーバーとして動作する時、または Web トラフィックを透過的に処理する時に使用するポートを指定します。
proxy.config.http.server_port_attr	STRING	X	サーバー ポートのオプションを指定します。以下のいずれかを指定できます： • C=SERVER_PORT_COMPRESSED • X=SERVER_PORT_DEFAULT • T=SERVER_PORT_BLIND_TUNNEL
proxy.config.http.server_other_ports	STRING	NULL	変数 **proxy.config.http.server_port** で指定されたポート以外で、着信 HTTP 要求とバインドする ポートを指定します。
proxy.config.http.ssl_ports	STRING	443 563 8081 8071 9443 9444	トンネリングに使用するポートを指定します。これは、スペースで区切られたリストで、1 から 65535 までのポート範囲を指定できます。 Content Gateway は指定されたポートのみトンネリングを許可します。
proxy.config.http.insert_request_via_str	INT	1	下記のいずれか 1 つを指定します。 • 0 = 文字列に追加情報を付加しない。 • 1 = すべての追加情報を付加する。 • 2 = 一部の追加情報を付加する。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http. insert_response_via_str	INT	1	下記のいずれか 1 つを指定します。 • 0 = 文字列に追加情報を付加しない。 • 1 = すべての追加情報を付加する。 • 2 = 一部の追加情報を付加する。
proxy.config.http. enable_url_expandomatic	INT	1	**.com** ドメイン拡張を有効化 (1) または無効化 (0) します。これは、先頭に **www.** を追加し 末尾に **.com** を付加し、拡張したアドレスにリダイレクトすることで、不適切なホスト名を解決するよう Content Gateway を設定します。たとえば、クライアントが **host** に対して要求を行った場合、Content Gateway は www.host.com に要求をリダイレクトします。
proxy.config.http. no_dns_just_forward_ to_parent	INT	0	有効化 (1) すると、Content Gateway は HTTP 親キャッシュが有効な時に要求されたホスト名の DNS ルックアップを行いません。
proxy.config.http. uncacheable_requests_ bypass_parent	INT	0	有効化 (1) すると、Content Gateway は キャッシュ不可能な要求の場合に親プロキシを迂回します。
proxy.config.http. keep_alive_enabled	INT	1	オリジン サーバーまたはクライアントとのキープアライブ接続を有効化 (1) または無効化 (0) します。
proxy.config.http. chunking_enabled	INT	1	Content Gateway がチャンクレスポンスを作成するかどうかを指定します。 • 0 = しない • 1 = 常に行う

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.send_http11_requests	INT	3	Content Gateway が オリジン サーバーとの通信時に、HTTP バージョン 1.1 を使用するように設定します。以下の値いずれかを指定できます： • 0 = オリジン サーバーとの通信時に HTTP 1.1 を使用しない。 • 1 = オリジン サーバーとの通信時に常に HTTP 1.1 を使用する。 • 2 = これまで、オリジン サーバーが HTTP 1.1 を使用していた場合は、HTTP 1.1 を使用する。 • 3 = クライアント要求が HTTP 1.1 で、これまで、オリジン サーバーが HTTP 1.1 を使用していた場合は、HTTP 1.1 を使用する。 ご注意：HTTP 1.1 を使用した場合は、Content Gateway はオリジン サーバーに対してパイプライン処理を行う キープアライブ接続を使用できます。HTTP 0.9 を使用した場合は、Content Gateway は オリジン サーバーに対してキープアライブ接続を使用できません。HTTP 1.0 を使用した場合は、Content Gateway は オリジン サーバーに対してパイプライン処理なしの キープアライブ接続を使用できます。
proxy.config.http.send_http11_asfirstrequest	INT	1	有効化 (1) すると、Content Gateway がサーバーへの最初の要求で HTTP 1.1 を送信するように指定します。そうでない場合は、**proxy.config.http.send_http11_requests** で指定されたデフォルト動作になります。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.share_server_sessions	INT	1	サーバー セッションの再利用を有効化 (1) または無効化 (0) します。 ご注意：IP スプーフィングが有効化されている場合、Content Gateway は自動的にこの変数を無効にします。
proxy.config.http.share_server_sessions_max	INT	2500	再利用できるサーバーのセッションの最大数を指定します。
proxy.config.http.ftp_enabled	INT	1	HTTP で送信された FTP 要求を Content Gateway が処理することを有効化 (1) または無効化 (0) します。
proxy.config.http.record_heartbeat	INT	0	**content_cop** ハートビートのログ記録を有効化 (1) または無効化 (0) します。
proxy.config.http.large_file_support	INT	1	有効化 (1) すると、Content Gateway は 2 GB 以上ファイルのダウンロードをサポートします。

親プロキシ設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.parent_proxy_routing_enable	INT	0	HTTP 親キャッシング オプションを有効化 (1) または無効化 (0) します。 *階層キャッシング*、111 ページを参照してください。
proxy.config.http.parent_proxy.retry_time	INT	300	利用できない親キャッシュに対する再試行接続間隔を指定します。
proxy.config.http.parent_proxy.fail_threshold	INT	10	親キャッシュに対して接続を失敗できる回数を指定します。この回数を過ぎると Content Gateway は親キャッシュが使用不能とみなします。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.parent_proxy.total_connect_attempts	INT	4	親キャッシュに対して接続を試みることができる合計回数を指定します。この回数を過ぎると Content Gateway は親キャッシュを迂回するか、要求に失敗します（**bypass.config** ファイルの **go_direct** オプションに依存します）。
proxy.config.http.parent_proxy.per_parent_connect_attempts	INT	2	複数の親を使用している場合に、親単位で接続を試みることができる合計回数を指定します。
proxy.config.http.parent_proxy.connect_attempts_timeout	INT	30	親キャッシュ接続試行のタイムアウト値を秒単位で指定します。
proxy.config.http.forward.proxy_auth_to_parent	INT	0	有効化 (1) すると、親プロキシに送信される要求から Proxy-Authorization ヘッダーが削除*されません*。 Content Gateway が子プロキシで 親プロキシが認証を実行する場合に、これを有効化にします。
proxy.config.http.child_proxy.read_auth_from_header	INT	0	Content Gateway が親プロキシの場合に、X-Authenticated-User および X-Forwarded-For フィールドを読み込みます。 1 = 有効化 0 = 無効化
proxy.local.http.parent_proxy.disable_ssl_connect_tunneling	INT	0	有効化 (1) すると、HTTPS 要求は親プロキシを迂回します。
proxy.local.http.parent_proxy.disable_unknown_connect_tunneling	INT	0	有効化 (1) すると、非 HTTPS トンネル要求は親プロキシを迂回します。

HTTP 接続タイムアウト（秒単位）

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.keep_alive_no_activity_timeout_in	INT	60	トランザクション終了後、後続の要求のために、クライアントとの接続を開きつづける時間を指定します。
proxy.config.http.keep_alive_no_activity_timeout_out	INT	60	トランザクション終了後、後続のデータ転送のために、オリジン サーバーへの接続を開き続ける時間を指定します。
proxy.config.http.transaction_no_activity_timeout_in	INT	120	トランザクションが停止した場合に、Content Gateway がクライアントとの接続を開き続ける時間を指定します。
proxy.config.http.transaction_no_activity_timeout_out	INT	120	トランザクションが停止した場合に、Content Gateway がオリジン サーバーとの接続を開き続ける時間を指定します。
proxy.config.http.transaction_active_timeout_in	INT	0	Content Gateway が、クライアントと接続されたままになる時間を指定します。タイムアウト時間前にクライアントへの転送が完了しない場合、Content Gateway は接続を閉じます。 デフォルト値の 0 は タイムアウトなしです。
proxy.config.http.transaction_active_timeout_out	INT	0	Content Gateway がオリジン サーバーへの接続要求の完了を待つ時間を指定します。このタイムアウト時間の前に、Content Gateway がオリジン サーバーへの転送を完了しない場合、接続要求は終了させられます。 デフォルト値の 0 は タイムアウトなしです。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.accept_no_activity_timeout	INT	120	秒単位でタイムアウト間隔を指定します。この時間を過ぎると、Content Gateway はアクティビティのない接続を閉じます。
proxy.config.http.background_fill_active_timeout	INT	60	Content Gateway が バックグラウンド読み込みを継続する時間を指定します。この時間を過ぎると、オリジン サーバー接続を放棄し切断します。
proxy.config.http.background_fill_completed_threshold	FLOAT	0.50000	プロキシが、オリジン サーバーからキャッシュに入れるドキュメントの取得（*バックグラウンド読み込み*）を継続中に、クライアントが中断した時に、既に転送された全ドキュメント サイズの割合を指定します。

オリジン サーバー接続の試行

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.connect_attempts_max_retries	INT	6	オリジン サーバーからの応答がない時に、Content Gateway が接続を再試行する最大回数を指定します。
proxy.config.http.connect_attempts_max_retries_dead_server	INT	2	オリジン サーバーが利用不可の時に、Content Gateway が接続を再試行する最大回数を指定します。
proxy.config.http.connect_attempts_rr_retries	INT	2	接続試行に失敗できる最大回数を指定します。この回数を過ぎると、サーバーがラウンド ロビン DNS エントリを使用している場合、ラウンド ロビン エントリはダウンとマークされます。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.connect_attempts_timeout	INT	60	オリジン サーバー接続のタイムアウト値を秒単位で指定します。
proxy.config.http.streaming_connect_attempts_timeout	INT	1800	ストリーミング コンテンツ接続のタイムアウト値を秒単位で指定します。
proxy.config.http.down_server.cache_time	INT	30	Content Gateway が到達できなかったオリジン サーバーを記憶する時間を秒単位で指定します。
proxy.config.http.down_server.abort_threshold	INT	10	オリジン サーバーの応答ヘッダーの送信が遅すぎるために、クライアントが接続を破棄した時に Content Gateway がオリジン サーバーを利用不可とマークするまでの秒数を指定します。

否定応答キャッシング

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http. negative_caching_enabled	INT	0	有効化 (1) すると、Content Gateway は否定応答をキャッシュします（要求されたページが存在しない場合の *404 Not Found* 等）。次回クライアントが同じページを要求した場合、Content Gateway はキャッシュからの否定応答を提供します。 Content Gateway は下記の否定応答をキャッシュします： 204 No Content 305 Use Proxy 400 Bad Request 403 Forbidden 404 Not Found 405 Method Not Allowed 500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Timeout
proxy.config.http. negative_caching_ lifetime	INT	1800	Content Gateway が 否定応答をキャッシュ内に保持する時間を指定します。

プロキシ ユーザー変数

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.anonymize_remove_from	INT	0	有効化 (1) すると、ユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う **From** ヘッダーを削除します。
proxy.config.http.anonymize_remove_referer	INT	0	有効化 (1) すると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う **Referer** ヘッダーを削除します。
proxy.config.http.anonymize_remove_user_agent	INT	0	有効化 (1) すると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う **User-Agent** ヘッダーを削除します。
proxy.config.http.anonymize_remove_cookie	INT	0	有効化 (1) すると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う **Cookie** ヘッダーを削除します。
proxy.config.http.anonymize_remove_client_ip	INT	1	有効化 (1) すると、プライバシーを強化するために、Content Gateway は トランザクションを伴う **Client-IP** ヘッダーを削除します。
proxy.config.http.anonymize_insert_client_ip	INT	0	有効化 (1) すると、クライアント IP アドレスを保持するために、Content Gateway は **Client-IP** ヘッダー挿入します。
proxy.config.http.append_xforwards_header	INT	0	有効化 (1) すると、Content Gateway は送信要求に **X-Forwards** ヘッダーを付加します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.anonymize_other_header_list	STRING	NULL	Content Gateway が、送信要求から削除するヘッダーを指定します。
proxy.config.http.snarf_username_from_authorization	INT	0	有効化 (1) すると、認証スキームが *Basic* の場合に LDAP の認証ヘッダーからユーザ名とパスワードを削除します。
proxy.config.http.insert_squid_x_forwarded_for	INT	0	有効化 (1) すると、Content Gateway は **X-Forwarded-For** ヘッダーにクライアント IP アドレスを追加します。
proxy.config.http.insert_x_authenticated user	INT	0	有効化 (1) すると、Content Gateway は プロキシ認証ユーザーを公表するために **X-Authenticated-User** ヘッダーを挿入します。

セキュリティ

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.push_method_enabled	INT	0	有効化 (1) すると、ユーザー要求なしにコンテンツを直接にキャッシュにプッシュする **filter.config** ルールを使用できます。既知のソース IP アドレスのみが PUSH 要求をキャッシュに対して実行するようにするために、PUSH アクションのフィルタリングルールを追加する必要があります。設定ファイル エディタの Method ドロップダウン リストで PUSH を有効化する前に、この変数を有効化する必要があります。

キャッシュ コントロール

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http. cache.http	INT	1	HTTP 要求のキャッシングを有効化 (1) または無効化 (0) します。
proxy.config.http. cache.ftp	INT	1	HTTP で送信された FTP 要求のキャッシングを有効化 (1) または無効化 (0) します。
proxy.config.http.cache. ignore_client_no_cache	INT	0	有効化 (1) すると、Content Gateway はキャッシュをバイパスするクライアント要求を無視します。
proxy.config.http.cache. ims_on_client_no_cache	INT	0	有効化 (1) すると、着信要求が **no-cache** ヘッダーを含む場合に Content Gateway はオリジン サーバーに条件付要求を発行します。
proxy.config.http.cache. ignore_server_no_cache	INT	0	有効化 (1) すると、Content Gateway はキャッシュをバイパスするオリジン サーバー要求を無視します。
proxy.config.http.cache. cache_responses_ to_cookies	INT	3	クッキーがキャッシュされる方法を指定します。 • 0 = クッキーに対するすべての応答をキャッシュしない • 1 = すべてのコンテンツ タイプをキャッシュする • 2 = イメージ タイプのみキャッシュする • 3 = テキスト コンテンツ タイプ以外すべてキャッシュする
proxy.config.http.cache. ignore_authentication	INT	0	有効化 (1) すると、応答内の **WWW-Authentication** ヘッダーを無視します。 **WWW-Authentication** ヘッダーは削除され、キャッシュされません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.cache_urls_that_look_dynamic	INT	0	動的と思われる URL のキャッシングを有効化 (1) または無効化 (0) します。
proxy.config.http.cache.enable_default_vary_headers	INT	0	**Vary** ヘッダーを含んでいない HTTP オブジェクトの代替バージョンのキャッシングを有効化 (1) または (0) 無効化します。
proxy.config.http.cache.when_to_revalidate	INT	0	いつコンテンツを再確認するかを指定します。 • 0 = キャッシュ ディレクティブまたはヒューリスティックを使用（デフォルト値）。 • 1 = ヒューリスティックの場合陳腐化。 • 2 = 常に陳腐化（常に再確認）。 • 3 = 陳腐化なし。 • 4 = 要求に **If-Modified-Since** ヘッダーがない場合キャッシュ ディレクティブまたはヒューリスティックを使用 (0)。要求に **If-Modified-Since** ヘッダーが含まれる場合、Content Gateway は常にキャッシュコンテンツを再確認し、プロキシ要求に **If-Modified-Since** ヘッダーを使用します。
proxy.config.http.cache.when_to_add_no_cache_to_msie_requests	INT	0	いつ Microsoft Internet Explorer の要求に **no-cache** ディレクティブを追加するかを指定します。以下のいずれかを指定できます。 • 0 = 0 = **no-cache** を MSIE 要求に追加しない。 • 1 = 1 = **no-cache** を IMS MSIE 要求に追加する。 • 2 = 2 = **no-cache** をすべての MSIE 要求に追加する。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.required_headers	INT	0	要求がキャッシュ可能であるために要求内で必要なヘッダー タイプを指定します。 • 0 = ドキュメントをキャッシュ可能にするために必要なヘッダーはない。 • 1 = 少なくとも **Last-Modified** ヘッダーは必要。 • 2 = 明示的寿命時間が必要、**Expires** または **Cache-Control**。
proxy.config.http.cache.max_stale_age	INT	604800	陳腐化応答の許容される最大期間を指定します。この期間を過ぎるとキャッシュできません。
proxy.config.http.cache.range.lookup	INT	1	有効化 (1) すると、Content Gateway はキャッシュ内の範囲要求をルックアップします。
proxy.config.http.cache.cache_301_responses	INT	0	[301] 応答ページのキャッシングを有効化 (1) または無効化 (0) します。

ヒューリスティック期限

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.heuristic_min_lifetime	INT	3600	キャッシュ内のドキュメントが最新と見なされる最小時間を指定します。
proxy.config.http.cache.heuristic_max_lifetime	INT	86400	キャッシュ内のドキュメントが最新と見なされる最大時間を指定します。
proxy.config.http.cache.heuristic_lm_factor	FLOAT	0.10000	最新性計算のためのエージング係数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.fuzz.time	INT	240	プロキシがリフレッシュのためにチェックするドキュメント陳腐化時間の秒単位の間隔を指定します。
proxy.config.http.cache.fuzz.probability	FLOAT	0.00500	指定したファズ タイム中にドキュメントでリフレッシュが行われる確率を指定します。

ダイナミック コンテンツおよびコンテンツ ネゴシエーション

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.vary_default_text	STRING	NULL	テキスト ドキュメントの場合に、Content Gateway が変化させるヘッダーを指定します。たとえば、**user-agent** を指定した場合、プロキシは検出されたドキュメントの異なるユーザー エージェントのバージョンをキャッシュします。
proxy.config.http.cache.vary_default_images	STRING	NULL	イメージの場合に、Content Gateway が 変化させるヘッダーを指定します。
proxy.config.http.cache.vary_default_other	STRING	NULL	テキストとイメージ以外の場合に、Content Gateway が変化させるヘッダーを指定します。

匿名 FTP パスワード

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.anonymous_passwd	STRING	*インストール中に提供された管理者電子メールの値*	アクセスするためにはパスワードを要求する FTP サーバーの匿名パスワードを指定します。 Content Gateway は、この変数のデフォルト値として Content Gateway ユーザー アカウント名を使用します。

キャッシュされた FTP ドキュメントのライフタイム

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.cache.document_lifetime	INT	259200	FTP ドキュメントが、キャッシュ内に存在する最大時間を指定します。

FTP 転送モード

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.binary_transfer_only	INT	0	有効化 (1) すると、HTTP クライアントから要求されたすべての FTP ドキュメントはバイナリモードのみで転送されます。 無効化 (0) すると、HTTP クライアントから要求されたすべての FTP ドキュメントは、ドキュメント タイプに依存して ASCII またはバイナリモードで転送されます。

カスタム ユーザー応答のページ

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config. body_factory. enable_customizations	INT	0	カスタムユーザー応答ページを有効化するか無効化するか、どの応答ページを使用するかを指定します。 • 0 = カスタム ユーザー応答ページを無効化します • 1 = デフォルト ディレクトリ内のみのカスタム ユーザー応答ページを有効化します • 2 = 言語別のユーザー応答ページを有効化します
proxy.config. body_factory. enable_logging	INT	0	カスタム応答ページのログ記録を有効化 (1) または無効化 (0) します。有効にすると、カスタム応答ページが使用または変更される毎に、Content Gateway はエラー ログに メッセージを記録します。
proxy.config. body_factory. template_sets_dir	STRING	config/ body_factory	カスタム応答ページのデフォルト ディレクトリを指定します。
proxy.config. body_factory.response_ suppression_mode	INT	0	Content Gateway が作成された応答ページをいつ抑制するかを指定します： • 0 = 作成された応答ページを抑制しない • 1 = 作成された応答ページを常に抑制する • 2 = 遮断されたトラフィックの場合のみ抑制する

FTP エンジン

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
FTP over HTTP			
proxy.config.ftp.data_connection_mode	INT	1	FTP 接続モードを指定します： • 1 = PASV 次に PORT • 2 = PORT のみ • 3 = PASV のみ
proxy.config.ftp.control_connection_timeout	INT	300	Content Gateway が FTP サーバーからの応答を待つ時間を指定します。
proxy.config.ftp.rc_to_switch_to_PORT	STRING	NULL	設定変数 **proxy.config.ftp.data_connection_mode** が 1 に設定されている場合に、PASV が失敗した時 Content Gateway が自動的に PORT コマンドにフェイルオーバーするときに使用する応答コードを指定します。 この変数は、HTTP クライアントからの FTP 要求のみに使用されます。
FTP プロキシ			
proxy.config.ftp.ftp_enabled	INT	0	FTP クライアントからの FTP 要求処理を有効化 (1) または無効化 (0) します。
proxy.config.ftp.cache_enabled	INT	0	FTP オブジェクトのキャッシングを有効化 (1) または無効化 (0) します。 このオプションを無効化すると、Content Gateway は、FTP サーバーからの FTP オブジェクトを常に処理します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.file_fresh_mdtm_checking_enabled	INT	0	FTP キャッシングを有効化する場合のみ適用します。 有効化 (1) すると、Content Gateway は、ファイルの最後の変更時間を取得するために、[RETR] コマンドの前に [MDTM] コマンドを送信します。 ファイルがキャッシュに入れられており、last_contact 時間が [MDTM] 応答と同じである場合、プロキシは、キャッシュ ファイルをクライアントに提供します。
proxy.config.ftp.logging_enabled	INT	1	FTP トランザクションのログ記録を有効化 (1) または無効化 (0) します。
proxy.config.ftp.proxy_server_port	INT	2121	FTP 接続に使用するポートを指定します。
proxy.config.ftp.open_lisn_port_mode	INT	1	データ転送のために FTP が開くリッスン ポートを指定します。 • 1 = オペレーティング システムが使用可能なポートを選択します。Content Gateway は 0 を送信し、リッスンが成功すれば新しいポート番号を取得します。 • 2 = Content Gateway 変数 **proxy.config.ftp.min_lisn_port** および **proxy.config.ftp.max_lisn_port**（後述）で指定されたポートの範囲で、リッスン ポートを決定します。
proxy.config.ftp.min_lisn_port	INT	32768	FTP クライアントが PASV を送信 または Content Gateway が FTP サーバーに PORT を送信する時に、データ接続のために Content Gateway によって使用されるリッスン ポートの範囲の最小値を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.max_lisn_port	INT	65535	FTP クライアントが PASV を送信 または Content Gateway が FTP サーバーに PORT を送信する時に、データ接続のために Content Gateway によって使用されるリッスン ポートの範囲の最大値を指定します。
proxy.config.ftp.server_data_default_pasv	INT	1	サーバー サイドとのデータ接続設定に使用するデフォルトの方法を指定します。 • 1 = Content Gateway は FTP サーバーに PASV を送信し、FTP サーバーはリッスン ポートを開きます。 • 0 = Content Gateway は最初に PORT を試みます（接続のプロキシ側にリッスン ポートをセットアップします）。
proxy.config.ftp.different_client_port_ip_allowed	INT	0	有効化 (1) すると、Content Gateway は、データ接続の確立を実行中の FTP クライアント以外のコンピュータに接続できます。 FTP クライアントは自分のサイドにリッスン ポートをセットアップするために PORT を使用します。そして、データ接続（ファイル転送に使用）を確立するために、Content Gateway がそのポートに接続することを許可します。リッスン ポートをセットアップする時、FTP クライアントは IP アドレスとリッスン ポートのポート番号を指定します。この変数が 0（ゼロ）の場合、クライアントから送信された IP アドレスと FTP クライアントを実行しているコンピュータの IP アドレス が異なる場合は、Content Gateway は FTP クライアントに接続できません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.try_pasv_times	INT	1024	FTP クライアントが PASV を送信した時に、Content Gateway がリッスン ポートのオープンを試みる回数を指定します。
proxy.config.ftp.try_port_times	INT	1024	FTP サーバーに PORT を送信する時に、Content Gateway がリッスン ポートのオープンを試みる最大回数を指定します。
proxy.config.ftp.try_server_ctrl_connect_times	INT	6	Content Gateway が FTP サーバーのコントロールリッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.try_server_data_connect_times	INT	3	Content Gateway が、FTP サーバーに PASV を送信し IP/ リッスン ポート情報を受信した時に、FTP サーバーのデータ リッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.try_client_data_connect_times	INT	3	FTP クライアントが IP/ リッスン ポート情報を付けて PORT を送信した時に、Content Gateway が FTP クライアントのデータ リッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.client_ctrl_no_activity_timeout	INT	900	FTP クライアント コントロール接続の非アクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.client_ctrl_active_timeout	INT	14400	FTP クライアント コントロール接続のアクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.server_ctrl_no_activity_timeout	INT	120	FTP サーバー コントロール接続の非アクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.server_ctrl_active_timeout	INT	14400	FTP サーバー コントロール接続のアクティブ タイムアウトを秒単位で指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.client_data_no_activity_timeout	INT	120	クライアント FTP データ転送接続がアイドル状態を維持する最大時間を秒単位で指定します。この時間を過ぎると接続は中断されます。
proxy.config.ftp.client_data_active_timeout	INT	14400	クライアントからの FTP データ転送接続の最大時間を秒単位で指定します。
proxy.config.ftp.server_data_no_activity_timeout	INT	120	サーバー FTP データ転送接続がアイドル状態を維持する最大時間を秒単位で指定します。この時間を過ぎると接続は中断されます。
proxy.config.ftp.server_data_active_timeout	INT	14400	サーバーからの FTP データ転送接続の最大時間を秒単位で指定します。
proxy.config.ftp.pasv_accept_timeout	INT	120	Content Gateway のリッスン データ ポートのタイムアウト値を指定します（PASV の場合、クライアント データ接続）。
proxy.config.ftp.port_accept_timeout	INT	120	Content Gateway のリッスン データ ポートのタイムアウト値を指定します（PORT の場合、サーバー データ接続）。
proxy.config.ftp.share_ftp_server_ctrl_enabled	INT	1	複数の匿名 FTP クライアントの間でのサーバー コントロール接続の共有を有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.share_only_after_session_end	INT	1	FTP サーバー コントロール接続が異なる FTP クライアント セッション間で共有される方法を指定します。 • 1 = FTP クライアント セッションが完了した時（通常、FTP クライアントが QUIT コマンドを送信）にのみ、他のクライアント セッションが FTP サーバー コントロール接続を使用することができます。 • 0 = FTP クライアント セッションが FTP サーバー接続を能動的に使用していない場合にのみ、他のクライアント セッションが FTP サーバー コントロール接続を使用することができます。たとえば、要求がキャッシュ ヒットであるか、またはアイドル セッション中である場合です。
proxy.config.ftp.server_ctrl_keep_alive_no_activity_timeout	INT	90	どの FTP クライアントも FTP サーバー コントロール接続を使用しなくなった時の、タイムアウト値を指定します。
proxy.config.ftp.reverse_ftp_enabled	INT	0	サポートされていません。
proxy.config.ftp.login_info_fresh_in_cache_time	INT	604800	220/230 応答（ログイン メッセージ）をキャッシュ内で最新とする時間を指定します。
proxy.config.ftp.data_source_port_20_enabled	INT	0	有効化 (1) すると、Active モードの FTP クライアントに対する送信データ転送接続にソース ポート 20 をバインドします。
proxy.config.ftp.directory_listing_fresh_in_cache_time	INT	86400	ディレクトリのリストがキャッシュ内で最新であり続ける時間を指定します。
proxy.config.ftp.file_fresh_in_cache_time	INT	259200	FTP ファイルがキャッシュ内で最新であり続ける時間を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.simple_directory_listing_cache_enabled	INT	1	引数（例、[dir] または [Is] ）なしのディレクトリのリストのキャッシングを有効化 (1) または無効化 (0) します。
proxy.config.ftp.full_directory_listing_cache_enabled	INT	1	引数（例、[s -al] または [ls *.txt] ）付きのディレクトリのリストのキャッシングを有効化 (1) または無効化 (0) します。

SOCKS プロセッサ

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.socks.socks_needed	INT	0	SOCKS オプションを有効化 (1) または無効化 (0) します。 *SOCKS ファイアウォール統合の設定*、211 ページを参照してください。
proxy.config.socks.socks_version	INT	4	SOCKS バージョンを指定します。
proxy.config.socks.default_servers	STRING	s1.example.com:1080;socks2:4080	Content Gateway が通信する SOCKS サーバーの名前とポートを指定します。
proxy.config.socks.accept_enabled	INT	0	SOCKS プロキシ オプションを有効化 (1) または無効化 (0) します。SOCKS プロキシとして、Content Gateway は SOCKS トラフィックを受信し（通常はポート 1080 上で）、すべての要求を SOCKS サーバーへ直接に転送します。
proxy.config.socks.accept_port	INT	1080	Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.socks.socks_server_enabled	INT	0	ご注意：Content Gateway がアプライアンス上にインストールされている場合にのみ設定します。
proxy.config.socks.socks_server_port	INT	61080	ご注意：Content Gateway がアプライアンス上にインストールされている場合にのみ設定します。

ネット サブシステム

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.net.connections_throttle	INT	45000	Content Gateway が処理できる接続の最大数を指定します。Content Gateway が追加のクライアント要求を受信した場合、それらは要求が処理されるまでキューに入れられます。 この変数を 100 未満にしないでください。

クラスタ サブシステム

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.cluster.cluster_port	INT	8086	クラスタ通信に使用するポートを指定します。
proxy.config.cluster.ethernet_interface	STRING	*your_interface*	クラスタ トラフィックに使用するネットワーク インターフェースを指定します。クラスタ内のすべてのノードは同じネットワーク インターフェースを使用しなければなりません。

キャッシュ

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.cache.permit.pinning	INT	0	キャッシュ ピンニング オプションを有効化 (1) または無効化 (0) します。このオプションで、指定時間の間、キャッシュにオブジェクトを残しておくことができます。**cache.config** ファイルでキャッシュ ピンニング ルールを設定します（*cache.config*、450 ページを参照）。
proxy.config.cache.ram_cache.size	INT	-1	RAM キャッシュのサイズをバイト単位で指定します。 値を -1 にすると、RAM キャッシュのサイズは自動的にディスク 1 GB につき約 41 MB になります。
proxy.config.cache.limits.http.max_alts	INT	3	Content Gateway がキャッシュできる HTTP 代替の最大数を指定します。
proxy.config.cache.max_doc_size	INT	0	キャッシュ内のドキュメントの最大サイズを指定します（バイト単位）。 0 = サイズ制限なし。

DNS

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.dns.search_default_domains	INT	1	ローカル ドメイン拡張を有効化 (1) または無効化 (0) します。有効化すると、Content Gateway は、ローカル ドメインを拡張することで不適切なホスト名を解決しようとします。たとえば、クライアントが **host_x** という名前の不適切なホスト名を要求した場合、かつ Content Gateway のローカル ドメインが **y.com** の場合、Content Gateway はホスト名を **host_x.y.com** に拡張します。
proxy.config.dns.splitDNS.enabled	INT	0	DNS サーバー選択を有効化 (1) または無効化 (0) します。有効 (1) にすると、Content Gateway は選択のために **splitdns.config** ファイルを参照します。 *Split DNS オプションの使用*、215 ページを参照してください。
proxy.config.dns.splitdns.def_domain	STRING	NULL	分割 DNS 要求のデフォルト ドメインを指定します。分割 DNS が使用する DNS サーバーを決定する前に、ホスト名がドメインを含まない場合に、この値はホスト名に自動的に付加されます。

設定変数	データタイプ	デフォルト値	説明
proxy.config.dns. url_expansions	STRING	NULL	ルックアップ失敗の後、自動的にホスト名に付加されるホスト名拡張子のリストを指定します。たとえば、Content Gateway にホスト名拡張子 **.org** を付加させたい場合、変数の値に **org** を指定します（Content Gateway は自動的にドット（.）を付加します）。 ご注意：変数 **proxy.config.http.enable_url_expandomatic** が 1（デフォルト値）に設定されている場合、このリストに **www.** および **.com** を加える必要はありません。Content Gateway は、指定した値を試みる前に自動的に **www.** および **.com** を試みます。
proxy.config.dns. lookup_timeout	INT	20	DNS ルックアップ タイムアウト時間を秒単位で指定します。タイムアウト時間が過ぎると、ルックアップの試行を中止します。 デフォルト値が proxy.config.hostdb.lookup_timeout より小さいので、優先されます。
proxy.config.dns.retries	INT	5	DNS ルックアップを試みる回数を指定します。この回数を超えると、試行を中止します。
proxy.config.dns. prefer_ipv4	INT	1	名前が IPv4 アドレスおよび IPv6 アドレス両方に解決される時、優先するアドレス タイプを指定します。
proxy.config.ipv6. ipv6_enabled	INT	0	IPv6 のサポートを有効化 (1) するか、無効化 (0) するかを指定します。

DNS プロキシ

Help | Content Gateway | バージョン 7.8.x

設定変数 データ タイプ	データ タイプ	デフォルト値	説明
proxy.config.dns.proxy.enabled	INT	0	クライアントに代わって、DNS 要求を解決する DNS プロキシ キャッシング オプションを有効化 (1) または無効化 (0) します。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。-*DNS プロキシ キャッシング*、123 ページを参照してください。
proxy.config.dns.proxy_port	INT	5353	Content Gateway が DNS トラフィックに使用するポートを指定します。

HostDB

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.hostdb.size	INT	200000	ホスト データベースに許可されるエントリの最大数を指定します。
proxy.config.hostdb.ttl_mode	INT	0	ホスト データベース時間をライブ (ttl) モードに指定します。 デフォルトでは、Content Gateway ホスト データベースは、名前サーバーによって設定された time-to-live (ttl) の値を監視します。Content Gateway を別の値に再設定できます。 下記のいずれかの値を指定できます。 0 - 名前サーバーによって設定された ttl の値に従います（デフォルト）。 1 = 名前サーバーによって設定された ttl の値を無視し、Content Gateway 設定変数 **proxy.config.hostdb.timeout** によって設定された値を使用します。この変数を環境に適した値に設定してください。 2 = 2 つの値（名前サーバーによって設定された値と Content Gateway によって設定された値）の小さい方の値を使用します。 3 = 2 つの値（名前サーバーによって設定された値と Content Gateway によって設定された値）の大きい方の値を使用します。
proxy.config.hostdb.timeout	INT	86400	フォアグラウンド タイムアウトを秒単位で指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.hostdb.fail.timeout	INT	60	失敗した DNS がキャッシュさる時間を秒単位で指定します。
proxy.config.hostdb.strict_round_robin	INT	0	無効化 (0) すると、オリジンサーバーが使用可能な限り、Content Gateway は 同じクライアントに同じオリジン サーバーを使用します。

ログ記録設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.logging_enabled	INT	1	ログ記録を有効化または無効化します。 • 0 = ログ記録無効化 • 1 = エラーのみ ログ記録 • 2 = トランザクションのみ ログ記録 • 3 = 完全ログ記録（エラー + トランザクション） *ログ ファイルの使用*、271 ページを参照してください。
proxy.config.log2.max_secs_per_buffer	INT	5	バッファ内のデータが ディスクにフラッシュされるまでの最大時間を指定します。
proxy.config.log2.max_space_mb_for_logs	INT	5120 Ç‹ Ç¾ÇÕ 20480	ログ記録ディレクトリに割り当てられる容量をメガバイト単位で指定します。 Content Gateway が V シリーズ アプライアンス上である場合は、そのサイズは 5120 (5 GB) に設定され、これを変更することはできません。 Content Gateway がスタンドアローン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.max_space_mb_for_orphan_logs	INT	25	ノードが照合クライアントとして動作している場合に、ログ記録ディレクトリに割り当てられる容量をメガバイト単位で指定します。
proxy.config.log2.max_space_mb_headroom	INT	100	ログ記録スペース限界の許容値をバイト単位で指定します。変数 **proxy.config.log2.auto_delete_rolled_file** が 1（有効化）に設定されている場合、空き容量がここで指定された値より少なくなった時にログファイルの自動削除がトリガされます。
proxy.config.log2.hostname	STRING	localhost	Content Gateway を実行しているコンピュータのホスト名を指定します。
proxy.config.log2.logfile_dir	STRING	/opt/WCG/logs	ログ記録ディレクトリの完全パスを指定します。
proxy.config.log2.logfile_perm	STRING	rw-r--r--	ログ ファイルのアクセス許可を指定します。標準的な UNIX フ ァイルのアクセス許可が使用されます（所有者、グループ、他のユーザー）。有効な値は下記のとおりです。 • - = 許可なし • r = 読み込み許可 • w = 書き込許可 • x = 実行許可 アクセス許可は、Content Gateway プロセスのアンマスク設定に従います。これは、設定ファイルで指定したとしても、002 のアンマスク設定が、other の書き込を許可しないことを意味します。 設定ファイルが変更された時、既存のログ ファイルのアクセス許可は変更されません。 Linux のみ。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2. custom_logs_enabled	INT	0	有効化 (1) すると、**logs_xml.config** の定義に従ったカスタム ログ ファイルの定義および作成をサポートします。 *logs_xml.config*、461 ページを参照してください。
proxy.config.log2. xml_logs_config	INT	1	ログ ファイルのロールオーバーが発生するサイズをメガバイト単位で指定します。*イベント ログ ファイルの取り込み*、284 ページを参照してください。
proxy.config.log2. squid_log_enabled	INT	0	squid ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2. squid_log_is_ascii	INT	1	squid ログ ファイルのタイプを指定します。 • 1 = ASCII • 0 = バイナリ
proxy.config.log2. squid_log_name	STRING	squid	squid ログ ファイル名を指定します。
proxy.config.log2. squid_log_header	STRING	NULL	squid ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2. common_log_enabled	INT	0	Netscape Common ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2. common_log_is_ascii	INT	1	Netscape Common ログ ファイルのタイプを指定します。 • 1 = ASCII • 0 = バイナリ
proxy.config.log2. common_log_name	STRING	common	Netscape Common ログ ファイル名を指定します。
proxy.config.log2. common_log_header	STRING	NULL	Netscape Common ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2. extended_log_enabled	INT	1	Netscape Extended ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
proxy.confg.log2. extended_log_is_ascii	INT	1	Netscape Extended ログ ファイルのタイプを指定します。 • 1 = ASCII • 0 = バイナリ
proxy.config.log2. extended_log_name	STRING	extended	Netscape Extended ログ ファイル名を指定します。
proxy.config.log2. extended_log_header	STRING	NULL	Netscape Extended ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2. extended2_log_enabled	INT	0	Netscape Extended-2 ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2. extended2_log_is_ascii	INT	1	Netscape Extended-2 ログ ファイルのタイプを指定します。 • 1 = ASCII • 0 = バイナリ
proxy.config.log2. extended2_log_name	STRING	extended2	Netscape Extended-2 ログ ファイル名を指定します。
proxy.config.log2. extended2_log_header	STRING	NULL	Netscape Extended-2 ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2. separate_host_logs	INT	0	有効化 (1) すると、Contentl Gateway は **log_hosts.config** ファイルにリストされている各オリジン サーバーごとに、個別の HTTP/FTP トランザクションのログ ファイルを作成します（*HTTP ホスト ログ分割、287 ページ*を参照してください）。

設定変数	データタイプ	デフォルト値	説明
proxy.local.log2.collation_mode	INT	0	ログ照合モードを指定します。 • 0 = 照合無効化。 • 1 = このホストはログ照合サーバー。 • 2 = このホストは照合クライアントで、照合サーバーに標準フォーマットを使用してエントリを送信。 ログ照合サーバーに、XML ベースのカスタム フォーマットを送信するための情報は、*logs_xml.config*、461 ページを参照してください。
proxy.confg.log2.collation_host	STRING	NULL	ログ照合サーバーのホスト名を指定します。
proxy.config.log2.collation_port	INT	8085	照合サーバーとクライアント間の通信に使用するポートを指定します。
proxy.config.log2.collation_secret	STRING	foobar	照合サーバー使用時に、無許可の情報の交換を防止し、ログ記録データを検証するために使用するパスワードを指定します。
proxy.config.log2.collation_host_tagged	INT	0	有効化 (1) すると、ログ エントリを作成した照合クライアントのホスト名を各エントリに含めるように、Content Gateway を設定します。
proxy.config.log2.collation_retry_sec	INT	5	照合サーバー接続再試行の間隔を秒単位で指定します。
proxy.config.log2.rolling_enabled	INT	1	ログ ファイル取り込みを有効化 (1) または無効化 (0) します。 *イベント ログ ファイルの取り込み*、284 ページを参照してください。
proxy.config.log2.rolling_interval_sec	INT	21600	ログ ファイル取り込み間隔を秒単位で指定します。最小値は 300（5 分）です。最大値は 86400 秒（1 日）です。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.rolling_offset_hr	INT	0	ファイル取り込みオフセット時刻を指定します。ログの取り込みを開始する時刻です。
proxy.config.log2.rolling_size_mb	INT	10	現在のファイルを閉じ、新しいファイルを開くサイズをメガバイト単位で指定します。
proxy.config.log2.auto_delete_rolled_files	INT	1	取り込みファイルの自動削除を有効化 (1) または無効化 (0) します。
proxy.config.log2.sampling_frequency	INT	1	トランザクション毎ではなく、トランザクションのサンプルのみをログ記録するように、Content Gateway を設定します。下記の値を指定できます： • 1 = トランザクション毎にログ記録 • 2 = 2 番目のトランザクション毎にログ記録 • 3 = 3番目のトランザクション毎にログ記録 など ...

URL リマップ ルール

Help | Content Gateway | バージョン 7.8.x

設定変数	データ タイプ	デフォルト値	説明
proxy.config.url_remap.default_to_server_pac	INT	0	プロキシ サーバー ポート（デフォルト 8080）上の PAC ファイルの要求が、PAC ポートにリダイレクトされることを有効化 (1) または無効化 (0) します。 このタイプのリダイレクトが動作するためには、変数 proxy.config.reverse_proxy.enabled が 1 に設定されている必要があります。
proxy.config.url_remap.default_to_server_pac_port	INT	-1	PAC ポートを設定します。Content Gateway プロキシ サーバー ポートへの PAC 要求は、このポートにリダイレクトされます。 **-1** を指定すると、PAC ポートは自動構成ポートに設定されます（デフォルト自動構成ポートは 8083 です）。これは、デフォルト設定です。 この変数は、異なるポートから PAC ファイルを取得するために、**proxy.config.url_remap.default_to_server_pac** 変数と一緒に使用することができます。このポートの PAC ファイルを処理するプロセスを作成し、実行する必要があります。たとえば、ポート 9000 をリッスンし、すべての要求に対する応答に PAC ファイルを書き込む Perl スクリプトを作成します。この変数を 9000 に設定した場合、ポート 8080 上でプロキシ サーバーから PAC ファイルを要求するブラウザは、Perl スクリプトによって提供された PAC ファイルを取得します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.url_remap.remap_required	INT	0	remap.config ファイルのマッピング ルールにリストされたオリジン サーバーからの要求のみを処理 するように、Content Gateway を設定するためには、この変数を 1 に設定します。要求が一致しない場合、ブラウザはエラーを受け取ります。
proxy.config.url_remap.pristine_host_hdr	INT	0	再マッピング中に要求内のクライアント ホスト ヘッダーを保持するためには、この変数を 1 に設定します。

スケジュール更新設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.update.enabled	INT	0	Scheduled Update オプションを有効化 (1) または無効化 (0) します。
proxy.config.update.force	INT	0	Force Immediate Update（直ちに更新を強制）を有効化 (1) または無効化 (0) します。有効にした場合、Content Gateway はすべてのスケジュール設定した更新のエントリを上書きし、、このオプションが無効にされるまで、更新を開始し続けます。
proxy.config.update.retry_count	INT	10	失敗した場合に、URL のスケジュール設定した更新を再試行する回数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.update.retry_interval	INT	2	失敗した場合に、URL のスケジュール設定した各更新の再試行の間隔を秒単位で指定します。
proxy.config.update.concurrent_updates	INT	100	許容する同時更新要求の最大数を指定します。このオプションは、スケジュール設定した更新が、ホストに過大な負荷をかけることを防止します。

SNMP の設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.snmp.master_agent_enabled	INT	0	
proxy.config.snmp_encap_enabled	INT	0	

プラグイン設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.plugin.plugin_dir	STRING	config/plugins	プラグインの位置するディレクトリを指定します。

WCCP の設定

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.wccp.enabled	INT	0	WCCP を有効化 (1) または無効化 (0) します。

FIPS（セキュリティ設定）

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.fips.security_enabled	INT	0	v7.5.3 FIPS から v7.7 へのカスタマー アップグレードの FIPS 設定を保存します。
proxy.config.fips.security_enabled_ui	INT	0	v7.5.3 FIPS から v7.7 へのカスタマー アップグレードの FIPS UI 設定を保存します。

SSL 復号化

Help | Content Gateway | バージョン 7.8.x

重要

すべての SSL 復号化の設定は、Content Gateway マネージャr 内で行う必要があります。下記の表内の変数を、records.config 内で直接編集してはいけません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.enabled	INT	1	有効化 (1) すると、Content Gateway はオリジン サーバーとの接続を確立する前に、SSL 接続を受け入れ、URL フィルタリングを実行します。 SSL 復号化を有効化するには、**proxy.config.ssl_decryption.use_decryption** を参照してください。
proxy.config.ssl_decryption.use_decryption	INT	0	有効化 (1) すると、Content Gateway は SSL トラフィックを受け入れ、復号化します。*暗号化データの使用*、159 ページを参照してください。
proxy.config.ssl_decryption_ports	INT	443	HTTPS ポートを指定します。Content Gateway は指定されたポートにのみ SSL 復号化およびポリシー ルックアップを許可します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl_server_port	INT	8080	Content Gateway が クライアント SSL トラフィックを受信待機するポート。
proxy.config.administrator_id	STRING	NULL	変更しないでください。 暗号化された管理者 ID を保持します。
proxy.config.ssl_decryption.tunnel_skype	INT	0	有効化 (1) すると、Content Gateway は Skype トラフィックを識別し、トンネリングします（明示的プロキシ環境のみ）。ユーザー ポリシーを適切に調整する必要があります。設定情報は、*SSL サポートの有効化、163 ページ*を参照してください。
proxy.config.ssl_decryption.tunnel_unknown_protocols	INT	0	SSL ポートを使用する未知のプロトコルのトンネリングを有効化 (1) または無効化します。
proxy.config.ssl_decryption.tunnel_unknown_protocols_timeout	INT	10	Content Gateway が [client hello] 応答を待つ時間を秒単位で指定します。この時間を過ぎると、要求は未知のプロトコルとしてトンネリングされます。
proxy.config.ssl.server.SSLv2	INT	0	有効化 (1) すると、Content Gateway は クライアントからの SSLv2 接続を受け入れます（この場合、[サーバー] は、クライアントへのサーバーとしての Content Gateway のロールを指します）。
proxy.config.ssl.server.SSLv3	INT	1	有効化 (1) すると、Content Gateway は クライアントからの SSLv3 接続を受け入れます（この場合、[サーバー] は、クライアントへのサーバーとしての Content Gateway のロールを指します）。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.server.TLSv1	INT	1	有効化 (1) すると、Content Gateway は クライアントからの TLSv1 接続を受け入れます（この場合、[サーバー] は、クライアントへのサーバーとしての Content Gateway のロールを指します）。
proxy.config.ssl.server.TLSv11	INT	1	有効化 (1) すると、Content Gateway は クライアントからの TLSv1.1 接続を受け入れます（この場合、[サーバー] は、クライアントへのサーバーとしての Content Gateway のロールを指します）。
proxy.config.ssl.server.TLSv12	INT	1	有効化 (1) すると、Content Gateway は クライアントからの TLSv1.2 接続を受け入れます（この場合、[サーバー] は、クライアントへのサーバーとしての Content Gateway のロールを指します）。
proxy.config.ssl.client.SSLv2	INT	0	有効化 (1) すると、Content Gateway は オリジン サーバーからの SSLv2 接続を受け入れます（この場合、[クライアント] は、オリジン サーバーへのクライアントとしての Content Gateway のロールを指します）。
proxy.config.ssl.client.SSLv3	INT	1	有効化 (1) すると、Content Gateway は オリジン サーバーからの SSLv3 接続を受け入れます（この場合、[クライアント] は、オリジン サーバーへのクライアントとしての Content Gateway のロールを指します）。
proxy.config.ssl.client.TLSv1	INT	1	有効化 (1) すると、Content Gateway は オリジン サーバーからの TLSv1 接続を受け入れます（この場合、[クライアント] は、オリジン サーバーへのクライアントとしての Content Gateway のロールを指します）。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.client.TLSv11	INT	1	有効化 (1) すると、Content Gateway は オリジン サーバーからの TLSv1.1 接続を受け入れます（この場合、[クライアント] は、オリジン サーバーへのクライアントとしての Content Gateway のロールを指します）。
proxy.config.ssl.client.TLSv12	INT	1	有効化 (1) すると、Content Gateway は オリジン サーバーからの TLSv1.2 接続を受け入れます（この場合、[クライアント] は、オリジン サーバーへのクライアントとしての Content Gateway のロールを指します）。
proxy.config.ssl.server.cipherlist_option	STRING	Default	クライアントからプロキシへの暗号の設定を指定します。下記のいずれかの値です。 Default High Medium Low *インバウンド トラフィックの場合の SSL 構成の設定、178 ページ*を参照してください。
proxy.config.ssl.server.cipherlist	STRING	ALL:!ADH:@STRENGTH:!EXP	cipher_list オプション設定値に対応する暗号リスト。
proxy.config.ssl.client.cipherlist_option	STRING	Default	暗号リストの設定を指定します。下記のいずれかの値です。 Default High Medium Low *アウトバウンド トラフィックの場合の SSL 構成の設定、180 ページ*を参照してください。
proxy.config.ssl.client.cipherlist	STRING	ALL:!ADH:@STRENGTH:!EXP	cipher_list オプション設定値に対応する暗号リスト。前の項目を参照してください。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.server.session_cache	INT	1	SSL サーバー セッション キャッシュを有効化 (1) または無効化します。
proxy.config.ssl.server.session_cache_timeout	INT	300	SSL サーバー セッション キャッシュ タイムアウト時間を指定します。デフォルトは 300 秒（5 分）です。
proxy.config.ssl.client.session_cache	INT	1	SSL クライアント セッション キャッシュを有効化 (1) または無効化します。
proxy.config.ssl.client.session_cache_timeout	INT	300	SSL クライアント セッション キャッシュ タイムアウト時間を指定します。デフォルトは 300 秒（5 分）です。
proxy.config.ssl.client.certification_level	INT	0	クライアント証明書が不要か、任意か、必須かを指定します。証明書レベルは下記のいずれかです。 0 = クライアント証明書は不要 1 = クライアント証明書は任意 2 = クライアント証明書は必須
proxy.config.ssl.server.cert.filename	STRING	server.crt.pem	サーバー証明書ファイルの名前を指定します。
proxy.config.ssl.server.private_key.filename	STRING	Domainkey.pem	サーバー証明書のプライベート キーを指定します。
proxy.config.ssl.server.private_key.path	STRING	/config	サーバー証明書のプライベート キー パスを指定します。
proxy.config.ssl.CA.cert.filename	STRING	NULL	Content Gateway がクライアントから受け入れる CA のリストを含むファイルの名前を指定します。 接続がクライアントから Content Gateway への接続であり、proxy.config.ssl.client.certification_level の値が 1 または 2 である場合、Content Gateway は CA リストをクライアントに送信します。
proxy.config.ssl.CA.cert.path	STRING	NULL	CA リストのファイルへのパスを指定します。前の項目を参照してください。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.client.cert.policy	INT	1	SSL 証明書のインシデントに対して、インシデントをトンネリングする (0)、または要求をブロックしてインシデント リストにエントリを作成する (1) を指定します。
proxy.config.ssl.client.verify.server	INT	0	Certificate Verification Engine (CVE) を有効化 (1) または無効化 (0) します。*証明書の検証*、182 ページを参照してください。
proxy.config.ssl.cert.verify.denycnmismatch	INT	1	CVE チェック：[Deny certificates where the common name does not match the URL（共通名が URL と一致しない場合に証明書を拒否する）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.allowcnwild	INT	1	CVE チェック：[Allow wildcard certificates（ワイルドカードの証明書を許可）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.denyexpired INT 1	INT	1	CVE チェック：[No expired or not yet valid certificates（期限切れまたはまだ有効でない証明書なし）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.certchain	INT	1	CVE チェック：[Verify entire certificate chain（証明書チェーン全体を検証）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.cert.verify.checkcrl	INT	1	CVE チェック：[Check certificate revocation by CRL（CRL による証明書取り消しをチェック）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.checkocsp	INT	0	CVE チェック：[Check certificate revocation by OCSP（OCSP による証明書取り消しをチェック）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.blockunknownocsp	INT	0	CVE チェック：[Block certificates with Unknown OCSP state（未知の OCSP 状態がある証明書をブロック）] を有効化 (1) または無効化します。 この設定は、CVE が有効化されている場合のみ適用します。
proxy.config.ssl.cert.verify.denymd5cert	INT	0	MD5 署名を使用する証明書の拒否を有効化 (1) します。
proxy.config.ssl.cert.verify.revprefer	INT	1	証明書取り消しチェックのために優先的に使用する方法を指定します。 1 = CRL 2 = OCSP

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl.cert.verify.blocknouri	INT	0	CVE チェック：[Block certificates with no CRL URI and with no OCSP URI（CRL URI がない証明書、および OCSP URI がない証明書をブロック）] を有効化 (1) または無効化します。
proxy.config.ssl.cert.verify.bypassfail INT 0	INT	0	証明書チェックが失敗した後ユーザーがサイトに進むことを許可する証明書チェック失敗バイパス オプションを有効化 (1) します。
proxy.config.ssl.cert.verify.bypasscache	INT	1	検証タイムアウト キャッシュを有効化 (1) します。
proxy.config.ssl.cert.verify.bypasscachetimeout	INT	6	検証バイパス キャッシュに入れられているエントリがタイムアウトになってパージされるまでの時間を秒単位で指定します。

ICAP

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.icap.enabled	INT	0	Websense Data Security Suite (DSS) の ICAP サポートを有効化 (1) または無効化 (0) します。*Websense Data Security の使用*、147 ページを参照してください。

設定変数	データタイプ	デフォルト値	説明

proxy.config.icap.ICAPUri	STRING	NULL	ICAP サービスの Uniform Resource Identifier を指定します。
			カンマ区切り形式のリストでバックアップ サーバーを指定できます。
			DSS 管理者から識別子を取得します。URI を下記の形式で入力します。
			`icap://hostname:port/path`
			*hostname*には、DSS Protector の IP アドレスまたはホスト名を入力します。
			デフォルトの ICAP ポートは 1344 です。
			Path は、ホスト コンピュータ上の ICAP サービスのパスです。
			例：
			`icap://ICAP_machine:1344/opt/icap_services`
			デフォルトの ICAP ポート 1344 を使用している場合はポートを指定する必要はありません。

proxy.config.icap.FailOpen	INT	1	設定： • 1 は、ICAP サーバーがダウンした場合 トラフィックを許可します。 • 0 は、ICAP サーバーがダウンした場合 ブロック ページを送信します。
proxy.config.icap.BlockHugeContent	INT	0	設定： • 0 に設定すると、送信されたファイルが Data Security Suite で指定されたサイズ制限より大きい場合にブロック ページを送信します。DSS のデフォルトのサイズ制限は 12 MB です。 • 1 に設定するとトラフィックを許可します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.icap. AnalyzeSecureContent	INT	1	設定： • 復号化されたトラフィックを宛先に直接に送信する場合、0 を指定します。 • 復号化されトラフィックを分析のために Websense Data Security に送信する場合、1 を指定します。
proxy.config.icap. AnalyzeFTP	INT	1	有効化 (1) すると、ネイティブな FTP アップロード ファイル転送を分析のために ICAP サーバーに送信します。
proxy.config.icap. ActiveTimeout	INT	5	読み込み / 応答タイムアウト（秒単位）。タイムアウトを超過した場合、アクティビティは失敗と見なされます。
proxy.config.icap. RetryTime	INT	5	停止したサーバーが復旧したかどうかをテストするための復旧時間（秒）。
proxy.config.icap. LoadBalance	INT	1	ICAP サーバーが指定されている時、下記のどちらかを設定します： • すべての利用可能なサーバーに要求を配信する場合は 1 に設定 • プライマリ サーバーにだけ要求を配信する場合は、0 に設定。

Data Security

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
proxy.config.dss.enabled	INT	0	コンピュータにインストールされている Data Security のサポートを有効化 (1) または無効化 (0) します。*Websense Data Security の使用*、147 ページを参照してください。
proxy.config.dss. AnalyzeFTP	INT	1	有効化 (1) すると、ネイティブな FTP アップロード ファイル転送を分析のために、コンピュータにインストールされている Data Security ポリシー エンジンに送信します。
proxy.config.dss. AnalyzeSecureContent	INT	1	設定： • 復号化されたトラフィックを宛先に直接に送信する場合、0 を指定します。 • 復号化されトラフィックを分析のために Websense Data Security に送信する場合、1 を指定します。
proxy.config.dss. analysis_timeout	INT	10000	1 つのファイルの分析に使用できる最大時間をミリ秒単位で指定します。この時間を過ぎると、分析は中断します。

接続性、分析、および境界条件

Help | Content Gateway | バージョン 7.8.x

設定変数	データタイプ	デフォルト値	説明
wtg.config.subscription_key	STRING	NULL	Websense Security Gateway または Websense Security Gateway Anywhere のサブスクリプション キーの値を保持します。
wtg.config.download_server_ip	STRING	download.websense.com	Websense ダウンロード サーバーのホスト名または IP アドレスを保持します。
wtg.config.download_server_port	INT	80	Websense ダウンロード サーバーのポート番号を保持します。
wtg.config.policy_server_ip	STRING		Websense Policy Server の IP アドレスを保持します。
wtg.config.policy_server_port	INT	55806	Websense Policy Server のポート番号を保持します。
wtg.config.wse_server_ip	STRING		Websense Filtering Service の IP アドレスを保持します。
wtg.config.wse_server_port	INT	15868	Websense Filtering Service WISP インターフェースのポート番号を保持します。
wtg.config.wse_server_timeout	INT	5000	Filtering Service との通信の最大時間をミリ秒単位で指定します。
wtg.config.ssl_bypassed_categories	STRING	NULL	この変数は、SSL 復号化をバイパスするカテゴリ識別子のリストです。 **この変数の値を変更しないでください**。これは、トラブルシューティングの支援のために含まれまれています。 SSL 復号化をバイパスするカテゴリを指定するためには、Web Security Manager を使用してください。

設定変数	データタイプ	デフォルト値	説明
wtg.config. ssl_decryption_bypass_ ip_based	INT	0	カテゴリー ルックアップ実行時に、SSL カテゴリー バイパス プロセスが、IP アドレス（ホスト名ではなく）のみを使用するよう設定します。 0 = 無効化 1 = 有効化
wtg.config.ssl_fail_open	INT	1	Filtering Service が到達できなくなった場合 SSL サイトを復号化するかどうかを指定します。 0 = 無効化 - Filtering Service が到達できなくなったとき、すべての SSL サイトを復号化します。 1 = 有効化 - Filtering Service が到達できなくなったとき、すべての SSL サイトを復号化**しません**。
wtg.config.fail_open	INT	1	Websense Web フィルタリング（Filtering Service）が利用できない場合、Content Gateway が要求を許可するか、ブロックするかを指定します。 設定： • ブロック ページを送信場合は 0 に設定 • 要求を許可を許可する場合は 1 に設定
wtg.config. fail_open_analytic_scan	INT	1	分析スキャンか機能しなくなった時の、Content Gateway の動作を指定します。 設定： • トラフィックをブロックする場合は 0 に設定 • URLマスターデータベースのルックアップを実行し、ポリシーを適用する場合は 1 に設定 **ご注意：**分析スキャンか機能しなくなった時はいつでも、アラームが発生します。

設定変数	データタイプ	デフォルト値	説明
wtg.config.archive_depth	INT	5	分析がアーカイブ ファイル上で実行される最大の深さを指定します。
wtg.config. max_decompressions	INT	10	アーカイブ ファイルが解凍される最大合計数を指定します（トランザクション単位）。この値は 25 を超えてはいけません。
wtg.config. max_subsamples	INT	10000	トランザクションを分類するために、Content Gateway が解凍し、分析するアーカイブ ファイル内の個別のファイルの最大数を指定します。
wtg.config. zipbomb_action	INT	1	内部で使用。高圧縮ファイル爆弾の分析ステータス。 **この変数の値を変更しないでください。**
wtg.config. max_mem_allowed	INT	1500	消費された時に、Content Gateway が より広範なメモリ モニタリングを実行するメモリの最大数をメガバイト単位で指定します。
wtg.config.lowmem_ behavior	INT	0	スキャンのバイパスを有効化 (1) または無効化 (0) します。ただし、フィルタは実行されます。
wtg.config.lowmem_ timeout	INT	120	メモリ不足管理のタイムアウト値（分単位）。この時間の後、[no management] にリセットされます。
wtg.config.rdnsclients	INT	0	ログ レコード内のクライアントのホスト名を、それぞれに対してリバース DNS を実行することによってログに記録する機能を有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
wtg.config. ip_ranges_not_to_scan	STRING	10.0.0.0- 10.255.255.255, 172.16.0.0- 172.31.255.255, 192.168.0.0- 192.168.255.255	スキャンしない内部 IP アドレスの範囲を指定します。デフォルトでは、このリストは標準のプライベートなルーティング不可の IP アドレスです。各範囲はカンマで区切られ、アドレス範囲はハイフンで結ばれます。 PAC ファイルを使用せずに、スキャンから標準の内部 IP アドレスを除外する明示的プロキシ配備で、これは特に有用です。
wtg.config. scan_ip_ranges	INT	1	wtg.config.ip_ranges_not_to_scan で指定された内部 IP アドレス範囲のバイパスを有効化 (1) または無効化 (0) します。上記を参照。

remap.config

Help | Content Gateway | バージョン 7.8.x

remap.config ファイルには、Websense Content Gateway がオリジン サーバーに接続せずに、HTTP 要求を永久的または一時的にリダイレクトするマッピング ルールが含まれます。

> **重要**
> このファイルを変更した後、プロキシを再起動するか、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で content_line -x を実行することによって変更を適用します。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

remap.config ファイルの各行は、マッピング ルールを含む必要があります。Content Gateway は 3 つのスペース区切りのフィールド（type、target、replacement）を認識します。下記の表は各フィールドのフォーマットについて説明しています。

フィールド	説明
type	下記のどちらかを入力します。 • **redirect** は、オリジン サーバーに接続せずに、永久的に HTTP 要求をリダイレクトします。永久的リダイレクトは、（HTTP ステータス コード 301 を返すことで）URL 変更をブラウザに通知しますので、ブラウザはブックマークを更新できます。 • **redirect_temporary** は、オリジン サーバーに接続せずに、一時的に HTTP 要求をリダイレクトします。一時的リダイレクトは、（HTTP ステータス コード 307 を返すことで）現在の要求のみの URL 変更をブラウザに通知します。 ご注意：**map** および **reverse_map** はサポートされません。
target	転送元 または *from*URL を入力します。4 つまでのコンポーネントを入力できます。 *scheme://host:port/path_prefix* *scheme* は `http`、`https`、または `ftp` です。
strict URL matching flag	要求された URL 全体との正確な一致を求める場合は、**[Match URL Exactly（URL を正確に一致させる）]** を有効化します。 このオプションが有効化されていない場合、URL はターゲットの終わりまで比較されます（**[From Path Prefix]**）。一致がある場合は、リダイレクトが適用されます。この方法では、リダイレクト URL がベース URL を含む場合に不適切なマッチングが行われる場合があります。*Mapping and Redirection（マッピングおよびリダイレクト）、371 ページ*を参照してください。
replacement	転送先 または *to* URL を入力します。4 つまでのコンポーネントを入力できます。 *scheme://host:port/path_prefix* *scheme* は **http**、**https**、または **ftp** に設定できます。

注意

target と replacement のスキーム タイプ（HTTP、HTTPS、FTP）は一致する必要があります。

例

下記のセクションは、**remap.config** ファイルのマッピング ルールの例を示しています。

リダイレクト マッピング ルール

下記のルールは、`www.company.com` からのすべての HTTP 要求を `www.company2.com` に*永久的*にリダイレクトします：

```
redirect http://www.company.com http://www.company2.com
```

下記のルールは、`www.company1.com` からのすべての HTTP 要求を `www.company2.com` に*一時的*にリダイレクトします：

```
redirect_temporary http://www.company1.com http://
www.company2.com
```

socks.config

Help | Content Gateway | バージョン 7.8.x

socks.config ファイルは、下記のサーバーを指定します。

- プロキシが指定のオリジン サーバーにアクセスするために使用する必要がある SOCKS サーバー、およびプロキシが SOCKS サーバー リストをチェックする順序。
- SOCKS サーバーを*経由せずに*、Content Gateway が直接アクセスするオリジン サーバー。

> **注意**
> すべての SOCKS の設定は、Content Gateway マネージャで行うことを推奨します。

> **重要**
> このファイルを変更したらコンピュータを再起動する必要があります。

手動で設定されたルールに一致しないトラフィックは、デフォルト ルールで処理されます。デフォルト ルールは、**Socks Servers** テーブル内で **default** オプションを有効化することで、各 SOCKS サーバーに設定されます。デフォルト ルールは、自動的に作成され、SOCKS Server ページに表示されます。デフォルト ルールは、**socks.config** ファイルに書き込まれません。宛先 IP アドレスは、[A l l] です。

フォーマット

プロキシが指定のオリジン サーバーに到達するために使用する SOCKS サーバーを指定するために、**socks.config** に下記の形式でルールを追加します。

```
dest_ip=ipaddress socksparent="alias1" [round_robin=value]
```

ここで、

ipaddress は、- または / で区切られたオリジン サーバーの IP アドレスまたは IP アドレスの範囲です。

alias1 は、**SOCKS Servers** リストで命名された SOCKS サーバーの別名です。

value は、Content Gateway が 1 つずつ SOCKS サーバーを試す場合は `strict` を指定します。ラウンド ロビン選択を発生さない場合は、`false` を選択します。

SOCKS サーバーを経由する*ことなしに*、Content Gateway が直接アクセスするオリジン サーバーを指定するためには、**socks.config** に下記の形式のルールを入力します。

```
no_socks ipaddress
```

ここで、*ipaddress* は、Content Gateway が直接アクセスするオリジン サーバーに関連付けられた IP アドレスまたは IP アドレスの範囲のカンマ区切り形式のリストです。下記のすべてのネットワーク ブロードキャスト アドレスを指定してはいけません。255.255.255.255.

> **注意**
>
> **socks.config** の各ルールは 最大 400 文字で構成されます。**socks.config** ファイル内のルールの順序は重要ではありません。

例

下記の例は、SOCKS サーバーの別名 [alias1] および [alias2] を経由して、IP アドレスの範囲 123.15.17.1 - 123.14.17.4 のオリジン サーバーに要求を送信するようにプロキシを設定します。オプション指定子 **round_robin** が **strict** に設定されているために、プロキシは、最初の要求を alias1 に送信し、2 番目の要求を alias2 に送信し、3 番目の要求を alias1 に送信します。

```
dest_ip=123.14.15.1 - 123.14.17.4
socksparent="alias; alias2" round_robin=strict
```

下記の例は、SOCKS サーバーを経由*せずに*、IP アドレス 11.11.11.1 のオリジン サーバーに直接アクセスするようにプロキシを設定します。

```
no_socks 11.11.11.1
```

下記の例は、SOCKS サーバーを経由*せずに*、IP アドレスの範囲 123.14.15.1 - 123.14.17.4 と IP アドレス 113.14.18.2 のオリジン サーバーに直接アクセスするように Content Gateway を設定します。

```
no_socks 123.14.15.1 - 123.14.17.4, 113.14.18.2
```

socks_server.config

Help | Content Gateway | バージョン 7.8.x

socks_server.config ファイルは、Content Gateway で利用可能な SOCKS サーバーを指定します。

フォーマット

SOCKS サーバー を指定するために、下記の形式を使用します。

```
alias=name host=IP_address|domain_name port=port_number
[username=user_name password=password] default=true|false
```

ここで、

name は SOCKS サーバーの名前です。

IP_address または *domain_name* は、貴社の DNS サービスで解決できる IP アドレスまたはドメイン名です。

port_number は、SOCKS サーバーがリッスンするポートです。

username および *password* は、SOCKS 5 認証のユーザ名とパスワードのペアです。パスワードは暗号化されます。

指定したサーバーをデフォルト SOCKS サーバーにするためには、default を *true* に設定します。デフォルト サーバー オプションがオンの場合、SOCKS サーバーは SOCKS ルールが一致しない場合に使用されます。

デフォルト サーバーに指定された SOCKS サーバーがない場合、ルールに一致しないトラフィックは、SOCKS サーバーを介してルーティングされません。

例：

この例は、ポート 61080 上の 127.0.0.1 で [default1] SOCKS サーバーを追加します。

```
alias=default1 host=127.0.0.1 port=61080 default=true
```

この例は、認証を使用する SOCKS サーバーを追加します。パスワード [465751475058] は、実際のパスワードではないことに注意してください。これは暗号化されています。

```
alias=test1 host=socks5.example.com port=1080 username=test
password=465751475058 default=false
```

このファイルを修正した場合、Content Gateway を再起動する必要があります。

> **注意**
> **socks_server.config** の各ルールは、400 文字を超えることはできません。

splitdns.config

Help | Content Gateway | バージョン 7.8.x

splitdns.config ファイルを使用して、Content Gateway が指定の条件のもとでホストを解決するために使用する DNS サーバーを指定できます。

DNS サーバーを指定するためには、ファイル内の各有効な行に下記の情報を提供する必要があります。

- 一次宛先指定子（先ドメイン、宛先ホスト、または URL 正規表現形式）。
- サーバー指令のセット（対応するポート番号をもつ 1 つ以上の DSN サーバーのリスト）。

各 DNS サーバーの定義に下記のオプション情報を含めることができます。

- ホスト解決のためのデフォルト ドメイン
- 複数のドメインが指定されている場合のドメイン検索順序を指定した検索リスト

詳細については、*Split DNS オプションの使用*、215 ページを参照してください。

> **重要**
> このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（/opt/WCG/bin）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

splitdns.config ファイルの各行は、下記のどちらかの形式を使用します。

```
dest_domain=dest_domain | dest_host | url_regex
named=dns_server
def_domain=def_domain search_list=search_list
```

下記の表は各フィールドを説明しています。

フィールド	使用できる値
dest_domain	有効なドメイン名。これは、宛先ドメインに基づく DNS サーバー選択を指定します。NOT 論理演算子を表す感嘆符（!）をドメインの前に付けることができます。
dest_host	有効なホスト名。これは、宛先ホストに基づく DNS サーバー選択を指定します。NOT 論理演算子を表す感嘆符（!）をホストの前に付けることができます。
url_regex	有効な URL 正規表現。これは、正規表現に基づく DNS サーバー選択を指定します。
dns_server	これは必須の指令です。これは、Content Gateway が宛先指定子に対して使用する DNS サーバーを識別します。コロン（:）を使用してポートを指定できます。指定しない場合、53 が使用されます。スペースまたはセミコロン（;）で区切ることで、複数の DSN サーバーを指定できます。 ドット表記の IP アドレスを使用して、ドメインを指定する必要があります。
def_domain	有効なドメイン名。このオプションの指令は、ホスト解決に使用するデフォルト ドメイン名を指定します。1 つのエントリのみ入力できます。デフォルト ドメインを提供しない場合、システムは **/etc/resolv.conf** からその値を決定します。
search_list	スペースまたはセミコロン（;）で区切られたドメインのリスト。これは、ドメイン検索の順序を指定します。検索リストを提供しない場合、システムは **/etc/resolv.conf** からその値を決定します。

例

下記の DNS サーバー選択定義を検討します。

```
dest_domain=internal.company.com named=255.255.255.255:212
255.255.255.254 def_domain=company.com
search_list=company.com company1.com
dest_domain=!internal.company.com named=255.255.255.253
```

下記の 2 つの要求について検討します。

- `http://minstar.internal.company.com`

  この要求は、最初の行にマッチし、255.255.255.255 ポート 212 の DNS サーバーを選択します。すべての解決要求は、デフォルト ドメインとして **company.com** を使用し、最初に検索するドメインのセットとして、**company.com** および **company1.com** を使用します。

- `http://www.microsoft.com`

  この要求は、2 番目の行にマッチします。従って、Content Gateway は、DNS サーバー 255.255.255.253 を選択します。**def_domain** または **search_list** が提供されなかった場合、Content Gateway は この情報を **/etc/resolv.conf** から取得します。

storage.config

Help | Content Gateway | バージョン 7.8.x

storage.config ファイルは、キャッシュを構成するすべてのファイル、ディレクトリ、または ハードディスク パーティションをリストします。

> **重要**
> このファイルを変更したらコンピュータを再起動する必要があります。

フォーマット

storage.config ファイルの形式は下記のとおりです。

```
pathname size
```

ここで、*pathname* は、パーティション、ディレクトリ、またはファイルの名前で、*size* は、名前の付けられたパーティション、ディレクトリ、またはファイルのバイト単位のサイズです。ディレクトリまたはファイルのサイスを指定する必要があります。Raw パーティションの場合、サイズ指定はオプションです。

あらゆるサイズのすべてのパーティションを使用できます。最高のパフォーマンスを得るために、下記のガイドラインを推奨します。

- Raw ディスク パーティションを使用する。
- 各ディスクで、すべてのパーティションを同じサイズにする。
- 各ノードで、すべてのディスク上の同じパーティション番号を使用する。

オペレーティングシステム要件に従って、パス名を指定する。下記の例を参照してください。

> **重要**
> **storage.config** ファイルで、フォーマット済み または Raw ディスクは、少なくとも 2 GB 必要です。推奨されるディスク キャッシュ サイズは、147 GB です。

update.config

Help | Content Gateway | バージョン 7.8.x

update.config ファイルは、Websense Content Gateway が 指定のローカル キャッシュ コンテンツの更新のスケジュールを実行する方法を制御します。ファイルには、更新をスケジュールしたいオブジェクトを指定した URL のリストが含まれます。

スケジュール設定した更新は、指定した時刻または間隔で、オブジェクトのローカル HTTP `GET` を実行します。各オブジェクトに対して下記のパラメータを制御できます。

- URL
- URL 指定要求ヘッダー（デフォルトを上書き）
- 更新時刻および間隔
- 再帰の深さ

> **重要**
> このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ（**/opt/WCG/bin**）で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

再帰的 URL 更新実行時に、スケジュール設定した更新は 下記のタグ / 属性のペアをサポートしています。

- <a href=“ ” >
- <img src=“ ” >
- <img href=“ ” >
- <body background=“ ” >

- <frame src=“ ” >
- <iframe src=“ ” >
- <fig src=“ ” >
- <overlay src=“ ” >
- <applet code=“ ” >
- <script src=“ ” >
- <embed src=“ ” >
- <bgsound src=“ ” >
- <area href=“ ” >
- <base href=“ ” >
- <meta content=“ ” >

スケジュール設定した更新は、数百の URL 入力からなる URL セットで動作するよう設計されています（再帰的 URL が含まれる場合は数千に拡張されます）。これは、インターネット クローラで使用されるのものような大規模な URL セットでの動作を意図したものでは*ありません*。

フォーマット

`update.config` ファイルの各行は、下記の形式を使用します。

URL`\`*request_headers*`\`*offset_hour*`\`*interval*`\`*recursion_depth*`\`

下記の表は各フィールドを説明しています。

フィールド	使用できる入力値
URL	HTTP および FTP ベースの URL。
request_headers	（*オプション*）。各 GET 要求で渡されたヘッダー（セミコロンで区切り）のリスト。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。デフォルトでは要求ヘッダーはありません。
offset_hour	更新時間を導出するために使用する基準時間。範囲は 00-23 時です。
interval	更新が行われる（オフセット時間からの）間隔（秒）。
recursion_depth	参照されている URL が再帰的に更新される（指定した URL からの）深さ。

例

下記の例は HTTP のスケジュール設定した更新を示します。

```
http://www.company.com\User-Agent:noname user
agent\13\3600\5\
```

この例では、URL と要求ヘッダー、オフセット時間 13（午後 1 時）、1 時間の間隔、再帰の深さ 5 を指定しています。 1 日に 1 回だけ更新するようにスケジュールするためには、間隔の値に 24 時間 x 60 分 x 60 秒 = 86400 を使用します。

下記の例は FTP のスケジュール設定した更新を示しています。

```
ftp://anonymous@ftp.company.com/pub/misc/
test_file.cc\\18\120\0\
```

この例は、FTP 要求、オフセット時間 18（午後 6 時）、2 分毎の間隔を指定しています。ユーザーは *anonymous* で、パスワードは **records.config** ファイルの *proxy.config.http.ftp.anonymous_passwd* 変数に指定する必要があります。

wccp.config

Help | Content Gateway | バージョン 7.8.x

wccp.config ファイルは、WCCP 設定情報とサービス グループの設定を保存します。**[Configure] > [MyProxy] > [Basic]** ページで WCCP を有効化した場合、WCC P サービス グループ設定は **[Configure] > [Networking] > [WCCP]** ページで設定できます。WCCP が Content Gatewa y への透過的なリダイレクトのために使用される場合、サービス グループを定義する必要があります。詳細については、*WCCP v2 デバイスによる透過的遮断、65 ページ*を参照してください。

F エラー メッセージ

Websense Content Gateway のエラー メッセージ

下の表は、システム ログ ファイルに表示されることがあるメッセージをリストしています。このリストは完全なリストではありません。発生する可能性があり、注意が必要となることがある警告メッセージを示しています。下記のリストに含まれていない警告メッセージの詳細については、www.websense.com にアクセスし、[Support & Knowledge Base] に移動してください。

処理の致命的エラー

メッセージ	説明
Accept port is not between 1 and 65535. Please check configuration.	records.config ファイルで指定されている着信 HTTP 要求を受け入れるポートは無効です。
Ftp accept port is not between 1 and 65535.	records.config ファイルで指定されている着信 FTP 要求を受け入れるポートは無効です。
Self loop is detected in parent proxy configuration.	親プロキシの名前およびポートが Content Gateway の名前およびポートと同じです。そのため、Content Gateway が親プロキシに要求を送信しようとした時、ループが作成されます。
Could not open the ARM device	ARM をロードできませんでした。この最もよくある理由は、ホスト システムのシステム カーネルの適合性の問題です。 ARM がロードされたかどうか確認するには、下記のコマンドを実行します。 /sbin/lsmod | grep arm

メッセージ	説明
content_manager failed to set cluster IP address	content_manager プロセスがクラスタ IP アドレスを設定できませんでした。クラスタ IP アドレスを確認してください。この IP アドレスがネットワーク内の他のデバイスによって使用されていないことを確認してください。
Unable to initialize storage. (Re) Configuration required.	起動中にキャッシュ初期化に失敗しました。キャッシュ構成をチェックし、構成または再構成する必要があります。

警告

メッセージ	説明
Logfile error:*error_number*	一般的なログ記録エラー。
Bad cluster major version range *version1-version2* for node *IP address* connect failed	互換性のないソフトウェア バージョンが問題を起こしています。
can't open config file *filename* for reading custom formats	カスタムログ記録は有効化されていますが、Content Gateway が **logs.config** ファイルを見つけることができません。
connect by disallowed client *IP address*, closing connection	指定されたクライアントは、Content Gateway への接続を許可されていません。そのクライアント IP アドレスは **ip_allow.config** ファイルにリストされていません。
Could not rename log *filename* to *rolled filename*	取り出し中にログ ファイルの名前を変更した時のシステム エラー。
Did *this_amount* of backup still to do *remaining_amount*	混雑にさしかかっています。
Different clustering minor versions *version 1, version 2* for node *IP address* continuing	互換性のないソフトウェア バージョンが問題を起こしています。
log format symbol *symbol_name* not found	カスタム ログ フォーマットが存在していないフィールド シンボルを参照しています。*イベント ログ記録のフォーマット、433 ページ*を参照してください。
missing field for field marker	ログ バッファの読み取りエラーが発生しました。
Unable to accept cluster connections on port:*cluster_port_number*	Websense テクニカル サポート にお問い合わせください。テクニカル サポートの連絡先については、www.websense.com/support/ を参照してください。

メッセージ	説明
Unable to open log file *filename*, errno=*error_number*	ログ ファイルを開くことができません。
Error accessing disk *disk_name*	Content Gateway がキャッシュ読み取り問題を起こした可能性があります。ディスクを交換する必要があることもあります。
Too many errors accessing disk *disk_name:*declaring disk bad	Content Gateway は、エラーがあまりに多く発生したので、キャッシュ ディスクを使用できません。ディスクが破損している可能性があり、交換する必要がある場合があります。
No cache disks specified in **storage.config** file:cache disabled	Content Gateway **storage.config** ファイルにどのキャッシュ ディスクもリストされていません。Content Gateway はプロキシ専用モードで実行しています。**storage.config** ファイルへのキャッシュに使用するディスクを追加する必要があります（*storage.config*、559 ページを参照）。
All disks are bad, cache disabled	キャッシュ ディスクに問題があり、キャッシングが無効化されています。キャッシュ ディスクが稼働していて、キャッシングのために適切にフォーマッティングされていることを確認してください。*キャッシュの構成*、113 ページを参照してください。
Missing DC parameter <missing_param> on auth.profile line	必須のパラメータが指定されていません。欠落しているパラメータの値を入力してください。
Bad DC parameter <bad_param> - <dc_name>	指定されている Domain Controller パラメータが無効です。上記のパラメータの有効な値を入力してください。
[ParentSelection] <error_description> for default parent proxy	子プロキシでの親プロキシの誤った構成のためにプロキシ チェーンが機能していません。子プロキシでの親プロキシの値のチェーン構成を確認してください。
WCCP2:Cannot find Interface name.Please check that the variable proxy.local.wccp2. ethernet_interface is set correctly	WCCP インターフェースの値が指定されていません。Content Gateway マネージャで、**[Configure] > [Networking] > [WCCP] > [General]** を順に選択してチェックするか、または **records.config** の proxy.local.wccp2.ethernet_interface に値を割り当てます。
ARMManager:Unable to read network interface configuration	**ipnat.conf** にフォーマットまたは設定エラーがあります。Content Gateway マネージャで、**[Configure] > [Networking] > [AEM] > [General]** を順に選択し、**[Edit File（ファイルを編集）]** をクリックして **ipnat.conf** を表示し訂正してください。

アラーム メッセージ

Help | Content Gateway | バージョン 7.8.x

下記の表は、Content Gateway マネージャで表示されることがあるアラーム メッセージを示しています。

メッセージ	説明 / ソリューション
The Content Gateway subscription has expired.	最寄りの Websense 顧客サービス代理店またはテクニカル サポートまでご連絡ください。
Content Gateway subscription download failed.	Content Gateway がサブスクリプション情報を確認するためダウンロード サーバーに接続することができませんでした。ダウンロード サーバーへの接続を確認してください。
After several attempts, Content Gateway failed to connect to the Websense Database Download Service.Please troubleshoot the connection.	Content Gateway がインターネットにアクセスできることを確認します。ファイアウォールおよびアップストリーム プロキシ サーバーの設定によって Content Gateway がダウロード サーバーに接続できない可能性がないか確認してください。
After several attempts, Content Gateway failed to connect to the Policy Server.Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Policy Server サービスが Web Security ホストで実行していることを確認してください、
After several attempts, Content Gateway failed to connect to the Policy Broker.Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Policy Broker サービスが Web Security ホストで実行していることを確認してください。
After several attempts, Content Gateway failed to connect to the Filter service.Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Filter Service 処理が Web Security ホストで実行していることを確認してください、
Communication with the analytics engine has failed.Content Gateway を再起動してください。	Content Gateway を再起動してください。

メッセージ	説明 / ソリューション
SSL decryption has been disabled due to an internal error, please restart Content Gateway.	SSL Support で致命的エラーが検出されました。Content Gateway を再起動してください。
[Rollback::Rollback] Config file is read-only:*filename*	Content Gateway の **config** ディレクトリ（デフォルトの場所は **/opt/WCG/config**）に移動し、指定されたファイルのアクセス権を確認し、必要な場合それらを変更してください。
[Rollback::Rollback] Unable to read or write config file *filename*	Content Gateway の **config** ディレクトリに移動し、指定されたファイルが存在しているを確認してください。そのファイルのアクセス権をチェックし、必要な場合はそれらを変更してください。
[Content Gateway Manager] Configuration File Update Failed *error_number*	Content Gateway の **config** ディレクトリに移動し、指定されたファイルのアクセス権を確認し、必要な場合はそれらを変更してください。
Access logging suspended - configured space allocation exhausted.	イベント ログ ファイルに割り当てられたファイル空間がいっぱいになりました。アクセスのログ記録を継続できるようにするには、空間を大きくするか、または一部のログ ファイルを削除する必要があります。これが起こるのを防ぐために、ログ ファイルの取り込みをより頻繁にし、自動削除機能を有効化することを検討してください。*イベント ログ ファイルの取り込み、284 ページ*を参照してください。
Access logging suspended - no more space on the logging partition.	イベント ログを含んでいるパーティション全体がいっぱいになりました。引き続きログ機能にアクセスするために、一部のログ ファイルを削除するか、移動してください。これが起こるのを防ぐために、ログ ファイルの取り込みをより頻繁にし、自動削除機能を有効化することを検討してください。*イベント ログ ファイルの取り込み、284 ページ*を参照してください。
Created zero length place holder for config file *filename*	Content Gateway の **config** ディレクトリに移動し、指定されたファイルを確認してください。その長さがまったくゼロである場合は、設定ファイルのバックアップ コピーを使用してください。
Content Gateway can't open *filename* for reading custom formats	**records.config** の変数 *proxy.config.log2.config_file* がカスタム ログ ファイル（デフォルトでは **logging/logs.config**）への正しいパスを含んでいることを確認してください。

メッセージ	説明 / ソリューション
Content Gateway could not open logfile *filename*	指定したファイルおよびログ記録ディレクトリのアクセス権を確認してください。
Content Gateway failed to parse line *line_number* of the logging config file *filename*	カスタム ログ設定ファイルを確認してください。構文エラーの可能性があります。正しいカスタム ログ フォーマットのフィールドについては、*カスタム ログ記録フィールド*、433 ページを参照してください。
vip_config binary is not setuid root, manager will be unable to enable virtual ip addresses	**content_manager** 処理が仮想 IP アドレスを設定できませんでした。Content Gateway の **bin** ディレクトリで **vip_config** のルートを設定する必要があります。
Content Gateway cannot parse the ICAP URI.Please ensure that the URI is entered correctly in Content Gateway Manager or in the *proxy.config.icap.ICAPUri* configuration variable.	Universal Resource Identifier（URI）が正しい形式ではありません。下記のとおり URI を入力してください。 `icap://hostname:port/path` URI の形式の詳細については、*Websense Data Security の使用*、147 ページを参照してください。
The specified ICAP server does not have a DNS entry.Please ensure that a valid DSS hostname is entered correctly in Content Gateway Manager or in the *proxy.config.icap.ICAPUri* configuration variable.	**records.config** ファイルのホスト名が DNS のどのエントリとも一致しません。有効な Websense Data Security Suite サーバーの名前が Content Gateway マネージャに正しく入力されていることを確認してください。 URI の形式の詳細については、*Websense Data Security の使用*、147 ページを参照してください。
Content Gateway is not able to communicate with the DSS server.Please try again.	Websense Data Security Suite が起動し実行していること、および変数 *proxy.config.icap.ICAPUri* で指定されているポートへの接続を受け入れることを確認してください。このメッセージが持続する場合は、Websense Data Security Suite 管理者に連絡してください。
Domain controller *domain_controller_name:port* is down.	指定された NTLM ドメイン コントローラが要求に応答せず、機能停止とマーク付けされています。ドメイン コントローラのステースを調べてください。

メッセージ	説明 / ソリューション
Windows domain [domain name] unreachable or bad membership status	このアラームは以下のどちらかを表すことがあります。 1.Active Directory が到達できない。AD サーバーが停止しているか、またはネットワーク接続の問題があります。 2.AD は到達できるが、Content Gateway との通信を妨げる設定問題がある。たとえば、AD が複数のサイトに設定されており、Content Gateway が置かれているサブネットがそれらのサイトのいずれかに追加されている場合にアラームが生成されます。

クライアントに送信される HTML メッセージ

Help | Content Gateway | バージョン 7.8.x

Websense Content Gateway は、ブラウザによって要求されたトランザクションで問題が発生した場合、ブラウザのクライアントに詳細なエラー メッセージを返します。これらの応答メッセージは、標準の HTTP 応答コードに対応しますが、より多くの情報を提供します。非常に頻繁に表示される HTTP 応答コードは、*標準 HTTP 応答メッセージ、572 ページ* に示しています。応答メッセージをカスタマイズできます。

下記の表は、Content Gateway のハード コード化された HTTP メッセージ、それらに対応する HTTP 応答コード、およびそれらに対応するカスタマイズ可能なファイルを示しています。

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Access Denied	403	場所 *URL* のドキュメントへのアクセスが許可されていません。	access#denied
Bad HTTP request for FTP Object	400	FTP オブジェクトの HTTTP 要求が不適切です。	ftp#bad_request
Cache Read Error	500	キャッシュからの読み取り中のエラー。要求を再度実行してください。	cache#read_error
Connection Timed Out	504	サーバーが長時間に渡りデーターを送信していませんでした。	timeout#inactivity
Content Length Required	400	Content-Length が指定されていなかったために、この要求は処理できませんでした。	request#no_content_length

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Cycle Detected	400	要求は HTTP プロキシ サイクルの原因となる可能性があるため禁止されました。	request#cycle_detected
禁止	403	*port_number* は、SSL 接続の許可されたポートではありません （禁止されたポート番号へのセキュアな SSL 接続の要求を行いました）。	access#ssl_forbidden
FTP Authentication Required	401	要求した FTP ドキュメント *URL* にアクセスするために、正しいユーザー名およびパスワードを指定する必要があります。	ftp#auth_required
FTP Connection Failed	502	サーバー *server_name* に接続できませんでした。	connect#failed_connect
FTP Error	502	FTP サーバー *server_name* がエラーを返しました。ドキュメント *URL* へのアクセス要求が失敗しました。	ftp#error
Host Header Required	400	要求を透過的にプロキシ処理する試みが行われましたが、この試みは、ブラウザが HTTP `Host` ヘッダーを送信していなかったために失敗しました。HTTP プロキシとして `https://` *proxy_name:proxy_port* を使用するように手動でブラウザを設定します。詳細についてはご使用のブラウザのマニュアルを参照してください。 代わりに、エンド ユーザーは HTTP `Host` ヘッダー フィールドをサポートするブラウザにアップグレードできます。	interception#no_host
Host Header Required	400	ブラウザが `Host` HTTP ヘッダー フィールドを送信していませんでした。そのため要求される仮想ホストを判別できませんでした。この Web サイトに正しくアクセスするために、HTTP `Host` ヘッダー フィールドをサポートするブラウザにアップグレードする必要があります。	request#no_host

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
HTTP Version Not Supported	505	オリジン サーバー *server_name* は、HTTP プロトコルのサポートされていないバージョンを使用しています。	response#bad_version
Invalid HTTP Request	400	この *client_request* HTTP 方式での *URL* へのアクセス要求を処理できませんでした。	request#syntax_error
Invalid HTTP Response	502	ホスト *server_name* がドキュメントの *URL* を正しく返しませんでした。	response#bad_response
Malformed Server Response	502	ホスト *server_name* がドキュメントの *URL* を正しく返しませんでした。	response#bad_response
Malformed Server Response Status	502	ホスト *server_name* がドキュメントの *URL* を正しく返しませんでした。	response#bad_response
Maximum Transaction Time exceeded	504	ドキュメントの *URL* の送信に時間がかかりすぎです。	timeout#activity
No Response Header From Server	502	ホスト *server_name* がドキュメントの *URL* を正しく返しませんでした。	response#bad_response
Not Cached	504	このドキュメントはキャッシュにはなく、また、クライアントはキャッシュされたコピーのみを受け入れます。	cache#not_in_cache
Not Found on Accelerator	404	ホスト *server_name* 上で *URL* が検出されませんでした。場所を確認し、再度実行してください。	urlrouting#no_mapping
NULL	502	ホスト *hostname* がドキュメントの *URL* を返しませんでした。	response#bad_response
Proxy Authentication Required	407	ユーザー名とパスワードを入力してログインしてください。	access#proxy_auth_required
Server Hangup	502	トランザクションが完了する前にサーバー *hostname* が接続を中止しました。	connect#hangup
Temporarily Moved	302	要求したドキュメント *URL* は新しい場所に移動しました。新しい場所は、*new_URL* です。	redirect#moved_temporarily

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Transcoding Not Available	406	ご利用のブラウザによって要求された形式でドキュメント *URL* を提供することはできません。	transcoding#unsupported
Tunnel Connection Failed	502	サーバー *hostname* に接続できませんでした。	connect#failed_connect
Unknown Error	502	ホスト *hostname* がドキュメントの *URL* を返しませんでした。	response#bad_response
Unknown Host	500	*hostname* というサーバーを見つけることができませんでした。サーバーには、DNS エントリがありません。おそらくサーバー名に誤ったつづりがあるか、そのサーバーが存在していないかのどちらかです。名前をダブルクリックして、再度実行してください。	connect#dns_failed
Unsupported URL Scheme	400	プロトコル スキームが未知のためにドキュメント *URL* の要求を実行できません。	request#scheme_unsupported

標準 HTTP 応答メッセージ

Help | Content Gateway | バージョン 7.8.x

下記の標準 HTTP 応答メッセージは情報を提供します。より完全なリストについては、*Hypertext Transfer Protocol ? HTTP/1.1 Specification* を参照してください。

メッセージ	説明
200	OK
202	受け入れられた
204	コンテンツなし
206	部分的コンテンツ
300	複数の選択肢
301	永久に移動させられた
302	検出された
303	他を参照
304	変更されていない
400	不適切な要求

メッセージ	説明
401	無許可：再度実行
403	禁止
404	見つからない
405	メソッドが許可されていない
406	許容できない
408	要求の時間切れ
500	内部サーバー エラー
501	適用されない
502	不良の Gateway
504	Gateway タイムアウト

G Copyrights

ヘルプ | Content Gateway | バージョン 7.8.x

Websense® Content Gateway オンライン ヘルプ

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

発行２１３, ２０１４
アメリカ合衆国にて印刷
R250913781

Websense Content Gateway の一部には、ライセンス契約に基づき使用された第三者の技術が含まれています。注記およびその所有権については、下記に掲載されています。

Websense Content Gateway のいくつかの部分には下記の技術が含まれます。

Boost.Asio

Version 1.47.0

Copyright (c) 2003-2012

Christopher M. Kohlhoff

Boost Software License - Version 1.0 - August 17th, 2003

本ライセンスの対象となるソフトウェアのコピーおよび付属マニュアル（以下、[本ソフトウェア] ）を取得された方に、下記の条件を前提として、無償で、本ソフトウェアを使用、コピー、表示、配布、実行および転送する、および本ソフトウェアの派生物を作成する、また、本ソフトウェアの提供を受けた第三者に上記のことを許可することを許諾します。

本ソフトウェアの著作権に関する注記および本章のすべての記述は、上記のライセンス許諾、本項における制限、および下記の免責事項を含めて、本ソフトウェア（全体またはその一部）のすべてのコピー、および本ソフトウェアのすべての派生物に組み込まれるものとしますが、ただし、そのようなコピーまたは派生物がソース言語プロセッサによって生成されコンピュータ上で使用される実行可能なオブジェクト コードの形式でのみ存在する場合は例外とします。

本ソフトウェアは無保証で提供されており、商品性、特定の用途に対する適合性、所有権、著作権侵害の不存在に関する保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも、著作権所有者または本ソフトウェアの販売者は、本ソフトウェアまたはその使用、もしくはその他の本ソフトウェアの取り扱いに関連して生じた、いかなる損害、またはその他の責任に対しても、それが契約上の行為によるか不正またはその他の行為によるかに関わりなく、責任を負いません。

gperftools

Copyright (c) 1998.

Regents of the University of California

All rights reserved.

以下の条件が満たされている場合は、変更の有無にかかわらず、ソースフォームおよびバイナリーフォームにより再配布および使用を許可します：

* ソース・コードの再配布においては、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が保持されている。

* バイナリ形式による再配布においては、そのマニュアルおよび（または）その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。

* University of California, Berkeley の名称またはそのコントリビューターの名称が、事前の特別の書面による承諾なしに本ソフトウェアから派生した製品の推奨または販売促進のために使用されない。

本ソフトウェアは、著作権保有者およびコントリビューターによって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも、著作権保有者またはコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害（代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない）に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為（過失またはその他）のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

INN

libdb および libtcmalloc

libmagic

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

このソフトウェアは、United States Department of Commerce のいかなる輸出規制の対象でもなく、すべての国または全世界に輸出できます。

以下の条件が満たされている場合は、変更の有無にかかわらず、ソースフォームおよびバイナリーフォームにより再配布および使用を許可します：

1. ソース・コードの再配布においては、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が、ファイルの先頭の直後に記載されている。

2. バイナリ形式による再配布においては、そのマニュアルおよび（または）その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。

本ソフトウェアは、著作者およびコントリビューターによって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも、著作者またはコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害（代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない）に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為（過失またはその他）のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

libregx

Copyright © 1992, 1993, 1994, 1997 Henry Spencer.All rights reserved.

このソフトウェアは、American Telephone and Telegraph Company または Regents of the University of California のすべてのライセンスの対象ではありません。

MRTG

Multi Router Traffic Grapher（MRTG）は、GNU General Public Licenses の条件に基づき無料で利用できます。

Copyright c 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

本プログラムは無償で許諾されたものであるので、準拠法によって許可されている範囲で、本プログラムの保証はありません。別途に書面において記載されていない限り、本プログラムは、著作権保有者および（または）他の当事者によって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。本プログラムの品質およびパフォーマンスに関する全リスクは、お客様が引き受けるものとします。本プログラムに問題が生じた場合、お客様が必要なサービス、修理、または修正のすべての費用を負うものとします。

Netscape Directory SDK 4.0 for C

Netscape Directory SDK 4.0 for C は、Netscape ONE SDK End User License Agreement（Netscape ONE SDK エンド ユーザー ライセンス 契約）に基づき無償で使用できます。

各コンポーネントは、無保証で提供されており、商品性、特定の用途および著作権侵害の不存在に対する適合性を含む（ただしそれに限定されない）明示または暗黙の一切の保証を否認します。コンポーネントの品質およびパフォーマンスに関する全リスクは、お客様の負担になります。コンポーネントが不良または不正確であると判明した場合、事情に応じて、Netscape やその供給業者ではなくお客様がサービスおよび修理の全費用を引き受けることとします。さらに、コンポーネントによって実装されているセキュリティ メカニズム（もしあれば）には固有の制限事項があり、またお客様は各コンポーネントがお客様の要件に十分に対応するものであることを判断する必要があります。この保証の放棄は、本契約の基本的部分を構成しています。一部の司法管轄区域は、暗黙の保証の除外を許可していません。その場合この権利放棄はお客様には適用されず、お客様は他の法律上の権利（司法管轄区域によって異なる）を有する場合があります。

OpenLDAP

OpenLDAP のパブリック・ライセンス

Version 2.8, 17 August 2003

以下の条件が満たされていることを条件に、変更の有無にかかわらず、本ソフトウェアおよび関連マニュアル（以下 [本ソフトウェア] ）の再配布および使用を許可します：

1. ソース・コードの形式の再配布においては、著作権に関する記述および注記が保持されている。

2. バイナリ形式による再配布においては、そのマニュアルおよび（または）その他の添付される資料に、著作権に関する記述および注記、この条件のリスト、および以下の免責事項が記載されている。

3. 再配布には、本書の逐語的コピーが含まれる。

OpenLDAP Foundation は本ライセンスを随時改訂できます。各改訂はバージョン番号によって識別されます。本ソフトウェアを、ライセンスのこの版、またはその後の改訂版の条件の下で使用できます。

ソフトウェアは、OPENLDAP FOUNDATION およびそのコントリビューターによって無保証で提供されており、商品性、および特定の用途に対する適合性関する保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも OPENLDAP FOUNDATION、そのコントリビューターまたはそのソフトウェアの著作者または所有者は、いかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害（代替品またはサービスの購入、代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない）に対しても、その原因や、責任に関する法理に関わりなく、また契約上の保証、厳格な責任に基づく保証、不法行為（過失またはその他）のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

著作者および著作権所有者の名称を、事前の特別の書面による承諾なしに本ソフトウェアの販売、使用またはその他の取り扱いの広告またはその他の方法で販売促進のために使用することはできません。本ソフトウェアの著作権の所有権は常に著作権保有者によって保持されます。

OpenLDAP は OpenLDAP Foundation の登録商標です。

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA.All rights reserved.
本マニュアルの逐語的コピーをコピーおよび配布することができます。

OpenSSL

Copyright (c) 1998-2002

The OpenSSL Project.All rights reserved.

以下の条件が満たされている場合は、変更の有無にかかわらず、ソースフォームおよびバイナリーフォームにより再配布および使用を許可します：

1. ソース・コードの再配布においては、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が保持されている。

2. バイナリ形式による再配布においては、そのマニュアルおよび（または）その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。

3. 本ソフトウェアの機能または使用方法を記述するすべての広告物には、下記の献辞を表示しなければならない。

[本製品には OpenSSL Project によって、OpenSSL ツールキットで使用するために開発されたソフトウェアが含まれます（http://www.openssl.org/）]

4. "OpenSSL Toolkit" および "OpenSSL Project" の名称を、事前の書面による承諾なしに本ソフトウェアから派生した製品の推奨または販売促進のために使用することはできない。書面による承諾を得るには、openssl-core@openssl.org にご連絡ください。

5. OpenSSL Project の事前の書面による承諾なしに、本ソフトウェアから派生した製品に "OpenSSL" という名称を付けたり、その名称 に "OpenSSL" という語句を含めてはいけない。

6. いかなる形式での再配布においても、下記の献辞を表示しなければならない。

[本製品には OpenSSL Project によって、OpenSSL ツールキットで使用するために開発されたソフトウェアが含まれます（http://www.openssl.org/）]

本ソフトウェアは、OpenSSL PROJECT によって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも、OpenSSL PROJECT またはそのコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害（代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない）に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為（過失またはその他）のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

本製品には、Eric Young（eay@cryptsoft.com）によって作成された暗号ソフトウェアが含まれます。本製品には、Tim Hudson（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。

SSLeay の当初ライセンス

Copyright (C) 1995-1998 Eric Young（eay@cryptsoft.com）
All rights reserved.

本パッケージは Eric Young（eay@cryptsoft.com）によって作成された SSL の実装です。本実装は、Netscapes SSL に適合するように作成されています。

本ライブラリは、下記の条件が守られる限り、商用および非商用に無償で使用できます。下記の条件は、本配布に含まれるすべてのコード、すなわち SSL コードだけでなく、RC4、RSA、lhash、DES 等のコードにも適用されます。本配布に含まれる SSL のマニュアルには、著作権所有者が Tim Hudson（tjh@cryptsoft.com）であること以外は、同じ著作権条件が適用されます。

著作権は Eric Young が保持しますから、コードの中の著作権に関する注記を削除することはできません。

本パッケージが製品内で使用される場合、Eric Young が使用されているライブラリの一部の作成者であることを明記しなければなりません。これはプログラムのセットアップ時のテキスト・メッセージの形式でも、パッケージに付属するマニュアル（オンラインまたはテキスト）に含めてもかまいません。

以下の条件が満たされている場合は、変更の有無にかかわらず、ソースフォームおよびバイナリーフォームにより再配布および使用を許可します：

1. ソース・コードの再配布においては、著作権の表記、一連の条件および下記の免責事項が記載されている。

2. バイナリ形式による再配布においては、そのマニュアルおよび（または）その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。

3. 本ソフトウェアの機能または使用方法を記述するすべての広告物には、下記の献辞を表示しなければならない。

[本製品には、Eric Young（eay@cryptsoft.com）によって作成された暗号ソフトウェアが含まれます。]

（使用しているライブラリからのルーチンが暗号関連でない場合は、[暗号] を削除してもかまいません）。

4. apps ディレクトリ（アプリケーション・コード）からの Windows 固有のコード（またはその派生物）を含める場合には、下記の献辞を含めなければならない。

[本製品には、Tim Hudson（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。]

本ソフトウェアは、ERIC YOUNG によって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む（ただしそれに限定されない）明示または暗黙の一切の保証は否認されています。いかなる場合でも、著作者またはコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害（代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない）に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為（過失またはその他）のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

本コードの公開されているバージョンおよび派生物のライセンスおよび配布条件を屁高することができません。

Tcl 8.3

Tcl ソフトウェアは、Regents of University of California、Sun Microsystems, Inc.、Scriptics Corporation、および他の当事者が著作権を有しています。

以下の条件は、個々のファイルにおいて明示的に否認されていない限り、本ソフトウェアに関連するすべてのファイルに適用します。作成者は、既存の著作権に関する注記が全てのコピーにおいて保持されること、およびこの注記がすべての配布物において逐語的に含まれていることを条件に、本ソフトウェアおよびそのマニュアルをいかなる目的においても、無償で使用、コピー、変更、配布、ライセンスすることを許諾します。承認された使用において、いかなる書面による契約、ライセンス、または使用料も要求されません。本ソフトウェアへの変更は、その作成者による著作権登録が可能であり、本契約に記載しているライセンス条件に従う必要はありませんが、但しライセンス条件を変更する場合は、それが適用される各ファイルの最初のページに新しいライセンス条件が明記される必要があります。

いかなる場合でも、作成者または販売代理店は、本ソフトウェア、そのマニュアル、またはその派生物の使用から生じたいかなる直接的、間接的、特殊的、偶発的、または結果的損害に対して、作成者がそのような損害が生じる可能性について通告を受けていた場合でも、すべての当事者に対して一切の責任を負いません。作成者および販売代理店は、特に、商品性、特定の目的に対する適合性、および著作権侵害の不存在に関する暗黙の保証を含む（ただしそれに限定されない）一切の保証を否認するものとします。本ソフトウェアは、無償で提供されており、作成者および販売代理店は、保守、サポート、更新、機能強化、変更を提供する責任はありません。

索引

U

W

X

あ

い