悪意のある URL または望ましくない URL からの保護

この章は、次の項で構成されています。

- URL 関連の保護および制御 （1 ページ）
- URL レトロスペクティブ判定と URL 修復 （3 ページ）
- URL フィルタリングの設定 （4 ページ）
- メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （13 ページ）
- URL フィルタリング用にスキャンできないメッセージの処理 （18 ページ）
- メールボックス内の悪意のある URL の修復 （18 ページ）
- コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出 （20 ページ）
- メッセージ フィルタを使用した、メッセージの悪意のある URL の検出 （22 ページ）
- URL フィルタリング結果のモニタ （23 ページ）
- メッセージ トラッキングの URL 詳細の表示 （23 ページ）
- URL フィルタリングのトラブルシューティング （24 ページ）
- URL カテゴリについて （32 ページ）

URL 関連の保護および制御

作業キューのアンチスパム、アウトブレイク、コンテンツおよびメッセージ フィルタリング プロセスには、悪意のあるリンクまたは望ましくないリンクに対する制御および保護が組み込まれています。これらは、以下を制御します。

- メッセージおよび添付ファイルの悪意のある URL からの保護を強化する。

  URL フィルタリングはアウトブレイク フィルタリングに組み込まれています。組織にすでに Cisco Web Security Appliance や、類似する Web ベースの脅威からの保護機能を導入している場合でも、この保護強化機能は脅威をその侵入時点でブロックするため、有用です。

また、コンテンツ フィルタやメッセージ フィルタを使用して、メッセージに含まれる URL に対してその URL の Web ベース レピュテーション スコア（WBRS）に基づいてアクションを実行することができます。

（注） ベストプラクティスとして、疑わしい、ニュートラル、好ましいまたは不明なレピュテーションを持つ URL は、クリック時の URL の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするように書き換えることをお勧めします。

- スパムの識別の改善

  電子メールゲートウェイは、メッセージのリンクのレピュテーションとカテゴリを、その他のスパム特定アルゴリズムと組み合わせて使用し、スパムを特定します。たとえば、メッセージのリンクがマーケティングの Web サイトに属している場合、メッセージはマーケティングに関するメッセージである可能性が高いです。

- 企業のアクセプタブル ユース ポリシーの適用のサポート

  URL のカテゴリ（アダルト コンテンツや違法行為など）を、コンテンツ フィルタおよびメッセージ フィルタと組み合わせて使用して、企業のアクセプタブル ユース ポリシーの適用を強化できます。

- 保護のために書き換えられたメッセージに含まれる URL を最も頻繁にクリックした組織内のユーザ、および最も頻繁にクリックされたリンクを識別できます。

関連項目

- 評価される URL （2 ページ）
- [Webインタラクショントラッキング（Web Interaction Tracking）] ページ

評価される URL

着信メッセージと発信メッセージ（添付ファイルを含む）に含まれる URL が評価されます。URL を表す有効な文字列（次を含む文字列）が評価されます。

- http、https、www
- ドメインまたは IP アドレス
- コロン（:）が先頭に付いたポート番号
- 大文字または小文字

メッセージがスパムであるかどうかを判定するために URL を評価するときに、これがロード管理に必要である場合は、着信メッセージのスクリーニングが発信メッセージよりも優先されます。

URL レトロスペクティブ判定と URL 修復

URL は、クラウドベースの Talos インテリジェンスサービスによって提供された URL レピュテーションとカテゴリに基づいてフィルタ処理されます。新しい情報の出現に伴い、URL レピュテーションは変化します。当初 URL が悪意があると評価されず、メッセージが受信者にリリースされることがあります。しかし、後でURL レピュテーションがユーザーのメールボックスに達してから、悪意のあるファイルに変化する可能性があります。Talos インテリジェンスサービスは、サンドボックスサーバーでの URL 判定を監視します。電子メールゲートウェイは、Talos からの URL のレトロスペクティブ判定の更新を 2 分ごとに 168 時間ポーリングします。いずれかの URL レピュテーションが [悪意あり（Malicious）] に変更された場合、Talos はレトロスペクティブ判定の更新を電子メールゲートウェイに送信します。電子メールゲートウェイは、必要なアクションを実行できるように、レトロスペクティブ判定の更新に関するアラートを送信します。

Cisco Secure Email Gateway は、分析のために送信された URL から 7 日以内に生成された URL レトロスペクティブ判定を処理します。電子メールゲートウェイは、7 日後に受信した判定に対して、設定されたポリシーアクションを実行しません。

さらに、メールボックス自動修復サービスを設定して、ユーザーのメールボックスの、悪意のある URL を含むメッセージを修復することもできます。たとえば、URL のレピュテーションが「悪意がある」に変更されたときには、受信者のメールボックスからメッセージを削除するようにEメールゲートウェイを設定することができます。設定されたポリシーアクションは、配信されたメッセージにのみ適用されます。

（注） URL レトロスペクティブ判定および修復機能は、受信メールでのみ使用できます。

Cisco Secure Email Gateway からの URL レトロスペクティブ判定のトラフィックは復号化できません。パススループロキシモードのみがサポートされています。ただし、ポーリング応答データは復号化できます。

同じ件名のすべての電子メールに悪意のある URL が含まれている場合、その電子メールはすべて修復されます。

Cisco Secure Email Gateway のファイアウォールルールを更新して、次のホスト名が URL レトロスペクションのグローバル登録およびポーリングサービスにアクセスできるようにする必要があります。

- prod-register-api.uce.cmd.cisco.com
- prodap-retro-api.uce.cmd.cisco.com
- prodeu-retro-api.uce.cmd.cisco.com
- produs-retro-api.uce.cmd.cisco.com

電子メールゲートウェイは、ホスト名（prod-register-api.uce.cmd.cisco.com）に設定された DNS サーバーに基づいて、いずれかの地理的リージョン（APJC、EU、アメリカなど）の URL レトロスペクション登録およびポーリングサービスに接続されます。

関連項目

- メールボックス内の悪意のある URL の修復 （18 ページ）

URL フィルタリングの設定

- URL フィルタリングの要件 （4 ページ）
- URL フィルタリングを有効にする （5 ページ）
- Talos インテリジェンスサービスへの接続について （8 ページ）
- Web インタラクション トラッキング （9 ページ）
- クラスタ構成での URL フィルタリング （10 ページ）
- URL フィルタリングの許可リストの作成 （10 ページ）
- サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ （11 ページ）

URL フィルタリングの要件

URL フィルタリングをイネーブルにする他に、必要な機能に応じてその他の機能をイネーブルにする必要があります。

スパムに対する保護の強化：

- スパム対策スキャンは、グローバルにイネーブルにするか、または該当するメール ポリシーごとにイネーブルにする必要があります。これには IronPort Anti-Spam 機能またはインテリジェント マルチスキャン機能のいずれかを使用できます。スパム対策の章を参照してください。

  マルウェアに対する保護の強化：

- アウトブレイク フィルタ機能はグローバルにイネーブルにするか、または該当するメール ポリシーごとにイネーブルにする必要があります。アウトブレイク フィルタに関する章を参照してください。

  URL のレピュテーションに基づいてアクションを実行するか、またはメッセージ フィルタとコンテンツ フィルタを使用してアクセプタブル ユース ポリシーを適用する場合：

- アウトブレイク フィルタ機能はグローバルにイネーブルにする必要があります。アウトブレイク フィルタに関する章を参照してください。

URL フィルタリングを有効にする

URL フィルタリングは、Web インターフェイスの **[セキュリティ サービス（Security Services）] > [URL フィルタ（URL Filtering）]** ページまたは CLI の **`websecurityconfig`** コマンドを使用してイネーブルにできます。

（注） URL フィルタリングを有効にすると、URL レトロスペクティブサービスも自動的に有効になります。詳細については、URL レトロスペクティブ判定と URL 修復 （3 ページ）を参照してください。

はじめる前に

- 使用する各 URL フィルタ機能の要件を満たしていることを確認してください。URL フィルタリングの要件 （4 ページ）を参照してください。
- （任意）すべての URL フィルタリング機能で無視する URL のリストを作成します。URL フィルタリングの許可リストの作成 （10 ページ）を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] を選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 [URLカテゴリおよびレピュテーションのフィルタの有効化（Enable URL Category and Reputation Filters）] チェックボックスをオンにします。

ステップ 4 （任意）メッセージを評価し、スパムやマルウェアが含まれているかどうかを確認するときに URL フィルタリングから除外する URL、およびすべてのコンテンツ フィルタリングとメッセージ フィルタリングから除外する URL のリストを作成した場合は、そのリストを選択します。

この設定により、メッセージがスパム対策またはアウトブレイク フィルタの処理をバイパスすることは通常はありません。

ステップ 5 （任意）**Web インタラクション トラッキング**を有効にします。Web インタラクション トラッキング （9 ページ）を参照してください。

ステップ 6 [URLフィルタリング（URL Filtering）] ページでは、**URL レトロスペクティブサービスのステータス**も確認できます。URL レトロスペクティブサービスを有効または無効にするには、CLI の `urlretroservice` コマンドを参照してください。

ステップ 7 （任意）[詳細設定（Advanced Settings）] をクリックし、次の表に示す必須パラメータを入力して、URL フィルタリングの詳細設定を行います。

パラメータ	Description
URL ルックアップタイムアウト（URL Lookup Timeout）	URL が特定のドメイン名の IP アドレスを要求するためにかかる時間を入力します。
メッセージ本文でスキャンされる URL の最大数（Maximum Number of URLs scanned in Message Body）	電子メールゲートウェイがメッセージ本文内でスキャンする URL の最大数を入力します。
メッセージ添付ファイルでスキャンされるURL の最大数（Maximum Number of URLs scanned in Message Attachments）	電子メールゲートウェイがメッセージの添付ファイルでスキャンするURLの最大数を入力します。
メッセージ内の URL テキストと HREF の書き換え（Rewrite URL text and HREF in Message）	書き換えられた URL 全体をメッセージ本文に表示する場合は、[はい（Yes）] オプションボタンを選択します。 または 書き換えられた URL 全体を HTML メッセージの HREF にのみ表示する場合は、[いいえ（No）] オプションボタンを選択します。

パラメータ	Description
URL Logging	メールログとメッセージトラッキングに URL の詳細を表示する場合は、[イネーブル化（Enable）] オプションボタンを選択します。 URLの詳細は、次のいずれかの条件に基づいてメールログとメッセージトラッキングに記録されます。 • メッセージ内のいずれかの URL のカテゴリが URL カテゴリフィルタと一致した • メッセージ内のいずれかの URL のレピュテーションスコアが URL レピュテーションフィルタと一致した • アウトブレイクフィルタ（イネーブルな場合）によってメッセージ内のずれかの URL が書き換えられた

ステップ 8 変更を送信し、保存します。

該当する前提条件を満たしており、すでにアウトブレイク フィルタとスパム対策保護を設定している場合は、スパムまたは悪意のある URL の拡張自動検出を利用するために、追加の設定を行う必要はありません。

次のタスク

- メッセージに含まれている URL のレピュテーションに基づいてアクションを実行する場合は、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （13 ページ）を参照してください。
- コンテンツ フィルタおよびメッセージ フィルタで URL カテゴリを使用するには（アクセプタブル ユース ポリシーを適用する場合など）、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （13 ページ）を参照してください。
- スパムの可能性があるメッセージの URL をすべて Cisco Web セキュリティ プロキシ サービスにリダイレクトするには、カスタムヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例を参照してください。
- （任意）エンドユーザ通知ページの外観をカスタマイズするには、サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ （11 ページ）を参照してください。
- この機能に関連する問題についてのアラートを受信することを確認します。将来の URL カテゴリ セットの変更 （49 ページ）、ご使用の AsyncOS リリースのリリース ノート、およびアラート受信者の追加を参照してください。

Talos インテリジェンスサービスへの接続について

URL レピュテーションとカテゴリは、クラウドベースの Talos インテリジェンスサービスによって提供されます。

電子メールゲートウェイは、ファイアウォール情報で URL フィルタリングサービス用に指定したポートを使用して、Talos インテリジェンスサービスに直接または Web プロキシ経由で接続します。通信は HTTPS 経由で相互証明書認証を使用して行われます。証明書は自動的に更新されます（サービス アップデートを参照）。必要な証明書の詳細については、URL フィルタリング機能の証明書 （8 ページ）に示されている場所から入手できるリリース ノートを参照してください。

[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで HTTP または HTTPS プロキシを設定している場合は、電子メールゲートウェイが Talos インテリジェンスサービスとの通信時にそのプロキシ設定を使用します。プロキシ サーバの使用の詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定を参照してください。

FIPS モードでは、Talos インテリジェンスサービスとの通信で FIPS 暗号方式が使用されます。

（注） 証明書はコンフィギュレーション ファイルには保存されません。

関連項目

- URL フィルタリング機能の証明書 （8 ページ）
- アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （27 ページ）
- アラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （27 ページ）

URL フィルタリング機能の証明書

AsyncOS は、URL フィルタリング機能に使用するクラウド サービスとの通信に必要な証明書を自動的に導入、更新するように設計されています。ただし、何らかの理由でシステムがこれらの証明書を更新できない場合には、ユーザのアクションを必要とするアラートがユーザに送信されます。

これらのアラート（[システム（System）] タイプ、[警告（Warning）] 重大度）を送信するように 電子メールゲートウェイが設定されていることを確認します。この説明については、アラート を参照してください。

無効な証明書に関するアラートを受信した場合は、Cisco TAC に連絡してください。Cisco TAC は必要な代替証明書を提供できます。代替証明書の使用手順については、Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （31 ページ）を参照してください。

Web インタラクション トラッキング

Web インタラクション トラッキング機能は、書き換えられた URL をクリックしたエンド ユーザおよび各ユーザ クリックに関連するアクション（許可、ブロック、不明）に関する情報を提供します。この機能をイネーブルにすると、Web インタラクション トラッキング レポートを使用して、クリックされた悪意のある上位 URL、悪意のある URL をクリックした上位ユーザなどの情報を確認できます。Web インタラクション トラッキング レポートの詳細については、[Web インタラクション トラッキング（Web Interaction Tracking）] ページを参照してください。

Web インタラクション トラッキング データは、クラウドベースの Cisco Aggregator Server によって提供されます。

関連項目

- Web インタラクション トラッキングの設定 （9 ページ）
- Cisco Aggregator Server への接続について （9 ページ）

Web インタラクション トラッキングの設定

要件に応じて、いずれかのグローバル設定ページで Web インタラクション トラッキングをイネーブルにできます。

- **アウトブレイク フィルタ**。アウトブレイク フィルタによって書き換えられた URL をクリックしたエンド ユーザを追跡します。アウトブレイク フィルタのグローバル設定の構成を参照してください。
- **URL フィルタリング**。ポリシーによって書き換えられた URL をクリックしたエンド ユーザを追跡します（コンテンツ フィルタおよびメッセージ フィルタを使用して）。URL フィルタリングを有効にする （5 ページ） を参照してください。

Cisco Aggregator Server への接続について

電子メール ゲートウェイは 30 分（構成不能）ごとに、ファイアウォール情報で URL フィルタリング サービス用に指定したポートを使用して、Cisco Aggregator Server に直接または Web プロキシ経由で接続します。通信は HTTPS 経由で相互証明書認証を使用して行われます。証明書は自動的に更新されます（サービス アップデートを参照）。

[セキュリティ サービス（Security Services）] > [サービスのアップデート（Service Updates）] ページで HTTP または HTTPS プロキシが設定されている場合、 電子メール ゲートウェイは Cisco Aggregator Server との通信にこれらを使用します。プロキシ サーバの使用の詳細については、アップグレードおよびアップデートをダウンロードするためのサーバ設定を参照してください。

FIPS モードでは、Cisco Aggregator Server との通信には FIPS 暗号が使用されます。

（注） 証明書はコンフィギュレーション ファイルには保存されません。

クラスタ構成での URL フィルタリング

- URL フィルタリングは、マシンごと、グループごと、またはクラスタごとに有効にできます。
- URL フィルタリングがマシンレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをマシン、グループ、またはクラスタレベルで設定できます。
- URL フィルタリングがグループレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをグループまたはクラスタレベルで設定する必要があります。
- URL フィルタリングがクラスタレベルで有効になっている場合、URL 許可リストおよび Web インタラクション トラッキングをクラスタレベルで設定する必要があります。
- メッセージ フィルタとコンテンツ フィルタのクラスタの標準ルールが適用されます。

URL フィルタリングの許可リストの作成

URL フィルタリング機能の設定時にグローバル許可リストを指定すると、その許可リストに含まれている URL は、レピュテーション、カテゴリ、アンチスパム、アウトブレイク フィルタリング、コンテンツフィルタリング、およびメッセージフィルタリングの対象として評価されません。ただし、これらの URL を含むメッセージは、アンチスパム スキャンおよびアウトブレイク フィルタによって通常どおりに評価されます。グローバル URL 許可リストを補足する目的で、コンテンツフィルタとメッセージフィルタの各 URL フィルタリング条件（ルール）およびアクションに URL 許可リストを指定することもできます。

アウトブレイク フィルタリングから許可リストの URL を分類するには通常、[メールポリシー：アウトブレイクフィルタ（Mail Policies: Outbreak Filters）] ページで設定した [ドメインのスキャンをバイパス（Bypass Domain Scanning）] オプションを使用します。URL フィルタリング用の URL 許可リストは、[ドメインのスキャンをバイパス（Bypass Domain Scanning）] に似ていますが、このオプションとは関係ありません。この機能の詳細については、URL 書き換えおよびドメインのバイパスを参照してください。

この項で説明する URL フィルタリング許可リストと、IP レピュテーションスコアに基づく送信者レピュテーション フィルタリングに使用される許可リストは無関係です。

はじめる前に

Web インターフェイスで URL リストを作成する代わりに、リストをインポートすることを検討してください。URL リストのインポート （11 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [URL リスト（URL Lists）] を選択します。

ステップ 2 [URL リストの追加（Add URL List）] を選択するか、または編集するリストをクリックします。

グローバルに指定するすべての URL が許可リストとして 1 つのリストにまとめられていることを確認します。URL フィルタリングにはグローバル許可リストを 1 つだけ選択できます。

ステップ 3 URL リストを作成して送信します。

サポートされる URL 形式のリストを表示するには、[URL（URL s）] ボックスにセミコロン（:）を入力し、[送信（Submit）] をクリックします表示される [詳細...（more...）] リンクをクリックします。

各 URL、ドメイン、または IP アドレスを 1 行ずつ入力するか、またはコンマで区切って入力することができます。

ステップ 4 変更を保存します。

次のタスク

- URL リストをグローバル許可リストとして指定するには、URL フィルタリングを有効にする （5 ページ）を参照してください。
- URL リストを、コンテンツフィルタまたはメッセージフィルタの特定の条件（ルール）またはアクションのための許可リストとして指定するには、メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （13 ページ）およびコンテンツ フィルタのアクションを参照してください。メッセージ フィルタについてはURL カテゴリ アクションおよびURL カテゴリ ルールも参照してください。

関連項目

- URL リストのインポート （11 ページ）

URL リストのインポート

URL リストをインポートし、URL フィルタリングの許可リストとして使用できます。

手順

ステップ 1 インポートするテキスト ファイルを作成します。

- 最初の行には URL リストの名前を指定する必要があります。
- 各 URL はそれぞれ別の行に入力する必要があります。

ステップ 2 ファイルをアプライアンスの `/configuration` ディレクトリにアップロードします。

ステップ 3 コマンドライン インターフェイスで `urllistconfig > new` コマンドを使用します。

サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ

アウトブレイク フィルタまたはポリシー（コンテンツ フィルタまたはメッセージ フィルタを使用して）で識別された悪意のある URL をエンドユーザがクリックすると、Cisco Web セキュ

リティ プロキシによってエンド ユーザの Web ブラウザに通知が表示されます。この通知には、サイトに悪意があり、サイトへのアクセスがブロックされている旨が記載されています。

アウトブレイク フィルタを使用して書き換えられた URL をエンド ユーザがクリックすると、通知ページが 10 秒間表示された後、クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトされます。

この通知ページの外観をカスタマイズして、企業ロゴ、連絡先情報など、組織のブランディングを表示できます。

（注） 通知ページをカスタマイズしない場合、エンド ユーザにはシスコ ブランドの通知ページが表示されます。

はじめる前に

- URL フィルタリングをイネーブルにします。URL フィルタリングを有効にする （5 ページ）を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [ブロック ページ カスタマイズ（Block Page Customization）] を選択します。

ステップ 2 **[有効（Enable）]** をクリックします。

ステップ 3 [ブロック ページ カスタマイズを有効にする（Enable Block Page customization）] チェックボックスをオンにして、次の詳細を入力します。

- 組織のロゴの URL。ロゴ イメージは、公にアクセス可能なサーバでホストすることが推奨されます。
- 組織名
- 組織の連絡先情報

ステップ 4 通知の言語を選択します。Web インターフェイスでサポートされるいずれかの言語を選択できます。

（注） エンドユーザのブラウザのデフォルト言語は、ここで選択した言語より優先されます。また、エンドユーザのブラウザのデフォルト言語が AsyncOS でサポートされていない場合は、ここで選択した言語で通知が表示されます。

ステップ 5 （任意）[ブロック ページ カスタマイズのプレビュー（Preview Block Page Customization）] をクリックして通知ページをプレビューします。

ステップ 6 変更を送信し、保存します。

次のステップ

次のいずれかの方法で URL の書き換えを設定します。

- アウトブレイク フィルタを使用します。URL のリダイレクトを参照してください。

- コンテンツ フィルタまたはメッセージ フィルタを使用します。メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行 （13 ページ） を参照してください。

メッセージに含まれる URL のレピュテーションまたはカテゴリに基づくアクションの実行

メッセージ本文またはメッセージの添付ファイルに含まれる URL リンクのレピュテーションまたはカテゴリに基づき、着信および発信電子メール ポリシーのメッセージ フィルタまたはコンテンツ フィルタを使用してアクションを実行できます。

アウトブレイク フィルタでは、マルウェアについてメッセージを評価するときにさまざまな要因が考慮されるため、URL レピュテーションだけではアグレッシブなメッセージ処理はトリガーされません。URL レピュテーションに基づいてフィルタを作成することをお勧めします。

たとえば、URL レピュテーション フィルタを使用して次のことを実行できます。

- （メッセージ本文に含まれる URL の場合のみ）ニュートラルまたは不明なレピュテーションの URL を書き換えて、クリック時の安全性評価のために Cisco Cloud Web Security プロキシ サービスにリダイレクトします。
- レピュテーションスコアが 信頼できないレピュテーションの範囲に該当する URL を含むメッセージをドロップします。

URL カテゴリ フィルタを使用して、次のことを実行できます。

- URL カテゴリをフィルタリングして、許容される Web の使用に関する組織のポリシーを適用します。たとえば、ユーザがオフィスでアダルト サイトやギャンブル サイトにアクセスできないようにする場合などです。
- 分類が可能となる十分な期間にわたって存在しない可能性がある、悪意のあるサイトからの保護を強化します。（メッセージ本文に含まれる URL の場合のみ）ユーザがリンクをクリックした時点で評価できるように、[未分類（Unclassified）] カテゴリの URL をすべて Cisco Cloud Web Security プロキシ サービスにリダイレクトできます。

関連項目

- URL 関連の条件(ルール）およびアクションの使用 （14 ページ）
- URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール （14 ページ）
- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （15 ページ）
- リダイレクト URL：エンドユーザのエクスペリエンス （17 ページ）

URL 関連の条件(ルール）およびアクションの使用

目的	例	操作内容
メッセージ全体に対してアクションを実行する。	メッセージを削除または検疫する。	URL レピュテーションまたは URL カテゴリの条件またはルールを作成し、URL レピュテーションまたは URL カテゴリのアクション以外のアクションと組み合わせます。 例外：URL レピュテーション条件またはルールをバウンスアクションと組み合わせないでください。
（メッセージ本文の URl の場合のみ）メッセージに含まれる URL を変更またはその動作を変更します。	メッセージに含まれる URL をテキストに置換するか、URL をクリックできない状態にします。	URL レピュテーションまたは URL カテゴリのアクションのみを作成します。個別の URL フィルタリング条件は使用しないでください。

コンテンツ フィルタを使用するには、メール ポリシーにそのフィルタを指定する必要があります。

関連項目

- URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール （14 ページ）
- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （15 ページ）

URL レピュテーションまたは URL カテゴリによるフィルタリング：条件およびルール

メッセージの本文および添付ファイルに含まれる URL のレピュテーションまたはカテゴリに基づいて、メッセージに対するアクションを実行できます。URL または URL の動作の変更以外のアクションを実行するには、**URL レピュテーション**または **URL カテゴリ**の条件を追加し、アクションを適用するレピュテーション スコアまたは URL カテゴリを選択します。

たとえば、[成人向け（Adult）] カテゴリの URL が含まれているすべてのメッセージに対して [ドロップする（最終アクション）（Drop (Final Action)）] アクションを適用するには、[成人向け（Adult）] カテゴリが選択されている [URL カテゴリ（URL Category）] タイプの条件を追加します。

カテゴリを指定しない場合、選択したアクションはすべてのメッセージに適用されます。

信頼できる URL、ニュートラルな URL、および信頼できない URL の URL レピュテーション スコア範囲が事前定義されているため、編集できません。ただし、代わりにカスタム範囲を指

定できます。指定されたエンドポイントは、指定した範囲に含まれます。たとえば、-8 から -10 までのカスタム範囲を作成する場合、-8 と -10 はこの範囲に含まれます。レピュテーションスコアを判断できない URL には 「不明」 を使用します。

（注） ニュートラルな URL レピュテーションとは、URL は現在はクリーンであるが、攻撃に陥りやすいため、今後悪意のある URL に変化する可能性があることを示します。このような URL に対して、管理者はノンブロッキング ポリシー（クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするなど）を作成できます

選択した URL 許可リストまたはグローバル URL 許可リストに含まれている URL は評価されません。

この条件と組み合わせるアクションは、メッセージに含まれる URL が、レピュテーション スコアまたは条件に指定されているカテゴリに一致する場合に実行されます。

メッセージに含まれる URL またはその動作を変更するには、URL レピュテーションまたは URL カテゴリのアクションのみを設定します。この目的のための別個の URL レピュテーションまたは URL カテゴリの条件またはルールは不要です。

（注） URL レピュテーションの条件をバウンス アクションと組み合わせないでください。

ヒント 特定の URL カテゴリを確認するには、未分類の URL と誤って分類された URL の報告 （48 ページ）のリンクを参照してください。

関連項目

- URL フィルタリングの許可リストの作成 （10 ページ）
- コンテンツ フィルタ

メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用

URL レピュテーションまたは URL カテゴリのアクションを使用し、URL のレピュテーションまたはカテゴリに基づいて、メッセージに含まれる URL またはその動作を変更します。

URL レピュテーションおよび URL カテゴリのアクションには、個別の条件は必要ありません。代わりに、URL レピュテーションまたは URL カテゴリのアクションで選択するレピュテーションまたはカテゴリに基づいて、選択したアクションが適用されます。

アクションは、そのアクションに指定された条件に一致する URL だけに適用されます。メッセージに含まれるその他の URL は変更されません。

カテゴリを指定しない場合、選択したアクションはすべてのメッセージに適用されます。

信頼できる URL、ニュートラルな URL、および信頼できない URL の URL レピュテーションスコア範囲は事前定義されているため、編集できません。ただし、代わりにカスタム範囲を指定できます。指定されたエンドポイントは、指定した範囲に含まれます。たとえば、-8 から -10 までのカスタム範囲を作成する場合、-8 と -10 はこの範囲に含まれます。レピュテーションスコアを判断できない URL には「不明」を使用します。

（注） ニュートラルな URL レピュテーションとは、URL は現在はクリーンであるが、攻撃に陥りやすいため、今後悪意のある URL に変化する可能性があることを示します。このような URL に対して、管理者はノンブロッキング ポリシー（クリック時の安全性評価のために Cisco Web セキュリティ プロキシにリダイレクトするなど）を作成できます

次の URL 関連のアクションは、メッセージ本文に含まれる URL のみに適用されます。

- URL を無効化して、クリックできないようにします。メッセージ受信者は、引き続きその URL を表示およびコピーできます。
- メッセージ受信者がリンクをクリックすると、トランザクションがクラウド内の Cisco Web セキュリティ プロキシにルーティングされるように URL をリダイレクトします。このプロキシでは、悪意のあるサイトである場合はアクセスがブロックされます。

  例：フィッシング攻撃で使用される悪意のあるサイトは、分類が可能となる十分な期間にわたって存在しないことがよくあるため、[未分類（Uncategorized）] カテゴリに含まれるすべての URL を Cisco Cloud Web Security プロキシ サービスにリダイレクトするとします。

  リダイレクト URL：エンドユーザのエクスペリエンス （17 ページ）も参照してください。

  URL を別のプロキシにリダイレクトするには、次の箇条書き項目の例を参照してください。

（注） このリリースでは、Cisco Cloud Web Security プロキシ サービスには設定可能なオプションがありません。たとえば、調整する脅威スコアのしきい値や、脅威スコアに基づいて指定するアクションがありません。

- URL を任意のテキストで置き換えます。

  メッセージに示されるテキストに元の URL を含めるには、$URL 変数を使用します。

  次に、例を示します。

  - [違法ダウンロード（Illegal Downloads）] カテゴリのすべての URL を次のテキストに置き換えます。

```
Message from your system administrator: A link to an illegal downloads web site
has been removed from this message.
```

- 元の URL と次の警告を組み込みます。

  ```
  警告! The following URL may contain malware: $URL
  ```

  次のようになります。警告：次の URL にはマルウェアが含まれている可能性があります。http://example.com。

- カスタム プロキシまたは Web セキュリティ サービスにリダイレクトします。

  ```
  http://custom_proxy/$URL
  ```

  これは http://custom_proxy/http://example.com となります。

選択した URL 許可リストまたはグローバル URL 許可リストに含まれている URL のレピュテーションまたはカテゴリは評価されません。

URL の危険を取り除くか、URL を置き換える場合は、署名メッセージで URL を無視することを選択できます。

URL レピュテーションまたは URL カテゴリのアクションを URL レピュテーションまたは URL カテゴリの条件（またはルール）と組み合わせることは推奨されません。組み合わせる条件(ルール）とアクションに異なるカテゴリが含まれている場合、一致することはありません。

ヒント 特定の URL カテゴリを確認するには、未分類の URL と誤って分類された URL の報告 （48 ページ）のリンクを参照してください。

関連項目

- URL フィルタリングの許可リストの作成 （10 ページ）
- カスタム ヘッダーを使用して、陽性と疑わしいスパム内の URL を Cisco Web セキュリティ プロキシにリダイレクトする：設定例
- コンテンツ フィルタ
- URL レピュテーション ルール
- URL カテゴリ ルール

リダイレクト URL：エンドユーザのエクスペリエンス

Cisco Cloud Web Security プロキシ サービスの評価に基づいて、次の処理が行われます。

- サイトが安全である場合、ユーザはターゲット Web サイトに誘導され、リンクがリダイレクトされたことを認識しません。
- 悪意のあるサイトの場合、そのサイトは悪意のあるサイトであり、アクセスがブロックされたことを示す通知がユーザに対して表示されます。

エンドユーザ通知ページの外観をカスタマイズして、企業ロゴ、連絡先情報など、組織のブランディングを表示できます。サイトに悪意がある場合にエンドユーザに表示する通知のカスタマイズ （11 ページ）を参照してください。

- Cisco Cloud Web Security プロキシ サービスとの通信がタイムアウトになった場合、ユーザに対しターゲット Web サイトへのアクセスが許可されます。
- その他のエラーが発生した場合、ユーザに対して通知が表示されます。

関連項目

- メッセージに含まれる URL の変更：フィルタでの URL レピュテーションまたは URL カテゴリのアクションの使用 （15 ページ）

URL フィルタリング用にスキャンできないメッセージの処理

次のシナリオでは、URL フィルタリング スキャンが失敗し、次のヘッダー *X-URL-LookUp-ScanningError* がメッセージに追加されます。

- URL レピュテーションとカテゴリを取得できない
- メッセージで短縮 URL を展開できない
- メッセージ本文や添付ファイル内の URL の数が最大 URL スキャンの制限を超えている

コンテンツ フィルタを追加、[その他のヘッダー（Other Header）] 条件に *X-URL-LookUp-ScanningError* ヘッダーを選択、およびメッセージで実行する適切な処置を設定できます。

メールボックス内の悪意のある URL の修復

レピュテーションに関係なく、URL は常に、ユーザーのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。Talos から受信した URL レトロスペクティブ判定に基づいてアラートを送信するように、E メールゲートウェイで URL フィルタリングを設定できます。URL 判定が悪意ありに変更されたときにユーザーのメールボックス内のメッセージに対して自動修復アクションを実行するように電子メールゲートウェイを設定することもできます。

はじめる前に

- 使用する各 URL フィルタ機能の要件を満たしていることを確認してください。URL フィルタリングの要件 （4 ページ）を参照してください。
- URL フィルタリングが有効にされていることを確認します。URL フィルタリングを有効にする （5 ページ） を参照してください。

- クラウドサービスにアクセスするためのライセンスキーが E メールゲートウェイでアクティブ化されていることを確認します。
- E メールゲートウェイでメールボックス自動修復機能が有効になっていることを確認します。電子メールゲートウェイでのアカウント設定の有効化を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] を選択します。

ステップ 2 [メールボックス自動修復（Mailbox Auto Remediation）] の [有効化（Enable）] をクリックします。

ステップ 3 [メールボックス自動修復の有効化（Enable Mailbox Auto Remediation）] チェックボックスを選択します。

ステップ 4 URL レピュテーション判定が「悪意がある」に変更された時点でエンドユーザーに送信されるメッセージに対して実行する修復アクションを設定します。

- [電子メールアドレスに転送（Forward to an email address）]：指定したユーザー（たとえば、電子メール管理者など）に悪意のある URL を転送する場合は、このオプションを選択します。
- [メッセージの削除（Delete the message）]：悪意のある URL をエンドユーザーのメールボックスから完全に削除する場合は、このオプションを選択します。
- [指定した電子メール アドレスに転送してメッセージを削除（Forward to an email address and delete the message）]。指定したユーザー（たとえば、電子メール管理者など）に悪意のある URL を転送して、悪意のある添付ファイルをエンドユーザーのメールボックスから完全に削除する場合は、このオプションを選択します。

（注） Office 365 サービスでは特定のフォルダからのメッセージの削除をサポートしていないため、それらのフォルダ（[削除済みアイテム（Deleted Items）] など）からメッセージを削除することはできません。

（注） [メールボックス自動修復（Mailbox Auto Remediation）] の設定を確定する前に、メールボックスでのメッセージの修復 を確認します。

ステップ 5 変更を送信し、保存します。

コンテンツ フィルタを使用した、メッセージの悪意のある URL の検出

‘URL Reputation’ コンテンツ フィルタを使用して、ETF によって悪意があるとして分類されたメッセージの URL を検出し、これらのメッセージに対して適切なアクションを実行します。

ETF の ‘URL Reputation’ コンテンツ フィルタは、以下のいずれかの方法で設定できます。

- 'URL Reputation' の条件と適切なアクションを使用する。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない。
- 'URL Reputation' の条件とアクションを使用する。

'URL Reputation' の条件とアクションを使用して悪意のある URL を検出するには、以下の手順を使用します。

（注）
- 'URL Reputation' の条件と任意の適切なアクションを使用するには、手順のステップ 11 ～ 20 は無視してください。
- 'URL Reputation' アクションと任意の条件を使用するか、条件を使用しない場合は、手順のステップ 4 ～ 10 は無視してください。

始める前に

- 電子メールゲートウェイで URL フィルタリングが有効にされていることを確認します。URL フィルタリングを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [URLフィルタリング（URL Filtering）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （1 ページ）を参照してください。
- 電子メールゲートウェイでアウトブレイクフィルタが有効にされていることを確認します。アウトブレイク フィルタを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [アウトブレイクフィルタ（Outbreak Filters）] ページに移動します。詳細については、アウトブレイク フィルタを参照してください。
- 電子メールゲートウェイでスパム対策エンジンが有効にされていることを確認します。スパム対策エンジンを有効にするには、Web インターフェイスの [セキュリティサービス（ecurity Services）] > [スパム対策（Anti-Spam）] ページに移動します。詳細については、スパムおよびグレイメールの管理を参照してください。
- （任意）URL リストを作成します。作成するには、Web インターフェイスで [メールポリシー（Mail Polices）] > [URLリスト（URL Lists）] ページに移動します。詳細については、悪意のある URL または望ましくない URL からの保護 （1 ページ）を参照してください。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

ステップ 2 [フィルタの追加（Add Filter）] をクリックします。

ステップ 3 コンテンツ フィルタの名前と説明を入力します。

ステップ 4 [条件を追加（Add Condition）] をクリックします。

ステップ 5 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 6 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 7 悪意のある URL を検出する ETF ソースを選択します。

ステップ 8 （任意）電子メールゲートウェイで脅威を検出しない許可リストに登録されている URL のリストを選択します。

ステップ 9 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [アクションを追加（Add Action）] をクリックします。

ステップ 12 [URLレピュテーション（URL Reputation）] をクリックします。

ステップ 13 [外部脅威フィード（External Threat Feeds）] を選択します。

ステップ 14 条件（ステップ 7）で選択した ETF ソースと同じ ETF ソースを選択したことを確認します。

ステップ 15 （任意）ステップ 8 で選択したものと同じ許可リストに登録されている URL のリストを選択します。

ステップ 16 メッセージの本文および件名および/またはメッセージの添付ファイルの悪意のある URL を検出するために必要な [次に含まれるURLを確認（Check URLs within）] オプションを選択します。

ステップ 17 メッセージの本文および件名および/またはメッセージの添付ファイルの URL に対して実行する必要なアクションを選択します。

（注） ステップ 16 で [（次に含まれるURLを確認）Check URLs within] オプションに [添付ファイル（Attachments）] を選択した場合、メッセージから添付ファイルを除去することのみが可能です。

ステップ 18 すべてのメッセージにアクションを実行するか、未署名のメッセージにアクションを実行するかを選択します。

ステップ 19 [OK] をクリックします。

ステップ 20 変更を送信し、保存します。

（注） Web ベースのレピュテーションスコア（WBRS）と電子メールゲートウェイの ETF に対して URL レピュテーション コンテンツ フィルタを設定している場合は、電子メールゲートウェイのパフォーマンスを向上するために、WBRS URL レピュテーション コンテンツ フィルタの順序を ETF URL レピュテーションフィルタの順序よりも高く設定することをお勧めします。

メッセージフィルタを使用した、メッセージの悪意のある URL の検出

例として、ETF エンジンを使用して悪意のあるメッセージの URL を検出し、URL を無効化するには、‘URL Reputation’ のメッセージ フィルタ ルール構文を使用します。

構文：

```
defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
<'URL_allowedlist'>,
<’message_attachments'> , <’message_body_subject’> ,))
{ url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

引数の説明

- ‘url-external-threat-feeds’ は、URL レピュテーションのルールです。
- ‘etf_source1’ は、メッセージまたはメッセージの添付ファイルの悪意のある URL を検出するために使用される ETF ソースです。
- 「URL_allowedlist」は、URL 許可リストの名前です。URL の許可リストが存在しない場合は「""」と表示されます。
- 'message_attachments' は、メッセージの添付ファイルの悪意のある URL をチェックするために使用します。メッセージの添付ファイルの悪意のある URL を検出するには '1' の値を使用します。
- 'message_body_subject' は、メッセージ本文と件名の悪意のある URL をチェックするために使用します。メッセージの本文と件名の悪意のある URL を検出するには '1' の値を使用します。

（注） メッセージの本文、件名、添付ファイルの悪意のある URL を検出するには '1,1' の値を使用します。

- ‘url-etf-defang’ は、悪意のある URL を含むメッセージに対して実行できるアクションの 1 つです。

  以下の例は、悪意のある URL を含むメッセージに対して適用できる ETF ベースのアクションです。

- url-etf-strip(['etf_source1'],"None", 1)
- url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
- url-etf-defang-strip(['etf_source1'], "None", 1)
- url-etf-proxy-redirect(['etf_source1'], "None", 1)
- url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
- url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
- url-etf-replace(['etf_source1'], "", "None", 1)
- url-etf-replace(['etf_source1'], "URL removed", "None", 1)
- url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
- url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- 'Preserve_signed' は、'1' または '0' で表されます。'1' は、このアクションが未署名のメッセージのみに適用されることを示し、'0' はこのアクションがすべてのメッセージに適用されることを示します。

以下の例では、ETF エンジンによってメッセージの添付ファイルで悪意のある URL が検出された場合、添付ファイルが除去されます。

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

URL フィルタリング結果のモニタ

検出された悪意のある URL およびニュートラルな URL に関するデータを表示するには、[モニタ（Monitor）] > [URL フィルタ（URL Filtering）] を選択します。このページのデータの詳細については、[URL フィルタリング（URL Filtering）] ページを参照してください。

ユーザーのメールボックスから修復された悪意のある URL を含むメッセージに関するデータを表示するには、[URL レトロスペクション（URL Retrospection）] ページを参照してください。

メッセージ トラッキングの URL 詳細の表示

アウトブレイク フィルタおよび関連するコンテンツ フィルタによって取得された URL のメッセージ トラッキングの詳細を表示するには、以下のことが必要です。

- メッセージ トラッキングが有効になっている必要があります。
- アウトブレイク フィルタおよび/または、URL レピュテーションもしくは URL カテゴリに基づくコンテンツ フィルタが稼働している必要があります。

- アウトブレイク フィルタについては、URL 書き換えが有効になっている必要があります。URL 書き換えおよびドメインのバイパスを参照してください。
- URL ロギングが有効になっている必要があります。URL のロギングと URL のメッセージ トラッキングの詳細の有効化を参照してください。
- URL レトロスペクティブ判定更新に基づいてユーザーのメールボックスから修復された悪意のある URL を持つメッセージに関する詳細を [メッセージトラッキング（Message Tracking）] に表示するには、メールボックス修復を有効にする必要があります。メールボックスでのメッセージの修復を参照してください。

表示されるデータの詳細については、メッセージ トラッキングの詳細 を参照してください。

これらの潜在的な機密情報に対する管理ユーザのアクセスを管理するには、メッセージ トラッキングでの機密情報へのアクセスの制御を参照してください。

URL フィルタリングのトラブルシューティング

関連項目

- ログの表示 （27 ページ）
- アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （27 ページ）
- アラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （27 ページ）
- Talos インテリジェンスサービスに接続できない （28 ページ）
- アラート：シスコ アグリゲータ サーバに接続できない（Unable to Connect to the Cisco Aggregator Server） （28 ページ）
- アラート：シスコ アグリゲータ サーバから Web インタラクション トラッキング情報を取得できない（Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server） （29 ページ）
- websecurityadvancedconfig コマンドの使用 （30 ページ）
- メッセージ トラッキング検索で指定のカテゴリのメッセージが見つからない （30 ページ）
- 悪意のある URL とマーケティング メッセージがアンチスパム フィルタまたはアウトブレイク フィルタでキャプチャされない （30 ページ）
- フィルタリングされたカテゴリの URL が正しく処理されない （31 ページ）
- エンドユーザが書き換え後の URL から悪意のあるサイトにアクセスする （31 ページ）
- Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （31 ページ）

アラートの表示

以下の表では、URL フィルタリングエンジンによって生成されるシステムアラートを記載しています。アラートの説明、アラートの重大度などが含まれます。

コンポーネント/アラート名	メッセージと説明	パラメータ
ECS REMEDIATION_INITIATION	アラートテキスト：「悪意のあるURLを持つメッセージに対してメール修復が開始されました：$message_id : $url（Mail remediation initiated for messages messages with malicious URLs: $message_id : $url）」 情報：ユーザーのメールボックスに既に配信されている悪意のあるURLを修復するために修復サービスによって開始されたメールボックス修復が成功または失敗したときに送信されるアラート。	• **message_id**：URL を含むメッセージのメッセージID。 • **url**：レトロスペクティブ判定を受け取る URL。
ECS 情報	アラートテキスト：「URL レトロスペクティブサービスから更新を受信しました。メッセージID、MID、およびURLの形式は $message_id : $mid : $url です。（Verdict update received from URL retrospective service. The message IDs, MIDs, and URLs are as below in the format: $message_id : $mid : $url）」 情報：メールゲートウェイがレトロスペクティブサーバーからURL レトロスペクティブ判定を受信したときに送信されるアラート。	• **message_id**：URL を含むメッセージのメッセージID。 • **mid**：メッセージ識別番号。 • **url**：レトロスペクティブ判定を受け取る URL。

コンポーネント/アラート名	メッセージと説明	パラメータ
ECS クリティカル	アラートテキスト：URL レピュテーションに関するレトロスペクティブ判定を受信するためのポーリングが、無効な証明書エラーで失敗しました。Cisco TAC に連絡して、サポートを受けてください。 警告：証明書が無効なために、メールゲートウェイがレトロスペクティブサーバーからの URL レトロスペクティブ判定を受信できなかった場合に送信されるアラート。Cisco TAC に連絡して、サポートを受けてください。	[該当なし（N/A）]
ECS 警告	アラートテキスト：URL レトロスペクティブ ポーリング サービスを再起動して、不正な要求形式を修正します。 警告：ポーリング要求の形式を修正するために、URL レトロスペクティブ ポーリング サービスを再起動するようにアラートが送信されました。	[該当なし（N/A）]
ECS クリティカル	接続エラー：レトロスペクティブ登録サービスに接続できません。Cisco TAC に連絡して、サポートを受けてください。 失敗の理由 • 無効な証明書エラー • クラウドサービスを利用できません。 • 接続要求が拒否されました（例：無効な証明書キー）。	該当なし

ログの表示

URL フィルタリング情報は、次のログに書き込まれます。

- メール ログ（mail_logs）。URL のスキャン結果に関する情報は（URL に応じてメッセージに対して実行されるアクション）、このログに書き込まれます。
- URL フィルタリング ログ（web_client）。URL ルックアップの試行時のエラー、タイムアウト、ネットワークの問題などに関する情報は、このログに書き込まれます。
- 修復ログ。このログには、URL レトロスペクティブサービスに基づくメールボックスの修復に関連する情報が投稿されます。
- Email Cloud Scanner ログRetrospective クラウドスキャナーから受信した URL レトロスペクティブ判定に関連する情報。

ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。ログの詳細については、ログを参照してください。

ユーザがメッセージに含まれているリダイレクトリンクをクリックしたときに発生する動作に関する情報は、ログには記録されません。

ログ内の「SDS」は、URL レピュテーションサービスを示します。「Beaker コネクタ」は Talos エンジンを指します。

アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate）

問題

登録クライアント証明書の取得中に発生したエラーに関する情報レベルのアラートを受信します。

解決方法

この証明書は、Talos インテリジェンスサービス（URL レピュテーションと URL カテゴリを取得するため）および Cisco Aggregator Server（Web インタラクション トラッキング データを取得するため）のクラウドベースのサービスに接続する必要があります。次のことを試してください。

1. ネットワークの問題（誤ったプロキシ設定やファイアウォールの問題など）が発生しているかどうかを確認します。
2. URL フィルタリング機能キーが有効であり、アクティブであることを確認します。
3. 問題が解決しない場合は、Cisco TAC にご連絡ください。

アラート：Beakerコネクタ：証明書が無効です（CertificateIsInvalid）

問題

無効な Beaker コネクタの証明書に関する重大なアラートを受信しました。

ソリューション

この証明書は、URL レピュテーションとカテゴリを取得する目的でクラウド内の Talos インテリジェンスサービスに接続する際に必要です。

証明書を取得して手動でインストールする場合は、Talos インテリジェンスサービスとの通信に必要な証明書の手動設定 （31 ページ）を参照してください。

Talos インテリジェンスサービスに接続できない

問題

[セキュリティサービス（Security Services）] > [URLフィルタリング（URL Filtering）] ページに、Talos インテリジェンスサービスへの接続の問題が継続的に示されます。

解決方法

- URL フィルタリングを有効にしているが変更をまだ確定していない場合は、変更を確定します。
- Talos インテリジェンスサービスとの接続に関する最新のアラートを確認します。最新アラートの表示を参照してください。該当する場合は、アラート：Beaker コネクタ：登録証明書の取得中のエラー（Error Fetching Enrollment Certificate） （27 ページ）およびアラート：Beaker コネクタ：証明書が無効です（Certificate Is Invalid） （27 ページ）を参照してください。
- [セキュリティ サービス（Security Services）]>[サービスのアップデート（Service Updates）] で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
- 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
- URL フィルタリングログで、Talos クライアントへのタイムアウト要求に関連するエラーが示されている場合は、コマンドライン インターフェイスで websecuritydiagnostics コマンドおよび **websecurityadvancedconfig** コマンドを使用し、調査および変更を行います。
  - 応答時間が、設定されている URL ルックアップタイムアウト以上である場合は、URL ルックアップタイムアウトの値を適宜増やします。
- URL スキャナ、Cisco Web セキュリティサービス、または Talos クライアントとの通信でタイムアウト以外のエラーが発生しているかどうかを URL フィルタリングログで確認します。ログに「Talos client」と記録されている場合、これは Talos インテリジェンスサービスを示します。このようなログメッセージを見つけた場合は、TAC にご連絡ください。

アラート：シスコ アグリゲータ サーバに接続できない（Unable to Connect to the Cisco Aggregator Server）

問題

次の警告アラートを受信：Cisco Aggregator Server に接続できません。

ソリューション

次の手順を実行します。

1. 電子メールゲートウェイからサーバのホスト名を ping して、電子メールゲートウェイと Cisco Aggregator Server との接続を確認します。CLI で aggregatorconfig コマンドを使用して、Cisco Aggregator Server のホスト名を表示します。
2. [セキュリティサービス（Security Services）]>[サービスのアップデート（Service Updates）] で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
3. 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
4. DNS サービスが実行されているかどうかを確認します。
5. 問題が解決しない場合は、Cisco TAC にご連絡ください。

アラート：シスコ アグリゲータ サーバから Web インタラクション トラッキング情報を取得できない（Unable to Retrieve Web Interaction Tracking Information from the Cisco Aggregator Server）

問題

次の警告アラートを受信：Cisco Aggregator Server から Web インタラクション トラッキング情報を取得できません。

ソリューション

次の手順を実行します。

1. [セキュリティ サービス（Security Services）]>[サービスのアップデート（Service Updates）] で指定されたプロキシを経由して接続している場合は、これが設定されており、正常に機能していることを確認します。
2. 接続を妨げている可能性があるネットワークの問題が他にあるかどうかを確認します。
3. DNS サービスが実行されているかどうかを確認します。
4. 問題が解決しない場合は、Cisco TAC にご連絡ください。

アラート：Email Cloud Scanner（ECS）：証明書が無効です

問題

無効な ECS コネクタの証明書に関する重大なアラートを受信しました。

解決方法

Email Cloud Scanner クライアントによるレトロスペクティブサーバー証明書の検証が失敗しました。この証明書は、クライアントに接続して URL レトロスペクティブ アップデートを取得するために必要です。このエラーを修正するには、シスコサポートに連絡してください。

アラート：Email Cloud Scanner（ECS）：ネットワークが到達不能です

問題

メールゲートウェイが URL Retrospective クラウドスキャナーサービスに到達できない場合は、重大なアラートを受け取ります。

解決方法

ファイアウォール設定を確認します。ネットワーク管理者に連絡して支援を受けます。

websecurityadvancedconfig コマンドの使用

本書で明示的に説明する変更を除き、TAC からの指示を受けずに websecurityadvancedconfig コマンドを使用して変更を行わないでください。

メッセージトラッキング検索で指定のカテゴリのメッセージが見つからない

問題

特定のカテゴリの URL が含まれているメッセージが、そのカテゴリでの検索で見つかりませんでした。

解決方法

予想されるメッセージが検索結果に表示されない を参照してください。

悪意のある URL とマーケティング メッセージがアンチスパム フィルタまたはアウトブレイク フィルタでキャプチャされない

問題

マーケティング リンクを含むメッセージと悪意のある URL が、アンチスパム フィルタまたはアウトブレイク フィルタによってキャプチャされません。

解決方法

- これは、Web サイトのレピュテーションとカテゴリは、アンチスパム フィルタとアウトブレイク フィルタがサイトについて判定するときに使用する多数の条件の 2 つに過ぎないために発生することがあります。アクション（URL の書き換え、URL のテキストでの置き換え、メッセージの隔離またはドロップなど）の実行に必要なしきい値を低くすることで、これらのフィルタの感度を上げることができます。詳細については、アウトブレイク フィルタ機能とメール ポリシー および スパム対策ポリシーの定義 を参照してください。あるいは、URL レピュテーション スコアに基づくコンテンツ フィルタまたはメッセージ フィルタを作成します。

- またこれは、電子メールゲートウェイが Talos インテリジェンスサービスに接続できない場合に発生することもあります。Talos インテリジェンスサービスに接続できない （28 ページ） を参照してください。

フィルタリングされたカテゴリの URL が正しく処理されない

問題

URL カテゴリに基づくコンテンツ フィルタまたはメッセージ フィルタで定義されているアクションは、適用されません。

解決方法

- トレース機能を使用してメッセージ処理パスを追跡します（トレース機能についてはトラブルシューティングに関する章で説明します）。
- これは、電子メールゲートウェイが Talos インテリジェンスサービスに接続できない場合に発生することがあります。Talos インテリジェンスサービスに接続できない （28 ページ）を参照してください。
- 接続に問題がない場合でも、URL を分類できないか、誤って分類することがあります。未分類の URL と誤って分類された URL の報告 （48 ページ）を参照してください。URL のカテゴリを判別するときにこのサイトを使用できます。

エンドユーザが書き換え後の URL から悪意のあるサイトにアクセスする

問題

悪意のある URL が Cisco Web セキュリティ プロキシにリダイレクトされましたが、エンドユーザがそのサイトにアクセスできます。

解決方法

これは次の場合に発生する可能性があります。

- サイトが悪意のあるサイトとして識別されていない。
- Cisco Web セキュリティ プロキシへの接続がタイムアウトした。このタイムアウトが発生することは非常にまれです。ネットワークの問題が原因で接続が妨げられていないことを確認します。

Talos インテリジェンスサービスとの通信に必要な証明書の手動設定

この手順は、 電子メールゲートウェイが Talos インテリジェンスサービスとの通信に必要な証明書を自動的に取得できない場合に使用します。

手順

ステップ 1 必須の証明書の取得

ステップ 2 [ネットワーク（Network）] > [証明書（Certificates）] を使用するか、またはコマンドライン インターフェイスで certconfig コマンドを使用して、証明書をアップロードします。

ステップ 3 コマンドライン インターフェイスで **websecurityconfig** コマンドを入力します。

ステップ 4 プロンプトに従って、Talos インテリジェンスサービス認証用のクライアント証明書を設定します。

URL カテゴリについて

関連項目

- URL カテゴリについて （32 ページ）
- URL のカテゴリの判別 （48 ページ）
- 未分類の URL と誤って分類された URL の報告 （48 ページ）
- 将来の URL カテゴリ セットの変更 （49 ページ）

URL カテゴリについて

これらの URL カテゴリは、AsyncOS の最近のリリースで Web セキュリティ アプライアンスに使用されているカテゴリと同じです。

URL カテゴリ	省略形	コード（Code）	説明	URL の例
アダルト（Adult）	adlt	1006	アダルト コンテンツを指しますが、ポルノだけではありません。アダルト向けのナイトクラブ（ストリップ クラブ、スワッピング クラブ、同伴サービス、ストリッパーなど）、セックスに関する全般情報（ポルノとは限らない）、性器ピアス、アダルト向けの製品やグリーティング カード、健康や疾病関連以外の性行為に関する情報なども含まれることがあります。	www.adultentertainmentexpo.com www.adultnetline.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
アドバタイズメント（Advertisements）	adv	1027	Web ページに表示されることの多いバナー広告やポップアップ広告。広告コンテンツを提供しているその他の広告関連 Web サイト。広告サービスおよび広告営業は、[事業および産業（Business and Industry）] カテゴリに分類されます。	www.adforce.com www.doubleclick.com
アルコール（Alcohol）	alc	1077	嗜好品としてのお酒、ビールやワインの醸造、カクテルのレシピ、リキュール販売、ワイナリー、ブドウ園、ビール工場、アルコール類の販売元など。アルコール中毒は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。バーおよびレストランは [飲食（Dining and Drinking）] カテゴリに分類されます。	www.samueladams.com www.whisky.com
芸術（Arts）	art	1002	画廊および展示会、芸術家および芸術作品、写真、文学および書籍、舞台芸術および劇場、ミュージカル、バレエ、美術館、デザイン、建築。映画およびテレビは [エンターテイメント（Entertainment）] に分類されます。	www.moma.org www.nga.gov
占星術（Astrology）	astr	1074	占星術、ホロスコープ、占い、数霊術、霊能者による助言、タロット。	www.astro.com www.astrology.com
オークション（Auctions）	auct	1088	オンラインまたはオフラインのオークション、オークション会社、オークション案内広告など。	www.craigslist.com www.ebay.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ビジネスおよび産業（Business and Industry）	busi	1019	マーケティング、商業、企業、ビジネス手法、労働力、人材、運輸、給与、セキュリティとベンチャーキャピタル、オフィス用品、産業機器（プロセス用機器）、機械と機械系、加熱装置、冷却装置、資材運搬機器、包装装置、製造、立体処理、金属製作、建築と建築物、旅客輸送、商業、工業デザイン、建築、建築資材、出荷と貨物（貨物取扱業務、トラック輸送、運送会社、トラック輸送業者、貨物ブローカと輸送ブローカ、優先サービス、荷高と貨物のマッチング、追跡とトレース、鉄道輸送、海上輸送、ロードフィーダ サービス、移動と保管）。	www.freightcenter.com www.staples.com
チャットおよびインスタント メッセージ（Chat and Instant Messaging）	chat	1040	Web ベースのインスタントメッセージングおよびチャット ルーム。	www.icq.com www.meebo.com
不正および盗用（Cheating and Plagiarism）	plag	1051	不正行為を助長し、学期末論文（盗用したもの）などの書物を販売したりします。	www.bestessays.com www.superiorpapers.com
児童虐待コンテンツ（Child Abuse Content）	cprn	1064	世界中の違法な児童性的虐待コンテンツ。	—

URL カテゴリ	省略形	コード（Code）	説明	URL の例
コンピュータセキュリティ（Computer Security）	csec	1065	企業ユーザおよび家庭ユーザ向けのセキュリティ製品およびセキュリティ サービス。	www.computersecurity.com www.symantec.com
コンピュータおよびインターネット（Computers and Internet）	comp	1003	コンピュータおよびソフトウェアに関する情報（ハードウェア、ソフトウェア、ソフトウェア サポートなど）、ソフトウェア エンジニア向けの情報、プログラミング、ネットワーク、Web サイト設計、Web およびインターネット全般、コンピュータ科学、コンピュータ グラフィック、クリップアートなど。フリーウェアとシェアウェアは、[フリーウェアおよびシェアウェア（Freeware and Shareware）] カテゴリに分類されます。	www.xml.com www.w3.org
出会い系（Dating）	date	1055	出会い系サイト、結婚紹介所など。	www.eharmony.com www.match.com
デジタル ポストカード（Digital Postcards）	card	1082	デジタルはがきおよび電子カードの送信。	www.all-yours.net www.delivr.net
飲食（Dining and Drinking）	food	1061	飲食店、レストラン、バー、居酒屋、パブ、レストラン ガイド、レストラン レビューなど。	www.hideawaybrewpub.com www.restaurantrow.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ダイナミックおよびレジデンシャル（Dynamic and Residential）	dyn	1091	ブロードバンドリンクの IP アドレス。通常は、ホームネットワークへのアクセスを試みているユーザを指します。たとえば、ホームコンピュータへのリモートセッションの場合などです。	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
教育（Education）	edu	1001	教育関連の Web サイト。たとえば、学校、短大、大学、教材、教師用資料、技術訓練、職業訓練、オンライントレーニング、教育問題、教育政策、学資援助、学校助成金、規範、試験など。	www.education.com www.greatschools.org
エンターテイメント（Entertainment）	ent	1093	映画、音楽、バンド、テレビ、芸能人、ファン サイト、エンターテイメントニュース、芸能界のゴシップ、エンターテイメントの会場などに関する詳細や批評など。[芸術（Arts）] カテゴリとの違いを確認してください。	www.eonline.com www.ew.com
過激（Extreme）	extr	1075	性的暴力または犯罪性のあるもの、暴力および暴力的行為、悪趣味な写真や血まみれの写真（解剖写真など）、犯行現場、犯罪被害者、事故被害者の写真、過度にわいせつな文章や写真、衝撃的な内容の Web サイトなど。	www.car-accidents.com www.crime-scene-photos.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ファッション（Fashion）	fash	1076	衣料、服飾、美容室、化粧品、アクセサリ、宝飾品、香水、身体改造に関連する図表や文章、タトゥー、ピアス、モデル事務所など。皮膚科関連製品は[健康および栄養（Health and Nutrition）]カテゴリに分類されます。	www.fashion.net www.findabeautysalon.com
ファイル転送サービス（File Transfer Services）	fts	1071	ダウンロードサービスおよびホスティングによるファイル共有を主目的とするファイル転送サービス	www.rapidshare.com www.yousendit.com
フィルタリング回避（Filter Avoidance）	filt	1025	検出されない匿名の Web 利用を促進および支援する Web サイト。例：cgi、php、および glype を使用した匿名プロキシサービス。	www.bypassschoolfilter.com www.filterbypass.com
金融（Finance）	fnnc	1015	会計実務、会計士、課税、税、銀行、保険、投資、国家経済、個人資産管理（各種保険、クレジット カード、個人退職金積立計画、遺産相続計画、ローン、住宅ローン）などの金融や財務関連のもの。株は[オンライン トレード（Online Trading）]に分類されます。	finance.yahoo.com www.bankofamerica.com
フリーウェアおよびシェアウェア（Freeware and Shareware）	free	1068	フリー ソフトウェアおよびシェアウェア ソフトウェアのダウンロードを提供します。	www.freewarehome.com www.shareware.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ギャンブル（Gambling）	gamb	1049	カジノ、オンライン ギャンブル、ブックメーカー、オッズ、ギャンブルに関する助言、ギャンブルの対象となっているレース、スポーツ ブッキング、スポーツ ギャンブル、株式スプレッドベッティング サービス。ギャンブル中毒に関する Web サイトは、[健康および栄養（Health and Nutrition）] カテゴリに分類されます。国営宝くじは、[宝くじ（Lotteries）] カテゴリに分類されます。	www.888.com www.gambling.com
ゲーム（Games）	game	1007	さまざまなカード ゲーム、ボード ゲーム、ワード ゲーム、ビデオ ゲーム、戦闘ゲーム、スポーツ ゲーム、ダウンロード型ゲーム、ゲーム批評、攻略本、コンピュータ ゲーム、インターネット ゲーム（ロールプレイング ゲームなど）。	www.games.com www.shockwave.com
政府および法律（Government and Law）	gov	1011	政府 Web サイト、外交関係、政府および選挙に関するニュースや情報、法律家、法律事務所、法律関連の出版物、法律関連の参考資料、裁判所、訴訟事件一覧表、法律関連の協会などの法律分野に関する情報、立法および判例、市民権問題、移民関連、特許、著作権、法執行制度および矯正制度に関する情報、犯罪報道、法的措置、犯罪統計、軍事（軍隊、軍事基地、軍組織）/テロ対策など。	www.usa.gov www.law.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ハッキング（Hacking）	hack	1050	Web サイト、ソフトウェア、およびコンピュータのセキュリティを回避する方法に関する議論。	www.hackthissite.org www.gohacking.com
ヘイト スピーチ（Hate Speech）	hate	1016	社会集団、肌の色、宗教、性的指向、障がい、階級、民族、国籍、年齢、性別、性同一性を基に、憎悪、不寛容、差別を助長する Web サイト。人種差別を扇動するサイト、性差別、人種差別の神学、人種差別の音楽、ネオナチ組織、特定民族至上主義、ホロコースト否定論。	www.kkk.com www.nazi.org
健康および栄養（Health and Nutrition）	hlth	1009	健康管理、疾病および障がい、医療、病院、医師、医薬品、精神衛生、精神医学、薬理学、エクササイズおよびフィットネス、身体障がい、ビタミン剤およびサプリメント、健康にかかわる性行為（疾病および健康管理）、喫煙、飲酒、薬物使用、健康にかかわるギャンブル（疾病および健康管理）、食物全般、飲食、調理およびレシピ、食物と栄養、健康維持および食事療法、レシピや料理に関する Web サイトを含む料理全般、代替医療など。	www.health.com www.webmd.com
ユーモア（Humor）	lol	1079	ジョーク、スケッチ、コミック、その他のユーモラスなコンテンツ。不快感を与える可能性のあるアダルト ユーモアは [アダルト（Adult）] に分類されます。	www.humor.com www.jokes.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
違法行為（Illegal Activities）	ilac	1022	窃盗、不正行為、電話ネットワークへの不法アクセスなどの犯罪を助長するサイト、コンピュータ ウィルス、テロリズム、爆弾、無秩序、殺人や自殺を描写したものやその実行方法を記述した Web サイト。	www.ekran.no www.thedisease.net
違法ダウンロード（Illegal Downloads）	ildl	1084	著作権契約に違反してソフトウェア保護を回避するための、ソフトウェア、シリアル番号、キー生成ツールなどをダウンロードできる Web サイト。Torrent は [ピアファイル転送（Peer File Transfer）] に分類されます。	www.keygenguru.com www.zcrack.com
違法ドラッグ（Illegal Drugs）	drug	1047	気晴らしのためのドラッグ、ドラッグ摂取の道具、ドラッグの購入と製造に関する情報。	www.cocaine.org www.hightimes.com
インフラストラクチャおよびコンテンツ配信ネットワーク（Infrastructure and Content Delivery Networks）	infr	1018	コンテンツ配信インフラおよび動的に生成されるコンテンツ、セキュリティで保護されているか、または分類が困難なために細かく分類できない Web サイトなど。	www.akamai.net www.webstat.net
インターネット電話（Internet Telephony）	v oip	1067	インターネットを利用した電話サービス。	www.evaphone.com www.skype.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
求職（Job Search）	job	1004	職業に関する助言、履歴書の書き方、面接に関するスキル、就職斡旋サービス、求人データバンク、職業紹介所、人材派遣会社、雇用主の Web サイトなど。	www.careerbuilder.com www.monster.com
下着および水着（Lingerie and Swimsuits）	ling	1031	下着および水着。特にモデルが着用している Web サイト。	www.swimsuits.com www.victoriassecret.com
宝くじ（Lotteries）	lotr	1034	宝くじ、コンテストおよび国が運営する宝くじ。	www.calottery.com www.flalottery.com
携帯電話（Mobile Phones）	cell	1070	Short Message Services（SMS; ショート メッセージ サービス）、着信音などの携帯電話用ダウンロード サービス。携帯電話会社の Web サイトは、[ビジネスおよび産業（Business and Industry）] カテゴリに分類されます。	www.cbfsms.com www.zedge.net
自然（Nature）	natr	1013	天然資源、生態学および自然保護、森林、原生地、植物、草花、森林保護、森林、原生林および林業、森林管理（再生、保護、保全、伐採、森林状態、間伐、計画的火入れ）、農作業（農業、ガーデニング、園芸、造園、種まき、除草、灌漑、剪定、収穫）、環境汚染問題（大気質、有害廃棄物、汚染防止、リサイクル、廃棄物処理、水質、環境産業）、動物、ペット、家畜、動物学、生物学、植物学。	www.enature.com www.nature.org

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ニュース（News）	news	1058	ニュース、ヘッドライン、新聞、テレビ局、雑誌、天気、スキー場の状態。	www.cnn.com news.bbc.co.uk
非政府組織（Non-Governmental Organizations）	ngo	1087	クラブ、圧力団体、コミュニティ、非営利組織および労働組合などの非政府組織。	www.panda.org www.unions.org
性的でないヌード（Non-Sexual Nudity）	nsn	1060	ヌーディズム、ヌード、自然主義、ヌーディストキャンプ、芸術的ヌードなど。	www.artenuda.com www.naturistsociety.com
オンライン コミュニティ（Online Communities）	comm	1024	アフィニティ グループ、Special Interest Group（SIG; 同じ興味を持つ人々の集まり）、Web ニュースグループ、Web 掲示板など。[プロフェッショナルネットワーキング（Professional Networking）] カテゴリまたは[ソーシャルネットワーキング（Social Networking）] カテゴリに分類される Web サイトはここには含まれません。	www.igda.org www.ieee.org
オンライン ストレージおよびバックアップ（Online Storage and Backup）	osb	1066	バックアップ、共有、およびホスティングを目的とした、オフサイト ストレージおよびピアツーピア型ストレージ	www.adrive.com www.dropbox.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
オンライン トレード（Online Trading）	trad	1028	オンライン証券会社、ユーザがオンラインで株取引できる Web サイト、株式市場、株式、債券、投資信託会社、ブローカー、株式市場の分析と解説、株式審査、株価チャート、IPO、株式分割に関する情報。株式スプレッド ベッティング サービスは [ギャンブル（Gambling）] に分類されます。その他の金融サービスは、[財務（Finance）] に分類されます。	www.tdameritrade.com www.scottrade.com
業務用電子メール（Organizational Email）	pem	1085	Outlook Web Access（OWA）などで業務用のメールを利用する際に使用する Web サイト。	—
パーク ドメイン（Parked Domains）	park	1092	広告ネットワークの有料リスティング サービスを利用してそのドメインのトラフィックから収益を得ようとする Web サイト、またはドメイン名を販売して収益を得ようと考えている「不正占拠者」が所有する Web サイト。有料広告リンクを返す偽の検索サイトも含まれます。	www.domainzaar.com www.parked.com
ピア ファイル転送（Peer File Transfer）	p2p	1056	ピアツーピア型のファイル要求 Web サイト。ファイル転送自体のトラッキングは行いません。	www.bittorrent.com www.limewire.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
個人サイト（Personal Sites）	pers	1081	個人が運営している個人関連の Web サイト、個人用ホームページサーバ、個人的コンテンツが公開されている Web サイト、特定のテーマがない個人ブログなど。	www.karymullis.com www.stallman.org
写真検索および画像（Photo Searches and Images）	img	1090	画像、写真、クリップアートの保存と検索を促進します。	www.flickr.com www.photobucket.com
政治（Politics）	pol	1083	政治家、政党、政治、選挙、民主主義、投票などに関連するニュースや情報の Web サイト。	www.politics.com www.thisnation.com
ポルノ（Pornography）	porn	1054	性的表現が露骨な文章または画像。性的表現が露骨なアニメや漫画、性的表現が露骨な描写全般、フェチ志向の文章や画像、性的表現が露骨なチャットルーム、セックスシミュレータ、ストリップポーカー、アダルト映画、わいせつな芸術、性的表現が露骨な Web メールなど。	www.redtube.com www.youporn.com
プロフェッショナル ネットワーキング（Professional Networking）	pnet	1089	キャリア開発や専門性開発を目的としたソーシャルネットワーキング。[ソーシャルネットワーキング（Social Networking）] も参照してください。	www.linkedin.com www.europeanpwn.net
不動産（Real Estate）	rest	1045	不動産の検索に役立つ情報、事務所および商業区画、賃貸、アパート、戸建てなどの不動産物件一覧、住宅建築など。	www.realtor.com www.zillow.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
参照	ref	1017	都道府県および市区町村の案内情報、地図、時刻、参照文献、辞書、図書館など	www.wikipedia.org www.yellowpages.com
宗教（Religion）	rel	1086	宗教に関するコンテンツ、宗教に関する情報、宗教団体。	www.religionfacts.com www.religioustolerance.org
SaaS および B2B（SaaS and B2B）	saas	1080	オンライン ビジネス サービス用 Web ポータル、オンライン会議など。	www.netsuite.com www.salesforce.com
子供向け（Safe for Kids）	kids	1057	幼児や児童向けに作成されているか、明示的に幼児や児童向けと認められている Web サイト。	kids.discovery.com www.nickjr.com
科学技術（Science and Technology）	sci	1012	科学技術（航空宇宙、電子工学、工学、数学など）、宇宙探査、気象学、地理学、環境、エネルギー（化石燃料、原子力、再生可能エネルギー）、通信（電話、電気通信）など。	www.physorg.com www.science.gov
検索エンジンおよびポータル（Search Engines and Portals）	srch	1020	検索エンジンなど、インターネット上の情報にアクセスするための起点となるサイト。	www.bing.com www.google.com
性教育（Sex Education）	sxed	1052	事実に基づいて性的情報を扱う Web サイト、性的健康、避妊、妊娠など	www.avert.org www.scarleteen.com
ショッピング（Shopping）	shop	1005	物々交換、オンライン購入、クーポン、無料提供、事務用品、オンライン カタログ、オンライン モールなど。	www.amazon.com www.shopping.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
ソーシャル ネットワーキング（Social Networking）	snet	1069	ソーシャル ネットワーキング関連。[プロフェッショナルネットワーキング（Professional Networking）] も参照してください。	www.facebook.com www.twitter.com
社会科学（Social Science）	socs	1014	社会に関係する科学と歴史、考古学、文化人類学、カルチュラル スタディーズ、歴史学、言語学、地理学、哲学、心理学、女性学。	www.archaeology.org www.anthropology.net
社会および文化（Society and Culture）	scty	1010	家族および家族関係、民族性、社会組織、家系、高齢者、保育など。	www.childcare.gov www.familysearch.org
ソフトウェア アップデート（Software Updates）	swup	1053	ソフトウェア パッケージに対する更新プログラムを提供している Web サイト。	www.softwarepatch.com www.versiontracker.com
スポーツおよびレクリエーション（Sports and Recreation）	sprt	1008	すべてのプロ スポーツおよびアマチュア スポーツ、レクリエーション活動、釣り、ファンタジー スポーツ（ゲーム）、公園、遊園地、レジャープール、テーマ パーク、動物園、水族館、温泉施設など。	www.espn.com www.recreation.gov
ストリーミング オーディオ（Streaming Audio）	aud	1073	リアルタイム ストリーミング オーディオ コンテンツ（インターネット ラジオやオーディオ フィードなど）。	www.live-radio.net www.shoutcast.com
ストリーミング ビデオ（Streaming Video）	vid	1072	リアルタイム ストリーミング ビデオ（インターネット テレビ、Web キャスト、動画共有など）。	www.hulu.com www.youtube.com

URL カテゴリ	省略形	コード（Code）	説明	URL の例
タバコ（Tobacco）	tob	1078	愛煙家の Web サイト、タバコ製造会社、パイプ、喫煙製品（違法薬物吸引用でないもの）など。タバコ依存は [健康および栄養（Health and Nutrition）] カテゴリに分類されます。	www.bat.com www.tobacco.org
乗り物（Transportation）	trns	1044	個人用の乗り物、自動車およびバイクに関する情報、新車、中古車、オートバイの購入、自動車愛好会、小型船舶、航空機、レジャー用自動車（RV）など。自動車レースおよびバイク レースは [スポーツおよびレクリエーション（Sports and Recreation）] に分類されます。	www.cars.com www.motorcycles.com
旅行（Travel）	trvl	1046	ビジネス旅行と個人旅行、旅行情報、トラベル リソース、旅行代理店、休暇利用のパック旅行、船旅、宿泊施設、交通手段、航空便の予約、航空運賃、レンタカー、別荘など。	www.expedia.com www.lonelyplanet.com
Unclassified	—	—	シスコのデータベースに存在しない Web サイトは、レポートのために未分類として記録されます。誤入力された URL もこれに含まれます。	—

URL カテゴリ	省略形	コード（Code）	説明	URL の例
武器（Weapons）	weap	1036	一般的な武器の購入および使用に関する情報（銃販売店、銃オークション、銃の案内広告、銃の付属品、銃の展示会、銃の訓練など）、銃に関する全般情報、その他の武器や狩猟関連画像のサイトなども含まれる場合があります。政府の軍に関する Web サイトは、[政府および法律（Government and Law）] カテゴリに分類されます。	www.coldsteel.com www.gunbroker.com
Web ホスティング（Web Hosting）	whst	1037	Web サイトのホスティング、帯域幅サービスなど。	www.bluehost.com www.godaddy.com
Web ページ翻訳（Web Page Translation）	tran	1063	Web ページの翻訳。	babelfish.yahoo.com translate.google.com
Web メール（Web-Based Email）	メール アドレス	1038	Web メール サービス。個人が自分の会社の電子メール サービスを利用するための Web サイトは、[業務用電子メール（Organizational Email）] カテゴリに分類されます。	mail.yahoo.com www.hotmail.com

URL のカテゴリの判別

特定の URL のカテゴリを確認するには、未分類の URL と誤って分類された URL の報告 （48 ページ）に示されているサイトを参照してください。

未分類の URL と誤って分類された URL の報告

誤って分類された URL や、未分類だが分類する必要がある URL を報告するには、次のサイトにアクセスしてください。

https://talosintelligence.com/reputation_center/support

送信された URL のステータスを確認するには、このページの [送信したURLのステータス（Status on Submitted URLs）] タブをクリックします。

将来の URL カテゴリ セットの変更

新たな流行やテクノロジーの出現に伴い、URL カテゴリ セットが変更されることがまれにあります。たとえば、カテゴリの追加、削除、名前変更、別のカテゴリとの結合、2 つのカテゴリへの分割などです。このような変更は既存のフィルタの結果に影響することがあるので、変更が生じた場合は、 電子メールゲートウェイからアラート（[システム（System）] タイプ、[警告（Warning）] 重大度）が送信されます。このようなアラートを受信したら、コンテンツ フィルタとメッセージフィルタを評価し、場合によっては、更新されたカテゴリで機能するようにこれらのフィルタを更新する必要があります。既存のフィルタは自動的には変更されません。確実にアラートが届くようにするには、アラート受信者の追加を参照してください。

次の変更では、カテゴリ セットの変更は不要であり、アラートは生成されません。

- 新たに分類されたサイトの定期的な分類。
- 誤って分類されたサイトの再分類

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。