



# ルックアップ

以下のトピックでは、Firepower システムで既知の（または未知の）エンティティに関する情報を検索する方法について説明します。

- ルックアップの概要（1 ページ）
- Whois ルックアップの実行（1 ページ）
- URL カテゴリとレビューションの検索（2 ページ）
- IP アドレスの地理位置情報の検出（3 ページ）

## ルックアップの概要

Firewall Management Center がインターネットに接続している場合、手動ルックアップ機能を使って次の情報を検索できます。

- 任意の IP アドレスについての Regional Information Registries (RIR) 情報 (whois)。
- URL フィルタリング機能によって分類された URL カテゴリおよびレビューション。
- 任意の IP アドレスについての地理位置情報（国名、国番号および大陸名）（最新の地理位置情報を確実に使用するように、Firewall Management Center 上の地理位置情報データベース (GeoDB) を定期的に更新することを強くお勧めします）。

## Whois ルックアップの実行

始める前に

- Firewall Management Center がインターネットにアクセスできることを確認します。セキュリティ、インターネットアクセス、および通信ポートを参照してください。

## 手順

ステップ1 [分析 (Analysis)] > [詳細 (Advanced)] > [Whois] を選択します。

ステップ2 IP アドレスを入力して、[検索 (Search)] をクリックします。

## URL カテゴリとレビューの検索

URL のカテゴリとレビューは手動で検索できます。この機能は、ポリシー処理を計画、調整、またはトラブルシューティングするために特定の URL をどのように評価するかを確認する場合や、Cisco ソリューションの外部のソースから明らかになる問題のある可能性のある URL を調査する場合に使用します。次に示す結果のカテゴリとレビューは、URL フィルタリング機能で使用されているものと同じです。

## 始める前に

- Firewall Management Center はインターネットにアクセスできる必要があります。セキュリティ、インターネットアクセス、および通信ポートを参照してください。
- URL フィルタリングと [不明な URL を Cisco Cloud に問い合わせる (Query Cisco cloud for unknown URLs)] オプションを有効にする必要があります。Cisco Secure Firewall Management Center デバイス構成ガイドの「the URL Filtering」の章を参照してください。
- 少なくとも 1 台のデバイスが Firewall Management Center に登録されており、そのデバイスには有効な URL フィルタリング ライセンスが割り当てられている必要があります。
- このタスクを実行するには、管理者ユーザーまたはセキュリティ アナリストユーザーである必要があります。

## 手順

ステップ1 [分析 (Analysis)] > [詳細 (Advanced)] > [URL] を選択します。

ステップ2 最大 250 個の URL およびパブリックなルーティング可能 IP アドレスを一般的な任意の形式で入力します（たとえば、URL には "http"、"www" またはサブドメインが含まれていても、省略されていてもよく、短縮形式であってもかまいません）。各エンティティは、スペースまたは改行で区切ります。

アスタリスク (\*) などのワイルドカードはサポートされていません。

ステップ3 [検索 (Search)] をクリックします。

入力した URL が多数あり、ネットワークが遅い場合は、処理に数分かかることがあります。

URL が無効であることを示すエラー メッセージが表示された場合は、スペリングを確認するか、URL の別のバリエーションを試行します。たとえば、「www」、「http」、「https」などのプレフィックスを追加または省略します。

URL は最大 6 つのカテゴリに属する可能性がありますが、レピュテーションは 1 つのみです。

**ステップ 4** (オプション) 列ヘッダーをクリックして、結果をソートします。

**ステップ 5** (オプション) CSV ファイルとして結果を保存するには、[CSV のエクスポート (Export CSV)] をクリックします。

CSV ファイルには、レピュテーション レベル用の追加の列が含まれているため、リスク基準でのソートが可能です。ゼロ (0) は、システムにリスクデータが不足している URL に対する不明なリスクを表しています。

### 次のタスク

有効なカテゴリとレピュテーションのリストを表示する場合は、[ポリシー (Policies)] > [アクセス制御 (Access Control)] > [アクセス制御 (Access Control)] に移動し、ポリシーをクリックするか新しいポリシーを追加して、[ルールの追加 (Add Rule)] をクリックし、[URL (URLs)] をクリックします。

## IP アドレスの地理位置情報の検出

地理位置情報ルックアップ機能を使用して、国名、ISO 3166-1 の 3 桁の国番号と、任意の IP アドレスに関連付けられた大陸名を検索します。

### 手順

**ステップ 1** [分析 (Analysis)] > [詳細 (Advanced)] > [地理位置情報 (Geolocation)] を選択します。

**ステップ 2** 1 つ以上の IP アドレスの地理位置情報を表示するには、アドレス (複数可) を入力して、[検索 (Search)] をクリックします。IPv4 アドレス、IPv6 アドレスのいずれか、または両方を指定できます。複数のアドレスは、カンマ、セミコロン、改行、スペース文字を使用して区切ります。

#### ヒント

テキストボックスをクリアするには、[クリア (Clear)] をクリックします。

**ステップ 3** データを並べ替えるには、列見出しをクリックします。IP アドレスを除くすべてのフィールドによって並べ替えが可能です。

**ステップ 4** (オプション) CSV として結果を保存するには、[CSV をエクスポートする (Export CSV)] をクリックします。

## ■ IP アドレスの地理位置情報の検出

## 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。