



ルックアップの使用

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 カテゴリとレピュテーションの検索](#)（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

Firepower 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 カテゴリおよびレピュテーション。
- 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、Firepower 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)。

関連トピック

[地理位置情報データベース \(GeoDB\) の更新](#)

Whois ルックアップの実行

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

始める前に

- Firepower 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)] > [ルックアップ (Lookup)] > [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。

関連トピック

[コンテキストメニュー](#)

URL カテゴリとレピュテーションの検索

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
URL フィルタリング	URL フィルタリング	Management Center	任意 (Any)	Admin/Any Security Analyst

URL のカテゴリとレピュテーション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ピュテーションは、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

- Firepower Management Center はインターネットにアクセスする必要があります。[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 フィルタリングが、Firepower Management Center で有効になっている必要があります。[集合型セキュリティ インテリジェンスでの通信の設定](#)を参照してください。

手順

ステップ1 [分析 (Analysis)] > [ルックアップ (Lookup)] > [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、カンマ、セミコロン、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" や "http(s)" のプレフィックスを省略します。

URL は最大 6 つのカテゴリに属する可能性があります。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、レピュテーションスコア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、不明なリスクを表します。

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、[ルール追加 (AddRule)] をクリックし、[URL (URLs)] タブをクリックします。

IP アドレスの地理位置情報の検出

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	Management Center	任意 (Any)	任意 (Any)

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)] > [ルックアップ (Lookup)] > [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。

関連トピック

[地理位置情報データベース \(GeoDB\) の更新](#)