

Umbrellaダッシュボードの新機能について

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[新しい機能](#)

[これらの機能の活用方法](#)

[ファイル検査](#)

[ファイル検査のテスト](#)

[宛先リストでURLをブロックできるようにする](#)

[レポート](#)

[包括フィードバックの送信](#)

はじめに

このドキュメントでは、Umbrellaダッシュボードの宛先リストによるファイルインスペクションとカスタムURLブロックについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Umbrellaダッシュボードに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

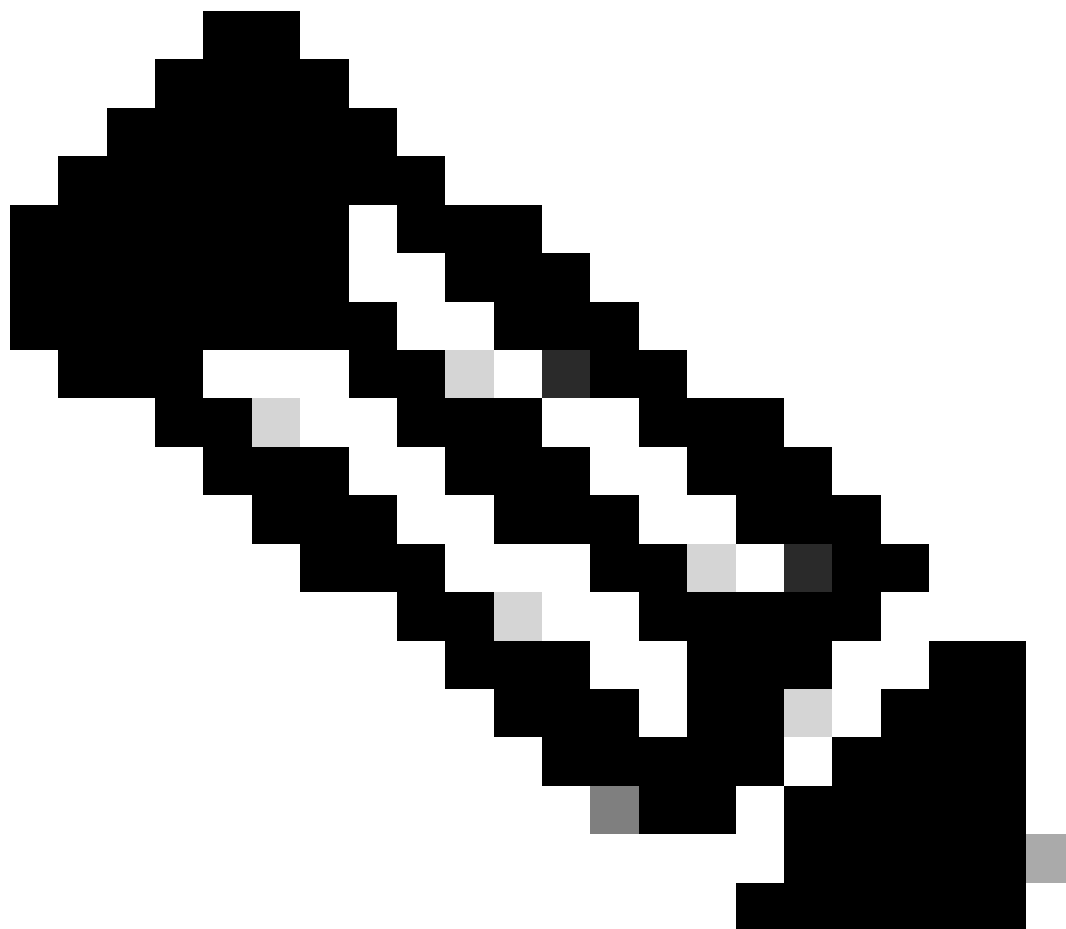
新しい機能

Umbrellaは、機能を向上させる新しい機能セットを提供します。この変更により、ダッシュボードに次の2つの新機能が追加されました。

- ファイルインスペクションは、IDがダウンロードしたファイルをスキャンして、悪意のあるコードが含まれているかどうかを確認し、含まれている場合はブロックします。

- ・ カスタムブロックURLを使用すると、宛先リスト内の独自のURLセットをブロックできます。これにより、ドメイン全体をブロックすることなく、特定のページをブロックする柔軟性が得られます。

この新機能を利用するには、新しいレポートと更新されたレポート、および新しいポリシー作成の機能を使用できます。ファイルインスペクション機能は、クラウドベースのセキュリティをさらに強化するインテリジェントプロキシインフラストラクチャの拡張を中心とした今後のリリースで計画されている機能の1つです。



注：これらの機能はお客様に合わせて徐々に展開されており、Umbrellaはこのリリースで徐々に拡張されるため、これらのアップデートは限定公開となっています。これらの機能に関するアラートがダッシュボードに表示された場合は、その機能を使用できます。これらの機能の詳細については、umbrella-support@cisco.comまでお問い合わせください。

ファイルインスペクション機能は、Umbrella InsightsまたはUmbrellaプラットフォームパッケージを使用しているお客様だけが利用できます。 [パッケージの詳細](#)については、シスコの代理店に

お問い合わせください。

これらの機能の活用方法

これらの新機能には、いくつかの場所からアクセスできます。ポリシーウィザードでは、概要ページからファイルインスペクションを有効にし、宛先リストを使用して、ブロックする宛先リストにカスタムURLを追加できます。また、カスタムURLブロックは、宛先リスト管理ページから個別に管理することもできます。

レポート側では、Umbrellaダッシュボードのレポートナビゲーションセクションが更新され、新しいレポートや更新されたレポートを簡単に検索できるようになりました。これらの機能を有効にする方法と、いくつかのレポートを確認する方法については、この記事の詳細を参照してください。

ファイル検査

ファイルインスペクションはインテリジェントプロキシの機能で、疑わしいドメインでホストされる悪意のあるコンテンツをファイルでスキャンする機能を追加することで、範囲と機能を拡張します。疑わしいドメインは信頼されておらず、悪意があるかどうかは不明です。

Umbrellaポリシーウィザードを使用すると、ファイルインスペクションを簡単に実装できます。Policies > Policy Listの順に移動し、ポリシーを展開するか、+ (追加) アイコンを選択して新しいポリシーを作成します。ポリシーウィザードで、サマリーページのファイルインスペクションが有効になっていることを確認します。または、インテリジェントプロキシを有効にした後で(詳細設定の下で)、新しいポリシーからファイルのインスペクションを選択します。 [詳細については、この機能の完全なドキュメントを参照してください。](#)

ファイル検査のテスト

ファイルインスペクションが有効なポリシーに登録されているデバイスから：

1. <http://proxy.opendnstest.com/download/eicar.com> を参照します。
2. 次のスクリーンショットのようなブロックページが表示されます。



This site is blocked due to a security threat.

http://proxy.opendnstest.com/download/eicar.com

Diagnostic Info

傘でブロックされたページ

宛先リストでURLをブロックできるようにする

URLをブロックするには、ブロックする送信先リストに入力するか、URL専用の新しいブロックする送信先リストを作成します。そのためには、Policies > Destination Listsの順に移動し、Destination listを展開し、URLを追加して、Saveを選択します。

A list of bad URLs

Destinations on this list will be **BLOCKED**

Enter a Domain or CIDR IP Range

ADD TO LIST

If a destination exists in both a blocked and allowed list, allowed destinations take precedence.

Destination	Type	Comments	
example.com/malware.php	URL	Add a comment	✖
domain.com/block.html	URL	Add a comment	✖

CANCEL

SAVE

包括ブロックされた宛先リスト

[詳細については、この機能の完全なドキュメントを参照してください。](#)

UmbrellaインフラストラクチャがURLを検査して、ブロックする宛先リストで定義されているURLと一致するかどうかを判断するには、次の条件が満たされている必要があります。

- ポリシーの一部として、インテリジェントプロキシとSSL復号化を有効にする必要があります。詳細については、[Umbrellaに関するドキュメント](#)を参照してください。

- Cisco UmbrellaルートCAは、このポリシーを使用してコンピュータにインストールする必要があります。これにより、https接続も確実にフィルタリングされます。詳細については、[Umbrellaに関するドキュメント](#)を参照してください。

ポリシー内の内容がユーザがアクセスしようとしている内容と一致する（そしてその後ブロックされる）ように、URLを正しく指定することが重要です。使用できる、または使用できないURLの詳細については、「[カスタムURL宛先リストの手引き](#)」を参照してください。

レポート

Umbrellaの新しいレポートと改善されたレポート：

- セキュリティ概要レポート：ネットワークアクティビティのスナップショットをグラフやチャートで簡単に確認できます。自分のIDとそのトラフィックのアクティビティを迅速に確認し、問題が発生している可能性のある場所を示すことができます。詳細については、[Umbrellaのドキュメントを参照してください](#)。
- セキュリティアクティビティレポート：Umbrella脅威インテリジェンスによってフラグ付けされているが、必ずしもブロックされていないセキュリティイベントを強調表示します。これには、インテリジェントプロキシおよびファイルインスペクションを使用してフィルタリングされたセキュリティイベントが含まれます。詳細については、[Umbrellaのドキュメントを参照してください](#)。
- アクティビティ検索レポート：さまざまなIDからのすべてのDNS、URL、およびIP要求の結果を日時の降順に並べて検索できます。このレポートには、選択した期間におけるUmbrella内のセキュリティ関連のアクティビティがすべて一覧表示されます。フィルタを使用して検索対象を絞り込み、必要な項目のみを表示できます。詳細については、[Umbrellaのドキュメントを参照してください](#)。

これらのレポートも簡単に入手できます。

包括フィードバックの送信

Umbrellaでは、これらの新機能についてどのように考えているか説明します。質問やコメントがあれば、Umbrellaから聞いてみましょう。フィードバックはumbrella-support@cisco.comに送信し、できるだけ詳細に記述してください。たとえば、スクリーンショット、使用しているブラウザ、OS、およびこれらの機能を使用しているシナリオなどがあります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。