Web セキュリティ管理の例

この章は、次の項で構成されています。

Web セキュリティ管理の例

この付録では、Cisco コンテンツ セキュリティ管理アプライアンスの機能を導入するいくつかの一般的な方法について説明します。内容は次のとおりです。

Web セキュリティ アプライアンスの例

このセクションでは、セキュリティ管理アプライアンスと Web セキュリティ アプライアンスを使用する例について説明します。

（注） これらのシナリオはすべて、セキュリティ管理アプライアンスおよび Web セキュリティ アプライアンスで Web レポーティングおよび Web トラッキングが有効であることを前提としています。Web トラッキングおよび Web レポーティングをイネーブルにする方法については、中央集中型 Web レポーティングおよびトラッキングの使用を参照してください。

例 1：ユーザの調査

次に、システム管理者が会社で特定のユーザを調査する例を示します。

このシナリオでは、ある従業員が勤務中に不適切な Web サイトにアクセスしている、という苦情を管理者が受け取っています。それを調査するには、システム管理者が Web アクティビティの詳細をトラッキングする必要があります。

Web セキュリティ管理の例

Webアクティビティをトラッキングすると、従業員の参照履歴に関する情報が記載されたWebレポートが作成されます。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）]>[レポート（Reporting）]>[ユーザ（Users）]を選択します。

ステップ 2 [ユーザ（Users）]テーブルで、調査する[ユーザID（User ID）]または[クライアントIPアドレス（Client IP address）]をクリックします。

ユーザ ID またはクライアント IP アドレスがわからない場合は、ユーザ ID またはクライアント IP アドレスをわかる範囲でテキスト フィールドに入力し、[ユーザIDまたはクライアントIPアドレスの検索（Find User ID or Client IP address）]をクリックします。IP アドレスが正確に一致していなくても結果は返されます。[ユーザ（Users）]テーブルに、指定したユーザ ID およびクライアント IP アドレスが入力されます。この例では、クライアント IP アドレス `10.251.60.24` の情報について検索しています。

ステップ 3 IP アドレス [10.251.60.24] をクリックします。

`10.251.60.24` の [ユーザの詳細（User Details）] ページが表示されます。

ユーザの詳細ページから総トランザクション別のURLカテゴリ、総トランザクション別のトレンド、一致するURLカテゴリ、一致するドメイン、一致するアプリケーション、検出されたマルウェアの脅威、および一致するポリシーを確認できます。

これらのカテゴリによって、`10.251.60.24` のユーザがブロックされている URL（ページの [ドメイン（Domains）]セクションに含まれる[ブロックされたトランザクション（Transactions Blocked）]列に表示）にアクセスしようとしていたことなどがわかります。

ステップ 4 [一致したドメイン（Domains Matched）]テーブルの下の [エクスポート（Export）] をクリックし、ユーザがアクセスしようとしていたドメインおよび URL のリストを表示します。

ここから Web トラッキング機能を使用して、この特定のユーザの Web 使用状況をトラッキングし、表示できます。

（注） Webレポーティングでは、アクセスされる特定のURLに限らず、ユーザがアクセスするすべてのドメイン情報を取得できる点に注意してください。ユーザがアクセスしている特定のURL、そのURL にアクセスした時刻、その URL が許可されているかどうかなどの情報を得るには、[Webトラッキング（Web Tracking）] ページの [プロキシサービス（Proxy Services）] タブを使用します。

ステップ 5 [ウェブ（Web）]>[レポート（Reporting）]>[Webトラッキング（Web Tracking）]を選択します。

ステップ 6 [プロキシサービス（Proxy Services）] タブをクリックします。

ステップ 7 [ユーザ/クライアントIPアドレス（User/Client IP Address）]テキスト フィールドにユーザ名または IP アドレスを入力します。

この例では、ユーザ `10.251.60.24` の Web トラッキング情報を検索します。

検索結果が表示されます。

このページから、IPアドレス`10.251.60.24`に割り当てられているコンピュータのユーザがアクセスしたトランザクションおよびURLのすべてのリストを確認できます。

関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

表 *1*：ユーザの調査の関連項目

機能名	機能情報
[ユーザ（User）] ページ	[ユーザ（Users）] レポート（Web）
[ユーザの詳細（User Details）] ページ	[ユーザの詳細（User Details）]（Web レポーティング）
レポート データのエクスポート	レポーティング データおよびトラッキング データのエクスポート
[Webトラッキング（Web Tracking）] ページの [プロキシサービス（Proxy Services）] タブ	Web プロキシ サービスによって処理されたトランザクションの検索

例 2：URL のトラッキング

このシナリオでは、セールスマネージャが、会社のサイトへのアクセスで、先週の上位5位を知りたい場合を考えます。さらに、どのユーザがこれらの Web サイトにアクセスしているかについても知りたいとします。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）] > [レポート（Reporting）] > [Web サイト（Web Sites）] を選択します。

ステップ 2 [時間範囲（Time Range）] ドロップダウン リストから [週（Week）] を選択します。

ステップ 3 [ドメイン（Domains）] セクションをスクロール ダウンすると、アクセスされているドメインまたは Web サイトが表示されます。

アクセス上位 25 位までの Web サイトは、[一致したドメイン（Domains Matched）] テーブルに表示されます。同じテーブルで [ドメイン（Domain）] または [IP] 列のリンクをクリックすると、特定のアドレスまたはユーザが参照した実際の Web サイトを確認できます。

関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

表 *2: URL* のトラッキングの関連項目

機能名	機能情報
[Webサイト（Web Sites）]ページ	[Web サイト（Web Sites）] レポート

例 3：アクセス数の多い URL カテゴリの調査

このシナリオでは、従業員が最近 30 日間にアクセスした上位 3 位までの URL を、人事部長が知りたい場合を考えます。また、ネットワーク管理者が、帯域幅の使用上をモニタしたり、ネットワークで最も帯域幅を使用している URL を特定したりするためにこの情報を取得するとします。

次の例は、複数の観点を持つ複数の人のためにデータを収集するが、生成するレポートは1つだけで済む方法を示します。

ステップ 1 セキュリティ管理アプライアンスで、[ウェブ（Web）] > [レポート（Reporting）] > [URL カテゴリ（URL Categories）] を選択します。

この例の [URLカテゴリ（URL Categories）] ページによると、総トランザクション別の上位 10 の URL カテゴリ グラフから、Instant Messaging、Hate Speech、Tattoo サイトなどの他に、282 k の未分類の URL にアクセスしていることがわかります。

ここで、[エクスポート（Export）] リンクをクリックして raw データを Excel スプレッドシートにエクスポートすると、このファイルを人事部長に送信できます。ネットワーク マネージャに URL ごとの帯域幅の使用量を知らせる必要があります。

ステップ 2 新しい ILLO が必要です - スキップ [使用帯域幅（Bandwidth Used）] 列を表示するには、[一致した URL カテゴリ（URL Categories Matched）] テーブルまでスクロールします。

[一致したURLカテゴリ（URL Categories Matched）] テーブルで、すべての URL カテゴリの帯域幅の使用量を確認することができます。もう一度 [エクスポート（Export）] リンクをクリックして、このファイルをネットワーク管理者に送信します。さらに細かく調べるには、[インスタントメッセージ（Instant Messaging）] リンクをクリックすると、どのユーザが帯域幅を大量に使用しているかが特定されます。次のページが表示されます。

このページから、ネットワーク管理者が Instant Messaging サイトの上位 10 ユーザを知ることができます。

このページから、最近 30 日間で 10.128.4.64 のユーザが Instant Messaging サイトに 19 時間 57 分アクセスしており、この期間の帯域幅の使用量が 10.1 MB であることがわかります。

関連項目

次の表にこの例で説明する各トピックをリストします。各項目の詳細については、リンクをクリックしてください。

Web セキュリティ管理の例

表 *3:* アクセスの多い *URL* カテゴリの調査の関連項目

機能名	機能情報
[URLカテゴリ（URL Categories）]ページ	[URLカテゴリ（URL Categories）] レポート
レポート データのエクスポート	レポーティング データおよびトラッキング データのエクスポート

Web セキュリティ管理の例