レポートとアラート

この章で説明する内容は、次のとおりです。

- エンドユーザーのアクティビティをモニターするレポートの生成 （1 ページ）
- セキュア アプライアンス レポート （14 ページ）
- 新しい Web インターフェイスでのセキュア アプライアンス レポート （33 ページ）

エンドユーザーのアクティビティをモニターするレポートの生成

この章で説明する内容は、次のとおりです。

- レポートの概要 （1 ページ）
- レポート ページの使用 （3 ページ）
- 新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）
- レポートの有効化 （10 ページ）
- レポートのスケジュール設定 （10 ページ）
- オンデマンドでのレポートの生成 （12 ページ）
- アーカイブ レポート （13 ページ）
- L4 トラフィック モニタ レポートのトラブルシューティング （13 ページ）

レポートの概要

SecureWeb Applianceでは概要レポートが生成されるので、ネットワークで起きていることを把握したり、特定のドメイン、ユーザ、カテゴリのトラフィックの詳細を表示することができます。レポートを実行して特定の期間内のシステムアクティビティをインタラクティブに表示したり、レポートをスケジュールして定期的に実行することができます。

関連項目

- レポート ページからのレポートの印刷とエクスポート （8 ページ）

レポートでのユーザー名の使用

認証をイネーブルにすると、Webプロキシで認証される際に、ユーザーはユーザー名でレポートに一覧表示されます。デフォルトでは、ユーザー名は認証サーバーに表示されるとおりに書き込まれます。ただし、すべてのレポートでユーザー名を識別できないようにすることができます。

（注） 管理者の場合は、常にレポートにユーザー名が表示されます。

手順

ステップ 1 [セキュリティサービス（Security Services）]>[レポート（Reporting）]を選択し、[設定を編集（Edit Settings）]をクリックします。

ステップ 2 [ローカルレポート（Local Reporting）] で、[レポートでユーザー名を匿名にする（Anonymize usernames in reports）] を選択します。

ステップ 3 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

レポート ページ

SecureWeb Applianceには以下のレポートがあります。

- マイ ダッシュボード（My Dashboard）（レポートの「ホームページ」。メニュー バーの左端にある [ホーム（Home）] アイコンをクリックしてアクセスすることもできます。）
- 概要
- Users
- ユーザ数（User Count）
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- Secure Endpoint
- ファイル分析（File Analysis）

- Cisco Secure Endpoint 判定の更新
- クライアント マルウェア リスク（Client Malware Risk）
- Web レピュテーション フィルタ（Web Reputation Filters）
- L4 トラフィック モニター（L4 Traffic Monitor）
- SOCKS プロキシ（SOCKS Proxy）
- ユーザの場所別レポート（Reports by User Location）
- Web トラッキング（Web Tracking）
- システム容量（System Capacity）
- システム ステータス（System Status）
- スケジュール設定されたレポート（Scheduled Reports）
- アーカイブ レポート（Archived Reports）

レポート ページの使用

さまざまなレポート ページにシステム アクティビティの概要が表示され、システム データを表示するための複数のオプションがあります。Webサイトおよびクライアント固有のデータをページごとに検索することもできます。

レポート ページでは、以下のタスクが実行できます。

オプション	タスクへのリンク
レポートで表示する時間範囲を変更する	時間範囲の変更 （3 ページ）
特定のクライアントとドメインを検索する	データの検索 （5 ページ）
チャートに表示するデータを選択する	チャート化するデータの選択 （5 ページ）
レポートを外部ファイルにエクスポートする	レポート ページからのレポートの印刷とエクスポート （8 ページ）

時間範囲の変更

[時間範囲（Time Range）] フィールドを使用して、各セキュリティ コンポーネントの表示データを更新できます。このオプションを使用して、定義済みの時間範囲のアップデートを生成できます。また、開始時刻と終了時刻を指定してカスタム時間範囲を定義することもできます。

（注） 選択した時間範囲は、[時間範囲（Time Range）] メニューで異なる値を選択するまで、すべてのレポート ページ全体で使用されます。

時間範囲	返されるデータ
時間（Hour）	60 分間と、追加で最大 5 分間
日（Day）	直近の 24 時間とその時点の 1 時間未満の時間を含めた時間に対して 1 時間間隔
週（Week）	直近の 7 日間にその時点の日にちを足した日数に対して 1 日間隔
月（30 日）（Month (30 days)）	直近の 30 日間にその時点の日にちを足した日数に対して 1 日間隔
昨日（Yesterday）	SecureWeb Applianceに定義されているタイム ゾーンを使用した直近の 24 時間（00:00 から 23:59）
カスタム範囲（Custom Range）	定義済みのカスタム時間範囲。 [カスタム範囲（Custom Range）] を選択すると、開始時刻と終了時刻を入力できるダイアログボックスが表示されます。

（注） すべてのレポートで、システム設定のタイム ゾーンに基づき、グリニッジ標準時（GMT）オフセットで日付および時刻情報が表示されます。ただし、データ エクスポートでは、世界の複数のタイム ゾーンの複数のシステムに対応するためにのみ、GMT で時刻が表示されます。

レポートの時間範囲の選択

ほとんどの事前定義レポート ページでは、含まれるデータの時間範囲を選択できます。選択した時間範囲は、[時間範囲（Time Range）] メニューで異なる値を選択するまで、すべてのレポート ページに対して使用されます。

使用可能な時間範囲オプションは、アプライアンスごとに異なり、またセキュリティ管理アプライアンス上の電子メール レポーティングおよび Web レポーティングによって異なります。

（注） レポート ページの時間範囲は、グリニッジ標準時（GMT）オフセットで表示されます。たとえば、太平洋標準時は、GMT + 7 時間（GMT + 07:00）です。

（注） すべてのレポートで、システム設定の時間帯に基づき、グリニッジ標準時（GMT）オフセットで日付および時刻情報が表示されます。ただし、データ エクスポートでは、世界の複数のタイム ゾーンの複数のシステムに対応するために、GMT で時刻が表示されます。

データの検索

一部のレポートには、特定のデータ ポイントを検索するために使用できるフィールドがあります。データを検索するときに、レポートは検索する特定のデータ セットのレポート データを調整します。入力する文字列に完全に一致する値や入力する文字列で始まる値を検索できます。以下のレポート ページには検索フィールドがあります。

検索フィールド	説明
ユーザー（Users）	ユーザー名またはクライアント IP アドレスでユーザーを検索します。
Web サイト（Web Sites）	ドメインまたはサーバーの IP アドレスでサーバーを検索します。
URL カテゴリ（URL Categories）	URL カテゴリを検索します。
アプリケーションの表示（Application Visibility）	AVC または ADC エンジンがモニターし、ブロックするアプリケーション名を検索します。
クライアント マルウェア リスク（Client Malware Risk）	ユーザー名またはクライアント IP アドレスでユーザーを検索します。

（注） クライアント IP アドレスおよびクライアント ユーザー ID を表示するには、認証を設定する必要があります。

チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。チャートのオプションは、レポートのテーブルの列見出しと同じです。

手順

ステップ 1 チャートの下の [チャートオプション（Chart Options）] をクリックします。

ステップ 2 表示するデータを選択します。

ステップ 3 [完了（Done）] をクリックします。

カスタム レポート

既存のレポートのページからチャート（グラフ）とテーブルを組み合わせてカスタム レポートのページを作成できます。

目的	操作内容
カスタム レポート ページにモジュールを追加	参照先： • カスタム レポートに追加できないモジュール （6 ページ）。 • カスタム レポート ページの作成 （6 ページ）
カスタム レポート ページの表示	1. [モニター（Monitor）] > [メール（Email）] または [Web] > [レポート（Reporting）] > [レポート（Reporting）] > [マイ レポート（My Reports）] を選択します。 2. 表示する時間範囲を選択します選択した時間範囲は [マイ レポート（My Reports）] ページのすべてのモジュールを含むすべてのレポートに適用されます。 新しく追加されたモジュールは関連するセクションの上部に表示されます。
カスタム レポート ページでのモジュールの再配置	目的の場所にモジュールをドラッグ アンド ドロップします。
カスタム レポート ページからのモジュールの削除	モジュールの右上にある [X] をクリックします。
カスタム レポートの PDF または CSV バージョンの生成	[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択し、[今すぐレポートを生成（Generate Report Now）] をクリックします。
カスタム レポートの PDF または CSV バージョンの定期的な生成	[レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

カスタム レポートに追加できないモジュール

- 検索結果（Web トラッキングの検索結果を含む）

カスタム レポート ページの作成

始める前に

- 追加するモジュールが追加可能であることを確認します。カスタム レポートに追加できないモジュール （6 ページ）を参照してください。

- モジュールの右上の [X] をクリックして、不要なデフォルト モジュールを削除します。

手順

ステップ 1 以下のいずれかの方法でカスタム レポート ページにモジュールを追加します。

（注）
一部のモジュールは、以下のいずれかの方法を使用した場合のみ利用できます。ある方式を使用してモジュールを追加できない場合は、別の方法を試してください。

- 追加するモジュールがある [メール（Email）] タブまたは [Web] タブのレポート ページに移動し、モジュールの上部にある [+]ボタンをクリックします。
- [レポート（Reporting）]>[マイレポート（My Reports）] に移動し、[+]ボタン（いずれかのセクションの上部にあります）をクリックして、追加するレポート モジュールを選択します。目的のモジュールを見つけるには、[マイ レポート（My Reports）] ページの各セクションにある [+] ボタンをクリックしなければならない場合があります。

  各モジュールは一度だけ追加できます。すでに特定のモジュールをレポートに追加している場合は、追加オプションが利用できなくなっています。

ステップ 2 カスタマイズした（たとえば、カラムの追加、削除、または順序変更をした、あるいはチャートにデフォルト以外のデータを表示した）モジュールを追加する場合は、これらのモジュールを [マイ レポート（My Reports）] ページでカスタマイズします。

モジュールがデフォルト設定に追加されます。元のモジュールの時間範囲は保持されません。

ステップ 3 別に凡例を持つチャート（たとえば、[概要（Overview）] ページからのグラフ）を追加する場合は、別途凡例を追加します。必要に応じて、説明するデータの隣にドラッグ アンド ドロップします。

レポートおよびトラッキングにおけるサブ ドメインとセカンド レベル ドメインの比較

レポーティングおよびトラッキングの検索では、セカンドレベルのドメイン（http://george.surbl.org/two-level-tldsに表示されている地域ドメイン）は、ドメイン タイプがサブドメインと同じように見えますが、サブドメインとは別の方法で処理されます。次に例を示します。

- レポートには、`co.uk` などの 2 レベルのドメインの結果は含まれませんが、`foo.co.uk` の結果は含まれます。レポートには、`cisco.com` などの主要な企業ドメインの下にサブドメインが含まれます。
- 地域ドメイン `co.uk` に対するトラッキング検索結果には、`foo.co.uk` などのドメインは含まれませんが、`cisco.com` に対する検索結果には `subdomain.cisco.com` などのサブドメインが含まれます。

レポート ページからのレポートの印刷とエクスポート

ページ右上隅の [印刷可能（PDF）（Printable (PDF)）] リンクをクリックすると、すべてのレポートページを印刷形式の PDF 版で生成できます。また、[エクスポート（Export）] リンクをクリックして、未処理データをカンマ区切り形式（CSV）ファイルとしてエクスポートすることもできます。

CSV エクスポートには未処理データのみが含まれるため、Web ベースのレポート ページからエクスポートされたデータには、パーセンテージなどの計算データが含まれていない場合があります（そのデータが Web ベースのレポートで表示される場合でも、含まれていない場合があります）。

レポート データのエクスポート

ほとんどのレポートには、未処理データをカンマ区切り形式（CSV）のファイルにエクスポートできる [エクスポート（Export）] リンクが用意されています。CSV ファイルにデータをエクスポートすると、Microsoft Excel などのアプリケーションを使用し、データにアクセスして処理することができます。

エクスポートされた CSV データは、 SecureWeb Applianceでのタイム ゾーン設定にかかわらず、すべてのメッセージトラッキングおよびレポーティングデータをグリニッジ標準時（GMT）で示します。GMT 時間への変換の目的は、アプライアンスに依存せずにデータを使用したり、複数のタイム ゾーンにあるアプライアンスからのデータを参照する際にデータを使用したりできるようにするためです。

以下の例は、Anti-Malware カテゴリ レポートの raw データ エクスポートのエントリであり、太平洋夏時間（PDT）が GMT 7 時間で表示されています。

```
 Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
  Transactions Monitored, Transactions Blocked, Transactions Detected
  1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

カテゴリ ヘッダー	値	説明
タイムスタンプ開始（Begin Timestamp）	1159772400.0	エポックからの秒数で表されたクエリ開始時刻。
タイムスタンプ終了（End Timestamp）	1159858799.0	エポックからの秒数で表されたクエリ終了時刻。
開始日（Begin Date）	2006-10-02 07:00 GMT	クエリの開始日。
End Date	2006-10-03 06:59 GMT	クエリの終了日。
Name	Adware	マルウェア カテゴリの名前。
Transactions Monitored	525	モニタリングされたトランザクション数。
Transactions Blocked	2100	ブロックされたトランザクション数。

カテゴリ ヘッダー	値	説明
検出されたトランザクション（Transactions Detected）	2625	トランザクションの総数＝（検出されたトランザクションの数）＋（ブロックされたトランザクションの数）。

（注） カテゴリ ヘッダーは、レポートのタイプごとに異なります。

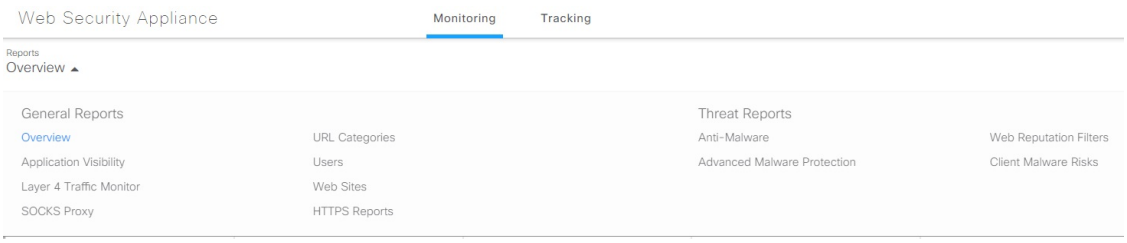
ローカライズされた CSV データをエクスポートすると、ブラウザによっては見出しが正しく表示されない場合があります。これは、ブラウザによっては、ローカライズされたテキストに対して適切な文字セットが使用されない場合があることから発生します。この問題の回避策として、ローカル マシンにファイルを保存し、[ファイル（File）] > [開く（Open）] を使用して任意の Web ブラウザでファイルを開きます。ファイルを開いたら、ローカライズされたテキストを表示するための文字セットを選択します。

新しい Web インターフェイスでのインタラクティブ レポート ページの使用

次の図に示す [レポート（Reports）] ドロップダウンを使用すると、 SecureWeb Applianceのレポートを表示することができます。

（注） [概要（Overview）] レポートページは、ランディングページ（ログイン後に表示されるページ）です。レポートまたはトラッキングページから新しい Web インターフェイスをリロードすると、デフォルトのランディングページ（[概要（Overview）] レポートページ）がロードされます。

図 *1*: レポートドロップダウン



Web レポートは、**一般的なレポート**と**脅威レポート**に分類されます。

新しい Web インターフェイスにアクセスするには、「新しい Web インターフェイスでのセキュア アプライアンス レポート」を参照してください。

関連項目

- （Web レポートのみ）チャート化するデータの選択 （66 ページ）

レポートの有効化

組織に複数の SecureWeb Applianceがあり、Cisco コンテンツ セキュリティ管理アプライアンスを使用して集約レポートのデータを管理および表示する場合、各 SecureWeb Applianceで集約管理レポートを有効にする必要があります。

アプライアンスの設定に基づいてレポートのタイプを選択できます。すべてのレポートをローカルで保存できます。。組織に複数の SecureWeb Applianceがあり、Cisco コンテンツセキュリティ管理アプライアンスを1つ使用している場合は、集約管理レポートを選択して集約したレポートデータを管理および表示できます。集約管理レポート、またはローカルレポートを選択すると、各 SecureWeb Applianceにこれらの設定が適用されます。

手順

ステップ 1 **[セキュリティサービス（Security Services）]** > **[レポート（Reporting）]** を選択し、[設定を編集（Edit Settings）] をクリックします。

a) アプライアンスでレポートを有効にする場合は、[ローカル レポート（Local Reporting）] をオンにします。アプライアンス ポータルにログインした後、レポートにアクセス可能になります。

b) Cisco コンテンツ セキュリティ管理アプライアンスを介してレポートを使用可能にする場合は、[集中管理レポート（Centralized Reporting）] をオンにします。

SecureWeb Applianceのみが、ローカル レポートについて収集されたすべてのデータを保存します。集約管理レポートがアプライアンスで有効な場合、 SecureWeb Applianceはシステム容量データとシステムステータスデータのみを保持します。これらは SecureWeb Applianceでローカルに使用できる唯一のレポートです。

管理アプライアンスでのこの機能の設定については、Cisco コンテンツセキュリティ管理アプライアンス ユーザー ガイドの集約管理 Web レポートの使用とトラッキングに関するトピックを参照してください。

ステップ 2 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

レポートのスケジュール設定

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール化したレポートは、前日、過去7日間、前月のデータを含めるように設定できます。

レポートをスケジュール設定できるレポート タイプは以下のとおりです。

- 概要
- Users
- Web サイト（Web Sites）
- URL カテゴリ（URL Categories）
- アプリケーションの表示（Application Visibility）
- マルウェア対策（Anti-Malware）
- Secure Endpoint
- Secure Endpoint 判定の更新
- クライアント マルウェア リスク（Client Malware Risk）
- Web レピュテーション フィルタ（Web Reputation Filters）
- L4 トラフィック モニター（L4 Traffic Monitor）
- SOCKS プロキシ（SOCKS Proxy）
- ユーザの場所別レポート（Reports by User Location）
- システム容量（System Capacity）
- マイ ダッシュボード（My Dashboard）

スケジュール設定されたレポートの追加

手順

ステップ 1 [レポート（Reporting）]>[スケジュールされたレポート（Scheduled Reports）] を選択し、[定期レポートの追加（Add Scheduled Report）] をクリックします。

ステップ 2 レポート [タイプ（Type）] を選択します。

ステップ 3 レポートのわかりやすい [タイトル（Title）] を入力します。

同じ名前のレポートを複数作成しないでください。

ステップ 4 レポートに含めるデータの時間範囲を選択します。

ステップ 5 生成されるレポートの [形式（Format）] を選択します。

デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。

ステップ 6 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 7 [スケジュール（Schedule）]セクションで、レポートを実行する周期（毎日、毎週、または毎月）と時間を選択します。

ステップ 8 [メールの送信先（Email to）] フィールドに、生成されたレポートを送信する相手の電子メール アドレスを入力します。

電子メール アドレスを指定しなかった場合は、レポートのアーカイブのみが行われます。

ステップ 9 データの [レポート言語（Report Language）] を選択します。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

スケジュール設定されたレポートの編集

手順

ステップ 1 [レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2 リストからレポートのタイトルを選択します。

ステップ 3 設定を変更します。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

スケジュール設定されたレポートの削除

手順

ステップ 1 [レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] を選択します。

ステップ 2 削除するレポートに対応するチェックボックスをオンにします。

ステップ 3 スケジュール設定されたすべてのレポートを削除するには、[すべて（All）] チェックボックスを選択します。

ステップ 4 削除して変更を確定します（[削除（Delete）] と [変更を確定（Commit Changes）]）。

（注）
削除されたレポートのアーカイブ版は削除されません。

オンデマンドでのレポートの生成

手順

ステップ 1 [レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] を選択します。

ステップ 2 [今すぐレポートを生成（Generate Report Now）] をクリックします。

ステップ 3 レポート [タイプ（Type）] を選択します。

ステップ 4 レポートのわかりやすい [タイトル（Title）] を入力します。

同じ名前のレポートを複数作成しないでください。

ステップ 5 レポートに含めるデータの時間範囲を選択します。

ステップ 6 生成されるレポートの [形式（Format）] を選択します。

デフォルト形式は PDF です。ほとんどのレポートで、raw データを CSV ファイルとして保存することもできます。

ステップ 7 設定するレポートのタイプに応じて、含める行数やデータをソートする列など、さまざまなレポート オプションを指定できます。必要に応じて、これらのオプションを設定します。

ステップ 8 [配信オプション（Delivery Options）] のいずれかを選択します。

- レポートの [アーカイブ（Archive）]（レポートが [アーカイブ レポート（Archived Reports）] ページに表示されます）。
- [今すぐ受信者にメールを送信（Email now to recipients）]（1 つまたは複数の電子メール アドレスを指定します）。

ステップ 9 データの [レポート言語（Report Language）] を選択します。

ステップ 10 [このレポートを配信（Deliver This Report）] をクリックして、レポートを生成します。

ステップ 11 変更を確定します。

アーカイブ レポート

[レポート（Reporting）] > [アーカイブ レポート（Archived Reports）] ページには、使用可能なアーカイブ済みのレポートが一覧表示されます。[レポートのタイトル（Report Title）] 列のそれぞれの名前は、そのレポートのビューにリンクしています。[表示（Show）] メニューは、一覧表示されたレポートのタイプをフィルタリングします。列見出しをクリックして、各列のデータをソートすることができます。

アプライアンスでは、スケジュール設定されたレポートごとに最大 12 のインスタンスが保存されます（最大で合計 1000 レポート）。アーカイブ済みのレポートは、アプライアンスの `/periodic_reports` ディレクトリに保管されます。アーカイブ済みのレポートは自動的に削除されます。新しいレポートが追加されると、古いレポートが削除され、常に 1000 という数が維持されます。12インスタンスという制限は、同じ名前と時間範囲のスケジュール設定された各レポートに適用されます。

L4 トラフィック モニタ レポートのトラブルシューティング

Web プロキシが転送プロキシとして設定され、L4 トラフィック モニタがすべてのポートをモニタするように設定されている場合、プロキシのデータ ポートの IP アドレスが記録され、クライアント IP アドレスとしてレポートに表示されます。Web プロキシがトランスペアレント

プロキシとして設定されている場合は、クライアント IP アドレスが正しく記録され、表示されるように IP スプーフィングを有効にします。これを行うには、『IronPort AsyncOS for Web User Guide』を参照してください。

関連項目

- [クライアント マルウェア リスク（Client Malware Risk）] ページ （22 ページ）
- L4 トラフィック モニタによって処理されたトランザクションの検索 （30 ページ）

セキュア アプライアンス レポート

この章で説明する内容は、次のとおりです。

- [概要（Overview）] ページ （15 ページ）
- [ユーザ（Users）] ページ （17 ページ）
- [ユーザー数（User Count）] ページ （18 ページ）
- [Webサイト（Web Sites）] ページ （18 ページ）
- [URLカテゴリ（URL Categories）] ページ （19 ページ）
- [アプリケーションの表示（Application Visibility）] ページ （20 ページ）
- [マルウェア対策（Anti-Malware）] ページ （21 ページ）
- Secure Endpoint ページ （22 ページ）
- [ファイル分析（File Analysis）] ページ （22 ページ）
- [セキュアエンドポイント判定のアップデート（Cisco Secure Endpoint Verdict Updates）] ページ （22 ページ）
- [クライアント マルウェア リスク（Client Malware Risk）] ページ （22 ページ）
- [Web レピュテーション フィルタ（Web Reputation Filters）] ページ （24 ページ）
- [L4 トラフィック モニター（L4 Traffic Monitor）] ページ （24 ページ）
- [SOCKS プロキシ（SOCKS Proxy）] ページ （25 ページ）
- [ユーザー ロケーション別のレポート（Reports by User Location）] ページ （25 ページ）
- [Web トラッキング（Web Tracking）] ページ （26 ページ）
- [システム容量（System Capacity）] ページ （31 ページ）
- [システムステータス（System Status）] ページ （32 ページ）

[概要（Overview）] ページ

[レポート（Reporting）] > [概要（Overview）] ページには、 SecureWeb Applianceでのアクティビティの概要が表示されます。このページには、 SecureWeb Applianceで処理される Web トラフィックに関するグラフおよびサマリー テーブルが含まれています。

表 *1*：システム概要

セクション	説明
Webプロキシ トラフィックの特徴（Web Proxy Traffic Characteristics）	過去 1 分間における 1 秒あたりの平均トランザクション数、過去 1 分間の平均帯域（bps）、過去 1 分間の平均応答時間（ms）、および現在の接続総数のリスト。
システム リソースの使用率（System Resource Utilization）	現在の全体的な CPU 負荷、RAMおよびレポート/ログディスク使用率のリスト。[システムステータス（System Status）] ページに切り替えるには、**[システムステータス詳細（System Status Details）]** をクリックします（詳細は 新しい Web インターフェイスの [システムステータス（System Status）] ページ （78 ページ） を参照）。 （注） このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、[システムステータス（System Status）] ページに表示される CPU 値と若干異なる場合があります。

表 *2*：時間範囲ベースのカテゴリと概要

セクション	説明
時間範囲：以下のセクションに表示されるデータの時間範囲を選択します。オプションは、[時間（Hour）]、[日（Day）]、[週（Week）]、[30日（30 Days）]、[前日（Yesterday）]、[カスタム範囲（Custom Range）] です。	
Webプロキシアクティビティ総数（Total Web Proxy Activity）	トランザクションの実際の数（縦の目盛り）、および（Webプロキシ）アクティビティが発生したおよその日付（横の時間軸）が表示されます。
Web プロキシの概要（Web Proxy Summary）	疑わしいまたは正常な Web プロキシ アクティビティの比率を表示できます。
L4 トラフィック モニターの概要（L4 Traffic Monitor Summary）	L4 トラフィック モニターによってモニターされ、ブロックされたトラフィックをレポートします。
疑わしいトランザクション（Suspect Transactions）	さまざまなセキュリティ コンポーネントによって疑わしいトランザクションと分類された Web トランザクションを表示できます。 トランザクションの実際の数、およびアクティビティが発生したおよその日付が表示されます。

セクション	説明
疑わしいトランザクションの概要（Suspect Transactions Summary）	ブロックまたは警告された疑わしいトランザクションの比率を表示できます。
上位 URL カテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	ブロックされた上位 10 の URL カテゴリが表示されます。
上位アプリケーション タイプ：総トランザクション数（Top Application Types: Total Transactions）	AVC または ADC エンジンによってブロックされた上位アプリケーションタイプが表示されます。
上位マルウェア カテゴリ：モニターまたはブロック（Top Malware Categories: Monitored or Blocked）	検出されたすべてのマルウェア カテゴリが表示されます。
ブロックまたは警告されたトランザクション数の上位ユーザー（Top Users Blocked or Warned Transactions）	ブロックされたトランザクションまたは警告されたトランザクションを生成しているユーザーが表示されます。認証されたユーザーはユーザー名で表示され、認証されていないユーザーは IP アドレスで表示されます。
Web トラフィック タップ ステータス	タップされていないトラフィック トランザクションおよびタップされたトラフィック トランザクションがグラフ形式で表示されます。
Web トラフィック タップ サマリ	タップされたトラフィック トランザクションおよびタップされていないトラフィック トランザクションの概要が、トラフィック トランザクションの合計とともに表示されます。
タップされた HTTP/HTTPS トラフィック	タップされた HTTP および HTTPS トラフィック トランザクションがグラフ形式で表示されます。
タップされたトラフィック サマリ	HTTP および HTTPS トラフィック トランザクションの概要が、HTTP および HTTPS トラフィック トランザクションの合計とともに表示されます。
EUP トランザクション	カプセル化された URL のトランザクションが表示されます。これらは、*translate.google.com* などの Web サイトから実行されたトランザクションです。
EUP トランザクションの概要	カプセル化された URL のトランザクションの概要が表示されます。
疑わしい EUP トランザクション	疑わしいと検出された、カプセル化された URL のトランザクションが表示されます。
疑わしい EUP トランザクションの概要	疑わしいと検出された、カプセル化された URL のトランザクションの概要が表示されます。

[ユーザ（Users）] ページ

[レポート（Reporting）]>[ユーザー（Users）]ページには、個々のユーザーの Web トラフィック情報を表示するためのリンクが提供されています。ネットワーク上のユーザーがインターネット、特定の Web サイト、または特定の URL で費やした時間と、ユーザーが使用した帯域幅の量を表示できます。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
ブロックされたトランザクション数別上位ユーザー（Top Users by Transactions Blocked）	ブロックされたトランザクションの数（横の目盛り）が最大のユーザー（縦の目盛り）が表示されます。
使用した帯域幅別上位ユーザー（Top Users by Bandwidth Used）	システム上で最も帯域幅（ギガバイト単位の使用量を示す横の目盛り）を使用しているユーザー（縦の目盛り）が表示されます。
ユーザー テーブル（Users Table）	個々のユーザーを一覧表示し、ユーザーごとに複数の統計情報を表示します。

[ユーザーの詳細（User Details）] ページ

[ユーザーの詳細（User Details）] ページには、[レポート（Reporting）] > [ユーザー（Users）] ページの [ユーザー テーブル（Users Table）] で選択した特定のユーザーに関する情報が表示されます。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
総トランザクション数別 URL カテゴリ（URL Categories by Total Transactions）	特定のユーザーが使用している特定の URL カテゴリのリストが表示されます。
総トランザクション数別トレンド（Trend by Total Transaction）	ユーザーが Web にいつアクセスしたかが表示されます。

セクション	説明
一致した URL カテゴリ（URL Categories Matched）	完了したトランザクションとブロックされたトランザクションの両方について、指定した時間範囲内で一致したすべての URL カテゴリが表示されます。
一致したドメイン（Domains Matched）	このユーザーがアクセスした特定のドメインまたは IP アドレスに関する情報が表示されます。 （注） このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。
一致したアプリケーション（Applications Matched）	AVC または ADC エンジンによって検出された、特定のユーザーが使用している特定のアプリケーションが表示されます。
検出されたマルウェア脅威（Malware Threats Detected）	特定のユーザーによって引き起こされているマルウェアの脅威の内、上位のものが表示されます。
一致したポリシー（Policies Matched）	この特定のユーザーに適用されている特定のポリシーが表示されます。

[ユーザー数（User Count）] ページ

[レポート（Reporting）]>[ユーザー数（User Count）]ページには、アプライアンスの認証されたユーザーと認証されていないユーザーの合計に関する情報が表示されます。このページには、直近の過去 30 日間、90 日間、および 180 日間のユニーク ユーザー数が表示されます。

（注） システムは、認証されたユーザーと認証されていないユーザーの合計を、1 日に 1 回計算します。

たとえば、5 月 22 日 23 時 59 分にユーザー数レポートを表示すると、システムは 5 月 22 日 0 時までの合計ユーザー数を表示します。

[Webサイト（Web Sites）] ページ

[レポート（Reporting）] > [Web サイト（Web Sites）] ページは、 SecureWeb Applianceで発生しているアクティビティ全体を集約したものです。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	このメニューからレポートに含めるデータの時間範囲を選択できます。
総トランザクション数別上位ドメイン（Top Domains by Total Transactions）	サイト上のアクセス上位ドメインがグラフ形式で表示されます。
ブロックされたトランザクション数別上位ドメイン（Top Domains by Transactions Blocked）	トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。
一致したドメイン（Domains Matched）	サイト上のアクセスされたドメインがインタラクティブなテーブルに表示されます。 （注） このドメインのデータを CSV ファイルにエクスポートする場合は、先頭から 300,000 件のエントリのみがファイルにエクスポートされるので注意してください。

[URLカテゴリ（URL Categories）] ページ

[レポート（Reporting）] > [URL カテゴリ（URL Categories）] ページでは、ネットワーク上のユーザーがアクセスしている URL カテゴリを表示できます。[URL カテゴリ（URL Categories）] ページを [アプリケーションの表示（Application Visibility）] ページおよび [ユーザー（Users）] ページと併用すると、特定のユーザーとそのユーザーがアクセスを試みているアプリケーションや Web サイトのタイプを調べることができます。

（注） すでに定義されている一連の URL カテゴリは更新されることがあります。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。
総トランザクション数別上位 URL カテゴリ（Top URL Categories by Total Transactions）	このセクションには、サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。

セクション	説明
ブロックまたは警告を受けたトランザクション数別上位 URL カテゴリ（Top URL Categories by Blocked and Warned Transactions）	トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。
一致した URL カテゴリ（URL Categories Matched）	指定した時間範囲における URL カテゴリ別のトランザクションの傾向、および各カテゴリで使用された帯域幅と費やされた時間が表示されます。 未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。 • 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループ ポリシーに適用できます。 • 評価およびデータベース更新用に、未分類の URL と誤って分類された URL をシスコにレポートできます。 • Web レピュテーション フィルタリングと、アンチマルウェア フィルタリングがイネーブルになっていることを確認してください。

URL カテゴリ セットの更新とレポート

SecureWeb Applianceでは、一連の定義済み URL カテゴリが定期的に自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL カテゴリ セットの更新後に生成されたレポート データには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

[アプリケーションの表示（Application Visibility）] ページ

[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページには、Application Visibility and Control または Application Discovery and Control エンジンで検出されたアプリケーションと、使用されているアプリケーションのタイプ、およびブロックされているアプリケーションのタイプが表示されます。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。

セクション	説明
[総トランザクション数の上位アプリケーションタイプ（Top Application Types by Total Transactions）]	このセクションには、サイト上でアクセスされた上位アプリケーション タイプがグラフ形式で表示されます。
ブロックされたトランザクション数別上位アプリケーション（Top Applications by Blocked Transactions）	トランザクションごとに発生するブロック アクションをトリガーした上位アプリケーション タイプが、グラフ形式で表示されます。
一致したアプリケーション タイプ（Application Types Matched）	[総トランザクション数別上位アプリケーション タイプ（Top Applications Type by Total Transactions）] グラフに表示されているアプリケーション タイプについて、さらに詳しい情報を表示できます。
一致したアプリケーション（Applications Matched）	指定した時間範囲内のすべてのアプリケーションが表示されます。

[マルウェア対策（Anti-Malware）] ページ

[レポート（Reporting）] > [マルウェア対策（Anti-Malware）] ページでは、Cisco DVS エンジンによって検出されたマルウェアをモニターおよび識別することができます。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
検出された上位マルウェア カテゴリ（Top Malware Categories Detected）	DVSエンジンによって検出された上位のマルウェア カテゴリが表示されます。
検出された上位マルウェア脅威（Top Malware Threats Detected）	DVS エンジンによって検出された上位のマルウェア脅威が表示されます。
マルウェア カテゴリ（Malware Categories）	[検出された上位マルウェア カテゴリ（Top Malware Categories Detected）] セクションに表示されている特定のマルウェア カテゴリに関する情報が表示されます。
マルウェア脅威（Malware Threats）	[上位マルウェア脅威（Top Malware Threats）] セクションに表示されている特定のマルウェアの脅威に関する情報が表示されます。

[マルウェア カテゴリ（Malware Category）] レポート ページ

手順

ステップ 1 [レポート（Reports）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2 [マルウェア カテゴリ（Malware Categories）] インタラクティブ テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[マルウェア脅威（Malware Threats）] レポート ページ

手順

ステップ 1 [レポート（Reports）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2 [マルウェア脅威（Malware Threats）] テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

Secure Endpoint ページ

ファイル レピュテーション フィルタリングとファイル分析 を参照してください。

[ファイル分析（File Analysis）] ページ

ファイル レピュテーションおよびファイル分析のレポートとトラッキング を参照してください。

[セキュアエンドポイント判定のアップデート（Cisco Secure Endpoint Verdict Updates）] ページ

ファイル レピュテーション フィルタリングとファイル分析 を参照してください。

[クライアント マルウェア リスク（Client Malware Risk）] ページ

[レポート（Reporting）]>[クライアント マルウェア リスク（Client Malware Risk）] ページは、クライアント マルウェア リスク アクティビティをモニターするために使用できるセキュリティ関連のレポーティング ページです。[クライアント マルウェア リスク（Client Malware Risk）] ページには、L4 トラフィック モニター（L4TM）によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
Web プロキシ：マルウェア リスク別上位クライアント（Web Proxy: Top Clients by Malware Risk）	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。
[L4トラフィックモニタ:検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）]	このチャートには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスが表示されます。
Web プロキシ：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）	[Webプロキシ：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）] テーブルには、[Web プロキシ：マルウェア リスク別上位クライアント（Web Proxy: Top Clients by Malware Risk）] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。
[L4トラフィックモニタ:マルウェアリスク別クライアント（L4 Traffic Monitor: Clients by Malware Risk）]	このテーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。

[Web プロキシ：マルウェア リスク別クライアント（Web Proxy: Clients by Malware Risk）] の [クライアントの詳細（Client Detail）] ページ

[クライアントの詳細（Client Detail）] ページには、指定した時間範囲における特定クライアントの Web アクティビティとマルウェア リスクの全データが表示されます。

手順

ステップ 1 [レポート（Reporting）] > [クライアント マルウェア リスク（Client Malware Risk）] を選択します。

ステップ 2 [Webプロキシ：クライアントマルウェアのリスク（Web Proxy - Client Malware Risk）] セクションで、[ユーザー ID/クライアント IP アドレス（User ID / Client IP Address）] 列のユーザー名をクリックします。

次のタスク

[ユーザーの詳細（User Details）] ページ （17 ページ）

[Web レピュテーション フィルタ（Web Reputation Filters）] ページ

[レポート（Reporting）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページは、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ（ユーザーが設定）の結果を表示する、セキュリティ関連のレポーティング ページです。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
Web レピュテーション アクション（トレンド）（Web Reputation Actions (Trend)）	指定した時間（横方向の時間軸）に対する Web レピュテーション アクションの総数（縦方向の目盛り）が、グラフ形式で表示されます。
Web レピュテーション アクション（ボリューム）（Web Reputation Actions (Volume)）	Web レピュテーション アクションのボリュームがトランザクション数との対比で表示されます。
ブロックされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Blocked Transactions）	レピュテーション スコアが低いためブロックされた脅威タイプが表示されます。
詳細にスキャンされたトランザクション別 Web レピュテーション脅威タイプ（Web Reputation Threat Types by Scanned Further Transactions）	トランザクションのスキャンを指示するレピュテーション スコアが生じた、脅威タイプが表示されます。
Web レピュテーションアクション（スコアによる内訳）（Web Reputation Actions (Breakdown by Score)）	各アクションの Web レピュテーション スコアの内訳が表示されます。

[L4 トラフィック モニター（L4 Traffic Monitor）] ページ

[レポート（Reporting）] > [L4 トラフィック モニター（L4 Traffic Monitor）] ページは、指定した時間範囲内に L4 トラフィック モニターが検出したマルウェア ポートとマルウェア サイトに関する情報を表示する、セキュリティ関連のレポーティング ページです。マルウェア サイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

L4 トラフィック モニターは、アプライアンスのすべてのポートに着信するネットワーク トラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベース テーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポート対象の時間範囲を選択できるメニュー。
上位クライアント IP（Top Client IPs）	組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスがグラフ形式で表示されます。
上位マルウェア サイト（Top Malware Sites）	L4 トラフィック モニターによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。
クライアント ソース IP（Client Source IPs）	頻繁にマルウェア サイトに接続している組織内のコンピュータの IP アドレスが表示されます。
マルウェア ポート（Malware Ports）	L4 トラフィック モニターによって最も頻繁にマルウェアが検出されたポートが表示されます。
検出されたマルウェア サイト（Malware Sites Detected）	L4 トラフィック モニターによって最も頻繁にマルウェアが検出されたドメインが表示されます。

[SOCKS プロキシ（SOCKS Proxy）] ページ

[レポート（Reporting）] > [SOCKS プロキシ（SOCKS Proxy）] ページでは、上位宛先およびユーザーに関する情報を含む、SOCKS プロキシを介して処理されたトランザクションのデータとトレンドを表示できます。

[ユーザー ロケーション別のレポート（Reports by User Location）] ページ

[レポート（Reporting）] > [ユーザーの場所別レポート（Reports by User Location）] ページで、ローカルおよびリモート ユーザーが実行しているアクティビティを確認できます。

対象となるアクティビティは以下のとおりです。

- ローカル ユーザーおよびリモート ユーザーがアクセスしている URL カテゴリ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトによってトリガーされているアンチマルウェア アクティビティ。
- ローカル ユーザおよびリモート ユーザがアクセスしているサイトの Web レピュテーション。
- ローカル ユーザおよびリモート ユーザがアクセスしているアプリケーション。
- ユーザ（ローカルおよびリモート）。
- ローカル ユーザおよびリモート ユーザがアクセスしているドメイン。

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートに含めるデータの時間範囲を選択できるメニュー。
Web プロキシ アクティビティ総数：リモート ユーザー（Total Web Proxy Activity: Remote Users）	指定した時間（横方向）におけるリモート ユーザーのアクティビティ（縦方向）が表示されます。
Web プロキシの概要（Web Proxy Summary）	ネットワーク上のローカル ユーザーとリモート ユーザーのアクティビティの要約が表示されます。
Web プロキシ アクティビティ総数：ローカル ユーザー（Total Web Proxy Activity: Local Users）	指定した時間（横方向）におけるリモート ユーザーのアクティビティ（縦方向）が表示されます。
検出された疑わしいトランザクション：リモート ユーザー（Suspect Transactions Detected: Remote Users）	指定した時間内（横方向）に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション（縦方向）が表示されます。
疑わしいトランザクションの要約（Suspect Transactions Summary）	ネットワーク上のリモート ユーザーの疑わしいトランザクションの要約が表示されます。
検出された疑わしいトランザクション：ローカル ユーザー（Suspect Transactions Detected: Local Users）	指定した時間内（横方向）に、リモート ユーザー向けに定義されたアクセス ポリシーによって検出された、疑わしいトランザクション（縦方向）が表示されます。
疑わしいトランザクションの要約（Suspect Transactions Summary）	ネットワーク上のローカル ユーザーの疑わしいトランザクションの要約が表示されます。

[Web トラッキング（Web Tracking）] ページ

[Web トラッキング（Web Tracking）] ページを使用して、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を取得します。必要に応じて、以下のタブのいずれかで検索を行います。

[Web トラッキング（Web Tracking）] ページ	タスクへのリンク
Web プロキシによって処理されたトランザクション（Transactions processed by the Web Proxy）	Web プロキシによって処理されるトランザクションの検索 （27 ページ）
L4 トラフィック モニターによって処理されたトランザクション（Transactions processed by the L4 Traffic Monitor）	L4 トラフィック モニタによって処理されたトランザクションの検索 （30 ページ）
SOCKS プロキシによって処理されたトランザクション（Transactions processed by the SOCKS Proxy）	SOCKS プロキシによって処理されるトランザクションの検索 （31 ページ）

または、透過的なパススルーなどの場合に、FQDN を使用して [Webトラッキング（Web Tracking）] ページで Web サイトデータを検索します。

（注） 透過的なリクエストでは、ドメインまたはサーバーの名前がトラッキングページに表示されます。ただし、透過的なパススルーを含む透過的な要求が SNI なしで送信されると、IP アドレスが表示されます。

Web プロキシによって処理されるトランザクションの検索

[レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [プロキシ サービス（Proxy Services）] タブを使用して、特定のユーザーまたはすべてのユーザーの Web の使用状況を追跡し、レポートできます。

所定の期間内に記録されたトランザクションのタイプ（ブロック、モニターリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。

（注） Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

手順

ステップ 1 [レポート（Reporting）] > [Web トラッキング（Web Tracking）] を選択します。

ステップ 2 [プロキシ サービス（Proxy Services）] タブをクリックします。

ステップ 3 設定項目を設定します。

設定	説明
時間範囲（Time Range）	レポート対象の時間範囲を選択します。
ユーザー/クライアント IP（User/Client IP）	（任意）レポートに表示される認証ユーザー名、または追跡対象のクライアント IP アドレスを入力します。IP 範囲を CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。
Web サイト（Website）	（任意）追跡対象の Web サイトを入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。 （注） SNI（サーバー名指定）で検索できます。SNI、TLS プロトコルの拡張子を使用して、クライアントは Web トランザクションの実行中に安全にホスト名を指定できます。単語全体を指定する必要があります。 SNI を有効にするには、 AMP、およびレピュテーションサービスを有効にする必要があります。
トランザクション タイプ（Transaction Type）	追跡対象のトランザクションのタイプを [すべてのトランザクション（All Transactions）]、[完了（Completed）]、[ブロックされた（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）] から選択します。

ステップ 4 （任意）[詳細設定（Advanced）] セクションを展開してフィールドを設定し、より詳細な条件で Web トラッキングの結果をフィルタリングします。

設定	説明
URL カテゴリ（URL Category）	URL カテゴリでフィルタリングするには、[URL カテゴリ別フィルタ（Filter by URL Category）] を選択し、フィルタリング対象とする URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。
アプリケーション（Application）	アプリケーションでフィルタリングするには、[アプリケーションによるフィルタ（Filter by Application）] を選択し、フィルタリングに使用するアプリケーションを選択します。 アプリケーション タイプでフィルタリングするには、[アプリケーションタイプによるフィルタ（Filter by Application Type）] を選択し、フィルタリングに使用するアプリケーション タイプを選択します。

設定	説明
ポリシー	このトランザクションに対して最終決定を行うポリシーの名前でフィルタするには、[アクション ポリシーによってフィルタ（Filter by Action Policy）] を選択し、フィルタリングに使用するポリシー グループ名（アクセス ポリシー、復号ポリシー、またはデータ セキュリティ ポリシー）を入力します。詳細については、アクセス ログ ファイル内の Web プロキシ情報の PolicyGroupName に関する説明を参照してください。
Secure Endpoint	Web トラッキング機能と Secure Endpoint 機能についてを参照してください。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。
WBRS	[WBRS] セクションでは、Web レピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[スコア範囲（Score Range）] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし（No Score）] を選択すると、スコアがない Web サイトをフィルタリングできます。 • Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ（Filter by Reputation Threat）] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。
AnyConnect セキュア モビリティ	ユーザーの場所（リモートまたはローカル）によってフィルタリングするには、[ユーザーの場所でフィルタ（Filter by User Location）] を選択し、フィルタリングするユーザー タイプを選択します。
ユーザー リクエスト	クライアントによって開始されたトランザクションでフィルタリングするには、[ユーザーが要求したトランザクションによるフィルタ（Filter by User-Requested Transactions）] を選択します。 （注） このフィルタをイネーブルにすると、検索結果に「最も想定される」トランザクションが含まれることがあります。

設定	説明
カプセル化された URL の保護	カプセル化された URL トランザクションでこのフィルタを有効にします。 （注） • HTTPS プロキシを有効にする必要があります。HTTPS プロキシのイネーブル化を参照してください • https://translate.google.com の Web レピュテーション スコアの範囲が復号する設定になっていることを確認します。復号ポリシー グループの Web レピュテーション フィルタの設定を参照してください

ステップ 5 [検索（Search）] をクリックします。

結果はタイム スタンプでソートされ、最新の結果が最上部に表示されます。

[詳細の表示（Display Details）] リンクの下のカッコ内の数値は、ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザーが開始したトランザクションによって発生した関連トランザクションの数を示します。

ステップ 6 （任意）[トランザクション（Transactions）] 列の [詳細の表示（Display Details）] をクリックし、各トランザクションに関する詳細情報を表示します。

（注）
1000 件を超える結果を表示する必要がある場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックすると、関連するトランザクションの詳細を除く raw データ一式が含まれた CSV ファイルを取得できます。

ヒント
結果内の URL が切り詰められている場合、アクセス ログで完全な URL を確認できます。

500 件までの関連トランザクションの詳細を表示するには、[関連トランザクション（Related Transactions）] リンクをクリックします。

次のタスク

- URL カテゴリ セットの更新とレポート （20 ページ）
- マルウェアのカテゴリについて
- Web トラッキング機能と Secure Endpoint 機能について

L4 トラフィック モニタによって処理されたトランザクションの検索

[レポート（Reporting）] > [Web トラッキング（Web Tracking）] ページの [L4 トラフィック モニター（L4 Traffic Monitor）] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- サイト、使用された IP アドレスまたはドメイン
- [ポート（Port）]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ

一致した検索結果のうち最初の 1000 件が表示されます。

SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、ユーザー、および宛先ドメイン、IPアドレス、またはポートなど含む、さまざまな基準を満たすトランザクションを検索できます。

手順

ステップ 1 [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 2 **[SOCKSプロキシ（SOCKS Proxy）]** タブをクリックします。
ステップ 3 結果をフィルタリングするには、**[詳細設定（Advanced）]** をクリックします。
ステップ 4 検索条件を入力します。
ステップ 5 **[検索（Search）]** をクリックします。

次のタスク

[SOCKS プロキシ（SOCKS Proxy）] ページ （25 ページ）

[システム容量（System Capacity）] ページ

[レポート（Reporting）]>[システム容量（System Capacity）]ページには、 SecureWeb Appliance のリソース使用率に関する現在および履歴情報が表示されます。

[システム容量（System Capacity）] ページにデータを表示する時間範囲を選択する場合、以下のことに留意することが重要です。

- **Hour レポート。**Hour レポートは、分テーブルに照会して、60 分間を超える分単位で、1 分間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。
- **Day レポート。**Day レポートは、時間テーブルに照会して、24 分間を超える時間単位で、1 時間にアプライアンスに記録されたアイテム（バイトや接続など）の正確な数を表示します。この情報は時間テーブルから収集されます。

Week レポートおよび 30 Days レポートは、Hour レポートおよび Day レポートと同じように動作します。

[システムステータス（System Status）] ページ

システム ステータスをモニターするには、[レポート（Reporting）] > [システム ステータス（System Status）] ページを使用します。このページは、 SecureWeb Applianceの現在のステータスと設定を表示します。

セクション	表示内容
SecureWeb Appliance のステータス	• システムの動作期間 • システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。 このページに表示される CPU 使用率値はさまざまな瞬間に個別に読み取られるため、システムの [概要（Overview）] ページ（[概要（Overview）] ページ （15 ページ））に表示される CPU 値と若干異なる場合があります。 システムによって使用されないRAMはWebオブジェクトキャッシュによって使用されるので、効率的に動作するRAM使用率は90%を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が100%に固定されない場合、システムは正常に動作しています。 （注） プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。
プロキシトラフィックの特性（Proxy Traffic Characteristics）	• 1 秒あたりのトランザクション • 帯域幅 • 応答時間 • キャッシュ ヒット率 • 接続
Web トラフィック タップ（Web Traffic Tap）	Web トラフィック タップ CPU 使用率。
高可用性	高可用性サービスのステータス。
外部サービス（External Services）	• Identity Services Engine

セクション	表示内容
現在の設定（Current Configuration）	Web プロキシ設定： • Web プロキシのステータス：イネーブルまたはディセーブル。 • 展開トポロジ • Web プロキシ モード：フォワードまたは透過。 • IP スプーフィング：イネーブルまたはディセーブル。 L4 トラフィック モニター設定： • L4 トラフィック モニターのステータス：イネーブルまたはディセーブル。 • L4 トラフィック モニターの配線。 • L4 トラフィック モニターのアクション：モニターまたはブロック。 Web トラフィック タップ設定： • Web トラフィック タップのステータス：イネーブルまたはディセーブル。 • Web トラフィック タップ インターフェイス：P1、P2、TI、T2 SecureWeb Appliance バージョン情報 ハードウェア情報

関連項目

[システム容量（System Capacity）] ページ （31 ページ）

新しい Web インターフェイスでのセキュア アプライアンス レポート

この章で説明する内容は、次のとおりです。

• 新しい Web インターフェイスの Web レポート ページの概要 （34 ページ）
• （Web レポートのみ）チャート化するデータの選択 （66 ページ）
• 新しい Web インターフェイスでの Web トラッキング （67 ページ）
• Web トラッキングの検索結果の使用 （73 ページ）

- 新しい Web インターフェイスでの Web レポートのスケジューリングとアーカイブ （75 ページ）
- 新しい Web インターフェイスの [システムステータス（System Status）] ページ （78 ページ）

新しい Web インターフェイスの Web レポート ページの概要

次の表は、 SecureWeb Appliance用 AsyncOS のサポートされている最新リリースで、Web インターフェイスの [レポート（Reports）] ドロップダウンから利用できるレポートを示します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用（9 ページ）を参照してください。 SecureWeb Applianceでこれ以前のリリースの AsyncOS を実行している場合は、これらのレポートの一部を利用できません。

表 *3 : [Web*レポート（*Web Reports*）*]* ドロップダウンのオプション

[レポート（Reports）] ドロップダウンのオプション	**操作**
一般的なレポート	
[概要（Overview）] ページ	[概要（Overview）] ページには、 SecureWeb Appliance でのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフおよび要約テーブルが含まれます。詳細については、[概要（Overview）]ページ （38 ページ）を参照してください。
[アプリケーションの表示（Application Visibility）] ページ	[アプリケーションの表示（Application Visibility）] ページでは、セキュリティ管理アプライアンスおよび SecureWeb Appliance内で特定のアプリケーションタイプに適用されているコントロールを適用し、表示できます。詳細については、[アプリケーションの表示（Application Visibility）]ページ （40 ページ）を参照してください。
[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ	指定した時間範囲内に L4 トラフィック モニタで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。詳細については、[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ （42 ページ）を参照してください。
[SOCKS プロキシ（SOCKS Proxy）] ページ	宛先、ユーザなど、SOCKS プロキシ トランザクションのデータを表示できます。詳細については、[SOCKS プロキシ（SOCKS Proxy）] ページ （45 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[URLカテゴリ（URL Categories）] ページ	[URLカテゴリ（URL Categories）] ページでは、アクセスされている次の上位 URL カテゴリを表示できます。 • トランザクションごとに発生するブロック アクションまたは警告アクションをトリガーした上位 URL。 • 完了したトランザクションと、警告とブロックが行われたトランザクションの両方を対象とした、指定した時間範囲内のすべての URL カテゴリ。これはインタラクティブな列見出しのあるインタラクティブ テーブルとなっていて、必要に応じてデータをソートできます。 詳細については、[URLカテゴリ（URL Categories）] ページ （47 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
[ユーザ（Users）] ページ	[ユーザ（Users）] ページには複数の Web トラッキング リンクが表示され、各ユーザの Web トラッキング情報を確認できます。 [ユーザ（Users）] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。 [ユーザ（Users）] ページのインタラクティブな [ユーザ（Users）] テーブルで個々のユーザをクリックすると、その特定のユーザの詳細情報が [ユーザの詳細（User Details）] ページに表示されます。 [ユーザの詳細（User Details）] ページでは、[ユーザ（Users）] ページの [ユーザ（Users）] テーブルで指定したユーザに関する具体的な情報を確認できます。このページから、お使いのシステムでの各ユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。 詳細については、[ユーザ（Users）] ページ （51 ページ）を参照してください。 システムにおける各ユーザの情報については、[ユーザの詳細（User Details）] ページ（Web レポーティング） （53 ページ）を参照してください。
[Webサイト（Web Sites）] ページ	[Webサイト（Web Sites）] ページでは、管理対象アプライアンスで発生しているアクティビティ全体を集約して表示できます。このページでは、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタできます。詳細については、[Webサイト（Web Sites）] ページ （56 ページ）を参照してください。
[HTTPS レポート（HTTPS Reports）]	[HTTPS レポート（HTTPS Reports）] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー（トランザクションまたは帯域幅の使用量）のすべてを集約しています。詳細については、[HTTPS レポート（HTTPS Reports）] ページ （49 ページ）を参照してください。

[レポート（Reports）] ドロップダウンのオプション	操作
脅威レポート	
[マルウェア対策（Anti-Malware）] ページ	[マルウェア対策（Anti-Malware）] ページでは、指定した時間範囲内にアンチマルウェア スキャン エンジンで検出された、マルウェア ポートとマルウェア サイトに関する情報を表示できます。レポートの上部には、上位の各マルウェア ポートおよび各マルウェア Web サイトの接続数が表示されます。レポートの下部には、検出されたマルウェア ポートとマルウェア サイトが表示されます。詳細については、[マルウェア対策（Anti-Malware）] ページ （59 ページ）を参照してください。
Secure Endpoint ページ	Secure Endpoint では、既知のファイルレピュテーションを取得し、レピュテーションサービスには未知である特定のファイルの動作を分析し、新しい情報が利用可能になったときに新たな脅威を継続的に評価し、ネットワークに侵入した後に脅威と判断されたファイルについて通知することによって、ゼロデイの脅威や標的型のファイルベースの脅威から保護します。詳細については、Secure Endpoint ページ （57 ページ）を参照してください。
[クライアント マルウェア リスク（Client Malware Risk）] ページ	[クライアントマルウェアリスク（Client Malware Risk）] ページは、セキュリティ関連のレポーティング ページです。このページを使用して、著しく頻繁にマルウェア サイトへ接続している可能性がある個々のクライアント コンピュータを特定できます。 詳細については、[クライアント マルウェア リスク（Client Malware Risks）] ページ （63 ページ）を参照してください。
[Web レピュテーション フィルタ（Web Reputation Filters）] ページ	指定した時間範囲内のトランザクションに対する、Web レピュテーション フィルタリングに関するレポートを表示できます。詳細については、[Web レピュテーション フィルタ（Web Reputation Filters）] ページ （64 ページ）を参照してください。

[滞留時間（Time Spent）] について

さまざまなテーブルの [滞留時間（Time Spent）] 列は、Web ページでユーザーが費やした時間を表します。各 URL カテゴリでユーザーが費やした時間。ユーザーを調査する目的で使用されます。URL のトラッキング時には、その特定の URL に各ユーザーが費やした時間。

トランザクションイベントに「viewed」のタグが付けられる（ユーザーが特定のURLに進む）と、[滞留時間（Time Spent）] の値の計算が開始され、Web レポーティング テーブルのフィールドとして追加されます。

費やされた時間を計算するため、AsyncOSはアクティブ ユーザーごとに、1分間のアクティビティに対して60秒という時間を割り当てます。この1分間の終わりに、各ユーザーが費やした時間は、そのユーザーが訪れた各ドメイン間で均等に配分されます。たとえば、あるユーザーがアクティブな1分間に4つの異なるドメインに進んだ場合、そのユーザーは各ドメインで15分ずつ費やしたと見なされます。

経過時間の値に関して、以下の注意事項を考慮してください。

- アクティブ ユーザーは、アプライアンスを介してHTTP トラフィックを送信し、Web サイトにアクセスした、すなわちAsyncOS が「ページ ビュー」と見なす動作を行ったユーザー名またはIP アドレスとして定義されています。
- AsyncOS では、クライアント アプリケーションが開始する要求とは逆に、ユーザーが開始するHTTP 要求としてページ ビューを定義します。AsyncOS はヒューリスティック アルゴリズムを使用して、可能な限り効果的にユーザー ページ ビューを識別します。

単位は時間：分形式で表示されます。

[概要（Overview）] ページ

[概要（Overview）] レポートページには、 SecureWeb Applianceでのアクティビティの概要が表示されます。これには、着信および発信トランザクションに関するグラフおよび要約テーブルが含まれます。

[概要（Overview）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [概要（Overview）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

[概要（Overview）] レポート ページの上部には、URL とユーザの使用量に関する統計情報、Web プロキシ アクティビティ、および各種トランザクション サマリーが表示されます。トランザクション サマリーには、さらに詳細なトレンド情報が示されます。たとえば、疑わしいトランザクションと、そのグラフの隣にそれらのトランザクションがブロックされた数、およびブロックされた方法が表示されます。

[概要（Overview）] レポート ページの下半分は、使用状況に関する情報に使用されます。つまり、表示されている上位 URL カテゴリ、ブロックされている上位アプリケーション タイプおよびカテゴリ、これらのブロックまたは警告を生成している上位ユーザが表示されます。

表 *4 : [*概要（*Overview*）*]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。

セクション	説明
[Webプロキシアクティビティ総数（Total Web Proxy Activity）]	現在セキュリティ管理アプライアンスで管理されているSecureWeb Applianceによって報告されるWebプロキシアクティビティを表示できます。 このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。 疑わしいWebプロキシアクティビティまたは正常なプロキシアクティビティの比率を、トランザクションの総数も含めて表示できます。
[疑わしいトランザクション（Suspect Transactions）]	管理者が疑わしいトランザクションと分類したWebトランザクションをグラフ形式で表示できます。 このセクションには、トランザクションの実際の数、およびアクティビティが発生したおよその日付がグラフ形式で表示されます。 ブロックまたは警告された疑わしいトランザクションの比率も表示できます。また、検出されてブロックされたトランザクションのタイプ、およびそのトランザクションが実際にブロックされた回数を確認できます。
[L4トラフィックモニタの概要（L4 Traffic Monitor Summary）]	現在セキュリティ管理アプライアンスで管理されているSecureWeb Applianceによって報告されるL4トラフィックをグラフ形式で表示できます。
上位URLカテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	ブロックされている上位のURLカテゴリが、URLカテゴリのタイプおよび特定タイプのカテゴリが実際にブロックされた回数を含め、グラフ形式で表示されます。 すでに定義されている一連のURLカテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート （48ページ）を参照してください。
上位アプリケーション タイプ：総トランザクション数（Top Application Types: Total Transactions）	ブロックされている上位アプリケーションタイプが、実際のアプリケーションタイプ名および特定のアプリケーションがブロックされた回数を含め、グラフ形式で表示されます。
上位マルウェアカテゴリ：モニタまたはブロック済み（Top Malware Categories: Monitored or Blocked）	検出されたすべてのマルウェアカテゴリをグラフ形式で表示できます。

セクション	説明
ブロックまたは警告されたトランザクション数の上位ユーザ（Top Users Blocked or Warned Transactions）	ブロックまたは警告されたトランザクションを生成している実際のユーザをグラフ形式で表示できます。ユーザは IP アドレスまたはユーザ名で表示できます。
[上位の脅威カテゴリ：WBRSによりブロック（Top Threat Categories: Blocked ）]	ブロックされたすべての脅威カテゴリを表示できます（グラフ形式）。

[アプリケーションの表示（Application Visibility）] ページ

（注） [アプリケーションの表示（Application Visibility）] の詳細については、『User Guide for AsyncOS for Cisco SecureWeb Appliance』の「Understanding Application Visibility and Control」のトピックを参照してください。

[アプリケーションの表示（Application Visibility）] レポートページでは、セキュリティ管理アプライアンスおよび SecureWeb Appliance内の特定のアプリケーションタイプに制御を適用することができます。

[アプリケーションの表示（Application Visibility）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [アプリケーションの表示（Application Visibility ）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

アプリケーション制御を使用すると、たとえば URL フィルタリングのみを使用する場合よりも Web トラフィックをきめ細かく制御できるだけでなく、次のタイプのアプリケーションおよびアプリケーション タイプに対する制御を強化できます。

- 回避アプリケーション（アノニマイザや暗号化トンネルなど）。
- コラボレーション アプリケーション（Cisco Webex、Facebook、インスタント メッセージングなど）。
- リソースを大量消費するアプリケーション（ストリーミング メディアなど）。

アプリケーションとアプリケーション タイプの違いについて

レポートに関連するアプリケーションを制御するには、アプリケーションとアプリケーションタイプの違いを理解することが非常に重要です。

- **アプリケーション タイプ**。1 つまたは複数のアプリケーションを含むカテゴリです。たとえば検索エンジンは、Google Search や Craigslist などの検索エンジンを含むアプリケーション タイプです。インスタント メッセージングは、Yahoo Instant Messenger や Cisco Webex などを含む別のアプリケーション タイプです。Facebook もアプリケーション タイプです。

（注） AVC のすべてのアプリケーション タイプが ADC に適用できるわけではありません。

- **アプリケーション**。アプリケーションタイプに属している特定のアプリケーションです。たとえば、YouTube はメディア アプリケーション タイプに含まれるアプリケーションです。
- **アプリケーション動作**。アプリケーション内でユーザが実行できる特定のアクションまたは動作です。たとえば、ユーザは Yahoo Messenger などのアプリケーションの使用中にファイルを転送できます。すべてのアプリケーションに、設定可能なアプリケーション動作が含まれているわけではありません。

[アプリケーションの表示（Application Visibility）] ページには次の情報が表示されます。

表 *5 : [アプリケーションの表示（Application Visibility）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
[総トランザクション数の上位アプリケーションタイプ（Top Application Types by Total Transactions）]	サイト上でアクセスされた上位のアプリケーション タイプがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。 たとえば、Yahoo Instant Messenger などのインスタント メッセージング ツール、Facebook、Presentation というアプリケーション タイプが表示されます。

セクション	説明
[ブロックされたトランザクション数の上位アプリケーション（Top Applications by Blocked Transactions）]	トランザクションごとに発生するブロックアクションをトリガーした上位アプリケーションタイプが、グラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。 たとえば、ユーザが Google Talk や Yahoo Instant Messenger などの特定のアプリケーションタイプを起動しようとしたが、特定のポリシーが適用されているために、ブロックアクションがトリガーされたとします。このアプリケーションは、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。
[一致したアプリケーションタイプ（Application Types Matched）]	[一致したアプリケーションタイプ（Application Types Matched）] インタラクティブ テーブルでは、[総トランザクション数の上位アプリケーションタイプ（Top Applications Type by Total Transactions）] テーブルに表示されているアプリケーションタイプに関するさらに詳しい情報を表示できます。 [アプリケーション（Applications）] カラムで、詳細を表示するアプリケーションをクリックできます。
[一致したアプリケーション（Applications Matched）]	[一致したアプリケーション（Applications Matched）] インタラクティブテーブルには、指定した時間範囲内のすべてのアプリケーションが表示されます。 さらに、[一致したアプリケーション（Application Matched）] セクション内で特定のアプリケーションを検索できます。このセクション下部のテキストフィールドに特定のアプリケーション名を入力し、[アプリケーションの検索（Find Application）] をクリックします。

[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ

[レイヤ4トラフィックモニター（Layer 4 Traffic Monitor Page）] レポートページには、指定した時間範囲内にレイヤ 4 トラフィックモニターによってお使いの SecureWeb Appliance上で検出されたマルウェアポートとマルウェアサイトに関する情報が表示されます。マルウェアサイトに頻繁にアクセスしているクライアントの IP アドレスも表示されます。

[Web サイト（Web Sites）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [Web サイト（Web Sites）] を選択します。詳細に

ついては、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

レイヤ 4 トラフィックモニターは、各 SecureWeb Applianceのすべてのポートに着信するネットワークトラフィックをリッスンし、ドメイン名と IP アドレスを独自のデータベーステーブルのエントリと照合して、着信トラフィックと発信トラフィックを許可するかどうかを決定します。

このレポートのデータを使用して、ポートまたはサイトをブロックするかどうかを判断したり、特定のクライアント IP アドレスが著しく頻繁にマルウェア サイトに接続している理由（たとえば、その IP アドレスに関連付けられたコンピュータが、中央のコマンド/コントロール サーバに接続しようとするマルウェアに感染しているなど）を調査したりできます。

表 *6 : [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
上位クライアントIP：検出されたマルウェア接続（Top Client IPs: Malware Connections Detected）	組織内で最も頻繁にマルウェア サイトに接続している上位のコンピュータの IP アドレスがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、チャート化するデータの選択 （5 ページ）を参照してください。 このグラフは、[クライアント マルウェア リスク（Client Malware Risks）]ページ （63 ページ）の[レイヤ4トラフィックモニタ：検出されたマルウェア接続（Layer 4 Traffic Monitor: Malware Connections Detected）]グラフと同じです。
上位マルウェアサイト：検出されたマルウェア接続（Top Malware Sites: Malware Connections Detected）	レイヤ 4 トラフィック モニタによって検出された上位のマルウェア ドメインがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、チャート化するデータの選択 （5 ページ）を参照してください。

セクション	説明
[クライアントソースIP（Client Source Ips）]	このインタラクティブテーブルを使用すると、組織内でマルウェア サイトに頻繁に接続しているコンピュータの IP アドレスを表示できます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[クライアントIPによるフィルタ（Filter by Client IP）] をクリックします。この機能を使用して、マルウェアがどのポートを使用してマルウェア サイトへ「誘導」しているかを判断できます。 各接続のポートや宛先ドメインなどの詳細情報を表示するには、テーブル内のエントリをクリックします。たとえば、ある特定のクライアント IP アドレスの [ブロックされたマルウェア接続（Malware Connections Blocked）] が高い数値を示している場合、その列の数値をクリックすると、ブロックされた各接続のリストが表示されます。このリストは、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （72 ページ）を参照してください。 このグラフは、[クライアント マルウェア リスク（Client Malware Risks）]ページ （63 ページ）の [レイヤ4トラフィックモニタ：検出されたマルウェア接続（Layer 4 Traffic Monitor: Malware Connections Detected）] グラフと同じです。
[マルウェアポート（Malware Ports）]	このインタラクティブテーブルを使用すると、レイヤ 4 トラフィック モニタによって最も頻繁にマルウェアが検出されたポートを表示できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[検出されたマルウェア接続の総数（Total Malware Connections Detected）] の数値をクリックすると、そのポートの各接続の詳細情報が表示されます。このリストは、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （72 ページ）を参照してください。

セクション	説明
[検出されたマルウェアサイト（Malware Sites Detected）]	このインタラクティブ テーブルを使用すると、レイヤ 4 トラフィック モニタが最も頻繁にマルウェアを検出したドメインを表示できます。 特定のポートのデータだけを含めるには、テーブル下部のボックスにポート番号を入力し、[ポート別にフィルタ（Filter by Port）] をクリックします。この機能を使用して、サイトまたはポートをブロックするかどうかを判断できます。 詳細を表示するには、テーブル内のエントリをクリックします。たとえば、[ブロックされたマルウェア接続（Malware Connections Blocked）] の数値をクリックすると、特定のサイトに対してブロックされた各接続のリストが表示されます。このリストは、[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] タブに検索結果として表示されます。リストの詳細については、レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （72 ページ）を参照してください。

関連項目

L4 トラフィック モニタ レポートのトラブルシューティング （13 ページ）

[SOCKS プロキシ（SOCKS Proxy）] ページ

[SOCKSプロキシ（SOCKS Proxy）] レポート ページでは、SOCKS プロキシを通じて処理されたトランザクションを、宛先およびユーザに関する情報を含めてグラフおよび表の形式で表示できます。

[SOCKS プロキシ（SOCKS Proxy）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [SOCKS プロキシ（SOCKS Proxy）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

（注） レポートに表示される宛先は、SOCKS クライアント（通常はブラウザ）が SOCKS プロキシに送信するアドレスです。

SOCKS ポリシー設定を変更するには、『*User Guide for AsyncOS for Cisco SecureWeb Appliances*』を参照してください。

表 *7 : [SOCKS*プロキシ（*SOCKS Proxy*）*]*ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
上位SOCKS宛先：トランザクション合計（Top Destinations for SOCKS: Total Transactions）	SOCKS プロキシによって検出された上位の宛先をグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
上位SOCKSユーザ：マルウェアトランザクション（Top Users for SOCKS: Malware Transactions）	SOCKS プロキシによって検出された上位のユーザをグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
[宛先（Destinations）]	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理された宛先ドメインまたはIPアドレスのリストを表示できます。 特定の宛先のデータのみを含めるには、テーブルの下部のボックスにドメイン名または IP アドレスを入力し、[ドメインまたはIPの検索（Find Domain or IP）] をクリックします。
Users	このインタラクティブ テーブルでは、SOCKS プロキシを通じて処理されたユーザまたはIPアドレスのリストを表示できます。 特定のユーザのデータのみを含めるには、テーブルの下部のボックスにユーザ名または IP アドレスを入力し、[ユーザID/クライアントIPアドレスの検索（Find User ID / Client IP Address）] をクリックします。

関連項目

SOCKS プロキシによって処理されるトランザクションの検索 （73 ページ）

[URLカテゴリ（URL Categories）] ページ

[URLカテゴリ（URL Categories）] レポート ページを使用して、システム上のユーザがアクセスしているサイトの URL カテゴリを表示できます。

[URL カテゴリ（URL Categories）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [URL カテゴリ（URL Categories）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

[URL カテゴリ（URL Categories）] ページには次の情報が表示されます。

表 *8 : [URL*カテゴリ（*URL Categories***）*]* ページの詳細**

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
上位 URL カテゴリ：総トランザクション数（Top URL Categories: Total Transactions）	サイト上でアクセスされた上位 URL カテゴリがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
上位URLカテゴリ：ブロックおよび警告されたトランザクション（Top URL Categories: Blocked and Warned Transactions）	トランザクションごとに発生するブロックまたは警告アクションをトリガーした上位 URL がグラフ形式で表示されます。たとえば、ユーザがある URL にアクセスしたが、特定のポリシーが適用されているために、ブロックアクションまたは警告がトリガーされたとします。この URL は、ブロックまたは警告されたトランザクションとしてこのグラフに追加されます。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
[上位 YouTube カテゴリ（Top Youtube Categories）]：[トランザクションの合計数 （Total Transactions）]	サイト上でアクセスされている上位の YouTube カテゴリを表示できます（グラフ形式）。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。

セクション	説明
[上位 YouTube カテゴリ（Top Youtube Categories）]：[ブロックされたトランザクションと警告されたトランザクション（Blocked and Warned Transactions）]	トランザクションごとに発生するブロックアクションまたは警告アクションをトリガーした上位の YouTube URL を表示できます（グラフ形式）。たとえば、ユーザが特定の YouTube URL にリダイレクトされ、特定のポリシーが適用されている場合は、ブロックアクションまたは警告がトリガーされました。この YouTube URL は、ブロックまたは警告されたトランザクションとしてこのグラフに一覧表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（66 ページ）を参照してください。
[一致したURLカテゴリ（URL Categories Matched）]	[一致したURLカテゴリ（URL Categories Matched）] インタラクティブ テーブルには、指定した時間範囲内における URL カテゴリ別のトランザクションの処理、使用された帯域幅、各カテゴリで費やされた時間が表示されます。 未分類の URL が多数ある場合は、未分類の URL の削減（48 ページ）を参照してください。

未分類の URL の削減

未分類の URL の比率が 15 ～ 20 % を上回る場合は、次のオプションを検討してください。

- 特定のローカライズされた URL の場合は、カスタム URL カテゴリを作成し、特定のユーザまたはグループポリシーに適用できます。これらのトランザクションは、代わりに [URL フィルタリングバイパス（URL Filtering Bypassed）] 統計情報に含まれるようになります。これを行うには、『AsyncOS for Cisco SecureWeb Appliance User Guide』でカスタム URL カテゴリについて参照してください。
- 既存またはその他のカテゴリに含めるべきサイトについては、誤って分類された URL と未分類の URL のレポート （49 ページ）を参照してください。

URL カテゴリ セットの更新とレポート

SecureWeb Applianceでは、一連の定義済み URL カテゴリが定期的に自動更新される場合があります。

これらの更新が行われると、古いカテゴリに関連づけられたデータが古すぎてレポートに含まれなくなるまで、古いカテゴリ名は引き続きレポートに表示されます。URL カテゴリ セットの更新後に生成されたレポートデータには新しいカテゴリが使用されるので、同じレポートに新旧両方のカテゴリが表示される場合があります。

[URL カテゴリ（URL Categories）] ページとその他のレポーティング ページの併用

[URL カテゴリ（URL Categories）] ページを [アプリケーションの表示（Application Visibility）] ページ（40 ページ）、[ユーザの詳細（User Details）] ページ（Web レポーティング）（53 ページ）、および [ユーザ（Users）] ページ（51 ページ）と併用して、特定のユーザーや特定のユーザーがアクセスしようとしているアプリケーションまたは Web サイトのタイプを調査できます。

たとえば、[URLカテゴリ（URL Categories）] ページ（47 ページ）からは、サイトでアクセスしたすべての URL カテゴリの詳細を示す人事リソース向けの高レベルレポートを生成できます。同じページの [URLカテゴリ（URL Categories）] インタラクティブ テーブルでは、URL カテゴリ「Streaming Media」に関するさらに詳しい情報を収集できます。[ストリーミングメディア（Streaming Media）] カテゴリ リンクをクリックすると、特定の [URLカテゴリ（URL Categories）] レポート ページが表示されます。このページには、ストリーミング メディア サイトにアクセスしている上位ユーザが表示されるだけでなく（[カテゴリ別の総トランザクション上位ユーザ（Top Users by Category for Total Transactions）] セクション）、YouTube.com や QuickPlay.com などのアクセスされたドメインも表示されます（[一致したドメイン（Domains Matched）] インタラクティブ テーブル）。

この時点で、特定のユーザに関するさらに詳しい情報を得られます。たとえば、特定のユーザによる使用が突出しているので、そのユーザのアクセス先を正確に確認する必要があるとします。ここから、[ユーザ（Users）] インタラクティブ テーブルのユーザをクリックすることができます。このアクションにより [ユーザ（Users）] ページ（51 ページ）が表示され、そのユーザーのトレンドを確認し、そのユーザーの Web での行動を正確に把握できます。

さらに詳しい情報が必要な場合は、インタラクティブ テーブルで [完了したトランザクション（Transactions Completed）] リンクをクリックして、Web トラッキングの詳細を表示できます。これにより、[Webトラッキング（Web Tracking）] ページに 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（67 ページ）が表示され、ユーザがサイトにアクセスした日付、完全な URL、その URL で費やされた時間などについて、実際の詳細情報を確認できます。

誤って分類された URL と未分類の URL のレポート

誤って分類された URL と未分類の URL について、次の URL で報告できます。

https://talosintelligence.com/tickets。

送信内容は評価され、今後のルール更新への組み込みに活用されます。

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。

[HTTPS レポート（HTTPS Reports）] ページ

[HTTPS レポート（HTTPS Reports）] レポート ページでは、管理対象のアプライアンスの HTTP/HTTPS トラフィック サマリー（トランザクションまたは帯域幅の使用量）のすべてを集約しています。

また、管理対象のアプライアンスを通過する個々の HTTP/HTTPS Web トラフィックの場合、クライアント側接続またはサーバ側接続のいずれかに基づいてサポート対象の暗号のサマリーを確認することもできます。

[HTTPS レポート（HTTPS Reports）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [HTTPS レポート（HTTPS Reports）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポートページの使用 （9 ページ）を参照してください。

表 *9 : [HTTPS*レポート（*HTTPS Reports*）*]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、時間範囲の変更 （3 ページ）を参照してください。
[Webトラフィックサマリー（Web Traffic Summary）]	アプライアンスの Web トラフィック サマリーは、次のいずれかの方法で表示できます。 • **トランザクション**：グラフ形式の HTTP または HTTPS Web トランザクションの数と表形式の HTTP または HTTPS Web トランザクションの割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。 • **帯域幅の使用量**：グラフ形式の HTTP または HTTPS Web トラフィックで消費される帯域幅の大きさと表形式の HTTP または HTTPS 帯域幅の使用量の割合に基づいて Web トラフィック サマリーを表示するには、ドロップダウン リストからこのオプションを選択します。
トレンド：Web トラフィック	次のいずれかの方法で必要な時間範囲に基づいてアプライアンスの Web トラフィックのトレンド グラフを表示することができます。 • **Web トラフィック トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTP と HTTPS Web トラフィックの累積トレンドを表示するには、ドロップダウン リストからこのオプションを選択します。 • **HTTPS トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTPS Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。 • **HTTP トレンド**：トランザクションまたは帯域幅の使用量に基づいて HTTP Web トラフィックのトレンドを表示するには、ドロップダウン リストからこのオプションを選択します。

セクション	説明
暗号	暗号のサマリーは、次のいずれかの方法で表示できます。 • クライアント側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのクライアント側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。 • サーバ側接続別：グラフ形式で HTTP または HTTPS Web トラフィックのサーバ側で使用される暗号のサマリーを表示するには、ドロップダウンリストからこのオプションを選択します。

[ユーザ（Users）] ページ

[ユーザ（Users）] レポート ページには、各ユーザの Web レポーティング情報を表示できる複数のリンクが表示されます。

[ユーザー（Users）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [ユーザー（Users）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

[ユーザ（Users）] ページでは、システム上のユーザ（1 人または複数）がインターネット、特定のサイト、または特定の URL で費やした時間と、そのユーザが使用している帯域幅の量を表示できます。

（注） セキュリティ管理アプライアンスがサポートできる SecureWeb Appliance上のユーザーの最大数は 500 です。

[ユーザ（Users）] ページには、システム上のユーザに関する次の情報が表示されます。

表 *10 : [ユーザ（Users）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。

セクション	説明
上位ユーザ：ブロックされたトランザクション（Top Users: Transactions Blocked）	上位ユーザ（IPアドレスまたはユーザ名で表示）と、そのユーザがブロックされたトランザクションの数がグラフ形式で表示されます。レポーティングを目的として、ユーザ名または IP アドレスを認識できないようにすることができます。このページやスケジュール済みのレポートでユーザー名を認識できないようにする方法の詳細については、『*User Guide for AsyncOS for Cisco Content Security Management Appliances*』を参照してください。デフォルト設定では、すべてのユーザー名が表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
上位ユーザ：使用帯域幅（Top Users: Bandwidth Used）	システム上で最も多くの帯域幅を使用している上位ユーザ（IPアドレスまたはユーザ名で表示）がグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。
ユーザ（Users）	このインタラクティブテーブルを使用すると、特定のユーザ ID またはクライアント IP アドレスを検索できます。[ユーザ（User）]テーブル下部のテキストフィールドに特定のユーザ ID またはクライアント IP アドレスを入力し、[ユーザID/クライアントIPアドレスの検索（Find User ID / 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。 特定のユーザをクリックすると、さらに具体的な情報を得ることができます。詳細については、[ユーザの詳細（User Details）] ページ（Web レポーティング） （53 ページ）を参照してください。

（注） クライアント IP アドレスの代わりにユーザ ID を表示するには、セキュリティ管理アプライアンスを設定し、LDAP サーバからユーザ情報を取得する必要があります。

[ユーザの詳細（User Details）] ページ（Web レポーティング）

[ユーザの詳細（User Details）] ページでは、[ユーザ（Users）] レポート ページのインタラクティブ テーブルで指定したユーザに関する具体的な情報を確認できます。

[ユーザの詳細（User Details）] ページでは、システムでの個々のユーザのアクティビティを調査できます。特に、ユーザ レベルの調査を実行している場合に、ユーザがアクセスしているサイト、ユーザが直面しているマルウェアの脅威、ユーザがアクセスしている URL カテゴリ、これらのサイトで特定のユーザが費やしている時間などを確認する必要があるときは、このページが役立ちます。

特定のユーザの [ユーザの詳細（User Details）] ページを表示するには、[ユーザ（Users）] レポート ページの [ユーザ（Users）] インタラクティブ テーブルでそのユーザをクリックします。

[ユーザの詳細（User Details）] ページには、システム上の個々のユーザに関係する次の情報が表示されます。

表 *11 : [ユーザの詳細（User Details）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
URLカテゴリ：トランザクション合計（URL Categories: Total Transactions）	特定のユーザが使用している特定の URL カテゴリがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート（20 ページ）を参照してください。
トレンド：トランザクション合計（Trend: Total Transactions）	このトレンド グラフを使用すると、特定のユーザのすべての Web トランザクションを表示できます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。 たとえば、1 日の特定の時刻に Web トラフィックに大きなスパイクが存在するかどうか、また、それらのスパイクがいつ発生したかが、このグラフからわかります。[時間範囲（Time Range）] ドロップダウン リストを使用すると、このグラフを拡張し、このユーザが Web を閲覧していた時間を表示するきめ細かさを増減できます。

セクション	説明
[一致したURLカテゴリ（URL Categories Matched）]	[一致したURLカテゴリ（URL Categories Matched）] インタラクティブ テーブルは、完了したトランザクションとブロックされたトランザクションの両方について、一致したカテゴリが表示されます。 テーブル下部のテキスト フィールドに入力して [URLカテゴリの検索（Find URL Category）] をクリックすると、特定の URL カテゴリを検索できます。カテゴリは正確に一致している必要はありません。 すでに定義されている一連の URL カテゴリは更新されることがあります。こうした更新によるレポート結果への影響については、URL カテゴリ セットの更新とレポート（20 ページ）を参照してください。
[一致したドメイン（Domains Matched）]	[一致したドメイン（Domains Matched）] インタラクティブ テーブルは、ユーザがアクセスしたドメインまたは IP アドレスを示します。また、ユーザがこれらのカテゴリで費やした時間、およびカラム ビューで設定したその他のさまざまな情報も参照できます。 テーブル下部のテキスト フィールドに入力して [ドメインまたはIPの検索（Find Domain or IP）] をクリックすると、特定のドメインまたは IP アドレスを検索できます。ドメインまたは IP アドレスは正確に一致している必要はありません。
[一致したアプリケーション（Applications Matched）]	[一致したアプリケーション（Applications Matched）] インタラクティブ テーブルには、特定のユーザが使用しているアプリケーションが表示されます。たとえば、Flash ビデオを多用するサイトにユーザがアクセスしている場合は、[アプリケーション（Application）] 列にそのアプリケーション タイプが表示されます。 テーブル下部のテキスト フィールドに入力して [アプリケーションの検索（Find Application）] をクリックすると、特定のアプリケーション名を検索できます。アプリケーションの名前は正確に一致している必要はありません。

セクション	説明
Secure Endpoint 検出された脅威	[セキュアエンドポイントで検出された脅威（Secure Endpoint Threats Detected）] インタラクティブテーブルには、Secure Endpointエンジンによって検出されたマルウェア脅威ファイルが表示されます。 テーブル下部のテキストフィールドに入力して[マルウェア脅威ファイルSHA 256の検索（Find malware Threat File SHA 256）] をクリックすると、マルウェア脅威ファイルの特定の SHA 値に関するデータを検索できます。アプリケーションの名前は正確に一致している必要はありません。
[検出されたマルウェア脅威（Malware Threats Detected）]	[検出されたマルウェア脅威（Malware Threats Detected）] インタラクティブ テーブルには、特定のユーザによってトリガーされた上位のマルウェア脅威が表示されます。 テーブル下部のテキストフィールドに入力して[マルウェア脅威の検索（Find Malware Threat）] をクリックすると、特定のマルウェア脅威名に関するデータを検索できます。マルウェア脅威の名前は正確に一致している必要はありません。
[一致したポリシー（Policies Matched）]	[一致したポリシー（Policies Matched）] インタラクティブテーブルには、Web へのアクセス時にこのユーザに適用されたポリシー グループが表示されます。 テーブル下部のテキストフィールドに入力して[ポリシー検索（Find Policy）] をクリックすると、特定のポリシー名を検索できます。ポリシーの名前は正確に一致している必要はありません。

（注） [クライアントマルウェアリスクの詳細（Client Malware Risk Details）] テーブルのクライアント レポートでは、ユーザ名の末尾にアスタリスク（*）が付いていることがあります。たとえば、クライアント レポートに「jsmith」と「jsmith*」の両方のエントリが表示される場合があります。アスタリスク（*）が付いているユーザ名は、ユーザの指定したユーザ名が認証サーバで確認されていないことを示しています。この状況は、認証サーバがその時点で使用できず、かつ認証サービスを使用できないときもトラフィックを許可するようにアプライアンスが設定されている場合に発生します。

[Webサイト（Web Sites）] ページ

[Webサイト（Web Sites）] レポート ページは、管理対象のアプライアンスで発生しているアクティビティ全体を集約したものです。このレポート ページを使用すると、特定の時間範囲内にアクセスされたリスクの高い Web サイトをモニタすることができます。

[Web サイト（Web Sites）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > [Web サイト（Web Sites）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

[Webサイト（Web Sites）] ページには次の情報が表示されます。

表 *12 : [Webサイト（Web Sites）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
上位ドメイン：トランザクション合計（Top Domains: Total Transactions）	Webサイト上でアクセスされた上位のドメインがグラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ） チャート化するデータの選択 （66 ページ）を参照してください。
上位ドメイン：ブロックされたトランザクション（Top Domains: Transactions Blocked）	トランザクションごとに発生するブロック アクションをトリガーした上位ドメインが、グラフ形式で表示されます。 グラフの表示をカスタマイズするには、グラフ上の ✓ をクリックします。詳細については、（Web レポートのみ） チャート化するデータの選択 （66 ページ）を参照してください。 たとえば、ユーザがあるドメインにアクセスしたが、特定のポリシーが適用されていたために、ブロック アクションがトリガーされたとします。このドメインはブロックされたトランザクションとしてこのグラフに追加され、ブロック アクションをトリガーしたドメイン サイトが表示されます。

セクション	説明
[一致したドメイン（Domains Matched）]	このインタラクティブ テーブルでは、Web サイト上でアクセスされたドメインを検索できます。特定のドメインをクリックすると、より詳細な情報を得ることができます。[Web トラッキング（Web Tracking）] ページに [プロキシサービス（Proxy Services）] タブが表示され、トラッキング情報と、特定のドメインがブロックされた理由を確認できます。 特定のドメインをクリックすると、そのドメインの上位ユーザ、そのドメインでの上位トランザクション、一致した URL カテゴリ、および検出されたマルウェアの脅威が表示されます。

Secure Endpoint ページ

Secure Endpoint は、次によりゼロデイやファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

ファイル レピュテーション フィルタリングとファイル分析の詳細については、ユーザーガイドまたは *SecureWeb Appliance*の *AsyncOS* のオンラインヘルプを参照してください。

Secure Endpoint レポートページには、次のレポートビューが表示されます。

- – [セキュアエンドポイントサマリー（Secure Endpoint Summary）] ページ
- Secure Endpoint – [ファイル分析（File Analysis）] ページ

Secure Endpoint レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）] > Secure Endpoint を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

Secure Endpoint – [セキュアエンドポイントサマリー（Cisco Secure Endpoint Summary）] ページ

[セキュアエンドポイント（Secure Endpoint）] レポートページの [セキュアエンドポイントサマリー（Cisco Secure Endpoint Summary）] セクションには、ファイル レピュテーション サービスによって識別された、ファイルベースの脅威が表示されます。

各 SHA にアクセスしようとしたユーザー、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。

[マルウェア脅威ファイル（Malware Threat File）] インタラクティブ テーブルのリンクをクリックすると、レポートに対して選択された時間範囲に関係なく、設定可能な最大時間範囲内で検

出されたそのファイルのすべてのインスタンスが [Webトラッキング（Web Tracking）] に表示されます。

圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Secure Endpoint）] レポートに含まれます。

[セキュアエンドポイント（Secure Endpoint）] ページの [セキュアエンドポイントサマリー（Cisco Secure Endpoint Summary）] セクションには、次の情報を表示できます。

- Secure Endpoint エンジンのファイル レピュテーション サービスによって識別されたファイルの概要（グラフ形式）。
- 上位のマルウェア脅威ファイル（グラフ形式）。
- ファイル タイプに基づいた上位の脅威ファイル（グラフ形式）。
- 選択した時間範囲のすべてのマルウェア脅威ファイルに関するトレンド グラフ。
- 上位のマルウェア脅威ファイルを一覧表示する [マルウェア脅威ファイル（Malware Threat Files）] インタラクティブ テーブル。
- このアプライアンスで処理され、トランザクションの処理後に判定が変わったファイルを一覧表示する [レトロスペクティブ判定変更（Retrospective Verdict Change）] インタラクティブテーブルを含むファイル。この状況の詳細については、お使いの SecureWeb Appliance のマニュアルを参照してください。

  1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。

  同一ファイルの複数の SecureWeb Appliance で判定のアップデートが異なる場合は、最も新しいタイムスタンプの結果が表示されます。

  SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内にこの SHA-256 が含まれた、すべてのトランザクションの Web トラッキング結果が表示されます。

Secure Endpoint – [ファイル分析（File Analysis）] ページ

[セキュアエンドポイント（Secure Endpoint）] レポートページの [ファイル分析（File Analysis）] セクションには、分析のために送信された各ファイルについて、時刻と判定（または中間判定）が表示されます。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。

オンプレミスの Cisco Secure Endpoint Malware Analytics アプライアンスでの導入の場合：Cisco Secure Endpoint Malware Analytics アプライアンスで許可リストに含まれているファイルは、「クリーン」として表示されます。許可リストについては、Cisco Secure Endpoint Malware Analytics のオンラインヘルプを参照してください。

ドリルダウンすると、各ファイルの脅威の特性およびスコアを含む詳細な分析結果が表示されます。

また、分析を実行したサーバーで SHA に関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある Cisco Secure Endpoint Malware Analytics リンクをクリックします。

圧縮ファイルまたはアーカイブ済みファイルから抽出したファイルが分析用に送信されると、抽出されたファイルの SHA 値のみが [ファイル分析（File Analysis）] レポートに含まれます。

[セキュアエンドポイント（Secure Endpoint）] レポートページの [ファイル分析（File Analysis）] セクションを使用すると、次の情報を表示できます。

- Secure Endpoint エンジンのファイル分析サービスによってファイル分析のためにアップロードされたファイルの数。
- ファイル分析要求が完了しているファイルのリスト。
- ファイル分析要求の処理待ちとなっているファイルのリスト。

[マルウェア対策（Anti-Malware）] ページ

[マルウェア対策（Anti-Malware）] レポートページはセキュリティ関連のレポーティングページであり、イネーブルなスキャン エンジン（Webroot、Sophos、McAfee、または Adaptive Scanning）によるスキャン結果が反映されます。

[マルウェア対策（Anti-Malware）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから [モニターリング（Monitoring）]>[マルウェア対策（Anti-Malware）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

このページを使用して、Web ベースのマルウェアの脅威を特定およびモニタすることができます。

（注） L4 トラフィック モニタリングで検出されたマルウェアのデータを表示するには、次を参照してください。[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ （42 ページ）

[マルウェア対策（Anti-Malware）] ページには次の情報が表示されます。

表 *13 : [マルウェア対策（Anti-Malware）] ページの詳細*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。

セクション	説明
上位マルウェアカテゴリ（Top Malware Categories）	特定のカテゴリタイプによって検出された上位のマルウェアカテゴリをグラフ形式で表示できます。有効なマルウェアカテゴリの詳細については、マルウェアのカテゴリについて（61 ページ）を参照してください。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（66 ページ）を参照してください。
上位マルウェア脅威（Top Malware Threats）	上位のマルウェア脅威をグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の✓をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択（66 ページ）を参照してください。
[マルウェアカテゴリ（Malware Categories）]	[マルウェアカテゴリ（Malware Categories）]インタラクティブ テーブルには、[上位マルウェアカテゴリ（Top Malware Categories）]チャートに表示されている個々のマルウェアカテゴリに関する詳細情報が表示されます。 [マルウェアカテゴリ（Malware Categories）]インタラクティブテーブル内のリンクをクリックすると、個々のマルウェアカテゴリおよびネットワークでの検出場所に関するさらに詳しい情報が表示されます。 例外：このテーブルの [アウトブレイクヒューリスティック（Outbreak Heuristics）] リンクを使用すると、そのカテゴリでいつトランザクションが発生したかを示すチャートが表示されます。 有効なマルウェアカテゴリの詳細については、マルウェアのカテゴリについて（61 ページ）を参照してください。
[マルウェア脅威（Malware Threats）]	[マルウェアの脅威（Malware Threats）] インタラクティブテーブルには、[上位マルウェア脅威（Top Malware Threats）] セクションに表示されている個々のマルウェアの脅威に関する詳細情報が表示されます。 「アウトブレイク（Outbreak）」のラベルと番号が付いている脅威は、他のスキャンエンジンとは別に、Adaptive Scanning 機能によって特定された脅威です。

[マルウェア カテゴリ（Malware Category）] レポート ページ

手順

ステップ 1 [レポート（Reports）] > [マルウェア対策（Anti-Malware）] を選択します。

ステップ 2 [マルウェア カテゴリ（Malware Categories）] インタラクティブ テーブルで、[マルウェア カテゴリ（Malware Category）] カラム内のカテゴリをクリックします。

[マルウェアの脅威（Malware Threat）] レポート

[マルウェア脅威（Malware Threats）] レポート ページには、特定の脅威にさらされているクライアント、および感染した可能性があるクライアントのリストが表示され、[クライアントの詳細（Client Detail）] ページへのリンクがあります。レポート上部のトレンド グラフには、指定した時間範囲内で脅威に関してモニターされたトランザクションおよびブロックされたトランザクションが表示されます。下部のテーブルには、指定した時間範囲内で脅威に関してモニターされたトランザクションおよびブロックされたトランザクションの実際の数が表示されます。

このレポートを表示するには、[マルウェア対策（Anti-Malware）] レポート ページの [マルウェアのカテゴリ（Malware Category）] 列でカテゴリをクリックします。

詳細については、テーブルの下の [サポートポータルマルウェア詳細（Support Portal Malware Details）] リンクをクリックしてください。

マルウェアのカテゴリについて

SecureWeb Appliance は、次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。

マルウェアのタイプ	説明
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネットアクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャルエンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システムプロセスやユーザアクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモートホスト/サイトにアクセスして、リモートホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモートホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。

マルウェアのタイプ	説明
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

[クライアント マルウェア リスク（Client Malware Risks）] ページ

[レポート（Reporting）]>[クライアント マルウェア リスク（Client Malware Risk）] ページは、クライアントマルウェア リスク アクティビティをモニターするために使用できるセキュリティ関連のレポーティング ページです。[クライアント マルウェア リスク（Client Malware Risk）] ページには、L4 トラフィック モニター（L4TM）によって特定された、頻度の高いマルウェア接続に関与しているクライアント IP アドレスが表示されます。

表 *14 : [クライアント マルウェア リスク（Client Malware Risks）] ページの詳細情報*

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
[Webプロキシ:モニタまたはブロックされた上位クライアント（Web Proxy: Top Clients Monitored or Blocked）]	このチャートには、マルウェアのリスクが発生した上位 10 人のユーザが表示されます。
[L4トラフィックモニタ:検出されたマルウェア接続（L4 Traffic Monitor: Malware Connections Detected）]	このチャートには、組織内で最も頻繁にマルウェア サイトに接続しているコンピュータの IP アドレスが表示されます。
[Webプロキシ:クライアントマルウェアリスク（Web Proxy: Client Malware Risk）]	[Webプロキシ：クライアントマルウェアリスク（Web Proxy: Client Malware Risk）] インタラクティブ テーブルには、[Webプロキシ：マルウェアリスク別上位クライアント（Web Proxy: Top Clients by Malware Risk）] セクションに表示されている個々のクライアントに関する詳細情報が表示されます。
L4トラフィックモニタ:マルウェアリスク別クライアント（L4 Traffic Monitor: Clients by Malware Risk）	[L4トラフィックモニタ：マルウェアリスク別クライアント（L4 Traffic Monitor: Clients by Malware Risk）] インタラクティブ テーブルには、組織内でマルウェア サイトに頻繁にアクセスしているコンピュータの IP アドレスが表示されます。

[Web レピュテーション フィルタ（Web Reputation Filters）] ページ

[Webレピュテーションフィルタ（Web Reputation Filters）] レポート ページでは、指定した時間範囲内のトランザクションに対する Web レピュテーション フィルタ（ユーザが設定）の結果を確認できます。

[Web レピュテーションフィルタ（Web Reputation Filters）] レポートページを表示するには、[レポート（Reports）] ドロップダウンから、[モニターリング（Monitoring）] > [Web レピュテーションフィルタ（Web Reputation Filters）] を選択します。詳細については、新しい Web インターフェイスでのインタラクティブ レポート ページの使用 （9 ページ）を参照してください。

Web レピュテーション フィルタとは

Web レピュテーション フィルタは、Web サーバの動作を分析し、URL ベースのマルウェアが含まれている可能性を判断するためのレピュテーション スコアを URL に割り当てます。この機能は、エンドユーザのプライバシーや企業の機密情報を危険にさらすURLベースのマルウェアを防ぐために役立ちます。 SecureWeb Appliance は、URL レピュテーション スコアを使用して、疑わしいアクティビティを特定するとともに、マルウェア攻撃を未然に防ぎます。Web レピュテーション フィルタは、アクセス ポリシーと復号ポリシーの両方と組み合わせて使用できます。

Web レピュテーション フィルタでは、統計データを使用してインターネット ドメインの信頼性が評価され、URLのレピュテーションにスコアが付けられます。特定のドメインが登録されていた期間、Web サイトがホストされている場所、Web サーバがダイナミック IP アドレスを使用しているかどうかなどのデータを使用して、特定の URL の信頼性が判定されます。

Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定されます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス

- ドメインのレジストラ情報
- IP アドレス情報

Web レピュテーションフィルタの詳細については、『*User Guide for AsyncOS for SecureWeb Appliances*』の「Web Reputation Filters」を参照してください。

[Webレピュテーションフィルタ（Web Reputation Filters）] ページには次の情報が表示されます。

表 *15 : [Web*レピュテーションフィルタ（*Web Reputation Filters*）*]* ページの詳細

セクション	説明
[時間範囲（Time Range）]（ドロップダウン リスト）	レポートの時間範囲を選択します。詳細については、レポートの時間範囲の選択 （4 ページ）を参照してください。
[Webレピュテーションアクション(トレンド)（Web Reputation Actions (Trend)）]	指定した時間における Web レピュテーション アクションの合計数をグラフ形式で表示できます。このセクションでは、時間の経過に伴う Web レピュテーション アクションの潜在的なトレンドを確認できます。
[Webレピュテーションアクション(ボリューム)（Web Reputation Actions (Volume)）]	Web レピュテーションアクションのボリュームをトランザクション数の比率で表示できます。
[WBRSによってブロックされるWebレピュテーションの脅威タイプ（Web Reputation Threat Types Blocked by WBRS）]	Web レピュテーションフィルタリングによってブロックされたトランザクションで発生した脅威のタイプをグラフ形式で表示できます。 （注） WBRS では、常に、脅威のタイプを識別できるわけではありません。

セクション	説明
[他のトランザクションで脅威タイプが検知されました（Threat Types Detected in Other Transactions）]	Web レピュテーション フィルタリングによってブロックされなかったトランザクションで発生した脅威のタイプをグラフ形式で表示できます。 グラフの表示をカスタマイズするには、グラフ上の をクリックします。詳細については、（Web レポートのみ）チャート化するデータの選択 （66 ページ）を参照してください。 これらの脅威がブロックされなかった理由には、次のようなものがあります。 • すべての脅威に、ブロッキングのしきい値を満たすスコアがあるわけではありません。ただし、アプライアンスのその他の機能は、これらの脅威を検出する可能性があります。 • ポリシーが、脅威を許可するよう設定されている可能性があります。 （注） WBRS では、常に、脅威のタイプを識別できるわけではありません。
Web レピュテーションアクション（スコアによる内訳）（Web Reputation Actions (Breakdown by Score)）	Adaptive Scanning がイネーブルでない場合、このインタラクティブ テーブルには各アクションの Web レピュテーション スコアの内訳が表示されます。
一致した脅威カテゴリ	一致した脅威カテゴリを表示できます（グラフ形式）。

Web レピュテーション設定の調整

指定済みの Web レピュテーションの設定は、レポート結果に基づいて調整することができます。たとえば、しきい値スコアを調整したり、Adaptive Scanning をイネーブルまたはディセーブルにしたりできます。Web レピュテーション設定の詳細については、『*User Guide for AsyncOS for Cisco SecureWeb Appliances*』を参照してください。

（Web レポートのみ）チャート化するデータの選択

各 Web レポーティング ページのデフォルト チャートには、一般に参照されるデータが表示されますが、代わりに異なるデータをチャート化するように選択できます。ページに複数のチャートがある場合は、チャートごとに変更できます。

通常、チャートのオプションは、レポート内のテーブルのカラムと同じです。ただし、チャート化できない列もあります。

チャートには、関連付けられたテーブルに表示するように選択した項目（行）数に関係なく、テーブルの列の使用可能なすべてのデータが反映されます。

手順

ステップ 1 特定のチャートで をクリックします。

ステップ 2 表示する必要があるデータを選択します。チャートのプレビューは、選択したオプションに従って表示されます。

ステップ 3 [Apply] をクリックします。

新しい Web インターフェイスでの Web トラッキング

[Webトラッキング検索（Web Tracking Search）] ページでは、個々のトランザクションまたは疑わしいトランザクションのパターンを検索し、その詳細を表示することができます。展開で使用するサービスに基づき、関連するタブで検索を行います。

- 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 （67 ページ）
- レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索 （72 ページ）
- SOCKS プロキシによって処理されるトランザクションの検索 （73 ページ）
- Web トラッキングの検索結果の使用 （73 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示 （74 ページ）

Web プロキシと レイヤ 4 トラフィックモニターの違いについては、『*User Guide for AsyncOS for Cisco SecureWeb Appliances*』の「Understanding How the SecureWeb Appliance Works」セクションを参照してください。

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

[Webトラッキング検索（Web Tracking Search）]ページの[プロキシサービス（Proxy Services）]タブを使用して、個々のセキュリティ コンポーネント、およびアクセプタブル ユース適用コンポーネントから収集された Web トラッキング データを検索できます。このデータには、レイヤ4トラフィック モニタリング データまたはSOCKSプロキシによって処理されたトランザクションは含まれません。

このデータを使用して、次の役割を補助することができます。

- **人事または法律マネージャ。**所定の期間内の従業員に関するレポートを調査します。

たとえば、[プロキシサービス（Proxy Services）] タブを使用して、ユーザがアクセスしている特定の URL について、ユーザがアクセスした時刻や、それが許可された URL であるかどうか、といった情報を取得できます。

- **ネットワーク セキュリティ管理者。**会社のネットワークが従業員のスマートフォンを介してマルウェアの脅威にさらされていないかどうかを調査します。

所定の期間内に記録されたトランザクション（ブロック、モニタリング、および警告されたトランザクション、完了したトランザクションなど）の検索結果を表示できます。URL カテゴリ、マルウェアの脅威、アプリケーションなど、複数の条件を使用してデータ結果をフィルタリングすることもできます。

（注） Web プロキシは、「OTHER-NONE」以外の ACL デシジョン タグを含むトランザクションのみレポートします。

[プロキシサービス（Proxy Services）] タブと他の Web レポーティング ページの併用例については、を参照してください。

手順

ステップ 1 セキュリティ管理アプライアンスで、ドロップダウン リストから [Web] を選択します。

ステップ 2 [URL カテゴリ（URL Categories）] ページとその他のレポーティング ページの併用 （49 ページ）[トラッキング（Tracking）] > [プロキシサービス（Proxy Services）] を選択します。

ステップ 3 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定（Advanced）] をクリックします。

ステップ 4 検索条件を入力します。

表 *16 : [プロキシサービス（Proxy Services）] タブの Web トラッキング検索条件*

オプション	説明
デフォルトの検索条件	
時間範囲（Time Range）	レポート対象の時間範囲を選択します。セキュリティ管理アプライアンスで使用できる時間範囲については、レポートの時間範囲の選択 （4 ページ）を参照してください。
ユーザ/クライアント IPv4またはIPv6	レポートに表示される認証ユーザ名、または追跡対象のクライアント IP アドレスを任意で入力します。IP 範囲を 172.16.0.0/16 のような CIDR 形式で入力することもできます。 このフィールドを空にしておくと、すべてのユーザに関する検索結果が返されます。

オプション	説明
Web サイト（Website）	追跡対象の Web サイトを任意で入力します。このフィールドを空にしておくと、すべての Web サイトに関する検索結果が返されます。
トランザクション タイプ（Transaction Type）	追跡対象のトランザクションのタイプを [すべてのトランザクション（All Transactions）]、[完了（Completed）]、[ブロックされた（Blocked）]、[モニタ対象（Monitored）]、または [警告対象（Warned）] から選択します。
高度な検索条件	
URL カテゴリ	URL カテゴリでフィルタリングするには、[URLカテゴリによるフィルタ（Filter by URL Category）] を選択し、フィルタリング対象とするカスタムまたは定義済み URL カテゴリの先頭文字を入力します。表示されたリストからカテゴリを選択します。 ドロップダウン リストに表示されるエンジン名に関係なく、カテゴリ名に一致する最近のトランザクションがすべて含まれます。
マルウェアの脅威	特定のマルウェアの脅威でフィルタリングするには、[マルウェア脅威によるフィルタ（Filter by Malware Threat）] を選択し、フィルタリングに使用するマルウェアの脅威名を入力します。 マルウェア カテゴリでフィルタリングするには、[マルウェアカテゴリによるフィルタ（Filter by Malware Category）] を選択し、フィルタリングに使用するマルウェア カテゴリを選択します。説明については、マルウェアのカテゴリについて （61 ページ）を参照してください。
アプリケーション	アプリケーションでフィルタ処理するには、[アプリケーション（Application）] を選択し、フィルタ処理するアプリケーションを選択します。 アプリケーションタイプでフィルタ処理するには、[アプリケーションタイプ（Application Type）] を選択し、フィルタ処理するアプリケーションタイプを選択します。
WBRS	[WBRS] セクションでは、Web ベースのレピュテーション スコアによるフィルタリングと、特定の Web レピュテーションの脅威によるフィルタリングが可能です。 • Web レピュテーション スコアでフィルタリングするには、[スコア範囲（Score Range）] を選択し、フィルタリングに使用する上限値と下限値を選択します。あるいは、[スコアなし（No Score）] を選択すると、スコアがない Web サイトをフィルタリングできます。 • Web レピュテーションの脅威でフィルタリングするには、[レピュテーション脅威によるフィルタ（Filter by Reputation Threat）] を選択し、フィルタリングに使用する Web レピュテーションの脅威を入力します。 WBRS スコアの詳細は、『IronPort AsyncOS for Web User Guide』を参照してください。

オプション	説明
脅威カテゴリ	特定の脅威カテゴリでフィルタ処理するには、[脅威カテゴリ（Threat Category）] セクションを展開し、必要な脅威カテゴリを選択します。 使用可能なすべての脅威カテゴリを選択するには、[すべて選択（Select All）] をクリックします。
YouTube カテゴリ	特定の YouTube カテゴリでフィルタ処理するには、[YouTube カテゴリ（YouTube Category）] セクションを展開し、表示する YouTube カテゴリを選択します。 使用可能なすべての YouTube カテゴリを選択するには、[すべて選択（Select All）] をクリックします。アクティブなカテゴリと非アクティブなカテゴリ別にフィルタ処理することもできます。
ポリシー	ポリシーグループでフィルタ処理するには、[ポリシー（Policy）] を選択し、フィルタ処理するポリシーグループ名を入力します。 このポリシーが SecureWeb Appliance で宣言済みであることを確認してください。
AnyConnect セキュア モビリティ（AnyConnect Secure Mobility）	リモートアクセスまたはローカルアクセスでフィルタ処理するには、[ユーザーの場所（User Location）] を選択し、アクセスタイプを選択します。すべてのアクセス タイプを含めるには、[フィルタを無効にする（Disable Filter）] を選択します （旧リリースでは、このオプションは Mobile User Security と呼ばれていました。）
Secure Endpoint	ファイル レピュテーション サービスで識別されたファイルベースの脅威をフィルタ処理するには、[ファイル名（Filename）] ボックスにファイル名を入力します。 SHA-256 ハッシュを使用してファイルをフィルタ処理するには、SHA-256 ハッシュ値を [ファイル SHA-256（File SHA-256）] ボックスに入力します。 ファイル判定に基づいてファイルをフィルタ処理するには、[セキュアエンドポイントファイル判定（Cisco Secure Endpoint File Verdict）] を選択し、判定タイプを選択します。使用可能なファイル判定タイプは、[クリーン（Clean）]、[悪意のある（Malicious）]、[不明（Unknown）]、[スキャン不可（UnScannable）]、および [低リスク（Lowrisk）] です。 判定タイプの [悪意のある（Malicious）] には、次の 3 つのサブカテゴリがあります。 • [マルウェア（Malware）] : [カスタム検出（Custom Detection）] や [カスタムしきい値（Custom Threshold）] 以外の理由によりブロックされたファイル。 • [カスタム検出（Custom Detection）] : AMP for Endpoints コンソールから受信したブロックリストに登録されているファイル SHA の割合。 • [カスタムしきい値（Custom Threshold）] : Cisco Secure Endpoint の設定中にしきい値設定が原因でブロックされたファイル。

オプション	説明
ユーザ リクエスト	ユーザによって実際に開始されたトランザクションでフィルタリングするには、[Web ユーザが要求したトランザクションによるフィルタ（Filter by Web User-Requested Transactions）] を選択します。 **注**：このフィルタを有効にすると、検索結果には「最良の推測」トランザクションが含まれます。

マルウェアのカテゴリについて

SecureWeb Appliance は、次のタイプのマルウェアをブロックできます。

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。アドウェア アプリケーションの中には、別々のプロセスを同時に実行して互いをモニタさせて、変更を永続化するものがあります。変異型の中には、マシンが起動されるたびに自らが実行されるようにするものがあります。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザがブラウザ検索オプション、デスクトップ、およびその他のシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザ ヘルパー オブジェクトは、広告の表示やユーザ設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザの完全で有効な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザの完全で有効な承諾なしにユーザを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザのシステムに不要な変更を加えたりします。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
アウトブレイク ヒューリスティック	このカテゴリは、他のアンチマルウェア エンジンとは別に、Adaptive Scanning によって検出されたマルウェアを示しています。

マルウェアのタイプ	説明
フィッシング URL	フィッシング URL は、ブラウザのアドレス バーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。フィッシングは、ソーシャル エンジニアリングと技術的欺瞞の両方を使用して個人データや金融口座の認証情報を盗み出す、オンライン ID 盗難の一種です。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが好ましくないと見なされるアプリケーションです。
システム モニタ	システム モニタには、次のいずれかのアクションを実行するソフトウェアが含まれます。 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。これらのインストールは、通常はユーザに気付かれることなく行われます。また、トロイのダウンローダはリモート ホストまたはサイトからダウンロード命令を取得するので、インストールごとにペイロードが異なる場合があります。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待つか、または感染したマシンをスキャンして銀行サイト、オークション サイト、あるいはオンライン支払サイトに関係するユーザ名とパスワードを探します。
ウイルス	ウイルスは、ユーザが気付かない間にコンピュータにロードされ、ユーザの意思に反して実行されるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、通常は悪質なアクションを実行するプログラムまたはアルゴリズムです。

レイヤ 4 トラフィック モニターによって処理されたトランザクションの検索

[Webトラッキング検索（Web Tracking Search）] ページの [レイヤ4トラフィックモニター（Layer 4 Traffic Monitor）] タブには、マルウェア サイトおよびポートへの接続に関する詳細情報が表示されます。マルウェア サイトへの接続は、次のタイプの情報によって検索できます。

- 時間範囲
- トランザクションを開始したマシンの IP アドレス（IPv4 または IPv6）

- 接続先 Web サイトのドメインまたは IP アドレス（IPv4 または IPv6）
- [ポート（Port）]
- 組織内のコンピュータに関連付けられた IP アドレス
- 接続タイプ

疑わしいサイトにあるホスト名、またはトランザクションを処理した SecureWeb Appliance を表示するには、[送信先IPアドレス（Destination IP Address）] 列見出しの [詳細を表示（Display Details）] リンクをクリックします。

この情報の詳細な使用方法については、[レイヤ4トラフィックモニタ（Layer 4 Traffic Monitor）] ページ （42 ページ）を参照してください。

SOCKS プロキシによって処理されるトランザクションの検索

ブロックまたは完了したトランザクション、トランザクションを開始したクライアントマシンの IP アドレス、および宛先ドメイン、IP アドレス、またはポートなど、さまざまな条件に一致するトランザクションを検索できます。カスタムURLカテゴリ、一致ポリシー、およびユーザロケーション（ローカルまたはリモート）により、結果をフィルタリングすることもできます。IPv4 および IPv6 アドレスがサポートされます。

手順

ステップ 1 **[トラッキング（Tracking）] > [SOCKSプロキシ（SOCKS Proxy）]** を選択します。

ステップ 2 検索オプションとフィルタリング オプションをすべて表示するには、[詳細設定（Advanced）] をクリックします。

ステップ 3 検索条件を入力します。

ステップ 4 **[検索（Search）]** をクリックします。

次のタスク

関連項目

[SOCKS プロキシ（SOCKS Proxy）] ページ （45 ページ）

Web トラッキングの検索結果の使用

- 詳細な Web トラッキング検索結果の表示 （74 ページ）
- Web トラッキング検索結果について （74 ページ）
- Web トラッキング検索結果のトランザクションの詳細の表示 （74 ページ）
- Web トラッキングおよびアップグレードについて （75 ページ）

詳細な Web トラッキング検索結果の表示

手順

ステップ 1 返された結果のページをすべて確認してください。

ステップ 2 現在表示されている数よりも多くの結果を各ページに表示するには、[表示された項目（Items Displayed）] メニューからオプションを選択します。

ステップ 3 条件に一致するトランザクションが、[表示された項目（Items Displayed）] メニューで選択できる最大トランザクション数より多い場合は、[印刷可能なダウンロード（Printable Download）] リンクをクリックし、一致するすべてのトランザクションを含む CSV ファイルを取得すると、完全な結果を確認できます。

この CSV ファイルには、関連トランザクションの詳細を除く、raw データ一式が含まれます。

Web トラッキング検索結果について

デフォルトでは、結果はタイムスタンプでソートされ、最新の結果が最上部に表示されます。

検索結果に表示される情報：

- URL がアクセスされた時刻。
- ロードされたイメージ、実行された JavaScript、アクセスされたセカンダリ サイトなど、ユーザが開始したトランザクションによって発生した関連トランザクションの数。関連トランザクションの数は、列見出しの [すべての詳細を表示(Display All Details)] リンクの下の各行に表示されます。
- 処理（トランザクションの結果。該当する場合、トランザクションがブロックまたはモニタされた理由、あるいは警告が発行された理由が表示されます）。

Web トラッキング検索結果のトランザクションの詳細の表示

目的	操作手順
リスト内の短縮 URL の完全な URL	トランザクションを処理したホスト SecureWeb Appliance をメモして、そのアプライアンスのアクセスログを確認します。
個々のトランザクションの詳細	[Webサイト（Website）] 列の URL をクリックします。
すべてのトランザクションの詳細	[Webサイト（Website）] 列見出しの [すべての詳細を表示...(Display All Details...)] リンクをクリックします。

目的	操作手順
500 件までの関連トランザクションのリスト	関連トランザクションの数は、検索結果リストの列見出しにある [詳細を表示（Display Details）] リンクの下のカッコ内に表示されます。 トランザクションの [詳細（Details）] ビューで [関連トランザクション（Related Transactions）] リンクをクリックします。

Web トラッキングおよびアップグレードについて

新しい Web トラッキング機能は、アップグレード前に実行されたトランザクションには適用できない場合があります。これは、これらのトランザクションについては、必須データが保持されていない場合があるためです。Web トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

新しい Web インターフェイスでの Web レポートのスケジューリングとアーカイブ

このセクションの内容は次のとおりです。

- 新しい Web インターフェイスでの Web レポートのスケジューリング （75 ページ）
- 新しい Web インターフェイスでの Web レポートのアーカイブ （77 ページ）

新しい Web インターフェイスでの Web レポートのスケジューリング

このセクションの内容は次のとおりです。

- 新しい Web インターフェイスでのスケジュール済み Web レポートの追加 （76 ページ）
- 新しい Web インターフェイスでのスケジュール済み Web レポートの編集 （76 ページ）
- 新しい Web インターフェイスでのスケジュール済み Web レポートの削除 （77 ページ）

日単位、週単位、または月単位で実行されるようにレポートをスケジュール設定することができます。スケジュール設定されたレポートは、前日、過去 7 日間、前月、過去の日（最大 250 日）、過去の月（最大 12 ヵ月）のデータを含めるように設定できます。また、指定した日数（2 ～ 100 日）または指定した月数（2 ～ 12 ヵ月）のデータを含めることもできます。

レポートの実行時間にかかわらず、直前の時間間隔（過去 1 時間、1 日、1 週間、または 1 ヵ月）のデータのみが含まれます。たとえば、日次レポートを午前 1 時に実行するようにスケジュールを設定した場合、レポートには前日の 00:00 から 23:59 までのデータが含まれます。

必要に応じた数（ゼロも含む）のレポート受信者を定義できます。電子メール受信者を指定しない場合でも、レポートはアーカイブされます。レポートを多数のアドレスに送信する必要がある場合、個別に受信者を設定するよりも、メーリング リストを作成するほうが容易です。

新しい Web インターフェイスでのスケジュール済み Web レポートの追加

手順

ステップ 1 [モニターリング（Monitoring）] > [スケジュールとアーカイブ（Schedule & Archive）] を選択します。

ステップ 2 [スケジュール済み/アーカイブ済み（Scheduled / Archived ）] タブで、[+] ボタンをクリックします。

ステップ 3 [レポートタイプ（Report Type）] ドロップダウンメニューからレポートタイプを選択します。

ステップ 4 [レポートタイトル（Report Title）] フィールドに、レポートのタイトルを入力します。

同じ名前の複数のレポートを作成することを防止するため、わかりやすいタイトルを使用することを推奨します。

ステップ 5 [含める時間範囲（Time Range to Include）] ドロップダウン メニューからレポートの時間範囲を選択します。

ステップ 6 生成されるレポートの形式を選択します。

デフォルト形式は PDF です。

ステップ 7 [配信オプション（Delivery Option）] セクションから、次のオプションのいずれかを選択します。

このオプションを選択すると、レポートが [アーカイブレポート（Archived Reports）] ページに表示されます。

（注）
[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートはアーカイブできません。

- レポートをアーカイブするには、[アーカイブのみ（Only Archive）] を選択します。
- レポートをアーカイブしてメール送信するには、[アーカイブおよび受信者にメール送信（Archive and Email to Recipients）] をクリックします。
- レポートを電子メールで送信するには、[受信者への電子メールのみ（Only Email to Recipients）] をクリックします。

[電子メールID（Email IDs）] フィールドで、受信者の電子メール アドレスを入力します。

ステップ 8 [スケジュール（Schedule）]領域で、レポートのスケジュールを設定する日、週、または月の横にあるオプション ボタンを選択します。

ステップ 9 [レポート言語（Report language）] ドロップダウンリストから、レポートを生成する必要がある言語を選択します。

ステップ 10 **[送信（Submit）]** をクリックします。

新しい Web インターフェイスでのスケジュール済み Web レポートの編集

アプライアンスの新しい Web インターフェイスでレポートを編集するには、[モニターリング（Monitoring）] > [スケジュールとアーカイブ（Schedule & Archive）] ページを選択します。編

集するレポートのレポートタイトルに対応するリンクをクリックします。設定を変更してから、[編集（Edit）] をクリックしてページで変更を送信します。

新しい Web インターフェイスでのスケジュール済み Web レポートの削除

アプライアンスの新しい Web インターフェイスでレポートを削除するには、[モニターリング（Monitoring）] > [スケジュール済み/アーカイブ済み（Scheduled/Archived）] ページを選択します。削除するレポートに対応するチェックボックスをオンにして、ゴミ箱アイコンをクリックします。

スケジュール済みのすべてのレポートを削除するには、レポートタイトルの横にあるチェックボックスをオンにします。削除されたレポートのアーカイブ版は削除されません。

新しい Web インターフェイスでの Web レポートのアーカイブ

- （新しい Web インターフェイス）オンデマンドでの Web レポートの生成 （77 ページ）
- 新しい Web インターフェイスでのアーカイブ済み Web レポートの表示と管理 （78 ページ）

（新しい Web インターフェイス）オンデマンドでの Web レポートの生成

スケジュールを設定できるレポートのほとんどは、オンデマンドでの生成も可能です。

レポートをオンデマンドで生成するには、次の手順を実行します

手順

ステップ 1 SecureWeb Applianceで、[モニタリング（Monitoring）]>[スケジュールとアーカイブ（Schedule & Archive）] を選択します。

ステップ 2 [アーカイブの表示（View Archived）] タブで、[+] ボタンをクリックします。

ステップ 3 [レポートタイプ（Report Type）]セクションで、ドロップダウンリストからレポートタイプを選択します。

このページのオプションは変更される場合があります。

ステップ 4 [レポートタイトル（Report Title）] セクションに、レポートのタイトルの名前を入力します。

AsyncOS では、レポート名が一意かどうかは確認されません。混乱を避けるために、同じ名前で複数のレポートを作成しないでください。

ステップ 5 [含める時間範囲（Time Range to Include）] ドロップダウン リストから、レポート データの時間範囲を選択します。

ステップ 6 [添付ファイルの詳細（Attachment Details）] セクションで、レポートの形式を選択します。

PDF. 配信用、アーカイブ用、またはその両方の用途でPDF形式のドキュメントを作成します。[PDF レポートをプレビュー（Preview PDF Report）] をクリックすると、ただちに PDF ファイルでレポートを表示できます。

ステップ 7 [配信オプション（Delivery Option）] セクションから、次のオプションのいずれかを選択します。

このオプションを選択すると、レポートが [アーカイブレポート（Archived Reports）] ページに表示されます。

（注）
[ドメイン毎のエグゼクティブサマリー（Domain-Based Executive Summary）] レポートはアーカイブできません。

- レポートをアーカイブするには、[アーカイブのみ（Only to Archive）] を選択します。
- レポートをアーカイブしてメール送信するには、[アーカイブおよび受信者にメール送信（Archive and Email to Recipients）] をクリックします。
- レポートを電子メールで送信するには、[受信者への電子メールのみ（Only Email to Recipients）] をクリックします。

[電子メールID（Email IDs）] フィールドで、受信者の電子メール アドレスを入力します。

ステップ 8 [レポート言語（Report language）] ドロップダウンリストから、レポートを生成する必要がある言語を選択します。

ステップ 9 [このレポートを配信（Deliver This Report）] をクリックして、レポートを生成します。

新しい *Web* インターフェイスでのアーカイブ済み *Web* レポートの表示と管理

ここでは、スケジュール設定されたレポートとして生成されたレポートの使用方法について説明します。

手順

ステップ 1 アプライアンスの新しい Web インターフェイスにログインします。

ステップ 2 [モニターリング（Monitoring）] > [スケジュールとアーカイブ（Schedule & Archive）] を選択します。

ステップ 3 [アーカイブの表示（View Archived）] タブを選択します。

ステップ 4 レポートを表示するには、[レポートタイトル（Report Title）] 列でレポート名をクリックします。[レポートタイプ（Report Type）] ドロップダウンリストでは、[アーカイブ済みレポート（Archived Reports）] タブにリストされているレポートのタイプをフィルタリングします。

ステップ 5 検索ボックスで特定のレポートを検索できます。

新しいWebインターフェイスの[システムステータス（SystemStatus）] ページ

SecureWeb Applianceで、[モニタリング（Monitoring）] > [システムステータス（System Status）] を選択して、システムステータスをモニターします。このページは、 SecureWeb Applianceの現

在のステータスと設定を表示します。ブラウザの時刻は、右上隅の[システムステータス（System Status）] ページに表示されます。

[システムステータス（System Status）] ページには次のタブがあります。

- 容量

デフォルトでは、[ステータス（Status）] タブが表示されます。

ステータス

[ステータス（Status）] ページには、次の情報が表示されます。

セクション	説明
SecureWeb Appliance のステータス	• システムの動作期間 • システム リソースの使用率：レポーティングおよびロギングに使用される CPU 使用率、RAM 使用率、およびディスク領域の使用率。 システムによって使用されない RAM は Web オブジェクト キャッシュによって使用されるので、効率的に動作する RAM 使用率は 90% を超える場合があります。システムで重大なパフォーマンス問題が発生していない場合で、この値が 100 % に固定されない場合、システムは正常に動作しています。 （注） プロキシバッファ メモリは、この RAM を使用する 1 つのコンポーネントです。
アラート（Alerts）	発生したアラートの名前と日付と時刻が表示されます。右上隅の上部にある [詳細（More）] またはアラート名をクリックすると、[すべてのアラート（All Alerts）] ポップアップが表示されます。[すべてのアラート（All Alerts）] ポップアップで、選択したアラート行が強調表示されます。 [すべてのアラート（All Alerts）] ポップアップには次の情報が表示されます。 • アラートの日付と時刻（Date and Time of Alert） • アラートレベル（Alert Level ）：[情報（Info）]、[警告（Warning）]、または [クリティカル（Critical）] • アラートクラス（Alert Class） • 問題（Problem）：アラートの簡単な説明 • 受信者（Recipient）：アラートの詳細が送信される電子メールアドレス

セクション	説明
ディスク使用率（Disk Usage）	ディスク使用率の値と RAID ストレージのステータスが表示されます。 RAID ストレージのステータスは、アプライアンスの設定によって異なります。仮想アプライアンスの場合、RAID ストレージのステータスには [不明（Unknown）] と表示され、物理アプライアンスには [Optimal（最適）] と表示されます。
プロキシステータス（Proxy Status）	プロキシの CPU 使用率とプロキシディスクの I/O 使用率を表示します。 また、プロキシ接続のバックログもポート番号と接続数とともに表示されます。
高可用性	フェールオーバーグループの名前、優先順位、およびステータスを表示します。 また、有効になっている高可用性フェールオーバーグループの数も表示されます。フェールオーバーグループが存在しない場合は、[設定されていません（Not Configured）] というサービスステータスが表示されます。

セクション	説明

プロキシトラフィックの特性（Proxy Traffic Characteristics）	次のプロキシトラフィックの特性が表示されます。
	• 1 秒あたりの要求数（Request Per Second）
	• 帯域幅
	• 応答時間（Response Time）
	• キャッシュヒット率（Cache Hit Rate）
	• 現在の接続数（Current Connections）：特定の日時の接続数について次の詳細が表示されます。
	  • アイドル状態のクライアント接続数
	  • アイドル状態のサーバー接続数
	  • クライアントの総接続数
	  • サーバーの総接続数
	
	これらのデータの平均値と最大値が表示されます。最後の1分間、最後の1時間、およびプロキシの再起動以降についての平均値が表示されます。最大値は、最後の1時間とプロキシの再起動以降について表示されます。
	（注）
	[RPSと帯域幅（RPS and Bandwidth）] の横にあるリンクアイコンをクリックすると、[キャパシティ（Capacity）] タブにリダイレクトされます。同様に、[応答時間（Response Time）] の横にあるリンクアイコンをクリックすると、[サービス（Services）] タブにリダイレクトされます。

容量

[キャパシティ（Capacity）] ページには、次の情報が表示されます。

セクション	説明
時間範囲（Time Range）	次の [時間範囲（Time Range）] オプションを表示します。 • 時間（Hour） • 日（Day） • Week • 30 日間 • 90 日間 • 昨日（Yesterday）（00:00 ～ 23:59） • 先月（Previous Calendar Month） • [カスタム範囲（Custom Range）]：使用可能な最も古いデータ 使用可能な最も古いデータを表示するには [適用（Apply）] をクリックし、操作をキャンセルするには [キャンセル（Cancel）] をクリックします。 （注） [時間範囲（Time Range）] オプションは、[キャパシティ（Capacity）] タブのすべての機能に適用されます。
システム CPU およびメモリの使用率	[システム CPU およびシステム メモリの使用率（System CPU and System Memory Usage）] では、次の操作を実行できます。 • しきい値を更新または設定します（例：0 ー 100％）。 • しきい値を変更します。 • CPU /メモリ使用率を表示します。カラーコードは次のとおりです。 • 赤色：しきい値を示します。 • 緑色：平均値を示します。しきい値を変更すると、それに応じて平均値も更新されます。 平均値は、合計値をレコードの長さで割った値です。 • 青色：システムメモリ使用率（%）を表示します。 [システム CPU およびメモリ使用率（System CPU and Memory Usage）] データは、[時間範囲（Time Range）] 選択に基づくパーセンテージで表示されます。データとグラフは、現在のデータに基づいて動的に変化します。

セクション	説明
帯域幅および RPS	次の帯域幅と RPS の詳細をグラフ形式で表示します。 • 全体：ダーク ブルーで表示 • HTTPS 復号：アクア ブルーで表示 凡例ブロックをクリックすると、[全体（Overall）] 情報と [HTTS 復号（HTTPS Decrypted）] 情報を有効または無効にすることができます。
機能別 CPU 利用率	各種 CPU 使用率オプションの色分けは次のとおりです。 • 薄い緑色：Web プロキシ • 濃い緑色：ロギング • 紫色：レポート • 黄色：WBRS • 暗い青色：Cisco Secure Endpoint • 薄い青色：Webroot • 水色：Sophos • 灰色：McAfee 凡例ブロックをクリックすると、オプションを有効または無効にすることができます。
クライアントまたはサーバー接続	平均および最大接続数を表示し、次のタスクを実行できます。 • 平均および最大接続数の有効化または無効化 • 平均および最大接続の詳細とグラフの表示

サービス

[サービス（Services）] ページには、サービスとそのステータスが表示されます。[サービス（Services）] リボンには、Cisco Secure Endpoint 、WCCP、ISE、および CTR のサービスステータスが表示されます。サービス名の横の色は、サービスステータスを示します。

- 赤：サービスの準備ができていません。
- グレー：サービスの準備はできていますが、無効になっています。
- 緑：サービスの準備ができており、有効になっています。

セクション	説明
日付（Date）	当日のサービスデータがデフォルトで表示されます。最大で過去7日間のデータを表示できます。特定の日のデータを表示するには、カレンダーから日付を選択します。
サービスのステータス（Service Status）	[サービスステータス（Service Status）] テーブルには、サービスのイベントとアラートが表示されます。テーブルには、1 時間のスロットに分割された 24 時間の時間間隔が表示されます。各ブロックには 1 時間の時間間隔でアラートが示されます。 ブロックの色が緑の場合は、対応する時間帯にクリティカルなアラートがないことを示します。1 時間に少なくとも 1 つ以上のクリティカルなアラートがある場合は、対応するブロックが赤で表示されます。未来のタイムスロットに対応するブロックは白で表示されます。 サービス名の近くの左側にあるアイコンには、最後のブロック（進行中の時間帯）の色が表示されます。 赤のブロックをクリックすると、最後の5つのアラートが発生した時間を確認できます。また、アラートの合計数も、[「n」イベント中 5（5 of 'n' Events）] と表示されます。ここで、「n」は、その時間に発生したアラートの合計数です。[その他（More）] をクリックすると、[すべてのアラート（All Alerts）] ポップアップが表示されます。 [すべてのアラート（All Alerts）] ポップアップには次の情報が表示されます。 • アラートの日付と時刻（Date and Time of Alert） • アラートレベル（Alert Level ）：[情報（Info）]、[警告（Warning）]、または [クリティカル（Critical）] • アラートクラス（Alert Class） • 問題（Problem）：アラートの簡単な説明 • 受信者（Recipient）：アラートの詳細が送信される電子メールアドレス

セクション	説明
サービス応答時間（Service Response Time）	[サービス応答時間（Service Response Time）] テーブルには、システムで実行されている各サービスの所要応答時間のパターンが表示されます。次の時間が表示されます。 • McAfee サービス時間（McAfee Service Time） • WBRS サービス時間（WBRS Service Time） • DNS 応答時間（DNS Response Time） • Webroot サービス時間（Webroot Service Time） • Cisco Secure Endpoint サービス時間 • Sophos サービス時間（Sophos Service Time） • サーバー応答時間（Server Response Time） テーブルには、1 時間のスロットに分割された 24 時間の時間間隔が表示されます。各ブロックは、1 時間のサービス応答パターンを表します。各サービスの応答時間は、次のタイムスロットに分割されます。 • 0.001 秒～ 0.06 秒 • 0.06 秒～ 0.6 秒 • 0.6 秒～ 1 秒 • 1 秒～ 6 秒 • 6 秒以降 デフォルトでは、テーブルにはすべてのサービスの 1 秒～ 6 秒の応答値が表示されます。詳細な分割部分を展開して表示することができます。 システムは、すべてのトランザクションの応答時間を計算します。その後で、各タイムスロットで発生したトランザクションボリュームのパーセンテージが表示されます。ブロックの色は、トランザクションボリュームのパーセンテージに基づいています。

セクション	説明
	応答時間が1秒未満の場合、トランザクション量の凡例は次のようになります。 • 濃い青色：41 ー 100% • 水色：11 ー 40% • 薄い青色：1 ー 10% • 白色：0% 応答時間が1秒以上の場合、トランザクション量の凡例は次のようになります。 • 赤色：41 ー 100% • 薄い赤色：26 ー 40% • 薄い青色：1 ー 25% • 白色：0% 応答時間のデータが秒単位で使用できない場合、凡例の色オプションは白になり、編集できません。[時間範囲（Time Range）] オプションをクリックして、サービス応答時間データを取得します。 データには、棒グラフと発生回数が含まれます。ただし、次のものは取得できません。 • 棒グラフ • 以前の日付の凡例データ 時間ブロックをクリックすると、その特定の時間の応答トレンドを棒グラフで表示するポップアップが開きます。 • 横軸：5 分間隔に分割されたタイムスロット • 垂直軸：タイムスロット内のトランザクション数 ポップアップのブロックにマウスのカーソルを合わせると、その時間間隔のトランザクション数が表示されます。

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。