ダッシュボードの使用

FireSIGHT システムダッシュボードは、システムによって収集および生成されたイベントに関するデータを含む、現在のシステムのステータスを概要的なビューとして提供します。またダッシュボードを使用して、展開のアプライアンスのステータスと全体の正常性に関する情報を表示することもできます。ダッシュボードへアクセスできるのは、特定のユーザ ロール（Administrator、Maintenance User、Security Analyst、Security Analyst（読み取り専用）、およびダッシュボードの権限のカスタム ロール）だけです。他のロールでは、デフォルトの起動ページとして、ロールに関連するページが表示されます。たとえば、Discovery Admin には、[ネットワーク検出（Network Discovery）] ページが表示されます。

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ウィジェットとは、FireSIGHT システムのさまざまな側面について情報を提供する、自己完結型の小さなコンポーネントです。FireSIGHT システムには、事前定義された複数のウィジェットが付属しています。たとえば、Appliance Information ウィジェットは、アプライアンスの名前、モデル、リモート マネージャ、および FireSIGHT システムソフトウェアの実行中のバージョンを通知します。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。

ダッシュボードは、複雑で高度にカスタマイズ可能なモニタリング機能です。多くのタイプのシステム データを表示するためのもうひとつの方法は、Context Explorer の使用です。これはプリセットの視覚的なコンテキスト セットで侵入、接続、および検出データを使用して情報を提供するものです。このコンテキストは、精度を向上させるためのフィルタを使用して、一時的にのみ変更することができます。FireSIGHT システムダッシュボードで使用できる包括的なデータとは異なり、Context Explorer はモニタリングの対象のネットワークがどのように見えて、どのように動作しているかを簡単にカラフルな図で示します。Context Explorer の詳細については、Context Explorer の使用（56-1 ページ）を参照してください。

各タイプのアプライアンスには、サマリ ダッシュボードというデフォルトのダッシュボードが付属しています。このダッシュボードは、一般ユーザに対して、ご利用の FireSIGHT システムの展開についての汎用的な FireSIGHT、侵入、脅威の検出、地理情報、システム ステータスの情報を提供します。ウィジェットには特定のアプライアンス タイプでのみ有用なものもあるため、ユーザが防御センター、仮想防御センター、または管理対象デバイスを使用しているかどうかによって、Summary Dashboard は異なります。

（注） 仮想管理対象デバイスには Web インターフェイスがないため、ダッシュボードをサポートしていません。

デフォルトでは、自身のアプライアンスのホーム ページに Summary Dashboard が表示されますが、別のデフォルト ホーム ページが表示されるようアプライアンスを設定することができます。

ヒント　ホーム ページを変更する場合は、[オーバービュー(Overview)] > [ダッシュボード(Dashboards)] を選択してダッシュボードにアクセスできます。詳細については、ダッシュボードの表示 (55-44 ページ)を参照してください。

表示されるデータは、管理対象デバイスのライセンスと導入方法、データを提供する機能を設定するかどうか、およびシリーズ 2アプライアンスと Blue Coat X-Series 向け Cisco NGIPS の場合はデータを提供する機能をサポートしているかどうかなどの要因に応じて異なることに注意してください。たとえばDC500 防御センターとシリーズ 2デバイスはいずれも、カテゴリまたはレピュテーションによる URL フィルタリングをサポートしていないため、DC500 防御センターではこの機能のデータは表示されず、シリーズ 2デバイスではこのデータが検出されません。

防御センターには、Summary Dashboard の他に、事前定義された次のダッシュボードが付属しています。

- Application Statistics ダッシュボードは、モニタリング対象のネットワークについて、アプリケーションのアクティビティおよび侵入イベントの詳しい情報を提供します。このダッシュボードを使用して、多くのトラフィックが生じているアプリケーション、許可および拒否された接続、侵入イベント、および使用中の一意のアプリケーションの数と、それらのアプリケーションの推定のリスクとビジネスとの関連性を追跡することができます。
- Connection Summary ダッシュボードは、接続データを使用して、モニタリング対象のネットワークのアクティビティについてテーブルおよびチャートを作成します。このダッシュボードを使用して、ポート、アプリケーション、ネットワークの接続とトラフィックに関連するイニシエータおよびレスポンダの IP、接続とトラフィックの全体量、位置情報を追跡することができます。データを生成するには、このダッシュボードの接続を記録する必要があります。接続およびセキュリティ インテリジェンスのデータについて(39-2 ページ)を参照してください。このウィジェットの出力は、接続のロギング設定によって異なることに注意してください。

ヒント　このダッシュボードのウィジェットは、トラフィックの合計をキロバイト(KB)単位で示します。トラフィックの合計(KB)は、1 秒あたりのトラフィック(KB/s)に、選択された時間枠に対象となった合計の秒数を掛けた値と同じです。

- Detailed Dashboard は、アドバンスト ユーザに対して、自身のFireSIGHT システムの展開について詳細な情報を提供します。この中には、収集された侵入イベント、ネットワーク検出、コンプライアンス、相関、トラフィック、システム ステータス データを要約した複数のウィジェットが含まれているだけでなく、シスコのニュースおよび製品のアップデートに関する情報を提供します。このダッシュボードを使用して、さまざまなネットワーク情報を一度にモニタリングすることができます。
- Files Dashboard は、管理対象のデバイスによってネットワークで検出されたファイル(マルウェア ファイルも含む)、取得されたファイル(デバイスに格納されており動的な分析のために送信されたファイル)、サブスクリプションベースの FireAMP 方式を使用して検出されたマルウェアについての詳細な情報を提供します。ネットワークベースのマルウェア データを含めるには、Malwareのライセンスを所有しており、このダッシュボードに対してマルウェアの検出を有効にしておくことが必要です。また、DC500 およびシリーズ 2デバイスまたは Blue Coat X-Series 向け Cisco NGIPS はいずれも、高度なマルウェア防御をサポートしていないため、DC500 はこのデータを表示できず、シリーズ 2デバイスと Blue Coat X-Series 向け Cisco NGIPS はこのデータを検出しません。詳細については、マルウェア防御とファイル制御について(37-2 ページ)を参照してください。

- URL Statistics ダッシュボードは、モニタリング対象のネットワークから外部 URL へ許可および拒否されたトラフィックについての詳細情報を、URL のカテゴリおよびレピュテーションでソートして提供します。URL カテゴリおよびレピュテーション データを含めるには、URL Filtering のライセンスを所有しており、このダッシュボードに対して URL Filtering を有効にしておくことが必要です。また、DC500 とシリーズ 2デバイスはいずれも、レピュテーションとカテゴリによる URL フィルタリングをサポートしていないため、DC500 はこのデータを表示できず、シリーズ 2デバイスはこのデータを検出しないことにも注意してください。レピュテーション ベースの URL ブロッキングの実行（16-12 ページ）を参照してください。
- [アクセス制御ユーザ統計（Access Controlled User Statistics）] ダッシュボードは、モニタリング対象のネットワークについて、ユーザのアクティビティおよび侵入イベントの詳しい情報を提供します。このダッシュボードを使用して、許可および拒否された接続、トラフィック、およびネットワーク上のユーザに関連付けられている侵入イベント、ネットワーク上の一意のユーザ数を追跡できます。このダッシュボードはユーザによって認識されるデータを利用しているため、このダッシュボードで意味のある統計を表示するためには、少なくとも 1 つの User Agent および 防御センター-Active Directory LDAP サーバ接続を設定している必要があります。Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

事前定義されたダッシュボードを使用し、それらのダッシュボードを修正することも、自身のニーズに合わせてカスタム ダッシュボードを作成することも可能です。アプライアンスのすべてのユーザでカスタム ダッシュボードを共有することも、自分専用に使用するカスタム ダッシュボードを作成することもできます。また、カスタム ダッシュボードを自分のデフォルトのダッシュボードに設定することもできます。

イベントのドリルダウン ページとテーブル ビューには、[ダッシュボード（Dashboard）] ツールバーのリンクが含まれているものがあります。このリンクをクリックして、関連する事前定義されたダッシュボードを表示することができます。次の表は、イベント ビューと、対応する事前定義されたダッシュボードの対応を示しています。事前定義されたダッシュボードまたはタブを削除すると、関連付けられているダッシュボードのリンクが機能しなくなることに注意してください。

表 55-1　イベント テーブルのダッシュボード リンク

テーブル	ダッシュボード リンク
接続イベント （[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]）	接続の概要（Connection Summary）
セキュリティ インテリジェンス イベント （[分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス（Security Intelligence）]）	接続の概要（Connection Summary）
侵入イベント （[分析（Analysis）] > [侵入（Intrusions）] > [イベント（Events）]）	Summary（[侵入イベント（Intrusion Events）] タブ）
マルウェア イベント （[分析（Analysis）] > [ファイル（Files）] > [マルウェア イベント（Malware Events）]）	Files（[マルウェア（Malware）] タブ）
ファイル イベント （[分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（File Events）]）	Files（[ファイル（Files）] タブ）

表 55-1　イベント テーブルのダッシュボード リンク（続き）

テーブル	ダッシュボード リンク
キャプチャ ファイル（Captured Files） （[分析（Analysis）] > [ファイル（Files）] > [キャプチャ ファイル（Captured Files）]）	Files（[ファイル ストレージ（File Storage）] タブ）
アプリケーション （[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション（Applications）]）	Application Statistics
アプリケーション詳細（Application Details） （[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーション詳細（Applications Details）]）	Application Statistics
侵入の痕跡（Indications of Compromise） （[分析（Analysis）] > [ホスト（Hosts）] > [侵入の痕跡（Indications of Compromise）]）	Summary（[脅威（Threats）] タブ）
Users （[分析（Analysis）] > [ユーザ（Users）] > [ユーザ（Users）]）	Access Controlled User Statistics
ユーザ アクティビティ（User Activity） （[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）]）	Access Controlled User Statistics
相関イベント（Correlation Events） （[分析（Analysis）] > [相関（Correlation）] > [相関イベント（Correlation Events）]）	Detailed（[相関（Correlation）] タブ）
ホワイトリスト イベント（White List Events） （[分析（Analysis）] > [相関（Correlation）] > [ホワイトリスト イベント（White List Events）]）	Detailed（[相関（Correlation）] タブ）

ダッシュボードおよび内容の詳細については、次のセクションを参照してください。

- ダッシュボード ウィジェットについて（55-4 ページ）
- 事前定義されたウィジェットについて（55-8 ページ）
- ダッシュボードの操作（55-42 ページ）

ダッシュボード ウィジェットについて

ライセンス：任意（Any）

ダッシュボードには 1 つ以上のタブがあり、それぞれのタブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。FireSIGHT システムには、事前定義された多数のダッシュボード ウィジェットが付属しています。それぞれのウィジェットは、FireSIGHT システムのさまざまな側面を理解するうえで役に立ちます。ウィジェットは、次の 3 つのカテゴリに分類されます。

- *Analysis & Reporting ウィジェット*は、FireSIGHT システムで収集および生成されたイベントに関するデータを表示します。
- *[その他(Miscellaneous)] ウィジェット*は、イベント データもオペレーション データも表示しません。現時点では、このカテゴリのウィジェットのみが RSS フィードを表示します。
- *Operations ウィジェット*は、FireSIGHT システムのステータスおよび全体の正常性に関する情報を表示します。

表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。また、各ダッシュボードには、動作を決定する一連のプリファレンスがあります。ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

(注)　所定の時間範囲でのイベント数を表示するウィジェットでは、イベント ビューアで利用できる詳細なデータのイベント数が、イベントの総数に反映されないことがあります。これは、ディスク領域の使用率を管理するために、古いイベントの詳細がシステムによってプルーニングされることがあるために発生します。イベント詳細のプルーニングを最小限にするために、対象の展開にとって最も重要なイベントだけを記録するようにイベント ロギングを調整できます。詳細については、ネットワーク トラフィックの接続のロギング(38-1 ページ)を参照してください。

詳細については、以下を参照してください。

- ウィジェットの可用性について(55-5 ページ)
- ウィジェットのプリファレンスについて(55-8 ページ)
- 事前定義されたウィジェットについて(55-8 ページ)
- ダッシュボードの操作(55-42 ページ)

ウィジェットの可用性について

ライセンス:任意(Any)

FireSIGHT システムには、事前定義された複数のダッシュボード ウィジェットが付属しています。表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。

- *無効な*ウィジェットは、ユーザが間違ったタイプのアプライアンスを使用しているため、表示することができないものです。
- *不正な*ウィジェットは、ユーザが必要なアカウントの権限を持っていないため、表示することができないものです。

たとえば、Current Sessions ウィジェットはすべてのアプライアンスで使用できますが、Administrator アカウント権限を持っているユーザしか使用できません。また、Appliance Status ウィジェットは、防御センター上で、Administrator、Maintenance User、Security Analyst、または Security Analyst(読み取り専用)アカウント権限を持っているユーザのみが使用できます。

不正なウィジェットまたは無効なウィジェットはダッシュボードに追加できませんが、他の種類のアプライアンスで作成された、または他のアクセス権限を持つユーザによって作成されたダッシュボードをインポートした場合、それらのダッシュボードには、不正または無効なウィジェットが含まれていることがあります。これらのウィジェットは使用できなくなり、ユーザが表示できない理由を示すエラー メッセージが表示されます。

ウィジェットは、アプライアンスがアクセス権を持っていないデータを表示できないことにも注意してください。たとえば、管理対象デバイスは、相関イベント、侵入イベント、検出イベントなどにアクセスできません。これらのデータ タイプのいずれかを表示するために設定された Custom Analysis ウィジェットが含まれている管理対象デバイスにダッシュボードをインポートすると、ウィジェットでエラー メッセージが表示されます。これらのウィジェットがタイムアウトした場合、またはそれ以外で問題が発生した場合には、個々のウィジェットでもエラー メッセージが表示されます。

ウィジェットの内容は、使用しているアプライアンスのタイプによって異なる場合があります。たとえば、防御センター上の Custom Analysis ウィジェットはディスカバリ情報を表示できますが、管理対象デバイスで Custom Analysis ウィジェットが設定されている場合は、この機能は使用できません。テーブルの列ヘッダーをクリックすると、表形式で生成されている任意の内容をソートできます。

不正なウィジェットと無効なウィジェット、および表示するデータがないウィジェットを削除または最小化できます。共有しているダッシュボード上でウィジェットを変更すると、アプライアンスのすべてのユーザに変更が反映されることに注意してください。詳細については、ウィジェットの最小化および最大化（55-50 ページ）およびウィジェットの削除（55-50 ページ）を参照してください。

次の表に、各アプライアンスが表示できる有効なウィジェットを示します。

表 55-2　FirePOWER アプライアンスとダッシュボード ウィジェットの可用性

ウィジェット	防御センター	すべての管理対象デバイス
アプライアンス情報（Appliance Information）	Yes	Yes
アプライアンス ステータス（Appliance Status）	Yes	No
相関イベント（Correlation Events）	Yes	No
現在のインターフェイス状態（Current Interface Status）	Yes	Yes
現在のセッション（Current Sessions）	Yes	Yes
カスタム分析（Custom Analysis）	Yes	No
ディスク使用量	Yes	Yes
インターフェイス トラフィック（Interface Traffic）	Yes	Yes
侵入イベント	Yes	No
ネットワーク準拠（Network Compliance）	Yes	No
製品ライセンスの認証（Product Licensing）	Yes	No
製品の更新（Product Updates）	Yes	Yes
RSS フィード（RSS Feed）	Yes	Yes
システムの負荷（System Load）	Yes	Yes

表 55-2　FirePOWER アプライアンスとダッシュボード ウィジェットの可用性(続き)

ウィジェット	防御センター	すべての管理対象デバイス
システム タイム(System Time)	Yes	Yes
ホワイトリスト イベント(White List Events)	Yes	No

次のテーブルに、各ウィジェットを表示するために必要なユーザ アカウントの権限を示します。Administrator、Maintenance User、Security Analyst、または Security Analyst(読み取り専用)のアクセス権を持つユーザ アカウントのみがダッシュボードを使用できます。

カスタム ロールを持つユーザは、自身のユーザ ロールの許可によって、ウィジェットのいずれかの組み合わせにアクセスできる場合もあれば、どのウィジェットにもアクセスできない場合もあります。

表 55-3　ユーザ ロールとダッシュボード ウィジェットの可用性

ウィジェット	管理者(Administrator)	Maintenance User	Security Analyst	Security Analyst (RO)
アプライアンス情報(Appliance Information)	Yes	Yes	Yes	Yes
アプライアンス ステータス(Appliance Status)	Yes	Yes	Yes	No
相関イベント(Correlation Events)	Yes	No	Yes	Yes
現在のインターフェイス状態(Current Interface Status)	Yes	Yes	Yes	Yes
現在のセッション(Current Sessions)	Yes	No	No	No
カスタム分析(Custom Analysis)	Yes	No	Yes	Yes
ディスク使用量	Yes	Yes	Yes	Yes
インターフェイス トラフィック(Interface Traffic)	Yes	Yes	Yes	Yes
侵入イベント	Yes	No	Yes	Yes
ネットワーク準拠(Network Compliance)	Yes	No	Yes	Yes
製品ライセンスの認証(Product Licensing)	Yes	Yes	No	No
製品の更新(Product Updates)	Yes	Yes	No	No
RSS フィード(RSS Feed)	Yes	Yes	Yes	Yes
システムの負荷(System Load)	Yes	Yes	Yes	Yes

表 55-3　ユーザ ロールとダッシュボード ウィジェットの可用性（続き）

ウィジェット	管理者（Administrator）	Maintenance User	Security Analyst	Security Analyst (RO)
システム タイム（System Time）	Yes	Yes	Yes	Yes
ホワイトリスト イベント（White List Events）	Yes	No	Yes	Yes

ウィジェットのプリファレンスについて

ライセンス：任意（Any）

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

ウィジェットのプリファレンスは単純なものにすることもできます。たとえば、次の図は Current Interface Status ウィジェットのプリファレンスを示しています。これは、内部ネットワークで有効になっているすべてのインターフェイスについて現在のステータスを表示します。このウィジェットでは、更新頻度のみを設定します。

ウィジェットのプリファレンスは、もっと複雑にすることもできます。たとえば、次の図は Custom Analysis ウィジェットのプリファレンスを示しています。これは高度にカスタマイズ可能なウィジェットで、これを使用すると、FireSIGHT システムで収集および生成されたイベントの詳細情報を表示できます。

ウィジェットのプリファレンスを変更する方法：

アクセス：Admin/Any Security Analyst/Maint

手順 1　プリファレンスを変更するウィジェットのタイトル バーで、プリファレンスの表示アイコン（ ）をクリックします。

そのウィジェットのプリファレンス セクションが表示されます。

手順 2　必要に応じて変更を加えます。

変更はすぐに反映されます。ユーザが個々のウィジェットに指定できるプリファレンスについては、事前定義されたウィジェットについて（55-8 ページ）を参照してください。

手順 3　プリファレンスのセクションを非表示にするには、ウィジェットのタイトル バーで、プリファレンスの非表示アイコン（ ）をクリックします。

事前定義されたウィジェットについて

ライセンス：任意（Any）

FireSIGHT システムにはいくつかの事前定義されたウィジェットが付属しています。ダッシュボード上でこれらのウィジェットを使用すると、展開におけるアプライアンスのステータスと全体の正常性に関する情報だけでなく、システムで収集および生成されたイベントに関するデータも含めて、現在のシステムのステータスを概要的なビューとして提供します。

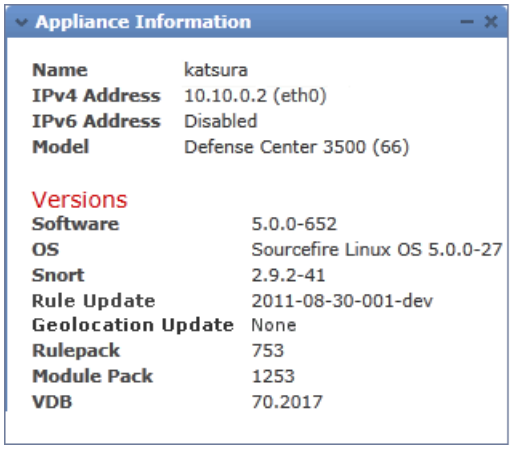
FireSIGHT システムに付属するウィジェットの詳細については、以降のセクションを参照してください。

（注） 表示できるダッシュボード ウィジェットは、使用しているアプライアンスのタイプと、自分のユーザ ロールによって異なります。詳細については、ウィジェットの可用性について（55-5 ページ）を参照してください。

[アプライアンス情報（Appliance Information）] ウィジェットについて

ライセンス：任意（Any）

Appliance Information ウィジェットは、アプライアンスのスナップショットを提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。



このウィジェットは以下の情報を提供します。

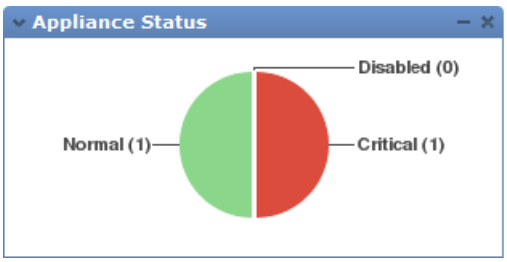
- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- ダッシュボードでアプライアンスにインストールされている、FireSIGHT システムソフトウェア、オペレーティング システム、Snort、ルール アップデート、ルール パック、モジュール パック、脆弱性データベース（VDB）、および地理情報のアップデートのバージョン（仮想防御センターは除く）
- 管理対象アプライアンスの場合は、管理アプライアンスとの通信リンクの名前とステータス
- ハイアベイラビリティ ペアの防御センターの場合は、防御センターによって最近行われた通信、およびピア防御センターの名前、モデル、および FireSIGHT システムソフトウェアとオペレーティング システムのバージョン

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

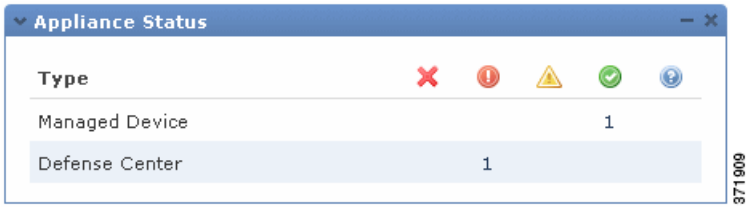
Appliance Status ウィジェットについて

ライセンス：任意（Any）

Appliance Status ウィジェットは、アプライアンスの正常性、およびそのアプライアンスが管理しているアプライアンスの正常性を示します。防御センターは、管理対象のデバイスに対して自動的に正常性ポリシーを適用しないため、ユーザは正常性ポリシーをデバイスへ手動で適用する必要があります。このようにしないと、デバイスのステータスは `Disabled` として示されます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。



ウィジェットのプリファレンスを変更して、アプライアンスのステータスを円グラフまたは表で表示するように設定できます。



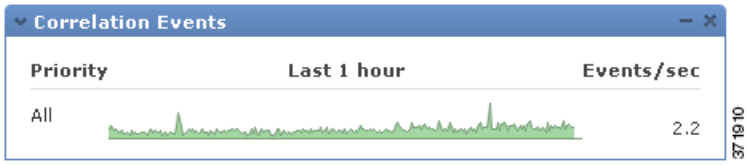
プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

円グラフの一部、またはアプライアンス ステータス表のいずれかの数字をクリックすると、[ヘルス モニタ（Health Monitor）] ページが表示され、対象のアプライアンス、およびそのアプライアンスが管理しているすべてのアプライアンスのコンパイル済みの正常性ステータスを参照することができます。詳細については、ヘルス モニタの使用（68-46 ページ）を参照してください。

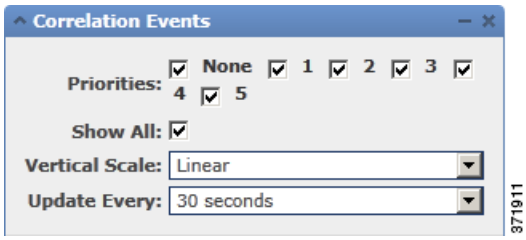
Correlation Events ウィジェットについて

ライセンス：FireSIGHT

Correlation Events ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの相関イベントの平均数を、優先度ごとに示します。このウィジェットは、Detailed Dashboard の [相関（Correlation）] タブにデフォルトで表示されます。



ウィジェットを設定して、線形（増分）や対数（10 の倍数）のスケールを選択するだけでなく、ウィジェットのプリファレンスを変更してさまざまな優先度の相関イベントを表示することができます。



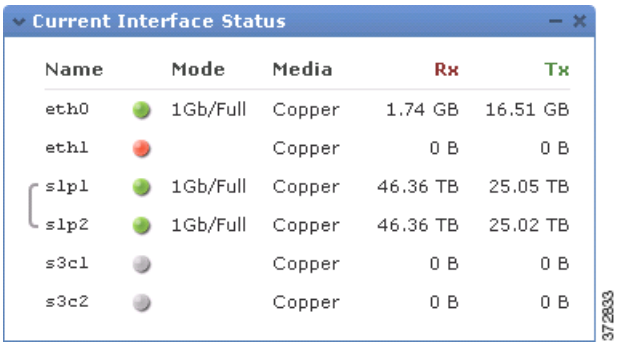
優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [プライオリティ（Priorities）] チェックボックスを選択します。優先度に関係なくすべての相関イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

グラフをクリックして特定の優先度の相関イベントを表示することも、[All] グラフをクリックしてすべての相関イベントを表示することもできます。いずれの場合も、イベントはダッシュボードの時間範囲に制限されます。ダッシュボードを介して相関イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の時間枠が変わります。相関イベントの詳細については、相関イベントの表示（51-61 ページ）を参照してください。

[現在のインターフェイス ステータス(Current Interface Status)] ウィジェットについて

ライセンス:任意(Any)

[現在のインターフェイス ステータス(Current Interface Status)] ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。防御センターでは、管理(eth0、eth1 など)インターフェイスを表示できます。管理対象デバイスでは、センシング(s1p1 など)インターフェイスのみを表示するか、または管理インターフェイスとセンシング インターフェイスの両方を表示するかを選択できます。インターフェイスは、タイプ(管理、インライン、パッシブ、スイッチド、ルーテッド、スタック、未使用)別にグループ化されます。



ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード(100Mb 全二重、または 10Mb 半二重など)
- インターフェイスのタイプ(銅線または光ファイバ)
- インターフェイスで受け取ったデータ量(Rx)および送信したデータ量(Tx)

リンク状態を表すボールの色は、次のように現在のステータスを示します。

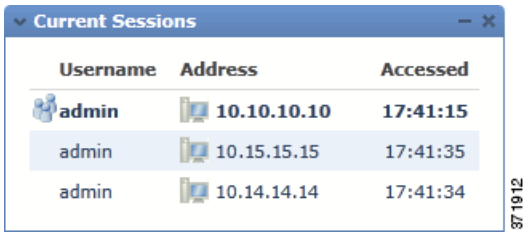
- 緑色:リンクがフル スピードでアップ状態になっています
- 黄色:リンクはアップ状態ですがフル スピードではありません
- 赤色:リンクはアップ状態ではありません
- 灰色:リンクは管理上無効になっています
- 青色:リンク ステート情報は使用できません(たとえば ASA)

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットのプリファレンスについて(55-8 ページ)を参照してください。

Current Sessions ウィジェットについて

ライセンス：任意（Any）

Current Sessions ウィジェットは、アプライアンスに現在ログインしているユーザ、セッションが生じたマシンに関連付けられている IP アドレス、各ユーザがアプライアンス上のページにアクセスした最後の（アプライアンスのローカル時間に基づいた）時間を示します。自分を表すユーザ（現在ウィジェットを表示しているユーザ）には、ユーザ アイコン（ ）のマークが付けられ、太字で示されます。ログオフするか非アクティブになってから 1 時間以内に、セッションはこのウィジェットのデータからプルーニングされます。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。



Current Sessions ウィジェットで、次のことができます。

- いずれかのユーザ名をクリックして、[ユーザ管理（User Management）] ページでユーザ アカウントを管理します。ユーザ アカウントの管理（61-46 ページ）を参照してください。
- ホスト アイコン（ ）、または IP アドレスの隣の侵害されたホスト アイコン（ ）をクリックして、関連付けられているマシンのホスト プロファイルを表示します。ホスト プロファイルの使用（49-1 ページ）を参照してください（ネットワーク検出での防御センターのみ）。
- いずれかの IP アドレスまたはアクセス時間をクリックして、その IP アドレスおよびその IP アドレスに関連付けられているユーザが Web インターフェイスにログオンした時間によって制約される監査ログを表示します。監査レコードの表示（69-2 ページ）を参照してください。

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

Custom Analysis ウィジェットについて

ライセンス：任意（Any）

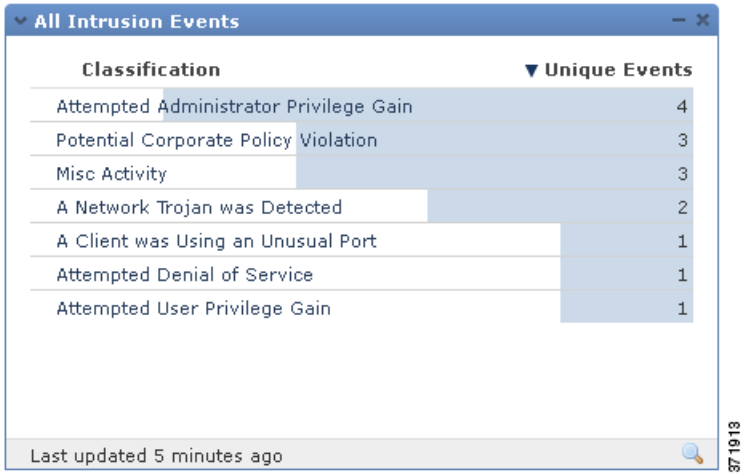
Custom Analysis ウィジェットは高度にカスタマイズ可能なウィジェットで、これを使用すると、FireSIGHT システムで収集および生成されたイベントの詳細情報を表示できます。

Custom Analysis ウィジェットには、ウィジェットの多数のプリセットが付属しています。これらのプリセットは、シスコで事前定義された設定のグループです。プリセットは例として機能し、これを使用して展開に関する情報へ素早くアクセスできます。これらのプリセットを使用することも、カスタム設定を作成することもできます。

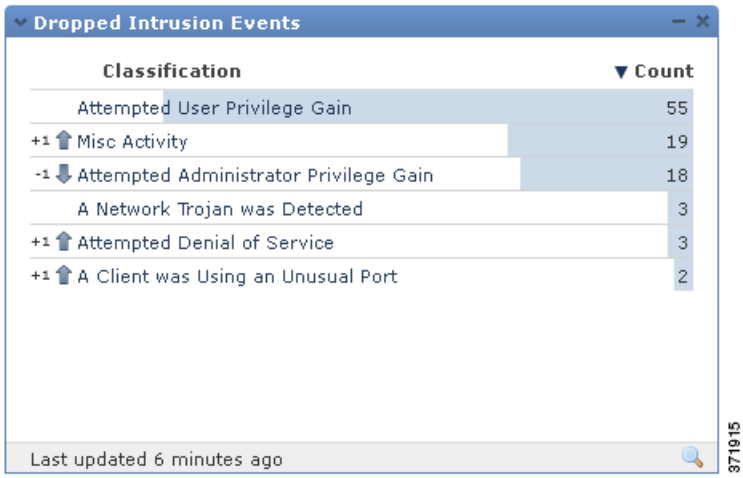
ウィジェットのプリファレンスを設定する場合、ウィジェットで表示するデータをどのようにグループ化するかを設定する集約方法の他に、どのテーブルおよび個々のフィールドを表示するかを選択する必要があります。

たとえば、[侵入イベント（Intrusion Events）] テーブルのデータを表示するようにウィジェットを設定して、最近の侵入イベントのリストを表示するよう Custom Analysis ウィジェットを設定することができます。[分類（Classification）] フィールドを選択し、このデータを [カウント（Count）] によって集約すると、各タイプのイベントがいくつ生成されたかが通知されます。この数には、侵入イベントについてレビューされたイベントが含まれていることに注意してください。イベント数をイベント ビューアで表示する場合は、レビューされたイベントは含まれません。

一方、[一意のイベント（Unique Events）] で集約すると、各タイプで一意の侵入イベントがいくつ発生したかが通知されます（たとえばネットワークの Trojan、企業ポリシーの潜在的な違反、行われたサービス妨害攻撃の検出個数など）。



オプションとして、保存されている検索（アプライアンスに付属している事前定義の検索、またはユーザが作成したカスタム検索のいずれか）を使用して、ウィジェットをさらに制約することができます。たとえば、最初の例（[分類（Classification）] フィールドを使用して [カウント（Count）] で集約する）を、[ドロップされたイベント（Dropped Events）] の検索を使用して制約すると、各タイプの侵入イベントがいくつドロップされたかが通知されます。



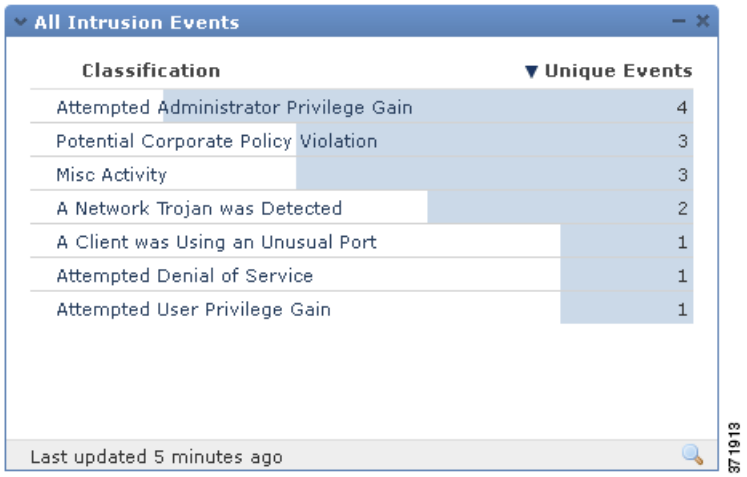
ウィジェットの背景の色付きバーは、各イベントの発生の相対数を示しています。このバーは右から左へ読みます。バーの色およびウィジェットに表示される行数を変更できます。また、発生頻度が最も多いイベントや、発生頻度が最も少ないイベントを表示するようウィジェットを設定することもできます。

矢印のアイコン（ ▼ ）は、表示のソート順を示し、制御します。下向きのアイコンは降順を表し、上向きのアイコンは昇順を表します。ソート順を変更するには、アイコンをクリックします。

最新の結果以降何らかの変更点があることを示すために、ウィジェットでは、各イベントの横に次の 3 つのアイコンのうちの 1 つを表示します。

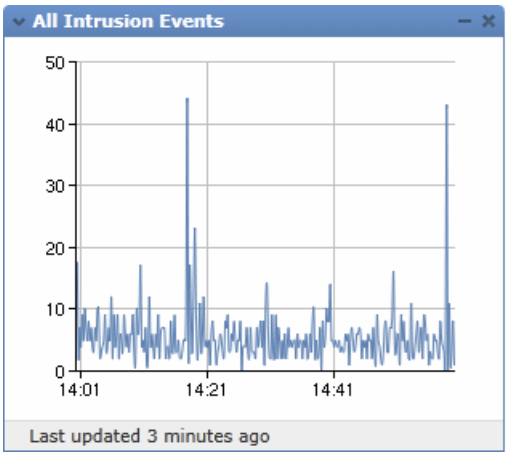
- 新しいイベント アイコン（ ）は、イベントが、最新の結果以降のものであることを示します。
- 上向き矢印のアイコン（ ）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に上がってきたことを示します。イベントが何段階上がってきたかを表す数字が、アイコンの横に示されます。
- 下向き矢印のアイコン（ ）は、ウィジェットが最後にアップデートされた後で、イベントがこの場所に下がってきたことを示します。イベントが何段階下がってきたかを表す数字が、アイコンの横に示されます。

ウィジェットは、アプライアンスのローカル時間に基づいて、最後にアップデートされた時間を表示します。ウィジェットは、ダッシュボードの時間範囲に基づいた頻度でアップデートされます。たとえば、ダッシュボードの時間範囲を 1 時間に設定すると、ウィジェットは 5 分ごとにアップデートされます。また、ダッシュボードの時間範囲を 1 年に設定すると、ウィジェットは 1 週間ごとにアップデートされます。ダッシュボードが次にアップデートされるタイミングを設定するには、ウィジェットの左下にある [最新更新（Last updated）] の通知にポインタを移動します。



(注)　保存されている検索を使用して Custom Analysis ウィジェットを制約し、その後で検索を編集すると、次にアップデートされるまでウィジェットには変更が反映されません。

一定期間のイベントまたは収集されたその他のデータに関する情報が必要な場合は、対象の展開で、一定期間に発生した侵入イベントの合計数を表示するような線グラフを表示するように Custom Analysis ウィジェットを設定することができます。一定期間のグラフでは、ウィジェットで使用するタイム ゾーンおよび線の色を選択できます。



最後に、ウィジェットのカスタム タイトルを選択できます。

Custom Analysis ウィジェットから、イベント ビュー(つまりワークフロー)を起動することができます。イベント ビューは、ウィジェットに表示されるイベントに関する詳細情報を提供します。詳細情報を表示するイベントをクリックすると、提供されます。

または、Custom Analysis ウィジェットのいずれかの IP アドレスを右クリックしてコンテキスト メニューを表示します。コンテキスト メニューから、関連するホストの詳細な情報を取得したり、Security Intelligence フィルタリングに対するグローバルなブラックリストまたはホワイトリストに情報を追加したりすることができます。

(注)　Custom Analysis ウィジェットをどのように設定するかによって、アプライアンス リソースの消費量が増えることがあります。赤い影の付いた Custom Analysis ウィジェットは、そのウィジェットの使用によりシステムのパフォーマンスが低下していることを示しています。ウィジェットが長時間赤い状態のままになっている場合は、そのウィジェットを削除する必要があります。

詳細については、次の項を参照してください。

- Custom Analysis ウィジェットの設定（55-17 ページ）
- Custom Analysis ウィジェットから関連付けられているイベントの表示（55-29 ページ）
- Custom Analysis ウィジェットの制限（55-30 ページ）
- コンテキスト メニューの使用（2-5 ページ）

Custom Analysis ウィジェットの設定

ライセンス：任意（Any）

他のウィジェットと同様に、Custom Analysis ウィジェットには動作を決定するための設定があります。Custom Analysis ウィジェットを設定するには、ウィジェットのプリファレンスについて（55-8 ページ）に記載されているように設定を表示します。

イベントの相対的な発生数を示す（棒グラフ）ようにウィジェットを設定するか、一定期間のグラフを示す（線グラフ）ようにウィジェットを設定するかによって、表示される設定のセットが異なります。

棒グラフを表示するようにウィジェットを設定するには、[フィールド（Field）] ドロップダウン リストから [時間（Time）] を除く任意の値を選択します。

線グラフを表示するようにウィジェットを設定するには、[フィールド（Field）] ドロップダウン リストから [時間（Time）] を選択します。

次の表は、Custom Analysis ウィジェットで設定できるさまざまな設定を示しています。

表 55-4　Custom Analysis ウィジェットの設定

使用する設定	制御する内容
役職（Title）	ウィジェットのタイトル。 タイトルを指定しない場合、アプライアンスは、設定済みのイベント タイプをウィジェットのタイトルとして使用します。
Preset	ウィジェットのプリセット。 Custom Analysis ウィジェットには多数のプリセットが付属しています。これらのプリセットは、シスコによって事前定義されたウィジェットの設定です。プリセットは例として機能し、これを使用して展開に関する情報へ素早くアクセスできます。これらのプリセットを使用することも、カスタム設定を作成することもできます。 プリセットの詳細については、Custom Analysis ウィジェットのプリセットの表を参照してください。
テーブル	ウィジェットが表示するイベント データが含まれているイベントのテーブル。
フィールド	表示するイベントタイプの特定のフィールド。 **ヒント**　一定期間のグラフを表示するには、[時間（Time）] を選択します。

表 55-4　Custom Analysis ウィジェットの設定(続き)

使用する設定	制御する内容
アグリゲート	ウィジェットの集約方法。 集約方法は、表示するデータをウィジェットがどのようにグループ化するかを設定します。ほとんどのイベント タイプで、デフォルトの集約基準は [カウント(Count)] です。
フィルタ	ウィジェットが表示するデータをさらに制限するための、ユーザ定義のアプリケーション フィルタ。 [アプリケーション統計(Application Statistics)] または [アプリケーション別の侵入イベント統計(Intrusion Event Statistics by Application)] テーブルのデータを表示している場合は、アプリケーション フィルタのみ使用できます。アプリケーション フィルタの詳細については、アプリケーション フィルタの操作(3-16 ページ)を参照してください。
検索(Search)	ウィジェットが表示するデータをさらに制限するために使用する、保存済みの検索。 検索を指定する必要はありませんが、プリセットの中には事前定義された検索が使用されるものがあります。 アスタリスク(*)なしでフィールド内のデータを使用する保存済みの接続イベント検索を作成すると、ウィジェットに誤ったデータが表示されます。接続イベントに基づいてカスタム分析ダッシュボードのウィジェットを制約できるのは、接続サマリを制限しているフィールドだけです。無効な検索はグレー表示され、選択できません。
表示(Show)	発生頻度が最も多いイベントを表示する([上位(Top)])か、発生頻度が最も少ないイベントを表示する([下位(Bottom)])か。
結果	表示する結果の行数。 結果は 10 ～ 25 行で表示できます。行数は 5 行ずつ増やすことができます。
ムーバーの表示	最新の結果以降の変更を示すアイコンを表示するかどうか。
タイム ゾーン	結果の表示に使用するタイム ゾーン。 タイム ゾーンは、時間ベースのフィールドを選択したときに常に表示されます。
カラー	各結果の相対的な発生数を示す、ウィジェット背景のバーの色。

以下の表で、Custom Analysis ウィジェットで使用できるプリセットについて説明します。また、各プリセットが防御センターで事前定義されたどのダッシュボードに使用されるかについても示します(事前定義されたダッシュボードがある場合)。次の点に注意してください。

- 管理対象デバイス上の事前定義されたダッシュボードには、Custom Analysis ウィジェットが含まれていません。
- DC500 防御センターは、サポートしていない機能のデータを表示しません。また、シリーズ 2 デバイスおよび Blue Coat X-Series 向け Cisco NGIPS は、サポートしていない機能のデータを検出しません。

特定のライセンス タイプの詳細については、サービス サブスクリプション(65-8 ページ)を参照してください。

表 55-5　Custom Analysis ウィジェットのプリセット

Preset	説明	事前定義されたダッシュボード	ライセンス
全侵入イベント（All Intrusion Events）	ダッシュボードの時間範囲で、モニタリング対象のネットワーク上の侵入イベントの合計数のグラフを表示します。	詳細ダッシュボード（Detailed Dashboard） サマリ ダッシュボード（Summary Dashboard）	Protection
全侵入イベント（非ドロップ）	発生頻度が最も多いタイプの侵入イベントを分類して表示します。ここでは、イベントの一部としてパケットはドロップしていません。	詳細ダッシュボード（Detailed Dashboard）	Protection
アプリケーションごとの接続許可（Allowed Connections by Application）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、アプリケーションごとにグループ化して表示します。	アプリケーション統計（Application Statistics）	FireSIGHT
アプリケーション リスクごとの接続許可（Allowed Connections by Application Risk）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、アプリケーションのリスク レベルによってグループ化して表示します。	アプリケーション統計（Application Statistics）	FireSIGHT
ビジネスとの関連性ごとの接続許可（Allowed Connections by Business Relevance）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、事業活動の推定される関連性によってグループ化して表示します。	アプリケーション統計（Application Statistics）	FireSIGHT
URL カテゴリごとの接続許可（Allowed Connections by URL Category）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、URL カテゴリごとにグループ化して表示します。	URL 統計（URL Statistics）	URL Filtering
URL レピュテーションごとの接続許可（Allowed Connections by URL Reputation）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、URL レピュテーションごとにグループ化して表示します。	URL 統計（URL Statistics）	URL Filtering
ユーザごとの接続許可（Allowed Connections by User）	モニタリング対象のネットワーク上で許可されたアプリケーションの接続を、接続しているユーザごとにグループ化して表示します。	アクセス制御されたユーザ統計（Access Controlled User Statistics）	FireSIGHT
マルウェア取り込みアプリケーション プロトコル（Application Protocols Introducing Malware）	ネットワークを介して送信されたマルウェア ファイルの数を、ファイルの送信に使用されたアプリケーション プロトコルごとにグループ化して表示します。	ファイル ダッシュボード（Files Dashboard）	Malware
ファイル転送アプリケーション プロトコル（Application Protocols Transferring Files）	ネットワークを介して送信されたファイルの数を、ファイルの送信に使用されたアプリケーション プロトコルごとにグループ化して表示します。	ファイル ダッシュボード（Files Dashboard）	Protection
マルウェア取り込みクライアント アプリケーション（Client Applications Introducing Malware）	FireAMP コネクタで検出されたマルウェアにアクセスした、または作成したアプリケーション、または親ファイルを表示します。	ファイル ダッシュボード（Files Dashboard）	FireAMPサブスクリプション

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
ファイル転送クライアント アプリケーション（Client Applications Transferring Files）	ネットワークを介してファイルを送信したアプリケーション、または親ファイルを表示します。	ファイル ダッシュボード（Files Dashboard）	Protection
Clients	モニタリング対象のネットワーク上のクライアントを、タイプごとに表示します。	詳細ダッシュボード（Detailed Dashboard）	FireSIGHT
接続に基づいたアプリケーション（Connections by Application）	モニタリング対象のネットワーク上のアプリケーションを、検出された接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
宛先の大陸別の接続（Connections by Destination Continent）	モニタリング対象のネットワークから送信された接続の宛先の大陸を、接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
宛先の国別の接続（Connections by Destination Country）	モニタリング対象のネットワークから送信された接続の宛先の国を、接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
イニシエータ IP 別の接続（Connections by Initiator IP）	モニタリング対象のネットワーク上のホスト IP アドレスを、接続（ホスト上の IP アドレスがセッションを開始した接続）の数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
接続に基づいたポート（Connections by Port）	モニタリング対象のネットワーク上のポートを、検出された接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
レスポンダ IP別の接続（Connections by Responder IP）	モニタリング対象のネットワーク上のホスト IP アドレスを、接続（セッションのレスポンダがホスト上の IP アドレスであった接続）の数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	接続の概要（Connection Summary）	FireSIGHT
セキュリティ インテリジェンス カテゴリ別の接続（Connections by Security Intelligence Category）	モニタリング対象のネットワーク上の Security Intelligence によってモニタリングまたはブロックされたすべての接続を、Security Intelligence のカテゴリごとにグループ化して表示します。	サマリ ダッシュボード（Summary Dashboard）	Protection
発信元の大陸別の接続（Connections by Source Continent）	モニタリング対象のネットワークと通信する大陸を、各大陸から開始された接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
発信元の国別の接続（Connections by Source Country）	モニタリング対象のネットワークと通信する国を、各国から開始された接続数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT
URL カテゴリ別の接続（Connections by URL Category）	モニタリング対象のネットワーク上のすべてのアプリケーションの接続を、URL カテゴリごとにグループ化して表示します。	サマリ ダッシュボード（Summary Dashboard）	URL Filtering

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
URL レピュテーション別の接続(Connections by URL Reputation)	モニタリング対象のネットワーク上のすべてのアプリケーションの接続を、URL レピュテーションごとにグループ化して表示します。	サマリ ダッシュボード(Summary Dashboard)	URL Filtering
一定期間の接続(Connections over Time)	ダッシュボードの時間範囲で、モニタリング対象のネットワーク上の合計接続数のグラフを表示します。	接続の概要(Connection Summary)	FireSIGHT
アプリケーションごとの接続拒否(Denied Connections by Application)	モニタリング対象のネットワーク上で拒否された接続を、アプリケーションごとにグループ化して表示します。	アプリケーション統計(Application Statistics)	FireSIGHT
URL カテゴリごとの接続拒否(Denied Connections by URL Category)	モニタリング対象のネットワーク上で拒否された接続を、URL カテゴリごとにグループ化して表示します。	URL 統計(URL Statistics)	URL Filtering
URL レピュテーションごとの接続拒否(Denied Connections by URL Reputation)	モニタリング対象のネットワーク上で拒否された接続を、URL レピュテーションごとにグループ化して表示します。	URL 統計(URL Statistics)	URL Filtering
ユーザごとの接続拒否(Denied Connections by User)	モニタリング対象のネットワーク上で拒否された接続を、接続しているユーザごとにグループ化して表示します。	アクセス制御されたユーザ統計(Access Controlled User Statistics)	FireSIGHT
アプリケーションごとのイベント ドロップ(Dropped Events by Application)	ドロップされた侵入イベントを、アプリケーションごとにグループ化して表示します。	アプリケーション統計(Application Statistics)	Protection + FireSIGHT
ユーザごとのイベント ドロップ(Dropped Events by User)	ドロップされた侵入イベントを、ユーザごとにグループ化して表示します。	アクセス制御されたユーザ統計(Access Controlled User Statistics)	Protection + FireSIGHT
ドロップされた侵入イベント(Dropped Intrusion Events)	侵入イベントの数を分類して表示します。ここでは、パケットがドロップされています。	詳細ダッシュボード(Detailed Dashboard) サマリ ダッシュボード(Summary Dashboard)	Protection
デバイスごとのダイナミックなトラフィック分析(Dynamic Analysis Traffic by Device)	分析用に Collective Security Intelligence クラウドに送信されたファイル データのサイズに基づいて、最もアクティブなデバイスを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
時間でのダイナミックなトラフィック分析(Dynamic Analysis Traffic over Time)	ダッシュボードの時間範囲で、取得され、分析用にクラウドに送信されたファイル データのサイズを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
ファイル アクション(File Actions)	ネットワークを介して送信されたファイルの数を、ファイルの処理に使用したファイル ルール アクションごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	ProtectionまたはMalware
ファイル カテゴリ(File Categories)	ネットワークを介して送信されたファイルの数を、ファイルのカテゴリごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
ファイル性質(File Dispositions)	マルウェア クラウド ルックアップ ファイル ルールの結果としてネットワーク トラフィック内で検出されたファイル数を、マルウェアの性質ごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
ファイル名(File Names)	ネットワークを介して送信されたファイルの数を、ファイル名ごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
デバイスごとのファイル格納(File Storage by Device)	最も多くのファイル データを格納したデバイスを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
傾向ごとのファイル格納(File Storage by Disposition)	デバイス上に格納されたファイル データのサイズ(KB)を、ファイルの性質に基づいて表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
タイプごとのファイル格納(File Storage by Type)	デバイス上に格納されたファイル データのサイズ(KB)を、ファイルのタイプに基づいて表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
時間でのファイル格納(File Storage over Time)	ダッシュボードの時間範囲で管理対象のデバイス上に格納されているファイル データのキロバイト数のグラフを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
時間の経過に伴うファイル転送(File Transfers over Time)	ダッシュボードの時間範囲で、ネットワーク トラフィック内でシステムによって検出されたファイル転送の合計数のグラフを表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
ファイルタイプ(File Types)	ネットワークを介して送信されたファイルの数を、ファイルのタイプごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
マルウェアに感染しているファイル タイプ(File Types Infected with Malware)	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出されたマルウェアの数を、ファイルのタイプごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
時間でのダイナミックな分析用送信ファイル(Files Sent for Dynamic Analysis over Time)	ダッシュボードの時間範囲で、ダイナミックな分析のために送信されたファイルの合計数のグラフを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
時間での保管ファイル(Files Stored over Time)	ダッシュボードの時間範囲で、管理対象のデバイス上に格納されたファイルの合計数のグラフを表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
ファイルを受信したホスト(Hosts Receiving Files)	ネットワーク上のホスト IP アドレスで受信した(ダウンロードした)ファイル数を、IP アドレスごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
マルウェアを受信するホスト(Hosts Receiving Malware)	ネットワーク上のホスト IP アドレスで受信したマルウェア ファイル数を、IP アドレスごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malwareライセンスまたは FireAMPサブスクリプション
ファイルを送信したホスト(Hosts Sending Files)	ネットワーク上のホスト IP アドレスから送信した(アップロードした)ファイル数を、IP アドレスごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Protection
マルウェアを送信するホスト(Hosts Sending Malware)	ネットワーク上のホスト IP アドレスから送信したマルウェア ファイル数を、IP アドレスごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
アプリケーションごとの x イベント影響(Impact X Events by Application)	予想される影響レベルが x(x は数字の 0 ～ 4)のイベントの数を、アプリケーションごとにグループ化して表示します。	アプリケーション統計(Application Statistics)	Protection + FireSIGHT
アプリケーション プロトコルごとの x イベント影響レベル(Impact Level X Events by Application Protocol)	予想される影響レベルが x(x は数字の 1 ～ 2)のイベントの数を、アプリケーション プロトコルごとにグループ化して表示します。	サマリ ダッシュボード(Summary Dashboard)	Protection + FireSIGHT
ユーザごとの x イベント影響レベル(Impact Level X Events by User)	予想される影響レベルが x(x は数字の 0 ～ 4)のイベントの数を、ユーザごとにグループ化して表示します。	アクセス制御されたユーザ統計(Access Controlled User Statistics)	Protection + FireSIGHT
ホストごとの侵入の痕跡(Indications of Compromise by Host)	トリガーされた侵入の痕跡の数を、関連付けられているホスト IP アドレスごとにグループ化して表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
要分析侵入イベント(Intrusion Events Requiring Analysis)	分析が必要な侵入イベントの数を、イベントの分類に基づいて表示します。	詳細ダッシュボード(Detailed Dashboard)	Protection + FireSIGHT
標的大陸ごとの侵入イベント(Intrusion Events by Destination Continent)	侵入イベントの対象となった大陸を、各大陸に関連付けられているイベントの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
標的国ごとの侵入イベント(Intrusion Events by Destination Country)	侵入イベントの対象となった国を、各国に関連付けられているイベントの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
発生大陸ごとの侵入イベント(Intrusion Events by Source Continent)	侵入イベントが生じた大陸を、各大陸から生じたイベントの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

Preset	説明	事前定義されたダッシュボード	ライセンス
発生国ごとの侵入イベント（Intrusion Events by Source Country）	侵入イベントが生じた国を、各国から生じたイベントの数に基づいて表示します。	サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
高重要度ホストへの侵入イベント（Intrusion Events to High Criticality Hosts）	侵入イベントを、重要度の高いホストで発生している侵入イベントの数に基づいて表示します。	詳細ダッシュボード（Detailed Dashboard）	Protection + FireSIGHT
マルウェア侵入（Malware Intrusions）	侵入イベントを、マルウェアを送信している接続で発生している侵入イベントの数に基づいて表示します。	ファイル ダッシュボード（Files Dashboard）	Malware
[マルウェア脅威（Malware Threats）]	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出されたマルウェアの脅威の数を、脅威の名前ごとにグループ化して表示します。	ファイル ダッシュボード（Files Dashboard）	Malwareライセンスまたは FireAMPサブスクリプション
時間での新たな侵入の痕跡（New Indications of Compromise over Time）	ダッシュボードの時間範囲で検出された、侵入の新しい痕跡のグラフを表示します。	サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
オペレーティング システム	オペレーティング システムを、ネットワーク内の各オペレーティング システムを実行しているホストの数に基づいて表示します。	詳細ダッシュボード（Detailed Dashboard）	FireSIGHT
潜在的ゼロデイ マルウェア（Possible Zero-Day Malware）	ファイルの性質が不明で、脅威スコアが High または Very High のいずれかであり、ゼロディ マルウェアである可能性が高い検出されたファイルを、ファイルが検出された回数に基づいて表示します。	ファイル ダッシュボード（Files Dashboard）	Malware
マルウェア取り込みプロセス（Processes Introducing Malware）	FireAMP コネクタによって検出されたマルウェアにアクセスしたシステム プロセス、またはそれらのマルウェアを作成したシステム プロセスを表示します。	ファイル ダッシュボード（Files Dashboard）	Malwareライセンスまたは FireAMPサブスクリプション
ビジネス関連性が低い危険なアプリケーション（Risky Applications with Low Business Relevance）	アプリケーション リスクのレベルが高く、予想されるビジネス関連性が低い、モニタリング対象のネットワーク上のすべてのアプリケーション接続を表示します。	サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
サーバ	サーバを、ホストの数ごとに表示します。	詳細ダッシュボード（Detailed Dashboard）	FireSIGHT
SSL アクション（SSL Actions）	暗号化されたトラフィックで行われた SSL ルール アクションの数を、頻度に基づいて表示します。	接続の概要（Connection Summary）	Any
SSL 証明書ステータス（SSL Certificate Status）	SSL 暗号化セッションでシステムが検出した証明書ステータスの数を、頻度に基づいて表示します。	接続の概要（Connection Summary）	Any
SSL 復号障害の原因（SSL Decryption Failure Reasons）	システムが SSL 暗号化セッションを正しく復号化できなかった理由の数を、頻度に基づいて表示します。	接続の概要（Connection Summary）	Any

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
時間での復号 SSL セッション(SSL Sessions Decrypted over Time)	ダッシュボードの時間範囲で、システムが復号化した SSL 暗号化セッションの数のグラフを表示します。	接続の概要(Connection Summary)	Any
時間での非復号 SSL セッション(SSL Sessions Not Decrypted over Time)	ダッシュボードの時間範囲で、システムが復号化しなかった SSL 暗号化セッションの数のグラフを表示します。	接続の概要(Connection Summary)	Any
時間でのエラー含有 SSL セッション(SSL Sessions with Errors over Time)	ダッシュボードの時間範囲で、内部エラーが含まれていることをシステムが検出した SSL 暗号化セッションの数のグラフを表示します。	接続の概要(Connection Summary)	Any
時間の経過に伴う脅威の検出(Threat Detections over Time)	ダッシュボードの時間範囲で、ネットワーク トラフィックにおいてシステム、または FireAMP コネクタのいずれかによって検出されたマルウェア脅威の合計数のグラフを表示します。	ファイル ダッシュボード(Files Dashboard)	Malwareライセンスまたは FireAMPサブスクリプション
上位攻撃者(Top Attackers)	モニタリング対象のネットワーク上の攻撃元のホスト IP アドレスを、リストされた IP アドレスが、イベントの発生元の接続での攻撃者である侵入イベントの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	Protection
上位検出クライアント アプリケーション(Top Client Applications Seen)	モニタリング対象のネットワーク上のクライアント アプリケーションを、クライアント アプリケーションによって伝送されたデータの合計(キロバイト)に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
上位検出オペレーティング システム(Top Operating Systems Seen)	モニタリング対象のネットワーク上のオペレーティング システムを、そのオペレーティング システムを持つネットワーク ホストの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
上位検出サーバ アプリケーション(Top Server Applications Seen)	モニタリング対象のネットワーク上のサーバ アプリケーションを、サービスを実行しているホストの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
上位ターゲット(Top Targets)	モニタリング対象のネットワーク上のホスト IP アドレスを、アドレスがイベントの発生元の接続の対象であった侵入イベントの数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	Protection
上位脅威(Top Threats)	脅威スコアの分布を、その脅威スコアを持つ格納ファイルの数に基づいて表示します。	ファイル ダッシュボード(Files Dashboard)	Malware
上位検出 Web アプリケーション(Top Web Applications Seen)	モニタリング対象のネットワーク上の Web アプリケーションを、クライアント アプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット（続き）

Preset	説明	事前定義されたダッシュボード	ライセンス
アプリケーションごとの合計イベント（Total Events by Application）	モニタリング対象のネットワーク上のアプリケーションを、アプリケーションによって生成された侵入イベントの数に基づいて表示します。	アプリケーション統計（Application Statistics）	Protection + FireSIGHT
アプリケーション プロトコルごとの合計イベント（Total Events by Application Protocol）	モニタリング対象のネットワーク上のアプリケーション プロトコルを、アプリケーション プロトコルに関連付けられている侵入イベントの数に基づいて表示します。	サマリ ダッシュボード（Summary Dashboard）	Protection + FireSIGHT
ユーザごとの合計イベント（Total Events by User）	モニタリング対象のネットワーク上のユーザを、各ユーザのアクティビティによって生成された侵入イベントの数に基づいて表示します。	サマリ ダッシュボード（Summary Dashboard） アクセス制御されたユーザ統計（Access Controlled User Statistics）	Protection + FireSIGHT
トラフィックに基づいたアプリケーション（Traffic by Application）	モニタリング対象のネットワーク上のアプリケーションを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいてアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	アプリケーション統計（Application Statistics） 接続の概要（Connection Summary） 詳細ダッシュボード（Detailed Dashboard）	FireSIGHT
アプリケーション カテゴリごとのトラフィック（Traffic by Application Category）	モニタリング対象のネットワーク上のアプリケーション カテゴリを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各カテゴリのアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	アプリケーション統計（Application Statistics） サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
アプリケーション リスクごとのトラフィック（Traffic by Application Risk）	モニタリング対象のネットワーク上のアプリケーションの予想されるリスク レベルを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各レベルでアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
ビジネスとの関連性ごとのトラフィック（Traffic by Business Relevance）	モニタリング対象のネットワーク上のアプリケーションの予想されるビジネスとの関連性レベルを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各レベルでアプリケーションによって伝送されたデータの合計キロバイト数に基づいて表示します。	サマリ ダッシュボード（Summary Dashboard）	FireSIGHT
接続先大陸ごとのトラフィック（Traffic by Destination Continent）	モニタリング対象のネットワークからアクセスされた大陸を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各大陸へ伝送されたデータの合計キロバイト数に基づいて表示します。	接続の概要（Connection Summary）	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
接続先国ごとのトラフィック(Traffic by Destination Country)	モニタリング対象のネットワークからアクセスされた国を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各国へ伝送されたデータの合計キロバイト数に基づいて表示します。	接続の概要(Connection Summary)	FireSIGHT
イニシエータ IP ごとのトラフィック(Traffic by Initiator IP)	モニタリング対象のネットワーク上のホスト IP アドレスを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて IP アドレスから伝送されたデータの合計キロバイト数に基づいて表示します。	接続の概要(Connection Summary) 詳細ダッシュボード(Detailed Dashboard)	FireSIGHT
イニシエータ ユーザごとのトラフィック(Traffic by Initiator User)	モニタリング対象のネットワーク上のユーザを、ユーザがログインしたホストで受信したデータの合計(キロバイト)に基づいて表示します。	詳細ダッシュボード(Detailed Dashboard) サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
トラフィックに基づいたポート(Traffic by Port)	モニタリング対象のネットワーク上のレスポンダ ポートを、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各ポートを介して伝送されたデータの合計キロバイト数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	接続の概要(Connection Summary)	FireSIGHT
レスポンダ IP ごとのトラフィック(Traffic by Responder IP)	モニタリング対象のネットワーク上の IP アドレスを、ダッシュボードの時間範囲で、(ホスト上の)IP アドレスによって受信したデータの合計キロバイト数に基づいて表示します。このウィジェットの出力は、接続のロギング設定によって異なります。	接続の概要(Connection Summary) 詳細ダッシュボード(Detailed Dashboard)	FireSIGHT
セキュリティ インテリジェンス カテゴリごとのトラフィック(Traffic by Security Intelligence Category)	モニタリング対象のネットワーク上の Security Intelligence カテゴリを、ダッシュボードの時間範囲で、各カテゴリの接続を介して伝送されたデータの合計キロバイト数に基づいて表示します。	サマリ ダッシュボード(Summary Dashboard)	Protection
送信元大陸ごとのトラフィック(Traffic by Source Continent)	モニタリング対象のネットワークへデータを伝送している大陸を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各大陸から伝送されたデータの合計キロバイト数に基づいて表示します。	接続の概要(Connection Summary)	FireSIGHT
送信元国ごとのトラフィック(Traffic by Source Country)	モニタリング対象のネットワークへデータを伝送している国を、ダッシュボードの時間範囲で、モニタリング対象のネットワークにおいて各国から伝送されたデータの合計キロバイト数に基づいて表示します。	接続の概要(Connection Summary)	FireSIGHT

表 55-5　Custom Analysis ウィジェットのプリセット(続き)

Preset	説明	事前定義されたダッシュボード	ライセンス
URL カテゴリごとのトラフィック(Traffic by URL Category)	モニタリング対象のネットワーク上のアプリケーション URL カテゴリを、ダッシュボードの時間範囲で、各カテゴリの URL と通信されたデータの合計キロバイト数に基づいて表示します。	URL 統計(URL Statistics)	URL Filtering
URL レピュテーションごとのトラフィック(Traffic by URL Reputation)	モニタリング対象のネットワーク上のアプリケーション URL レピュテーション タイプを、ダッシュボードの時間範囲で、各レピュテーションの URL と通信されたデータの合計キロバイト数に基づいて表示します。	URL 統計(URL Statistics)	URL Filtering
ユーザごとのトラフィック(Traffic by User)	モニタリング対象のネットワーク上のユーザを、ダッシュボードの時間範囲で、各ユーザと通信されたデータの合計キロバイト数に基づいて表示します。	なし	FireSIGHT
トラフィック経過時間(Traffic over Time)	ダッシュボードの時間範囲で、モニタリング対象のネットワークで伝送されたデータの合計キロバイト数のグラフを表示します。	接続の概要(Connection Summary) 詳細ダッシュボード(Detailed Dashboard)	FireSIGHT
時間での一意アプリケーション(Unique Applications over Time)	ダッシュボードの時間範囲で、モニタリング対象のネットワークで検出された一意のアプリケーションの合計のグラフを表示します。	アプリケーション統計(Application Statistics) サマリ ダッシュボード(Summary Dashboard)	FireSIGHT
時間での一意ユーザ(Unique Users over Time)	ダッシュボードの時間範囲で、モニタリング対象のネットワークで検出された一意のユーザの合計のグラフを表示します。	アクセス制御されたユーザ統計(Access Controlled User Statistics)	FireSIGHT
マルウェアの影響を受けるユーザ(Users Affected by Malware)	システム、または FireAMP コネクタによってネットワーク トラフィック内で検出された脅威の数を、ユーザごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malware + FireSIGHT、またはFireAMPサブスクリプション
ファイルを転送するユーザ(Users Transferring Files)	ネットワークを介して伝送されているファイルの数を、送信者ごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malware + FireSIGHT
マルウェア取り込み Web アプリケーション(Web Applications Introducing Malware)	モニタリング対象のネットワーク上の Web アプリケーション(FireAMP コネクタで検出されたマルウェアにアクセスしたアプリケーション、またはこのようなマルウェアを作成したアプリケーション)を表示します。	ファイル ダッシュボード(Files Dashboard)	Malwareライセンスまたは FireAMPサブスクリプション
Web アプリケーション伝送ファイル(Web Applications Transferring Files)	ネットワークを介して送信されたファイルの数を、ファイルの送信に使用された Web アプリケーションごとにグループ化して表示します。	ファイル ダッシュボード(Files Dashboard)	Malwareライセンスまたは FireAMPサブスクリプション
ホワイトリスト違反(White List Violations)	ホワイト リスト違反のホストを、違反件数ごとに表示します。	詳細ダッシュボード(Detailed Dashboard)	FireSIGHT

Custom Analysis ウィジェットから関連付けられているイベントの表示

ライセンス：任意（Any）

Custom Analysis ウィジェットで表示されるように設定しているデータの種類によっては、イベント ビュー（つまりワークフロー）を起動することができます。イベント ビューは、ウィジェットに表示されるイベントの詳細情報を提供します。

ダッシュボードからイベント ビューを起動すると、対象のイベント タイプについてのデフォルト ワークフローにイベントが表示されますが、これはダッシュボードの時間範囲による制約を受けます。また、設定した時間枠の数、および表示するイベントのタイプによっても、アプライアンスに対する適切な時間枠が変更されます。

たとえば、防御センターに複数の時間枠が設定されており、Custom Analysis ウィジェットから正常性イベントにアクセスすると、デフォルトの正常性イベント ワークフローにイベントが表示され、正常性のモニタリング時間枠はダッシュボードの時間範囲に変更されます。

もうひとつの例として、1 つの時間枠を設定していて Custom Analysis ウィジェットから任意のタイプのイベントにアクセスすると、イベントはそのイベント タイプのデフォルト ワークフローに表示され、グローバル時間枠がダッシュボードの時間範囲に変更されます。

時間枠の詳細については、デフォルトの時間枠（71-6 ページ）および検索での時間制約の指定（60-6 ページ）を参照してください。

Custom Analysis ウィジェットから関連付けられているイベントを表示する方法：

アクセス：Admin/Any Security Analyst/Maint

手順 1　ウィジェットをどのように設定したかによって、次の 2 つのオプションがあります。

- イベントの相対的な発生数を表示するように設定されたウィジェット（つまり棒グラフ）で、任意のイベントをクリックして、そのイベント、およびウィジェットのプリファレンスによる制約を受ける関連イベントを表示します。また、ウィジェットの右下にあるすべて表示のアイコン（  ）をクリックして、ウィジェットのプリファレンスによる制約を受けるすべての関連イベントを表示することもできます。
- 一定期間の接続データを表示するよう設定されているウィジェットで、ウィジェットの右下にあるすべて表示のアイコンをクリックして、ウィジェットのプリファレンスによる制約を受けるすべての関連イベントを表示します。

特定のイベント タイプの操作については、以下の項を参照してください。

- セキュリティ インテリジェンス リストとフィードの操作（3-5 ページ）
- 監査レコードの表示（69-2 ページ）
- 侵入イベントの表示（41-10 ページ）
- ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）
- ファイル イベントの表示（40-9 ページ）
- マルウェア イベントの表示（40-20 ページ）
- キャプチャ ファイルの表示（40-34 ページ）
- ホストの表示（50-21 ページ）
- ホスト属性の表示（50-30 ページ）
- 侵入の痕跡の表示（50-36 ページ）
- サーバの表示（50-40 ページ）
- アプリケーションの詳細の表示（50-50 ページ）

- 脆弱性の表示（50-55 ページ）
- サードパーティの脆弱性の表示（50-61 ページ）
- 接続データとセキュリティ インテリジェンスのデータの表示（39-17 ページ）
- ユーザの表示（50-66 ページ）
- ユーザ アクティビティ イベントの表示（50-73 ページ）
- 相関イベントの表示（51-61 ページ）
- ホワイト リスト イベントの表示（52-34 ページ）
- ホワイト リスト違反の表示（52-39 ページ）
- ヘルス イベントの表示（68-55 ページ）
- ルール更新ログの表示（66-24 ページ）
- アクティブ スキャンの結果での作業（47-22 ページ）
- 地理位置情報の使用（58-24 ページ）
- カスタム テーブルについて（59-1 ページ）

Custom Analysis ウィジェットの制限

ライセンス：任意（Any）

Custom Analysis ウィジェットを使用する場合に、留意すべきいくつかの重要な点があります。

共有ダッシュボード上でウィジェットを設定する場合は、ユーザのアカウント権限によって、すべてのユーザがすべてのイベント タイプのデータを表示できるわけではないことに注意してください。たとえば、Maintenance Users は検出イベントを表示できません。

同様に、別のアプライアンスからインポートされたダッシュボードを使用している場合は、すべてのアプライアンスがすべてのイベント タイプのデータにアクセスできるわけではないことに注意してください。たとえば、管理対象のデバイスに相関データは格納されません。ダッシュボードに、ユーザが表示できないデータを表示する Custom Analysis ウィジェットが含まれている場合、ウィジェットに、そのユーザにデータの表示権限がないことが示されます。ただし、そのユーザ（およびダッシュボードを共有している他のユーザ）は、ウィジェットの設定を変更して、自分が表示できるデータを表示することも、ウィジェットを削除することもできることに注意してください。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

ユーザがアクセスできる検索は、プライベートで保存した検索だけです。共有ダッシュボード上にウィジェットを設定し、プライベートの検索を使用してイベントを制約すると、ウィジェットは、他のユーザがログインしたときにその検索を使用しないようにリセットされます。ウィジェットのビューにも影響します。これを防ぐには、ダッシュボードをプライベート（非公開）で保存します。

Custom Analysis ウィジェットは、システム ポリシーの [ダッシュボード（Dashboard）] 設定から有効または無効にします。詳細については、ダッシュボードの設定（63-15 ページ）を参照してください。

Disk Usage ウィジェットについて

ライセンス：任意（Any）

Disk Usage ウィジェットは、ディスク使用率のカテゴリに基づいて、ハード ドライブで使用される領域のパーセンテージを表示します。また、アプライアンスのハード ドライブの各パーティションで使用される領域のパーセンテージおよび容量も示します。Disk Usage ウィジェットがデバイスにインストールされている場合、または防御センターが、マルウェア ストレージ パックが含まれているデバイスを管理している場合は、Disk Usage ウィジェットはマルウェア ストレージ パックについて同じ情報を表示します。このウィジェットは、Default Dashboard および Summary Dashboard の [ステータス（Status）] タブにデフォルトで表示されます。

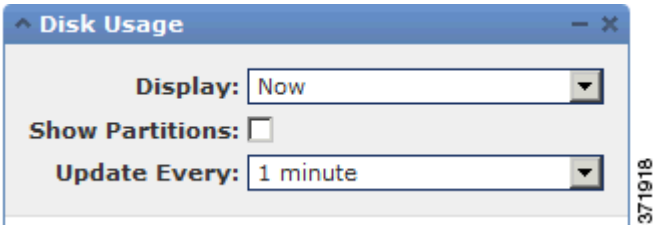
[カテゴリ別（By Category）] スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 55-6　ディスク使用率のカテゴリ

ディスク使用率のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
ファイル（Files）	システムに格納されたすべてのファイル
バックアップ	すべてのバックアップ ファイル
変更点	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
その他	システムのトラブルシューティング ファイルおよびその他のファイル
未使用	アプライアンス上の残りの空き領域

By Category スタック バーのディスク使用率カテゴリにポインタを合わせると、使用可能なディスク領域のうち、そのカテゴリで使用された領域の割合、ディスク上の実際のストレージ領域、およびそのカテゴリで使用可能なディスク領域の合計を表示することができます。マルウェア ストレージ パックがインストールされている場合は、Files カテゴリで使用できるディスク領域の合計は、マルウェア ストレージ パックで使用できるディスク領域になることに注意してください。詳細については、キャプチャ ファイル ストレージについて（40-3 ページ）を参照してください。

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、[カテゴリ別（By Category）] スタック バーのみを表示したり、スタック バーと admin（/）、`/Volume`、および `/boot` パーティションの使用率、および `/var/storage` パーティションを表示したりするようにウィジェットを設定できます。



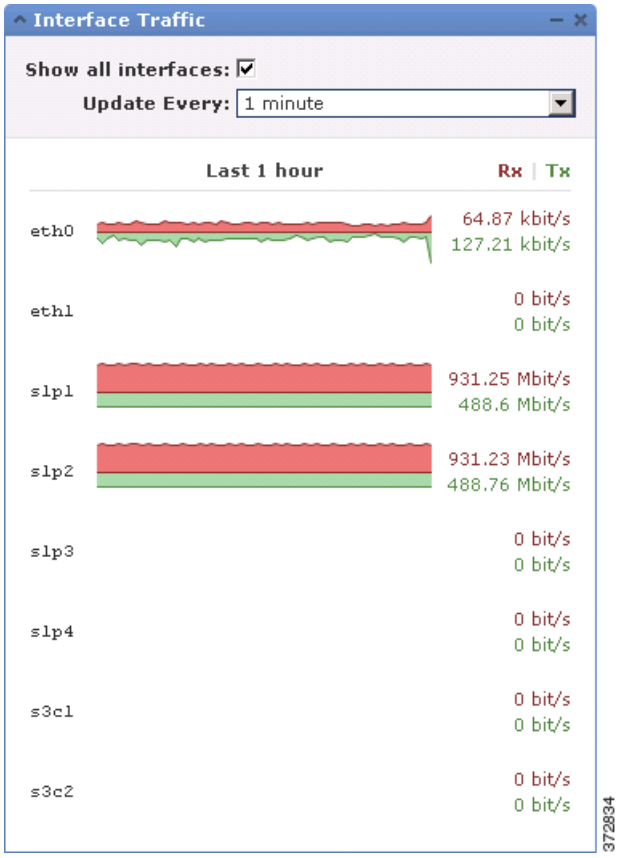
ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

インターフェイス トラフィック ウィジェットについて

ライセンス：任意（Any）

Interface Traffic ウィジェットは、ダッシュボードの時間範囲において、アプライアンスの管理（`eth0` など）インターフェイスおよびセンシング（`s1p1` など）インターフェイス上で受信した（Rx）トラフィックおよび送信した（Tx）トラフィックの割合を示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。

アウトバウンド（送信）トラフィックには、フロー制御パケットが含まれます。このため、アプライアンス上のパッシブ インターフェイスは送信トラフィックを示し、イベントを生成する場合があります。これは予期された動作です。ダイナミックな解析を設定していない場合でも、Malwareライセンスが有効になっているデバイスはシスコクラウドへの接続を定期的に試行することにも注意してください。このため、これらのデバイスは送信トラフィックを示します。これもまた予期された動作です。

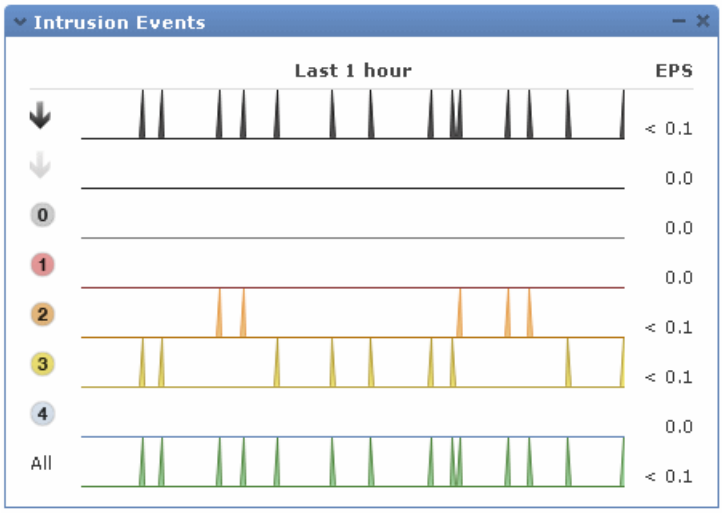


ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。管理対象デバイスでは、設定は、使用されていないインターフェイスのトラフィック レートをウィジェットに表示するかどうかも制御します(デフォルトでは、ウィジェットにはアクティブなインターフェイスのトラフィック レートのみが表示されます)。詳細については、ウィジェットのプリファレンスについて(55-8 ページ)を参照してください。

Intrusion Events ウィジェットについて

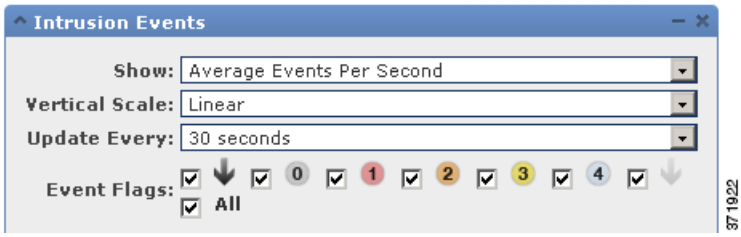
ライセンス:Protection

Intrusion Events ウィジェットは、ダッシュボードの時間範囲で発生した侵入イベントを、優先度ごとに表示します。これには、ドロップされたパケットおよびさまざまな影響を含む、侵入イベントの統計が含まれています。このウィジェットは、Summary Dashboard の [侵入イベント(Intrusion Events)] タブにデフォルトで表示されます。



管理対象デバイスで、このウィジェットは、ドロップされた（つまり、パッシブに配置されたデバイスではドロップされたと考えられる）侵入イベント、すべての侵入イベント、またはその両方の統計を表示できます。ローカル イベント ストレージを有効にしなければならないことに注意してください。有効にしないと、ウィジェットには表示するデータがありません。[All] で示される合計の割合には、ドロップされたイベントの割合は含まれないことにも注意してください。

管理対象のデバイスではなく、防御センターでは、ウィジェットの設定を変更して、ドロップされた（またはドロップされたと考えられる）パケットを持つ侵入イベント、およびさまざまな影響を表示するようにウィジェットを設定することができます。防御センター およびデバイス上でドロップされたイベント、およびドロップされたと考えられるイベントを表示することができます。次の図は、ウィジェットの設定の防御センターバージョンを示しています。



ウィジェットの設定では、次のことができます。

- 防御センターで、1 つ以上の [イベント フラグ（Event Flags）] チェックボックスを選択して、ドロップされたパケット、ドロップされたと考えられるパケット、または特定の影響を持つイベントを別のグラフで表示することができます。影響やルールの状態に関係なくすべての侵入イベントについて別のグラフを表示する場合は、[すべて（All）] を選択します。詳細については、影響レベルを使用してイベントを評価する（41-41 ページ）を参照してください。
- [表示（Show）] を選択して、[1 秒あたりの平均イベント（Average Events Per Second）] または [合計イベント（Total Events）] を選択します。
- [縦軸（Vertical Scale）] を選択して、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

Intrusion Events ウィジェットでは、次のことができます。

- 防御センターで、ドロップされたパケット、ドロップされたと考えられるパケット、または特定の影響に対応するグラフをクリックして、そのタイプの侵入イベントを表示します
- ドロップされたイベントに対応するグラフをクリックして、ドロップされたイベントを表示します
- ドロップされたと考えられるイベントに対応するグラフをクリックして、ドロップされたと考えられるイベントを表示します
- [All] グラフをクリックして、すべての侵入イベントを表示します。

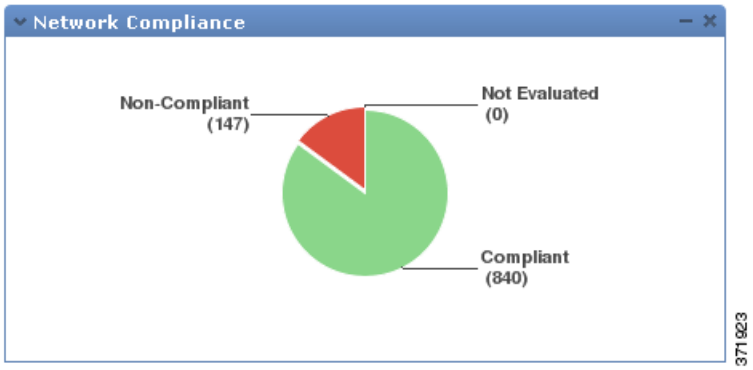
結果のイベント ビューは、ダッシュボードの時間範囲に制約されることに注意してください。ダッシュボードを介して侵入イベントにアクセスすると、そのアプライアンスに対するイベント（またはグローバル）の時間枠が変わります。侵入イベントの詳細については、侵入イベントの表示（41-10 ページ）を参照してください。

ルールの状態、または侵入ポリシーのインライン ドロップ動作に関係なく、パッシブな配置のパケットはドロップされないことに注意してください。

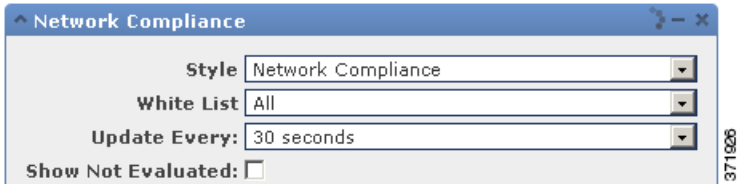
Network Compliance ウィジェットについて

ライセンス：FireSIGHT

Network Compliance ウィジェットは、ユーザが設定したホワイト リストに対するホストのコンプライアンスを要約します（FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照してください）。デフォルトでは、このウィジェットにアクティブな相関ポリシーにおけるすべてのコンプライアンス ホワイト リストに対して準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフが表示されます。このウィジェットは、Detailed Dashboard の [相関（Correlation）] タブにデフォルトで表示されます。



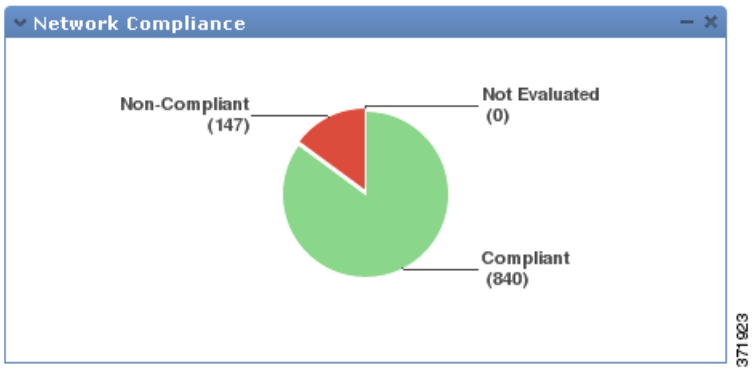
ウィジェットの設定を変更して、すべてのホワイト リスト、または特定のホワイト リストのいずれかについてネットワーク コンプライアンスを表示するようにウィジェットを設定できます。



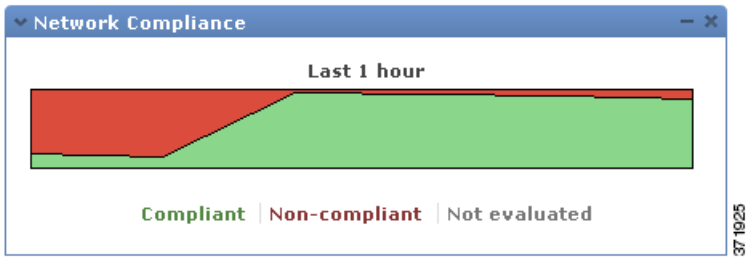
すべてのホワイト リストに対してネットワーク コンプライアンスを表示するよう選択すると、あるホストが、アクティブな相関ポリシーのいずれのホワイト リストにも準拠していない場合、ウィジェットはそのホストが非準拠であるとみなします。

また、このウィジェットの設定を使用すると、ネットワーク コンプライアンスの表示で次の 3 つのスタイルのうちどれを使用するかを指定することができます。

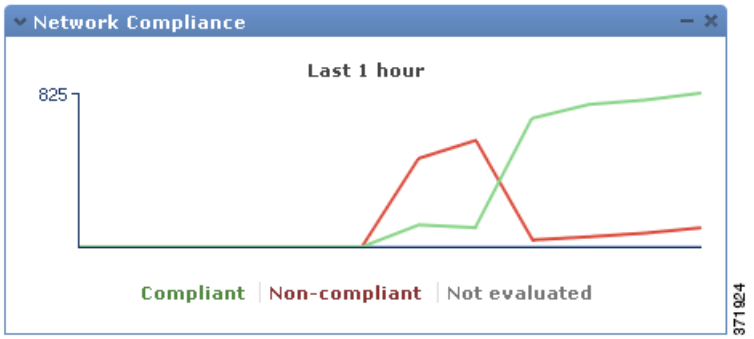
[ネットワーク コンプライアンス(Network Compliance)] スタイル(デフォルト)は、準拠しているホスト、準拠していないホスト、および評価されなかったホストの数を示す円グラフを表示します。ホストの違反の件数を表示するには、円グラフをクリックします。このようにすると、少なくとも 1 つのホワイト リストに違反しているホストが表示されます。詳細については、ホワイト リスト違反の表示(52-39 ページ)を参照してください。



[経時ネットワーク コンプライアンス(%)(Network Compliance over Time (%))] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの相対的な割合を示す積み重ね面積グラフを表示します。



[経時ネットワーク コンプライアンス(Network Compliance over Time)] スタイルは、ダッシュボードの時間範囲において準拠しているホスト、準拠していないホスト、およびまだ評価されていないホストの数を示す折れ線グラフを表示します。

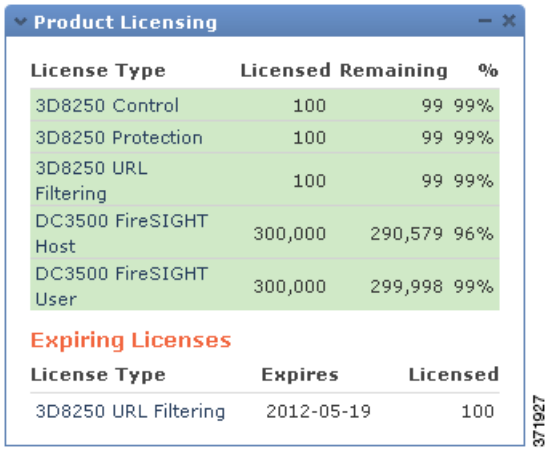


設定は、ウィジェットをアップデートする頻度を調整します。まだ評価されていないイベントを非表示にするには、[未評価の表示（Show Not Evaluated）] ボックスを選択します。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

[製品ライセンス（Product Licensing）] ウィジェットについて

ライセンス：任意（Any）

[製品ライセンス（Product Licensing）] ウィジェットは、防御センターに現在インストールされているデバイスおよび機能のライセンスを示します。また、ライセンス契約されているアイテム（ホストやユーザ）の数、許可される残りのライセンス契約アイテム数も示します。これは、事前定義されたどのダッシュボードにおいてもデフォルトでは表示されません。



このウィジェットの上部のセクションには、一時的なライセンスも含めて、防御センターにインストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、一時的なライセンスおよび期限の切れたライセンスのみが表示されます。たとえば FireSIGHT Host に対して 2 つの機能ライセンスを持っており、1 つは永久ライセンスで 750 台のホストが使用可能で、もうひとつは一時ライセンスで追加の 750 台のホストが使用可能であるとします。この場合、ウィジェットの上部のセクションには、ライセンス契約された 1500 台のホストの FireSIGHT Host 機能ライセンスが表示されますが、[期限の切れたライセンス（Expiring Licenses）] セクションには、750 台のホストの FireSIGHT Host 機能ライセンスが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

任意のライセンス タイプをクリックすると、ローカル設定の [ライセンス（License）] ページに移動して、機能ライセンスを追加または削除することができます。詳細については、FireSIGHT システム のライセンス（65-1 ページ）を参照してください。

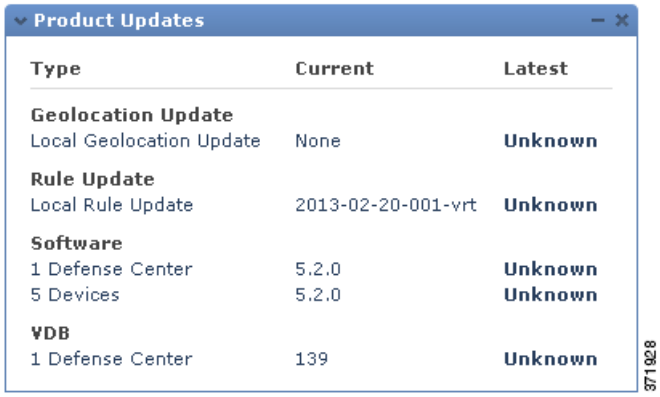
[製品アップデート(Product Updates)] ウィジェットについて

ライセンス:任意(Any)

[製品アップデート(Product Updates)] ウィジェットは、アプライアンスに現在インストールされているソフトウェア(FireSIGHT システムソフトウェアおよびルール アップデート)の概要と、そのソフトウェアについてダウンロードされているがまだインストールされていない使用可能なアップデートの情報を提供します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス(Status)] タブにデフォルトで表示されます。

このウィジェットは、ユーザがソフトウェアのアップデートをダウンロード、プッシュ、またはインストールするスケジュールされたタスクを設定していない場合、ソフトウェアの最新バージョンを [不明(Unknown)] と表示します。ウィジェットではスケジュールされたタスクを使用して、最新のバージョンを決定するためです。詳細については、タスクのスケジュール(62-1 ページ)を参照してください。

ウィジェットは、ソフトウェアをアップデートできるページへのリンクも提供します。ウィジェットの防御センターバージョンには類似のリンクがあり、このリンクを使用して管理対象のデバイスでソフトウェアをアップデートすることができます。



ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて(55-8 ページ)を参照してください。

製品アップデート ウィジェットでは、次のことができます。

- FireSIGHT システムソフトウェア、ルール アップデート、地理情報のアップデート、または VDB の最新バージョンをクリックして、アプライアンスを手動でアップデートします。
- システム ソフトウェア、地理情報データベース、または VDB をアップデートするには、システムソフトウェアの更新(66-1 ページ)を参照してください。
- 最新のルール アップデートをインポートするには、ルールの更新とローカル ルール ファイルのインポート(66-16 ページ)を参照してください。
- 最新バージョンをクリックするか、または [最新(Latest)] 列の [不明(Unknown)] リンクをクリックして、FireSIGHT システムソフトウェア、ルール アップデート、または VDB の最新バージョンをダウンロードするためのスケジュールされたタスクを作成します。タスクのスケジュール(62-1 ページ)を参照してください。

RSS Feed ウィジェットについて

ライセンス：任意（Any）

RSS Feed ウィジェットは、ダッシュボードに RSS フィードを追加します。デフォルトでは、ウィジェットはシスコセキュリティ ニュースのフィードを示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス（Status）] タブにデフォルトで表示されます。

また、企業ニュース、Snort.org ブログ、または脆弱性調査チーム（VRT）ブログの事前設定済みのフィードを表示するようウィジェットを設定することができます。ウィジェットの設定内に URL を指定して、他の RSS フィードに対するカスタム接続を作成することもできます。

フィードは 24 時間ごとにアップデートされます（ただしユーザはフィードを手動でアップデートできます）。また、ウィジェットはアプライアンスのローカル時間に基づいて、フィードが最後にアップデートされた時間を表示します。アプライアンスは、（事前設定された 2 つのフィードについて）Web サイトに対するアクセス権を持っている、または設定したいずれかのカスタムフィードに対するアクセス権を持っている必要があります。

ウィジェットを設定する場合には、フィードからいくつのストーリーをウィジェットに表示するか、およびヘッドラインとともにストーリーの説明を表示するかどうかを選択することができます。ただしすべての RSS フィードで説明が使用できるわけではないことに注意してください。

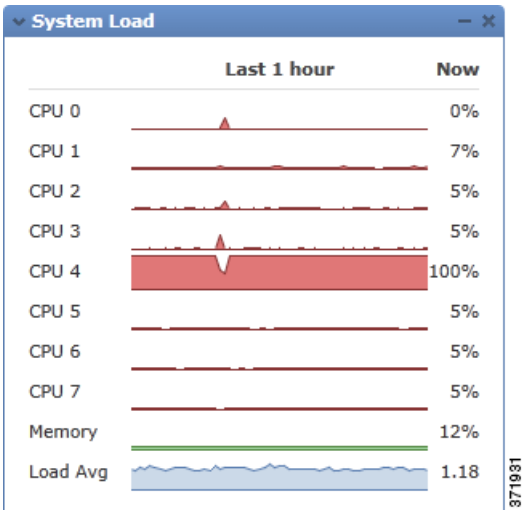
RSS Feed ウィジェットでは、次のことができます。

- フィード内のストーリーのいずれかをクリックして、ストーリーを表示します
- [もっと見る（more）] リンクをクリックして、フィードの Web サイトへ移動します
- アップデート アイコン（ ）をクリックして、フィードを手動でアップデートします

[システム負荷(System Load)] ウィジェットについて

ライセンス:任意(Any)

[システム負荷(System Load)] ウィジェットは、アプライアンス上の(各 CPU についての)CPU の使用率、メモリ(RAM)の使用率、およびシステムの負荷(実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる)を現在、およびダッシュボードの時間範囲について表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス(Status)] タブにデフォルトで表示されます。



ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて(55-8 ページ)を参照してください。

[システム時刻(System Time)] ウィジェットについて

ライセンス:任意(Any)

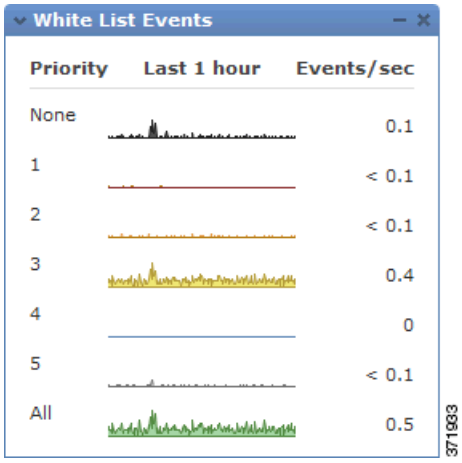
[システム時刻(System Time)] ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。このウィジェットは、詳細ダッシュボードおよびサマリ ダッシュボードの [ステータス(Status)] タブにデフォルトで表示されます。

ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。詳細については、ウィジェットのプリファレンスについて(55-8 ページ)を参照してください。

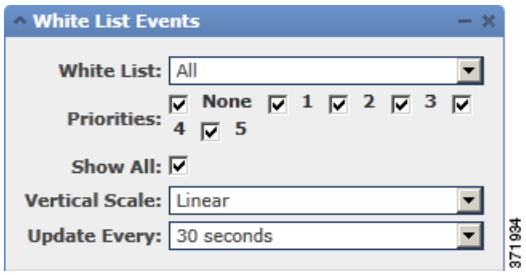
White List Events ウィジェットについて

ライセンス：FireSIGHT

White List Events ウィジェットは、ダッシュボードの時間範囲における 1 秒あたりの平均イベント数を、優先度ごとに表示します。このウィジェットは、Default Dashboard の [相関（Correlation）] タブにデフォルトで表示されます。



ウィジェットの設定を変更して、さまざまな優先度のホワイト リスト イベントを表示するようウィジェットを設定できます。



ウィジェットの設定では、次のことができます。

- 優先度を持たないイベントも含めて、特定の優先度のイベントに対して別のグラフを表示するには、1 つ以上の [プライオリティ（Priorities）] チェックボックスを選択します。
- 優先度に関係なくすべてのホワイト リスト イベントに対して追加のグラフを表示するには、[すべて表示（Show All）] を選択します。
- [縦軸（Vertical Scale）] を選択して、[線形（Linear）]（増分）または [対数（Logarithmic）]（10 の倍数）のスケールを選択できます。

プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットのプリファレンスについて（55-8 ページ）を参照してください。

グラフをクリックして特定の優先度のホワイト リスト イベントを表示することも、[すべて（All）] グラフをクリックしてすべてのホワイト リスト イベントを表示することもできます。いずれの場合も、イベントは、ダッシュボードの時間範囲に制約されます。ダッシュボードを介してホワイト リスト イベントにアクセスすると、防御センターに対するイベント（またはグローバル）の時間枠が変わります。ホワイト リスト イベントの詳細については、ホワイト リスト イベントの表示（52-34 ページ）を参照してください。

ダッシュボードの操作

ライセンス: 任意（Any）

ダッシュボードに示されるウィジェットを表示および変更できます。

[ダッシュボード管理（Dashboard Management）] ページでダッシュボードを管理します（ダッシュボードの表示（55-44 ページ）を参照してください）。ダッシュボードを作成、表示、変更、エクスポート、および削除できます。

各ダッシュボードでは、ページに所有者（ダッシュボードを作成したユーザ）が表示され、ダッシュボードがプライベートかどうかも示されます。Administrator 権限を持っていない場合は、自分のプライベート ダッシュボードのみを表示できます。他のユーザが作成したプライベート ダッシュボードを表示または変更することはできません。

最後に、ページには、どのダッシュボードがデフォルトかが示されます。ユーザの設定でデフォルトのダッシュボードを指定します。詳細については、デフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

ダッシュボード操作の詳細については、以下を参照してください。

- カスタム ダッシュボードの作成（55-42 ページ）
- ダッシュボードの表示（55-44 ページ）
- ダッシュボードの変更（55-46 ページ）
- ダッシュボードの削除（55-50 ページ）
- 設定のエクスポート（A-1 ページ）

カスタム ダッシュボードの作成

ライセンス: 任意（Any）

新しいダッシュボードを作成する場合は、ユーザが作成した、またはシスコで事前定義されている既存のダッシュボードをベースとして使用するよう選択できます。この場合は、既存のダッシュボードのコピーが作成されます。ユーザは自身のニーズに合わせてコピーを変更できます。また、既存のダッシュボードをベースとして使用せずに、新しい空のダッシュボードを作成することもできます。

また、タブの変更間隔およびページの更新間隔を指定する（または無効にする）必要があります。これらの設定は、ダッシュボードがタブを自動変更する頻度、およびダッシュボード全体のページを更新する頻度を定義します。

ダッシュボード全体を更新すると、共有のダッシュボードに対して他のユーザが行った設定またはレイアウトの変更や、他のコンピュータ上のプライベート ダッシュボードに対して、ダッシュボードが最後に更新された後で自分が行った変更を確認できます。これは、ダッシュボードが常に表示されているネットワーク オペレーション センター（NOC）などで有用です。ダッシュボードを変更する場合には、ローカル コンピュータで変更を行うことができます。この場合、NOC のダッシュボードは、ユーザが指定した間隔で自動的に更新され、NOC のダッシュボードを手動で更新しなくても変更が表示されます。データのアップデートを確認するためにダッシュボード全体を更新する必要はありません。個々のウィジェットは設定に従ってアップデートされます。

最後に、新しいダッシュボードをプライベート ダッシュボードとして保存して、そのダッシュボードをユーザ アカウントに関連付けることができます。ダッシュボードをプライベートとして保存しない場合、アプライアンスの他のすべてのユーザがダッシュボードを表示できるようになります。

すべてのユーザ ロールがすべてのダッシュボード ウィジェットに対してアクセス権を持っているわけではないため、多くの権限を持つユーザが作成したダッシュボードを、それよりも少ない権限を持つユーザが参照する場合、ダッシュボードのすべてのウィジェットを使用できないことがあることに注意してください。ダッシュボード上に、許可されていないウィジェットが表示されることがありますが、これらのウィジェットは無効です。

また、ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザが共有ダッシュボードを変更できることにも注意してください。特定のダッシュボードを自分のみが変更できるようにするには、そのダッシュボードをプライベートとして保存します。

ヒント　新しいダッシュボードを作成する代わりに、別のアプライアンスからダッシュボードをエクスポートし、それを自分のアプライアンスへインポートすることができます。その後でニーズに合わせて、インポートしたダッシュボードを編集することができます。自分が表示できるダッシュボードは、使用しているアプライアンスのタイプ、および自分のユーザ ロールによって異なることに注意してください。たとえば、防御センターで作成され、管理対象のデバイスにインポートされたダッシュボードには、無効なウィジェットが表示されることがあります。詳細については、設定のインポートおよびエクスポート（A-1 ページ）を参照してください。

新しいダッシュボードを作成するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）] を選択します。

[ダッシュボード管理（Dashboard Management）] ページが表示されます。

手順 2　[ダッシュボードの作成（Create Dashboard）] をクリックします。

[ダッシュボードの作成（Create Dashboard）] ページが表示されます。

手順 3　[ダッシュボードのコピー（Copy Dashboard）] ドロップダウンリストを使用して、新しいダッシュボードのベースとして使用するダッシュボードを選択します。

事前定義のダッシュボードまたはユーザ定義のダッシュボードを選択できます。オプションとして、[なし（None）]（デフォルト）を選択して、空のダッシュボードを作成することもできます。

手順 4　ダッシュボードの名前と説明（オプション）を入力します。

手順 5　[タブ変更頻度（Change Tabs Every）] フィールドで、ダッシュボードでタブを変更する頻度（分単位）を指定します。

ダッシュボードを一時停止した場合や、ダッシュボードのタブが 1 つのみの場合を除き、この設定により、指定した間隔で次のタブが表示されます。タブの自動変更を無効にするには、[タブ変更頻度（Change Tabs Every）] フィールドに 0 を入力します。

手順 6　[ページ更新頻度（Refresh Page Every）] フィールドで、現在のダッシュボード タブを新しいデータで更新する頻度を（分単位で）指定します。この値は、[タブ変更頻度（Change Tabs Every）] の設定より大きい値にする必要があります。

ダッシュボードを一時停止しない限り、この設定により、指定した間隔でダッシュボード全体が更新されます。定期的なページ更新を無効にするには、[ページ更新頻度（Refresh Page Every）] フィールドに 0 を入力します。

この設定は、個々のウィジェットの多くで使用可能なアップデート間隔とは異なることに注意してください。ダッシュボードのページを更新すると個々のウィジェットのアップデート間隔はリセットされますが、[ページ更新頻度（Refresh Page Every）] 設定を無効にしていても、ウィジェットはそれ自身の設定に従ってアップデートされます。

手順 7　オプションで、ダッシュボードを自分のユーザ アカウントと関連付けて、他のユーザがダッシュボードを表示および変更できないようにするために、[プライベートとして保存（Save As Private）] チェック ボックスを選択します。

手順 8　[保存（Save）] をクリックします。

ダッシュボードが作成され、Web インターフェイスに表示されます。これで、タブやウィジェットを追加して（既存のダッシュボードをベースにしている場合は、ウィジェットを再配置および削除して）、ニーズに合わせてダッシュボードを調整できるようになりました。詳細については、ダッシュボードの変更（55-46 ページ）を参照してください。

ダッシュボードの表示

ライセンス：任意（Any）

デフォルトでは、アプライアンスのホーム ページにデフォルトのダッシュボードが表示されます。デフォルトのダッシュボードを定義していない場合は、ホーム ページに [ダッシュボードの管理（Dashboard Management）] ページが示され、ここで表示するダッシュボードを選択できます。いつでも、[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] を選択して、アプライアンスに対して設定したデフォルトのダッシュボードを表示できます。使用可能なすべてのダッシュボードの詳細を表示する場合は、[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）] を選択します。

ヒント　ダッシュボード ページではないページを含む、別のデフォルト ホーム ページを表示するようにアプライアンスを設定できます。デフォルトのダッシュボードを変更することもできます。詳細については、ホームページの指定（71-2 ページ）およびデフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

各ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前（デフォルト）から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は [アプライアンス情報（Appliance Information）] ウィジェットには影響を与えません。このウィジェットは、アプライアンスの名前、モデル、および FireSIGHT システム ソフトウェアの現在のバージョンなどの情報を提供します。

企業による FireSIGHT システムの展開では、新しいイベントが古いイベントに置き換わる頻度によっては、時間範囲を長期に変更しても、Custom Analysis ウィジェットなどのウィジェットでは役立たない場合があることに注意してください。

ダッシュボードを一時停止することもできます。これにより変更を表示したり、分析を中断したりせずに、ウィジェットで提供されたデータを調べることができます。ダッシュボードを一時停止すると、次のような影響があります。

- Update Every ウィジェットの設定に関係なく、個々のウィジェットでアップデートが停止します。
- ダッシュボードのプロパティの [タブ周期頻度（Cycle Tabs Every）] 設定に関係なく、ダッシュボードのタブの自動変更が停止します。
- ダッシュボードのプロパティの [ページ更新頻度（Refresh Page Every）] 設定に関係なく、ダッシュボードのページの更新が停止します。
- 時間範囲を変更しても影響はありません。

分析が完了したら、ダッシュボードの一時停止を解除できます。ダッシュボードの一時停止を解除すると、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。また、ダッシュボードのプロパティで指定した設定に従って、ダッシュボード タブの自動変更が再開され、ダッシュボード ページの更新が再開されます。

ダッシュボードに対するシステム情報のフローを中断するような接続の問題、または他の問題が発生した場合、ダッシュボードは自動的に一時停止し、問題が解決するまでエラー通知を表示します。

(注)　ダッシュボードが一時停止しているかどうかに関係なく、セッションは通常、非アクティブな状態が 1 時間（または設定した他の時間）続いた場合、ユーザをログアウトします。ダッシュボードを長期間パッシブにモニタリングする場合は、一部のユーザをセッション タイムアウトしないよう設定したり、システムのタイムアウト設定を変更することを検討してください。詳細については、ユーザ ログイン設定の管理（61-51 ページ）およびユーザ インターフェイスの設定（63-31 ページ）を参照してください。

ダッシュボードを表示するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] を選択します。デフォルトのダッシュボードが定義されているかどうかによって、次の 2 つのオプションがあります。

- デフォルトのダッシュボードを定義している場合は、それが表示されます。別のダッシュボードを表示するには、[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] メニューを使用します。
- デフォルトのダッシュボードを定義していない場合は、[ダッシュボード管理（Dashboard Management）] ページが表示されます。表示するダッシュボードの隣の [表示（View）] をクリックします。

選択したダッシュボードが表示されます。

ダッシュボードの時間範囲を変更するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　[リストを表示（Show the Last）] ドロップダウンリストから、ダッシュボードの時間範囲を選択します。

ダッシュボードを一時停止しない限り、ページ上で該当するすべてのウィジェットがアップデートされ、最新の時間範囲が反映されます。

ダッシュボードを一時停止するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　時間枠のコントロールで、一時停止のアイコン（  ）をクリックします。

一時停止を解除するまで、ダッシュボードは一時停止します。

ダッシュボードの一時停止を解除するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　一時停止しているダッシュボードの時間範囲のコントロールで、再生のアイコン（▶）をクリックします。

ダッシュボードの一時停止が解除されます。

ダッシュボードの変更

ライセンス：任意（Any）

ダッシュボードには 1 つ以上のタブがあります。タブは追加、削除、および名前変更できます。ダッシュボードのタブの順序は変更できないことに注意してください。

各タブには、3 列のレイアウトで 1 つ以上のウィジェットを表示できます。ユーザは、ウィジェットを最小化および最大化する、タブに対してウィジェットを追加および削除する、タブ上でウィジェットを再配置する、といったことができます。

ダッシュボードの基本的なプロパティを変更することもできます。このプロパティには、名前と説明、タブの自動変更とページ更新の間隔、およびダッシュボードを他のユーザと共有するかどうかが含まれています。

ロールに関係なく、ダッシュボードへアクセスできるすべてのユーザは、共有ダッシュボードを変更できることに注意してください。特定のダッシュボードを自分だけが変更できるようにするには、ダッシュボードのプロパティでプライベート ダッシュボードとして設定します。

シスコの事前定義のダッシュボード内の Custom Analysis ウィジェットのすべての設定が、ウィジェットのプリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しい Custom Analysis ウィジェットを作成して復元することができます。詳細については、次を参照してください。

ヒント　シスコの事前定義のダッシュボード内の Custom Analysis ウィジェットのすべての設定が、ウィジェットのシステム プリセットに対応しています。これらのウィジェットの 1 つを変更または削除した場合は、適切なプリセットをベースにして新しい Custom Analysis ウィジェットを作成して復元することができます。詳細については、Custom Analysis ウィジェットの設定（55-17 ページ）を参照してください。

詳細については、次の項を参照してください。

- ダッシュボードのプロパティの変更（55-47 ページ）
- タブの追加（55-47 ページ）
- タブの削除（55-48 ページ）
- タブの名前変更（55-48 ページ）
- ウィジェットの追加（55-48 ページ）
- ウィジェットの再配置（55-49 ページ）
- ウィジェットの最小化および最大化（55-50 ページ）
- ウィジェットの削除（55-50 ページ）

ダッシュボードのプロパティの変更

ライセンス：任意（Any）

次の手順を使用してダッシュボードの基本的なプロパティを変更します。このプロパティには、名前と説明、タブの自動変更とページ更新の間隔、およびダッシュボードを他のユーザと共有するかどうかが含まれています。

ダッシュボードのプロパティを変更するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）] を選択します。

[ダッシュボード管理（Dashboard Management）] ページが表示されます。

手順 2　プロパティを変更するダッシュボードの隣の編集アイコン（ ）をクリックします。

[ダッシュボードの編集（Edit Dashboard）] ページが表示されます。変更可能なさまざまな設定の詳細については、カスタム ダッシュボードの作成（55-42 ページ）を参照してください。

手順 3　必要な変更を行い、[保存（Save）] をクリックします。

ダッシュボードが変更されます。

タブの追加

ライセンス：任意（Any）

ダッシュボードへタブを追加するには、次の手順を使用します。

ダッシュボードにタブを追加するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　タブを追加するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-44 ページ）を参照してください。

手順 2　既存のタブの右側で、タブの追加アイコン（ + ）をクリックします。

ポップアップ ウィンドウが表示され、タブに名前を指定するよう要求されます。

手順 3　（25 文字までの）タブの名前を入力し、[OK] をクリックするか、または単純に [OK] をクリックしてデフォルトの名前を受け入れます。タブの名前はいつでも変更できます。タブの名前変更（55-48 ページ）を参照してください。

新しいタブが追加されます。これで、新しいタブにウィジェットを追加できるようになりました。詳細については、ウィジェットの追加（55-48 ページ）を参照してください。

タブの削除

ライセンス：任意（Any）

次の手順を使用して、ダッシュボードのタブ、およびそのすべてのウィジェットを削除します。ダッシュボードから最後のタブを削除することはできません。各ダッシュボードには少なくとも 1 つのタブが必要です。

ダッシュボードからタブを削除するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　タブを削除するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-44 ページ）を参照してください。

手順 2　削除するタブで、削除のアイコン（ ✖ ）をクリックします。

手順 3　タブを削除することを確認します。

タブが削除されます。

タブの名前変更

ライセンス：任意（Any）

ダッシュボード タブの名前を変更するには、次の手順を使用します。

タブの名前を変更するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　タブの名前を変更するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-44 ページ）を参照してください。

手順 2　名称変更するタブをクリックします。

手順 3　タブのタイトルをクリックします。

ポップアップ ウィンドウが表示され、タブの名前を変更するよう要求されます。

手順 4　タブの名前（最大 25 文字）を入力し、[OK] をクリックします。

タブの名前が変更されます。

ウィジェットの追加

ライセンス：任意（Any）

ダッシュボードにウィジェットを追加するには、最初に、ウィジェットを追加するタブを決定する必要があります。タブにウィジェットを追加すると、アプライアンスによって自動的に、含まれているウィジェットが最も少ない列に追加されます。すべての列に同じ数のウィジェットがある場合、新しいウィジェットは最も左の列に追加されます。ダッシュボード タブには最大 15 個のウィジェットを追加できます。

ヒント　追加したウィジェットは、タブの任意の場所に移動できます。ただし、タブからタブへはウィジェットを移動できません。詳細については、ウィジェットの再配置（55-49 ページ）を参照してください。

ダッシュボードにウィジェットを追加するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　ウィジェットを追加するダッシュボードを表示します。

詳細については、ダッシュボードの表示（55-44 ページ）を参照してください。

手順 2　ウィジェットを追加するタブを選択します。

手順 3　[ウィジェットの追加（Add Widgets）] をクリックします。

[ウィジェットの追加（Add Widgets）] ページが表示されます。

ユーザが追加できるウィジェットは、使用しているアプライアンスのタイプと、自分のユーザロールによって異なります。ウィジェットは、Analysis & Reporting、Miscellaneous、および Operations の機能に従って整理されます。カテゴリ名をクリックして各カテゴリのウィジェットを表示することも、[すべてのカテゴリ（All Categories）] をクリックしてすべてのウィジェットを表示することもできます。

手順 4　追加するウィジェットの隣の [追加（Add）] をクリックします。

ヒント　（複数の RSS Feed ウィジェット、または複数の Custom Analysis ウィジェットを追加する場合など）同じタイプの複数のウィジェットを追加するには、[追加（Add）] をもう一度クリックします。

ウィジェットはすぐにダッシュボードに追加されます。[ウィジェットの追加（Add Widgets）] ページには、新しく追加したウィジェットも含めて、各タイプのウィジェットがタブ上にいくつあるかが示されます。

手順 5　オプションで、ウィジェットの追加が終了したときに、[完了（Done）] をクリックしてダッシュボードに戻ることもできます。

ウィジェットを追加したタブがもう一度表示され、変更が反映されます。

ウィジェットの再配置

ライセンス：任意（Any）

タブ上で、任意のウィジェットの場所を変更できます。ただし、別のタブにはウィジェットを移動できないことに注意してください。ウィジェットを別のタブに表示する場合は、現在のタブからいったん削除してから新しいタブに追加する必要があります。

ウィジェットを移動するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　移動するウィジェットのタイトル バーをクリックし、新しい場所へドラッグします。

ウィジェットの最小化および最大化

ライセンス：任意（Any）

ウィジェットを最小化してビューを単純化したり、その後で最大化してもう一度表示したりできます。

ウィジェットを最小化するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　ウィジェットのタイトル バーで、最小化のアイコン（ − ）をクリックします。

ウィジェットを最大化するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　ウィジェットのタイトル バーで、最大化のアイコン（ □ ）をクリックします。

ウィジェットの削除

ライセンス：任意（Any）

タブに表示する必要がなくなったウィジェットを削除します。

ウィジェットを削除するには、次のようにします。

アクセス：Admin/Any Security Analyst/Maint

手順 1　ウィジェットのタイトル バーで、閉じるアイコン（ ✖ ）をクリックします。

手順 2　ウィジェットを削除することを確認します。

タブからウィジェットが削除されます。

ダッシュボードの削除

ライセンス：任意（Any）

使用する必要がなくなった場合は、ダッシュボードを削除します。

デフォルトのダッシュボードを削除する場合は、新しいデフォルトを定義する必要があります。そうしない場合、ダッシュボードを表示しようとするたびに、アプライアンスからダッシュボードを選択するよう要求されます。詳細については、デフォルトのダッシュボードの指定（71-9 ページ）を参照してください。

ダッシュボードを削除するには、次の手順を実行します。

アクセス：Admin/Any Security Analyst/Maint

手順 1　[オーバービュー（Overview）] > [ダッシュボード（Dashboards）] > [管理（Management）] を選択します。

[ダッシュボード管理（Dashboard Management）] ページが表示されます。

手順 2　削除するダッシュボードの隣の削除アイコン（ ）をクリックします。

手順 3　ダッシュボードを削除することを確認します。

ダッシュボードが削除されます。