用 語 集

7000 シリーズ

シリーズ 3 FirePOWER 管理対象デバイスのグループ。このシリーズのデバイスには、70xx ファミリ（3D7010、3D7020、3D7030 モデル）と 71xx ファミリ（3D7110、3D7115、3D7120、3D7125、AMP7150 モデル）が含まれます。

8000 シリーズ

シリーズ 3 FirePOWER 管理対象デバイスのグループ。このシリーズのデバイスには、81xx ファミリ（3D8120、3D8130、3D8140、AMP8150 モデル）、82xx ファミリ（3D8250、3D8260、3D8270、3D8290 モデル）、および 83xx ファミリ（3D8350、3D8360、3D8370、3D8390 モデル）が含まれます。8000 シリーズ デバイスは、一般的に、7000 シリーズ デバイスより強力です。

ASA FirePOWER

Cisco ASA with FirePOWER Services の省略名。

Cisco ASA with FirePOWER Services

Cisco Adaptive Security Appliance（ASA）管理対象デバイスのグループ。このシリーズのデバイスには、ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40、および ASA5585-X-SSP-60 の各モデルが含まれます。

CLI

コマンドライン インターフェイスを参照してください。

Context Explorer

侵入、接続、ファイル、ジオロケーション、マルウェア、およびディスカバリ ポリシーを使用して、モニタ対象ネットワークに関する詳細でインタラクティブなグラフィカル情報を表示するページ。それぞれのセクションに、詳細なリストを伴う、鮮明な折れ線グラフ、棒グラフ、円グラフ、およびドーナツ グラフの形式で情報が表示されます。分析を微調整するためのカスタム フィルタの作成と適用を容易に行うことができ、また、グラフ領域をクリックするか、その上にマウス カーソルを移動することにより、データ セクションをより詳細に調査できます。高度にカスタマイズ可能で、区分化され、リアルタイムで更新されるダッシュボードに比べて、Context Explorer は、手動で更新され、そのデータの広範なコンテキストを提供するように設計され、アクティブ ユーザ調査用に設計された単一の一貫性のあるレイアウトで構成されています。

Control ライセンス

ユーザとアプリケーションの条件をアクセス コントロール ルールに追加することによって、ユーザ制御とアプリケーション制御の実装を可能にするライセンス。また、スイッチングとルーティング（DHCP リレーと NAT を含む）を実行するように管理対象デバイスを設定したり、管理対象デバイスのクラスタリングを設定したりすることもできます。

eStreamer

イベント データを防御センターまたは管理対象デバイスから外部のクライアント アプリケーションにストリーム配信するための FireSIGHT システム コンポーネント。

Event Streamer

eStreamer を参照してください。

FireAMP Connector

サブスクリプション ベースの FireAMP 展開内のユーザがコンピュータやモバイル デバイスなどのエンドポイント上にインストールする軽量エージェント。このコネクタは、シスコ クラウドと通信しながら、組織全体のマルウェアをすばやく特定して検疫するための情報を交換します。

FireAMP サブスクリプション

組織で FireAMP を高度なマルウェア対策（AMP）ソリューションとして使用するための別途購入されるサブスクリプション。管理対象デバイスでネットワークベースの AMP を実行するためのマルウェア ライセンスと比較してください。

FireAMP ポータル

組織のサブスクリプション ベースの FireAMP 展開を設定するための Web サイト（http://amp.sourcefire.com/）。

FireAMP

マルウェアの発生、持続的脅威、および標的型攻撃を検出、把握、およびブロックするシスコのエンタープライズクラスでエンドポイント ベースの高度なマルウェア分析および保護ソリューション。組織で FireAMP サブスクリプションが使用されている場合は、個別のユーザがエンドポイント（コンピュータ、モバイル デバイス）上で軽量の FireAMP Connector をインストールしてから、シスコ クラウドと通信します。これにより、マルウェアをすばやく特定して検疫するだけでなく、それらの発生を検出して、それらのトラジェクトリを追跡し、それらの影響を把握して、効果的な回復方法を習得することができます。FireAMP ポータルは、カスタム保護を構築したり、特定のアプリケーションの実行をブロックしたり、カスタム ホワイトリストを作成したりするためにも使用できます。ネットワークベースの高度なマルウェア対策と比較してください。

FireSIGHT ライセンス

ユーザが、ホスト、アプリケーション、およびユーザ検出を実行するための 防御センター 上のデフォルト ライセンス。FireSIGHT ライセンスは、防御センターとその管理対象デバイスを使用してモニタ可能な個別のホストとユーザの数だけでなく、アクセス コントロール ルールでユーザ制御を実行するために使用可能なアクセス制御ユーザの数も決定します。

GeoDB

ジオロケーション データベースを参照してください。

LDAP 認証

Lightweight Directory Access Protocol（LDAP）ディレクトリ サーバに保存された LDAP ディレクトリと比較することによって、ユーザ クレデンシャルを確認する外部認証の形式。

Lights-Out Management（LOM）

アウトオブバンド Serial over LAN（SoL）管理接続を使用して、アプライアンスの Web インターフェイスにログインせずに、アプライアンスをリモートでモニタまたは管理可能なシリーズ 3 の機能。シャーシのシリアル番号の表示やファンの速度や温度などの状態のモニタなど、限られたタスクを実行できます。

NAT ポリシー

NAT によるルーティングを実行するための NAT ルールを使用するポリシー。

NAT

ネットワーク アドレス変換。プライベート ネットワーク上の複数のホスト間で単一のインターネット接続を共有するために最もよく使用される機能。ディスカバリを使用すれば、システムはネットワーク デバイスを論理インターフェイスとして識別できます。加えて、FireSIGHT システムのレイヤ 3 展開では、NAT ポリシーを使用して NAT によるルーティングを設定できます。

NetMod

管理対象デバイス用のセンシング インターフェイスを含むそのデバイスのシャーシ内に設置するモジュール。

Protection ライセンス

侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンス フィルタリングを実行するためのシリーズ 3 とバーチャル デバイス用のライセンス。ライセンスがない場合は、シリーズ 2 デバイスがセキュリティ インテリジェンスを除く Protection 機能を自動的に使用します。

RADIUS 認証

Remote Authentication Dial In User Service。ネットワーク リソースへのユーザ アクセスの認証、許可、およびアカウンティングのために使用されるサービス。FireSIGHT システム ユーザが RADIUS サーバ経由で認証できるようにするための外部認証オブジェクトを作成できます。

SFP モジュール

71xx ファミリ デバイス上のネットワーク モジュールに挿入された Small Form-factor Pluggable トランシーバ。SFP モジュール上のセンシング インターフェイスは設定可能なバイパスを許可しません。

URL カテゴリ

マルウェアやソーシャル ネットワーキングなどの URL の一般的な分類。

URL フィルタリング ライセンス

URL カテゴリと URL レピュテーション情報に基づいて URL フィルタリングを実行可能なライセンス。URL フィルタリング ライセンスは期限切れになる場合があります。

URL フィルタリング

防御センターによってシスコ クラウドから取得された URL の URL カテゴリと URL レピュテーション情報と相関がある、モニタ対象ホストから要求された URL に基づいてネットワーク上を伝送可能なトラフィックを決定するアクセス コントロール ルールを作成するための機能。許可またはブロックする URL を個別にまたはグループで指定することによって、Web トラフィックに対するきめ細かなカスタム制御を実現することもできます。

UTC 時間

協定世界時。UTC はグリニッジ標準時（GMT）とも呼ばれ、世界中のあらゆる場所に共通の標準時間です。FireSIGHT システムは UTC を使用しますが、タイム ゾーン機能を使用して現地時刻を設定できます。

VDB

脆弱性データベースを参照してください。

VLAN

仮想ローカル エリア ネットワーク。VLAN は、地理的場所ではなく、部門や主な用途など、その他の基準でホストをマップします。モニタ対象ホストのホスト プロファイルには、そのホストに関連付けられたすべての VLAN 情報が表示されます。VLAN 情報は、イベントをトリガーしたパケット内の最も内側の VLAN タグとして、侵入イベントにも含まれています。侵入ポリシーとターゲット コンプライアンス ホワイト リストを VLAN でフィルタ処理することができます。レイヤ 2 展開とレイヤ 3 展開では、管理対象デバイス上の仮想スイッチと仮想ルータを VLAN タグ付きトラフィックを適切に処理するように設定できます。

VPN

シスコ 管理対象デバイス上の仮想ルータ間または管理対象デバイスからリモート デバイスや他のサードパーティ製 VPN エンドポイントまでのセキュアな VPN トンネルを構築するための機能。

VPN ライセンス

シスコ 管理対象デバイス上の仮想ルータ間または管理対象デバイスからリモート デバイスや他のサードパーティ製 VPN エンドポイントまでのセキュアな VPN トンネルを構築するためのライセンス。

VRT

シスコ VRT を参照してください。

Web アプリケーション

HTTP トラフィックの内容または HTTP トラフィックに対して要求された URL を表すアプリケーションの一種。

zone

セキュリティ ゾーンを参照してください。

アクセス コントロール ポリシー

管理対象デバイスでモニタするネットワーク トラフィックのアクセス制御を実行するためにそれらのデバイスに適用するポリシー。アクセス コントロール ポリシーには、複数のアクセス コントロール ルールを含めることができます。また、これらのルールの条件を満たさないトラフィックの処理とロギングを決定するデフォルト アクションも指定します。アクセス コントロール ポリシーは、HTTP 応答ページ、セキュリティ インテリジェンス、およびその他の詳細設定を指定することもできます。

アクセス コントロール ルール

FireSIGHT システム がモニタ対象ネットワーク トラフィックを検査するために使用し、きめ細かなアクセス制御を可能にするための一連の条件。アクセス コントロール ルールはアクセス コントロール ポリシーを設定し、単純な IP アドレス マッチングの実行、または複数のユーザ、アプリケーション、ポート、または URL が関係する複雑な接続の特性を決定することができます。アクセス コントロール ルール アクションによって、ルールの条件を満たすトラフィックをシステムがどのように処理するかが決定されます。その他のルール設定によって、接続をログに記録する方法（および記録するかどうか）と、一致するトラフィックを侵入ポリシーとファイル ポリシーのどちらで検査するかが決定されます。

アクセス リスト

システム ポリシーで設定された IP アドレスのリスト。アプライアンスにアクセス可能なホストを表します。デフォルトでは、すべての人がポート 443（HTTPS）を使用してアプライアンスの Web インターフェイスにアクセスし、ポート 22（SSH）を使用してコマンド ラインにアクセスすることができます。また、ポート 161 を使用して SNMP アクセスを追加することもできます。

アクセス制御

ネットワークを通過可能なトラフィックを指定、検査、およびログに記録するための FireSIGHT システム の機能。アクセス制御は、侵入検知および防御、ファイル制御、および高度なマルウェア対策の各機能を含み、ディスカバリ機能で検査可能なトラフィックも特定します。

アプライアンス

防御センターまたは管理対象デバイス。アプライアンスは物理にも仮想にもすることができます。

アプリケーション プロトコル

サーバとホスト上のクライアント アプリケーション間の通信中に検出されたアプリケーション プロトコル トラフィック（SSH や HTTP など）を表すアプリケーションの種類。

アプリケーション

検出済みのネットワーク アセット、通信手段、または HTTP コンテンツ。これに対するアクセス コントロール ルールを作成できます。システムは、アプリケーション プロトコル、クライアント アプリケーション、および Web アプリケーションという 3 種類のアプリケーションを検出します。

アプリケーション制御

アクセス制御の一部として、ネットワークを通過可能なアプリケーション トラフィックを指定するための機能。

アラート

システムが特定のイベントを生成したことを示す通知。アラートは、特定のアクセス コントロール ルールによってログに記録された侵入イベント（影響フラグを含む）、検出イベント、マルウェア イベント、相関ポリシー違反、ヘルス ステータスの変化、および接続に基づいて通知できます。アラートはほとんどの場合、電子メール、Syslog、または SNMP トラップ経由で通知できます。

イベント ビューア

イベントを表示して操作するためのシステム コンポーネント。イベント ビューアは、ワークフローを使用して、広範なイベント ビューを表示してから、興味のあるイベントだけを含む絞り込まれたイベント ビューを表示します。イベント ビューでは、ワークフローをドリルダウンしたり、検索を使用したりすることによって、イベントを制限できます。

イベント

イベント ビューアでワークフローを使用して表示可能な特定の出来事に関する詳細情報のコレクション。イベントは、ネットワークに対する攻撃、検出されたネットワーク アセットの変化、組織のセキュリティ ポリシーやネットワーク利用ポリシーの違反などを表すことができます。システムは、変わりやすいアプライアンスのヘルス ステータス、Web インターフェイスの使用状況、ルール更新、および起動された修復に関する情報を含むイベントも生成します。最後に、システムは、これらの「イベント」が特定の出来事を表していない場合でも、その他の特定の情報をイベントとして表示します。たとえば、イベント ビューアを使用して、検出されたホスト、アプリケーション、およびそれらの脆弱性に関する詳細情報を表示できます。

インポート

アプライアンス間でさまざまな設定を転送するために使用可能な手段。同じタイプの別のアプライアンスからエクスポートした設定をインポートすることができます。

インライン インターフェイス

インライン展開でトラフィックを処理するように設定されたセンシング インターフェイス。ペア内のインライン セットにインライン インターフェイスを追加する必要があります。

インライン セット

インライン インターフェイスの 1 つ以上のペア。

インライン展開

管理対象デバイスがネットワーク上にインラインで配置される FireSIGHT システム の展開。この設定では、デバイスがスイッチング、ルーティング、アクセス制御、および侵入検知および防御を使用してネットワーク トラフィック フローに影響を与える場合があります。

ウィジェット

ダッシュボード ウィジェットを参照してください。

エンドポイント

ユーザが組織の高度なマルウェア対策戦略の一部として FireAMP Connector をインストールするコンピュータまたはモバイル デバイス。

カスタム ユーザ ロール

特殊なアクセス権限を持つユーザ ロール。カスタム ユーザ ロールは、メニュー ベースのアクセス許可とシステム アクセス許可のセットを有し、完全にオリジナルにすることも、事前定義されたユーザ ロールに基づくこともできます。

仮想スイッチ

ネットワーク経由で着信トラフィックと発信トラフィックを処理するスイッチド インターフェイスのグループ。レイヤ 2 展開では、管理対象デバイス上に仮想スイッチを設定して、ネットワークを論理セグメントに分割しながらスタンドアロン ブロードキャスト ドメインとして動作させることができます。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用してパケットの送信先を決定します。

仮想防御センター

仮想ホスティング環境内の独自の設備に展開可能な防御センター。

仮想ルータ

レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループ。レイヤ 3 展開では、宛先 IP アドレスに基づいてパケット転送を決定することにより、パケットをルーティングするように仮想ルータを設定できます。静的ルートを定義したり、Routing Information Protocol（RIP）および Open Shortest Path First（OSPF）ダイナミック ルーティング プロトコルを設定したり、ネットワーク アドレス変換（NAT）を実装したりできます。

管理インターフェイス

FireSIGHT システム アプライアンスの管理に使用するネットワーク インターフェイス。ほとんどの展開において、管理インターフェイスは内部の保護されたネットワークに接続されます。センシング インターフェイスと比較してください。

管理対象デバイス

デバイスを参照してください。

クライアント アプリケーション

クライアントを参照してください。

クライアント

クライアント アプリケーションとも呼ばれる。あるホスト上で動作しながら、特定の処理を別のホスト（サーバ）に依存するアプリケーション。たとえば、電子メール クライアントを使用すれば、電子メールを送受信することができます。あるホスト上のユーザが特定のクライアントを使用して別のホストにアクセスしていることをシステムが検出すると、そのクライアントの名前とバージョン（入手可能な場合）を含む情報をホスト プロファイルとネットワーク マップで報告します。

クラスタリング

2 つのピア シリーズ 3 デバイスまたはスタック間のネットワーキング機能と構成データの冗長性を実現可能にする機能。クラスタリングは、ポリシー適用、システム更新、および登録のための単一の論理システムを提供します。冗長な防御センターを設定可能なハイ アベイラビリティと比較してください。

高度なマルウェア対策

略して AMP。FireSIGHT システムのネットワークベースのマルウェア検出機能とマルウェア クラウド検索機能。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

コマンドライン インターフェイス

シリーズ 3 と仮想デバイス上の制限付きテキスト ベース インターフェイス。CLI ユーザが実行可能なコマンドは、そのユーザに割り当てられたアクセス レベルによって異なります。

コンテキスト メニュー

Web インターフェイス上のさまざまなページで利用可能なポップアップ メニュー。FireSIGHT システム の他の機能にアクセスするためのショートカットとして使用できます。メニューの内容は、表示しているページ、調査している特定のデータ、割り当てられたユーザ ロールなどさまざまな要素によって異なります。コンテキスト メニュー オプションには、侵入ルール、イベント、およびホスト情報へのリンク、さまざまな侵入ルール設定、Context Explorer へのクイック リンク、IP アドレスによるセキュリティ インテリジェンス グローバル ブラックリストまたはグローバル ホワイトリストをホストに追加するためのオプション、およびグローバル ホワイトリストに SHA-256 ハッシュ値を使用してファイルを追加するためのオプションがあります。

サーバ

アプリケーション プロトコル トラフィックによって識別される、ホスト上にインストールされたサーバ アプリケーション（クライアント アプリケーションと比較してください）。

ジオロケーション データベース

ルーティング可能な IP アドレスに関連付けられた既知のジオロケーション データの定期更新データベース（GeoDB とも呼ばれる）。

ジオロケーション

接続タイプやインターネット サービス プロバイダーなどのモニタ対象ネットワーク上のトラフィック内で検出されたルーティング可能な IP アドレスの地理的発生源に関するデータを提供する機能。ジオロケーション データベース、接続イベント、侵入イベント、ファイル イベント、およびマルウェア イベントだけでなく、ホスト プロファイルに保存されたジオロケーション情報も表示できます。

シスコ VRT

シスコの脆弱性調査チーム。

シスコ インテリジェンス フィード

レピュテーションを下げるためにシスコ VRT によって決定される IP アドレスの定期更新リストのコレクション。フィード内の各リストは、特定のカテゴリ（オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）など）を表します。アクセス コントロール ポリシーでは、セキュリティ インテリジェンスを使用していずれかのカテゴリまたはすべてのカテゴリをブラックリストに追加できます。インテリジェンス フィードは定期的に更新されるため、それを使用することにより、システムは確実に最新情報を使用してネットワーク トラフィックをフィルタ処理できます。

シスコ クラウド

防御センターがマルウェア、セキュリティ インテリジェンス、URL フィルタリング データなどの最新の関連情報を入手可能な、*クラウド サービス*とも呼ばれる、シスコ ホステッド外部サーバ。マルウェア クラウド検索も参照してください。

システム ポリシー

メール中継ホスト プリファレンスや時刻同期設定などの、1 つの展開内の複数のアプライアンスと同様の設定。防御センターを使用して、システム ポリシーをそれ自体とその管理対象デバイスに適用します。

修復

システムに対する攻撃の可能性を軽減するアクション。修復を設定し、それらを相関ポリシー内で相関ルールとコンプライアンス ホワイト リストに関連付けることによって、トリガーされたときに防御センターで修復が起動されるようにできます。これにより、その場で解決できない攻撃を自動的に軽減するだけでなく、システムが組織のセキュリティ ポリシーに準拠していることを保証することもできます。防御センターには事前に定義された修復が付属していますが、柔軟な API を使用してカスタム修復を作成することもできます。

詳細設定

設定に特定の専門知識が必要なプリプロセッサ機能またはその他の侵入ポリシー機能。通常、詳細設定は、ほとんどまたはまったく変更を必要とせず、すべての展開に共通ではありません。

シリーズ 2

シスコ アプライアンス モデルの第 2 シリーズ。リソース、アーキテクチャ、およびライセンスの制限により、シリーズ 2 アプライアンスは、FireSIGHT システム機能の一部しかサポートしません。シリーズ 2 デバイスには、3D500、3D1000、3D2000、3D2100、3D2500、3D3500、3D4500、3D6500、および 3D9900 が含まれます。シリーズ 2 防御センターには、DC500、DC 1000、および DC 3000 が含まれます。

シリーズ 3

シスコ アプライアンス モデルの第 3 シリーズ。シリーズ 3 アプライアンスには、7000 シリーズと 8000 シリーズのデバイスだけでなく、DC750、DC1500、および DC3500 防御センターも含まれます。

侵入

ネットワーク上で発生したセキュリティ違反、攻撃、または悪用。

侵入イベント

侵入ポリシー違反を記録するイベント。侵入イベント データには、悪用の日付、時刻、および種類だけでなく、攻撃とそのターゲットに関するその他のコンテキスト情報も含まれます。

侵入検知および防御

ネットワーク トラフィックのセキュリティ ポリシー違反のモニタリングとインライン展開における悪意のあるトラフィックをブロックまたは変更できる能力。FireSIGHT システムでは、侵入ポリシーとアクセス コントロール ルールまたはデフォルト アクションを関連付けるときに侵入検知および防御を実行します。

侵入ポリシー

ネットワーク トラフィックの侵入とセキュリティ ポリシー違反を検査するように設定可能なさまざまなコンポーネント。これらのコンポーネントには、プロトコル ヘッダー値、ペイロードの内容、および特定のパケット サイズの特性を検査する侵入ルール、侵入ルールでよく使用される変数、FireSIGHT の推奨ルール設定、プリプロセッサやその他の検出およびパフォーマンス機能などの詳細設定、および関連するプリプロセッサ オプション用のイベントを生成可能なプリプロセッサ ルールが含まれます。ネットワーク トラフィックがアクセス コントロール ルールの条件を満たしている場合は、侵入ポリシーを使用してそのトラフィックを検査できます。侵入ポリシーとデフォルト アクションを関連付けることもできます。

侵入ルール

モニタ対象ネットワーク トラフィックに適用された場合に、潜在的な侵入、セキュリティ ポリシー違反、およびセキュリティ違反を特定するキーワードと引数のセット。システムはルール条件に基づいてパケットを比較します。パケット データが条件と一致すると、ルールがトリガーされ、侵入イベントが生成されます。侵入ルールにはドロップ ルールとパス ルールが含まれています。

スイッチド インターフェイス

レイヤ 2 展開でトラフィックを切り替えるために使用するインターフェイス。タグなし VLAN トラフィックを処理する物理スイッチド インターフェイスをセットアップすることも、VLAN タグが指定されたトラフィックを処理する論理スイッチド インターフェイスをセットアップすることもできます。

スイッチ

マルチポート ブリッジとして機能するネットワーク デバイス。ネットワーク検出を使用すれば、システムでスイッチがブリッジとして識別されます。加えて、管理対象デバイスを複数のネットワーク間でパケット スイッチングを実行する仮想スイッチとして設定できます。

スケジュールされたタスク

一度だけ実行するように、または、定期的に実行するようにスケジュール可能な管理タスク。

スタック構成

2 ～ 4 つの物理デバイスをスタック構成で接続することにより、ネットワーク セグメント上で検査するトラフィック量を増やすための機能。スタック構成を設定するときに、スタックする各デバイスのリソースを単一の共有構成に統合します。

スタック

検出リソースを共有する 2 ～ 4 つの接続されたデバイス。

脆弱性

ホストが被る可能性のある特定の侵害を指す表現。防御センターは、脆弱性がある各ホストの脆弱性に関する情報をホスト プロファイルで提供します。加えて、脆弱性ネットワーク マップを使用して、システムがモニタ対象ネットワーク全体で検出した脆弱性の全体図を入手できます。ホストが特定の侵害に対して脆弱ではなくなったと判断した場合は、特定の脆弱性を非アクティブにすることも、無効としてマークすることもできます。

脆弱性データベース

VDB とも呼ばれる、ホストが影響を受ける可能性のある既知の脆弱性のデータベース。システムは、各ホストで検出されたオペレーティング システム、アプリケーション プロトコル、およびクライアントと VDB を相互に関連づけることによって、特定のホストでネットワーク侵害のリスクが増大するかどうかを判断しやすくします。VDB 更新には、新しい脆弱性と更新された脆弱性だけでなく、新しいアプリケーション ディテクタと更新されたアプリケーション ディテクタも含まれます。

セキュリティ インテリジェンス フィード

システムが設定された間隔で定期的にダウンロードする IP アドレスの動的コレクションであるセキュリティ インテリジェンス オブジェクトの一種。フィードは定期的に更新されるため、それらを使用することにより、セキュリティ インテリジェンス機能で最新の情報を使用してネットワーク トラフィックがフィルタ処理されることが保証されます。シスコ インテリジェンス フィードも参照してください。

セキュリティ インテリジェンス リスト

セキュリティ インテリジェンス オブジェクトとして防御センターに手動でアップロードする IP アドレスの単純な静的コレクション。このリストは、セキュリティ インテリジェンス フィードだけでなく、グローバル ブラックリストとグローバル ホワイトリストも拡張または最適化するために使用します。

セキュリティ インテリジェンス

ソース IP アドレスまたは宛先 IP アドレスに基づいて、アクセス コントロール ポリシー単位でネットワークを通過可能なトラフィックを指定するための機能。これは、トラフィックがアクセス コントロール ルールによって分析される前に、特定の IP アドレスをブラックリストに追加する（そのアドレスからのまたはそのアドレスへのトラフィックを拒否する）場合に特に便利です。オプションで、セキュリティ インテリジェンス フィルタリング用のモニタ設定を使用できます。これにより、システムでブラックリストに追加された接続を分析できるようになりますが、ブラックリストと一致したものがログに記録されます。

セキュリティ ゾーン

さまざまなポリシーと設定でトラフィック フローを管理および分類するために使用可能な 1 つ以上のインライン、パッシブ、スイッチド、またはルーテッド インターフェイスのグループ分け。単一のゾーン内のインターフェイスで複数のデバイスをカバーできます。単一のデバイスに複数のセキュリティ ゾーンを設定することもできます。トラフィックを処理する前に、設定するそれぞれのインターフェイスをセキュリティ ゾーンに割り当てる必要があります。すべてのインターフェイスを 1 つのセキュリティ ゾーンに所属させることもできます。

セキュリティ ポリシー

ネットワークを保護するための組織のガイドライン。たとえば、セキュリティ ポリシーで、ワイヤレス アクセス ポイントの使用を禁止します。セキュリティ ポリシーにアクセプタブル ユース ポリシー（AUP）を含めることもできます。これにより、組織のシステムの使用方法に関するガイドラインが従業員に提供されます。

セキュリティ ポリシー違反

ネットワークのセキュリティ違反、攻撃、悪用、またはその他の不正使用。

接続

2 つのホスト間のモニタ対象セッション。アクセス コントロール ポリシー内の管理対象デバイスによって検出された接続をログに記録できます。ネットワーク検出ポリシーで NetMod 接続ロギングを設定します。

設定可能なバイパス

バイパス モードを設定可能なインライン セットの特性。

センシング インターフェイス

ネットワーク セグメントのモニタに使用されるデバイス上のネットワーク インターフェイス。管理インターフェイスと比較してください。

相関

ネットワーク上の脅威にリアルタイムに対処する相関ポリシーの作成に使用可能な機能。相関の修復コンポーネントは、ポリシー違反に対処するための独自のカスタム修復モジュールを作成してアップロードできる柔軟な API を提供します。

タスク キュー

アプライアンスが実行する必要のあるジョブのキュー。ポリシーを適用したり、ソフトウェア アップデートをインストールしたり、その他の長時間ジョブを実行したりすると、ジョブがキューに入れられ、そのステータスが [Task Status] ページに表示されます。[Task Status] ページには、ジョブの詳細なリストが表示され、10 秒ごとに再描画され、そのステータスが更新されます。

ダッシュボード ウィジェット

FireSIGHT システムの側面に対する理解を促す小型の自己完結型ダッシュボード コンポーネント。

ダッシュボード

システムによって収集または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 ステータスを一目で確認できるようにする表示。システムに付属のダッシュボードを増強するために、選択したダッシュボード ウィジェットにデータを設定したさまざまなカスタム ダッシュボードを作成できます。モニタ対象ネットワークの外観や動作に関する広範で簡略化されたカラフルな画像を提供する Context Explorer と比較してください。

タップ モード

各パケットのコピーが分析され、ネットワーク トラフィック フローはデバイスをパススルーせず妨害されない 3D9900 とシリーズ 3 デバイス上で使用可能な高度なインライン セット オプション。パケットそのものではなく、パケットのコピーが処理されるため、デバイスは、アクセス コントロール ポリシーと侵入ポリシーがトラフィックをドロップ、変更、またはブロックするように設定されていてもパケット ストリームに影響を与えることはできません。

データベース アクセス

サードパーティ製クライアントによる防御センター データベースへの読み取り専用アクセスを可能にする機能。

テーブル ビュー

イベント情報をデータベース テーブル内のフィールドごとに 1 列ずつ表示するワークフロー ページの一種。イベント分析を実行するときに、ドリルダウン ページを使用して調査するイベントを絞り込んでから、興味のあるイベントの詳細が表示されたテーブル ビューに移動することができます。テーブル ビューの多くは、システムに付属のワークフロー内の最後から 2 つ目のページです。

ディスカバリ ポリシー

ネットワーク検出ポリシーを参照してください。

ディスカバリ

管理対象デバイスを使用してネットワークをモニタし、ネットワークの完全で永続的なビューを提供する FireSIGHT システムのコンポーネント。ネットワーク検出によって、ネットワーク上のホスト（ネットワーク デバイスとモバイル デバイスを含む）の台数や種類だけでなく、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびオープン ポートに関する情報も特定されます。また、ネットワーク上のユーザ アクティビティをモニタするようにシスコ管理対象デバイスを設定して、ポリシー違反、攻撃、またはネットワークの脆弱性の原因を特定できるようにすることもできます。

適用

ポリシーまたはそれに対する変更を有効にするために実行するアクション。ほとんどのポリシーは防御センター から管理対象デバイスに適用されます。ただし、相関ポリシーは管理対象デバイスの設定への変更に関与しないため、ユーザがアクティブ化または非アクティブ化します。

デコーダ

スニファで取り込んだパケットをプリプロセッサによって理解可能な形式に置き換える侵入検知および防御のコンポーネント。

デバイス クラスタリング

クラスタリングを参照してください。

デバイス スタッキング

スタック構成を参照してください。

デバイス

さまざまなスループットで使用可能な、フォールトトレラント設計で特定用途向けのアプライアンス。デバイス上で有効にされたライセンス対象機能に応じて、それらを利用し、受動的にトラフィックをモニタしてネットワーク アセット、アプリケーション トラフィック、およびユーザ アクティビティの包括的マップを作成したり、侵入検知および防御を実行したり、アクセス制御を実行したり、スイッチングとルーティングを設定したりできます。防御センターを使用してデバイスを管理する必要があります。

デフォルト アクション

アクセス コントロール ポリシーの一部として、ポリシー内のルールの条件を満たさないトラフィックの処理方法を決定します。アクセス コントロール ルールもセキュリティ インテリジェンス設定も含まないアクセス コントロール ポリシーを適用した場合は、デフォルト ポリシー アクションによってネットワーク上の非ファストパス トラフィックの処理方法が決定されます。デフォルト アクションは、余分な検査を行わずにトラフィックをブロックまたは信頼するように設定したり、ネットワーク検出ポリシーまたは侵入ポリシーを使用してトラフィックを検査したりするように設定できます。

トランスペアレント インライン モード

デバイスを「Bump In The Wire」として機能させ、送信元と宛先に関係なく、それが認識するすべてのネットワーク トラフィックを転送可能にするための高度なインライン セット オプション。

ネットワーク デバイス

FireSIGHT システムで、ブリッジ、ルータ、NAT デバイス、または論理インターフェイスとして特定されたホスト。

ネットワーク ファイル トラジェクトリ

ホストがネットワーク経由でファイルを転送する場合のファイルのパスの視覚的表現。SHA-256 ハッシュ値が関連付けられたファイルの場合は、トラジェクトリ マップに、ファイルを転送したすべてのホストの IP アドレス、ファイルが検出された時刻、ファイルのマルウェア処理、関連するファイル イベント、マルウェア イベントなどが表示されます。

ネットワーク マップ

ネットワークの詳細な表現。ネットワーク マップを使用すれば、ネットワーク上で実行中のホスト、モバイル デバイス、およびネットワーク デバイスの観点だけでなく、関連するホスト属性、アプリケーション プロトコル、および脆弱性の観点でもネットワーク トポロジを表示できます。

ネットワーク検出

ディスカバリを参照してください。

ネットワーク検出ポリシー

NetMod 対応デバイスによってモニタされたネットワークを含む特定のネットワーク セグメントに対してシステムが収集するディスカバリ ポリシーの種類（ホスト、ユーザ、およびアプリケーション データなど）を指定するポリシー。ネットワーク検出ポリシーは、インポート解決プリファレンスとアクティブ検出ソース プライオリティも管理します。

バーチャル デバイス

仮想ホスティング環境内の独自の設備に展開可能な管理対象デバイス。バーチャル デバイスを仮想スイッチまたは仮想ルータとして設定することはできません。

ハイ アベイラビリティ

デバイスのグループを管理するように冗長な物理 防御センター を設定するための機能。イベント データは管理対象デバイスから両方の 防御センター に流れ、ほとんどの設定要素が両方の 防御センター 上で維持されます。プライマリ 防御センター で障害が発生した場合は、セカ

ンダリ 防御センター を使用して中断せずにネットワークをモニタできます。冗長なデバイスを指定可能なクラスタリングと比較してください。

バイパス モード

何らかの理由でセット内のセンシング インターフェイスで障害が発生した場合にトラフィックの流れを維持できるようにするインライン セットの特性。

ハイブリッド インターフェイス

システムで仮想ルータと仮想スイッチ間のトラフィックをブリッジするための管理対象デバイス上の論理インターフェイス。

パッシブ インターフェイス

パッシブ展開でトラフィックを分析するように設定されたセンシング インターフェイス。

パッシブ検出

管理対象デバイスによって受動的に収集されたトラフィックの分析を通したディスカバリ ポリシーのコレクション。アクティブ検出と比較してください。

非バイパス モード

何らかの理由でセット内のセンシング インターフェイスで障害が発生した場合にトラフィックをブロックするインライン セットの特性。

ファイル タイプ

PDF、EXE、MP3 などのファイル形式の特定の種類。

ファイル トラジェクトリ

ネットワーク ファイル トラジェクトリを参照してください。

ファイル ポリシー

システムがファイル制御と高度なマルウェア対策を実行するために使用するポリシー。ファイル ルールによって生成されたファイル ポリシーは、アクセス コントロール ポリシー内のアクセス コントロール ルールから呼び出されます。

ファイル制御

アクセス制御の一部として、ネットワークを通過可能なファイルの種類を指定してログに記録するための機能。

ファストパス ルール

分析する必要のないトラフィックに処理のバイパスを許可するため、限定的な条件を使用して、デバイスのハードウェア レベルで設定するルール。

フィード

セキュリティ インテリジェンス フィードを参照してください。

物理インターフェイス

NetMod 上の物理ポートを表すインターフェイス。

プリプロセッサ ルール

プリプロセッサまたはポートスキャン フロー ディテクタに関連付けられた侵入ルール。プリプロセッサ ルールでイベントを生成する場合は、そのルールを有効にする必要があります。プリプロセッサ ルールには、プリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。

プリプロセッサ

侵入ポリシーによって検査されるトラフィックを正規化し、不適切なヘッダー オプションの識別、IP データグラムの最適化、TCP ステートフル インスペクションとストリーム リアセンブルの提供、およびチェックサムの確認によるネットワーク層とトランスポート層のプロトコル異常の特定を支援する機能。プリプロセッサは、特定の種類のパケット データをシステムで分析可能な形式で表現できます。このようなプリプロセッサは、データ正規化プリプロセッサまたはアプリケーション層プロトコル プリプロセッサと呼ばれます。アプリケーション層プロトコルのエンコーディングを正規化すれば、データが別の方法で表現されるパケットに同じコンテンツ関連侵入ルールを効率的に適用し、意味のある結果を得ることができます。プリプロセッサは、パケットが設定されたプリプロセッサ オプションをトリガーするたびにプリプロセッサ ルールを生成します。

ヘルス ポリシー

展開内のアプライアンスのヘルスをチェックするときに使用される基準。ヘルス ポリシーは、ヘルス モジュールを使用して、FireSIGHT システム のハードウェアとソフトウェアが正しく動作しているかどうかを示します。デフォルトのヘルス ポリシーを使用することも、独自のものを作成することもできます。

ヘルス モジュール

展開内のアプライアンスの CPU 使用率や空きディスク領域などの特定の性能的側面のテスト。ユーザがヘルス ポリシーで有効にするヘルス モジュールは、モニタしている性能的側面が特定のレベルに達したときにヘルス イベントを生成します。

ヘルス モニタ

展開内のアプライアンスのパフォーマンスを継続的にモニタする機能。ヘルス モニタは、適用されたヘルス ポリシー内のヘルス モジュールを使用してアプライアンスをテストします。

防御センター

デバイスを管理し、それらが生成したイベントを自動的に集約して関連付けるための集中管理点。

保護されたネットワーク

ファイアウォールなどのデバイスによって他のネットワーク ユーザから保護された組織の内部ネットワーク。FireSIGHT システムを使用して配信される侵入ルールの多くは、保護されたネットワークと保護されていない（または外部の）ネットワークを定義する変数を使用します。

ホスト

ネットワークに接続され、一意の IP アドレスが割り当てられたデバイス。FireSIGHT システムにとって、ホストは、モバイル デバイス、ブリッジ、ルータ、NAT デバイス、または論理インターフェイスとして分類されない特定のホストです。

ホスト入力

スクリプトまたはコマンドライン ファイルを使用してサードパーティ ソースからデータをインポートしてネットワーク マップ内の情報を拡張するための機能。この Web インターフェイスはいくつかのホスト入力機能も提供します。オペレーティング システムまたはアプリケーション プロトコル ID を変更したり、脆弱性を有効または無効にしたり、クライアント ポートとサーバ ポートを含むネットワーク マップからさまざまな項目を削除したりできます。

ポリシー

アプライアンスに最も頻繁に設定を適用するためのメカニズム。アクセス コントロール ポリシー、相関ポリシー、ファイル ポリシー、ヘルス ポリシー、侵入ポリシー、ネットワーク検出ポリシー、およびシステム ポリシーを参照してください。

マルウェア イベント

シスコの高度なマルウェア対策ソリューションのいずれかによって生成されるイベント。ネットワークベースのマルウェア イベントは、シスコ クラウドがネットワーク トラフィック内で検出されたファイルのマルウェア処理を戻したときに生成されます。その処理が変化すると、遡及的なマルウェア イベントが生成されます。展開された FireAMP Connector が脅威を検出したり、マルウェアの実行をブロックしたり、マルウェアを検疫したり、マルウェアの検疫に失敗したりした場合に生成されるエンドポイント ベースのマルウェア イベントと比較してください。

マルウェア クラウド検索

防御センターがシスコ クラウドと通信して、ファイルの SHA-256 ハッシュ値に基づいてネットワーク トラフィック内で検出されたファイルのマルウェア処理を決定するプロセス。

マルウェア ブロッキング

シスコのネットワークベースの高度なマルウェア対策（AMP）ソリューションのコンポーネント。マルウェア検出 が検出されたファイルのマルウェア処理を完了したら、そのファイルをブロックすることも、そのアップロードまたはダウンロードを許可することもできます。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

マルウェア ライセンス

ネットワーク トラフィック内の高度なマルウェア対策（AMP）を実行するためのライセンス。ファイル ポリシーを使用すれば、管理対象デバイスによって検出された特定のファイル タイプに対してマルウェア クラウド検索を実行するようにシステムを設定できます。FireAMP サブスクリプションと比較してください。

マルウェア対策

高度なマルウェア対策を参照してください。

マルウェア検出

シスコのネットワークベースの高度なマルウェア対策（AMP）ソリューションのコンポーネント。ネットワーク トラフィックを検査する全体的なアクセス制御設定の一部として管理対象デバイスに適用されるファイル ポリシー。その後で、防御センターは検出された特定のファイル タイプのマルウェア クラウド検索を実行し、ファイルのマルウェア処理をユーザに警告するイベントを生成します。続けて AMP マルウェア ブロッキングが実行されて、ファイルをブロックするか、そのアップロードまたはダウンロードを許可します。この機能を FireAMP サブスクリプションが必要なシスコのエンドポイント ベースの AMP ツールである FireAMP と比較してください。

モニタ

アクセス コントロール ポリシーで、セキュリティ インテリジェンス ブラックリストまたはアクセス コントロール ルールと一致するトラフィックをログに記録するが、システムにはトラフィックを即座に許可またはブロックするのではなく、評価を継続させる方法。

モバイル デバイス

FireSIGHT システムで、ディスカバリ機能によって可搬型のハンドヘルド デバイス（携帯電話やタブレットなど）として特定されたホスト。多くの場合、システムは、モバイル デバイスがジェイルブレイクされているかどうかを検出できます。

ユーザ アクティビティ

システムがユーザ ログイン（オプションで、失敗したログイン試行を含む）または防御センター データベースに対するユーザ レコードの追加または削除を検出したときに生成されるイベント。

ユーザ エージェント

ユーザがネットワークにログインするとき、または、その他の理由で Active Directory クレデンシャルに対して認証されるときにそのユーザをモニタするため、サーバにインストールするエージェント。アクセス制御ユーザのユーザ アクティビティは、ユーザ エージェントから報告されるときにだけアクセス制御に使用されます。

ユーザ ロール

FireSIGHT システムのユーザに付与されるアクセス レベル。たとえば、イベント アナリスト、FireSIGHT システムを管理している管理者、サードパーティ製ツールを使用して防御センター データベースにアクセスしているユーザなどのための Web インターフェイスにさまざまなアクセス権限を付与することができます。特殊なアクセス権限を持つカスタム ロールを作成することもできます。

ユーザ

ネットワーク アクティビティが管理対象デバイスまたはユーザ エージェントによって検出されたユーザ。

ユーザ認識

組織で脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けたり、ユーザにユーザ制御の実行を許可したりするための機能。

ユーザ制御

アクセス制御の一部として、ネットワークに出入りしたり、ネットワーク内部を移動したりするユーザ関連トラフィックを指定してログに記録するための機能。

リスト

セキュリティ インテリジェンス リストを参照してください。

リンク ステート伝達

インライン セット内のどちらかのインターフェイスがダウンしたときに自動的にペア内の 2 つ目のインターフェイスをダウンさせるバイパス モードのインライン セットのオプション。ダウンしたインターフェイスが復旧すると、2 つ目のインターフェイスも自動的に復旧します。つまり、ペア化されたインターフェイスのリンク ステートが変化すると、それに合わせてもう一方のインターフェイスのリンク ステートが自動的に変化します。

ルータ

ネットワーク間でパケットを転送する、ゲートウェイに配置されたネットワーク デバイス。ネットワーク検出を使用すれば、システムでルータを識別できます。加えて、管理対象デバイスを、複数のインターフェイス間でトラフィックをルーティングする仮想ルータとして設定できます。

ルーテッド インターフェイス

レイヤ 3 展開でトラフィックをルーティングするインターフェイス。タグなし VLAN トラフィックを処理する物理ルーテッド インターフェイスをセットアップすることも、VLAN タグが指定されたトラフィックを処理する論理ルーテッド インターフェイスをセットアップすることもできます。また、静的なアドレス解決プロトコル（ARP）エントリをルーテッド インターフェイスに追加することもできます。

ルール アクション

ルールの条件を満たすネットワーク トラフィックの処理方法を指定した設定。アクセス コントロール ルール アクションとファイル ルール アクションを参照してください。

ルール

ネットワーク トラフィックの検査基準を提供する、通常はポリシー内にある構造。

ルール更新

必要に応じて、新しいまたは更新された標準テキストのルール、共有オブジェクトのルール、およびプリプロセッサ ルールを含む侵入ルールの更新。ルール更新では、ルールの削除、デフォルト侵入ポリシー設定の変更、およびシステム変数とルール カテゴリの追加または削除が行われる場合があります。

ルール状態

侵入ポリシー内の侵入ルールが有効になっている（[Generate Events] または [Drop and Generate Events] に設定されている）か、無効になっている（[Disable] に設定されている）か。ルールを有効にした場合は、ネットワーク トラフィックの評価に使用されます。ルールを無効にした場合は、使用されません。

レイヤ

侵入ポリシー内の侵入ルール、プリプロセッサ ルール、および詳細設定構成の完全なセット。ポリシー内の組み込みレイヤにカスタム ユーザ レイヤを追加できます。侵入ポリシー内の上位レイヤの設定が下位レイヤの設定より優先されます。

レピュテーション（IP アドレス）

セキュリティ インテリジェンスを参照してください。

論理インターフェイス

タグ付きトラフィックが物理インターフェイスを通過したときに特定の VLAN タグ付きトラフィックを処理するように定義された仮想サブインターフェイス。