コンテキスト エクスプローラの使用

以下のトピックでは、Firepower システムでコンテキスト エクスプローラを使用する方法について説明します。

コンテキスト エクスプローラについて

Firepower システムの Context Explorer には、モニタ対象ネットワークのステータスに関するコンテキストでの詳細でインタラクティブなグラフィカル情報が表示されます。これには、アプリケーション、アプリケーション統計、接続、位置情報、侵害の兆候、侵入イベント、ホスト、サーバ、セキュリティ インテリジェンス、ユーザ、ファイル（マルウェア ファイルを含む）、関連 URL に関するデータが含まれます。各セクションには、このデータが鮮やかな色の折れ線グラフ、棒グラフ、円グラフ、ドーナツ グラフの形式で表示され、グラフとともに詳しいリストが示されます。1 番目のセクションに表示される時間の経過に伴うトラフィックとイベント数の変化を示した折れ線グラフは、ネットワークのアクティビティにおける最近の傾向の概要を示します。

分析を細かく調整するためのカスタム フィルタを容易に作成および適用できます。またグラフ エリアをクリックするか、カーソルをグラフ エリアに置くことでデータ セクションを詳しく調べることができます。過去 1 時間から過去 1 年までの期間を反映するように Explorer の時間範囲を設定することもできます。Context Explorer にアクセスできるユーザは、管理者、セキュリティ アナリスト、またはセキュリティ アナリスト（読み取り専用）のユーザ ロールが割り当てられているユーザだけです。

Firepower システムのダッシュボードは細かくカスタマイズすることができます。このダッシュボードは区分化されており、リアルタイムで更新されます。一方、Context Explorer は手動で更新され、より幅広いデータのコンテキストを提供することを目的としており、アクティブなユーザ操作のために単一で一貫性のあるレイアウトを備えています。

特定のニーズに基づいてネットワークとアプライアンスのリアルタイムのアクティビティをモニタするには、ダッシュボードを使用します。逆に、詳細かつ明確なコンテキストで事前に定義されている最新のデータ セットを調査するには、Context Explorer を使用します。たとえば、ネットワークのホストのうち Linux を使用しているホストは 15% であるが、ほぼすべての YouTube トラフィックはこれらのホストによるものであることが判明した場合、Linux ホストのデータのみを表示するフィルタ、YouTube 関連のアプリケーション データのみを表示するフィルタ、あるいはこの両方のフィルタを簡単に適用できます。コンパクトで対象が絞り込まれているダッシュボード ウィジェットとは異なり、Context Explorer の各セクションは、Firepower システムの専門知識を持つユーザと一般的なユーザの両方に役立つ形式で、システム アクティビティを鮮明なビジュアル表現で提供します。

表示されるデータは、管理対象デバイスのライセンスおよび導入状況や、そのデータを提供する機能を設定しているかどうかによって異なります。また、Context Explorer のすべてのセクションで、フィルタを適用して表示するデータを制限することもできます。

マルチドメイン導入では、先祖ドメインで Context Explorer を表示すると、すべてのサブドメインからの集約データが表示されます。リーフ ドメインでは、そのドメインに固有のデータだけを表示できます。

ダッシュボードと Context Explorer の違い

次の表に、ダッシュボードと Context Explorer の主な相違点の要約を示します。

表 *1 :* 比較：ダッシュボードと *Context Explorer*

機能	ダッシュボード	コンテキスト エクスプローラ（Context Explorer）
表示可能なデータ	Firepower システムによってモニタされる任意の対象	アプリケーション、アプリケーション統計、位置情報、ホストの侵害の兆候、侵入イベント、ファイル（マルウェア ファイルを含む）、ホスト、セキュリティ インテリジェンス イベント、サーバ、ユーザ、および URL
カスタマイズ可能かどうか	• ダッシュボードで選択されているウィジェットはカスタマイズ可能です • 個々のウィジェットはさまざまなレベルでカスタマイズ可能です	• 基本レイアウトは変更できません • 適用されたフィルタは Explorer URL に示され、後で使用するためにブックマークできます
データの更新頻度	自動（デフォルト）、ユーザ設定	手動（Manual）
データのフィルタリング	一部のウィジェットで可能です（ウィジェット設定を編集する必要があります）	Explorer のすべての部分で可能であり、複数フィルタに対応しています

機能	ダッシュボード	コンテキストエクスプローラ（Context Explorer）
グラフィカル コンテキスト	一部のウィジェット（特にカスタム分析（Custom Analysis））では、データをグラフ形式で表示できます	すべてのデータの豊富なグラフィカル コンテキスト（独自の詳細なドーナツ グラフを含む）
関連 Web インターフェイス ページへのリンク	一部のウィジェット	すべてのセクション
表示データの時間範囲	ユーザ設定	ユーザ設定

関連トピック

ダッシュボードについて

[時系列のトラフィックおよび侵入イベント数（TrafficandIntrusionEvent Counts Time）] グラフ

Context Explorer の上部には、時間の経過に伴うトラフィックおよび侵入イベント数の変化を示す折れ線グラフが表示されます。X 軸は時間間隔を示します（選択されている時間枠に応じて、5 分～ 1 か月の範囲）。Y 軸は、KB 単位のトラフィック（青色の線）と侵入イベント数（赤色の線）を示します。

X 軸の最小間隔が 5 分であることに注意してください。これに対応するため、選択された時間範囲の開始点と終了点が、システムにより、最も近い 5 分間間隔に調整されます。

このセクションには、デフォルトでは選択された時間範囲のすべてのネットワーク トラフィックと、生成されたすべての侵入イベントが示されます。フィルタを適用すると、フィルタに指定されている条件に関連するトラフィックと侵入イベントだけがグラフに表示されます。たとえば、[OS 名（OS Name）] に `Windows` を指定してフィルタリングすると、時間グラフには Windows オペレーティング システムを使用するホストに関連するトラフィックとイベントだけが表示されます。

侵入イベント データ（[優先順位（Priority）] が `High` に設定されたものなど）に基づいて Context Explorer をフィルタ処理すると、青色のトラフィックを示す線が非表示になり、侵入イベントだけにより焦点を当てることができます。

トラフィックとイベント数に関する正確な情報を表示するには、グラフの線上の任意のポイントにポインタを置きます。また、色付きの線の 1 つにポインタを置くと、その線がグラフの前面に移動し、コンテキストがより明確になります。

このセクションのデータは、主に [侵入イベント（Intrusion Events）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

[侵害の兆候（Indications of Compromise）] セクション

コンテキスト エクスプローラの [侵害の兆候（IOC）（Indications of Compromise (IOC)）] セクションには、モニタ対象ネットワーク上でセキュリティが侵害されている可能性があるホストの概要を示す 2 つのインタライクティブ セクション（トリガーとして使用された主な IOC 種類の割合のビューと、トリガーとして使用された兆候の数をホストごとに表したビュー）が表示されます。

[兆候別ホスト（Hosts by Indication）] グラフ

[兆候別ホスト（Hosts by Indication）] グラフはドーナツ形式であり、モニタ対象ネットワーク上のホストでトリガーとして使用された侵害の兆候（IOC）を割合で表示します。内側のリングは IOC カテゴリ（[CnC 接続（CnC Connected）] や [マルウェア検出（Malware Detected）] など）ごとに分割されており、外側のリングではそれがさらに具体的なイベントの種類（[影響 2 侵入イベント - 管理者として試行（Impact 2 Intrusion Event — attempted-admin）] や [ファイル転送中に脅威を検出（Threat Detected in File Transfer）] など）ごとに分割されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ホスト別兆候（Indications by Host）] グラフ

[ホスト別兆候（Indications by Host）] グラフは棒グラフ形式であり、モニタ対象ネットワーク上の最も IOC が顕著な 15 のホストでトリガーとして使用された固有の侵害の兆候（IOC）の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [ホスト（Hosts）] テーブルと [ホスト侵害の兆候（Indications of Compromise）] テーブルから取得されます。

[ネットワーク情報（Network Information）] セクション

Context Explorer の [ネットワーク情報（Network Information）] セクションには、モニタ対象ネットワーク上の接続トラフィックの全体の概要（トラフィックに関連付けられている送信元、宛先、ユーザ、およびセキュリティ ゾーン、ネットワーク上のホストで使用されているオペレーティング システムの内訳、Firepower システムがネットワーク トラフィックに対して実行したアクセス制御アクションの割合のビュー）を示す6つのインタラクティブ グラフが含まれています。

[オペレーティング システム（Operating Systems）] グラフ

[オペレーティング システム（Operating Systems）] グラフはドーナツ グラフ形式で、モニタ対象ネットワークのホストで検出されたオペレーティング システムを割合で表示します。内側の

リングは OS 名（Windows や Linux など）ごとに分割され、外側のリングではそのデータがさらにオペレーティング システムのバージョン（Windows Server 2008 や Linux 11.x など）ごとに分割されています。密接に関連するいくつかのオペレーティング システム（Windows 2000、Windows XP、Windows Server 2003 など）は 1 つにまとめられます。ごくまれにしか使用されないオペレーティング システムや認識されないオペレーティング システムは[その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [ホスト（Hosts）] テーブルから取得されます。

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフ

[送信元 IP 別トラフィック（Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元IP別トラフィック（Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフ

[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の送信元ユーザのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた送信元IPアドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフ

[アクセス コントロール アクション別の接続（Connections by Access Control Action）] グラフは円グラフ形式であり、Firepower システム導入でモニタ対象トラフィックに対して実行されたアクセス制御アクション（[ブロック（Block）] や [許可（Allow）] など）の割合のビューを表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元ユーザ別トラフィック（Traffic by Source User）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフ

[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最もアクティブな上位 15 の宛先 IP アドレスのネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた宛先 IP アドレスごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別トラフィック（Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[入力/出力のセキュリティ ゾーン別トラフィック（TrafficbyIngress/EgressSecurityZone）] グラフ

[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは棒グラフ形式で、モニタ対象ネットワークで設定されているセキュリティ ゾーンごとに、その着信/発信ネットワーク トラフィック カウント（KB/秒）および固有接続数を表示します。このグラフは、必要に応じて、入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

リストされたセキュリティ ゾーンごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、出力セキュリティゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されたトグルボタンの [出力（Egress）] をクリックします。デフォルトのビューに戻すには、[入力（Ingress）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [入力（Ingress）] ビューに戻ります。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[入力/出力のセキュリティ ゾーン別トラフィック（Traffic by Ingress/Egress Security Zone）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルから取得されます。

[アプリケーション情報（Information）] セクション

Context Explorer の [アプリケーション情報（Information）] セクションには、3 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワーク上でのアプリケーションアクティビティの概要（アプリケーションに関連するトラフィック、侵入イベント、およびホストを、各アプリケーションに割り当てられている推定リスクまたは推定ビジネス関連度ごとに編成したもの）を示します。[アプリケーション詳細リスト（Application Details List）] は、各アプリケーションとそのリスク、ビジネス関連度、カテゴリ、ホスト数を示すインタラクティブなリストです。

このセクションのすべての「アプリケーション」インスタンスについて、[アプリケーション情報（Application Information）] のグラフのセットは、デフォルトでは特にアプリケーション プロトコル（DNS、SSH など）を検査します。クライアント アプリケーション（PuTTY や Firefox など）や Web アプリケーション（Facebook や Pandora など）を特に検査するように [アプリケーション情報（Application Information）] セクションを設定することもできます。

[アプリケーション情報（Application Information）] セクションへのフォーカスの移動

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1　**[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]** を選択します。

ステップ 2 [アプリケーション プロトコル情報（Application Protocol Information）] セクションにポインタを重ねます。

（注） 以前に同じ Context Explorer セッションでこの設定を変更している場合は、セクション タイトルが [クライアント アプリケーション情報（Client Application Information）] または [Web アプリケーション情報（Web Application Information）] と表示されることがある点に注意してください。

ステップ 3 [アプリケーションプロトコル（Application Protocol）]、[クライアントアプリケーション（Client Application）]、または [Web アプリケーション（Web Application）] をクリックします。

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（TrafficbyRisk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフはドーナツ形式で、モニタ対象ネットワークで検出されたアプリケーション トラフィックを、アプリケーションの推定リスク（デフォルト）または推定のビジネスとの関連性（ビジネス関連度）ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル（`Medium` や `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` や `NetBIOS` など）ごとに分割されます。まれにしか検出されないアプリケーションは [その他（Other）] にまとめられます。

このグラフは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Context Explorer の時間範囲を変更しても、グラフは変化しません。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとにトラフィックが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [Business Relevance] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [リスク（Risk）] ビューに戻ります。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[リスク/ビジネスとの関連性とアプリケーション別トラフィック（Traffic by Risk/Business Relevance and Application）] グラフは非表示になります。

このグラフのデータは、主に [接続イベント（Connection Events）] テーブルと [アプリケーション統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別侵入イベントおよびアプリケーション（Intrusion Events by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出された侵入イベントと、これらのイベントに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定のリスクまたはビジネスとの関連性レベル（`Medium` や `High` など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（`SSH` や `NetBIOS` など）ごとに分割されます。稀に検出されるアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされるか、または（該当する場合には）アプリケーション情報が表示されます。

ヒント グラフに制約を適用して、ビジネスとの関連性とアプリケーションごとに侵入イベントが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [アプリケーションの統計（Application Statistics）] テーブルから取得されます。

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフ

[リスク/ビジネスとの関連度別ホストおよびアプリケーション（Hosts by Risk/Business Relevance and Application）] グラフはドーナツ形式であり、モニタ対象ネットワークで検出されたホストと、これらのホストに関連するアプリケーションを、アプリケーションの推定リスク（デフォルト）または推定ビジネス関連度ごとの割合で表示します。内側のリングは推定リスク/ビジネス関連度レベル（[中（Medium）] または [高（High）] など）ごとに分割され、外側のリングではそのデータがさらに具体的なアプリケーション（[SSH] または [NetBIOS] など）ごとに分割されます。非常に少数のアプリケーションは [その他（Other）] にまとめられます。

ドーナツ グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント グラフに制約を適用して、ビジネスとの関連性とアプリケーションに基づいてホストが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [ビジネスとの関連性（Business Relevance）] をクリックします。デフォルト ビューに戻すには [リスク（Risk）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [リスク（Risk）] ビューに戻ることに注意してください。

このグラフのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

アプリケーション詳細リスト

[アプリケーション情報（Application Information）] セクション下部に表示される [アプリケーション詳細リスト（Application Details List）] は、モニタ対象ネットワークで検出される各アプリケーションの推定リスク、推定ビジネス関連度、カテゴリ、ホスト数の情報を示す表です。アプリケーションは、関連ホスト数の降順でリストされます。

[アプリケーション詳細リスト（Application Details List）] テーブルをソートすることはできませんが、テーブル内の項目をクリックして、その情報でフィルタリングまたはドリルダウンしたり、（該当する場合に）アプリケーション情報を表示したりすることができます。このテーブルのデータは主に [アプリケーション（Applications）] テーブルから取得されます。

このリストは日時制約に関係なく、使用可能なすべてのデータを反映することに注意してください。Explorer の時間範囲を変更しても、リストは変化しません。

[セキュリティ インテリジェンス（Security Intelligence）] セクション

Context Explorer の [セキュリティ インテリジェンス（Security Intelligence）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上の、ブラックリストに登録されているトラフィック、または Security Intelligence によってモニタされているトラフィックの全体の概要が示されます。これらのグラフでは、カテゴリ、送信元 IP アドレス、および宛先 IP アドレスに基づいてそれらのトラフィックがソートされ、トラフィックの量（KB/秒）と該当する接続の数の両方が表示されます。

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフ

[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上のトラフィックのセキュリティインテリジェンスの上位のカテゴリに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[カテゴリ別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Category）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフ

[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の送信元 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[送信元 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Source IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフ

[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは棒グラフ形式で、モニタ対象ネットワーク上でセキュリティ インテリジェンスによってモニタされたトラフィックの上位の宛先 IP アドレスに関する、ネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたカテゴリごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[宛先 IP 別セキュリティ インテリジェンス トラフィック（Security Intelligence Traffic by Destination IP）] グラフは非表示になります。

このグラフのデータは主に [セキュリティ インテリジェンス イベント（Security Intelligence Events）] テーブルから取得されます。

[侵入情報（Intrusion Information）] セクション

Context Explorer の [侵入情報（Intrusion Information）] セクションには 6 つのインタラクティブ グラフと 1 つの表形式リストが表示されます。これらのグラフとリストは、モニタ対象ネットワークの侵入イベントの概要（侵入イベントに関連付けられている影響レベル、攻撃元、攻撃対象先、ユーザ、優先レベル、およびセキュリティ ゾーンと、侵入イベントの分類、優先度、カウントを示す詳細なリスト）を示します。

[影響別侵入イベント（Intrusion Events by Impact）] グラフ

[影響別侵入イベント（Intrusion Events by Impact）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを推定影響レベル（0～4）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルと [IDS 統計情報（IDS Statistics）] テーブルから取得されます。

[上位の攻撃者（Top Attackers）] グラフ

[上位の攻撃者（Top Attackers）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた）上位の各攻撃元ホストIPアドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のユーザ（Top Users）] グラフ

[上位のユーザ（Top Users）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最大侵入イベント数に関連付けられたユーザと、イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [IDS のユーザ統計（IDS User Statistics）] テーブルと [侵入イベント（Intrusion Events）] テーブルから取得されます。このグラフには、権限のあるユーザのデータが表示されます。

[優先度別侵入イベント（Intrusion Events by Priority）] グラフ

[優先度別侵入イベント（Intrusion Events by Priority）] グラフは円グラフ形式であり、モニタ対象ネットワークの侵入イベントを、推定優先度レベル（[高（High）]、[中（Medium）]、[低（Low）] など）のグループごとの割合で表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[上位のターゲット（Top Targets）] グラフ

[上位のターゲット（Top Targets）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の（侵入イベントを発生させた接続で攻撃対象となった）上位のターゲットホスト（攻撃対象ホスト）の IP アドレスの侵入イベント数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフ

[入力/出力の上位セキュリティ ゾーン（Top Ingress/Egress Security Zones）] グラフは棒グラフ形式で、モニタ対象ネットワーク上で設定されている各セキュリティ ゾーン（グラフ設定に応じて入力または出力）に関連付けられている侵入イベントの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、出力セキュリティ ゾーンのトラフィックだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [出力（Egress）] をクリックします。デフォルトのビューに戻すには、[入力（Ingress）] をクリックします。このグラフは、Context Explorer から外部へ移動しても、デフォルトの [入力（Ingress）] ビューに戻ります。

このグラフのデータは、主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

このグラフは、必要に応じて、入力（デフォルト）セキュリティ ゾーン情報または出力セキュリティ ゾーン情報のいずれかを表示するように設定できます。

侵入イベント詳細リスト

[侵入情報（Intrusion Information）] セクション下部に表示される [イベント詳細リスト（Event Details List）] は、モニタ対象ネットワークで検出された各侵入イベントの分類、推定優先度、イベント数の情報を示すテーブルです。イベントは、イベント数の降順でリストされます。

[イベント詳細リスト（Event Details List）] テーブルはソートできませんが、テーブルの項目をクリックして、その情報でフィルタリングまたはドリルダウンすることができます。このテーブルのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[ファイル情報（Files Information）] セクション

Context Explorer の [ファイル情報（Files Information）] セクションには、6 つのインタラクティブ グラフが表示されます。これらのグラフは、モニタ対象ネットワーク上のファイルとマルウェア イベントの概要を示します。

このうち 5 つのグラフには、AMP for Firepower データ（ネットワーク トラフィックで検出されたファイルのファイル タイプ、ファイル名、マルウェアの性質、これらのファイルを送信（アップロード）および受信（ダウンロード）したホスト）が表示されます。最後のグラフには、AMP for Firepower または AMP for Endpoints のどちらで検出されたかにかかわらず、組織内で検出されたすべてのマルウェア脅威が表示されます。

（注）　侵入情報でフィルタリングすると、[ファイル情報（File Information）] セクション全体が非表示になります。

[上位のファイル タイプ（Top File Types）] グラフ

[上位のファイル タイプ（Top File Types）] グラフはドーナツ グラフ形式で、ネットワーク トラフィックで検出されたファイル タイプの割合のビュー（外側のリング）と、ファイル カテゴリのグループごとの割合のビュー（内側のリング）を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[上位のファイル名（Top File Names）] グラフ

[上位のファイル名（Top File Names）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された上位の一意のファイル名の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[性質別ファイル（Files by Disposition）] グラフ

[性質別ファイル（Files by Disposition）] グラフは円グラフ形式であり、AMP for Firepower で検出されたファイルのマルウェアの性質の割合のビューを表示します。Firepower Management Center がマルウェア クラウド検索を行ったファイルにのみ性質が設定されることに注意してください。クラウド検索をトリガーしなかったファイルには、`N/A` という性質が設定されます。`Unavailable` という性質は、Firepower Management Center がマルウェア クラウド検索を実行できなかったことを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[送信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、送信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを送信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには、[ファイル（Files）] をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフ

[受信ファイル数上位のホスト（Top Hosts Receiving Files）] グラフは棒グラフ形式で、ネットワーク トラフィックで検出された、受信ファイル数上位のホストの IP アドレスに関するファイルの数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

ヒント　グラフに制約を適用して、マルウェアを受信したホストだけが表示されるようにするには、グラフにポインタを置き、表示されたトグル ボタンの [マルウェア（Malware）] をクリックします。デフォルトのファイルのビューに戻すには、[ファイル（Files）] をクリックします。このグラフは、Context Explorer から外部へ移動してもデフォルトのファイルのビューに戻ります。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルから取得されます。

[上位のマルウェア検出（Top Malware Detections）] グラフ

[上位のマルウェア検出（Top Malware Detections）] グラフは棒グラフ形式で、AMP for Firepower と AMP for Endpoints のいずれによるものかに関係なく、組織で検出された上位のマルウェア脅威の数を表示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタ処理またはドリル ダウンが実行されます。

このグラフで AMP for Firepower のデータを表示するには、マルウェアのライセンスを持っている必要があることに注意してください。

このグラフのデータは、主に [ファイル イベント（File Events）] テーブルと [マルウェア イベント（Malware Events）] テーブルから取得されます。

[地理位置情報（Geolocation Information）] セクション

Context Explorer の [地理位置情報（Geolocation Information）] セクションには、3 つのインタラクティブなドーナツ グラフが表示されます。これらのグラフは、モニタ対象ネットワークのホストがデータを交換している国の概要（イニシエータ国またはレスポンダ国ごとの固有接続数、送信元または宛先の国ごとの侵入イベント数、および送信側または受信側の国ごとのファイル イベント数）を示します。

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフの表示

[イニシエータ/レスポンダの国別接続（Connections by Initiator/Responder Country）] グラフはドーナツ グラフ形式であり、ネットワーク上での接続にイニシエータ（デフォルト）またはレスポンダとして関わる国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、接続でレスポンダとなっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [レスポンダ（Responder）] をクリックします。デフォルト ビューに戻すには [イニシエータ（Initiator）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [イニシエータ（Initiator）] ビューに戻ることに注意してください。

このグラフのデータは主に [接続サマリー データ（Connection Summary Data）] テーブルから取得されます。

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフ

[送信元/宛先国別侵入イベント（Intrusion Events by Source/Destination Country）] グラフはドーナツ グラフ形式であり、ネットワーク上の侵入イベントにイベントの送信元（デフォルト）または宛先として関わる国の割合を表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、侵入イベントの宛先となっている国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [宛先（Destination）] をクリックします。デフォルト ビューに戻すには [送信元（Source）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信元（Source）] ビューに戻ることに注意してください。

このグラフのデータは主に [侵入イベント（Intrusion Events）] テーブルから取得されます。

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフ

[送信側/受信側の国別ファイル イベント（File Events by Sending/Receiving Country）] グラフはドーナツ グラフ形式であり、ネットワーク上のファイルイベントでファイルの送信側（デフォルト）または受信側として検出された国の割合のビューを表示します。内側のリングでは、これらの国が大陸別にグループ化されています。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でフィルタリングまたはドリルダウンされます。

ヒント　グラフに制約を適用して、ファイルを受信する国だけが表示されるようにするには、グラフにポインタを置き、表示されるトグル ボタンの [受信者（Receiver）] をクリックします。デフォルト ビューに戻すには [送信者（Sender）] をクリックします。Context Explorer から外部へ移動することでも、グラフがデフォルトの [送信者（Sender）] ビューに戻ることに注意してください。

このグラフのデータは主に [ファイル イベント（File Events）] テーブルから取得されます。

[URL 情報（URL Information）] セクション

Context Explorer の [URL 情報（URL Information）] セクションには、3 つのインタラクティブな棒グラフが表示されます。これらのグラフには、モニタ対象ネットワーク上のホストがデータを交換するために使用する URL の全体の概要（URL に関連付けられているトラフィックと固有接続数を個々の URL、URL カテゴリ、および URL レピュテーションでソートしたもの）が示されます。URL 情報でフィルタ処理を実行することはできません。

（注）　侵入イベントの情報でフィルタ処理を実行すると、[URL 情報（URL Information）] セクション全体が非表示になります。

このグラフで URL カテゴリとレピュテーション データを含めるには、URL フィルタリング ライセンスを所有している必要があることに注意してください。

[URL 別トラフィック（Traffic by URL）] グラフ

[URL 別トラフィック（Traffic by URL）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される上位 15 の URL のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL ごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL 別トラフィック（Traffic by URL）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[接続イベント（Connection Events）]テーブルから取得されます。

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフ

[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求される URL カテゴリ（`Search Engines` や `Streaming Media` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされたURLカテゴリごとに、青色の棒はトラフィックデータ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL カテゴリ別トラフィック（Traffic by URL Category）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に[URL 統計（URL Statistics）]テーブルと[接続イベント（Connection Events）] テーブルから取得されます。

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフ

[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは棒グラフ形式で、モニタ対象ネットワーク上の最も要求されるURL レピュテーション グループ（`Well known` や `Benign sites with security risks` など）のネットワーク トラフィック カウント（KB/秒）と固有接続数を表示します。リストされた URL レピュテーションごとに、青色の棒はトラフィック データ、赤色の棒は接続データを示します。

グラフ上の任意の部分にポインタを置くと、詳細情報が表示されます。グラフの任意の部分をクリックすると、その情報でドリルダウンが実行されます。

（注） 侵入イベントの情報でフィルタ処理を実行すると、[URL レピュテーション別トラフィック（Traffic by URL Reputation）] グラフは非表示になります。

このグラフでURLカテゴリとレピュテーションデータを含めるには、URLフィルタリング ライセンスを所有している必要があることに注意してください。

このグラフのデータは、主に [URL 統計（URL Statistics）] テーブルと [接続イベント（Connection Events）] テーブルから取得されます。

Context Explorer の更新

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer は、表示している情報を自動的に更新しません。新しいデータを組み込むには、Explorer を手動で更新する必要があります。

Context Explorer 自体をリロードすると（ブラウザ プログラムの更新または Context Explorer から外部へ移動した後に戻る操作などによるリロード）、すべての表示情報が更新されますが、セクション設定（入力（Ingress）/出力（Egress）グラフや [アプリケーション情報（Application Information）] セクションなど）に対して行った変更は保持されず、また、読み込みに時間がかかることがある点に注意してください。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]** を選択します。

ステップ 2 右上にある [リロード（Reload）] をクリックします。

[リロード（Reload）] ボタンは、更新が終了するまでグレー表示になります。

Context Explorer の時間範囲の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

過去 1 時間（デフォルト）から過去 1 年までの期間を反映するように、Context Explorer の時間範囲を設定できます。時間範囲を変更しても、Context Explorer は変更を反映するために自動的に更新されないことに注意してください。新しい時間範囲を適用するには、Explorer を手動で更新する必要があります。

時間範囲の変更は、Context Explorer から外部に移動したり、ログイン セッションを終了しても維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [リストを表示（Show the last）] ドロップダウンリストから、時間範囲を選択します。

ステップ 3 オプションで、新しい時間範囲のデータを表示するには、[リロード（Reload）] をクリックします。

ヒント [フィルタの適用（Apply Filters）] をクリックすると、時間範囲の更新が適用されます。

Context Explorer のセクションの最小化および最大化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer では 1 つ以上のセクションを最小化して非表示にできます。これは、特定のセクションだけを強調する場合や、ビューをシンプルにしたい場合に便利です。[トラフィックおよび侵入イベント数/時間（Traffic and Intrusion Event Counts Time）] グラフは最小化できません。

Context Explorer のセクションでは、ページを更新したり、アプライアンスからログアウトしたりしても、設定した最小化または最大化の状態が維持されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 セクションを最小化するには、セクションのタイトル バーにある最小化アイコン（－）をクリックします。

ステップ 3 セクションを最大化するには、最小化されたセクションのタイトルバーにある最大化アイコン（□）をクリックします。

Context Explorer データのドリルダウン

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer で許容されている詳細レベルよりもさらに詳細にグラフを調べたりデータをリストしたりするには、当該データのテーブル ビューにドリルダウンします。（[一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] グラフではドリル ダウンできないことに注意してください。）たとえば、[送信元 IP 別のトラフィック（Traffic by Source IP）] グラフの IP アドレスでドリルダウンすると、[接続イベント（Connection Events）] 表の [アプリケーション詳細付きの接続（Connections with Application Details）] ビューが表示されます。このビューには、選択した送信元 IP アドレスに関連するデータのみが表示されます。

調べるデータのタイプに応じて、コンテキスト メニューに追加のオプションが表示されることがあります。特定の IP アドレスに関連付けられているデータ ポイントの場合、選択した IP アドレスのホストまたは whois 情報を表示するためのオプションが表示されます。特定のアプリケーションに関連付けられているデータ ポイントの場合、選択したアプリケーションに関するアプリケーション情報を表示するためのオプションが表示されます。特定のユーザに関連付けられているデータ ポイントの場合、ユーザのユーザ プロファイル ページを表示するためのオプションが表示されます。侵入イベントのメッセージに関連付けられているデータ ポイントの場合、そのイベントに関連する侵入ルールに関するルール ドキュメントを表示するオプションが表示されます。特定の IP アドレスに関連付けられているデータ ポイントの場合、そのアドレスをブラックリストまたはホワイトリストに追加するためのオプションが表示されます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] 以外の任意のセクションで、調査するデータ ポイントをクリックします。

ステップ 3 選択するデータ ポイントに応じて、表示されるオプションが異なります。

- テーブル ビューでこのデータの詳細を表示するには、[詳細な分析を表示（Drill into Analysis）] を選択します。

- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、関連するホストに関する詳細情報を参照するには、[ホスト情報の表示（View Host Information）] を選択します。
- 特定の IP アドレスのデータ ポイントを選択している場合に、そのアドレスで whois 検索を行うには、[Whois] を選択します。
- 特定のアプリケーションに関連付けられているデータ ポイントを選択している場合に、そのアプリケーションに関する詳細情報を参照するには、[アプリケーション情報の表示（View Application Information）] を選択します。
- 特定のユーザに関連付けられているデータ ポイントを選択している場合に、そのユーザに関する詳細情報を参照するには、[ユーザ情報の表示（View User Information）] を選択します。
- 特定の侵入イベント メッセージに関連付けらているデータ ポイントを選択している場合に、関連する侵入ルールに関する詳細情報を参照するには、[ルール ドキュメントの表示（View Rule Documentation）] を選択します。
- 特定の IP アドレスに関連付けられているデータ ポイントを選択している場合に、Security Intelligence グローバル ブラックリストまたはホワイトリストにその IP アドレスを追加するには、[今すぐブラックリストに追加（Blacklist Now）] または [今すぐホワイトリストに追加（Whitelist Now）] のいずれか該当するオプションを選択します。

コンテキスト エクスプローラのフィルタ

コンテキスト エクスプローラに最初に表示される基本的で広範なデータをフィルタリングして、ネットワーク上のアクティビティのより詳細な状況を把握することができます。フィルタは URL 情報以外のすべての種類の Firepower システム データに対応し、除外と包含がサポートされており、Context Explorer のグラフ データ ポイントをクリックするだけですぐに適用でき、Explorer 全体に反映されます。一度に最大 20 のフィルタを適用できます。

コンテキスト エクスプローラ データにフィルタを追加する方法はいくつかあります。

- [フィルタの追加（Add Filter）] ダイアログを使用する。
- コンテキスト メニューを使用する（エクスプローラのデータ ポイントを選択する場合）。
- 特定の詳細表示ページ（[アプリケーションの詳細（Application Detail）]、[ホスト プロファイル（Host Profile）]、[ルールの詳細（Rule Detail）]、[ユーザ プロファイル（User Profile）]）に表示されるテキスト リンクを使用する。これらのリンクをクリックすると、コンテキスト エクスプローラが自動的に開き、詳細表示ページの当該データに基づいてコンテキスト エクスプローラがフィルタリングされます。たとえば、ユーザ `jenkins` のユーザ詳細ページで [コンテキスト エクスプローラ（Context Explorer）] リンクをクリックすると、エクスプローラにはそのユーザに関連するデータだけが表示されます。

ファイル タイプの中には、相互に互換性がないタイプがあります。たとえば、侵入イベント関連のフィルタ（**Device** や **Inline Result** など）を、接続イベント関連フィルタ（**Access Control Action** など）と同時に適用することはできません。これは、システムでは接続イベント デー

タを侵入イベントデータによってソートできないためです。互換性のないフィルタの同時適用はシステムによって自動的に防止されます。互換性の問題が存在する場合、より後に適用された方のフィルタ タイプと互換性のないタイプのフィルタは非表示になります。

複数のフィルタがアクティブな場合、同じデータ タイプの値は OR 検索条件として扱われます。つまり、いずれか1つの値と一致するデータがすべて表示されます。異なるデータ タイプの値は AND 検索条件として扱われます。つまり、データは各フィルタ データ タイプの 1 つ以上の値と一致する必要があります。たとえば、`Application: 2channel`、`Application: Reddit`、および `User: edickinson` というフィルタ セットで表示されるデータは、ユーザ `edickinson` に関連付けられており、**かつ**アプリケーション `2channel` **または**アプリケーション `Reddit` に関連付けられている必要があります。

マルチドメイン展開では、先祖ドメインでコンテキストエクスプローラを表示している場合に複数の子孫ドメインでフィルタリングできます。この場合、**IP Address** フィルタも追加する場合は注意してください。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

表示されるデータは、管理対象デバイスのライセンスおよび展開方法やデータを提供する機能を設定するかどうかなどの要因によって異なります。

（注） フィルタは、必要とする正確な Firepower データ コンテキストをいつでも取得できるシンプルかつ俊敏性に優れたツールとして機能します。永続的に設定するものではなく、コンテキストエクスプローラから外部に移動するか、セッションを終了すると消去されます。後で使用するためにフィルタ設定を保存するには、フィルタ処理されたコンテキストエクスプローラ ビューの保存 （28 ページ）を参照してください。

データ タイプ フィールド オプション

次の表に、フィルタとして使用できるデータ タイプと、各データ タイプの例と説明を示します。

表 2: フィルタ データ タイプ

タイプ（Type）	値の例	定義（Definition）
アクセス コントロール アクション（Access Control Action）	`Allow`、`Block`	トラフィックを許可またはブロックするためにアクセス コントロール ポリシーにより実行されるアクション。
アプリケーション カテゴリ（Application Category）	`web browser`、`email`	アプリケーションの主要機能の一般的な分類。
アプリケーション	`Facebook`、`HTTP`	アプリケーションの名前。

タイプ（Type）	値の例	定義（Definition）
アプリケーションのリスク（Application Risk）	`Very High、Medium`	アプリケーションの推定セキュリティリスク。
アプリケーションタグ（Application Tag）	`encrypts communications、sends mail`	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを使用できます（タグを使用しないことも可能です）。
アプリケーション タイプ（Application Type）	`Client、Web Application`	アプリケーションタイプ（アプリケーションプロトコル、クライアント、または Web アプリケーション）。
ビジネスとの関連性（Business Relevance）	`Very Low、High`	（娯楽ではない）ビジネスアクティビティに対するアプリケーションの推定関連度。
大陸（Continent）	`North America、Asia`	モニタ対象ネットワークで検出されたルーティング可能なIPアドレスに関連付けられている大陸。
国（Country）	`Canada、Japan`	モニタ対象ネットワークで検出されたルーティング可能なIPアドレスに関連付けられている国。
Device	`device1.example.com、192.168.1.3`	モニタ対象ネットワーク上のデバイスの名前または IP アドレス。
ドメイン（Domain）	`Asia Division、Europe Division`	グラフ表示するネットワーク アクティビティを行うデバイスのドメイン。このデータ タイプはマルチドメイン展開の場合にのみ存在します。
イベントの分類（Event Classification）	`Potential Corporate Policy Violation、Attempted Denial of Service`	侵入イベントの簡単な説明。侵入イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
イベント メッセージ（Event Message）	`dns response、P2P`	イベントによって生成されるメッセージ。イベントをトリガーしたルール、デコーダ、またはプリプロセッサにより決定されます。
ファイル傾向（File Disposition）	`Malware、Clean`	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの性質。

タイプ（Type）	値の例	定義（Definition）
ファイル名	`Packages.bz2`	ネットワーク トラフィックで検出されたファイルの名前。
ファイル SHA256（File SHA256）	任意の 32 ビット文字列	Firepower Management Center によるマルウェア クラウド検索の実行対象ファイルの SHA-256 ハッシュ値。
ファイル タイプ（File Type）	`GZ`、`SWF`、`MOV`	ネットワーク トラフィックで検出されたファイルのタイプ。
ファイル タイプ カテゴリ（File Type Category）	`Archive`、`Multimedia`、`Executables`	ネットワーク トラフィックで検出されたファイルのタイプの一般カテゴリ。
[IPアドレス（IP Address）]	`192.168.1.3`、`2001:0db8:85a3::0000/24`	IPv4 または IPv6 のアドレス、アドレス範囲、またはアドレス ブロック。 IP アドレスを検索すると、そのアドレスが送信元または宛先のいずれかになっているイベントが返されることに注意してください。
影響レベル（Impact Level）	`Impact Level 1`、`Impact Level 2`	モニタ対象ネットワークでのイベントの推定影響レベル。
インライン結果（Inline Result）	`dropped`、`would have dropped`	トラフィックがドロップされたか、ドロップされた可能性があるか、またはシステムによりトラフィックが処理されていないかのいずれかです。
IOC カテゴリ（IOC Category）	`High Impact Attack`、`Malware Detected`	トリガーとして使用された侵害の兆候（IOC）イベントのカテゴリ。
IOC イベント タイプ（IOC Event Type）	`exploit-kit`、`malware-backdoor`	特定の侵害の兆候（IOC）に関連付けられている ID。その兆候をトリガーしたイベントを示します。
マルウェア脅威名（Malware Threat Name）	`W32.Trojan.a6b1`	マルウェア脅威の名前。
OS 名（OS Name）	`Windows`、`Linux`	オペレーティング システムの名前。
OS Version	`XP`、`2.6`	オペレーティング システムの特定のバージョン。
[プライオリティ（Priority）]	`high`、`low`	イベントの推定緊急度。

タイプ（Type）	値の例	定義（Definition）
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	`Malware`、`Spam`	セキュリティ インテリジェンスにより判別される危険なトラフィックのカテゴリ。
セキュリティ ゾーン	`My Security Zone`、`Security Zone X`	トラフィックが分析されたインターフェイスのセット。インライン展開の場合は、トラフィックが通過するインターフェイスのセット。
SSL	`yes`、`no`	SSL暗号化トラフィックまたはTLS暗号化トラフィック。
ユーザ（User）	`wsmith`、`mtwain`	モニタ対象ネットワーク上のホストにログインしたユーザの ID。

[フィルタの追加（Add Filter）] ウィンドウからのフィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

この手順を使用して、[フィルタの追加（Add Filter）] ウィンドウでフィルタを最初から作成します。（コンテキスト メニューを使用して、クイック フィルタを作成することもできます。）

Context Explorer の左上にある [フィルタ（Filters）] の下のプラス アイコン（+）をクリックすると表示される [フィルタの追加（Add Filter）] ウィンドウには、次の 2 つのフィールドだけが表示されます。

- [データ タイプ（Data Type）] ドロップダウン リストには、Context Explorer に制約を適用するために使用できる多数の Firepower システム データ タイプが含まれています。データ タイプの選択後に、そのタイプの固有の値を [フィルタ（Filter）] フィールドに入力します（たとえば、[大陸（Continent）] タイプの場合は値 [アジア（Asia）] など）。ユーザ支援のため、[フィルタ（Filter）] フィールドでは、選択したデータ タイプのさまざまな値の例がグレー表示で示されます。（フィールドにデータを入力すると、これらは消去されます。）
- [フィルタ（Filter）] フィールドには、イベント検索と同様に、* や ! などの特殊検索パラメータを入力できます。フィルタ パラメータの前に ! 記号を付けることで排他的なフィルタを作成できます。

（注） 追加したフィルタは自動的には適用されません。Context Explorer でフィルタを表示するには、[フィルタの適用（Apply Filters）] をクリックする必要があります。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 左上にある [フィルタ（Filter）] の下で、プラス アイコン（+）をクリックします。

ステップ 3 [データ タイプ（Data Type）] ドロップダウンリストから、フィルタリングの条件として使用するデータ タイプを選択します。

ステップ 4 [フィルタ（Filter）] フィールドに、フィルタリングの条件として使用するデータ タイプ値を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 オプションで、前述の手順を繰り返し、必要なフィルタ セットが設定されるまで、フィルタを追加します。

ステップ 7 [フィルタの適用（Apply Filters）] をクリックします。

関連トピック

データ タイプ フィールド オプション （23 ページ）
検索の制約

コンテキスト メニューからのクイック フィルタの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

Context Explorer のグラフとリスト データを詳しく調べるときに、データ ポイントをクリックし、コンテキスト メニューを使用してそのデータに基づいてフィルタ（包含または除外）を簡単に作成できます。コンテキスト メニューを使用して、[アプリケーション（Application）]、[ユーザ（User）]、[侵入イベント メッセージ（Intrusion Event Message）] データ タイプの情報、あるいは任意の個別ホストでフィルタリングする場合、フィルタ ウィジェットには、そのデータ タイプの該当する詳細ページ（アプリケーション データの場合は [アプリケーションの詳細（Application Detail）] など）にリンクするウィジェット情報アイコンが表示されます。URL データではフィルタリングできないことに注意してください。

特定のグラフまたはリストのデータを詳しく調査する場合にもコンテキストメニューを使用できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 [一定期間のトラフィックおよび侵入イベント（Traffic and Intrusion Events over Time）] セクションと URL データを含むセクション以外の Explorer セクションで、フィルタリングするデータポイントをクリックします。

ステップ 3 次の 2 つの対処法があります。

- このデータにフィルタを追加するには、[フィルタの追加（Add Filter）] をクリックします。
- このデータに除外フィルタを追加するには、[除外フィルタの追加（Add Exclude Filter）] をクリックします。このフィルタが適用されると、除外された値に関連付けられて**いない**すべてのデータが表示されます。除外フィルタでは、フィルタ値の前に感嘆符（!）が表示されます。

フィルタ処理されたコンテキスト エクスプローラ ビューの保存

コンテキストエクスプローラから外部に移動した後、またはセッションを終了した後に、コンテキストエクスプローラのフィルタ設定を保持するには、適切なフィルタを適用したコンテキスト エクスプローラのブラウザ ブックマークを作成します。適用されるフィルタはコンテキスト エクスプローラ ページ URL に組み込まれているので、そのページのブックマークを読み込むと、対応するフィルタも読み込まれます。

手順

適切なフィルタが適用されたコンテキスト エクスプ ローラーのブラウザ ブックマークを作成します。

フィルタ データの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 該当するフィルタ ウィジェットの情報アイコン（ⓘ）をクリックします。

フィルタの削除

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
機能に応じて異なる	機能に応じて異なる	任意（Any）	任意（Any）	Admin/Any Security Analyst

手順

ステップ 1 **[分析（Analysis）] > [コンテキスト エクスプローラ（Context Explorer）]**を選択します。

ステップ 2 左上の [フィルタ（Filters）] の下で、任意のフィルタ ウィジェットのクリア アイコン（✖）をクリックします。

ヒント　すべてのフィルタを一括削除するには、[クリア（Clear）] ボタンをクリックします。