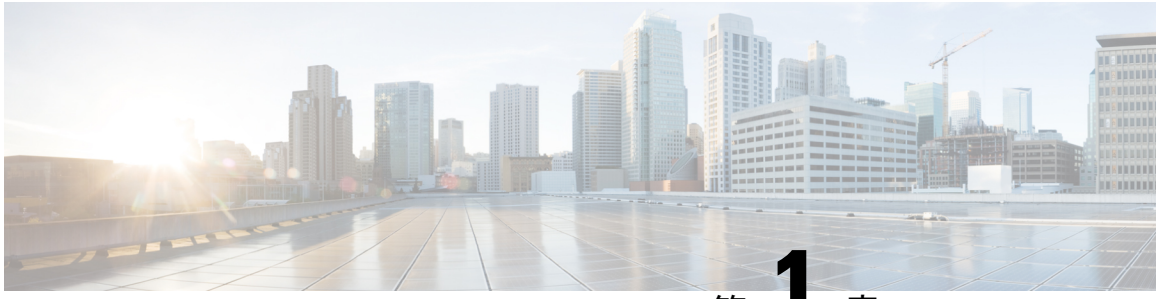
# Cisco Security Analytics and Logging（オンプレミス）：ファイアウォールイベント統合ガイド

**初版**：2021 年 5 月 26 日

**最終更新**：2021 年 10 月 28 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

# はじめに



## 概要

このガイドでは、ファイアウォールのイベントデータを保存し、より長い保存期間でストレージを増やすようにシスコのセキュリティ分析とロギング（オンプレミス）を設定する方法について説明します。Cisco Secure Network Analytics（旧 Stealthwatch）アプライアンスを展開し、Firewall 展開に統合することで、イベントデータを Secure Network Analytics アプライアンスにエクスポートできます。

その後、次の操作を実行できます。

- Firepower Management Center にイベントを保存し、Secure Network Analytics 展開にイベントを保存します。
- このリモートデータソースを指定して、Firepower Management Center でこれらのイベントを表示します。
- イベントビューアを使用して、Cisco Secure Network Analytics Manager（旧 Stealthwatch 管理コンソール）Web アプリケーション UI からイベントデータを確認します。
- Firepower Management Center UI からイベントビューアに相互起動して、相互起動元の情報に関する追加のコンテキストを表示します。

（注） オンプレミスではなく Cisco Cloud にファイアウォール イベント データを保存する場合、詳細については Cisco Security Analytics and Logging (SaaS) documentation を参照してください。

## サポートされるイベント タイプ

- FTD セキュリティイベント
  - 接続

- 侵入（Intrusion）
- ファイルおよびマルウェア

- FTD データプレーンイベント
- ASA イベント

# 概念とアーキテクチャ

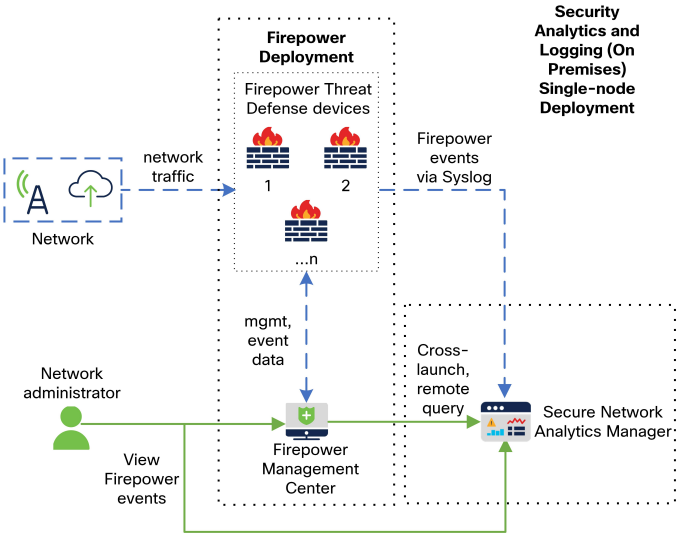
セキュリティ分析とロギング（オンプレミス） の展開では、Secure Network Analytics アプライアンスを使用して別のシスコ製品の展開環境（Firepower アプライアンス展開など）からのデータを保存します。Firepower 展開の場合、Firepower セキュリティイベントおよびデータプレーンイベントを UDP を介した syslog として Firepower Management Center が管理する Firepower Threat Defense デバイスから マネージャ にエクスポートして、その情報を保存します。セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0 では、syslog を介して ASA デバイスから マネージャ にイベントをエクスポートする機能が追加されました。

Secure Network Analytics の展開には次の 2 つのオプションがあります。

- 単一ノード：スタンドアロンの Manager を展開してイベントを受信および保存し、そこからイベントを確認および照会します。
- マルチノード：イベントを受信する Cisco Secure Network Analytics フローコレクタ、イベントを保存する Cisco Secure Network Analytics データストア（Cisco Secure Network Analytics データノード X 3 を装備）、イベントを確認および照会できる Manager を展開します。

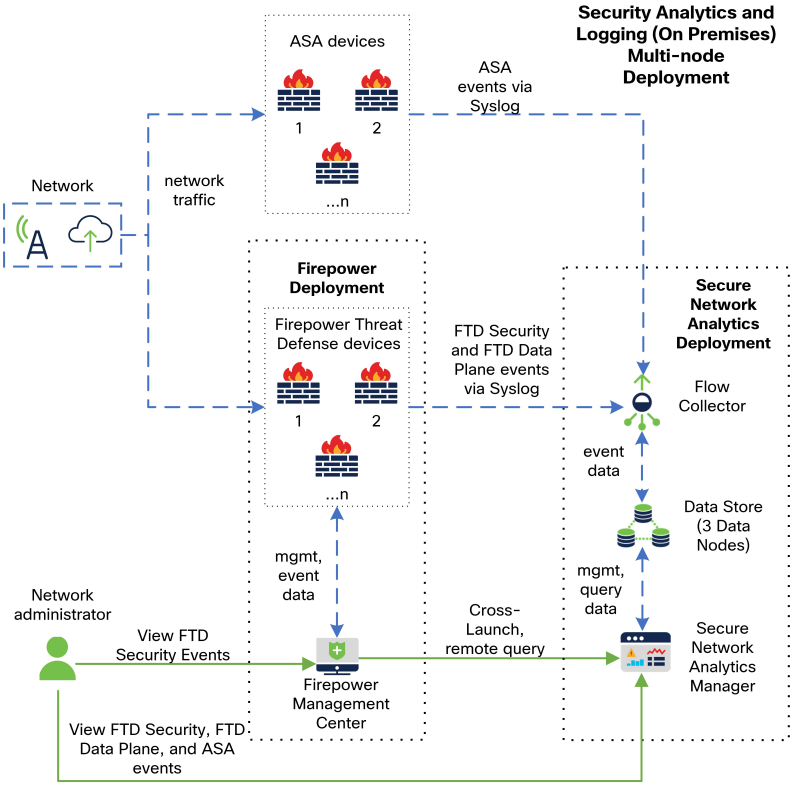
（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと 3 つのデータノード（マルチノード）を管理するマネージャのインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャにアプリケーションをインストールすることはできません。詳細については、トラブルシューティング （41 ページ）を参照してください。

マネージャ を使用した 単一ノード の展開の例については、次の図を参照してください。

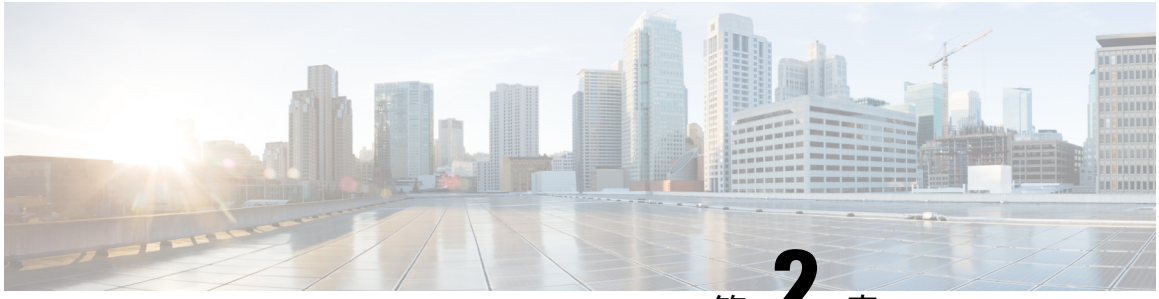



この展開では、Firepower Threat Defense デバイスは Firepower のイベントを マネージャ に送信し、Manager がこれらのイベントを保存します。ユーザは Firepower Management Center の UI からマネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。

マネージャ、3 つのデータノード、およびフローコレクタを使用したマルチノードの展開の例については、次の図を参照してください。



この展開では、Firepower Threat Defense デバイスおよび ASA デバイスはファイアウォールのイベントをフローコレクタに送信します。フローコレクタは、保存のためにデータストア（データノード X 3）にイベントを送信します。ユーザは Firepower Management Center の UI から マネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。



第 2 章

# 展開



## 要件とベストプラクティス

セキュリティ分析とロギング（オンプレミス）を展開してファイアウォールのイベントデータを保存するための要件とベストプラクティスを次に示します。

### ファイアウォール アプライアンス

次のファイアウォール アプライアンスを展開する必要があります。

| ソリューションのコンポーネント | 必要なバージョン | シスコのセキュリティ分析とロギング（オンプレミス）のライセンス | 注記 |
|---|---|---|---|
| Firepower Management Center（ハードウェアまたは仮想） | v7.0+<br>以前のバージョンを実行している Firepower Management Center の場合は、https://cisco.com/go/sal-on-prem-docsを参照してください。 | なし | • Firepower Management Center ごとに 1 つの マネージャ。また、必要に応じて 1 つのフローコレクタと 1 つのデータストア（データノード X 3）を展開できます。 |

| ソリューションのコンポーネント | 必要なバージョン | シスコのセキュリティ分析とロギング（オンプレミス）のライセンス | 注記 |
|---|---|---|---|
| Firepower 管理対象のデバイス | v7.0+（ウィザードを使用）<br>Firepower Threat Defense v6.4 以降（syslog を使用）<br>NGIPS v6.4（syslog を使用） | なし | |
| ASA デバイス | v9.12+ | なし | • セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード 展開でサポートされています。 |

**Secure Network Analytics アプライアンス**

Secure Network Analytics の展開には次のオプションがあります。

- 単一ノード：マネージャ のみを展開してイベントを取り込んで保存したり、イベントを確認および照会します。
- マルチノード：フローコレクタを展開してイベントを取り込み、データストアを展開してイベントを保存し、マネージャ を展開してイベントを確認および照会します。

注 Secure Network Analytics ハードウェアと Secure Network Analytics VE アプライアンスを混在させて展開することはできません。

表 *1*：単一ノード

| ソリューションのコンポーネント | 必要なバージョン | セキュリティ分析とロギング（オンプレミス） のライセンス | 注記 |
|---|---|---|---|
| マネージャ | Secure Network Analytics v7.3.1+ | なし | • マネージャ 2210 ハードウェアアプライアンスまたはマネージャ の仮想エディション（VE）のいずれかを展開できます。<br>• 複数台の Firepower Threat Defense デバイスからイベントを受信できます。これらはすべて 1 つの Firepower Management Center によって管理されます。<br>• イベントを取り込んで マネージャの Web アプリケーションでファイアウォールイベントを表示するには セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。 |
| セキュリティ分析とロギング（オンプレミス） アプリ | セキュリティ分析とロギング（オンプレミス）アプリケーション v2.0+ | GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング | マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。 |

表 *2:* マルチノード

| ソリューションのコンポーネント | 必要なバージョン | セキュリティ分析とロギング（オンプレミス） のライセンス | 注記 |
|---|---|---|---|
| マネージャ | Secure Network Analytics v7.3.2+ | なし | • マネージャ 2210 ハードウェアアプライアンスまたはマネージャ の仮想エディション（VE）のいずれかを展開できます。<br>• イベントを取り込んで マネージャの Web アプリケーションでファイアウォールイベントを表示するには セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。 |

| ソリューションのコンポーネント | 必要なバージョン | セキュリティ分析とロギング（オンプレミス） のライセンス | 注記 |
|---|---|---|---|
| Flow Collector | Secure Network Analytics v7.3.2+ | なし | • Flow Collector 4210 ハードウェアアプライアンスまたはフローコレクタ VE アプライアンスのいずれかを展開できます。<br>• 複数台の Firepower Threat Defense デバイスからイベントを受信できます。これらはすべて 1 つの Firepower Management Center によって管理されます。<br>• 複数の ASA デバイス（v7.4+）から ASA イベントを受信できます。 |
| データストア（データノード X 3） | Secure Network Analytics v7.3.2+ | なし | • Data Store 6200（データノード X 3）ハードウェアまたはデータストア VE（データノード VE X 3）のいずれかを展開できます。<br>• フローコレクタで受信したファイアウォールイベントを保存できます。 |
| セキュリティ分析とロギング（オンプレミス） アプリ | セキュリティ分析とロギング（オンプレミス）アプリケーション v2.0+ | GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング | マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。 |

これらのコンポーネントに加えて、すべてのアプライアンスが NTP を使用して時刻を同期できることを確認する必要があります。

Firepower または Secure Network Analytics アプライアンスのコンソールにリモートでアクセスする場合は、SSH 経由のアクセスを有効にできます。

# Secure Network Analytics のライセンス

ライセンスなしで、セキュリティ分析とロギング（オンプレミス） を 90 日間評価モードで使用できます。90 日間経過した後も セキュリティ分析とロギング（オンプレミス） の使用を継続するには、ファイアウォール展開から Secure Network Analytics アプライアンスに syslog データで送信する見込みの 1 日あたりの GB に基づいて、スマートライセンスのロギングとトラブルシューティングのスマートライセンスを取得する必要があります。

（注） ライセンスの計算のために、データ量は最も近い GB 数（切り捨て）で報告されます。たとえば、1 日あたり 4.9 GB を送信する場合は、4 GB と報告されます。

Secure Network Analytics アプライアンスのライセンスに関する詳細については、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。

# Secure Network Analytics Resource Allocation

セキュリティ分析とロギング（オンプレミス） に展開した場合、Secure Network Analytics は次の取り込みレートを提供します。

- ハードウェアまたはバーチャルエディション（VE）の 単一ノード の展開では、平均で最大約 20,000 イベント/秒（EPS）でショートバーストでは最大 35,000 EPS を取り込むことができます。
- バーチャルエディション（VE）の マルチノード の展開では、平均で最大約 5,000 EPS、ショートバーストでは最大 175,000 EPS を取り込むことができます。
- ハードウェア マルチノード の展開では、平均で最大約 10 万 EPS、ショートアーストでは最大 350,000 EPS を取り込むことができます。

割り当てたハードドライブストレージに基づいて、数週間または数か月にわたってデータを保存できます。これらの推定値は、ネットワーク負荷、トラフィックスパイク、イベントごとに送信される情報など、さまざまな要因の影響を受けます。

（注） EPS の取り込みレートが高いと、セキュリティ分析とロギング（オンプレミス） アプリケーションがデータをドロップする場合があります。さらに、接続、侵入、ファイル、マルウェアのイベントのみではなく、すべてのイベントタイプを送信する場合は、全体的な EPS の増加にしたがい、データをドロップする場合があります。この場合はログファイルを確認します。

### 単一ノード VE の推奨事項

最適なパフォーマンスを得るために、マネージャ VE を展開する場合は、次のリソースを割り当てます。

| リソース | 推奨 |
|---|---|
| CPU | 12 |
| RAM | 64 GB |
| ハードドライブストレージ | 2 TB |

割り当てるストレージスペースに基づいて、大まかに次の期間のデータを 単一ノード の展開環境に保存できます。

| 平均 EPS | 平均日次イベント | 1 TB ストレージの推定保持期間 | 2 TB ストレージの推定保持期間 | 4 TB ストレージの推定保持期間 |
|---|---|---|---|---|
| 1,000 | 8,650 万 | 250 日 | 500 日 | 1000 日 |
| 5,000 | 4 億 3,000 万 | 50 日 | 100 日 | 200 日 |
| 10,000 | 8 億 6,500 万 | 25 日 | 50 日 | 100 日 |
| 20,000 | 17 億 3,000 万 | 12.5 日 | 25 日 | 50 日 |

マネージャが最大ストレージキャパシティに達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。

（注） この推定取り込みおよび保管の期間について、これらのリソース割り当てでマネージャ VE をテストしました。仮想アプライアンスに十分な CPU または RAM を割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。ストレージ割り当てを 4 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

### マルチノード 推奨事項

最適なパフォーマンスを得るために、マネージャ VE、フローコレクタ VE、および データストア VE を展開する場合は、次のリソースを割り当てます。

**表 *3*：マネージャ *VE***

| リソース | 推奨 |
|---|---|
| CPU | 8 Intel Xeon、最小 2.29 GHz |
| RAM | 64 GB |

| リソース | 推奨 |
|---|---|
| ハードドライブストレージ | 480 GB |

表 *4 : Flow Collector VE*

| リソース | 推奨 |
|---|---|
| CPU | 8 Intel Xeon、最小 2.29 GHz |
| RAM | 70 GB |
| ハードドライブストレージ | 480 GB |

表 *5 :* データノード *VE*（データストアの一部として）

| リソース | 推奨 |
|---|---|
| CPU | 12 Intel Xeon、データノードあたり最小 2.29 GHz |
| RAM | データノードあたり 32 GB |
| ハードドライブストレージ | データノード VE あたり 5 TB、または 3 つのデータノードで合計 15 TB |

割り当てるストレージスペースに基づいて、大まかに次の期間のデータを マルチノード の展開環境に保存できます。

| 平均 EPS | 平均日次イベント | 仮想 | ハードウェア |
|---|---|---|---|
| 1,000 | 8,650 万 | 1,500 日 | 3,000 日 |
| 5,000 | 4 億 3,000 万 | 300 日 | 600 日 |
| 10,000 | 8 億 6,500 万 | 150 日 | 300 日 |
| 20,000 | 17 億 3,000 万 | 75 日 | 150 日 |
| 25,000 | 21 億 6,000 万 | 60 日 | 120 日 |
| 50,000 | 43 億 2,000 万 | 30 | 60 日 |
| 75,000 | 64 億 8,000 万 | サポート対象外 | 40 日間 |
| 100,000 | 86 億 4,000 万 | サポート対象外 | 30日間 |

データストアが最大ストレージキャパシティに達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。

（注） この推定取り込みおよび保存の期間について、これらのリソース割り当てでこれらの仮想アプライアンスをテストしました。仮想アプライアンスに十分なCPUまたはRAMを割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。ストレージ割り当てを 4 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

# 通信ポート

次の表に単一ノードの展開の場合にセキュリティ分析とロギング（オンプレミス）を統合するために開く必要がある通信ポートを示します。

| 送信元（クライアント） | 宛先（サーバ） | ポート | プロトコルまたは目的 |
|---|---|---|---|
| 外部インターネット（NTP サーバ） | Firepower Management Center、Firepower Threat Defense デバイス、およびマネージャ | 123/UDP | すべて同じ NTP サーバへの NTP 時刻同期 |
| ユーザワークステーション | Firepower Management Centerおよびマネージャ | 443/TCP | Web ブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン |
| Firepower Management Center によって管理される Firepower Threat Defense デバイス | マネージャ | 8514/UDP | Firepower Threat Defense デバイスからの syslog のエクスポート、マネージャへの取り込み |
| Firepower Management Center | マネージャ | 443/TCP | Firepower Management Center からマネージャへのリモートクエリ |

次の表にマルチノードの展開の場合にセキュリティ分析とロギング（オンプレミス）を統合するために開く必要がある通信ポートを示します。さらに、Secure Network Analytics 展開で開く必要があるポートについては、『Data Store Hardware Deployment and Configuration Guide』と『Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。

| 送信元（クライアント） | 宛先（サーバ） | ポート | プロトコルまたは目的 |
|---|---|---|---|
| 外部インターネット（NTP サーバ） | Firepower Management Center、Firepower Threat Defense デバイス、マネージャ、フローコレクタ、およびデータストア | 123/UDP | すべて同じ NTP サーバへの NTP 時刻同期 |
| ユーザワークステーション | Firepower Management Centerおよびマネージャ | 443/TCP | Web ブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン |
| Firepower Management Center によって管理される Firepower Threat Defense デバイス | Flow Collector | 8514/UDP | Firepower Threat Defense デバイスからの syslog のエクスポート、フローコレクタへの取り込み |
| ASA デバイス | Flow Collector | 514/UDP | ASA デバイスからの syslog のエクスポート、フローコレクタへの取り込み |
| Firepower Management Center | マネージャ | 443/TCP | Firepower Management Center から マネージャへのリモートクエリ |

# 設定の概要

次に、イベントデータを保存するための展開の大まかな設定手順を説明します。

導入を開始する前に、次のタスクを確認してください。

| コンポーネントとタスク | 手順 |
|---|---|
| 単一ノード の導入 | 次の選択肢があります。<br>• マネージャ 2210 をネットワークに展開し、eth0 管理インターフェイスの IP アドレスやその他の情報の割り当てを含む初期設定を実行します。詳細については、『x2xx Series Hardware Installation Guide』と『Secure Network Analytics System Configuration Guide』を参照してください。<br>• マネージャ VE ISO をダウンロードし、マネージャ VE をハイパーバイザに展開します。初期設定を実行し、eth0 管理インターフェイスの IP アドレスとその他の情報を割り当てます。詳細については、『Secure Network Analytics Virtual Edition Installation Guide』を参照してください。 |
| マルチノード の導入 | 次の選択肢があります。<br>• ハードウェア マネージャ、フローコレクタ、および 3 つのデータノードをネットワークに展開します。各アプライアンスの初期設定を実行し、データストアを初期化します。詳細については、『x2xx Series Hardware (with Data Store) Appliance Installation Guide』を参照してください。<br>• マネージャ VE ISO、フローコレクタ VE ISO、およびデータノード ISO をダウンロードします。1 つの マネージャ VE、1 つのフローコレクタ VE、および 3 つのデータノード VE をハイパーバイザに展開します。各アプライアンスの初期設定を実行し、データストアを初期化します。詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。 |
| セキュリティ分析とロギング（オンプレミス） アプリケーションをダウンロードして マネージャにインストールし、ファイアウォールのイベントを受信して保存するように Secure Network Analytics の展開を設定 | • マネージャ で、[集中管理（Central Management）] の [アプリケーションマネージャ（App Manager）] に移動し、 アプリケーションをダウンロードします。Firepower デバイスからイベントを受信するように設定します。<br>• スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと 3 つの データノード（マルチノード）を管理する マネージャ のインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。詳細については、トラブルシューティング （41 ページ）を参照してください。<br>• アプリケーションの使用方法の詳細については、セキュリティ分析とロギング（オンプレミス）リリースノートとアプリケーションのヘルプを参照してください。 |

| コンポーネントとタスク | 手順 |
|---|---|
| イベントを セキュリティ分析とロギング（オンプレミス）に送信するように Firepower Management Center を設定 | 次の選択肢があります。<br>• イベントを Secure Network Analytics アプライアンスに送信するように Firepower Management Center を設定します。<br>• 「データプレーンイベントログの設定」セクションを使用して、データ プレーン イベント ロギングを設定します。<br>• 「Firepower Management Center での優先度が低い接続イベントの保存の停止」セクションを使用して、Firepower Management Center のロギング負荷を軽減します。 |
| イベントを セキュリティ分析とロギング（オンプレミス）に送信するように ASA デバイスを設定 | • イベントを Secure Network Analytics アプライアンスに送信するように ASA デバイスを設定します。ASA デバイスの設定 （29 ページ）を参照してください。<br>• ASA イベントは、セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。 |
| 次の手順の確認 | 次の手順を確認します。<br>• 詳細については、Firepower のオンラインヘルプを参照してください。「Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Firepower Management Center での作業」を参照してください。<br>• Secure Network Analytics の使用方法については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。 |

# 単一ノードの展開と設定

### 始める前に

- マネージャ（v7.3+）をネットワークに展開し、その管理 IP アドレスに Firepower Management Center の管理 IP アドレスと Firepower Threat Defense デバイスの管理 IP アドレスの両方から到達可能であることを確認します。さらに設定する場合に備えて、管理 IP アドレスをメモしておきます。詳細については、『Secure Network Analytics Virtual Edition Installation Guide』を参照してください。
- Secure Network Analytics 製品インスタンスを適切に登録します。マネージャ VE ライセンスは登録後にアカウントに自動的に追加されます。詳細については、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。

### 手順

マネージャ VE を展開するには、『Secure Network Analytics Virtual Edition Installation Guide』の手順に、マネージャ 2210 を展開する場合は、『x2xx Series Hardware Installation Guide』と『Secure Network Analytics System Configuration Guide』の手順に従います。

（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと 3 つのデータノード（マルチノード）を管理するマネージャ のインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。詳細については、トラブルシューティング （41 ページ） を参照してください。

# マルチノードの展開と設定

重要 マネージャ またはフローコレクタを セキュリティ分析とロギング（オンプレミス） で使用するように設定した後に、アプライアンスの設定を更新してこの設定を変更することはできません。選択を間違えた場合は、アプライアンスを RFD する必要があります。セキュリティ分析とロギング（オンプレミス） に Secure Network Analytics を使用してファイアウォールイベント情報を保存する場合にのみ、この機能を有効にしてください。

### 始める前に

- マネージャ、フローコレクタ、および3つのデータノード（v7.3.2+）をネットワークに展開したこと、Firepower Threat Defense デバイスの管理 IP アドレスがフローコレクタ管理 IP アドレスに到達可能であること、および Firepower Management Center の管理 IP アドレスが マネージャ の管理 IP アドレスに到達可能であることを確認します。さらに設定する場合に備えて、管理 IP アドレスをメモしておきます。
- Secure Network Analytics 製品インスタンスを適切に登録します。マネージャ VE ライセンスは登録後にアカウントに自動的に追加されます。詳細については、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。

### 手順

『x2xx Series Hardware (with Data Store) Appliance Installation Guide』の手順に従って Secure Network Analytics ハードウェアアプライアンスを展開するか、『Virtual Edition (with Data Store) Appliance Installation Guide』に従って Secure Network Analytics 仮想アプライアンスを展開します。

（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと3つのデータノード（マルチノード）を管理するマネージャ のインストールがサポートされています。3つのデータノードを管理せずに1つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。詳細については、トラブルシューティング （41 ページ） を参照してください。

# マネージャ の設定

セキュリティ分析とロギング（オンプレミス） に対して Secure Network Analytics の展開を設定するには、マネージャ に セキュリティ分析とロギング（オンプレミス） アプリケーションをインストールします。これにより、ファイアウォールデバイスからイベントを受信するように マネージャ が設定されます。

（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと3つのデータノード（マルチノード）を管理するマネージャ のインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャ にアプリケーションをインストールすることはできません。詳細については、トラブルシューティング （41 ページ） を参照してください。

## セキュリティ分析とロギング（オンプレミス）アプリケーションのインストール

マネージャ に セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールします。詳細については、『セキュリティ分析とロギング（オンプレミス）Release Notes』を参照してください。

**手順**

**ステップ 1** セキュリティ分析とロギング（オンプレミス）アプリケーションをダウンロードするには、https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

**ステップ 2** マネージャ にログインします。

**ステップ 3** [グローバル設定（Global Settings）] アイコンをクリックします。

**ステップ 4** [集中管理（Central Management）] を選択します。

**ステップ 5** [アプリケーションマネージャ（App Manager）] タブをクリックします。

**ステップ 6** [参照（Browse）] をクリックします。

**ステップ 7** 画面に表示される指示に従って、アプリケーションファイルをアップロードします。

### 次のタスク

**注意** セキュリティ分析とロギング（オンプレミス）アプリケーションをアンインストールすると、ファイアウォールイベントデータを含むすべての関連情報がマネージャから削除されます。単一ノード展開がある場合は、スタンドアロンのマネージャの制限も解除されます。セキュリティ分析とロギング（オンプレミス）アプリケーションをアンインストールした後、トラフィックを検査するために、従来の Secure Network Analytics 展開の一部としてスタンドアロンマネージャで 1 つ以上のフローコレクタを管理できます。

- イベントを Secure Network Analytics アプライアンスに送信するように Firepower Management Center を設定します。
- イベントを Secure Network Analytics アプライアンスに送信するように ASA デバイスを設定します。ASA デバイスの設定 （29 ページ） を参照してください。

# Firepower の設定

セキュリティ分析とロギング（オンプレミス） に対して Firepower を設定する場合、次のオプションがあります。

- Firepower Threat Defense デバイスが Firepower 7.0+ を実行している場合は、設定ウィザードを使用します。詳細については、「Firepower Management Center でのウィザードの設定」を参照してください。
- Firepower Threat Defense デバイスが Firepower 6.4 ～ 6.8 を実行している場合は、syslog エクスポートを手動で設定します。詳細については、7.0 より前のバージョンを実行している管理対象デバイスの場合は、syslog を使用する （22 ページ） を参照してください。

## Firepower Management Center でのウィザードの設定

この手順では、すべての Firepower Management Center ユーザの統合を設定します。

### 始める前に

- Firepower システムが予期したとおりに動作し、送信するイベントを生成する必要があります。
- Firepower イベントデータを受信できるように Secure Network Analytics およびセキュリティ分析とロギング（オンプレミス） の製品を設定します。
- Firepower の次のいずれかのユーザロールが必要です。

- 管理者
- アナリスト（Analyst）
- セキュリティ アナリスト（Security Analyst）

- 現在、イベントの直接送信をサポートしているデバイスのバージョンから Secure Network Analytics に syslog を使用してイベントを送信している場合、それらのデバイスの syslog を無効にして（または syslog の設定を含めないアクセス コントロール ポリシーをそれらのデバイスに割り当てて）リモートボリュームでイベントが重複しないようにします。
- 次の情報を収集します。
  - マネージャ のホスト名または IP アドレス。
  - （フローコレクタを使用し、拡張ストレージキャパシティに対して複数の Secure Network Analytics アプライアンスを集約する場合）フローコレクタの IP アドレス。（この設定にはホスト名を使用できません。）
  - 管理者権限を持つ Secure Network Analytics アプライアンスのアカウントのログイン情報。

    これらのログイン情報は Firepower Management Center に保存されません。これらの情報は、マネージャ の Firepower Management Center の読み取り専用アナリスト API アカウントを確立するために一度使用されます。これには専用アカウントは必要ありません。管理者自身のログイン情報を使用できます。

    登録プロセス中に マネージャ からログアウトする場合があります。このウィザードを開始する前に、進行中の作業を完了してください。
  - [最初の使用時に信頼する（trust on first use）] オプションを使用しない場合は、マネージャ からの SSL 証明書を使用します。

## 手順

**ステップ 1** Firepower Management Center で、[システム（System）] > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics and Logging）] に移動します。

**ステップ 2** 拡張ストレージキャパシティにスタンドアロン Secure Network Analytics アプライアンス（単一ノード）またはフローコレクタ（マルチノード）を使用するオプションをクリックします。

**ステップ 3** ウィザードを完了します。

フィールドの周囲に赤いボックスが表示されている場合は、フィールドにカーソルを合わせるとエラーメッセージが表示されます。

**ステップ 4** 変更内容を管理対象のデバイスに展開します。

### 次のタスク

- セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開を使用している場合は、「データプレーンイベントログの設定」セクションを使用して、データプレーンイベントの送信を有効にします。
- 7.0 より前のバージョンを実行しているサポート対象のデバイスを Firepower Management Center で管理している場合は、7.0 より前のバージョンを実行している管理対象デバイスの場合は、syslog を使用する （22 ページ）を参照してください。
- イベントが Secure Network Analytics アプライアンスに正常に保存されていることを確認した後、すべてのイベントがリモートからも使用可能な Firepower Management Center に確実に保存されるまでの時間を確保します。次に、Firepower Management Center での優先度が低い接続イベントの保存の停止 （27 ページ）を参照してください。

（注） これらの設定のいずれかを変更する必要がある場合は、ウィザードを再度実行します。設定を無効にするか、またはウィザードを再度実行した場合でも、アカウントのログイン情報を除くすべての設定が保持されます。

## データプレーンイベントログの設定

アプライアンスのプラットフォーム設定ポリシーの UI オプションでデータプレーンロギングを設定します。

（注） データプレーンイベントは、セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。

### 始める前に

- Firepower Management Center の Firepower Management Center でのウィザードの設定を使用して、データプレーンイベントログの Secure Network Analytics への送信を有効にしてください。

### 手順

**ステップ 1** ロギングをイネーブルにします。

a) [Syslog] > [ロギングの設定（Logging Setup）] > [基本ロギング設定（Basic Logging Settings）] に移動します。

b) [Enable Logging] チェックボックスをオンにします。

**ステップ 2** ロギングトラップを設定します。

a) [Syslog] > [ロギング接続先（Logging Destinations）] に移動します。
b) [+ ロギング接続先の追加（+ Add Logging Destination）] をクリックします。
c) [ロギング接続先（Logging Destinations）] で、[Syslogサーバー（Syslog Servers）] を選択します。
d) [イベントクラス（Event Class）] で、[重大度によるフィルタ（Filter on Severity）] を選択します。
e) 重大度を選択します。

**ステップ 3** ロギングファシリティを設定します。

a) [Syslog] > [Syslog設定（Syslog Settings）] > [ファシリティ（Facility）] に移動します。
b) [ファシリティ（Facility）] で、[default = LOCAL4(20)] を選択します。

# 7.0 より前のバージョンを実行している管理対象デバイスの場合は、syslog を使用する

バージョン 6.4 以降を実行しているデバイスを Firepower Management Center で管理する場合は、このドキュメントのウィザードを実行して Firepower Management Center にイベントを表示し、Firepower Management Center から Secure Network Analytics に相互起動をできるようにしてから、7.0 より前の FTD デバイスから セキュリティ分析とロギング（オンプレミス） にイベントを送信するために syslog を使用するように Firepower システムを設定できます。

## 設定の概要：以前のバージョンで FTD デバイスからイベントを送信する

セキュリティ分析とロギング（オンプレミス） に対して Firepower の展開を設定するには、次の手順を実行します。

- ポリシー名やルール名などの Firepower オブジェクト名にカンマが含まれていないことを確認してください。これにより問題が発生する可能性があります。代わりに、ハイフンなど他の特殊文字を使用します。
- Firepower Management Center の管理 IP アドレスと Firepower Threat Defense の管理 IP アドレスをメモします。詳細については、Firepower のマニュアルを参照してください。
- Secure Network Analytics 取り込みアプライアンスの管理 IP アドレスを使用してネットワーク ホスト オブジェクトを作成します。
- UDP 経由で Secure Network Analytics 取り込みアプライアンスに syslog をエクスポートするように Firepower Threat Defense デバイスを設定します。
- オプションで、エクスポートされた syslog を接続、侵入、ファイル、およびマルウェアイベントのみに制限し、パフォーマンスを向上させます。
- アクセス コントロール ポリシーを有効にして syslog に記録します。
- 接続、侵入、ファイル、およびマルウェアイベントの syslog への記録を設定します。

（注） サポートされていないイベントタイプをアプライアンスにエクスポートすると、これらのイベントはドロップされ、保存されません。ただし、イベントでは1秒あたりにエクスポートされたイベント数（EPS）全体をカウントします。エクスポートからこれらのイベントを削除すると、エクスポートされる EPS 全体が減少し、全体的なパフォーマンスが向上します。

（注） 異なるイベントタイプを異なる宛先のsyslogに送信する場合は、シスコサポートにご連絡ください。

## ネットワーク ホスト オブジェクトの作成

### 始める前に

- Firepower Management Center Web インターフェイスに管理者、アクセス管理者、またはネットワーク管理者としてログインします。

### 手順

**ステップ 1** [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] を選択します。

**ステップ 2** オブジェクト タイプのリストから [ネットワーク（Network）] を選択します。

**ステップ 3** [ネットワークを追加（Add Network）] ドロップダウンリストで、[オブジェクトの追加（Add Object）] を選択します。

**ステップ 4** [名前（Name）] に、*csal-sw-appliance* などのオブジェクト名または別のわかりやすい名前を入力します。

**ステップ 5** [説明（Description）] にセキュリティ分析とロギング（オンプレミス） *Secure Network Analytics appliance for event export* のような説明を入力します。

**ステップ 6** [ネットワーク（Network）] フィールドに、マネージャの *eth0* 管理 IP アドレスを入力します。

**ステップ 7** [保存（Save）] をクリックします。

## syslog を Secure Network Analytics にエクスポートするための Firepower Threat Defense 設定の構成

### 手順

**ステップ 1** Firepower Management Center Web インターフェイスで、[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] を選択し、Firepower Threat Defense デバイスに関連付けられた Firepower Threat Defense ポリシーを作成または編集します。

**ステップ 2** 左側のナビゲーションペインで、[Syslog] をクリック。

**ステップ 3** [Syslogサーバー（Syslog Servers）] をクリックし、[追加（Add）] をクリックして新しい syslog サーバー（この場合は Secure Network Analytics アプライアンス）を追加します。

**ステップ 4** [IPアドレス（IP Address）] ドロップダウンリストから *csal-sw-appliance* を選択します。

**ステップ 5** [プロトコル（Protocol）] で *UDP* を選択します。

**ステップ 6** [ポート（Port）] に *8514* と入力します。

**ステップ 7** [到達方法（Reachable By）] で、[デバイス管理インターフェイス（Device Management Interface）] をオンにします。

**ステップ 8** [Syslogの設定（Syslog Settings）] をクリックします。

**ステップ 9** [syslogメッセージのタイムスタンプを有効化（Enable Timestamp on Syslog Messages）] をオンにします。

**ステップ 10** [タイムスタンプ形式（Timestamp Format）] で *RFC 5424 (yyyy-MM-ddTHH:mm:ssZ)* を選択します。セキュリティ分析とロギング（オンプレミス）には RFC 5424 タイムスタンプ形式が必要です。

**ステップ 11** [ロギングのセットアップ（Logging Setup）] をクリックします。

**ステップ 12** [Cisco EMBLEM形式のログメッセージ（UDPのみ）（Log messages in Cisco EMBLEM format (UDP only)）] をオンにします。

## 接続、侵入、ファイル、およびマルウェアイベントのみをエクスポートするための Firepower Threat Defense 設定の構成（オプション）

エクスポートされた syslog を接続、侵入、ファイル、およびマルウェアイベントのみに制限し、1 秒あたりの送信イベント数を制限してパフォーマンスを向上させる場合は、Firepower Threat Defense 設定で syslog イベントリストを構成できます。

（注） 接続、侵入、ファイル、およびマルウェアイベントだけでなくすべてのイベントタイプを送信すると、全体的な EPS が増えるにつれて、アプリケーションがデータをドロップする可能性があります。この場合はログファイルを確認します。詳細についてはトラブルシューティング（41 ページ）を参照してください。

次のメッセージ ID をイベントリストに追加します。

**表 *6*:**

| メッセージ ID | イベント タイプ（Event Type） |
|---|---|
| 430001 | 侵入イベント |
| 430002 | 接続の開始時に記録された接続イベント |
| 430003 | 接続の終了時に記録された接続イベント |

| メッセージ ID | イベント タイプ（Event Type） |
|---|---|
| 430004 | ファイルイベント |
| 430005 | マルウェアイベント |

手順

**ステップ 1** Firepower Threat Defense ポリシーの左側にあるナビゲーションペインで、[Syslog] をクリックします。

**ステップ 2** [イベントリスト（Event Lists）] をクリックします。

**ステップ 3** [追加（Add）] をクリックします。

**ステップ 4** [名前（Name）] に、*SecurityAnalyticsandLogging* などのわかりやすい名前を入力します。スペースは使用できません。

**ステップ 5** [メッセージID（Message ID）] をクリックします。

**ステップ 6** [追加（Add）] をクリックします。

**ステップ 7** [メッセージID（Message ID）] フィールドに *430001-430005* と入力します。

**ステップ 8** [OK] をクリックします。

**ステップ 9** [OK] をクリックします。

**ステップ 10** 設定を**保存**します。

## アクセス コントロール ポリシーごとの syslog エクスポートの有効化

前の手順で設定した Firepower Threat Defense の syslog 設定を使用するように各アクセス コントロール ポリシーを設定します。

手順

**ステップ 1** アクセス コントロール ポリシーで、[ロギング（Logging）] を選択します。

**ステップ 2** [FTD6.3以降:デバイスに展開されているFTDプラットフォーム設定ポリシーで設定されたsyslog設定を使用します（FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device）] をオンにします。

**ステップ 3** [保存（Save）] をクリックします。

## アクセスコントロールルールごとの syslog への接続イベントロギングの有効化

アクセス コントロール ルール レベルで syslog への接続イベントロギングを有効にします。

手順

ステップ 1 Firepower Management Center Web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックし、アクセス コントロール ポリシーを編集します。

ステップ 2 接続イベントロギングを設定するルールの横にある アイコンをクリックします。

ステップ 3 [ロギング（Logging）] タブをクリックします。

ステップ 4 [接続の開始時にロギングする（Log at Beginning of Connection）] または [接続の終了時にロギングする（Log at End of Connection）] を指定します。パフォーマンスを最適化するためには、接続の開始と終了の両方ではなく、どちらか一方をロギングします。

ステップ 5 ファイルイベントをログに記録する場合は、[ファイルのロギング（Log Files）] を選択します。

ステップ 6 [syslog サーバー（Syslog Server）] を有効にします。

ルールが [アクセスコントロールログでデフォルトの syslog 設定を使用する（Using default syslog configuration in Access Control Logging）] であることを確認します。オーバーライドを有効にしないでください。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 syslog への接続イベントロギングを有効にするアクセスコントロールルールごとに、手順 1 ー 6 を繰り返します。

ステップ 9 Firepower の設定が完了したら、[展開する（Deploy）] > [展開（Deployment）] に移動し、ポリシーを管理対象デバイスに展開できます。変更はポリシーを展開するまで有効になりません。設定が完了していない場合は、Firepower 設定を続行します。

## syslog へのファイルおよびマルウェアイベントのロギングを有効化

アクセス コントロール ポリシー レベルでの syslog へのファイルおよびマルウェアイベントのロギングを有効にします。また、各アクセスコントロールルールには、ファイルイベントとマルウェアイベントを生成するためのファイルポリシーが関連付けられている必要があります。

手順

ステップ 1 Firepower Management Center Web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] をクリックし、アクセス コントロール ポリシーを編集します。

ステップ 2 [ロギング（Logging）] タブをクリックします。

ステップ 3 [ファイル/マルウェアイベントのsyslogメッセージを送信する（Send Syslog messages for File and Malware events）] をオンにして、ファイルおよびマルウェアイベントのロギングを有効にします。

ルールが [アクセスコントロールログでデフォルトの syslog 設定を使用する（Using default syslog configuration in Access Control Logging）] であることを確認します。オーバーライドを有効にしないでください。

**ステップ 4** [保存（Save）] をクリックします。

**ステップ 5** ファイルポリシーに関連付けられているアクセスコントロールルールごとに、「アクセスコントロールルールごとの syslog への接続イベントロギングの有効化」の手順に従って、Firepower の展開で syslog にファイルイベントが記録されるようにします。

**ステップ 6** Firepower の設定が完了したら、[展開する（Deploy）] > [展開（Deployment）] に移動し、ポリシーを管理対象デバイスに展開できます。変更はポリシーを展開するまで有効になりません。設定が完了していない場合は、Firepower 設定を続行します。

## syslog への侵入イベントロギングの有効化

侵入ポリシーレベルでの syslog への侵入イベントのロギングを有効にします。また、侵入イベントを生成するには、各アクセスコントロールルールに関連付けられた侵入ポリシーが必要です。

**手順**

**ステップ 1** Web インターフェイスから、[ポリシー（Policies）]>[アクセスコントロール（Access Control）] > [侵入（Intrusion）] の順にクリックして、侵入ポリシーに移動します。

**ステップ 2** ロギングを設定する侵入ポリシーの横にある [編集（Edit）] アイコンをクリックします。

**ステップ 3** [詳細設定（Advanced Settings）] > [Syslogアラート（Syslog Alerting）] > [有効（Enabled）] をクリックします。

**ステップ 4** [戻る（Back）] をクリックします。

**ステップ 5** 左側にあるナビゲーションウィンドウの [ポリシー情報（Policy Information）] をクリックします。

**ステップ 6** [変更を確定（Commit Changes）] をクリックします。

**ステップ 7** 設定が完了したら、[展開する（Deploy）] > [展開（Deployment）] に移動し、ポリシーを管理対象デバイスに展開できます。変更はポリシーを展開するまで有効になりません。設定が完了していない場合は、設定を続行します。

# Firepower Management Center での優先度が低い接続イベントの保存の停止

接続イベントの大部分は、特定された脅威に関連付けられていません。この大量のイベントを Firepower Management Center に保存しないようにすることができます。

Firepower Management Center に保存されていないイベントは、https://www.cisco.com/c/en/us/products/collateral/security/%20firesight-management-center/datasheet-c78-736775.html のデータシートで指定されているように、Firepower Management Center アプライアンスの最大フローレートにカウントされません。

次の接続イベントは優先度が高いと見なされ、接続イベントの保存を無効にした場合でも常に Firepower Management Center に保存されます。

- セキュリティ イベント
- 侵入イベントに関連付けられた接続イベント
- ファイルイベントに関連付けられた接続イベント
- マルウェアイベントに関連付けられた接続イベント

優先度が低い接続イベントを Firepower Management Center に保存しないことで、より多くのストレージスペースを他のイベントタイプに割り当てることができ、脅威を調査するための時間が長くなります。この設定は、統計情報の収集には影響しません。

この設定は、この Firepower Management Center によって管理されているすべてのデバイスからのイベントに適用されます。

### 始める前に

⚠

**注意** この手順により、現在 Firepower Management Center に保存されているすべての接続イベントが直ちに完全に削除されます。

この手順を実行する前に、保持する優先度が低いすべての接続が Secure Network Analytics アプライアンスにすでに存在していることを確認します。通常、Firepower Management Center がイベントを Secure Network Analyticsに正常に送信していることを確認した後、しばらくしてからこのオプションを有効にすることをお勧めします。

### 手順

**ステップ 1** Firepower Management Center での優先度が低い接続イベントの保存を停止する方法は次の 2 つです。

どちらの方法でも同じ効果があります。

- イベントを セキュリティ分析とロギング（オンプレミス） に送信するためのウィザードを完了したら、[システム（System）]>[ロギング（Logging）]>[セキュリティ分析とロギング（Security Analytics and Logging）] に移動し、[FMC で保存するイベントを少なくする（Store Fewer Events on FMC）] オプションを有効にします。
- [システム（System）] > [設定（Configuration）] > [データベース（Database）] に移動し、[接続データベース（Connection Database）] セクションを探して、[最大接続イベント数（Maximum Connection Events）] をゼロ（0）に設定します。

  この値を 0 以外に設定すると、優先度が低いすべての接続イベントが最大フローレートにカウントされます。この設定は接続サマリーには影響しません。

**ステップ 2** 変更を保存します。

---

**次のタスク**

[システム（System）] > [設定（Configuration）] > [データベース（Database）] ページで、他のすべてのイベントタイプのストレージ制限を増やします。

# ASA デバイスの設定

ASA のシステムログにより、ASA デバイスのモニタリングおよびトラブルシューティングに必要な情報が得られます。ASA イベントタイプのリストについては、『Cisco ASA Series Syslog Messages』を参照してください。

（注） ASA イベントストレージは、セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。

セキュリティ分析とロギング（オンプレミス） に、syslog イベントを送信させるには、ASA デバイスでロギングを設定する必要があります。

- ロギングの有効化
- Secure Network Analytics フローコレクタへの出力先の設定

（注） EMBLEM ロギング形式とセキュアロギングは、セキュリティ分析とロギング（オンプレミス）ではサポートされていません。

## ASA デバイスから syslog イベントを送信するための CLI コマンド

セキュリティイベントの syslog メッセージを ASA デバイスから セキュリティ分析とロギング（オンプレミス）に送信するには、次の設定コマンドを使用します。

**始める前に**

- 要件と前提条件のセクションを確認します。
- ASA デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの IP アドレスとポート番号を取得します。

## 手順

**ステップ 1** ロギングを有効にします。

**logging enable**

例：

```
ciscoasa(config)# logging enable
```

**ステップ 2** syslog サーバー（フローコレクタ）に送信する syslog メッセージを指定します。

**logging trap** {*severity_level* | *message_list*}

例：

フローコレクタに送信する syslog メッセージの重大度の値（1 ー 7）または名前を指定できます。

```
ciscoasa(config)# logging trap errors
```

例：

また、フローコレクタに送信する syslog メッセージを特定したカスタムメッセージリストを指定することもできます。

```
ciscoasa(config)# logging list specific_event_list message 106100
ciscoasa(config)# logging list specific_event_list message 302013-302018
ciscoasa(config)# logging trap specific_event_list
```

**ステップ 3** フローコレクタにメッセージを送信するように ASA を設定します。

**logging host** *interface_name syslog_ip* [**protocol**/*port*]

例：

```
ciscoasa(config)# logging host management 209.165.201.3 17/8514
```

（注）
1. syslog_ip と port については、フローコレクタ IP および対応する syslog ポート番号を指定します（手順については、「はじめる前に」を参照）。
2. UDP プロトコルを示すには *17* を指定します。

**ステップ 4** （任意）syslog メッセージのタイムスタンプ形式を設定します。

**logging timestamp** *{rfc5424}*

例：

```
ciscoasa(config)# logging timestamp
```

```
ciscoasa(config)# logging timestamp rfc5424
```

RFC5424 で指定されているタイムスタンプの形式は yyyy-MM-THH:mm:ssZ です（文字 Z は UTC タイムゾーンを示す）。

（注） RFC5424 は、ASA 9.10(1) 以降でのみサポートされています。

**ステップ 5** （任意）syslog メッセージをデバイス ID とともに表示するように ASA を設定します。

**logging device-id** {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id context-name
```

EMBLEM ロギング形式は、この統合ではサポートされていません。そのため、syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

# ASA デバイスから syslog イベントを送信するための ASDM 設定

セキュリティイベントの ASA syslog メッセージを セキュリティ分析とロギング（オンプレミス）に送信するように ASDM を設定するには、次の手順を使用します。

### 始める前に

- 要件と前提条件のセクションを確認します。
- ASA デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの IP アドレスとポート番号を取得します。

### 手順

**ステップ 1** ASDM にログインします。

**ステップ 2** ロギングを有効にします。

a) **[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ロギング（Logging）]** > **[ロギングのセットアップ（Logging Setup）]** をクリックします。

b) [Enable logging] チェックボックスをオンにして、ロギングをオンにします。

（注） この統合は EMBLEM 形式をサポートしていません。そのため、[EMBLEM で syslog を送信（Send syslogs in EMBLEM）] チェックボックスがオフになっていることを確認します。

**ステップ 3** syslog サーバー（フローコレクタ）のロギングフィルタ設定を指定します。

a) **[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ロギング（Logging）]** > **[ロギングフィルタ（Logging Filters）]** を選択します。

b) テーブルから [syslog サーバー（Syslog Servers）] を選択し、[編集（Edit）] をクリックします。

c) [ロギングフィルタの編集（Edit Logging Filters）] ダイアログボックスで、次のいずれかのロギングフィルタ設定を選択します。

重大度に基づいて syslog メッセージをフィルタ処理するには、[重大度によるフィルタ（Filter on severity）] をクリックし、重大度を選択します。

（注） ASA は、指定されたレベルまでの重大度のシステムログメッセージを生成します。

または

メッセージ ID に基づいて syslog メッセージをフィルタ処理するには、[イベントリストの使用（Use event list）] をクリックします。必要な syslog メッセージ ID で作成されたイベントリストを選択するか、[新規（New）] をクリックして、syslog メッセージ ID または ID の範囲でリストを作成することができます。

d) 設定を保存します。

**ステップ 4** フローコレクタのアドレスとポートを使用して外部 syslog サーバーを設定します。

a) **[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ロギング（Logging）]** > **[syslog サーバー（Syslog Server）]** を選択します。

b) [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。

c) [syslog サーバーの追加（Add Syslog Server）] ダイアログボックスで、次を指定します。

- [インターフェイス（Interface）]：syslog サーバーとの通信に使用するインターフェイス。
- [IPアドレス（IP Address）]：マネージャ の Central Management から取得したフローコレクタ IP。
- [プロトコル（Protocol）]：UDP を選択します。
- [ポート（Port）]：対応するフローコレクタの syslog ポート（デフォルトでは 8514）。

（注） UDP を選択した場合は、[メッセージを Cisco EMBLEM 形式でロギング（Log messages in Cisco EMBLEM format）] チェックボックスを使用できます。この統合は EMBLEM 形式をサポートしていません。そのため、このチェックボックスがオフになっていることを確認します。

**ステップ 5** [保存（Save）] をクリックして設定に変更を適用します。

# ASA デバイスから syslog イベントを送信するための CSM 設定

セキュリティイベントの ASA syslog メッセージを セキュリティ分析とロギング（オンプレミス） に送信するように Cisco Security Manager（CSM）を設定するには、次の手順を使用します。

### 始める前に

- 要件と前提条件のセクションを確認します。
- ASA デバイスがフローコレクタに到達できることを確認します。
- マネージャ の Central Management からフローコレクタの IP アドレスとポート番号を取得します。
- EMBLEM ロギング形式とセキュアロギングは、この統合ではサポートされていません。

### 手順

**ステップ 1** Cisco Security Manager の [設定マネージャ（Configuration Manager）] ウィンドウにログインします。

**ステップ 2** syslog ロギングを有効にします。

a) 次のいずれかを実行して [syslog ロギングのセットアップ（Syslog Logging Setup）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングのセットアップ（Logging Setup）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングのセットアップ（Logging Setup）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

b) [syslog ロギングのセットアップ（Syslog Logging Setup）] ページで、[ロギングの有効化（Enable Logging）] チェックボックスをオンにして syslog ロギングをオンにします。[**保存（Save）**] をクリックします。

（注） この統合は EMBLEM 形式をサポートしていません。そのため、[EMBLEM で syslog を送信（Send syslogs in EMBLEM）] チェックボックスがオフになっていることを確認します。

**ステップ 3** syslog サーバー（フローコレクタ）のロギングフィルタ設定を指定します。

a) ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[ロギングフィルタ（Logging Filters）]** を選択します。

b) テーブルの [ロギングの宛先（Logging Destination）] 列で [syslog サーバー（Syslog Servers）] を選択し、[編集（Edit）] をクリックします。syslog サーバーオブジェクトが見つからない場合は、[行の追加（Add Row）] をクリックします。

c) [ロギングフィルタの追加/編集（Add/Edit Logging Filters）] ダイアログボックスで、次のいずれかのロギングフィルタ設定を選択します。

- 重大度に基づいて syslog メッセージをフィルタ処理するには、[重大度によるフィルタ（Filter on severity）] をクリックし、重大度を選択します。

  （注） ASA は、指定されたレベルまでの重大度のシステムログメッセージを生成します。

- メッセージ ID に基づいて syslog メッセージをフィルタ処理するには、[イベントリストの使用（Use event list）] をクリックし、ドロップダウンリストから任意のイベントリストを選択します。

  （注） イベントリストが定義されていない場合、ドロップダウンリストは空白になります。少なくとも 1 つのイベントリストを定義する必要があります（**[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[イベントリスト（Event Lists）]**）。

d) 設定を保存します。

**ステップ 4** （任意）ロギングパラメータを設定します。

a) （デバイスビュー）**[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[Syslog]** > **[サーバーのセットアップ（Server Setup）]** を選択します。

b) syslog メッセージのタイムスタンプ形式を設定するには、[各 syslog メッセージのタイムスタンプの有効化（Enable Timestamp on Each Syslog Message）] チェックボックスをオンにして、[タイムスタンプ形式の有効化（rfc5424）（Enable Timestamp Format(rfc5424)）] チェックボックスをオンにします。

（注） RFC5424 は、ASA 9.10(1) 以降でのみサポートされています。

c) （任意）syslog メッセージをデバイス ID とともに表示するように ASA を設定します。

- [インターフェイス（Interface）]：このオプションボタンをクリックして、ASA デバイスのインターフェイスを選択します。
- [ユーザー定義 ID（User Defined ID）]：このオプションボタンをクリックして、ASA デバイスのすべての syslog メッセージに追加する目的の名前を入力します。
- [ホスト名（Host Name）]：syslog メッセージをデバイスのホスト名とともに表示するには、このオプションボタンをクリックします。

（注） syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

d) [**保存（Save）**] をクリックします。

**ステップ 5** syslog メッセージの宛先となる外部ロギングサーバーを設定します。

a) 次のいずれかを実行して [syslog サーバー（Syslog Servers）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ロギング（Logging）]** > **[syslog サーバー（Syslog Servers）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）]** > **[ロギング（Logging）]** > **[syslog サーバー（Syslog Servers）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

b) [追加（Add）] をクリックして、新しい Syslog サーバーを追加します。

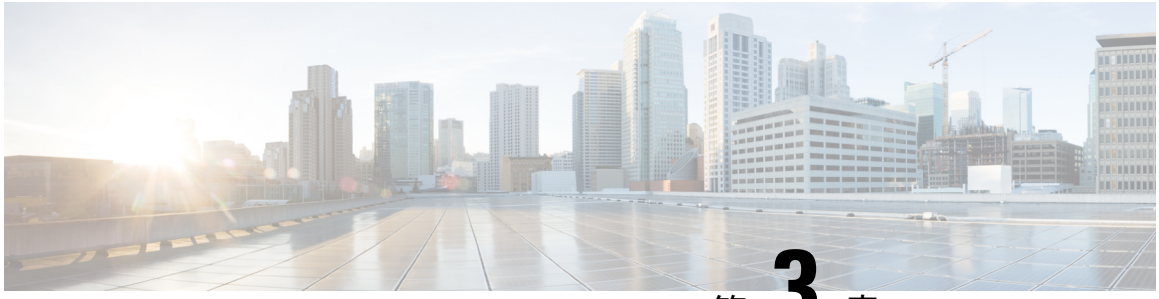
c) [syslog サーバーの追加/編集（Add/Edit Syslog Server）] ダイアログボックスで、次を指定します。

- [インターフェイス（Interface）]：syslog サーバーとの通信に使用するインターフェイス。
- [IPアドレス（IP Address）]：マネージャ の Central Management から取得したフローコレクタ IP。
- [プロトコル（Protocol）]：UDP を選択します。
- [ポート（Port）]：対応するフローコレクタの syslog ポート（デフォルトでは 8514）。

（注） UDP を選択した場合は、[メッセージを Cisco EMBLEM 形式でロギング（Log messages in Cisco EMBLEM format）] チェックボックスを使用できます。この統合は EMBLEM 形式をサポートしていません。そのため、このチェックボックスがオフになっていることを確認します。

d) [OK] をクリックして設定を保存し、ダイアログボックスを閉じます。定義した syslog サーバーが、テーブルに表示されます。

**ステップ 6** 設定の変更を送信して展開します。



第 3 章

# 次のステップ



## 次のステップ

セキュリティ分析とロギング（オンプレミス） の一部として syslog イベントデータを Secure Network Analytics アプライアンスに渡すようにファイアウォール展開を設定したら、次の手順を実行できます。

- Firepower の詳細については、Firepower Management Center のオンラインヘルプを参照してください。
- Secure Network Analytics の詳細については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。

## Secure Network Analytics アプライアンスに保存されている接続イベントを使用した Firepower Management Center での作業

デバイスがセキュリティ分析とロギング（オンプレミス） を使用して Secure Network Analytics アプライアンスに接続イベントを送信している場合、Firepower Management Center のイベントビューアとコンテキストエクスプローラでリモートに保存されたイベントを表示および操作し、レポートの生成時にそれらのイベントを含めることができます。Firepower Management Center のイベントから相互起動して、Secure Network Analytics アプライアンスの関連データを表示することもできます。

デフォルトでは、指定した時間範囲に基づいて適切なデータソースが自動的に選択されます。データソースをオーバーライドする場合は、次の手順を使用します。

**重要** データソースを変更すると、選択した内容は、サインアウト後でも、変更するまでは、イベントデータソース（レポートを含む）に依存するすべての関連する分析機能で維持されます。選択した内容は他の Firepower Management Center ユーザーには適用されません。

選択したデータソースは、優先順位の低い接続イベントにのみ使用されます。他のすべてのイベントタイプ（侵入、ファイル、マルウェアイベント、それらのイベントに関連付けられた接続イベント、およびセキュリティ インテリジェンス イベント）は、データソースに関係なく表示されます。

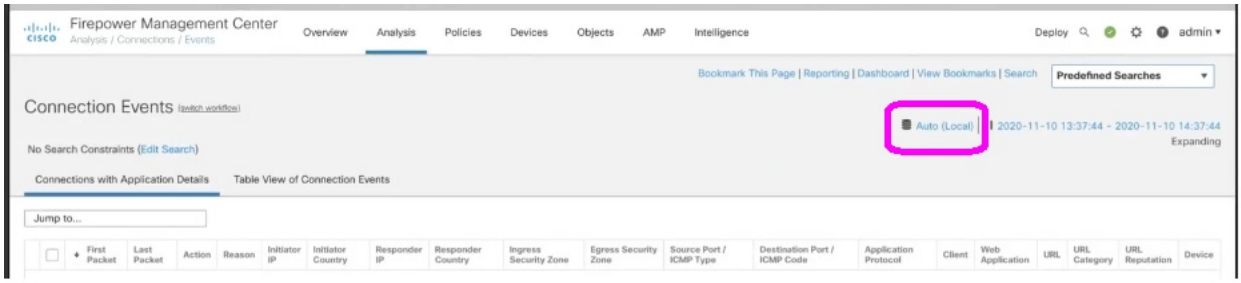
### 始める前に

ウィザードを使用して接続イベントを セキュリティ分析とロギング（オンプレミス） に送信しました。

### 手順

**ステップ 1** Firepower Management Center Web インターフェイスで、接続イベントデータを表示するページ（[Analysis] > [Connections] > [Events] など）に移動します。

**ステップ 2** ページに表示されるデータソースをクリックし、オプションを選択します。




**注意** [Local] を選択すると、ローカルデータが選択した時間範囲全体で使用できない場合でも、Firepower Management Center で使用可能なデータのみ表示されます。この状況が発生していることは通知されません。

**ステップ 3** （任意）Secure Network Analytics アプライアンスで関連データを直接表示するには、IP アドレスやドメインなどの値を右クリック（統合イベントビューアでクリック）し、相互起動オプションを選択します。

# 相互起動を使用したイベントの調査

Firepower Management Center でイベントを表示しているときに、特定のイベントデータ（たとえば、IP アドレス）を右クリックして、マネージャ で関連するデータを表示できます。

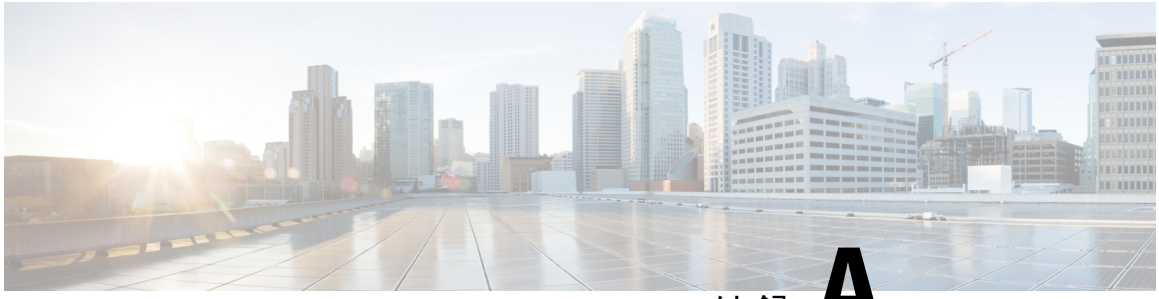
**手順**

**ステップ 1** Firepower Management Center でイベントが表示される次のページのいずれかに移動します。

- ダッシュ ボード（[概要（Overview）] > [ダッシュボード（Dashboards）]）、または
- イベントビューアページ（イベントのテーブルが含まれている [分析（Analysis）] メニューにあるオプション）

**ステップ 2** 対象のイベントフィールドを右クリックして、セキュリティ分析とロギング（オンプレミス）相互起動リソースを選択します。別のブラウザウィンドウに マネージャ が開きます。まだログインしていない場合は、ユーザー名とパスワードの入力を求められることがあります。クエリを実行するデータの量、マネージャ の速度と需要によってはクエリが処理されるまでに時間がかかる場合があります。

**ステップ 3** マネージャ にサインインします。



付録 A

# トラブルシューティング



# トラブルシューティング

### セキュリティ分析とロギング（オンプレミス） 一般的なトラブルシューティング情報

マネージャ VE では、次のログファイルにセキュリティ分析とロギング（オンプレミス）に関連するトラブルシューティング情報が記載されています。

- `/lancope/var/logs/containers/sal.log`：一般的なアプリケーションのロギング情報
- `/lancope/var/logs/sal_preinstall.log`：アプリケーションのインストールプロセスに固有の情報
- `/lancope/var/logs/containers/svc-db-ingest.log`：イベントの取り込みとデータベースに固有の情報

### システム設定/初回セットアップ時の不適切な セキュリティ分析とロギング（オンプレミス） 設定

マネージャ またはフローコレクタでシステムの初期設定を実行するときに初回セットアップウィザードを使用すると、セキュリティ分析とロギング（オンプレミス）用にデータストアと連携するように Secure Network Analytics アプライアンスを設定できます。マネージャ とフローコレクタの両方の選択で [はい（Yes）] を選択する必要があり、そうしないと、Secure Network Analytics 展開にファイアウォールイベント情報が保存されません。

いずれかの選択で [いいえ（No）] を指定した場合、後でこの設定を変更することはできません。アプライアンスを RFD して工場出荷時のデフォルト設定を復元するか、仮想エディションアプライアンスの場合は新しいアプライアンスを展開してセキュリティ分析とロギング（オンプレミス）を適切に設定する必要があります。

### 単一ノード展開時の セキュリティ分析とロギング（オンプレミス）アプリケーション インストールの失敗（管理対象フローコレクタ）

スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと3つのデータノード（マルチノード）を管理するマネージャのインストールがサポートされています。1 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合、マネージャにアプリケーションをインストールすることはできません。この状況でアプリケーションをインストールしようとすると、インストールは失敗します。これが原因であることを確認するには、`/lancope/var/logs/sal_preinstall.log` でログファイルを確認します。次のメッセージまたは同様のメッセージが表示された場合、インストールで管理対象フローコレクタが検出されたことになります。

```
Checking flow collectors...
1 Flow Collector(s) detected
Flow Collector(s) are present in inventory -- aborting installation.
```

アプリケーションをインストールするには、すべての管理対象フローコレクタをCentral Managerのアプライアンスインベントリから削除したうえで再試行してください。

⚠

**注意** セキュリティ分析とロギング（オンプレミス）アプリケーションをアンインストールすると、Firepower イベントデータを含むすべての関連情報が マネージャ から削除され、スタンドアロンの マネージャ 制限も解除されます。セキュリティ分析とロギング（オンプレミス）アプリケーションをアンインストールした後、トラフィックを検査するために、従来の Secure Network Analytics 展開の一部としてスタンドアロン マネージャ で 1 つ以上のフローコレクタを管理できます。

### セキュリティ分析とロギング（オンプレミス）アプリケーションのドロップイベント

アプリケーションは、次のような状況でイベントをドロップすることがあります。

- 接続、ファイル、マルウェア、および侵入イベントだけでなく、すべてのイベントタイプを syslog にエクスポートする
- 平均イベント/秒（EPS）の取り込みレートが 20,000 を超えている
- 期間を延長するためのバースト EPS の取り込みレートが 35,000 を超えている

`/lancope/var/logs/containers/sal.log` ログファイルの情報を確認し、アプリケーションがイベントをドロップしているかどうかを判断します。「`events_dropped`」を含むエントリがないかファイルを検索します。

問題が解消されない場合は、シスコサポートまでお問い合わせください。

### セキュリティ分析とロギング（オンプレミス）アプリケーションのクラッシュ

セキュリティ分析とロギング（オンプレミス）アプリケーションがクラッシュした場合（過剰な取り込みレートを起因とする場合など）、マネージャを再起動します。これにより、アプリケーションも再起動されます。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。