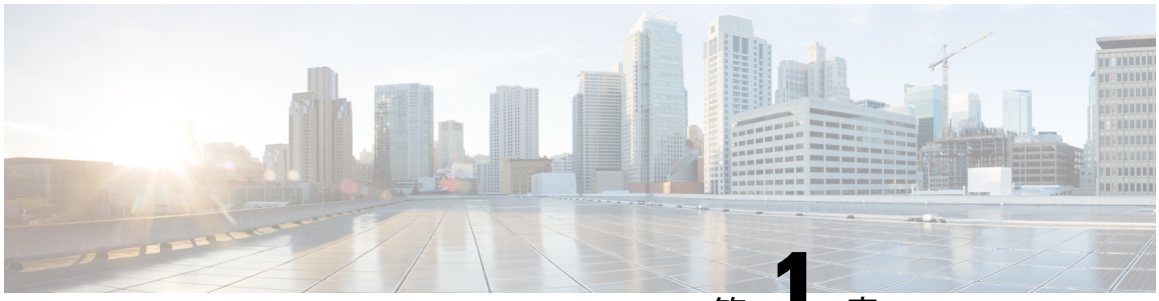
Cisco Security Analytics and Logging（オンプレミス）v3.1 スタートアップガイド

初版：2022 年 4 月 18 日

最終更新：2022 年 4 月 18 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

シスコのセキュリティ分析とロギング（オンプレミス）スタートアップガイド：ファイアウォールイベントの統合

（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）のマニュアルを参照してください。

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） 展開では、Secure Network Analytics アプライアンスを使用して、別のシスコ製品展開からのデータを保存できます。Secure Firewall 展開の場合、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 Management Center が管理する Secure Firewall 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。

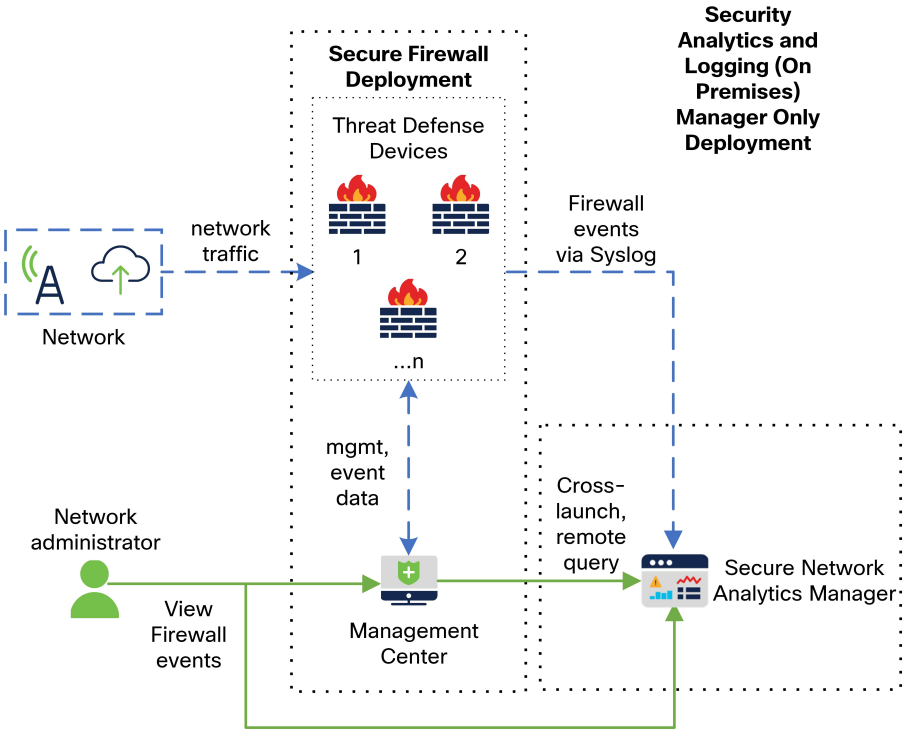
Secure Network Analytics の展開には次の 2 つのオプションがあります。

- マネージャのみ：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。

- データストア：イベントを受信する Cisco Secure Network Analytics フローコレクタ（最大 5 つ）、イベントを保存する Cisco Secure Network Analytics データストア（3 つの Cisco Secure Network Analytics データノードのセットのうち 1 つ、3 つ、またはそれ以上を装備）、イベントを確認および照会できる Manager を展開します。

マネージャのみ

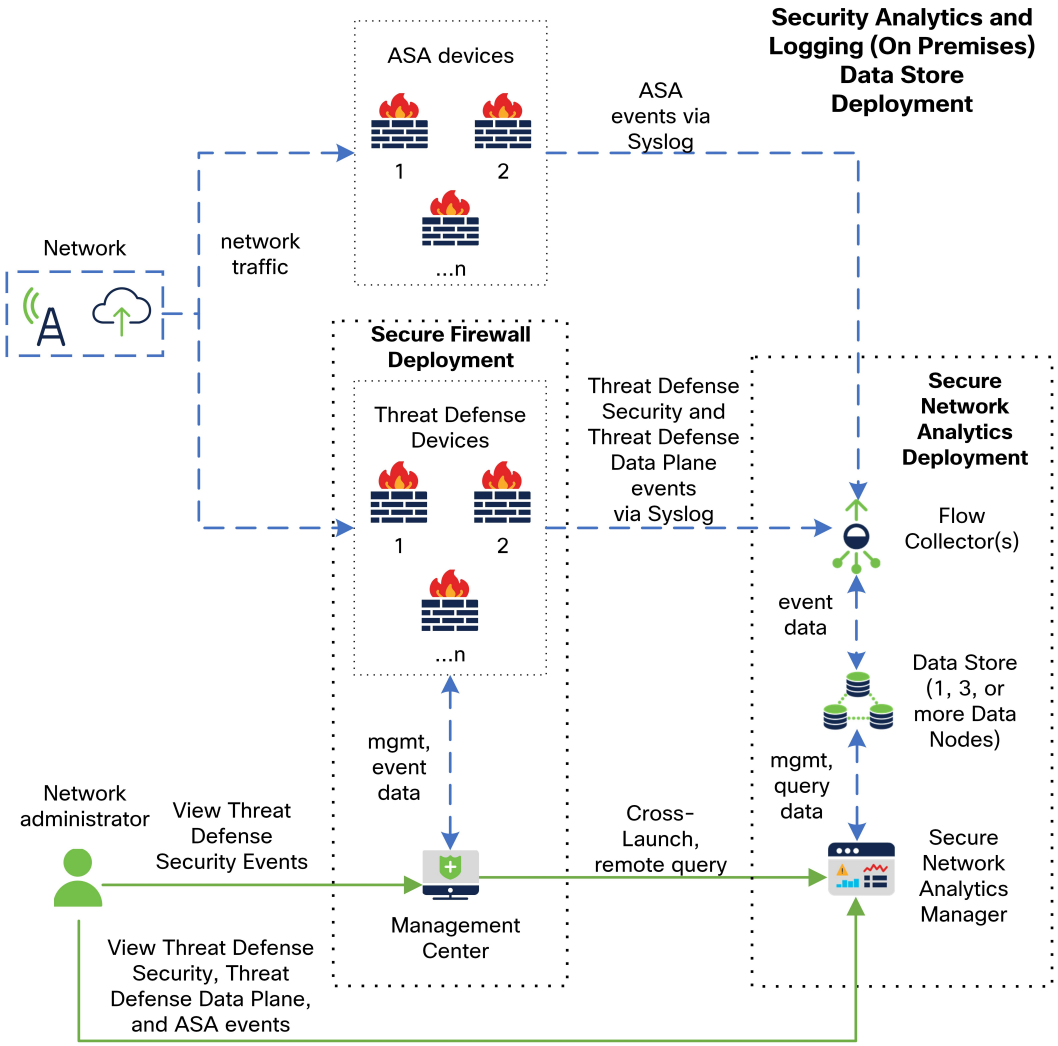
マネージャのみ の展開の例については、次の図を参照してください。



この展開では、Threat Defense デバイスは Secure Firewall 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 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、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。

データストア

マネージャ、データノード、およびフローコレクタを使用した データストア 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、Threat Defense および Secure Firewall 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にイベントを送信します。ユーザは 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、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。

参考資料

次の表に、セキュリティ分析とロギング（オンプレミス）アプライアンスの互換性、展開、使用に関する参照資料を示します。

表 *1:*

ドキュメント	説明
Secure Firewall リリースノート	『Secure Firewall Release Notes』を参照して、最新の Secure Firewall リリースに関する最新情報（直前の情報を含む）を確認してください。
Secure Network Analytics Smart Licensing Guide	Secure Network Analytics の製品インスタンスを登録し、Secure Network Analytics アプライアンスのライセンスを取得する方法については、『Secure Network Analytics Smart Licensing Guide』を参照してください。
Secure Network Analytics Installation Guide	Secure Network Analytics アプライアンスを展開する方法については、『Secure Network Analytics Installation Guide』を参照してください。
Secure Network Analytics Configuration Guide	Secure Network Analytics アプライアンスを設定する方法については、『Secure Network Analytics Configuration Guide』を参照してください。
Secure Network Analytics Release Notes	『Secure Network Analytics Release Notes』を参照して、最新の Secure Network Analytics リリースに関する最新情報（直前の情報を含む）を確認してください。
セキュリティ分析とロギング（オンプレミス）Release Notes	『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、最新のセキュリティ分析とロギング（オンプレミス）リリースおよびセキュリティ分析とロギング（オンプレミス） アプリケーションに関する最新情報（直前の情報を含む）を確認してください。

Secure Firewall をまだ展開していないか、予想される接続、侵入、ファイル、およびマルウェアイベントを生成するように Secure Firewall 展開を設定していない場合は、次を参照してください。

表 *2*：

ドキュメント	説明
Secure Firewall 互換性ガイド	『Secure Firewall Compatibility Guide』を参照し、Secure Firewall Management Center および Secure Firewall Threat Defense のデバイス アプライアンス モデルのバージョンサポートを確認してください。
Secure Firewall のインストールおよびコンフィギュレーション ガイド	Secure Firewall アプライアンスのインストールおよび設定の方法については、Secure Firewall のインストールおよび設定のガイドを参照してください。
Secure Firewall Management Center Configuration Guide	『Secure Firewall Management Center Configuration Guide』を参照して、Secure Firewall アプライアンスのライセンスと、Secure Firewall Management Center によって管理される Secure Firewall Threat Defense デバイス、アクセス コントロール ポリシー、侵入ポリシー、およびファイルポリシーの設定を確認してください。

要件

次に、ファイアウォールのイベントデータを保存するためにセキュリティ分析とロギング（オンプレミス） を展開するためのアプライアンス要件を示します。

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
Management Center（ハードウェアまたは仮想）	v7.2+ 以前のバージョンを実行している 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	• Management Center ごとに 1 つの マネージャ。また、必要に応じて複数のフローコレクタとデータストアを展開できます。

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
Secure Firewall 管理対象のデバイス	v7.0+（ウィザードを使用） Threat Defense v6.4 以降（syslog を使用） NGIPS v6.4（syslog を使用）	なし	• Threat Defense v6.4 以降で syslog を使用する方法については、「以前のバージョンの Threat Defense デバイスからのイベントの送信」を参照してください。
ASA デバイス	v9.12+	なし	

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。

- マネージャのみ：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。
- データストア：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。

表 *3:* マネージャのみ

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 v7.4.0+	なし	• 複数台の 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 Management Center によって管理されます。 • 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）アプリケーション	セキュリティ分析とロギング（オンプレミス） アプリ v3.1+	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 *4:* データストア

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 v7.4.0+	なし	• 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。 • Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリで必要です。

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 v7.4.0+	なし	• データストア用に設定された複数のフローコレクタを展開できます。 • 複数台の 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 Management Center によって管理されます。 • 複数の ASA デバイスから ASA イベントを受信できます。 • Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリで必要です。
データストア	Secure Network Analytics v7.4.0+	なし	• 3 つのデータノードのセットに 1 つ、3 つ、またはそれ以上を展開できます。 • 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。 • Secure Network Analytics v7.4.1 はシングルノードデータストアとマルチテレメトリで必要です。

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
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	セキュリティ分析とロギング（オンプレミス） アプリ v3.1+	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。

Secure Firewall 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 マネージャのみ 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。
- 3 つのデータノードを備えたバーチャルエディション（VE）データストアの展開では、平均で最大約 50k EPS を取り込むことができ、最大 175k EPS の短いバーストが可能です。
- 3 つのデータノードを備えたハードウェア データストア 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。

マネージャのみ 推奨事項

マネージャ VE リソース

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

マネージャ 2210 仕様

ハードウェアの仕様については、マネージャ 2210 仕様書を参照してください。

推定保持期間

マネージャ VE に割り当てるストレージスペースに基づいて、または マネージャ 2210 を使用している場合は、マネージャのみのみの展開でおおよそ次の時間枠のデータを保存できます。

平均 EPS	平均日次イベント	1TB ストレージの推定保持期間	2TB ストレージの推定保持期間	4 TB ストレージ（ハードウェア）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 2 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。

データストア 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。

（注） シングルノードデータストアを使用している場合、または Secure Network Analytics でマルチテレメトリを有効にしている場合、リソースの割り当てとストレージ容量は次の推奨事項と異なる場合があります。詳細については、「Secure Network Analytics アプライアンスの設置ガイド（ハードウェアまたはバーチャルエディション）とシステム コンフィギュレーション ガイド v7.4.1」を参照してください。

表 *5*: マネージャ *VE*

リソース	推奨
CPU	8
RAM	64 GB
ハードドライブストレージ	480 GB

表 *6*: *Flow Collector VE*

リソース	推奨
CPU	8
RAM	70 GB
ハードドライブストレージ	480 GB

表 *7*: 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	データノードあたり 12
RAM	データノードあたり 32 GB

リソース	推奨
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

ハードウェア仕様

ハードウェアの仕様については、アプライアンスの仕様書を参照してください。

推定保持期間（3 つのデータノード）

データストア VE に割り当てるストレージスペースに基づいて、またはハードウェア展開がある場合は、データストア 展開でおおよそ次の時間枠でデータを保存できます。

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日間	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。ストレージ容量を増やすには、Secure Network Analytics システム コンフィギュレーション ガイドを使用してデータノードを追加します。

（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。データノードのストレージ割り当てを 5 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

次の表にマネージャのみ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。

表 *8*：マネージャのみ

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
Management Center、Threat Defense デバイス、およびマネージャ	外部インターネット（NTP サーバー）	123/UDP	すべて同じ NTP サーバへの NTP 時刻同期
ユーザーワークステーション	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
Management Center によって管理される Threat Defense デバイス	マネージャ	8514/UDP	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
Management Center	マネージャ	443/TCP	Management Center から マネージャ へのリモートクエリ

次の表にデータストア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 展開のために開く必要があるポートについては、「x2xx シリーズ ハードウェアアプライアンス設置ガイド」または「Virtual Edition アプライアンス インストール ガイド」を参照してください。

表 *9*：データストア

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
Management Center、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	外部インターネット（NTP サーバー）	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	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

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
Management Center によって管理される Threat Defense デバイス	Flow Collector	8514/UDP	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	8514/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
Management Center	マネージャ	443/TCP	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、ファイアウォールイベントの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
マネージャのみ の導入	次の選択肢があります。 • 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 Appliance Installation Guide』と『Secure Network Analytics System Configuration Guide』を参照してください。 • 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 Appliance Installation Guide』と『Secure Network Analytics System Configuration Guide』を参照してください。

コンポーネントとタスク	手順
データストア の導入	• マネージャ、フローコレクタ、および1、3、またはそれ以上（3つのセット）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 Appliance Installation Guide』、『Virtual Edition Appliance Installation Guide』および『Secure Network Analytics System Configuration 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	• アプリファイル、app-smc-sal-3.1.0-v2.swu を https://software.cisco.com からダウンロードします。 • 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インストールします。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。
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 Secure Firewall Management Center を設定	次の選択肢があります。 • イベントを Secure Network Analytics アプライアンスに送信するように Secure Firewall Management Center を設定します。 • 『Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide』の『*Configure Secure Firewall Management Center to Send Data Plane Event Logs to Secure Network Analytics using Syslog*』セクションを使用してデータプレーンイベントログを設定します。 • 「Stop Storing Low-Priority Connection Events on the Secure Firewall Management Center」を使用して、Secure Firewall 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	• 『*Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide*』 の『ASA Devices Configuration』 セクションを使用して、Secure Network Analytics アプライアンスにイベントを送信するように ASA デバイスを設定します。

コンポーネントとタスク	手順
次の手順の確認	次の手順を確認します。 • 詳細については、Secure Firewall のオンラインヘルプを参照してください。『Cisco Security Analytics and Logging (On Premises) v3.1: Firewall Event Integration Guide』の「*Work in the Management Center with Connection Events Stored on a Secure Network Analytics Appliance*」セクションを参照してください。 • 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。

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。

- Management Center オンラインヘルプを確認します。
- 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。