展開前

セキュリティ分析とロギング（オンプレミス）を展開する前に、『Getting Started with Security Analytics and Logging Guide』および『Security Analytics and Logging On Premises: Firewall Event Integration Guide』を確認してください。

重要 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 でのアプリケーションのインストール、または Cisco Secure Network Analytics フローコレクタ NetFlow 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。

バージョンの互換性

次の表に、セキュリティ分析とロギング（オンプレミス）の展開でファイアウォールのイベントデータの保存に Secure Network Analytics の使用が必要なソリューションのコンポーネントの概要を示します。

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	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+ 以前のバージョンを実行している FMC 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 Cisco Secure Network Analytics データストア（データノード X 3）を展開できます。
Firepower 管理対象のデバイス	v7.0+（ウィザードを使用） FTD v6.4+（syslog を使用） NGIPS v6.4	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。

- 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。 • 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。 • 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。 • イベントを取り込んで Secure Network Analytics 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。 • 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。
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。 • 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。

ソフトウェアのダウンロード

次の点に注意してください。

- **パッチ**：アップグレードする前に、アプライアンスに最新のロールアップパッチをインストールしていることを確認してください。Cisco Software Central（https://software.cisco.com）の Cisco スマートアカウントからファイルをダウンロードできます。
- **ファイルのダウンロード**：

1. 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。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ソフトウェアのダウンロード（Software Download）] を選択します。
3. [セキュリティ（Security）] > [Network Visibility and Segmentation（ネットワークの可視性とセグメンテーション）] > [Secure Analytics（Stealthwatch）] > [Secure Network Analytics仮想マネージャ（Secure Network Analytics Virtual Manager）] > [アプリケーション - Security Analytics and Loggingオンプレミス（App - Security Analytics and Logging On Prem）] を選択します。
4. Security Analytics and Logging オンプレミス アプリケーション ファイル app-smc-sal-2.0.2.swu をダウンロードします。

サードパーティ製アプリケーション

アプライアンスへのサードパーティ製アプリケーションのインストールはサポートしていません。

ブラウザ

Firepower と Secure Network Analytics は、Google Chrome および Mozilla Firefox の最新バージョンをサポートしています。