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（マネージャのみ）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 Cisco Secure Network Analytics データノード（データストア）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。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
Secure Firewall 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。
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	• 脅威に対する防御 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 *1:* 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 v7.4.2	なし	• 複数台の 脅威に対する防御 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。 • イベントの取り込みのために セキュリティ分析とロギング（オンプレミス） アプリをインストールし、マネージャでファイアウォールイベントを表示させてください。
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	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 v3.2.0	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、イベントの取り込みを有効にするように設定します。

表 *2:* 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 v7.4.2	なし	• イベントの取り込みのために セキュリティ分析とロギング（オンプレミス） アプリをインストールし、マネージャでファイアウォールイベントを表示させてください。
Flow Collector	Secure Network Analytics v7.4.2	なし	• データストア用に設定された最大 5 つのフローコレクタを展開できます。 • 複数台の 脅威に対する防御 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。
データストア	Secure Network Analytics v7.4.2	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。

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）アプリケーション v3.2.0	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、イベント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。

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-3.2.0-v2.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

Secure Firewall および 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。

翻訳について
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。