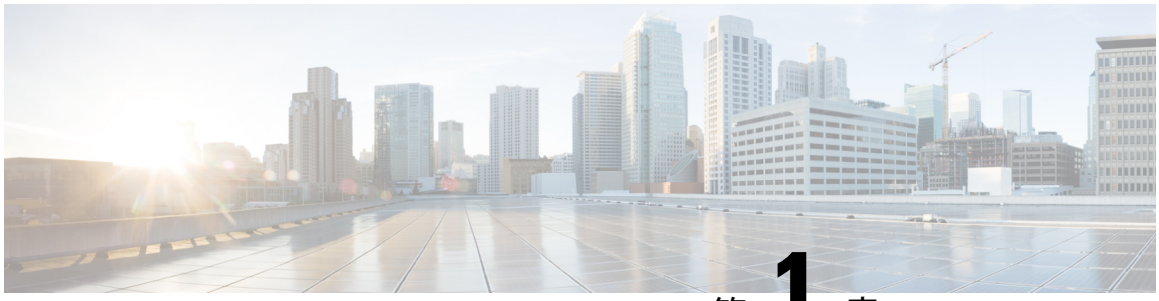
Cisco Security Analytics and Logging（オンプレミス）v2.0.2 リリースノート

初版：2021 年 5 月 26 日

最終更新：2021 年 12 月 20 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

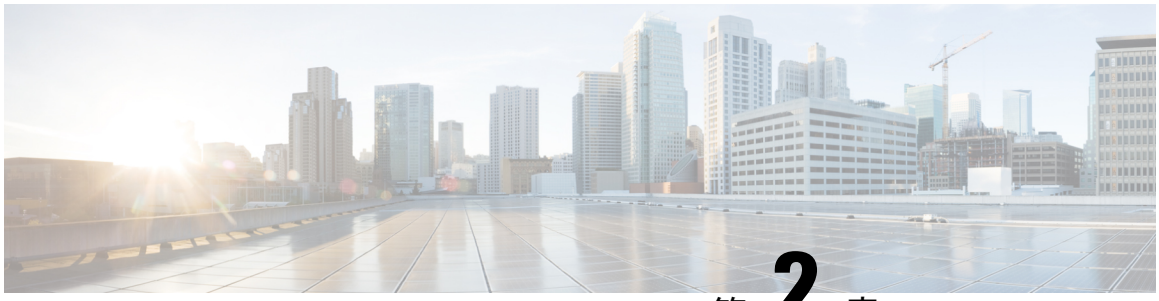
はじめに

概要

このドキュメントでは、シスコのセキュリティ分析とロギング（オンプレミス）v2.0.2 の新機能と改善点、バグ修正、および既知の問題について説明します。詳細については、cisco.com をご覧ください。

用語

このガイドでは、Cisco Secure Network Analytics Manager（旧 Stealthwatch 管理コンソール）Virtual Edition などの仮想製品を含むすべてのファイアウォールまたは Cisco Secure Network Analytics（旧 Stealthwatch）製品に対し「アプライアンス」という用語を使用しています。



第 2 章

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**：

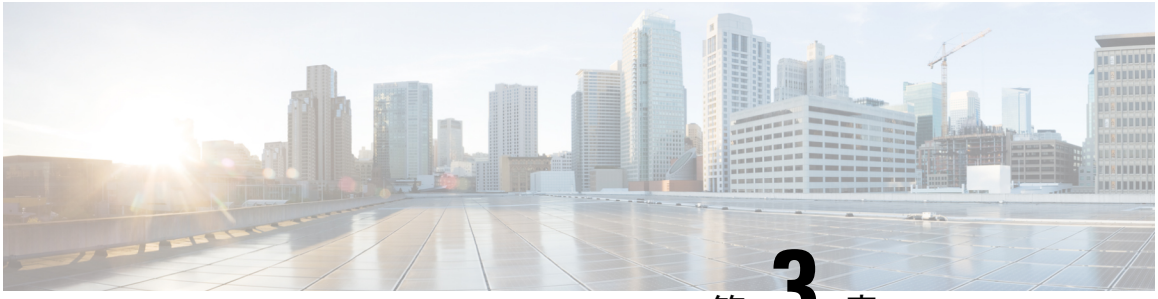
1. https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。
2. [ダウンロードとアップグレード（Download and Upgrade）] セクションで、[ソフトウェアのダウンロード（Software Download）] を選択します。
3. [セキュリティ（Security）] > [Network Visibility and Segmentation（ネットワークの可視性とセグメンテーション）] > [Secure Analytics（Stealthwatch）] > [Secure Network 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。



第 3 章

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

Central Management のアプリケーションマネージャを使用して セキュリティ分析とロギング（オンプレミス） をインストールします。ブラウザは Chrome または Firefox を使用することをお勧めします。

1. マネージャ にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [集中管理（Central Management）] を選択します。
4. [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。
5. [参照（Browse）] をクリックします。
6. 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。

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 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。

- Secure Network Analytics とアプリケーションの互換性 （9 ページ）
- リソース使用状況 （11 ページ）

Secure Network Analytics とアプリケーションの互換性

Secure Network Analytics の更新の際、現在インストールされているアプリケーションは保持されます。ただし、アプリケーションと新しい Secure Network Analytics バージョンとの間に互換性がない場合があります。Secure Network Analytics の特定のバージョンでサポートされるアプ

リケーションのバージョンを確認するには、『Secure Network Analytics Apps Version Compatibility Matrix』を参照してください。

マネージャにインストールできるアプリケーションのバージョンは1つのみです。インストール済みのアプリケーションを管理するには、[アプリケーションマネージャ（App Manager）] ページを使用します。このページから、アプリケーションのインストール、更新、アンインストール、またはステータスの確認を実行できます。確認可能なアプリケーションのステータスについては、以下の表を参照してください。

より新しいバージョンのアプリケーションがあっても [アプリケーションマネージャ（App Manager）] に表示されないことがあるため、必ず Cisco Software Central で新しいバージョンがないかどうかを確認してください。

重要 アプリケーションを新しいバージョンに更新するには、新しいバージョンを既存のバージョンにそのままインストールします。既存のアプリケーションをアンインストールする必要はありません。セキュリティ分析とロギング（オンプレミス）をアンインストールすると、一時ファイルやファイアウォール イベント データなど、関連付けられているすべてのファイルが削除されます。

表 3:

ステータス	定義	対処
UpToDate	インストール済みのアプリケーションは最新バージョンです。	特に対処の必要はありません。
UpdateAvailable	新しいバージョンの Secure Network Analytics にアップグレードしています。既存のアプリケーションは、このバージョンの Secure Network Analytics でサポートされていますが、このアプリケーションの新しいバージョンがあります。	必要な場合は、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（これにより既存のバージョンが置き換えられます）。
UpgradeRequired	新しいバージョンの Secure Network Analytics にアップグレードしましたが、既存のアプリケーションは、現在使用している Secure Network Analytics バージョンでサポートされていません。	このアプリケーションを引き続き使用するには、Cisco Software Central にアクセスして最新バージョンのダウンロードとインストールを行ってください（既存のバージョンが置き換えられます）。

ステータス	定義	対処
AppNotSupported	新しいバージョンの Secure Network Analytics にアップグレードしています。このアプリケーションは、現在使用しているバージョンの Secure Network Analytics でサポートされなくなる可能性があります。このアプリケーションが廃止されたか、このアプリケーションの新しいバージョンがまだリリースされていない可能性があります。	新しいバージョンがリリースされたかどうかを確認するには、Cisco Software Central に移動します。
NewApp	これは新しいアプリケーションです。	必要な場合は、Central Manager を使用してこの新しいアプリケーションをインストールしてください。
Error	関連付けられているアプリケーションのインストール、アップグレード、または削除プロセスが正常に完了しませんでした。	Secure Network Analytics サポートに連絡してください（サポートの連絡先情報については、本書の最後のセクションを参照）。このアプリケーションが、部分的にインストール、アップグレード、または削除された可能性があります。その場合は修正が必要です。

Secure Network Analytics アプリケーションのバージョンに関する詳細については、『Secure Network Analytics Apps Version Compatibility Matrix』を参照してください。

リソース使用状況

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

- マネージャ が次の場合にのみ展開できます。
  - フローコレクタを管理しない、または
  - フローコレクタと 3 つのデータノードを管理している
- インストールには次のディスク容量が必要です。
  - `/lancope`：50 MB

- `/lancope/var`：10 MB（このディスク容量は開始点であり、システムにデータが蓄積されるにつれて消費量が増加することに注意）
- イベントを保持するために推奨されるディスク容量の詳細については、『Security Analytics and Logging (On Premises): Firewall Event Integration Guide』を参照してください。1 TB、2 TB、および 4 TB のディスクストレージを持つ マネージャ に対し、イベント保持のテストを実行済みです。

ディスク使用状況の統計を確認する

アプライアンスのディスク使用状況の統計情報を取得するには、次の手順を実行します。

始める前に

- Secure Network Analytics Web アプリケーションに管理者としてログインします。

手順

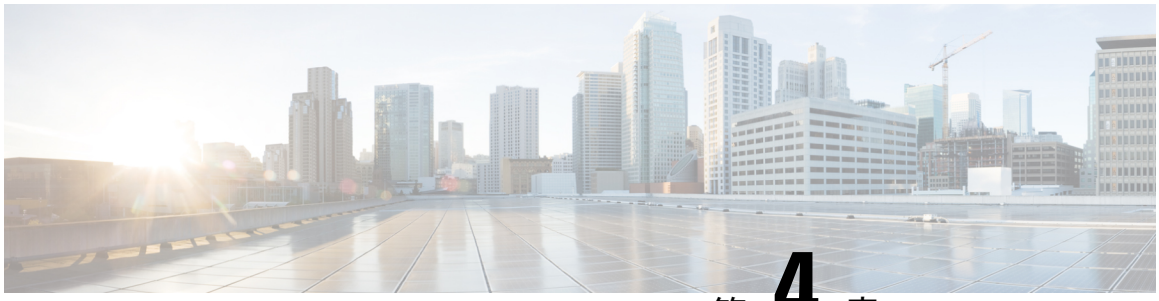
ステップ 1 [グローバル設定（Global Settings）] アイコンをクリックし、ドロップダウンメニューから [集中管理（Central Management）] を選択します。

ステップ 2 [アプライアンスマネージャ（Appliance Manager）] タブをクリックします。

ステップ 3 アプライアンスの [アクション（Actions）] メニューをクリックし、コンテキストメニューから [アプライアンス統計情報の表示（View Appliance Statistics）] を選択します。

ステップ 4 プロンプトが表示されたら、アプライアンス管理インターフェイスにログインします。

ステップ 5 [ディスク使用量（Disk Usage）] セクションまでスクロールします。



第 4 章

新機能

現在のシスコのセキュリティ分析とロギング（オンプレミス）リリースの新機能と改善点は次のとおりです。

新機能

Secure Network Analytics データストアによる拡張ストレージ

拡張されたFirepowerイベントストレージ容量のために、ハードウェアまたは仮想Secure Network Analytics データストアおよびフローコレクタを Secure Network Analytics Manager で展開できるようになりました。Secure Network Analytics アプライアンスを展開するときは、初回セットアップ時に、データストアで展開するために、および シスコのセキュリティ分析とロギング（オンプレミス）展開の一部として使用するためにアプライアンスを構成することができます。

重要 Secure Network Analytics Manager またはフローコレクタを シスコの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。この設定は、Secure Network Analytics を シスコのセキュリティ分析とロギング（オンプレミス） に使用して Firepower イベント情報を保存する場合にのみ有効にしてください。

統合の詳細については『Security Analytics and Logging (On Premises): Firewall Event Integration Guide』、データストアを使用した Secure Network Analytics ハードウェアの展開の詳細については『Install Version 7.3.x with Hardware Appliances』、データストアを使用した仮想 Secure Network Analytics アプライアンスの展開の詳細については『Install Version 7.3.x with Virtual Appliances』を参照してください。

Firepower Management Center からのリモートクエリ

Firepower Management Center から Secure Network Analytics 内に保存されているイベントをクエリできるようになりました。この構成の詳細については『Security Analytics and Logging (On Premises): Firewall Event Integration Guide』、リモートクエリ機能の詳細については Firepower Management Center OLH を参照してください。

Firepower Management Center の構成ウィザード

Firepower Management Center のウィザードを使用して、すべての Firepower Management Center ユーザーにシスコのセキュリティ分析とロギング（オンプレミス）を設定できるようになりました。ウィザードの使用方法の詳細については、『Security Analytics and Logging (On Premises): Firewall Event Integration Guide』を参照してください。

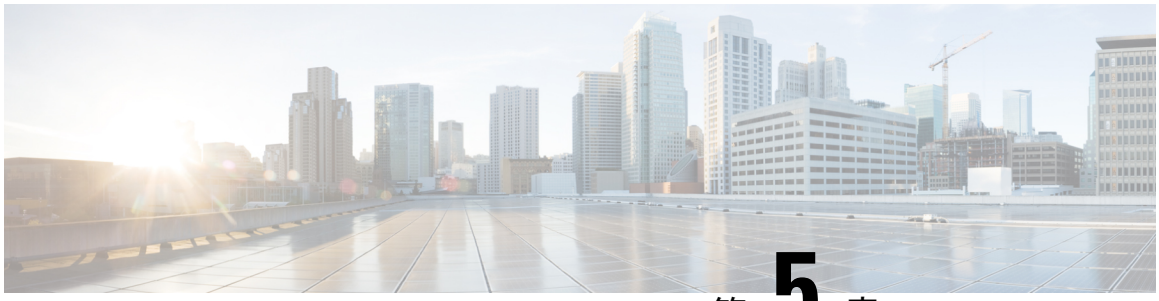
イベントビューアの検索

シスコのセキュリティ分析とロギング（オンプレミス）アプリのイベントビューアで、イベント内の文字列を検索して、特定のイベントをより迅速に見つけることができるようになりました。

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
  - Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
  - 電子メールでケースを開く場合：tac@cisco.com
  - 電話でサポートを受ける場合：1-800-553-2447（米国）
  - ワールドワイドサポート番号：https://www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_ contacts.html



第 5 章

解決済みの問題と既知の問題

解決済みの問題

表 *4 : v2.0.2*

障害	説明
LVA-2811	Apache Log4J 2 を v2.15 に更新しました。

表 *5 : v2.0.1*

障害	説明
SWONE-14331	Firepower がファイルイベントとマルウェアイベントに対して誤った SyslogID を断続的に送信していた問題を修正しました。
SWONE-15345	単一ノード展開での Firepower からのタイムスタンプの処理が更新されました。

既知の問題

v2.0.2

なし

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。