Cisco Secure Network Analytics

リリースノート 7.4.0

目次

はじめに

概要

このドキュメントでは、Cisco Secure Network Analytics（旧 Stealthwatch）v7.4.0 リリースの新機能と改善点、バグ修正、および既知の問題について説明します。Secure Network Analytics の詳細については、Cisco.com をご覧ください。

再ブランディング

Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。注目すべきその他の主な変更点は、Stealthwatch Management Console が Cisco Secure Network Analytics Manager になったことです。完全なリストについては、次の表を参照してください。

以前のブランディング	新しいブランディング 初出時	新しいブランディング 2 度目以降
Cisco Stealthwatch Cloud	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud プライベート ネットワーク モニタリング	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Stealthwatch Cloud パブリック クラウド モニタリング	Cisco Secure Cloud Analytics	Secure Cloud Analytics
Cisco Stealthwatch Enterprise または Cisco Stealthwatch	Cisco Secure Network Analytics	Secure Network Analytics
Cisco Stealthwatch データノード	Cisco Secure Network Analytics データノード	データノード
Cisco Stealthwatch データストア	Cisco Secure Network Analytics データストア	データストア
暗号化トラフィック分析（ETA）	暗号化トラフィック分析	暗号化トラフィック分析
Stealthwatch エンドポイントライセンス	Cisco Secure Network Analytics エンドポイントライセンス	エンドポイントライセンス
Stealthwatch Flow Collector	Cisco Secure Network Analytics Flow Collector	Flow Collector

以前のブランディング	新しいブランディング 初出時	新しいブランディング 2 度目以降
Stealthwatch Flow Collector データベース（FCDB）	Cisco Secure Network Analytics Flow Collector データベース	Flow Collector データベース
Stealthwatch Flow Collector NetFlow（FCNF）	Cisco Secure Network Analytics Flow Collector NetFlow	Flow Collector（NetFlow）
Stealthwatch Flow Collector sFlow（FCSF）	Cisco Secure Network Analytics Flow Collector sFlow	Flow Collector（sFlow）
Stealthwatch Flow Sensor（FS）	Cisco Secure Network Analytics Flow Sensor	フローセンサー
Stealthwatch Management Console（SMC）	Cisco Secure Network Analytics Manager	マネージャ
Stealthwatch Cloud センサー	Cisco Secure Cloud Analytics センサー	センサー
Stealthwatch 脅威インテリジェンスフィードまたは脅威インテリジェンスライセンス	Cisco Secure Network Analytics 脅威フィード	脅威フィード
UDP Director	Cisco Secure Network Analytics UDP Director	UDP Director

用語

このガイドでは、Secure Network Analytics Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 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。

「**クラスタ**」は、マネージャによって管理される Secure Network Analytics アプライアンスのグループです。

更新する前に

更新プロセスを開始する前に、『Update Guide』を確認してください。

ソフトウェア バージョン

アプライアンスソフトウェアをバージョン 7.4.0 に更新するには、アプライアンスにバージョン 7.3.0、7.3.1、または 7.3.2 がインストールされている必要があります。以下の点にも注意してください。

- **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**：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。[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。[セキュリティ(Security)] > [ネットワークの可視性とセグメンテーション(Network Visibility and Segmentation)] > [**Secure Network Analytics**] の順に選択します。

- **アプライアンス ソフトウェア バージョンの段階的更新**:たとえば、Secure Network Analytics v7.1.x を使用している場合は、各アプライアンスを v7.1.x から v7.2.x に更新した後、v7.2.x を v7.3.2 に更新します。各更新ガイドは、Cisco.com で入手できます。
- ダウングレード:更新すると、更新時にインストールされる新機能をサポートするために必要な変更がデータ構造や設定に対して行われるため、バージョンのダウングレードはサポートされていません。
- **TLS**:Secure Network Analytics TLS v1.2 が必要です。
- **サードパーティ製アプリケーション**:Secure Network Analytics は、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をサポートしていません。

サポートされているハードウェア プラットフォーム

各システム バージョンでサポートされているハードウェア プラットフォームについては、Hardware and Version Support Matrix を参照してください。

CIMC ファームウェアバージョン

共通の更新プロセスまたはハードウェアに固有の共通の更新パッチを使用して、CIMC ファームウェアバージョンを必ず更新してください。

次の表に示すアプライアンスの場合、M4 に共通の更新プロセスは UCS C シリーズ M4 ハードウェアに適用され、共通の更新パッチは M5 ハードウェアに適用されます。

M4 ハードウェア	M5 ハードウェア
SMC 2220	SMC 2210
FC 4200	FC 4210
FC 5020 エンジン	_
FC 5020 データベース	_
FC 5200 エンジン	FC 5210 エンジン
FC 5200 データベース	FC 5210 データベース
FS 1200	FS 1210
FS 2200	_
FS 3200	FS 3210
FS 4200	FS 4210、FS 4240
UD 2200	UD 2210

証明書チェック

v7.4.0 への更新には、シスコのバンドルに共通の更新によって使用中の環境に問題が発生しないことを確認するため、証明書チェックが含まれています。証明書を使用している場合は、証明書の完全なチェーンが（個別のファイルとして）Central Management の信頼ストアに存在することを確認します。信頼ストアにエンドエンティティ証明書のみがある場合は、アップグレードは失敗します。

シスコのバンドル

最新のシスコのバンドルに共通の更新パッチがインストールされていることを確認してください。詳細については、Cisco Bundles Common Update Patch の readme を参照してください。このパッチでは

- 厳選したルート認証局（CA）の事前検証済みのデジタル証明書を提供しています。これには、
- シスコのサービスとの接続に使用するコア証明書バンドルと、シスコ以外のサービスとの接続に使用する外部証明書バンドルが含まれます。

高可用性

UDP Director で高可用性が構成されていて、Secure Network Analytics を v7.4.0 に更新する予定の場合は、更新を開始する前に、UDP Director の高可用性設定を必ず書き留めておいてください。更新が完了したら、高可用性を再構成する必要があります。Secure Network Analytics の更新の詳細については、更新ガイドを参照してください。

サードパーティ製アプリケーション

Secure Network Analytics は、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をサポートしていません。

ブラウザ

- **互換性のあるブラウザ**：Secure Network Analytics は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。
- **Microsoft Edge**：Microsoft Edge には、ファイル サイズの制限がある可能性があります。Microsoft Edge を使用して、ソフトウェア アップデート ファイル（SWU）をアップロードしないことをお勧めします。
- **ショートカット**：ブラウザのショートカットを使用して、いずれかの Secure Network Analytics アプライアンスのアプライアンス管理インターフェイスにアクセスしている場合、更新プロセスの完了後はショートカットが機能しないことがあります。その場合は、ショートカットを一旦削除してから再作成してください。
- **証明書**：一部のブラウザでは、アプライアンス アイデンティティ証明書の有効期限の要件が変更されています。アプライアンスにアクセスできない場合は、『SSL/TLS Certificates for Managed Appliances Guide』を参照して証明書を置き換えるか、Cisco サポートまでお問い合わせください。

代替アクセス

> ⚠ 今後のサービスのニーズを想定し、Secure Network Analytics アプライアンスにアクセスする代替方法を有効にしておく必要があります。

次のいずれかのオプションを使用して Secure Network Analytics アプライアンスにアクセスできることを確認してください。

仮想アプライアンス：コンソール（コンソールポートへのシリアル接続）

KVM を介してアプライアンスにアクセスするには、Virtual Manager のドキュメントを参照してください。または、VMware を介してアプライアンスに接続するには、vSphere の vCenter Server Appliance 管理インターフェイスのドキュメントを参照してください。

ハードウェア：コンソール（コンソールポートへのシリアル接続）

ラップトップまたはモニター付きキーボードを使用してアプライアンスに接続するには、「インストールとアップグレードガイド」ページにリストされている最新の『Secure Network Analytics Hardware Installation Guide』を参照してください。

ハードウェア：CIMC（UCS アプライアンス）

CIMC を介してアプライアンスにアクセスするには、『Cisco Integrated Management Controller (CIMC) Configuration Guides』 ページにリストされているプラットフォームの最新のガイドを参照してください。

別の方法

今後サービスが必要になった場合に備えて、次の手順に従い、Secure Network Analytics アプライアンスにアクセスする別の方法を有効にします。

仮想またはハードウェアの方法を使用してアプライアンスにログインできない場合は、アプライアンスのネットワーク インターフェイスで一時的に SSH を有効にできます。

> ⚠ SSH を有効にすると、システムの侵害リスクが増加します。必要な場合にのみ SSH を有効にし、使用が終了したら無効にすることが重要です。

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. アプライアンスの [アクション（Actions）] メニューをクリックします。
5. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
6. [アプライアンス（Appliance）] タブを選択します。
7. [SSH] セクションを見つけます。
8. SSH アクセスのみを有効にするか、ルートアクセスも有効にするかを選択します。

    - [SSHの有効化（Enable SSH）]：アプライアンスへの SSH アクセスを許可するには、このチェックボックスをオンにします。
    - [ルートSSHアクセスの有効化（Enable Root SSH Access）]：アプライアンスへのルートアクセスの有効化を許可するには、このチェックボックスをオンにします。

9. [設定の適用（Apply settings）] をクリックします。
10. 画面に表示される指示に従って、変更を保存します。

> ⚠ SSH は、使用が終了したら必ず無効にしてください。

新着情報

Secure Network Analytics v7.4.0 リリースの新機能と改善点は次のとおりです。

証明書の失効

Manager アプライアンスの ID 証明書が 60 日以内に期限切れになる場合、Secure Network Analytics のログインページに警告が表示されます。証明書の有効期限が切れると、システムにアクセスできなくなります。証明書の有効期間を変更するか、証明書を置き換えるには、『管理対象アプライアンスの SSL/TLS 証明書ガイド』を参照してください。

DoDIN およびコモンクライテリアへの準拠

米国国防総省情報ネットワーク(DoDIN)またはコモンクライテリア(CC)に準拠するように Secure Network Analytics を設定するには、『DoDIN Military Unique Deployment Guide』または『Common Criteria Administrative Guide』の手順に従ってください。『Stealthwatch コンプライアンスガイド』の公開は終了しました。

診断パック

[診断パック(Diagnostics Pack)] メニューをアプライアンス管理インターフェイスからアプライアンスコンソールの [システム設定(System Configuration)] に移動しました。診断パックがあると、Cisco サポートによる問題のトラブルシューティングが必要な場合に役立ちます。v7.4.0 のアプライアンスの診断パックを作成するには、『System Configuration Guide』の指示に従ってください。

Flow Collector データベースのパスワード

[集中管理(Central Management)] ページの [データベース(Database)] タブを選択して、すべての Flow Collector データベースのデフォルトパスワードを変更できるようになりました。Flow Collector データベースのデフォルトパスワードを変更することをお勧めします。

> このオプションは、Data Store 展開の Flow Collector ではサポートされていません。

セッション設定

ユーザーセッションの最大時間は 12 時間です。12 時間後、ユーザーはログインし直す必要があります。この設定は変更できません。

[保護されたセッションタイムアウト(Protected Sessions Time-Out)] では、[管理者専用機能(Administrator-Only Functions)] またはユーザーの非アクティブ時間を 12 時間を超えるように設定できます。ただし、設定によって、システム全体のユーザーセッションのタイムアウトが変更されることはありません。12 時間後、ユーザーはログインし直す必要があります。

Cisco Security Analytics and Logging(オンプレミス)

> セキュリティ分析とロギング(オンプレミス) の以前のバージョンをアンインストールしないでください。アンインストールすると、既存のデータが削除されます。

システムを v7.4.0 に更新した後、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) v3.0.0 にアップグレードしてください。アプリの以前のバージョンは、v7.4.0 と互換性がありません。アップグレードしないと セキュリティ分析とロギング(オンプレミス) にアクセスできません。

セキュリティ分析とロギング（オンプレミス）機能拡張には次のようなものがあります。

- **マルチノード**：マルチノードソリューションは、FTD、ASA、または NGIPS デバイスから ASA イベントを収集して分析します。
- **イベントビューア**：イベントビューアを使用すると、エクスポートするデバイスタイプ（FTD、ASA、または NGIPS）に基づいて ASA イベントをフィルタリングできます。
- イベントタイプ：[イベントタイプ（Event Type）] 列では、ASA イベントをフィルタリングできます。
- **ASA 固有のイベント**：ASA イベントに固有の列を使用して、ASA イベントを検索できます。

セキュリティ分析とロギング（オンプレミス）展開の詳細については、次のドキュメントを参照してください。

- Cisco Security Analytics and Logging（オンプレミス）のリリースノート
- Cisco Security Analytics and Logging（オンプレミス）スタートアップガイド
- オンプレミスにおける Cisco Security Analytics and Logging：Firepower イベント統合ガイド

レポートビルダー

レポートビルダーを別個のアプリから v7.4.0 のコア Secure Network Analytics に移動しました。アプリは、v7.4.0 へのアップデートの一部として自動的に削除されます。

> ⚠ 既存の レポートビルダー アプリケーションはアンインストールしないでください。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。

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。レポートビルダー をアンインストールすると、保存済みのレポートや一時ファイルを含めて、関連付けられているすべてのファイルが削除されます。レポートビルダー の既存のアプリは削除しないでください。更新ガイドの手順に従ってください。

Secure Network Analytics を v7.4.0 に更新すると、以前のバージョンと同じ場所にあるレポートビルダーのダッシュボードにアクセスできます。

1. Manager にログインします。
2. [ダッシュボード（Dashboards）] メニューを選択します。
3. [レポートビルダー（Report Builder）] を選択します。

サーバーの ID 検証

v7.4.0 では、TLS 接続に対してより厳格なセキュリティチェックが追加されました。これには、追加の証明書要件が含まれる場合があります。すべての新しい構成について、指示に従っていることを確認してください。

- **監査ログの宛先**：ヘルプの手順に従います。（[ユーザ（User）]）アイコン を選択して [監査ログの宛先（Audit Log Destination）] を検索します。
- **シスコISEまたは Cisco ISE-Pic**：『ISE and ISE-PIC Configuration Guide』の手順に従います。また、関連情報については、「**厳密な ISE サーバー ID 検証**」を参照してください。
- **応答管理に対する SMTP の設定**：ヘルプの指示に従ってください。（[ユーザ（User）]）アイコン を選択して「SMTP 構成」を検索します。

サーバー ID 検証：更新の準備

v7.4.0 への更新の一部として、次の構成を見直して、それらがサーバー ID 検証の要件を満たしていることを確認します。

- [監査ログの保存先（TLS経由のSyslog）（Audit Log Destination（Syslog over TLS））]
- SMTP 構成（応答管理の電子メール通知）

更新を開始する前に、構成を確認してください。構成が要件を満たしていない場合、更新は失敗します。詳細については更新ガイドを参照してください。

監査ログの宛先の要件

更新の前に、監査ログの宛先構成が**次の両方の要件**を満たしていることを確認してください。

- Syslog over TLS をサポートする syslog サーバーからのルート認証局（CA）SSL 証明書がアプライアンスの信頼ストアに含まれていることを確認します。監査ログの宛先が構成されている各アプライアンスの信頼ストアを確認します。
- syslog サーバーの ID 証明書の [サブジェクト（Subject）] フィールドまたは [サブジェクトの別名（Subject Alternative Name）] フィールドに syslog サーバーの IP アドレスが含まれていない場合は、アドレスを監査ログの宛先が構成されている各アプライアンスの信頼ストアに追加します。

信頼ストアにアクセスするには、マネージャ にログインします。[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] を選択します。アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン をクリックします。[アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。[全般（General）] タブを選択し、[信頼ストア（Trust Store）] セクションまでスクロールします。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

SMTP 設定の要件

更新の前に、SMTP 設定が**次の要件のいずれか**を満たしていることを確認してください。

- 認証局（CA）からの SMTP サーバー ID 証明書に、Secure Network Analytics で設定した IP アドレスまたはホスト名と一致する [サブジェクト（Subject）] または [サブジェクトの別名（Subject Alternative Name）] があることを確認します。**または**
- マネージャの信頼ストアに SMTP サーバー ID 証明書を追加します。

マネージャ 信頼ストアにアクセスするには、マネージャ にログインします。[グローバル設定（Global Settings）] アイコン > [集中管理（Central Management）] を選択します。マネージャ の ••• （[省略記号（Ellipsis）]）アイコンをクリックします。[アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。[全般（General）] タブを選択し、[信頼ストア（Trust Store）] セクションまでスクロールします。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

厳密な ISE サーバー ID 検証

Manager が Cisco Identity Services Engine（ISE）または Cisco Identity Services Engine Passive Identity Connector（ISE-PIC）クラスタノードと通信するときにサーバー ID 検証を要求するには、厳格な ISE サーバー ID 検証を有効にします。

他のセキュリティチェックに加えて、ISE サーバー ID 証明書が次のいずれかを満たす場合は、通信を許可します。

- これには、共通名またはサブジェクト代替名としてリストされている pxGrid ノード名または ID 情報（FQDN など）が含まれます。または、
- Manager の信頼ストア内の証明書と一致します。

以前のバージョンから Secure Network Analytics を更新する場合は、この設定を有効にすることを選択できます。Secure Network Analytics の新しいバージョンをインストールすると、この設定はデフォルトで有効になります。

この設定を有効または無効にするには、[展開（Deploy）] > [Cisco ISE設定（Cisco ISE Configuration）] を選択します。詳細については、『ISE and ISE-PIC Configuration Guide』を参照してください。

Secure Network Analytics アプリケーション（Apps）

Secure Network Analytics は、Secure Network Analytics の機能を強化および拡張する、独自にリリース可能なオプションの機能です。

Secure Network Analytics アプリケーションのリリーススケジュールは、通常の Secure Network Analytics のアップグレードプロセスとは無関係です。そのため、Secure Network Analytics のコアリリースとリンクさせなくても、必要に応じて Secure Network Analytics アプリケーションを更新できます。Secure Network Analytics の新しいリリースに対応するように設計されたアプリが、すぐにインストールできない場合があります。アプリケーションの最新バージョンが提供されるまでに数週間かかる場合もあります。

最新の Secure Network Analytics アプリケーションの情報と可用性については、次を参照してください。

- Secure Network Analytics アプリケーションのバージョン互換性マトリクス
- Secure Network Analytics アプリケーションのリリースノート

Analytics ベータ版

v7.4.0 の時点で、Analytics ベータ版は、Data Store で展開されたシステムでのみ機能します。Data Store のないシステムで Analytics ベータ版を実行していて、v7.4.0 以降にアップグレードすると、システムで Analytics ベータ版を使用できなくなります。

[アラートの詳細（Alert Details）] ページと [アラート設定（Alerts Settings）] ページで、MITRE ATT&CK の戦術および手法のタグを確認できるようになりました。

アラーム抑制

アラーム属性に基づいて、悪意のないことが予想される既知のデバイス間の既知の通信に対してルールを設定できるようになりました。通信がルール基準（ポート、プロトコル、IP アドレスなど）に一致すると、Analytics で通常生成されるアラームを抑制し、ノイズが少なく効果的なシステムになります。

> 構成のバックアップを実行すると、アラート抑制リストが含まれます。

単一の Flow Collector イメージに対する NetFlow および sFlow のサポート

netFlow と sFlow に単一の Flow Collector イメージを設定できるようになりました。これにより、モードを NetFlow から sFlow に、または sFlow から NetFlow に切り替えることができます。

Data Store でのデータ圧縮の有効化

データ圧縮を有効にして、Flow Collector と Data Store 間の帯域幅使用量を削減できるようになりました。これは、Flow Collector から Data Store へのネットワーク帯域幅が制限されているシナリオで特に便利です。圧縮を有効にすると、この帯域幅使用量を最大 90% 削減できます。

Data Store の導入オプション

Data Store を使用した Secure Network Analytics に対し、排他的なハードウェア導入または仮想の導入に加えて、v7.4.0 では、ハードウェアと仮想の混合導入オプションも提供されます。v7.4.0 以降、Secure Network Analytics では DS6200 ハードウェア Data Store で、仮想 マネージャ と Flow Collector の組み合わせがサポートされるようになりました。

すべてのアプライアンスに同じバージョンの Secure Network Analytics がインストールされていることを確認し、選択した展開のドキュメントを確認してください。開始する前に、すべての要件を理解することが重要です。

- **ハードウェアと Virtual Edition（VE）アプライアンスの組み合わせ**
- **ハードウェアアプライアンスのみ**
- **Virtual Edition（VE）アプライアンスのみ**

ハードウェアと Virtual Edition（VE）アプライアンスの組み合わせ

以下のガイドを使用して、マネージャ VE および Flow Collector VE を使用した Data Store 6200 の導入を行います。

手順	ドキュメント	説明
準備	リリース ノート	最新の Data Store 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。
準備	Data Store 6200 仕様シート	物理的なレイアウトと機能を確認します。
1.	x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド	物理ハードウェアアプライアンス（ラック、ケーブルなど）をインストールします。
2.	『Data Store 仮想エディション導入および構成ガイド』	マネージャ VE を導入して構成します。「**Manager Configuration for Use with a Data Store**」セクションを参照してください。 • リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。 • アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。

3.	『x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド』 および『Data Store Hardware Deployment and Configuration Guide』	各 Data Node を展開して構成します。 「**Data Node の設定**」セクションの指示に従って、Data Node 間通信ポート設定を構成してください。 展開の考慮事項と前提条件については、『Data Store Hardware Deployment and Configuration Guide』を参照してください。
4.	『Data Store 仮想エディション導入および構成ガイド』	Flow Collector VE を導入して構成します。「**Flow Collector Configuration for Use with a Data Store**」セクションを参照してください。 • リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。 • アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。
5.	『Data Store 仮想エディション導入および構成ガイド』	Data Store を初期化します。「**Data Store の初期化と設定**」セクションを参照します。 フローインターフェイス統計の保持と Data Store の圧縮を設定します。
6.	スマート ライセンシング ガイド	評価期間（90 日間）が終了する前に、Secure Network Analytics 展開とアプライアンスのライセンスを取得します。

ハードウェアアプライアンスのみ

次のガイドを使用して、Data Store 6200 を使用して Secure Network Analytics ハードウェアを導入します。

手順	ドキュメント	説明
準備	リリース ノート	最新の Data Store 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。
準備	ハードウェアおよびソフトウェア バージョンのサポート マトリックス	Data Store で使用できる Manager および Flow Collector アプライアンスモデルを確認します。
準備	アプライアンスの仕様シート	アプライアンスの物理的なレイアウトと機能を確認します。

1.	x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド	Manager、Data Store、および Flow Collector ハードウェアをインストールします。
2.	『x2xx シリーズ ハードウェア（Data Store 付属）アプライアンス設置ガイド』 および『Data Store Hardware Deployment and Configuration Guide』	『Data Store Hardware Deployment and Configuration Guide』に示されている順序でアプライアンスを構成します（「**Data Store Installation**」セクションを参照）。 1. マネージャ 2. Data Node：Data Node 間の通信ポート設定を構成するための指示に従っていることを確認してください。 3. Flow Collector 4. Data Store を初期化します。 5. フローインターフェイス統計の保持と Data Store の圧縮を設定します。 ハードウェアのインストールと初回セットアップの詳細については、『x2xx ハードウェア（Data Store 付き）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。 アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。
3.	スマート ライセンシング ガイド	評価期間（90 日間）が終了する前に、Secure Network Analytics 展開とアプライアンスのライセンスを取得します。

Virtual Edition（VE）アプライアンスのみ

次のガイドを使用して、Data Store Virtual Edition とともに Secure Network Analytics Virtual Edition をデプロイします。

手順	ドキュメント	説明
準備	リリース ノート	最新の Data Store 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。
1.	『Data Store 仮想エディション導入および構成ガイド』 および『Virtual Edition (with Data Store) Appliance Installation Guide』	『Data Store Virtual Edition の導入および設定ガイド』に示されている順序でアプライアンスを導入および設定します（「**Data Store の設置**」セクションを参照）。 1. マネージャ VE 2. Data Node：Data Node 間の通信ポート設定を構成するための指示に従っていることを確認してください。

		3. Flow Collector VE 4. Data Store を初期化します。 5. フローインターフェイス統計の保持と Data Store の圧縮を設定します。 リソース要件、ISO の展開、および初回セットアップの詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。 アプライアンス設定ツールの詳細については、『System Configuration Guide』を参照してください。
2.	スマート ライセンシング ガイド	評価期間(90 日間)が終了する前に、Secure Network Analytics 展開とアプライアンスのライセンスを取得します。

サポートへのお問い合わせ

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:800-553-2447(米国)
  - ワールドワイド サポート番号:
    www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

修正点

このセクションでは、旧リリースでお客様から報告された問題（バグ/不具合）に関してこのリリースで行われた修正点の概要を示します。参照用に、Secure Network Analytics 問題（SWD または LSQ）番号が示されています。

バージョン 7.4.0

障害	説明
SWD-15701	カスタム緩和スクリプトを無効にしようとすると発生する NullExceptionPointer の問題を修正しました。（LSQ-5159）
SWD-16053	ドキュメントからエンドポイント コンセントレータへの参照を削除しました。（LSQ-5930）
SWD-16075	スマートライセンスが強化されました。（LSQ-5431）
SWD-16087	フローベースのアイデンティティがユーザーレポートにありません。
SWD-16183	ルールに DPI 定義がある場合、Secure Network Analytics カスタムアプリケーションがトラフィックにタグ付けしない問題を修正しました。（LSQ-5456）
SWD-16206	ASA フローのバイトカウントが 0 クライアントバイトを示し、NAT 送信元アドレスを表示することに関連する問題を修正しました。（LSQ-5320）
SWD-16217	ファイル /etc/udev/rules.d/70-persistent-net.rules が空であることに起因する v7.2.1 Flow Sensor コンソールでの segfault エラーの問題を修正しました。
SWD-16296	idgen から生成された ID が失われる問題を修正しました。
SWD-16314	v7.3.0 でエクスポータレベルでの sFlow のフロー検索が結果を返さない問題を修正しました。（LSQ-5508）
SWD-16340	「関連付けられたフロー」検索で IP アドレスまたはプロトコルがフィルタリングされない問題を修正しました。
SWD-16366	次の内容をドキュメントに追加しました：デフォルトの Data Store の保持期間は 7 日ではありません。
SWD-16369	偵察アラームの再発生に関する Syslog メッセージを修正しました。（LSQ-5527）
SWD-16396	dpdk の使用時に、エクスポータの eth0 の MTU に関連するフローセンサーの問題を修正しました。

障害	説明
SWD-16401	カスタム緩和スクリプトを無効にしようとすると SMC NullExceptionPointer で発生する問題を修正しました。(LSQ-5159)
SWD-16413	クライアントポート 443 を使用したコグニティブレポートの TLS TCP (HTTPS)トラフィックに関連する問題を修正しました。
SWD-16416	セキュリティイベントの発生率が特に高いことに起因する、アーカイブ時間後に「スレッドが中断されました」というメッセージが表示される v7.3.1 Flow Collector エンジンの問題を修正しました。
SWD-16417	セキュリティイベントの発生率が特に高いことに起因する、「host_flow_condition」の v7.3.1 Flow Collector エンジン SIGSEGV の問題を修正しました。
SWD-16428	v7.3.0 および v7.3.1 の SNMP ポーリングが保留状態で停止し、何日も、場合によっては何週間も結果が返されない問題を修正しました。(LSQ-5521、LSQ-5496)。
SWD-16432	Flow Sensor が誤った FlowSensorInitiator 要素を送信することがある問題を修正しました。
SWD-16441	ベースラインデータファイルがバックアップから除外されました。(LSQ-5617)
SWD-16453	すべての内部ホストグループのデフォルトポリシーと、[ホストがターゲットの場合(When Host Is Target)] 設定を無効にするとどうなるかを文書化しました。
SWD-16489	v7.3.1 のライセンスファイルがないと、[プロキシの取得(Proxy Ingest)] オプションがグレー表示される問題を修正しました。(LSQ-5624)
SWD-16503	Flow Collector データベースの Vertica Backup Restore(VBR)がサポートされていないことを明確にするようにドキュメントを更新しました。(LSQ-5636)
SWD-16576	order-by フローで CDS TopConversations のデフォルトのクエリが失敗する問題を修正しました。
SWD-16588	SecureX ユーザーロールが SecureX リボンにアクセスできない問題を修正しました。
SWD-16626	AVC サブアプリケーション値フィールドと 1 バイトの TCP フラグフィールドを処理する際のデコードエラーの問題を修正しました。

障害	説明
SWD-16629	各アラームタイプに関連する syslog 変数に関する詳細を含むようにドキュメントを更新しました。
SWD-16635	解決可能な ISE ノードの ISE 統合の前提条件を含むようにドキュメントを更新しました。
SWD-16647	Web UI のフロー検索の高度なパラメータの使用に関するドキュメントコンテンツを追加しました。
SWD-16669	Webhook URL が 200 文字に制限されることを示す情報を UI に追加しました。
SWD-16844	認証クエリ方法のパフォーマンスに関連する LDAP タイムアウトの問題を修正しました。（LSQ-5652）
SWD-16902	ドメインに関するより詳細なコンテンツを含めるように、Cognitive Analytics 構成ガイドを更新しました。

既知の問題

このセクションでは、このリリースに存在する既知の問題（バグ）について概要を示します。可能な場合には、回避策も示しています。参照用に問題番号が示されています。

障害	説明	回避策
LVA-719	Active Directory ルックアップ設定パスワードは、設定ファイルにクリアテキストで保存されます。	**詳細**：パスワードは、ローカルファイルシステム、アプライアンス管理インターフェイスのファイルブラウザ（管理者の資格情報が必要）、および暗号化されていないバックアップ設定ファイルでアクセスできます。 **緩和オプション**：Active Directory ルックアップを設定する場合： • ユーザーアカウントの権限を制限し、アカウントの誤用を監視します。 • バックアップ設定ファイルを暗号化します。ヘルプの「バックアップ設定の暗号化」を参照してください。 Active Directory ルックアップを無効にする場合： • Active Directory ルックアップ設定を削除します。Manager で [展開（Deploy）] > [Active Directory] に移動します。 • 暗号化されていないバックアップ設定ファイルを削除します。ヘルプの「バックアップ設定の暗号化」および「バックアップ設定ファイル」を参照してください。
SWD-12574	ユーザーがログイン試行に失敗せずにコマンドライン インターフェイスにログインすると、エポック日付（1970 年 1 月 1 日）が表示される場合があります。	現在使用可能なものはありません。
SWD-13964	データベースの復元に、暗号化された設定のバックアップは含まれません。	doDbRestore コマンドに `-r` を追加し、設定のバックアップを復元せずにデータベースの復元を実行してから、暗号化されたバックアップを手動で復元します。

障害	説明	回避策
SWD-14057	マネージャ アプライアンス管理では、[パケットキャプチャ(Packet Capture)] ページは空白になります。	パケットキャプチャは マネージャ アプライアンス管理から削除されました。別の方法:[ヘルプ(Help)] > [ヘルプ(Help)] を選択し、マネージャ パケットキャプチャの手順に従います。
SWD-14855	Firefox を使用している場合、手順 6 でフローセンサー AST が表示されない場合があります。この場合、Central Management にアプライアンスを追加します。	別のブラウザを使用してください。Firefox を使用している場合は、キャッシュをクリアしてページを更新します。
SWD-15002	設定の復元が RFD 後に失敗します。	アプライアンスを工場出荷時のデフォルトにリセットすると、Central Management を使用して設定を復元できません。サポートが必要な場合は、シスコサポートまでお問い合わせください。
SWD-16183	DPI 定義を使用したカスタム アプリケーション ルールはトラフィックにタグ付けしないため、フロー検索のアプリケーション名には、カスタムアプリケーション名の代わりに HTTPS(未分類)が表示されます。	現在使用可能なものはありません。
SWD-16223	スマートライセンスで、複数の予約のうち 1 つしか表示されません。	現在使用可能なものはありません。
SWD-16226	Web UI のエクスポータ SNMP で、認証パスワードとプライバシーパスワードがプレーンテキストで保存されます。	現在使用可能なものはありません。
SWD-16346	非アクティブなエクスポータの誤ったステータスがエンジンから返されます。	現在使用可能なものはありません。

障害	説明	回避策
SWD-16378	ダッシュボードおよびレポートの Data Node に関するシステムアラームが、正しい問題を示していない場合があります。タイムフレームの表示（ボックスの右上）に、Data Node がダウンしてからの実際の経過時間よりもはるかに短い時間が表示されることがあります。 [詳細を表示（View Details）] を選択し、[システムレポートの表示（View System Report）] を選択すると、過去 30 日間のアラームが表示されます。	システムレポートでは、[アラーム（Alarm）] 列の上部にある [検索（Search）] ボックスを使用して、特定のアラームの説明を入力できます。次に、[日時（Date/Time）] 列でソートして、特定のアラームの最も古いものや最新のものを確認できます。 また、カレンダーから [日（Day）] を選択し、[次の値より前（Is Before）] で [検索（Search）] アイコンの値を選択して、発生した最初の日を検索することもできます。
SWD-16382	FMC のユーザーが IP サブネットフィルタ（10.10.1.0/24）を指定すると、Data Store クエリサービスバックエンドでクエリが失敗します。	ipRange 比較演算子を使用すると、FMC で回避策が利用可能になります。ただし、コードの変更が必要であり、アーキテクチャまたはリリースのタイミングによっては実行できない場合があります。
SWD-16383	SAL CONNECTION_END_EVENT last_packet_second の計算に問題があります。	現在使用可能なものはありません。
SWD-16408	ISE クライアントが、非 UTC タイムゾーンを含むユーザーセッションを解析しません。	回避策は、ISE を UTC 時間に設定することです。
SWD-16733	SWUv2 は、Data Store の更新プロセスを変更します。	データノードファイナライザ SWU を適用する前に、SMC が更新されるまで待ってください。必要なダウンタイムに懸念がある場合は、シスコサポートにお問い合わせください。
SWD-16781	Cisco ISE（Identity Services Engine）にアクセスすると、「接続ステータス：失敗（Connection Status: Failed）」メッセージが表示されます。	v7.4.0 に更新する前に、ISE の証明書チェーンが完全であることを確認してください。詳細については、『Cisco Secure Network Analytics ISE and ISE-PIC Configuration Guide 7.4』の 5 ページから始まる「Option 1 – Deploying Certificates Using ISE Internal Certificate Authority (Recommended)」セクションを参照してください。手動同期を実行し

障害	説明	回避策
	ログに「サービス `<service name>` がこの `ISE` クラスタで見つかりません `(Service <service name> cannot be found on this ISE Cluster)`」が表示される場合は、ISE 統合が空のサービスリストで失敗したことを示しています。	て、ISE のレプリケーションアラームの問題も修正してください。 **注**：詳細については、ISE トラブルシューティング テクニカルノートの記事「Troubleshoot Secure Network Analytics – ISE Integration "Connection Failed – Service Cannot Be Found On This ISE Cluster"」を参照してください。 v7.4.0 に更新済みで、このメッセージが表示された場合は、シスコサポートにお問い合わせください。
SWD-16858	v7.3.0 から更新すると、Data Store システム上の SMC が Data Store データベースを停止します。	dbadmin ユーザーとして、Data Node でデータベースを手動で再起動します。 `admintools -t start_db -d sw -p <dbadmin password>`
SWD-16862	SWUv1 ファイナライザパッチは SWUv2 ファイナライザの代わりに使用されていると、アップグレードをブロックします。	間違ったパッチのインストールが失敗した後、正しいパッチをインストールします。
SWD-16929	ISE が 8,192 バイトを超えるメッセージを受信すると、pxGrid 2.0 で ISE セッションを受信するためのバッファサイズが不十分なため、ISE セッションのトピックが通常どおりに機能しません。	現在利用可能なものはありませんが、パッチが計画されています。
NA	FlowSensor VE では、[アプリケーション識別情報のエクスポート（Export Application Identification）] はデフォルトでオフになっています。	アプリケーション識別を有効にするには、詳細設定を手動で選択する必要があります。

ログの変更

リビジョン	改訂日	説明
1_0	2021 年 9 月 30 日	最初のバージョン。
2_0	2021 年 11 月 2 日	一般提供（GA）。
2_1	2021 年 11 月 18 日	「Data Store でのデータ圧縮の有効化」セクションを追加しました。
3_0	2021 年 12 月 13 日	「Data Store の導入オプション」セクションを追加し、「修正点」セクションを更新しました。

リリースサポート情報

リリース 7.4.0 の公式一般公開（GA）日は 2021 年 11 月 2 日 です。

一般的なソフトウェアのメンテナンスサポート、パッチ、一般的なメンテナンスリリースに関するサポートタイムライン情報、もしくは Cisco Stealthwatch リリース サポート ライフサイクルに関するその他の情報については、Cisco Stealthwatch® ソフトウェアリリースモデルおよびリリース サポート タイムライン製品速報を参照してください。

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL：https://www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

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。