# Cisco Secure Network Analytics

ETA Cryptographic Audit v3.2.1 リリースノート

# 目次

# はじめに

このドキュメントでは、ETA Cryptographic Audit（暗号化トラフィック分析）3.2.x の一般的な情報を提供します。ETA Cryptographic Audit の最新バージョンは v3.2.1 です。

TLS フィンガープリントレポートは、クライアント プロセス レポートに置き換えられました。このレポートには、特定の期間に相互通信している、選択されたホストグループによって使用されるクライアントプロセスの概要が表示されます。

- ETA Cryptographic Audit は、Secure Network Analytics データストアが展開されている Cisco Secure Network Analytics（旧 Stealthwatch）で動作するようになりました。
- クライアントプロセスは、Secure Network Analytics データストアが展開されている Secure Network Analytics では機能しません。

## 概要

### ETA Cryptographic Audit

ETA Cryptographic Audit レポートでは次のことが行われます。

- サブジェクト（サーバー）とそのピア（クライアント）間の暗号化パラメータが調査されます。特に、次の内容が表示されます。
  - 独自のデータを保存する重要なサーバーへの暗号化された接続の数
  - 使用されている TLS バージョンと暗号スイート
  - データ量
  - キー長
- トレンドの変化と「転換」が検出されます。
- 最新ではない、またはサポートが不十分なサーバーとアプリケーションが識別されます。
- ネットワークの主要な領域との間で送受信される暗号化トラフィックの概要が提供されます。
- 監査や重要なネットワークセグメントでのセキュア通信を確保するために必要な、暗号化準拠の概要が提供されます。
- コンプライアンスの証明（PCI、FIPS など）が提供されます。ネットワークの重要な部分について、暗号化されたチャネルで、最新かつレビューおよび改訂されたポリシーが使用されていることが示されます。

Secure Network Analytics ユーザーの場合は、ETA（暗号化トラフィック分析）Cryptographic Audit を使用できます。ただし、ユーザーが権限を持つホストグループの結果のみが表示されます。

### クライアントプロセス

クライアント プロセス レポートでは次のことが行われます。

- Cisco ISE（Identity Services Engine） などのエンドポイントセキュリティなしでセキュアな接続を開始するクライアントプロセスが識別されます。

- セキュアな（TLS）接続を開始するホストプロセスが可視化され、ETA テクノロジーと TLS フィンガープリント機能を活用して、Cisco Mercury リサーチプロジェクトで使用された知識ベースに基づいてプロセスが識別されます。
- XLS レポートへのデータのエクスポートが許可されます。
- フロー検索にピボットするオプションが提供されます。

# はじめる前に

ETA Cryptographic Audit をインストールする前に、このセクションをお読みください。

> ETA Cryptographic Audit は、輸出管理に関する法律および規制の対象となります。お客様は、ETA Cryptographic Audit をダウンロードすることにより、当該政府機関からの事前の書面による許可なく、ETA Cryptographic Audit を禁止された宛先、エンドユーザー、または最終用途向けに故意に（直接的または間接的に）輸出または再輸出しないことに同意したことになります。

暗号化データを含む結果を表示するには、トラフィックをフローコレクタに送信する ETA 対応デバイスが必要です。

## クライアントプロセス

アプリケーションをインストールする前に、次のことを行う必要があります。

該当するフローコレクタごとに、ネットワーク環境で TLS フィンガープリントを有効にします。クライアントプロセス機能はデフォルトで無効になっています。フローコレクタに対して有効にするには、次の手順を実行します。

1. 該当するフロー コレクタ インターフェイスにログインします。
2. ページの左側にあるナビゲーションウィンドウで、[サポート（Support）] > [詳細設定（Advanced Settings）] をクリックします。
3. ページの上部にある enable_tls_fingerprint ラベルで、[オプション値（Option Value）] フィールドに表示されている 0（ゼロ）を 1 に変更します（0 は、機能が無効であることを示します）。

クライアントプロセスを有効にするフローコレクタごとに、手順 1 ～ 3 を繰り返す必要があります。

## Cisco Secure Network Analytics との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、Cisco Secure Network Analytics アプリケーションバージョンの互換性マトリックス [英語] 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。

⚠ 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。ETA Cryptographic Audit をアンインストールすると、一時ファイルも含め、関連付けられているすべてのファイルが削除されます。

| 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）。 |
| 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。 |
| 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。 | シスコの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。 |

Cisco Software Central から ETA Cryptographic Audit アプリケーションをダウンロードするには、次の手順を実行します。

1. [ダウンロードとアップグレード(Download and Upgrade)] セクションで、[ダウンロードにアクセス(Access downloads)] を選択します。
2. [製品の選択(Select a Product)] 検索バーで、**Cisco Secure Network Analytics** と入力して Enter を押します。
3. リストから [Cisco Secure Network Analytics Manager 2210] を選択します。
4. リストから [アプリケーション – ETA Cryptographic Audit(App – ETA Cryptographic Audit)] を選択します。

## リソース使用状況

ETA Cryptographic Audit については、次のことが当てはまります。

- 複数のフローコレクタおよびドメインをサポートします。
- 次のディスク容量が必要です。
    - /lancope : 1 MB
    - /lancope/var : 240 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)

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。

1. Web アプリケーションで、[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 [Central Management] を選択します。
2. [Appliance Manager] タブをクリックします。
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、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。
4. プロンプトが表示されたら、関連付けられたインターフェイスにログインします。
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。

## フェールオーバー

インストールの際、ETA Cryptographic Audit はプライマリ SMC とセカンダリ SMC の両方にインストールされます。セカンダリ マネージャで ETA Cryptographic Audit を使用するために、フェールオーバー状態になるのを待つ必要はなく、いつでもセカンダリ マネージャで使用できます。

## バックアップ

ETA Cryptographic Audit のデータと設定をバックアップできるか確認するには、次の表を参照してください。

| **このタイプのバックアップを実行すると…** | **関連するデータはバックアップされますか。** |
|---|---|
| 設定 | • インストールはバックアップされません。<br>• アプリケーション固有の設定はバックアップされません。 |
| データベース | • アプリケーション固有のデータはバックアップされません。 |

## ETA 暗号 Audit のインストール

ETA Cryptographic Audit をインストールするには、Central Management にアクセスし、[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。

- Secure Network Analytics の使用可能なディスク容量が 100 ～ 300 MB の場合、Secure Network Analytics の残りのディスク容量を示すメッセージが表示されます。この状況では、使用可能なディスク容量よりも多くのディスク容量を ETA Cryptographic Audit アプリケーションが必要としている可能性があります。ETA Cryptographic Audit アプリケーションに必要なディスク容量を確認するには、このドキュメントの「**リソース使用状況**」を参照してください。
- Secure Network Analytics が使用可能なディスク容量が 100 MB 未満の場合、このアプリケーションはインストールできません。

## アプリの互換性に関する注意事項

Secure Network Analytics アプリケーションは Secure Network Analytics の v7.0.0 で導入されました。

Secure Network Analytics アプリケーションは、スマートフォンにインストールするアプリと概念的に似ています。これらは、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 アプリケーションは、[Central Management] メニューオプションの [SMC Webアプリケーション(SMC Web App)] からアクセスできる [アプリケーションマネージャ(App Manager)] を使用してインストール、更新、削除できます。

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 のカスタマーエクスペリエンスをシンプルにするため、任意の時点でインストールできる Secure Network Analytics アプリケーションのバージョンは 1 つのみになっています(アプリストアモデルと同様)。アプリケーションの互換性については最大限尽力していますが、アプリケーションのすべてのバージョンが Secure Network Analytics のすべてのバージョンと互換性があるわけではありません。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 アプリケーションのバージョン互換性マトリックス」を参照してください。

一部のアプリケーションでは、Secure Network Analytics の最新バージョンへのアップグレードが必要になる場合があります。さらに、システムをアップグレードする際に、一部またはすべてのアプリケーションをアップグレードする必要が生じる場合があります。

シスコは、Secure Network Analytics アプリケーションをいつでも中止する権利を留保しています。廃止の根拠には以下の状況が含まれますが、これらに限定されません。

1. アプリケーションによって提供されるものと同等の機能が、アプリケーションの新しいバージョン、新しいアプリケーション、または Secure Network Analytics の機能を介して、他の方法で提供されるようになった場合。
2. アプリケーションによって提供される機能が、当社のカスタマーベースに関連があるか、または役立つとみなされなくなった場合。

Secure Network Analytics アプリケーションを廃止すると決定された場合、廃止が実行される少なくとも 60 日前に通知されます。Secure Network Analytics アプリケーションは現在 Secure Network Analytics ライセンスに含まれていますが、シスコは、将来特定の Secure Network Analytics アプリケーションのライセンス料を請求する権利を留保しています。

# オンライン ヘルプ

このアプリケーションのオンラインヘルプにアクセスするには、ページの右上隅にある  ([ヘルプ(Help)])アイコン をクリックします。

# 修正点

このセクションでは、今回のリリースで実施された修正の概要を示します。参照用に Secure Network Analytics の問題番号または導入事例番号が表示されています。

## バージョン 3.0.0

| 障害 | 説明 |
|---|---|
| SWONE-5915 | ETA Cryptographic Audit レポートに記載される IP アドレスの最大数を 100 から 1000 に増やしました。 |
| SWONE-9541 | ユーザーが認識できない方法で ETA Cryptographic Audit が応答しなかった場合、ユーザーは意味のあるエラーメッセージを受け取るようになりました。 |
| SWONE-9752 | セカンダリ SMC で ETA Cryptographic Audit を使用できるようになりました。 |
| SWONE-9818 | 特定の状況下で、ETA Cryptographic Audit レポート全体を印刷できない問題を修正しました。 |
| SWONE-9869 | フローコレクタのサブセットが失敗した場合、ETA Cryptographic Audit は引き続き機能します。 |
| SWONE-10583 | 監査レポートの結果に正しい接続数が表示されるようになりました。 |
| SWONE-10960 | ETA Cryptographic Audit からフロー検索を実行すると、TLS v1.3 の結果を受け取るようになりました。 |
| SWONE-11106 | 診断パックのエラーログを改善しました。 |
| SWONE-11139 | ETA Cryptographic Audit で、レポートの文字セットが正しく指定されるようになりました。 |

## バージョン 3.1.0

このバージョンに修正は必要ありませんでした。

## バージョン 3.2.0

| 障害 | 説明 |
|---|---|
| SWONE-14575 | バックエンドエラーの発生時に、少し詳細な情報（FC に到達できない/クエリを実行できない（FC not reachable/unable to execute a query）を含むエラーメッセージが表示されるようになりました。 |
| SWONE-14284 | 10,000 以上の行を含むテーブルで作業する場合に応答時間の遅れがなくなりました。 |
| SWONE-15181 | 監査レポートを実行し、開始時刻と一致するように終了時刻を設定すると、警告が表示され、エントリの 1 つを調整するまでクエリを送信できなくなりました。 |
| SWONE-15822 | 監査レポートのカレンダーで開始時刻と終了時刻を選択しても、カレンダーがフリーズしなくなりました。 |
| SWONE-16329 | フィルタ機能が正しく動作するようになりました。 |
| SWONE-16692 | ページ下部のページ番号が正しく表示されるようになりました。 |
| SWONE-17450 | ページ上のさまざまな要素が正しく表示されるようになりました（[レポートのタイプ（Type of Report）] ドロップダウンリスト、[サブジェクトホストグループ（Subject Host Groups）] および [ピアホストグループ（Peer Host Groups）] パネル）。 |

## バージョン 3.2.1

このバージョンに修正は必要ありませんでした。

# サポートに連絡

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。

**コール**

- 最寄りのシスコ パートナー
- シスコ サポート
  - （米国）1-800-553-2447
  - ワールドワイドサポート番号：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

**ケースのオープン**

- Web：http://www.cisco.com/c/en/us/support/index.html
- 電子メール：tac@cisco.com

# 著作権情報