



# Cisco Secure Network Analytics

v7.4.2 グローバル脅威アラートコンフィギュレーションガイド



---

# 目次

はじめに .....	3
サポート .....	3
暗号化トラフィック分析 サポート .....	4
ユーザーとデータロール .....	4
データ .....	5
Secure Network Analytics フローレコード .....	5
暗号化トラフィック分析フローレコード .....	6
Web ログデータ .....	6
マネージャ .....	7
ダッシュボード コンポーネントの設定 .....	7
内部ホスト .....	8
Flow Collector の設定 .....	10
プロキシ設定 .....	11
検証 .....	13
Docker サービス .....	13
暗号化トラフィック分析 統合 .....	13
既知の問題 .....	14
関連資料 .....	15
サポートへの問い合わせ .....	16

## はじめに

シスコグローバル脅威アラート(旧 Cisco Cognitive Intelligence)は、疑わしい Web トラフィックや Cisco Secure Network Analytics(旧 Stealthwatch)のフローレコードを迅速に検出し、環境内でのプレゼンス確立の試みや、すでに発生中の攻撃に対処します。Secure Network Analytics は、Secure Network Analytics で有効化されると、分析のためにグローバル脅威アラートクラウドにフローレコードを送信します。デフォルトでは、グローバル脅威アラートが、内部/外部のホストグループトラフィックおよび DNS 要求の Secure Network Analytics フローレコードを処理します。内部トラフィックをモニタするには、追加のホストグループを指定できます。グローバル脅威アラートは、シスコの暗号化トラフィック分析を使用して暗号化されたトラフィックの悪意のあるパターンも検出します。

グローバル脅威アラートは Secure Network Analytics と連携し、フローレコードとネットワークアドレス変換(NAT)を分析します。Secure Network Analytics フローレコードをグローバル脅威アラートに送信するのに追加のライセンスは必要ありませんが、Secure Network Analytics からグローバル脅威アラートに Web トラフィックデータを送信するには、インターネット境界 NAT データが必要です。これらの製品に関する詳細情報へのリンクについては、このドキュメントの最後にある「[関連資料](#)」を参照してください。



- グローバル脅威アラートは Amazon Web Services(AWS)クラウドに移行したため、URL と IP アドレスが新しくなりました。詳細については、次の Field Notice を参照してください:  
[Field Notice - 2018 年 5 月](#)  
[Field Notice - 2018 年 10 月](#)

## サポート



スマートライセンス予約が使用されている場合、グローバル脅威アラートはサポートされません。

- マネージャ(旧 Stealthwatch 管理コンソール)および Flow Collector は、プロキシサーバー経由でインターネットに接続するよう設定できます。詳細については、「[プロキシ設定](#)」を参照してください。
- グローバル脅威アラートは、そのドメインに関連付けられたフローコレクタが有効になっている限り、各ドメインを分析します。生成されたアラートのリストは、すべてのドメインから取得されたデータの集約です。ドメインごとに分割されていません。
- 特定のクライアント IP アドレスが複数のドメインに存在する場合、グローバル脅威アラートは、該当するすべてのドメインにわたってこの IP アドレスのすべてのアラートを識別し、これらのアラートを結果の同じグループに配置します。ただし、ホストグループのデータはフローコレクタごとに個別に収集されるため、グローバル脅威アラートダッシュボードで結果をホストグループ別にフィルタ処理できます(メインメニューから **[統合の監視(Monitor INTEGRATIONS)]** > **[グローバル脅威アラート(Global Threat Alerts)]** を選択します)。
- グローバル脅威アラートは Flow Collector(sFlow) ではサポートされていません。
- FIPS 暗号化ライブラリが有効になっている場合、グローバル脅威アラートは使用できません。

## 暗号化トラフィック分析 サポート

暗号化トラフィック分析 対応スイッチおよびルータを備えている場合、グローバル脅威アラートは暗号化トラフィック分析 情報のみ検出できます。Secure Network Analytics および 暗号化トラフィック分析 の詳細については、[暗号化トラフィック分析 ホワイトペーパー](#)、および[暗号化トラフィック分析 導入ガイド](#)を参照してください。

## ユーザーとデータロール

次のユーザが	次のデータロールを使用する場合	アクセス可能なもの
プライマリ Admin (Primary Admin)	すべてのデータ (読み取りおよび書き込み)	<ul style="list-style-type: none"> <li>グローバル脅威アラートダッシュボード</li> <li>グローバル脅威アラートコンポーネント</li> </ul>
パワーアナリスト (Power Analyst)		
設定マネージャ (Configuration Manager)	すべてのデータ(読み取り専用)*	<ul style="list-style-type: none"> <li>グローバル脅威アラートダッシュボード</li> </ul>
アナリスト(Analyst)		

\* 設定マネージャとアナリストのデータロールを変更し、グローバル脅威アラートへのフルアクセスを提供できます。詳細については、ユーザ管理の設定に関するヘルプトピックを参照してください。

## データ

次の2つのカテゴリのデータがダブリンのAWSデータセンターに送信されます。

- 次の条件のいずれかが満たされた場合の、Secure Network Analytics フローレコード。
  - 内部/外部ホストグループのトラフィックのレコード
  - 特定の内部ホストグループトラフィックのレコード(「[内部ホスト](#)」を参照してください)
  - サーバポートが53の場合のDNS要求レコード
  - 暗号化トラフィック分析 対応スイッチおよびルータをお持ちの場合は、暗号化トラフィック分析のレコード
- Secure Network Analytics プロキシログをお持ちの場合は、Web ログデータ

### Secure Network Analytics フローレコード

Secure Network Analytics フローレコードには次のものが含まれます。

- |                          |                                  |                         |
|--------------------------|----------------------------------|-------------------------|
| • ホストエンドポイントの IP アドレス    | • 開始時刻                           | • 最終アクティブ時刻             |
| • TCP ポートまたは UDP ポート     | • ポート範囲                          | • 自律システム番号              |
| • mac アドレス               | • グループ ID                        | • VM ID                 |
| • プロトコル データ*             | • SYN パケット数                      | • RST パケット数             |
| • 期間ごとの送信時のバイト およびパケットの数 | • TrustSec セキュリティグループ タグの ID と名前 | • フロー開始以降のバイト とパケットの合計数 |
| • FIN パケット数              | • 既知のサービス ポート                    | • プロトコル                 |
| • フロー ID                 | • アプリケーション ID                    | • パケットシェーパ アプリケーション ID  |
| • サービス ID                | • フローセンサー アプリケーション ID            | • NBAR アプリケーション ID      |
| • Palo Alto アプリケーション ID  | • VLAN ID (Admin. VLAN ID)       | • 接続数                   |
| • ユーザ名                   | • 再送信数                           | • サーバ応答時間               |
| • MPLS ラベル               | • エクスポートのリスト                     | • フローシーケンス番号            |
| • ラウンドトリップ時間             | • Flow Collector IP アドレス         | • SVRD メトリック            |

\*プロトコルデータフィールドには、URL、SSL 証明書、ヘッダーデータ用の特殊文字などのその他の情報が含まれます。

## 暗号化トラフィック分析フローレコード

暗号化トラフィック分析 フローレコードは、暗号化トラフィック分析 対応スイッチおよびルータをお持ちの場合のみ送信されます。Secure Network Analytics および 暗号化トラフィック分析 の詳細については、[暗号化トラフィック分析 ホワイトペーパー](#)、および[暗号化トラフィック分析 導入ガイド](#)を参照してください。

暗号化トラフィック分析 フローレコードには次のものが含まれます。

- 初期データパケット (IDP)\*
- TLS セッション UD
- パケットの長さや時間のシーケンス (SPLT)
- 選択した暗号スイート
- Transport Layer Security (TLS) バージョン

\* 初期データパケット (IDP)には、サーバ名表示 (SNI)、プロトコルバージョン、提供および選択された暗号スイートと HTTP ヘッダーフィールド (暗号化されていない HTTP トラフィックの場合) など、プロトコル関連のデータとヘッダーがほとんど含まれています。HTTPS/HTTP 以外のプロトコルの場合は、クライアント/サーバ通信の最初の 1500 バイトのプロトコルヘッダーが含まれています (通常は、データの残りの部分を復号することなく、プロトコルレベルで暗号化されます)。

## Web ログ データ

Web ログ データの目的の 1 つは、NAT を介してルーティング不可能な内部 IP とルーティング可能な外部パブリック IP の間の変換を提供することです。

 プロキシログの設定 Secure Network Analytics サポートについては、[『Cisco Secure Network Analytics プロキシログ設定ガイド』](#)を参照してください。

Web ログ データには以下が含まれます。

- タイムスタンプ
- サーバ IP アドレス
- クライアント TCP ポート
- クライアントからサーバに転送されたバイト数
- HTTP Referrer ヘッダー
- user-agent 文字列
- 経過時間
- クライアント ユーザ名 (オプション)
- サーバ TCP ポート
- サーバからクライアントに転送されたバイト数
- HTTP 応答ステータスコード
- 応答 MIME タイプまたはコンテンツタイプ
- クライアント IP アドレス
- サーバ名
- 要求された URL/URI
- HTTP 要求メソッド
- HTTP Location ヘッダー
- Web セキュリティプロキシによって実行されるアクション



# マネージャ

## ダッシュボードコンポーネントの設定

マネージャ上のグローバル脅威アラートコンポーネントを設定するには、次の手順を実行します。

- ❗ アプライアンスはすべて、グローバル脅威アラートに接続するために NTP サーバーを使用して同期されたクロックを備えている必要があります。

- ❗ デュアル マネージャのペアでは、設定後、セカンダリ マネージャはグローバル脅威アラートに接続しません。これが Flow Collector の受信データに干渉することなく、プライマリ マネージャがグローバル脅威アラートに接続してウィジェットを適切に表示します。プライマリ マネージャが失敗した場合、セカンダリ マネージャがグローバル脅威アラートに接続してウィジェットを表示します。元のプライマリ マネージャが起動すると、両方のマネージャがグローバル脅威アラートに正常に接続します。

- ❗ 少なくとも 1 つのマネージャにインターネットアクセスが必要です。プロキシ設定も必要な場合は、詳細について「[プロキシ設定](#)」を参照してください。

- マネージャから次の IP アドレスおよびポート 443 に通信できるように、ネットワークファイアウォールを設定します。

サービス	URL エイリアス	サービス IP
CTA 公開ランディングページ	<a href="https://cta.eu.amp.cisco.com/">https://cta.eu.amp.cisco.com/</a> <a href="https://cognitive.cisco.com/">https://cognitive.cisco.com/</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105
CTA ログインページ	<a href="https://cta.eu.amp.cisco.com/">https://cta.eu.amp.cisco.com/</a> <a href="https://td.cloudsec.sco.cisco.com/CWSP/">https://td.cloudsec.sco.cisco.com/CWSP/</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105
CTA TAXII サービス	<a href="https://cta.eu.amp.cisco.com/taxii">https://cta.eu.amp.cisco.com/taxii</a> <a href="https://taxii.cloudsec.sco.cisco.com">https://taxii.cloudsec.sco.cisco.com</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105

- ❗ パブリック DNS が許可されていない場合は、マネージャでローカルに解決方法を設定する必要があります。

2. マネージャにログインします。
3. **[グローバルの構成 (Configure GLOBAL)]** > **[集中管理 (Central Management)]** を選択します。
4. マネージャの **[アクション (Action)]** 列にある **…** (**[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。
5. **[全般 (General)]** タブをクリックします。
6. **[外部サービス (External Services)]** で **[グローバル脅威アラートを有効にする (Enable グローバル脅威アラート)]** チェックボックスをオンにし、**セキュリティインサイトダッシュボード** および **ホストレポート** 上の **グローバル脅威アラートコンポーネント** を有効化します。
7. (オプション) **グローバル脅威アラートがクラウドから自動的にアップデートを送信できるようにするには**、**[自動更新 (Automatic Updates)]** チェックボックスをオンにします。

自動更新は、主にグローバル脅威アラートクラウドのセキュリティの修正と小さな機能強化をカバーします。これらの更新は、通常の Secure Network Analytics リリースプロセスを通じて行うこともできます。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。マネージャで自動更新を有効にした場合、Flow Collector でも自動更新を有効にする必要があります。

8. **[設定の適用 (Apply settings)]** をクリックします。

サービスが更新され、**セキュリティインサイトダッシュボード** および **ホストレポート** 上の **グローバル脅威アラートコンポーネント** が表示されるまでに数分かかります。

9. (省略可) **インターネットプロキシをアップロードするには**、**[ネットワークサービス (Network Services)]** に移動します。**[インターネットプロキシ (Internet Proxy)]** セクションまでスクロールダウンし、**[有効 (Enable)]** チェックボックスをオンにします。フォームに入力してから、**[設定の適用 (Apply Settings)]** をクリックします。


## 内部ホスト

デフォルトでは、グローバル脅威アラートが、内部/外部のホストグループトラフィックおよび DNS 要求の Secure Network Analytics フローレコードを処理します。分析用にクラウドに送信するデータを追加するには、Secure Network Analytics フローレコードを送信する内部ホストグループを設定します。特定のホストグループをグローバル脅威アラートモニタリングに追加する方法は、企業の内部サーバー（メールサーバー、ファイルサーバー、Web サーバー、認証サーバーなど）に使用されます。これらのサーバーにエンドユーザーからのトラフィックを追加すると、該当のデバイスで実行されているマルウェアによって悪用される可能性がある、データの露出の可視性を改善できます。データを送信するホストグループをすべて選択するのではなく、内部サーバを表すホストグループのみを選択してください。

グローバル脅威アラートが内部ホストのトラフィックを監視することを許可するには、次の手順を実行します。

1. マネージャにログインします。
2. **[検出の設定 (Configure DETECTION)]** > **[ホストグループ管理 (Host Group Management)]** に移動します。
3. 該当する内部ホストグループをクリックし、**[グローバル脅威アラートへのフローの送信 (Send Flow to グローバル脅威アラート)]** チェックボックスをオンにします。



 この機能により、選択した親ホストグループの下にあるすべてのホストグループのトラブルシューティングのモニタリングが有効になります。潜在的なパフォーマンスの問題を避けるため、このオプションは子ホストグループでのみ有効にすることをお勧めします。

4. [保存 (Save)] をクリックします。

## Flow Collector の設定

Flow Collector (NetFlow) 上のグローバル脅威アラートコンポーネントを設定するには、次の手順を実行します。

**i** アプライアンスはすべて、グローバル脅威アラートに接続するために NTP サーバーを使用して同期されたクロックを備えている必要があります。

**i** 正確な結果を得るには、それぞれの Flow Collector にグローバル脅威アラートを設定する必要があります。

**i** 設定後、グローバル脅威アラートエンジンにネットワークの挙動を学習させるため、2 日間の猶予を与えます。

1. Flow Collector から次の IP アドレスおよびポート 443 に通信できるように、ネットワークファイアウォールを設定します。

サービス	URL エイリアス	サービス IP
CTA 公開ランディングページ	<a href="https://cta.eu.amp.cisco.com/">https://cta.eu.amp.cisco.com/</a> <a href="https://cognitive.cisco.com/">https://cognitive.cisco.com/</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105
CTA ログインページ	<a href="https://cta.eu.amp.cisco.com/">https://cta.eu.amp.cisco.com/</a> <a href="https://td.cloudsec.sco.cisco.com/CWSP/">https://td.cloudsec.sco.cisco.com/CWSP/</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105
CTA TAXII サービス	<a href="https://cta.eu.amp.cisco.com/taxii">https://cta.eu.amp.cisco.com/taxii</a> <a href="https://taxii.cloudsec.sco.cisco.com">https://taxii.cloudsec.sco.cisco.com</a> (エイリアス)	AWS EIPs: *34.242.41.248  • 34.242.94.137 • 34.251.54.105
CTA データ取り込みサービス	<a href="https://etr.cta.eu.amp.cisco.com">https://etr.cta.eu.amp.cisco.com</a> <a href="https://etr.cloudsec.sco.cisco.com">https://etr.cloudsec.sco.cisco.com</a> (エイリアス)	AWS EIP: *34.251.210.21  • 34.255.162.33 • 54.194.49.205

**i** パブリック DNS が許可されていない場合は、Flow Collector でローカルに解決方法を設定する必要があります。

2. マネージャにログインします。
3. **[グローバルの構成 (Configure GLOBAL)]** > **[集中管理 (Central Management)]** を選択します。
4. Flow Collector (NetFlow) の **[アクション (Action)]** 列にある **...** (**[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。
5. **[全般 (General)]** タブをクリックします。
6. **[外部サービス (External Services)]** で **[グローバル脅威アラートを有効にする (Enable グローバル脅威アラート)]** チェックボックスをオンにし、Flow Collector からグローバル脅威アラートエンジンにデータを送信できるようにします。
7. (オプション) グローバル脅威アラートがクラウドから自動的にアップデートを送信できるようにするには、**[自動更新 (Automatic Updates)]** チェックボックスをオンにします。

自動更新は、主にグローバル脅威アラートクラウドのセキュリティの修正と小さな機能強化をカバーします。これらの更新は、通常の Secure Network Analytics リリースプロセスを通じて行うこともできます。いつでもこのオプションを無効にして、クラウドからの自動更新を停止できます。Flow Collector で自動更新を有効にした場合、マネージャでも自動更新を有効にする必要があります。

8. **[設定の適用 (Apply settings)]** をクリックします。

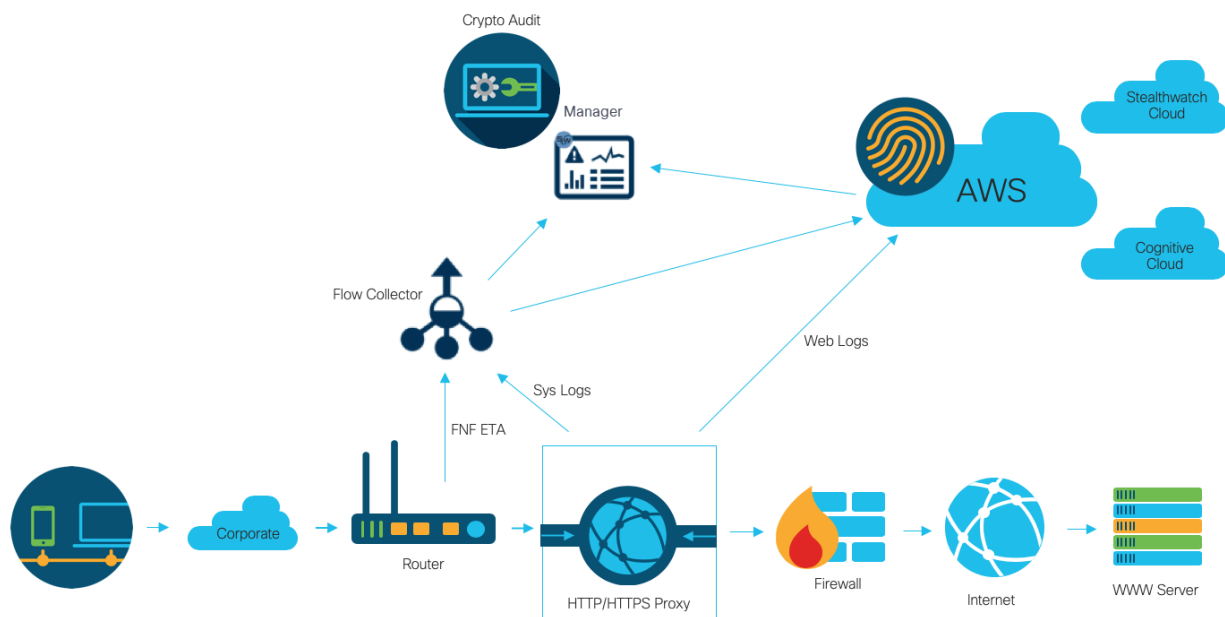
## プロキシ設定

これを実現するには、マネージャおよび Flow Collector がプロキシサーバー経由でインターネットに接続するよう設定します。グローバル脅威アラートは、SSL インスペクションが無効になっている HTTP/HTTPS プロキシをサポートしています。Secure Network Analytics は SOCKS プロキシをサポートしていません。

Web プロキシの設定方法の詳細については、このドキュメントの「**マネージャ**」セクションを参照してください。プロキシログの設定の詳細については、[『Cisco Secure Network Analytics プロキシログの設定ガイド』](#)を参照してください。

セットアップの設定については、次の図を参照してください。

- i** この設定では、WSA のプロキシを透過モードにする必要があります。詳細については、[『グローバル脅威アラートシステムにログファイルをアップロードするための WSA の設定』](#)を参照してください。



次の場合、プロキシを使用するとグローバル脅威アラートから最高の結果が得られます。

- Flow Collector はプロキシより前にフローを収集します
- プロキシログはクラウドに直接送信されます。

次の場合、プロキシを使用すると Secure Network Analytics から最高の結果が得られます。

- プロキシログは Flow Collector に直接送信されます
- 暗号化トラフィック分析 を有効にします

プロキシをクラウドに直接接続する方法の詳細については、

[「グローバル脅威アラートシステムにログファイルをアップロードするための Blue Coat ProxySG の設定」](#)

**i** [、「グローバル脅威アラートシステムにログファイルをアップロードするための McAfee ウェブゲートウェイの設定」、](#)

[「グローバル脅威アラートシステムにログファイルをアップロードするための WSA の設定」](#)を参照してください。

# 検証

## Docker サービス

グローバル脅威アラートが適切に設定されていることを確認するには、次の手順を実行します。

**i** グローバル脅威アラートを無効にするには、[集中管理 (Central Manager)] > [アプライアンス設定の編集 (Edit Appliance Configuration)] > [全般 (General)] に移動し、各マネージャおよび Flow Collector (NetFlow) の [グローバル脅威アラートを有効にする (Enable グローバル脅威アラート)] チェックボックスをオフにします。

1. マネージャおよび Flow Collector でグローバル脅威アラートが有効になっているか確認してください。
2. セキュリティインサイトダッシュボードおよびホストレポート上にグローバル脅威アラートコンポーネントが表示されているか確認してください。
3. ナビゲーションメニューから、[統合の監視 (Monitor INTEGRATIONS)] > [グローバル脅威アラート] をクリックします。グローバル脅威アラートダッシュボードページが開きます。ページの右上にあるメニューから [デバイスアカウント (Device Accounts)] をクリックします。設定されている各 Flow Collector のアカウントでデータがアップロードされていて、準備ステータスになっていることを確認します。

## 暗号化トラフィック分析 統合

グローバル脅威アラートは、暗号化トラフィック分析ソリューション内でマルウェア検出機能を導入します。暗号化トラフィック分析ソリューションが正しくセットアップされていることを確認するため、グローバル脅威アラートは、特定のテストサイトドメインを使用して暗号化トラフィック分析テストインシデントを生成できます。これらのテストインシデントを生成するには、HTTPS セッションが暗号化トラフィック分析対応スイッチおよびルータを通過するホストを使用して、次のテストサイトのいずれかを参照します。

- マルウェア: <https://examplemalware.com>
- ボットネット: <https://examplebotnet.com>
- フィッシング: <https://internetbadguys.com>

**i** 最初は検出結果にリスクレーティング 5 と表示されます。上記の複数の URL にアクセスしたり、同じ URL に繰り返しアクセスしたりといった不正または反復的な動作が行われると、リスクレーティングが増大する可能性があります。

- TOR 検出: TOR ブラウザをダウンロードしてインストールし (<https://www.torproject.org/projects/torbrowser.html.en>)、いくつかのウェブサイトアクセスしてください。
- TOR 検出は、リスクレーティング 4 の「TORリレー (TOR relay)」または「潜在的に望ましくないアプリケーション (Possibly Unwanted Application)」と表示されます。

## 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。

問題番号	説明	回避策
CHOPIN-25314	Secure Network Analytics ユーザーの権限が引き上げられたり、引き下げされたりした場合(例: 読み取り専用から読み取り/書き込みへ、またはその逆)、その変更がグローバル脅威アラートに反映されるまで最大で 30 分かかります。	現在使用可能なものはありません。
SWD-13834	設定を復元した後、グローバル脅威アラートは無効になっています。	これを修正するには、バックアップ復元プロセスの後、手動でグローバル脅威アラートを有効にします。
NA	ユーザーが複数の Secure Network Analytics システムにログインしている場合、グローバル脅威アラート内の 2 番目のシステムにはログインできません。	この問題を解決するには、次の手順に従います。 <ul style="list-style-type: none"> <li>最初のログインが期限切れになるまで 30 分待機します。</li> <li>最初のシステムでグローバル脅威アラートからログアウトします</li> </ul>



---

## 関連資料

- グローバル脅威アラートの詳細については、製品の Web サイト (<https://cognitive.cisco.com>) にアクセスするか、[http://www.cisco.com/c/en/us/td/docs/security/web\\_security/scancenter/administrator/guide/b\\_ScanCenter\\_Administrator\\_Guide/b\\_ScanCenter\\_Administrator\\_Guide\\_chapter\\_011110.html](http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011110.html) にある製品マニュアルを参照してください。
- すべてのシスコクラウド製品のクラウド利用規約とオファーの説明については、<http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html> を参照してください。
- Cisco Universal Cloud 契約については、[http://www.cisco.com/c/dam/en\\_us/about/doing\\_business/legal/docs/universal-cloud-agreement.pdf](http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf) を参照してください。
- オファー全般については、[http://www.cisco.com/c/dam/en\\_us/about/doing\\_business/legal/docs/omnibus-cloud-security.pdf](http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/omnibus-cloud-security.pdf) を参照してください。
- Secure Network Analytics プロキシログおよび Web プロキシの詳細については、<https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html> を参照してください。

## 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](mailto: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：  
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

---

## 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)