

# Cisco Secure Network Analytics

フェールオーバー コンフィギュレーションガイド 7.4.1



---

# 目次

はじめに .....	5
はじめる前に .....	5
セキュリティ分析とロギング(オンプレミス) .....	5
アプライアンス ステータス .....	5
設定要件 .....	5
管理者ユーザー .....	5
設定ファイルとデータベースのバックアップ .....	6
証明書 .....	6
フェールオーバーロール .....	6
設定の順序 .....	6
設定の変更 .....	6
ソフトウェア バージョン .....	6
フェールオーバー設定の保存 .....	7
プライマリマネージャ .....	7
セカンダリ マネージャ(読み取り専用) .....	7
パスワード .....	7
ドメインの変更 .....	7
フローコレクタ .....	7
外部サービス .....	7
ロールの変更 .....	7
証明書 .....	7
プライマリマネージャの復元 .....	8
プライマリマネージャの再起動 .....	8
ネットワーク インターフェイスの変更 .....	8
フェールオーバー設定の概要 .....	9
1. フェールオーバーロールの計画 .....	10
2. マネージャ設定とデータベースのバックアップ .....	11
1. バックアップ設定ファイルの作成 .....	11
2. マネージャ データベースのバックアップ .....	11
1. データベースのスナップショットの削除 .....	12
2. データベースのバックアップ .....	12
3. データベースのスナップショットの削除 .....	14
4. データベースのバックアップの確認 .....	15

<b>3. 信頼ストアへの証明書の追加</b> .....	<b>16</b>
信頼ストアの要件 .....	16
証明書チェーン .....	16
信頼ストアへの証明書のアップロード .....	16
1. アプライアンス アイデンティティ証明書のダウンロード .....	16
2. マネージャ信頼ストアへの証明書の追加 .....	17
<b>Data Store 初期化後のフェールオーバーの設定</b> .....	<b>18</b>
フェールオーバーペアの設定 .....	18
Data Store 初期化後にマネージャを追加 .....	18
<b>4. フェールオーバーペアの設定</b> .....	<b>20</b>
はじめる前に .....	20
1. マネージャアプライアンスステータスの確認 .....	20
2. セカンダリマネージャの設定 .....	21
3. プライマリマネージャの設定 .....	21
<b>5. フェールオーバー設定の確認</b> .....	<b>23</b>
1. 設定の変更の確認 .....	23
2. フローコレクションの確認 .....	24
<b>フェールオーバーロールの変更</b> .....	<b>26</b>
時刻 .....	26
1. プライマリマネージャのバックアップ .....	26
2. アプライアンスステータスの確認 .....	26
3. フェールオーバー設定の変更 .....	27
1. プライマリ マネージャをセカンダリに変更する .....	27
2. セカンダリ マネージャをプライマリに変更する .....	28
4. 設定の変更の確認 .....	28
<b>ネットワーク インターフェイスの変更</b> .....	<b>29</b>
1. フェールオーバー設定の削除 .....	29
2. マネージャネットワーク インターフェイスの変更 .....	29
3. マネージャフェールオーバーの設定 .....	29
<b>フェールオーバー設定の削除</b> .....	<b>30</b>
1. アプライアンス ステータスの確認 .....	30
2. フェールオーバーロールの確認 .....	31
3. フェールオーバー設定の削除 .....	31
4. Central Management からのセカンダリ マネージャの削除 .....	32
5. セカンダリ マネージャ証明書の削除 .....	32

---

6. セカンダリ マネージャを工場出荷時の初期状態にリセットする .....	33
<b>トラブルシューティング .....</b>	<b>34</b>
マネージャがオフラインまたは障害状態になっている .....	34
信頼エラー .....	35
セカンダリマネージャにフローが表示されない .....	35
パスワードの有効期限切れ .....	35
<b>サポートへの問い合わせ .....</b>	<b>36</b>

## はじめに

フェールオーバー設定を使用して、2つの Cisco Secure Network Analytics Manager (旧 Stealthwatch Management Console または SMC) 間にフェールオーバー関係を確立すると、一方をもう一方のバックアップとして機能させることができます。

プライマリ マネージャで障害が発生した場合は、セカンダリ マネージャを手動でプライマリ マネージャに設定してシステムのモニタリングを継続できます。

**!** プライマリ マネージャがオフラインになっても、マネージャのロールは自動的に交換されないので注意してください。このガイドに示されている順序でマネージャロールを変更してください。

## はじめる前に

フェールオーバー設定を開始する前に、Cisco Secure Network Analytics (旧 Stealthwatch) アプライアンスをインストールして、システム設定を完了します。手順については、[Cisco Secure Network Analytics 設置ガイド](#) [英語] および [Cisco Secure Network Analytics システム コンフィギュレーションガイド](#) [英語] を参照してください。

**i** Secure Network Analytics システムで Data Store 展開を使用している場合は、Data Store 初期化の前にフェールオーバーを設定することをお勧めします。すでに初期化済みの Data Store がある場合は、このガイドの「[Data Store 初期化後のフェールオーバーの設定](#)」セクションの手順を参照してください。

また、フェールオーバー設定の要件と実装に備えて、このガイドで詳細および手順を確認してください。

## セキュリティ分析とロギング (オンプレミス)

一方のマネージャで Cisco Security Analytics and Logging (オンプレミス) が有効になっている場合は、フェールオーバー設定を開始する前に、もう一方のマネージャでも有効になっていることを確認します。

両方のマネージャで セキュリティ分析とロギング (オンプレミス) を有効にするには、[Cisco Security Analytics and Logging \(オンプレミス\) : Firepower イベント統合ガイド](#) [英語] を参照してください。

## アプライアンス ステータス

Secure Network Analytics で設定の変更を開始する前に、アプライアンスのステータスが [接続済み (Connected)] と表示されていることを確認します。このガイドには、ステータスを確認する手順が含まれています。

**!** フェールオーバー設定が完了するまで、他の設定を変更したり、[集中管理 (Central Management)] からアプライアンスを追加または削除したりしないでください。

## 設定要件

このガイドには、正常に設定するために重要な、次を含む詳細事項が記載されています。

### 管理者ユーザー

フェールオーバーを設定するには、管理者ユーザーとしてマネージャにログインします。

## 設定ファイルとデータベースのバックアップ

各マネージャの設定とデータベースをバックアップする時間を計画します。フェールオーバー設定に問題がある場合はバックアップファイルが必要で、マネージャを完全に復元するためには両方のバックアップが必要です。手順については、「[2. マネージャ設定とデータベースのバックアップ](#)」を参照してください。

## 証明書

フェールオーバーを設定する前に、必要なアプライアンスの信頼ストアに正しい証明書を保存してください。この手順では、アプライアンス間の信頼を確立して、互いに通信できるようにします。手順については、「[3. 信頼ストアへの証明書の追加](#)」を参照してください。

## フェールオーバーロール

フェールオーバー設定を保存すると、プライマリ マネージャがアプライアンスをアクティブに監視および管理し、セカンダリ マネージャが読み取り専用になります。プライマリまたはセカンダリフェールオーバー ロールで設定するマネージャを計画するには、「[フェールオーバー設定の保存](#)」および「[1. フェールオーバーロールの計画](#)」を参照してください。

セカンダリ マネージャが Central Management でアプライアンスを管理している場合は、フェールオーバー設定を開始する前にプライマリ マネージャ(または別のマネージャ)にアプライアンスを移動します。手順については、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) を参照してください。



アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)をマネージャ信頼ストアに保存してください。

## 設定の順序

セカンダリ マネージャを設定してからプライマリ マネージャを設定します。手順については、「[4. フェールオーバーペアの設定](#)」を参照してください。



プライマリ マネージャを設定する前に、セカンダリ マネージャをフェールオーバー用に設定してください。フェールオーバー設定を保存すると、セカンダリ マネージャドメイン設定が削除されるため、手順を順番に実行してください。

## 設定の変更

フェールオーバー設定が完了するまで、他の設定を変更したり、[集中管理(Central Management)]からアプライアンスを追加または削除したりしないでください。

## ソフトウェア バージョン

このガイド記載の手順に進む前に、Secure Network Analytics v7.4.1 以降が Manager にインストールされていることを確認してください。



## フェールオーバー設定の保存

フェールオーバー設定を保存すると、プライマリおよびセカンダリ マネージャの間に信頼関係と構成チャンネルが確立されます。また、次のシステム変更が発生します。

### プライマリマネージャ

プライマリ マネージャはそのドメイン設定、ユーザー設定、およびポリシーをセカンダリ マネージャにプッシュします。

### セカンダリ マネージャ(読み取り専用)

セカンダリ マネージャドメイン設定が削除されます。セカンダリはすべてのユーザーに対して読み取り専用になり、プライマリ マネージャと同期します。

### パスワード

プライマリ マネージャからローカルユーザーとパスワードログイン情報がセカンダリ マネージャにプッシュされるため、両方が同期されます。つまり、プライマリ マネージャとセカンダリ マネージャへのログインには同じパスワードを使用します。セカンダリ マネージャのパスワードを変更するには、プライマリ マネージャにログインします。

### ドメインの変更

プライマリ マネージャは、ホストグループ、ユーザー、ポリシーなどのドメイン設定の変更を自動的にセカンダリ マネージャと共有します。

セカンダリ マネージャへの通信チャンネルがダウン（[[構成チャンネルがダウン (Config Channel Down)]]）している間に、プライマリ マネージャ上のドメイン設定を変更した場合、セカンダリ マネージャの通信チャンネルが復旧するとすぐに、プライマリ マネージャから完全な設定プッシュが送信されます。

### フローコレクタ

フローコレクタは、データを自動的に両方のマネージャに送信します。

### 外部サービス

外部サービスがプライマリ マネージャで設定されている場合は、セカンダリ マネージャでも外部サービスを設定してください。たとえば、プライマリ マネージャで脅威フィードを有効にする場合は、セカンダリ マネージャでも有効にします。

### ロールの変更

セカンダリ マネージャをプライマリ フェールオーバー ロールに昇格させる必要がある場合は、ロールを順番に変更してください。順序は重要で、ロールは自動的に交換されません。

- プライマリがオフラインになっている場合、詳細については「[トラブルシューティング](#)」を参照してください。
- フェールオーバーロールを変更するには、「[フェールオーバーロールの変更](#)」を参照してください。

### 証明書

マネージャがフェールオーバー用に設定されている場合、次のように信頼ストアが自動的に更新されます。

- すべての管理対象アプライアンスの信頼ストアにセカンダリ マネージャ アイデンティティ証明書とチェーン(該当する場合)が追加されます。
- すべての管理対象アプライアンスのアイデンティティ証明書とチェーン(該当する場合)は、プライマリ マネージャ Central Management に追加されると、セカンダリ マネージャ信頼ストアに追加されます。

## プライマリマネージャの復元

フェールオーバー用に設定されているプライマリ マネージャを復元する場合、復元完了後に、セカンダリ マネージャがプライマリ マネージャと同期されます。

## プライマリマネージャの再起動

再起動したためにプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが[接続済み(Connected)]に戻り、セカンダリ マネージャが検出されると、プライマリはフェールオーバーロールを再開します。

- プライマリ マネージャのロールがセカンダリに変更され、解決しない場合は、「[トラブルシューティング](#)」を参照してください。
- フェールオーバーロールを変更するには、「[フェールオーバーロールの変更](#)」を参照してください。

## ネットワーク インターフェイスの変更

マネージャがフェールオーバー用に設定されている場合は、マネージャのネットワーク インターフェイス、ホスト名、またはネットワークドメイン名を変更する前に、フェールオーバー関係を削除します。詳細については、「[ネットワーク インターフェイスの変更](#)」を参照してください。



# フェールオーバー設定の概要

フェールオーバーを設定するには、次の手順を完了してください。

1. フェールオーバーロールの計画
2. マネージャ設定とデータベースのバックアップ
3. 信頼ストアへの証明書の追加
4. フェールオーバーペアの設定
5. フェールオーバー設定の確認

# 1. フェールオーバーロールの計画

フェールオーバー設定を開始する前に、プライマリまたはセカンダリフェールオーバーロールで設定するマネージャを計画します。

- IP アドレス: 各マネージャの IP アドレスを確認します。
- セカンダリ マネージャ: セカンダリ マネージャが Central Management でアプライアンスを管理している場合は、フェールオーバー設定を開始する前にプライマリ マネージャ(または別のマネージャ)にアプライアンスを移動します。手順については、[Cisco Secure Network Analytics システムコンフィギュレーションガイド](#) [英語] を参照してください。

**!** アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)をマネージャ信頼ストアに保存してください。

**!** フェールオーバー構成を開始する前に、両方のマネージャでセキュリティ分析とロギング(オンプレミス)が有効になっていることを確認してください。両方のマネージャでセキュリティ分析とロギング(オンプレミス)を有効にするには、[Cisco Security Analytics and Logging\(オンプレミス\): Firepower イベント統合ガイド](#) [英語] を参照してください。

- フェールオーバー設定の保存: フェールオーバー設定を保存すると、プライマリ マネージャがアプライアンスをアクティブに監視および管理し、セカンダリ マネージャが読み取り専用になります。詳細については、「[フェールオーバー設定の保存](#)」を参照してください。

計画済み フェールオーバー ロール	要約	IP アドレス (IP Address)
Primary マネージャ	アクティブに監視および管理する Secure Network Analytics	
Secondary マネージャ	読み取り専用	

## 2. マネージャ設定とデータベースのバックアップ



フェールオーバー用にマネージャを設定する前に、各アプライアンスの設定とデータベースをバックアップします。マネージャを完全に復元するには、両方のバックアップが必要です。

新規インストール: マネージャが新規インストールで、今後設定を復元する必要がない場合は、この手順をスキップできます。次の項に進みます。「[3. 信頼ストアへの証明書の追加](#)」。

**!** バックアップがないと、フェールオーバー設定中に問題が発生した場合にファイルを回復できません。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。

### 1. バックアップ設定ファイルの作成

各マネージャのバックアップ設定ファイルを作成するには、次の手順を実行します。マネージャが Central Manager としてアプライアンスも管理している場合、マネージャ バックアップ設定ファイルと Central Management バックアップ設定ファイルが作成されます。

1. **セカンダリ** 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。[Central Management] を選択します。
3. マネージャの  ([省略記号 (Ellipsis)]) アイコンをクリックします。
4. [Support] を選択します。
5. [Configuration Files] タブを選択します。
6. [Backup Actions] ドロップダウンメニューをクリックします。
7. [Create Backup] を選択します。
8. [Download] をクリックします。安全な場所にファイルを保存します。
9. プライマリ マネージャにログインします。手順 2 ~ 8 を繰り返して、プライマリ マネージャのバックアップ設定ファイルを保存します。

### 2. マネージャ データベースのバックアップ

マネージャ データベースをリモートファイルシステムにバックアップするには、Central Management とアプライアンス管理インターフェイスを使用します。

1. データベースのスナップショットの削除
2. データベースのバックアップ
3. データベースのスナップショットの削除
4. データベースのバックアップの確認

**!** プライマリ マネージャとセカンダリ マネージャでデータベースのバックアップ手順を完了していることを確認します。

## 1. データベースのスナップショットの削除

バックアップファイルを作成する前に、次の手順を使用して、マネージャ データベースに保存されているスナップショットをすべて削除してください。

**!** マネージャ データベースのスナップショットは必ず削除してください。これは、バックアップを成功させるために不可欠な手順です。

1. マネージャ アプライアンスコンソールに admin としてログインします。
2. **スナップショットの確認:** 次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select * from
database_snapshots;"
```

3. **スナップショット(存在する場合)の削除:** 次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. **スナップショットフォルダが削除されるまで待機:** 次を確認します。

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

結果が空でない場合は、そのまま待機します。データベースのサイズによっては、フォルダが削除されるまで数分かかる場合があります。

5. 手順 1 ~ 4 を繰り返して、保存されているすべてのマネージャ データベースのスナップショットを削除します。

## 2. データベースのバックアップ

次の手順を使用して、マネージャ データベースをバックアップします。また、次の情報を確認してください。

- **領域:** リモートファイル システムに、データベースのバックアップを保存するための十分な空き領域があることを確認します。
- **時間:** データベースを 1 回バックアップすると、以後は前回のバックアップからの変更点だけがバックアップされるため、バックアップにかかる時間は短くなります。このプロセスでは、1 分あたり約 0.5 GB ~ 2 GB のデータがバックアップされます。

1. マネージャ 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。

Central Management で、マネージャ ... ([省略記号 (Ellipsis)]) アイコン > [アプライアンス統計情報の表示 (View Appliance Statistics)] の順にクリックします。

Central Management Appliance Manager Update Manager App Manager Smart Licensing Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type	IP Address	Actions
Connected		Manager		<ul style="list-style-type: none"> <li>Edit Appliance Configuration</li> <li><b>View Appliance Statistics</b></li> <li>Support</li> <li>Reboot Appliance</li> <li>Shut Down Appliance</li> <li>Remove This Appliance</li> </ul>
Connected	nfl	Flow Collector		...
Connected	fs	Flow Sensor		...
Connected	fr	UDP Director		...

2. 次の手順を実行して、リモートファイルシステム上に必要となるデータベース バックアップ保存容量を確認します。

- [ホーム (Home)] をクリックします。
- [ディスク使用量 (Disk Usage)] セクションを見つけます。
- `/lancope/var` ファイルシステムの [Used (byte)] 列を確認します。データベースのバックアップを保存するためには、リモートファイルシステム上に少なくともこの数値にその15%を足した分の空き容量が必要です。

### Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	45%	19.1G	8.09G	10.04G
<code>/lancope/var</code>	43%	33.32G	14G	18.62G

3. [設定 (Configuration)] > [リモートファイルシステム (Remote File System)] の順にクリックします。

### Remote File System

IP Address:	<input type="text"/>
Port Number:	<input type="text" value="445"/>
Share Name:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
Security Protocol:	<input type="radio"/> ntlm <input checked="" type="radio"/> ntlmv2

4. バックアップ ファイルを保存するリモート ファイル システムの設定を使用して、フィールドに入力します。

Secure Network Analytics ファイル共有では CIFS (Common Internet File System)、別名 SMB (Server Message Block) というプロトコルが使用されます。

5. [適用 (Apply)] をクリックして、設定ファイルに設定を適用します。

パスワードを入力しても [適用 (Apply)] ボタンが有効にならない場合、[リモートファイルシステム (Remote File System)] ページの空白部分を 1 回クリックすると有効になります。

6. [テスト (Test)] をクリックして、Secure Network Analytics アプライアンスとリモートファイルシステムが相互に通信できることを確認します。

テストが完了したら、[リモートファイルシステム (Remote File System)] ページの下部に次のメッセージが表示されていることを確認します。

**File sharing appears to be properly configured.**

7. [サポート (Support)] > [データベースのバックアップおよび復元 (Backup/Restore Database)] の順にクリックします。
8. [バックアップの作成 (Create Backup)] をクリックします。このプロセスは長時間かかる場合があります。

- バックアッププロセスの開始後は、マウスをページから離してもプロセスは中断されません。ただし、バックアップの実行中に、[キャンセル (Cancel)] をクリックすると、アプライアンスを再起動しないとバックアップを再開できなくなる場合があります。
- バックアップが完了するまで、画面に表示される指示に従います。
- バックアッププロセスの詳細を確認するには、[ログの表示 (View Log)] をクリックします。

9. [閉じる (Close)] をクリックして進捗状況ウィンドウを閉じます。



終了する前にバックアップをキャンセルする場合は、必ずデータベースのスナップショットを削除してください。手順については、「[3. データベースのスナップショットの削除](#)」を参照してください。

### 3. データベースのスナップショットの削除

バックアップファイルを保存後、次の手順を使用してマネージャ データベースのスナップショットを削除します。



マネージャ データベースのスナップショットは必ず削除してください。

1. マネージャ アプライアンスコンソールに admin としてログインします。
2. **スナップショットの確認**: 次のように入力します。



```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select * from
database_snapshots;"
```

3. **スナップショット(存在する場合)の削除:** 次のように入力します。

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. **スナップショットフォルダが削除されるまで待機:** 次を確認します。

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

結果が空でない場合は、そのまま待機します。データベースのサイズによっては、フォルダが削除されるまで数分かかる場合があります。

5. 手順 1 ~ 4 を繰り返して、保存されているすべてのマネージャデータベースのスナップショットを削除します。

#### 4. データベースのバックアップの確認

「[2. マネージャデータベースのバックアップ](#)」バックアップし、各マネージャのデータベースのバックアップを保存したことを確認します。

## 3. 信頼ストアへの証明書の追加

次の手順を使用して、必要なアプライアンス アイデンティティ証明書とチェーンを信頼ストアに保存します。

### 信頼ストアの要件

この手順では、次の要件について説明します。

- セカンダリ マネージャ証明書をプライマリ マネージャ信頼ストアに追加する。
- プライマリ マネージャ証明書をセカンダリ マネージャ信頼ストアに追加する。

### 証明書チェーン

アプライアンス アイデンティティ証明書に証明書チェーンが含まれている場合、信頼ストアに証明書チェーン(ルートおよび中間)を必ず追加してください。

### 信頼ストアへの証明書のアップロード

各ファイルを個別にアップロードします。

#### 1. アプライアンス アイデンティティ証明書のダウンロード

次の手順を使用して、アプライアンス アイデンティティ証明書をダウンロードして保存します。手順は、使用しているブラウザによって異なります。

証明書がすでに保存されている場合は、この手順をスキップできます。「[2. マネージャ信頼ストアへの証明書の追加](#)」に進みます。



ブラウザのロックまたはセキュリティアイコンをクリックすることもできます。画面に表示される指示に従って証明書をダウンロードします。手順は、使用しているブラウザによって異なります。

1. ブラウザのアドレスバーで、IP アドレスの後のパスを `/secrets/v1/server-identity` に置き換えます。

例: `https://<IPaddress>/secrets/v1/server-identity`

2. 画面に表示される指示に従って証明書を保存します。


**オープン:** ファイルを表示するには、テキストファイル形式を選択します。

**トラブルシューティング:** 証明書をダウンロードするためのプロンプトが表示されない場合は、自動的にダウンロードされている場合があるため、[ダウンロード (Downloads)] フォルダを確認するか、または別のブラウザを試します。

3. 各マネージャで手順 1 と 2 を繰り返します。

## 2. マネージャ信頼ストアへの証明書の追加

次の手順を使用して、セカンダリ マネージャ アプライアンス アイデンティティ証明書とチェーン（該当する場合）をプライマリ マネージャ信頼ストアに保存します。

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。[集中管理 (Central Management)] を選択します。
3. [アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] と表示されていることを確認します。
4. マネージャの [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. [アプライアンスマネージャ (Appliance Manager)] > [全般 (General)] タブで、[信頼ストア (Trust Store)] セクションを見つけます。
7. [新規追加 (Add New)] をクリックします。

 各アプライアンス アイデンティティ証明書とチェーン（ルートおよび中間）証明書を個別にアップロードしていることを確認します。

8. [フレンドリ名 (Friendly Name)] フィールドに、証明書の名前を入力します。
9. [ファイルの選択 (Choose File)] をクリックします。証明書を選択します。
10. [証明書の追加 (Add Certificate)] をクリックします。[信頼ストア (Trust Store)] リストに証明書が表示されていることを確認します。
11. 手順 6 ~ 9 を繰り返して、他の必要な証明書を信頼ストアに追加します。
  - セカンダリ マネージャにログインしている場合は、プライマリ マネージャ証明書を追加します。
  - プライマリ マネージャにログインしている場合は、セカンダリ マネージャ証明書を追加します。
12. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って操作します。
13. [接続済み (Connected)]: [アプライアンスマネージャ (Appliance Manager)] ページで、[アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] に戻っていることを確認します。
14. 他のマネージャで手順 1 ~ 13 を繰り返します。

## Data Store 初期化後のフェールオーバーの設定

Data Store を使用して Cisco Secure Network Analytics を展開した場合は、Data Store を初期化する前にフェールオーバーを設定してください。Data Store を初期化した後にフェールオーバーを設定する場合は、以下のセクションの手順に従って、Data Store とのセキュア通信のためにセカンダリ Manager を設定します。

Data Store 初期化後にフェールオーバーを設定するプロセスの概要を以下に示します。

1. [フェールオーバーペアを設定します。](#)
2. [セカンダリ Manager を追加します。](#)

### フェールオーバーペアの設定

このガイドの「[4. フェールオーバーペアの設定](#)」セクションの指示に従って、フェールオーバーペアを設定します。このプロセスが完了すると、セカンダリ マネージャの [アプライアンスマネージャ (Appliance Manager)] に「Data Store が設定されていません (Data Store Not Configured)」というメッセージが表示されます。以下の「[Data Store 初期化後にマネージャを追加](#)」の手順に従って、セカンダリ マネージャを設定します。

### Data Store 初期化後にマネージャを追加


Data Store をすでに初期化している場合は、次の手順に従って Data Store に Manager を追加します。

データストアなしで使用するように設定した既存の マネージャ または Flow Collector がある場合は、各アプライアンスを工場出荷時のデフォルトにリセット (RFD) してから、データストア ありで使用するように設定して展開に追加する必要があります。

1. RFD: 『[Secure Network Analytics System Configuration Guide](#)』の「Resetting Factory Defaults」セクションの指示に従ってください。

**i** 現在のネットワーク設定を保持するか破棄するかを選択できます。破棄する場合は、それらのネットワーク設定を再設定する必要があります。

2. 「1. Configuring Your Environment using First Time Setup」と「2. Configuring the Managed System」(『[Secure Network Analytics System Configuration Guide](#)』に記載) の手順に従って、アプライアンスを設定し Central Management に追加します。初回セットアップでアプライアンスを設定します。
3. プライマリ マネージャのアプライアンスコンソールに root としてログインします。
4. 「SystemConfig」と入力して、Enter キーを押します。
5. [データストア (Data Store)] を選択します。
6. [SSH] を選択します。アプライアンス間で SSH が有効になるまで待ちます。
7. [データストア (Data Store)] メニューから [新しいアプライアンス (New Appliances)] を選択します。画面の指示に従います。
8. SystemConfig を終了します。

 [データストア (Data Store)] メニューを終了すると、システムで以前の SSH 設定が復元されます。

9. Central Management をチェックして、アプライアンスのステータスが [接続済み (Connected)] になっていることを確認します。

## 4. フェールオーバーペアの設定

次の手順を使用して、フェールオーバー用のマネージャを設定します。フェールオーバー設定を保存すると、セカンダリマネージャドメイン設定が削除されます。セカンダリは読み取り専用になり、プライマリマネージャと同期します。詳細については、「[フェールオーバー設定の保存](#)」を参照してください。


### はじめる前に

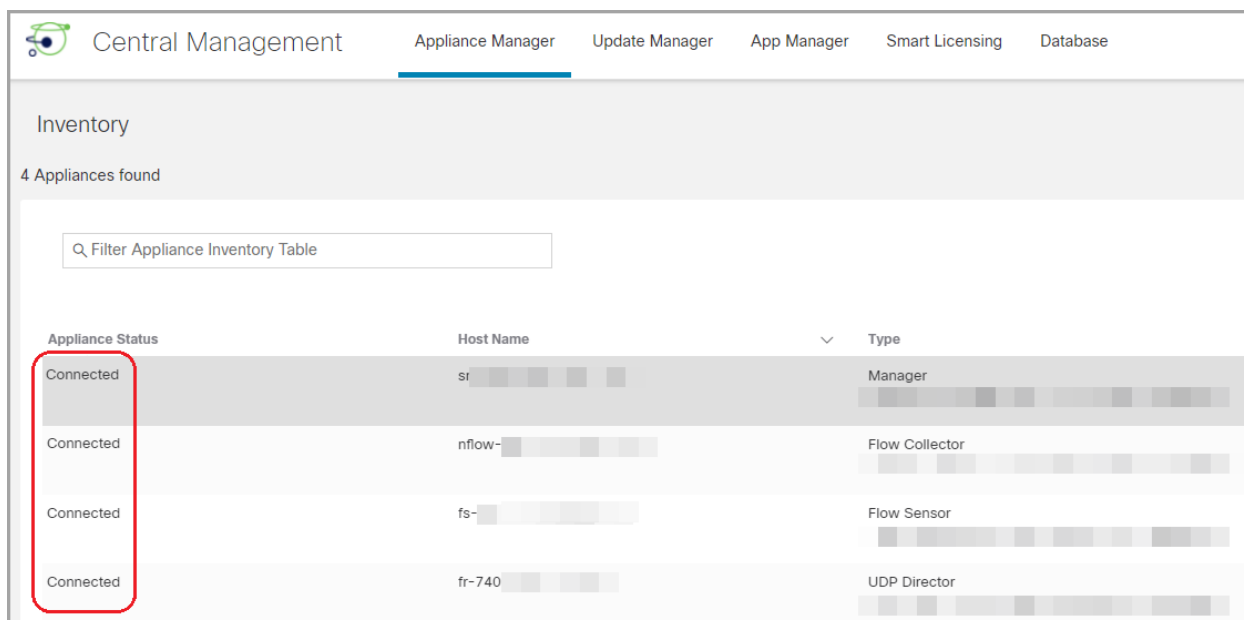
これらの手順を開始する前に、次の手順を完了してください。

1. フェールオーバーロールの計画
2. マネージャ設定とデータベースのバックアップ
3. 信頼ストアへの証明書の追加

**▲** プライマリマネージャを設定する前に、セカンダリマネージャをフェールオーバー用に設定してください。フェールオーバー設定を保存すると、セカンダリマネージャドメイン設定が削除されるため、手順を順番に実行してください。

### 1. マネージャアプライアンスステータスの確認

1. プライマリ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。[Central Management] を選択します。
3. 各アプライアンスの [アプライアンスステータス (Appliance Status)] が [接続済み (connected)] と表示されていることを確認します。



Central Management | Appliance Manager | Update Manager | App Manager | Smart Licensing | Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director



4. **セカンダリ** マネージャにログインします。
5. [グローバル設定 (Global Settings)] アイコンをクリックします。[集中管理 (Central Management)] を選択します。
6. [アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] と表示されていることを確認します。
7. 両方のマネージャにログインしたまま、次の手順に進みます。

## 2. セカンダリマネージャの設定

フェールオーバー設定を保存すると、セカンダリ マネージャドメイン設定が削除されます。セカンダリは読み取り専用になり、プライマリ マネージャと同期します。詳細については、「[フェールオーバー設定の保存](#)」を参照してください。

1. **セカンダリ** マネージャで、[セキュリティ分析ダッシュボード (Security Insight Dashboard)] タブをクリックします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [マネージャ設定 (Manager Configuration)] を選択します。
4. [フェールオーバー設定 (Failover Configuration)] タブをクリックします。
5. [フェールオーバーロール (Failover Role)] ドロップダウンメニューをクリックします。[セカンダリ (Secondary)] を選択します。

The screenshot shows the 'Manager Configuration' page with the 'Failover Configuration' tab selected. A blue informational message at the top states: 'Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).' Below this, the 'Failover Role\*' dropdown menu is highlighted with a red box and shows 'Secondary' selected. At the bottom, there is a section for 'Other Manager' with an 'IP Address\*' field containing '141' and a 'Failover Role' dropdown menu set to 'Primary'.

6. [IPアドレス (IP Address)] フィールドにその他のマネージャの IP アドレスを入力します。そのマネージャがプライマリ マネージャになります。
7. [保存 (Save)] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。

## 3. プライマリマネージャの設定

1. **プライマリ** マネージャで、[セキュリティ分析ダッシュボード (Security Insight Dashboard)] タブをクリックします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [マネージャ設定 (Manager Configuration)] を選択します。
4. [フェールオーバー (Failover)] タブをクリックします。
5. [フェールオーバーロール (Failover Role)] ドロップダウンメニューをクリックします。[プライマリ (Primary)] を選択します。

Manager Configuration

Name: [redacted] IP Address: [redacted] 121 Model: [redacted] Serial: [redacted] Seal

Data Retention DSCP Configuration Failover Configuration

Failover Configuration Cancel Save

● Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).

Failover Role\*  
Primary

Other Manager

IP Address\* [redacted].103 Failover Role  
Secondary

6. [IPアドレス (IP Address)] フィールドに、セカンダリ マネージャの IP アドレスを入力します。
7. [保存 (Save)] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。


## 5. フェールオーバー設定の確認

次の手順を使用して、マネージャがフェールオーバーおよび通信用に設定されていることを確認します。

### 1. 設定の変更の確認

プライマリ マネージャにフェールオーバー設定の変更が表示されることを確認します。各アプライアンスの [アプライアンスステータス (Appliance Status)] に [接続済み (connected)] と表示されていることも確認します。

1. プライマリ マネージャで、Central Management を開きます。

[グローバル設定 (Global Settings)]  アイコンをクリックします。[集中管理 (Central Management)] を選択します。

2. 次を確認します。





- セカンダリ マネージャがインベントリに表示されていること。
- 各アプライアンスの [アプライアンスステータス (Appliance Status)] に [接続済み (connected)] と表示されていること。


### プライマリおよびセカンダリ マネージャの表示の確認

Inventory

4 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	fs- [redacted] -1	Flow Sensor FSVE-KVM-	[redacted] 134	
Config Changes Pending	nflow- [redacted]  5-2	Flow Collector FCNFVE-KVM-	[redacted] 135	
Config Changes Pending	[redacted] -103-4	Manager	[redacted] 103	
Connected	[redacted] -141-4	Manager	[redacted] 141	

 [集中管理 (Central Management)] が更新されるまで待ちます。アプライアンスの [アプライアンスステータス (Appliance Status)] に [設定の変更が保留中 (Config Changes Pending)] と表示されます。

すべてのアプライアンスが [接続済み (connected)] になっていることの確認

Central Management | Appliance Manager | Update Manager | App Manager | Smart Licensing | Database

Inventory

4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

## 2. フローコレクションの確認

次の手順を使用して、セカンダリマネージャが読み取り専用として動作し、フローを受信していることを確認します。

1. セカンダリマネージャにログインします。
2. マネージャが読み取り専用であることを示す通知が表示されます。セカンダリマネージャが読み取り専用に変更されていない場合は、フェールオーバー設定を確認します。

Warning - Secondary Manager

You have logged in to your secondary Manager, which is a read-only device that is managed by your primary Manager. To change settings, log in to your primary Manager.

For assistance, please contact [Cisco Support](#).

OK

3. [セキュリティ分析ダッシュボード (Security Insight Dashboard)] で、フローコレクショントレンドを確認します。



4. フローコレクションが進行中の場合、アクションは不要です。フェールオーバー設定が完了しました。

フローコレクションが停止している場合は、Central Management を使用して、次の順番でフローコレクタおよびセカンダリ マネージャを再起動します（または「[トラブルシューティング](#)」を参照します）。


- プライマリ マネージャにログインします。
- [グローバル設定 (Global Settings)] アイコンをクリックします。[集中管理 (Central Management)] を選択します。
- Flow Collector を見つけます。
- [アクション (Actions)] メニューをクリックします。
- [アプライアンスの再起動 (Reboot Appliance)] を選択します。画面に表示される指示に従って操作します。
- フローコレクタ: 手順を繰り返して、Central Management ですべての Flow Collector を再起動します。
- セカンダリ マネージャ: 手順を繰り返して、セカンダリ マネージャを再起動します。



再起動したためにプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが [接続済み (Connected)] に戻り、セカンダリ マネージャが検出されると、プライマリはフェールオーバーロールを再開します。プライマリ マネージャのロールがセカンダリに変更され、解決しない場合は、「[トラブルシューティング](#)」を参照してください。

# フェールオーバーロールの変更

次の手順を使用して、プライマリおよびセカンダリ マネージャのロールを変更します。ロールは自動的に交換されないことに注意してください。

 フェールオーバー設定を変更すると、セカンダリ マネージャドメインの設定が削除されるため、手順を順番に実行してください。


## 時刻

セカンダリ マネージャをプライマリに昇格させると、すべてのアプライアンスのステータスが [構成チャンネルがダウン (Config Channel Down)] から [接続済み (connected)] に変わるまでに少なくとも 1 時間かかることがあります。[集中管理 (Central Management)] でステータスをモニターします。手順については、「[5. フェールオーバー設定の確認](#)」を参照してください。

## 1. プライマリマネージャのバックアップ

フェールオーバーロールを変更する前に、今後設定を復元する必要がある場合に備えてプライマリ マネージャをバックアップします。詳細については、「[2. マネージャ設定とデータベースのバックアップ](#)」を参照してください。

## 2. アプライアンスステータスの確認

1. プライマリ 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。[集中管理 (Central Management)] を選択します。
3. 各アプライアンスの [アプライアンスステータス (Appliance Status)] が [接続済み (connected)] と表示されていることを確認します。
  - マネージャ: プライマリまたはセカンダリ マネージャの [アプライアンスステータス (Appliance Status)] が [構成チャンネルがダウン (Config Channel Down)] と表示されている場合は、通信設定を確認し「[トラブルシューティング](#)」を参照してください。
  - その他のアプライアンス: フローコレクタ、フローセンサー、または UDP Director のアプライアンスステータスに [構成チャンネルがダウン (Config Channel Down)] と表示されている場合は、設定を確認し、Central Management を使用してアプライアンスを再起動します ([アクション (Actions)] メニューの [アプライアンスの再起動 (Reboot Appliance)])。その他のトラブルシューティングについては、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド](#) [英語] を参照してください。



Appliance Status	Host Name	Type
Connected	sr-...	Manager
Connected	nflow-...	Flow Collector
Connected	fs-...	Flow Sensor
Connected	fr-740	UDP Director

### 3. フェールオーバー設定の変更

次の手順を使用して、プライマリ マネージャをセカンダリに変更し、セカンダリ マネージャをプライマリに昇格させます。

この設定では、プライマリ マネージャがセカンダリ マネージャになり、そのドメイン設定が削除されます。セカンダリは読み取り専用になり、新しく昇格したプライマリ マネージャと同期します。詳細については、「[フェールオーバー設定の保存](#)」を参照してください。

**!** フェールオーバー設定の変更が完了するまで、[集中管理(Central Management)] でアプライアンスを追加または削除しないでください。

#### 1. プライマリ マネージャをセカンダリに変更する

1. 現在のプライマリ マネージャで、[セキュリティ分析ダッシュボード (Security Insight Dashboard)] タブをクリックします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [マネージャ設定 (Manager Configuration)] を選択します。
4. [フェールオーバー設定 (Failover Configuration)] タブをクリックします。
5. [フェールオーバーロール (Failover Role)] が [プライマリ (Primary)] と表示されていることを確認します。

プライマリ マネージャが [セカンダリ (Secondary)] と表示されている場合は、「[トラブルシューティング](#)」を参照してください。

6. [フェールオーバーロール (Failover Role)] ドロップダウンメニューをクリックします。[セカンダリ (Secondary)] を選択します。
7. [保存 (Save)] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。

## 2. セカンダリ マネージャをプライマリに変更する


1. **セカンダリ** 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. [マネージャ設定 (Manager Configuration)] を選択します。
4. [フェールオーバー設定 (Failover Configuration)] タブをクリックします。
5. フェールオーバーロールがセカンダリとして表示されていることを確認します。
6. [フェールオーバーロール (Failover Role)] ドロップダウンメニューをクリックします。[プライマリ (Primary)] を選択します。
7. [保存 (Save)] をクリックします。
8. 画面に表示される指示に従って、変更を保存します。

## 4. 設定の変更の確認

フェールオーバー設定の変更を確認するには、「[5. フェールオーバー設定の確認](#)」に進み、手順に従います。

# ネットワーク インターフェイスの変更

マネージャがフェールオーバー用に設定されている場合は、アプライアンスのネットワーク インターフェイス、ホスト名、またはネットワークドメイン名を変更する前に、フェールオーバー関係を削除します。全体的な手順は次のとおりです。

 フェールオーバー設定を削除すると、すべてのドメイン設定データがセカンダリ マネージャから削除されます。すべての手順を順番に実行してください。

## 1. フェールオーバー設定の削除


手順については、「[フェールオーバー設定の削除](#)」を参照してください。

## 2. マネージャネットワーク インターフェイスの変更

[管理対象アプライアンスの SSL/TLS 証明書ガイド](#) [英語] の手順に従います。

手順の一環として、アプライアンスを Central Management から一時的に削除します。アプライアンス アイデンティティ証明書が自動的に置き換えられます。

アプライアンス アイデンティティ証明書は、この手順の一環として自動的に置き換えられます。

 アプライアンスがカスタム証明書を使用している場合は、これらの設定の変更について [シスコサポート](#) にお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

## 3. マネージャ フェールオーバーの設定

このガイドの手順に従い、フェールオーバーを設定します。マネージャをバックアップし、新しい証明書をマネージャ信頼ストアに追加します。


# フェールオーバー設定の削除

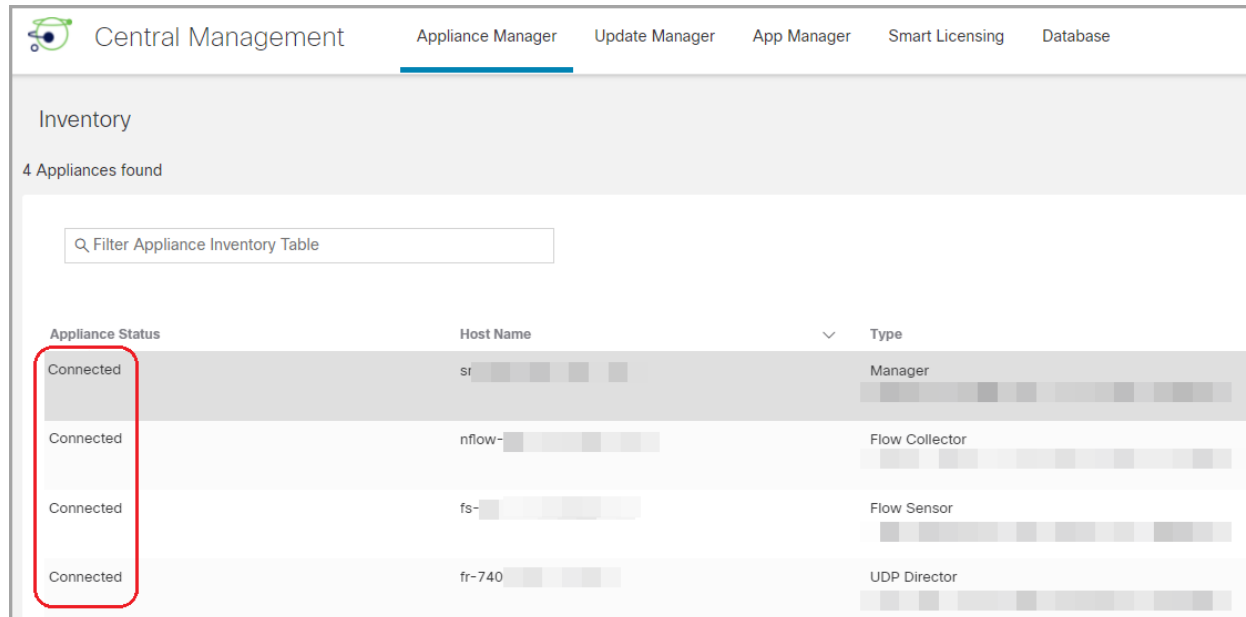
フェールオーバー設定を削除する前に、両方のマネージャのステータスを確認し、手順を順番に実行してください。

**!** フェールオーバー設定を削除すると、すべてのドメイン設定データがセカンダリ マネージャから削除されます。

## 1. アプライアンス ステータスの確認

開始する前に、プライマリ マネージャにセカンダリ マネージャが管理対象アプライアンスとして表示されていること、および両方の Manager が [接続済み (Connected)] と表示されていることを確認します。

1. **プライマリ 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。[集中管理 (Central Management)] を選択します。
3. 各アプライアンスの [アプライアンスステータス (Appliance Status)] が [接続済み (connected)] と表示されていることを確認します。
  - マネージャ: プライマリまたはセカンダリ マネージャの [アプライアンスステータス (Appliance Status)] が [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、通信設定を確認し「[トラブルシューティング](#)」を参照してください。
  - その他のアプライアンス: フローコレクタ、フローセンサー、または UDP Director のアプライアンスステータスに [構成チャネルがダウン (Config Channel Down)] と表示されている場合は、設定を確認し、Central Management を使用してアプライアンスを再起動します ([アクション (Actions)] メニューの [アプライアンスの再起動 (Reboot Appliance)])。その他のトラブルシューティングについては、[Cisco Secure Network Analytics システム コンフィギュレーション ガイド](#) [英語] を参照してください。



Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

## 2. フェールオーバーロールの確認

1. **プライマリ** マネージャで、[セキュリティ分析ダッシュボード (Security Insight Dashboard)] タブをクリックします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。[マネージャ設定 (Manager Configuration)] を選択します。
3. [フェールオーバー設定 (Failover Configuration)] タブをクリックします。
4. [フェールオーバーロール (Failover Role)] が [プライマリ (Primary)] と表示されていることを確認します。

Manager Configuration

Name: IP Address: 121 Model: Serial: 3eaf

Data Retention DSCP Configuration Failover Configuration

Failover Configuration Cancel Save

Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).

Failover Role\*  
Primary

Other Manager

IP Address\* .103 Failover Role  
Secondary

5. **セカンダリ** マネージャにログインします。手順 1 ~ 4 に従って、[フェールオーバーロール (Failover Role)] が [セカンダリ (Secondary)] として表示されていることを確認します。
  - 各マネージャのフェールオーバーロールが正しい場合は、両方のマネージャで [フェールオーバー設定 (Failover Configuration)] タブを開いたままにし、「**3. フェールオーバー設定の削除**」に進みます。
  - 両方のマネージャがセカンダリとして表示されている場合は、フェールオーバー設定を更新して、1つのプライマリ マネージャと1つセカンダリ マネージャが存在する状態にしてから、削除を進めます。手順については、「**フェールオーバーロールの変更**」を参照してください。

**!** 「**フェールオーバーロールの変更**」の設定の順序と手順に従ってください。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。

## 3. フェールオーバー設定の削除

次の手順を使用して、フェールオーバー設定を削除します。次の手順を順番に実行してください。

**!** フェールオーバー設定を削除すると、すべてのドメイン設定データがセカンダリ マネージャから削除されます。

1. プライマリ マネージャの [フェールオーバー設定 (Failover Configuration)] タブに移動します。
2. [削除 (Delete)] をクリックします。
3. 画面の指示に従って、フェールオーバー設定を削除します。

**!** フェールオーバー設定を削除すると、すべてのドメイン設定データがセカンダリ マネージャから削除されます。

4. セカンダリ マネージャの [フェールオーバー設定 (Failover Configuration)] タブに移動します。
5. [削除 (Delete)] をクリックします。
6. 画面の指示に従って、フェールオーバー設定を削除します。

## 4. Central Management からのセカンダリ マネージャの削除

1. プライマリ マネージャで、Central Management を開きます。

[グローバル設定 (Global Settings)] アイコンをクリックします。[集中管理 (Central Management)] を選択します。

2. セカンダリ マネージャを見つけます。

**!** 削除する前に、セカンダリ マネージャの IP アドレスを確認します。

3. [アクション (Actions)] メニューをクリックします。[このアプライアンスを削除 (Remove This Appliance)] を選択します。
4. 画面に表示される指示に従って、Central Management からセカンダリ マネージャを削除します。

## 5. セカンダリ マネージャ証明書の削除

次の手順を使用して、その他のアプライアンスの信頼ストアからセカンダリ マネージャ証明書を削除します。

**!** 証明書を削除する前に、セカンダリ マネージャの IP アドレスを確認します。

1. プライマリ マネージャの Central Management に戻ります。次を確認します。
  - セカンダリ マネージャがインベントリに表示されていないこと。
  - 各アプライアンスの [アプライアンスステータス (Appliance Status)] に [接続済み (Connected)] と表示されていること。
2. 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。
3. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
4. [全般 (General)] タブをクリックします。[信頼ストア (Trust Store)] セクションを見つけます。
5. セカンダリ マネージャ証明書を見つけます。
6. [削除 (Delete)] をクリックして、各セカンダリ マネージャ証明書を信頼ストアから削除します。
7. [集中管理 (Central Management)] の各アプライアンスに対して手順 2 ~ 6 を繰り返します。

---

## 6. セカンダリ マネージャを工場出荷時の初期状態にリセットする

セカンダリ マネージャを使用するには、工場出荷時の初期状態にリセットします。[Cisco Secure Network Analytics システム コンフィギュレーション ガイド \[英語\]](#) の手順に従います。

この手順では、次の手順を実行します。

- アプライアンスを工場出荷時の初期状態にリセットする。
- IP アドレスを設定する。
- アプライアンス セットアップ ツールを使用してマネージャを設定する。

# トラブルシューティング

## マネージャがオフラインまたは障害状態になっている

ネットワークがダウンした場合、マネージャをシャットダウンして再起動した場合やその他のさまざまな理由で、プライマリ マネージャがオフラインになることがあります。

再起動したためにプライマリ マネージャがオフラインになった場合、アプライアンスのステータスが [接続済み (Connected)] に戻り、セカンダリ マネージャが検出されると、プライマリはフェールオーバーロールを再開します。

プライマリ マネージャ ロールがセカンダリに変更され、解決しない場合は、次のシナリオを確認して、必要な作業を決定します。

**i** 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。

次の場合...	結合できるフィールド	次の操作
プライマリ マネージャで障害が発生したか、またはシャットダウンして再起動しました。	既存のセカンダリ マネージャをプライマリに手動で昇格しました。プライマリがオンラインです。	新しいプライマリ マネージャがプライマリとしてのロールを維持します。再起動すると、元のプライマリ マネージャが自動的にセカンダリとしての新しいロールを担います。
プライマリ マネージャで障害が発生したか、またはシャットダウンして再起動しました。	既存のセカンダリ マネージャをプライマリに手動で昇格していないため、オンラインのプライマリ マネージャがありません。	元のプライマリ マネージャを再起動すると、プライマリと元のセカンダリ マネージャの両方がセカンダリのロールを担います。いずれかのマネージャをプライマリ マネージャに昇格させます。手順については、「 <a href="#">フェールオーバーロールの変更</a> 」を参照してください。
ネットワークが停止し、復元されました。	既存のセカンダリ マネージャをプライマリに手動で昇格しました。プライマリがオンラインです。	新しいプライマリ マネージャがプライマリとしてのロールを維持します。再起動すると、元のプライマリ マネージャが自動的にセカンダリとしての新しいロールを担います。
ネットワークが停止し、復元されました。	既存のセカンダリ マネージャをプライマリに手動で昇格していないため、オンラインのプライマリ マネージャがありません。	元のプライマリ マネージャはプライマリとしてのロールを自動的に再開し、元のセカンダリ マネージャはセカンダリ マネージャとしてのロールを自動的に再開します。



## 信頼エラー

マネージャが信頼されていないというエラーが表示された場合は、信頼ストアの証明書を確認します。手順については、「[3. 信頼ストアへの証明書の追加](#)」を参照してください。

## セカンダリマネージャにフローが表示されない

セカンダリマネージャにフローが表示されない場合は、セカンダリマネージャ証明書が Flow Collector の信頼ストアに保存されていることを確認します。手順については、「[3. 信頼ストアへの証明書の追加](#)」を参照してください。

## パスワードの有効期限切れ

フェールオーバー設定が保存されると、プライマリマネージャからローカルユーザーとパスワードログイン情報がセカンダリマネージャにプッシュされるため、両方が同期されます。つまり、プライマリマネージャとセカンダリマネージャへのログインには同じパスワードを使用します。セカンダリマネージャのパスワードを変更するには、プライマリマネージャにログインします。

プライマリマネージャがダウンし、パスワードの有効期限が切れた場合、セカンダリマネージャを使用してパスワードを変更することはできません。この場合、プライマリマネージャアプライアンスのステータスが [接続済み (Connected)] に戻るまで待ちます。その後、パスワードを変更できます。

- パスワードをデフォルトにリセットするには、[Cisco Secure Network Analytics システム コンフィギュレーションガイド \[英語\]](#) を参照してください。
- プライマリマネージャを工場出荷時の初期状態にリセットする、返品許可を処理する、または再導入する必要がある場合は、セカンダリマネージャも工場出荷時の初期状態にリセットしてから、フェールオーバー関係を再設定する必要があります。工場出荷時の初期状態にリセットするには、[Cisco Secure Network Analytics システム コンフィギュレーションガイド \[英語\]](#) を参照してください。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。

## 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)