

FTDのフェールオーバーステータスメッセージについて

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[フェールオーバーステータスメッセージ](#)

[使用例 – フェールオーバーなしのデータリンクダウン](#)

[使用例 – インターフェイスのヘルスエラー](#)

[使用例 – ディスク使用率が高い](#)

[使用例 – Lina Traceback](#)

[使用例 – Snortインスタンスの停止](#)

[使用例 – ハードウェアまたは電源の障害](#)

[使用例 – MIO-Heartbeat障害 \(ハードウェアデバイス\)](#)

[関連情報](#)

概要

このドキュメントでは、Secure Firewall Threat Defense(FTD)のフェールオーバーステータスメッセージを理解する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure FTDのハイアベイラビリティ(HA)セットアップ
- Cisco Firewall Management Center(FMC)の基本的な操作性

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FMC v7.2.5
- Cisco Firepower 9300シリーズ v7.2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

フェールオーバーのヘルスマモニタリングの概要：

FTDデバイスは、各ユニットの全体的な健全性とインターフェイスの健全性を監視します。FTDは、ユニットのヘルスマモニタリングとインターフェイスモニタリングに基づいて各ユニットの状態を判別するためにテストを実行します。HAペアの各ユニットの状態を判別するテストが失敗すると、フェールオーバーのイベントがトリガーされます。

フェールオーバーステータスメッセージ

使用例 – フェールオーバーなしのデータリンクダウン

FTD HAでインターフェイスモニタリングが有効になっていない場合、データリンク障害の場合、インターフェイスに対するヘルスマモニタテストが実行されないため、フェールオーバーイベントはトリガーされません。

この図は、データリンク障害のアラートを示していますが、フェールオーバーアラートはトリガーされません。

The screenshot shows the Cisco Secure Management Center interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, and user 'admin'. Below the navigation, there are status indicators: 'Normal (2)', 'Deployment Pending (1)', and 'Upgrade (0)'. A notification box is highlighted with a red border, containing the text: 'Interface Status - 10.82.141.171', 'Interface 'Ethernet1/3' is not receiving any packets', and 'Interface 'Ethernet1/3' has no link'. Below the notification, there is a table with columns: Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The table contains two rows of device information.

Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:4 Security Module - 1	Essentials, IPS (2 more...)	FTD HA	🔄
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.c Security Module - 1	Essentials, IPS (2 more...)	FTD HA	🔄

リンクダウンアラート

データリンクの状態とステータスを確認するには、次のコマンドを使用します。

- show failover – 各ユニットおよびインターフェイスのフェールオーバーステータスに関する情報を表示します。

Monitored Interfaces 1 of 1291 maximum

```
...
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Waiting)
Interface INSIDE (172.16.10.1): No Link (Not-Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Waiting)
Interface INSIDE (172.16.10.2): Normal (Waiting)
Interface OUTSIDE (192.168.20.2): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
```

インターフェイスの状態が「Waiting」の場合、インターフェイスはアップ状態であるにもかかわらず、ピアユニットの対応するインターフェイスからまだhelloパケットを受信していないことを意味します。

一方、「No Link (Not-Monitored)」という状態は、インターフェイスの物理リンクがダウンしているが、フェールオーバープロセスによってモニタされていないことを意味します。

停止を避けるために、対応するスタンバイIPアドレスを持つすべての機密インターフェイスでインターフェイスヘルスマニタを有効にすることを強くお勧めします。

インターフェイスモニタリングを有効にするには、Device > Device Management > High Availability > Monitored Interfaces.

次の図に、「Monitored Interfaces」タブを示します。

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
DMZ	192.168.10.1	192.168.10.2				<input checked="" type="checkbox"/>
OUTSIDE	192.168.20.1	192.168.20.2				<input checked="" type="checkbox"/>
diagnostic						<input checked="" type="checkbox"/>
INSIDE	172.16.10.1	172.16.10.2				<input checked="" type="checkbox"/>

監視対象インターフェイス

モニタ対象のインターフェイスとスタンバイIPアドレスのステータスを確認するには、次のコマンドを実行します。

- show failover – 各ユニットおよびインターフェイスのフェールオーバーステータスに関する情報を表示します。

Monitored Interfaces 3 of 1291 maximum

```
...
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
```

```

Interface DMZ (192.168.10.1): Normal (Monitored)
Interface INSIDE (172.16.10.1): No Link (Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Monitored)
Interface INSIDE (172.16.10.2): Normal (Monitored)
Interface OUTSIDE (192.168.20.2): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)

```

使用例 – インターフェイスのヘルスエラー

モニタ対象のインターフェイスでユニットが15秒間helloメッセージを受信せず、1つのユニットでインターフェイステストが失敗しても、もう1つのユニットでは動作している場合、そのインターフェイスは障害が発生したとみなされます。

障害が発生したインターフェイスの数に対して定義したしきい値を満たし、アクティブユニットのインターフェイスの障害数がスタンバイユニットのインターフェイス数より多い場合は、フェールオーバーが発生します。

インターフェイスしきい値を変更するには、 [Devices > Device Management > High Availability > Failover Trigger Criteria](#).

次の図に、インターフェイスの障害時に生成されるアラートを示します。

The screenshot shows the Cisco Secure GUI interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, and user 'admin'. Below the navigation, there is a status bar showing 'Normal (2)', 'Deployment Pending (0)', 'Upgrade (0)', and 'Snort 3 (2)'. A table lists devices with columns for Model, Version, Chassis, Licenses, and Access Control. Two devices are listed: 'Firepower 9300 with FTD' with version 7.2.5 and chassis 'F241-24-04-FPR9K-1.cisco.com:4: Security Module - 1'. A notification panel on the right displays three alerts:

- Cluster/Failover Status - 10.82.141.169**: SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY_FAILED (Interface check)
- Interface Status - 10.82.141.171**: Interface 'Ethernet1/4' has no link
- Cluster/Failover Status - 10.82.141.171**: SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Check peer event for reason)

リンクがダウンした場合のフェールオーバーイベント

失敗の理由を確認するには、次のコマンドを使用します。

- `show failover state` – このコマンドでは、両方のユニットのフェールオーバー状態と、フェールオーバーの理由として最後に報告されたものが表示されます。

<#root>

firepower#

show failover state

```
This host - Primary
             Active      Ifc Failure      19:14:54 UTC Sep 26 2023
Other host - Secondary
             Failed      Ifc Failure      19:31:35 UTC Sep 26 2023
                   OUTSIDE: No Link
```

- `show failover history` - フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更と状態変更の理由が表示されます。

<#root>

firepower#

show failover history

```
=====
From State          To State          Reason
=====
19:31:35 UTC Sep 26 2023
Active              Failed            Interface check
                   This host:1
                   single_vf: OUTSIDE
                   Other host:0
```

使用例 – ディスク使用率が高い

アクティブユニットのディスク領域が90 %以上使用されている場合は、フェールオーバーイベントがトリガーされます。

次の図は、ディスクがいっぱいになったときに生成されるアラートを示しています。

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ admin | SECURE

Normal (2) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (2)

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:44 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.co Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕

PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Check peer event for reason)
 SECONDARY (FLM1946BCEX)
 FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services-. Peer failed services-diskstatus))

Cluster/Failover Status - 10.82.141.171 ✕

PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Other unit wants me Standby)
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY_FAILED (Detect Inspection engine failure(My failed services-diskstatus. Peer failed services-))

Disk Usage - 10.82.141.171 ✕

/ngfw using 98%: 186G (4.8G Avail) of 191G

ディスク使用によるフェールオーバー

失敗の理由を確認するには、次のコマンドを使用します。

- `show failover history` - フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更とその理由が表示されます。

<#root>

firepower#

`show failover history`

```

=====
From State                To State                Reason
=====
20:17:11 UTC Sep 26 2023
Active                    Standby Ready           Other unit wants me Standby
                           Inspection engine in other unit ha
20:17:11 UTC Sep 26 2023.
Active                    Standby Ready           Failed Detect Inspection engine fa
                           due to disk failure

```

- `show failover` - 各ユニットのフェールオーバーステータスに関する情報を表示します。

<#root>

firepower#

`show failover | include host|disk`

```

This host: Primary - Failed
            slot 2: diskstatus rev (1.0) status (down)
Other host: Secondary - Active
            slot 2: diskstatus rev (1.0) status (up)

```

- `df -h` – マウントされているすべてのファイル・システムに関する情報を表示します。この情報には、合計サイズ、使用領域、使用率、マウント・ポイントが含まれます。

```
<#root>
```

```
admin@firepower:/ngfw/Volume/home$
```

```
df -h /ngfw
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda6 191G 186G 4.8G 98% /ngfw
```

使用例 – Lina Traceback

回線トレースバックの場合、フェールオーバーイベントがトリガーされる可能性があります。

次の図は、lina tracebackの場合に生成されるアラートを示しています。

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a table of devices. The table has columns for 'Model', 'Version', 'Chassis', 'Licenses', and 'Access Control'. Two devices are listed: 'Firepower 9300 with FTD' with version 7.2.5 and chassis 'F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1'. The right side of the interface shows a notification panel with a 'Dismiss all notifications' button and four alerts:

- Cluster/Failover Status - 10.82.141.171**: PRIMARY (FLM19389LQR) FAILOVER_STATE_ACTIVE (HELLO not heard from peer)
- Interface Status - 10.82.141.171**: Interface 'Ethernet1/1' is not receiving any packets, Interface 'Ethernet1/2' is not receiving any packets, Interface 'Ethernet1/3' is not receiving any packets, Interface 'Ethernet1/4' is not receiving any packets
- Appliance Heartbeat - F241.24.04-FMC4600**: Appliance 10.82.141.169 is not sending heartbeats.
- Process Status - 10.82.141.169**: lina exited 2 time(s).

lina tracebackによるフェールオーバー

失敗の理由を確認するには、次のコマンドを使用します。

- `show failover history` – フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更とその理由が表示されます。

```
<#root>
```

```
firepower#
```

```
show failover history
```

```
=====
From State                To State                Reason
=====
```

```
8:36:02 UTC Sep 27 2023
```

Standby Ready	Just Active	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Just Active	Active Drain	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Drain	Active Applying Config	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Config Applied	Active	HELLO not heard from peer (failover link up, no response from peer)

lina tracebackの場合は、次のコマンドを使用してコアファイルを検索します。

```
<#root>
```

```
root@firepower:/opt/cisco/csp/applications#
```

```
cd /var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 29016
```

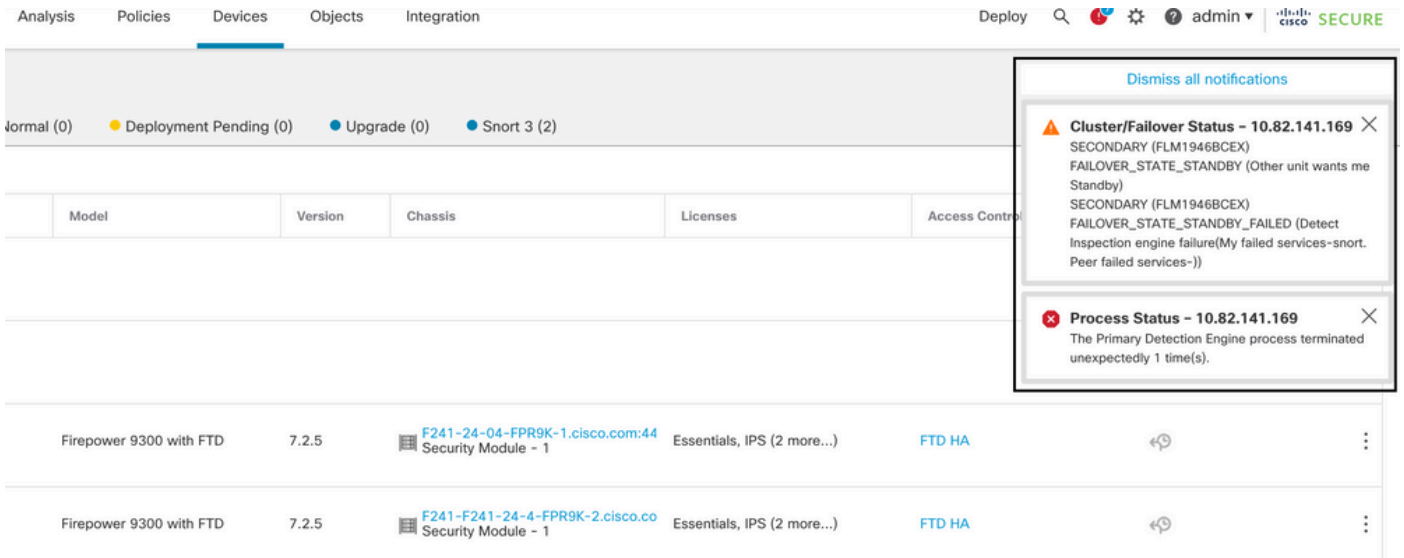
```
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

lina tracebackの場合は、トラブルシューティングファイルを収集し、コアファイルをエクスポートして、Cisco TACに連絡することを強くお勧めします。

使用例 – Snortインスタンスの停止

アクティブユニットのSnortインスタンスの50 %以上がダウンした場合は、フェールオーバーがトリガーされます。

次の図は、Snortが失敗した場合に生成されるアラートを示しています。



snortトレースバックによるフェールオーバー

次の目的で、障害の原因を確認するには、次のコマンドを使用します。

- show failover history – フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更とその理由が表示されます。

<#root>

firepower#

show failover history

```

=====
From State                To State                Reason
=====
21:22:03 UTC Sep 26 2023
Standby Ready            Just Active            Inspection engine in other unit has failed
                        due to snort failure

21:22:03 UTC Sep 26 2023
Just Active             Just Active            Active Drain Inspection engine in other unit
                        due to snort failure

21:22:03 UTC Sep 26 2023
Active Drain            Active Drain            Active Applying Config Inspection engine in o
                        due to snort failure

21:22:03 UTC Sep 26 2023
Active                  Active                  Applying Config Active Config Applied Inspect
                        due to snort failure

```

- show failover – ユニットのフェールオーバーステータスに関する情報を表示します。

<#root>

firepower#

```
show failover | include host|snort
```

```
This host: Secondart - Active  
slot 1: snort rev (1.0) status (up)  
Other host: Primary - Failed  
slot 1: snort rev (1.0) status (down)  
Firepower-module1#
```

Snort tracebackの場合は、次のコマンドを使用してcrashinfoファイルまたはコアファイルを検索します。

```
<#root>
```

```
For snort3:
```

```
root@firepower#
```

```
cd /ngfw/var/log/crashinfo/
```

```
root@firepower:/ngfw/var/log/crashinfo#
```

```
ls -l
```

```
total 4
```

```
-rw-r--r-- 1 root root 1052 Sep 27 17:37 snort3-crashinfo.1695836265.851283
```

```
For snort2:
```

```
root@firepower#
```

```
cd/var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -al
```

```
total 256912
```

```
-rw-r--r-- 1 root root 46087443 Apr 9 13:04 core.snort.24638.1586437471.gz
```

Snortトレースバックの場合は、トラブルシューティングファイルを収集し、コアファイルをエクスポートして、Cisco TACに連絡することを強くお勧めします。

使用例 – ハードウェアまたは電源の障害

FTDデバイスは、helloメッセージを使用してフェールオーバーリンクを監視することで、相手側ユニットの健全性を判断します。ユニットがフェールオーバーリンクで3回連続してhelloメッセージを受信せず、モニタ対象のインターフェイスでテストが失敗した場合は、フェールオーバーイベントがトリガーされる可能性があります。

次の図に、電源障害が発生した場合に生成されるアラートを示します。

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

Model	Version	Chassis	Licenses	Access Cor
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.cor Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisc Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Interface Status - 10.82.141.171 ✕
Interface 'Ethernet1/1' has no link
Interface 'Ethernet1/2' has no link

Cluster/Failover Status - 10.82.141.171 ✕
CLUSTER_STATE_GENERAL_FAILURE (Failover Stateful link down)
CLUSTER_STATE_GENERAL_FAILURE (Failover LAN link down)
PRIMARY (FLM19389LQR)
FAILOVER_STATE_ACTIVE (HELLO not heard from peer)

電源障害を伴うフェールオーバー

次の目的で、障害の原因を確認するには、次のコマンドを使用します。

- `show failover history` - フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更とその理由が表示されます。

<#root>

firepower#

`show failover history`

```
=====
```

From State	To State	Reason
22:14:42 UTC Sep 26 2023 Standby Ready	Just Active	HELLO not heard from peer (failover link down)
22:14:42 UTC Sep 26 2023 Just Active	Active Drain	HELLO not heard from peer (failover link down)
22:14:42 UTC Sep 26 2023 Active Drain	Active Applying Config	HELLO not heard from peer (failover link down)
22:14:42 UTC Sep 26 2023 Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link down)
22:14:42 UTC Sep 26 2023 Active Config Applied	Active	HELLO not heard from peer (failover link down)

- `show failover state` - このコマンドでは、両方のユニットのフェールオーバー状態と、フェールオーバーの理由として最後に報告されたものが表示されます。

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Failed	Comm Failure	22:14:42 UTC Sep 26 2023

使用例 – MIO-Heartbeat障害 (ハードウェアデバイス)

アプリケーションインスタンスは、定期的にハートビートをスーパーバイザに送信します。ハートビート応答が受信されない場合は、フェールオーバーイベントをトリガーできます。

次の目的で、障害の原因を確認するには、次のコマンドを使用します。

- show failover history – フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバー状態の変更とその理由が表示されます。

<#root>

firepower#

show failover history

```
=====
From State                To State                Reason
=====
02:35:08 UTC Sep 26 2023
Active                    Failed                   MIO-blade heartbeat failure
02:35:12 UTC Sep 26 2023
Failed                    Negotiation              MIO-blade heartbeat recovered
.
.
.
02:37:02 UTC Sep 26 2023
Sync File                 System Bulk Sync         Detected an Active mate
02:37:14 UTC Sep 26 2023
Bulk Sync                 Standby Ready            Detected an Active mate
```

MIO-heartbeatに障害が発生した場合は、トラブルシューティングファイルを収集し、FXOSからテクニカルログを表示して、Cisco TACに連絡することを強くお勧めします。

firepower4100/9300の場合は、show tech-support chassisとshow tech-support moduleを収集します。

FPR1000/2100およびSecure Firewall 3100/4200の場合は、show tech-supportフォームを収集します。

関連情報

- [FTDのハイアベイラビリティ](#)
- [Firepower アプライアンスでの FTD 高可用性の設定](#)
- [firepowerファイル生成手順のトラブルシューティング](#)
- [ビデオ – FXOSでshow tech-supportファイルを生成する方法](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。