

# MITERフレームワークを使用したSecure FMCでの潜在的な脅威の表示と対処

## 内容

---

[はじめに](#)

[バックグラウンド情報](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[MITERフレームワークの利点](#)

[侵入ポリシーのMITERフレームワークを表示する](#)

[侵入イベントの表示](#)

---

## はじめに

このドキュメントでは、MITERフレームワークを使用して、セキュアなFirepower Management Center(FMC)で潜在的な脅威を表示して対処する方法について説明します。

## バックグラウンド情報

MITER ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge)フレームワークは、システムに損害を与えることを目的として脅威アクターによって配布される戦術、手法、手順(TTP)に関する洞察を提供する広範なナレッジベースおよび手法です。ATT&CKは、それぞれオペレーティングシステムまたは特定のプラットフォームを表すマトリックスにコンパイルされます。「戦術」と呼ばれる攻撃の各ステージは、「手法」と呼ばれる、これらのステージを達成するために使用される特定の手法にマッピングされます。

ATT&CKフレームワークの各テクニックには、テクニック、関連する手順、考えられる防御と検出、および実際の例に関する情報が付随しています。また、MITER ATT&CKフレームワークには、使用している一連の戦術および手法に基づいて脅威グループ、活動グループ、または脅威アクターを指すグループも組み込まれています。このフレームワークでは、グループを使用して動作を分類および文書化できます。

MITERの詳細については、<https://attack.mitre.org>を参照してください。

## 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。

- Snortに関する知識
- セキュアFMC
- セキュアなFirepower Threat Defense(FTD)

## 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。

- このドキュメントは、すべてのFirepowerプラットフォームに適用されます
- ソフトウェアバージョン7.3.0を実行するセキュアFTD
- ソフトウェアバージョン7.3.0を実行するSecure Firepower Management Center Virtual(FMC)

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たものです。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。

## MITERフレームワークの利点

- MITER ATT&CK(Adversary Tactics Techniques and Common Knowledge)フレームワークに基づいて管理者がトラフィックに対して行動できるようにする侵入イベントに、MITER Tactics, Techniques, and Procedures(TTP)が追加されました。これにより、管理者はより詳細にトラフィックを表示および処理でき、脆弱性タイプ、ターゲットシステム、または脅威カテゴリ別にルールをグループ化できます。
- MITER ATT&CKフレームワークに従って侵入ルールを編成できます。これにより、特定の攻撃者の戦術と手法に従ってポリシーをカスタマイズできます。

## 侵入ポリシーのMITERフレームワークを表示する

MITERフレームワークを使用すると、侵入ルールをナビゲートできます。MITERは、ルールグループのもう1つのカテゴリであり、Talosルールグループの一部です。複数レベルのルールグループに対するルールナビゲーションがサポートされており、ルールの柔軟性と論理的なグループ化が向上します。

1. Policies > Intrusionの順に選択します。
2. 侵入ポリシーが選択されていることを確認します。
3. 表示または編集する侵入ポリシーの横にあるSnort 3バージョンをクリックします。ポップアップ表示されたSnortヘルパーガイドを閉じます。
4. Group Overrideslayerをクリックします。

グループオーバーライド層は、階層構造のルールグループのすべてのカテゴリをリストします。各ルールグループの最後のリーフルールグループに移動できます。

< Policies / Intrusion / MITRE\_ATTACK

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description MITRE\_ATTACK

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

2 items  x v +

MITRE (1 group) 1

ATT&CK Framework (1 group) 1

Search through all Rule Groups

MITRE 1 Groups

Group Name Security Level

ATT&CK Framework mixed

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techn...

6. Group Overridesの下で、Allがドロップダウンリストで選択されているため、侵入ポリシーのすべてのルールグループが左側のペインに表示されます。

7. マイタをクリックします左側のペインに表示されます。



注意：この例では「MITER」が選択されていますが、特定の要件に応じて「ルール・カテゴリ」ルール・グループ、または他のルール・グループとその下にある後続のルール・グループを選択できます。すべてのルールグループはMITERフレームワークを使用します。

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test\_policy

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

101 items  x v +

MITRE (1 group) 1

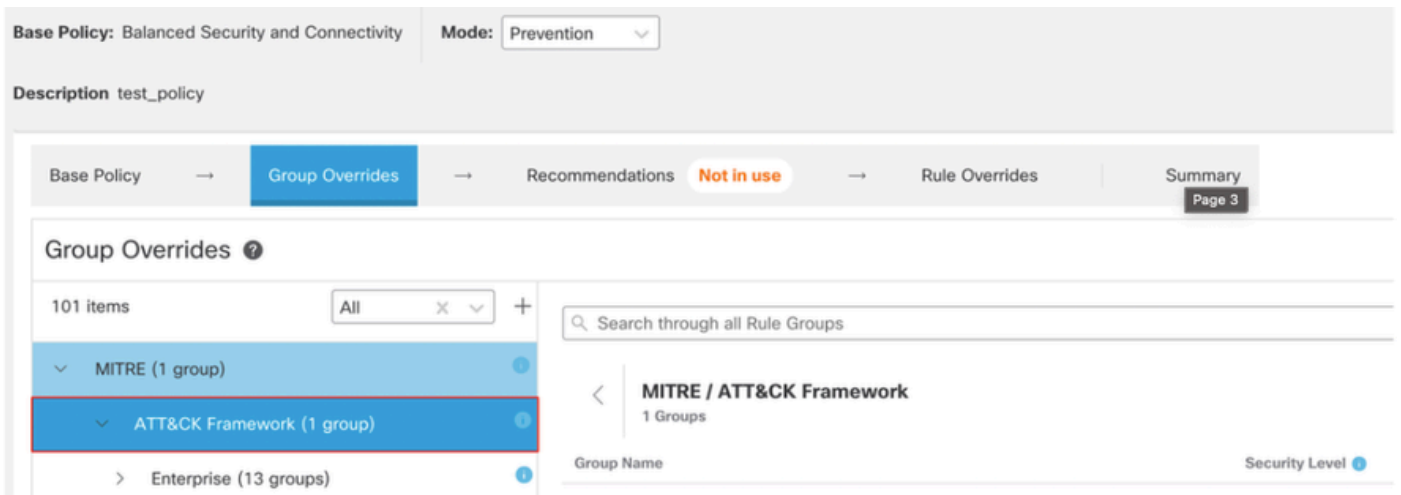
Rule Categories (9 groups) 1

Search through all Rule Groups

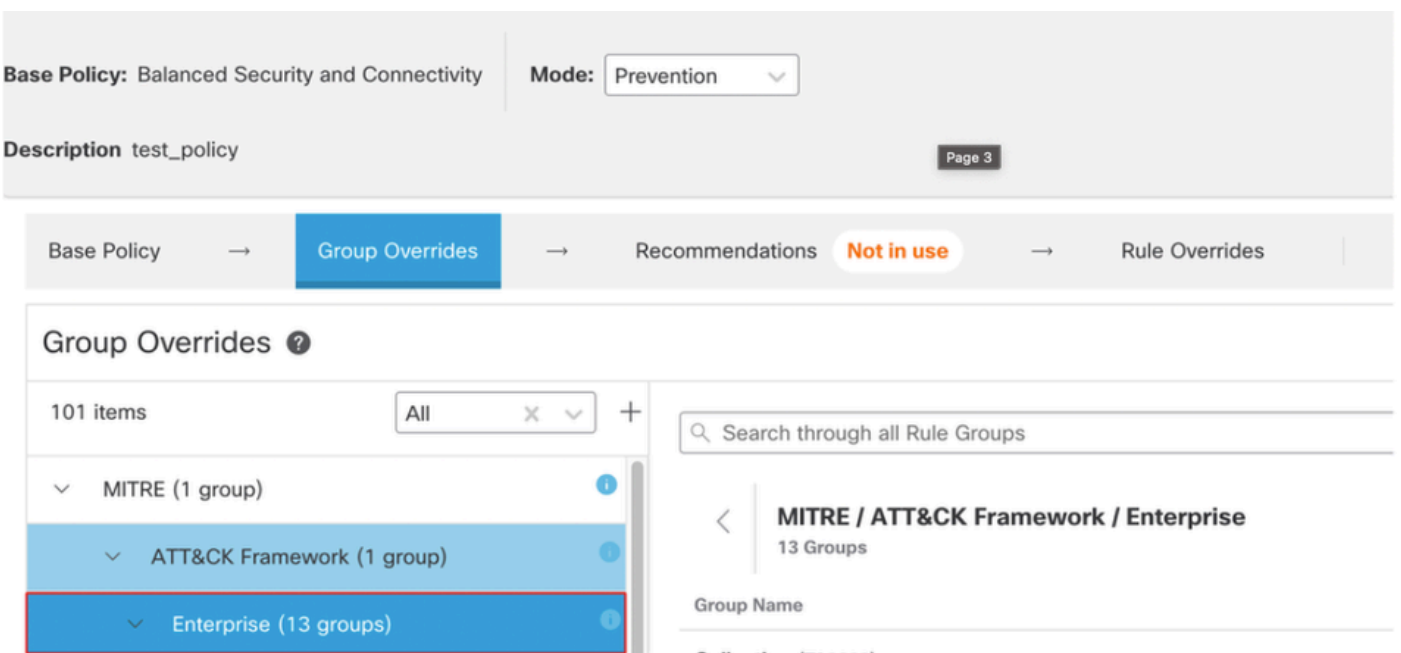
Rule Groups

To optimize intrusion policy configuration, you can configure the various rule group categories enable or disable groups and increase or decrease security levels, thus enriching intrusion eve

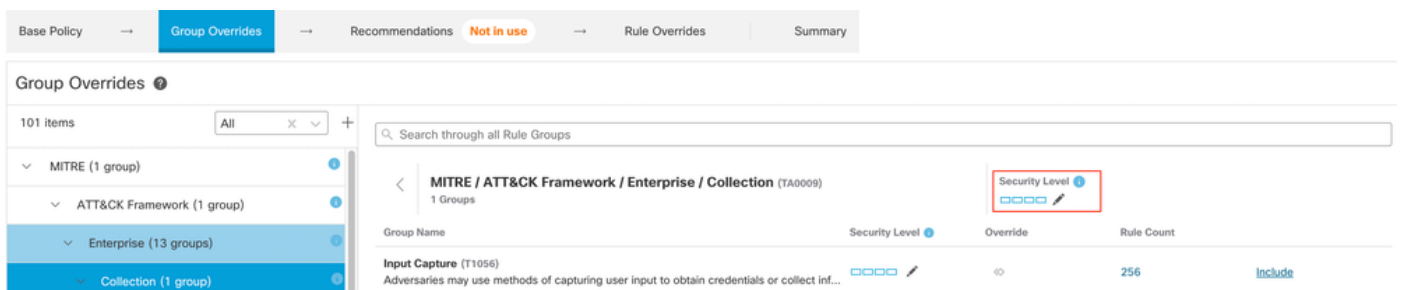
8. 「MITER」 の下の 「ATT&CK Framework」 をクリックして展開します。



9. 「ATT&CK Framework」で「Enterprise」をクリックして展開します。



10. ルールグループのセキュリティレベルの横にある編集(✎)をクリックして、エンタープライズ内の関連付けられているすべてのルールグループのセキュリティレベルを一括して変更しますルールグループカテゴリ。



セキュリティ規則グループの編集

11. 例として、Edit Security Levelウィンドウでsecurity level 3を選択して、Saveをクリックします。

# Edit Security Level



Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks.

↶ Revert to default

Cancel

Save

セキュリティレベル

12. 「Enterprise」 の下の 「Initial Access」 をクリックして展開します。

13. Initial Access の下で、最後のリーフグループである Exploit Public-Facing Application をクリックします。

The screenshot shows the 'Group Overrides' section of a security tool. The breadcrumb path is 'Base Policy' → 'Group Overrides' → 'Recommendations' (Not in use) → 'Rule Overrides' → 'Summary'. The 'Initial Access' group is expanded, showing five sub-groups: 'Drive-by Compromise', 'Exploit Public-Facing Application', 'External Remote Services', and 'Phishing'. The 'Exploit Public-Facing Application' group is selected. The main panel displays details for this group, including its name, description, security level (represented by four blue squares), and a table of rules.

Group Name	Security Level	Override	Rule Count	
<b>Drive-by Compromise</b> (T1189) Adversaries may gain access to a system through a user visiting a website over the nor...	□□□□	⊖	8783	<a href="#">Include</a>
<b>Exploit Public-Facing Application</b> (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing comput...	□□□□	⊖	11976	<a href="#">Include</a>
<b>External Remote Services</b> (T1133) Adversaries may leverage external-facing remote services to initially access and/or per...	□□□□	⊖	443	<a href="#">Include</a>
<b>Phishing</b> (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms o...	□□□□	⊖	304	<a href="#">Include</a>
<b>Valid Accounts</b> (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaini...	□□□□			

初期アクセスグループ

14. 「ルールの上書き」で「ルールの表示」をクリックしますボタンをクリックして、各ルールの各種ルール、ルールの詳細、ルールの処理などを表示します。

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

ルールの上書きのルール

15. 「推奨事項」をクリックしますレイヤを選択し、Startをクリックして、シスコが推奨するルールの使用を開始します。侵入ルールの推奨事項を使用して、ネットワークで検出されたホスト資産に関連する脆弱性を対象にすることができます。参照してください。

Base Policy → Group Overrides → **Recommendations** Not in use → Rule Overrides | Summary

Cisco Recommended Rules ⓘ

**Start using recommendations**

You can use Cisco Recommended Rules to target vulnerabilities associated with host assets detected in the network

[Start](#)

推奨事項

# Cisco Recommended Rules



Security Level (Click to select)

Accept Recommendation to Disable Rules

**Higher Efficiency** - Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

Protected Networks

Add +

Cancel

Generate

Generate and Apply

16. Summary をクリックしますポリシーに対する現在の変更の全体像を把握するためのレイヤ。ポリシーのルール配布、グループの上書き、ルールの上書きなどを表示できます。

Rule ID	Action	Alert
1:62647	Block	Alert
1:61683	Drop	Alert
1:61681	Drop	Block
1:61684	Drop	Drop

ポリシーサマリー

## 侵入イベントの表示

MITER ATT&CKテクニックおよびルールグループは、クラシックイベントビューアおよびユニファイドイベントビューアの侵入イベントで表示できます。Talosは、Snortルール(GID:SID)からMITER ATT&CKテクニックおよびルールグループへのマッピングを提供します。これらのマッピ

ングは、Lightweight Security Package(LSP)の一部としてインストールされます。

開始する前に、Snortルールによってトリガーされるイベントを検出してログに記録するために、侵入およびアクセスコントロールポリシーを導入する必要があります。

1. 「分析」 > 「侵入」 > 「イベント」の順にクリックします。

2. イベントのテーブルビューをクリックしますタブをクリックします ( 図を参照 ) 。

Events By Priority and Classification (switch workflow) || 2022-07-19 09:05:58 - 2022-07-19 09:05:58

No Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification **Table View of Events** Packets

Jump to...

	Time ×	Priority ×	Impact ×	Inline Result ×	Reason ×	Source IP ×	Source Country ×	Destination IP ×
▼	2022-07-19 11:17:10	high	2	Would block	Interface in Passive or Tap mode	192.168.0.227		146.112.255.69
▼	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.4.106
▼	2022-07-19 11:17:06	medium	3	Would block	Interface in Passive or Tap mode	54.68.177.240	USA	192.168.7.214
▼	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.7.241

イベント

3. マイターATT&CKカラムのヘッダーを調べると、侵入イベントの手法を確認できます。

Access Control Policy ×	Access Control Rule ×	Network Analysis Policy ×	MITRE ATT&CK ×	Rule Group ×
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

マイター列ヘッダー

4. クリック 1テクニックをクリックして、次の図に示すようにMITER ATT&CK Techniquesを表示します。この例では、公開アプリケーションを不正利用します手法です

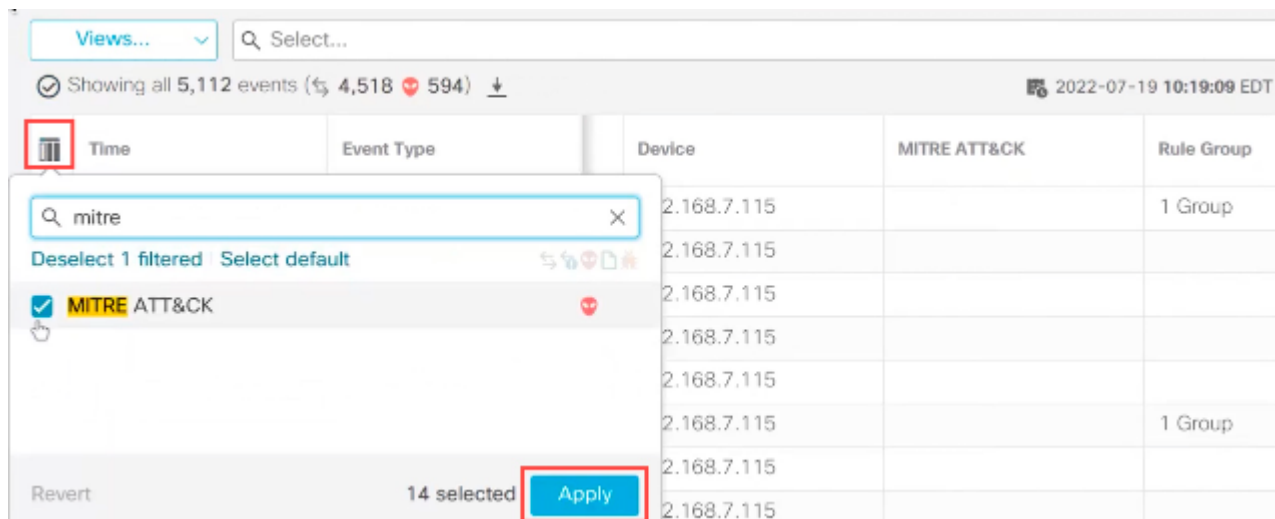
MITRE ATT&CK Techniques

- Enterprise
  - Initial Access
    - Exploit Public-Facing Application

Close

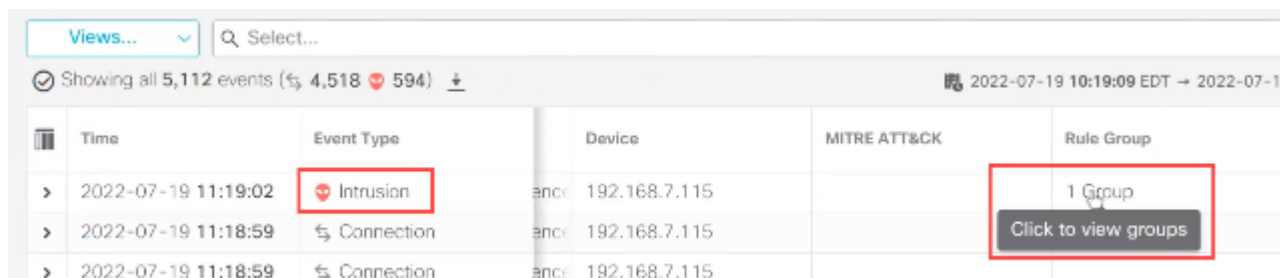
マイターATT&CKテクニック

- Close をクリックします。
- Analysis > Unified Events の順にクリックします。
- 列セレクトアイコンをクリックすると、MITRE ATT&CK and Rule Group columns を有効にできます。



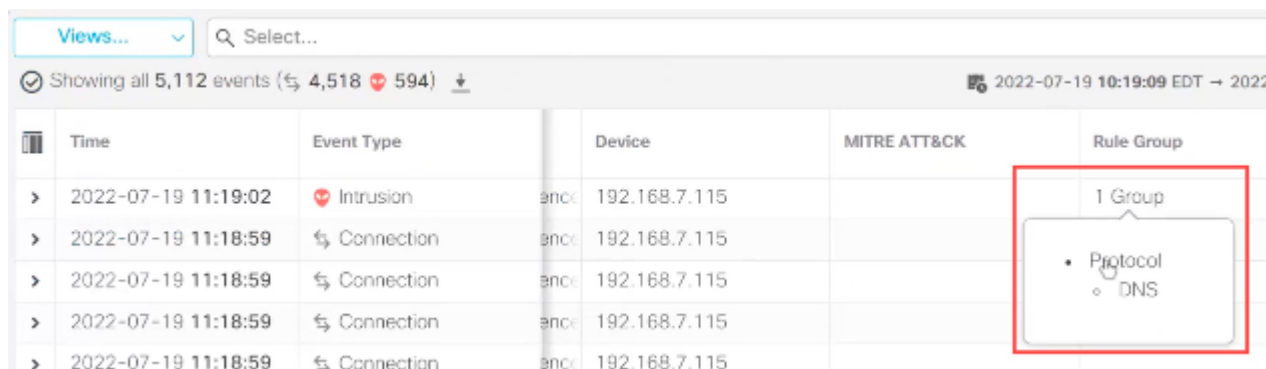
マイター攻撃を有効にする

- 次の例に示すように、侵入イベントは、1つのルールグループにマッピングされたイベントによってトリガーされました。Rule Groupの下にある1 Groupをクリックします。カラム。



[ルール]領域

- 例として、親ルールグループであるProtocolとその下のDNSルールグループを表示できます。



プロトコルの表示

- Protocol をクリックすると、少なくとも1つのルールグループ (Protocol > DNS) を持つすべての侵入イベントを検索できます。次の例に示すように、検索結果が表示されます。

Views... Rule Group Protocol Select...

Showing all 501 events (501) 2022-07-19 10:19:09 EDT → 2022-07-19 11:19:09 EDT 1h

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Snort ID
2022-07-19 11:19:08	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	snort: 192.168.7.115		Protocol • DNS	1:254:16
2022-07-19 11:19:03	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:02	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	snort: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	snort: 192.168.7.115		1 Group	1:254:16

ルールグループプロトコル

## 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。