

# ASA バージョン 9.2 の VPN SGT の分類と適用の設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ISE の設定](#)

[ASA の設定](#)

[確認](#)

[トラブルシューティング](#)

[要約](#)

[関連情報](#)

## 概要

このドキュメントでは、VPN ユーザ向けに適応型セキュリティ アプライアンス ( ASA ) リリース 9.2.1 の TrustSec セキュリティ グループ タグ ( SGT ) 分類の新機能を使用する方法について説明します。次の例では、それぞれ異なる SGT とセキュリティ グループ ファイアウォール ( SGFW ) が割り当てられた 2 つの VPN ユーザを示します。これらの VPN ユーザ間のトラフィックはフィルタリングされます。

## 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。

- ASA CLI 設定およびセキュア ソケット レイヤ ( SSL ) VPN 設定に関する基本的な知識
- ASA でのリモート アクセス VPN 設定に関する基本的な知識
- Identity Services Engine ( ISE ) および TrustSec サービスに関する基本的な知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

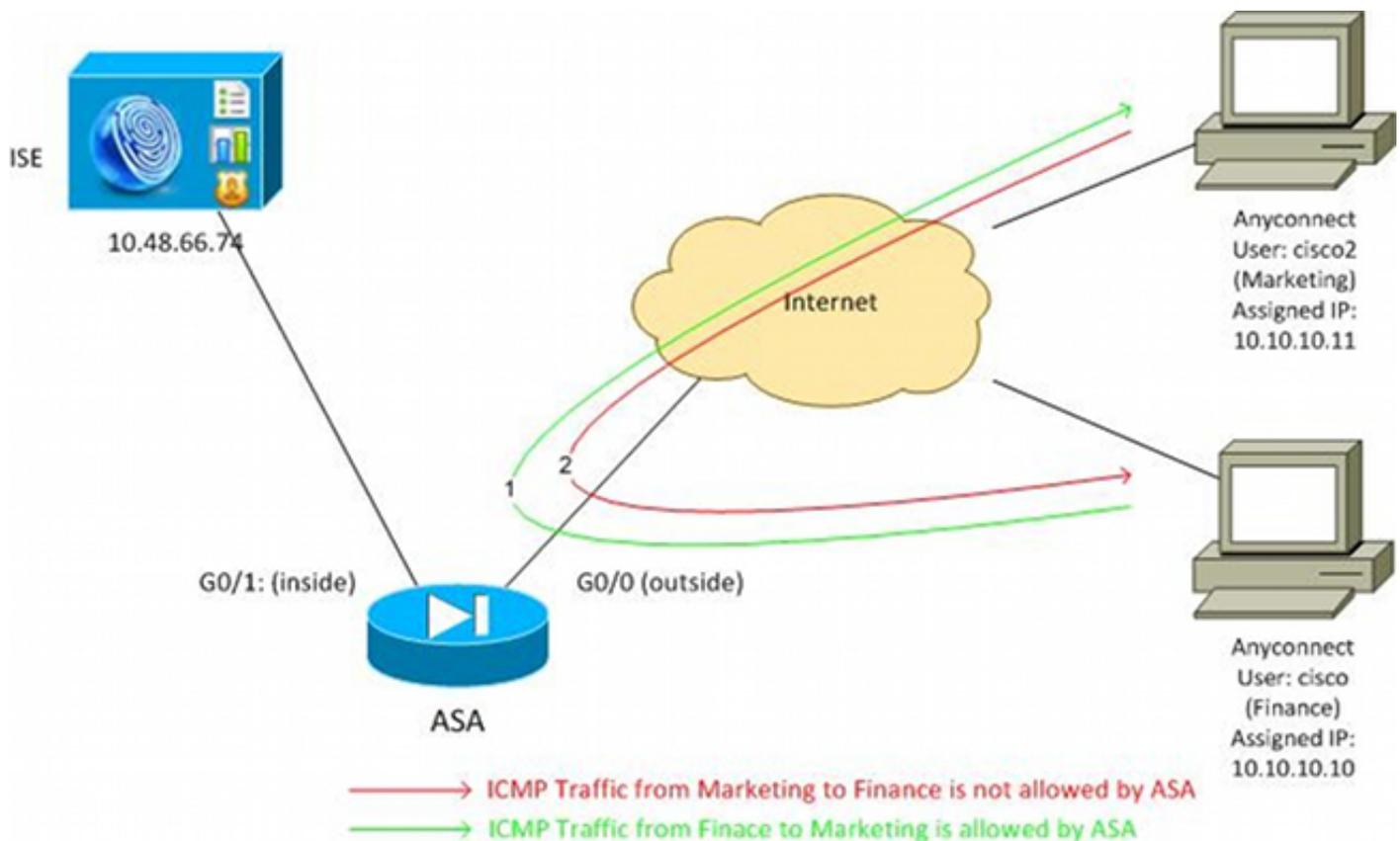
- Cisco ASA ソフトウェア バージョン 9.2 以降
- Cisco AnyConnect Secure Mobility Client リリース 3.1 がインストールされた Windows 7
- Cisco ISE リリース 1.2 以降

## 設定

注：このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#)(登録ユーザ専用)を使用してください。

## ネットワーク図

VPN ユーザ「cisco」は財務 ( Finance ) チームに割り当てられているため、マーケティング ( Marketing ) チームへのインターネット制御メッセージプロトコル ( ICMP ) 接続を開始できません。VPN ユーザ「cisco2」はマーケティング チームに割り当てられているため、接続を開始することができます。



## ISE の設定

1. [Administration] > [Identity Management] > [Identities] を選択して、ユーザ「cisco」 ( Finance から取得 ) および「cisco2」 ( Marketing から取得 ) を追加し、設定します。
2. [Administration] > [Network Resources] > [Network Devices] を選択して、ASA をネットワークデバイスとして追加し、設定します。
3. [Policy] > [Results] > [Authorization] > [Authorization Profiles] を選択して、Finance および Marketing 認証プロファイルを追加し、設定します。両方のプロファイルに、すべてのトラ

フィックを許可するダウンロード可能アクセスコントロールリスト ( DACL ) という 1 つの属性のみが含まれています。次に Finance の例を示します。

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is selected. On the left, a tree view shows the navigation structure, with 'Authorization Profiles' highlighted. The main content area displays the configuration for the 'Finance\_Profile' authorization profile. The 'Name' field is set to 'Finance\_Profile', and the 'Access Type' is set to 'ACCESS\_ACCEPT'. The 'Service Template' checkbox is unchecked. Under the 'Common Tasks' section, the 'DACL Name' dropdown menu is set to 'PERMIT\_ALL\_TRAFFIC'.

各プロファイルには特定の制限付き DACL が含まれている可能性があります。このシナリオではすべてのトラフィックが許可されます。強制実行するのは、各 VPN セッションに割り当てられた DACL ではなく、SGFW です。SGFW によってフィルタリングされるトラフィックは、DACL で使用される IP アドレスではなく SGT を使用できます。

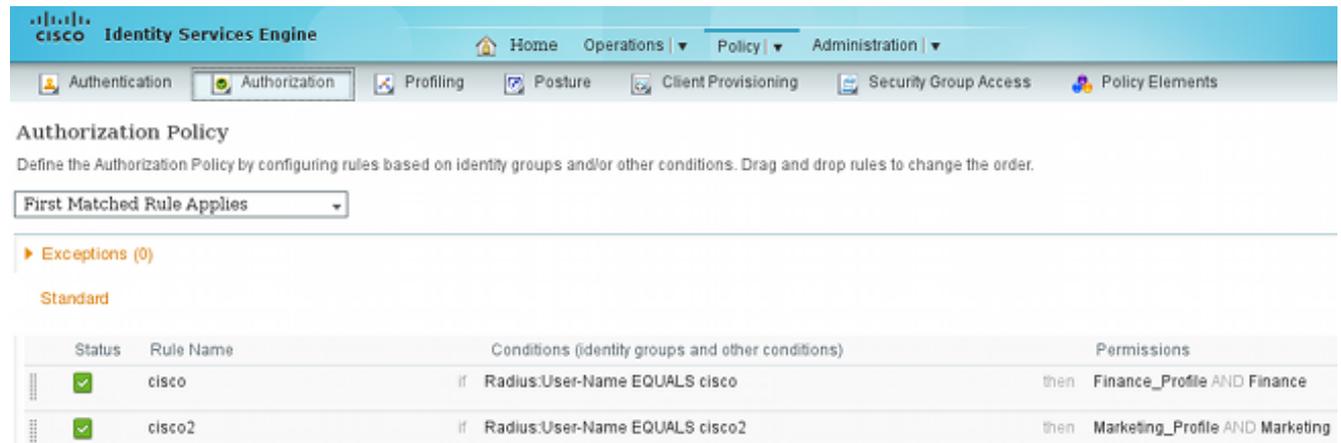
4. [Policy] > [Results] > [Security Group Access] > [Security Groups] を選択して、Finance および Marketing の SGT グループを追加し、設定します。

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Results' tab is selected. On the left, a tree view shows the navigation structure, with 'Security Groups' highlighted. The main content area displays the 'Security Groups' configuration page. At the top, there are buttons for 'Edit', 'Add', 'Import', and 'Export'. Below this is a table with the following data:

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	Finance	2 / 0002
<input type="checkbox"/>	Marketing	3 / 0003
<input type="checkbox"/>	Unknown	0 / 0000

5. [Policy] > [Authorization] を選択して、2 つの許可ルールを設定します。最初のルールは、

Finance\_profile ( トラフィック全体を許可する DACL ) を SGT グループ Finance とともに「cisco」ユーザに割り当てます。 2 番目のルールは、Marketing\_profile ( トラフィック全体を許可する DACL ) を SGT グループ Marketing とともに「cisco2」ユーザに割り当てます。



The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The page title is "Authorization Policy" and it includes a description: "Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order." A dropdown menu is set to "First Matched Rule Applies". Below this, there is a section for "Exceptions (0)" and a "Standard" section containing a table of rules.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	cisco	if Radius:User-Name EQUALS cisco	then Finance_Profile AND Finance
✓	cisco2	if Radius:User-Name EQUALS cisco2	then Marketing_Profile AND Marketing

## ASA の設定

### 1. 基本的な VPN 設定を完了します。

```
webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
accounting-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable

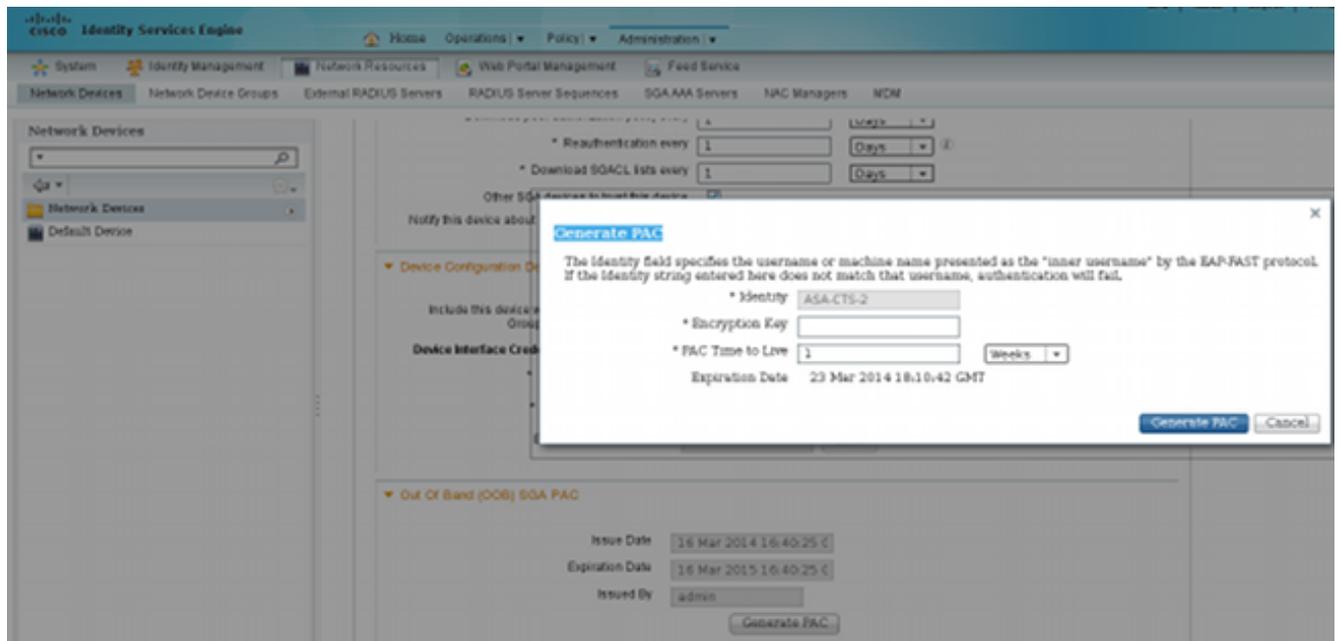
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

### 2. ASA AAA および TrustSec の設定を完了します。

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
key *****
cts server-group ISE
```

TrustSec クラウドに参加するためには、ASA が Protected Access Credential ( PAC ) で認証する必要があります。ASA は自動 PAC プロビジョニングをサポートしていないため、そのファイルを ISE で手動で生成し、ASA にインポートする必要があります。

### 3. [Administration] > [Network Resources] > [Network Devices] > [ASA] > [Advanced TrustSec Settings] を選択して、ISE で PAC を生成します。[Out of Band (OOB) PAC] プロビジョニングを選択して、ファイルを生成します。



4. PAC を ASA にインポートします。生成されたファイルは HTTP/FTP サーバに配置できます。ASA はこれを使用して、ファイルをインポートします。

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
!PAC Imported Successfully
ASA#
ASA# show cts pac
```

PAC-Info:

```
Valid until: Mar 16 2015 17:40:25
AID:          ea48096688d96ef7b94c679a17bdad6f
I-ID:         ASA-CTS-2
A-ID-Info:    Identity Services Engine
PAC-type:     Cisco Trustsec
```

PAC-Opaque:

```
000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
11d8378829cc007b91ced9117a
```

適切な PAC がある場合は、ASA が自動的に環境の更新を実行します。これにより、現在の SGT グループに関する情報が ISE からダウンロードされます。

```
ASA# show cts environment-data sg-table
```

Security Group Table:

```
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries
```

SG Name	SG Tag	Type
ANY	65535	unicast
Unknown	0	unicast
<b>Finance</b>	<b>2</b>	unicast
<b>Marketing</b>	<b>3</b>	unicast

5. SGFW を設定します。最後のステップでは、Finance から Marketing までの ICMP トラフィックを可能にする外部インターフェイスで ACL を設定します。

```
access-list outside extended permit icmp security-group tag 2 any security-group tag 3 any
```

```
access-group outside in interface outside
```

さらに、タグではなくセキュリティグループ名を使用できます。

```
access-list outside extended permit icmp security-group name Finance any
```

```
security-group name Marketing any
```

インターフェイス ACL による VPN トラフィックの処理を確実にを行うために、インターフェイス ACL を介した検証のない VPN トラフィックをデフォルトで許可するオプションを無効にする必要があります。

```
no sysopt connection permit-vpn
```

これで、ASA は VPN ユーザを分類し、SGT に基づいて強制実行する準備ができました。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

「[アウトプットインタープリタツール \(登録済み お客様のみ\)](#)が特定の **show** コマンドを発行します。アウトプットインタープリタツール (登録ユーザ専用) を使用して、**show** コマンド出力。

VPN が確立されると、ASA は各セッションに適用される SGT を示します。

```
ASA(config)# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username      : cisco                Index      : 1
Assigned IP   : 10.10.10.10          Public IP   : 192.168.10.68
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 35934                Bytes Rx    : 79714
Group Policy  : GP-SSL                Tunnel Group : RA
Login Time    : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN        : none
Audt Sess ID  : c0a8700a000010005325d60b
Security Grp : 2:Finance
```

```
Username      : cisco2               Index      : 2
Assigned IP   : 10.10.10.11          Public IP   : 192.168.10.80
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 86171                Bytes Rx    : 122480
Group Policy  : GP-SSL                Tunnel Group : RA
Login Time    : 17:52:27 CET Sun Mar 16 2014
Duration     : 0h:19m:45s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN        : none
Audt Sess ID  : c0a8700a000020005325d6cb
Security Grp : 3:Marketing
```

SGFW は Finance ( SGT=2 ) から Marketing ( SGT=3 ) までの ICMP トラフィックを許可します。そのためユーザ「cisco」はユーザ「cisco2」を ping できます。

```
C:\Users\admin>ping 10.10.10.11 -S 10.10.10.10

Pinging 10.10.10.11 from 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=3ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Reply from 10.10.10.11: bytes=32 time=6ms TTL=128
Reply from 10.10.10.11: bytes=32 time=5ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

カウンタは次のように増加します。

```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
tag 2(name="Finance") any security-group tag 3(name="Marketing")
any (hitcnt=4) 0x071f07fc
```

接続が作成されました。

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco)
```

ICMP インспекションが有効であるため、リターントラフィックが自動的に受け入れられます。

Marketing (SGT=3) から Finance (SGT=2) までを ping しようとする、次のようになります。

```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ASA は次のように報告します。

```
Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2,
3:Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by
access-group "outside" [0x0, 0x0]
```

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次のドキュメントを参照してください。

- [Catalyst 3750X シリーズ スイッチでの TrustSec Cloud と 802.1x MACsec の設定例](#)
- [ASA と Catalyst 3750X シリーズ スイッチ TrustSec の設定例とトラブルシューティング ガイド](#)

## 要約

この記事では、VPN ユーザを分類して基本的な強制実行を行う方法を簡単な例を説明します。さらに SGFW は、VPN ユーザとネットワーク内のその他の部分との間のトラフィックをフィルタリングします。SXP ( TrustSec SGT Exchange Protocol ) は、IP と SGT 間のマッピング情報を取得するために ASA で使用できます。これにより ASA は、正しく分類されたすべてのセッションタイプ ( VPN または LAN ) について強制実行できます。

バージョン 9.2 以降の ASA ソフトウェアでは、ASA は RADIUS Change of Authorization ( CoA ) もサポートします ( RFC 5176 )。正常な VPN ポスチャの後で ISE から送信される RADIUS CoA パケットには、SGT とともに cisco-av-pair が含まれることがあります。SGT は準拠ユーザを別の ( よりセキュアな ) グループに割り当てます。詳細な例については、「[関連情報](#)」セクションの記事を参照してください。

## 関連情報

- [ISE との ASA バージョン 9.2.1 VPN ポスチャの設定例](#)
- [ASA と Catalyst 3750X シリーズ スイッチ TrustSec の設定例とトラブルシューティング ガイド](#)
- [Cisco TrustSecスイッチ設定ガイド : Cisco TrustSecについて](#)
- [セキュリティ アプライアンスのユーザ認証に外部サーバを設定](#)
- [Cisco ASA シリーズ VPN CLI 構成ガイド 9.1](#)
- [『Cisco Identity Services Engine User Guide, Release 1.2 \( Cisco Identity Services Engine ユーザガイドリリース 1.2 \) 』](#)
- [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。