ファイアウォールと NAT に対する Sun RPC ALG サポート

ファイアウォールおよび NAT 対応の Sun RPC ALG のサポート機能により、ファイアウォールおよびネットワーク アドレス変換（NAT）における Sun Microsystems（Sun）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートが追加されます。Sun RPC は、リモート サーバ プログラム内の関数をクライアント プログラムが呼び出すことができるようにするアプリケーション層プロトコルです。このモジュールでは、Sun RPC ALG を設定する方法について説明します。

ファイアウォールおよび NAT の Sun RPC ALG サポートに関する制約事項

- レイヤ 4 またはレイヤ 7 クラス マップのインスペクション アクションを設定した場合、ポート マッパー プロトコルのウェルノウン ポート（111）に一致するパケットはレイヤ 7 のインスペクションなしでファイアウォールを通過します。レイヤ 7 のインスペクションがない場合、ファイアウォール ピンホールはトラフィック フロー用に開放されず、Sun リモート プロシージャ コール（RPC）がファイアウォールによってブロックされます。回避策として、Sun RPC プログラム番号に対応する **match program-number** コマンドを設定します。
- ポート マッパー プロトコル バージョン 2 のみがサポートされます。他のバージョンはサポートされません。
- RPC バージョン 2 のみサポートされます。

ファイアウォールおよび NAT の Sun RPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。ALG は、アプリケーション レイヤ プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを NAT が実行します。IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

Sun RPC

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）は、Sun RPC プロトコルのディープ パケット インスペクションを実行します。Sun RPC ALG は、管理者が一致フィルタを設定できるプロビジョニング システムと連動します。一致フィルタはそれぞれ、Sun RPC パケット内で検索される一致基準を定義し、それにより、基準に一致するパケットのみ許可されます。

RPC では、クライアント プログラムは、サーバ プログラム内のプロシージャを呼び出します。RPC ライブラリは、プロシージャ引数をネットワーク メッセージ内にパッケージ化し、そのメッセージをサーバに送信します。次にサーバは、RPC ライブラリを使用して、ネットワーク メッセージからプロシージャ引数を取り出し、指定されたサーバ プロシージャを呼び出します。サーバ プロシージャが RPC に戻ると、戻り値がネットワーク メッセージ内にパッケージ化され、クライアントに送り返されます。

Sun RPC プロトコルの詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

ファイアウォール向けの Sun RPC ALG のサポート

ポリシーおよびクラス マップを使用して作成されるゾーンベース ファイアウォールを使用して Sun RPC ALG を設定できます。レイヤ 7 クラス マップを使用することで、ネットワーク管理者は一致フィルタを設定できます。フィルタはSunRPCパケット内で検索されるプログラム番号を指定します。Sun RPC レイヤ 7 ポリシーマップは、**service-policy** コマンドを使用するレイヤ 4 ポリシーマップの子ポリシーとして設定します。

レイヤ 7 ファイアウォール ポリシーを設定しないで Sun RPC レイヤ 4 クラス マップを設定すると、Sun RPC トラフィックにより戻されるトラフィックはファイアウォールを通過しますが、セッションはレイヤ 7 で検査されません。セッションが検査されないため、後続の RPC コールはファイアウォールによってブロックされます。Sun RPC レイヤ 4 クラス マップおよびレイヤ 7 ポリシーを設定すると、レイヤ 7 インスペクションが使用できるようになります。空のレイヤ7ファイアウォールポリシー、つまり、一致フィルタが設定されていないポリシーを設定できます。

NAT 向けの Sun RPC ALG のサポート

デフォルトでは、ネットワーク アドレス変換（NAT）が有効な場合、Sun RPC ALG は自動的に有効になります。NAT で Sun RPC ALG を無効にするには、**no ip nat service alg** コマンドを使用します。

ファイアウォールおよび NAT の Sun RPC ALG サポートの設定方法

ファイアウォールおよびNAT が有効にされている場合に Sun RPC を動作させるには、ALG で Sun RPC パケットを検査する必要があります。また ALG では、ダイナミック ファイアウォール セッションの確立や NAT 変換後のパケット コンテンツの修正など、Sun RPC 固有の問題も処理します。

Sun RPC ALG 用のファイアウォールの設定

Sun RPC プロトコルの検査アクションを設定している場合（つまり、レイヤ 4 クラスマップで **match protocol sunrpc** コマンドを指定している場合）は、レイヤ 7 Sun リモートプロシージャコール（RPC）ポリシーマップを設定する必要があります。

セキュリティ ゾーンと検査ルールの両方を同じインターフェイス上で設定しないことを推奨します。これは、このような設定は機能しない場合があるためです。

Sun RPC ALG 対応のファイアウォールを設定するには、次の作業を実行します。

ファイアウォール ポリシー用のレイヤ 4 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 4 クラス マップを設定するには、この作業を実行します。**class-map type inspect** コマンドで **match-all** キーワードを指定すると、クラスマップ内の（プログラム番号として指定された）すべてのSunリモートプロシージャコール

（RPC）レイヤ 7 フィルタに Sun RPC トラフィックがマッチします。**class-map type inspect** で **match-any** キーワードを指定すると、クラスマップ内の（プログラム番号として指定された）少なくとも 1 つの Sun RPC レイヤ 7 フィルタに Sun RPC トラフィックがマッチする必要があります。

レイヤ 4 クラスマップを設定するには、**class-map type inspect {match-any | match-all}** *classm-map-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any sunrpc-l4-cmap`	レイヤ 4 検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sunrpc`	指定されたプロトコルに基づき、クラスマップの一致基準を設定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール ポリシー用のレイヤ 7 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 7 クラス マップを設定するには、この作業を実行します。この設定により、Sun RPC を使用する mount（100005）、ネットワーク ファイル システム（NFS）（100003）などのプログラムが使用可能になります。100005 および

100003 は Sun RPC プログラムの番号です。デフォルトでは、Sun RPC ALG はすべてのプログラムをブロックします。

Sun RPC プログラムおよびプログラム番号の詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

レイヤ 7 クラスマップを設定するには、**class-map type inspect** *protocol-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match program-number** *program-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	レイヤ 7（アプリケーション固有）検査タイプ クラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match program-number** *program-number* 例： `Device(config-cmap)# match program-number 100005`	許可する RPC プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Sun RPC ファイアウォール ポリシー マップの設定

Sun リモート プロシージャ コール（RPC）ファイアウォール ポリシーマップを設定するには、この作業を実行します。ポリシー マップを使用して、レイヤ 7 ファイアウォール ポリシーのクラス マップで定義する Sun RPC レイヤ 7 クラスごとにパケット転送を許可します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *protocol-name policy-map-name*
4. **class type inspect** *protocol-name class-map-name*
5. **allow**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	レイヤ 7（プロトコル固有）検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *protocol-name class-map-name* 例： `Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	アクションの実行対象となるトラフィック クラスを指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**allow** 例： `Device(config-pmap-c)# allow`	パケット転送を許可します。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 7 ポリシー マップをレイヤ 4 ポリシー マップにアタッチする

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class** {*class-map-name* | **class-default**}
5. **inspect** [*parameter-map-name*]
6. **service-policy** *protocol-name policy-map-name*
7. **exit**
8. **class class-default**
9. **drop**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc-l4-pmap`	レイヤ 4 検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class** {*class-map-name*	**class-default**} 例： `Device(config-pmap)# class sunrpc-l4-cmap`	アクションを実行する対象（クラス）を関連付け、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**service-policy** *protocol-name policy-map-name* 例： `Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	レイヤ 7 ポリシー マップをトップレベルのレイヤ 4 ポリシー マップにアタッチします。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、QoS ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 8	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定する前にデフォルト クラス（一般的にクラスデフォルト クラスと呼ばれます）を指定し、QoS ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 10	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。ただし、1 つのセキュリティ ゾーンのみ作成でき、もう 1 つのセキュリティ ゾーンはシステム定義のセキュリティ ゾーンにすることができます。システム定義のセキュリティゾーンまたはセルフゾーンを作成するには、**self** キーワードを指定した **zone-pair security** コマンドを設定します。

（注） セルフ ゾーンを選択する場合、検査アクションは設定できません。

このタスクの内容は以下のとおりです。

- セキュリティ ゾーンを作成します。
- ゾーン ペアを定義します。
- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}

6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
12. **zone-member security** *zone-name*
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
16. **zone-member security** *zone-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-client`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。 • ゾーン ペアでは、デフォルト ゾーンまたはセルフ ゾーンを送信元ゾーンまたは宛先ゾーンとして使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-server`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定では送信元ゾーンと宛先ゾーンという、ゾーン ペアを作成するための 2 つのセキュリティ ゾーンが必要です。

	コマンドまたはアクション	目的
		• ゾーン ペアでは、デフォルト ゾーンを送信元ゾーンまたは宛先ゾーンとして使用できます。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* 例： `Device(config)# zone-pair security clt2srv source z-client destination z-server`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 12	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-client`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 15	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-server`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールと NAT に対する Sun RPC ALG サポートの設定例

例：ファイアウォール ポリシー用のレイヤ 4 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any sunrpc-l4-cmap
Device(config-cmap)# match protocol sunrpc
Device(config-cmap)# end
```

例：ファイアウォール ポリシー用のレイヤ 7 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap
Device(config-cmap)# match program-number 100005
Device(config-cmap)# end
```

例：Sun RPC ファイアウォール ポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap
Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap
Device(config-pmap-c)# allow
Device(config-pmap-c)# end
```

例：レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップのアタッチ

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpcl4-pmap
Device(config-pmap)# class sunrpcl4-cmap
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：セキュリティ ゾーンとゾーン ペアの作成とゾーン ペアへのポリシー マップのアタッチ

```
Device# configure terminal
Device(config)# zone security z-client
Device(config-sec-zone)# exit
Device(config)# zone security z-server
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv source z-client destination z-server
Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# ip address 192.168.6.5 255.255.255.0
Device(config-if)# zone-member security z-client
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/1/1
Device(config-if)# ip address 192.168.6.1 255.255.255.0
Device(config-if)# zone-member security z-server
Device(config-if)# end
```

例：Sun RPC ALG 用のファイアウォールの設定

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）サポート用のファイアウォール設定の例を以下に示します。

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
 match program-number 100005
!
class-map type inspect match-any sunrpc-l4-cmap
 match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
 class type inspect sunrpc sunrpc-l7-cmap
  allow
!
!
policy-map type inspect sunrpc-l4-pmap
 class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
```

```
!
 class class-default
  drop
!
!
zone security z-client
!
zone security z-server
!
zone-pair security clt2srv source z-client destination z-server
 service-policy type inspect sunrpc-l4-pmap
!
interface GigabitEthernet 2/0/0
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
interface GigabitEthernet 2/1/1
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
!
```

ファイアウォールと NAT に対する Sun RPC ALG サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
IP アドレッシング コマンド	『IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 1057	『*RPC: Remote Procedure Call Protocol Specification Version 2*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールと NAT に対する Sun RPC ALG サポートに関する機能情報

表 *1*: ファイアウォールと *NAT* に対する *Sun RPC ALG* サポートに関する機能情報

機能名	リリース	機能情報
ファイアウォールと NAT に対する Sun RPC ALG サポート	Cisco IOS XE リリース 3.2S	ファイアウォールと NAT に対する Sun RPC ALG サポート機能は、ファイアウォールと NAT に Sun RPC ALG のサポートを追加します。 次のコマンドが導入または変更されました。**match protocol**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。