

ルールベースのコンプライアンスポリシーの設定

- ルールベースのコンプライアンスポリシー （1 ページ）
- ルールベースのコンプライアンスポリシーの作成 （2 ページ）
- Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートして Catalyst Center にインポートする （14 ページ）
- Catalyst Centerからルールベースのコンプライアンスポリシーをエクスポートし、別の Catalyst Center にインポートします。 （15 ページ）

ルールベースのコンプライアンスポリシー

ルールベースのコンプライアンスでは、Catalyst Center がネットワーク全体で定期的に評価して違反を検出するカスタム設定ルールおよびポリシーを作成できます。プラットフォーム固有のコンプライアンス ポリシー ルールでは、文字列の比較、正規表現、式の評価を使用することが可能です。これらは、設定、CLI show コマンド、デバイスプロパティに適用されます。各ルールには、変数、複数の条件、設定可能な違反メッセージとともに違反のシビラティレベルを含めることができます。

たとえば、次のようなポリシーを設定できます。

- ACL ロギングがオフであることを確認する。
- ネットワークで Telnet が無効になっていることを確認する。
- ログイン認証で外部 AAA サーバーが使用されていることを確認する。
- RADIUS サーバーの最小数を設定する。
- DHCP リース時間を特定の日数で設定する。
- コンソール接続が許可されていることを確認する。
- 失敗したログイン試行のトラッキングを有効にする。
- パスワードポリシーを確認する。

スケールの考慮事項

ルールベースのコンプライアンスでは、ポリシー、ルール、条件を柔軟に定義できる必要があります。ただし、過負荷を防ぐための制限も必要です。

これらの制限は、システムレベルとデバイスごとのレベルの両方で推奨されます。

カテゴリ（**Category**）	システム制限	個別の制限
ポリシー	500	
ルール	5000	1 ポリシー：最大 20 個のルール
変数	12,500（ルールの 50% で変数を使用（ルールあたり平均 5 個））	1 ルール：最大 10 個の変数
条件	25,000（ルールあたり平均 5 個）	1 ルール：最大 10 個の条件

ルールベースのコンプライアンスポリシーの作成

ルールベースのコンプライアンスポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。、**[ポリシー（Policy）]**>**[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [Create Policy] をクリックします。

1. [コンプライアンスポリシーの作成（Create compliance policy）] スライドインペインで、[ポリシー名（Policy Name）] フィールドにポリシー名を入力します。
2. [説明（Description）] フィールドに任意の説明を入力します。
3. [Save] をクリックします。

ルールベースのコンプライアンス ポリシー ルールの作成

ルールベースのコンプライアンスポリシーの新しいルールを作成するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 （任意）[ルール（Rule）] ペインで、[ルールの追加（Add rule）] をクリックして新しいルールを追加し、次の設定を完了します。

a) [ルール名（Rule Name）] フィールドに、ルールの名前を入力します。

b) [説明（Description）] フィールドに、ルールの説明を入力します。

c) （オプション）[影響と推奨される修正の追加（Add impact and suggested fix）] を展開し、次の値を設定します。

- [影響（Impact）] - ルールが生成する違反の影響に関する簡単なメモを入力します。
- [推奨される修正（Suggested fix）] - ルールが生成する違反の推奨される修正に関するメモを入力します。

（注） ルールは、選択した条件に一致するデバイスでのみ実行されます。デバイスファミリまたはデバイスシリーズのみを選択した場合、ルールはデバイスファミリまたはデバイスシリーズのすべてのデバイスに適用されます。

ステップ 4 [ソフトウェアタイプ（Software type）] ドロップダウンリストから、ソフトウェアタイプを [IOX]、[IOS-XE]、または [シスココントローラ（Cisco Controllers）] として選択します。

ステップ 5 [デバイスファミリ（Device family）] ドロップダウンリストから、デバイスファミリを [ルータ（Routers）]、[スイッチとハブ（Switches and Hubs）]、または [ワイヤレスコントローラ（Wireless Controllers）] として選択します。

ステップ 6 [デバイスシリーズ（Device series）] または [デバイスモデル（Device models）] のいずれかのトグルボタンをクリックします。

ステップ 7 ルールを適用するデバイスシリーズまたはデバイスモデルのチェックボックスをオンにします。

ステップ 8 [保存（Save）] をクリックしてルールを作成します。

コンプライアンス ポリシー ルールへの条件の追加

ルールベースのコンプライアンス ポリシー ルールに条件を追加するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [ルール（Rules）] ペインで、ルールの名前をクリックします。

ステップ 4 [条件（Conditions）] ペインを展開します。[条件を追加（Add Condition）] をクリックします。

ステップ 5 [条件の追加（Add Conditions）] ペインで、ルールに条件を追加します。

a) 基本設定を構成するのか、詳細設定を構成するのかに基づいて条件を設定します。

b) 基本設定を構成する場合は、[条件（Conditions）] ペインを展開します。

c) [範囲（Scope）] ドロップダウンリストから、条件の範囲を選択し、基本設定の次の設定を完了します。

表 *1*: 基本設定

選択内容	結果
設定	[演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [Value] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

選択内容	結果
デバイスのコマンド出力	[Showコマンド（Show command）] フィールドで、show コマンドを選択するか、カスタム show コマンドを入力してリストに追加します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [Value] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

[アクション（Actions）] ペインを展開し、基本設定の次の設定を完了します。

選択内容	結果
続行	違反を発生させずに続行します。
違反を発生して続行	条件の範囲に基づいて違反のシビラティを設定します。 • [違反のシビラティ（Violation severity）] ドロップダウンリストから、違反のシビラティを選択します。 • [カスタム違反メッセージ（Custom violation message）] フィールドに、任意のユーザー定義違反メッセージを入力します。

d) 詳細条件を設定する場合は、[条件の追加（Add condition）] ペインで [詳細設定（Advance settings）] を有効にし、設定を解析してアクションを実行するための追加オプションにアクセスします。
e) [条件（Conditions）] ペインを展開します。[範囲（Scope）] ドロップダウンリストから、条件の範囲を選択し、詳細設定の次の設定を完了します。

表 *2:* 詳細設定

選択内容	結果
設定	

選択内容	結果
	[ブロックとして解析（Parse as Blocks）] チェックボックスをオンにして、実行コンフィギュレーション全体をブロックに分割し、各ブロック内の条件一致基準値を検索します。 [ブロック開始式（Block start expression）] と [ブロック終了式（Block end expression）] を入力します。ブロックは、開始表現と終了表現に基づいて分割されます。 （オプション）[詳細ブロックオプション（Advance block options）] をクリックして、違反オプションを選択します。 • [いずれかのブロックに違反がある場合に違反が発生（Raise violation if ANY block has a violation）] : 1 つまたは複数の違反が発生する可能性があります。 • [複数の違反（違反ブロックごとに1つの違反）が発生（Raise multiple violations - one violation per violating block）] : すべてのブロックに対して実行が継続され、多くの違反が発生します。 • [すべての違反ブロックに対して1つの違反が発生（Raise a single violation for all violating blocks）] : 違反のあるブロックが検出されると、実行が停止します。 • [すべてのブロックに違反がある場合にのみ違反が発生（Raise violation only if ALL blocks have a violation）] : ルールに対して 1 つの違反のみ発生します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [値（Value）] フィールドに値を入力します。

選択内容	結果
	[正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。
デバイスのコマンド出力	[Showコマンド（Show command）] フィールドで、show コマンドを選択するか、カスタム show コマンドを入力してリストに追加します。 [演算子（Operator）] ドロップダウンリストから、選択した範囲に必要な演算子を選択します。 • 文字列を含む • 文字列を含まない • 表現に一致 • 表現に一致しない • 式の評価 [値（Value）] フィールドに値を入力します。 [正規表現のテスト（Test regular expression）] をクリックし、正規表現演算子のテストデータを使用して入力した正規表現の値をテストします。

[アクション（Actions）] ペインを展開し、次の設定を完了します。

選択内容	結果
[続行（Continue）] としてアクションを照合	違反を発生させずに、次の条件のチェックに進みます（存在する場合）。
不一致時のアクションとして [違反を発生させて続行（Raise a violation and continue）] を選択	違反と違反メッセージのシビラティを設定することによって違反を引き起こします。 • [違反のシビラティ（Violation severity）] ドロップダウンリストから、違反のシビラティを選択します。 • [カスタム違反メッセージ（Custom violation message）] フィールドに、任意のユーザー定義違反メッセージを入力します。

例：ブロック オプション

このコンプライアンスポリシーでは、ある特定のブロック内に定義されている不正または未承認のSNMPコミュニティ文字列があるかどうかを確認します。ブロック内で検出された場合、ポリシーは「承認されていないコミュニティ文字列<1.1>を検出しました（Detected unauthorized community string <1.1>）」というメッセージで違反を報告し、すべての非準拠 SNMP 文字列をブロックから削除します。

ペイン	ペインエリア	フィールド	値
ルール情報（Rule Information）		ルールタイトル（Rule Title）	snmp-server community having non-standard entries
プラットフォームの選択（Platform Selection）			Cisco IOS デバイス、Cisco IOS-XE デバイス
Condition 1			
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	Condition Match Criteria	演算子	Matches the expression
		値	snmp-server community (.*)
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させません（Does Not Raise a Violation）
Condition 2			

ペイン	ペインエリア	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	以前に一致したブロック（Previously Matched Blocks）
	ブロック オプション（Block Options）	ブロック開始表現（Block Start Expression） （このフィールドは、[ブロックとして解析（Parse as Blocks）] チェックボックスがオンになっている場合にのみ有効になります）	^snmp-server community .*
	Condition Match Criteria	演算子	Matches the expression
		値	snmp-server community ((public RO)|(private RW))
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させます。
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	承認されていないコミュニティ文字列 <1.1> を検出しました。（Detected unauthorized community string <1.1>.）

（注） 上記の例では、最初の条件での一致基準は 1.1、1.2 などと呼びます。2 番目の条件での一致基準は 2.1、2.2 などと呼びます。

条件およびアクションの例：NTP サーバーの冗長性

このコンプライアンス ポリシーは、デバイスでコマンド **ntp server** が少なくとも 2 回表示されるかどうかを確認します。表示されない場合、ポリシーは、「少なくとも2つのNTPサーバーを構成する必要があります（At least two NTP servers must be configured）」というメッセージで違反を発生させます。

ペイン	ペインエリア	フィールド	値
[条件の詳細（Condition Details）]	**[条件範囲の詳細（Condition Scope Details）]**	条件の範囲（Condition Scope）	設定（Configuration）
	Condition Match Criteria	演算子	Matches the expression
		値	(ntp server.*\n){2,}
アクションの詳細（Action Details）	**一致アクションの選択（Select Match Action）**	アクションの選択（Select Action）	続行（Continue）
	不一致アクションの選択（Select Does Not Match Action）	アクションの選択（Select Action）	違反を発生させる
		違反メッセージタイプ（Violation Message Type）	ユーザー定義の違反メッセージ
		違反テキスト（Violation Text）	At least two NTP servers must be configured.

ポリシールールへの変数の追加

ルールベースのコンプライアンスポリシー規則に新しい変数を追加するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）]** > **[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [ルール（Rules）] ペインで、ルールの名前をクリックします。

ステップ 4 （任意） [変数（Variables）] ペインを展開します。**[変数の追加（Add Variable）]** をクリックして、ルールに変数を追加します。

a) 変数名、識別子、および説明を対応するフィールドに入力します。
b) [データタイプ（Data type）] ペインを展開し、データタイプを選択します。

選択内容	結果
文字列	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 **4.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。整数データ型には整数を使用します。 [最大長（Maximum Length）] : 文字列の最大長を入力します。 [有効な正規表現（Valid regex）] : 文字列入力を検証するための有効な正規表現を入力します。
整数	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 **4.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。整数データ型には整数を使用します。 [最小値（Minimum value）] : 整数の最小値を入力します。 [最大値（Maximum value）] : 整数の最大値を入力します。

選択内容	結果
ブール	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値のリストを提供するには、[値のリスト（Is list of values）] チェックボックスをオンにします。 **3.** [追加（Add）] をクリックします。次に、対応するフィールドに名前と値を追加します。[Save] をクリックします。 （オプション）[デフォルト値（Default value）] : [true] または [false] を選択します。
IP address	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。
Interface	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の準拠チェック時に複数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにします。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。
IPマスク	**1.** （オプション）[入力必須（Input required）] チェックボックスをオンにして、入力必須条件を定義します。 **2.** （オプション）ルール変数の値を指定するには、[複数の値を受け入れる（Accept multiple values）] チェックボックスをオンにし、準拠チェック中に複数の値を指定します。 （オプション）[デフォルト値（Default value）] : デフォルト値を入力します。

c) [プレビュー（Preview）] セクションには、設定された変数のプレビューが表示されます。[Save] をクリックします。

サイトへのポリシーの割り当て

次の手順を実行して、ルールベースのコンプライアンスポリシーをサイトに割り当てます。

手順

ステップ 1 メインメニューから次を選択します。 **[ポリシー（Policy）] > [ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。

ステップ 2 [ルールベースのコンプライアンスポリシー（Rule -Based Compliance Policies）] テーブルで、ポリシー名をクリックしてポリシーダッシュボードを開きます。

ステップ 3 [サイト（Sites）] ペインで、右上隅にある [サイトへの割り当て（Assign to sites）] をクリックします。

または、ポリシーテーブルから割り当てるには、対応するチェックボックスをオンにして、[サイト（Sites）] 列で [割り当て（Assign）] をクリックします。

ステップ 4 **[サイトへの割り当て（Assign to sites）]** スライドインペインで、サイト階層内のサイトの横にあるチェックボックスをオンにして選択し、[割り当て（Assign）] をクリックします。

ポリシーは、選択したサイトの対象デバイスに適用されます。

Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートして Catalyst Center にインポートする

Cisco Prime Infrastructure からコンプライアンスポリシーを XML としてエクスポートし、Catalyst Center にインポートするには、次の手順を実行します。

- 必要に応じて、個別のコンプライアンスポリシーをエクスポートし、別のサーバーにインポートできます。

手順

ステップ 1 Cisco Prime Infrastructure の GUI で、[設定（Configuration）] > [コンプライアンス（Compliance）] > [ポリシー（Policies）] の順に選択します。

ステップ 2 コンプライアンスポリシーをエクスポートするには、次の手順を実行します。

a) [コンプライアンスポリシー（Compliance Policies）] ナビゲーションエリアから、ポリシーの横にある [i] アイコンにカーソルを合わせます。

b) ポップアップウィンドウで、[XMLとしてポリシーをエクスポート（Export Policy as XML）] ハイパーリンクをクリックし、ファイルを保存します。

ステップ 3 コンプライアンスポリシーを Catalyst Center にインポートするには、次の手順を実行します。

a) 左上隅にあるメニューアイコンをクリックし、**[ポリシー（Policy）]>[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）]** の順に選択します。
b) [ポリシーのインポート（Import policies）] をクリックすると、[コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインが開きます。
c) [コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインで、XML ファイルをアップロードエリアにドラッグアンドドロップします。または、[ファイルをクリックするかこのエリアにドラッグしてアップロード（Click or drag files to this area to upload）] をクリックし、XML ファイルを見つけて [インポート（Import）] をクリックします。

Catalyst Centerからルールベースのコンプライアンスポリシーをエクスポートし、別の Catalyst Center にインポートします。

この手順を使用して、Catalyst Center からコンプライアンスポリシーをエクスポートし、別の Catalyst Center インスタンスにインポートします。

- 主に Catalyst Center インスタンス間のポリシーのエクスポートに使用される JSON ファイルをインポートできます。
- 個別のコンプライアンスポリシーをインポートし、必要に応じて、それらのポリシーを別のサーバーに転送することができます。
- アクティビティ センター ページには、成功したインポートと失敗したインポートの両方に関する詳細が表示されるため、ポリシーの監視とトラブルシュートが容易になります。

手順

ステップ 1 左上隅にあるメニューアイコンをクリックし、[ポリシー（Policy）]>[ルールベースのコンプライアンスポリシー（Rule-Based Compliance Policies）] の順に選択します。

ステップ 2 コンプライアンスポリシーをエクスポートするには、次の手順を実行します。

a) ポリシーテーブルで、目的のポリシーの横にあるチェックボックスをオンにします。
b) [エクスポート（Export）] をクリックします。ZIP ファイルから JSON ファイルを抽出し、ローカルデスクトップに保存します。

ステップ 3 コンプライアンスポリシーを Catalyst Center にインポートするには、次の手順を実行します。

a) [ポリシーのインポート（Import policies）] をクリックすると、[コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインが開きます。
b) [コンプライアンスポリシーのインポート（Import compliance policy）] スライドインペインで、XML ファイルをアップロードエリアにドラッグアンドドロップします。または、[ファイルをクリックする

かこのエリアにドラッグしてアップロード（Click or drag files to this area to upload）] をクリックし、XML ファイルを見つけて [インポート（Import）] をクリックします。

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。

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。

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。

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。

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。

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。

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。

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。