RV132WまたはRV134W VPNルータでの攻撃防御の設定

目的

攻撃保護を使用すると、ディスカバリ、フラッディング、エコーストームなどの一般的なタイプの攻撃からネットワークを保護できます。ルータではデフォルトで攻撃防御が有効になっていますが、パラメータを調整することで、ネットワークの感度を高め、検出される攻撃に対する応答性を高めることができます。

この記事では、RV132WおよびRV134W VPNルータに攻撃防御を設定する方法について説明します。

該当するデバイス

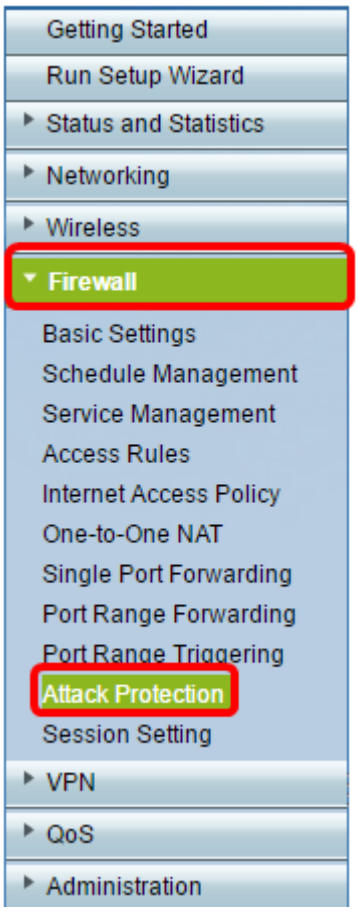
- RV 132W
- RV134W

[Software Version]

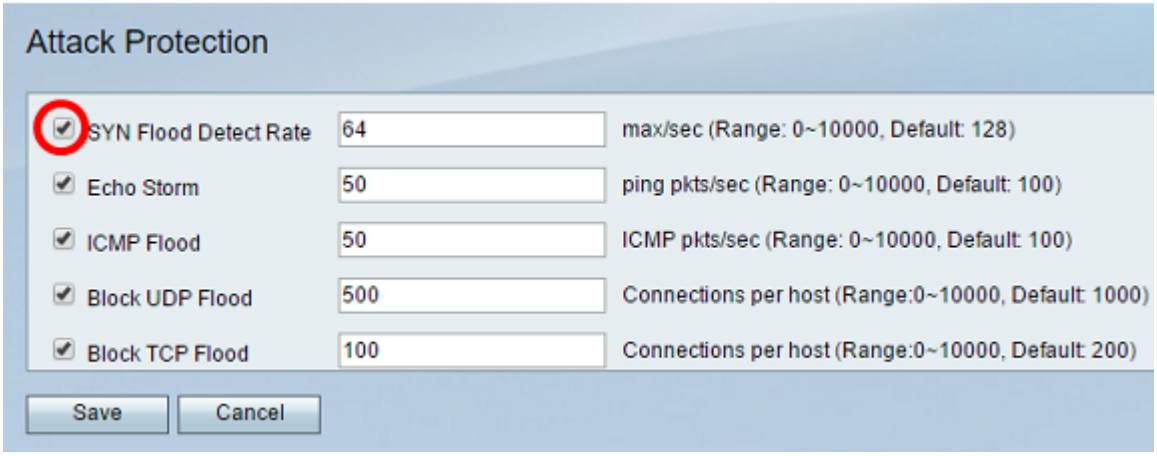
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

攻撃防御の設定

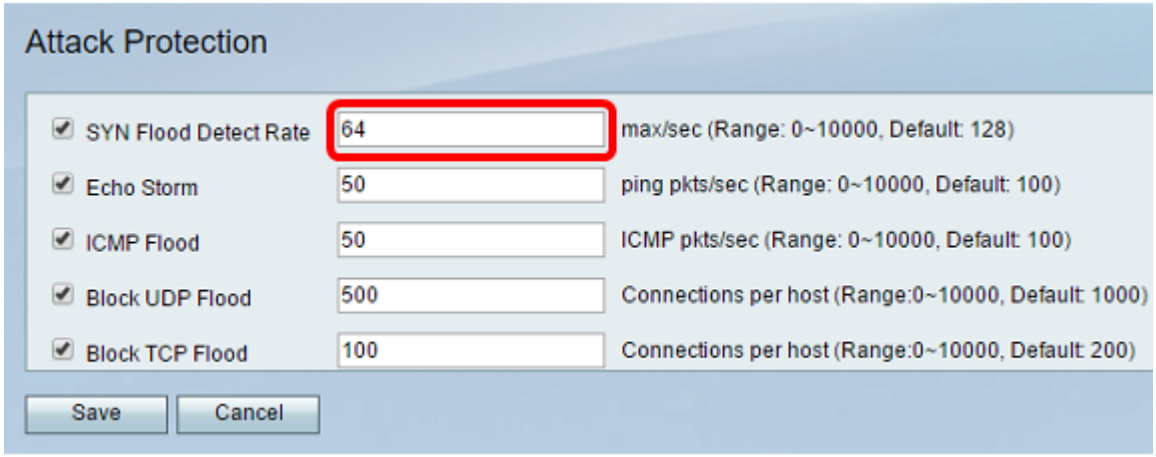
ステップ 1：Webベースのユーティリティにログインし、[Firewall] > [Attack Protection] を選択します。



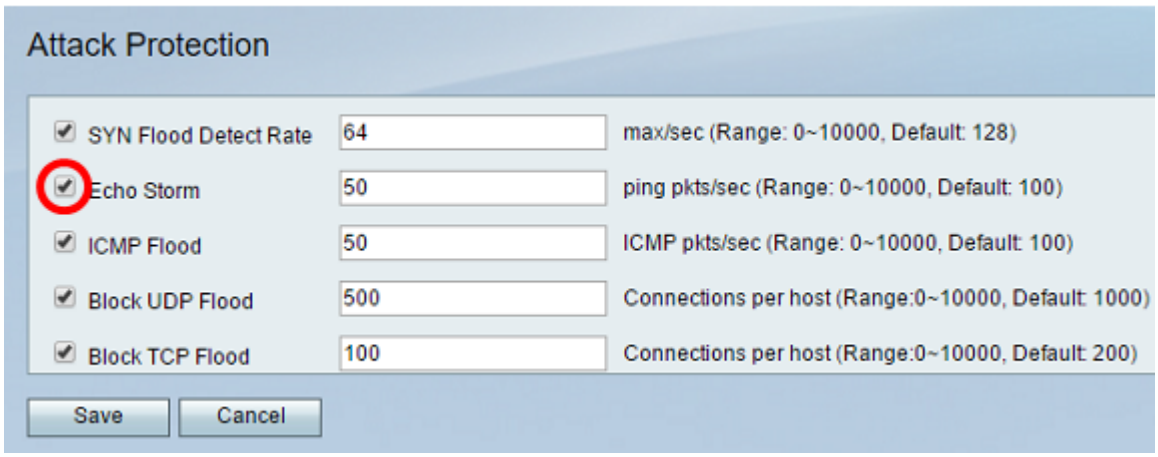
ステップ 2：[SYNフラッド検出レート(SYN Flood Detect Rate)]チェックボックスがオンになっていることを確認し、機能がアクティブであることを確認します。これはデフォルトでオンになっています。



ステップ 3：[SYN Flood Detect Rate] フィールドに値を入力します。デフォルト値は128 SYNパケット/秒です。0 ~ 10000の値を入力できます。SYNフラッド侵入が発生しているとセキュリティアプライアンスが判断する原因となるSYNパケットの1秒あたりの数です。ゼロの値は、SYNフラッド検出機能が無効であることを示します。この例では、64が入力されています。これは、アプライアンスが1秒あたり64個のSYNパケットのみでSYNフラッド侵入を検出することを意味し、デフォルト設定よりも機密性が高くなります。

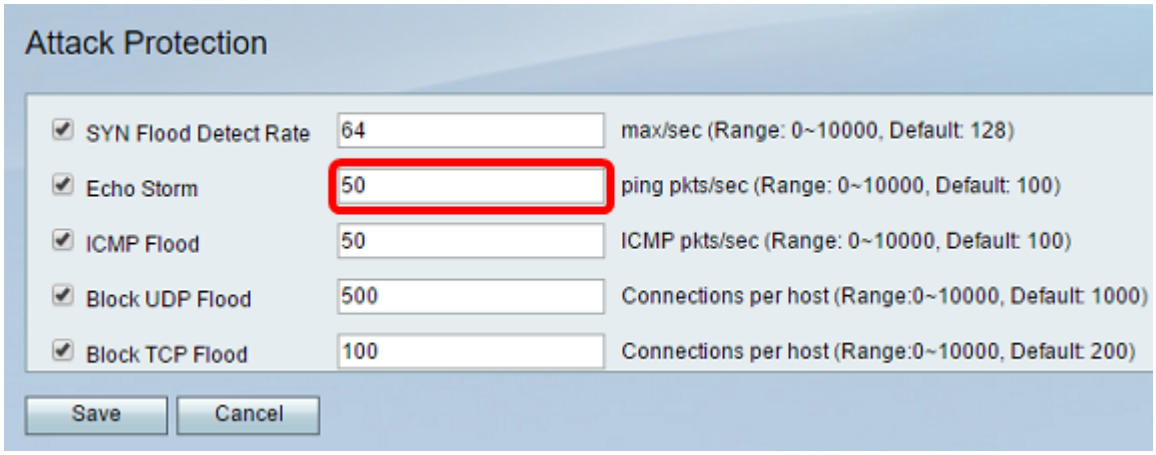


ステップ 4：[エコーストーム(Echo Storm)]チェックボックスがオンになっていることを確認し、機能がアクティブであることを確認します。これはデフォルトでオンになっています。

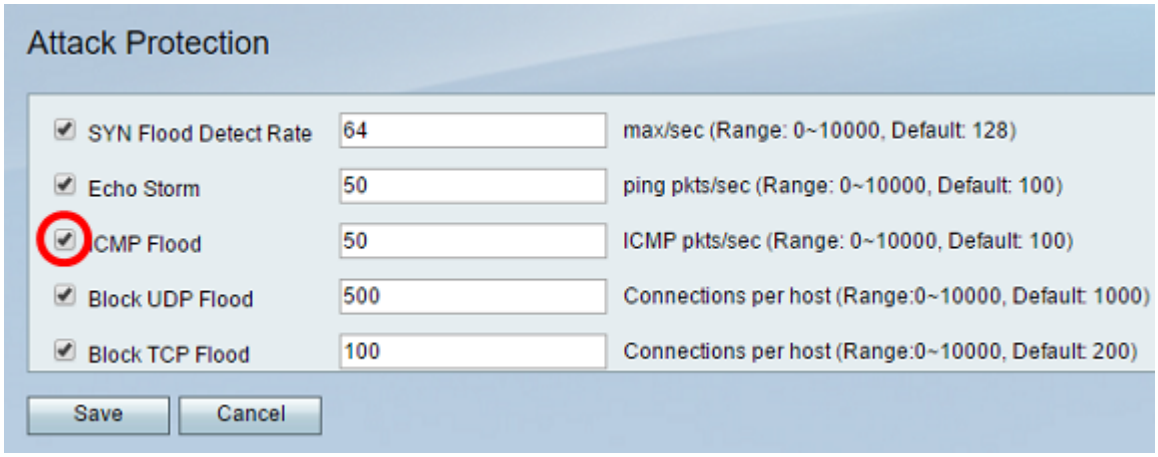


ステップ 5：[Echo Storm] フィールドに値を入力します。デフォルト値は毎秒100回のpingです。0 ~ 10000の値を入力できます。これは、エコーストーム侵入イベントが発生していることをセキュリティアプライアンスが判断する1秒あたりのpingの数です。ゼロの値は、エコーストーム機能が無効であることを示します。

注：この例では、アプライアンスは毎秒50回のpingでエコーストームを検出します。

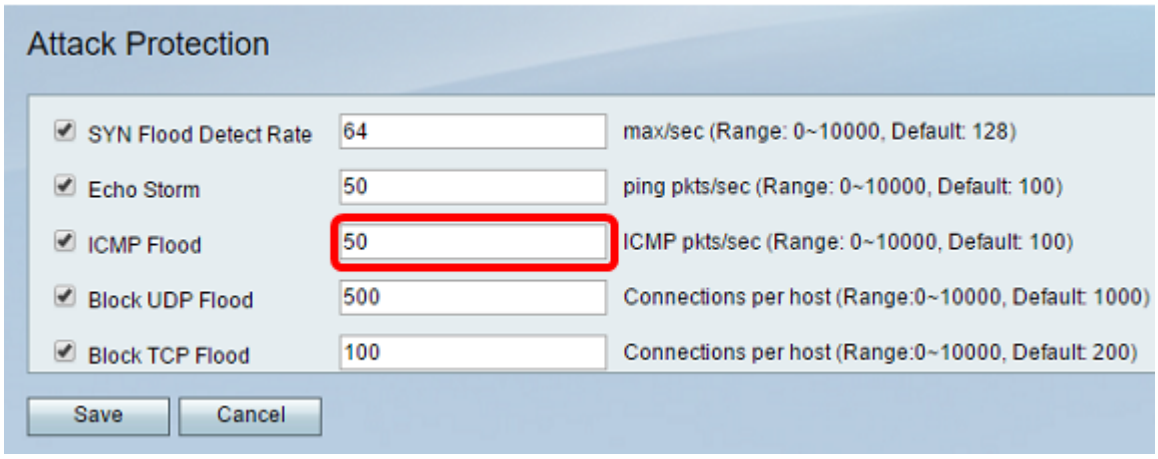


手順 6：[インターネット制御メッセージプロトコル(ICMP)フラッド(Internet Control Message Protocol (ICMP) Flood)]チェックボックスがオンになっていることを確認し、機能がアクティブであることを確認します。この機能はデフォルトでオンになっています。

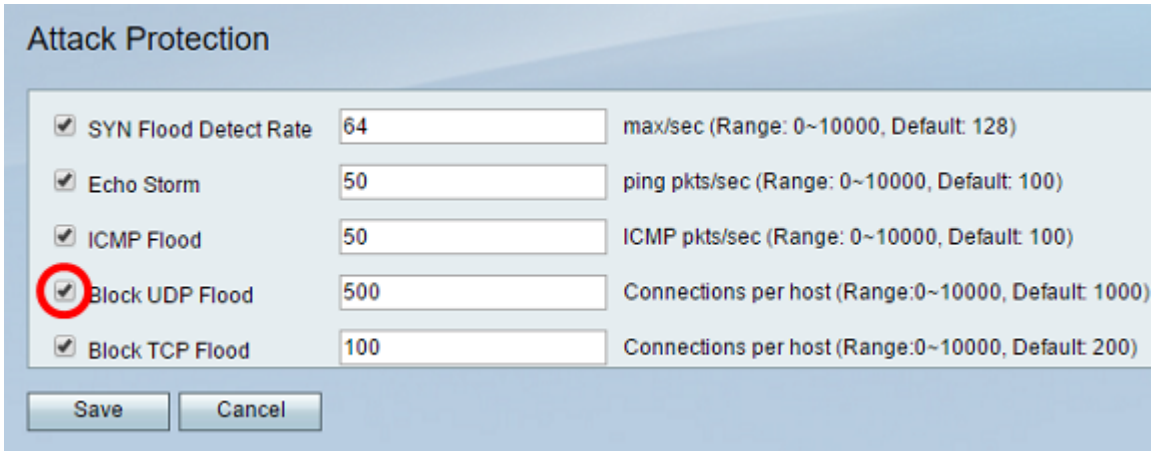


手順 7：[ICMP Flood] フィールドに数値を入力します。デフォルト値は100 ICMPパケット/秒です。0 ~ 10000の値を入力できます。これは、ICMPフラッド侵入イベントが発生していることをセキュリティアプライアンスが判断する1秒あたりのICMPパケット数です。ゼロの値は、ICMPフラッド機能が無効であることを示します。

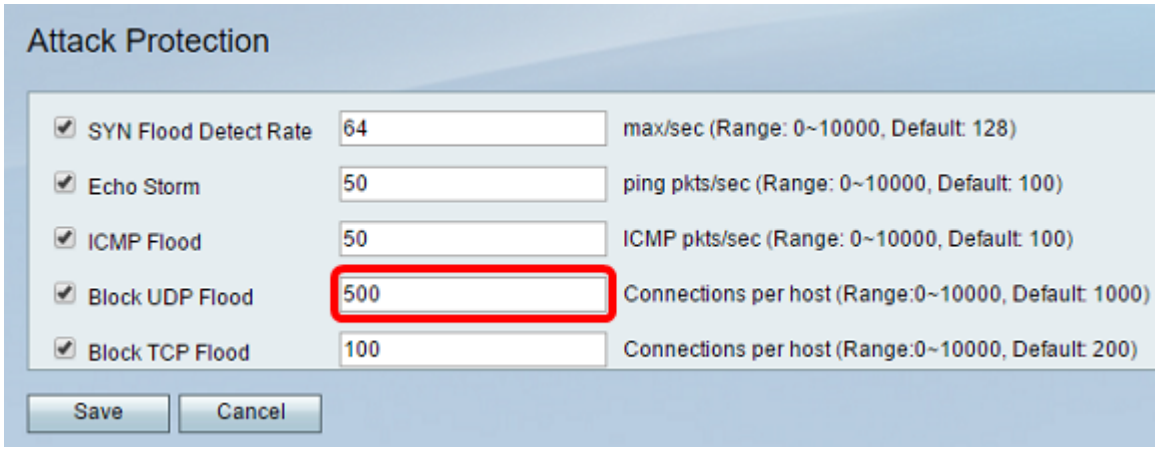
注：この例では、入力された値は50であるため、ICMPフラッディングの影響をデフォルト設定よりも受けやすくなっています。



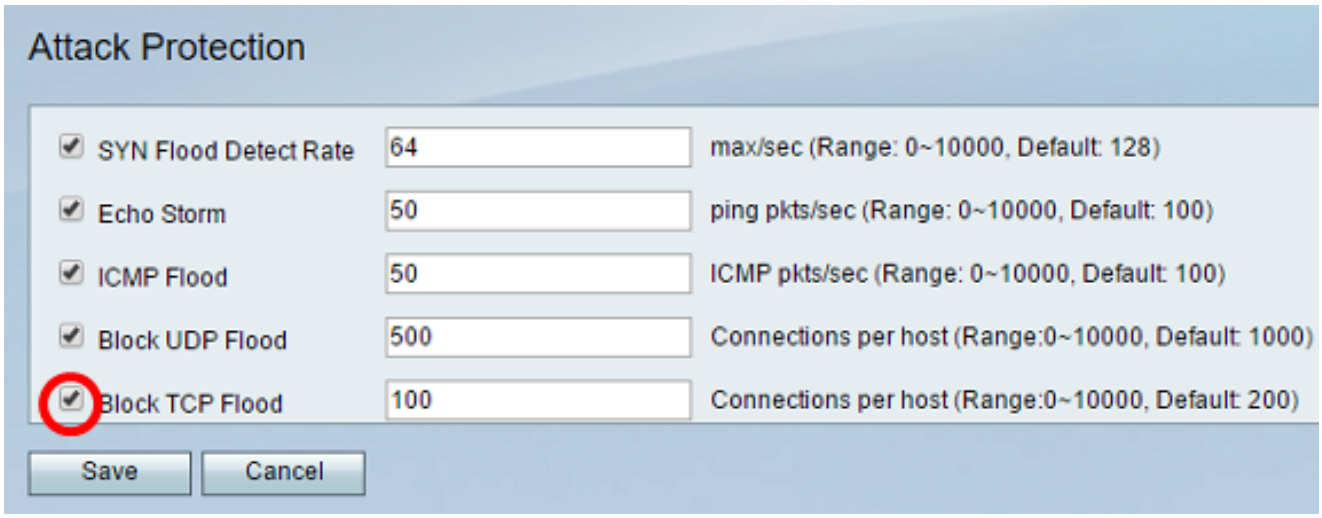
ステップ 8：[UDPフラッドをブロックする(Block UDP Flood)]チェックボックスがオンになっていることを確認して、機能がアクティブになっていることを確認し、セキュリティアプライアンスがローカルエリアネットワーク(LAN)上の1台のコンピュータからの1秒あたり150を超える同時アクティブユーザデータグラムプロトコル(UDP)接続を受け入れないようにします。このオプションはデフォルトでオンになっています。



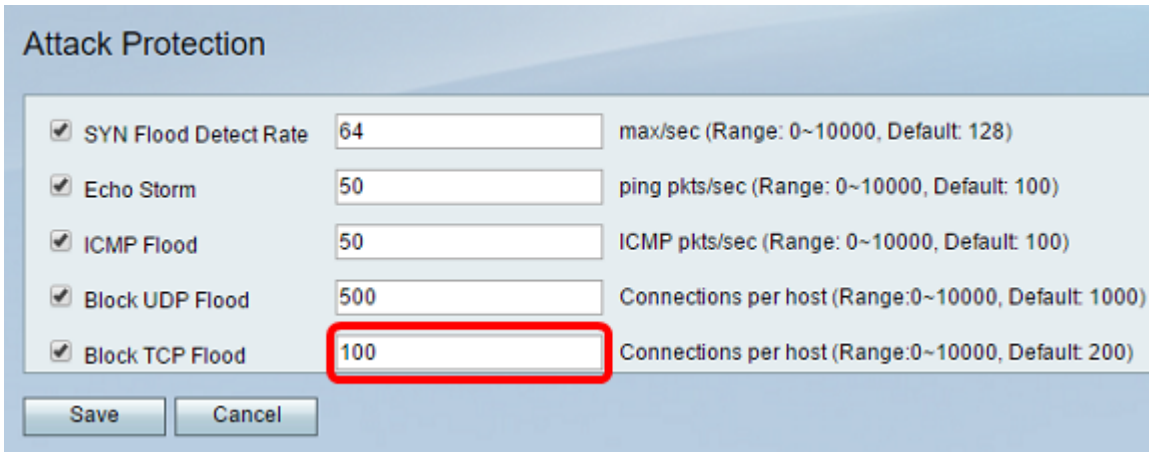
ステップ 9：[Block UDP Flood] フィールドに0 ~ 10000の値を入力します。デフォルト値は 1000 です。この例では、入力する値は500であるため、感度が高くなります。



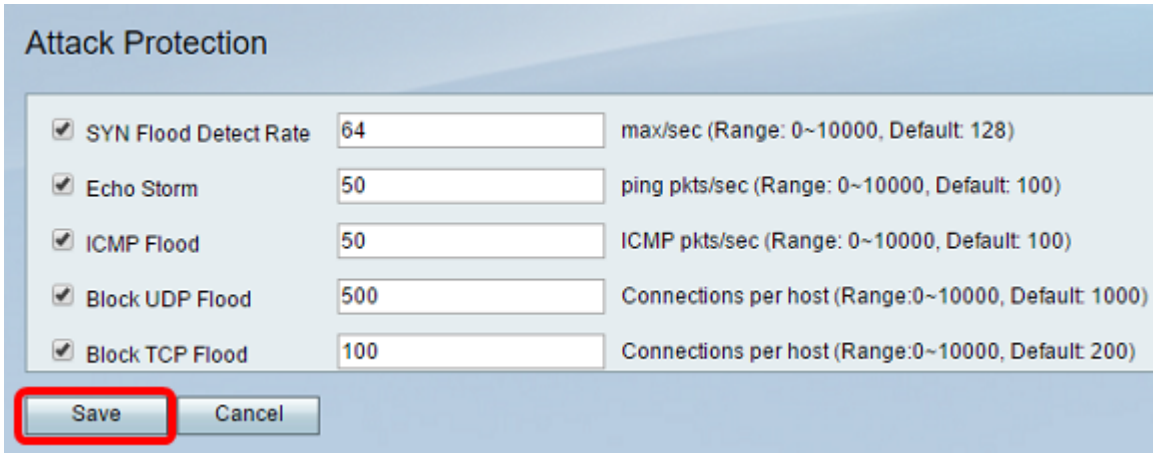
ステップ 10：無効なTransmission Control Protocol（TCP；伝送制御プロトコル）パケットをすべて廃棄するには、[Block TCP Flood]チェックボックスがオンになっていることを確認します。このオプションはデフォルトでオンになっています。



ステップ 11SYNフラッド攻撃からネットワークを保護するには、[Block TCP Flood] フィールドに0 ~ 10000の値を入力します。デフォルト値は 200 です。この例では、100と入力して、感度を高めています。



ステップ 12[Save] をクリックします。



これで、RV132WまたはRV134Wルータに攻撃防御が正しく設定されました。

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。