Cisco Identity Services Engine リリース 3.3 ネットワークコンポーネントの互換性

改訂：2023 年 12 月 14 日

概要

Cisco ISE は、RADIUS、関連する RFC 規格、TACACS+ などのプロトコル規格をサポートしています。詳細については、ISE コミュニティリソースを参照してください。

Cisco ISE は、標準ベースの認証に共通の RADIUS 動作を実装するシスコまたはシスコ以外の RADIUS クライアント ネットワーク アクセス デバイス（NAD）との相互運用性をサポートします。

Cisco ISE は、管理プロトコルに準拠するサードパーティの TACACS+ クライアントデバイスと完全に相互に機能します。TACACS+ 機能がサポートされるかどうかは、そのデバイス固有の実装によって異なります。

RADIUS

Cisco ISE は、標準プロトコルに準拠するサードパーティの RADIUS デバイスと完全に相互に機能します。RADIUS 機能がサポートされるかどうかは、そのデバイス固有の実装によって異なります。

ポスチャアセスメント、プロファイリング、および Web 認証を含むものなど、特定の高度な使用例は、シスコ以外のデバイスでは一貫して利用できないか、機能が制限される場合があります。すべてのネットワークデバイスとそのソフトウェアのハードウェア機能または特定のソフトウェアリリースのバグを検証することをお勧めします。

ネットワークデバイスが動的および静的 URL リダイレクトのいずれもサポートしない場合、Cisco ISE は URL リダイレクトをシミュレートすることにより認証 VLAN 構成を提供します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Secure Wired Access」の章にある「Third-Party Network Device Support in Cisco ISE」のセクションを参照してください。

TACACS+

Cisco ISE は、管理プロトコルに準拠するサードパーティの TACACS+ クライアントデバイスと完全に相互に機能します。TACACS+ 機能がサポートされるかどうかは、そのデバイス固有の実装によって異なります。

ネットワークスイッチで Cisco ISE の特定の機能を有効にする方法については、『Cisco Identity Services Engine Administrator Guide』の「Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions」の章を参照してください。

ISE コミュニティ リソース

「Does ISE Support My Network Access Device?」

サードパーティ製 NAD プロファイルについては、「ISE Third-Party NAD Profiles and Configs」を参照してください。

Nexus デバイスの TACACS+ の設定方法については、『Cisco ISE Device Administration Prescriptive Deployment Guide』を参照してください。

（注）

- 一部のスイッチモデルと IOS バージョンがサポート終了日に達した可能性があります。また、Cisco TAC では相互運用性がサポートされていない可能性があります。
- Cisco ISE プロファイリングサービスについては、最新バージョンの NetFlow を使用する必要があります。NetFlow バージョン 5 を使用する場合は、アクセスレイヤのプライマリ NAD でのみ使用できます。

ワイヤレス LAN コントローラの場合は、次の点に注意してください。

- MAC 認証バイパス（MAB）は、RADIUS ルックアップによる MAC フィルタリングをサポートしています。
- MAC フィルタリングを使用したセッション ID と COA のサポートにより、MAB のような機能が提供されます。
- DNS ベースの ACL 機能は WLC 8.0 以前でサポートされています。すべてのアクセスポイントが DNS ベースの ACL をサポートしているわけではありません。詳細については、『Cisco Access Points Release Notes』を参照してください。

Cisco ISE で検証されるデバイスの詳細については、「Network Device Capabilities Validated with Cisco Identity Services Engine」を参照してください。

サポートされるプロトコル規格、RFC、および IETF ドラフト

Cisco ISE は、次のプロトコル規格、Requests for Comments（RFC）、および IETF ドラフトに準拠しています。

- **サポートされている IEEE 標準規格**
  - IEEE802.1X-Std-2001
  - IEEE802.1X-Std-2004
- **サポートされている IETF RFC**
  - RFC2138 - RADIUS
  - RFC2246 - TLSv1.0
  - RFC2548 - Microsoft Vendor-specific RADIUS Attributes
  - RFC2759 - Microsoft PPP CHAP Extensions, Version 2
  - RFC2865 - RADIUS
  - RFC2866 - RADIUS Accounting
  - RFC2867 - RADIUS Accounting Modifications for Tunnel Protocol Support
  - RFC2868 - RADIUS Attributes for Tunnel Protocol Support
  - RFC2869 - RADIUS Extensions
  - RFC3579 - RADIUS Support For EAP
  - RFC3580 - IEEE 802.1X RADIUS Usage Guidelines
  - RFC3748 - EAP

- RFC4017 - EAP Method Requirements for Wireless LANs
- RFC4851 - EAP-FAST
- RFC5176 - Dynamic Authorization Extensions to RADIUS
- RFC5216 - EAP-TLS Authentication Protocol
- RFC5281 - Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
- RFC5422 - Dynamic Provisioning Using Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST)
- RFC5425 - Transport Layer Security (TLS) Transport Mapping for Syslog
- RFC6587 - Transmission of Syslog Messages over TCP
- RFC7360 - Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS

次の RFC が部分的にサポートされます。

- RFC2548 - Microsoft Vendor-specific RADIUS Attributes
- RFC2882 - Network Access Servers Requirements: Extended RADIUS Practices
- RFC7030 - Enrollment over Secure Transport (EST)（BYOD フローの一部としてサポート）
- RFC7170 - Tunnel Extensible Authentication Protocol (TEAP) Version 1

- **サポートされている IETF ドラフト**
  - IETF ドラフト - PEAP Version 0
  - IETF ドラフト - PEAP Version 1
  - IETF ドラフト - PEAP Version 2
  - IETF ドラフト - Microsoft EAP CHAP Extensions Version 2

RADIUS プロキシサービスの AAA 属性

RADIUS プロキシサービスの場合、次の認証、許可、およびアカウンティング（AAA）属性を RADIUS 通信に含める必要があります。

- Calling-Station-ID（IP または MAC_ADDRESS）
- RADIUS::NAS_IP_Address
- RADIUS::NAS_Identifier

サードパーティ VPN コンセントレータの AAA 属性

VPN コンセントレータを Cisco ISE と統合するには、次の認証、許可、およびアカウンティング（AAA）属性を RADIUS 通信に含める必要があります。

- Calling-Station-ID（MAC または IP アドレスによる個々のクライアントの追跡）
- User-Name（ログイン名によるリモートクライアントの追跡）
- NAS-Port-Type（VPN としての接続タイプの決定に役立つ）
- RADIUS Accounting Start（セッションの正式な開始をトリガーします）
- RADIUS Accounting Stop（セッションの正式な終了をトリガーし、ISE ライセンスをリリースします)
- IP アドレス変更時の RADIUS アカウンティング暫定更新（たとえば、SSL VPN 接続は Web ベースからフルトンネルクライアントに移行します）

（注） VPNデバイスの場合、信頼できるネットワーク上にあるエンドポイントを追跡するには、RADIUSアカウンティングメッセージの Framed-IP-Address 属性をクライアントの VPN 割り当て IP アドレスに設定する必要があります。

システム要件

Cisco ISE の設定を継続使用する場合は、次のシステム要件が満たされていることを確認してください。

このCisco ISEリリースのハードウェアプラットフォームおよびインストールの詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

スマートライセンスをサポートする SSM オンプレミス サーバー リリースの詳細については、ご使用のリリースの『Cisco ISE Administrator Guide』の「Licensing」の章にある、スマートライセンス用に Smart Software Manager をオンプレミスで設定するトピックを参照してください。

サポート対象ハードウェア

Cisco ISE 3.3 は、次の Secure Network Server（SNS）ハードウェア プラットフォームにインストールできます。

表 *1*: サポートされるプラットフォーム

ハードウェア プラットフォーム	設定
Cisco SNS-3615-K9（小規模）	アプライアンスハードウェアの仕様については、『Cisco Secure Network Server Appliance Hardware Installation Guide』を参照してください。
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	
Cisco SNS-3715-K9（小規模）	
Cisco SNS-3755-K9（中規模）	
Cisco SNS-3795-K9（大規模）	

サポートされる仮想環境

Cisco ISE は次の仮想環境プラットフォームをサポートしています。

- Cisco ISE リリース 3.3 は、VMware ESXi 6.7 をサポートする最後のリリースです。

  Cisco ISE リリース 3.0 以降のリリースでは、VMware ESXi 7.0.3 以降のリリースに更新することを推奨します。

  vTPM デバイスの場合は、VMware ESXi 7.0.3 以降のリリースにアップグレードする必要があります。

  - OVA テンプレート：ESXi 6.7 以降および ESXi 7.*x* の VMware バージョン 14 以降。
  - ISO ファイルは ESXi 6.7 以降のリリースをサポートしています。

  次のパブリック クラウド プラットフォーム上の VMware クラウドソリューションに Cisco ISE を展開できます。

  - Amazon Web サービス（AWS）の VMware クラウド：Cisco ISE をAWS の VMware クラウドが提供するソフトウェアデファインド データセンターでホストします。
  - Azure VMware ソリューション：Azure VMware ソリューションは、Microsoft Azure 上でネイティブに VMware ワークロードを実行します。Cisco ISE を VMware 仮想マシンとしてホストできます。
  - Google Cloud VMware Engine：Google Cloud VMware Engine は、Google Cloud 上の VMware によってソフトウェアデファインド データセンターを実行します。VMware Engine によって提供されるソフトウェアデファインド データセンターで、VMware 仮想マシンとして Cisco ISE をホストできます。

- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V
- QEMU 2.12.0-99 上の KVM
- Nutanix AHV 20220304.392

次のパブリック クラウド プラットフォーム上に Cisco ISE をネイティブに展開できます。

- Amazon Web Services（AWS）
- Microsoft Azure
- Oracle Cloud Infrastrucure（OCI）

（注） Cisco ISE 3.1 以降では、仮想マシン（VM）インスタンス（任意のペルソナを実行）のホスト間での移行に VMware マイグレーション機能を使用できます。Cisco ISE はホットマイグレーションとコールドマイグレーションの両方をサポートします。ホットマイグレーションは、ライブマイグレーションまたは vMotion とも呼ばれます。ホットマイグレーション中に Cisco ISE をシャットダウンしたり、電源をオフにしたりする必要はありません。可用性を損なうことなく、Cisco ISE VM を移行できます。

仮想マシンの要件に関する情報については、お使いの Cisco ISE バージョンの『Cisco Identity Services Engine Installation Guide』を参照してください。

連邦情報処理標準（FIPS）モードのサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco FIPS オブジェクト モジュール バージョン 7.2（証明書 #3790）を使用します。FIPS コンプライアンス要求の詳細については、Global Government Certifications を参照してください。

Cisco ISE で FIPS モードが有効になっている場合は、次の点を考慮してください。

- すべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。
- 楕円曲線デジタル署名アルゴリズム（ECDSA）の秘密キーには、224 ビット以上を指定する必要があります。
- Diffie–Hellman Ephemeral（DHE）暗号方式は 2048 ビット以上の Diffie–Hellman（DH）パラメータを使用して動作します。
- SHA1 は、ISE ローカルサーバー証明書の生成を許可されていません。
- EAP-FAST の匿名 PAC プロビジョニングオプションは無効です。
- ローカル SSH サーバーは FIPS モードで動作します。
- RADIUS の場合、次のプロトコルは FIPS モードではサポートされていません。
    - EAP-MD5
    - PAP
    - CHAP
    - MS-CHAPv1
    - MS-CHAPv2
    - LEAP

検証済みブラウザ

Cisco ISE 3.3 は、次のブラウザで検証済みです。

- Mozilla Firefox バージョン 113 および 114
- Google Chrome バージョン 112 および 114
- Microsoft Edge バージョン 112

検証済み外部 ID ソース

（注） サポートされている Active Directory バージョンは、Cisco ISE と Cisco ISE-PIC の両方で同じです。

表 *2 :* 検証済み外部 *ID* ソース

外部 ID ソース	バージョン
Active Directory [1]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [2]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [3]	Windows Server 2019
LDAP サーバー	
SunONE LDAP ディレクトリサーバー	バージョン 5.2
OpenLDAP ディレクトリサーバー	バージョン 2.4.23
任意の LDAP v3 準拠サーバー	LDAP v3 準拠のすべてのバージョン
LDAP としての AD	Windows Server 2022（パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み）
トークンサーバー	
RSA ACE/サーバー	6.x シリーズ
RSA 認証マネージャ	7.x および 8.x シリーズ
Any RADIUS RFC 2865 準拠のトークン サーバー	RFC 2865 準拠のすべてのバージョン
セキュリティ アサーション マークアップ言語（SAML）シングルサインオン（SSO）	
Microsoft Azure	最新
Oracle Access Manager（OAM）	バージョン 11.1.2.2.0
Oracle Identity Federation（OIF）	バージョン 11.1.1.2.0
PingFederate サーバー	バージョン 6.10.0.4
PingOne クラウド	最新
セキュア認証	8.1.1
SAMLv2 準拠の ID プロバイダー	SAMLv2 準拠の任意の ID プロバイダバージョン
Open Database Connectivity（ODBC）アイデンティティソース	

外部 ID ソース	バージョン
Microsoft SQL Server	Microsoft SQL Server 2012
Oracle	Enterprise Edition リリース 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
ソーシャルログイン（ゲストユーザーアカウントの場合）	
Facebook	最新

[1] Cisco ISE には最大 200 のドメインコントローラのみを追加できます。制限を超えると、次のエラーが表示されます：

```
Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200
```

[2] Cisco ISE は、Microsoft Windows Active Directory 2012 R2 のすべてのレガシー機能をサポートしていますが、保護ユーザーグループなどの Microsoft Windows Active directory 2012 R2 の新機能はサポートされていません。

[3] Cisco ISE 2.6 パッチ 4 は、Microsoft Windows Active Directory 2012 R2 のすべてのレガシー機能をサポートしています。

詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

サポートされている統合エンドポイント管理およびモバイルデバイス管理サーバー

サポートされる MDM サーバーは、次のベンダーの製品です。

- Absolute
- Blackberry：BES
- Blackberry：Good Secure EMM
- Cisco Meraki Systems Manager
- Citrix XenMobile 10.x（オンプレミス）
- Globo
- IBM MaaS360
- Ivanti（旧 MobileIron UEM）、コアおよびクラウド UEM サービス

  Cisco ISE 3.1 におけるランダムおよび変更 MAC アドレスの処理に関するユースケースでは、MobileIron Core 11.3.0.0 ビルド 24 以降のリリースを統合し、GUID 値を受け取る必要があります。

（注） 一部のバージョンの MobileIron は Cisco ISE では動作しません。MobileIron はこの問題を認識しており、修正があります。詳細については、MobileIron 社までお問い合わせください。

- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Microsoft Endpoint Manager Intune
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE（以前の AirWatch）
- 42Gears

サーバーを Cisco ISE と統合するためにエンドポイント管理サーバーで実行する必要がある設定については、「Integrate UEM and MDM Servers With Cisco ISE」を参照してください。

ISE コミュニティ リソース

How To: Meraki EMM / MDM Integration with ISE

サポート対象のウイルス対策およびマルウェア対策製品

Cisco ISE ポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco AnyConnect ISE ポスチャのサポート表を参照してください。

サポート対象の暗号方式

Cisco ISE のクリーンインストールまたは新規インストールでは、SHA1 暗号はデフォルトで無効になっています。ただし、既存のバージョンの Cisco ISE からアップグレードする場合、SHA1 暗号は以前のバージョンのオプションのままです。SHA1 暗号の設定は、[SHA1暗号を許可する（Allow SHA1 Ciphers）] フィールド（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]）を使用して表示および変更できます。

（注） この暗号は、管理者ポータルには適用されません。連邦情報処理標準モード（FIPS）で実行している場合、アップグレードでは管理者ポータルから SHA1 暗号が削除されません。

Cisco ISE は、TLS バージョン 1.0、1.1、および 1.2 をサポートします。

Cisco ISE は、RSA および ECDSA サーバー証明書をサポートしています。次の楕円曲線をサポートしています。

- secp256r1
- secp384r1
- secp521r1

（注） Cisco ISE は、OpenJDK 1.8 の現在の導入における制限により、楕円曲線に関する SHA256withECDSA 署名アルゴリズムを含む中間証明書をサポートしていません。

次の表に、サポートされている暗号スイートが表示されています。

暗号スイート	**Cisco ISE が EAP サーバーとして設定されている場合** **Cisco ISE が RADIUS DTLS サーバーとして設定されている場合**	**Cisco ISE が、HTTPS またはセキュア LDAP サーバーから CRL をダウンロードする場合** **Cisco ISE がセキュアな LDAP クライアントとして設定されている場合** **Cisco ISE が CoA の RADIUS DTLS クライアントとして設定されている場合**
TLS 1.0 のサポート	TLS 1.0 が許可されている場合 （DTLS サーバーは DTLS 1.2 のみをサポート） Cisco ISE 2.3 以上では、[TLS 1.0を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.0 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.0 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウの [TLS 1.0 を許可（Allow TLS 1.0）] チェックボックスをオンにします。Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）]**。	TLS 1.0 が許可されている場合 （DTLS クライアントは DTLS 1.2 のみをサポート）

TLS 1.1 のサポート	TLS 1.1 が許可されている場合	TLS 1.1 が許可されている場合
ECC DSA 暗号方式		
ECDHE-ECDSA-AES256-GCM-SHA384	対応	対応
ECDHE-ECDSA-AES128-GCM-SHA256	対応	対応
ECDHE-ECDSA-AES256-SHA384	対応	対応
ECDHE-ECDSA-AES128-SHA256	対応	対応
ECDHE-ECDSA-AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECDHE-ECDSA-AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECC RSA 暗号方式		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
DHE RSA 暗号方式		
DHE-RSA-AES256-SHA256	非対応	対応
DHE-RSA-AES128-SHA256	非対応	対応
DHE-RSA-AES256-SHA	非対応	SHA-1 が許可されている場合
DHE-RSA-AES128-SHA	非対応	SHA-1 が許可されている場合
RSA 暗号方式		
AES256-SHA256	対応	対応
AES128-SHA256	対応	対応

AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
3DES 暗号方式		
DES-CBC3-SHA	3DES/SHA-1 が許可されている場合	3DES/DSS および SHA-1 が有効になっている場合
DSS 暗号方式		
DHE-DSS-AES256-SHA	非対応	3DES/DSS および SHA-1 が有効になっている場合
DHE-DSS-AES128-SHA	非対応	3DES/DSS および SHA-1 が有効になっている場合
EDH-DSS-DES-CBC3-SHA	非対応	3DES/DSS および SHA-1 が有効になっている場合
弱い RC4 暗号方式		
RC4-SHA	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっていて、SHA-1 が許可されている場合	非対応
RC4-MD5	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっている場合	非対応
EAP-FAST 匿名プロビジョニングのみの場合： ADH-AES-128-SHA	対応	非対応
ピア証明書の制限		
KeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

ExtendedKeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。 • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	サーバー証明書では ExtendedKeyUsage=Server Authentication が必要です

検証済み OpenSSL のバージョン

Cisco ISE 3.3 は、OpenSSL 1.1.1t および Cisco SSL 7.3.265 で検証済みです。

検証済みのクライアントマシンのオペレーティングシステム、サプリカント、およびエージェント

このセクションでは、検証されたクライアントマシンのオペレーティングシステム、ブラウザ、および各クライアントマシンタイプのエージェントバージョンを示します。すべてのデバイスでは、Web ブラウザで cookie が有効になっている必要もあります。Cisco AnyConnect ISE のサポートチャートは、次から入手できます。 https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

次のクライアントマシンタイプは、Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）およびポスチャワークフローで検証されています。

- Apple iOS
- Apple macOS
- Google Android
- Google Chromebook
- Linux
- Microsoft Windows

Cisco ISE 2.7 パッチ 8 以降、Cisco ISE 3.0 パッチ 7 以降、Cisco ISE 3.1 パッチ 5 以降、Cisco ISE 3.2 パッチ 1 以降、および Cisco ISE 3.3 以降のリリースは、Windows、macOS、および Linux オペレーティングシステム用の AnyConnect と Cisco Secure Client の両方をサポートします。

すべての標準 802.1X サプリカントは、Cisco ISE でサポートされる標準認証プロトコルをサポートしている限り、Cisco ISE、リリース 2.4 以降の標準および高度な機能で使用できます。VLAN 変更許可機能をワイヤレス展開で動作させるには、サプリカントで VLAN 変更時の IP アドレスの更新がサポートされている必要があります。

ポスチャおよび個人所有デバイス持ち込み（BYOD）のフローは、最新のポスチャ フィード アップデートに基づき、Cisco ISE UI にリストされているオペレーティングシステムの一般提供リリースでサポートされます。ポスチャおよび BYOD フローは、Cisco ISE UI にリストされているベータ版の macOS リリースでも動作する可能性があります。たとえば、**macOS 12 ベータ版（すべて）** が Cisco ISE UI にリストされている場合、ポスチャおよび BYOD フローは、macOS 12 ベータ版のエンドポイントで動作する可能性があります。ベータ版オペレーティングシステムのリリースは、初期リリースと一般提供リリースの間で大幅に変更されることが多いため、サポートはベストエフォートベースで提供されます。

オペレーティングシステム（OS）を新しいバージョンに更新すると、ポスチャフィードサーバーで更新された OS バージョンのサポートおよび再構築に遅延（数時間または 1 日）が発生する場合があります。

Apple iOS

このクライアントマシンタイプは、BYOD およびポスチャワークフローで検証されています。

Apple iOS デバイスは Cisco ISE または 802.1x で 保護拡張認証プロトコル（PEAP）を使用し、パブリック証明書には iOS デバイスが検証する必要がある CRL 分散ポイントが含まれますが、ネットワークアクセスなしではそれを実行できません。ネットワークに対して認証するには、iOS デバイスで [確定/承諾（confirm/accept）] をクリックします。

Cisco ISE で検証済みの Apple iOS のバージョンは次のとおりです。

- Apple iOS 16.x
- Apple iOS 15.x
- Apple iOS 14.x
- Apple iOS 13.x
- Apple iOS 12.x
- Apple iOS 11.x

（注）

- Apple iOS 12.2 以降のバージョンを使用している場合は、ダウンロードした証明書/プロファイルを手動でインストールする必要があります。これを行うには、Apple iOS デバイスで [設定（Settings）]>[全般（General）]>[プロファイル（Profile）] を選択し、[インストール（Install）] をクリックします。
- Apple iOS 12.2 以降のバージョンを使用している場合、RSA キーサイズは 2048 ビット以上である必要があります。それ以外の場合は、BYOD プロファイルのインストール中にエラーが表示されることがあります。
- Apple iOS 13 以降のバージョンを使用している場合は、[SAN] フィールドに **<<FQDN>>** を **DNS 名**として追加して、ポータルロールの自己署名証明書を再生成します。
- Apple iOS 13 以降のバージョンを使用している場合は、**SHA-256**（またはそれ以上）が署名アルゴリズムとして選択されていることを確認します。

Apple macOS

このクライアントマシンタイプは、BYOD およびポスチャワークフローで検証されています。

表 *3 : Apple macOS*

クライアントマシンのオペレーティングシステム	**AnyConnect**
Apple macOS 13.x	4.10.05111 以降
Apple macOS 12.6	4.10.05111 以降
Apple macOS 12.5	4.10.04071 以降
Apple macOS 11.6	4.9.04043 以降
Apple macOS 10.15	4.8.01090 以降
Apple macOS 10.14	4.8.01090 以降
Apple macOS 10.13	4.8.01090 以降

Cisco ISE は、AnyConnect 4.x の以前のリリースで動作します。ただし、新しい機能をサポートしているのは、新しい AnyConnect リリースのみです。

（注） Apple macOS 11 の場合、Cisco AnyConnect 4.9.04043 以降と MAC OSX コンプライアンスモジュール 4.3.1466.4353 以降を使用する必要があります。

Apple macOS 11 を使用している場合、Cisco Network Setup Assistant のインストール中にプロファイルを手動でインストールするように求めるプロンプトが表示されることがあります。この場合、次の手順を実行する必要があります。

1. ダウンロードフォルダに移動します。

2. cisco802dot1xconfiguration.mobileconfig ファイルをダブルクリックします。
3. [システム（System）] > [環境設定（Preferences）] を選択します。
4. [プロファイル（Profiles）] をクリックします。
5. プロファイルをインストールします。
6. Cisco Network Setup Assistant で表示されたプロンプトで [OK] をクリックしてインストールを続行します。

（注） MAC OSX バージョン 3.1.0.1 のサプリカント プロビジョニング ウィザード バンドルは、すべての Cisco ISE リリースに共通です。Cisco ISE 2.4 パッチ 12、Cisco ISE 2.6 パッチ 8、Cisco ISE 2.7 パッチ 3、および Cisco ISE 3.0 パッチ 2 で検証済みです。

Cisco ISE ポスチャエージェントでサポートされる Windows と MAC OSX のマルウェア対策、パッチ管理、ディスク暗号化、およびファイアウォール製品については、Cisco AnyConnect-ISE ポスチャのサポート表を参照してください。

（注）
- すべてのブラウザで、報告される Apple macOS バージョンが 10.15.7 までに制限されるようになり、ユーザープライバシーが向上しています。
- プロビジョニング中は Apple macOS 11 のエンドポイントを識別できません。これは、クライアントが Apple macOS 11 を実行している場合に、ポスチャおよび BYOD フローにおける CP ポリシーの照合で問題になります。回避策として、Apple macOS 11 のポスチャおよび BYOD フローについては、CP ポリシーのマッピングをすべての macOS にして続行します。
- 分類中は Apple macOS 11 のエンドポイントを識別できません。そのため、クライアントが Apple macOS 11 を実行している場合は、プロファイリングポリシーの照合で問題になります。

Cisco ISE リリース 3.0 以降、サポートされているすべての Apple macOS リリースでエージェントレスポスチャ機能を使用できます。Cisco ISE リリースの『Cisco ISE Administrators Guide』の「Compliance」の章のトピック「Agentless Posture」を参照してください。

Google Android

このクライアントマシンタイプは、BYOD およびポスチャワークフローで検証されています。

Cisco ISE は、特定のデバイスでの Android 実装のオープンアクセス機能により、特定の Android OS バージョンとデバイスの組み合わせをサポートしない場合があります。

Cisco ISE で検証済みの Google Android のバージョンは次のとおりです。

- Google Android 13.x
- Google Android 12.x
- Google Android 11.x
- Google Android 10.x

- Google Android 9.x
- Google Android 8.x
- Google Android 7.x

サプリカントプロビジョニングウィザード（SPW）を開始する前に、Android 9.x および 10.x デバイスでロケーションサービスが有効になっていることを確認してください。

Android は、共通名（CN）を使用しなくなりました。ホスト名は subjectAltName（SAN）拡張子に含まれている必要があります。そうでない場合、信頼の確立に失敗します。自己署名証明書を使用している場合は、ポータルの SAN ドロップダウンリストからドメイン名または IP アドレスオプションを選択して、Cisco ISE 自己署名証明書を再生成します。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します。**[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

Android 9.x を使用している場合は、Cisco ISE の ポスチャフィードを更新して、Android 9 の NSA を取得する必要があります。

Google Chromebook

このクライアントマシンタイプは、BYOD およびポスチャワークフローで検証されています。

Google Chromebook は管理対象デバイスであり、ポスチャサービスをサポートしていません。詳細については、『Cisco Identity Services Engine Administration Guide』を参照してください。

表 4 : Google Chromebook

クライアントマシンのオペレーティングシステム	Web ブラウザ	Cisco ISE
Google Chromebook	Google Chrome バージョン 49 以降	Cisco ISE 2.4 パッチ 8

Cisco ISE BYOD またはゲストポータルは、URL が正常にリダイレクトされても、Chrome オペレーティングシステム 73 で起動に失敗する場合があります。Chrome オペレーティングシステム 73 でポータルを起動するには、次の手順を実行します。

1. [サブジェクトの別名（Subject Alternative Name）] フィールドに入力することで、ISE GUI から新しい自己署名証明書を生成します。DNS と IP アドレスの両方を入力する必要があります。
2. 証明書をエクスポートし、エンドクライアント（chrome book）にコピーします。
3. [設定（Settings）] > [詳細（Advanced）] > [プライバシーとセキュリティ（Privacy And Security）] > [証明書の管理（Manage certificates）] > [当局（Authorities）] を選択します。
4. 証明書をインポートします。
5. ブラウザを終了し、ポータルのリダイレクトを試みます。

Chromebook 76 以降では、EAP の内部 CA を使用して EAP-TLS 設定を設定している場合は、SAN フィールドを含む CA 証明書チェーンを Google 管理コンソール（[デバイス管理（Device Management）] > [ネットワーク（Network]） > [証明書（Certificates）]）にアップロードします。CA チェーンがアップロードされると、Cisco ISE 証明書が信頼できるもの

と見なされるように、[Cisco ISEが SANで生成した証明書（Cisco ISE generated certificate with SAN）] フィールドは [Chromebook権限（Chromebook Authorities）] セクションの下にマッピングされます。

サードパーティの CA を使用している場合は、Google 管理コンソールに CA チェーンをインポートする必要はありません。[設定（Settings）] > [詳細（Advanced）] > [プライバシーとセキュリティ（Privacy And Security）] > [証明書の管理（Manage certificates）] > [サーバー認証局（Server Certificate authority）] を選択し、ドロップダウンリストから [シスコのデフォルトの認証局を使用（Use Any default certificate authority）] を選択します。

Linux

このクライアントマシンタイプは、BYOD およびポスチャワークフローで検証されています。

表 *5 : Linux*

クライアントマシンのオペレーティングシステム	**Cisco AnyConnect**
Red Hat Enterprise Linux（RHEL）	Cisco AnyConnect リリース 4.10 MR2[4.10.02086] 以降
RHEL 7.5 以降	
RHEL 8.1 以降	
RHEL 9.x	
SUSE Linux Enterprise Server（SLES）	
SLES 12.3 以降	
SLES 15.x	
Ubuntu	
Ubuntu 18.04	
Ubuntu 20.04	
Ubuntu 22.04	
Ubuntu 23.04	

Microsoft Windows

表 *6 : Microsoft Windows*

クライアントマシンのオペレーティングシステム	サプリカント（802.1X）	**Cisco Temporal Agent**	**AnyConnect**[4]
Microsoft Windows 11			

クライアントマシンのオペレーティングシステム	サプリカント（802.1X）	Cisco Temporal Agent	AnyConnect[4]
• Windows 22H2 • Windows 11 Enterprise • Windows 11 Pro • Windows 11 Education • Windows 11 Home	• Microsoft Windows 802.1x クライアント • AnyConnect ネットワーク アクセス マネージャ	4.10.04065 以降	4.10.04065 以降
Microsoft Windows 10			
• Windows 22H2 • Windows 21H2 • Windows 21H1 • Windows 20H2 • Windows 20H1 • Windows 19H2 • Windows 19H1 • Windows 10 Enterprise • Windows 10 Enterprise N • Windows 10 Enterprise E • Windows 10 Enterprise LTSB • Windows 10 Enterprise N LTSB • Windows 10 Pro • Windows 10 Pro N • Windows 10 Pro E • Windows 10 Education • Windows 10 Home • Windows 10 Home 中国語 • Windows 10.0 SLP（シングル言語パック）	• Microsoft Windows 10 802.1X クライアント • AnyConnect ネットワーク アクセス マネージャ	4.5 以降	4.8.01090 以降

[4] AnyConnect ネットワーク アクセス マネージャ（NAM）がインストールされている場合、NAM は Windows ネイティブサプリカントよりも 802.1X サプリカントとして優先され、BYOD フローをサポートしません。NAM を完

全に、または特定のインターフェイスで無効にする必要があります。詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。

BYOD、ゲスト、およびクライアントプロビジョニングポータルの Firefox 70 でのワイヤレスリダイレクションを有効にするには、次のようにします。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]** を選択します。
2. [SHA1暗号を許可（Allow SHA1 ciphers）] チェックボックスをオンにします。SHA1 暗号はデフォルトで無効になっています。
3. Firefox ブラウザで、**[オプション（Options）] > [プライバシー&設定（Privacy & Settings）] > [証明書の表示（View Certificates）] > [サーバー（Servers）] > [例外の追加（Add Exception）]** を選択します。
4. *https://<FQDN>:8443/* を例外として追加します。
5. [証明書の追加（Add Certificate）] をクリックし、Firefox ブラウザを更新します。

Cisco ISE リリース 3.0 以降、サポートされているすべての Microsoft リリースでエージェントレスポスチャ機能を使用できます。Cisco ISE リリースの『Cisco ISE Administrators Guide』の「Compliance」の章のトピック「Agentless Posture」を参照してください。

スポンサー、ゲスト、およびマイデバイスポータルの検証済みオペレーティングシステムとブラウザ

これらの Cisco ISE ポータルは、次のオペレーティングシステムとブラウザの組み合わせをサポートしています。これらのポータルでは、Web ブラウザで cookie が有効になっている必要があります。

表 7: 検証済みオペレーティングシステムとブラウザ

サポートされているオペレーティングシステム[5]	ブラウザのバージョン
Google Android[6] 12.x、11.x、10.x、9.x、8.x、7.x	• ネイティブブラウザ • Mozilla Firefox • Google Chrome
Apple iOS 16.x、15.x、14.x、13.x、12.x、11.x	• Safari
Apple macOS 13、12.6、12.5、11.6、10.15、10.14、10.13	• Mozilla Firefox • Safari • Google Chrome
Microsoft Windows 10	• Microsoft IE 11.x • Mozilla Firefox • Google Chrome

[5] 公式にリリースされた最新の 2 つのブラウザバージョンは、Microsoft Windows を除くすべてのオペレーティングシステムでサポートされています。サポートされている Internet Explorer のバージョンについては、表 14 を参照してください。

[6] Cisco ISE は、特定のデバイスでの Android 実装のオープンアクセス機能により、特定の Android OS バージョンとデバイスの組み合わせをサポートしない場合があります。

オンボードおよび証明書プロビジョニングのための検証済みデバイス

BYOD 機能には、Cisco Wireless LAN Controller（WLC）7.2 以降のサポートが必要です。既知の問題または警告については、『Release Notes for the Cisco Identity Services Engine』を参照してください。

（注） シスコがサポートする最新のクライアント オペレーティング システムのバージョンを入手するには、ポスチャの更新情報を確認します。手順は次のとおりです。

1. Cisco ISE GUI で [メニュー（Menu）] アイコン（☰）をクリックして選択します。**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[ポスチャ（Posture）]** > **[更新（Updates）]** を選択します。
2. [今すぐ更新（Update Now）] をクリックします。

表 *8 : BYOD* オンボードおよび証明書プロビジョニング：検証済みデバイスおよびオペレーティングシステム

デバイス	オペレーティングシステム	シングル SSID	デュアル SSID（**open > PEAP（no cert）または open > TLS**）	オンボーディング方式
Apple iDevice	Apple iOS 16.x、15.x、14.x、13.x、12.x、11.x Apple iPad OS 13.x	対応	対応[7]	Apple プロファイルの設定（ネイティブ）
Google Android	12.x、11.x、10.x、9.x、8.x、7.x	対応[8]	対応	Cisco Network Setup Assistant
Barnes & Noble Nook（Android）HD/HD+[9]	—	—	—	—
Windows	Windows 10 EAP TEAP には、Microsoft Windows 10 バージョン 2004（OS ビルド 19041.1）以降が必要です。	対応[10]	対応	2.2.1.53 以降
Windows	Mobile 8、Mobile RT、Surface 8、および Surface RT	非対応	非対応	—

デバイス	オペレーティングシステム	シングル SSID	デュアル SSID（**open > PEAP（no cert）**または **open > TLS**）	オンボーディング方式
Apple macOS	Apple macOS 13、12.6、12.5、11.6、10.15、10.14、10.13	対応	対応	2.2.1.43 以降

[7] プロビジョニング後にセキュア SSID に接続します。

[8] Android バージョン 6.0 以降を使用している場合、Cisco サプリカント プロビジョニング ウィザード（SPW）を使用してシステム作成の SSID を変更することはできません。SPW からネットワークを削除するように求められたら、このオプションを選択して [戻る（Back）] ボタンを押し、プロビジョニングフローを続行する必要があります。

[9] Barnes & Noble Nook（Android）は、Google Play ストア 2.1.0 がインストールされている場合に機能します。

[10] 接続の際にワイヤレスプロパティを設定しているとき（[セキュリティ（Security）] > [認証方式（Auth Method）] > [設定（Settings）] > [サーバー証明書の検証（Validate Server certificate）]）、有効なサーバー証明書オプションをオフにします。このオプションをオンにした場合は、正しいルート証明書が選択されていることを確認します。

検証済みのセキュリティ製品の統合（pxGrid 経由）

表 *9*：検証済みのセキュリティ製品の統合（*pxGrid* 経由）

製品	Cisco ISE 3.3	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0
Cisco Firepower Management Center	Firepower Threat Defense と Cisco Firepower Management Center 7.2.4 Firepower Threat Defense と Firepower Device Management 7.2.4	Firepower Threat Defense と Cisco Firepower Management Center 7.1 Firepower Threat Defense と Firepower Device Management 7.1 Firepower Threat Defense と Cisco Firepower Management Center 7.2 Firepower Threat Defense と Firepower Device Management 7.3 Firepower Threat Defense と Cisco Firepower Management Center 7.3	Firepower Threat Defense と Cisco Firepower Management Center 7.0.1 Firepower Threat Defense と Firepower Device Management 7.0.1 Firepower Threat Defense と Cisco Firepower Management Center 7.1 Firepower Threat Defense と Firepower Device Management 7.1 Firepower Threat Defense と Cisco Firepower Management Center 7.2 Firepower Threat Defense と Firepower Device Management 7.2	

製品	Cisco ISE 3.3	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0
				Firepower Threat Defense と Cisco Firepower Management Center 6.6.5 Firepower Threat Defense と Firepower Device Management 6.6.5 Firepower Threat Defense と Cisco Firepower Management Center 6.6.7 Firepower Threat Defense と Firepower Device Management 6.6.7 Firepower Threat Defense と Cisco Firepower Management Center 7.0 Firepower Threat Defense と Firepower Device Management 7.0 Firepower Threat Defense と Cisco Firepower Management Center 7.0.1 Firepower Threat Defense と Firepower Device Management 7.0.1 Firepower Threat Defense と Cisco Firepower Management Center 7.0.2 Firepower Threat Defense と Firepower Device Management 7.0.2 Firepower Threat Defense と Cisco Firepower Management Center 7.1

製品	Cisco ISE 3.3	Cisco ISE 3.2	Cisco ISE 3.1	Cisco ISE 3.0
				Firepower Threat Defense と Firepower Device Management 7.1 Firepower Threat Defense と Cisco Firepower Management Center 7.2 Firepower Threat Defense と Firepower Device Management 7.2
Cisco Stealthwatch Management	Cisco Stealthwatch Management 7.4.1 Cisco Stealthwatch Management 7.4.2	Cisco Stealthwatch Management 7.3.2 Cisco Stealthwatch Management 7.4.1	Cisco Stealthwatch Management 7.4.1 Cisco Stealthwatch Management 7.4.2	Cisco Stealthwatch Management 7.3.1 Cisco Stealthwatch Management 7.3.2 Cisco Stealthwatch Management 7.4
Cisco Web セキュリティアプライアンス	Cisco Web セキュリティアプライアンス 14.5.1	Cisco Web セキュリティアプライアンス 14.5.0* Cisco Web セキュリティアプライアンス 14.5.1	Cisco Web セキュリティアプライアンス 11.5.1 Cisco Web セキュリティアプライアンス 12.5.4 Cisco Web セキュリティアプライアンス 14.0.2 Cisco Web セキュリティアプライアンス 14.5.0	Cisco Web セキュリティアプライアンス 11.5.1 Cisco Web セキュリティアプライアンス 12.0.5 Cisco Web セキュリティアプライアンス 12.5.3 Cisco Web セキュリティアプライアンス 12.5.4 Cisco Web セキュリティアプライアンス 14.0.2 Cisco Web セキュリティアプライアンス 14.0.3 Cisco Web セキュリティアプライアンス 14.5.0

* Cisco Web セキュリティアプライアンス 14.5.0 の統合を成功させるには、Cisco ISE リリース 3.2 で外部 RESTful サービス（ERS）を無効状態にする必要があります。これは既知の制限であり、警告 CSCwc91516 で追跡できます。

（注） Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。 pxGrid 1.0 ベース（XMPP ベース）の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

検証済み Cisco Digital Network Architecture Center リリース

Cisco ISE は Cisco DNA Center と統合できます。Cisco DNA Center と連携するように Cisco ISE を設定する方法については、Cisco DNA Center のドキュメントを参照してください。

Cisco ISE と Cisco DNA Center との互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

検証済み Cisco Prime Infrastructure リリース

Cisco Prime Infrastructure リリース 3.6 以降を Cisco ISE 2.6 以降と統合して、Cisco ISE のモニターリングおよびレポート機能を活用できます。

検証済み Cisco Firepower Management Center リリース

Cisco Firepower Management Center リリース 6.4 以降は、Cisco ISE 2.6 以降と統合可能です。

検証済み Cisco Stealthwatch Management リリース

Cisco Stealthwatch Management リリース 6.9 以降は、Cisco ISE 2.6 以降と統合可能です。

検証済み Cisco WAN サービス管理者リリース

Cisco WAN サービス管理者 11.5.1 以降のリリースは Cisco ISE 2.7 以降のリリースと統合できます。

脅威中心型 NAC のサポート

Cisco ISE は、次のアダプタで検証されます。

- SourceFire FireAMP
- Cognitive Threat Analytics（CTA）アダプタ
- Rapid7 Nexpose
- Tenable Security Center

- Qualys（TC-NAC フローで現在サポートされているのは Qualys Enterprise Edition のみです）

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Ciscoシスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。