Cisco Identity Services Engine リリース 2.7 ネットワークコンポーネントの互換性

改訂：2023 年 9 月 12 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。

検証済みネットワーク アクセス デバイス

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。

デバイスサポートをマーキングするには、次の表記法を使用します。

- √ ：完全サポート
- X：サポート対象外
- ！：限定的なサポート、一部の機能はサポートされていません。

次の機能は各特徴でサポートされています。

表 *1*：特徴と機能

特徴	機能
AAA	802.1 x、MAB、VLAN の割り当て、dACL
プロファイリング	RADIUS CoA およびプロファイリングプローブ
BYOD	RADIUS CoA、URL リダイレクション、および SessionID
ゲスト	RADIUS CoA、ローカル Web 認証、URL リダイレクション、および SessionID
Guest URL（元の URL）	RADIUS CoA、ローカル Web 認証、URL リダイレクション、および SessionID
ポスチャ	RADIUS CoA、URL リダイレクション、および SessionID
MDM	RADIUS CoA、URL リダイレクション、および SessionID
TrustSec	SGT の分類

検証済みシスコアクセススイッチ

表 *2*: 検証済みシスコアクセススイッチ

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
IE2000 IE3000	Cisco IOS 15.2(2)E4 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)EB	√	√	√	√	*X*	√	√	√
IE4000 IE5000	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
CGS 2520	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(3)E3	√	√	√	√	*X*	√	√	√
Catalyst 1000	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	—
	Cisco IOS 15.2(7)E3	√	√	√	√	√	√	√	—
Catalyst 2960 LAN Base	Cisco IOS 15.0(2)SE11	√	√	√	√	*X*	√	√	*X*
	Cisco IOS v12.2(55)SE5[4]	√	√	√	!	*X*	!	!	*X*
Catalyst 2960-C Catalyst 3560-C	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)EX3	√	√	√	√	√	√	√	√
Catalyst 2960-L	Cisco IOS 15.2(6.1.27)E2	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.2(6)E2	√	√	√	√	√	√	√	*X*

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
CATALYST 2960-Plus Catalyst 2960-SF	Cisco IOS 15.2(2)E4	√	√	√	√	√	√	√	√
	Cisco IOS 15.0(2)SE7	√	√	√	√	√	√	√	*X*
Catalyst 2960-S	Cisco IOS 15.2(2)E6	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(2)E9	√	√	√	√	√	√	√	*X*
	Cisco IOS 15.0.2SE10a Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	*X*
	Cisco IOS 12.2.(55)SE5	√	√	√	√	√	√	√	*X*
Catalyst 2960–XR Catalyst 2960–X	Cisco IOS 15.2(2)E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2.6E1(ED) Cisco IOS 15.2(2)E9 Cisco IOS 15.2(7)E0a	√	√	√	√	√	√	√	√
	Cisco IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
Catalyst 2960-CX Catalyst 3560-CX	Cisco IOS 15.2(3)E1	√	√	√	√	√	√	√	√
	Cisco IOS 15.2(3)E	√	√	√	√	√	√	√	√

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
Catalyst 3560-G Catalyst 3750-G Cat 3750-E	Cisco IOS 15.2(2) E6 Cisco IOS 12.2(55)SE5 Cisco IOS 12.2(55)SE10 Cisco IOS 12.2(55)SE11 Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560V2	Cisco IOS 12.2(55)SE10	√	√	√	√	√	√	√	√
Catalyst 3750V2	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560-E	Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3560-X	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(2)E6 Cisco IOS 15.2(4)E9	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3650 Catalyst 3650-X	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
Catalyst 3750-E	Cisco IOS 15.2(2) E6 Cisco IOS 15.0(2)SE11	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3750-X	Cisco IOS 15.2(2) E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	Cisco IOS 12.2(55)SE5	√	√	√	√	√	√	√	√
Catalyst 3850	Cisco IOS XE 16.3.3 Cisco IOS XE 3.6.5E Cisco IOS XE 3.6.7E Cisco IOS XE 3.6.9E Cisco IOS 16.6.2 ES Cisco IOS 16.9.1 ES Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.3.5.SE	√	√	√	√	√	√	√	√
Catalyst 4500-X	Cisco IOS XE 3.6.6 E Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(6)E	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 7-E、7L-E	Cisco IOS XE 3.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 3.4.4 SG	√	√	√	√	*X*	√	√	√
Catalyst 4500 Supervisor 6-E、6L-E	Cisco IOS 15.2(2)E4	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.2(2)E	√	√	√	√	*X*	√	√	√

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
Catalyst 4500 Supervisor 8-E	Cisco IOS XE 3.6.4 Cisco IOS XE 3.6.8E Cisco IOS 15.2(6)E Cisco IOS 3.11.0 E ED	√	√	√	√	*X*	√	√	√
	Cisco IOS XE 3.3.2 XO	√	√	√	√	*X*	√	√	√
Catalyst 5760	Cisco IOS XE 3.7.4	√	√	√	√	*X*	√	√	√
	—	—	—	—	—	—	—	—	—
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6500-E （Supervisor 720）	Cisco IOS 15.1(2)SY7	√	√	√	√	*X*	√	√	√
	Cisco IOS v12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (VS-S2T-l0G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
CATALYST 6807-XL Catalyst 6880-X (VS-S2T-l0G)	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.0(1)SY1	√	√	√	√	*X*	√	√	√
Catalyst 6500-E (Supervisor 32)	Cisco IOS 12.2(33)SXJ10	√	√	√	√	*X*	√	√	√
	Cisco IOS 12.2(33)SXI6	√	√	√	√	*X*	√	√	√
Catalyst 6848ia	Cisco IOS 152-1.SY1a	√	√	√	√	*X*	√	√	√
	Cisco IOS 15.1(2) SY+	√	√	√	√	*X*	√	√	√

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
CATALYST 9200	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9200-H	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9200-L	Cisco IOS XE 16.10.1 Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.9.2	√	√	√	√	√	√	√	√
Catalyst 9300	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9300H Catalyst 9300L	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
Catalyst 9300S Catalyst 9300 24H	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√

デバイス	検証済み OS[1] 最小 OS[3]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[2]
Catalyst 9400 Catalyst 9400 LC Catalyst 9400 PoE	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.9.1 Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9500	Cisco IOS XE 16.6.2 ES Cisco IOS XE 16.8.1a Cisco IOS XE 16.6.4	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.6.2 ES	√	√	√	√	√	√	√	√
Catalyst 9500H	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
Catalyst 9600 Catalyst 9600 LC	Cisco IOS XE 16.12.1 Cisco IOS XE 17.1.1 Cisco IOS XE 17.2.1	√	√	√	√	√	√	√	√
	Cisco IOS XE 16.12.1	√	√	√	√	√	√	√	√
最新バージョン	!	√	√	!	*X*	√	!	*X*	

[1] 検証済み OS は、互換性と安定性のためにテストされたバージョンです。
[2] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。
[3] 最小 OS は、機能が導入されたバージョンです。
[4] IOS 12.x バージョンは、CSCsx97093 のため、ポスチャフローとゲストフローを完全にはサポートしていません。回避策として、Cisco ISE で URL リダイレクトを設定するときに、「coa-skip-logical-profile」に値を割り当てます。

Cisco ISE は、Cisco Catalyst スイッチの SNMP CoA をサポートしています。Cisco Catalyst スイッチの SNMP CoA では、次の機能がサポートされています。

- ポスチャ
- BYOD
- ゲスト

デバイスセンサー用にサポートされている Catalyst プラットフォームについては、「https://communities.cisco.com/docs/DOC-72932」を参照してください。

検証済みサード パーティ アクセス スイッチ

表 *3*: 検証済みサード パーティ アクセス スイッチ

デバイス	検証済み OS[5] 最小 OS[7]	AAA	プロファイリング	BYOD	ゲスト	ポスチャ	MDM	TrustSec[6]
Avaya ERS 2526T	4.4	√	!	X	X	X	X	X
	4.4	√	!	X	X	X	X	X
Brocade ICX 6610	8.0.20	√	√	√	√	√	X	X
	8.0.20	√	√	√	√	√	X	X
Extreme X440-48p	ExtremeXOS 15.5	√	X	√	√	√	X	X
	ExtremeXOS 15.5	√	X	√	√	√	X	X
HP H3C HP ProCurve	5.20.99	√	√	√	√	√	X	X
	5.20.99	√	√	√	√	√	X	X
HP ProCurve 2900	WB 15.18.0007	√	√	√	√	√	X	X
	WB 15.18.0007	√	√	√	√	√	X	X
Juniper EX3300	12.3R11.2	√	√	√	√	√	X	X
	12.3R11.2	√	√	√	√	√	X	X

[5] 検証済み OS は、互換性と安定性のためにテストされたバージョンです。
[6] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。
[7] 最小 OS は、機能が導入されたバージョンです。

サードパーティ製デバイスのサポートの詳細については、次を参照してください。 https://communities.cisco.com/docs/DOC-64547

検証済み Cisco ワイヤレス LAN コントローラ

表 *4*：検証済み *Cisco* ワイヤレス *LAN* コントローラ

デバイス	検証済み OS[8]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[9]
WLC 2100	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最小）	!	√	X	!	X	X	X	X
WLC 2504	AirOS 8.5.120.0（ED）	√	√	√	√	√	√	√	√
WLC 3504	AirOS 8.5.105.0	√	√	√	√	√	√	√	未検証
WLC 4400	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最小）	!	√	X	!	X	X	X	X
WLC 2500	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0（最小）	!	√	√	√	X	√	√	X
WLC 5508	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.3.114.x	√	√	√	√	X	√	√	√
	AireOS 8.3.140.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 7.0.116.0（最小）	!	√	X	!	X	X	X	√

デバイス	検証済み OS[8]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[9]
WLC 5520	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AireOS 8.5.1.x	√	√	√	√	√	√	√	√
	AireOS 8.6.1.x	√	√	√	√	√	√	√	√
	AirOS 8.6.101.0(ED)	√	√	√	√	√	√	√	√
	AireOS 8.1.122.0（最小）	√	√	√	√	X	√	√	√
WLC 7500	AireOS 8.0.140.0	√	√	√	√	X	√	√	X
	AireOS 8.2.121.0	√	√	√	√	X	√	√	√
	AireOS 8.2.154.x	√	√	√	√	X	√	√	√
	AireOS 8.3.102.0	√	√	√	√	X	√	√	√
	AireOS 8.4.100.0	√	√	√	√	X	√	√	√
	AirOS 8.5.120.0（ED）	√	√	√	√	√	√	√	√
	AireOS 7.2.103.0（最小）	!	√	X	X	X	X	X	X
WLC 8540	AireOS 8.1.131.0	√	√	√	√	X	√	√	X
	AireOS 8.1.122.0（最小）	√	√	√	√	X	√	√	X
Catalyst 9800-CL	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-L	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√

デバイス	検証済み OS[8]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[9]
Catalyst 9800-40	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9800-80	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
Catalyst 9300 の Catalyst 9800	IOS XE 16.12.1 IOS XE 17.1.1 IOS XE 17.2.1	√	√	√	√	√	√	√	√
	IOS XE 16.10.1	√	√	√	√	√	√	√	√
vWLC	AireOS 8.0.135.0	√	√	√	√	X	√	√	X
	AireOS 7.4.121.0（最小）	√	√	√	√	X	√	√	X
WiSM1 6500	AireOS 7.0.252.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最小）	!	√	X	!	X	X	X	X
WiSM2 6500	AireOS 8.0.135.0	√	√	√	√	X	√	√	√
	AireOS 7.2.103.0（最小）	!	√	√	√	X	√	√	√
WLC 5760	IOS XE 3.6.4	√	√	√	√	√	√	√	√
	IOS XE 3.3（最小）	√	√	√	√	X	√	√	√
ISR の WLC（ISR2 ISM、SRE700、および SRE900）	AireOS 7.0.116.0	!	√	X	!	X	X	X	X
	AireOS 7.0.116.0（最小）	!	√	X	!	X	X	X	X
最新バージョン（最小）	√	√	√	√	√	√	√	X	

デバイス	検証済み OS[8]	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec[9]
Catalyst Access Point-C9117AXI 上の Cisco 組み込みワイヤレスコントローラ	IOS XE 16.12.1	√	√	√	√	√	√	√	*X*
	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	*X*
Catalyst Access Point-C9115 上の Cisco 組み込みワイヤレスコントローラ	IOS XE 16.12.1 IOS XE 17.1.1	√	√	√	√	√	√	√	*X*
	IOS XE 16.12.1	√	√	√	√	√	√	√	*X*

[8] 検証済み OS は、互換性と安定性のためにテストされたバージョンです。
[9] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。

サポートされているオペレーティングシステムの完全なリストについては、『Cisco Wireless Solutions Software Compatibility Matrix』を参照してください。

（注）

- Android、Apple、および Windows デバイスの一部の OS バージョンでは、認証後の CWA および BYOD フローのために ISE サーバーへの追加アクセスが必要になる場合があります。このような場合、ポータルがホストされているのと同じ TCP ポートを使用して、認証後の ACL で PSN へのアクセスを許可する必要があります。
- CSCvi10594 により、IPv6 RADIUS CoA は AireOS リリース 8.1 以降では失敗します。回避策として、IPv4 RADIUS を使用するか、Cisco ワイヤレス LAN コントローラを AireOS リリース 8.0 にダウングレードできます。
- Cisco ワイヤレス LAN コントローラ（WLC）およびワイヤレス サービス モジュール（WiSM） は、ダウンロード可能な ACL（dACL）をサポートしていませんが、名前付き ACL はサポートしています。自律型 AP の導入では、エンドポイントポスチャはサポートされません。プロファイリングサービスは、WLC リリース 7.0.116.0 から開始した 802.1 X 認証 WLAN と WLC 7.2.110.0 から始まる MAB 認証 WLAN でサポートされます。FlexConnect は、以前はハイブリッド リモート エッジ アクセス ポイント（HREAP）モードと呼ばれていましたが、WLC 7.2.110.0 以降の中央認証構成の導入でサポートされています。FlexConnect サポートに関する追加情報については、該当するワイヤレス コントローラ プラットフォームのリリースノートを参照してください。

サポートされているシスコのアクセス ポイント

表 *5:* サポートされているシスコのアクセス ポイント

シスコアクセスポイント	最小 Cisco Mobility Express バージョン	AAA	プロファイリング	BYOD	ゲスト	Guest URL（元の URL）	ポスチャ	MDM	TrustSec
Cisco Aironet 1540 シリーズ	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1560 シリーズ	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815i	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815m	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 1815w	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 2800 シリーズ	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*
Cisco Aironet 3800 シリーズ	Cisco Mobility Express 8.7.106.0	√	*X*	√	√	*X*	*X*	*X*	*X*

検証済みサードパーティワイヤレス LAN コントローラ

表 *6*：検証済みサードパーティワイヤレス *LAN* コントローラ

デバイス	検証済み OS[10] 最小 OS[12]	AAA	プロファイリング	BYOD	ゲスト	ポスチャ	MDM	TrustSec[11]
Aruba 3200[13] Aruba 3200XM Aruba 650	6.4	√	√	√	√	√	X	X
	6.4	√	√	√	√	√	X	X
	6.4	√	√	√	√	√	X	X
Aruba 7000 Aruba IAP	6.4.1.0	√	√	√	√	√	X	X
	6.4.1.0	√	√	√	√	√	X	X
Motorola RFS 4000	5.5	√	√	√	√	√	X	X
	5.5	√	√	√	√	√	X	X
HP 830	35073P5	√	√	√	√	√	X	X
	35073P5	√	√	√	√	√	X	X
Ruckus ZD1200	9.9.0.0	√	√	√	√	√	X	X
	9.9.0.0	√	√	√	√	√	X	X

[10] 検証済み OS は、互換性と安定性のためにテストされたバージョンです。
[11] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。
[12] 最小 OS は、機能が導入されたバージョンです。
[13] Aruba 3200 は、ISE 2.2 パッチ 2 以降でサポートされています。

サードパーティ製デバイスのサポートの詳細については、次を参照してください。 https://communities.cisco.com/docs/DOC-64547

検証済みのシスコルータ

表 *7*：検証済みのシスコルータ

デバイス	検証済み OS 最小 OS	AAA	プロファイリング	BYOD	ゲスト	ポスチャ	MDM	TrustSec[14]
ISR 88x、89x シリーズ	IOS 15.3.2T（ED）	√	X	X	X	X	X	X
	IOS 15.2 (2) T	√	X	X	X	X	X	X

デバイス	検証済み OS 最小 OS	AAA	プロファイリング	BYOD	ゲスト	ポスチャ	MDM	TrustSec[14]
ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X	IOS XE 17.1.1 IOS XE 17.2.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
ISR 19x、29x、39x シリーズ	IOS 15.3.2T（ED）	√	!	X	!	X	X	√
	IOS 15.2 (2) T	√	!	X	!	X	X	√
CE 9331	IOS XE 17.1.1	√	X	X	X	X	X	√
	IOS XE 17.1.1	√	X	X	X	X	X	√
CGR 2010	IOS 15.3.2T（ED）	√	!	X	!	X	X	√
	IOS 15.3.2T（ED）	√	!	X	!	X	X	√
4451-XSM-X L2/L3 Ethermodule	IOS XE 3.11	√	√	√	√	√	√	√
	IOS XE 3.11	√	√	√	√	√	√	√

[14] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。

（注） CoA が正しく機能するために、Cisco ISR シリーズが SM-X-40G8M2X および SM-X-16G4M2X モジュールで動作するために必要な最低限の IOS バージョンは、IOS XE 17.4.1 です。

検証済み Cisco リモートアクセス

表 8 : 検証済み *Cisco* リモートアクセス

デバイス	検証済み OS[15] 最小 OS[17]	AAA	プロファイリング	BYOD	ゲスト	ポスチャ	MDM	TrustSec[16]
ASA 5500、ASA 5500-X（リモートアクセスのみ）	ASA 9.2.1	該当なし	該当なし	√	NA	√	X	√
	ASA 9.1.5	該当なし	該当なし	X	該当なし	X	X	X

[15] 検証済み OS は、互換性と安定性のためにテストされたバージョンです。
[16] Cisco TrustSec 機能のサポートの完全なリストについては、 Cisco TrustSec の製品情報を参照してください。
[17] 最小 OS は、機能が導入されたバージョンです。

検証済みの Cisco Meraki デバイス

表 *9 : ISE* を使用した *Cisco Meraki* アクセス制御機能

モデル	802.1X	MAB	VLAN	GPACL	適応型ポリシー	URL Redirect	CoA	プロファイリング
ワイヤレス								
MR20、MR70、MR28、MR78	√	√	√	√	*X*	√	√	*X*
MR30H、MR36、MR42/E、MR44、MR45、MR46/E、MR52、MR53E、MR56、MR74、MR76、MR86	√	√	√	√	√	√	√	*X*
在宅勤務者								
Z3/C	√	√	*X*	*X*	√ Transport MX18.1+	*X*	*X*	*X*
スイッチング								
MS120、MS125	√	√	√	*X*	*X*	*X*	√	CDP+LLDP
MS210、MS225、MS250	√	√	√	√	*X*	√	√	CDP+LLDP
MS350、MS355	√	√	√	√	*X*	√	√	CDP+LLDP
MS390	√	√	√	√	√	√	√	フルデバイスセンサー CDP/LLDP/DHCP

モデル	802.1X	MAB	VLAN	GPACL	適応型ポリシー	URL Redirect	CoA	プロファイリング
MS410、MS425、MS450（集約）	√	√	√	√	*X*	√	√	CDP+LLDP
セキュリティと Cisco SD-WAN								
MX64/W、MX67/C/W、MX68CW/W、MX75、MX84、MX85、MX95、MX100、MX105、MX250、MX450	√ 802.1X または MAB	√ 802.1X または MAB	*X*	*X*	√ Transport MX18.1+	*X*	*X*	*X*

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。

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 *10*：検証済み外部 *ID* ソース

外部 ID ソース	バージョン
Active Directory 1819	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 20	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 21	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
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

外部 ID ソース	バージョン
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	
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

[18] CISCO ISE OCSP 機能は Microsoft Windows Active Directory 2008 以降でのみ使用できます。

[19] 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：

`<DC FQDN> の作成エラー：許可される DC の数が最大数 200 を超えています`

[20] 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。

[21] 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。

検証済み MDM サーバー

検証済みのモバイルデバイス管理（MDM）サーバーには、次のベンダーの製品が含まれています。

- Absolute
- VMware AirWatch
- Citrix XenMobile
- Globo

- Good Technology
- IBM MaaS360
- JAMF ソフトウェア
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe
- Microsoft Intune - モバイル デバイス用
- Microsoft SCCM -デスクトップ デバイス用

管理者ポータルでサポートされているブラウザ

- Mozilla Firefox 96 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 97 以前のバージョン （バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

サポート対象ハードウェア

Cisco ISE リリース 2.7 は、次のプラットフォームにインストールできます。

表 *11* : 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-3515-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* アプライアンスハードウェアの設置ガイド』を参照してください。
Cisco SNS-3595-K9（大規模）	
Cisco SNS-3615-K9（小規模）	
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	

インストール後、上記の表に記載されているプラットフォームで、管理、モニターリング、pxGrid などの特定のコンポーネントペルソナを使用して Cisco ISE を設定できます。これらのペルソナに加えて、Cisco ISE では、プロファイリ

ングサービス、セッションサービス、脅威中心型 NAC サービス、TrustSec 用の SXP サービス、TACACS+ デバイス管理サービス、およびパッシブ ID サービスなど、ポリシーサービス内に他のタイプのペルソナが含まれています。

注意

- Cisco ISE 3.1 以降のリリースは、Cisco Secured Network Server（SNS）3515 アプライアンスをサポートしていません。
- Cisco SNS 3400 シリーズ アプライアンスは、Cisco ISE リリース 2.4 以降ではサポートされていません。
- 16 GB 未満のメモリの割り当ては、VM アプライアンスの設定ではサポートされていません。Cisco ISE の動作に問題が発生した場合、すべてのユーザーは、Cisco Technical Assistance Center に連絡する前に割り当てメモリを 16 GB 以上に変更する必要があります。
- レガシー アクセス コントロール サーバー（ACS）およびネットワーク アクセス コントロール（NAC）アプライアンス（Cisco ISE 3300 シリーズを含む）は、Cisco ISE リリース 2.0 以降ではサポートされていません。

検証済み仮想環境

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。

- VMware ESXi 5.x（5.1 U2 以降は RHEL 7 をサポート）、6.x、7.x

（注） ESXi 5.x サーバーに Cisco ISE をインストールまたはアップグレードしている場合に、ゲスト OS として RHEL 7 をサポートするには、VMware のハードウェアバージョンを 9 以降にアップデートしてください。RHEL 7 は、VMware のハードウェアバージョン 9 以降でサポートされます。

- QEMU 1.5.3-160 上の KVM
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V

注意 Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。ISE ノードを起動するには、再起動が必要です。

検証済み Cisco Digital Network Architecture Center リリース

表 *12* : 検証済み *Cisco Digital Network Architecture Center* リリース

検証済み Cisco DNA Center バージョン	検証済み Cisco ISE リリース
1.2.12.0	Cisco ISE 2.7
1.3.0.0	Cisco ISE 2.7
1.3.0.6	Cisco ISE 3.0
1.3.1.0	Cisco ISE 2.4 パッチ 9、パッチ 11 Cisco ISE 2.6 パッチ 2 Cisco ISE 2.7
1.3.1.4	Cisco ISE 2.4 パッチ 12 Cisco ISE 2.6 パッチ 6 Cisco ISE 2.7 パッチ 2 Cisco ISE 3.0
1.3.2.0	Cisco ISE 2.4 パッチ 10、パッチ 11 Cisco ISE 2.7
1.3.3.0	Cisco ISE 2.7 パッチ 1 Cisco ISE 3.0
1.3.3.4	Cisco ISE 2.6 パッチ 6
1.3.3.5	Cisco ISE 2.4 パッチ 13 Cisco ISE 2.7 パッチ 2
2.1.1.0	Cisco ISE 2.4 パッチ 12 Cisco ISE 2.6 パッチ 6、パッチ 7 Cisco ISE 2.7 パッチ 1、パッチ 2 Cisco ISE 3.0
2.1.1.1	Cisco ISE 3.0
2.1.2.0	Cisco ISE 2.4 パッチ 12、パッチ 13 Cisco ISE 2.6 パッチ 6、パッチ 8 Cisco ISE 2.7 パッチ 1、パッチ 3 Cisco ISE 3.0

検証済み Cisco DNA Center バージョン	検証済み Cisco ISE リリース
2.1.2.4	Cisco ISE 3.0 パッチ 1
2.1.2.5	Cisco ISE 3.0 パッチ 1、パッチ 2
2.1.2.6	Cisco ISE 2.4 パッチ 14 Cisco ISE 2.7 パッチ 4
2.2.1.0	Cisco ISE 2.4 パッチ 13、パッチ 14 Cisco ISE 2.6 パッチ 7、パッチ 8、パッチ 9 Cisco ISE 2.7 パッチ 2 Cisco ISE 3.0 パッチ 1、パッチ 3
2.2.2.0	Cisco ISE 2.4 パッチ 14 Cisco ISE 2.6 パッチ 8、パッチ 9 Cisco ISE 2.7 パッチ 2、パッチ 3、パッチ 4 Cisco ISE 3.0 パッチ 1

Cisco Digital Network Architecture Center（Cisco DNA Center）との Cisco ISE の互換性の詳細については、「CISCO SD-Access Compatibility Matrix」を参照してください。

検証済み Cisco Mobility Services Engine リリース

Cisco ISE は Cisco Mobility Services Engine（MSE）リリース 8.0.110.0 と統合して、ロケーションサービス（コンテキスト認識サービスとも呼ばれます）を提供します。このサービスでは、ワイヤレスデバイスの場所を追跡できます。

Cisco ISE を Cisco MSE と統合する方法については、次を参照してください。

- Mobility Services Engine（MSE）および Identity Services Engine（ISE）2.0 のロケーションベースの認証
- 『*Cisco Firepower Threat Defense Virtual for MicrosoftAzure Quick Start Guide*』

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 Stealthwatch リリース

Cisco ISE 2.7 は、 Cisco Stealthwatch リリース 7.0 で検証されています。

検証済み Cisco WAN サービス管理者リリース

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）

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
- Microsoft Windows

Cisco ISE リリース 2.3 以降では、Cisco AnyConnect および Cisco Temporal Agent のみがサポートされています。

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。

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 12.x
- Google Android 11.x
- Google Android 10.x
- Google Android 9.x
- Google Android 8.x
- Google Android 7.x

Cisco ISEで検証済みのAndroidデバイスは次のとおりです。Cisco ISEでBYODフローがサポートされるデバイスのリストについては、「」のセクションを参照してください。

表 *13*：検証済み *Android* デバイス

デバイス モデル	**Android バージョン**
Google Pixel 3	10
OnePlus 6	10
Samsung S9	9
Google Nexus 6P	8.1
Huawei Mate Pro 10	8

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（[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] の下）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。

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。

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

Cisco ISE で検証済みの iPhone/iPad デバイスは次のとおりです。Cisco ISE で BYOD フローがサポートされるデバイスのリストについては、「」のセクションを参照してください。

表 *14 :* 検証済み *iPhone/iPad* デバイス

デバイス モデル	iOS バージョン
iPhone X	iOS 13
iPhone 8	iOS 12.3
iPhone 7	iOS 13.2
iPhone 6	iOS 12.6
iPhone 5s	iOS 12、iOS 10.3
iPad	iPad OS 13.1

（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 *15 : 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	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。

Microsoft Windows

表 16 : 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[22]
Microsoft Windows 11			
• 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			

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[22]
• 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

[22] 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。

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 *17 : 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。

その他のオペレーティングシステム

表 *18 :* その他のオペレーティングシステム

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 [23]	サプリカント（802.1X）
Red Hat Enterprise Linux（RHEL）	• Google Chrome • Mozilla Firefox	広範囲にわたってテストされていない [24]

[23] Google Chrome は 32 ビット Linux システムをサポートしていません。

[24] 802.1X のサポートはシスコでは広範囲にわたってテストされていませんが、IEEE 802.1X 標準に準拠している限り、どの 802.1X サプリカントもサポートされます。

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 *19*：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[25]	ブラウザのバージョン
Google Android[26]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

[25] 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。

[26] 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（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [更新（Updates）] を確認し、[今すぐ更新（Update Now）] をクリックします。

表 *20 : 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[27]	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[28]	対応	Cisco Network Setup Assistant
Barnes & Noble Nook（Android）HD/HD+[29]	—	—	—	—
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[30]	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	—
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

[27] プロビジョニング後にセキュア SSID に接続します。

[28] 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。

[29] 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。

[30] 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。

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

検証済み OpenSSL のバージョン

Cisco ISE は、OpenSSL 1.0.2.x（CiscoSSL 6.0）を使用して検証されます。

サポートされる暗号スイート

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

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

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。このウィンドウを表示するには、[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）] を選択します。	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 Cisco ISE 2.3 以上では、[TLS 1.1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 1.1 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 1.1 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウ（[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）]）で [TLS 1.1を許可（Allow TLS 1.1）] チェック ボックスをオンにします。	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	×	SHA-1 が許可されている場合
DHE-RSA-AES128-SHA	×	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	×	3DES/DSS および SHA-1 が有効になっている場合
DHE-DSS-AES128-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
EDH-DSS-DES-CBC3-SHA	×	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	×
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	×
EAP-FAST 匿名プロビジョニングのみの場合： ADH-AES-128-SHA	はい	いいえ
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

Cisco ISE と相互運用するための CA の要件

Cisco ISE で CA サーバーを使用しているときは、次の要件を満たしている必要があります。

- キー サイズは 1024、2048、またはそれ以上にする必要があります。CA サーバーでは、キー サイズは証明書テンプレートを使用して定義されます。サプリカント プロファイルを使用して Cisco ISE でキー サイズを定義できます。
- キーの使用法では、拡張された署名と暗号化を許可する必要があります。
- SCEP プロトコルを介して GetCACapabilities を使用する場合は、暗号化アルゴリズムと要求ハッシュがサポートされている必要があります。RSA と SHA1 を使用することをお勧めします。
- Online Certificate Status Protocol（OCSP）がサポートされます。これは BYOD では直接使用されませんが、OCSP サーバーとして機能できる CA は証明書失効に使用できます。

（注） Enterprise Java Beans 認証局（EJBCA）は、プロキシ SCEP の Cisco ISE ではサポートされていません。EJBCA は、PEAP、EAP-TLS などの標準 EAP 認証について Cisco ISE でサポートされます。

- エンタープライズ PKI を使用して Apple iOS デバイスの証明書を発行する場合は、SCEP テンプレートでキーの使用法を設定し、[キーの暗号化（Key Encipherment）] オプションを有効にする必要があります。

Microsoft CA を使用する場合は、証明書テンプレートのキー使用法拡張機能を編集します。[暗号化（Encryption）] 領域で、[キーの暗号化でのみキーの交換を許可する（Allow key exchange only with key encryption (key encipherment)）] オプションボタンをクリックし、[ユーザーデータの暗号化を許可する（Allow encryption of user data）] チェックボックスもオンにします。

- Cisco ISE は、EAP-TLS 認証の信頼できる証明書およびエンドポイント証明書に対して、RSASSA-PSS アルゴリズムの使用をサポートしています。証明書を表示すると、署名アルゴリズムは、アルゴリズム名ではなく、1.2.840.113549.1.1.10 としてリストされます。

（注） BYOD フローに Cisco ISE 内部の CA を使用する場合、管理証明書は（外部 CA で）RSASSA-PSS アルゴリズムを使用して署名できません。Cisco ISE 内部の CA は、このアルゴリズムを使用して署名された管理証明書を検証できず、要求が失敗します。

証明書ベースの認証のためのクライアント証明書の要件

Cisco ISE による証明書ベースの認証では、クライアント証明書が次の要件を満たしている必要があります。

表 *21* : クライアント *RSA* および *ECC* の証明書要件

RSA		
サポートされているキーサイズ	1024、2048、および 4096 ビット	
サポートされているセキュアハッシュアルゴリズム（SHA）	SHA-1 および SHA-2（SHA-256 を含む）	
ECC [3132]		
サポートされる曲線タイプ	P-192、P-256、P-384、および P-521	
サポートされているセキュアハッシュアルゴリズム（SHA）	SHA-256	
クライアントマシンのオペレーティングシステムとサポートされている曲線タイプ		
Windows	8 以降	P-256、P-384、P-521
Android	4.4 以降 （注） Android 6.0 は、ECC 証明書をサポートするために 2016 年 5 月のパッチが必要です。	すべての曲線タイプ（P-192 曲線タイプをサポートしていない Androidv6.0 を除く）。

[31] Windows 7 と Apple iOS は、EAP-TLS 認証用の ECC をネイティブでサポートしていません。
[32] Cisco ISE のこのリリースでは、Mac OS X デバイスでの ECC 証明書の使用はサポートされていません。

【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。