Cisco Secure Client 機能、ライセンス、OS、リリース 5.x

最終更新：2025 年 7 月 23 日

Cisco Secure Client（AnyConnect を含む）の機能、ライセンス、リリース 5.x

このマニュアルでは、Cisco Secure Client リリース 5.1 の機能、ライセンス要件、および Secure Client（AnyConnect を含む）がサポートするエンドポイント オペレーティング システムについて説明します。サポートされている暗号アルゴリズムとユーザー補助に関する推奨事項も含まれています。

サポートされるオペレーティング システム

Cisco Secure Client 5.1 は、次のオペレーティングシステムをサポートします。

Windows

- Windows 11（64 ビット）
- ARM64 ベースの PC 用に Microsoft 社がサポートしているバージョンの Windows 11（VPN クライアント、DART、Cisco Secure Firewall ポスチャ、Network Visibility モジュール、Cisco Umbrella モジュール、ISE ポスチャ、Cisco Zero Trust Access モジュール）
- Windows 10 x86（32 ビット）および x64（64 ビット）

macOS（64 ビットのみ）

- macOS 15 Sequoia
- macOS 14 Sonoma
- macOS 13 Ventura

Linux

- Red Hat：9.x および 8.x（8.1 以降のみをサポートする ISE ポスチャモジュールを除く）
- Ubuntu：24.04 および 22.04
- SUSE（SLES 15（x86_64））
    - VPN：制限付きのサポート。ISE ポスチャのインストールにのみ使用されます。

- Cisco Secure Firewall ポスチャまたは Network Visibility Module ではサポートされていません。
- ISE ポスチャ：12.3（以降のバージョン）および 15.0（以降のバージョン）

OS の要件およびサポートノートについては、『Release Notes for Cisco Secure Client』を参照してください。ライセンス利用規約、および各種ライセンスの発注可能状況および具体的な契約条件の内訳については、「オファー説明書および補足条項」を参照してください。

Cisco Secure Client モジュールおよび機能に適用されるライセンス情報とオペレーティングシステムの制限については、下記の機能マトリクスを参照してください。

サポートされている暗号アルゴリズム

次の表に、Cisco Secure Client でサポートされている暗号アルゴリズムを示します。暗号アルゴリズムと暗号スイートは、優先度の高いものから順に示されています。この優先度は、すべてのシスコ製品が準拠する必要があるシスコの製品セキュリティベースラインによって決定されます。PSB の要件は随時変更されるため、以降のバージョンの Secure Client でサポートされる暗号アルゴリズムはそれに応じて変更されます。

TLS 1.3、1.2、および DTLS 1.2 暗号スイート（VPN）

標準 RFC 命名規則	OpenSSL 命名規則
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHA-RSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256

標準 RFC 命名規則	OpenSSL 命名規則
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

TLS 1.2 暗号スイート（ネットワーク アクセス マネージャ）

標準 RFC 命名規則	OpenSSL 命名規則
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA

DTLS 1.0 暗号スイート（VPN）

標準 RFC 命名規則	OpenSSL 命名規則
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

IKEv2/IPsecアルゴリズム

暗号化

- ENCR_AES_GCM_256
- ENCR_AES_GCM_192
- ENCR_AES_GCM_128
- ENCR_AES_CBC_256
- ENCR_AES_CBC_192
- ENCR_AES_CBC_128

疑似ランダム関数

- PRF_HMAC_SHA2_256
- PRF_HMAC_SHA2_384
- PRF_HMAC_SHA2_512
- PRF_HMAC_SHA1

Diffie-Hellman グループ

- DH_GROUP_256_ECP：グループ 19
- DH_GROUP_384_ECP：グループ 20
- DH_GROUP_521_ECP：グループ 21
- DH_GROUP_3072_MODP：グループ 15

- DH_GROUP_4096_MODP：グループ 16

整合性

- AUTH_HMAC_SHA2_256_128
- AUTH_HMAC_SHA2_384_192
- AUTH_HMAC_SHA1_96
- AUTH_HMAC_SHA2_512_256

ライセンス オプション

Cisco Secure Client 5.1 を使用するには、Premier または Advantage ライセンスを購入する必要があります。必要なライセンスは、使用する予定の Secure Client の機能と、サポートするセッションの数によって異なります。これらのユーザーベースのライセンスには、サポートへのアクセス、一般的な BYOD トレンドと調整ができるソフトウェア アップデートが含まれます。

Secure Client 5.1 ライセンスは Cisco Secure Firewall 適応型セキュリティアプライアンス（ASA）、サービス統合型ルータ（ISR）、クラウドサービスルータ（CSR）、および Aggregated Services Router（ASR）と、Identity Services Engine（ISE）などのその他の非 VPN ヘッドエンドで使用されます。ヘッドエンドに関係なく一貫したモデルが使用されるため、ヘッドエンドの移行が発生した場合も影響はありません。

導入には次の Cisco Secure ライセンスが 1 つまたは複数必要になる場合があります。

ライセンス	説明
Advantage	PC やモバイルプラットフォーム（Secure Client および標準ベースの IPsec IKEv2 ソフトウェアクライアント）の VPN 機能、FIPS、基本的なエンドポイント コンテキスト コレクション、および 802.1x Windows サプリカントなどの基本的な Secure Client 機能をサポートします。
Premier	Network Visibility モジュール、クライアントレス VPN、VPN ポスチャエージェント、統一されたポスチャエージェント、次世代暗号化/スイート B、SAML、すべての Plus サービスと Flex ライセンスなどの高度な機能に加えて、すべての基本的な Secure Client Advantage 機能もサポートします。

ライセンス	説明
VPN のみ（永久）	PCおよびモバイルプラットフォームのためのVPN機能、Secure Firewall ASA でのクライアントレス（ブラウザベース）VPN ターミネーション、ASA と連携した VPN 専用コンプライアンスおよびポスチャエージェント、FIPS コンプライアンス、ならびにSecure Clientおよびサードパーティ IKEv2 VPN クライアントでの次世代暗号化（スイート B）をサポートします。VPN のみのライセンスは、Secure Client をリモートアクセス VPN サービス専用に使用したい場合で、総ユーザー数が多い、または予測できない環境に最も適しています。Secure Client のその他の機能またはサービス（Cisco Umbrella Roaming、ISE ポスチャ、Network Visibility Module、または Network Access Managerなど）は、このライセンスでは使用できません。

Advantage および Premier ライセンス

Cisco Commerce Workspace Web サイトから、サービス階層（Advantage または Premier）と期間（1、3、または 5 年）を選択します。必要なライセンスの数は、Secure Client を使用する一意のユーザーまたは承認ユーザーの数に基づきます。Secure Client のライセンスは同時接続に基づいて付与されるものではありません。同じ環境に Advantage ライセンスと Premier ライセンスを混在させることができ、ユーザーごとに必要なライセンスの数は 1 つのみです。

Cisco Secure 5.1 のライセンスをお持ちのお客様は、以前のリリースの AnyConnect もご利用になれます。

機能マトリックス

Cisco Secure 5.1 のモジュールおよび機能と、最小リリース要件、ライセンス要件、およびサポートされるオペレーティングシステムを次の項に示します。

Cisco Secure Client の展開と構成

特長	ASA/ASDM の最小リリース	必要なライセンス	Windows	macOS	Linux
遅延アップグレード	ASA 9.16 ASDM 7.16	Advantage	○	○	○
Windows サービスのロックダウン	ASA 9.16 ASDM 7.16	Advantage	○	×	×
ポリシー、ソフトウェア、プロファイルロックの更新	ASA 9.16 ASDM 7.16	Advantage	○	○	○

特長	ASA/ASDM の最小リリース	必要なライセンス	Windows	macOS	Linux
自動更新	ASA 9.16 ASDM 7.16	Advantage	○	○	○
事前展開	ASA 9.16 ASDM 7.16	Advantage	○	○	○
クライアントプロファイルの自動更新	ASA 9.16 ASDM 7.16	Advantage	○	○	○
Cisco Secure Client プロファイルエディタ	ASA 9.16 ASDM 7.16	Advantage	○	○	○
ユーザ制御可能な機能	ASA 9.16 ASDM 7.16	Advantage	○	○	○*

* VPN 接続で Secure Client を最小化する機能、または信頼できないサーバーへの接続をブロックする機能

AnyConnect VPN のコア機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
SSL（TLS および DTLS）（アプライアンスごとの VPN を含む）	ASA 9.16 ASDM 7.16	Advantage	○	○	○
SNI（TLS および DTLS）	適用対象外	Advantage	○	○	○
TLS 圧縮	ASA 9.16 ASDM 7.16	Advantage	○	○	○
DTLS の TLS へのフォールバック	ASA 9.16 ASDM 7.16	Advantage	○	○	○
IPsec/IKEv2	ASA 9.16 ASDM 7.16	Advantage	○	○	○
スプリット トンネリング	ASA 9.16 ASDM 7.16	Advantage	○	○	○
ダイナミック スプリット トンネリング	ASA 9.16	Advantage、Premier、または VPN のみ	○	○	×

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
強化されたダイナミック スプリット トンネリング	ASA 9.16	Advantage	○	○	×
トンネルからの動的除外とトンネルへの動的包含の両方	ASA 9.16	Advantage	○	○	×
スプリット DNS	ASA 9.16 ASDM 7.16	Advantage	○	○	×
ブラウザ プロキシの無視	ASA 9.16 ASDM 7.16	Advantage	○	○	×
Proxy Auto Config（PAC）ファイルの生成	ASA 9.16 ASDM 7.16	Advantage	○	×	×
Internet Explorer の [接続（Connections）] タブのロック	ASA 9.16 ASDM 7.16	Advantage	○	×	×
最適ゲートウェイ選択	ASA 9.16 ASDM 7.16	Advantage	○	○	×
Global Site Selector（GSS）の互換性	ASA 9.16 ASDM 7.16	Advantage	○	○	○
ローカル LAN へのアクセス	ASA 9.16 ASDM 7.16	Advantage	○	○	○
同期化のためのクライアント ファイアウォール ルールによるテザー デバイスのアクセス	ASA 9.16 ASDM 7.16	Advantage	○	○	○
クライアント ファイアウォールルールによるローカル プリンタのアクセス	ASA 9.16 ASDM 7.16	Advantage	○	○	○
IPv6	ASA 9.16 ASDM 7.16	Advantage	○	○	×
さらなる IPv6 の実装	ASA 9.16 ASDM 7.16	Advantage	○	○	○

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
証明書のピン留め	依存関係なし	Advantage	○	○	○
管理 VPN トンネル	ASA 9.16 ASDM 7.16	Premier	○	○	×

接続機能および切断機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
高速ユーザースイッチング	適用対象外	適用対象外	○	×	×
クライアントレス接続と Secure Client 接続の同時使用	ASA 9.16 ASDM 7.16	Premier	○	○	○
Start Before Logon（SBL）	ASA 9.16 ASDM 7.16	Advantage	○	×	×
接続時および切断時のスクリプト実行	ASA 9.16 ASDM 7.16	Advantage	○	○	○
接続時の最小化	ASA 9.16 ASDM 7.16	Advantage	○	○	○
起動時の自動接続	ASA 9.16 ASDM 7.16	Advantage	○	○	○
自動再接続（システムの一時停止で切断、システムの再開で再接続）	ASA 9.16 ASDM 7.16	Advantage	○	○	×

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
リモート ユーザ VPN 確立（許可または拒否）	ASA 9.16 ASDM 7.16	Advantage	○	×	×
ログオン実行（別のユーザがログインすると、VPN セッションを終了）	ASA 9.16 ASDM 7.16	Advantage	○	×	×
VPN セッションの維持（ユーザがログオフし、その後このユーザまたは別のユーザがログインした場合）	ASA 9.16 ASDM 7.16	Advantage	○	×	×
Trusted Network Detection（TND）	ASA 9.16 ASDM 7.16	Advantage	○	○	○
常時オン（ネットワークにアクセスするには、VPN を接続する必要がある）	ASA 9.16 ASDM 7.16	Advantage	○	○	×
DAP による常時オン除外	ASA 9.16 ASDM 7.16	Advantage	○	○	×

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
接続障害ポリシー（VPN 接続に障害が発生した場合、インターネット アクセスを許可または不許可）	ASA 9.16 ASDM 7.16	Advantage	○	○	×
キャプティブ ポータルの検出	ASA 9.16 ASDM 7.16	Advantage	○	○	○
キャプティブ ポータルの修復	ASA 9.16 ASDM 7.16	Advantage	○	○	×
強化されたキャプティブ ポータル修復	依存関係なし	Advantage	○	○	×
デュアルホーム検出	依存関係なし	適用対象外	○	○	○

認証および暗号化機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
証明書のみの認証	ASA 9.16 ASDM 7.16	Advantage	○	○	○
RSA SecurID/SoftID の統合	依存関係なし	Advantage	○	×	×
スマートカードのサポート	依存関係なし	Advantage	○	○	×
SCEP（マシン ID を使用する場合はポスチャ モジュールが必要）	依存関係なし	Advantage	○	○	×

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
証明書の一覧表示および選択	依存関係なし	Advantage	○	×	×
FIPS	依存関係なし	Advantage	○	○	○
IPsec IKEv2 の SHA-2（デジタル署名、整合性、および PRF）	ASA 9.16 ASDM 7.16	Advantage	○	○	○
強力な暗号化（AES-256 およびトリプル DES 168）	依存関係なし	Advantage	○	○	○
NSA Suite-B（IPsec のみ）	ASA 9.16 ASDM 7.16	Premier	○	○	○
CRL チェックの有効化	依存関係なし	Premier	○	×	×
SAML 2.0 SSO	ASA 9.16 ASDM 7.16	Premier または VPN のみ	○	○	○
強化された SAML 2.0	ASA 9.16	Premier または VPN のみ	○	○	○
拡張 Web 認証用の外部ブラウザ SAML パッケージ	ASA 9.16 ASDM 7.16	Premier または VPN のみ	○	○	○
複数の証明書の認証	ASA 9.16 ASDM 7.16	Advantage、Premier、または VPN のみ	○	○	○

インターフェイス

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
GUI	ASDM 7.16	Advantage	○	○	○
コマンド ライン	ASA 9.16	適用対象外	○	○	○
API	依存関係なし	適用対象外	○	○	○

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
Microsoft コンポーネント オブジェクト モジュール（COM）	依存関係なし	適用対象外	○	×	×
ユーザ メッセージのローカリゼーション	依存関係なし	適用対象外	○	○	○
カスタム MSI トランスフォーム	依存関係なし	適用対象外	○	×	×
ユーザー定義のリソースファイル	依存関係なし	適用対象外	○	○	×
クライアント ヘルプ	ASA 9.16 ASDM 7.16	適用対象外	○	○	×

Cisco Secure Firewall ポスチャ（旧称 HostScan）とポスチャアセスメント

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
エンドポイント アセスメント	ASA 9.16	Premier	○	○	○
エンドポイント修復	ASDM 7.16	Premier	○	○	○
検疫	依存関係なし	Premier	○	○	○
検疫のステータスおよび中止メッセージ	ASA 9.16 ASDM 7.16	Premier	○	○	○
Cisco Secure Firewall ポスチャパッケージの更新	ASA 9.16 ASDM 7.16	Premier	○	○	○
ホスト エミュレーション検出	依存関係なし	Premier	○	×	×
OPSWAT v4	ASA 9.16 ASDM 7.16	Premier	○	○	○
ディスク暗号化	ASA 9.17(1) ASDM 7.17.1	適用対象外	○	○	○

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
AutoDART	依存関係なし	適用対象外	○	○	○

ISE ポスチャ

特長	Secure Client の最小リリース	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
ISE ポスチャ CLI	5.0.01xxx	依存関係なし	依存関係なし	適用対象外	○	×	×
ポスチャ状態の同期	5.0	依存関係なし	3.1	適用対象外	○	○	○
認可変更（CoA）	5.0	ASA 9.16 ASDM 7.16	2.0	Advantage	○	○	○
ISE ポスチャ プロファイル エディタ	5.0	ASA 9.16 ASDM 7.16	依存関係なし	Premier	○	○	○
AC Identity Extensions（ACIDex）	5.0	依存関係なし	2.0	Advantage	○	○	○
ISE ポスチャ モジュール	5.0	依存関係なし	2.0	Premier	○	○	○
USB 大容量ストレージ デバイス（v4 のみ）の検出	5.0	依存関係なし	2.1	Premier	○	×	×
OPSWAT v4	5.0	依存関係なし	2.1	Premier	○	○	×
ポスチャのステルスエージェント	5.0	依存関係なし	2.2	Premier	○	○	×
エンドポイントの継続的モニタリング	5.0	依存関係なし	2.2	Premier	○	○	×

特長	Secure Client の最小リリース	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
次世代のプロビジョニングおよびディスカバリ	5.0	依存関係なし	2.2	Premier	○	○	×
アプリケーションの強制終了およびアンインストール機能	5.0	依存関係なし	2.2	Premier	○	○	×
Cisco Temporal Agent	5.0	依存関係なし	2.3	ISE Premier	○	○	×
強化された SCCM アプローチ	5.0	依存関係なし	2.3	Premier：Secure Client および ISE	○	×	×
オプションモードのポスチャ ポリシー拡張機能	5.0	依存関係なし	2.3	Premier：Secure Client および ISE	○	○	×
プロファイルエディタでの定期的なプローブの間隔	5.0	依存関係なし	2.3	Premier：Secure Client および ISE	○	○	×
ハードウェアインベントリの可視性	5.0	依存関係なし	2.3	Premier：Secure Client および ISE	○	○	×
非準拠デバイスの猶予期間	5.0	依存関係なし	2.4	Premier：Secure Client および ISE	○	○	×
ポスチャの再スキャン	5.0	依存関係なし	2.4	Premier：Secure Client および ISE	○	○	×

特長	Secure Client の最小リリース	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
Secure Client のステルスモード通知	5.0	依存関係なし	2.4	Premier：Secure Client および ISE	○	○	×
UAC プロンプトの無効化	5.0	依存関係なし	2.4	Premier：Secure Client および ISE	○	×	×
猶予期間の拡張	5.0	依存関係なし	2.6	Premier：Secure Client および ISE	○	○	×
カスタム通知制御と修復ウィンドウの revamp	5.0	依存関係なし	2.6	Premier：Secure Client および ISE	○	○	×
エンドツーエンドのエージェントレス ポスチャ フロー	5.0	依存関係なし	3.0	Premier：Secure Client および ISE	○	○	×

Network Access Manager

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
コア	ASA 9.16 ASDM 7.16	Advantage	○	×	×
IEEE 802.3 の有線サポート	依存関係なし	適用対象外	○	×	×
IEEE 802.11 の無線サポート	依存関係なし	適用対象外	○	×	×
事前ログオンおよびシングル サインオン認証	依存関係なし	適用対象外	○	×	×
IEEE 802.1X	依存関係なし	適用対象外	○	×	×

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
IEEE 802.1AE MACsec	依存関係なし	適用対象外	○	×	×
EAP メソッド	依存関係なし	適用対象外	○	×	×
FIPS 140-2 レベル 1	依存関係なし	適用対象外	○	×	×
モバイルブロードバンドのサポート	ASA 9.16 ASDM 7.16	適用対象外	○	×	×
IPv6	ASDM 9.0	適用対象外	○	×	×
NGE および NSA Suite-B	ASDM 7.16	適用対象外	○	×	×
VPN 接続の TLS 1.2*	依存関係なし	適用対象外	○	×	×
WPA3 Enhanced Open（OWE）および WPA3 Personal（SAE）のサポート	依存関係なし	適用対象外	○	×	×

* RADIUS サーバーとして ISE を使用する場合は、次のガイドラインに注意してください。

ISE は、リリース 2.0 で TLS 1.2 のサポートを開始しています。TLS 1.2 を使用した Cisco Secure Client と 2.0 より以前の ISE リリースを使用する場合、Network Access Manager と ISE は TLS 1.0 とネゴシエートします。そのため、RADIUS サーバーに Network Access Manager および ISE 2.0（以降）搭載の EAP-FAST を使用する場合、ISE も適切なリリースにアップグレードする必要があります。

非互換性に関する警告：2.0 移行の ISE を使用している場合は、続行する前にかならずこちらをお読みください。

ISE RADIUS はリリース 2.0 以降 TLS 1.2 をサポートしてきましたが、CSCvm03681 により追跡される TLS 1.2 を使用した EAP-FAST の ISE 導入に不具合が見つかりました。この不具合は、ISE の 2.4p5 リリースで修正されました。

上記のリリースより以前の TLS 1.2 をサポートする ISE の EAP-FAST を使用して、NAM が認証に使用される場合、認証は失敗し、エンドポイントはネットワークにアクセスできません。

AMP イネーブラ

機能	最低限の ASA/ASDM リリース	最低限の ISE リリース	ライセンス	Windows	macOS	Linux
AMP イネーブラ	ASDM 7.16 ASA 9.16	ISE 1.4	Advantage	適用対象外	○	適用対象外

ネットワーク可視性モジュール

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
ネットワーク可視性モジュール	ASDM 7.16 ASA 9.16	Premier	○	○	○
データ送信レートへの調整	ASDM 7.16 ASA 9.16	Premier	○	○	○
NVM タイマーのカスタマイズ	ASDM 7.16 ASA 9.16	Premier	○	○	○
データ収集のブロードキャストおよびマルチキャスト オプション	ASDM 7.16 ASA 9.16	Premier	○	○	○
匿名プロファイルの作成	ASDM 7.16 ASA 9.16	Premier	○	○	○
より広範囲なデータ収集とハッシュによる匿名化	ASDM 7.16 ASA 9.16	Premier	○	○	○
コンテナとしての Java のサポート	ASDM 7.16 ASA 9.16	Premier	○	○	○
カスタマイズするキャッシュの設定	ASDM 7.16 ASA 9.16	Premier	○	○	○
定期的なフロー レポート	ASDM 7.16 ASA 9.16	Premier	○	○	○
フロー フィルタ	依存関係なし	Premier	○	○	○

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
スタンドアロン NVM	依存関係なし	Premier	○	○	○
Cisco Secure Cloud Analytics との統合	依存関係なし	適用対象外	○	×	×
プロセスツリーの階層	依存関係なし	適用対象外	○	○	○

Secure Umbrella モジュール

Secure Umbrella モジュール	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
Secure Umbrella モジュール	ASDM 7.16 ASA 9.16	ISE 2.0	Advantage または Premier のいずれか Umbrella のライセンスが必須	○	○	×
Umbrella セキュア Web ゲートウェイ	依存関係なし	依存関係なし	適用対象外	○	○	×
OpenDNS IPv6 のサポート	依存関係なし	依存関係なし	適用対象外	○	○	×

Cisco Umbrella ライセンスの詳細については、「https://www.opendns.com/enterprise-security/threat-enforcement/packages/」を参照してください。

ThousandEyes Endpoint Agent モジュール

機能	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
Endpoint Agent	依存関係なし	依存関係なし	適用対象外	○	○	×

カスタマーエクスペリエンスのフィードバック

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
カスタマーエクスペリエンスのフィードバック	ASA 9.16 ASDM 7.16	Advantage	○	○	×

Diagnostic and Reporting Tool（DART）

ログ タイプ	必要なライセンス	Windows	macOS	Linux
VPN	Advantage	○	○	○
クラウド管理	適用対象外	○	○	×
Duo Desktop	適用対象外	○	○	×
Endpoint Visibility モジュール	適用対象外	○	×	×
ISE ポスチャ	Premier	○	○	○
ネットワーク アクセス マネージャ	Premier	○	×	×
Network Visibility Module	Premier	○	○	○
Secure Firewall ポスチャ	Premier	○	○	○
Secure Endpoint	適用対象外	○	○	×
ThousandEyes	適用対象外	○	○	×
Umbrella	適用対象外	○	○	×
Zero Trust Access モジュール	適用対象外	○	○	×

ユーザー補助の推奨事項

シスコは、特定の Voluntary Product Accessibility Template（VPAT）コンプライアンス基準を遵守することで、ユーザー補助を強化し、すべてのユーザーにシームレスなエクスペリエンスを提供することに従事しています。シスコの製品は、さまざまなユーザー補助ツールと効果的に

統合するように設計されており、特定のニーズを持つ個人が使いやすく、アクセスできるようにしています。

JAWS スクリーンリーダー

Windows ユーザーの場合、JAWS スクリーンリーダーとその機能を使用して、障がいを持つユーザーを支援することをお勧めします。JAWS（Job Access with Speech）は、視覚障がいを持つユーザーに音声フィードバックとキーボードショートカットを提供する強力なスクリーンリーダーです。ユーザーは、音声出力と点字表示を使用して、アプリケーションや Web サイトを遷移できます。JAWS とを統合することにより、視覚障がいを持つユーザーは、すべての機能に効率的にアクセスして操作することができ、全体的な生産性とユーザー体験が向上します。

Windows オペレーティングシステム（OS）のユーザー補助ツール

Windows の拡大鏡

Windows の拡大鏡ツールを使用すると、画面上のコンテンツを拡大でき、視覚が弱いユーザーの可視性が向上します。ユーザーは拡大縮小を簡単に行えるため、テキストと画像が鮮明で読みやすくなります。

Windows では、表示解像度を 1280px x 1024px 以上に設定します。[ディスプレイでの拡大縮小（Scaling on Display）] 設定を変更することで 400% まで拡大でき、Secure Client で 1 つまたは 2 つのモジュールタイルを表示できます。200% を超える拡大を行うと、（モニターのサイズによっては）Secure Client の詳細ウィンドウの内容が十分に表示されない場合があります。コンテンツベースの Web ページや出版物で一般的に使用され、レスポンシブ Web デザインとも呼ばれる Reflow はサポートしていません。

色を反転

反転色機能には、コントラストテーマ（水色、夕暮れ、夜空）と Windows カスタムテーマがあります。ユーザーは Windows 設定で [コントラストテーマ（Contrast Theme）] を変更して、Secure Client に高コントラストモードを適用し、特定の視覚障がい者が画面上の要素を読みやすく、操作しやすくする必要があります。

キーボード ナビゲーション ショートカット

Secure Client はコンテンツベースの Web アプリケーションではないため、UI 内には独自のコントロールとグラフィックがあります。効率的に遷移するため、Cisco Secure Client ではさまざまなキーボードショートカットがサポートされています。以下の推奨事項に従い、説明されているツールとショートカットを使用することで、ユーザーは Secure Client の操作を強化し、よりアクセス可能で効率的なエクスペリエンスを確保できます。

- タブの遷移：プライマリ（タイル）ウィンドウ、DART セットアップダイアログ、および各モジュールのサブダイアログ内の個々のパネル遷移には Tab キーを使用します。スペースバーまたは Enter キーを押すと、アクションがトリガーされます。フォーカスされてい

る項目は濃い青色で示され、フォーカスがずれたことを示す表示は、コントロールの周囲に枠で表示されます。

- モジュールを選択：上下矢印キーを使用して、左側のナビゲーションバーで特定のモジュール間を移動します。
- モジュールプロパティページ：左右矢印キーを使用して個々の設定タブ間を遷移し、パネル遷移には Tab キーを使用します。
- 詳細ウィンドウ：Alt + Tab を使用してウィンドウを選択し、Esc を使用してウィンドウを閉じます。
- グループテーブルリストの遷移：PgUp/PgDn またはスペースバー/Enter を使用して、特定のグループを展開または折りたたみます。
- アクティブな Cisco Secure Client UI の最小化/最大化： Windows ロゴキー + 上下矢印。
- ダイアログについて：Tab キーを使用してこのページ内を移動し、スペースバーを使用して使用可能なハイパーリンクを起動します。

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。