



Q&A

Cisco Secure Services Client 4.0.5

概要

以下の Q&A では、Cisco® Secure Services Client の基本的な情報を説明します。さらに、「製品の詳細」以降では、このクライアントの機能およびシスコのソリューションとの相互運用性に関して、より詳しく説明します。

Q. Cisco Secure Services Client とは何ですか。

A. Cisco Secure Services Client バージョン 4.0 は、デバイス上に常駐させてユーザ アイデンティティを管理し、安全なネットワーク接続を確立するためのクライアント ソフトウェアです。Cisco Secure Services Client は、エンタープライズ ネットワークにアイデンティティ ベースのネットワーク アクセス コントロールを実装して管理するための、エンドポイント セキュリティおよび管理ソリューションとしての機能を備えています。業界標準の 802.1X の実装により、IT 管理者はレイヤ 2 セキュリティ フレームワークを使用してエンドポイント デバイスを保護することができます。Cisco Secure Services Client は全プラットフォームに対応し、有線および無線ネットワーク上で共通の認証フレームワークを提供します。表 1 に、Cisco Secure Services Client 4.0.5 の主な機能を示します。

表 1 Cisco Secure Services Client 4.0.5

対象ユーザ	中小・中堅企業および大企業
サポートされる 802.1X EAP タイプ	EAP-MD5、EAP-TLS、EAP-TTLS、LEAP、EAP-FAST、PEAP、MSCHAPv2、GTC
サポートされる OS	Windows 2000 日本語版、Windows XP 日本語版
サポートされる暗号化方式	WEP、Dynamic WEP (802.1X)、TKIP、AES、WPA-PSK、WPA2-PSK、WPA、WPA2

Q. Cisco Secure Services Client の製品名の由来を教えてください。

A. Cisco Secure Services Client という名前は、この製品が業界標準の 802.1X 規格をサポートしているため、有線および無線ネットワーク上でセキュアかつ拡張可能なデバイス認証を実行できることと、ユーザおよびデバイスのアイデンティティに基づいて、クライアントにさまざまなサービスを提供できることに由来しています。提供可能なサービスは次のとおりです。

- 認証サービス：802.1X
- ネットワーク アドミッション用のアイデンティティ サービス：有線および無線ネットワーク対応の Cisco Trust Agent、NAC (Network Admission Control)
- データおよび管理用の暗号化サービス：WPA および WPA2
- Cisco Compatible Extensions：パフォーマンス最適化、音声サービス、ロケーション サービス (対応予定)
- クライアント管理サービス：クライアント プロファイルの自動設定

Q. Cisco Secure Services Client の機能は、Meetinghouse AEGIS SecureConnect クライアントと同じですか。

A. はい。Meetinghouse Data Communications 社の買収に伴い、AEGIS SecureConnect クライアントはシスコ製品となりました。Cisco Secure Services Client は、AEGIS SecureConnect 製品を名称変更したものです。

Q. Cisco Secure Services Client を使用する利点とは何ですか。

A. Cisco Secure Services Client を使用すると、IT 部門では 802.1X ベースのセキュリティ戦略の設計および実装が可能となり、有線および無線ネットワークに対する防御機能を備えたセキュアな周辺機器として、新たなエンドポイント デバイスを使用できるようになります。これにより、IT 管理者はアイデンティティ ベースのネットワーク セキュリティを導入することで、マシンとユーザの権限付与、デバイスの整合性の維持、企業ネットワークに対するセキュリティ侵犯の軽減を同時に実現できます。

また、このソリューションは、有線イーサネットおよび Wi-Fi アクセス コントロール ポリシーの簡素化と適用を目的として設計されており、デバイス、ネットワーク、および認証テクノロジーに依存しません。表 2 に、Cisco Secure Services Client の主な機能と利点を示します。

表 2 Cisco Secure Services Client の機能と利点

特性	機能	利点
統合された有線および無線ネットワーク クライアント	有線イーサネットと Wi-Fi セキュリティの統合	エンドポイント クライアント数を削減して IT 管理を簡素化
業界標準のサポート	IEEE、IETF、Wi-Fi Alliance、Cisco Compatible Extensions	さまざまなネットワーク アダプタとソリューションに対する優れたサポート性
エンドポイントの整合性	非適合デバイスの検疫と修復を実施	ネットワークの他のデバイスに影響を与える可能性のある、不正なソフトウェアによるホスト PC の脆弱化の危険性を最小化
シングル サインオン (SSO) に対応	Microsoft AD および Novell eDirectory の SSO をサポート	エンド ユーザに対する複雑性を軽減することで、IT 部門の運用コストを削減
グループ ポリシーの有効化	アイデンティティ グループ (ダイナミック VLAN 割り当て、ダウンロード可能な ACL [Access Control List; アクセス コントロール リスト] など) に基づいてネットワーク ポリシーを適用可能	アドミッション コントロール以外に、ネットワーク接続されたリソースに対するユーザ アクセスの制限機能を提供
管理制御	特定のセキュリティ プロファイルとポリシーを、選択的に定義および制限可能	エンドポイント セキュリティ ポリシーを一元的にプロビジョニングおよび実施すると同時に、ユーザ定義のホットスポットとホーム プロファイルも有効

Cisco Secure Services Client を使用すると、次のような利点も得られます。

- シスコの EAP-FAST プロトコルのサポート (NAC [Network Admission Control] の一部として)
- 有線および無線の LAN 接続 (無線アクセスでは WPA2 をサポート)
- 設定可能なネットワーク プロファイルと導入ツールにより、ネットワーク アクセスを効率化
- サーバおよびクライアント証明書のネットワーク アクセス ポリシーの実施
- シンプルで柔軟性に優れたユーザ インターフェイス
- 既存の AAA (Authentication, Authorization, and Accounting; 認証、認可、アカウントिंग) /RADIUS サーバとの相互運用性により、アップグレード コストを削減
- Cisco Compatible Extensions バージョン 4.0 のサポート

Q. Cisco Secure Services Client と他のシスコ クライアントとの相互運用性について教えてください。

A. Cisco Secure Services Client は、エンタープライズ クライアント セキュリティ向けにエンドツーエンド ソリューションを提供するシスコの取り組みを代表する製品です。Cisco Secure Services Client の発売以前、シスコでは Cisco Trust Agent に OEM の 802.1X サプリカントをバンドルしていましたが、これは有線の NAC 構成のみを対象としていました。Cisco Secure Services Client では、有線および無線ネットワークに対応するフル機能のサプリカントを提供できます。Cisco Secure Services 802.1X クライアント ソフトウェア サプリカントは、Cisco Access Control Server (ACS) RADIUS サーバの機能を大幅に向上させ、有線および無線の両方のセキュリティ ポリシーについて、お客様に優れたセキュリティ管理機能を提供します。Cisco Secure Services Client では、Cisco Compatible Extensions プログラムを通じたシスコの取り組みを発展させ、より広範なクライアント デバイスに対して一貫した 802.1X のサポートが可能になりました。表 3 に、Cisco Secure Services Client と、Cisco Trust Agent クライアントおよび Cisco Compatible Extensions クライアントの比較を示します。

表 3 シスコ クライアントの比較表

	Cisco Trust Agent クライアント (OEM サプリカントをバンドル)	Cisco Compatible Extensions クライアント	Cisco Aironet デスクトップ ユーティリティ	Cisco Secure Services Client
サポートされるネットワーク インターフェイス	有線のみ	無線のみ	無線のみ	有線および無線
802.1X サプリカント	EAP、OS、および GUI のサポートに制限あり	制限あり(ベンダーによって異なる)	シスコ クライアント アダプタに限定	完全対応
セキュリティ プロファイル の一元管理	×	×	×	○
ユーザ/IT エクスペリエンス	トラブルシューティング と管理に制限あり	デバイス製造元によって 実装が異なる	シスコ クライアント アダプタに限定	全アダプタに関して一律
NAC のサポート	○ (有線のみ)	状況に応じて異なる	×	○ (有線および無線)
購入費用	無償	無償 (製品にバンドル)	無償 (シスコ クライアント アダプタに付属)	有償 (シート単位)

- Q.** Cisco Secure Services Client は、Cisco Secure Access Control Server (ACS) でサポートされていますか。
- A.** はい。Cisco Secure Services Client は、Cisco Secure ACS プラットフォームで完全にサポートされています。クライアント サプリカントとバックエンド認証サーバを組み合わせることで、有線および無線ネットワーク全体に強固なクライアント認証機能を備えた包括的なソリューションを提供できます。
- Q.** Cisco Secure Services Client と Cisco Unified Wireless Network の相互運用性について教えてください。
- A.** Cisco Secure Services Client を使用すると、企業の有線および無線ネットワークに対する、さまざまなクライアント デバイスのセキュアな認証が可能になります。サプリカントは Cisco Unified Wireless Network で完全にサポートされており、既存のシスコ製アクセス ポイントおよび Wireless LAN Controller 製品と併用できます。
- Q.** 既存の NAC (Network Admission Control) 戦略に対する Cisco Secure Services Client の位置付けを教えてください。
- A.** Cisco Secure Services Client は、アドミッション コントロール テクノロジーとして 802.1X を選択されたお客様に対し、統合された有線および無線 802.1X クライアントを提供することで NAC フレームワークを強化します。
- Q.** Cisco Secure Services Client は、Cisco NAC アプライアンスでサポートされていますか。
- A.** 現在、Cisco Secure Services Client は、アプライアンス ベースで提供される NAC ではサポートされていません。シスコでは、統合フレームワークおよびアプライアンス ソリューション セットを提供できるよう目指しています。このため、Cisco Secure Services Client では、お客様の運用要件に合わせてクライアントや認証タイプを選択できるようになっています。
- Q.** Cisco Secure Services Client に関し、Trusted Computing Group (TCG) の Trusted Network Connect (TNC) ワーキンググループに参加する予定はありますか。
- A.** シスコでは現在、TCG および TNC に参加する予定はありません。シスコでは、エンドポイントの整合性に必要なプロトコルは、他のインターネット プロトコルの標準化を行っている Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の主導下で開発する必要があると考えています。現在は IETF において、エンドポイントの整合性に関するプロトコルがよりよいものとなるよう、TNC のメンバーと協力して標準化を進めています。
- Q.** Cisco Secure Services Client の製品番号と発注方法を教えてください。
- A.** Cisco Secure Services Client は、シスコのグローバル プライス リストに記載されており、シスコの標準製品として発注できます。発注の際は、製品番号：AIR-SC4.0-XP2K を使用してください。

製品の詳細

- Q.** Cisco Secure Services Client で複数のネットワーク プロファイルを保持し、自宅と会社の両方で使用することはできますか。
- A.** はい。Cisco Secure Services Client でサポートされるプロファイル数には制限がないため、自宅、会社、外出先など、任意の場所から使用できます。
- Q.** Cisco Secure Services Client では、オープン アクセス ポイントとセキュリティ保護されたアクセス ポイントの両方に接続できますか。
- A.** はい。Cisco Secure Services Client は、オープン アクセス ポイントとセキュリティ保護されたアクセス ポイントの両方をサポートするように設定できます。
- Q.** Cisco Secure Services Client は、WPA と WPA2 をサポートしていますか。
- A.** はい。Cisco Secure Services Client バージョン 4.0 は、Wi-Fi Alliance の WPA および WPA2 暗号化規格に完全に準拠しています。
- Q.** Cisco Secure Services Client は、コンシューマ レベルのアクセス ポイントと互換性がありますか。WPA-PSK または WPA2-PSK を使用して、ホーム ネットワークのセキュリティ保護を実行できますか。
- A.** はい。Cisco Secure Services Client 4.0 は、Wi-Fi 認定のホーム ネットワーキング機器と互換性があります。プライバシーを確保するために、お使いの機器では WPA-PSK または WPA2-PSK を使用するよう設定しておくことを推奨します。
- Q.** Cisco Secure Services Client でサポートされている EAP 認証方式を教えてください。
- A.** EAP-MD5、EAP-MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2)、EAP-TLS、EAP-FAST、EAP-GTC (Generic Token Card)、Cisco LEAP、PEAP、EAP-TTLS がサポートされています。
- Q.** Cisco Secure Services Client でサポートされている暗号化方式を教えてください。
- A.** WEP、Dynamic WEP (802.1X)、WPA、WPA2、AES (Advanced Encryption Standard)、TKIP (Temporal Key Integrity Protocol)、WPA-PSK、WPA2-PSK がサポートされています。
- Q.** Cisco Secure Services Client 4.0 でサポートされているオペレーティング システムを教えてください。
- A.** Windows 2000 日本語版および Windows XP 日本語版がサポートされています。
- Q.** その他のオペレーティング システムをサポートする予定はありますか。
- A.** はい。Cisco SSC ロードマップには、企業の有線および無線デバイスで使用される主要なオペレーティング システムのサポートが含まれています。これにより、デスクトップ パソコン、ノート型パソコン、サーバ、無線電話、ハンドヘルド デバイスなど、すべてのデバイスに対して一貫したエンドポイント セキュリティおよび管理機能の提供が可能となります。

©2006 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0609R) 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。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
<http://www.cisco.com/jp>
お問い合わせ先(シスココンタクトセンター)
<http://www.cisco.com/jp/service/contactcenter>
0120-092-255 (通話料無料)
電話受付時間：平日10:00~12:00、13:00~17:00