

Cisco Secure Access Control Server 4.0

概要

Q. Cisco® Secure Access Control Server(ACS)とは何ですか。

A. Cisco Secure ACS はスケーラビリティとパフォーマンスに優れたアクセス コントロール サーバです。統合型の RADIUS サーバまたは TACACS+ サーバ システムとして運用され、ネットワークから企業のリソースにアクセスするユーザの Authentication, Authorization, Accounting(AAA; 認証、認可、アカウントिंग)を制御します。Cisco Secure ACS を使用すると、ネットワークへのユーザ アクセスの制御、ユーザまたはユーザのグループに対するさまざまなタイプのネットワーク サービスの認証、およびネットワーク ユーザの全行動の記録が可能になります。Cisco Secure ACS は、ダイヤルアップ アクセス サーバのアクセス コントロールとアカウントング、ケーブルおよび DSL ブロードバンド ソリューション、ファイアウォール、VPN、Voice over IP (VoIP) ソリューション、ストレージ、およびスイッチド LAN と無線 LAN をサポートします。また、ネットワーク マネージャは同じ AAA フレームワークを使用して、(TACACS+ により)管理者の権限の範囲およびグループを管理し、内部でネットワークを変更、アクセス、および設定する方法を制御します。

Q. Cisco Secure ACS が必要な理由は何ですか。

A. 変化の激しいネットワークの成長と、増大するセキュリティ上の脅威により、アクセス コントロールの管理において新しい需要が発生しています。IEEE 802.1X などの新しいテクノロジーにより、ネットワーク全体で AAA が使用可能になり、ユーザ アクセス コントロールの要件が拡大するにつれて、ネットワーク全体にアイデンティティ ネットワーキングを浸透させる必要性が高まってきました。Cisco Secure ACS は、中央集中型のアイデンティティ ネットワーキング ソリューションの認証、ユーザと管理者のアクセス、およびポリシー制御を結合することで、アクセス セキュリティを拡張します。これにより、柔軟性と機動性が高くなり、セキュリティが向上し、ユーザの生産性を高めることができます。

Q. Cisco Secure ACS は、ソフトウェア製品ですか、ハードウェア製品ですか。

A. Cisco Secure ACS は、Cisco Secure ACS for Windows(Windows サーバへのインストール用)または Cisco Secure ACS Solution Engine(Cisco Secure ACS ライセンスがブリインストールされた 1 RU アプライアンス)として提供されます。

Q. Cisco Secure ACS for Windows と Cisco Secure ACS Solution Engine の違いは何ですか。

A. Cisco Secure ACS Solution Engine は、Cisco Secure ACS for Windows と同じ特長および機能を備えていますが、セキュリティが強化された専用アプライアンス パッケージです。Cisco Secure ACS Solution Engine には、Cisco Secure ACS Solution Engine の運用および管理のための追加機能も含まれています。詳細については、[Cisco Secure ACS Solution Engine に関する Q&A](#) を参照してください。

Q. Cisco Secure ACS for Windows または Cisco Secure ACS Solution Engine のどちらを購入した方が良いでしょうか。

A. Cisco Secure ACS for Windows は、運用環境(ハードウェア サーバ、OS [オペレーティングシステム]、導入されているサービスなど)の制御を検討しているお客様に適しています。IT 企業では、セキュリティの運用部門とサーバ/OS の運用部門が異なる場合が多いため、専用ア

プライアンスによるセキュリティ ソリューションを使用することで、問題の発見が早くなり、アプライアンスの管理が簡単になります。また、アプライアンス ソリューションには、セキュリティの強化、ワンストップ サポート、「プラグアンドプレイ」ソリューションなどの利点もあります。

デバイスのサポート

Q. Cisco Secure ACS でサポートされているデバイス、Cisco IOS® ソフトウェア リリース、およびサードパーティのディレクトリは何ですか。

A. システムおよびソフトウェアの最小要件の詳細なリストは、Cisco Secure ACS 4.0 ユーザ ガイドに付属の『Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.0』を参照してください。

Q. Cisco Secure ACS でサポートされているネットワーク アクセス ゲートウェイは何ですか。

A. Cisco Secure ACS は、すべての Cisco IOS ルータ、VPN アクセス製品、VoIP ソリューション、ケーブル ブロードバンド アクセス、コンテンツ ネットワーク、無線ソリューション、ストレージ ネットワーク、および 802.1X 対応の Cisco Catalyst® スイッチを含む、広範なネットワーク アクセス製品をサポートしています。Cisco Secure ACS は、標準に完全に準拠した RADIUS および TACACS+ サーバとして、RADIUS または TACACS+ をサポートするさまざまなサードパーティ製のアクセスおよびデバイス管理コンソールとしても機能します。

セキュリティ イニシアティブ

Q. Cisco Secure ACS は、シスコシステムズの Identity Based Networking Services (IBNS)にどのように適合していますか。

A. Cisco Secure ACS は、802.1X IEEE 標準に基づいて構築されたアーキテクチャである Cisco IBNS ソリューションの主要コンポーネントです。Cisco Secure ACS は、従来はアクセス コントロールがネットワークのエッジで管理されていた LAN(有線および無線)内で、中央集中型の認証サーバとして RADIUS ベースの AAA 機能を提供します。特に、IBNS と Cisco Secure ACS を組み合わせることで、次の利点があります。

- Public Key Infrastructure(PKI; 公開鍵インフラストラクチャ)、トークン、および Smartcard による強力な認証。これは特に、無線 LAN 環境で重要です。無線 LAN 環境では、強力な相互認証方法が使用されていない場合、不正なセキュリティ攻撃に対する脆弱性が非常に高くなるためです。
- 柔軟なポリシー割り当て(ユーザごとの割り当て、VLAN 割り当てなど)
- ユーザ アカウンティング、監査、および LAN 内でのユーザの行動を追跡してモニタするための機能
- IBNS は、識別されたエンティティ(ユーザベースおよびデバイスベース)と、一元的に作成された Cisco Secure ACS によって管理されるポリシーを結合することで、きめ細かい制御と高い柔軟性を実現します。

Q. Cisco Secure ACS は、LAN 内でどのようにして Cisco IBNS を拡張するのですか。

A. Cisco Secure ACS は、一元的な Web ベースのグラフィカル インターフェイスで認証、アクセス コントロール、およびユーザ プロファイリングとトラッキングを結合し、その制御範囲をネットワーク内の何百または何千もの有線および無線アクセス ポイントに広げることで、Cisco IBNS アーキテクチャ内の LAN アクセス セキュリティを拡張します。Cisco Secure ACS による強化は、ID 認証や安全なネットワーク接続だけにとどまりません。ポート セキュリティを備えた補助 VLAN および 802.1X に対応した Cisco Architecture for Voice, Video and Integrated Data(AVVID)サポート、およびユーザごとの VLAN および Access Control List (ACL; アクセス コントロール リスト)の動的プロビジョニングも提供します。IBNS とその LAN

における機能の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns75/networking_solutions_sub_solution_home.html

Q. Cisco Secure ACS は、Cisco Network Admission Control(NAC)にどのように適合していますか。

A. Cisco Secure ACS 4.0 は、NAC フレームワークにおいてポリシー決定ポイントとして機能します。設定されたポリシーを使用して、Cisco Trust Agent から受信したクレデンシャルを評価し、ホストの状態を判断します。その後、AAA クライアント ACL を、クライアントがレイヤ 2 ネットワーク経由で接続されている場合はポリシーベースの ACL やプライベート VLAN を、ホストの状態に基づいて送信します。ホスト クレデンシャルの評価では、OS パッチ レベルやウイルス対策ソフトウェアの DAT ファイルのバージョンなど多数の固有のポリシーについて評価することができます。Cisco Secure ACS は、モニタリング システムで使用するために、ポリシー評価の結果を記録します。また、Cisco Secure ACS 4.0 では、サードパーティの監査ベンダーが応答のなかったホストを監査してから、ネットワークへのアクセスを許可することができます。ポリシーは Cisco Secure ACS によってローカルに評価することも、Cisco Secure ACS がクレデンシャルを転送した外部ポリシー サーバにその評価結果を返させることもできます。たとえば、ウイルス対策ソフトウェア ベンダーに固有の証明書はそのベンダーのアンチウイルス ポリシー サーバへ転送し、監査ポリシー要求は監査ベンダーへ転送することができます。

新機能とプロトコルのサポート

Q. Cisco Secure ACS 4.0 の新機能は何ですか。

A. Cisco Secure ACS 4.0 では、次の機能が追加されました。

- Cisco NAC フェーズ 2 のサポート
- ネットワーク アクセス ポリシー: Cisco Secure ACS は、この機能を使用して、ネットワーク アクセス デバイスまたは要求の属性に基づいて、要求の認証/許可方法を動的に決定することができます。
- スケーラビリティとパフォーマンスの改善: 標準準拠の RDMS を導入することで、Cisco Secure ACS 4.0 のスケーラビリティとパフォーマンスが大幅に改善されました。
- 有線 LAN 環境での Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling(EAP-FAST)による認証のサポート
- ダウンロード可能な IP ACL
- Extensible Authentication Protocol-Transport Level Security (EAP-TLS) 認証のための Certificate Revocation List(CRL)の比較
- Machine Access Restrictions(MAR)
- Network Access Filtering(NAF)
- レプリケーションの拡張(さまざまなレベルでユーザおよびグループを個別のレプリケーション コンポーネントとして選択)、およびプロファイルなどの追加コンポーネントのレプリケーションのサポート。このリリースで導入された特長および機能の詳細については、Cisco Secure ACS 4.0 for Windows のデータシートを参照してください。

Q. EAP-Microsoft Challenge Handshake Authentication Protocol (MSCHAP) v2 と EAP-Generic Token Card (GTC) Protected Extensible Authentication Protocol (PEAP) サプリカントの違いは何ですか。

- A.** どちらのサプリカントも PEAP をサポートしていますが、TLS トンネルによるクライアント認証の方法が異なります。Microsoft PEAP サプリカントは、MSCHAPv2 によるクライアント認証のみをサポートしています。これにより、Windows NT Domain や Active Directory など、MSCHAPv2 をサポートするユーザ データベースへのアクセスが制限されます。(EAP-GTC に基づく) Cisco PEAP サプリカントは、One-Time Password (OTP; ワンタイム パスワード) およびログオン パスワードによるクライアント認証をサポートしています。これにより、RSA Security や Secure Computing Corporation などのベンダーの OTP データベースや、Lightweight Directory Access Protocol (LDAP)、Microsoft、Novell Directory Service (NDS) などのログオン パスワード データベースが利用できます。

また、EAP-GTC の実装により、TLS 暗号化トンネルが確立されるまでユーザ名アイデンティティは公開されません。これにより、認証フェーズでユーザ名がブロードキャストされないため機密性が高まります。Cisco Secure ACS Version 3.2 以上は、EAP-MSCHAPv2 サプリカントと EAP-GTC PEAP サプリカントの両方をサポートします。

Q. PEAP 認証は、無線 LAN と有線 LAN の両方の認証に使用できますか。

- A.** はい。Cisco PEAP は、当初は無線認証の EAP タイプ (Cisco Aironet[®] アダプタ カードを使用) として開発されましたが、PEAP と Cisco Secure ACS を使用して、PEAP IETF ドラフト版 RFC に準拠した PEAP 対応サプリカントを使用することで、有線および無線認証の両方に対応しています。

Q. EAP タイプ認証を使用する場合、Cisco Secure ACS ではどのユーザ データベースを使用できますか。

- A.** 使用する EAP 認証タイプによって、Cisco Secure ACS では、表 1 に示すように、さまざまなユーザ データベースをサポートしています。

表 1 ユーザ データベースと EAP 互換性サポートのマトリクス

データベース	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MSCHAPv2)	EAP-FAST (フェーズ 0)	EAP-FAST (フェーズ 2)
Cisco Secure ACS	○	○	○	○	○	○	○
Windows	○	×	○	○	○	○	○
Active Directory							
LDAP	×	×	○	○	×	×	○
Novell NDS	×	×	×	○	×	×	○
Open Database Connectivity (ODBC; オープンデータベース接続)	○	○	○	○	○	○	○
LEAP プロキシ RADIUS サーバ	○	×	×	○	○	○	○
すべてのトークンサーバ	×	×	×	○	×	×	×

Q. EAP の詳細を入手する方法を教えてください。

- A.** EAP の詳細については、次の URL にアクセスして、『Cisco Aironet and Cisco Secure ACS Security Implementation for the Cisco Wireless Security Suite including PEAP,』

LEAP, and EAP-TLS』の Q&A を参照してください。

<http://www.cisco.com/en/US/products/index.html>

Q. EAP-FAST とは何ですか。

- A.** EAP-FAST は、シスコが開発した一般に利用可能な新しい IEEE 802.1X EAP タイプで、強力なパスワード ポリシーの施行が困難で、802.1X EAP タイプの認証を希望するお客様をサポートします。EAP-FAST は、デジタル認証が不要で、さまざまなユーザおよびパスワード データベース タイプ、およびパスワードの有効期限と変更をサポートし、柔軟性があり、導入と管理が簡単な EAP です。EAP-FAST の詳細と、その他の EAP タイプとの比較については、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

Q. マシン認証とは何ですか。また、Cisco Secure ACS ではマシン認証をどのようにサポートしているのですか。

- A.** マシン認証は起動時に実行され、Windows ドメイン コントローラを認証して通信を開始し、インタラクティブなユーザ認証セッションとは関係なく、マシン グループ ポリシーを適用します。Cisco Secure ACS では、ユーザ セッションが開始される前に 802.1X ポートでマシン認証が行われます。このとき、Cisco Secure ACS にマシン名が送信され(この際に有効な証明書が使用されるかどうかは使用する EAP メソッドによって異なります)、マシン ID が検証されます。Cisco Secure ACS は、Windows Active Directory に対して EAP-TLS または PEAP-EAP-MSCHAPv2 を使用したマシン認証をサポートします。また、Cisco Secure ACS 4.0 には、Windows マシン認証の拡張機能としてマシン アクセス制限(MAR)が含まれています。MAR を使用すると、管理者はマシンにユーザを柔軟にバインドできるため、許可されていないマシンによるネットワーク接続を回避できます。Cisco Secure ACS は、通常その後に行われるユーザベースの認証セッションとは関係なく、マシン認証を個別の認証セッションとして処理します。ユーザまたはマシン認証は、Windows 2003/XP の設定ページで設定されます。

Q. Cisco Secure ACS では、不明なマシン認証やグループ マッピングはサポートされていますか。

- A.** はい。不明なユーザ認証やグループ マッピングと同様に、不明なマシンの証明書が Windows Active Directory に存在するかが、Cisco Secure ACS によって認証できます。

Q. Cisco Secure ACS では、LDAP にどのようなサポートを提供していますか。

- A.** Cisco Secure ACS は、LDAP によってディレクトリ サーバに保存されたレコードを使用したユーザ認証をサポートしています。Cisco Secure ACS は、LDAP 汎用インターフェイスによって、Novell や Sun LDAP サーバなど、代表的なディレクトリ サーバをサポートしています。ディレクトリ サーバを利用した認証の場合、パスワード認証プロトコルのパスワードを使用できます。

また、Cisco Secure ACS では、Windows 2003 の Active Directory Service もサポートしています。Cisco Secure ACS は、複数の LDAP 認証要求を、以前のような順次処理ではなく、同時に処理することができます。この機能により、無線構成など、タスク中心のアプリケーションにおける Cisco Secure ACS 4.0 のパフォーマンスが大幅に改善されました。LDAP の詳細については、次の URL にある White Paper『Configuring LDAP for Cisco Secure ACS』(英語)を参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html

- Q. Cisco Secure ACS は、Microsoft Active Directory 内のユーザを認証するために Windows NT LanManager (NTLMv2) をサポートしていますか。**
- A.** はい。
- Q. Cisco Secure ACS は、OTP や、RSA SecurID トークンなどのトークン システムをサポートしていますか。**
- A.** はい。Cisco Secure ACS は、ActivCard、Cryptocard、PassGo Technologies、RSA Data Security、Secure Computing、および Vasco のトークン ソリューションと通信するように設定できます。Cisco Secure ACS は RADIUS 汎用インターフェイスを備えているため、新しいベンダーの OTP にも対応できます。RFC 準拠の RADIUS インターフェイスを提供する OTP ベンダーは、Cisco Secure ACS 3.0 以上を使用する必要があります。Windows NT、NetWare、UNIX など、すべての OS にトークン認証サーバをインストールできます。
- Q. Cisco Secure ACS は、Smartcard などの強力な PKI ベースの認証タイプをサポートしていますか。**
- A.** はい。Cisco Secure ACS Version 3.0 以上は、標準的な PKI ベースの Smartcard ソリューションすべてと通信するように設定できます。シスコでは特に、Schlumberger (Cyberflex)、ActivCard (Gold)、および Aladdin (eToken) との Smartcard のインターオペラビリティを検証しました。
- Q. Cisco Secure ACS には、一定の期間が経過すると、ユーザにパスワードを強制的に変更させる機能があります。この機能は、認証に Windows Active Directory を使用している場合にも使用できますか。**
- A.** 従来、この機能は、認証に Cisco Secure ACS データベースを使用している場合のみ、機能していました。Cisco Secure ACS のパスワード エージング サポートの新しい拡張機能により、現在は、Microsoft Active Directory ドメインに対するパスワード エージングがサポートされるようになりました。この機能は、Microsoft OS の MSCHAP v2 パスワード変更サポートによって提供され、Cisco VPN Client Version 3.5、Cisco Wireless PEAP クライアントなど、さまざまなデスクトップ クライアントでも使用できます。
- Q. Cisco Secure ACS への管理通信を保護できますか。**
- A.** はい。Cisco Secure ACS Version 3.1 以上は、(Web GUI による) Cisco Secure ACS への管理アクセスを Secure Sockets Layer (SSL) によって保護することで、Cisco Secure ACS 設定のセキュリティ全体を向上させます。このセキュリティ強化により、証明書を使用したサーバ認証と暗号化トンネル サポートが実現し、すべての管理アクセスが SSL によって暗号化されます。
- Q. ユーザは、Network Address Translation (NAT; ネットワーク アドレス変換) を実行しているファイアウォールを経由して Cisco Secure ACS GUI にアクセスできますか。**
- A.** はい。Cisco Secure ACS は、セッションごとに固有のポートを使用し、また一部の構成可能な固有のポートのみがファイアウォールを通過するのを許可します。これにより、ユーザは、NAT を実行しているゲートウェイ デバイスの前にあるワークステーションから、Cisco Secure ACS GUI にアクセスできます。

Q. Cisco Secure ACS で使用されるポートとプロトコルは何ですか。

A. Cisco Secure ACS は、表 2 に示す TCP/UDP ポートを使用します。

表 2 Cisco Secure ACS ポートの用途

サービス名	UDP	TCP
Dynamic Host Configuration Protocol (DHCP)	68	–
RADIUS 認証および許可(オリジナル版ドラフト RFC)	1645	–
RADIUS アカウンティング(オリジナル版ドラフト RFC)	1646	–
RADIUS 認証および許可(改訂版 RFC)	1812	–
RADIUS アカウンティング(オリジナル版ドラフト RFC)	1813	–
TACACS+ AAA	–	49
レプリケーションおよび RDBMS の同期	–	2000
Cisco Secure ACS リモート ロギング	–	2001
HTTP 管理アクセス(ログイン時)	–	2002
Cisco Secure ACS 分散ロギング(アプライアンスのみ)	–	2003
管理アクセス(ログイン後)のポート範囲	–	1024
設定変更可能なデフォルト	–	65,535

Q. Cisco Secure ACS に対応しているレポートおよびモニタ機能は何ですか。

A. Cisco Security Monitoring, Analysis, and Response System (MARS) です。これらは、Cisco Secure ACS に高度なレポートおよびモニタ機能を提供します。

Q. ドメイン コントローラに対して適切な Windows 認証が行われるようにするには、メンバーサーバで稼働している Cisco Secure ACS サーバにどのようなセキュリティ コンテキストが必要ですか。

A. セキュリティ コンテキストは、ローカル サービス アカウントで定義されます。メンバー サーバで Cisco Secure ACS を稼働し、Windows 認証を実行するために必要な権限設定のガイドラインについては、Cisco Secure ACS インストレーション ガイドを参照してください。

Q. Cisco Secure ACS は、TACACS+ 要求と RADIUS 要求を同時に処理できますか。

A. はい。

Q. ユーザ パスワードは、Cisco Secure ACS にどのように格納されますか。

A. 次の URL にある Cisco Secure ACS ユーザ ガイドを参照してください。

http://www.cisco.com/jp/service/manual_j/sec/acs/ntug24/index.shtml

Q. Cisco Secure ACS は、パスワードの有効期限などの条件に基づくパスワードの強制変更をサポートしていますか。

A. パスワード エージングは、ローカル ユーザと、Microsoft Windows Active Directory データベース内のユーザに対して使用できます。プロセスの詳細については、次の URL を参照してください。

http://www.cisco.com/jp/service/manual_j/sec/acs/ntug24/chapter06/g.shtml

- Q. Cisco Secure ACS をインストールする必要があるのは、Microsoft Windows ドメイン コントローラだけですか。**
- A.** いいえ。Cisco Secure ACS は、ドメイン コントローラではない Windows 2000/2003 サーバにもインストールできます。引き続き、Microsoft Windows Active Directory などの Windows データベースの Windows ユーザを認証するように設定できます。
- Q. Cisco Secure ACS 4.0 のライセンスはどのようになっていますか。**
- A.** Cisco Secure ACS 製品は、サーバごとにライセンス供与されています。ポート、ユーザ、およびネットワーク アクセス サーバの数に制限はありません。使用可能な製品番号と詳細については、<http://www.cisco.com/go/acs> の Cisco Secure ACS 4.0 の製品情報を参照してください。

スケーラビリティ

- Q. Cisco Secure ACS ソリューションのスケーラビリティは、どのようになっていますか。**
- A.** 拡張性の高いアクセス サーバは、UNIX プラットフォームで実行する必要があると考えているお客様が多いのですが、これは Cisco Secure ACS には当てはまりません。Cisco Secure ACS のガイドラインとパフォーマンス分析によると、各 Cisco Secure ACS サーバは、構成、プラットフォーム、および使用条件にもよりますが、サーバ 1 台あたり 10,000 ~ 300,000 のユーザをサポートでき、20,000 を超えるデバイスに対応できます。ユーザ アクセス コントロールのフレームワークの拡大における主な問題は、バック エンドにあります。Oracle や Sybase など、高パフォーマンスのバックエンド データベースにリンクすることで、シスコは、数十万のユーザ レコードを処理するお客様向けに、クラスタ環境で Cisco Secure ACS for Windows 2003 を導入した例があります。
- Q. Cisco Secure ACS サーバ 1 台が処理できるユーザドメインの数に制限はありますか。**
- A.** いいえ。Cisco Secure ACS サーバが処理できるユーザドメインの数に、ハードウェア制限はありません。
- Q. Cisco Secure ACS Server for Windows で検証済みのパッチはどれですか。**
- A.** シスコシステムズでは、Cisco Secure ACS for Windows に関して、Windows 2000 Server および Windows Server 2003 のすべての Microsoft セキュリティ パッチを正式にサポートしており、これらをインストールすることを推奨しています。これまで、これらのパッチを使用したことに起因する Cisco Secure ACS for Windows の問題は一切発生していません。これらのセキュリティ パッチのいずれかをインストールしたことで Cisco Secure ACS に問題が発生した場合は、シスコ製品販売代理店にお問い合わせください。シスコでは、販売代理店と協力し、可能なかぎり迅速に問題を解決できるよう全面的にサポートさせていただきます。
- Q. 数百のユーザドメインがある大規模な分散環境では、認証タイムアウトを回避するために、どの Cisco Secure ACS を使用するのが適していますか。**
- A.** 認証タイムアウトに影響する主な要素は、ユーザが存在する場所(ドメイン コントローラの場所)に対する Cisco Secure ACS サーバの場所です。デバイス レベルでの AAA クライアントのタイムアウトを長くすることで、Cisco Secure ACS からの応答に時間がかかるという問題に対処する方法もあります。これが不可能な場合は、(認証中に)ドメイン名を指定したり、Cisco Secure ACS をユーザドメインの近くに配置するなどの方法も可能です。

発注情報

Q. Cisco Secure ACS 4.0 for Windows の発注方法を教えてください。

- A.** ネットワークに旧バージョンがインストールされておらず、新たに Cisco Secure ACS を購入される場合は、次の製品番号 CSACS-4.0-WIN-K9 をご指定ください。

なお、Cisco Secure ACS 4.0 はメジャーバージョンアップであるため、Software Application Support (SAS 契約) の対象とはなりません。

Cisco Secure ACS 1.x、2.x、3.x または Cisco Secure ACS for UNIX をすでにお使いのお客様は、次の製品番号 CSACS-4.0-WINUP-K9 をご指定ください。

Q. バックアップ用サーバの購入またはライセンス供与は可能ですか。

- A.** いいえ。バックアップおよびリカバリ用に、Cisco Secure ACS サーバの個別のライセンスを購入する必要があります。Cisco Secure ACS サーバは、リカバリまたはフェールオーバーサーバとして使用できます。Cisco Secure ACS はネットワーク内で一元的に制御サービスを提供しているため、フェールオーバーおよびリカバリ用のバックアップサーバを使用することを推奨します。

Q. Cisco Secure ACS for Windows の評価用コピーを入手できますか。

- A.** はい。Cisco Secure ACS の 90 日間のトライアルバージョンを <http://www.cisco.com/go/acs/> からダウンロードできます。評価用コピーを希望される場合は、シスコ代理店の担当者にお問い合わせください。

Q. Cisco Secure ACS for Windows を、90 日間のトライアルバージョンから完全な製品バージョンに移行する場合、トライアルバージョンをアンインストールする必要がありますか。

- A.** いいえ。トライアルバージョンをアンインストールしなくても、トライアルバージョンから完全な製品バージョンに簡単にアップグレードできます。トライアルデータベースに入力した設定、ユーザ、およびデバイスデータはすべて保持されます。

関連情報

Cisco Secure ACS の詳細については、次の URL を参照してください。

<http://www.cisco.com/jp/go/acs>

©2007 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。(0701R)

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/go/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

お問い合わせ先