



データシート

Cisco Secure Access Control Server 4.0 for Windows

Cisco® Secure Access Control Server (ACS) は、シスコのインテリジェント インフォメーション ネットワークに統合的なアイデンティティ ネットワーキング ソリューションと安全なユーザ サービスを提供し、企業ネットワークのすべてのユーザ、管理者、およびネットワーク インフラストラクチャのリソースの統合と制御を行います。

製品概要

今日、ネットワークにアクセスする方法は増え続けており、企業において、セキュリティ違反や不正なユーザ アクセスが重大な問題になっています。IEEE 802.11 無線 LAN およびユビキタスブロードバンド インターネット接続が広く採用されるようになるにつれ、セキュリティ問題は、ネットワークの周辺だけに留まらず、ネットワークの内側でも発生するようになってきました。そのため、このようなセキュリティの脆弱性を緩和するためのアイデンティティ ネットワーキング テクノロジーに注目が集まっています。

企業では、Public Key Infrastructure (PKI; 公開鍵インフラストラクチャ) や One-Time Password (OTP; ワンタイム パスワード) などの強力な認証方式を使用することで、パブリック ネットワークから企業内のリソースにアクセスするユーザを制御するようになっています。ネットワーク管理者は、ユーザ ID、およびネットワーク アクセス タイプとネットワークにアクセスするために使用するマシンのセキュリティに関連付けられた、柔軟な許可ポリシーを提供するソリューションを模索しています。さらに、もっとも重要な機能として、貴重なネットワーク リソースが不必要かつ過度に使用されるのを阻止するために、ネットワーク ユーザの接続を集中的に追跡およびモニタする機能が必要です。

Cisco Secure ACS は、スケーラビリティおよびパフォーマンスに優れたアクセス制御サーバであり、統合型の RADIUS サーバまたは TACACS+ サーバとして機能します。Cisco Secure ACS は、認証、ユーザおよび管理者のアクセス権限、およびポリシー制御などを統合するアイデンティティ管理機能を提供し、アクセス セキュリティを強化します。これにより、柔軟性、機動性、セキュリティ、およびユーザの生産性が大幅に向上します。また、ユーザがネットワークにアクセスする方法に関係なく、すべてのユーザに統一されたセキュリティ ポリシーを適用します。Cisco Secure ACS は、ネットワークへのユーザ アクセスおよびネットワーク管理者によるアクセスの増加に伴う管理の負担を軽減します。Cisco Secure ACS では、すべてのユーザ アカウントを 1 つの中央データベースで管理することで、すべてのユーザのアクセス権を一元的に制御し、ネットワーク全体で数百または数千のアクセス ポイントに同じ情報を提供します。Cisco Secure ACS は、アカウントング サービスとして、ネットワーク ユーザの動作を詳細にレポートおよびモニタする機能を提供し、ネットワーク上のすべてのアクセス接続とデバイス構成の変更を記録します。Cisco Secure ACS は、有線および無線 LAN、ダイヤルアップ、ブロードバンド、コンテンツ、ストレージ、Voice over IP (VoIP)、ファイアウォール、VPN など、さまざまなアクセス方式をサポートします。

Cisco Secure ACS は、Cisco Identity-Based Networking Services (IBNS) アーキテクチャの主要なコンポーネントです。Cisco IBNS は、802.1X (ポートベースのネットワーク アクセス制御を行うための IEEE 標準) や Extensible Authentication Protocol (EAP) などのポート セキュリティ標準に基づいており、従来はネットワーク境界で管理されていた Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントング) セキュリティを強化し、LAN 内のすべての接続ポイントにまで広げました。この新しいアーキテクチャでは、シスコ スイッチと無線アクセス ポイントが RADIUS プロトコルを介して Cisco Secure ACS に問い合わせを行うため、新しいポリシー制御 (ユーザごとのリソース割り当て制限、VLAN 割り当て、および Access-Control List [ACL; アクセス制御リスト]) を組み入れることが可能となります。

Cisco Secure ACS は、Cisco Network Admission Control (NAC) の主要なコンポーネントでもあります。Cisco NAC は、シスコシステムズが推進する業界のイニシアティブです。ネットワーク インフラストラクチャを使用して、ネットワーク コンピューティング リソースにアクセスするすべてのデバイスをセキュリティ ポリシーに適合させ、それによって、ウイルスやワームによる被害を最小限に食い止めます。NAC ソリューションを使用すれば、所定のセキュリティ ポリシーに準拠した信頼できるエンドポイント デバイス (PC、サーバ、PDA など) に対してのみネットワーク アクセスを許可し、不適切なデバイスのアクセ

スを制限できます。Cisco NAC は、シスコ自己防衛型ネットワーク構想の一部であり、レイヤ 2 およびレイヤ 3 ネットワークでのネットワーク アドミッション制御を可能にするためのインフラストラクチャです。将来的には、エンドポイントとネットワーク セキュリティの相互動作をさらに拡張し、感染の拡散を抑制する機能が組み込まれます。この革新的な機能は、ポリシーに適合したシステムが攻撃を受けた場合、不正なシステムまたは感染したシステムの状態をレポートすることを可能にします。そのため、感染したシステムをネットワークの他の部分から動的に隔離し、ウイルス、ワーム、およびさまざまな脅威の拡散を大幅に抑制できます。

Cisco Secure ACS は強力なアクセス制御サーバであり、WAN または LAN 接続を拡張しようとする企業に対して、パフォーマンスおよびスケーラビリティに優れたさまざまな機能を提供します。表 1 に、Cisco Secure ACS の主な利点を示します。

表 1 Cisco Secure ACS の主な利点

利点	説明
使いやすさ	Web ベースのユーザ インターフェイスにより、ユーザ プロファイル、グループ プロファイル、および Cisco Secure ACS の設定全般を容易に行えます。
スケーラビリティ	大規模なネットワーク環境に対応するように設計されており、冗長サーバ、リモート データベース、および データベース レプリケーションとバックアップ サービスをサポートします。
拡張性	Lightweight Directory Access Protocol (LDAP) 認証転送により、Sun、Novell、Microsoft などの主要なディレクトリ ベンダーが提供するディレクトリに格納されたユーザ プロファイルを使った認証が可能となります。
管理性	Windows Active Directory をサポートしているため、Windows のユーザ名とパスワード管理を利用できます。また、Windows Performance Monitor を使用して、リアルタイムの統計情報を表示できます。
運用性	Cisco Secure ACS の各管理者に異なるアクセス レベルを割り当て、ネットワーク デバイスをグループ化することにより、制御を簡単にし、柔軟性を最大限に高めます。これにより、ネットワーク内のすべてのデバイスで、セキュリティ ポリシーの実行および変更が容易になります。
柔軟性	Cisco IOS [®] ソフトウェアには AAA サポートが組み込まれているため、Cisco Secure ACS は、シスコ製ネットワーク アクセス サーバのほとんどで使用できます (Cisco IOS ソフトウェア リリースが RADIUS または TACACS+ をサポートしている必要があります)。
統合性	Cisco IOS ルータおよび VPN ソリューションとの緊密な連携により、マルチシャーシ マルチリンク ポイント ツーポイント プロトコル (PPP)、Cisco IOS ソフトウェアのコマンド実行権限などの機能を提供します。
サードパーティ製品のサポート	RFC に準拠した RADIUS インターフェイスを提供するすべての OTP ベンダー (RSA、PassGo、Secure Computing、ActiveCard、Vasco、CryptoCard など) のトークン サーバをサポートします。
制御	時間帯、ネットワークの使用、ログインしているセッション数、および曜日によるアクセス制限を動的に割り当てることができます。

機能と利点

Cisco Secure ACS 4.0 は、次の新機能と利点を備えています。

- Cisco NAC のサポート** — Cisco Secure ACS 4.0 は、NAC 導入時にポリシー決定ポイントとして機能します。設定可能なポリシーを使用して、Cisco Trust Agent から受け取ったクレデンシャルを評価し、ホストの状態を検証して、ユーザごとの判断結果をネットワーク アクセス デバイスへ送信します。判断結果には、ACL、ポリシーベースの ACL、プライベート VLAN 割り当てがあります。ホスト クレデンシャルの評価時には、OS のパッチ レベル、アンチウイルス DAT ファイルのバージョンなど、さまざまな固有のポリシーを適用できます。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。それによって、適切なエージェント テクノロジーを装備していないホストも、ネットワーク アクセスを許可する前に、サードパーティの監査製品によって監査することができます。Cisco Secure ACS ポリシーの適用範囲は、Cisco Secure ACS がクレデンシャルを転送する外部ポリシー サーバにまで広げることができます。たとえば、アンチウイルス ベンダー固有のクレデンシャルは、そのベンダーのアンチウイルス ポリシー サーバに転送し、監査ポリシー要求は監査ベンダーに転送することができます。

- スケーラビリティの改善** — Cisco Secure ACS 4.0 は、業界標準の RDMBS システムを使用するようにアップグレードされたため、サポートされるデバイス (AAA クライアント) 数は 10 倍まで、ユーザ数は 3 倍まで増えました。また、Cisco Secure ACS がサポートするプロトコルポートフォリオのパフォーマンス (1 秒あたりのトランザクション数) が大幅に向上しました。
- プロファイルベースのポリシー** — Cisco Secure ACS 4.0 は、ネットワーク アクセス プロファイルと呼ばれる新機能をサポートします。この機能を使用して、管理者は、ネットワークの場所、ネットワーク デバイス グループのメンバーシップ、プロトコル タイプ、またはユーザが接続時に経由するネットワーク デバイスによって送信された特定の RADIUS 属性値に従って、アクセス要求を分類できます。さらに、認証、アクセス制御、および許可に関するポリシーを特定のプロファイルにマッピングできます。プロファイルベースのポリシーの例として、無線アクセスとリモート (VPN) アクセスに異なるアクセス ポリシーを適用することができます。
- 拡張レプリケーション コンポーネント** — Cisco Secure ACS 4.0 では、レプリケーションが改善され、拡張されました。管理者は、ネットワーク アクセス プロファイル、およびポストチャ妥当性確認設定、AAA クライアントとホスト、外部データベース設定、グローバル認証設定、ネットワーク デバイス グループ、辞書、共有プロファイル コンポーネント、追加のロギング属性など、関連するすべての設定を複製できます。
- EAP-Flexible Authentication via Secure Tunneling (FAST) の拡張サポート** — EAP-FAST は、シスコによって開発され公開された新しいタイプの IEEE 802.1X EAP であり、強力なパスワード ポリシーを実行できないお客様や 802.1X EAP タイプの導入を考えているお客様に有効です。このようなお客様は、デジタル認証を必要とせず、さまざまなタイプのユーザおよびパスワード データベースを使用でき、パスワードの失効および変更をサポートし、柔軟性があり、さらに導入と管理が容易なタイプの 802.1X EAP を必要としています。たとえば、お客様が、強力なパスワード ポリシーを実行できないため、証明書を使用していない場合は、EAP-FAST に移行することで、辞書攻撃からの保護が可能となります。Cisco Secure ACS 4.0 では、各種無線クライアント アダプタに対応する EAP-FAST サブリカントのサポートが追加されています。
- ダウンロード可能な IP ACL** — Cisco Secure ACS 4.0 では、この機能をサポートするすべてのレイヤ 3 ネットワーク デバイスでもユーザごとの ACL サポートが可能となります。このようなデバイスには、Cisco PIX[®] セキュリティ アプライアンス、Cisco VPN ソリューション、および Cisco IOS ルータなどがあります。これによって、ユーザまたはグループごとに適用される一連の ACL が定義できます。この機能は、適切な ACL ポリシーを実行できるようにすることで、NAC のサポートを補完します。ネットワーク アクセス フィルタとともに使用すると、ダウンロード可能な ACL をデバイスごとに設定できるため、ユーザまたはアクセス デバイスに固有の ACL を適用できます。
- Certification Revocation List (CRL; 証明書失効リスト) の比較** — Cisco Secure ACS 4.0 は、X.509 CRL プロファイルを使用した証明書失効をサポートします。CRL は、失効した証明書を識別するタイムスタンプ付きのリストで、認証局または CRL の発行者によって署名され、パブリック リポジトリで公開されています。Cisco Secure ACS 4.0 は、LDAP または HTTP を使用して、設定された CRL Distribution Point (CDP) から CRL を定期的に取得し、EAP-Transport Layer Security (EAP-TLS) 認証時に使用できるように保存します。EAP-TLS 認証時にユーザが提示した証明書が、取得した CRL に存在する場合、Cisco Secure ACS はそれを認証せず、ユーザのアクセスを拒否します。この機能は、組織変更が頻繁にある場合に特に重要であり、不正なネットワークの使用から貴重な企業資産を保護します。
- Machine Access Restrictions (MAR)** — Cisco Secure ACS 4.0 には、Windows マシン認証の拡張機能として MAR が含まれています。Windows マシン認証が有効な場合、MAR を使用することにより、Windows 外部ユーザ データベースを使用して認証を行う EAP-TLS ユーザおよび Microsoft Protected Extensible Authentication Protocol (PEAP) ユーザの権限を制御できます。設定された時間内であればマシン認証を通過していないコンピュータを使用してネットワークにアクセスするユーザを特定のユーザ グループとして許可します。必要に応じて、許可を制限するように設定することもできます。ネットワーク アクセスをまとめて拒否することもできます。
- Network Access Filtering (NAF)** — Cisco Secure ACS 4.0 には、新しいタイプの共有プロファイル コンポーネントとして NAF が組み込まれています。NAF を使用すると、ネットワーク デバイス名、ネットワーク デバイス グループ、またはネットワーク デバイスの IP アドレスに基づいて、ネットワーク アクセス制限およびダウンロード可能な ACL を柔軟に適用することができます。IP アドレスに基づいて NAF を適用する場合には、IP アドレスの範囲とワイルドカードを使用して指定することもできます。以前は、すべてのデバイスに対して同一のアクセス制限または ACL を使用する必要がありましたが、この機能により、ネットワーク アクセス制限とダウンロード可能な ACL をきめ細かく設定できます。NAF によって可能になる柔軟なネットワーク デバイス制限ポリシーの定義は、大規模なネットワーク環境に共通の要件です。

- ・ シスコ ハードウェア デバイスの追加サポート — Cisco Secure ACS 4.0 には、Cisco Wireless LAN Controller と Cisco ASA 5500 シリーズのサポートが含まれます。

システム要件

Cisco Secure ACS には、Cisco Secure ACS Windows と Cisco Secure ACS Solution Engine という 2 つのオプションがあります。Cisco Secure ACS Solution Engine は、Cisco Secure ACS ライセンスがプリインストールされ、セキュリティが強化された 1 RU のアプリケーションです。

Cisco Secure ACS for Windows を実装する場合、表 2 に示す最小ハードウェア要件を満たす Windows サーバが必要です。また、英語 OS 上での動作のみサポート対象となっています。

表 2 Cisco Secure ACS for Windows の最小サーバ仕様

仕様	最小要件
プロセッサ速度	Pentium 4 プロセッサ、1.8 GHz 以上
メモリ	1 GB 以上の RAM
ハードドライブ	250 MB 以上の空きディスク容量
ディスプレイ解像度	800 × 600 以上 (256 色)

発注情報

Cisco Secure ACS は、世界各国の正規のシスコ製品販売チャネルから購入できます。Cisco Secure ACS Windows には、Microsoft Windows ワークステーションへのインストールに必要なコンポーネントがすべて含まれています。ただし、現在は、英語 OS のみをサポートしています。Cisco Secure ACS Solution Engine は、Cisco Secure ACS ソフトウェア ライセンスがプリインストールされた状態で出荷されます。製品番号については、Cisco Secure ACS 4.0 製品情報を参照してください。付属の Remote Agent は英語 OS 上での動作のみサポート対象となります。

シスコ製品の購入方法の詳細は、「[発注方法](#)」を参照してください。

サービスおよびサポート

シスコは、お客様のネットワークを支援するためのさまざまなサービスプログラムを提供しています。シスコの画期的なプログラムは、スタッフ、プロセス、ツール、およびパートナーを統合した独自のサポート体制のもとに提供され、お客様からの高い支持と信頼を得ています。シスコは、お客様のネットワークへの投資を最大限に活用し、ネットワーク運用を最適化するとともに、最新アプリケーションに対応できるようにネットワークを整備し、よりインテリジェントなネットワークを構築することによって、お客様の事業拡大を支援しています。シスコが提供するサービスおよびサポートの詳細は、[Cisco Technical Support Services](#) をご覧ください。

その他の情報

製品の詳細については、<http://www.cisco.com/jp/product/hs/security/acs/> のセキュリティ製品から ACS のページをご覧ください。

©2005 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
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。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/go/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先