データ シート

Cisco Secure Access Control Server Version 3.3 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、包括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 サービスを提供します。これは、すべての企業ユーザ、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を統合および制御するレイヤです。

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、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。インターネットの利用が増加するにつれて、ネットワーク管理者は、セキュアなトランザクションを保証し、ウィルスや DoS 攻撃の広がりを防ぐために、ユーザだけでなくデバイスについても認証しなければならないという課題に直面しています。このような問題は、ネットワークの境界だけでなく、ネットワークの内部にも存在します。IEEE 802.11 無線 LAN や常時接続の高速インターネット接続（DSL、ケーブルなど）が普及したことで、組織のネットワーク内部では、これらの問題がさらに深刻になっています。このような、どこにでも存在しうるセキュリティの脆弱性を緩和するためにアイデンティティ ネットワーキング テクノロジーへの投資を行うことは、運用および投資回収率のいずれの観点からも、検討に値します。

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は、アクセス制御管理ソリューションにおける新しい分野を生み出しています。企業では、公開鍵インフラストラクチャや二因子認証など、強力な形式の認証を使用することで、パブリック ネットワークや VPN 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、エンド ポイントのユーザの身元だけでなく、ユーザがアクセスするサービスの種類や、ネットワークへのアクセスに使用するマシンの種類にも及ぶ、柔軟な許可ポリシーを提供できるソリューションを模索しています。また、ユーザが接続に使用するアクセス手段にかかわらず、ネットワーク ユーザの動作を追跡およびモニタする機能は、貴重なネットワーク リソースの不必要な使用や過度な使用を識別するために非常に重要です。

Cisco® Secure Access Control Server（ACS）を使用すれば、アイデンティティ ネットワーキングを実現し、ユーザまたはデバイスに合わせたサービスを提供するネットワークにすることができます。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、中央集中型の RADIUS サーバまたは TACACS+ サーバとして機能します。Cisco Secure ACS は、中央集中型のアイデンティティ ネットワーキング ソリューションにより、認証、ユーザまたは管理者によるアクセス、およびポリシー制御を組み合わせることで、アクセス セキュリティを拡張します。これにより、優れた柔軟性と機動性を実現し、セキュリティを向上させ、ユーザの生産性を高めることができます。Cisco Secure ACS は、ネットワークへのユーザ アクセスおよび管理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、アカウンティング 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することで、IT 運用のコストを削減します。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、VoIP、ファイアウォール、VPN など、さまざまなアクセス接続タイプをサポートします。

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、アカウンティング）セキュリティを強化し、LAN 全体にまで広げました。この新しいアーキテクチャでは、ユーザごとのリソース割り当て制限、VLAN、ACL などを新しいポリシー制御として組み入れることが可能となり、認証システム（スイッチ、無線アクセス ポイントなど）は RADIUS クライアントとして機能して AAA サーバに対してこれらの制御に関する問い合わせを行います。

Cisco Secure ACS は、Cisco Network Admission Control（NAC）ソリューション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開発したマルチベンダー プログラムで、ウィルスやワームなど、新しいセキュリティの脅威による被害を防ぐことを目的としています。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 端末、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、不適合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第 1 段階として位置付けられるものであり、後の段階の基盤となります。今後の段階では、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拡張して、感染を抑制する機能が組み込まれます。これにより、システムに準拠したエンドポイントまたはその他のシステム要素から、不正なシステムまたは感染したシステムによる不正使用が報告されるようになります。シスコでは、このインテリジェントな機能を使用することで、感染したシステムをネットワークのその他のシステムから動的に隔離し、ウィルス、ワーム、およびその他の脅威の伝播を最小化できると考えています。

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考える企業に対して、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

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 を容易に設定できます。
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構築されており、冗長サーバ、リモート データベース、およびユーザ データベース 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 および Windows NT データベース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、制御を簡単にして、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 ソフトウェアのリリースが、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、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（ワンタイム パスワード）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。

ACS Version 3.3 の主な機能

Cisco NAC のサポート — Cisco Secure ACS 3.3 は、NAC におけるポリシー決定ポイントとして機能します。Cisco Secure ACS は、設定されたポリシーを使用して、Cisco Trust Agent によって送信された証明書を評価し、ホストの状態を判断して、ホストの状態に適した AAA クライアント ACL を送信します。ホスト証明書の評価により、オペレーティング システムのパッチ レベル、アンチウィルス 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実行できます。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。ポリシーは、Cisco Secure ACS によってローカルで評価することもできますし、Cisco Secure ACS から外部ポリシー サーバへ証明書を転送し、そのサーバから評価結果を受け取ることもできます。たとえば、あるアンチウィルス ベンダー固有の証明書は、そのベンダーのアンチウィルス ポリシー サーバに転送できます。

無線認証に対する EAP-Flexible Authentication via Secure Tunneling（FAST）のサポート — EAP-FAST は、シスコによって開発され公開された新たなタイプの 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、Cisco EAP を使用しているお客様が、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でも、EAP-FAST に移行することにより、辞書攻撃からの保護が可能となります。Cisco Secure ACS 3.3 には、シスコ製品と互換性のあるクライアント デバイスおよび Cisco Aironet® 802.11a/b/g WLAN クライアント アダプタで使用できる、EAP-FAST サプ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 Version 3.3 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（Cisco PIX® Firewall、Cisco VPN ソリューション、および Cisco IOS ルータ）でユーザごとの ACL サポートが可能となります。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。NAF とともに使用すると、ダウンロード可能な ACL を AAA クライアント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 3.3 では、X.509 CRL プロファイルを使用した、証明書失効のサポートが追加されています。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 3.3 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-TLS 認証時に使用できるよう保存します。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、ユーザへ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 3.3 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 3.3 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、AAA クライアント名、ネットワーク デバイス グループ、または AAA クライアントの 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 アドレスの範囲ワイルドカードでの指定も可能です。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。

Cisco Security Agent と Cisco Secure ACS Solution Engine の統合 — Cisco Secure ACS 3.3 Solution Engine には、スタンドアロンの Cisco Security Agent がプリインストールされています。アプライアンスのベース イメージとして組み込まれたことにより、Day Zero 攻撃から Cisco Secure ACS Solution Engine を保護できます。Cisco Security Agent によって利用可能になる新しい動作ベースのテクノロジーは、ウィルスやワームなどの常に変化する脅威から Cisco Secure ACS Solution Engine を保護します。

レプリケーション拡張機能 — Cisco Secure ACS 3.3 を使用すると、ユーザ データベースとグループ データベースを個別に複製できます。ユーザ アカウントへの変更を複製した場合、グループを複製する必要はありません。同様に、グループを複製した場合、ユーザを複製する必要はありません。このように個々の複製が可能となったため、レプリケーション イベント中に Cisco Secure ACS 間で送信されるデータ量が削減されます。また、Cisco Secure ACS レプリケーション パートナーとのネットワーク接続に時間がかかる環境に対応できるように、設定変更可能なレプリケーション タイムアウト オプションが追加されました。

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 のアプライアンスです。

Cisco Secure ACS 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 Windows の最小サーバ仕様

プロセッサ速度	550 MHz 以上
メモリ	256 MB 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）

Cisco Secure ACS Solution Engine は、表 3 に示す仕様に準拠した Cisco 1112 プラットフォームで動作します。

表 3
Cisco Secure ACS Solution Engine サーバの仕様

プロセッサ速度	Pentium 4、3.2 GHz
メモリ	1 GB の RAM
ハード ドライブ	80 GB の空きディスク容量
インターフェイス	内蔵 10/100 イーサネット コントローラ× 2、フロッピー ディスク ドライブ× 1

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 Version 3.3 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。シスコの画期的なサービスプログラムは、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/ のセキュリティ製品から ACS のページをご覧ください。その他のお問い合わせやご質問については、シスコ製品販売代理店までお願いいたします。

CISCO SYSTEMS

シスコシステムズ株式会社

お問合せ先

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

04.08