Cisco Secure Access Control System 5.6

製品概要

Cisco® Secure Access Control System（ACS）は、企業のネットワーク アクセス ポリシーとアイデンティティ戦略を結び付けます。Cisco Secure ACS は、世界で最も信頼された、ポリシー ベースの企業アクセスおよびネットワーク デバイスの管理コントロール プラットフォームであり、Fortune 500 企業のほぼ 80 % に導入されています。

Cisco TrustSec® ソリューションの主要コンポーネントの 1 つである Cisco Secure ACS は、RADIUS および TACACS+ サービスを提供する非常に高度化されたポリシー プラットフォームです。アクセス コントロール管理とコンプライアンスに関する今日の要求を満たすために必要な、ますます複雑化するポリシーに対応しています。Cisco Secure ACS により、デバイス管理や、無線/有線 IEEE 802.1x、およびリモート（VPN）ネットワーク アクセスを目的としたアクセス ポリシーの集中管理が可能になります。図 1 は、Cisco UCS® C220 M3 ラック サーバ プラットフォームを基盤とした、Cisco Secure Network Server（SNS）3415 アプライアンスです。

Cisco Secure ACS 5.6 ソフトウェアは、販売終了となった Cisco Secure ACS Engine 向けの既存の Cisco 1120 と 1121 アプライアンスに加え、Cisco SNS 3415 および 3495 アプライアンスで実行することができます。

図 1　Cisco Secure Access Control System 5.6 ソフトウェア向けの Cisco Secure Network Server 3415 アプライアンス

日常業務の遂行において、企業ネットワークへの依存度はますます高まっています。また、ネットワークにアクセスできる方法が増加するに伴い、企業においては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。ネットワーク セキュリティの責任者と管理者は、ユーザ ID だけではなく、ネットワーク アクセス タイプ、アクセスが必要な使用時間帯、ネットワークへのアクセスに使用するマシンのセキュリティなどのコンテキストにも関連付けられた柔軟な認証/許可ポリシーに対応できるソリューションを必要としています。さらに、企業のコンプライアンスに準拠するよう、ネットワーク デバイスの使用状況を効果的に監査し、デバイス管理のアクティビティをモニタするとともに、ネットワーク全体にデバイス アクセス ポリシーのより広範な可視性と制御を提供する必要性がますます高まっています。

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 ポリシー システムです。デバイス管理、認証、ユーザ アクセス ポリシーなどの機能を集中管理し、これらの機能の管理やサポートの負担を軽減します。

機能と特長

Cisco Secure ACS 5.6 は、ポリシー アドミニストレーション ポイント（PAP）およびポリシー デシジョン ポイント（PDP）として機能し、ポリシーベースのネットワーク デバイスのアクセス制御を実現し、以下のような多数のアイデンティティ管理機能を提供します。

- 標準のコンプライアンスに必要とされる監査機能とレポート機能を完備した、IPv4 および IPv6 ネットワークにおける比類のない、柔軟で詳細なデバイス管理
- 複雑なポリシー要求に柔軟に対応する、属性主導でルールベースの強力なポリシー モデル
- 直感的なナビゲーションとワークフローを実現し、IPv4/IPv6 両クライアントからアクセス可能で軽量な Web ベースの GUI

- 優れたコントロールと可視性を可能にする、統合された高度なモニタリング、レポート、トラブルシューティング機能
- 外部のアイデンティティおよびポリシー データベース（Microsoft Active Directory および Lightweight Directory Access Protocol（LDAP）でアクセス可能なデータベースなど）との統合により、ポリシー構成とメンテナンスがシンプル化
- 大規模な展開を可能にし、可用性の高いソリューションを提供する分散型展開モデル

ルールベースのポリシー モデル Cisco Secure ACS 5.6 は、多様な条件下でのさまざまな権限付与規則の適用に対応します。そのため、ポリシーはコンテキスト対応型で、権限の付与は 1 つのグループ メンバーシップによるものに限定されることはありません。統合機能により、外部データベースの情報をアクセス ポリシー ルールで直接参照でき、属性をポリシー条件と許可規則の両方で使用することができます。

Cisco Secure ACS 5.6 はアクティビティおよびシステム ヘルス情報の収集と報告を集中管理し、分散型展開の最大限の管理容易性を実現します。モニタリングや診断などの事前対応型の動作、および報告やトラブルシューティングなどの事後対応型の動作にも対応しています。展開全体にわたるセッション モニタリング、しきい値ベースの通知、エンタイトルメント レポート、診断ツールなどの高度な機能を搭載しています。

表 1 に、Cisco Secure ACS 5.6 の主な機能と利点を示します。

表 1　Cisco Secure ACS 5.6 の主な機能と利点

機能	利点
アクセス コントロールおよび機密保持における完全なソリューション	Cisco Secure ACS 5.6 は、ポリシー コンポーネント、インフラストラクチャ適用コンポーネント、エンドポイント コンポーネント、プロフェッショナル サービスなどの Cisco TrustSec コンポーネントと併用できます。
認証、許可、アカウンティング（AAA）プロトコル	Cisco Secure ACS 5.6 は、ネットワーク アクセス コントロール用の RADIUS と、ネットワーク デバイス アクセス コントロール用の TACACS+ の、2 つの異なる AAA プロトコルをサポートします。Cisco Secure ACS は、ネットワーク全体にアクセス ポリシーを適用する単一のシステムです。Payment Card Industry（PCI）などの標準のコンプライアンスに必要とされるネットワーク デバイス構成と変更管理を強化します。Cisco Secure ACS 5.6 の AAA 機能は、IPv4 と IPv6 の両方のネットワークで TACACS+ ベースのデバイス管理に対応できます。
データベース オプション	Cisco Secure ACS 5.6 は、Microsoft Active Directory サーバ、LDAP サーバ、RSA トークン サーバなどの、既存の外部アイデンティティ リポジトリとの統合に加え、統合型ユーザ リポジトリをサポートします。この機能により、Cisco Secure ACS クラスタで複数の LDAP サーバが使用でき、Cisco Secure ACS ノード（インスタンス）ごとにプライマリとバックアップの LDAP サーバが使用できるようになります。さらに、各 Cisco Secure ACS インスタンスを、別の Microsoft Active Directory ドメインに接続できます。Cisco Secure ACS 5.6 では、Microsoft Active Directory サーバと LDAP サーバに複数値の属性を定義できます。これにより、Microsoft Active Directory のブール値を使用することや、Microsoft Active Directory の IPv4 アドレス属性に値を代入することなどが可能になります。複数のデータベースを同時に使用できることで、アイデンティティ ストア シーケンスによるアクセス ポリシーの強化に、優れた柔軟性を発揮します。さらに、外部の Microsoft Active Directory データベースと LDAP データベースに Cisco Secure ACS の管理者を追加し、これらのアイデンティティ ストアを使用して認証することができます。
認証プロトコル	Cisco Secure ACS 5.6 では、PAP、MS-CHAP、拡張認証プロトコル（EAP）-MD5、Protected EAP（PEAP）、EAP-Flexible Authentication through Secure Tunneling（FAST）、EAP-Transport Layer Security（TLS）、PEAP-TLS などの、さまざまな認証プロトコルをサポートします。また、CHAP/MSCHAP プロトコルでの TACACS+ 認証、LDAP サーバで TACACS+ と EAP-GTC を使用する際の PAP ベースのパスワード変更をサポートします。
アクセス ポリシー	Cisco Secure ACS 5.6 は、ルールベースの属性主導ポリシー モデルをサポートしており、認証プロトコル要件、デバイス制限、時間帯による制限、およびその他のアクセス要件などを含むアクセス ポリシー コントロールに、大幅に強化された能力と柔軟性を発揮します。Cisco Secure ACS は、ダウンロード可能アクセス コントロール リスト（dACL）、VLAN 割り当て、およびその他の許可パラメータを適用できます。さらに、アイデンティティ、グループ マッピング、および許可ポリシーのルールに、Cisco Secure ACS で使用可能な任意の 2 種類の属性値の比較を利用できます。
中央集中型の管理	Cisco Secure ACS 5.6 は、完全に再設計された、軽くて使いやすい Web ベースの GUI を装備しています。効率的な増分レプリケーション方式により、変更をプライマリ システムからセカンダリ システムに迅速に反映し、分散型展開の全体にわたって中央集中型の管理を実現します。ソフトウェア アップグレードも GUI で管理でき、プライマリ システムによってセカンダリ インスタンスへ配布できます。
規模の大きい Cisco Secure ACS 導入での高可用性のサポート	Cisco Secure ACS 5.6 は、1 つの Cisco ACS クラスタで最大 22 のインスタンス（1 つのプライマリ インスタンスと 21 のセカンダリ インスタンス）をサポートします。これらのいずれかのインスタンスをホット（アクティブ）スタンバイ システムとして機能させ、元のプライマリ システムで障害が発生した場合に手動でプライマリ システムに移行することができます。
プログラマチック インターフェイス	Cisco Secure ACS 5.6 は、内部データベース内のユーザとアイデンティティ グループ、ネットワーク デバイス、およびホスト（エンドポイント）の作成、読み出し、更新、削除の操作に対するプログラマチック インターフェイスをサポートします。さらに、同じ Web サービス API で、Cisco Secure ACS の管理者と役割のリストをエクスポートする機能も追加できます。

機能	利点
モニタリング、報告、トラブルシューティング	Cisco Secure ACS 5.6 には、Web ベースの GUI からアクセス可能な、モニタリング、報告、トラブルシューティングの統合コンポーネントが含まれています。このツールにより、設定されたポリシーおよび認証と許可のアクティビティにおいて、ネットワーク全体にわたり優れた可視性が提供されます。ログは、他のシステムでも使用できるよう表示およびエクスポートが可能です。Cisco Secure ACS 5.6 での新しいレポート生成メカニズムにより、パフォーマンスが著しく向上し、さらに使いやすくなりました。ただし、Cisco UCS ACS 5.5 以前のリリースでは使用できた、レポートの「対話型ビューア」オプションによるレポートのカスタマイズ機能はありません。「カラムの表示/非表示」や「カラムの並べ替え」などの一部のオプションは、Cisco Secure ACS の後続リリースやパッチで追加される予定です。
プロキシ サービス	Cisco Secure ACS 5.6 は、ネットワーク アクセス デバイス（NAD）から外部サーバに着信 AAA リクエストを転送し、このようなリクエストを開始した NAD にそのサーバからの応答を戻すことによって、外部 AAA サーバの RADIUS または TACACS+ プロキシとして機能できます。Cisco Secure ACS 5.6 には、外部 AAA サーバから返信された応答だけでなく、外部 AAA サーバに送信されたプロキシされている AAA リクエストで、RADIUS 属性を追加および上書きする機能もあります。
プラットフォーム オプション	Cisco Secure ACS 5.6 は、クローズドの強化された Linux ベースの Cisco SNS 3415 と 3495 アプライアンスとして、または VMware ESX/ESXi 5.1/5.5 用のソフトウェア オペレーティング システム イメージとして利用できます。また、販売終了となった以前の Cisco Secure ACS Engine 用 Cisco 1121 アプライアンスでもサポートされています。

システム要件

Cisco Secure ACS 5.6 は、セキュリティ機能が強化された 1 ラック ユニット（1 RU）の Linux ベースのアプライアンスとして利用できます。Cisco SNS 3415 と 3495 アプライアンス、および以前の Cisco Secure ACS Engine 用 Cisco 1121 アプライアンスには、Cisco Secure ACS ソフトウェアがプリインストールされています。また、VMware ESX/ESXi 5.1/5.5 の仮想マシンへのインストール用に、ソフトウェア オペレーティング システム イメージとしても利用できます。表 2 と表 3 に、Cisco SNS 3415 と 3495 アプライアンスのシステム仕様をそれぞれ示します。VMware ESXi システムの要件については、表 4 を参照してください。

表 2　Cisco SNS 3415 アプライアンスの仕様

コンポーネント	仕様
CPU	2.4-GHz Intel E5-2609、80 ワット（W）、4 コア、10-MB キャッシュ、DDR3、1600 MHz
システム メモリ	合計 16 GB：4 GB DDR3 1600 MHz RDIMM X 4
ハード ディスク ドライブ（HDD）	600 GB 6 Gbps SAS 10,000 RPM HDD
ソフトウェア RAID コントローラ	Cisco Secure ACS アプリケーション ソフトウェアでは使用されない
光学式ストレージ	なし
ネットワーク接続	1 GB ネットワーク インターフェイス カード（NIC）インターフェイス X 4 **注：**管理機能に使用できるのは Ethernet0 のみ。すべてのインターフェイスが AAA リクエストをリッスンします。
I/O ポート	• 背面パネル：DB9 シリアル ポート X 1、USB 2.0 ポート X 2、DB15 VGA ポート X 1、NIC コネクタ • 前面パネル：キーボード、ビデオ、およびマウス（KVM）コンソール コネクタ（USB ポート X 2）、VGA ポート X 1、シリアル ポート X 1
トラステッド プラットフォーム モジュール	はい
SSL アクセラレーション カード	いいえ
ラックマウント	4 ポスト マウント
物理寸法（1RU）（高さ X 幅 X 奥行）	1.7 X 16.92 X 28.5 インチ（4.32 X 43.0 X 72.4 cm）
重量	12.2 kg（27.1 ポンド）

電力	仕様
電源数	1
電源容量	650 W 汎用（入力電圧：90 ～ 260 V、47 ～ 63 Hz）

環境	仕様
動作温度範囲	5 ～ 40 °C（41 ～ 104 °F）、高度が 305 m（1000 フィート）上がるごとに最高温度は 1 °C 低下
動作高度	0 ～ 3,000 m（0 ～ 10,000 フィート）

表 3　Cisco SNS 3495 アプライアンスの仕様

コンポーネント	仕様
CPU	2.4 GHz Intel E5-2609 X 2、80 W、4 コア、10 MB キャッシュ、DDR3、1600 MHz
システム メモリ	合計 32 GB：4 GB DDR3 1600 MHz RDIMM X 8
ハード ディスク ドライブ	600 GB 6 Gbps SAS 10,000 RPM HDD X 2
ハードウェア RAID コントローラ	レベル 0 および 1 LSI 2008 SAS RAID メザニン カード
光学式ストレージ	なし
ネットワーク接続	1-GB NIC インターフェイス X 4 **注：**管理機能に使用できるのは Ethernet0 のみ。すべてのインターフェイスが AAA リクエストをリッスンします。
I/O ポート	• 背面パネル：DB9 シリアル ポート X 1、USB 2.0 ポート X 2、DB15 VGA ポート X 1、NIC コネクタ • 前面パネル：KVM コンソール コネクタ（USB ポート X 2）、VGA ポート X 1、シリアル ポート X 1
トラステッド プラットフォーム モジュール	はい
SSL アクセラレーション カード	はい
ラックマウント	4 ポスト マウント
物理寸法（1RU）（高さ X 幅 X 奥行）	1.7 X 16.92 X 28.5 インチ（4. 32 X 43.0 X 72.4 cm）
重量	12.2 kg（27.1 ポンド）

電力	仕様
電源数	2
電源容量	650 W 汎用（入力電圧：90 ～ 260 V、47 ～ 63 Hz）

環境	仕様
動作温度範囲	5 ～ 40 °C（41 ～ 104 °F）、高度が 305 m（1000 フィート）上がるごとに最高温度は 1 °C 低下
動作高度	0 ～ 3,000 m（0 ～ 10,000 フィート）

表 4　Cisco Secure ACS 5.6 VMware 要件

コンポーネント	仕様
VMware バージョン	VMware ESX および ESXi 5.1 および 5.5
CPU	2 CPU（デュアル CPU、Intel Xeon プロセッサ、Core 2 Duo または 2 つのシングル CPU）
システム メモリ	4 GB RAM
ハード ディスク要件	60 ～ 750 GB のユーザ設定が可能（150 GB 以上を推奨）
NIC	Cisco Secure ACS アプリケーションに使用できるネットワーク NIC（1 Gbps）

発注情報

Cisco Secure ACS 製品は、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 5.6 の部品番号および発注情報については、Cisco Secure ACS 5.6 製品情報を参照してください。

シスコ製品の購入方法の詳細は、最寄りのシスコ代理店にお問い合わせいただくか、「購入案内」ホームページを参照してください。

サービスとサポート

シスコは、お客様の成功を支援する幅広いサービス プログラムを用意しています。これらのプログラムは、スタッフ、プロセス、ツール、パートナーを独自に組み合わせたかたちで提供され、お客様から高い評価を受けています。シスコのサービスは、ネットワーク インテリジェンスおよびビジネスの能力を高めるためのネットワーク投資の保護、ネットワーク運用の最適化、および新しいアプリケーションのためのネットワークの準備を支援します。シスコ サービスの詳細については、シスコ テクニカル サポート サービスを参照してください。

詳細情報

Cisco Secure ACS の最新情報は、http://www.cisco.com/jp/go/acs/ をご覧ください。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

C78-732914-00JA 14.12