CHAPTER 1

ACS 5.4 の導入

ここでは、次の内容について説明します。

ACS の概要

ACS は、規格準拠の認証、許可、アカウンティング（AAA）サービスをネットワークに提供するポリシーベースのセキュリティ サーバです。ACS を使用すると、シスコおよびシスコ以外のデバイスとアプリケーションを簡単に管理できます。

有力な企業ネットワーク アクセス コントロール プラットフォームである ACS は、ネットワーク アクセス コントロールと ID 管理の統合ポイントとして機能します。

ACS 5.x では、動的な条件と属性に基づいてネットワーク アクセスを制御できる、ルール ベースのポリシー モデルを提供します。ルール ベースのポリシーは、複雑なアクセス ポリシー ニーズを満たす設計になっています。ACS のルール ベースのポリシー モデルの詳細については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

2 つの主要な AAA プロトコルである RADIUS と TACACS+ のより強力なコンテキストにおいて、ACS では次の基本的な機能領域を提供します。

- RADIUS プロトコルのフレームワークにおいては、ACS ではネットワークへの有線および無線アクセスをユーザおよびホスト マシンごとに制御し、使用されるネットワーク リソースのアカウンティングを管理します。

  ACS では、PAP、CHAP、MSCHAPv1、MSCHAPv2 などの複数の RADIUS ベースの認証方式がサポートされています。さらに、EAP-MD5、LEAP、PEAP、EAP-FAST、EAP-TLS など、EAP プロトコル ファミリの多くのメンバーもサポートされています。

  また、ACS では、PEAP または EAP-FAST と連携する場合、EAP-MSCHAPv2、EAP-GTC、および EAP-TLS もサポートされます。認証方式の詳細については、「Authentication in ACS 5.4」を参照してください。

- TACACS+ プロトコルのフレームワークにおいては、ACS を使用すると、スイッチ、無線アクセス ポイント、ルータ、ゲートウェイなどのシスコおよびシスコ以外のネットワーク デバイスを簡単に管理できます。また、ダイヤルアップ、バーチャル プライベート ネットワーク（VPN）、ファイアウォールなどのサービスやエンティティの管理にも役立ちます。

ACS は、ネットワークに接続しようとするユーザとデバイスを識別する、ネットワーク内のポイントとなります。この ID 設定は、ローカル ユーザ認証用の ACS 内部 ID リポジトリを使用して直接実行される場合、および、外部 ID リポジトリを使用して実行される場合があります。

たとえば、ACS では、Active Directory を外部 ID リポジトリとして使用してユーザを認証し、ネットワークへのユーザ アクセス権を付与できます。ID の作成およびサポートされる ID サービスの詳細については、第 8 章「ユーザおよび ID ストアの管理」を参照してください。

ACS には、ACS の展開の管理に役立つ高度な監視ツール、レポート ツール、およびトラブルシューティング ツールが備えられています。ACS の監視機能、レポート機能、およびトラブルシューティング機能の詳細については、第 11 章「ACS での監視とレポート」を参照してください。

ACS を使用したデバイス管理およびネットワーク アクセス シナリオの詳細については、第 4 章「ACS を使用した一般的なシナリオ」を参照してください。

Cisco Secure ACS には次の機能があります。

- VPN および無線ユーザのアクセス ポリシーの適用
- デバイス管理の簡略化
- 高度な監視ツール、レポート ツール、およびトラブルシューティング ツールの提供

ACS 5.3 と比較して、ACS 5.4 にはいくつかの変更点および拡張機能があります。新機能および変更された機能の完全なリストは、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/release/notes/acs_54_rn.html

関連トピック

- 「ACS の分散展開」（P.1-2）
- 「ACS 管理インターフェイス」（P.1-3）

ACS の分散展開

ACS 5.4 は、標準の Cisco Linux ベース アプライアンスにあらかじめ搭載された状態で提供され、完全な分散展開をサポートします。

ACS の展開は、単一のインスタンスで構成されることも、複数のインスタンスで構成されることもあります。後者の場合、インスタンスは分散環境に展開され、システム内のすべてのインスタンスが集中管理されます。この場合、1 つの ACS インスタンスが *プライマリ インスタンス*となり、その他の ACS インスタンスは *セカンダリ インスタンス*としてプライマリ インスタンスに登録できます。すべてのインスタンスが展開全体に対する設定を持つため、設定データには冗長性が発生します。

プライマリ インスタンスによって、展開されたインスタンスの設定が集中化されます。プライマリ インスタンスで行った設定変更は、セカンダリ インスタンスに自動的に複製されます。

セカンダリ インスタンスへの *完全複製*を強制実行できます。完全複製は、新しいセカンダリ インスタンスの登録時、およびセカンダリ インスタンスとプライマリ インスタンスの間の複製のギャップが大きい場合に使用されます。

関連項目

- 「ACS 4.x と 5.4 の複製」（P.1-2）

ACS 4.x と 5.4 の複製

ACS 4.x では、プライマリ インスタンスからセカンダリ インスタンスに複製するデータベース オブジェクト タイプ（またはクラス）を選択する必要があります。オブジェクトを複製すると、設定の完全なコピーがセカンダリ インスタンスに作成されます。

ACS 5.4 では、プライマリ インスタンスに加えられたすべての設定変更が、セカンダリ インスタンスに即時に複製されます。*前回の複製後*に行われた設定変更だけがセカンダリ インスタンスに伝播されます。

ACS 4.x では差分複製機能がなく、完全複製機能だけが備えられていたため、複製のためのサービス ダウンタイムが発生しました。ACS 5.4 では、サービス ダウンタイムのない差分複製機能が備えられています。

また、設定変更が複製されなかった場合は、セカンダリ インスタンスへの完全複製を*強制実行*することもできます。完全複製は、新しいセカンダリ インスタンスを登録するとき、およびセカンダリ インスタンスとプライマリ インスタンスの間の複製のギャップが大きい場合に使用されます。

表 1-1 に、ACS 4.x と 5.4 の複製の違いをいくつか示します。

表 1-1　ACS 4.x と 5.4 の複製の違い

ACS 4.x	ACS 5.4
複製するデータ項目を選択できる。	複製するデータ項目を選択できない。デフォルトでは、すべてのデータ項目が複製されます。
マルチレベルまたはカスケード複製がサポートされている。	固定のフラット複製だけがサポートされている。カスケード複製はサポートされていません。
外部データベース設定などの一部のデータ項目は複製されない。	データベース キー、データベース証明書およびマスター キーを除く、すべてのデータ項目が複製される。サーバ証明書、証明書署名要求（CSR）、秘密キーは複製されますが、インターフェイスには表示されません。

分散展開の設定の詳細については、「システムの動作の設定」（P.17-1）を参照してください。

（注）　Network Address Translation（NAT）は、ACS 分散展開環境ではサポートされていません。つまり、プライマリまたはセカンダリ インスタンスのネットワーク アドレスを変換すると、データベースの複製が正しく機能しないことがあり、共有秘密の不一致エラーが表示される場合があります。

ACS のライセンス モデル

ACS を操作するには、有効なライセンスが必要です。Web インターフェイスに初めてアクセスするときに、ACS によって有効なベース ライセンスのインストールを要求するプロンプトが表示されます。分散展開では、各サーバに固有の基本ライセンスが必要です。

インストールできるライセンスの種類の詳細については、「ライセンスの種類」（P.18-35）を参照してください。ライセンスの詳細については、「ライセンスの概要」（P.18-35）を参照してください。

関連項目

- 「ACS の分散展開」（P.1-2）

ACS 管理インターフェイス

ここでは、次の内容について説明します。

- 「ACS Web ベース インターフェイス」（P.1-4）

- 「ACS コマンドライン インターフェイス」（P.1-4）
- 「ACS プログラム インターフェイス」（P.1-5）

ACS Web ベース インターフェイス

ACS Web ベース インターフェイスを使用して、ACS の展開を完全に設定し、監視とレポートの操作を実行できます。Web インターフェイスでは、設定する領域に関わりなく、一貫性のあるユーザ エクスペリエンスが提供されます。

ACS Web インターフェイスは、6.x から 9.x までの Microsoft Internet Explorer の HTTPS 対応バージョンおよび 3.x から 10.x までの Mozilla Firefox バージョンでサポートされます。

新しい Web インターフェイス設計と構成には、次の機能があります。

- ユーザの視点でのポリシー管理に基づいて構成された、新しいポリシー モデルを反映する。新しいポリシー モデルは、ポリシー要素間に以前に存在していた複雑な相互関係が分離されているため、使いやすさが向上しました。

  ポリシー要素とは、たとえば、ユーザ グループ、ネットワーク デバイス グループ（NDG）、ネットワーク アクセス フィルタ、ネットワーク アクセス プロファイルなどです。

- 多くの一般的なシナリオに適用できる論理的な順序で、設定タスクを提示する。

  たとえば、最初に [Policy Elements] ドロワでポリシーの条件と認可を設定したあと、[Policies] ドロワに移動し、定義済みポリシー要素を使用してポリシーを設定します。

- 項目のリストのソートやフィルタリングなどの新しいページ機能を提供する。

詳細については、「Web インターフェイスの使用方法」（P.5-3）を参照してください。

関連トピック

- 「ACS コマンドライン インターフェイス」（P.1-4）

ACS コマンドライン インターフェイス

テキストベースのインターフェイスである ACS コマンドライン インターフェイス（CLI）を使用して、一部の設定および操作タスクと監視を実行できます。ACS 固有の CLI にアクセスするには、ACS 5.4 による管理者認証が必要です。

ACS 以外のコンフィギュレーション モードを使用するには、ACS 管理者である必要はなく、また、ACS 5.4 にログインする必要もありません。ACS コンフィギュレーション モードのコマンド セッションは、診断ログに記録されます。

ACS 5.4 は、Cisco 1121 Secure Access Control System（CSACS-1121）または Cisco 3415 Secure Access Control System（CSACS-3415）で出荷されます。ADE-OS ソフトウェアでは、次のコマンド モードがサポートされています。

- EXEC：これらのコマンドを使用して、システムレベルの操作タスクを実行します。操作タスクとは、たとえば、アプリケーションのインストール、起動、停止、ファイルのコピーとインストール、バックアップの復元、情報の表示などです。

  また、特定の EXEC モード コマンドには、ACS 固有の機能があります。たとえば、ACS インスタンスの開始、ACS ログの表示とエクスポート、ACS 設定の出荷時のデフォルト設定への復元などです。このようなコマンドについては、マニュアルに詳しく記載されています。

- ACS 設定：これらのコマンドを使用して、ACS の管理およびランタイム コンポーネントのデバッグ ログ レベルを設定（イネーブルまたはディセーブル）します。また、システム設定を表示します。
- 設定：これらのコマンドを使用して、ADE-OS 環境のアプライアンス サーバに対して追加の設定タスクを実行します。

（注）　CLI には、設定のリセット オプションがあります。このオプションが発行されると、すべての ACS 設定情報がリセットされますが、ネットワーク設定などのアプライアンス設定は保持されます。

CLI の使用については、『*Command Line Interface Reference Guide for Cisco Secure Access Control System 5.4*』を参照してください。

関連項目

- 「ACS Web ベース インターフェイス」（P.1-4）

ACS プログラム インターフェイス

ACS 5.4 には、ソフトウェア開発者とシステム インテグレータが一部の ACS 機能にプログラムを通じてアクセスできる Web サービスおよびコマンドライン インターフェイス（CLI）コマンドが備えられています。ACS 5.4 では、ACS を監視およびトラブルシューティングするカスタム アプリケーションを作成する場合に使用できる、Monitoring and Report Viewer データベースにもアクセスできます。

UCP Web サービスでは、ACS 内部データベースに定義されているユーザが、最初に認証を受けてから自身のパスワードを変更できます。ACS では、企業に展開できるカスタム Web ベース アプリケーションを作成できるように UCP Web サービスを公開しています。

Monitoring and Report Viewer Web サービスでは、ACS のイベントをトラッキングおよびトラブルシューティングするカスタム アプリケーションを作成できます。

ACS によって提供されている CLI コマンドを使用して、ACS オブジェクトに対する Create, Read, Update, and Delete（CRUD; 作成、読み取り、更新、および削除）操作を実行するシェル スクリプトを開発できます。また、自動化されたシェル スクリプトを作成して、一括操作を実行することもできます。

REST PI（Representational State Transfer Programming Interface）は、ユーザ、ホスト、ID グループ、ネットワーク デバイス、ネットワーク デバイス グループ、およびネットワーク デバイス グループ タイプなどのエンティティを自分の管理アプリケーションで管理し、ACS にこれらのエンティティを移動することができるようにします。このように、これらのエンティティを定義して、その後で独自のシステムや ACS で使用できます。

これらの Web サービスおよびそれらの機能にアクセスする方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/sdk/acs_sdk.html

ACS でサポートされているハードウェア モデル

表 1-2 に、ACS 5.4 でサポートされているハードウェア モデルの詳細を示します。

表 1-2　ACS 5.4 でサポートされているハードウェア モデル

Config	HDD	RAM	NIC
UCS 3415	500 GB	8 GB	2 x 2（4-1 Gb）
IBM 1121	2 x 250 GB	4 GB	4 x 10/100/1000 RJ-45
CAM25-1-2-4	2 x 250 GB	4 x 1 GB	2 x 1 GE
VMware ESX i5.0	60 ～ 750 GB	4 GB	NIC x 2