CHAPTER 2

ACS 4.x から ACS 5.4 への移行

ACS 4.x では、TACACS+ コマンド セットなどのポリシーおよび認証情報は、ユーザおよびユーザ グループ レコードに格納されます。ACS 5.4 では、ポリシーおよび認証情報は独立した共有コンポーネントであり、ポリシーを設定するときに、構築ブロックとして使用します。

新しいポリシー モデルの構築ブロック、つまりポリシー要素を使用してポリシーを再構築すると、新しいポリシー モデルを最大限かつ効率的に活用できます。この方法を使用すると、適切な ID グループ、ネットワーク デバイス グループ（NDG）、条件、認可プロファイル、およびルールを作成することが必要となります。

ACS 5.4 には、ACS 4.x の移行サポート バージョンから ACS 5.4 マシンにデータを転送する、移行ユーティリティが備えられています。ACS 5.4 移行プロセスでは、ACS 5.4 にデータをインポートする前に、手動でデータを解決する管理的介入が必要となる場合があります。

このプロセスは、バージョン ACS 3.x から ACS 4.x へのアップグレード プロセスとは異なります。ACS 3.x から ACS 4.x へのアップグレード プロセスでは、ACS 4.x システムが ACS 3.x と同じ方法で動作するため、管理的介入は不要です。

ACS 5.4 の移行ユーティリティでは、展開内のすべての ACS 4.x サーバを ACS 5.4 に移行する複数インスタンス移行がサポートされています。複数インスタンスの移行の詳細については、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/migration/guide/migration_guide.html

アップグレードは、ACS 5.3 サーバから ACS 5.4 へのデータ転送プロセスです。アップグレード プロセスの詳細については、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/installation/guide/csacs_upg.html

この章の内容は、次のとおりです。

移行プロセスの概要

移行ユーティリティは、次の 2 つのフェーズでデータ移行プロセスを完了します。

- 分析およびエクスポート
- インポート

分析およびエクスポート フェーズでは、5.4 にエクスポートするオブジェクトを指定します。移行ユーティリティではこれらのオブジェクトを分析し、データを集約してエクスポートします。

分析およびエクスポート フェーズが完了すると、移行ユーティリティによって、すべてのデータ互換性エラーを示すレポートが生成されます。このエラーは、これらのオブジェクトを正常に 5.4 にインポートするために手動で解決できます。

分析およびエクスポート フェーズは反復的なプロセスであり、インポートされるデータに確実にエラーがなくなるまで複数回繰り返すことができます。分析およびエクスポート フェーズが完了すると、インポート フェーズを実行してデータを ACS 5.4 にインポートできるようになります。

ここでは、次の内容について説明します。

移行の要件

移行ユーティリティを実行するには、次のマシンを配置する必要があります。

- 移行元の ACS 4.x マシン：このマシンには、ACS 4.x Solution Engine または ACS for Windows 4.x マシンのいずれかを使用できます。移行元のマシンでは、移行サポート バージョンの ACS が稼働している必要があります。詳細については、「移行サポート バージョン」（P.2-2）を参照してください。
- 移行マシン：このマシンは、移行元のマシンと同じバージョンの ACS（パッチを含む）が稼働している Windows プラットフォームである必要があります。ACS 運用マシンまたは ACS アプライアンス マシンは、移行マシンとして使用できません。ACS for Windows が稼働している Windows サーバである必要があります。移行マシンには 2 GB RAM が必要です。
- 移行先の ACS 5.4 マシン：インポート プロセスを開始する前に、ACS 5.4 設定データをバックアップし、ACS 5.4 で移行インターフェイスがイネーブルになっていることを確認します。新しい ACS 5.4 データベースにデータをインポートすることを推奨します。移行インターフェイスをイネーブルにするには、ACS CLI から次のように入力します。

  ```
  acs config-web-interface migration enable
  ```

移行サポート バージョン

ACS 5.4 では、次の ACS 4.x バージョンからの移行がサポートされています。

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

（注）　ここに記載されている移行サポート バージョンに対して、最新のパッチをインストールしておく必要があります。また、他のバージョンの ACS 4.x がインストールされている場合は、ACS 5.4 に移行する前に、サポート対象バージョンのいずれかにアップグレードして、そのバージョンの最新パッチをインストールする必要があります。

はじめる前に

ACS 4.x から ACS 5.4 にデータを移行する前に、次のことを確認します。

- ACS 4.x 移行元マシンにデータベース破損の問題がないこと。
- 移行元マシンと移行マシンに、同じ ACS バージョン（パッチを含む）がインストールされていること。
- 移行マシンに単一の IP アドレスが設定されていること。
- 移行元の ACS 4.x データがバックアップしてあること。
- 移行マシンと ACS 5.4 サーバの間に完全なネットワーク接続があること。
- ACS 5.4 サーバで移行インターフェイスがイネーブルになっていること。
- 移行ユーティリティの実行中は、ACS 5.4 のデフォルトのスーパー管理者アカウント **acsadmin** だけを使用すること。

リモート デスクトップを使用して、移行マシンに接続し、移行ユーティリティを実行することはできません。移行ユーティリティは移行マシンで実行するか、VNC を使用して移行マシンに接続する必要があります。

（注）　ACS 5.4 移行ユーティリティは、Windows 2008 64 ビットではサポートされません。

移行ファイルのダウンロード

ACS 5.4 の移行アプリケーション ファイルおよび移行ガイドをダウンロードするには、次の手順を実行します。

ステップ 1　[System Administration] > [Downloads] > [Migration Utility] を選択します。

[Migration from 4.x] ページが表示されます。

ステップ 2　[Migration application files] をクリックして、移行ユーティリティを実行する場合に使用するアプリケーション ファイルをダウンロードします。

ステップ 3　[Migration Guide] をクリックして、『*Migration Guide for Cisco Secure Access Control System 5.4*』をダウンロードします。

ACS 4.x から ACS 5.4 への移行

ACS 4.x の任意の移行サポート バージョンから ACS 5.4 にデータを移行できます。移行ユーティリティによって、次の ACS 4.x データ エンティティが移行されます。

- ネットワーク デバイス グループ（NDG）
- AAA クライアントおよびネットワーク デバイス
- 内部ユーザ
- （Interface Configuration セクションの）ユーザ定義フィールド
- ユーザ グループ
- 共有シェル コマンド認可セット
- （ユーザ属性に移行される）ユーザ TACACS+ Shell Exec 属性
- （シェル プロファイルに移行される）グループ TACACS+ Shell Exec 属性
- ユーザ TACACS+ コマンド認可セット
- グループ TACACS+ コマンド認可セット
- 共有ダウンロード可能 ACL
- EAP-FAST マスター キー
- 共有 RADIUS Authorization Component（RAC; RADIUS 認可コンポーネント）
- RADIUS VSA

（注） 移行ユーティリティでは、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）設定データは移行されず、証明書の移行もサポートされていません。

ACS 4.x から ACS 5.4 にデータを移行するには、次の手順を実行します。

ステップ 1　ACS 4.x サーバで、現在、移行サポート バージョンのいずれも稼働していない場合は、ACS 4.x バージョンを移行サポート バージョンにアップグレードします。

ACS の移行サポート バージョンのリストについては、「移行サポート バージョン」（P.2-2）を参照してください。

ステップ 2　移行マシン（Windows サーバ）に同じ移行サポート バージョンの ACS をインストールします。

ステップ 3　ACS 4.x データをバックアップして、移行マシンで復元します。

ステップ 4　移行マシンに移行ユーティリティを保存します。

移行ユーティリティは、Installation and Recovery DVD から取得できます。

ステップ 5　移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。

ステップ 6　分析およびエクスポート フェーズで発生した問題を解決します。

ステップ 7　移行マシンで、移行ユーティリティのインポート フェーズを実行します。

インポート フェーズでは、データを 5.4 サーバにインポートします。

（注）　大規模な内部データベースがある場合、スタンドアロンの 5.x プライマリ サーバにデータをインポートし、複数のセカンダリ サーバに接続しているサーバにはデータをインポートしないことを推奨します。データの移行が完了すると、セカンダリ サーバをスタンドアロンの 5.x プライマリ サーバに登録できるようになります。

移行ユーティリティの使用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/migration/guide/migration_guide.html

データを移行したあと、移行されたオブジェクトを使用してポリシーを再構築できます。

ACS 4.x から ACS 5.4 への機能マッピング

ACS 5.4 では、認可、シェル プロファイル、属性、およびその他のポリシー要素を、ユーザまたはグループ定義の一部としてではなく、独立した再利用可能なオブジェクトとして定義します。

表 2-1 に、ACS 5.4 での ID、ネットワーク リソース、およびポリシー要素の設定場所を示します。この表を使用して、移行したデータ ID を表示または変更します。ACS 5.4 ポリシー モデルの概要については、第 3 章「ACS 5.x ポリシー モデル」を参照してください。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
ネットワーク デバイス グループ	[Network Configuration] ページ	[Network Resources] > [Network Device Groups] 「ネットワーク デバイス グループの作成、複製、および編集」（P.7-2）を参照してください。	NDG はポリシー ルール内の条件として使用できます。 ACS 5.4 では NDG 共有パスワードがサポートされていません。移行後は、メンバー デバイスに NDG 共有パスワード情報が格納されます。
ネットワーク デバイスおよび AAA クライアント	[Network Configuration] ページ	[Network Resources] > [Network Devices and AAA Clients] 「ネットワーク デバイスおよび AAA クライアント」（P.7-5）を参照してください。	RADIUS キー ラップのキー（KEK および MACK）は、ACS 4.x から ACS 5.4 に移行されます。
ユーザ グループ	[Group Setup] ページ	[Users and Identity Stores] > [Identity Groups] 「ID 属性の管理」（P.8-7）を参照してください。	ID グループはポリシー ルール内の条件として使用できます。
内部ユーザ	[User Setup] ページ	[Users and Identity Stores] > [Internal Identity Stores] > [Users] 「内部 ID ストアの管理」（P.8-4）を参照してください。	ACS 5.4 は、内部 ID ストアに対してだけ内部ユーザを認証します。 認証に外部データベースを使用していた移行済みユーザには、最初のアクセス時に変更が必要なデフォルトの認証パスワードが割り当てられます。
内部ホスト	[Network Access Profiles] > [Authentication]	[Users and Identity Stores] > [Internal Identity Stores] > [Hosts] 「ID ストアでのホストの作成」（P.8-16）を参照してください。	内部ホストは、[Host Lookup] の ID ポリシーで使用できます。
ID 属性（ユーザ定義フィールド）	[Interface Configuration] > [User Data Configuration]	[System Administration] > [Configuration] > [Dictionaries] > [Identity] > [Internal Users] 「ディクショナリの管理」（P.18-5）を参照してください。	定義済みの ID 属性フィールドが [User Properties] ページに表示されます。これらをアクセス サービス ポリシーの条件として使用できます。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング （続き）

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
コマンド セット（コマンド認可セット）	次のいずれかが必要です。 • [Shared Profile Components] > [Command Authorization Set] • [User Setup] ページ • [Group Setup] ページ	[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Set] 「管理デバイス用のコマンド セットの作成、複製、および編集」（P.9-31）を参照してください。	デバイス管理アクセス サービスの認可ポリシー ルールの結果として、コマンド セットを追加できます。
Shell exec パラメータ	[User Setup] ページ	[System Administration] > [Dictionaries] > [Identity] > [Internal Users] 「ディクショナリの管理」（P.18-5）を参照してください。	定義済みの ID 属性フィールドが [User Properties] ページに表示されます。 これらをアクセス サービス ポリシーの条件として使用できます。
シェル プロファイル（shell exec パラメータまたはシェル コマンド認可セット）	[Group Setup] ページ	[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profile] 「デバイス管理用のシェル プロファイルの作成、複製、および編集」（P.9-25）を参照してください。	デバイス管理アクセス サービスの認可ポリシー ルールの結果として、シェル プロファイルを追加できます。
日時条件（時間帯アクセス） 日時条件は移行できません。ACS 5.4 で再作成する必要があります。	[Group Setup] ページ	[Policy Elements] > [Session Conditions] > [Date and Time] 「日付と時刻の条件の作成、複製、および編集」（P.9-3）を参照してください。	日時条件は、サービス セレクション ポリシーのポリシー ルールまたはアクセス サービスの認可ポリシーに追加できます。
RADIUS 属性	次のいずれかが必要です。 • [Shared Profile Components] > [RADIUS Authorization Component] • [User Setup] ページ • [Group Setup] ページ ユーザおよびグループ設定の RADIUS 属性は移行できません。ACS 5.4 で再作成する必要があります。	[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] > [Common Tasks] タブ または [Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profile] > [RADIUS Attributes] タブ 「ネットワーク アクセス用の認可プロファイルの作成、複製、および編集」（P.9-19）を参照してください。	RADIUS 属性は、ネットワーク アクセス認可プロファイルの一部として設定できます。 ネットワーク アクセス サービスの認可ポリシーの結果として認可プロファイルを追加できます。

表 2-1　ACS 4.x から ACS 5.4 への機能マッピング （続き）

設定内容	ACS 4.x での選択	ACS 5.4 での選択	5.4 の追加情報
ダウンロード可能 ACL	共有プロファイル コンポーネント	[Policy Elements] > [Authorization and Permissions] > [Named Permission Objects] > [Downloadable ACLs] 「ダウンロード可能 ACL の作成、複製、および編集」（P.9-33）を参照してください。	ネットワーク アクセス認可プロファイルに Downloadable ACL（DACL; ダウンロード可能 ACL）を追加できます。 認可プロファイルを作成したあと、ネットワーク アクセス サービスの認可ポリシーの結果としてこれを追加できます。
RADIUS VSA	インターフェイス コンフィギュレーション	[System Administration] > [Configuration] > [Dictionaries] > [Protocols] > [RADIUS] > [RADIUS VSA] 「RADIUS ベンダー固有属性の作成、複製、および編集」（P.18-6）を参照してください。	RADIUS VSA 属性は、ネットワーク アクセス認可プロファイルの一部として設定します。 ネットワーク アクセス サービスの認可ポリシーの結果として認可プロファイルを追加できます。

移行の一般的なシナリオ

次に、ACS 5.4 への移行時に発生する一般的なシナリオを示します。

- 「CSACS 1120 の ACS 4.2 から ACS 5.4 への移行」（P.2-8）
- 「ACS 3.x から ACS 5.4 への移行」（P.2-9）
- 「他の AAA サーバから ACS 5.4 へのデータの移行」（P.2-9）

CSACS 1120 の ACS 4.2 から ACS 5.4 への移行

展開において、CSACS 1120 にある ACS 4.2 を ACS 5.4 に移行する場合は、次の手順を実行する必要があります。

ステップ 1　移行マシンに Cisco Secure Access Control Server 4.2 for Windows をインストールします。

ステップ 2　CSACS 1120 で ACS 4.2 データをバックアップします。

ステップ 3　移行マシンでデータを復元します。

ステップ 4　移行マシンで、移行ユーティリティの分析およびエクスポート フェーズを実行します。

ステップ 5　CSACS 1120 に ACS 5.4 をインストールします。

ステップ 6　移行マシンのデータを、ACS 5.4 がインストールされている CSACS 1120 にインポートします。

各手順の詳しい説明については、http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/migration/guide/migration_guide.html を参照してください。

ACS 3.x から ACS 5.4 への移行

使用環境に ACS 3.x を展開している場合、ACS 5.4 への直接移行はできません。次の手順を実行する必要があります。

ステップ 1　ACS 4.x の移行サポート バージョンにアップグレードします。移行サポート バージョンのリストについては、「移行サポート バージョン」（P.2-2）を参照してください。

ステップ 2　ACS 3.x のアップグレード パスを確認します。

- ACS Solution Engine 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_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037

- ACS for Windows については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/install.html#wp1102849

ステップ 3　ACS 3.x サーバを ACS 4.x の移行サポート バージョンにアップグレードします。

アップグレード後、ACS 4.x から ACS 5.4 への移行方法を示した手順を実行します。詳細については、『*Migration Guide for Cisco Secure Access Control System 5.4*』を参照してください。

他の AAA サーバから ACS 5.4 へのデータの移行

ACS 5.4 では、ACS Web インターフェイスおよび CLI を使用して、さまざまな ACS オブジェクトの一括インポートを実行できます。インポートできる ACS オブジェクトは次のとおりです。

- ユーザ
- ホスト
- ネットワーク デバイス
- ID グループ
- NDG
- ダウンロード可能 ACL
- コマンド セット

ACS では、カンマ区切り形式（.csv）ファイルを使用して、データの一括インポートを実行できます。データは、ACS が要求する形式で .csv ファイルに入力する必要があります。ACS には、ACS 5.4 にインポート可能なそれぞれのオブジェクト用に .csv テンプレートが用意されています。このテンプレートは Web インターフェイスからダウンロードできます。

他の AAA サーバから ACS 5.4 にデータを移行するには、次の手順を実行します。

ステップ 1　.csv ファイルにデータを入力します。

.csv テンプレートの概要の詳細については、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/cli_imp_exp.html#wp1064565

ステップ 2　ACS 5.4 アプライアンスを設定します。

ステップ 3　ACS 5.4 に対してデータの一括インポートを実行します。

ACS オブジェクトの一括インポートの実行の詳細については、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/cli_imp_exp.html#wp1056244

これで、他の AAA サーバのデータを ACS 5.4 で使用できます。