CHAPTER 3

ACS 5.3 の設定の移行方法

この章では ACS 4.x から 5.3 の移行について説明し、次の項で構成されています。

移行方法

ACS 5.3 設定モデルは ACS 3.x および 4.x と異なります。ACS 3.x および 4.x から ACS 5.3 に直接データと設定を移行することはできません。ACS 5.3 の移行には、手動の再設定が必要になります。ACS 5.3 では、移行プロセス用に次のツールを提供しています。

移行ユーティリティ

移行ユーティリティは ACS 4.x Windows マシンで実行するツールです。このツールを使用して、ACS 4.x バックアップ ファイルをインポートしたり、データを分析したり、データを ACS 5.3 にインポートする前に必要な変更を行ったりすることができます。

移行ユーティリティは、表 3-1 に示す移行をサポートしています。移行ユーティリティは、[System Configuration] > [Downloads] の、ACS 5.3 Web インターフェイスからダウンロードできます。

移行ユーティリティによって、ACS 4.x Windows マシンから ACS 5.3 マシンにデータを移行します。このプロセスは、ACS のバージョン 3.x から 4.x または任意の 4.x アップグレードのアップグレード プロセスと異なります。

アップグレード プロセスでは、ACS 4.x システムは管理サポートを必要とせずに、同じように機能します。移行プロセスでは、ACS 5.3 にデータをインポートする前に、データを統合し、手動で解決する管理サポートが必要となる場合があります。

ACS 5.3 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 5.3 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。複数の ACS 4.x インスタンスを区別するため、プレフィクスを追加できます。プレフィクスを使用して、データ要素のサーバ固有 ID を保持し、異なるサーバのオブジェクト名の重複を避けます。

ACS 4.x 展開の移行は、複雑なプロセスで、十分に計画する必要があります。移行を実行する前に、ACS 4.x レプリケーション階層を考慮する必要があります。

たとえば、ある ACS 4.x サーバに、別の ACS 4.x サーバから複製されたデータがある場合、データは同じであるため、これらの両方の ACS サーバから同じデータ セットを移行する必要はありません。そのため、展開内の ACS インスタンスの移行の順序は十分に考慮する必要があります。

CSV インポート ツール

ACS 5.3 では、表 3-1 に示すように、カンマ区切り値（CSV）テキスト ファイルからデータ オブジェクトの一部をインポートできます。Web インターフェイスを使用して、ACS 5.3 のすべてのデータ オブジェクトを手動で設定しない場合は、CSV テキスト ファイルで設定を作成し、設定をインポートできます。

多くのインスタンスで、デバイスやユーザ情報などの ACS 設定データは ACS の外部に保存されています。このデータをテキスト形式でエクスポートして、ACS 5.3 にインポートできます。

CSV インポート ツールの詳細については、『*Software Developer's Guide for the Cisco Secure Access Control System 5.3*』の「Using the Scripting Interface」の章を参照してください。

表 3-1　ACS 5.3 移行ユーティリティとインポート ツールのオプション

ACS 5.3 設定領域	ACS 5.3 移行ユーティリティのサポート	ACS 5.3 インポート ツール
NDG	Yes	Yes
ネットワーク デバイス	Yes	Yes
RADIUS プロキシ サーバ	No	No
内部ユーザ/ホスト	Yes	Yes
ID グループ	Yes	Yes
外部 ID ストア	No	No
ポリシー要素	共有コマンド セット、RAC、共有 DACL	共有コマンド セット、共有 DACL
アクセス ポリシー	No	No
モニタリングとレポート	No	No
システム管理	FAST マスター キー、VSA	No

移行に関する推奨事項

- 小規模の ACS 設定の場合は、手動の設定と CSV インポートを組み合わせて使用します。これは次のような場合です。
  - ユーザを ACS で管理していない
  - ネットワーク デバイス ワイルドカードを使用している
  - ユーザとネットワーク デバイスの情報が CSV テキスト形式で使用できる
- その他の設定では、手動の設定と CSV インポートに加えて ACS 5.3 移行ユーティリティを使用します。

移行ユーティリティについて

移行ユーティリティを使用して、さまざまなタイプのデータを ACS 4.x から ACS 5.3 に移行します。ACS 4.x Windows ソース マシンに加えて、ACS 4.x 移行マシンと ACS 5.3 ターゲット マシンを展開する必要があります。

移行プロセスには次の 2 つのフェーズがあります。

- 分析およびエクスポート
- インポート

移行ユーティリティを ACS 4.x 移行マシンで実行します。移行マシンは ACS 4.x を実行する Windows プラットフォームです。分析フェーズとエクスポート フェーズを別々に複数回実行して、データがインポート フェーズに適切かどうかを確認できます。

分析フェーズに合格したデータはエクスポートして、ACS 5.3 にインポートできます。ACS 5.3 ポリシーの詳細については、『*User Guide for the Cisco Secure Access Control System* 5.3』を参照してください。

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 5.3 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。

移行ユーティリティは ACS 4.x データ要素のサブセットをサポートします。完全なリストについては、表 4-1（P.4-3）の「移行プロセスでサポートされるすべての ACS 要素」を参照してください。

ACS 4.x から 5.3 への移行

ここでは、ACS 4.x から ACS 5.3 の移行に使用する手法について説明します。ここでは、次の内容について説明します。

- 「複数インスタンスの移行」（P.3-3）
- 「ACS 5.3 の移行フェーズ」（P.3-4）
- 「データ モデル編成」（P.3-4）

複数インスタンスの移行

ACS 5.3 には、すべての ACS 4.x インスタンスのデータを保持する 1 つのプライマリ データベースがあります。このプライマリ データベースに各 ACS 4.x インスタンスのデータが移行されます。ACS 4.x では、システム設定全体の個別のサブセットを別々の ACS インスタンスで管理できるように、選択したデータのレプリケーションを定義できます。

ACS 5.3 には、すべての ACS インスタンスに複製される統合データベースが含まれています。統合データベースには、各 ACS 4.x インスタンスのすべてのローカル設定定義が格納されます。

ACS 5.3 の移行フェーズ

ACS 5.3 は 2 フェーズの移行方式に従います。

- 「分析フェーズ」（P.3-4）
- 「移行フェーズ」（P.3-4）

分析フェーズ

このフェーズでは、既存の ACS 4.x 設定の分析が実行されます。可能性のある移行の問題が報告され、解決方法があれば推奨されます。移行ユーティリティを実行する前に、移行マシンに ACS 4.x をインストールし、データを復元する必要があります。

ACS 4.x サーバのバックアップから復元されたデータに対して分析ツールを実行できます。分析ツールを複数回実行して、必要に応じて、移行マシンの ACS 4.x 設定を変更できます。

（注）　分析フェーズとエクスポート フェーズは、移行プロセスの 1 つのフェーズとして実装されます。分析レポートには、分析とエクスポートの両方の情報が含まれます。

移行フェーズ

このフェーズでは、移行ユーティリティは ACS 4.x サーバから設定データを抽出し、ACS 5.3 サーバにインポート可能な形式で移行されるようにデータを準備します。移行ツールには、次のような 1 つ以上のカテゴリでデータを移行するオプションがあります。

- インベントリ データ移行（ユーザ、ネットワーク デバイス、MAC）
- ポリシー データ移行（ネットワーク デバイス グループ、ID グループ、コマンド セット、RAC、VSA、DACL）

データ モデル編成

ACS 5.3 は、ポリシーベースのアクセス コントロール システムです。ACS 5.3 での*ポリシー モデル*という用語は、ポリシー管理者のポリシー要素、ポリシー オブジェクト、およびポリシー規則を表しています。ACS 5.3 では、以前のバージョンで使用されていたグループベースのモデルの代わりに、規則ベース ポリシー モデルが使用されています。

規則ベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力で柔軟なアクセス コントロールを実現できます。ポリシー モデルの詳細については、『*User Guide for Cisco Secure Access Control System 5.3*』を参照してください。

次に、ACS 5.3 の 3 つの主なデータ モデル関連ポイントを示します。

- 「モデル編成」（P.3-5）
- 「モデル ストレージ」（P.3-5）
- 「レプリケーション モデル」（P.3-5）

モデル編成

ACS 5.3 ではネットワーク アクセス プロファイル（NAP）関連機能が、RADIUS と TACACS+ の両方の完全なポリシーベースの認証、認可、アカウンティング（AAA）ソリューションに拡張されています。

一連の RADIUS 属性などの特定のポリシーと認証情報は、ACS 4.x のように、ユーザまたはグループ レコード内に保存されません。代わりに、返された認証データのすべてのセットが選択されます。

モデル ストレージ

移行プロセスでは、次の基準を満たす ACS 4.x データが対象になります。

- ACS 5.3 モデルに変換できる
- ダイナミックユーザなどの実行時の操作中に生成されないデータから構成される

レプリケーション モデル

ACS 5.3 では、ACS 4.x の複数のデータベース インスタンスを組み合わせて、1 つのデータベースに移行されます。ACS 4.x では、システム設定全体の個別のサブセットを別々の ACS インスタンスで管理できるように、選択したデータのレプリケーションを定義できます。

ACS 5.3 には、すべての ACS インスタンスに複製される統合データベースが含まれています。この統合データベースには、各 ACS 4.x インスタンスのすべてのローカル設定定義が格納されます。

ACS 5.3 データ モデルは、ACS 4.x データ モデルよりはるかに統一性があります。ACS 5.3 データ モデルには、単一のマスター インスタンスが含まれ、ここですべての設定変更が行われます。内在するすべてのセカンダリ インスタンスは、設定の完全なコピーを保持し、設定のすべての変更の更新を受け取ります。

複数インスタンスの移行のサポート

ACS 4.x の複数のインスタンスを ACS 5.3 に移行するには、次の手順を実行します。

ステップ 1　移行する ACS 4.x インスタンスを選択します。

プライマリ ACS 4.x インスタンス（展開に存在する場合）を最初に移行する必要があります。選択した ACS 4.x インスタンスをバックアップします。

ステップ 2　バックアップした ACS 4.x インスタンスを移行マシンに復元します。

ステップ 3　移行プロセスを実行します。

ステップ 4　1 つの ACS 4.x インスタンスの移行プロセスが完了したら、別のインスタンスに進むか、プロセスを終了します。

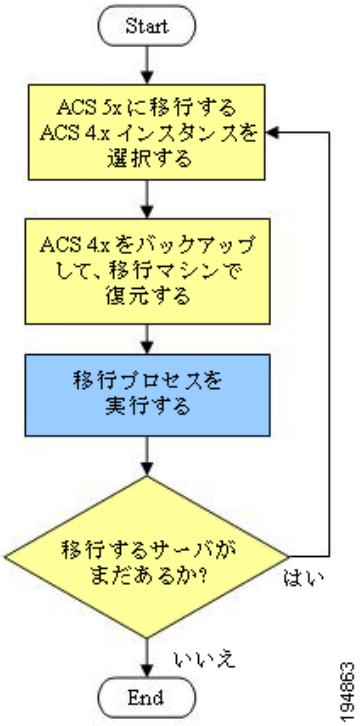
ACS 4.x のインスタンスを復元すると、以前の ACS 4.x インスタンス データが削除されます。

分析およびエクスポート フェーズでは、複数インスタンスに関して変更は行われません。

たとえば、移行ユーティリティは異なる ACS 4.x インスタンス間で重複したオブジェクトを検出しません。複数の ACS 4.x インスタンスに存在する重複した矛盾するデータ オブジェクトは、移行のインポート フェーズで検出され、報告されます。

図 3-1 に複数インスタンスの移行プロセスを示します。

図 3-1　　複数インスタンスの移行プロセス



データの移行

移行プロセスでは、ソース ACS 4.x サーバからデータがエクスポートされ、対応するデータ エンティティがターゲット ACS 5.3 サーバにインポートされます。エクスポート プロセスは稼動中の 4.x サーバでは実行しません。代わりに、ACS 4.x ソース サーバからデータベースをバックアップし、追加の ACS 4.x 移行マシンにデータを復元し、そこで移行ユーティリティを実行する必要があります。

（注）　移行プロセスを開始する前に、ACS 4.x ソース マシンで完全なデータベース バックアップを実行する必要があります。バックアップしたデータを追加の ACS 4.x 移行マシンに復元し、データを ACS 5.3 マシンにインポートする前に問題を修正します。

ACS 4.x データベースのパスワードは 37 文字以内にする必要があります。

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 データに対して分析とエクスポートを実行し、AnalyzeAndExport 要約レポートと Analyze and Export 完全レポートを確認します。

「ACS 4.x データの分析およびエクスポート」（P.6-36）を参照してください。このフェーズでは、次の手順を実行します。

- 移行できないデータの問題を特定し、手動の移行の考慮事項を確認します。「移行の問題の解決」（P.D-3）を参照してください。
- 移行の前に修正する問題を特定します。
- 統合するデータを特定します。詳細は「データの統合」（P.6-37）を参照してください。

分析およびエクスポート フェーズに合格したデータのみをエクスポートし、後で ACS 5.3 にインポートできます。

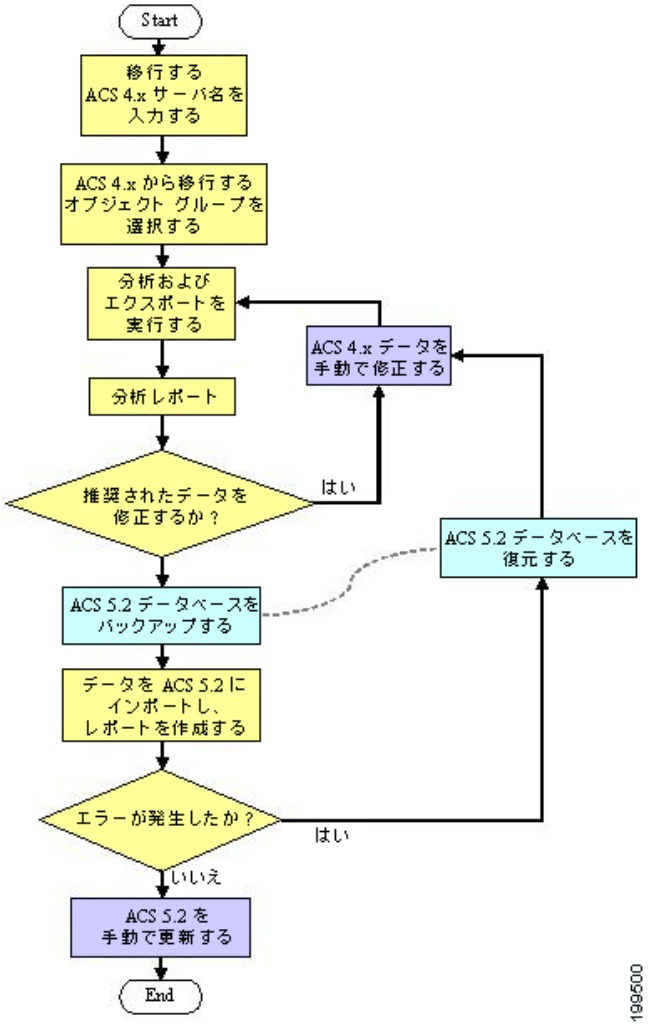
ステップ 2　ACS 5.3 ターゲット マシン データベースをバックアップします。

ステップ 3　ACS 4.x データを ACS 5.3 にインポートし、インポート要約レポートを確認します。

「ACS 5.3 への ACS 4.x データのインポート」（P.6-37）を参照してください。

図 3-2 に移行プロセスを示します。

図 3-2　移行プロセス



オブジェクト グループの選択

完全移行または部分移行の実行を選択できます。部分移行では、移行するオブジェクト グループを選択する必要があります。

オブジェクト グループは、オブジェクト間の依存関係に従って定義されます。アプリケーションでサポートされるオブジェクト タイプのグループか、またはサポートされるすべてのオブジェクト タイプを移行できます。次のオブジェクトのグループから選択できます。

- すべてのオブジェクト：移行プロセスでサポートされているすべての ACS オブジェクト
- すべてのユーザ オブジェクト：ID グループおよびユーザから抽出されたすべてのオブジェクト
- すべてのデバイス オブジェクト：ネットワーク デバイスと NDG
- 共有コマンド セット
- 共有ダウンロード可能アクセス コントロール リスト（DACL）

- マスター キー：Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）マスター キー
- 共有 RADIUS Authorization Components（RAC; RADIUS 認可コンポーネント）および Vendor Specific Attributes（VSA; ベンダー固有属性）

分析およびエクスポート

ACS 4.x の既存の設定を分析し、データ移行の実行の成功に影響する可能性のある移行の問題を特定する必要があります。

このフェーズでは、次のことを特定します。

- 移行できないデータの問題。移行前にこのデータを修正する機会もあります。
- 移行前に修正する問題。
- 統合するデータ。詳細は「データの統合」（P.6-37）を参照してください。

（注）　分析フェーズに合格したデータのみがエクスポートでき、後で ACS 5.3 にインポートされます。

エクスポート プロセスでは、ACS 4.x データの選択した一連のオブジェクトが、インポート プロセス時に処理される外部データ ファイルにエクスポートされます。

エクスポート プロセスでは次の問題が報告されます。

- エクスポートされなかったデータとその理由。
- エクスポートされたデータと統計情報。

インポート

ACS 4.x からのデータ エクスポート ファイルは ACS 5.3 にインポートされます。

インポートは完全なデータベースに対して実行できます。ACS 5.3 データベースを手動でバックアップすることをお勧めします。データのインポート プロセス中に予期しないエラーが発生した場合、データベースのバックアップ バージョンを使用して、システムを復元できます。

複数インスタンスのサポート

複数インスタンスの移行では、すべてのインスタンスが同じ移行マシンに復元され、すべてのインスタンスの結果が保持されます。複数インスタンスのサポートに関連する各データ タイプの特定の変更の詳細については、「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

ACS 5.3 の複数インスタンスのサポートには、次の主な機能があります。

- 「重複オブジェクトの報告」（P.3-10）
- 「インスタンスごとのオブジェクト名プレフィクス」（P.3-10）
- 「共有オブジェクトの処理」（P.3-10）

重複オブジェクトの報告

複数の ACS 4.x インスタンスの重複データ オブジェクトはインポート フェーズで検出されます。ほとんどのデータ タイプでは、名前で重複を識別できます。さらに、インポート レポートで、重複オブジェクトに関する情報が報告されます。「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

インスタンスごとのオブジェクト名プレフィクス

各 ACS 4.x インスタンスに異なる名前プレフィクスを定義できます。プレフィクスを使用して、データ要素のサーバ固有 ID を保持し、異なるサーバのオブジェクトの名前の重複を避けます。（ACS 4.x インスタンスごとの）移行ユーティリティの各実行の始めに名前のプレフィクスを変更できます。

インスタンス固有のプレフィクスを指定できるため、ACS 4.x インスタンス間の重複に関係なくすべてのデータをインポートできます。グローバル名プレフィクスまたはオブジェクトタイプごとの名前プレフィクスを設定できます。これにより、共有オブジェクト間の関連付けを維持できます。「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

共有オブジェクトの処理

NDG、ユーザ属性定義、ユーザ グループなどの ACS 4.x インスタンス間の共有オブジェクトは 1 回だけ移行されます。ただし、複数インスタンスの関連付けのサポートのため、ACS 5.3 データのステータスに従ってオブジェクトの関連付けが作成されます。詳細については、「ACS 4.x オブジェクトの移行」（P.6-9）を参照してください。

たとえば、ユーザ *A* がグループ *BB* に関連づけられており、ユーザもグループも移行されなかった場合、ACS 5.3 で両方のオブジェクトが作成され、関連付けられます。