Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行

データの移行および導入のシナリオ

Cisco Secure ACS と Cisco ISE は別のハードウェア プラットフォーム上に配置され、異なるオペレーティング システム、データベース、および情報モデルを持ちます。このため、Cisco Secure ACS から Cisco ISE へ標準のアップグレードを実行することはできません。代わりに、Cisco Secure ACS to Cisco ISE Migration Tool が Cisco Secure ACS からのデータを読み取り、Cisco ISE に対応するデータを作成します。

シングル アプライアンスにおけるデータ移行プロセスは、分散環境におけるアプライアンスのデータ移行プロセスとは異なります。以降のセクションでは、これらのトピックについてとりあげます。

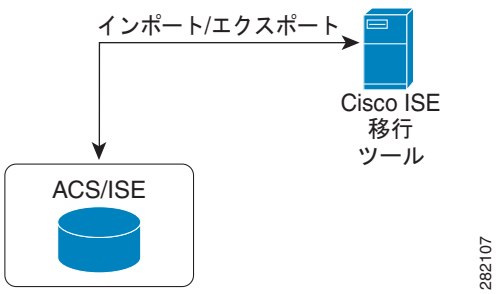
- 「シングル Cisco Secure ACS アプライアンスからのデータの移行」（P.3-1）
- 「分散環境におけるデータの移行」（P.3-2）

シングル Cisco Secure ACS アプライアンスからのデータの移行

ご使用の環境内にシングル Cisco Secure ACS アプライアンスがある場合（または複数の Cisco Secure ACS アプライアンスがあるが、分散した配置内にない場合）は、「Cisco Secure ACS データをエクスポートおよびインポートするための移行ツールの使用方法」（P.5-1）に記載されているように、Cisco Secure ACS-Cisco ISE Migration Tool を Cisco Secure ACS アプライアンスに対して実行します。

図 3-1 は、Cisco ISE Release 1.0 ソフトウェアがインストールされるアプライアンスと同じアプライアンス上に、Cisco Secure ACS 5.1 がインストールされている展開シナリオを示しています（シングルアプライアンス展開）。他の Cisco Secure ACS Release から Cisco ISE リリースへのサポートされている移行については、表 1-1 を参照してください。

図 3-1　　シングル アプライアンスにインストールされる Cisco Secure ACS および Cisco ISE



また、Cisco Secure ACS および Cisco ISE が同じハードウェア（CSACS-1121 アプライアンス）を使用している場合も、次の移行手順を使用できます。

ステップ 1　Cisco Secure ACS to Cisco ISE Migration Tool を、スタンドアロンの Windows マシンにインストールします。

ステップ 2　Cisco Secure ACS アプライアンスから Cisco Secure ACS Release 5.3 データをエクスポートします。

ステップ 3　Cisco Secure ACS のデータをバックアップします。

ステップ 4　アプライアンスを Cisco ISE Release 1.2 ソフトウェアで再作成します。

ステップ 5　Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへインポートします。

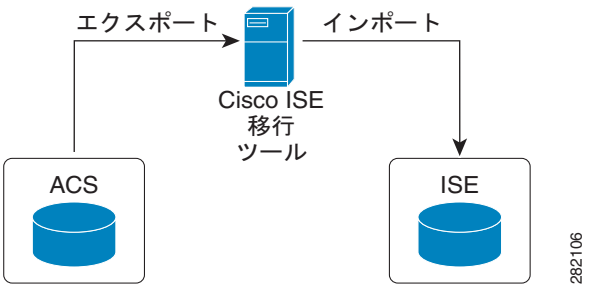
（注）　Cisco Secure ACS Release 5.3 のデータを Cisco ISE Release 1.2 アプライアンスへ移行開始する準備ができた場合は、移行先がスタンドアロンの Cisco ISE ノードであることを確認します。移行が正常に終了した後に、何らかの展開設定（Administrator ISE や Policy Service ISE のペルソナなど）を開始することができます 移行のインポート フェーズは、サポートされているハードウェア アプライアンス上で、Cisco ISE ソフトウェアの新しい「クリーンな」インストールにおいて実行する必要があります。サポートされているハードウェア アプライアンスのリストについては、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*』を参照してください。

分散環境におけるデータの移行

分散環境では、1 つのプライマリ Cisco Secure ACS アプライアンス、およびこのプライマリ アプライアンスと相互運用する 1 つ以上のセカンダリ Cisco Secure ACS アプライアンスがあります。

図 3-2 は、Cisco Secure ACS および Cisco ISE が異なるアプライアンスにインストールされている場合の展開シナリオについて説明しています（デュアルアプライアンス展開）。

図 3-2　異なるアプライアンスにインストールされている Cisco Secure ACS および Cisco ISE



分散環境で Cisco Secure ACS を実行する場合は、以下のようにする必要があります。

ステップ 1　プライマリ Cisco Secure ACS アプライアンスをバックアップし、それを移行マシン上で復元します。

ステップ 2　プライマリ Cisco Secure ACS アプライアンスに対して Cisco Secure ACS to Cisco ISE Migration Tool を実行します。

（注）　大規模な内部データベースがある場合、シスコではスタンドアロンのプライマリ アプライアンスから移行を実行し、複数のセカンダリ アプライアンスへ接続されているプライマリ アプライアンスへの移行は実行しないことを推奨しています。移行プロセスの完了後、セカンダリ アプライアンスを登録できます。

（注）　Cisco Secure ACS-Cisco ISE Migration Tool は約 20 時間稼働して、10,000 個のデバイス、25,000 人のユーザ、100,000 個のホスト、100 個の ID グループ、420 個のダウンロード可能アクセス コントロール リスト（DACL）、320 個の許可プロファイル、6 個のデバイス階層、および 20 個のネットワーク デバイス グループ（NDG）を移行することができます。

Cisco Secure ACS データの Cisco ISE への移行

Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいています。Cisco Secure ACS データが Cisco ISE に移行されると、その部分の間にギャップが常に存在します。

一般的に、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へデータを移行する場合に、以下の移行ルールを考慮する必要があります。

- 特殊文字は移行されない。
- enum 型の属性（RADIUS、VSA、ID、およびホスト）は、使用可能な値を持つ整数として移行される。
- （属性のデータ型に関係なく）すべてのエンドポイント属性は String データ型として移行される。
- Cisco ISE ログに追加される RADIUS 属性および VSA 値をフィルタすることはできない。

ポリシー規則の検証

Cisco Secure ACS と Cisco ISE のポリシー モデルは異なるので、バージョンが変わると、次の理由のためにすべての Cisco Secure ACS ポリシーおよび規則を移行できるとは限りません。

- ポリシーで使用されている属性がサポートされていない
- 構造がサポートされていない、または条件付きである（大半は、以前に複雑な条件が設定されている）
- 演算子がサポートされていない

ルールが移行できない場合、データ整合性だけでなく、セキュリティ面のために、全体としてのポリシー モデルは移行できませんでした。ポリシーのギャップ分析レポートで問題のあるルールの詳細情報を表示できます。サポート対象外のルールを修正または削除しない場合、ポリシーは Cisco ISE へ移行されません。

表 3-1　サポートされていない規則要素

規則要素	サポート対象	説明
日時	非サポート	反復的な週次設定を持つ許可ポリシー内の日時条件は、Cisco ISE へ移行されません。結果として、ルールも移行されません。
日時	非サポート	認証ポリシー内の日時条件は Cisco ISE へ移行されません。結果として、ルールも移行されません。
In	一部サポートあり	「In」オペランドは階層に使用され、「Is」は文字列タイプのみに使用されます。これは「Matches」を使用して変換することができます。
Not In	一部サポートあり	「Not in」オペランドは階層に使用され、「Is」は文字列タイプのみに使用されます。これは「Matches」を使用して変換することができます。
Contains Any	一部サポートあり	「Contains Any」オペランドは、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。
Contains All	非サポート	「Contains All」オペランドは、Active Directory および Lightweight Directory Access Protocol などの外部グループにのみ使用されます。
論理式の組み合わせ	非サポート	条件内でこれらのオペランドを使用しているルールは移行されません。 • a || b || c || ... や a && b && c && ... 以外の論理式（(a || b) && c など）を持つ複合条件が含まれている認証ポリシー。 • a && b && c && 以外のローカル式を持つ複合条件が含まれている許可ポリシーは、ルール条件の一部として移行されません。代わりに、いくつかの高度な論理式に対してライブラリ複合条件を手動で使用することができます。
ネットワーク条件	非サポート	ネットワーク条件のみが含まれているルールは移行されません。条件にネットワーク条件、およびサポート対象の他の条件が含まれている場合、ネットワーク条件は無視され、ルール条件の一部として移行されません。
ユーザ属性	一部サポートあり	データ型が「String」以外のユーザ属性を含む条件付きルールは移行されません。

表 3-1　サポートされていない規則要素 （続き）

規則要素	サポート対象	説明
ホスト属性	非サポート	条件でホスト属性を参照している場合、認証は失敗します。 ホスト（エンドポイント）属性を持つ条件が含まれている許可ポリシーは、Cisco ISE 許可ポリシーへ移行されません。
TACACS 属性	非サポート	Cisco ISE は、Terminal Access Controller Access-Control System（TACACS）をサポートしません。TACACS 属性を使用する Cisco Secure ACS サービス セレクション ポリシー ルールは移行されません。

Cisco Secure ACS Release 5.3 からの移行の準備

Cisco ISE Release 1.2 のポリシー セット モードでのみ Cisco Secure ACS Release 5.3 データを移行する必要があります。

Cisco Secure ACS から正常に移行した後に簡易モードに変更しないことを推奨します。Cisco ISE に移行されたすべてのポリシーが失われる可能性があるからです。それらの移行されたポリシーを取得することはできませんが、簡易モードからポリシー セット モードに切替えることができます。

Cisco Secure ACS データを Cisco ISE に移行し始める前に、次のことを考慮してください。

- Cisco ISE Release 1.2 の新規インストール上に移行します。
- サービス セレクション ポリシー（SSP）の有効なルールごとに 1 つのポリシー セットを生成し、SSP のルール順序に従って順序付けします。

（注）　SSP のデフォルト規則の結果であるサービスは、Cisco ISE Release 1.2 で設定されたデフォルト ポリシーになります。移行プロセスで作成されたすべてのポリシー セットで、最初の一致ポリシー セットが一致タイプになります。

ポリシー サービスの移行のガイドライン

Cisco Secure ACS から Cisco ISE へのポリシー サービスの移行を確実するには、次を確認する必要があります。

- Cisco Secure ACS Release 5.3 で無効またはモニタになっている SSP ルールを持つサービス セレクション ポリシー（SSP）がある場合、それらは Cisco ISE に移行されません。
- Cisco Secure ACS Release 5.3 のデバイス管理サービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。Cisco ISE は、デバイス管理をサポートしていません。
- Cisco Secure ACS Release 5.3 のプロキシサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。プロキシ サービスを実装する Cisco ISE は異なります。
- Cisco Secure ACS Release 5.3 のグループ マッピング ポリシーを含むネットワーク アクセス サービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。Cisco ISE は、グループ マッピング ポリシーをサポートしません。

- ID ポリシーに Cisco Secure ACS Release 5.3 の RADIUS ID サーバになるルールが含まれるサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。認証に RADIUS ID サーバを使用する Cisco ISE は異なります。
- Cisco Secure ACS Release 5.3 の属性またはポリシー要素を使用するポリシーを含むサービスを要求する有効な SSP ルールがある場合、それは Cisco ISE に移行されません。

ポリシー サービスごとの移行のガイドライン

はじめる前に

「Cisco Secure ACS Release 5.3 からの移行の準備」（P.3-5）を参照してください。

- Cisco ISE のサービスの名前を使用してポリシー セットを作成できます。ポリシー セットが Cisco Secure ACS Release 5.3 の SSP デフォルト規則の結果であるサービスに一致する場合、ポリシー セットは Cisco ISE Release 1.2 のデフォルトのポリシー セットになります。
- Cisco Secure ACS Release 5.3 の SSP ルールの条件は、Cisco ISE Release 1.2 のポリシー セットのエントリ条件になります。Cisco ISE Release 1.2 のデフォルトのポリシー セットの場合、必要なエントリ条件はありません。
- Cisco Secure ACS Release 5.3 の DenyAccess サービスを Cisco ISE Release 1.2 に変換すると、認証および許可ポリシーが次のように変更されます。
  - 許可ポリシーでのみ、結果を持つデフォルトの外部ルールが、許可されるプロトコルに対して Default Network Access に設定され、ID ソースに対して DenyAccess に設定されます。
  - 許可ポリシーでのみ、デフォルトのルール セットが DenyAccess に設定されます（標準権限）。
- Cisco Secure ACS Release 5.3 のサービスの ID ポリシーを、Cisco ISE Release 1.2 のポリシー セットの許可ポリシーに変換する場合、次の手順を実行します。
  - 単一で有効な外部ルールを持つ許可ポリシーを作成します。
  - 外部ルールの条件をデバイスとして指定します。場所はすべての場所で開始します（これは常に一致した条件です）。
  - デフォルトの外部ルールの結果を、許可されるプロトコルに対して Default Network Access に設定し、ID ソースに対して DenyAccess に設定します。

  外部ルールの結果は、関連するサービスの許可されたプロトコルです。認証ポリシーの内部ルールは、関連する ID ポリシーのルールです。認証ポリシーの内部ルールの順序は、関連する ID ポリシーのルールと同じ順序に従います。認証ポリシーの内部ルールの状態（有効、無効、またはモニタ）は、関連する ID ポリシー規則の状態従います。
- Cisco Secure ACS Release 5.3 のサービスの許可ポリシーを、Cisco ISE Release 1.2 のポリシー セットの許可ポリシーに変換する場合、
  - ローカル例外許可ポリシーのポリシー セットのルールは、関連するサービスの例外許可ポリシーのルールです。
  - 許可ポリシーのポリシー セットのルールは、関連するサービスの許可ポリシーのルールです。
  - ローカル例外許可ポリシーおよび許可ポリシーのポリシー セットのルールの順序は、関連するサービスのローカル例外許可ポリシーおよび許可ポリシーのルールの順序に従います。
  - ローカル例外許可ポリシーおよび許可ポリシーのポリシー セットのルールの状態（有効、無効、モニタ）は、関連するサービスのローカル例外許可ポリシーおよび許可ポリシーのルールの状態に従います。