Cisco Secure ACS から Cisco ISE へのデータ移行

Cisco Secure Access Control System（ACS）のリリース 5.3 から Cisco Identity Services Engine（ISE）リリース 1.2 へのデータ移行には、最小限のユーザの介入とすべての設定データが必要です。

この章では、次のトピックについて取り上げます。

- 「Cisco Secure ACS から Cisco ISE へのサポートされているデータ移行」（P.1-1）
- 「Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のポリシー モデル」（P.1-2）
- 「Cisco ISE および Cisco Secure ACS の導入モデル」（P.1-3）
- 「移行機能」（P.1-3）

Cisco Secure ACS から Cisco ISE へのサポートされているデータ移行

Cisco Secure ACS to Cisco ISE Migration Tool を使用した、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのデータ移行がサポートされます。Cisco Secure ACS の以前のリリース（*3.x* または *4.x*）を実行している場合は、を参照してください *「Cisco Secure ACS の以前のリリースからの移行」（P.-viii）*。

（注） 各 Cisco Secure ACS または Cisco ISE リリースで動的に変化している機能ギャップのために、すべての Cisco Secure ACS データを Cisco ISE に移行できるわけではありません。Cisco Secure ACS to Cisco ISE Migration Tool には、サポートされていないオブジェクトの完全なリストが含まれています。詳細については、図 4-1 を参照してください。

Cisco Secure ACS Release 5.3 データベースから Cisco ISE Release 1.2 に移行すると、データ移行で次がサポートされます。

- Cisco ISE Release 1.2 で Cisco Secure ACS Release 5.3 の新機能をサポートします。
- データを Cisco Secure ACS Release 5.3 から移行すると、Cisco ISE Release 1.2 の新機能がサポートされます。
- Cisco Secure ACS Release 5.3 と Cisco ISE Release 1.2 の間の設定のギャップを最小します。つまり、データ移行は、Cisco ISE で以前にサポートされていなかった Cisco Secure ACS 機能をサポートします。

表 1-1　Cisco Secure ACS Release から Cisco ISE Release へのサポートされている移行

	Cisco Secure ACS 3.x、4.x、および 5.0	Cisco Secure ACS 5.1	Cisco Secure ACS 5.2	Cisco Secure ACS 5.3
Cisco ISE 1.0	非サポート	サポート対象	非サポート	非サポート
Cisco ISE 1.1	非サポート	サポート対象	サポート対象	非サポート
Cisco ISE 1.2	非サポート	非サポート	非サポート	サポート対象

関連項目

Cisco Secure ACS Release 5.3 からのデータの移行については、第 3 章「Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 へのデータの移行」を参照してください。

Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のポリシー モデル

認証ポリシーおよび許可ポリシーは、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行されます。Cisco Secure ACS と Cisco ISE の両方にはシンプルなルール ベースの認証パラダイムがありますが、Cisco Secure ACS と Cisco ISE は異なるポリシー モデルに基づいており、そのため Cisco Secure ACS ポリシーから Cisco ISE への移行が少し複雑になります。

ただし、Cisco ISE Release 1.2 は、Cisco Secure ACS Release 5.3 のサービス セレクション ポリシー（SSP）に類似した、ポリシー セットと呼ばれる新しいポリシー モデルをサポートし、ポリシー移行プロセスの簡素化に役立っています。

Cisco Secure ACS 5.3 と Cisco ISE のポリシー モデルの違い

- Cisco Secure ACS Release 5.3 サービス セレクション ポリシー（SSP）は、SSP のルールに基づいて適切なサービスに要求を配信しますが、Cisco ISE ポリシー セットは、ポリシー セットのエントリ基準を含むルールを保持します。ポリシー セットの順序はエントリ ルールと同じ順序で、SSP ルールの順序に類似しています。
- サービスを要求せずにポリシー サービスを定義でき、それは、Cisco Secure ACS の SSP ルールによってポリシー サービスを非アクティブと定義できることを意味します。しかし、Cisco ISE のポリシー セットを参照するエントリ ルールのないのポリシー セットを持つことはできません。
- Cisco Secure ACS で SSP ルールを無効またはモニタ対象と定義でき、ポリシー セットの同等のエントリ ルールは Cisco ISE で常に有効です。SSP ルールが Cisco Secure ACS で無効またはモニタ対象になっている場合、SSP のルールによって要求されたポリシー サービスは Cisco ISE に移行できません。
- 複数の SSP ルールが Cisco Secure ACS で同じサービスまたはサービスの再利用を要求する場合があります。しかし、各ポリシー セットは独自のエントリ条件を持っているので、Cisco ISE でポリシー セットを再利用することはできません。複数の SSP ルールによって要求された 1 つのサービスを移行する場合、そのサービスのコピーである複数のポリシー セットを作成する必要があります。つまり、Cisco Secure ACS で同じサービスを要求する SSP ルールごとに Cisco ISE のポリシー セットを作成する必要があります。

- Cisco Secure ACS Release 5.3 には、既成の DenyAccess サービスがあり、そのサービスは Cisco Secure ACS のデフォルトの SSP ルールの、ポリシーも許可されるプロトコルも持たず、自動的にすべての要求を拒否します。Cisco ISE には同等のポリシー セットはありません。
- ID ポリシーは、Cisco Secure ACS Release 5.3 の ID ソース（ID ソースおよび ID ストア順序）になるルールのフラットなリストです。認証ポリシーは、2 レベルのルール、外部ポリシー ルール、内部ポリシー ルールを保持します。外部ポリシーは許可されるプロトコルになり、内部ポリシー ルールのセットへのエントリ基準です。内部ポリシー ルールは ID ソースになります。
- 許可されるプロトコルは、（特定のポリシーに接続されるのでなく）Cisco Secure ACS Release 5.3 で条件付けられていない（サービス全体を指す SSP の条件を除く）サービス全体に接続されます。許可されるプロトコルは、Cisco ISE で条件付けられた外部ルールの結果としての認証ポリシーだけに適用されます。
- Cisco Secure ACS Release 5.3 および Cisco ISE Release 1.2 の両方に、各許可ポリシーに接続されるオプションの例外ポリシーが含まれます。Cisco ISE Release 1.2 には、例外ポリシーに加えて、すべての許可ポリシーに影響を与えるオプションのグローバル例外ポリシーがあります。Cisco Secure ACS Release 5.3 には、グローバル例外ポリシーに相当するものがありません。許可のために、ローカル例外ポリシーが最初に処理され、続いてグローバル例外ポリシーおよび許可ポリシーが処理されます。

Cisco ISE および Cisco Secure ACS の導入モデル

Cisco Identity Services Engine（ISE）の導入モデルは、1 つのプライマリ ノードと複数のセカンダリ ノードで構成されます。展開内の各 Cisco ISE ノードには、Administration、Policy Service、Monitoring のペルソナいずれか 1 つ以上を設定することができます。Cisco ISE をインストールした後は、すべてのノードがスタンドアロンの状態になります。Cisco ISE ノードのいずれか 1 つを、Administration ペルソナとして稼働するプライマリに定義する必要があります。プライマリ ノードを定義すると、ネットワークに対して、Policy Service ペルソナや Monitoring ペルソナで他の Cisco ISE ノードのペルソナを設定できます。次に、プライマリ ノードに他のセカンダリ ノードを登録し、相互に特定のロールを定義できます。Cisco ISE ノードをセカンダリ ノードとして登録すると、Cisco ISE はプライマリ ノードからセカンダリ ノードへのデータベース リンクをすぐに作成し、複製のプロセスを開始します。すべての設定変更はプライマリの Administration ISE ノード上で行われ、セカンダリ ノードへ複製されます。Monitoring ISE ノードはログ コレクタとして機能します。

Cisco Secure Access Control System（ACS）の導入モデルは、1 つのプライマリ、および複数のセカンダリ Cisco Secure ACS サーバで構成されます。ここで設定の変更は、プライマリ Cisco Secure ACS サーバ上で行われます。これらの設定はセカンダリ Cisco Secure ACS サーバへ複製されます。すべてのプライマリおよびセカンダリ Cisco Secure ACS サーバで AAA 要求を処理できます。プライマリ Cisco Secure ACS サーバは Monitoring Viewer および Report Viewer のデフォルトのログ コレクタでもありますが、任意の Cisco Secure ACS サーバをログ コレクタに設定することができます。

移行機能

移行ツールは、Cisco Secure ACS データを Cisco ISE へ転送し、主要な 3 つの手順を実行します。

1. Cisco Secure ACS からデータをエクスポートする。
2. 移行ツール内でデータを保持する。
3. Cisco ISE にデータをインポートする。

Cisco Secure ACS 5.3 から Cisco ISE Release 1.2 への移行プロセスの主な機能は以下のとおりです。

- 「データのエクスポート」（P.1-4）
- 「データの持続性」（P.1-4）
- 「データのインポート」（P.1-4）
- 「オブジェクトの拡張性」（P.1-4）
- 「ハイ アベイラビリティ」（P.1-5）
- 「レポート」（P.1-5）
- 「UTF-8 のサポート」（P.1-7）
- 「ISE 802.1X サービスに対する FIPS サポート」（P.1-8）
- 「Cisco Secure ACS/Cisco ISE バージョンの検証」（P.1-9）

データのエクスポート

移行プロセスの最初のステージは、Cisco Secure ACS の Programmatic Interface（PI）を使用して Cisco Secure ACS データをエクスポートすることです。データのエクスポート元である Cisco Secure ACS Release 5.3 システムへログインし、データを移行アプリケーションにエクスポートするように要求します。エクスポートされたデータを Cisco ISE Release 1.2 アプライアンスへ正常にインポートできるかどうかを確認するために、検証します。データが不正な場合、ステータスがエクスポート レポートに記録されます。

データの持続性

Cisco ISE は、Cisco Secure ACS から Cisco ISE へのアップグレードをサポートしていません。このため、Cisco Secure ACS アプライアンスから Cisco ISE へアップグレードする場合は、Cisco Secure ACS Release 5.3 をアンインストールし、Cisco ISE Release 1.2 メージでアプライアンスを再作成する必要があります。再作成が行われ、インポート ステージが始まる前に、移行ツールは Cisco Secure ACS データを保持します。保持されているデータは、暗号化形式になっています。

データのインポート

インポート ステージでは、移行ツールに Cisco Secure ACS からの情報が含まれており、Cisco ISE へデータをインポートする準備ができています。Cisco ISE をインストールするのに同じマシンを使用する場合は、Cisco ISE Release 1.2 イメージで Cisco Secure ACS マシンを再作成し、インポート操作を開始する必要があります。Cisco ISE に対して別のマシンを使用する場合は、インストール直後で何も設定されていないクリーンなマシンを使用します。

インポートの進捗を表示するには、Cisco Secure ACS-Cisco ISE Migration Tool のユーザ インターフェイスを使用します。転送中のオブジェクト タイプ、および配信に対して保留中になっているオブジェクトの数を参照できます。このプロセス中のすべてのエラーは、インポート レポートに記録されます。

オブジェクトの拡張性

移行ツールは、表 1-2 に記載されているオブジェクトのスケールをサポートしています。

表 1-2　Cisco Secure ACS から Cisco ISE Release 1.2 への移行に対するオブジェクトの拡張性

オブジェクト	小規模な展開	中規模な展開	大規模な展開
1 つの展開あたりのユーザ（AD[1] /LDAP[2] / 内部）	1,000	10,000	25,000
ホスト/エンドポイント	1,000	10,000	100,000
ネットワーク デバイス	500	1,000	10,000
ID グループ	1	5	20
許可プロファイル	5	10	30
ユーザ ディクショナリ	2	5	20
ユーザ属性	1	5	8
ユーザ グループ	2	10	100
DACL[3]（それぞれ 1,600 エントリが含まれている）	5	20	50

1. AD は Microsoft Windows Active Directory の頭文字です（Glossary の Active Directory を参照してください）。
2. LDAP は Lightweight Directory Access Protocol の頭文字です（Glossary の LDAP を参照してください）。
3. DACL はダウンロード可能アクセス コントロール リストの頭文字です（Glossary の DACL を参照してください）。

ハイ アベイラビリティ

Cisco Secure ACS to Cisco ISE Migration Tool は、インポートまたはエクスポート操作の各ステージのチェックポイントを保持します。これは、インポートまたはエクスポート プロセスが失敗しても、プロセスを最初から再起動する必要がないことを意味します。障害発生前の最後のチェックポイントから開始できます。

移行プロセスが失敗すると、移行ツールはプロセスを終了します。障害の後で移行ツールを再起動すると、ダイアログボックスが表示され、以前のインポートまたはエクスポートを再開するか、または、以前のプロセスを破棄し、新しい移行プロセスを開始するか選択できます。前のプロセスを再開することを選択した場合、移行プロセスは最後のチェックポイントから再開されます。障害が発生した時点から再開する場合、前のプロセスから実行するためにレポートも再開されます。

レポート

3 つの Cisco ISE レポートは、Cisco Secure ACS 5.3 データの移行中に生成されます。レポート ファイルを他のユーザと共有する場合、または他の場所に保存する場合は、移行ツールのディレクトリの Reports フォルダにレポート ファイルがあります。

- import_report.txt
- export_report.txt
- policy_gap_report.txt

エクスポート レポート：Cisco Secure ACS データベースのデータをエクスポートするときに発生した特定の情報またはエラーについて示します。レポートの最後にはデータ分析のセクションがあり、Cisco Secure ACS と Cisco ISE 間の機能ギャップについて記載されます。エクスポート レポートには、インポートされないエクスポートされたオブジェクトのエラー情報が含まれます。表 1-3 を参照してください。

表 1-3　Cisco Secure ACS to Cisco ISE Migration Tool のエキスポート レポート

レポート タイプ	メッセージタイプ	メッセージの説明
エクスポート	情報	正常にエクスポートされたデータ オブジェクトの名前が示されます。
	警告	エクスポートの障害、または（TACACS ベースのデバイスなど）データ オブジェクトが Cisco ISE Release 1.2 でサポート対象外であるため試行されなかったにエクスポートが示されます。

インポート レポート：Cisco ISE アプライアンスへデータをインポートするときに発生した特定の情報またはエラーについて示します。表 1-4 を参照してください。

表 1-4　Cisco Secure ACS to Cisco ISE Migration Tool のインポート レポート

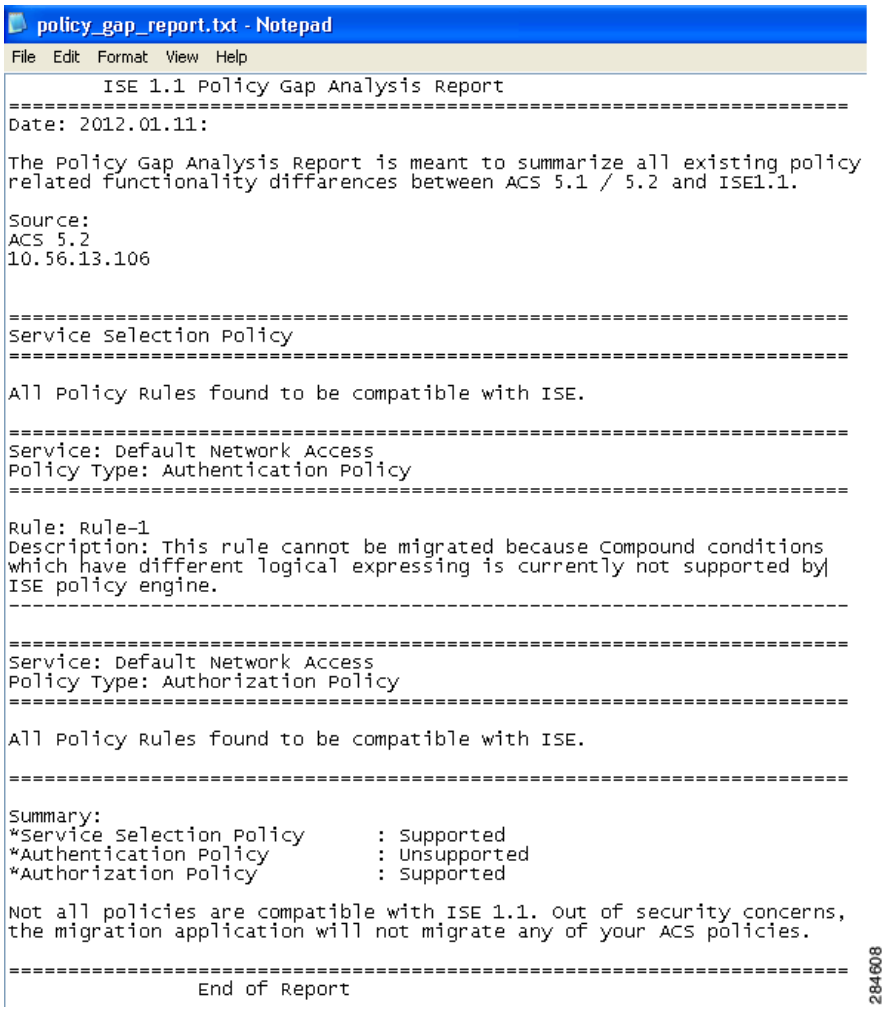
レポート タイプ	メッセージタイプ	メッセージの説明
インポート	情報	正常にインポートされたデータ オブジェクトの名前が示されます。
	エラー	データ オブジェクトのエラーの原因を次のように識別します。 • オブジェクトがすでに存在します • オブジェクト名が文字数制限を超えています • オブジェクト名にサポートされていない特殊文字が含まれています • オブジェクトにサポートされていないデータ文字が含まれています

ポリシー ギャップ分析レポート：Cisco Secure ACS と Cisco ISE 間のポリシー ギャップに関連する特定の情報について示し、エクスポートの完了後に移行ツールのユーザ インターフェイスで [ポリシー ギャップ分析レポート（Policy Gap Analysis Report）] ボタンをクリックして使用できます。図 1-1 を参照してください。

エクスポート フェーズ中に、移行ツールは、認証および許可ポリシーのギャップを識別します。いずれかのポリシーが移行されなかった場合は、ポリシーがポリシー ギャップ分析レポートに記載されます。レポートには、ポリシーに関連して、矛盾するルールおよび条件がすべて記載されます。また、移行できなかったデータ、および手動で対応した理由についても記載されます。

条件の中には、Cisco ISE の用語を使用して自動的に移行できるものがあります。たとえば、「Device Type In」と名付けられた条件は「Device Type Equals」として移行されます。条件がサポートされている場合、または自動的に変換可能な場合は、その条件はレポートには記載されません。「Not Supported」または「Partially supported」として条件が検出された場合、ポリシーはインポートされずに、条件がレポートに記載されます。移行の実施管理者は、責任を持って条件の修正または削除を行う必要があります。それらが修正または削除されない場合、ポリシーは Cisco ISE へ移行されません。

図 1-1　ポリシー ギャップ分析レポートの例



UTF-8 のサポート

Cisco ISE Release 1.2 は、いくつかの管理設定に対して 8 ビットの Unicode Transformation Format（UTF-8）をサポートしています。以下の設定項目は、UTF-8 エンコーディングでエクスポートおよびインポートされます。

- **ネットワーク アクセスのユーザ設定**
  - ユーザ名
  - パスワードおよびパスワードの再入力
  - 名
  - 姓
  - E メール
- **RSA**：RSA プロンプトおよびメッセージは、サプリカントによってエンドユーザに示されます。
  - メッセージ
  - プロンプト

- **RADIUS トークン**：RADIUS トークン プロンプトは、エンド ユーザのサプリカントに示されます。
  - [認証（Authentication）] タブ > [プロンプト（Prompts）]
  - 管理設定
  - 管理者のユーザ名およびパスワード
  - UTF-8 を使用した管理者の設定
- **ポリシー**：
  - [認証（Authentication）] > [AV 式の値（Value for AV expression）]
  - [許可（Authorization）] > [その他の条件（Other Conditions）] > [AV 式の値（Value for AV expression）]
  - 属性 - 値の条件
  - [認証（Authentication）] > [単純条件 / 複合条件（Simple Condition/compound Condition）] > [AV 式の値（Value for AV expression）]
  - [許可（Authorization）] > [単純条件 / 複合条件（Simple Condition/compound Condition）] > [AV 式の値（Value for AV expression）]

ISE 802.1X サービスに対する FIPS サポート

連邦処理標準（FIPS）をサポートするために、Cisco Secure ACS-Cisco ISE Migration Tool はデフォルトのネットワーク デバイス キーラップ データを移行します。

（注） 移行プロセスを完了する前に、Cisco ISE FIPS モードは有効にしないでください。

FIPS 準拠およびサポートされているプロトコル：

- Process Host Lookup
- Extensible Authentication Protocol-Translation Layer Security（EAP-TLS）
- Protected Extensible Authentication Protocol（PEAP）
- EAP-Flexible Authentication via Secure Tunneling（FAST）

FIPS 非準拠およびサポート対象外のプロトコル：

- EAP- メッセージ ダイジェスト 5（MD5）
- Password Authentication Protocol および ASCII
- Challenge Handshake Authentication Protocol（CHAP）
- Microsoft Challenge Handshake Authentication Protocol version 1（MS-CHAPv1）
- Microsoft Challenge Handshake Authentication Protocol version 2（MS-CHAPv2）
- Lightweight Extensible Authentication Protocol（LEAP）

Cisco Secure ACS/Cisco ISE バージョンの検証

Cisco Secure ACS to Cisco ISE Migration Tool はエクスポート フェーズを開始する前に、Cisco Secure ACS release のバージョンを特定します。Cisco Secure ACS のバージョンが 5.3 よりも古いかまたは新しい場合、移行プロセスは開始されません。また、Cisco ISE へデータをインポートする前に、この移行ツールで Cisco ISE release のバージョンが 1.2 であることを検証します。