CHAPTER 1

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行概要

この章では、Cisco Identity Services Engine（ISE）および Cisco Secure Access Control System（ACS）の概要について説明します。この章の内容は、次のとおりです。

概要

Cisco ISE の展開モデルは、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、および 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、プライマリに定義する（Administration ペルソナとして稼働する）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 や Monitoring などの他の 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。

1 つの 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）の展開モデルは、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。

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することが可能で、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つことができます。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、移行ツールおよび手順を使用できます。この手順では、Cisco Secure ACS からデータを読み込み、Cisco ISE 内に対応するデータを作成します。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、この移行手順を使用できます。Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行プロセスでは、必要なユーザの介入は最小限で、Cisco Secure ACS から Cisco ISE へすべての設定データを移行できます。

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

Cisco ISE は、Cisco Secure ACS-ISE 1.1 Migration Tool を使用して Cisco Secure ACS 5.1 および 5.2 からのデータ移行をサポートしています。Cisco Secure ACS 3.x または Cisco Secure ACS 4.x を実行する場合、最初に Cisco Secure ACS 5.0 へアップグレードする必要があります。

Cisco Secure ACS 5.0 へのアップグレード後、Cisco Secure ACS 5.1 または 5.2 へアップグレードできます。この時点で、Cisco Secure ACS-ISE Migration Tool を使用して Cisco ISE 1.1 へ移行できます。

（注）　Cisco Secure ACS 5.0 から Cisco Secure ACS 5.1/5.2 へ直接アップグレードすることも可能です。Cisco Secure ACS から Cisco ISE への移行を試行する前に、Cisco Secure ACS の以前のリリースから Cisco Secure ACS 5.1/5.2 へのすべてのアップグレードを完了しておく必要があります。

Cisco Secure ACS 3.x または 4.x から Cisco Secure ACS 5.0 へのデータ移行については、第 5 章「Cisco Secure ACS 3.x および 4.x から ACS 5.1/5.2 へのデータ移行」を参照してください。

ソフトウェア要件

表 1-1 に、Cisco ISE 1.1 で移行を行うための最小限のソフトウェア要件を記載しています。

表 1-1　Cisco ISE 1.1 で移行するためのソフトウェア要件

オペレーティング システム	Cisco Secure ACS-Cisco ISE Migration Tool は Windows および Linux マシン上で稼働します。マシンには、Java をインストールしておく必要があります。詳細については、「システム要件」（P.3-2）を参照してください。
最小ディスク領域	必要な最小ディスク領域は 1 GB です。 この領域は、移行ツールのインストールでのみ必要なわけではありません。移行ツールで、移行したデータを保存し、レポートやログを生成する目的でも領域を使用します。
最小構成の RAM	必要な最小 RAM は 2 GB です。 約 300,000 人のユーザ、50,000 個のホスト、50,000 個のネットワーク デバイスを備えている場合、最小 RAM として 2 GB を推奨しています。

Cisco Secure ACS-Cisco ISE Migration Tool を実行する前に、Cisco ISE Release 1.1 へのアップグレードが完了していること、および ACS 5.1 と 5.2 の最新パッチをインストールしていることを確認してください。

機能説明

移行ツールは、Cisco Secure ACS データを Cisco ISE へ転送します。ここでは主に次の 3 つの手順があります。

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. データを Cisco ISE 1.1 へインポートする。

Cisco Secure ACS 5.1/5.2 から Cisco ISE 1.1 への移行プロセスの主な機能は以下のとおりです。

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 ACS データをエクスポートすることです。Cisco Secure ACS と接続し、Cisco Secure ACS データを移行アプリケーションへエクスポートするよう要求するには、クレデンシャルを提供する必要があります。この間に、エクスポートされたデータを Cisco ISE 1.1 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、検証する必要があります。データが不正な場合、このステータスは移行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 1.1 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 をアンインストールし、Cisco ISE 1.1 イメージでアプライアンスを再作成する必要があります。再作成が行われる前、および次のステージ（インポート）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。

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 1.1 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 1.1 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なければなりません。

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、移行レポートに記録されます。

拡張性

移行アプリケーションは、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 ISE 1.1 で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-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ステートを保持します。これにより、インポートまたはエクスポートで障害が発生したために、いずれかのポイントでインポートまたはエクスポートのプロセスが失敗した場合でも、最初から開始するのではなく、障害の発生前で、発生したタイミングに一番近いチェックポイントから開始することができます。

インポートまたはエクスポートのフェーズで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。障害の後で移行を再開すると、ダイアログボックスが表示されます。

前のインポート/エクスポートを再開するか、前のプロセスを廃棄して新しいプロセスを開始するか、選択することができます。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オブジェクト タイプから再開されます。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

Cisco Secure ACS-Cisco ISE Migration Tool を使用して、Cisco Secure ACS 5.1/5.2 のデータを Cisco ISE アプライアンスへ移行する場合に、以下の 3 つのレポートを使用できます。

- **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。図 1-1 を参照してください。

  エクスポート レポートには、エクスポートされるがインポートされないオブジェクトのエラー情報が含まれます。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 間のデータの機能ギャップ分析について記載されます。

- **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。図 1-2 を参照してください。

- **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ます。図 1-3 を参照してください。

  Cisco ISE 1.1 は、この新しいレポートを導入しています。このレポートはエクスポートが完了した後で使用できます。レポートを表示するには、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ます。

  いずれかの認証ポリシーまたは許可ポリシーが移行されなかった場合は、ポリシーがこのレポートに記載されます。このレポートには、2 つの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 の用語を使用して移行できるものがあります。たとえば、「Device Type In」は「Device Type Equals」として移行されます。このような場合には、条件は自動的に移行されます。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 1 つ以上の条件が検出された場合、ポリシー全体はインポートされずに、それらの条件がレポートに記載されます。

表 1-3 で、インポート レポートおよびエクスポート レポートのレポート タイプ、メッセージ タイプ、メッセージの内容について説明します。

表 1-3　Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool のレポート

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に基づいたエラー、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 1.1 でサポート対象外であるためにエクスポートが試行されなかったことによるエラーが示されます。

表 1-3　Cisco Secure ACS 5.1/5.2-Cisco ISE Migration Tool のレポート （続き）

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 オブジェクトがすでに存在（重複）するためにインポートできないデータ オブジェクト エラーが示されます。
	エラー	名前の長さが Cisco ISE の文字数制限を超えているためにインポートできないデータ オブジェクト エラーが示されます。
	エラー	Cisco ISE でサポートしていない特殊文字が名前に含まれているために、インポートできないデータ オブジェクト エラーが示されます。
	エラー	Cisco ISE で使用できない、またはサポートされていないデータ文字がオブジェクトに含まれているために、インポートできないデータ オブジェクト エラーが示されます。

図 1-1　エクスポート レポートの例

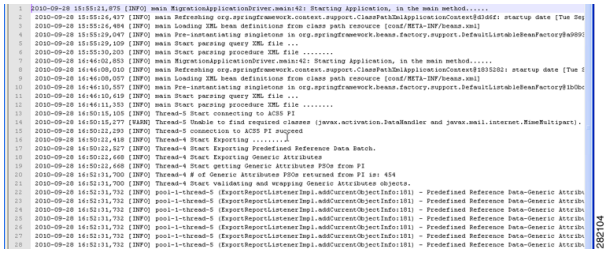
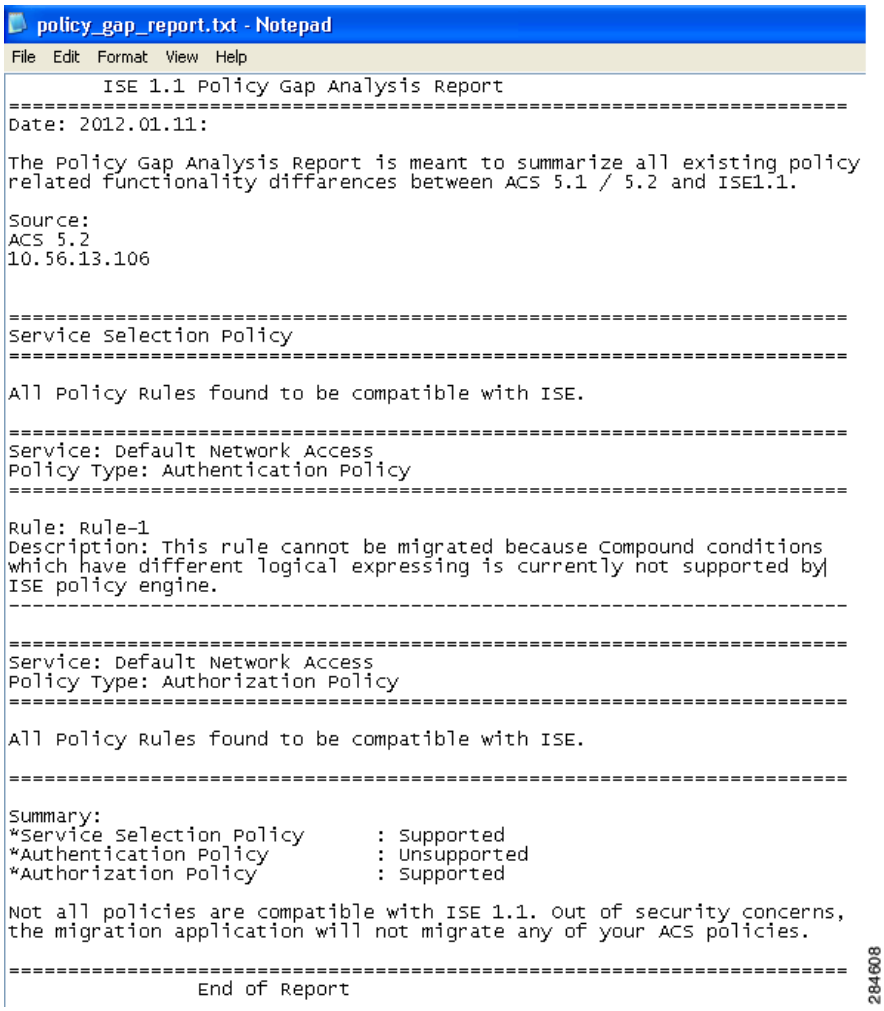


図 1-2　インポート レポートの例

```
==========================================================
Migration Report
Migration Phase: Import into ISE
Date: Tue Sep 28 17:05:59 IST 2010
Machine: 10.56.13.190
==========================================================


==========================Object Group==============================
Object Group: Predefined Reference Data
==========================Object Group==============================
Object Group: Dictionaries
==========================Object Type===============================
Object Type: VSA Vendors

Info Type: INFO
> 2010.09.28 17:06:07'055 : Added configuration: Cisco VPN 5000
> 2010.09.28 17:06:07'945 : Added configuration: US Robotics
> 2010.09.28 17:06:08'633 : Added configuration: Ascend
> 2010.09.28 17:06:09'367 : Added configuration: Nortel ( Bay )
> 2010.09.28 17:06:10'117 : Added configuration: RedCreek
> 2010.09.28 17:06:10'867 : Added configuration: Juniper
> 2010.09.28 17:06:11'586 : Added configuration: Cisco Aironet
> 2010.09.28 17:06:12'320 : Added configuration: Cisco Airespace

==========================Object Type===============================
Object Type: RADIUS VSAs

Info Type: INFO
> 2010.09.28 17:06:13'523 : Added configuration: Cisco
> 2010.09.28 17:06:14'148 : Added configuration: Cisco
> 2010.09.28 17:06:14'774 : Added configuration: Cisco
> 2010.09.28 17:06:15'477 : Added configuration: Cisco
> 2010.09.28 17:06:16'086 : Added configuration: Cisco
> 2010.09.28 17:06:16'680 : Added configuration: Cisco
> 2010.09.28 17:06:17'430 : Added configuration: Cisco
> 2010.09.28 17:06:18'242 : Added configuration: Cisco
> 2010.09.28 17:06:18'867 : Added configuration: Cisco
> 2010.09.28 17:06:19'477 : Added configuration: Cisco
> 2010.09.28 17:06:20'070 : Added configuration: Cisco
> 2010.09.28 17:06:20'664 : Added configuration: Cisco
> 2010.09.28 17:06:21'305 : Added configuration: Cisco
> 2010.09.28 17:06:21'914 : Added configuration: Cisco
> 2010.09.28 17:06:22'539 : Added configuration: Cisco
> 2010.09.28 17:06:23'180 : Added configuration: Cisco
> 2010.09.28 17:06:23'774 : Added configuration: Cisco
> 2010.09.28 17:06:24'383 : Added configuration: Cisco
```

282105

図 1-3　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 1.1 は、いくつかの管理設定に対して Universal Character Set Transformation Format 8 ビット（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-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 のバージョンを特定します。Cisco Secure ACS のバージョンが 5.1 よりも古い場合、または 5.2 よりも新しい場合、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 のバージョンが 1.1 であることを検証します。