データ構造マッピング

この付録では、Cisco Secure ACS リリース 5.5 または 以降から Cisco ISE リリース 2.3 に移行されるデータ オブジェクト、一部が移行されるデータ オブジェクト、および移行されないデータ オブジェクトについて説明します。

- データ構造マッピング，1 ページ
- Cisco Secure ACS 4.2 からの移行でサポートされるデータ オブジェクト，1 ページ
- 移行されるデータ オブジェクト，2 ページ
- 一部が移行されるデータ オブジェクト，4 ページ
- 移行されないデータ オブジェクト，4 ページ
- データ情報マッピング，5 ページ

データ構造マッピング

へのデータ構造マッピングは、エクスポートフェーズの実行時に移行ツールでデータ オブジェクトを分析および検証するプロセスです。

Cisco Secure ACS 4.2 からの移行でサポートされるデータ オブジェクト

Cisco Secure ACS 4.2 から Cisco ISE 2.3 への移行でサポートされるデータ オブジェクトは次のとおりです。

- ユーザ
- ユーザ グループ
- ユーザ属性

- ネットワーク デバイス
- ネットワーク デバイス グループ（NDG）ノード
- NDG ルート タイプ

移行されるデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure ACS リリース 5.5 以降から Cisco ISE に移行されます。

- ネットワーク デバイス グループ（NDG）タイプと階層
- IPv4 または IPv6 アドレスを持つネットワーク デバイス
- デフォルト ネットワーク デバイス
- ネットワーク デバイスの範囲（すべてのオクテット内）
- 外部 RADIUS サーバ
- 外部 TACACS+ サーバ
- TACACS+ サーバの順序
- TACACS+ 設定
- ステートレス セッション再開機能の設定
- ID グループ
- 内部ユーザ
- 内部ユーザ認証キャッシュ
- イネーブル パスワードの変更がある内部ユーザ
- パスワード タイプが外部 ID ストアとして設定された内部ユーザ
- 日付が超過している場合のユーザ アカウントの無効化
- n 日間の非アクティブ後にユーザ アカウントを無効にするためのグローバル オプション
- 内部エンドポイント（ホスト）
- Lightweight Directory Access Protocol（LDAP）
- LDAP ID ストアのグループ名属性に対する共通名と識別名
- Microsoft Active Directory（AD）
- RSA
- RADIUS トークン
- 証明書認証プロファイル

- 日時条件（部分的にサポート。「サポートされていないルール要素」を参照）
- ネットワーク条件（エンド ステーション フィルタ、デバイス フィルタ、デバイス ポート フィルタ）
- 最大ユーザ セッション数
- RADIUS 属性およびベンダー固有属性（VSA）の値
- RADIUS ベンダー ディクショナリ
- 内部ユーザ属性
- 内部エンドポイント属性
- TACACS+ プロファイル
- ダウンロード可能アクセス コントロール リスト（DACL）
- ID（認証）ポリシー
- TACACS+ の認証、認可、承認の例外ポリシー（ポリシー オブジェクトの場合）
- 日時条件
- TACACS+ コマンド セット
- ネットワーク アクセスの許可例外ポリシー
- ネットワーク アクセスのサービス選択ポリシー
- RADIUS プロキシ サービス
- TACACS+ プロキシ サービス
- ユーザ パスワードの複雑度
- ID 順序および RSA プロンプト
- UTF-8 データ
- EAP 認証プロトコル：PEAP-TLS
- ユーザ チェック属性
- ダイヤルイン属性
- 暗号バインディング属性
- 許可されているプロトコルに対する脆弱な暗号サポート
- ID 順序の高度なオプション
- ポリシー条件で使用可能な追加属性：AuthenticationIdentityStore
- 追加の文字列演算子：Start with、Ends with、Contains、Not contains
- RADIUS ID サーバ属性

- EAP-MD5、EAP-TLS、LEAP、PEAP および EAP-FAST 認証における長さを含むフラグ（L ビット）

一部が移行されるデータ オブジェクト

次のデータ オブジェクトは、Cisco Secure ACS リリース 5.5 または 以降から Cisco ISE リリース 2.3 に部分的に移行されます。

- IP アドレスと日付型のホスト属性は移行されない。
- RSA sdopts.rec ファイルおよびセカンダリ情報は移行されない。
- マルチ Active Directory ドメイン（プライマリに結合された Active Directory ドメインのみ）は移行される。
- プライマリ ACS インスタンスに定義された LDAP 設定は移行される。セカンダリ ACS インスタンス固有の設定は移行されない。

移行されないデータ オブジェクト

次のデータ オブジェクトは、Cisco Secure ACS リリース 5.5 以降から Cisco ISE リリース 2.3 に移行されません。

- モニタリング レポート
- スケジュール バックアップ
- リポジトリ
- 管理者、ロール、および管理者の設定
- カスタマー/デバッグ ログ設定
- 展開情報（セカンダリ ノード）
- 証明書（認証局およびローカル証明書）
- Trustsec 関連の設定
- RSA ノード欠落の秘密の表示
- ポリシー条件で使用可能な追加属性：NumberOfHoursSinceUserCreation
- ホストのワイルドカード
- OCSP サービス
- SSL/TCP 経由の syslog メッセージ
- 設定可能な著作権バナー

データ情報マッピング

この項には、エクスポート プロセス中にマッピングされるデータ情報を一覧表示する表が記載されています。これらの表には、Cisco Secure ACS リリース 5.5 または 以降からのオブジェクト カテゴリと、Cisco ISE リリース 2.3 における対応カテゴリが含まれています。この項のデータマッピング表には、移行プロセスのエクスポート ステージのデータ移行時にマップされるデータ オブジェクトのステータス（有効または無効）が記載されています。

ネットワーク デバイス マッピング

Cisco Secure ACS のプロパティ	**Cisco ISE** のプロパティ
Name	そのまま移行
Description	そのまま移行
Network device group	そのまま移行
Single IP address	そのまま移行
Single IP and subnet address	そのまま移行
IP 範囲	[IP の除外（Exclude IP）] オプションがあるすべてのオクテットの IP 範囲が移行されます
TACACS information	そのまま移行
RADIUS shared secret	そのまま移行
TACACS+ Shared Secret	そのまま移行
CTS	そのまま移行
SNMP	SNMP データは Cisco ISE でのみ使用できるため、移行されたデバイス用の SNMP 情報はありません。
Model name	このプロパティは Cisco ISE でのみ有効です（値はデフォルトで「unknown」）。
Software version	このプロパティは Cisco ISE でのみ有効です（値はデフォルトで「unknown」）。

NDG タイプ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description

（注） Cisco Secure ACS リリース 5.5 または以降は、同じ名前の複数のネットワーク デバイス グループ（NDG）をサポートできます。Cisco ISE リリース 2.3 は、この命名方式をサポートしていません。したがって、定義されている名前の最初の NDG タイプのみが移行されます。

NDG 階層マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Parent	このプロパティには特別なプロパティは関連付けられません。この値は、NDG 階層名の一部としてのみ入力されるためです（NDG タイプはこのオブジェクト名のプレフィックスです）。

デフォルト ネットワーク デバイスのマッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Default network device status	Default network device status
Network device group	移行されない
TACACS+ 共有秘密	共有秘密鍵（Shared Secret）
TACACS+ Single Connect デバイス	シングル接続モードを有効にする（Enable Single Connect Mode）
レガシー TACACS+ Single Connect サポート	レガシー シスコ デバイス

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
TACACS+ ドラフト準拠 Single Connect サポート	TACACS+ ドラフト コンプライアンス Single Connect サポート
RADIUS - shared secret	共有秘密鍵（Shared Secret）
RADIUS - CoA port	移行されない
RADIUS - Enable keywrap	Enable keyWrap
RADIUS - Key encryption key	Key encryption key
RADIUS - Message authenticator code key	Message authenticator code key
RADIUS - Key input format	Key input format

ID グループ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Parent	このプロパティは、階層の詳細の一部として移行されます。

（注） Cisco ISE リリース 2.3 には、ユーザ ID グループとエンドポイント ID グループが含まれています。Cisco Secure ACS リリース 5.5 または以降の ID グループは Cisco ISE リリース 2.3 へ、ユーザ ID グループおよびエンドポイント ID グループとして移行されます。これは、ユーザをユーザ ID グループに割り当て、エンドポイントをエンドポイント ID グループに割り当てる必要があるためです。

ユーザ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Description	Description
Status	このプロパティは移行する必要ありません。（このプロパティは Cisco ISE には存在しません）
Identity group	Cisco ISE の ID グループへ移行します
Password	Password
Enable password	Password
Change password on next login	移行されない
User attributes list	ユーザ属性は Cisco ISE からインポートされ、ユーザに関連付けられます
Expiry days	サポート対象

ホスト（エンドポイント）マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
MAC address	そのまま移行
Status	移行されない
Description	そのまま移行
Identity group	エンドポイント グループとの関連を移行します。
Attribute	エンドポイント属性が移行されます。
Authentication state	これは Cisco ISE でのみ有効なプロパティです（値は固定値「Authenticated」）。
Class name	これは Cisco ISE でのみ有効なプロパティです（値は固定値「TBD」）。
Endpoint policy	これは Cisco ISE でのみ有効なプロパティです（値は固定値「Unknown」）。
Matched policy	これは Cisco ISE でのみ有効なプロパティです（値は固定値「Unknown」）。

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Matched value	これは Cisco ISE でのみ有効なプロパティです（値は固定値「0」）。
NAS IP address	これは Cisco ISE でのみ有効なプロパティです（値は固定値「0.0.0.0」）。
OUI	これは Cisco ISE でのみ有効なプロパティです（値は固定値「TBD」）。
Posture status	これは Cisco ISE でのみ有効なプロパティです（値は固定値「Unknown」）。
Static assignment	これは Cisco ISE でのみ有効なプロパティです（値は固定値「False」）。

LDAP マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Server connection information	そのまま移行。
Directory organization information	そのまま移行。
Directory groups	そのまま移行
Directory attributes	移行は（Cisco Secure ACS to Cisco ISE Migration Tool を使用して）手動で行われます。

（注） プライマリ ACS インスタンスに定義された LDAP 設定のみ移行されます。

Active Directory マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
ドメイン名（Domain Name）	そのまま移行

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
ユーザ名（User name）	そのまま移行
パスワード（Password）	そのまま移行
Allow password change	そのまま移行
Allow machine access restrictions	そのまま移行
Aging time	そのまま移行
User attributes	そのまま移行
グループ（Groups）	そのまま移行
Multiple domain support	プライマリ ACS インスタンスに結合されているドメインのみ移行

証明書認証プロファイルのマッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Principle user name（X.509 属性）	Principle user name（X.509 属性）
Binary certificate comparison with certificate from LDAP or AD	Binary certificate comparison with certificate from LDAP or AD
AD or LDAP name for certificate fetching	AD or LDAP name for certificate fetching。

ID ストア順序マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Certificate based, certificate authentication profile	Certificate based, certificate authentication profile
Password based	Authentication search list
Advanced options > if access on current IDStore fails than break sequence	Do not access other stores in the sequence and set the “AuthenticationStatus” attribute to “ProcessError.”
Advanced options > if access on current IDStore fails then continue to next	Treated as “User Not Found” and proceed to the next store in the sequence.
Attribute retrieval only > exit sequence and treat as “User Not Found”	未サポート（無視される）

許可プロファイルのマッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
DACLID（ダウンロード可能 ACL ID）	そのまま移行
Attribute type（静的および動的）	• 静的属性の場合はそのまま移行されます。 • 動的属性の場合はそのまま移行されます。
Attributes（静的タイプに対してのみフィルタされる）	RADIUS attributes

シェル プロファイル属性マッピング

Cisco Secure ACS	Cisco ISE
共通タスク属性	
[名前（Name）]	[名前（Name）]
説明	説明

Cisco Secure ACS	Cisco ISE
デフォルト権限（静的および動的）	デフォルト権限（0 ～ 15）
最大権限（静的）	最大権限（0 ～ 15）
アクセス コントロール リスト（静的および動的）	アクセス コントロール リスト（静的および動的）
自動コマンド（静的および動的）	自動コマンド（静的および動的）
コールバック確認なし（静的および動的）	—
エスケープなし（静的および動的）	エスケープなし（True または False）
ハングアップなし（静的および動的）	—
タイムアウト（静的および動的）	タイムアウト（静的および動的）
アイドル時間（静的および動的）	アイドル時間（静的および動的）
コールバック回線（静的および動的）	—
コールバック ロータリー（静的および動的）	—
カスタム属性（Custom Attributes）	
属性（Attribute）	[名前（Name）]
要件（必須およびオプション）	タイプ（必須およびオプション）
値（静的および動的）	値（静的および動的）

コマンド セット属性マッピング

Cisco Secure ACS	Cisco ISE
[名前（Name）]	[名前（Name）]
説明	説明
次の表にないコマンドを許可します	次にリストされていないコマンドを許可します

Cisco Secure ACS	Cisco ISE
付与（許可、拒否、常に拒否）	付与（許可、拒否、常に拒否）
コマンド（Command）	コマンド（Command）
引数	引数

ダウンロード可能な ACL マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
DACL content	DACL content

RADIUS ディクショナリ（ベンダー）マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Vendor ID	Vendor ID
Attribute prefix	このプロパティは移行する必要ありません。
Vendor length field size	Vendor attribute type field length.
Vendor type field size	Vendor attribute size field length.

（注） 移行ツールは、ベンダーの ID と属性に基づいて、ベンダーとその属性の移行をサポートします。

ベンダー名が Cisco Secure ACS でユーザ定義され、Cisco ISE で事前定義されていて、それらの ID が異なる場合、エクスポート プロセスは成功しますがインポート プロセスは失敗します。ベンダー名が Cisco Secure ACS および Cisco ISE で事前定義されていて、それらの ID が同じ場合は、警告メッセージが表示されます。ベンダー名が Cisco Secure ACS でユーザ定義され、Cisco ISE で事前定義されていて、それらの ID が同じ場合、エクスポート プロセスは失敗します。

RADIUS ディクショナリ（属性）マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Attribute ID	この値は NDG 階層名の一部としてのみ入力されるため（NDG タイプはこのオブジェクト名のプレフィックスです）、これに関連する特定のプロパティはありません。
Direction	Cisco ISE ではサポート対象外
Multiple allowed	Cisco ISE ではサポート対象外
Attribute type	そのまま移行
Add policy condition	Cisco ISE ではサポート対象外
Policy condition display name	Cisco ISE ではサポート対象外

（注） Cisco Secure ACS リリース 5.5 または 以降のインストールの一部ではない、ユーザ定義の RADIUS 属性のみ移行する必要があります。

ID ディクショナリ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute	Attribute name
Description	Description
Internal name	Internal name
Attribute type	Data type
Maximum length	移行されない
Default value	移行されない
Mandatory fields	移行されない
ユーザ（User）	ディクショナリ プロパティはこの値（「user」）を承認します。

ID 属性ディクショナリ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Attribute	Attribute name
Description	Internal name
Name	そのまま移行
Attribute type	Data type
該当プロパティなし	Dictionary（ユーザ ID 属性の場合は値「InternalUser」で設定し、ホスト ID 属性の場合は「InternalEndpoint」で設定します）。
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値 = display name
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値 = internal name

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Cisco Secure ACS からまだエクスポートまたは抽出されていない	使用可能な値はデフォルトです。
Maximum length	なし
Default value	なし
Mandatory field	なし
Add policy condition	なし
Policy condition display name	なし

外部 RADIUS サーバ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Server IP address	Hostname
Shared secret	Shared secret
Authentication port	Authentication port
Accounting port	Accounting port
Server timeout	Server timeout
Connection attempts	Connection attempts

外部 TACACS+ サーバ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
IP address	ホスト名/アドレス（Host IP）
接続ポート（Connection Port）	接続ポート（Connection Port）
ネットワーク タイムアウト（Network Timeout）	Timeout
Shared secret	Shared secret

RADIUS トークン マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
Description	Description
Safeword server	Safeword server
Enable secondary appliance	Enable secondary appliance
Always access primary appliance first	Always access primary appliance first
Fallback to primary appliance in minutes	Fallback to primary appliance in minutes
Primary appliance IP address	Primary appliance IP address
Primary shared secret	Primary shared secret
Primary authentication port	Primary authentication port
Primary appliance TO (timeout)	Primary appliance TO
Primary connection attempts	Primary connection attempts
Secondary appliance IP address	Secondary appliance IP address
Secondary shared secret	Secondary shared secret
Secondary authentication port	Secondary authentication port
Secondary appliance TO	Secondary appliance TO
Secondary connection attempts	Secondary connection attempts

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Advanced > treat reject as authentication flag fail	Advanced > treat reject as authentication flag fail
Advanced > treat rejects as user not found flag	Advanced > treat rejects as user not found flag
Advanced > enable identity caching and aging value	Advanced > enable identity caching and aging value
Shell > prompt	Authentication > prompt
Directory attributes	Authorization > attribute name（Cisco Secure ACS のディクショナリ属性リストに属性「CiscoSecure-Group-Id」が含まれている場合は、この属性に移行されます。それ以外の場合はデフォルト値は「CiscoSecure-Group-Id」になります）。

RSA マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name は常に RSA
Description	移行されない
Realm configuration file	Realm configuration file
Server TO	Server TO
Reauthenticate on change to PIN	Reauthenticate on change to PIN
RSA instance file	移行されない
Treat rejects as authentication fail	Treat rejects as authentication fail
Treat rejects as user not found	Treat rejects as user not found
Enable identity caching	Enable identity caching
Identity caching aging time	Identity caching aging time

RSA プロンプト マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Passcode prompt	Passcode prompt
Next Token prompt	Next Token prompt
PIN Type prompt	PIN Type prompt
Accept System PIN prompt	Accept System PIN prompt
Alphanumeric PIN prompt	Alphanumeric PIN prompt
Numeric PIN prompt	Numeric PIN prompt