Cisco Secure ACS 5.3 および Cisco ISE Release 1.2 のデータ構造マッピング

この付録では、Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 に移行される、一部が移行される、および移行されないデータ オブジェクトが含まれる機能ギャップについて説明します。

この付録では、以下の移行関連のトピックについて説明します。

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 Access Control System（ACS）から Cisco Identity Services Engine（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
- 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
- 外部 RADIUS サーバ
- ID グループ
- 内部ユーザ
- 内部エンドポイント（ホスト）
- Lightweight Directory Access Protocol（LDAP）
- Microsoft Active Directory（AD）
- RSA（一部サポート、表 A-25 を参照）
- RADIUS トークン（表 A-24 を参照）
- 証明書認証プロファイル
- 日付と時間の条件（一部サポート、「ポリシー規則の検証」（P.3-3）を参照）
- RADIUS 属性およびベンダー固有属性（VSA）の値（表 A-5 および 表 A-6 を参照）

- RADIUS ベンダー ディクショナリ（表 A-5 および 表 A-6 の注釈を参照）
- 内部ユーザ属性（表 A-1 および 表 A-2 を参照）
- 内部エンドポイント属性
- 許可プロファイル
- 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
- ネットワーク アクセスの許可ポリシー
- 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
- 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（「UTF-8 のサポート」（P.1-7）を参照）
- EAP 認証プロトコル：PEAP-TLS
- ユーザ チェック属性
- 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

移行されないデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure Access Control System（ACS）から Cisco ISE Release 1.2 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）
- Security Group Access Control List（SGACL）
- セキュリティ グループ（SG）
- サポートされている Security Group Access（SGA）デバイスの AAA サーバ
- セキュリティ グループ マッピング
- Network Device Admission Control（NDAC）ポリシー
- SGA 出力マトリクス
- ネットワーク デバイス内の SGA データ
- SGA 許可ポリシー結果のセキュリティ グループ タグ（SGT）

- 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）
- デバイスの AAA ポリシー
- Dial-In 属性のサポート
- TACACS+ プロキシ
- TACACS+ CHAP と MSCHAP 認証
- TACACS+ シェル プロファイルの属性置換
- RSA ノード欠落の秘密の表示
- 最大ユーザ セッション数
- アカウントのディセーブル化
- ユーザ パスワード タイプ
- 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
- ネットワーク デバイスの範囲

一部が移行されるデータ オブジェクト

以下のデータ オブジェクトは、Cisco Secure Access Control System（ACS）から Cisco ISE Release 1.2 に一部が移行されます。

- 日付型の ID および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。
- RADIUS ID サーバ属性（属性 CiscoSecure-Group-Id のみ移行される）。

サポート対象属性およびデータ型

表 A-1　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行されるユーザ属性

Cisco Secure ACS Release 5.3 でサポートされるユーザ属性	Cisco ISE Release 1.2 のターゲット データ型
String	String
UI32	未サポート
IPv4	未サポート
Boolean	未サポート
Date	未サポート
Enum	未サポート

表 A-2　ユーザ属性：ユーザとの関連

Cisco Secure ACS Release 5.3 のユーザに関連付けられている属性	Cisco ISE Release 1.2
String	サポート
UI32	—
IPv4	—
Boolean	—
Date	—

表 A-3　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 に移行されるホスト属性

Cisco Secure ACS Release 5.3 でサポートされるホスト属性	Cisco ISE Release 1.2 のターゲット データ型
String	String
UI32	UI32
IPv4	IPv4
Boolean	Boolean
Date	未サポート
Enum	使用可能な値の整数

表 A-4　ホスト属性：ホストとの関連

Cisco Secure ACS Release 5.3 のホストに関連付けられている属性	Cisco ISE Release 1.2
String	サポート
UI32	サポート（値は String に変換される）
IPv4	サポート（値は String に変換される）
Boolean	サポート（値は String に変換される）
Date	サポート（値は String に変換される）
Enum	サポート（値は String に変換される）

表 A-5　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へ移行される RADIUS 属性

Cisco Secure でサポートされる RADIUS 属性 ACS 5.3	Cisco ISE Release 1.2 のターゲット データ型
UI32	UI32
UI64	UI64
IPv4	IPv4
Hex String	Octect String
String	String
Enum	使用可能な値の整数

表 A-6　RADIUS 属性：RADIUS サーバとの関連

Cisco Secure ACS Release 5.3 の RADIUS サーバに関連付けられている属性	Cisco ISE Release 1.2
UI32	サポート
UI64	サポート
IPv4	サポート
Hex String	サポート（Hex string は Octet String に変換される）
String	サポート
Enum	サポート（Enum は使用可能な値の整数）

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。表には、Cisco Secure ACS Release 5.3 のオブジェクト カテゴリと、Cisco ISE Release 1.2 の相当するカテゴリが記載されています。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 ステージ中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。

- 表 A-7（ネットワーク デバイス プロパティ マッピング）
- 表 A-8（Active Directory プロパティ マッピング）
- 表 A-9（外部 RADIUS サーバ プロパティ マッピング）
- 表 A-10（ホスト/エンドポイント プロパティ マッピング）
- 表 A-11（ID ディクショナリ プロパティ マッピング）
- 表 A-12（ID グループ プロパティ マッピング）
- 表 A-13（LDAP プロパティ マッピング）
- 表 A-14（NDG タイプ マッピング）
- 表 A-15（NDG 階層マッピング）
- 表 A-16（RADIUS ディクショナリ ベンダー マッピング）
- 表 A-17（RADIUS ディクショナリ属性マッピング）
- 表 A-18（ユーザ マッピング）
- 表 A-19（証明書認証プロファイル）
- 表 A-20（許可プロファイル マッピング）
- 表 A-21（DACL マッピング）
- 表 A-22（外部 RADIUS サーバ マッピング）
- 表 A-23（ID 属性ディクショナリ マッピング）
- 表 A-24（RADIUS トークン マッピング）
- 表 A-25（RSA マッピング）
- 表 A-26（RSA プロンプト）
- 表 A-27（ID ストア順序）

- 表 A-28（デフォルトのネットワーク デバイス）

表 A-7　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのネットワーク 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
Collection of IP and subnet addresses	非サポート
TACACS information	TACACS は Cisco ISE Release 1.2 でサポート対象外のため移行されません。
RADIUS 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」）。

（注）　TACACS としてのみ設定されているネットワーク デバイスは、移行に対してサポートされず、移行されないデバイスとして記載されています。

表 A-8　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への Active Directory マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Domain name	そのまま移行
User name	そのまま移行
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
Groups	そのまま移行

（注） Cisco Secure ACS to Cisco ISE Migration Tool は、Active Directory データが移行された後で **join** コマンドを発行します。ドメイン名、ユーザ名、およびパスワードが不正な場合、この動作は失敗することがあります。また、「join」操作中の失敗を避けるには、Cisco ISE アプライアンスが Active Directory のサーバ時間と同期していることが重要です。

表 A-9　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への外部 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	そのまま移行
Description	そのまま移行
Server IP address	そのまま移行
Shared secret	そのまま移行
Authentication port	そのまま移行
Accounting port	そのまま移行
Server timeout	そのまま移行
Connection attempts	そのまま移行

表 A-10　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのホスト（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」）。
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」）。

表 A-11　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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
User	ディクショナリ プロパティはこの値（「user」）を承認します。

表 A-12　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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 にはユーザ ID グループおよびエンドポイント ID グループが含まれています。Cisco Secure ACS Release 5.3 の ID グループは Cisco ISE 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。

表 A-13　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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。（[サーバ接続（Server Connection）] タブ、図 A-1（P.A-9）を参照）。
Directory organization information	そのまま移行。（[ディレクトリ構成（Directory Organization）] タブ、図 A-2（P.A-9）を参照）
Directory groups	そのまま移行
Directory attributes	移行は（Cisco Secure ACS-Cisco ISE Migration Tool を使用して）手動で行われます。

図 A-1　[サーバ接続（Server Connection）] タブ

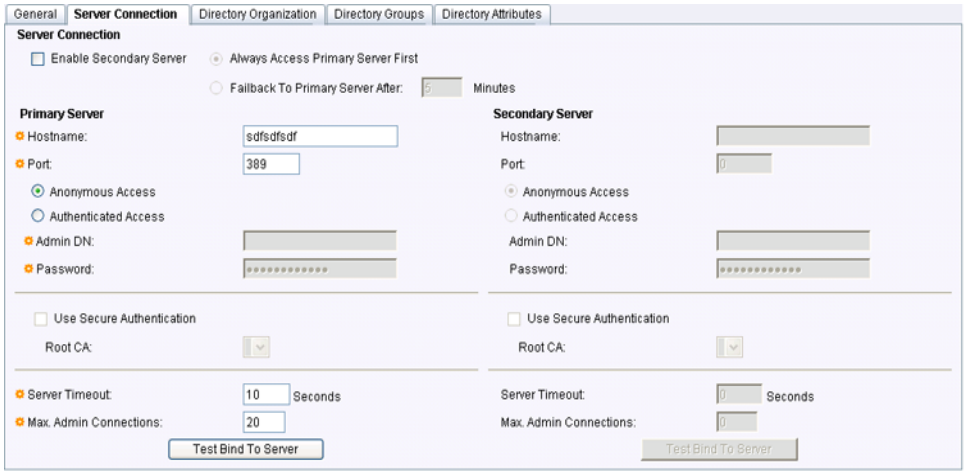

図 A-2　[ディレクトリ構成（Directory Organization）] タブ

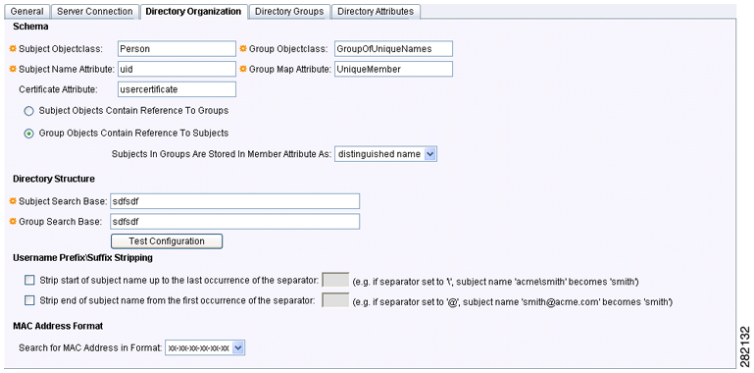

表 A-14　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への NDG タイプ マッピング

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 Release 5.3 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 は、この命名規則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。

表 A-15　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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)。

（注）　コロン（:）を持つルート名が含まれている NDG は移行されません。これは、Cisco ISE Release 1.2 で、コロンを有効な文字として認識しないためです。

表 A-16　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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）　Cisco Secure ACS Release 5.3 インストールの一部ではない、RADIUS ベンダーのみ移行する必要があります。これはユーザ定義ベンダーにのみ影響します。

表 A-17　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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	この値には特定のプロパティを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)。
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

表 A-17　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS ディクショナリ（属性）マッピング （続き）

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
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 Release 5.3 インストールの一部ではない、これらの RADIUS 属性のみ移行する必要があります（ユーザ定義属性のみ移行する必要があります）。

表 A-18　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのユーザ マッピング

Cisco Secure ACS のプロパティ	Cisco ISE のプロパティ
Name	Name
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	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）。
Change password on next login	このプロパティは移行する必要ありません。
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。

表 A-19　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への証明書認証プロファイル 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.

表 A-20　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への許可プロファイル 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、Dynamic VLAN は除き、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

表 A-21　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのダウンロード可能 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

表 A-22　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への外部 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

表 A-23　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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

表 A-23　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID 属性ディクショナリ マッピング （続き）

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

表 A-24　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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

表 A-24　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RADIUS トークン マッピング （続き）

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)。

表 A-25　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への 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

表 A-26　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への RSA プロンプト

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

表 A-27　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 への ID ストア順序

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

表 A-28　Cisco Secure ACS Release 5.3 から Cisco ISE Release 1.2 へのデフォルト ネットワーク デバイス

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
Authentication Options - TACACS+	移行されない
RADIUS - shared secret	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