CHAPTER 2

スキーマ エレメント

概要

この章では、配信パッケージ ファイルの作成に必要な命名規則、使用可能なエレメントおよびアトリビュートの値、エレメント構造とエレメントの組み合わせの詳細仕様を説明します。

この章は、次の項で構成されています。

（注） この章のエレメントの説明では、必ず完全スキーマ パスも紹介しています。通常、パスが複数存在する場合の表記方法は 2 種類あり、次の短縮形が使用されます。

パス configuration/networks/[*wifiNetwork* | *wiredNetwork*]/ の短縮形は、次の独立した 2 つのパスに展開されます。

configuration/networks/wifiNetwork/

configuration/networks/wiredNetwork/

パス configuration/networks/[*wifiNetwork* | *wiredNetwork]/authenticationNetwork/ [machineAuthentication* | *userAuthentication* | *machineUserAuthentication/machine* | *machineUserAuthentication/user*]/ の短縮形は、次の独立した 8 つのパスに展開されます。

configuration/networks/wifiNetwork/authenticationNetwork/machineAuthentication/

configuration/networks/wifiNetwork/authenticationNetwork/userAuthentication/

configuration/networks/wifiNetwork/authenticationNetwork/machineUserAuthentication/machine/

configuration/networks/wifiNetwor/authenticationNetwork/machineUserAuthentication/user/

configuration/networks/wiredNetwork/authenticationNetwork/machineAuthentication/

configuration/networks/wiredNetwork/authenticationNetwork/userAuthentication/

configuration/networks/wiredNetwork/authenticationNetwork/machineUserAuthentication/machine/

configuration/networks/wiredNetwork/authenticationNetwork/machineUserAuthentication/user/

（注）　この章では、エレメントに他のエレメントとの相関関係による制約がある場合に、要件がビジネス ルール文に記載されています。ビジネス ルールの概念は、第 1 章「エンタープライズ展開」の「スキーマの確認」を参照してください。

配信パッケージの設定

配信パッケージの作成を開始します。次のエレメントを設定します。

configuration

スキーマ パス：

configuration

基本エレメント *configuration* は、配信パッケージのコンテナを構成します。エレメント値は指定されません。

このエレメントには次の必須アトリビュートがあります。

- major_version - 値 = 4 であることが要求されます。
- minor_version - 値 = 1 であることが要求されます。
- maintenance_version - 値 = 2 であることが要求されます。
- xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" - ここでの定義のコピーです。
- xsi:noNamespaceSchemaLocation="C:¥yourPath¥distributionPackage.xsd" - 特定の .xml 配信パッケージ ファイルのインスタンス生成に使用されるスキーマへの絶対パスまたは相対パスが格納されます。この例では distributionPackage.xsd をポイントします。

  この値が重要とされるのは、市販の XML 開発ツールを使用する場合に限られます。sscConfigProcess ユーティリティは、このアトリビュート値を使用しないため、配信パッケージ .xml ファイルでは次のテキストを使用します。

  xsi:noNamespaceSchemaLocation="distributionPackage.xsd"

（注）　XML ファイルを市販ツールまたはこのマニュアルのサンプルから作成した場合、配信パッケージ .xml ファイルの 1 行目には次のテキストが格納されます。
<?xml version="1.0" encoding="UTF-8"?>

この行を組み込む必要があるかどうかは、使用する配信パッケージ ファイル作成ツールの選択によって異なります。postprocessing ユーティリティおよび SSC の場合、XML ファイルにこの文は必要ありません。

ステップ 1　「ライセンスの設定」に定義されているタスクを実行します。

ステップ 2　「ポリシーの設定」に定義されているタスクを実行します。

ステップ 3　「接続設定の実行」に定義されているタスクを実行します。

ステップ 4　「ネットワークの設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の基本エレメント *configuration* およびその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-1　基本エレメント

```
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:¥yourPath¥distributionPackage.xsd" minor_version="1"
major_version="4">
    <license>your-license</license>
    <networkPolicy>
        {child elements}
    </networkPolicy>
    <networks>
        {child elements}
    </networks>
    <connectionSettings>
        {child elements}
    </connectionSettings>
    <userControlPolicy>
        {child elements}
    </userControlPolicy>
</configuration>
```

ライセンスの設定

次のエレメントを設定します。

license

スキーマ パス：

configuration/license

オプション エレメント *license* の値では、展開されるエンドユーザ SSC のライセンスが指定されます。

license の影響を受ける項目は次のとおりです。

- 個別の認証方式
- ネットワーク アダプタ メディアのタイプ - 有線か、無線か
- スマート カードによるクレデンシャル
- Wi-Fi WPA2/802.11i（Wi-Fi WPA は、無線メディア サポートの規格です）
- Cisco Trust Agent（CTA）もインストールされている場合は CTA の処理

コンパニオン ユーザ管理ポリシー エレメントの *allowLicensing* によって、エンドユーザによる必要なライセンスの入力が可能になります。

（注） エンドユーザ SSC のライセンス許可を管理する必要がある場合は、エンドユーザ SSC の初期展開時にこのエレメントに使用する企業ライセンスを使用する必要があります。その後の配信パッケージの更新時に、このオプション エレメントを組み込む必要はありません。

例 2-2　license

```
<license>T244-YKGP-UMG5-Y2F2-5KMH-5OYX-DAR4-POND-52Z5-MHJZ-3LOD-SLYL-U5YA-IUKU-M3TC-JN
O7-3MEM-LGAA</license>
```

ポリシーの設定

配信パッケージ ファイルのすべてに、展開される SSC のポリシーの設定定義が組み込まれている必要があります。

（注）　ライセンスによって付与される権限は、すべてのポリシー設定より優先されます。たとえば、無線メディア サポートのポリシーを設定し、ライセンスが有線メディアのみを対象としている場合、展開された配信パッケージ ファイルは SSC に受け入れられますが、有線ネットワークしかサポートされません。ライセンスとポリシーの関係は、postprodessing ユーティリティでは検証されません。

ユーザ管理ポリシー

次のエレメントを設定します。

userControlPolicy

スキーマ パス：

configuration/userControlPolicy

必須エレメント *userControlPolicy* により、SSC のユーザ管理ポリシーを指定するコンテナが構成されます。エレメント値は指定されません。

次の手順で、*userControlPolicy* の次の子エレメントを設定します。子エレメントの順序は手順に表示されている順序に制限されます。

ステップ 1　ユーザ インターフェイスに関する次のポリシー エレメントを設定します。

clientUIType

スキーマ パス：

configuration/userControlPolicy/clientUIType

必須エレメント *clientUIType* の値により、ユーザ インターフェイスのタイプが指定されます。

このエレメントには次の値があります。

- preset - エンドユーザが新たなネットワークを作成できないようにするもので、管理下にあるネットワーク以外にエンド ステーションからアクセスできないようにする場合に適した選択です。Preset クライアントには、エンドユーザが取得できるステータスを事前定義されたネットワークに限定できる制限付きのユーザ インタフェースが設定されます。
- configurable - エンドユーザによる新たなネットワークの作成を許可するもので、企業ネットワークからホームや出張先のネットワークに移動するエンド ステーションに適した選択です。Configurable クライアントには、エンドユーザがステータスを取得したり、ネットワークを定義できる堅牢なユーザ インタフェースが設定されます。

ステップ 2　ライセンス方式に関する次のポリシー エレメントを設定します。

allowLicensing

スキーマ パス：

configuration/userControlPolicy/allowLicensing

必須エレメント *allowLicensing* のブール値により、エンドユーザがユーザ インターフェイスから直接、SSC のライセンスを許可できるかどうかが指定されます。

このエレメントには次の値があります。

- true - 新しいライセンスの直接インストールが可能な Activate Product Features ダイアログへのアクセスをエンドユーザに許可します。
- false - ユーザ インターフェイスによるライセンス許可はできません。ライセンスの許可を配信パッケージからのみに制御する場合は、この設定を使用します。

ステップ 3　メディア サポートに関する次のポリシー エレメントを設定します。

allowedMedia

スキーマ パス：

configuration/userControlPolicy/allowedMedia

必須エレメント *allowMedia* により、サポート対象のメディア タイプを指定するコンテナが構成されます。エレメント値は指定されません。

（注）　使用可能なメディア タイプも、優先権を持つライセンスによって制御されます。言い換えると、ライセンスで有線メディアのみが許可される場合に、配信パッケージのこのエレメントで Wi-Fi サポートを指定しても効力はありません。

ビジネス ルール：子エレメントを 1 つ以上指定する必要があります。

次の子エレメントの一方または両方を指定します。2 つの子エレメントの順序に制約はありません。

wifi

スキーマ パス：

configuration/userControlPolicy/allowedMedia/wifi

オプション エレメント *wifi* の存在によって、無線（Wi-Fi）接続のサポートが指定されます。これは値がない空白エレメントです。

wired

スキーマ パス：

configuration/userControlPolicy/allowedMedia/wired

オプション エレメント *wired* の存在によって、有線接続のサポートが指定されます。これは値がない空白エレメントです。

次の例は、配信パッケージ XML の *userControlPolicy* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-3　userControlPolicy

```
<userControlPolicy>
    <clientUIType>configurable</clientUIType>
    <allowLicensing>false</allowLicensing>
    <allowedMedia>
        <wired/>
        <wifi/>
    </allowedMedia>
</userControlPolicy>
```

ネットワーク ポリシー

次のエレメントを設定します。

networkPolicy

スキーマ パス：

configuration/networkPolicy

必須エレメント *networkPolicy* により、使用可能なネットワークの設定方法、およびエンドユーザのアクセスが可能な設定を指定するコンテナが構成されます。エレメント値は指定されません。

次の手順で、*networkPolicy* の次の子エレメントを設定します。子エレメントの順序は手順に表示されている順序に制限されます。

ステップ 1　アソシエーション モードに関する次のポリシー エレメントを設定します。

allowedAssociationModes

スキーマ パス：

configuration/networkPolicy/allowedAssociationModes

必須エレメント *allowedAssociationModes* により、すべての、または使用する無線ネットワーク設定で使用が許可される無線アソシエーション モードを指定するコンテナが構成されます。エレメント値は指定されません。

このポリシーの指定は、配信パッケージ ファイルのほかの場所に管理者が作成したネットワーク、および展開された SSC のユーザ インターフェイスからエンドユーザが作成したネットワークに適用されます。

ビジネス ルール：無線ネットワークも設定する場合（エレメント *wifiNetwork*）は、子エレメントを 1 つ以上指定する必要があります。

次の無線アソシエーション モードを 1 つ以上指定します。

子エレメントの順序に制約はありません。

有線のみの環境の場合は、エレメント *open* のみが必要です。

- 暗号なしの Wi-Fi オープン アソシエーションまたは有線オープン アソシエーション - エレメント *open* を使用します。
- Wi-Fi WPA Personal - エレメント *wpa-Personal* を使用します。
- Wi-Fi WPA Enterprise - エレメント *wpa-Enterprise* を使用します。
- Wi-Fi WPA2 Personal - エレメント *wpa2-Personal* を使用します。
- Wi-Fi WPA2 Enterprise - エレメント *wpa2-Enterprise* を使用します。

- 静的 WEP 暗号化の従来の無線オープン アソシエーション（*staticWep*）または WEP 共有キー使用の共有アソシエーション（*shared*）または、802.1X WEP 暗号化のオープン アソシエーション（*dynamicWep*）- エレメント *wep* を使用します。

open

wpa-Personal

wpa-Enterprise

wpa2-Personal

wpa2-Enterprise

wep

スキーマ パス：

configuration/networkPolicy/allowedAssociationModes/open
configuration/networkPolicy/allowedAssociationModes/wpa-Personal
configuration/networkPolicy/allowedAssociationModes/wpa-Enterprise
configuration/networkPolicy/allowedAssociationModes/wpa2-Personal
configuration/networkPolicy/allowedAssociationModes/wap2-Enterprise
configuration/networkPolicy/allowedAssociationModes/wep

これらのエレメントのいずれかが存在することによって、アソシエーション モードのサポートが指定されます。これらのエレメントはすべて、値がない空白エレメントです。

ステップ 2　認証方式に関する次のポリシー エレメントを設定します。

allowedEapMethods

スキーマ パス：

configuration/networkPolicy/allowedEapMethods

必須エレメント *allowedEapMethods* により、ネットワーク設定のいずれかで一次（または外部トンネル）認証プロトコルに対する使用を許可する EAP 方式を指定するコンテナが構成されます（トンネルされる EAP 方式の内部トンネルでの使用が許可される一連の EAP 方式は、このポリシーによる影響を受けません）。エレメント値は指定されません。

このポリシーの指定は、配信パッケージ ファイルのほかの場所に管理者が作成したネットワーク、および展開された SSC のユーザ インターフェイスからエンドユーザが作成したネットワークに適用されます。

（注）　使用可能な EAP 方式は、優先権を持つライセンスによる制御も受けます。言い換えると、ライセンスで EAP-FAST が許可されない場合は、配信パッケージのこのエレメントで FAST サポートを指定しても効力はありません。

ビジネス ルール：認証ネットワークも設定する場合（エレメント *authenticationNetwork*）は、子エレメントを 1 つ以上指定する必要があります。

次の認証方式を 1 つ以上指定します。

子エレメントの順序に制約はありません。

- EAP-MD5 - エレメント *eapMd5* を使用します。

- EAP-MSCHAPv2D5 - エレメント *eapMschapv2* を使用します。
- EAP-GTC - エレメント *eapGtc* を使用します。
- EAP-FAST - エレメント *eapFast* を使用します。
- EAP-PEAP - エレメント *eapPeap* を使用します。
- EAP-TTLS - エレメント *eapTtls* を使用します。
- EAP-TLS - エレメント *eapTls* を使用します。
- LEAP - エレメント *leap* を使用します。

eapMd5

eapMschapv2

eapGtc

eapFast

eapPeap

eapTtls

eapTls

leap

スキーマ パス：

configuration/networkPolicy/allowedEapMethods/eapMd5
configuration/networkPolicy/allowedEapMethods/eapMschapv2
configuration/networkPolicy/allowedEapMethods/eapGtc
configuration/networkPolicy/allowedEapMethods/eapFast
configuration/networkPolicy/allowedEapMethods/eapPeap
configuration/networkPolicy/allowedEapMethods/eapTtls
configuration/networkPolicy/allowedEapMethods/eapTls
configuration/networkPolicy/allowedEapMethods/leap

これらのエレメントのいずれかが存在することによって、認証方式のサポートが指定されます。これらのエレメントはすべて、値がない空白エレメントです。

ステップ 3　信頼できるサーバに関する次のポリシー エレメントを設定します。

serverValidationPolicy

スキーマ パス：

configuration/networkPolicy/serverValidationPolicy

必須エレメント *serverValidationPolicy* により、認証ネットワークで要求される関連付けられた認証サーバの確認の処理方法を指定するコンテナが構成されます。エレメント値は指定されません。

次のポリシーのいずれか 1 つを指定します。

- 全ネットワークにサーバ確認を強制 - エレメント *alwaysValidate* を使用します。
- ネットワークごとにサーバ確認を設定 - エレメント *allowUserValidationControl* を使用します。

選択したポリシーは、配信パッケージ ファイルのほかの場所に管理者が作成したネットワーク、および展開された SSC のユーザ インターフェイスからエンドユーザが作成したネットワークに適用されます。

allowUserValidationControl

スキーマ パス：

configuration/networkPolicy/serverValidationPolicy/allowUserValidationControl

allowUserValidationControl エレメントの存在によって、サーバの確認の個別設定が可能になります。サーバの確認が実行されるかどうかは、各ネットワーク内で EAP 方式別に設定されます。これは値がない空白エレメントです。

alwaysValidate

スキーマ パス：

configuration/networkPolicy/serverValidationPolicy/alwaysValidate

alwaysValidate エレメントの存在によって、相互認証方式を使用するすべての認証ネットワークで、認証処理の一環として必ずサーバの確認が実行されることが指定されます。これは、IT 管理者が配信パッケージで作成したネットワーク、およびエンドユーザがユーザ インターフェイスから作成したネットワークに適用されます。

ビジネス ルール：すべてのネットワークの *validateServerIdentity* エレメントの値が true に設定されている必要があります。

次の子エレメントを設定して、エンドユーザによる信頼できるサーバ ルール作成のポリシーを処理します。

allowUserTrustedServers

スキーマ パス：

configuration/networkPolicy/serverValidationPolicy/alwaysValidate/allowUserTrustedServers

必須エレメント *allowUserTrustedServers* のブール値によって、エンドユーザ各自がローカルで作成したプライベート ネットワークでの、信頼できるサーバの定義を許可するかどうかが指定されます（IT 管理者によって定義され、エンドユーザに展開される信頼できるサーバについては、エンドユーザによる編集ができず、このポリシー エレメントの影響も受けません）。

このエレメントには次の値があります。

- true - エンドユーザが信頼できるサーバ ルールを作成できます。
- false - エンドユーザは信頼できるサーバ ルールを作成できません。これに応じて展開されるユーザ インターフェイスも変更されます。

ステップ 4　複数の接続操作に関する次のポリシー エレメントを設定します。

allowUserSimultaneousConnectionsControl

スキーマ パス：

configuration/networkPolicy/allowUserSimultaneousConnectionsControl

必須エレメント *allowUserSimultaneousConnectionsControl* のブール値によって、SSC の複数のネットワーク アダプタの処理方法を指定する設定の変更制御をエンドユーザに許可するかどうかが指定されます（展開モードは、コンパニオン接続設定エレメント *simultaneousConnections* によって設定されます）。

このエレメントには次の値があります。

- true - エンドユーザが接続の実行方法を変更できます。
- false - エンドユーザは接続の実行方法を変更できません。これに応じて展開されるユーザ インターフェイスも変更されます。

ビジネス ルール：展開される接続設定エレメント *simultaneousConnections* が singleHomed に設定されている場合、セキュリティの保護程度の低いモードへの変更がエンドユーザに許可されず、このオプションを使用できません。

ステップ 5　クレデンシャル保存に関する次のポリシー エレメントを設定します。

allowedCredentialStorage

スキーマ パス：

configuration/networkPolicy/allowedCredentialStorage

必須エレメント *allowedCredentialStorage* により、ユーザに要求して直接取得したクレデンシャルを保存する期間を指定するコンテナが構成されます。エレメント値は指定されません。

ビジネス ルール：要求によるクレデンシャル収集方式を使用する認証ネットワークも設定する場合（エレメント *prompt/credentialsStorage*）は、子エレメントを 1 つ以上指定する必要があります。

ユーザに要求したクレデンシャルの保存期間として、次の中から 1 つ以上を指定します。

子エレメントが複数ある場合、その順序は表示されている順序に制限されます。

- 永久、つまり変更されるまで - エレメント *forever* を使用します。
- 現在のログイン セッションの継続中 - エレメント *logonSession* を使用します。
- 指定期間 - エレメント *duration* を使用します。

このポリシーの指定は、配信パッケージ ファイルのほかの場所に管理者が作成したネットワーク、および展開された SSC のユーザ インターフェイスからエンドユーザが作成したネットワークに適用されます。

forever

スキーマ パス：

configuration/networkPolicy/allowedCredentialStorage/forever

このオプション エレメントの存在によって、ユーザのクレデンシャルの永続的な保存のサポートが指定されます。クレデンシャル認証の失敗の場合、または認証サーバからパスワード変更要求が出力された場合、ユーザには現在保存されている値に置き換わる新しいクレデンシャルの入力が求められます。初回の要求および保存の完了後、このオプションは静的クレデンシャルのように機能します。これは値がない空白エレメントです。

logonSession

スキーマ パス：

configuration/networkPolicy/allowedCredentialStorage/logonSession

このオプション エレメントの存在によって、現行ログイン セッションの期間に限定されたユーザのクレデンシャルの保存のサポートが指定されます。ユーザがログアウトすると、クレデンシャルが削除されます。これは値がない空白エレメントです。

duration

スキーマ パス：

configuration/networkPolicy/allowedCredentialStorage/duration

このオプション エレメントの存在によって、指定期間に限定されたユーザのクレデンシャルの保存のサポートが指定されます。指定期間の満了後はクレデンシャルが削除されます。ただし、接続は保持され、直ちに再要求されることはありません。タイムアウト後に出力されるその後の再認証要

求によって、ユーザのクレデンシャルを再入力するように要求されます。このエレメントの値では、この保存タイプを使用するように定義されたすべてのネットワークに適用されるグローバル タイムアウト期間（分単位）が指定されます。

制約：指定時間は 1 ～ 3600 の範囲にする必要があります（1 分～約 2 日半）

ステップ 6　複数の接続操作に関する次のポリシー エレメントを設定します。

allowUserWpaHandshakeValidationControl

スキーマ パス：

configuration/networkPolicy/allowUserWpaHandshakeValidationControl

必須エレメント *allowUserWpaHandshakeValidationControl* のブール値によって、SSC の WPA ハンドシェイクの検証の処理方法を指定する設定の変更制御をエンドユーザに許可するかどうかが指定されます（展開モードは、コンパニオン接続設定エレメント *validateWpaHandshake* によって設定されます）。

このエレメントには次の値があります。

- true - エンドユーザが WPA プロトコルの処理方法を変更できます。
- false - エンドユーザは WPA プロトコルの処理方法を変更できません。これに応じて展開されるユーザ インターフェイスも変更されます。
  ユーザは使用している機能やネットワーク アダプタに関する知識が十分でない場合もあるため、シスコではこの設定を推奨しています。詳細は、接続設定エレメント *validateWpaHandshake* を参照してください。

有線専用の環境の場合は、このエレメントが使用されず、いずれの値も設定できます。

ステップ 7　ネットワーク接続の範囲に関する次のポリシー エレメントを設定します。

allowPublicProfileCreation

スキーマ パス：

configuration/networkPolicy/allowPublicProfileCreation

必須エレメント *allowPublicProfileCreation* のブール値により、エンドユーザが SSC のユーザ インターフェイスから作成したネットワークの接続範囲が指定されます。

このエレメントには次の値があります。

- true - エンドユーザは次の実行が可能なパブリック ネットワークを定義できます。
  - 全ユーザで共有されるネットワークの作成
  - マシン接続コンテキストのネットワークの作成
- false - エンドユーザに許可されるのは各自のプライベート ネットワークの作成に限定されます。これに応じて展開されるユーザ インターフェイスも変更されます。

（注）　管理者が配信ネットワークで定義するネットワークはすべてパブリックです。

ステップ 8　クライアント証明書に関する次のポリシー エレメントを設定します。

allowedClientCertificates

スキーマ パス：

configuration/networkPolicy/allowedClientCertificates

必須エレメント *allowedClientCertificates* により、Extended Key Usage フィールドに基づくクライアント証明書のフィルタリングを実行するかどうかを指定するコンテナが構成されます。エレメント値は指定されません。

次のポリシーのいずれか 1 つを指定します。

- フィルタリング不要：エレメント *noEkuFilter* を使用します。
- フィルタリング必須：エレメント *certificateEkuFilterExpression* を使用します。

選択したポリシーは、配信パッケージ ファイルのほかの場所に管理者が作成したネットワーク、および展開された SSC のユーザ インターフェイスからエンドユーザが作成したネットワークに適用されます。

noEkuFilter

スキーマ パス：

configuration/networkPolicy/allowedClientCertificates/noEkuFilter

noEkuFilter エレメントの存在によって、クライアント証明書の Extended Key Usage フィールドに基づく使用制限がないことが指定されます。これは値がない空白エレメントです。

certificateEkuFilterExpression

スキーマ パス：

configuration/networkPolicy/allowedClientCertificates/certificateEkuFilterExpression

certificateEkuFilterExpression エレメントの存在によって、クライアント証明書は拡張キー使用法（EKU）が許可されている場合にのみ使用されることが指定されます。このエレメントの値には、EKU 仕様が格納されています。値は、次の EKU キーワードのいずれかの（カッコで囲まれた）ブール（and, or, not）式です。

- ServerAuth
- ClientAuth
- CodeSign
- SecureEmail
- IpsecEndSystem
- IpsecTunnel
- IpsecUser
- TimeStamp
- SmartCardLogon

（注）　次に、配信パッケージに使用される上記の EKU キーワードと実際の証明書の EKU 文字列の関係を示します。
ServerAuth：サービス認証
ClientAuth：クライアント認証
CodeSign：コード署名
SecureEmail：セキュリティ保護された電子メール
IpsecEndSystem：IP セキュリティ エンドシステム
IpsecTunnel：IP セキュリティ トンネル終端
IpsecUser：IP セキュリティ ユーザ
TimeStamp：タイム スタンプ
SmartCardLogon：スマート カード ログオン

例 2-4　allowedClientCertificates

```
<allowedClientCertificates>
    <certificateEkuFilterExpression>ClientAuth or
SmartCardLogon</certificateEkuFilterExpression>
</allowedClientCertificates>

<allowedClientCertificates>
    <certificateEkuFilterExpression>(not ServerAuth and
ClientAuth)</certificateEkuFilterExpression>
</allowedClientCertificates>
```

次の例は、配信パッケージ XML の *networkPolicy* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-5　networkPolicy

```
<networkPolicy>
    <allowedAssociationModes>
        <!--open network-->
        <open/>
        <!--shared key network-->
        <staticWep/>
        <shared/>
        <wpa-Personal/>
        <wpa2-Personal/>
        <!--authenticating network-->
        <dynamicWep/>
        <wpa-Enterprise/>
        <wpa2-Enterprise/>
    </allowedAssociationModes>
    <allowedEapMethods>
        <!--wired only-->
        <eapMd5/>
        <eapMschapv2/>
        <eapGtc/>
        <!--wired or wireless-->
        <eapFast/>
        <eapPeap/>
        <eapTls/>
        <eapTtls/>
        <leap/>
    </allowedEapMethods>
    <serverValidationPolicy>
        <alwaysValidate>
            <allowUserTrustedServers>true</allowUserTrustedServers>
        </alwaysValidate>
    </serverValidationPolicy>
    <allowUserSimultaneousConnectionsControl>false</allowUserSimultaneousConnectionsCo
ntrol>
    <allowedCredentialStorage>
        <forever/>
        <logonSession/>
        <duration>5</duration>
    </allowedCredentialStorage>
    <allowUserWpaHandshakeValidationControl>false</allowUserWpaHandshakeValidationCont
rol>
    <allowPublicProfileCreation>false</allowPublicProfileCreation>
    <allowedClientCertificates>
        <noEkuFilter/>
    </allowedClientCertificates>
</networkPolicy>
```

接続設定の実行

次のエレメントを設定します。

connectionSettings

スキーマ パス：

configuration/connectionSettings

必須エレメント *connectionSettings* により、ネットワーク接続のすべてのグローバルな動作面に関する展開の設定を実行するコンテナが構成されます。エレメント値は指定されません。

次の手順で、*connectionSettings* エレメントの次の子エレメントを設定します。子エレメントの順序は手順に表示されている順序に制限されます。

ステップ 1　次の接続設定エレメントを設定します。

simultaneousConnections

スキーマ パス：

configuration/connectionSettings/simultaneousConnections

必須エレメント *simultaneousConnections* の値は、すべてのネットワークの接続の多重性を指定します。

このエレメントには次の値があります。

- singleHomed - 同時に可能な接続が 1 つに制限されます（マルチホーム設定が抑止されます）。
- multiHomed - 複数の同時接続が許可されます（マルチホーム ネットワーク接続が許可されます）。選択したネットワークでは、実装および管理されているすべての有線および無線ネットワーク アダプタの接続を SSC が試行します。

エンドユーザが展開された（初期）設定を上書きできるかどうかは、コンパニオン ネットワーク ポリシー エレメント *allowUserSimultaneousConnectionsControl* によって制御されます。

ビジネス ルール : singleHomed が設定されている場合、ペアになる一方のネットワーク ポリシー エレメント *allowUserSimultaneousConnectionsControl* を false に設定する必要があります。エンドユーザは管理者による操作の制限モードの選択を上書きできません。

ステップ 2　次の接続設定エレメントを設定します。

validateWpaHandshake

スキーマ パス：

configuration/connectionSettings/validateWpaHandshake

必須エレメント *validateWpaHandshake* のブール値によって、SSC による WPA ハンドシェイクの検証の処理方法が指定されます。WPA の高度なキー管理に必要なドライバ機能は、古い組み込み型のネットワーク アダプタでは使用できない場合もあります。旧型のアダプタを広く基盤とする環境に対応するため、SSC には WPA/WPA2 のセキュリティ バイパス機能があり、4 方向ハンドシェイクでは RSN プローブ応答 / ビーコン IE 確認の必要はありません。

このエレメントには次の値があります。

- true - WPA/WPA2 ハンドシェイクの検証を有効にします（推奨）。
  この設定は、エンドステーションのすべてに規格の要件に従った WPA/WPA2 ドライバに完全に準拠した無線アダプタがある場合に使用します。

- false - WPA/WPA2 ハンドシェイクの検証を無効にします。
  この設定は、無線アダプタのドライバが不完全であることが認識されている特殊な場合にのみ使用します。

有線専用の環境の場合は、このエレメントが使用されず、いずれの値も設定できます。

エンドユーザが展開された（初期）設定を上書きできるかどうかは、コンパニオン ネットワーク ポリシー エレメント *allowUserWpaHandshakeValidationControl* によって制御されます。

次の例は、配信パッケージ XML の *connectionSettings* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-6　connectionSettings

```
<connectionSettings>
    <simultaneousConnections>singleHomed</simultaneousConnections>
    <validateWpaHandshake>false</validateWpaHandshake>
</connectionSettings>
```

ネットワークの設定

ヒント　ネットワークの設定は、配信パッケージ定義の中心部分で、最も複雑な部分でもあります。これに対応するため、付録 A「ネットワーク決定ツリー フロー チャート」には、ネットワーク接続の設定の XML スキーマ決定ツリーの概要があり、この項の図解的な索引として使用できます。

次のエレメントを設定します。

networks

スキーマ パス：

configuration/networks

エレメント *networks* により、事前定義された企業ネットワークのコンテナが構成されます。エレメント値は指定されません。子およびそのコンテンツのそれぞれが個別のネットワークの設定を表します。

これはオプション エレメントです。省略すると、展開されたエンドユーザ クライアントに管理者定義のネットワークがないことになります。この場合は、エンドユーザだけがネットワーク定義を作成することになります。

（注）　クライアントは一方的な選択を行うことができません。ネットワークの設定は主として認証サーバおよびそれに関連付けられたアクセス デバイスのポリシーによって決定されます。この全体的な環境に従って、クライアントを適切に設定する必要があります。

ネットワークの定義で最初に必要な選択は、接続のメディア タイプに従ってネットワーク タイプを選択することです。

次の項目：「ネットワーク メディア タイプの選択」

ネットワーク メディア タイプの選択

次のネットワーク メディア タイプのいずれか 1 つを指定します。

- 802.3 有線（イーサネット）- エレメント *wiredNetwork* を使用します。
- 802.11 無線（Wi-Fi）- エレメント *wifiNetwork* を使用します。

wiredNetwork

スキーマ パス：

configuration/networks/wiredNetwork

オプション エレメント *wiredNetwork* により、イーサネット（802.3）ネットワークを設定するコンテナが構成されます。エレメント値は指定されません。

ビジネス ルール：*wiredNetwork* エレメントは 1 つのみ使用することができます。すべての有線（イーサネット）アダプタを適用できる有線ネットワークが 1 つに限られます。

ビジネス ルール：これは、ポリシーで有線メディア タイプがサポートされる場合にのみ有効な選択です。「ユーザ管理ポリシー」の項のエレメント wired を参照してください。

次の項目：「有線ネットワークの設定」

wifiNetwork

スキーマ パス：

configuration/networks/wifiNetwork

オプション エレメント *wifiNetwork* は、個別の Wi-Fi（802.11）ネットワークを設定するコンテナを構成します。エレメント値は指定されません。複数の wifiNetwork エレメントを定義できます。

ビジネス ルール：これは、ポリシーで無線メディア タイプがサポートされる場合にのみ有効な選択です。「ユーザ管理ポリシー」の項のエレメント wifi を参照してください。

次の項目：「Wi-Fi ネットワーク基本エレメント」

次の例は、配信パッケージ XML の *networks* エレメントとその子エレメントを示しています。2 つの使用可能な子エレメントの順序に制約はありません。

例 2-7　networks

```
<networks>
    <wiredNetwork>
        {child elements}
    </wiredNetwork>
    <wifiNetwork>
        {child elements}
    </wifiNetwork>
    <wifiNetwork>
        {child elements}
    </wifiNetwork>
</networks>
```

Wi-Fi ネットワークの設定

次の項のタスクを実行して、Wi-Fi ネットワークを設定します。

1. 「Wi-Fi ネットワーク基本エレメント」
2. 「Wi-Fi ネットワークのセキュリティ クラスの選択」

有線ネットワークの設定

次の項のタスクを実行して、有線ネットワークを設定します。

1. 「有線ネットワーク基本エレメント」
2. 「有線ネットワークのセキュリティ クラスの選択」

Wi-Fi ネットワーク基本エレメント

次のエレメントを設定します。

displayName

スキーマ パス：

configuration/networks/wifiNetwork/displayName

必須エレメント *displayName* の値により、SSC の各種ダイアログで表示専用として使用されるユーザフレンドリな名前が指定されます。

ssid

スキーマ パス：

configuration/networks/wifiNetwork/ssid

必須エレメント *ssid* の値には、アクセスポイントの設定名、つまり Service Set Identifier（SSID; サービスセット ID）が格納されます。SSID は、同一圏内の複数の無線ネットワークの区別に使用される一意の ID です。

（注）　この値は、アクセス ポイントの設定によって定義されます。

制約：SSID は 32 文字の ASCII 文字に限定されます。

ビジネス ルール : SSID は一意です。複数の *ssid* エレメントに同じ値を使用することはできません。

associationRetries

スキーマ パス：

configuration/networks/wifiNetwork/associationRetries

必須エレメント *associationRetries* の値によって、接続の際に SSC がアクセス ポイントとのアソシエーションを試行する回数が指定されます。無線送信には可変性があるため、一般に認証セッションではアソシエーションを数回再試行してから、これを放棄して送信における偶発的な脱落ビットに過敏になることを回避しようとします。

さらに、*associationRetries* がネットワーク別に設定されている場合でも、1 つのグローバル設定のみが全ネットワークに適用されます。展開後、SSC では設定されているすべてのネットワークの入力から、最大値を抽出してグローバル値として使用します。

配信パッケージ ファイルに無線ネットワークが含まれない場合、ライセンスとポリシーによって許可される場合にエンドユーザによって作成される無線ネットワークには、デフォルト値の 3 が使用されます。

制約：再試行回数は 99 に制限されます。

デフォルト：推奨値は、3 です。

beaconing

スキーマ パス：

configuration/networks/wifiNetwork/beaconing

必須エレメント *beaconing* のブール値によって、アクセス ポイントが名前をアドバタイズすることによって、SSC がアクセス ポイントの物理的な存在の判定に使用する基準が設定されるかどうかが指定されます。

このエレメントには次の値があります。

- True - アクティブ プローブにビーコンまたは応答が出力され、標準の無線スキャンによって検出されます。
- False - 標準スキャンで検出されるようには設定されないため、存在を検出するにはアクティブな検索処理が必要です。非ビーコン アクセス ポイントは、非表示アクセス ポイントと呼ばれます。

次の例は、配信パッケージ XML の *wifiNetwork* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-8　partial wifiNetwork

```
<wifiNetwork>
    <displayName>My Corporate Wi-Fi Network</displayName>
    <ssid>MyCorpNet</ssid>
    <associationRetries>3</associationRetries>
    <beaconing>true</beaconing>
    <!--{your choice of network security class goes here}-->
</wifiNetwork>
```

Wi-Fi ネットワークのセキュリティ クラスの選択

ネットワークに次のセキュリティ クラスのいずれか 1 つを指定します。

- オープン ネットワーク - エレメント *openNetworkUserConnection* を使用します。SSID を事前に指定する必要があるため、エンドユーザにオープン ネットワークを展開することはほとんどありません。エンドユーザは、許可がある場合に限り、特定のオープン ネットワークに接続するネットワーク プロファイルを作成できます。
- 共有キー ネットワーク - エレメント *sharedKeyNetwork* を使用します。一般に共有キー ネットワークは、ネットワーク管理者が共有秘密情報を管理するホーム ネットワーク アクセス デバイスを、モバイル エンドユーザが保有している場合にのみ展開されます。エンドユーザは、許可がある場合に限り、各自のホーム アクセス ポイントに接続するネットワーク プロファイルを作成できます。
- 認証ネットワーク - エレメント *authenticationNetwork* を使用します。これは、使用する認証サーバとポリシー、および使用するクレデンシャル環境との整合性がある企業ネットワークを事前設定する必要がある場合に最適な選択です。

openNetworkUserConnection

スキーマ パス：

configuration/networks/wifiNetwork/openNetworkUserConnection

オプション エレメント *openNetworkUserConnection* により、オープン無線ネットワークを設定するコンテナが構成されます。SSC のオープン ネットワークは、いかなる形態のデータの暗号化も使用しないため、最低レベルのネットワーク セキュリティ保護クラスになります。エレメント値は指定されません。

ビジネス ルール：これは、ポリシーで *open* アソシエーション モードがサポートされる場合にのみ有効な選択です。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

次の項目：「オープン Wi-Fi ネットワークの設定」

sharedKeyNetwork

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork

オプション エレメント *sharedKeyNetwork* により、クライアントとアクセス ポイントの両方で事前定義された静的キーを使用する無線ネットワークを設定するコンテナが構成されます。このキーは最終的にはデータの暗号化に使用されます。このネットワーク クラスは、主にホーム / スモール オフィス環境で機能します。エレメント値は指定されません。

次の項目：「共有キー Wi-Fi ネットワークの設定」

authenticationNetwork

スキーマ パス：

configuration/networks/wifiNetwork/authenticationNetwork

オプション エレメント *authenticationNetwork* により、802.1X 無線ネットワークを設定するコンテナが構成されます。認証 /802.1X ネットワークには、無線のセキュリティに対してクライアントとサーバの相互認証、およびネットワークによる暗号化キーの提供という 2 つの重要な特徴が追加されます。このネットワーク クラスは、最高のセキュリティ レベルの選択肢です。エレメント値は指定されません。

次の項目：「認証 Wi-Fi ネットワークの設定」

次の例は、配信パッケージ XML の *wifiNetwork* エレメントとその子エレメントの 3 つのセキュリティ クラスを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-9　wifiNetwork

```
<wifiNetwork>
    <displayName>My Corporate Wi-Fi Network</displayName>
    <ssid>MyCorpNet</ssid>
    <associationRetries>3</associationRetries>
    <beaconing>true</beaconing>
    <openNetworkUserConnection>
        {child elements}
    </openNetworkUserConnection>
</wifiNetwork>

<wifiNetwork>
    <displayName>My Corporate Wi-Fi Network</displayName>
    <ssid>MyCorpNet</ssid>
    <associationRetries>3</associationRetries>
    <beaconing>true</beaconing>
    <sharedKeyNetwork>
        {child elements}
    </sharedKeyNetwork>
</wifiNetwork>

<wifiNetwork>
    <displayName>My Corporate Wi-Fi Network</displayName>
    <ssid>MyCorpNet</ssid>
    <associationRetries>3</associationRetries>
    <beaconing>true</beaconing>
    <authenticationNetwork>
        {child elements}
    </authenticationNetwork>
</wifiNetwork>
```

オープン Wi-Fi ネットワークの設定

次のエレメントを設定します。

autoConnect

スキーマ パス：

configuration/networks/wifiNetwork/openNetworkUserConnection/autoConnect

必須ブール エレメント *autoConnect* により、ユーザ コンテキスト接続処理のネットワーク選択アルゴリズムにこのネットワークを含めるかどうかが指定されます。言い換えると、このエレメントによって、ユーザのシステムへのログイン時に自動接続が行われるかどうかが決定されます。ユーザ コンテキスト接続のみが有効化され、処理されます。

このエレメントには次の値があります。

- True - 自動接続が有効化されています。

- False - 自動接続が無効になっています。接続は常に手動で開始されます。

次の例は、配信パッケージ XML の *openNetworkUserConnection* エレメントとその子エレメントを示しています。

例 2-10　openNetworkUserConnection

```
<openNetworkUserConnection>
    <autoConnect>true</autoConnect>
</openNetworkUserConnection>
```

共有キー Wi-Fi ネットワークの設定

共有キー ネットワークに次の接続コンテキストのいずれか 1 つを指定します。

- マシン専用接続 - エレメント *machineConnection* を使用します。
- ユーザ専用接続 - エレメント *userConnection* を使用します。

machineConnection

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection

オプション エレメント *machineConnection* により、マシン コンテキスト接続のみをサポートするネットワークの設定コンテナが構成されます。接続は、システムのブート時に設定されたマシン クレデンシャルを使用して実行され、ユーザがシステムにログインまたはログオフする際に保持されています。エレメント値は指定されません。

次の項目：「共有キー、マシン ネットワークの設定」

userConnection

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection

オプション エレメント *userConnection* により、ユーザ コンテキスト接続のみをサポートするネットワークの設定コンテナが構成されます。接続は、ユーザがシステムにログオンする際に設定されたユーザ クレデンシャルを使用して実行され、ユーザがシステムからログオフするまで保持されます。エレメント値は指定されません。

次の項目：「共有キー、ユーザ ネットワークの設定」

次の例は、配信パッケージ XML の *sharedKeyNetwork* エレメントとその子エレメントを示しています。

例 2-11　sharedKeyNetwork

```
<sharedKeyNetwork>
    <machineConnection>
        {child elements}
    </machineConnection>
</sharedKeyNetwork>

<sharedKeyNetwork>
    <userConnection>
        {child elements}
    </userConnection>
</sharedKeyNetwork>
```

共有キー、マシン ネットワークの設定

次のエレメントを設定します。

keySettings

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings

必須エレメント *keySettings* により、共有キー プロトコルのタイプを指定するコンテナが構成されます。エレメント値は指定されません。

次の項目：「共有キーのタイプの選択」

次の例は、配信パッケージ XML における共有キー ネットワークの *machineConnection* エレメントとその子エレメントを示しています。

例 2-12　machineConnection

```
<machineConnection>
    <keySettings>
        {child elements}
    </keySettings>
</machineConnection>
```

共有キー、ユーザ ネットワークの設定

次のエレメントを設定します。

autoConnect

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/autoConnect

必須ブール エレメント *autoConnect* により、ユーザ コンテキスト接続処理のネットワーク選択アルゴリズムにこのネットワークを含めるかどうかが指定されます。言い換えると、このエレメントによって、ユーザのシステムへのログイン時に自動接続が行われるかどうかが決定されます。

このエレメントには次の値があります。

- True - 自動接続が有効化されています。
- False - 自動接続が無効になっています。接続は常に手動で開始されます。

keySettings

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings

必須エレメント *keySettings* により、共有キー プロトコルのタイプを指定するコンテナが構成されます。エレメント値は指定されません。

次の項目：「共有キーのタイプの選択」

次の例は、配信パッケージ XML における共有キー ネットワークの *userConnection* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-13　userConnection

```
<userConnection>
    <keySettings>
        {child elements}
    </keySettings>
    <autoConnect>true</autoConnect>
</userConnection>
```

共有キーのタイプの選択

ネットワークに次のキー タイプのいずれか 1 つを指定します。

- WEP - エレメント wep を使用します。
- WPA - エレメント wpa を使用します。
- WPA2 - エレメント wpa2 を使用します。

wep

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep

オプション エレメント *wep* により、Wired Equivalent Privacy（WEP）の共有キーまたは静的キーを設定するコンテナが構成されます。このエレメントの存在によって、WEP キー タイプが指定されます。エレメント値は指定されません。

これらは、旧来のセキュリティ ソリューションで、クライアントとネットワーク アクセス デバイス間のデータ プライバシー保護のメカニズムは低レベルで基礎的なものに限られ脆弱です。これらの旧来の方式は、下位互換性のためにサポートされますが、企業レベルのセキュリティ ソリューションの重要要素ではありません。

ビジネス ルール：これは、ポリシーで *wep* アソシエーション モードがサポートされる場合にのみ有効な選択です。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

次の項目：「WEP 共有キーの設定」

wpa

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wpa

オプション エレメント *wpa* により、WPA-Personal モードを設定するコンテナが構成されます。このエレメントの存在によって、WPA キー タイプが指定されます。エレメント値は指定されません。

Wi-Fi Protected Access（WPA）は、Wi-Fi Alliance のセキュリティ ソリューションで、従来の 802.11 暗号化方式である WEP に改良を加えたものです。WPA-Personal では、パスフレーズ preshared key（PSK）が使用されます。

ビジネス ルール：これは、ポリシーで *wpa-Personal* アソシエーション モードがサポートされる場合にのみ有効な選択です。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

次の項目：「WPA/WPA2 共有キーの設定」

wpa2

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa2

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wpa2

オプション エレメント *wpa2* により、WPA2-Personal モードを設定するコンテナが構成されます。このエレメントの存在によって、WPA2 キー タイプが指定されます。エレメント値は指定されません。

WPA2 は、正規の 802.11i 規格に準拠した最近のアップグレードです。WPA2 は、802.11i 相互運用性に対する Wi-Fi Alliance の格付けです。WPA2 は WPA の欠陥に対処するためにリリースされたのではありません。WPA2 で重要とされていることは、新しく強力な暗号（AES）を義務付けていることです。また、WPA2 ではアソシエーション要求 / 応答メッセージ、およびキー交換メッセージに複雑な改善が導入されています。WPA2-Personal では、パスフレーズ preshared key（PSK）が使用されます。

ビジネス ルール：これは、ポリシーで *wpa2-Personal* アソシエーション モードがサポートされる場合にのみ有効な選択です。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

次の項目：「WPA/WPA2 共有キーの設定」

WEP 共有キーの設定

次の手順で Wi-Fi、WEP 共有キー ネットワークを設定します。

ステップ 1　次のエレメントを設定します。

ieee80211Authentication

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/ieee80211Authentication

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/ieee80211Authentication

必須エレメント *ieee80211Authentication* により、SSC とアクセス ポイント間で使用されるアソシエーションのタイプを設定するコンテナが構成されます。エレメント値は指定されません。

次の項目：「WEP アソシエーションの選択」

ステップ 2　項「WEP キー形式の選択」に定義されているタスクを実行します。

次の例は、配信パッケージ XML における WEP の *keySetting* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-14　WEP keySettings

```
<keySettings>
    <wep>
        <wepAscii40 encrypt="true">aaaaa</wepAscii40>
        <ieee80211Authentication>
            <shared/>
        </ieee80211Authentication>
    </wep>
</keySettings>
```

WEP アソシエーションの選択

次の WEP アソシエーション モードのいずれか 1 つを指定します。

- オープン - エレメント *open* を使用します。
- 共有 - エレメント *shared* を使用します。

open

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/ieee80211Authentication/open

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/ieee80211Authentication/open

オプション エレメント *open* の存在によって、802.11 オープン アソシエーション モードが指定されます。SSC の場合、オープン アソシエーションが使用される共有キー ネットワークは従来の「静的 WEP」ネットワークです。これは値がない空白エレメントです。

このエレメントには必須のブール アトリビュート *encrypt* があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

shared

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/ieee80211Authentication/shared

オプション エレメント *shared* の存在によって、802.11 共有アソシエーション モードが指定されます。SSC の場合、共有アソシエーションが使用される共有キー ネットワークは、従来の「共有 WEP」ネットワークです。これは値がない空白エレメントです。

次の例は、配信パッケージ XML の *ieee80211Authentication* エレメントの 2 種類の選択を示しています。

例 2-15

```
<ieee80211Authentication>
    <shared/>
</ieee80211Authentication>

<ieee80211Authentication>
    <open/>
</ieee80211Authentication>
```

WEP キー形式の選択

ネットワークに対して、次のキー形式および長さのいずれか 1 つを指定します。

- 40 ビット キーの ASCII - エレメント *wepAscii40* を使用します。
- 128 ビット キーの ASCII - エレメント *wepAscii128* を使用します。
- 40 ビット キーの Hex - エレメント *wepHex40* を使用します。
- 128 ビット キーの Hex - エレメント *wepHex128* を使用します。

wepAscii40

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/wepAscii40

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wep/wepAscii40

オプション エレメント *wepAscii40* により、ASCII 形式とキーの長さ 40 ビットが指定されます。

このエレメントには必須のブール アトリビュート *encrypt* があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 5 文字の印刷可能 ASCII 文字であることが要求されます。

wepAscii128

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/wepAscii128

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wep/wepAscii128

オプション エレメント *wepAscii128* により、ASCII 形式とキーの長さ 128 ビットが指定されます。

このエレメントには必須のブール アトリビュート *encrypt* があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 13 文字の印刷可能 ASCII 文字であることが要求されます。

wepHex40

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/wepHex40

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wep/wepHex40

オプション エレメント *wepHex40* により、Hex 形式とキーの長さ 40 ビットが指定されます。

このエレメントには必須のブール アトリビュート *encrypt* があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 10 文字の Hex 文字であることが要求されます。

wepHex128

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wep/wepHex128

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wep/wepHex128

オプション エレメント *wepHex128* により、Hex 形式とキーの長さ 128 ビットが指定されます。

このエレメントには必須のブール アトリビュート *encrypt* があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 26 文字の Hex 文字であることが要求されます。

次の例は、配信パッケージ XML の *wep* 子エレメントの 4 種類の選択を示しています。

例 2-16　wep の選択肢

```
<wepAscii40 encrypt="true">aaaaa</wepAscii40>

<wepAscii128 encrypt="true">aaaaaaaaaaaaa</wepAscii128>

<wepHex40 encrypt="true">AAAAAAAAAA</wepHex40>

<wepHex128 encrypt="true">ABCDEFABCDEFABCDEFABCDEFAB</wepHex128>
```

WPA/WPA2 共有キーの設定

次の手順で Wi-Fi、WPA/WPA2 共有キー ネットワークを設定します。

ステップ 1　次のエレメントを設定します。

encryption

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa/encryption

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa/encryption

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa2/encryption

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa2/encryption

必須エレメント **encryption** により、データ暗号化方式が指定されます。

このエレメントには次の値があります。

- TKIP - WPA アソシエーションの標準方式です。下位互換性のため WPA2 アソシエーションでもサポートされます。
- AES - 通常は WPA2 アソシエーションにリンクされますが、WPA 準拠のアクセス デバイスの一部でも使用できます。現在、Wi-Fi で標準化されている最高レベルのデータ セキュリティ モードです。

ステップ 2　次のエレメントを設定します。

key

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa/key

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa/key

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa2/key

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa2/key

必須エレメント **key** により、WPA または WPA2 キーの形式を設定するコンテナが構成されます。エレメント値は指定されません。

次の項目：「WPA/WPA2 のキー形式の選択」.

次の例は、配信パッケージ XML における WPA/WPA2 の *keySetting* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-17　WPA keySettings

```
<keySettings>
    <wpa>
        <key>
            <ascii encrypt="true">mySecret</ascii>
        </key>
        <encryption>TKIP</encryption>
    </wpa>
</keySettings>

<keySettings>
    <wpa2>
        <key>
            <ascii encrypt="true">mySecret</ascii>
        </key>
        <encryption>TKIP</encryption>
    </wpa2>
</keySettings>
```

WPA/WPA2 のキー形式の選択

ネットワークに次のキー形式のいずれか 1 つを指定します。

- ASCII - エレメントを使用します。
- Hex - エレメントを使用します。

ascii

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa/key/ascii

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa/key/ascii

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa2/key/ascii

configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa2/key/ascii

オプション エレメント **ascii** により、ASCII 形式が指定されます。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 8 ～ 63 文字の印刷可能 ASCII 文字であることが要求されます。

hex

スキーマ パス：

configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa/key/hex
configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa/key/hex
configuration/networks/wifiNetwork/sharedKeyNetwork/machineConnection/keySettings/wpa2/key/hex
configuration/networks/wifiNetwork/sharedKeyNetwork/userConnection/keySettings/wep/wpa2/key/hex

オプション エレメント **hex** によって Hex 形式が指定されます。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：この値は 64 文字の Hex 文字であることが要求されます。

次の例は、配信パッケージ XML の *key* エレメントとその子エレメントの 2 種類の選択を示しています。

例 2-18　key

```
<key>
    <ascii encrypt="true">mySecret</ascii>
</key>

<key>
    <hex
encrypt="true">1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF</hex>
</key>
```

認証 Wi-Fi ネットワークの設定

次の手順で認証 Wi-Fi ネットワークを設定します。

ステップ 1　「認証アソシエーション モードの設定」に定義されているタスクを実行します。

ステップ 2　「認証ネットワーク基本エレメントの設定」に定義されているタスクを実行します。

ステップ 3　「認証ネットワークの接続コンテキストの選択」に定義されているタスクを実行します。

ステップ 4　「Wi-Fi EAP 方式の選択」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の Wi-Fi の *authenticationNetwork* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-19　authenticationNetwork の部分

```
<authenticationNetwork>
    <!--{your choice of network connection context goes here}-->
    <serverValidation>
        {child elements}
    </serverValidation>
    <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
    <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
    <associationMode>
        {child element}
    </associationMode>
</authenticationNetwork>
```

認証アソシエーション モードの設定

次のエレメントを設定します。

associationMode

スキーマ パス：

configuration/networks/wifiNetwork/authenticationNetwork/associationMode

必須エレメント *associationMode* により、SSC とアクセス ポイント間で使用されるアソシエーションのタイプを設定するコンテナが構成されます。エレメント値は指定されません。

次の項目：「アソシエーション モードの選択」

アソシエーション モードの選択

ネットワークに次のアソシエーション モードのいずれか 1 つを指定します。

- 動的 WEP - エレメント dynamicWep を使用します。
- WPA-Enterprise - エレメント wpa-Enterprise を使用します。
- WPA2-Enterprise - エレメント wpa2-Enterprise を使用します。

ビジネス ルール：使用可能なアソシエーション モードはポリシーでサポートされているものに限られます。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

dynamicWep

スキーマ パス：

configuration/networks/wifiNetwork/authenticationNetwork/associationMode/dynamicWep

オプション エレメント *dynamicWep* により、802.11 オープン アソシエーション モードが Wired Equivalent Privacy（WEP）動的キーが装備されたネットワークと組み合わせて使用されることが指定されます。このエレメントの存在によって、動的 WEP が指定されます。これは値がない空白エレメントです。

この旧来のセキュリティ ソリューションでは、クライアントとネットワーク アクセス デバイス間の基本的なデータ プライバシーが提供されます。この旧来の方式は、下位互換性のためにサポートされますが、企業レベルのセキュリティ ソリューションの重要要素ではありません。

wpa-Enterprise

スキーマ パス：

configuration/networks/wifiNetwork/authenticationNetwork/associationMode/wpa-Enterprise

オプション エレメント *wpa-Enterprise* により、Wi-Fi WPA-Enterprise アソシエーション モードが指定されます。このエレメントの存在によって、WPA-Enterprise が指定されます。

Wi-Fi Protected Access（WPA）は、Wi-Fi Alliance のセキュリティ ソリューションで、従来の 802.11/802.1X の動的 WEP に改良を加えたものです。WPA-Enterprise では、キー交換の前に認証が義務付けられ、802.1X 認証を使用してキー交換の暗号化シードが提供されます。

このエレメントには次の値があります。

- TKIP - WPA アソシエーションの標準方式です。下位互換性のため WPA2 アソシエーションでもサポートされます。
- AES - 通常は WPA2 アソシエーションにリンクされますが、WPA 準拠のアクセス デバイスの一部でも使用できます。現在、Wi-Fi で標準化されている最高レベルのデータ セキュリティ モードです。

wpa2-Enterprise

スキーマ パス：

configuration/networks/wifiNetwork/authenticationNetwork/associationMode/wpa2-Enterprise

オプション エレメント *wpa2-Enterprise* により、Wi-Fi WPA2-Enterprise アソシエーション モードが指定されます。このエレメントの存在によって、WPA2-Enterprise が指定されます。

WPA2 は、正規の 802.11i 規格に準拠した最近のアップグレードです。WPA2 は、802.11i 相互運用性に対する Wi-Fi Alliance の格付けです。WPA2 は WPA の欠陥に対処するためにリリースされたのではありません。WPA2 で重要とされていることは、新しく強力な暗号（AES）を義務付けていることです。また、WPA2 ではアソシエーション要求 / 応答メッセージ、およびキー交換メッセージに複雑な改善が導入されています。

このエレメントには次の値があります。

- TKIP - WPA アソシエーションの標準方式です。下位互換性のため WPA2 アソシエーションでもサポートされます。
- AES - 通常は WPA2 アソシエーションにリンクされますが、WPA 準拠のアクセス デバイスの一部でも使用できます。現在、Wi-Fi で標準化されている最高レベルのデータ セキュリティ モードです。

次の例は、配信パッケージ XML の *associationMode* エレメントとその子エレメントの 3 種類の選択を示しています。

例 2-20　associationMode

```
<associationMode>
    <dynamicWep/>
</associationMode>

<associationMode>
    <wpa-Enterprise>TKIP</wpa-Enterprise>
</associationMode>

<associationMode>
    <wpa2-Enterprise>AES</wpa2-Enterprise>
</associationMode>
```

認証ネットワーク基本エレメントの設定

次の手順で、認証ネットワークの基本エレメントを設定します。

ステップ 1　次の認証再試行エレメントを設定します。

ネットワーク アクセス デバイスの一部には、ポートを開いてユーザを特殊な VLAN に切り替える機能など、認証の失敗を処理する特別な機能があります。これらのネットワーク アクセス デバイスに対応するため、SSC には管理者が設定できるパラメータがあります。これらのパラメータを使用することで、切断にいたるまでの接続試行回数を調整して、複数回の認証の失敗に基づくアクセス デバイスによる高度な決定を実現できるようにします。

（注）　接続パフォーマンスへの影響の理解、企業ネットワークのアクセス デバイス固有のニーズおよび機能に関する知識がない限り、デフォルト設定の変更は推奨されません。エンドユーザの一般的な使用に供する展開の前に、変更のすべてを総合的にテストする必要があります。

interactiveAuthenticationRetries

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/interactiveAuthenticationRetries

必須エレメント *interactiveAuthenticiationRetries* の値によって、認証セッションの失敗の後の SSC の再試行回数が指定されます。対話式はユーザの介入によって障害が修正される場合に使用されます。これは一般に、ユーザのテキスト入力が必要な接続の試行、またはユーザの修正が可能な Enter Your Credentials のダイアログに関連付けられたリスト選択に適用されます。

無線ネットワークの場合、*interactiveAuthenticiationRetries* がネットワーク別に設定されている場合でも、1 つのグローバル設定のみがすべてのネットワークに適用されます。展開後、SSC では設定されているすべてのネットワークの入力から、最大値を抽出してグローバル値として使用します。

有線ネットワークの場合、SSC が使用する値は単一の有線ネットワークで設定された値に基づいており、設定されている無線ネットワークとは関係ありません。

配信パッケージ ファイルに特定のメディア タイプのネットワークが含まれない場合、ライセンスとポリシーによって許可される場合にエンドユーザによって作成されるその特定ネットワーク タイプのネットワークには、システム デフォルト値の 4 が割り当てられます。

制約：再試行回数は 99 に制限されます。

デフォルト：シスコでは、この値に 4 を推奨しています。この値はシスコ スイッチの Failed Authentication VLAN 機能をサポートします。サプリカントは、使用スイッチの再試行回数の設定より 1 つ多く設定します。これにより、制限付き VLAN に対する SSC の試行回数が 1 回多くなります。対話式再試行カウントが増加すると、ユーザ ダイアログ プロンプトの発生も多くなります。

nonInteractiveAuthenticationRetries

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/nonInteractiveAuthenticationRetries

必須エレメント *nonInteractiveAuthenticiationRetries* の値により、認証セッションの失敗の後の SSC の再試行回数が指定されます。非対話式はユーザの介入が障害の修正に有益でない場合に使用されます。これは一般に、シングルサインオン、PSK の不一致、その他のサーバ証明書の確認に関連するすべての失敗など、Enter Your Credentials ダイアログが関連しない接続の試行に適用されます。

無線ネットワークの場合、*nonInteractiveAuthenticiationRetries* がネットワーク別に設定されている場合でも、1 つのグローバル設定のみがすべてのネットワークに適用されます。展開後、SSC では設定されているすべてのネットワークの入力から、最大値を抽出してグローバル値として使用します。

有線ネットワークの場合、SSC が使用する値は単一の有線ネットワークで設定された値に基づいており、設定されている無線ネットワークとは関係ありません。

配信パッケージ ファイルに特定のメディア タイプのネットワークが含まれない場合、ライセンスとポリシーによって許可される場合にエンドユーザによって作成されるその特定ネットワーク タイプのネットワークには、システム デフォルト値の 4 が割り当てられます。

制約：再試行回数は 99 に制限されます。

デフォルト：シスコでは、この値に 4 を推奨しています。この値はシスコ スイッチの Failed Authentication VLAN 機能をサポートします。サプリカントは、使用スイッチの再試行回数の設定より 1 つ多く設定します。これにより、制限付き VLAN に対する SSC の試行回数が 1 回多くなります。非対話式試行カウントが増加すると、マシンの起動や、ネットワーク接続失敗時のシステムに対するユーザのログイン接続の時間が長期化します。

ステップ 2　次のサーバ確認エレメントを設定します。

serverValidation

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation

オプション エレメント *serverValidation* により、認証時に使用されるサーバの確認を設定するコンテナが構成されます。エレメント値は指定されません。

- このエレメントは、サーバ証明書の確認が必要な場合に追加します。
- サーバ証明書の確認が不要な場合は、このエレメントを省略してください。

ビジネス ルール：オプションの子エレメント、*validationRules*、または *trustedServerIds* を 1 つ以上指定する必要があります。

次の項目：「サーバの確認の設定」

サーバの確認の設定

ステップ 1　次のように、信頼できるサーバの一覧を設定します。

a. サーバの証明書を使用し、その確認が必要な場合は、項「証明書で信頼できるサーバ ルールの設定」に定義されているタスクを実行します。

b. 匿名（認証なし）、自律的な PAC プロビジョニング、または手動の PAC プロビジョニングで EAP-FAST を使用する場合は、項「PAC で信頼できるサーバ ルールの設定」に定義されているタスクを実行します。

展開されたすべての信頼できるサーバ ルールのタイプは、SSC のユーザ インターフェイスに表示されるように Machine/All Users（パブリック プロファイル）です。展開された規則はロックされ、変更はできません。

さらに、*serverValidation* がネットワーク別に設定されている場合でも、展開されたすべての信頼できるサーバ ルールがすべてのネットワークに適用されます（言い換えると、Release 4.1 での使用も、以前の Release 4.0.x シリーズと同じです）。

ステップ 2　次の手順で、信頼できる認証局（CA）の証明書の展開方法を設定します。

次の必要な CA 証明書の展開方法のいずれか 1 つを指定します。

- 別個に展開 - エレメント *trustAnyRootCaFromOs* を使用します。
- 配信パッケージの一部として展開 - エレメント *trustedRootCaCerts* を使用します。

trustAnyRootCaFromOs

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustAnyRootCaFromOs

オプション エレメント *trustAnyRootCaFromOs* の存在により、サーバ証明書の信頼に使用されるすべての信頼できるルート CA および中間 CA の証明書が個別の展開処理によって適切な Windows 証明書ストアに格納されることが指定されます。これは値がない空白エレメントです。

これは、Release 4.1.0 より前の SSC の CA 証明書の展開に対応します。

trustedRootCaCerts

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedRootCaCerts

オプション エレメント *trustedRootCaCerts* の存在により、サーバ証明書の信頼に使用されるすべての信頼できるルート CA および中間 CA の証明書の直接展開に使用されるコンテナが指定されます。エレメント値は指定されません。

このオプションを使用した場合は、展開後に SSC によって Windows の信頼できる機関（信頼できるルート CA）証明書ストアに証明書が自動的に格納されます。ただし、これらの展開された証明書は記憶され、接続の認証時に Windows のストアのコンテンツのフィルタに使用されます。

trustedRootCaCerts がネットワーク別に設定されている場合でも、すべての展開された CA 証明書がすべてのネットワークに適用されます。たとえば、CA1 をネットワーク 1 に、CA2 をネットワーク 2 に展開した場合、ネットワーク 1 を認証するときに CA1 と CA2 の両方によってネットワーク 1 のサーバ証明書が確認されるという要領になります。

次の項目：「CA 証明書の追加」

（注）　自己署名証明書
サーバ証明書は自己署名できます（証明書チェーン長 0 が設定されます）。適切なストアの信頼できるルート エンティティのリストに掲載されていれば、この証明書が SSC で信頼されます。

次の例は、配信パッケージ XML の *serverValidation* エレメントとその子エレメントの 2 種類の証明書ソース オプションを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-21　serverValidation

```
<serverValidation>
    <validationRules>
        {child element}
    </validationRules>
    <trustedServerIds>
        {child element}
    </trustedServerIds>
    <trustedRootCaCerts>
        {child element}
    </trustedRootCaCerts>
</serverValidation>

<serverValidation>
    <validationRules>
        {child element}
    </validationRules>
    <trustedServerIds>
        {child element}
    </trustedServerIds>
    <trustAnyRootCaFromOs/>
</serverValidation>
```

証明書で信頼できるサーバ ルールの設定

サーバの証明書を使用し、その確認が必要な場合は、次のエレメントを設定します。

この使用には、認証あり、自律的 PAC プロビジョニングの EAP-FAST が含まれます。この場合、サーバ証明書の確認によって、自動的に作成された PAC 規則への信頼が送信されます。言い換えると、エレメント *trustedServerId* を改めて指定する必要がなくなります。

validationRules

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/validationRules

エレメント *validationRules* により、証明書確認規則を指定するコンテナが構成されます。証明書では複数のオプション アトリビュートのセットを使用できるため、確認規則で特定の証明書アトリビュートを指定することができます。次の規則タイプを 1 つ以上指定します。

- 証明書フィールド Subject Alternative Name を基準にする規則 - エレメント *matchSubjectAlternativeName* を使用します。
- 証明書フィールド Subject を基準にする規則 - エレメント *matchSubjectName* を使用します。

ビジネス ルール：子エレメントを 1 つ以上指定する必要があります。

matchSubjectAlternativeName

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/validationRules/matchSubjectAlternativeName

このオプション エレメントが存在すると、次の証明書フィールドの検索を指定することになります。

- Subject Alternative Name：DNSName

  これは一般に Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）の形式で、最上位レベル（ルート）ドメイン名までのすべての上位レベルのドメイン名を含むドメイン名です（例：engr.mycompany.com）。

matchSubjectAlternativeName エレメントは、必要な数だけ追加できます。

このエレメント値にはサーバの証明書のコンテンツとの比較チェックで使用されるテキスト文字列が格納されます。

必要なアトリビュートの値

- **name** - このアトリビュートの値によって規則の表示名が指定されます。
- **match** - このアトリビュートの値によって、設定されたテキストを比較テストで使用する方法が指定されます。
  - 完全一致 - 証明書フィールドにエレメント *matchSubjectAlternativeName* と完全に一致する値が格納されている必要があります。
  - 後方一致 - 証明書フィールドがエレメント *matchSubjectAlternativeName* の値で終わっている必要があります。

    一般にこの値は FQDN の定量化に使用され、たとえば *matchSubjectAlternativeName* に「mycompany.com」が含まれる場合、Subject Alternative Name が engr.mycompany.com または mkrt.mycompany.com などの場合に信頼できるとみなされます。

matchSubjectName

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/validationRules/matchSubjectName

このオプション エレメントの存在によって、次の証明書フィールドの検索が指定されます。

- Subject：CN（通常名）

  これは一般に単純な ASCII 文字列です。複数の通常名が指定されている場合は、証明書に記載されているものがすべて検索されます。
- Subject : DN（ドメイン名）- DC（ドメイン コンポーネント）アトリビュート セットの複合。たとえば DC=Mycompany、DC=com、の DC セットの場合は、Mycompany.com というドメイン名になります。

  したがって一般にこのフィールドは完全修飾ドメイン名（FQDN）を表し、最上位レベル（ルート）ドメイン名までのすべての上位レベルのドメイン名を含むドメイン名です（例：engr.mycompany.com）。

matchSubjectName エレメントは、必要な数だけ追加できます。

このエレメント値にはサーバの証明書のコンテンツとの比較チェックで使用されるテキスト文字列が格納されます。

必要なアトリビュートの値

- **name** - このアトリビュートの値によって規則の表示名が指定されます。
- **match** - このアトリビュートの値によって、設定されたテキストを比較テストで使用する方法が指定されます。
  - 完全一致 - 証明書フィールドにエレメント *matchSubjectName* と完全に一致する値が格納されている必要があります。
  - 後方一致 - 証明書フィールドがエレメント *matchSubjectName* の値で終わっている必要があります。

一般にこの値は FQDN の定量化に使用され、たとえば *matchSubjectName* に「mycompany.com」が含まれる場合、Subject が engr.mycompany.com または mkrt.mycompany.com などの場合に信頼できるとみなされます。

次の例は、配信パッケージ XML の *validationRules* エレメントとその子エレメントを示しています。子エレメントの順序や数に制約はありません。

例 2-22　validationRules

```
<validationRules>
    <matchSubjectAlternativeName name="Cert Rule 1"
match="endsWith">myCorp.com</matchSubjectAlternativeName>
    <matchSubjectName name="Cert Rule 2" match="exactly">My
Corporation</matchSubjectName>
    <matchSubjectAlternativeName name="Cert Rule 3"
match="endsWith">myCorp2.net</matchSubjectAlternativeName>
</validationRules>
```

PAC で信頼できるサーバ ルールの設定

匿名（認証なし）、自律的 PAC プロビジョニングの EAP-FAST を使用している場合は、次のエレメントを設定します。

（注） 認証ありの自律的 PAC プロビジョニングの EAP-FAST を使用している場合は、SSC でサーバ証明書（*validationRules*）から PAC に信頼が転送されるため、このエレメントは必要ありません。

trustedServerIds

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds

必須エレメント *trustedServerIds* により、FAST PAC 確認規則を指定するコンテナが構成されます。エレメント値は指定されません。

次の子エレメントを設定します。

trustedServerId

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId

必須エレメント *trustedServerId* は、個別の FAST PAC 確認規則のコンテナを構成します。エレメント値は指定されません。

trustedServerId エレメントは、必要な数だけ追加できます。

必要なアトリビュートの値

- **name** - このアトリビュートの値によってユーザ インターフェイスでの規則の表示名が指定されます。

PAC 規則情報に次のソースのいずれか 1 つを指定します。

- postprocess ユーティリティによってデータを入力 - エレメント *reference* を使用します（推奨）。

- 各自でデータを入力 - エレメント *aid* および *aidInfo* を使用します。

reference

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId/reference

エレメント *reference* により、PAC ファイル ID のコンテナが構成されます。エレメント値は指定されません。

子エレメントを設定します。

aidReference

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId/reference/aidReference

エレメント *aidReference* の値により、PAC の完全パスが指定されます。このファイルは postprocess sscPackageProcess ユーティリティからのアクセスが可能である必要があります。XML 配信パッケージ ファイルの postrocess ツールは、PAC ファイルを取得して規則情報を自動的に抽出し、*aidReference* エレメントを *aid* および *aidInfo* エレメントに置換します。オプションの *secretKey* エレメントはすべて、処理対象の配信パッケージ ファイルから削除されます。

ヒント　参照される PAC ファイルは、サーバ A-ID が適切であれば Cisco ACS でエクスポートされた任意の FAST PAC ファイルで十分に機能します。PAC ファイル自体は、配信パッケージに組み込まれていません。

secretKey

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId/reference/secretKey

オプション エレメント *secretKey* は、*aidReference* で識別された PAC がキーで読み取り保護されている場合に指定されますこのエレメントの値には、キー値が格納され、この値は postprocess ツールから必要な情報へのアクセスに使用されます。

aid

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId/aid

エレメント *aid* の値により、PAC の権限アイデンティティ（A-ID）が指定されます。

制約：HEX 形式

aidInfo

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedServerIds/trustedServerId/aidInfo

エレメント *aidInfo* の値により、PAC の A-ID のフレンドリ名が指定されます。

制約：ASCII 形式

次の例は、配信パッケージ XML の *trustedServerId* エレメントとその子エレメントを示しています。複数の子エレメントの順序は表示されている順序に制限されます。

例 2-23　trustedServerId

```
<trustedServerIds>
    <trustedServerId name="PAC AID Rule 1">
        <reference>
            <aIdReference>E:¥path¥pacFile1</aIdReference>
            <secretKey>1234</secretKey>
        </reference>
    </trustedServerId>
    <trustedServerId name="PAC AID Rule 2">
        <reference>
            <aIdReference>E:¥path¥pacFile2</aIdReference>
        </reference>
    </trustedServerId>
</trustedServerIds>

<trustedServerIds>
    <trustedServerId name="PAC AID Rule 1">
        <aid>9eb4674987654a4796f62abc6e403060</aid>
        <aidInfo>Corp ACS</aidInfo>
    </trustedServerId>
</trustedServerIds>
```

CA 証明書の追加

次のエレメントを設定します。

certificate

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedRootCaCerts/certificate

必須エレメント *certificate* により、CA 証明書のコンテンツを格納するコンテナが構成されます。展開後に SSC によって Windows の信頼できる機関（信頼できるルート CA）証明書ストアに証明書が自動的に格納されます。エレメント値は指定されません。

certificate エレメントは、必要な数だけ追加できます。

次のエレメントを指定し、設定します。

caReference

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/serverValidation/trustedRootCaCerts/certificate/caReference

エレメント *caReference* の値により、CA 証明書への完全パスが指定されます。このファイルは postprocess sscPackageProcess ユーティリティからのアクセスが可能である必要があります。XML 配信パッケージ ファイルの postprocess ツールは、証明書ファイルを取得して情報を自動的に符号化し（base64 文字列）、*content* エレメントを読み込み、*content* エレメントで *caReference* エレメントを置換します。

サポートされている証明書ファイルの形式は .pem です。*content* エレメントの *format* アトリビュートが値 pem で追加され、設定されます。

次の例は、配信パッケージ XML の *certificate* エレメントとその子エレメントを示しています。

例 2-24　certificate

```
<certificate>
    <caReference>E:¥path¥CaCertFile.pem</caReference>
</certificate>
```

認証ネットワークの接続コンテキストの選択

ネットワークに次の接続コンテキストのいずれか 1 つを指定します。

- マシン専用接続 - エレメント *machineAuthentication* を使用します。
- ユーザ専用接続 - エレメント *userAuthentication* を使用します。
- マシン / ユーザ接続 - エレメント *machineUserAuthentication* を使用します。

machineAuthentication

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication

オプション エレメント *machineAuthentication* により、マシン コンテキスト接続のみをサポートするネットワークの設定コンテナが構成されます。接続は、システムのブート時に設定されたマシン クレデンシャルを使用して実行され、ユーザがシステムにログインまたはログオフする際に保持されています。『Cisco Secure Services Client User Guide』では、拡張マシン専用コンテキスト接続と呼ばれています。エレメント値は指定されません。

次の項目：「認証が行われるマシン専用のネットワークの設定」

userAuthentication

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication

オプション エレメント *userAuthentication* により、ユーザ コンテキスト接続のみをサポートするネットワークの設定コンテナが構成されます。接続は、ユーザがシステムにログオンする際に設定されたユーザ クレデンシャルを使用して実行され、ユーザがシステムからログオフするまで保持されます。『Cisco Secure Services Client User Guide』では、ユーザ専用コンテキスト接続と呼ばれています。エレメント値は指定されません。

次の項目：「認証が行われるユーザ専用のネットワークの設定」

machineUserAuthentication

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication

オプション エレメント *machineUserAuthentication* により、マシン コンテキスト接続とユーザ コンテキスト接続の両方をサポートするネットワークの設定コンテナが構成されます。接続は、システム起動時に設定されたマシン クレデンシャルを使用して実行され、ユーザがシステムにログオンする際に設定されたユーザ クレデンシャルによって再認証が正常完了した場合に保持されます。ユー

ザがシステムからログオフすると、マシン接続が復旧されます。『Cisco Secure Services Client User Guide』では、マシンおよびユーザ コンテキスト接続と呼ばれています。エレメント値は指定されません。

次の項目：「認証が行われるマシンとユーザのネットワークの設定」

次の例は、配信パッケージ XML の *authenticationNetwork* エレメントとその子エレメントの 3 種類の接続コンテキストを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-25　authenticationNetwork

```
<authenticationNetwork>
    <machineAuthentication>
        {child elements}
    </machineAuthentication>
    <serverValidation>
        {child elements}
    </serverValidation>
    <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
    <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
    <associationMode>
        {child element}
    </associationMode>
</authenticationNetwork>

<authenticationNetwork>
    <userAuthentication>
        {child elements}
    </userAuthentication>
    <serverValidation>
        {child elements}
    </serverValidation>
    <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
    <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
    <associationMode>
        {child element}
    </associationMode>
</authenticationNetwork>

<authenticationNetwork>
    <machineUserAuthentication>
        {child elements}
    </machineUserAuthentication>
    <serverValidation>
        {child elements}
    </serverValidation>
    <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
    <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
    <associationMode>
        {child element}
    </associationMode>
</authenticationNetwork>
```

認証が行われるマシン専用のネットワークの設定

次の手順で認証が行われるマシン専用 Wi-Fi ネットワークを設定します。

ステップ 1　「認証が行われるマシン クレデンシャル ソース エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「認証の接続非依存基本エレメントの設定」に定義されているタスクを実行します。

ステップ 3　「静的クレデンシャル認証のエレメントの設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *machineAuthentication* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-26　machineAuthentication

```
<machineAuthentication>
    <collectionMethod>
        {child elements}
    </collectionMethod>
    <useAnonymousId>true</useAnonymousId>
    <staticIdentity encrypt="true">machineName</staticIdentity>
    <staticPassword encrypt="true">machineSecret</staticPassword>
    <eapMethods>
        {child elements}
    </eapMethods>
</machineAuthentication>
```

認証が行われるマシン クレデンシャル ソース エレメントの設定

次のエレメントを設定します。

collectionMethod

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication/collectionMethod

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/machine/collectionMethod

必須エレメント *collectionMethod* により、マシン クレデンシャルのソースとタイプを設定するコンテナが構成されます。これは値がない空白エレメントです。

マシン接続に次のクレデンシャル タイプのいずれか 1 つを指定します。

- Active Directory - エレメント *auto* を使用します。
- 事前定義 - エレメント *static* を使用します。

auto

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication/collectionMethod/auto

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/machine/collectionMethod/auto

オプション エレメント *auto* の存在により、Microsoft Active Directory（AD）が提供するマシン クレデンシャルの使用が指定されます。サポートされるタイプは次のとおりです。

- マシン証明書 - TLS ベース EAP 方式で使用する必要があります。

  通常、ここには単一の証明書のみが格納されます。ただし、複数の証明書が存在する場合、最初に検出された有効な証明書が使用されます（たとえば、古い証明書に置き換えられる新しい証明書のプロビジョニング時の一時的な重複や、異なる複数の認証局によるプロビジョニングの場合）。

この証明書によって PIN を要求したり、強力なプライベート キー保護を設定することはできません。

（注）　マシンのアイデンティティはマシン証明書（Subject Alternative Name の dnsName フィールド）によって提供されます。

- マシン パスワード - EAP-MSCHAPv2 などの、パスワードを基準にした EAP 方式で使用する必要があります。

（注）　コンピュータが含まれるドメイン コントローラがマシン認証を実行している必要があります。コンピュータのポリシーで、コンピュータのマシン証明書またはパスワードを自動的に登録する必要があります。

これは値がない空白エレメントです。

static

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication/collectionMethod/static

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/machine/collectionMethod/static

オプション エレメント *static* の存在により、配信パッケージの一部として（設定ファイル）展開された事前定義のクレデンシャルの使用が指定されます。これは値がない空白エレメントです。

ビジネス ルール：このオプションを使用する場合は、「静的クレデンシャル認証のエレメントの設定」で取り上げられているエレメントを追加し、設定する必要があります。

ビジネス ルール：マシン認証の場合、クライアント証明書および EAP FAST PAC の使用を除いて、静的クレデンシャルではパスワードをベースにした EAP 方式のみが要求されます。このため、EAP TLS、EAP FAST、EAP PEAP、または EAP TLS の内部方式による FAST の方式は使用できません。

次の例は、配信パッケージ XML の *collectionMethod* エレメントとその子エレメントの 2 種類の選択を示しています。

例 2-27　collectionMethod（マシン）

```
<collectionMethod>
    <auto/>
</collectionMethod>

<collectionMethod>
    <static/>
</collectionMethod>
```

認証の接続非依存基本エレメントの設定

次のエレメントを設定します。

useAnonymousId

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
[machineAuthentication | userAuthentication | machineUserAuthentication/machine |
machineUserAuthentication/user]/useAnonymousId

必須ブール エレメント *useAnonymousId* により、トンネル EAP 方式のフェーズ 1、外部（非保護）トンネルで使用される EAP Response/Identity メッセージのコンテンツが指定されます。

このエレメントには次の値があります。

- False - このオプションの場合 SSC は以下のように動作します。
  - すべての EAP 方式を許可
  - すべての EAP 応答で UserName を送信

  このモードを使用した場合、クライアントによって Identity 応答で UserName@Domain が送信されます。ただし、ドメインのルーティング（@Domain）はオプションです。ユーザ アイデンティティ（UserName）は暗号化されずに送信されます。[UserName] は、すべてのフェーズ 2、内部トンネル（保護アイデンティティ）の EAP Identity 応答で常に送信されます。

  （注）　一般に、PEAP 方式を使用する Microsoft AAA サーバにはこの設定が必要です。

- True - このオプションの場合 SSC は以下のように動作します。
  - 許容される認証方式のセットがトンネルを使用するものに制限されます。
    ビジネス ルール：対応する *eapMethod* エレメントで EAP FAST、PEAP か TTLS のみが指定されている必要があります。
  - 外部（非保護）トンネルの EAP Identity 応答での UserName の送信が制限されます。

  このモードを使用した場合、クライアントでは Identity 応答に anonymous@Domain が送信されます。

  （注）　Cisco ACS 3.3 AAA サーバのドメインを使用している場合は、この設定を使用する必要があります。

静的クレデンシャル認証のエレメントの設定

次のエレメントを設定します。

ビジネス ルール : これらのエレメントが必要になるのは、対応するクレデンシャル *collectionMethod* エレメントが静的に設定されている場合に限られます。

staticIdentity

スキーマ パス：

configuration/networks/[[wifiNetwork | wiredNetwork]]/authenticationNetwork/
[machineAuthentication | userAuthentication | machineUserAuthentication/machine |
machineUserAuthentication/user]/staticIdentity

オプション エレメント *staticIdentity* の値により、EAP Response/Identity メッセージのコンテンツが指定されます。アイデンティティの形式は Network Access Identifier（NAI）で、汎用形式は UserName@Domain です。ただし @Domain（領域とも呼ばれる）の使用はオプションです（ドメインを使用するかどうかは、固有の認証サーバの要件によって異なります）。

従来の NT4 形式 Domain¥UserName も使用可能です。

ドメインの指定がある場合は、特に処理は行われません。ドメインのエイリアス（完全修飾でない）であるか、完全修飾ドメイン名であるかにかかわりなく、設定されているものが EAP Response メッセージで送信されます。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：指定されるアイデンティティには、63 文字までの ASCII 文字が使用でき、大文字と小文字が区別されます。

staticPassword

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/[machineAuthentication | userAuthentication | machineUserAuthentication/machine | machineUserAuthentication/user]/staticPassword

オプション エレメント *staticPassword* の値により、パスワードの共有秘密情報が指定されます。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

制約：指定されるパスワードには、80 文字までの ASCII 文字が使用でき、大文字と小文字が区別されます。

（注）　ユーザ コンテキスト接続で静的クレデンシャルを使用する場合は、配信パッケージ ファイルに個別値が必要なことがあります。この場合は、エンドユーザのそれぞれに個別のファイルが設定され、共通配信パッケージ ファイルのグローバル展開は適用されません。

認証が行われるユーザ専用のネットワークの設定

次の手順で認証が行われるユーザ専用の Wi-Fi ネットワークを設定します。

ステップ 1　「認証のユーザ専用接続状況エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「認証のユーザ クレデンシャル ソース（1）エレメントの設定」に定義されているタスクを実行します。

ステップ 3　「認証の接続非依存基本エレメントの設定」に定義されているタスクを実行します。

ステップ 4　「静的クレデンシャル認証のエレメントの設定」に定義されているタスクを実行します。

ステップ 5　「FAST PAC エレメントの設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *userAuthentication* エレメントとその子エレメントの 2 種類の接続状況オプションを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-28　userAuthentication

```
<userAuthentication>
    <autoConnect>
        {child element}
    </autoConnect>
    <collectionMethod>
        {child element}
    </collectionMethod>
    <useAnonymousId>true</useAnonymousId>
    <staticIdentity encrypt="true">userName</staticIdentity>
    <staticPassword encrypt="true">userSecret</staticPassword>
    <pacs>
        {child elements}
    </pacs>
    <eapMethods>
        {child elements}
    </eapMethods>
</userAuthentication>

<userAuthentication>
    <manualConnect/>
    <collectionMethod>
        {child element}
    </collectionMethod>
    <useAnonymousId>true</useAnonymousId>
    <staticIdentity encrypt="true">userName</staticIdentity>
    <staticPassword encrypt="true">userSecret</staticPassword>
    <pacs>
        {child elements}
    </pacs>
    <eapMethods>
        {child elements}
    </eapMethods>
</userAuthentication>
```

認証のユーザ専用接続状況エレメントの設定

ユーザ接続に次の接続開始タイプのいずれか 1 つを指定します。

- 自動接続 - エレメント *autoConnect* を使用します。
- 手動接続 - エレメント *manualConnect* を使用します。

autoConnect

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/autoConnect

オプション エレメント *autoConnect* の存在により、ユーザがシステムにログインする際にユーザ コンテキスト ネットワーク接続の自動開始の試行が指定されます。エレメント値は指定されません。

次の子エレメントを設定する必要があります。

connectBeforeLogon

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/autoConnect/connectBeforeLogon

必須ブール エレメント *connectBeforeLogon* により、ログイン要求を基準にして接続が開始されることが指定されます。

このエレメントには次の値があります。

- True - ユーザが Windows にログインする前にネットワークへの接続が開始されます。

  このオプションは、Microsoft Active Directory または Novell ドメインなどのドメイン ログイン環境でネットワークが使用され、特定の Microsoft Group Policy Object（GPO）の使用をサポートするために早期のネットワーク接続が必要な場合にのみ使用します。

  このタイプのネットワーク配置の自動接続では、パスワードとスマート カード クレデンシャルのみがサポートされます（特に、Windows User-Personal 証明書ストア クレデンシャルはユーザのログインの完了前にはアクセスできないため、サポートされません）。
  ビジネス ルール：対応する *certificateSource* エレメントが存在する場合は、*smartCardOnlyCertificate* 子エレメントが選択されている必要があります。
- False - ユーザがデスクトップの Windows へのログインを完了してからネットワークへの接続が開始されます。

  このオプションは、早期ネットワーク接続が必要でない場合に使用します。このモードの場合、使用可能なユーザ クレデンシャル タイプに関する制限はありません。

次の例は、配信パッケージ XML の *autoConnect* エレメントとその子エレメントを示しています。

例 2-29　autoConnect

```
<autoConnect>
    <connectBeforeLogon>true</connectBeforeLogon>
</autoConnect>
```

manualConnect

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/manualConnect

オプション エレメント *manualConnect* の存在により、ユーザがシステムにログインする際にユーザ コンテキスト ネットワーク接続の自動開始が行われないことが指定されます。ユーザはデスクトップから SSC を開き、手動でネットワークの選択および接続を行う必要があります。これは値がない空白エレメントです。

認証のユーザ クレデンシャル ソース（1）エレメントの設定

次のエレメントを設定します。

collectionMethod

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod

必須エレメント *collectionMethod* により、ユーザ クレデンシャルのソースとタイプを設定するコンテナが構成されます。これは値がない空白エレメントです。

ユーザ接続に次のクレデンシャル タイプのいずれか 1 つを指定します。

- ユーザがオンデマンドで入力 - エレメント *prompt* を使用します。
- オペレーティング システムのクレデンシャル - エレメント *singleSignOn* を使用します。
- 事前定義 - エレメント *static* を使用します。

- マシンの Active Directory - エレメント *autoMachine* を使用します。

prompt

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/prompt

オプション エレメント *prompt* の存在により、接続の試行時にユーザのクレデンシャルが要求されることが指定されます。エレメント値は指定されません。

次の項目：「要求されるクレデンシャル保存の選択」

singleSignOn

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/singleSignOn

オプション エレメント *singleSignOn* の存在により、ユーザ名とパスワードなど、ユーザがオペレーティング システムへのログイン時に入力するクレデンシャル（資格情報）が認証にも使用されることが指定されます。SSC のプロビジョニングは必要ありません。これはシングルサインオンとも呼ばれています。SSC では、ユーザの Windows または Novell のログイン名とパスワードに基づくシングルサインオン認証がサポートされます。これは値がない空白エレメントです。

static

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/static

オプション エレメント *static* の存在により、配信パッケージ（設定ファイル）の一部として展開された事前定義のクレデンシャルが使用され、永続的に（または、最短でも更新時までは）保存されることが指定されます。これは値がない空白エレメントです。

ビジネス ルール：このオプションを使用する場合は、項「静的クレデンシャル認証のエレメントの設定」のエレメントを追加し、設定する必要があります。

ビジネス ルール：静的クレデンシャルでは、クライアント証明書の使用を除いて、パスワードを基準にした EAP 方式が必要です。このため、EAP TLS、EAP PEAP、または EAP TLS の内部方式による FAST の方式は使用できません。

autoMachine

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/autoMachine

オプション エレメント *autoMachine* の存在により、既存の Active Directory のマシン クレデンシャルの使用が指定されます。『Cisco Secure Services Client User Guide』では、ユーザ専用マシン コンテキスト接続と呼ばれています。これは値がない空白エレメントです。

（注）　このオプションは、SSC の以前の 4.0.x リリースとの互換性を保持しています。大多数の環境では、新たにサポートされる静的オプションに置き換わります。

次の例は、配信パッケージ XML の *collectionMethod* エレメントとその子エレメントの 4 種類の選択を示しています。

例 2-30　collectionMethod（ユーザ）

```
<collectionMethod>
    <prompt>
        <credentialsStorage>
            {child elements}
        </credentialsStorage>
    </prompt>
</collectionMethod>

<collectionMethod>
    <singleSignOn/>
</collectionMethod>

<collectionMethod>
    <static/>
</collectionMethod>

<collectionMethod>
    <autoMachine/>
</collectionMethod>
```

認証のユーザ クレデンシャル ソース（2）エレメントの設定

次のエレメントを設定します。

collectionMethod

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod

必須エレメント collectionMethod は、ユーザ クレデンシャルのソースとタイプを設定するコンテナを構成します。これは値がない空白エレメントです。

ユーザ接続に次のクレデンシャル タイプのいずれか 1 つを指定します。

- ユーザがオンデマンドで入力 - エレメント *prompt* を使用します。
- オペレーティング システムのクレデンシャル - エレメント *singleSignOn* を使用します。
- 事前定義 - エレメント *static* を使用します。

prompt

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/prompt

オプション エレメント *prompt* の存在により、接続の試行時にユーザのクレデンシャルが要求されることが指定されます。エレメント値は指定されません。

次の項目：「要求されるクレデンシャル保存の選択」

singleSignOn

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/singleSignOn

オプション エレメント *singleSignOn* の存在により、ユーザ名とパスワードなど、ユーザがオペレーティング システムへのログイン時に入力するクレデンシャル（資格情報）が認証にも使用されることが指定されます。SSC のプロビジョニングは必要ありません。これはシングルサインオンとも呼ばれています。SSC では、ユーザの Windows または Novell のログイン名とパスワードに基づくシングルサインオン認証がサポートされます。これは値がない空白エレメントです。

static

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/static

オプション エレメント *static* の存在により、配信パッケージ（設定ファイル）の一部として展開された事前定義のクレデンシャルが使用され、永続的に（または、最短でも更新時までは）保存されることが指定されます。これは値がない空白エレメントです。

ビジネス ルール：このオプションを使用する場合は、項「静的クレデンシャル認証のエレメントの設定」のエレメントを追加し、設定する必要があります。

ビジネス ルール：静的クレデンシャルには、パスワードを基準にした EAP 方式が必要です。このため、EAP TLS、EAP PEAP、または EAP TLS の内部方式による FAST の方式は使用できません。

次の例は、配信パッケージ XML の *collectionMethod* エレメントとその子エレメントの 3 種類の選択を示しています。

例 2-31　collectionMethod（マシン / ユーザ）

```
<collectionMethod>
    <prompt>
        <credentialsStorage>
            {child elements}
        </credentialsStorage>
    </prompt>
</collectionMethod>

<collectionMethod>
    <singleSignOn/>
</collectionMethod>

<collectionMethod>
    <static/>
</collectionMethod>
```

要求されるクレデンシャル保存の選択

次のエレメントを設定します。

credentialsStorage

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/prompt/credentialsStorage

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/prompt/credentialsStorage

必須エレメント *credentialsStorage* により、ユーザに要求したクレデンシャルの保存時間を設定するコンテナが構成されます。これは値がない空白エレメントです。

要求したクレデンシャルに対して、次のクレデンシャル保存時間のいずれか 1 つを指定します。

- 永続的に保存 - エレメント *forever* を使用します。
- ログイン中の保存 - エレメント *logonSession* を使用します。
- 指定期間の保存 - エレメント *duration* を使用します。

ビジネス ルール：ポリシーでサポートされるクレデンシャル保存方式のみを使用できます。「ネットワーク ポリシー」の項のエレメント allowedCredentialStorage を参照してください。

forever

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/collectionMethod/prompt/credentialsStorage/forever

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/prompt/credentialsStorage/forever

オプション エレメント *forever* の存在により、要求されたクレデンシャルが永続的に（最短でも更新時までは）保存されることが指定されます。保存後は、クレデンシャルが静的に展開された場合と同様に使用されます。これは値がない空白エレメントです。

logonSession

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthenticationcollectionMethod/prompt/credentialsStorage/logonSession

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/prompt/credentialsStoragelogonSession

オプション エレメント *logonSession* の存在により、要求されたクレデンシャルが現在のログイン セッションの期間以降は保存されないことが指定されます。ユーザは、システムにログインするたびにクレデンシャル（資格情報）を入力しなおす必要があります。これは値がない空白エレメントです。

duration

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthenticationcollectionMethod/prompt/credentialsStorage/duration

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/collectionMethod/prompt/credentialsStorage/duration

オプション エレメント *duration* の存在により、要求されたクレデンシャルがネットワーク ポリシーで設定された期間だけ保存されることが指定されます。ユーザ セッションの進行中に期間が切れても、クレデンシャルは要求されません。ただし、タイムアウト後は、Request for Credentials ダイアログで再認証要求が行われ、ユーザに対してクレデンシャルの再入力が強制されます。再入力によって、期間のタイマが再び開始されます。これは値がない空白エレメントです。

次の例は、配信パッケージ XML の *credentialStorage* エレメントとその子エレメントの 3 種類の設定オプションを示しています。

例 2-32　credentialsStorage

```
<credentialsStorage>
    <forever/>
</credentialsStorage>

<credentialsStorage>
    <logonSession/>
</credentialsStorage>

<credentialsStorage>
    <duration/>
</credentialsStorage>
```

FAST PAC エレメントの設定

次のエレメントを設定します。

pacs

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/pacs

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/pacs

オプション エレメント *pacs* により、この展開配信パッケージ（設定ファイル）を使用した、ユーザの EAP-FAST トンネル PAC の手動プロビジョニングをサポートするコンテナが構成されます。エレメント値は指定されません。

ビジネス ルール：このエレメントが存在する場合は、このネットワークで EAP-FAST を設定する必要があることを意味します。特に、同じ wifiNetwork または wiredNetwork エレメントには対応する *eapMethods*/*eapFast* エレメントが存在している必要があります。

次の子エレメントを設定する必要があります。

pac

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/pacs/pac

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/pacs/pac

必須エレメント *pac* により、個別のトンネル PAC の情報のコンテナが構成されます。エレメント値は指定されません。

pac エレメントは、必要な数だけ追加できます。

次の手順を実行して、トンネル PAC の情報を設定します。

ステップ 1　次のエレメントを指定し、設定します。

pacReference

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/pacs/pac/pacReference

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/pacs/pac/pacReference

エレメント *pacReference* の値では、PAC ファイルへの完全パスが指定されます。このファイルは postprocess sscPackageProcess ユーティリティからのアクセスが可能である必要があります。XML 配信パッケージ ファイルの postrocess ツールは、PAC ファイルを取得して、情報を自動的に符号化し（base64 文字列）、*content* エレメントを読み込み、*content* エレメントで *pacReference* エレメントを置換します。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

ステップ 2　次のエレメントを設定します。

secretKey

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/userAuthentication/pacs/pac/secretKey

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/pacs/pac/secretKey

オプション エレメント *secretKey* の値により、Cisco ACS がパスワード保護対象として PAC を作成した場合のシークレット（パスワード）が指定されます。

このエレメントには必須のブール アトリビュート encrypt があり、固定値 True が設定されます。これによって、postprocess sscPackageProcess ユーティリティでこのエレメントを暗号化する（している）必要があることが指定されます。

（注）　ユーザのトンネル PAC のプロビジョニングを手動で実行する配信パッケージを使用する場合は、配信パッケージ ファイルに個別値が必要です。エンドユーザのそれぞれに個別のファイルが設定され、共通配信パッケージ ファイルのグローバル展開は適用されません。

次の例は、配信パッケージ XML の *pacs* エレメントとその子エレメントを示しています。複数の子エレメントの順序は表示されている順序に制限されます。

例 2-33　pacs

```
<pacs>
    <pac>
        <pacReference encrypt="true">E:¥path¥pacFile</pacReference>
    </pac>
</pacs>

<pacs>
    <pac>
        <pacReference encrypt="true">E:¥path¥pacFile</pacReference>
        <secretKey encrypt="true">my pac secret</secretKey>
    </pac>
</pacs>
```

認証が行われるマシンとユーザのネットワークの設定

次の手順で認証が行われるマシンとユーザ コンテキストの Wi-Fi ネットワークを設定します。

ステップ 1　マシン部分を設定します。

a. 「認証が行われるマシン クレデンシャル ソース エレメントの設定」に定義されているタスクを実行します。

b. 「認証の接続非依存基本エレメントの設定」に定義されているタスクを実行します。

c. 「静的クレデンシャル認証のエレメントの設定」に定義されているタスクを実行します。

ステップ 2　ユーザ部分を設定します。

a. 「認証のユーザ接続状況エレメントの設定」に定義されているタスクを実行します。

b. 「認証のユーザ クレデンシャル ソース（2）エレメントの設定」に定義されているタスクを実行します。

c. 「認証の接続非依存基本エレメントの設定」に定義されているタスクを実行します。

d. 「静的クレデンシャル認証のエレメントの設定」に定義されているタスクを実行します。

e. 「FAST PAC エレメントの設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *machineUserAuthentication* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-34　userAuthentication

```
<machineUserAuthentication>
    <machine>
        <collectionMethod>
            {child element}
        </collectionMethod>
        <useAnonymousId>true</useAnonymousId>
        <staticIdentity encrypt="true">machineName</staticIdentity>
        <staticPassword encrypt="true">machineSecret</staticPassword>
    </machine>
    <user>
        <autoConnect>true</autoConnect>
        <collectionMethod>
            {child element}
        </collectionMethod>
        <useAnonymousId>true</useAnonymousId>
        <staticIdentity encrypt="true">userName</staticIdentity>
        <staticPassword encrypt="true">userSecret</staticPassword>
        <pacs>
            {child elements}
        </pacs>
    </user>
    <eapMethods>
        {child elements}
    </eapMethods>
</machineUserAuthentication>
```

認証のユーザ接続状況エレメントの設定

ユーザ接続に次の接続開始タイプのいずれか 1 つを指定します。

- 自動接続 - エレメント *autoConnect* を使用します。
- 手動接続 - エレメント *manualConnect* を使用します。

autoConnect

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/autoConnect

オプション エレメント *autoConnect* の存在により、ユーザがシステムにログインする際にユーザ コンテキスト ネットワーク接続の自動開始の試行が指定されます。エレメント値は指定されません。

次の子エレメントを設定する必要があります。

connectBeforeLogon

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/autoConnect/connectBeforeLogon

必須ブール エレメント *connectBeforeLogon* により、ログイン要求を基準にして接続が開始されることが指定されます。

このエレメントには次の値があります。

- True - ユーザが Windows にログインする前にネットワークへの接続が開始されます。

  このオプションは、Microsoft Active Directory ドメインなどドメイン ログイン環境でネットワークを使用し、早期のネットワーク接続が必要な場合に使用します。このオプションでは、次のことが可能です。

  - ユーザ コンテキスト接続での特定の Microsoft Group Policy Object（GPO）の処理
  - 必要に応じて、マシンおよびユーザ コンテキスト間を転送する際の IP アドレス変更に対処（たとえば、VLAN 変更が伴う場合）

  このタイプのネットワーク配置の自動接続では、パスワードとスマート カード クレデンシャルのみがサポートされます（特に、Windows User-Personal 証明書ストア クレデンシャルはユーザのログインの完了前にはアクセスできないため、サポートされません）。
  ビジネス ルール：対応する *certificateSource* エレメントが存在する場合は、*smartCardOnlyCertificate* 子エレメントが選択されている必要があります。
- False - ユーザがデスクトップの Windows へのログインを完了してからネットワークへの接続が開始されます。

  このオプションは、早期ネットワーク接続が必要でない場合に使用します。Microsoft Active Directory ドメインなどドメイン ログイン環境でネットワークを使用する場合、このオプションによって次のことが可能になります。

  - マシンおよびユーザ コンテキスト間を転送する際に IP アドレス変更が不要な場合、ユーザ コンテキスト接続での特定の Microsoft Group Policy Object（GPO）の処理

  このモードの場合、使用可能なユーザ クレデンシャル タイプに関する制限はありません。

次の例は、配信パッケージ XML の *autoConnect* エレメントとその子エレメントを示しています。

例 2-35　autoConnect

```
<autoConnect>
    <connectBeforeLogon>true</connectBeforeLogon>
</autoConnect>
```

manualConnect

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineUserAuthentication/user/manualConnect

オプション エレメント *manualConnect* の存在により、ユーザがシステムにログインする際にユーザ コンテキスト ネットワーク接続の自動開始が行われないことが指定されます。ユーザはデスクトップから SSC を開き、手動でネットワークの選択および接続を行う必要があります。これは値がない空白エレメントです。

有線ネットワーク基本エレメント

次のエレメントを設定します。

displayName

スキーマ パス：

configuration/networks/wiredNetwork/displayName

必須エレメント *displayName* の値により、SSC の各種ダイアログで表示専用として使用されるユーザフレンドリな名前が指定されます。

有線ネットワークのセキュリティ クラスの選択

ネットワークに次のセキュリティ クラスのいずれか 1 つを指定します。

- オープン ネットワーク - エレメント *openNetworkMachineConnection* を使用します。ネットワークが認証なしのスイッチで構成されるが、接続を監視および表示する場合に、選択します。
- 認証ネットワーク - エレメント *authenticationNetwork* を使用します。使用する認証サーバとポリシー、および使用するクレデンシャル環境との整合性がある企業ネットワークを事前設定する必要がある場合に選択します。

openNetworkMachineConnection

スキーマ パス：

configuration/networks/wiredNetwork/openNetworkMachineConnection

オプション エレメント *openNetworkMachineConnection* の存在によって、オープンの有線ネットワークが指定されます。SSC のオープン ネットワークは、いかなる形態のデータの暗号化も使用しないため、最低レベルのネットワーク セキュリティ保護クラスになります。これは値がない空白エレメントです。

ビジネス ルール：これは、ポリシーで *open* アソシエーション モードがサポートされる場合にのみ有効な選択です。「ネットワーク ポリシー」の項のエレメント allowedAssociationModes を参照してください。

authenticationNetwork

スキーマ パス：

configuration/networks/wiredNetwork/authenticationNetwork

オプション エレメント *authenticationNetwork* により、802.1X 有線ネットワークを設定するコンテナが構成されます。認証 /802.1X ネットワークには、有線のセキュリティに対してクライアントとサーバの相互認証、およびネットワークによる暗号化キーの提供という 2 つの重要な特徴が追加されます。このネットワーク クラスは、最高のセキュリティ レベルの選択肢です。エレメント値は指定されません。

次の項目：「認証有線ネットワークの設定」

次の例は、配信パッケージ XML の *wiredNetwork* エレメントとその子エレメントの 2 つのセキュリティ クラスを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-36　wiredNetwork

```
<wiredNetwork>
    <displayName>My Corporate Ethernet Network</displayName>
    <openNetworkMachineConnection/>
</wiredNetwork>

<wiredNetwork>
    <displayName>My Corporate Ethernet Network</displayName>
    <authenticationNetwork>
        {child elements}
    </authenticationNetwork>
</wiredNetwork>
```

認証有線ネットワークの設定

次の手順で認証有線ネットワークを設定します。

ステップ 1　「認証ネットワーク基本エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「認証ネットワークの接続コンテキストの選択」に定義されているタスクを実行します。

ステップ 3　「有線 EAP 方式の選択」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の有線の *authenticationNetwork* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-37　authenticationNetwork の部分

```
<authenticationNetwork>
    <!--{your choice of network connection context goes here}-->
    <serverValidation>
        {child elements}
    </serverValidation>
    <interactiveAuthenticationRetries>4</interactiveAuthenticationRetries>
    <nonInteractiveAuthenticationRetries>4</nonInteractiveAuthenticationRetries>
</authenticationNetwork>
```

Wi-Fi EAP 方式の選択

「Wi-Fi/ 有線 EAP 方式の選択」に定義されているタスクを実行します。

有線 EAP 方式の選択

次のエレメントを設定します。

eapMethods

スキーマ パス：

configuration/networks/wiredNetwork/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods

必須エレメント *eapMethods* により、ネットワークでサポートされる EAP 方式をリストするコンテナが構成されます。認証プロセスの EAP ネゴシエーション フェーズで、SSC がサポート対象として設定されていない特定の EAP 方式の要求をサーバから受信した場合は、代替 EAP 方式の順序付きリストで応答します。サーバはこのリストを処理して、使用可能な代替を検索します。使用可能な代替が検索された場合は、相互に合意できる方式で再度ネゴシエートが行われますが、検索できなかった場合は認証が失敗します。リストの順序は、XML で選択された子エレメントの順序によって決定されます。

ビジネス ルール：1 つ以上の子エレメント（1 つ以上の EAP 方式）を指定する必要があります。

ビジネス ルール：使用可能な EAP 方式はポリシーでサポートされているものに限られます。「ネットワーク ポリシー」のエレメント *allowedEapMethods* を参照してください。

次の有線専用 EAP 方式を 1 つ以上指定します。

- EAP-MD5 - エレメント *eapMd5* を使用します。
- EAP-MSCHAPv2 - エレメント *eapMschapv2* を使用します。
- EAP-GTC - エレメント *eapGtc* を使用します。

あるいは、「Wi-Fi/ 有線 EAP 方式の選択」に掲載されている共通 EAP 方式を 1 つ以上指定します。

eapMd5

スキーマ パス：

configuration/networks/wiredNetwork/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapMd5

オプション エレメント *eapMd5* の存在により、このネットワークでの Message Digest 5（EAP-MD5）認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eapMschapv2

スキーマ パス：

configuration/networks/wiredNetwork/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapMschapv2

オプション エレメント *eapMschapv2* の存在により、このネットワークでの Microsoft チャレンジ ハンドシェーク認証プロトコル v2（EAP-MSCHAPv2）認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eapGtc

スキーマ パス：

configuration/networks/wiredNetwork/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapGtc

オプション エレメント *eapGtc* の存在により、このネットワークでの Generic Token Card（EAP-GTC）認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

次の例は、配信パッケージ XML における有線専用の *eapMethods* エレメントとその子エレメントを示しています。子エレメントの順序に制約はありません。

例 2-38　eapMethods（有線）

```
<eapMethods>
    <eapMd5/>
    <eapMschapv2/>
    <eapGtc/>
</eapMethods>
```

Wi-Fi/ 有線 EAP 方式の選択

次のエレメントを設定します。

eapMethods

スキーマ パス：

configuration/networks/wiredNetwork | wifiNetwork/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods

必須エレメント *eapMethods* により、ネットワークでサポートされる EAP 方式をリストするコンテナが構成されます。認証プロセスの EAP ネゴシエーション フェーズで、SSC がサポート対象として設定されていない特定の EAP 方式の要求をサーバから受信した場合は、代替 EAP 方式の順序付きリストで応答します。サーバはこのリストを処理して、使用可能な代替を検索します。使用可能な代替が検索された場合は、相互に合意できる方式で再度ネゴシエートが行われますが、検索できなかった場合は認証が失敗します。リストの順序は、XML にリストされている子エレメントの選択順序によって決定されます。

ビジネス ルール：1 つ以上の子エレメント、言い換えると、1 つ以上の EAP 方式を指定する必要があります。

ビジネス ルール：使用可能な EAP 方式はポリシーでサポートされているものに限られます。「ネットワーク ポリシー」の項のエレメント allowedEapMethods を参照してください。

次の共通（Wi-Fi またはイーサネット）EAP 方式を 1 つ以上指定します。

- EAP-FAST - エレメント *eapFast* を使用します。
- EAP-PEAP - エレメント *eapPeap* を使用します。
- EAP-TTLS - エレメント *eapTtls* を使用します。
- EAP-TLS - エレメント *eapTls* を使用します。
- EAP-LEAP - エレメント *leap* を使用します。

eapFast

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast

オプション エレメント *eapFast* の存在により、このネットワークでのシスコのイニシアティブの認証方式である Flexible Authentication via Secure Tunnelling（EAP-FAST）のサポートが指定されます。

次の項目：「EAP-FAST の設定」

eapPeap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapPeap

オプション エレメント *eapPeap* の存在により、このネットワークでの Microsoft およびシスコの双方のイニシアティブの認証方式である Protected Extensible Authentication Protocol（EAP-PEAP）のサポートが指定されます。

次の項目：「EAP-PEAP の設定」

eapTtls

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls

オプション エレメント *eapTtls* の存在により、このネットワークでの Funk のイニシアティブの認証方式である Tunneled Transport Layer Security（EAP-TTLS）のサポートが指定されます。

次の項目：「EAP-TTLS の設定」

eapTls

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTls

オプション エレメント *eapTls* の存在により、このネットワークでの Transport Layer Security（EAP-TLS）認証方式のサポートが指定されます。

次の項目：「EAP-TLS の設定」

leap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/leap

オプション エレメント *leap* の存在により、このネットワークでの Light Extensible Authentication Protocol（LEAP）認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

（注） LEAP はシスコのイニシアティブで、先行標準（802.1X）の例の 1 つであり、クライアントとサーバ間の相互認証に共有秘密情報を使用する専用の認証方式です。SSC では従来の互換性の保持のためにサポートされています。

次の例は、配信パッケージ XML における有線または無線の *eapMethods* エレメントとその子エレメントを示しています。子エレメントの順序に制約はありません。

例 2-39　eapMethods（有線または無線）

```
<eapMethods>
    <leap/>
    <eapFast>
        {child elements}
    </eapFast>
    <eapPeap>
        {child elements}
    </eapPeap>
    <eapFast>
        {child elements}
    </eapTls>
    <eapFast>
        {child elements}
    </eapTls>
    <eapTtls>
        {child elements}
    </eapTtls>
</eapMethods>
```

EAP-FAST の設定

次の手順で EAP-FAST を設定します。

ステップ 1　「EAP 基本エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「FAST クライアント証明書の設定」に定義されているタスクを実行します。

ステップ 3　「内部方式の設定」に定義されているタスクを実行します。

（注）　匿名（認証なし）、自律的 PAC プロビジョニングのみの EAP-FAST は EAP-FAST 規格の初期バージョン v1 に対応します。
認証あり、自律的 PAC プロビジョニングの EAP-FAST は、バージョン v1a で導入されました。このバージョンには下位互換性があり、初期の認証なしの方式もサポートされます。

次の例は、配信パッケージ XML の *eapFast* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-40　eapFast

```
<eapFast>
    <validateServerIdentity>true</validateServerIdentity>
    <enableFastReconnect>true</enableFastReconnect>
    <protectClientCertificate>true</protectClientCertificate>
    <certificateSource>
        {child element}
    </certificateSource>
    <innerEapMethods>
        {child elements}
    </innerEapMethods>
</eapFast>
```

EAP-PEAP の設定

次の手順で EAP-PEAP を設定します。

ステップ 1　「EAP 基本エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「PEAP クライアント証明書の設定」に定義されているタスクを実行します。

ステップ 3　「内部方式の設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *eapPeap* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-41　eapPeap

```
<eapPeap>
    <validateServerIdentity>true</validateServerIdentity>
    <enableFastReconnect>true</enableFastReconnect>
    <protectClientCertificate>false</protectClientCertificate>
    <certificateSource>
        {child element}
    </certificateSource>
    <innerEapMethods>
        {child elements}
    </innerEapMethods>
</eapPeap>
```

EAP-TTLS の設定

次の手順で EAP-TTLS を設定します。

ステップ 1　「EAP 基本エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「TTLS 内部方式の設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *eapTtls* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-42　eapTtls

```
<eapTtls>
    <validateServerIdentity>true</validateServerIdentity>
    <enableFastReconnect>true</enableFastReconnect>
    <innerMethods>
        {child element}
    </innerMethods>
</eapTtls>
```

EAP-TLS の設定

次の手順で EAP-TLS を設定します。

ステップ 1　「EAP 基本エレメントの設定」に定義されているタスクを実行します。

ステップ 2　「クライアント証明書ソースの設定」に定義されているタスクを実行します。

次の例は、配信パッケージ XML の *eapTls* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-43　eapTls

```
<eapTls>
    <validateServerIdentity>true</validateServerIdentity>
    <enableFastReconnect>true</enableFastReconnect>
    <certificateSource>
        {child element}
    </certificateSource>
</eapTls>
```

EAP 基本エレメントの設定

次のエレメントを設定します。

validateServerIdentity

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap | eapTtls | eapTls/validateServerIdentity

必須のブール エレメント *validateServerIdentity* により、認証時に SSC がクライアント側のサーバの確認を実行するかどうかが指定されます。

このエレメントには次の値があります。

- True - サーバの証明書を確認します。
- False - サーバの証明書を確認しません。

  セキュリティのレベルを低下させるため、このオプションは*推奨されない*もので、通常はデバッグにのみ使用されます（サーバの証明書が認証失敗の原因であるかどうかを判定するため）。このオプションを使用した場合、無線ネットワークは Wi-Fi 準拠ではなくなります。

ビジネス ルール：*validateSeverIdentity* の値が True の場合は同一ネットワークにサーバ確認の詳細を設定するオプション エレメント *serverValidation* が存在している必要があります。

ビジネス ルール：ネットワーク ポリシーで必須の確認が指定されている場合は、この値を True にする必要があります。「ネットワーク ポリシー」のエレメント *alwaysValidate* を参照してください。

enableFastReconnect

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap | eapTtls | eapTls/enableFastReconnect

必須のブール エレメント *enableFastReconnect* により、再認証の要求時に SSC がキャッシュされたクレデンシャル情報を使用して高速なセッション再開を実行するかどうかが指定されます（状況に応じて外部トンネル方式、内部トンネル方式の双方に適用されます）。

このエレメントには次の値があります。

- True - 高速セッション再開を許可します。
- False - 高速セッション再開を許可しません。

（注）　ネットワーク プロファイルで、SSL セッションの開始に関連する複数の EAP 認証方式が指定され（エレメント eapFast | eapPeap | eapTtls | eapTls）、いずれかの方式でエレメント *enableFastReconnect* が True に設定されている場合、このネットワーク プロファイルに関連付けられているすべての方式で高速セッション再開が有効になります。

FAST クライアント証明書の設定

これらのエレメントに要求される一連の手順は、例 2-40 を参照してください

ステップ 1　次のエレメントを設定します。

protectClientCertificate

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast/protectClientCertificate

必須のブール エレメント *protectClientCertificate* により、要求があった場合に SSC が証明書を保護されない状態で送信するかどうかが指定されます。

このエレメントには次の値があります。

- True - 次のように指定します。

  保護を有効化し、クライアント証明書は使用します、または

  クライアント証明書は使用しません。

  FAST PAC プロビジョニングの保護なし（フェーズ 1）部分でサーバからクライアント証明書を要求された場合は次のようになります。

  — プロトコルの保護ありのフェーズ 2 まで待機するため、この時点ではすべての証明書（このオプションで許可されるもの）の送信が SSC によって拒否されます（実際には、まずサーバの証明書に基づいてトンネルが確立され、フェーズ 2 の開始前に SSC からクライアント証明書が送信されます）。

  Cisco ACS でクライアント証明書の使用が設定されていない場合は、フェーズ 2 で証明書が要求されません。このため、この値を使用して不要なクライアント証明書の要求を回避することが重要になります。

- False - 保護を無効化し、クライアント証明書は使用します。
  FAST PAC プロビジョニングの保護なし（フェーズ 1）部分でサーバからクライアント証明書を要求された場合は次のようになります。

  — クライアント証明書が利用可能であれば、送信されます。

  — クライアント証明書がない場合は、何も送信されず、サーバ ポリシーによって認証の続行または失敗が判定されます。

FAST PAC プロビジョニングの保護あり（フェーズ 2）部分でのクライアント証明書の使用には影響しません。サーバがセキュリティが保護されたトンネル内でのクライアント証明書の送信を要求するように設定されている場合、クライアントは常にいずれかの使用を試行します。利用可能なものがなく送信されない場合、接続は失敗します。

ステップ 2　「クライアント証明書ソースの設定」に定義されているタスクを実行します。

PEAP クライアント証明書の設定

これらのエレメントに要求される一連の手順は、例 2-41 を参照してください

ステップ 1　次のエレメントを設定します。

protectClientCertificate

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapPeap | eapTtls/protectClientCertificate

必須のブール エレメント *protectClientCertificate* により、要求があった場合に SSC が証明書を保護されない状態で送信するかどうかが指定されます。

このエレメントには次の値があります。

- True - 保護を有効化します。
  プロトコルの保護なし（フェーズ 1）部分でサーバからクライアント証明書を要求された場合は次のようになります。
  - クライアント証明書はサーバに送信されません（この EAP 方式ではクライアント証明書を保護された状態で送信する方法がないため）。サーバ ポリシーによって認証の続行または失敗が判定されます。
- False - 保護を無効にします。
  プロトコルの保護なし（フェーズ 1）部分でサーバからクライアント証明書を要求された場合は次のようになります。
  - クライアント証明書が利用可能であれば、送信されます。
  - クライアント証明書がない場合は、何も送信されず、サーバ ポリシーによって認証の続行または失敗が判定されます。

ステップ 2　「クライアント証明書ソースの設定」に定義されているタスクを実行します。

クライアント証明書ソースの設定

次のエレメントを設定します。

certificateSource

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap | eapTls/certificateSource

エレメント *certificateSource* は、クライアント証明書のソースを指定するコンテナを構成します。エレメント値は指定されません。

制約：*certificateSource* は *eapTls* エレメントで必要とされます。

ビジネス ルール：*certificateSource* は、eapPeap および eapFast エレメント内の、認証サーバのポリシーによって設定される外部トンネルに関するオプションです。ただし、対応する内部方式に EAP TLS が指定されている場合は必須です。

クライアント証明書に次のソースのいずれか 1 つを指定します。

- スマート カードからのみ取得 - エレメント *smartCardOnlyCertificate* を使用します。
- Windows 証明書ストアまたはスマート カードから取得 - エレメント *smartCardOrOsCertificate* を使用します。

スマート カード証明書のプロパティ

- 1 つのスマート カード リーダー（最初に検出されたもの）のみがサポートされます。
- 1 つのスマート カードの複数の証明書がサポートされます。
- スマート カードは、Cryptgraphic Service Provider（CSP）機能に対応する Microsoft CryptoAPI および SCard インターフェイスをサポートする必要があります。さらに、スマート カード リーダーとスマート カードのすべての組み合わせが PC/SC インターフェイスを介して相互動作して、同じ CSP 機能の低レベルのサポートを行う必要があります。
- スマート カード PIN（2 要素認証）がサポートされます。Enter Your Credentials ダイアログまたはオペレーティング システムの GINA によって要求が行われます。PIN の動作は、ネットワークに設定されたユーザ クレデンシャル収集方式によって異なります。
  - collectionMethod/prompt | static - PIN は保存されないため、サーバが開始する再認証の要求（EAP 方式で高速セッション再開が設定されている場合を除く）、ローミング、再認証の失敗、アソシエーションの消失、休止状態からの再開などの状況では、再度要求されます。
  - collectionMethod/singleSignOn - ログオン セッションの継続中は PIN が保存されます。このため、後からポップアップで要求されることはありません。

Windows 証明書のプロパティ

- 認証プロセスの一環として Windows ユーザ証明書が要求される場合は、別のタスクとして適切にインストールしておく必要があります。
  - ユーザ証明書は、現在ログインしている Windows ユーザの個人用証明書ストアから取得されます。
  - マシン証明書は、ローカル コンピュータの個人用証明書ストアから取得されます。
- 選択の際は有効な証明書のみが表示されます。期限切れの証明書は表示されません。また、期限切れが近い有効証明書には証明書の期限が切れるまでの残存日数を表示する警告が組み込まれます。
- 自動ユーザ接続を設定している場合、強力な秘密キーの保護の証明書ではログオンが失敗し、使用できません。このプロパティの証明書は、デスクトップで常に手動接続を行うように設定された場合にのみサポートされます。

- 選択ドロップダウン リストで選択された証明書の識別情報は、次のようにさまざまなフィールドから取得されます。
  - テキスト ボックス名 - Subject: CN（通常名）
  - 発行先 : - Subject: CN（通常名）
  - 発行元 : - Subject: CN（通常名）
  - 別名 : - Subject Alternate Name: DNSName
  - 有効期限 : - Valid to
  - 拡張キー使用法 - Extended Key Usage

smartCardOnlyCertificate

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap | eapTtls | eapTls/certificateSource/smartCardOnlyCertificate

オプション エレメント *smartCardOnlyCertificate* により、クライアント証明書の取得がスマート カードからのみに限定されることが指定されます。これは値がない空白エレメントです。

ビジネス ルール：対応する接続コンテキストが *machineAuthentication* の場合、OS ストアのマシン証明書を使用する必要があるため、このオプションは使用できません

smartCardOrOsCertificate

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap | eapTtls | eapTls/certificateSource/smartCardOrOsCertificate

オプション エレメント *smartCardOrOsCertificate* により、クライアント証明書をスマート カードまたは Windows 証明書ストアから取得できることが指定されます。これは値がない空白エレメントです。

次の例は、配信パッケージ XML の *certificateSource* エレメントとその子エレメントの 2 種類の選択を示しています。

例 2-44　certificateSource

```
<certificateSource>
    <smartCardOrOsCertificate/>
</certificateSource>

<certificateSource>
    <smartCardOnlyCertificate/>
</certificateSource>
```

内部方式の設定

次のエレメントを設定します。

innerEapMethods

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap/innerEapMethods

必須エレメント *innerEapMethods* により、外部 EAP 方式に対してサポートされる内部 EAP 方式をリストするコンテナが構成されます。認証プロセスの EAP ネゴシエーション フェーズで、SSC がサポート対象として設定されていない特定の EAP 方式の要求をサーバから受信した場合は、代替 EAP 方式の順序付きリストで応答します。サーバはこのリストを処理して、使用可能な代替を検索します。使用可能な代替が検索された場合は、相互に合意できる方式で再度ネゴシエートが行われますが、検索できなかった場合は認証が失敗します。リストの順序は、XML にリストされている子エレメントの選択順序によって決定されます。エレメント値は指定されません。

ビジネス ルール : 1 つ以上の子エレメント（1 つ以上の内部 EAP 方式）を指定する必要があります。

次の FAST/PEAP 内部 EAP 方式を 1 つ以上指定します。

- EAP-MSCHAPv2 - エレメント *eapMschapv2* を使用します。
- EAP-GTC - エレメント *eapGtc* を使用します。
- EAP-TLS - エレメント *eapTls* を使用します。

eapMschapv2

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap/innerEapMethods/eapMschapv2

オプション エレメント *eapMschapv2* の存在により、このネットワークでの Microsoft チャレンジ ハンドシェーク認証プロトコル v2（EAP-MSCHAPv2）内部認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eapGtc

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap/innerEapMethods/eapGtc

オプション エレメント *eapGtc* の存在により、このネットワークでの Generic Token Card（EAP-GTC）内部認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eapTls

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/
machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/
eapFast | eapPeap/innerEapMethods/eapTls

オプション エレメント *eapTls* の存在により、このネットワークでの Transport Layer Security（EAP-TLS）内部認証方式のサポートが指定されます。

ビジネス ルール：このオプションを使用する場合は、「クライアント証明書ソースの設定」のエレメントを追加し、設定する必要があります。

次の子エレメントを設定する必要があります。

validateServerIdentity

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap/innerEapMethods/eapTls/validateServerIdentity

必須のブール エレメント *validateServerIdentity* により、セキュリティが保護された内部トンネル内での認証時に SSC がクライアント側のサーバの確認を実行するかどうかが指定されます。

このエレメントには次の値があります。

- True - サーバの証明書を確認します。
- False - サーバの証明書を確認しません。

  セキュリティのレベルを低下させるため、このオプションは推奨されないもので、通常はデバッグにのみ使用されます（サーバの証明書が認証失敗の原因であるかどうかを判定するため）。このオプションを使用した場合、無線ネットワークは Wi-Fi 準拠ではなくなります。

ビジネス ルール：*validateSeverIdentity* の値が True の場合は同一ネットワークにサーバ確認の詳細を設定するオプション エレメント *serverValidation* が存在している必要があります。

次の例は、配信パッケージ XML の *innerEapMethods* エレメントとその子エレメントを示しています。子エレメントの順序と数に制約はありません。

例 2-45　innerEapMethods

```
<innerEapMethods>
    <eapMschapv2/>
    <eapGtc/>
    <eapTls>
        <validateServerIdentity>true</validateServerIdentity>
    </eapTls>
</innerEapMethods>
```

TTLS 内部方式の設定

次のエレメントを設定します。

innerMethods

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap/innerMethods

必須エレメント *innerMethods* により、外部 EAP 方式でサポートされる内部方式をリストするコンテナが構成されます。従来の方式と EAP-TTLS 内の EAP 方式の使用は相互排他的であるため同時に指定することはできません。エレメント値は指定されません。

次の内部方式のクラスのいずれか 1 つを指定します。

- 従来の方式 - エレメント *legacy* を使用します。
- EAP 方式 - エレメント *eap* を使用します。

legacy

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/legacy

オプション エレメント *legacy* により、従来の TTLS 内部方式のいずれかを設定するコンテナが構成されます。エレメント値は指定されません。

次の従来の TTLS 内部方式のいずれか 1 つを指定します。

- PAP - エレメント *pap* を使用します。
- CHAP - エレメント *chap* を使用します。
- MSCHAP - エレメント *mschap* を使用します。
- MSCHAPv2 - エレメント *mschapv2* を使用します。

pap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/legacy/pap

オプション エレメント *pap* の存在により、このネットワークでの内部認証方式に Password Authentication Protocol（PAP）が使用されることが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

chap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/legacy/chap

オプション エレメント *chap* の存在により、このネットワークでの内部認証方式に Challenge-Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）が使用されることが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

mschap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/legacy/mschap

オプション エレメント *mschap* の存在により、このネットワークでの内部認証方式に Microsoft チャレンジ ハンドシェーク認証プロトコル（MSCHAP）が使用されることが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

mschapv2

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/legacy/mschapv2

オプション エレメント *mschapv2* の存在により、このネットワークでの内部認証方式に Microsoft チャレンジ ハンドシェーク認証プロトコル v2（MSCHAPv2）が使用されることが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eap

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapTtls/innerMethods/eap

オプション エレメント *eap* により、標準の EAP 方式のいずれかを設定するコンテナが構成されます。認証プロセスの EAP ネゴシエーション フェーズで、SSC がサポート対象として設定されていない特定の EAP 方式の要求をサーバから受信した場合は、代替 EAP 方式の順序付きリストで応答します。サーバはこのリストを処理して、使用可能な代替を検索します。使用可能な代替が検索された場合は、相互に合意できる方式で再度ネゴシエートが行われますが、検索できなかった場合は認証が失敗します。リストの順序は、XML にリストされている子エレメントの選択順序によって決定されます。エレメント値は指定されません。

ビジネス ルール : 1 つ以上の子エレメント、言い換えると、1 つ以上の内部 EAP 方式を指定する必要があります。

次の内部 EAP 方式を 1 つ以上指定します。

- EAP-MSCHAPv2 - エレメント *eapMschapv2* を使用します。
- EAP-MD5 - エレメント *eapMd5* を使用します。

eapMschapv2

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap/innerMethods/eapMschapv2

オプション エレメント *eapMschapv2* の存在により、このネットワークでの Microsoft チャレンジ ハンドシェーク認証プロトコル v2（EAP-MSCHAPv2）内部認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

eapMd5

スキーマ パス：

configuration/networks/[wifiNetwork | wiredNetwork]/authenticationNetwork/machineAuthentication | userAuthentication | machineUserAuthentication/eapMethods/eapFast | eapPeap/innerMethods/eapMd5

オプション エレメント *eapMd5* の存在により、このネットワークでの Message Digest 5（EAP-MD5）内部認証方式のサポートが指定されます。追加の設定は必要ありません。これは値がない空白エレメントです。

次の例は、配信パッケージ XML の *innerMethods* エレメントとその子エレメントを示しています。子エレメントの順序は表示されている順序に制限されます。

例 2-46　innerMethods

```
<innerMethods>
    <legacy>
        <pap/>
    </legacy>
</innerMethods>

<innerMethods>
    <legacy>
        <chap/>
    </legacy>
</innerMethods>

<innerMethods>
    <legacy>
        <mschap/>
    </legacy>
</innerMethods>

<innerMethods>
    <legacy>
        <mschapv2/>
    </legacy>
</innerMethods>

<innerMethods>
    <eap>
        <eapMd5/>
        <eapMschapv2/>
    </eap>
</innerMethods>
```