CHAPTER 6

エンドユーザおよびクライアント ソフトウェアの分類

ユーザおよびクライアント ソフトウェアの分類:概要

識別プロファイルによるユーザおよびユーザ エージェント(クライアント ソフトウェア)の分類は、以下の目的のために行われます。

- ポリシーの適用に対するトランザクション要求をグループ化します(SaaS を除く)。
- 識別および認証の要件の指定

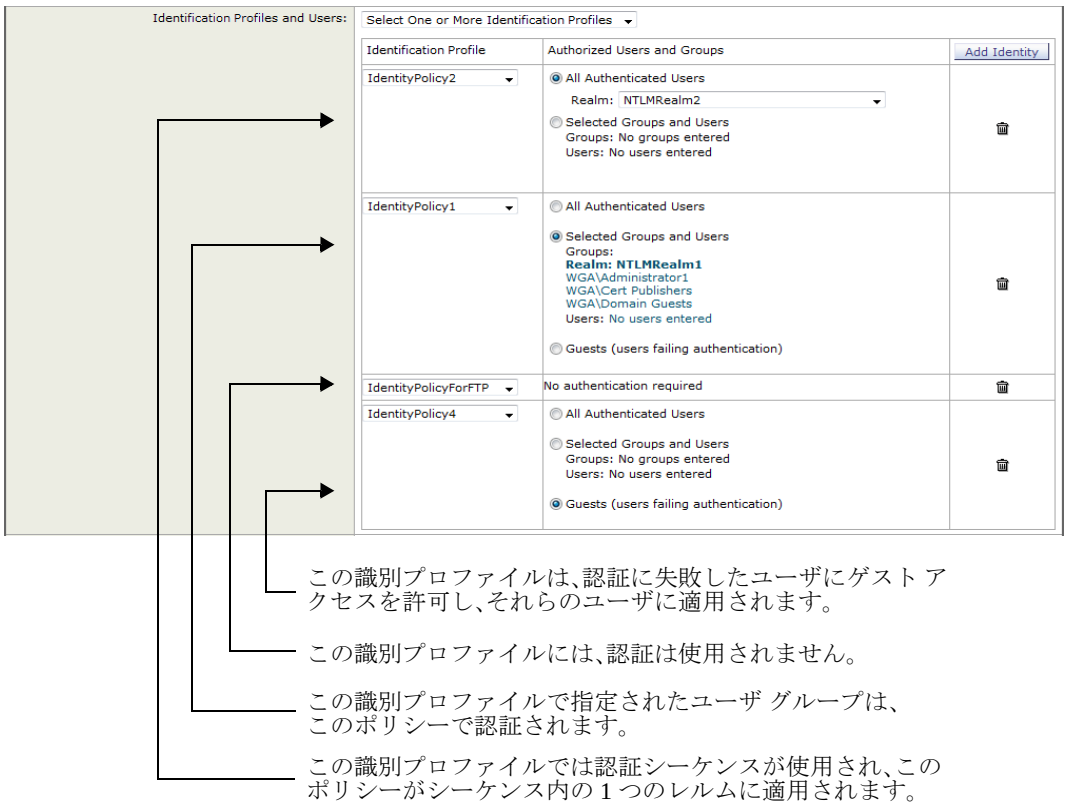
AsyncOS はすべてのトランザクションに識別プロファイルを割り当てます。

- カスタム識別プロファイル:AsyncOS は、そのアイデンティティの条件に基づいてカスタム プロファイルを割り当てます。
- グローバル識別プロファイル:AsyncOS は、カスタム プロファイルの条件を満たさないトランザクションに グローバル プロファイルを割り当てます。デフォルトでは、グローバル プロファイルには認証が必要ありません。

AsyncOS は最初から順番に識別プロファイルを処理します。グローバル プロファイルは最後のプロファイルです。

識別プロファイルには 1 つの条件だけを含めることができます。複数の条件を含む識別プロファイルはすべての条件を満たす必要があります。

1 つのポリシーによって複数の識別プロファイルを要求できます。



ユーザおよびクライアント ソフトウェアの分類:ベスト プラクティス

- 一般的な識別プロファイルを少数作成して、すべてのユーザまたは少数の大きなユーザ グループに適用します。より詳細に管理する場合は、プロファイルではなくポリシーを使用します。
- 一意の条件で識別プロファイルを作成します。
- 透過 モードで展開する場合は、認証をサポートしていないサイトの識別プロファイルを作成します。認証のバイパス (5-32 ページ) を参照してください。

識別プロファイルの条件

これらのトランザクションの特性は、以下の識別プロファイルの定義に使用できます。

オプション	説明
Subnet	クライアント サブネットは、ポリシーのサブネット リストに一致している必要があります。
プロトコル	トランザクションで使用されるプロトコル（HTTP、HTTPS、SOCKS、またはネイティブ FTP）
[ポート（Port）]	要求のプロキシ ポートは、識別プロファイルのポート リストに記載されている必要があります（リストに記載がある場合）。明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。
ユーザ エージェント（User Agent）	要求を行うユーザ エージェント（クライアント アプリケーション）は、識別プロファイルのユーザ エージェント リストに記載されている必要があります（リストに記載がある場合）。一部のユーザ エージェントは認証を処理できないため、認証を必要としないプロファイルを作成する必要があります。ユーザ エージェントには、アップデータやブラウザ（Internet Explorer、Mozilla Firefox など）などのプログラムが含まれています。
URL カテゴリ（URL Category）	要求 URL の URL カテゴリは、識別プロファイルの URL カテゴリ リストに記載されている必要があります（リストに記載がある場合）。
認証要件（Authentication requirements）	識別プロファイルが認証を必要とする場合は、クライアントの認証クレデンシャルが識別プロファイルの認証要件と一致する必要があります。

ユーザおよびクライアント ソフトウェアの分類

はじめる前に

- 認証レルムを作成します。Active Directory 認証レルムの作成（NTLMSSP および基本）（5-15 ページ）または LDAP 認証レルムの作成（5-17 ページ）を参照してください。
- 識別プロファイルへの変更を確定するときに、エンド ユーザを再認証する必要があります。
- クラウド コネクタ モードの場合は、追加の識別プロファイル オプション（マシン ID）を使用できます。ポリシーの適用に対するマシンの識別（3-8 ページ）を参照してください。
- （任意）認証シーケンスを作成します。認証シーケンスの作成（5-28 ページ）を参照してください。
- （任意）識別プロファイルにモバイル ユーザを含める場合は、セキュア モビリティをイネーブルにします。
- （任意）認証サロゲートについて理解しておきます。識別済みユーザの追跡（5-35 ページ）を参照してください。

手順 1　[Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

手順 2　[プロファイルの追加（Add Profile）] をクリックしてプロファイルを追加します。

手順 3　[識別プロファイルの有効化（Enable Identification Profile）] チェックボックスを使用して、このプロファイルをイネーブルにするか、プロファイルを削除せずにただちにディセーブルにします。

手順 4　[名前（Name）] に一意のプロファイル名を割り当てます。

手順 5　[説明（Description）] は任意です。

手順 6　[上に挿入（Insert Above）] フィールドのドロップダウン リストで、このプロファイルを配置するポリシー テーブル内の位置を選択します。

（注）　認証を必要とする最初の識別プロファイルの上に、認証を必要としない識別プロファイルを配置します。

手順 7　[ユーザ識別方式（User Identification Method）] セクションで、識別方式を選択して関連パラメータを指定します。表示されるオプションは、選択した方法によって異なります。

3 種類の方式（認証/識別から除外、認証済みユーザ）と、ユーザを透過的に識別する 3 種類の方法（ISE、ASA（AnyConnect セキュア モビリティ経由）、適切に設定された認証レルム）があります。後者には Active Directory レルム、または Novell eDirectory として設定された LDAP レルムのいずれかが含まれます。

a.　[ユーザ識別方式（User Identification Method）] ドロップダウン リストから識別方式を選択します。

オプション	説明
認証/識別を免除（Exempt from authentication/ identification）	ユーザは基本的に IP アドレスによって識別されます。追加のパラメータは必要ありません。
認証済みユーザ（Authenticate users）	ユーザは入力した認証クレデンシャルによって識別されます。
ISE によってユーザを透過的に識別（Transparently identify users with ISE）	ISE サービスがイネーブルの場合に使用できます（[ネットワーク（Network）] > [Identity Services Engine]）。これらのトランザクションの場合、ユーザ名および関連するセキュリティ グループ タグは Identity Services Engine から取得されます。詳細については、ISE サービスを認証および統合するためのタスク（8-4 ページ）を参照してください。
ASA によってユーザを透過的に識別（Transparently identify users with ASA）	ユーザは、Cisco 適応型セキュリティ アプライアンスから受信した現在の IP アドレス対ユーザ名のマッピングによって識別されます（リモート ユーザのみ）。このオプションは、セキュア モビリティがイネーブルになっており、ASA と統合されている場合に表示されます。ユーザ名は ASA から取得され、関連ディレクトリ グループは指定された認証レルムまたはシーケンスから取得されます。
認証レルムによってユーザを透過的に識別（Transparently identify users with authentication realm）	このオプションは、1 つ以上の認証レルムが透過的識別をサポートするように定義されている場合に使用できます。

（注）　少なくとも 1 つの識別プロファイルに認証または透過的識別が設定されている場合、ポリシー テーブルでは、ユーザ名、ディレクトリ グループ、セキュリティ グループ タグによるポリシー メンバーシップの定義がサポートされます。

b. 選択した方式に適したパラメータを指定します。この表に示したすべてのセクションが選択ごとに表示されるわけではありません。

認証レルムまたはゲスト特権へのフォールバック（Fallback to Authentication Realm or Guest Privileges）	ユーザ認証を ISE から取得できない場合: • [ゲスト権限をサポート（Support Guest Privileges）]: トランザクションは続行を許可され、すべての識別プロファイルのゲストユーザと後続のポリシーを照合します。 • [トランザクションをブロック（Block Transactions）]: ISE で識別できないユーザにインターネット アクセスを許可しません。 • [ゲスト特権をサポート（Support Guest privileges）]: 無効なクレデンシャルにより認証に失敗したユーザにゲスト アクセスを許可する場合、このチェックボックスをオンにします。
認証レルム（Authentication Realm）	[レルムまたはシーケンスを選択（Select a Realm or Sequence）]: 定義済みの認証レルムまたはシーケンスを選択します。 [スキームの選択（Select a Scheme）]: 認証スキームを選択します。 • [Kerberos]: クライアントは Kerberos チケットによって透過的に認証されます。 • [基本（Basic）]: クライアントは常にユーザにクレデンシャルを要求します。ユーザがクレデンシャルを入力すると、通常は、入力したクレデンシャルを保存するかどうかを指定するチェックボックスがブラウザに表示されます。ユーザがブラウザを開くたびに、クライアントはクレデンシャルの入力を要求するか、または以前に保存したクレデンシャルを再送信します。 クレデンシャルは、保護されていないクリア テキスト（Base64）として送信されます。クライアントと Web セキュリティ アプライアンス間でのパケット キャプチャにより、ユーザ名やパスフレーズが開示される可能性があります。 • [NTLMSSP]: クライアントは、Windows のログイン クレデンシャルを使用して透過的に認証します。ユーザはクレデンシャルの入力を求められません。 ただし、以下の場合、クライアントはユーザにクレデンシャルの入力を求めます。 – Windows クレデンシャルによる認証が失敗した。 – ブラウザのセキュリティ設定が原因で、クライアントが Web セキュリティ アプライアンスを信頼しない。 クレデンシャルは、3 ウェイ ハンドシェイク（ダイジェスト形式の認証）により安全に送信されます。パスフレーズが接続を介して送信されることはありません。 • [ゲスト特権をサポート（Support Guest privileges）]: 無効なクレデンシャルにより認証に失敗したユーザにゲスト アクセスを許可する場合、このチェックボックスをオンにします。
グループ認証のレルム（Realm for Group Authentication）	• [レルムまたはシーケンスを選択（Select a Realm or Sequence）]: 定義済みの認証レルムまたはシーケンスを選択します。

認証サロゲート（Authentication Surrogates）	認証の成功後にトランザクションをユーザに関連付ける方法を指定します（オプションは Web プロキシの展開モードにより異なります）。 • [IP アドレス（IP Address）]：Web プロキシは、特定の IP アドレスの認証済みユーザを追跡します。透過的ユーザ識別の場合は、このオプションを選択します。 • [永続的なクッキー（Persistent Cookie）]：Web プロキシは、アプリケーションごとに各ユーザ用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザを追跡します。アプリケーションを終了してもクッキーは削除されません。 • [セッション クッキー（Session Cookie）]：Web プロキシは、アプリケーションごとに各ドメインの各ユーザ用に永続的クッキーを生成することにより、特定のアプリケーション上の認証済みユーザを追跡します。（ただし、ユーザが同じアプリケーションの同じドメインに対して異なるクレデンシャルを指定すると、クッキーは上書きされます）。アプリケーションを終了するとクッキーは削除されます。 • [サロゲートなし（No Surrogate）]：Web プロキシは、サロゲートを使用してクレデンシャルをキャッシュせず、新しい TCP 接続ごとに認証済みユーザを追跡します。このオプションを選択すると、Web インターフェイスは適用されくなったその他の設定をディセーブルにします。このオプションは、明示的な転送モードに設定し、[ネットワーク（Network）] > [認証（Authentication）] ページでクレデンシャルの暗号化をディセーブルにしたときにのみ使用できます。 • [明示的フォワード要求に同じサロゲート設定を適用（Apply same surrogate settings to explicit forward requests）]：透過的要求に使用するサロゲートを明示的要求に適用する場合にオンにします（クレデンシャルの暗号化が自動的にイネーブルになります。）このオプションは、Web プロキシがトランスペアレントモードで展開されている場合にのみ表示されます。 **（注）** [グローバル認証設定（Global Authentication Settings）] で、すべての要求に対する認証サロゲートのタイムアウト値を定義できます。

手順 8　[メンバーシップの定義（Membership Definition）] セクションで、選択した識別方式に適したメンバーシップ パラメータを指定します。以下の表に示すオプションは、すべてのユーザ識別方式で使用できるわけではありません。

メンバーシップの定義	
ユーザの場所別メンバーの定義（Define Members by User Location）	この識別プロファイルを次に対して適用するように設定します：[ローカルユーザのみ（Local Users Only）]、[リモートユーザのみ（Remote Users Only）]、または [両方（Both）]。ここでの選択は、この識別プロファイルで使用可能な認証設定に影響します。
サブネット別メンバの定義（Define Members by Subnet）	この識別プロファイルを適用するアドレスを入力します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。 **（注）** 何も入力しない場合は、すべての IP アドレスにこの識別プロファイルが適用されます。

プロトコル別メンバの定義（Define Members by Protocol）	この識別プロファイルを適用するプロトコルを選択します。適用するすべてのプロトコルを選択してください。 • [HTTP/HTTPS]：FTP over HTTP、および 基礎のプロトコルとして HTTP または HTTPS を使用するすべての要求に適用されます。基礎のプロトコルには、FTP over HTTP、および HTTP CONNECT を使用してトンネリングされるその他のプロトコルも含まれます。 • [ネイティブ FTP（Native FTP）]：ネイティブ FTP 要求にのみ適用されます。 • [SOCKS]：SOCKS ポリシーにのみ適用されます。
マシン ID によるメンバーの定義（Define Members by Machine ID）	• [このポリシーではマシン ID を使用しないでください（Do Not Use Machine ID in This Policy）]：ユーザはマシン ID によって識別されません。 • [マシン ID をベースにしたユーザ認証ポリシーの定義（Define User Authentication Policy Based on Machine ID）]：ユーザは基本的にマシン ID によって識別されます。 [マシン グループ（Machine Groups）] 領域をクリックして、[認証済みマシン グループ（Authorized Machine Groups）] ページを表示します。 追加する各グループごとに、[ディレクトリ検索（Directory Search）] フィールドに追加するグループの名前を入力し、[追加（Add）] をクリックします。リストからグループを削除するには、グループを選択して [削除（Remove）] をクリックします。 [完了（Done）] をクリックして前のページに戻ります。 [マシン ID（Machine IDs）] 領域をクリックして、[認証済みマシン（Authorized Machines）] ページを表示します。 [認証済みマシン（Authorized Machines）] で、マシン ID を入力してポリシーに関連付け、[完了（Done）] をクリックします。 **（注）** マシン ID による認証はコネクタ モードのみでサポートされ、Active Directory を必要とします。

詳細設定（Advanced）	このセクションを展開して、追加のメンバーシップ要件を定義します。 • [プロキシ ポート（Proxy Ports）]：Web プロキシへのアクセスに使用する 1 つ以上のプロキシ ポートを指定します。ポート番号をカンマで区切って入力します。明示的な転送接続の場合、プロキシ ポートはブラウザで設定されます。 透過接続の場合は、宛先ポートと同じです。 ポート別の ID の定義は、アプライアンスが明示的な転送モードで展開されている場合、またはクライアントがアプライアンスに明示的に要求を転送する場合に最もよく機能します。クライアント要求が透過的にアプライアンスにリダイレクトされる場合は、ポート別の ID の定義によって一部の要求が拒否されることがあります。 • [URL カテゴリ（URL Categories）]：ユーザ定義または定義済みの URL カテゴリを選択します。デフォルトでは、両方のメンバーシップが除外されます。つまり、[追加（Add）] 列で選択されていない限り、Web プロキシはすべてのカテゴリを無視します。 URL カテゴリによってメンバーシップを定義する必要がある場合、そのカテゴリに対する認証要求から除外する必要のあるときは ID グループにのみ定義します。 • [ユーザ エージェント（User Agents）]：クライアント要求で見つかったユーザ エージェントごとにポリシー グループ メンバーシップを定義します。一般的に定義されているエージェントを選択するか、正規表現を使用して独自のブラウザを定義できます。 また、これらのユーザ エージェントの指定を含めるか除外するかも指定します。つまり、メンバーシップの定義に選択したユーザ エージェントのみを含めるか、選択したユーザ エージェントを明確に除外するかどうかを指定します。

手順 9　変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

関連項目

- エンドユーザ クレデンシャルの取得の概要（5-1 ページ）
- ポリシー タスクによる Web 要求の管理：概要（10-3 ページ）

ID の有効化/無効化

はじめる前に

- 識別プロファイルをディセーブルにすると、関連するポリシーからその識別プロファイルが削除されるので注意してください。
- 識別プロファイルを再度イネーブルにしても、その識別プロファイルはポリシーに再び関連付けられません。

手順 1　[Web セキュリティ マネージャ（Web Security Manager）] > [識別プロファイル（Identification Profiles）] を選択します。

手順 2　識別プロファイル テーブルのプロファイルをクリックして、そのプロファイルの[識別プロファイル（Identification Profile）] ページを開きます。

手順 3　[クライアント/ユーザ識別プロファイルの設定(Client/User Identification Profile Settings)] の真下にある [識別プロファイルの有効化(Enable dentification IProfile)] をオンまたはオフにします。

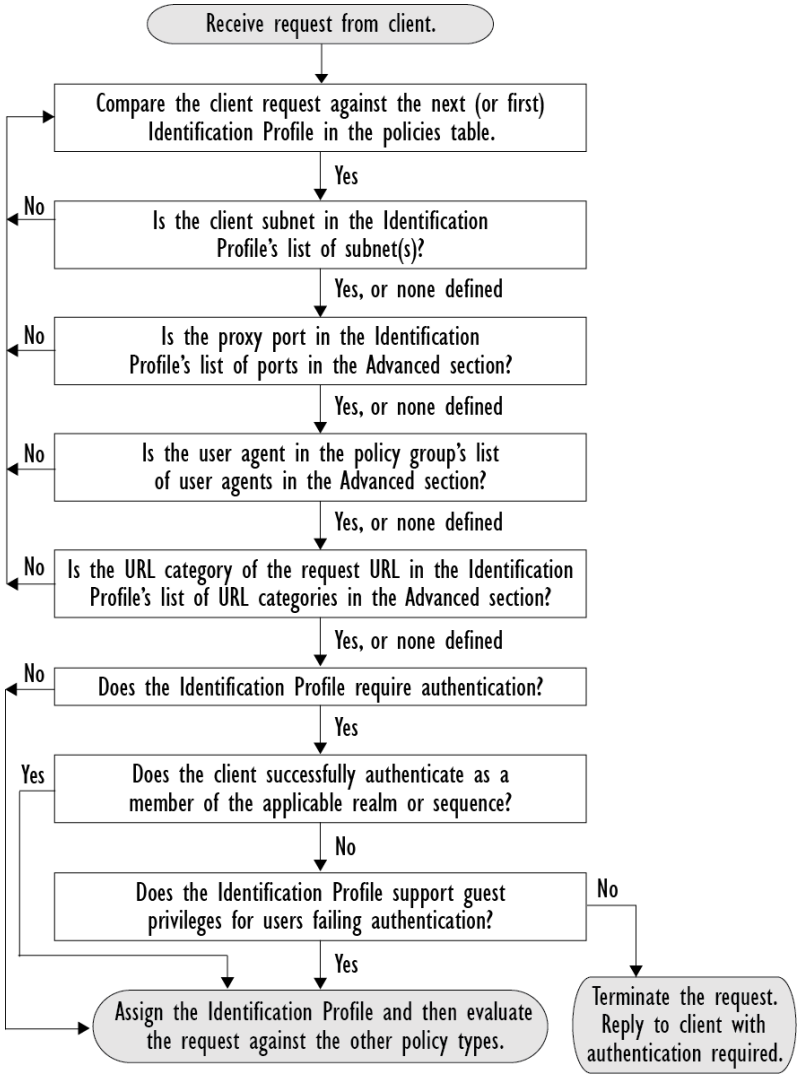
手順 4　変更を送信して確定します([送信(Submit)] と [変更を確定(Commit Changes)])。

識別プロファイルと認証

次の図に、識別プロファイルが次を使用するように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

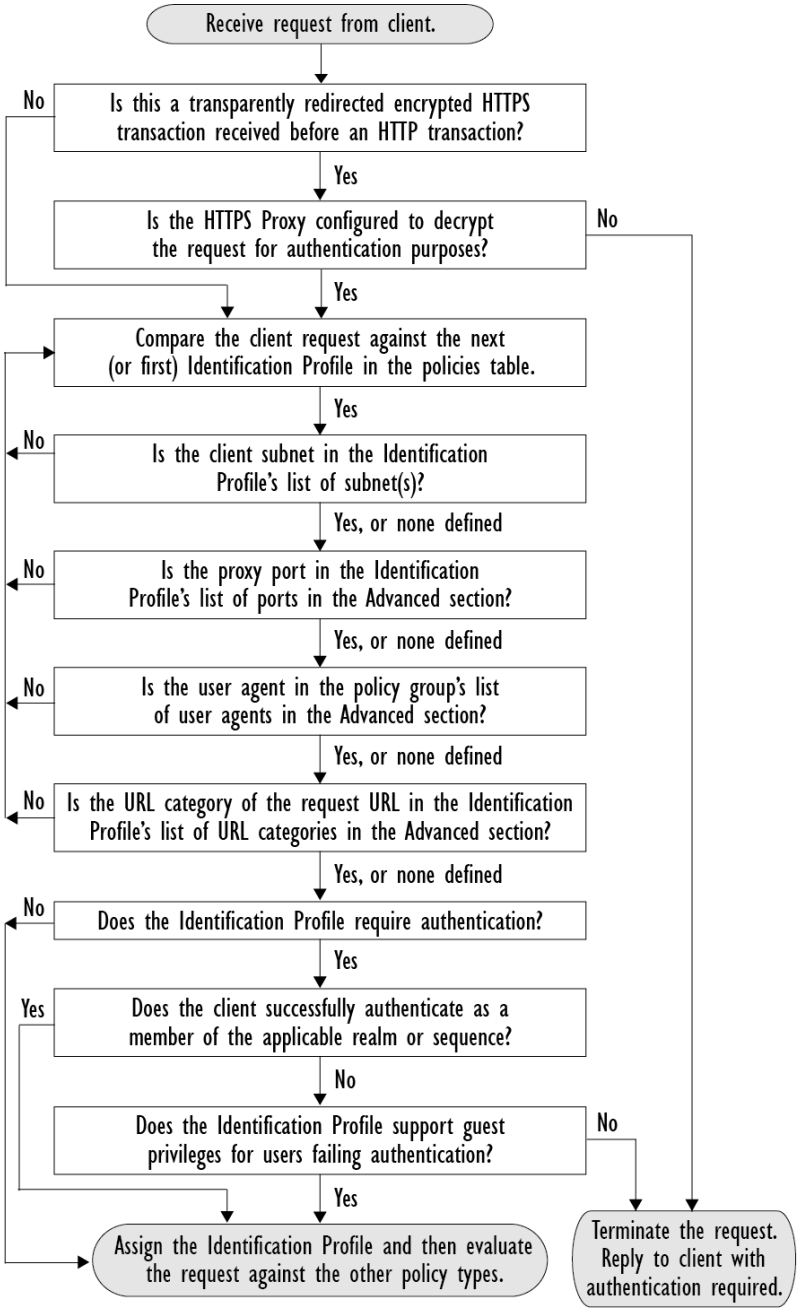
- 認証サロゲートなし
- 認証サロゲートとしての IP アドレス
- 透過的要求を使用する認証サロゲートとしてのクッキー
- 明示的要求を使用する認証サロゲートとしてのクッキー(クレデンシャルの暗号化がイネーブルになっている場合)

図 6-1　識別プロファイルと認証プロセス:サロゲートおよびIP ベースのサロゲートなし



次の図に、識別プロファイルが認証サロゲートとして Cookie を使用し、クレデンシャルの暗号化を有効にして、要求が明示的に転送されるように設定されているときに、Web プロキシがクライアント要求を識別プロファイルに対して評価する方法を示します。

図 6-2　　識別プロファイルと認証プロセス:Cookie ベースのサロゲート



識別プロファイルのトラブルシューティング