


# ネットワーク アドミッション コントロール フレームワーク 導入ガイド

はじめに.....	5
ネットワーク アドミッション コントロールの概要 .....	5
アドミッション コントロールの目的.....	5
パートナーシップ .....	5
Cisco NAC : アーキテクチャとシステム コンポーネント .....	6
アーキテクチャの概要.....	6
NAC の実施 : .....	6
決定と修復 : .....	7
NAC システム コンポーネント.....	10
CISCO TRUST AGENT (CTA) .....	10
CTA サブリカント .....	11
ポストチャ プラグイン.....	11
エージェントレス ホスト.....	12
ネットワーク アクセス デバイス (NAD) .....	13
CISCO SECURE ACCESS CONTROL SERVER (ACS) .....	13
修復 (RemEdiation) サーバ.....	14
ポストチャ検証 (Posture Validation) サーバ.....	14
監査 (Audit) サーバ .....	14
レポートイング.....	15
プロトコル.....	15
EAP.....	15
EAP-FAST.....	16
HCAP.....	16
GAME .....	17
NAC アセスメント方式.....	17
NAC L3 IP.....	17
NAC L2 IP.....	18
NAC L2 802.1x.....	20
エージェントレス ホスト.....	21
静的な例外 (ホワイトリスト) .....	21
ダイナミックな監査.....	21
NAC ポリシー戦略.....	22
ネットワーク アドミッション ポリシーの設計 .....	22
ポリシーの作成と要件.....	22
ポリシーの定義 .....	23
クレデンシャル .....	24
アイデンティティ クレデンシャル.....	24
汎用デバイス クレデンシャル.....	25
Microsoft マシン クレデンシャル.....	25
ユーザ クレデンシャル .....	25
ポストチャ クレデンシャル .....	25
アイデンティティ対ポストチャ.....	26
ネットワークのセグメントと分離.....	27
セグメント .....	27
分離.....	27
デフォルト ネットワーク アクセス.....	28

NAC Agentless Host (NAH; NAC エージェントレス ホスト) オプション.....	28
静的な NAD ホワイトリスト.....	28
ACS での集中管理型のホワイトリスト.....	29
ダイナミックなホストの監査.....	29
パッチ管理の統合.....	29
プロセス.....	29
検疫時のパッチ適用.....	30
NAC のスケーラビリティとアベイラビリティ.....	30
スケーラビリティ.....	30
ユーザとホスト.....	31
Cisco Secure Access Control Server (ACS).....	31
プロトコル許可レート.....	31
NAC タイマー.....	31
保留期間.....	32
その他のスケーラビリティの制限要素.....	32
スケーラビリティの計算.....	33
ロード バランシング.....	33
IOS RADIUS サーバ フェールオーバー.....	33
IOS RADIUS サーバのロード バランシング.....	34
Content Services Switch を使用した RADIUS サーバのロード バランシング.....	34
NAC 設計時の考慮事項.....	35
NAC アセスメント方式.....	35
NAC L3 IP.....	35
NAC L2 IP.....	37
NAC L2 802.1x.....	38
CTA と Windows のブート シーケンス.....	39
IEEE 802.1x と NAC L2 IP.....	42
NAC エージェントレス ホスト (NAH).....	43
NAC L2/L3 IP とエージェントレス ホスト.....	43
NAC L2 802.1x とエージェントレス ホスト.....	43
NAH のまとめ.....	45
NAC アセスメント方式の機能とトレードオフ.....	45
NAC 導入の比較.....	46
NAC ソリューションのコンポーネント.....	47
Cisco Trust Agent.....	47
NAD.....	48
Cisco IOS ルータ.....	48
Cisco VPN コンセントレータ.....	48
Cisco スイッチ.....	48
Cisco Secure ACS 4.0.....	49
パフォーマンスとスケーラビリティ.....	49
管理.....	49
その他.....	49
ディレクトリ サービス.....	49
サポートする認証プロトコル.....	50
ディレクトリのスケーラビリティ.....	50
まとめ.....	51



付録.....	52
略語.....	52
NAC アトリビュートのリファレンス.....	59
Attribute Namespace.....	59
アトリビュートのデータ型.....	59
アトリビュートのリファレンス.....	60
NAC の RADIUS アトリビュート.....	63
NAC 方式と RADIUS 要求アトリビュート.....	64

## はじめに

### ネットワーク アドミッション コントロールの概要

Network Admission Control (NAC ; ネットワーク アドミッション コントロール) は、シスコシステムズが主導する業界のイニシアチブを基盤に構築された一連のテクノロジーとソリューションです。NAC は、ネットワーク インフラストラクチャを活用して、ネットワーク コンピューティング リソースにアクセスしようとするすべてのデバイスにセキュリティ ポリシーへの適合を強制することにより、ウイルス、ワーム、スパイウェアなどの新しいセキュリティの脅威がもたらす損害を抑制します。お客様は NAC を利用することによって、エンドポイント デバイス (PC、サーバ、PDA など) のうち、信頼できるポリシー適合デバイスにはネットワーク アクセスを許可し、非適合デバイスについてはアクセスを制限できます。

NAC フレームワーク テクノロジーによって、インテリジェントなネットワーク インフラストラクチャと、アンチウイルスをはじめとするセキュリティおよび管理ソフトウェア ソリューションの 60 社を超える業界主要メーカーのソリューションが統合されます。

### アドミッション コントロールの目的

かつてユーザとデバイスは、ユーザが誰でデバイスが何かを基準に認証が行われ、その状態は認証されていませんでした。NAC は、健全なクライアント ワークステーションのみに完全なネットワーク アクセスを提供することを実現します。NAC は、アンチウイルス、パッチ管理、パーソナル ファイアウォール ソフトウェアと連動し、クライアントにネットワーク アクセスを許可する前に、クライアントの状態 (ポスチャ) のアセスメントを実施します。NAC によって、ネットワーク クライアントが最新のウイルス シグニチャとオペレーティング システム パッチを使用し、ウイルスに感染していないことを保証することができます。クライアントにアンチウイルス シグニチャまたはオペレーティング システムのアップデートが必要な場合、NAC はクライアントに所定のアップデートを実施するように指示します。クライアントのセキュリティが低下している場合や、ネットワーク内でウイルスのアウトブレイクが発生した場合は、NAC がクライアントを検疫ネットワーク セグメントに配置します。クライアントは、アップデート プロセスや必要な駆除処理を完了した後に再度検証され、健全なステータスと通常のネットワーク アクセスが与えられます。

### パートナーシップ

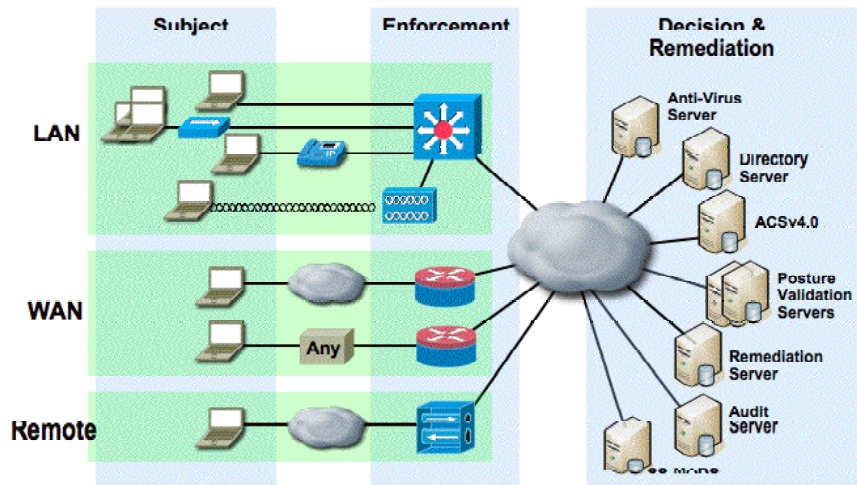
シスコでは、あらゆる問題に対応するために、アンチウイルス、パッチ管理、パーソナル ファイアウォール分野のエキスパートとのパートナーシップを通じて NAC ソリューションを拡張しています。主要ベンダはすべて NAC パートナー プログラムに参加していますので、お客様はこれまでのセキュリティ アプリケーションへの投資を保護することができます。NAC パートナーシップ プログラムの詳細については、シスコの Web サイト <http://www.cisco.com/jp/specialprog/nacprog/>を参照してください。

# CISCO NAC :アーキテクチャとシステム コンポーネント

## アーキテクチャの概要

Cisco NAC は、ホストの状態（ポスチャ）のアクセスメントを実施することにより、未許可または脆弱なエンドポイントからのネットワークへのアクセスを防止します。一般的なホストは、デスクトップ コンピュータ、ラップトップ、サーバですが、IP 電話、ネットワーク プリンタ、その他のネットワーク接続デバイスもホストとして使用できます。

図 1. NAC 導入シナリオ



Cisco NAC は、ネットワーク アクセス方式を問わずに実施できます。ネットワーク アクセスを試みるホストからポスチャ情報を収集し、ルータ、スイッチ、ワイヤレス アクセス ポイント、VPN コンセントレータを通じてアクセス ポリシーに適合させることができます。

Cisco NAC ポスチャ検証プロセスで使用される主なコンポーネントは次のとおりです。

### デバイス :

- **ホスト** — NAC を実施するネットワークにアクセスするマシン。
- **Posture Plugin (PP ; ポスチャ プラグイン)** — ホストに常駐するシスコまたはサードパーティ製の DLL。同一のデバイスに常駐するポスチャ エージェントにホストのポスチャ クレデンシャルを提供します。
- **Posture Agent (PA ; ポスチャ エージェント)** — ホスト上で 1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネットワークと通信する、ホスト上の仲介役として機能するホスト エージェント ソフトウェア。シスコのポスチャ エージェント製品は、Cisco Trust Agent (CTA) です。
- **修復 (Remediation) クライアント** — OS のパッチなど特定のクライアント ソフトウェアを更新するために修復サーバと連動する、修復管理ソリューションのコンポーネントの 1 つ。

### NAC の実施 :

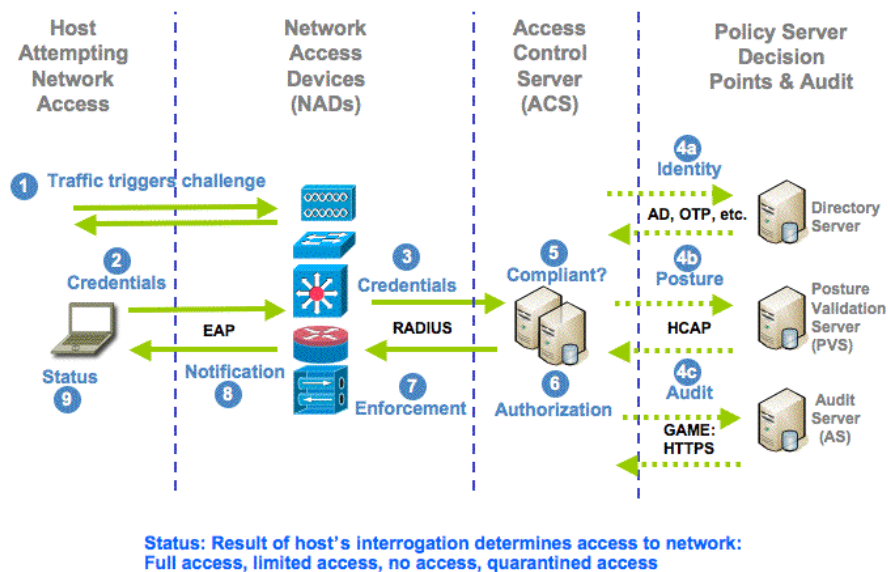
- **Network Access Device (NAD ; ネットワーク アクセス デバイス)** — NAC の実施ポイントとして機能するネットワーク デバイス。Cisco アクセス ルータ (800 - 7200) 、VPN ゲートウェイ (VPN 3000 シリーズ) 、Catalyst レイヤ 2 および レイヤ 3 スイッチ、ワイヤレス アクセス ポイントなどが含まれます。

## 決定と修復：

- **AAA サーバ** — Authentication, Authorization and Accounting (AAA ; 認証、許可、アカウントリング) サーバ。1 つまたは複数の認証や許可の決定を収集して単一のシステムの認証結果を決定し、NAD で NAC を実施するためにこの決定をネットワーク アクセス プロファイルにマッピングする、NAC の中心となるポリシー サーバ。Cisco Secure Access Control Server (ACS) は、NAC をサポートするシスコの AAA サーバ製品です。
- **ディレクトリ サーバ** — ユーザ、マシン、または両方の認証を行うための中央集中型のディレクトリ サーバ。ディレクトリ サービスには、Lightweight Directory Access Protocol (LDAP)、Microsoft Active Directory (AD)、Novell Directory Services (NDS)、One-time Token Password Servers (OTP) などがあります。
- **PVS** — ポスチャ検証 (Posture Validation) サーバ。NAC におけるアプリケーション別のポリシー決定ポイントとして機能し、1 つまたは複数のポスチャ プラグインから収集したポスチャ クレデンシャルと一連のポリシー ルールを照合して認証を実施します。アンチウイルス サーバ、セキュリティ アプリケーション サーバなどが PVS に該当します。
- **修復 (Remediation) サーバ** — ポリシーに非適合のホストを適合させるために使用する管理ソリューション。専用のパッチ管理アプリケーションのほか、ソフトウェアを配布する Web サイトのような簡略なものも修復サーバに該当します。ホストへのパッチの適用と修復を効率化するほどリスクは低くなります。
- **監査 (Audit) サーバ** — ホストに対して Vulnerability Assessment (VA ; 脆弱性アセスメント) を行い、ネットワーク アドミッションの前にホストの適合性のレベルやリスクを判定するサーバまたはソフトウェア

図 2 に、NAC アーキテクチャの主要なコンポーネントと、ネットワーク アクセスの許可または拒否に使用する許可プロセスの概要を示します。

図 2. NAC コンポーネントと許可プロセス



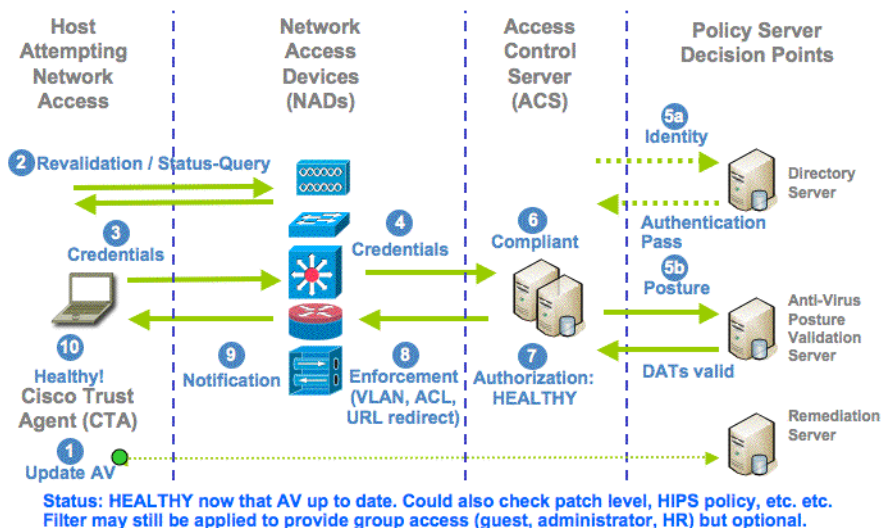
次に示す NAC 許可プロセスの手順の番号は、図 2 の数字に対応していますので参照してください。

1. NAC 対応のネットワーク アクセス デバイスが、ネットワーク リソースへの接続または使用を試みるホストを検出すると、ポスチャ検証が開始されます。
2. NAD は、新しいエンドポイントを検出すると、AAA サーバ (ACS) とポスチャ エージェントとの間に通信パスを確立します。通信パスが確立されると、AAA サーバはエンドポイントに対して、1 つまたは複数のポスチャ プラグインのポスチャ クレデンシャルを要求します。

3. ホストは、ホスト上の NAC 対応ソフトウェアコンポーネントが利用可能なポスチャ プラグインから収集したポスチャ クレデンシャルで要求に応答します。
4. AAA サーバは、ローカルでポスチャ情報を検証するか、外部のポスチャ検証サーバに一部の決定を委託します。
5. AAA サーバは、すべての代理サーバから各ポスチャの結果（ポスチャ トークン）を収集し、ホストの総合的な適合性（システム ポスチャ トークン）を決定します。
6. タイマーの RADIUS アトリビュート、VLAN 割り当て、Downloadable ACL（Access Control List）で構成されるネットワーク アクセス プロファイルの認可のために、アイデンティティ検証結果とシステム ポスチャ トークンがマッピングされます。
7. これらの RADIUS アトリビュートが NAD に送信され、ホストで NAC が実施されます。
8. 各プラグインにそれぞれのアプリケーションのポスチャとシステム全体のポスチャを通知するポスチャ ステータスが、ホストの CTA に送信されます。
9. CTA の通知ダイアログを使用して、ホストのユーザにメッセージを送信し、ネットワークにおけるホストの状態を通知できます（オプション）。

図 3 に、主要な NAC コンポーネントと、ホストを検疫（Quarantine）ステートから健全（Healthy）ステートに移行するために使用する修復プロセスの概要を示します。

図 3. NAC コンポーネントと、Quarantine から Healthy への修復プロセス



次に示す NAC 修復プロセスの手順の番号は、図 3 の数字に対応していますので参照してください。

1. **Quarantine** ステートに置かれたホストは、**Antivirus (AV)** ; アンチウイルス) ソフトウェアのアップデート用のサードパーティ製の修復サーバにリダイレクトされます。
2. **Cisco Trust Agent** がポストチャ プラグインに **AV** ソフトウェアの情報をポーリングし、変更があったことを確認すると、**NAD** から再検証が開始されます。**NAD** は、**AAA** サーバ (**ACS**) とポストチャ エージェントとの間に通信パスを確立します。通信パスが確立されると、**AAA** サーバはエンドポイントに対して、1 つまたは複数のポストチャ プラグインのポストチャ クレデンシャルを要求します。
3. ホストは、ホスト上の **NAC** 対応ソフトウェアコンポーネントが利用可能なポストチャ プラグインから収集したポストチャ クレデンシャルで要求に応答します。
4. **AAA** サーバは、ローカルでポストチャ情報を検証するか、外部のポストチャ検証サーバに一部の決定を委託します。
5. **AAA** サーバは、すべての代理サーバから各ポストチャ結果 (ポストチャ トークン) を収集し、ホストの総合的な適合性 (システム ポストチャ トークン) を決定します。
6. タイマーの **RADIUS** アトリビュート、**VLAN** 割り当て、**Downloadable ACL** で構成されるネットワーク アクセス プロファイルの認可のために、アイデンティティ検証結果とシステム ポストチャ トークンがマッピングされます。
7. これらの **RADIUS** アトリビュートが **NAD** に送信され、ホストで **NAC** が実施されます。
8. 各プラグインにそれぞれのアプリケーションのポストチャとシステム全体のポストチャを通知するポストチャ ステータスが、ホストの **CTA** に送信されます。
9. **CTA** の通知ダイアログを使用して、ホストのユーザにメッセージを送信し、ネットワークにおけるホストの状態を通知できます (オプション)。
10. ホストの **AV** ソフトウェアが最新の状態で稼働します。**AV** ポストチャ検証サーバにより、この状態は検証済みです。その結果、ホストは **Quarantine** ステートから **Healthy** ステートに移行されます。

すべてのポストチャ決定ポイント (**AAA** サーバまたは **PVS**) は、ルールベースのポリシー エンジンを使用して 1 つまたは複数のホスト クレデンシャル セットを検証し、結果として 1 つまたは複数の **Application Posture Token (APT)** ; アプリケーションポストチャ トークン) を決定します。**APT** は、ホスト上の特定のベンダ アプリケーションの適合性チェックの結果を表します。その後、**AAA** サーバは代理 **PVS** および 独自のポリシー エンジンからすべての **APT** を収集し、ホストの総合的な適合性を表す単一の **System Posture Token (SPT)** ; システム ポストチャ トークン) を決定します。したがって、総合的な **SPT** を構成する **APT** のうち 1 つでも適合性チェックで適合性が認められない場合、その結果が総合的な **SPT** に反映されます。**APT**、**SPT** とも、予め定義されている次のトークンを使って表されます。

**Healthy** —ホストはポリシーに適合しています。ホストからネットワークへのアクセスは制限されません。

**Checkup** —ホストはポリシーの適合範囲内ですが、入手可能なアップデートがあります。このステートは、ホストをプロアクティブに **Healthy State** に修復するために使用されます。

**Transition** —ホストのポストチャ検証が行われています。ホストにはポストチャ検証が完了するまで暫定的なアクセスが提供されます。すべての **NAC** 対応アプリケーションが稼働していない可能性があるホスト ブート プロセス中、またはホストからポストチャ情報を入手していない監査プロセス中に使用されるステートです。

**Quarantine** —ホストはポリシーに適合していません。このホストのネットワーク アクセスは修復のための検疫ネットワークのみに制限されて修復が行われます。このホストはアクティブな脅威ではありませんが、既知の攻撃やウイルス感染に脆弱です。

**Infected** —ホストは他のホストにとってアクティブな脅威です。このホストからのネットワーク アクセスは厳格に制限するか、完全に拒否する必要があります。

**Unknown** —ホストのポストチャを特定できません。正確なポストチャを特定できるまで、ホストを検疫し、監査または修復を行います。

アイデンティティ認証およびポストチャ検証は、ホストがネットワークへのアクセスを要求したときに発生します。ネットワークアクセス デバイス (NAD) は、レイヤ 2 または レイヤ 3 トランスポート方式を通じてホストからポストチャ クレデンシャルを取得します。どの程度のネットワーク アクセスがホストに許可されるかは、ホストのアイデンティティおよび/またはポストチャポリシー ルールへの適合性のレベルによって決定されます。通常これらのポストチャ クレデンシャルは、ホストのオペレーティング システム、およびアンチウイルス、ファイアウォール、侵入検知システムなどのアプリケーションの状態を示します。たとえばネットワーク管理者は、「有効なスキャン エンジン バージョン Y.Y.Y、およびシグニチャ ファイル バージョン Z.Z.Z を使用するベンダ XXX のアンチウイルス アプリケーションが必要、この条件を満たさない場合は検疫ロールを割り当て、ホストからのネットワーク アクセスをアンチウイルス サーバのみに制限」といったアンチウイルス ポリシーを NAC に設定します。

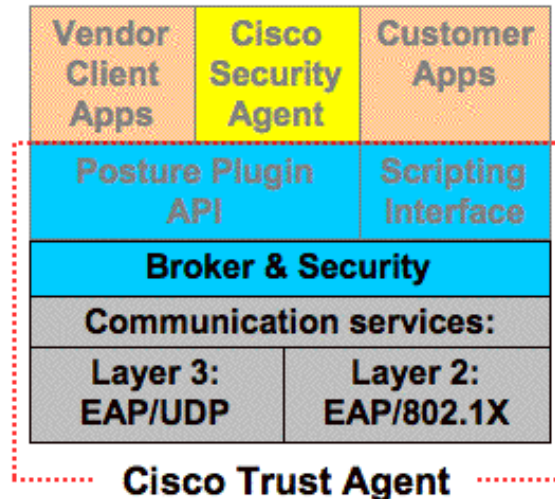
## NAC システム コンポーネント

### CISCO TRUST AGENT (CTA)

ポストチャ エージェント (PA) は、すべてのポストチャ プラグインからポストチャ クレデンシャルを収集してネットワークと通信する、ホスト上の単一のコンタクト ポイントとして機能します。このモジュールは、これらのポストチャ クレデンシャルを交換するために、ネットワークとの信頼関係も提供します。Cisco Trust Agent (CTA) は、NAC のためのシスコのポストチャ エージェント製品です。

CTA は、ベンダ (例 : McAfee、Symantec、Trend Micro、Cisco) およびアプリケーション タイプ (例 : PA、OS、AV、FW) 別に登録されたポストチャ プラグインのレコードを保持します。CTA は、ポストチャ プラグインとネットワークとの間でポストチャ要求とポストチャ通知の多重化/逆多重化を行います。また CTA は、ポストチャ プラグインにポストチャ変更があったかどうかを判断し、さまざまな EAP トランスポートで利用可能なメカニズムを使用して NAD に通知します。CTA は、ネットワークとポストチャプラグインの間でやりとりするクレデンシャルと通知の解釈は行いません。CTA が行う処理は、プラグインとネットワーク間でやりとりする要求と応答に必要な多重化と逆多重化のみです。Cisco Trust Agent のアーキテクチャを次の図に示します。

図 4. Cisco Trust Agent のアーキテクチャ



ポスチャ エージェント は、自身のポスチャ プラグインを装備し、自身のクレデンシャル (PA 名とバージョンなど) と、ホストに関する最小限のクレデンシャル セット (ホストのオペレーティング システム情報など) を提供します。また通知要求をサポートし、ユーザに情報メッセージを表示します。

#### CTA サプリカント

CTA サプリカントは、NAC 対応 802.1x サプリカントです。NAC 対応とは、サプリカントが EAP-FAST プロトコルを使用して 802.1x トランスポート内でアイデンティティおよびポスチャ情報両方を伝送できることを意味します。つまりこのサプリカントは、ユーザとマシン アイデンティティだけでなく、マシンのポスチャ情報も提供できます。

現在、CTA サプリカントは有線インターフェイスをサポートしています。Cisco NAC でワイヤレスをサポートする必要がある場合は、Cisco NAC パートナーから有線とワイヤレス両方をサポートするサプリカントを入手できます。

#### ポスチャ プラグイン

ポスチャ プラグインは、ホストに常駐する DLL で、同一のデバイスに常駐するポスチャ エージェントにホストのポスチャ クレデンシャルを提供します。ポスチャ プラグインは、ベンダおよびアプリケーション タイプごとに 1 つ存在します。ポスチャ プラグインは CTA と各クライアント ソフトウェアの間のアダプタとして機能し、ポスチャ要求および応答で使用するポスチャ クレデンシャルを処理します。

ポスチャ プラグインが提供するポスチャ クレデンシャルの一部の例を示します。

- ソフトウェア名 — ソフトウェア製品名。
- ソフトウェア バージョン — ソフトウェア製品のバージョン (例 : 4.2.0.75) 。
- ソフトウェア リリース日 — ソフトウェアの発行日。
- ソフトウェアのイネーブル/ディセーブル状況 — ソフトウェアが現在ホスト上で稼働中かどうか。
- 設定パラメータ — 標準またはベンダ固有のアプリケーション設定を含みます。

- マシン ポスチャ ステート — マシン ポスチャ ステートは、起動しているマシンのステータスに関する情報を ACS に通知するために CTA が提供します。Booting（起動中）、Running（稼動中）、または Logged in（ログイン中）の 3 つのステータスのうち、1 つがレポートされます（Windows プラットフォーム）。

CTA は、ポスチャ エージェントから次のようなポスチャ クレデンシヤルと通知を受信します。

- Application Posture Token (APT; アプリケーション ポスチャ トークン) — AAA サーバによるポスチャ検証の結果決定された特定のアプリケーション、エージェント、またはソフトウェアコンポーネントのポスチャ
- System Posture Token (SPT; システム ポスチャ トークン) — すべてのクレデンシヤル (PA、OS、AV、FW、IDS、その他の対象アプリケーション) の検証結果から決定されたホスト全体としてのポスチャ
- (オプション) 修復に必要な情報 (実行するアクション、修復で使用するサーバの URL)

ポスチャ プラグインは、ポスチャ エージェントからの最後のポスチャ クレデンシヤル要求後に発生したポスチャ変更をポスチャ エージェントに通知する機能も装備しています。

**注:** ポスチャ プラグインはレジストリまたはファイルを直接スキャンする可能性があるため、クライアント ソフトウェアとポスチャ プラグインとの間のプロセス内通信メカニズムは完全に任意で、ベンダによって異なります。

### エージェントレス ホスト

イーサネットはネットワーク接続の標準として幅広く使用されていますが、イーサネット対応デバイスの多くは、ネイティブ プロトコル スタックにおいて IEEE 802.1x サブリカント機能をサポートしていません。このようなホストは、エージェントレスとみなされます。これらのホストは、ネイティブな 802.1x サブリカントを装備していないためアドミッションに必要なネットワークからのチャレンジに応答できません。

現在、このエージェントレス カテゴリに分類されるネットワーク接続デバイスのクラスは数多く存在します。デスクトップやサーバ コンピュータなどのデバイスのクラスもありますが、比較的大きいクラスは、プリンタ、コピー機、カメラ、電話、センサー、その他の多くの専用アプライアンスを含むクラスです。これらのデバイスは、次のような理由のために IEEE 802.1x サブリカントをサポートしていません。

- ホストのオペレーティング システムのプロトコル スタックが Cisco Trust Agent (CTA) または 802.1x サブリカントにサポートされていない。
- アプライアンスに十分なストレージ、メモリ、または CPU が装備されていない。
- サブリカント機能は利用できるが、デフォルトでイネーブルにされていない。
- レイヤ 3 (L3) ネットワーク認証チャレンジをブロックするパーソナル ファイアウォールがホストでイネーブルにされている。

プロトコル スタックでこれらのホストからアイデンティティまたはポスチャ クレデンシヤルを収集するメカニズムがなければ、NAC をグローバルに管理できないため、導入に影響が及びます。この影響を抑えるために、NAC は IP または MAC アドレスの静的なリストに基づいたホワイトリストまたはブラックリストを使用する、エージェントレス ホストの複数の処理方法を提供します。また、NAC ソリューションに導入された監査サーバ コンポーネントを使用すると、静的なリストを管理せずに、脆弱性アセスメント手法を使用してホストをダイナミックに検証できます。

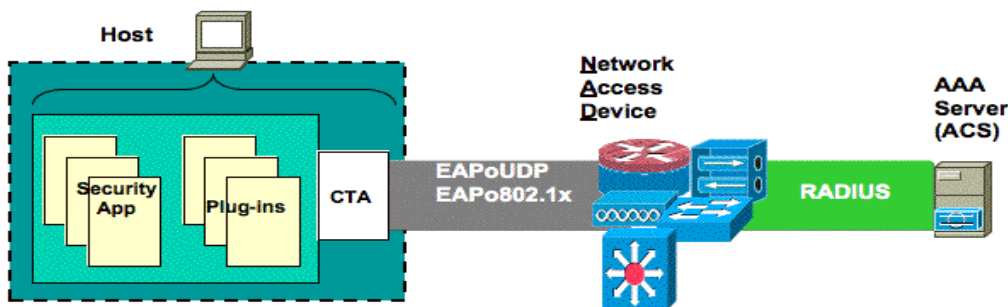
エージェントレス ホストの処理メカニズムについては、本書の後半でさらに詳しく説明します。各方法の設定についての詳しい情報は、『ネットワーク アドミッション コントロール コンフィギュレーション ガイド』を参照してください。

## ネットワーク アクセス デバイス (NAD)

ネットワーク アクセス デバイス (NAD) は、AAA サーバから RADIUS アトリビュートによって送信された許可ポリシーに基づいて、ネットワーク アクセスを制御します。

NAD は、レイヤ 2 (L2) またはレイヤ 3 (L3) ポート、またはインターフェイス上にホストを検出すると、AAA サーバへの許可プロセス開始を要求する前に、ホスト上の PA との間に通信の確立を試みます。NAD と PA 間の通信は、NAD に応じて L2 メカニズム (802.1x) または L3 トランスポート (EAPoUDP) を介して行われます。PA の応答は、NAD によって AAA サーバに転送され、アクセス要求が開始されます。ホストと AAA サーバとの信頼が確立され、セキュアなトンネルで通信を開始すると、PA はアイデンティティおよびポストチャ クレデンシャルで応答します。NAD は、このプロセスでホストと AAA サーバとの間で交換されるすべてのメッセージを中継するエージェントとしての役割を果たします。AAA サーバは、許可を完了すると、NAD にネットワーク アクセス プロファイルを送信し、ホストで NAC が実施されます。

図 5. ホスト、NAD、AAA サーバの通信



ポストチャ検証終了後、次のポストチャ検証までの間に NAD は定期的にステータス クエリーを発行し、NAD に接続する各ホストが最初にポストチャ検証されたホストと同じデバイスかどうか、(EAPoUDP の場合は) ホストのポストチャに変更がないかどうかを確認します。これを実現するメカニズムは、AAA サーバの関与や、ポストチャ プラグインによるクレデンシャルの送信を必要としない Challenge-Response プロトコルです。このプロトコルは、ホストのクレデンシャルが変更された場合 (修復後のホストの再検証など)、または新しいホストが以前に許可された IP アドレスを使用して接続する場合に、AAA サーバによる完全なポストチャ再検証を開始するために使用されます。

NAD は、特定のホストがシステム管理者の設定に応じてポストチャ検証プロセスをバイパスできるように、IP または MAC アドレスに基づいたローカルの例外リストもサポートしています。また、ポストチャ エージェントがインストールされていないホスト (エージェントレス ホスト) に適用するアクセス ポリシーを AAA サーバに問い合わせることも可能です。

## CISCO SECURE ACCESS CONTROL SERVER (ACS)

Cisco Secure ACS サーバは、アイデンティティの認証だけでなく、ホストのポストチャ クレデンシャルの許可も処理する RADIUS 機能を装備する AAA サーバです。Cisco Secure ACS サーバは、ポリシー決定の結果をネットワーク アクセス プロファイルにマッピングし、NAC の実施のためにこのプロファイルを送信します。ACS サーバは、ポストチャ許可の決定を 1 つまたは複数の外部ポストチャ検証サーバに委託するように設定できます。外部サーバへの委託により、スケーラビリティの向上、特定のポリシー ドメインの決定の委託、あるいはベンダ固有のアトリビュートの処理が可能になります。

ACS サーバは、ベンダおよびアプリケーション タイプのアトリビュートを使用して、ドメインまたはネームスペースとしてローカルおよび外部ポリシー データベースにレコードを保持します。ACS サーバは、これらのデータベース間のポストチャ要求

と応答の多重化/逆多重化を行います。各ポリシー データベースには、管理者が定義したルールで構成される 1 つまたは複数のポリシーが格納されています。各ポリシーでは、ベンダおよびアプリケーション タイプごとにポストチャ クレデンシャルを検証し、各コンポーネントの適合性レベルを定義するアプリケーション ポストチャ トークン (APT) を作成します。次に ACS サーバは、すべての APT を収集してシステム ポストチャ トークン (SPT) と呼ばれる最終的なポストチャ アセスメント結果を決定します。SPT には、最も非適合な APT が反映されます。その後 ACS サーバは SPT をアクセス プロファイルにマッピングし、ホストで NAC を実施するためにこのプロファイルを送信します。APT、SPT に加え、オプションで設定されたユーザ通知またはアクション通知も PA に送信され、許可サイクルが完了します。

### 修復 (REMIEDIATION) サーバ

修復サーバは、ホストまたはクライアントが組織内のポリシーに適合するために利用可能なホスト ソフトウェアのアップデートを保管するリポジトリです。修復サーバには、OS アップデート、セキュリティ パッチ、ホスト エージェント ソフトウェア、その他のソフトウェア コンポーネントなどが保管されています。

現在のポストチャ情報に基づきホストが非適合であると決定された場合、URL リダイレクションを通じてこのホストのユーザを修復サーバ転送にすることができます。この URL でホストがセキュリティ ポリシーに適合するために必要なソフトウェアのダウンロード手順をユーザに通知して修復プロセスを開始できます。

通常、修復サーバは、サーバとクライアントをともにサポートする大規模な修復ソリューションの一部です。

### ポストチャ検証 (POSTURE VALIDATION) サーバ

ポストチャ検証サーバ (PVS) は、ポストチャ クレデンシャルを検証して 1 つまたは複数の APT を作成する任意のサーバです。ACS サーバは PVS のインスタンスですが、PVS は主にドメイン固有のポストチャ クレデンシャル許可をサポートする代理サーバを指す用語として使用されます。たとえば AV サーバは、最新のスキャン エンジンおよびシグニチャ ファイル バージョンを把握しているため、AV 固有のポストチャ決定を下す PVS として機能できます。

PVS は、AAA サーバと PVS との通信に Host Credential Authorization Protocol (HCAP) を使用して、次の機能を実行できます。

- AAA サーバまたは PVS からのポストチャ クレデンシャル要求を受け付ける。
- 適合ポリシーと比較してクレデンシャルを許可する、または他の PVS に決定を委託する。
- AAA サーバに次の要素で応答する。
  - アプリケーション ポストチャ トークン (APT) : ポストチャ クレデンシャルの検証結果。
  - (オプション) ホストのドメイン固有の修復に役立つポストチャ通知。実行するアクション、修復サーバの URL などを通知します。

### 監査 (AUDIT) サーバ

監査サーバは、ホストに対して Vulnerability Assessment (VA; 脆弱性アセスメント) を行い、ネットワーク アドミッションの前にホストの適合性のレベルやリスクを判定する、NAC ソリューションの最新のコンポーネントです。ネットワーク スキャニング、リモート ログイン、ブラウザベースのエージェントなどの VA 手法は、通常 IEEE 802.1x サプリカントまたは CTA が提供している情報を収集するために使用されます。監査サーバコンポーネントは、Cisco NAC プログラムに参加する特定のベンダによって提供されるため、お客様は自社のポリシーのニーズや導入の要件に合わせて、最適な VA ベンダとテクノロジーを選択できます。

監査サーバは、Generic Authorization Message Exchange (GAME) プロトコルを使用して ACS と監査情報をやりとりします。ACS は、監査サーバとエージェントレス ホストの監査プロセスを開始します。監査サーバは監査プロセスを実行し、ACS は監査サーバに定期的に監査結果をポーリングします。監査サーバは、監査プロセスを完了するとホストのポスチャ ステートを ACS に通知します。

Cisco NAC フレームワークと統合するすべてのベンダおよび製品の最新リストについては、Cisco NAC プログラム ページ (<http://www.cisco.com/go/nac/>) を参照してください。

## レポートिंग

認証の失敗、成功、各結果の理由など NAC 関連イベントの情報は、ACS レポートで確認できます。各レポートのフィールドはカスタマイズできるので、必要に応じて関連情報や追加情報も表示できます。ACS のレポートは、主に NAC 認証の問題のトラブルシューティングに使用します。

さらに ACS の NAC 情報は、Cisco Secure Monitoring Analysis and Response System (CS-MARS) アプライアンスにもエクスポートできます。MARS アプライアンスは、イベントの相関関係情報、およびネットワーク上の NAC イベントに関するビジュアルな詳細情報を提供します。

CS-MARS アプライアンスでは、NAC に関連する複数のデフォルト レポートング オプションが利用できます。管理者は、現在検疫されている総ホスト数などの NAC のデフォルト レポートの表示のほか、カスタム レポートも作成できます。

さらに CS-MARS により、管理者は NAC 関連のイベントを即座に確認し、クライアントのネットワーク内の物理的な配置場所、特定のスイッチおよびスイッチポートのレベルも特定できます。

## プロトコル

ここでは、Cisco NAC で使用されるプロトコルについて説明します。

### EAP

Extensible Authentication Protocol (EAP) は、ホストと AAA サーバ間のアイデンティティおよび認証クレデンシャルを交換できるリクエスト-レスポンス プロトコルです。EAP は、MSCHAPv2、証明書ベースの認証、Public Key Infrastructure (PKI ; 公開キー インフラストラクチャ) を含むさまざまな認証方式をサポートしています。EAP は、RFC 2284 で定義されています。

EAP プロトコルには、NAC のために次のような拡張が追加されています。

- EAP-TLV
- EAPoUDP

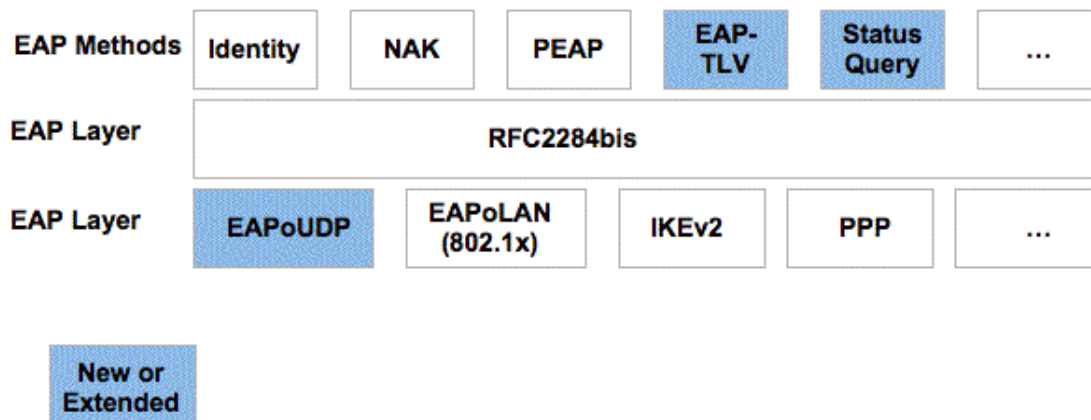
EAP Type Length Value (EAP-TLV) 拡張は、ポスチャの Attribute Value Pairs (AVP; アトリビュート値ペア) およびポスチャ通知を含むポスチャ クレデンシャルの転送のために追加されました。

また NAC には、ステータス クエリーという拡張も追加されました。ステータス クエリーは、クレデンシャルの完全な認証を行わずにピアのポスチャ ステータスを安全に照会する新しい EAP 方式です。この機能は、NAC L3 IP および NAC L2 IP でのみ利用できます。

EAP over UDP (EAPoUDP) は、NAC L2 IP および NAC L3 IP で EAP 情報をトランスポートするための EAP プロトコル内の機能です。

EAP および EAP 拡張に関する情報を次の図に示します。

図 6. EAP の概要



### EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) は、TLS をベースとする RFC 3748 に準拠した EAP 方式です。シスコでは、Internet Engineering Task Force (IETF) に EAP-FAST のドラフトを投稿しています。このドラフトは、IETF の Web サイト (<http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-03.txt>) で公開されています。

EAP-FAST は、対称鍵アルゴリズムを使用して認証プロセスのトンネル化を実現します。トンネルの確立には、AAA サーバを通じて、EAP-FAST により動的なプロビジョニングおよび管理が可能な Protected Access Credential (PAC) を使用します。

- フェーズ 1：ホストおよび AAA サーバは、PAC を使用して相互に認証し、セキュアなトンネルを確立します。
- フェーズ 2：確立されたトンネルでクライアントの認証を実行します。
- フェーズ 0 (任意)：このフェーズは頻繁には使用されませんが、クライアントに動的に PAC をプロビジョニングできるようにします。

EAP-FAST と NAC で利用できるオプションに関する追加情報については、本書の「NAC 設計時の考慮事項」のセクションで説明します。

### HCAP

Host Credential Authorization Protocol (HCAP) は、ACS サーバと NAC パートナーのポストチャ検証サーバ間に通信を提供します。HCAP は、HTTP (S) セッションを使用して ACS およびベンダ サーバ間のセキュアな通信をサポートし、EAP ベースのクレデンシャル交換を行います。

ACS は、1 つまたは複数のベンダ サーバにクライアントのクレデンシャルを送信し、各ベンダ サーバからポストチャ トークン応答と通知メッセージ (オプション) を受信します。

**注:** HCAP は、ACS とアンチウイルス サーバなどの PVS (ポストチャ検証サーバ) との通信に使用されるプロトコルです。

## GAME

Generic Authorization Message Exchange (GAME) は、HTTPS を使用して ACS サーバと NAC パートナーの監査サーバ間のセキュアな通信を提供するプロトコルです。GAME は、ACS とパートナーの監査サーバ間の Security Assertion Markup Language (SAML) を拡張します。

ACS は、パートナーの監査サーバによるエージェントレス ホスト (CTA を持たないホスト) のポスチャ検証を開始できます。ACS サーバは、監査サーバからの監査の決定を定期的にポーリングします。ポスチャ検証プロセスが完了すると、監査サーバはクライアントまたはホストのポスチャ ステータを送信して ACS に応答します。

## NAC アセスメント方式

Cisco NAC は、ネットワークにアクセスを試みるホストのアイデンティティおよびポスチャ検証をさまざまな方式で開始できます。多くの場合、使用できる方式は、既存のセキュリティ ポリシーと、ホストが接続を試みるネットワーク アクセス デバイスによって異なります。Cisco NAC アセスメント方式には、次のものがあります。

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- IEEE 802.1x と NAC L2 IP
- エージェントレス ホスト

### NAC L3 IP

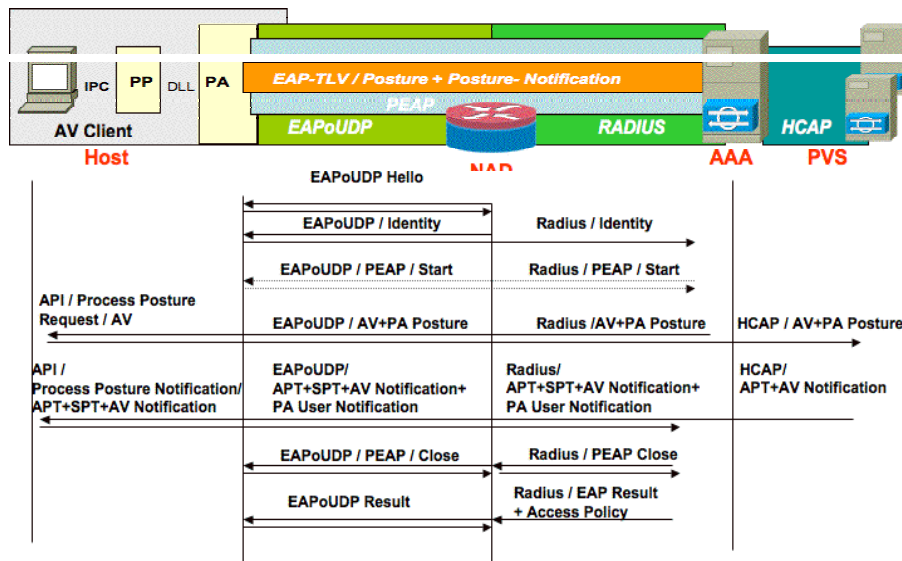
NAC L3 IP は、NAC の初期リリースの一部として導入されました。

ルータ上の NAC L3 IP ポスチャ検証プロセスは、NAC L3 IP が設定されたルータ インターフェイスがレイヤ 3 パケットを受信したときに開始されます。NAC プロセスが始まると、ルータは EOU hello メッセージを送信し、クライアント ホストはこのメッセージに対して EOU hello を返します。NAD とクライアントが相互に認識したら、NAD はクライアントにアイデンティティを要求します。NAD はアイデンティティを受信すると EAP over RADIUS パケットでアイデンティティを Cisco Secure ACS に渡します。次に Cisco Secure ACS がクライアント ホストとの PEAP セッションを開始します。

**注:** ルータはこの時点ではパススルー デバイスとしての役割を果たします。PEAP セッションのどの部分もプロキシするのではなく、UDP から RADIUS に PEAP パケットをカプセル化しなおすだけです。

PEAP セッションが確立されると、Cisco Secure ACS はクライアント上の登録済みのソフトウェアのクレデンシャルをクライアントに要求します。クライアント上の CTA は、CTA に登録済みのポスチャ プラグインにクレデンシャルとアトリビュートを問い合わせます。これらのクレデンシャルとアトリビュートが収集され、PEAP セッションで Cisco Secure ACS に送信されます。この初期化フェーズ中、ルータ インターフェイスが受信したパケットにはインターフェイスに設定されているアクセス リストが適用されます。アドミッション コントロールとともに使用される場合、アクセス リストは、アドミッション コントロール プロセスを開始するパケットと開始しないパケットを識別します。このプロセスの詳細を次の図に示します。

図 7. NAC L3 IP ポスチャ検証プロセス



Cisco Secure ACS が、要求したクレデンシャルを CTA から受け取ると、ACS サーバはクレデンシャルとアトリビュートをデータベースのローカルおよび外部ポリシーと照合します。

各ポリシーは、単一のクレデンシャルに対して 1 つの APT と、ポスチャ エージェント別に設定されたアクションをクライアントに返します。最も制限されているアプリケーション ポスチャ トークンは、SPT として使用されます。SPT によって、Cisco Secure ACS がクライアントを配置するグループと、このクライアントの総合的なポスチャ結果が決まります。実際のルールは、Cisco Secure ACS のグループ ポリシーに設定されています。ルールは、Downloadable ACL、URL リダイレクション、タイマー調整の形で適用されます。NAD は、ホストのポスチャの変更の有無を調べるためにホストに定期的にお問い合わせを行います。

NAD は、URL リダイレクションを通じてクライアントを自動的に AV サーバに転送し、クライアントが Web にアクセスするときにアップデートさせることができます。

Cisco Secure ACS では、特定のホストの修復プロセスを正常に完了させるために、このホストに対する NAD 上のステータス クエリー値を短縮できます。すべてのアプリケーション ポスチャが検証済みなので、アプリケーション APT は健全な状態に戻り、結果としてホストは「Healthy」SPT を取得できます。この後、DHCP のアドレッシングの変更や DHCP クライアントの変更などの変更が発生すると、クライアントのステータス クエリーは失敗し、検証プロセスがもう一度開始されます。クライアントから応答がないと、デフォルトのポリシーが NAD にダウンロードされ、総合的なネットワーク セキュリティ ポリシーに応じてクライアントのネットワーク アクセスが制限されます。

## NAC L2 IP

NAC L2 IP は、ホストのポスチャ アセスメントのトランスポートに EAP over UDP (EoU) を使用する点で NAC L3 IP と似ていますが、レイヤ 2 スイッチ ポートのレイヤ 3 に実装される点が NAC L3 IP と大きく異なります。

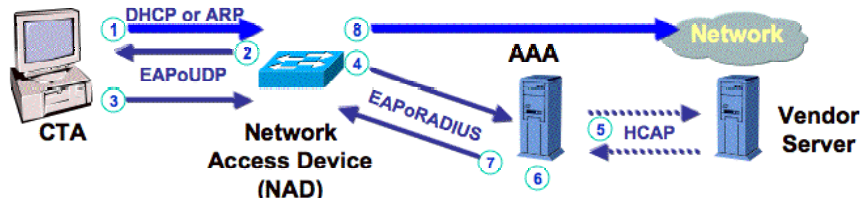
また NAC L2 IP には、Intercept ACL の概念がありません。NAC L2 IP では、NAD がホストから次のいずれかを受信したときにポスチャ アセスメントが開始されます。

- DHCP 要求
- ARP 要求

NAD は、ホストから最初の DHCP または ARP 要求を受信すると、EoU ハンドシェイクを開始し、ポスチャ検証プロセスを開始します。このプロセスは、クライアントからの受信 DHCP 要求によって開始される場合、

ホスト、NAD、ACS サーバ間で実施されるこのプロセスを次の図に示します。

図 8. ポスチャ検証の通信フロー



1. DHCP または ARP 要求により、NAD がプロセスを開始します。
2. NAD が CTA とのポスチャ検証を開始します (EAPoUDP)。
3. CTA がポスチャ クレデンシヤルを NAD に送信します (EAPoUDP)。
4. NAD がポスチャ クレデンシヤルを AAA に送信します (EAPoRADIUS)。
5. AAA がポスチャ認証の一部をベンダ サーバに委託します (HCAP)
6. AAA がポスチャを検証し、許可権限 (Healthy、Checkup、Quarantine) を決定します。
7. AAA が許可ポリシーを NAD に送信します (ACL、URL リダイレクション)。
8. ホスト上のアプリケーションにも通知が送信される場合があります。
9. ホストの IP アクセスが許可 (または拒否、制限、URL リダイレクト) されます。

ホストのポスチャ ステートがポリシー サーバによって決定されると、各 NAD の ACL により NAC が実施されます。スイッチには、まず必要なトラフィックのみにネットワーク アクセスを制限するデフォルトの ACL が設定されています。デフォルト ACL では、たとえば DHCP、DNS、WWW などのプロトコルのフローと、ホストのポスチャ検証前にアクセスを与えるべきその他のデフォルト トラフィックを許可する必要があります。すでに説明したように、どのトラフィックがポスチャ検証を開始するかではなく、ホストのポスチャ検証前にデフォルトでどのトラフィックを許可するかを指定する点が NAC L3 IP の Intercept ACL の概念とは異なります。デフォルト ACL の設定に関する追加情報については、『ネットワーク アドミッション コントロール コンフィギュレーション ガイド』を参照してください。

Healthy、Quarantine などの各ポスチャ トークンに対応する ACL は、Downloadable ACL として ACS に定義されています。これらの ACL は、ACS から NAD にダウンロードされると、スイッチポートに設定されているデフォルト ACL に優先して適用されます。

さらに NAC L2 IP は、IEEE 802.1x アイデンティティ検証を補完する独立したポスチャ検証方式としても機能することができます。NAC L2 IP は 802.1x から独立しているため、IEEE 802.1x が設定されたポートと同じポートに設定可能です。NAC L2 IP は、802.1x ユーザおよびマシン認証が実行された後にホストのポスチャ検証を実行できます。この機能については、次のセクションで詳しく説明します。

## NAC L2 802.1X

NAC L2 802.1x は、802.1x を活用してユーザおよびホストの認証情報を提供し、EAP-FAST プロトコルを使用してホストのポストチャ情報もトランスポートします。NAC L2 802.1x は、レイヤ 2 スイッチ ポート上で 802.1x を介してホストのアクセスを開始します。

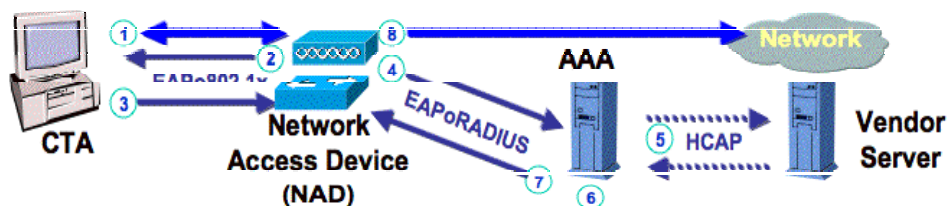
NAC L2 802.1x では、TLS トンネルでアイデンティティおよびポストチャ情報を転送するために、EAP 方式として EAP-FAST をサポートするサブリカントが必要です。CTA に組み込まれたサブリカントは、EAP-FAST をサポートするほか、EAP-GTC、EAP-MSCHAPv2、およびクライアント側認証のための EAP-TLS をサポートします。

802.1x が提供するアイデンティティ情報には、ホストのユーザおよびマシン両方の情報を含むことができます。ユーザおよびマシン認証については、本書の「NAC 設計時の考慮事項」のセクションで説明します。

NAC L2 802.1x では、スイッチでのダイナミックな VLAN 割り当てを通じてポリシーを実施します。VLAN は、割り当てられたポストチャ トークンに基づいてホスト単位で割り当てられます。ACS がホストに割り当てるポストチャ トークンを決定すると、RADIUS アトリビュート 64、65、81 を通じてスイッチに VLAN 情報が送信されます。VLAN トラフィックを正しくセグメント化する ACL が事前に設定されていることが前提となります。

次に NAC L2 802.1x の認証プロセスの図と手順を示します。

図 9. NAC L2 802.1x



1. NAD とエンドポイント間に 802.1x 接続が確立されます。
2. NAD がエンドポイントにクレデンシャルを要求します (EAPo802.1x)。
3. 要求されるクレデンシャルには、ユーザ、デバイスおよび/または ポストチャのクレデンシャルが含まれます。
4. CTA が NAC 対応サブリカントを通じて NAD にクレデンシャルを送信します (EAPo802.1x)。
5. NAD が AAA にクレデンシャルを送信します (EAPoRADIUS)。
6. AAA はポストチャ認証の一部をベンダ サーバに委託できます (HCAP)。
7. ユーザ/デバイスのクレデンシャルが認証データベース (LDAP、Active Directory など) に送信されます。
8. AAA がクレデンシャルを検証し、許可する権限を決定します。
9. たとえば、ゲストには GUEST アクセス、健全でないデバイスには QUARANTINE アクセスを与えます。
10. AAA が許可ポリシーを NAD に送信します (VLAN 割り当て)。
11. ホストのアプリケーションにも通知が送信される場合があります。
12. ホストに VLAN が割り当てられ、IP アクセス (または拒否、制限) が与えられます。

NAC L2 IP と違い、NAC L2 802.1x には NAD がホストに対して実施するステータス クエリー プロセスの概念がありません。再認証プロセスの開始には、セッション タイムアウト値が使用されます。この値は、各スイッチのローカルに設定することも、RADIUS アトリビュート 27 で ACS に設定することもできます。この値が ACS に設定されると、スイッチに設定された値は自動的に無効になります。

セッション タイムアウト値に加え、CTA がホストのポストチャ ステータスをローカルで確認し、ホストのポストチャ検証を開始することもできます。デフォルトでは、CTA はホストのポストチャ プラグインに 5 分間隔でポーリングし、パートナー ソフトウェアのステータスに変更がないかどうかを確認します。変更が検出されると、CTA サプリカントは EAP over LAN (EAPoL) Start をスイッチに送信して再認証とポストチャ アセスメントを開始します。

CTA 2.0 と NAC L2 802.1x には、Asynchronous Status Query (ASQ; 非同期ステータス クエリー) という新機能が追加されました。ASQ により、ホストにインストールされているセキュリティ ソフトウェアは、ポストチャ プラグインを介して、ホスト上のソフトウェアに関連するすべてのステータス変更を更新して CTA に通知することができます。たとえば、Cisco Security Agent がローカル ホストに変更を検出した場合、ポストチャ プラグインを介して最新情報が CTA に送信されるため、CTA サプリカントはスイッチによるホストの再アセスメントを開始できます。Cisco Security Agent は、ASQ 機能をサポートした最初のソフトウェアです。

NAC L2 802.1x の詳しい導入オプションと考慮点については、本書の後半で説明します。

### エージェントレス ホスト

エージェントレス ホストとは、CTA がインストールされていないため、アイデンティティおよびポストチャ検証プロセスに参加できないホストです。

一般的には未知のホストの意味で、ポストチャ エージェント ソフトウェアがロードされていないクライアントを指します。IP 電話、ネットワーク プリンタを含む IP デバイスはこれらのクライアントに該当します。CTA やポストチャ エージェント ソフトウェアがロードされていない PC およびワークステーションも未知のホストと考えられます。これらのワークステーションは、主に MacOS、Solaris、サポートされていないバージョンの Windows が稼動しているものです。

### 静的な例外 (ホワイトリスト)

未知のホストを処理する方法の 1 つは、Cisco IOS ソフトウェアまたは中央の ACS にホストの IP アドレスと MAC アドレスをベースに静的なポリシーを設定することです。ホストは、作成された例外に基づいてポストチャ検証プロセスのバイパスを許可され、ネットワークにアクセスすることができます。

### ダイナミックな監査

NAC には、監査サーバを使用してエージェントレス ホストをダイナミックに監査する機能が新たに追加されました。ダイナミックな監査では、エージェントレス ホストがネットワークに接続したときにエージェントレス ホストの監査または脆弱性スキャンを開始するポリシーを作成します。監査の結果として得られたポストチャ トークンは、ACS に転送され、ホストに割り当てられます。ホストは、このポストチャ トークンに基づいてネットワークへのアクセスが許可されます。

管理者が使用できるエージェントレス ホストの処理オプションは、NAC アセスメント方式によって異なります。詳しくは、本書の「NAC 設計時の考慮事項」のセクションで説明します。

## NAC ポリシー戦略

NAC は、ユーザ アイデンティティ、ホスト アイデンティティ、およびホストのポスチャ適合性に対する単一の連携的なセキュリティ ポリシーを使用してネットワーク アクセスを実施するセキュリティ ソリューションです。NAC フレームワークでは、単一の許可の決定を下すために複数のセキュリティ アプリケーションにアクセスの決定を委託できます。自社の NAC の目標を設定するためには、まず包括的なセキュリティ ポリシーとは何かを理解し、ポリシーを作成する必要があります。

### ネットワーク アドミSSION ポリシーの設計

すべての AAA セキュリティ テクノロジーの基本は、誰が、何に、いつ、どこから、どのようにアクセスできるのかを評価し、制御することです。従来「誰が」の部分は、ユーザ名とパスワード、デジタル証明書、ワンタイム トークン パスワード、あるいはバイオメトリックの形式の単純なユーザおよび/またはホストのアイデンティティでした。Cisco NAC は、AAA 認証の範囲を拡張し、ユーザおよびホストのアイデンティティだけでなく、ホストのポスチャ、つまりホストのハードウェアとソフトウェア設定の適合性も完全に検証します。ネットワークは、NAC プログラムに参加するセキュリティ アプリケーションのサポートにより、ホストへのネットワーク アクセスを許可する前に次の要素を検証できます。

- オペレーティング システムのタイプ、バージョン、パッチのレベル
- レジストリ設定、ファイルの存在、サイズ
- Cisco Security Agent (CSA) の設定と状態
- アンチウイルス ソフトウェアのバージョン、シグニチャ ファイルのレベル、状態
- パーソナル ファイアウォール エンジンのバージョン、ルール セット、状態
- 特定のハードウェア コンポーネントの有無

この進化したセキュリティは、ウイルスとワームがパッチ未適用のオペレーティング システムやアプリケーションの脆弱性を素早く簡単にしかも大規模に悪用できるようになったことにより不可欠になりました。これらの脅威は、組織のセキュリティや組織が存続していく上で、悪意あるユーザやハッカーよりも大きな脅威となる可能性があります。コンピュータ システムに常に最新の OS パッチとセキュリティ ソフトウェア アップデートを適用しておくことは、極めて重要なのです。

#### ポリシーの作成と要件

NAC 導入の目的は、アクセスが許可されていない非適合のネットワーク ホストに付随するすべての問題の発生を防止することです。許可は、アイデンティティだけでなく、ホストの OS や複数のクライアント側エージェントおよびアプリケーションの適合性にも基づいて決定することができます。大規模な組織では、アイデンティティ サーバ、デスクトップ ソフトウェア、サーバ ソフトウェア、アプリケーション管理、ネットワーク セキュリティ、およびサポートの管理と運営は、その分野のエキスパートで構成されるチームごとに行われます。これらすべてのチームが結集して包括的な連携型のセキュリティ ポリシーを作成し、維持していくことは困難で時間がかかる作業です。

NAC セキュリティ ポリシーは、ネットワーク (LAN、WAN、ワイヤレス、リモート アクセス、エクストラネット) および情報技術 (デスクトップ、サーバ、アプリケーション、サポート) チームの代表者が、協業で構築し、維持していく必要があります。その際に、次の内容を決定する必要があります。

- ポリシーの作成とポリシーの実施の責任者。
- 全社的なネットワーク アドミSSIONの現在の要件。すべてのアクセス方式 (有線、ワイヤレス、VPN、エクストラネットなど) で要件は同じか。
- ネットワーク内の管理対象外のマシンおよび非標準的なマシン (ラボ、ゲスト、コンサルタント、エクストラネット、キオスクなど) に対するポリシー。

- 認証およびアプリケーションの適合性を決定する現在のセキュリティ ポリシー。現在のポリシーで十分か、検証の範囲を広げる必要があるか。
- 現在のネットワーク セグメント化の方法 (VLAN か ACS か)。
- ポリシー担当者が現在のポリシーの更新や変更について話し合いを持つ頻度。
- (小さい変更でも) 変更の決定に必要とする定足数。
- セキュリティ ポリシーを実施するビジネス ケースが経営陣にサポートされているか。ユーザは管理されることを嫌い、反発されることも考えられる。

組織として必要なポリシーと作成方法について基本的に合意したら、ポリシーの定義を開始します。

### ポリシーの定義

ネットワーク アドミッション ポリシーは、許可を決定するための複数の基本要素で構成されます。次に、ポリシーの各要素の説明と、複数の例およびオプションのリストを示します。

**Who** — ネットワーク アクセス要求者のアイデンティティとグループ

ユーザ アイデンティティ — ユーザおよびグループ、またはゲスト特権を基準にアクセスを差別化

ホスト アイデンティティ — 企業の資産、管理対象外ホスト別にアクセスを差別化

ホスト ポスチャ — ハードウェア/ソフトウェア インベントリおよびセキュリティ ソフトウェアの状態

**Where** — ポリシーが異なるロケーション

地理 — 特定のポリシー ルールまたは法律で規制される都市、国、その他の地域

論理 — ロビー、ラボ、セキュリティ強化エリアなど、特有のセキュリティ要件を持つ論理的な場所

**When** — 状況に応じたアクセス制限とアカウントिंगおよび監査のためのイベント ログギング

時間 — 時間、曜日、その他の時間的な制限

割り当て — アカウントのバランス、時間、アクティブなインスタンスに基づいたセッション制限

ログ — リソースの使用率とセキュリティ フォレンジックの監査

**How** — ネットワーク アクセス方式、プロトコル、ポリシーの要件

LAN-802.1x 対応 レイヤ 2 (L2) スイッチ ポートによるアクセス

ワイヤレス — 建物内および周囲からのワイヤレス アクセス

WAN — レイヤ 3 (L3) ルーテッド ネットワーク内のチョークポイント

VPN — リモート アクセス

**What** — アクセス方式の機能に基づいたネットワーク権限と機能

オープン — アクセス要件または制限なし

グループ — グループまたはロールに基づいたネットワークの論理的なセグメント

エクストラネット — アウトソーシングまたはリソース共有のためのパートナー接続

ユーティリティ – プリンティング サービスおよびその他の専用デバイス

ゲスト – インターネットのみのゲスト アクセス

はじめから組織内で発生しうるすべてのシナリオを考慮すると混乱を招きますので、簡単な例から定義を開始してください。セキュリティ ポリシーは、複雑でなくても効率的に機能します。

この簡単な例でも、従業員を認証し、ゲスト ユーザと許可されていないユーザにインターネット アクセスを提供できます。

Who	Where	When	How	What
ユーザ：従業員	任意	任意	IEEE 802.1x (有線およびワイヤレス) VPN + トークン カード	任意
ユーザ：ゲスト	任意	午前 7 時 – 午後 6 時	ワイヤレス ホットスポット	インターネットのみ

機密データやウイルスがもたらす潜在的な問題をさらに懸念する企業は、より制限されたポリシーを必要とします。次のポリシーは、「企業資産、イメージ、従業員とそれ以外を区別する」ポリシーと言えます。

Who	Where	When	How	What
ユーザ：従業員 ホスト：企業資産 ポスチャ：OS パッチ + AV	本社	任意	NAC L2 802.1x	任意
ユーザ：従業員 ポスチャ：OS パッチ + AV	VPN	任意	VPN + NAC L3 IP	任意
ユーザ：コールセンター ホスト：企業資産 ポスチャ：OS パッチ + AV	インド	任意	NAC L2 802.1x	イントラネットのみ
プリンタ	任意	任意	Mac-Auth-Bypass	プリンタ サーバのみ
ゲスト	任意	任意	なし	なし

これらの例は非常に基本的ですが、アクセス方式、クレデンシャルの要件、パーティショニング オプションの組み合わせは明確です。対応が必要なシナリオはすべて文書化する必要がありますが、シナリオに対処するポリシー数は最小限に抑えてください。異なるポリシー オプションを数多く使用する必要がある場合は、一度に多くの変更を実施することを避け、段階的に要件を追加するようにしてください。

## クレデンシャル

### アイデンティティ クレデンシャル

アイデンティティとは、認証システムが認識する人、デバイス、またはその組み合わせの一意の名前です。アイデンティティ クレデンシャルとは、認証トランザクションで使用されるパスワードや証明書などのオブジェクトです。IEEE 802.1x では、これらのクレデンシャルにより、認証システムがスイッチ上の 802.1x サブリカントを認識するかどうかが決まります。また、サブリ

クライアントがネットワークへのアクセス権を得るために正しいクレデンシアルを持っているか、このサブクライアントに対してどのような許可が適切であるのかも、これらのクレデンシアルによって決まります。すでに説明したように、NAC L2 802.1x では、アイデンティティおよびポストチャ両タイプのクレデンシアルに基づいてアドミッションの決定を下すために、単一の EAP カンパセーションで両方のクレデンシアルを転送することができます。ネットワーク管理者は、NAC L2 802.1x を使用する場合に ACS 内部でアクセスが許可されるのは、アイデンティティ クレデンシアルにより正常にサブクライアントが認証されたときのみであることに注意してください。アイデンティティ クレデンシアルの認証が失敗すると、ポストチャ クレデンシアルの検証は行われず、サブクライアントはネットワークへのアクセスを拒否されます。

NAC L2 802.1x の機能を詳しく理解するために、サブクライアントは NAC システムに通常 2 つのタイプのアイデンティティ クレデンシアルを送信可能であることを認識することが重要です。デバイスの設定は検証するクレデンシアルのタイプに依存するため、このことは設計と密接な関係があります。

### 汎用デバイス クレデンシアル

1 つめは、デバイス クレデンシアルと呼ばれるクレデンシアルです。この認証方式では、コンピュータのユーザの前にマシン認証が行われます。このタイプのクレデンシアルは、デバイスがユーザ認証の前にネットワークにアクセスして何らかの機能を実行する必要がある場合、またはデバイスがサーバやプリンタなどエンドユーザが通常使用するデバイスではない場合に使用されます。デバイス クレデンシアル (パスワードなど) は、サブクライアントがデバイスの起動時にアクセスして、NAC システムに自身を認証できるように、ホストに保管することができます。

### Microsoft マシン クレデンシアル

Microsoft は、自社環境でのデバイス クレデンシアルのログイン メカニズムをマシン認証と呼んでいます。Microsoft は、起動時にコンピュータのアイデンティティおよびクレデンシアル (Active Directory System ID または マシン証明書) を使用してクライアントのシステムを認証するマシン認証機能を提供しています。したがって、クライアントはドメイン グループ ポリシー オブジェクト (GPO) モデルの更新および参加に必要なセキュアなチャネルを確立することができます。マシン認証により、コンピュータは、起動時にデバイス ドライバをロードした直後に 802.1x を使用してネットワークに対して自身を認証することができます。

### ユーザ クレデンシアル

Windows オペレーティングシステムは、起動時に 802.1x を介してマシン認証を行った後、Windows ドメイン コントローラと通信してマシン グループ ポリシーを取得できるため、802.1x の使用によりドメイン GPO が機能しなくなる問題が解消されました。

ユーザが Ctrl + Alt + Delete キーを押すと、クレデンシアルを入力するための Microsoft Graphic Identification and Authentication (GINA) ダイアログが PC に表示されます。GINA が表示されたら、ユーザはコンピュータまたは Windows ドメインにログインことができ、ログインに使用したユーザ名とパスワードを 802.1x 認証のアイデンティティ クレデンシアルとして使用できます。この 2 つめのタイプのクレデンシアルは、一般にユーザ認証と呼ばれています。

### ポストチャ クレデンシアル

ポストチャ クレデンシアルは、ステータスおよび設定情報を示すハードウェアおよびソフトウェアのアトリビュートで、セキュリティ ポリシーとのポストチャの適合性検証に使用できます。アプリケーション ベンダおよびネットワーク管理者が重要とみなし、チェックするクライアント マシンのアトリビュートはすべてポストチャ クレデンシアルとして使用できます。次の表に、CTA が送信可能な基本的なアトリビュートのデータ型を示します。

OctetArray	Integer32	Unsigned32	String (UTF-8)	IPv4Addr
=, !=	=, <, >, !=, >=, <=	=, <, >, !=, >=, <=	=, !=, contains, start with, regular-expression	ワイルドカードとマスク

すべての NAC クレデンシヤル（アトリビュート）は、単一のホスト上の各ベンダのアプリケーションのプロパティを区別するために、ネームスペースを使用して階層的に表現されます。NAC ネームスペースは、次に示す方法でベンダ、アプリケーションタイプ、アトリビュート名で構成されます。

Vendor: Application-Type: Attribute

たとえば、Cisco:PA : OS-Type は Cisco Trust Agent のアトリビュートの 1 つです。次の表に、CTA がネイティブに使用できる情報と、他のアプリケーション ポスチャ プラグインが提供できる情報の例を示します。各ベンダは通常、個々のアプリケーション タイプに共通のアトリビュートを提供し、ベンダ固有または製品に特有の機能のためのアトリビュートもさらに提供する場合があります。

アプリケーション :	CTA	CTA	CSA	アンチウイルス
Vendor :	Cisco	Cisco	Cisco	各種
Application-Type :	PA	Host	HIP	AV
Attribute :	PA-Name PA-Version OS-Type OS-Version OS-Release OS-Kernel-Version Machine-Posture-State	ServicePacks HotFixes HostFQDN	CSAMCName, CSAOperationalState CSAStates CSAVersion TimeSinceLastSuccessfull Poll	Software-Name Software-ID Software-Version Scan-Engine-Version DAT-Version DAT-Date Protection-Enabled

ネットワーク設計者は、自社のセキュリティ ポリシーをサポートするアドミッション コントロールを行うために、追加のアプリケーション プラグインが必要な場合があることに注意してください。たとえば企業のセキュリティ ポリシーで、クライアント マシンにクライアント OS の最新のホットフィックスだけでなく、最新バージョンのアンチウイルス DAT ファイルを要求する場合、ネットワーク管理者はこの情報を CTA に提供するアプリケーション プラグインが必要となり、アンチウイルス ベンダから CTA に適切な AV プラグインを入手する必要があります。

### アイデンティティ対ポスチャ

NAC の許可方式は、アイデンティティおよびグループ メンバーシップの単純な問題の域を超えて、アイデンティティとポスチャに応じて異なるレベルのアクセスを提供することを可能にしました。したがって管理者は、アトリビュートに基づいてアクセスを優先することができます。グループのメンバーシップは、ネットワーク アドミッションの基本的な要素ですが、ホストのポスチャが健全である場合にのみ適用されます。ホストのポスチャが健全でない場合、脆弱またはウイルスに感染したホストは大きな脅威であるため、グループ アイデンティティの権限を無効にし、ウイルスとワームから保護するためにアクセスを制限する必要があります。

アイデンティティとポスチャの許可の優先度を理解するために、組織のアイデンティティ グループとポスチャ ステートの表を作成します。この表には、特定のセキュリティ ポリシーに対するアイデンティティとポスチャの各組み合わせの優先順位を記入します。次に、各グループまたはステートと、ネットワーク上でどのような動作を許可/拒否するかを制御するネットワーク アクセス権を関連づけます。

	Healthy	Quarantine	Unknown
Employees	Employees	EmployeeQuarantine	EmployeeQuarantine
Contractors	Contractors	ContractorQuarantine	ContractorQuarantine
Guests	Guests	Guests	Guests

また、すべてのネットワーク アクセス方式がアイデンティティおよびポストチャ クレデンシャル両方を提供するわけではないことに注意してください。次の表に示すように、使用できるクレデンシャルは NAC アクセス方式のタイプによって制限されます。

機能	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
開始メカニズム	データ リンク	DHCP または ARP	ルーティングされたパケット
マシン アイデンティティ	•		
ユーザ アイデンティティ	•		
ポストチャ	•	•	•
監査		•	•

## ネットワークのセグメントと分離

AAA サーバは、許可の決定を下すと、ホストとユーザに対して実施する各設定ポリシーを NAD に送信します。最も一般的なポリシー実施メカニズムは RADIUS セッション タイマー、VLAN 割り当て、ACL、URL リダイレクション、QOS パラメータです。これらのメカニズムにより、ネットワーク管理者はネットワーク セグメントを使用してセキュリティ ポリシーを実施し、許可されたネットワーク リソースのみへのアクセスを許可できます。NAD でのポリシー実施機能は、ネットワーク アクセス方式と NAD のハードウェア機能に完全に依存します。

## セグメント

NAC を導入する前に、使用する NAD の機能と自社のネットワーク アーキテクチャを考慮して、どのネットワーク リソースへのアクセスの許可/拒否を行う必要があるか、どのようなメカニズムを使用できるのかを理解する必要があります。一般的にネットワークのセグメント化は、LAN スイッチとワイヤレス アクセス ポイントで IEEE 802.1x を使用してホストにダイナミックに VLAN を割り当てることによって行われます。これにより、ホストは VLAN ACL の対象となり、同一 VLAN 内の他のリソースのみと通信することが保証されます。VPN とリモート アクセス ネットワークの場合には、ACL を使用して IP アドレスおよびプロトコルによって宛先が制限されます。両メカニズムとも、ユーザおよびホストと、許可されていないネットワーク リソースを効果的にセグメント化することができます。

## 分離

アイデンティティおよびポストチャ ポリシーに基づいたネットワークのセグメント化は、NAC 導入の基本です。同様に、これらのポリシーをネットワーク内のどこで実施し、許可されていないすべてのホストを効果的に分離することも極めて重要です。効果的に分離を行うには、ネットワークのエッジで NAC を実施し、ウイルス感染したホストがアンチウイルスや修復目的で使用するリソース以外のすべてのネットワーク ホストと接触しないようにする必要があります。ネットワークのディストリビューション レイヤまたはコアで NAC を実施すれば管理対象の NAC チョークポイントを最小限に抑られるように思われますが、それではウイルス感染したホストの抑止にほとんど意味をなしません。

NAC は、すべてのネットワーク エッジで広域に実施することで非常に効果的な防御策を提供しますが、ネットワーク内に追加のセキュリティ ゾーンを構築するためにも使用できます。NAC をルーテッド ネットワーク インターフェイスまたはチョークポイントで実施することにより、ネットワーク内の特定のエリアへのアクセスに別のセキュリティ要件への適合を強制することができます。

## デフォルト ネットワーク アクセス

分離に関連する事項として、NAC セキュリティ ポリシーの作成にあたり、デフォルトのネットワーク ポリシーを理解する必要があります。デフォルト ポリシーは、ユーザとホストが許可されなかったときに提供するネットワーク アクセスです。許可されないユーザやホストは、ハッカーだけではなく、ゲストやコントラクター、スケーラビリティやアベイラビリティの問題で AAA サーバに障害が発生した場合には正当なユーザもこのホストに含まれます。理由に関わらず、このようなシナリオが発生した場合、NAD はこれらのユーザに設定済みのデフォルト ネットワーク アクセスを提供します。NAC L2 802.1x 接続の場合は、アクセスは許可されません。NAC L2/L3 IP の場合は、デフォルト ACL で許可されているアクセスのみが許可されます。デフォルト アクセスは、組織のセキュリティ ポリシーおよびシナリオに応じて、アクセスの完全な拒否、完全な許可、インターネットのみのアクセス、一部のカスタマイズされた一連のネットワーク サービス、またはそのすべてを設定できます。

## NAC AGENTLESS HOST (NAH; NAC エージェントレス ホスト) オプション

すべての NAC 導入が直面する最大の問題の 1 つは、アイデンティティおよびポストチャ クレデンシャルの許可方法ではなく、アイデンティティやポストチャが利用できないときの処理方法です。ここまで本書で説明してきたすべての NAC ポリシーは、すべてのネットワーク ホストがネットワークからのアイデンティティおよびポストチャ クレデンシャルの要求に応答できることを前提としていました。しかし、ネットワーク許可に必要とされる各種プロトコルをサポートしない/できないネットワーク接続デバイスは数多く存在します。このクラスのデバイスには、ネットワーク プリンタ、コピー機から、OS が埋め込まれているデバイス、OS が強化されているデバイス、パーソナル ファイアウォールがイネーブルにされている PC まですべてが含まれます。NAC エージェントレス ホストと呼ばれるこれらのデバイスは、認証プロセスの異なるレベルで複数の方法を使って処理することができます。

表 1. NAC エージェントレス ホスト (NAH) の概要

NAH 処理方式	クレデンシャル	長所	短所
静的な NAD ホワイトリスト	MAC/IP アドレスまたは CDP デバイス タイプ ワイルドカード検索可能	シンプルで分散的な設定	アイデンティティ認証に弱い 分散型の静的なアドレス リストの管理が必要 中央のロギング機能なし
ACS の集中管理型ホワイトリスト	MAC/IP アドレス ワイルドカード検索可能	アドレス管理の一元化	アイデンティティ認証に弱い 静的なアドレス リストの管理が必要
ダイナミックなホストの監査	ネットワーク スキャン、 リモートログイン、または ブラウザ オブジェクト ダウンロードから入手したポストチャ	ダイナミックなポストチャベースの アセスメント 静的な MAC/IP アドレス リスト の管理が不要	追加の NAC コンポーネントの管理が必要

### 静的な NAD ホワイトリスト

Cisco IOS および CatOS は、MAC アドレス、IP アドレス、または Cisco Discovery Protocol (CDP) デバイス アイデンティティによってホストを静的に認証する機能を提供します。新しいホストを検出した NAD は、このホストの静的な許可が NAD 自体に予め設定されているとホストへのチャレンジを行いません。一方 ACS は、このホストの認証や許可の記録を求める RADIUS 要求を受け取りません。

## ACS での集中管理型のホワイトリスト

NAD は、静的にホストを許可できない場合、設定に応じて ACS にエージェントレス要求を送信することができます。ACS は、Network Access Restriction (NAR; ネットワーク アクセス制限) と呼ばれるホワイトリストで MAC または IP アドレスを検索し、発見するとこのホストを指定された許可グループに関連付けます。

### ダイナミックなホストの監査

ACS は、オプション設定によりホストの許可を監査サーバに委託することができます。監査サーバは、脆弱性アセスメント手法を使用して、通常の Request/Response チャレンジでは入手できないポストチャ クレデンシャルを取得する NAC コンポーネントです。この機能は、さまざまな技術を使用してホストのポストチャを特定する、サードパーティの脆弱性アセスメント ベンダが提供しています。次の表に各テクノロジーの概要を示しますので、お客様の NAC 導入に最適な技術を決断する際にご活用ください。

テクノロジー	長所	短所
ネットワーク スキャン	高速 管理対象・非対象ホストに対応	パーソナル ファイアウォールを使用するホストに対しては限定的なユーティリティ
リモート ログイン	リードオンリーの控えめなログイン	リモート ログインのために管理者アカウントが必要 非管理対象ホストに実施できない
ダウンロード可能なブラウザ オブジェクト	パーソナル ファイアウォールをバイパス	ブラウザ オブジェクトのダウンロードのためにユーザに操作が必要 ユーザのパーミッションがアセスメントの範囲を制限

NAC でのエージェントレス ホストの問題は、すべての組織が解決する必要があります。NAH の処理方法はいずれも理想的とは言えませんので、複数の NAH 処理方法を使用してエージェントレス ホストが関わるすべてのアドミッション シナリオを効果的に処理する必要があります。

## パッチ管理の統合

Cisco NAC フレームワークは、セキュリティ ポリシーに従って、アイデンティティとポストチャ クレデンシャルを基準にネットワーク アクセスを許可し実施させるアーキテクチャとメカニズムを提供します。NAC 対応ネットワークは、駆除、シグニチャファイルのアップデート、OS パッチ適用、クライアント ソフトウェア配布を行って直接非適合ホストの修復を行うわけではありません。ホストの実際の修復は、検疫ネットワーク セグメントを活用し、ユーザまたはサポート チーム自身が行うか、またはパッチ管理ソリューションを通じて行う必要があります。NAC の導入を成功させるためには、自動パッチ管理ソリューションと NAC の統合は不可欠です。

### プロセス

理想的な環境では、組織のクライアント ソフトウェア配布戦略とアンチウイルス サービスにより、すべてのシステムへのパッチの適用とアップデートがタイムリーに実施されます。これが実現すれば、すべてのホストが **Healthy** ポストチャを取得してネットワークへのアクセスが許可され、アイデンティティのみをベースにホストをセグメント化できます。このアップデート プロセスが失敗すると、理由に関わらず、ホストはネットワークによって検疫され、ホストとそのユーザはネットワーク上で非生産的な状態に置かれます。この場合、検疫によるユーザの生産性と体験への影響を最小限に抑えるために、できるだけ迅速にホストマシンを修復しなければなりません。

すべてのエンド ユーザに各自のシステムを脆弱でないウイルス フリーの状態に保つよう期待することは非現実的です。したがって組織は、検疫されたホストのパッチ戦略を確立する必要があります。サポート スタッフによるソフトウェア CD のユーザへの配布から、すべての必要なソフトウェアを保管する Web サーバ、パッチ ベンダが提供するパッチ管理ソリューションまで、

どのような手段もパッチング ソリューションとなります。できるだけ迅速かつ効率的にユーザを **Healthy** ポスチャに戻すために最適な手段を決定するのは、セキュリティ ポリシー チームの役割です。シスコでは、**NAC** と統合し、ネットワークの検疫が発生したときに自動的にパッチ適用を開始するサードパーティ製の専用パッチ管理ソリューションの使用を推奨します。

## 検疫時のパッチ適用

Cisco NAC フレームワークには、ポリシー サーバからエンドユーザ、CTA、そのポスチャ プラグインに対して通知を送信できる許可応答機能があります。この応答を通じて、ユーザはなぜネットワーク アクセスが制限されたのかを理解し、現在のセキュリティ ポリシーを詳細に説明する **Web** ページを表示し、パッチ クライアントを開いてアップデートをダウンロードできます。シスコでは、ネットワーク ポリシーの実施と検疫時のパッチの自動適用を緊密に統合したこのような連携的なセキュリティを実践することを推奨します。

パッチ管理ソリューション オプションを調査する前に、自社の導入にとってどのような **NAC** 通知機能が重要であるかを理解する必要があります。NAC では、次のような機能を利用できます。

- CAT ポップアップ ダイアログを通じたユーザへの通知
- CTA を通じてブラウザを自動的に起動し、特定の **URL** を表示する
- 特定の **URL** へのブラウザの **URL** リダイレクション
- ネットワーク許可または検疫によるパッチ クライアントの起動
- ネットワーク許可時のパッチ サーバの通知によるパッチ クライアントの起動

上記のリストをもとに、現在のパッチ ソリューションと統合が必要な機能があるかどうかを確認し、パッチ ベンダが提供するソリューションの調査の必要があるかどうかを判断できます。また、**NAC** プログラムに参加するベンダの製品と **NAC** フレームワークとの統合の度合いは、製品によって大きく異なることに注意してください。CTA プラグインを介してポスチャ クレデンシャルを提供するだけの製品もあれば、HCAP を介して **ACS** とポスチャ検証サービスを完全に統合し、カスタマイズされたクライアント通知を提供する製品もあります。最も効率的なパッチング ソリューションを容易に導入できるように、各パッチ ベンダに **NAC** 統合オプションを確認してください。

## NAC のスケーラビリティとアベイラビリティ

ほぼすべてのネットワークには何らかの **AAA** 機能がありますが、通常は **VPN** または **ワイヤレス** アクセス接続に対してのみ使用されています。**NAC** はこの概念に変革をもたらし、すべてのホストにネットワークの入り口でアクセス許可を要求するとともに、継続的なポスチャ検証を実施します。**AAA** インフラの活用をこのように拡大する場合、**AAA** サーバとその代理サーバは需要の拡大に合わせてスケーラブルであること、また重要なネットワーク サービスとして高度なアベイラビリティを提供することの 2 つの点が求められます。**AAA** インフラストラクチャのスケーラビリティとアベイラビリティを向上させられなければ、正当なユーザと健全なホストの生産性が損なわれる可能性があります。

**NAC** フレームワーク アーキテクチャは、拡張可能なセキュリティ ポリシーを集中管理し、非常に大規模でヘテロジニアスなネットワークのエッジでネットワーク アクセスを制御するために設計されています。このように設計されていますが、**NAC** を成功させるためには、アーキテクチャ内でパフォーマンスに影響する主要な要因と予測されるボトルネックを理解することが重要です。これにより、最も重要なコンポーネント、その必要数、パフォーマンスの調整で重要な領域を予測することができます。

### スケーラビリティ

**NAC** 導入のスケーラビリティは、実質的に 1 つの要素、つまり特定の期間内に完了する許可数で測定されます。この数値は、通常 1 秒あたりのトランザクション数 (**TPS**) で表します。

## ユーザとホスト

ユーザとホストの数で測定するネットワークの規模は、NAC インフラストラクチャのスケラビリティを決定する際に最初に考慮する要素です。この数値をもとに、AAA サーバで発生する 1 日当たりの最小許可数を割り出すことができます。組織のセキュリティ ポリシーでユーザのアイデンティティのみ、またはホストのポスチャのみの認証を要求する場合は、両方を割り出す必要はありません。

また、1 日に発生するユーザの行動にも考慮が必要です。ユーザは、1 日のうちに VPN を介して自宅からネットワークにログインし、その後出勤してオフィスで LAN に接続し、ミーティング中にワイヤレスでローミングし、オフィスのデスクに戻りアップデートのインストール後にコンピュータを再起動し、自宅に戻って就寝前に VPN を介して電子メールをチェックすることもあるでしょう。セキュリティ ポリシーや使用するプロトコルによっては、これらの各イベントの発生時に追加の許可プロセスが開始される場合もあります。

管理者は、各ユーザが 1 日にコンピュータを再起動またはローミングする回数の平均値を算出し、AAA サービスにかかる平均的な負荷を割り出す必要があります。大きな問題となるのは、比較的短時間に数百または数千のユーザがアクセスを要求する、一時的な使用急増（スパイク）です。スパイクは、単純にすべてのユーザがデスクトップ コンピュータを立ち上げる始業時や、予期しない停電によってすべてのリソースが同時にオンラインに復帰するときに発生します。予期可能な場合はこれらのイベントも考慮するようにしてください。

スケラビリティに関連してユーザとホストが影響を与えるもう 1 つの領域は、サーバとストレージ システムの規模です。バックエンド サーバには、大量のトランザクション処理能力に加え、より多くの RAM と ディスク ストレージが必要となります。発生する多数の新しい認証イベントや、プライバシーと監査証跡に関連する法規制を考慮すると、長期的なストレージのニーズは大幅に増大する可能性があります。

## Cisco Secure Access Control Server (ACS)

ネットワーク アドミッションのすべての要求は、Cisco Secure Access Control Server (ACS) による許可が必要です。Cisco Secure ACS は、すべての NAC 許可の決定を統合する 中心的なポリシー エンジンであり、現在すべての NAC プロトコルおよび方式をサポートしている唯一の AAA サーバです。したがって Cisco Secure ACS は、NAC 環境を拡張する際にアーキテクチャ内で最も重要な単一のコンポーネントです。Cisco Secure ACS とセキュリティ ポリシーの一部の要素は、Cisco Secure ACS のスケラビリティに大きな影響を及ぼします。

### プロトコル許可レート

ネットワーク認証プロトコルの選択肢は数多く存在します。それぞれのプロトコルが提供するセキュリティや機能のレベルは異なり、そのレベルが認証レートに直接反映されます。非常にシンプルで安全性の低い Request/Response プロトコルもあれば、トンネルのカプセル化のネゴシエーションや必要なクレデンシャルの転送のためにホストと AAA サーバ間で多くのラウンドトリップを必要とするプロトコルも存在します。NAC で必要な平均 ACS サーバ数は、選択した認証プロトコルの許可レートと TPS 数に基づいて算出することができます。

### NAC タイマー

NAC では、ネットワークのスケラビリティに影響を与える複数のタイマーが使用されます。各 NAD の Cisco IOS には各タイマーのグローバル デフォルト値が設定されます。これらのグローバルな IOS 値は、IOS 設定コマンドや、ACS のセッションベースで無効にされる可能性があります。NAC の導入当初は、比較的長い間隔にタイマーを設定しておき、許可処理のパフォーマンスに応じて間隔を短くすることを推奨します。

## セッション タイムアウト/再検証

Session Timeout (RADIUS アトリビュート 27) は、NAC におけるユーザとホストのクレデンシャルの完全な再認証プロセスを開始します。Session Timeout は、ネットワーク内の各ホストの再認証期間をコントロールするため、AAA のスケーラビリティに影響を及ぼす最も重要なタイマーです。

### EAP over UDP ステータス クエリー

EAP over UDP (EoU) プロトコルは、レイヤ 3 (L3) 接続を介してホストにポスチャを求めるチャレンジ要求で使用されます。RADIUS Session Timeout による再検証と再検証の間に、NAD は Status Query (SQ ; ステータス クエリー) を実行して許可されたホストに定期的にポーリングします。ステータス クエリーは、次の 3 つの機能を提供します。

1. 前回許可された IP アドレスにホストが現在も存在するかどうかを検出します。ポーリング以外に、ホストがレイヤ 3 ネットワークとの接続を切断したかどうかを把握する方法はありません。
2. ACS が許可時に提供した EoU セッション キーを使用し、ホストが同一であることを暗号を使って確認します。この確認が失敗すると、再検証が発生します。
3. 最後の再検証またはステータス クエリー後のポスチャ変更の有無を Cisco Trust Agent に確認します。ポスチャに変更が発生している場合、ホストのポスチャは再検証されます。

ステータス クエリーは、NAD がホストに対して開始する軽量のオペレーションで、NAD のパフォーマンスにほとんど影響を及ぼしません。このタイマーを使用することにより、NAD は再検証より短い間隔で非同期でポスチャの変更を検出することが可能になり、ACS による頻繁な再検証の必要性を低減できます。

### 保留期間

EAP over UDP で許可されない NAC エージェントレス ホストは、デフォルト ネットワーク アクセスが与えられたままの状態になります。この場合、保留タイマーが失効するまでエージェントレス ホストに対する次のポスチャのチャレンジは行われません。これにより、許可の開始を再三試みて DoS 攻撃 (サービス拒絶攻撃) を仕掛けようとするホストを効果的に放置できます。

### その他のスケーラビリティの制限要素

ACS の設定には、実際のパフォーマンスに影響を及ぼさないものの、一部の導入シナリオでのスケーラビリティを制限する要素が他にも存在します。

- ACS は、ネットワーク アクセス デバイスとして最大 50,000 のアドレス可能エントリをサポートします。各 NAD で使用される個別の IP アドレスを使用する代わりに、IP アドレス範囲の使用を検討する必要があります。ACS の GUI を使用して NAD のリストを継続的にアップデートする必要性をなくするために、ベスト プラクティスとして単一のワイルドカード エントリ (\*. \*.\*.\*) の使用を推奨します。
- NAC エージェントレス ホスト シナリオでは、ホワイトリスト内の MAC アドレスとのマッチングを行う Mac-Auth-Bypass 認証が使用されます。ACS に登録できる MAC アドレス数は、ネットワーク アクセス プロファイル (NAP) 当たり 10,000 に制限されています。
- ACS は、MAC アドレス マッチをベースにホスト ポスチャの決定を監査サーバに委託できます。ACS は、監査サーバ設定当たり 1024 までの MAC アドレスをサポートしています。

## スケーラビリティの計算

次に、Cisco NAC の導入で使用する Cisco Secure ACS 数を割り出すために推奨する方法を説明します。特定の規模のユーザーデータベースのサポートに必要な ACS 数は、多くの要因によって異なります。まず、ユーザ当たりの 1 日平均最小トランザクション数を 1 回と考え、次のような予想可能なタイマー値や動作に基づいて、平均トランザクション数を増やしていきます。

- RADIUS セッション タイムアウト値
- VPN リモート アクセス ログイン
- 有線およびワイヤレス ネットワーク インターフェイスでのマルチホーム アクセス
- ワイヤレス ローミング
- パッチの適用、汎用オペレーティング システム、アプリケーションの異常に起因するコンピュータの再起動
- ユーザ当たりのデバイス数 (デスクトップ、ラップトップ、PDA など)
- ホストのポストチャが変更される頻度

この時点で割り出したユーザ当たりのトランザクション数を使用して、1 日当たりのトランザクション数を算出します。

$$\text{Transactions\_per\_Day} = \text{Transactions\_per\_User\_per\_Day} \times \text{Number\_of\_Users}$$

この値を、1 日の秒数で割って TPS に変換します。

$$\text{Transactions\_per\_Second} = \text{Transactions\_per\_Day} / (24 \times 60 \times 60)$$

この平均トランザクション レートと ACS 認証プロトコルの許可レートから、必要な Cisco Secure ACS サーバの最小数を算出します。

$$\text{ACS\_Count} = \text{Transactions\_per\_Second} / \text{ACS\_Protocol\_Authorization\_Rate}$$

この数字は、1 日の全時間帯の平均値で、常に 100 % の負荷がかかっていることを想定し、ポリシーの複製や保守によるサーバのダウンタイム、時折発生するリンクのダウンを考慮していないため、絶対最小値です。この最小 ACS 数を 0.4 で割った値を、実際のレートと負荷を確認できるまで暫定的な値として使用することを推奨します。プロトコル許可レートを、使用するネットワーク アクセス方式で重み付けすることにより、最終的な ACS 数の精度を高めることができます。

## ロード バランシング

NAC 環境の ACS のパフォーマンスを向上させるために、ACS サーバにはロードバランシングとフェールオーバーを設定できます。ロード バランシングは、次の 3 つのいずれかの方法で行うことができます。

1. IOS RADIUS サーバ フェールオーバー
2. IOS サーバ ロード バランシング (SLB)
3. Content Services Switch または Content Services Module を使用したロード バランシングとフェールオーバー

### IOS RADIUS サーバ フェールオーバー

認証サーバのフェールオーバーは、IOS の 12.1 からサポートされています。このコンセプトでは、1 つのネットワーク アクセス デバイ스에複数の RADIUS 認証サーバを設定する必要があります。アクセス ルータに 3 つの RADIUS サーバが設定されています。RADIUS サーバ 1 に障害が発生すると、設定されたタイムアウト期間の経過後にルータは自動的に RADIUS サーバ 2 に接続し、2 つのクライアントを認証します。同様に、RADIUS サーバ 2 に障害が発生すると、ルータは RADIUS 3 サーバを使用してクライアントの認証を試みます。タイムアウト期間は、次のコマンドを使用して設定できます。

複数のコマンド オプションを使用して認証試行中のルータのパフォーマンスを制御することができます。

- **Timeout** — ルータが要求を再送信する前に、RADIUS 要求への応答を待機する秒数を指定します。Timeout のデフォルト値は 5 です。
- **Retransmit** — RADIUS 要求をサーバに再送する回数を指定します。デフォルト値は 3 です。
- **Deadtime** — RADIUS 認証要求が認証要求に回答しない RADIUS サーバをバイパスする分数を指定します。デフォルト値は 10 分です。

これら 3 つの設定に適切な値を設定することにより、ルータの認証パフォーマンスを改善できます。1 つの ACS サーバから別の ACS サーバへのフェイルオーバー時間を最小限に抑えるためには、フェイルオーバー開始までの時間を短縮する値を設定する必要がありますが、設定を短縮しすぎて、ルータに不必要なタイムアウトを発生させ、応答するサーバを非応答とみなすことがないようにしてください。テストの結果から、デフォルト設定値で ACS フェールオーバー中に NAC は優れたパフォーマンスを維持できることが分かっています。必要な場合は、Retransmit の回数を 3 回から 2 回に、Timeout を 5 秒から 3 秒に、Deadtime を 2 分に変更します。これにより、ルータが ACS サーバが応答しないと判断し、次のサーバに切り替えるまでの時間が 6 秒になります。また、非応答サーバには復元または再起動までに 2 分間与えられます。

**aaa group server** コマンドによって既存のサーバ ホストをグループ化し、設定されたサーバ ホストのサブセットを選択して特定のサービスのために使用することができます。Cisco IOS で複数の RADIUS サーバを設定する方法については、[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_configuration\\_guide09186a008017d583.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html) を参照してください。

### IOS RADIUS サーバのロード バランシング

7200 ルータおよび 6500 シリーズ スイッチ プラットフォームでサポートされている RADIUS サーバ ロード バランシング機能は、IOS を通じて実施できます。このケースでは、上記の説明のとおり RADIUS サーバが AAA サーバ グループに配置されています。さらに、AAA サーバ グループの NAC 認証のパフォーマンスを最適化するために、ロード バランシング アルゴリズムを(デフォルトの「Weighted Round Robin」から)「Weighted Least Connections」に設定します。

上記の例では、RADIUS 認証 (UDP 1812 番ポートで発生) と RADIUS アカウンティング (UDP 1813 番ポートで発生) 両方の認証のロード バランスを行います。sticky コマンドは、クライアントの接続間の間隔が指定された期間を超えない場合に同一のクライアントからの接続が同一の実サーバを使用するように指定します。また、両方の仮想サーバが同一の sticky グループ (group 1) および同一のサーバ ファーム (AAAFARM) に設定されています。クライアントがどちらかの仮想サーバにアクセスすると、このクライアントの IP アドレスが group 1 の IOS SLB データベースに追加され、最初の RADIUS アクセス要求のために選択された実サーバと関連付けられます。このクライアントからの次の要求は、どちらの仮想サーバに対するものでも常に同一の実サーバに送信されます。上記の設定により、sticky データベースは、無活動期間の 86,400 秒間エントリを保管します。

### Content Services Switch を使用した RADIUS サーバのロード バランシング

NAC 認証デバイスと Cisco Secure ACS サーバ間の認証要求のロード バランスのために、Cisco Content Services Switch (CSS) または Cisco Content Switch Module (CSM) などのネットワーク ロード バランシング デバイスを同様に使用できます。この設定では、NAD は CSS または CSM に設定された仮想 ACS サーバを表す仮想 IP アドレスを参照します。

**注:** サイト間でのフェールオーバーを設定することも可能ですが、同一 LAN 上にローカルのフェールオーバーシステムを構築することを推奨します。これによって、ローカル ネットワークで高速で信頼性の高い認証を行うことができます。ロード バランシングも同様の方法で実施できます。

## NAC 設計時の考慮事項

### NAC アセスメント方式

NAC は、すべてのネットワーク アクセス媒体に適合ポリシーを適用するために、さまざまなアセスメント方式で実施できます。各方式は、各アクセス媒体に対して個別に適用することも、ネットワーク内の複数のロケーションで適用することもできます。ネットワーク設計者は、アセスメント方式を詳しく理解し、自社のセキュリティ ポリシーに最適なアセスメント方式を選択する必要があります。アセスメント方式の選択にあたって、主に次の 5 つの点を考慮してください。

- 開始メカニズム
- 要求されるクレデンシヤル
- 許可機能
- 非応答のエージェントレスホスト (NAH) の処理
- NAD のスケーラビリティ

ここでは、NAC アセスメント方式に関連する設計時の一般的な考慮事項について説明します。各アセスメント方式の特定のプラットフォームの考慮事項は、このガイドの後半で詳しく説明します。これから説明する事項をまとめた表をこのセクションの最後に掲載します。

#### NAC L3 IP

NAC L3 IP は、2004 年夏の NAC の初期リリースの一部として初めに導入されたアセスメント方式です。

NAC 対応の Catalyst スイッチで NAC L3 IP を使用する際の最初の考慮点は、NAC L3 IP ポスチャ検証プロセスの開始方法と NAH への対応です。NAC L3 IP と NAC L2 IP は、共にポスチャのみのクレデンシヤルを検証し、同一の許可機能 (URL リダイレクション、Downloadable ACL) をサポートする非常に似たアセスメント方式であるため、ネットワーク設計者は NAC L3 IP の特徴を詳しく理解する必要があります。

この 2 つのアセスメント方式の 1 つめの違いについては、このガイドの「Cisco NAC : アーキテクチャとシステム コンポーネント」のセクションですでに説明しました。NAC L3 IP は、IP アドミッション ACL が設定されたルータ インターフェイスに到着したレイヤ 3 パケットによって開始される点で NAC L2 IP と異なります。NAC L2 IP は、スイッチ インターフェイスが ARP または DHCP トラフィック (オプション) を受信したときに開始されます。両方式とも インターフェイス ACL でデフォルトのセキュリティ ポリシーを適用しますが、NAC L3 IP の場合、この開始 ACL をカスタマイズできるので、開始ポリシーをさらに柔軟に設定できます。したがって、ネットワーク管理者は NAH デバイス タイプ (プリンタなど) を処理するオプションが得られます。この開始メカニズムの違い、そして NAC L3 IP をサポートするプラットフォーム (IOS ソフトウェアベースのルータ、VPN 3000) から、NAC L3 IP は、主に集約 (WAN、VPN、WLAN など) のためのアセスメント方式として位置づけられます。ただし Catalyst レイヤ 3 スイッチが現在 NAC L3 IP をサポートしていないため、現在の導入オプションでは、キャンパス インフラストラクチャのディストリビューション レイヤで NAC L3 IP は使用できません。ディストリビューション レイヤに 7200 などの高速 IOS ルータを配置するオプションもありますが、ディストリビューション レイヤで求められるトラフィックの集約スルーputtを考慮すると、多くの場合これらのルータは使用できません。

2 つめの違いは、NAC L3 IP ではパートナーの監査サーバを介した NAH の監査を行えないことです。現在の IOS リリースはこのエージェントレス ホスト処理シナリオをサポートしていません。この機能は、NAC 対応の IOS ベースのソフトウェア ルータの出荷により、6 ヶ月以内にサポートされる予定です。VPN 3000 などのその他の NAC L3 IP 対応デバイスについては、NAH の監査サポート対応時期は未定です。

また、NAC L3 IP では、NAD のスケーラビリティに関連するパラメータが他のアセスメント方式とは異なります。現在 NAC L3 IP をサポートしているデバイスはソフトウェアベースのフォワーディング デバイスであるため、NAC のスケーラビリティについては主に次の要素を考慮する必要があります。

- NAC L3 IP のフォワーディング パフォーマンス
- NAC L3 IP 同時セッションのメモリ消費
- セッション存続時間とステータス クエリー タイマーのプロセッサ消費
- デバイスが処理可能な同時 NAH 数

これらのスケーラビリティ関連事項のうち、下の 2 つの要素はネットワーク管理者が設計プロセスで調整できます。

管理者が調整できる最初の要素は、セッション存続時間とステータス クエリー タイマーのプロセッサ消費です。セッション存続時間タイマーは、頻繁に完全なアセスメントを実施するために使用します。この値が低すぎると、より頻繁にポスチャ要求が ACS に送信され、ポスチャ アセスメント要求を処理する ACS の機能に直接影響が及びます。したがって、セッション存続時間タイマーの値が低すぎる場合、必要な ACS サーバ数が増大する可能性があります。一方ステータス クエリー タイマーは、ポスチャの変更や新しいレイヤ 3 ホストを迅速に検出するために使用されます。ステータス クエリー タイマーの値を (NAD または ACS で) 低く設定しすぎると、多数のデバイスをサポートする NAD のプロセッサ使用率が高くなり、NAD は重要なコントロール プレーン機能を実行できなくなることがあります。これらの要素を考慮して、「Healthy」ホストのポスチャ アセスメントを実施する場合は、セッション存続時間およびステータス クエリー タイマーをデフォルト値から変更しないことを推奨します。また、これらのタイマーを低い値に変更するのは、ポスチャ アセスメントで「Quarantine」または「Infected」と判断されたデバイスのポスチャ アセスメント変更をより頻繁にチェックする必要がある場合のみにしてください。

管理者がスケーラビリティに関連して考慮する 2 つめの要素は、現在 IOS ベース ルータ プラットフォームでは、プラットフォーム上で同時に存在可能な NAH セッションのデフォルト値が 100 に設定されている点です。このしきい値に到達すると、NAD はこれ以上 EAPoUDP セッションを生成せず、NAC セッション テーブルから EAPoUDP または NAH デバイスが削除されるまでデフォルト インターフェイス ポリシーを適用します。NAC L3 IP を使用する NAD で 100 の NAH セッションが同時に存在することはまれですが、環境への NAC の導入時にはこの状態が発生する可能性があります。たとえば、ネットワーク管理者がクライアントに CTA を配布する前に NAC をイネーブルにした場合です。IOS ベースのプラットフォームでは、この値は `ip admission ratelimit<100-1000>` コマンドを使用して変更できます。すべてのデータ プレーンおよびコントロールプレーントラフィックは、NAC L3 IP プラットフォーム上の汎用 CPU によって処理されるため、スケーラビリティに関連するこれらの考慮点の値は、プラットフォームのパフォーマンス値に依存します。

またネットワーク管理者は、ポスチャ検証タイマーが失効した後の NAD のターミネート アクションの設定も設計時に考慮しなければなりません。シスコでは、IETF RADIUS Termination Action アトリビュート 29 を使用して ACS にターミネート アクションを設定することをネットワーク管理者に推奨します。ACS に「RADIUS 要求」としてターミネート アクションが定義されていない場合、NAC L2 IP セッションはデフォルト設定によってセッション テーブルから削除され、完全なポスチャ アセスメントを開始するトラフィックが生成されるまで、接続デバイスにデフォルト インターフェイス ACL セキュリティ ポリシーが適用されるためです。この場合、クライアントが実行中のアプリケーション セッションは、完全なポスチャ アセスメント時に中断する可能性があります。IETF RADIUS Termination Action (アトリビュート 29) が RADIUS Access-Accept とともに送信されると、完全なポスチャ アセスメントの実行中もこの NAC セッションは維持されるため、クライアントはこの間もアプリケーション セッションを継続できます。

さらに管理者には、NAC L3 IP の導入の際に、まず NAC を監査モードで導入することを推奨します。これは、初期導入ですべてのポスチャ アセスメント トークンに対する NAC 許可を「permit ip any any」を設定することを意味します。これによりネットワーク管理者は、環境への NAC の導入によってヘルプ デスクに負荷が増加したり、許可の拒否によってアプリケーションが

使用不能になる事態を最小限に抑えることができます。NAC は、監査モードでも NAC デバイスを識別できるほか、エンド デバイスの適合性レベルに関する重要なレポートを提供できます。

## NAC L2 IP

すでに説明したように、NAC L2 IP は NAC L3 IP と同様にトランスポート メカニズムとして EAP over UDP を使用し、ポスチャのみのクレデンシャル アセスメントを行います。また NAC L3 IP のように、スイッチ ポートのデフォルト ポリシーは、インターフェイス ACL です。一部のケースでは、ネットワーク管理者がデフォルト インターフェイス ACL で何を許可するべきかを考慮する必要があります。たとえば、NAC L2 IP ポートが IP 電話をサポートする必要がある場合、ネットワーク管理者は IP 電話が起動し、プロビジョニングを行うために、どのようなポートが必要かを考慮し、これらのポートをインターフェイス ACL に追加しなければなりません。また、NAC のポスチャ アセスメントはネットワークの入り口で実施されるため、ネットワーク管理者は Windows ドメイン ログイン、グループ ポリシー アップデート、ログイン スクリプトなどのネットワーク機能へのインターフェイス ACL の影響も考慮する必要があります。たとえば、ネットワーク管理者がこのような Windows 機能をすべて許可する必要がある場合、NAC L2 IP のインターフェイス ACL に次のポートを追加できます。

- 88 kerberos
- 445 domain -smb direct host
- 389 domain ldap
- 123 domain ntp
- 135 domain rpc endpoint mapper
- 1026 domain ntds

ネットワーク管理者は、このような設定によって Microsoft Windows ネットワーキング システムを継続して機能させることができます。ただし、Windows ネットワーキング環境とのこのシームレスな統合は、マルウェアがかってこれらのポートを活用して企業に感染を広めたことを配慮して行わなければなりません。インターフェイス ACL へのポートの追加と除外は、ネットワーク管理者が判断するビジネス リスクの問題です。

すでに説明したように、NAC L2 IP と NAC L3 IP との大きな違いは、NAC L2 IP が ARP または DHCP トラフィックによって開始される点です。NAC L2 IP セッションは、ARP プロブを使用して行われる定期的なステータス クエリーの「Are you still there?」メッセージにホストが応答するか、終了されるまでアクティブです。セッションは、次のイベントによって終了できません。

- APR プロブ タイムアウト
- CLI によるセッション ターミネート
- AAA サーバからの RADIUS Access Accept がセッション タイムアウトによるセッションの削除を指示したとき

NAC L2 IP の NAD の ACL はハードウェアに実装され、NAC セッション数はプラットフォームのハードウェアによって制限されるため、NAC L2 IP の NAD については、設計時の負荷のフォワーディングや同時セッションの影響の考慮点は限られています。NAC L2 IP の設計上の大きな考慮事項は、NAC L3 IP と同様に、セッション存続時間およびステータス クエリー タイマーのプロセッサ消費量です。セッション存続時間タイマーは、NAC L3 IP と同じように NAC L2 IP でも ACS のスケラビリティに影響を及ぼします。また、ステータス クエリー タイマーもコントロール プレーンの CPU 使用率に直接影響を与えます。NAC L2 IP でもステータス クエリー タイマーの値を (NAD または ACS で) 低く設定すると、スイッチ コントロール プレーンの CPU の使用率が高くなり、スイッチが重要なコントロール プレーン機能を実行できなくなることがあります。したがって、ここでも「Healthy」ホストのポスチャ アセスメントを実施する場合は、ポスチャ検証およびステータス クエリー タイマーの値をデフォルト値から変更しないことを推奨します。また、これらのタイマーを低い値に変更するのは、ポスチャ アセスメントで

「Quarantine」または「Infected」と判断されたデバイスのポスチャ アセスメント変更をより頻繁にチェックする必要がある場合のみにしてください。

ポスチャ検証タイマーが失効した後の NAD のターミネート アクションの設定も設計時に考慮が必要です。シスコでは、IETF RADIUS アトリビュート 29 を使用して ACS にターミネート アクションを設定することをネットワーク管理者に推奨します。ACS に「RADIUS 要求」としてターミネート アクションが定義されていないと、NAC L2 IP セッションがデフォルト設定によってセッション テーブルから削除され、完全なポスチャ アセスメントを開始するトラフィックが生成されるまで接続デバイスにはデフォルト インターフェイス ACL セキュリティ ポリシーが適用されるためです。この場合、クライアントが実行しているアプリケーション セッションは、完全なポスチャ アセスメント中に中断する可能性があります。IETF RADIUS Termination Action (アトリビュート 29) が RADIUS Access-Accept とともに送信されれば、完全なポスチャ アセスメント中もこの NAC セッションは維持されるため、クライアントは完全なポスチャ アセスメント中もアプリケーション セッションを継続できます。

NAC L2 IP の大きなメリットの 1 つは、ポート当たり複数のホストをサポートするように設計されていることです。ネットワーク管理者は、NAC L3 IP と違い、NAC L2 IP ではサポート可能なポート当たりのホスト数の制限に注意してください。スイッチング プラットフォームによってハードウェア実装が異なるため、サポートするポート当たりのデバイス数はプラットフォームによって異なります。

NAC L2 IP の導入についての最後の推奨点は、NAC L3 IP と同じように、まず NAC を監査モードで導入することです。これは、初期導入ですべてのポスチャ アセスメント トークンに対する NAC 許可を「permit ip any any」を設定することを意味します。これによりネットワーク管理者は、環境への NAC の導入によってヘルプ デスクに負荷が増加したり、許可の拒否によってアプリケーションが使用不能になる事態を最小限に抑えることができます。NAC は、監査モードでも NAH デバイスを識別できるほか、エンド デバイスの適合性レベルに関する重要なレポートを提供できます。

## NAC L2 802.1X

NAC L2 802.1X 規格は、LAN トランスポートを介して EAP メッセージを伝送するプロトコルと、このトランスポートを使用して第一ホップの L2 ポート上で NAC をサポートすることを定義しています。

NAC L2 802.1X にはステータス クエリー メッセージに相当する機能がないため、NAD がクライアントの再アセスメントを実施するための唯一の方法は、NAD のセッション存続時間タイマーを低く設定して完全な 802.1x トランザクションを開始することです。ただし、これはスイッチと ACS に大きなオーバーヘッドをかけるため、最適なソリューションとは言えません。

NAC で 802.1x オーセンティケータとして機能する NAD は、次の状況で EAP 交換を開始する必要があります。

- ホストが最初にネットワークに接続したとき
- AAA ポスチャ検証ポリシーに変化がないかどうか（新しい AV シグニチャ ファイルが公開されたなど）を確認するために、スイッチ上で定期的な再認証を開始するとき
- クライアントのポスチャの変更、または認証クレデンシアルの変更時に、クライアントが EAP 交換を開始したとき

EAP 交換を開始する NAD の制限のために、CTA は NAC 対応ネットワークに対する通知機能を装備しました。この機能は、CTA の「非同期ステータス クエリー (Asynchronous Status Query)」と呼ばれ、CTA ポスチャ プラグインのステータスが変更されると、変更されたステータスと NAC ネットワークのアドミッション ポリシーを比較するためにアイデンティティおよびポスチャ クレデンシアル クエリーを再開する必要があることをネットワークに通知します。CTA は、2 つの方法で非同期ステータス クエリーを開始できます。

1 つめは、CTA が EAPOL-Start メッセージを送信して新しい EAP 交換を開始するようにポスチャ プラグインをプログラムする方法です。Cisco Security Agent (CSA) は、CSA バージョン 4.5.1 からこの機能を実装しています。このバージョンでは、CSA

の稼働ステータスに変更があるたびに、非同期ステータス クエリーを開始できます。たとえば、「Healthy」アドミッション ポリシーで指定されている CTA のネットワーク アクセス要件がアクティブであることとします。ポストチャ クレデンシャルを提供したときに CSA はアクティブであったため、アドミッション ポリシーに適合し、ホストはネットワークにアクセスします。次に、悪質（ワームまたはウイルス）または悪質でない（エンドユーザ）アクションによって CSA がディセーブルになり、CSA の稼働ステータスに変更されたとします。この変更によって、CSA から CTA、そして CTA サブリカントへの非同期通知が開始され、スイッチに EAPOL-Start が送信されます。この EAPOL-Start は、新たに NAC アイデンティティおよびポリシー クレデンシャル検証を開始しますが、CSA は稼働ステータスが非アクティブであるため、「Healthy」アドミッション ポリシーに適合しません。結果として別のアドミッション ポリシー（たとえば「Infected」）が適用され、新しい許可ポリシー（通常はダイナミックな VLAN 割り当て）がスイッチに送信され、CSA のステータスがアクティブに変更されるまでこのデバイスは隔離されます。CSA のステータスがアクティブに変更されると、上記の説明と同じような順序で再度 NAC アイデンティティおよびポストチャ クレデンシャル チェックが開始されます。これで PC が「Healthy」アドミッション ポリシーに適合すると、スイッチ上の「Healthy」VLAN に戻されます。

もう 1 つは、CTA の非同期ステータス タイマーを使用する方法です。このタイマーが失効すると、CTA 内の機能が始動し、登録済みのすべてのポストチャ プラグインに対してポーリングを行います。いずれかのポストチャ プラグインがステータスの変更をレポートすると、CTA はすべての既存セッションに EAPOL-Start を送信します。この非同期タイマーは、300 秒に設定されています。この値は CTA にハードコーディングされているため、ネットワーク管理者は修正できません。

NAC L2 IP と同様に、ポストチャ検証タイマーが失効した後の NAD のターミネート アクションの設定も設計時に考慮しなければなりません。シスコでは、IETF RADIUS Termination Action アトリビュート 29 を使用して ACS にターミネート アクションを設定することをネットワーク管理者に推奨します。ACS に「RADIUS 要求」としてターミネート アクションが定義されていない場合、NAC L2 802.1x ステート マシンは完全な再検証中にデフォルトで「認証済み > 切断 > 認証中 > 認証済み」にステートを移行します。ステート マシンは「切断」ステートに移行すると、ポートで EAPOL 以外のすべてのトラフィックを拒否します。この場合、クライアントが実行しているアプリケーション セッションは、完全なポストチャ アセスメント中に中断する可能性があります。IETF RADIUS Termination Action (アトリビュート 29) が RADIUS Access-Accept とともに送信されると、NAC L2 802.1x ステート マシンは「認証済み > 接続中 > 認証中 > 認証済み」にステートが移行され、「切断」ステートには入らないため、デバイスは完全なポストチャ アセスメント中もトラフィックを継続して受け付けることができ、クライアントはこの間もアプリケーション セッションを継続できます。

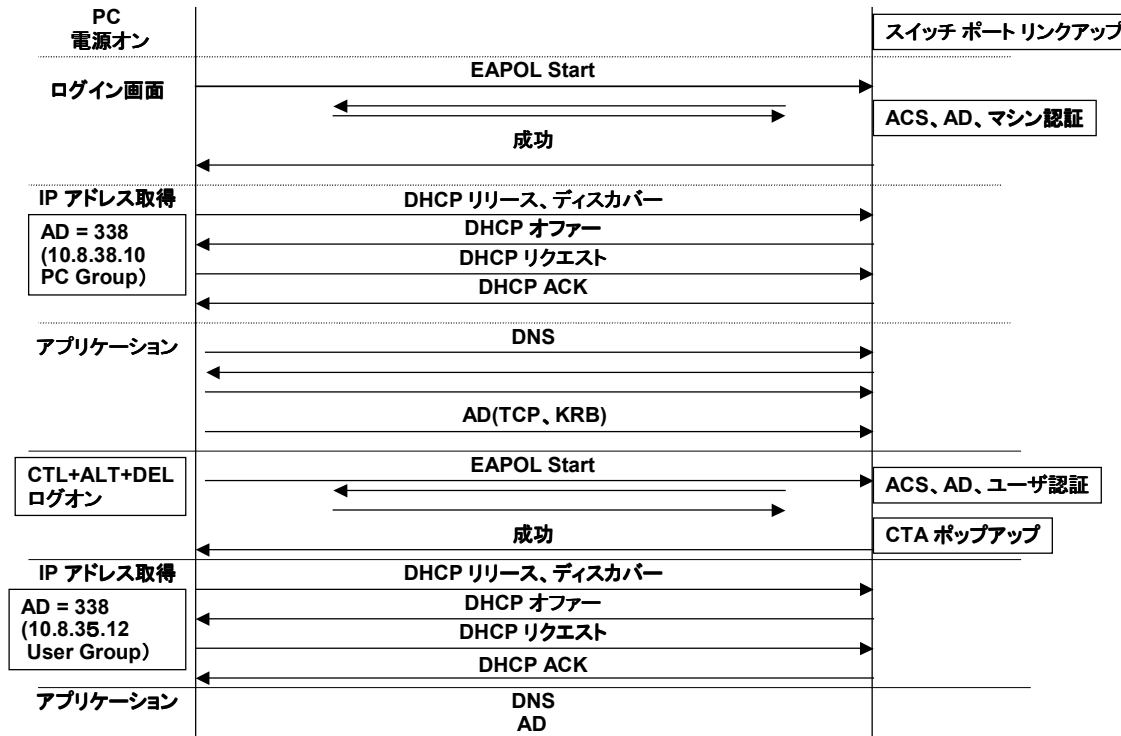
## CTA と Windows のブート シーケンス

Windows OS は、起動時に 802.1x を介してマシン認証を行い、Windows ドメイン コントローラと通信してマシン グループポリシーを取得できるので、802.1x の使用によってドメイン GPO が機能しなくなる問題が解消されます。

GINA が表示されたら、ユーザはコンピュータまたは Windows ドメインにログインすることができ、ログインに使用したユーザ名とパスワードを 802.1x 認証のアイデンティティ クレデンシャルとして使用できます。この 2 つめのタイプのクレデンシャルは、ユーザ認証と呼ばれています。

CTA と CTA に付属する有線サブリカントの導入により、デバイスの起動シーケンスは Windows サブリカントを使用した場合の起動シーケンスと同様になりましたが、ネットワーク管理者は相違点に注意してください。たとえば、認証およびアセスメントが成功するたびに、CTA サブリカントはネットワーク ディスカバリを行い、VLAN 割り当てのために IP アドレスを更新する必要があるかどうかを確認します。この Windows と CTA の起動のフローのプロセスを次の図に示します。

# Windows と CTA の起動フロー



Courtesy of Hiromi Mizutani

© 2005 Cisco Systems, Inc. All rights reserved.

1

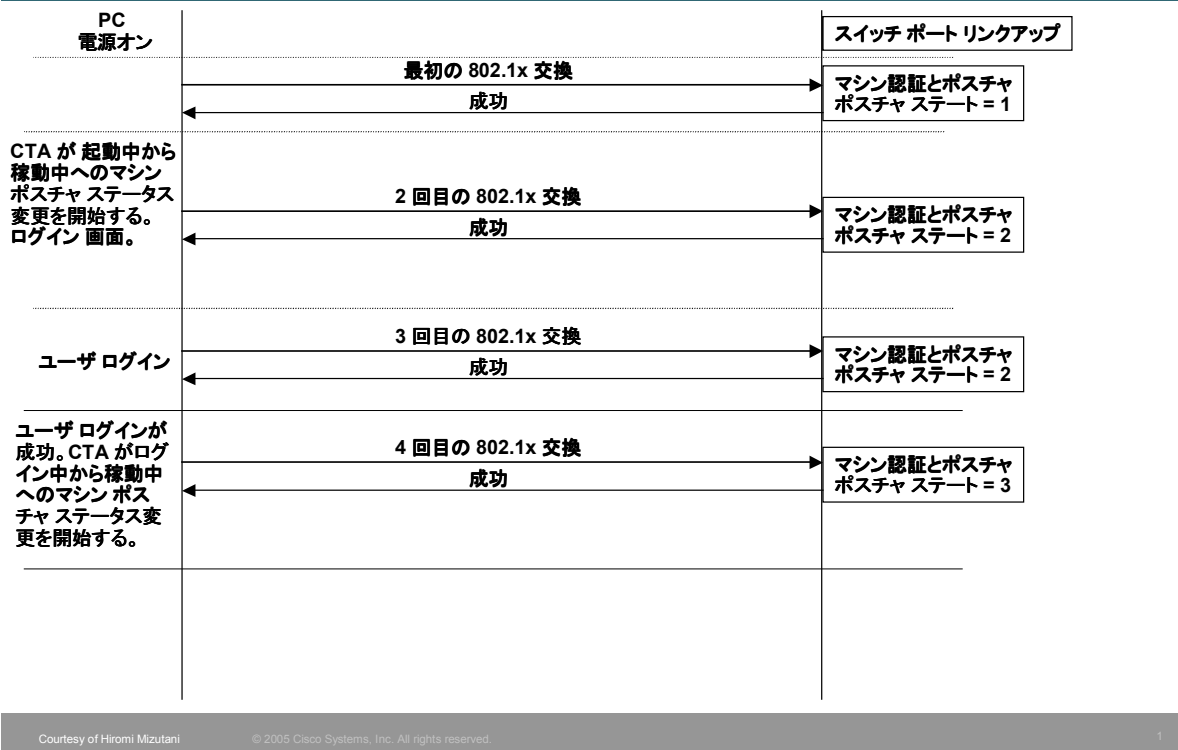
すでに説明したように、CTA 2.0 には、起動中でアプリケーション プラグイン情報が利用できない場合でも、アドミッションの決定に活用できるマシン ポスチャ ステートという新しい概念が導入されました。たとえば、起動時のアセスメントの際には AV サービスは起動していない可能性があります。マシン ポスチャ ステートの Booting (起動中) を使用して AV のインストールの有無のみのチェックが行えます。また、マシン ポスチャ ステートの Running (稼動中) を使用して AV のバージョンが正しいかどうか、またサービスの起動時にイネーブルにされるかどうかを確認できます。

マシン ポスチャ ステート クレデンシャルの使用は、NAC L2 802.1x に影響を与えます。マシン ポスチャ ステート クレデンシャルを問い合わせられている CTA は、マシン ポスチャ ステートが別のステートに移行されると EAPOL-Start トラフィックを生成して新しいポスチャ アセスメントを開始します。たとえば、マシンのステートが起動中から稼動中に移行した場合、CTA は サプリカントで EAPOL-Start を生成します。次に、マシンおよびユーザ認証シナリオとすべてのマシン ポスチャ ステートの手順と、その図を示します。

- マシンが起動する。
- サプリカントがポスチャとともにマシン認証を実行する (最初の 802.1x 交換)。
- マシン上のすべてのサービスが完了し、マシンのステートが起動中から稼動中に変更されたため、CTA がポスチャ ステータスの変更を開始する。
- サプリカントがポスチャとともにマシン認証を実行する (2 回目の 802.1x 交換)。
- ユーザがログインする。

- サプリカントがポストチャとともにユーザ認証を実行する（3 回目の 802.1x 交換）。
- ログインが完了し、マシンのステータスが稼動中からログイン中に変更されたため、CTA がポストチャ ステータスの変更を開始する。
- サプリカントがポストチャとともにユーザ認証を実行する（4 回目の 802.1x 交換）。

## Windows と CTA の起動フローとマシン ポスチャ



すでに説明したように、CTA は EAP-FAST を使用してマシンおよびユーザ認証を行います。ネットワーク管理者は、PAC がどのように CTA にプロビジョニングされるのかを理解する必要があります。

EAP-FAST は、3 つの基本フェーズで構成されます。

- フェーズ 0（オプション）：PAC が最初にクライアントに配布されます。
- フェーズ 1： PAC を使用してセキュアなトンネルが確立されます。
- フェーズ 2： 確立されたトンネルでクライアントが認証されます。

EAP-FAST 仕様では、PAC のプロビジョニング方法に、アウトオブバンド プロビジョニングおよびインバンド プロビジョニングの 2 つがあります。NAC L2 802.1x に対応する CTA サプリカントを使用する場合は、インバンド プロビジョニングでのみ PAC をプロビジョニングできます。CTA サプリカントは、ACS サーバによってインバンド プロビジョニングが許可されている場合で、クライアント側の認証がマシンに割当てられた証明書（マシン証明書）を使用して成功したマシン認証、または成功したユーザ認証の場合にのみ、ホストに PAC をプロビジョニングします。NAC L2 802.1x 対応の CTA サプリカントは、アウトオブバンド プロビジョニングをサポートしません。

NAC L2 802.1x 導入でも、NAC L2 IP および NAC L3 IP と同様に、まず NAC を監査モードで導入することをネットワーク管理者に推奨します。NAC L2 802.1x では、クライアントに対する主要な許可方式が VLAN 割り当てなので、監査モードの設定は他のアセスメント方式と若干異なります。ネットワーク設計者には VLAN 割り当てを返さないようにするか（クレデンシャルチェックが成功した場合もポートのデフォルト VLAN によりアクセスを許可する）、すべてのポストチャ アセスメント トークンに対して常に同一の VLAN 割り当てを返すことを推奨します。これによりネットワーク管理者は、環境への NAC の導入によってヘルプ デスクに負荷が増加したり、許可の拒否によってアプリケーションが使用不能になる事態を最小限に抑えることができます。また、サブリカントが認証に失敗すると、ユーザは 802.1x トランザクションにも常に失敗し、ネットワークへのアクセスを拒否されることに注意してください。

NAC L2 802.1x でも、監査モードからの段階的な導入をネットワーク設計者に推奨します。Microsoft ネットワーキング環境内では、マシン認証およびユーザ認証両方で VLAN 割り当てを実施すると、GPO および ログイン スクリプトが失敗する場合があります。ネットワーク設計者がマシンまたはユーザ認証いずれかのみで VLAN 割り当てを実施すると、通常この VLAN 割り当てでは正常に機能します。NAC L2 802.1x でポストチャおよびアイデンティティに対して VLAN 割り当てが発生する可能性がある場合は、ポストチャ アセスメントでネガティブなポストチャ トークンが返されたときのみ VLAN 割り当てを実施することをネットワーク設計者に推奨します。これにより、デバイスがアイデンティティおよびポストチャ クレデンシャル チェックに成功し、ポートのネイティブな VLAN または 同一の VLAN によってネットワークへのアクセスを許可されると、通常の Windows ネットワーキング機能は保証され、GPO およびログイン スクリプトは正常に機能します。一方、アイデンティティおよびポストチャ アセスメントで検疫または感染トークンが返されたときには VLAN が割り当てられます。このときは Microsoft ネットワーキング機能が正常に機能しなくなる可能性があります、「検疫」または「感染」トークンの場合はコンピューティング デバイスの基本機能に不具合があるので、不具合のあるデバイスを検疫して修復する代わりに通常の機能が利用できなくなると考えてください。

## IEEE 802.1X と NAC L2 IP

NAC 導入には、Microsoft OS のネイティブなサブリカントなどのポストチャ クレデンシャル チェックをサポートしない既存の IEEE 802.1x サブリカントを使用してホストのアイデンティティ クレデンシャルを検証し、ホストにネットワークへのアクセスを許可する方式もあります。この方式では、ホストのポストチャ クレデンシャルの検証に NAC L2 IP を使用できます。この階層型のアプローチは、次のいずれかの理由がある場合に必要となります。

- ホストに 802.1x 非対応のサブリカントがインストール済みで、IBNS ソリューション上に NAC が導入されている。
- ネットワーク管理者がアイデンティティおよびポストチャ クレデンシャルの検証を行うだけでなく、NAC L2 IP のみでサポートされている NAH 監査機能を利用する必要がある。

NAC L2 IP および 802.1x 両方のサポートは、NAD のスイッチポート単位で同時に設定可能です。

ネットワーク設計者は、この導入方式では ACS に 2 倍のトランザクションの負荷がかかること、そして 802.1x と NAC L2 IP の許可が別に行われることの 2 つの点に考慮する必要があります。これらの問題は、ともにネットワーク設計者が影響を低減できます。最初の問題は、サーバ ロード バランシング環境に ACS サーバを追加し、ACS をリニアに拡張することによって影響を低減できます。2 つめの問題は、すべてのクレデンシャル チェック許可方式を重複させないようにすることで影響を低減できます。たとえば、ネットワーク設計者は 802.1x による接続許可を Downloadable ACL を使用せずに VLAN 割り当てによるのみ実施し、NAC L2 IP は Downloadable ACL で接続許可を実行するようにします。

この解決策を適用するための詳しい設定方法については、『ネットワーク アドミSSION コントロール コンフィギュレーション ガイド』を参照してください。

## NAC エージェントレス ホスト (NAH)

NAC では、NAC またはその他の適合性許可を実施できないホストに対して複数の方法でネットワーク アクセスを許可することができます。プリンタ、スキャナ、コピー機、カメラ、センサー、バッジ リーダー、専用機器などのネットワーク接続デバイスがこのカテゴリに分類されます。また、サポートされていない OS、強化された OS、または埋め込み型の OS を搭載するコンピュータ、パーソナル ファイアウォールも NAH デバイスに該当します。

## NAC L2/L3 IP とエージェントレス ホスト

NAC L2 IP および NAC L3 IP では、エージェントレス ホスト処理に非常に柔軟に対応ができます。次のオプションを使用してエージェントレス ホストを処理できます。

- スイッチに設定する静的な例外
- ACS に設定する静的な例外
- エージェントレス ホストの監査 (NAC L3 IP では将来的にサポート)

スイッチには、ホストが特定の MAC または IP アドレスに基づいてポストチャ検証プロセスをバイパスできるようにする静的な例外を設定できます。CDP の静的な例外は、シスコ IP 電話のみをサポートします。

ACS にも、特定のホストが MAC アドレスに基づいてポストチャ検証プロセスをバイパスできるようにする静的な例外を設定できます。個別のアドレスまたはワイルドカード アドレスでの指定が可能です。

NAC L2 IP は (NAC L3 IP では将来的に)、パートナーの監査サーバを利用したエージェントレス ホストの監査も開始できます。ホストの監査実行後、監査サーバは監査の結果に基づいたポストチャ トークンを ACS に送信します。この結果は NAD に送信され、ACL および URL リダイレクションの形でポリシーが実施されます。この機能により、ネットワーク管理者はどのエージェントレス ホストにどのようなタイプのネットワーク アクセスを許可するかをきめ細かく決定することができます。

## NAC L2 802.1x とエージェントレス ホスト

NAC L2 802.1x 内では、管理者は次の複数のオプションを使用してエージェントレス ホストを処理できます。

- シスコ IP 電話のための CDP ベースの例外
- MAC Authentication Bypass
- ゲスト VLAN
- 認証失敗 VLAN

現在シスコは、CDP トラフィックを生成し、Catalyst スイッチに対して自身の認証を実行するシスコ IP 電話用の例外を作成するメカニズムを提供しています。この CDP の特定を通じ、スイッチはシスコ IP 電話を音声 VLAN に配置し、NAC プロセスから除外します。

MAC Authentication Bypass は、ポート単位で設定する IBNS 機能です。スイッチは、スイッチに接続しているホストの MAC アドレスを使って Cisco Secure ACS サーバに RADIUS 要求を送信します。この MAC アドレスが ACS の内部データベースで見つかった場合、ACS サーバは Access-Accept で応答を返し、ホストはネットワークへのアクセスを許可されます。この MAC 認証は 802.1x の後に発生するので、802.1x 認証を完了できないすべてのデバイスのアクセスを拒否するデフォルトの 802.1x セキュリティ ポリシーをバイパスします。MAC Authentication Bypass は、ネットワークへの NAH アクセスを許可できる有効な機能です。また MAC アドレスの Organizationally Unique Identifier (OUI; 組織固有識別子) を使用して MAC アドレスをワイルドカード指定することにより、同じ OUI 範囲内のアドレスを持つデバイスにネットワークへのアクセスを許可することができます。ネットワークへのアクセスを許可する必要がある場合でも 802.1x 対応サブリカントを持たないプリンタやターミナルなどのデバイスにとって便利な機能です。MAC Authentication Bypass はダイナミックな機能なので、ネットワーク管理者はネットワーク内のす

すべてのポートに設定することができ、プリンタが接続されるポートに明示的に設定する必要はありません。**MAC Authentication Bypass** は、本書作成の時点では Catalyst 6500 でのみサポートされています。

ゲスト VLAN により、802.1x 非対応ホストは 802.1x 認証を使用するネットワークにアクセスすることが可能になります。802.1x で会話しないデバイスに割り当てるゲスト VLAN は、ポート単位で定義できます。1 つの VLAN を 802.1x ゲスト VLAN として設定すると、すべての 802.1x 非対応ホスト (EAPOL-Identity Request に応答できないホストまたは EAPOL-Start を送信できないホスト) はこの VLAN に配置されます。ゲスト VLAN としては、プライベート VLAN および RSPAN VLAN を除き、任意の VLAN を設定できます。ポートがすでにゲスト VLAN 上に転送を行っているときに、そのホストのネットワーク インターフェイス上で 802.1x サポートをイネーブルにすると、このポートはただちにゲスト VLAN から外され、オーセンティケータが認証の発生を待機します。ポート上での 802.1x 認証をイネーブルにすると、802.1x プロトコルが開始されます。ホストが一定の時間内にオーセンティケータから送信されたパケットに応答できない場合、オーセンティケータはこのポートをゲスト VLAN に配置します。ゲスト VLAN は、シングル認証モードおよびマルチホスト モード両方でサポートされています。

ゲスト VLAN 機能と比較される機能が認証失敗 VLAN です。従来の 802.1x ポートの場合、スイッチは、アイデンティティ情報が認証サーバで認証されるまでこのポートに接続されているサブリカントにネットワークへのアクセスを提供しません。認証失敗 VLAN は、ポートベースで設定できます。サブリカントが 802.1x 認証に 3 回失敗すると、ポートは認証失敗 VLAN に配置され、サブリカントはここからネットワークにアクセスします。認証失敗 VLAN は、ゲスト VLAN から独立していますが、ゲスト VLAN と認証失敗 VLAN を同一の VLAN に設定することも可能です。802.1x 非対応ホストと認証失敗ホストを同一に扱う場合には、両方のホストを同一の VLAN (ゲスト VLAN または認証失敗 VLAN) に設定します。

認証失敗 VLAN は、トンネル化された大半の EAP 方式を使用する際は使用できません。これは、トンネル化方式が man-in-the-middle 攻撃を回避することを目的に設計されているためです。トンネル化方式では、認証サーバからサブリカントに EAP-Success (または Failure) が TLS トンネル内部で渡されます。また、オーセンティケータ (スイッチ) からサブリカントに EAPOL-Success (または Failure) も渡されます。トンネル化方式は、これらの 2 つの EAP メッセージの相互の整合性を保証することを目的に設計されました。認証は、暗号化された TLS トンネル内で EAP-Success メッセージが送信され、その後クリアテキストの EAPOL-Success が送信された場合にのみ成功します。サブリカント、認証サーバとも他のすべての組み合わせは無効とみなします。最初の EAP-Success メッセージは TLS トンネル チャネル内で保護されているので偽造できませんが、次のクリアテキストの Success および Failure メッセージは、攻撃者が送信することがあるためです。認証失敗のケースでは、サブリカントはトンネル内で (またはトンネル自体の) 認証失敗のメッセージを受信し、ステート マシンを保留状態に移行し、802.1x ステートマシンの起動を繰り返し試みます。サブリカントとスイッチはリンク上で 802.1x 会話を行っていたので、サブリカントは、リンクの先に 802.1x オーセンティケータが存在するとみなし、Access-Accept を受信するまで IP アドレス要求を行いません。しかし、スイッチは許可および転送ステートにポートを移行してしまい、サブリカントからの EAPOL-Start に応答しないため、サブリカントは Access-Accept を受信しません。PEAPv1 と EAP-FAST の 2 つは、TLS トンネル内で EAP ステータス メッセージを転送する主要なトンネリング プロトコルなので、認証失敗 VLAN はこれらの EAP 方式とともに使用できません。ただし、これは完全にサブリカントの動作に依存するため、ネットワーク管理者は、認証失敗 VLAN がネットワークに実装する EAP 方式およびサブリカントとともに使用できるかどうかを確認するためにテストを実施してください。

## NAH のまとめ

すべての NAH オプションを次の表にまとめました。

コンポーネント	方式	長所	短所
NAD	CDP 検出		
NAD	静的な MAC アドレス	アドレスのワイルド指定	ルータの第一ホップのみ 静的なリストの保守が必要
NAD	静的な IP アドレス	アドレスのワイルド指定	静的なリストの保守が必要
ACS	ネットワーク アクセス プロファイル フィルタ	集中管理型リスト アドレスのワイルド指定	静的なリストの保守が必要
ACS	MAC Authentication Bypass グループ マッピング	集中管理型リスト アドレスのワイルド指定	静的なリストの保守が必要

## NAC アセスメント方式の機能とトレードオフ

次の表に各アセスメント方式の機能とトレードオフをまとめました。次のセクションでは、この表の内容、および各アセスメント方式と NAH 処理に関する設計時のその他の考慮点について説明します。

機能	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
開始メカニズム	データ リンク アップ	DHCP または ARP	転送されたパケット
マシン アイデンティティ	✓		
ユーザ アイデンティティ	✓		
ポスチャ	✓	✓	✓
VLAN 割り当て	✓		
URL リダイレクション		✓	✓
Downloadable ACL	6500 のみ (ポリシー ベース ACL)	✓	✓
ポスチャ ステータス クエリー		✓	✓
802.1x ポスチャ変更	✓		

## NAC 導入の比較

導入モデル	長所	短所
アイデンティティおよびポスチャ	NAC L2 802.1x でアイデンティティとポスチャを統合して検証 L2 での実施 Identity Based Networking Services (IBNS) に準拠	NAC L2 IP および NAC L3 IP ではサポートされていない 無線サポートのために、サブリカント ライセンスの購入が必要 監査を未サポート (将来的にサポート)
IEEE 802.1x	IBNS に準拠	ポスチャ検証なし 監査を未サポート
ポスチャのみ (レイヤ 3)	NAC L2 IP および NAC L3 IP NAH 監査をサポート (NAC L3 IP では将来的にサポート) サブリカントはオプション	アイデンティティ検証なし
IEEE 802.1x およびポスチャ	IBNS に準拠 ポスチャを検証 監査をサポート (NAC L3 IP では将来的にサポート)	個別の許可 (VLAN 割り当ての後にポスチャ検証) ACS サーバへの負荷が 2 倍 複数のクライアントまたは管理の複雑さ

# NAC ソリューションのコンポーネント

## Cisco Trust Agent

CTA 2.0 は、以下を通じて入手できます。

- cisco.com での直接配布
- CSA 4.5.1 (新しいエージェント キットの作成) または CTA 2.0 エージェント キットが統合された CSA 5.0
- 各パートナー (Trend、InfoExpress など)
- パートナーは、CTA の別途インストールを不要にするために、将来 CTA 準拠テクノロジーを提供する製品に統合する予定です。

CTA 2.0 には、次のような複数のインストール オプションがあります。

- サイレント インストール (別パッケージ)
- NAC 対応 ネイティブ 802.1x サプリカントあり/なし (別パッケージ)
- スクリプティング インターフェイス サポートあり/なし (すべてのバージョンのインストール オプション)
- すべてのバージョンが集中管理型のポスチャ ブローカーと OS/ホットフィックス 情報を ACS に提供

CTA には、ポスチャ エージェントと 802.1x 有線サプリカントの 2 つのコンポーネントが含まれています。ポスチャ エージェントの導入に関する考慮点は限られています。主な作業は、CTA の導入時に、すべての Cisco Secure ACS インストールや認証チェーンの信頼される Certificate Authority (CA ; 認証局) のデジタル証明書を格納する「certs」フォルダをインストール ディレクトリに配置することです。証明書に署名した認証局は、どのようなケースでもクライアント システムの信頼されるルート CA である必要があります。したがって、大規模なインストールでは自己署名の証明書の使用は推奨せず、Public Key Infrastructure (PKI; 公開キー インフラストラクチャ) の使用を推奨します。自己署名証明書には実質上失効機能が存在せず、また最大で 1 年間有効であることから、大規模なインストールではこの方式は拡張性と安全性が不十分です。

RedHat Linux 用の CTA 2.0 クライアントには、有線、ワイヤレスとも 802.1x サプリカントが含まれないことに注意してください。802.1x 環境では、IEEE 802.1x サプリカントを使用してネットワークにアクセスするクライアントを認証し、さらに CTA を使用してポスチャ検証を実行する必要があります。この導入方式の詳細な情報については、「IEEE 802.1x と NAC L2 IP」のセクションを参照してください。

CTA は、現在、ハイアベイラビリティを目的とした冗長化リンク上でのクライアントのデュアルホーミングをサポートしていません。

NAC L2 802.1x 環境では、CTA はステータスの変更の有無を確認するために 300 秒間隔でプラグインにポーリングします。このタイマーの間隔は固定されています。CTA は変更を検出すると、サプリカントを始動させ、EPoL 検証を再度行います (EPoL-Start)。

CTA の詳細情報については、次の URL を参照してください。

<http://www.cisco.com/jp/product/hs/security/cta/>

CTA 2.0 の一般情報 (最新の対応 オペレーティング システムを含む) については、次のデータシートを参照してください。

[http://www.cisco.com/jp/product/hs/security/cta/prodlit/cta\\_ds.shtml](http://www.cisco.com/jp/product/hs/security/cta/prodlit/cta_ds.shtml)

## NAD

すべてのアドミッション コントロール環境において極めて重要なのはパフォーマンスで、特に応答時間です。デバイスがネットワークへの新しい接続を開始するたびにポスチャが検証されるので、このやりとりをリアルタイムで実行するために十分な NAD 帯域幅を確保する必要があります。選定した NAD の最新のパフォーマンス データは、お客様担当のアカウント チームから入手できます。次に一般的なベスト プラクティスを示します。

- 現在のパフォーマンス テスト結果を考慮すると、ステータス クエリー タイマーが与える影響は低いと考えられます。たとえばリモート アクセス環境で平均よりデバイスの移動性が高いために、より間隔が短いタイマーが必要な場合を除き、デフォルト値を利用することを推奨します。
- NAD と ACS にとってプロセッサを最も消費するのは再検証タイマーです。セキュリティ ポリシーにより、より短い間隔でチェックが必要で、ローカルの NAD がその負荷をサポートできる場合を除き、デフォルト値を利用することを推奨します。
- ポート (スイッチ) 当たり、またはデバイス (ルータ、コンセントレータ、アクセス ポイント) 当たりのデバイス数は、プラットフォームによって異なります。導入の前にこの数値を確認します。通常、許可されるデバイス数は、有効化されている機能によって異なります。

通常、NAD は URL リダイレクションで HTTPS をサポートしていません。

DoS 攻撃 (サービス拒絶攻撃) が発生する可能性を低減するために、Cisco IOS は デフォルトで NAD あたり 100 の NAC エージェントレス ホスト (NAH) のみを許可する設定になっています。通常はこの設定で問題はありますが、まずはシスコのベスト プラクティスに従い、十分なポスチャ適合が確立されるまで監査モードで NAC を導入する必要があるため、高密度、または LAN 環境では NAH がこの上限に到達する可能性があります。したがって、導入当初はニーズに対応するためにこの数値を高めに設定し、ローカル ポリシーで継続的に高い値が必要とされる場合 (特定の時間に 100 デバイスを超える管理対象外のデバイス セグメントが存在する) を除いて、後でデフォルト値に戻すことを推奨します。NAC L3 IP ルータ、NAC L2 IP スイッチを含む IOS NAD にこの設定を行います。

### CISCO IOS ルータ

認証プロキシは、イネーブルにされている場合、EoU より先に開始されます。また、EoU に配置された ACL は、認証プロキシによって配置された ACL を無効にし、ユーザやグループを認識しません。スイッチ サービス モジュール上に認証機能を提供するために NAC L2 802.1x を使用できますが、この場合の主要なアクセス ポリシー適用方式は VLAN 割り当てです。したがって、グループレベルのアクセス コントロール ポリシーを実施するためには、スイッチ サービス モジュールに VLAN ACL を事前に定義しておく必要があります。

### CISCO VPN コンセントレータ

3000 シリーズ VPN コンセントレータでは、ポスチャに基づいて適用されるアクセス フィルタがユーザ グループのマッピングに基づいて適用されるフィルタを上書きすることに注意してください。ACL マージはありません。

### CISCO スイッチ

すべての Cisco Catalyst スイッチの NAC 機能のサポートに関連する注意点は次のとおりです。

- 現在、NAC L2 802.1x でのダイナミックな割り当てのためにプライベート VLAN はサポートされていません。
- 現在、スイッチ上の NAC L2 802.1x は監査 (GAME) 統合をサポートしていません。
- NAC L2 IP および NAC L2 802.1x は、アクセスおよびマルチ VLAN アクセス ポート (CDP IP 電話のみ) のみでサポートされており、トランク ポートではサポートされていません。

- NAC L2 IP の場合、ARP 検査メカニズムを考慮すると、スイッチをルータと同様に使用し、レイヤ 3 デバイスの背後に配置してポスチャ検証を行うことはできません（通常は、レイヤ 3 デバイスのソース MAC アドレスのみ確認できます）。
- NAC L2 IP では、クライアントとスイッチ間で任意の L2 ホップ数が許可されています。

## CISCO SECURE ACS 4.0

### パフォーマンスとスケーラビリティ

ACS 4.0 のデータベース オペレーションは、Windows レジストリから SQL Sybase に移行されました。これによりパフォーマンスの向上が期待されますが、現在はテストの実施中です。最新情報については、お客様担当のシスコ アカウント チームにお問い合わせください。

NAC 設定をサポートするために、ACS のアドミッション用に十分な帯域幅を確保するようにしてください。NAD パフォーマンスに関するセクションで説明したように、再検証タイマーは最もプロセッサを消費する機能なので、このタイマーには必要最小限の値を設定してください。ベスト プラクティスではトランザクション レートは 1 秒当たり 10 回を想定していますが、（バックエンドの認証サーバ（Active Directory など）への遅延だけを考えても）導入によってこの値は大幅に異なります。説明のとおり、新しいパフォーマンス データでは、この値は増加すると考えられます。

また、ポリシー定義の一部には制限があります。MAC Authentication Bypass がイネーブルにされているネットワーク アクセス プロファイルの各インスタンスがローカルの ACS データベースでサポートできる MAC アドレス数は、最大 10,000 です。したがって、10,000 を超える MAC 例外が必要で、ワイルドカードの使用が不可能な場合は、NAD デバイスのグループ化を通じて ネットワーク アクセス プロファイルの境界上で MAB リストをセグメント化する必要があります。この制限は、802.1x/MBA および NAC L2 IP の集中管理型の MAC ホワイトリストに適用されます。NAC L2 IP の場合は、監査例外に MAC アドレス 1,000 までの制限があります。

### 管理

スケーラブルなポリシー変更のために、ポリシーの複製は欠かせない機能です。最初のポリシー作成作業は時間がかかるプロセスなので、ACS 複製機能を使用して集中管理されたポリシー変更をタイムリーに全社に複製することを推奨します。この方法は、ウォームやその他のアウトブレイクへの対応のための迅速なポリシー変更の実施にも最適です。

NAC 設定のトラブルシューティングを容易に行うことができるように、CTA のみを要求するポリシーを定義することを推奨します。つまり、ネットワーク アクセス プロファイルで必要なクレデンシャルを CTA のみとする内部ポリシーを作成します。たとえば、5 つのタイプのクレデンシャルが要求される場合に、エージェントが何らかの理由で 4 つのクレデンシャルしかレポートしなかったとします。このような場合、このポリシーを設定していなければ、許可要求は単純に失敗してしまい、貴重なログ情報生成されません。

### その他

ACS 4.0 についての注意ですが、ACS 3.3 と違い、ACS 4.0 は EoU 例外用の集中管理 IP ホワイトリストをサポートしていません。各 NAD の集中管理（MAB を使用）またはローカルの MAC 例外が適切でなく、この方式を必要とする場合、取り得るオプションは NAD のローカル IP 例外のみです。

### ディレクトリ サービス

組織が拡大すると、一元的でスケーラブルにアイデンティティ管理を行うためにディレクトリ サービスの使用が不可欠になります。ディレクトリ サービスは、電子メール アカウント名やコンタクト情報の管理だけでなく、ネットワークおよびアプリケーション認証に使用するアイデンティティ、パスワード、証明書、その他の情報を同期化するためにも使用できます。認証要求が発生するたび、AAA サーバはディレクトリ サーバに認証の決定を委託します。ディレクトリ サーバは、ACK とグループ割り当てか拒否を返します。

## サポートする認証プロトコル

チャレンジレスポンス通信では、ほぼすべての認証プロトコルが Extensible Authentication Protocol (EAP) をベースとしています。EAP プロトコルは、ユーザ名/パスワード、デジタル証明書、ワンタイム パスワード (OTP) クレデンシヤルに対応するさまざまな認証方式をサポートしています。しかし、各ディレクトリ サービスがすべての EAP ベース プロトコルと方式をサポートしているわけではありません。次の表で、自社で使用する NAC 方式、および主要なディレクトリ サーバがサポートするプロトコルをご確認ください。

プロトコル	方式	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
EAP-FAST	MS-CHAPv2	•		
	EAP-TLS	•		
	EAP-GTC	•		
PEAP	MS-CHAPv2	•		

表 2. NAC がサポートする EAP プロトコルとその方式


データベース	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTL)	PEAP (EAP-MSCHAPv2)	EAP-FAST フェーズ 0	EAP-FAST フェーズ 2
ACS Internal	•	•	•	•	•	•	•
Windows SAM	•			•	•	•	•
Windows AD	•		•	•	•	•	•
LDAP			•	•			•
ODBC	•	•	•	•	•	•	•
LEAP Proxy RADIUS サーバ	•			•	•	•	•
すべてのトークン サーバ				•			

表 3. ディレクトリ サーバがサポートする EAP 方式

Cisco Secure ACS は他の AAA の要件に対応するために EAP 以外のプロトコルもサポートしています。最も基本的なネットワーク チャレンジ プロトコルである PAP は、Cisco Secure ACS および Microsoft がともにサポートしています。しかし PAP は単純なプロトコルなので、すべてのクレデンシヤルが暗号化されずに送信されることを考慮してください。もう 1 つのオプションである CHAP は、エンドユーザ クライアントから AAA クライアントへの通信の際にパスワードを暗号化し、PAP よりも高度なレベルのセキュリティを提供します。Apple クライアントに対応するために、ARAP もサポートされています。

## ディレクトリのスケーラビリティ

互換性を確立したら、ディレクトリ サービス インフラストラクチャのスケーラビリティを考慮する必要があります。既存のディレクトリ サーバ インフラストラクチャは、日常的なユーザおよびマシン ログインの負荷に対応できるように構築されていますが、NAC の再検証の負荷に対応できるほどのスケーラビリティを備えていない可能性があります。また、ネットワークの遅



延による認証時間の短縮、およびサーバ障害発生時に冗長性を提供できるように、ディレクトリ サーバの組織全体への地理的な分散が必要となる場合もあります。

#### **まとめ**

NAC フレームワークは、ワーム、ウイルス、スパイウェア、マルウェアからのプロアクティブな保護を実現するために、エンドポイント（ラップトップ、PC、PDA、サーバなど）のセキュリティ ポリシーへの適合を保証し、セキュリティを飛躍的に向上させます。

さらに NAC フレームワークは、複数のベンダのセキュリティおよび管理ソフトウェアと幅広く統合し、ネットワーク インフラストラクチャおよびベンダ ソフトウェアへの既存の投資を保護します。

NAC は、ネットワーク自体によるセキュリティの脅威の特定、防止、適応能力を飛躍的に改善するためのシスコの自己防衛型ネットワーク構想の一角をなします。

# 付録

## 略語

略語	説明
ACE	Access Control Entry (アクセス コントロール エントリ)
ACK	Acknowledgement (受信応答)
ACL	Access Control List (アクセス コントロール リスト)
ACS	Access Control Server
AD	Active Directory (Microsoft)
AID	Authority Identity (機関 ID)
AP	Access Point (アクセス ポイント)
API	Application Programming Interface (アプリケーション プログラミング インターフェイス)
ARP	Address Resolution Protocol
AV	Anti Virus (アンチウイルス)
CAM	Clean Access Manager (CCA)
CAS	Clean Access Server (CCA)
CCA	Cisco Clean Access
CDP	Cisco Discovery Protocol
CHAP	Challenge Handshake Authentication Protocol
CSA	Cisco Security Agent
CTA	Cisco Trust Agent
CTASI	CTA Scripting Interface
DB	Database (データベース)
DC	Domain Controller (ドメイン コントローラ) (Microsoft)
DFS	Distributed File System (分散ファイル システム)
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name (認定者名)
DNS	Domain Name Service (ドメイン ネーム サービス)
DoS	Denial of Service (サービス拒絶)
DOT1X	IEEE 802.1x
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAPoRADIUS	EAP over RADIUS
EAPoUDP	EAP over UDP
EOU	EAP Over UDP
FAST	Flexible Authentication Secure Tunnel
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication (Microsoft)

GPO	Group Policy Object (グループ ポリシー オブジェクト) (Microsoft)
GTC	Generic Token Card
HA	High Availability (ハイ アベイラビリティ)
HAL	Hardware Abstraction Layer (ハードウェア抽象化レイヤ)
HCAP	Host Credential Authentication Protocol
HIPS	Host Intrusion Prevention System (ホスト侵入防止システム)
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secured
IAS	Internet Access Server (Microsoft)
IBNS	Identity Based Networking Services
IDS	Intrusion Detection System (侵入検知システム)
IID	Initiator Identity
IOS	Internetworking Operating System
IP	Internet Protocol (インターネット プロトコル)
L2	Layer 2 (レイヤ 2)
L2TP	Layer 2 Tunneling Protocol (レイヤ 2 トンネリング プロトコル)
L3	Layer 3 (レイヤ 3)
LAN	Local Area Network (ローカル エリア ネットワーク)
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control (メディア アクセス制御)
MITM	Man In The Middle (中間者)
MS	Microsoft (マイクロソフト)
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MVAP	Multi VLAN Access Ports
NAC	Network Admission Control (ネットワーク アドミッション コントロール)
NAD	Network Access Device (ネットワーク アクセス デバイス)
NAF	Network Access Filter (ネットワーク アクセス フィルタ)
NAH	NAC Agentless Host (NAC エージェントレス ホスト)
NAK	Negative Acknowledgement (否定応答)
NAR	Network Access Restriction (ネットワーク アクセス制限)
NAT	Network Address Translation (ネットワーク アドレス変換)
NDIS	
NDS	Netware Directory Services (Novell)
NRH	Non Responding Host (非応答ホスト)
NTLM	
ODBC	Open Database Connect
OOB	Out Of Band (アウトオブバンド)
OS	Operating System (オペレーティング システム)

OTP	One Time Password (ワンタイム パスワード)
PA	Posture Attribute (ポスチャ アトリビュート)
PAC	Provisioned Access Credential
PACL	Port ACL (ポート ACL)
PAE	Port Access Entity (ポート アクセス エンティティ)
PBACL	Policy Based ACL (ポリシーベース ACL)
PEAP	Protected EAP
PKI	Public Key Infrastructure (公開キー インフラストラクチャ)
PPTP	
PVLAN	Private VLAN (プライベート VLAN)
QoS	Quality of Service
RAC	RADIUS Attribute Component
RPC	Remote Procedure Call (リモート プロシージャ コール)
SAML	Security Assertion Markup Language
SIMS	Security Information Management System (セキュリティ情報管理システム)
SLB	Server Load Balancing (サーバ負荷バランシング)
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SQ	Status Query (ステータス クエリー)
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TLS	Tunnel Layer Security
TLV	Type Length Value
UDP	Universal Datagram Protocol
URL	Universal Resource Locator
VACL	VLAN ACL
VLAN	Virtual Local Area Network (仮想 LAN)
VoIP	Voice over IP
VPN	Virtual Private Network (バーチャル プライベート ネットワーク)
VSA	Vendor Specific Attribute (ベンダー固有アトリビュート)
VVID	Voice VLAN Identifier
WAN	Wide Area Network (ワイド エリア ネットワーク)
WEP	Wireless Encrypted Protection
WLAN	Wireless LAN (無線 LAN)
WoL	Wake on LAN

用語	Deprecated Term	定義
AAA		Authentication, Authorization, and Accounting (認証、認可、アカウントिंग) サーバ。通常 AAA は、「トリプル エー」と呼ばれます。AAA サーバは、1 つまたは複数の認証、許可、またはその両方の決定をもとにシステムの単一の結果を決定し、NAD でポリシーを適用するためにこの決定をネットワーク アクセス プロファイルにマッピングする NAC の中心的なサーバです。
Access-Accept		ユーザが認証されたことをアクセス サーバに通知する RADIUS サーバからの応答パケット。このパケットには、ユーザに割り当てられた AAA 機能を定義するユーザ プロファイルが含まれます。
Access-Challenge		認証の前にユーザに追加情報の提供を要求する RADIUS サーバからの応答パケット。
Access-Reject		ユーザが認証されなかったことをアクセス サーバに通知する RADIUS サーバからの応答パケット。
Access-Request		ユーザの認証を要求するアクセス サーバが RADIUS サーバに送信する要求パケット。
Accounting		ネットワーク管理サブシステムの Accounting (アカウントング) は、リソース利用状況に関するネットワーク データを収集する機能です。
ACE		Access Control Entry (アクセス コントロール エントリ)。ACL エントリには、タイプ、エントリが参照するユーザまたはグループの修飾子、一連のアクセス権が指定されます。一部のエントリ タイプのグループまたはユーザの修飾子は未定義です。
ACL		Access Control List (アクセス コントロール リスト)
ACS		Access Control Server または Cisco Secure Access Control Server
Action (アクション) (ACS)		
Assessment Result (アセスメント結果) (ACS)		
Condition (状態) (ACS)		
Condition Set (状態セット) (ACS)		
Credential Type (クレデンシャル タイプ) (ACS)		
Credential Validation Databases (クレデンシャル検証データベース) (ACS)		
Notification String (通知文字列) (ACS)		
Posture Assessment (ポスチャ アセスメント) (ACS)		
Profile (プロファイル) (ACS)		
Rule (ルール) (ACS)		

Rule Sets (ルール セット) (ACS)		
APT、Application Posture Token (アプリケーション ポスチャ トークン)		特定のベンダのアプリケーションのポスチャ検証の結果。
Audit Server (監査サーバ)		ホスト 上の PA を使用せずにポスチャのクレデンシャルを判定できるサーバ。このサーバは、ホストのポスチャ クレデンシャルを判定するとともに、ポスチャ検証サーバとしても機能できる必要があります。
authentication (認証)		ネットワーク管理セキュリティでは、人物またはプロセスのアイデンティティを検証することです。
authorization (許可)		各サービスのワンタイム認証または許可、ユーザごとのアカウント リストとプロフィール、ユーザ グループ、IP、IPX、ARA および Telnet をサポートするリモート アクセス コントロール手法。
AVP、attribute-value pair (アトリビュート値ペア)		アトリビュート値ペア。
CSA、Cisco Security Agent		Cisco Security Agent は、サーバおよびデスクトップ コンピューティング システムを脅威から保護します。ホストへの侵入防止、分散型ファイアウォール、悪質なモバイルコードからの保護、オペレーティング システムの完全性の保証、監査ログを単一のエージェント パッケージに融合してさまざまなセキュリティ機能を提供します。総合的なセキュリティ戦略の一角をなす Cisco Security Agent は、ネットワーク アドミッション コントロールと SAFE ブループリントを強化し、エンドポイントにまで保護機能を拡張します。
CSM、Cisco Security Manager		
CTA、Cisco Trust Agent	CTA Lite、 CTA サプリカント	CTA はシスコのポスチャ エージェント製品で、有線のみをサポートするサブリカントが組み込まれています。
CTASI		CTA Scripting Interface
Host (ホスト)	ホスト	ネットワーク リソースへの接続や使用を試みる任意のマシン。
MAC Exception Handling (MAC 例外処理)	MAC Auth Bypass	
CS-MARS		Cisco Security Monitoring, Analysis and Response System (CS-MARS) は、攻撃への対応、監視、被害の拡散防止のためのハイ パフォーマンスでスケーラブルなアプリケーション ファミリです。ネットワーク インテリジェンス、コンテキストの相関分析、ベクトル分析、異常検出、ホットスポット識別、および被害の拡散防止の自動化機能が統合された CS-MARS により、ネットワークおよびセキュリティ デバイスをより効果的に使用することができます。
NAC		Network Admission Control (ネットワーク アドミッション コントロール)。NAC は、ネットワーク インフラストラクチャを活用して、ネットワーク コンピューティング リソースにアクセスしようとするすべてのデバイスにセキュリティ ポリシーへの適合を強制することにより、ウイルスとワームがもたらす損害を抑制する、シスコシステムズが主導する業界イニシアチブです。NAC は、ネットワーク 自体によるセキュリティの脅威の自動的な特定、防止、適応を実現するためにネットワーク インテリジェンスを強化する、シスコの自己防衛型ネットワーク 構想の一角をなします。
NAC Partetners (NAC パートナー)	ベンダー、参加者	

NAC L2 802.1x	LAN ポート 802.1x、 L2 802.1x	
NAC L2 IP	LAN ポート IP、L2IP、 LPIP	
NAC L3 IP	GWIP	
NAD、Network Access Device (ネット ワーク アクセス デ バイス)		ネットワーク アクセス デバイスは、ホストに許可されたネットワーク アクセス権を与 えるポリシーを適用するポイントです。
NAF、Network Access Filter (ネットワーク アクセス フィルタ)		NAF は、1 つまたは複数のネットワーク エLEMENT (IP アドレス、AAA クライアント (ネットワーク デバイス)、ネットワーク デバイス グループ (NDG) ) の組み合 わせて構成される名前付きのグループです。NAF により、AAA クライアントをベース に Downloadable ACL またはネットワーク アクセス制限を指定し、これを通じてユー ザにネットワークへのアクセスを許可することができます。各 AAA クライアントを明 示的にリストする必要はありません。
NAH、NAC Agentless Host (NAC エージェント レス ホスト)	NRH, Non-responsive host	ポスチャ検証を実施するための 802.1x サプリカントまたは CTA がインストールされ ていないホスト。
NDG、Network Device Group (ネットワーク デバイス グループ)		単一の論理的なグループとして機能するネットワーク デバイスの集合。
PA、Posture Agent (ポス チャ エージェント)		1 つまたは複数のポスチャ プラグインからポスチャ クレデンシャルを収集してネット ワークに安全にそれらの情報を通知する、ホスト上の単一のコンタクト ポイントとして 機能するアプリケーション。
PDP、Policy Decision Point (ポリ シー決定ポイント)		ポリシー管理および条件フィルター機能を提供します。
PEP、Policy Enforcement Point (ポリシー適用ポイ ント)		ACS がポリシー適用ポイントとして機能し、ポリシーを管理します。
posture credentials (ポス チャ クレデンシャル)		ネットワーク エンドポイントの特定の時期のハードウェアおよびソフトウェア (OS お よびアプリケーション) 情報を示すステータス情報。
Plugin (プラグイン)、 posture plugin (ポスチャ プラグイン)	PP、 ポスチャ プラグイン	同一のエンドポイント上のポスチャ エージェントに、エンドポイントのポスチャ認証お よびネットワーク認証のために必要な、ホストのポスチャ クレデンシャルを提供する サードパーティ製 DLL。
posture validation (ポス チャ検証)		1 つまたは複数のポスチャ認証サーバとその適合ポリシーを使用して行う、ネットワ ーク エンドポイントのポスチャ クレデンシャルの認証。
EAP		
EAP-FAST		EAP Flexible Authentication by Secure Tunneling
EoU、EAPoUDP		Extensible Authentication Protocol over User Datagram Protocol
GAME		Generic Authorization Message Exchange
HCAP		Host Credential Authorization Protocol

IID、Initiator Identity		マシン認証における IID は、ホストの Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) (例: jdoe-pc.cisco.com) です。ユーザ認証における IID は、ユーザ名 (例: jdoe) です。
PEAP		Protected EAP
PV		Posture Validation (ポスチャ検証)。ユーザのマシン (ホスト) の一般的な状態と健全性を示す一連のアトリビュートを検証します。
PVS、Policy Server (ポリシー サーバ)、 Vendor Policy Server (ベンダポリシー サーバ)、 Posture Validation Server (ポスチャ検証サーバ)、 External Posture Validation Server (外部ポスチャ検証サーバ)		ポスチャ検証に使用されるシスコまたはサードパーティ製のサーバ。ポスチャ認証サーバは、NAC におけるアプリケーション別のポリシー決定ポイントとして機能し、一連のポリシー ルールと照合してポスチャ クレデンシャルを検証します。
RAC		RADIUS Attribute Component
RADIUS		Remote Authentication Dial-In User Service。ネットワーク アクセスの AAA の一元化を可能にする、幅広く利用されているプロトコルです。
SCM		Switchport Configuration Manager
SDM		Security Device Manager (セキュリティ デバイス マネージャ)
SPT、System Posture Token (システム ポスチャ トークン)		1 つまたは複数のアプリケーション ポスチャ トークンを収集して決定されたホストの単一のポスチャ検証結果です。
token (トークン)、 posture token (ポスチャ トークン)、 posture state (ポスチャ ステート)		
Token: Healthy		ホストはポリシーに適合しています。ホストからネットワークへのアクセスは制限されません。
Token: Check-up		ホストはポリシーの適合範囲内ですが、更新を入手可能です。このステートは、ホストを Healthy State にプロアクティブに修復するために使用されます。
Token: Transition		ホストのポスチャ検証が行われています。ホストにはポスチャ検証が完了するまで暫定的なアクセスが提供されます。すべてのサービスが稼動していない可能性があるホストブート プロセス中または検証結果が判明していないときに使用されるステートです。
Token: Quarantine		ホストはポリシーに適合していません。このホストのネットワーク アクセスは検疫ネットワークのみに制限されて修復が行われます。このホストはアクティブな脅威ではありませんが、既知の攻撃やウイルス感染に脆弱です。
Token: Infected		ホストは他のホストにとってアクティブな脅威です。このホストのネットワーク アクセスは厳格に制限するか、完全に拒否する必要があります。
Token: Unknown		ホストのポスチャを特定できません。正確なポスチャを特定できるまで、ホストの検疫、監査、または修復を行います。
VMS		
VSA、Vendor Specific Attribute (ベンダ固有アトリビュート)		大半のベンダが VSA を使用して付加価値機能をサポートします。

# NAC アトリビュートのリファレンス

## Attribute Namespace

すべての NAC アトリビュートは、ベンダおよびアプリケーション タイプに基づいたネームスペースで指定します。各ベンダおよびアプリケーションのタイプは、EAP 交換では番号で表されますが、通常は次のフォーマットで参照されます。

Vendor-ID: Application-Type: Attribute

Vendor-ID は、グローバルに一意のベンダ識別子を含む 32 ビットのフィールドです。上位オクテットは 0、下位 3 オクテットは International Assigned Numbers Authority により定義されているベンダの SMI ネットワーク管理プライベート エンタプライズコードがネットワーク バイト順に格納されます。シスコシステムズの Vendor ID は 9 です。

Application Type は、グローバルに一意のポストチャ アプリケーション タイプを表す 16 ビットのフィールドです。現在 Application Type は次のように定義されています。

ベンダ	Application Type	Application Type 名	説明
*	1	PA	ポストチャ エージェント
*	2	Host	ホスト情報
*	3	AV	アンチウイルス
*	4	FW	ファイアウォール
*	5	HIPS	ホスト侵入保護サービス
*	6	Audit	監査

**注:** 最新のアプリケーション タイプの詳細な情報については、(NAC パートナー ページの URL) を参照してください。

32768 - 65535 - ローカルでの使用のために予約済み (グローバルに一意の必要がないカスタム プラグインまたはスクリプトを単一の組織内で記述するお客様が使用できます。)

## アトリビュートのデータ型

データ型	演算子	説明
OctetArray	=, !=	可変長の任意のデータ。
Integer32	=, <, >, !=, >=, <=	ネットワーク バイト順の 32 ビットの符号付きの値。
Unsigned32	=, <, >, !=, >=, <=	ネットワーク バイト順の 32 ビットの符号なしの値。
String	=, !=, >, <, >=, <=, contains, does not contain, start with, end with, regular-expression	OctetArray データ型から派生したデータ型。ISO/IEC IS 10646-1 文字セットを使用して UTF-8 変換フォーマット (UTF-8) で表される人間に解読可能な文字列。 注 1: 7 ビット US-ASCII でエンコードされた情報は、UTF-8 文字セットと US-ASCII 文字セットは同一です。 注 2: UTF-8 は、1 つの文字/コード ポイントを表現するために複数バイトが必要となることがあるため、UTF8String のオクテット長はエンコードされた文字数とは異なることがあります。
IPv4Address	ワイルドカードとマスク	OctetArray データ型から派生したデータ型。IPv4Address には、最も重要なオクテットを先頭に 4 オクテットを含む必要があります。 例: "10.11.12.13" IPv4Address = 0A 0B 0C 0D

IPv6Address	ワイルドカードとマスク	OctetArray データ型から派生したデータ型。IPv6Address には、最も重要なオクテットを先頭に 16 オクテットを含む必要があります。 例: "0A0A:0B0B:0C0C:0D0D:0E0E:0F0F:1010:1111" IPv6Address = 0A 0A 0B 0B 0C 0C 0D 0D 0E 0E 0F 0F 10 10 11 11
Time	=、<、>、!=、>=、<=	Unsigned32 データ型から派生したデータ型。Coordinated Universal Time (UTC; 協定世界時) 1970 年 1 月 1 日からの秒数を表します。
Version	=、<、>、!=、>=、<=	OctetArray データ型から派生したデータ型。8 オクテットは 4 つの 2 オクテット セットに分割されます。最も重要な 2 オクテットにはメジャー バージョン、次の 2 オクテットにはマイナー バージョン、最後の 4 オクテットにはベンダが定義する 2 つのオクテット値を指定します。通常、3 つめのオクテットはレビジョン番号、最後のオクテットはビルド番号です。 例: "3.5.1.350" の値: 00 03 00 05 00 01 01 5E 注: 使用されないすべてのフィールドは 0 に設定する必要があります。

#### アトリビュートのリファレンス

Application-Posture-Token (APT) AVP は、Request-Response によって特定のベンダおよびアプリケーション タイプから送信されるポストチャ AVP の検証結果を表します。この AVP は Posture Notification 用の AVP で、NAC ソリューションの Client API Posture Notification 要求、EAP-TLV Posture-Notification 要求、および HCAP Posture Validation 応答の各インターフェイス間で送信できます。

System-Posture-Token (SPT) AVP は、Request-Response によって 1 つまたは複数のベンダおよびアプリケーション タイプから送信されるポストチャ AVP の総合的な検証結果を表します。この AVP は Posture Notification 用の AVP で、NAC ソリューションの Client API Posture Notification 要求、EAP-TLV Posture-Notification 要求、および HCAP Posture Validation 応答の各インターフェイス間で送信できます。

ベンダ (番号)	アプリケーション タイプ (番号)	アトリビュート名	アトリビュート番号	型	値またはフォーマット
* (任意)	* (任意)	Application-Posture-Token	1	Unsigned32	0 = Healthy 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
* (任意)	* (任意)	System-Posture-Token	2	Unsigned32	0 = HealthySystem 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown
Cisco (9)	PA	PA-Name	3	String	ポストチャ エージェント名。 シスコの場合は「Cisco Trust Agent」
Cisco (9)	PA	PA-Version	4	Version	フォーマット = major.minor.revision.build

Cisco (9)	PA	OS-Type	5	String	ホストのオペレーティング システム名。 Windows Server 2003 Datacenter Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Web Edition Windows Server 2003 Standard Edition Windows XP Home Edition Windows XP Professional Windows 2000 Datacenter Server Windows 2000 Advanced Server Windows 2000 Server Windows NT Workstation 4.0 Windows NT Server 4.0、Enterprise Edition Windows NT Server 4.0 Windows NT 4.0 Windows NT 3.51 Windows 95 Windows 95 OSR2 Windows 98 Windows 98 SE Windows Me
Cisco (9)	PA	OS-Version	6	Version	ホストのオペレーティング システムのバージョン。 フォーマット : major.minor.revision.build
Cisco (9)	PA	User-Notification	7	String	値には 1 つ以上の文字を含みます。 例 : Your anti-virus signature file is out-of-date. Please update your signature file from wwwin-companyxyz..remediation-server.com
Cisco (9)	PA	OS-Kernel	8	String	例 : Linux 2.4.20-8 i386
Cisco (9)	PA	Kernel Version	9	Version	ホストのオペレーティング システムのバージョン。 フォーマット : major.minor.revision.build
Cisco (9)	OS	Machine-Posture-State	11		このアトリビュートは、マシンの稼動状況を示します。 1 - 起動中 2 - 稼動中 3 - ログイン中
Cisco (9)	OS	ServicePacks	6	String	例 : ServicePack 4
Cisco (9)	OS	HotFixes	7	String	例 :  KB12345 Q21345
Cisco (9)	OS	HostFQDN	8	String	例 : ghoward-xp1.amer.cisco.com

Cisco (9)	OS	Package	100	Extended Query Protocol	
* (任意)	AV	Software-Name	3	String	ソフトウェア製品名。
* (任意)	AV	Software-ID	4	Unsigned32	ソフトウェア製品の数値識別子。
* (任意)	AV	Version	5	Version	ソフトウェアのバージョン。
* (任意)	AV	Scan-Engine-Version	6	Version	AV スキャン エンジンのバージョン。
* (任意)	AV	DAT-Version	7	Version	値には AV シグニチャ ファイルのバージョンを含みます。 例 : 559.0.0.0, 4.5.2.0
* (任意)	AV	DAT-Date	8	Time	AV シグニチャ ファイルのリリース時刻。
* (任意)	AV	Protection-Enabled	9	Unsigned32	0 = ディセーブル 1 = イネーブル
* (任意)	AV	Action	10	String	フォーマットとコンテンツはベンダによって異なります。 サポートされている最長文字列は 255 文字です。
Cisco (9)	HIP	CSAVersion	5	Version	CSA のバージョン。
Cisco (9)	HIP	CSAOperationalState	9	Unsigned32	0 = ディセーブル 1 = イネーブル
Cisco (9)	HIP	TimeSinceLastSuccessful Poll	11	Unsigned32	
Cisco (9)	HIP	CSAMCName	327 68	String	
Cisco (9)	HIP	CSAStatus	327 69	String	値は " " によって区切られます。 global_testmode_on rootkit_detected ipforwarding_on
Cisco (9)	HIP	DaysSinceLastSuccessful Poll	327 70	Unsigned32	例 : 3

## NAC の RADIUS アトリビュート

次の表に、シスコのベンダ固有アトリビュート (VSA) を含む、NAC に関連するすべての RADIUS アトリビュートを示します。

NAC-L2-802.1x	NAC-L2-IP	NAC-L3-IP	番号	アトリビュート名	説明
✓			1	User-Name	アクセス要求の EAP アイデンティティ応答からコピーされる。
	✓	✓	8	Framed-IP-Address	ホストの IP アドレス。
	✓	✓	26	Vendor-Specific Cisco (9, 1) CiscoSecure-Defined-ACL	ACL 名。 ACS により自動的に送信される。
✓			26	Vendor-Specific Cisco (9, 1) sec:pg	ポリシーベースの ACL 割り当て。Catalyst 6000 のみに適用。 sec:pg=<group-name>
	✓	✓	26	Vendor-Specific Cisco (9, 1) url-redirect	リダイレクション URL。 url-redirect=<URL>
	✓	✓	26	Vendor-Specific Cisco (9, 1) url-redirect-acl	リダイレクト URL のために名前付きの ACL を適用。 ACL は NAD のローカルへの定義が必要。IOS スイッチでのみ使用可能。 url-redirect-acl=<ACL-Name>
✓	✓	✓	26	Vendor-Specific Cisco (9, 1) posture-token	ポストチャ トークン/ステート名。 ACS により自動的に送信される。
	✓	✓	26	Vendor-Specific Cisco (9, 1) status-query-timeout	ステータス クエリー タイマーを設定。
	✓	✓	26	Vendor-Specific Cisco (9, 1) host-session-id	監査に使用されるセッション識別子。 ACS により自動的に送信される。
?	✓	✓	26	Vendor-Specific Microsoft = 311	ステータス クエリーのキー : MS-MPPE-Recv-Key ACS により自動的に送信される。
✓	✓	✓	27	Session-Timeout	再検証タイマーを設定 (秒)。
✓	✓	✓	29	Termination-Action	セッション タイムアウトのアクション。 (0) Default : セッションの終了 (1) RADIUS Request : 再認証
✓			64	Tunnel-Type	13=VLAN
✓			65	Tunnel-Medium-Type	6=802

✓	✓	✓	79	EAP Message	Access Request および Access Challenge の EAP 要求/応答パケット。 <ul style="list-style-type: none"> <li>• Access Accept では EAP Success</li> <li>• Access Reject では EAP Failure</li> </ul>
?	?	?	80	Message Authenticator	パケットの完全性を保証するための HMAC-MD5。
✓			81	Tunnel-Private-Group-ID	VLAN 名。

## NAC 方式と RADIUS 要求アトリビュート

RADIUS アトリビュート	NAC L2 802.1x	NAC L2 IP	NAC L3 IP	NAH/クライアントレス	MAC-Auth-Bypass
[1] Username	○	○	○		
[6] Service-Type				10	10
[8] Framed IP Address		○	○		
[26/9/1]VSA		aaa:service=ip_admission	aaa:service=ip_admission	aaa:service=ip_admission	
[26/9/1]VSA		audit-session-id=#	audit-session-id=#	audit-session-id=#	

©2006 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。  
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。  
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館  
<http://www.cisco.com/jp/>

お問い合わせ先 (シスコ コンタクトセンター)  
<http://www.cisco.com/jp/service/contactcenter/>

お問合せ先