



FAQ

## ネットワーク アドミッション コントロール

このドキュメントは、Network Admission Control (NAC; ネットワーク アドミッション コントロール) に関するテクニカル FAQ です。

このドキュメントには、Cisco IOS ルータ上の NAC L3 IP、Cisco IOS および CatOS スイッチ上の NAC L2 IP、Cisco IOS および CatOS スイッチ上の NAC L2 802.1x の NAC 機能とアーキテクチャに関する情報が記載されています。

## 目次

概要.....	6
Q. NAC はシスコ以外のデバイスで実施できますか？.....	6
Q. NAC を無効にする方法を教えてください。.....	6
Q. NAC を使用するために必要なハードウェアおよびソフトウェア コンポーネントを教えてください。.....	6
Q. NAC をサポートしているルータ プラットフォームと IOS バージョンを教えてください。.....	6
Q. NAC をサポートしているスイッチ プラットフォームを教えてください。.....	7
Q. さまざまな NAC コンポーネントの設定方法がすべて記載されているドキュメントはありますか？.....	7
Q. Cisco Clean Access (NAC アプライアンス) と NAC フレームワークとの違いを教えてください。.....	7
Q. NAC ポスチャ ステートとは何ですか？ それぞれのステートは何を示しているかを教えてください。.....	8
Q. Posture Plugin (PP; ポスチャ プラグイン) と Posture Agent (PA; ポスチャ エージェント) の違いを教えてください。.....	9
プロトコル.....	9
Q. EAP とは何ですか？.....	9
Q. NAC には、どのような EAP 拡張機能が必要ですか？.....	9
Q. EAPoUDP が使用するポート番号を教えてください。.....	9
Q. EAP-FAST とは何ですか？.....	9
Q. EAP-FAST と PEAP の相違点は何ですか？.....	9
Q. EAP-FAST をサポートする 802.1x サブリカントを教えてください。.....	9
Q. NAC L2 802.1x は、EAP-FAST を使用してどのような PAC プロビジョニング方式をサポートしていますか？.....	10
アドミッション方式.....	10
Q. NAC L2 IP とは何ですか？.....	10
Q. NAC L2 IP の ACL の例はありますか？.....	10
Q. NAC L2 IP を使用する場合、サブリカントは必要ですか？.....	10
Q. NAC L2 802.1x とは何ですか？.....	10
Q. Microsoft が提供する現在の Windows XP サブリカントは NAC をサポートしていますか？.....	11
Q. GAME とは何ですか？.....	11
Q. HCAP とは何ですか？.....	11
CISCO TRUST AGENT (CTA).....	11
Q. NAC には CTA が必要ですか？.....	11
Q. CTA はどこからダウンロードできますか？.....	11
Q. CTA 2.0 がサポートしているオペレーティング システムとアトリビュートを教えてください。.....	11

Q. 各 CTA インストール ファイルの違いを教えてください。 .....	12
Q. CTA 2.0 は Microsoft Windows から補足的な情報を収集できますか？ .....	12
Q. CTA 2.0 には 802.1x サブリカントが含まれていますか？ .....	12
Q. CTA 2.0 は非同期ステータス クエリーをサポートするということですが、非同期ステータス クエリーとは何ですか？ .....	12
Q. CTA は、どのネットワーク ポートで NAC チャレンジをリッスンしますか？ .....	12
Q. CTA にはログファイルがありますか？ある場合、どこに保管されますか？またサイズに制限はありますか？ .....	14
Q. 他の企業の ACS サーバと通信する際、CTA はどのようにオーソライズされますか？CTA が使用する ACS またはルート Certification Authority (CA; 認証局) のデジタル証明書は、どのようにしてインストールするのですか？ .....	14
Q. CTA に自社の ACS サーバとの通信のみを許可し、パブリック CA に署名された証明書を持つ ACS との通信を許可しないようにするにはどうすればよいのですか？ .....	14
Q. CTA のインストール時に 1 つまたは複数の ACS またはルート CA の証明書を自動的に追加できますか？ .....	14
Q. シスコ パートナーの xyz 社のポスチャ プラグインをインストールしました。このプラグインが CTA に正しく登録されているかどうかを確認する方法を教えてください。 .....	15
Q. CTA のパートナー プラグインが正しくインストールされ、機能していることを確認する方法を教えてください。 .....	15
Q. CSUtil.exe を使用して ACS に Attribution Definition File (ADF) ファイルをインポートすると、次のようなエラー メッセージが返されます。ADF ファイルに問題があるのですか？ .....	15
Q. CTA が表示できるユーザ通知メッセージの最大サイズを教えてください。 .....	15
Q. CTA ユーザ通知ダイアログは、非 ASCII (ユニコード、マルチバイト) 文字をサポートしますか？ .....	15
Q. CTA はホストで発生するポスチャ変更をどのようにして把握するのですか？ .....	16
Q. PEAP トンネルを開始するために PA から送信される EAP アイデンティティとは何ですか？ユーザ名、マシン名、あるいは IP アドレスですか？ .....	16
Q. CTA はなぜ Windows XP と連動しないのですか？ .....	16
Q. CTA が Windows のユーザ名およびパスワード クレデンシャルを使用できるようにするシングル サインオンの設定方法を教えてください。 .....	16
Q. CTA にクライアントのインターネット ブラウザを自動起動させるにはどうすればよいのですか？ .....	16
CISCO SECURITY AGENT (CSA) .....	17
Q. NAC をサポートしている CSA のバージョンを教えてください。これらの CSA は Cisco Trust Agent をインストールしますか？またどのようなアトリビュートを提供しますか？ .....	17
Q. Cisco Trust Agent は、CSA のステータスの変更をネットワーク アクセス デバイスに通知するために非同期ステータス変更機能を使用しますか？ .....	17
NAC L3 IP (ルータ) .....	17
Q. ルータの NAC L3 IP 設定のサンプルはありますか？ .....	17
Q. NAC 認証を開始させる最初のパケットがホストから送信されるとどうなりますか？ .....	20
Q. NAC と認証プロキシは同一のインターフェイスに共存できますか？その場合、最初に始動するのはどちらですか？ .....	21

Q. NAC は Easy VPN と連動しますか？ .....	21
Q. NAC に割り当てられたダイナミック ACL はインターフェイス ACL からいつ削除されますか？ .....	21
Q. NAD で show eou all コマンドを実行すると、さまざまな AuthTypes および Posture-Tokens が返されます。どのような意味があるのですか？ .....	21
Q. NAC は Host Standby Routing Protocol ( HSRP ) と連動しますか？プライマリ ルータに障害が発生した場合、セカンダリ ルータはすべての NAC セッションの再認証を行う必要がありますか？ .....	23
Q. AAA サーバがビジーな場合に発生する RADIUS フェールオーバーの時間を改善することはできますか？ .....	23
Q. NAD が非応答 ( クライアントレス ) ホストを許可するようになるにはどのように設定すればよいのですか？ .....	23
Q. 特定のホスト セッションに URL リダイレクションが適用されていることを確認する方法を教えてください。 .....	24
Q. URL リダイレクションがホスト セッションに適用されていますが、ホストの Web ブラウザが指定された URL にリダイレクトされません。 .....	25
Q. ルータで NAC を有効化すると、SL_DEF_ACL という名前の ACL が作成されます。これは何に使用されるのですか？ .....	25
Q. ホストが大きなファイルをダウンロードしている間にポスチャ再検証が発生するとどうなりますか？ダウンロードし直す必要がありますか？ .....	25
NAC L2 IP ( スイッチ ) .....	25
Q. スイッチの場合、NAD 上の NAC 認証プロセスは何によって開始されますか？ .....	25
Q. クライアントは NAC L2 IP を機能させるために、スイッチ インターフェイスに ACL が必要ですか？ .....	25
Q. IOS スイッチの NAC L2 IP 設定のサンプルはありますか？ .....	25
Q. CatOS スイッチの NAC L2 IP 設定のサンプルはありますか？ .....	31
Q. ACS から Downloadable ACL がスイッチに適用されていることを確認する方法を教えてください。 .....	32
Q. ACS から Downloadable ACL が特定のスイッチ ポートに適用されていることを確認する方法を教えてください。 .....	34
Q. IP Device Tracking コマンドとは何ですか？どのような目的で使用されますか？ .....	34
NAC L2 802.1X .....	34
Q. NAC L2 802.1x ではクライアントからどのようなタイプのクレデンシャルが送信されますか？ .....	34
Q. NAC L2 802.1x でクライアントが認証されませんでした。Windows のタスクバーには CTA アイコンが表示されていません。 .....	34
Q. スイッチのインターフェイスの 802.1x 情報を表示する方法を教えてください。 .....	34
Q. 特定のスイッチ ポートが適切な VLAN に配置されていることを確認する方法を教えてください。 .....	35
Q. Cisco IOS が稼働しているスイッチの NAC L2 802.1x 設定のサンプルはありますか？ .....	36
Q. CatOS が稼働しているスイッチの NAC L2 802.1x 設定のサンプルはありますか？ .....	42
CISCO SECURE ACCESS CONTROL SERVER ( ACS ) .....	43
Q. NAC をサポートしている ACS のバージョンを教えてください。 .....	43
Q. ACS 4.0 には、バージョン 3.3.1 とは異なる新しい NAC 設定エリアがあります。その違いを教えてください。 .....	43

Q. 無償で提供されている NAC 用の ACS の試用版はどこでダウンロードできるのですか？	43
Q. マスター ACS サーバとスレーブ ACS サーバ間で NAC ポリシーを複製できますか？	44
Q. NAC 認証を制御するためのシスコ独自のベンダー固有属性 (VSA) は何ですか？	44
Q. ACS 4.0 にはどのようなデフォルト プロファイル テンプレートがありますか？どのテンプレートを選択して設定を開始すればよいのですか？	44
Q. ACS のグループ設定を使用して再検証期間を設定できますか？	44
Q. ステータス クエリー期間と再検証期間の違いを教えてください。	44
Q. ユーザ通知メッセージを他の言語で作成することはできますか？	45
Q. ACS データ ディレクトリにどのようなベンダー アトリビュートが保管されているかを確認する方法を教えてください。	45
Q. 現在使用している ACS のバージョンには、ベンダー xyz 社の NAC クレデンシャル タイプおよびアトリビュートが表示されません。新しい NAC クレデンシャル タイプを ACS データ ディレクトリにインポートする方法を教えてください。	45
Q. ASC のユーザ通知メッセージの最大サイズを教えてください。	46
Q. ACS ではどのような正規表現がサポートされていますか？	46
Q. == および != 演算子を使用して文字列をマッチングできますか？	46
Q. Network Access Profiles で作成した新しいプロファイルで、active の列に「NO」と表示されるのはなぜですか？	46
Q. 複数のプロファイルが設定されている場合、ACS はどのようにして使用するプロファイルを決定するのですか？	46
Q. ACS は設定されたすべてのアトリビュートをチェックするのですか？	46
Q. ACS があるホストを拒否し、このイベントを Failed Attempts ログに記録しました。何が問題なのですか？	46
Q. ACS アプライアンスにパートナーのアトリビュート定義ファイル (ADF) をインストールする方法を教えてください。	47
Q. 複数のアンチウイルス エージェントをチェックするには、ACS をどのように設定すればよいのですか？	47
Q. ACS が Host Credential Authorization Protocol (HCAP) ポスチャ検証サーバから応答を受信できない場合どうなりますか？	50
パートナー	50
Q. xyz 社は NAC をサポートしていますか？どの企業のソフトウェアのバージョンが NAC をサポートしているのですか？どのパートナーが NAC のレポート ソリューションを提供していますか？	50
Q. シスコはすべてのパートナーのすべての NAC アトリビュートの包括的なリポジトリを保持していますか？	50
Q. Cisco Secure ACS インストールで特定のベンダーの NAC アトリビュート ファイルを確認できません。どこで取得できるのですか？またどのようにインポートすればよいのですか？	51
略語と用語	51

## 概要

Q. NAC はシスコ以外のデバイスで実施できますか？

A. いいえ。EAPoUDP プロトコルをサポートしているのは、シスコのデバイスのみです。

Q. NAC を無効にする方法を教えてください。

A. NAC 対応の各インターフェイスで **no ip admission <policy-name>** コマンドを実行します。

Q. NAC を使用するために必要なハードウェアおよびソフトウェア コンポーネントを教えてください。

A. NAC ソリューションを構成する主要なコンポーネントは次の 3 つです。

- [Cisco Trust Agent \(CTA\)](#) が稼働しているネットワーク エンドポイント
- ネットワーク アクセス ポリシーを適用するための 1 つまたは複数の NAC 対応インターフェイスを装備する [シスコ ネットワーク アクセス デバイス \(NAD\)](#)
- エンドポイントの適合性の検証を実施する [Cisco Secure Access Control Server \(ACS\)](#)

Q. NAC をサポートしているルータ プラットフォームと IOS バージョンを教えてください。

A. NAC は、Cisco IOS 12.3 (8) T またはそれ以降の Advanced Security フィーチャ セットでサポートされます。プラットフォームの最新のサポート状況については、<http://www.cisco.com/jp/go/nac/> を参照してください。

ルータ モデル	IOS バージョン
Cisco 83x シリーズ ルータ	12.3 (8) T およびそれ以降
Cisco 850 シリーズ ルータ	12.3 (14) T およびそれ以降
Cisco 870 シリーズ ルータ	12.3 (14) T およびそれ以降
Cisco 1700 シリーズ ルータ	12.3 (8) T およびそれ以降
Cisco 1812J ルータ	12.3 (8) T およびそれ以降
Cisco ISR 1800 シリーズ ルータ	12.3 (8) T およびそれ以降
Cisco 2600XM	12.3 (8) T およびそれ以降
Cisco 2691 マルチサービス プラットフォーム	12.3 (8) T およびそれ以降
Cisco ISR 2800 シリーズ ルータ	12.3 (8) T およびそれ以降
Cisco 3640 マルチサービス プラットフォーム	12.3 (8) T およびそれ以降
Cisco 3660-ENT シリーズ ルータ	12.3 (8) T およびそれ以降
Cisco 3725/3745 マルチサービス アクセス ルータ	12.3 (8) T およびそれ以降
Cisco ISR 3800 シリーズ ルータ	12.3 (11) T およびそれ以降
Cisco 7200 シリーズ	12.3 (8) T およびそれ以降

Q. NACをサポートしているスイッチプラットフォームを教えてください。

A. NACフレームワークをサポートするIOSおよびCatOSベーススイッチを次の表にまとめました。

スイッチモデル、スーパーバイザー	OSバージョン	NAC L2 802.1X	NAC L2 IP	NAC L3 IP	NAC エージェントレス ホスト
6500 Sup32、720	ネイティブIOS	-	12.2 (18) SXF2	-	NAC L2 IP
6500—Sup2	ネイティブIOS	-	-	-	-
6500—Sup32、720、Sup2	ハイブリッド/CatOS	CatOS 8.5	CatOS 8.5	-	-
4000 Series—Sup2+、3-5	IOS	12.2 (25) SG	12.2 (25) SG	-	12.2 (25) SG (NAC L2 IP)
3550	IOS IP Services および IP Base	12.2 (25) SED	12.2 (25) SED	-	12.2 (25) SED
3750、3560	IOS - Advanced IP Services、IP Services、IP Base	12.2 (25) SED	12.2 (25) SED	-	12.2 (25) SED
2970	IOS - LAN Base	12.2 (25) SED	-	-	-
2960	IOS - LAN Base	12.2 (25) SED	-	-	-
2950	IOS	12.1 (22) EA6			
	-	-	-		
2940、2955	IOS	12.1 (22) EA6			
	-	-	-		
6500—Sup1A	すべて	なし	いいえ	いいえ	いいえ
5000	すべて	なし	いいえ	いいえ	いいえ
4000/4500	CATOS	なし	いいえ	いいえ	いいえ
3500XL	すべて	なし	いいえ	いいえ	いいえ
2900XM	すべて	なし	いいえ	いいえ	いいえ

Q. さまざまな NAC コンポーネントの設定方法がすべて記載されているドキュメントはありますか？

A. <http://www.cisco.com/jp/go/nac/> で公開されている『[シスコ ネットワーク アドミッション コントロールの実装](#)』およびその他の技術資料を参照してください。

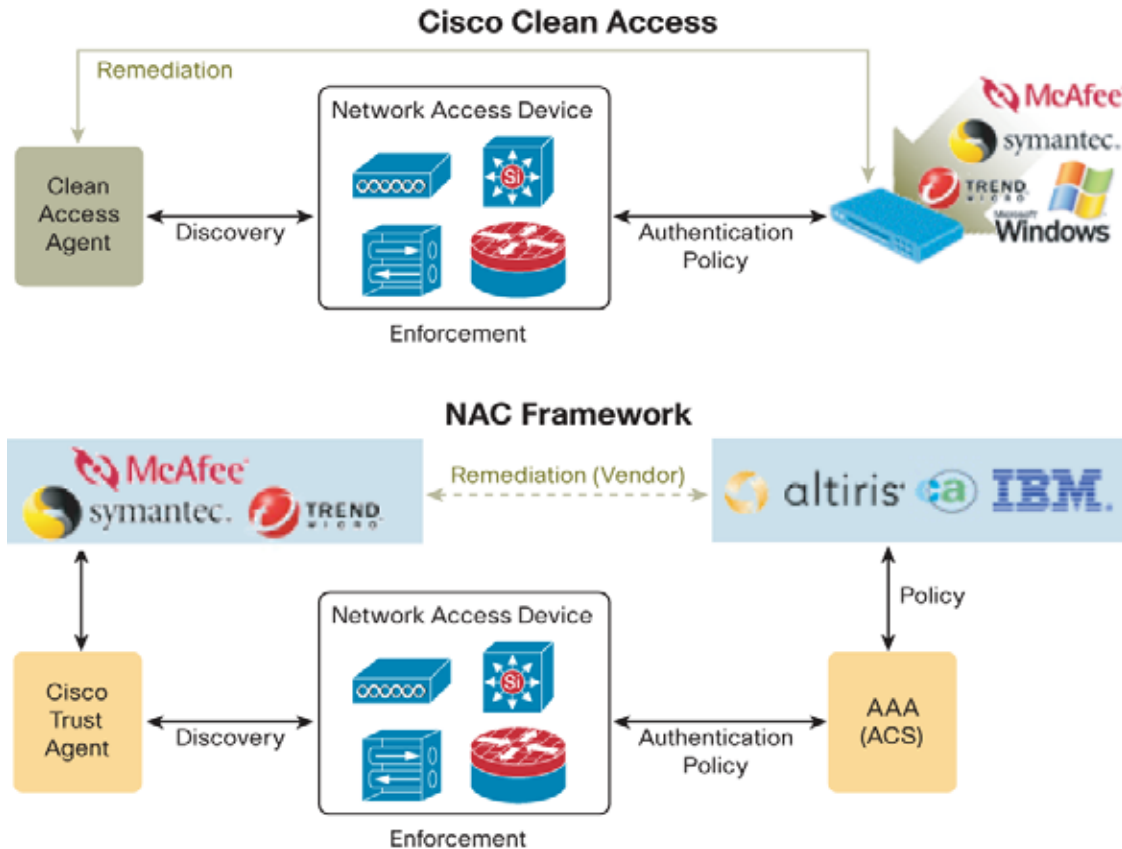
Q. Cisco Clean Access (NAC アプライアンス) と NAC フレームワークとの違いを教えてください。

A. NAC フレームワークは、Virtual Private Network (VPN; バーチャル プライベート ネットワーク) や無線を含む新規および既存のシスコ ネットワーク インフラストラクチャや NAC パートナーの製品を使用して、NAC をレイヤ 2 および レイヤ 3 に展開します。詳しい情報については、ネットワーク アドミッション コントロールの Q&A を参照してください。

NAC アプライアンスである Cisco Clean Access ソリューションは、ネットワーク インフラストラクチャと統合する豊富な機能を装備する製品です。NAC アプライアンスは、NAC フレームワークをサポートしていないネットワーク インフラストラクチャにアドミッション コントロールおよびポスチャ アセスメント機能を提供します。

次の図にこの2つのソリューションの動作を示しました。

図 1 Cisco Clean Access と NAC フレームワーク



Q. NAC ポスチャ ステートとは何ですか？ それぞれのステートは何を示しているかを教えてください。

- A.
- **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、更新を入手可能です。このステートは、ホストを Healthy ステートに修復するために使用されます。
  - **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。
  - **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。
  - **Infected** —ホストは他のエンドポイント デバイスにとって脅威となる可能性があります。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、認証、または修復を行います。

Q. Posture Plugin (PP; ポスチャ プラグイン) と Posture Agent (PA; ポスチャ エージェント) の違いを教えてください。

A. ポスチャ プラグインは、ホストにインストールされるソフトウェア コンポーネントで、ポスチャ クレデンシャルをポスチャ エージェントに渡します。ポスチャ エージェントもホストにインストールされますが、ブローカーとしての役割を果たし、ホストのポスチャ プラグインからクレデンシャルを収集してネットワークと通信します。Cisco Trust Agent は、シスコシステムズが提供しているポスチャ エージェントです。ポスチャ エージェントは、ネットワークとの通信に EAPoUDP または 802.1x を使用します。

## プロトコル

Q. EAP とは何ですか？

A. Extensible Authentication Protocol (EAP) は、RFC 2284 で定義されているリクエスト レスポンス プロトコルです。

EAP は、ピアと AAA (Authentication, Authorization, and Accounting) サーバ間でのアイデンティティおよび認証クレデンシャルの交換に使用されます。シスコ NAC は、NAC L2 IP および NAC L2 802.1x で EAPoUDP および EAPoLAN を使用します。

Q. NAC には、どのような EAP 拡張機能が必要ですか？

A. EAP Type Length Value (EAP-TLV) 拡張がポスチャの 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に使用されます。

ステータス クエリー方式を使用することで、クレデンシャルの完全な再認証を行わずにピアのポスチャ ステータスを確実に照会できます。

Q. EAPoUDP が使用するポート番号を教えてください。

A. EAPoUDP は UDP 21862 番ポートを使用します。

Q. EAP-FAST とは何ですか？

A. 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) にインフォメーションナル ドラフト (draft-cam-winget-eap-fast-02.txt) を投稿して、仕様を公開しています。

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: クライアントおよび 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。

Q. EAP-FAST と PEAP の相違点は何ですか？

A. PEAP はさまざまな機能を提供しますが、デジタル証明書を必要とします。また、すべてのクライアント デバイスでサポートされているわけではありません。PEAP と同様に、EAP-FAST はさまざまな認証方法をサポートするトンネル化プロトコルですが、デジタル証明書を必要とせず、ほぼすべてのクライアント デバイスで利用することができます。

Q. EAP-FAST をサポートする 802.1x サブリカントを教えてください。

A. 有線のみに対応する CTA 2.0 の lite サブリカントが EAP-FAST をサポートしています。無線のサポートが必要であれば、Meetinghouse AEGIS クライアント (サブリカント) (<http://www.mtghouse.com/>) が EAP-FAST をサポートしています。

Q. NAC L2 802.1x は、EAP-FAST を使用してどのような PAC プロビジョニング方式をサポートしていますか？

A. NAC L2 802.1x に対応する CTA サブ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 PAC をプロビジョニングできます。CTA サブリカントは、ACS サーバがインバンド プロビジョニングを許可している場合にのみ、ホスト上で PAC をプロビジョニングします。CTA がホスト上で PAC をプロビジョニングするためには、マシンに割当てられた証明書（マシン証明書）を使用するマシン認証が成功するか、ユーザ認証が成功して、クライアントが認証されなければなりません。CTA サブリカントは、NAC L2 802.1x を使ったアウトオブバンド プロビジョニングをサポートしません。

### アドミッション方式

Q. NAC L2 IP とは何ですか？

A. ルータ プラットフォームにおける NAC と同様に、接続されているすべてのエンドポイントにはアプリケーション ポスチャのアセスメントが実行されます。アイデンティティ ベースの認証は行われません。ポスチャが検証されると、ポスチャ ステートに基づいてポリシーが適用されます。ポスチャ情報は、EAP over UDP プロトコルを使って転送されます。ポスチャ検証は、任意の新しい ARP 要求（ARP インスペクション）または DHCP バインディング（DHCP スヌーピング）によって開始されます。ポスチャ情報がポリシーの要件を満たさない場合は、修復プロセスが実施されます。セキュリティ ポリシーの要件に違反するすべてのエンドポイントからのトラフィックは、AAA サーバからダウンロードされた Access Control List（ACL; アクセス コントロール リスト）によって制限されます。ダウンロードされた ACL は、デフォルトのポート ACL の前に挿入されます。

Q. NAC L2 IP の ACL の例はありますか？

A.

```
ip access-list extended interface_acl
remark Allow EAPoUDP
permit udp any any eq 21862
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark Allow HTTP access to update server
permit tcp any host 10.0.200.30 eq www
remark Allow ICMP for test purposes
permit icmp any any
remark Implicit Deny
deny ip any any
```

Q. NAC L2 IP を使用する場合、サブリカントは必要ですか？

A. いいえ。NAC L2 IP は、EAP over UDP を使用して NAC L3 IP と同様のポスチャ チェックを実行します。

Q. NAC L2 802.1x とは何ですか？

A. NAC に対応したこの 802.1x 展開手法により、ユーザのアイデンティティ、マシンのアイデンティティ、およびポスチャ検証情報を 802.1x アクセス コントロール カンパセーションに収集することができます。NAC L2 802.1x は、クライアントとサーバの間で EAP-FAST 方式を使用してこの情報を交換します。

Q. Microsoft が提供する現在の Windows XP サプリカントは NAC をサポートしていますか？

A. いいえ。NAC L2 802.1x は EAP 方式として EAP-FAST を使用します。EAP-FAST は、TLS トンネルでユーザおよびマシンのクレデンシャルを転送できるように修正されており、また CTA を通じたポストチャックもサポートしています。Microsoft Windows 802.1x サプリカントは、EAP-FAST をサポートしておらず、ポストチャックにも対応していません。NAC 対応サプリカントを使用できない場合には、Microsoft サプリカントを使用してユーザ認証を行い、補足手段として NAC L2 IP を使用してポストチャックを行うことができます。詳しい情報については、『[NAC フレームワーク導入ガイド](#)』を参照してください。

Q. GAME とは何ですか？

A. Generic Authorization Message Exchange の略で、Security Assertion Markup Language (SAML) を拡張し、https セッションを通じて ACS とパートナーの監査サーバが通信を行うために使用されるプロトコルです。

ACS は、ベンダーの監査サーバを利用して NAC エージェントレス ホストの監査を開始します。その後 ACS は、監査の判定を取得するために定期的にポーリングを行います。監査サーバは、監査が完了するとポストチャックステータスを ACS に返します。

Q. HCAP とは何ですか？

A. Host Credential Authorization Protocol です。ACS は、1 つまたは複数の HTTP(S) セッションを通じて 1 つまたは複数のベンダーサーバに、クライアントの EAP ベースのクレデンシャルを転送します。その後 ACS は、各ベンダーサーバからポストチャックトークン応答とオプションの通知メッセージを受信します。

## CISCO TRUST AGENT (CTA)

Q. NAC には CTA が必要ですか？

A. はい。NAC は、エンドポイントのポストチャッククレデンシャルを提供するために Cisco Trust Agent (CTA) が必要です。CTA をインストールしていないホストに対しては、MAC または IP アドレスに基づいた例外をルータまたは ACS に手動で設定することにより、ネットワークへのアクセスを許可できます。Cisco IP フォンなどデバイスのタイプによる例外も、ルータの Cisco Discovery Protocol (CDP) を使って許可できます。

Q. CTA はどこからダウンロードできますか？

A. シスコにユーザ登録されているお客様は、www.cisco.com から無償で CTA をダウンロードできます。

Q. CTA 2.0 がサポートしているオペレーティングシステムとアトリビュートを教えてください。

A. 次の表を参照してください。

CTA バージョン	OS	アトリビュート
2.0	<ul style="list-style-type: none"><li>Windows NT 4.0</li><li>Windows 2000 Professional および Server (SP4)</li><li>Windows XP Professional (SP1 まで)</li><li>Windows 2003</li></ul>	<ul style="list-style-type: none"><li>Cisco:PA:PA-Name</li><li>Cisco:PA:PA-Version</li><li>Cisco:PA:OS-Type</li><li>Cisco:PA:OS-Version</li><li>Cisco:PA:MachinePostureState</li></ul>
2.0	<ul style="list-style-type: none"><li>Red Hat Linux 9</li><li>Red Hat Enterprise Linux v3</li></ul>	<ul style="list-style-type: none"><li>Cisco:PA:PA-Name</li><li>Cisco:PA:OS-Version</li><li>Cisco:PA:Kernal-Version</li><li>Cisco:PA:MachinePostureState</li><li>Cisco:PA:OS-Type</li><li>Cisco:PA:OS-Version</li></ul>

Q. 各 CTA インストール ファイルの違いを教えてください。

A.

CTA .exe ファイル	説明
ctasetup-win-[version].exe	このパッケージのインストールは、各ステップでユーザの確認が必要となります。エンド ユーザはインストール中に、ライセンス契約への同意、インストール先フォルダの選択、その他のインストールオプションの選択を求められます。このパッケージは、CTA スクリプティング インターフェイスのみをインストールします。このパッケージではサブリカントはインストールされません。
ctasetup-supplciant-win-[version].exe	このパッケージのインストールは、対話形式で行われます。エンド ユーザは、ライセンス契約への同意、インストール先フォルダの選択、その他のインストールオプションの選択を求められます。このパッケージは、CTA スクリプティング インターフェイスおよびサブリカント両方をインストールできます。エンド ユーザは、インストールする CTA 機能についても選択できます。
CtaAdminEx-win-[version].exe	このパッケージのインストールは、ユーザの介在なしに進行します。管理者は、このパッケージから ctasilent-win-[version].exe ファイルを抽出します。管理者は、エンド ユーザに代わってライセンス契約に同意し、エンド ユーザにオプションの選択を要求しない完全なサイレント インストールとしてこのファイルを展開します。このパッケージではサブリカントはインストールされません。
CtaAdminEx-supplciant-win-[version].exe	このパッケージでは、エンド ユーザ用のサイレント インストール パッケージを作成します。管理者は、このパッケージから ctasilent-supplciant-win-[version].exe ファイルを抽出します。管理者は、エンド ユーザに代わってライセンス契約に同意し、エンド ユーザにオプションの選択を要求しない完全なサイレント インストールとして ctasilent-supplciant-win-[version].exe ファイルを展開します。このパッケージでは、サブリカントがインストールされます。

Q. CTA 2.0 は Microsoft Windows から補足的な情報を収集できますか？

A. はい。Host Posture Plugin for Windows が、現在使用されている Windows Service Pack、マシン名、Windows に適用済みのホットフィックスのリストを返します。

Q. CTA 2.0 には 802.1x サブリカントが含まれていますか？

A. はい。CTA には、有線の 802.1x 接続のみをサポートする 802.1x サブリカントが含まれています。無線環境で NAC をサポートする必要がある場合は、無線に対応する Meetinghouse または Funk サブリカントの購入が必要です。

Q. CTA 2.0 は非同期ステータス クエリーをサポートするということですが、非同期ステータス クエリーとは何ですか？

CTA 2.0 がサポートする非同期ステータス クエリーにより、CTA はクライアントに変更が発生したことをネットワーク アクセス デバイス (NAD) に通知することができます。変更が発生した場合、ネットワークはアイデンティティおよびポスチャ ステータス クエリーを実行して、定義されているアドミッション ポリシーと変更された状態を比較する必要があります。非同期ステータス クエリーは、NAC L2 802.1x でサポートされています。

Q. CTA は、どのネットワーク ポートで NAC チャレンジをリッスンしますか？

A. CTA は、デフォルトで UDP 21862 番ポートを使用する EAP-over-UDP (EAPoUDP) を使用してネットワーク アクセス デバイスと通信します。デフォルトの EAPoUDP ポートを変更するには、ctad.ini 設定ファイルを編集します。ctad.ini 設定ファイルのすべてのオプションについては、『Cisco Trust Agent アドミニストレータ ガイド』を参照してください。

どのポートを使用する場合も、インストールされているパーソナルファイアウォールソフトウェアが該当ポートへの着信トラフィックを許可していることを確認してください。許可されていない場合、CTA はネットワーク アクセス デバイスからの NAC チャレンジに応答できません。

Q. CTA にはログファイルがありますか？ある場合、どこに保管されますか？またサイズに制限はありますか？

A. CTA はトラブルシューティングのためのロギング機能を装備していますが、デフォルトでは無効に設定されています。

ロギング機能を有効化するには、CTA 設定ディレクトリ C:\Documents and Settings\All Users\Application Data\Cisco Systems\CiscoTrustAgent\ 内の ctalogd.tmp ファイルの名前を ctalogd.ini に変更します。CTA が新しい EAPoUDP 要求を受信すると、Logs サブディレクトリにログ ファイルが作成されます。ログ ファイルが作成されない場合は、ファイルが誤った名前に変更されたか、CTA が EAPoUDP 要求を受信していない可能性があります。CTA は、パーソナルファイアウォールがネットワーク アクセス デバイスからの要求をブロックしているために EAPoUDP 要求を受信できないことがあります。

ログ ファイルの最大サイズは、デフォルトで 4MB に設定されていますが、ctalogd.ini ファイルを編集することにより変更が可能です。ログ ファイルが最大サイズに達すると、新しいログ ファイルが作成されます。ログ ファイルの数が増えてくので、全体でのログのサイズに制限はありません。

ログファイルのカスタマイズ方法の詳細については、『Cisco Trust Agent アドミニストレータ ガイド』のイベント ロギングに関するセクションを参照してください。

Q. 他の企業の ACS サーバと通信する際、CTA はどのようにオーソライズされますか？CTA が使用する ACS またはルート Certification Authority (CA; 認証局) のデジタル証明書は、どのようにしてインストールするのですか？

A. CTA のデフォルト設定では、エンドポイントが信頼するルートストアに存在する認証チェーン内の CA (DST、Thwate、Verisign など) によって署名されたデジタル証明書を持つすべての ACS を信頼するようになっています。自己署名の証明書やプライベート CA の証明書を使用する場合、ホストにまだ証明書が配布されていないければ、手動でホストに証明書を追加する必要があります。

CTA はクライアントへのインストール中に証明書をインポートできるので、CTA インストール ファイル (.exe) と同じディレクトリに certs という名前のフォルダを作成しておきます。CTA は、インストール中にこのフォルダから .cer を自動的に検索してインポートします。

CTA に手動で証明書を追加する場合には、CTA が提供する CTACert.exe プログラムを使用できます。CTA に ACS またはルート認証局の新しいデジタル証明書を追加するには、次のコマンドを使用します。

```
ctacert.exe /add "cert_path" /store "Root"
```

ここで Root は、ルートストアに証明書を保管することを意味します。この操作を実行するには、ローカル マシンの Administrator 権限が必要です。

Q. CTA に自社の ACS サーバとの通信のみを許可し、パブリック CA に署名された証明書を持つ ACS との通信を許可しないようにするにはどうすればよいのですか？

A. いくつかのオプションがあります。

- 各 ACS で自己署名の証明書を使用し、各 CTA インストールにこれらすべての証明書を追加します。これは、拡張性の高い手法ではありません。
- すべての ACS 証明書への署名にプライベート CA (Microsoft Certificate Server) を使用し、ホストのルート証明書ストアにプライベート CA のパブリック証明書をインストールします。
- ctad.ini ファイルを作成し、CTA が受け付ける証明書を証明書のアトリビュートに応じて制限するように編集します。

Q. CTA のインストール時に 1 つまたは複数の ACS またはルート CA の証明書を自動的に追加できますか？

A. はい。CTASetup.exe は、certs サブディレクトリ内の使用可能なすべての証明書を自動的にインストールします。

CTASetup.exe と同じディレクトリにこのディレクトリを作成し、証明書を配置してからこのセットアップ プログラムを実行してください。

Q. シスコパートナーの xyz 社のポストチャ プラグインをインストールしました。このプラグインが CTA に正しく登録されているかどうかを確認する方法を教えてください。

A. NAC の認証後に、CTA ログ ファイルの processPostureRequests メッセージで確認できます ([ロギングを有効にする方法については、上記の質問「CTA にログファイルはありますか？ある場合、どこに保管されますか？またサイズに制限はありますか？」を参照してください](#))。CTA ログ エントリの例を示します。

```
26 14:37:09.496 11/17/2004 Sev=Info/4 PPMgr/0xE3600006 processPostureRequests returned (8) in dll
C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\CiscoSecurityAgentPlugin.dll.
27 14:37:09.496 11/17/2004 Sev=Info/4 PPMgr/0xE3600006 processPostureRequests returned (8) in
dll C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\CiscoHostPlugin.dll.
```

また、ACS Passed Authentications ログのロギングされたクレデンシャルでも確認できます。

Q. CTA のパートナー プラグインが正しくインストールされ、機能していることを確認する方法を教えてください。

A. C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\ にプラグインがあるかどうかを確認します。

このフォルダにプラグインが存在すれば、CTA デバッグを有効にすることにより、プラグインと CTA が連動していることを確認できます。デバッグを有効にするには、ctalogd.ini ファイルを編集します。

```
C:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\ctalogd.ini
```

このファイルの以下のエントリを次のように修正します。

```
PPMgr=15
Plugin=15
```

ctalogd.ini ファイルを保存してから閉じます。次の EoU チャレンジの際に、Logs サブディレクトリの下に登録済みプラグインの詳細情報を含むログ ファイルが表示されます。

Q. CSUtil.exe を使用して ACS に Attribution Definition File (ADF) ファイルをインポートすると、次のようなエラー メッセージが返されます。ADF ファイルに問題があるのですか？

```
CSUtil v4.0 (1.12), Copyright 1997-2005, Cisco Systems Inc
[attr#0]: Error: cannot manually add attributes with the reserved ID of 1 or 2
[attr#1]: Error: cannot manually add attributes with the reserved ID of 1 or 2
Attribute 6101:3:1 (Application-Posture-Token) automatically added to dictionary (DB).
Attribute 6101:3:2 (System-Posture-Token) automatically added to dictionary (DB)
[attr#2]: Attribute 6101:3:3 (Software-Name) added to the dictionary (DB).
```

A. この出力に表示されているエラーは、ATP および STP に関する一般的なエラーです。ADF のインポートに問題がある場合には、ログファイルやポリシーにこのようなエラーは表示されません。

Q. CTA が表示できるユーザ通知メッセージの最大サイズを教えてください。

A. CTA v1.0 は、1000 のシングルバイト文字を表示できます。ASC がユーザ メッセージを 1000 文字までに制限します。

Q. CTA ユーザ通知ダイアログは、非 ASCII (ユニコード、マルチバイト) 文字をサポートしますか？

A. はい。CTA は UTF-8 エンコード文字列の表示をサポートしていますが、現在 ACS はメッセージの UTF-8 エンコードをサポートしていません。したがって、ユーザ通知ダイアログでは ASCII 文字のみ使用できます。

Q. CTA はホストで発生するポスチャ変更をどのようにして把握するのですか？

A. CTA は、ステータス クエリー プロセス中にポスチャのステータス変更の有無をポスチャ プラグインに確認します。それぞれのソフトウェアアプリケーションとエージェントのステータス変更の検知は、各ポスチャ プラグインが行います。

Q. PEAP トンネルを開始するために PA から送信される EAP アイデンティティとは何ですか？ ユーザ名、マシン名、あるいは IP アドレスですか？

A. PEAP トンネルを開始するために PA から送信される EAP アイデンティティは、空 (ヌル) の文字列です。PEAP トンネル内で提供される EAP アイデンティティは、NAC 認証の対象となるクライアントのマシン名：ユーザ名です。ログインしているユーザがない場合は、ユーザ名は SYSTEM に置き換えられます。

Q. CTA はなぜ Windows XP と連動しないのですか？

A. お客様が Windows XP と Service Pack 2 を使用している場合には連動しない可能性があります。Service Pack 2 の新しいファイアウォール機能が、NAC が使用するデフォルトの EAP-over-UDP ポート (UDP 21862 番ポート) をブロックするためです。Windows ファイアウォールを無効にするか、UDP 21862 番ポートへのトラフィックを許可するように設定してください。

Q. CTA が Windows のユーザ名およびパスワード クレデンシャルを使用できるようにするシングル サインオンの設定方法を教えてください。

A. シングル サインオン (SSO) を設定するには、サブリカントメニューの CTA deployment profile configuration で、「User Credentials」の「Use Single Sign-on for password credentials」のチェックボックスをチェックします。適切なサブディレクトリに XML ファイルを移動してから、クライアントを再起動します。デフォルトで作成されるディレクトリは、Cisco Systems, Inc\Cisco Trust Agent 802.1x wired client\profiles\networks and Cisco Systems, Inc\Cisco Trust Agent 802.1x wired client\profiles\policies です。

この作業が終了しているときは、ACS のネットワーク アクセス プロファイルで EAP-GTC が有効化されていないことを確認します。EAP-GTC は、常にサブリカントにパスワードを要求します。

Q. CTA にクライアントのインターネット ブラウザを自動起動させるにはどうすればよいのですか？

A. CTA 2.0 は、ACS で事前定義された URL を受信すると、クライアント マシン上でデフォルトの Web ブラウザを自動的に開くことができます。この URL は、通知文字列フィールドに各ポスチャ検証ルールを定義するときに設定できます。通知文字列に入力があると、CTA はクライアント デバイス上でデフォルトの Web ブラウザを起動し、この URL の表示を試みます。たとえば、検疫ルールのポスチャ アセスメント通知文字列に <http://x.x.x.x/quarantine.html> と入力すると、自動的にブラウザを起動して検疫アセスメントを行うことができます。

## CISCO SECURITY AGENT (CSA)

Q. NACをサポートしている CSA のバージョンを教えてください。これらの CSA は Cisco Trust Agent をインストールしますか？またどのようなアトリビュートを提供しますか？

A. 次の表を参照してください。

CSA バージョン	CTA インストール	アトリビュート
4.02+	しない	<ul style="list-style-type: none"><li>• Cisco:Host:ServicePacks</li><li>• Cisco:Host:Hotfixes</li><li>• Cisco:HIP:CSAVersion</li></ul>
4.5	する	<ul style="list-style-type: none"><li>• Cisco:HIP:CSAVersion</li><li>• Cisco:HIP:CSAOperationalState</li><li>• Cisco:HIP:CSAMCName</li><li>• Cisco:HIP:CSAStatus</li><li>• Cisco:HIP:DaysSinceLastSuccessfulPoll</li></ul>

Q. Cisco Trust Agent は、CSA のステータスの変更をネットワーク アクセス デバイスに通知するために非同期ステータス変更機能を使用しますか？

A. はい。非同期ステータス変更機能は CSA 4.5.1 でサポートされています。CSA に変更が発生した場合（ユーザが CSA を無効化したときなど）、CSA から Cisco Trust Agent への非同期ステータス クエリーが開始され、ネットワーク アクセス デバイスに EAPOL-Start が送信されます。非同期ステータス変更機能は、NAC L2 802.1x でのみサポートされています。

## NAC L3 IP (ルータ)

Q. ルータの NAC L3 IP 設定のサンプルはありますか？

A. はい。次の NAC 設定のサンプルは、2つのインターフェイスのみを装備する Cisco ISR 1800 シリーズ ルータのもので、クライアントのサブネットは 192.168.150.0/24、サーバのサブネットは 192.168.1.0/24 です。NAC 固有の設定エントリは太字で示しています。

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
!  
hostname NACPack-1800  
!  
aaa new-model  
!  
!  
aaa authentication login default none  
aaa authentication eou default group radius
```

```
aaa session-id common
ip subnet-zero
ip cef
!
!
ip auth-proxy inactivity-timer 5
ip admission inactivity-timer 5
ip admission name NAC eapoudp
!
ip ips po max-events 100
ip domain name cisco.com
ip name-server 192.168.1.5
no ftp-server write-enable
!
!
identity profile eapoudp
  description Exception list for CTA-less devices
  device authorize type cisco ip phone policy NAC_Exempt_Devices
  device authorize ip-address 192.168.150.10 policy NAC_Exempt_Devices
identity policy NAC_Exempt_Devices
  description NAC policy for authorized devices
  access-group ACL_Permit_All
eou clientless username clientless
eou clientless password clientless
eou allow clientless
eou timeout hold-period 60
eou timeout status-query 30
eou timeout revalidation 300
eou logging
!
!
interface FastEthernet0/0
  description NAC Server Network
  ip address 192.168.1.1 255.255.255.0
```

```

duplex auto
speed auto
!
interface FastEthernet0/1
description NAC Client Network
ip address 192.168.150.1 255.255.255.0
ip access-group ACL_Guest_Access in
ip admission NAC
duplex auto
speed auto
!
router eigrp 1
network 192.168.1.0
network 192.168.150.0
!
ip classless
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended ACL_Guest_Access
remark Allow EAPoUDP, DHCP, Remediation only for Guest Access
permit udp any any eq 21862
permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
permit tcp any host 192.168.1.7 eq www
deny ip any 192.168.1.0 0.0.0.255
permit ip any any
ip access-list extended ACL_NAC_Exempt
deny ip any any log
ip access-list extended ACL_Permit_All
permit ip any any log
!
ip radius source-interface FastEthernet0/0
!

```

```
radius-server host 192.168.1.2 auth-port 1645 acct-port 1646
radius-server key cisco123
radius-server vsa send authentication
!
control-plane
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  privilege level 15
  transport input telnet ssh
line vty 5 15
  privilege level 15
  transport input telnet ssh
!
end
```

Q. NAC 認証を開始させる最初のパケットがホストから送信されるとどうなりますか？

A. ルータのインターフェイスに適用されるアクセス コントロール リスト (ACL) およびダイナミックに挿入されるアクセス コントロール エントリ (ACE) によって異なります。これらのパケットは、デフォルトの ACL に拒否された場合、ルータが NAC 認証サーバからこのトラフィックを許可するダイナミック ACL を受信して挿入するまでドロップされます。ACS からダウンロードされたダイナミック ACL は、インターフェイス ACL より前に適用されるので、ポリシーの要件に応じて許可するアクセスを増やしたり減らしたりできます。

したがってデフォルトのインターフェイス ACL は、特にゲストにアクセスを提供する場合、ホストが必要とする最小限の L3 および L4 ネットワーク サービスを許可する必要があります。最小限のネットワーク サービスには、次のようなものがあります。

- EAPoUDP 応答 ( permit udp any any eq 21862 )
- DHCP 要求 ( permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps )
- ICMP エコー応答 ( permit icmp any any )
- DNS 要求 ( permit udp any any eq dns )
- NTP 要求 ( permit udp any any eq ntp )
- 証明書失効リスト (CRL) チェックの許可
- スプーフィングの防止 ( ローカル サブネットとは異なるアドレスから発信されているパケットのドロップ )
- ゲスト ユーザに対するインターネットへのデフォルト ネットワーク アクセスの提供

ルータ インターフェイス宛でのブロードキャスト、マルチキャストおよびトラフィックは、暗示的にポスチャリングから除外されます。ルータがホストから EAPoUDP 応答を受信できるように、インターフェイス ACL は EAPoUDP パケットを許可する必要があります。

Q. NAC と認証プロキシは同一のインターフェイスに共存できますか？ その場合、最初に始動するのはどちらですか？

A. 認証プロキシと NAC は同一のネットワーク インターフェイスで共存できます。認証プロキシが NAC より先に始動します。NAC のために NAD にダウンロードされた ACL は、認証プロキシの ACL を上書きします。

Q. NAC は Easy VPN と連動しますか？

A. Easy VPN サーバと NAC は同じインターフェイスに共存できます。Cisco Easy VPN Client バージョン 3.6.4 およびそれ以降は、NAC メッセージをサポートします。暗号化および解読プロセスは NAC 処理に干渉しません。

Q. NAC に割り当てられたダイナミック ACL はインターフェイス ACL からいつ削除されますか？

A. NAC に割り当てられたダイナミック ACL エントリは、別のポスチャ再検証によって変更されるか、一定の無活動期間の後に削除されます。この無活動期間は、無活動タイマー ( `ip admission inactivity-timer minutes` ) で定義されます。ダイナミック ACL が削除されると、他の NAC 認証が発生するまでデフォルトのインターフェイス ACL がホストに適用されます。デフォルトの無活動期間は 60 分です。

Q. NAD で `show eou all` コマンドを実行すると、さまざまな AuthTypes および Posture-Tokens が返されます。どのような意味があるのですか？

A. `show eou all` コマンドは、NAD が管理する NAC セッションの状態を表示します。

```
NACPack-1800# show eou all
```

```
-----
Address          Interface      AuthType      Posture-Token  Age (min)
-----
192.168.150.10   FastEthernet0/1  STATIC        -----        1
192.168.150.11   FastEthernet0/1  UNKNOWN       -----        1
192.168.150.12   FastEthernet0/1  Clientless    -----        1
192.168.150.13   FastEthernet0/1  Clientless    Healthy        1
192.168.150.14   FastEthernet0/1  EAP           -----        1
192.168.150.15   FastEthernet0/1  EAP           Healthy        1
192.168.150.16   FastEthernet0/1  EAP           Quarantine     1
```

上記のように、NAC には Authentication Types ( AuthTypes ) と Posture Token の多様な組み合わせがあります。

AuthType	Posture-Token	ステータス
STATIC	-----	NAD は、RADIUS を介して ACS に EAP 要求を行うことなく、ローカルの アイデンティティ プロファイルを使用してホストを認証しました。したがって ACS からのポスチャ トークンが存在せず、Posture-Token フィールドには ----- とだけ表示されています。
UNKNOWN	-----	<ul style="list-style-type: none"> <li>NAD も ACS もホストを認証できませんでした。次のような理由が考えられます。</li> <li>ホストに CTA がインストールされていませんでした。この場合、次のシナリオの 1 つが該当します。</li> <li>静的なルータ認証または ACS の Network Access Restriction ( NAR; ネットワークアクセス制限 ) で許可されるべき正規の Nonresponsive Host ( NRE; 非応答ホスト ) です。</li> </ul>

AuthType	Posture-Token	ステータス
		<ul style="list-style-type: none"> <li>CTA (およびその他のエージェント) を必要とする、修復が必要なホストです。</li> <li>管理者の管理対象外のゲスト ユーザ (顧客、コンサルタントなど) です。</li> <li>ホストにインストールされているパーソナル ファイアウォールが、NAD からの EAPoUDP チャレンジを UDP 21862 番ポートで受信する CTA の機能をブロックしています。</li> <li>NAD への CTA 応答をブロックするネットワークベース ファイアウォールが設置されています。</li> <li>ホストと ACS 間で EAP プロトコルに障害が発生しました。次のような理由が考えられます。</li> <li>ホストの CTA は、ACS または ACS のルート CA のデジタル証明書が追加されていないため、EAP を介した ACS へのクレデンシャルの提供を拒否しています。</li> <li>ホストの CTA には ACS または ACS のルート CA のデジタル証明書が追加されていますが、サブジェクト名が CTA の ctad.ini ファイルで許可されている証明書と一致しません。</li> <li>ACS のデジタル証明書が失効しました。ホストまたは ACS の時間同期の問題が原因の可能性がります。</li> <li>ACS にデジタル証明書がインストールされていません。</li> <li>ホストは ACS ネットワーク アクセス制限 (NAR) に許可されているクライアントレス ホストとして設定されていないため、ACS は認証に失敗しました。</li> </ul>
Clientless	-----	ホストは CTA がインストールされていませんが ACS にクライアントレス ホストとして認証されました。ポスチャトークン名は、このクライアントレス ユーザが割り当てられている ACS に Vendor Specific Attribute (VSA; ベンダー固有属性) を使用して定義されていないため、----- です。
Clientless	Healthy	ホストには CTA がインストールされていませんが、ACS に許可され、ポスチャ ステータス Healthy が与えられました。
EAP	-----	<ul style="list-style-type: none"> <li>ホストの CTA は、EAPoUDP を介して ACS との通信に成功しましたが、Posture-Token 名は NAD にダウンロードされませんでした。次のような理由が考えられます。</li> <li>ポスチャ トークン名は、このクライアントレス ユーザが割り当てられている ACS グループに Posture-Token VSA を使用して定義されていません。</li> <li>ネットワーク アクセス制限 (NAR) により完全な認証が妨げられています。ACS Failed Attempts ログ (ACS で Reports and Activities &gt; Failed Attempts を選択) で理由を確認してください。</li> </ul>
EAP	Healthy	ホストは ACS に認証され、ポスチャ ステータス Healthy が与えられました。
EAP	Quarantine	ホストは ACS に認証され、ポスチャ ステータス Quarantine が与えられました

Q. NAC は Host Standby Routing Protocol (HSRP) と連動しますか？プライマリ ルータに障害が発生した場合、セカンダリ ルータはすべての NAC セッションの再認証を行う必要がありますか？

A. NAC は HSRP と連動しますが、NAD から別の NAD への NAC セッション情報のステートフルなフェールオーバーは行われません。セカンダリ サーバは、すべてのホストの再認証を行います。

Q. AAA サーバがビジーな場合に発生する RADIUS フェールオーバーの時間を改善することはできますか？

A. `radius-server timeout <seconds>` コマンドを使用により、サーバをアクセス不能と決定するまでの IOS の待機時間を短縮できます。デフォルト値は 5 秒です。

`radius-server deadtime <minutes>` コマンドを使用すると、アクセス不能と判定されたサーバをバイパスする期間を IOS に通知できます。デフォルト値は 0 です。デフォルト値の場合、IOS はこのサーバを迂回せず、すべての新しい要求がリストの最初のサーバに送信されます

ユーザ体験に影響を与えずにパフォーマンスとスケーラビリティを改善するために、複数の ACS サーバを設置して IOS サーバロード バランシング (SLB) 機能の使用を検討することを推奨します。

Q. NAD が非応答 (クライアントレス) ホストを許可するようになるにはどのように設定すればよいのですか？

A. ルータに下記のいずれかを設定することで、CTA がインストールされていない非応答ホスト (NRE) を許可することができます。

1 つめは、ルータに設定されているアイデンティティ プロファイルおよびポリシーを使用し、IP アドレスまたは CDP デバイス タイプに応じてホストを静的に許可します。

```
identity profile eapoudp
  description Exception list for non-responsive devices
  device authorize type cisco ip phone policy NAC_Exempt_Devices
  device authorize ip-address 192.168.150.10 policy NAC_Exempt_Devices
identity policy NAC_Exempt_Devices
  description NAC policy for authorized devices
  access-group ACL_Permit_All
ip access-list extended ACL_Permit_All
  permit ip any any log
```

これらのホストは、ルータの STATIC 接続タイプに表示されます。

```
-----
Address          Interface          AuthType  Posture-Token  Age (min)
-----
192.168.150.10  FastEthernet0/1  STATIC    -----        1
```

2 つめは、特定のユーザ名とパスワードを使用する ACS にルータから RADIUS 要求を送信する方法です。ACS のこのユーザ プロファイル (この例では clientless) は、CTA を使用せずに MAC または IP アドレスに基づいて特定のホストを認証するネットワーク アクセス制限 (NAR) が設定されています。このオプションは、以下のコマンドを使用してルータに設定できます。

```
eou clientless username clientless
eou clientless password clientless
eou allow clientless
```

このクライアントレス 方式を使用して許可されるホストの AuthType は CLIENTLESS です。

```
NACPack-1800#show eou all
```

```
-----
Address          Interface          AuthType  Posture-Token  Age (min)
-----
192.168.150.7   FastEthernet0/1  CLIENTLESS  Unknown        0
```

この方法を使用する場合、このクライアントレス ユーザ名およびパスワードの組み合わせを ACS にも設定する必要があります。

3 つめの方法は、Catalyst 6500 でサポートされている MAC Authentication Bypass です。MAC-Auth-Bypass は Catalyst 6500 上で有効化され、MAC アドレスのリストは ACS に指定されます。次の例は、802.1x 認証のために正しい RADIUS 設定が行われていることを想定しています。MAC-Auth-Bypass を有効化するには、次のコマンドを使用します。

```
6506-dut> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
6506-dut> (enable) set port mac-auth-bypass 2/1 enable
Mac-Auth-Bypass successfully enabled on 2/1.
```

Q. 特定のホストセッションに URL リダイレクションが適用されていることを確認する方法を教えてください。

A. URL リダイレクションは、ポスチャ認証およびダウンロードされた ACL の適用後にオプションで実施されます。URL リダイレクションによって、Web ブラウザのユーザに自身のポスチャステータスを通知したり、ネットワークセキュリティポリシーに適合するために何をすべきかを気づかせたりすることができます。

NAD 上の特定のホストセッションに URL リダイレクションが適用されているかどうかを確認するには、**show eou ip <ip-address>** コマンドを使用します。

```
NACPack-1800#show eou ip 192.168.150.5
Address           : 192.168.150.5
Interface         : FastEthernet0/1
AuthType          : EAP
PostureToken      : Quarantine
Age (min)         : 0
URL Redirect      : http://192.168.1.7/quarantine.htm
ACL Name          : #ACSACL#-IP-Quarantine-41b7a0bf
Revalidation Period : 30 Seconds
Status Query Period : 30 Seconds
```

Q. URL リダイレクションがホストセッションに適用されていますが、ホストの Web ブラウザが指定された URL にリダイレクトされません。

A. URL リダイレクションは、次のシナリオでは機能しません。

- NAD HTTP サーバが無効化されている。ip http server コマンドで NAD Web サーバを有効化してください。
- NAC 対応インターフェイスにインターフェイス ACL が適用されていない。NAC 対応インターフェイスにインターフェイス ACL を適用してください。
- ACL エントリがクライアントの URL 宛先ホストをブロックしない。URL リダイレクションは、ユーザのブラウザが要求している宛先が ACL にブロックされるときにのみ行われます。クライアントのブラウザに指定されていた URL の宛先サーバが ACL に許可されている場合は、URL リダイレクションは行われません。

Q. ルータで NAC を有効化すると、SL\_DEF\_ACL という名前の ACL が作成されます。これは何に使用されるのですか？

A. これは適用されないテンプレート ACL です。このテンプレートは Advanced Security イメージによって自動的に作成されます。

Q. ホストが大きなファイルをダウンロードしている間にポスチャ再検証が発生するとどうなりますか？ダウンロードし直す必要がありますか？

A. NAD は、EAPoUDP を使用してポスチャの再検証を行うとき、認証が完了するまで以前と同じアクセス レベルを適用します。ポスチャ検証結果が以前と変わらない場合、エンドポイントのネットワーク フローは干渉されません。検証結果が以前と異なり、新しいポスチャに対して適用されるルールがこのタイプのトラフィックを禁止した場合は、エンドポイントのネットワーク フローが中断され、ネットワーク セッションがドロップされる可能性があります。

### NAC L2 IP (スイッチ)

Q. スwitchの場合、NAD 上の NAC 認証プロセスは何によって開始されますか？


A. NAD がクライアントから最初の DHCP 要求または ARP 要求を受信したときに開始されます。

Q. クライアントは NAC L2 IP を機能させるために、スイッチ インターフェイスに ACL が必要ですか？

A. NAC L2 IP は機能するためにインターフェイス ACL を必要としませんが、認証が行われる前に特定のタイプのトラフィックのみを許可するデフォルト ACL をスイッチ ポートに適用しておくことを推奨します。


Q. IOS スwitchの NAC L2 IP 設定のサンプルはありますか？

A.  
!  
version 12.2  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname NAC2Pack-3750  
!  
aaa new-model  
aaa authentication login local\_only line  
aaa authentication eou default group radius  
aaa authorization network default group radius  
aaa authorization auth-proxy default group radius  
!  
aaa session-id common  
vtp domain NAC  
vtp mode transparent  
ip subnet-zero  
ip routing



```
no ip domain-lookup
ip domain-name nac.cisco.com
ip name-server 10.0.200.10
ip admission name NAC-L2-IP eapoudp
!
ip dhcp snooping vlan 1000
ip dhcp-server 10.0.200.10
ip device tracking
!
eou allow clientless
eou timeout hold-period 3600
eou timeout status-query 10
eou timeout revalidation 3600
eou logging
!
vlan internal allocation policy ascending
!
vlan 10
  name employees
vlan 20
  name contractors
vlan 30
  name utilities
vlan 40
  name guests
vlan 50
  name healthy
vlan 60
  name checkup
vlan 70
  name transition
vlan 80
  name quarantine
vlan 90
```

```
name infected
vlan 100
name unknown
vlan 110
name voice
vlan 200
name server VLAN
vlan 255
name NAD MGMT
vlan 1000
name NAC L2 IP Default VLAN
!
interface GigabitEthernet1/0/2
description NAC-L2-IP
switchport access vlan 1000
switchport mode access
ip access-group interface_acl in
spanning-tree portfast
ip admission NAC-L2-IP
!
interface Vlan10
description Employees VLAN
ip address 10.6.10.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan20
description Contractors VLAN
ip address 10.6.20.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan30
description Utilities VLAN
ip address 10.6.30.1 255.255.255.0
ip helper-address 10.0.200.10
```



```
!  
interface Vlan40  
  description Guests VLAN  
  ip address 10.6.40.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan50  
  description Healthy VLAN  
  ip address 10.6.50.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan60  
  description Checkup VLAN  
  ip address 10.6.60.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan70  
  description Transition VLAN  
  ip address 10.6.70.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan80  
  description Quarantine VLAN  
  ip address 10.6.80.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan90  
  description Infected VLAN  
  ip address 10.6.90.1 255.255.255.0  
  ip helper-address 10.0.200.10  
!  
interface Vlan100  
  description Unknown VLAN  
  ip address 10.6.100.1 255.255.255.0
```

```
ip helper-address 10.0.200.10
!
interface Vlan110
description Voice VLAN
ip address 10.6.110.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan200
description Server VLAN
ip address 10.0.200.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan1000
description Default Interface VLAN
ip address 10.6.1.1 255.255.255.0
ip helper-address 10.0.200.10
!
ip http server
ip http authentication aaa
no ip http secure-server
!
ip radius source-interface GigabitEthernet1/0/24
!
ip access-list extended audit_acl
permit tcp any any eq www
ip access-list extended interface_acl
permit udp any any eq 21862
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit icmp any any
ip access-list extended quarantine_url_redir_acl
deny tcp any host 10.0.200.30 eq www
deny tcp any host 10.0.200.101 eq www
permit tcp any any eq www
```

```
!  
radius-server attribute 6 on-for-login-auth  
radius-server attribute 8 include-in-access-req  
radius-server attribute 25 include-in-access-req  
radius-server host 10.0.200.20 auth-port 1645 acct-port 1646 key cisco123  
radius-server source-ports 1645-1646  
radius-server vsa send authentication  
!
```

Q. CatOS スイッチの NAC L2 IP 設定のサンプルはありますか？

A.

```
#version 8.5(0.123)JAC  
!  
#Nac  
set eou enable  
!  
#radius  
set radius server 10.0.200.20 auth-port 1812 primary  
set radius key cisco123  
!  
set vlan 10 name employees type ethernet mtu 1500 said 100010 state active  
set vlan 20 name contractors type ethernet mtu 1500 said 100020 state active  
set vlan 30 name utilities type ethernet mtu 1500 said 100030 state active  
set vlan 40 name guests type ethernet mtu 1500 said 100040 state active  
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active  
set vlan 60 name checkup type ethernet mtu 1500 said 100060 state active  
set vlan 70 name transition type ethernet mtu 1500 said 100070 state active  
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active  
set vlan 90 name infected type ethernet mtu 1500 said 100090 state active  
set vlan 100 name unknown type ethernet mtu 1500 said 100100 state active  
set vlan 110 name voice type ethernet mtu 1500 said 100110 state active  
set vlan 200 name servers type ethernet mtu 1500 said 100110 state active  
set vlan 255 name nads_mgmt type ethernet mtu 1500 said 100255 state active  
set vlan 1000 name default_L2IP type ethernet mtu 1500 said 100110 state active  
!
```

```

#acl
!
#security ACLs
clear security acl all
!
set security acl ip nac-l2-ip permit arp
set security acl ip nac-l2-ip permit dhcp-snooping
! Required for CatOS
set security acl ip nac-l2-ip permit arp-inspection any any
set security acl ip nac-l2-ip permit eapoudp
commit security acl all
set security acl map nac-l2-ip 1000
!
#module 2
set vlan 1000 2/1
set port eou 2/2 auto
!
end

```

Q. ACS から Downloadable ACL がスイッチに適用されていることを確認する方法を教えてください。

A. スイッチで **show ip access-lists** コマンドを入力します。次の例は、ACS からダウンロードされた Healthy\_ACL がスイッチに適用されていることを示しています。

```

NAC4948#show ip access-lists
Extended IP access interface_acl
    10 permit udp any any eq 21862
    20 permit udp any host 10.0.200.10 eq domain
    30 permit udp any eq bootpc any eq bootps
    40 permit icmp any any
Extended IP access list quarantine_url_redir_acl
    10 deny tcp any host 10.0.200.30 eq www
    30 permit tcp any any eq www
Extended IP access list xACSACLx-IP-Healthy_ACL-433866ab
    10 permit ip any any

```

Q. ACS から Downloadable ACL が特定のスイッチ ポートに適用されていることを確認する方法を教えてください。

A. 次の例に示すように `show ip access-list interface x/x` コマンドを入力します。クライアントの IP アドレスが ACL の送信元を指定している `any` とダイナミックにリプレースされます。

```
NAc4948#show ip access-list interface GigE 1/1
IP Admission access control entires (Inbound)
    permit ip host 10.7.1.2 any
```

Q. IP Device Tracking コマンドとは何ですか？どのような目的で使用されますか？

A. IP Device Tracking Table (IP デバイストラッキングテーブル) は IP デバイスをトラッキングし、それらのホストがまだ存在しているかどうかを確認するプローブを定期的に生成します。LPIP (LAN Port IP) に使用される EOU セッションは、IP Device Tracking Table にホストが表示されるかどうかに基づいて作成と削除が行われます。

## NAc L2 802.1X

Q. NAc L2 802.1x ではクライアントからどのようなタイプのクレデンシャルが送信されますか？

A. Microsoft Windows 環境では、2 つのアイデンティティ クレデンシャル セットをネットワークに提示できます。

1 つめのセットは、ユーザ認証の前にマシンを認証するマシン認証の概念に基づいています。Microsoft は、ブート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ャルを使用してクライアントシステムを認証するマシン認証機能を提供しています。クライアントは、マシン認証後、ドメイン Group Policy Object (GPO; グループ ポリシー オブジェクト) 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します。

マシン認証により、コンピュータは、ブート時にデバイス 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の認証を実施します。コンピュータは、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ます。マシン認証によって、802.1x の使用時にドメイン GPO が機能しなくなる問題が改善されました。

802.1x で使用される 2 つめのタイプのクレデンシャルは、ユーザ認証です。ユーザが Graphic Identification and Authentication (GINA) (ログイン画面) でコンピュータまたは Windows ドメインにログインすると、ログインに使用したユーザ名とパスワードが 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されます。

Q. NAc L2 802.1x でクライアントが認証されませんでした。Windows のタスクバーには CTA アイコンが表示されていません。

A. サブリカントを含む CTA インストール ファイルがインストールされているかどうか確認してください。サブリカントを含まない CTA のバージョンがインストールされている場合は、サブリカントメニューにアクセスできないため、Windows タスクバーにサブリカント アイコンが表示されません。したがって NAc L2 802.1x によるクライアント認証は実施できません。

Q. スイッチのインターフェイスの 802.1x 情報を表示する方法を教えてください。

A.

```
show dot1x all
Dot1x Info for interface GigabitEthernet 1/1
-----
Supplicant MAC 000d.80cd.cda6
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
```

```

Posture           = Healthy
ReAuthPeriod     = 3600 Seconds (From Authentication Server)
ReAuthAction     = Terminate
TimeToNextReauth = 3570 Seconds
PortStatus       = AUTHORIZED
MaxReq           = 2
MaxAuthReq       = 2
HostMode         = Single
PortControl      = Auto
ControlDirection = Both
QuietPeriod      = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod     = From Authentication Server
ServerTimeout    = 30 Seconds
SuppTimeout      = 30 Seconds
TxPeriod         = 30 Seconds
Guest-Vlan       = 0

```

Q. 特定のスイッチ ポートが適切な VLAN に配置されていることを確認する方法を教えてください。

A.

```
show vlan
```

```

VLAN Name                Status    Ports
-----
1    default                active    Ge1/5, Ge1/6, Ge1/7, Ge1/8
                                     Ge1/9, Ge1/10, Ge1/13, Ge1/15
                                     Ge1/16, Ge1/17, Ge1/18, Ge1/19
                                     Ge1/20, Ge1/21, Ge1/22, Ge1/23
                                     Ge1/24, Gi1/2
10   employees              active    Ge1/3
20   contractors            active
30   utilities              active
40   guests                 active
50   healthy                active   Ge1/1
60   checkup                active

```

```
70 transition active
80 quarantine active
90 infected active
100 unknown active Ge1/4, Ge1/11, Ge1/14
110 voice active
200 servers active Ge1/12
255 nads active
```

クライアントスイッチポートがVLAN 50 (healthy) に配置されていることが確認できます。

このインターフェイス コマンドは、インターフェイスのスイッチポート情報の確認にも使用できます。

```
show int GigE 1/1 switchport
```

```
Name: Ge1/1
```

```
Switchport: Enabled
```

```
Administrative Mode: static access
```

```
Operational Mode: static access
```

```
Administrative Trunking Encapsulation: negotiate
```

```
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: Off
```

```
Access Mode VLAN: 50 (healthy)
```

```
...output truncated
```


Q. Cisco IOS が稼動しているスイッチの NAC L2 802.1x 設定のサンプルはありますか？

A. 次の内容を参照してください。


```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NAC2Pack-3750
!
!
aaa new-model
aaa authentication login local_only line
```




```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
clock timezone PST -8
switch 1 provision ws-c3750g-24t
vtp domain NAC
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name nac.cisco.com
ip name-server 10.0.200.10
!
ip dhcp-server 10.0.200.10
!
dot1x system-auth-control
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
    name employees
vlan 20
    name contractors
vlan 30
    name utilities
vlan 40
    name guests
vlan 50
    name healthy
```



```
vlan 60
  name checkup
vlan 70
  name transition
vlan 80
  name quarantine
vlan 90
  name infected
vlan 100
  name unknown
vlan 110
  name voice
vlan 200
  name servers
vlan 255
  name nads
vlan 1000
  name l2ip
!
interface GigabitEthernet1/0/1
  description NAC-L2-802.1x
  switchport mode access
dot1x reauthentication
dot1x port-control auto
dot1x timeout reauth-period server
spanning-tree portfast
!!
interface Vlan10
  description Employees VLAN
  ip address 10.6.10.1 255.255.255.0
  ip helper-address 10.0.200.10
!
interface Vlan20
  description Contractors VLAN
```



```
ip address 10.6.20.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan30
description Utilities VLAN
ip address 10.6.30.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan40
description Guests VLAN
ip address 10.6.40.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan50
description Healthy VLAN
ip address 10.6.50.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan60
description Checkup VLAN
ip address 10.6.60.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan70
description Transition VLAN
ip address 10.6.70.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan80
description Quarantine VLAN
ip address 10.6.80.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan90
```



```
description Infected VLAN
ip address 10.6.90.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan100
description Unknown VLAN
ip address 10.6.100.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan110
description Voice VLAN
ip address 10.6.110.1 255.255.255.0
ip helper-address 10.0.200.10
!
interface Vlan200
description Servers VLAN
ip address 10.0.200.1 255.255.255.0
ip helper-address 10.0.200.10
!

ip http server
ip http authentication aaa
no ip http secure-server
!
ip radius source-interface GigabitEthernet1/0/24
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 include-in-access-req
radius-server host 10.0.200.20 auth-port 1645 acct-port 1646 key cisco123
radius-server source-ports 1645-1646
radius-server vsa send authentication
!
```

Q. CatOS が稼働しているスイッチの NAC L2 802.1x 設定のサンプルはありますか？

A.

```
#version 8.5(0.123)JAC
!
#dot1x
set dot1x radius-keepalive disable
!
!
#radius
set radius server 10.0.200.20 auth-port 1812 primary
set radius key cisco123
!
set vlan 10 name employees type ethernet mtu 1500 said 100010 state active
set vlan 20 name contractors type ethernet mtu 1500 said 100020 state active
set vlan 30 name utilities type ethernet mtu 1500 said 100030 state active
set vlan 40 name guests type ethernet mtu 1500 said 100040 state active
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active
set vlan 60 name checkup type ethernet mtu 1500 said 100060 state active
set vlan 70 name transition type ethernet mtu 1500 said 100070 state active
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active
set vlan 90 name infected type ethernet mtu 1500 said 100090 state active
set vlan 100 name unknown type ethernet mtu 1500 said 100100 state active
set vlan 110 name voice type ethernet mtu 1500 said 100110 state active
set vlan 255 name nads type ethernet mtu 1500 said 100255 state active
!
!
#acl
!
#security ACLs
clear security acl all
#nac_pbacl
set security acl ip nac_pbacl permit arp
set security acl ip nac_pbacl permit arp-inspection any any
set security acl ip nac_pbacl permit dhcp-snooping
```

```
set security acl ip nac_pbacl permit udp any any eq 53
set security acl ip nac_pbacl permit ip group healthy_hosts any
set security acl ip nac_pbacl permit ip group quarantine_hosts 10.0.200.0 0.0.0.
255
set security acl ip nac_pbacl permit ip 10.0.200.0 0.0.0.255 group quarantine_ho
sts
set security acl ip nac_pbacl permit ip group quarantine_hosts host 10.40.80.1
set security acl ip nac_pbacl permit ip host 10.40.80.1 group quarantine_hosts
#
commit security acl all
set security acl map nac_pbacl 80
set security acl map nac_pbacl 50 statistics enable
!
set port dot1x 2/2 port-control auto
```

## CISCO SECURE ACCESS CONTROL SERVER ( ACS )

Q. NAC をサポートしている ACS のバージョンを教えてください。

A. ACS バージョン 3.3.1 またはそれ以降で NAC L3 IP をサポートしています。ACS バージョン 4.0 およびそれ以降では、NAC L2 IP および NAC L2 802.1x をサポートしています。

Q. ACS 4.0 には、バージョン 3.3.1 とは異なる新しい NAC 設定エリアがあります。その違いを教えてください。

A. 新しいバージョンでは、External User Database エリアから NAC 固有の設定が削除されました。また、Posture Validation Policy は「Posture Validation」ボタンで設定します。

ACS 4.0 には、アクセス サービスのためのネットワーク アクセス プロファイルの概念も導入されました。これらのプロファイルは、着信認証の確認に使用されます。アクセス サービスは、ポスチャ ポリシーと認証コンポーネントを結びつけます。このサービスはネットワーク アクセス プロファイルで設定します。

Q. 無償で提供されている NAC 用の ACS の試用版はどこでダウンロードできるのですか？

A. ユーザ登録されているお客様は、90 日間無償で使用できる ACS の試用版を <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-eval> からダウンロードできます。

Q. マスター ACS サーバとスレーブ ACS サーバ間で NAC ポリシーを複製できますか？

A. はい。ACS v3.3.1 では NAC ポリシーを複製できます。ただし、NAC 外部データベースは複製されません。したがってポリシーを複製するには、ポリシーの複製先のスレーブサーバにすべての NAC 外部データベースを同じ名前で作成しておく必要があります。この情報については、『ACS 3.3 リリースノート』を参照してください。

Q. NAC 認証を制御するためのシスコ独自のベンダー固有属性 ( VSA ) は何ですか？

A. ACS が、各ユーザおよびグループに対して設定できる VSA を提供しています。

- posture-token : NAC セッションに表示されるポスチャ トークン文字列です。
- status-query-timeout : ルータのステータス クエリー タイマーを上書きします。

- url-redirect : Web ブラウザをリダイレクトするための URL です。

これらのアトリビュートは、cisco-av-pair セクションの Cisco IOS/PIX RADIUS Attributes の下の ACS User or Group Setup で設定します。VSA 設定の例を示します。

```
posture-token=Quarantine
url-redirect=http://remediation.cisco.com/Quarantine/
status-query-timeout=30
```

VSA 名は大文字と小文字が区別されます。VSA 名には、上記の例のようにすべて小文字を使用する必要があります。

Q. ACS 4.0 にはどのようなデフォルト プロファイル テンプレートがありますか？どのテンプレートを選択して設定を開始すればよいのですか？

A. ACS 4.0 にはあらかじめ 7 つのプロファイル テンプレートが用意されています。

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless ( NAC L2 802.1x )
- Authentication Bypass ( 802.1x フォールバック )
- Agentless Host

これらのうち 1 つのテンプレートを選択するには、「Network Access Profiles」から「Add Template Profile」を選択します。新しいプロファイルのベースとして使用するテンプレートを選択してください。

Q. ACS のグループ設定を使用して再検証期間を設定できますか？

A. はい。グループ設定の IOS/PIX アトリビュート エリアの IETF RADIUS Attribute #027 Session-Timeout を使用して設定します。

Q. ステータス クエリー期間と再検証期間の違いを教えてください。

A. エンドポイントの最初のポスチャ検証の終了後、ステータス クエリー期間と再認証期間両方が設定され、NAD で実行されます。特定の EAPoUDP セッションの各値は、確認可能です。

```
NACPack-1800#show eou ip 192.168.150.5
Address           : 192.168.150.5
Interface         : FastEthernet0/1
AuthType          : EAP
PostureToken      : Healthy
Age (min)         : 2
URL Redirect      :
ACL Name          : #ACSACL#-IP-Healthy-41b7a0bf
Revalidation Period : 600 Seconds
Status Query Period : 30 Seconds
```

ステータス クエリー期間は、NAD からエンドポイントへの軽量のポーリングを比較的短い間隔（300 秒未満）で開始させます。この間隔が短いほど、NAC はポスチャの変更をより早く検出し、適切なレベルのポリシーを適用することができます。ステータス クエリーは次のような複数の目的を達成します。

- ステータス クエリーは、ポーリング タスクを ACS から NAD に移行し、ポスチャ検証のために ACS にかかる負荷を軽減します。
- IP (L3) ルータはリンク レベル (L2) でのエンドポイントの切断を検出できないため、ステータス クエリーによって特定のエンドポイントがまだネットワーク上に存在するかどうかを確認します。エンドポイントが応答しない場合、NAC セッションは EAPoUDP テーブルから削除されます。
- ステータス クエリーは、暗号を使用してエンドポイントが前回ポスチャ認証されたエンドポイントと同一かどうかを確認します。この確認は、最後のポスチャ検証中に PEAP トンネルによって生成された暗号化鍵を使用して行われます。DHCP によって割当てられたアドレスを持つエンドポイントがネットワーク接続を切断したあとに、別のホストが同じ IP アドレスを使用することがあるため、この確認が必要となります。鍵が一致しない場合には、この EAPoUDP テーブルのエントリは NAD から削除され、ポスチャ認証のために新しいエンドポイントに対して EAPoUDP 要求が送信されます。
- ステータス クエリーにより、CTA は各ポスチャ プラグインに対し、それぞれのエージェントやアプリケーションに変更がないかどうかの確認を開始します。CTA はプラグインのすべての応答を収集し、NAD に単一のステータス結果を返します。いずれかのアプリケーションのポスチャに変更があった場合、NAD はポスチャの再検証を実行します。
- 再検証期間は、実質上 EAPoUDP セッション期間です。再検証期間が失効すると、最後のステータス クエリーの結果に関わらず、NAD にとってエンドポイントのポスチャは無効になります。この場合、NAD はエンドポイントに新しい EAPoUDP チャレンジを送信し、ACS によるポスチャ認証も開始されます。再検証期間が比較的短いと（300 秒以下）ACS サーバへの負荷が高くなるので注意してください。

Q. ユーザ通知メッセージを他の言語で作成することはできますか？

A. いいえ。NAC は文字列データ タイプの UTF-8 エンコードをサポートしていますが、現在のバージョンの ACS は 通知メッセージの UTF-8 へのエンコードをサポートしていません。

Q. ACS データ ディレクトリにどのようなベンダー アトリビュートが保管されているかを確認する方法を教えてください。

A. 次のコマンドを使用して ACS for Windows の現在の NAC データ ディレクトリの内容を表示できます。

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -dumpAVP avpdump.txt
```

ACS Solution Engine のアトリビュート ファイルをエクスポートするには、System Configuration > CNAC Attributes Management 画面で Dump Attributes オプションを使用してアトリビュート定義ファイルのダウンロードを行います。

Q. 現在使用している ACS のバージョンには、ベンダー xyz 社の NAC クレデンシャル タイプおよびアトリビュートが表示されません。新しい NAC クレデンシャル タイプを ACS データ ディレクトリにインポートする方法を教えてください。

A. まず、ベンダーから使用するアトリビュート記述ファイル (\*.ini or \*.txt) を取得する必要があります。新しい NAC アトリビュート ファイルのインポート方法は、『Cisco Secure ACS for Windows Server ユーザ ガイド』に記載されています。ACS for Windows では、次のインポート コマンドを使用します。

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -addAVP new_avps.ini
```

アトリビュートは、ACS Solution Engine の System Configuration > CNAC Attributes Management 画面で FTP サーバからインポートできます。

Q. ASC のユーザ通知メッセージの最大サイズを教えてください。

A. ASC は、ユーザメッセージを 1000 のシングルバイト文字までに制限します。ダブルバイト言語の UTF-8 エンコードはサポートされていません。

Q. ACS ではどのような正規表現がサポートされていますか？

A.

- **^(カレット)** — ^ 演算子は、文字列の先頭とマッチします。たとえば、^Ci は、文字列「Cisco」や「Ciena」にマッチします。
- **\$(ドル記号)** — \$ 演算子は、文字列の末尾とマッチします。たとえば、co\$ は、文字列「Cisco」や「Tibco」にマッチします。

Q. == および != 演算子を使用して文字列をマッチングできますか？

A. == および != 演算子は、文字列のすべての文字の完全マッチです。これは、ACS Passed Authentications ログで生成された文字列の内容を確認するのに便利です。文字列によっては、文字列の先頭、末尾、またはその両方で「|」文字をデリミタとして使用することがあります。

サブ文字列のチェックのみを行う場合は、contains 演算子を使用します。

Q. Network Access Profiles で作成した新しいプロファイルで、active の列に「NO」と表示されるのはなぜですか？

A. プロファイルを有効にするには、Network Access Profile setup ページで active を選択する必要があります。

Q. 複数のプロファイルが設定されている場合、ACS はどのようにして使用するプロファイルを決めるのですか？

A. ACS はアクティブな Network Access Profiles の順序付けされたリストを検証し、RADIUS トランザクションをプロファイルに 1 つマッピングします。ACS は、トランザクションの最初のアクセス要求をマッピングするときに最小に合致したものを適用します。

Q. ACS は設定されたすべてのアトリビュートをチェックするのですか？

A. ACS 4.0 は、ユーザが Network access profile の ポスチャポリシーの設定で選択またはチェックしたアトリビュートのみをチェックします。

Q. ACS があるホストを拒否し、このイベントを Failed Attempts ログに記録しました。何が問題なのですか？

A. まず Reason フィールドで、この拒否が「外部サーバからトークンを受け取っていない」といったポスチャ検証エラーによって発生しているかどうかを確認します。また、Mandatory Credential Type の指定が多いことを示す「必須のクレデンシャルがマッチしていない」というようなメッセージを伴う拒否も頻繁に発生します。

シスコでは、要件を最小限に抑えた CTA - Only NAC データベースを作成することを強く推奨します。この設定では、Mandatory Credential Type として Cisco:PA のみを要求します。CTA - Only NAC データベースは、他のデータベースよりも先に使用されないように、Unknown User Policy の選択データベース リストの最後に配置します。このデータベースにフェールオーバーされたホストは、必要とされる他のクレデンシャルタイプを持たないため、検疫が必要となります。この手法により、ホストを拒否することなく、ホストを特定して検疫することが可能になります。

Failed Attempts ログに表示される他のメッセージの例を示します。

Authen-Failure-Code Field	Filter Information Field	ステータス
External DB Account Restriction		<p>NAC データベース設定に問題がありました。</p> <ul style="list-style-type: none"><li>• 外部 Posture Validation Server (PVS; ポスチャ検証サーバ) からポスチャトークンを受信していない可能性があります。サーバが正しく設定されていること、ACS が PVS の正しい URL を要求していることを確認してください。</li><li>• NAC データベースの Mandatory Credential Type に指定されているクレデンシャルのタイプが多すぎる可能性があります。Mandatory Credential Type として Cisco:PA のみを要求する、要件を最小限に抑えた NAC 外部データベースを作成します。これにより、CTA だけでホストを特定し、検疫して必要な更新を行うことが可能になります。</li></ul>

Authen-Failure-Code Field	Filter Information Field	ステータス
User Access Filtered	No Access Filters Passed.	ネットワーク アクセス制限 (NAR) によってエンドポイントをフィルタリングしようとしたが、フィルタがマッチしなかったためエンドポイントは認証されませんでした。これは、非応答エンドポイント (NRE) (ゲスト ユーザまたは CTA が必要なエンドポイント) の拒否を意味します。エンドポイントを NRE として認証する必要がある場合は、NAR を更新してください。

Q. ACS アプライアンスにパートナーのアトリビュート定義ファイル (ADF) をインストールする方法を教えてください。

A. ACS Solution Engine の UI 画面で、FTP を介して NAC の ADF ファイルをインポートできます。

ADF インポート画面は、System Configuration > CNAC Attribute Management にあります (『Cisco Secure ACS SE Version 3.3 ユーザガイド』を参照)。

[http://www.cisco.com/en/US/partner/products/sw/secursw/ps5338/products\\_user\\_guide\\_chapter09186a0080233621.html#wp617750](http://www.cisco.com/en/US/partner/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080233621.html#wp617750)

パートナー ADF に定義されているフィールドの例を示します。

```
[attr#0]
vendor-id=
vendor-name=
application-id=
application-name=
attribute-id=
attribute-name=
attribute-profile=
attribute-type=
```

Q. 複数のアンチウイルス エージェントをチェックするには、ACS をどのように設定すればよいのですか？

A. ACS 外部 NAC データベースおよびポリシーを次の例と同様に設定してください。

作成した各 NAC データベースには、必ず Database Group Mappings および Unknown User Policy を設定してください。NAC 認証を成功させるために必要です。

以下に NAC のために ACS に設定するマルチベンダーのアンチウイルス ポリシーの例を示します。

NAC データベース (ポリシー定義については、下部のローカル ポリシーを参照してください)。

#### CTA-Only

Mandatory Credential Types	Credential Validation Policies
Cisco:PA	<ul style="list-style-type: none"> <li>CTA-Policy</li> <li>Windows-Basic-Policy</li> </ul>

## CTA+NAI

Mandatory Credential Types	Credential Validation Policies
Cisco:PA NAI:AV	<ul style="list-style-type: none"><li>• CTA-Policy</li><li>• Windows-Basic-Policy</li><li>• NAI-Policy</li></ul>

## CTA+Symantec

Mandatory Credential Types	Credential Validation Policies
Cisco:PA Symantec:AV	<ul style="list-style-type: none"><li>• CTA-Policy</li><li>• Windows-Basic-Policy</li><li>• Symantec-Policy</li></ul>

## CTA+Trend

Mandatory Credential Types	Credential Validation Policies
Cisco:PA Trend:AV	<ul style="list-style-type: none"><li>• CTA-Policy</li><li>• Windows-Basic-Policy</li><li>• Trend-Policy</li></ul>

ローカル ポリシー（ポリシーは複数のデータベースで再利用できます）

## CTA-Policy

Rules	Credential Type	Token	Action
Cisco:PA:PA-Version >= 1.0.53	Cisco:PA	Healthy	
Default	Cisco:PA	Quarantine	

## Windows-Basic-Policy

Rules	Credential Type	Token	Action
Cisco:PA:OS-Type contains Windows 2000 Cisco:PA:OS-Version >= 5.0.2195.0	Cisco:Host*	Healthy	
Cisco:PA:OS-Type contains Windows XP Cisco:PA:OS-Version >= 5.1.0.0	Cisco:Host	Healthy	
Default	Cisco:Host	Quarantine	

## NAI-Policy

Rules	Credential Type	Token	Action
NAI:AV:Software-Version >= 7.1.0.0 NAI:AV:Scan-Engine-Version >= 4.3.20 NAI:AV:Dat-Version >= 4.0.4367.0 NAI:AV:Protection-Enabled = 1	NAI:AV	Healthy	
Default	NAI:AV	Quarantine	

## Symantec-Policy

Rules	Credential Type	Token	Action
Symantec:AV:Software-Version >= 8.1.0.825 Symantec:AV:Scan-Engine-Version >= 1.3.0.12 Symantec:AV:Dat-Version >= 2005.1.20.8 Symantec:AV:Protection-Enabled = 1	Symantec:AV	Healthy	
Default	Symantec:AV	Quarantine	

## Trend-Policy

Rules	Credential Type	Token	Action
Trend:AV:Software-Version >= 6.5.0.0 Trend:AV:Scan-Engine-Version >= 7.1.0.1003 Trend:AV:Dat-Version >= 1.919.0.0 Trend:AV:Protection-Enabled = 1	Trend:AV	Healthy	
Default	Trend:AV	Quarantine	

Q. ACS が Host Credential Authorization Protocol ( HCAP ) ポスチャ検証サーバから応答を受信できない場合どうなりますか？

A. ポスチャ検証サーバ ( PVS ) が応答できない場合、ACS は Access-Reject でルータの RADIUS 要求に応答します。次に ACS は、外部 PVS から応答を受信しなかったことを示すログメッセージを Failed Attempts ログに記録します。ルータは、定義されている保留期間の間、EoU セッションを INIT ステートに置き、( NAC 対応インターフェイス ACL に従って ) デフォルトのネットワークアクセスのみを許可します。この保留期間の失効後、エンドポイントがルータにトラフィックを送信すると、NAC 認証プロセスが再度開始されます。

## パートナー

Q. xyz 社は NAC をサポートしていますか？どの企業のソフトウェアのバージョンが NAC をサポートしているのですか？どのパートナーが NAC のレポートソリューションを提供していますか？

A. 各ベンダー サポートの詳細情報は、次の NAC Partner Program サイトの NAC Participant List を参照してください。

<http://www.cisco.com/en/US/partners/pr46/nac/partners.html>

Q. シスコはすべてのパートナーのすべての NAC アトリビュートの包括的なリポジトリを保持していますか？

A. いいえ。お客様が各ベンダーから NAC アトリビュートを取得する必要があります。

Q. Cisco Secure ACS インストールで特定のベンダーの NAC アトリビュート ファイルを確認できません。どこで取得できるのですか？またどのようにインポートすればよいのですか？

A. ベンダーの NAC アトリビュートファイルを .ini または .txt ファイル形式で取得する必要があります。これらのアトリビュートファイルは、ベンダーがソフトウェアとともに提供します。新しい NAC アトリビュート ファイルのインポート方法の概要はこの文書の ACS セクションに、詳しい情報は『Cisco Secure ACS ユーザ ガイド』に掲載されています。

## 略語と用語

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

略語	説明
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 )

略語	説明
<b>NDIS</b>	
<b>NDS</b>	Netware Directory Services (Novell)
<b>NRH</b>	Non Responding Host (非応答ホスト)
<b>NTLM</b>	
<b>ODBC</b>	Open Database Connect
<b>OOB</b>	Out Of Band (アウトオブバンド)
<b>OS</b>	Operating System (オペレーティングシステム)
<b>OTP</b>	One Time Password (ワンタイムパスワード)
<b>PA</b>	Posture Attribute (ポスチャアトリビュート)
<b>PAC</b>	Provisioned Access Credential
<b>PACL</b>	Port ACL (ポート ACL)
<b>PAE</b>	Port Access Entity (ポートアクセスエントリ)
<b>PBACL</b>	Policy Based ACL (ポリシーベース ACL)
<b>PEAP</b>	Protected EAP
<b>PKI</b>	Public Key Infrastructure (公開キー インフラストラクチャ)
<b>PPTP</b>	
<b>PVLAN</b>	Private VLAN (プライベート VLAN)
<b>QoS</b>	Quality of Service
<b>RAC</b>	RADIUS Attribute Component
<b>RPC</b>	Remote Procedure Call (リモート プロシージャ コール)
<b>SAML</b>	Security Assertion Markup Language
<b>SIMS</b>	Security Information Management System (セキュリティ情報管理システム)
<b>SLB</b>	Server Load Balancing (サーバ負荷バランシング)
<b>SMB</b>	Server Message Block
<b>SNMP</b>	Simple Network Management Protocol
<b>SQ</b>	Status Query (ステータス クエリー)
<b>SSL</b>	Secure Sockets Layer
<b>TCP</b>	Transport Control Protocol
<b>TLS</b>	Tunnel Layer Security
<b>TLV</b>	Type Length Value
<b>UDP</b>	Universal Datagram Protocol
<b>URL</b>	Universal Resource Locator
<b>VACL</b>	VLAN ACL
<b>VLAN</b>	Virtual Local Area Network (仮想 LAN)
<b>VoIP</b>	Voice over IP
<b>VPN</b>	Virtual Private Network (バーチャルプライベートネットワーク)
<b>VSA</b>	Vendor Specific Attribute (ベンダー固有属性)

略語	説明
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	定義
802.1x、dot1x	IEEE 802.1x。レイヤ 2 のネットワーク認証方式を定めた標準。無線ネットワーク用の 802.11a/b/g と混同しないようにしてください。
AAA	Authentication, Authorization, and Accounting (認証、認可、アカウントリング)。通常は、ダイヤルアップ、無線、VPN、802.1x などのユーザのネットワーク アクセスを認証する機能です。中央の AAA サーバは、1 つまたは複数の認証サーバによる認証決定をもとにシステムの単一の結果を判定します。NAD でポリシーを適用するために、AAA サーバは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します。
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 (アカウントリング) 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
APT	Application Posture Token (アプリケーション ポスチャ トークン)。ベンダーのアプリケーションの適合性チェックの結果で、そのコンポーネントの健全性を示します。ポスチャ検証のすべての APT がプライマリ PVS によって統合され、System Posture Token (SPT; システム ポスチャ トークン) が作成されます。
APT、Application Posture Token (アプリケーション ポスチャ トークン)	ベンダー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 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。

用語	定義
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 リストとプロファイル、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)
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、単一のエージェント パッケージへの監査ログなどを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、エンドポイントにまで保護機能を拡張して、ネットワーク アドミッション コントロールと SAFE プルプリントを強化します。
CSM	Cisco Security Manager
CS-MARS	Cisco Systems Mitigation 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ライアンス 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。
CTA	Cisco Trust Agent。シスコの PA の製品インスタンスです。PA ポスチャ プラグインが含まれます。
CTA, Cisco Trust Agent	CTA はシスコのポスチャ エージェント実装で、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
DAI	Dynamic ARP Inspection
DHCP Snooping (DHCP スヌーピング)	<ul style="list-style-type: none"> <li>DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリング、および DHCP スヌーピング バインディング データベース (または DHCP スヌーピング バインディング テーブル) の構築および維持により、ネットワーク セキュリティを提供するセキュリティ機能です。</li> <li>DHCP スヌーピングは、信頼できないホストと DHCP サーバ間でファイアウォールのような機能を果たします。DHCP スヌーピングを使用して、エンドユーザに接続する信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続する信頼できるインターフェイスとを区別することができます。</li> <li>DHCP スヌーピングにより、クライアント IP アドレス、MAC アドレス、ポート、VLAN 番号、リースおよびバディン グタイプを格納する DHCP バインディング テーブルが作成されます。この機能は、スイッチ上の特定の VLAN 上で有効化できます。スイッチは、レイヤ 2 VLAN ドメイン内ですべての DHCP メッセージ ブリッジングを代行受信します。</li> </ul>
EAP	Extensible Authentication Protocol
EAP-FAST	<ul style="list-style-type: none"> <li>Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) は、TLS ベースの RFC 3748 に準拠する EAP 方式です。</li> <li>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。</li> </ul>
EAP-FAST	EAP Flexible Authentication by Secure Tunneling
EAP-GTC	EAP Generic Token Card
EAPOL	EAP over LAN
EAP-TLS	EAP Transport Layer Security

用語	定義
Endpoint (エンドポイント)	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
EoU、EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol.
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication ( Microsoft )
HCAP	Host Credential Authorization Protocol
Host (ホスト)	エンドポイント デバイスの別名
Host (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。
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。
MAB	MAC Authentication Bypass ( MAC-Auth-Bypass )
Machine Authentication (マシン認証)	マシン認証は、アイデンティティとして、Active Directory に登録されている実際のコンピュータ名を使用して行われます。クレデンシャルは、使用される EAP のタイプに応じて、パスワードベースまたは PKI 証明書ベースのクレデンシャルを使用できます。
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2
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、ウイルスやワームがもたらす損害を抑制します。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 L2 802.1x	シスコの CatOS および IOS スイッチで 802.1x プロトコルを使用するシスコの NAC 実装です。
NAC L2 IP	シスコ スイッチがレイヤ 2 で EAPoUDP を介して行う NAC
NAC L3 IP	シスコ ルータが レイヤ 3 で EAP over UDP を介して行う NAC
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、エンドポイント デバイス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。NAD として、シスコ ルータ、スイッチ、アクセス ポイント、VPN コンセントレータなどを使用できます。
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 ) ) の組み合わせで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 )
NAH、NAC Agentless Host (NAC エージェントレス ホスト)	802.1x サブリカントまたは CTA がインストールされていないためポスチャ検証を実施できないホスト
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
NRH	Nonresponsive Host ( 非応答ホスト )

用語	定義
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と通信する、エンドポイン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。シスコのポスチャ エージェントは、Cisco Trust Agent (CTA) です。
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するアプリケーション。
PAC	Protected Access Credential
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機能を提供します。
PEAP	Protected EAP
PEAP-GTC	Protected EAP Generic Token Card
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。
Plugin (プラグイン)、Posture Plugin (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 (ポスチャ)	現在のホストのステータスと設定。アンチウイルスのレベル、ホットフィックス、OS タイプなどが含まれます。
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と通信するエンドポイン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。シスコのポスチャ エージェントは、Cisco Trust Agent (CTA) です。
Posture Credentials (ポスチャ クレデンシャル)	エンドポイント デバイス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) 情報を示すステート情報
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) 情報を示すステート情報
Posture Plugin (ポスチャ プラグイン)	エンドポイントのポスチャ 検証およびネットワーク認証のために同一のエンドポイント上のポスチャ 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 検証サーバとその適合ポリシーを使用して行う、エンドポイント デバイスのポスチャ クレデンシャルの認証
Posture Validation (ポスチャ 検証)	1 つまたは複数のポスチャ 検証サーバとその適合ポリシーを使用した、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
Posture Validation Server (ポスチャ 検証サーバ)	ポスチャ 検証サーバは、NAC において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 クレデンシャルを認証します。
PP	Posture Plugin (ポスチャ プラグイン)
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。
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 (ベンダー 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 検証サーバは、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 ルールとポスチャ クレデンシャルを検証します。

用語	定義
PVS、Posture Validation Server (ポスチャ検証サーバ)、Policy Server (ポリシーサーバ)、Vendor Policy Server (ベンダーポリシーサーバ)、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。ポスチャ検証サーバは、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エンドポイント デバイスの単一のポスチャ検証結果です。エンドポイントのポスチャ検証から得られた最終的なポスチャ ステートとなります。
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: 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 に修復するために使用されます。
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: 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: 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: 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: 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、認証、または修復を行います。
User Authentication (ユーザ認証)	ログイン時に 802.1x を使用してユーザ情報を確認する手法。ユーザ認証は、ユーザの Active Directory (ドメイン) のクレデンシャル、またはクライアント側の証明書で提供されるクレデンシャルを通じて実行できます。
VSA、Vendor Specific Attribute	大半のベンダーが VSA を使用して付加価値機能をサポートします。

©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>