

日立電線スイッチングハブ

Apresia3400/4300/5400/13000 シリーズ

AEOS Ver. 7 アプリケーションノート

(AccessDefender 編)

制定・改訂来歴表

No.	年 月 日	内 容
-	2008年6月10日	新規作成
A	2009年1月9日	AccessDefender phase2 機能対応 <ul style="list-style-type: none"> ・ローミング ・linkdown ログアウト無効 ・802.1X ・DHCP スヌーピング ・強制認証 DVLAN
B	2009年11月30日	<ul style="list-style-type: none"> ・Apresia3448GT、Apresia3448G-PSR、Apresia5412 シリーズを追加 ・2.6.1 DHCP スヌーピングの動作モードを修正 ・2.7 認証機能と仕様を修正 ・7.6.1.2 認証ページリダイレクト機能設定例を修正 ・7.6.2.2 認証ページリダイレクト機能設定例を修正 ・9.2.1 秘密鍵および CSR の生成を修正 ・10. AccessDefender 機能に関するリリース情報を修正
C	2010年7月30日	<ul style="list-style-type: none"> ・Apresia3424GT-HiPoE、Apresia5428GT を追加 ・表 2-2 AccessDefender 機能と仕様を修正 ・表 2-4 動作可否確認済みブラウザ(認証ページリダイレクト使用時)を修正 ・図 2-5 Web 認証と MAC 認証を併用する場合の認証フローの注釈を修正 ・2.4 Web 認証と MAC 認証の混在ポートでの認証フローを修正 ・2.5 Web/MAC 認証(Web 認証時の MAC 認証先行)を追加 ・2.6.3 動作確認済サブリカント一覧項を追加 ・2.7 802.1X/MAC 認証(802.1X 認証時の MAC 認証先行)を追加 ・2.9.1 認証端末数とフィルタリソースの関係についてを修正 ・2.9.2 最大接続端末数について(DHCP スヌーピング)を修正 ・3.2.6 ローカルデータベースの編集(追加)を追加 ・3.2.7 ローカルデータベースの編集(削除)を追加 ・3.3 認証順序変更(Web 認証、MAC 認証のみ)を追加 ・3.4 移行条件変更機能(Web 認証、MAC 認証のみ)を追加 ・3.5 認証方法選択機能(Web 認証のみ)を追加 ・3.6 認証拒否機能を追加 ・3.7 DHCP パケットの MAC 認証除外を追加 ・3.8 認証開始時の EAP-Request/Identity の抑制を追加 ・3.9 認証失敗時のステータス保持時間の変更を追加 ・3.10 TTL フィルターを追加 ・3.11 PING ログアウトを追加 ・5.3 Windows 標準サブリカントにおける 802.1X 認証の問題点を追加 ・6.4 Web/MAC 認証構成例を追加 ・6.8 802.1X/MAC 認証構成例を追加 ・7.1.3 認証方法選択機能の認証ページカスタマイズを追加 ・8.1 認証ログ表示例(syslog)を修正

D	2010年11月25日	<ul style="list-style-type: none"> ・表 5-1 制限事項および注意事項を修正 ・表 10-1 AEOS Ver. 7での機能追加・変更点(AccessDefender 関連機能)を修正 ・5.4 VRRP 併用時の注意点を追加
E	2011年10月27日	<ul style="list-style-type: none"> ・表 2-5 動作可否確認済みブラウザ(認証ページリダイレクト使用時)を修正 ・表 2-6 ログアウト処理についてを修正 ・表 3-1 AccessDefender 設定項目を修正 ・表 5-1 制限事項および注意事項を修正 ・表 8-3 AccessDefender 設定時のコンフリクトメッセージ一覧を修正 ・2.1.2 Web 認証の認証フロー(VLAN 変更での運用の場合)の記載内容を修正 ・2.1.2 Web 認証の認証フロー(VLAN 変更での運用の場合)の注意事項を修正 ・2.5 Web/MAC 認証(Web 認証時の MAC 認証先行)の記載内容を修正 ・2.8.2 DHCP スヌーピングの動作フローから注意事項を削除 ・6.1 Web 認証構成例を修正 ・6.3 Web 認証、MAC 認証の混在環境構成例を修正 ・6.9 DHCP スヌーピング構成例を修正 ・6.10 DHCP スヌーピング/MAC 認証(固定/動的 VLAN)の混在環境構成例を修正 ・6.11 DHCP スヌーピング/Web 認証(固定 VLAN)の混在環境構成例を修正 ・6.12 DHCP スヌーピング/Web 認証(動的 VLAN)の混在環境構成例を修正 ・7.6.1.1 認証フローの注意事項を修正 ・7.6.2.1 認証フローの注意事項を修正 ・7.6.3.2 HTTPS を用いる際の注意点の設定例を修正 ・9.2.1 秘密鍵および CSR の生成に注意事項を追加

はじめに

本書は、日立電線製 BOX 型スイッチングハブ APRESIA シリーズのファームウェア AEOS Ver. 7 の機能概要および構成・設定例を記述しています。それ以外のハードウェアに関する説明および操作方法については、ハードウェアマニュアルおよびインストールガイドを参照下さい。また各種コマンドに関する説明は、最新のコマンドリファレンスを参照して下さい。

適用機種一覧表

シリーズ名称		製品名称	AEOS バージョン
Apresia3400 シリーズ	Apresia3424 シリーズ	Apresia3424GT-SS	Ver. 7. 27. 01
		Apresia3424GT-PoE	
		Apresia3424GT-HiPoE	
	Apresia3448 シリーズ	Apresia3448GT	
		Apresia3448G-PSR	
Apresia4300 シリーズ	Apresia4328 シリーズ	Apresia4328GT	
		Apresia4348GT	
	Apresia4348 シリーズ	Apresia4348GT-PSR	
Apresia5400 シリーズ		Apresia5412GT-PoE	
		Apresia5428GT	
Apresia13000 シリーズ		Apresia13000-48X	
		Apresia13000-24GX-PSR	



この注意シンボルは、そこに記述されている事項が人身の安全と直接関係しない注意書きに関するものであることを示し、注目させる為に用います。

Apresia は、日立電線(株)の登録商標です。

AEOS は、日立電線(株)の登録商標です。

AccessDefender は、日立電線(株)の登録商標です。

MMRP は、日立電線(株)の登録商標です。

Ethernet は、富士ゼロックス(株)の登録商標です。

Microsoft は、米国およびその他の国における米国 Microsoft Corp. の登録商標です。

Windows は、米国およびその他の国における米国 Microsoft Corp. の登録商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。

その他、記載の会社名および製品名は、それぞれの会社の商標もしくは登録商標です。

使用条件と免責事項

ユーザーは、本製品を使用することにより、本ハードウェア内部で動作するルーティングソフトウェアを含む全てのソフトウェア(以下、本ソフトウェアといいます)に関して、以下の諸条件に同意したものといたします。

本ソフトウェアの使用に起因する、または本ソフトウェアの使用不能によって生じたいかなる直接的または間接的な損失・損害等(人の生命・身体に対する被害、事業の中断、事業情報の損失またはその他の金銭的損害を含み、これに限定されない)については、その責を負わないものとします。

本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブルすることはできません。

本ソフトウェアを本ハードウェアから分離すること、または本ハードウェアに組み込まれた状態以外で本ソフトウェアを使用すること、または本ハードウェアでの使用を目的とせず本ソフトウェアを移動することはできません。

目次

制定・改訂来歴表	1
1. 概要	8
1.1 AccessDefender概要	8
1.2 AccessDefenderがサポートする認証方式	9
1.3 ユーザー認証	10
1.4 IEEE802.1X	11
1.4.1 802.1Xで使用される認証方式	13
1.4.2 EAPのパケットフォーマット	14
1.5 DHCPスヌーピング概要	15
2. AccessDefenderの仕組み	16
2.1 Web認証(Webブラウザによるユーザー認証)	16
2.1.1 Web認証の認証フロー(VLAN固定で運用する場合)	16
2.1.2 Web認証の認証フロー(VLAN変更での運用の場合)	17
2.2 ゲートウェイ認証	19
2.3 MAC認証(MACアドレスによる端末認証)	20
2.4 Web認証とMAC認証の混在ポートでの認証フロー	21
2.5 Web/MAC認証(Web認証時のMAC認証先行)	22
2.6 802.1X認証	24
2.6.1 802.1X認証の認証フロー	24
2.6.2 Unicast-EAP機能	25
2.6.3 動作確認済サブリカント一覧	26
2.7 802.1X/MAC認証(802.1X認証時のMAC認証先行)	27
2.8 DHCPスヌーピング	29
2.8.1 DHCPスヌーピングの動作モード	29
2.8.2 DHCPスヌーピングの動作フロー	30
2.9 認証機能と仕様	32
2.9.1 認証端末数とフィルタリソースの関係について	34
2.9.2 最大接続端末数について(DHCPスヌーピング)	35
2.10 Webサーバー応答及び仮想IPの仕組み	36
2.10.1 Webサーバーの仮想IPの仕組み	36
2.10.2 認証ページリダイレクトを使用する際の注意点	38
2.11 ブラウザーの依存性について	39
2.12 ログアウト処理について	40
2.13 入力可能な文字について(ユーザーID/パスワード共通)	41
3. AccessDefender機能の設定	42
3.1 APRESIAの設定項目	42
3.2 ローカルデータベース認証と強制認証	44
3.2.1 ローカルデータベースによる認証(Web/MAC認証のみ)	46
3.2.2 ローカル認証DBフォーマット	46
3.2.3 ローカルデータベースの登録(ダウンロード)	47
3.2.4 ローカルデータベースのバックアップ(アップロード)	48
3.2.5 ローカルデータベースの削除	48
3.2.6 ローカルデータベースの編集(追加)	48
3.2.7 ローカルデータベースの編集(削除)	49
3.2.8 強制認証機能	50
3.2.9 強制認証機能(802.1X)	51
3.3 認証順序変更(Web認証、MAC認証のみ)	52
3.4 移行条件変更機能(Web認証、MAC認証のみ)	53
3.5 認証方法選択機能(Web認証のみ)	54
3.6 認証拒否機能	55

3.7 DHCPパケットのMAC認証除外	56
3.8 認証開始時のEAP-Request/Identityの抑制	57
3.9 認証失敗時のステータス保持時間の変更	58
3.10 TTLフィルター	59
3.11 PINGログアウト	61
4. 認証サーバー (RADIUSサーバー) の設定項目	63
4.1 認証サーバーの設定項目 (Web/MAC認証)	64
4.1.1 RADIUSクライアントの登録 (clients.confファイルなど)	64
4.1.2 ユーザー情報の登録 (usersファイルなど)	64
4.1.3 拡張設定 (VLAN IDの設定)	65
4.2 認証サーバーの設定項目 (802.1X)	66
4.2.1 EAPの設定 (eap.confファイルなど)	66
4.2.2 RADIUSクライアントの登録 (clientsファイルなど)	67
4.2.3 ユーザー情報の登録 (usersファイルなど)	67
4.2.4 拡張設定 (VLAN IDの設定)	67
4.3 RADIUSサーバーの冗長化	68
4.4 AccessDefenderで使用するRADIUS属性	69
4.5 RADIUSサーバー設定例 (Windows 2000 server "IAS") (Web/MAC認証)	70
4.5.1 RADIUSクライアントの設定	71
4.5.2 ユーザー・グループ情報の設定 (リモートアクセスポリシーの設定)	72
4.5.3 VSAの設定 (動的VLAN変更時のみ必要)	76
5. 制限事項および注意事項	79
5.1 バージョンアップ時の注意点	87
5.2 動的VLAN割り当て使用時の注意点	87
5.2.1 動的VLAN割り当て時のログイン失敗	87
5.2.2 単一のアクセスポート配下に複数端末を接続する際の注意点	88
5.3 Windows標準サブリカントにおける 802.1X認証の問題点	89
5.3.1 ActiveDirectoryのグループポリシーを使用した回避	90
5.3.2 Windowsクライアントに修正プログラムを適用する方法での改善	103
5.3.3 EAPOL Start受信による認証の抑止を用いた回避方法	106
5.4 VRRP併用時の注意点	107
6. 構成例	109
6.1 Web認証構成例	109
6.2 MAC認証構成例	112
6.3 Web認証、MAC認証の混在環境構成例	114
6.4 Web/MAC認証構成例	117
6.5 ゲートウェイ認証構成例 (サーバーファーム手前に適用)	119
6.6 ゲートウェイ認証構成例 (中央拠点アクセス手前に適用)	122
6.7 802.1X認証構成例	125
6.8 802.1X/MAC認証構成例	127
6.9 DHCPスヌーピング構成例	129
6.10 DHCPスヌーピング/MAC認証 (固定/動的VLAN) の混在環境構成例	131
6.11 DHCPスヌーピング/Web認証 (固定VLAN) の混在環境構成例	133
6.12 DHCPスヌーピング/Web 認証 (動的VLAN) の混在環境構成例	135
7. 応用設定	138
7.1 認証ページのカスタマイズ	138
7.1.1 APRESIA内部ページのカスタマイズ	138
7.1.2 外部Webサーバー上の任意のページへの埋め込み	139
7.1.3 認証方法選択機能の認証ページカスタマイズ	140
7.2 ユーザー認証時の持ち込み端末制限	141
7.3 NAS (Network Access Server) 属性	142
7.3.1 NAS-IP-address	142
7.3.2 NAS-identifier	143

7.3.3 NAS属性の組み合わせ	144
7.4 MACアドレスの自動収集	145
7.5 未認証端末の packets 強制転送(認証バイパス)	147
7.5.1 認証バイパスの概要	147
7.5.2 認証バイパスによる強制転送設定例(1)	149
7.5.3 認証バイパスによる強制転送設定例(2)	150
7.5.4 Windowsドメイン環境への適用	151
7.6 認証ページのリダイレクト機能	152
7.6.1 HTTPプロキシが無い環境(直接Internetへ接続)の場合	153
7.6.2 HTTPプロキシサーバーが存在する環境の場合	156
7.6.3 SSLとWebループ検知の併用	159
7.7 正規固定IPアドレス端末の接続(DHCPスヌーピング)	162
7.7.1 static-entry設定による方法	162
7.7.2 認証バイパス設定による方法	162
8. AccessDefender関連ログ	163
8.1 認証ログ表示例(syslog)	163
8.2 設定時のコンフリクトメッセージ一覧	166
9. SSL設定について	167
9.1 SSL設定概要	168
9.2 証明書要求を装置で発行する場合	169
9.2.1 秘密鍵およびCSRの生成	169
9.2.2 CSRのアップロード	172
9.2.3 証明書の発行	172
9.2.4 証明書のダウンロード	172
9.3 証明書要求を装置で発行しない場合	173
9.3.1 秘密鍵およびCSRの生成	173
9.3.2 証明書の発行	177
9.3.3 証明書および秘密鍵のダウンロード	178
9.3.4 信頼されたルート証明機関として登録	179
9.4 認証URLへアクセス	182
9.5 証明書の削除(初期化)	182
9.6 中間CA証明書対応について	183
9.6.1 中間CA証明書とは	183
9.6.2 証明書要求を装置で発行する場合	184
9.6.3 証明書要求を装置で発行しない場合	185
9.6.4 認証URLへアクセス(証明書の確認)	194
10. AccessDefender機能に関するリリース情報	195

1. 概要

1.1 AccessDefender概要

Internet が活用されるにしたがい、増え続ける脅威に対応するため、様々な機器が開発・導入されています。しかし、機能毎の機器にかかるコスト増加や、使いこなしを含めた運用面が問題になってきており、外部セキュリティにおいては、機能統合で機能性、運用性を向上しつつコストを低減した UTM(Unified Threat Management)が主流になってきています。

これに対し内部セキュリティにおいては、相次ぐ情報漏洩といった問題がクローズアップされ、認証スイッチングハブ(以下認証スイッチまたは装置と略します)などの導入が進みつつありますが、外部セキュリティに比べ対策が遅れているのが現実です。更なる脅威に対応する準備として、単なる認証ではなく、内部セキュリティに特化した新たな対策が必要となっています。

内部セキュリティに必要なセキュリティ要件としては、

- ネットワーク認証の高度化
- 正規ユーザーの不正利用排除
- 柔軟な個別通信制御

など、攻撃を受ける場所が一定ではなく、柔軟な制御が可能なセキュリティ機能が求められます。

また、内部セキュリティに求められるその他の要件としては、

- 多くの台数を管理できる運用性
- スイッチングハブと同程度のスループット
- 十分な低コスト

など、いわゆる LAN に適用するために必要となる、コスト/物理的な要件などが挙げられます。

これらの要件に対し、日立電線(株)は統合による機能強化、運用性向上を実現する UTM の思想を適用することで、内部セキュリティに必要な機能を統合し、コストや運用性を犠牲にせず高いセキュリティを実現する、新たな次世代内部セキュリティとして、「iUTM(Internal UTM)構想」を提唱しています。

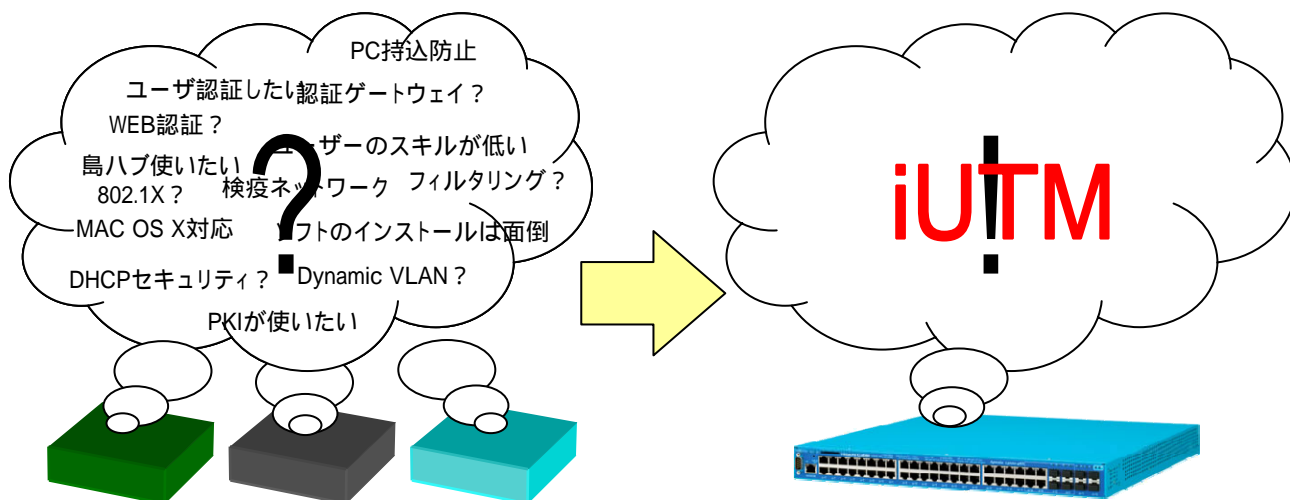


図 1-1 AccessDefender による iUTM 構想の実現

AccessDefender とは、この iUTM 構想を実現するために、ネットワーク認証を中心に、様々なセキュリティ機能を融合し、強固なセキュリティと柔軟性に富んだネットワークを実現する、ライセンス不要の統合セキュリティソリューションです。

APRESIA に実装された AccessDefender 機能は、認証サーバーを使用し、接続されたユーザーや端末を認証後、LAN に接続許可します。それにより、不正なユーザーもしくは端末が APRESIA のポートを通じて LAN に接続することを制限します。

ユーザーや端末が認証されるまでは、APRESIA の認証バイパス設定によって許可されたトラフィック以外のトラフィックを破棄します。認証成功後、通常のトラフィックが中継されます。

! AccessDefender の設定にはいくつかの制限事項や注意事項があります。内容については、各章及び 5 制限事項および注意事項 を参照して下さい。

1.2 AccessDefender がサポートする認証方式

下表に AccessDefender がサポートする認証方式を記します。4 つの認証方式をシームレスにサポートし、それぞれの環境に合わせた最適なセキュリティを実現します。

表 1-1 AccessDefender がサポートする認証方式

項目	レイヤ 2 制御 (MAC アドレスベース)			レイヤ 3 制御 (IP アドレスベース)
	IEEE802.1X	Web 認証	MAC 認証	ゲートウェイ認証
認証要素	ユーザー認証 端末認証	ユーザー認証	端末認証	ユーザー認証
PKI 利用	○	×	×	×
認証サーバー	RADIUS (EAP 対応)	RADIUS	RADIUS	RADIUS
認証用クライアントソフト	IEEE802.1X 対応 サブリカント	汎用 Web ブラウザー	なし	汎用 Web ブラウザー
適用クライアント OS	サブリカント 利用可能 OS	汎用 Web ブラウザー 利用可能 OS	制限無し	汎用 Web ブラウザー 利用可能 OS
Dynamic VLAN	○	○	○	×
島ハブ/無線 AP カスケード	△ (EAP 透過可能 機器のみ)	○	○	○
ルータ/L3 スイッチ/WAN 経由の認証	×	×	×	○

1.3 ユーザー認証

ユーザー名・パスワードを使用し、正規のユーザーだけにアクセスを許可するユーザー認証方式は、既存の認証基盤を使用できることや、ワンタイムパスワードなど、より強固なセキュリティを実現できることから、よく使用されるセキュリティ手段です。

ユーザー認証方式による不正ユーザーのブロックについての一般的な概念を説明します。

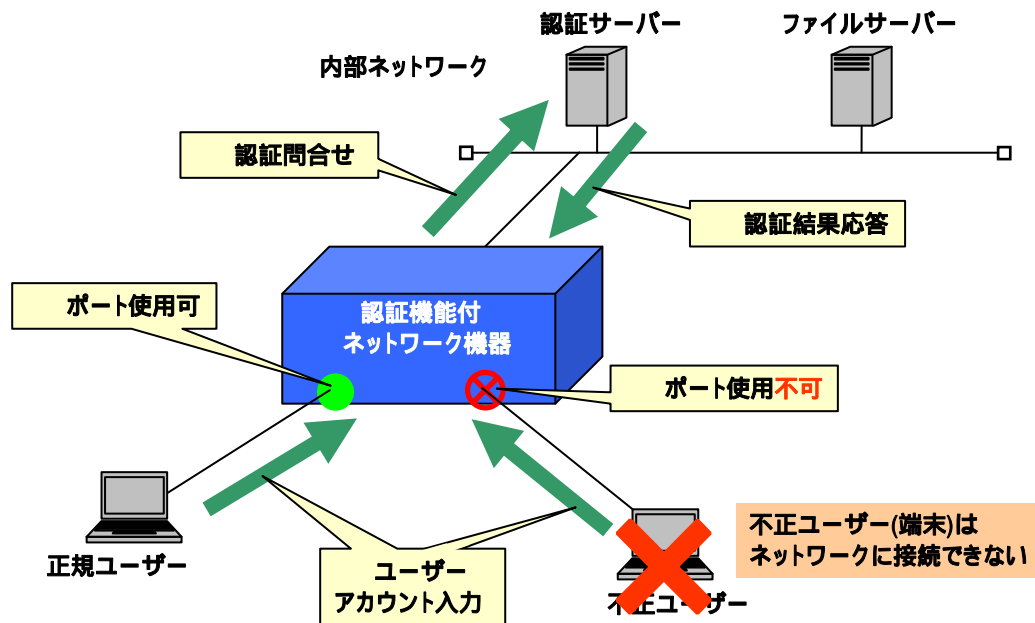


図 1-2 ユーザー認証方式による不正ユーザーのブロック

- ①. 内部ネットワークに接続する時に、ユーザーアカウントを入力します。
- ②. 入力されたアカウント情報をもとに認証サーバーに問合せします。
- ③. 正規ユーザーであるかが認証サーバーにより認証され、結果が返されます。
- ④. 正規ユーザーが接続しているポートは使用可能となり、不正ユーザーが接続しているポートは使用不可状態となります。

このように、認証サーバーに登録されていないユーザーや端末は物理的にネットワークへの接続が不可能になります。

1.4 IEEE802.1X

IEEE802.1X(以下 802.1X と略します)とは、IEEE802.1(Bridging & Management)シリーズの規格の一つで、電子証明書や ID/パスワードを使用してクライアントと認証サーバー間で認証を行い、認証されていないクライアントからの通信を(認証要求を除いて)すべて遮断し、許可されたユーザー(クライアント)のみに対してポートを開放するように規定されています。

認証には、802.1X 対応認証サーバー(Authentication Server)と、802.1X に対応したユーザー端末ソフトウェア(サブリカント)が必要となります。

認証の際に使用されるプロトコルは、EAP(PPP Extensible Authentication Protocol)と呼ばれ、Authenticator を介してサブリカントと Authentication Server の間で認証情報がやり取りされます。

図 1-3 に 802.1X動作システムの基本構成を示します。ユーザー認証時、オーセンティケーターはサブリカントと認証サーバー間の認証情報の橋渡しをし、サブリカントが認証されるまでは、EAPメッセージだけを許可します。認証成功すると、その他の通常トラフィックを許可します。サブリカントと認証サーバーは、オーセンティケーターを介してどのEAPタイプで認証するかをネゴシエートします。

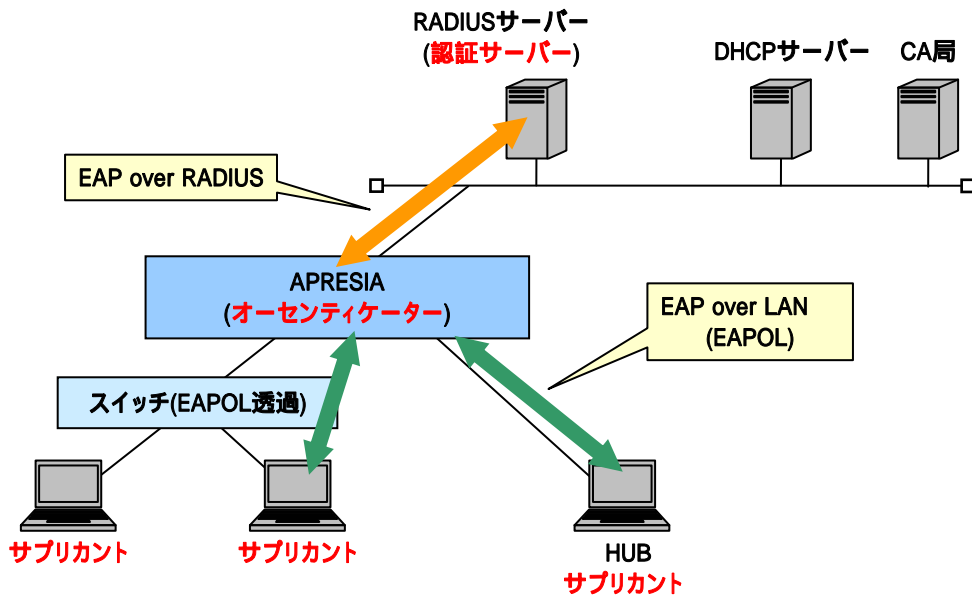


図 1-3 802.1X 動作システム概要

- サブリカント： PC などの端末
- オーセンティケーター： スイッチや無線アクセスポイントなど、アクセス制御する機器
- 認証サーバー： 端末を認証するサーバー (RADIUS サーバー)

基本的に 802.1X 機能では、スイッチの 1 つのポートに 1 つの端末を接続し、ポート単位で許可・遮断をコントロールします。

■メリット

- 業界標準として、様々な機器に実装されている。
- Windows2000(SP4)以上の OS では標準サポートされている。
- PKI(電子証明書)を利用した強固な認証が可能。

■デメリット

- 島ハブが利用できない、または利用しにくい(通常 1 ポート 1 端末を実現する必要がある)
- プリンタや IP 電話などのサイレント(自発的に認証対象となるフレームを送信しない)機器の認証に対応困難
- サプリカントを標準搭載しない OS があり、サプリカントが別途必要な場合がある。
- 証明書の管理・運用が面倒

802.1X 認証で使用する EAP メッセージは、特殊なマルチキャストアドレスを使用する MAC フレームでやり取りされます。この特殊なマルチキャストアドレスの MAC フレームは、一般的なスイッチでは破棄されるため、802.1X 機能が有効となっているポート配下にデスクトップスイッチなどを接続して複数の端末を接続する場合には、EAP メッセージを中継するスイッチを接続する必要があります。

APRESIA の 802.1X 認証機能では、1 ポートで複数端末の認証を行う「Multiple-Authentication」機能をサポートしています。本機能を使用することにより、端末と APRESIA の間にハブや L2 スイッチを接続し、複数の端末を収容、かつ個別に各端末を認証することが可能となります(EAPOL メッセージを中継する機器を接続する必要があります)。1 ポート 1 端末に制限する場合は、port max-client コマンドを使用して制限をかけてください。

AccessDefender の 802.1X は RADIUS サーバーに Tunnel-Private-Group-Id 属性を設定することにより、サプリカントの認証後、サプリカントの MAC アドレス毎に VLAN を動的に変更することが可能です。

1.4.1 802.1Xで使用される認証方式

802.1X では EAP(PPP Extensible Authentication Protocol : PPP を拡張したプロトコル)メッセージを使用します。APRESIA がサポートする EAP 認証方式は、EAP-MD5(Message Digest 5)、PEAP(Protected EAP)、EAP-TLS(Transport Level Security)、EAP-TTLS(Tunneled TLS)です。以下に特徴を示します。

表 1-2 EAP 認証機能の比較

	電子証明書		クライアント/サーバー間の双方向認証	特徴
	サーバー	クライアント		
EAP-MD5	不要	不要	ID/パスワードのみで、サーバーの認証は行わない	<ul style="list-style-type: none"> ➤ ユーザー識別にユーザーID/パスワードを使用 ➤ サーバー認証機能がないため、セキュリティレベルは他の方式より低い ➤ 導入・運用管理が容易(NA と同レベル)
PEAP	要	不要	サーバーの電子証明書と ID/パスワード	<ul style="list-style-type: none"> ➤ ユーザー識別にユーザーID/パスワードもしくは電子証明書、サーバー認証に電子証明書を使用 ➤ 経路が TLS トンネルで暗号化される(トンネル内でさらに EAP を利用) ➤ 比較的管理面で負担が少なく、かつ強固な認証が可能 ➤ サポートクライアントが限定される(基本的に Windows 系 OS)
EAP-TTLS	要	不要	サーバーの電子証明書と ID/パスワード	<ul style="list-style-type: none"> ➤ ユーザー識別にユーザーID/パスワード、サーバー認証に電子証明書を使用 ➤ 経路が TLS トンネルで暗号化される(トンネル内で、様々な認証プロトコルを使用可能) ➤ 比較的管理面で負担が少なく、かつセキュアな認証が可能 ➤ OS 標準搭載ではないため、別途サブリカントが必要
EAP-TLS	要	要	電子証明書	<ul style="list-style-type: none"> ➤ ユーザー識別やサーバー認証に電子証明書を使用 ➤ 双方向で電子証明書を使用するため最もセキュリティが高い ➤ 電子証明書の導入や運用管理の負荷が高い

1.4.2 EAPのパケットフォーマット

サブリカントと Authenticator 間では、EAP パケットは MAC フレームのデータ部に格納されており、これを EAPOL フレームと呼びます。

Authenticator と RADIUS サーバー間では、RADIUS パケットの中に EAP パケットが格納されています。Authenticator が EAP パケットを中継し、サブリカントと RADIUS サーバー間で EAP パケットをやり取りします。

EAP パケットには各種認証情報が埋め込まれており、その先頭部分の Code 部にリクエスト(Request)、レスポンス(Response)、認証成功(Success)、認証失敗(Failure)の情報が入ります。

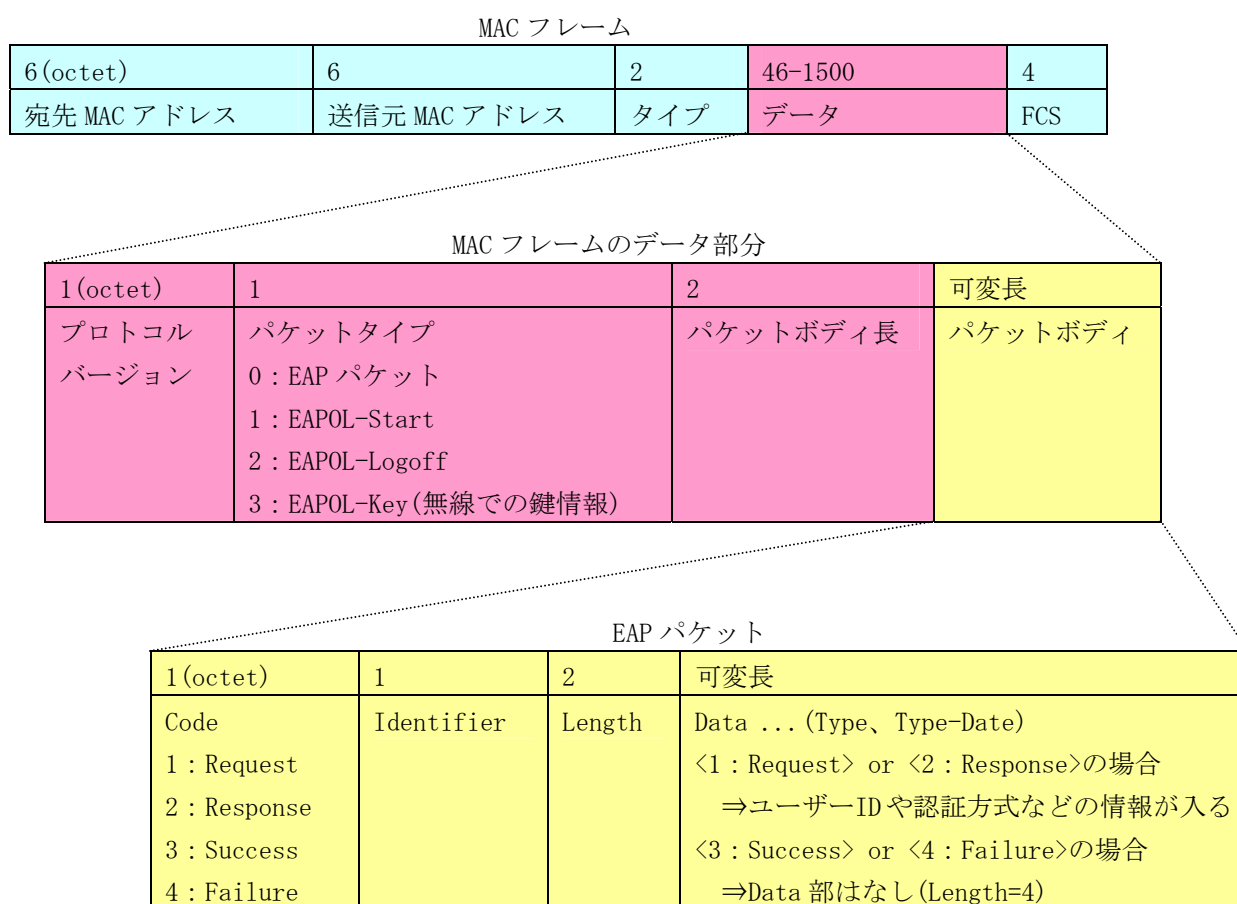


図 1-4 EAPOL のフレームフォーマット

1.5 DHCPスヌーピング概要

DHCP スヌーピング機能は、DHCP サーバーと DHCP クライアントでやり取りされる DHCP パケットを APRESIA でスヌーピング(覗き見)し、端末に払い出された IP アドレス情報をもとに、DHCP クライアントが接続されたポートに対して、払い出された IP アドレスを送信元とする IP、ARP 通信のみを許可する機能です。

本機能により下記が実現可能となり、ネットワークのセキュリティを高めることが可能となります。

- 正規 DHCP サーバーよりアドレスを配布された端末のみネットワークへ接続可能
- 固定 IP アドレス端末の持ち込みによるネットワーク接続を禁止
- 不正に設置された DHCP サーバーによるアドレス配布を禁止
- ARP 詐称(ARP スプーフィング)を起点とした LAN 盗聴の防止

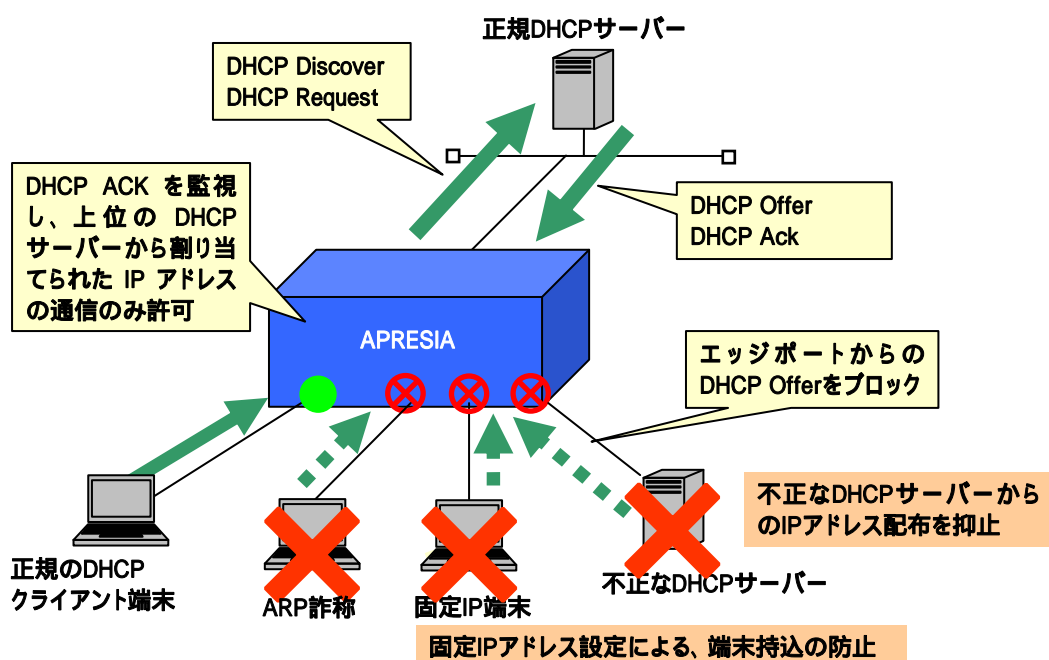


図 1-5 DHCP スヌーピング構成例

2. AccessDefenderの仕組み

2.1 Web認証(Webブラウザによるユーザー認証)


Web 認証は、Web ブラウザーを使用し、認証時にユーザー名/パスワードにより認証を行う機能です。RADIUS サーバー(ローカル認証使用時はローカルデータベース)にユーザー毎に VLAN 情報を追加した場合、認証時にユーザーの属性に従って動的に VLAN を割り当てることが可能です。また、1 ポートで複数端末の認証が可能であり、認証端末毎に VLAN を割り当てることが可能です。

また、パケットフィルタ-2 の認証バイパス機能を利用することにより、特定の端末のみ Web 認証を行わないで、通信を許可させることが可能です。

2.1.1 Web認証の認証フロー(VLAN固定で運用する場合)

認証成功後にユーザー毎にVLANを割り当てずに、APRESIAの認証ポートに設定されているVLANを固定で使用する場合の認証フローを図 2-1 に示します。

- ①-②. DHCP 端末で認証する場合、最初に端末は APRESIA を経由してネットワーク上位の正規 DHCP サーバーから正規 IP アドレスを入手します。
未認証端末の packets は認証ポートを経由した通信を制限されているため、未認証端末であっても DHCP packets を転送処理させる設定が必要です。
- ③-⑥. Web ブラウザーを起動し、認証用 URL を入力します。
APRESIA より認証画面が表示されます。ここでユーザー名とパスワードを入力します。入力された情報をもとに APRESIA は RADIUS サーバーに対してユーザー問合せを行います。
- ⑦-⑧. RADIUS サーバーは自身のデータベースを参照し、該当ユーザーが存在するときは認証成功を通知します。APRESIA は自身のポートに端末の情報を登録し、同時に認証成功したことを示す Web ページを表示します。
- ⑨. 端末はこの時点で通信が可能となります。

 認証成功後にVLANを切り替える・切り替えないの選択は、RADIUSサーバーへのVLAN情報登録有無に依存しています。VLAN情報登録については、4.1.3 拡張設定(VLAN IDの設定) を参照して下さい。

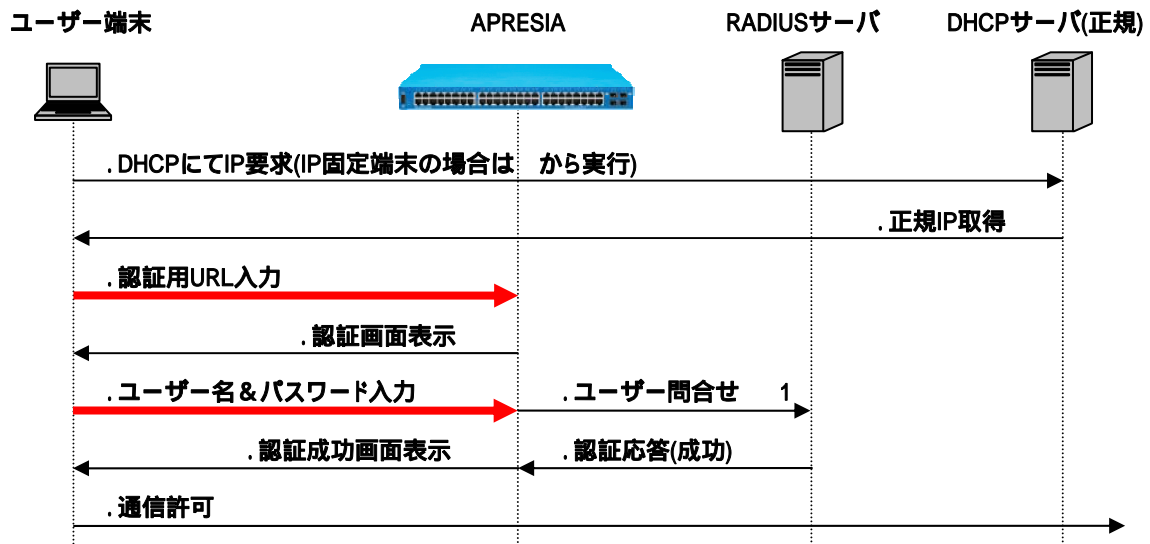


図 2-1 Web 認証フロー (VLAN 固定)

※1：ユーザー問い合わせの「Access-Request」は、次の属性をサポートしています。

- ・NAS-IP-Address : 認証要求している RADIUS クライアント (APRESIA) の IP アドレス
- ・NAS-Port : クライアントが接続されている物理ポート番号
- ・NAS-Identifier : 認証要求端末が属している VLAN ID (VID)
- ・Calling-Station-Id : 認証端末の MAC アドレス

2.1.2 Web認証の認証フロー (VLAN変更での運用の場合)

RADIUS サーバーのユーザー属性情報として VLAN 情報が登録されている場合、その属性にしたがって認証成功後にユーザー毎に VLAN を動的に変更して割り当てることができます。認証ポートに予め設定する VLAN を暫定 VLAN、認証後に RADIUS サーバーから通知される VID の VLAN を正規 VLAN と呼びます。

この場合の認証フローを図 2-2 に示します。

- ①-②. この時点では端末は暫定 VLAN に属します。最初に端末は APRESIA に設定した暫定 VLAN 用の DHCP サーバーから、リース期間の短い暫定 IP アドレスを入手します。
- ③-⑥. Web ブラウザーを起動し、認証用 URL を入力します。
APRESIA より認証画面が表示されます。ここでユーザー名とパスワードを入力します。この情報をもとに APRESIA は RADIUS サーバーに対してユーザー問い合わせを行います。

- ⑦-⑧. RADIUS サーバーは自身のデータベースを参照し、該当ユーザーが存在するときは認証成功を通達します。同時にそのユーザーに割り当てられている VLAN の VID を通知します。APRESIA は端末の情報と併せて、RADIUS サーバーから通知された VID を設定します。同時に認証成功したことを示す Web ページを表示します。端末はこの時点で通信が可能となりますが、実際にはまだ暫定 IP アドレスを保持したままとなっています。
- ⑨-⑪. ②で入手した IP アドレスのリース期間満了後、この暫定アドレスをリリースし、正規 IP アドレスを入手してから通信が可能となります。

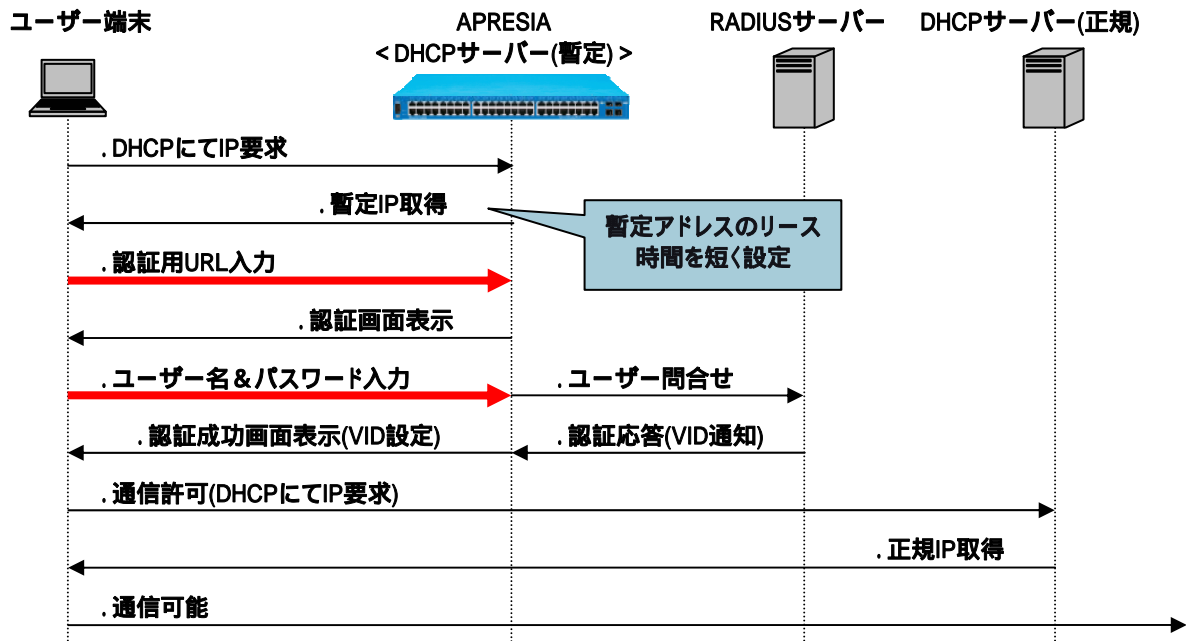


図 2-2 Web 認証フロー (VLAN 変更)

- ❗ 動的にプロトコル VLAN を割り当てることはできません。
- ❗ 認証後に端末に割り当てられる VLAN は「show vlan」コマンドでは確認できません。「show access-defender client」コマンドで確認して下さい。
- ❗ 本装置の DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります。

2.2 ゲートウェイ認証

クライアントと認証スイッチが別ネットワークに存在するようなケースでは、ゲートウェイ認証方式により、クライアントの認証環境の構成が可能です。用途としては図 2-3 のようなサーバーファームへの入口手前での認証や、WANを経由して本社へアクセスしてくる支社のユーザーの認証などがあります。

認証後の端末は IP アドレスによって管理されます。その他の項目（認証フローや認証画面など）に関しては通常の Web 認証と同様のため、エッジでの Web 認証と同一インターフェースでユーザーの利用環境を統一することができます。

■サーバーファームの手前で認証が可能

- 特定サーバーへのアクセスのみ、ネットワーク認証を適用可能
- 通常業務はエッジでの MAC 認証などとの組み合わせが可能

■複数拠点をまとめて1箇所で認証可能

- 多数の小規模拠点にスイッチを配置することなく、センタ拠点にアクセスするときのみ認証を適用し、導入コストを削減
- WAN 障害時でも、拠点内通信を継続することが可能

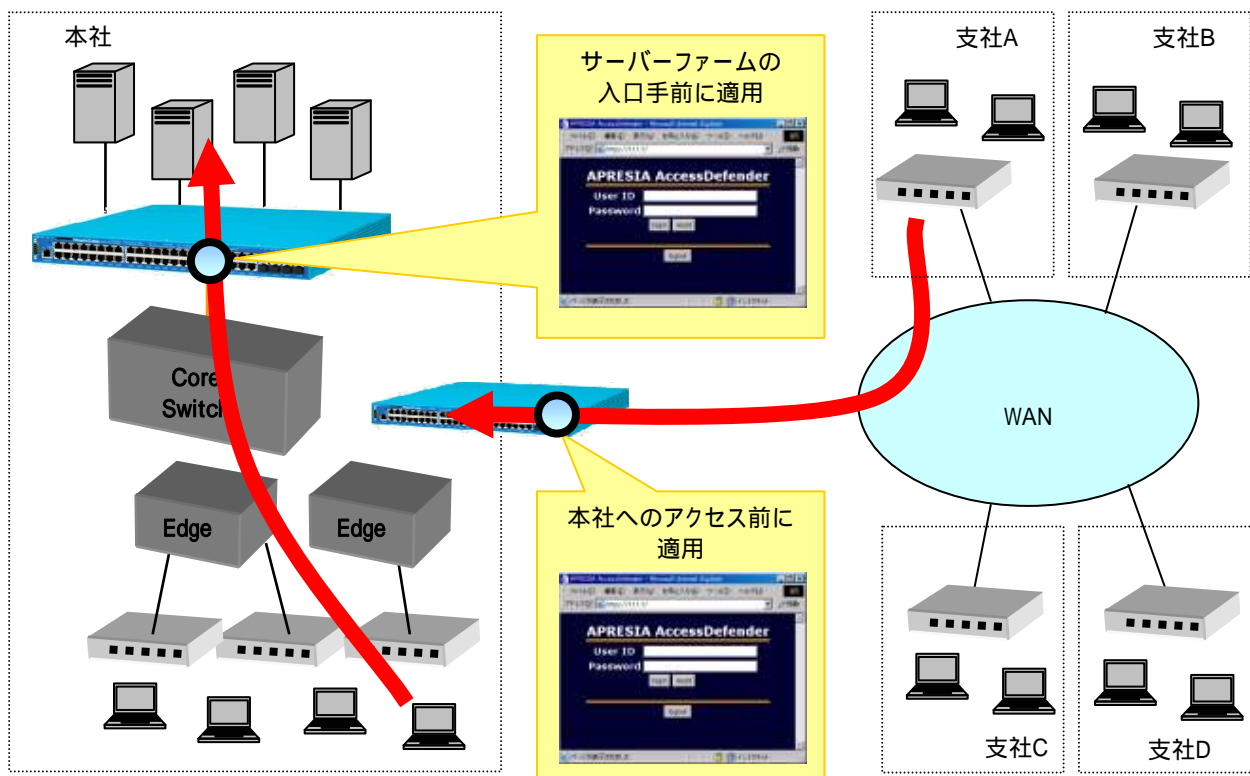


図 2-3 ゲートウェイ認証適用イメージ

- ❗ ゲートウェイ認証ではクライアントの情報として MAC アドレスではなく IP アドレスを使用するため、MAC 認証は適用できません。
- ❗ ゲートウェイ認証では動的に VLAN を変更することはできません。

2.3 MAC認証(MACアドレスによる端末認証)

端末の MAC アドレスにより、自動的に端末認証するモードです。MAC アドレスのみによる端末認証を設定できます。

MAC認証の認証フローを図 2-4 に示します。

端末から任意のフレームが送出されると、そのフレームの送信元 MAC アドレスをユーザー名とした端末認証が自動的に実行されます(①-④)。

固定 IP 端末の場合は認証成功後、そのまま通信が可能となります。

DHCP 端末の場合、認証成功後に DHCP サーバーから IP アドレスを入手した後、通信が可能となります。

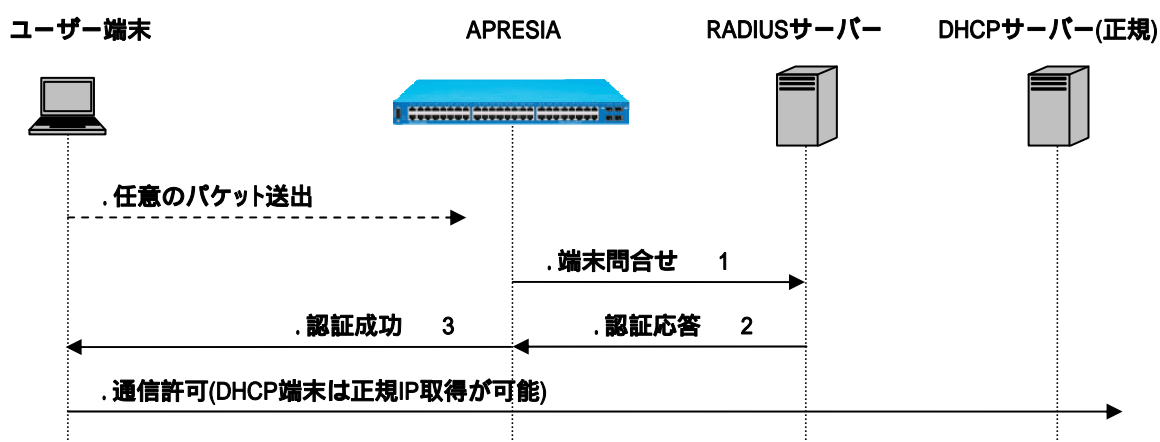


図 2-4 認証フロー(MAC ベース認証)

※1: Web 認証と同じ属性をサポートしています。

※2: RADIUS サーバーに VLAN 情報が登録されている場合、通知される VID の VLAN に動的に変更されます。

※3: 認証失敗した場合には、その端末のパケットは一定時間(300 秒)の間破棄されます(discard 登録)。

! discard 登録できる MAC アドレスの上限値は 100 個です。

2.4 Web認証とMAC認証の混在ポートでの認証フロー

AccessDefender では、Web によるユーザー認証と MAC アドレスによる端末認証を同一ポートで併用することが可能です。最初に MAC 認証が実行され、その後必要に応じて Web によるユーザー認証を実行します。どちらかで認証成功すれば通信が可能となります。

端末から任意のフレームが送出されると、そのフレームの送信元 MAC アドレスをユーザー名とした端末認証が自動的に実行されます(①-④)。④の認証結果が成功、すなわち MAC アドレスによる端末認証が成功した場合は、その時点で通信可能となり、DHCP 端末の場合は DHCP サーバーから IP アドレスを入手することができます(⑥)。

④の認証結果が失敗した場合は、通常ユーザー認証と同様のフローを実行します。このユーザー認証が成功すれば通信が可能となります(⑦-⑱)。

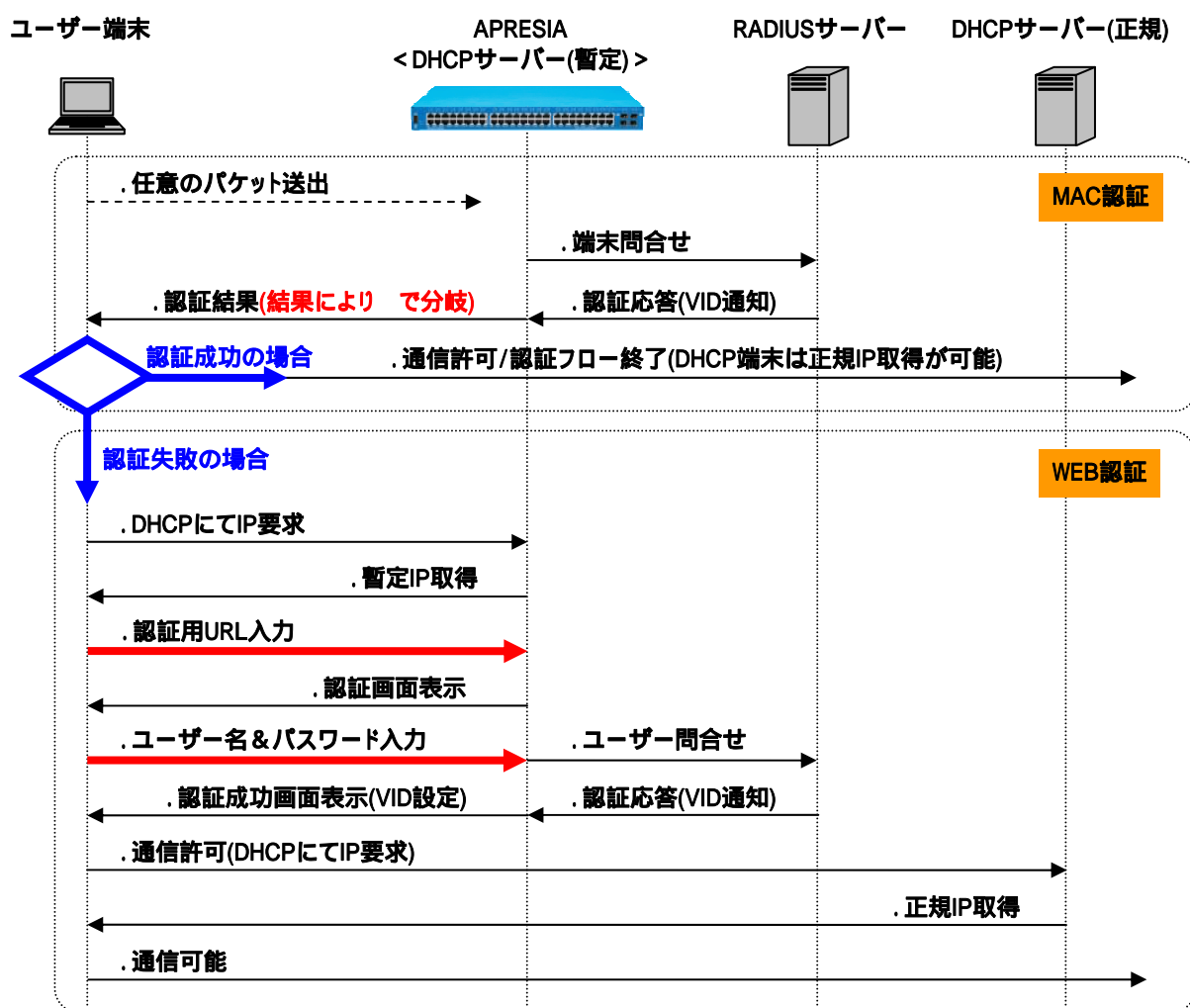


図 2-5 Web 認証と MAC 認証を併用する場合の認証フロー

※ MAC 認証に失敗した場合、当該端末のパケットは一定時間(300 秒)破棄されます(discard 登録)。discard 登録数は最大 100 個です。

2.5 Web/MAC認証(Web認証時のMAC認証先行)

Web/MAC 認証は、Web ブラウザーを使用したユーザー認証に先立ち、MAC アドレスによる認証を行う機能です。MAC アドレスによる認証が成功した場合のみ、Web によるユーザー認証を実行します。どちらの認証にも成功した場合のみ通信ができます。

動的に VLAN を割り当てる場合は、RADIUS サーバー(ローカル認証使用時はローカルデータベース)にユーザー毎に VLAN 情報を追加します。認証端末毎に VLAN を割り当てることはできません。

Web/MAC認証の認証フローを図 2-6 に示します。

- ①-②. DHCP 端末で認証する場合、最初に端末は APRESIA を経由してネットワーク上位の正規 DHCP サーバーから正規 IP アドレスを入手します。
未認証端末の packets は認証ポートを経由した通信を制限されているため、VLAN 固定での運用時は、未認証端末であっても DHCP packets を転送処理させる設定が必要です。
- ③-⑥. Web ブラウザーを起動し、認証用 URL を入力します。
APRESIA より認証画面が表示されます。ここでユーザー名とパスワードを入力します。入力された情報での認証に先立ち、ユーザー端末の MAC アドレスをもとに APRESIA は RADIUS サーバーに対して端末問合せ(MAC 認証)を行います。
- ⑦-⑧. RADIUS サーバーは自身のデータベースを参照し、該当ユーザー端末が存在するときは認証成功を通知します。認証に成功した場合のみ APRESIA はユーザー名とパスワードで RADIUS サーバーに対してユーザー問合せ(Web 認証)を行います。
- ⑨-⑩. RADIUS サーバーは自身のデータベースを参照し、該当ユーザーが存在するときは認証成功を通知します。APRESIA は自身のポートに端末の情報を登録し、同時に認証成功したことを示す Web ページを表示します。
- ⑪. 端末はこの時点で通信が可能となります。

! Web/MAC 認証における、MAC 認証の動的な VLAN 割り当ては無効になります。

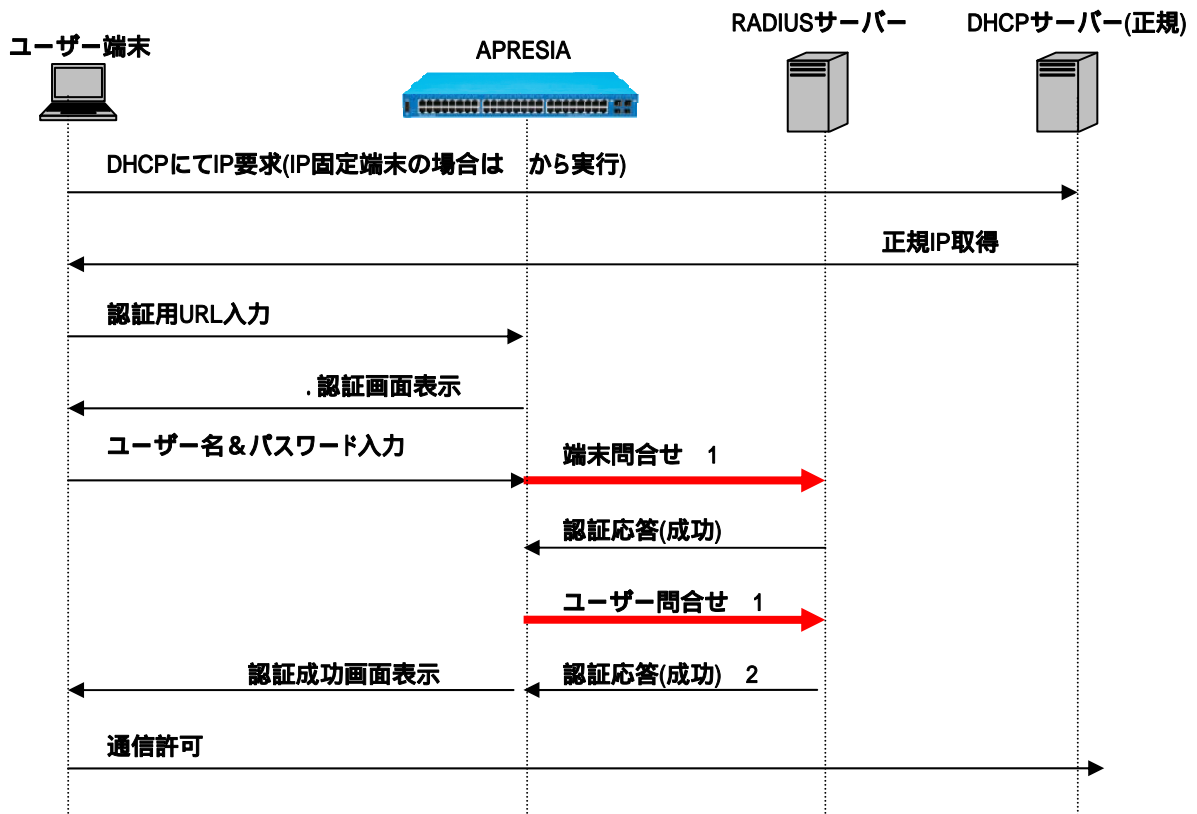


図 2-6 Web/MAC 認証フロー

※1 : Web 認証、MAC 認証と同様の属性をサポートします。

※2 : RADIUS サーバーに VLAN 情報が登録されている場合、通知される VLAN ID の VLAN に動的に変更されます。

2.6 802.1X認証

2.6.1 802.1X認証の認証フロー

APRESIAで実装されている802.1X認証の認証フローを図2-7に示します。

- ①-②. 端末から任意のフレームが送出され認証ポートに端末のMACアドレスが登録されます。
- ③. 登録されたMACアドレスに対してEAP要求(EAP RequestID)をユニキャストで送信します
※ サブリカントのMACアドレスがFDB登録された後、30秒毎(固定)に行っているFDBチェック処理で新MACが検出された時にEAP-RequestIDが送信されます。
※ 認証処理をやり直すため、EAP Failureも併せて送信される場合があります。
- ④-⑧. ユーザーアカウントを入力し、認証シーケンスが実行されます。最終的にRADIUSサーバーから認証成功メッセージが通達された時点で、遮断されていた通常トラフィックが許可されます。RADIUSサーバーの登録属性値にしたがって端末のMACアドレス毎にVLANが変更されます。
- ⑨-⑩. DHCP端末の場合、上位のDHCPサーバーよりIPアドレスを入手します。
- ⑪. 端末はこの時点で通信が可能となります。

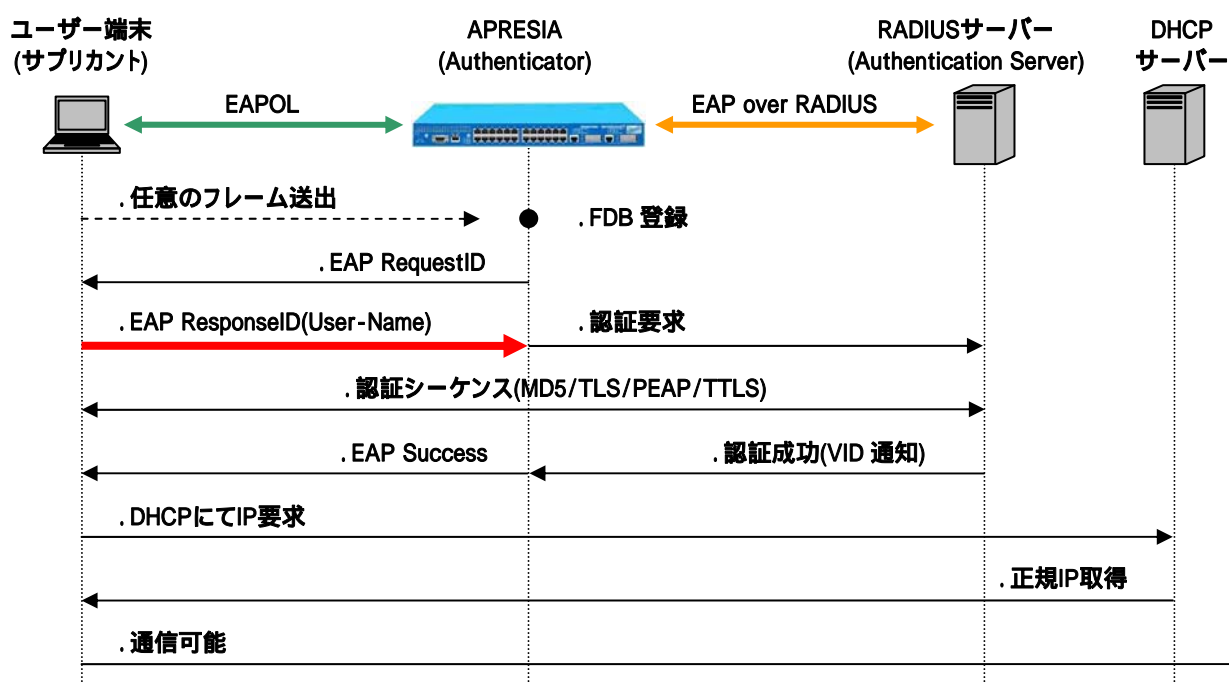


図 2-7 802.1X 認証フロー



認証時の負荷軽減のため、EAP Request ID パケットはマルチキャストではなく常にユニキャストで送信されます。

2.6.2 Unicast-EAP機能

802.1X 認証で使用する EAP メッセージは、サブリカントと Authenticator 間では特殊なマルチキャストアドレスを使用する MAC フレームでやり取りされます(EAPOL フレーム)。この特殊なマルチキャストアドレスの MAC フレームは、一般的なスイッチでは破棄されるため、802.1X 機能が有効となっているポート配下にデスクトップスイッチなどを接続して複数の端末を接続する場合には、EAP を透過する特殊なスイッチを接続する必要があります。

本機能はデフォルト有効で無効設定変更できません。

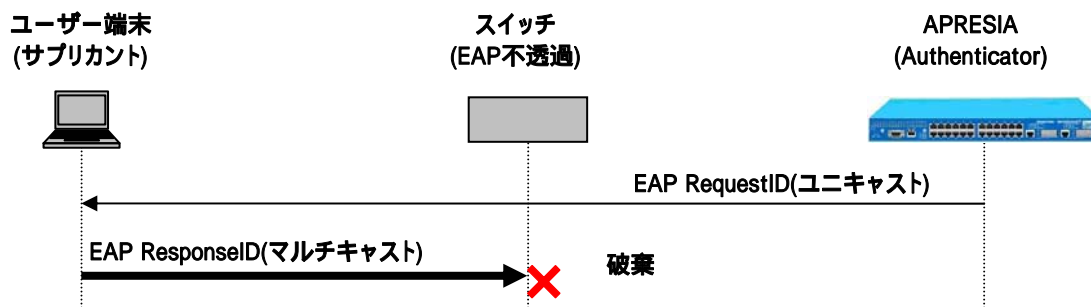


図 2-8 EAP 不透過による EAPOL フレーム破棄

APRESIA の Unicast-EAP 機能を用いることにより、サブリカントから受信する EAPOL フレームの宛先 MAC アドレスが特定のユニキャストアドレス (00-40-66-33-1D-A9) の場合でも認証が可能となります。

EAP 透過機能を持たない装置を介してサブリカントと接続する場合においても、サブリカントから送出される EAPOL フレームの宛先 MAC アドレスに特定のユニキャストアドレスを設定することにより、EAPOL フレームが破棄されることがなくなり、配下に接続するスイッチの制限がなくなります。

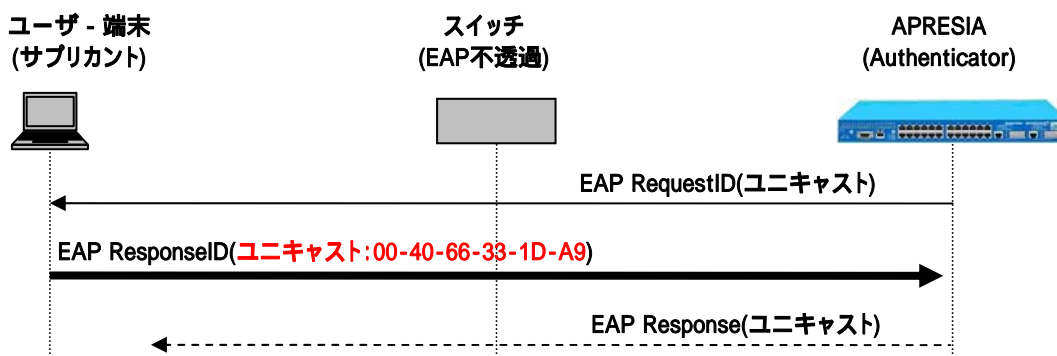


図 2-9 Unicast-EAP 機能有効時

! 本機能を使用するためには、特定ユニキャストで EAPOL フレームを送出できるサブリカントを使用する必要があります (Windows 標準サブリカントは宛先アドレスを変更できないため本機能を使用できません)。

2.6.3 動作確認済サブライアント一覧

802.1X 認証に関して、以下のサブライアントで動作可否を確認しています。これ以外のサブライアントを用いる場合は事前検証の上、導入してください。

表 2-1 動作可否確認済サブライアント

サブライアント	OS	認証方式
Windows 標準サブライアント	Windows XP SP2	EAP-MD5/PEAP/TLS
	Windows XP SP3	EAP-MD5/PEAP/TLS
	Windows Vista SP1/SP2	PEAP/TLS
	Windows 7	PEAP/TLS
MAC OS X 標準サブライアント	MAC OS X v10.5	PEAP/TLS
iNetSec Inspection Center 802.1X サブライアント (V3.0L20)	Windows XP SP2/SP3	EAP-MD5/PEAP/TLS
Odyssey Client Manager (4.32.0.2347)	Windows XP SP2/SP3	EAP-MD5/EAP-TTLS

2.7 802.1X/MAC認証(802.1X認証時のMAC認証先行)

802.1X/MAC 認証は、802.1X 認証時に先立ち、MAC アドレスによる認証を行う機能です。MAC アドレスによる認証が成功した場合のみ、802.1X 認証を実行します。どちらの認証にも成功した場合のみ通信ができます。

動的に VLAN を割り当てる場合は、RADIUS サーバー(ローカル認証使用時はローカルデータベース)にユーザー毎に VLAN 情報を追加します。認証端末毎に VLAN を割り当てることはできません。

802.1X/MAC認証の認証フローを図 2-10 に示します。

- ①-②. 端末から任意のフレームが送出され認証ポートに端末の MAC アドレスが登録されます。
- ③. 登録された MAC アドレスに対して EAP 要求(EAP RequestID)をユニキャストで送信します。
※サブリカントの MAC アドレスが FDB 登録された後、30 秒毎(固定)に行っている FDB チェック処理で新 MAC が検出された時に EAP-RequestID が送信されます。
※認証処理をやり直すため、EAP Failure も併せて送信される場合があります。
- ④-⑤. ユーザーアカウントを入力します。入力された情報での認証に先立ち、ユーザー端末の MAC アドレスをもとに APRESIA は RADIUS サーバーに対して端末問合せ(MAC 認証)を行います。
- ⑥-⑩. RADIUS サーバーは自身のデータベースを参照し、該当ユーザー端末が存在するときは認証成功を通知します。認証に成功した場合のみ 802.1X 認証の認証シーケンスが実行されます。
最終的に RADIUS サーバーから認証成功メッセージが通知された時点で、遮断されていた通常トラフィックが許可されます。
RADIUS サーバーの登録属性値にしたがって端末の MAC アドレス毎に VLAN が変更されます。
- ⑪-⑫. DHCP 端末の場合、上位の DHCP サーバーより IP アドレスを入手します。
- ⑬. 端末はこの時点で通信が可能となります。

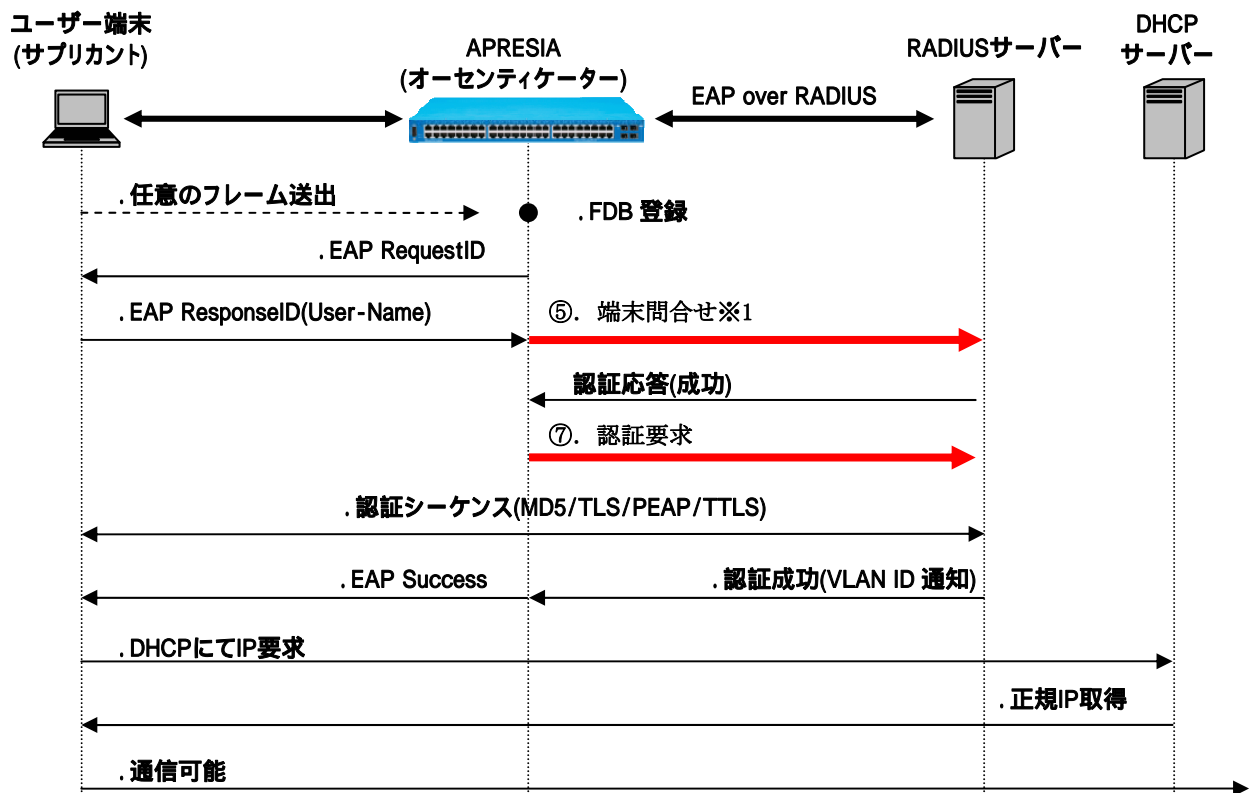


図 2-10 802.1X/MAC 認証フロー

- ❗ 802.1X/MAC 認証使用時は 802.1X 認証ポートが全て 802.1X/MAC 認証モードとなります。802.1X 認証、802.1X/MAC 認証の併用はできません。
- ❗ 802.1X/MAC 認証における、MAC 認証の動的な VLAN 割り当ては無効になります。
- ❗ 認証時の負荷軽減のため、EAP Request ID パケットはマルチキャストではなく常にユニキャストで送信されます。

2.8 DHCPスヌーピング

2.8.1 DHCPスヌーピングの動作モード

DHCP スヌーピング機能は、動作モードとして、PERMIT モード、DENY モードの 2 つの動作モードがあり、常にどちらかのモードで動作します。(デフォルト設定では PERMIT モード)

以下に PERMIT モード、DENY モード、それぞれの動作モードにおける動作概要を示します(各動作モード時の具体的な動作フローは次項で説明します)

■PERMIT モード動作時

- DHCP スヌーピングしたアドレスが送信元となる通信： 許可
- DHCP スヌーピングしたアドレスが送信元ではない通信： 許可
- 不正な DHCP サーバーからの DHCP offer パケット： 禁止(遮断)

■DENY モード動作時

- DHCP スヌーピングしたアドレスが送信元となる通信： 許可
- DHCP スヌーピングしたアドレスが送信元ではない通信： 禁止(遮断)
- 不正な DHCP サーバーからの DHCP offer パケット： 禁止(遮断)

動作モードはタイマによる自動切り替え(PERMIT モード⇒DENY モードのみ)、およびコマンドラインからの手動切り替えの 2 通りで実現可能です。また、モード切り替え時は、切り替え前までにスヌーピングした送信元情報を保有した状態で、動作モードのみ移行します。

なお、DENY モードで運用中にスイッチの再起動等を行った場合、すでに登録済みの送信元アドレス情報が削除されることで、新たにユーザー端末からの DHCP パケットをスヌーピングするまで、一時的な通信断が発生する場合があります。この場合、PERMIT モードからの自動切り替えタイマを利用し、モード切り替えタイマ設定値を DHCP サーバーで配布しているリース期間に合わせるなど DHCP の適用環境に合わせて設定することで、通信断を回避することができます。

図 2-11 にPERMITモードで起動した場合の、動作モードの概要を以下に示します。

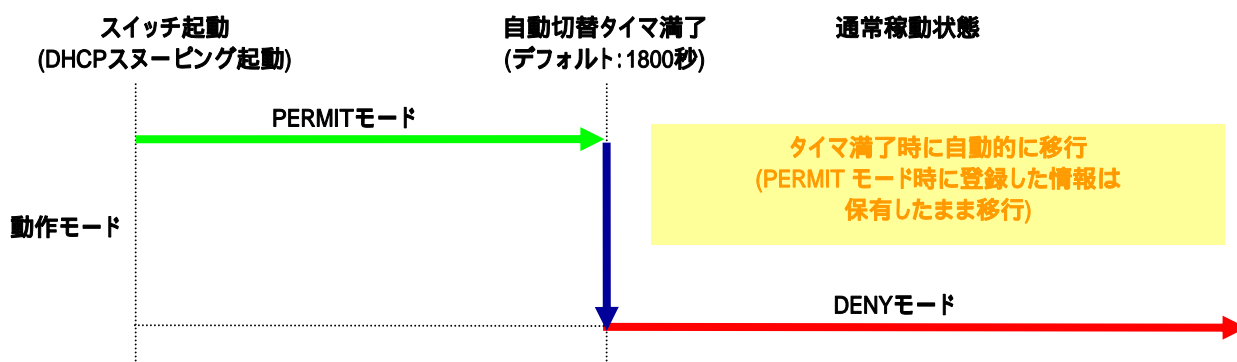


図 2-11 DHCP スヌーピング動作モード概要

! DENY モードから PERMIT モードへのタイマによる自動切替は行われません。実施する場合、コマンドラインより手動で行う必要があります。

2.8.2 DHCPスヌーピングの動作フロー

図 2-12、図 2-13 にDHCPスヌーピングの各モードの動作フローを示します。

PERMIT、DENY いずれの動作モードにおいても、正規 DHCP サーバーから払い出される DHCP ACK パケットに従い、ユーザー端末が接続されたポートに対して、払い出した IP アドレスを送信元とするパケットのみを許可するフィルタを登録します。また、ユーザー端末から DHCP Release パケットを受信した場合は、既に登録済みの送信元アドレス情報を削除します。

なお、DHCP リリースパケットによる IP アドレスの開放が行われなかった場合は、DHCP サーバーより払い出されたリース期間と同じ期間を経過した後、登録済みのフィルタ情報を自動的に削除します。

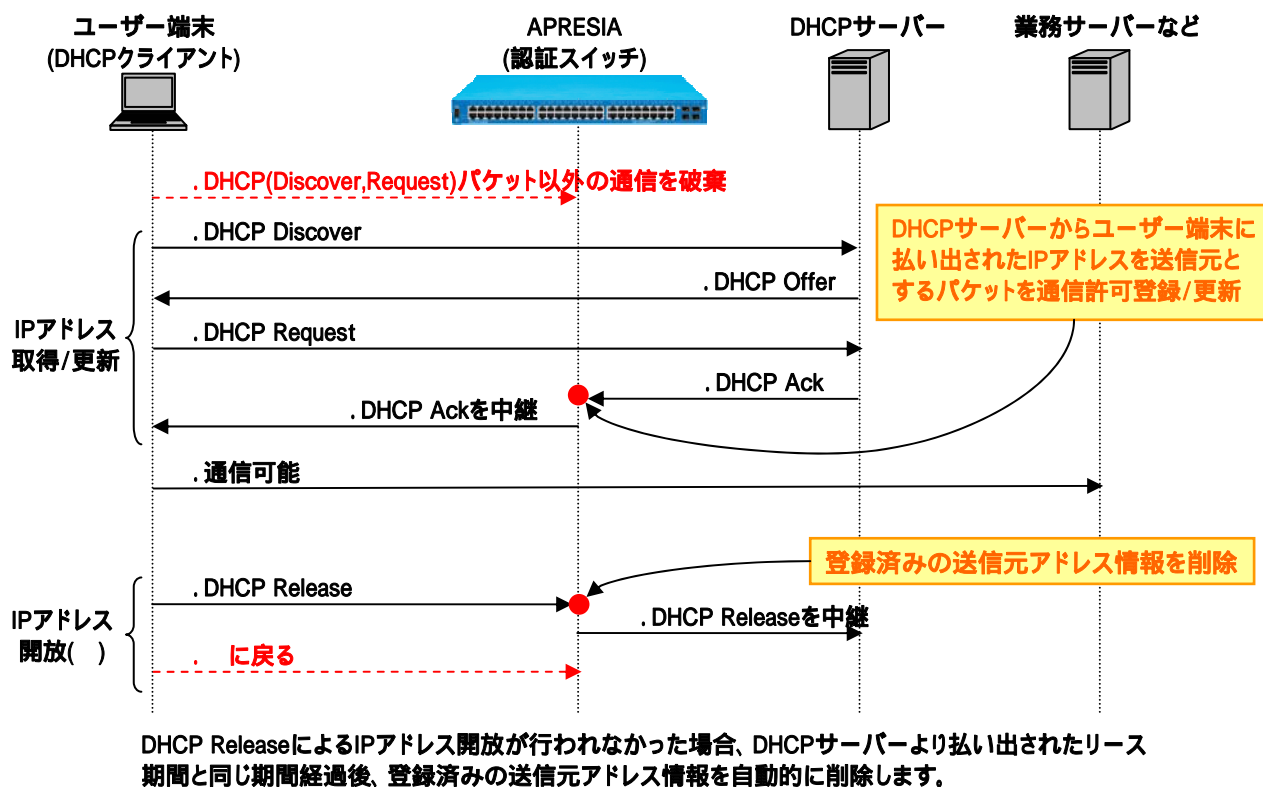


図 2-12 DENY モード時の動作フロー

- ❗ DHCP スヌーピング機能では、リンクダウンによるログアウトを行いません。リンクダウン後もリース期間が満了するまで登録が継続されます。
- ❗ 正規 DHCP サーバーが接続されるポートでは、DHCP スヌーピングを有効にしないでください。

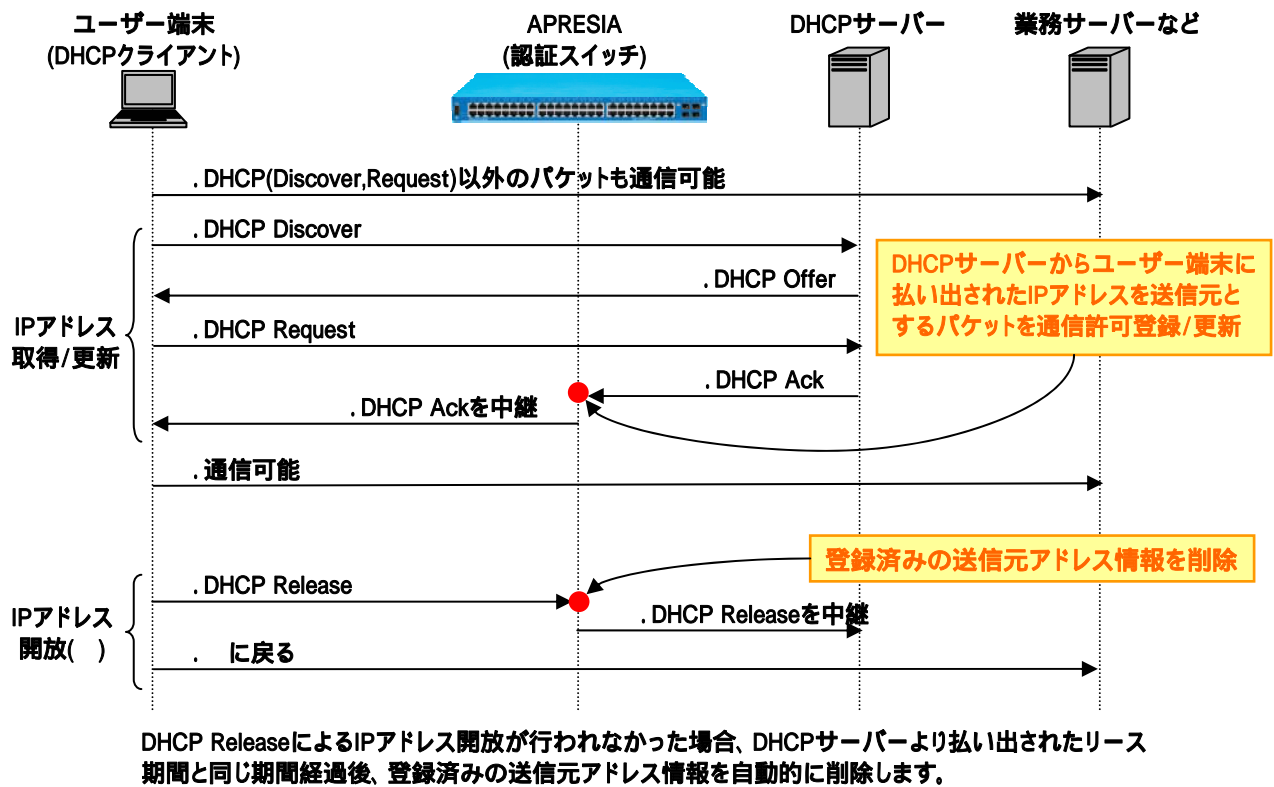


図 2-13 PERMIT モード時の動作フロー

- ❗ PERMIT モード時は、固定 IP 端末からの通信も可能となります。自動切り替えタイマを設定し、DENY モードに移行するように設定ください。
- ❗ PERMIT モードからの切り替えタイマを設定していない場合、1800 秒で DENY モードに切り替わります。タイマを 0(ゼロ)に指定した場合、自動切り替えは行われません。

2.9 認証機能と仕様

AccessDefender機能と仕様を表 2-2 に示します。

表 2-2 AccessDefender 機能と仕様

仕様		Aprsia3400 シリーズ Aprsia4300 シリーズ Aprsia5400 シリーズ	Aprsia13000 シリーズ	備考
認証 方式	IEEE802.1X	○ (EAP-MD5、EAP-TLS、PEAP、EAP-TTLS)		ゲートウェイ認証は Aprsia13000 シリーズの み対応
	Web 認証	○		
	MAC 認証	○		
	ゲートウェイ 認証	×	○	
認証 ページ リダイ レクト	HTTP/HTTPS	○		HTTP のみ(HTTPS はリダイ レクトされない)
	Proxy 利用環 境	○		
	外部 Web サー バーへのリダ イレクト	○		
認証 サー バー	対応サーバー	RADIUS		強制認証/ローカルデー タベースは単独使用可能
	バックアップ	Primary, Secondary/強制認証/ローカルデー タベース		
	ローカルデー タベース	3000 行 (ファイルサイズが 245600byte 以下の場合)		
最大収 容端末 数 注意※	Web/MAC/802. 1X/ゲート ウェイ	1408 端末/台 (Aprsia3400/4348/ 5400 シリーズ) 512 端末/台 (Aprsia4328GT)	1408 端末/台 (Aprsia13000-48X) 2816 端末/台 (Aprsia13000-24GX)	利用環境により、最大収容 端末数が異なる場合あり ゲートウェイ認証は Aprsia13000 シリーズの み対応
	Dynamic VLAN	256 端末/台 (Aprsia3400/4348/ 5400 シリーズ) 128 端末/台 (Aprsia4328GT)	256 端末/台	
	DHCP スヌー ピング	804 端末/台 (Aprsia3400/4348/ 5400 シリーズ) 356 端末/台 (Aprsia4328GT)	804 端末/台 (Aprsia13000-48X) 1608 端末/台 (Aprsia13000-24GX)	
	その他	IP 環境	固定 IP/DHCP	
	VLAN 環境	固定 VLAN/Dynamic VLAN		Web 認証の Dynamic VLAN 端末は、DHCP 環境必須 モード区別なし

	認証ページ カスタマイズ	○	内部保存/外部サーバー併 用可能
	認証バイパス	○	
全般	<ul style="list-style-type: none"> • Web、MAC、802.1X、DHCP スヌーピングの同一ポート併用可能 • 認証ポートにおいて、認証不要端末の登録が可能 		

※：Web 認証の場合、最大収容端末数は減少します。詳細は次ページの「認証端末数とフィルタリソースの関係について」を参照下さい。

2.9.1 認証端末数とフィルタリソースの関係について

AccessDefender では認証前後の端末制御にパケットフィルター2 を用います。パケットフィルター2 のハードリソースは機種毎に異なり、リソース内で AccessDefender、認証バイパス、ユーザー設定のフィルタ、各種機能で共有して使う形となります(割当は show packet-filter2 reserved-group にて確認可能です)。

表 2-3 に AccessDefender で使用するフィルタリソース(最大構成例)を示します。各数字(1~14)は packet-filter2 のグループ番号を表しています(数字が小さいほど優先順位は高くなります)。

表 2-3 AccessDefender で使用するフィルタリソース(最大構成例)

Apresia3400 シリーズ Apresia13000-24GX-PSR Apresia4328GT
 Apresia4348 シリーズ
 Apresia5400 シリーズ
 Apresia13000-48X

	14 グループ×128 ルール	14 グループ×256 ルール	7 グループ×128 ルール
1	ユーザー領域/認証バイパス/各種機能で使用		
2	AccessDefender 制御用(必須)※		
3	認証端末用(任意)1153~1280	認証端末用(任意)2305~2560	認証端末用(任意)257~384
4	認証端末用(任意)1025~1152	認証端末用(任意)2049~2304	認証端末用(任意)129~256
5	認証端末用(任意)897~1024	認証端末用(任意)1793~2048	認証端末用(必須)1~128
6	認証端末用(任意)769~896	認証端末用(任意)1537~1792	AccessDefender 制御用(必須)
7	認証端末用(任意)641~768	認証端末用(任意)1281~1536	AccessDefender 制御用(必須)
8	認証端末用(任意)513~640	認証端末用(任意)1025~1280	/
9	認証端末用(任意)385~512	認証端末用(任意)769~1024	
10	認証端末用(任意)257~384	認証端末用(任意)513~768	
11	認証端末用(任意)129~256	認証端末用(任意)257~512	
12	認証端末用(必須)1~128	認証端末用(必須)1~256	
13	AccessDefender 制御用(必須)		
14	AccessDefender 制御用(必須)		

※：認証端末用(任意)は、最大認証端末数を縮小することで、ユーザー領域/認証バイパス/各種機能用として割当可能となります。

※：グループ1の「ユーザー領域/認証バイパス/各種機能用」を AccessDefender 制御用に割り当て、認証端末用にあと1グループを割り当てることができます(MAC 認証)。

なお、Web 認証では、DNS や DHCP 等最低1つの認証バイパス用 Group の確保を推奨します。また各種機能には、下記等が含まれますので、認証機能と併用する場合は、リソースの上限を超えないよう最大端末数を制限して下さい(詳細についてはコマンドリファレンスを参照)。

- ユーザーループ検知 1 グループ確保要
- Flush FDB 1 グループ確保要
- MMRP-Plus(/MMRP) 1 グループ以上確保要(MMRP-Plus/MMRP のリング数に応じて選択)

! パケットフィルター2 の認証バイパス設定は、必ず AccessDefender のグループ番号より、小さい番号を設定して下さい。

2.9.2 最大接続端末数について(DHCPスヌーピング)

DHCPスヌーピング適用時の最大接続端末数の一覧を表 2-4 に示します。DHCPスヌーピング機能では、201 端末目以降(Apresia13000-24GX-PSRは 401 端末目以降)の接続はパケットフィルター2 のルール数を 2 つ使用 します。

例：最大ルール数が 1024 ルールの場合、DHCP スヌーピング機能では 612 端末が認証可能です。

ルール数の計算式(Apresia13000-48X の場合)

$$200 + (612 - 200) \times 2 = 1024 (\text{ルール})$$

適用機種により DHCP スヌーピングの最大接続端末数、および、パケットフィルター2 で必要な利用グルー プ数が異なりますので、ご注意ください。

なお、最大接続端末数は、DHCP スヌーピング機能のみを動作させた場合、および、DHCP スヌーピングと MAC/Web/802.1x 認証機能を併用した場合のいずれも同様となります。

表 2-4 DHCP スヌーピング最大接続端末数一覧表

機種名	Apresia4328GT	Apresia3400 シリーズ Apresia4348 シリーズ Apresia5400 シリーズ Apresia13000-48X	Apresia13000-24GX-PSR
PF2 利用グループ数			
4	128	128	256
5	228	228	456
6	292	292	584
7	356	356	712
8	—	420	840
9	—	484	968
10	—	548	1096
11	—	612	1224
12	—	676	1352
13	—	740	1480
14	—	804	1608

! DHCPスヌーピング機能の最大接続端末数は、MAC/Web/802.1x認証機能の最大接続端末数(表 2-3)と比較して少ないので、ご注意ください。

! DHCP スヌーピング機能を利用する場合、パケットフィルター2 の利用グループ数が、MAC/Web/802.1x 認証機能のみで適用する場合と異なる場合がありますので、ご注意 ください。

(例)Apresia4328GT で最大接続端末数 250 とする場合、利用するパケットフィルター 2 の利用グループ数は 6 となります。

2.10 Webサーバー応答及び仮想IPの仕組み

2.10.1 Webサーバーの仮想IPの仕組み

一般的な認証スイッチには、Webサーバーに実IPを用いて、VLAN×認証スイッチ分のIPを消費したり、実IPを重複させて設定し上位ネットワークで競合が起こらないように運用回避したりする等、運用性が考慮されていないケースも多いですが、AccessDefenderでは、認証端末がどのAPRESIA配下/VLAN配下に存在しても、同一宛先の認証ページアクセスによりWeb認証ができるよう【仮想IP】の仕組みを採用しています。

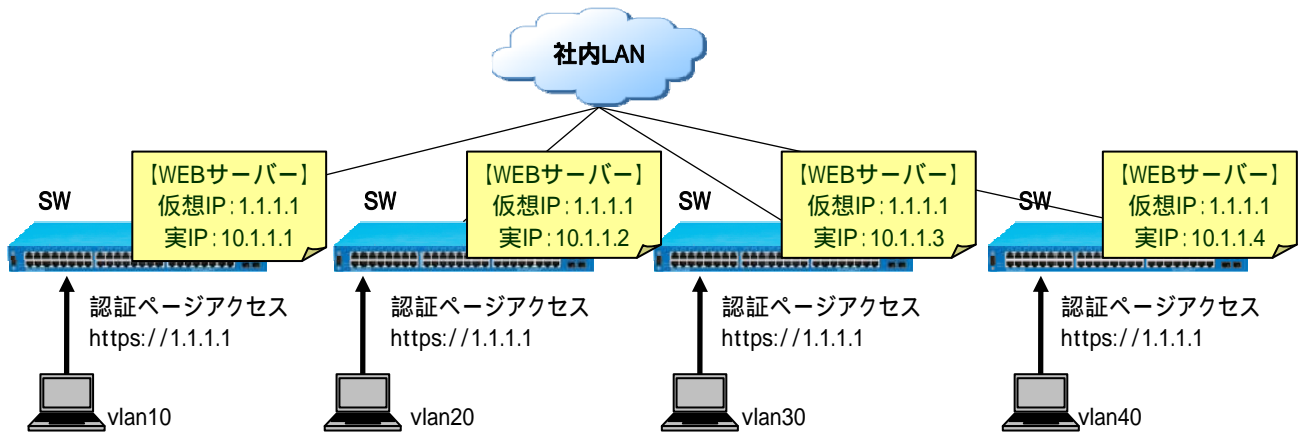


図 2-14 仮想 IP による認証 URL アクセス

どのVLANからの仮想IP宛アクセスも、APRESIAは実IPを持っているVLANからリプライを返します(送信元IPは1.1.1.1)。APRESIAの管理IPと認証端末のセグメントが異なる場合は、上位L3スイッチングハブ(以下L3スイッチと略します)にてルーティングが必要となります(特殊なルーティング設定は不要)。

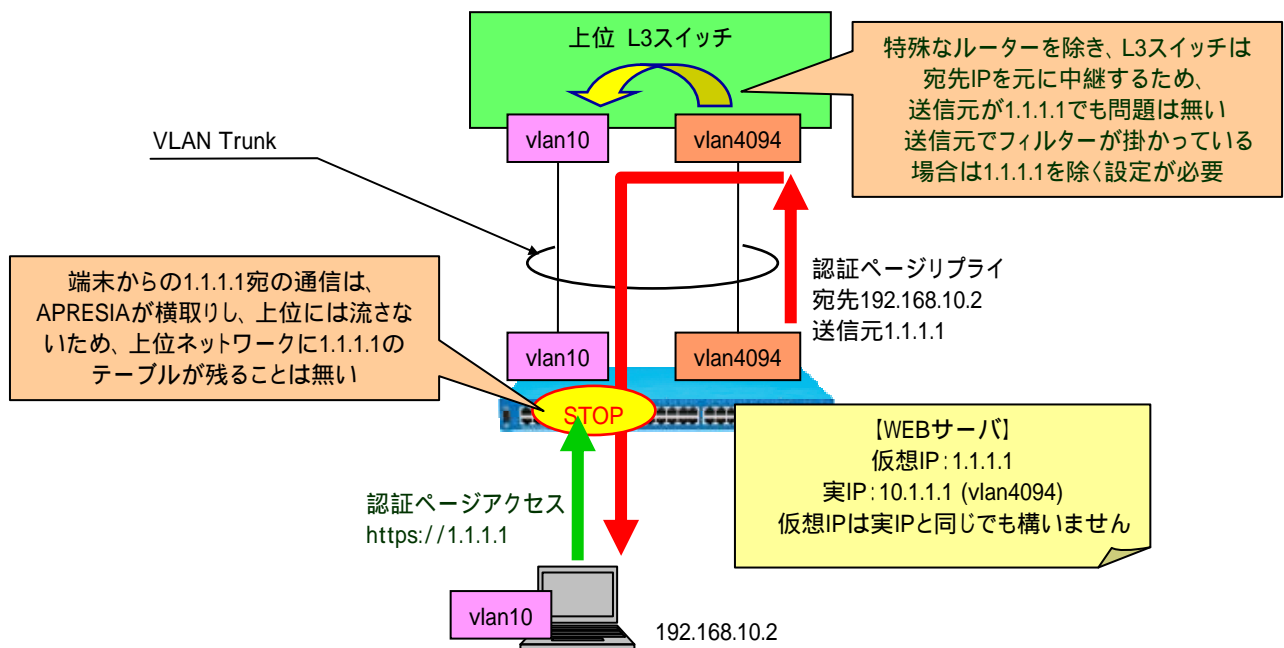


図 2-15 認証ページのリプライ応答

※ NA ではユーザーVLANからダイレクトにリプライを返していたため、AccessDefenderとの仕様差異に注

意してください。

2.10.2 認証ページリダイレクトを使用する際の注意点

本機能は、未認証端末から送信される HTTP リクエスト(宛先 IP アドレスは任意)を認識し、強制的に認証 Web ページを表示する機能です。

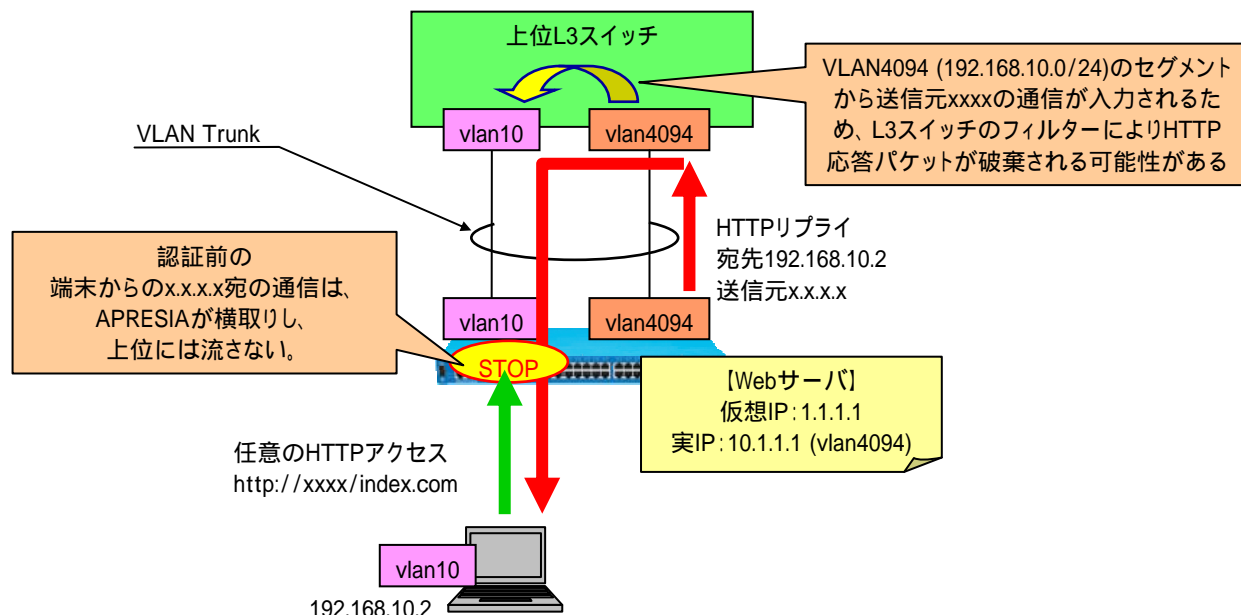
認証ページリダイレクトを使用する際は、上位 L3 スイッチのフィルタ設定の注意が必要となります。

L3 スイッチの送信元 IP アドレスを制限するフィルタ条件に APRESIA の HTTP 応答パケット等が合致する場合、以下のような対処が必要となります。

- L3 スイッチに、APRESIA 接続 VLAN(vlan4094)のフィルタを解除する
- L3 スイッチに、APRESIA の送信元 MAC を許可するフィルタを設定する
- L3 スイッチに、送信元 TCP ポート 80/443/Proxy ポートを許可するフィルタを設定する
- APRESIA に、ユーザーVLAN(vlan10)にも IP を設定する

※ 但し下記に注意してください。

- ・ ブロードキャストフレームを APRESIA が受信するようになる。
- ・ 未認証の端末から APRESIA へのアクセス(ICMP/Telnet/SNMP)が可能になる。



※NA ではユーザーVLAN からダイレクトにリプライを返していたため、AccessDefender との仕様差異に注意してください。

2.11 ブラウザーの依存性について

認証ページリダイレクトに関して、以下のブラウザで動作可否を確認しています。これ以外のブラウザ/OS を用いる場合は事前検証の上、導入下さい。

表 2-5 動作可否確認済みブラウザ(認証ページリダイレクト使用時)

ブラウザ	OS	リダイレクト可否
Internet Explorer 6	Windows XP SP2	○
Sleipnir 2.6.2(Trident/Gecko)	Windows XP SP2	○
Opera 6.1	Windows XP SP2	○
Opera 7.0	Windows XP SP2	○
Opera 9.1	Windows XP SP2	○
Opera 9.2	Windows XP SP2	○
FireFox 2	Windows XP SP2	○
Safari 3.1	Windows XP SP2	○
Internet Explorer 7	Windows Vista	○
Internet Explorer 8	Windows 7 Pro	○
Internet Explorer 9	Windows 7 Pro	○
FireFox 6.0.2	Windows 7 Pro	○
Safari 5.1	Windows 7 Pro	○
Firefox 1.0	Red Hat Enterprise Linux ES4 (Kernel 2.6.9-5.EL)	○
Firefox 1.5	CentOS 4.6(Final) (Kernel 2.6.9-67.0.1.EL)	○
NetScape Communicator 4.7	MacOS9.2 (Mac OS X 10.3.9 Classic)	○
Internet Explorer 5.0	MacOS9.2 (Mac OS X 10.3.9 Classic)	○
Internet Explorer 5.2	MacOS X 10.3.9	○
FireFox 2	MacOS X 10.3.9	○
Safari 1.x	MacOS X 10.3.9	○
Opera 9.1	MacOS X 10.3.9	○
Opera 9.2	MacOS X 10.3.9	○

2.12 ログアウト処理について

AccessDefender機能使用時のログアウト処理について表 2-6 に示します。

7種類のログアウト処理をサポートしており、端末の接続状況に応じて柔軟なログアウト処理が可能です。

表 2-6 ログアウト処理について

No	ログアウト方法	動作概要	Syslog 表示	Web 認証	MAC 認証	dot1x 認証
1	ログアウトボタン ※1	認証画面のログアウトボタンによりユーザーが手動でログアウト	web	○	—	—
2	リンクダウン	APRESIAの認証ポートがリンクダウンした際に、当該ポートで認証済の全端末をログアウト	link down	○	○	○
3	エージング	一定時間通信が行われなかった端末をログアウト	aging	○	○	○
4	Max Timeout	認証後一定時間が経過した端末をログアウト	maxtime	○	○	○
5	CLI コマンド	管理者がCLIで認証済端末のMACアドレスを指定してログアウト	cli	○	○	—
6	設定変更	認証関連、認証ポートの設定変更を行った際にログアウト	config change	○	○	○
7	認証済端末の再認証	Web 認証で、認証済の端末が再度 Web 認証を行った場合に、最初の認証状態をログアウト	overwrite	○	—	—

※1：設定によらず、常に有効となります。



ログアウトの設定は装置単位となります。ポート毎に設定を変更することはできません。

2.13 入力可能な文字について(ユーザーID/パスワード共通)

ユーザーID とパスワードには、ASCII コードの印字可能な文字が入力可能です。使用する RADIUS サーバーの仕様にしたが、RADIUS サーバーの定義ファイルに定義する必要があります。

①認証 Web ページで入力可能な文字数

【ユーザーID】 63 文字

【パスワード】 63 文字

- ユーザーID、パスワード共に 64 文字目を入力しようとしても入力できません。

②認証 Web ページで入力可能な文字

【ユーザーID】 数字、アルファベット、!"#\$%&'()=^|`{+*} <>?_~¥@[:;],./

【パスワード】 数字、アルファベット、!"#\$%&'()=^|`{+*} <>?_~¥@[:;],./

- ユーザーID、パスワード共に、キーボードから直接入力できる文字は全て有効となります。
- APRESIA の設定コンソール上では「?」はコマンドヘルプと認識されるため、MAC 認証用のパスワード設定では「?」は入力できません。ただし、「?」が入力された状態の startup-config を TFTP サーバーから取り込めば使用可能です。
- RADIUS サーバーにより制御文字の扱いが異なりますので、使用する RADIUS サーバーの仕様にしたがう必要があります。
- 日本語はユーザーID で入力はできますが、認証不可(失敗)となります。
- ユーザーID、パスワード共に、「&」、>、「<」は、そのまま文字列として認証可能です。
- ユーザーID、パスワード共に、
といった HTML タグ形式もそのままの文字列として認証可能です。

3. AccessDefender機能の設定

AccessDefender 機能を使用する際には、APRESIA 側で下記条件を満たしている必要があります。

- APRESIA に管理用 IP アドレスが設定されていること
- APRESIA と RADIUS サーバーが通信可能であること (ローカルデータベースのみで認証する場合は不要です)

3.1 APRESIAの設定項目

APRESIAの設定項目を表 3-1 に示します。

「○」は必須設定項目、「－」は設定不要・不可項目、空白は任意設定項目であることを示しています。

表 3-1 AccessDefender 設定項目

No	項目	default 設定	認証方法				備考
			Web	MAC	1X	DHCP	
1	AccessDefender 有効化	disable	○	○	○	○	
2	RADIUS サーバー ※1 ・ INDEX ・ IP アドレス ・ UDP ポート番号 ・ タイムアウト時間 ・ リトライ回数 ・ 共有鍵(シークレットキー) ・ Primary/Secondary 指定 ・ ローカル認証 ・ 強制認証 ・ デッドタイム	なし なし 1812 3 秒 3 回 なし なし なし なし なし	○ ○ ○ ○ ○	○ ○ ○ ○ ○	○ ○ ○ ○ ○	－ － － － － － － － － － －	1～8 1～65535 1～30 秒 1～5 回 最大 127 文字 1～8 1～1440 分
3	認証ポート ・ Web 認証 ・ MAC 認証 ・ dot1x 認証 ・ DHCP スヌーピング	なし なし なし なし	○ － － －	－ ○ － －	－ － ○ －	－ － － ○	ポート併用可能
4	MAC 認証パスワード	なし	－	○	－		
5	認証 Web ページ ・ HTTP ポート番号 ・ HTTPS ポート番号 ・ 認証用 IP アドレス (URL) ・ リダイレクト URL ・ リダイレクト対象ポート (HTTP) ・ リダイレクト対象ポート (HTTPS) ・ リダイレクト対象ポート (Proxy)	なし なし なし なし なし なし なし	○ ○ ○ ○	－ － － － － － －	－ － － － － － －	1～65535 1～65535 最大 255 文字 ポート 80 ポート 443 1～65535	

6	再認証(802.1X) ・ 再認証有効 ・ 再認証間隔	なし 3600 秒	— —	— —	— —	— —	5-2147483647 秒
7	リトライ関係(802.1X) ・ サプリカントからの応答タイムアウト ・ サプリカントへの要求最大再送回数	30 秒 2 回	— —	— —	— —	— —	5-65535 秒 1-10 回
8	ログアウト条件 ・ エージング ・ 接続時間	0 秒 0 秒			— —	— —	10 秒~1 ヶ月 10 秒~1 ヶ月
9	最大接続台数 ・ ポート番号 ・ 最大接続台数(1 ポートあたり) ・ 最大接続台数(装置あたり)	なし なし なし				○ ○ ○ ○	
10	DHCP スヌーピング ・ 静的フィルタ登録 ※2 ・ 自動切換えモードタイマ ※3	なし なし	— —	— —	— —		
11	その他 ・ 制御用先頭グループ ※4 ・ 802.1X 初期化実行 ・ 802.1X 再認証実行	なし なし なし	— —	— —	— —	— —	随時(その都度実行します)
12	SSL 用秘密鍵(鍵長) ※5	1024bit			— —	— —	512~2048bit
13	syslog(IP/facility/priority) ※6	なし					
14	packet-filter2 ・ 強制転送(認証バイパス)	なし					

※1：ローカルデータベースのみで認証する場合は外部 RADIUS サーバーの設定は不要です。

※2：ポートに対して、静的にフィルタを登録することで、DHCP スヌーピング機能が有効なポートであっても、特定の固定 IP 端末からの通信を許可します。

※3：PERMIT モードで起動後、自動的に DENY モードに切替わるまでの時間です。

※4：通常では設定する必要はありません。

※5：ファームウェアには予めテスト用の証明書と秘密鍵が埋め込まれており、証明書をインストールしなくても本機能を使用できます。別途証明書を用意する場合は 9 SSL設定について で紹介するいずれかの手順で、証明書/秘密鍵をインストールして下さい。

※6：syslog サーバーでの統合管理をする場合は必須です。AccessDefender 関連のログは優先度が notice 以上になります(DHCP スヌーピングの一部ログを除く)。

3.2 ローカルデータベース認証と強制認証

APRESIA に設定されている RADIUS サーバーからの応答がタイムアウトした場合などに、APRESIA 内部に保存されているデータベースを用いて認証したり (ローカルデータベース認証)、強制的に認証を成功させたりする (強制認証) 機能です。

主な使用目的としては RADIUS サーバーの障害対策 (RADIUS サーバー自体の障害、センタ内のネットワーク障害、回線障害など) が挙げられますが、ローカルデータベース認証は RADIUS サーバーに関する設定を行わないことにより、APRESIA 単独での認証が可能単独での使用が可能のため、小規模ユーザーにはネットワーク認証の導入がより簡単に行えます。

ローカルデータベース認証と強制認証の概念図を

図 3-1 に示します。

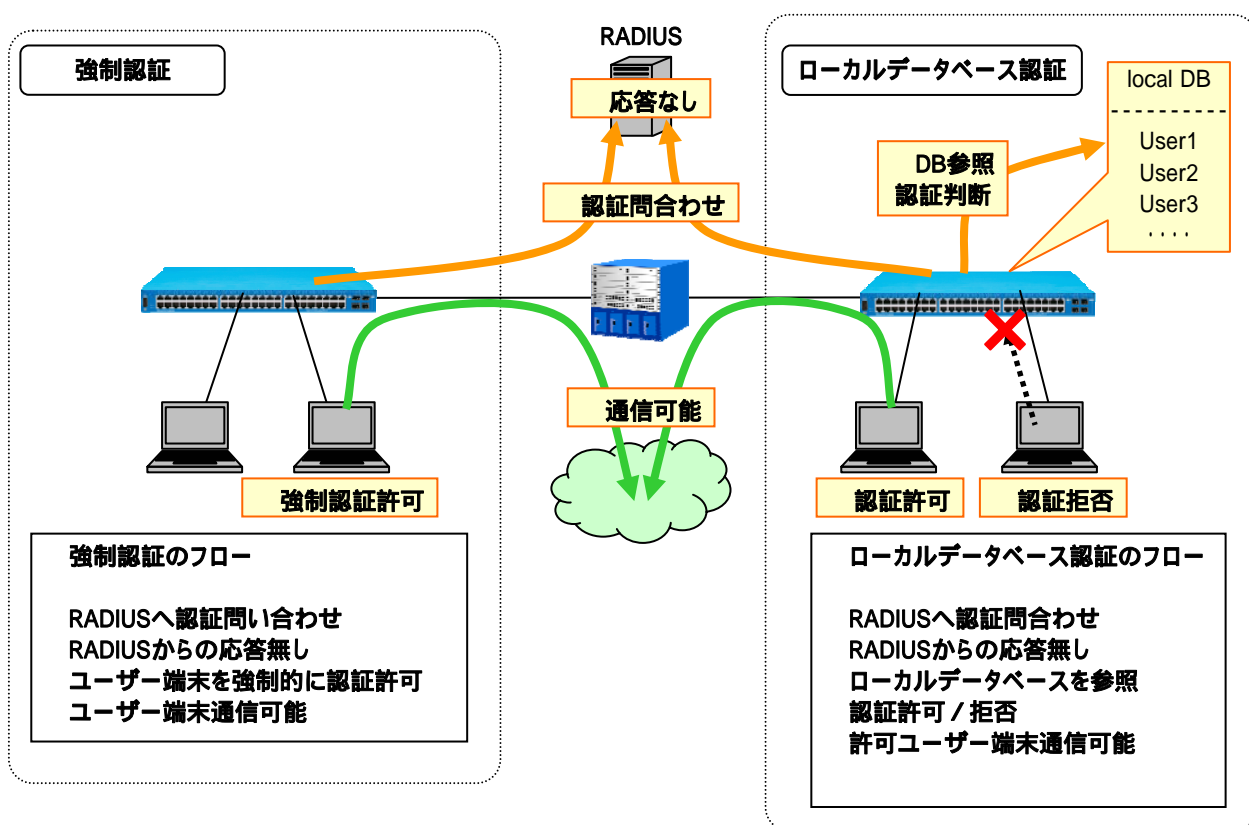



図 3-1 ローカルデータベース認証と強制認証

ローカルデータベース認証と強制認証の設定コマンドは以下となります。

```
(config)# aaa authentication {web|mac} radius <INDEX1> [<INDEX2>] [local | force [vlan <VID>]]
    . . . INDEX1          Primary RADIUS サーバーの INDEX (1-8)
    . . . INDEX2          secondary RADIUS サーバーの INDEX (1-8)
    . . . local           ローカルデータベース認証を実行
    . . . force           強制認証を実行
    . . . vlan <VID>     強制認証後の VLAN
```



ローカル認証と強制認証を同時に設定することはできません。

 ローカル認証および強制認証は、ポート毎ではなく装置単位での設定となります。

3.2.1 ローカルデータベースによる認証(Web/MAC認証のみ)

APRESIA 内部にユーザー名・パスワード・VID を格納したローカルデータベース(aaa-local-db)を保持し、このデータベースを用いて AccessDefender 認証を実行します。ローカル認証を有効にしている場合、RADIUS サーバーが無い場合や RADIUS サーバーからの応答がタイムアウトした場合ならびにシークレットキーが異なる場合、APRESIA 内部に保存しているデータベースを用いて認証を実行します。

APRESIA側にRADIUSサーバーの設定があり、ローカル認証機能を使用している場合の動作を表 3-2 に示します。

表 3-2 ローカル認証機能有効時の動作(APRESIA 側の RADIUS 設定あり)

RADIUS サーバーとの通信可否	認証動作
通信可能かつ RADIUS プロトコルの応答あり	通常の認証
通信可能だが RADIUS プロトコルの応答なし	ローカル認証
通信不可	ローカル認証
シークレットキーの相違	ローカル認証

! APRESIA 側に RADIUS サーバーの設定がなく、ローカル認証機能が有効となっている場合は、ローカルデータベースでのみ認証が行われます。

3.2.2 ローカル認証DBフォーマット

APRESIA内部に保存するローカル認証用DBのフォーマットを表 3-3 に示します。

表 3-3 ローカル認証 DB フォーマット

項目	内容
形式	userid, password [, vid]の CSV 形式(userid, password は最大 63 文字)
最大登録行数	3000 行

<ローカルデータベースの登録例>

temp01, temp01, 10
temp02, temp02
temp03, temp03, 30
00096b82c51e, 1q2w3d, 100

! MAC 認証の場合、MAC アドレス(16 進文字列、区切り文字無しの 16 文字)を、userid として登録して下さい。なお、アルファベットは小文字(a-f)で記述する必要があります。

3.2.3 ローカルデータベースの登録(ダウンロード)

作成したローカルデータベースファイルは、TFTP を用いて APRESIA に登録(ダウンロード)します。登録は AccessDefender 有効時にも可能で、新しいファイルが上書きされます。

```
# copy tftp <TFTP_IPADDR> <FILE> aaa-local-db
      . . . TFTP_IPADDR          TFTP サーバーの IP アドレス
      . . . FILE                 ローカルデータベースファイル名
```

! 登録行数が 3001 行以上ある、または書式に従わない行が存在する、もしくはファイルサイズが 245600byte を超えるいずれかの場合、その内容を表示してダウンロード処理を中断します。

! ローカルデータベースのファイルにおいて、改行のみの行がある場合、ダウンロードできません。ローカルデータベースのファイル中に改行のみの行を含めないでください。

APRESIAに登録(ダウンロード)時に表示されるコンソールメッセージの例を表 3-4 に示します。

表 3-4 ローカルデータベースの登録(ダウンロード)時のコンソールメッセージ表示例(抜粋)

内容	表示例
正常なファイルの場合	Writing to flash memory... done.
3000 行以上ある場合	local-db : over max user ldb.txt : download fail
改行のみの行がある場合	Invalid format: line: 298 ldb.txt : download fail
書式不適合な行がある場合	Invalid format: line: 10 user10, ,user10, 10 ldb.txt : download fail

! Apresia4300 シリーズにおいて、Ver7.11.04 以前から Ver7.12.01 以降へバージョンアップする際、装置のローカルデータベースは引き継がれません。7.12.01 以降へバージョンアップする場合、一度 TFTP サーバーへアップロードして、バージョンアップ後、再度ダウンロードして下さい。

3.2.4 ローカルデータベースのバックアップ(アップロード)

APRESIA に登録してあるローカルデータベースは、TFTP を用いてサーバーにアップロードできます。

```
# copy aaa-local-db tftp <TFTP_IPADDR> <FILE>
    . . . TFTP_IPADDR      TFTP サーバーの IP アドレス
    . . . FILE              ローカルデータベースファイル名
```

! ダウンロードするコマンドと酷似しているため注意して下さい。

3.2.5 ローカルデータベースの削除

APRESIA に登録済みの DB を削除するには「erase aaa-local-db」コマンドを実行します。登録されている全てのアカウントが削除されます。

```
# erase aaa-local-db
    . . . 登録済みローカルデータベースを削除
```

! 特定のアカウントのみを削除する場合には、該当アカウントを削除したファイルを新たに上書き登録して下さい。

3.2.6 ローカルデータベースの編集(追加)

本装置に保存されている AccessDefender ローカルデータベースにエントリーを追加します。
<PASSWORD>省略時はパスワード無しとして、<VID>省略時は VLAN ID:0 として登録されます。

```
# aaa-local-db add user <USERID> [password <PASSWORD>] [vlan <VID>]
    . . . USERID          ユーザーID <1-63(文字)>
    . . . PASSWORD        パスワード <1-63(文字)>
    . . . VID             VLAN ID <1-4094>
```

登録時に表示されるコンソールメッセージの例を表 3-5 に示します。

表 3-5 登録時のコンソールメッセージ表示例

内容	表示例
正常な場合	Writing to flash memory... done.
3000 件以上となる場合	% aaa-local-db : over max user
最大サイズを超える場合	% aaa-local-db : over max file size
使用禁止文字を指定した場合	% Invalid user ID.

3.2.7 ローカルデータベースの編集(削除)

本装置に保存されている AccessDefender ローカルデータベースのエントリを削除します。

```
# aaa-local-db del user <USERID>  
      . . . USERID                ユーザーID <1-63(文字)>
```

削除時に表示されるコンソールメッセージの例を表 3-6 に示します。

表 3-6 削除時のコンソールメッセージ表示例

内容	表示例
正常な場合	Writing to flash memory... done.
使用禁止文字を指定した場合	% Invalid user ID.

3.2.8 強制認証機能





RADIUS サーバーからの応答が正常に返ってこない場合などの救済措置として強制的にネットワーク接続を許可することが可能です。

強制認証を有効にした場合、RADIUS サーバーの設定が無い場合や RADIUS サーバーからの応答がタイムアウトした場合、ならびにシークレットキーが異なる場合、未認証のままネットワークに強制的に接続することができます。

APRESIA側にRADIUSサーバーの設定があり、強制認証機能を使用している場合の動作を表 3-7 に示します。

表 3-7 強制認証機能有効時の動作 (APRESIA 側の RADIUS 設定あり)

RADIUS サーバーとの通信可否	認証動作
通信可能かつ RADIUS プロトコルの応答あり	通常の認証
通信可能だが RADIUS プロトコルの応答なし	強制認証
通信不可	強制認証
シークレットキーの相違	強制認証

-  ローカル認証と強制認証を同時に設定することはできません。
-  ローカル認証および強制認証は、ポート毎ではなく装置単位での設定となります。
-  APRESIA側にRADIUSサーバーの設定がなく、強制認証機能が有効となっている場合、RADIUS認証なしで強制的に接続許可されます。接続された端末の情報は認証ログとして全て残るため、これを利用して端末のMACアドレスを収集することが可能です(詳細は 7.4 MACアドレスの自動収集 を参照下さい)。
-  強制認証機能はセキュリティ上の問題となる可能性がありますので、十分検討の上使用して下さい。

3.2.9 強制認証機能(802.1X)

本機能を有効にすることにより、認証端末が、装置に設定されている全ての認証サーバーにアクセスできない場合、予め設定されている VLAN に接続し認証成功となります。これにより、RADIUS サーバーへの通信が不可状態に陥っても限定された通信だけは一時的に確保することができますようになります。

強制認証の設定コマンドは以下となります。

```
(config)# aaa authentication dot1x radius <INDEX1> [<INDEX2>] [force [vlan <VID>]]
```

...	INDEX1	Primary RADIUS サーバーの INDEX (1-8)
...	INDEX2	secondary RADIUS サーバーの INDEX (1-8)
...	force	強制認証を実行
...	vlan <VID>	強制認証後の VLAN

RADIUS サーバーから正常な応答がある場合には、

図 3-2 のように通常の認証が実行されますが、RADIUS サーバーから正常な応答がなかった場合、強制認証機能が有効時では、以下のような認証フローにより、設定された VLAN に変更されます(複数の RADIUS サーバーの設定やリトライの処理を省略しています)。

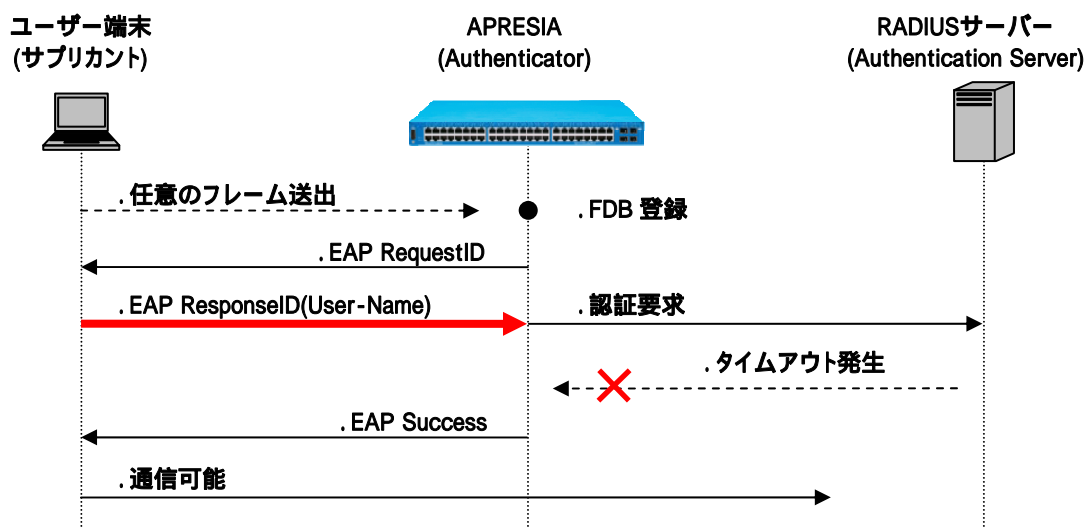


図 3-2 強制認証機能有効時における RADIUS 無応答時の認証フロー

! 本機能が有効の場合、設定されている RADIUS サーバー全てがタイムアウトの時に、サブリカントに EAP-Success を返します。しかしサブリカントの仕様によっては EAP-Success を受信しても認証成功状態にならず、通信できない場合や、認証成功後も EAPOL-Start 送信を繰り返し、認証処理を繰り返す場合もあります。

3.3 認証順序変更(Web認証、MAC認証のみ)

本機能を有効にすることにより、ローカルログインを優先することができます。ローカルデータベースに登録のないユーザーまたは問い合わせの結果パスワードが不一致であった場合は RADIUS サーバーへの問い合わせまたは、強制認証を行います。

認証順序変更の設定コマンドは以下となります。

```
(config)# aaa authentication web | mac local [radius <INDEX1> [<INDEX2>] [force [vlan <VID>]]]
    . . . INDEX1           Primary RADIUS サーバーの INDEX(1-8)
    . . . INDEX2           Secondary RADIUS サーバーの INDEX(1-8)
    . . . force            強制認証を実行
    . . . vlan <VID>      強制認証後の VLAN
```

ローカルログインが成功した場合は認証成功となりますが、失敗した場合は 図 3-3 のようにRADIUSサーバーへの問合せまたは、強制認証を行います。

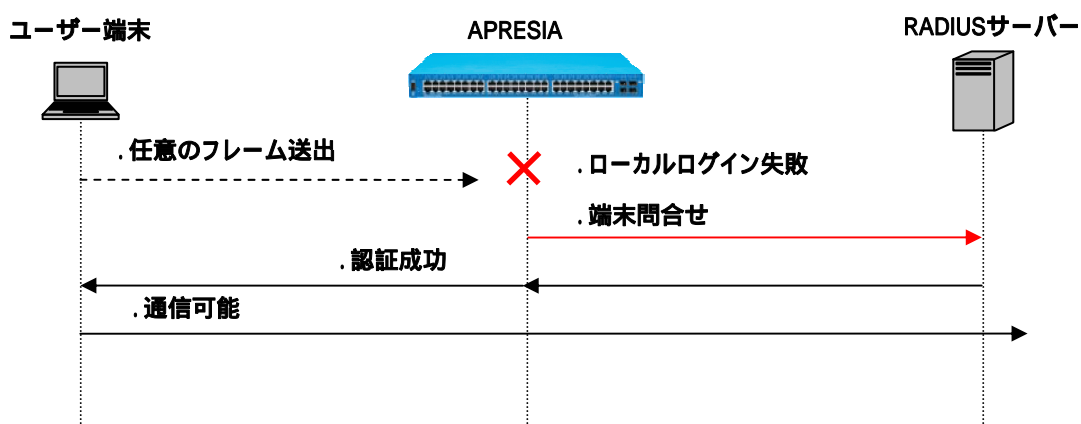


図 3-3 認証順序変更時におけるローカルログイン失敗時の認証フロー(MAC 認証)

! 本機能を使用する場合は、3.4 移行条件変更機能を併せて設定する必要があります。設定しない場合はローカルログイン失敗後の端末問合せは行われませんので注意してください。詳しくは3.4 移行条件変更機能を参照してください。

3.4 移行条件変更機能(Web認証、MAC認証のみ)

本機能を有効にすることにより、RADIUS サーバーからの認証拒否応答受信による認証失敗時にセカンダリーRADIUS サーバーまたはローカルログイン、強制認証機能での認証が有効となります。

移行条件変更機能の設定コマンドは以下となります。

```
(config)# aaa authentication web | mac control sufficient
```

RADIUSサーバーから認証拒否応答があった場合、移行条件変更機能が有効時では図 3-4 のようにセカンダリーRADIUSサーバーまたはローカルログイン、強制認証機能へ移行します。

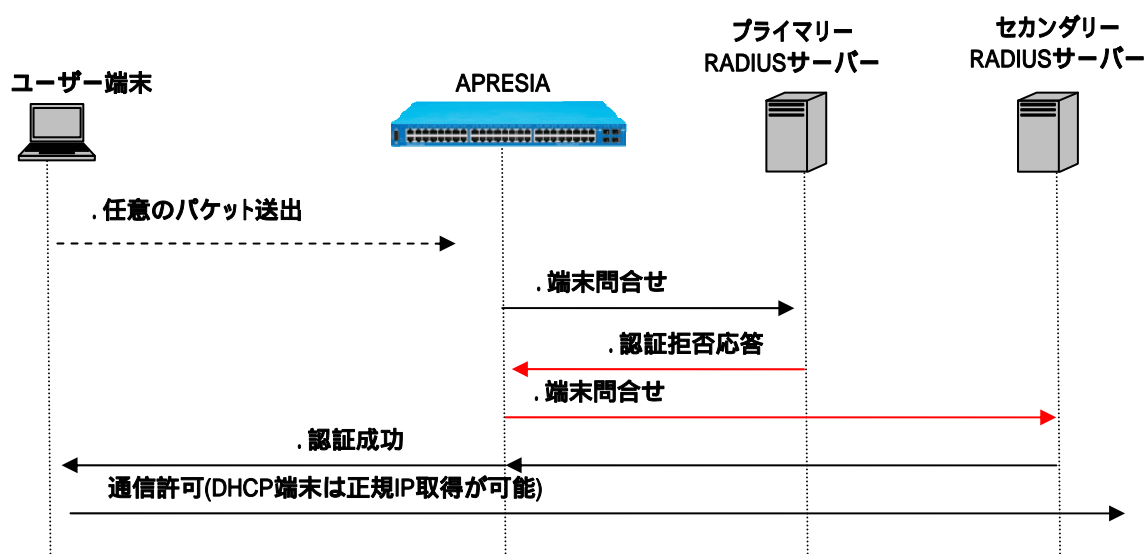


図 3-4 移行条件変更機能有効時における RADIUS 認証拒否時の認証フロー (MAC 認証)

! 認証方法として RADIUS サーバーと強制認証を選択している場合、RADIUS サーバーでのユーザー名またはパスワード誤りによる認証失敗時は強制認証へ移行しません。RADIUS サーバーがタイムアウトした際は強制認証へ移行します。

3.5 認証方法選択機能(Web認証のみ)

本機能を有効にすることにより、ユーザーがブラウザ上で認証 ID を指定し、あらかじめ認証 ID 毎に設定した認証方法を選択することが可能になります。

本機能を使用するためには、認証ページ内に認証IDを埋め込む必要があります。認証ページのカスタマイズ方法は、7.1.3 を参照してください。

認証方法選択機能の設定コマンドは以下となります。

```
(config)# aaa authentication web <1-4> radius <INDEX1> [INDEX2] [local] |(force [vlan <VID>])
(config)# aaa authentication web <1-4> local [radius <INDEX1> [INDEX2] [force [vlan <VID>]]]
(config)# aaa authentication web <1-4> force [vlan <VID>]
```

認証方法選択機能を使用したときの認証動作を図 3-5 に示します。

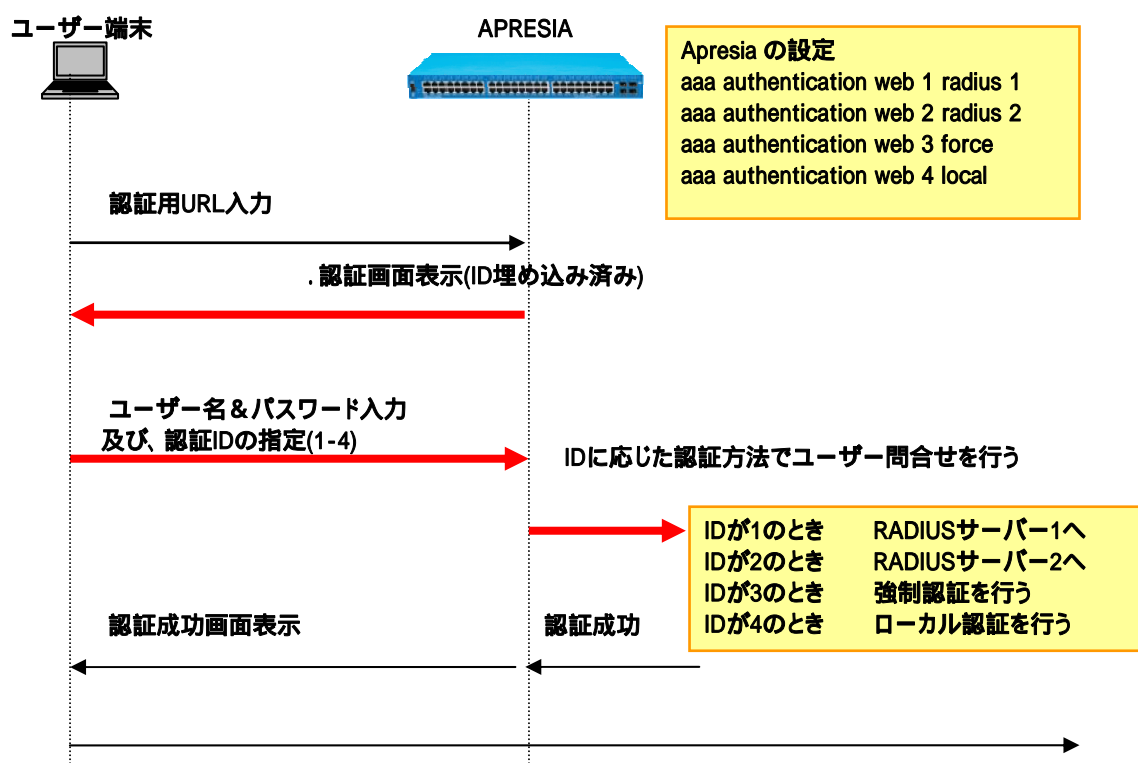


図 3-5 認証方法選択機能の認証フロー

3.6 認証拒否機能

本機能にて認証端末の IP アドレスまたは、MAC アドレスを指定することにより、指定した端末の認証を一時的に拒否することができます。

主な使用目的としては APRESIA に対して繰り返し不正な認証要求をしてくる端末の MAC アドレスを指定して、一定時間の認証を拒否し、認証負荷軽減するなどが挙げられます。

本機能を使用する場合、事前に packet-filter2 max-rule コマンドで deny-rule の設定が必要です。

認証拒否機能の実行コマンドは以下となります。

```
# access-defender-deny (ip <IPADDR> | (mac <MACADDR>) timer <MINUTES>
    . . . IPADDR                認証拒否する端末の IP アドレス
    . . . MACADDR              認証拒否する端末の MAC アドレス
    . . . MINUTES              認証拒否時間(1-60)
```

WEB認証の場合は 図 3-6 のように認証用URLへのアクセスが不可となります。

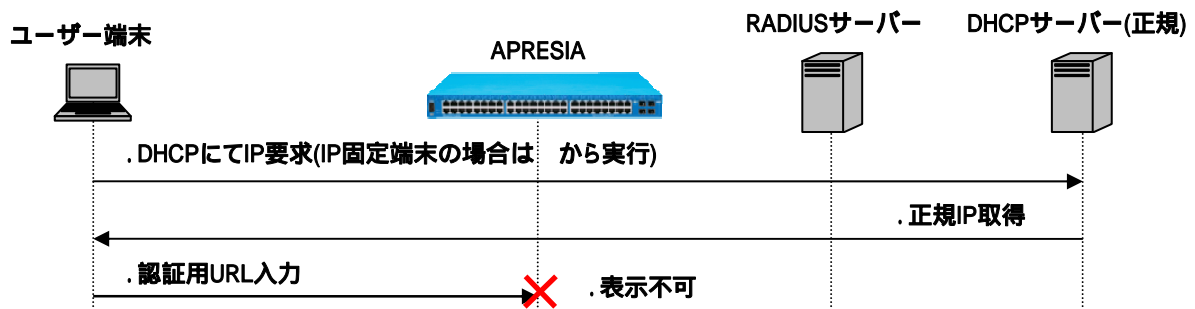


図 3-6 Web 認証端末の認証拒否

! MAC 認証ポートにて access-defender-deny ip の指定端末から本装置宛に PING 通信した場合、MAC 認証が行われます。

3.7 DHCPパケットのMAC認証除外

本機能を有効にすることにより、認証端末から送信されるUDPポート67(DHCPサーバー)宛パケットをMAC認証の対象外とします。これにより、IPアドレス取得中に認証が成功しVLANが動的に割当たり、DHCPのシーケンスが中断される現象を回避することができます。

DHCPパケットのMAC認証除外設定コマンドは以下となります。

```
(config-a-def)# mac-authentication ignore-dhcp
```

本機能を使用しない場合、図 3-7 のように、IPアドレス取得中にVLANが動的に割当たることによりDHCPのシーケンスが中断されることがあります。

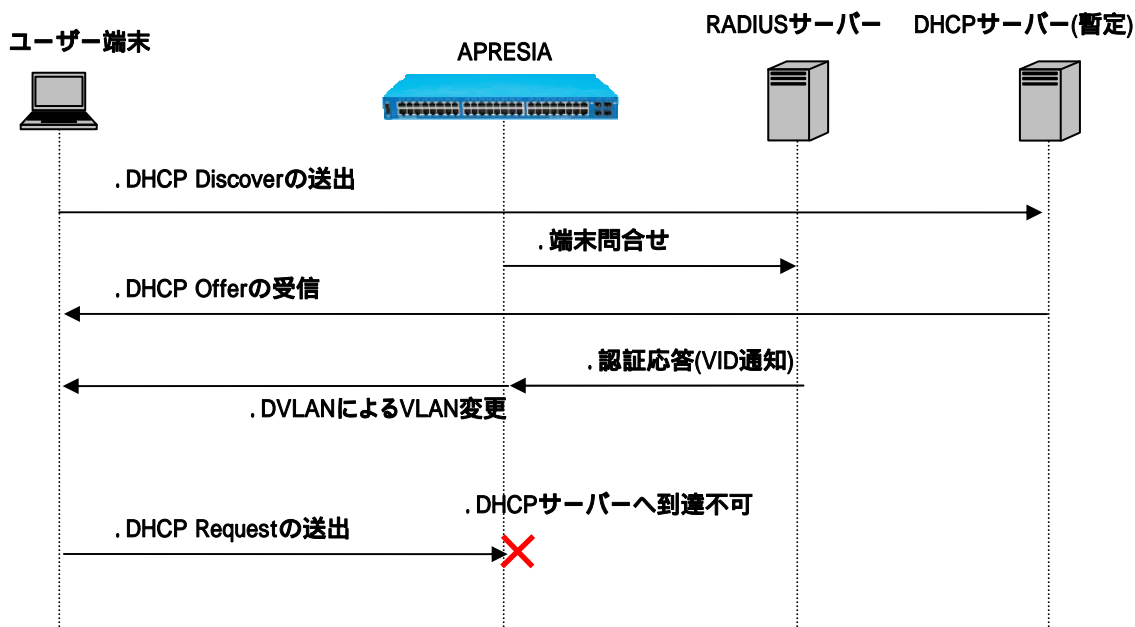


図 3-7 DHCPパケットをMAC認証対象とする場合の認証フロー

3.8 認証開始時のEAP-Request/Identityの抑制

サブリカントに対する EAP-Request/Identity の送信を抑制または送信間隔の変更が可能です。0 を指定した場合は自発的な EAP-Request/Identity を送信しません。

EAP-request/Identity 送信間隔の設定コマンドは以下となります。

```
(config-a-def)# dot1x port <PORTRANGE> timeout tx-period <SECS>
    . . . PORTRANGE                ポート番号
    . . . SECS                      ステータス保持時間 (0, 5-65535)
```

図 3-8 のように認証ポートに端末のMACアドレスが登録されても本コマンドにて、ステータス保持時間に 0 を指定した場合は、登録されたMACアドレスに対してEAP要求(EAP RequestID)を送信しません。

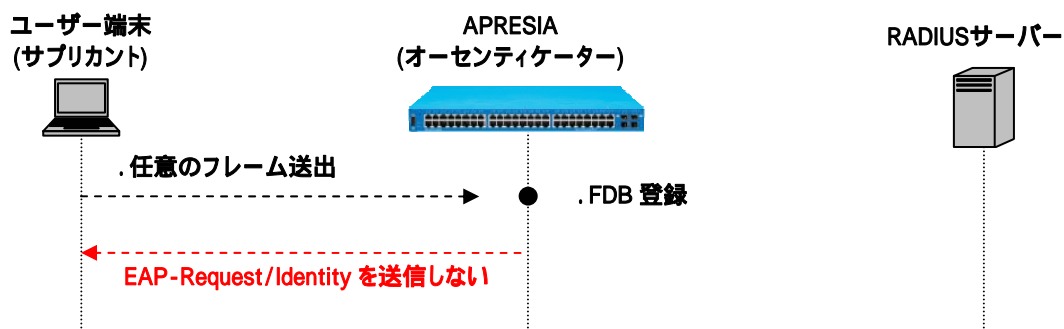


図 3-8 認証開始時の EAP-Request/Identity の抑制

! 本機能において 0 を設定していても、サブリカントからの EAPOL-Start に対しては、EAP-Request/Identity を送信します。

3.9 認証失敗時のステータス保持時間の変更

802.1Xでの認証処理が失敗したとき、ステータスを認証失敗状態として60秒間そのサブリカントに対して認証動作を行いません。そうすることで、不正な端末の認証失敗繰り返しによる負荷を軽減させています。本機能を使用することで、ステータス保持時間を変更することが可能です。0を指定した場合、認証失敗時のステータスを保持しません。

認証失敗時のステータス保持時間の設定コマンドは以下となります。

```
(config-a-def)# dot1x port <PORTRANGE> timeout quiet-period <SECS>
```

...	PORTRANGE	ポート番号
...	SECS	ステータス保持時間 (0, 5-65535)

図 3-9 のように認証失敗時からステータス保持時間が経過するまで、サブリカントからのEAPOL Startに回答せず、認証開始しません。その間、サブリカントに対するAPRESIAからのEAP-Request/Identityも送信されません。

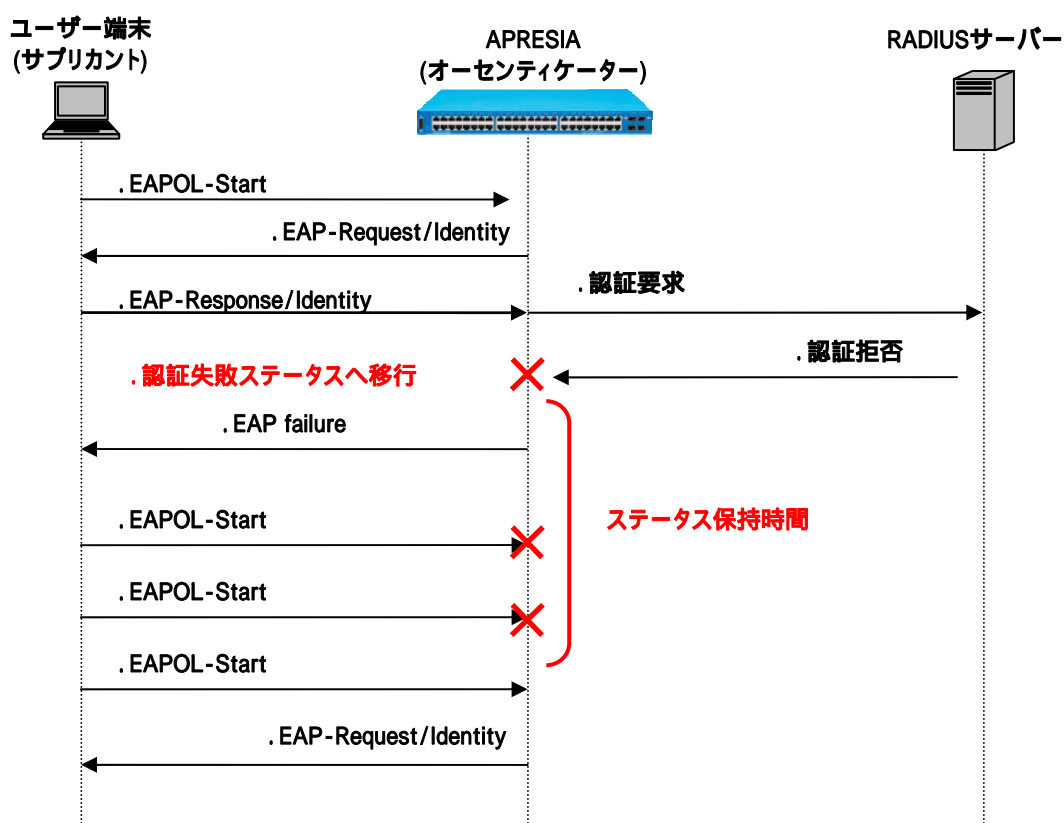


図 3-9 認証失敗ステータス保持

3.10 TTLフィルター

本機能を有効にすることにより、Web 認証において、指定した TTL 値の IP パケットのみ認証可能となります。これにより、ルーターの経由数に応じて接続を制限することができます。

TTL 値は最大 8 個指定可能です。

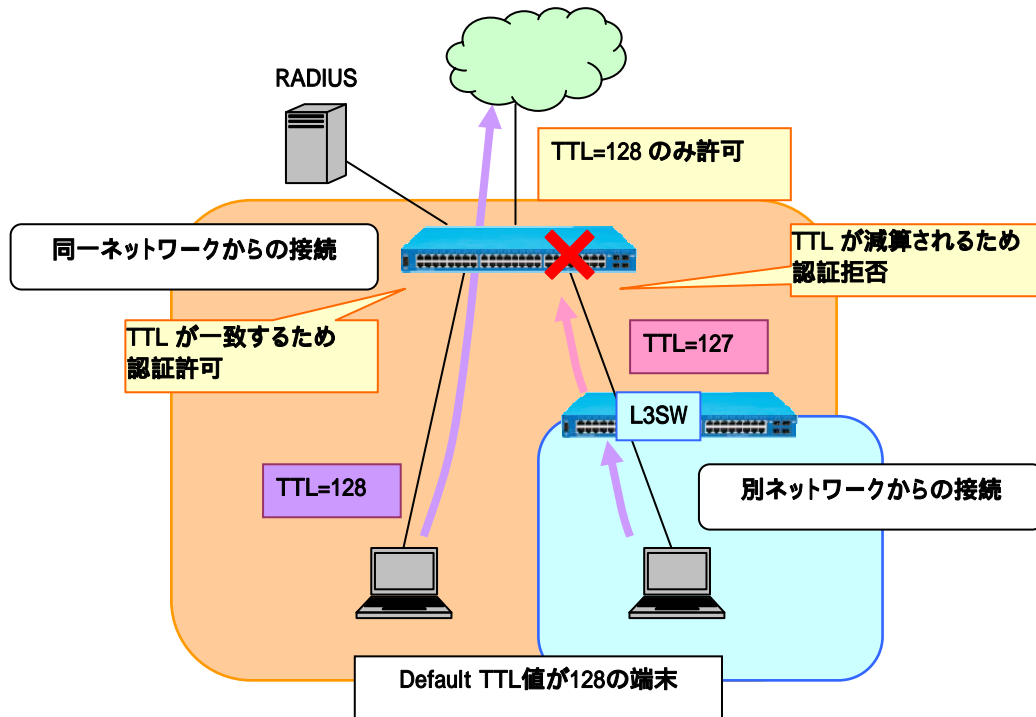


図 3-10 TTL フィルター

TTL フィルターの設定コマンドは以下となります。

```
(config-a-def)# web-authentication ttl <TTL> port <PORT>
(config-a-def)# web-authentication ttl <TTL> lag <LAG>
```

...	TTL	IP ヘッダの TTL (Time To Live) 値 <1-255>
...	PORT	TTL フィルターを設定するポート番号
...	LAG	TTL フィルターを設定する LAG 番号

TTL フィルター機能を使用したときの認証動作を図 3-11 に示します。

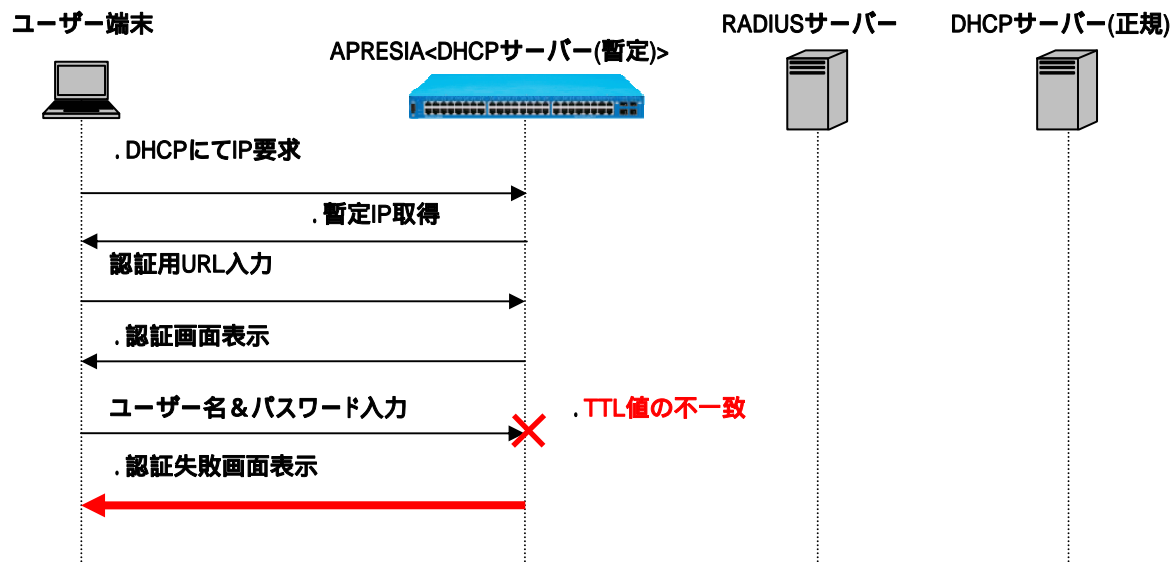


図 3-11 TTL 値不一致時の認証フロー

3.11 PINGログアウト

本機能を有効にすることにより、認証済み端末から、指定した宛先 IP アドレスまたは、指定した TTL 値の ICMP Request パケットを装置が受信すると、当該認証済み端末はログアウトされ未認証状態となります。

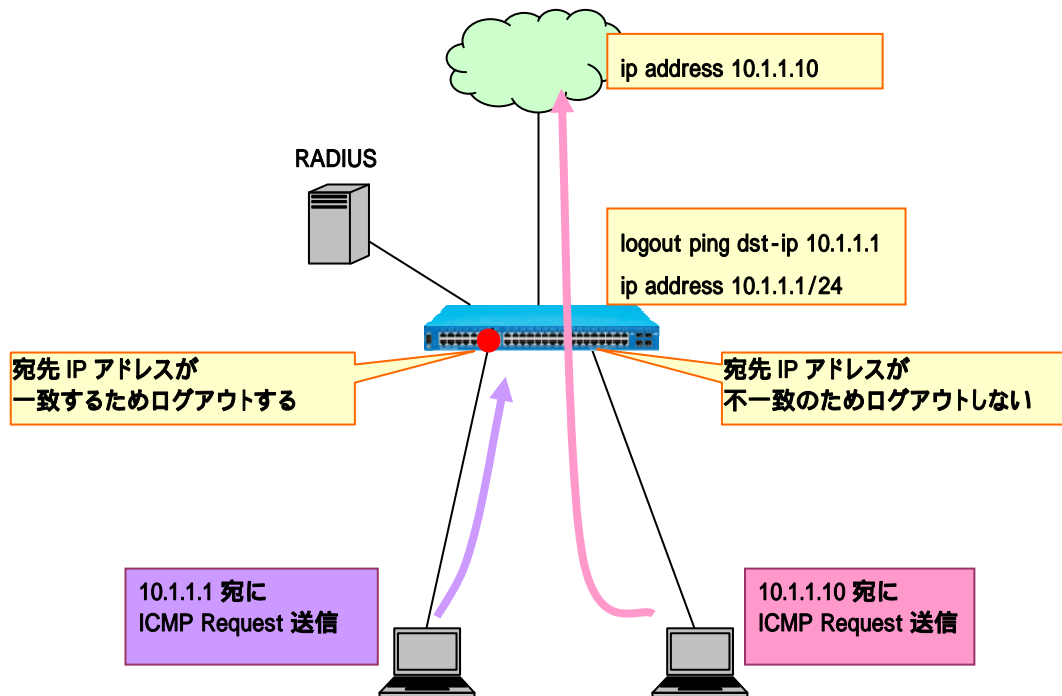


図 3-12 宛先 IP アドレス一致による PING ログアウト

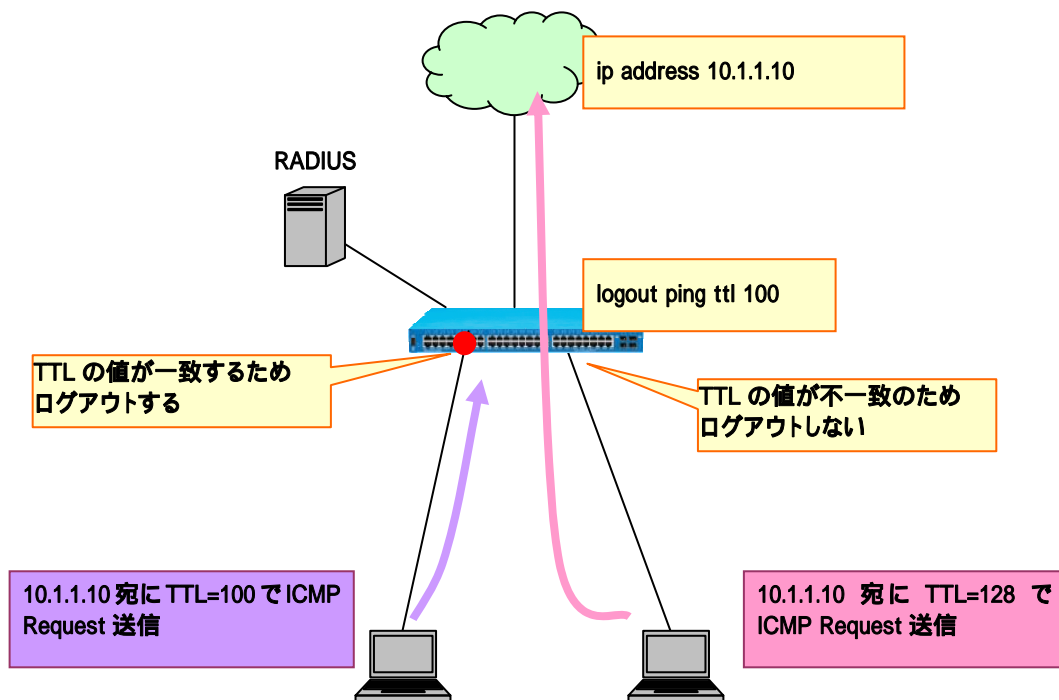


図 3-13 TTL 値一致による PING ログアウト

PING ログアウトの設定コマンドは以下となります。

```
(config-a-def)# logout ping dst-ip <IPADDR>
```

```
(config-a-def)# logout ping ttl <TTL>
```

```
    . . . IPADDR
```

宛先 IP アドレス

```
    . . . TTL
```

IP ヘッダの TTL(Time To Live) 値 <1-255>



本機能は Web 認証、ゲートウェイ認証でのみ有効です。



logout ping dst-ip と logout ping ttl コマンド併用時は、2つの条件を満たした場合に認証済み端末がログアウトされます。

4. 認証サーバー (RADIUSサーバー) の設定項目

認証サーバー (RADIUS サーバー) 側に必要となる設定項目について FreeRADIUS を例に説明します。
FreeRADIUS の設定ファイルは、標準では /usr/local/etc/raddb (もしくは /etc/raddb) 配下に置かれます。

主な設定ファイルは以下の通りです。

radiusd.conf

- RADIUS サーバーに関する各種設定ファイル (ログや Proxy 設定など)

clients.conf

- RADIUS クライアントの登録ファイル

users

- RADIUS サーバーのユーザーアカウント登録ファイル

dictionary

- VSA 属性の登録ファイル
 - ◇ /usr/local/share/freeradius 配下に置かれます



APRESIA がサポートする RADIUS 認証方式は PAP (Password Authentication Protocol) のみです。CHAP (Challenge Handshake Authentication Protocol) には対応していませんので設定の際は注意して下さい。

4.1 認証サーバーの設定項目(Web/MAC認証)

4.1.1 RADIUSクライアントの登録(clients.confファイルなど)

RADIUS クライアントとして APRESIA の管理アドレスを登録します。シークレットキーは APRESIA と RADIUS サーバーとで同じにしておく必要があります。

<clients.conf ファイルの設定例>

```
client 192.168.100.0/24 {
    secret          = apresia
    shortname       = APRESIA
}
```

4.1.2 ユーザー情報の登録(usersファイルなど)

認証サーバーとなる RADIUS サーバーのデータベースにユーザー名とパスワードを登録します(外部 LDAP サーバーなどの外部ユーザーデータベースと連携することも可能です)。

MAC ベース認証の場合、認証する端末の MAC アドレスを「ユーザー名」として登録します。例えば MAC アドレス「00:01:02:03:0a:0b」の端末を認証する場合、ユーザー名を「000102030a0b」と登録します。パスワードは、APRESIA に設定した MAC 認証用パスワードを登録します。

<users ファイルの設定例>

```
user1          Auth-Type = Local, Password = "user1"
               NA-Vlan-Id = 33
user2          Auth-Type = Local, Password = "user2", Calling-Station-Id = "000bd004a20d"
000bdbd64209   Auth-Type = Local, Password = "testing123"
               NA-Vlan-Id = 33
```

4.1.3 拡張設定(VLAN IDの設定)

認証成功後に動的に VLAN を変更する場合、認証成功時に APRESIA に引き渡す VLAN ID を格納する属性をあらかじめ登録しておく必要があります。

この属性値は一般にベンダ独自属性(VSA : Vendor Specific Attribute)と呼ばれます。

登録した属性を各々のユーザーにアクセス許可属性として登録し、そのユーザーからの認証要求の場合に、設定した VLAN ID を APRESIA に渡します。

➤ ベンダーID と属性番号を RADIUS サーバーに追加(dictionary ファイル等)

- ベンダーID 278
- ベンダー属性番号 192
- 属性の種類 整数(INTEGER 型)
- 属性値 ユーザー・端末にバインドする VLAN ID

<dictionary ファイルの設定例(編集)>

次行を既存の dictionary ファイルに追加します。

```
$INCLUDE dictionary.hcl
```

<dictionary.hcl の登録例(新規作成)>

dictionary ファイルで指定したファイル名で新規作成します。

VENDOR	Hitachi-Cable	278	
BEGIN-VENDOR	Hitachi-Cable		
ATTRIBUTE	NA-Vlan-Id	192	integer
END-VENDOR	Hitachi-Cable		



認証後の VLAN ID は「show vlan」コマンドでは確認できません。「show access-defender client」コマンドで確認して下さい。

4.2 認証サーバーの設定項目(802.1X)

認証サーバー(RADIUS サーバー)側に必要となる設定項目について FreeRADIUS を例に説明します。FreeRADIUS の設定ファイルは、標準では/usr/local/etc/raddb(もしくは/etc/raddb)配下に置かれます。

主な設定ファイルは以下の通りです。

radiusd.conf

- RADIUS サーバーに関する各種設定ファイル(ログや Proxy 設定など)

eap.conf

- EAP を使った認証(EAP-MD5、PEAP など)を設定するファイル

clients.conf

- RADIUS クライアントの登録ファイル

users

- その RADIUS サーバーのユーザーアカウント登録ファイル

4.2.1 EAPの設定(eap.confファイルなど)

どの EAP タイプで認証するかを指定します。

証明書(サーバー証明書、ルート CA 証明書)などの保管場所を指定します。

<eap.conf ファイルの設定例(抜粋)>

```
eap {
    default_eap_type = tls
    tls {
        private_key_password = apresia
        private_key_file = ${raddbdir}/certs/srv.pem
        certificate_file = ${raddbdir}/certs/srv-cert.pem
        CA_file = ${raddbdir}/certs/cacert.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
        fragment_size = 1024
    }
}
```

4.2.2 RADIUSクライアントの登録(clientsファイルなど)

RADIUS クライアントとして APRESIA の管理アドレスを登録します。シークレットキーは APRESIA と RADIUS サーバーとで同じにしておく必要があります。

<clients.conf ファイルの設定例>

```
client 192.168.100.0/24 {
    secret          = apresia
    shortname       = APRESIA
}
```

4.2.3 ユーザー情報の登録(usersファイルなど)

認証サーバーとなる RADIUS サーバーのデータベースにユーザー名とパスワードを登録します。

<users ファイルの設定例>

```
user01  Auth-Type := EAP, User-Password == "user01"
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 10
user02  Auth-Type := EAP, User-Password == "user02"
user03  Auth-Type := EAP, User-Password == "user03"
```

※ EAP-TLS で認証する場合、電子証明書で認証するためここでのパスワード登録は不要です。

4.2.4 拡張設定(VLAN IDの設定)

デフォルトモードを使用する場合、APRESIA に引き渡す VLAN ID を格納する属性をあらかじめ登録しておくことで認証成功時に設定した VLAN へ動的に変更されます。登録した属性を各々のユーザーにアクセス許可属性として登録し、そのユーザーからの認証要求の場合に、設定した VLAN ID を APRESIA に渡します。

各ユーザー(もしくはグループ)に登録する属性を表 4-1 に示します。

「Tunnel-Type」と「Tunnel-Medium-Type」属性に設定する値はそれぞれ「13(VLAN)」「6(IEEE802)」と固定値で、「Tunnel-Private-Group-ID」属性値のみ可変値となります。

表 4-1 動的 VLAN 変更で使用する RADIUS 属性

属性	属性値	設定値	備考
Tunnel-Type	使用するトンネリングプロトコル	13 (VLAN)	固定
Tunnel-Medium-Type	データ転送媒体のプロトコル	6 (IEEE802)	固定
Tunnel-Private-Group-ID	トンネルが属するグループ ID	割り当てる VID または VLAN 名称	可変

<users ファイルの設定例>

```
user01  Auth-Type := EAP, User-Password == "user01"
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 10
```

4.3 RADIUSサーバーの冗長化

RADIUS サーバーのデッドタイムを設定することにより、応答がない RADIUS サーバーには指定時間の間、問い合わせを行わないようにすることが可能です。

```
(config)# aaa radius deadtime <MIN>
                . . . MIN                デッド時間(1-1440) default なし
```

応答がない RADIUS サーバーには指定時間の間は問い合わせを行いません。



RADIUS サーバーの設定があり、ローカルデータベース認証や強制認証機能が設定されている場合、全ての RADIUS サーバーからの応答がタイムアウトした後にローカルデータベース認証や強制認証が実行されます。この認証順序を変更することはできません。

4.4 AccessDefenderで使用するRADIUS属性

AccessDefender 機能で APRESIA がサポートしている RADIUS 属性を示します。

表 4-2 AccessDefender で使用する RADIUS 属性(Web/MAC)

属性	属性値
User-Name	認証されるユーザー名
User-Password	パスワード
Callback-Number	コールバックナンバー
NAS-IP-Address	認証要求している RADIUS クライアントの IP アドレス
NAS-Port	クライアントが接続されている物理ポート番号
NAS-Identifier	認証された端末が属している VlanID
Calling-Station-Id	認証端末の MAC アドレス

表 4-3 AccessDefender で使用する RADIUS 属性(802.1X)

属性	属性値
User-Name	ログインユーザー名
Service-Type	提供するサービスタイプ(Framed-User(2)固定)
Framed-MTU	サブリカントと Authenticator 間の最大フレームサイズ(1452 固定)
NAS-IP-Address	認証要求している Authenticator の IP アドレス
NAS-Port	サブリカントが接続されている Authenticator の物理ポート番号
NAS-Port-Type	ユーザー認証に使用している物理ポートのタイプ(Ethernet(15)固定)
Calling-Station-Id	サブリカントの MAC アドレス
EAP-Message	EAP メッセージの送受信に使用
Message-Authenticator	RADIUS パケットの内容を保証するために使用
State	Authenticator と RADIUS サーバー間の State 情報の保持
Tunnel-Type	動的 VLAN 割り当て用応答属性(VLAN(13)に設定)
Tunnel-Medium-Type	動的 VLAN 割り当て用応答属性(IEEE802(6)に設定)
Tunnel-Private-Group-ID	動的 VLAN 割り当て用応答属性(割り当てる VID または VLAN 名称を設定)

4.5 RADIUSサーバー設定例(Windows 2000 server "IAS")(Web/MAC認証)

Windows 2000 server に付属しているインターネット認証サービス (IAS:Internet Authentication Service) を使用する場合の設定例を示します。

ここでは Active Directory のユーザー情報を用いて認証する場合の設定例を示します (Active Directory で IAS を承認してもらう必要があります)。

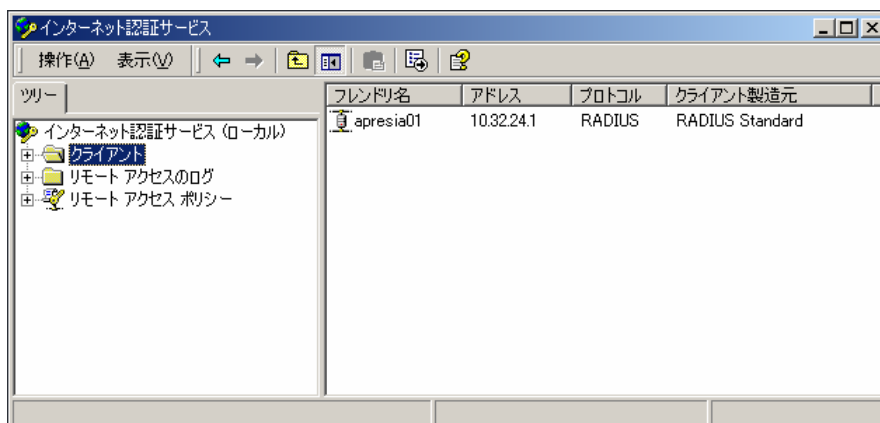


図 4-1 インターネット認証サービス (IAS) 設定画面

Windows Server 2003 のインターネット認証サービス (IAS) でも設定内容はほぼ同じです。

IAS が Active Directory のユーザーを認証できるようにするには、IAS を実行しているサーバーを Active Directory に登録し、ユーザーのダイアログプロパティをドメインから読み取る権限を与える必要があります。

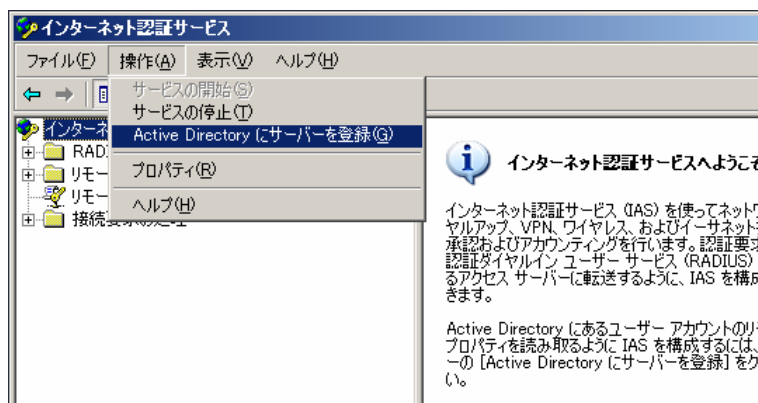


図 4-2 Active Directory にサーバーを登録

4.5.1 RADIUSクライアントの設定

IAS 設定画面より、RADIUS クライアントを登録していきます。シークレットキーは APRESIA と RADIUS サーバーで同じにしておく必要があります。

- ①. 新規に追加する場合は、RADIUS クライアントを新規作成します。
フレンドリ名は例えば APRESIA のシステム名などを入力し、「プロトコル」は RADIUS を選択します。

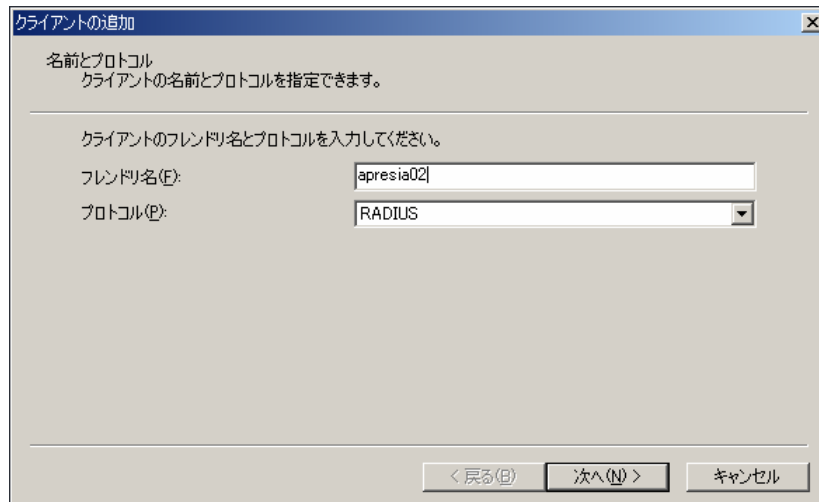


図 4-3 RADIUS クライアントの追加(1)

- ②. 「クライアントのアドレス」に、APRESIA の管理 IP アドレスを入力し、「共有シークレット」は APRESIA に設定したシークレットキーを入力して下さい。入力したら「完了」をクリックし追加終了です。

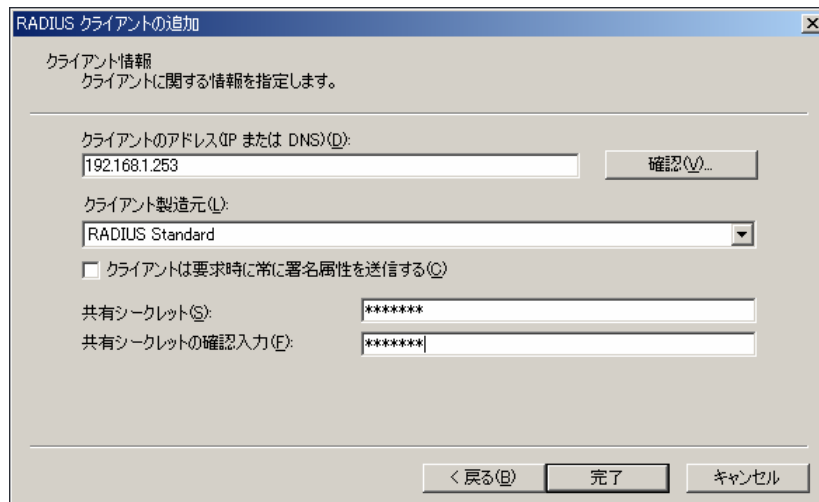


図 4-4 RADIUS クライアントの追加(2)

4.5.2 ユーザー・グループ情報の設定(リモートアクセスポリシーの設定)

ユーザー・グループ情報は予め Active Directory のユーザーDB に登録しておきます。このユーザー・グループ情報を用いてリモートアクセスポリシーを設定します。MAC アドレス認証オプションを使用する場合は、MAC アドレスをユーザー名として同様に登録します。このときのパスワードは、APRESIA に設定する MAC 認証用パスワードを設定します。

- ①. 新しいリモートアクセスポリシーを作成します。リモートアクセスポリシーの文字列上で右クリックし、「新しいリモートアクセスポリシー」を選択して下さい。表示されるウィンドウ内の「ポリシーのフレンド名」に適切な文字列を入力します。

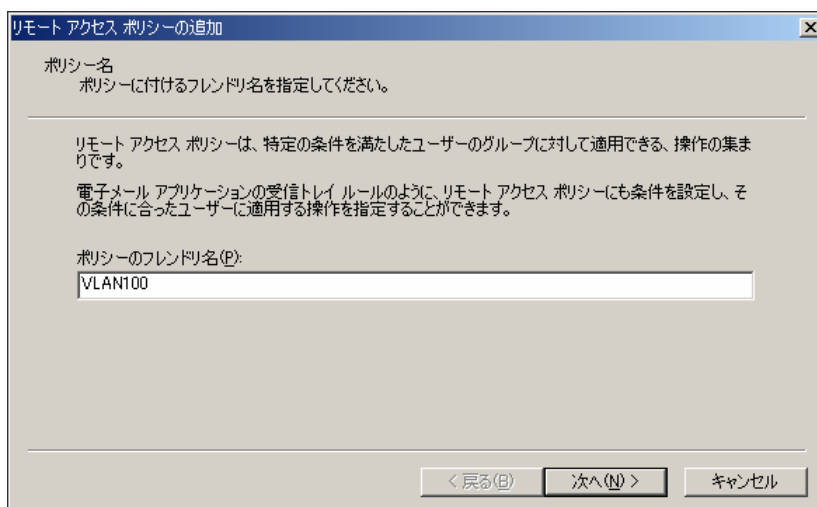


図 4-5 リモートアクセスポリシーの設定(1)

- ②. ポリシーの条件設定の画面が表示されるので、「追加」をクリックし、追加する属性を選択します。Active Directory の情報を使用して認証するため、属性の種類は「Windows-Groups」を選択します。

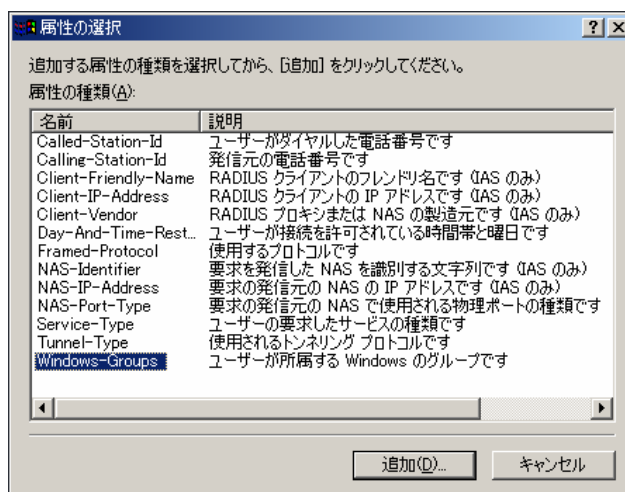


図 4-6 リモートアクセスポリシーの設定(2)

- ③. グループの追加画面が表示されるので、「追加」をクリックし、リモートアクセスポリシーを適用させたいグループを選択します。追加後「OK」をクリックします。

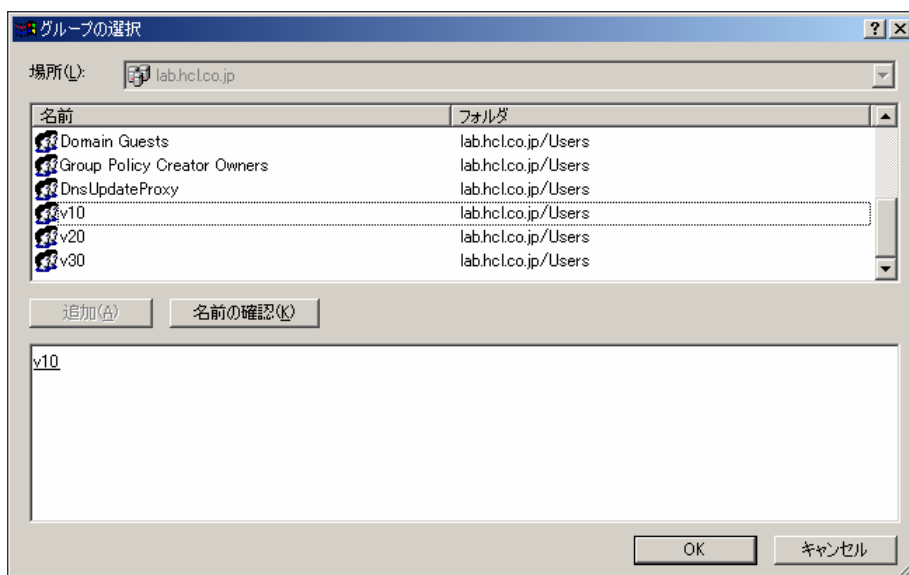


図 4-7 リモートアクセスポリシーの設定(3)

- ④. 追加したグループが表示されるので、追加情報に問題がなければ「次へ」をクリックします。

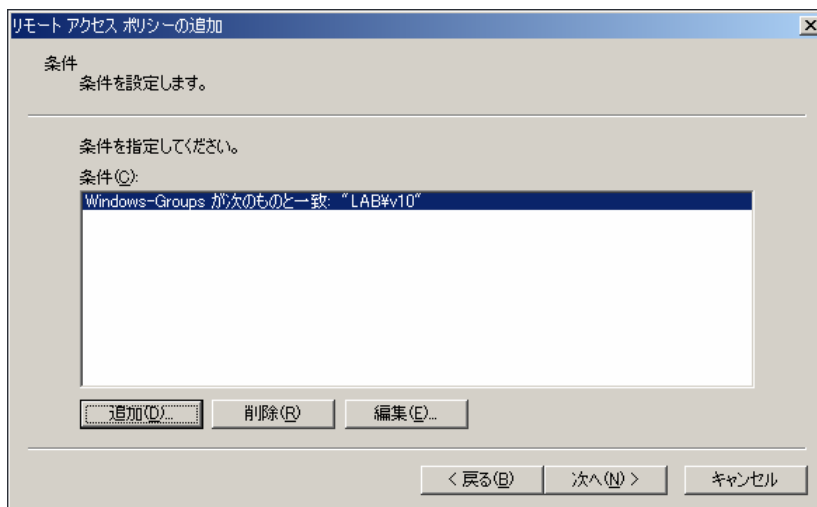


図 4-8 リモートアクセスポリシーの設定(4)

- ⑤. 「リモートアクセスに許可を与える」を選択し、「次へ」をクリックします。

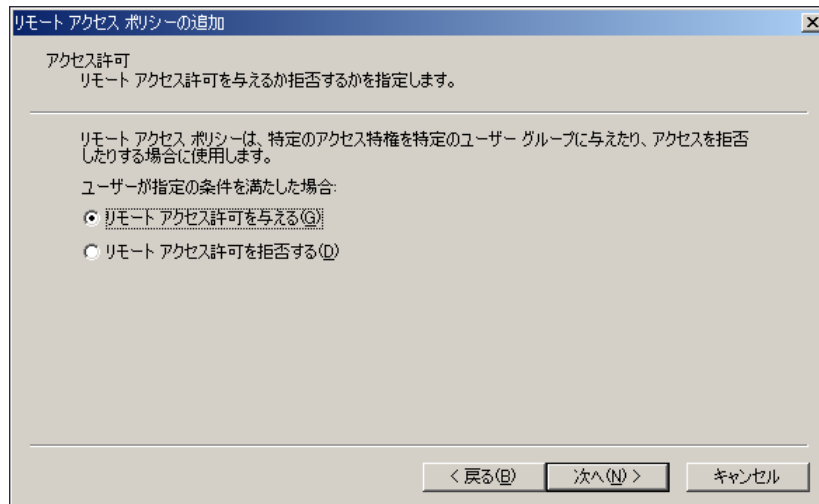


図 4-9 リモートアクセスポリシーの設定 (5)

- ⑥. プロファイルの編集を実行する必要があるため、「プロファイルの編集」をクリックします。

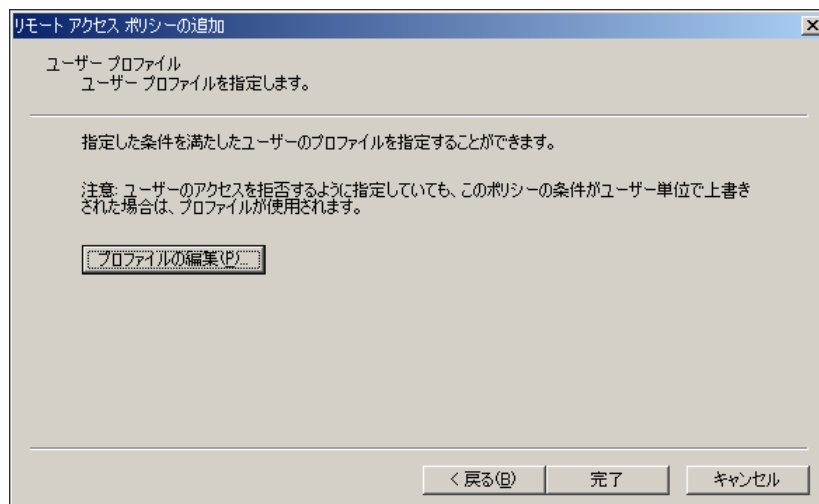


図 4-10 リモートアクセスポリシーの設定 (6)

- ⑦. 「認証」 タブを選択し、「暗号化されていない認証 (PAP、SPAP)」 にチェックします。

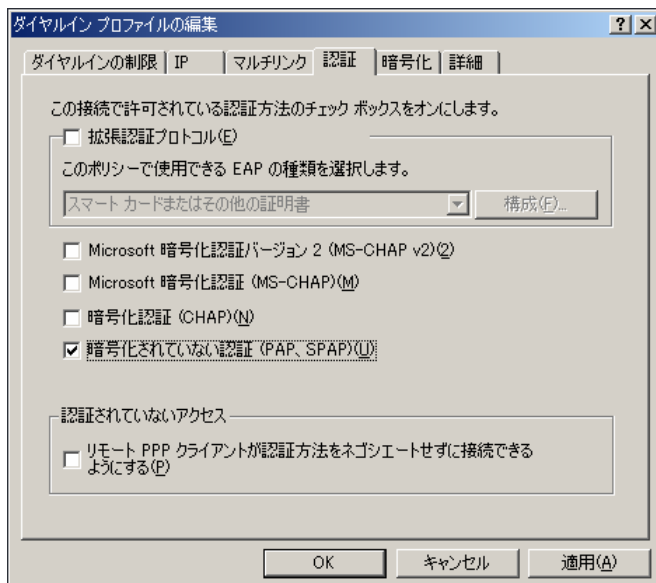


図 4-11 リモートアクセスポリシーの設定 (7)

- ⑧. 「OK」 をクリックすると 図 4-10 の画面に戻りますが、その前に下記ダイアログボックスが表示されます。必要に応じて「はい」か「いいえ」を選択します。図 4-10 の画面で「完了」をクリックしてリモートアクセスポリシー追加を終了します。

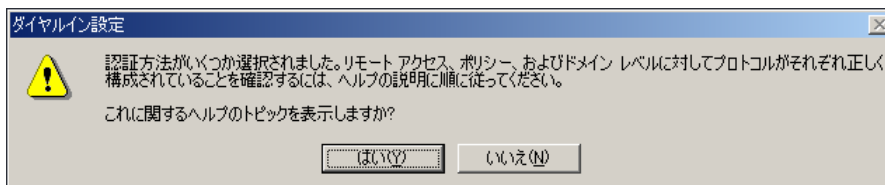


図 4-12 リモートアクセスポリシーの設定 (8)

4.5.3 VSAの設定(動的VLAN変更時のみ必要)

VLAN ID を格納するベンダ独自属性(VSA : Vendor-Specific Attribute)を設定します。VLAN を動的に変更したくない場合はこの設定は不要です。

- ①. 図 4-11 の画面上で「詳細」タブを選択し、「追加」をクリックします。

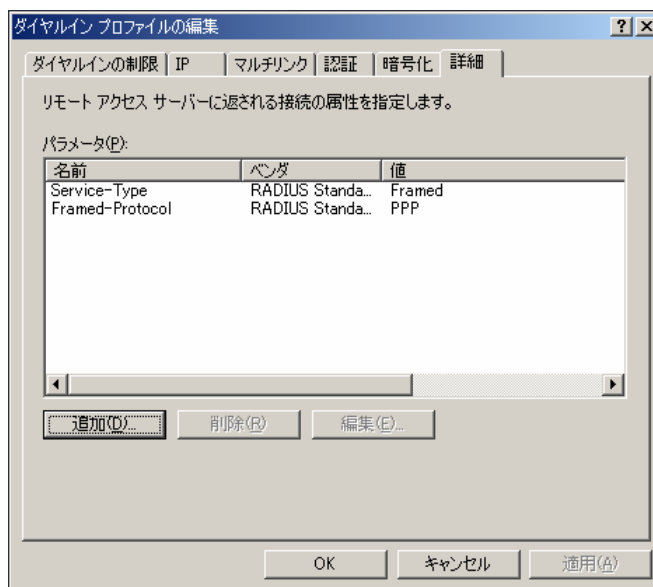


図 4-13 Vendor-Specific Attribute の設定(1)

- ②. 属性の追加画面で「Vendor-Specific」を選択し、「追加」をクリックします。

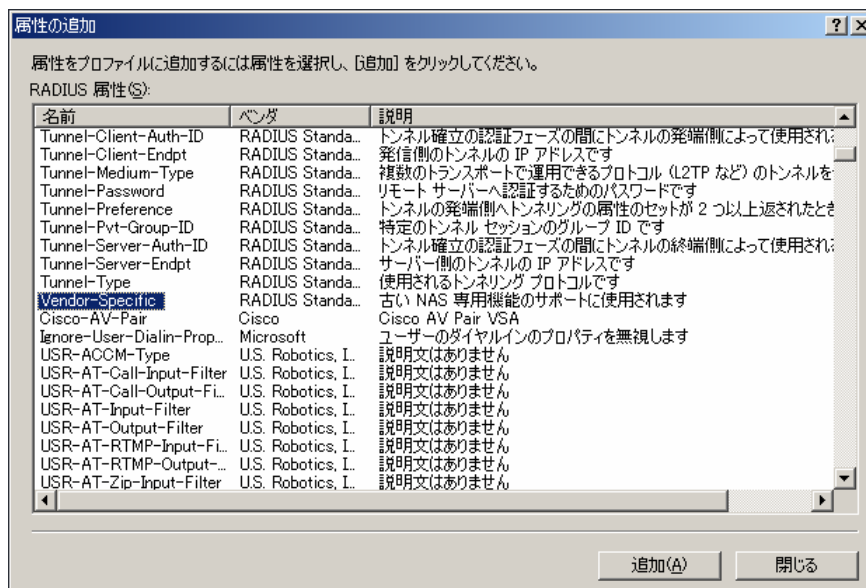


図 4-14 Vendor-Specific Attribute の設定(2)

- ③. 複数値の属性情報画面で「追加」をクリックします。

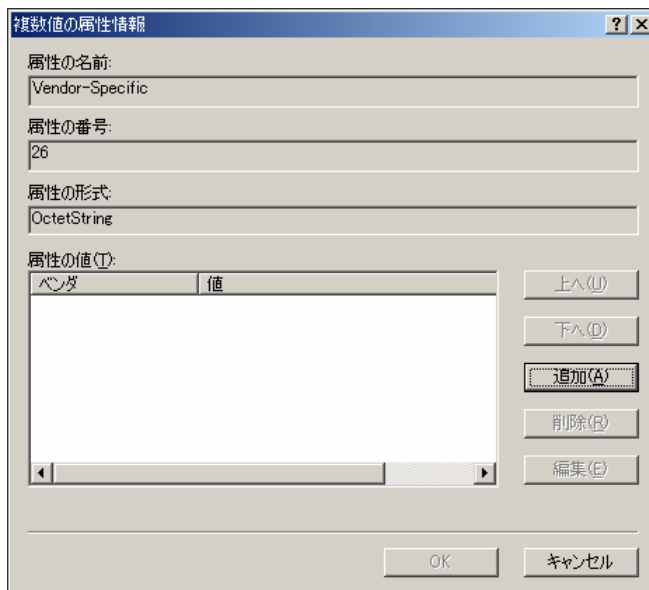


図 4-15 Vendor-Specific Attribute の設定 (3)

- ④. ベンダ特有の属性情報画面で「ベンダコードを入力する」欄に日立電線のベンダコード「278」を入力します。また、RADIUS RFC 仕様に準拠するかどうかの指定では「準拠する」を選択し、「属性の構成」をクリックします。

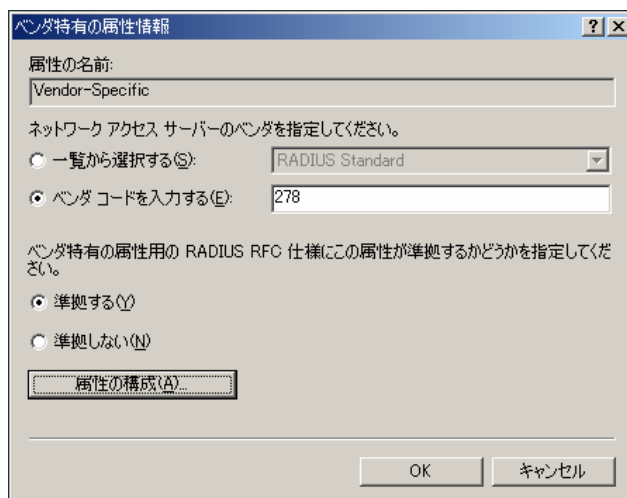
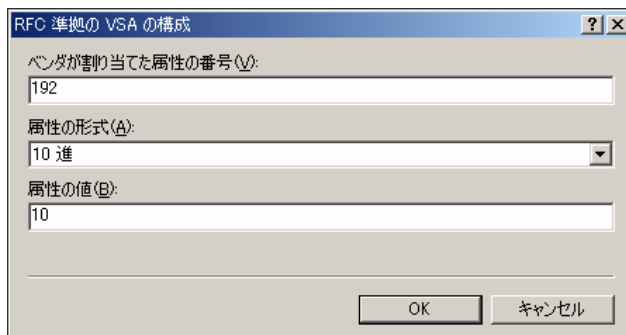


図 4-16 Vendor-Specific Attribute の設定 (4)

- ⑤. RFC 準拠の VSA の構成画面で、「ベンダが割り当てた属性の番号」欄に「192」を入力します。「属性の形式」は「10 進」を選択し、「属性の値」欄に APRESIA に引き渡す VLAN ID を入力します。



RFC 準拠の VSA の構成

ベンダが割り当てた属性の番号: 192

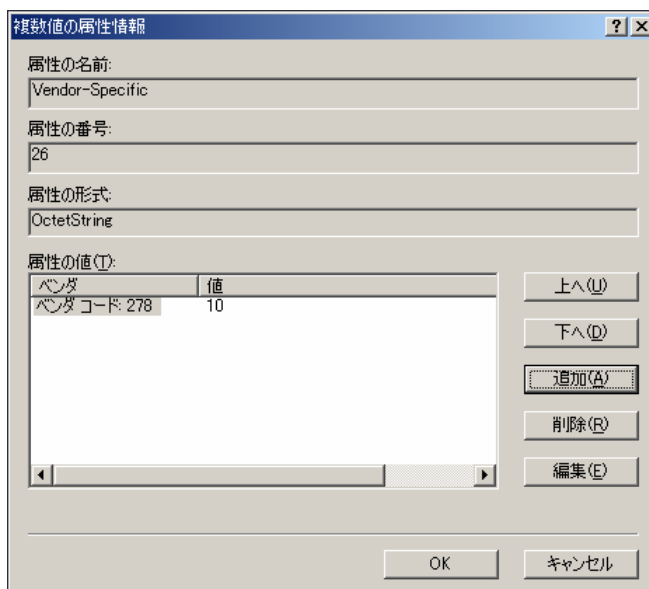
属性の形式(A): 10 進

属性の値(B): 10

OK キャンセル

図 4-17 Vendor-Specific Attribute の設定 (5)

- ⑥. 図 4-15 の画面において、設定した VSA の情報が表示されます。問題なければ「OK」をクリックします。



複数値の属性情報

属性の名前: Vendor-Specific

属性の番号: 26

属性の形式: OctetString

属性の値(I):

ベンダ	値
ベンダコード: 278	10

上へ(U) 下へ(D) 追加(A) 削除(R) 編集(E)

OK キャンセル

図 4-18 Vendor-Specific Attribute の設定 (6)

- ⑦. 図 4-13 の画面に戻ります。IAS標準で用意されているパラメータ (Service-Type、Framed-Protocol) は削除し、その後「OK」をクリックします。

5. 制限事項および注意事項

AccessDefender設定時における制限事項および注意事項などを表 5-1 に示します。

! 最新の情報は、随時発行される Field Notice を参照下さい。

表 5-1 制限事項および注意事項

No.	項目	制限事項および注意事項
1	AccessDefender	<ul style="list-style-type: none"> • AccessDefender 認証ポートで OSPF、RIP、スパニングツリープロトコル (STP/RSTP/MSTP) は併用できません。 • AccessDefender 認証ポートでポートセキュリティー、MMRP、MMRP2 aware、MMRP-Plus は併用できません。 • MAC 認証ポートで VRRP を併用する場合、VRRP パケットの仮想 MAC アドレスを認証させてください。 • 認証端末の所属する VLAN に IP アドレスを設定して使用する場合、認証状態を問わず、端末から本装置への通信 (telnet や SNMP) が可能です。 <ul style="list-style-type: none"> ➤ 通信を制限したい場合は、telnet 及び SNMP のアクセス制限機能により、アクセス可能な端末を制限して下さい。 • DHCP リレーが設定されている場合、端末の認証有無の状態にかかわらず、DHCP リレーが動作し、IP の取得が可能です。 • AccessDefender 機能による認証ポートにリンクアグリゲーション、ポートリダundantを設定する場合は、対象ポートの認証方法を全て同一にし、併せてリンクダウンログアウト無効 (logout linkdown port disable) とローミング (roaming port enable) を設定して下さい。 • 認証成功後にその認証ポートを他の認証モードに変更した場合、変更前の認証モードが有効のままとなります。 <ul style="list-style-type: none"> ➤ 認証モードを変更する場合は、認証端末がログアウト後に再認証するか、認証中の端末に対し再認証をして下さい。 • LLDP や LACP 機能による論理リンクダウン検知時には、認証端末はログアウト行われません。 • OSPF/RIP/IGMP/スパニングツリープロトコル (STP/RSTP/MSTP) 等のプロトコル制御用マルチキャストフレームは MAC 認証の対象となります。(これらフレームを送出する機器の MAC アドレスは、Discard 登録対象となります。) • IEEE802.1X 認証は、Supplicant から受信する EAPOL フレームの宛先 MAC アドレスが以下いずれか条件の場合のみ、STP との併用が可能です。 <ul style="list-style-type: none"> ➤ IEEE802.1X 認証用で使用される固有 MAC アドレス (00:40:66:33:1D:A9) ➤ 装置の自局 MAC アドレスの場合 • 複数認証モード (MAC 認証、Web 認証、802.1X) を組み合わせて認証する際、ログイン済み端末と MAC アドレスが重複した場合は新たな認証要求は失敗します。 • ログアウトせずに認証済み端末の接続ポートを変更する場合、ローミン

		<p>グ機能を使用してください。</p> <ul style="list-style-type: none"> • 認証済み端末数が最大認証数に達した状態でも、端末の Web 画面上に認証成功と表示される場合があります。 <ul style="list-style-type: none"> ➤ 最大認証数 1024 に対して、1021 端末が認証済みの状態で 5 端末が同時認証 • 動的な VLAN 割り当てと trunk 設定とが一致した場合、端末認証による VLAN(untag)設定が優先され、当該 VLAN における tag 中継は行われません。 • 同一ポートにおいて複数端末/複数 VLAN を動的に割り当てる場合、認証済み端末の IP アドレスを認証済み別セグメントに設定すると不要な arp フレームが転送されることがあります。 <ul style="list-style-type: none"> ➤ パケットフィルタ2 機能の arp-sender-ip を設定することにより、不要なフレームの転送を防止することが出来ます。 • 動的な VLAN 割り当てによる収容端末数は下記の通りです。なお、実装上の仕様により、下記に満たない場合でも登録出来ないことがあります。 <ul style="list-style-type: none"> ➤ Apresia4328 : 128 ➤ Apresia3424/4348/13000 シリーズ: 256 • AccessDefender 設定時に、MLD スヌーピング機能、MMRP/MMRP-Plus/MMRP2 aware 機能の 3 機能同時併用は出来ません。 • MAC 認証と動的な VLAN 割り当て使用時に暫定 VLAN 上に DHCP サーバーがある場合、mac-authentication ignore-dhcp の設定が必要です。 • Web/MAC 認証で行われる MAC 認証に対する動的な VLAN 変更の指定は無効となります。 • 認証成功後にその認証ポートの認証モードを変更しても、変更前の認証成功端末の通信設定は変わりません。変更した認証モードを認証端末へ反映させる場合には、認証成功端末がログアウトした後に再認証するか、認証成功端末に対し再認証をして下さい。
2	Web 認証	<ul style="list-style-type: none"> • Web 認証で用いるユーザーID、パスワードは 63 文字まで入力可能ですが、使用する RADIUS サーバーの仕様に従い、定義する必要があります。 • 同一ポートで他の認証(MAC 認証/IEEE802.1X)を併用して設定した場合は、他の認証で既にログインが完了している時は、Web 認証は行われません。 • ユーザーID とパスワードに使用できる文字は、ASCII コードの印字可能な文字です。但し、「¥」「”」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義して下さい。 • 本装置の DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります。 • Web 認証ポートに認証バイパスが設定されている場合、認証バイパス対象パケットの中継に対して認証 Web ページを表示できません。 • パケットフィルタ2 の認証バイパスを AccessDefender よりも大きいグループ番号で設定すると AccessDefender の Web 認証、及び、MAC 認証の discard 登録の設定が優先となり、認証バイパスは有効に動作しません。

		<ul style="list-style-type: none"> ➤ パケットフィルター2 の認証バイパス設定は、必ず AccessDefender のグループ番号より、小さい番号を設定して下さい。 • Web 認証ポートでは、未認証端末からの ARP フレームは、遮断されません。DHCP-スヌーピングポートと併用している場合は、DHCP-スヌーピングに登録されることで ARP フレームの中継が行われます。 • Web 認証、ゲートウェイ認証において同一の IP アドレスでログインした場合、最後にログインした認証方法が有効になります。 • 認証端末が DHCP サーバーより、IP アドレスを取得して Web 認証を行なう場合は、パケットフィルター2 を利用して、未認証端末から送信する DHCP フレームの通信を許可させる必要があります。 • Web 認証ログイン中に、ログアウトせずに接続ポートを移動した場合は、Web 認証でのみ再ログインが可能です。 • 装置の認証 Web サーバーと認証端末間の通信は、装置のルーティングテーブルに従って行われます(装置を L2 として使用している場合には、デフォルトゲートウェイの設定に従う)。このため認証 Web サーバーと認証端末間の通信は、上位ルータを経由して行われる場合があります。 <ul style="list-style-type: none"> ➤ 装置を L2 として使用し、自局 IP アドレスと認証端末 IP アドレスが異なるサブネットとなる場合等、上位ルータを経由します。 • ゲートウェイ認証でログインした端末が、ログイン後に端末の IP アドレスを変更すると通信不可となります。 • ゲートウェイ認証において、動的な VLAN 変更を指定しても無効となります。(動的な VLAN 変更は行われません) • ゲートウェイ認証と、Web 認証(gateway オプションなし)、Web/MAC 認証、MAC 認証、IEEE802.1X、IEEE802.1X/MAC 認証、DHCP スヌーピング、ポートセキュリティーは同一ポートに設定できません。 • ゲートウェイ認証は Apressia13000 シリーズでのみ有効です。 • リンクアグリゲーショングループ内のメンバーポートは Web 認証または Web/MAC 認証に方式を統一して設定してください。 • web-authentication http-port コマンドによる認証 Web サーバーの TCP ポート番号に 23(telnet プロトコル)、及び、web-authentication https-port コマンド、または、web-authentication redirect proxy-port コマンドで指定した番号は指定出来ません。 • web-authentication https-port コマンドによる認証 Web サーバーの TCP ポート番号に 23(telnet プロトコル)、及び、web-authentication http-port コマンド、または、web-authentication redirect proxy-port コマンドで指定した番号は指定出来ません。 • 不正な秘密鍵と証明書が装置にダウンロードされている状態では、Web 認証動作(SSL)は保証されません。 • 認証用 Web サーバーの IP アドレスに、装置の IP アドレスと同一のネットワークアドレスを持つ IP アドレスは設定しないで下さい。 • Web/MAC 認証における MAC 認証用パスワードに使用できる文字は、ASCII コードの印字可能な文字です。但し、「¥」「”」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義して下さい。 • 設定した Web/MAC 認証における MAC 認証用パスワードは、“show
--	--	--

		<p>running-config” コマンド、“show flash-config” コマンドにおいては暗号化されて表示されます。</p> <ul style="list-style-type: none"> Ver. 7.19 以前から 7.20 以降へ VerUp した場合、Web/MAC 認証ポートには Web/MAC 認証を有効にするポート指定 (web-authentication port mac-authentication コマンド)が必要です。
3	MAC 認証	<ul style="list-style-type: none"> discard で登録できる MAC アドレスは、100 個までです。 認証時に認証端末毎に動的に VLAN を割り当てる場合、認証前の VLAN 用の DHCP サーバーは、認証スイッチの DHCP サーバーをご使用下さい。認証スイッチ以外の DHCP サーバーを使用した場合、認証後の VLAN の IP アドレスに切り替わらないことがあります(認証後の VLAN の DHCP サーバーにつきましては、認証スイッチの DHCP サーバーである必要はありません)。 DHCP での IP アドレス取得中に認証が成功し、VLAN が IP アドレス取得よりも先に動的に割当たった場合、DHCP のシーケンスが途中で止まり IP アドレスが取得出来なくなります。その際は、mac-authentication ignore-dhcp コマンドを使用してください。 認証フレームとして VLAN タグつきフレームを受信した場合、認証端末の VLAN ID は VLAN タグの VLAN ID になります。 MAC 認証ポートに認証バイパスを設定した場合でも、MAC 認証が動作しますが、認証結果(成功、拒否(discard 状態)、失敗)に係わらず、認証バイパスの設定が優先されます。 MAC 認証ログイン中に、ログアウトせずに接続ポートを移動した場合は、MAC 認証でのみ再ログインが可能です。 パスワードに使用できる文字は、ASCII コードの印字可能な文字です。但し、「¥」「”」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義して下さい。 設定したパスワードは、“show running-config” コマンド、“show flash-config” コマンドにおいては暗号化されて表示されます。
4	802.1X	<ul style="list-style-type: none"> STP と併用する場合、サブリカントから受信する EAPOL フレームの宛先 MAC アドレスが特定のユニキャストアドレス、(00-40-66-33-1D-A9)または、装置の自局 MAC アドレスの場合のみ、動作が保証されます。 MAC 認証と併用する場合、IEEE802.1X にて認証済みの端末が discard 登録されている場合がありますが、認証済み端末は通信可能です。当該端末は show access-defender client で discard として表示が残っていますが、discard 登録は 300 秒経過後に自動的に解除されます。 IEEE802.1X/MAC 認証における MAC 認証用パスワードに使用できる文字は、ASCII コードの印字可能な文字です。但し、「¥」「”」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義してください。 設定した IEEE802.1X/MAC 認証における MAC 認証用パスワードは、“show running-config” コマンド、“show flash-config” コマンドにおいては暗号化されて表示されます。 IEEE802.1X/MAC 認証を有効にした場合、dot1x port で指定した全ポートで IEEE802.1X/MAC 認証が有効になります。

5	DHCP スヌーピング	<ul style="list-style-type: none"> • DHCP スヌーピング機能を有効にするには、packet-filter2 max-rule を設定する必要があります。 • DHCP リレー機能を同時に有効にすることは出来ません。 • PERMIT モード時に他の認証を併用している時は、他の認証状態に関係なく通信が可能です。 • DHCP スヌーピング機能を有効にすると、装置全体で DHCP のパケットが中継出来るようになります。ただし、internal-dhcp-vlan で指定した VLAN では中継されません。 • DHCP スヌーピング機能では、linkdown による logout を行いません。linkdown 後でもリース期間満了になるまで登録が継続されます。 • 装置を認証スイッチとレイヤー3 スイッチとして併用する場合、DHCP スヌーピング機能と他の認証(MAC 認証、Web 認証、802.1X)を同一ポートで併用できません。 • 同一 VLAN インターフェースにて DHCP サーバーと DHCP スヌーピング機能を併用する場合、dhcp-snooping internal-dhcp-vlan を設定する必要があります。 • DHCP スヌーピング有効時は DHCP パケットをパケットフィルター2の認証バイパス対象に設定しないでください。 • mac-authentication モードと DHCP サーバー機能は併用できません。 • PERMIT モード中にタイマーを再設定した場合、それまでの経過時間はリセットされます。 • dhcp-snooping static-entry port コマンドで登録された静的フィルタは自動では削除されません。フィルタを削除する場合、手動で削除する必要があります。 • 各ポートで登録可能な静的フィルタの上限数は(クライアント制限数-動的に登録されているフィルタ数)となります。 • 既に登録されている動的フィルタと同じポート、同じ IP アドレスの静的フィルタを登録した場合、その動的フィルタに対して静的フィルタが上書きされます。 • DHCP スヌーピングの Static エントリーを設定している場合、他の認証を有効にした後に DHCP スヌーピングを有効(dhcp-snooping enable)にして下さい。
6	認証ローミング	<ul style="list-style-type: none"> • 認証ローミングは、同一装置内の roaming port enable、同一の認証方式が設定されているポート間でのみ有効です。 • AccessDefender のローミング機能は、NA 機能のローミング機能と以下の点で異なるためご注意ください。 <ul style="list-style-type: none"> ➤ ローミング前のポートのリンクダウンによるログアウトが発生します。このログアウトを発生させたくない場合には、ローミング前のポートに logout linkdown port disable コマンドを設定して下さい。 ➤ ローミングにより接続ポートを変更しても、show access-defender client で表示されるポート番号は、ログイン時のポート番号が表示されます(ローミング機能が有効なポートにはポート番号の先頭に*が付きます)。 • 設定変更により、ローミングポートの設定が変わっても変更以前にログ

		<p>インした端末はログアウトせず、設定変更以前のローミングポートの設定状態でログインしたままとなります。設定の変更が反映されるのは、変更後にログインした端末のみとなります。</p>
7	RADIUS	<ul style="list-style-type: none"> secret key に使用できる文字は、ASCII コードの印字可能な文字です。但し、「¥」「”」は RADIUS サーバーでは制御文字として扱われます。これら文字を使用する場合には、RADIUS サーバーの仕様に従い、定義して下さい。 設定した secret key は、“show running-config” コマンド、“show flash-config” コマンドにおいては暗号化されて表示されます。 強制認証はセキュリティ上の問題となる可能性がありますので、十分検討の上使用して下さい。設定されていない INDEX を指定した場合は、ERROR 通知を行い設定はされません。 IEEE802.1X 認証の冗長構成では、aaa radius deadtime の併用を推奨します。 認証方法として RADIUS サーバーと強制認証を選択している場合、RADIUS サーバーでのユーザー名またはパスワード誤りによる認証失敗時は強制認証へ移行しません。RADIUS サーバーがタイムアウトした際は強制認証へ移行します。
8	SSL	<ul style="list-style-type: none"> ssl gencsr rsakey コマンドでは “?” は入力できません。 <ul style="list-style-type: none"> Country についてはローマ字アルファベットの大文字 (‘A’ ~ ‘Z’) のみ入力可能です。 証明書や秘密鍵のファイル名として、& ; ` ¥ % * ? ^ < ^ () [] { } \$ の各文字は使用出来ません。 証明書や秘密鍵のファイル名として、文字列 . / は使用出来ません。 <ul style="list-style-type: none"> / はディレクトリ指定として扱われます。 秘密鍵が暗号化されている場合、パスフレーズを入力する旨メッセージが表示されます。秘密鍵を暗号化時に使用したパスフレーズを入力して下さい。なお、暗号化の方式については DES、3DES にのみ対応します。 正しくない秘密鍵をダウンロードした場合、パスフレーズの入力が求められますが、復号化に失敗します。このため有効な秘密鍵となりません。 中間証明書には、証明書チェーン (第三の証明書、第二の証明書を連結したもの) をお使い下さい。 web-authentication https-port が設定されている場合、証明書、秘密鍵はダウンロードできません。 <ul style="list-style-type: none"> ダウンロードする場合は一旦 web-authentication https-port の設定を削除してください。
9	認証ページリダイレクト	<ul style="list-style-type: none"> 本機能を有効にする場合、web-authentication redirect http、web-authentication redirect https、web-authentication redirect proxy-port コマンドでリダイレクトを行なう対象プロトコルを設定する必要があります。 外部の認証 Web ページを参照せず、リダイレクト先に本装置の認証 Web ページを表示させる場合、本装置の URL (認証 Web サーバーの IP アドレスと TCP ポート番号) を指定する必要があります。 HTTP リダイレクトを設定する場合、リダイレクト先 URL のポート番号を 80 以外に設定してください。

		<ul style="list-style-type: none"> • HTTPS リダイレクトを設定する場合、リダイレクト先 URL のポート番号を 443 以外に設定してください。 • 本機能を有効にする場合、web-authentication ip コマンドで、任意の IP アドレスをあらかじめ設定しておく必要があります。 • Web 認証端末の Gateway(next hop)アドレスを認証装置の IP アドレスに設定した状態では使用出来ません。 • 認証 Web サーバーの TCP ポート(web-authentication http-port、web-authentication https-port)は、ネットワーク上の Web サーバーと必ず異なるポート番号を設定して下さい。 • 本機能で HTTPS がリダイレクトされた場合、ブラウザーに「証明書エラー」、「セキュリティの警告」、「信頼できない接続」などセキュリティに関わる警告が表示されます。これは HTTPS の仕様によるもので装置の異常ではありません。装置に正式な証明書をダウンロード、またはブラウザーに CA 証明書を追加した場合でも、警告は表示されます。 • プロキシ宛をリダイレクト対象とした場合、認証端末が HTTPS プロトコルを使用した場合、リダイレクトはされません。 • プロキシポート番号に 23(telnet プロトコル)、及び、web-authentication http-port コマンド、または、web-authentication https-port コマンドで指定した番号は指定出来ません。
10	packet-filter2	<ul style="list-style-type: none"> • Web 認証、MAC 認証、802.1X、DHCP スヌーピングのうちいずれか1つが有効である(enable に設定)場合、packet-filter2 max-rule コマンドや packet-filter2 group コマンドは使用出来ません。 • 指定したルール数を確保するのに必要なグループが、連番で予約出来ない場合は、packet-filter2 max-rule コマンドは設定出来ません。 • 装置 1 台あたりの最大認証端末数はパケットフィルタ2 の最大ルール数となります。(DHCP スヌーピング機能を除く)。 <ul style="list-style-type: none"> ➤ 端末の認証が同時に行われた場合の性能を保証するものではありません。 • DHCP スヌーピング機能では、201 端末目以降(Apresia13000-24GX は 401 端末目以降)は 1 端末につき 2 ルール使用します。 • 本装置再起動後は構成情報の記載順にパケットフィルタ2 のグループが確保されます。他機能で確保済みのグループを本コマンドで指定した場合、AccessDefender 機能は有効になりません。
11	ローカル認証	<ul style="list-style-type: none"> • ローカルデータベースの最大ファイルサイズは 245600 バイトです。 • ローカルデータベースのファイルにおいて、改行のみの行がある場合、ダウンロード出来ません。ローカルデータベースのファイル中に改行のみの行を含めないで下さい。 • MAC ベース認証の場合、MAC アドレス(16 進文字列、区切り文字無しの 16 文字)を、ユーザーID として登録して下さい。 <ul style="list-style-type: none"> ➤ アルファベットは小文字(a-f)で記述する必要があります。 • ファイル名として、& ; ` ¥ * ? ~ < ^ () [] { } \$ の各文字は使用出来ません。 • ファイル名として、文字列 ./ / は使用出来ません。 <ul style="list-style-type: none"> ➤ / はディレクトリ指定として扱われます。 • 改行コードは、“¥n” を使用して下さい。“¥r¥n” は使用出来ません。 • ローカルデータベースの最終行に改行(改行コード“¥n”)を入れてくだ

		<p>さい。</p> <ul style="list-style-type: none"> 重複したユーザーIDのエントリが含まれるローカルデータベースは本装置に保存できません。 Apresia4300 シリーズにおいて、7.11.04 以前のファームウェアでダウンロードしたlocal-dbは、ファームウェアの更新後に使用出来なくなります。ファームウェアの更新後に、tftpサーバーからlocal-dbを再度ダウンロードして下さい。更新手順については 3.2.3ローカルデータベースの登録(ダウンロード)をご参考下さい。
12	show コマンド	<ul style="list-style-type: none"> 動的に VLAN が割り当てられた認証端末から、動的な VLAN が割り当てられていないユーザー名で再ログインした場合、再ログイン前の VLAN ID が表示されます。 ユーザー名は 63 文字まで表示されますが、一行に収まらない場合は折り返して表示されます。 show access-defender client コマンドの Aging 時間は、5 秒毎に更新されます。 show access-defender dhcp-snooping mode-status コマンドの remaining time は 10 秒毎に更新されます。 show access-defender packet-filter2 rule-statistics コマンド及び show access-defender port-configuration コマンドにおいて gateway は、Apresia13000 シリーズでのみ表示されます。

5.1 バージョンアップ時の注意点

Apresia4300 シリーズにおいて、Ver7. 11. 04 以前から Ver7. 12. 01 以降へバージョンアップする際、装置のローカルデータベースは引き継がれません。

ファームのバージョンアップを行う際には、下記手順で行ってください。

- ① ローカルデータベースを” copy aaa-local-db tftp” コマンドで TFTP サーバーにアップロード
- ② ファームをバージョンアップ
- ③ 新しいファームで起動
- ④ ① のローカルデータベースを” copy tftp aaa-local-db” コマンドで機器へダウンロード

5.2 動的VLAN割り当て使用時の注意点

5.2.1 動的VLAN割り当て時のログイン失敗

認証成功後に動的に VLAN を割り当てる場合、設定した上限登録数に満たない場合でもログインに成功しないことがあります。

MAC認証/Web認証/802. 1Xの認証方式で、認証成功後に動的にVLANを割り当てる場合における端末収容数は下記の通りとなりますが、収容数が下記を超えていない状態でも表 5-2 に示す平均台数でログインに失敗する可能性があります。

事象が発生した場合は、ログイン失敗した端末を別のスイッチに接続して下さい。

本事象は動的 VLAN 変更時のみ発生するため、動的に VLAN を変更する構成の場合にはログイン失敗台数を見込んだ収容端末数で設計することをお勧めします。

動的 VLAN 割当時の端末収容数(動的 VLAN 割り当てを使用しない端末はこの収容数には含みません)

- Apresia4328 シリーズ 128 端末
- Apresia3400/4348/5400/13000 シリーズ 256 端末

表 5-2 動的 VLAN 割り当てにおける平均ログイン失敗端末台数

	4328 シリーズ	3400/4348/5400/13000 シリーズ
32 端末あたり	0.001 台	0.001 台
64 端末あたり	0.020 台	0.001 台
128 端末あたり	0.529 台	0.042 台
256 端末あたり	—	1.066 台

※各端末数において任意の端末をランダム抽出しログインさせる動作を 1 回とし、これを 10,000 回試行した場合における 1 回あたりの発生端末数を表しています。

※本事象によるログイン失敗時に表示されるログは以下となります。

```
<process:warning> A-Def : <web|mac|dot1x> : vlan assignment failed :uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> new vid=<vid>
```


5.2.2 単一のアクセスポート配下に複数端末を接続する際の注意点

単一のアクセスポート配下に複数端末を接続した場合、セグメント(VLAN ID)と IP アドレスが不一致状態であるパケットを転送してしまう場合があります。

図 5-1 に示した構成例において、端末 1 および端末 2 が Web 認証後、DHCP サーバーから正規 IP アドレスを取得した状態で端末 2 がログアウトすると、端末 2 は正規 IP アドレスが残存した状態で暫定 VLAN である temp にアサインされます。この状態で認証バイパスターゲットから端末 2 へ通信を行うと、L3 スイッチは VLAN ID:10 の tag パケットを認証スイッチへ転送しますが、認証スイッチはアクセスポートかつ VLAN ID:10 の端末 1 が所属している認証ポートへパケットを転送してしまい、端末 2 がセグメント(VLAN ID)と IP アドレスが不一致状態であるにもかかわらず通信が可能です。

セグメント(VLAN ID)と IP アドレスが不一致状態であるパケットをパケットフィルタ 2 により破棄(deny)することによって、このような動作を回避できます。この際、パケットフィルタ 2 の deny 設定は必ず認証バイパスのグループ番号より小さい番号を設定してください。

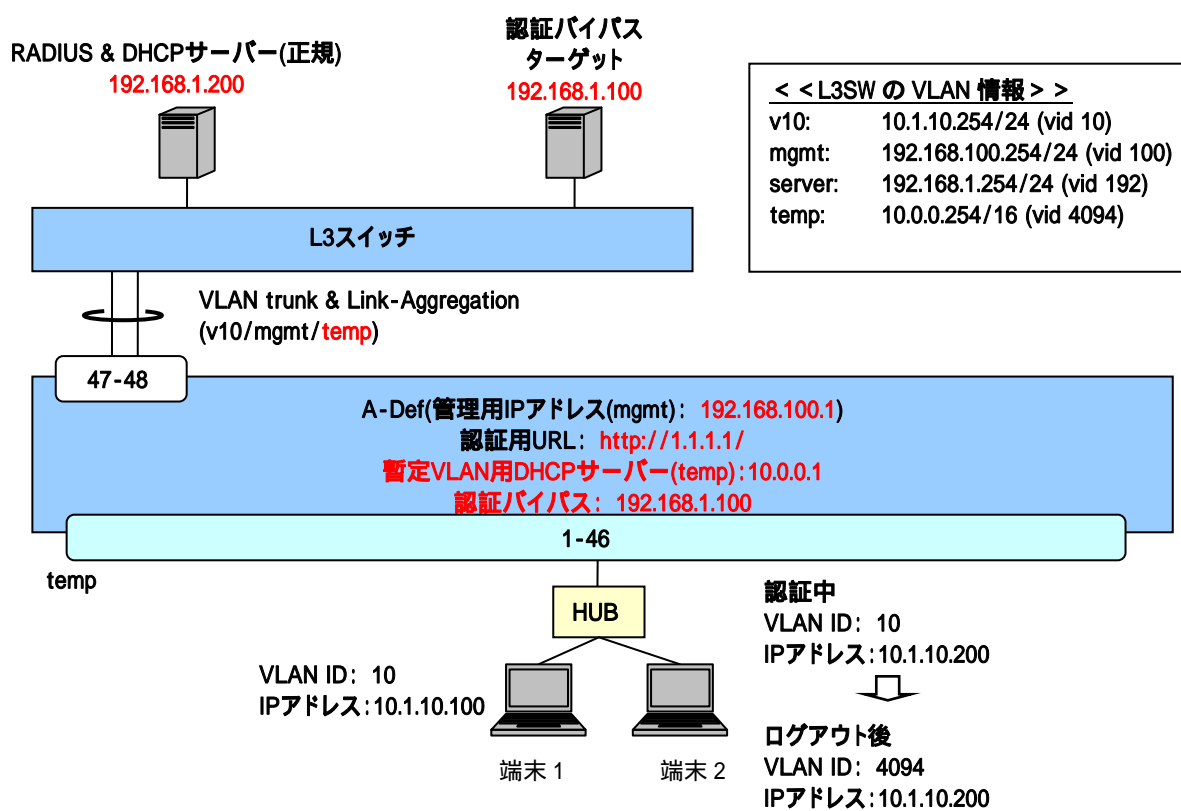


図 5-1 別 VLAN ID の IP アドレスを取得してしまう構成例

5.3 Windows標準サブリカントにおける 802.1X認証の問題点

802.1X 認証のシングルサインオン環境でログイン済みの Windows 端末に対し、外部からリモート接続を行うと次のような現象が発生します。リモート接続切断後、再度 Windows 端末上でログオンを行うと認証に失敗してしまいます。本現象が発生した場合は、およそ 20 分間認証できない状態となり、復旧には端末側の復旧(ポートのリンクダウンや再起動)が必要となってしまいます。

本現象は Windows 端末上でのユーザー切り替え(ログオフ/ログオン)の実施においても同様に発生します。

対象 OS : Windows XP SP3、Windows Vista、Windows 7

この場合の認証フローを図 5-2 に示します。

- ①-②. シングルサインオンにて認証済みのユーザー端末に対して、リモートデスクトップ端末よりリモートデスクトップ接続を行うと、ユーザー端末にてログオンしていたユーザーがログオフすると同時に、APRESIA に対して EAPOL-Start を送出します。
- ③-④. APRESIA は既にログイン済みの端末からの EAPOL-Start を受信すると、サブリカントに対して EAP-Request、Identity を送信して再認証を開始します。
- ⑤-⑦. これを受けたユーザー端末は、ログオフ済みのため、コンピューター名による EAP 応答を返します。しかし、RADIUS サーバーにコンピューター認証用の登録がない場合、認証拒否応答を返され認証失敗します。
- ⑧-⑩. APRESIA は RADIUS サーバーからの認証拒否を受信した後、サブリカントに対して EAP-Failure を送信します。ここで EAP-Failure を受信すると、Windows 端末のサブリカントは 20 分間認証動作を停止してしまいます。

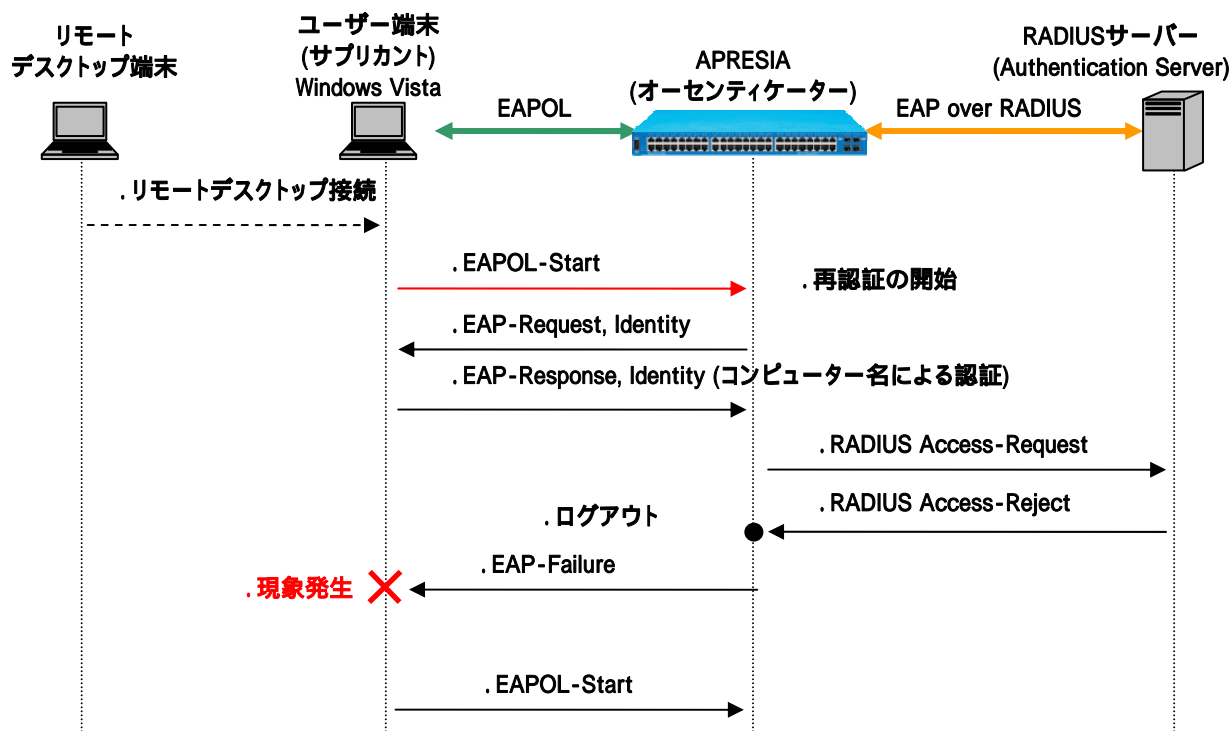


図 5-2 リモートデスクトップ接続によるログアウト時の問題点

5.3.1 ActiveDirectoryのグループポリシーを使用した回避

! このセクションの内容はサポート対象外となります。

グループポリシーとはActive Directory ドメイン内でのクライアントの動作を集中制御するための設定です。本機能を使用して、クライアントに「ワイヤード(有線)ネットワーク (IEEE 802.3)ポリシー」を適用することで、シングルサインオン時のログオン問題を回避することができます。

以下にグループポリシーオブジェクトの設定方法を示します。

グループポリシーオブジェクトの設定

(1) グループポリシー管理エディタを開く

サーバーマネージャの「機能」 - 「グループポリシーの管理」 - 「フォレスト:ドメイン名」 - 「ポリシー名」の右クリックメニューから、「編集(E)」を選択し、「グループポリシー管理エディタ」を開きます。

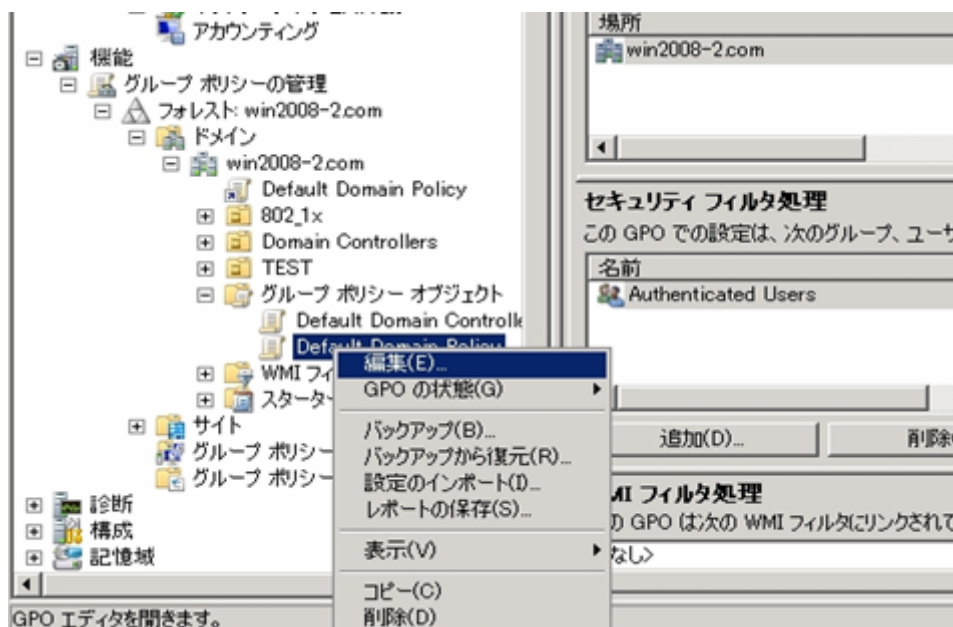


図 5-3 Default Domain Policy の編集

(2) ワイヤードネットワークポリシーにて、新しい Windows Vista ポリシーの作成

グループポリシー管理エディタの「コンピュータの構成」 - 「ポリシー」 - 「Windows の設定」 - 「ワイヤード(有線)ネットワーク (IEEE802.3)ポリシー」を選択します。

右のウィンドウにて右クリックし、「新しい Windows Vista ポリシーの作成」を選択します。

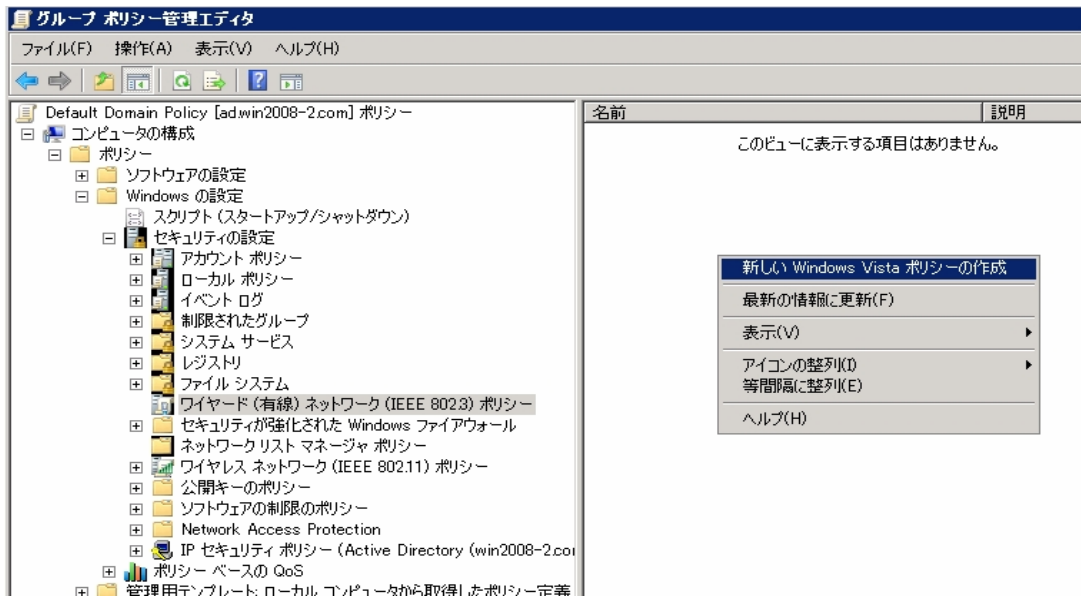


図 5-4 新しい Windows Vista ポリシーの作成

(3) 新しい Vista ワイヤード(有線)ネットワークポリシーのプロパティの設定

作成した「新しい Vista ワイヤード(有線)ネットワークポリシー」のプロパティにて、以下の設定を行います。

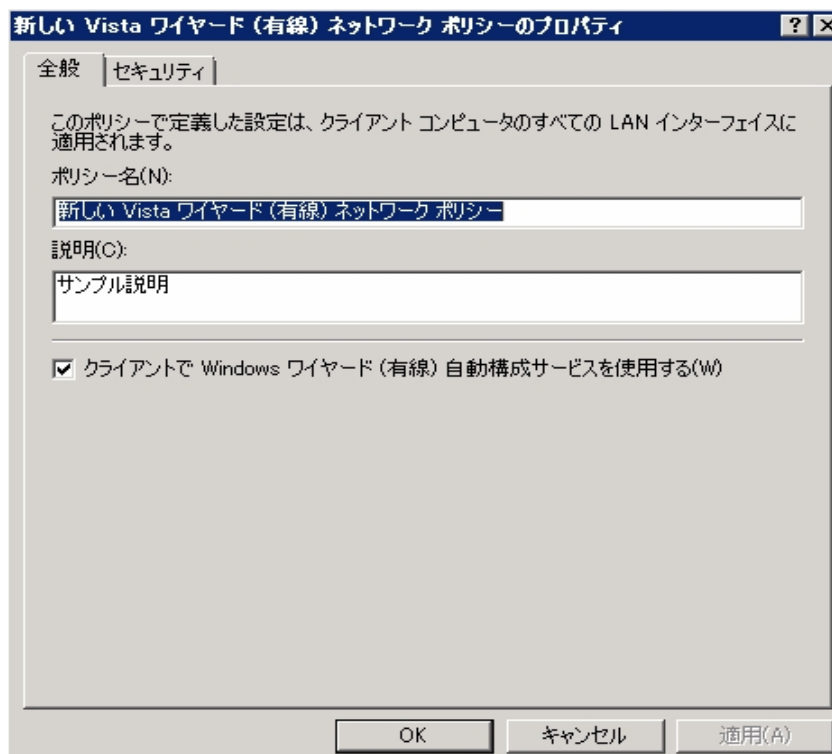


図 5-5 全般タブ

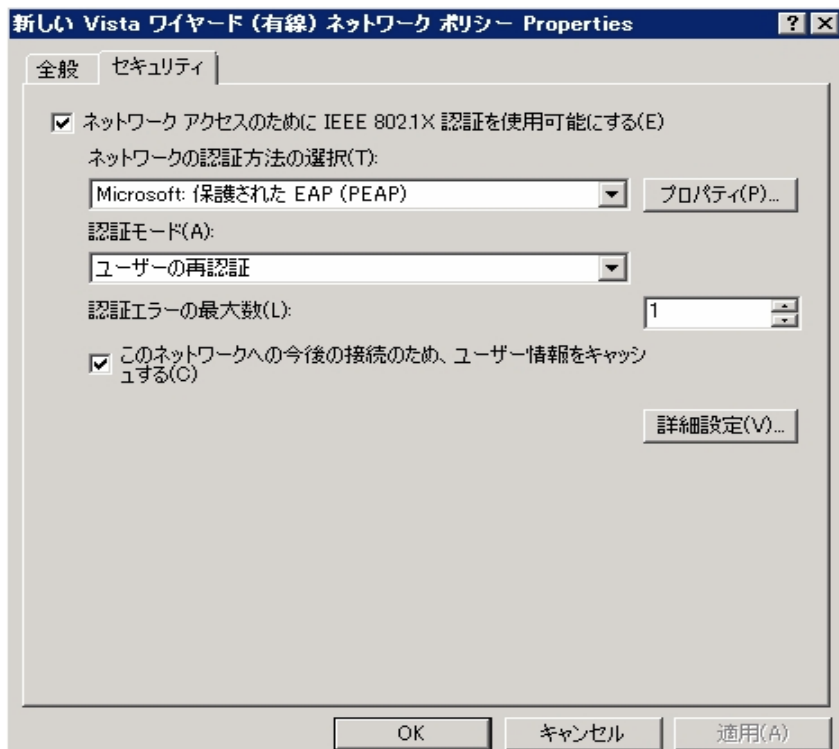


図 5-6 セキュリティタブ

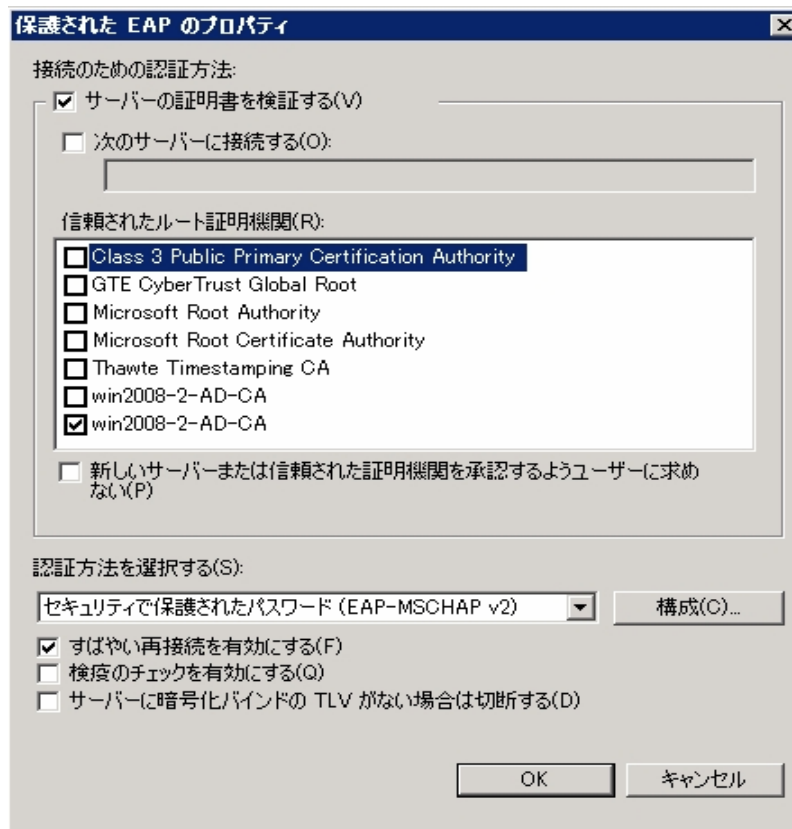


図 5-7 保護された EAP のプロパティ

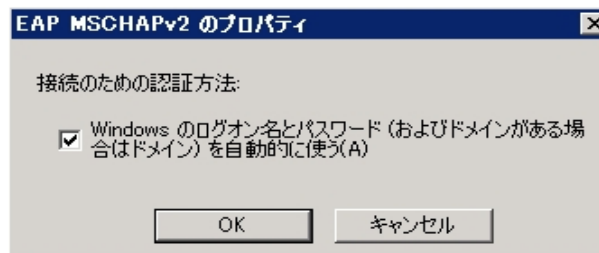


図 5-8 EAP MSCHAPv2 の構成

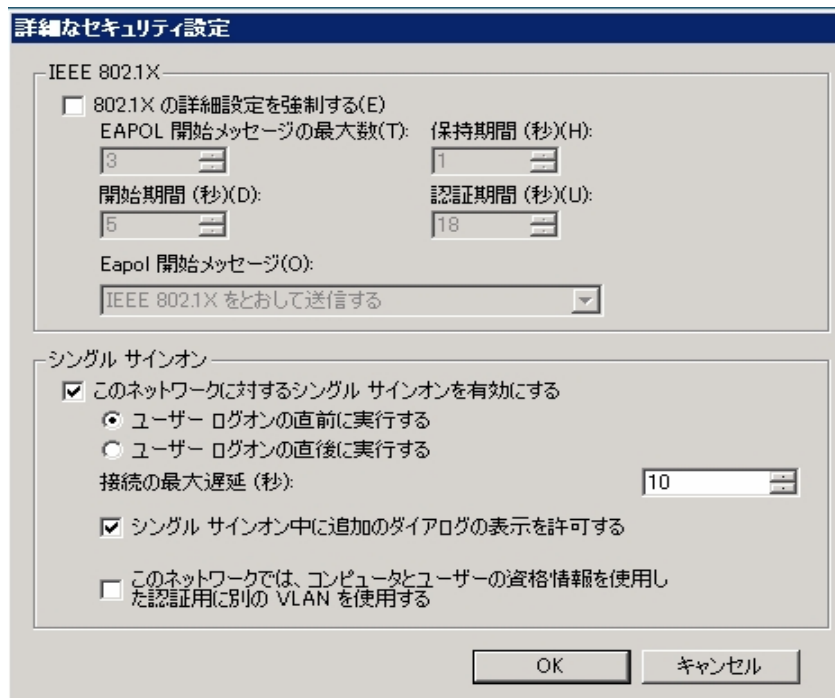


図 5-9 詳細なセキュリティ設定

- ❗ グローバルポリシーにて設定を配信するため、該当の Active Directory に参加していなければ、適用することができません。
- ❗ 初回にグローバルポリシーを適用するためにはクライアント端末のリポートが必要です。(リポート処理を必要とするのは初回適用時のみです。)

※Windows Server 2003 の場合は以下の手順で拡張設定を行う必要があります。

- 1) Windows 2003 Server のスキーマ拡張

拡張手順

- (a) スキーマの拡張に使用する ldif ファイル(802.3Schema.ldf)の作成

以下の内容をコピーし、そのファイルを 802.3Schema.ldf として Windows Server 2003 上に保存します。

```
# -----
# Copyright (c) 2006 Microsoft Corporation
#
# MODULE:      802.3Schema.ldf
```

```

# -----

# -----
#   define schemas for these attributes:
#ms-net-ieee-8023-GP-PolicyGUID
#ms-net-ieee-8023-GP-PolicyData
#ms-net-ieee-8023-GP-PolicyReserved
# -----

dn: CN=ms-net-ieee-8023-GP-PolicyGUID, CN=Schema, CN=Configuration, DC=X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-8023-GP-PolicyGUID
adminDisplayName: ms-net-ieee-8023-GP-PolicyGUID
adminDescription: This attribute contains a GUID which identifies a specific 802.3 group policy
object on the domain.
attributeId: 1.2.840.113556.1.4.1954
attributeSyntax: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
rangeUpper: 64
schemaIdGuid:: WrCn1LK4WU+cJTnm6oWhA==
showInAdvancedViewOnly: TRUE
systemFlags: 16

dn: CN=ms-net-ieee-8023-GP-PolicyData, CN=Schema, CN=Configuration, DC=X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-8023-GP-PolicyData
adminDisplayName: ms-net-ieee-8023-GP-PolicyData
adminDescription: This attribute contains all of the settings and data which comprise a group
policy configuration for 802.3 wired networks.
attributeId: 1.2.840.113556.1.4.1955
attributeSyntax: 2.5.5.12
omSyntax: 64
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
rangeUpper: 1048576
schemaIdGuid:: i5SYg1d0kU29TY1+1mnJ9w==
showInAdvancedViewOnly: TRUE
systemFlags: 16

```

```
dn: CN=ms-net-ieee-8023-GP-PolicyReserved,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: attributeSchema
ldapDisplayName: ms-net-ieee-8023-GP-PolicyReserved
adminDisplayName: ms-net-ieee-8023-GP-PolicyReserved
adminDescription: Reserved for future use
attributeId: 1.2.840.113556.1.4.1956
attributeSyntax: 2.5.5.10
omSyntax: 4
isSingleValued: TRUE
systemOnly: FALSE
searchFlags: 0
rangeUpper: 1048576
schemaIdGuid:: xyfF0wYm602M/RhCb+7Izg==
showInAdvancedViewOnly: TRUE
systemFlags: 16
```

```
# -----
# Reload the schema cache to pick up altered classes and attributes
# -----
```

```
dn:
changetype: ntdsSchemaModify
add: schemaUpdateNow
schemaUpdateNow: 1
-
```

```
# -----
# define schemas for the parent class:
#ms-net-ieee-8023-GroupPolicy
# -----
```

```
dn: CN=ms-net-ieee-8023-GroupPolicy,CN=Schema,CN=Configuration,DC=X
changetype: ntdsSchemaAdd
objectClass: classSchema
ldapDisplayName: ms-net-ieee-8023-GroupPolicy
adminDisplayName: ms-net-ieee-8023-GroupPolicy
adminDescription: This class represents an 802.3 wired network group policy object. This class
contains identifiers and configuration data relevant to an 802.3 wired network.
governsId: 1.2.840.113556.1.5.252
objectClassCategory: 1
rdnAttId: 2.5.4.3
subClassOf: 2.5.6.0
systemMayContain: 1.2.840.113556.1.4.1956
systemMayContain: 1.2.840.113556.1.4.1955
```



```

systemMayContain: 1.2.840.113556.1.4.1954
systemPossSuperiors: 1.2.840.113556.1.3.30
systemPossSuperiors: 1.2.840.113556.1.3.23
systemPossSuperiors: 2.5.6.6
schemaIdGuid:: ajqgmRmrRkSTUAY4e00tmw==
defaultSecurityDescriptor:
D: (A;;RPWPCRCDCCLORCWOWSDDTSW;;;DA) (A;;RPWPCRCDCCLORCWOWSDDTSW;;;SY) (A;;RPLCLORC;;;AU)
showInAdvancedViewOnly: TRUE
defaultHidingValue: TRUE
systemOnly: FALSE
defaultObjectCategory: CN=ms-net-ieee-8023-GroupPolicy,CN=Schema,CN=Configuration,DC=X
systemFlags: 16

# -----
# Reload the schema cache to pick up altered classes and attributes
# -----
dn:
changetype: ntdsSchemaModify
add: schemaUpdateNow
schemaUpdateNow: 1
-

```

(b) Ldifde.exe ユーティリティを使用した Active Director スキーマの拡張

Windows Server 2003 にて、コマンドプロンプトを起動し、802.3Schema.ldf の格納したフォルダへ移動します。(例では C:\Users\直下)

```

C:\Users\Administrator>cd C:\
C:\>

```

(c) スキーマの導入

コマンドプロンプトにて以下のコマンドを投入する。

(サーバー “lab4.hcl.co.jp” にスキーマ導入する場合)

```
ldifde -i -v -k -f 802.11Schema.ldf -c DC=X DC=lab4,DC=hcl,DC=co,DC=jp
```

```

C:\>ldifde -i -v -k -f 802.11Schema.ldf -c DC=X DC=lab4,DC=hcl,DC=co,DC=jp
Connecting to "ws2003en.lab4.hcl.co.jp"
Logging in as current user using SSPI
Importing directory from file "802.11Schema.ldf"
Loading entries
1: CN=ms-net-ieee-80211-GP-PolicyGUID,CN=Schema,CN=Configuration,DC=lab4,DC=hcl,DC=co,DC=jp
Entry modified successfully.

2: CN=ms-net-ieee-80211-GP-PolicyData,CN=Schema,CN=Configuration,DC=lab4,DC=hcl,DC=co,DC=jp

```

```

Entry modified successfully.

3:
CN=ms-net-ieee-80211-GP-PolicyReserved, CN=Schema, CN=Configuration, DC=lab4, DC=hcl, DC=co, DC=jp
Entry modified successfully.

4: (null)
Entry modified successfully.

5: CN=ms-net-ieee-80211-GroupPolicy, CN=Schema, CN=Configuration, DC=lab4, DC=hcl, DC=co, DC=jp
Entry modified successfully.

6: (null)
Entry modified successfully.

6 entries modified successfully.

The command has completed successfully

C:\>

```

(d) スキーマの確認

- a) [スタート] → [ファイル名を指定して実行] を選択する
- b) [名前] ボックスに以下のように入力し、[OK] ボタンをクリックする
 regsvr32 schmmgmt.dll
- c) MMC スナップインにて [Active Directory スキーマ] コンソールを追加
- d) ms-net-ieee-8023-GroupPolicy があることを確認する

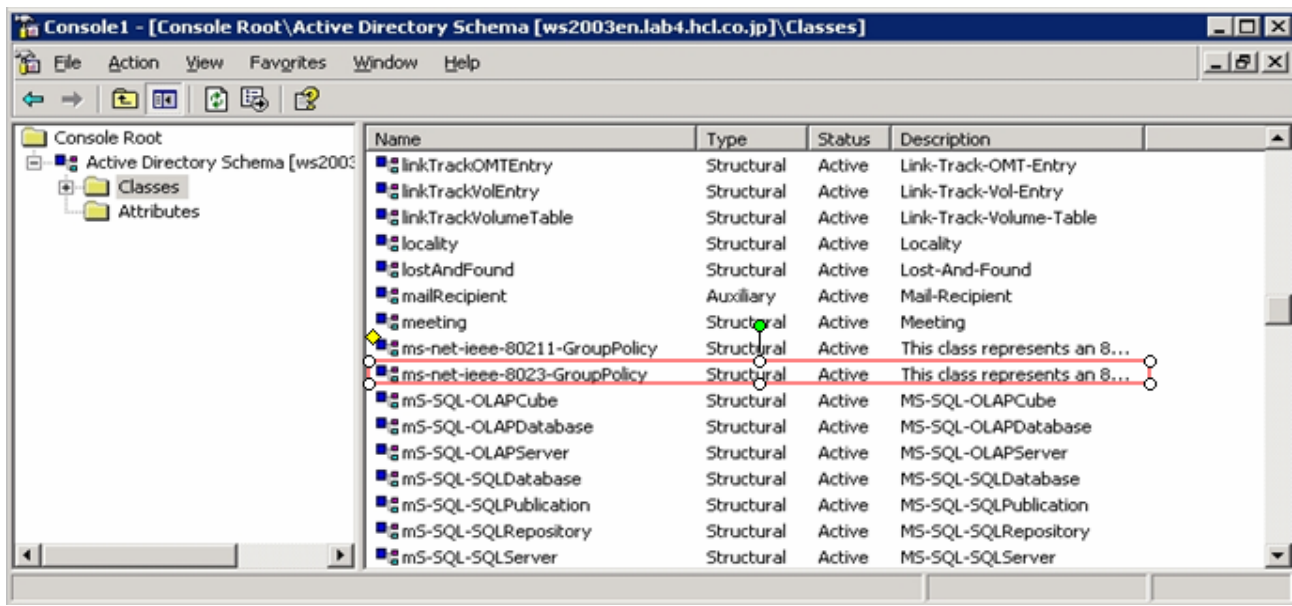


図 5-10 スキーマの確認

2) Windows Vista にてリモートサーバー管理ツール(RSAT)をインストール

Windows 2003 Server の Windows Vista ワイヤードグループポリシーを設定するには、以下の URL よりリモートサーバー管理ツールをダウンロードして Windows Vista 端末にインストールした後、リモートにて Server 側のグループポリシーを設定します。(インストール後の有効化が必要です。)

<http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960>

以下の手順でリモートサーバー管理ツールを有効化します。

- a) [スタート] → [コントロールパネル] → [プログラムと機能] → [Windows の機能の有効化または無効化] をダブルクリックします。
- b) “リモートサーバー管理ツール” 及び “グループポリシー管理ツール” にチェックを入れます。

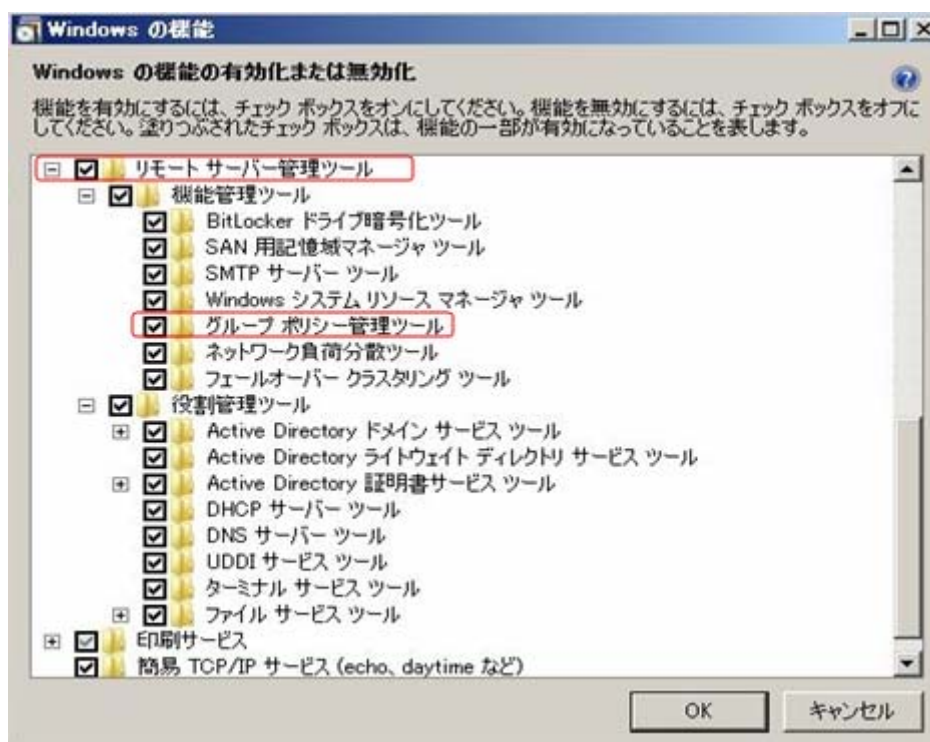


図 5-11 スキーマの確認

3) Windows Vista リモートサーバー管理ツールの操作

- a) [スタート] → [コントロールパネル] → [管理ツール] → [グループポリシーの管理] をダブルクリックし、グループポリシー管理ツールを起動します。
- b) フォレストの追加
 - a) [グループポリシーの管理] を右クリックから [フォレストの追加] を選択

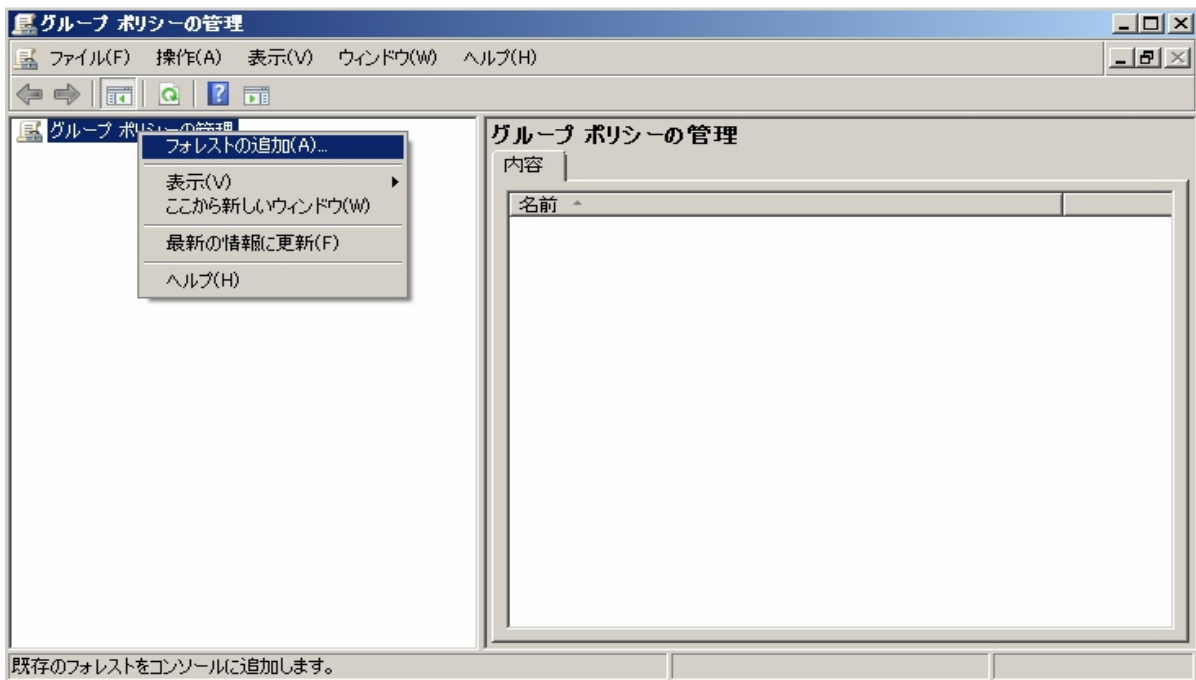


図 5-12 フォレストの追加

- b) フォレスト内のドメイン名を入力

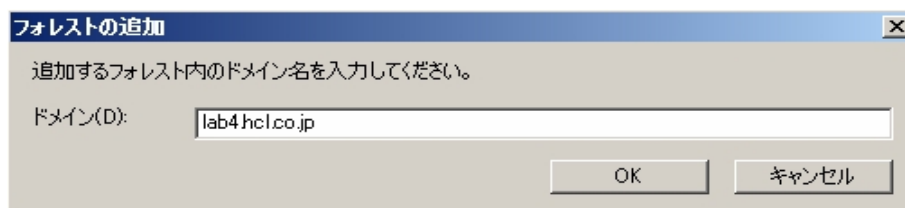


図 5-13 フォレスト内ドメイン名の入力

- c) フォレスト追加完了

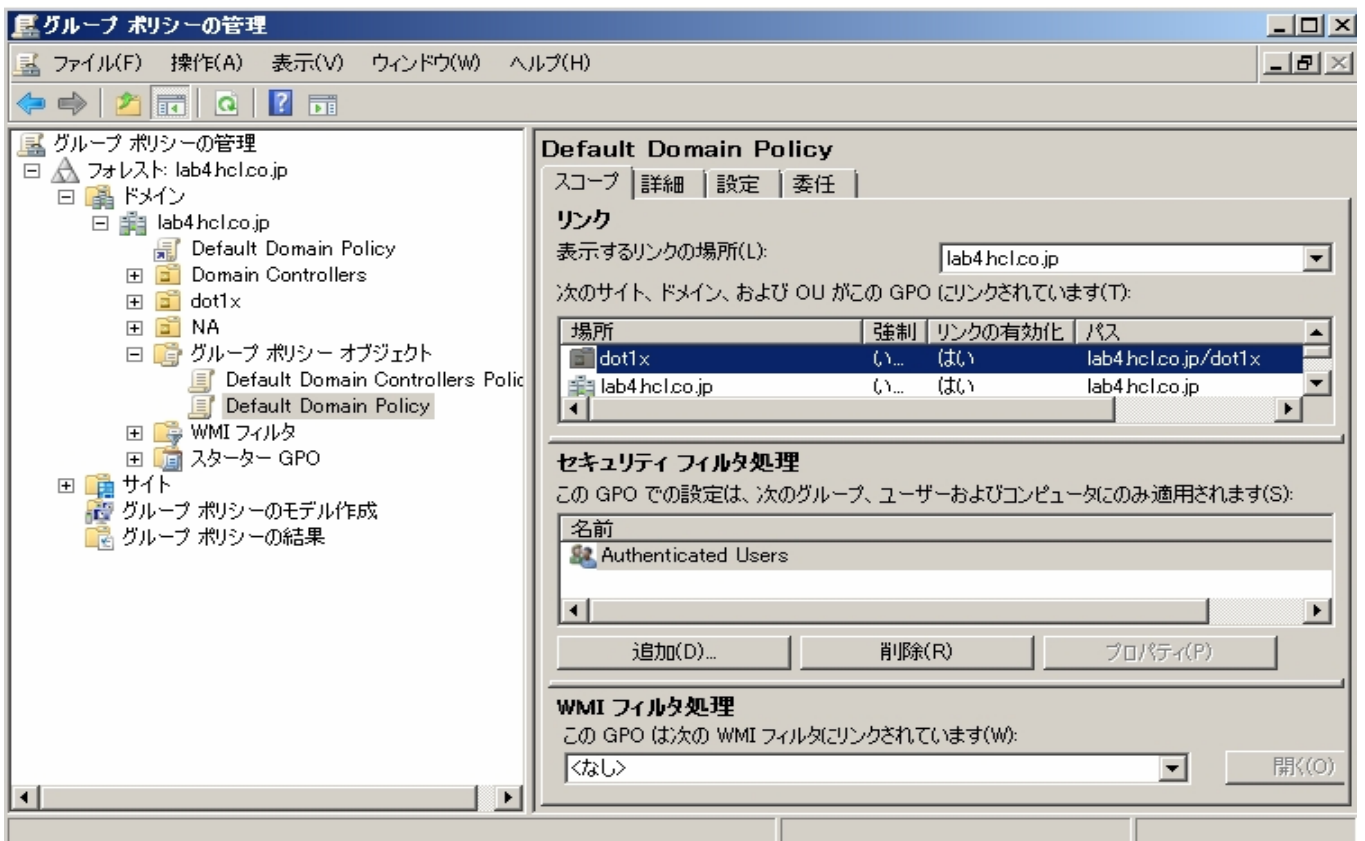


図 5-14 フォレスト追加完了

- (c) グループポリシーの設定
- a) [Default Domain Policy]を右クリックし[編集]を選択

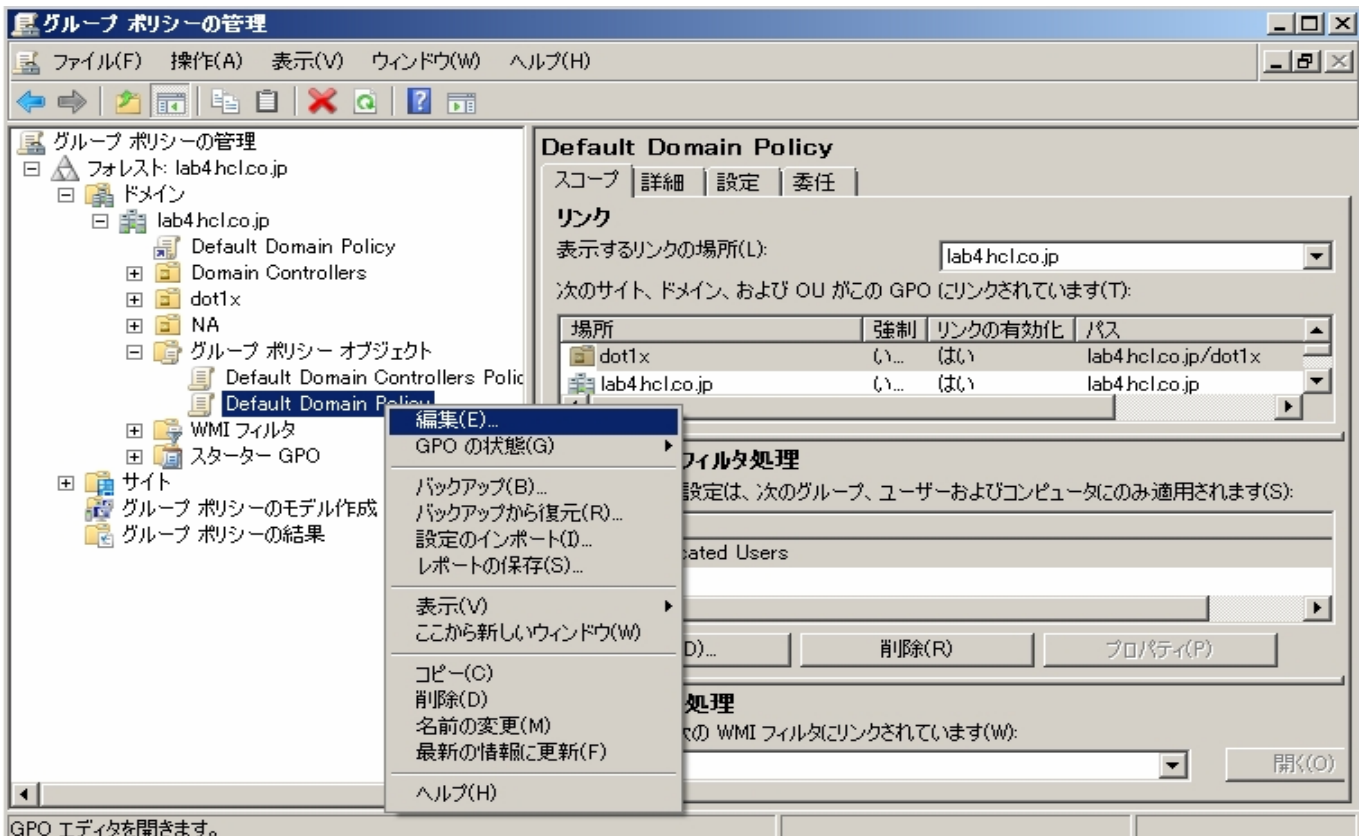


図 5-15 グループポリシーの編集

b) Windows 2008 Server と同様の手順でワイヤードの設定を行う

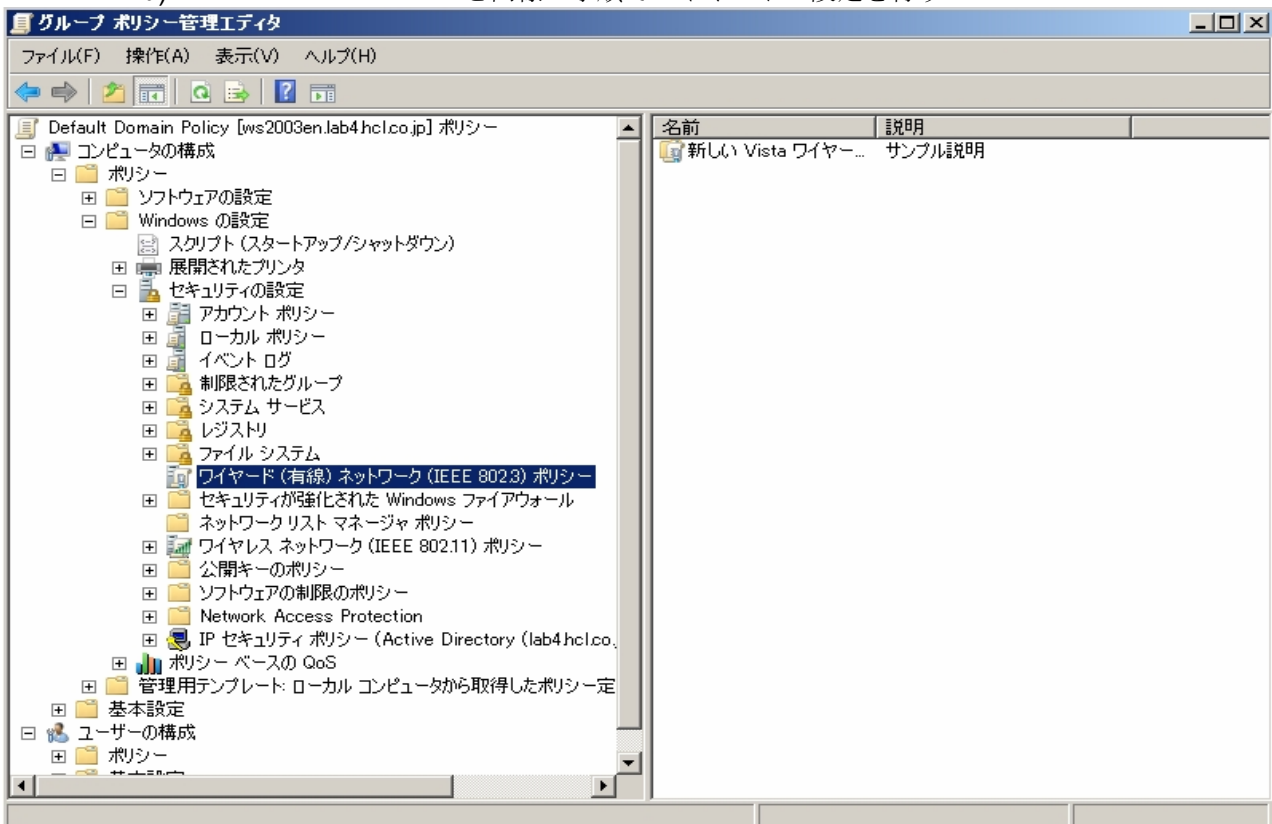


図 5-16 ワイヤードネットワークポリシーの編集



Windows2003 で構成された Active Directory を用いた場合、Windows7 に対しては本現象解決に関するグローバルポリシーが適用されません。Windows7 には個別にシングルサインオンの設定を行うことで、本現象を回避することができます。

5.3.2 Windowsクライアントに修正プログラムを適用する方法での改善

! このセクションの内容はサポート対象外となります。

本現象は 802.1x 再ログイン時に Windows 端末が約 20 分程度 APRESIA からの認証要求を受け付けない状態になっているために発生しています。この時間(無応答時間)を調整することで、現象を改善することができます。(現象発生から、EAPOL-Start 送出までの時間を短縮します。)

Microsoft の公開情報(以下 URL)に従い、個別に修正プログラムを適用した後レジストリ変更によって無応答時間を調整します。Windows7 は修正プログラムを適用しなくともレジストリ変更によって無応答時間を調整することができます。

<http://support.microsoft.com/kb/957931>

これにより直接個別の端末に設定するため、Active Directory に参加していなくとも効果を得ることができます。

レジストリ設定の変更手順は以下になります。

- (1) レジストリ エディタを開きます。これを行うには、[スタート]→[ファイル名を指定して実行]を実行し、regedit を入力して Enter を押します。

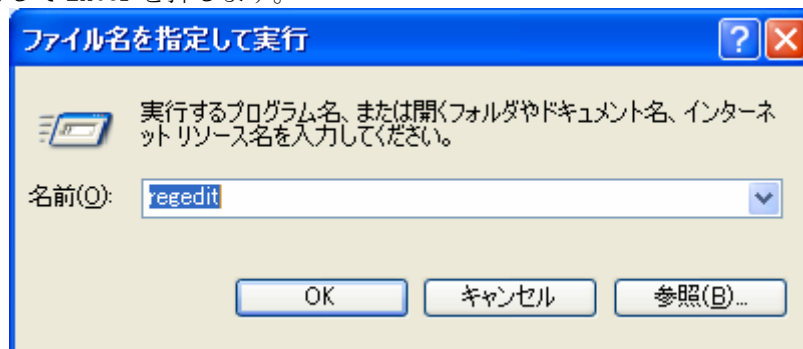


図 5-17 レジストリ エディタの起動

- (2) 次のレジストリサブキーを見つけて右クリックします。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥dot3svc

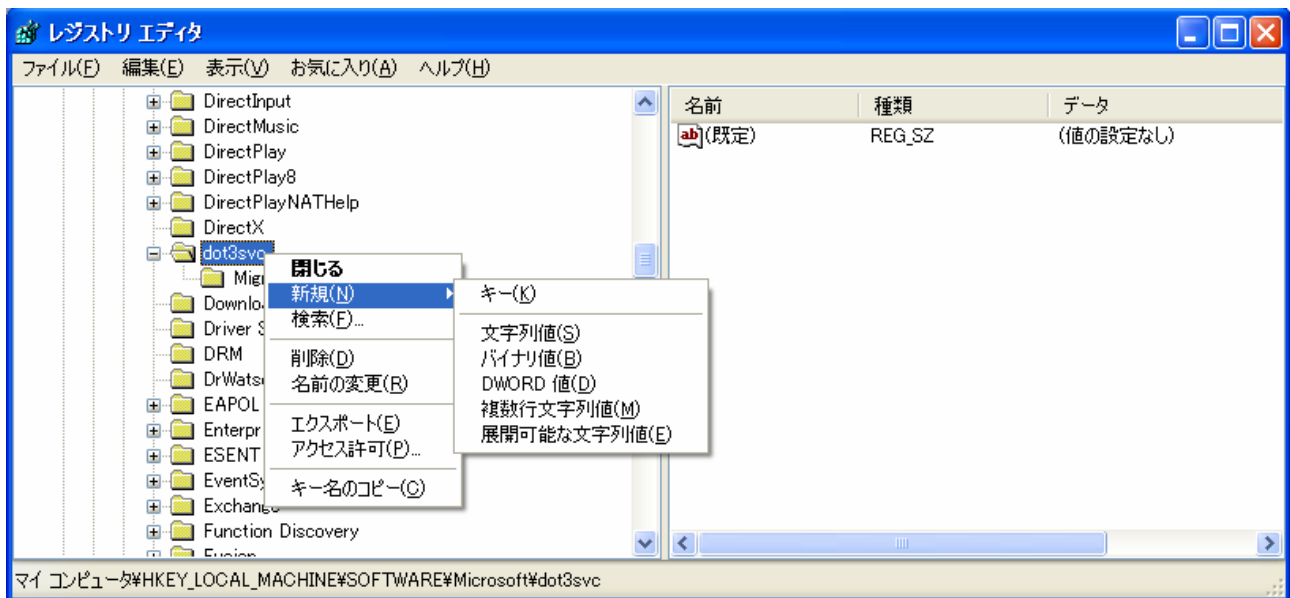


図 5-18 レジストリ変更

- (3) [新規作成]をクリックして DWORD 値を選択します。
- (4) BlockTime を入力して Enter を押します。

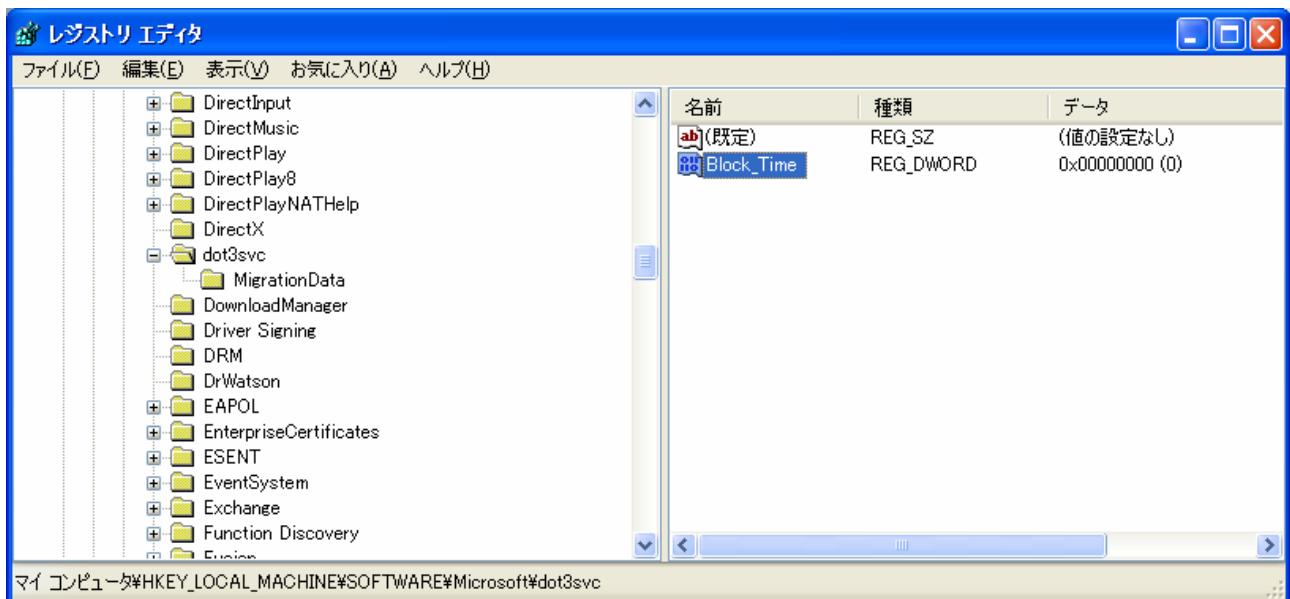


図 5-19 レジストリ変更

- (5) [BlockTime]を右クリックし、修正を実行します。
- (6) [10 進ベース]を選択します。
- (7) [値のデータ] ボックスで 0 を入力して [OK] をクリックします。

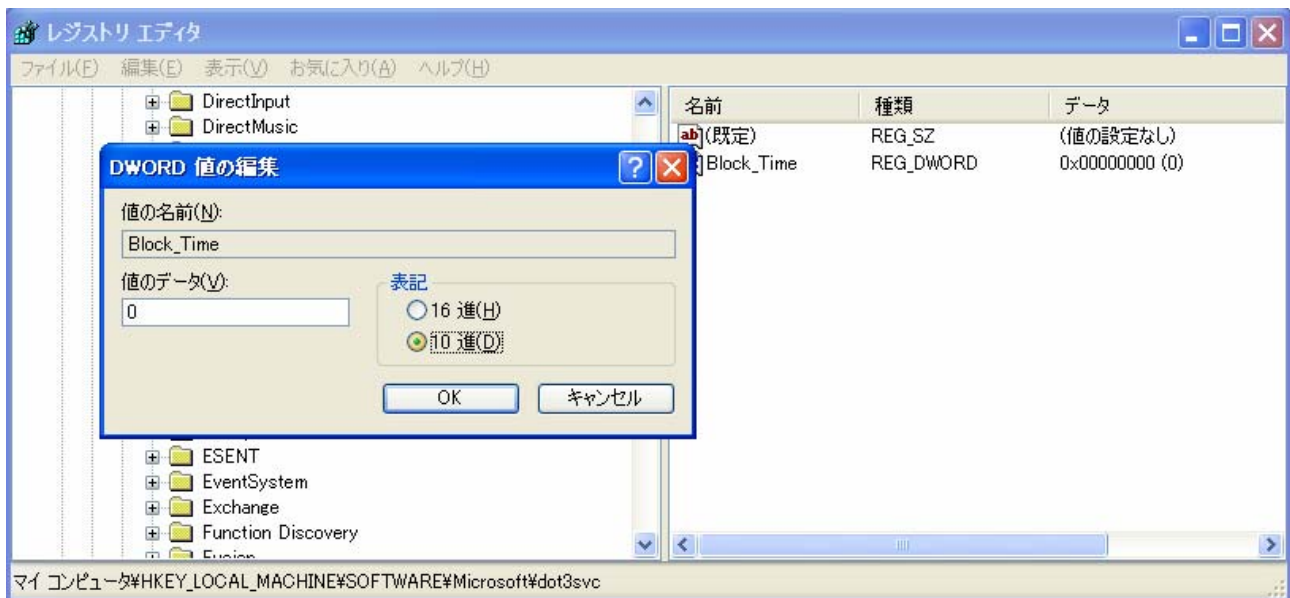


図 5-20 レジストリ変更

(8) レジストリ エディタを終了します。

! 修正プログラムの適用は Windows Vista は SP1 以上、Windows XP は SP3 以上である必要があります。

5.3.3 EAPOL Start受信による認証の抑止を用いた回避方法

EAPOL Start 受信による認証の抑止コマンドを使用することにより、個別の端末や Active Directory に手を加えず、本現象を回避することができます。

EAPOL Start 受信による認証の抑止の設定コマンドは以下となります。サブリカントから EAPOL Start フレームを受信しても、APRESIA は EAP-Request/Identity を返さず、認証動作を行いません。サブリカント契機での認証を抑止することで、認証負荷の軽減、不意の再認証の回避ができます。

```
(config-a-def)# dot1x port <PORTRANGE> ignore-eapol-start
                . . . PORTRANGE          ポート番号
```

しかし、本機能を設定することで、サブリカントからの EAPOL-Start に応答しなくなるため、以下のような影響が発生します。

- ・ 802.1x 認証が切断されないため、ログオフによるユーザーの切り替えが行えません。
- ・ Windows からの初期化要求に反応しなくなるため、定期的に行われるスイッチからの初期化要求がくるまで、認証が開始できなくなります。スイッチ側からの定期初期化要求送出間隔は 30 秒です。

以下の図のような動作になります。

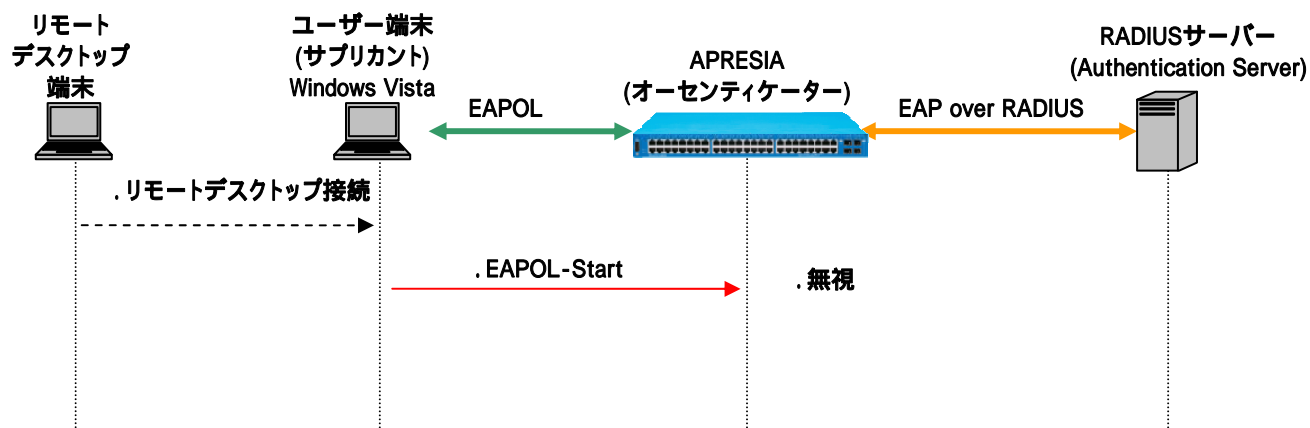


図 5-3 EAPOL Start 受信による認証の抑止コマンドによる回避

- ❗ 本装置からの定期初期化要求送出間隔は、`dot1x port <PORTRANGE> timeout tx-period <SECS>` コマンドで設定可能です。0 を指定した場合、定期初期化要求は再送されません。詳細は、3.8 認証開始時の EAP-Request/Identity の抑制を参照ください。
- ❗ 本機能を使用すると本装置が EAP-Request/Identity を送信するまで認証を開始しません。送信のタイミングに関しては、3.8 認証開始時の EAP-Request/Identity の抑制を参照ください。

5.4 VRRP併用時の注意点

AccessDefender と VRRP を併用する場合、以下に挙げる注意点に留意して使用してください。

- MAC 認証を使用する場合、VRRP パケット未認証状態では VRRP ステータスが収束しないため、VRRP の仮想 MAC アドレスを RADIUS サーバー、ローカルデータベース、または強制認証で認証。RADIUS サーバーにて VRRP の仮想 MAC アドレスを認証させると、RADIUS サーバー障害時に VRRP ステータスが収束しないため、ローカルデータベースまたは強制認証を推奨
- Web 認証使用時に VRRP の切替りが発生した場合、新たなマスターにおいて再認証が必要
- DHCP スヌーピングは併用不可

MAC認証とVRRP併用構成例を図 5-21 に示します。VRRPの仮想MACアドレスはローカルデータベースにて認証、端末はローカルデータベースで認証失敗後、RADIUSサーバーにて認証させます。ルーティングプロトコルとしてOSPFを使用し、v100 にてVRRPを動作させます。

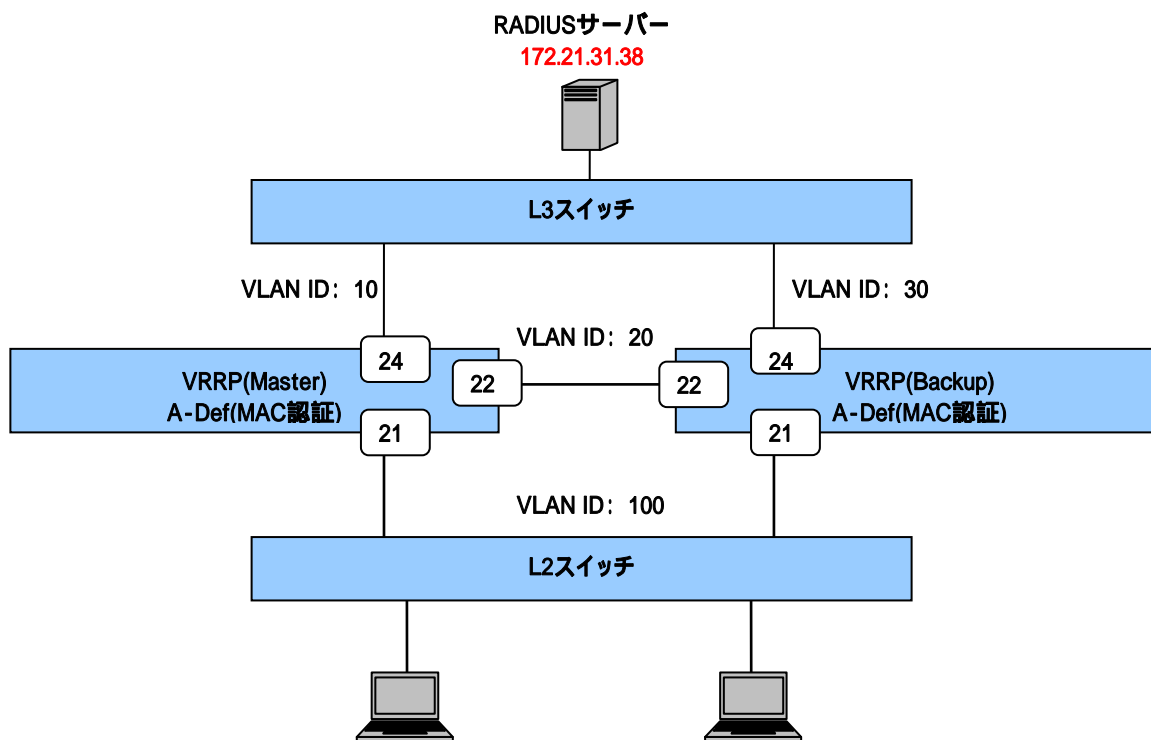


図 5-21 MAC 認証と VRRP 併用構成例

図 5-21 での VRRP (Master) の代表的な設定例を示します。

```
(config)# vlan database
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 20 name v20
(config-vlan)# vlan 100 name v100
    . . . VLAN の設定

(config)# interface port 21
(config-if-port)# switchport access vlan 100
(config)# interface port 22
```

```
(config-if-port)# switchport access vlan 20
(config)# interface port 24
(config-if-port)# switchport access vlan 10
    . . . ポートに VLAN を設定
```

```
(config)# interface vlan 100
(config-if)# ip address 172.18.100.1/24
(config)# interface vlan 10
(config-if)# ip address 172.18.41.2/24
(config)# interface vlan 20
(config-if)# ip address 172.18.61.1/24
    . . . VLAN に IP アドレスを設定
```

```
(config)# router ospf 1
(config-router)# passive-interface vlan 100
(config-router)# network 0.0.0.0 0.0.0.0 area 0
    . . . OSPF を設定
```

```
(config)# router vrrp 100
(config-router)# virtual-ip 172.18.100.1 master
(config-router)# interface vlan 100
(config-router)# enable
    . . . VRRP を設定
```

```
(config)# aaa radius 1 host 172.21.31.38 key apresia
(config)# aaa authentication mac local radius 1
(config)# aaa authentication mac control sufficient
    . . . 認証方法の設定
```

※ ローカルデータベースでの認証不可の場合、INDEX1 の RADIUS サーバーにて認証

```
(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
    . . . 最大認証端末(128 台)の設定
```

```
(config-a-def)# mac-authentication port 21
    . . . MAC 認証ポートの設定
```

```
(config-a-def)# mac-authentication password zzzzz
    . . . MAC 認証用パスワードの設定
```

```
(config)# mac-authentication enable
    . . . MAC 認証の有効化
```

6. 構成例

6.1 Web認証構成例

AccessDefender での Web 認証設定例を説明します。APRESIA に登録する認証用 URL を全 APRESIA について統一することにより、ユーザーはどの APRESIA 配下に接続しているかを意識せずにアクセスすることが可能となります。

認証される前にユーザーが属する暫定VLANを認証ポートに設定し、Uplinkポートには、接続が想定される全てのVLANをTrunkとして設定しておきます。暫定VLANに接続される端末は当該VLAN内のみに通信が制限されているため、他の未認証ポートに接続している端末とも相互通信はできません。認証成功後は、ポートに対して正規VLANが割り当てられるのではなく、端末に対して正規VLANが割り当てられます(図 6-1 の構成例のように同一ハブ配下に複数のVLANの端末を接続可能です)。

認証前後で端末が所属する VLAN が動的に変更されるため、Web 認証では DHCP 環境が必須要件となります。暫定 VLAN 用と正規 VLAN 用の DHCP サーバーが必要となりますが、暫定 VLAN 用 DHCP サーバーは認証スイッチ内部や外部に設定可能です(本装置の DHCP サーバー機能を併用して、端末へ動的に VLAN を割り当てる場合、認証前 VLAN 用の DHCP サーバーと、認証後 VLAN 用の DHCP サーバーは同一装置内に設定しないでください。認証後 VLAN の IP アドレスに切り替わらないことがあります)。

APRESIA の DHCP サーバー機能の設定はネットワークアドレス毎に行い、この設定単位をポリシーと呼びます。ポリシー条件として、IP アドレスが設定された有効な VLAN が存在し、かつ、その VLAN に物理ポートが割り当てられていることが必要となります。したがって、認証スイッチ内部で動作させる暫定 VLAN 用 DHCP サーバーのポリシーを作成するためには、暫定 VLAN に対して有効な IP アドレスを設定する必要があります。暫定 VLAN はネットワーク内の全認証スイッチで同一となるため(ゲートウェイは上位 L3 スイッチ)、各認証スイッチに割り当てる暫定 VLAN の IP アドレス重複を避ける必要があります。また、未認証端末に割り振る暫定 IP アドレスの重複も避ける必要があります。各認証スイッチに設定する DHCP サーバーのリース空間は、認証スイッチ毎に変える必要があります。この場合、暫定 VLAN の IP アドレスの枯渇を防ぐため、ネットマスクは 8bit や 16bit などしておく必要があります。

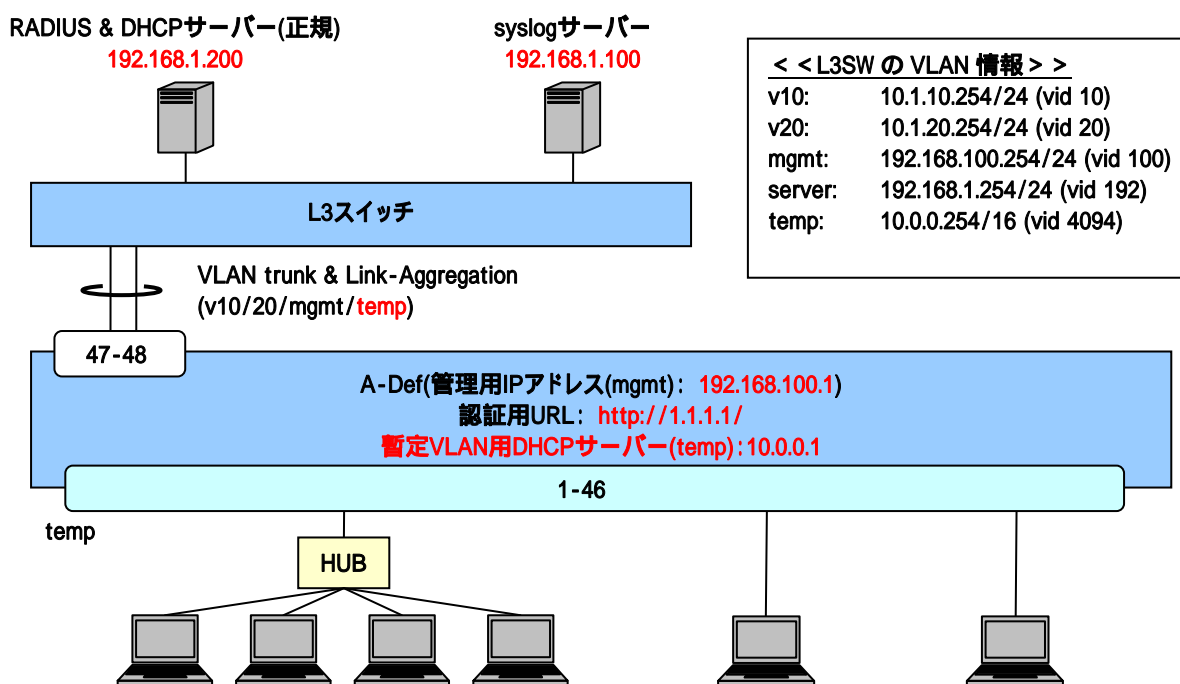


図 6-1 Web 認証構成例

図 6-1 の構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 info
    . . . syslog サーバーの登録(優先度 info 以上のログを送信)

(config)# packet-filter2
(config-filter)# 2 assign port 1-46
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
    . . . packet-filter2 の設定(DHCP の通信許可)
        (VLAN 固定時の DHCP 環境では必須)

(config)# vlan database
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 20 name v20
(config-vlan)# vlan 100 name mgmt
(config-vlan)# vlan 4094 name temp
    . . . VLAN の設定(管理用 VLAN 名は"mgmt"、暫定 VLAN を"temp"とする)

(config)# interface port 1-44
(config-if-port)# switchport access vlan 4094

(config)# interface port 45-46
(config-if-port)# media utp
(config-if-port)# switchport access vlan 4094
    . . . 暫定 VLAN を access ポートとして設定
        ※ 認証前のポートは完全に孤立状態のため、未認証端末同士も通信不可

(config)# interface port 47-48
(config-if-port)# utp auto-negotiation disable
(config-if-port)# utp link-speed-duplex 100m/full
(config-if-port)# media utp
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10, 20, 100, 4094
(config-if-port)# link-aggregation 1
    . . . Uplink ポートの設定(想定される全 VLAN を Trunk として設定)

(config)# interface vlan 100
(config-if)# ip address 192.168.100.1/24
(config)# interface vlan 4094
(config-if)# ip address 10.0.0.1/16
    . . . 管理用 VLAN(mgmt) と暫定 VLAN(temp) のアドレス設定(暫定 VLAN 用
        DHCP サーバーの設定のため)
```

※ 暫定 VLAN はネットワーク内の全認証スイッチで同一のため、各認証スイッチに割当てする暫定 VLAN の IP アドレス重複を避ける必要あり

```
(config)# ip route 0.0.0.0/0 192.168.100.254
```

・・・デフォルトルートの設定

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication web radius 1
```

・・・RADIUS サーバー関連の設定(プライマリ) (必須)

※ この例では、INDEX1 の RADIUS を Web 認証のプライマリとしています。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# web-authentication port 1-46
```

・・・Web 認証ポート(1-46) (必須)

```
(config-a-def)# web-authentication ip 1.1.1.1
```

```
(config-a-def)# web-authentication http-port 80
```

・・・認証 URL(http://1.1.1.1/) (必須)

※ 全ての APRESIA で統一することが可能

```
(config-a-def)# logout aging-time 300
```

・・・ログアウト(エージング : 300 秒)

```
(config)# web-authentication enable
```

・・・Web 認証の有効化 (必須)

```
(config)# dhcp policy temp
```

```
(config-dhcp)# network 10.0.0.0/16
```

```
(config-dhcp)# range 1 10.0.0.10 10.0.0.20
```

```
(config-dhcp)# router 10.0.0.254
```

```
(config-dhcp)# lease 10
```

```
(config)# dhcp policy enable temp
```

```
(config)# dhcp server address-check arp
```

```
(config)# dhcp server enable
```

・・・暫定 VLAN 用 DHCP サーバーの設定(リース時間は 10 秒)

※ リースする暫定 IP アドレスの重複も避ける必要があり、設定する DHCP サーバーのリース空間は、認証スイッチ毎に変える必要があります。

※ リース時間は端末の IP アドレス更新仕様に合わせて適切な値に調整してください。

- ❗ DHCP 環境の場合、DHCP の強制通信許可が必要です (Web 認証有効時に ARP は自動的に強制転送されます)。
- ❗ 上位の L3 スイッチには暫定 VLAN の設定が必要です。

6.2 MAC認証構成例

動的 VLAN 変更を有効にする場合、ユーザー毎に VLAN を動的に割当するという動作をするため、認証される前にユーザーが属する暫定 VLAN を設定します。暫定 VLAN は、認証スイッチ内のみを設定しておきます。Web 認証のように、暫定 VLAN を上位 L3 スイッチに対して Trunk 接続する必要はありません。アップリンクポートには、接続が想定される全ての VLAN を Trunk として設定しておく必要があります。

MAC 認証のみを設定する場合、Web 認証用の認証 URL 設定は不要です。また、認証前に強制的に上位ネットワークに転送する必要もないため、各種認証バイパスも不要です。

認証ポートに割り振られる暫定 VLAN に接続される端末は、当該 VLAN 内のみに通信が制限されていますので、APRESIA 自局にもアクセスできません。また、他の未認証ポートに接続している端末とも相互通信はできません。認証されるまでは完全に孤立状態となります。

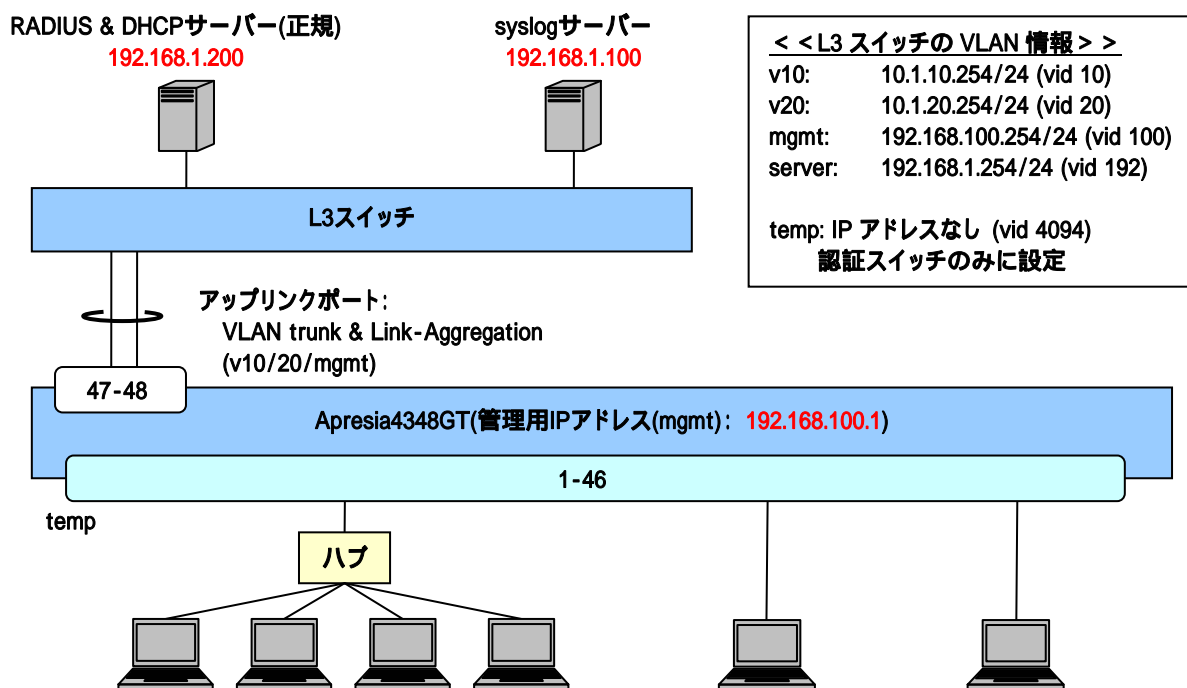


図 6-2 MAC 認証構成例

図 6-2 の構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 info
    ... syslog サーバーの登録(優先度 info 以上のログを送信)

(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication mac radius 1
    ... RADIUS サーバー関連の設定(プライマリ) (必須)
```

※ この例では、INDEX1 の RADIUS を MAC 認証のプライマリとしています。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# mac-authentication port 1-46
```

・・・MAC 認証ポート(1-46) (必須)

```
(config-a-def)# mac-authentication password 1q2w3e
```

・・・MAC 認証用のパスワード設定 (必須)

```
(config)# mac-authentication enable
```

・・・MAC 認証の有効化 (必須)

```
(config)# interface port 47-48
```

```
(config-if-port)# utp auto-negotiation disable
```

```
(config-if-port)# utp link-speed-duplex 100m/full
```

```
(config-if-port)# media utp
```

```
(config-if-port)# switchport mode trunk
```

```
(config-if-port)# switchport trunk add 10,20,100
```

```
(config-if-port)# link-aggregation 1
```

・・・Uplink ポートの設定(想定される全 VLAN を Trunk 設定しておく)



MAC 認証のみの場合、暫定 VLAN は認証スイッチ内のみを設定しておきます。Web 認証のように、暫定 VLAN を上位 L3 スイッチに対して Trunk 接続する必要はありません。

※ VLAN設定および管理用VLANのアドレス設定は 図 6-1 と同じなので省略します。ただし、暫定VLANには IPアドレスを設定する必要はありません。

6.3 Web認証、MAC認証の混在環境構成例

Web 認証と MAC 認証を混在させる場合の設定例を説明します。この場合、Web 認証と MAC 認証で各々必須の設定項目を入力する必要があります。

認証用 URL は、Web 認証と同様に APRESIA に登録する認証用 URL を全 APRESIA について統一します。

認証 URL を統一することにより、ユーザーはどの APRESIA 配下に接続しているかを意識せずにアクセスすることが可能となります。また、MAC 認証用にパスワードを設定しておきます。

以下の 図 6-3 のように、認証ポート配下のスイッチングハブやハブ内でPCとプリンタを接続し、PCはWeb認証で認証させ、プリンタはMAC認証で認証させることが可能です。

MAC アドレスを各 APRESIA のポートにスタティックに登録して認証不要端末として扱う必要がなくなるため、プリンタや固定 IP フォンの接続場所を自由に変更することができます。

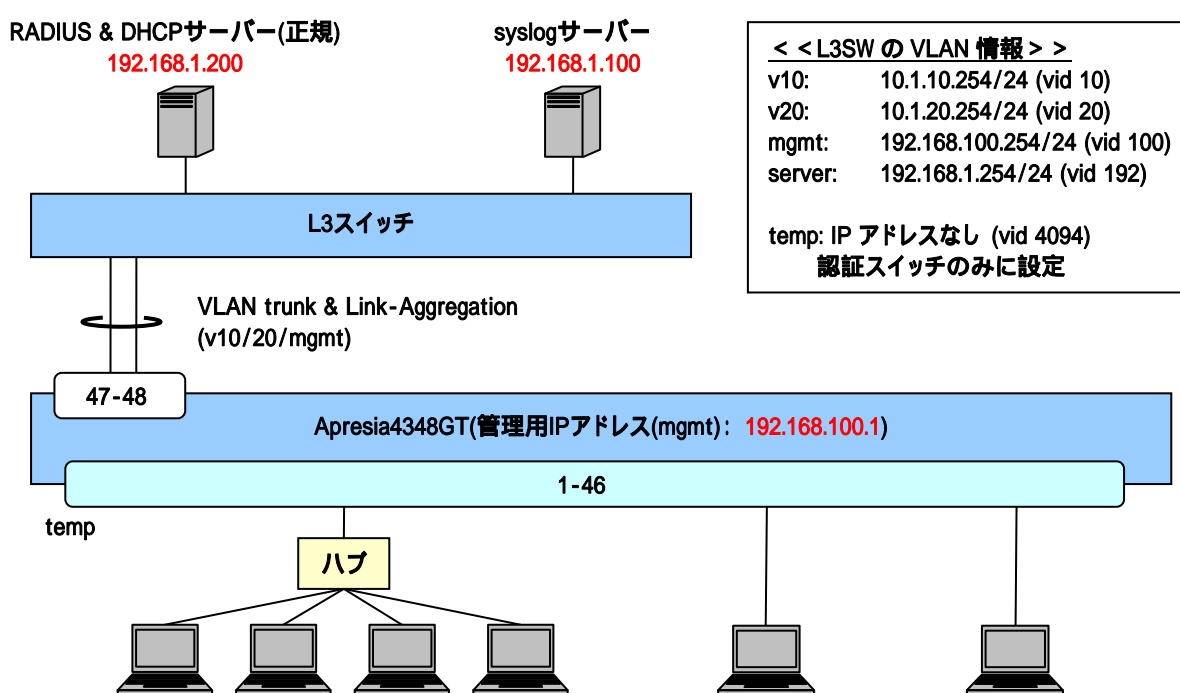


図 6-3 Web 認証と MAC 認証の併用構成例

図 6-3 の構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 info
    ... syslog サーバーの登録(優先度 info 以上のログを送信)

(config)# packet-filter2
(config-filter)# 2 assign port 1-46
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
    ... packet-filter2 の設定(DHCP の通信許可)
        (VLAN 固定時の DHCP 環境では必須)

(config)# vlan database
```

```
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 20 name v20
(config-vlan)# vlan 100 name mgmt
(config-vlan)# vlan 4094 name temp
```

・・・VLAN の設定(管理用 VLAN 名は"mgmt"、暫定 VLAN を"temp"とする)

```
(config)# interface port 1-44
(config-if-port)# switchport access vlan 4094
(config)# interface port 45-46
(config-if-port)# media utp
(config-if-port)# switchport access vlan 4094
```

・・・暫定 VLAN を access ポートとして設定

※ 認証前のポートは完全孤立状態のため、未認証端末同士も通信不可

```
(config)# interface port 47-48
(config-if-port)# utp auto-negotiation disable
(config-if-port)# utp link-speed-duplex 100m/full
(config-if-port)# media utp
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10, 20, 100, 4094
(config-if-port)# link-aggregation 1
```

・・・Uplink ポートの設定(想定される全 VLAN を Trunk 設定しておく)

```
(config)# interface vlan 100
(config-if)# ip address 192.168.100.1/24
(config)# interface vlan 4094
(config-if)# ip address 10.0.0.1/16
```

・・・管理用 VLAN(mgmt) と暫定 VLAN(temp) のアドレス設定(暫定 VLAN 用 DHCP サーバーの設定のため)

※ 暫定 VLAN はネットワーク内の全認証スイッチで同一のため、各認証スイッチに割当てる暫定 VLAN のアドレス重複を避ける必要あり

```
(config)# ip route 0.0.0.0/0 192.168.100.254
```

・・・デフォルトルートの設定

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication web radius 1
(config)# aaa authentication mac radius 1
```

・・・RADIUS サーバー関連の設定(プライマリ) (必須)

※ この例では、INDEX1 の RADIUS を Web/MAC のプライマリとしています。

```
(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# web-authentication port 1-46
```

・・・Web 認証ポート(1-46) (必須)

```
(config-a-def)# web-authentication ip 1.1.1.1
```

```
(config-a-def)# web-authentication http-port 80
```

・・・認証 URL(http://1.1.1.1/) (必須)

※ 全ての APRESIA で統一することが可能

```
(config-a-def)# mac-authentication port 1-46
```

・・・MAC 認証ポート(1-46) (必須)

```
(config-a-def)# mac-authentication password 1q2w3e
```

・・・MAC 認証用のパスワード設定 (必須)

```
(config-a-def)# logout aging-time 300
```

・・・ログアウト(エージング : 300 秒)

```
(config)# web-authentication enable
```

```
(config)# mac-authentication enable
```

・・・Web/MAC 認証の有効化 (必須)

```
(config)# dhcp policy temp
```

```
(config-dhcp)# network 10.0.0.0/16
```

```
(config-dhcp)# range 1 10.0.0.10 10.0.0.20
```

```
(config-dhcp)# router 10.0.0.254
```

```
(config-dhcp)# lease 10
```

```
(config)# dhcp policy enable temp
```

```
(config)# dhcp server address-check arp
```

```
(config)# dhcp server enable
```

・・・ 暫定 VLAN 用 DHCP サーバーの設定(リース時間は 10 秒)

※ リースする暫定 IP アドレスの重複も避ける必要があります、設定する DHCP
サーバーのリース空間は、認証スイッチ毎に変える必要があります。

※ リース時間は端末の IP アドレス更新仕様に合わせて適切な値に調整し
てください。

6.4 Web/MAC認証構成例

Web/MAC 認証設定例を説明します。Web 認証の設定に加え Web/MAC 認証機能を有効にする必要があります。認証用 URL は、Web 認証と同様に APRESIA に登録する認証用 URL を全 APRESIA について統一します。認証用 URL を統一することにより、ユーザーはどの APRESIA 配下に接続しているかを意識せずにアクセスすることが可能となります。

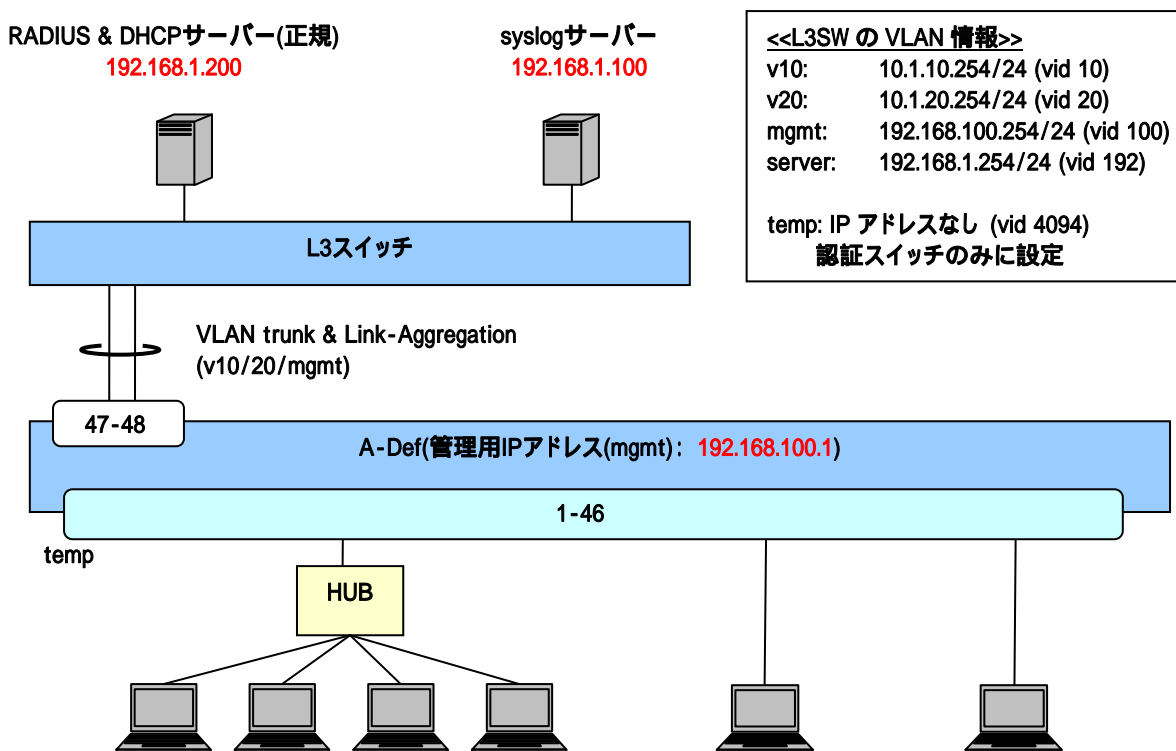


図 6-4 Web/MAC 認証の構成例

図 6-4 の構成例における認証スイッチの設定例を示します。(VLAN、インターフェース構成などは図 6-1 と同一のため、設定例は省略します)

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication web radius 1
```

・・・RADIUS サーバー関連の設定(プライマリー) (必須)

※ Web/MAC 認証は Web 認証の設定で動作します。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

```
(config-a-def)# web-authentication port 1-46 mac-authentication
```

・・・Web/MAC 認証ポート(1-46) (必須)

(config-a-def)# **web-authentication ip 1.1.1.1**

(config-a-def)# **web-authentication http-port 80**

・・・ 認証 URL (http://1.1.1.1/) (必須)

※ 全ての APRESIA で統一することが可能

(config-a-def)# **web-authentication mac-authentication-password 1q2w3e**

・・・ Web/MAC 認証用のパスワード設定 (必須)

(config-a-def)# **logout aging-time 300**

・・・ ログアウト (エージング : 300 秒)

(config)# **web-authentication enable**

・・・ Web 認証の有効化 (必須)

(config)# **dhcp policy temp**

(config-dhcp)# **network 10.0.0.0/16**

(config-dhcp)# **range 1 10.0.0.10 10.0.0.20**

(config-dhcp)# **router 10.0.0.254**

(config-dhcp)# **lease 10**

(config)# **dhcp policy enable temp**

(config)# **dhcp server address-check arp**

(config)# **dhcp server enable**

・・・ 暫定 VLAN 用 DHCP サーバーの設定 (リース時間は 10 秒)

※リース時間は端末の IP アドレス更新仕様に合わせて適切な値に調整してください。

6.5 ゲートウェイ認証構成例(サーバーファーム手前に適用)

クライアントと認証スイッチが別ネットワークに存在するようなケースではゲートウェイ認証方式により、認証環境の構成が出来ます。

構成例として、サーバーファームの手前に置く場合の設定例を紹介します。

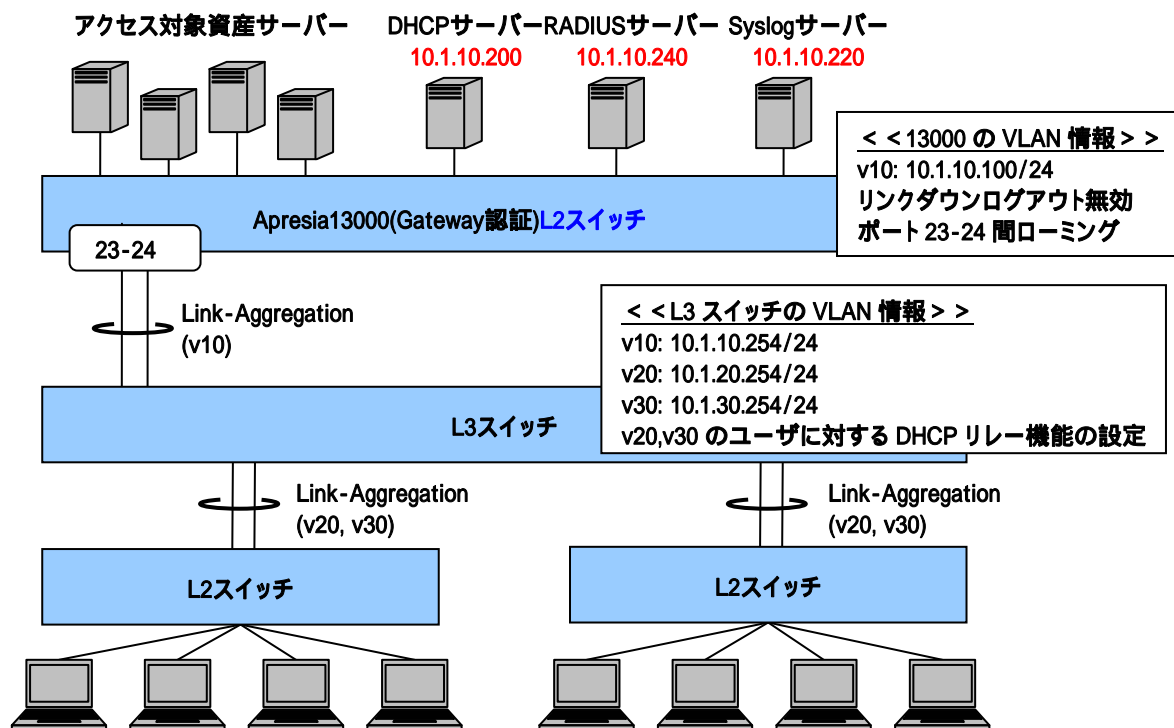


図 6-5 ゲートウェイ認証構成例(サーバーファーム手前適用)

図 6-5 の構成例でのゲートウェイ認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 10.1.10.220 local0 notice
    ... syslog サーバーの登録(優先度 notice 以上のログを送信)

(config)# packet-filter2
(config-filter)# 1 assign port 23-24
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
    ... packet-filter2 の設定(DHCP リレーパケットの通信許可)
    (DHCP 環境では必須)

(config-filter)# 1 2 condition ipv4 dst tcp/udp 514 udp
(config-filter)# 1 2 action authentication-bypass
    ... syslog パケットの通信許可(その他、必要な通信を通信許可)

(config)# vlan database
(config-vlan)# vlan 10 name v10
```


・・・VLAN の設定

```
(config)# interface port 23-24
```

```
(config-if-port)# utp advertise delete 10m/half
```

```
(config-if-port)# utp advertise delete 10m/full
```

```
(config-if-port)# utp advertise delete 100m/half
```

```
(config-if-port)# utp advertise delete 100m/full
```

```
(config-if-port)# switchport access vlan 10
```

```
(config-if-port)# link-aggregation 1
```

・・・ポート 23, 24 を 1Gbps、全二重に固定

・・・ポート 23, 24 を LAG ポート(グループ 1)として設定

```
(config)# interface vlan 10
```

```
(config-if)# ip address 10.1.10.100/24
```

・・・VLAN10 に IP アドレスを設定 (必須)

上位に L3 スイッチが存在しないのでユーザーVLAN に IP アドレスをアサインし、直接応答させます。

```
(config)# ip route 0.0.0.0/0 10.1.10.254
```

・・・デフォルトルートの設定(必須)

```
(config)# aaa radius 1 host 10.1.10.240 key apresia
```

```
(config)# aaa authentication web radius 1
```

・・・RADIUS サーバー関連の設定(プライマリ) (必須)

※ この例では、INDEX1 の RADIUS を Web 認証のプライマリとしています。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# web-authentication port 23-24 gateway
```

・・・Gateway 認証ポートの指定(23-24) (必須)

```
(config-a-def)# web-authentication ip 10.1.10.100
```

```
(config-a-def)# web-authentication https-port 443
```

・・・認証URL(<https://10.1.10.100>) (必須)

スイッチに設定した IP アドレスと同一の IP を指定

```
(config-a-def)# logout aging-time 600 0 0 0
```

・・・ログアウト(エージング : 600 秒)

```
(config-a-def)# logout linkdown port 23-24 disable
```




・・・リンクダウンログアウトの無効(LAG 収容の為)

(config-a-def)# **roaming port 23-24 enable**

・・・ポート間ローミング機能の有効(LAG 収容の為)

(config)# **web-authentication enable**

・・・Web 認証機能の有効 (必須)

-  ゲートウェイ認証における制限事項は Access Defender における一般的な制限事項に準拠します。
-  一対多の NAT 機器が配下に存在する場合は動作しません。
-  認証状態を問わず、端末から本装置への通信(telnet, SNMP)が可能です。通信を制限したい場合は、telnet 及び SNMP のアクセス制限機能により、アクセス可能な端末を制限してください。(上位にルーティング可能な L3 機器がある場合はユーザーVLAN にアドレスを付与せずに対応)

6.6 ゲートウェイ認証構成例(中央拠点アクセス手前に適用)

クライアントと認証スイッチが別ネットワークに存在するようなケースではゲートウェイ認証方式により、認証環境の構成が出来ます。

構成例として、広域イーサや Internet VPN 経由の極小規模拠点を本社側にて認証する場合の設定例を紹介します。

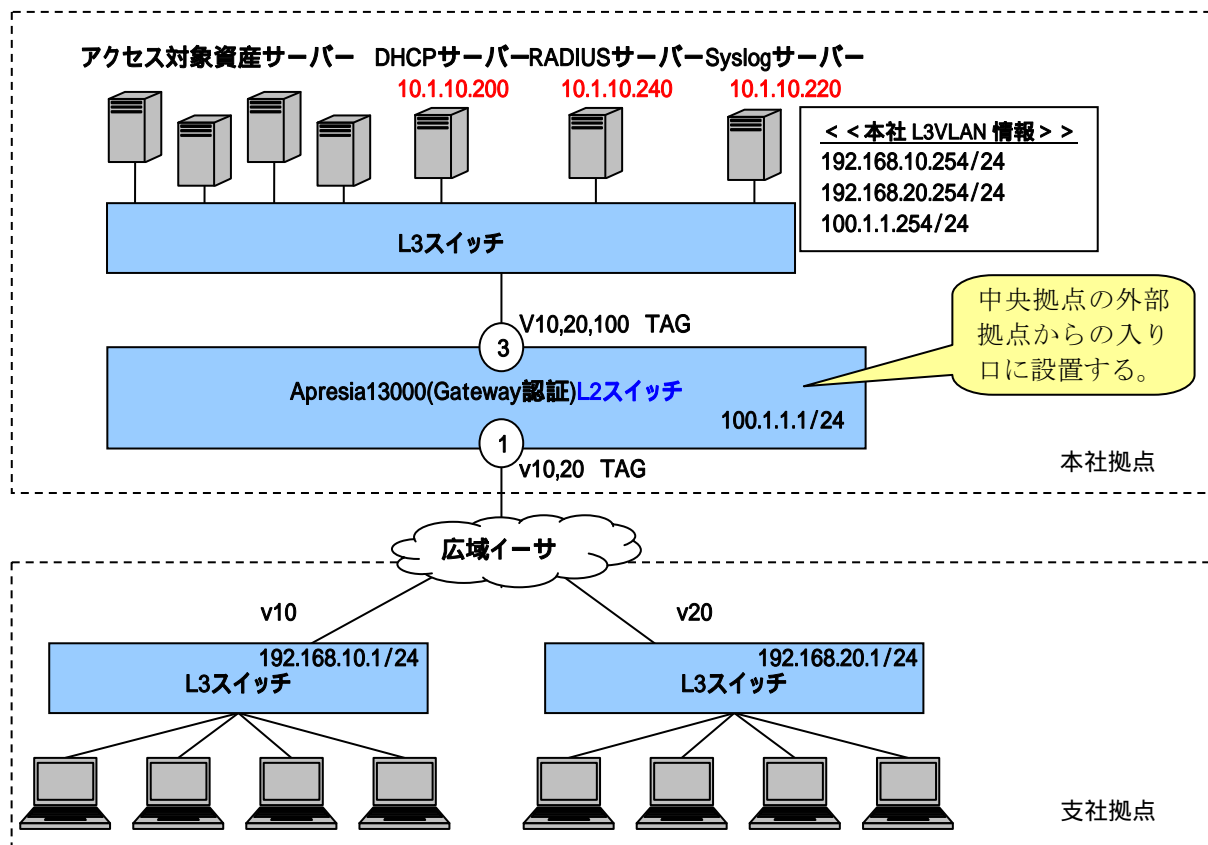


図 6-6 ゲートウェイ認証構成例(中央拠点アクセス構成)

図 6-6 の構成例でのGateway認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 10.1.10.220 local0 notice
    ... syslog サーバーの登録(優先度 notice 以上のログを送信)

(config)# packet-filter2
(config-filter)# 1 assign port 1-2
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
    ... packet-filter2 の設定(DHCP リレーの通信許可) (DHCP 環境では必須)

(config-filter)# 1 2 condition ipv4 src ip 192.168.10.0/24
(config-filter)# 1 2 action authentication-bypass
(config-filter)# 1 3 condition ipv4 src ip 192.168.20.0/24
```

```
(config-filter)# 1 3 action authentication-bypass
```

- ・・・WAN側の管理フレームを中継
想定されるフレーム：OSPF、RIP、VRRP、その他のスイッチ管理フレーム
その他、必要な通信を通信許可してください。

```
(config)# vlan database
```

```
(config-vlan)# vlan 10 name V10
```

```
(config-vlan)# vlan 20 name V20
```

```
(config-vlan)# vlan 100 name mgmt
```

- ・・・VLANの設定(管理用VLAN名は"mgmt")

```
(config)# interface port 1-2
```

```
(config-if-port)# description WAN
```

```
(config-if-port)# switchport mode trunk
```

```
(config-if-port)# switchport trunk add 10,20
```

- ・・・ポート1にVLAN10,20を適用(WAN接続用)
ポート2はPort障害時のバックアップ用

```
(config)# interface port 3
```

```
(config-if-port)# description honsya-L3
```

```
(config-if-port)# switchport mode trunk
```

```
(config-if-port)# switchport trunk add 10,20,100
```

- ・・・Port1にVLAN10,20,100を適用(本社L3スイッチ接続用)

```
(config)# interface vlan 100
```

```
(config-if)# ip address 100.1.1.1/24
```

- ・・・VLAN10にIPアドレスを設定

```
(config)# ip route 0.0.0.0/0 100.1.1.254
```

```
(config)# aaa radius 1 host 10.1.10.240 key apresia
```

```
(config)# aaa authentication web radius 1 force
```

- ・・・認証データベースにRadius1を使用し応答がなければ強制認証を動作

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

- ・・・最大認証端末(128台) (必須)
※この例では、128台を最大としています。

```
(config-a-def)# web-authentication port 1-2 gateway
```

- ・・・ゲートウェイ認証ポートの指定 (必須)

```
(config-a-def)# web-authentication redirect url https://100.1.1.1:443
```

```
(config-a-def)# web-authentication redirect http
```

```
(config-a-def)# web-authentication redirect proxy-port 8080
```

- ・・・ 認証ページリダイレクト機能の設定
 - ※http80, proxy8080 宛の通信があった場合に Web 認証画面を表示
 - ※プロキシ環境の場合、ブラウザの設定はプロキシポートを 8080 にし

て

100.1.1.1 はプロキシ除外設定としてください。
※プロキシ環境ではない場合、HTTP 80 の通信があればリダイレクトされます。

```
(config-a-def)# web-authentication ip 100.1.1.1
(config-a-def)# web-authentication https-port 443
    ・・・ 認証URL (https://100.1.1.1/443) (必須)
```

```
(config-a-def)# logout aging-time 600 0 0 0
    ・・・ ログアウト(エージング : 600 秒)
```

```
(config-a-def)# logout linkdown port 1-2 disable
    ・・・ リンクダウンログアウトの無効
    ユーザーのログアウト状態とリンクダウンは関係ないため推奨
```

```
(config-a-def)# roaming port 1-2 enable
    ・・・ ポート間ローミング機能の有効
    バックアップポートへの認証状態引継のため推奨
```

```
(config)# web-authentication enable
    ・・・ Web 認証機能の有効(必須)
```

6.7 802.1X認証構成例

802.1X の設定例を説明します。

APRESIA の認証ポート直結により 802.1X 認証をすることも可能ですが、APRESIA の認証ポート配下に EAP 透過型のスイッチ(もしくはダムハブ)を接続し、サブリカントを複数台収容、かつ、サブリカント毎に個別認証することも可能です。

また、RADIUS サーバーにトンネル属性を設定することにより、認証時にユーザー(端末)毎に動的に VLAN を割り当てることが可能になります。

認証前の端末は、APRESIA の認証ポートによって通信が完全に制限されているため、APRESIA のポートを経由して他の端末との通信はできません。ただし、EAP フレームを中継(EAP 透過)するスイッチ(もしくはダムハブ)内での通信はその限りではありません。

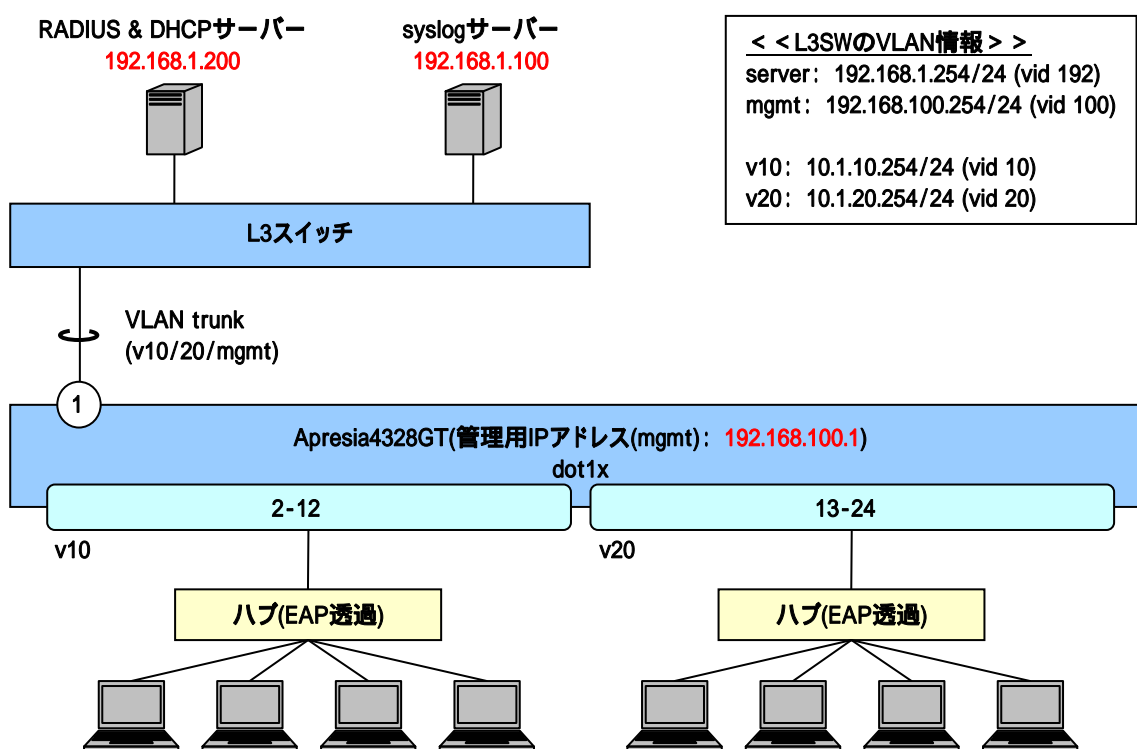


図 6-7 802.1X 構成例

図 6-7 の 802.1X 構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 notice
    ... syslog サーバーの登録(優先度 notice 以上のログを送信)

(config)# vlan database
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 20 name v20
(config-vlan)# vlan 100 name mgmt
    ... VLAN の設定(管理用 VLAN 名は"mgmt")
```

```
(config)# interface port 1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10,20,100
```

・・・Uplink ポートの設定

```
(config)# interface port 2-12
(config-if-port)# switchport access vlan 10
(config)# interface port 13-24
(config-if-port)# switchport access vlan 20
```

・・・VLAN のポートアサイン設定

```
(config)# interface vlan 100
(config-if)# ip address 192.168.100.1/24
```

・・・管理用 VLAN のアドレス設定

```
(config)# ip route 0.0.0.0/0 192.168.100.254
```

・・・デフォルトルートの設定

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication dot1x radius 1
```

・・・802.1X 認証用の RADIUS サーバーの登録 (必須)

※ 他の認証方式と合わせて最大 8 台まで登録可能ですが、
802.1X 用としては 2 台まで登録可能です。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大クライアントサポート数の設定 (必須)

```
(config-a-def)# dot1x port 2-24
```

・・・認証ポートの設定 (必須)

```
(config-a-def)# dot1x port 2-24 reauthentication
```

・・・再認証有効設定

```
(config)# dot1x enable
```

・・・802.1X 認証の有効化 (必須)

6.8 802.1X/MAC認証構成例

802.1X/MAC の設定例を説明します。この場合、802.1X 認証の設定に加え 802.1X/MAC 認証機能を有効にする設定項目を入力する必要があります。

802.1X 認証と同様に、APRESIA の認証ポート配下に EAP 透過型のスイッチ(もしくはダムハブ)を接続し、サブリカントを複数台収容、かつ、サブリカント毎に個別認証することも可能です。

また、RADIUS サーバーにトンネル属性を設定することにより、認証時にユーザー(端末)毎に動的に VLAN を割り当てることが可能になります。

認証前の端末は、APRESIA の認証ポートによって通信が完全に制限されているため、APRESIA のポートを経由して他の端末との通信はできません。ただし、EAP フレームを中継(EAP 透過)するスイッチ(もしくはダムハブ)配下の端末間通信はこの限りではありません。

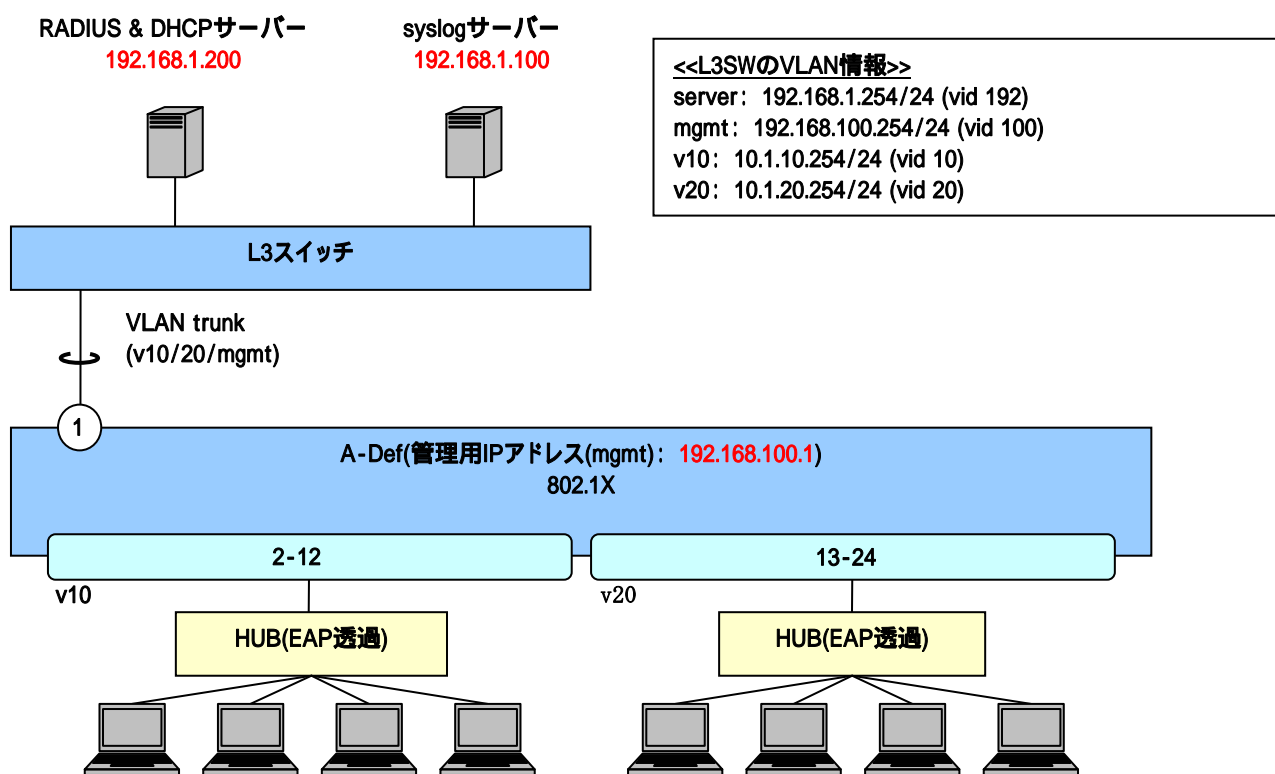


図 6-8 802.1X/MAC 構成例

図 6-8 の 802.1X構成例での認証スイッチの代表的な設定例を示します。(VLAN、インターフェース構成などは図 6-7 と同一のため、設定例は省きます)

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication dot1x radius 1
```

- ・・・802.1X 認証用の RADIUS サーバーの登録 (必須)
- ※ 他の認証方式と合わせて最大 8 台まで登録可能ですが、802.1X 用としては 2 台まで登録可能です。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```


・・・最大認証端末(128 台) (必須)

```
(config-a-def)# dot1x port 2-24
```

・・・認証ポートの設定 (必須)

```
(config-a-def)# dot1x port 2-24 reauthentication
```

・・・再認証有効設定

```
(config-a-def)# dot1x mac-authentication-password 1q2w3e
```

・・・802.1X/MAC 認証用のパスワード設定および、有効化 (必須)

```
(config)# dot1x enable
```

・・・802.1X 認証の有効化 (必須)

6.9 DHCPスヌーピング構成例

AccessDefender での DHCP スヌーピング設定例を説明します。

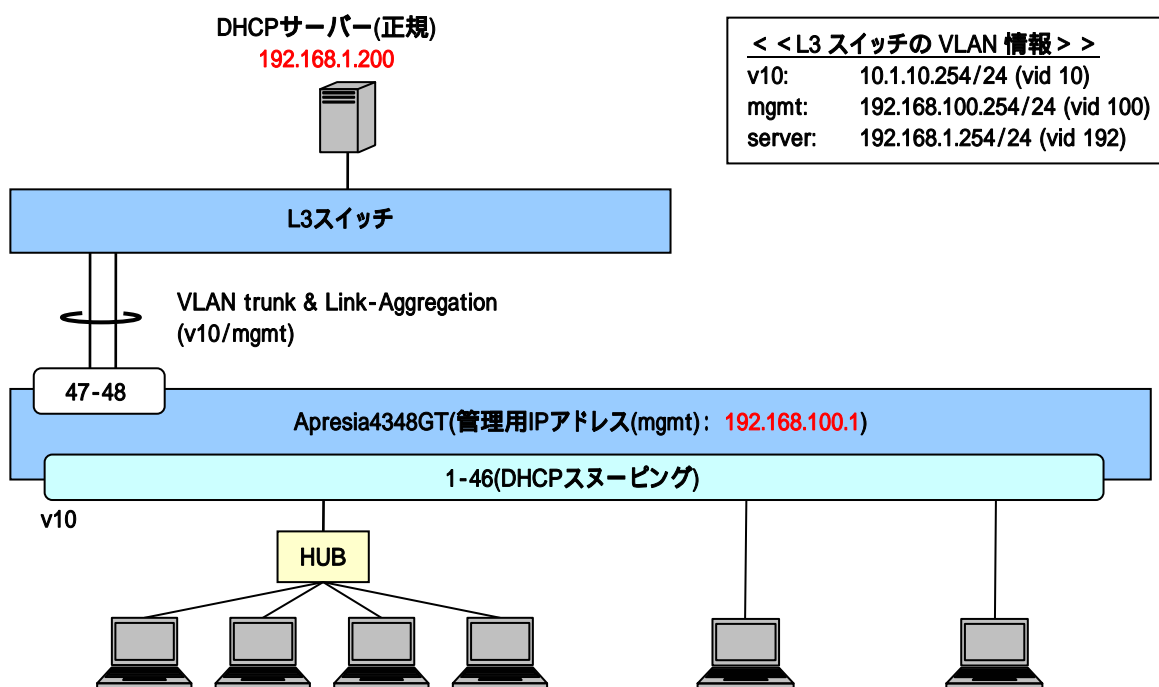


図 6-9 DHCP スヌーピング構成例

図 6-9 の構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 info
    ... syslog サーバーの登録(優先度 info 以上のログを送信)

(config)# vlan database
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 100 name mgmt
    ... VLAN の設定(管理用 VLAN 名は"mgmt")

(config)# interface port 1-44
(config-if-port)# switchport access vlan 10
(config)# interface port 45-46
(config-if-port)# media utp
(config-if-port)# switchport access vlan 10
    ... VLAN10 を access ポートとして設定

(config)# interface port 47-48
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10,100
(config-if-port)# link-aggregation 1
```

・・・Uplink ポートの設定

```
(config)# interface vlan 100
```

```
(config-if)# ip address 192.168.100.1/24
```

・・・管理用 VLAN(mgmt)のアドレス設定

```
(config)# interface vlan 10
```

```
(config-if)# ip address 10.1.10.1/24
```

・・・VLAN10(vid10)のアドレス設定

```
(config)# ip route 0.0.0.0/0 192.168.100.254
```

・・・デフォルトルートの設定

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# dhcp-snooping port 1-46
```

・・・DHCP スヌーピングを実施するポート番号を指定(1-46) (必須)

```
(config-a-def)# dhcp-snooping mode timer 600
```

・・・自動的に DENY モードに切り替わるまでの時間を設定

```
(config)# dhcp-snooping enable
```

・・・DHCP スヌーピングの有効化 (必須)

6.10 DHCPスヌーピング/MAC認証(固定/動的VLAN)の混在環境構成例

DHCP スヌーピングと MAC 認証(固定 VLAN)を混在させる場合の設定例を説明します。

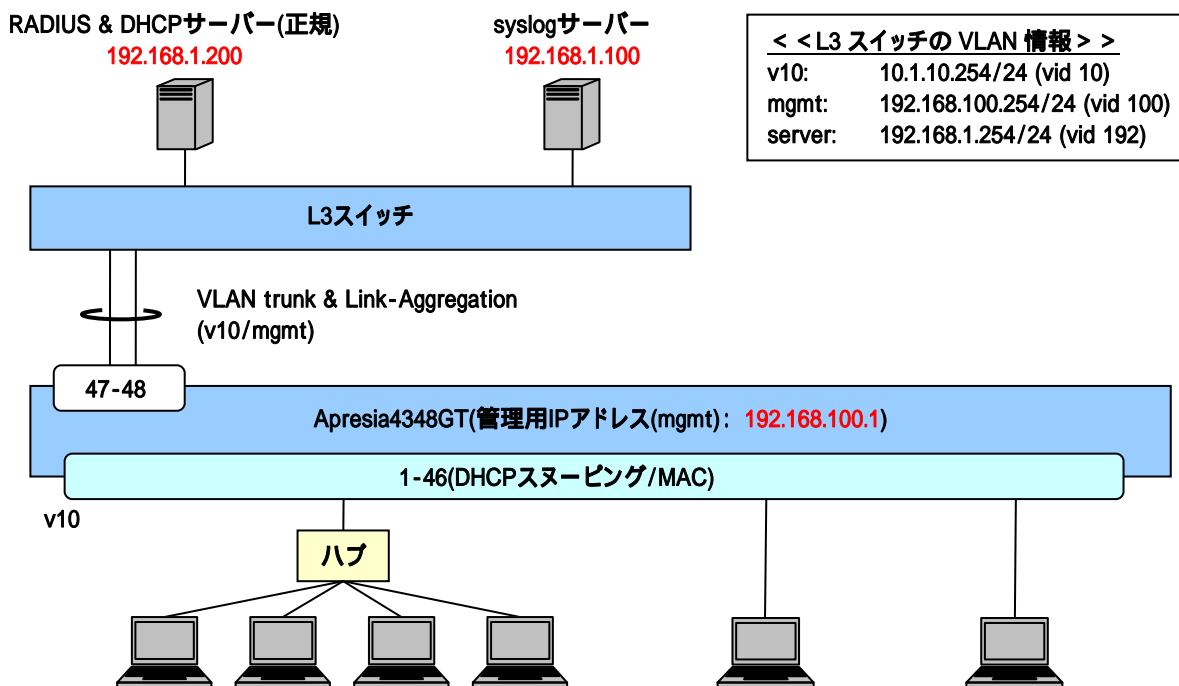


図 6-10 DHCP スヌーピングと MAC 認証の併用構成例

図 6-10 の構成例での認証スイッチの代表的な設定例を示します(VLAN、インターフェース構成などは図 6-9 と同一のため、設定例は省きます)

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication mac radius 1
```

・・・RADIUS サーバー関連の設定(プライマリ) (MAC 認証時必須)

※ この例では INDEX1 の RADIUS をプライマリ認証サーバーとしています。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# dhcp-snooping port 1-46
```

・・・DHCP スヌーピングを実施するポート番号を指定(1-46) (必須)

```
(config-a-def)# dhcp-snooping mode timer 600
```

・・・自動的に DENY モードに切り替わるまでの時間を設定

```
(config-a-def)# mac-authentication port 1-46
```


・・・MAC 認証ポート(1-46) (MAC 認証時必須)

```
(config-a-def)# mac-authentication password 1q2w3e
    . . . MAC 認証用のパスワード設定 (MAC 認証時必須)
```

```
(config-a-def)# logout aging-time 300
    . . . ログアウト(エージング : 300 秒)
```

```
(config)# dhcp-snooping enable
```

```
(config)# mac-authentication enable
    . . . DHCP スヌーピング/MAC 認証の有効化 (必須)
```

 DHCP スヌーピングと MAC 認証を混在させる場合、MAC 認証は固定 VLAN モード、動的 VLAN モードとも同様の構成となります。

6.11 DHCPスヌーピング/Web認証(固定VLAN)の混在環境構成例

DHCP スヌーピングと Web 認証(固定 VLAN) を混在させる場合の設定例を説明します。

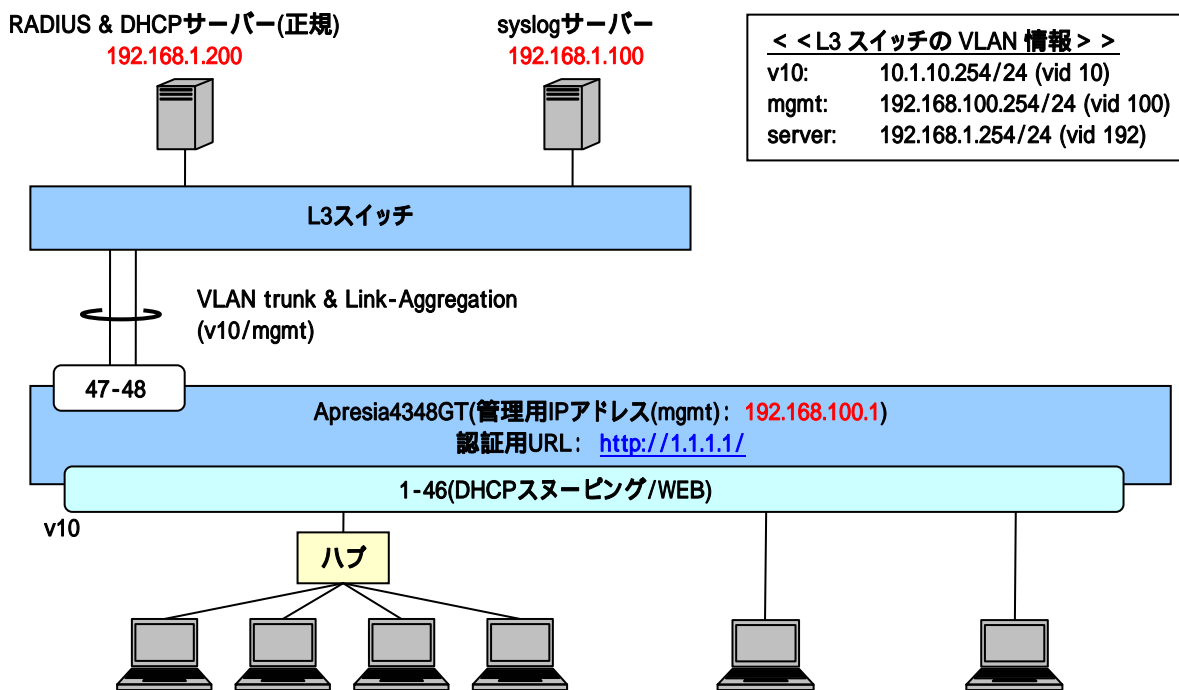


図 6-11 の構成例での認証スイッチの代表的な設定例を示します(VLAN、インターフェース構成などは図 6-9 と同一のため、設定例は省きます)

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
```

```
(config)# aaa authentication web radius 1
```

・・・RADIUS サーバー関連の設定(プライマリ) (Web 認証時必須)

※ この例では、INDEX1 の RADIUS をプライマリ認証サーバーとしています。

す。

```
(config)# access-defender
```

```
(config-a-def)# packet-filter2 max-rule 128
```

・・・最大認証端末(128 台) (必須)

※ この例では、128 台を最大としています。

```
(config-a-def)# dhcp-snooping port 1-46
```

・・・DHCP スヌーピングを実施するポート番号を指定(1-46) (必須)

```
(config-a-def)# dhcp-snooping mode timer 600
```

・・・自動的に DENY モードに切り替わるまでの時間を設定

```
(config-a-def)# web-authentication port 1-46
```

・・・Web 認証ポート(1-46) (Web 認証時必須)

```
(config-a-def)# web-authentication ip 1.1.1.1
```

```
(config-a-def)# web-authentication http-port 80
```

・・・認証 URL(http://1.1.1.1/) (Web 認証時必須)

```
(config-a-def)# logout aging-time 300
```

・・・ログアウト(エージング : 300 秒)

```
(config)# dhcp-snooping enable
```

```
(config)# web-authentication enable
```

・・・DHCP スヌーピング/Web 認証の有効化 (必須)

-
- ❗ DHCP スヌーピング機能で DHCP パケットを正規 DHCP サーバーに中継するため、Web 認証前に DHCP 通信を許可するための認証バイパス設定は不要です。
 - ❗ 端末の ARP フレームは DHCP スヌーピング登録後、自動的に許可されます。
 - ❗ DHCP サーバー機能併用時、DHCP パケットは中継されません。そのため、異なった VLAN インターフェイスで各機能を有効にした場合、DHCP サーバー機能と DHCP スヌーピング機能は併用できません。

6.12 DHCPスヌーピング/Web 認証(動的VLAN)の混在環境構成例

DHCP スヌーピングと Web 認証(動的 VLAN) を混在させる場合の設定例を説明します。

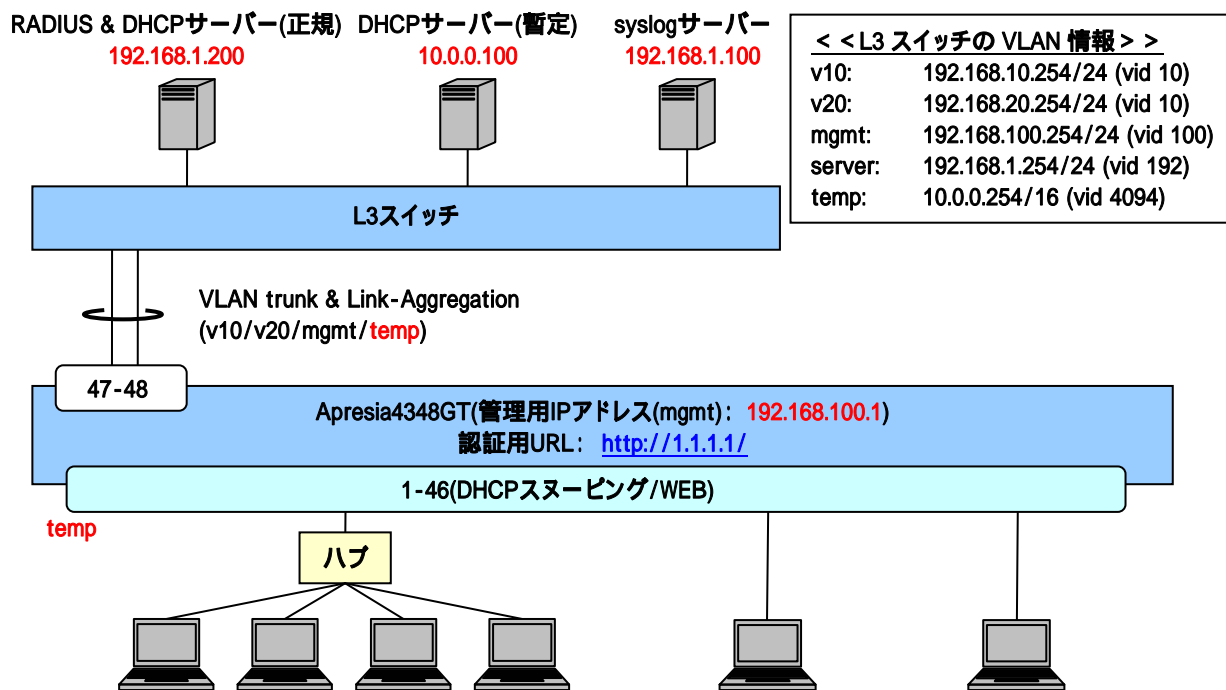


図 6-12 DHCP スヌーピングと Web 認証(動的 VLAN) の併用構成例

図 6-12 の構成例での認証スイッチの代表的な設定例を示します。

```
(config)# logging ip 192.168.1.100 local0 info
    ... syslog サーバーの登録(優先度 info 以上のログを送信)

(config)# vlan database
(config-vlan)# vlan 10 name v10
(config-vlan)# vlan 20 name v20
(config-vlan)# vlan 100 name mgmt
(config-vlan)# vlan 4094 name temp
    ... VLAN の設定
    (管理用 VLAN を"mgmt"、ユーザーVLAN を"v10, v20"、暫定 VLAN を"temp"とする)

(config)# interface port 1-44
(config-if-port)# switchport access vlan 4094
(config)# interface port 45-46
(config-if-port)# media utp
(config-if-port)# switchport access vlan 4094
    ... 暫定 VLAN を access ポートとして設定

(config)# interface port 47-48
```



```
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10,20,100,4094
(config-if-port)# link-aggregation 1
    . . . Uplink ポートの設定 (想定される全 VLAN を Trunk 設定しておく)
```

```
(config)# interface vlan 10
(config-if)# ip address 192.168.10.1/24
(config)# interface vlan 20
(config-if)# ip address 192.168.20.1/24
(config)# interface vlan 100
(config-if)# ip address 192.168.100.1/24
(config)# interface vlan 4094
(config-if)# ip address 10.0.0.1/16
    . . . 管理用 VLAN (mgmt) とユーザー VLAN (v10, 20)、暫定 VLAN (temp) の
        アドレス設定
```

```
(config)# ip route 0.0.0.0/0 192.168.100.254
    . . . デフォルトルートの設定
```

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication web radius 1
    . . . RADIUS サーバー関連の設定 (プライマリ) (Web 認証時必須)
        ※ この例では、INDEX1 の RADIUS をプライマリ認証サーバーとしています。
```

```
(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
    . . . 最大認証端末 (128 台) (必須)
        ※ この例では、128 台を最大としています。
```

```
(config-a-def)# dhcp-snooping port 1-46
    . . . DHCP スヌーピングを実施するポート番号を指定 (1-46) (必須)
```

```
(config-a-def)# dhcp-snooping mode timer 600
    . . . 自動的に DENY モードに切り替わるまでの時間を設定
```

```
(config-a-def)# web-authentication port 1-46
    . . . Web 認証ポート (1-46) (Web 認証時必須)
```

```
(config-a-def)# web-authentication ip 1.1.1.1
(config-a-def)# web-authentication http-port 80
    . . . 認証 URL (http://1.1.1.1/) (Web 認証時必須)
```

```
(config-a-def)# logout aging-time 300
    . . . ログアウト (エージング : 300 秒)
```

```
(config)# dhcp-snooping enable
```

```
(config)# web-authentication enable
```

・・・ DHCP スヌーピング/Web 認証の有効化 (必須)

- ❗ DHCP スヌーピング機能で DHCP パケットを正規 DHCP サーバーに中継するため、Web 認証前に DHCP 通信を許可するための認証バイパス設定は不要です。
- ❗ 端末の ARP フレームは DHCP スヌーピング登録後、自動的に許可されます。
- ❗ 認証 URL にアクセスする際、暫定 VLAN 上で ARP を許可する必要があるため、暫定 VLAN も DHCP スヌーピングを有効にする必要があります。
- ❗ 暫定 DHCP サーバーは暫定 VLAN に設置し、暫定 DHCP サーバーと正規 DHCP サーバーは同一サーバー上ではなく、サーバーを分けて設置してください。
- ❗ DHCP サーバー機能併用時、DHCP パケットは中継されません。そのため、異なった VLAN インターフェースで各機能を有効にした場合、DHCP サーバー機能と DHCP スヌーピング機能は併用できません。

7. 応用設定

7.1 認証ページのカスタマイズ

7.1.1 APRESIA内部ページのカスタマイズ

AccessDefender では、ログイン認証ページ、認証成功ページ、認証失敗ページ、ログアウト成功ページ、ログアウト失敗ページ、リダイレクト失敗ページの各ページをカスタマイズすることが出来ます。

下記コマンドを用いて、カスタマイズしたページを本装置に保存します。erase コマンドを使用して保存した Web ページを削除した場合は、デフォルトページ(工場出荷時の状態)が使用されます。

# copy tftp <IP-ADDRESS> <FILENAME> <login-page login-success-page login-failure-page logout-success-page logout-failure-page redirect-error-page>	
. . . IP-ADDRESS	TFTP サーバーの IP アドレス
. . . FILENAME	ファイル名
. . . login-page	ログイン認証ページ
. . . login-success-page	認証成功ページ
. . . login-failure-page	認証失敗ページ
. . . logout-success-page	ログアウト成功ページ
. . . logout-failure-page	ログアウト失敗ページ
. . . redirect-error-page	リダイレクト失敗ページ

APRESIA 内部の認証ページをカスタマイズするポイントは以下です。デフォルトの画面は実際に表示されるページのソースを参照してください(各ファイル最大 5,120 バイト)。

- ユーザー名、パスワードの変数名をそれぞれ name、pass にする
- form の method を POST に指定する

<ログイン用の form 例>

```
<form method="POST" action="/cgi-bin/adefflogin.cgi">
<table>
<tr><th width="184">ユーザーアカウント</th><td width="220">
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">パスワード</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<input type="submit" value="login">
<input type="reset" value="reset">
</form>
```

<ログアウト用の form 例>

```
<form method="POST" action="/cgi-bin/adefflogout.cgi">
<input type="submit" value="logout">
</form>
```

7.1.2 外部Webサーバー上の任意のページへの埋め込み

AccessDefender で使用する認証用のフォームを APRESIA 外部のページに埋め込む方法です。

APRESIA のユーザー認証用 CGI 本体は装置内部のファームウェアに実装されているため、CGI そのものを別サーバーで実行することはできませんが、ユーザー認証ページの form の action を「/cgi-bin/adefflogin.cgi」から「http:// AccessDefender 認証用 IP アドレス:port/cgi-bin/adefflogin.cgi」に変更することで外部の Web サーバー上の任意のページでユーザー認証ページを表示・実行することが可能となります。(SSL 有効時には「https:// AccessDefender 認証用 IP アドレス:port/cgi-bin/adefflogin.cgi」)

ポイントは以下です。

- form の action を APRESIA の認証 CGI に指定する
- ユーザー名、パスワードの変数名をそれぞれ name、pass にする
- form の method を POST に指定する
- 未認証端末から外部の Web サーバーに対する通信を許可しておく
- 認証 URL が FQDN(Fully Qualified Domain Name) の場合には DNS サーバーへの通信も許可しておく

認証 URL の設定が「http://1.1.1.1:8080/」の場合に外部のページに埋め込むフォームの例を示します。

<ログイン用の form 例>

```
<form method="POST" action="http://1.1.1.1:8080/cgi-bin/adefflogin.cgi">
<table>
<tr><th width="184">ユーザーアカウント</th>
<td width="220">
<input name="name" type="text" value="" size="30" maxlength="63">
</td></tr>
<tr><th width="184">パスワード</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63">
</td></tr>
</table>
<input type="submit" value="login">
<input type="reset" value="reset">
</form>
```

<ログアウト用の form 例>

```
<form method="POST" action="http://1.1.1.1:8080/cgi-bin/adefflogout.cgi">
<input type="submit" value="logout">
</form>
```

7.1.3 認証方法選択機能の認証ページカスタマイズ

3.5 認証方法選択機能(Web認証のみ)用にAPRESIA内部の認証ページをカスタマイズするポイントは以下です。デフォルトの画面は実際に表示されるページのソースを参照してください(最大ファイルサイズは 5,120 バイト)。

- ・ ユーザー名、パスワードの変数名をそれぞれ name、pass にします。
- ・ 認証 ID の変数名を authid にします。type はご利用の環境に合わせて指定してください。
- ・ form の method を POST に指定します。

〈認証方法選択用の form 例(ユーザー選択型)〉

```
<form method="POST" action="/cgi-bin/adefflogin.cgi">
<table>
<tr><th width="184">ユーザーアカウント</th><td width="220">
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">パスワード</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<tr><th width="184">認証方法の選択</th><td width="220">
<input type="radio" name="authid" value="1">認証方法 1<br>
<input type="radio" name="authid" value="2">認証方法 2<br>
<input type="radio" name="authid" value="3">認証方法 3<br>
<input type="radio" name="authid" value="4">認証方法 4<br>
</td></tr>
<input type="submit" value="login">
<input type="reset" value="reset">
</form>
```

〈ログイン用の form 例(埋め込み型)〉

```
<form method="POST" action="http://1.1.1.1:8080/cgi-bin/adefflogin.cgi">
<table>
<tr><th width="184">ユーザーアカウント</th><td width="220">
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">パスワード</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<input type="hidden" name="authid" value="2">
<input type="submit" value="login">
<input type="reset" value="reset">
</form>
```

7.2 ユーザー認証時の持ち込み端末制限

Web 認証によるユーザー認証時に、ユーザーが使用している端末の MAC アドレスを同時に確認することにより、持ち込み端末を制限することが可能です。RADIUS の Calling-Station-Id 属性を使用します。

ユーザー名とパスワードと MAC アドレスの組み合わせによる認証方法となります。

- そのユーザーは指定された端末でのみ認証可能(1 対 1)
- RADIUS サーバーに Calling-Station-Id の設定が必要です。APRESIA への特別な設定は不要です。

下図の例の場合、「userA」は、「aa:aa:aa:aa:aa:aa」の端末でしか認証されません。

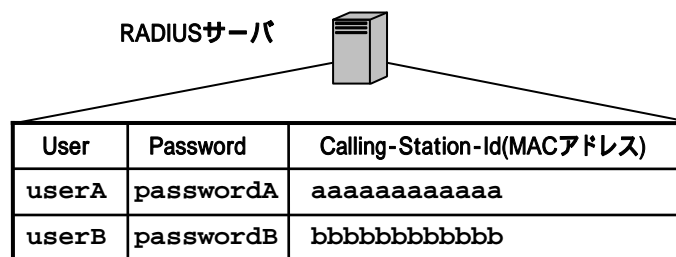


図 7-1 Calling-Station-Id 属性による認証の場合のユーザーデータベース

- ❗ 1 つのユーザーエントリに対して複数の Calling-Station-Id 属性を設定可能な RADIUS サーバーを使用する場合は、登録されている複数の端末の内いずれかを使用すれば認証成功します。

7.3 NAS(Network Access Server)属性

認証時に、NAS(Network Access Server)の属性を使用して、ユーザーがアクセス可能なネットワークを制限することが可能です。

現在サポートしている属性としては「NAS-IP-address」と「NAS-Port」および「NAS-identifier」があります。それぞれの属性を使用した場合のアクセス制限について概要を説明します。

7.3.1 NAS-IP-address

「NAS-IP-address」属性の値は、端末がアクセスしている装置(スイッチングハブ)の IP アドレスになります。実際の値は APRESIA の管理 IP アドレスが設定されます。

! RADIUS サーバーに NAS-IP-Address の設定が必要です。APRESIA への特別な設定は不要です。

図 7-2 の例では、以下のような動作になります。

- userA は、172.16.10.1 の管理 IP アドレスを持つ装置でのみ認証される。
- userB は、172.16.10.2 の管理 IP アドレスを持つ装置でのみ認証される。

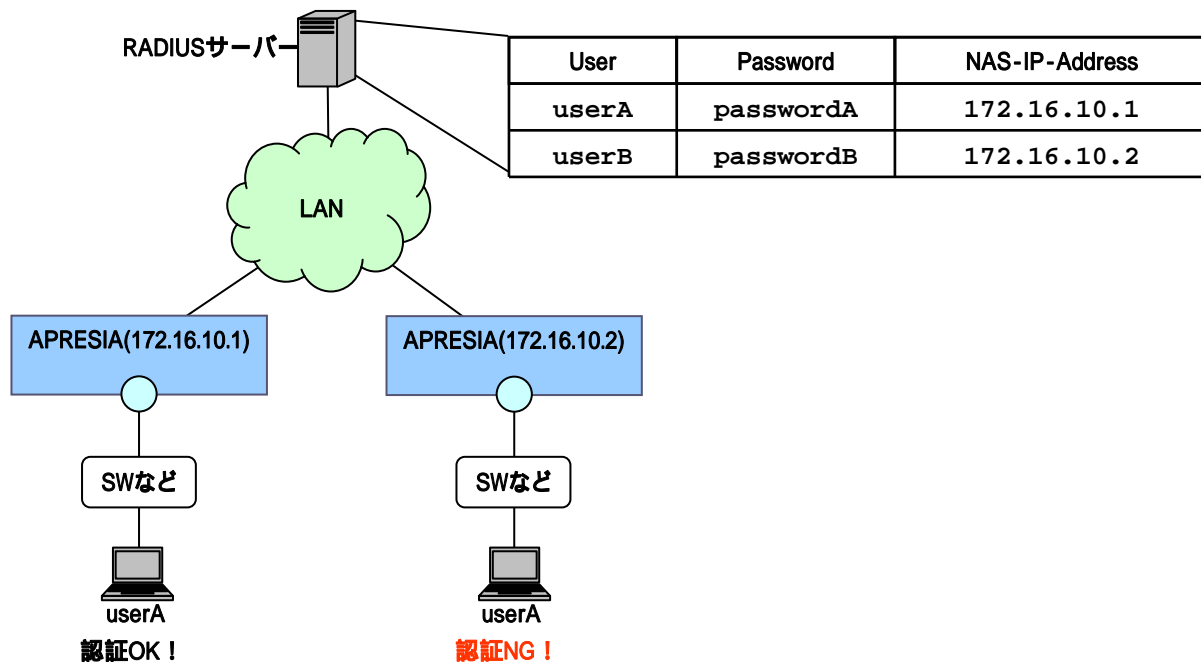


図 7-3 NAS-IP-address 設定時のアクセス制限

7.3.2 NAS-identifier

「NAS-identifier」属性の値は、端末がアクセスしている装置(スイッチングハブ)の該当ポートの VLAN ID(VID)になります。

! RADIUS サーバーに NAS-Identifier の設定が必要です。APRESIA への特別な設定は不要です。

下図の例では、以下のような動作になります。

- userA は、VID : 1010 のネットワークでのみ認証される。
- userB は、VID : 1020 のネットワークでのみ認証される。

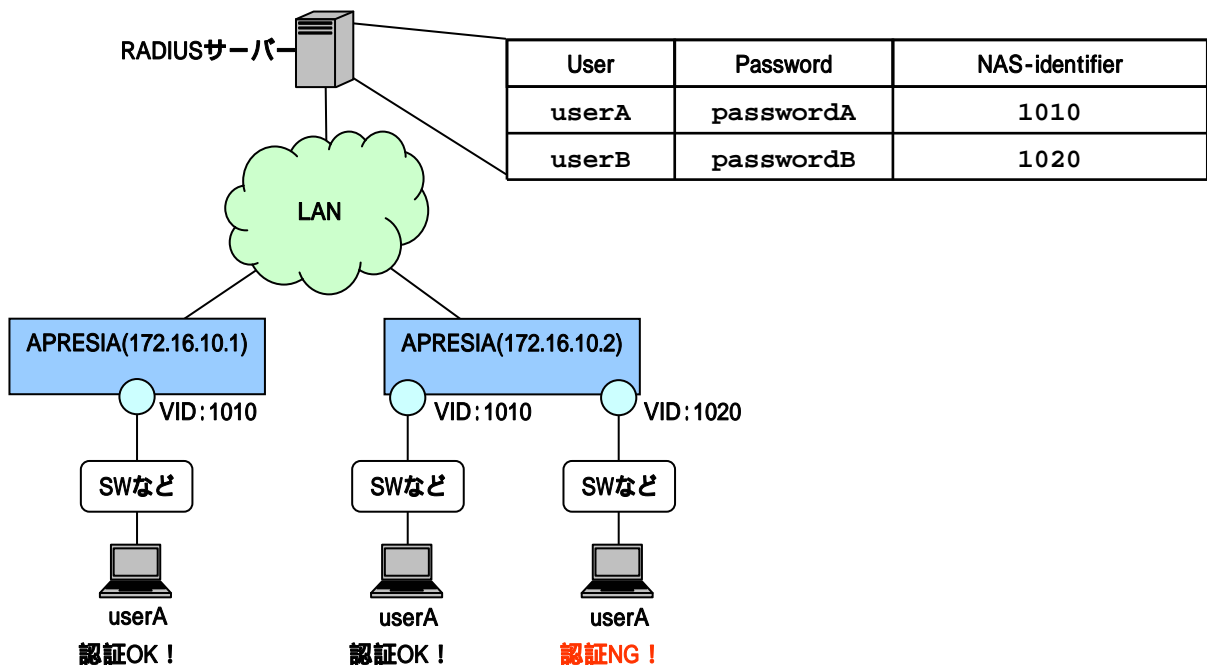


図 7-4 NAS-identifier 設定時のアクセス制限

7.3.3 NAS属性の組み合わせ

認証制限として下記の NAS 属性の組み合わせもサポートします。

- ❗ RADIUS サーバーに NAS-IP-Address 及び NAS-Identifier の設定が必要です。APRESIA への特別な設定は不要です。
- ❗ NAS-Port 属性を併用する場合も同様の手法で設定可能です。

下図の例では、以下のような動作になります。

- userA は、172.16.10.1 の管理 IP アドレスを持つ装置で、かつ VID : 1010 のネットワークのみで認証される。
- userB は、172.16.10.2 の管理 IP アドレスを持つ装置で、かつ VID : 1020 のネットワークのみで認証される。

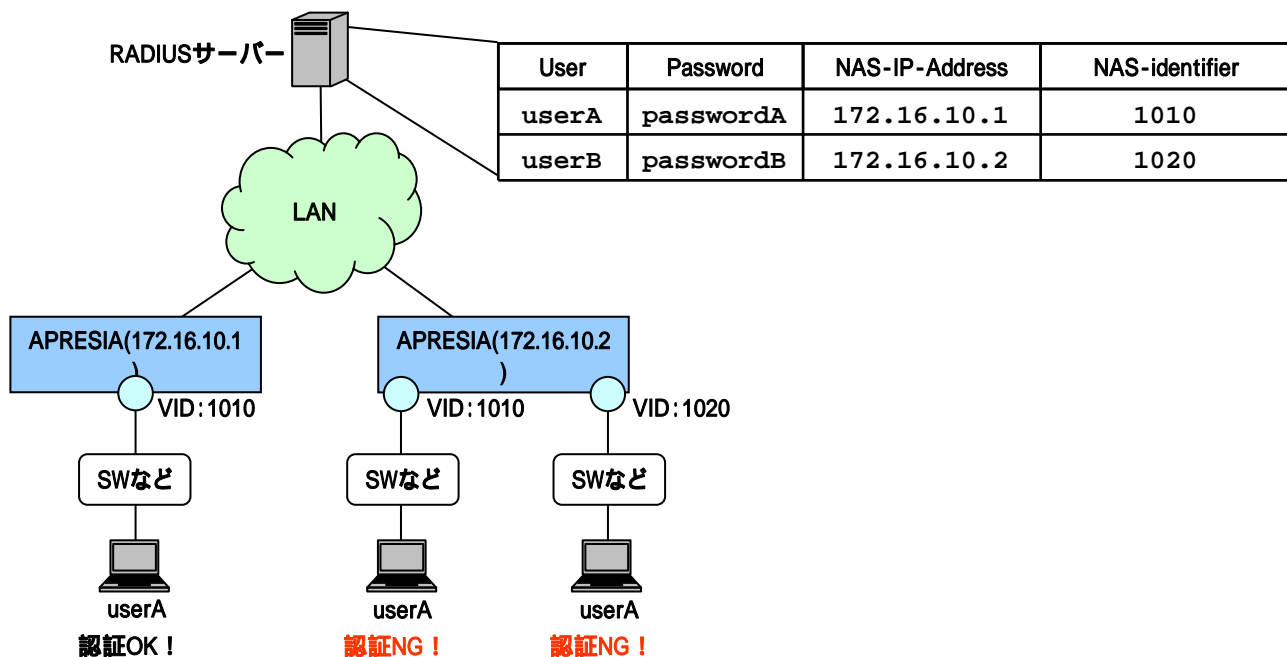


図 7-5 NAS-IP-address+NAS-identifier 組合せ設定時のアクセス制限

7.4 MACアドレスの自動収集

ユーザー端末のMACアドレスにより持ち込み端末の接続を制限するケース(例 7.2 ユーザー認証時の持ち込み端末制限)において、各端末のMACアドレスを収集する手段は様々ありますが、AccessDefender認証の「MAC認証」と「強制認証機能」を組み合わせると容易に各端末のMACアドレスを収集することが可能となります。図 7-6 に構成例を示します。

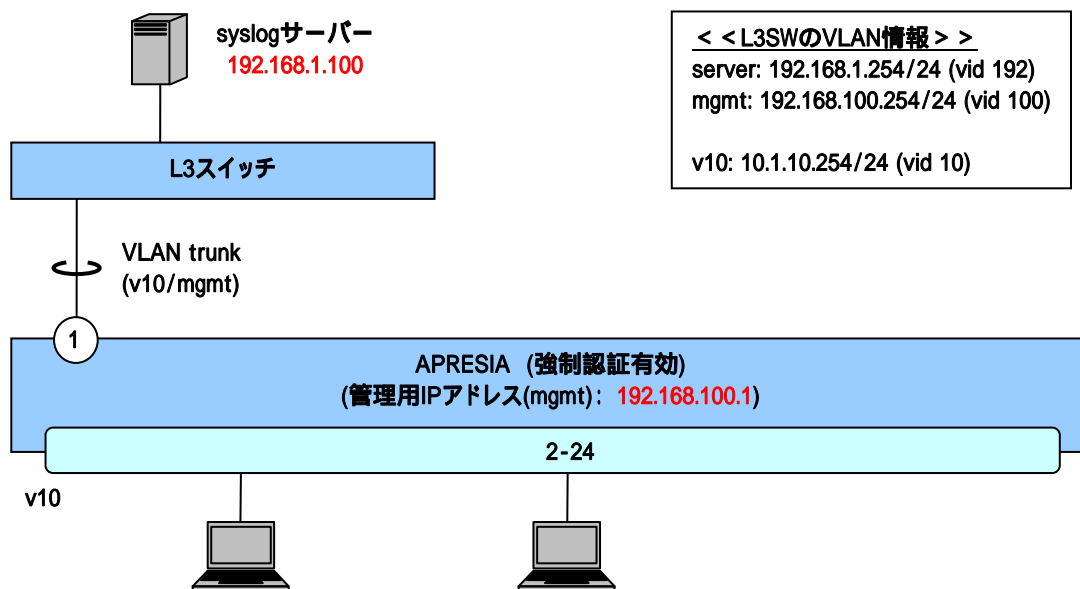


図 7-6 強制認証機能を使用した MAC アドレス自動収集

必要となる設定は、syslog サーバーと MAC 認証(強制認証有効)です。強制的に認証成功させるため、RADIUS サーバーの設定は必要ありません。また MAC 認証用のパスワードの設定も不要です。

最低限必要な設定を以下に示します。

```
(config)# logging ip 192.168.1.100 local0 notice
... syslog サーバー設定

(config)# aaa authentication mac force
... MAC 認証の強制認証機能を有効

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 1024
... 最大認証端末の設定(この例では、1,024 台を最大としています)

(config-a-def)# mac-authentication port 2-24
... MAC 認証有効ポート(2-24)の設定

(config)# mac-authentication enable
... MAC 認証の有効化
```

syslog サーバーには、1 台の端末が認証される毎に下記のようなログが記録されます。このログから、どの端末がどの APRESIA のポートに接続されたかを把握することが可能です。

```
<process:notice> A-Def : force authentication succeeded : uid=00096b82c51e
<process:notice> A-Def : mac : login succeeded : uid=00096b82c51e
                                mac=00:09:6b:82:c5:1e ip=0.0.0.0 port=5 vid=10
```

! ユーザー名と MAC アドレスを合わせて収集したい場合には Web 認証と強制認証機能を組み合わせて下さい。ただし間違ったアカウントを入力しても強制認証機能により認証成功してしまうため注意して下さい。

7.5 未認証端末の packets 強制転送(認証バイパス)

7.5.1 認証バイパスの概要

許可されたユーザーや端末のみアクセス可能なネットワークを実現することがネットワーク認証導入の目的となります。しかし、Windows ドメイン認証や検疫機能など、特定の条件に該当する通信は認証状態にかかわらず通信を許可したいという運用上必要な相反する課題があります。

そこで、適切な設定によるセキュリティホール化の防止(セキュリティ強度の維持)と、セキュリティ強化が業務に支障を与えないことが必要となります。AccessDefender では、認証バイパスという機能を用いて、柔軟な条件設定とパケット制御でセキュリティ強度の維持と実運用に必要な通信の確保を高次元に両立することが可能となります。

運用上の要求としては下記 2 パターンが考えられ、それぞれ次のような制御が考えられます。

- 【パターン①】未認証通信許可
 - IP 電話は認証なしで通信したい MAC アドレスのベンダコードで許可
- 【パターン②】認証前通信許可
 - Web 認証前に DHCP から IP アドレスを取得したい UDP ポート番号で許可
 - 802.1X で認証する前に端末に GPO を適用したい 宛先 IP アドレスで許可
 - ※GPO(グループ・ポリシー・オブジェクト)

このように、認証バイパスを用いることにより、L1~L4 の情報と優先度を組み合わせ、きめ細かな設定が可能となります。なお、本方式ではパケットはハードウェア転送されます。

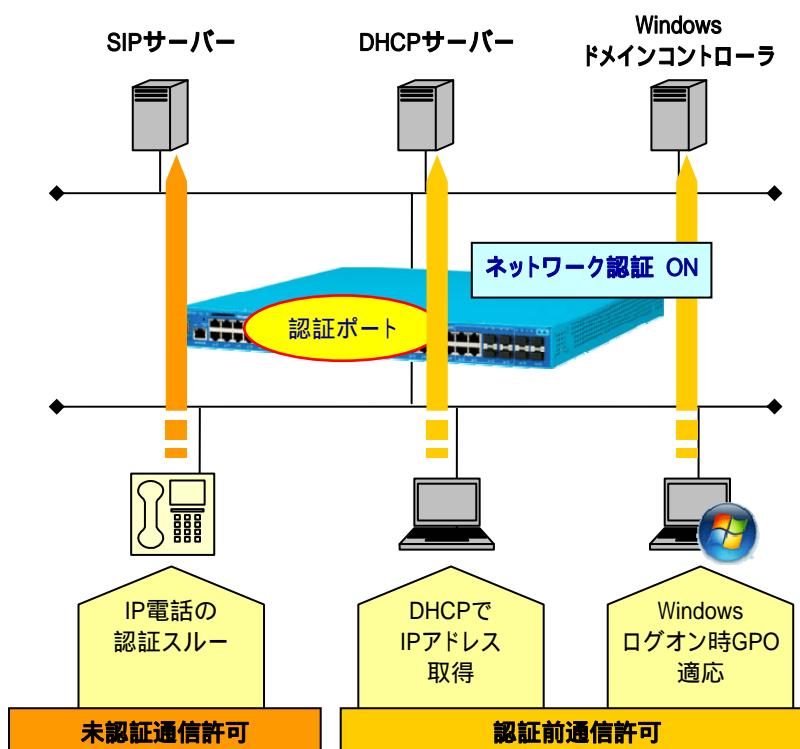


図 7-7 認証バイパス機能の概要

以下に、認証バイパスによる主な許可条件の一覧を示します。

受信パケットに対する識別条件(assign)によって、装置の受信パケットからパケットフィルター2 によるフィルタ対象パケットを識別し、フィルタ対象パケットとフィルタ条件(condition)を比較し、フィルタ条件を満たしたパケットに対して処理(action)を実行します。

識別条件に関する詳細については、コマンドリファレンスのパケットフィルター2 の項目を参照下さい。

表 7-1 認証バイパスの主な許可条件

仕様		AccessDefender 認証バイパス	備考
主なフィルタ条件	送信先	Ether Type VLAN ID MAC アドレス (マスク指定可能) IPv4 アドレス (マスク指定可能) IPv6 アドレス (マスク指定可能) TCP/UDP ポート番号 (レンジ指定可能)	
	送信元	Ether Type VLAN ID MAC アドレス (マスク指定可能) IPv4 アドレス (マスク指定可能) IPv6 アドレス (マスク指定可能) TCP/UDP ポート番号 (レンジ指定可能)	
	その他	TOS 関連 プロトコル TCP Flag (syn ack 等)	
その他仕様	優先度	1~14	ただし、利用環境により、他の機能による予約設定あり
	フィルタ適用範囲指定	ポート (レンジ指定可能) VLAN (マスク指定可能)	

7.5.2 認証バイパスによる強制転送設定例(1)

下記例のような要求に対する認証バイパスの設定例を記載します。

- 認証前に DHCP/DNS を通したい
- 認証 SW 配下の SW を管理したいが認証は除外したい

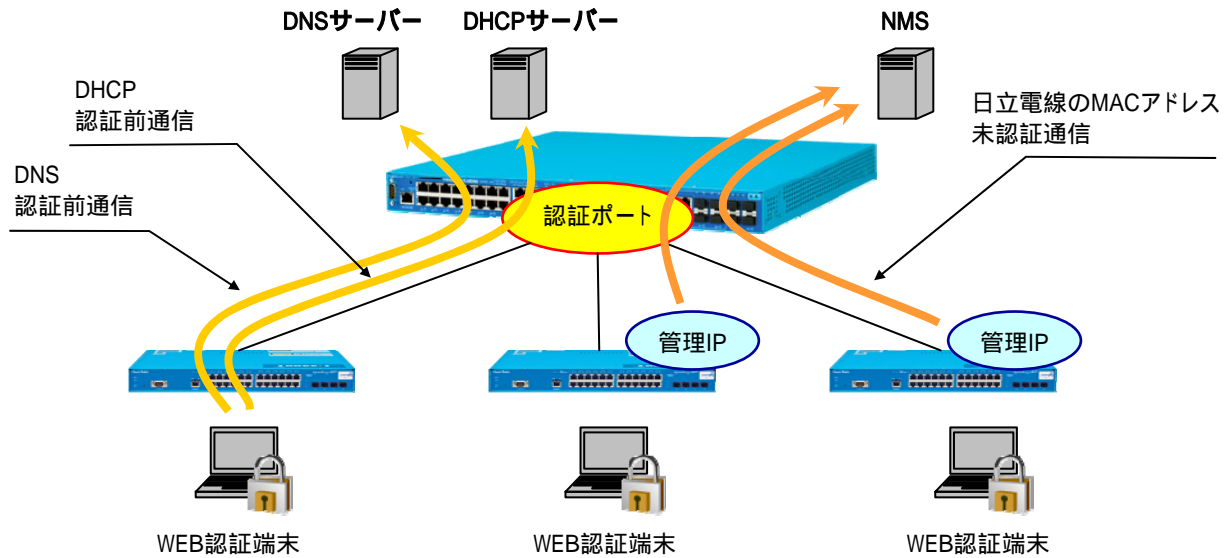


図 7-8 認証バイパス要求例(1)

```
(config)# packet-filter2
(config-filter)# 1 assign port 1-44
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
    . . . グループ 1、ルール 1 で DHCP (67/UDP) を許可
    ※ グループ 1 の有効ポートは 1-44

(config-filter)# 1 2 condition ipv4 dst tcp/udp 53
(config-filter)# 1 2 action authentication-bypass
    . . . グループ 1、ルール 2 で DNS (53/TCP) を許可

(config-filter)# 2 assign port 1-44
(config-filter)# 2 1 condition src mac 00:40:66:00:00:00 mask ff:ff:ff:00:00:00
(config-filter)# 2 1 action authentication-bypass
    . . . グループ 2、ルール 1 でベンダコード 00:40:66 の MAC アドレスを許可
    ※ グループ 2 の有効ポートは 1-44
```

! グループ/ルールの番号は、数字が小さいほど優先順位が高くなります。

7.5.3 認証バイパスによる強制転送設定例(2)

下記例のような要求に対する認証バイパスの設定例を記載します。

- 事務用セグメントの vlan100 だけ認証したい
- vlan300 は、NMS との UDP 通信(1~10000 番)のみに限定したい

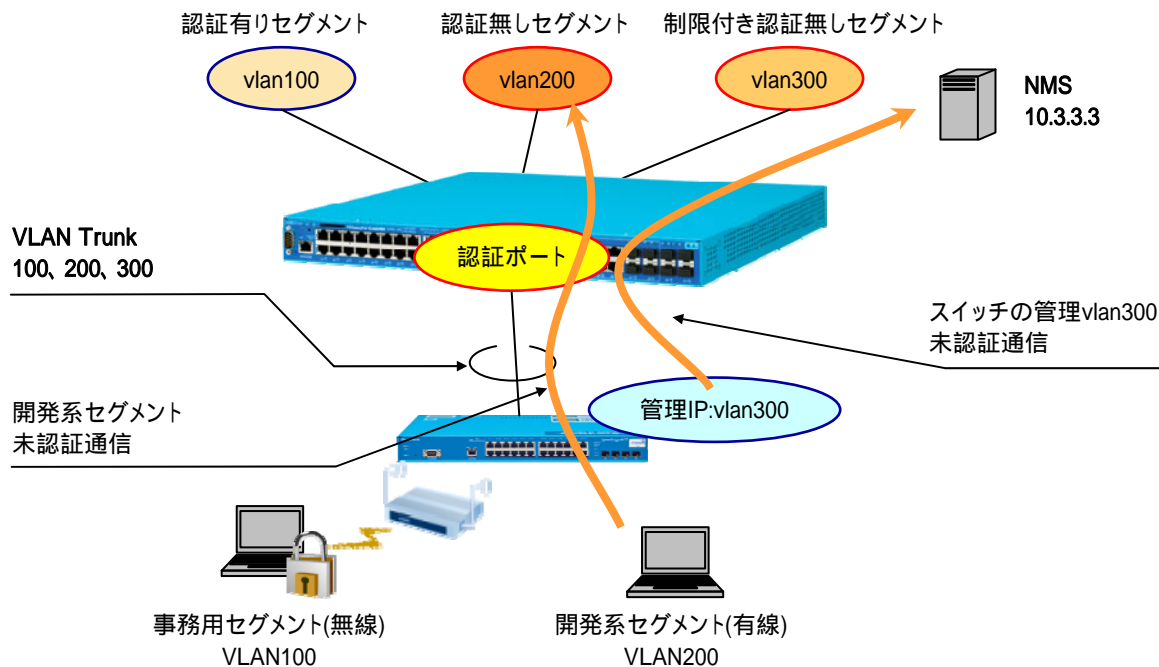


図 7-9 認証バイパス要求例(2)

```
(config)# packet-filter2
```

```
(config-filter)# 1 assign port 1-44
```

```
(config-filter)# 1 1 condition ethernet vid 200
```

```
(config-filter)# 1 1 action authentication-bypass
```

・・・グループ 1、ルール 1 で VLAN200 を許可

※ グループ 1 の有効ポートは 1-44

```
(config-filter)# 2 assign port 1-44
```

```
(config-filter)# 2 assign vlan 300
```

```
(config-filter)# 2 1 condition ipv4 dst ip 10.3.3.3
```

```
(config-filter)# 2 1 condition ipv4 dst tcp/udp 1-10000 udp
```

```
(config-filter)# 2 1 action authentication-bypass
```

・・・グループ 2、ルール 1 で宛先 IP が 10.3.3.3 で且つ UDP のみを許可

※ グループ 2 の有効ポートは 1-44(有効 VLAN は VLAN300)

7.5.4 Windowsドメイン環境への適用

一般的に、Windows ドメイン環境において Web ブラウザーを使用するネットワーク認証機能を共存させる場合、ドメインへのログオンができなくなるケースが発生することがあります。これは、ネットワーク認証を実行する前の状態(未認証状態)ではドメインコントローラとの通信が制限されていることに起因します。Web ブラウザーを使用するには端末のデスクトップを起動する必要がありますが、ドメインへのログオンができないためデスクトップが正常に起動できません。

APRESIA の AccessDefender 認証では、本問題を認証バイパス機能で解決可能です。

表 7-2 AccessDefender 認証がサポートする Windows ドメイン環境への適用手段

方式	認証順序	特徴
認証バイパス	1. Windows ドメイン認証 ↓ 2. AccessDefender 認証	<ul style="list-style-type: none"> AccessDefender 認証前に必要なドメインコントローラ宛の通信に対し認証バイパスを使って許可 検疫ネットワークへのアップグレードが可能 <ul style="list-style-type: none"> ドメイン認証時にネットワーク認証を行わないので、検疫ソフトウェアから認証タイミングの制御が可能

認証バイパス方式の概念図を図 7-10 に示します。

認証バイパスによりドメインコントローラへの通信が許可されているため、ドメインログオンは通常通り行うことが可能です。その他のサーバーには AccessDefender 認証成功後に通信が可能となります。

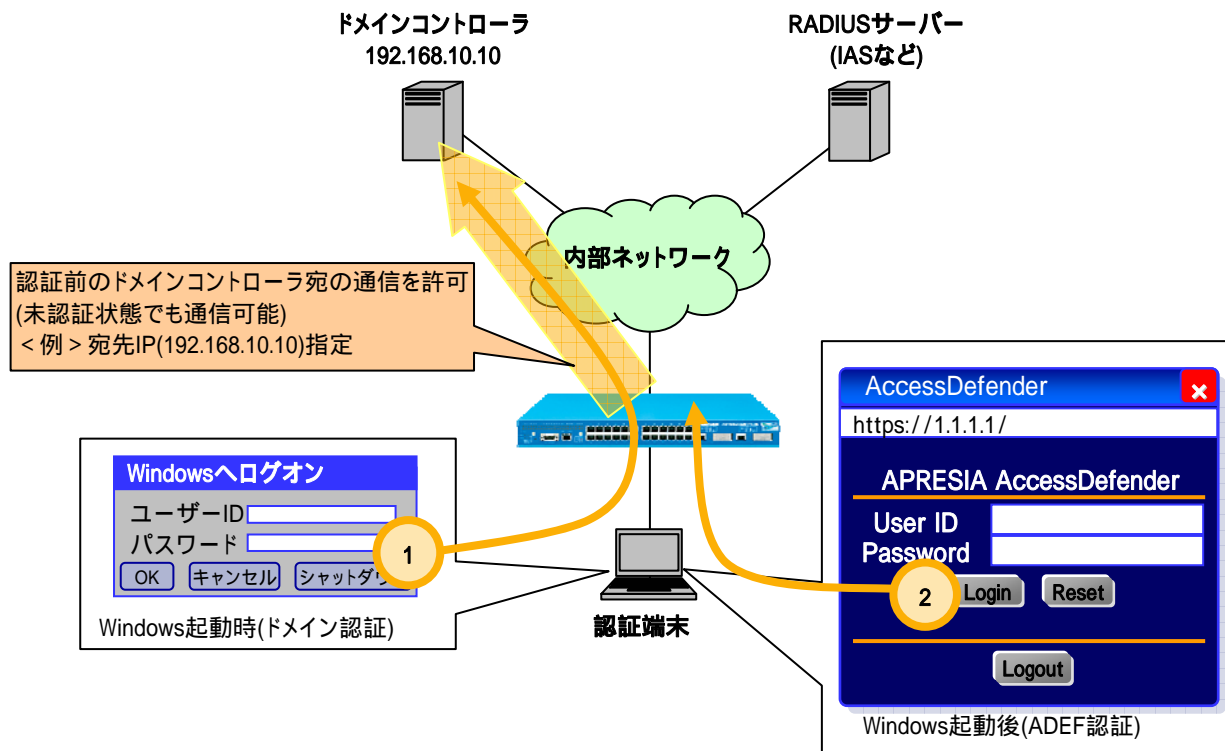


図 7-10 認証バイパスによる Windows ドメイン環境への適用

7.6 認証ページのリダイレクト機能

通常、未認証端末は認証する際にAPRESIAの認証ページ(例えば、<http://1.1.1.1/> など)に直接アクセスし、表示される認証画面にユーザーアカウントを入力することで認証が実行されます。

本機能は、未認証端末から送信される HTTP リクエスト(宛先 IP アドレスは任意)を認識し、強制的に認証 Web ページを表示する機能です。未認証ユーザーの HTTP アクセスでは自動的に認証ページが表示されますので、使用するユーザーに対して APRESIA の認証 URL を改めて通知する必要はなくなり、よりスムーズに認証ネットワークを運用することが可能となります。

本機能は HTTP/HTTPS を選択でき、HTTP を使用する場合は宛先ポート番号が 80、HTTPS を使用する場合は宛先ポート番号が 443 の HTTP リクエストがリダイレクトの対象となります。

- 自動的に認証画面を表示可能
 - ユーザーが任意のサイトを閲覧しようとする時、APRESIA が指定されたアドレスへリダイレクト
 - セキュリティを重視するユーザーには、リダイレクトを OFF にすることも可能
- 外部のサーバーへもリダイレクト可能
 - 内部、外部を意識せずに、1つの URL へリダイレクトでき、Web ベースの検疫などに活用可能
- HTTP プロキシ環境でも適用可能
 - 除外アドレスを設定し忘れても、専用のループ検知画面をブラウザに表示する安心設計

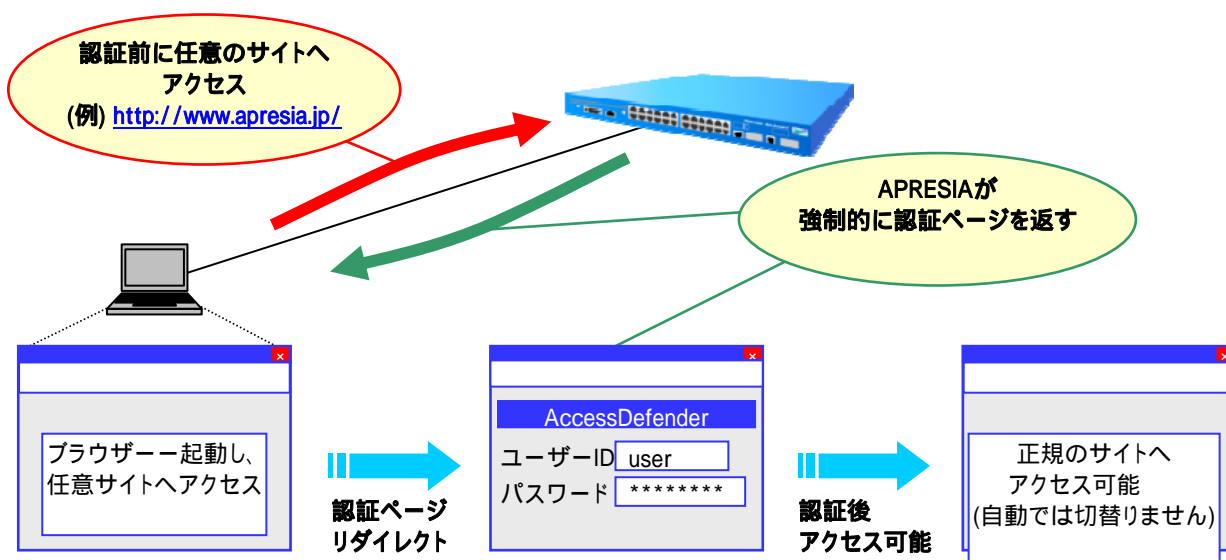


図 7-11 認証ページのリダイレクト機能概念図

- ❗ URL を FQDN(完全修飾ドメイン名)で指定できるように未認証端末から DNS サーバーへの通信許可設定、もしくは認証端末のホストテーブル(hosts)への登録による名前解決が必要です。
- ❗ 認証端末の Gateway(next hop)アドレスを認証装置の IP アドレスに設定した状態では使用できません。

7.6.1 HTTPプロキシが無い環境(直接Internetへ接続)の場合

7.6.1.1 認証フロー

リダイレクト先 URL が設定されている場合、APRESIA は HTTP のステータスコード “302” と共に設定された URL を返信します。ステータスコード “302” を受け取ったブラウザは指定された URL に再度アクセスするため、外部 Web サーバーの認証ページを表示することが可能となります(ステータスコードについての詳細は、RFC2068 “Hypertext Transfer Protocol -- HTTP/1.1” を参照下さい)。

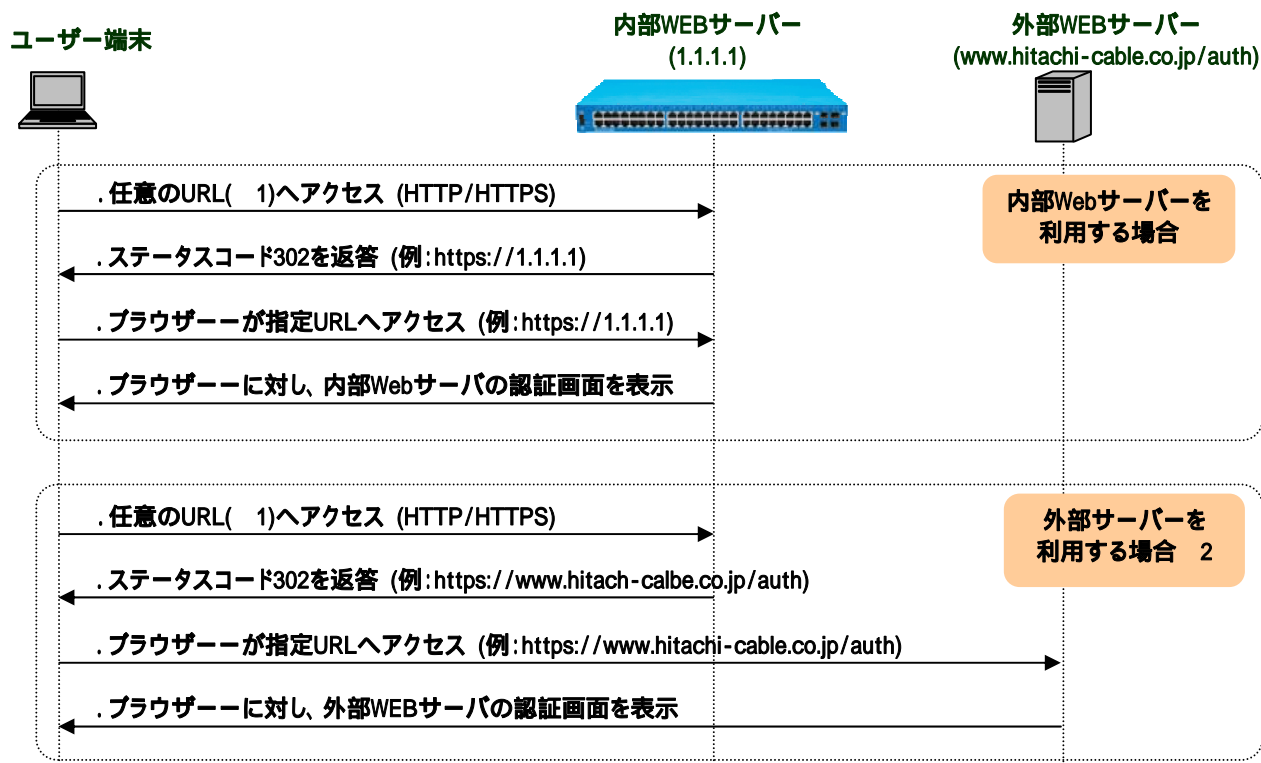


図 7-12 プロキシサーバーがない環境での認証フロー

※1：任意アクセスした Web サーバー (FQDN) の名前解決を行うために、DNS の通信を認証前に許可する必要があります。

※2：外部サーバーへの通信を認証前に許可する必要があります。

! ブラウザーからリダイレクト先認証 URL へのアクセスがリダイレクト対象にならないように、リダイレクト先認証 URL のポート番号を 80、443 以外に設定してください。

7.6.1.2 認証ページリダイレクト機能設定例

APRESIA 標準の認証ページを使用する場合の設定例を示します。

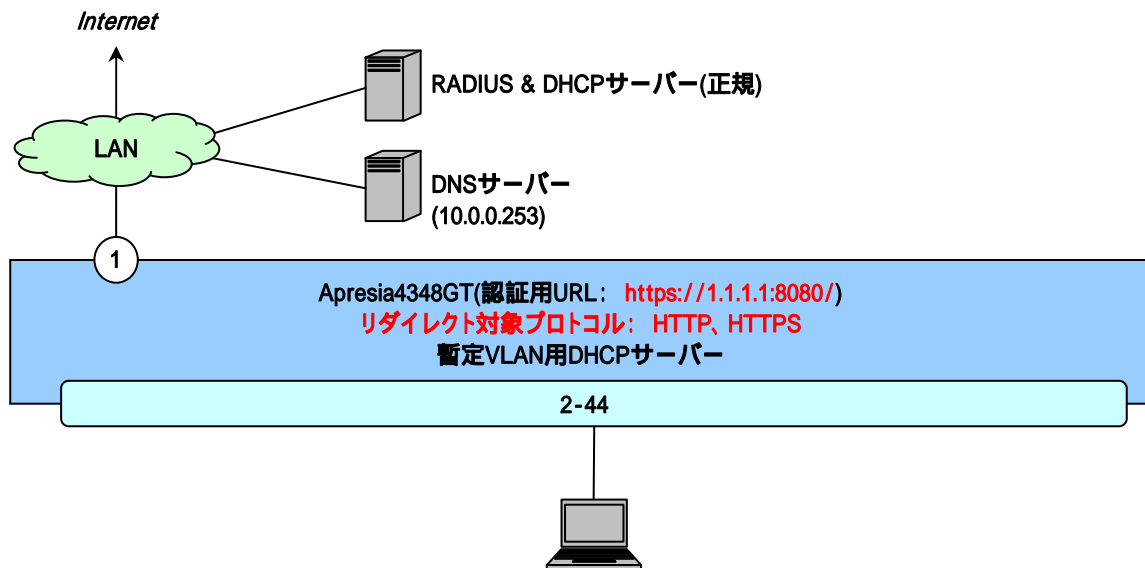


図 7-13 認証ページリダイレクト構成例 (APRESIA 標準認証画面使用)

図 7-13 の構成例での認証ページリダイレクト機能の関連設定のみを抜き出した設定例です (RADIUSサーバーや認証ポート等の設定は省略しています)。

```
(config)# packet-filter2
(config-filter)# 1 1 assign port 2-44
(config-filter)# 1 1 condition ipv4 dst tcp/udp 53
(config-filter)# 1 1 action authentication-bypass
    . . . 認証バイパスによる DNS の強制転送設定 (必須)

(config)# access-defender
(config-a-def)# web-authentication redirect url https://1.1.1.1:8080/
    . . . リダイレクト先 URL を指定 (必須)

(config-a-def)# web-authentication redirect http
(config-a-def)# web-authentication redirect https
    . . . 対象プロトコルとして、HTTP 及び HTTPS を指定 (必須)

(config-a-def)# web-authentication ip 1.1.1.1
(config-a-def)# web-authentication https-port 8080
    . . . 認証用 URL の設定 (必須)

(config)# dhcp policy temp
(config-dhcp)# network 10.0.0.0/16
```

```
(config-dhcp)# range 1 10.0.0.10 10.0.0.20
(config-dhcp)# dns-server 10.0.0.253
(config-dhcp)# router 10.0.0.254
(config-dhcp)# lease 10
(config)# dhcp policy enable temp
(config)# dhcp server address-check arp
(config)# dhcp server enable
```

・・・ 暫定 VLAN 用 DHCP サーバーの設定(リース時間は 10 秒)

※リース時間は端末の IP アドレス更新仕様に合わせて適切な値に調整してください。

注) 暫定 VLAN 用 DHCP サーバーに DNS サーバーの設定が無い場合、端末は DNS による名前解決ができず認証画面を表示できない場合があります。

7.6.2 HTTPプロキシサーバーが存在する環境の場合

7.6.2.1 認証フロー

プロキシサーバーがない場合と同様に、リダイレクト先 URL が設定されている場合、APRESIA は HTTP のステータスコード “302” と共に設定された URL を返信します。ステータスコード “302” を受け取ったブラウザは指定された URL に再度アクセスするため、外部 Web サーバーの認証ページを表示することが可能となります(ステータスコードについての詳細は、RFC2068 “Hypertext Transfer Protocol -- HTTP/1.1” を参照下さい)。

ただし、指定した認証 URL に対するアクセスにはプロキシ除外設定を各ブラウザに設定しておく必要があります。除外設定を入れていない場合、APRESIA はループを検知し、内部のループ検知専用画面を表示します。

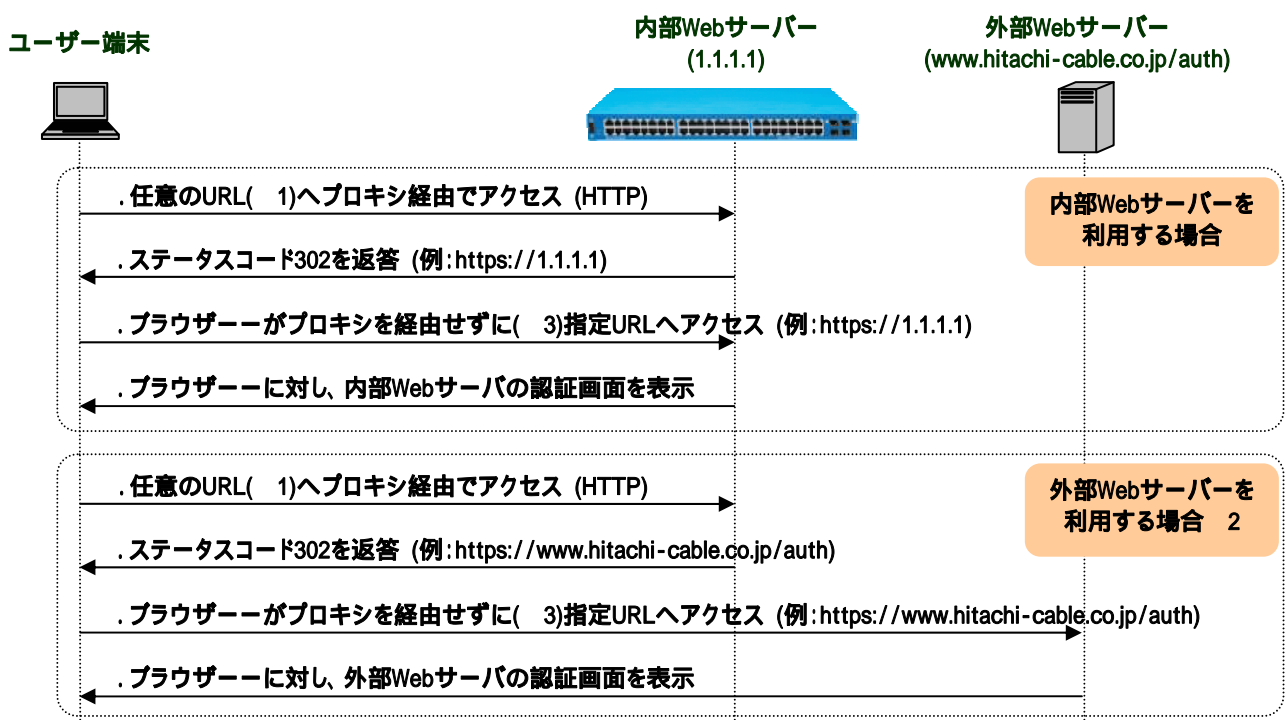


図 7-14 プロキシサーバーがある環境での認証フロー

※1: 任意アクセスした Web サーバー (FQDN) の名前解決を行うために、DNS の通信を認証前に許可する必要があります。

※2: 外部 Web サーバーへの通信を認証前に許可する必要があります。

※3: Web ブラウザーのプロキシ設定で、指定 URL を除外設定として指定する必要があります。未設定の場合に、指定 URL に対しプロキシ経由でアクセスした場合、APRESIA がループ検知画面を表示します。

! ブラウザーからリダイレクト先認証 URL へのアクセスがリダイレクト対象にならないように、リダイレクト先認証 URL のポート番号を 80、443 以外に設定してください。

! Web ブラウザーのプロキシ設定で、指定 URL を除外指定する必要があります。

! 認証端末がHTTPSプロトコルを使用した場合、リダイレクトされません。回避方法については 7.6.3.2 HTTPSを用いる際の注意点を参照下さい。

7.6.2.2 認証ページリダイレクト機能設定例

APRESIA 標準の認証ページを使用する場合の設定例を示します。

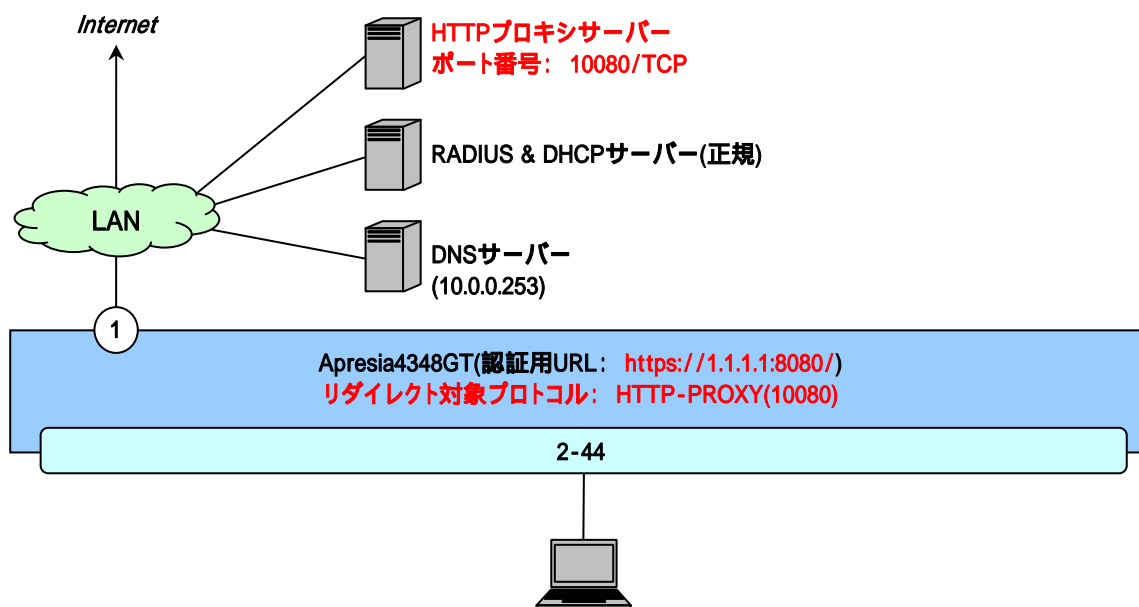


図 7-15 認証ページリダイレクト構成例(プロキシ環境)

図 7-15 の構成例での認証ページリダイレクト機能の関連設定のみを抜き出した設定例です (RADIUSサーバーや認証ポート等の設定は省略しています)。

```
(config)# packet-filter2
(config-filter)# 1 1 assign port 2-44
(config-filter)# 1 1 condition ipv4 dst tcp/udp 53
(config-filter)# 1 1 action authentication-bypass
    ... 認証バイパスによる DNS の強制転送設定 (必須)

(config)# access-defender
(config-a-def)# web-authentication redirect url https://1.1.1.1:8080/
    ... リダイレクト先 URL を指定 (必須)

(config-a-def)# web-authentication redirect proxy-port 10080
    ... 対象プロトコルとして、プロキシサーバーを指定 (必須)

(config-a-def)# web-authentication ip 1.1.1.1
(config-a-def)# web-authentication https-port 8080
    ... 認証用 URL の設定 (必須)

(config)# dhcp policy temp
```

```
(config-dhcp)# network 10.0.0.0/16
(config-dhcp)# range 1 10.0.0.10 10.0.0.20
(config-dhcp)# dns-server 10.0.0.253
(config-dhcp)# router 10.0.0.254
(config-dhcp)# lease 10
(config)# dhcp policy enable temp
(config)# dhcp server address-check arp
(config)# dhcp server enable
```

・・・ 暫定 VLAN 用 DHCP サーバーの設定(リース時間は 10 秒)

※リース時間は端末の IP アドレス更新仕様に合わせて適切な値に調整してください。

注) 暫定 VLAN 用 DHCP サーバーに DNS サーバーの設定が無い場合、端末は DNS による名前解決ができず認証画面を表示できない場合があります。

7.6.3 SSLとWebループ検知の併用

7.6.3.1 Webループ検知が必要な状況

AccessDefender では、HTTP/HTTPSに加え、任意のプロキシポートアクセスの場合においても認証ページリダイレクトを行うことが可能です。

但し、端末がリダイレクト先の IP アドレスを除外アドレスに設定していない場合、リダイレクト先への通信をプロキシ経由で行うことによる Web ループ (ユーザー端末から指定 URL へのアクセスがリダイレクトされる) が発生します。

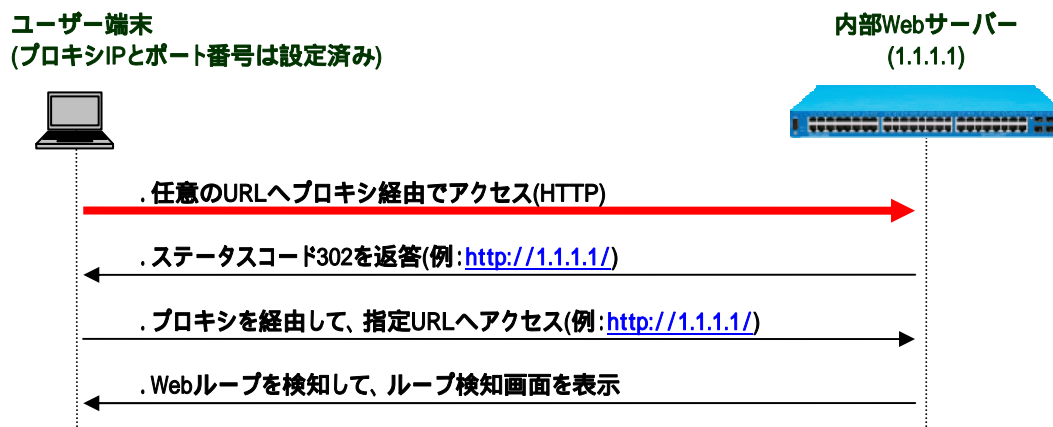


図 7-16 HTTP プロキシ使用時の Web ループ検知

※：リダイレクト先 URL をプロキシアクセス除外設定にしていない場合

Web ループを検知した場合、下図のような検知画面を表示し、ループ発生を抑制します。



図 7-17 Web ループ検知画面

ループ検知画面のリプライ、及び内部認証ページのカスタマイズ機能を用いて、使用するユーザーに対して適切な警告画面を返すことが可能となります。

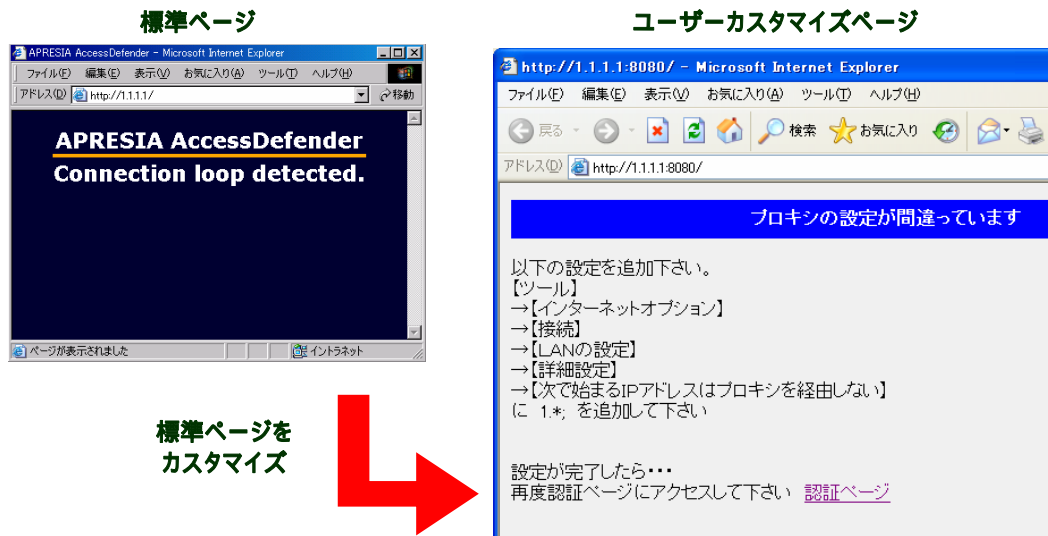


図 7-18 Web ループ検知画面のカスタマイズ

7.6.3.2 HTTPSを用いる際の注意点

プロキシ経由でHTTPS ページにアクセスする場合は、認証ページリダイレクトが実行されない仕様のため、以下のような現象が発生します。

この場合、Web ループ検知画面も表示されないため、使用ユーザーに不可理由を通知することができません。

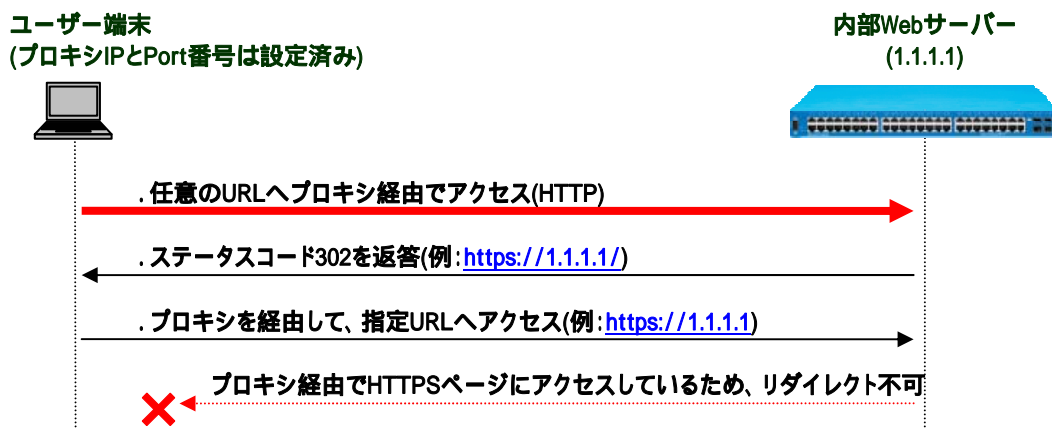


図 7-19 プロキシ経由での HTTPS アクセス

※：Web ループ検知画面も表示されません。

本現象を回避するためには、リダイレクト URL は HTTPS ではなく HTTP とし、認証ページカスタマイズによりログインボタン入力時のみ SSL 通信が行われるようにすることが必要となります。

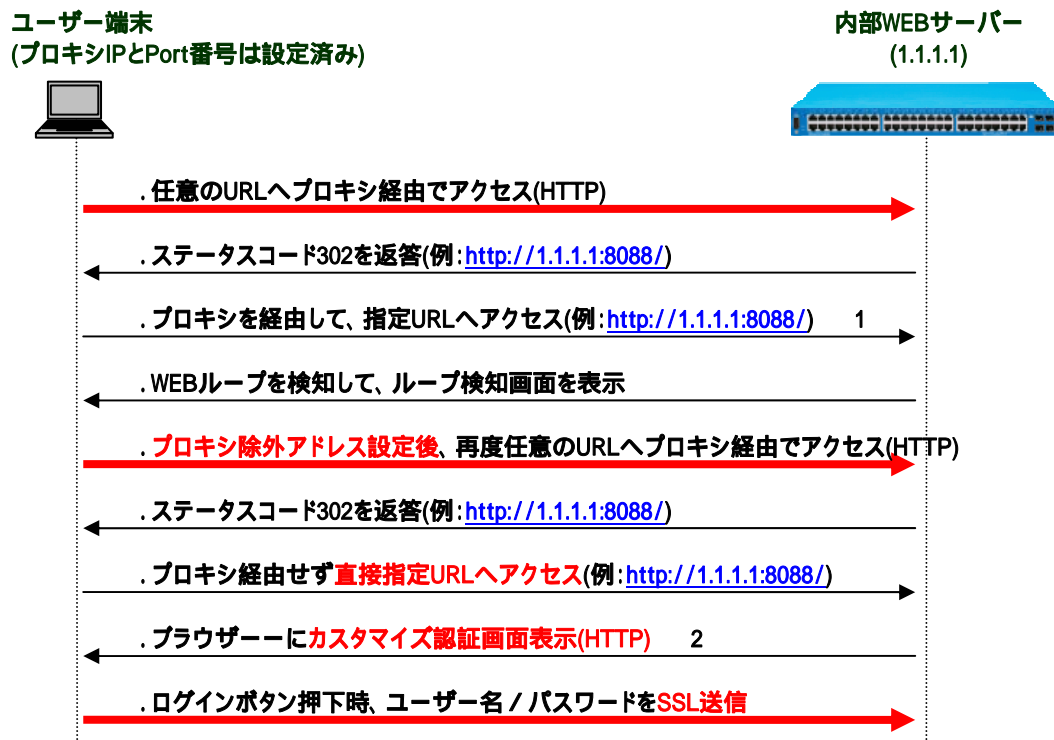


図 7-20 プロキシ経由で HTTPS ページにアクセスする場合

※1：リダイレクト先 URL をプロキシアクセス除外設定にしていない場合。

※2：ログインボタン押下時のみ SSL 送信するようにカスタマイズします。

上記フローの⑧で使用する認証ページに以下のようなカスタマイズを施すことにより、ログインボタン押下し、ユーザー名/パスワードを APRESIA の認証 CGI に送付する際には SSL 通信が行われ、セキュリティ確保が可能となります。

<ログイン用の form 例>

```
<form method="POST" action="https://1.1.1.1/cgi-bin/adefflogin.cgi">
```

APRESIA 側の認証機能の設定例

```
(config-a-def)# web-authentication redirect url http://1.1.1.1:8088/
(config-a-def)# web-authentication redirect proxy-port 10080
(config-a-def)# web-authentication ip 1.1.1.1

(config-a-def)# web-authentication http-port 8088 ①
(config-a-def)# web-authentication https-port 443 ②
```

・・・AccessDefender では①、②が両方設定できるため、本回避策が可能

7.7 正規固定IPアドレス端末の接続(DHCPスヌーピング)

DHCP スヌーピングを有効としたポートで正規固定 IP アドレス端末を接続する場合、下記のいずれかの方法により対応可能です。以下にそれぞれの場合の設定例を示します。

- ① IP アドレスを指定して許可したい場合 ⇒ static-entry 設定
- ② MAC アドレスを指定して許可したい場合 ⇒ 認証バイパス設定

7.7.1 static-entry設定による方法

ポート 1 に 192.168.1.10 という固定 IP アドレス端末を接続する場合、以下のように設定します。

```
(config)# access-defender
(config-a-def)# dhcp-snooping static-entry port 1 192.168.1.10
```

- ❗ static-entry コマンドで登録された静的フィルタは、自動では削除されません。フィルタを削除する場合、手動で削除する必要があります。
- ❗ 各ポートで登録可能な静的フィルタの上限数は(クライアント制限数 - 動的に登録されているフィルタ数)となります。

7.7.2 認証バイパス設定による方法

ポート 1 に 00:00:00:00:00:01 という MAC アドレス端末を接続する場合、以下のように設定します。

```
(config)# packet-filter2
(config-filter)# 2 assign port 1
(config-filter)# 2 1 condition src mac 00:00:00:00:00:01
(config-filter)# 2 1 action authentication-bypass
```

- ❗ 認証バイパス機能にて IP アドレスを指定して許可する場合、ARP フレームが許可されていないため通信できません。IP アドレスを条件とする場合には、static-entry コマンドをご使用ください。
- ❗ 認証バイパスによる MAC アドレス指定を使用する場合、IP アドレスに関係なく、条件に指定した MAC アドレスの通信を許可します。

8. AccessDefender関連ログ

8.1 認証ログ表示例(syslog)

認証が成功した場合や失敗した場合、またはログイン・ログアウト時に、認証ログとして APRESIA の syslog に詳細ログが記録されます。このログを用いて容易なユーザートラッキング(どこで・誰が・どの端末で・いくつ接続しているか?)が可能となります。APRESIA のコンソール上で「show logging」コマンドを入力することでログを確認することができますが、syslog サーバーでの統合管理を推奨します。

表示されるログの詳細は「ログ・トラップ対応一覧」を参照下さい。

表 8-1 認証ログ表示例

No.	レベル	メッセージ例	内容
1	notice	<radius force local> authentication succeeded : uid=<user>	認証成功
2	notice	<web gateway mac dot1x dhcpsnooping> : login succeeded : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	ログイン成功
3	notice	<radius force local> authentication failed : uid=<user>	認証失敗
4	notice	<web gateway mac dot1x dhcpsnooping> : login failed : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	ログイン失敗
5	notice	<web gateway mac dot1x dhcpsnooping> : logout (<type>) : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	ログアウト※
6	warning	<web gateway mac dot1x dhcpsnooping discard> : the number of terminals on switch is full : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	認証端末数の制限によるログイン不可(認証済み端末数が装置の最大数に達している)
7	warning	<web gateway mac dot1x dhcpsnooping> : the number of terminals on port <port> is full : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	1ポート最大認証数によるログイン不可(認証済み端末数がポートの最大数に達している)
8	warning	mac : the number of discard terminals on switch is full : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid>	discard 登録数の制限による登録不可(DISCARD 端末の最大数に達している)
9	warning	<web mac dot1x> : vlan assignment failed : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	VLAN 変更処理失敗
10	warning	radius(<IP address>) timeout : uid=<user>	RADIUS タイムアウト (RADIUS サーバーからの応答を受信できなかった)
11	warning	port <port number> has already been assigned to another	VLAN 変更制限機能有効

		vlan : uid=<user> port=<port number> [new vid=<vid>]	時の VLAN 変更失敗 (RADIUS/Local 認証結果受信時)
12	warning	{web mac dot1x} : port <port number> has already been assigned to another vlan : uid=<user> mac=<mac address> ip=<ip address> port=<port number> vid=<vid> [new vid=<vid>]	VLAN 変更制限機能有効時の VLAN 変更失敗(端末設定時)
13	warning	<web gateway mac dot1x dhcpsnooping> : duplicate terminal : uid=<user> mac=<MAC address> ip=<IP address> port=<port> vid=<vid> [new vid=<vid>]	端末キー重複による登録失敗
14	info	dhcpsnooping : mode-timer started.	モードタイマ設定変更
15	info	dhcpsnooping : mode changed to DENY automatically.	タイマ終了による DENY モードへの変更
16	info	dhcpsnooping : mode changed to deny manually.	CLI によるモード変更 (PERMIT から DENY)
17	info	dhcpsnooping : mode changed to permit manually.	CLI によるモード変更 (DENY から PERMIT)
18	info	dhcpsnooping : mode changed to mac-authentication mode enable	CLI によるモード変更 (mac-authentication 有効)
19	info	dhcpsnooping : mode changed to mac-authentication mode disable	CLI によるモード変更 (mac-authentication 無効)
20	notice	web : login rejected : uid=<user> mac=<MACaddress> ip=<IP address> port=<port> vid=<vid> ttl=<ttl>	TTL フィルタによるログイン拒否

※表示されるログアウトタイプは以下となります。

表 8-2 ログアウトで表示されるタイプ一覧

TYPE	ログアウト種別
aging	aging によるログアウト
web	ユーザー認証 Web 画面でのログアウトボタン押下によるログアウト
maxtime	最大接続時間によるログアウト
cli	access-defender-logout コマンドによるログアウト
config change	設定変更によるログアウト
link down	ポートのリンクダウンによるログアウト
overwrite	同一の認証端末がログインしたことによるログアウト
logoff	logoff 受信によるログアウト
reauth failure	再認証失敗によるログアウト
reauth failure supp-timeout	再認証時にサブリカント応答無しによるログアウト
reauth vlan change	再認証時に VLAN 変更検出によるログアウト
reauth user name change	再認証時にユーザーネーム変更検出によるログアウト
port initialization	ポート設定初期化によるログアウト
release	IP リリースによるログアウト

expire	IP リース期間満了によるログアウト
--------	--------------------

8.2 設定時のコンフリクトメッセージ一覧

AccessDefenderに関連する設定コンフリクト(設定上の禁則)メッセージを表 8-3 に示します。

表 8-3 AccessDefender 設定時のコンフリクトメッセージ一覧

No.	表示メッセージ	説明
1	Violation of NA Status and AccessDefender Status.	AccessDefender と NA の併用設定はできません。
2	Violation of TCP Port Number.	認証 URL のポート番号、及びプロキシサーバーのポート番号の設定値として、23(telnet)は指定できません。 認証 URL のポート番号、及びプロキシサーバーのポート番号の設定値として、同じ PORT は指定できません。
3	No Packet-filter2 entry.	packet-filter2 max-rule 未設定時、web-authentication enable と mac-authentication enable は指定できません。
4	Violation of RADIUS Index.	aaa radius authentication web(mac) index1 と index2 の設定値として、同じ index は指定できません。
5	No RADIUS entry.	aaa radius authentication web(mac) 指定 index1 または index2 が index 登録されていない場合は、指定できません。
6	% DHCP: cannot start dhcp-snooping.	packet-filter2 max-rule 未設定時は、DHCP スヌーピング機能を有効にできません。
7	% Invalid SSL files.	正しい SSL 用サーバー証明書(チェーン証明書含む)を入れる必要があります。

9. SSL設定について

SSL(Secure Socket Layer)とは、サーバー⇄端末間で機密性の高い情報を安全にやり取りできるようにするための暗号化通信の規約です。SSL を利用することで、ネットワーク上で通信し合う端末とサーバーの間で暗号化したデータをやり取りできるようになり、データの盗聴などを防ぐことができます。

APRESIA で SSL を有効にすると、AccessDefender 認証時に入力するユーザー名とパスワードを暗号化し、安全に認証することが可能になります。

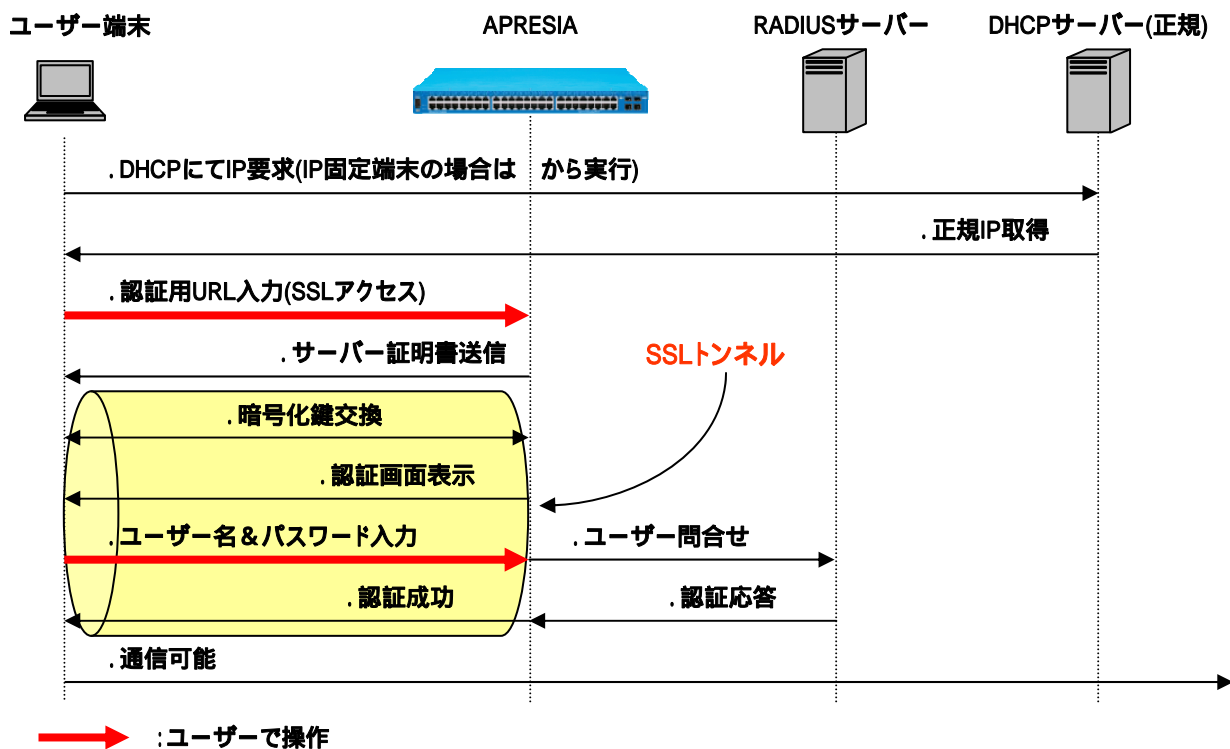


図 9-1 SSL での認証フロー

! AccessDefender では、中間 CA 証明書を Ver7.12 よりサポートしています。詳細は 9.6 中間 CA 証明書対応についてを参照下さい。

9.1 SSL設定概要

APRESIA のファームウェアには予めテスト用の証明書と秘密鍵が埋め込まれており、新たに証明書をインストールしなくても本機能を使用できます。

別途証明書を用意する場合は以下のいずれかの手順で、証明書/秘密鍵をインストールして下さい。

■証明書要求(CSR : Certificate Signing Request)を装置で発行する場合(9.2 証明書要求を装置で発行する場合)で説明

①. 秘密鍵およびCSRの生成

「`ssl gencsr rsakey`」コマンドにより、秘密鍵およびCSRを生成します。

②. CSRのアップロード

「`copy csr tftp`」コマンドにより、本機からCSRをTFTPサーバー上にアップロードします。

③. 証明書の発行

CSRを認証局(CA)に送付し、証明書を発行してもらいます。

④. 証明書のダウンロード

TFTPサーバー上に証明書をおき、「`copy tftp server file https-file`」コマンドにより、本機に証明書をダウンロードします。

■証明書要求を装置で発行しない場合(9.3 証明書要求を装置で発行しない場合)で説明

①. 秘密鍵およびCSRの生成

OpenSSLなどのソフトウェアを使用し、秘密鍵およびCSRを生成します。

②. 証明書の発行

CSRを認証局(CA)に送付し、証明書を発行してもらいます。

③. 証明書および秘密鍵のダウンロード

TFTPサーバー上に証明書および秘密鍵をおき、「`copy tftp server file https-file`」コマンドにより、本機に証明書および秘密鍵をダウンロードします。

! HTTPS プロトコル標準のポート番号(443)を使用する場合は、明示的に指定して下さい。

! APRESIA にダウンロード可能なファイル形式は PEM(Privacy Enhanced Mail)形式のみです。

! ダウンロードした証明書と秘密鍵は即時に反映されます。

! 証明書や秘密鍵のファイル名は最大 128 文字です。また、使用可能な文字は、ASCIIコードの印字可能な文字のうち、「"」「?」を除いた文字です。また、先頭文字には「!」「#」も使用することはできません。

! 秘密鍵は厳重に管理して下さい。

9.2 証明書要求を装置で発行する場合

9.2.1 秘密鍵およびCSRの生成


「ssl genscr rsakey」コマンドにより、秘密鍵および CSR を生成します。秘密鍵作成の公開鍵暗号方式は RSA を使用し、メッセージダイジェストアルゴリズムは MD5 を使用します。作成した秘密鍵は暗号化されていない状態で保存されます。既に証明書要求と秘密鍵がある場合で本コマンドを使用すると、それぞれに上書きします。


```
(config)# ssl genscr rsakey [<key-length>]
    . . . 証明書要求と秘密鍵を作成(鍵長を指定(512-2048) 省略した場合 1024)
```

```
(config)# ssl genscr rsakey 512
Country Name (2 letter code) [JP]:
State or Province Name (full name) [Some-State]:TOKYO
Locality Name (eg, city) [Some-City]:CHIYODA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HCL
Organizational Unit Name (eg, section) []:SE
Common Name (YOUR domain name) []:1.1.1.1
Email Address []:test@hitachi-cable.co.jp
Generating a 512 bit RSA private key
.....+++++++
.....+++++++
Writing new private key
Writing to flash memory...
done.
```

表 9-1 CSR 生成時の入力項目

項目	内容	例	文字数制限
Country	国別記号	JP	2
State or Province	都道府県	TOKYO	1-128
Locality	市区町村名	CHIYODA	1-128
Organization	組織名	HCL	1-64
Organizational Unit	部門名	SE	1-64
Common Name	ドメイン名	1.1.1.1	1-64
Email Address	電子メールアドレス	test@hitachi-cable.co.jp	1-128

 文字 '?' は入力できません。また、Country についてはローマ字アルファベットの大文字 ('A' ~ 'Z') のみ入力可能です。

 表 9-1 の入力項目のいずれの項目も省略できません。

❗ Common Name(CN)は、APRESIAの認証URLで指定するホスト名にする必要があります(この例では「https://1.1.1.1/」が認証URLになります)。認証URLとCNが異なる場合、セキュリティ警告が表示されます。

❗ 鍵長が長くなるに従い、Web認証時のCPU処理負荷は高くなります。

一致しない場合、下記のようなセキュリティ警告が表示されます。

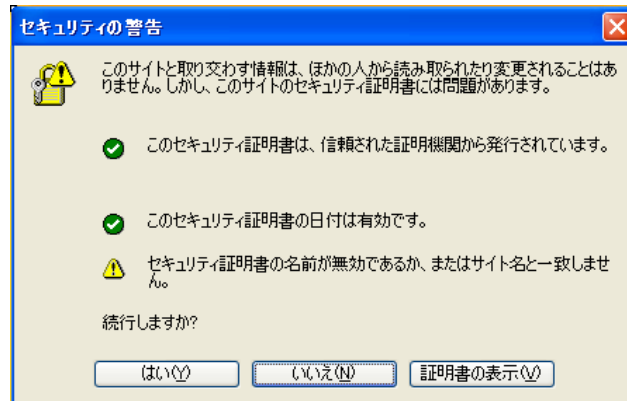


図 9-2 認証URL不一致によるセキュリティ警告

生成したCSRは「show ssl csr」コマンドで確認できます。

```
# show ssl csr
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=JP, ST=TOKYO, L=CHIYODA, O=HCL, OU=SE, CN=1.1.1.1/emailAddress=test@hitachi-cable.co.jp
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (512 bit)
      Modulus (512 bit):
        00:b3:c9:c0:db:20:07:b9:36:de:9b:4c:5d:3b:10:
        0e:3b:59:87:0f:21:ae:8c:62:fd:4a:4a:97:16:d4:
        9c:d6:b5:50:4c:4c:78:cf:c8:82:0d:b4:05:94:b0:
        6c:df:7f:a8:1d:77:8a:32:38:97:a3:91:b0:14:74:
        e2:f5:e1:bc:77
      Exponent: 65537 (0x10001)
    Attributes:
      a0:00
    Signature Algorithm: md5WithRSAEncryption
      73:42:85:b3:f3:a9:9a:be:25:a0:8b:c4:be:32:ec:60:79:2b:
      a8:89:7c:b8:b2:9a:a9:c8:6a:e0:df:c4:de:3d:3a:80:a5:7f:
      2c:ff:6f:8a:97:4b:9c:1f:51:58:60:5c:ee:c0:49:8e:0e:23:
      90:5e:41:e1:5a:4d:d6:8d:b5:5a
```

#

9.2.2 CSRのアップロード

「copy csr tftp」コマンドにより、装置から CSR を TFTP サーバー上にアップロードします。


```
# copy csr tftp 192.168.1.1 CSR
    . . . TFTP サーバー(192.168.1.1)へCSRのアップロード
```

9.2.3 証明書の発行

CSR を認証局に送付し、証明書を発行してもらいます。

9.2.4 証明書のダウンロード

TFTP サーバー上に証明書をおき、「copy tftp server file https-file」コマンドにより、装置に証明書をダウンロードします。ファイルの中身は次のようになっています(PEM形式)。

 APRESIA にダウンロード可能なファイル形式は PEM 形式のみです。

<証明書>


```
-----BEGIN CERTIFICATE-----
MIICQDCCAakCAQIwDQYJKoZIhvcNAQEEBQAwwY0xCzAJBgNVBAYTAkpQM4wDAYD
VQQIEwVUub2t5bzETMBEGA1UEBxMKQ2hpeW9kYS1rdTEMMAoGA1UEChMDSENMMQww
CgYDVQQLEwNMQUIxHDAaBgNVBAMUE0FwcmVzaWFfQ0EoMS4xLjEuMSkxHzAdBgkq
. . . . . 中略 . . . . .
5oy7tc+1mAKshvPTNdjFHSQiptfymyJnGd/50//Zz0a5tXk+eQQLpLpypx2d6oWN
WvAD2CC763Z9GRQbDY1ITb8Mz86YoJ061LpNhc8906fE1pIQf+LJxrdTUfAUe0mo
kugHFw==
-----END CERTIFICATE-----
```

```
# copy tftp 192.168.1.1 apresiacerts.pem https-certificate
    . . . TFTP サーバー(192.168.1.1)からサーバー証明書のダウンロード
```

9.3 証明書要求を装置で発行しない場合

<留意事項>

本セクションの記載内容は、AccessDefender 認証時に SSL 通信させるためのサーバー証明書と秘密鍵を生成する目的の簡易的な認証局(プライベート CA)の設定を含んでいます。記載されている内容そのままでの認証局運用を避けて下さい。

 このセクションの内容はサポート対象外となります。

9.3.1 秘密鍵およびCSRの生成

OpenSSL などのソフトウェアを使用し、秘密鍵および CSR を生成します。このセクションでは、Linux 版 OpenSSL(0.9.7a)を使用し、プライベート CA から作成しています。

- ①. プライベート CA とするマシンの設定ファイル(/usr/share/ssl/openssl.cnf)を編集
vi などのエディタを使用し、下記 2 箇所のコメントを外します。

```
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.

. . . . . 中略 . . . . .

[ usr_cert ]
. . . . . 中略 . . . . .

# This is OK for an SSL server.
nsCertType = server          ← コメントを外す

. . . . . 中略 . . . . .

[ v3_ca ]
. . . . . 中略 . . . . .

# Some might want this also
nsCertType = sslCA, emailCA  ← コメントを外す

. . . . . 中略 . . . . .
```

- ②. プライベート CA 用の秘密鍵と証明書の生成

事前に変更しておいた「openssl.cnf」ファイルを用いて CA を作成します。
本例では OpenSSL の Perl スクリプトを使用しています。

```
# mkdir /opt/apresia_certs
    ... プライベート CA のディレクトリを作成

# cd /opt/apresia_certs
    ... 作成したプライベート CA ディレクトリへ移動

# /usr/share/ssl/misc/CA.pl -newca
    ... Perl スクリプトにより CA 証明書と秘密鍵を生成
```

```
# /usr/share/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)
【新規作成のため、そのまま Enter キーを押す】
Making CA certificate ...
Generating a 1024 bit RSA private key
.....++++++
....++++++
writing new private key to './demoCA/private/cakey.pem'           ← CA 用秘密鍵の生成
Enter PEM pass phrase: 【CA 用秘密鍵のパスフレーズの入力】
Verifying - Enter PEM pass phrase: 【CA 用秘密鍵のパスフレーズの再入力】
-----

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [GB]:JP                               【国コード】
State or Province Name (full name) [Berkshire]:Tokyo            【都道府県名】
Locality Name (eg, city) [Newbury]:Chiyoda-ku                  【市町村名】
Organization Name (eg, company) [My Company Ltd]:HCL           【組織名】
Organizational Unit Name (eg, section) []:LAB                   【組織内ユニット名】
Common Name (eg, your name or your server's hostname) []:APRESIA_CA 【サーバー名】
Email Address []:admin@apresia.jp                               【メールアドレス】
#
```

 **秘密鍵のパスフレーズを絶対に忘れないようにして下さい。**

実行後、次のようなディレクトリとファイルが自動生成されます。

```
# ll /opt/apresia_certs/demoCA/
total 24
-rw-r--r-- 1 root root 1265 Dec 17 17:39 cacert.pem (CA 証明書)
drwxr-xr-x 2 root root 4096 Dec 17 17:37 certs
drwxr-xr-x 2 root root 4096 Dec 17 17:37 crl
-rw-r--r-- 1 root root 0 Dec 17 17:37 index.txt
drwxr-xr-x 2 root root 4096 Dec 17 17:37 newcerts
drwxr-xr-x 2 root root 4096 Dec 17 17:37 private (CA 秘密鍵格納ディレクトリ)
-rw-r--r-- 1 root root 3 Dec 17 17:37 serial
#
```

③. CA 証明書を端末にインストールするための DER(Distinguished Encoding Rules)ファイルの生成

```
# openssl x509 -inform PEM -in cacert.pem -outform DER -out ca.der
```

生成される「ca.der」を端末上で実行し、作成したプライベート CA(この例では APRESIA_CA)を「信頼されたルート証明機関」に登録しておくると以下のようなセキュリティ警告が表示されなくなります。

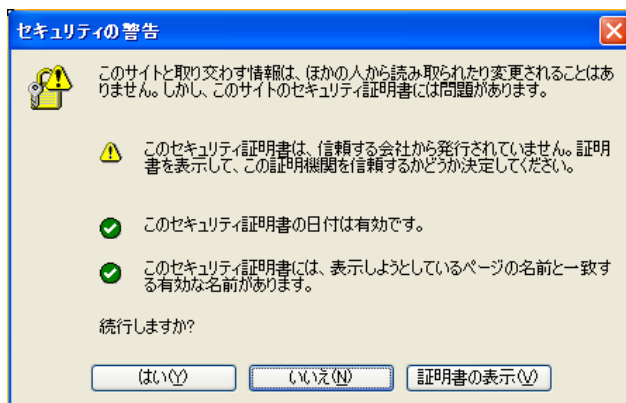


図 9-3 信頼されたルート証明機関に登録前のセキュリティ警告

④. APRESIA 用の秘密鍵の生成

```
# openssl genrsa -out apresiakey.pem 512 ← 鍵長 512 ビットの秘密鍵を生成(暗号化なし)
Generating RSA private key, 512 bit long modulus
.....+++++++
.+++++++
e is 65537 (0x10001)
#
```

⑤. 生成した APRESIA の秘密鍵を使用して証明書発行要求を生成

```
# openssl req -new -key apresiakey.pem -out apresia.csr
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:**JP**

State or Province Name (full name) [Berkshire]:**Tokyo**

Locality Name (eg, city) [Newbury]:**Chiyoda-ku**

Organization Name (eg, company) [My Company Ltd]:**Hitachi-Cable**

Organizational Unit Name (eg, section) []:**SE**

Common Name (eg, your name or your server's hostname) []:**1.1.1.1**

← 重要ポイント

Email Address []:**test@hitachi-cable.co.jp**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: **【Enter キー入力】**

An optional company name []: **【Enter キー入力】**

#

! Common Name(CN)は、APRESIAの認証 URL で指定するホスト名にする必要があります(この例では「https://1.1.1.1/」が認証 URL になります)。認証 URL と CN が異なる場合、セキュリティ警告が表示されます。

一致しない場合、下記のようなセキュリティ警告が表示されます。

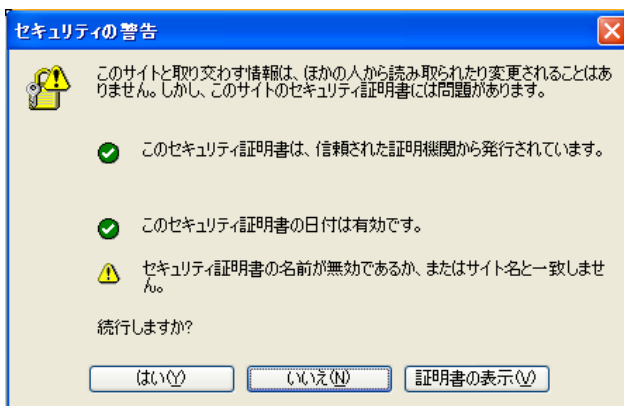


図 9-4 認証 URL 不一致によるセキュリティ警告

9.3.2 証明書の発行

CSR を認証局に送付し、証明書を発行してもらいます。本例では最初に生成したプライベート CA で署名しています。

- ①. 生成した CSR を元に、作成したプライベート CA で X.509 サーバー証明書の生成と署名
例では証明書有効期限が 1 年 ("-days" オプションで指定) となっています。

```
# openssl x509 -CA cacert.pem -CAkey private/cakey.pem -CAserial serial -req -days 365 -in
apresia.csr -out apresiacerts.pem
Signature ok
subject=/C=JP/ST=Tokyo/L=Chiyoda-ku/O=Hitachi-Cable/OU=SE/CN=1.1.1.1/emailAddress=test@hitachi
-cable.co.jp
Getting CA Private Key
Enter pass phrase for private/cakey.pem: 【CA 用秘密鍵のパスフレーズを入力】
#
```

9.3.3 証明書および秘密鍵のダウンロード

TFTP サーバー上に証明書および秘密鍵をおき、「copy tftp server file https-file」コマンドにより、本機に証明書および秘密鍵をダウンロードします。

それぞれファイルの中身は次のようになっています (PEM 形式)。



APRESIA にダウンロード可能なファイル形式は PEM 形式のみです。



秘密鍵が暗号化されている場合、パスフレーズを入力する旨メッセージが表示されます。秘密鍵を暗号化時に使用したパスフレーズを入力して下さい。なお、暗号化の方式については DES、3DES にのみ対応します。



正しくない秘密鍵をダウンロードした場合、パスフレーズの入力が求められますが、復号化に失敗します。このため有効な秘密鍵となりません。

<証明書>

```
-----BEGIN CERTIFICATE-----
MIICQDCCAakCAQIwDQYJKoZIhvcNAQEEBQAwwY0xCzAJBgNVBAYTAKpQM4wDAYD
VQQIEwVUub2t5bzETMBEGA1UEBxMKQ2hpeW9kYS1rdTEMMAoGA1UEChMDSENMMQww

. . . . . 中略 . . . . .

WvAD2CC763Z9GRQbDY1ITb8Mz86YoJ061LpNhc8906fE1pIQf+LJxrdTUfAUe0mo
kugHFw==
-----END CERTIFICATE-----
```

<秘密鍵>

```
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBANrIo6vXJPQax8WVyg+tmI27F7Idn0ukmznI1W4nChjSlp/yw3hD
i+iZDjtYHHWnbVffMU0/OK8dAM9zwesR00UCAwEAAQJAAAbJYCnD0fF/oxINQuaZi

. . . . . 中略 . . . . .

Jt+Hd71LcgrDuwIhAJZ0gMKvAWtxYii jwJStP1GR17nSqz jGud/uzhWbmBDnAiEA
s0utik/2ZIZ11A1Wua+1XR0c311+hIusGvQMrLt1tnM=
-----END RSA PRIVATE KEY-----
```

```
# copy tftp 192.168.1.1 apresiacerts.pem https-certificate
. . . TFTP サーバー (192.168.1.1) からサーバー証明書のダウンロード

# copy tftp 192.168.1.1 apresiakey.pem https-private-key
. . . TFTP サーバー (192.168.1.1) から秘密鍵のダウンロード
```

9.3.4 信頼されたルート証明機関として登録

生成したプライベート CA 証明書の DER 形式のファイルを端末上で実行し、プライベート CA(この例では APRESIA_CA)を「信頼されたルート証明機関」に登録します。

- ①. プライベート CA 証明書の DER 形式のファイル(この例では ca.der)を端末上で実行し、【証明書のインストール】をクリックします。

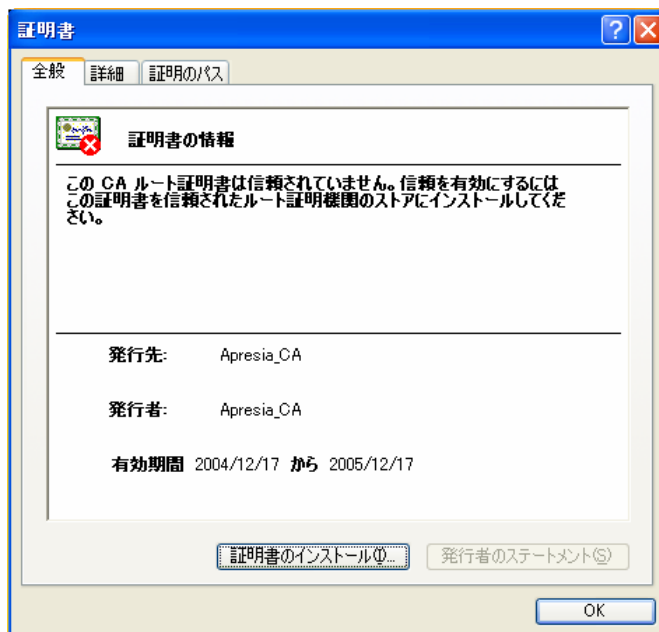


図 9-5 プライベート CA の登録

- ②. 証明書のインポートウィザードが起動します。【次へ】をクリックします。

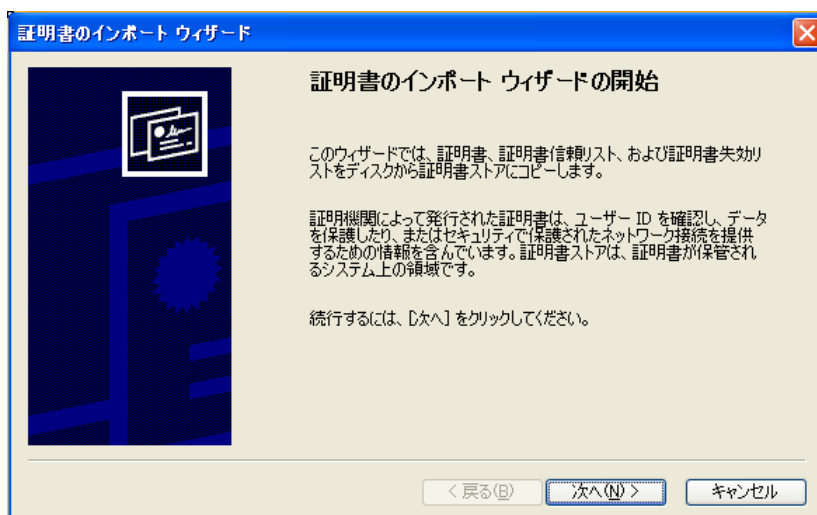


図 9-6 証明書インポートウィザード起動

- ③. 証明書を保存する証明書ストアを選択します。「自動的に証明書ストアを選択する」を選択し、【次へ】をクリックします。

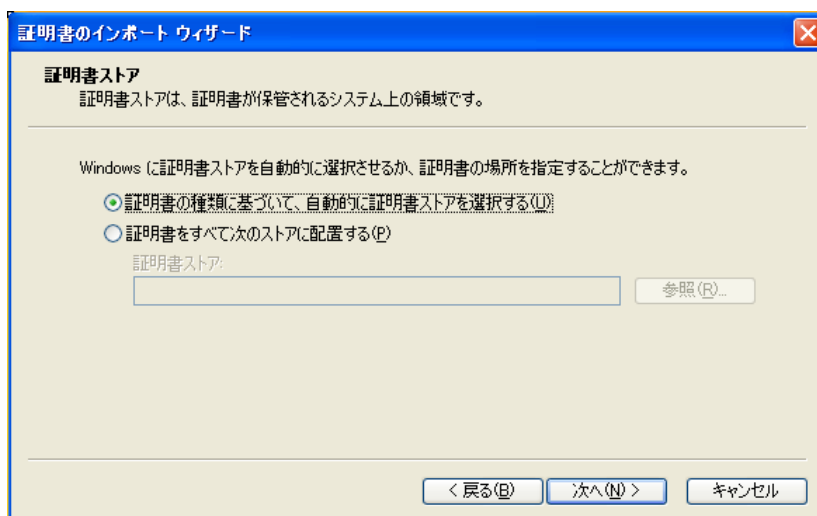


図 9-7 証明書ストア指定

- ④. 証明書のインポートウィザードが完了します。【完了】をクリックします。

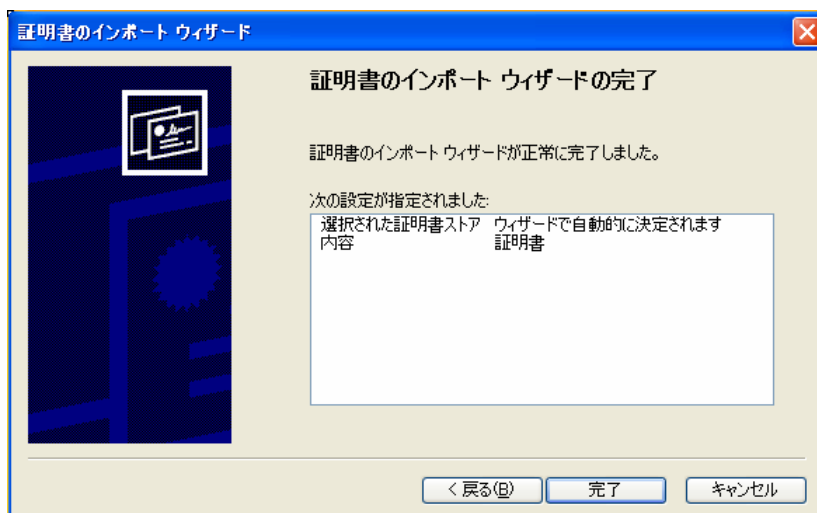


図 9-8 証明書インポートウィザード完了

- ⑤. ルート証明書ストアに追加するダイアログボックスが表示されます。【はい】をクリックします。

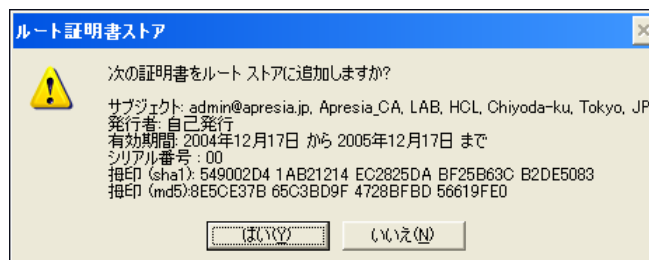


図 9-9 ルート証明書ストアへの追加

⑥. 正常にインポートされ、ルートストアへの追加が完了します。【OK】をクリックします。

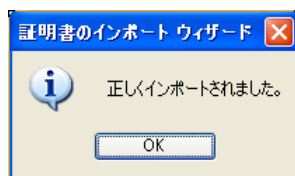


図 9-10 ルートストアへの追加完了

⑦. Internet Explorer の【ツール】－【インターネットオプション】から【コンテンツ】タブを選択し、【証明書】ボタンをクリックすると、信頼されたルート証明機関に追加されたプライベート CA が確認できます。

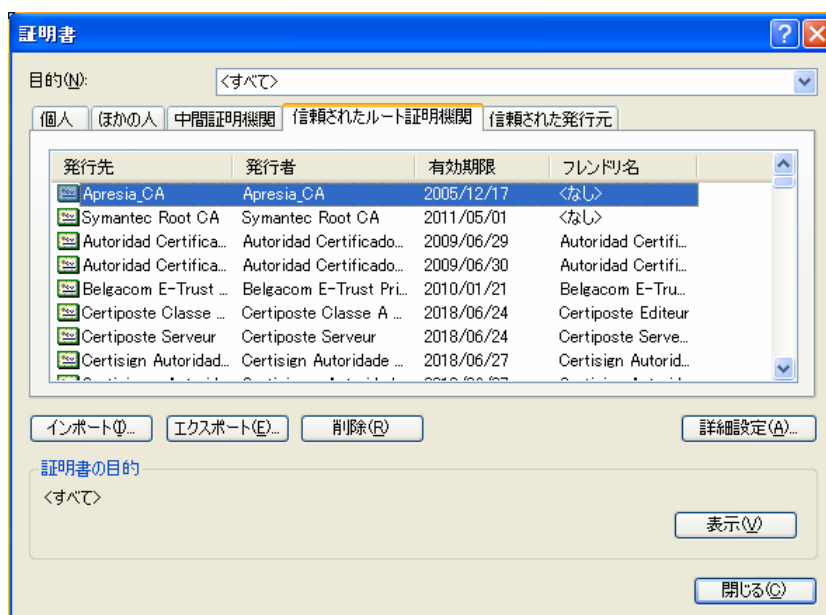


図 9-11 追加されたプライベート CA

9.4 認証URLへアクセス

APRESIA に設定してある認証 URL に対して SSL でアクセスします。

APRESIA にダウンロードしたサーバー証明書と秘密鍵が正しく認識され、端末にプライベート CA の証明書が正しくインポートされていれば、セキュリティ警告が表示されることなく認証画面が表示されます。



図 9-12 認証 URL へのアクセス (SSL 使用)

9.5 証明書の削除(初期化)

作成した証明書要求や証明書、秘密鍵を初期化することができます。デフォルトの状態に戻すには次コマンドを入力して下さい。即時に反映されます。

```
# erase ssl-files
Erasing from flash memory...
done.
```

! ファームウェアをバージョンアップしても証明書は初期化されません。

9.6 中間CA証明書対応について

9.6.1 中間CA証明書とは

中間 CA 証明書とは、サーバー証明書を直接発行している認証局の証明書です。中間 CA 局が署名しているサーバー証明書を使用する場合、証明書チェーンを検証するために中間 CA 証明書もあわせてサーバーに設定する必要があります。証明書の階層構造と、中間 CA 証明書を使用した SSL サーバー認証の概念図を示します。

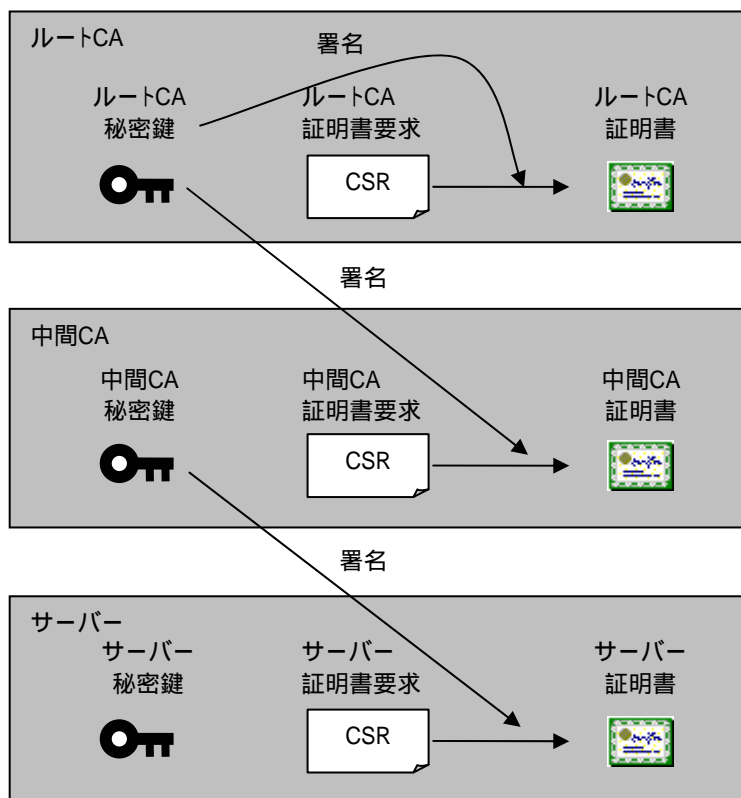


図 9-13 SSL 証明書の階層構造

クライアントは、証明書の有効性を確認する際に、階層すべての証明書を検証します。通常ブラウザにはルート CA 局の証明書が信頼する証明書として格納されているため、サーバーには下位の階層の証明書を設定しておく必要があります。

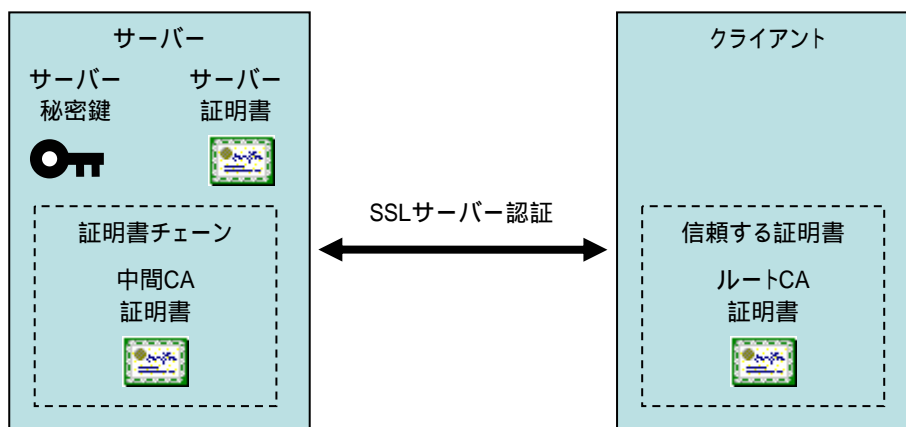


図 9-14 SSL サーバー認証(中間 CA 証明書使用)

9.6.2 証明書要求を装置で発行する場合

証明書要求を装置で発行する場合、9.2 項(証明書要求を装置で発行する場合)を参考にCSRを発行し、中間 CA局にてサーバー証明書を発行してもらいます。

入手したサーバー証明書と、中間 CA 証明書をマージし、1つのファイルにしてから APRESIA にダウンロードしてください。

ダウンロード方法は 9.2.4 証明書のダウンロード のコマンドと同じです。

<サーバー証明書と中間 CA 証明書をマージしたチェーン証明書の例>

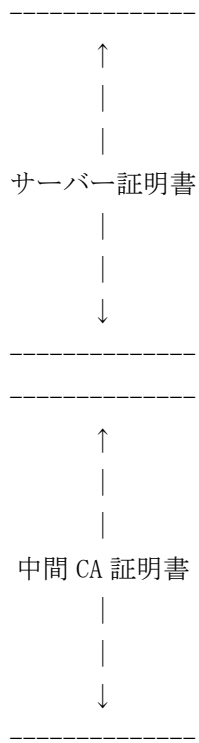
```
-----BEGIN CERTIFICATE-----
MIIDlzCCAwwCgAwIBAgIJAKlq1Sk5D/FCMAOGCSqGSIb3DQEBBQUAMIGXMQswCQYD
VQQGEwJKUDEOMAwGA1UECBMFV9reW8xEzARBgNVBAcTckNoaXlvZGeta3UxZjAU

. . . . . 中略 . . . . .

uGyyaIKP8/57MeIWb4vkDZF+D9XuOYbiqRJIWuIwjr2UFM4P69zBkfEoHeblWboz
RLlvbJdfTKcCreI=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIJAKlq1Sk5D/FBMAOGCSqGSIb3DQEBBQUAMHwxCzAJBgNV
BAYTAkpQM4wDAYDVQQIEwVub2t5bzEWMBQGA1UEChMNSG10YWNoaXlvZGeta3UxZjAU
ZTEl

. . . . . 中略 . . . . .

5nA52bQIcEcDketgTWcNg5Tidf0JE1xDJiDnB7v3IGVY59J3rycVusdyN4+cPgFY
CN8nTz0q
-----END CERTIFICATE-----
```



! ファイル結合順を逆にすると正しいチェーン証明書とはなりませんのでご注意ください。
誤った証明書を入れている場合、HTTPS ポートを有効にした際にエラーメッセージが表示されます。

```
(config-a-def)# web-authentication https-port 443
% Invalid SSL files.
```

9.6.3 証明書要求を装置で発行しない場合

<留意事項>

本セクションの記載内容は、AccessDefender 認証時に SSL 通信させるためのサーバー証明書と秘密鍵を生成する目的の簡易的な認証局(プライベート CA、中間 CA)の設定を含んでいます。

特定ベンダの OS における設定事例を引用しており、実際の運用環境と異なる場合があります。このため記載されている内容そのままでの認証局運用を避けて下さい。



このセクションの内容はサポート対象外となります。

9.6.3.1 発行作業概要

OpenSSL などのソフトウェアを使用し、秘密鍵および CSR を生成します。このセクションでは、Linux 版 OpenSSL (0.9.8i) を使用し、プライベート CA、及び中間 CA を作成しています。

- 1. openssl.cnf の環境設定(中間 CA 証明書に対応するために必要な設定)
↓
- 2. ルート CA 証明書の作成
↓
- 3. 中間 CA 証明書の作成
↓
- 4. サーバー証明書の作成
↓
- 5. チェーン証明書の作成
↓
- 6. APRESIA の環境作成(チェーン証明書とサーバー用秘密鍵のインストール)
↓
- 7. 認証端末の環境作成(ルート CA 証明書のインストール)

9.6.3.1.1 /usr/local/ssl/openssl.cnf の環境設定

(1) [CA_default] に unique_subject を no にする以下の定義を追加
デフォルトでは、“#”でコメントアウトされているので、“#”を削除します。

```
[ CA_default ]  
... (省略) ...  
unique_subject = no          ← コメントを外す  
... (省略) ...
```

(2) my_v3_ext の定義を追加
/usr/local/ssl/openssl.cnf の一番最後に以下の定義を追加します。

```
[ my_v3_ext ]  
basicConstraints = CA:true          ← 追加
```

9.6.3.1.2 ルートCA証明書の作成

事前に変更しておいた「openssl.cnf」ファイルを用いてルートCAを作成します。本例ではOpenSSLのPerlスクリプトを使用しています。

```
# /usr/local/ssl/misc /CA.pl -newca  
CA certificate filename (or enter to create)  
【新規作成のため、そのまま Enter キーを押す】  
Making CA certificate ...  
Generating a 1024 bit RSA private key  
.....+++++  
.....+++++  
writing new private key to './demoCA/private/cakey.pem'          ← CA用秘密鍵の生成  
Enter PEM pass phrase:      【CA用秘密鍵のパスフレーズの入力】  
Verifying - Enter PEM pass phrase:  【CA用秘密鍵のパスフレーズの入力】  
-----  
  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
  
Country Name (2 letter code) [AU]:JP  
State or Province Name (full name) [Some-State]:Tokyo  
Locality Name (eg, city) []:Chiyoda-ku  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi-Cable  
Organizational Unit Name (eg, section) []:NE  
Common Name (eg, YOUR name) []:Apresia_RootCA  
Email Address []:admin@apresia.jp  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:      【Enter キー入力】  
An optional company name []:  【Enter キー入力】  
Using configuration from /usr/local/ssl/openssl.cnf  
Enter pass phrase for ./demoCA/private/cakey.pem:  【CA用秘密鍵のパスフレーズの入力】  
Check that the request matches the signature
```

Signature ok

Certificate Details:

Serial Number:

a9:6a:d5:29:39:0f:f1:40

Validity

Not Before: Nov 6 14:12:00 2008 GMT

Not After : Nov 6 14:12:00 2011 GMT

Subject:

countryName = JP
stateOrProvinceName = Tokyo
organizationName = Hitachi-Cable
organizationalUnitName = NE
commonName = Apresia_RootCA
emailAddress = admin@apresia.jp

X509v3 extensions:

X509v3 Subject Key Identifier:

80:89:AC:3B:E9:F3:4F:06:0B:D7:8D:41:3A:34:57:98:97:4C:21:39

X509v3 Authority Key Identifier:

keyid:80:89:AC:3B:E9:F3:4F:06:0B:D7:8D:41:3A:34:57:98:97:4C:21:39

DirName:/C=JP/ST=Tokyo/O=Hitachi-Cable/OU=NE/CN=Apresia_RootCA/

emailAddress=admin@apresia.jp

serial:A9:6A:D5:29:39:0F:F1:40

X509v3 Basic Constraints:

CA:TRUE

Certificate is to be certified until Nov 6 14:12:00 2011 GMT (1095 days)

Write out database with 1 new entries

Data Base Updated

実行後、2つのファイルが主に生成されます。

- cacert.pem(ルート CA 証明書)
- cakey.pem(ルート CA 用秘密鍵)



秘密鍵のパスフレーズを絶対に忘れないようにして下さい。

作成したルート CA 証明書は、端末にインストールするために DER(Distinguished Encoding Rules)形式のファイル(ca.der)に変換しておきます。

```
# openssl x509 -inform PEM -in cacert.pem -outform DER -out ca.der
```

9.6.3.1.3 中間CA証明書の作成

(1) 中間 CA の秘密鍵と証明書要求の作成

```
# /usr/local/ssl/misc/CA.pl -newreq
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:      【中間 CA 用秘密鍵のパスフレーズの入力】
Verifying - Enter PEM pass phrase:      【中間 CA 用秘密鍵のパスフレーズの入力】
-----

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Tokyo
Locality Name (eg, city) []:Chiyoda-ku
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi-Cable
Organizational Unit Name (eg, section) []:NE
Common Name (eg, YOUR name) []:Apresia_IntermediateCA
Email Address []:ica@apresia.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:      【Enter キー入力】
An optional company name []:   【Enter キー入力】
Request is in newreq.pem, private key is in newkey.pem
```

実行後、2つのファイルが生成されます。

- newkey.pem(中間 CA 用秘密鍵)
- newreq.pem(証明書要求)



秘密鍵のパスフレーズを絶対に忘れないようにして下さい。

(2) 中間 CA の秘密鍵と証明書要求のファイル名の変更

```
# mv newkey.pem icakey.pem
# mv newreq.pem icareq.pem
```

(3) 中間 CA 証明書の作成(ルート CA の秘密鍵による署名)

```
# openssl ca -policy policy_anything -extensions my_v3_ext -out icacert.pem -infile icareq.pem
Using configuration from /usr/local/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/akey.pem:      【CA用秘密鍵のパスフレーズの入力】
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number:
    a9:6a:d5:29:39:0f:f1:41
  Validity
    Not Before: Nov  6 14:19:00 2008 GMT
    Not After  : Nov  6 14:19:00 2009 GMT
  Subject:
    countryName           = JP
    stateOrProvinceName  = Tokyo
    localityName         = Chiyoda-ku
    organizationName     = Hitachi-Cable
    organizationalUnitName = NE
    commonName           = Apresia_IntermediateCA
    emailAddress        = ica@apresia.jp
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:TRUE
Certificate is to be certified until Nov  6 14:19:00 2009 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

実行後、コマンドで指定したファイルが生成されます。

- icacert.pem(中間 CA 証明書)

9.6.3.1.4 サーバ証明書の作成

(1) APRESIA 認証用 Web サーバの秘密鍵と証明書要求の作成

```
# /usr/local/ssl/misc/CA.pl -newreq
Generating a 1024 bit RSA private key
.+++++
.....+++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:      【サーバ用秘密鍵のパスフレーズの入力】
Verifying - Enter PEM pass phrase:      【サーバ用秘密鍵のパスフレーズの入力】
-----

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Tokyo
Locality Name (eg, city) []:Chiyoda-ku
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi-Cable
Organizational Unit Name (eg, section) []:NE
Common Name (eg, YOUR name) []:1.1.1.1                ← 重要ポイント
Email Address []:srv@apresia.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:      【Enter キー入力】
An optional company name []:   【Enter キー入力】
Request is in newreq.pem, private key is in newkey.pem
```

実行後、2つのファイルが生成されます。

- newkey.pem(中間 CA 用秘密鍵)
- newreq.pem(証明書要求)

! Common Name(CN)は、APRESIAの認証 URL で指定するホスト名にする必要があります(この例では「https://1.1.1.1/」が認証 URL になります)。認証 URL と CN が異なる場合、セキュリティ警告が表示されます。

! 秘密鍵のパスフレーズを絶対に忘れないようにして下さい。

(2) サーバー用秘密鍵と証明書要求のファイル名の変更

```
# mv newkey.pem srvkey.pem
# mv newreq.pem srvreq.pem
```

(3) サーバー証明書の作成(中間 CA の秘密鍵による署名)

```
# openssl ca -policy policy_anything -keyfile icakey.pem -cert icacert.pem -out srvcert.pem
-infiles srvreq.pem
```

```
Using configuration from /usr/local/ssl/openssl.cnf
```

```
Enter pass phrase for icakey.pem: 【中間 CA 用秘密鍵のパスフレーズの入力】
```

```
Check that the request matches the signature
```

```
Signature ok
```

```
Certificate Details:
```

```
Serial Number:
```

```
a9:6a:d5:29:39:0f:f1:42
```

```
Validity
```

```
Not Before: Nov  6 14:22:00 2008 GMT
```

```
Not After : Nov  6 14:22:00 2009 GMT
```

```
Subject:
```

```
countryName           = JP
stateOrProvinceName   = Tokyo
localityName           = Chiyoda-ku
organizationName       = Hitachi-Cable
organizationalUnitName = NE
commonName             = 1.1.1.1
emailAddress           = srv@apresia.jp
```

```
X509v3 extensions:
```

```
X509v3 Basic Constraints:
```

```
CA:FALSE
```

```
Netscape Comment:
```

```
OpenSSL Generated Certificate
```

```
X509v3 Subject Key Identifier:
```

```
C5:D2:1E:9F:13:8C:05:F2:1D:C1:98:FE:84:C8:0E:63:E0:7C:57:3A
```

```
X509v3 Authority Key Identifier:
```

```
DirName:/C=JP/ST=Tokyo/O=Hitachi-Cable/OU=NE/CN=Apresia_RootCA/
emailAddress=admin@apresia.jp
serial:A9:6A:D5:29:39:0F:F1:41
```

```
Certificate is to be certified until Nov  6 14:22:00 2009 GMT (365 days)
```

```
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
```



```
Write out database with 1 new entries
Data Base Updated
```

実行後、コマンドで指定したファイルが生成されます。

- `srvcert.pem` (サーバー証明書)

9.6.3.1.5 チェーン証明書の作成

サーバー証明書 (`srvcert.pem`) に中間 CA 証明書 (`icacert.pem`) をマージしたチェーン証明書を作成します。

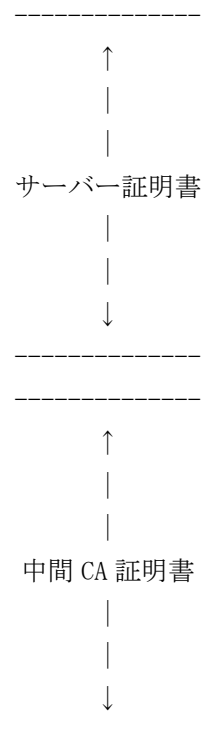
```
# cat srvcert.pem icacert.pem > chaincert.pem
```

<サーバー証明書と中間 CA 証明書をマージしたチェーン証明書の例>

```
-----BEGIN CERTIFICATE-----
MIID1zCCAwCgAwIBAgIJAK1q1Sk5D/FCMA0GCSqGSIb3DQEBBQUAMIGXMQswCQYD
VQQGEwJKUDEOMAwwGA1UECBMFVG9reW8xEzARBgNVBACTCkNoaXlvZGeta3UxFljAU
. . . . . 中略 . . . . .

uGyyaIKP8/57MeIwB4vkDZF+D9Xu0YbiqRJIWuIwjR2UFM4P69zBkfEoHeblWboz
RLLvbJdfTKcCreI=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICojCCAagugAwIBAgIJAK1q1Sk5D/FBMA0GCSqGSIb3DQEBBQUAMHwxCzAJBgNV
BAYTAkpQMq4wDAYDVQQIEwVUb2t5bzEWMBQGA1UEChMNSG10YWNoaS1DYWJsZTEl
. . . . . 中略 . . . . .

5nA52bQIcEcDketgTWcNg5Tidf0JE1xDJiDnB7v3IGVY59J3rycVusdyN4+cPgFY
CN8nTz0q
-----END CERTIFICATE-----
```



! ファイル結合順を逆にすると正しいチェーン証明書とはなりませんのでご注意ください。
誤った証明書を入れている場合、HTTPS ポートを有効にした際にエラーメッセージが表示されます。

```
(config-a-def)# web-authentication https-port 443
% Invalid SSL files.
```

9.6.3.1.6 APRESIAの環境作成(チェーン証明書とサーバー用秘密鍵のダウンロード)

生成したチェーン証明書(chaincert.pem)とサーバー用秘密鍵(srvkey.pem)を APRESIA にダウンロードします。

(1)チェーン証明書のダウンロード


```
# copy tftp 192.168.1.1 chaincert.pem https-certificate
```

・・・TFTP サーバー(192.168.1.1)からチェーン証明書のダウンロード

(2)サーバー用秘密鍵のダウンロード

```
# copy tftp 192.168.1.1 srvkey.pem https-private-key
```

・・・TFTP サーバー(192.168.1.1)からサーバー秘密鍵のダウンロード

 秘密鍵は厳重に管理して下さい。

9.6.3.1.7 認証端末の環境作成(ルートCA証明書のインストール)

ルート CA 証明書(ca.der)を信頼されたルート証明機関として端末にインストールします。
方法は 9.3.4 信頼されたルート証明機関として登録 を参照下さい。

9.6.4 認証URLへアクセス(証明書の確認)

APRESIA にダウンロードしたチェーン証明書と秘密鍵が正しく認識され、端末にルート CA 証明書が正しくインポートされていれば、セキュリティ警告が表示されることなく認証画面が表示されます。

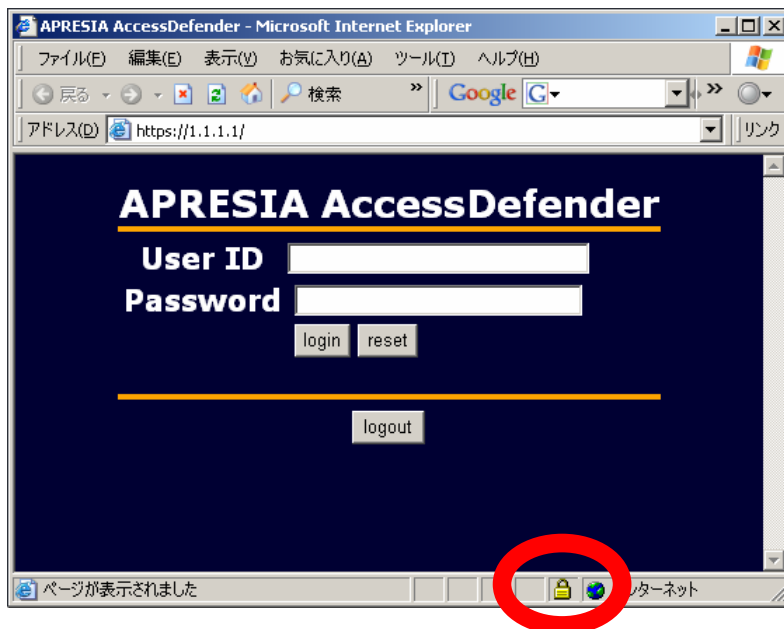


図 9-15 認証 URL へのアクセス (SSL 使用)

認証画面が表示されているウィンドウの上記赤丸部分の鍵アイコンをダブルクリックすることで、SSL で使用されている証明書のパスなどが確認できます。

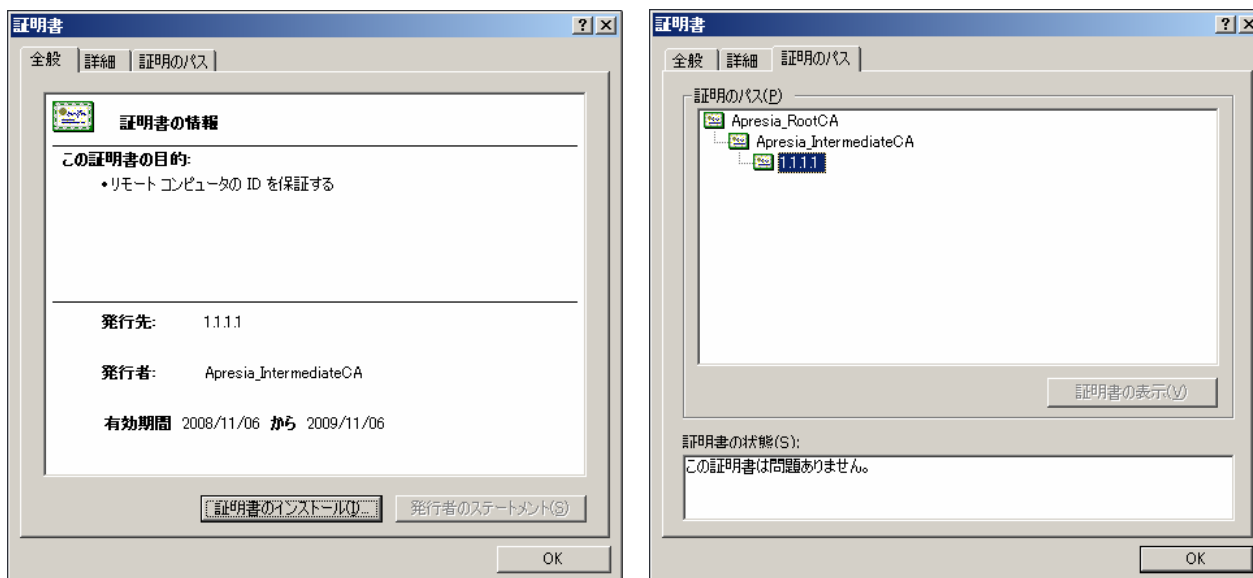


図 9-16 証明書情報表示例

10. AccessDefender機能に関するリリース情報

AEOS Ver. 7 で実装されているAccessDefender機能に関する機能追加・変更・修正点を表 10-1 にまとめています。AccessDefender以外の機能の内容や、AccessDefender機能に関する機能追加・変更点がないバージョンは本表には含まれていません。

表 10-1 AEOS Ver. 7 での機能追加・変更点(AccessDefender 関連機能)

バージョン	管理番号	内容
7.08.01	AEOS-70801-RC001	Apresia4328GT に対応
	AEOS-70801-RC002	Apresia4328GT にて下記機能に対応 <ul style="list-style-type: none"> AccessDefender 機能 packet-filter2 authentication-bypass 機能
	AEOS-70801-RC005	packet-filter2 機能に使用中のグループ数を参照するコマンド“show packet-filter2 reserved-group”を追加
7.08.02	AEOS-70802-RC004	高負荷時に認証 Web サーバーが停止する可能性がある問題を修正
7.08.03	AEOS-70803-RC001	Apresia4328GT シリーズにおいて、Web 認証を行っている (MAC 認証との併用を含む) 場合に、APRESIA が Web 認証ポートに接続した認証前の端末 (MAC アドレスが xx:06:xx:xx:xx:xx) の ARP を解決できず、ユーザー認証 (IP 通信) 不可となる問題を修正 ➤ 関連情報 : FN 13A13-1
7.09.01	AEOS-70901-RC001	Apresia4348 シリーズに対応 (ローダファームウェアは version 1.02.02 以降対応)
	AEOS-70901-RC005	Apresia4348 シリーズ及び Apresia13000-48X において、AccessDefender 機能に対応
	AEOS-70901-RC006	AccessDefender 機能において下記サポート <ul style="list-style-type: none"> logout aging 及び logout timeout の設定可能範囲を拡張 L3 中継との併用をサポート (L3 の経路制御プロトコル (RIP, OSPF) とのポート併用及び VRRP 機能との併用は不可)
	AEOS-70901-RC061	AccessDefender 機能において、aaa-loc1-db をダウンロードしていない状態では“aaa authentication”が設定できない問題を修正
	AEOS-70901-RC062	AccessDefender 機能において、Web 認証成功時に RADIUS サーバーから返却される VSA (NA-Vlan-ID) において、ベンダー ID が 278 (HCL) 以外の場合でも属性値が 192 (NA-Vlan-ID) なら NA-Vlan-ID として処理される問題を修正
7.10.01	AEOS-71001-RC001	Apresia13000-24GX-PSR に対応 (ローダファームウェアは version 1.03.01 以降対応)
	AEOS-71001-RC005	discard に登録できる MAC アドレス数を 32→100 個に変更
	AEOS-71001-RC017	特定ブラウザで認証ページリダイレクトを用いた認証ページの表示が行われない問題を修正
	AEOS-71001-RC018	認証 Web ページをダウンロード中「copy tftp WEB-PAGE」に「erase WEB-PAGE」を実施すると消去失敗メッセージ「% Cannot write Web files.」が表示されるが実際は消去されてしまう問題を修正

7. 11. 04	AEOS-71101-RC002	<p>下記機能拡張 (AccessDefender Phase2 機能に対応)</p> <p>本機能対応に伴い、旧来の 802. 1X 機能、DHCP スヌーピング機能の使用ができなくなります (AEOS-70901-ER013 (Apresia13000-48X において、「show dot1x」コマンドが VIEW モードにて実行できない問題) もなくなります)</p> <ul style="list-style-type: none"> ・ Web 認証高速化 ・ ローミング ・ linkdown ログアウト無効 ・ 802. 1X ・ DHCP スヌーピング ・ 強制認証 DVLAN <p>➤ 関連情報：AEOS-70901-ER013</p>
	AEOS-71101-RC007	<p>ログ仕様を一部変更 (詳細はログ・トラップ対応一覧を参照)</p> <p>➤ 関連情報：TD61-3755</p>
	AEOS-71102-RC001	<p>AccessDefender コマンド関連の構成情報「show running config」の表示位置を変更</p>
	AEOS-71104-RC002	<p>Web、MAC、802. 1X 認証で動的な VLAN 変更をした端末がログアウトすると、同一 VID の認証済の他端末が通信不可となる問題を修正 (7. 11. 01 (CF)、7. 11. 02 (CF) のみで発生)</p> <p>➤ 関連情報：AEOS-71102-ER001</p>
	AEOS-71104-RC003	<p>802. 1X 認証とポートリダウンド機能を同時に設定すると機器が再起動する問題を修正 (7. 11. 01 (CF)、7. 11. 02 (CF) のみで発生)</p>
7. 12. 01	AEOS-71201-RC001	<p>新機種に対応</p> <ul style="list-style-type: none"> ・ Apresia3424GT-SS ・ Apresia3424GT-PoE
	AEOS-71201-RC002	<p>パケットフィルタ 2 機能において、condition に src arp-sender-ip 設定を追加</p>
	AEOS-71201-RC008	<p>中間 CA 証明書に対応</p>
	AEOS-71201-RC009	<p>local-db のサイズを拡張 (28Kbyte⇒256Kbyte)</p>
	AEOS-71201-RC010	<p>「show ssl」コマンドを VIEW モードに追加</p>
	AEOS-71201-RC032	<p>認証高負荷時に login success/failure ログの時間情報が異常値となる問題を修正</p>
	AEOS-71201-RC033	<p>「no dot1x port <PORT>」コマンドによるログアウト時、ログにログアウト要因が linkdown と出力される問題を修正</p>
	AEOS-71201-RC034	<p>802. 1X による認証数が多い場合に、802. 1X の設定変更 (「no dot1x enable」「no dot1x port <PORT>」「dot1x port <PORT> initialize」) を行った場合に CLI の応答が遅い問題を修正</p>
	AEOS-71201-RC035	<p>「sshd keygen rsa1 4096」コマンドで作成した鍵を show コマンドで正しく表示できない問題を修正</p>
AEOS-71201-RC036	<p>「web-auth https-port」が設定され、かつ「ssl gensr」コマンドで証明書要求・秘密鍵を生成されている状態で、web-auth 設定を無効⇒有効 (「no web-auth enable」⇒「web-auth enable」または装置再起動) とすると、認証画面を表示できない問題を修正</p>	

	AEOS-71201-RC037	MAC 認証ポートに端末が登録されている状態で、MAC 認証のポート設定を無効(no mac-authentication port)にすると、認証状態が不正に残り、登録端末の通信が出来ない場合がある問題を修正
	AEOS-71201-RC038	aaa authentication 未設定時、「show access-defender aaa-local-db」が表示されない問題を修正
7. 13. 01	AEOS-71301-RC003	AccessDefender 機能に下記機能を追加しました。 <ul style="list-style-type: none"> - Web/MAC 認証モードを追加しました。 - コマンドラインからのログアウト方式を拡張し、ユーザーID/IP/MAC 指定による認証端末のログアウトを可能にしました。 - ポートベース VLAN 機能を追加しました。 - DHCP スヌーピング機能が DHCP インフォームフレームに対応しました。 - MAC 認証による動的 VLAN 生成時に DHCP による IP アドレス取得を可能にしました。
	AEOS-71301-RC023	AccessDefender 機能において、aaa authentication mac radius <INDEX> と aaa authentication web radius <INDEX>設定が両方ある場合に aaa radius <INDEX> host <IPADDR>を変更(上書き)しても動作に反映されない問題を修正しました。
	AEOS-71301-RC028	Apresia13000-48X および 4348 シリーズの AccessDefender 機能において、通信中の端末が aging logout する問題を修正しました。
7. 14. 01	AEOS-71401-RC002	Apresia4328GT において、MAC 認証、Web 認証、IGMP スヌーピング機能、MLD スヌーピング機能の併用が可能になりました(MAC、Web 認証は固定 VLAN のみ対応)。
	AEOS-71401-RC004	AccessDefender 機能において、WEB 認証動作中に web-authentication enable と no web-authentication enable を継続的に実施すると、WEB 認証が行えなくなる問題を修正しました。
7. 15. 01	AEOS-71501-RC008	AccessDefender と IGMP-Snooping/MLD スヌーピングのポート併用に対応しました。
	AEOS-71501-RC019	AccessDefender の DHCP スヌーピング機能において、VLAN タグ内のユーザープライオリティが 0 以外の DHCP フレームをスヌーピングしない問題を修正しました。
	AEOS-71501-RC020	AccessDefender の DHCP スヌーピング機能において、別装置の DHCP サーバーが DHCP スヌーピング対象の複数端末に同一 IP アドレスを配布している状態(DHCP サーバーを再起動した場合等に発生)では、DHCP スヌーピング対象の端末のログアウトが行えない問題を修正しました。
	AEOS-71501-RC021	AccessDefender のダイナミック VLAN 機能において、同一ポート/同一 VLAN に属する複数の認証済み端末が完全に同期したタイミングでログアウトすると認証済み VLAN の設定が不正に残る問題を修正しました。
7. 16. 02	AEOS-71602-RC009	AccessDefender 機能において、MAC 認証後端末に対してのみ DHCP スヌーピング動作をさせる機能を追加しました。これに伴い下記のコマンドを追加、拡張しました。 <ul style="list-style-type: none"> • dhcp-snooping mode mac-authentication コマンド • show access-defender dhcp-snooping configuration コマンド • show access-defender dhcp-snooping status コマンド • show access-defender dhcp-snooping mode status コマンド

	AEOS-71602-RC003	AccessDefender 機能において、装置がデフォルトで持つ Web サーバー証明書の発行元と発行者を” Apresia” に統一しました。
7. 17. 01	AEOS-71701-RC010	AccessDefender 機能において、Web 認証の高速化及び RADIUS を用いた認証の高速化を行いました。
	AEOS-71701-RC023	AccessDefender 機能において、802. 1X 認証がサブリカント側から認証開始すると、タイミングによって認証失敗する場合があります問題を修正しました。
	AEOS-71701-RC024	AccessDefender 機能において、ローカルデータベースを連続してダウンロードを行うと装置が再起動する問題を修正しました。
	AEOS-71701-RC025	AccessDefender 機能において、” dhcp-snooping static-entry” 登録の失敗(packetfilter2のリソース不足)時に構成情報(running-config)に設定が入る問題を修正しました。
7. 18. 01	AEOS-71801-RC003	AccessDefender 機能において、” dhcp-snooping mode mac-authentication” コマンド実行時のログを” <process:info> A-Def : dhcpsnooping : mode changed to macauthentication mode enable” に変更しました。
7. 19. 01	AEOS-71901-RC002	AccessDefender 機能において、Web 認証において認証方法を<ID>で指定できるようにしました(認証方法選択機能)。 <ul style="list-style-type: none"> ” aaa authentication web <ID> radius <INDEX1> [<INDEX2>] [local force]” ” aaa authentication web <ID> local [radius <INDEX1> [<INDEX2>]]”
	AEOS-71901-RC003	AccessDefender 機能において、認証方法の順序を変更できるようにし、かつ、複数の認証方法が設定されている場合は、認証移行条件(最初の認証方法で失敗した時に次の認証方法に移行するかどうか)を設定できるようにしました(認証順序・移行条件変更機能)。 <ul style="list-style-type: none"> ” aaa authentication (web [<ID>] mac) radius <INDEX1> [<INDEX2>] [local (force [vlan <VID>])]” ” aaa authentication (web [<ID>] mac) local [radius <INDEX1> [<INDEX2>] force [vlan <VID>]]” ” aaa authentication (web [<ID>] mac) force [vlan <VID>]]” ” aaa authentication dot1x radius <INDEX1> [<INDEX2>] [force [vlan <VID>]]” ” aaa authentication dot1x force [vlan <VID>]]” ” aaa authentication (web [<ID>] mac) control sufficient”
	AEOS-71901-RC004	AccessDefender 機能において、認証を拒否する端末を設定できるようにしました(認証拒否機能)。 <ul style="list-style-type: none"> ” packet-filter2 max-rule <MAX-RULE> [deny-rule <DENY-RULE>]” ” access-defender-deny mac <MAC address> timer <1-60min>” ” access-defender-deny ip <IP address> timer <1-60min>” ” show access-defender deny”
	AEOS-71901-RC005	AccessDefender 機能において、エージングログアウトとログイン時間ログアウトにおいて、認証方式([dot1x gateway mac web])を指定できるようにしました(認証方式指定ログアウト機能) <ul style="list-style-type: none"> ” logout aging-time <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]] [dot1x gateway mac web]” ” logout timeout <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]]”

		[dot1x gateway mac web]”
	AEOS-71901-RC019	AccessDefender 機能において、SSL 脆弱性問題を修正しました。
	AEOS-71901-RC020	AccessDefender 機能において、Web 認証+認証 Bypass 設定有りの場合、ARPrequest 送出まで数十秒かかることがある問題を修正しました。
7. 20. 01	AEOS-72001-RC002	AccessDefender 機能において、802. 1X 認証に先立ち端末の MAC アドレスによる認証を実施する 802. 1X/MAC 認証機能のコマンド(“dot1x mac-authentication-password”)をサポートしました。
	AEOS-72001-RC003	AccessDefender 機能において、Web 認証と Web/MAC 認証を装置内で併用するコマンド(“web-authentication port <PORT> mac-authentication”)を追加しました。
	AEOS-72001-RC007	AccessDefender 機能において、リンク状態変化の監視を高速化(約 5 秒から約 1 秒に)しました。
	AEOS-72001-RC008	AccessDefender 機能において、MAC 認証の性能を向上させました。
	AEOS-72001-RC009	AccessDefender 機能において、802. 1X 認証と MAC 認証をポート併用した場合に 802. 1X 認証登録後に MAC 認証の Discard 登録を削除するようにしました。また、再認証時に不要な duplicate ログが発生しないようにしました。
7. 21. 01	AEOS-72101-RC021	AccessDefender 機能において、802. 1X 認証のログインまたはログアウトが複数端末で一斉に行われる動作を長時間継続した場合、ごく稀に装置が再起動する問題を修正しました。
	AEOS-72101-RC022	AccessDefender 機能において、802. 1X 認証の” logout aging-time” 値が設定されており、認証済み端末が無通信状態の間に、” logout aging-time” 値の設定を変更すると、変更前の設定値でエージングログアウトされる問題を修正しました。
7. 22. 01	AEOS-72201-RC001	AccessDefender 機能において、時刻指定ログアウトに対応しました。 下記コマンドで設定した時刻になると、認証方式毎に認証済み端末のログアウトを行い、未認証状態にします。 ・logout clock HH:MM [dot1x gateway mac web] ※gateway の指定は Apressial3000 シリーズのみ有効
	AEOS-72201-RC002	AccessDefender 機能において、VRRP 機能とのポート併用をサポートしました。
	AEOS-72201-RC003	AccessDefender 機能の 802. 1X 認証において、ログアウトのログメッセージを他認証のメッセージに合わせるように仕様を変更しました。
	AEOS-72201-RC010	AccessDefender 機能において、NA 機能が設定された装置に AccessDefender 機能の設定をダウンロードすると認証が正常に動作しない問題を修正しました。
	AEOS-72201-RC011	AccessDefender 機能において、Web 認証に関する設定の数/設定文字数が最大の場合に、装置が再起動する問題を修正しました。
	AEOS-72201-RC012	AccessDefender 機能において、%s を含んだ UserID にて Web 認証ができない問題を修正しました。
7. 23. 01	AEOS-72301-RC003	AccessDefender 機能において、MAC 認証、Web 認証、ゲートウェイ認証でログイン成功/ログイン失敗/ログアウト時のトラップ出力をサポートしました。

7. 24. 01	AEOS-72401-RC003	Apressia5412GT-HRSS/5412GT-HRSS-DC48V/5412GT-HRSS-DC110V において、AccessDefender 機能をサポートしました。
	AEOS-72401-RC004	AccessDefender 機能において、認証ポートのリンクダウンがリンクダウン監視時間(” logout linkdown time <TIME>” で設定)継続しない場合は、認証済み端末をログアウトさせない機能をサポートしました。 <ul style="list-style-type: none"> • ” logout linkdown time port <PORTS> enable” • ” logout linkdown time <TIME>”
7. 26. 01	AEOS-72601-RC022	AccessDefender機能において、最終行に改行がないローカルデータベースをダウンロード後に” aaa-local-db add user” コマンドでユーザー追加を行うと、ローカルデータベースの内部情報が不正になる問題を修正しました。

AEOS Ver. 7 アプリケーションノート
(AccessDefender 編)

Copyright(c) 2011 Hitachi Cable, Ltd.

2008年6月初版

2011年10月第6版

日立電線株式会社

東京都千代田区外神田四丁目14番1号

秋葉原UDX