TD61-4455L

Apresia13000/13100/13200/15000 シリーズ

AEOS Ver. 8 アプリケーションノート

(AccessDefender 編)

APRESIA Systems 株式会社

制 定 ・ 改 訂 来 歴 表

No.	年　　月　　日	内　　容
-	2010 年 5 月 5 日	• AEOS Ver.8.06 ベースにて新規作成
A	2010 年 7 月 9 日	• AEOS Ver.8.07 に対応 • 1.5 DHCP Snooping 概要を追加 • 2.5 Web/MAC 認証(Web 認証時の MAC 認証先行)を追加 • 2.6.3 動作確認済サプリカント一覧を追加 • 2.7 DHCP Snooping を追加 • 2.8 認証機能と仕様を修正 • 2.8.2 最大認証端末数について(DHCP Snooping)を追加 • 2.10 ログアウト処理についてを修正 • 3.1 APRESIA の設定項目を修正 • 3.8 認証方法選択機能(Web 認証のみ)を追加 • 4.1 Web 認証の設定例を修正 • 4.3 Web 認証、MAC 認証の混在環境の設定例を修正 • 4.4 Web/MAC 認証を追加 • 4.5 ゲートウェイ認証(サーバーファーム手前に適用)の構成を修正 • 4.8 DHCP Snooping を追加 • 4.9 DHCP Snooping/MAC 認証の混在環境構成例を追加 • 4.10 DHCP Snooping/Web 認証(固定 VLAN)の混在環境構成例を追加 • 4.11 DHCP Snooping/Web 認証(動的 VLAN)の混在環境構成例を追加 • 6.1.3 認証方法選択機能の認証ページカスタマイズを追加 • 6.6.1.3 認証ページリダイレクト機能設定例を修正 • 6.6.2.3 認証ページリダイレクト機能設定例を修正 • 6.7 固定 IP アドレス端末の接続(DHCP Snooping)を追加 • 7 制限事項、及び注意事項を修正 • 7.2 Windows 標準サプリカントにおける 802.1X の問題点を修正
B	2010 年 10 月 19 日	• Apresia13200 シリーズに対応 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 8-1 認証ログ表示例を修正 • 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 • 2.7 802.1X/MAC 認証(802.1X の認証時の MAC 認証先行)を追加 • 2.9.2 最大認証端末数について(DHCP Snooping)の説明を修正 • 3.3.5 ローカルデータベースの編集(追加)を追加 • 3.3.6 ローカルデータベースの編集(削除)を追加 • 3.9 認証拒否機能の注意事項を削除 • 3.11 PING ログアウトを追加 • 4.8 802.1X/MAC 認証を追加
C	2011 年 1 月 20 日	• 表 7-1 制限事項、及び注意事項を修正 • 3.9 認証バイパスの見出しと記載場所を変更 • 3.11 認証ページのリダイレクト機能の記載場所を変更 • 3.12 DHCP Snooping の固定 IP アドレス端末接続の見出しと記載場所を変更 • 6.5 端末認証後のパケットフィルター2(アクション none)を追加

No.	年　月　日	内　　容
D	2011 年 3 月 30 日	• 適用機種一覧を修正 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 2-3 AccessDefender で使用するパケットフィルター2 のグループ数を修正 • 表 2-4 パケットフィルター2 のグループを使用するコマンドを追加 • 表 2-5 DHCP Snooping 最大認証端末数一覧表を修正 • 表 3-3 ローカルデータベースフォーマットを修正 • 表 5-1 認証応答で使用するベンダー独自属性を追加 • 表 7-1 制限事項、及び注意事項を削除 • 1.6 ユーザーポリシーコントロール概要を追加 • 2.5 Web/MAC 認証(Web 認証時の MAC 認証先行)の注意事項を削除 • 2.7 802.1X/MAC 認証(802.1X の認証時の MAC 認証先行)の注意事項を削除 • 2.9 ユーザーポリシーコントロールの動作フローを追加 • 2.10.1 認証端末数とパケットフィルター2 のグループ数を修正 • 2.10.2 DHCP Snooping の認証端末数を修正 • 3.3.5 ローカルデータベースの編集(追加)を修正 • 4.13 ユーザーポリシーコントロール構成例を追加 • 5.1.2 ユーザー情報の登録(users ファイルなど)を修正 • 5.1.3 拡張設定(VLAN ID/クラス ID の設定)を修正 • 5.5.3 VSA の設定(VLAN ID/クラス ID 変更時のみ必要)を修正 • 5.6.4 Web 認証、MAC 認証のネットワークポリシー設定を修正 • 7 制限事項、及び注意事項を修正
E	2011 年 10 月 27 日	• 表 2-6 動作可否確認済みブラウザー(認証ページリダイレクト使用時)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 • 2.5 Web/MAC 認証(Web 認証時の MAC 認証先行)から注意事項を削除 • 3.7 移行条件変更機能(Web 認証、MAC 認証のみ)に注意事項を追加 • 3.11.1.2 認証フローの注意事項を修正 • 3.11.2.2 認証フローの注意事項を修正 • 3.11.3.3 HTTPS を用いる際の注意点の設定例を修正 • 3.18 Web/MAC 認証の MAC 認証属性を追加 • 4.1 Web 認証の設定例を修正 • 4.3 Web 認証、MAC 認証の混在環境の設定例を修正 • 4.9 DHCP Snooping の設定例を修正 • 4.13.1 クラス ID 端末環境の設定例を修正 • 4.13.2 クラス ID 端末/クラス ID 未付与端末の混在環境の設定例を修正 • 9.2.1 秘密鍵、及び CSR の生成に注意事項を追加
F	2013 年 11 月 29 日	• 全章を対象に誤字・脱字・体裁を修正 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 2-3 AccessDefender で使用するパケットフィルター2 のグループ数を修正 • 表 2-4 パケットフィルター2 のグループを使用するコマンドを修正

No.	年　月　日	内　　容
		• 表 2-7 ログアウト処理を修正 • 表 3-3 ローカルデータベースフォーマットを修正 • 表 5-1 認証応答で使用するベンダー独自属性を修正 • 表 5-3 認証応答で使用するベンダー独自属性を追加 • 表 8-1 認証ログ一覧を修正 • 表 8-2 ログアウトで表示されるタイプ一覧を修正 • 表 8-3 AccessDefender 設定時のコンフリクトメッセージ一覧を修正 • 表 10-1 各バージョンでの機能追加、変更点を追加 • 図 2-11 Web/802.1X 認証(AND)の認証フロー(802.1X 先行時)を追加 • 図 3-14 プロキシサーバーがある環境での認証フローを修正 • 図 3-15 認証ページリダイレクト構成例(プロキシ環境)を修正 • 図 3-27 Web/MAC 認証(AND)の MAC 認証属性フローを変更 • 図 4-2 Web 認証構成例(MLAG 併用)を追加 • 図 4-4 MAC 認証構成例(MLAG 併用)を追加 • 図 4-7 ゲートウェイ認証構成例(サーバーファーム手前適用)を修正 • 図 4-8 ゲートウェイ認証構成例(サーバーファーム手前適用、MLAG 併用)を追加 • 図 4-11 802.1X 構成例(MLAG 併用)を追加 • 図 4-13 Web/802.1X 認証(AND)構成例を追加 • はじめにを修正 • 適用機種一覧表を修正 • 2.1 Web 認証(Web ブラウザーによるユーザー認証)に注意事項を追加 • 2.2 ゲートウェイ認証に注意事項を追加 • 2.3 MAC 認証(MAC アドレスによる端末認証)を修正 • 2.5 Web/MAC 認証(AND) (Web 認証時の MAC 認証先行)を修正、及び注意事項を削除 • 2.7 802.1X/MAC 認証(AND) (802.1X の認証時の MAC 認証先行)を修正 • 2.8 Web/802.1X 認証(AND) (Web 認証と 802.1X の併用認証)を追加 • 2.9.2 DHCP Snooping の動作フローを修正 • 2.11.2 DHCP Snooping の認証端末数を修正 • 2.13 ログアウト処理についてを修正 • 3.2 ローカルデータベース認証と強制認証を修正 • 3.3 ローカルデータベースによる認証(Web 認証、MAC 認証のみ)に注意事項を追加 • 3.3.2 ローカルデータベースの登録(ダウンロード)を修正 • 3.3.3 ローカルデータベースのバックアップ(アップロード)を修正 • 3.3.5 ローカルデータベースの編集(追加)を修正 • 3.5 強制認証機能(802.1X)を修正 • 3.6 認証順序変更(Web 認証、MAC 認証のみ)を修正 • 3.7 移行条件変更機能(Web 認証、MAC 認証のみ)を修正 • 3.8 認証方法選択機能(Web 認証のみ)を修正 • 3.11.1.2 認証ページリダイレクト機能設定例を修正 • 3.11.2.2 認証ページリダイレクト機能設定例を修正 • 3.12.1 static-entry 設定による方法に注意事項を追加、及び修正

No.	年　月　日	内　　容
		• 3.13 TTL フィルターを修正 • 3.16 認証開始時の EAP-Request/EAP-Identity の抑制を修正 • 3.17 認証失敗時のステータス保持時間の変更を修正 • 3.18 Web/MAC 認証(AND)の MAC 認証属性を修正 • 4.1 Web 認証を修正 • 4.2 Web 認証(MLAG 併用)を追加 • 4.3 MAC 認証を修正 • 4.4 MAC 認証(MLAG 併用)を追加 • 4.5 Web 認証、MAC 認証の混在環境を修正 • 4.6 Web/MAC 認証(AND)を修正 • 4.7 ゲートウェイ認証(サーバーファーム手前に適用)を修正 • 4.8 ゲートウェイ認証(サーバーファーム手前に適用、MLAG 併用)を追加 • 4.9 ゲートウェイ認証(中央拠点アクセス手前に適用)を修正 • 4.10 802.1X を修正 • 4.11 802.1X(MLAG 併用)を追加 • 4.12 802.1X/MAC 認証(AND)を修正 • 4.13 Web/802.1X 認証(AND)を追加 • 4.14 DHCP Snooping を修正 • 4.15 DHCP Snooping、MAC 認証の混在環境を修正 • 4.16 DHCP Snooping、Web 認証(固定 VLAN)の混在環境を修正 • 4.17 DHCP Snooping、Web 認証(動的 VLAN)の混在環境を修正 • 4.18.1 クラス ID 端末環境を修正 • 4.18.2 クラス ID 端末/クラス ID 未付与端末の混在環境を修正 • 5.2.4 拡張設定(VLAN ID/クラス ID の設定)を修正 • 6.4 MAC アドレスの自動収集を修正 • 7.2.3 EAPOL Start 受信による認証の抑止を用いた回避方法を修正 • 9.1 SSL 設定概要を修正 • 9.2.1 秘密鍵と証明書要求の生成を修正 • 9.2.2 証明書要求のアップロードを修正 • 9.2.4 証明書のダウンロードを修正 • 9.3.3 証明書と秘密鍵のダウンロードを修正 • 10 各バージョンでの機能追加、変更点を追加
G	2014 年 8 月 29 日	• 全章を対象に誤字・脱字・体裁を修正 • 適用機種一覧表を修正 • 使用条件と免責事項を修正 • 表 2-1 動作可否確認済みサプリカントを修正 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 2-3 AccessDefender で使用するパケットフィルター2 のグループ数を修正 • 表 2-4 パケットフィルター2 のグループを使用するコマンドを修正 • 表 2-5 DHCP Snooping で使用するパケットフィルター2 のグループ数を修正 • 表 2-6 動作可否確認済みブラウザー(認証ページリダイレクト使用時)を修正

No.	年　月　日	内　容
		• 表 6-2 AccessDefender 併用時のパケットフィルター2 動作を修正 • 表 10-1 各バージョンでの機能追加、変更点を修正 • 図 3-16 スヌーピングプロキシ機能の認証ページ強制表示フローを追加 • 図 4-7 ゲートウェイ認証構成例(サーバーファーム手前適用)を修正 • 2.11.2 DHCP Snooping の認証端末数を修正、及び注意事項を削除 • 2.12.3 動作確認済ブラウザーに注意事項を追加 • 3.12 スヌーピングプロキシ機能による認証ページの強制表示を追加 • 3.14 TTL フィルターを修正 • 3.17 認証開始時の EAP-Request/EAP-Identity の抑制を修正 • 3.18 認証失敗時のステータス保持時間の変更を修正 • 6.1.1 APRESIA 内部ページのカスタマイズを修正 • 6.1.2 外部 Web サーバー上の任意のページへの埋め込みを修正 • 6.1.3 認証方法選択機能の認証ページカスタマイズを修正 • 7.2.3 EAPOL-Start 受信による認証の抑止を用いた回避方法を修正
H	2014 年 10 月 3 日	• 全章を対象に誤字・脱字・体裁を修正 • 適用機種一覧表を修正 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 2-4 パケットフィルター2 のグループを使用するコマンドを修正
I	2017 年 6 月 16 日	• 全章を対象に誤字・脱字・体裁を修正 • 3.11.3.2 HTTPS を用いる際の注意点を修正 • 5.1.3 拡張設定(VLAN ID/クラス ID の設定)を修正
J	2019 年 3 月 29 日	• 全章を対象に誤字・脱字・体裁を修正 • 適用機種一覧表を修正 • 表 2-2 AccessDefender 機能の仕様を修正 • 表 2-4 パケットフィルター2 のグループを使用するコマンドを修正 • 表 2-7 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 3-3 ローカルデータベースフォーマットを修正 • 表 3-4 ダウンロード時のコンソールメッセージ表示例を修正 • 表 3-5 登録時のコンソールメッセージ表示例を修正 • 表 3-6 削除時のコンソールメッセージ表示例を修正 • 表 3-8 port オプションの有無による動作の違いを追加 • 表 3-11 無通信監視対象フレーム(パケット)を追加 • 表 3-12 無通信時間のリセットタイミングを追加 • 表 3-13 各設定条件における 802.1X の動作を追加 • 表 5-4 AccessDefender 機能(Web 認証、MAC 認証)で使用する RADIUS 属性を修正 • 表 5-5 802.1X 機能で使用する RADIUS 属性を修正 • 表 8-1 認証ログ一覧を修正 • 表 8-2 ログアウトで表示されるタイプ一覧を修正 • 表 8-3 AccessDefender 設定時のコンフリクトメッセージ一覧を修正 • 表 10-1 各バージョンでの機能追加、変更点を修正 • 図 2-13 DENY モード時の動作フローを修正 • 図 3-19 プロキシ経由での HTTPS アクセスを修正

No.	年　月　日	内　　容
		• 図 3-22 TTL フィルターを修正 • 図 3-30 ローミング機能(通信ポート)の切り替え例を追加 • 図 3-31 HTTP プロトコルシーケンスと HTTP/HTTPS セッションタイムアウト動作を追加 • 図 3-32 認証端末のユーザーID(MAC アドレス)による MAC 認証を追加 • 図 3-33 トランクポートでのタグ付き EAP フレームによる 802.1X を追加 • 図 4-1 Web 認証構成例を修正 • 図 4-2 Web 認証構成例(MLAG 併用)を修正 • 図 4-5 Web 認証と MAC 認証の併用構成例を修正 • 図 4-6 Web/MAC 認証(AND)構成例を修正 • 図 4-7 ゲートウェイ認証構成例(サーバーファーム手前適用)を修正 • 図 4-8 ゲートウェイ認証構成例(サーバーファーム手前適用、MLAG 併用)を修正 • 図 4-9 ゲートウェイ認証構成例(中央拠点アクセス構成)を修正 • 図 4-13 Web/802.1X 認証(AND)構成例を修正 • 図 4-16 DHCP Snooping と Web 認証(固定 VLAN)の併用構成例を修正 • 図 4-17 DHCP Snooping と Web 認証(動的 VLAN)の併用構成例を修正 • 図 4-18 ユーザーポリシーコントロール構成例 1 を修正 • 図 4-19 ユーザーポリシーコントロール構成例 2 を修正 • 図 6-2 NAS-IPv6-Address 設定時のアクセス制限の追加 • 図 7-22 MAC 認証と VRRP 併用構成例の追加 • 2.2 ゲートウェイ認証の注意事項を修正 • 2.9.2 DHCP Snooping の動作フローの注意事項を修正 • 2.13 ログアウト処理についての注意事項を修正 • 3.3.2 ローカルデータベースの登録(ダウンロード)を修正 • 3.6 認証順序変更(Web 認証、MAC 認証のみ)を修正 • 3.7 移行条件変更機能(Web 認証、MAC 認証のみ)を修正 • 3.8 認証方法選択機能(Web 認証のみ)を修正 • 3.10 認証拒否機能の注意事項を修正 • 3.11 認証ページのリダイレクト機能を修正 • 3.11.1.2 認証ページリダイレクト機能設定例を修正 • 3.11.2.2 認証ページリダイレクト機能設定例を修正 • 3.11.3.2 プロキシ利用環境における HTTPS 通信の注意を修正 • 3.17 認証開始時の EAP-Request/EAP-Identity の抑制を修正 • 3.20 ローミング機能を追加 • 3.21 SSL プロトコルの脆弱性対応を追加 • 3.22 HTTP/HTTPS セッションタイムアウト時間の設定を追加 • 3.23 認証端末のユーザーID(MAC アドレス)による MAC 認証を追加 • 3.24 DHCP Snooping のエージングログアウト機能を追加 • 3.25 MAC 認証有効ポートにおける認証バイパス対象フレームの認証回避を追加 • 3.26 トランクポートでのタグ付き EAP フレームによる 802.1X を追加 • 4.1 Web 認証を修正 • 4.2 Web 認証(MLAG 併用)を修正

No.	年　月　日	内　容
		• 4.4 MAC 認証(MLAG 併用)を修正 • 4.5 Web 認証、MAC 認証の混在環境を修正 • 4.6 Web/MAC 認証(AND)を修正 • 4.7 ゲートウェイ認証(サーバーファーム手前に適用)を修正 • 4.8 ゲートウェイ認証(サーバーファーム手前に適用、MLAG 併用)を修正 • 4.9 ゲートウェイ認証(中央拠点アクセス手前に適用)を修正 • 4.11 802.1X(MLAG 併用)の注意事項を修正 • 4.13 Web/802.1X 認証(AND)を修正 • 4.16 DHCP Snooping、Web 認証(固定 VLAN)の混在環境を修正 • 4.17 DHCP Snooping、Web 認証(動的 VLAN)の混在環境を修正 • 4.18.1 クラス ID 端末環境を修正 • 4.18.2 クラス ID 端末/クラス ID 未付与端末の混在環境を修正 • 6.1.3 認証方法選択機能の認証ページカスタマイズを修正 • 6.3.2 NAS-IPv6-Address を追加 • 6.5 端末認証後のパケットフィルター2(アクション none)を修正 • 7.3 VRRP 併用時の注意点を追加 • 9.2.1 秘密鍵と証明書要求の生成を修正 • 9.6.2 証明書要求を装置で発行しない場合を修正
K	2019 年 7 月 12 日	• 全章を対象に誤字・脱字・体裁を修正 • 適用機種一覧表を修正 • 表 10-1 各バージョンでの機能追加、変更点を修正 • 3.11.2.1 認証フローの注意事項を修正
L	2019 年 9 月 30 日	• 全章を対象に誤字・脱字・体裁を修正 • 3.11.3.2 プロキシ利用環境における HTTPS 通信の注意を削除

はじめに

本書は、スイッチングハブ APRESIA シリーズのファームウェア AEOS Ver. 8 の機能概要、及び構成・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、及び操作方法については、ハードウェアマニュアルを参照してください。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ください。

適用機種一覧表

シリーズ名称		製品名称	バージョン
Apresia13000 シリーズ		Apresia13000-X24-PSR	Ver. 8.36.01
Apresia13100 シリーズ		Apresia13100-48X-PSR	
Apresia 13200 シリーズ	Apresia 13200-28GT シリーズ	Apresia13200-28GT	Ver. 8.37.01
		Apresia13200-28GT-PoE	
	Apresia 13200-48X シリーズ	Apresia13200-48X	
		Apresia13200-48X-PSR	
	Apresia 13200-52GT シリーズ	Apresia13200-52GT-PSR	
		Apresia13200-52GT	
Apresia 15000 シリーズ	Apresia 1500-32XL シリーズ	Apresia15000-32XL-PSR	
		Apresia15000-32XL-PSR-1GLIM	
	Apresia 1500-64XL シリーズ	Apresia15000-64XL-PSR	
		Apresia15000-64XL-PSR-1GLIM	

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。

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すべてのソフトウェア(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。

(a) 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。

(b) 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

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、機能ごと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、弊社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。

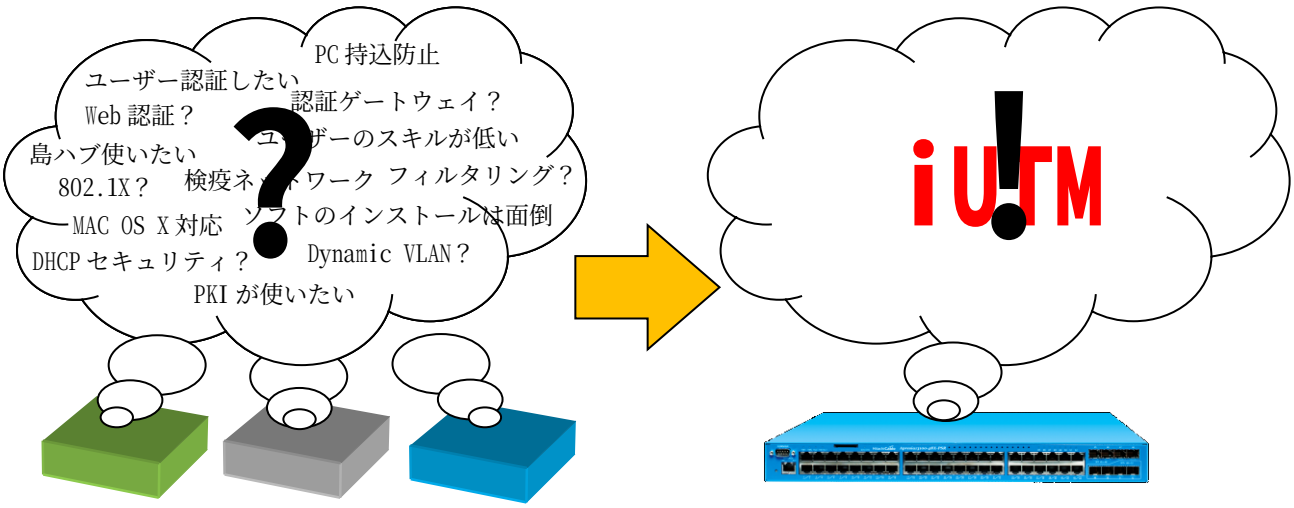


図 1-1 AccessDefender による iUTM 構想の実現

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。これにより、不正なユーザー、または端末が 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 7．制限事項、及び注意事項を参照してください。

1.2 AccessDefender がサポートする認証モード

AccessDefender は、表 1-1 に示す 4 つの認証モードと DHCP Snooping 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モード

項目	L2 制御 (MAC アドレスベース)			L3 制御 (IP アドレスベース)
	802.1X	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	802.1X 対応 サプリカント	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	サプリカント 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)	○	○	○
ルーター/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。

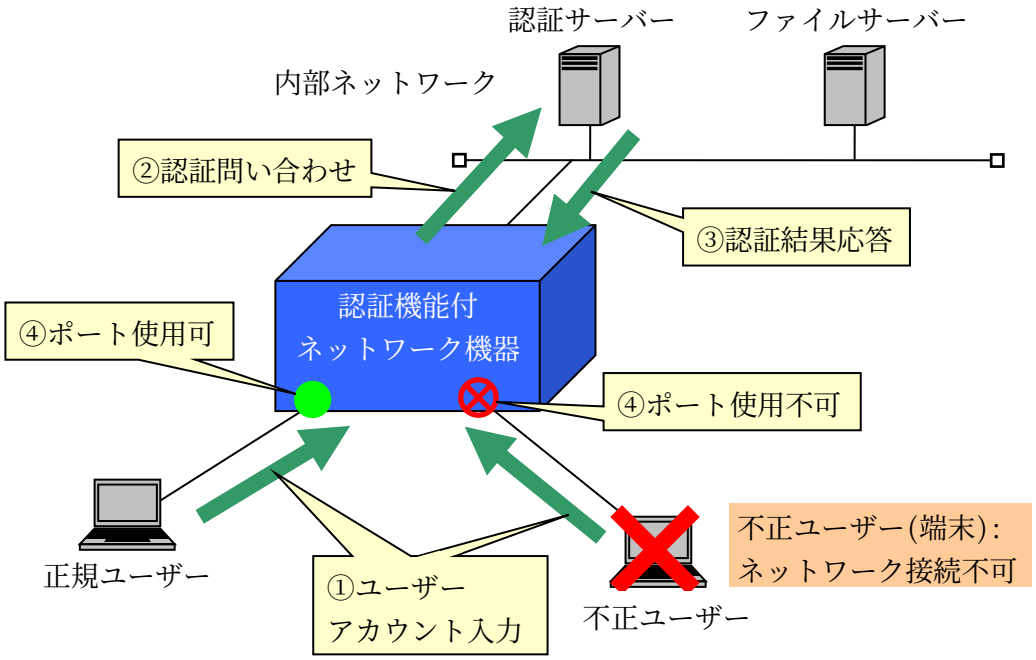


図 1-2 ユーザー認証による不正ユーザーのブロック

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い合わせします。
③ 正規ユーザー該非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。

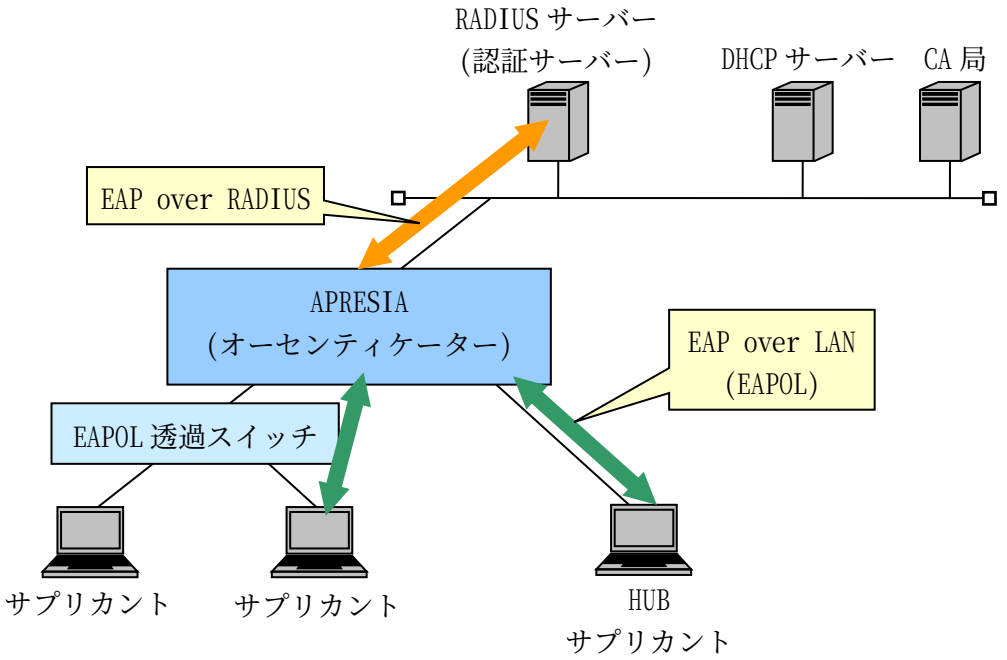
1.4 IEEE 802.1X

IEEE 802.1X(以下 802.1X とします)とは、IEEE 802.1(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(サプリカント)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、オーセンティケーターを介してサプリカントと 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プリカントと認証サーバー間の認証情報の橋渡しをし、サプ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。サプ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。



- サプリカント：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)
- EAPOL 透過スイッチ：EAP メッセージを中継するスイッチ
- CA 局：電子的な身分証明書を発行し、管理する機関

図 1-3 802.1X 動作システム概要

基本的に 802.1X 機能では、スイッチの 1 ポートに 1 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 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(EAPOL 透過)スイッチを接続する必要があります。

APRESIA の 802.1X 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で、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 アドレスごとに 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	• 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(ユーザー認証と同レベル)
PEAP	要	不要	サーバーの電子証明書と ID/パスワード	• ユーザー識別にユーザーID/パスワード、または電子証明書、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	• 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、別途サプリカントが必要
EAP-TLS	要	要	電子証明書	• 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

サプリカントとオーセンティケーター間では、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。

オーセンティケーターと 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。オーセンティケーターが EAP パケットを中継し、サプリカントと 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。

MAC フレーム

6(octet)	6	2	46-1500	4
宛先 MAC アドレス	送信元 MAC アドレス	タイプ	データ	FCS

MAC フレームのデータ部分

1(octet)	1	2	可変長
プロトコル バージョン	パケットタイプ 0：EAP パケット 1：EAPOL-Start 2：EAPOL-Logoff 3：EAPOL-Key(無線での鍵情報)	パケットボディ長	パケットボディ

EAP パケット

1(octet)	1	2	可変長
Code 1：Request 2：Response 3：Success 4：Failure	Identifier	Length	Data ... (Type、Type-Date) <1：Request> or <2：Response>の場合 --> ユーザーID や認証方式などの情報が入る <3：Success> or <4：Failure>の場合 --> Data 部はなし(Length=4)

図 1-4 EAPOL のフレームフォーマット

1.5 DHCP Snooping 概要

DHCP Snooping 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通信を許可する機能です。

本機能により以下が実現可能となり、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

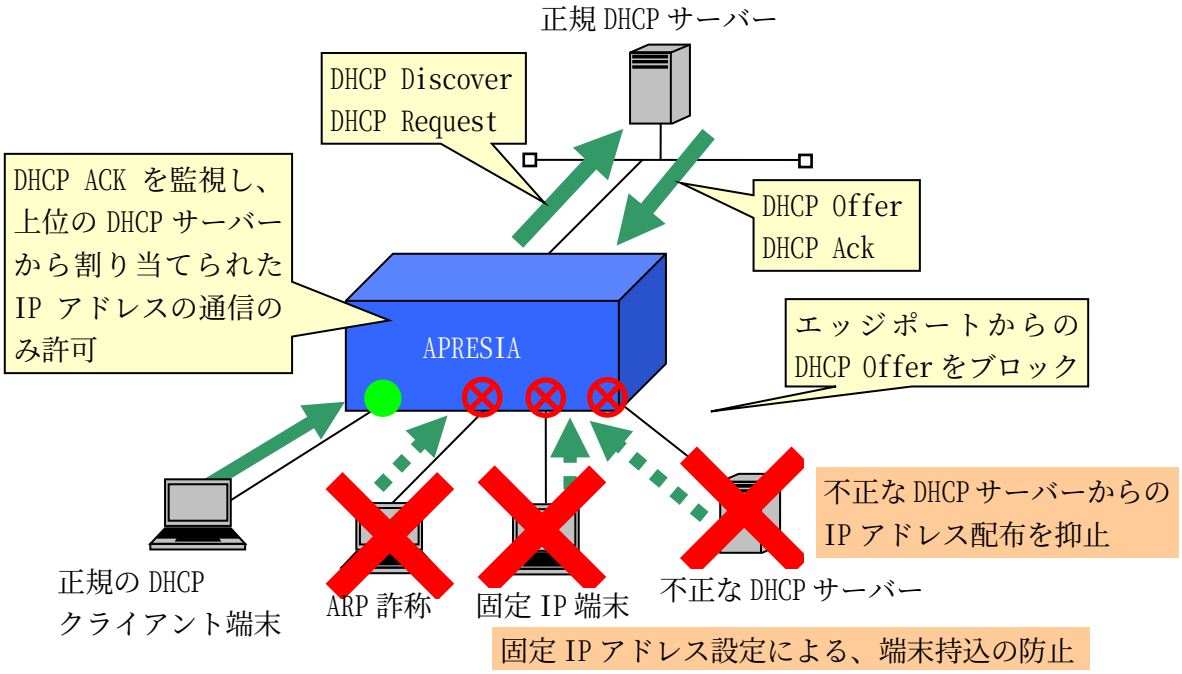


図 1-5 DHCP Snooping 構成例

1.6 ユーザーポリシーコントロール概要

ユーザーポリシーコントロールは、認証端末に識別子(クラス ID)を付与して認証端末ごとにフレーム制御ポリシーを適用する機能です。ユーザーポリシーコントロールを使用することにより、アクセス制御、優先制御、ミラーリングなどを認証端末ごとに制御することが可能です。認証端末ごとの制御はパケットフィルター2 機能にて実現されます。

識別子(クラス ID)は RADIUS サーバー、またはローカルデータベースに保持します。

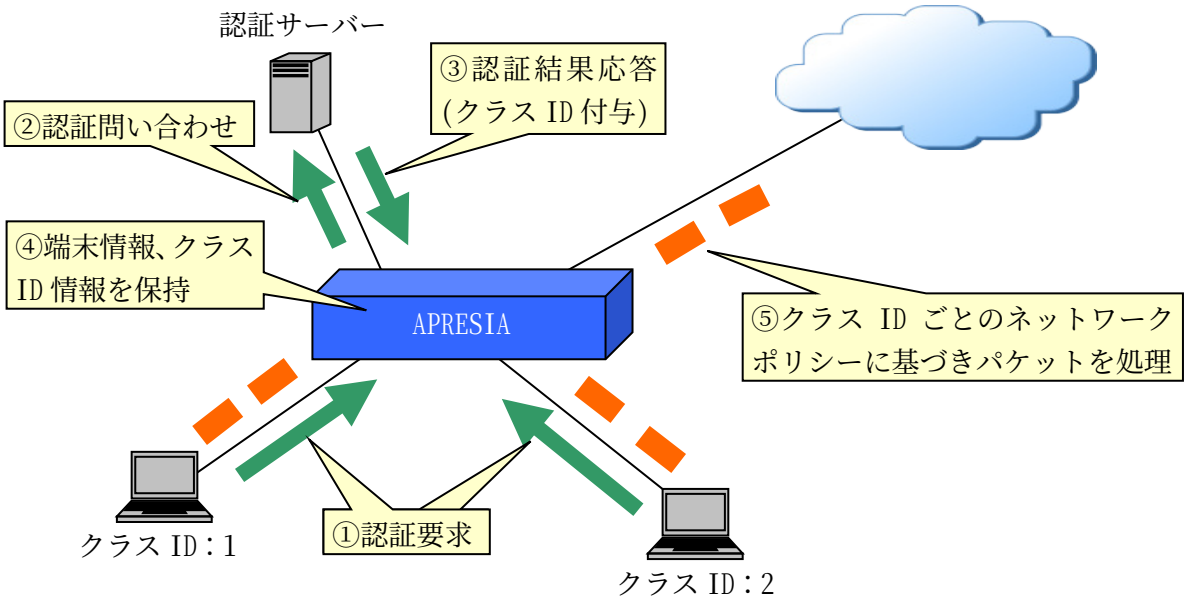


図 1-6 ユーザーポリシーコントロール概要

① 端末が認証を要求します。
② 端末情報を基に認証サーバーに問い合わせます。
③ 端末が認証サーバーにより認証され、クラス ID 情報を含んだ結果が応答されます。
④ APRESIA が端末情報とクラス ID を保持します。
⑤ 端末からのパケットをクラス ID ごとのフレーム制御ポリシーに基づき処理します。

2 AccessDefender の仕組み

2.1 Web 認証(Web ブラウザー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)にユーザーごとに 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、認証端末ごとに VLAN を割り当てることも可能です。

パケットフィルター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。

HTTPS の Web 認証を行った際、証明書が不正な場合に証明書エラーのページが開きますが、ブラウザーの動作により表示されるまで少し時間がかかる事があります。

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ごとに 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。
未認証端末のパケット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 パケット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。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、5.1.3 拡張設定(VLAN ID/クラス ID の設定)を参照してください。

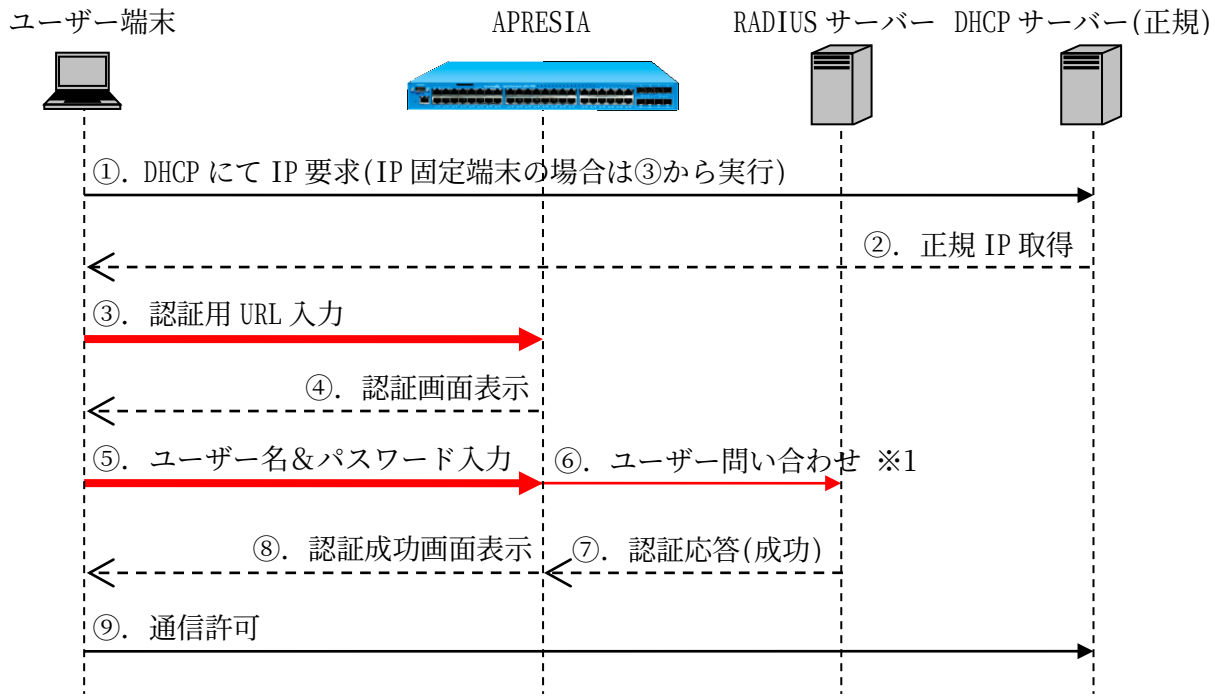


図 2-1 Web 認証フロー(VLAN 固定)

※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 ：認証端末が接続されているインターフェース番号
- NAS-Identifier ：認証要求端末が属している VLAN ID
- 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、その属性に従って認証成功後にユーザーごとに VLAN を動的に変更して割り当てることができます。認証ポートにあらかじめ設定する VLAN を暫定 VLAN、認証後に RADIUS サーバーから通知される VLAN ID 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。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 VLAN ID を通知します。
APRESIA は端末の情報とあわせて、RADIUS サーバーから通知された VLAN ID 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。

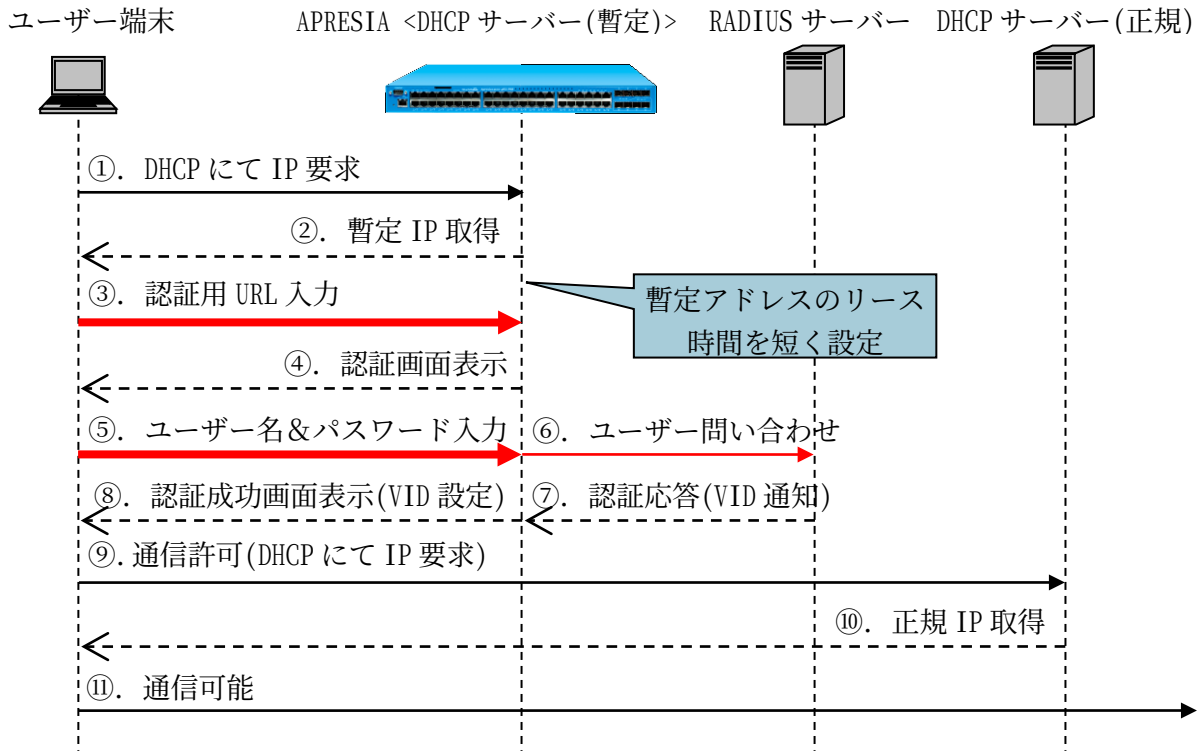


図 2-2 Web 認証フロー(VLAN 変更)

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ください。

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 認証などとの組合せが可能

■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、センター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

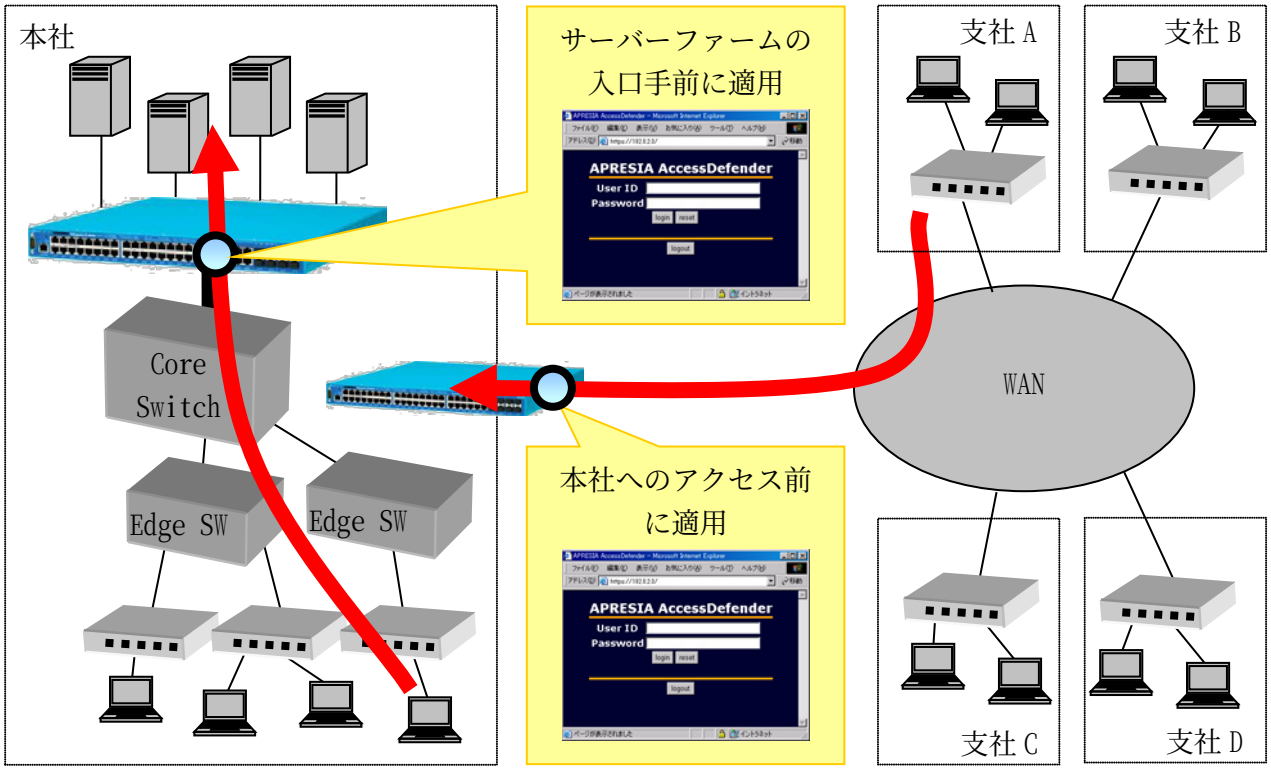


図 2-3 ゲートウェイ認証の適用イメージ

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。

ゲートウェイ認証とその他の認証(Web 認証、Web/MAC 認証(AND)、Web/802.1X 認証

(AND)、MAC 認証、802.1X、802.1X/MAC 認証(AND))、及び DHCP Snooping は同一ポートで併用できません。

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。

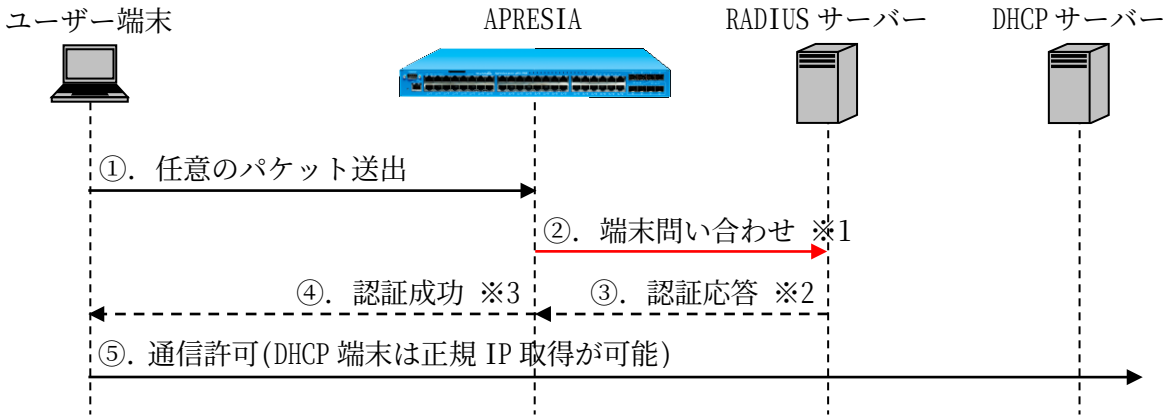


図 2-4 認証フロー(MAC ベース認証)

※1. Web 認証と同じ属性をサポートしています。

※2. RADIUS サーバーに属性情報が登録されている場合、該当する属性値が割り当てられます(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)。

※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。

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。

2.4 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、通常の Web による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(⑦-⑰)。

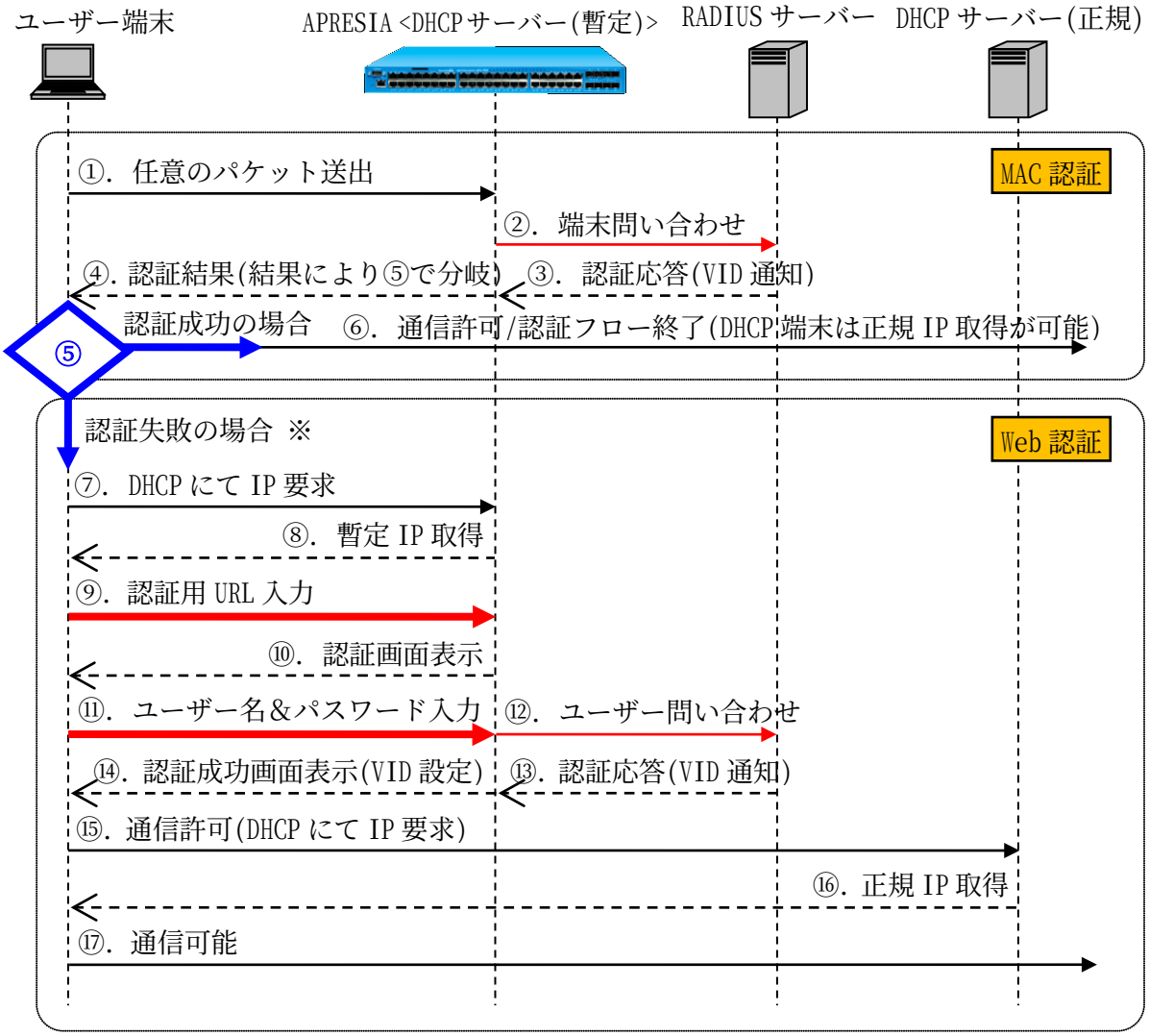


図 2-5 Web 認証と MAC 認証を併用する場合の認証フロー

※ 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(AND) (Web 認証時の MAC 認証先行)

Web/MAC 認証(AND)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)にユーザーごとに VLAN 情報を追加します。認証端末ごとに VLAN を割り当てることはできません。

Web/MAC 認証(AND)の認証順の変更は、3.19 Web/MAC 認証(AND)の MAC 認証属性を参照してください。

Web/MAC 認証(AND)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。
未認証端末のパケット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 パケット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い合わせ(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達します。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い合わせ(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達します。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。

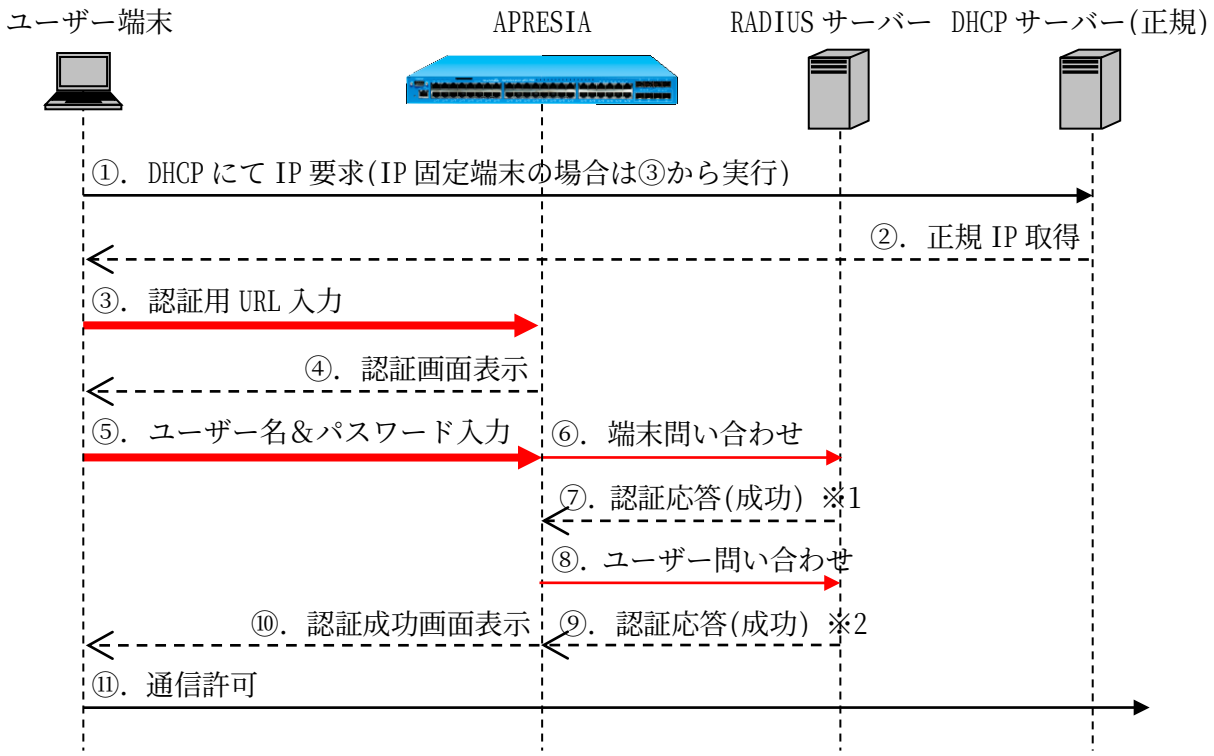


図 2-6 Web/MAC 認証(AND)フロー

※1. RADIUS サーバーへ MAC 認証の属性情報が登録されている場合でも、Web 認証に先立ち成功した MAC 認証の属性値は割り当てられません。

※2. RADIUS サーバーへ Web 認証の属性情報が登録されている場合、該当する属性値が割り当てられます(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)。

認証端末の MAC 認証と Web 認証の両モードにおいて認証が成功した場合のみ通信可能となります。

2.6 802.1X

2.6.1 802.1X の認証フロー

APRESIA で実装されている 802.1X 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-Request/EAP-Identity)をユニキャストで送信します。
※ 30 秒ごとの FDB チェック処理で新たな MAC アドレス検出時に EAP-Request/EAP-Identity が送信されます。
※ 認証処理をやり直すため、EAP Failure もあわ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従って端末の MAC アドレスごとに 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。

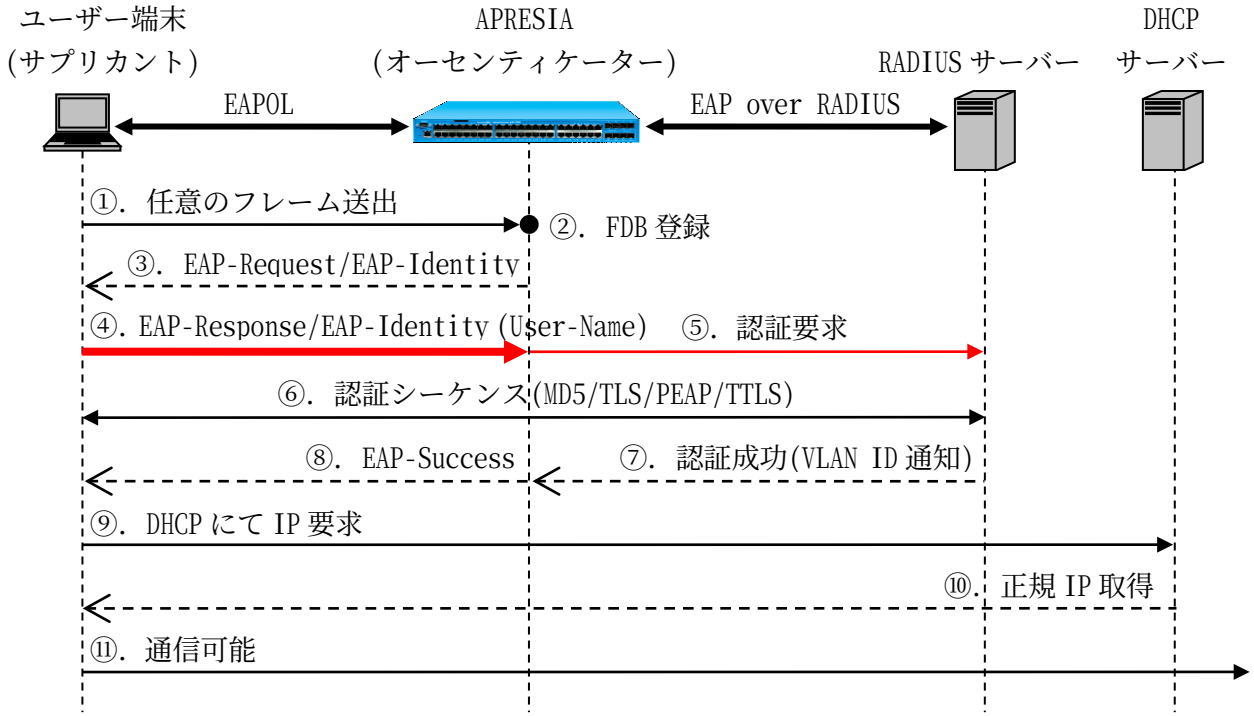


図 2-7 802.1X の認証フロー

認証時の負荷軽減のため、EAP-Request/EAP-Identity 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 で使用する EAP メッセージは、サプリカントとオーセンティケーター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。

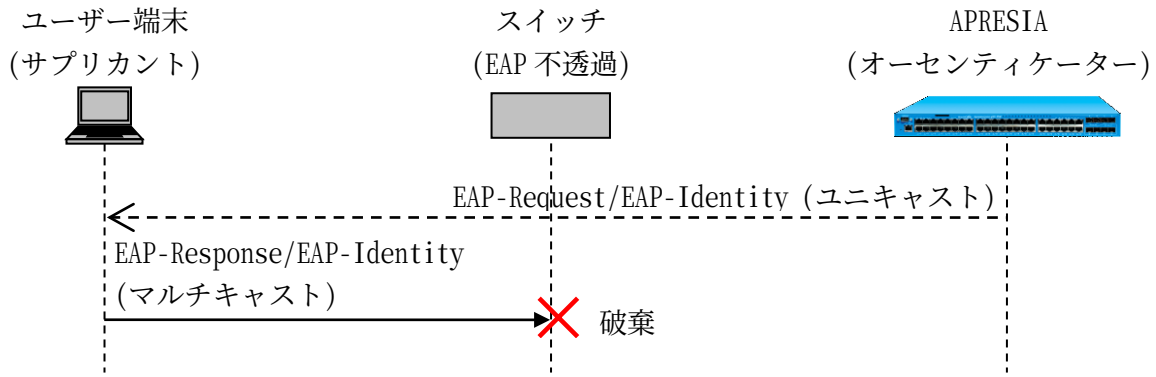


図 2-8 EAP 不透過による EAPOL フレーム破棄

APRESIA の Unicast-EAP 機能を用いることにより、サプ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プリカントと接続する場合においても、サプ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。

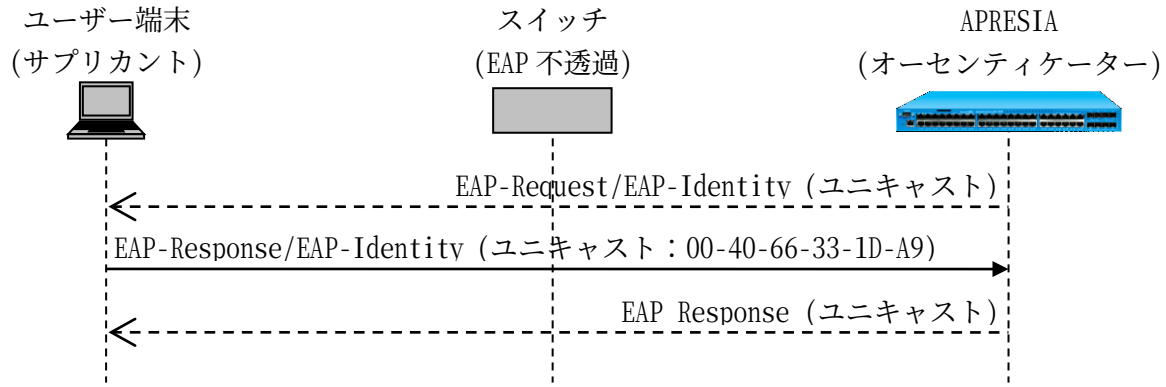


図 2-9 Unicast-EAP 機能有効時

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プリカントを使用する必要があります(Windows 標準サプ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 動作確認済サプリカント一覧

802.1X に関して、以下のサプリカントで動作可否を確認しています。これ以外のサプリカ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 動作可否確認済みサプリカント

サプリカント	OS	認証方式
Windows 標準サプリカント	Windows XP SP2	EAP-MD5/PEAP/TLS
	Windows XP SP3	EAP-MD5/PEAP/TLS
	Windows Vista SP1/SP2	PEAP/TLS
	Windows 7	PEAP/TLS
iNetSec Inspection Center 802.1X サプリカント(V3.0L20)	Windows XP SP2/SP3	EAP-MD5/PEAP/TLS ※ユニキャスト EAP 対応確認済み
Odyssey Client Manager (4.32.0.2347)	Windows XP SP2/SP3	EAP-MD5/PEAP/TLS/EAP-TTLS

2.7 802.1X/MAC 認証(AND) (802.1X の認証時の MAC 認証先行)

802.1X/MAC 認証(AND)は、802.1X に先立ち、端末の 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 を実行します。どちらの認証にも成功した場合に通信が可能となります。

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)にユーザーごとに VLAN 情報を追加します。認証端末ごとに VLAN を割り当てることはできません。

802.1X/MAC 認証(AND)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-Request/EAP-Identity)をユニキャストで送信します。

※ 30 秒ごとの FDB チェック処理で新たな MAC アドレス検出時に EAP-Request/EAP-Identity が送信されます。

※ 認証処理をやり直すため、EAP Failure もあわ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 RADIUS サーバーに対して端末問い合わせ(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達します。認証に成功した場合のみ 802.1X 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従って端末の MAC アドレスごとに 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. 端末の通信が可能となります。

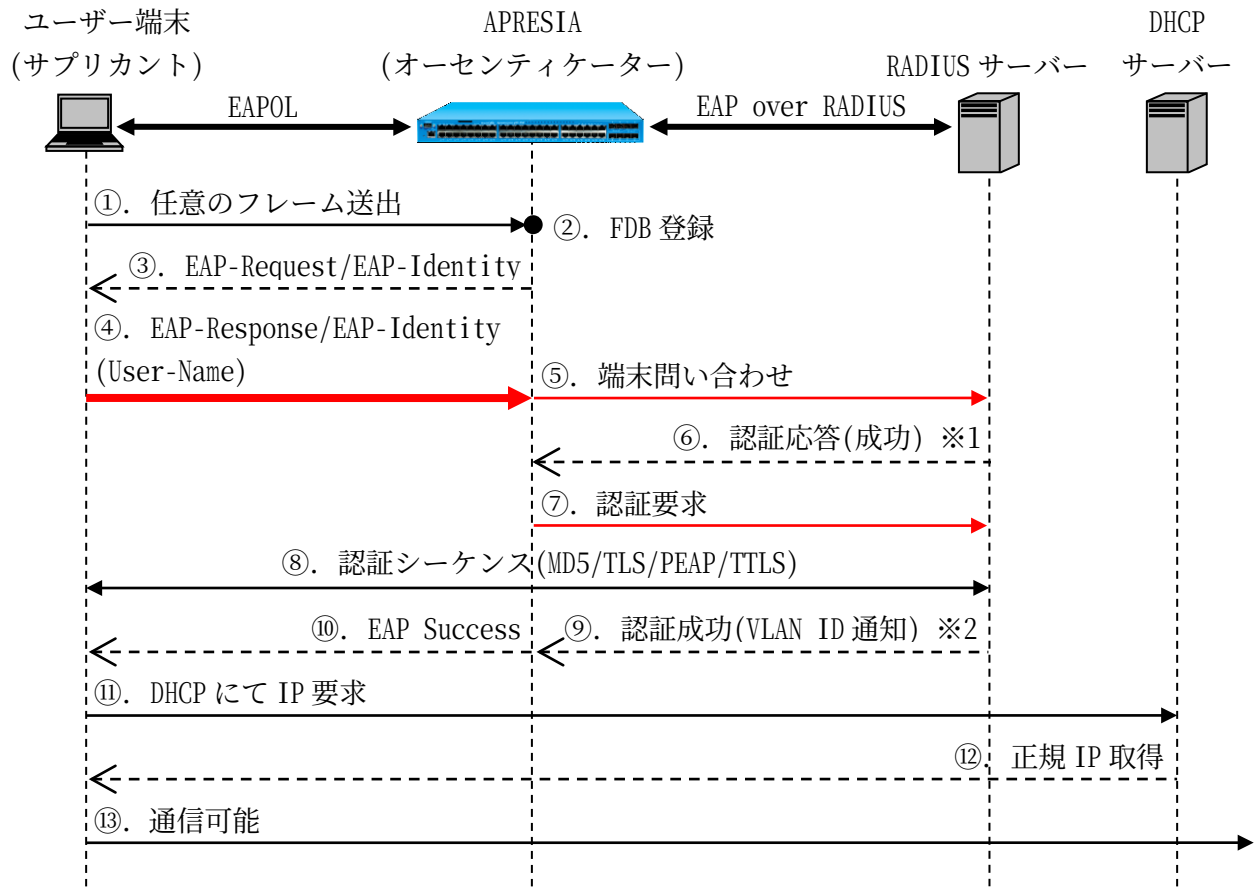


図 2-10 802.1X/MAC(AND)認証フロー

※1. 802.1X に先立ち成功した MAC 認証の属性値は割り当てられません。
※2. RADIUS サーバーへ 802.1X の属性情報が登録されている場合、該当する属性値が割り当てられます(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)。

認証時の負荷軽減のため、EAP-Request/EAP-Identity 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。

認証端末の MAC 認証と 802.1X の両モードにおいて認証が成功した場合のみ通信可能となります。

2.8 Web/802.1X 認証(AND) (Web 認証と 802.1X の併用認証)

Web/802.1X 認証(AND)は、Web 認証と 802.1X の両方で認証を行う機能です。両方の認証に成功した場合のみ通信ができます。802.1X の詳細は、2.6 802.1X を参照してください。

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)にユーザーごと/端末ごとに VLAN 情報を追加します。ユーザー属性情報は両方の認証にも成功している場合のみ、後に成功した認証の属性値が割り当てられます。片方の認証にしか成功していない状態では、どちらの属性値も割り当てられません。

802.1X が先に行われた場合の Web/802.1X 認証(AND)の認証フローを図 2-11 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-Request/EAP-Identity)をユニキャストで送信します。
※ 30 秒ごとの FDB チェック処理で新たな MAC アドレス検出時に EAP-Request/EAP-Identity が送信されます。
※ 認証処理をやり直すため、EAP Failure もあわせて送信される場合があります。

④-⑨. 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。RADIUS サーバーから認証成功メッセージが通達された場合でも、この時点では片方の認証にしか成功していない状態のため、遮断されていた通常トラフィックは許可されません。
RADIUS サーバーの登録属性値に従った端末の MAC アドレスごとの VLAN 変更もされません。

⑩-⑪. 以降、通常の Web によるユーザー認証と同様のフローを実行します。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。

⑫-⑮. 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い合わせを行います。

⑯-⑰. 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。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。この時点で両方の認証に成功している状態となるため、遮断されていた通常トラフィックが許可されます。
また、RADIUS サーバーの登録属性値に従ってユーザーごとに VLAN が変更されます。

⑱-⑲. 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。

⑳. 端末の通信が可能となります。

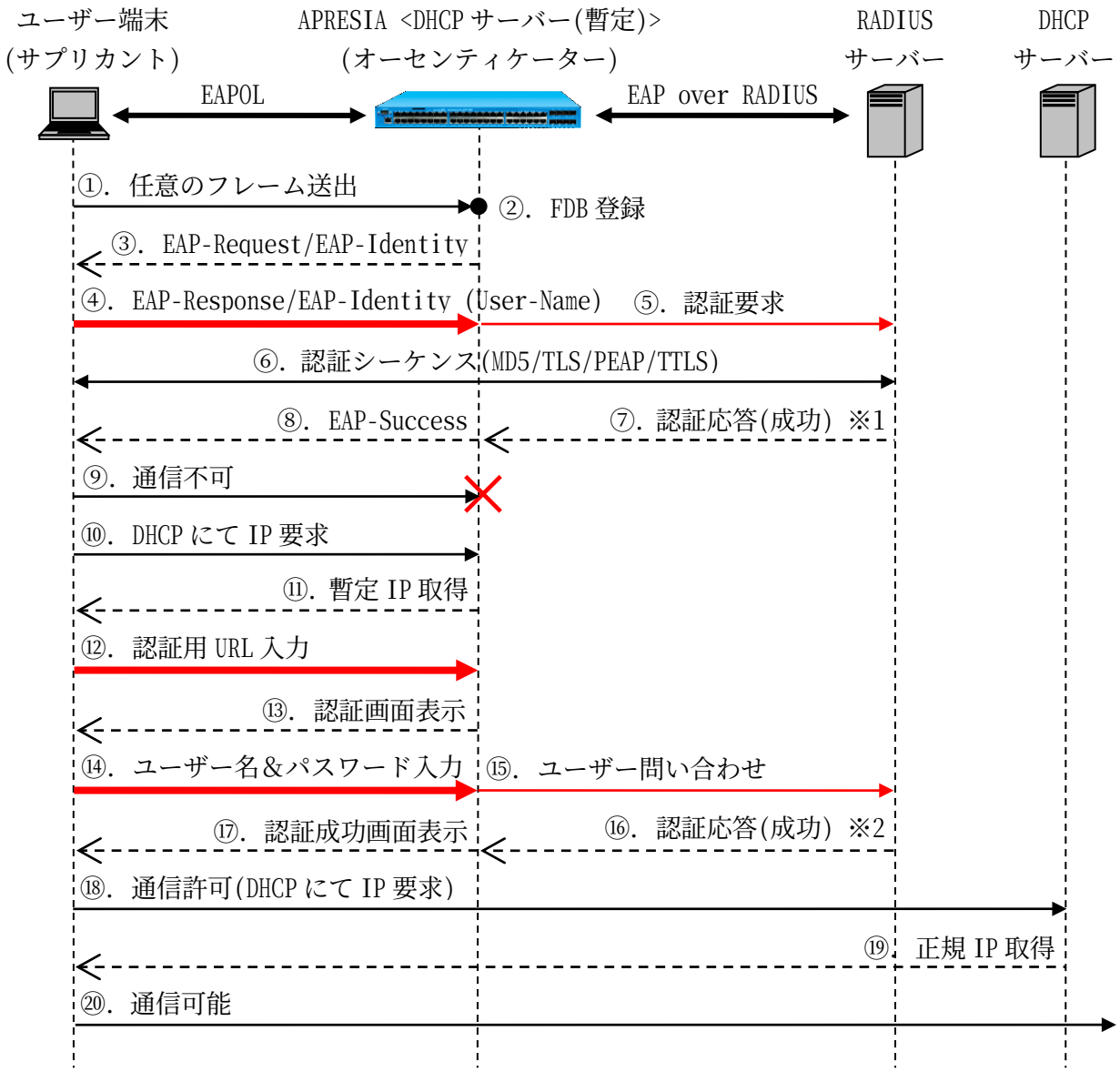


図 2-11 Web/802.1X 認証(AND)の認証フロー(802.1X 先行時)

※1. 片方の認証のみに成功した状態では、RADIUS サーバーへ認証の属性情報が登録されている場合でも、先に成功した認証の属性値は割り当てられません。

※2. 両方の認証に成功した状態では、RADIUS サーバーへ認証の属性情報が登録されている場合、後に成功した認証の属性値が割り当てられます(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)。

Web 認証が先に行われた場合は、801.1X 認証のフロー(①-⑧)と Web 認証のフロー(⑩-⑰)を入れ替えた認証フローとなります。Web 認証成功後、802.1X も成功した時点で遮断されていた通常トラフィックが許可され、802.1X の登録属性値に従って MAC アドレスごとに VLAN が変更されます。

また、Web 認証の代わりに Web/MAC 認証(AND)を行うことも可能です。この場合、Web/MAC 認証(AND)における MAC 認証、Web 認証と 802.1X のすべての認証に成功した場合のみ通信ができます。Web/802.1X 認証(AND)と同様に、RADIUS サーバーに登録されている属性情報は、すべての認証に成功している場合にのみ、最後に成功した認証の属性値が割り当てられます。

認証フローは図 2-11 の内、Web 認証のフロー(⑫-⑰)を、図 2-6 の Web/MAC 認証(AND)フロー(③-⑩)

に置き換えたものとして参照してください。

認証端末の Web 認証(または Web/MAC 認証(AND))と 802.1X の両モードにおいて認証が成功した場合のみ通信可能となります。

Web/802.1X 認証(AND)ポートで 802.1X、または Web のみ認証済みの端末は無通信端末の扱いとなり、エージングログアウトの設定が有効の場合、設定時間が満了した時点でログアウトされます。

Web/802.1X 認証(AND)に設定されたポートが Web 認証ポート、802.1X の認証ポートに設定済みの場合、ログイン済みの Web 認証端末、802.1X の認証端末はログアウトされます。

2.9 DHCP Snooping

2.9.1 DHCP Snooping の動作モード

DHCP Snooping は PERMIT モード、DENY モードの 2 つの動作モードがあります。デフォルト設定は PERMIT モードです。

以下に PERMIT モード、DENY モード、それぞれの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 Snooping したアドレスが送信元となる通信　　：許可
- DHCP Snooping 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 Snooping したアドレスが送信元となる通信　　：許可
- DHCP Snooping 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、タイマーによる自動切り替え(PERMIT モード --> DENY モードのみ)、及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。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。

DENY モード運用中にスイッチの再起動などを行った場合、登録済みの送信元アドレス情報が削除されます。そのため、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します。この場合、PERMIT モードからの自動切り替えタイマー設定値を 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ることで、通信断を回避することができます。

図 2-12 に PERMIT モードで起動した場合の動作モード概要を示します。

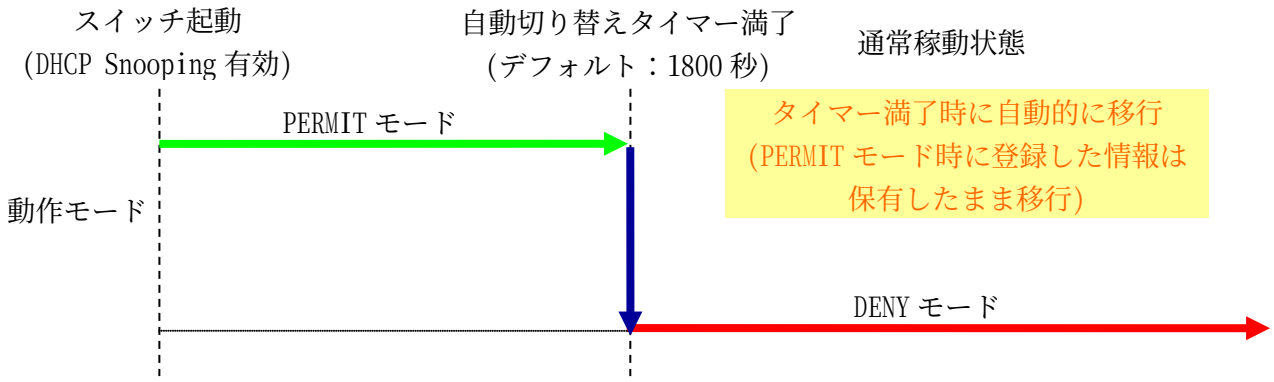


図 2-12 DHCP Snooping 動作モード概要

2.9.2 DHCP Snooping の動作フロー

図 2-13、図 2-14 に各モードの動作フローを示します。

PERMIT モード、DENY モードのいずれにおいても、正規 DHCP サーバーから払い出される DHCP ACK パ

ケットに従い、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ーをユーザー端末が接続されたポートに登録します。ユーザー端末から DHCP Release パケットを受信した場合は、登録済みの送信元アドレス情報を削除します。

DHCP Release パケットにより IP アドレスが開放されなかった場合、DHCP サーバーより払い出されたリース期間経過後、登録済みのフィルターを自動的に削除します。

認証機能と DHCP Snooping の併用構成では、DHCP Snooping にのみ登録されている端末は ARP のみ通信可能となります。また、その状態から他の認証機能で認証が成功した場合は、IP アドレスによる通信が可能となります。

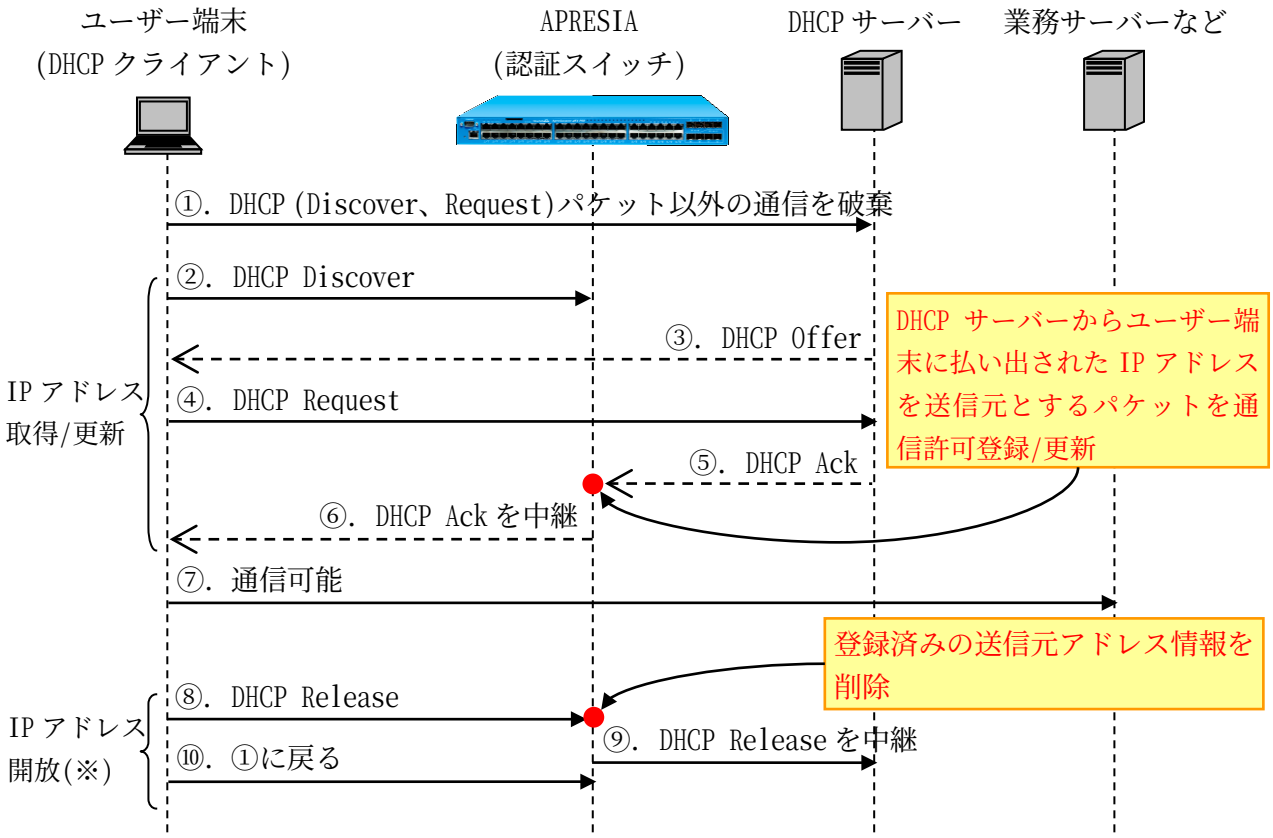


図 2-13 DENY モード時の動作フロー

※ DHCP Release による IP アドレス開放が行われなかった場合、DHCP サーバーより払い出されたリース期間と同じ期間経過後、登録済みの送信元アドレス情報を自動的に削除します。

DHCP Snooping は、スヌーピングされない端末の IPv4、ARP 通信のみを遮断する機能です。

DHCP Snooping で登録された端末は、リンクダウンではログアウトしません。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 Snooping を有効にしないでください。

認証機能と DHCP Snooping の併用構成で、DHCP Snooping にのみ登録されている端末は、認証不可状態(失敗状態)では通信ができません。また、その状態で認証機能の設定を削除しても、通信はできません。通信を行うためには、DHCP Snooping を有効にする必要があるので再ログインを行って下さい。

DHCP Snooping を使用する場合、DHCP パケットの中継動作は以下のような動作となります。

- **DHCP Snooping 有効ポートで受信した DHCP サーバー宛の DHCP パケットは、ソフトウェア中継されます。**
- **DHCP Snooping 無効ポートで受信した DHCP サーバー宛の DHCP パケットは、ハードウェア中継されます。**
- **DHCP クライアント宛の DHCP パケットは、DHCP Snooping 有効、無効ポートに係わらずソフトウェア中継されます。**

DHCP Snooping とパケットフィルター2 機能を併用し、AccessDefender よりも優先度の高いフィルター対象に DHCP パケットが含まれる場合、DHCP パケットが正しくソフトウェア中継されるように action コマンドの"permit"、"authentication-bypass"を使用しないでください。

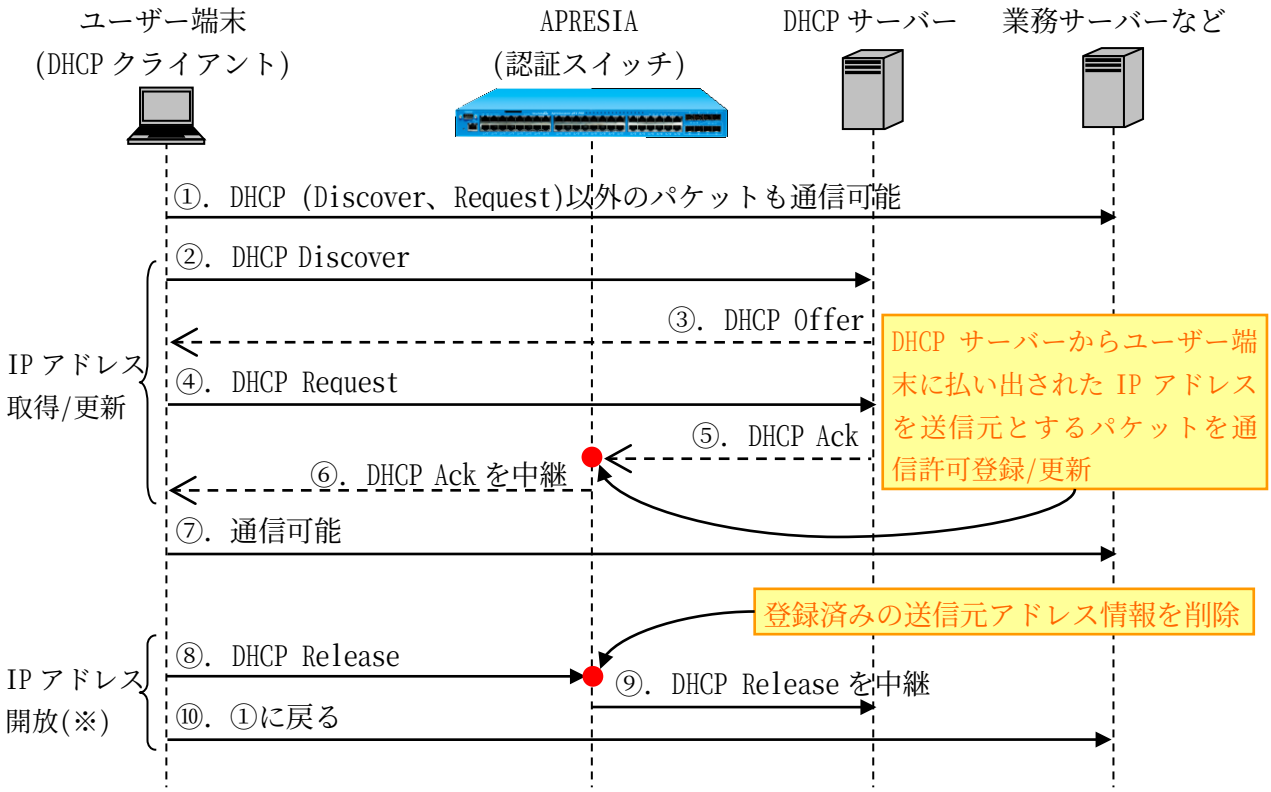


図 2-14 PERMIT モード時の動作フロー

※ DHCP Release による IP アドレス開放が行われなかった場合、DHCP サーバーより払い出されたリース期間と同じ期間経過後、登録済みの送信元アドレス情報を自動的に削除します。

PERMIT モード時は、固定 IP アドレス端末からの通信も可能です。自動切り替えタイマーを設定し、DENY モードへ移行するように設定してください。

PERMIT モードからの切り替えタイマー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。タイマーを 0 に指定した場合、自動切り替えは行われません。

2.10 ユーザーポリシーコントロールの動作フロー

認証端末に対してクラス ID が付与されている場合、クラス ID をパケットフィルター2 のフィルター条件(コンディション)に指定することができ、認証端末ごとのパケットフィルター2 適用が可能となります。クラス ID は RADIUS サーバー、またはローカルデータベースに設定することにより端末へ付与されます。使用できる認証モードは Web 認証、MAC 認証、802.1X です。クラス ID 未付与の認証端末には、aaa default class コマンドで設定したデフォルトクラス ID が適用されます(デフォルト設定はクラス ID：0)。

フィルター条件にクラス ID を指定したルールは、クラス ID が一致する端末のみに適用されます。クラス ID 未指定のルールは、すべての端末に適用されます。認証前の端末はクラス ID が適用されないため、本機能により認証後の端末にのみパケットフィルター2 を適用することが可能です。

ユーザーポリシーコントロールの動作フローを図 2-15 に示します。

①-②. ユーザー端末から受信した認証要求を RADIUS サーバーへ問い合わせます。

③. 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。この際、データベースにクラス ID が登録されていれば、クラス ID 情報もあわせて通達します。

④-⑤. ユーザー端末からの通信に関して、クラス ID の付与/未付与を確認します。

⑥. クラス ID が付与された端末であれば、クラス ID が設定されたパケットフィルター2 のルールを適用してパケットを処理します。

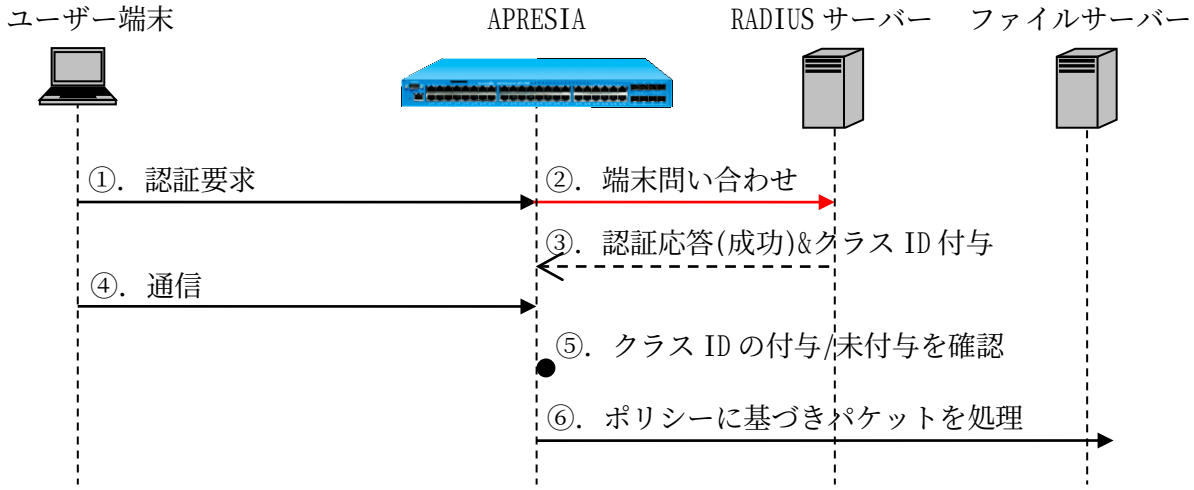


図 2-15 ユーザーポリシーコントロール動作フロー

2.11 認証機能と仕様

AccessDefender 機能の仕様を表 2-2 に示します。

表 2-2 AccessDefender 機能の仕様

項目		仕様	備考
認証モード	802.1X	○ (EAP-MD5、EAP-TLS、PEAP、EAP-TTLS)	
	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	○	
	Proxy 利用環境	○	HTTP のみ(HTTPS はリダイレクトされない)
	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	
	バックアップ	プライマリー、セカンダリー/強制認証/ローカルデータベース	強制認証/ローカルデータベースは単独使用可能
	ローカルデータベース	3000 行 改行コード LF の場合：258032 バイト 改行コード CR+LF の場合：(ファイルサイズ - 登録行数) ≦ 258032 を満たすサイズ	
最大収容数※	Web/MAC/802.1X/ゲートウェイ	Apresia13000 シリーズ：1024 端末/台 Apresia13100/13200 シリーズ：5632 端末/台 Apresia13200-28GT シリーズ：1408 端末/台 Apresia15000 シリーズ：768 端末/台	• 利用環境により、最大収容端末数が異なる場合あり • Apresia13200-28GT シリーズは、クラス ID (ユーザーポリシーコントロール)未サポート
	Dynamic VLAN/クラス ID	Apresia13000 シリーズ：1024 端末/台 Apresia13100/13200 シリーズ：2048 端末/台 Apresia13200-28GT シリーズ：256 端末/台 Apresia15000 シリーズ：768 端末/台	
	DHCP Snooping	Apresia13000 シリーズ：612 端末/台 Apresia13100/13200 シリーズ：3216 端末/台 Apresia13200-28GT シリーズ：804 端末/台 Apresia15000 シリーズ：484 端末/台	
その他	IP アドレス環境	固定 IP アドレス/DHCP	Web 認証の Dynamic VLAN 端末は、DHCP 環境必須
	VLAN 環境	固定 VLAN/Dynamic VLAN	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		• Web、MAC、802.1X、DHCP Snooping 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ーリソー

スの関係について」を参照してください。

2.11.1 認証端末数とパケットフィルター2 のグループ数

AccessDefender では認証前後の端末制御にパケットフィルター2 のグループを使用します。パケットフィルター2 のグループは AccessDefender、認証バイパス、ユーザー設定のフィルター、各種機能で共有して使用されます。グループの割当状況は show packet-filter2 reserved-group コマンドにて確認可能です。

表 2-3 に AccessDefender で使用するパケットフィルター2 のグループ数を示します。各数字(1～14)はパケットフィルター2 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 で使用するパケットフィルター2 のグループ数

使用するグループ数	使用用途			
	Apresia13000 シリーズ	Apresia13100/13200 シリーズ	Apresia13200-28GT シリーズ	Apresia15000 シリーズ
1	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)
2	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)
3	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)	AccessDefender 制御用(必須)
4	認証端末用(必須)1～128	認証端末用(必須)1～512	認証端末用(必須)1～128	認証端末用(必須)1～128
5	認証端末用(任意)129～256	認証端末用(任意)513～1024	認証端末用(任意)129～256	認証端末用(任意)129～256
6	認証端末用(任意)257～384	認証端末用(任意)1025～1536	認証端末用(任意)257～384	認証端末用(任意)257～384
7	認証端末用(任意)385～512	認証端末用(任意)1537～2048	認証端末用(任意)385～512	認証端末用(任意)385～512
8	認証端末用(任意)513～640	認証端末用(任意)2049～2560	認証端末用(任意)513～640	認証端末用(任意)513～640
9	認証端末用(任意)641～768	認証端末用(任意)2561～3072	認証端末用(任意)641～768	認証端末用(任意)641～768
10	認証端末用(任意)769～896	認証端末用(任意)3073～3584	認証端末用(任意)769～896	-
11	認証端末用(任意)897～1024	認証端末用(任意)3585～4096	認証端末用(任意)897～1024	-
12	-	認証端末用(任意)4097～4608	認証端末用(任意)1025～1152	-
13	-	認証端末用(任意)4609～5120	認証端末用(任意)1153～1280	-
14	-	認証端末用(任意)5121～5632	認証端末用(任意)1281～1408	-

※ 最大認証端末数を縮小することにより、認証端末用(任意)のグループをユーザー領域/認証バイパス/各種機能用として使用できます。

Web 認証を使用する場合、DNS や DHCP の認証バイパス用に最低 1 グループの確保を推奨します。

表 2-4 にパケットフィルター2 のグループ数を使用する機能を示します。AccessDefender とこれらの機能を併用する場合は、グループ数の上限を超えないように最大端末数を制限してください(詳細は、コマンドリファレンスのパケットフィルター2 を参照してください)。

表 2-4 パケットフィルター2 のグループを使用するコマンド

機能	使用するグループ数
VLAN ごとのカウンター (counter vlan enable コマンド)	1～2
MLAG(mlag enable コマンド)	1
FDB 書き換わり多発検知 (mac-address-table frequent-station-move-notify enable コマンド)	1
ユーザーループ検知 (loop-watch enable コマンド)	Apresia13000 シリーズ：11 Apresia13100/13200-48X/13200-52GT シリーズ：4 Apresia13200-28GT シリーズ：1 Apresia15000 シリーズ：9
Flush FDB (flush-fdb rp-e enable コマンド)	1
Flush FDB (flush-fdb rp-g enable コマンド)	1
MMRP-Plus (mmrp-plus enable コマンド)	Apresia13000/13200-28GT シリーズ：1～2 Apresia13100/13200-48X/13200-52GT シリーズ：1 Apresia15000 シリーズ：1～3
MMRP-Plus(FDB フラッシュ制御フレーム受信) (mmrp-plus receive-flush-fdb enable コマンド)	1
IP アドレス(ip address コマンド)、 VB IP(vb ip address コマンド)	左記の 2 機能合わせて使用するグループ数 Apresia13000/13200-28GT シリーズ：0～5 Apresia13100/13200-48X/13200-52GT シリーズ：0～1 Apresia15000 シリーズ：0～4
IPv6 アドレス (ipv6 address コマンド、ipv6 enable コマンド)	Apresia13000/15000 シリーズ：1 ※1 Apresia13100/13200-48X/13200-52GT シリーズ：0～1 Apresia13200-28GT シリーズ：0～3
IGMP snooping (ip igmp snooping unregistered-filter コマンド)	1
MLD snooping (ipv6 mld snooping unregistered-filter コマンド)	1
BFS(bfs mode コマンド)	1
FCoE Forwarder(fcoe group コマンド) ※2	Apresia15000 シリーズ：1～9
Virtual BoxCore(vb enable コマンド)	1

※1. AEOS Ver. 8.23.01 以前のファームウェアを使用している場合、使用グループ数は Apresia13000/15000 シリーズ：1 となります。
※2. AccessDefender とは併用できません。

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ください。大きい番号で指定すると、AccessDefender が優先となり、認証バイパス設定が無効となります。

DHCP Snooping 併用時の最大認証端末数は表 2-5 となります。

3.10 認証拒否機能を使用する場合は、他に 1 グループが必要となります。

2.11.2 DHCP Snooping の認証端末数

表 2-5 に DHCP Snooping で使用するパケットフィルター2 のグループ数を示します。Apresia13100/13200-48X/13200-52GT シリーズにおける 801 端末目以降の認証、Apresia13000/13200-28GT/15000 シリーズにおける 201 端末目以降の認証では、パケットフィルター2 のルールを 2 つ使用します。

例(Apresia13100-48X-PSR)：最大ルール数が 1024 ルールの場合、DHCP Snooping では 912 端末が認証可能です。

端末数の計算式

800+(1024-800)/2＝912(端末)

表 2-5 DHCP Snooping で使用するパケットフィルター2 のグループ数

使用するグループ数	機種名			
	Apresia13000 シリーズ	Apresia13100/13200 シリーズ	Apresia13200-28GT シリーズ	Apresia15000 シリーズ
4	1～128	1～512	1～128	1～128
5	129～228	513～912	129～228	129～228
6	229～292	913～1168	229～292	229～292
7	293～356	1169～1424	293～356	293～356
8	357～420	1425～1680	357～420	357～420
9	421～484	1681～1936	421～484	421～484
10	485～548	1937～2192	485～548	-
11	549～612	2193～2448	549～612	-
12	-	2449～2704	613～676	-
13	-	2705～2960	677～740	-
14	-	2961～3216	741～804	-

DHCP Snooping の最大認証端末数は、MAC/Web/802.1X 認証機能の最大認証端末数(表 2-3)と比較して少ないので、ご注意ください。

DHCP Snooping 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。

2.12 Web サーバー応答、及び仮想 IP の仕組み

2.12.1 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するなど、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。

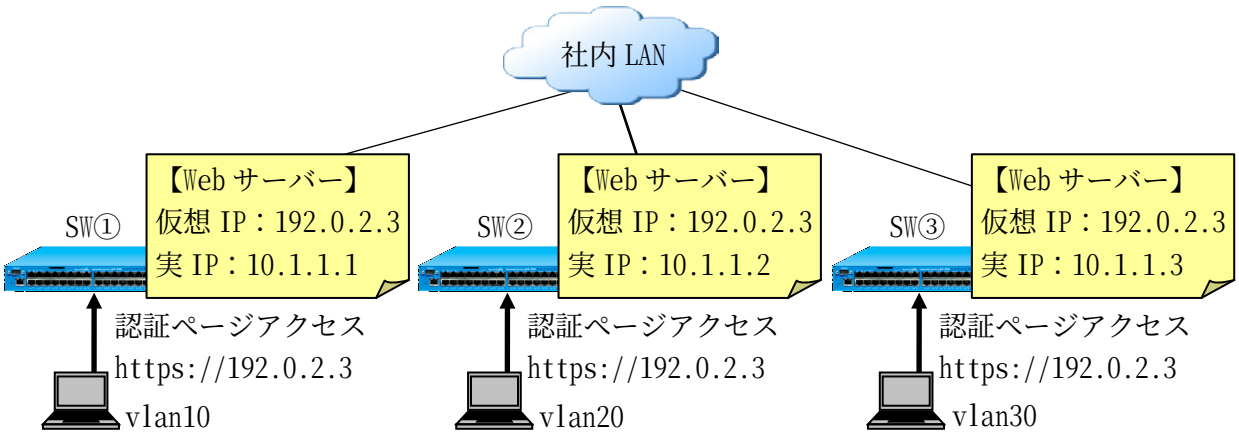


図 2-16 仮想 IP による認証 URL アクセス

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 192.0.2.3)。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)。

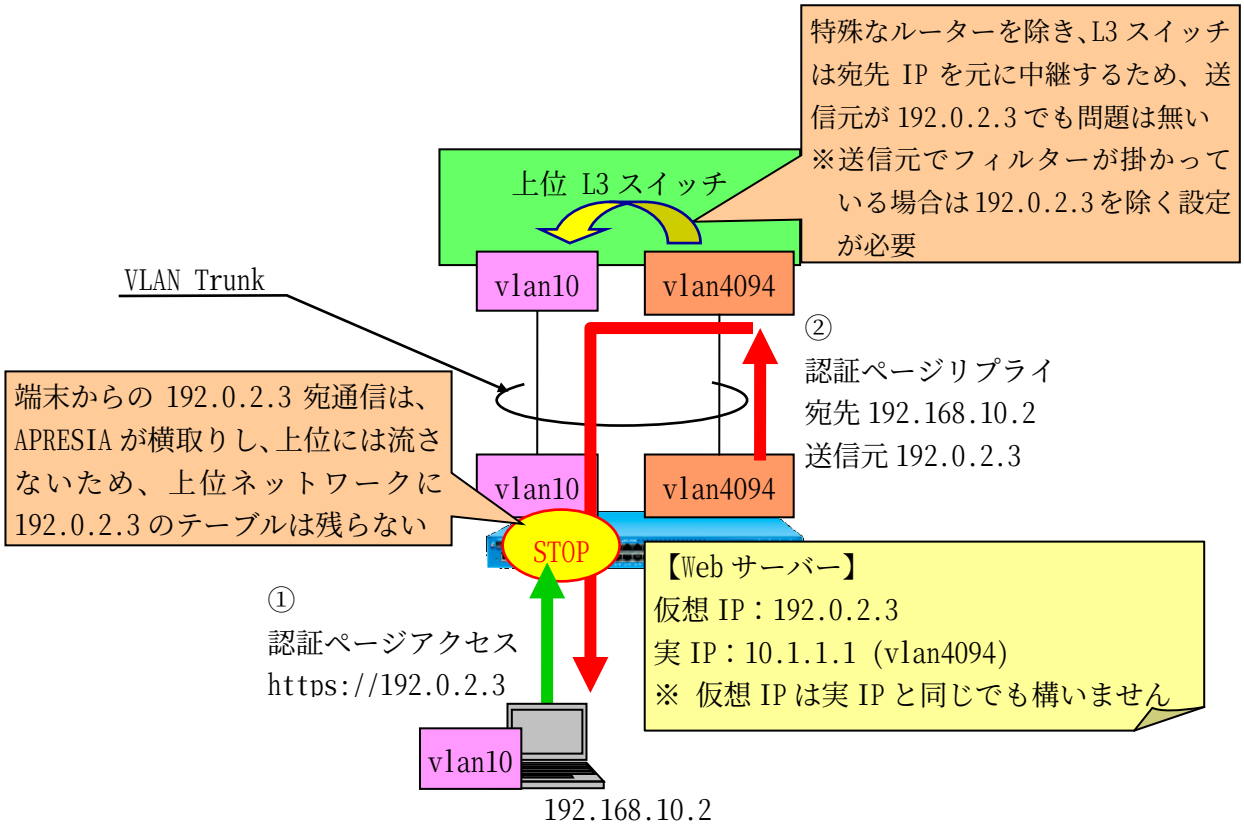


図 2-17 認証ページのリプライ応答

2.12.2 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ー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ー条件に APRESIA の HTTP 応答パケットなどが合致する場合、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)のフィルターを解除する
- L3 スイッチに、APRESIA の送信元 MAC を許可するフィルターを設定する
- 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ーを設定する
- APRESIA に、ユーザーVLAN(vlan10)にも IP を設定する

  ※ ただし以下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

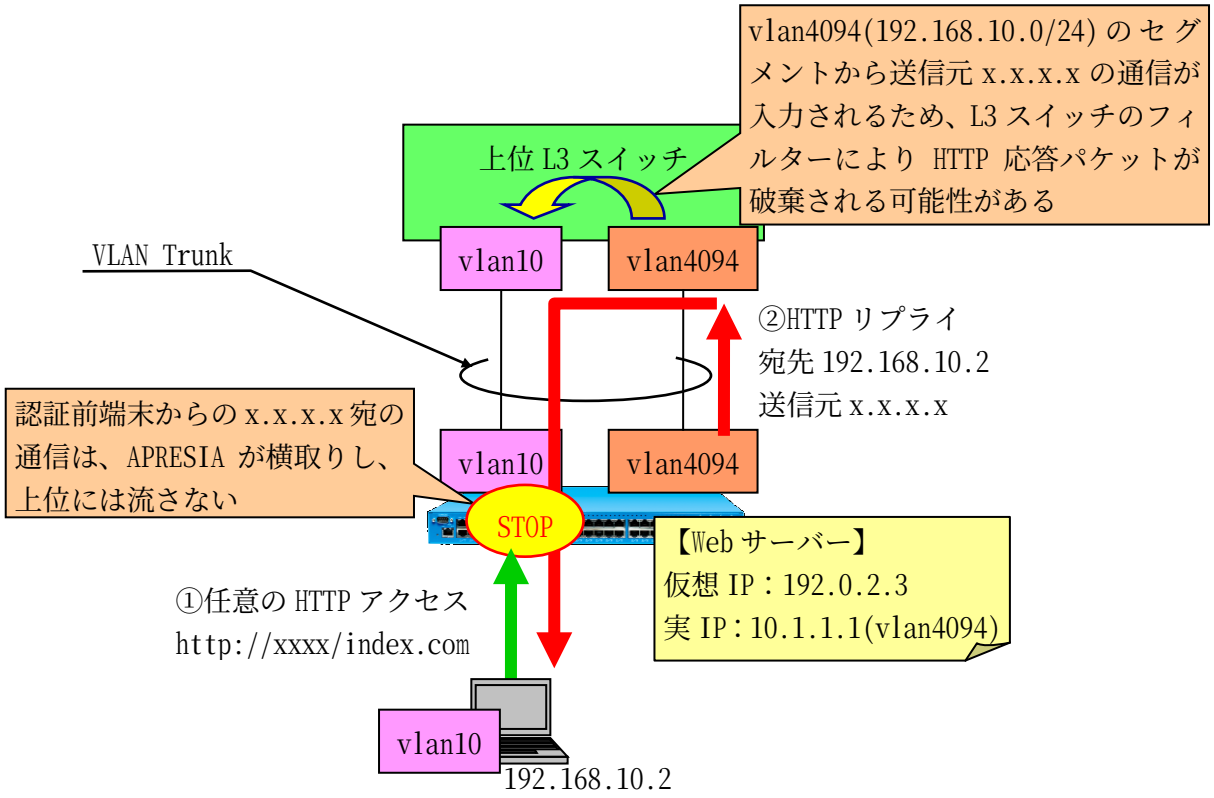


図 2-18 認証ページリダイレクト使用時の注意点

2.12.3 動作確認済ブラウザー

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

表 2-6 動作可否確認済みブラウザー(認証ページリダイレクト使用時)

ブラウザー	OS	リダイレクト可否
Internet Explorer 6	Windows XP SP2	○
Internet Explorer 7	Windows Vista Business	○
Internet Explorer 8	Windows XP SP3	○
Internet Explorer 8	Windows 7 Pro	○
Internet Explorer 9	Windows 7 Pro	○
Internet Explorer 10	Windows 8	○
Internet Explorer 11	Windows 8.1	○
Opera 10.10	Windows 7 Pro	○
Opera 10.51	Windows XP SP3	○
Firefox 3.6	Windows 7 Pro	○
Safari 4.0	Windows XP SP3	○
Google Chrome 4.1	Windows XP SP3	○
Firefox 3.5	Ubuntu 9.10	○
Safari 1.2	Mac OS 10.3.9	○
Safari	iOS 6.0.1	○
標準ブラウザー	Android 4.0.4	○

iOS 6 をご利用の場合、Wi-Fi 接続時の"www.apple.com"への自動アクセスをリダイレクトした認証画面から認証する場合、認証情報が APRESIA へ正常に送信されず認証に失敗することがあります。その場合、一度認証画面に戻り再度認証を行うことで、正常にログインできます。

AEOS 8.23.01 より前のバージョンで Windows 8.1 の Internet Explorer 11 をご利用の場合、認証ページのログアウトボタンが動作しないことがあります。その場合、Web ページカスタマイズ機能で当該ページの submit のフォームに任意の name 属性を追加してください。
例. 「 <input type="submit" name="action" value="logout"> 」

2.13 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 2-7 に示します。

17 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 2-7 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	802.1X	DHCP Snooping
1	ログアウトボタン ※	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 IP アドレス、MAC アドレス、ユーザーID 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	○	-	-	-
8	Logoff 受信	サプリカントからの logoff 受信によるログアウト	logoff	-	-	○	-
9	再認証失敗	再認証失敗によるログアウト	reauth failure	-	-	○	-
10	再認証失敗	再認証時にサプリカント応答なしによるログアウト	reauth failure (supp-timeout)	-	-	○	-
11	再認証時の vlan 変更検出	再認証時の vlan 変更検出によるログアウト	reauth vlan change	-	-	○	-
12	再認証時のユーザーネーム変更検出	再認証時のユーザーネーム変更検出によるログアウト	reauth user name change	-	-	○	-
13	再認証時のクラス ID 変更検出	再認証時のクラス ID 変更検出によるログアウト	reauth class change	-	-	○	-
14	ポート設定初期化	ポート設定初期化によるログアウト	port initialization	-	-	○	-
15	IP リリース	IP リリースによるログアウト	release	-	-	-	○

No	ログアウト方法	動作概要	Syslog 表示	Web 認証	MAC 認証	802.1X	DHCP Snooping
16	IP リース期間満了	IP リース期間満了によるログアウト	expire	-	-	-	○
17	logout ping 受信	logout ping 受信によるログアウト	ping	○	-	-	-

※ 設定によらず、常に有効となります。

リンクダウンによるログアウトの設定のみポート単位での設定変更が可能となります。それ以外のログアウトの設定は装置単位となり、ポートごとに設定を変更することはできません。

2.14 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い、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

(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、パスワードともに、キーボードから直接入力できる文字はすべて有効
- APRESIAの設定コンソール上では「?」はコマンドヘルプと認識するため、MAC認証用のパスワード設定では「?」は入力できない
  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
- RADIUSサーバーにより制御文字の扱いが異なるため、使用するRADIUSサーバーの仕様にしたがう必要がある
- 日本語はユーザーIDで入力はできるが、認証不可(失敗)となる
- ユーザーID、パスワードともに、「&amp」、「&gt」、「&lt」は、そのまま文字列として認証可能
- ユーザーID、パスワードともに、
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

3 AccessDefender 機能の設定

AccessDefender 機能を使用する際には、APRESIA 側で以下の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)

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・設定不可項目、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	802.1X	DHCP Snooping	
1	AccessDefender 有効化	disable	○	○	○	○	
2	RADIUS サーバー ※1						
	INDEX	なし	○	○	○	-	1～8
	IPv6_INDEX	なし	○	○	○	-	9～16
	IP アドレス	なし	○	○	○	-	
	IPv6 アドレス	なし	○	○	○	-	
	UDP ポート番号	1812				-	1～65535
	タイムアウト時間	3 秒				-	1～30 秒
	リトライ回数	3 回				-	1～5 回
	共有鍵(シークレットキー)	なし	○	○	○	-	1～127 文字
	Primary/Secondary 指定	なし	○	○	○	-	1～16
	ローカル認証	なし			-	-	
	強制認証	なし				-	
	デッドタイム	なし				-	1～1440 分
3	認証ポート						
	Web 認証	なし	○	-	-	-	ポート併用可能
	MAC 認証	なし	-	○	-	-	
	802.1X	なし	-	-	○	-	
	DHCP Snooping	なし	-	-	-	○	
4	MAC 認証パスワード	なし	-	○	-	-	
5	認証 Web ページ						
	HTTP ポート番号	なし	○	-	-	-	1～65535
	HTTPS ポート番号	なし	○	-	-	-	1～65535
	認証用 IP アドレス(URL)	なし	○	-	-	-	
	リダイレクト URL	なし		-	-	-	最大 255 文字
	リダイレクト対象ポート(HTTP)	なし		-	-	-	ポート 80
	リダイレクト対象ポート(HTTPS)	なし		-	-	-	ポート 443
	リダイレクト対象ポート(Proxy)	なし		-	-	-	1～65535
6	再認証(802.1X)						

No	項目	default 設定	認証方法				備考
			Web	MAC	802.1X	DHCP Snooping	
	再認証有効	なし	-	-		-	
	再認証間隔	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	30 秒	-	-		-	5～65535 秒
8	ログアウト条件						
	エージング	0 秒					10 秒～1 ヶ月
	接続時間	0 秒				-	10 秒～1 ヶ月
9	最大接続台数						
	ポート番号	なし					
	最大接続台数(1 ポートあたり)	なし					
	最大接続台数(装置あたり)	なし	○	○	○	○	
10	DHCP Snooping						
	静的フィルター登録 ※2	なし	-	-	-		
	自動切換えモードタイマー ※3	なし	-	-	-		
11	その他						
	制御用先頭グループ ※4	なし					
	802.1X 初期化実行	なし					随時(その都度実行します)
	802.1X 再認証実行	なし					
12	SSL 用秘密鍵(鍵長) ※5	1024 bit		-	-	-	512～2048 bit
13	syslog(IP/facility/priority) ※6	なし					
14	パケットフィルター2						
	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、静的にフィルターを登録することで、DHCP Snooping 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. 自動で設定されます。

※5. ファームウェアには、あらかじ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ください。

※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 Snooping 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、センター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なため、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。

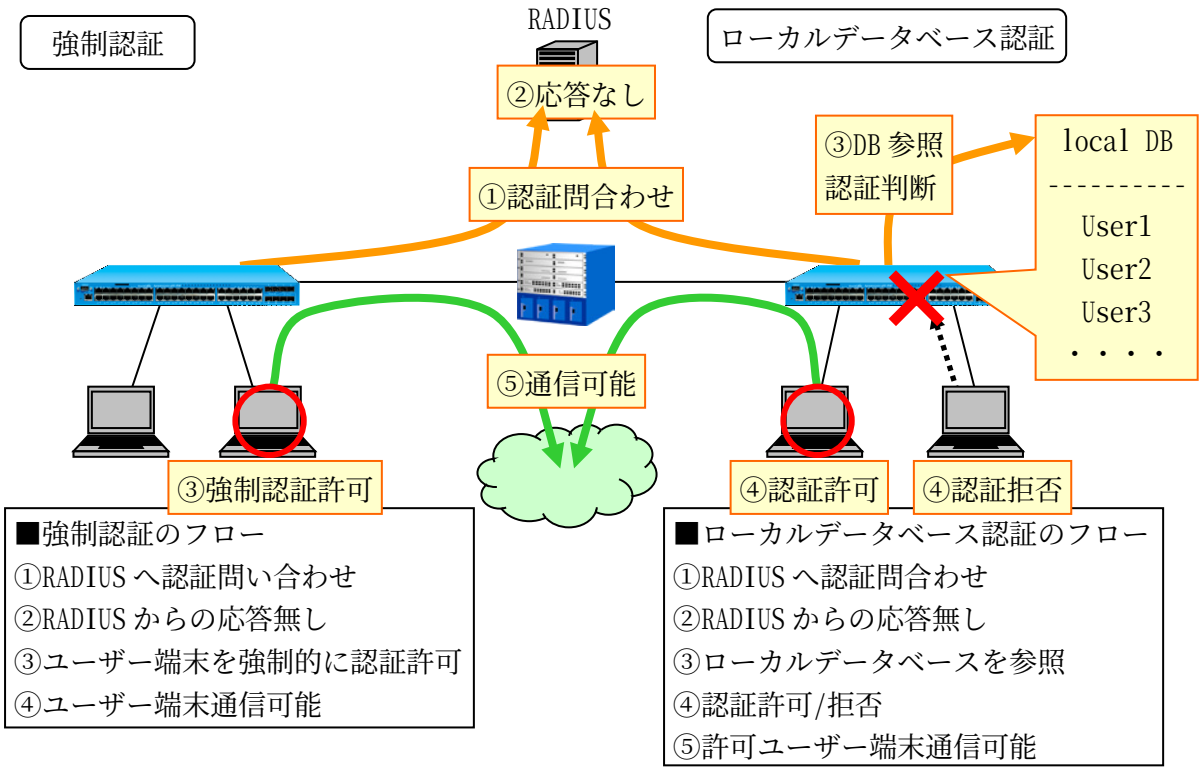


図 3-1 ローカルデータベース認証と強制認証

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 [<ID>] <*RADIUS1*> | <*LOCAL*> | <*FORCE*>
(config)# aaa authentication mac <*RADIUS1*> | <*LOCAL*> | <*FORCE*>
RADIUS1 = radius <INDEX1> [<INDEX2>] [local | <*FORCE*>]
LOCAL = local [radius <INDEX1> [<INDEX2>] [<*FORCE*>]]
FORCE = force [vlan <VID>]

・・・ID　　認証 ID <1-4>
・・・INDEX1　　プライマリーRADIUS サーバーのインデックス <1-16>
・・・INDEX2　　セカンダリーRADIUS サーバーのインデックス <1-16>
・・・local　　ローカルデータベース認証を実行
・・・force　　強制認証を実行
・・・VID　　認証後の VLAN ID <1-4094>

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、及び強制認証は、ポートごとではなく装置単位での設定となります。

3.3 ローカルデータベースによる認証(Web 認証、MAC 認証のみ)

APRESIA 内部にユーザー名・パスワード・VLAN ID 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。

MLAG 併用時、ローカルデータベースは first 装置と second 装置で一致させるようにしてください。RADIUS サーバーを使用する場合、first 装置と second 装置で同一のサーバーを参照するなど、同一の認証データを使用するようにしてください。

3.3.1 ローカルデータベースフォーマット

APRESIA 内部に保存するローカルデータベースのフォーマットを表 3-3 に示します。

表 3-3 ローカルデータベースフォーマット

項目	内容
形式	userid,password[,vid][,classid]の CSV 形式 (userid、password は最大 63 文字)
最大登録行数	3000 行
最大ファイルサイズ	改行コード LF の場合：258032 バイト 改行コード CR+LF の場合：(ファイルサイズ - 登録行数) ≦ 258032 を満たすサイズ

<ローカルデータベースの登録例>

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

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 として登録してください。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。

3.3.2 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 サーバー、または SD メモリーカードを用いて APRESIA に登録(ダウンロード)します。登録は AccessDefender 有効時も可能で、新しいファイルが上書きされます。

```
# copy ( tftp <IPADDR> ) | memory-card <FILE> aaa-local-db
# copy tftp <IPv6ADDR> [ manage | ( vlan <VID> ) ] <FILE> aaa-local-db
              ・・・IPADDR          TFTP サーバーの IP アドレス
              ・・・IPv6ADDR        TFTP サーバーの IPv6 アドレス
              ・・・VID             VLAN ID
              ・・・FILE            ファイル名 <1-128(文字)>
```

登録行数が 3001 行以上ある、書式に従わない行が存在する、またはファイルサイズが最大サイズ(改行コード LF の場合：258032 バイト、改行コード CR+LF の場合：(ファイルサイズ - 登録行数) ≦ 258032 を満たすサイズ)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 ダウンロード時のコンソールメッセージ表示例

内容	表示例
正常なファイルの場合	Writing to flash memory... done.
指定したファイルが存在しない場合	Error code 1: File not found.
ファイルサイズが上限を超えている場合	aaa-local-db : over max file size ldb.txt : download fail
3000 行以上ある場合	aaa-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
書式不適合の行がある場合	Invalid format: line: 10 user10,,user10,10

	ldb.txt : download fail
同一ユーザー名の行が複数存在する場合	Invalid format: luseruser is duplicated. ldb.txt : download fail

3.3.3 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 サーバー、または SD メモリーカードにアップロードできます。

```
# copy aaa-local-db ( tftp <IPADDR> ) | memory-card <FILE>
# copy aaa-local-db tftp <IPv6ADDR> [ manage | ( vlan <VID> ) ] <FILE>
              ・・・IPADDR          TFTP サーバーの IP アドレス
              ・・・IPv6ADDR        TFTP サーバーの IPv6 アドレス
              ・・・VID             VLAN ID
              ・・・FILE            ファイル名 <1-128(文字)>
```

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ください。

3.3.4 ローカルデータベースの削除

APRESIA に登録済みのローカルデータベースを削除するには erase aaa-local-db コマンドを実行します。登録されているすべ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ください。

3.3.5 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、<CLASSID>省略時はクラス ID 無しとして登録されます。

```
# aaa-local-db add user <USERID> [ <OPTIONS> ]
OPTIONS には以下オプションが複数指定可能
OPTIONS = ( password <PASSWORD> ) | ( vlan <VID> ) | ( class <CLASSID> )
              ・・・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>
              ・・・CLASSID         クラス ID <1-4095>
```

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
ユーザー名に使用禁止文字を指定した場合	% Invalid user ID.
ユーザー名に 64 文字以上を指定した場合	% Too long user ID.
パスワードに使用禁止文字を指定した場合	% Invalid password.
パスワードに 64 文字以上を指定した場合	% Too long password.

3.3.6 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ローカルデータベースのエントリーを削除します。

```
# 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.
ユーザー名に 64 文字以上を指定した場合	% Too long user ID.
未登録のユーザー名を指定した場合	% The user does not exist.

3.4 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。

強制認証を有効にすると、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へ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、及び強制認証は、ポートごと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すべて残るため、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 6.4 MAC アドレスの自動収集を参照してください)。

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ください。

3.5 強制認証機能(802.1X)

本機能を有効にすることで、認証端末が装置に設定されているすべての認証サーバーにアクセスできない場合、あらかじめ設定されている 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るようになります。

強制認証の設定コマンドは以下となります。

(config)# aaa authentication dot1x <*RADIUS2*> | <*FORCE*>
RADIUS2 = radius <INDEX1> [<INDEX2>] [<*FORCE*>]
FORCE = force [vlan <VID>]
・・・INDEX1　プライマリーRADIUS サーバーのインデックス <1-16>
・・・INDEX2　セカンダリーRADIUS サーバーのインデックス <1-16>
・・・force　強制認証を実行
・・・VID　認証後の VLAN ID <1-4094>

RADIUS サーバーから正常な応答がある場合には、図 2-7 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は、図 3-2 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)。

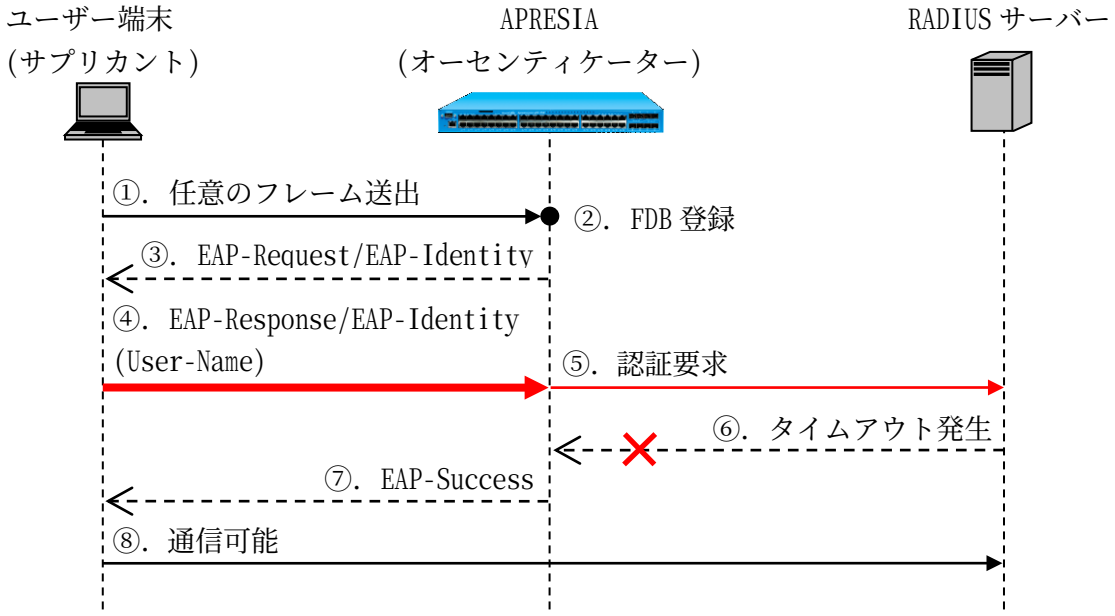


図 3-2 強制認証機能有効時における RADIUS 無応答時の認証フロー

本機能が有効の場合、設定されている全 RADIUS サーバーがタイムアウトの時に、サプリカントに EAP-Success を返します。しかし、サプ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。

3.6 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で、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。認証ポートごとに設定する場合は、port オプションを指定してください。port オプションを省略した場合は、装置全体に対して有効になります。port オプション指定の設定と port オプション省略の設定を両方設定する場合、指定したポートでは、port オプション指定の設定が優先されます。

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 [<ID>] <*RADIUS1*> | <*LOCAL*> | <*FORCE*> [port <PORTRANGE>]
(config)# aaa authentication mac <*RADIUS1*> | <*LOCAL*> | <*FORCE*> [port <PORTRANGE>]
RADIUS1 = radius <INDEX1> [<INDEX2>] [local | <*FORCE*>]
RADIUS2 = radius <INDEX1> [<INDEX2>] [<*FORCE*>]
LOCAL = local [radius <INDEX1> [<INDEX2>] [<*FORCE*>]]
FORCE = force [vlan <VID>]

・・・ID	認証 ID <1-4>
・・・INDEX1	プライマリーRADIUS サーバーのインデックス <1-16>
・・・INDEX2	セカンダリーRADIUS サーバーのインデックス <1-16>
・・・force	強制認証を実行
・・・VID	認証後の VLAN ID <1-4094>
・・・PORTRANGE	ポート番号 (複数指定可能)

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 サーバーへの問い合わせ、または強制認証を行います。

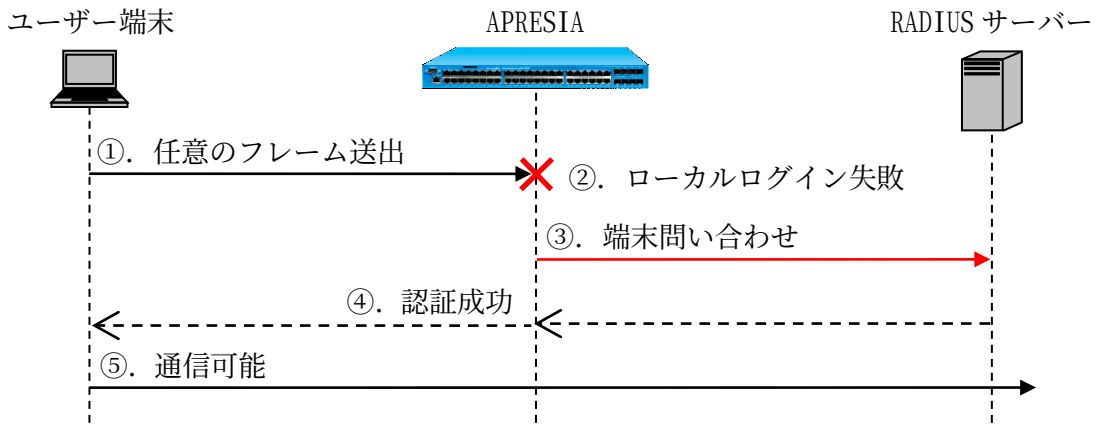


図 3-3 認証順序変更時におけるローカルログイン失敗時の認証フロー(MAC 認証)

本機能を使用する場合は、3.7 移行条件変更機能をあわ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い合わせは行われませんので注意してください。詳しくは、3.7 移行条件変更機能を参照してください。

port オプション指定の場合は、check-vb-common-config コマンドの差分確認、及び sync-vb-common-config コマンドの同期処理の対象から外れます。

LAG/MLAG インターフェースの認証ポートは未サポートです。port オプションを省略して設定してください。

3.7 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で、複数の承認(プライマリー/セカンダリーRADIUS サーバー、ローカルログイン、強制認証機能)が設定されている場合、いずれか１つに成功すれば認証成功となります。RADIUS サーバーからの認証拒否応答受信による認証失敗時は、セカンダリーRADIUS サーバー、ローカルログイン、または強制認証での認証が有効となります。認証ポートごとに設定する場合は、port オプションを指定してください。port オプションを省略した場合は、装置全体に対して有効になります。

port オプションの有無による動作の違いを表 3-8 に示します。

表 3-8 port オプションの有無による動作の違い

port オプション	物理ポート	LAG/MLAG インターフェース
有り	指定されたポートのみ有効	無効
無し	全ポート有効	全インターフェース有効

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 [ <ID> ] ) | mac control sufficient [ port <PORTRANGE> ]
(config)# aaa authentication login control sufficient
                ・・・ID                認証 ID <1-4>
                ・・・PORTRANGE         ポート番号 (複数指定可能)
```

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。

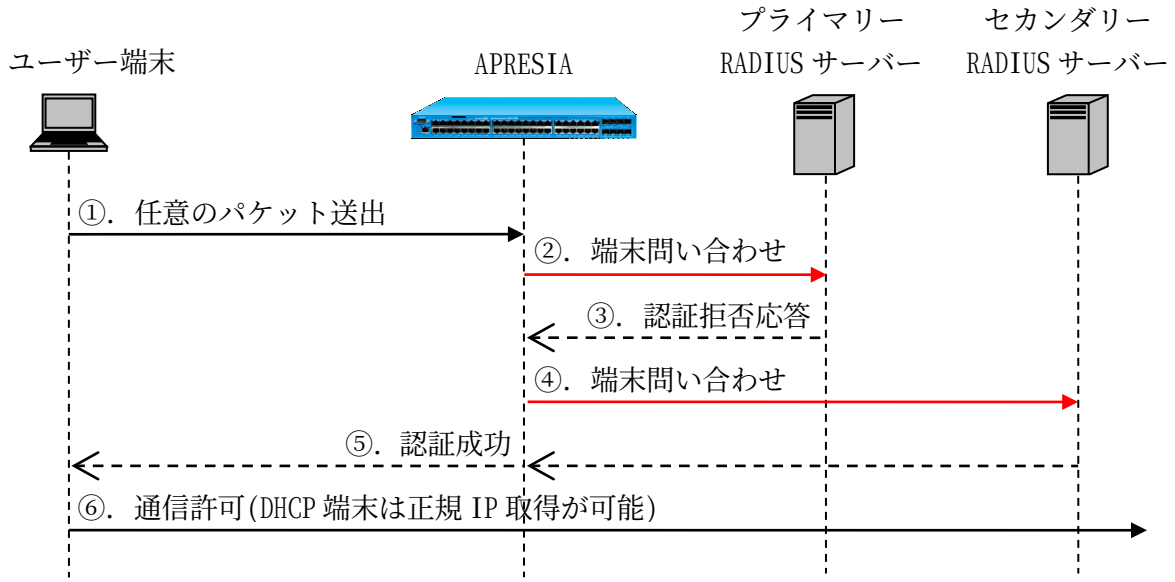


図 3-4 移行条件変更機能有効時における RADIUS 認証拒否時の認証フロー(MAC 認証)

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。

port オプション指定の場合は check-vb-common-config コマンドの差分確認、及び sync-vb-common-config コマンドの同期処理の対象から外れます。

LAG/MLAG インターフェースの認証ポートは未サポートです。port オプションを省略して設定してください。

3.8 認証方法選択機能(Web 認証のみ)

本機能を有効にすることで、ユーザーがブラウザー上で認証 ID を指定し、あらかじめ認証 ID ごと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、6.1.3 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 [<ID>] <*RADIUS1*> | <*LOCAL*> | <*FORCE*> [port <PORTRANGE>]
RADIUS1 = radius <INDEX1> [<INDEX2>] [local | <*FORCE*>]
LOCAL = local [radius <INDEX1> [<INDEX2>] [<*FORCE*>]]
FORCE = force [vlan <VID>]

・・・ID　　認証 ID <1-4>
・・・INDEX1　　プライマリーRADIUS サーバーのインデックス <1-16>
・・・INDEX2　　セカンダリーRADIUS サーバーのインデックス <1-16>
・・・local　　ローカルデータベース認証を実行
・・・force　　強制認証を実行
・・・VID　　認証後の VLAN ID <1-4094>
・・・PORTRANGE　ポート番号（複数指定可能）

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。

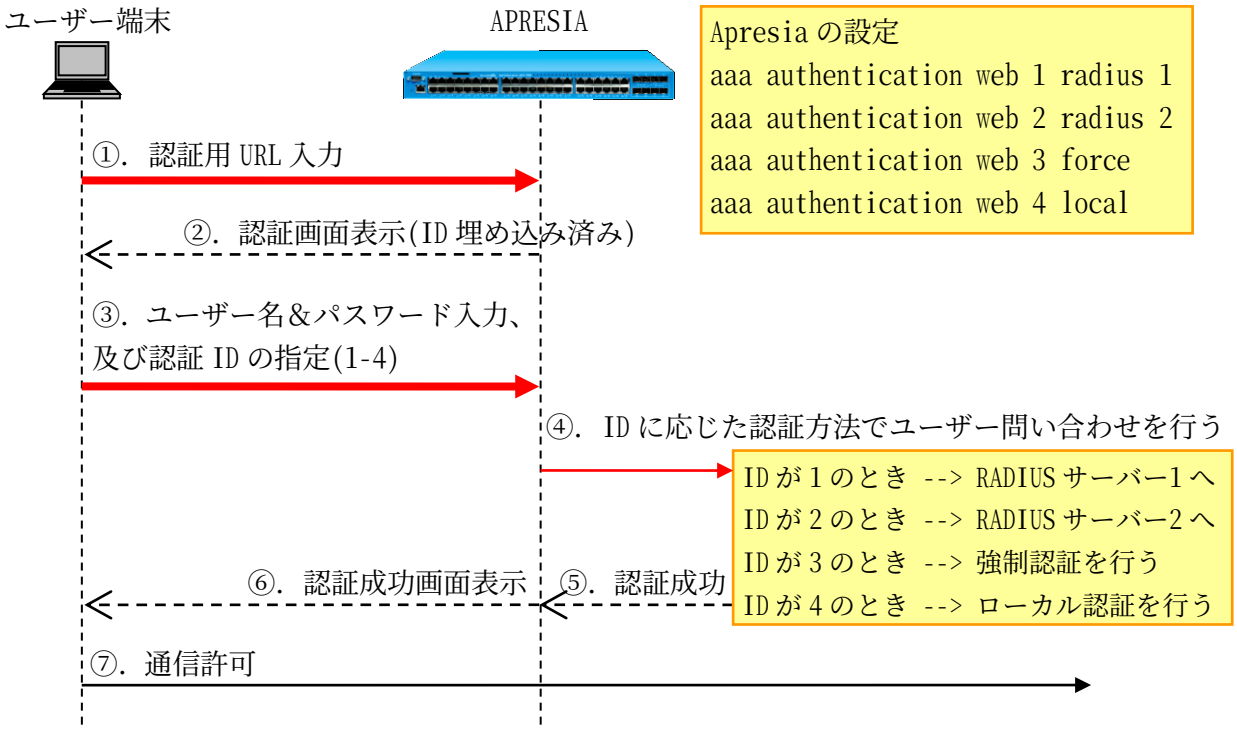


図 3-5 認証方法選択機能の認証フロー

3.9 認証バイパス

3.9.1 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以下の 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 アドレスのベンダーコードで許可

【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。

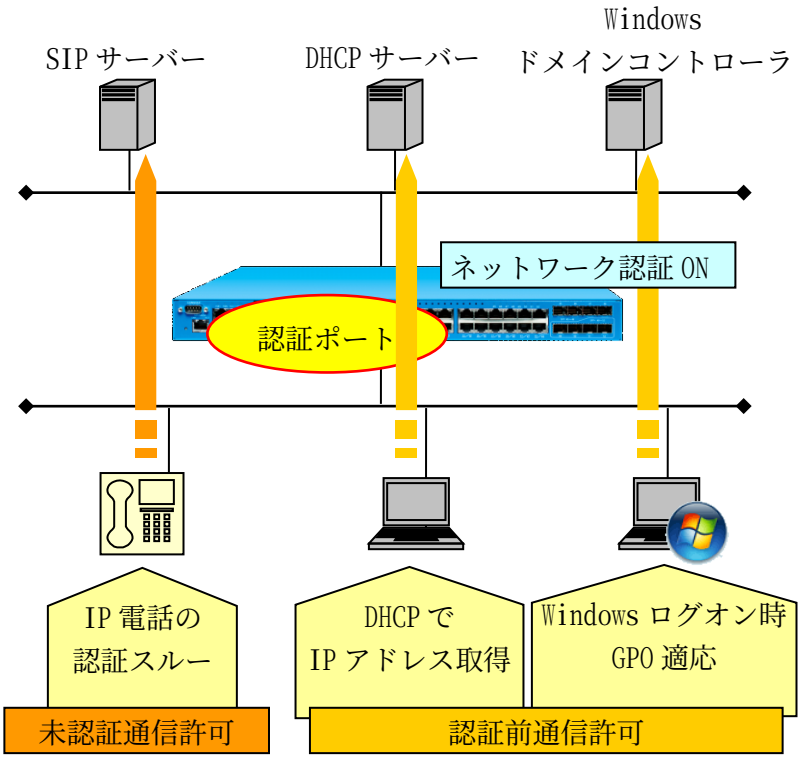


図 3-6 認証バイパス機能の概要

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 によるフィルター対象パケットを識別し、フィルター対象パケットとフィルター条件(condition)を比較し、フィルター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 の項目を参照してください。

表 3-9 認証バイパスの主な許可条件

仕様		AccessDefender 認証バイパス	備考
主なフィルター条件	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
	フィルター適用範囲指定	ポート(レンジ指定可能) VLAN (マスク指定可能)	

3.9.2 認証バイパスによる強制転送設定例(1)

以下の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

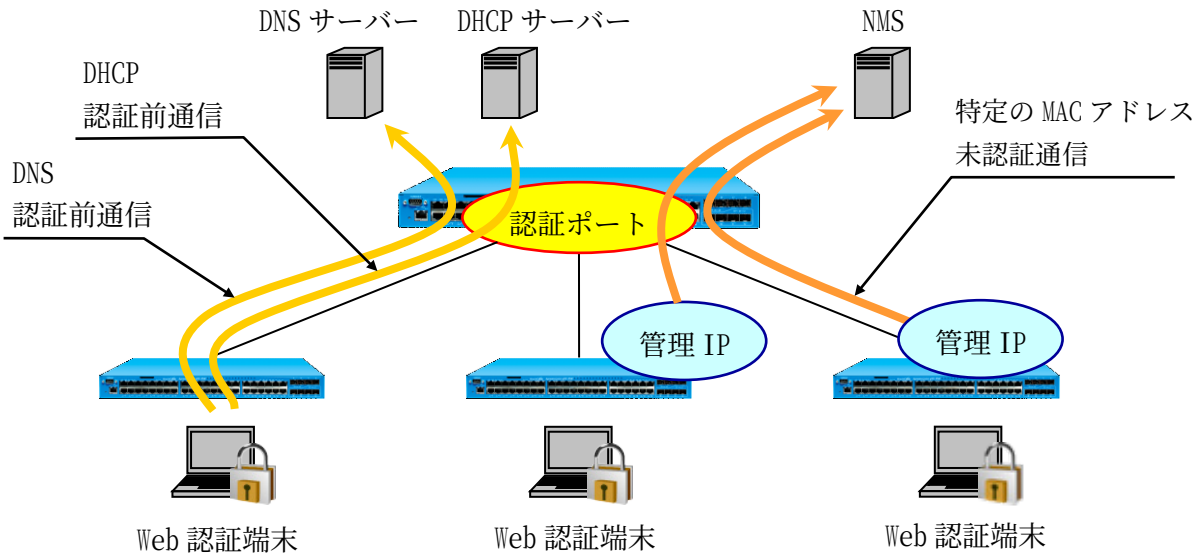


図 3-7 認証バイパス要求例(1)

```
(config)# packet-filter2
(config-filter)# 1 assign port 1/1-44
(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 とします。

(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 1/1-44
(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 でベンダーコード 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 とします。
```

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。AccessDefender よりも大きい番号で指定すると、AccessDefender が優先となり、認証バイパス設定が無効となります。

3.9.3 認証バイパスによる強制転送設定例(2)

以下の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

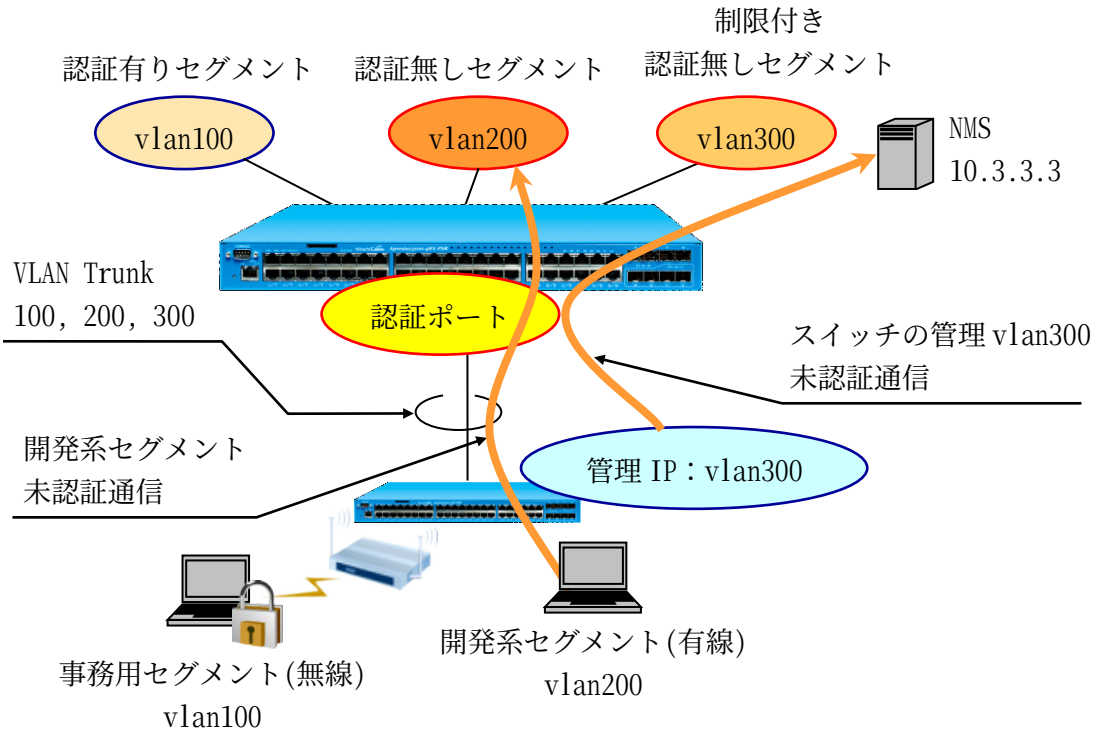


図 3-8 認証バイパス要求例(2)

```
(config)# packet-filter2
(config-filter)# 1 assign port 1/1-44
(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 とします。

(config-filter)# 2 assign port 1/1-44
(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：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)とします。
```

3.9.4 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、ドメインへログオンできない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 3-10 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	• 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 ※ 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 3-9 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。

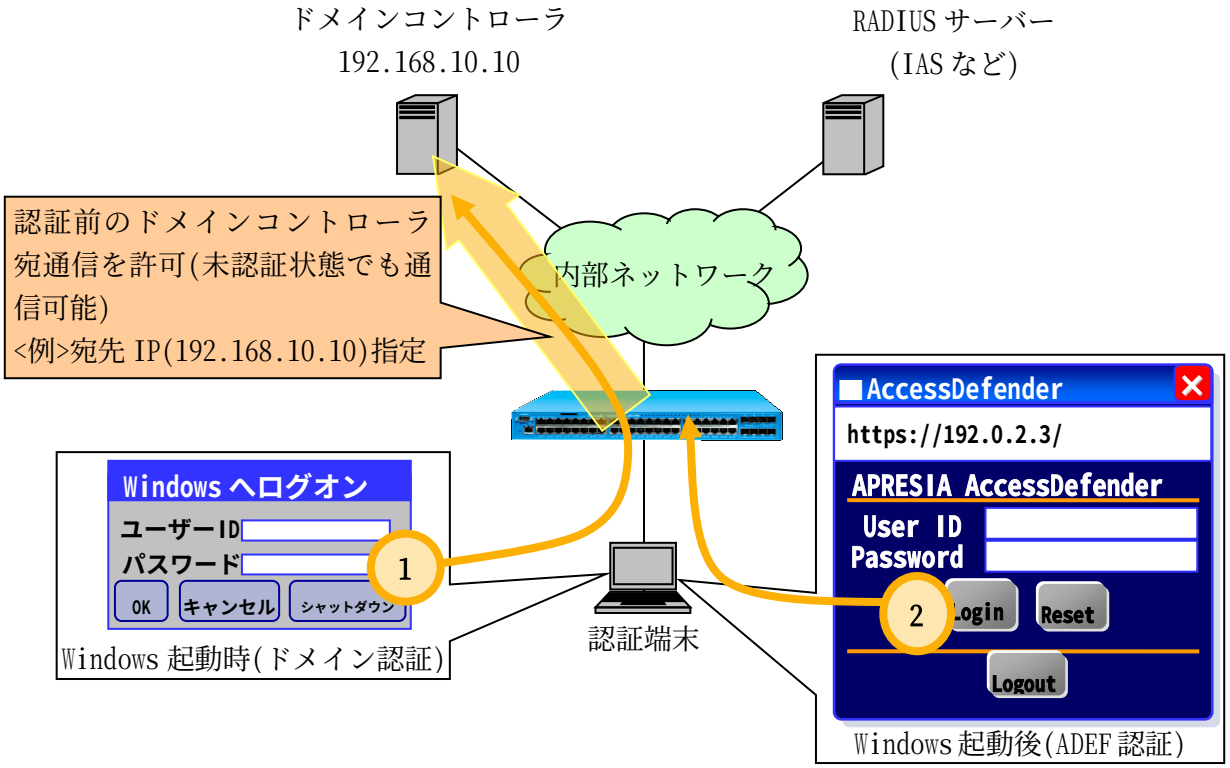


図 3-9 認証バイパスによる Windows ドメイン環境への適用

3.10 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 を設定する必要があります。

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(分)>
```

Web 認証の場合は図 3-10 のように認証用 URL へのアクセスが不可となります。

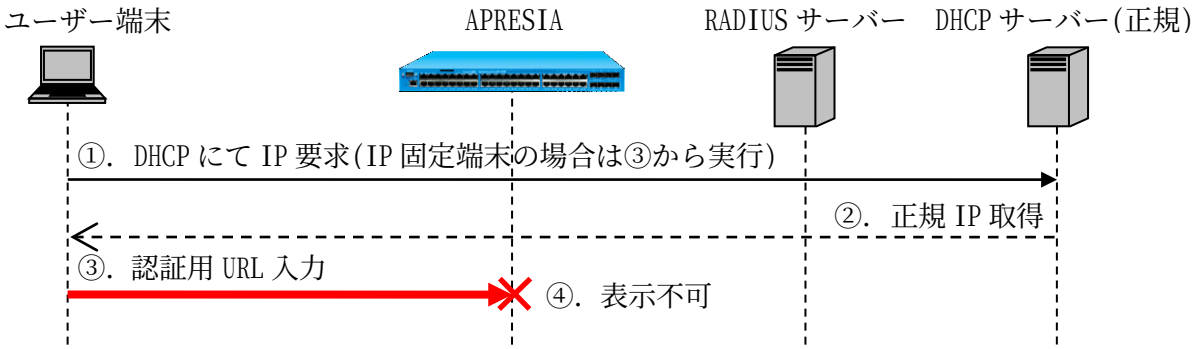


図 3-10 Web 認証端末の認証拒否

access-defender-deny コマンド ip 指定端末からの ARP によって MAC 認証が行われる場合があります。MAC 認証が成功しても認証拒否時間内は通信できません。

3.11 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://192.0.2.3/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と、APRESIA が指定されたアドレスへリダイレクトする
- 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ーに表示する安心設計である

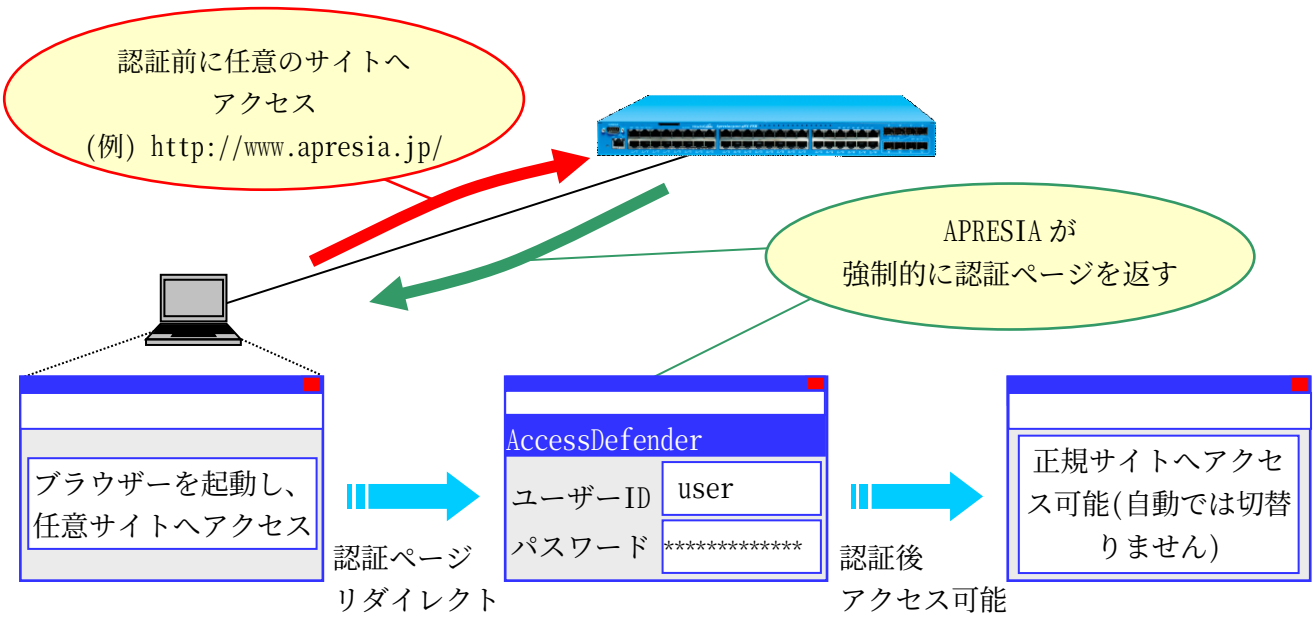


図 3-11 認証ページのリダイレクト機能概念図

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、また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。

3.11.1 HTTP プロキシが無い環境(直接 Internet へ接続)

3.11.1.1 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"とともに設定された 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ーは指定された 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、RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1 を参照してください)。

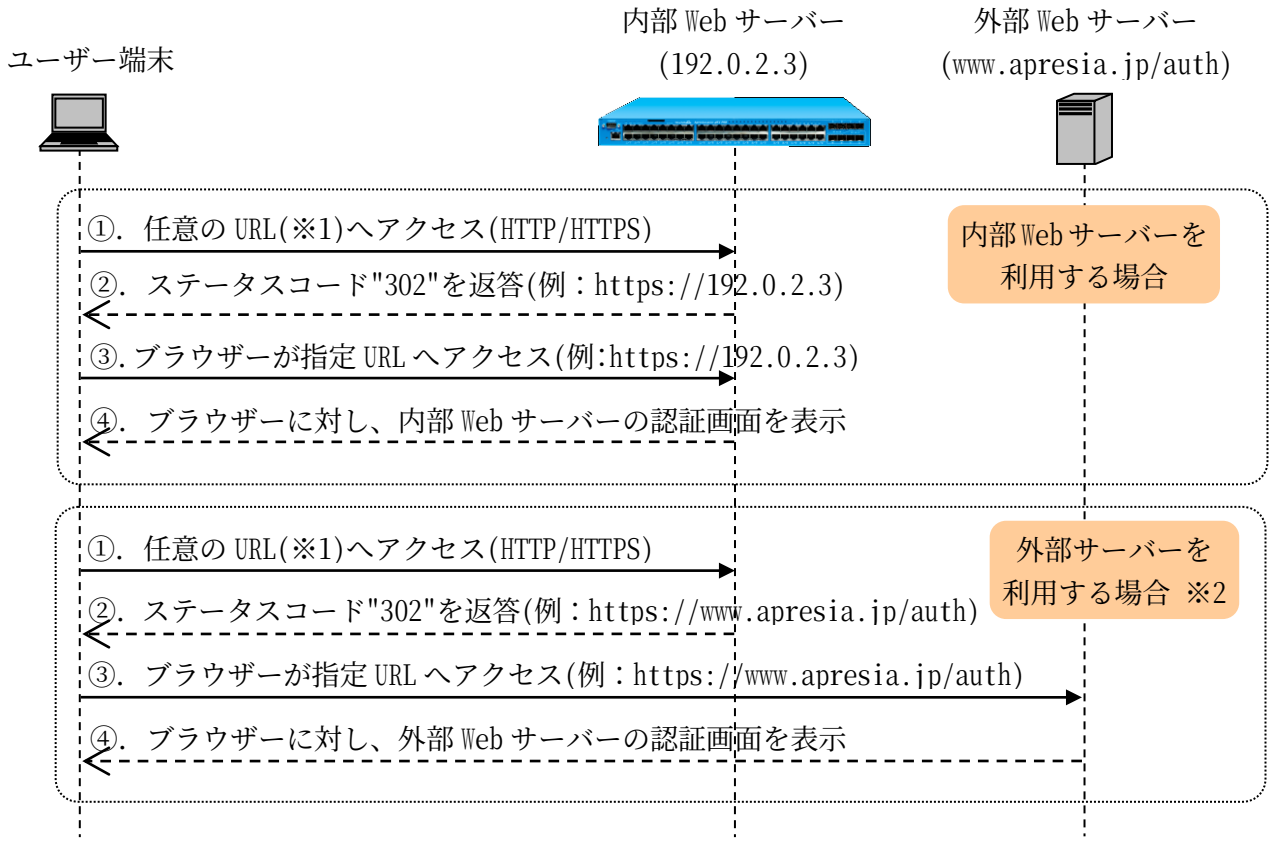


図 3-12 プロキシサーバーがない環境での認証フロー

※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。

3.11.1.2 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。

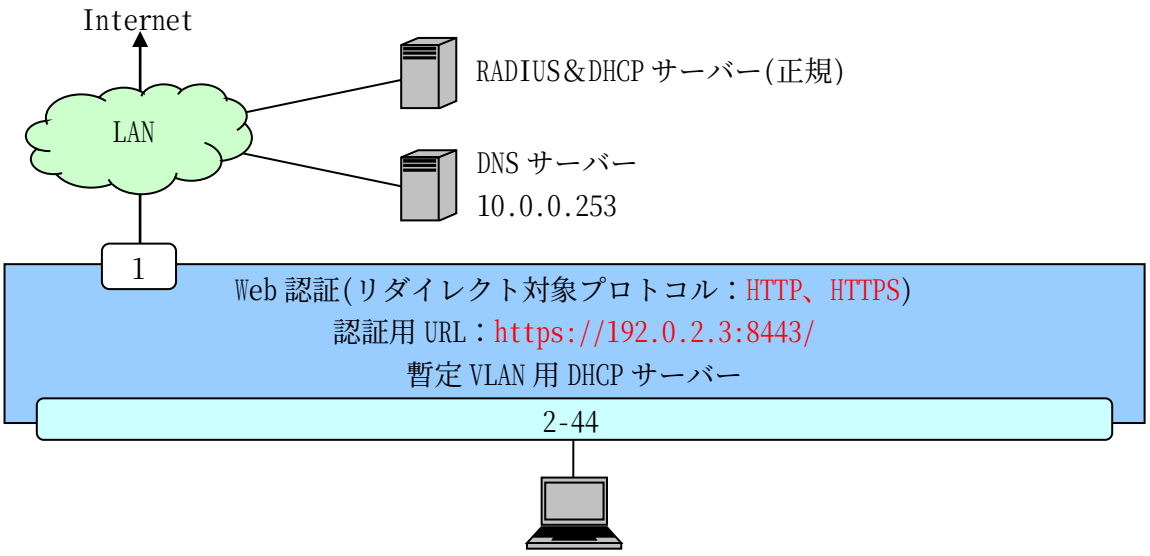


図 3-13 認証ページリダイレクト構成例(APRESIA 標準認証画面使用)

図 3-13 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などの設定は省略しています)。

```
(config)# packet-filter2
(config-filter)# 1 1 assign port 1/2-44
(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://192.0.2.3:8443/
                ・・・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 192.0.2.3
(config-a-def)# web-authentication https-port 8443
                ・・・認証 URL(https://192.0.2.3:8443/)（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 30
(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 30 秒)

※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に
合わせて適正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。

3.11.2 HTTP プロキシサーバーが存在する環境

3.11.2.1 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"とともに設定された 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ーは指定された 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、RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1 を参照してください)。

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ー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。

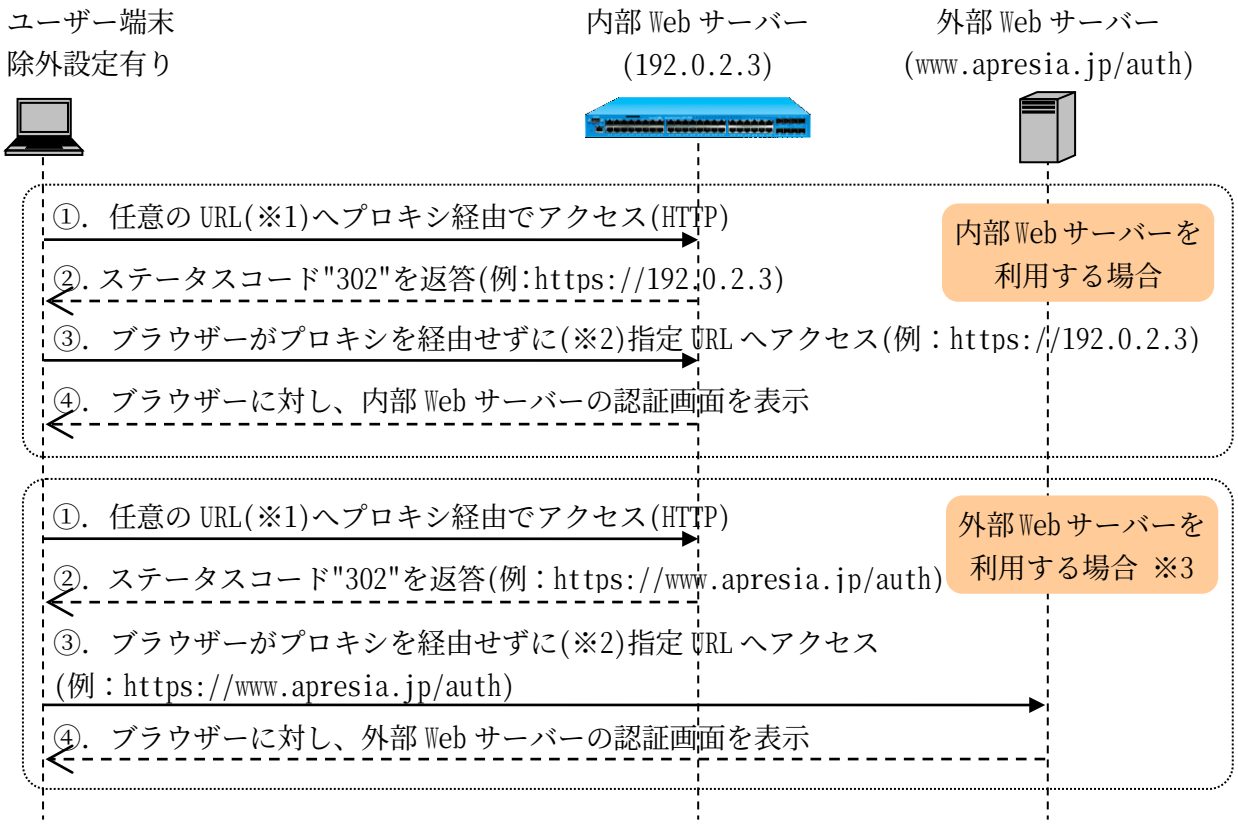


図 3-14 プロキシサーバーがある環境での認証フロー

※1. 任意にアクセスした 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. 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。

※3. 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。

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。

ユーザー端末が HTTPS プロトコルを使用した場合にリダイレクトするには、web-authentication redirect https コマンドの設定が必要です。

3.11.2.2 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。

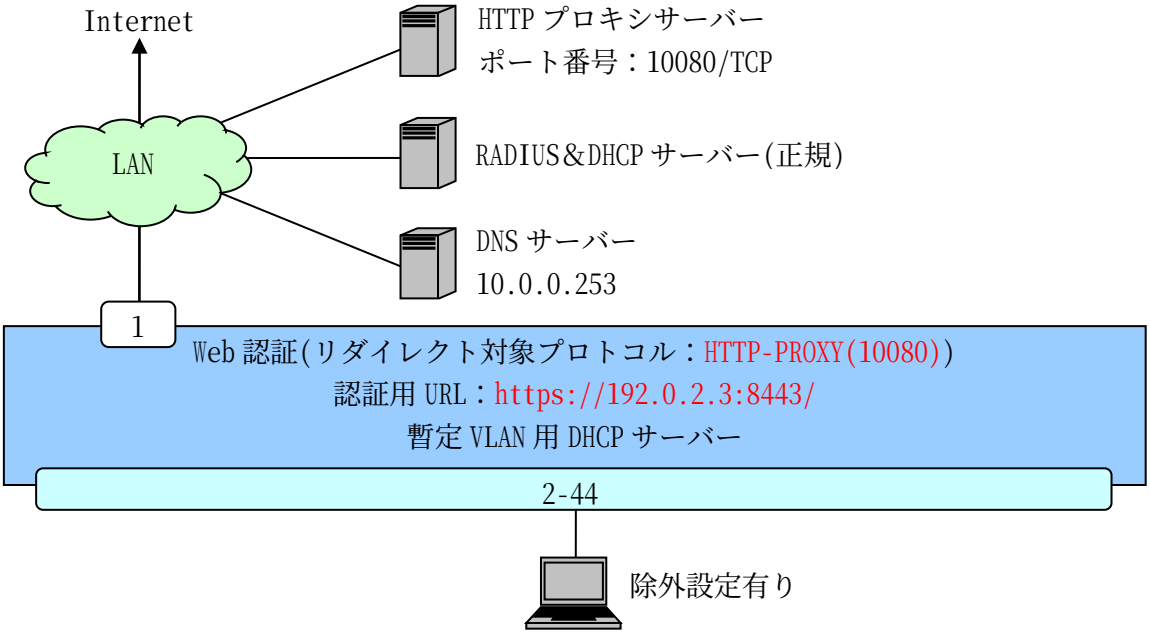


図 3-15 認証ページリダイレクト構成例(プロキシ環境)

図 3-15 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などの設定は省略しています)。

```
(config)# packet-filter2
(config-filter)# 1 1 assign port 1/2-44
(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://192.0.2.3:8443/
                ・・・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 192.0.2.3
(config-a-def)# web-authentication https-port 8443
```

・・・認証 URL(https://192.0.2.3:8443/) (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 30
(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 30 秒)

※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に
合わせて適正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。

3.11.3 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。

ただし、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。

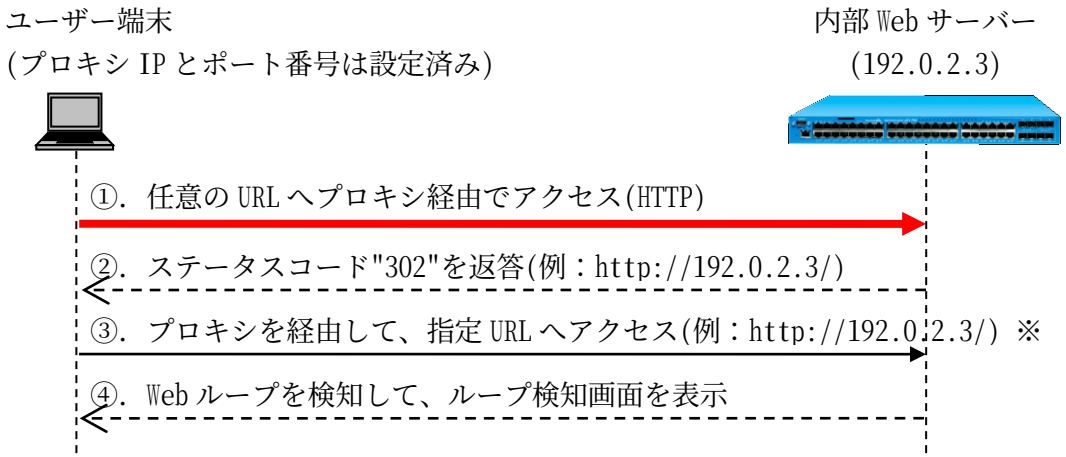


図 3-16 HTTP プロキシ使用時の Web ループ検知

※ 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 3-17 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。

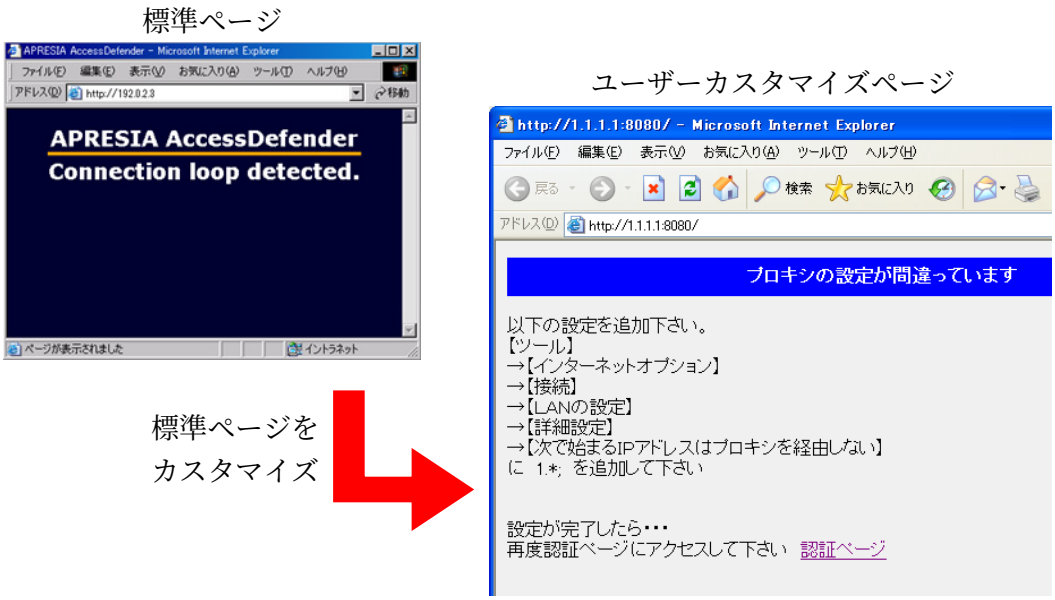


図 3-18 Web ループ検知画面のカスタマイズ

3.12 スヌーピングプロキシ機能による認証ページの強制表示

HTTP プロキシ環境下で認証ページを表示させるためには、3.11 認証ページのリダイレクト機能のほかにスヌーピングプロキシ機能を使用することが可能です。

本機能は、認証端末が指定したプロキシポート番号を経由して任意の Web ページを参照したとき、強制的に認証 Web ページを表示させる機能です。リダイレクトは行わず装置の認証 Web ページを返します。

プロキシリダイレクト機能のように、Web ブラウザーのプロキシ設定で、内部認証 Web ページの URL を例外指定する必要はありません。

3.12.1 認証フロー

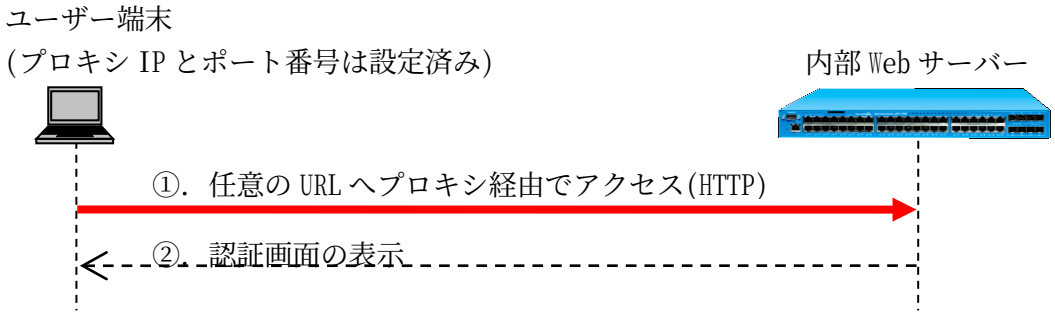


図 3-19 スヌーピングプロキシ機能の認証ページ強制表示フロー

APRESIA 側の認証機能の設定例

```
(config-a-def)# web-authentication snooping proxy-port 10080
```

認証端末が HTTPS プロトコルを使用した場合、認証ページは表示されません。

外部認証 Web ページを表示させることはできません。

リダイレクト先 URL の設定は不要です。

本機能と web-authentication redirect proxy-port コマンドは同時に設定できません。

web-authentication redirect proxy-port コマンド設定済みのポート指定による上書き設定はできません。

認証成功後は認証 Web ページを表示させることはできません。ログアウトなどで Web 認証画面を表示させる場合は、認証 Web サーバーの IP アドレスをブラウザーのプロキシ例外に設定し、プロキシポートから認証 Web サーバーの IP アドレスにアクセスしてください。

3.13 DHCP Snooping の固定 IP アドレス端末接続

DHCP Snooping 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、以下のいずれかの方法により対応可能です。

- IP アドレスを指定して許可する場合　--> static-entry 設定
- MAC アドレスを指定して許可する場合　--> 認証バイパス設定

以下にそれぞれの設定例を示します。

3.13.1 static-entry 設定による方法

ポート 1/1 に 192.168.1.10 の固定 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 1/1 192.168.1.10
```

LAG ID：1 に 192.168.1.20 の固定 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 lag 1 192.168.1.20
```

各インターフェースで登録可能な最大スタティックエントリー数は(最大認証端末数－ダイナミックエントリー数)です。

3.13.2 認証バイパス設定による方法

ポート：1/1 に MAC アドレス：00:00:00:00:00:01 の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 1/1
(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おいて、条件に IP アドレスを指定しても 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。

認証バイパス機能による MAC アドレス指定を行う場合、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。

3.14 TTL フィルター

本機能を有効にすることで、Web 認証において、指定した TTL(Time To Live)値の IP パケットのみ認証可能となります。これにより、ネットワークの距離に応じて接続を制限することができます。TTL フィルターは最大 8 個まで指定可能です。

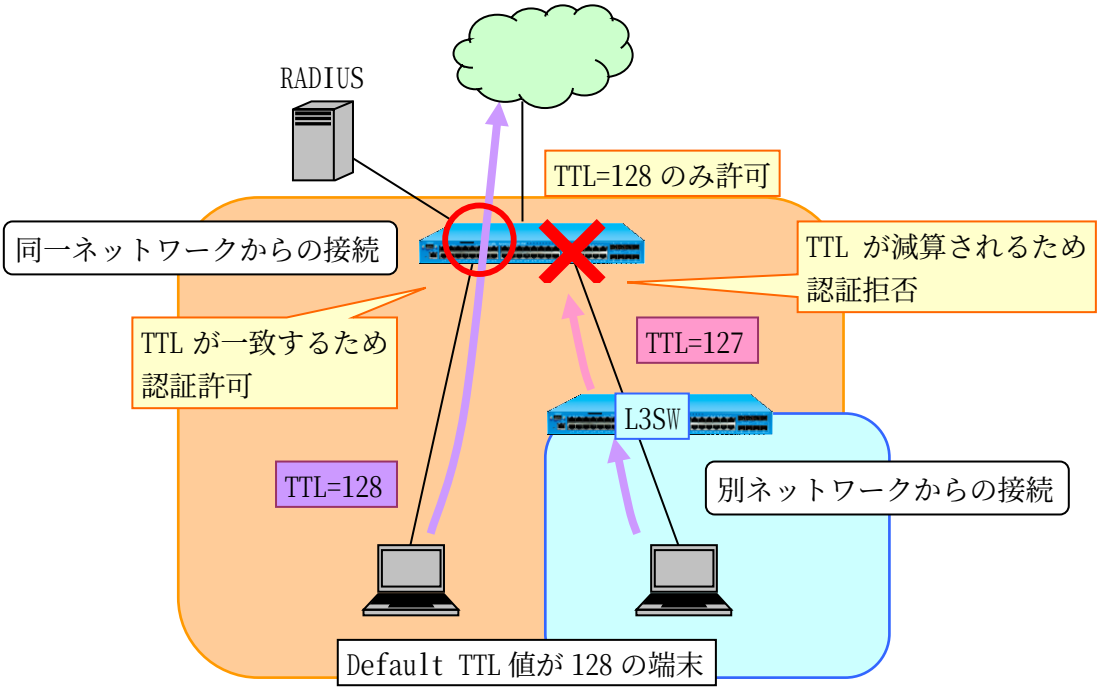


図 3-20 TTL フィルター

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> <*INTERFACE*>
INTERFACE = (port <PORTRANGE>) | (lag <LAGRANGE>) | (mlag <MLAGRANGE>)
・・・TTL　　IP ヘッダの TTL 値 <1-255>
・・・PORTRANGE　　ポート番号 (複数指定可能)
・・・LAGRANGE　　LAG ID <1-32> (複数指定可能)
・・・MLAGRANGE　　ドメイン名/MLAG ID <1-64> (複数指定可能)

TTL フィルター機能を使用したときの認証動作を図 3-23 に示します。

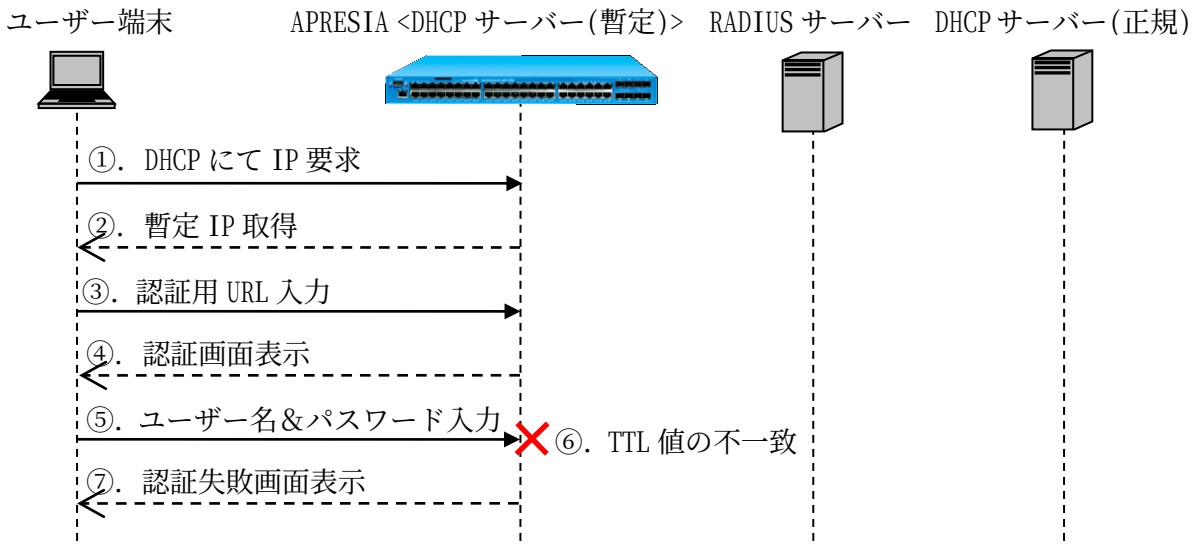


図 3-21 TTL 値不一致時の認証フロー

3.15 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(Time To Live)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自動的にログアウトされ未認証状態となります。

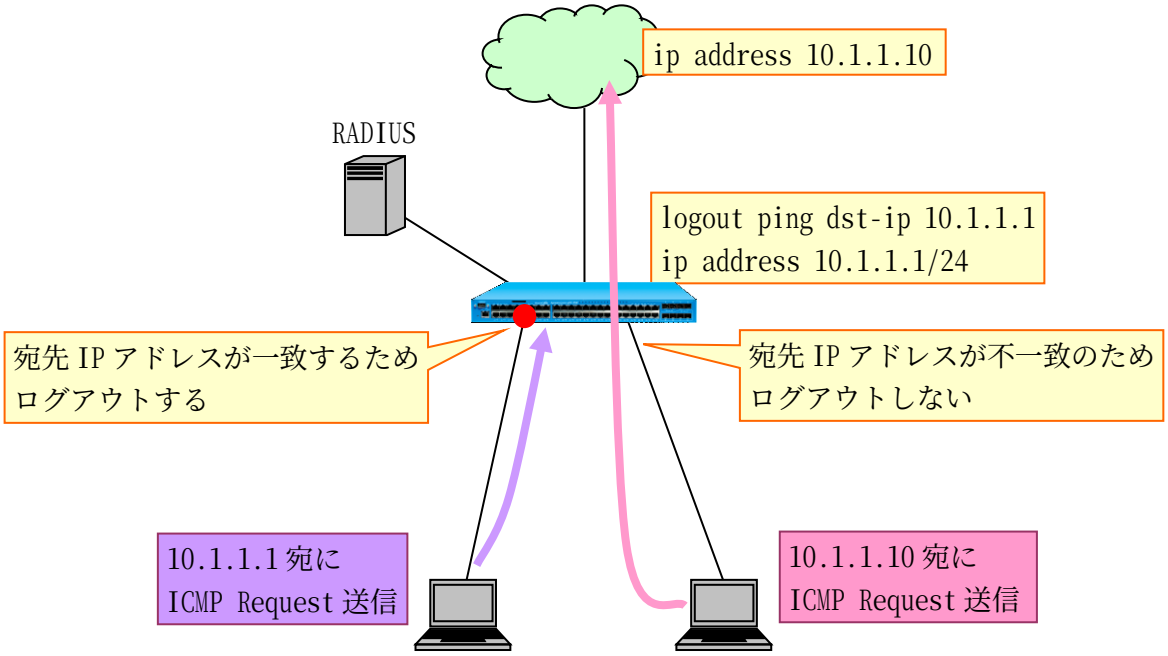


図 3-22 宛先 IP アドレス一致による PING ログアウト

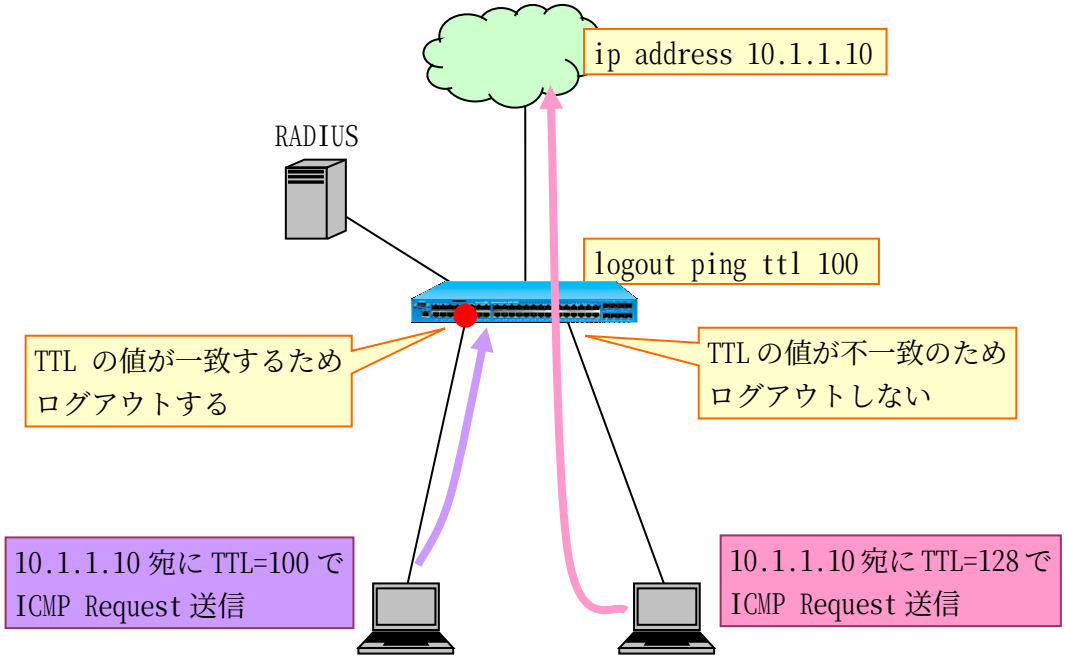


図 3-23 TTL 値一致による PING ログアウト

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 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 コマンドと 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。

3.16 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 が動的に割当たることで DHCP 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 3-26 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。

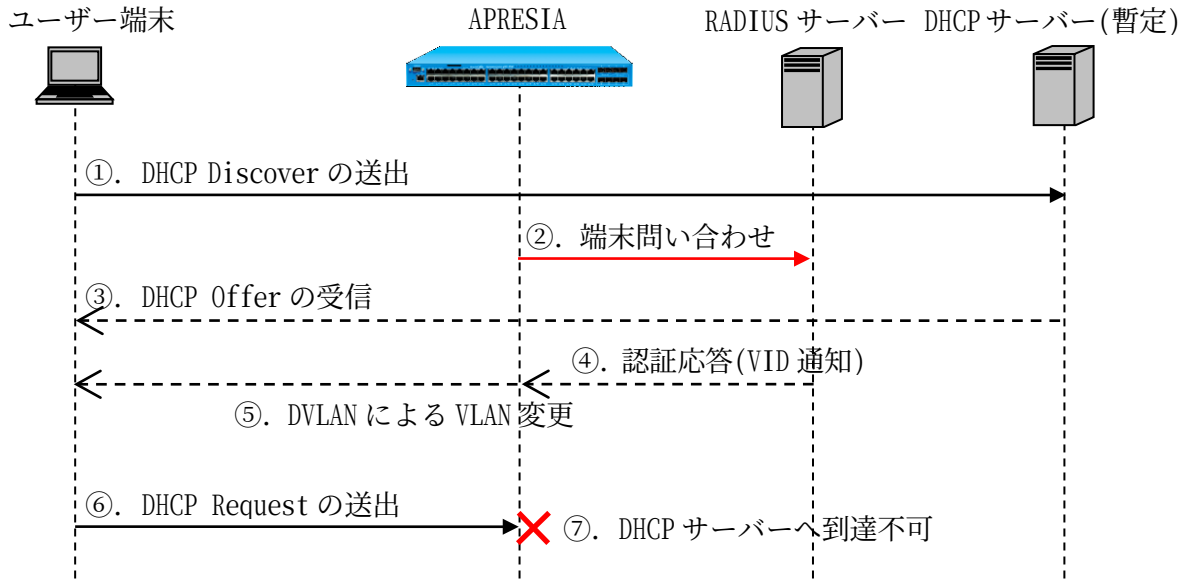


図 3-24 DHCP パケットを MAC 認証の対象とする場合のフロー

3.17 認証開始時の EAP-Request/EAP-Identity の抑制

サプリカントに対する EAP-Request/EAP-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/EAP-Identity を送信しません。

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

(config-a-def)# dot1x <*INTERFACE*> timeout tx-period <SECS>
INTERFACE = (port <PORTRANGE>) | (lag <LAGRANGE>) | (mlag <MLAGRANGE>)
・・・PORTRANGE　　ポート番号（複数指定可能）
・・・LAGRANGE　　LAG ID <1-32>（複数指定可能）
・・・MLAGRANGE　　ドメイン名/MLAG ID <1-64>（複数指定可能）
・・・SECS　　送信間隔 <0，5-65535(秒)>

図 3-27 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、本コマンドにて送信間隔に 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-Request/EAP-Identity)を送信しません。

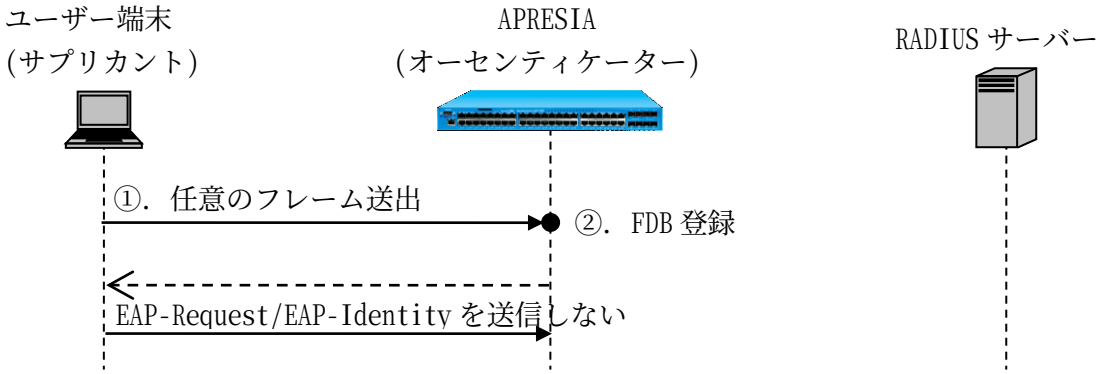


図 3-25 認証開始時の EAP-Request/EAP-Identity の抑制

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

3.18 認証失敗時のステータス保持時間の変更

802.1X では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 秒間そのサプ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、不正な端末が認証失敗を繰り返すことによる負荷を軽減させています。本機能を設定することで、ステータス保持時間の変更が可能です。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 <INTERFACE> timeout quiet-period <SECS>
INTERFACE = (port <PORTRANGE>) | (lag <LAGRANGE>) | (mlag <MLAGRANGE>)
                ・・・PORTRANGE          ポート番号(複数指定可能)
                ・・・LAGRANGE           LAG ID <1-32> (複数指定可能)
                ・・・MLAGRANGE          ドメイン名/MLAG ID <1-64> (複数指定可能)
                ・・・SECS               ステータス保持時間 <0, 5-65535(秒)>
```

図 3-28 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、サプリカントからの EAPOL-Start に応答せず、認証を開始しません。その間、サプリカントに対する APRESIA からの EAP-Request/EAP-Identity も送信されません。

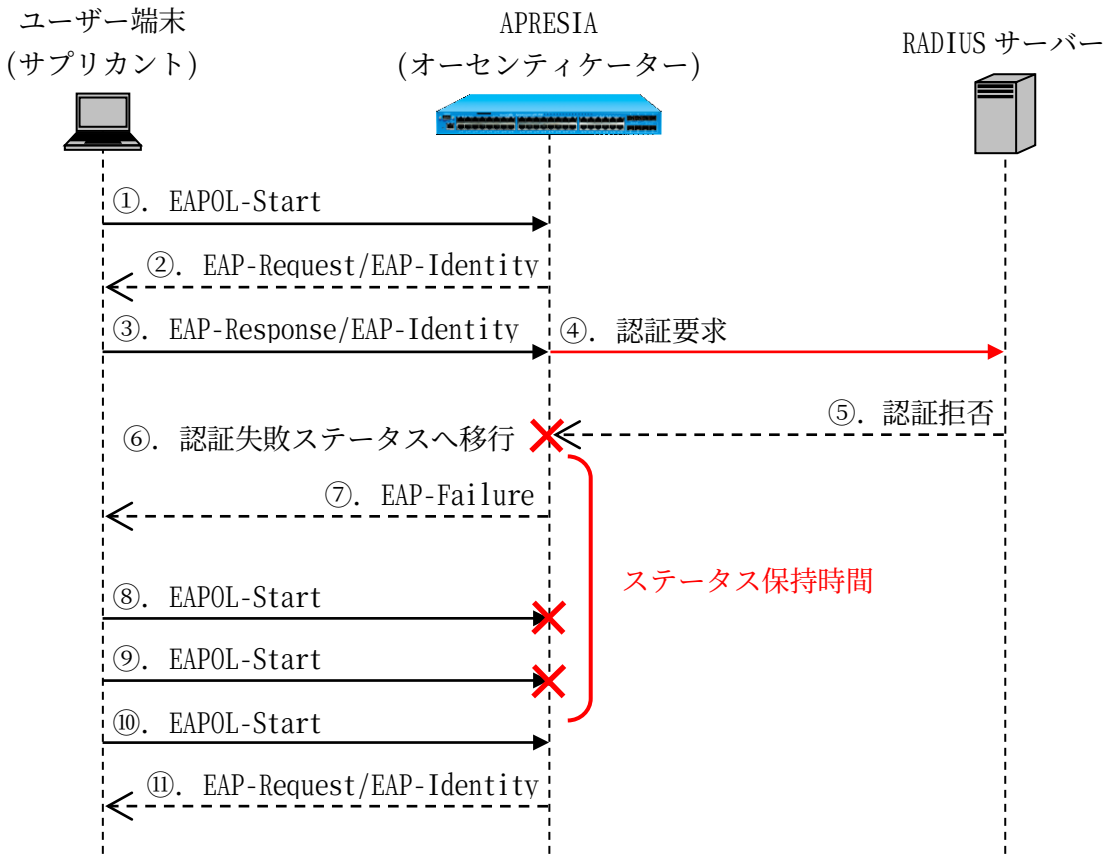


図 3-26 認証失敗ステータス保持

3.19 Web/MAC 認証(AND)の MAC 認証属性

Web/MAC 認証(AND)は認証順を変更することで、MAC 認証成功時の属性値を適用させることができます。認証順を変更した場合、Web ブラウザーを使用したユーザー認証後に、MAC アドレスによる認証を行います。Web によるユーザー認証が成功した場合のみ、MAC アドレスによる認証を実行します。どちらの認証にも成功した場合のみ通信ができます。

どちらの認証にも成功した場合、RADIUS サーバーから通知された Web 認証成功時の属性情報は無視し、MAC 認証成功時の属性情報をもとに動的 VLAN ID、クラス ID を割り当てます。

Web/MAC 認証(AND)の MAC 認証属性への変更コマンドは以下となります。
MAC 認証、Web 認証の認証順に戻す場合は、設定を削除してください。

```
(config-a-def)# web-authentication mac-authentication-attribute mac
```

MAC 認証属性へ変更した場合における Web/MAC 認証(AND)の認証フローを図 3-29 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。
未認証端末のパケット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 パケット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、ユーザー問い合わせ(Web 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、該当ユーザーが存在するときは認証成功を通達します。認証に成功した場合のみ APRESIA はユーザー端末の MAC アドレスで RADIUS サーバーに対して端末問い合わせ(MAC 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、該当ユーザー端末が存在するときは認証成功を通達します。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。

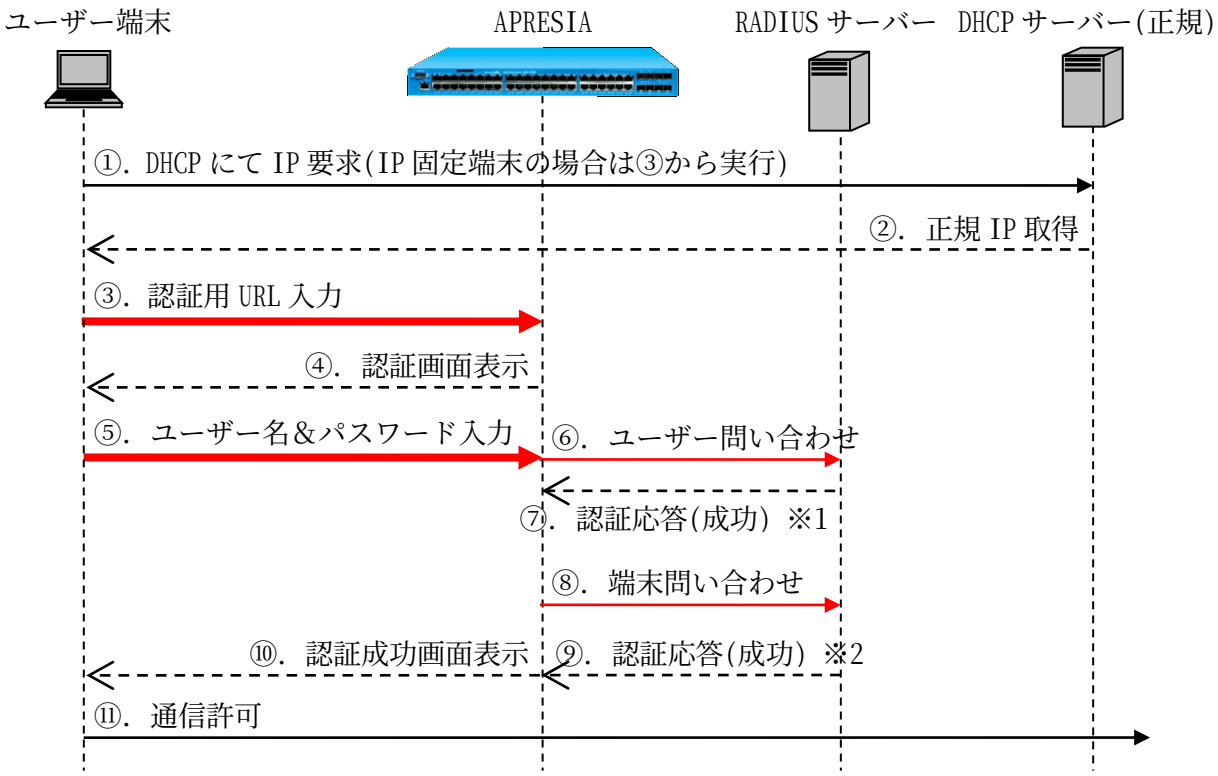


図 3-27 Web/MAC 認証(AND)の MAC 認証属性フロー

※1. RADIUS サーバーへ Web 認証の属性情報が登録されている場合でも、MAC 認証に先立ち成功した Web 認証の属性値は割り当てられません。

※2. RADIUS サーバーへ MAC 認証の属性情報が登録されている場合、該当する属性値が割り当てられます(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)。

認証端末の MAC 認証と Web 認証の両モードにおいて、認証が成功した場合のみ通信可能となります。

3.20 ローミング機能

本機能を有効にすることで、リンクダウンによって切り替わる認証済みの端末の通信インターフェース(通信ポート、LAG、または MLAG の全メンバーポート)を変更することができます。

ローミング機能の設定コマンドは以下となります。

(config-a-def)# roaming (port <PORTRANGE>) | (lag <LAGRANGE>) | (mlag <MLAGRANGE>) enable

・・・PORTRANGE　　ポート番号（複数指定可能）
・・・LAGRANGE　　LAG ID <1-32>（複数指定可能）
・・・MLAGRANGE　　ドメイン名/MLAG ID <1-64>（複数指定可能）

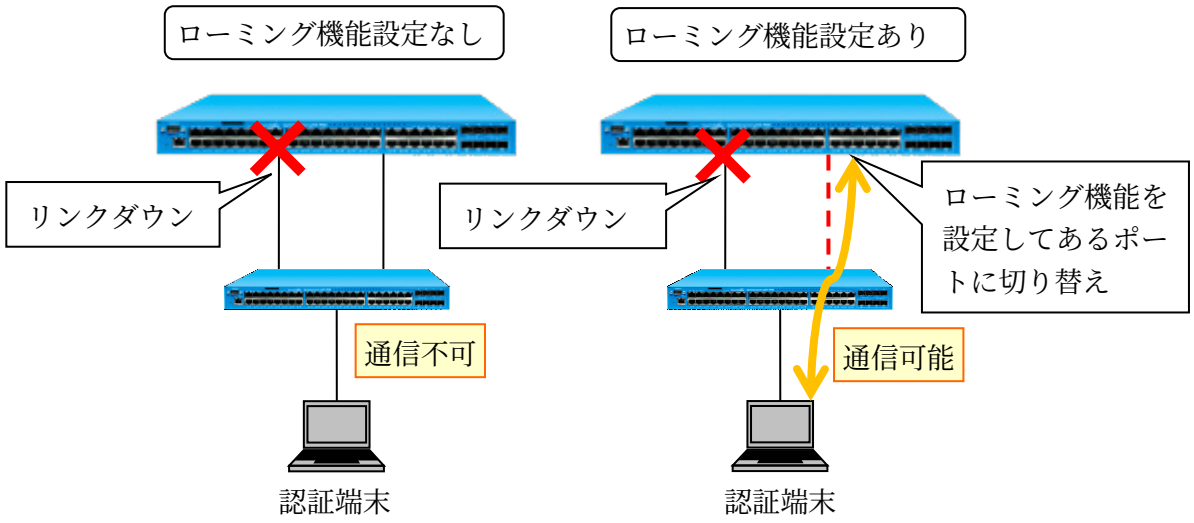


図 3-28 ローミング機能(通信ポート)の切り替え例

ローミングは、同一装置内の roaming port enable コマンド、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。

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 disable コマンドを設定してください。

ローミングを行って接続ポートを変更しても、show access-defender client コマンド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)

ローミングポートの設定を変更しても変更以前にログインした端末はログアウトしません。設定変更前の設定状態でログイン状態を保持します。設定変更後にログインした端末は変更後の設定が反映されます。

ローミング機能が有効なポートで端末の認証が成功し、その後 VLAN が変更された場合、ローミング機能が有効なすべてのポートにおいて、変更後の VLAN のトラフィックが中継されます。

認証端末が存在しないローミングポートの認証を無効にした場合、他のローミングポートで認証を行った端末がログアウトするまで、動的な VLAN、及びクラス ID の変更は解除されません。動的な VLAN、及びクラス ID の変更を解除するためには、再起動、または一旦認証を無効にしてください。

3.21 SSL プロトコルの脆弱性対応

認証用 Web サーバーで使用する SSL プロトコルのバージョン 2(SSLv2)、及びバージョン 3(SSLv3)は脆弱性の問題が確認されているため、Ver8.25.01 以降のファームウェアからはデフォルトの設定では利用不可となっています。利用する場合には SSLv2、SSLv3 を有効にする必要があります。

SSLv2、及び SSLv3 を有効にする設定コマンドは以下となります。

```
(config-a-def)# web-authentication sslv2 enable
(config-a-def)# web-authentication sslv3 enable
```

SSLv2 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

SSLv2 は中間証明書が利用できません。中間証明書を利用する場合は、TLS(Transport Layer Security)を利用することを推奨します。

SSLv2 を使用する場合、SHA-1、または SHA-2 で作成した証明書は使用できません。

SSLv3 は脆弱性が確認されているため、本コマンドの設定は推奨しません。

3.22 HTTP/HTTPS セッションタイムアウト時間の設定

Web 認証において、HTTP/HTTPS クライアント用に予約されたセッション数は制限されているため、すべてのセッションが占有されている場合、新しいクライアントは Web 認証を開始できません。

本機能は Web 認証で使用する HTTP/HTTPS セッションにおける、クライアントのタイムアウト時間を設定し、一定時間応答がないセッションを自動的に切断して解放することで、新しいクライアントが Web 認証を開始できるようにします。

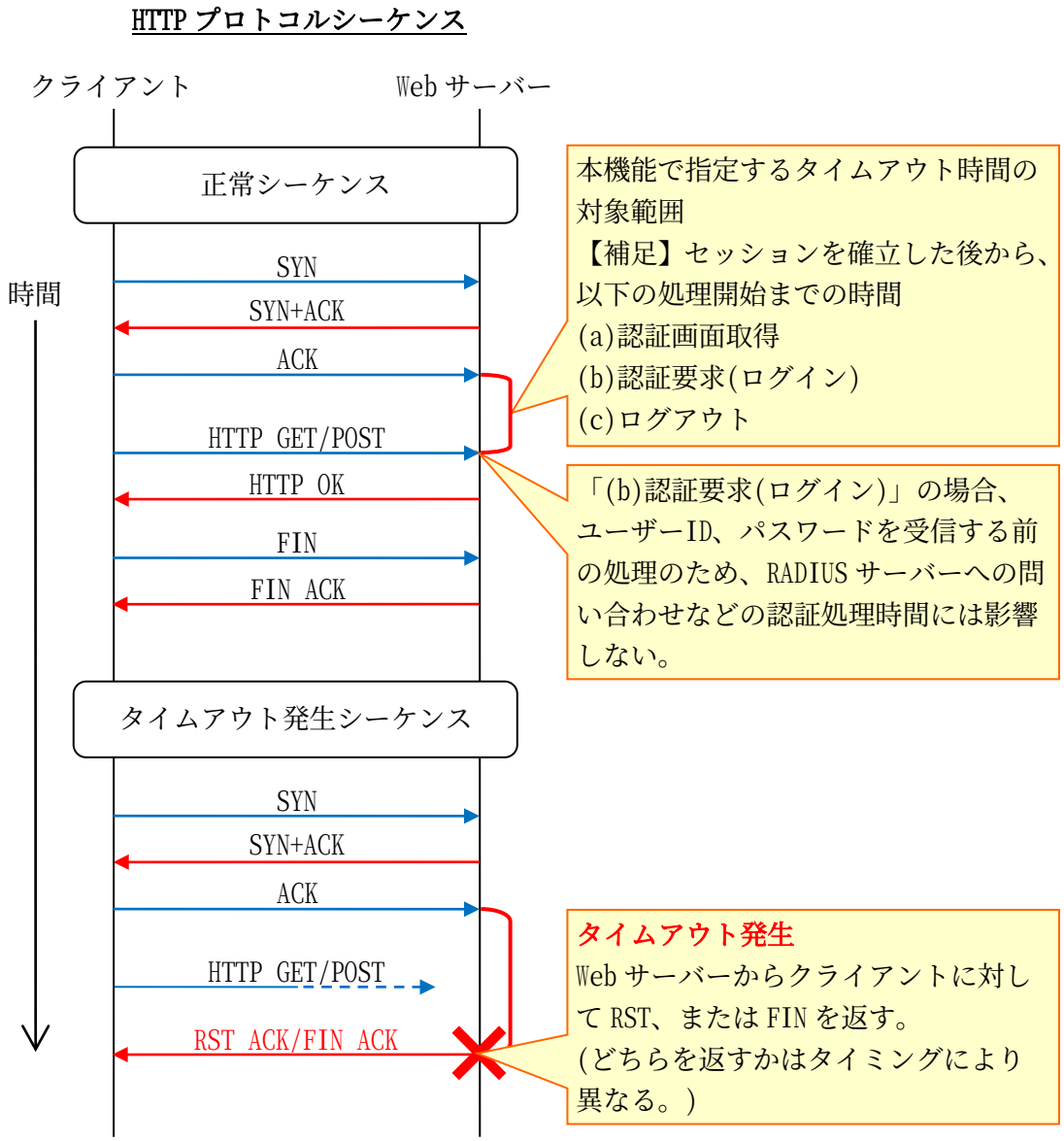


図 3-29 HTTP プロトコルシーケンスと HTTP/HTTPS セッションタイムアウト動作

HTTP/HTTPS セッションタイムアウト時間を設定するコマンドは以下となります。

(config-a-def)# web-authentication http-session-timeout <SECONDS>
・・・SECONDS　　HTTP/HTTPS セッションタイムアウト時間 <1-60(秒)>

3.23 認証端末のユーザーID(MAC アドレス)による MAC 認証

MAC 認証のパスワードは、mac-authentication password コマンドで固定値を設定していますが、本機能により MAC 認証のパスワードを認証端末のユーザーID と同じ文字列にすることで認証端末ごとにパスワードを設定することが可能となります。

本機能による MAC 認証の場合、認証方法によって、RADIUS サーバー、またはローカルデータベースに MAC 認証のパスワードとしてユーザーID と同じ文字列を登録しておく必要があります。

MAC 認証のユーザーID は、16 進文字列(英小文字)、区切り文字無し 12 文字の MAC アドレスです。

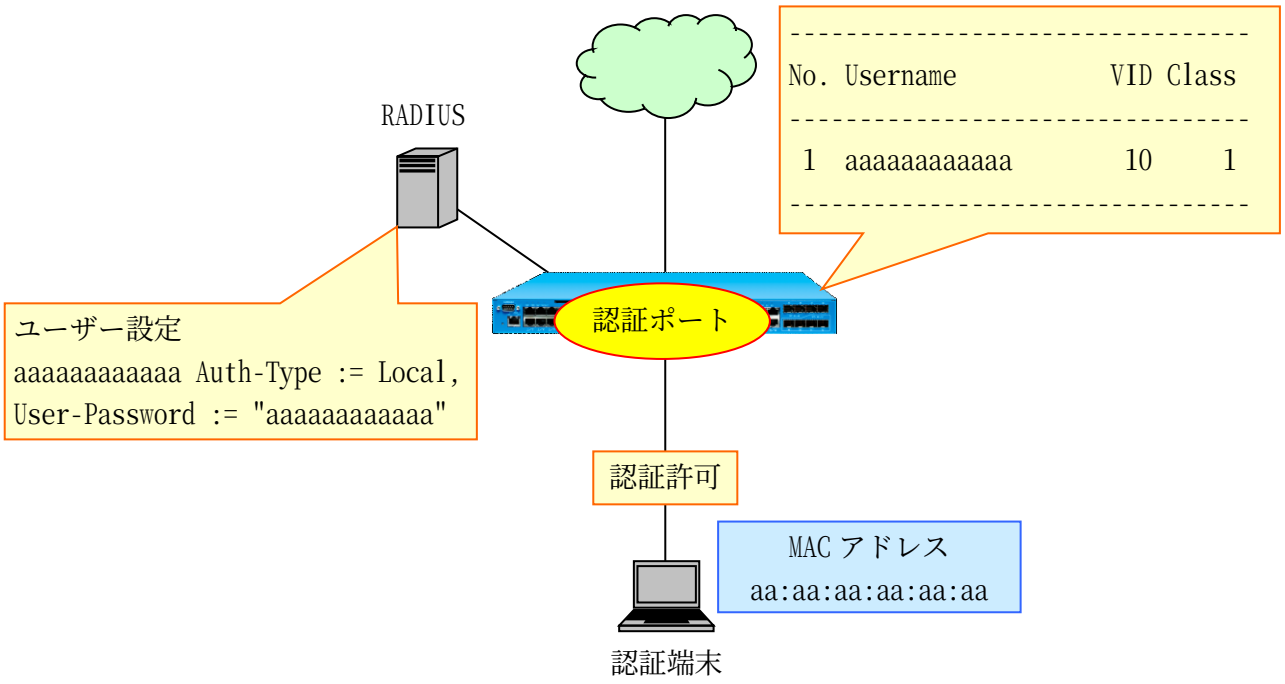


図 3-30 認証端末のユーザーID(MAC アドレス)による MAC 認証

MAC 認証のパスワードを認証端末のユーザーID と同じ文字列にする設定コマンドは以下となります。

```
(config-a-def)# mac-authentication password-mac-address
```

本コマンドは、MAC 認証単体のみ有効となります(Web/MAC 認証(AND)、802.1X/MAC 認証には影響しません)。本コマンド設定時に、Web/MAC 認証(AND)、または 802.1X/MAC 認証と併用する場合、aaa authentication web コマンド、及び aaa authentication dot1x コマンドで指定する RADIUS サーバー、もしくはローカルデータベースは aaa authentication mac コマンドで指定する RADIUS サーバー、もしくはローカルデータベースと同じものを指定しないでください。

3.24 DHCP Snooping のエージングログアウト機能

DHCP Snooping でも他の認証機能と同様にエージングログアウト機能をサポートしています。

DHCP Snooping のエージングログアウト時間は、以下のコマンドの"dhcp-snooping"オプションを指定して設定します。

(config-a-def)# logout aging-time <SECONDS> [<MINUTES> [<HOURS> [<DAYS>]]] [web | gateway | mac | dot1x | dhcp-snooping]

・・・SECONDS　　エージング間隔 <0,10-86400(秒)>
・・・MINUTES　　エージング間隔 <0-59(分)>
・・・HOURS　　エージング間隔 <0-23(時間)>
・・・DAYS　　エージング間隔 <0-31(日)>

設定したエージングログアウト時間を経過した無通信状態の認証済み端末を自動的にログアウトさせます。無通信監視対象となるフレーム(パケット)を表 3-11 表 に示します。

表 3-11 無通信監視対象フレーム(パケット)

認証方式	無通信監視対象フレーム(パケット)
DHCP Snooping	① Sender IP が認証端末の ARP パケット ② 送信元 IP が認証端末の IP パケット
DHCP Snooping と Web 認証/MAC 認証/802.1X の いずれかを併用	① DHCP Snooping で登録された場合 Sender IP が認証端末の ARP パケット ② Web/MAC/802.1X で認証された場合 送信元 MAC アドレスが認証端末である IP パケット
DHCP Snooping と Web/802.1X 認証(AND)を 併用	DHCP Snooping と Web/802.1X 認証(AND)が独立して 以下のパケットを監視 ① DHCP Snooping で登録された場合 Sender IP が認証端末の ARP パケット ② Web/802.1X 認証(AND)で認証された場合 送信元 MAC アドレスが認証端末である IP パケット

DHCP Snooping において、エージングログアウト時間よりも最大リース時間が長い場合、エージングログアウト後はリース満了となるまで通信ができなくなります。

show access-defender client コマンドにおける無通信時間のリセットタイミングを表 3-12 に示します。

表 3-12 無通信時間のリセットタイミング

認証済み端末の 認証種別 (認証種別コード:Codes)	リセットタイミングの条件							
	無通信監視対象パケット受信時 ※1	logout aging-time コマンドの設定変更						その他
		web	gateway	mac	802.1X	dhcp-snooping	認証方式指定なし	
Web 認証(W)	○	○	-	-	-	-	○	

認証済み端末の認証種別(認証種別コード:Codes)	リセットタイミングの条件							
	無通信監視対象パケット受信時 ※1	logout aging-time コマンドの設定変更						その他
		web	gate way	mac	802.1X	dhcp-snooping	認証方式指定なし	
ゲートウェイ認証(G)	○	-	○	-	-	-	○	
Mac 認証(M)	○	-	-	○	-	-	○	
802.1X(X)	○	-	-	-	○	-	○	
DHCP Snooping(D)	○	-	-	-	-	○	○	
Web 認証と DHCP Snooping の併用(WD)	○	○	-	-	-	○	○	※2 ※3
Mac 認証と DHCP Snooping の併用(MD)	○	-	-	○	-	○	○	※2
802.1X と DHCP Snooping の併用(XD)	○	-	-	-	○	○	○	※2 ※3

○:無通信時間がリセットされる。 -:無通信時間がリセットされない。

※1. 認証済みの端末において、パケットフィルター2 で通信を許可されたパケットを対象とします。

※2. 一方の認証方式でログイン、またはログアウトした場合、無通信を監視する対象パケットが変わるため、無通信時間がリセットされます。

※3. DHCP Snooping と Web/802.1X 認証(AND)を併用している場合、それぞれの認証方式で独自に無通信監視を行うため、一方の認証方式の無通信時間がリセットされても、もう一方の認証方式の無通信時間はリセットされません。

DHCP Snooping と Web/802.1X 認証(AND)を併用している場合、show access-defender client コマンドにおいて、Web 認証と 802.1X が同時にログインしている状態のときは、DHCP Snooping の無通信時間は表示されません。

3.25 MAC 認証有効ポートにおける認証バイパス対象フレームの認証回避

本機能を有効にすることで、MAC 認証有効ポートにおいて、自局 IP アドレス宛などの CPU 宛てのフレーム、及びソフトウェア中継されるフレームのうち、認証バイパスの対象フレームの場合は MAC 認証を行わないようにすることができます。

MAC 認証有効ポートにおいて、認証バイパスの対象フレームの場合は MAC 認証を行わないようにする機能を有効にする設定コマンドは以下となります。

```
(config)# mac-authentication bypass-frame-check enable
```

MAC 認証ポートにおいて、以下の条件の場合、本コマンドを設定しても認証バイパスの対象フレームの判定ができないため、未サポートです。

(1) VLAN 設定

- **ignore-tag 設定時**
- **tag-type 設定時**

(2) パケットフィルター2 設定

- **condition c-vid 設定時**
- **action routing 設定時**

(3) 受信フレーム

- **ダブルタグフレーム受信時**

3.26 トランクポートでのタグ付き EAP フレームによる 802.1X

本機能を有効にすることで、802.1X における VLAN タグ付き EAP フレームによる認証が可能となります。これにより、トランクポートを 802.1X の認証ポートとして使用することができます。本機能を有効にした場合でも、VLAN タグなし EAP フレームによる 802.1X は可能です。

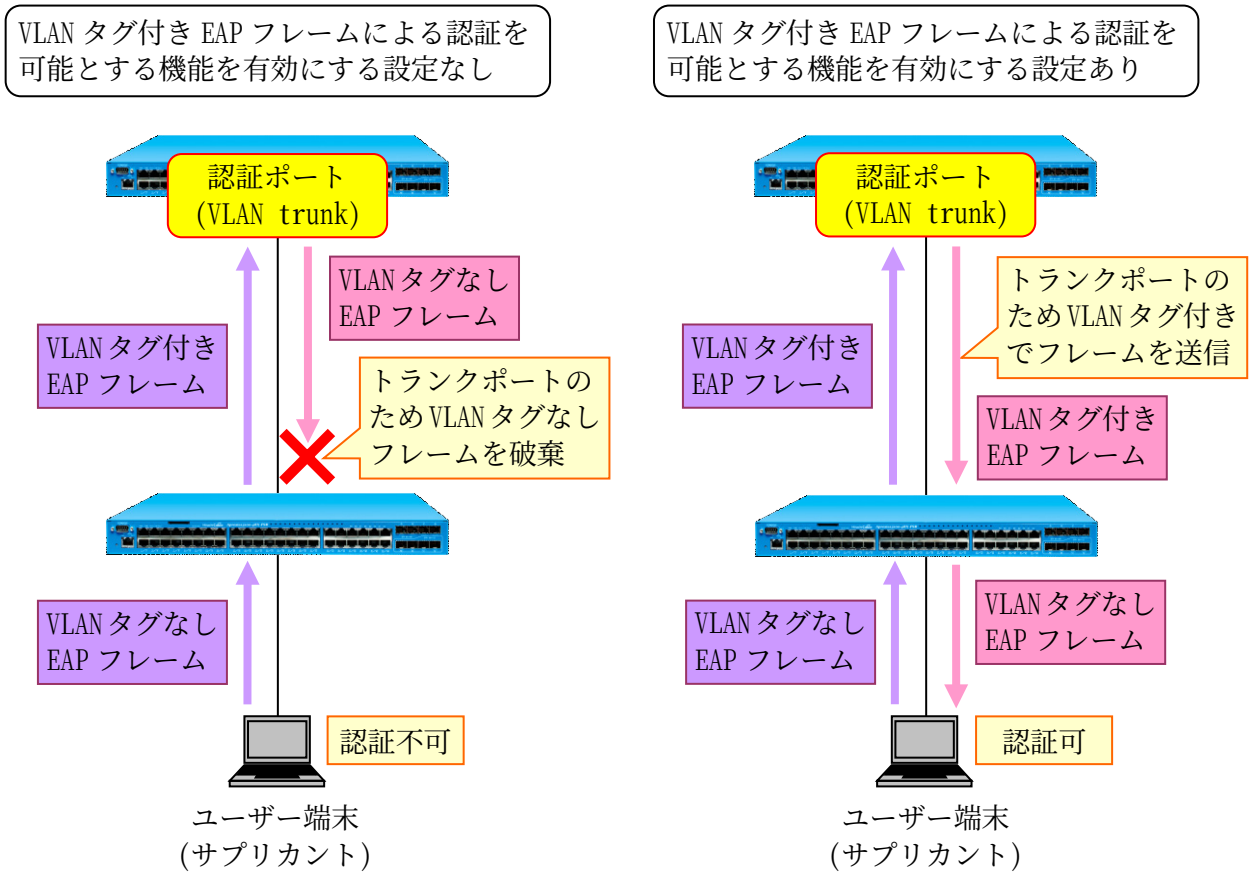


図 3-31 トランクポートでのタグ付き EAP フレームによる 802.1X

802.1X の VLAN タグ付き EAP フレームによる認証を可能とする機能を有効にする設定コマンドは以下となります。

```
(config-a-def)# dot1x tagged-eap-frame enable
```

各設定条件における 802.1X の動作を表 3-13 に示します。

表 3-13 各設定条件における 802.1X の動作

ポートの VLAN モード	本機能の設定	EAP フレーム		動的 VLAN	802.1X 動作
		受信	送信		
アクセスポート	○	VLAN タグ無し	VLAN タグ無し	○	動的 VLAN(アクセスポート)でログイン
				-	ポートの VLAN でログイン
		VLAN タグ設定済 VLAN	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ未設定 VLAN	送信しない	-	認証不可※1※2

ポートの VLAN モード	本機能の設定	EAP フレーム		動的 VLAN	802.1X 動作
		受信	送信		
アクセスポート	-	VLAN タグ無し	VLAN タグ無し	○	動的 VLAN(アクセスポート)でログイン
				-	ポートの VLAN でログイン
		VLAN タグ設定済 VLAN	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ未設定 VLAN	VLAN タグ無し	-	認証不可※1※2
トランクポート(ネイティブ VLAN 設定あり)	○	VLAN タグ無し	VLAN タグ無し	○	動的 VLAN(アクセスポート)でログイン
				-	ネイティブ VLAN でログイン
		VLAN タグ設定済 VLAN(ネイティブ VLAN)	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ設定済 VLAN(ネイティブ VLAN 以外)	VLAN タグ受信と同じ VLAN	○	動的 VLAN(アクセスポート)でログイン※2
				-	VLAN タグの VLAN でログイン
		VLAN タグ未設定 VLAN	送信しない	-	認証不可※1※2
	-	VLAN タグ無し	VLAN タグ無し	○	動的 VLAN(アクセスポート)でログイン
				-	ネイティブ VLAN でログイン
		VLAN タグ設定済 VLAN(ネイティブ VLAN)	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ設定済 VLAN(ネイティブ VLAN 以外)	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ未設定 VLAN	VLAN タグ無し	-	認証不可※1※2
トランクポート(ネイティブ VLAN 設定なし)	○	VLAN タグ無し	送信しない	-	認証不可※1※2
		VLAN タグ設定済 VLAN	VLAN タグ受信と同じ VLAN	○	動的 VLAN(アクセスポート)でログイン※2
				-	VLAN タグの VLAN でログイン
		VLAN タグ未設定 VLAN	送信しない	-	認証不可※1※2
	-	VLAN タグ無し	VLAN タグ無し	○	動的 VLAN(アクセスポート)でログイン※2
				-	VLAN ID:0 でログイン※2
		VLAN タグ設定済 VLAN	VLAN タグ無し	-	認証不可※1※2
		VLAN タグ未設定 VLAN	VLAN タグ無し	-	認証不可※1※2

○：設定あり　-：設定なし

※1. EAP フレームの送信と受信で整合性が取れないため認証不可

※2. 非サポート

トランクポートで 802.1X でログインした端末が、ログインしたまま当該トランクポートの別 VLAN に移動した場合、show access-defender client コマンドの VID 表示は移動前の VLAN のままとなります。また、移動先の VLAN で再認証に成功してもログイン状態は変わらないため、本事象に変わりはありません。但し、本事象が発生しても移動先の VLAN で通信は可能です。

4 構成例

4.1 Web 認証

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 において統一することで、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、接続が想定されるすべての 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 4-1 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ごとに行い、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値となるため(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、各認証スイッチに設定する DHCP サーバーのリース空間は、認証スイッチごと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 などにしておく必要があります。

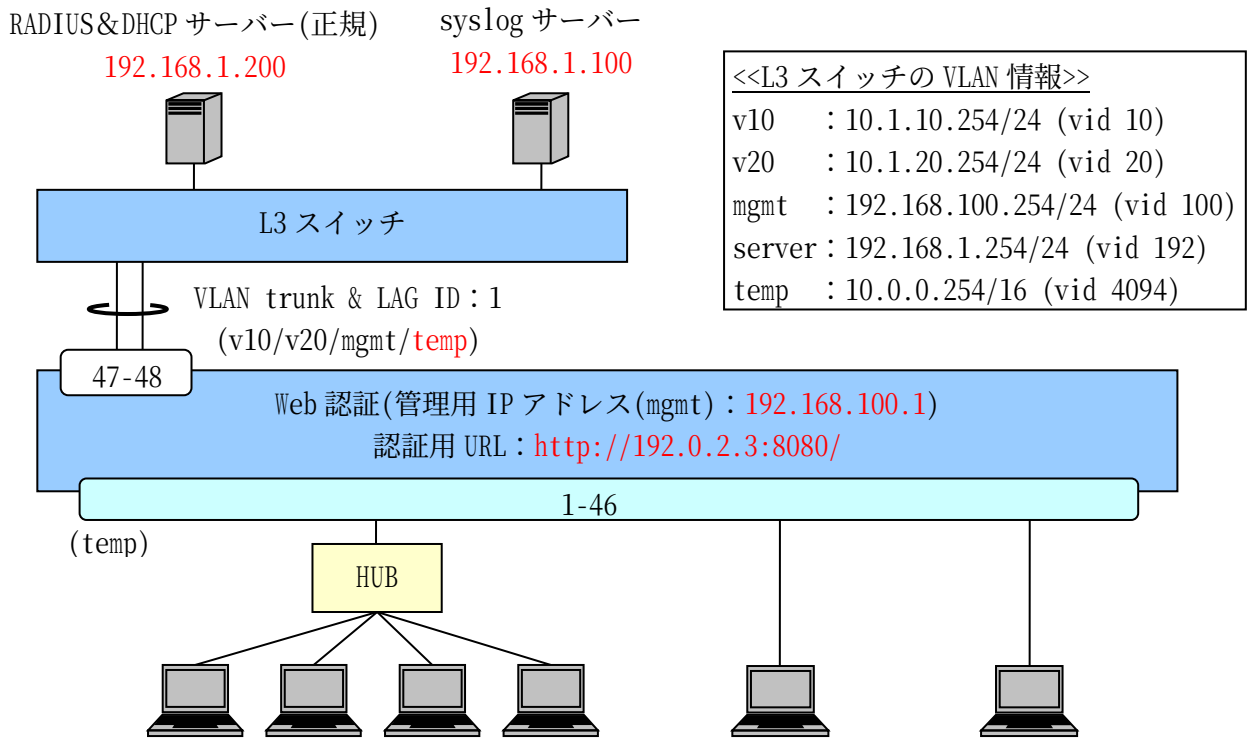


図 4-1 Web 認証構成例

図 4-1 の構成例における認証スイッチの設定例を示します。

```
(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 1/1-46
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
              ・・・パケットフィルター2 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 名を"mgmt"、暫定 VLAN 名を"temp"、
                   動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 4094
              ・・・暫定 VLAN を access ポートとして設定
                   ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
(config-if-lag)# switchport trunk add 10,20,100,4094
(config)# interface port 1/47-48
(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-vlan)# ip address 192.168.100.1/24
(config)# interface vlan 4094
(config-if-vlan)# ip address 10.0.0.1/16
              ・・・管理用 VLAN(mgmt)と暫定 VLAN(temp)の IP 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 IP アドレス重複を避ける
                      必要があります。

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

```
(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)
※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

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

```
(config-a-def)# web-authentication port 1/1-46
```
・・・Web 認証ポート(1/1-46) (必須)

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (必須)
※ すべての APRESIA で統一することが可能です。

```
(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 30
(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 30 秒)
※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に
合わせて適正な値に調整してください。

各ポートを LAG メンバーポートに設定する前に、interface lag コマンドにより設定する LAG インターフェースを作成しておく必要があります。

上位の L3 スイッチには暫定 VLAN の設定が必要です。

4.2 Web 認証(MLAG 併用)

Web 認証の認証インターフェースに MLAG を指定する場合は、当該 MLAG インターフェースを片 MLAG 設定で動作させる必要があります(図 4-2 の MLAG ID：1 のように、片側の MLAG 装置にのみメンバーポートの存在する MLAG インターフェースを認証インターフェースとして使用可能です)。MLAG の用語や動作については、別冊の「MLAG アプリケーションノート」を参照してください。

両方の MLAG 装置にメンバーポートの存在している MLAG インターフェースを、認証インターフェースに指定して下位スイッチと接続する構成は、下位スイッチの分散により認証用 URL の入力時は MLAG の first 装置へ振り分けられ(first 装置より認証画面を表示)、ユーザー名とパスワードの入力時は MLAG の second 装置へ振り分けられると、認証動作が MLAG 装置間を跨いでいることになり、この場合認証シーケンスを完了できないため、使用しないでください。

設定例の説明は 4.1 と同様のため、4.1 を参照してください。

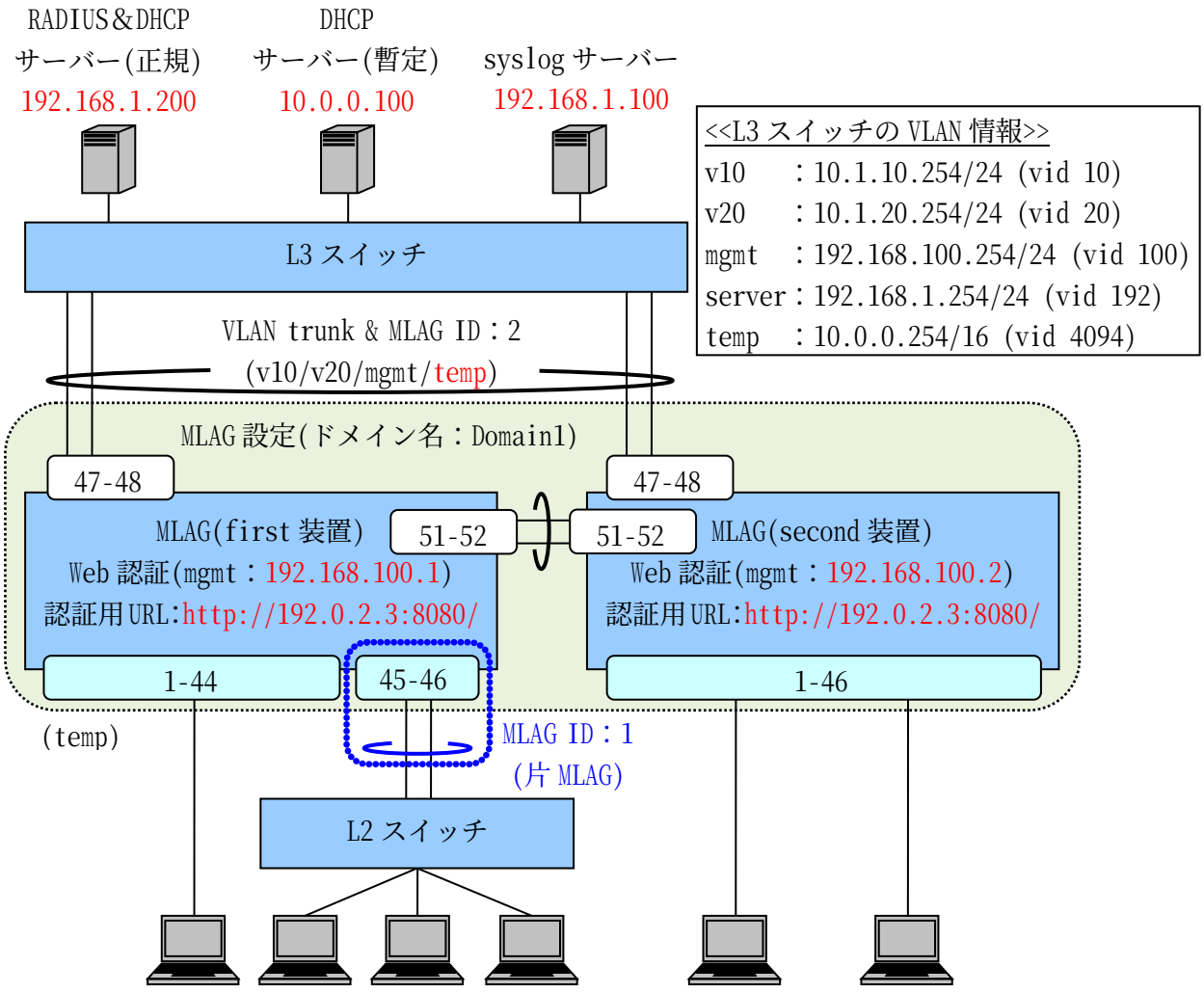


図 4-2 Web 認証構成例(MLAG 併用)

図 4-2 の構成例における認証スイッチの設定例を示します。

<MLAG(first 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 first
(config)# mlag enable
```
・・・MLAG の設定(first 装置)、有効化
※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(config)# packet-filter2
(config-filter)# 2 assign port 1/1-46
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
```
・・・パケットフィルター2 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 名を"mgmt"、暫定 VLAN 名を"temp"、
動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

```
(config)# interface port 1/1-44
(config-if-port)# switchport access vlan 4094
(config)# interface mlag Domain1/1
(config-if-mlag)# switchport access vlan 4094
(config)# interface port 1/45-46
(config-if-port)# mlag Domain1/1
```
・・・暫定 VLAN を access ポートとして設定
※ 認証前のポートは未認証端末同士も通信不可となります。

```
(config)# interface mlag Domain1/2
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100,4094
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```
・・・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-vlan)# ip address 192.168.100.1/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定
※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

```
(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)
※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

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

```
(config-a-def)# web-authentication port 1/1-44
(config-a-def)# web-authentication mlag Domain1/1
```
・・・Web 認証ポート(1/1-44、MLAG ID：1) (必須)

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (必須)
※ すべての APRESIA で統一することが可能です。

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

```
(config)# mlag mac-address-table-update enable
```
・・・MAC アドレス更新機能の有効化
※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
対向装置の FDB 学習の補助を行います。

```
(config)# web-authentication enable
```
・・・Web 認証の有効化 (必須)

<MLAG(second 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 second
(config)# mlag enable
```
・・・MLAG の設定(second 装置)、有効化
※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(config)# packet-filter2
(config-filter)# 2 assign port 1/1-46
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
```
・・・パケットフィルター2 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 名を"mgmt"、暫定 VLAN 名を"temp"、
動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

```
(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 4094
```
・・・暫定 VLAN を access ポートとして設定
※ 認証前のポートは未認証端末同士も通信不可となります。

```
(config)# interface mlag Domain1/1
```
・・・片 MLAG 対向装置への MLAG インターフェースの設定(MLAG ID：1 用)
・・・※ 片 MLAG 設定で動作させる場合でも、両方の MLAG 装置に MLAG
インターフェースを作成する必要があります(メンバーポートは
設定しない)。

```
(config)# interface mlag Domain1/2
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100,4094
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```
・・・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-vlan)# ip address 192.168.100.2/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定
※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

```
(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)
※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

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

```
(config-a-def)# web-authentication port 1/1-46
              ・・・Web 認証ポート(1/1-46) (必須)

(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
              ・・・認証 URL(http://192.0.2.3:8080/) (必須)
                   すべての APRESIA で統一することが可能です。

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

(config)# mlag mac-address-table-update enable
              ・・・MAC アドレス更新機能の有効化
                   ※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
                      対向装置の FDB 学習の補助を行います。

(config)# web-authentication enable
              ・・・Web 認証の有効化 (必須)
```

各ポートを MLAG メンバーポートに設定する前に、interface mlag コマンドにより設定する MLAG インターフェースを作成しておく必要があります。

上位の L3 スイッチには暫定 VLAN の設定が必要です。

MLAG 併用時、first 装置と second 装置で認証結果の同期は行われません。

MLAG 併用時、ローカルデータベースは first 装置と second 装置で一致させるようにしてください。RADIUS サーバーを使用する場合、first 装置と second 装置で同一のサーバーを参照するなど、同一の認証データを使用するようにしてください。

MLAG の動作仕様上、定期的なフラッディングやブロードキャストが発生しない通信環境では、片側の MLAG 装置のみ FDB 登録されるため、以下の動作となる可能性があります。

- **ユニキャスト通信のフラッディングが発生し続ける**
- **端末の接続ポートが移動された場合、通信断が発生する**

これらの動作が問題となる場合は、mlag mac-address-table-update enable コマンドを有効にして下さい。

4.3 MAC 認証

動的 VLAN 変更を有効にする場合、ユーザーごとに VLAN を動的に割当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に設定しておきます。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、接続が想定されるすべての 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。

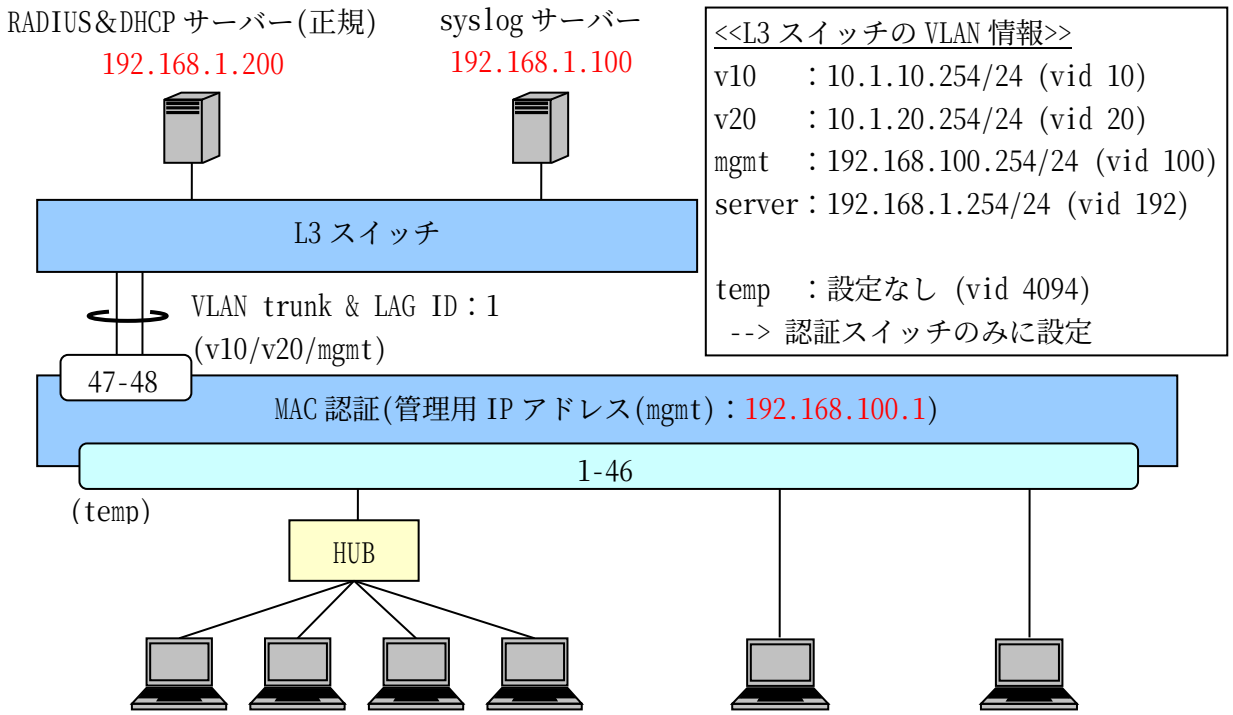


図 4-3 MAC 認証構成例

図 4-3 の構成例における認証スイッチの設定例を示します。

```
(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 名を"mgmt"、暫定 VLAN 名を"temp"、
                    動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)
```

```
(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 4094
              ・・・暫定 VLAN を access ポートとして設定
                   ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
(config-if-lag)# switchport trunk add 10,20,100
(config)# interface port 1/47-48
(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-vlan)# ip address 192.168.100.1/24
              ・・・管理用 VLAN(mgmt)の IP アドレス設定
                   ※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

(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(プライマリー) (必須)
                   ※ INDEX：1 の RADIUS サーバーを MAC 認証のプライマリーとしています。

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
              ・・・最大認証端末(128 台) (必須)
                   ※ 128 台を最大としています。

(config-a-def)# mac-authentication port 1/1-46
              ・・・MAC 認証ポート(1/1-46) (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)
```

MAC 認証のみの場合、暫定 VLAN は認証スイッチ内のみに設定しておきます。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。

4.4 MAC 認証(MLAG 併用)

MAC 認証の認証インターフェースに MLAG を指定する場合は、端末からのパケットのみで認証処理が完了するため、通常の MLAG インターフェースで動作させることができます(図 4-4 の MLAG ID：1 のように、両側の MLAG 装置にメンバーポートの存在する MLAG インターフェースを認証インターフェースとして使用可能です)。

1 台の端末は、MLAG インターフェース配下に接続する L2 スイッチの分散により、両側の MLAG 装置で認証されることになります。

設定例の説明は 4.3 と同様のため、4.3 を参照してください。

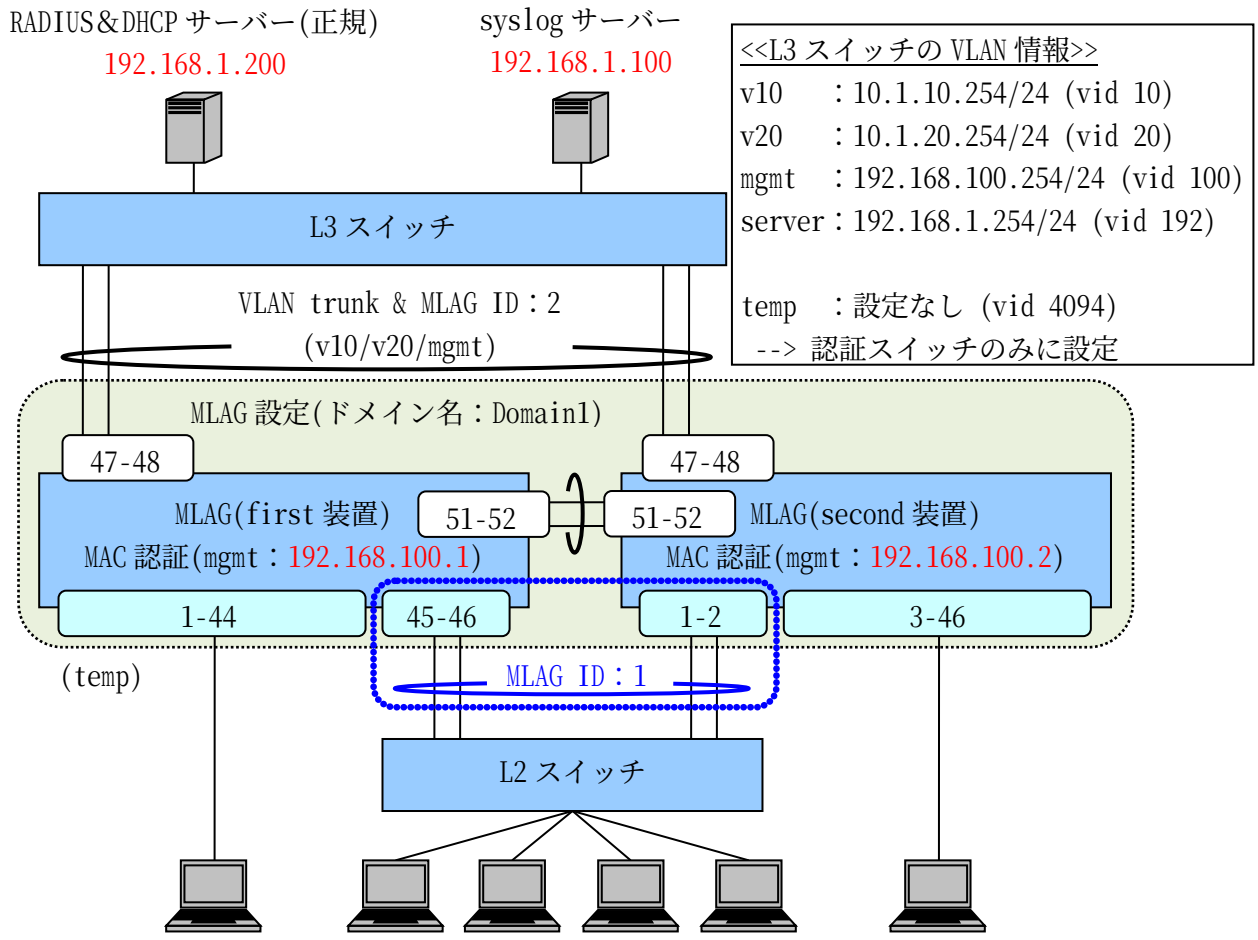


図 4-4 MAC 認証構成例(MLAG 併用)

図 4-4 の構成例における認証スイッチの設定例を示します。

<MLAG(first 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 first
(config)# mlag enable
                ・・・MLAG の設定(first 装置)、有効化
                    ※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。
```

```
(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 名を"mgmt"、暫定 VLAN 名を"temp"、
動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

```
(config)# interface port 1/1-44
(config-if-port)# switchport access vlan 4094
(config)# interface mlag Domain1/1
(config-if-mlag)# switchport access vlan 4094
(config)# interface port 1/45-46
(config-if-port)# mlag Domain1/1
```
・・・暫定 VLAN を access ポートとして設定
※ 認証前のポートは未認証端末同士も通信不可となります。

```
(config)# interface mlag Domain1/2
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```
・・・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-vlan)# ip address 192.168.100.1/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定
※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

```
(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(プライマリー) (必須)
※ INDEX：1 の RADIUS サーバーを MAC 認証のプライマリーとしています。

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

```
(config-a-def)# mac-authentication port 1/1-44
(config-a-def)# mac-authentication mlag Domain1/1
```

・・・MAC 認証ポート(1/1-44、MLAG ID：1) (必須)

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

```
(config)# mlag mac-address-table-update enable
```
・・・MAC アドレス更新機能の有効化
※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
対向装置の FDB 学習の補助を行います。

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

<MLAG(second 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 second
(config)# mlag enable
```
・・・MLAG の設定(second 装置)、有効化
※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(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 名を"mgmt"、暫定 VLAN 名を"temp"、
動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

```
(config)# interface mlag Domain1/1
(config-if-mlag)# switchport access vlan 4094
(config)# interface port 1/1-2
(config-if-port)# mlag Domain1/1
(config)# interface port 1/3-46
(config-if-port)# switchport access vlan 4094
```
・・・暫定 VLAN を access ポートとして設定
※ 認証前のポートは未認証端末同士も通信不可となります。

```
(config)# interface mlag Domain1/2
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```
・・・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-vlan)# ip address 192.168.100.2/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定
※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

```
(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(プライマリー) (必須)
※ INDEX：1 の RADIUS サーバーを MAC 認証のプライマリーとしています。

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

```
(config-a-def)# mac-authentication port 1/3-46
(config-a-def)# mac-authentication mlag Domain1/1
```
・・・MAC 認証ポート(1/3-46、MLAG ID：1) (必須)

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

```
(config)# mlag mac-address-table-update enable
```
・・・MAC アドレス更新機能の有効化
※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
対向装置の FDB 学習の補助を行います。

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

MAC 認証のみの場合、暫定 VLAN は認証スイッチ内のみに設定しておきます。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。

MLAG 併用時、first 装置と second 装置で認証結果の同期は行われません。

MLAG 併用時、ローカルデータベースは first 装置と second 装置で一致させるようにしてください。RADIUS サーバーを使用する場合、first 装置と second 装置で同一のサーバーを参照するなど、同一の認証データを使用するようにしてください。

認証インターフェースに MLAG を設定した場合、当該 MLAG が片 MLAG の場合を除いて

タイムアウト時間(logout timeout コマンド)、エージングログアウト時間(logout aging-time コマンド)は未サポートです。

MLAG の動作仕様上、定期的なフラッディングやブロードキャストが発生しない通信環境では、片側の MLAG 装置のみ FDB 登録されるため、以下の動作となる可能性があります。

- ユニキャスト通信のフラッディングが発生し続ける
- 端末の接続ポートが移動された場合、通信断が発生する

これらの動作が問題となる場合は、mlag mac-address-table-update enable コマンドを有効にして下さい。

4.5 Web 認証、MAC 認証の混在環境

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 において統一します。

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。また、MAC 認証用にパスワードを設定しておきます。

図 4-5 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。

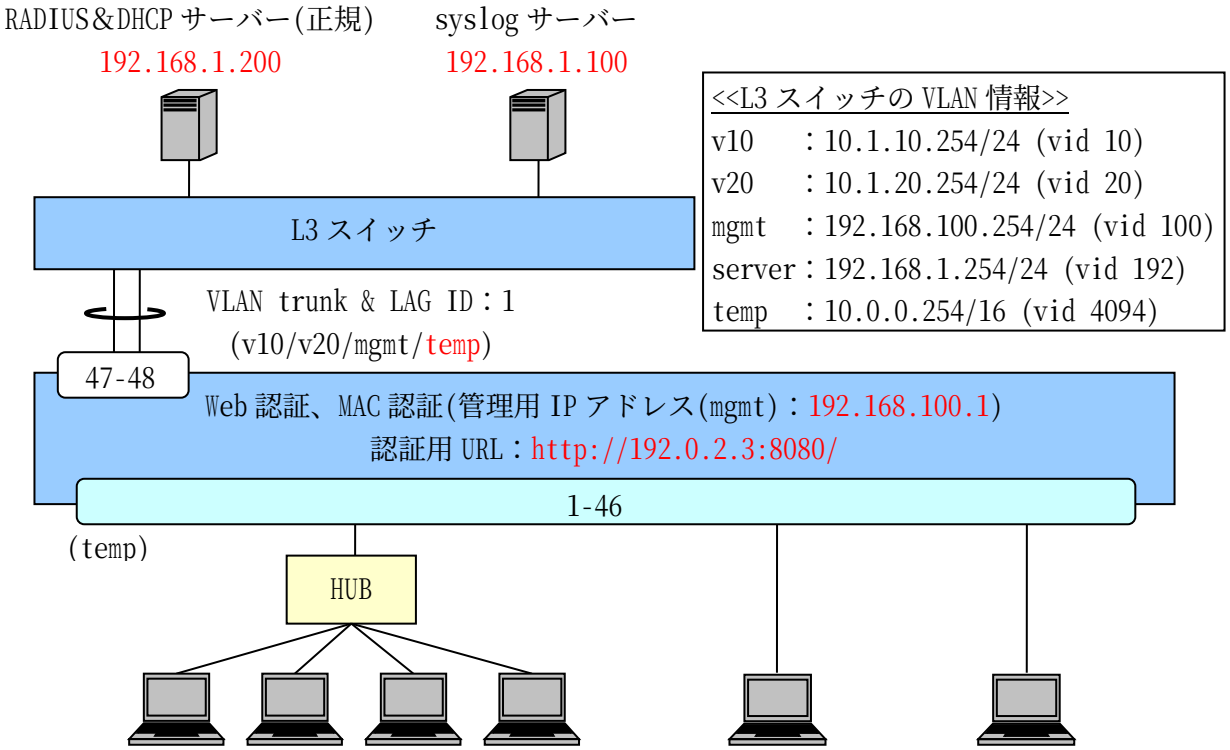


図 4-5 Web 認証と MAC 認証の併用構成例

図 4-5 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 4-1 と同一のため、図 4-1 を参照してください)。

```
(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(プライマリー) (必須)
                  ※ INDEX : 1 の RADIUS サーバーを Web 認証、MAC 認証のプライマリー
                     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)
```

※ 128 台を最大としています。

```
(config-a-def)# web-authentication port 1/1-46
```
・・・Web 認証ポート(1/1-46) (必須)

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (必須)
※ すべての APRESIA で統一することが可能です。

```
(config-a-def)# mac-authentication port 1/1-46
```
・・・MAC 認証ポート(1/1-46) (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 認証、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 30
(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 30 秒)
※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に
合わせて適正な値に調整してください。

4.6 Web/MAC 認証(AND)

Web/MAC 認証(AND)設定例を説明します。Web 認証の認証ポートを Web/MAC 認証(AND)ポートに設定し、Web/MAC 認証(AND)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 において統一します。

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。

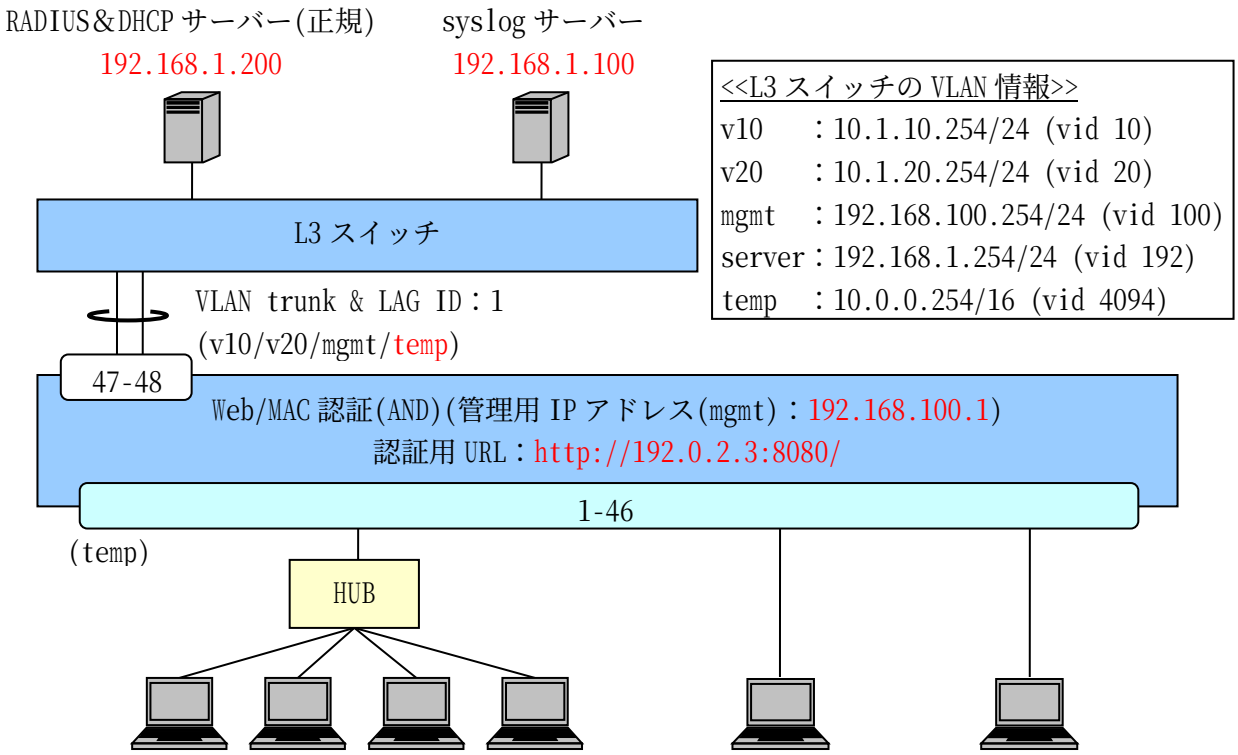


図 4-6 Web/MAC 認証(AND)構成例

図 4-6 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 4-1 と同一のため、図 4-1 を参照してください)。

```
(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(AND)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)
                    ※ 128 台を最大としています。

(config-a-def)# web-authentication port 1/1-46 mac-authentication
                ・・・Web/MAC 認証(AND)ポート(1/1-46) (必須)

(config-a-def)# web-authentication ip 192.0.2.3
```

```
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (必須)
※ すべての APRESIA で統一することが可能です。

```
(config-a-def)# web-authentication mac-authentication-password 1q2w3e
```
・・・Web/MAC 認証(AND)用のパスワード設定、及び有効化 (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 30
(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 30 秒)
※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に
合わせて適正な値に調整してください。

4.7 ゲートウェイ認証(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、ゲートウェイ認証により認証環境の構成が可能です。

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。

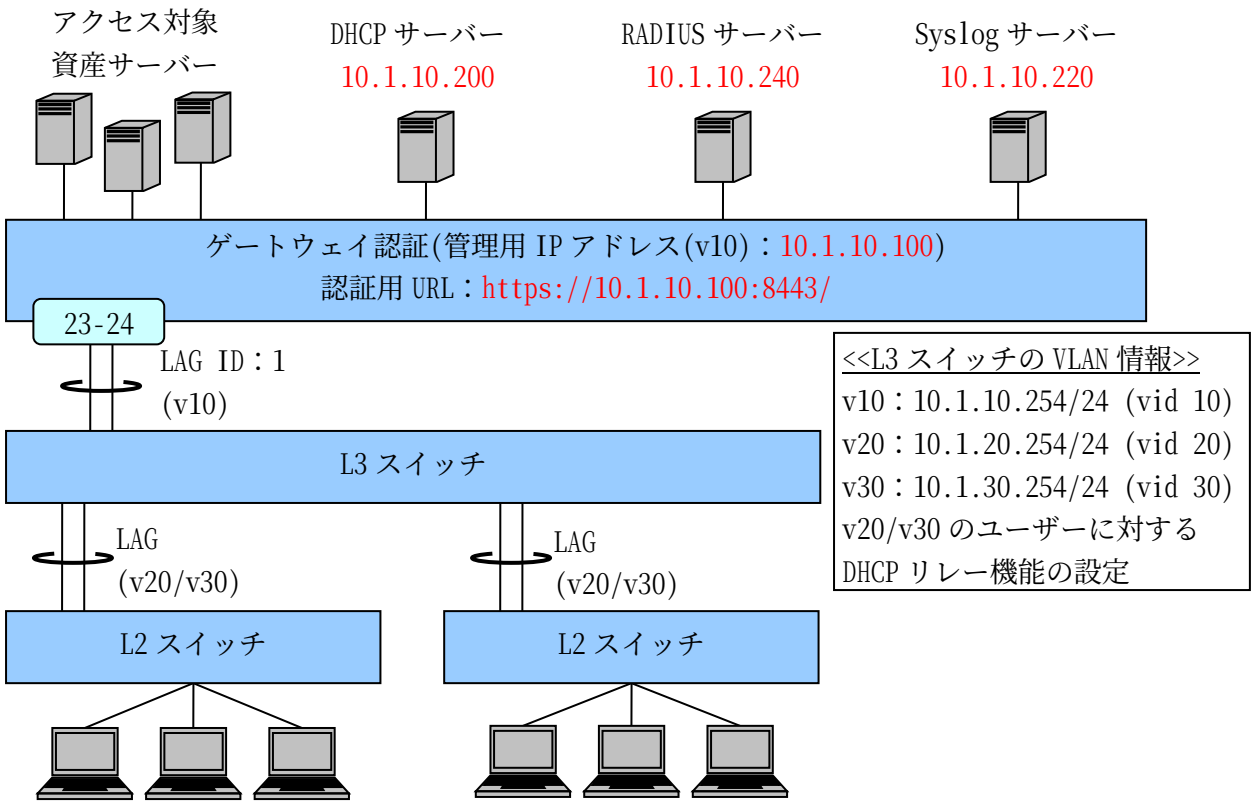


図 4-7 ゲートウェイ認証構成例(サーバーファーム手前適用)

図 4-7 の構成例における認証スイッチの設定例を示します。

```
(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 1/23-24
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
                ・・・パケットフィルター2 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 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、必要な通信を許可)

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

・・・VLAN の設定(ユーザーVLAN(管理用 VLAN)名を"v10"とする)
※ 認証スイッチと RADIUS サーバーが同一ネットワークに存在するため、
ユーザーVLAN(v10)を管理用VLANとし、RADIUSサーバーへアクセスします。

```
(config)# interface lag 1
(config-if-lag)# switchport access vlan 10
(config)# interface port 1/23-24
(config-if-port)# link-aggregation 1
```
・・・ユーザーVLAN を access ポートとして設定

```
(config)# interface vlan 10
(config-if-vlan)# ip address 10.1.10.100/24
```
・・・管理用 VLAN(v10)の IP アドレス設定 (必須)

```
(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(プライマリー) (必須)
※ ゲートウェイ認証は 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)
※ 128 台を最大としています。

```
(config-a-def)# web-authentication lag 1 gateway
```
・・・ゲートウェイ認証ポート(LAG ID：1) (必須)

```
(config-a-def)# web-authentication ip 10.1.10.100
(config-a-def)# web-authentication https-port 8443
```
・・・認証 URL(https://10.1.10.100:8443/) (必須)
※ 管理用 IP アドレスを認証 URL に指定します。

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

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

ゲートウェイ認証における制限事項は、AccessDefender 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)。

4.8 ゲートウェイ認証(サーバーファーム手前に適用、MLAG 併用)

ゲートウェイ認証の認証インターフェースに MLAG を指定する場合は、Web 認証と同様、当該 MLAG インターフェースを片 MLAG 設定で動作させる必要があります(図 4-8 の MLAG ID：1、または MLAG ID：2 のように、片側の MLAG 装置にのみメンバーポートの存在する MLAG インターフェースを認証インターフェースとして使用可能です)。

両方の MLAG 装置にメンバーポートの存在する MLAG インターフェースを認証インターフェースに指定し、下位スイッチと接続する構成は、当該スイッチの分散により認証用 URL の入力時は MLAG の first 装置へ振り分けられ(first 装置より認証画面を表示)、ユーザー名とパスワードの入力時は MLAG の second 装置へ振り分けられると、認証動作が MLAG 装置間を跨いでいることになり、この場合認証シーケンスを完了できないため、使用しないでください。

設定例の説明は 4.7 と同様のため、4.7 を参照してください。

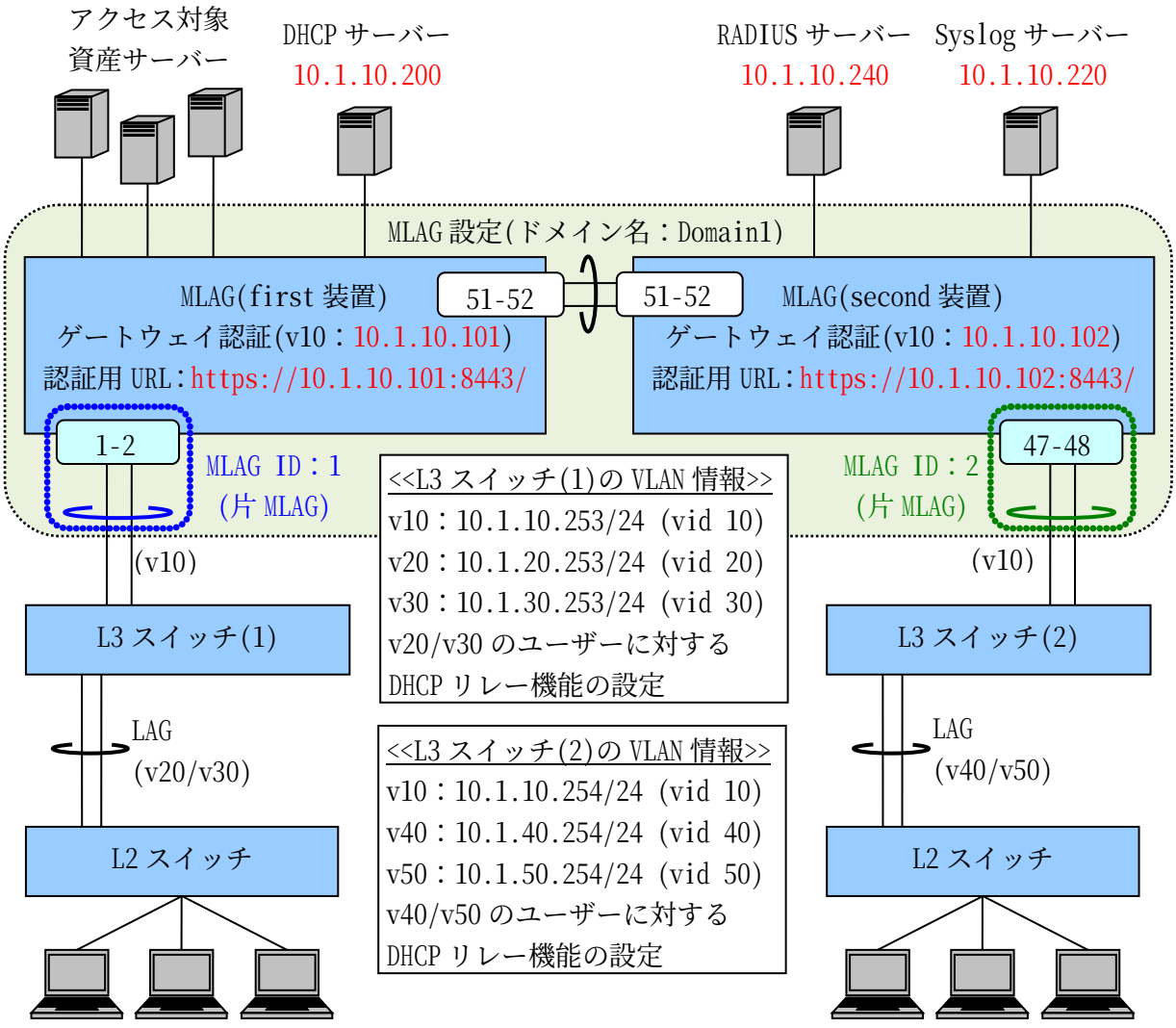


図 4-8 ゲートウェイ認証構成例(サーバーファーム手前適用、MLAG 併用)

図 4-8 の構成例における認証スイッチの設定例を示します。

<MLAG(first 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 first
(config)# mlag enable
```

・・・MLAG の設定(first 装置)、有効化

※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(config)# packet-filter2
(config-filter)# 2 assign port 1/1-2
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
```

・・・パケットフィルター2 の設定(DHCP リレーの通信許可) (DHCP 環境では必須)

```
(config-filter)# 2 2 condition ipv4 dst tcp/udp 514 udp
(config-filter)# 2 2 action authentication-bypass
```

・・・syslog パケットの通信許可(その他、必要な通信を許可)

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

・・・VLAN の設定(ユーザーVLAN(管理用 VLAN)名を"v10"とする)

※ 認証スイッチと RADIUS サーバーが同一ネットワークに存在するため、
ユーザーVLAN(v10)を管理用VLANとし、RADIUSサーバーへアクセスします。

```
(config)# interface mlag Domain1/1
(config-if-mlag)# switchport access vlan 10
(config)# interface port 1/1-2
(config-if-port)# mlag Domain1/1
```

・・・ユーザーVLAN を access ポートとして設定

```
(config)# interface mlag Domain1/2
```

・・・片 MLAG 対向装置への MLAG インターフェースの設定(MLAG ID：2 用)

※ 片 MLAG 設定で動作させる場合でも、両方の MLAG 装置に MLAG
インターフェースを作成する必要があります(メンバーポートは
設定しない)。

```
(config)# interface vlan 10
(config-if-vlan)# ip address 10.1.10.101/24
```

・・・管理用 VLAN(v10)の IP アドレス設定 (必須)

```
(config)# ip route 0.0.0.0/0 10.1.10.253
```

・・・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(プライマリー) (必須)

※ ゲートウェイ認証は 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)
※ 128 台を最大としています。

```
(config-a-def)# web-authentication mlag Domain1/1 gateway
```
・・・ゲートウェイ認証ポート(MLAG ID：1) (必須)

```
(config-a-def)# web-authentication ip 10.1.10.101
(config-a-def)# web-authentication https-port 8443
```
・・・認証 URL(https://10.1.10.101:8443/) (必須)
※ 管理用 IP アドレスを認証 URL に指定します。

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

```
(config)# mlag mac-address-table-update enable
```
・・・MAC アドレス更新機能の有効化
※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
対向装置の FDB 学習の補助を行います。

```
(config)# web-authentication enable
```
・・・Web 認証の有効化 (必須)

<MLAG(second 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 second
(config)# mlag enable
```
・・・MLAG の設定(second 装置)、有効化
※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(config)# packet-filter2
(config-filter)# 2 assign port 1/47-48
(config-filter)# 2 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 2 1 action authentication-bypass
```
・・・パケットフィルター2 の設定(DHCP リレーの通信許可) (DHCP 環境では必須)

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

```
(config)# vlan database
(config-vlan)# vlan 10 name v10
```
・・・VLAN の設定(ユーザーVLAN(管理用 VLAN)名を"v10"とする)
※ 認証スイッチと RADIUS サーバーが同一ネットワークに存在するため、
ユーザーVLAN(v10)を管理用VLANとし、RADIUSサーバーへアクセスします。

```
(config)# interface mlag Domain1/2
(config-if-mlag)# switchport access vlan 10
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```
・・・ユーザーVLAN を access ポートとして設定

```
(config)# interface mlag Domain1/1
```
・・・片 MLAG 対向装置への MLAG インターフェースの設定(MLAG ID：1 用)
※ 片 MLAG 設定で動作させる場合でも、両方の MLAG 装置に MLAG
インターフェースを作成する必要があります（メンバーポートは
設定しない)。

```
(config)# interface vlan 10
(config-if-vlan)# ip address 10.1.10.102/24
```
・・・管理用 VLAN(v10)の IP アドレス設定（必須)

```
(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(プライマリー)（必須)
※ ゲートウェイ認証は 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)
※ 128 台を最大としています。

```
(config-a-def)# web-authentication mlag Domain1/2 gateway
```
・・・ゲートウェイ認証ポート(MLAG ID：2)（必須)

```
(config-a-def)# web-authentication ip 10.1.10.102
(config-a-def)# web-authentication https-port 8443
```
・・・認証 URL(https://10.1.10.102:8443/)（必須)
※ 管理用 IP アドレスを認証 URL に指定します。

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

(config)# mlag mac-address-table-update enable
・・・MAC アドレス更新機能の有効化
※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
対向装置の FDB 学習の補助を行います。

(config)# web-authentication enable
・・・Web 認証の有効化 (必須)

ゲートウェイ認証における制限事項は AccessDefender 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)。

MLAG 併用時、first 装置と second 装置で認証結果の同期は行われません。

MLAG 併用時、ローカルデータベースは first 装置と second 装置で一致させるようにしてください。RADIUS サーバーを使用する場合、first 装置と second 装置で同一のサーバーを参照するなど、同一の認証データを使用するようにしてください。

MLAG の動作仕様上、定期的なフラッディングやブロードキャストが発生しない通信環境では、片側の MLAG 装置のみ FDB 登録されるため、以下の動作となる可能性があります。
- **ユニキャスト通信のフラッディングが発生し続ける**
- **端末の接続ポートが移動された場合、通信断が発生する**

これらの動作が問題となる場合は、mlag mac-address-table-update enable コマンドを有効にして下さい。

4.9 ゲートウェイ認証(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、ゲートウェイ認証により認証環境の構成が可能です。

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

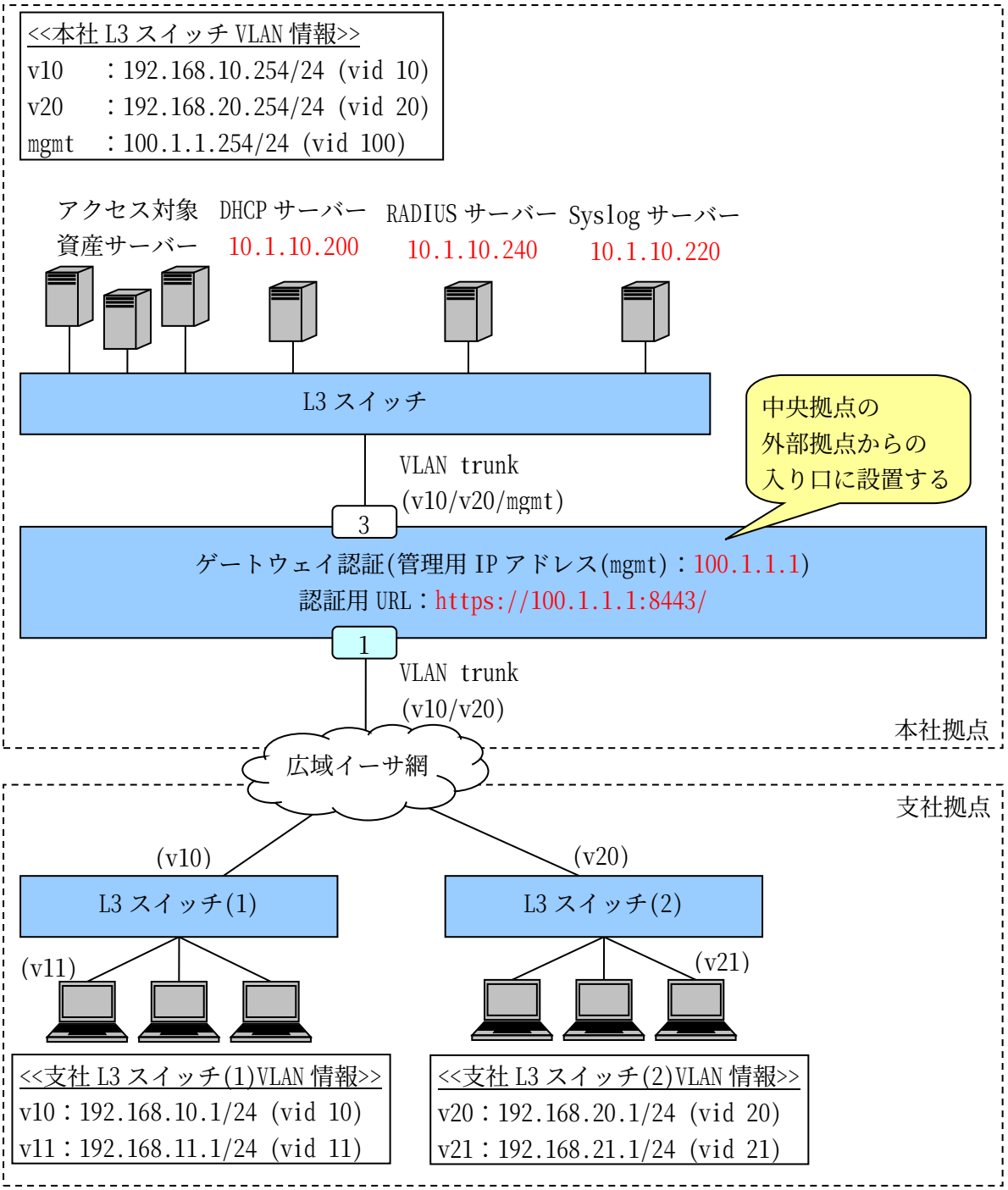


図 4-9 ゲートウェイ認証構成例(中央拠点アクセス構成)

図 4-9 の構成例における認証スイッチの設定例を示します。

```
(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 1/1
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
```

・・・パケットフィルター2 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
```

・・・支社拠点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 名を"mgmt"、ユーザーVLAN 名を"v10"、"v20"とする)

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

・・・ユーザーVLAN を Trunk ポートとして設定(WAN 接続用)

```
(config)# interface port 1/3
(config-if-port)# description honsya-L3
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10,20,100
```

・・・Uplink ポートの設定(本社 L3 スイッチ接続用)

```
(config)# interface vlan 100
(config-if-vlan)# ip address 100.1.1.1/24
```

・・・管理用 VLAN(mgmt)の IP アドレス設定

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

・・・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 force
```

・・・認証データベースに INDEX：1 の RADIUS サーバーを使用して応答がなければ
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)
                  ※ 128 台を最大としています。

(config-a-def)# web-authentication port 1/1 gateway
              ・・・ゲートウェイ認証ポート(1/1) (必須)

(config-a-def)# web-authentication redirect url https://100.1.1.1:8443
(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 認証画面を表示します。
                  ※ プロキシ環境の場合、ブラウザー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、http80 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 8443
              ・・・認証 URL(https://100.1.1.1:8443/) (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)# web-authentication enable
              ・・・Web 認証機能の有効化 (必須)
```

4.10 802.1X

802.1X の設定例を説明します。

APRESIA の認証ポートにサプリカントを直接接続することにより 802.1X の認証を行うことも可能ですが、APRESIA の認証ポート配下に EAP 透過型のスイッチ(またはリピーターハブ)を接続し、サプリカントを複数台収容、かつサプリカントごとに個別認証することも可能です。

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)ごとに動的に 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(またはリピーターハブ)内での通信はその限りではありません。

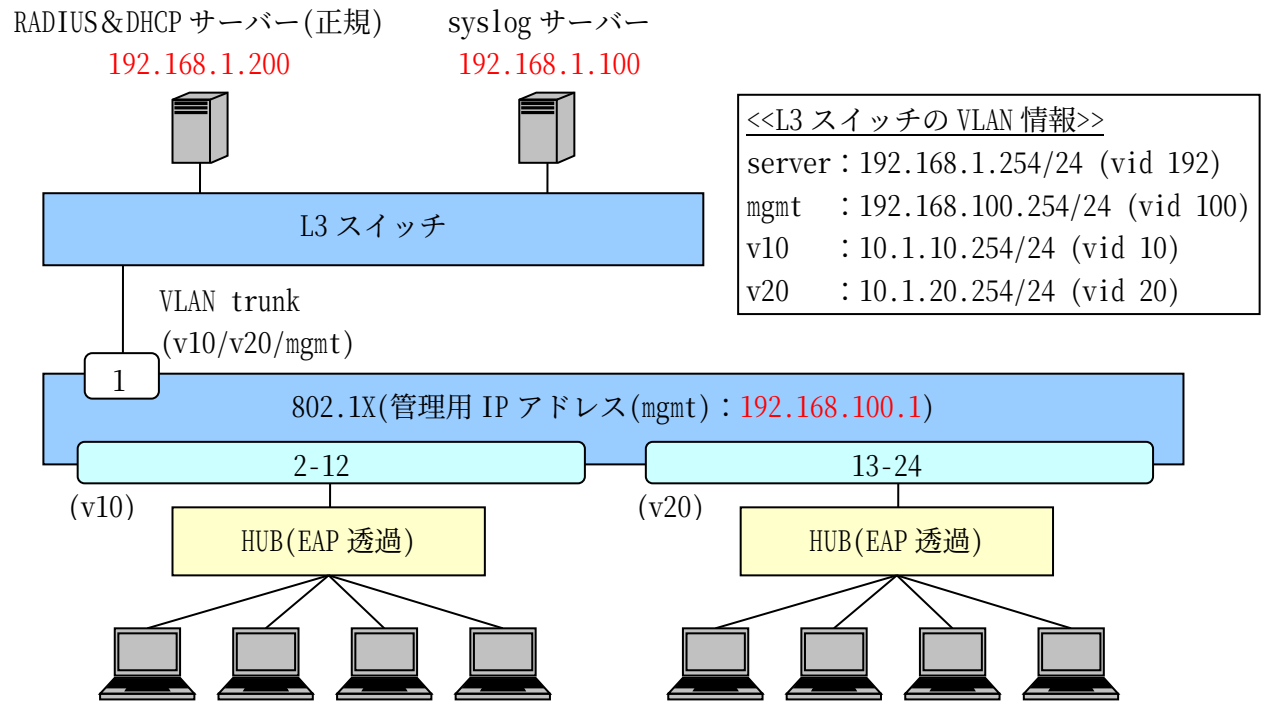


図 4-10 802.1X 構成例

図 4-10 の構成例における認証スイッチの設定例を示します。

```
(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 名を"mgmt"、ユーザーVLAN 名を"v10"、"v20"とする)

(config)# interface port 1/2-12
(config-if-port)# switchport access vlan 10
```

```
(config)# interface port 1/13-24
(config-if-port)# switchport access vlan 20
              ・・・ユーザーVLAN を access ポートとして設定
                    ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface port 1/1
(config-if-port)# switchport mode trunk
(config-if-port)# switchport trunk add 10,20,100
              ・・・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-vlan)# ip address 192.168.100.1/24
              ・・・管理用 VLAN(mgmt)の IP 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 (必須)

(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication dot1x radius 1
              ・・・RADIUS サーバー関連の設定(プライマリー) (必須)
                    ※ INDEX：1 の RADIUS サーバーを 802.1X のプライマリーとしています。

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
              ・・・最大認証端末(128 台) (必須)
                    ※ 128 台を最大としています。

(config-a-def)# dot1x port 1/2-24
              ・・・802.1X の認証ポート(1/2-24) (必須)

(config-a-def)# dot1x port 1/2-24 reauthentication
              ・・・再認証有効設定

(config)# dot1x enable
              ・・・802.1X の有効化 (必須)
```

4.11 802.1X(MLAG 併用)

802.1X の認証インターフェースに MLAG を指定する場合は、当該 MLAG インターフェースを片 MLAG 設定で動作させる必要があります(図 4-11 の MLAG ID：1、または MLAG ID：2 のように、片側の MLAG 装置にのみメンバーポートの存在する MLAG インターフェースを認証インターフェースとして使用可能です)。

両方の MLAG 装置にメンバーポートの存在する MLAG インターフェースを認証インターフェースに指定し、下位の EAP フレームを中継(EAP 透過)するスイッチと接続する構成は、下位スイッチの分散により端末から任意のフレーム送出時は MLAG の first 装置へ振り分けられ(端末の MAC アドレスを登録し、端末へ EAP-Request を送信)、端末からの EAP-Response 送信時は MLAG の second 装置へ振り分けられると、認証動作が MLAG 装置間を跨いでいることになり、この場合認証シーケンスを完了できないため、使用しないでください。

設定例の説明は 4.10 と同様のため、4.10 を参照してください。

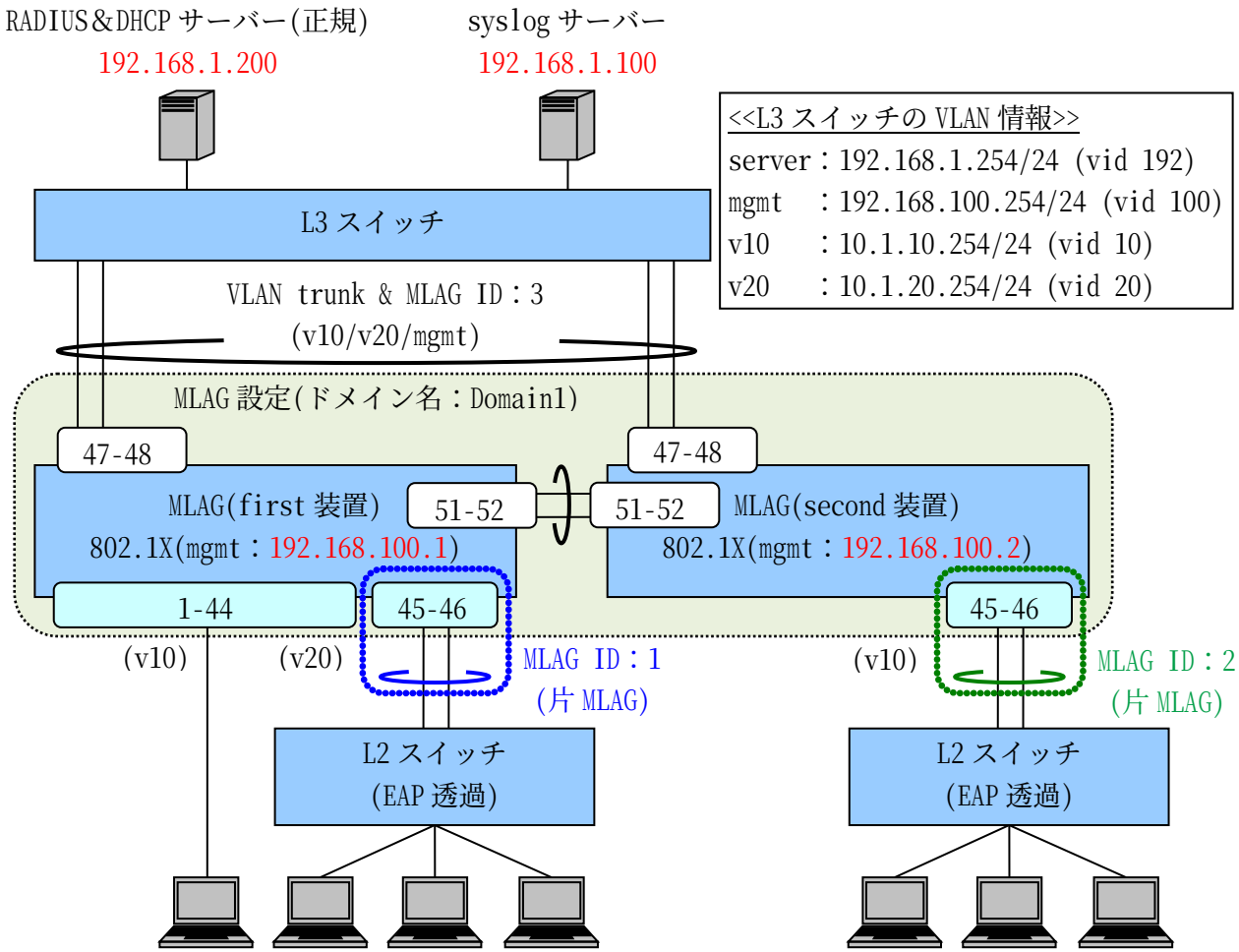


図 4-11 802.1X 構成例(MLAG 併用)

図 4-11 の構成例における認証スイッチの設定例を示します。

<MLAG(first 装置)>

```
(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)# mlag domain Domain1 bridge-port 1/51-52 first
(config)# mlag enable
```
・・・MLAG の設定(first 装置)、有効化
※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

```
(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 名を"mgmt"、ユーザーVLAN 名を"v10"、"v20"とする)

```
(config)# interface port 1/1-44
(config-if-port)# switchport access vlan 10
(config)# interface mlag Domain1/1
(config-if-mlag)# switchport access vlan 20
(config)# interface port 1/45-46
(config-if-port)# mlag Domain1/1
```
・・・ユーザーVLAN を access ポートとして設定
※ 認証前のポートは未認証端末同士も通信不可となります。

```
(config)# interface mlag Domain1/2
```
・・・片 MLAG 対向装置への MLAG インターフェースの設定(MLAG ID：2 用)
※ 片 MLAG 設定で動作させる場合でも、両方の MLAG 装置に MLAG インターフェースを作成する必要があります(メンバーポートは設定しない)。

```
(config)# interface mlag Domain1/3
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/3
```
・・・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-vlan)# ip address 192.168.100.1/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定 (必須)

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

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication dot1x radius 1
```
・・・RADIUS サーバー関連の設定(プライマリー) (必須)
※ INDEX：1 の RADIUS サーバーを 802.1X のプライマリーとしています。

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

(config-a-def)# dot1x port 1/1-44
(config-a-def)# dot1x mlag Domain1/1
              ・・・802.1X の認証ポート(1/1-44、MLAG ID：1) (必須)

(config-a-def)# dot1x port 1/1-44 reauthentication
(config-a-def)# dot1x mlag Domain1/1 reauthentication
              ・・・再認証有効設定

(config)# mlag mac-address-table-update enable
              ・・・MAC アドレス更新機能の有効化
                  ※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、
                     対向装置の FDB 学習の補助を行います。

(config)# dot1x enable
              ・・・802.1X の有効化 (必須)
```

<MLAG(second 装置)>

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

(config)# mlag domain Domain1 bridge-port 1/51-52 second
(config)# mlag enable
              ・・・MLAG の設定(second 装置)、有効化
                  ※ MLAG を有効にするには、上記設定後、設定保存と装置再起動が必要です。

(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 名を"mgmt"、ユーザーVLAN 名を"v10"、"v20"とする)

(config)# interface mlag Domain1/2
(config-if-mlag)# switchport access vlan 10
(config)# interface port 1/45-46
(config-if-port)# mlag Domain1/2
              ・・・ユーザーVLAN を access ポートとして設定
                  認証前のポートは未認証端末同士も通信不可となります。

(config)# interface mlag Domain1/1
              ・・・片 MLAG 対向装置への MLAG インターフェースの設定(MLAG ID：1 用)
```

※ 片 MLAG 設定で動作させる場合でも、両方の MLAG 装置に MLAG インターフェースを作成する必要があります(メンバーポートは設定しない)。

```
(config)# interface mlag Domain1/3
(config-if-mlag)# switchport mode trunk
(config-if-mlag)# switchport trunk add 10,20,100
(config)# interface port 1/47-48
(config-if-port)# mlag Domain1/2
```

・・・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-vlan)# ip address 192.168.100.2/24
```

・・・管理用 VLAN(mgmt)の IP 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 (必須)

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication dot1x radius 1
```

・・・RADIUS サーバー関連の設定(プライマリー) (必須)

※ INDEX：1 の RADIUS サーバーを 802.1X のプライマリーとしています。

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

・・・最大認証端末(128 台) (必須)

※ 128 台を最大としています。

```
(config-a-def)# dot1x mlag Domain1/2
```

・・・802.1X の認証ポート(MLAG ID：2) (必須)

```
(config-a-def)# dot1x mlag Domain1/2 reauthentication
```

・・・再認証有効設定

```
(config)# mlag mac-address-table-update enable
```

・・・MAC アドレス更新機能の有効化

※ 両方の MLAG 装置の FDB 学習状況に偏りが発生するため、対向装置の FDB 学習の補助を行います。

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

・・・802.1X の有効化 (必須)

MLAG 併用時、first 装置と second 装置で認証結果の同期は行われません。

MLAG 併用時、RADIUS サーバーを使用する場合、first 装置と second 装置で同一のサー

バーを参照するなど、同一の認証データを使用するようにしてください。

MLAG の動作仕様上、定期的なフラッディングやブロードキャストが発生しない通信環境では、片側の MLAG 装置のみ FDB 登録されるため、以下の動作となる可能性があります。

- ユニキャスト通信のフラッディングが発生し続ける
- 端末の接続ポートが移動された場合、通信断が発生する

これらの動作が問題となる場合は、`mlag mac-address-table-update enable` コマンドを有効にして下さい。

4.12 802.1X/MAC 認証(AND)

802.1X/MAC 認証(AND)の設定例を説明します。802.1X の認証ポートを 802.1X/MAC 認証(AND)ポートに設定し、802.1X/MAC 認証(AND)機能を有効にする必要があります。

802.1X と同様に、APRESIA の認証ポート配下に EAP 透過型スイッチ(またはリピーターハブ)を接続し、サプリカントを複数台収容、かつサプリカントごとに個別認証することも可能です。

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)ごとに動的に VLAN を割り当てることが可能です。

認証前の端末は、APRESIA の認証ポートによって通信が制限されているため、APRESIA のポートを経由して他の端末とは通信できません。ただし、EAP フレームを中継(EAP 透過)するスイッチ(またはリピーターハブ)内での通信はその限りではありません。

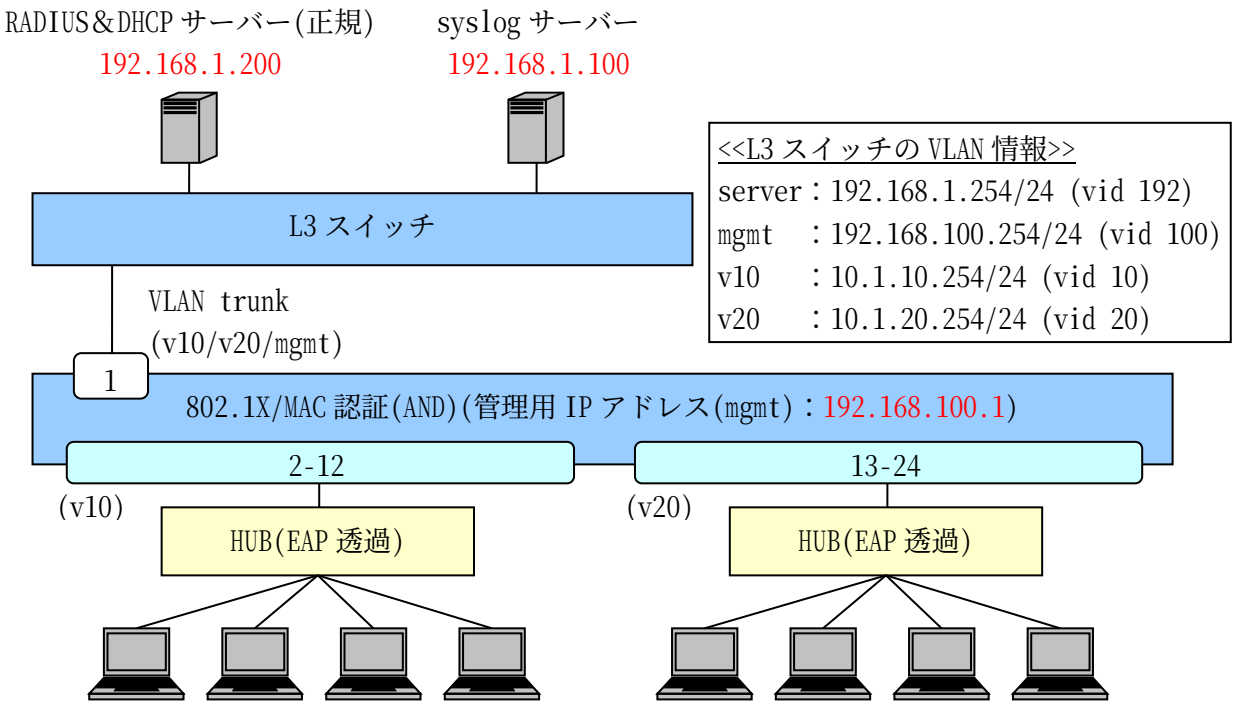


図 4-12 802.1X/MAC 認証(AND)構成例

図 4-12 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 4-10 と同一のため、図 4-10 を参照してください)。

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication dot1x radius 1
                ・・・RADIUS サーバー関連の設定(プライマリー) (必須)
                    ※ 802.1X/MAC 認証(AND)は 802.1X 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)
                    ※ 128 台を最大としています。
```

```
(config-a-def)# dot1x port 1/2-24
                ・・・802.1X の認証ポート(1/1-24) (必須)

(config-a-def)# dot1x port 1/2-24 reauthentication
                ・・・再認証有効設定

(config-a-def)# dot1x mac-authentication-password 1q2w3e
                ・・・802.1X/MAC(AND)認証用のパスワード設定、及び有効化 (必須)

(config)# dot1x enable
                ・・・802.1X の有効化 (必須)
```

4.13 Web/802.1X 認証(AND)

Web/802.1X 認証(AND)設定例を説明します。Web 認証の認証ポートを Web/802.1X 認証(AND)ポートに設定し、Web/802.1X 認証(AND)機能を有効にする必要があります。また、802.1X を行うために、別途 802.1X の有効化設定も必要です。

Web/802.1X 認証(AND)は、Web 認証と 802.1X を個別に実施し、どちらの認証にも成功している場合のみ通信が可能になります。認証成功後に割り当てられる正規 VLAN は、後に成功した認証の属性情報で割り当てられます。両方の認証が成功している状態から、片方の認証をログアウトした場合は、Web/802.1X 認証(AND)が成功していない状態のため通信は不可になります。再度、両方の認証が成功した際にも、後に成功した認証の属性情報で正規 VLAN が割り当てられます。

Web 認証の説明は 4.1 と同様のため、4.1 を参照してください。802.1X の説明は 4.10 と同様のため、4.10 を参照してください。

Web 認証の代わりに Web/MAC 認証(AND)と 802.1X の併用認証(AND)を行う場合は、Web/MAC 認証(AND)ポートの設定と、Web/MAC 認証(AND)用のパスワードを追加設定してください。Web/MAC 認証(AND)の詳細は、4.6 を参照してください。

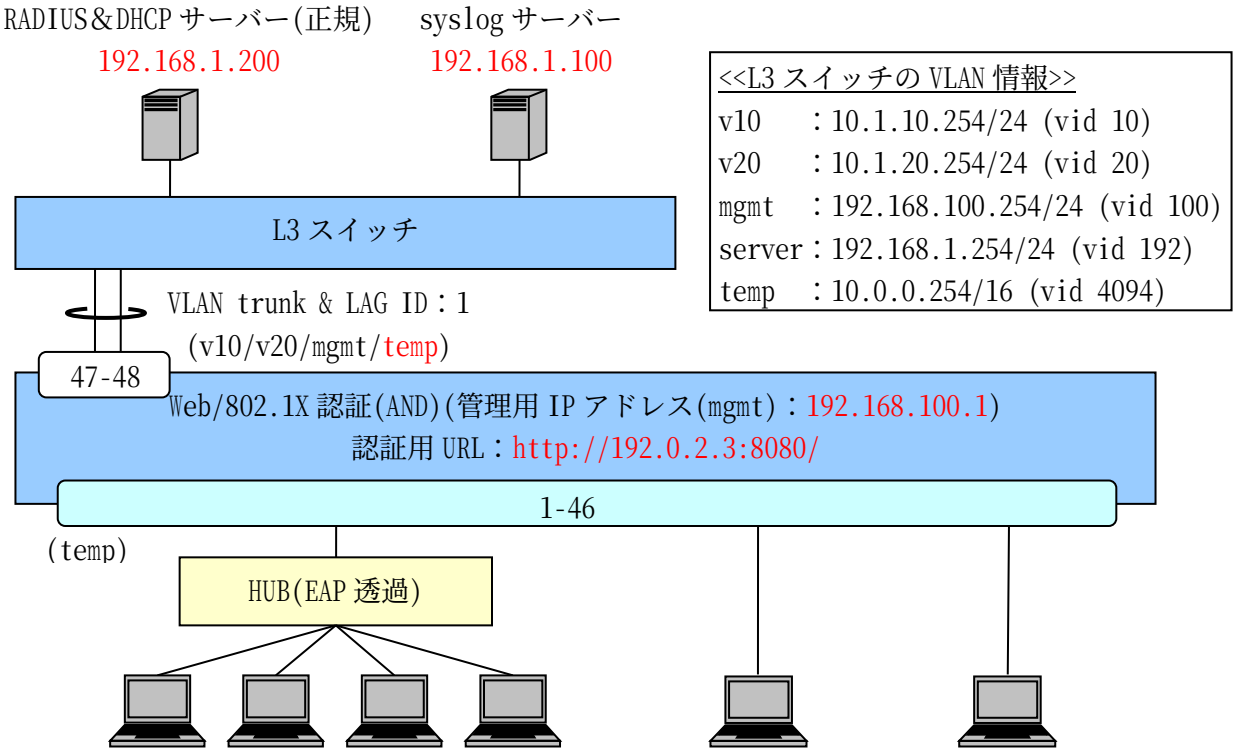


図 4-13 Web/802.1X 認証(AND)構成例

図 4-13 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 4-1 と同一のため、図 4-1 を参照してください)。

```
(config)# aaa radius 1 host 192.168.1.200 key apresia
(config)# aaa authentication web radius 1
(config)# aaa authentication dot1x radius 1
```

・・・RADIUS サーバー関連の設定(プライマリー) (必須)

※ Web/802.1X 認証(AND)は Web 認証、802.1X 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)
※ 128 台を最大としています。

```
(config-a-def)# web-authentication port 1/1-46 dot1x
```
・・・Web/802.1X 認証(AND)ポート(1/1-46) (必須)
※ 802.1X の認証ポート(dot1x port 1/1-46)の設定は不要です。

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (必須)
※ すべての APRESIA で統一することが可能です。

```
(config-a-def)# dot1x port 1/1-46 reauthentication
```
・・・再認証有効設定

```
(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)# dot1x enable
```
・・・802.1X 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 30
(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 30 秒)
※ 暫定 VLAN 用 DHCP サーバーのリース時間が短いと、
正規 IP アドレスを取得できない場合があるため、利用環境に合わせて
適正な値に調整してください。

Web/802.1X 認証(AND)を使用する場合、Web 認証の有効設定(web-authentication enable コマンド)と 802.1X の有効設定(dot1x enable コマンド)をする必要があります。

4.14 DHCP Snooping

DHCP Snooping の設定例を説明します。

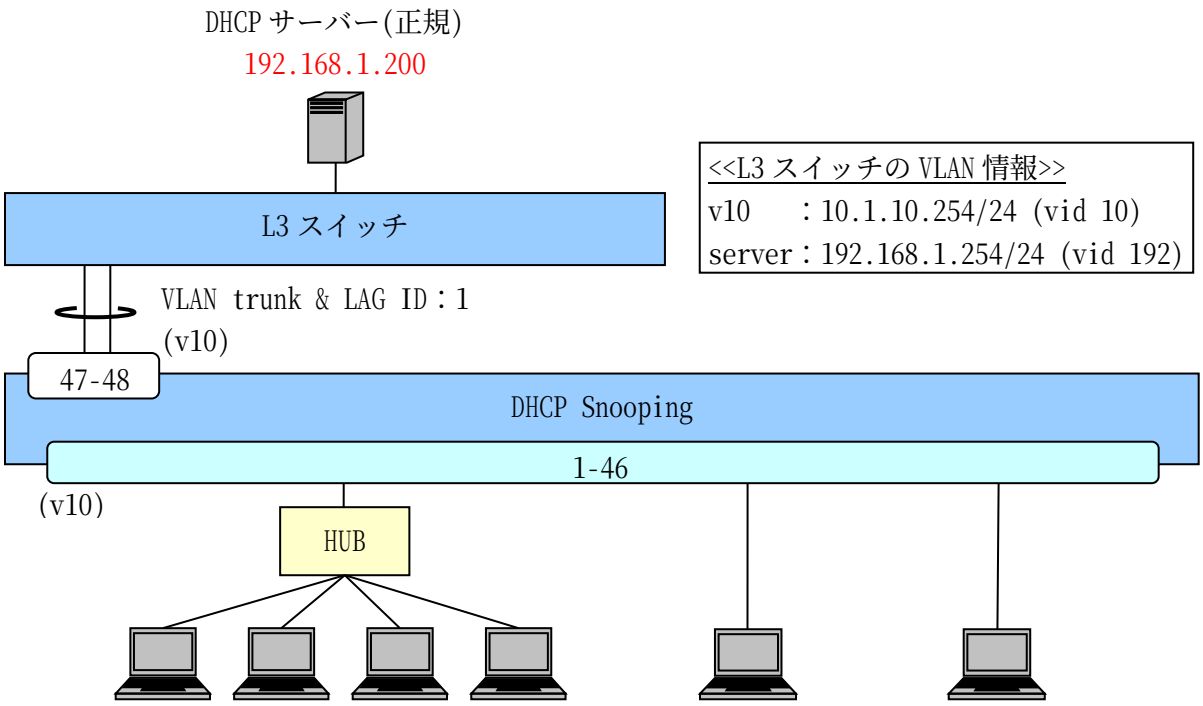


図 4-14 DHCP Snooping 構成例

図 4-14 の構成例における認証スイッチの設定例を示します。

```
(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
                ・・・VLAN の設定(ユーザーVLAN 名を"v10"とする)

(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 10
                ・・・ユーザーVLAN を access ポートとして設定

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
(config-if-lag)# switchport trunk add 10
(config)# interface port 1/47-48
(config-if-port)# link-aggregation 1
                ・・・Uplink ポートの設定

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

・・・最大認証端末(128 台) (必須)
※ 128 台を最大としています。

(config-a-def)# dhcp-snooping port 1/1-46
・・・DHCP Snooping ポート(1/1-46) (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設定

(config)# dhcp-snooping enable
・・・DHCP Snooping の有効化 (必須)

MLAG 併用時、DHCP Snooping は未サポートです。

4.15 DHCP Snooping、MAC 認証の混在環境

DHCP Snooping と MAC 認証を混在させる場合の設定例を説明します。

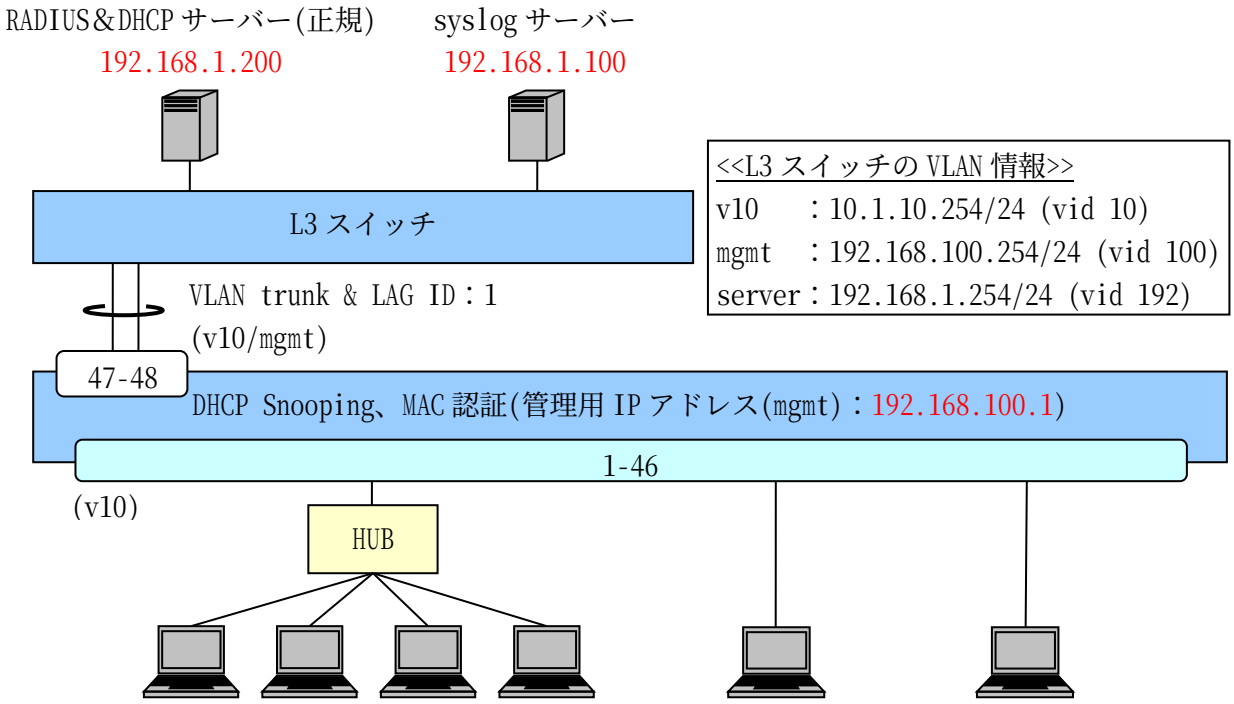


図 4-15 DHCP Snooping と MAC 認証の併用構成例

図 4-15 の構成例における認証スイッチの設定例を示します。

```
(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 名を"mgmt"、ユーザーVLAN 名を"v10"とする)

(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 10
              ・・・ユーザーVLAN を access ポートとして設定
                  ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
(config-if-lag)# switchport trunk add 10,100
(config)# interface port 1/47-48
(config-if-port)# link-aggregation 1
              ・・・Uplink ポートの設定
```

```
(config)# interface vlan 100
(config-if-vlan)# ip address 192.168.100.1/24
              ・・・管理用 VLAN(mgmt)の IP 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 (必須)

(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(プライマリー) (MAC 認証時必須)
                    ※ INDEX：1 の RADIUS サーバーを MAC 認証のプライマリーとしています。

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
              ・・・最大認証端末(128 台) (必須)
                    ※ 128 台を最大としています。

(config-a-def)# dhcp-snooping port 1/1-46
              ・・・DHCP Snooping ポート(1/1-46) (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設定

(config-a-def)# mac-authentication port 1/1-46
              ・・・MAC 認証ポート(1/1-46) (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 Snooping、MAC 認証の有効化 (必須)
```

DHCP Snooping と MAC 認証を併用する場合、MAC 認証の固定 VLAN モード、動的 VLAN モードに関わらず構成は同じです。

4.16 DHCP Snooping、Web 認証(固定 VLAN)の混在環境

DHCP Snooping 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。

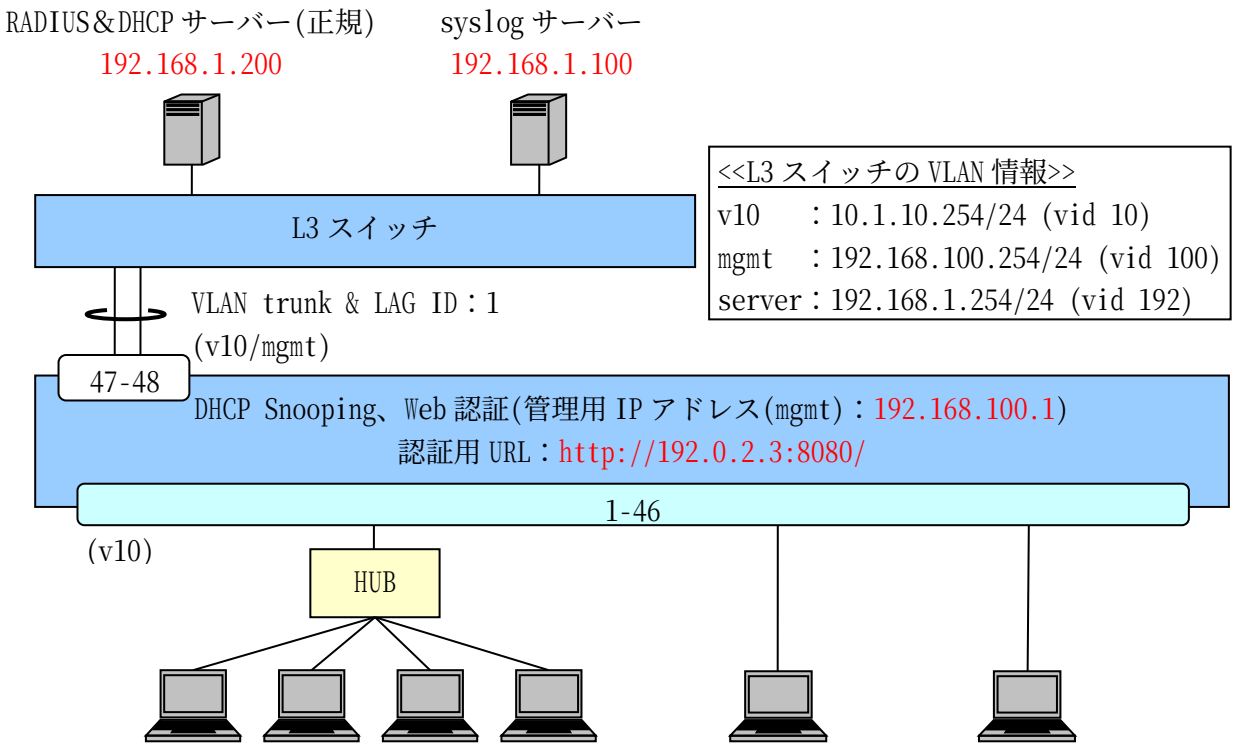


図 4-16 DHCP Snooping と Web 認証(固定 VLAN)の併用構成例

図 4-16 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 4-15 と同一のため、図 4-15 を参照してください)。

```
(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) (Web 認証時必須)
                    ※ INDEX : 1 の RADIUS サーバーを Web 認証のプライマリーとしています。

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
                ・・・最大認証端末(128 台) (必須)
                    ※ 128 台を最大としています。

(config-a-def)# dhcp-snooping port 1/1-46
                ・・・DHCP Snooping ポート(1/1-46) (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設定

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

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
              ・・・認証 URL(http://192.0.2.3:8080/) (Web 認証時必須)
                   ※ すべての APRESIA で統一することが可能です。

(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 Snooping、Web 認証の有効化 (必須)
```

DHCP Snooping 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 Snooping 登録後、自動的に許可されます。

同一 VLAN インターフェースにおいて DHCP サーバー機能併用時は、dhcp-snooping internal-dhcp-vlan コマンドの設定が必要です。

4.17 DHCP Snooping、Web 認証(動的 VLAN)の混在環境

DHCP Snooping 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。

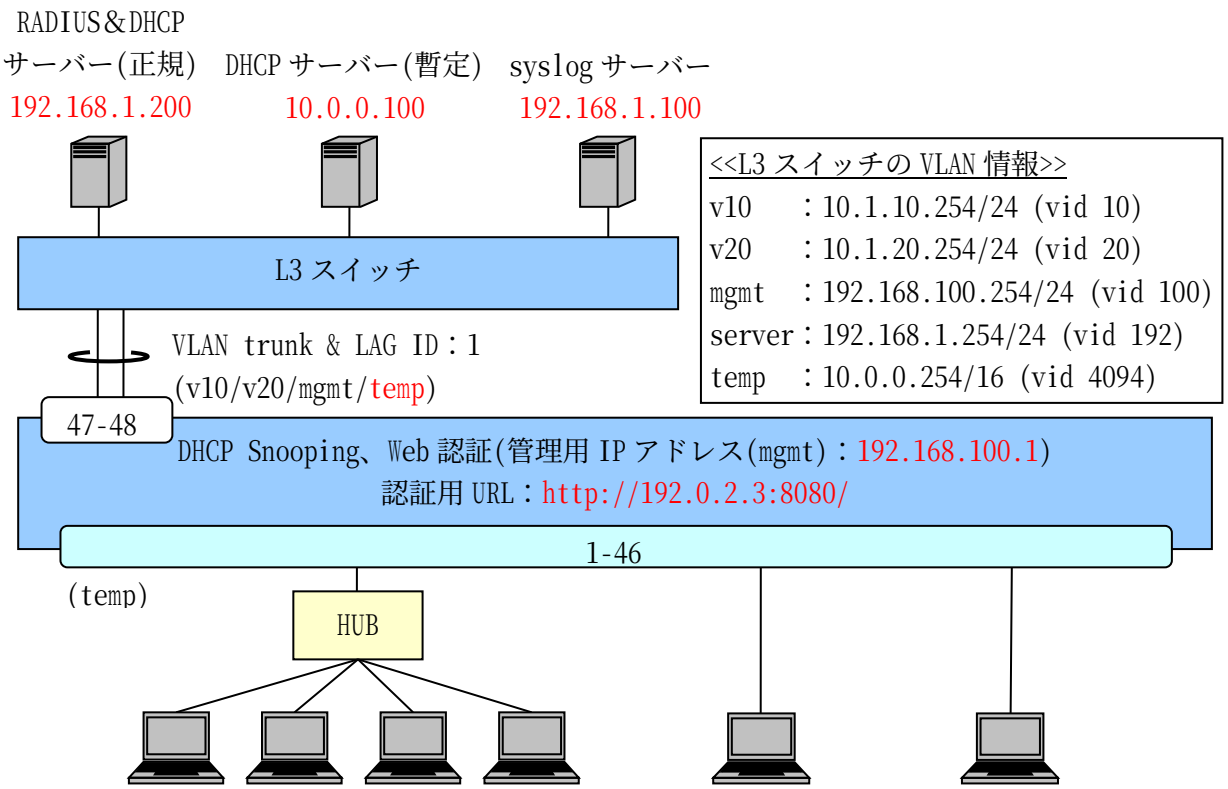


図 4-17 DHCP Snooping と Web 認証(動的 VLAN)の併用構成例

図 4-17 の構成例における認証スイッチの設定例を示します。

```
(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 名を"mgmt"、暫定 VLAN 名を"temp"、
                   動的 VLAN 変更後の正規ユーザーVLAN 名を"v10"、"v20"とする)

(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 4094
              ・・・暫定 VLAN を access ポートとして設定
                   ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
```

```
(config-if-lag)# switchport trunk add 10,20,100,4094
(config)# interface port 1/47-48
(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-vlan)# ip address 192.168.100.1/24
```
・・・管理用 VLAN(mgmt)の IP アドレス設定
※ 暫定 VLAN には IP アドレスを設定する必要はありません。

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

```
(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) (Web 認証時必須)
※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

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

```
(config-a-def)# dhcp-snooping port 1/1-46
```
・・・DHCP Snooping ポート(1/1-46) (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設定

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

```
(config-a-def)# web-authentication ip 192.0.2.3
(config-a-def)# web-authentication http-port 8080
```
・・・認証 URL(http://192.0.2.3:8080/) (Web 認証時必須)
※ すべての APRESIA で統一することが可能です。

```
(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 Snooping、Web 認証の有効化 (必須)

DHCP Snooping 有効時は 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 Snooping 登録後、自動的に許可されます。

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。

同一 VLAN インターフェースにおいて DHCP サーバー機能併用時は、dhcp-snooping internal-dhcp-vlan コマンドの設定が必要です。

4.18 ユーザーポリシーコントロール構成例

ユーザーポリシーコントロールの設定例を説明します。

パケットフィルター2 のフィルター条件(コンディション)にクラス ID を設定することによって、認証端末ごとのフレーム制御ポリシー適用を実現します。

RADIUS サーバーにクラス ID を設定することにより、認証時にユーザー(端末)ごとに動的にクラス ID を割り当てます。

4.18.1 クラス ID 端末環境

図 4-18 にクラス ID 端末環境の構成例を示します。クラス ID を使用して User1、User2 から DHCP サーバー、RADIUS サーバーへのアクセス制限、User3、User4 から資産サーバーへのアクセス制限、User1 から資産サーバーへの優先度変更、User3 から DHCP サーバー、RADIUS サーバーへの優先度を変更します。

具体的な設定としては、User1、User2 の 10.1.10.0/24 宛パケットを破棄、User3、User4 の 20.0.0.0/24 宛パケットを破棄、User1 の 20.0.0.0/24 宛パケットを qp7 へ変更、User3 の 10.1.10.0/24 宛パケットを qp7 へ変更します。

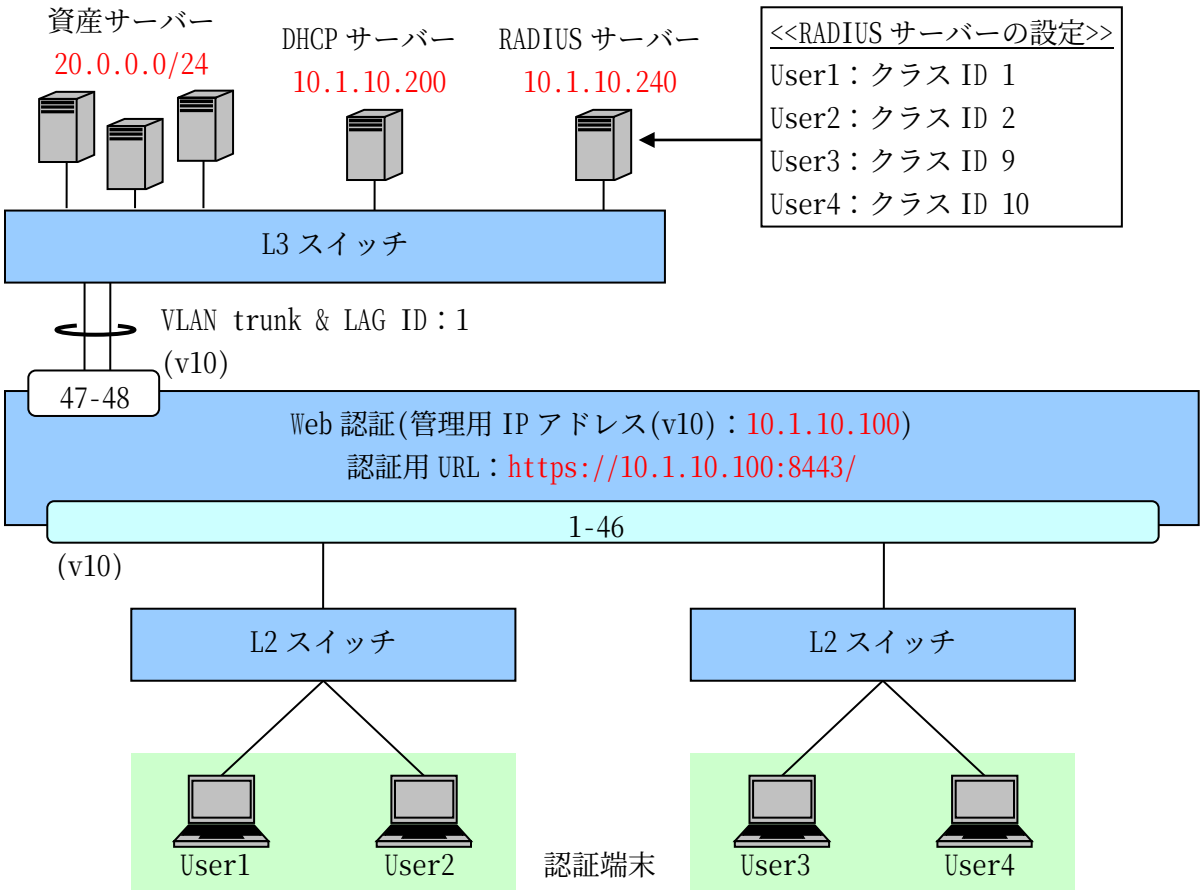


図 4-18 ユーザーポリシーコントロール構成例 1

図 4-18 の構成例(Web 認証(固定 VLAN))における認証スイッチの設定例を示します。

```
(config)# packet-filter2
(config-filter)# 1 assign port 1/1-46
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
```

```
(config-filter)# 1 1 action authentication-bypass
              ・・・パケットフィルター2 の設定(DHCP の通信許可)
                   (VLAN 固定時の DHCP 環境では必須)

(config-filter)# 2 assign port 1/1-46
(config-filter)# 2 1 action deny
(config-filter)# 2 1 condition dst ip 10.1.10.0/24
(config-filter)# 2 1 condition class 1 mask 0xffe
              ・・・クラス ID：1、2 の設定(10.1.10.0/24 宛パケットを破棄)

(config-filter)# 2 2 action deny
(config-filter)# 2 2 condition dst ip 20.0.0.0/24
(config-filter)# 2 2 condition class 9 mask 0xffe
              ・・・クラス ID：9、10 の設定(20.0.0.0/24 宛パケットを破棄)

(config-filter)# 3 assign port 1/1-46
(config-filter)# 3 1 action permit
(config-filter)# 3 1 action qos qp7
(config-filter)# 3 1 condition dst ip 20.0.0.0/24
(config-filter)# 3 1 condition class 1
              ・・・クラス ID：1 の設定(20.0.0.0/24 宛パケットの優先度変更)

(config-filter)# 3 2 action permit
(config-filter)# 3 2 action qos qp7
(config-filter)# 3 2 condition dst ip 10.1.10.0/24
(config-filter)# 3 2 condition class 9
              ・・・クラス ID：9 の設定(10.1.10.0/24 宛パケットの優先度変更)

(config)# qos enable
              ・・・QoS の有効化(優先度制御用)

(config)# vlan database
(config-vlan)# vlan 10 name v10
              ・・・VLAN の設定(ユーザーVLAN(管理用 VLAN)名を"v10"とする)
                   ※ 認証スイッチと RADIUS サーバーが同一ネットワークに存在するため、
                      ユーザーVLAN(v10)を管理用VLANとし、RADIUSサーバーへアクセスします。

(config)# interface port 1/1-46
(config-if-port)# switchport access vlan 10
              ・・・ユーザーVLAN を access ポートとして設定
                   ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface lag 1
(config-if-lag)# switchport mode trunk
(config-if-lag)# switchport trunk add 10
```

```
(config)# interface port 1/47-48
(config-if-port)# link-aggregation 1
              ・・・Uplink ポートの設定

(config)# interface vlan 10
(config-if-vlan)# ip address 10.1.10.100/24
              ・・・管理用 VLAN(v10)の IP アドレス設定 (必須)

(config)# ip route 0.0.0.0/0 10.1.10.254
              ・・・デフォルトルートの設定

(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(プライマリー) (必須)
                   ※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

(config)# access-defender
(config-a-def)# packet-filter2 max-rule 128
              ・・・最大認証端末(128 台) (必須)
                   ※ 128 台を最大としています。

(config-a-def)# web-authentication port 1/1-46
              ・・・Web 認証ポート(1/1-46) (必須)

(config-a-def)# web-authentication ip 10.1.10.100
(config-a-def)# web-authentication https-port 8443
              ・・・認証 URL(https://10.1.10.100:8443/) (必須)
                   ※ この例では、同一ネットワークに閉じた認証のため、ゲートウェイ認証
                      のように管理用 IP アドレスを認証 URL に指定していますが、Web 認証では
                      任意の認証 URL 指定で問題ありません。

(config)# web-authentication enable
              ・・・Web 認証の有効化 (必須)
```

4.18.2 クラス ID 端末/クラス ID 未付与端末の混在環境

図 4-19 にクラス ID 端末/クラス ID 未付与端末が混在している環境の構成例を示します。クラス ID 端末にはクラス ID 指定のパケットフィルター2 を適用します。クラス ID 未付与端末には、aaa default class コマンドで指定したデフォルトクラス ID：10 指定のパケットフィルター2 を適用します。フレーム制御ポリシーは 4.18.1 と同様とします。

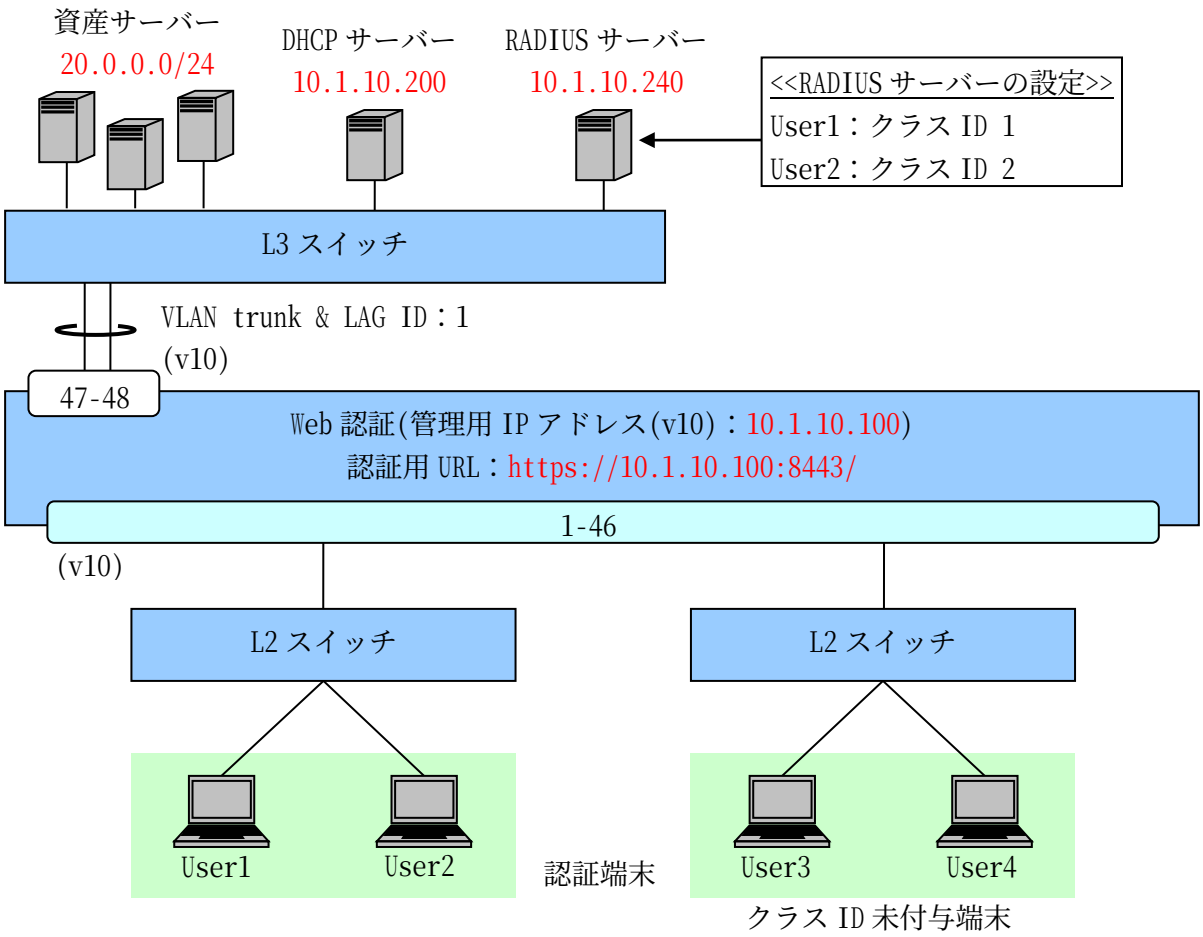


図 4-19 ユーザーポリシーコントロール構成例 2

図 4-19 の構成例(Web 認証(固定 VLAN))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 4-18 と同一のため、図 4-18 を参照してください)。

```
(config)# packet-filter2
(config-filter)# 1 assign port 1/1-16
(config-filter)# 1 1 condition ipv4 dst tcp/udp 67 udp
(config-filter)# 1 1 action authentication-bypass
                ・・・パケットフィルター2 の設定(DHCP の通信許可)
                    (VLAN 固定時の DHCP 環境では必須)

(config)# aaa default class 10
                ・・・デフォルトクラス ID に 10 を設定

(config-filter)# 2 assign port 1/1-16
```

```
(config-filter)# 2 1 action deny
(config-filter)# 2 1 condition dst ip 10.1.10.0/24
(config-filter)# 2 1 condition class 1 mask 0xffe
```
・・・クラス ID：1、2 の設定(10.1.10.0/24 宛パケットを破棄)

```
(config-filter)# 2 2 action deny
(config-filter)# 2 2 condition dst ip 20.0.0.0/24
(config-filter)# 2 2 condition class 10
```
・・・デフォルトクラス ID の設定(20.0.0.0/24 宛パケットを破棄)

```
(config-filter)# 3 assign port 1/1-16
(config-filter)# 3 1 action permit
(config-filter)# 3 1 action qos qp7
(config-filter)# 3 1 condition dst ip 20.0.0.0/24
(config-filter)# 3 1 condition class 1
```
・・・クラス ID：1 の設定(20.0.0.0/24 宛パケットの優先度変更)

```
(config-filter)# 3 2 action permit
(config-filter)# 3 2 action qos qp7
(config-filter)# 3 2 condition dst ip 10.1.10.0/24
(config-filter)# 3 2 condition class 10
```
・・・デフォルトクラス ID の設定(10.1.10.0/24 宛パケットの優先度変更)

```
(config)# qos enable
```
・・・QoS の有効化(優先度制御用)

```
(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(プライマリー) (必須)
※ INDEX：1 の RADIUS サーバーを Web 認証のプライマリーとしています。

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

```
(config-a-def)# web-authentication port 1/1-46
```
・・・Web 認証ポート(1/1-46) (必須)

```
(config-a-def)# web-authentication ip 10.1.10.100
(config-a-def)# web-authentication https-port 8443
```
・・・認証 URL(https://10.1.10.100:8443/) (必須)
※ この例では、同一ネットワークに閉じた認証のため、ゲートウェイ認証のように管理用 IP アドレスを認証 URL に指定していますが、Web 認証では任意の認証 URL 指定で問題ありません。

```
(config)# web-authentication enable
                ・・・Web 認証の有効化 (必須)
```

5 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(または/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 認証は、PAP(Password Authentication Protocol)のみです。CHAP(Challenge Handshake Authentication Protocol)には対応していません。

5.1 認証サーバーの設定項目(Web 認証、MAC 認証)

5.1.1 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 IP 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
}
```

5.1.2 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,
                Access-Defender-Class = 10
user2           Auth-Type = Local, Password = "user2", Calling-Station-Id = "000102030a0b"

000bdbd64209    Auth-Type = Local, Password = "testing123"
                NA-Vlan-Id = 33
```

5.1.3 拡張設定(VLAN ID/クラス ID の設定)

認証成功後に動的に VLAN を変更する場合やクラス ID を割り当てる場合、認証成功時に APRESIA に引き渡す VLAN ID/クラス 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、一般にベンダー独自属性(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/クラス ID を APRESIA に渡します。表 5-1 に認証応答で使用するベンダー独自属性を示します。

表 5-1 認証応答で使用するベンダー独自属性

属性	独自属性の値	動的な VLAN 変更	クラス ID
Vendor-Specific	ベンダーID	278	278
	ベンダー属性番号	192	193
	値	割り当てる VLAN ID	割り当てるクラス ID
	属性の型	整数(INTEGER)	整数(INTEGER)

<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                  APRESIA                 278
BEGIN-VENDOR            APRESIA
ATTRIBUTE               NA-Vlan-Id              192     integer
ATTRIBUTE               Access-Defender-Class   193     integer
END-VENDOR              APRESIA
```

5.2 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(または/etc/raddb)配下に置かれます。

主な設定ファイルは以下です。

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

5.2.1 EAP の設定(eap.conf ファイルなど)

EAP のタイプを指定します。

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
       }
}
```

5.2.2 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 IP アドレスを登録します。シークレットキーは APRESIA と RADIUS サーバーで合わせる必要があります。

<clients.conf ファイルの設定例>

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

5.2.3 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。

5.2.4 拡張設定(VLAN ID/クラス 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と、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(またはグループ)に登録する属性を表 5-2 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(IEEE 802)」と固定値で、「Tunnel-Private-Group-Id」属性値のみ可変値となります。

表 5-2 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(IEEE 802)	固定
Tunnel-Private-Group-Id	トンネルが属するグループ ID	割り当てる VLAN ID、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
```

認証成功後にクラス ID を割り当てる場合は、Web 認証、MAC 認証と同様です。表 5-3 に認証応答で使用するベンダー独自属性を示します。詳細は、5.1.3 拡張設定(VLAN ID/クラス ID の設定)を参照してください。

表 5-3 認証応答で使用するベンダー独自属性

属性	独自属性の値	クラス ID
Vendor-Specific	ベンダーID	278
	ベンダー属性番号	193
	値	割り当てるクラス ID
	属性の型	整数(INTEGER)

5.3 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(分)> (デフォルトは設定なし)

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、すべての 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。

5.4 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 5-4 AccessDefender 機能(Web 認証、MAC 認証)で使用する RADIUS 属性

属性	属性値
User-Name	認証されるユーザー名
User-Password	パスワード
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-IPv6-Address	認証要求している RADIUS クライアントの IPv6 アドレス(リンクローカルアドレス)
NAS-Port	認証端末が接続されているインターフェース番号
NAS-Identifier	認証された端末が属している VLAN ID
Calling-Station-Id	認証端末の MAC アドレス

表 5-5 802.1X 機能で使用する RADIUS 属性

属性	属性値
User-Name	認証されるユーザー名
Service-Type	提供するサービスタイプ(Framed-User(2)固定)
Framed-MTU	サプリカントとオーセンティケーター間の最大フレームサイズ(1452 固定)
NAS-IP-Address	認証要求しているオーセンティケーターの IP アドレス
NAS-IPv6-Address	認証要求しているオーセンティケーターの IPv6 アドレス(リンクローカルアドレス)
NAS-Port	サプリカントが接続されているオーセンティケーターのインターフェース番号
NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ(Ethernet(15)固定)
Calling-Station-Id	サプリカントの 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	オーセンティケーターと 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(IEEE 802(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 VLAN ID、または VLAN 名称)

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

このセクションの内容はサポート対象外となります。

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)。

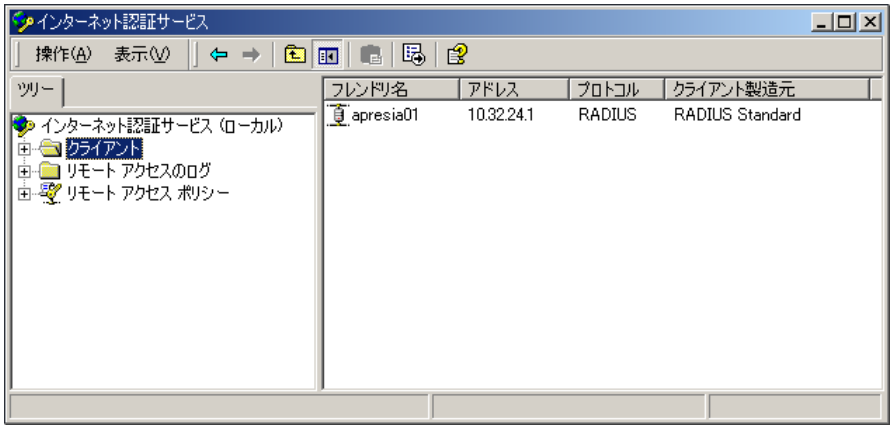


図 5-1 インターネット認証サービス(IAS)設定画面

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、ユーザーのダイヤルイン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。

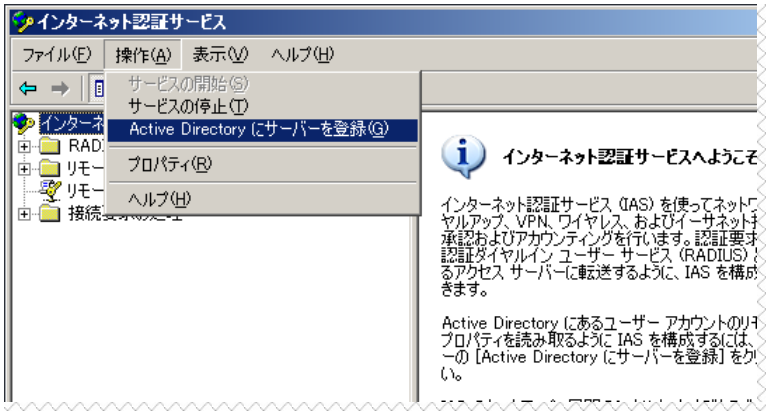


図 5-2 Active Directory にサーバーを登録

5.5.1 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。

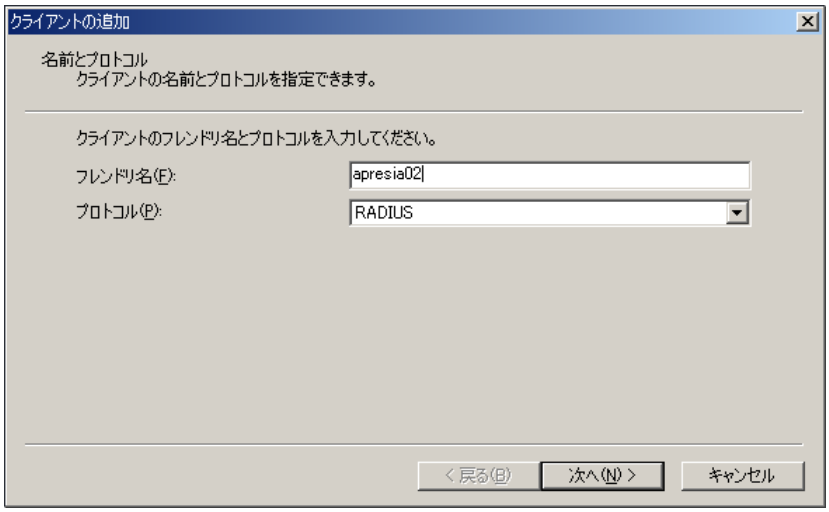


図 5-3 RADIUS クライアントの追加(1)

(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」には APRESIA に設定したシークレットキーを入力してください。入力したら「完了」をクリックし追加終了です。

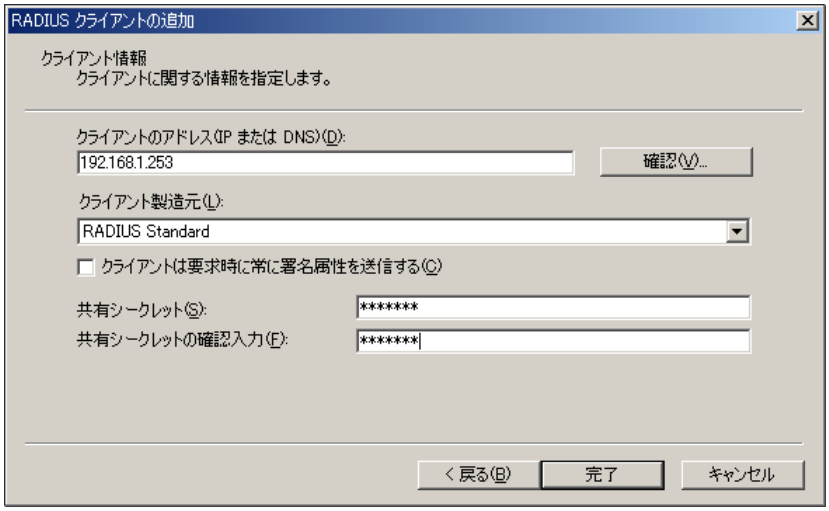


図 5-4 RADIUS クライアントの追加(2)

5.5.2 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、あらかじめ Active Directory のユーザーデータベース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」を選択してください。表示されるウィンドウ内の「ポリシーのフレンドリ名」に適当な文字列を入力します。

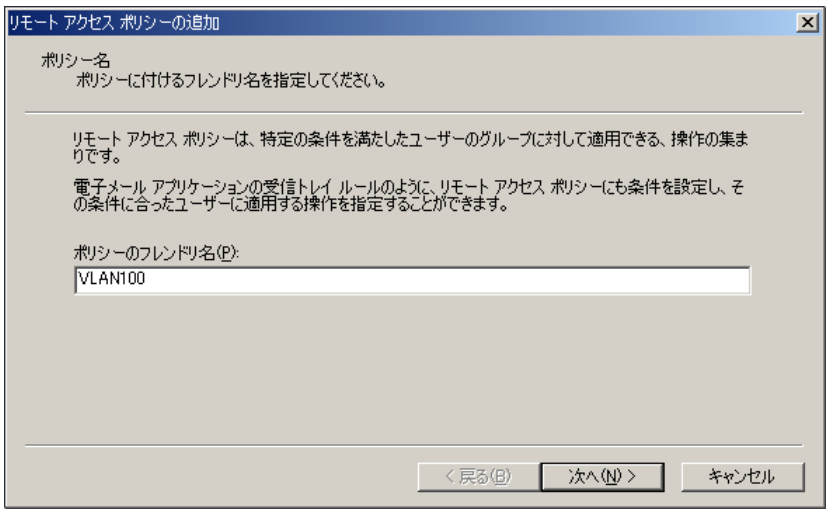


図 5-5 リモートアクセスポリシーの設定(1)

(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。

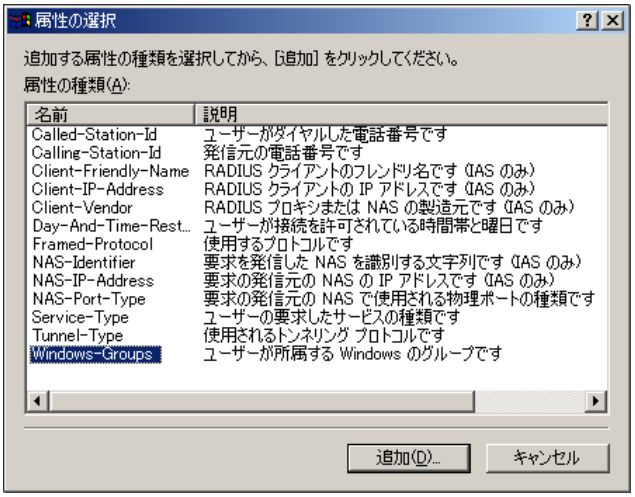


図 5-6 リモートアクセスポリシーの設定(2)

(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。

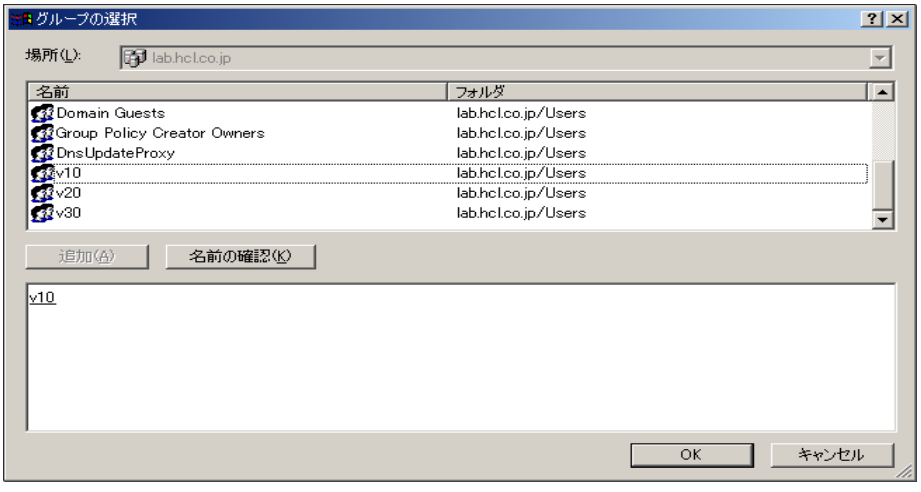


図 5-7 リモートアクセスポリシーの設定(3)

(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。

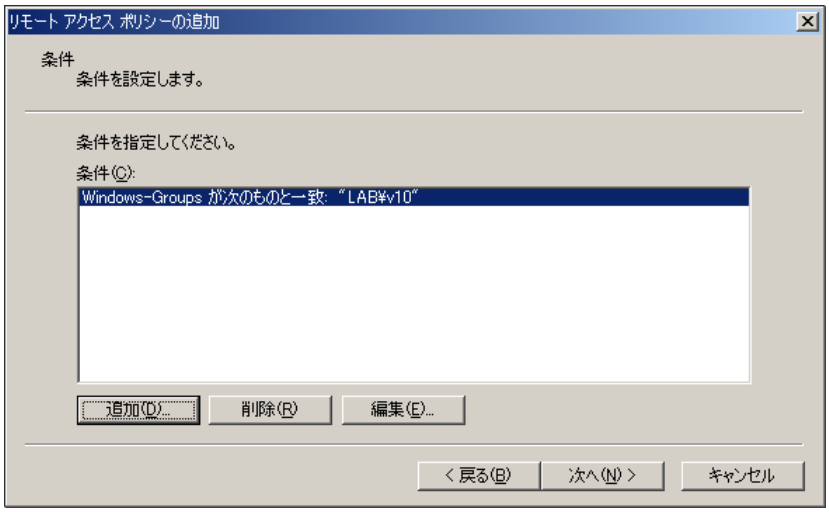


図 5-8 リモートアクセスポリシーの設定(4)

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

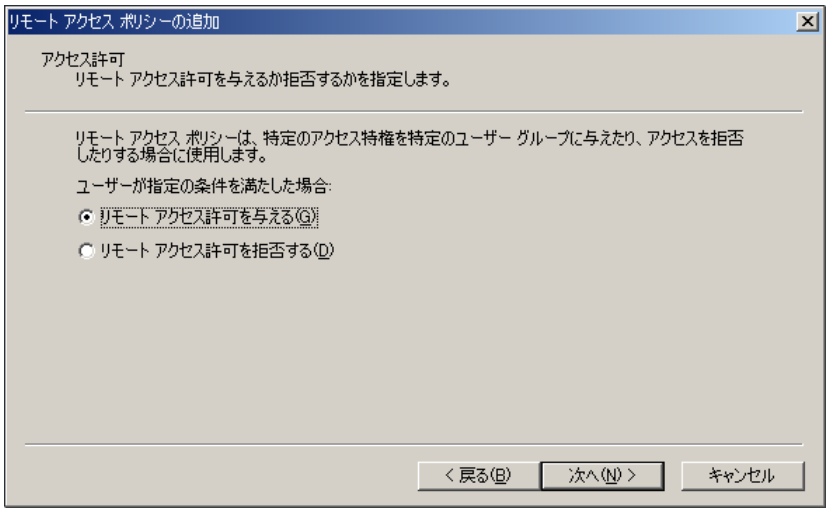


図 5-9 リモートアクセスポリシーの設定(5)

(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。

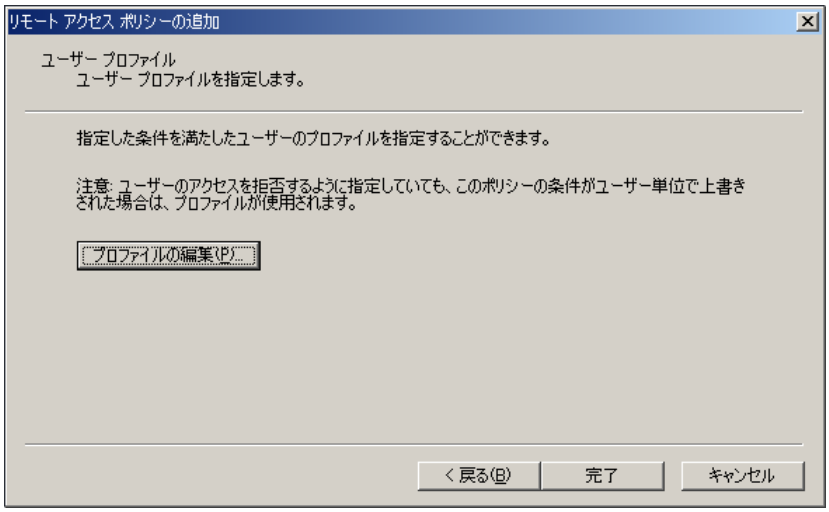


図 5-10 リモートアクセスポリシーの設定(6)

(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。

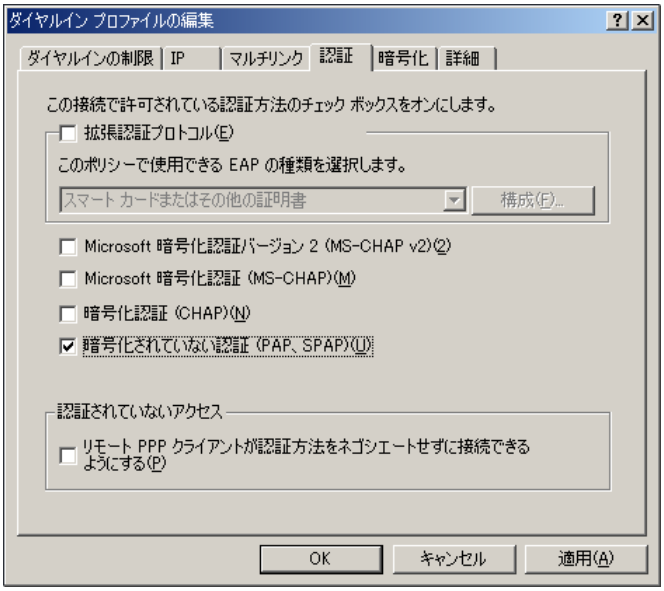


図 5-11 リモートアクセスポリシーの設定(7)

(8) 「OK」をクリックすると図 5-10 の画面に戻りますが、その前に以下の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 5-10 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。

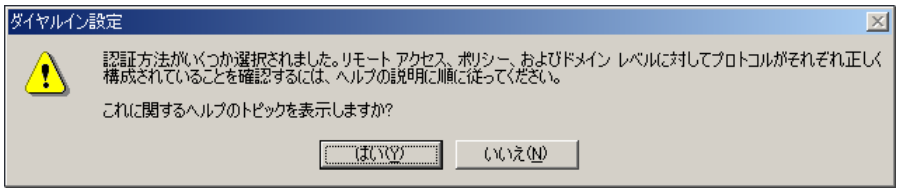


図 5-12 リモートアクセスポリシーの設定(8)

5.5.3 VSA の設定(VLAN ID/クラス ID 変更時のみ必要)

VLAN ID/クラス ID を格納するベンダー独自属性(VSA：Vendor-Specific Attribute)を設定します。

(1) 図 5-11 の画面上で「詳細」タブを選択し、「追加」をクリックします。

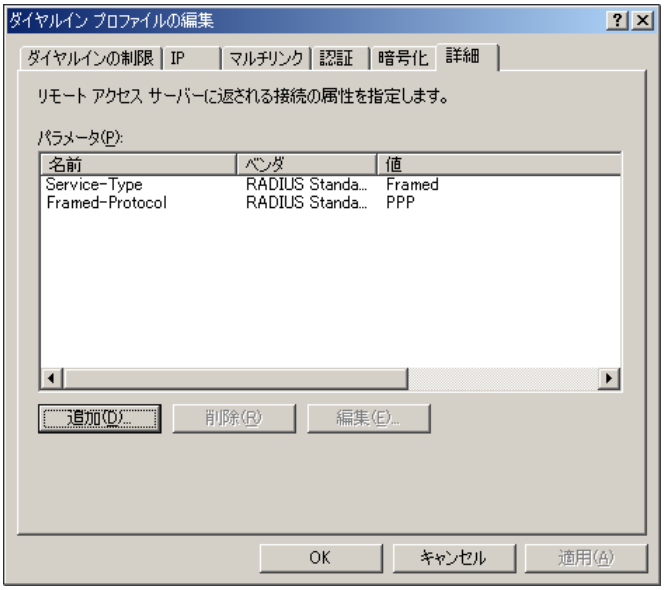


図 5-13 Vendor-Specific Attribute の設定(1)

(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。

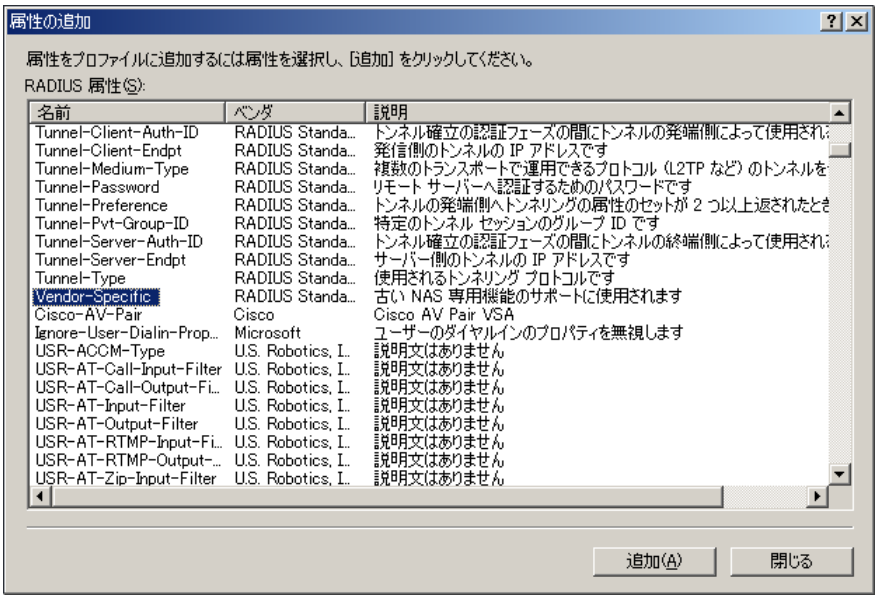


図 5-14 Vendor-Specific Attribute の設定(2)

(3) 複数値の属性情報画面で「追加」をクリックします。

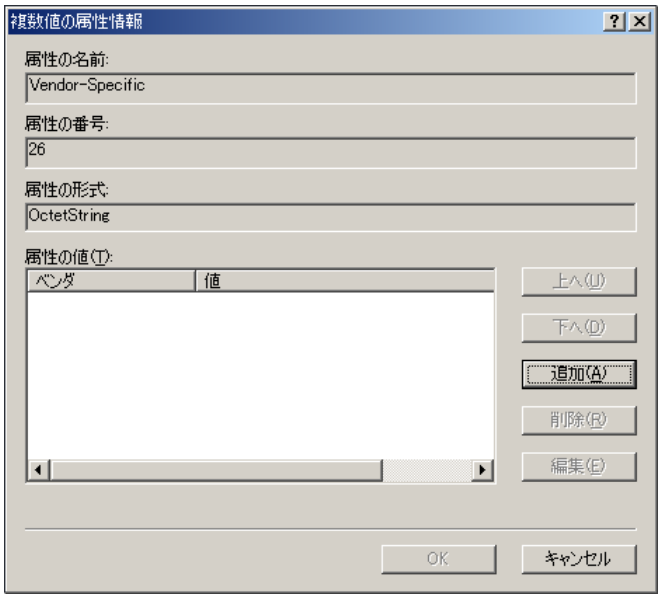


図 5-15 Vendor-Specific Attribute の設定(3)

(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」欄に弊社のベンダーコード「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。

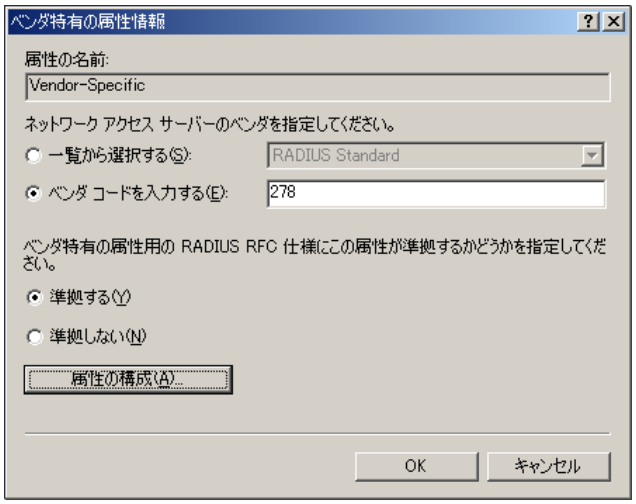


図 5-16 Vendor-Specific Attribute の設定(4)

(5) RFC 準拠の VSA の構成画面で、VLAN ID を設定する場合、「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。クラス ID を設定する場合、「ベンダが割り当てた属性の番号」欄に「193」、「属性の形式」に「10 進」を選択し、「属性の値」欄に APRESIA に引き渡すクラス ID を入力します。

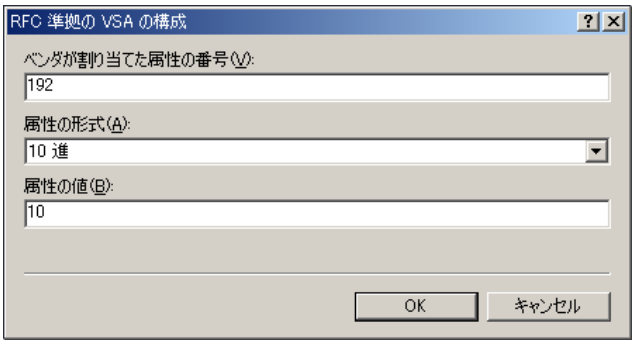


図 5-17 Vendor-Specific Attribute の設定(5)

(6) 図 5-15 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。

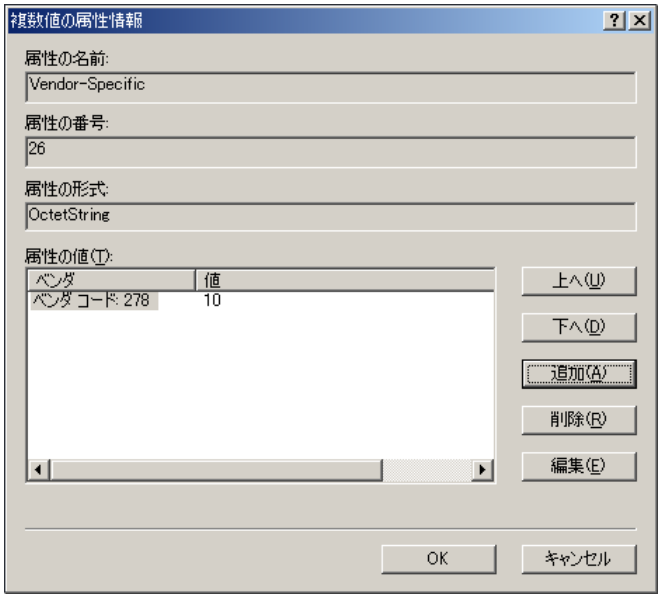


図 5-18 Vendor-Specific Attribute の設定(6)

(7) 図 5-13 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。

5.6 RADIUS サーバー設定例(Windows Server 2008)

このセクションの内容はサポート対象外となります。

Windows Server 2008 を使用した場合の設定例を示します。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。

以下コンポーネントは事前にインストールされているものとします。
- Active Directory
- IIS
- Active Directory 証明書サービス(802.1X の TLS 認証に必要)
- NPS (Network Policy Server)

ドメイン名は"win2008-2.com"が設定されているものとします。

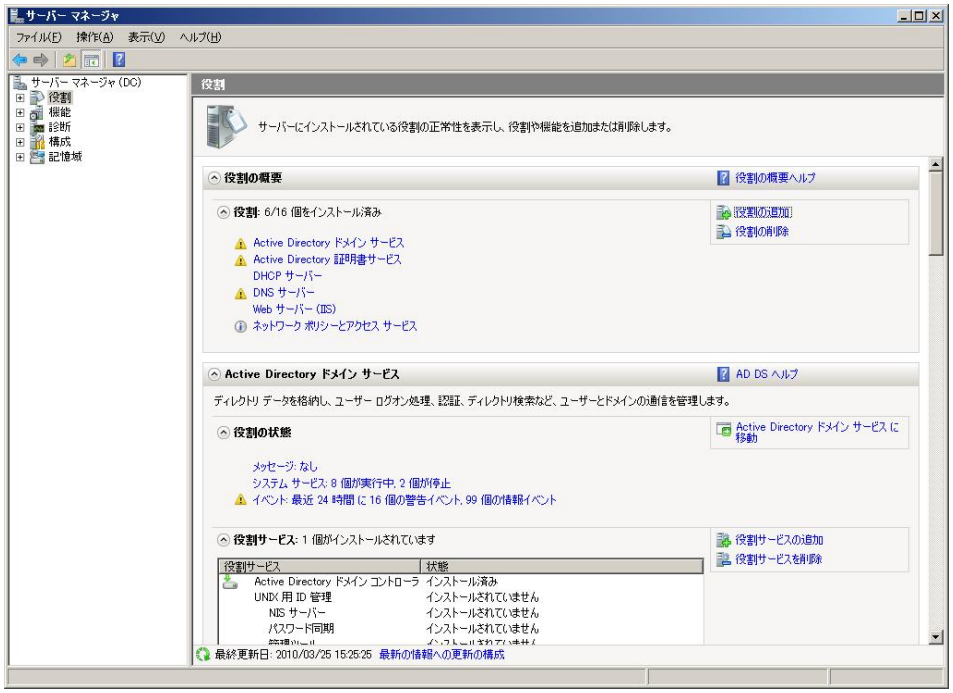


図 5-19 Windows Server 2008 の追加コンポーネントの確認

5.6.1 NPS の設定

NPS を Active Directory サーバーへ登録します。

「スタート」-「管理ツール」-「ネットワークポリシーサーバー」を選択して起動します。
「NPS(ローカル)」を右クリックし、「Active Directory にサーバーを登録」を選択します。

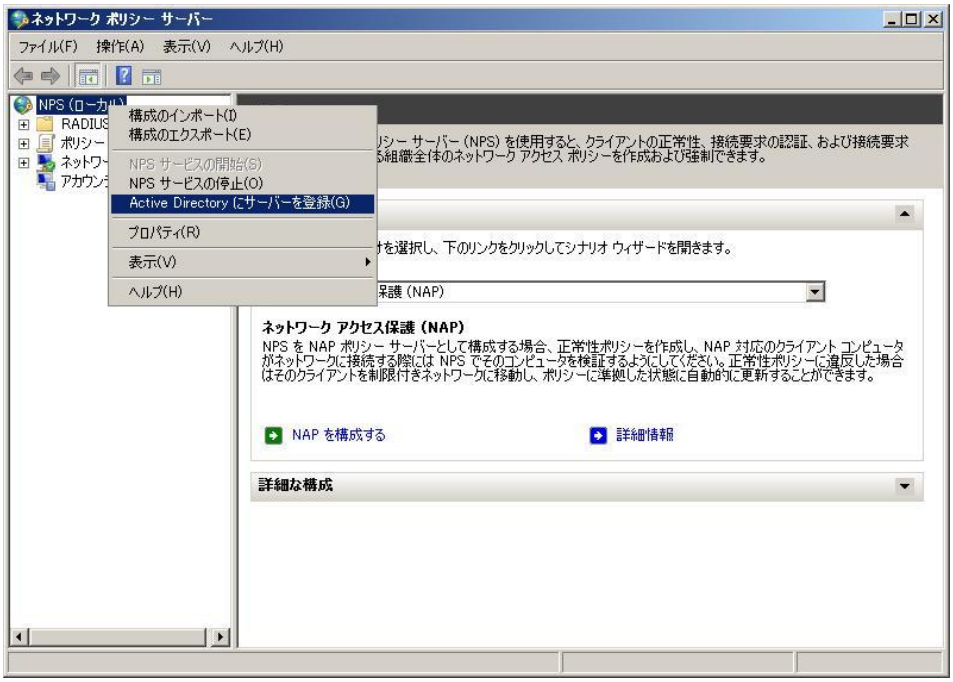
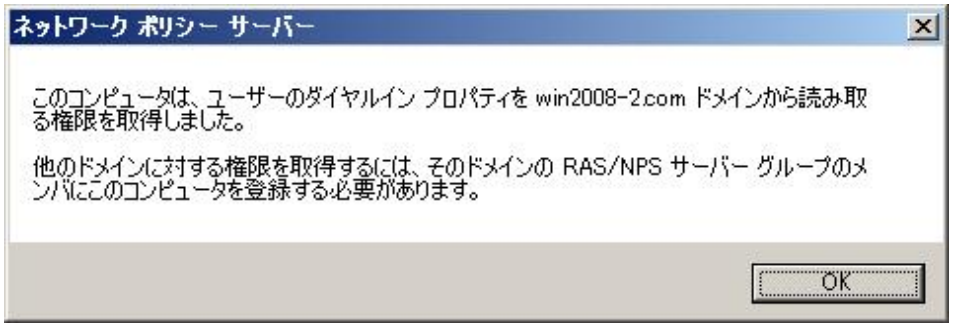


図 5-20 Active Directory へのサーバー登録

以下が表示されるので、「OK」を押します。

続けて以下が表示されるので、「OK」を押します。



5.6.2 RADIUS クライアントの設定

サーバーマネージャ画面より、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) 「サーバーマネージャ」-「役割」-「ネットワークポリシーとアクセスサービス」-「NPS(ローカル)」-「RADIUS クライアントとサーバー」-「RADIUS クライアント」を右クリックし、「新規 RADIUS クライアント」を選択します。

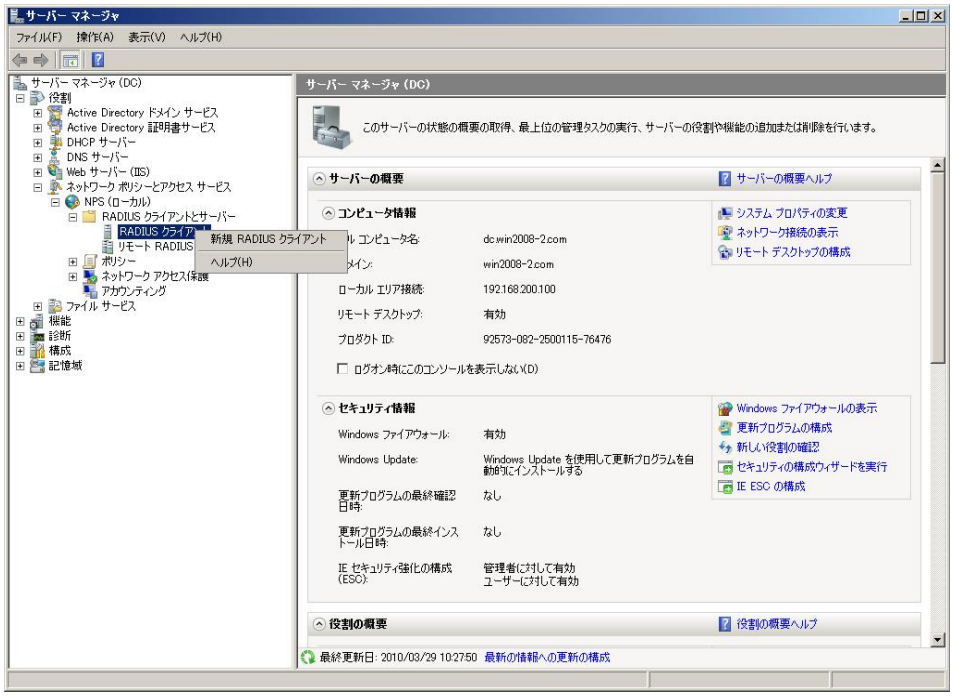


図 5-21 新規 RADIUS クライアントの設定追加

(2) フレンドリ名は例えばAPRESIAのシステム名などを入力し、「アドレス(IP、またはDNS)」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「OK」をクリックし追加終了です。

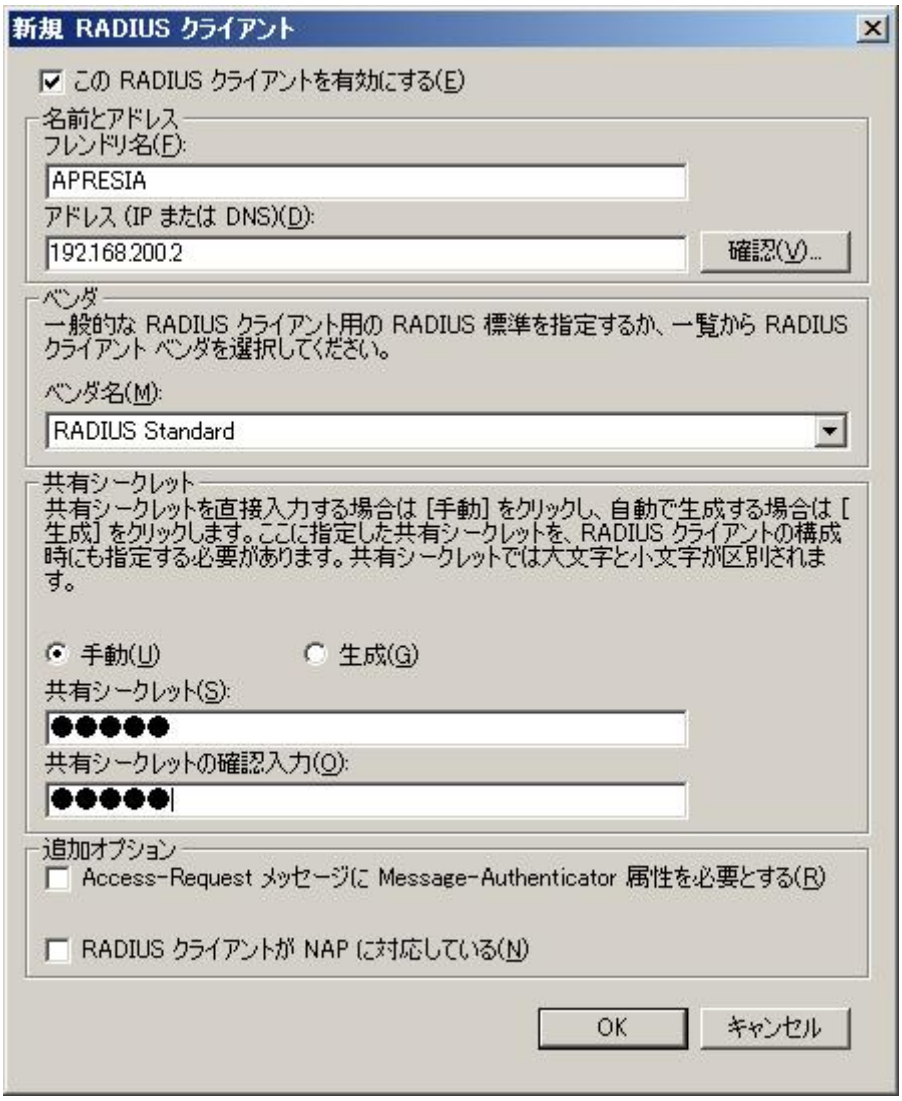


図 5-22 新規RADIUSクライアントの設定

5.6.3 Web認証、MAC認証の設定

Web認証、MAC認証時のWindows Server 2008の設定を示します。

(1) ユーザーの作成

Web認証用のユーザーIDパスワードを設定します。

「サーバーマネージャ」-「Active Directory ドメインサービス」-「Active Directory ユーザーとコンピュータ」-「ドメイン名」-「Users」を選択します。

「Users」で右クリックして、「新規作成」-「ユーザー」を選択します。

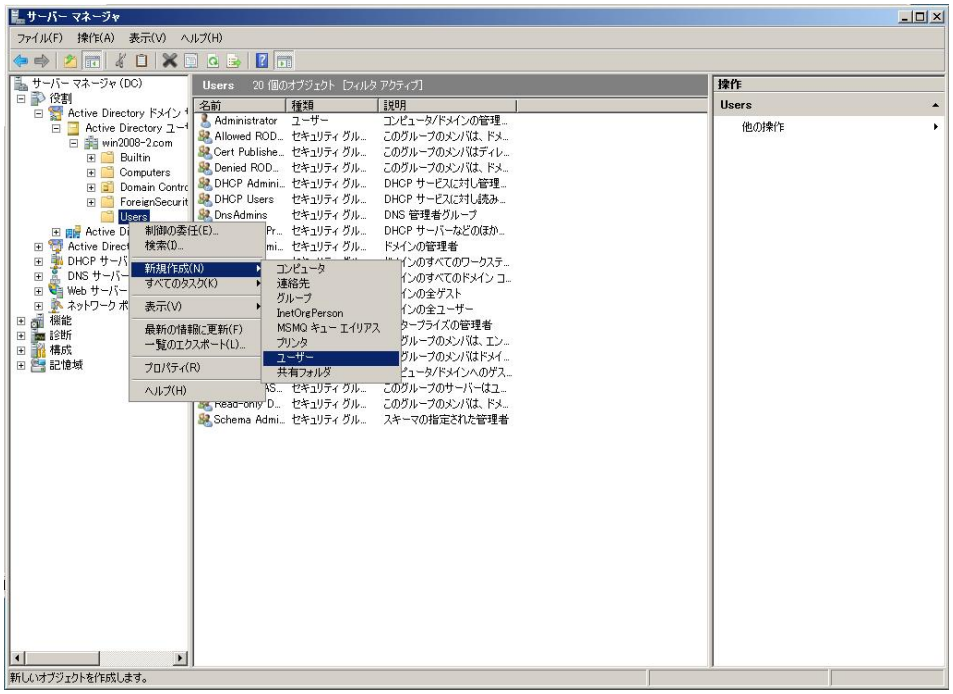


図 5-23 ユーザーの新規作成

(2) ユーザーの作成

「姓」に任意のユーザー名を登録します(ここでは"web"とします)。「姓」を登録すると、「フルネーム」にも同内容が反映されます。

「ユーザーログオン」も「姓」と同一の内容を入力します。

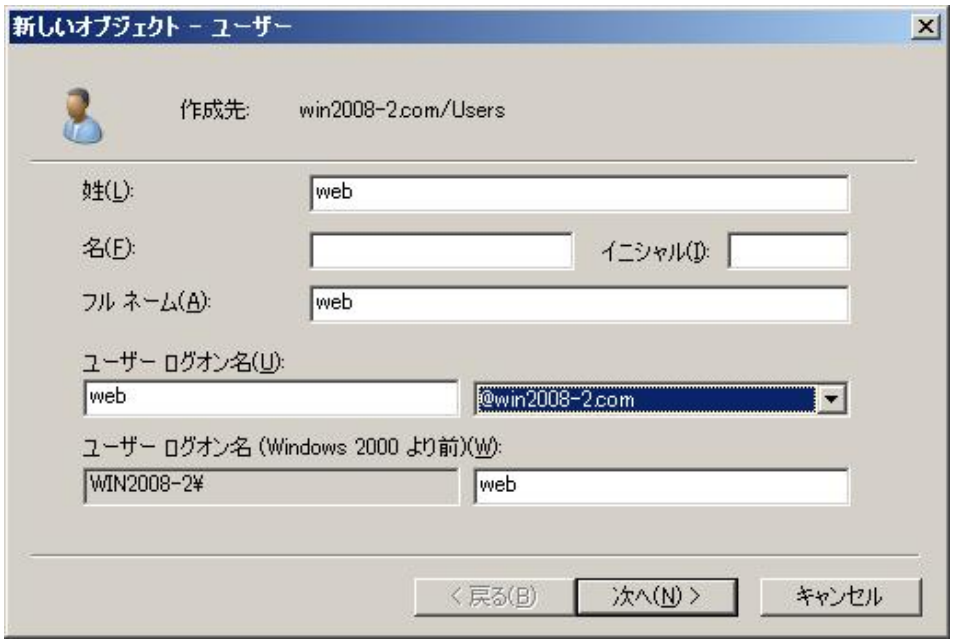


図 5-24 ユーザーの設定

※ MAC 認証の場合は、認証端末の MAC アドレスを設定します。

「00-11-22-33-44-55-66」の場合「00112233445566」で設定します。

(3) パスワードの設定

パスワードを設定します。

MAC 認証の場合は APRESIA で設定したものを指定して、「次へ」を押します。

図 5-25 パスワードの設定

(4) 設定の完了

「完了」を押します。

図 5-26 ユーザー設定の完了

(5) グループの作成

「サーバーマネージャ」-「Active Directory ドメインサービス」-「Active Directory ユーザーとコンピュータ」-「ドメイン名」-「Users」を選択します。

「Users」で右クリックして、「新規作成」-「グループ」を選択します。

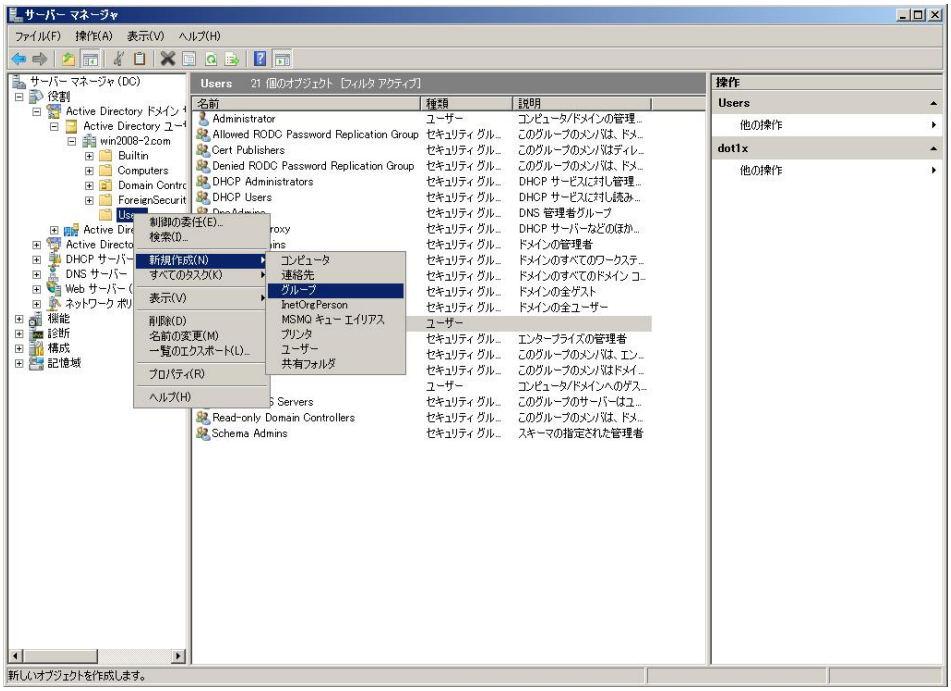


図 5-27 グループの新規作成

(6) グループ名の設定

グループ名(ここでは"WebGroup")を入力して、「OK」を押します。

図 5-28 グループの設定

(7) 所属するグループの設定

「サーバーマネージャ」の右画面にて、作成したユーザーを右クリックしてプロパティを選択します。

「所属するグループ」タブを選択し、「追加」ボタンを押します。

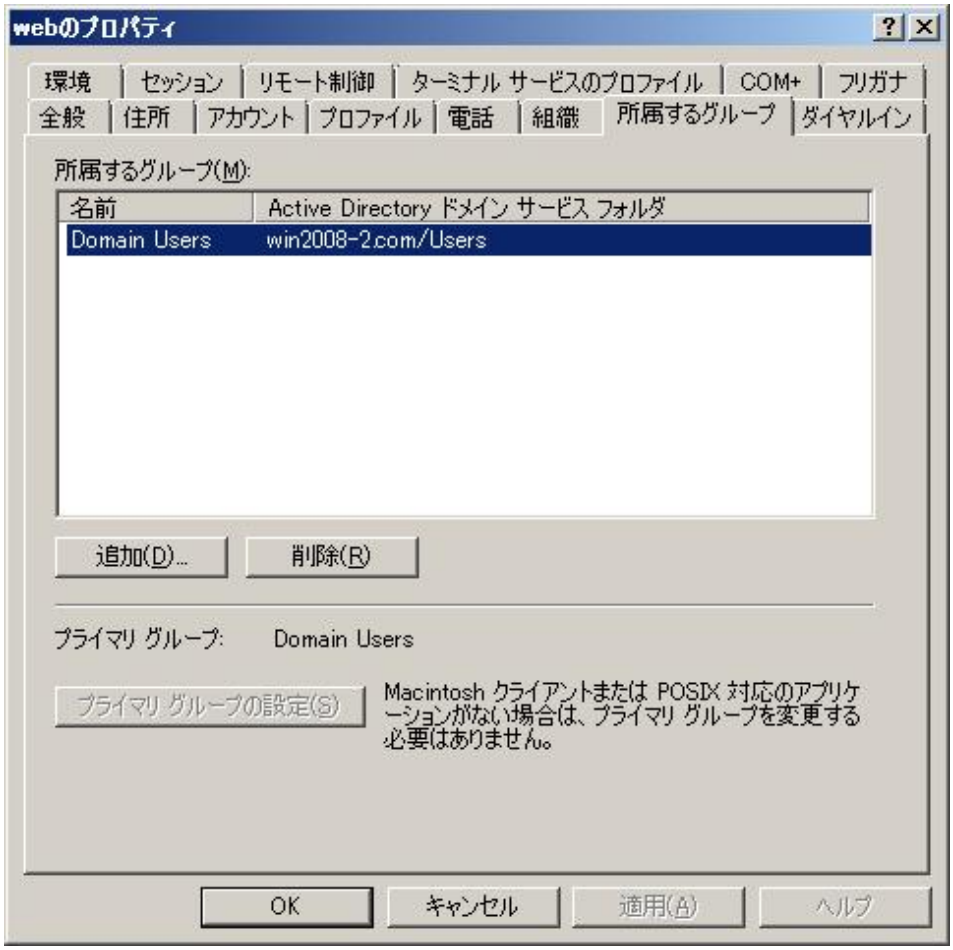


図 5-29 所属するグループの設定

(8) グループの選択

選択するオブジェクト名に、所属させるグループ名(ここでは"WebGroup")を入力して、「名前の確認」ボタンを押すと、以下のような表示になります。

「OK」を押します。

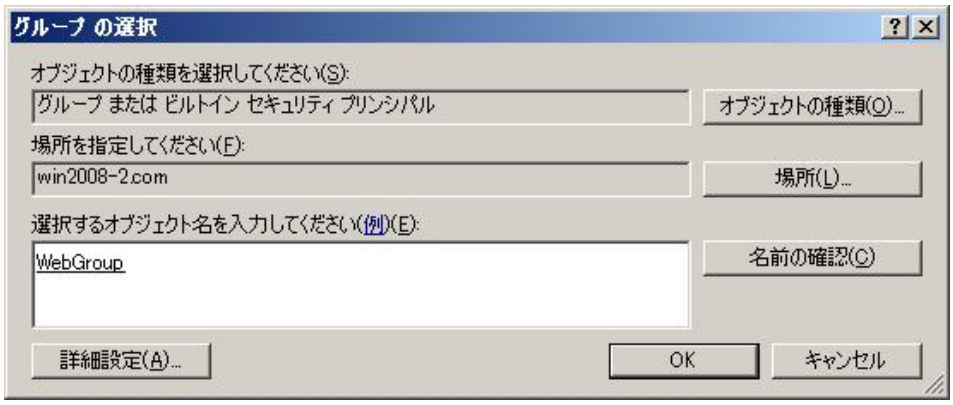


図 5-30 グループの選択

(9) 所属グループ追加確認

「所属するグループ」に指定したグループ("WebGroup")が追加されていることを確認します。

図 5-31 所属グループ追加確認

(10) アクセス許可の設定

「ダイヤルイン」タブを選択して、「リモートアクセス許可」を「アクセス許可」に設定して、「OK」を押します。

図 5-32 アクセス許可の設定

5.6.4 Web 認証、MAC 認証のネットワークポリシー設定

(1) ネットワークポリシーの作成

「サーバーマネージャ」-「役割」-「ネットワークポリシーとアクセスサービス」-「NPS(ローカル)」-「ポリシー」-「ネットワークポリシー」を右クリックして「新規」を選択します。

図 5-33 ネットワークポリシーの新規作成

(2) ポリシー名の設定

任意のポリシー名(ここでは"WebPolicy")を入力して、「次へ」を押します。

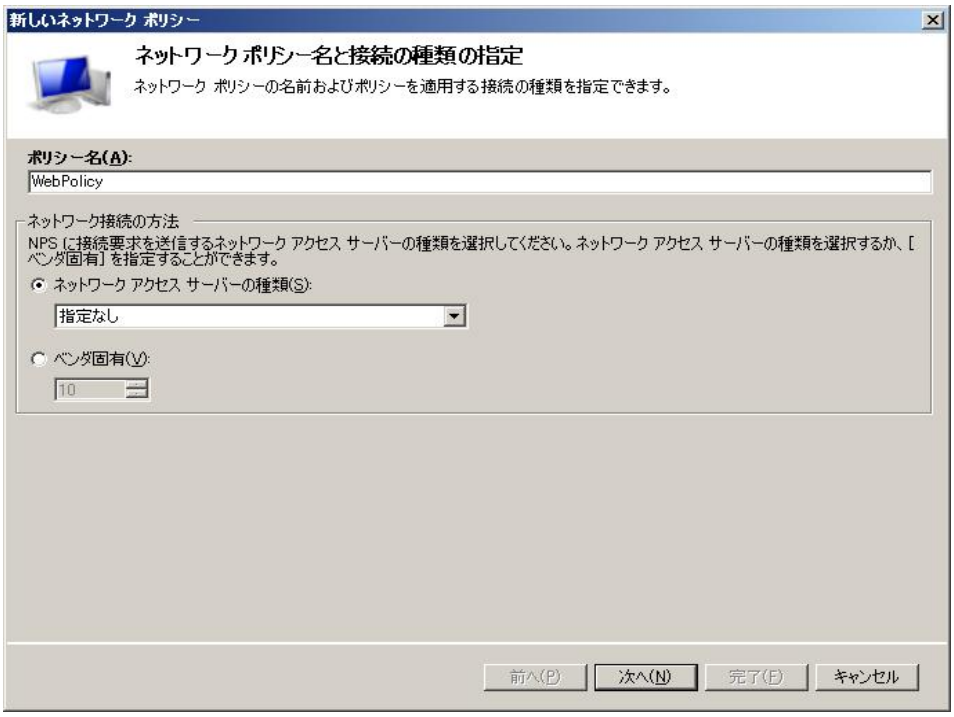


図 5-34 ポリシー名の設定

(3) 条件の指定

「追加」ボタンを押します。

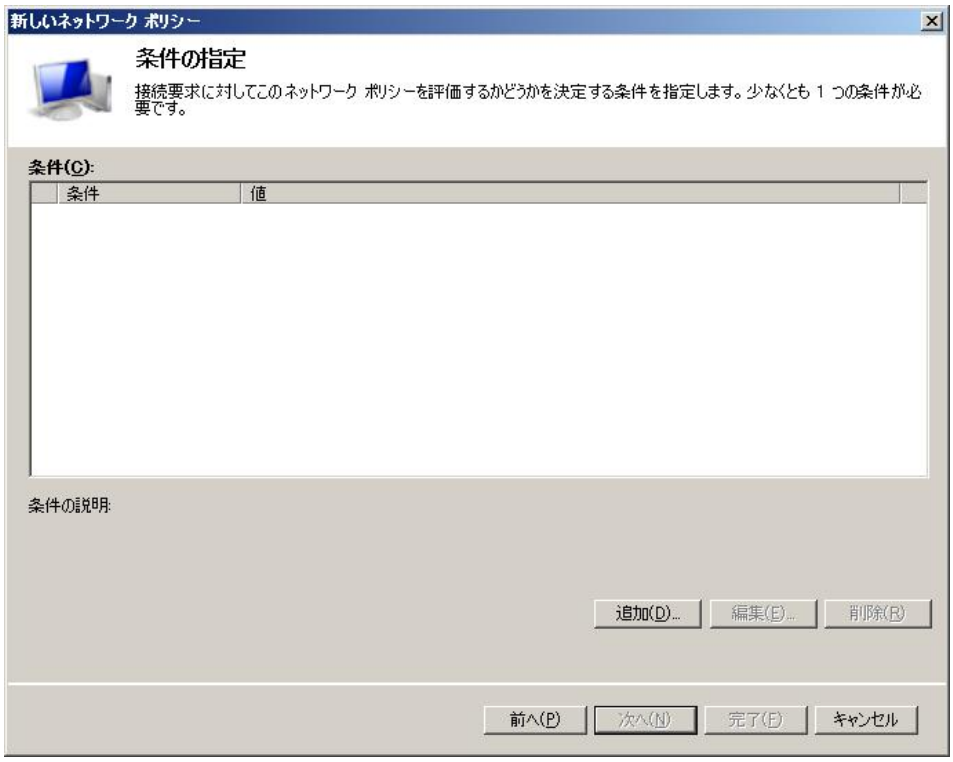


図 5-35 条件の設定

(4) 条件の選択

Windows グループを選択し、「追加」ボタンを押します。

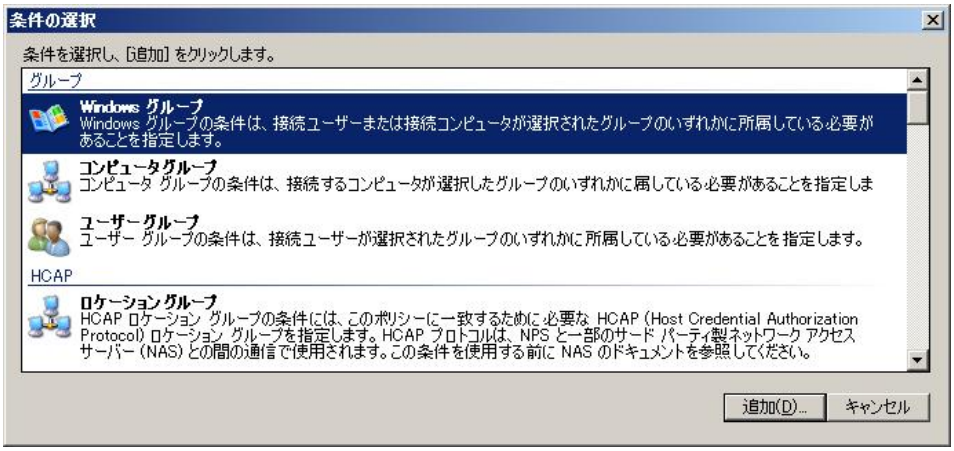


図 5-36 条件の選択

(5) グループの選択

グループ選択画面にて、選択するオブジェクト名に作成したグループ(ここでは"WebGroup")を入力して、「名前の確認」ボタンを押します。

以下の表示になったら、「OK」を押します。

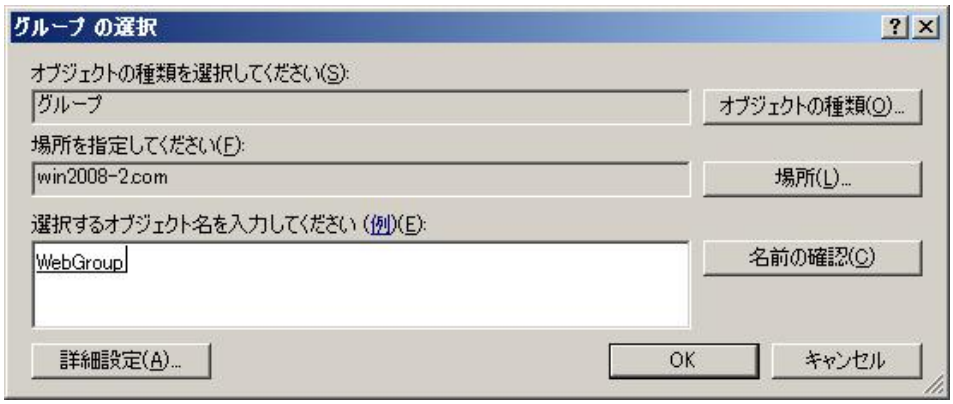


図 5-37 グループの選択

(6) Windows グループの追加確認

Windows グループ画面にて、選択したグループが追加されていることを確認して、「OK」を押します。

図 5-38 Windows グループの確認

(7) 条件指定の確認

設定した内容が反映されていることを確認して、「次へ」を押します。

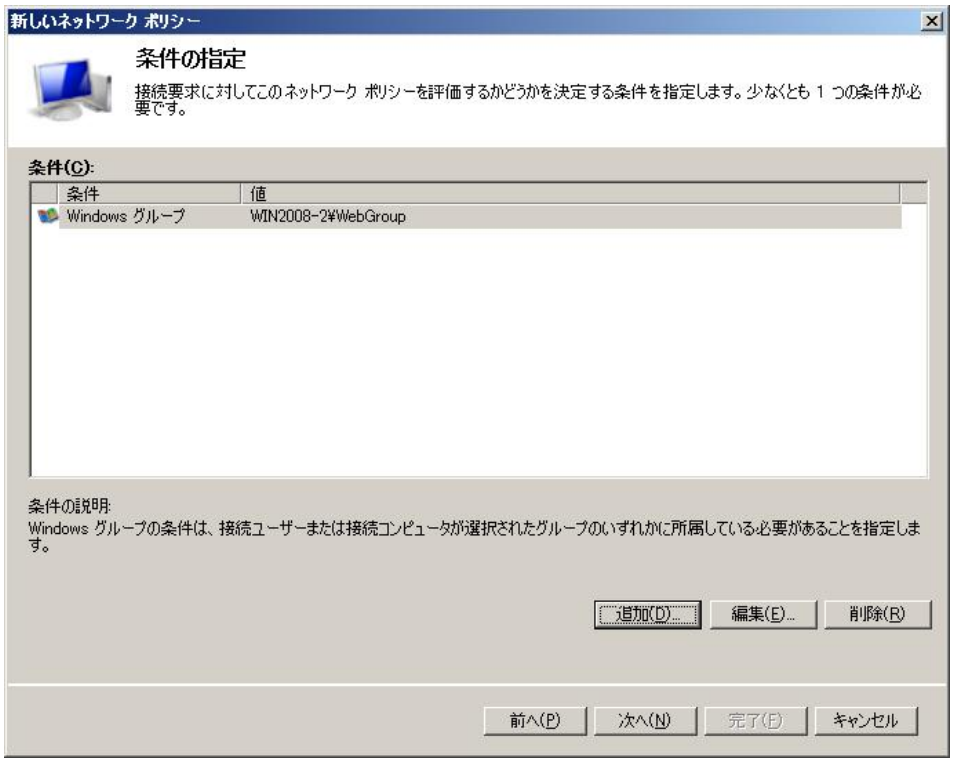


図 5-39 条件指定の確認

(8) アクセス許可の指定

「アクセスを許可する」が選択されていることを確認して、「次へ」を押します。

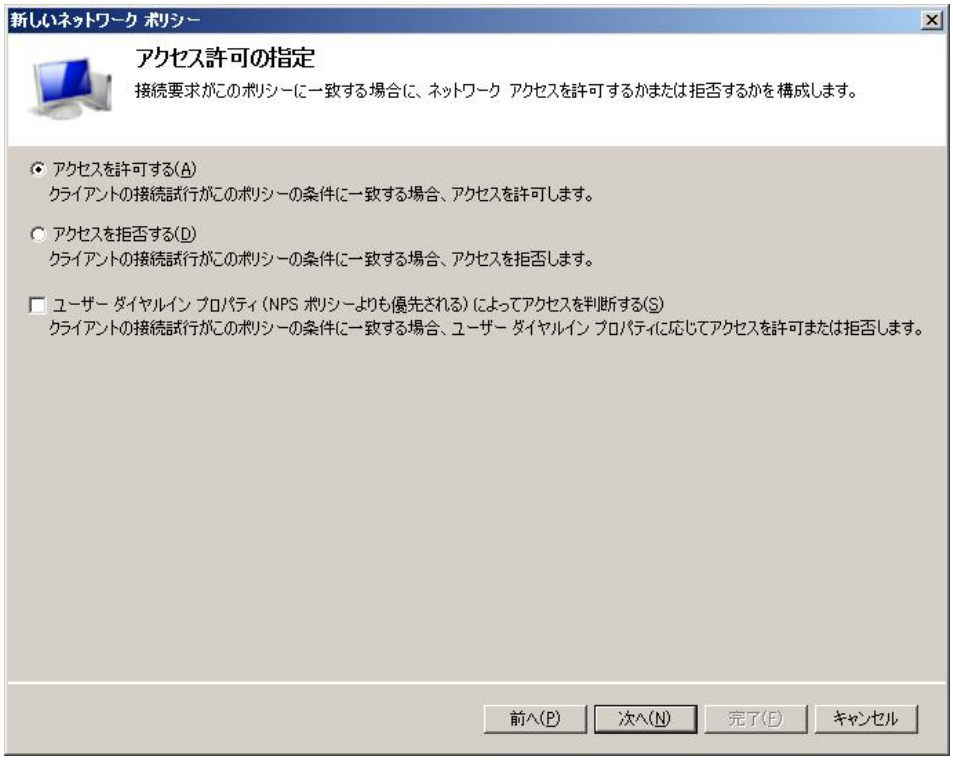


図 5-40 アクセス許可の指定

(9) 認証方法の構成

「暗号化されていない認証(PAP、SNAP)」をチェックして、「次へ」を押します。

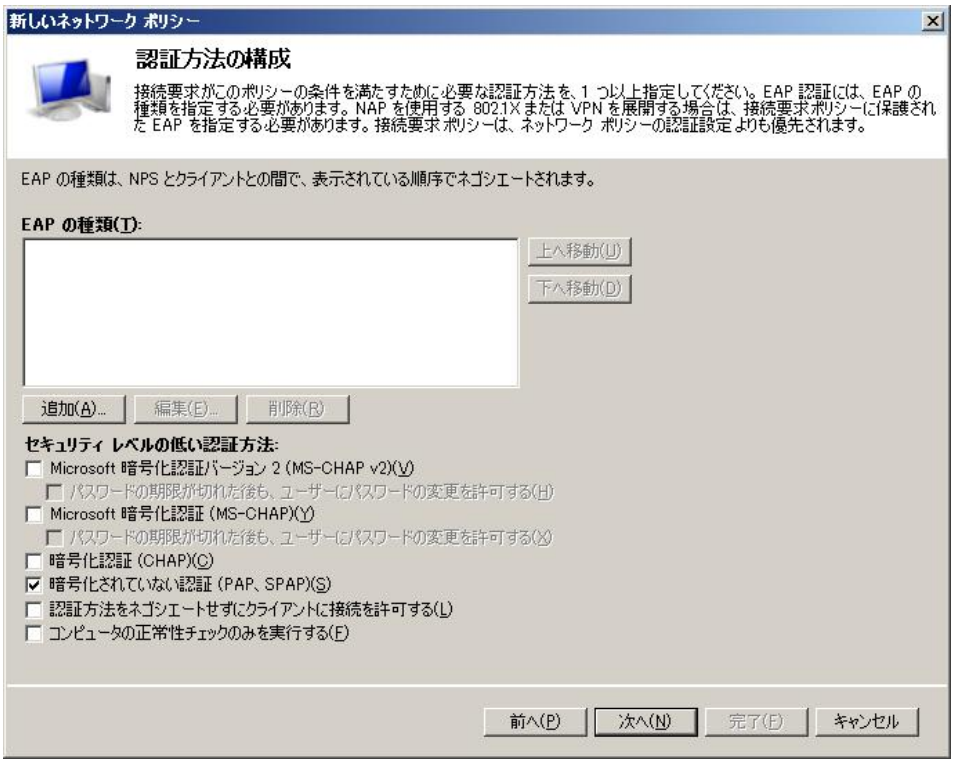
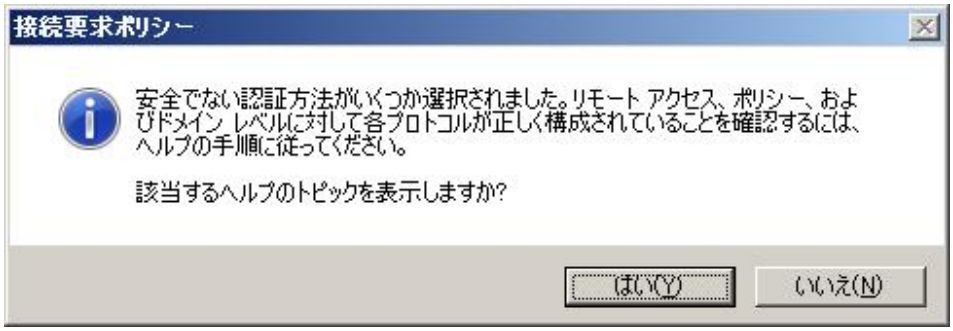


図 5-41 認証方法の構成

以下が表示されるので、「いいえ」を押します。



(10) 制約の構成

「次へ」を押します。

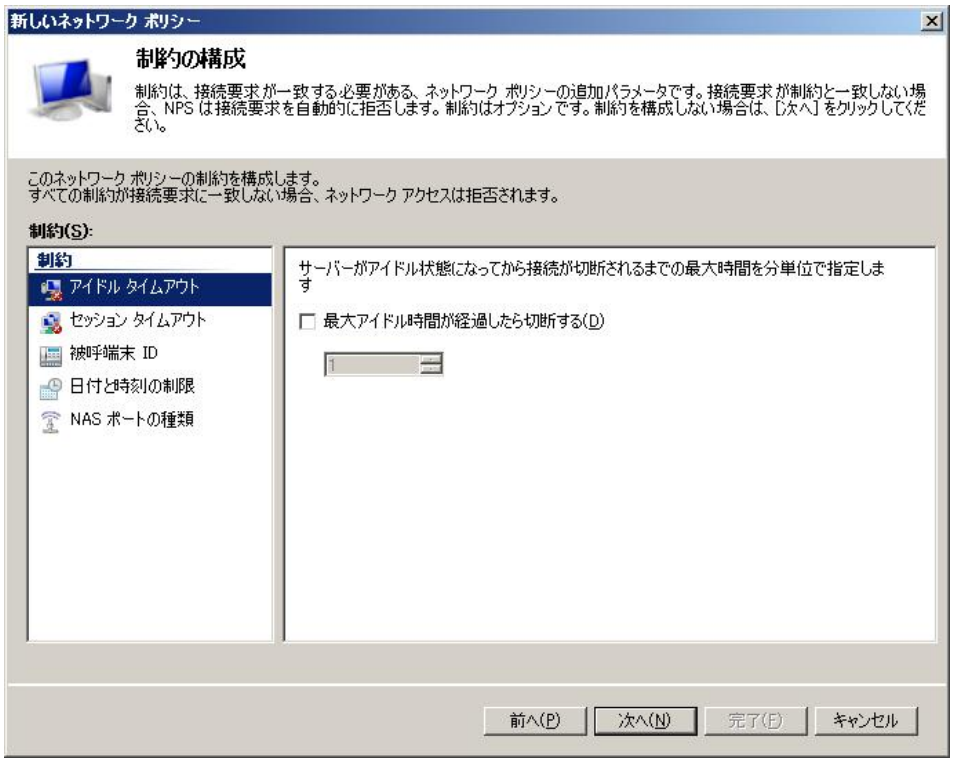


図 5-42 制約の構成

(11)VSA の設定

認証成功後に、動的に VLAN を変更する場合やクラス ID を割り当てる場合は以下を設定します。

「ベンダ固有」を選択して、「追加」ボタンを押します。

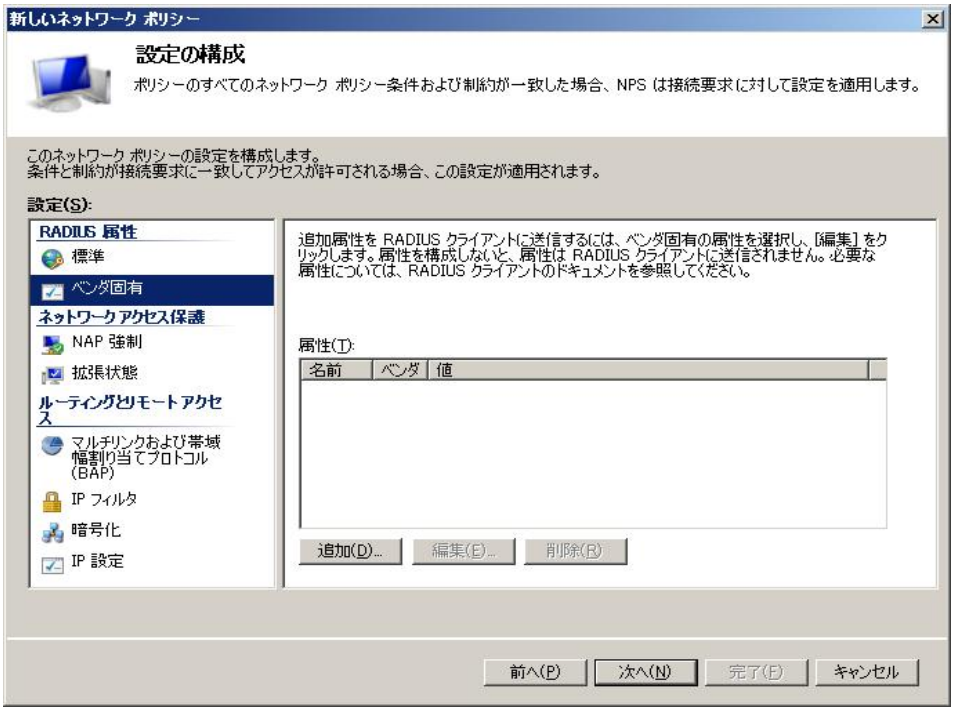


図 5-43 DVLAN の設定

「ベンダ」で「カスタム」を選択します。
「属性」に以下が表示されたことを確認して、「追加」を押します。

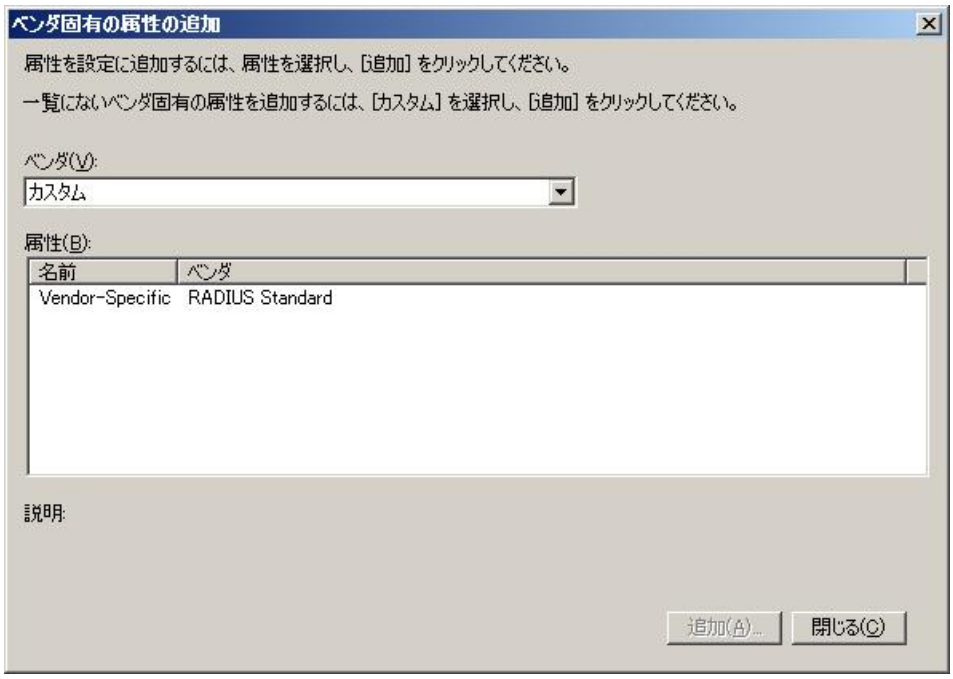


図 5-44 ベンダ固有の属性の追加

VSA の構成
「属性の情報」画面にて「追加」を押します。

図 5-45 属性の情報

「ベンダ固有の属性情報」画面にて、ネットワークアクセスサーバーのベンダーを「ベンダコードを入力する」を選択して、"278"を指定します。

RADIUS RFC のベンダ固有の属性に関する仕様が、準拠するにチェックされていることを確認して、「属性の構成」を押します。

図 5-46 ベンダーコードの入力

「RFC 準拠の VSA の構成」画面にて以下を設定します。

[VLAN ID]

- ベンダが割り当てた属性の番号：192(固定)
- 属性の形式：10 進数
- 属性値：認証成功後に割り当てる VLAN ID

[クラス ID]

- ベンダが割り当てた属性の番号：193(固定)
- 属性の形式：10 進数
- 属性値：認証成功後に割り当てるクラス ID

以上を設定後、「OK」を押します。

図 5-47 属性番号の設定

以下追加されていることを確認して、「OK」を押します。

「ベンダ固有の属性追加」画面で「閉じる」を押します。

図 5-48 VSA 設定の確認

以下追加されていることを確認して、「次へ」を押します。

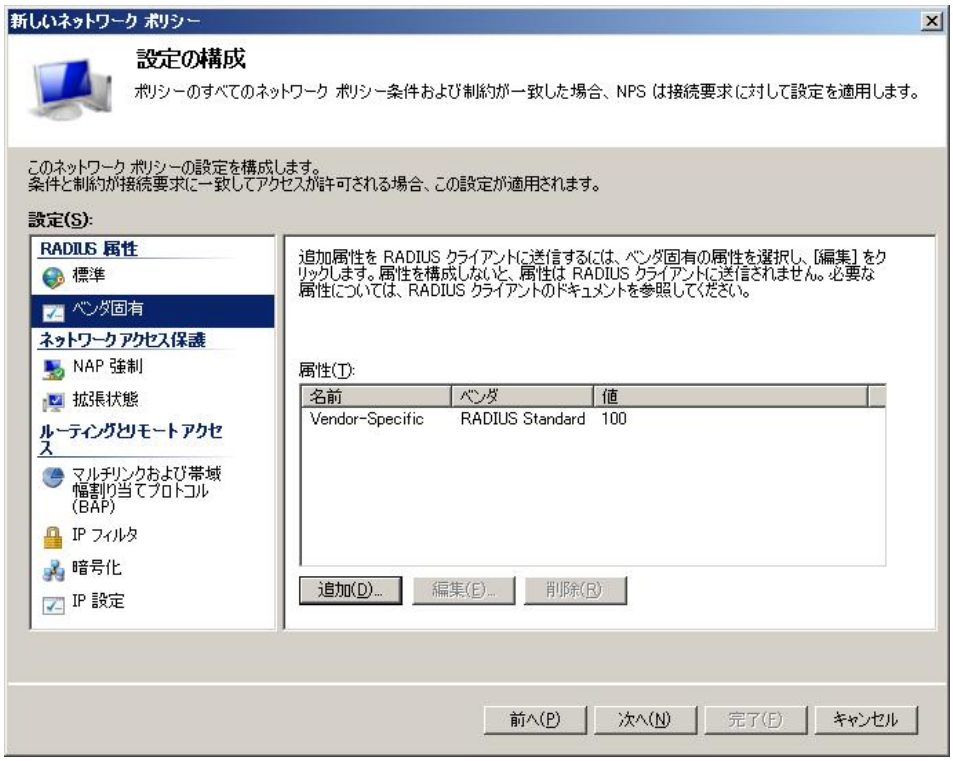


図 5-49 設定の構成

「OK」を押します。

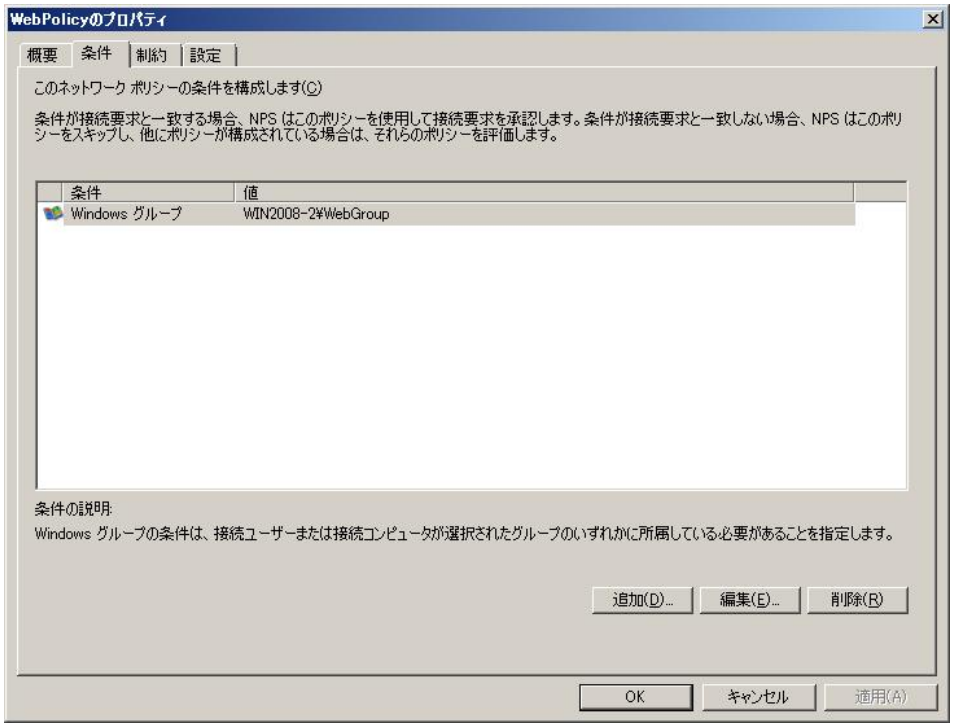


図 5-50 ポリシー設定の確認

(12) 設定した内容を確認して、「完了」を押します。

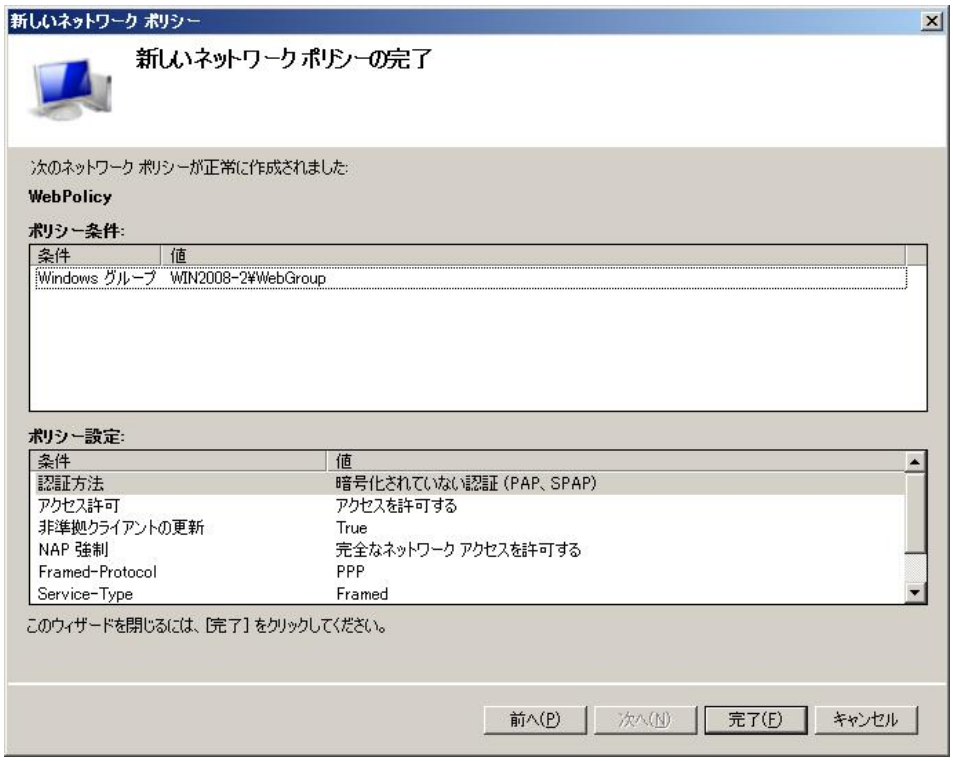


図 5-51 ポリシー設定の完了

(13) ネットワークポリシーの確認

サーバーマネージャ画面にて、新しいポリシーが反映されていることを確認します。

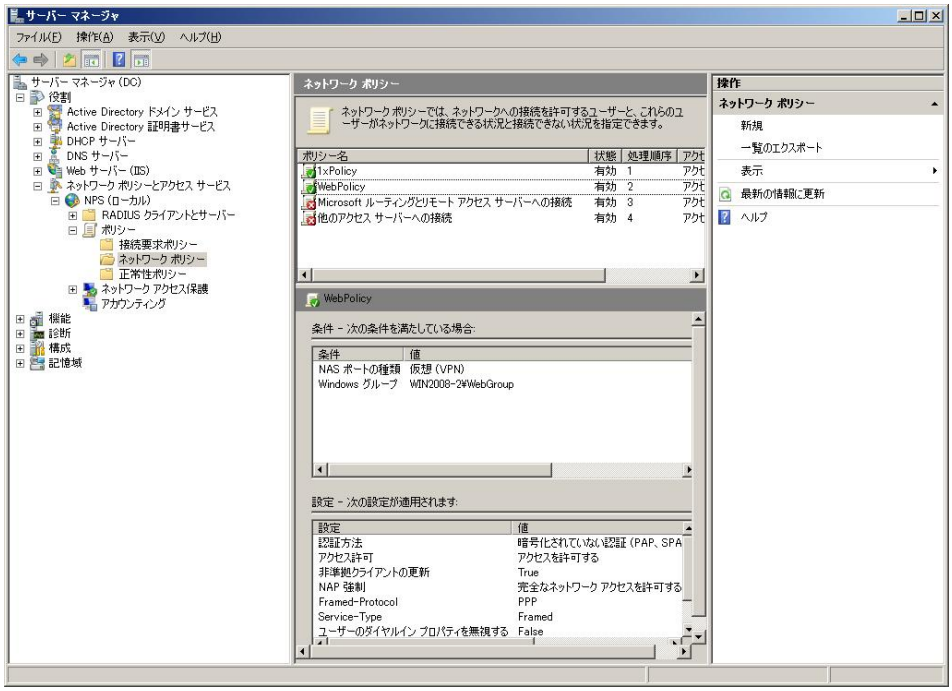


図 5-52 ポリシー追加の確認

(14) 接続要求ポリシーの設定

「サーバーマネージャ」-「役割」-「ネットワークポリシーとアクセスサービス」-「NPS(ローカル)」-「ポリシー」-「接続要求ポリシー」を選択後、右画面にて「すべてのユーザーに Windows 認証を使用」を右クリックして、「プロパティ」を選択します。

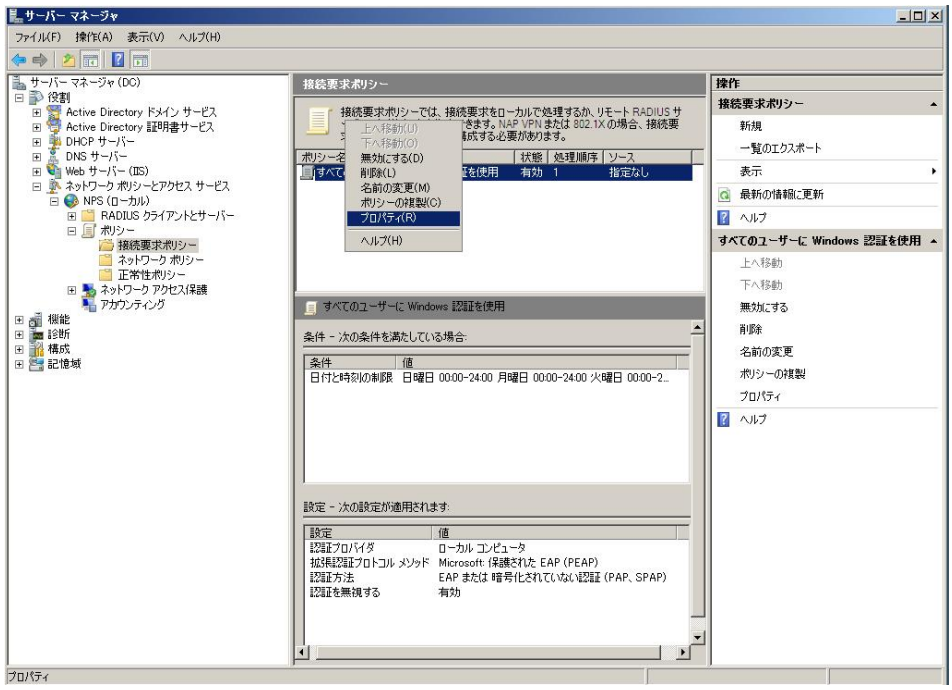


図 5-53 接続要求ポリシーの設定

「設定」タブを選択して、「暗号化されていない認証(PAP、SNAP)」にチェックをつけ、「OK」を押します。

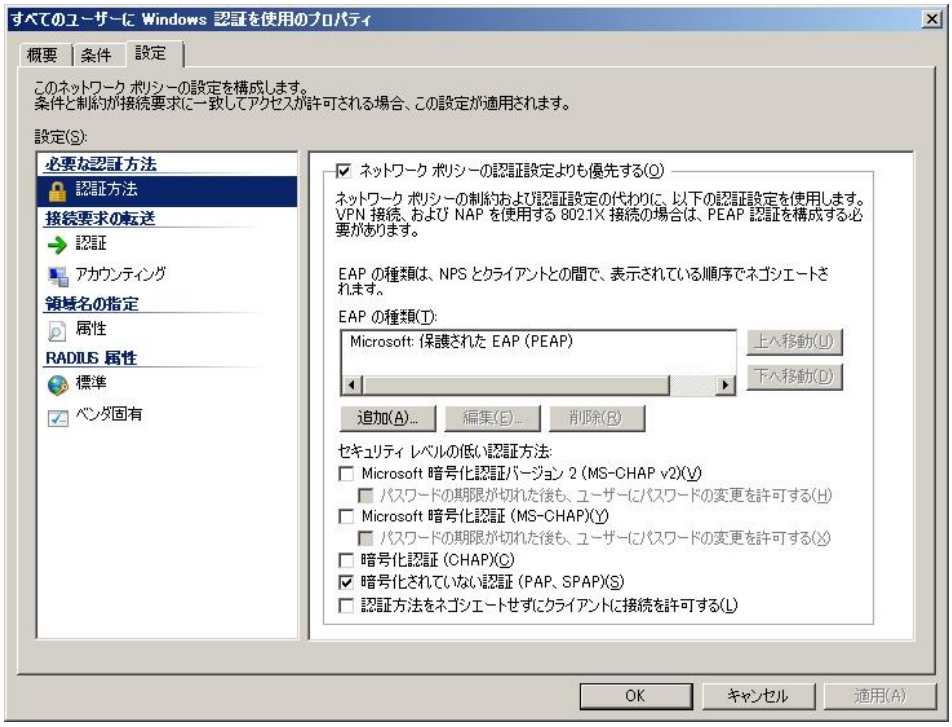


図 5-54 許可する認証方法の設定

5.6.5 認証クライアントのドメイン参加

Windows 7 を例に認証クライアントのドメイン参加手順を示します。

ドメインコントローラと通信可能なネットワークにクライアント PC を接続し、通信可能な TCP/IP の設定をします。有線 DNS サーバーにはドメインコントローラの IP アドレスを設定します。

認証クライアントにて、「スタート」-「コンピューター」のプロパティを開き、「設定の変更」を選択します。

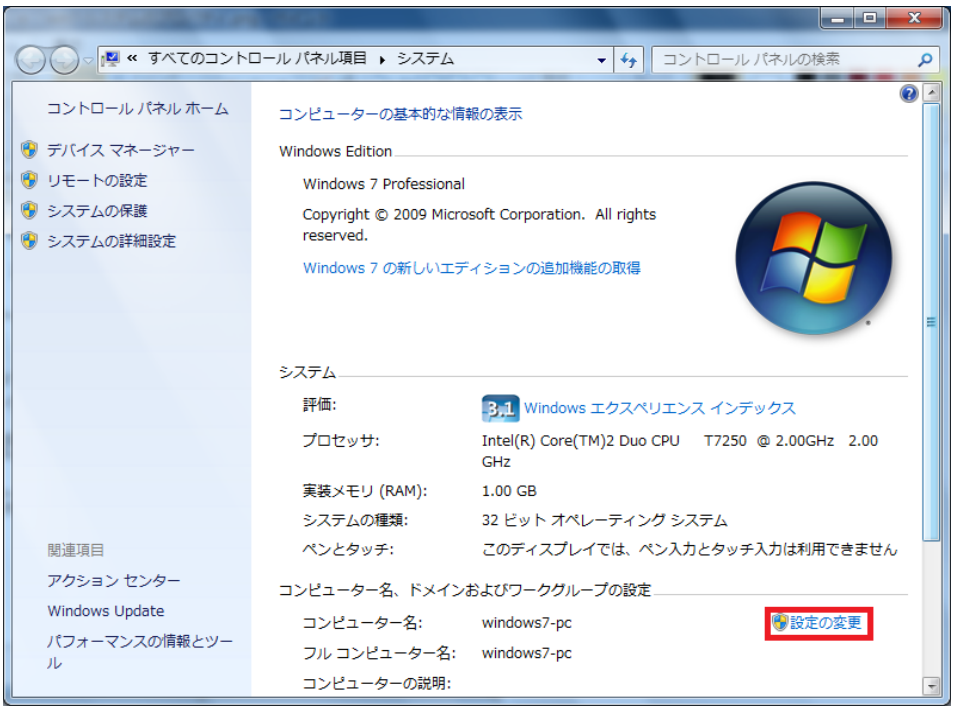


図 5-55 クライアントのシステム画面

「コンピューター名」タブを選択して、「変更」ボタンを押します。

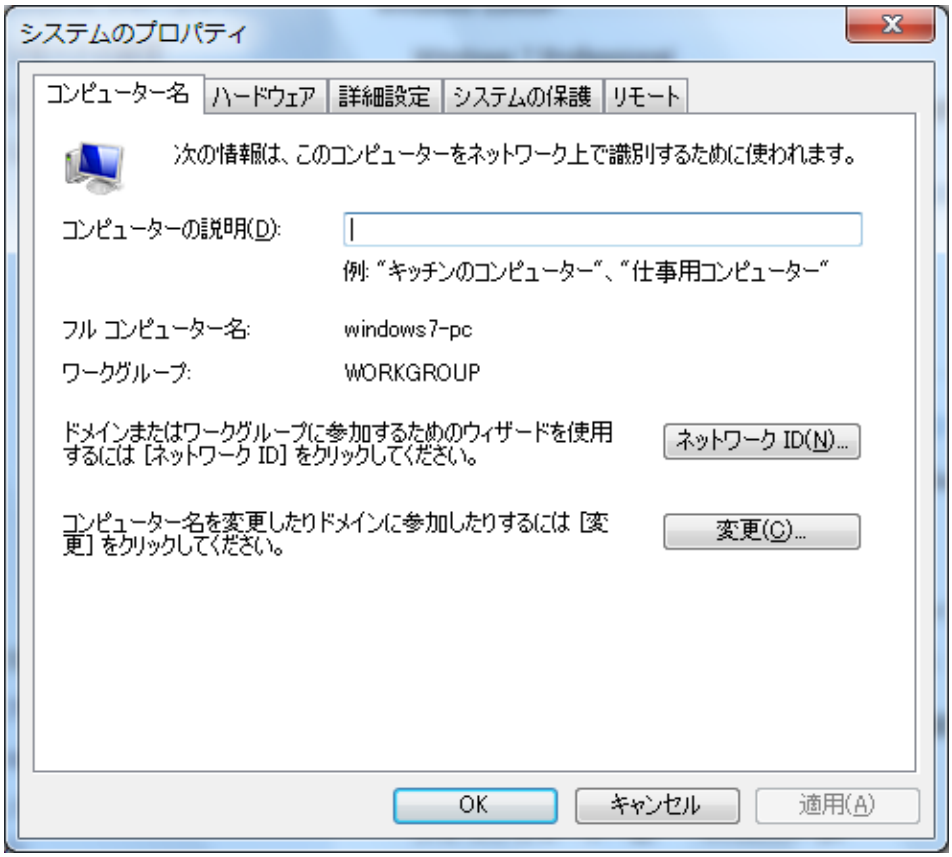


図 5-56 システムのプロパティ

「コンピューター名/ドメイン名の変更」画面にて、所属するグループで「ドメイン」を選択して、「OK」を押します。

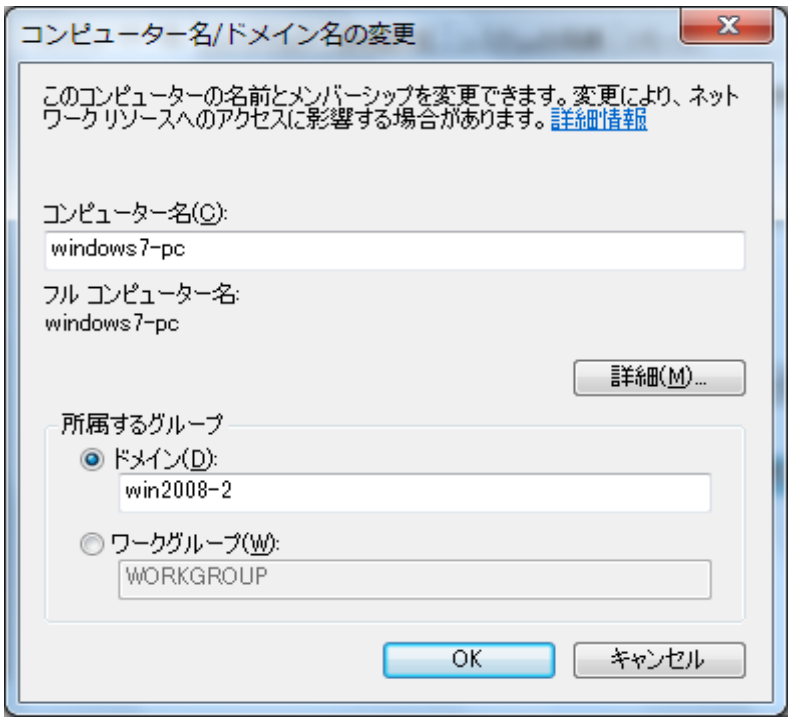


図 5-57 ドメイン名の設定

「Windows セキュリティ」画面が表示され、ドメインに参加するためのアカウント/パスワードが求められるので、5.6.3 で設定した Web 認証用のユーザー/パスワードを入力して、「OK」を押します。

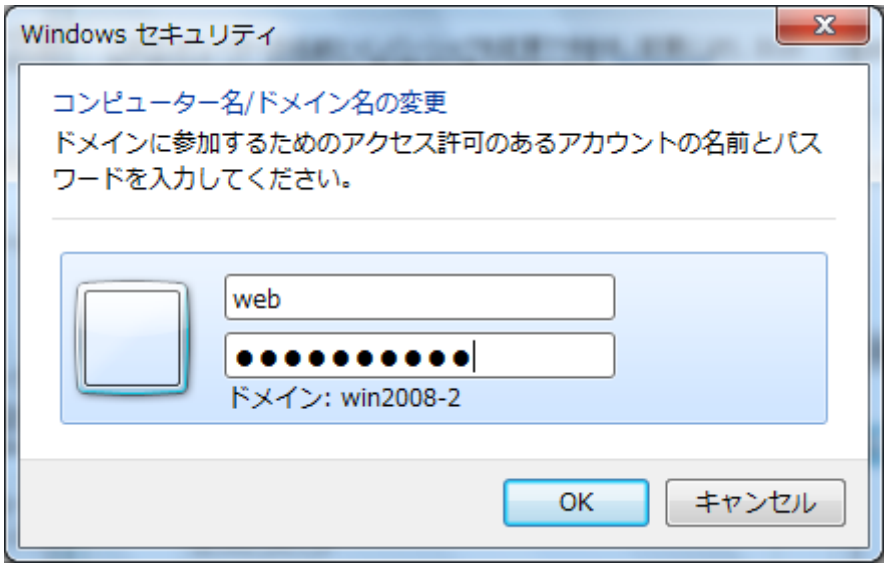


図 5-58 認証

ドメイン参加が成功した場合、以下が表示されます。

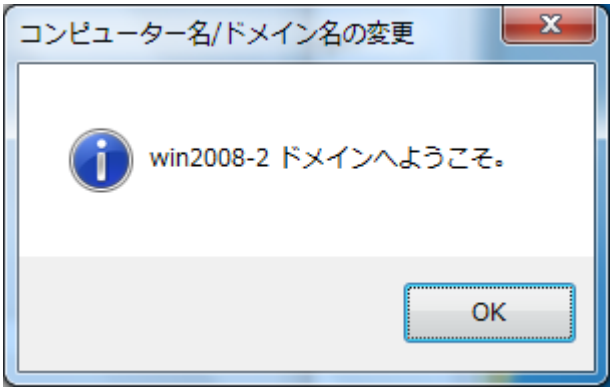


図 5-59 認証の成功

認証クライアントを再起動後、ログオン画面にて「ユーザーの切り替え」-「他のユーザー」を選択します。ログオン先のドメイン名を確認して、5.6.3 で作成したユーザー名/パスワードでログオンします。

図 5-60 ドメインへのログオン

5.6.6 802.1X の設定

802.1X の認証時の Windows Server 2008 の設定を示します。

Windows ドメインに参加し、シングルサインオン構成での認証方法を記載します。また、以下に示す設定の認証方法は PEAP、EAP-TLS です。

(1) ユーザーの作成

802.1X の認証用のユーザーID/パスワードを設定します。

「サーバーマネージャ」-「Active Directory ドメインサービス」-「Active Directory ユーザーとコンピューター」-「ドメイン名」-「Users」を選択します。

「Users」で右クリックして、「新規作成」-「ユーザー」を選択します。

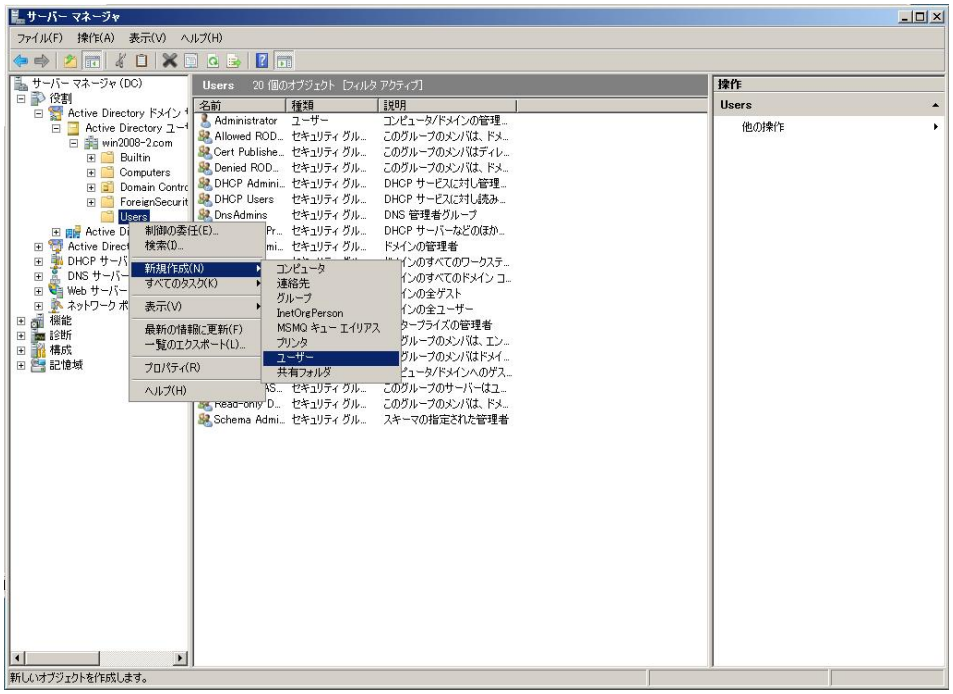


図 5-61 802.1X のユーザー新規作成

(2) ユーザー名の登録

「姓」に任意のユーザー名を登録します(ここでは"dot1x"とします)。「姓」を登録すると、「フルネーム」にも同内容が反映されます。

「ユーザーログオン」も「姓」と同一の内容を入力します。

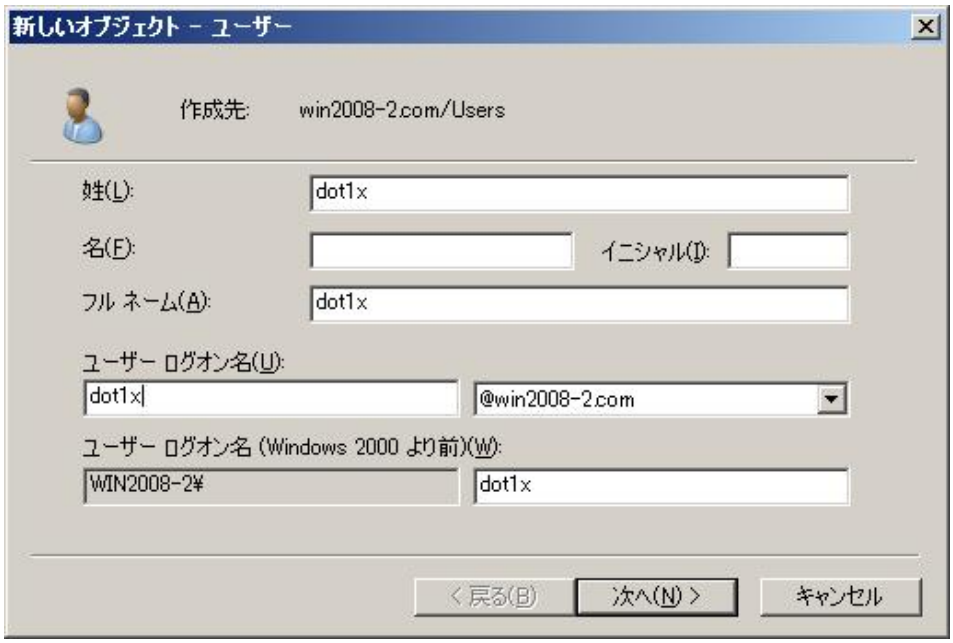


図 5-62 ユーザー名の登録

(3) パスワードの設定

パスワードを設定します。「次へ」を押します。

図 5-63 パスワードの設定

(4) 設定の完了

「完了」を押します。

図 5-64 ユーザー設定の確認

(5) グループの作成

「サーバーマネージャ」-「Active Directory ドメインサービス」-「Active Directory ユーザーとコンピュータ」-「ドメイン名」-「Users」を選択します。

「Users」で右クリックして、「新規作成」-「グループ」を選択します。

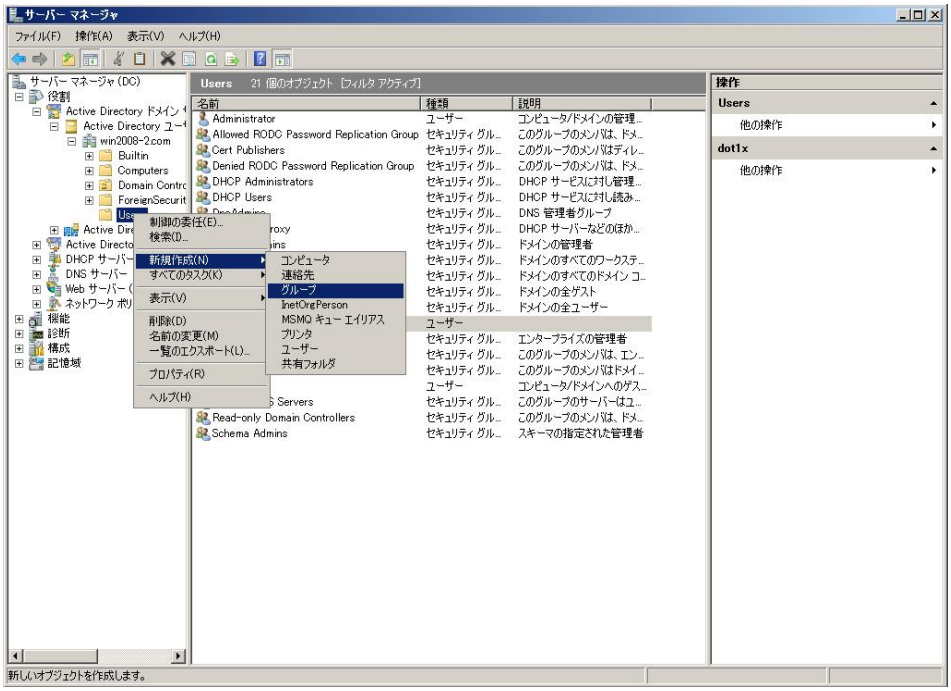


図 5-65 グループの作成

(6) グループ名の設定

グループ名(ここでは"1xGroup")を入力して、「OK」を押します。

図 5-66 グループ名の設定

(7) 所属するグループの設定

「サーバーマネージャ」の右画面にて、作成したユーザーを右クリックして「プロパティ」を選択します。

「所属するグループ」タブを選択し、「追加」ボタンを押します。

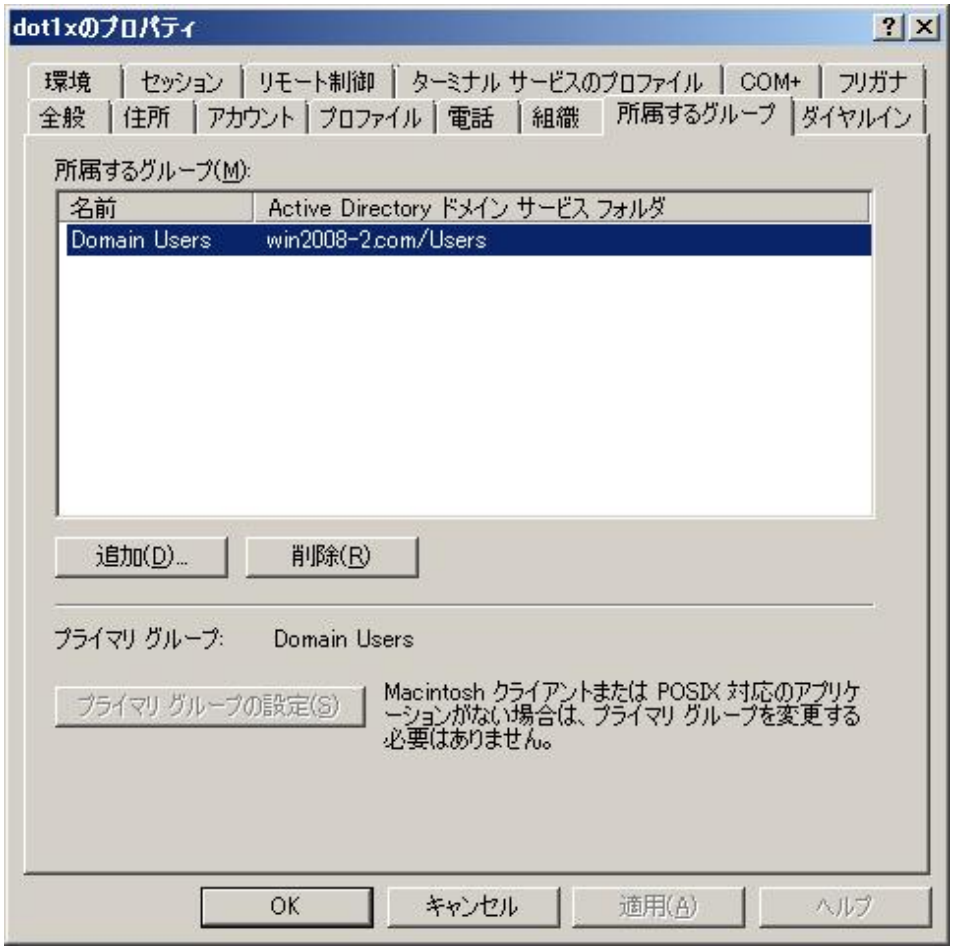


図 5-67 所属するグループ

(8) グループの選択

選択するオブジェクト名に、所属させるグループ名(ここでは"1xGroup")を入力して、「名前の確認」ボタンを押すと、以下のような表示になります。

「OK」を押します。

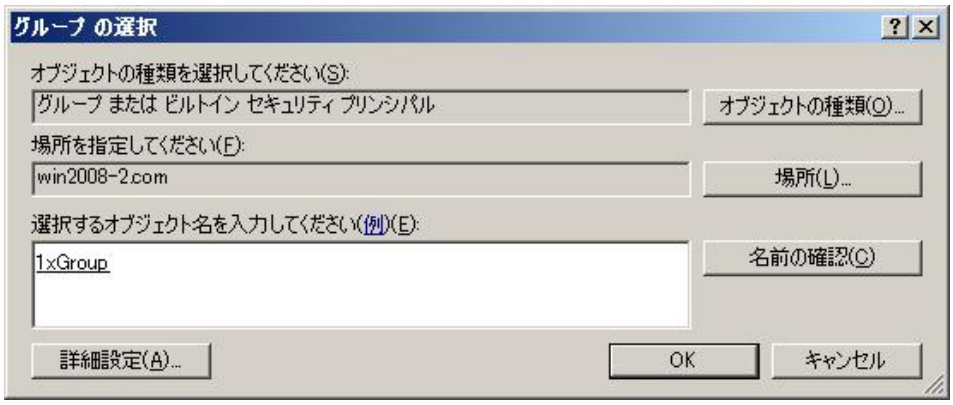


図 5-68 グループの選択

(9) 所属グループ追加確認

「所属するグループ」に指定したグループ("1xGroup")が追加されていることを確認します。

図 5-69 グループの設定確認

(10) アクセス許可の設定

「ダイヤルイン」タブを選択して、「リモートアクセス許可」を「アクセス許可」に設定して、「OK」を押します。

図 5-70 アクセス許可の設定

5.6.7 802.1X のネットワークポリシー設定

(1) ネットワークポリシーの作成

「サーバーマネージャ」-「役割」-「ネットワークポリシーとアクセスサービス」-「NPS(ローカル)」-「ポリシー」-「ネットワークポリシー」を右クリックして「新規」を選択します。

図 5-71 ネットワークポリシーの新規作成

(2) ポリシー名の設定

任意のポリシー名(ここでは"1xPolicy"とします)を入力して、「次へ」を押します。

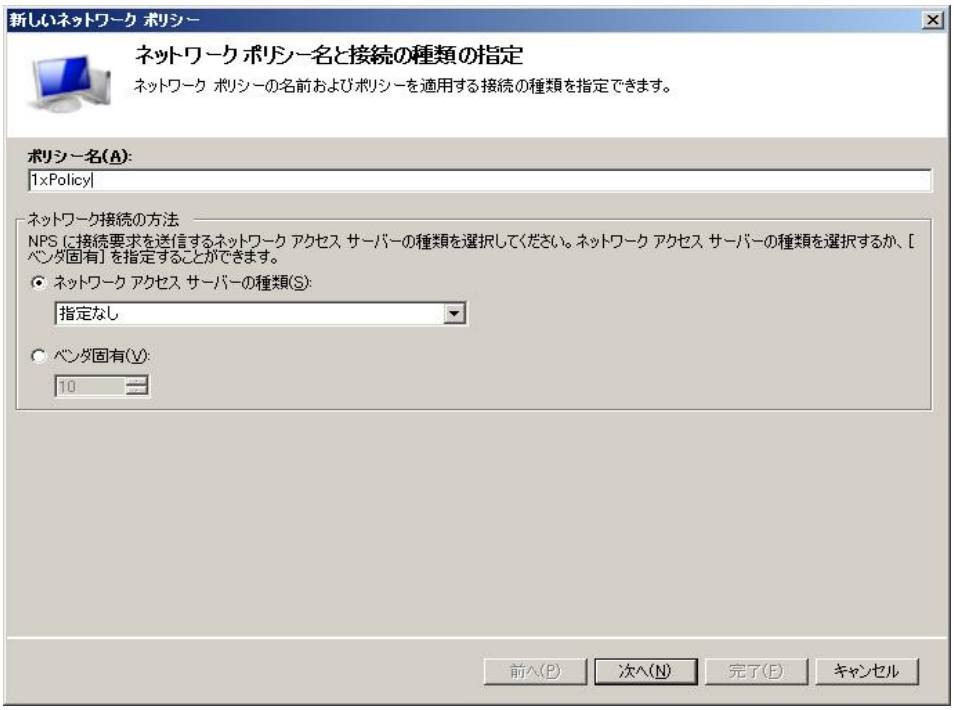


図 5-72 ポリシー名の設定

(3) 条件の指定

「追加」ボタンを押します。

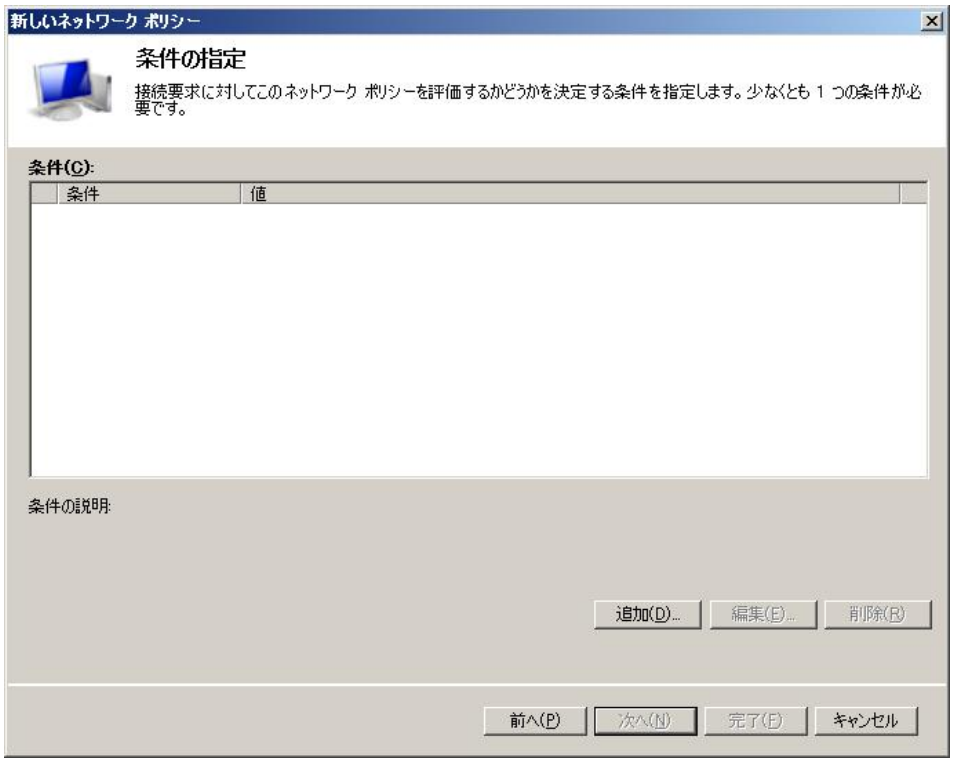


図 5-73 条件の指定

(4) 条件の選択

NAS ポートの種類を選択し、「追加」ボタンを押します。

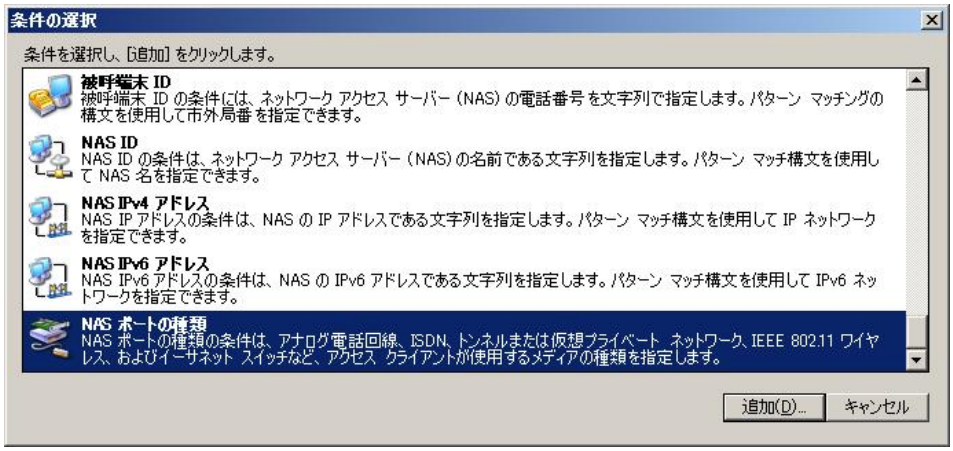


図 5-74 NAS ポートの選択

(5) NAS ポートの種類

「一般的な 802.1X 接続トンネルの種類」で「イーサネット」を選択し、「OK」ボタンを押します。

図 5-75 NAS ポートの種類

(6) NAS ポート設定の確認

設定した内容が追加されていることを確認し、「追加」ボタンを押します。

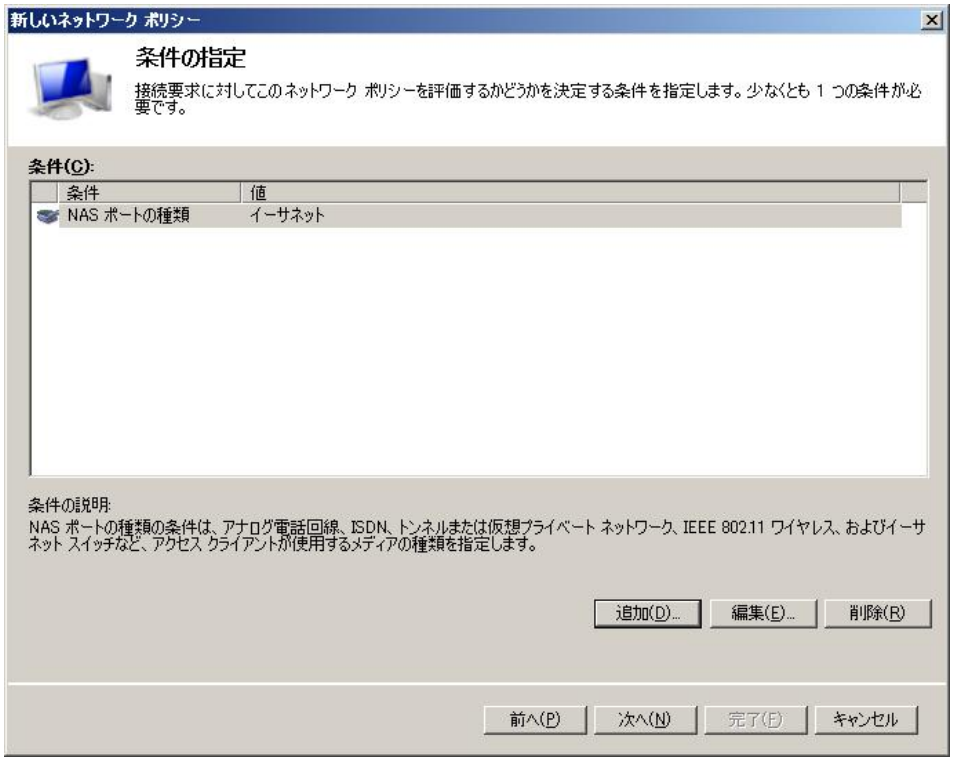


図 5-76 NAS ポートの設定確認

(7) 条件の選択

Windows グループを選択し、「追加」ボタンを押します。

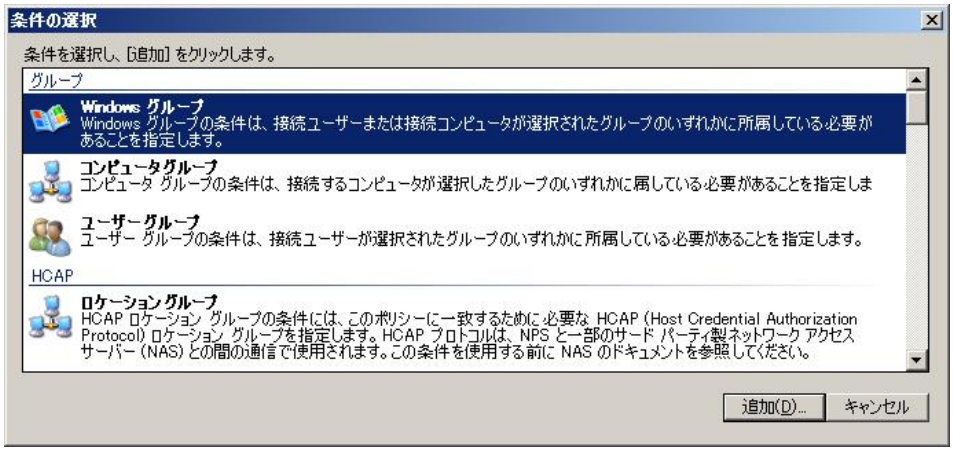


図 5-77 Windows グループの選択

(8) グループの選択

グループ選択画面にて、選択するオブジェクト名に作成したグループ(ここでは"1xGroup")を入力して、「名前の確認」ボタンを押します。

以下の表示になったら、「OK」を押します。

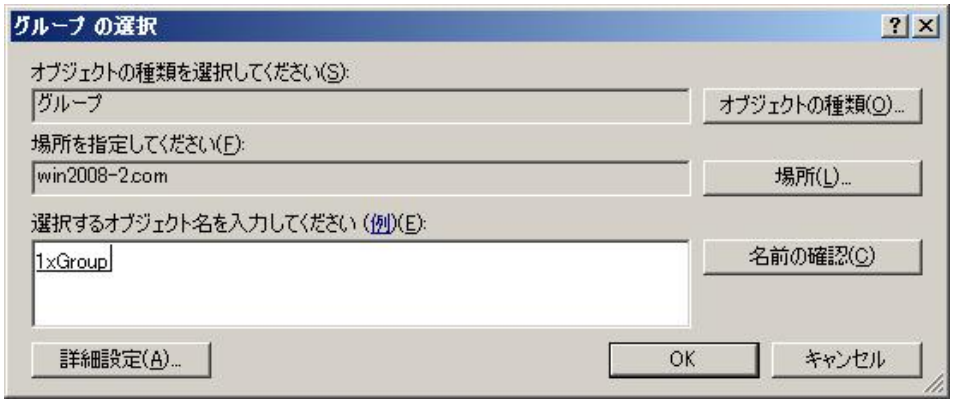


図 5-78 Windows グループの設定

(9) Windows グループの追加確認

Windows グループ画面にて、選択したグループが追加されていることを確認して、「OK」を押します。

図 5-79 Windows グループの設定確認

(10) 条件指定の確認

設定した内容が反映されていることを確認して、「次へ」を押します。

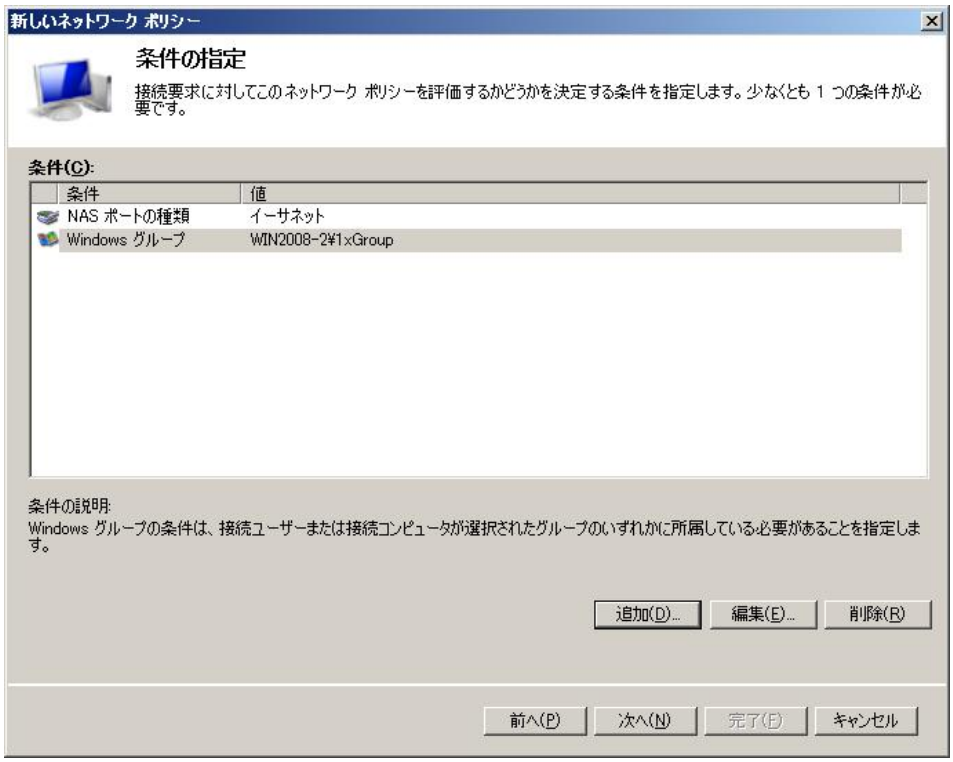


図 5-80 Windows グループの設定確認

(11) アクセス許可の指定

「アクセスを許可する」が選択されていることを確認して、「次へ」を押します。

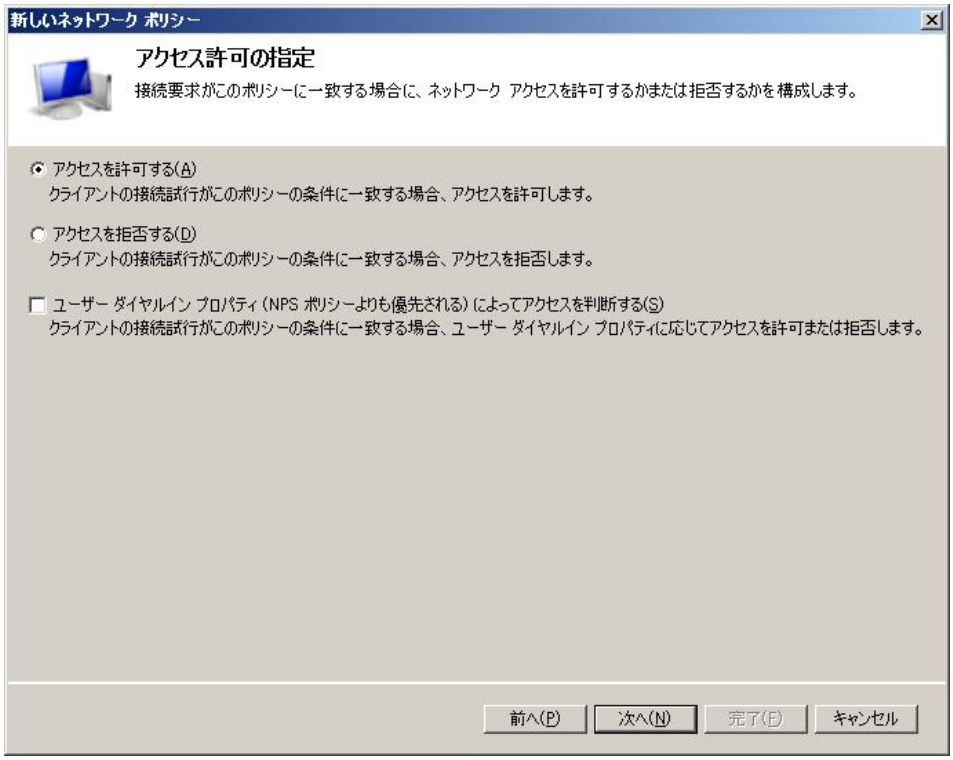


図 5-81 アクセス許可の設定

(12) 認証方法の構成

RADIUS サーバーで認証を許可する EAP 認証方式の設定を行います。使用したい認証方式を選択して設定を行ってください。どちらの認証方式も必要な場合は、両方設定してください。

- PEAP の場合

「追加」ボタンを押して、「Microsoft: 保護された EAP(PEAP)」を選択して、「OK」を押します。

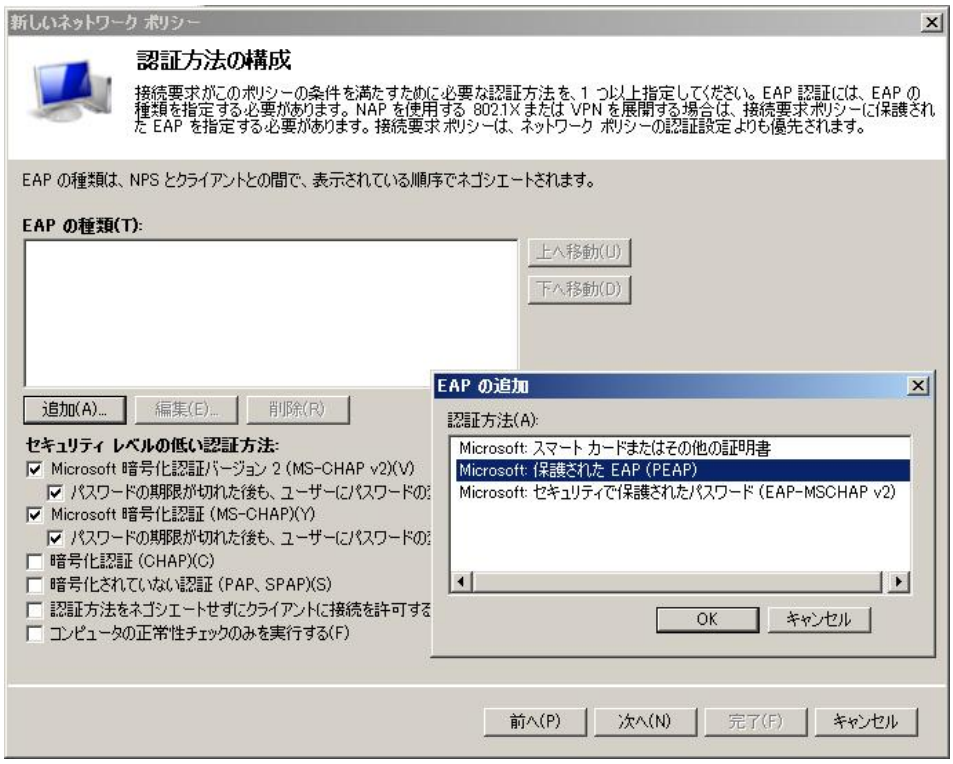


図 5-82 認証方法(PEAP)の選択

「EAP の種類」に追加された「Microsoft: 保護された EAP(PEAP)」を選択して、「編集」を押します。

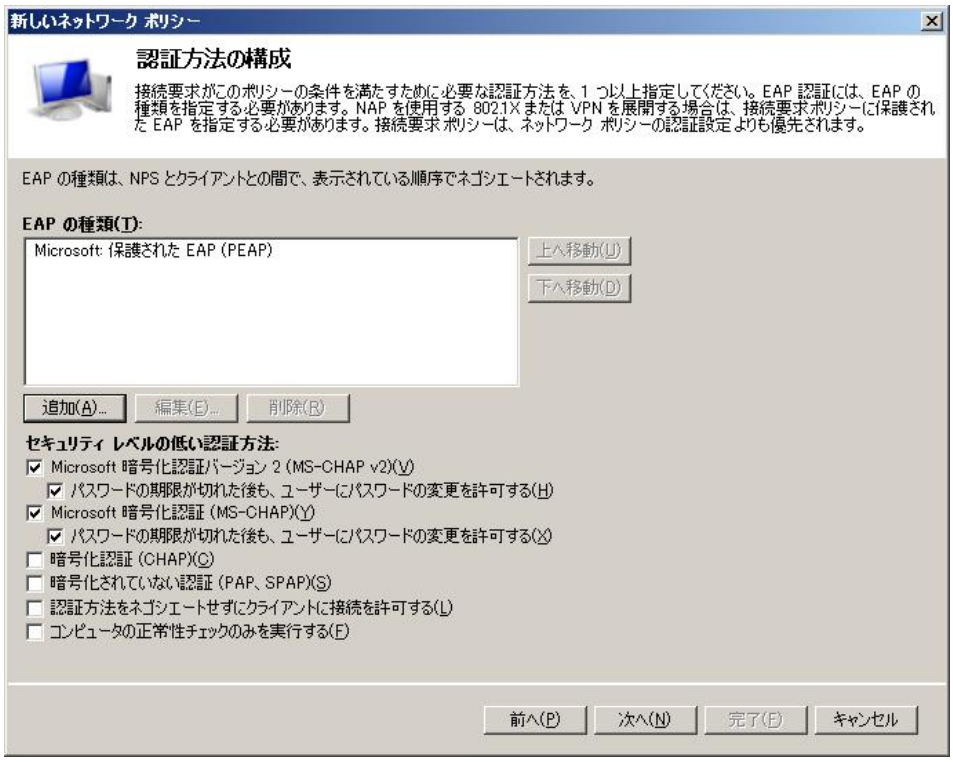


図 5-83 認証方式(PEAP)の確認

「保護された EAP プロパティの編集」画面にて、該当するサーバー証明書が選択されていることを確認して、「OK」を押します。

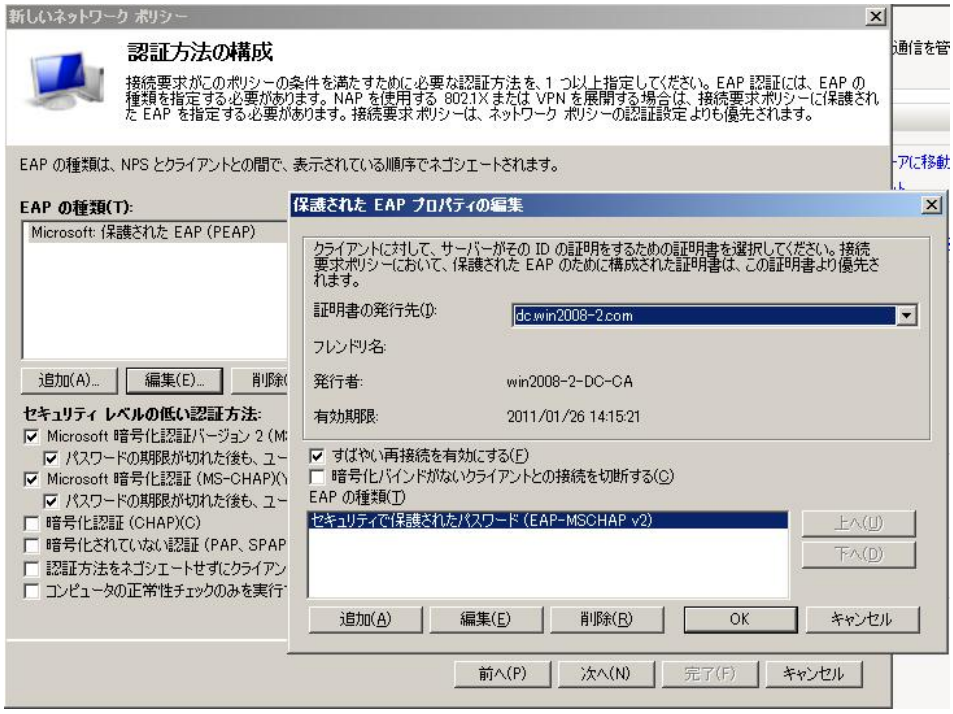


図 5-84 証明書の確認

- TLS の場合

「追加」ボタンを押して、「Microsoft: スマートカードまたはその他の証明書」を選択して、「OK」

を押します。

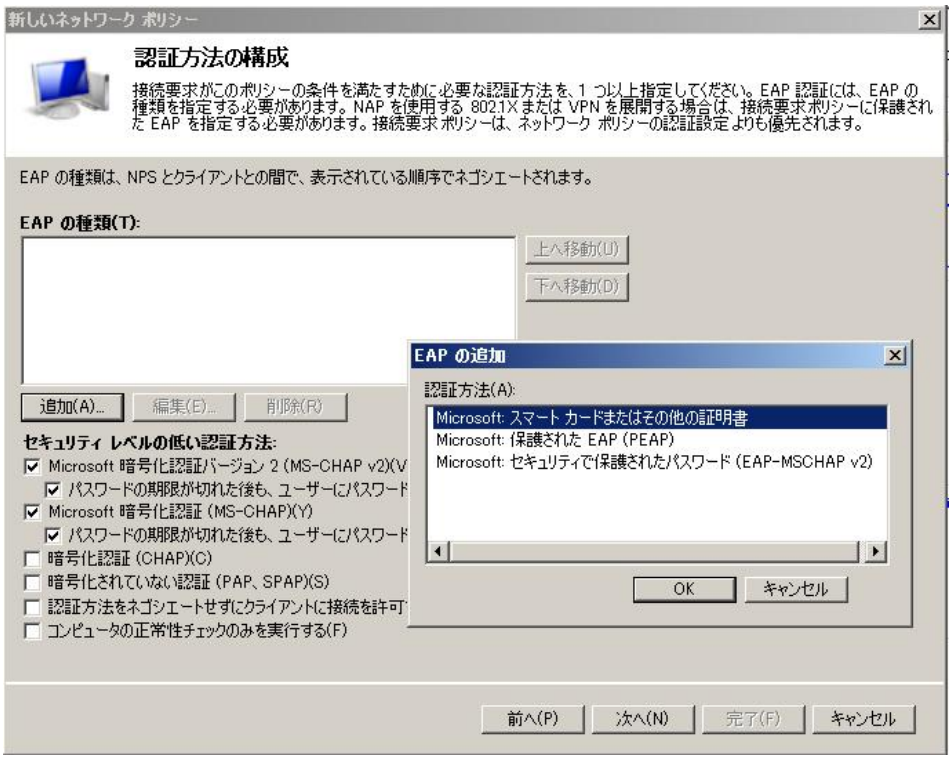


図 5-85 認証方法(TLS)の選択

「EAP の種類」に追加された「Microsoft: スマートカードまたはその他の証明書」を選択して、「編集」を押し、「保護された EAP プロパティの編集」画面にて、該当するサーバー証明書が選択されていることを確認して、「OK」を押します。

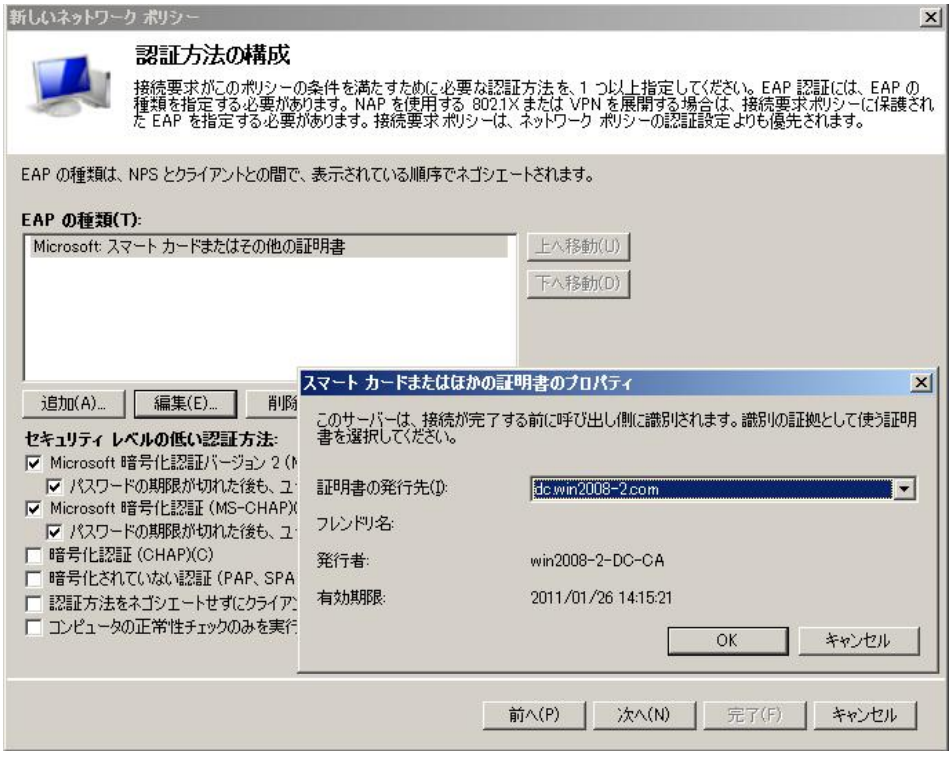


図 5-86 認証方式(TLS)の確認

(13) 制約の構成

「次へ」を押します。

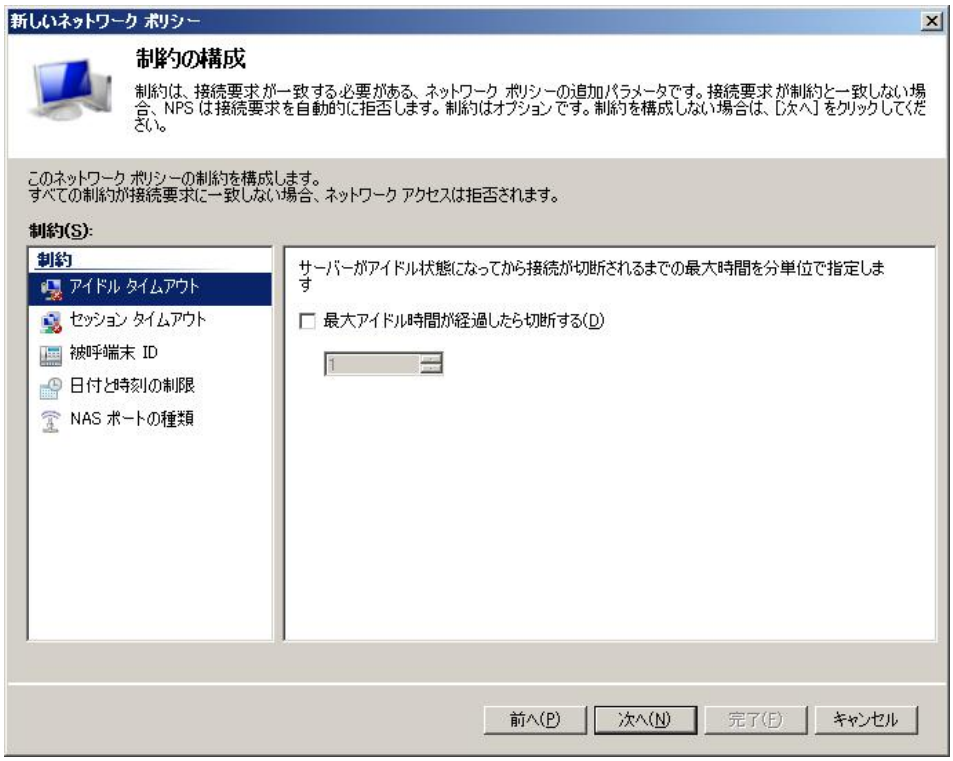


図 5-87 制約の構成

(14) DVLAN の設定

動的 VLAN 認証が必要な場合は、以下のアトリビュートを設定します。

Tunnel-Medium-Type = "802"(固定)
Tunnel-Pvt-Group-ID = "100"(認証成功後に割り当てる VLAN の ID)
Tunnel-Type = "VLAN"(固定)

「標準」を選択して、「追加」ボタンを押します。

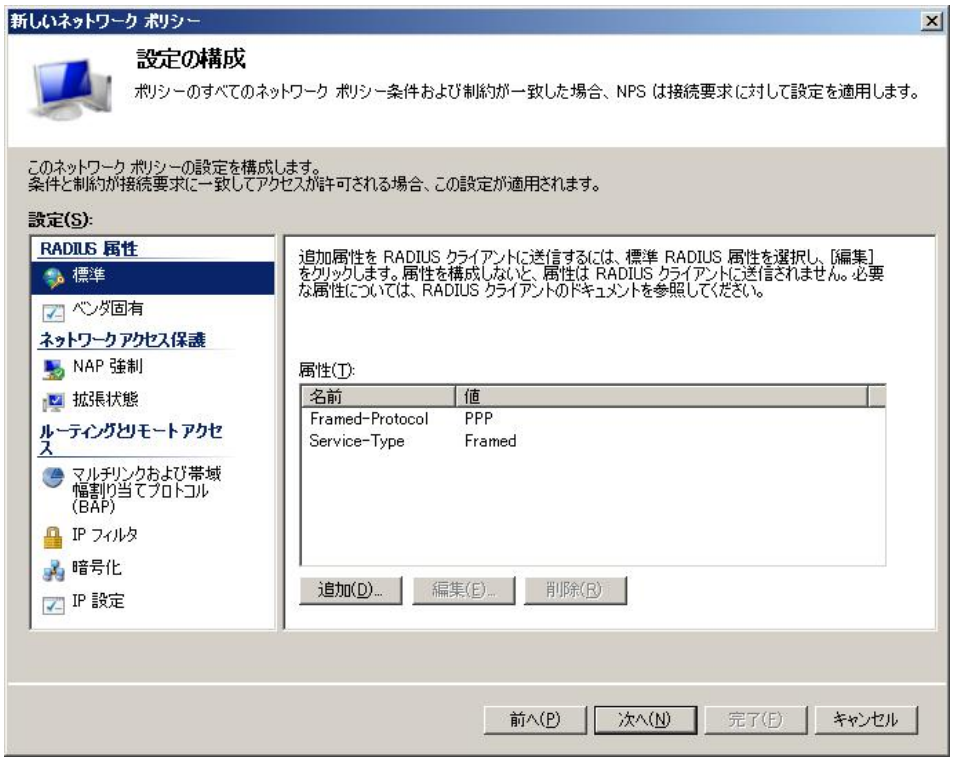


図 5-88 設定の構成

「標準 RADIUS 属性の追加画面」にて「Tunnel-Medium-Type」を選択して、「追加」を押します。

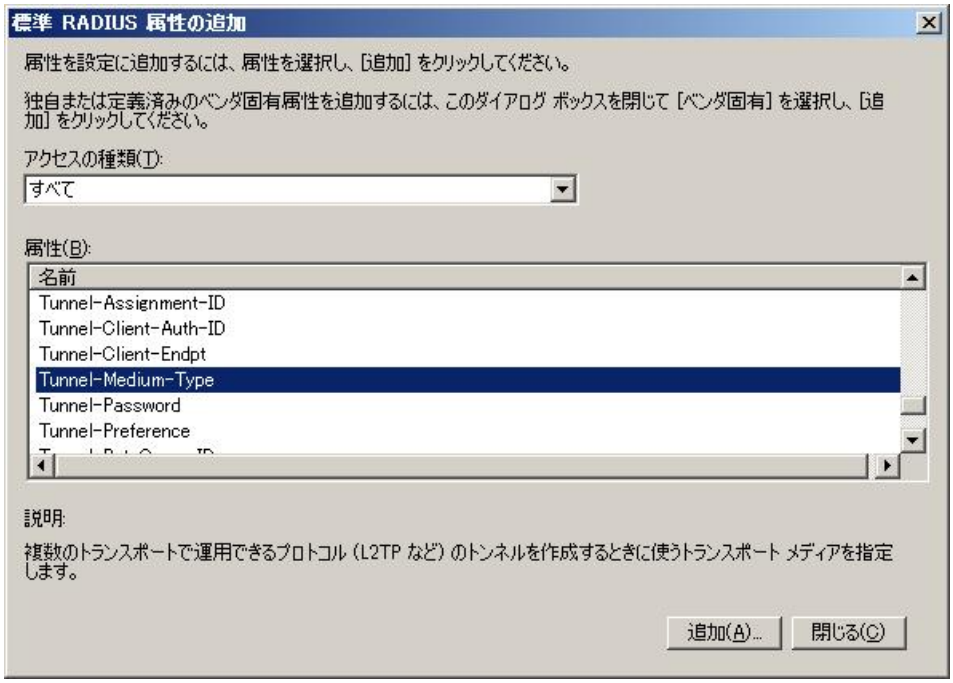


図 5-89 Tunnel-Medium-Type の追加

「属性の情報」画面にて「追加」を押します。

図 5-90 属性の情報設定

「属性の情報」画面にて、「802.1x で一般に使用する」が選択されていること、「802(includes all 802 media plus Ethernet canonical format)」が選択されていることを確認して、「OK」を押します。

図 5-91 属性の情報設定

「属性の情報」画面にて、設定した内容が追加されていることを確認し、「OK」を押します。

図 5-92 属性の情報設定確認

続けて「追加」を押し、「標準 RADIUS 属性の追加」画面にて「Tunnel-Pvt-Group-ID」を選択して、「追加」を押します。

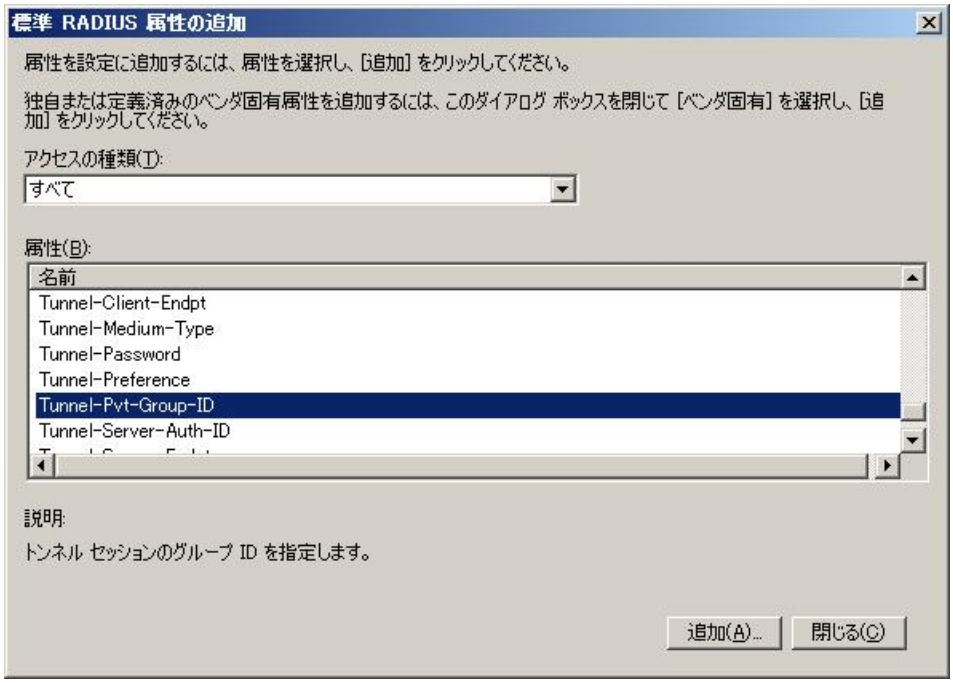


図 5-93 Tunnel-Pvt-Group-ID の追加

「属性の情報」画面にて、「追加」を押し、認証成功後に割り当てる VLAN の ID を設定して、「OK」を押します(ここでは"100"を指定)。

図 5-94 属性の情報設定

「属性の情報」画面で、設定した内容が追加されていることを確認して「OK」を押します。

図 5-95 属性の情報設定

続けて「追加」を押し、「標準 RADIUS 属性の追加」画面で「Tunnel-Type」を選択して、「追加」を押します。

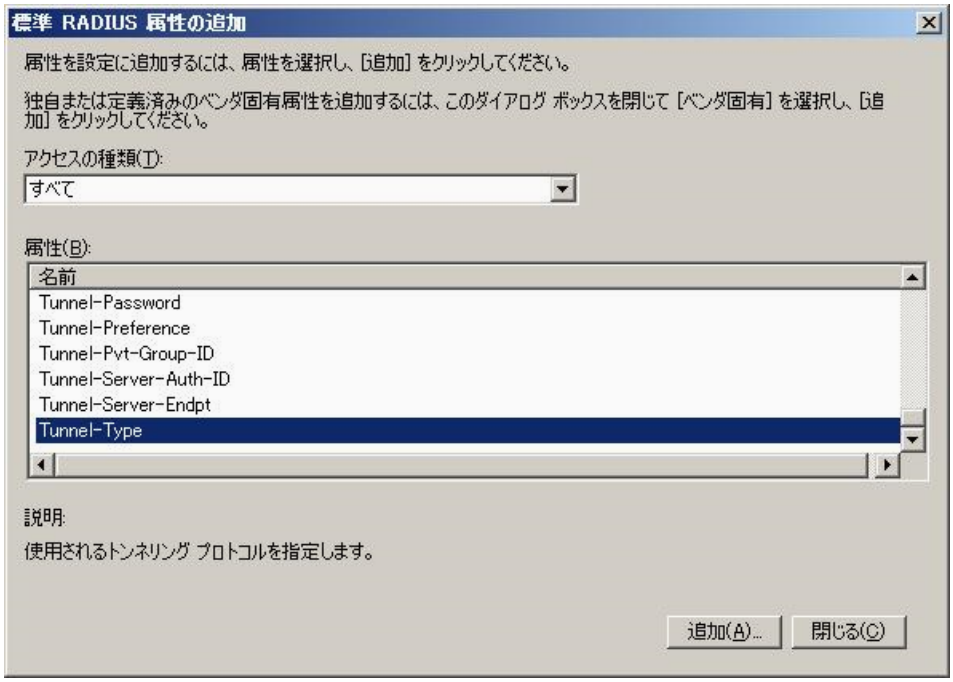


図 5-96 Tunnel-Type の追加

「属性の情報」画面にて「追加」を押します。

続けて、以下の画面で「802.1xで一般的に使用する」にチェックされていること、「Virtual LANs(VLAN)」が選択されていることを確認して、「OK」を押します。

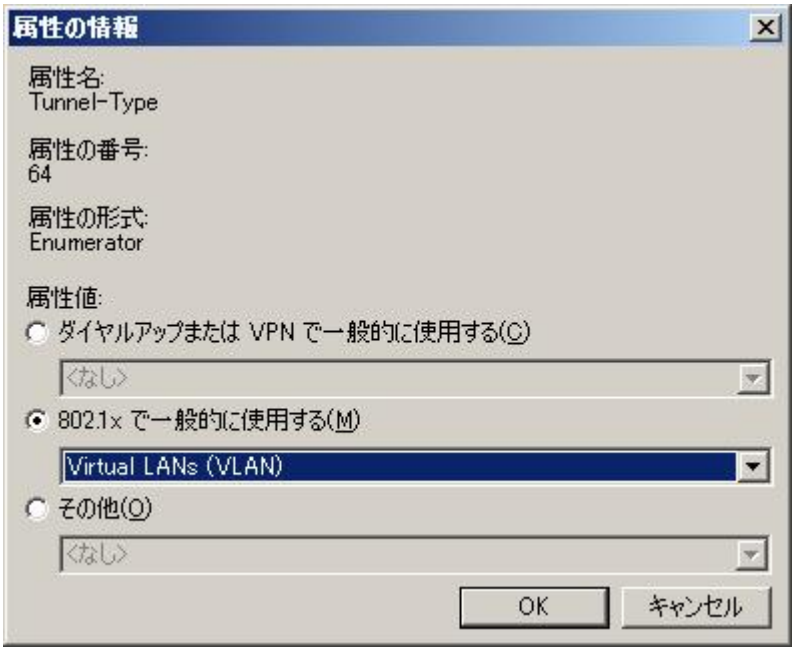


図 5-97 属性の情報設定

「属性の情報」画面にて、設定した内容が追加されていることを確認して、「OK」を押します。

図 5-98 属性の情報設定

追加したアトリビュートが反映されていることを確認して、「次へ」を押します。

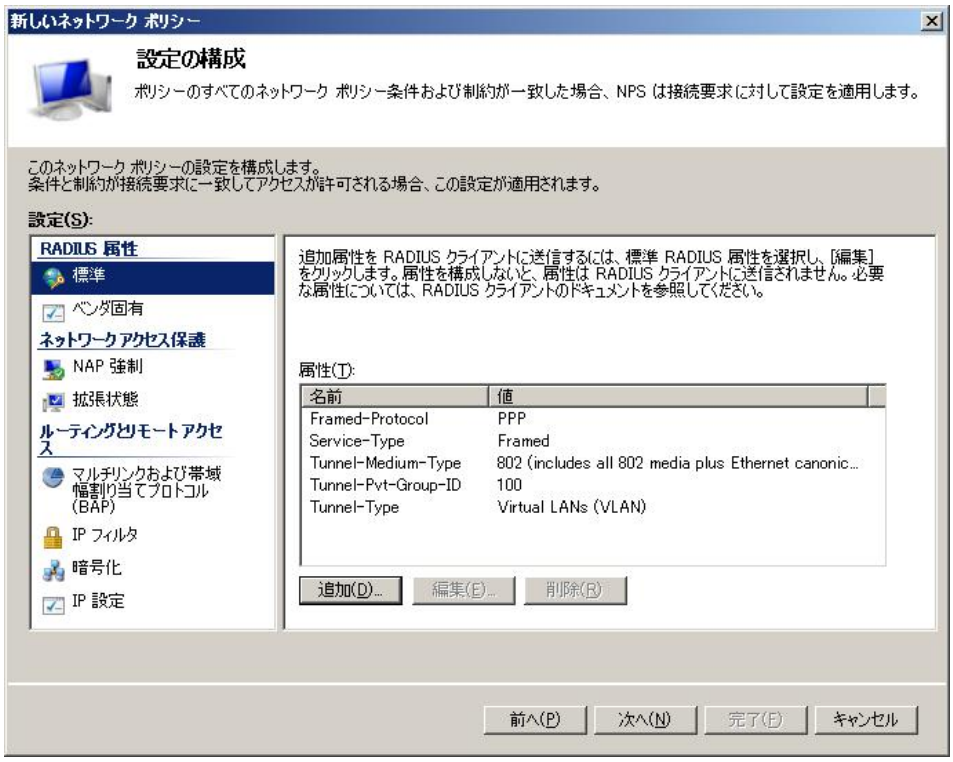


図 5-99 追加したアトリビュートの確認

新しいネットワークポリシーの設定内容を確認して、「完了」を押します。

図 5-100 ネットワークポリシーの確認

サーバーマネージャ画面に反映されていることを確認します。

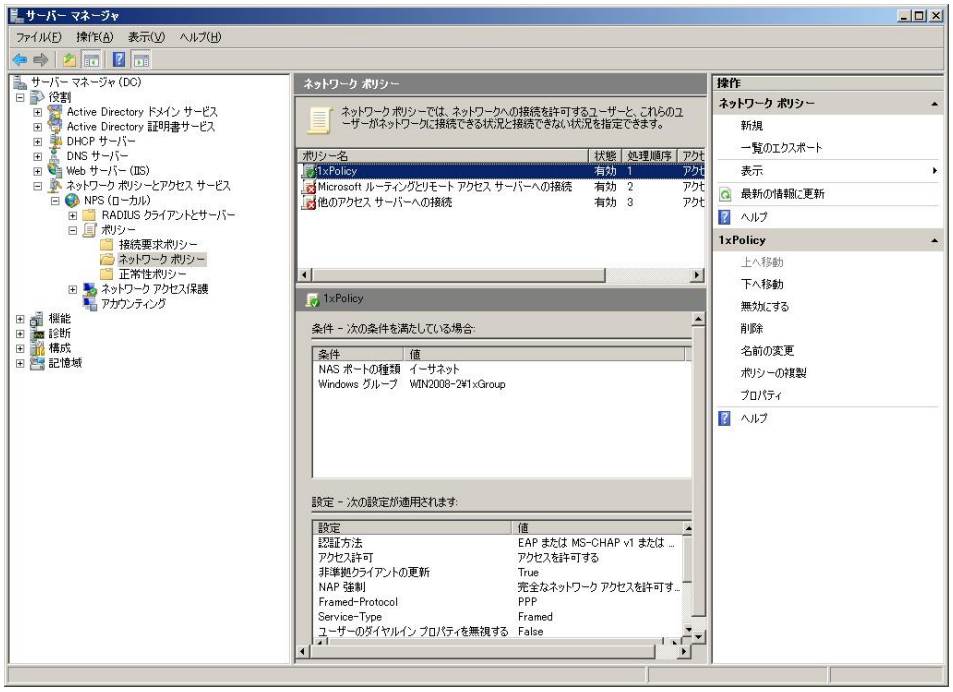


図 5-101 サーバーマネージャでの確認

5.7 802.1X のクライアントの設定

このセクションの内容はサポート対象外となります。

Windows 標準の 802.1X サプリカントの設定方法について示します。本項では Windows Vista での設定方法を記載します。

5.6.5 認証クライアントのドメイン参加と同様の手順でドメインへ参加します。
※ 接続時のユーザー名/パスワードは 5.6.6 802.1X の設定で作成したユーザーを指定します(ここでは"dot1x")。

認証クライアントを再起動後、PC の管理者アカウントでログオンします。

5.7.1 PEAP 設定

PEAP を使用した 802.1X の設定方法を示します。

「スタート」-「ネットワーク」-「ネットワークと共有センター」を開きます。「ネットワーク接続の管理」を選択し、該当するネットワーク接続を右クリックしてプロパティを開きます。

プロパティ画面にて、「認証」タブを選択して、「IEEE802.1X 認証を有効にする」をチェックします。ネットワーク認証方法に「Microsoft: 保護された EAP(PEAP)」を選択して、「設定」を押します。

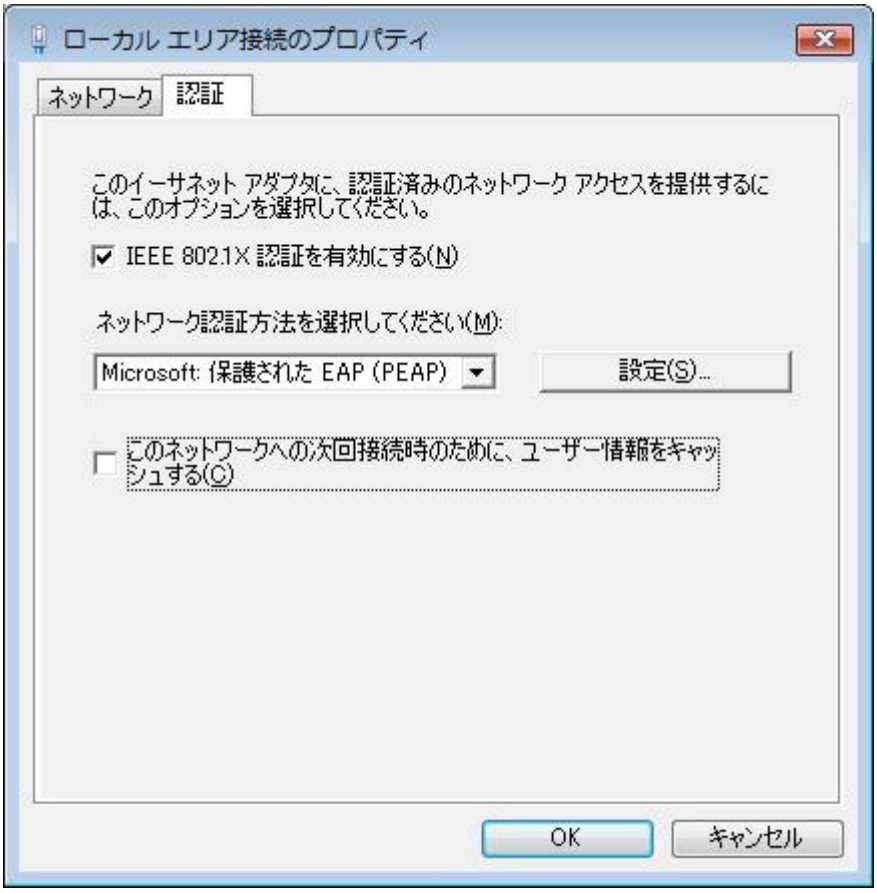


図 5-102 ローカルエリア接続のプロパティ

「保護された EAP のプロパティ」画面にて、「サーバーの証明書を検証する」をチェックして、「信頼されたルート証明機関」で、「win2008-2-DC-CA」を選択します。

「認証方法を選択する」にて、「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」が選択されていることを確認して、「構成」を押します。

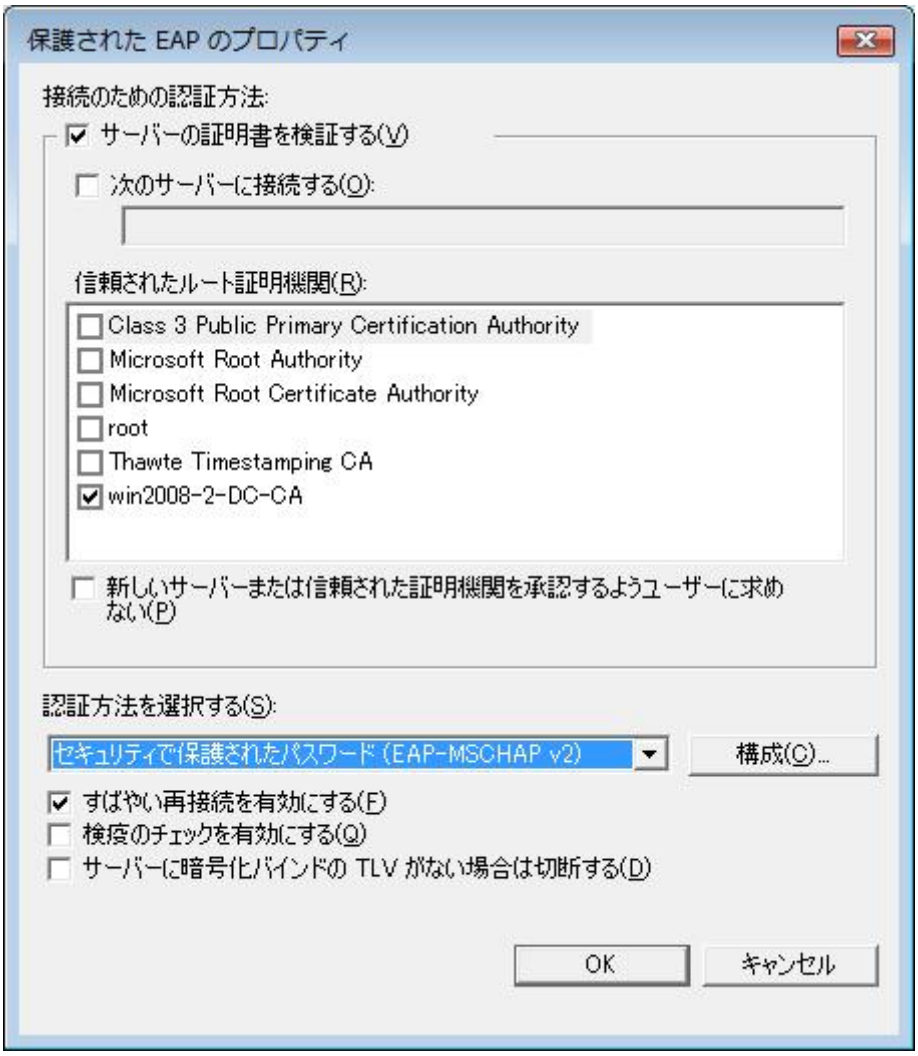


図 5-103 保護された EAP のプロパティ

「EAP MSCHAPv2 のプロパティ」画面にて、「Windows のログオン名とパスワード(及びドメインがある場合はドメイン)を自動的に使う」がチェックされていることを確認して、「OK」を押します。

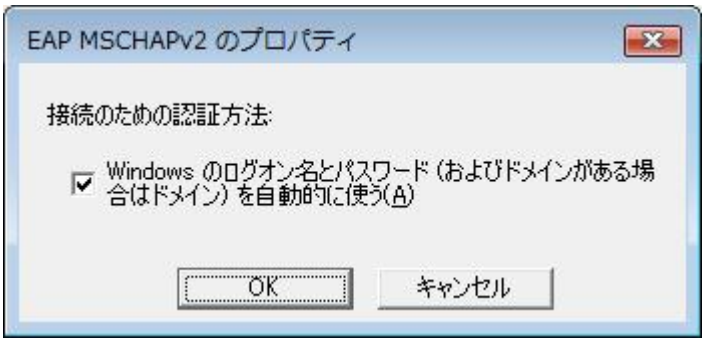


図 5-104 EAP MSCHAPv2 のプロパティ

5.7.2 TLS の設定

TLS を使用した 802.1X の設定方法を示します。

本項では証明書 Web 登録サービスを使用して、ユーザー証明書を取得します。

(1) ユーザー証明書のダウンロード

サーバーと通信可能なネットワークに認証クライアントを接続します。

Internet Explorer を使用して、「http://(サーバーIP アドレス)/certsrv/」にアクセスします。

認証画面が表示されることを確認して、5.6.6 802.1X の設定で作成したユーザーを指定します(ここでは"dot1x")。

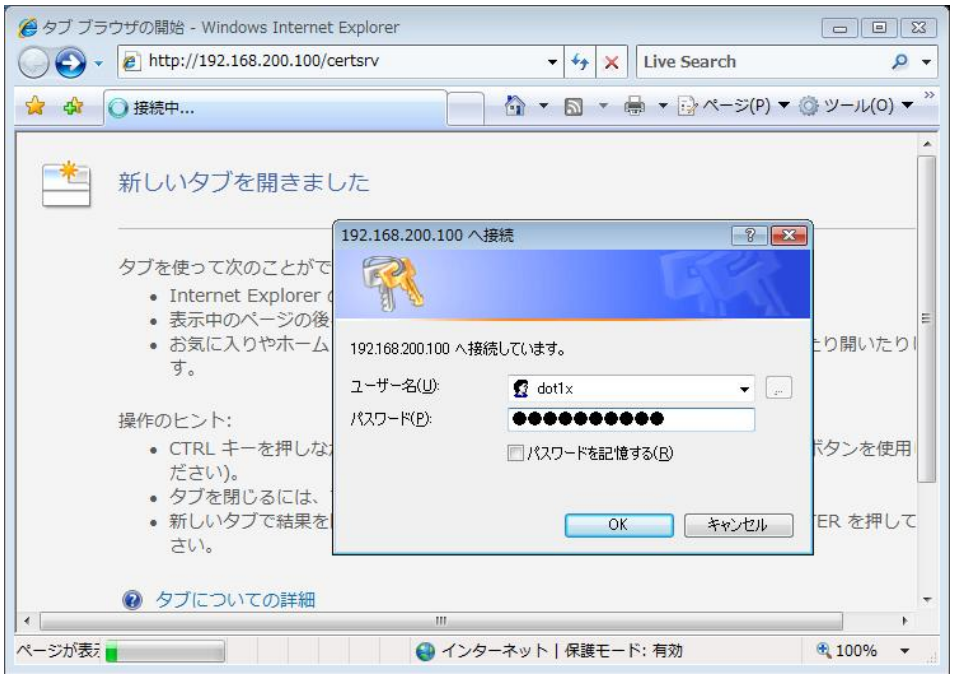


図 5-105 サーバーへの Web アクセス

認証が成功すると、「Microsoft Active Directory 証明書サービス」画面が表示されます。
「タスクの選択」より「証明書を要求する」をクリックします。

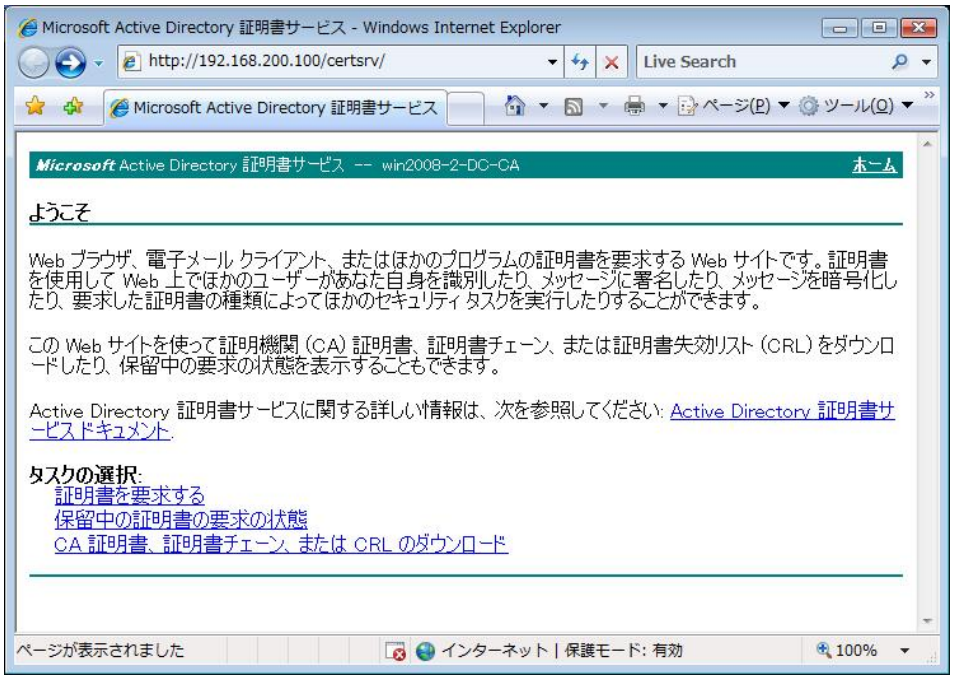


図 5-106 証明書の要求

「証明書の要求」から「ユーザー証明書」をクリックします。

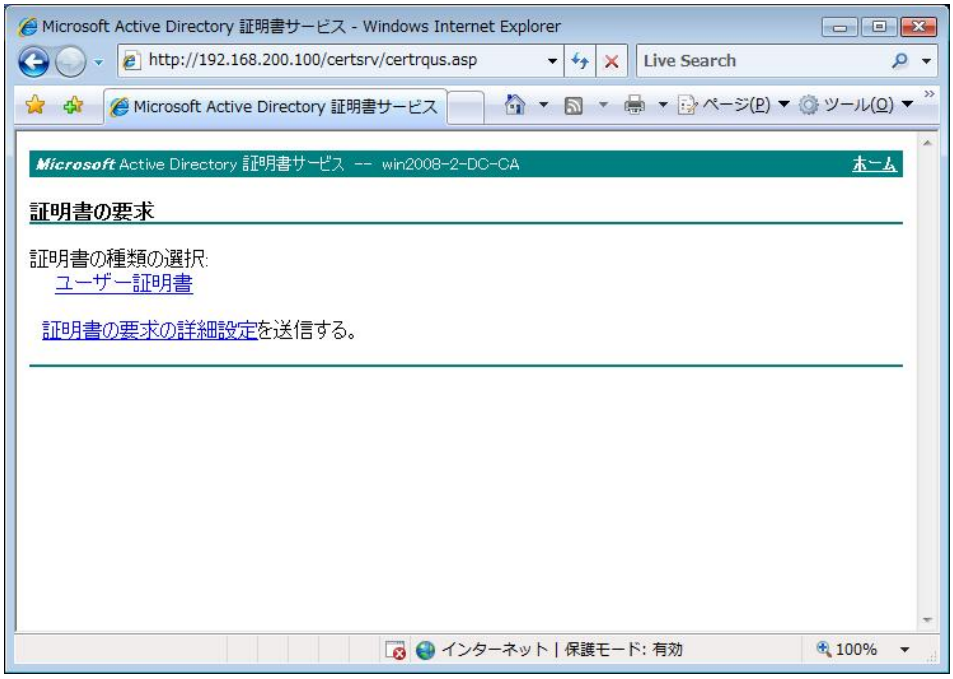


図 5-107 ユーザー証明書の要求

※ クライアントの Internet Explorer のセキュリティ設定にて、警告が出てダウンロードができない場合は、以下を設定してください。本項実施後、忘れずに設定を戻しておくよう注意してください。

- Internet Explorer の「ツール」-「インターネットオプション」を選択

- 「セキュリティ」タブを選択し、「レベルのカスタマイズ」ボタンを押す
- 「ActiveX コントロールとプラグイン」の中の「スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行(セキュリティで保護されていない)」を有効にして、「OK」を押す

「送信」ボタンを押します。

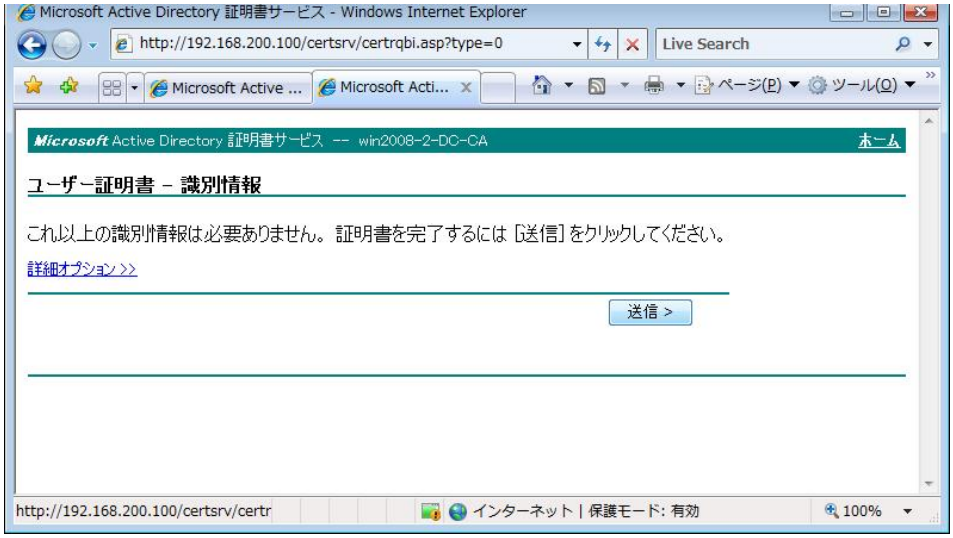


図 5-108 ユーザー証明書の送信

警告が表示されますが、「はい」を押します。

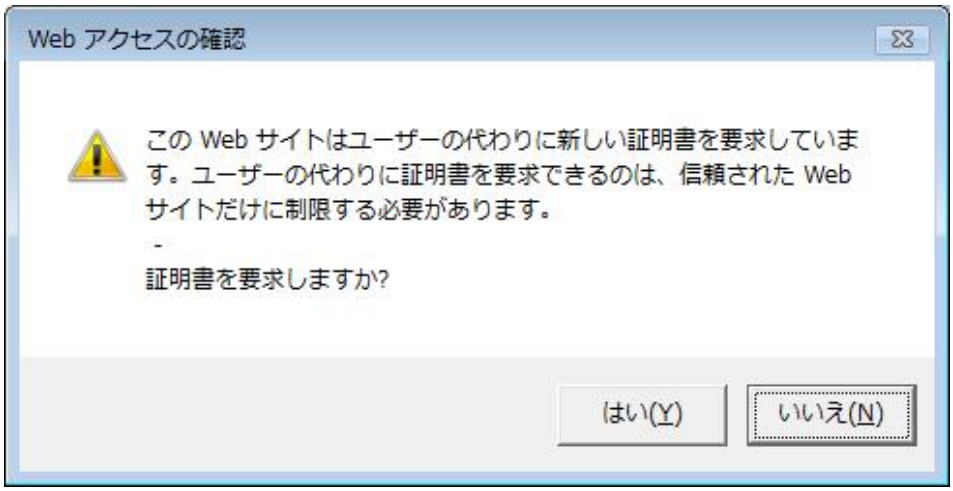


図 5-109 Web アクセスの確認

「この証明書のインストール」をクリックします。

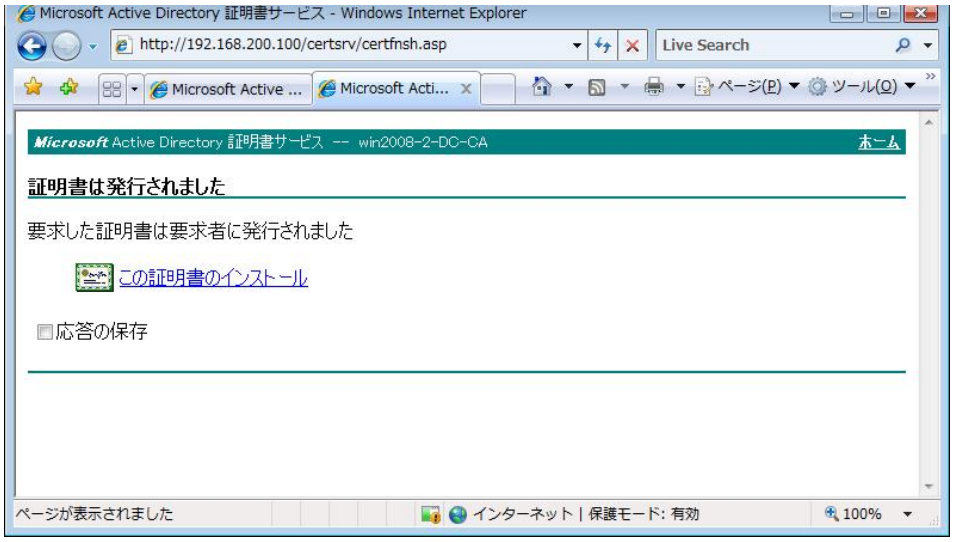


図 5-110 証明書のインストール

警告が表示されますが、「はい」を押します。

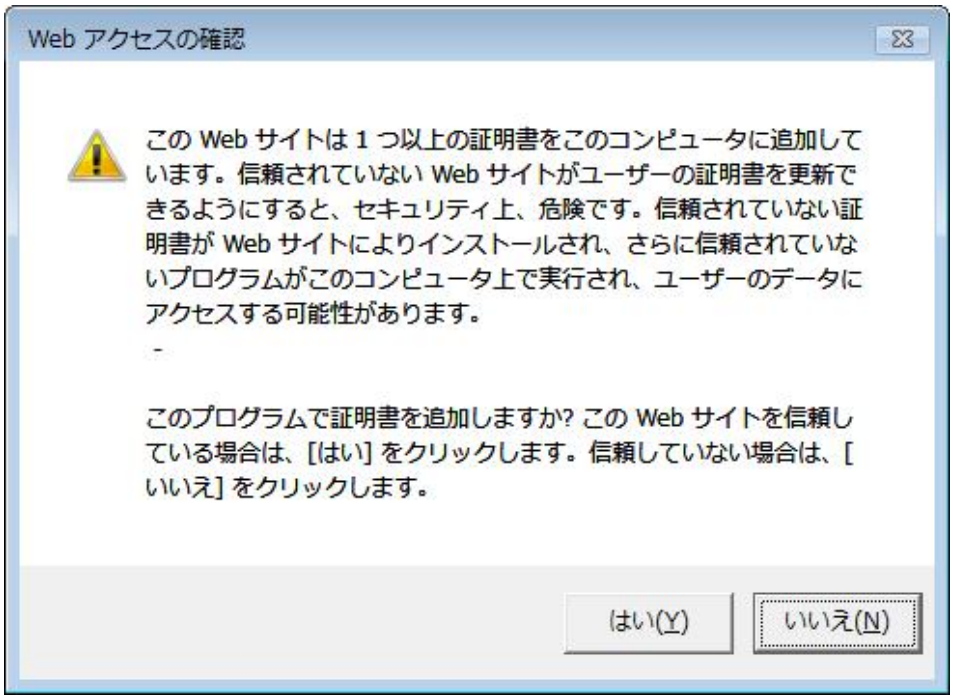


図 5-111 警告

以下画面が表示されると、ユーザー証明書のインストール完了です。

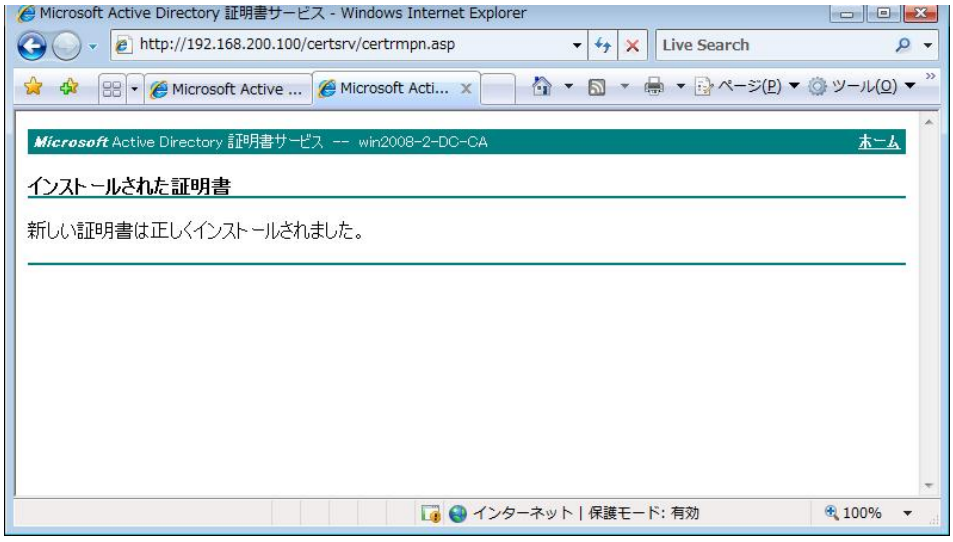


図 5-112 インストールの完了

インストールの確認

Internet Explorer の「インターネットオプション」を開き、「コンテンツ」タブを選択して「証明書」をクリックします。

「証明書」画面の「個人」タブにて、該当する証明書がインストールされていることを確認します。

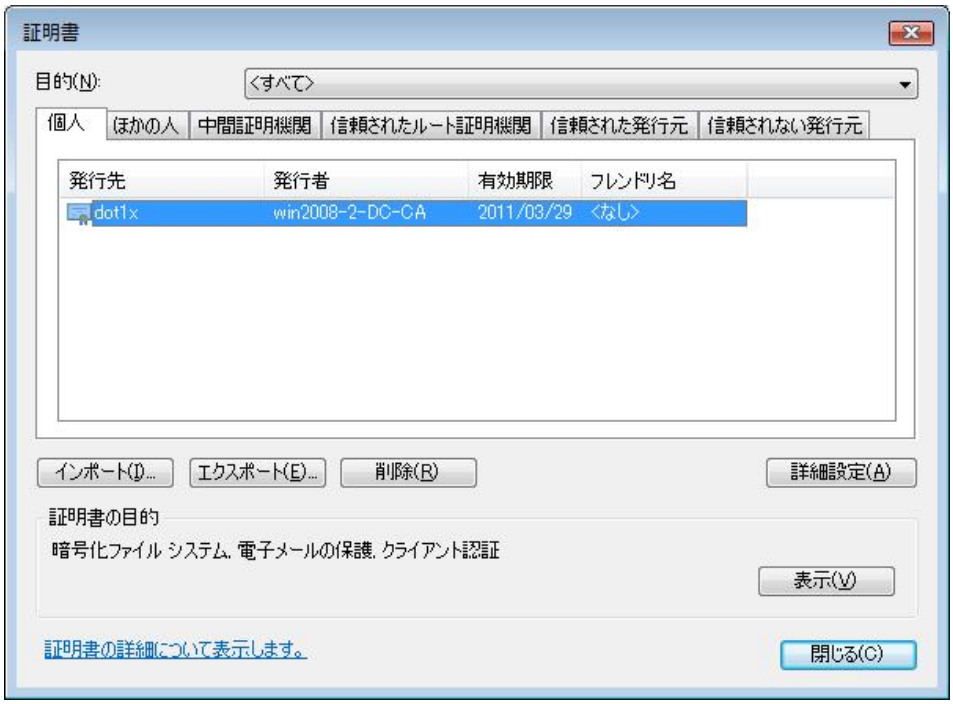


図 5-113 証明書の確認

(2) TLS の設定

「スタート」-「ネットワーク」-「ネットワークと共有センター」を開きます。「ネットワーク接続の管理」を選択して、該当するネットワーク接続を右クリックして、プロパティを開きます。

プロパティ画面にて、「認証」タブを選択して、「IEEE802.1X 認証を有効にする」をチェックします。

ネットワーク認証方法に「Microsoft: スマートカードまたはその他の証明書」を選択して、「設定」を押します。

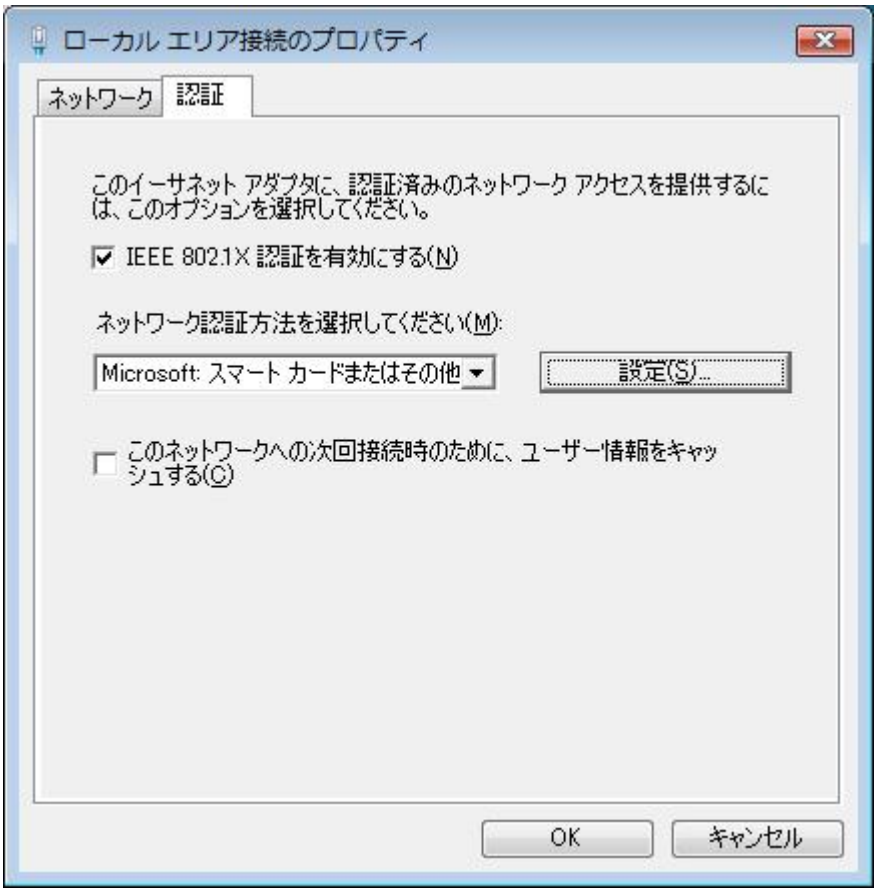


図 5-114 ローカルエリアのプロパティ

「スマートカードまたはその他の証明書のプロパティ」画面にて、「接続のための認証方法」で「このコンピュータの証明書を使う」がチェックされていることを確認します。

「信頼されたルート証明機関」で、「win2008-2-DC-CA」を選択して、「OK」を押します。

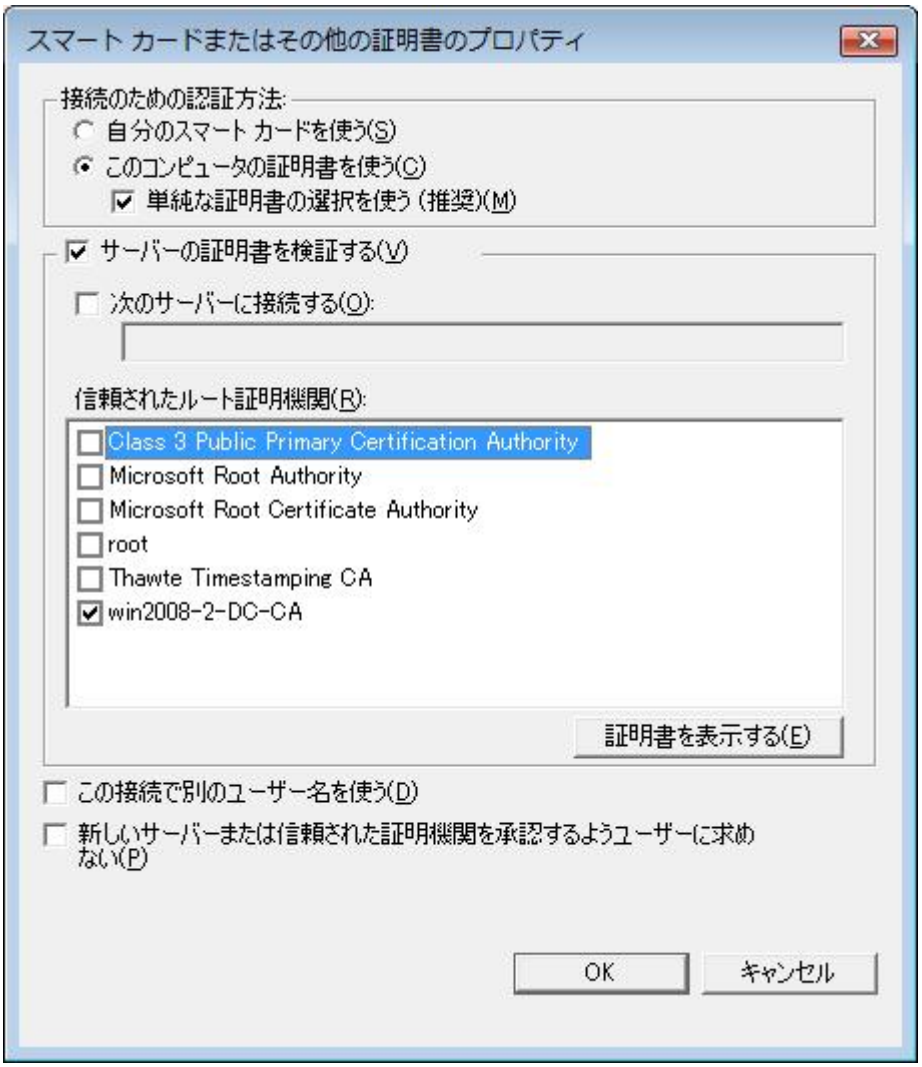


図 5-115 TLS の設定

6 応用設定

6.1 認証ページのカスタマイズ

6.1.1 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できます。

以下のコマンドを用いて、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 <IPADDR> ) | memory-card <FILE> <WEB_PAGE>
# copy tftp <IPv6ADDR> ) [ manage | ( vlan <VID> ) ] <FILE> <WEB_PAGE>
# erase <WEB_PAGE>
WEB_PAGE = <PAGE1> | <PAGE2> | <PAGE3> | <PAGE4> | <PAGE5> | <PAGE6>
PAGE1 = login-page
PAGE2 = login-success-page
PAGE3 = login-failure-page
PAGE4 = logout-success-page
PAGE5 = logout-failure-page
PAGE6 = redirect-error-page
```

・・・IPADDR	TFTP サーバーの IP アドレス
・・・IPv6ADDR	TFTP サーバーの IPv6 アドレス
・・・VID	VLAN ID
・・・FILE	ファイル名 <1-128(文字)>
・・・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(最大ファイルサイズは 5120 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

<ログイン用の form 例>

```
<form method="POST" action="/cgi-bin/adeflogin.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" name="action" value="login">
<input type="reset" value="reset">
</form>
```

<ログアウト用の form 例>

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

6.1.2 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 そのものを別の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/adeflogin.cgi 」 か ら 「 http://AccessDefender 認 証 用 IP ア ド レス:port/cgi-bin/adeflogin.cgi」に変更することで、外部 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 有効時は「https://AccessDefender 認証用 IP アドレス:port/cgi-bin/adeflogin.cgi」)。

ポイントは以下です。

- form の action を APRESIA の認証 CGI に指定
- 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
- 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://192.0.2.3:8080/」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://192.0.2.3:8080/cgi-bin/adeflogin.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" name="action" value="login">
<input type="reset" value="reset">
</form>
```

<ログアウト用の form 例>

```
<form method="POST" action="http://192.0.2.3:8080/cgi-bin/adeflogout.cgi">
<input type="submit" name="action" value="logout">
</form>
```

6.1.3 認証方法選択機能の認証ページカスタマイズ

3.8 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 5120 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
- 認証 ID の変数名を authid にする(type は使用中の環境に合わせて指定)
- form の method を"POST"に指定

<認証方法選択用の form 例(ユーザー選択型)>

```
<form method="POST" action="/cgi-bin/adeflogin.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" name="action" 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://192.0.2.3:8080/cgi-bin/adeflogin.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" name="action" value="login">
<input type="reset" value="reset">
</form>
```

6.2 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(APRESIA への特別な設定は不要)

表 6-1 の場合、「userA」は、「aa:aa:aa:aa:aa:aa」の端末でしか認証されません。

表 6-1 Calling-Station-Id 属性による認証の場合のユーザーデータベース

User	Password	Calling-Station-Id(MAC アドレス)
userA	passwordA	aa:aa:aa:aa:aa:aa
userB	passwordB	bb:bb:bb:bb:bb:bb

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。

6.3 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は、「NAS-IP-Address」、「NAS-Port」、及び「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。

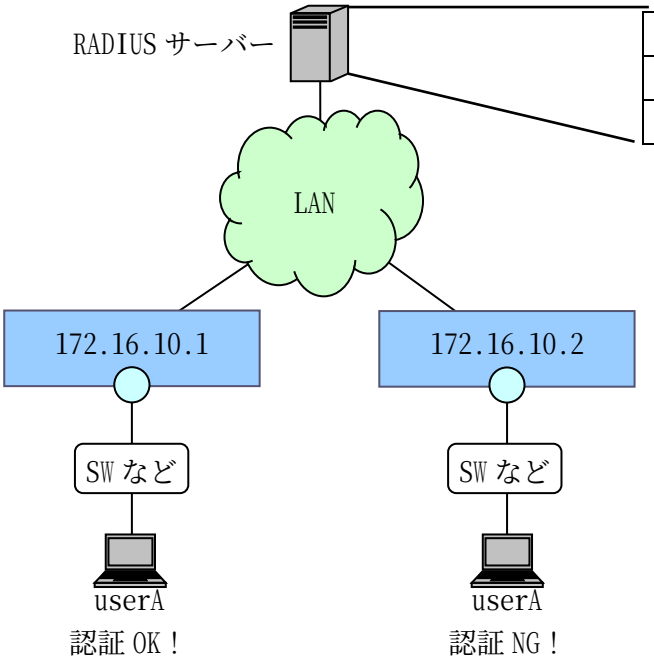
6.3.1 NAS-IP-Address

「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 6-1 の例では、以下の動作になります。

- 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



User	Password	NAS-IP-Address
userA	passwordA	172.16.10.1
userB	passwordB	172.16.10.2

図 6-1 NAS-IP-Address 設定時のアクセス制限

6.3.2 NAS-IPv6-Address

「NAS-IPv6-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 IPv6 アドレスになります。実際の値は APRESIA のリンクローカルアドレスが設定されます。

RADIUS サーバーに NAS-IPv6-Address の設定が必要です。APRESIA への特別な設定は不要です。

図 6-2 の例では、以下の動作になります。

- userA は、fe80::212:34ff:5566:7778 のリンクローカルアドレスを持つ装置でのみ認証される
- userB は、fe80::212:34ff:5566:7779 のリンクローカルアドレスを持つ装置でのみ認証される

User	Password	NAS-IPv6-Address
userA	passwordA	fe80::212:34ff:5566:7778
userB	passwordB	fe80::212:34ff:5566:7779

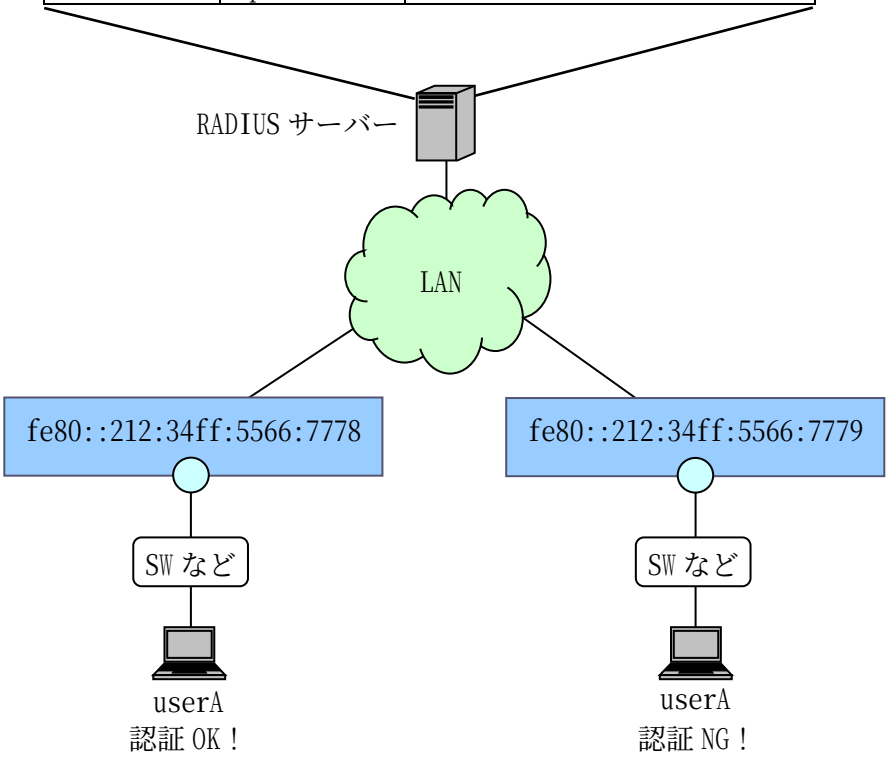


図 6-2 NAS-IPv6-Address 設定時のアクセス制限

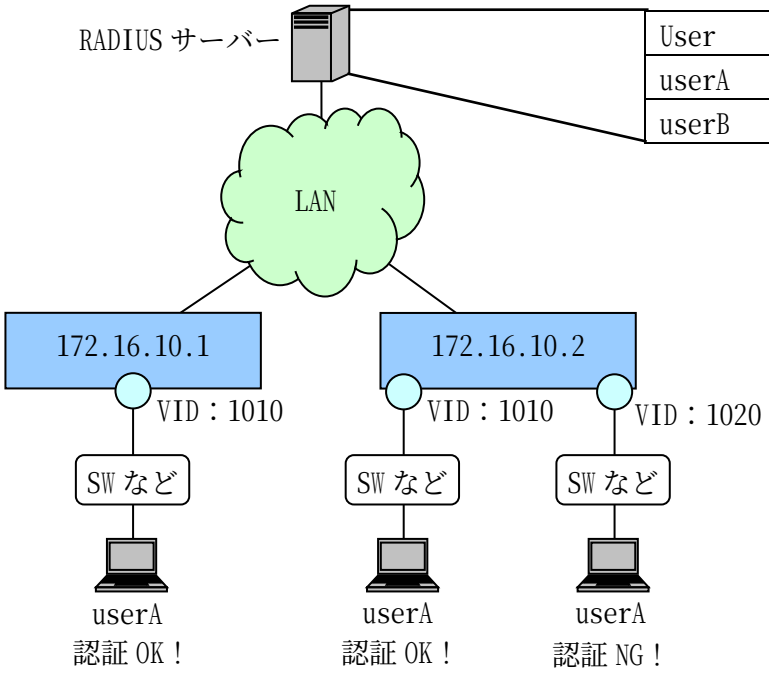
6.3.3 NAS-Identifier

「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 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。

図 6-3 の例では、以下の動作になります。

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



User	Password	NAS-Identifier
userA	passwordA	1010
userB	passwordB	1020

図 6-3 NAS-Identifier 設定時のアクセス制限

6.3.4 NAS 属性の組み合わせ

認証制限として以下の 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。

図 6-4 の例では、以下の動作になります。

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

User	Password	NAS-IP-Address	NAS-Identifier
userA	passwordA	172.16.10.1	1010
userB	passwordB	172.16.10.2	1020

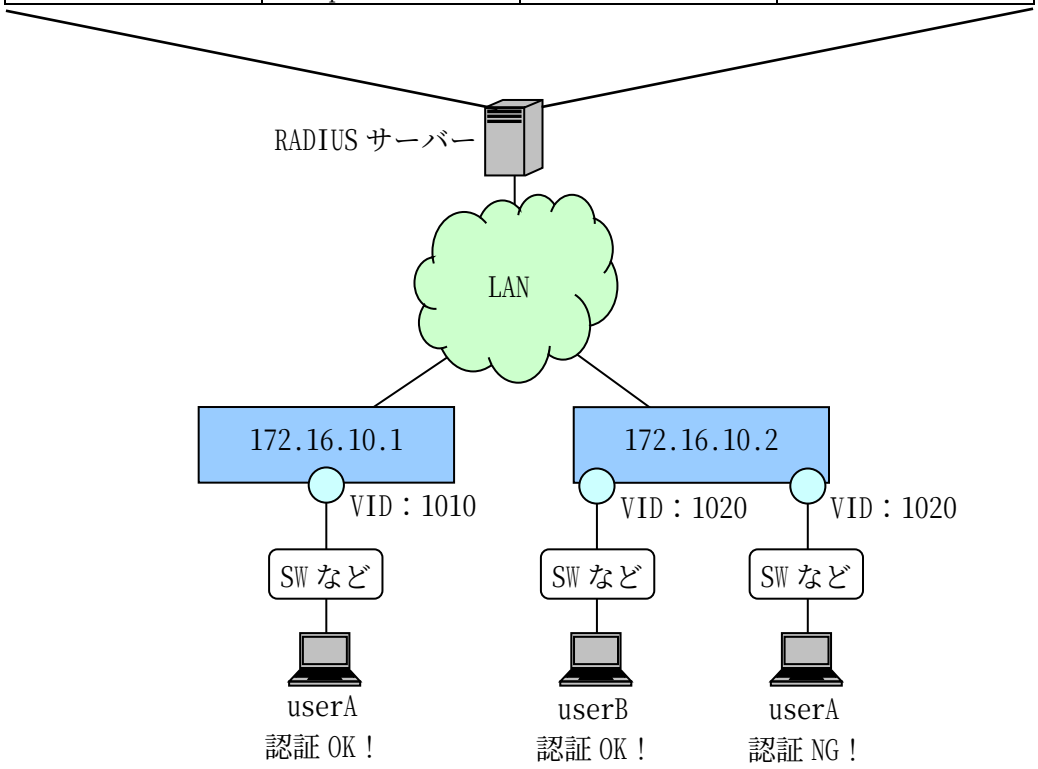


図 6-4 NAS-IP-Address＋NAS-Identifier 組合せ設定時のアクセス制限

6.4 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 6.2 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色々ありますが、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 6-5 に構成例を示します。

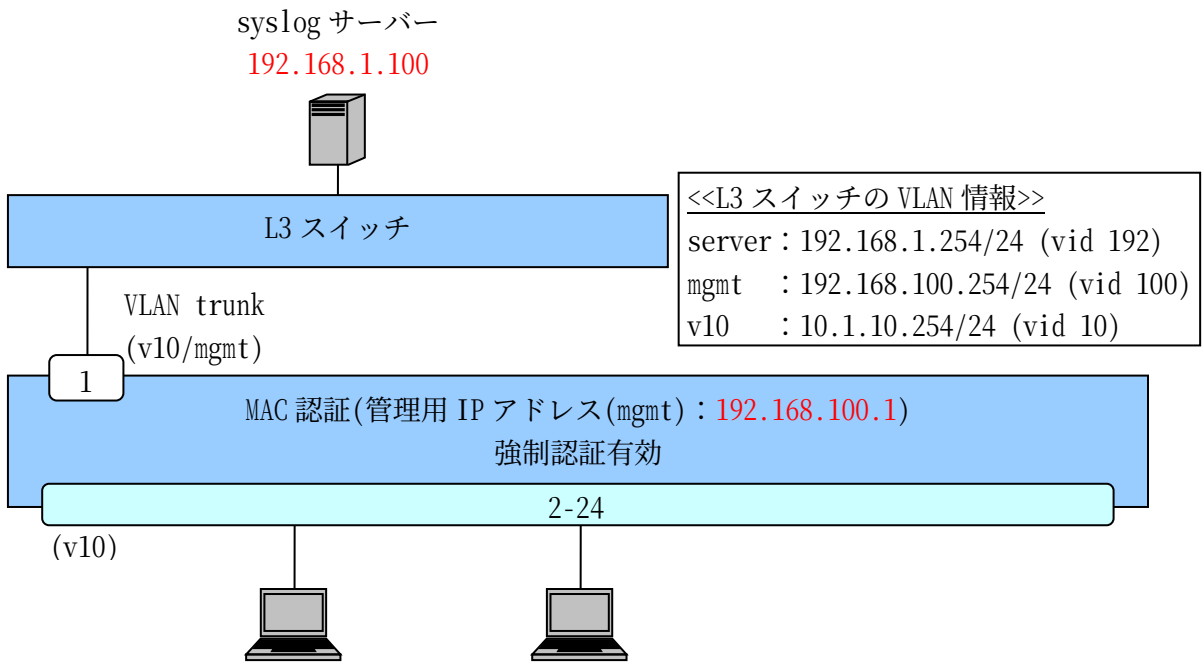


図 6-5 強制認証機能を使用した MAC アドレス自動収集

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 サーバーの登録(優先度：notice 以上のログを送信)

(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(1024 台) (必須)
                    ※ 1024 台を最大としています。

(config-a-def)# mac-authentication port 1/2-24
                ・・・MAC 認証ポート(1/2-24) (必須)

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

syslog サーバーには、1 台の端末が認証されるごとに以下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=1/5 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ください。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させてしまうため、注意してください。

6.5 端末認証後のパケットフィルター2(アクション none)

端末認証後のみパケットを転送するフィルターを適用したい場合、パケットフィルター2 機能のアクション none を使用します。

表 6-2 に、AccessDefender のパケットフィルター2 グループ番号より小さいグループ番号で、パケットフィルター2 を設定したときの動作を示します(パケットフィルター2 のグループを使用する機能は、グループ番号が小さいほど優先的に動作します)。認証成功端末からのアクション none 対象パケットは転送されますが、認証失敗端末からのアクション none 対象パケットは転送されません。

表 6-2 AccessDefender 併用時のパケットフィルター2 動作

アクション	対象パケット受信時の動作
none	認証後のみ転送
authentication-bypass	認証結果に関わらず転送(認証処理は未動作) ※
permit	認証結果に関わらず転送(認証処理は動作)
deny	認証結果に関わらず破棄

※ MAC 認証有効ポートに認証バイパスを設定したとき、認証バイパスの対象となるフレームが自局 IP アドレス宛などの CPU 宛てである場合やソフト中継される場合、認証が動作します。
MAC 認証に失敗し、discard 登録された端末の通信が認証バイパスの対象となる場合でも、認証バイパスにより通信は可能です。
この認証動作を回避する場合は、mac-authentication bypass-frame-check enable コマンドを有効に設定してください。但し、mac-authentication bypass-frame-check enable コマンドには使用制限があります。詳細は 3.25 MAC 認証有効ポートにおける認証バイパス対象フレームの認証回避の注意事項を参照してください。

同一グループにアクション none と deny を設定した場合、小さいルール番号の動作が優先されます。

図 6-6 に AccessDefender とパケットフィルター2 のアクション none、及び deny を併用した構成例を示します。192.168.100.100/32 宛パケットにアクション none、192.168.100.0/24 宛パケットに deny を設定します。端末 A(認証済)から 192.168.100.100/32 宛パケットは認証スイッチで転送されますが、端末 B(未認証)から 192.168.100.100/32 宛パケットは破棄されます。一方、アクション deny 対象パケットは認証結果に関わらず破棄されるため、端末 A、及び端末 B から 192.168.100.0/24 宛(192.168.100.100/32 除く)のパケットは破棄されます。なお、本動作は AccessDefender のパケットフィルター2 グループ番号より小さいグループ番号で、アクション none、及び deny を設定した場合の動作です。

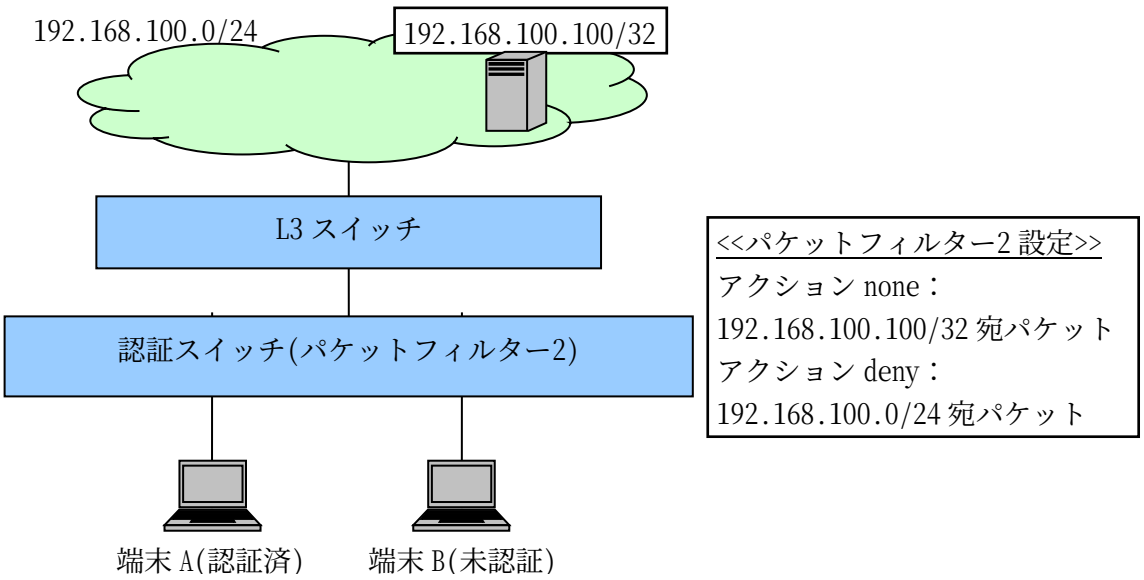


図 6-6 AccessDefender(アクション none 併用)構成例

図 6-6 の構成例における認証スイッチの設定例を示します(VLAN、認証の基本的な設定は省略します)。

```
(config)# access-defender
(config-a-def)# packet-filter2 group 6
              ・・・AccessDefender が使用するパケットフィルター2 の先頭グループ番号を設定

(config)# packet-filter2
(config-filter)# 1 1 action none
(config-filter)# 1 1 condition ipv4 dst ip 192.168.100.100/32
(config-filter)# 1 1 assign vlan 1
              ・・・グループ 1、ルール 1 にアクション none を設定

(config-filter)# 1 2 action deny
(config-filter)# 1 2 condition ipv4 dst ip 192.168.100.0/24
(config-filter)# 1 2 assign vlan 1
              ・・・グループ 1、ルール 2 にアクション deny を設定
```

7 制限事項、及び注意事項

AccessDefender における制限事項、及び注意事項を示します。

最新情報はコマンドリファレンス、リリースノート、フィールドノーティスを参照してください。

7.1 動的 VLAN 割り当て使用時の注意点

7.1.1 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 7-1 に示した構成例において、端末 1、及び端末 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 のタグ付き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となってしまいます。

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、パケットフィルター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、パケットフィルター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。

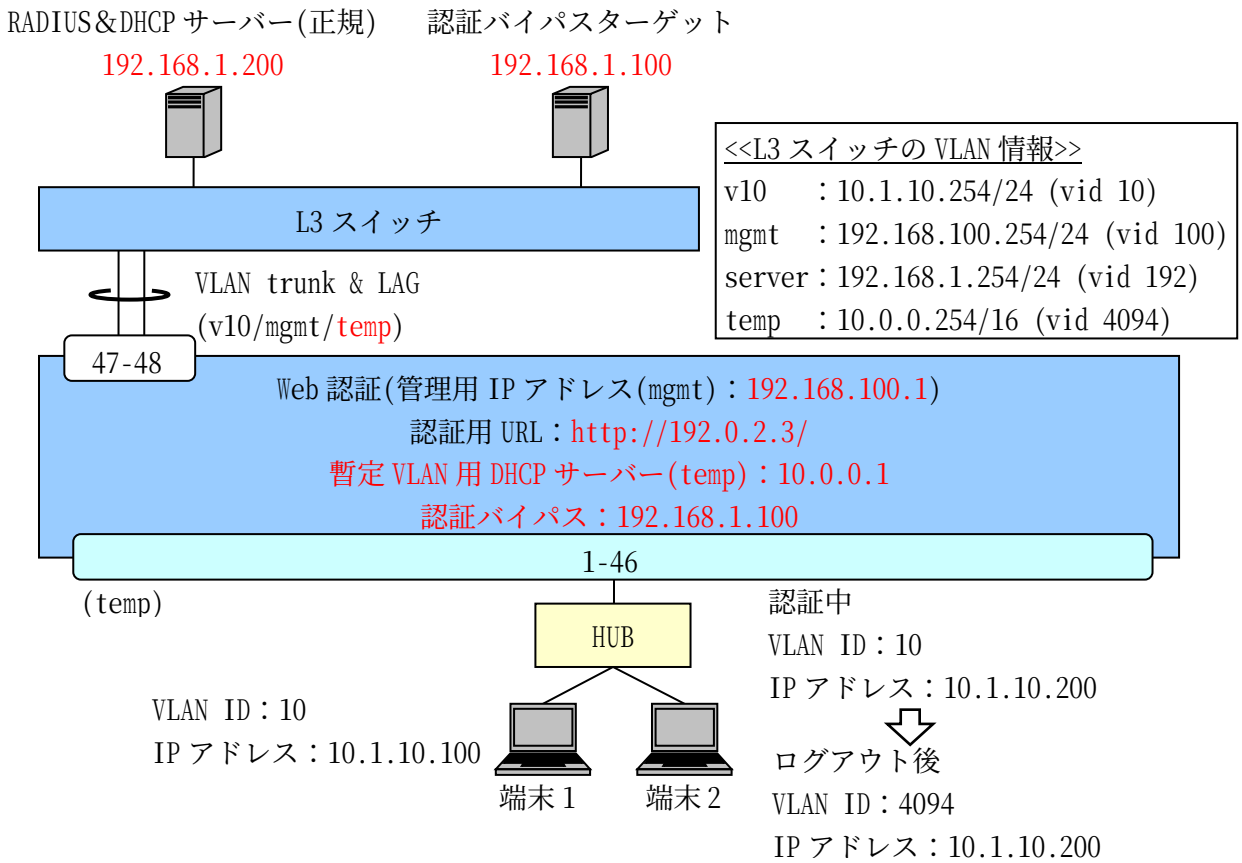


図 7-1 別 VLAN ID の IP アドレスを取得してしまう構成例

7.2 Windows 標準サプリカントにおける 802.1X の問題点

802.1X 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 7-2 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、サプリカントに対して EAP-Request/EAP-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、サプリカントに対して EAP-Failure を送信します。ここで EAP-Failure を受信すると、Windows 端末のサプリカントは 20 分間認証動作を停止してしまいます。

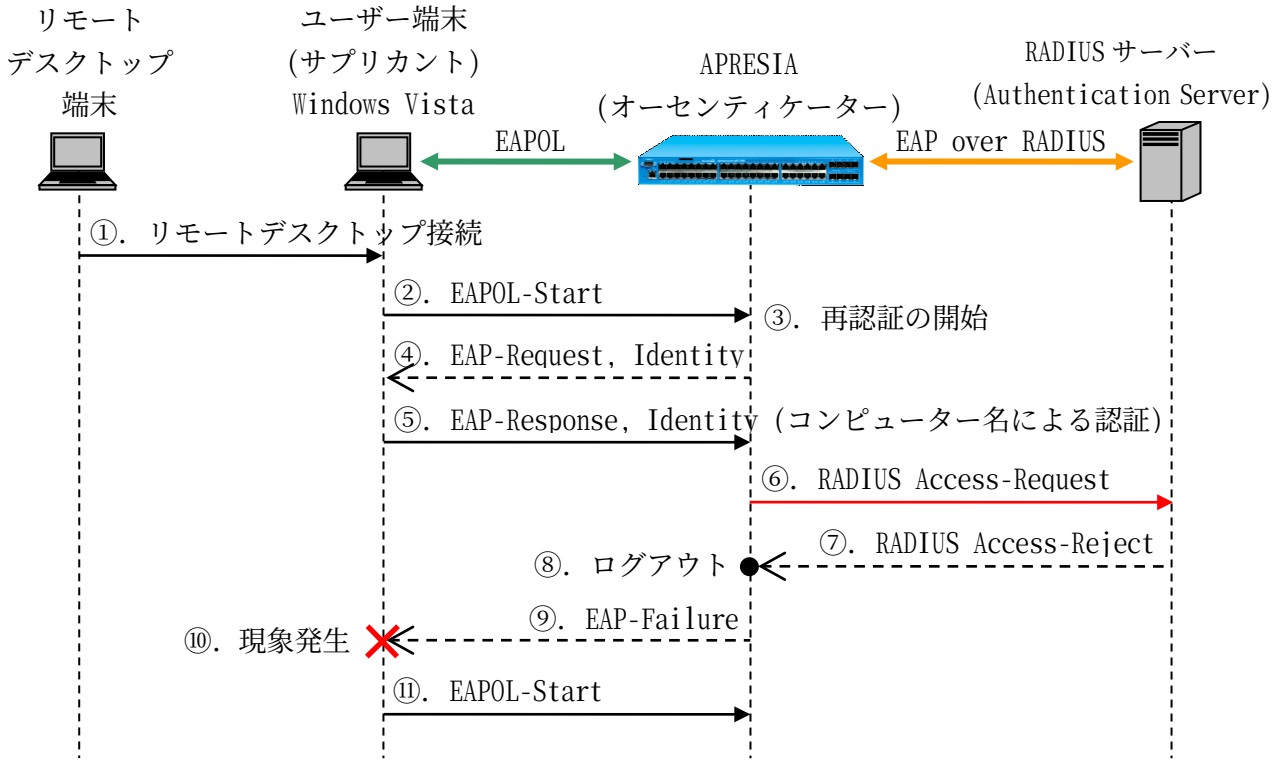


図 7-2 リモートデスクトップ接続によるログアウト時の問題点

7.2.1 Active Directory 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。

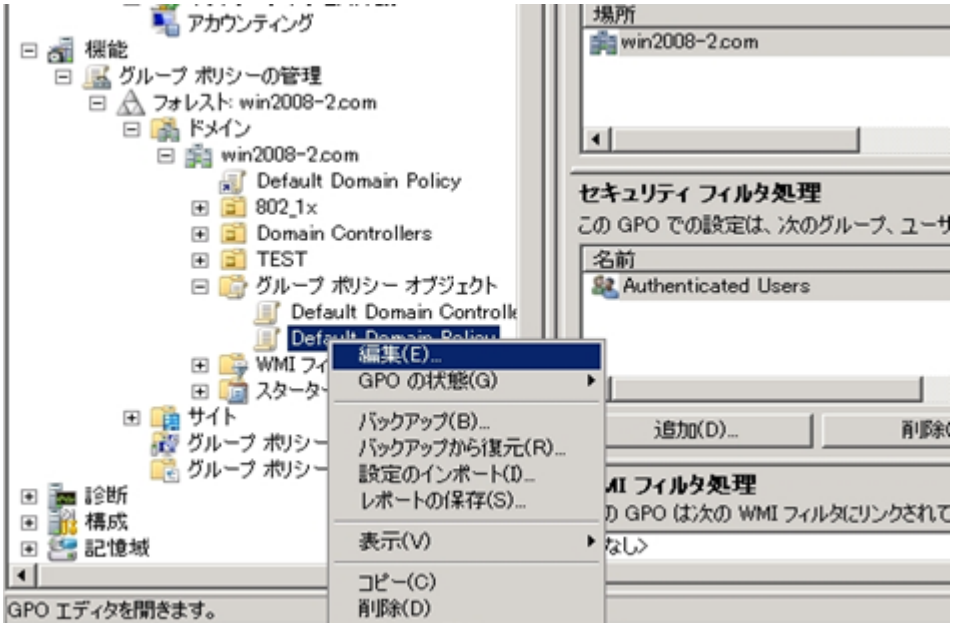


図 7-3 Default Domain Policy の編集

(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(IEEE 802.3)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。

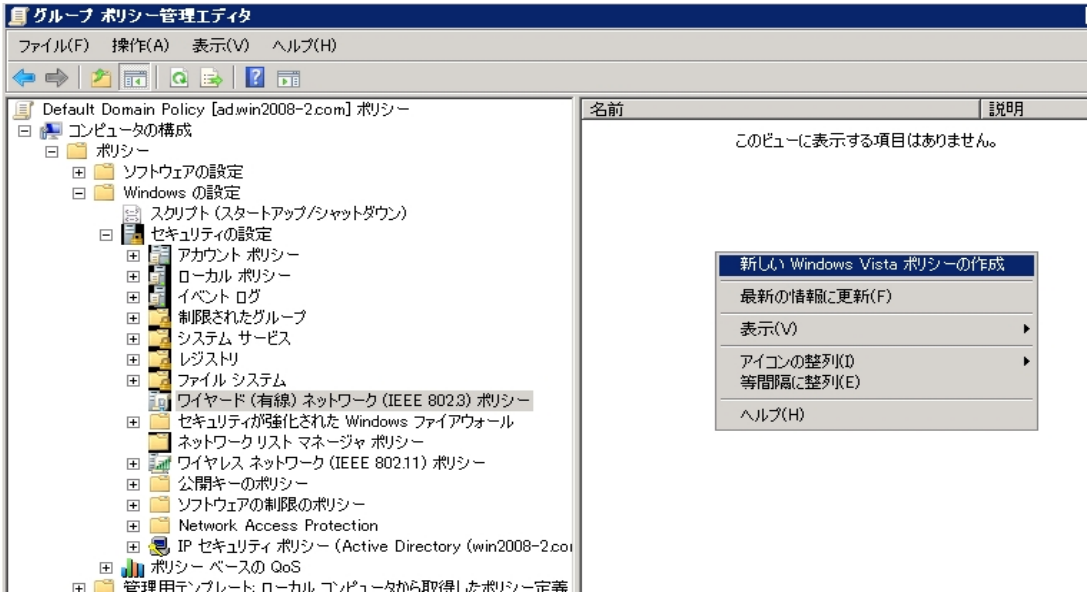


図 7-4 新しい Windows Vista ポリシーの作成

(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。

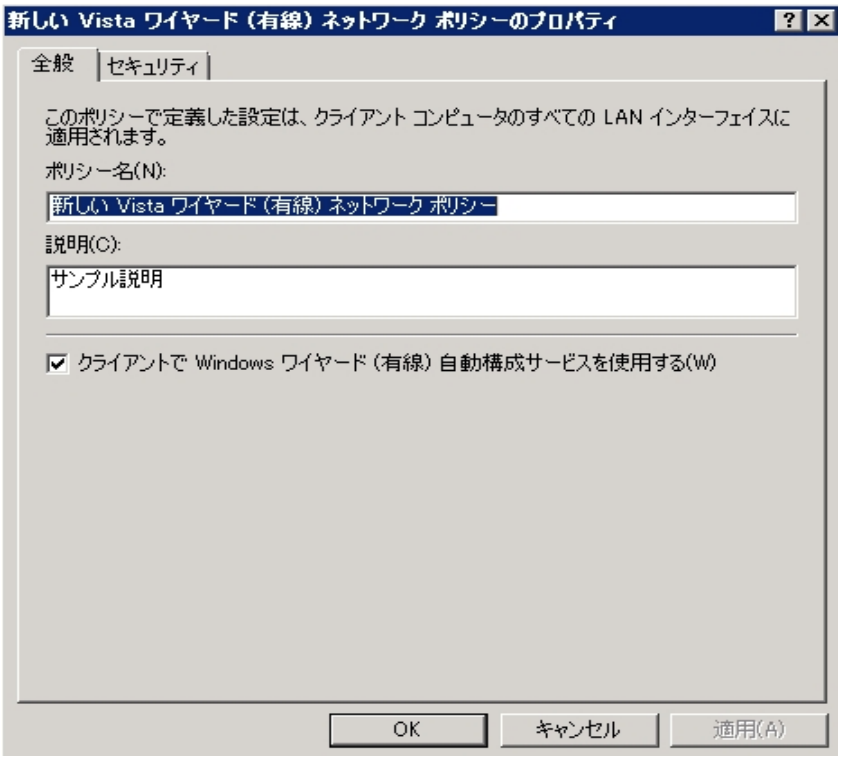


図 7-5 全般タブ

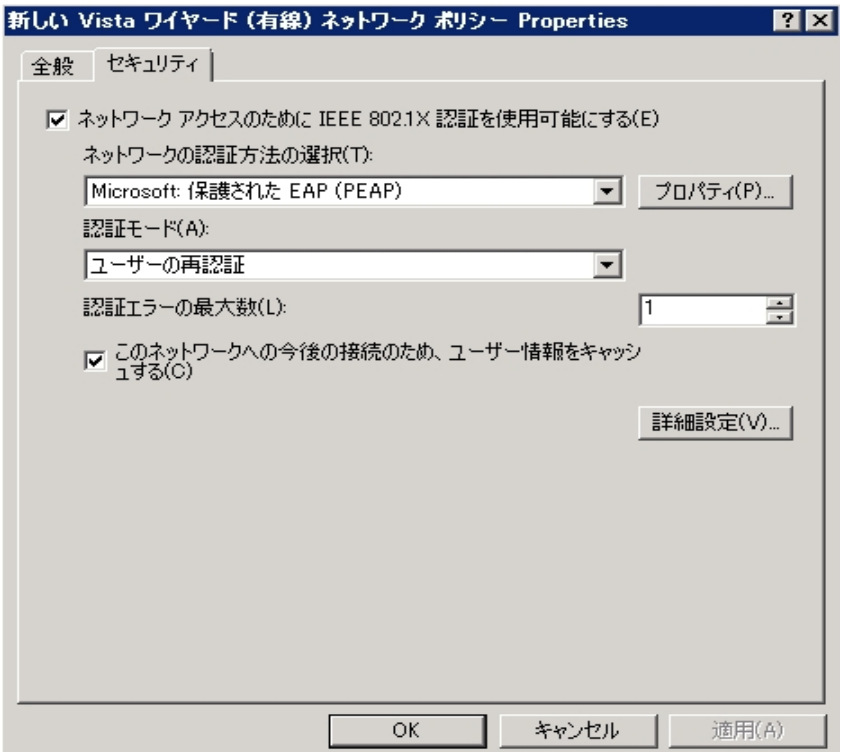


図 7-6 セキュリティタブ

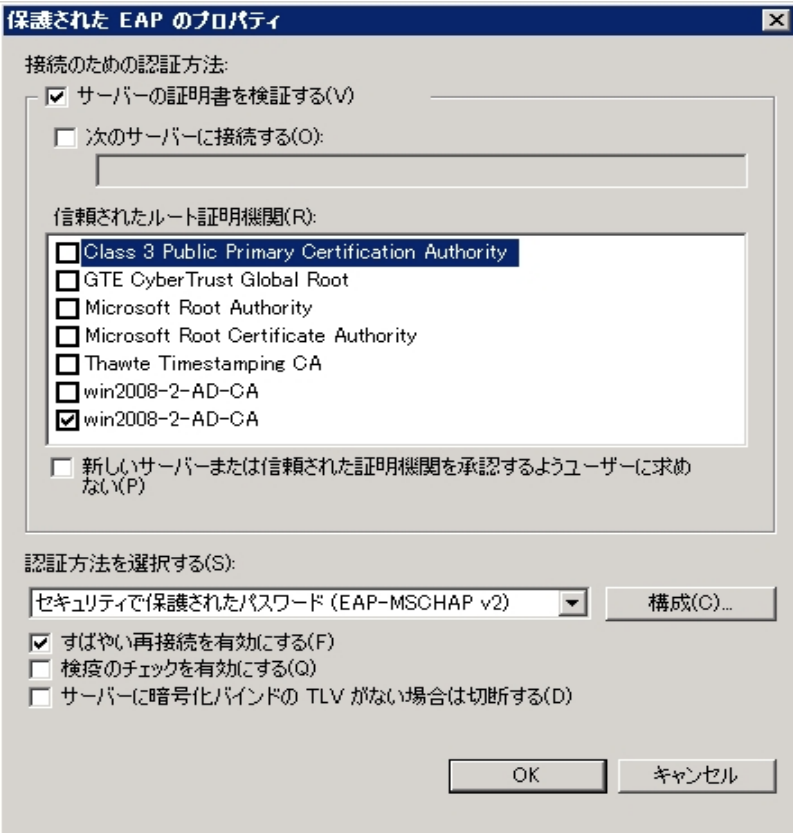


図 7-7 保護された EAP のプロパティ

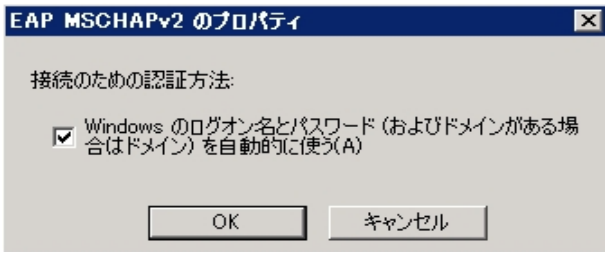


図 7-8 EAP MSCHAPv2 の構成

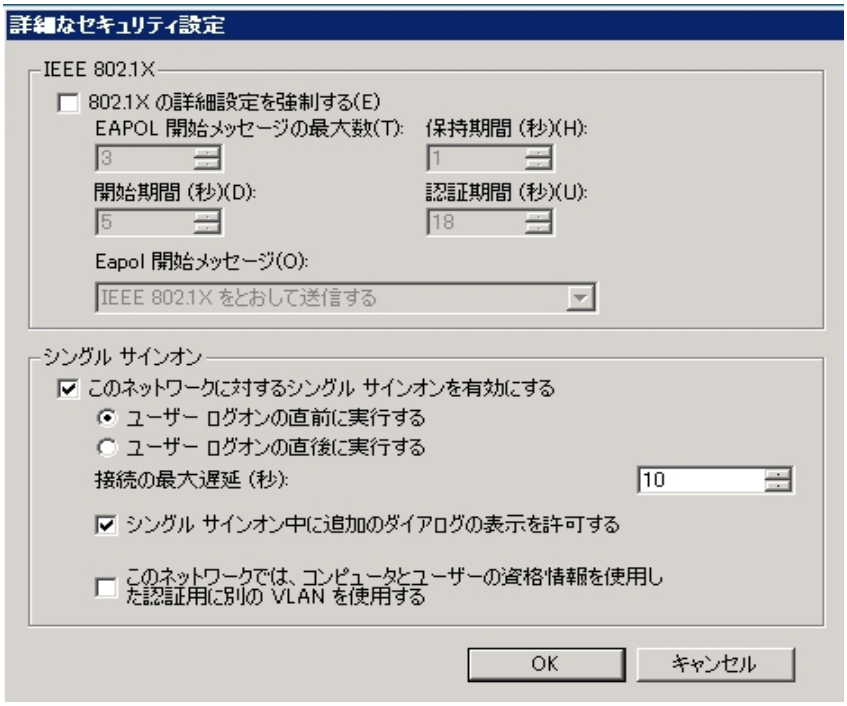


図 7-9 詳細なセキュリティ設定

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ブートが必要です(リブ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:: WrCnlLK4WU+cJTnmm6oWhA==
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:: xyfFOwYm602M/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;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;DA)(A;;RPWPCRCCDCLCLORCWOWDSDDTSW;;;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 Directory 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:¥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

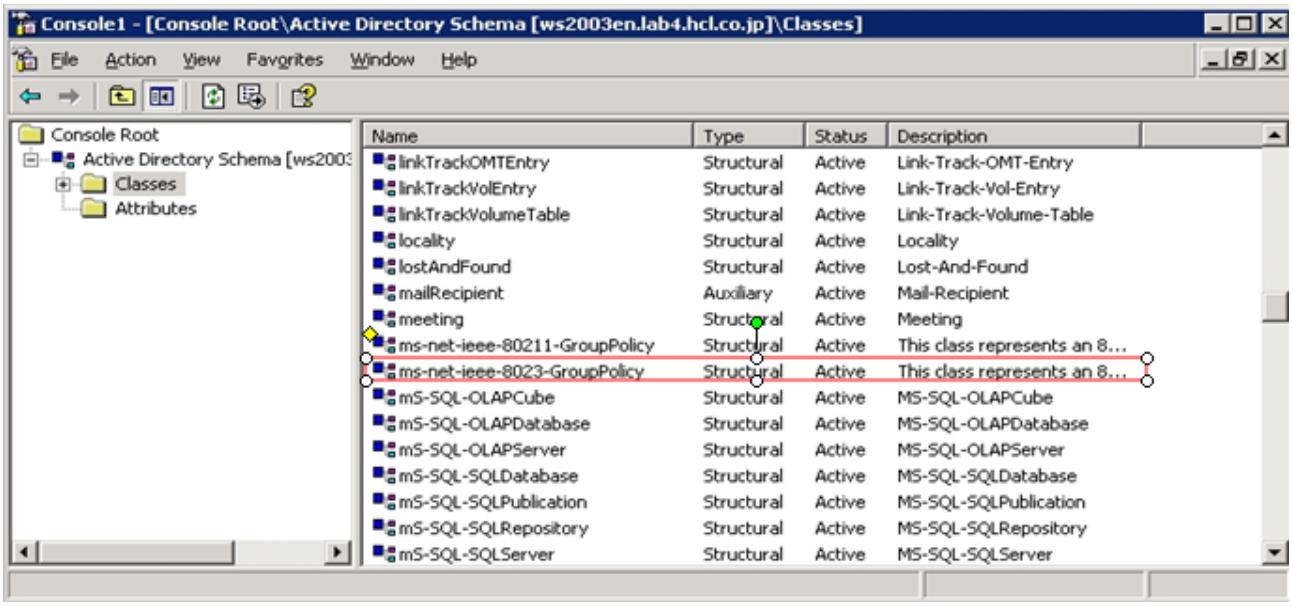


図 7-10 スキーマの確認

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。

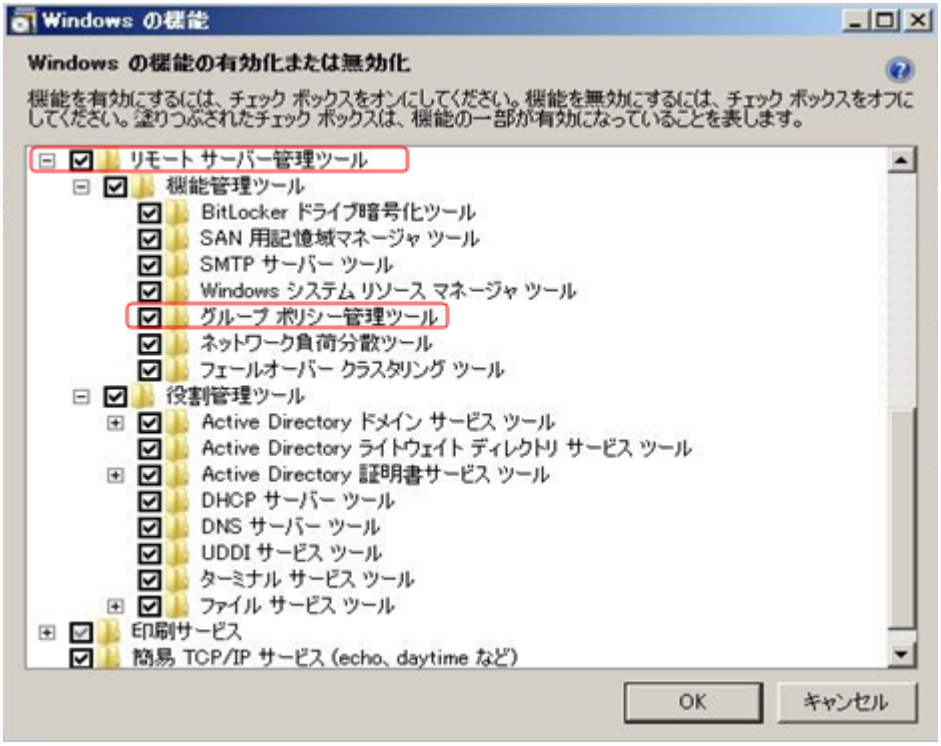


図 7-11 スキーマの確認

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

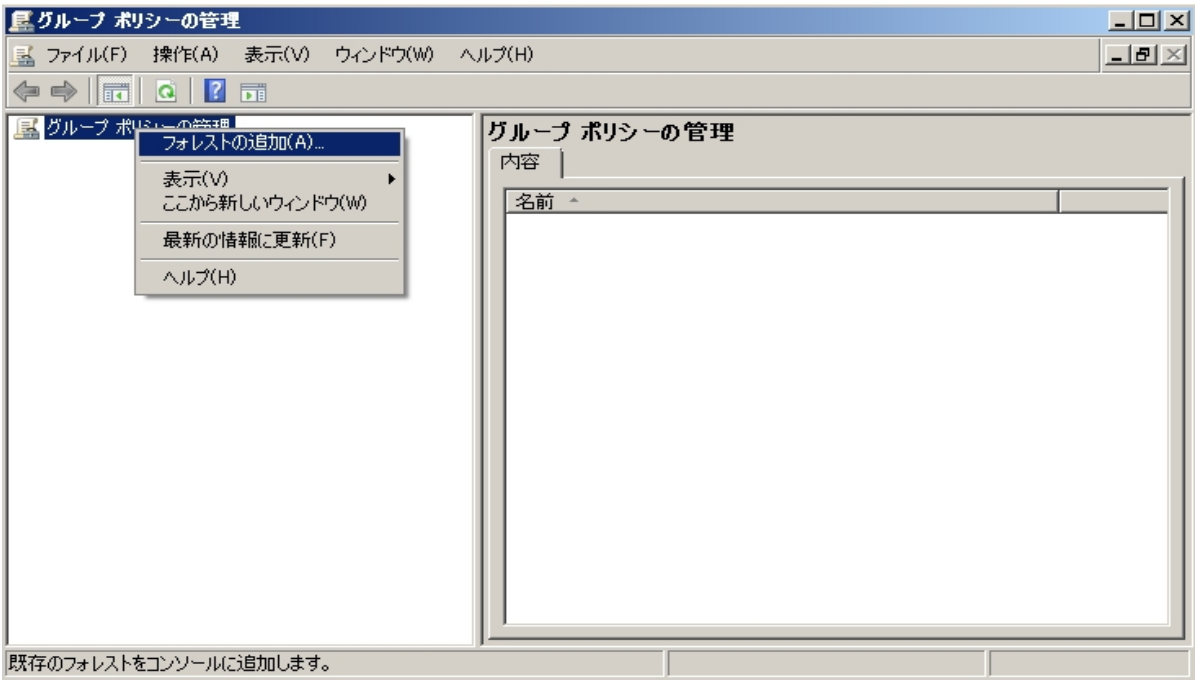


図 7-12 フォレストの追加

b) フォレスト内のドメイン名を入力

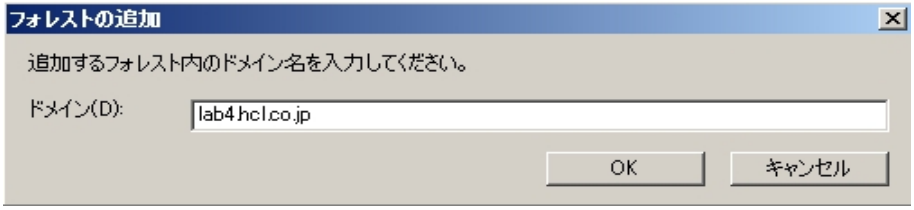


図 7-13 フォレスト内ドメイン名の入力

c)　フォレスト追加完了

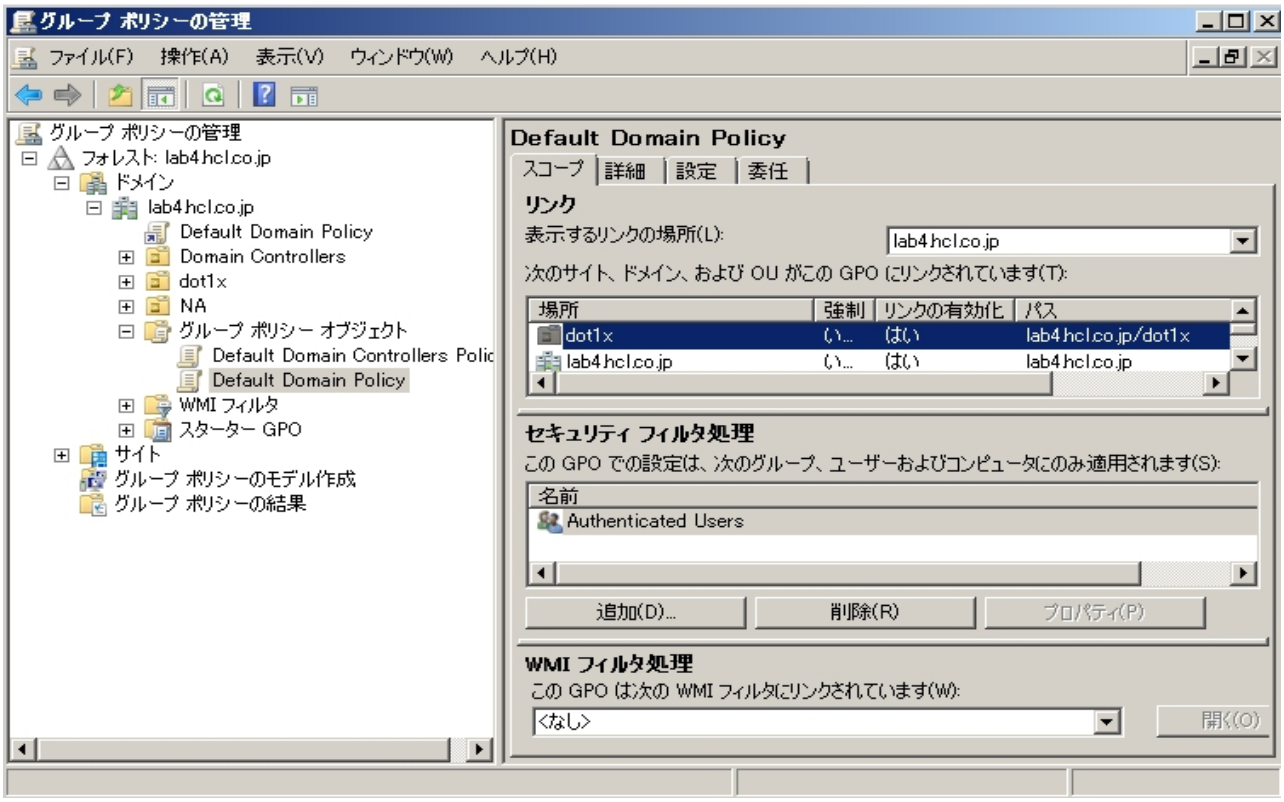


図 7-14 フォレスト追加完了

(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

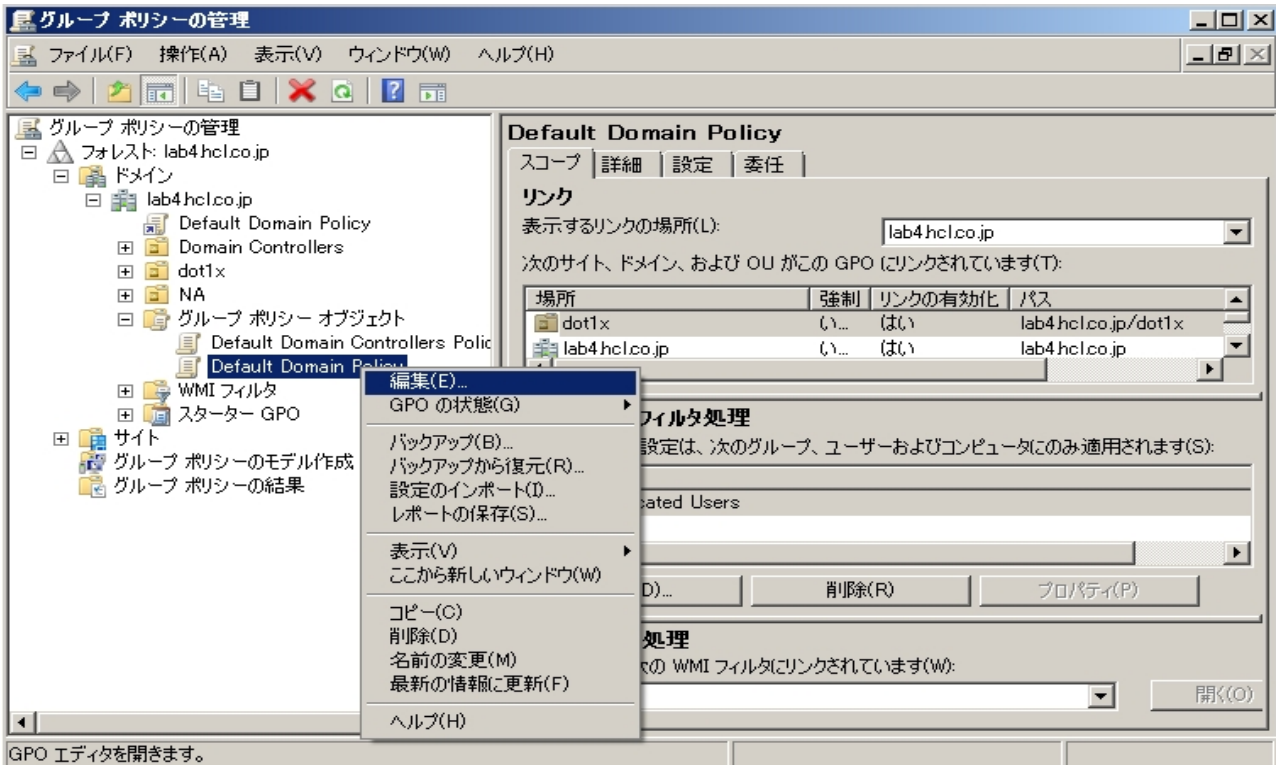


図 7-15 グループポリシーの編集

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

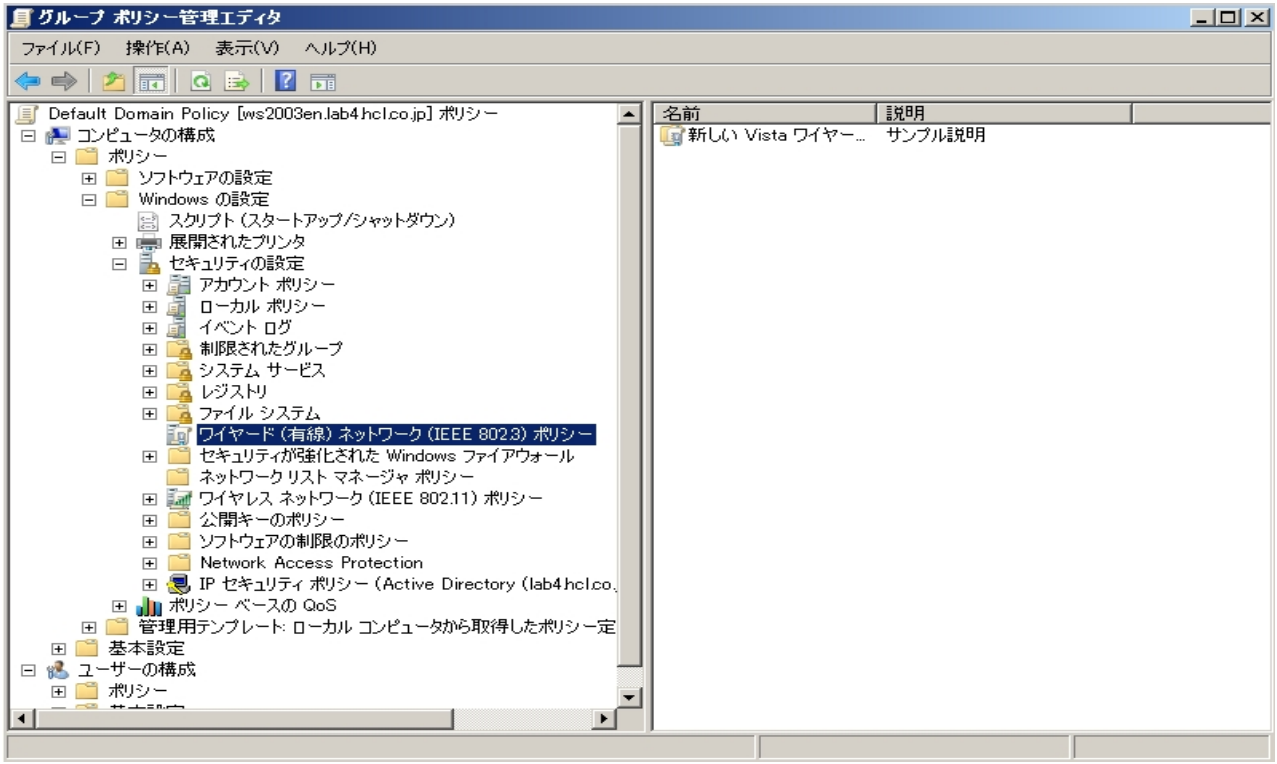


図 7-16 ワイヤードネットワークポリシーの編集

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。

7.2.2 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

よって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。

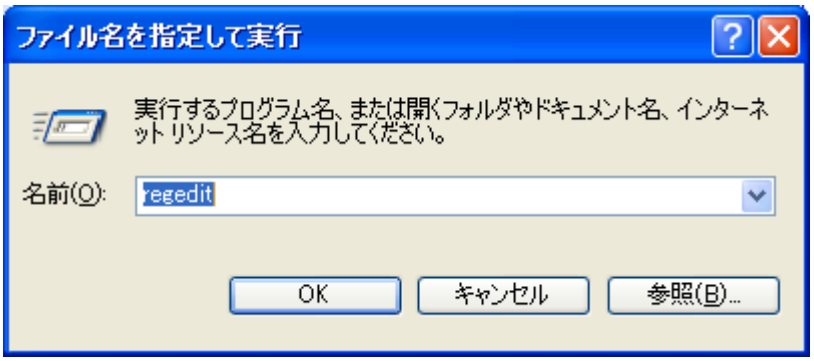


図 7-17 レジストリエディタの起動

(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

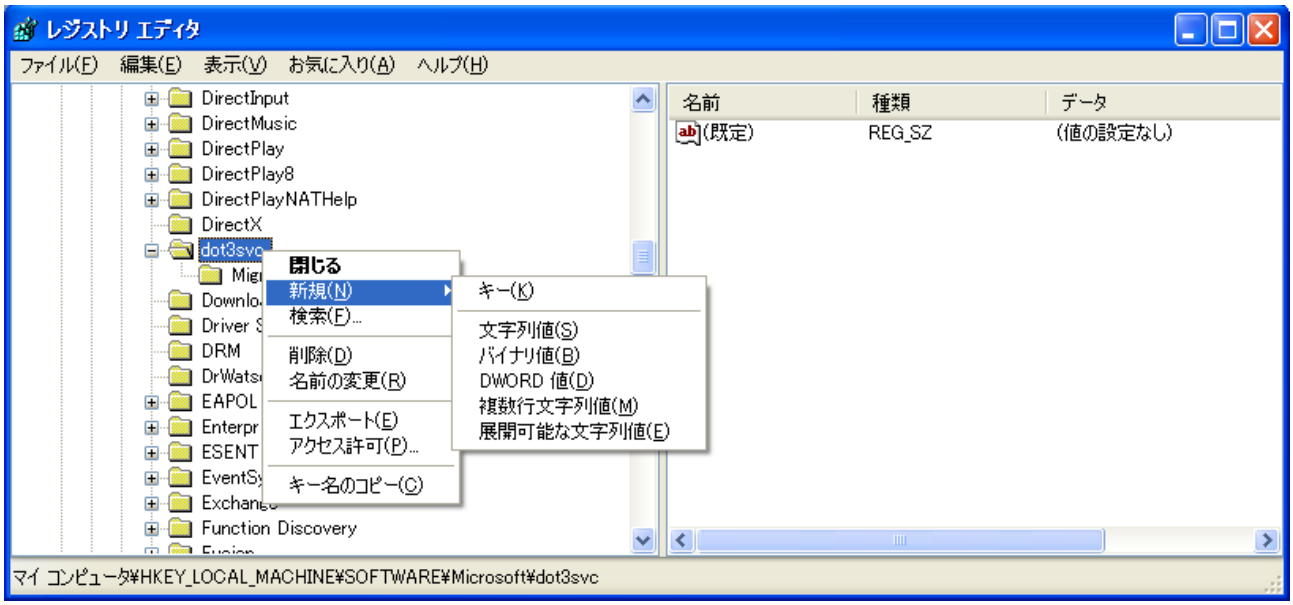


図 7-18 レジストリ変更

(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。

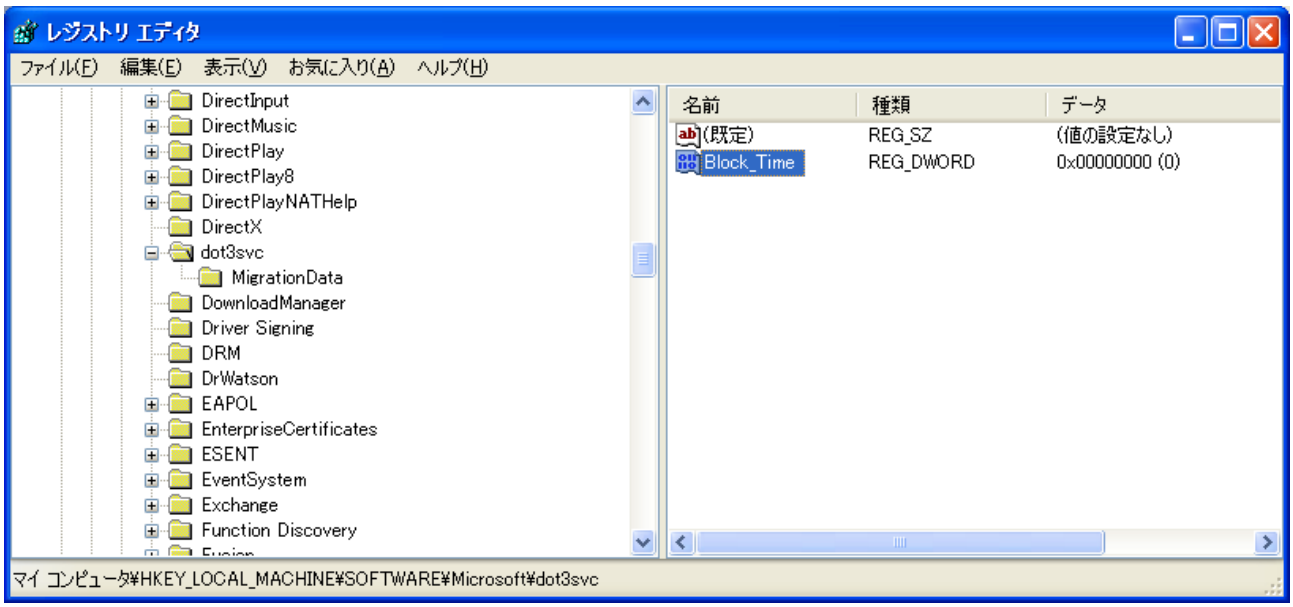


図 7-19 レジストリ変更

(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。

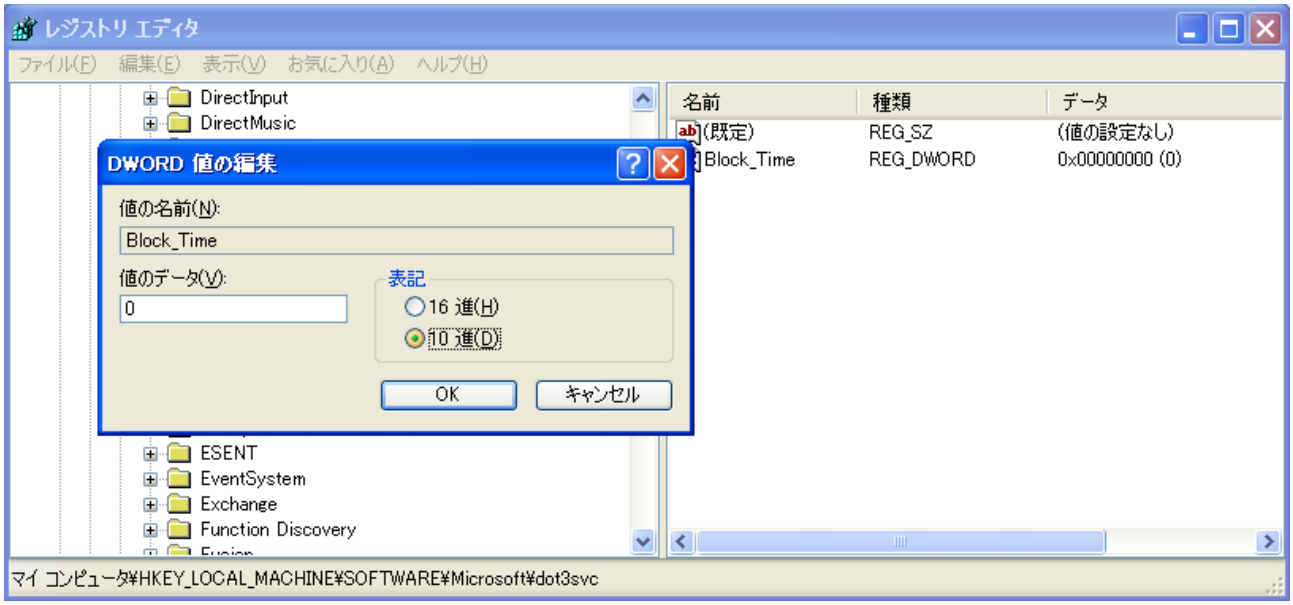


図 7-20 レジストリ変更

(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。

7.2.3 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で、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。サプリカントから EAPOL-Start フレームを受信しても、APRESIA は EAP-Request/EAP-Identity を返さず、認証動作を行いません。サプ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、不意な再認証の回避ができます。

(config-a-def)# dot1x (port <PORTRANGE>) | (lag <LAGRANGE>) | (mlag <MLAGRANGE>) ignore-eapol-start

・・・PORTRANGE　　ポート番号（複数指定可能）
・・・LAGRANGE　　LAG ID <1-32>（複数指定可能）
・・・MLAGRANGE　　ドメイン名/MLAG ID <1-64>（複数指定可能）

しかし、本機能を設定することでサプリカントからの 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 の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ない
- Windows からの初期化要求に反応しなくなるため、定期的に発行されるスイッチからの初期化要求がくるまで、認証が開始できない(スイッチ側からの定期初期化要求送出間隔は 30 秒)

以下の図 7-21 のような動作になります。

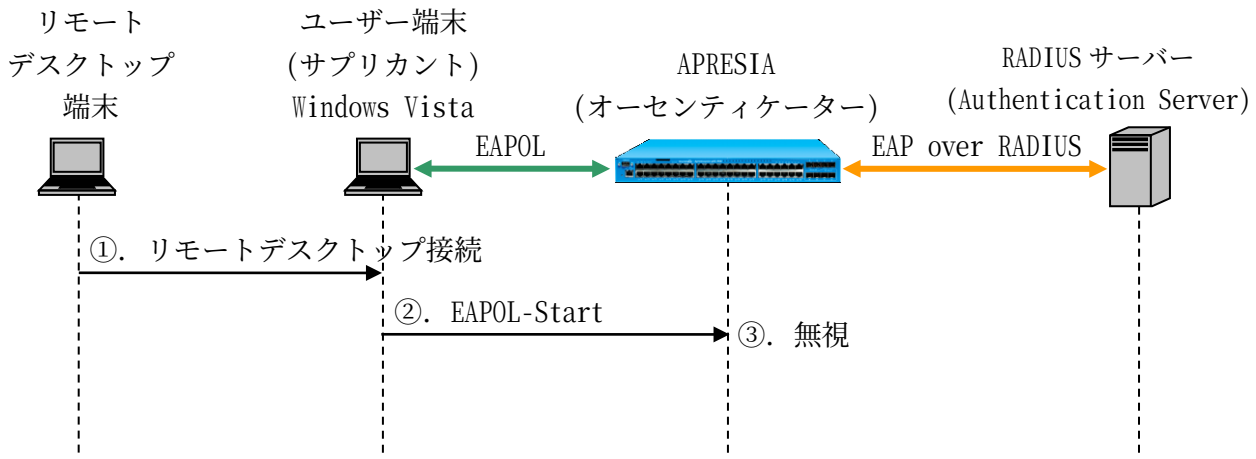


図 7-21 EAPOL-Start 受信による認証の抑止コマンドによる回避

スイッチ側からの定期初期化要求送出間隔は、dot1x timeout tx-period コマンドで短縮することが可能ですが、0(送出しない)は指定しないように注意してください。詳細は、3.17 認証開始時の EAP-Request/EAP-Identity の抑制を参照してください。

本機能を使用すると、本装置が EAP-Request/EAP-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、3.17 認証開始時の EAP-Request/EAP-Identity の抑制を参照してください。

7.3 VRRP 併用時の注意点

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

(1) VRRP は VB は未サポートです。

(2) 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させてください。

(3) AccessDefender 認証ポートを VRRP の VLAN インターフェースとして設定している状態で、仮想 MAC アドレスを認証させる場合は以下のいずれかの処置を行ってください。

- access-defender static mac コマンドを設定する場合は VLAN ID に VRRP の VLAN インターフェース以外を指定する。
- MAC 認証で動的 VLAN を利用する場合は VRRP の VLAN インターフェース以外を指定する。

(4) 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します。

(5) 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です。

(6) DHCP Snooping との併用はできません。

MAC 認証と VRRP 併用構成例を図 7-22 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。

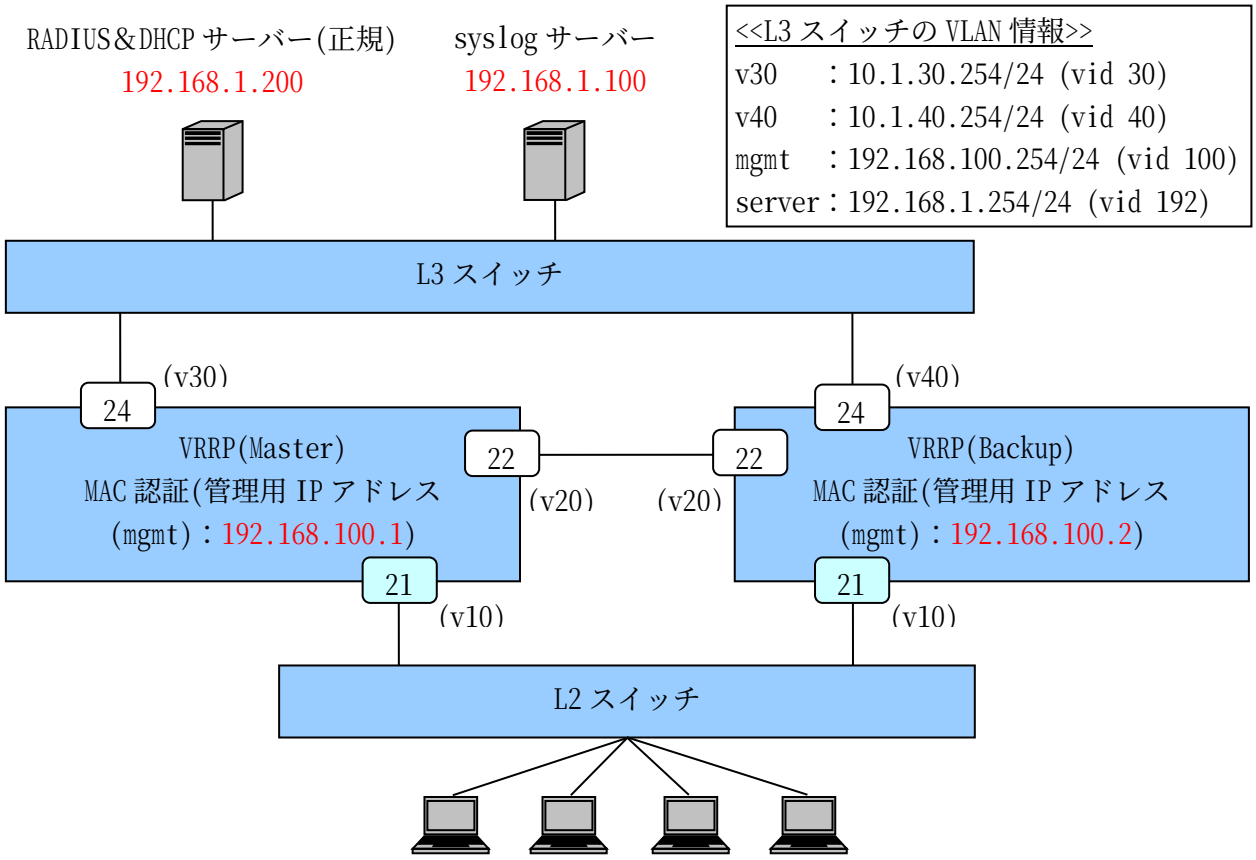


図 7-22 MAC 認証と VRRP 併用構成例

図 7-22 での VRRP(Master)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 30 name v30
(config-vlan)# vlan 100 name mgmt
              ・・・VLAN の設定(管理用 VLAN 名を"mgmt"、
                   ユーザーVLAN 名を"v10"、"v20"、"v30"とする)

(config)# interface port 1/21
(config-if-port)# switchport access vlan 10
(config)# interface port 1/22
(config-if-port)# switchport access vlan 20
(config)# interface port 1/24
(config-if-port)# switchport access vlan 30
              ・・・ユーザーVLAN を access ポートとして設定
                   ※ 認証前のポートは未認証端末同士も通信不可となります。

(config)# interface vlan 10
(config-if-vlan)# ip address 192.168.10.1/24
(config)# interface vlan 20
(config-if-vlan)# ip address 192.168.20.1/24
(config)# interface vlan 30
(config-if-vlan)# ip address 192.168.30.2/24
              ・・・ユーザーVLAN に IP アドレスを設定

(config)# interface vlan 100
(config-if-vlan)# ip address 192.168.100.1/24
              ・・・管理用 VLAN(mgmt)の IP 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 (必須)

(config)# router ospf 1
(config-router)# passive-interface vlan 10
(config-router)# network 0.0.0.0 0.0.0.0 area 0
              ・・・OSPF を設定 (必須)

(config)# router vrrp 10 vlan 10
(config-router)# virtual-ip 192.168.10.1 master
(config-router)# accept-mode enable
(config-router)# enable
```

・・・VRRP(Master)を設定（必須）

```
(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(プライマリー)（必須）

※ INDEX：1 の RADIUS サーバーを MAC 認証のプライマリーとしています。

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

・・・最大認証端末(128 台)（必須）

※ 128 台を最大としています。

```
(config-a-def)# mac-authentication port 1/21
```

・・・MAC 認証ポート(1/21)（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）

8 AccessDefender 関連ログ

8.1 認証ログ表示(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」を参照してください。

表 8-1 認証ログ一覧

No.	レベル	メッセージ構文	内容
1	notice	<radius|force|local> authentication succeeded : uid=<USER>	認証成功
2	notice	<web|gateway|mac|dot1x|dhcpsnooping|static> : login succeeded : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : login succeeded : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : login succeeded : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>]	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|static> : login failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> [vid=<VID>] [new vid=<VID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : login failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> [vid=<VID>] [new vid=<VID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : login failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port= MLAG <DOMAIN>/<MLAG ID> [vid=<VID>] [new vid=<VID>]	ログイン失敗
5	notice	<web|gateway|mac|dot1x|dhcpsnooping|static> : logout(<TYPE>): uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : logout(<TYPE>): uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : logout(<TYPE>): uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> [vid=<VID>] [new vid=<VID>] [class=<CLASSID>]	ログアウト ※
6	warning	<web|gateway|mac|dot1x|dhcpsnooping|discard|deny|static> : the number of terminals on switch is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> [vid=<VID>]	装置の最大認証数によるログイン不可

No.	レベル	メッセージ構文	内容
		<web|gateway|mac|dot1x|dhcpsnooping|discard|deny|static> : the number of terminals on switch is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> [vid=<VID>] <web|gateway|mac|dot1x|dhcpsnooping|discard|deny|static> : the number of terminals on switch is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> [vid=<VID>]	
7	warning	<web|gateway|mac|dot1x|dhcpsnooping|static> : the number of terminals on port <PORTNO> is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> [vid=<VID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : the number of terminals on port <LAGNO> is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> [vid=<VID>] <web|gateway|mac|dot1x|dhcpsnooping|static> : the number of terminals on port MLAG <DOMAIN>/<MLAG_ID> is full : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> [vid=<VID>]	インターフェースの最大認証数によるログイン不可
8	warning	<web|mac|dot1x> : vlan assignment failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> vid=<VID> new vid=<VID> <web|mac|dot1x> : vlan assignment failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> vid=<VID> new vid=<VID> <web|mac|dot1x> : vlan assignment failed : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> vid=<VID> new vid=<VID>	VLAN 変更失敗
9	warning	port <PORTNO> has already been assigned to another vlan : uid=<USER> port=<PORTNO> [new vid=<VID>] port <LAGNO> has already been assigned to another vlan : uid=<USER> port=<LAGNO> [new vid=<VID>] port MLAG <DOMAIN>/<MLAG ID> has already been assigned to another vlan : uid=<USER> port=MLAG <DOMAIN>/<MLAG ID> [new vid=<VID>]	VLAN 変更失敗(RADIUS/Local 認証結果受信時)
10	warning	<web|mac|dot1x|static> : port <PORTNO> has already been assigned to another vlan : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> vid=<VID> [new vid=<VID>] <web|mac|dot1x|static> : port <LAGNO> has already been assigned to another vlan : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> vid=<VID> [new vid=<VID>] <web|mac|dot1x|static> : port MLAG <DOMAIN>/<MLAG ID> has already been assigned to another vlan : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> vid=<VID> [new vid=<VID>]	VLAN 変更失敗(端末設定時)
11	warning	radius(<IPADDR>) timeout : uid=<USER>	RADIUS タイムアウト(RADIUS サーバーからの

No.	レベル	メッセージ構文	内容
			応答を受信できなかった)
12	info	dhcpsnooping : mode-timer started	MODE TIMER 設定変更
13	info	dhcpsnooping : mode changed to deny automatically	TIMER 終了による MODE の変更(DENY)
14	info	dhcpsnooping : mode changed to deny manually	CLI による MODE 変更(DENY)
15	info	dhcpsnooping : mode changed to permit manually	CLI による MODE 変更(PERMIT)
16	info	dhcpsnooping : mode changed to mac-authentication mode enable	CLI による MODE 変更(MAC-AUTHENTICATION 有効)
17	info	dhcpsnooping : mode changed to mac-authentication mode disable	CLI による MODE 変更(MAC-AUTHENTICATION 無効)
18	notice	web : login rejected : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<PORTNO> vid=<VID> ttl=<TTL> web : login rejected : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=<LAGNO> vid=<VID> ttl=<TTL> web : login rejected : uid=<USER> mac=<MACADDR> ip=<IPADDR> port=MLAG <DOMAIN>/<MLAG ID> vid=<VID> ttl=<TTL>	TTL フィルタによるログイン拒否
19	info	<CLIENT_IP>(<USER_AGENT>) <PROTOCOL> <URL>	認証 Web アクセス

※ 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	インターフェース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	再認証時にサプ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
reauth class change	再認証時にクラス ID 変更検出によるログアウト
port initialization	インターフェース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

TYPE	ログアウト種別
ping	logout ping 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 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。
2	No Packet-filter2 entry.	packet-filter2 max-rule コマンド未設定時、web-authentication enable コマンドと mac-authentication enable コマンドは指定できません。
3	Violation of RADIUS Index.	aaa authentication コマンド設定時、RADIUS サーバーの指定 index1 と index2 の設定値として、同じ index は指定できません。
4	No RADIUS entry.	aaa authentication コマンド設定時、RADIUS サーバーの指定 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。
5	% 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

SSL(Secure Socket Layer)とは、サーバーと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サーバーと端末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可能になります。

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。

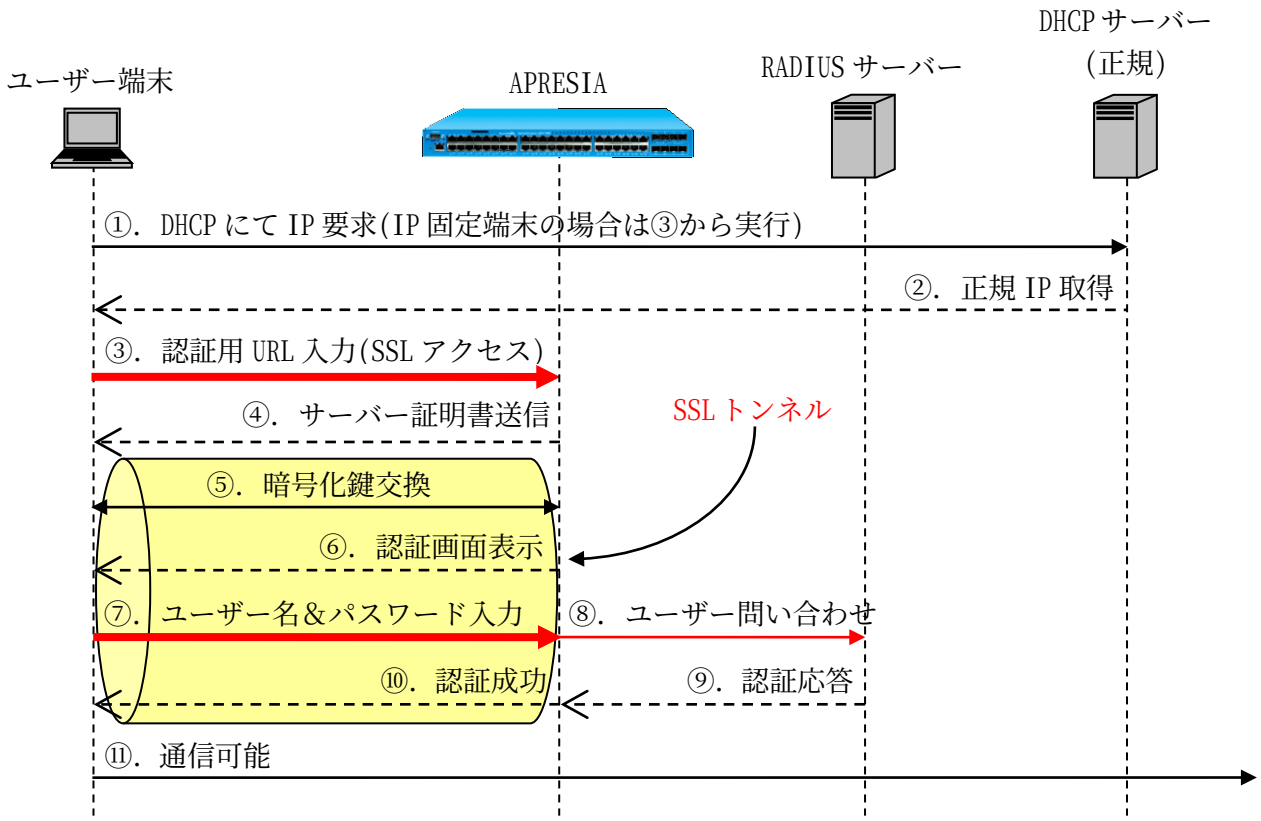


図 9-1 SSL での認証フロー

9.1 SSL 設定概要

APRESIA のファームウェアには、あらかじ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ください。

■証明書要求(CSR：Certificate Signing Request)を装置で発行する場合(詳細は 9.2 証明書要求を装置で発行する場合を参照)

(1) 秘密鍵と証明書要求の生成
ssl gencsr コマンドにより、秘密鍵と証明書要求を生成します。

(2) 証明書要求のアップロード
copy csr tftpコマンドにより､本装置から証明書要求をTFTPサーバー上にアップロードします。

(3) 証明書の発行
証明書要求を認証局(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 file https-file コマンドにより、本装置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(詳細は 9.3 証明書要求を装置で発行しない場合を参照)

(1) 秘密鍵と証明書要求の生成
OpenSSL などのソフトウェアを使用し、秘密鍵と証明書要求を生成します。

(2) 証明書の発行
証明書要求を認証局(CA)に送付し、証明書を発行してもらいます。

(3) 証明書と秘密鍵のダウンロード
TFTP サーバー上に証明書と秘密鍵をおき、copy file https-file コマンドにより、本装置に証明書と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、明示的に指定してください。

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ください。

9.2 証明書要求を装置で発行する場合

9.2.1 秘密鍵と証明書要求の生成

ssl gencsr コマンドにより、秘密鍵と証明書要求を生成します。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 gencsr rsakey [ <KEYLENGTH> ]
                ・・・KEYLENGTH          鍵長を指定 <512-2048>
                                          • 省略した場合 1024
```

```
(config)# ssl gencsr rsakey 512
Country Name (2 letter code):JP
State or Province Name (full name):Tokyo
Locality Name (eg, city):shibuya-ku
Organization Name (eg, company):apresia
Organizational Unit Name (eg, section):network
Common Name (YOUR domain name):192.0.2.3
Email Address:xxx@apresia.jp
Generating a 512 bit RSA private key
..++++++++++++
...++++++++++++
Writing new private key
Writing to flash memory...
done.
```

表 9-1 証明書要求の項目

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	shibuya-ku	1～128
Organization	組織名	example.corp	1～64
Organizational Unit	部門名	section 1	1～64
Common Name	ドメイン名(必須)	http://www.example.com/	1～64
Email Address	電子メールアドレス	ttt@example.com	1～128

※Common Name 以外は省略可能

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。

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://192.0.2.3/」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、以下のようなセキュリティ警告が表示されます。

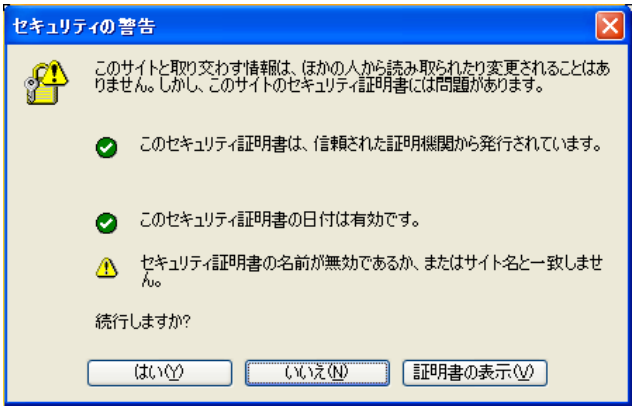


図 9-2 認証 URL 不一致によるセキュリティ警告

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。

生成した証明書要求は 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=shibuya-ku, O=apresia, OU=network, CN=192.0.2.
3/emailAddress=xxx@apresia.jp
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:9e:db:91:c9:1e:42:3c:fd:7a:06:c0:be:a2:89:
                    6a:10:56:8f:a0:2b:d2:c9:36:f5:f0:b7:ad:e4:2b:
                    86:5e:5d:36:43:3b:75:45:7f:bc:9f:e1:11:b7:db:
                    5a:18:a9:25:8b:5f:1a:37:e6:01:1e:40:6c:7c:1f:
                    fb:7d:fc:4f:f9
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: md5WithRSAEncryption
         29:3b:aa:46:97:64:0a:b2:b9:71:b0:1d:f2:40:0c:96:fa:cd:
         47:4b:e4:67:9a:cf:47:4f:df:87:8e:21:7e:4f:a6:bd:de:1a:
         7b:ce:5a:98:31:47:74:b3:a9:0f:e5:bd:54:81:4f:25:ff:ad:
         08:6e:be:07:76:b2:04:be:b9:ff
#
```

9.2.2 証明書要求のアップロード

copy csr tftp コマンドにより、装置から証明書要求を 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)へ証明書要求のアップロード
```

9.2.3 証明書の発行

証明書要求を認証局に送付し、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 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-----
MIICQDCCAakCAQIwDQYJKoZIhvcNAQEEBQAwgY0xCzAJBgNVBAYTAkpQMQ4wDAYD
VQQIEwVUb2t5bzETMBEGA1UEBxMKQ2hpeW9kYS1rdTEMMAoGA1UEChMDSENMMQww
CgYDVQQLEwNMQUIxHDAaBgNVBAMUE0FwcmVzaWFfQ0EoMS4xLjEuMSkxHzAdBgkq

・・・・・ 中略 ・・・・・

5oy7tc+1mAKshvPTNdjFHSQiptfymyJnGd/50//Zz0a5tXk+eQQLpLpypx2d6oWN
WvAD2CC763Z9GRQbDYlITb8Mz86YoJ061LpNhc8906fE1pIQf+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ください。

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 秘密鍵と証明書要求の生成

OpenSSL などのソフトウェアを使用し、秘密鍵と証明書要求を生成します。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、以下の 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                     【市区町村名】
Organization Name (eg, company) [My Company Ltd]:apresia          【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ください。

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。

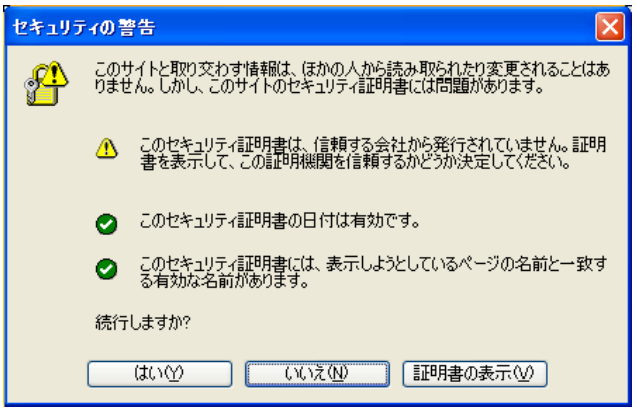


図 9-3 信頼されたルート証明機関に登録前のセキュリティ警告

(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]:apresia
Organizational Unit Name (eg, section) []:SE
Common Name (eg, your name or your server's hostname) []:192.0.2.3     <-- 重要ポイント
Email Address []:xxx@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】
#
```

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://192.0.2.3/」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、以下のようなセキュリティ警告が表示されます。

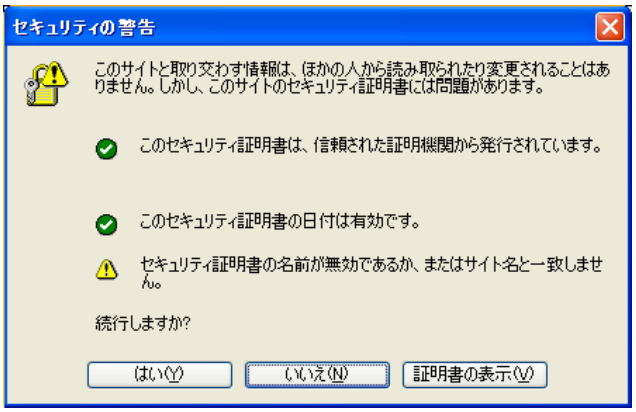


図 9-4 認証 URL 不一致によるセキュリティ警告

9.3.2 証明書の発行

証明書要求を認証局に送付し、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) 生成した証明書要求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)としています。

```
# 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=apresia/OU=SE/CN=192.0.2.3/emailAddress=xxx@apresia
.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 証明書と秘密鍵のダウンロード

TFTP サーバー上に証明書と秘密鍵をおき、copy file https-file コマンドにより、本装置に証明書と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)。

<証明書>

```
-----BEGIN CERTIFICATE-----
MIICQDCCAakCAQIwDQYJKoZIhvcNAQEEBQAwgY0xCzAJBgNVBAYTAkpQMQ4wDAYD
VQQIEwVUb2t5bzETMBEGA1UEBxMKQ2hpeW9kYS1rdTEMMAoGA1UEChMDSENMMQww

・・・・・ 中略 ・・・・・

WvAD2CC763Z9GRQbDYlITb8Mz86YoJO61LpNhc89O6fE1pIQf+LJxrdTUfAUe0mo
kugHFw==
-----END CERTIFICATE-----
```

<秘密鍵>

```
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBANrio6vXJPQax8WVyg+tmI27F7IdnOukmznI1W4nChjSlp/yw3hD
i+iZDjtYHHWnbVffMUO/OK8dAM9zwesROOUCAwEAAQJAAbJYCnDOfF/oxINQuaZi

・・・・・ 中略 ・・・・・

Jt+Hd7lLcgrDuwIhAJZOgMKvAWtxYiijwJStP1GR17nSqzjGud/uzhWbmBDnAiEA
s0utik/2ZIZl1A1Wua+1XR0c3l1+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
```

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の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ください。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、復号に失敗します。このため有効な秘密鍵となりません。

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。

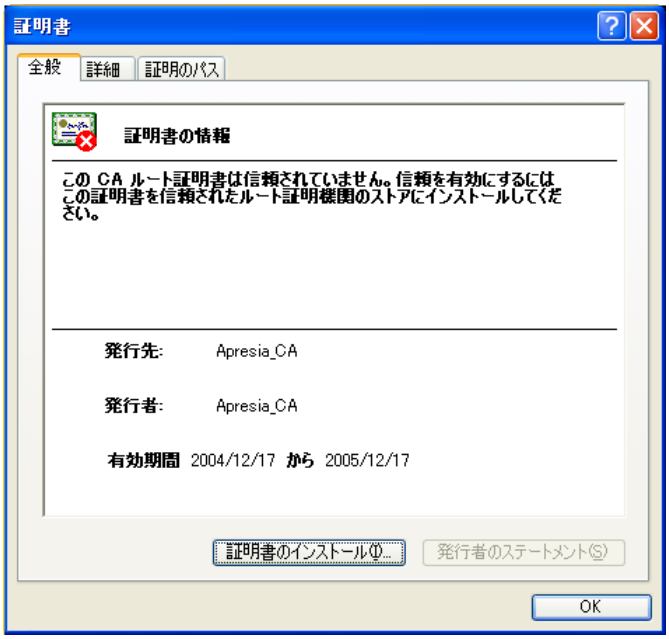


図 9-5 プライベート CA の登録

(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。

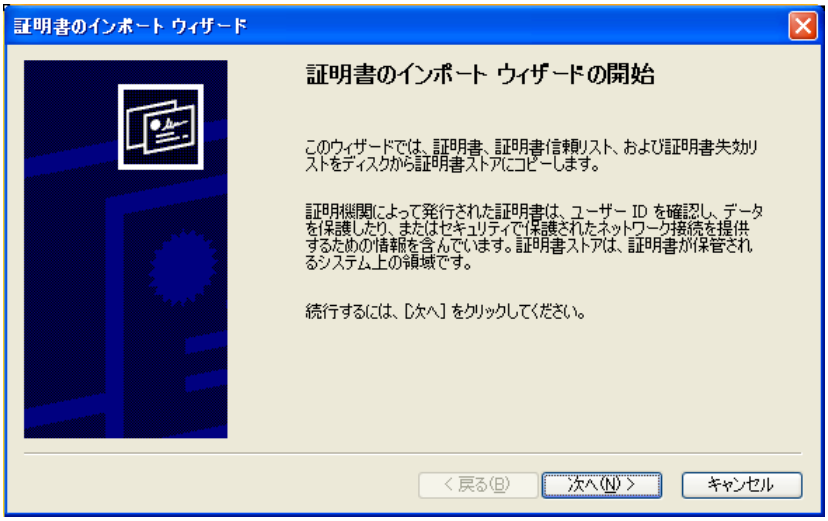


図 9-6 証明書インポートウィザード起動

(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。

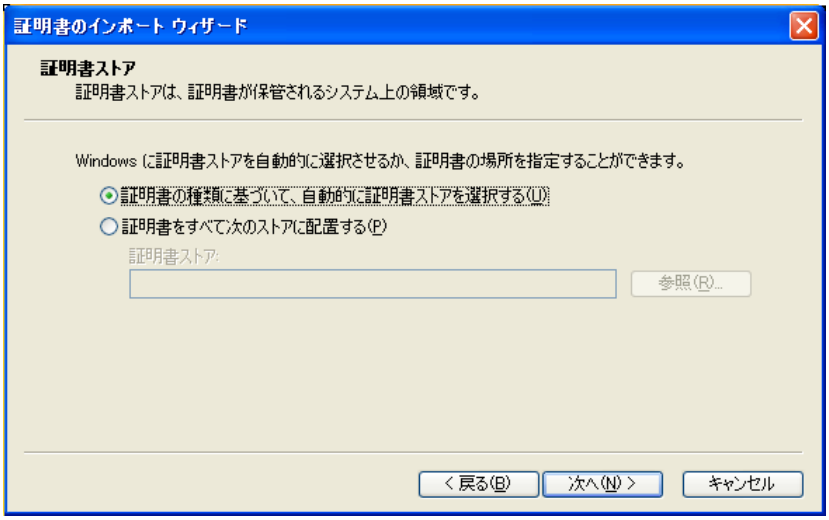


図 9-7 証明書ストア指定

(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。

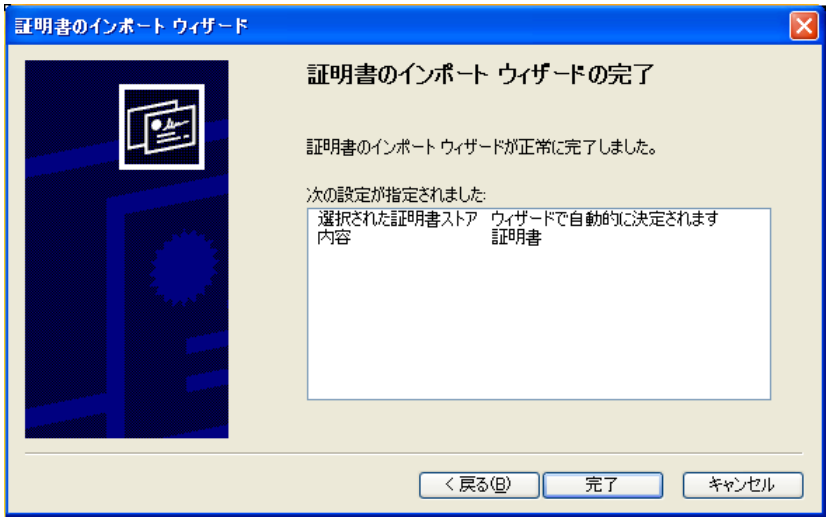


図 9-8 証明書インポートウィザード完了

(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。

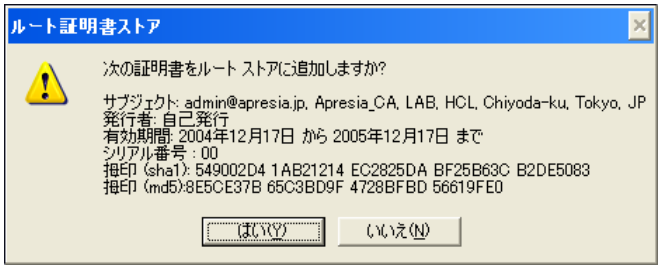


図 9-9 ルート証明書ストアへの追加

(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。

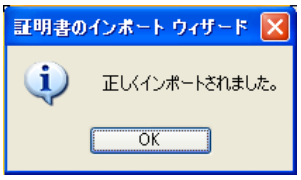


図 9-10 ルートストアへの追加完了

(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。

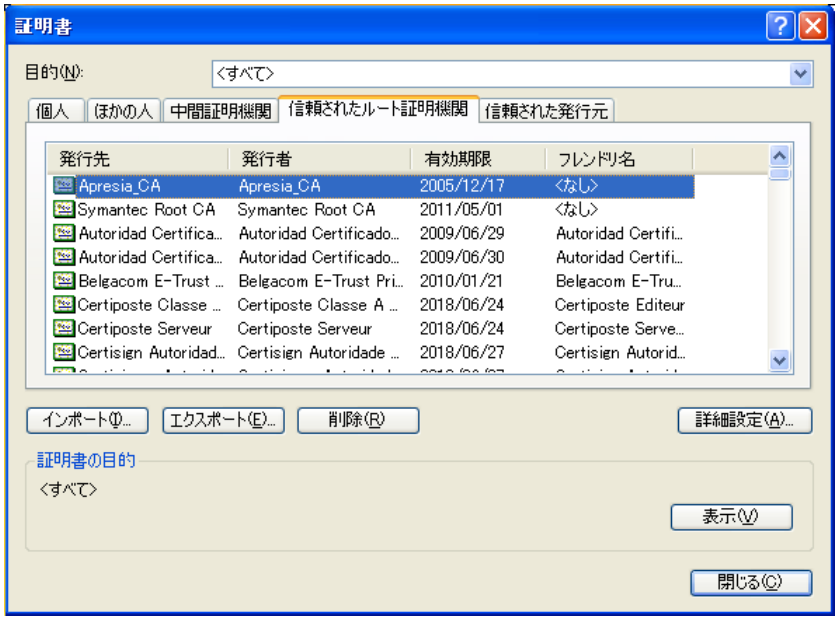


図 9-11 追加されたプライベート CA

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。

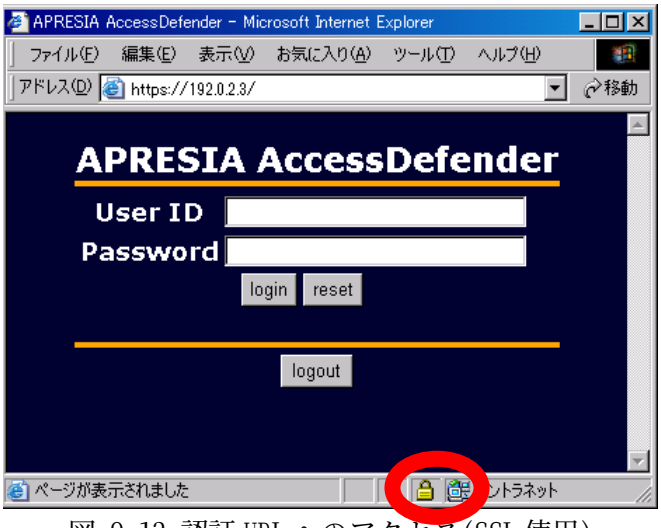


図 9-12 認証 URL へのアクセス(SSL 使用)

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ください。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

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。

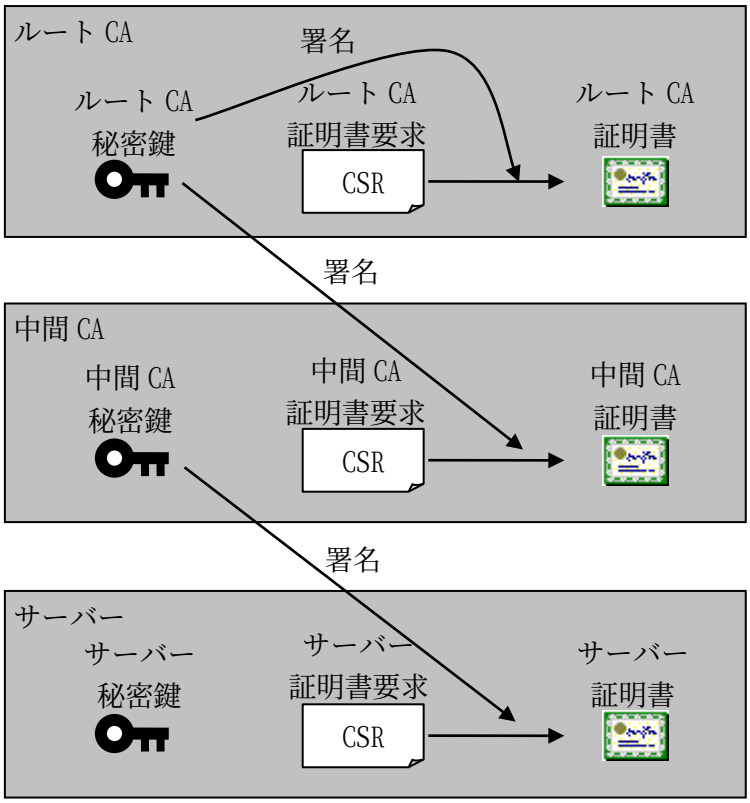


図 9-13 SSL 証明書の階層構造

クライアントは、証明書の有効性を確認する際に、全階層の証明書を検証します。通常ブラウザーにはルート 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。

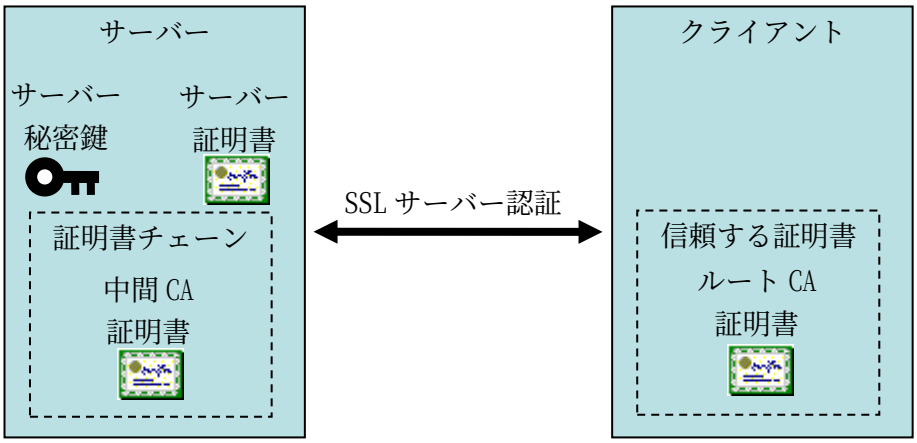


図 9-14 SSL サーバー認証(中間 CA 証明書使用)

9.6.1 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)を参考に証明書要求を発行し、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-----
MIIDlzCCAwCgAwIBAgIJAKlq1Sk5D/FCMA0GCSqGSIb3DQEBBQUAMIGXMQswCQYD
VQQGEwJKUDEOMAwGA1UECBMFVG9reW8xEzARBgNVBAcTCkNoaXlvZGEta3UxFjAU

・・・・・ 中略 ・・・・・

uGyyaIKP8/57MeIWb4vkDZF+D9XuOYbiqRJIWuIwjR2UFM4P69zBkfEoHeblWboz
RLLvbJdfTKcCreI=-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIJAKlq1Sk5D/FBMA0GCSqGSIb3DQEBBQUAMHwxCzAJBgNV
BAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzEWMBQGA1UEChMNSGl0YWNoaS1DYWJsZTEL

・・・・・ 中略 ・・・・・

5nA52bQIcEcDketgTWcNg5Tidf0JE1xDJiDnB7v3IGVY59J3rycVusdyN4+cPgfY
CN8nTz0q
-----END CERTIFICATE-----
```

サーバー証明書

中間 CA 証明書

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 8443
% Invalid SSL files.
```

9.6.2 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ください。

このセクションの内容はサポート対象外となります。

OpenSSL などのソフトウェアを使用し、秘密鍵と証明書要求を生成します。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。

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)
↓
ルート CA 証明書の作成
↓
中間 CA 証明書の作成
↓
サーバー証明書の作成
↓
チェーン証明書の作成
↓
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)
↓
認証端末の環境作成(ルート CA 証明書のインストール)

(1) /usr/local/ssl/openssl.cnf の環境設定

• [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)・・・
```

• [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
```

(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]:apresia
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          = apresia
            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=apresia/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ください。

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
```

(3) 中間 CA 証明書の作成

- 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]:apresia
```

```
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(中間 CA 用証明書要求)

秘密鍵のパスフレーズを絶対に忘れないようにしてください。

- 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
```

- 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 -infiles
icareq.pem
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:f1:41
        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          = apresia
            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)

(4) サーバー証明書の作成

- APRESIA 認証用 Web サーバー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:    【サーバー用秘密鍵のパスフレーズの入力】
Verifying - Enter PEM pass phrase:    【サーバー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]:apresia
Organizational Unit Name (eg, section) []:NE
Common Name (eg, YOUR name) []:192.0.2.3                    <-- 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(サーバー用秘密鍵)
- newreq.pem(サーバー用証明書要求)

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://192.0.2.3/」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ください。

- 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
```

- 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          = apresia
            organizationalUnitName    = NE
            commonName                = 192.0.2.3
            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=apresia/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)

(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>

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.
```

(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。

- 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
```

- 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ください。

(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してください。

9.6.3 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。

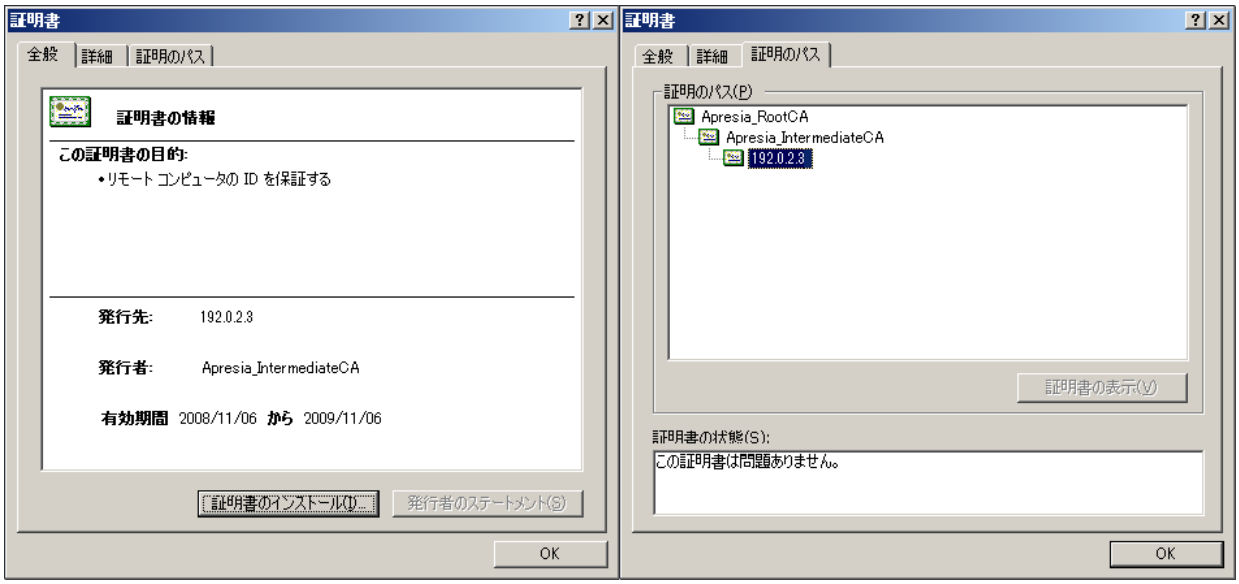


図 9-16 証明書情報表示例

10 各バージョンでの機能追加、変更点

AccessDefender に関する各バージョンでの機能追加、変更点を表 10-1 にまとめます。最新の情報に関しては、リリースノートやフィールドノーティスを参照してください。

表 10-1 各バージョンでの機能追加、変更点

Version	管理番号	内容
8.06.01	AEOS-80601-RC001	AccessDefender 機能において下記をサポートしました。 • MAC 認証 • Web 認証 • dot1X 認証 • Gateway 認証 下記機能が将来サポートになります。 • DHCP-Snooping 機能 • 認証方式の選択 • VLAN 変更制限機能 • Web/MAC("web-authentication mac-authentication-password")機能 • リンクアグリゲーションポート("interface lag")での認証 • L3 機能との併用
8.06.02	AEOS-80602-RC002	AccessDefender 機能において、dot1X 認証動作中に設定("dot1x port 1/1-2 re-authenticate")を繰り返し行うと装置が再起動する可能性を修正しました。
8.07.01	AEOS-80701-RC004	AccessDefender 機能において、以下の機能をサポートしました。 • DHCP Snooping 機能 • L3 機能との併用 • リンクアグリゲーション機能との併用 • Web/MAC 認証 • 認証方法選択("aaa authentication web <ID>")
8.07.01	AEOS-80701-RC028	AccessDefender 機能において、"mac-authentication password <PASSWORD>"を 57 文字以上設定した場合、装置再起動後に設定が反映されない問題を修正しました。
8.08.01	AEOS-80801-RC003	AccessDefender 機能の WEB 認証・Gateway 認証において、TTL フィルター機能をサポートしました。 • "web-authentication ttl <TTL> port <PORTRANGE>" • "web-authentication ttl <TTL> lag <LAGRANGE>"
8.08.01	AEOS-80801-RC004	AccessDefender 機能の WEB 認証・Gateway 認証において、PING ログアウト機能をサポートしました。 • "logout ping dst-ip <IPADDR>" • "logout ping ttl <TTL>"
8.08.01	AEOS-80801-RC005	AccessDefender 機能において、ローカルデータベースを装置内で追加･削除できる機能をサポートしました。 • "aaa-local-db add user <USERID> [password <PASSWORD>] [vlan <VID>]" • "aaa-local-db del user <USERID>"
8.08.01	AEOS-80801-RC006	AccessDefender 機能において、802.1X 認証に先立ち端末の MAC アドレス

Version	管理番号	内容
		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。
8.08.01	AEOS-80801-RC031	AccessDefender 機能において、DHCP-snooping の log 出力内容"Mode changed to DENY automatically"を"mode changed to DENY automatically"と大文字から小文字に仕様を変更しました。
8.08.01	AEOS-80801-RC063	AccessDefender 機能において、"no web-authentication http-port"コマンドを行っても内部で利用していたパケットフィルター2 のルールが削除されないためコマンドで設定した http-port でアクセスできる問題を修正しました。
8.08.01	AEOS-80801-RC064	AccessDefender 機能において、access-defender-deny 設定時でも、IP オプション付きパケットを中継してしまう問題を修正しました。
8.08.01	AEOS-80801-RC065	SSL 機能において、"ssl gencsr rsakey"実行時に Ctrl+C --> Ctrl+T を実行すると不正なメッセージが表示される問題を修正しました。
8.08.02	AEOS-80802-RC010	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仕様を変更しました。
8.08.02	AEOS-80802-RC030	DHCP Snooping 機能において、本機能が有効な状態"dhcp-snooping enable"で DHCP Snooping の設定を行なっていないポートでユニキャスト DHCP パケットを L3 中継しない問題を修正しました。
8.08.02	AEOS-80802-RC034	AccessDefender 機能において、%s を含んだ UserID で Web 認証ができない問題を修正しました。
8.10.01	AEOS-81001-RC001	Apresia13000-X24-PSR において、AccessDefender 機能(802.1X 以外)をサポートしました。
8.10.01	AEOS-81001-RC002	AccessDefender 機能において、認証機能(ゲートウェイ認証以外)でユーザー毎にパケットフィルター2 機能を適用拡張できる機能をサポートしました。
8.10.01	AEOS-81001-RC023	DHCP Snooping 機能において、DHCP サーバーと DHCP クライアントが別 VLAN で同一装置内に存在する場合、別装置で DHCP リレーされた DHCP ACK パケットを破棄してしまう問題を修正しました。
8.10.02	AEOS-81002-RC002	AccessDefender 機能において、同時認証性能を向上させるために WEB 認証の改善をしました。
8.10.02	AEOS-81002-RC010	AccessDefender 機能において、MAC 認証と access-defender-logout を繰り返し実行し、"% Handle init error"のエラーメッセージ出力後に"no mac-authentication enable"コマンドを実行すると装置が再起動する問題を修正しました。
8.11.01	AEOS-81101-RC010	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。 • "logout linkdown time port <PORTS> enable" • "logout linkdown time <TIME>"
8.11.01	AEOS-81101-RC011	AccessDefender 機能において、WEB/MAC 認証の認証順番が WEB 認証、MAC 認証の順番で認証が行われ、MAC 認証成功時の属性情報をもとに VLAN/クラスを変更する機能をサポートしました。 • "web-authentication mac-authentication-attribute mac"

Version	管理番号	内容
8.11.01	AEOS-81101-RC014	AccessDefender 機能において、同時認証性能を向上させるために Web 認証の改善をしました。
8.11.01	AEOS-81101-RC034	AccessDefender 機能において、装置再起動時にデフォルトの SSL の証明書と秘密鍵が組み込まれないため、リダイレクト機能が有効にならない問題を修正しました。
8.11.01	AEOS-81101-RC036	DHCP Snooping 機能において、"internal-dhcp-vlan"設定時に VLAN に IP アドレスが設定されていない場合、"dhcp-snooping enable"後のプロンプト応答が遅い問題を修正しました。
8.12.01	AEOS-81201-RC031	Access-Defender 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。
8.13.08	AEOS-81308-RC015	802.1X 機能において、装置起動時に 802.1X 機能が無効となってしまう場合がある問題を修正しました。
8.14.01	AEOS-81401-RC009	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。
8.15.01	AEOS-81501-RC009	AccessDefender 機能において、スヌーピングプロキシ機能に対応しました。 • "web-authentication snooping proxy-port <PROXY-PORT>"
8.15.01	AEOS-81501-RC010	AccessDefender 機能において、認証端末をスタティックで登録できるコマンドをサポートしました。 • "access-defender static mac <MACADDR> vlan <VID> class <CLASSID> port <PORTNO>" • "access-defender static mac <MACADDR> vlan <VID> class <CLASSID> lag <LAGNO>"
8.15.01	AEOS-81501-RC053	AccessDefender 機能において、vlan が多数設定ある状態で装置を再起動すると、802.1x 認証の設定があるにも関わらず動作しない問題を修正しました。
8.15.01	AEOS-81501-RC054	AccessDefender 機能において、vlan が多数設定ある状態で装置を再起動すると、下記コマンドが装置に反映されない問題を修正しました。 • "dhcp-snooping enable"
8.17.01	AEOS-81701-RC003	Apresia15000 シリーズにおいて、AccessDefender 機能の MAC 認証に対応しました。
8.17.01	AEOS-81701-RC030	AccessDefender 機能において、下記コマンドの OPTION 範囲をポート番号、リンクアグリゲーション番号まで指定できるように仕様を変更しました。 • "access-defender static mac <MACADDR> (port <PORTNO> | (lag <LAGNO>)"
8.17.01	AEOS-81701-RC081	AccessDefender 機能において、DHCP-snooping 機能を有効にすると IP フラグメントされた UDP パケット※が中継されない問題を修正しました。 ※IP フラグメントされた UDP パケットの 2 個目以降(IP offset ≠ 0)のパケットで UDP データ部分の先頭から 3、4 オクテット目の値が 10 進数で 67 か 68(16 進数で 0x0043 か 0x0044)であるパケット
8.17.01	AEOS-81701-RC082	AccessDefender 機能において、dot1x の認証ポートに static 端末を設定

Version	管理番号	内容
		し、"access-defender-logout mac"コマンドでログアウトさせようとした場合、エラーメッセージが表示されない問題を修正しました。
8.17.01	AEOS-81701-RC083	AccessDefender 機能において、"dot1x enable"設定後に"ignore-eapol-start"を設定し、"no access-defender"を実行しても設定が削除できない問題を修正しました。
8.17.01	AEOS-81701-RC084	AccessDefender 機能において、"dhcp-snooping mode deny"、"no dhcp-snooping mode deny"コマンドを連続設定時に mode changed の以下のログが出力されない問題を修正しました。 • "<process:info> A-Def : dhcpsnooping : mode changed to DENY manually" • "<process:info> A-Def : dhcpsnooping : mode changed to PERMIT manually"
8.17.04	AEOS-81704-RC009	AccessDefender 機能において、"ignore-eapol-start"設定後に"no dot1x port|lag"で設定を削除すると"no packet-filter2 max-rule"あるいは"no access-defender"コマンドを実行しても"Configuration error"が表示され、設定が削除されない問題を修正しました。
8.17.04	AEOS-81704-RC010	AccessDefender において、802.1x の設定変更を行う場合、AccessDefender の設定変更ができず、"show running-config"に AccessDefender の設定が表示されないことがある問題を修正しました。(AEOS8.17.01 のみ)
8.18.02	AEOS-81802-RC006	Apresia15000 シリーズにおいて、DHCP Snooping 機能を除く AccessDefender 機能をサポートしました。
8.18.02	AEOS-81802-RC019	AccessDefender 機能において、DHCP Snooping 機能を除き MLAG 機能との併用をサポートしました。詳細についてはコマンドリファレンスを参照してください。
8.18.02	AEOS-81802-RC035	AccessDefender 機能において、WEB 認証と 802.1X 認証の AND 認証をサポートしました。両認証に成功した端末のみの通信が許可されます。 • "web-authentication port <PORT> dot1x"
8.18.02	AEOS-81802-RC036	AccessDefender 機能において、認証端末の WEB へのアクセスログを出力する下記コマンドをサポートしました。 • "logging access-defender web-access on" ※本コマンドはトラブルシューティング用のコマンドとなります。通常運用時の使用は避けてください。
8.18.02	AEOS-81802-RC037	AccessDefender 機能において、MLAG インターフェースを表示させる下記コマンドをサポートしました。 • "show access-defender dot1x mlag" • "show access-defender dot1x statistics mlag"
8.18.02	AEOS-81802-RC062	AccessDefender 機能において、端末の認証処理を開始する際、同一の MAC アドレスの端末がすでに認証済端末として登録されている場合、端末キー重複による登録失敗のログを出力しないように仕様を変更しました。
8.18.02	AEOS-81802-RC136	AccessDefender 機能において、Apple 社の Macintosh 上のブラウザーからユーザー名、パスワードに円記号"¥"を入れると、"%"と誤認識されてしまい、正しくログインできない問題を修正しました。
8.18.02	AEOS-81802-RC137	AccessDefender 機能において、"packet-filter2 group <GROUP>"コマンドで他機能が使用している packet-filter2 グループを指定した場合、

Version	管理番号	内容
		AccessDefender 機能の設定ができない問題を修正しました。
8.18.02	AEOS-81802-RC138	AccessDefender 機能において、AccessDefender 用の packet-filter2 のリソースがない状態で、"dot1x enable"コマンドを実行した場合のエラーメッセージにピリオドがない問題を修正しました。
8.18.02	AEOS-81802-RC139	AccessDefender 機能において、trunk ポートで認証時に、ポートにアサインされている VLAN と同じ VID に、端末の VLAN が動的に変更された時に trunk VLAN の設定が消える問題を修正しました。
8.18.02	AEOS-81802-RC140	AccessDefender 機能において、1000 件以上のユーザーがローカルデータベースに登録されている場合、"show access-defender aaa-local-db"の表示がずれる問題を修正しました。
8.18.02	AEOS-81802-RC141	AccessDefender 機能において、全ての認証タイプ(WEB 認証、IEEE802.1X 認証、MAC 認証)と DHCP Snooping 機能併用時に、"show access-defender client"で"Cls"列の値が表示されない問題を修正しました。
8.18.02	AEOS-81802-RC142	AccessDefender 機能において、認証ポートに LAG インターフェースとポートの両方を設定した際に、IEEE802.1X 認証が成功せず通信できない問題を修正しました。
8.18.02	AEOS-81802-RC143	AccessDefender 機能において、"packet-filter2 max-rule"と"dot1x ignore-eapol-start"を設定し、"no dot1x port | lag"で設定を削除すると、"packet-filter2 max-rule/group"設定が消せなくなる問題を修正しました。
8.18.02	AEOS-81802-RC144	AccessDefender 機能において、"packet-filter2 max-rule"の設定がない状態で、"no dot1x enable"を実行するとエラーメッセージが出る問題を修正しました。
8.18.02	AEOS-81802-RC145	AccessDefender 機能において、IEEE802.1X 認証の設定変更を行う場合、AccessDefender の設定変更ができず、"show running-config"に AccessDefender の設定が表示されないことがある問題を修正しました。
8.18.02	AEOS-81802-RC146	AccessDefender 機能において、EAP フレームが FDB に登録されない問題を修正しました。
8.18.03	AEOS-81803-RC007	AEOS-81001-ER023【AccessDefender 機能において、Class の値が 4 桁になると"show access-defender client"の改行表示がずれる問題があります。】に関して、AEOS8.18.02 において改修済みであったことが確認されたため、記載を削除いたします。
8.19.01	AEOS-81901-RC021	MMRP-Plus 機能の分散マススイッチのマスターポート、及び分散スレーブスイッチのスレーブポートにおけるポートリスタート機能併用時において、当該ポートでの AccessDefender 機能の併用をサポートしました。ただし、IEEE802.1X 認証、ゲートウェイ認証、動的 VLAN、スタティック認証、ユーザーポリシーコントロールは未サポートです。
8.19.01	AEOS-81901-RC030	AccessDefender 機能において、デフォルトの Web 認証画面がスマートフォンの画面に対応して最適表示されるようにしました。変更後の画面を適用するためには、ファームウェア更新後に下記コマンドを実行して各 Web 認証画面を初期化してください。 • "erase login-page" • "erase success-page" • "erase failure-page"

Version	管理番号	内容
		• "erase logout-success-page" • "erase logout-failure-page" • "erase redirect-error-page" ※"factory-default"コマンドにより一括して初期化することも可能です。この場合、構成情報やログなどもあわせて初期化されることに注意してください。
8.19.01	AEOS-81901-RC035	AccessDefender 機能において、Virtual BoxCore 機能との併用時、"packet-filter2 max-rule" コマンドのコマンドモードを、VB-ALL-ACCESSDEFENDER(共通)から VB-ID/IDRange-ACCESSDEFENDER に変更しました。
8.19.01	AEOS-81901-RC036	AccessDefender 機能において、Virtual BoxCore 機能との併用時、以下コマンドのコマンドモードを、VB-ALL-CONFIG から VB-ID/IDRange-CONFIG に変更しました。 • "[no] dot1x enable" • "[no] dhcp-snooping enable" • "[no] mac-authentication enable" • "[no] web-authentication enable"
8.19.01	AEOS-81901-RC115	AccessDefender 機能において、TELNET/SSH で接続して"ssl gencsr rsakey"コマンドを実行している際、CSR 生成のための識別名(Distinguished Name)入力待ちの状態でセッションが切断されると CPU 使用率が 100%のままになる問題を修正しました。
8.19.01	AEOS-81901-RC116	AccessDefender 機能において、Virtual BoxCore 機能との併用時、VB モードから"show access-defender client"コマンドを実行した際に不要な注釈が表示される問題を修正しました。
8.19.01	AEOS-81901-RC117	AccessDefender 機能において、IEEE802.1X 認証機能を使用している場合、ある端末の認証が中断され該当端末の認証が新規に行われた場合、Apresia から送信する RADIUS パケットが不正となり、認証できない場合がある問題を修正しました。 ※AEOS8.18.03 以前のバージョンで本問題が発生した場合、下記の方法で復旧が可能です。回避策はありません。 • 問題の発生した端末が接続されているポートのリンクダウン • 下記いずれかのコマンドの実行 (1)"dot1x initialize" (2)"no dot1x enable", "dot1x enable" (3)"no dot1x port", "dot1x port"
8.19.01	AEOS-81901-RC118	AccessDefender 機能において、Web/IEEE802.1X 認証(AND)の設定("web-authentication port dot1", "web-authentication lag dot1x", "web-authentication mlag dot1x"のいずれか)がある場合、以下コマンドを実行した際にメモリーリークする問題を修正しました。 • "show running-config" • "copy running-config flash-config" • "write memory" • "show tech-support"
8.19.01	AEOS-81901-RC119	AccessDefender 機能において、"show access-defender

Version	管理番号	内容
		lag-configuration"コマンドを実行した際にメモリーリークする問題を修正しました。
8.19.01 8.19.03	AEOS-81901-RC155 AEOS-81903-RC004	AEOS-81001-ER023【AccessDefender 機能において、Class の値が 4 桁になると"show access-defender client"の改行表示がずれる問題があります。】に関して、AEOS8.18.02 において改修済みであったことが確認されたため、記載を削除いたします。
8.20.01	AEOS-82001-RC020	AccessDefender 機能において、VLAN 変更制限機能をサポートしました。 サポート内容の詳細はコマンドリファレンスを参照ください。 • "vlan mode dynamic port-base" • "vlan mode static"
8.20.01	AEOS-82001-RC021	AccessDefender 機能において、以下の syslog をサポートしました。 • "A-Def : port <port number> has already been assigned to another vlan : uid=<user id> port=<port number> [new vid=<vid>]" • "A-Def : {web|mac|dot1x} : port <port number> has already been assigned to another vlan : uid=<user id> mac=<mac address> ip=<ip address> port=<port number> vid=<vid> [new vid=<vid>]"
8.20.01	AEOS-82001-RC022	Apresia15000 シリーズの AccessDefender 機能において、DHCP Snooping 機能をサポートしました。サポート内容の詳細はコマンドリファレンスを参照ください。 • "dhcp-snooping enable" • "dhcp-snooping port" • "dhcp-snooping mode deny" • "dhcp-snooping mode mac-authentication" • "dhcp-snooping mode timer" • "dhcp-snooping static-entry" • "dhcp-snooping internal-dhcp-vlan"
8.20.01	AEOS-82001-RC031	AccessDefender 機能の IEEE802.1X 認証機能において、最大同時認証端末数を超えたために認証に失敗した端末に対する動作仕様を以下のように変更しました。 • 変更前："dot1x timeout quiet-period"コマンドで設定した認証失敗時のステータス保持時間の間は再認証要求を受け付けない • 変更後：再認証要求を受け付ける
8.20.01	AEOS-82001-RC102	AccessDefender 機能の IEEE802.1X 認証機能において、ローミング機能が無効の状態で認証済端末をログアウトせず他の認証ポートに移動し再認証した場合、再認証ログ、及び"show access-defender client"の表示の端末のポートは移動後のポートに更新されますが、正常に認証できず通信できなくなる問題を修正しました。
8.20.01	AEOS-82001-RC131	AEOS-81101-ER019 の記載【AccessDefender 機能において、同時認証時の syslog が一部出力されない問題があります。】に関して、8.17.01 以降での修正が確認できましたので、今回のリリースノートより記載削除いたします。
8.21.01	AEOS-82101-RC025	Access-Defender 機能と MMRP-Plus 機能との併用時、MMRP-Plus の分散マスターポート、分散スレーブポートでの MAC 認証における動的 VLAN 割り当てをサポートしました。

Version	管理番号	内容
8.21.01	AEOS-82101-RC068	SSL 機能の以下コマンドについて、VB-ALL モード、VB-ID/IDRange モードでも実行できるように仕様を変更しました。 • "copy csr tftp"
8.22.01	AEOS-82201-RC017	保守/運用コマンド機能において、機能毎の詳細情報を取得できる以下のコマンドをサポートしました。障害発生などの際には本コマンドと"show tech-support"コマンドの取得結果をサポート窓口に送付ください。 • "show tech-support mmrp-plus" • "show tech-support access-defender" • "show tech-support bfs" • "show tech-support link-aggregation" • "show tech-support spanning-tree" • "show tech-support packet-filter2" • "show tech-support icmp redirect" • "show tech-support vrrp"
8.22.01	AEOS-82201-RC096	AccessDefender 機能の DHCP Snooping 機能において、出力されるログの末尾に不要なピリオドがあった問題を修正しました。 • "A-Def : dhcpsnooping : mode changed to deny manually" • "A-Def : dhcpsnooping : mode changed to permit manually" • "A-Def : dhcpsnooping : mode-timer started" • "A-Def : dhcpsnooping : mode changed to deny automatically"
8.22.01	AEOS-82201-RC097	Apresia13000-X24-PSR 、 及 び Apresia13200-28GT シ リ ー ズ の AccessDefender 機能において、"show access-defender dhcp-snooping configuration"を実施した場合、"LAG Lease-limit"フィールドの LAG ID 29～32 の箇所が表示されない問題を修正しました。
8.22.01	AEOS-82201-RC098	AccessDefender 機能の IEEE802.1X 認証機能において、RADIUS サーバーからの Access-Accept メッセージに State 属性が含まれる場合、本来なら認証に成功するはずの端末が認証済端末として Apresia に登録されず当該端末からの通信ができない問題を修正しました。
8.23.01	AEOS-82301-RC013	AccessDefender 機能において、認証ページ、認証成功ページの submit フォームの仕様を以下のように変更しました。 • 変更前："<input type="submit" value="logout">" • 変更後："<input type="submit" name="action" value="logout">" この変更により、Internet Explorer 11 をお使いの場合においても、認証ページ、認証成功ページからログアウトボタンによるログアウトが可能になります。
8.23.01	AEOS-82301-RC042	AccessDefender 機能の IEEE802.1X 認証において、下記いずれかの場合にログが正しく出力されない問題を修正しました。 • IEEE802.1X 認証が有効な MLAG インターフェースのドメインに"%"が含まれる • ユーザー名に"%"が含まれる
8.23.01	AEOS-82301-RC043	AccessDefender 機能の IEEE802.1X 認証において、下記いずれかの場合に不正な再起動を起こす可能性がある問題を修正しました。 • IEEE802.1X 認証が有効な MLAG インターフェースのドメインに"%"が含

Version	管理番号	内容
		まれる • ユーザー名に"%"が含まれる
8.23.01	AEOS-82301-RC044	AccessDefender 機能において、複数の端末が同時に Web 認証を実施し、そのうちのある端末が認証に失敗した場合、それ以降まれに以下いずれかの状態になることがある問題を修正しました。 • 一部の Web 認証が行えなくなる • すべての Web 認証、MAC 認証が行えなくなる
8.24.01	AEOS-82401-RC016	SSL 機能において、SHA-2 ハッシュアルゴリズムを使用したサーバー証明書を使用できるように仕様を変更しました。
8.24.01	AEOS-82401-RC017	SSL 機能において、"ssl gencsr"コマンドによる CSR 作成時に、CN(Common Name)以外の識別名を省略可能なように仕様を変更しました。 これに伴い、以下の識別名についてのデフォルト値を削除しました。 ※ これらの識別名については、未入力で[Enter]を入力すると値は省略されたものとみなされますのでご注意ください。 • Country Name • State or Province Name • Locality Name • Organization Name • Organizational Unit Name
8.24.01	AEOS-82401-RC018	AccessDefender 機能の Web 認証機能において、HTTPS 通信に TLS1.1、TLS1.2 を使用できるように仕様を変更しました。
8.24.01	AEOS-82401-RC019	AccessDefender 機能の Web 認証機能において、同時認証性能数の改善を行いました。
8.24.01	AEOS-82401-RC020	AccessDefender 機能の IEEE802.1X 認証機能において、同時認証性能数の改善を行いました。
8.24.01	AEOS-82401-RC021	AccessDefender 機能の DHCP Snooping 機能において、DHCP Snooping 機能有効時に DHCP Snooping 無効ポートで受信した以下のいずれかに該当するパケットの中継動作を、破棄からハードウェア中継に変更しました。 • 宛先 UDP ポート番号が 67 の DHCP パケットで、"access-defender-deny"コマンドで設定された認証拒否端末からのもの • 宛先 UDP ポート番号が 67 の DHCP パケットで、"dhcp-snooping internal-dhcp-vlan"コマンドで指定した VLAN からのもの • 宛先 UDP ポート番号が 67 で、DHCP パケットフォーマットと異なるもの ※ UDP ポート番号 67 は一般的に DHCP サーバーの使用ポートです。 また、以下に該当するパケットの中継動作を、ソフトウェア中継からハードウェア中継に変更しました。 • 宛先 UDP ポート番号が 67 の DHCP パケット(前項のいずれにも該当しないもの)
8.24.01	AEOS-82401-RC022	AccessDefender 機能の DHCP Snooping 機能において、DHCP Snooping 機能有効時に下記条件のいずれかに該当する DHCP 無効ポート宛パケットの中継動作を、破棄からソフトウェア中継に変更しました。 • 宛先 UDP ポート番号が 68 で、DHCP パケットフォーマットと異なるもの • 宛先 UDP ポート番号が 68 で、宛先ポート番号が 67 でない DHCP REQUEST

Version	管理番号	内容
		に対する DHCP ACK • 宛先UDPポート番号が68で、クライアントのIP情報がないDHCP REQUESTに対する DHCP ACK ※ UDP ポート番号 68 は一般的に DHCP クライアントの使用ポートです。 これにより、DHCP Snooping 機能を有効にした装置の DHCP Snooping 無効ポート配下に PXE ブートクライアントを接続することが可能になります。
8.24.01	AEOS-82401-RC023	AccessDefender 機能において、"show tech-support access-defender"コマンドの"dump information"で取得できる情報を追加しました。
8.24.01	AEOS-82401-RC024	AccessDefender 機能において、"aaa-local-db del user"コマンドで存在しないユーザーを指定して実行した際にエラーメッセージが表示されなかったものを、以下のエラーメッセージを表示するように仕様を変更しました。 • "% The user does not exist."
8.24.01	AEOS-82401-RC082	AccessDefender 機能において、認証機能が有効な LAG インターフェース、MLAG インターフェースにポートを追加した場合、追加したポートで動的 VLAN、クラス ID が機能しない問題を修正しました。
8.24.01	AEOS-82401-RC083	AccessDefender 機能において、"aaa authentication {web | mac} local radius <INDEX>"コマンドの"<INDEX>"に"9-16"を設定できず、その結果 IPv6 の RADIUS サーバーを指定することができない問題を修正しました。
8.24.01	AEOS-82401-RC084	Apresia13200-28GT シリーズの AccessDefender 機能において、クラス ID(未サポート)として 0 以外を指定して使用すると、動的 VLAN を割り当てない場合でも不正に動的 VLAN 用のリソースを消費してしまう問題を修正しました。
8.24.01	AEOS-82401-RC085	AccessDefender 機能において、DHCP Snooping 機能が有効な状態で、設定した最大認証端末数を越えた際に DHCP Snooping 無効ポートで DHCP Request パケットを中継しない問題を修正しました。
8.24.01	AEOS-82401-RC086	AccessDefender 機能において、"dhcp-snooping mode timer <TIME>"コマンドで設定する DENY モードへの切り替わり時間が、設定値よりも最大 10 秒短くなる問題を修正しました。

8.24.01	AEOS-82401-RC087	AccessDefender 機能の IEEE802.1X 認証において、認証無効の状態で一部のインターフェースの IEEE802.1X 認証設定を削除すると、その他の IEEE802.1X 認証設定インターフェースで受信したフレームを破棄し続ける問題を修正しました。
		• インターフェースの IEEE802.1X 設定
		  • dot1x (port PORTRANGE) | (lag LAGRANGE) | (mlag MLAGRANGE)
		  • web-authentication (port PORTRANGE) | (lag LAGRANGE) | (mlag MLAGRANGE) dot1x

8.24.01	AEOS-82401-RC088	AccessDefender 機能の DHCP Snooping 機能において、設定変更に伴う"dhcp-snooping mode timer"の起動時に、下記ログが出力されない場合がある問題を修正しました。 • "A-Def : dhcpsnooping : mode-timer started"
8.24.01	AEOS-82401-RC089	AccessDefender 機能の DHCP Snooping 機能において、以下の手順で"dhcp-snooping static-entry"コマンドの設定、削除を実行した後に、"no

Version	管理番号	内容
		dhcp-snooping static-entry port | lag"コマンドを任意のインターフェースを指定して実行すると、手順(1)、及び(2)のログを再度出力してしまう問題を修正しました。 (1) "dhcp-snooping static-entry"コマンドを実行し、スタティック登録を行う (2) "no dhcp-snooping static-entry port | lag"コマンドをインターフェースまで指定して実行し(1)の設定を削除する
8.25.01	AEOS-82501-RC010	AccessDefender 機能の認証 Web サーバーが使用する SSL プロトコルについて、SSLv2 を有効化するコマンド、及び SSLv3 を有効化するコマンドをサポートしました。 • "web-authentication sslv2 enable" • "web-authentication sslv3 enable"
8.25.01	AEOS-82501-RC024	AccessDefender 機能の認証 Web サーバーが使用する SSL プロトコルについて、デフォルト状態では SSLv2、及び SSLv3 は無効となるように仕様を変更しました。 デフォルト状態で使用可能なプロトコルは、TLS1.0、TLS1.1、TLS1.2 になります。SSLv2/SSLv3 を有効化する場合は、以下のコマンドを実行してください。 • "web-authentication sslv2 enable" • "web-authentication sslv3 enable"
8.25.01	AEOS-82501-RC025	AccessDefender 機能において、同一ポートで IEEE802.1X 認証機能と MAC 認証機能を併用する場合、IEEE802.1X 認証で認証成功、かつ MAC 認証で認証失敗した端末が、MAC 認証側で discard 登録されないように仕様を変更しました。
8.25.01	AEOS-82501-RC062	AccessDefender 機能において、IEEE 802.1X と DHCP Snooping 併用ポートで認証済みの端末に対して、"access-defender-logout user"コマンドをユーザーID 指定で実行した場合に、指定したユーザーID の端末の DHCP Snooping がログアウトしない問題を修正しました。
8.25.01	AEOS-82501-RC063	AccessDefender 機能において、"dhcp-snooping mode deny"コマンドが設定済みで"dhcp-snooping enable"設定時(無効から有効)に、以下のログが出力されていなかった問題を修正しました。 • "A-Def : dhcpsnooping : mode changed to deny manually"
8.26.01	AEOS-82601-RC023	AccessDefender 機能において、認証処理の見直しを行いました。
8.26.01	AEOS-82601-RC024	AccessDefender 機能において、IEEE802.1X 機能有効時、かつ FDB 登録数が多い場合における CPU 負荷を低減させました。
8.26.01	AEOS-82601-RC056	AccessDefender 機能において、DHCP Snooping 登録端末数が装置の最大数に達している状態から新規に DHCP Snooping 端末を登録しようとする場合、以下に示す「装置の最大認証数によるログイン不可」のログが出力されない問題を修正しました。 • "A-Def : dhcpsnooping : the number of terminals on switch is full :"
8.26.01	AEOS-82601-RC057	AccessDefender 機能において、DHCP Snooping 登録端末数が"max-client"コマンドで設定されるインターフェース毎の認証可能設定数に達している状態から当該インターフェースに新規に DHCP snooping 端末を登録しようとする場合、以下に示す「インターフェースの最大認証数によるログイ

<table>
<tr><th>Version</th><th>管理番号</th><th>内容</th></tr>
<tr><td></td><td></td><td>ン不可」のログが出力されない問題を修正しました。
• "A-Def : dhcpsnooping : the number of terminals on port <PORTNO> is full :"
• "A-Def : dhcpsnooping : the number of terminals on port <LAGNO> is full :"
• "A-Def : dhcpsnooping : the number of terminals on port MLAG <DOMAIN>/<MLAG ID> is full :"</td></tr>
<tr><td>8.26.01</td><td>AEOS-82601-RC058</td><td>AccessDefender 機能のスタティック認証において、以下の要因により認証に失敗した際に出力される Syslog に不要な"new vid"が含まれる問題を修正しました。
• 装置の最大認証数超え
• インターフェースの最大認証数超え
• VLAN 変更失敗</td></tr>
<tr><td>8.26.01</td><td>AEOS-82601-RC059</td><td>AccessDefender 機能において、FDB の登録数が多いときに認証ポートで登録された MAC アドレス宛の EAP フレーム送信が遅延する問題を修正しました。</td></tr>
<tr><td>8.26.01</td><td>AEOS-82601-RC060</td><td>AccessDefender 機能において、以下の条件を満たした場合に装置が不正に再起動を起こすことがある問題を修正しました。

【発生条件】
条件の組合せと問題の発生確率はバージョンによって異なります。【事象】欄を参照ください。
(1) IEEE802.1X 機能有効時に、多数のサプリカントから EAP フレームを高レートで受信
(2) (1)の状態において、表 1 に記載するコマンドのいずれかを実行
(3) (1)の状態において、IEEE802.1X 認証ポート間で認証端末がローミング

表 1 条件(2)対象コマンド一覧
<table><tr><td>mmrp-plus ring master master-port <PORTNO> slave-port <PORTNO.</td></tr><tr><td>mmrp-plus ring master master-port <PORTNO> slave-lag <LAGNO></td></tr><tr><td>mmrp-plus ring master master-lag <LAGNO> slave-port <PORTNO></td></tr><tr><td>mmrp-plus ring uplink port <PORTRANGE></td></tr><tr><td>interface port <PORTRANGE></td></tr><tr><td>dot1x port <PORTRANGE> initialize</td></tr><tr><td>dot1x port <PORTRANGE> re-authenticate</td></tr><tr><td>[no] dot1x port <PORTRANGE></td></tr><tr><td>[no] web-authentication port <PORTRANGE> dot1x</td></tr><tr><td>[no] dot1x port <PORTRANGE> timeout quiet-period</td></tr><tr><td>[no] dot1x port <PORTRANGE> timeout tx-period</td></tr><tr><td>[no] dot1x port <PORTRANGE> timeout re-authperiod</td></tr><tr><td>[no] dot1x port <PORTRANGE> timeout supp-timeout</td></tr><tr><td>[no] dot1x port <PORTRANGE> reauthentication</td></tr></table></td></tr>
</table>

Version	管理番号	内容
		[no] dot1x port <PORTRANGE> ignore-eapol-start show access-defender dot1x port <PORTRANGE> 【事象】 8.25.XX のバージョンでは、(1)の条件のみで装置が再起動することがあります。さらに(2)(3)の条件を伴うことで発生確率が高くなります。 8.24.XX 以前のバージョンでは、(1)(2)の条件をどちらも満たした場合に装置が再起動することがあります。さらに(3)の条件を伴うことで発生確率が高くなります。 また、いずれのバージョンにおいても IEEE802.1X 関連ログのタイムスタンプが不正となることがあります。
8.26.01	AEOS-82601-RC061	Apresia15000 シリーズの AccessDefender 機能において、動的 VLAN の割り当てが 256 端末までしかできない問題を修正しました。 修正前のバージョンでは、257 個以上の端末に動的 VLAN 割り当てを試みると以下の問題が発生していました。 • 257 個目以降の動的 VLAN の割り当てが行えず、認証が失敗する • 動的 VLAN を伴わない認証端末が認証成功した場合においても当該端末からの通信が行えなくなる 動的 VLAN の割り当てが 257 端末以上になるより前に認証成功した端末については、通信に影響はありません。
8.27.01	AEOS-82701-RC011	AccessDefender 機能において、"show access-defender lag-configuration"の gateway 表示説明行の最後に「,」がない問題を修正しました。
8.27.01	AEOS-82701-RC012	AccessDefender 機能において、スタティック認証設定時、エラーメッセージの末尾に"."がない問題を修正しました。
8.27.01	AEOS-82701-RC013	AccessDefender 機能において、ゲートウェイ認証と他の認証方式の認証ポートの設定において、エラーメッセージの一部が大文字になる問題を修正しました。
8.27.01	AEOS-82701-RC014	AccessDefender 機能において、"dot1x timeout"のヘルプメッセージの内容が"sec"、"secs"と統一されていない問題を修正しました。修正後は、ヘルプメッセージで時間の単位(秒)は"s"と表示されます。
8.27.01	AEOS-82701-RC019	AccessDefender 機能と VRRP 機能の併用をサポートしました。 ただし、AccessDefender 機能の DHCP Snooping 機能と VRRP 機能の併用は未サポートです。
8.28.01	AEOS-82801-RC037	AccessDefender 機能において、Web 認証で SSL2.0 を利用する場合、SHA-1、または SHA-2 で作成した証明書との組み合わせが使用できなくなりました。
8.28.01	AEOS-82801-RC038	AccessDefender 機能と MMRP-Plus 機能、MLAG 機能との併用時において、MLAG 機能有効時における認証ポートと MMRP-Plus のリングポートの設定禁則エラーメッセージの見直しを行いました。
8.28.01	AEOS-82801-RC077	AccessDefender 機能において、Web 認証の認証中に以下のコマンドを実行して構成情報に変更が生じた場合、装置からクライアント宛の認証応答パケットの送信元 IP アドレスが 127.0.0.1 となる問題を修正しました。

Version	管理番号	内容
		• "web-authentication port" • "web-authentication lag" • "web-authentication mlag" • "web-authentication http-port" • "web-authentication https-port" • "web-authentication ip" • "web-authentication redirect url" • "web-authentication redirect http" • "web-authentication redirect https" • "web-authentication redirect proxy-port" • "web-authentication snooping proxy-port" 本問題修正前のバージョンでこの問題が発生すると、クライアント側のブラウザーにて認証結果が表示されなくなります。
8.29.01	AEOS-82901-RC009	AccessDefender 機能において、Web 認証で使用する HTTP/HTTPS セッションタイムアウト時間を設定するコマンドをサポートしました。 • "web-authentication http-session-timeout <SECONDS>" TCP の 3 ウェイハンドシェイク後、本コマンドで設定したタイムアウト時間内に HTTP/HTTPS リクエストを本装置の Web サーバーが受信できない場合に、当該セッションを切断します。
8.29.01	AEOS-82901-RC017	AccessDefender 機能において、"logging access-defender web-access on" コマンドを設定した際の認証処理の見直しを行いました。
8.30.01	AEOS-83001-RC004	AccessDefender 機能において、MAC 認証のパスワードとして認証端末の MAC アドレスを使用するコマンドをサポートしました。 • "mac-authentication password-mac-address"
8.30.01	AEOS-83001-RC024	AccessDefender 機能の DHCP Snooping 機能において、"dhcp-snooping static-entry"コマンドを設定した場合、"show access-defender client" コマンドの"VID"フィールドに"0"と表示される問題を修正しました。 同様に、出力されるログに"vid=0"が表示される問題を修正しました。
8.30.01	AEOS-83001-RC025	AccessDefender 機能の DHCP Snooping 機能において、規格外である 286 オクテット未満(FCS を含む)の DHCP パケットを受け取ると、DHCP Snooping 機能が停止することがある問題を修正しました。 本問題の修正前のバージョンで本問題が発生した場合は、装置を再起動することで復旧が可能です。
8.31.02	AEOS-83102-RC006	AccessDefender 機能の"aaa authentication"コマンドにおいて、"port" オプションをサポートしました。 • "aaa authentication web [<ID>] <RADIUS1> | <LOCAL> | <FORCE> [port <PORTRANGE>]" • "aaa authentication mac <RADIUS1> | <LOCAL> | <FORCE> [port <PORTRANGE>]" 本オプションを設定することにより、認証ポート毎に RADIUS サーバー、ローカル、強制認証を設定することが可能になります。 本オプションは認証方式として Web 認証、MAC 認証を指定した際にのみ設

<table>
<tr><th>Version</th><th>管理番号</th><th>内容</th></tr>
<tr><td></td><td></td><td>定可能です。IEEE802.1X は未サポートです。
本オプション設定時は、"aaa authentication control"コマンドとの併用は未サポートです。</td></tr>
<tr><td>8.31.02</td><td>AEOS-83102-RC007</td><td>AccessDefender 機能の"logout aging-time"コマンドにおいて、"dhcp-snooping"オプションをサポートしました。
• "logout aging-time <TIME> dhcp-snooping"

設定した無通信時間を経過すると、認証済み端末を自動的にログアウトさせます。
無通信監視対象となるパケットは以下の通りです。

<table>
<tr><th></th><th>認証方式</th><th>無通信監視対象パケット</th></tr>
<tr><td>(1)</td><td>DHCP Snooping のみ</td><td>① Sender IP が認証端末の ARP パケット
② 送信元 IP が認証端末の IP パケット</td></tr>
<tr><td>(2)</td><td>DHCP Snooping と Web/IEEE802.1X 認証(AND)を併用</td><td>DHCP Snooping と Web/IEEE802.1X 認証(AND)が独立して以下のパケットを監視
① DHCP Snooping
Sender IP が認証端末の ARP パケット
② Web/IEEE802.1X 認証(AND)
送信元 MAC アドレスが認証端末である IP パケット</td></tr>
<tr><td>(3)</td><td>DHCP Snooping と(2)以外の認証方式の併用</td><td>① DHCP Snooping で登録された場合
Sender IP が認証端末の ARP パケット
② Web/MAC/IEEE802.1X で認証された場合
送信元 MAC アドレスが認証端末である IP パケット</td></tr>
</table>
</td></tr>
<tr><td>8.31.02</td><td>AEOS-83102-RC009</td><td>SSL 機能において、デフォルトのサーバー証明書、及び秘密鍵を変更しました。
証明書要求(CSR)発行に必要な項目の内、以下の表に示す項目の値、及び有効期限が変更になります。

<table>
<tr><th>項目</th><th>8.30.XX 以前</th><th>8.31.02 以降</th><th>備考</th></tr>
<tr><td>Organization</td><td>Hitachi Cable, Ltd.</td><td>Example Domain.</td><td></td></tr>
<tr><td>Organization Unit</td><td>Information Systems Group</td><td>Example Group.</td><td></td></tr>
<tr><td>Email Address</td><td>apresia@hitachi-cable.co.jp</td><td>example@example.com</td><td></td></tr>
<tr><td>有効期限</td><td>2009/8/19～2029/8/14</td><td>2017/1/25～2037/1/20</td><td>時刻情報は省略</td></tr>
</table>
</td></tr>
</table>

Version	管理番号	内容
		本仕様変更は、バージョンアップ後に"erase ssl-files"コマンド、もしくは"factory-default"コマンドを実行することで反映されます。 サーバー証明書の内容は、"show ssl https-certificate"コマンドで表示可能です。
8.31.02	AEOS-83102-RC017	AccessDefender 機能において、"logout aging-time"コマンド、または"logout aging-time dot1x"コマンドが設定されている状態で、"no access-defender"コマンドを実行して、構成情報から"logout aging-time"コマンド、または"logout aging-time dot1x"コマンドの設定を削除した後、IEEE802.1X の認証設定をした場合、"logout aging-time"コマンド、または"logout aging-time dot1x"コマンドの設定がないにも関わらず、IEEE802.1X のログイン端末に対して、エージングログアウト機能が動作する問題を修正しました。
8.31.02	AEOS-83102-RC018	AccessDefender 機能において、"logout timeout"コマンド、または"logout timeout dot1x"コマンドが設定されている状態で、"no access-defender"コマンドを実行して、構成情報から"logout timeout"コマンド、または"logout timeout dot1x"コマンドの設定を削除した後、IEEE802.1X の認証設定をした場合、"logout timeout"コマンド、または"logout timeout dot1x"コマンドの設定がないにも関わらず、IEEE802.1X のログイン端末に対して、タイムアウト機能が動作する問題を修正しました。
8.31.02	AEOS-83102-RC019	AccessDefender 機能において、"dot1x port"コマンドの設定が無く、かつ"dot1x mac-authentication-password"コマンドの設定がある状態で、"no access-defender"コマンドで設定を削除した後に IEEE802.1X 認証を行うと、IEEE802.1X/MAC 認証の動作が行われる問題を修正しました。
8.31.02	AEOS-83102-RC020	AccessDefender 機能において、"aaa authentication dot1x"コマンドで"local"オプションが指定できる問題を修正しました。
8.32.01	AEOS-83201-RC019	Apresia13100/13200-48X/13200-52GT シリーズの AccessDefender 機能において、動的 VLAN の割り当て(DVLAN)、またはクラス ID を使用して認証した端末が、一度でも「同時に 244 台以上ログインした状態」になった後に特定の端末がログアウトすると、認証処理が動作しなくなることがある問題を修正しました。 本問題は 8.21.01 以降のバージョンで発生していたものです。 Apresia15000 シリーズでも同様の問題がありましたが、8.26.01 以降で修正されています。 事象の詳細は、フィールドノーティス"FN_29A84-1"を参照ください。
8.33.01	AEOS-83301-RC005	AccessDefender 機能において、"show tech-support access-defender"コマンド実行時に取得できる情報の見直しを行いました。
8.34.01	AEOS-83401-RC004	AccessDefender 機能において、MAC 認証有効ポートで受信する自装置の CPU 宛てのフレーム、およびソフトウェア中継されるフレームのうち、認証バイパスの対象フレームの場合は MAC 認証を行わないようにする機能をサポートしました。 • "mac-authentication bypass-frame-check enable"
8.34.01	AEOS-83401-RC005	AccessDefender 機能の"aaa authentication control"コマンドにおいて、"port"オプションをサポートしました。

Version	管理番号	内容
		• "aaa authentication (web [<ID>]) mac control sufficient [port <PORTRANGE>]" 本オプションを設定することにより、複数の認証(プライマリー/セカンダリーRADIUS サーバー、ローカル、強制)が設定されている場合、認証ポート毎にいずれか 1 つの認証に成功することで認証を成功させることが可能となります。 本オプションは認証方式として Web 認証、MAC 認証を指定した際にのみ設定可能です。
8.34.01	AEOS-83401-RC006	AccessDefender 機能の"aaa authentication"コマンドにおいて、"port"オプションを設定した際の"aaa authentication control"コマンドとの併用をサポートしました。
8.34.01	AEOS-83401-RC009	AccessDefender 機能において、認証処理の見直しを行いました。
8.35.01	AEOS-83501-RC004	AccessDefender 機能の IEEE802.1X 認証において、VLAN タグ付きの EAP フレームによる認証を可能とする機能をサポートしました。 • "dot1x tagged-eap-frame enable"
8.36.01	AEOS-83601-RC016	AccessDefender 機能において、ログイン中の端末が接続しているインターフェースに対して"dot1x port"コマンドで上書き設定を行うと"config change"の要因でログアウトする問題を修正しました。
8.37.01	AEOS-83701-RC005	AccessDefender 機能において Web 認証でプロキシリダイレクトを使用する際において、認証端末が HTTPS プロトコルを使用した場合にもリダイレクトを行うように仕様を変更しました。

AEOS Ver. 8 アプリケーションノート
(AccessDefender 編)

2010 年 5 月 初版
2019 年 9 月 第 13 版

APRESIA Systems 株式会社
東京都中央区築地二丁目 3 番 4 号
築地第一長岡ビル
https://www.apresiasystems.co.jp/