



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
А	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
		 6.7 固定 IP アドレス端木の接続(DHCP Snooping)を追加 2 均限事項 みずご会事項を換工
		 7 利限事項、及び注息事項を修止 7.0 Windows 標準サプリカントにおける 000 4V の問題上を修正
р	2010年10日10日	• 7.2 WINDOWS 標準リノリカノトにのける 802.1X の同題只を修止
Б	2010年10月19日	• Aprestats200 シリースに対応 • ま 2.2 Access Defender 機能の仕様を修正
		
		• 2.7 Web 認証と WAG 認証() RU2 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_Spooping)の説明を修正
		 335 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
С	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
		 3.11.3.3 HTPS を用いる際の注意点の設定例を修止
		• 3.18 Web/MAC 認証の MAC 認証属性を追加
		 4.3 Web 認証、MAU 認証の混仕境現の設定例を修正 4.0 DUOD 0
		• 4.9 DHCP Shooping の設定1例を1修正
		• 4.13.1 クフス ID 端木環境の設定例を修止
	2012 年 11 日 20 日	▼ 3.2.1 l l l l l l l l l l l l l l l l l l l
	2013年11月29日	 ・ 土早で刈家に決手・加手・仲裁を修正 ・ 主 2 2 AccoreDatandar 機能の仕様を修正
		▼ 衣 2-2 ACCESSDETEILLET (機能の圧厥を形止) ■ 素 2-3 AccessDefender で使用するパケットフィルター? のグループ粉な
		- 12 2-3 AULESSDETEILUET C使用するハワッドノイルクー2 00クルーノ数を 修正
		◎ == 2-4 パケットフィルター2のグループた使用するコフンドを修正
		・ 衣 2-4 ハワットフィルター2 のフルーノを使用するコミノトを修止

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 認証ログー覧を修正
				• 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
				• 2.7 802.17/MAC 認証(AND) (802.17 の認証時の MAC 認証元1))を修正 。 2.9 Web (802.17 前江(AND) (Web 詞江 F 802.17 の従田詞江)を追加
				• 2.8 Web/802.1A 認証(AND) (Web 認証と 802.1A の併用認証)を追加
				● 2.9.2 DHCP Shoopingの動作ノローを修正
				● 2.11.2 DHCP Shooping O認証确本奴を修正 ● 2.12 ログマウト加理についてた修正
				・2.13 ログゲット処理についてを修正
				頃を戸加 • 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 3	年8月2	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
Н	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 1	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
				 表 5-5 802.1X 機能で使用する RADIUS 属性を修正
				 表 8-1 認証ログー覧を修正
				• 表 8-2 ログアウトで表示されるタイブー覧を修正
				 表 8-3 AccessDefender 設定時のコンフリクトメッセージー覧を修正
				 ・ 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 ブロキシ経由での 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)を修止 5.6 認証順序変更(Web 認証、MAC 認証のみ)を修止
				• 3.11 認証ヘーンのリダイレクト機能を修止
				• 3.11.1.2 認証ペーンリダイレクト機能設定例を修正
				• 3.11.2.2 認証ペーンリッイレクト機能設定例を修正
				 3.11.3.2 ノロキン利用環境にのける FILPS 通信の注意を修正 2.17 初証開始時の EAD Poguest /EAD Identity の抑制を修正
				◆ 3.20 ローマング機能を追加 ● 3.21 SQL プロトコルの胎弱性対応を追加
				 ● 3.21 35L ノロドコルの施弱性対応を追加 ● 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 初証端末のコーザーID(MAC アドレス)による MAC 初証を追加
				 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。

シリ	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	Apresia	Apresia13200-28GT	Ver. 8.37.01
13200 シリーズ	13200-28GT シリーズ	Apresia13200-28GT-PoE	
	Apresia	Apresia13200-48X	
	13200-48X シリーズ	Apresia13200-48X-PSR	
	Apresia	Apresia13200-52GT-PSR	
	13200-52GT シリーズ	Apresia13200-52GT	
Apresia	Apresia	Apresia15000-32XL-PSR	
15000 シリーズ	1500-32XL シリーズ	Apresia15000-32XL-PSR-1GLIM	
	Apresia	Apresia15000-64XL-PSR	
	1500-64XL シリーズ	Apresia15000-64XL-PSR-1GLIM	

適用機種一覧表



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。
- APRESIA は、APRESIA Systems 株式会社の登録商標です。
- AEOS は、APRESIA Systems 株式会社の登録商標です。
- AccessDefender は、APRESIA Systems 株式会社の登録商標です。
- BoxCore は、APRESIA Systems株式会社の登録商標です。
- MMRP は、APRESIA Systems 株式会社の登録商標です。
- Ethernet/イーサネットは、富士ゼロックス株式会社の登録商標です。
- Microsoft は、米国、及びその他の国における米国 Microsoft Corp.の登録商標です。
- Windows は、米国、及びその他の国における米国 Microsoft Corp.の登録商標です。
- Linux は、Linus Torvalds 氏の米国、及びその他の国における登録商標、または商標です。
- Internet Explorer は、米国 Microsoft Corp.の登録商標です。
- Wi-Fi は、Wi-Fi Alliance の登録商標です。
- Macintosh、Mac OS は、米国 Apple Computer, Inc.の登録商標、または商標です。
- Safari は、米国 Apple Computer, Inc.の登録商標、または商標です。
- iOS は、Cisco 社の登録商標、または商標です。
- Android は、Google Inc.の登録商標です。
- その他記載の会社名、及び製品名は、それぞれの会社の商標、または登録商標です。

制	定・	改訂来歷表	. 1
13	じめ	ວໄວ	. 8
1	概要	₹	14
	1.1	AccessDefender 概要	14
	1.2	AccessDefender がサポートする認証モード	15
	1.3	ユーザー認証	16
	1.4	IEEE 802.1X	17
	1	.4.1 802.1X で使用される認証方式	19
	1	.4.2 EAP のパケットフォーマット	20
	1.5	DHCP Snooping 概要	21
	1.6	ユーザーポリシーコントロール概要	22
2	Acce	essDefender の仕組み	23
	2.1	Web 認証(Web ブラウザーによるユーザー認証)	23
	2	.1.1 Web 認証の認証フロー(VLAN 固定で運用する場合)	23
	2	.1.2 Web 認証の認証フロー(VLAN 変更での運用の場合)	24
	2.2	ゲートウェイ認証	26
	2.3	MAC 認証(MAC アドレスによる端末認証)	28
	2.4	Web 認証と MAC 認証の混在ポートでの認証フロー	29
	2.5	Web/MAC 認証(AND) (Web 認証時の MAC 認証先行)	30
	2.6	802.1X	32
	2	.6.1 802.1Xの認証フロー	32
	2	.6.2 Unicast-EAP 機能	33
	2	.6.3 動作確認済サプリカント一覧	34
	2.7	802.1X/MAC 認証(AND) (802.1X の認証時の MAC 認証先行)	35
	2.8	Web/802.1X 認証(AND) (Web 認証と 802.1X の併用認証)	37
	2.9	DHCP Snooping	40
	2	.9.1 DHCP Snoopingの動作モード	40
	2	.9.2 DHCP Snoopingの動作フロー	40
	2.1) ユーザーポリシーコントロールの動作フロー	44
	2.1	1 認証機能と仕様	45
	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	46
	2	.11.2 DHCP Snoopingの認証端末数	48
	2.1	2 Web サーバー応答、及び仮想 IP の仕組み	50
	2	.12.1 Web サーバーの仮想 IP の仕組み	50
	2	.12.2 認証ページリダイレクトを使用する際の注意点	51
	2	.12.3 動作確認済ブラウザー	52
	2.1	3 ログアウト処理について	54
	2.14	4 入力可能な文字について(ユーザーID/パスワード共通)	56
3	Acc	essDefender 機能の設定	57
-	3.1	APRESIAの設定項目	57
	3.2	ローカルデータベース認証と強制認証	59
	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)	61
	3	.3.1 ローカルデータベースフォーマット	61
	3	.3.2 ローカルデータベースの登録(ダウンロード)	62

目次

	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)	. 63
	3.3.4 ローカルデータベースの削除	. 63
	3.3.5 ローカルデータベースの編集(追加)	. 63
	3.3.6 ローカルデータベースの編集(削除)	. 64
	3.4 強制認証機能	. 65
	3.5 強制認証機能(802.1X)	. 66
	3.6 認証順序変更(Web 認証、MAC 認証のみ)	. 67
	3.7 移行条件変更機能(Web 認証、MAC 認証のみ)	. 69
	3.8 認証方法選択機能(Web 認証のみ)	. 71
	3.9 認証バイパス	. 72
	3.9.1 認証バイパスの概要	. 72
	3.9.2 認証バイパスによる強制転送設定例(1)	. 74
	3.9.3 認証バイパスによる強制転送設定例(2)	. 75
	3.9.4 Windows ドメイン環境への適用	. 76
	3.10 認証拒否機能	. 77
	3.11 認証ページのリダイレクト機能	. 78
	3.11.1 HTTP プロキシが無い環境(直接 Internet へ接続)	. 79
	3.11.2 HTTP プロキシサーバーが存在する環境	. 82
	3.11.3 Web ループ検知が必要な状況	. 85
	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	. 87
	3.12.1 認証フロー	. 87
	3.13 DHCP Snooping の固定 IP アドレス端末接続	. 88
	3.13.1 static-entry設定による方法	. 88
	3.13.2 認証バイパス設定による方法	. 88
	3.14 TTL フィルター	. 89
	3 15 PING ログアウト	
	3.16 DHCP パケットの MAC 認証除外	. 93
	3 17 認証開始時の FAP-Request / FAP-I dentity の抑制	. 94
	3 18 認証失敗時のステータス保持時間の変更	. 95
	3 19 Web/MAC 認証(AND)の MAC 認証属性	. 00
	3 20 ローミング機能	98
	3.21 SSI プロトコルの脆弱性対応	100
	3 22 HTTP/HTTPS セッションタイムアウト時間の設定	101
	3 23 認証端末のコーザーID(MAC アドレス)による MAC 認証	102
	3 24 DHCP Snooping のエージングログアウト機能	103
	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	105
	3 26 トランクポートでのタグ付き FAP フレームによる 802 1X	106
4	構成例	108
т	4.1 Web 認証	108
	4.2 Web 認証(MLAG 併用)	111
	4 3 MAC 認証	116
	4.4 MAC 認証(MI AG 併田)	110
	4.5 Web 認証 MAC 認証の混在理情	122
		125
	ィッ (meb) (mno ஸ…(n)(b)	120
	+・/ ノ Ⅰ ノエ1 吣Щ(ソ ̄ハ ̄ノブ ̄ム丁刖に週用) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	121

	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)	130
	4.9 ゲートウェイ認証(中央拠点アクセス手前に適用)	135
	4.10 802.1X	138
	4.11 802.1X(MLAG 併用)	140
	4.12 802.1X/MAC 認証(AND)	145
	4.13 Web/802.1X 認証(AND)	147
	4.14 DHCP Snooping	149
	4.15 DHCP Snooping、MAC 認証の混在環境	151
	4.16 DHCP Snooping、Web 認証(固定 VLAN)の混在環境	153
	4.17 DHCP Snooping、Web 認証(動的 VLAN)の混在環境	155
	4.18 ユーザーポリシーコントロール構成例	158
	4.18.1 クラス ID 端末環境	158
	4.18.2 クラス ID 端末/クラス ID 未付与端末の混在環境	161
5	認証サーバー(RADIUS サーバー)の設定項目	164
	5.1 認証サーバーの設定項目(Web 認証、MAC 認証)	164
	5.1.1 RADIUS クライアントの登録(clients.conf ファイルなど)	164
	5.1.2 ユーザー情報の登録(users ファイルなど)	164
	5.1.3 拡張設定(VLAN ID/クラス ID の設定)	165
	5.2 認証サーバーの設定項目(802.1X)	166
	5.2.1 EAPの設定(eap.conf ファイルなど)	166
	5.2.2 RADIUS クライアントの登録(clients ファイルなど)	166
	5.2.3 ユーザー情報の登録(users ファイルなど)	166
	5.2.4 拡張設定(VLAN ID/クラス IDの設定)	167
	5.3 RADIUS サーバーの冗長化	168
	5.4 AccessDefender で使用する RADIUS 属性	169
	5.5 RADIUS サーバー設定例(Windows 2000 server "IAS")(Web 認証/MAC 認証)	170
	5.5.1 RADIUS クライアントの設定	170
	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)	171
	5.5.3 VSA の設定(VLAN ID/クラス ID 変更時のみ必要)	175
	5.6 RADIUS サーバー設定例(Windows Server 2008)	178
	5.6.1 NPSの設定	178
	5.6.2 RADIUS クライアントの設定	180
	5.6.3 Web 認証、MAC 認証の設定	181
	5.6.4 Web 認証、MAC 認証のネットワークポリシー設定	188
	5.6.5 認証クライアントのドメイン参加	199
	5.6.6 802.1Xの設定	202
	5.6.7 802.1X のネットワークポリシー設定	209
	5.7 802.1X のクライアントの設定	225
	5.7.1 PEAP 設定	225
	5.7.2 TLSの設定	227
6	応用設定	234
	6.1 認証ページのカスタマイズ	234
	6.1.1 APRESIA 内部ページのカスタマイズ	234
	6.1.2 外部 Web サーバー上の任意のページへの埋め込み	235
	6.1.3 認証方法選択機能の認証ページカスタマイズ	236

	6.2 ユーザー認証時の持ち込み端末制限	237
	6.3 NAS(Network Access Server)属性	238
	6.3.1 NAS-IP-Address	238
	6.3.2 NAS-IPv6-Address	238
	6.3.3 NAS-Identifier	239
	6.3.4 NAS 属性の組み合わせ	240
	6.4 MAC アドレスの自動収集	242
	6.5 端末認証後のパケットフィルター2(アクション none)	244
7	制限事項、及び注意事項	246
	7.1 動的 VLAN 割り当て使用時の注意点	246
	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	246
	7.2 Windows 標準サプリカントにおける 802.1X の問題点	247
	7.2.1 Active Directory のグループポリシーを使用した回避	248
	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	259
	7.2.3 EAPOL-Start 受信による認証の抑止を用いた回避方法	261
	7.3 VRRP 併用時の注意点	263
8	AccessDefender 関連ログ	266
	8.1 認証ログ表示(syslog)	266
	8.2 設定時のコンフリクトメッセージ一覧	270
9	SSL 設定	271
	9.1 SSL 設定概要	272
	9.2 証明書要求を装置で発行する場合	273
	9.2.1 秘密鍵と証明書要求の生成	273
	9.2.2 証明書要求のアップロード	275
	9.2.3 証明書の発行	275
	9.2.4 証明書のダウンロード	275
	9.3 証明書要求を装置で発行しない場合	276
	9.3.1 秘密鍵と証明書要求の生成	276
	9.3.2 証明書の発行	279
	9.3.3 証明書と秘密鍵のダウンロード	280
	9.3.4 信頼されたルート証明機関として登録	281
	9.4 認証 URL ヘアクセス	284
	9.5 証明書の削除(初期化)	284
	9.6 中間 CA 証明書	285
	9.6.1 証明書要求を装置で発行する場合	286
	9.6.2 証明書要求を装置で発行しない場合	286
	9.6.3 認証 URL ヘアクセス(証明書の確認)	294
1(0 各バージョンでの機能追加、変更点	296

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。

		L3 制御					
項目		(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	ユーザー認証	端末認証	ユーザー認証			
	端末認証						
PKI 利用		×	×	×			
認証サーバー	RADIUS	RADIUS	RADIUS	RADIUS			
	(EAP 対応)						
認証用クライアント	802.1X 対応	汎用 Web ブラウザー	なし	汎用 Web ブラウザー			
ソフト	サプリカント						
適用クライアント OS	サプリカント	汎用 Web ブラウザー	制限無し	汎用 Web ブラウザー			
	利用可能 OS	利用可能 OS		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							

表 1-1 AccessDefender がサポートする認証モード

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

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。 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。 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。 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。

	電子証明書		クライアント/サー	特徴
	サーバー	クライ	バー間の双方向認証	
		アント		
EAP-MD5	不要	不要	ID/パスワードのみ	• ユーザー識別にユーザーID/パスワードを使用
			で、サーバーの認証	• サーバー認証機能がないため、セキュリティレ
			は行わない	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	• ユーザー識別にユーザーID/パスワード、または
			書と ID/パスワード	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	• ユーザー識別にユーザーID/パスワード、サー
			書と ID/パスワード	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

表 1-2 EAP 認証機能の比較

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。



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

端末が認証を要求します。

端末情報を基に認証サーバーに問い合わせます。

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。 APRESIA が端末情報とクラス ID を保持します。

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、プ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。

- 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。
- . 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。
- . 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。

. 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。

- 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。
- . 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。
- . 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。

- . 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。
- 9

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(-)。

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(-)。 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()。

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(--)。



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。

- 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。
- . 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。
- 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。
- . 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。
- . 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。

- .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。
- 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。

. 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。

- . 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。

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。

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	Windows XP SP2/SP3	EAP-MD5/PEAP/TLS
サプリカント(V3.0L20)		ユニキャスト EAP 対応確認済み
Odyssey Client Manager	Windows XP SP2/SP3	EAP-MD5/PEAP/TLS/EAP-TTLS
(4.32.0.2347)		

表 2-1 動作可否確認済みサプリカント

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。

- .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。
 - 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。
- .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。
- 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。
- . 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。
- . 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。

- .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。
- 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。
- 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。
- . 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。
- . 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。
- 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。
- . 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。
- . 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(-)と Web 認証のフロー(-)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(-)を、図 2-6の Web/MAC 認証(AND)フロー(-)

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 of fer 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。



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。

- .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。
- 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。
- . 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。
 - 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。

	項目	仕様	備考
認証	802.1X		
モード		(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	HTTP/HTTPS		
ジリダイ	Proxy 利用環境		HTTP のみ(HTTPS はリダ
レクト			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	対応サーバー	RADIUS	
サーバー	バックアップ	プライマリー、セカンダリー/強制認証/	強制認証/ローカルデー
		ローカルデータベース	タベースは単独使用可能
	ローカルデータ	3000 行	
	ベース	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	Web/MAC/802.1X/	Apresia13000 シリーズ:1024 端末/台	 利用環境により、最大
収容数	ゲートウェイ	Apresia13100/13200 シリーズ:5632 端末/台	収容端末数が異なる場
		Apresia13200-28GT シリーズ:1408 端末/台	合あり
		Apresia15000 シリーズ:768 端末/台	• Apresia13200-28GT シ
	Dynamic VLAN/	Apresia13000 シリーズ:1024 端末/台	リーズは、クラス ID
クラス ID		Apresia13100/13200 シリーズ:2048 端末/台	(ユーザーポリシーコ
		Apresia13200-28GT シリーズ:256 端末/台	ントロール)未サポー
		Apresia15000 シリーズ:768 端末/台	۲ - F
	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/Dvnamic VLAN	モード区別なし
	認証ページ		内部保存/外部サーバー
	カスタマイズ		併用可能
	認証バイパス		
全般	· ·	・ Web、MAC、802.1X、DHCP Snoopingの同一ポ・	
		● 認証ポートにおいて、認証不要端末の登録が	可能

表 2-2 AccessDefender 機能の仕様

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)。

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

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

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)。

機能	使用するグループ数
VLAN ごとのカウンター	1~2
(counter vlan enable コマンド)	
MLAG(mlag enable コマンド)	1
FDB 書き換わり多発検知	1
(mac-address-table	
frequent-station-move-notify enable コマン	
ド)	
ユーザーループ検知	Apresia13000 シリーズ:11
(loop-watch enable コマンド)	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	1
(flush-fdb rp-e enable コマンド)	
Flush FDB	1
(flush-fdb rp-g enable コマンド)	
MMRP-Plus	Apresia13000/13200-28GT シリーズ:1~2
(mmrp-plus enable コマンド)	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)	1
(mmrp-plus receive-flush-fdb enable コマン	
ド)	
IPアドレス(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
VB IP(vb ip address コマンド)	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	Apresia13000/15000 シリーズ:1 1
(ipv6 address コマンド、ipv6 enable コマン	Apresia13100/13200-48X/13200-52GT シリーズ:0~1
<u> ド)</u>	Apresia13200-28GT シリーズ:0~3
IGMP snooping	1
(ip igmp snooping unregistered-filter コマ	
ンド)	
MLD snooping	1
(ipv6 mld snooping unregistered-filter ⊐	
マンド)	
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

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

- 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 端末目以降の認証では、 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)

使用する	機種名							
グループ数	Apresia13000	Apresia13100/13200	Apresia13200-28GT	Apresia15000				
	シリーズ	シリーズ	シリーズ	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	-				

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



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。

9

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(vIan10)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



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。

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	i0S 6.0.1	
標準ブラウザー	Android 4.0.4	

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)

- IOS6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。

No	ログアウト方法	動作概要	Syslog	Web	MAC	802.1X	DHCP
			表示	認証	認証		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	ー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 v lan 変更検出	再認証時の v lan 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	-	-	-	

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	Web	MAC	802.1X	DHCP
			表示	認証	認証		Snooping
16	IP リース期間満了	IP リース期間満了によるログ	expire	-	-	-	
		アウト					
17	logout ping 受信	logout ping 受信によるログア	ping		-	-	-
		ウト					

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、「&」、「>」、「&It」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。

No	項目	default			認証方法		備考
		設定	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)						

表 3-1 AccessDefender 設定項目

No	項目	default			認証方法		備考
		設定	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
	802.1X 再認証実行	なし					行します)
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> セカンダリーRADIUS サーバーのインデックス <1-16> $\cdot \cdot \cdot INDEX2$ • • • 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、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。

14 0						
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					

表 3-3 ローカルデータベースフォーマット

<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

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。

<pre># copy (tftp <ipaddr>) memory-</ipaddr></pre>	card <file> aaa-local-db</file>
<pre># copy tftp <ipv6addr> [manage </ipv6addr></pre>	(vlan <vid>)] <file> aaa-local-db</file></vid>
• • • I PADDR	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。

れ い キ ノ ノンロ	
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	Error code 1: File not found.
ない場合	
ファイルサイズが上限を超	aaa-local-db : over max file size
えている場合	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

表 3-4 ダウンロード時のコンソールメッセージ表示例

	ldb.txt : download fail	
同一ユーザー名の行が複数	Invalid format:	
存在する場合	1useruser 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。

<pre># copy aaa-local-db (tftp <lpaddr>)</lpaddr></pre>	memory-card <file></file>
<pre># copy aaa-local-db tftp <lpv6addr> </lpv6addr></pre>	manage (vlan <vid>)] <file></file></vid>
• • • I PADDR	TFTP サーバーの IP アドレス
• • • I Pv6ADDR	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

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> [<</userid>	OPTIONS>]	
<i>OPTIONS</i> には以下オプションが複数指定可能		
<pre>OPTIONS = (password <password>) (</password></pre>	(vlan <vid>) (class <classid>)</classid></vid>	
• • • USERID	ユーザーID <1-63(文字)>	
• • • PASSWORD	パスワード <1-63(文字)>	
• • • VID	VLAN ID <1-4094>	
• • • CLASSID	クラス ID <1-4095>	

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。

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

表 3-5 登録時のコンソールメッセージ表示例

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>	
· · · 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	% Too long user ID.
定した場合	
未登録のユーザー名を指定し	% The user does not exist.
た場合	

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 < <i>RADIUS2</i> > < <i>FORCE</i> >		
<pre>RADIUS2 = radius <index1> [<</index1></pre>	INDEX2>] [< <i>FORCE</i> >]	
<pre>FORCE = force [vlan <vid>]</vid></pre>		
••• 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>] <<i>RADIUS1</i>> <<i>LOCAL</i>> <<i>FORCE</i>> [port <portrange></portrange></id>		
(config)# aaa authentication mac <i><radius1< i="">> <i><local< i="">> <i><force< i="">> [port <portrange>]</portrange></force<></i></local<></i></radius1<></i>		
RADIUS1 = radius <index1> [<index2>] [local <<i>FORCE</i>>]</index2></index1>		
<i>RADIUS2</i> = radius <index1> [<index2></index2></index1>] [< <i>FORCE</i> >]	
<i>LOCAL</i> = local [radius <index1> [<index2>] [<<i>FORCE</i>>]]</index2></index1>		
<i>FORCE</i> = force [vlan <vid>]</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> ローカルデータベース認証を実行 • • • local • • • 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】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 】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。

仕	羕	AccessDefender 認証バイパス	備考
主なフィルター	送信先	Ether Type	
条件		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		ポート(レンジ指定可能)	
	適用範囲指定	VLAN (マスク指定可能)	

表 3-9 認証バイパスの主な許可条件

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



0

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



グループ2の有効ポートは1-44(有効 VLAN は vIan300)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、ドメインヘ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	• AccessDefender 認証前に、必要なドメインコントローラ
	\downarrow	宛の通信に対し認証バイパスを使って許可
	2. AccessDefender認証	• 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。

<pre># access-defender-deny (ip <ipaddr>)</ipaddr></pre>) (mac <macaddr>) timer <minutes></minutes></macaddr>
• • • 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ヘリダイレクトする
- 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 ヘリダイレクトでき、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(<u>https://192.0.2.3:8443/</u>)(必須) (config)# dhcp policy temp (config-dhcp)# network 10.0.0/16

(config-dhcp)# range 1 10.0.0.10 10.0.0.20

(config-dhcp)# dns-server 10.0.0.253

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)。

・・・認証 URL(<u>https://192.0.2.3:8443/</u>)(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。



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。





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



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

A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 00:00:00:00:00:00 (config-filter)# 2 1 action authentication-bypass

0

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。



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 t	tl <ttl> <<i>INTERFACE</i>></ttl>
<pre>INTERFACE = (port <portrange>) (</portrange></pre>	lag <lagrange>) (mlag <mlagrange>)</mlagrange></lagrange>
• • • 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。



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。



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 < <i>INTERFACE</i> > timeout tx-period <secs></secs>							
<i>INTERFACE</i> = (port <portrange>) (lag <lagrange>) (mlag <mlagrange>)</mlagrange></lagrange></portrange>							
• • • 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 <i NTERFACE> timeout quiet-period <secs></secs>						
<i>INTERFACE</i> = (port <portrange>) (lag <lagrange>) (mlag <mlagrange>)</mlagrange></lagrange></portrange>						
• • • 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。

- . 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。
- . 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。
- . 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。
- . 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。
 - 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)。
- 記証端末の 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	<pre><portrange>) (lag <lagrange>) (mlag <mlagrange>) enable</mlagrange></lagrange></portrange></pre>
• • • 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。



HTTP プロトコルシーケンス

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</days></hours></minutes>
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。

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

表 3-11 冊通信欧祖対象フレーム(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。

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

表 3-12 無通信時間のリセットタイミング

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

ポートの	本機能	EAP フレー	Ъ	動的	802.1X 動作
VLANモード	の設定	受信	送信	VLAN	
アクセス		VLAN タグ無し	VLAN タグ無し		動的 VLAN(アクセスポート)
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

表 3-13 各設定条件における 802.1X の動作

ポートの	本機能	EAPフレーム		動的	802.1X 動作
VLANモード	の設定	受信	送信	VLAN	
アクセス	-	VLAN タグ無し	VLAN タグ無し		動的 VLAN(アクセスポート)
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		VLAN タグ無し	VLAN タグ無し		動的 VLAN(アクセスポート)
ポート					でログイン
(ネイティ				-	ネイティブ VLAN でログイン
ブ VLAN 設定		VLAN タグ設定済 VLAN	VLAN タグ無し	-	認証不可 1 2
あり)		(ネイティブ VLAN)			
		VLAN タグ設定済 VLAN	VLAN タグ受信		動的 VLAN(アクセスポート)
		(ネイティブ VLAN 以	と同じ VLAN		でログイン 2
		外)		-	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	VLAN タグ無し	-	認証不可 1 2
		(ネイティブ VLAN)			
		VLAN タグ設定済 VLAN	VLAN タグ無し	-	認証不可 1 2
		(ネイティブ VLAN 以			
		外)			
		VLAN タグ未設定 VLAN	VLAN タグ無し	-	認証不可 1 2
トランク		VLAN タグ無し	送信しない	-	認証不可 1 2
ポート		VLAN タグ設定済 VLAN	VLAN タグ受信		動的 VLAN(アクセスポート)
(ネイティ			と同じ VLAN		でログイン 2
ブ VLAN 設定				-	VLAN タグの VLAN でログイン
なし)		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 10.0.0/16 (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(<u>http://192.0.2.3:8080/</u>) (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の構成例における認証スイッチの設定例を示します。

(config)# vlan database (config-vlan)# vlan 10 name v10 (config-vlan)# vlan 20 name v20 (config-vlan)# vlan 100 name 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)=""></mlag(first>
(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)# 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)



- 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 10.0.0/16
(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 10.0.0/16 (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)# 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(<u>https://10.1.10.100:8443/</u>)(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。

ー対多の 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。



・・・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(<u>https://10.1.10.101:8443/</u>) (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)# 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)=""></mlag(first>	
(config)# logging ip 192.168.1.100 local0 notice	
・・・syslog サーバーの登録(優失度: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 dotix factus f ・・・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.daf)# packet filter2 may rule 120
(config-a-def)# packet-fifter2 max-fute 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)。

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 ip 192.0.2.3 (config-a-def)# web-authentication http-port 8080 ・・・認証 URL(<u>http://192.0.2.3:8080/</u>) (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。

・・・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)
```

0

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-a-def)# web-authentication ip 192.0.2.3 (config-a-def)# web-authentication http-port 8080 ・・・認証 URL(<u>http://192.0.2.3:8080/</u>) (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の構成例における認証スイッチの設定例を示します。

(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。

- は 端末の ARP フレームは DHCP Snooping 登録後、自動的に許可されます。
- 動
 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 20.0.0/24 (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 gos gp7 (config-filter)# 3 1 condition dst ip 20.0.0/24 (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 gos gp7 (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 ユーリーホリシーコンドロール構成例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-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 20.0.0/24 (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 gos gp7 (config-filter)# 3 1 condition dst ip 20.0.0/24 (config-filter)# 3 1 condition class 1 ・・・クラス ID:1の設定(20.0.0/24 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(<u>https://10.1.10.100:8443/</u>)(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。

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
1			

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-ld = 33 ,
	Access-Defender-Class = 10
user2	Auth-Type = Local, Password = "user2", Calling-Station-Id = "000102030a0b"
000bdbd64209	Auth-Type = Local, Password = "testing123" NA-VIan-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。

			· —
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
	值	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)

表 5-1 認証応答で使用するベンダー独自属性

<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-VIan-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>

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。

属性	属性值	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、	可変
		または VLAN 名称	

表 5-2 動的 VLAN 変更で使用する RADIUS 属性

<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。

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)

表 5-3 認証応答で使用するベンダー独自属性

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	属性值
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
Tunne I - 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)。

🍫 インターネット認証サービス					
│ 操作(A) 表示(V) │ (= ⇒ │ 🔁 🗍	🖬 📄 🖪 🛛	2			
ツリー	フレンドリ名	アドレス	1 วิตหวม	クライアント製造元	
 ・クターネット認証サービス (ローカル) ・ ・ ・	apresia01	10.32.24.1	RADIUS	RADIUS Standard	

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。

🤣 ብンターネ	ット認証サ	1-EZ			
ファイル(E)	操作(<u>A</u>)	表示♡	ヘルプ(円)		
	サービス サービス	の開始(S) の停止(T)			
🕐 1 29 - 4 🗄 - 🧰 RAD	Active	Directory (サーバーを登録(<u>a</u>)	
🗄 🚞 UE –	プロパテ	т(<u>R</u>)			
🤨 リモー 田・ 🧰 接続	ヘルプひ	Ð			インターネット認証サービス_(IAS)を使ってネットワ
13074	24.002-1				ヤルアップ、VPN、ワイヤレス、およびイーサネット予 承認およびアカウンティングを行います。認証要求
					認証ダイヤルイン ユーザー サービス (RADIUS) { るアクセス サーバーに転送するように、IAS を構成 きます。
					Active Directory にあるユーザー アカウントのリイ プロパティを読み取るように IAS を構成するには、 一の [Active Directory にサーバーを登録] をり い。
I	~~~~	~~~~	·····	~	

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。

RADIUS クライアントの追加	×
クライアント情報	
クライアンドに関する情報を指定します。	
クライアントのアドレス(IP また(は DNS)(<u>D</u>):	
192.168.1.253 確認公…	
クライアント製造元(L):	
RADIUS Standard	
□ クライアントは要求時に常に署名属性を送信する(Q)	
共有シークレット(S): *******	
共有シークレットの確認入力(E): *******	
·	-
く戻る(B) 完了 キャンセル	
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。

リモート	アクセス ポリシーの追加	×
ポリ	シー名 ポリシーに付けるフレンドリ名を指定してください。	
	リモート アクセス ポリシーは、特定の条件を満たしたユーザーのグループに対して適用できる、操作の集ま りです。	_
	電子メール アブリケーションの受信トレイ ルールのように、リモート アクセス ポリシーにも条件を設定し、そ の条件に合ったユーザーに適用する操作を指定することができます。	
	ポリシーのフレンドリ名(P): MAN100	
		-
	〈戻る(四) 次へ(11) > キャンセル	

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。

1	国 居性の選択				
	追加する属性の種類を選択してから、「追加」 をクリックしてください。 属性の種類(A):				
	名前	説明			
	Called-Station-Id Calling-Station-Id Client-Friendly-Name Client-IP-Address Client-Vendor Day-And-Time-Rest Framed-Protocol NAS-Identifier NAS-IP-Address NAS-Port-Type Service-Type Tunnel-Type Windows-Groups	ユーザーが攻イヤルした電話番号です 発信元の電話番号です RADIUS クライアントのフレンドリ名です (IAS のみ) RADIUS クライアントの IP アドレスです (IAS のみ) RADIUS クライアントの IP アドレスです (IAS のみ) ユーザーが接続を許可されている時間帯と曜日です (使用するプロトコルです 要求を発信した NAS を識別する文字列です (IAS のみ) 要求の発信元の NAS の IP アドレスです (IAS のみ) 要求の発信元の NAS の IP アドレスです (IAS のみ) 要求の発信元の NAS の IP アドレスです (IAS のみ) 要求の発信元の NAS で使用される物理ポートの種類 ユーザーの要求したサービスの種類です (使用されるトンネリング プロトコルです ユーザーが所属する Windows のグループです))) です		
	•		►		
		道加(<u>D</u>) キャンセノ	ŀ		

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。

≫ <mark>∎</mark> グループの選択		? ×
場所(L): 🗊 lab.hel.co.jp		T
名前	フォルダ	
🕵 Domain Guests	lab.hcl.co.jp/Users	
🕵 Group Policy Creator Owners	lab.hcl.co.jp/Users	
🕵 DnsUpdateProxy	lab.hcl.co.jp/Users	_
🚮v10	lab.hcl.co.jp/Users	
<u>∰</u> v20	lab.hcl.co.jp/Users	
	lab.hcl.co.jp/Users	-
<u>追加(A)</u> <u>×10</u>		
	OK	

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。

リモート アクセス ポリシーの追加	X
条件 条件を設定します。	
条件を指定してください。	
条件(<u>C</u>):	
Windows-Groups が次のものと一致: "LAB¥v10"	
< 戻る(B) (次へ(N) > (キャンセル	

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。

リモート アクセス ポリシーの追加	×
アクセス許可 リモート アクセス許可を与えるか拒否するかを指定します。	
リモート アクセス ポリシーは、特定のアクセス特権を特定のユーザー グループに与えたり、アクセスを拒否 したりする場合に使用します。	
ユーザーが指定の条件を満たした場合:	
● リモート アクセス許可を与える(④)	
○ リモート アクセス許可を拒否する(D)	
< 戻る(B) 次へ(N) > キャンセル	

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。

リモート アクセス ポリシーの追加	×
ユーザー プロファイル ユーザー プロファイルを指定します。	
指定した条件を満たしたユーザーのブロファイルを指定することができます。	
注意: ユーザーのアクセスを拒否するように指定していても、このポリシーの条件がユーザー単位で上書き された場合は、プロファイルが使用されます。	
[フロファイルの編集也…]	
〈戻る(B) 完了 キャンセル	

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。

ダイヤルイン プロファイルの編集	? ×
ダイヤルインの制限 IP マルチリンク 認証 暗号化 詳細	
この接続で許可されている認証方法のチェック ボックスをオンにします。 「拡張認証プロトコル(E) このポリシーで使用できる EAP の種類を選択します。 スマート カードまたはその他の証明書 「」 構成(E)…	
🥅 Microsoft 暗号化認証バージョン 2(MS-CHAP v2)②	
☐ Microsoft 暗号化認証 (MS-CHAP)(M)	
□ 暗号化認証 (CHAP)(N)	
✓ 諸号化されていない認証 (PAP、SPAP)(U)	
- 認証されていないアクセス	
	v I
	·)

(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。

ダイヤルイン	設定 🗾 🕺 🕺
	認証方法がいくつか選択されました。リモート アクセス、ポリシー、およびドメイン レベルに対してプロトコルがそれぞれ正しく 構成されていることを確認するには、ヘルプの説明に順に従ってください。 これに関するヘルプのトピックを表示しますか?
	<u>(北)支(M)</u>

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。

ダイ	ヤルイン プロファイルの	扁集	<u>? ×</u>
ß	『イヤルインの制限 IF	マルチリンク 認証 暗号化 詳細]
	リモート アクセス サーノ	<-−に返される接続の属性を指定します。	
	パラメータ(P):		
	名前	ベンダ 値	
	Service-Type Framed-Protocol	RADIUS Standa Framed RADIUS Standa PPP	
	•		
	<u>追加(0)</u>	削除(R) 編集(E)	
		OK キャンセル	適用(<u>A</u>)

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。

屋性をプロファイル(に)自ちのオス((住屋性を)避け」、「自ちの」を力しい力して(ださい)
는 NTATE 12 YEAR AND A SHARE AND A MADE TO MADA AND A THEAD AND A CARACTERS
RADIUS 属性(S):
名前 べンダ 説明 ▲
Tunnel-Client-Auth-ID RADIUS Standaトンネル確立の認証フェーズの間にトンネルの発端側によって使用され、 Tunnel-Client-Furdat
Tunnel-Medium-Type RADIUS Standa 発行詞のパンネルのゴアアドレスです Tunnel-Medium-Type RADIUS Standa 複数のトランスポートで運用できるプロトコル(12TP など)のトンネルを
Tunnel-Password RADIUS Standaリモートサーバーへ認証するためのパスワードです
Tunnel-Preference RADIUS Standa トンネルの発端側ヘトンネリングの属性のセットが 2 つ以上返されたとき
Tunnel-Pvt-Group-ID RADIUS Standa 特定のトライル ゼッソヨンのクルーフ ID (19 Tunnel-Server-Auth-ID RADIUS Standa トンスル確立の認証フェーズの問題といえルの終端側によって使用されと
Tunnel-Server-Endpt RADIUS Standa サーバー側のトンネルの IP アドレスです
Tunnel-Type RADIUS Standa 使用されるトンネリング プロトコルです
Vendor-Specific RADIUS Standa 古() NAS 専用機能のサポートに使用されます Cipage AV-Pair Cipage AV-Pair VSA
Janore-User-Dialin-Prop Microsoft フレザーのダイヤルインのプロパティを無視します
USR-ACCM-Type U.S. Robotics, I 説明文はありません
USR-AT-Call-Input-Filter U.S. Robotics, I 説明文はありません USR AT Coll October 5: U.S. Robotics, I 説明文はありません
USR-AT-Call-Output-Film U.S. Robotics L. 説明文はありません USR-AT-Input-Filter U.S. Robotics I 説明文はありません
USR-AT-Output-Filter U.S. Robotics, I 説明文はありません
USR-AT-RTMP-Input-Fi U.S. Robotics, I 説明文はありません
USR-AT-RIMP-OutputU.S. Robotics, L. 説明又はありません USR-AT-Zin-Toput-Filter, U.S. Robotics, I. 説明史はありません。
道加(A) 閉じる

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。

複数値の属性情報	?×
属性の名前に	
Vendor-Specific	
周性の番号:	
26	
属性の形式に	
OctetString	
属性の値(1):	
ベンダ 値	上へ(<u>U</u>)
	下へ回
	」 追加(A)
	<u>削除(R)</u>
↓	編集(E)
OK	キャンセル

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。

ベンダ特有の属性情報		? ×
属性の名前:		
Vendor-Specific		
ネットワーク アクセス サーバーのべこ	/ダを指定してください。	
○ 一覧から選択する(S):	RADIUS Standard	V
● ベンダ コードを入力する(<u>E</u>):	278	
べンダ特有の属性用の RADIUS F さい。	RFC 仕様にこの属性が準拠するかどうかを打	皆定してくだ
● 準拠する(⊻)		
○ 準拠しない(N)		
属性の構成(A)		
	OK*	1ンセル

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。

RFC 準拠の VSA の構成	? ×
ベンダが書り当てた属性の番号 ♡2:	
192	
属性の形式(A):	
10 進	T
属性の値(B):	
10	
OK ++>	セル

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。

複数値の属性情報	? ×
属性の名前に	
Vendor-Specific	
属性の番号	
26	
属性の形式	
OctetString	
属性の値(T):	
	上へ(<u>U</u>)
	下へ(D)
	追加(A)
	削除(<u>R</u>)
4	編集(E)
OK	キャンセル

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。

a 🔊 👘 🔽					
サーバー マネージャ (DC)	役割				
 【後書】 【機能 診断 構成 記憶域 	サーバーにインストールされている役割の正常性を表示し、役割や機能を追加または	削除します。			
	○ 役割の概要	🕜 役割の概要ヘルプ			
	⑦ 役割: 6/16 個をインストール済み	■ 【没裏Nの2週加1 ■ 役割の消収余			
	Active Directory ドメイン サービス Active Directory 証明書サービス				
	DHCP サーバー				
	▲ DNS サーバー				
	Web サーバー (IIS)				
	⊕ ネッドノーショネッシーとアッセス サービス				
	 Active Directory ドメイン サービス 	👔 AD DS ヘルプ			
	ディレクトリ データを格納し、ユーザー ログオン処理、認証、ディレクトリ検索など、ユーザーとドメインの通信を管理します。				
	◎ 役割の状態	Contractive Directory ドメイン サービス に移動			
	Jude, 25, tol				
	シリモーン なし システムサービス:8 個が実行中 2 個が停止				
	▲ イベント: 最近 24 時間 に 16 個の警告イベント, 99 個の情報イベント				
		💦 役割サービスの追加			
	役割サービス 状態	語、役割サービスを削除			
	📩 Active Directory ドメイン コントローラ インストール済み				
	UNIX 用 ID 管理 インストールされていません				
	NU0 9 T/T 1 J/X P T/C(1) U U U U				
	パフロード同期 インフトールおれていません				

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。

ネットワーク 3	村リシー サーバー		
771ル(F) 探	1作(A) 表示(V) へ 2 〒	ЛИ-7(H)	
● NPS (□-カ) ■ ■ RADIUS ■ ■ ポリシー ■ 素 ネットワー ■ アカウン:	構成のインボート(D 構成のエクスボート(D NPSサービスの開始 NPSサービスの停止 Active Directory (2	E) (S) (O) サーバーを登録(G)	リシー サーバー (NPS) を使用すると、クライアントの正常性、接続要求の認証、および接続要求 S組織全体のネットワーク アクセス ポリシーを作成わよび強制できます。
	プロパティ(R)		「を選択し、下のリンクをクリックしてシナリオ ウィザードを聞きます。
	表示(V)		
		スットワーク アクセ NPS を NAP ポリシ がネットワークに接続 はそのクライアントを NAP を構成す	【休護(NAP) ・サーバーとして構成する場合、正常性ポリシーを作成し、NAP 対応のウライアントコンピュータ する際には NPS でそのコンピュータを検証するようにしてください。正常性ポリシーに違反した場合 制限付きネットワークに移動し、ポリシーに準拠した状態に自動的に更新することができます。 オる 译録 詳細情報
		詳細な構成	
)		

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。

ネットワーク ポリシー サーバー	×
NPS が Active Directory のユーザーを認証できるようにするには、NPS を実行しているコンピュータが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持っている必要があります。	
ユーザーのダイヤルイン プロパティを win2008-2.com ドメインから読み取る権限をこのコンピュ 一タに与えますか?	
OK キャンセル	

続けて以下が表示されるので、「OK」を押します。

ネットワーク ポリシー サーバー	×
このコンピュータは、ユーザーのダイヤルイン ブロパティを win2008-2.com ドメインから読み取 る権限を取得しました。	
他のドメインに対する権限を取得するには、そのドメインの RAS/NPS サーバー グループのメ ンバにこのコンピュータを登録する必要があります。	
(OK	
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。

サーバー マネージャ						
7ァイル(F) 操作(A) 表示(V) ヘルプ(H)						
■ サーバー マネージャ (DC)	サーバー マネージャ (DC)	サーバー マネージャ (DC)				
■ Total ■ Active Directory ドメインサービス ■ Active Directory 証明書サービス ■ DHCPサーバー ■ DHCPサーバー	このサーバーの状態の概	要の取得、最上位の管理タスクの実行、サーバーの役割	割や機能の追加または削除を行います。			
 Ⅲ 崎 Web サーバー (IIS) □ 🏂 ネットワーク ポリシーとアクセス サービス 	◇ サーバーの概要		🛿 サーバーの概要ヘルプ			
	◆ コンピュータ情報 ライアント レ コンピュータ名・	dc.win2008-2.com	 システム プロパティの変更 ネットワーク接続の表示 リモート デスクトップの構成 			
	アリン・ ローカル エリア接続: リモート デスクトップ: プロダクト ID: □ ログオン特にこのコンソール4	WH2000-2200m 192168200100 有効 92573-082-2500115-76476 :表示しないCD)				
	 セキュリティ情報 Windows ファイアウォール: Windows Update: 	有効 Windows Update を使用して更新プログラムを自 動むにインストールする わし	 			
	日時: 更新プログラムの最終インス トール日時:	なし				
	IE セキュリティ強化の構成 (ESC):	管理者に対して有効 ユーザーに対して有効				
	○ 役割の概要		👔 役割の概要ヘルプ			
	6 最終更新日: 2010/03/29 10:275	0 最新の情報への更新の構成				

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。

名前とアドレスーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー	
フレンドリ名(E):	
	12月100
192.108.200.2	
ペンダー 一般的な RADIUS クライアント用の RADIUS 標準を指定す クライアント ペンダを選択してください。	ちか、一覧から RADIUS
ペンダ名(<u>M</u>):	
RADIUS Standard	*
共有シークレット 共有シークレット 左成] をクリックします。ここに指定した共有シークレットを、RA 時にも指定する必要があります。共有シークレットでは大文字 す。	自動で生成する場合は [DIUS クライアントの構成 と小文字が区別されま
共有シークレット 共有シークレットを直接入力する場合は [手動] をクリックし、 生成] をクリックします。ここに指定した共有シークレットを、RA 時にも指定する必要があります。共有シークレットでは大文字 す。 ・ 手動(U) ・ 生成(G) サキシークレット(S)	自動で生成する場合は [DIUS クライアントの構成 と小文字が区別されま
共有シークレット 共有シークレットを直接入力する場合は [手動] をクリックし、 生成] をクリックします。ここに指定した共有シークレットを、RA 時にも指定する必要があります。共有シークレットでは大文字 す。 ・ 手動(U) ・ 生成(G) 共有シークレット(S):	自動で生成する場合は「 DIUS クライアントの構成 と小文字が区別されま
共有シークレット 共有シークレットを直接入力する場合は [手動] をクリックし、 生成] をクリックします。ここに指定した共有シークレットを、RA 時にも指定する必要があります。共有シークレットでは大文字 す。 ● 手動(<u>U</u>) ● 生成(<u>G</u>) 共有シークレット(<u>S</u>): ●●●●● 共有シークレットの確認入力(O):	自動で生成する場合は [DIUS クライアントの構成 と小文字が区別されま
共有シークレット 共有シークレットを直接入力する場合は [手動] をクリックし、 生成] をクリックします。ここに指定した共有シークレットでは大文字 時にも指定する必要があります。共有シークレットでは大文字 す。 ● 手動(U) ○ 生成(G) 共有シークレット(S): ● ● ● ● ● 共有シークレットの確認入力(Q): ● ● ● ● ●	自動で生成する場合は [DIUS クライアントの構成 と小文字が区別されま
 共有シークレット 共有シークレットを直接入力する場合は [手動] をクリックし、 生成] をクリックします。ここに指定した共有シークレットでは大文字 ・ 手動(U) ・ 手動(U) ・ 生成(G) 共有シークレット(S): ●●●●● 共有シークレットの確認入力(Q): ●●●●● 自物オブション。 	自動で生成する場合は「 DIUS クライアントの構成 と小文字が区別されま

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。

第.サーバー マネージャ	-0-×
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	
♦ ⇒ 2 1 4 1 × 1 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
■ サーバーマネージャ(DC) Users 20 個のオブジェクト [フィルタ アクティブ]	操作
□ シ (2割) □ S Active Directory ドメイン 1 名前 種類 説明	Users 🔺
Active Directory 2 → A	他仍操作
MUOR WINN TALI (FIX OR 3.)	

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。

救生(<u>L</u>):	web	
名(<u>F</u>):		イニシャル(1):
フル ネーム(<u>A</u>):	web	
ユーザー ログオン名	<u>U):</u>	
web	@win	2008-2.com 🔽
ユーザー ログオン名	(Windows 2000 より前)(<u>W</u>):	

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。

パスワード(<u>P</u>):	•••••	_
パスワードの確認入力(の):	•••••	
□ ユーザーは次回ログオン	時にパスワード変更が必要(M)	
ニューザーはパスワードを3	変更できない(<u>S</u>)	
▼ パスワードを無期限にす	<u>ଟ(W)</u>	
アカウントは無効(Q)		

図 5-25 パスワードの設定

(4) 設定の完了

「完了」を押します。

-						
6	作成先:	win2008-	-2.com/User	S		
[完了]を	クリックすると、〉	欠のオブジェク	トが作成されま	tj:		
フルネー	L; web					<u> </u>
ユーザー	ログオン名: we	b@win2008-'	2.com			
パスワート	≪を無期限(こす	3				
						-
						1
			く戻る	5(B)	完了	キャンセル

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。

レサーバー マネージャ					_0
ファイル(F) 操作(A) 表	〒(V) ヘルプ(H)				
🗢 🔿 🖄 📅 🖌 (1 🗙 🖬 🖪 🖻 🛛 🖬				
🚹 サーバー マネージャ (DC	Users 21 個のオブジェクト [フィルタ アクティブ]			操作	
□ 診役割	名前	種類	説明	Users	
E Structure Director	tory 2 -1 Administrator	ユーザー	コンピュータ/ドメインの管理	他の操作	
🖂 🏥 win2008	-2.com	セキュリティ グルー	このグループのメンバはディレ	dot1x	
日 日	n m m m m m m m m m m m m m	2 セキュリティ グル. 2 セキュリティ グル. セキュリティ グル.	このがルークのよりな、ドシ、 DHCP サービスノオレ管理。 DHCP サービスノオレ管理。 DHCP サービスノオレ管理。 DHCP サービスクロレスチュ ドメインの管理者がループ DHCP サーバーなどのおか、 ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ドメインの営業スト ビンターブライズの管理者 このがループのシノパスドメイ。 コンピュージドメインの営業ス このがループのシノパスドメイ。 コンピュージドメインの営業ス	他の持作	

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。

いオブジェクト - グループ	
《作成先: win2008	-2.com/Users
ヴループ名(<u>A</u>):	
WebGroup	
グループ名 (Windows 2000 以前)(M	D:
WebGroup	
┌ グループのスコープ ─────	「グループの種類」
○ ドメイン ローカル(Q)	セキュリティ(S)
 ● グローバル(G) ● ユニバーサル(U) 	○ 配布(<u>D</u>)
	AP721

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。

3月 セッション 般 住所 7 所属するグループ(ー / リモート制御 ターミナル サービスのプロファイル COM+ フリガ ?カウント プロファイル 電話 組織 所属するグループ ダイヤル4 (<u>M</u>):
名前 Domain Users	Active Directory ドメイン サービス フォルダ win2008-2.com/Users
	1
いたようくたい	A DECOMPTION AND A
追加(<u>D</u>)	
<u>追加(D</u>) クライマリ グルーブ	Bupat EV Domain Users
<u>追加(D</u>) プライマリ グループ プライマリ グルー	HIPFILEY Domain Users Omain Users Macintosh クライアントまたは POSDX 対応のアプリケーションがない場合は、プライマリ グループを変更する 必要はありません。
<u>追加(D</u>)… プライマリ グループ プライマリ グルー	HIPFALEY Domain Users Omain Users Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。
<u>追加(D</u>) プライマリ グループ プライマリ グルー	HIPFALEY Domain Users Omain Users Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。

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。

グルーナ の選択	<u>? ×</u>
オブジェクトの種類を選択してください(S):	
リルーフ または ビルトイン セキュリティ フリンソイハル 場所を指定してくださ()(F):	オフジェクトの種類の
win2008-2.com	場所(<u>L</u>)
選択するオブジェクト名を入力してください(例)(E):	
WebGroup	名前の確認(<u>C</u>)
詳細設定(A)	OK キャンヤル

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。

殷 住所 アナ 所属するグループ(<u>№</u>	コウント プロファイル 電話 組織 所属するグループ ダイヤルィ ():
名前	Active Directory ドメイン サービス フォルダ
Domain Users	win2008-2.com/Users
<u>iena(D)</u>	
・ライマリ クルーフ : ブライマリ グルーフ	Domain Users 1の設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。

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。

webのプロパティ	? ×
環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリオ 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤル	げ 化
┌─リモート アクセス許可	
○ アクセスを許可(W)	
○ アクセスを拒否(D)	
○ NPS ネットワーク ポリシーでアクセスを制御(P)	
○ コールバックしない(C)	
○ 呼び出し元による設定 (ルーティングとリモート アクセス サービスのみ)(S)	
○ 常に次の電話番号にコールバック(⊻):	
□ 静的 IP アドレスを割り当てる(1)	
このダイヤルイン接続に対して有効にする IP アド レスを定義してください。 静的 IP アドレス(D	
□ 静的ルートを適用(<u>R</u>)	
このダイヤルイン接続に対して有効にするルートを定 載してください。	
OK キャンセル 適用(<u>A</u>) ヘルプ	

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。

トーバー マネージャ				
イル(F) 操作(A) 表示(V) ヘルプ(H)				
al 🔁 📰 🛛 🔽				
サーバー マネージャ (DC)	ジャ (DC) Active Directory ドメイン サービス			
H Active Directory トメイン リービス FI Active Directory 証明書サービス	ディレクトリデーな友格納し、フーザーログオン処理、認識、ディレクトリ検索など、フーザーとドメインの追	創作を管理します。		
± 🙀 DHCP サーバー				
■ ▲ DNS サーバー				
E 🧤 Web サーバー (IIS) □ 🍈 さットローカ ポリシュトアカセス サードス	○ 欄要			
= € NPS (□-±)				
🗉 🧮 RADIUS クライアントとサーバー	▲ 1ヘント: 最近 24 時間に 16 個の警告1ヘント, 103 個の情報1ヘント	ドレンスを通知		
□ ■ ポリシー	7 119 1/01 B 7/1/3 1/01	•		
「私売要求ホリント」	レベル イベント ID 日付と時刻 ソース 1 70パティ			
1 新規(N)	① 情報 701 2010/03/25 15:29:56 NTDS→ ■ すべてのイベン	トを非表示		
🗉 🎭 ネット 🔍 ルブ(H) 関	① 情報 1869 2010/03/25 15:29:54 Active			
Pカウラフィッシューー	10 指軸 700 2010/03/25 15:29:54 NTDS のはまた 100 0010 /00 /05 15:09:54 NTDS			
120日に	1 情報 1394 2010/03/25 15:15:23 Activ			
構成	()情報 1000 2010/03/25 15:14:53 Activ			
言記憶域	▲警告 2886 2010/03/25 15:14:53 Active			
	① 情報 1004 2010/03/25 15:12:51 Active			
	システム サービス: 8 個が実行中、2 個が停止	1		
	Active Directory Domain Serv ntds 実行中 自 ● 停止			
	💁 DFS Namespace dfs 実行中 自 🕞 開始			
	G DFS Replication dfsr 実行中 自 Ⅰ 再起動			
	Clip Distributed Link Tracking Clie trkwks 1912 7			
	Thersite Messaging ismserv 事行中 自工			
	THERE IS A REAL PROPERTY OF A RE			
	設印第 AD DS ドメイン フルトローラ サービス。20サービスが停止されている場合は、ユーザー は、ネットワークへロケアできません。20サービンが悪効な場合は、明ティがにこれに依存 しているサービス経営部に受きません。			
	○ 役割サービス: 1 個がインストールされています 後割サービスの	kisho		
	(2) 最終更新日: 2010/03/25 15:52:23 最新の情報への更新の構成			

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。

所しいネットワー	ーク ポリシー	×
	ネットワークポリシー名と接続の種類の指定	
	ネットワーク ポリシーの名前およびポリシーを適用する接続の種類を指定できます。	
100		
ポリシー名(4	D:	
WebPolicy		
ーネットワーク接	结心方法	-
NPS (:接続專	************************************	
ヘノダ回有」。	を指定すること/小でですす。 ケアクヤス サーバーの種類(S):	
指定なし		
In		
		1
		1

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。

新しいネットワー	り 税シー 🔀
	条件の指定 接続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なくとも 1 つの条件が必 要です。
条件(<u>C</u>):	
条件	値
条件の説明	
Ŷ	<u>前へ(P)</u> 次へ(N) 完了(E) キャンセル

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。

条件の選択	X
条件を選択し、「追加」をクリックします。	
<u>グループ</u>	-
Windows グループ Windows グループの条件は、接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要が あることを指定します。	
コンピュータグループ コンピュータ グループの条件は、接続するコンピュータが選択したグループのいずれかに属している必要があることを指定しま	
ユーザーグループ ユーザーグループの条件は、接続ユーザーが選択されたグループのいずれかに所属している必要があることを指定します。	
HCAP	
ロケーショングループ HCAP ロケーショングループの条件には、このポリシーに一致するために必要な HCAP (Host Credential Authorization Protocol) ロケーション グループを指定します。HCAP プロトコルは、NPS と一部のサード パーティ製ネットワーク アクセス サーバー (NAS) との間の通信で使用されます。この条件を使用する前に NAS のドキュメントを参照してください。	•

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。

グループ の選択	<u>? ×</u>
オブジェクトの種類を選択してください(S):	
グループ	オブジェクトの種類(の)
場所を指定してください(<u>F</u>):	
win2008-2.com	場所(<u>L</u>)
選択するオブジェクト名を入力してください (<u>例)(E</u>):	
WebGroup	名前の確認(©)
12230 (J. 96) (S. 96)	

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。

/		
)08–2¥WebGro	ир	

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。

所しいネットワー	
	条件の指定 接続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。 少なくとも 1 つの条件が必 要です。
条件(<u>C</u>):	
条件 1110 条件	値
条件の説明: Windows グル	ッーブの条件は、接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要があることを指定しま
₫.	
	[<u>」追加(D)</u>] 編集(E) 削除(B)
	<u> 前へ(P)</u> 次へ(N) 完了(E) キャンセル

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。

新しいネットワー	ーク ポリシー X
	アクセス許可の指定 接続要求がこのポリシーに一致する場合に、ネットワーク アクセスを許可するかまたは拒否するかを構成します。
 ○ アクセスを クライアント ○ アクセスを クライアント □ ユーザー ? クライアント 	許可する(A) ・の接続試行がこのポリシーの条件に一致する場合、アクセスを許可します。 拒否する(D) ・の接続試行がこのポリシーの条件に一致する場合、アクセスを拒否します。 ダイヤルイン プロパティ (NPS ポリシーよりも優先される) によってアクセスを判断する(S) ・の接続試行がこのポリシーの条件に一致する場合、ユーザー ダイヤルイン プロパティに応じてアクセスを許可または拒否します。
	<u> 前へ(P)</u> 次へ(N) 完了(E) キャンセル

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。

新しいネットワーク ポリシー 🛛 🗾 🛛 🗾 🗾
認証方法の構成 接続要求がこのポリシーの条件を満たすために必要な認証方法を、1 つ以上指定してください。EAP 認証には、EAP の 種類を指定する必要があります。NAP を使用する 8021Xまたは VPN を展開する場合は、接続要求ポリシーに採展され た EAP を指定する必要があります。接続要求ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。
EAP の種類(I): 上へ移動(U) 定人移動(U) 下へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「市へ移動(D) 「「「「「「」」」」 「「「」」」 「「」」」 「「」」」 「」 「「」」」 「」<
前へ(P) 次へ(N) 完了(E) キャンセル

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。

新しいネットワー	-ウ ポリシー <u>×</u>
	制修りの構成 制約は、接続要求が一致する必要がある、ネットワーク ポリシーの追加パラメータです。接続要求が制約と一致しない場 合、NPS は接続要求を自動的に拒否します。制約はオブションです。制約を構成しない場合は、じたへ」をクリックしてくだ さい。
このネットワーク すべての制約功 制約(S): 割約	 カボジーの車路1を構成します。 ウイムアウト ウタイムアウト キャノー・がアイドル状態になってから接続が切断されるまでの最大時間を分単位で指定します ・レタイムアウト ま、ID ・日の種類

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。

新しいネットワーク ポリシー	×
おりシーのすべてのネ	ットワーク ポリシー条件および制約が一致した場合、NPS は接続要求に対して設定を適用します。
このネットワーク ポリシーの設定を構成 条件と制約が接続要求に一致してアク	します。 クセスが許可される場合、この設定が適用されます。
RADILS <u>属性</u>	道加属性を RADIUS クライアントに送信するには、ペンダ固有の属性を選択し、[編集] をク リックします。属性を構成しないと、属性は RADIUS クライアントに送信されません。必要な 属性については、RADIUS クライアントのドキュメントを参照してください。 属性(1): 名前 ペンダ 値
2 12 設定	
	前へ(P) 次へ(N) 完了(E) キャンセル

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。

ベンダ固有の	禹性の追加	×
属性を設定に	:追加するには、属性を選択し、[追加] をクリックし	てください。
一覧にないべ べンダ(V):	ンダ固有の属性を追加するには、「カスタム」を選択	(し、「)自加] をクリックしてください。
カスタム		v
属性(<u>B</u>):		
名前		
訳19月 :		

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。

属性の情報			×
属性名: Vendor-Spec	ific		
属性の番号: 26			
属性の形式: OctetString			
属性値(丁):			
ベンダ	値		追加(<u>A</u>)
			編集(E)
			削除(<u>R</u>)
			上へ移動(山)
			下へ移動(<u>D</u>)
		ОК	キャンセル

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。

ベンダ固有の属性情報		×
属性名(工): ベンダ固有		
ネットワーク アクセス サーバーのベン	ダを指定してください。	
○ 一覧から選択する(S):	RADIUS Standard	-
● ベンダコードを入力する(E):	278	÷
RADIUS RFC のベンダ固有の属性 かを指定してください。	自に関する仕様にこの属性が準拠	<u>u</u> するかどう
● 準拠する(Y)		
○ 準拠しない(N)		
属性の構成(<u>A</u>)		
	OK +	ャンセル

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。

ベンダが割り当てた属性の番号(V): 192	
1.2.7.7.	
属性の形式(A):	
10 進数	_
属性値(<u>B)</u> :	
100	1

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。

属性の情報	×
属性名: Vendor-Specific	
属性の番号: 26	
属性の形式: OctetString	
属性値(<u>T</u>):	
べンダ 値	追加(<u>A</u>)
<u>ベンダコード: 278 100</u>	編集(E)
	上へ移動(山)
	下へ移動(D)
0	K

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。

ホリシーのすべしの。 このネットワークポリシーの設定を構 条件と制約が接続要求に一致して)	ペットワーク ボッシー染件および制品が一致した場合、NPS は接続要求に対して設定を運用します。 成します。 ックセスが許可される場合、この設定が適用されます。
 設定(S): RADILS 属性 標準 ベング固有 ネットワークアクセス保護 NAP 強制 拡張状態 	追加属性を RADIUS クライアンドに送信するには、ペンダ固有の属性を選択し、[編集] をク リックします。属性を構成しないと、属性は RADIUS クライアンドに送信されません。必要な 属性については、RADIUS クライアントのドキュメントを参照してください。 属性(①): 名前 ペンダ 値
ルーティングとリモートアクセ マルチリンクおよび帯域 幅割り当てフロトコル (BAP) F フィルタ 義 暗号化	Vendor-Specific RADIUS Standard 100
☑ IP 設定	

図 5-49 設定の構成

「OK」を押します。

Poli	cyのプロパティ	
要	条件 制約 設計	
.のネ	ットワーク ポリシーの条(牛を構成します(℃)
2件力	が接続要求と一致する	場合、NPS はこのポリシーを使用して接続要求を承認します。条件が接続要求と一致しない場合、NPS はこのポリ
/-ह	:スキップし、他にポリシー	が構成されている場合は、それらのポリシーを評価します。
		値
10	Windows グループ	WIN2008-2¥WebGroup
:件()	DII兑8月:	
indo	wws グループの条件は、	接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要があることを指定します。
_		

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。

次のネットワーク ポリシーが正常に作成されまし WebPolicy ポリシー条件: 条件 例indows グループ Windows グループ	სt≂
次のネットワーク ポリシーが正常に作成されまし WebPolicy ポ リシー条件: 条件 「Windows グループ WIN2008-2¥WebGroup	ut:
WebPolicy ポリシー条件: 条件 値 Windows グループ WIN2008-2¥WebGroup	,
ボリシー条件 : 条件 値 Windows グループ WIN2008-2¥WebGroup)
条件 値 Windows グループ WIN2008-2¥WebGroup	3
Windows グループ WIN2008-2¥WebGroup)
*リシー詩定:	
約シー設定: 条件	値
約シー設定: 条件 認証方法	値 暗号化されていない認証 (PAP、SPAP)
ポリシー設定: 条件 認証方法 アクセス許可	値 暗号化されていない認証 (PAP、SPAP) アクセスを許可する
ドリシー設定: 条件 認証方法 アクセス許可 非準拠クライアントの更新	値 暗号化されていない認証 (PAP、SPAP) アクセスを許可する True
ポリシー設定: 条件 認証方法 アクセス許可 非準拠クライアントの更新 NAP 強制	値 暗号化されていない認証 (PAP、SPAP) アクセスを許可する True 完全なネットワーク アクセスを許可する
秋リシー設定: 条件 認証方法 アクセス許可 非準拠クライアントの更新 NAP 強制 Framed-Protocol	値 暗号化されていない認証 (PAP、SPAP) アクセスを許可する True 完全なネットワーク アクセスを許可する PPP
秋リシー設定: 条件 認証方法 アクセス許可 非準拠クライアントの更新 NAP 強制 Framed-Protocol Service-Type	値 暗号化されていない認証 (PAP、SPAP) アクセスを許可する True 完全なネットワーク アクセスを許可する PPP Framed

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。

第.サーバー マネージャ				- 🗆 ×
🗢 🔿 📶 🔣 🖬				
サーバーマネージャ(DO) 日 投稿 日 人名tive Directory F3メ(ンサービス 日 人名tive Directory F3メ(ンサービス 日 DN5 サーバー 日 DN5 サーバー 日 DN5 サーバー 日 MACtive Directory F3メ(ンサービス 日 DN5 サーバー 日 MACtive Directory F3メ(ンサービス 日 MACtive Directory F3メ(ンサービス 日 MACtive Directory F3メ(ンサービス 日 MACtive Directory F3メ(D)・ 日 Active Directory F3メ(D)・ 日 MACtive Directory F3×(D)・ 日 MAC	ネットワーク ポリシーでは、ネットワークへの接続を計与す ーザーがネットワークに接続できる状況と接続できないな ポリシー名。 パージーがネットワークに接続できる状況と接続できないな がしたり。 パージーがネットワークに接続できる状況と接続できないな WebPolicy パージーングとリモート アクセス サーバーへの接続 パージーングとリモート アクセス サーバーへの接続 パージーングとリモート アクセス サーバーへの接続 パージーングとリモート アクセス サーバーへの接続 パージーング サーバーへの接続 パージーング サーバーへの接続 パージーング サーバーへの接続 パージーング サーバーへの接続 パージーング サーバーへの接続 パージーング サーバーへの接続 パージーン WIN2008-24WebCaroup パージーン WIN2008-24WebCaroup パージーン WIN2008-24WebCaroup パージーン アクレン フロバラーを振行すり パージーン プロバラーを振行すり アクレン フロバラーを振行する パージー ジョン アルイン フロバラーを振行する パージー ジョン アルイン フロバラーを振行する	るユーザーと、これらのユ 況を指定できます。	操作 ネットワーク ポリシー 新規 一覧のエクスポート 表示 ④ 最新の情報に更新 2 ヘリレフ	•

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。

ファイル(F) 操作(A) 表示(V) ヘルブ(H)		
🗢 🤿 🖄 💼 🖬		
🏊 サーバー マネージャ (DC)	接続要求ポリシー	操作
□ 診 役割 ■ 第 Active Directory KMインサービス		接続要求ポリシー
 ● Active Directory 証明書サービス ● DHCP サーバー ● DHCP サーバー ● DNS サーバー 	日本1000000000000000000000000000000000	新規 - 一覧のエクスポート
■ 戦 Web サーバー (IIS)	「すべて」 削除(L) 「を使用 有効 1 指定なし	- 表示
□	名前の変更(M) ポリシーの創動(C)	最新の情報に更新
🗉 🧮 RADIUS クライアントとサーバー	プロパティ(R)	
□ 」「ポリシー ◎ 椿続要求ポリシー	ヘルプ(H)	すべてのユーザーに Windows 認証を使用
🧧 ネットワーク ポリシー		上へ移動
正常性ポリシー 田 14 ネットワーク アクセス保護		下八移動
🦷 アカウンティング	🧾 すべてのユーザーに Windows 認証を使用	無効にする
 ■ 西川 100000 ■ 100000 	条件 - 次仍条件を満たして()る場合:	前服余
E		名前の変更
	条件 1000-24:00 月曜日 00:00-24:00 火曜日 00:00-24:00 火曜日 00:00-2…	ポリシーの複製
		プロパティ
		2 NH7
	設定 - 次の設定が適用されます:	
	認証プロバイダ ローカル コンピュータ	
	拡張認証プロトコル メソッド Microsoft: 保護された EAP (PEAP) 認知すたは FAP または 暗号化されていたい認知 (PAP SPAP)	
	記記証を無視する 有効	
		-1
		-

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。

すべてのユーザーに Windows 認証を使用のプ	ロパティ	×
概要 条件 設定		
このネットワークポリシーの設定を構成します。 条件と制約が接続要求に一致してアクセスが許 設定(S): 必要な認証方法	可される場合、この設定が適用されます。 ☞ ネットワーク ポリシーの認証設定よりも優先する(①)	_
 	ネットワーク ポリシーの制約および認証設定の代わりに、以下の認証設定を使用します。 VPN 接続、および NAP を使用する 802.1X 接続の場合は、PEAP 認証を構成する必要があります。	
 Pカウンティング <u>領域名の指定 </u> 属性 	EAP の種類は、NPS とりライアントとの間で、表示されている順序でネゴシェートされます。 EAP の種類(1):	
RADILS 局性	Microsoft 1米護された EAP (PEAP) ・ ・ 上へ移動(①) 下へ移動(①)	
	道加(A) 編集(E) 問則除(E) セキュリティ レベリルの低い認証方法: Microsoft 暗号化認証ガージョン 2 (MS-CHAP v2)(y) 「パスワードの専期限が切れた後も、ユーザー(こパスワードの変更を許可する(H) Microsoft 暗号化認証 (MS-CHAP)(y) 『パスワードの専期限が切れた後も、ユーザー(こパスワードの変更を許可する(S) 暗号化認証 (CHAP)(Q) 呼号化に認証 (CHAP)(Q) 呼号化されていない認証 (PAP、SPAP)(S) 認証方法をネゴシエートせずにクライアンドに接続を許可する(L)	
	OK キャンセル 道用)(A)

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。



「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。

システムのプロパティ	X
コンピューター名 ハードウェア	詳細設定 システムの保護 リモート
次の情報は、この	コンピューターをネットワーク上で識別するために使われます。
コンピューターの説明(<u>D</u>):	1
	例: "キッチンのコンピューター"、"仕事用コンピューター"
フル コンピューター名:	windows7-pc
ワークグループ:	WORKGROUP
ドメインまたはワークグループにき するには [ネットワーク ID] をク	参加するためのウィザードを使用 リックしてください。
コンピューター名を変更したりド 更] をクリックしてください。	らインに参加したりするには 「変 変更(C)…
	OK キャンセル 適用(A)

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。

コンピューター名/ドメイン名の変更
このコンピューターの名前とメンバーシップを変更できます。変更により、ネット ワークリソースへのアクセスに影響する場合があります。 <mark>詳細情報</mark>
コンピューター名(<u>C</u>): windows7-pc
フル コンピューター名: windows7-pc 詳細(M)
所属するグループ ● ドメイン(D): win2008-2
◎ ワークグループ(<u>W</u>): WORKGROUP
OK キャンセル

「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。

Windows セキュリ	
コンピューター ドメインに参加 ワードを入力し	名/ドメイン名の変更 するためのアクセス許可のあるアカウントの名前とパス てください。
	web ●●●●●●●●● ドメイン: win2008-2
	OK キャンセル

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。

コンピューター名/ドメイン名の変更
() win2008-2 ドメインへようこそ。
ОК

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。

web
別のドメインにログオンするには
ユーザーの切り替え(<u>W</u>)
See Windows ⁻ 7 Professional

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。

瓢 サーバー マネージャ	
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	
■ サーバー マネージャ(DC) Users 20 個のオブジェクト [フィルタ アクティブ]	操作
□ ● ② 役割 □ ◎ Active Directory Kdイン1 名前 種類 説明	Users 🔺
● Matter Directory F×/ン+ 経営 推理 189月 ● Administrator 2-ザ コンピューダ/ドメインの管理 このガルーブのシンパは、ドメ ● Baltin Baltin Computers このガルーブのシンパは、ドメ ● Computers BDPP Administrator 2-ザ コンピューダ/ドメインの管理 ● Domain Contre BDPP Administrator このガルーブのシンパは、ドメ ● Computers BDPP Administrator こやすコリティグル このガルーブのシンパは、ドメ ● Computers BDPP Administrator こやすコリティグル DHOP サージにははあっ ● Foreignesson BDPA Administrator こやすコリティグル DHOP サージになけはあっ ● Active Director BMB/D 等にない Put-Vort Administrator Put-Vort Administrator ● Active Director BMB/D 等にない Put-Vort Administrator Put-Vort Administrator Put-Vort Administrator ● Active Director Bort Administrator Put-Vort Administrator Put-Vort Administrator Put-Vort Administrator ● Active Director Bort Administrator Put-Vort Administrator Put-Vort Administrator Put-Vort Admini	Users A
新しいオブジェクトを作成します。	

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。

效生(<u>L</u>):	dot1×			
名(<u>F</u>):			イニシャル(①:	
フル ネーム(<u>A</u>):	dot1x			
ユーザー ログオン名(<u>U</u>):			
dot1x		@win2008	-2.com	•
ユーザー ログオン名	(Windows 2000 J	:り前)(<u>W</u>):		
WIN2008-2¥		dot1x		

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。

パスワード(<u>P</u>):		******		
パスワードの確認入力(<u>_</u> :	******	•	
ニ ユーザーは次回ログ	オン時にパスワード家	変更が必要(<u>M</u>)		
ニューザーはパスワー	"を変更できない(<u>S</u>))		
▼ パスワードを無期限	(こする(W)			
■ アカウントは無効(0))			

図 5-63 パスワードの設定

(4) 設定の完了

「完了」を押します。

しいオブジ	፤ ታት - ኋ-ሣ	_			2
8	作成先:	win2008-2	.com/Users		
[完了] を	をクリックすると、パ	マのオブジェクトオ	が作成されます:		
フルネー	-7: dot1x				<u>_</u>
ユーザー	- ログオン名: dot	1×@win2008-:	2.com		
パスワー	ドを無期限にする	5			
					_
			< 戻る(<u>B</u>)	完了	キャンセル
			19. 	- W	

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。

ファイル(F) 操作(A) 表:	〒(V) ヘルプ(H)				
🧇 🔿 🖄 📅 🖌 🕻) 🗙 🖸 o 🍙 🛛 🖬				
27/1/LF) 操作(A) 後 1 マス-ジャ(D) - マス-ジャ(D) マス-ジャ(D) マス-ジャ(D) マス-ジャ(D) 	(ドメイン・ (ドメーン・ (ドン・ (ドン・ (ドメーン・)) (ドン・ (ドン・ (ドン・)) (ドン・ (ドン・)) (ドン・ (ドン・ (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ドン・)) (ド・))	エクト 101 <th>説明 ンピューダ/ドメインの管理。 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 DHOP サージンズ対し管理。 DHOP サージンズ対し管理。 FXインの管理 ディンの管理者 ログワ サーバーなどのほか… FXインの管理者 ログワループのシンパは、ドメー、 ログワループのシンパは、ドメー、 ログリーブーンのサーバーはユ、 ログリーブのサーバーにはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーは里者</th> <th>他の操作を 他の操作を</th> <th>-</th>	説明 ンピューダ/ドメインの管理。 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 ログループのシンパは、ドメ、 DHOP サージンズ対し管理。 DHOP サージンズ対し管理。 FXインの管理 ディンの管理者 ログワ サーバーなどのほか… FXインの管理者 ログワループのシンパは、ドメー、 ログワループのシンパは、ドメー、 ログリーブーンのサーバーはユ、 ログリーブのサーバーにはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーはユ、 ログリーブのサーバーは里者	他の操作を 他の操作を	-
<	E				

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。

🧏 作成先: win2008	3-2.com/Users
グループ名(<u>A</u>):	
1×Group	
グループ名 (Windows 2000 以前)(⊻	Ø:
1xGroup	
_ วัน–วํดุุุ่ม–วํ	「グループの種類
○ ドメイン ローカル(Q)	 セキュリティ(S)
● グローバル(<u>G</u>)	○ 配布(D)
○ ユニバーサル(<u>U</u>)	

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。

lot1xのプロパティ	<u>?</u>	×
環境 セッション 全般 住所 アカ	リモート制御 │ ターミナル サービスのプロファイル │ COM+ │ フリガナ ウント│プロファイル│電話 │組織 ─所属するグループ │ダイヤルイン	1
所属するグループ(<u>M</u>)):	
名前 Domain Users	Active Directory ドメイン サービス フォルダ win2008-2.com/Users	
追加(<u>D</u>)	削除(尺)	
ブライマリクループ:	Domain Users	
プライマリ グループ	の設定(S) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する	
	心安はめりません。	

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。

グループ の選択	<u>? ×</u>
オブジェクトの種類を選択してください(<u>S</u>):	
グループ または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(Q)
場所を指定してください(E):	
win2008-2.com	場所(<u>L</u>)
選択するオブジェクト名を入力してください(例)(E):	
1xGroup	名前の確認(C)
a succession	
No. and a second s	

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。

IXWJU/\JY	<u>?</u>]
環境 │ セッション 診験 │住所 │ アナ	│ リモート制御 │ ターミナル サービスのプロファイル │ COM+ │ フリガナ コウント │ プロファイル │ 電話 │ 組織 ─ 所属するグループ │ダイヤルイン 0、
「個9のクルース」	ア Active Directory ドメイン サービス フォルダ
1xGroup	win2008-2 com/Users
Domain Users	win2008-2.com/Users
	<u>肖۱除(E)</u>
プライマリ グループ:	Domain Users
プライマリ グループ: ブライマリ グルーつ	Domain Users 7の設定(8) Macintosh クライアントまたは POSIX 対応のアプリケ ーションがない場合は、プライマリ グループを変更する 必要はありません。

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。

dot1xのプロパティ ?	×
環境 セッション リモート制御 ターミナル サービスのプロファイル COM+ フリガナ 全般 住所 アカウント プロファイル 電話 組織 所属するグループ ダイヤルイン	1
© <u>アクセスを許可(W)</u>	
 ○ アクセスを拒否(D) ○ NPS ネットワーク ポリシーでアクセスを制御(P) 	
□ 発信者番号を確認(⊻):	
 ○ コールバックしない(○) ○ 呼び出し元による設定 (ルーティングとリモート アクセス サービスのみ)(S) 	
○ 常に次の電話番号にコールバック(⊻):	
静的 IP アドレスを割り当てる(1) このダイヤルイン接続に対して有効にする IP アド レスを定義してください。 静的 IP アドレス(1)…	
■ 静的ルートを適用(R) このダイヤルイン接続に対して有効にするルートを定 載してください。	
OK キャンセル 適用(<u>A</u>) ヘルブ	

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。

		_
ル(F) 操作(A) 表示(V) ヘルプ(H)		
a 🔁 📅 🖬		
ナーバー マネージャ (DC)	Active Directory ドメイン サービス	
P (2番) S Active Directory ドメイン サービス B Active Directory 説明書サービス B DHCP サーバー B DNS サーバー B DNS サーバー B M Web サーバー B A Sh7D-ク ポリシーとアクセス サービス	ディレクトリ データを格納し、ユーザーログオン処理、認証、ディレクトリ検索など、ユーザーとドメインの適信を管理	します。
 ・ ・ ・	⊙ 🔒 イベント: 最近 24 時間 に 16 個の警告イベント、103 個の情報イベント 📻 イベント ビューアに移動	
	7 119 1 NON	
■ 接続要求ポリシー た <u>⇒k□=5 批(S)</u> = 新規(N)	レベル イベント 1D 日付と時刻 ソース▲ ③ 体報 701 2010/03/25 15:29:56 NTDC- ■ すべてのイベントを非表示	ŧ
田 🎥 ネット ヘルブ(日) 豊	① 情報 1869 2010/03/25 15:29:54 Activi ① 情報 700 2010/03/25 15:29:54 NTDS	
■ 標能 = 2005	① 情報 102 2010/03/25 15:29:54 NTDE	
ason 補成	1 194世 1394 2010/03/20 15:15:23 Activi () 情報 1000 2010/03/25 15:14:53 Activi	
言記憶域	A 警告 2886 2010/03/25 15:14:53 Activ	
	G 1 1004 2010/03/25 15:12:51 Actrw.▲	
	 システムサービス:8 個が実行中、2 個が停止 ペ、サービスに移動 	
	表示名 サービス名 状態 ス 📓 基本設定	
	Active Directory Domain Serv ntds 実行中 自 ● 停止 の DES Namesesse dfa 事行中 自	
	DFS Renlication dfsr 里行中 自	
	② Distributed Link Tracking Clie trkwks 停止 手	
	🤹 File Replication ntfrs 停止 手	
	Intersite Messaging ismserv 軍行中 自工	
	記9月 AD DSドメインコントローラサービス。このサービスが停止されている場合は、ユーザー は、ネットワークハログオンできません。このサービスが無効な場合は、明元6%にこれに依存 しているサービスを開始できません。	
	🔇 最終更新日: 2010/03/25 15:52:23 最新の情報への更新の構成	

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。

しいネットワーク ポリシー	×
ネットワークポリシー名と接続の種類の指定	
ネットワーク ポリシーの名前およびポリシーを適用する接続の種類を指定できます。	
ボリシー名(<u>A</u>): 1xPolicy	
なットワーク接続の方法	
NPS に接続要求を送信するネットワーク アクセス サーバーの種類を選択してください。 ネットワーク アクセス サーバーの種類を選択 ペンダ同有1 を指定する、とができます。	でするか、[
● ネットワーク アクセス サーバーの種類(S):	
指定なし 🔽	
○ べンダ固有(1):	
10 ===	
前へ(P) 次へ(N) 完了(P) 年	のセル

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。

新しいネットワー	り ポリシー 🗾
	条件の指定 接続要求に対してこのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。 少なくとも 1 つの条件が必 要です。
条件(<u>C</u>):	
条件	値
条件の説明	
	<u>前へ(P)</u> 茨へ(N) 完了(E) キャンセル

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。

条件の選択	×
条件を選択し、「追加」をクリックします。	1000
接呼 端末 ID 狭呼端末 ID の条件には、ネットワーク アクセス サーバー (NAS) の電話番号を文字列で指定します。パターン マッチングの 構文を使用して市外局番を指定できます。	
NAS ID NAS ID の条件は、ネットワーク アクセス サーバー (NAS)の名前である文字列を指定します。 パターン マッチ構文を使用し て NAS 名を指定できます。	
NAS IPv4 アドレス NAS IP アドレスの条件は、NAS の IP アドレスである文字列を指定します。パターン マッチ構文を使用して IP ネットワーク を指定できます。	
NAS IPv6 アドレス NAS IPv6 アドレスの条件は、NAS の IPv6 アドレスである文字列を指定します。パターン マッチ構文を使用して IPv6 ネットワークを指定できます。	
NAS ボートの種類 NAS ボートの種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート、ネットワーク、IEEE 802.11 ワイヤ レス、およびイーサネット スイッチなど、アクセス クライアントが使用するメディアの種類を指定します。	•
<u>追加(D)</u> キャンセル	

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。

NAS ボートの種類	×
このポリシーに一致するために必要なアクセス メディアの種類を指定します。 一般的なダイヤルアップおよび VPN トンネルの種類(<u>D</u>)	
 □ ISDN 同期 □ 仮想 (VPN) □ 同期 (T1 回線) □ 非同期 (モデム) 	
一般的な 802.1X 接続トンネルの種類(X)	
🗖 FDDI	
 ✓ イーサネット □ トークン リング □ ワイヤレス - IEEE 802.11 	
その他(①	
ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-DMT - Asymmetric DSL Discrete Multi-Tone G3 Fax	
OK キャンセル	

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。

	ーク ポリシー	
	接続要求に対してこのネットワーク ポリシーを評価するかとうかを決定す 要です。	「る条件を指定します。少なくとも 1 つの条件が必
条件(<u>C</u>):	1.24	1
	10 ドートの種類 イーサネット	
I		
100000000000000000000000000000000000000		
条件の説明: NAS ポートのi	播類の条件は アキロガ雷託回線 ISDN トルネルまたは仮相づうイベート	ネットワーク IEEE 80211 ワイヤレス およびイーサ
条件の説明: NAS ポートの: ネット スイッチវ	種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート など、アクセス クライアントが使用するメディアの種類を指定します。	ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ
条件の説明: NAS ポートの ネット スイッチ	種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート など、アクセス クライアントが使用するメディアの種類を指定します。 「	ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ
条件の説明: NAS ポートの ネット スイッチ?)種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート など、アウセス クライアントが使用するメディアの種類を指定します。 [ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ 追加(D) 編集(E) 削除(B)
条件の説明: NAS ポートの ネット スイッチ)種類の条件は、アナログ電話回線、ISDN、トンネルまたは仮想プライベート など、アクセス クライアントが使用するメディアの種類を指定します。 [ネットワーク、IEEE 802.11 ワイヤレス、およびイーサ 道加(<u>D</u>) 編集(<u>E</u>) 削除(<u>R</u>)

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。

バルーナ	9
1	Windows グループ Windows グループの条件は、接続ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要が あることを指定します。
	コンピュータグループ コンピュータ グループの条件は、接続するコンピュータが選択したグループのいずれかに属している必要があることを指定しま
1 2	ユーザーグループ ユーザーグループの条件は、接続ユーザーが選択されたグループのいずれかに所属している必要があることを指定します。
HCAP	
	ロケーション グループ HCAP ロケーション グループの条件には、このポリシーに一致するために 必要な HCAP (Host Credential Authorization Protocol) ロケーション グループを指定します。HCAP プロトコルは、NPS と一部のサード パーティ製ネットワーク アクセス サーバー (NAS) との間の通信で使用されます。この条件を使用する前に NAS のドキュメントを参照してください。

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。

ブンゴントの理想を選択していたさいした。 グループ	オブジェクトの種類(<u>O</u>)
易所を指定してください(E):	
win2008-2.com	場所(」)
羀択するオブジェクト名を入力してください (<u>例)(E</u>):	
璧択するオブジェクト名を入力してください (<u>例)(E</u>): 1×Group	名前の確認(2)

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。

グループ			
WIN2008-2¥	1xGroup		

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。

もしいネットワーク	ナポリシー	×
	条件の指気 接続要求に対 要です。	- ここのネットワーク ポリシーを評価するかどうかを決定する条件を指定します。少なくとも 1 つの条件が必
条件(<u>C</u>):		
条件		値
🥣 NAS ポー	トの種類	イーサネット
Windows	グループ	WIN2008-2¥1×Group
条件の説明: Windows グルー す。	一プの条件は、接	売ユーザーまたは接続コンピュータが選択されたグループのいずれかに所属している必要があることを指定しま
		<u>〕追加(D)</u> 編集(E)
		前へ(P) 次へ(N) 完了(F) キャンセル

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。

新しいネットワ・	ーク ポリシー <u>×</u>
	アクセス許可の指定 接続要求がこのポリシーに一致する場合に、ネットワーク アクセスを許可するかまたは拒否するかを構成します。
 ○ アクセスを クライアント ○ アクセスを クライアント □ ユーザー・ クライアント 	許可する(A) ・の接続試行がこのポリシーの条件に一致する場合、アクセスを許可します。 拒否する(D) ・の接続試行がこのポリシーの条件に一致する場合、アクセスを拒否します。 ダイヤルイン プロパティ (NPS ポリシーよりも優先される) によってアクセスを判断する(S) ・の接続試行がこのポリシーの条件に一致する場合、ユーザー ダイヤルイン プロパティに応じてアクセスを許可または拒否します。
	前へ(P) 次へ(N) 完了(E) キャンセル

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。

認証方法の構成 認証方法の構成 接換要求がこのポリシーの条件を満たすために必要な認証方法を、1 つ以上指定してください。EAP 認証には、EAP の 推算を指定する必要があります。NAP を使用する 8021X または VPN を展開する場合は、接換要求ポリシーに(保護され た EAP を指定する必要があります。接換要求 ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。 EAP の種類(1): 上へ移動が(0): 「方へ移動(0): 上へ移動(0): 「適加(A) 編集(f) 「別除(P): 上へ移動(0): 「方へ移動(0): 下へ移動(0): 「方へ移動(0): 下へ移動(0): 「方へ移動(0): 下へ移動(0): 「方へ移動(0): 「小谷動(0): 「方へ移動(0): 「小谷動(0): 「ク、「お動(0): 「小谷動(0): 「ないのの低い認証方法: 「別除(P): 「ク、「お動(1): 「上へ移動(0): 「方へ移動(0): 「おけっくしたいの(1): 「 「おりう・したいの(1): 「 「「「「」」」」」」」」」」」」」」」」 「 「 「 「 」」」」」」」」」」」」」」」」」」」 「 「 」 「 へたいの(1): 「 」 「 」 」」」」」」」」」」」」」」」」」」」」 「 」 「 」 」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	新しいネットワーク ポリシー	×
EAP の種類は、NPS とクライアントとの間で、表示されている順序でネゴシェートされます。 EAP の種類(T): 上へ移動(U) 下へ移動(D) 注意加(A). 循葉(E). 育即除(P) セキュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証バージョン 2 (MS-CHAP v2)(V) ダ /パスワードの期限が切れた後も、ユーザー(こパスワードの) ✓ Microsoft 暗号化認証 (MS-CHAP(Y)) ✓ パスワードの期限が切れた後も、ユーザー(こパスワードの) ● 暗号化認証 (CHAP)(G) 暗号化記録証 (CHAP)(G) 暗号化に認証 (CHAP)(G) 電号化に認証 (CHAP)(G) 電台水1(C) ない認証 (CHAP)(G) 電台水1(C) ない認証 (CHAP)(G) (MC< キャンセル	認証方法の構成 接続要求がこのポリシーの条件を満たすために 種類を指定する必要があります。NAPを使用 た EAP を指定する必要があります。接続要求	必要な認証方法を、1 つ以上指定してください。 EAP 認証には、 EAP の する 8021Xまだは VPN を展開する場合は、 接続要求ポリシーに保護され ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。
道力加(A) 無集(E) 町野余(R) 芝生ュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証バージョン 2 (MS-CHAP v2)(V) グ パスワードの期限が切れた後も、ユーザー(こパスワードの) Microsoft 信号化認証(MS-CHAP)(Y) Microsoft 保護されたパスワード (EAP-MSCHAP v2) グ パスワードの期限が切れた後も、ユーザー(こパスワードの) 暗号化認証(CHAP)(C) Microsoft 保護されたパスワード (EAP-MSCHAP v2) 管号化だ和E(CHAP)(C) Microsoft セキュリティで(保護されたパスワード (EAP-MSCHAP v2) ご該証方法をネゴシエートせず(こクライアントに接続を許可する) OK キャンセル	EAP の種類は、NPS とクライアントとの間で、表示されている順序 EAP の種類(T):	Fでネゴシエートされます。 <u> 上へ移動(U)</u> 下へ移動(D)
	ighn(A) 編集(E) 前期余(R) セキュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証レパージョン 2 (MS-OHAP v2)(V) ✓ パスワードの期限が切れた後も、ユーザー(こパスワードの): ✓ Microsoft 暗号化認証 (MS-OHAP)(Y) ✓ パスワードの期限が切れた後も、ユーザー(こパスワードの): F 常月に認証 (OHAP)(C) 暗号化と認証 (OHAP)(C) F 暗号化と記証 (OHAP)(C) 記証方法をネゴシエートせず(こクライアントには続を許可する コンピュータの正常性チェックのみを実行する(F)	EAP の追加 認証方法(A): Microsoft スマートカードまたはその他の証明書 Microsoft 保護された EAP (PEAP) Microsoft セキュリティで(保護されたパスワード (EAP-MSCHAP v2)

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。

新しいネットワー	り ポリシー 🛛 🛛 🗾 🛛 🗾
	認証方法の構成 接続要求がこのポリシーの条件を満たすために必要な認証方法を、1 つ以上指定してください。 EAP 認証には、EAPの 種類を指定する必要があります。 NAP を使用する 802.1X または VPN を展開する場合は、接続要求ポリシーに保護され た EAP を指定する必要があります。 接続要求ポリシーは、ネットワークポリシーの認証設定よりも優先されます。
EAP の種類は、 EAP の種類(1)	NPS とクライアントとの間で、表示されている順序でネゴシェートされます。 D:
i追加(A) i追加(A) セキュリティレ マ パスワー マ パスワー 「 暗号化記题 同 暗号化記题 同 記証方法を コンピュータの	上へ移動(D) 講菜(E) 前野余(B) 下へ移動(D) 下へ移動(D) 「小和動(D) 「小和しい(C) 「小和しい(C) 「いれ(D) 「いれ(D) 「小和しい(D) 「小和しい(D) 「小和しい(D) 「小和し(D) 「小和し(D) 「小和し(D) 「小和し(D) 「小和し(D)
	<u> 前へ(P)</u> 次へ(N) 完了(E) キャンセル

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。

ましいネットワーク ポリシー 認証方法の構成	<u>×</u>	」 通信を智
接続要求がこのポリシーの線 種類を指定する必要があり た EAP を指定する必要がす	を件を満たすために必要な認証方法を、1 つ以上指定してください。EAP 認証には、EAP の ます。NAP を使用する 802.1X または VPN を展開する場合は、接続要求ポリシーに保護され がます。接続要求ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。	
EAP の種類は、NPS とクライアントとの間で、新	表示されている順序でネゴシエートされます。	-ア(ご移動
EAP の種類(T):	呆護された EAP プロパティの編集	×
Microsoft: 1未該された EAP (PEAP) ji自加(A) 編集(E) 削助余(セキュリティ レベルの低い認証方法: 「 Microsoft 暗号化認証パージョン 2 (M: マ パスワードの期限が切れた後も、ユー 「 Microsoft 暗号化認証(MS-CHAP)() マ パスワードの期限が切れた後も、ユー 暗号化認証(MS-CHAP)() 暗号化認証(MS-CHAP)()	クライアントに対して、サーバーがその ID の証明をするための証明書を選択してください。接続 要求ポリシーにおいて、保護された EAP のために構成された証明書は、この証明書より優先されます。 証明書の発行先():	
 □ 暗号化されていない認証(PAP、SPAP □ 認証方法をネゴシエートせずにクライアン □ コンピュータの正常性チェックのみを実行 	j追tu(A) 編集(E) 削除(B) OK キャンセ	
-	<u>前へ(P)</u> 次へ(N) 完了(F) キャンセル	

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。

新しいネットワーク ポリシー	x
記証方法の構成 接続要求がこのポリシーの条件を満たすた 推想を指定する必要があります。NAP を使 た EAP を指定する必要があります。接続要	めに必要な認証方法を、1 つ以上指定してください。 EAP 認証には、 EAP の 使用する 802.1Xまだは VPN を展開する場合は、 接続要求ポリシーに保護され 変求ポリシーは、ネットワーク ポリシーの認証設定よりも優先されます。
EAP の種類は、NPS とクライアントとの間で、表示されている	順序でネゴシエートされます。
 注意加(A) 編集(E) 削除(R) セキュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証パージョン 2 (MS-CHAP v2)(V ✓ パスワードの期限が切れた後も、ユーザーにパスワード ✓ Microsoft 暗号化認証 (MS-CHAP)(Y) ✓ パスワードの期限が切れた後も、ユーザーにパスワード ■ 暗号化認証 (CHAP)(C) ■ 暗号化とれて(いない認証 (PAP、SPAP)(S) ■ 認証方法をネゴシエートせずにクライアントに接続を許可: □ コンピュータの正常性チェックのみを実行する(F) 	上へ移動(U) 下へ移動(D) EAP の追加 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

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。

新しいネットワーク ポリシー		×
認証方法の構成 接続要求がこのポリシーの 種類を指定する必要があ た EAP を指定する必要があ	条件を満たすため(こ必要な認 ります。NAP を使用する 802: あります。接続要求ポリシー(3	証方法を、1 つ以上指定してください。 EAP 認証には、 EAP の IXまたは VPN を展開する場合は、 接続要求ポリシーに保護され 、 ネットワーク ポリシーの認証設定よりも優先されます。
EAP の種類は、NPS とクライアントとの間で、 EAP の種類(T):	表示されている順序でネゴショ	
Microsoft スマートカードまたはその他の意 ききhor(A) 「毎年(C) 81/85	亚明書 スマート カードまたはほかの言	上へ移動(U) 下へ移動(D) 王明書のブロパティ
セキュリティレベルの低い認証方法: ✓ Microsoft 暗号化認証バージョン 2 (1)	このサーバーは、接続が完了 書を選択してください。	する前に呼び出し(側に識別されます。識別の証拠として使う証明
 ✓ パスワードの期限が切れた後も、ユ・ ✓ Microsoft 暗号(上認証 (MS-CHAP)) ✓ パスワードの期限が切れた後も、ユ・ 	証明書の発行先(1): フレンドリ名:	dc.win2008-2.com
 「暗号化認証 (CHAP)(C) 「暗号化されていない認証 (PAP、SPA 「認証方法をネゴシエートせず(こクライア)」 	発行者: 有効期限:	win2008-2-DC-CA 2011/01/26 14:15:21
□ンピュータの正常性チェックのみを実行 _		OK キャンセル
		前へ(P) 次へ(N) 完了(F) キャンセル

図 5-86 認証方式(TLS)の確認

(13) 制約の構成

「次へ」を押します。

新しいネットワーク ポリシー	×
制約の構成 制約は、接続 合、NPS は接続 さい。	く 見求が一致する必要がある、ネットワーク ポリシーの追加パラメータです。接続要求が制約と一致しない場 売要求を自動的に拒否します。制約はオブションです。制約を構成しない場合は、[次へ] をクリックしてくだ
このネットワーク ポリシーの制約対 すべての制約が接続要求に一部 制約(S): 1187 1197 118	構成します。 しない場合、ネットワーク アクセスは拒否されます。 サーバーがアイドル状態になってから接続が切断されるまでの最大時間を分単位で指定しま 最大アイドル時間が経過したら切断する(D)
	前へ(P) 次へ(N) 完了(E) キャンセル

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。

新しいネットワーク ポリシー	×
ジェク構成 ポリシーのすべてのネ	ットワーク ポリシー条件および制約が一致した場合、NPS は接続要求に対して設定を適用します。
このネットワーク ポリシーの設定を構成 条件と制約が接続要求に一致してア!	します。 カセスが許可される場合、この設定が適用されます。
 設定(S): RADILS 属性 編準 ペンダ固有 ネットワークアクセス保護 NAP 強制 拡張状態 ルーティングとリモートアクセス マルチリンクおよび帯域 (幅割り当てプロトコル (BAP) P アコルタ 	追加属性を RADIUS クライアントに送信するには、標準 RADIUS 属性を選択し、[編集] を切ックします。属性を構成しないと、属性は RADIUS クライアントに送信されません。必要な属性については、RADIUS クライアントのドキュメントを参照してください。 属性(D): 名前 値 Framed-Protocol PPP Service-Type Framed
	追加(D) 編集(E) 削除(B)
	前へ(P) 次へ(N) 完了(F) キャンセル

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。

標準 RADIUS 属性の追加	×
・ 属性を設定に追加するには、属性を選択し、「追加」をクリックしてください。	
独自または定義済みのベンダ固有属性を追加するには、このダイアログ ボックスを閉じて [ベンダ固有] を選択し、[追加] をクリックしてください。	
アクセスの種類(工):	
র্সনের্ব 💽	
屬性(B):	
名前	
Tunnel-Assignment-ID	-
Tunnel-Client-Auth-ID	
Tunnel-Client-Endpt	
Tunnel-Medium-Type	
Tunnel-Password	
Tunnel-Preference	
	-
1400	
· 記忆9月:	
複数のトランスポートで運用できるプロトコル(L2TP など)のトンネルを作成するときに使うトランスポートメディアを指定	
।টেবৃ	
追加(<u>A</u>) 閉じる(<u>C</u>)	
	_

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。

属性の情報		×
属性名: Tunnel-Medium-Type		
属性の番号: 65		
属性の形式: Enumerator		
属性値(工):		
ベンダ 値		追加(<u>A</u>)
		編集(目)
		削除(尺)
		上へ移動(以)
		下へ移動(D)
	OK	キャンセル

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、「0K」を押します。

属性の情報	×
属性名: Tunnel-Medium-Type	
属性の番号: 65	
属性の形式: Enumerator	
居性値: ● 802.1×で一般的に使用する(M)	
802 (includes all 802 media plus	s Ethernet canonical format) 🛛 💌
C その他(Q)	
くなし〉	*
	OK キャンセル

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。

禹性の情報		×
属性名: Tunnel-Medium-Ty	pe	
属性の番号: 65		
属性の形式: Enumerator		
周性10(1): ベンダ	[值]	追加(<u>A</u>)
RADIUS Standard	1 802 (includes all 802 media plus	編集(E)
		前序(<u>R</u>)
		上へ移動(以)
		下へ移動(D)
	ОК	キャンセル

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。

準 RADIUS 属性の追加	
寄性を設定に追加するには、属性を選択し、[j自t	ウロ] をクリックしてください。
虫自または定義済みのベンダ固有属性を追加する 10]をクリックしてください。	るには、このダイアログ ボックスを閉じて [ベンダ固有] を選択し、 [追
2クセスの種業(I):	
すべて	•
<u> 寄性(B)</u> :	
名前	
Tunnel-Client-Endpt	
Tunnel-Medium-Type	
Tunnel-Password	
Tunnel-Preference	
Tunnel-Pvt-Group-ID	
Tunnel-Server-Auth-ID	
a se su	1.1
лºн:	
・ンネル セッションのグループ ID を指定します。	
	iBhn(A) 問じる(C)

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)。

属性の情報	×
属性名: Tunnel-Pvt-Group-ID	
属性の番号: 81	
属性の形式: OctetString	
入力する値の形式(<u>E</u>):	
C 16 進数(<u>H</u>)	
100	
	OK キャンセル

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。

出现 III 和 IIII 和 III 和 IIII 和 IIIIII	2017	
unnel-Pvt-Group	-ID	
諸性の番号: 1		
耐性の形式: ctetString		
割性値(<u>T</u>): ベンダ	値	追加(<u>A</u>)
RADIUS Standard 100	8 100	編集(5)
		前序余(<u>R</u>)
		上へ移動(山)
		下へ移動(D)

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。

属性を設定に追加するには、属性を選択し、G追加」をクリックしてください。 注自または定義済みのペンダ固有属性を追加するには、このダイアログ ボックスを閉じて「ペンダ固有」を選択し、G追 加」をクリックしてください。 アクセスの種類(T): すべて ■ 配件(B): ■ 配件(B): ■ 配件(B): ■ の の の の の の の の の の の の の	標準 RADIUS 属性の追加	2
独自まだは定義済みのペンダ固有腐性を追加するには、このダイアログ ボックスを閉じて [ペンダ固有] を選択し、6追 加 をクリックしてください。 アクセスの種類(①): マー・マー・マー・マー・マー・マー・マー・マー・マー・マー・マー・マー・マー・マ	属性を設定に追加するには、属性を選	択し、〔追加〕 をクリックしてください。
P7/セスの種類(1): すべて ■ ■ ■ ■ ■ ■ ■ ■ ■	独自または定義済みのベンダ固有属性 加] をクリックしてください。	を追加するには、このダイアログ ボックスを閉じて [ベンダ固有] を選択し、[追
すべて ■ 電性(B): 名前 Tunnel-Password Tunnel-Preference Tunnel-Pvt-Group-ID Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ↓ 説明: 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)	アクセスの種類(工):	
居性(B): 名前 Tunnel-Password Tunnel-Preference Tunnel-Pvt-Group-ID Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ↓ 就明: 使用されるトンネリング プロトコルを指定します。	すべて	×
ABIELED: 名前 Tunnel-Password Tunnel-Preference Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ・ 説明 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)		
Tunnel-Password Tunnel-Password Tunnel-Password Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ▼ ■ 説明: 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)	周住(<u>B)</u> : 反前	
Tunnel-Preference Tunnel-Preference Tunnel-Preference Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ・ 説明: 使用されるトンネリング プロトコルを指定します。 道加(A) 閉じる(C)	Tunnel-Password	
Tunnel-Pvt-Group-ID Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ・ 説明: 使用されるトンネリング プロトコルを指定します。 道加(A) 閉じる(C)	Tunnel-Preference	
Tunnel-Server-Auth-ID Tunnel-Server-Endpt Tunnel-Type ・ 説明: 使用されるトンネリング プロトコルを指定します。 道加(A) 閉じる(C)	Tunnel-Pvt-Group-ID	
Tunnel-Server-Endpt Tunnel-Type ・ 説明: 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)	Tunnel-Server-Auth-ID	
Tunnel-Type ・ 説明: 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)	Tunnel-Server-Endpt	
↓ 説明: 使用されるトンネリング プロトコルを指定します。 追加(A) 閉じる(C)	Tunnel-Type	
説明: 使用されるトンネリング プロトコルを指定します。 追加(A)		
説明: 使用されるトンネリング プロトコルを指定します。 追加(A)… 閉じる(C)		P
iX回fi 使用されるトンネリング プロトコルを指定します。 追加(A) 」 閉じる(C)		
使用されるトンネリング プロトコルを指定します。 追加(<u>A</u>) 】 閉じる(<u>C</u>)	言兄"月:	
<u>追加(A)</u> 閉じる(<u>C</u>)	使用されるトンネリング プロトコルを指定	します。
<u>追加(A)</u> 閉じる(<u>C</u>)		
<u>追加(A)</u> 閉じる(<u>C</u>)		
		追加(<u>A</u>) 閉じる(<u>C</u>)

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。

属性の情報		×
属性名: Tunnel-Type		
属性の番号: 64		
属性の形式: Enumerator		
属性値: C ダイヤルフップキたけ VPN でー・	ぬりに(申田才ふ(の)	
(なし)	x= 11C1X/113 @/@/	-
● 802.1×で一般的に使用する(M)	i i i i i i i i i i i i i i i i i i i	
Virtual LANs (VLAN)		-
C その他(<u>O</u>)		
くなし>		Ŧ
	OK キャンセル	

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。

国性の情報			×
属性名: Tunnel-Type			
属性の番号: 64			
属性の形式: Enumerator			
・属性値(T): ベンダ			i自加(A)
RADIUS Stand	dard Virtual LANs (VLAN)		編集(E)
			削除(尺)
			上へ移動(山)
			下へ移動(D)
		OK	キャンセル

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。

新しいネットワーク ポリシー		×
設定の構成 ポリシーのすべてのネット	ワーク ポリシー条件および制	約が一致した場合、NPS は接続要求に対して設定を適用します。
このネットワーク ポリシーの設定を構成し 条件と制約が接続要求に一致してアクセ 設定(S)-	ます。 2スが許可される場合、この設う	定が適用されます。
RADILS 属性 ● 標準 ② ペンダ固有 ネットワークアクセス保護 ⑤ NAP 強制	追加属性を RADIUS クライ を切っりします。 属性を構成 な属性については、 RADIUS 属性(I):	アンドご送信するには、標準 RADIUS 属性を選択し、「編集] しないと、属性は RADIUS クライアントご送信されません。必要 クライアントのドキュメントを参照してください。
₩ 拡張状態	名前	(値)
<u>ルーライングとリモートアクセス</u> で、マルチリンクおよび帯域 幅割り当てプロトコル (BAP) 日 アイルタ	Framed-Protocol Service-Type Tunnel-Medium-Type Tunnel-Pvt-Group-ID Tunnel-Type	PPP Framed 802 (includes all 802 media plus Ethernet canonic 100 Virtual LANs (VLAN)
💑 暗号化 🗾 IP 設定	追加(<u>D</u>) 編集(E)
		<u>前へ(P) 次へ(N) 完了(E) キャンセル</u>

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。

しいネットワーク ポリシー	x
新しいネットワー	ークポリシーの完了
次のネットワーク ポリシーが正常に作	成されました
1xPolicy	
ポリシー条件:	
条件 値	
NAS ポートの種類 イーサネット Windows グループ WIN2008-2¥1	xGroup
ポリシー設定: 「 ^{友供}	体
深証 認証方法 アクセス許可 非準拠クライアントの更新 NAP 強制 Framed-Protocol Service-Type	Tee EAP または MS-CHAP v1 または MS-CHAP v1 (パスワードの期限が切れた後、ユ アクセスを許可する True 完全なネットワーク アクセスを許可する PPP Framed
このウィザードを閉じるには、「完了」 を	

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。

瓢サーバー マネージャ		_ 🗆 ×
ファイル(E) 操作(A) 表示(V) ヘルプ(H)		
🗢 🔿 🔰 🖬 🛛 🖬		
■ サーバー マネージャ (DC)	ネットワーク ポリシー 操作	
D → 「クス) R Active Directory 記明書サービス D → Active Directory 記明書サービス D → DHOP サーバー D → DHOP サーバー D → DHOP サーバー Web サーバー(IIS) Active Directory 記明書サービス D → NPO (1 → DHO) RADILS 9-470-1とサーバー RADILS 9-470-1 RADILS 9-470-1	スキトワーク おりワークに キャトワーク おりシーでは、ネットワークへの特徴性な14可す3.2 ーサーと、これらの2. FRT オットワーク、活動ださる状況だと描述できない。状況を指定できます。 新規 プロシークに、指載ださる状況だと描述できない。状況を指定できます。 新規 プロシークに オカカ・1 プロシークに オカカ・1 プロシークに オカカ・1 プロシークに オカカ・1 プロシークに オカカ・1 プロシークに オカカ・1 プロシーク オカカ・1 プロシーク オカカ・3 プロシーク オカカ・3 プロシーク オカカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカ・3 プロシーパーへの接後 オカカ・3 プロシーパーへの接後 オカウ・7 プロシーパーク オーパシー プロシーク オーパシー プロシーク オージー パーク イリーク パーク イリーク パーク イリーク パーク オーショー パーク オーショー パーク オーショー パーク オーシュー パーク オーシュー パーク オーシュー パーク オーシュー パーク オーシュー パーク アクレクショ <td></td>	

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。

🤑 ローカル エリア接続のプロパティ	3
ネットワーク認証	-10
このイーサネット アダプタに、認証済みのネットワーク アクセスを提供するに は、このオプションを選択してください。 ▼ IEEE 802.1× 認証を有効にする(<u>N</u>) ネットワーク認証方法を選択してください(<u>M</u>):	
日 このネットワークへの) 次回接続時のために、ユーザー情報をキャッシュする(C)	
OK キャンセル	

「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。

- マ サーバーの - 次のサー - 「	証明書を検証する(⊻) - バーに接続する(<u>○</u>):		
' 信頼されたル	ート証明機関(<u>R</u>):		
Class 3	Public Primary Certification A	uthority	
Microsof	t Root Authority		
	t Root Certificate Authority		
Thawte	Fimestamping CA		
Junio2008	-2-DC-CA		
 新しいサ・ ない(P) 認証方法を選択 	-バーまたは信頼された証明機関 マする(<u>S</u>):	を承認するようユーナ	ザーに求め
ビ 新しいサ・ない(P) 認証方法を選択	-バーまたは信頼された証明機関 でする(<u>S</u>): 護されたパスワード (EAP-MSC)	を承認するようユー! IAP v2)	ザーに求め 構成(<u>C</u>)
 ■ 新しいサ・ない(P) 2000 2010 2010<!--</td--><td>-バーまたは信頼された証明機関 でする(<u>S</u>): 譲されたパスワード(EAP-MSC) 譲続を有効にする(<u>F</u>)</td><td>を承認するようユー† IAP v2)</td><td>ザー(こ求め 構成(<u>C</u>)…</td>	-バーまたは信頼された証明機関 でする(<u>S</u>): 譲されたパスワード(EAP-MSC) 譲続を有効にする(<u>F</u>)	を承認するようユー† IAP v2)	ザー(こ求め 構成(<u>C</u>)…

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。

EAP MSCHAPv2 のプロパティ
接続のための認証方法:
✓ Windows のログオン名とパスワード (およびドメインがある場合はドメイン)を自動的に使う(A)
<u> </u>

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")。

🏈 タブ ブラウザの開始 - Windows Interne	t Explorer		
🖉 💽 🗸 🙋 http://192.168.200.100/	certsrv	👻 🐓 🗙 🛛 Live Search	ب
😭 🏠 🕢 接続中		🚹 🔹 🗟 🔹 🖶 🔹 🔂 ページ(P)	▼ ③ ツール(0) ▼ [≫]
新しいタブを開きま	した		
	192.168.200.10	0 へ接続 ? [×
タブを使って次のことがで • Internet Explorer • 表示中のページの後		45	
• お気に入りやホーム	192.168.200.100	へ接続しています。	とり開いたり
9.	ユーザー名(山):	👩 dot1x 👻	
操作のヒント:	パスワード(<u>P</u>):	•••••	
 CTRL キーを押しな ださい)。 タブを閉じるには、 		── パスワードを記憶する(<u>B</u>)	ドタンを使用
 新しいタブで結果を さい。 		OK キャンセル	ER を押して
 タブについての詳細 	Ш		
ページが表示	9 1	′ンターネット 保護モード: 有効	a 100% 🔻

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。

(i) I = 100 - 100/certsrv/ (ii) I = 100/certsrv/ (iii) I = 100/certsrv/ (iiii) I = 100/certsrv/ (iiii) I = 100/certsrv/ (iii) I = 1	+ م
🚖 🎄 🌈 Microsoft Active Directory 証明書サービス 🍡 🗟 🔻 🗟 🔻 🗟 ページ(Ⴒ) 🔻 🍈 ツー	uL(<u>0</u>) ▼ [≫]
Microsoft Active Directory 証明書サービス win2008-2-DC-CA	<u>к-д</u>
Web ブラウザ、電子メール クライアント、またはほかのプログラムの証明書を要求する Web サイトです。証明を使用して Web 上でほかのユーザーがあなた自身を識別したり、メッセージに署名したり、メッセージを暗号たり、要求した証明書の種類によってほかのセキュリティ タスクを実行したりすることができます。	唐 兆し
この Web サイトを使って証明機関(CA)証明書、証明書チェーン、または証明書失効リスト(CRL)をダウードしたり、保留中の要求の状態を表示することもできます。	חענ
Active Directory 証明書サービスに関する詳しい情報は、次を参照してください: <u>Active Directory 証明</u> <u>ービスドキュメント</u> .	書サ
タスクの選択: 証明書を要求する <u>保留中の証明書の要求の状態</u> <u>CA 証明書、証明書チェーン、または CRL のダウンロード</u>	
ページが表示されました 🛛 🔯 🌑 インターネット 保護モード: 有効 🔍 100)% ▼
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。

Microsoft Active Directory 証明書サービス - Windows Internet Explorer ローロー
Coor € http://192.168.200.100/certsrv/certrqus.asp v 4 X Live Search ℓ v
🚖 🏘 🎉 Microsoft Active Directory 証明書サーピス 🍡 🖄 ▼ 🗟 ▼ 🖶 ▼ 📴 ページ(Ⴒ) ▼ 🍈 ツール(Ⴍ) ▼ 🎽
Microsoft Active Directory 証明書サービス win2008-2-DO-CA ホーム
証明書の種類の選択: ユーザー証明書
200% ▼

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。

Microsoft Active Directory 証明書リーヒス	 Windows Internet Explorer 		<u>.</u>		
http://192.168.200.100/cert	tsrv/certrqbi.asp?type=0	- + ×	Live Search	3	ρ
r 🏟 🔠 🕶 🏈 Microsoft Active 🥻	Microsoft Acti ×	🗄 • 🗟 • 🖗	▶ ▼ 🔂 ページ(<u>P</u>)	▼ () ツール(<u>0</u>)	•
Microsoft Active Directory 証明書サービス	win2008-2-DC-CA			<u><u></u> <u></u>ሐ−⊿</u>	
レーザー証明書 - 識別情報					
わし上の識別情報は必要ありません。	■THH書を完了するにけ「	美信]を力し₀力し.7	マイギネロ		
4 WALLON®W/JJT月FR(みめ)また(0)りみと70。 (細オプマンコン))			L VLCV '8		
		送信	i >]		
		送信	i>		
		送信	>		
		送信	>		-
		送信			-
		送信		0	-

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。

Web アク	セスの確認		83
A	この Web サイトはユーザーの代わり す。ユーザーの代わりに証明書を要 サイトだけに制限する必要がありま - 証明書を要求しますか?	りに新しい証明書を 求できるのは、信頼 す。	要求していま された Web
		(\$tu)(Y)	<u>いいえ(N)</u>

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。

🏈 Microsoft Active Directory 証明書サービス - Windows Internet Explorer	
CO V 2 http://192.168.200.100/certsrv/certfnsh.asp V 47 X Live Search	• ۹
$\Rightarrow \Rightarrow \textcircled{Microsoft Active} \textcircled{Microsoft Acti \times} \textcircled{Microsoft Acti \times} \textcircled{Microsoft Active} \textcircled{Microsoft Active}$	◎ ツール(<u>0</u>) ▼ [≫]
Microsoft Active Directory 証明書サービス win2008-2-DD-CA	<u>ħ-4</u>
証明書は発行されました	
要求した証明書は要求者に発行されました	
この証明書のインストール	
■応答の保存	
ページが表示されました 🙀 🚱 インターネット 保護モード: 有効	€ 100% ▼

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。

Web アクセスの確認		23
この Web います。信 きるように 明書が We いプログラ アクセスす - このプログ ている場合 いいえ]を	サイトは 1 つ以上の証明書をこのコンピュータに追加 瀬されていない Web サイトがユーザーの証明書を更 すると、セキュリティ上、危険です。信頼されていな b サイトによりインストールされ、さらに信頼されてい ふがこのコンピュータ上で実行され、ユーザーのデー る可能性があります。 つんで証明書を追加しますか? この Web サイトを信頼 は、[はい] をクリックします。信頼していない場合は クリックします。	して 新で い証 いな タに 見し に、[
	(\$\$\(<u>Y</u>)	√え(<u>N</u>)

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。

🏈 Microsoft Active Directory 証明書サービス - Windows Internet Explorer	
Correct Anterna State Anterna	- ۹
$ \begin{array}{c} & & \\ & & \\ & & \\ & \\ & \\ & \\ & \\ & \\ $	③ツール(<u>0</u>) ▼ [≫]
<i>Microsoft</i> Active Directory 証明書サービス win2008-2-DC-CA	<u>ホーム</u>
インストールされた証明書	
 新しい証明書は正しくインストールされました。	
ng palanga konga nama Kapatan na na ang kapatan na n	
	*
- 🛺 🕥 インターネット 保護モード: 有効	🔍 100% 🔻

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。

目的(<u>N</u>):	<ব শ ্য>			
個人 ほかの人 ロ	中間証明機関 信頼された	モルート証明機関 信	頼された発行元	信頼されない発行元
発行先	発行者	有効期限	フレンドリ名	
dot1x	win2008-2-DC-0	CA 2011/03/2	9 <なし>	
	エクスポード(E)) (前吻	<u>}(B)</u>		
インボート(D) [] 証明書の目的	エクスポート(E)) (前1) 間	<u>₹(B)</u>		[詳細設定(<u>A</u>)
インボート(①) [: 証明書の目的 暗号化ファイルシス:	Eクスポード(E)) 削弱 テム、電子メールの(呆護、クラ	(R)		[詳細設定(<u>A</u>)
インボート(①) [: 証明書の目的 暗号化ファイル シス:	Eクスポート(E)) 削除 テム、電子メールの(呆護、クラ	〒2015 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●		詳細設定(A) 表示(⊻)
インボート(D) [: 証明書の目的 暗号化ファイル シス: 証明書の詳細についる	エクスポート(E)) 削勝 テム、電子メールの(保護、クラ て表示します。	★(<u>R)</u>		詳細設定(<u>A</u>) 表示(<u>V</u>) 問!:3(C)

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。

🌻 ローカル エリア接続のプロパティ
ネットワーク認証
このイーサネット アダプタに、認証済みのネットワーク アクセスを提供するに は、このオプションを選択してください。 ▼ IEEE 802.1X 認証を有効にする(N) ネットワーク認証方法を選択してください(M): Microsoft: スマート カードまたはその他 ▼
 OK キャンセル

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。

- 接続のための認証方法:	
(目分の人マートカートを使う)	~
↓ このコノビューダの証明者を使いて 同 単純な証明書の選択を使う	ビ 5(##3考)(M)
- 🔽 サーバーの証明書を検証する(⊻)	I
□ 次のサーバーに接続する(_):	
1言東見されたルート言止9月後度11月2	
Class 3 Public Primary Certifi	ication Authority
Microsoft Root Authority	diam'ny
I Microsoft Root Certificate Au	athority
✓ win2008-2-DC-CA	
	証明書を表示する(<u>E</u>)
この接続で別のユーサー名を使うし	<i>у</i>
新しいサーバーまたは信頼された証明 か()(P)	明機関を承認するようユーザーに求め
100 NL/	
	OK Assistant

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
                                           TFTP サーバーの IP アドレス
             • • • I PADDR
                                           TFTP サーバーの IPv6 アドレス

    IPv6ADDR

              •••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
                                           ログアウト成功ページ

    · · · logout-success-page

                                           ログアウト失敗ページ

    · · · logout-failure-page

             • • • 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">

ユーザーアカウント
<input name="name" type="text" value="" size="30" maxlength="63">
パスワード
<input name="pass" type="password" size="30" maxlength="63">
```

```
<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">
ユーザーアカウント
<input name="name" type="text" value="" size="30" maxlength="63">
パスワード
<input name="pass" type="password" size="30" maxlength="63">
パスワードwidth="220">
パスワードwidth="220">
パスワードwidth="220">
パスワードwidth="220">
パスワードwidth="220">
パスワードwidth="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220">width="220"><
```

<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">
ユーザーアカウント
<input name="name" type="text" value="" size="30" maxlength="63">パスワード
<input name="pass" type="password" size="30" maxlength="63">認証方法の選択
<input name="pass" type="password" size="30" maxlength="63">認証方法の選択
<input name="authid" value="1">認証方法 1<br><input type=radio name="authid" value="1">認証方法 2<br><input type=radio name="authid" value="1">認証方法 2<br><input type=radio name="authid" value="1">認証方法 3<br><input type=radio name="authid" value="3">認証方法 4<br>:nput type=radio name="authid" value="1">:認証方法 4<br>:nput type=radio name="authid" value="10gin">:nput type=radio name="authid" value="1">:認証方法 4<br>:nput type="submit" name="action" value="login">:nput type="reset" value="reset">
```

<ログイン用の form 例(埋め込み型)>

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



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



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



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



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。

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

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

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)。

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。

- ・ 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。
- 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。
- . 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。
- 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。



(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。

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 💦 🛛 🤶
全般 セキュリティ
このポリシーで定義した設定は、クライアント コンピュータのすべての LAN インターフェイスに 適用されます。 ポリシー名(N):
新しい Vista ワイヤード (有線) ネットワーク ポリシー
[党8月(C):
サンプル説明
☑ クライアントで Windows ワイヤード (有線) 自動構成サービスを使用する(W)
) OK キャンセル 適用(A)

図 7-5 全般タブ

新しい Vista ワイヤード (有線) ネットワーク ポリシー Propertie	s ? 🗙
全般 セキュリティ	
 マネットワーク アクセスのために IEEE 802.1× 認証を使用可能にす ネットワークの認証方法の選択(T): Microsoft: (保護された EAP (PEAP) 認証モード(A): 	る(E)] <u>プロパティ(P)</u>
ユーサーの再設証 認証エラーの最大数(L): ▼ このネットワークへの今後の接続のため、ユーザー情報をキャ ユずる(C)	」 1 ジジ EX4mE改会() 0
OK キャンセル	, 適用(A)

図 7-6 セキュリティタブ

保護された EAP のブロパティ	×
接続のための認証方法: ┌─── サーバーの証明書を検証する(V)	
□ 次のサーバーに接続する(0): □ □	
信頼されたルート証明機関(R):	
 Class 3 Public Primary Certification Authority GTE CyberTrust Global Root Microsoft Root Authority Microsoft Root Certificate Authority Thawte Timestamping CA win2008-2-AD-CA ✓ win2008-2-AD-CA ✓ win2008-2-AD-CA ✓ min2008-2-AD-CA 	
- 認証方法を選択する(S):	
セキュリティで保護されたパスワード (EAP-MSCHAP ∨2) ▼ 構成(C)	
 ✓ すばやい再接続を有効にする(F) □ 検疫のチェックを有効にする(Q) □ サーバーに暗号化バインドの TLV がない場合は切断する(D) 	
OK キャンセル	
図 7-7 保護された EAP のプロパティ	

EAP MSCHAPv2 のプロパティ 🛛 🗙
接続のための認証方法:
☑ Windows のログオン名とパスワード (およびドメインがある場合はドメイン)を自動的に使う(A)
OK キャンセル

図 7-8 EAP MSCHAPv2の構成

詳細なセキュリティ設定
-IEEE 802.1X
802.1Xの詳細設定を強制する(E) EAPOL開始メッセージの最大数(T): 保持期間(秒)(H): 3 1 開始期間(秒)(D): 認証期間(秒)(U):
5 🚍 18 🚍
Eapol 開始メッセージ(O):
IEEE 802.1X をとおして送信する 🚽
「シングル サインオン
▼ このネットワークに対するシングル サインオンを有効にする
◎ ユーザー ログオンの直前に実行する
○ ユーザー ログオンの直後に実行する
接続の最大遅延(秒): 10 📑
▶ シングル サインオン中に追加のダイアログの表示を許可する
□ このネットワークでは、コンピュータとユーザーの資格情報を使用し た認証用に別の VLAN を使用する
OK キャンセル

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 Idif ファイル(802.3Schema.Idf)の作成
 以下の内容をコピーし、そのファイルを 802.3Schema.Idf 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 IdapDisplayName: 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. attributeld: 1.2.840.113556.1.4.1954 attributeSyntax: 2.5.5.12 omSyntax: 64 isSingleValued: TRUE systemOnly: FALSE searchFlags: 0 rangeUpper: 64 schemaldGuid:: WrCnILK4WU+cJTnmm6oWhA== showInAdvancedViewOnly: TRUE systemFlags: 16 dn: CN=ms-net-ieee-8023-GP-PolicyData,CN=Schema,CN=Configuration,DC=X changetype: ntdsSchemaAdd objectClass: attributeSchema IdapDisplayName: 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 schemaldGuid:: i5SYg1d0kU29TY1+1mnJ9w== showInAdvancedViewOnly: TRUE

systemFlags: 16 dn: CN=ms-net-ieee-8023-GP-PolicyReserved, CN=Schema, CN=Configuration, DC=X changetype: ntdsSchemaAdd objectClass: attributeSchema IdapDisplayName: ms-net-ieee-8023-GP-PolicyReserved adminDisplayName: ms-net-ieee-8023-GP-PolicyReserved adminDescription: Reserved for future use attributeld: 1.2.840.113556.1.4.1956 attributeSyntax: 2.5.5.10 omSyntax: 4 isSingleValued: TRUE systemOnly: FALSE searchFlags: 0 rangeUpper: 1048576 schemaldGuid:: xyfF0wYm602M/RhCb+7lzg== 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 IdapDisplayName: 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
schemaldGuid:: ajggmRmrRkSTUAy4e00tmw==
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

Tonsole1 - [Console Root\Active	Directory Schema [ws2003en.lab4	.hcl.co.jp]\Cl	asses]		_ 🗆 🗵
Bile Action View Favorites	Mindow Help				_8×
⇔ → 🗈 📧 🕃 🚱 😤					
Console Root	Name	Туре	Status	Description	
Active Directory Schema [ws2003	■# linkTrackOMTEntry	Structural	Active	Link-Track-OMT-Entry	
Classes	InkTrackVolEntry	Structural	Active	Link-Track-Vol-Entry	
Attributes	■@linkTrackVolumeTable	Structural	Active	Link-Track-Volume-Table	
	■@locality	Structural	Active	Locality	
	BlostAndFound	Structural	Active	Lost-And-Found	
	mailRecipient	Auxiliary	Active	Mail-Recipient	-
	meeting	Structoral	Active	Meeting	
	sms-net-ieee-80211-GroupPolicy	Structural	Active	This class represents an 8	
	state	Structural	Active	This class represents an 8	
	S-SQL-OLAPCube	Structural	Active	MS-SQL-OLAPCube	
	Solution Contemporate Sector Contemporation Sector	Structural	Active	MS-SQL-OLAPDatabase	
	Solution Contract Con	Structural	Active	MS-SQL-OLAPServer	
	mS-SQL-SQLDatabase	Structural	Active	MS-SQL-SQLDatabase	
	mS-SQL-SQLPublication	Structural	Active	MS-SQL-SQLPublication	
	mS-SQL-SQLRepository	Structural	Active	MS-SQL-SQLRepository	
	Solution States and Soluti	Structural	Active	MS-SQL-SQLServer	•

図 7-10 スキーマの確認

 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

追加するフォレスト内のドメイン名を入力してください。	テレストの追加				X
	追加するフォレスト内のドン	イン名を入力してください。			
ドメイン(D): lab4.hcl.co.jp	ドメイン(D): [lab4]	cl.co.jp			
<u>OK</u> キャンセル			ОК	キャンセル	

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

屋 グルーナ ボリシーの管理	
🔜 ファイル(F) 操作(A) 表示(V) ウィンドウ(W) ^	\/J)(H)X
🗢 🔿 🖄 🚾 🙆 🖬 🖬	
 ダループ ポリシーの管理 フォレスト: lab4hclco.jp □ ● ドメイン □ ● Ish4hclco.jp □ Default Domain Policy □ ● dot1x □ ● ガループ ポリシー オブジェクト □ ● Fault Domain Controllers Police □ ● クループ ポリシー オブジェクト □ ● Default Domain Controllers Police □ ● Default Domain Policy □ ● Default Domain Policy □ ● Default Domain Policy □ ● サイト ● グループ ポリシーのモデル作成 ● グループ ポリシーの結果 	Default Domain Policy スコーブ 詳細 設定 委任 リンク 表示するリンクの場所(L): 「ab4hcl.co.jp 次のサイト、ドメイン、および OU がこの GPO (こリンクされています(T): 場所 登制 リンクの有効化 パス 「dot1x ()… (は、) 「ab4hcl.co.jp/dot1x 「ab4hcl.co.jp ()… (は、) 「ab4hcl.co.jp/dot1x 「ab4hcl.co.jp ()… (は、) 「ab4hcl.co.jp ()… ての GPO での設定は、汁気のグループ、ユーザーおよびコンピュータにのみ 適用されます(S): 名前 ▲ Authenticated Users 」 道加(D)… 削除(R) グロパティ(P) WMI フィルタ処理 この GPO (お次の WMI フィルタにリンクされています(W): 「なし> 開く(Q)

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

■グルーフ ポリシーの管理		
🔜 ファイル(F) 操作(A) 表示(V) ウィンドウ(V	Ŵ ヘルプ(H)	_8×
← ⇒ 2 m		
ダルーブ ポリシーの管理 マオレスト: lab4 holco.jp 日 論 ドメイン 日 論 ドメイン 日 論 bd4 holco.jp 日 酒 lab4 holco.jp 日 酒 Domain Controllers 日 酒 NA 日 酒 グルーブ ポリシー オブジェクト ■ Default Domain Controllers ■ NA 日 酒 グルーブ ポリシー オブジェクト ■ Default Domain Controllers ■ ひん ● 愛 グルーブ ポリシーのモデル作成 グルーブ ポリシーの結果 レポー 表示(ここか) コピー 削除(名前(最新) 1	Default Domain Po スコーブ 詳細 設定 リンク 表示するリンクの場所(L): 次のサイト、ドメイン、および 場所 ご dot1x 合は1x Pop7(B) Pop7(B)	olicy 委任 「lab4 hcl.co.jp ▼ び OU がこの GPO (こリンクされています(T): 「強制」リンクの有効化 パス い… (はい lab4 hcl.co.jp/dot1× (、… (はい lab4 hcl.co.jp/dot1× (、… (はい lab4 hcl.co.jp/dot1× 「」 」 」 」 ● プロパティ(P) アコパティ(P) 「開く(O)
GPO エディタを聞きます。		

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。

ファイル名	を指定して実行 ? 🔀
-	実行するプログラム名、または開くフォルダやドキュメント名、インターネ ットリソース名を入力してください。
名前(0):	regedit
	OK キャンセル 参照(B)
	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

🧃 レジストリ エディタ			
ファイル(E) 編集(E) 表示(V) お気に入り(A) ヘルプ(H)			
i∎ - i DirectInput i∎ - i DirectMusic i∎ - i DirectPlay	▲ 名前 ●●)(既定)	種類 REG_SZ	データ (値の設定なし)
DirectPlay8 DirectPlayNATHelp DirectX dotSsve Mig mig mig Downlo Downlo Driver S DRM DrWats DrWats DrWats EAPOL DrWats ESENT ESENT ESENT ESENT ESENT Exchanse Exchanse Exchanse	直 (直(<u>M</u>) 字列/直(<u>E</u>)		
	~ <		
マイ コンピュータ¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥dot3s	;		

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。

💣 レジストリ エディタ			
ファイル(E) 編集(E) 表示(V) お気に入り(A) ヘルプ(H)			
🖬 🧰 DirectInput	🔺 名前	種類	データ
	ab](既定)	REG_SZ	(値の設定なし)
DWORD 値の編集	PIC Block_Time	REG_DWORD	0×00000000 (0)
値の名前(N):			
Block_Time			
値のデータ(V): 表記			
0 16 進(日)			
○ 10 進(D)			
OK ++>\tr			
😥 🧰 Exchange			
Function Discovery	~ <		
マイ コンピュータ¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥dot3svc			

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。

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)

265/312

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。

No.	レベル	メッセージ構文	内容
1	notice	<radius force local> authentication succeeded : uid=<user></user></radius force local>	認証成功
2	notice	<pre><web gateway mac dot1x dhcpsnooping static> : login</web gateway mac dot1x dhcpsnooping static></pre>	ログイン成功
		Succeeded : uId= <user> mac=<macaddr> IP=<ipaddr> port=<porino></porino></ipaddr></macaddr></user>	
		[VId= <vid>] [new VId=<vid>] [Class=<ulassid>]</ulassid></vid></vid>	
		<pre><weblgateway mac dot1x dncpsnooping static> : login </weblgateway mac dot1x dncpsnooping static></pre>	
		SUCCEEded : UID= <user> mac=<macaddr> IP=<ipaddr> port=<lagnu></lagnu></ipaddr></macaddr></user>	
		[VId= <vid>] [new VId=<vid>] [Class=<ulassid>]</ulassid></vid></vid>	
		<pre><web gateway mac dot1x dncpsnooping static> : login </web gateway mac dot1x dncpsnooping static></pre>	
		SUCCEEded : UId= <user> mac=<macaddr> IP=<ipaddr> port=MLAG</ipaddr></macaddr></user>	
		<pre>CDUMAIN>/<mlag id=""> [VId=<vid>] [new VId=<vid>] [class=<classid>]</classid></vid></vid></mlag></pre>	
3	notice	<pre><radius force local> authentication failed : uid=<user></user></radius force local></pre>	認証失敗
4	notice	<pre><web gateway mac dot1x dhcpsnooping static> : login failed :</web gateway mac dot1x dhcpsnooping static></pre>	ログイン失敗
		uid= <user> mac=<macaddr> ip=<ipaddr> port=<portno></portno></ipaddr></macaddr></user>	
		[vid= <vid>] [new vid=<vid>]</vid></vid>	
		<pre><web gateway mac dot1x dhcpsnooping static> : login failed :</web gateway mac dot1x dhcpsnooping static></pre>	
		uid= <user> mac=<macaddr> ip=<ipaddr> port=<lagno> [vid=<vid>]</vid></lagno></ipaddr></macaddr></user>	
		[new vid= <vid>]</vid>	
		<pre><web gateway mac dot1x dhcpsnooping static> : login failed :</web gateway mac dot1x dhcpsnooping static></pre>	
		uid= <user> mac=<macaddr> ip=<ipaddr> port= MLAG <domain>/<mlag< th=""><th></th></mlag<></domain></ipaddr></macaddr></user>	
		ID> [vid= <vid>] [new vid=<vid>]</vid></vid>	
5	notice	<pre><web gateway mac dot1x dhcpsnooping static> : logout(<type>):</type></web gateway mac dot1x dhcpsnooping static></pre>	ログアウト
		uid= <user> mac=<macaddr> ip=<ipaddr> port=<portno></portno></ipaddr></macaddr></user>	
		[vid= <vid>] [new vid=<vid>] [class=<classid>]</classid></vid></vid>	
		<pre><web gateway mac dot1x dhcpsnooping static> : logout(<type>):</type></web gateway mac dot1x dhcpsnooping static></pre>	
		uid= <user> mac=<macaddr> ip=<ipaddr> port=<lagno> [vid=<vid>]</vid></lagno></ipaddr></macaddr></user>	
		[new vid= <vid>] [class=<classid>]</classid></vid>	
		<pre><web gateway mac dot1x dhcpsnooping static> : logout(<type>):</type></web gateway mac dot1x dhcpsnooping static></pre>	
		uid= <user> mac=<macaddr> ip=<ipaddr> port=MLAG <domain>/<mlag< th=""><th></th></mlag<></domain></ipaddr></macaddr></user>	
		ID> [vid= <vid>] [new vid=<vid>] [class=<classid>]</classid></vid></vid>	
6	warning	<pre><web gateway mac dot1x dhcpsnooping discard deny static> :</web gateway mac dot1x dhcpsnooping discard deny static></pre>	装置の最大認証数による
		the number of terminals on switch is full : uid= <user></user>	ログイン不可
		<pre>mac=<macaddr> ip=<ipaddr> port=<portno> [vid=<vid>]</vid></portno></ipaddr></macaddr></pre>	

表 8-1 認証ログ一覧

No.	レベル	メッセージ構文	内容
		<pre><web gateway mac dot1x dhcpsnooping discard deny static></web gateway mac dot1x dhcpsnooping discard deny static></pre>	
		the number of terminals on switch is full : uid= <user></user>	
		<pre>mac=<macaddr> ip=<ipaddr> port=<lagno> [vid=<vid>]</vid></lagno></ipaddr></macaddr></pre>	
		<pre><web gateway mac dot1x dhcpsnooping discard deny static></web gateway mac dot1x dhcpsnooping discard deny static></pre>	
		the number of terminals on switch is full : uid= <user></user>	
		<pre>mac=<macaddr> ip=<ipaddr> port=MLAG <domain>/<mlag id=""></mlag></domain></ipaddr></macaddr></pre>	
		[vid= <vid>]</vid>	
7	warning	<pre><web gateway mac dot1x dhcpsnooping static> : the number of</web gateway mac dot1x dhcpsnooping static></pre>	インターフェースの最大
		terminals on port <portno> is full : uid=<user> mac=<macaddr></macaddr></user></portno>	認証数によるログイン不
		ip=<1PADDR> port= <portno> [vid=<v1d>]</v1d></portno>	可
		<pre><web gateway mac dot1x dhcpsnooping static> : the number of</web gateway mac dot1x dhcpsnooping static></pre>	
		terminals on port <lagno> is full : uid=<user> mac=<macaddr></macaddr></user></lagno>	
		ip=<1PADDR> port= <lagno> [vid=<v1d>]</v1d></lagno>	
		<pre><web gateway mac dot1x dhcpsnooping static> : the number of</web gateway mac dot1x dhcpsnooping static></pre>	
		terminals on port MLAG <domain>/<mlag_id> is full : uid=<user></user></mlag_id></domain>	
		mac= <macaddr> ip=<ipaddr> port=MLAG <domain>/<mlag id=""></mlag></domain></ipaddr></macaddr>	
		[vid= <vid>]</vid>	
8	warning	<pre><web mac dot1x> : vlan assignment failed : uid=<user></user></web mac dot1x></pre>	VLAN
		mac= <macaddr> ip=<ipaddr> port=<portno> vid=<vid> new</vid></portno></ipaddr></macaddr>	
		vid= <vid></vid>	
		<pre><web mac dot1x> : vlan assignment failed : uid=<user></user></web mac dot1x></pre>	
		mac= <macaddr> ip=<ipaddr> port=<lagno> vid=<vid> new vid=<vid></vid></vid></lagno></ipaddr></macaddr>	
		<pre><web mac dot1x> : vian assignment failed : uid=<user></user></web mac dot1x></pre>	
		mac= <macaddr> IP=<ipaddr> port=MLAG <domain>/<mlag id=""></mlag></domain></ipaddr></macaddr>	
		VId= <vid> new VId=<vid></vid></vid>	
9	warning	port <porino> has already been assigned to another vian :</porino>	VLAN 安史天 敗
		uid= <user> poil=<purinu> [new vid=<vid>]</vid></purinu></user>	(RADIUS/LOCAT 認証結果
		port <lagno> has arready been assigned to another vian.</lagno>	文"后时)
		uid= <usek> poil=<lagnu> [new vid=<vid>]</vid></lagnu></usek>	
		another when : wide discrete mass arready been assigned to	
		vidVID- 1	
10	warning	<pre><weblmacldot1xlstatic> : port <portno> has already been</portno></weblmacldot1xlstatic></pre>	└/IAN 変更失敗(端末設定
10	warning	assigned to another vian: uid= <user> mac=<macaddr> in=<ipaddr></ipaddr></macaddr></user>	時)
		port = < PORTNO> vid = < VID> [new vid = < VID>]	(U''
		<pre><weblmacldot1xlstatic> : port <lagno> has already been assigned</lagno></weblmacldot1xlstatic></pre>	
		to another vian : uid= <user> mac=<macaddr> ip=<ipaddr></ipaddr></macaddr></user>	
		port= <lagno> vid=<vid> [new vid=<vid>]</vid></vid></lagno>	
		<pre><web mac dot1x static> : port MLAG <domain>/<mlag id=""> has</mlag></domain></web mac dot1x static></pre>	
		already been assigned to another vlan : uid= <user> mac=<macaddr></macaddr></user>	
		ip= <ipaddr> port=MLAG <domain>/<mlag id=""> vid=<vid> [new</vid></mlag></domain></ipaddr>	
		vid= <vid>]</vid>	
11	warning	radius(<ipaddr>) timeout : uid=<user></user></ipaddr>	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></ipaddr></macaddr></user>	TTL フィルタによるログ
		port= <portno> vid=<vid> ttl=<ttl></ttl></vid></portno>	イン拒否
		<pre>web : login rejected : uid=<user> mac=<macaddr> ip=<ipaddr></ipaddr></macaddr></user></pre>	
		port= <lagno> vid=<vid> ttl=<ttl></ttl></vid></lagno>	
		<pre>web : login rejected : uid=<user> mac=<macaddr> ip=<ipaddr></ipaddr></macaddr></user></pre>	
		port=MLAG <domain>/<mlag id=""> vid=<vid> ttl=<ttl></ttl></vid></mlag></domain>	
19	info	<client_ip>(<user_agent>) <protocol> <url></url></protocol></user_agent></client_ip>	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。

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

表 8-2 ログアウトで表示されるタイプ一覧

ТҮРЕ	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。

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。

表 8-3 AccessDefender 設定時のコンフリクトメッセージ一覧

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。
 (2) 証明書の発行
- (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。



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 鍵長な

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...

例 項目 内容 文字数制限 JP Country 国別記号 2 State or Province 1~128 都道府県 Tokyo 1~128 市区町村名 shibuya-ku Locality 組織名 1~64 Organization example.corp 1~64 Organizational Unit | 部門名 section 1 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

表 9-1 証明書要求の項目

Common Name 以外は省略可能



done.

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。



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 WvAD2CC763Z9GRQbDYIITb8Mz86YoJ061LpNhc8906fE1pIQf+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</pre>

・・・・・ 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「openssI.cnf」ファイルを用いて CA を作成します。
 本例では OpenSSL の PerI 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. - - - - -【国コード】 Country Name (2 letter code) [GB]:JP 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】 【メールアドレス】 Email Address []:admin@apresia.jp

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。

```
# II /opt/apresia_certs/demoCA/
total 24
- rw-r--r--
                                    1265 Dec 17 17:39 cacert.pem(CA 証明書)
             1 root
                        root
drwxr-xr-x 2 root
                                    4096 Dec 17 17:37 certs
                        root
                                    4096 Dec 17 17:37 crl
drwxr-xr-x 2 root
                        root
                                       0 Dec 17 17:37 index.txt
-rw-r--r-- 1 root
                        root
drwxr-xr-x
             2 root
                                    4096 Dec 17 17:37 newcerts
                        root
```

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-rr	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

(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

WvAD2CC763Z9GRQbDYIITb8Mz86YoJ061LpNhc8906fE1pIQf+LJxrdTUfAUe0mo
kugHFw==
-----END CERTIFICATE-----

<秘密鍵>

-----BEGIN RSA PRIVATE KEY-----MIIBPAIBAAJBANrio6vXJPQax8WVyg+tml27F7ldnOukmznl1W4nChjSIp/yw3hD

i+iZDjtYHHWnbVffMU0/OK8dAM9zwesR00UCAwEAAQJAAbJYCnD0fF/oxINQuaZi

・・・・・中略・・・・・

Jt+Hd7ILcgrDuwIhAJZ0gMKvAWtxYiijwJStP1GR17nSqzjGud/uzhWbmBDnAiEA s0utik/2ZIZI1A1Wua+1XR0c3I1+hlusGvQMrLt1tnM= -----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。

証明書 ?	X	
全般 詳細 証明のパス	_	
証明書の情報 この CA ルート証明書は信頼されていません。信頼を有効にするには、		
というですると言われてれたか「「言語の弦楽」のストアにインストールしていた さい。		
登行告: Anresia CA		
発行者: Apresia_CA		
有効期間 2004/12/17 から 2005/12/17		
)	
ОК		

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。

証明書のインボート ウィザード 🛛 🛛 🛛
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。
●証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
○証明書をすべて)次のストアに配置する(P)
証明書ストア
参照(<u>R</u>)
< 戻る(B) 次へ(N) > キャンセル

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。

_
rtu I

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。

証明書					? 🛛
目的(<u>N</u>):	<	すべて>			~
個人(ほかの	しん 中間証	月機関 信頼されたルート語	四月機関 信頼され	した発行元	
祭行生		怒行来	右动期限	ついたおける	
- HIJL	~~		2005 (10 (17		
Apresia	LOA In Deet CA	Apresia_CA	2000/12/17	602</td <td></td>	
Symani		Symanted Root CA	2011/05/01		
Autoria	ad Certifica	Autoridad Certificado	2009/00/29	Autoridad Certifi	
Mutoria	ad Certifica	Release E-Tweet Pail	2009/00/30	Autoridad Certin	
Beigaci	om E-Trust	Beigacom E-Trust Fri	2010/01/21	Beigacom E-Tru	
Certipo 🖾 Certipo	ste Glasse	Centiposte Classe A	2018/00/24	Certiposte Editeur	
Certipo 🖾 Certipo	ste Gerveur	Certiposte Serveur	2018/00/24	Certiposte Serve	
	n Autoridad	Certisign Autoridade	2010/00/27	Certisign Autoria	×
(1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型) (1)ポート(型)					

図 9-11 追加されたプライベート CA

9.4 認証 URL ヘアクセス

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。

🖉 APRESIA AccessDefender - Microsoft Internet Explorer 📃	
」ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)	-
アドレス(D) 🍯 https://192.0.2.3/	>移動
	
APRESIA AccessDefender	
lleer ID	
UserID	
Password	
login reset	
logout	
	7
🙆 ページが表示されました	
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.



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>



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 ↓ 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]	
<pre>basicConstraints = CA:true</pre>	< 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。
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: = JPcountryName 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。

openss1 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:
                                      = JP
             countryName
             stateOrProvinceName
                                      = Tokyo
             localityName
                                      = Chiyoda-ku
                                     = apresia
             organizationName
             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 ヘアクセス(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。

ADDESTA AccessDefender - Misrosoft Internet Euplorer
] ③ 戻る ▾ ④ ▾ 🖹 🛃 🏠 🔎 検索 🛛 👋 Google 💽 ▾ 🔤 🔹 🚺
アドレス(D) 🚳 https://192.0.2.3/
×
APRESIA AccessDefender
User ID
Password
login reset
logout
🗃 ページが表示されました

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。

証明書	<mark>? ×</mark> 証明書	? ×
全般 詳細 証明のパス 証明書の情報 この証明書の目的: ・リモート コンピュータの ID を保証する 発行先: 192.0.2.3	全般 詳細 証明のパス 証明のパス(P) 副 Apresia_RootCA 副 Apresia_IntermediateCA 1920.2.3	
発行者: Apresia_IntermediateCA 有効期間 2008/11/06 から 2009/11/06 「証明書のインストールU」」 発行者のステートメント(S)		
ОК		

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。

Version	管理番号	内容
8.06.01	AE0S-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 变更制限機能
		• 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	AE0S-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>")</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</password>
		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>"</portrange></ttl>
		• "web-authentication ttl <ttl> lag <lagrange>"</lagrange></ttl>
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>"</ipaddr>
		• "logout ping ttl <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</password></userid>
		<vid>]"</vid>
		• "aaa-local-db del user <userid>"</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

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
		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ボ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 User ID で Web 認証ができない
8.10.01	AE0S-81001-RC001	Apresia13000-X24-PSR において、AccessDefender 機能(802.1X 以外)をサ
	1500 04004 00000	
8.10.01	AE0S-81001-RC002	AccessDefender 機能において、認証機能(ケートワェイ認証以外)でユー
		サー毎にハケットノイルター2 機能を週用拡張でさる機能をサホートしま - +
0.40.04	1500 04004 00000	
8.10.01	AE05-81001-RC023	
8 10 02	AE08-81002-PC002	
0.10.02	AL00-01002-10002	
8 10 02	AF0S-81002-RC010	血の(X音をしるした。 AccessDefender 機能において MAC 認証と access-defender-logout を繰
0.10.02	NE00 01002 N0010	1000000000000000000000000000000000000
		mac-authentication enable"コマンドを実行すると装置が再起動する問
		調を修正しました。
8.11.01	AE0S-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、</time>
		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"</ports>
		• "logout linkdown time <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</port>
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
		"web-authentication snooping proxy-port <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
		• "access-defender static mac <macaddr> Vian <vid> class <classid></classid></vid></macaddr>
		port <pukinu></pukinu>
		access-detender statte mac <macaddes <vid="" viait=""> class <classid> log <l "<="" agnos="" td=""></l></classid></macaddes>
8 15 01	AE08-81501-P0053	Tay <launo> AccossDefender 機能において、vien が名物設定ある状態で装置を再起動</launo>
0.15.01	AE03-01501-R0055	
8 15 01	AF0S-81501-RC054	AccessDefender 機能において、vlan が多数設定ある状能で装置を再起動
0.10.01		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	AF0S-81701-RC003	Apresia15000 シリーズにおいて、AccessDefender 機能の MAC 認証に対応
••••••		
8.17.01	AE0S-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什様を変更しました。
		• "access-defender static mac <macaddr> (port <portno> (lag</portno></macaddr>
		<pre></pre>
8.17.01	AE0S-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	AE0S-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</process:info>
		manually"
		• " <process:info> A-Def : dhcpsnooping : mode changed to PERMIT</process:info>
		manually"
8.17.04	AE0S-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
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。
	1500 04000 00000	• "web-authentication port <puri> dot1x"</puri>
8.18.02	AE0S-81802-RC036	AccessDefender 機能において、認証端木の WEB へのアクセスロクを出力
		 「logging access-detender web-access on" キュコン・ドはし ニゴルン・ニーニッン・ゲロのココン・ドトセンセオ、予告等
		ー 本コマノトはトラノルシューティノク用のコマノトとなりまり。 通吊連
0 10 00	AFOC 01000 DC007	
8.18.02	AEUS-81802-RU037	Accessberender 機能にあいて、MLAG インターノエースを衣示させるト記
		コマントをリホートしました。
		 show access-defender dotty statistics mlag"
0 10 02	AEAS 91902 PC062	 Show access-defender doffx Statistics mag AccessDefender 機能において、端本の認証加囲を開始する際、同一のMAC
0.10.02	AL03-01002-10002	Accessberender 機能にのいて、端木の認証処理を開始する際、同一のMAC
		アーレスの調不がってに心脏消頭不らして豆球されている物白、頭不干 「「「」」」である「「」」」では、「」」では、「」」、「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「
8 18 02	AF0S-81802-R0136	王家による王家八派のロアを出げるないようには旅を交更したのに。 AccessDefender 機能において Annle 社の Macintosh トのブラウザーから
0.10.02		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
8,18,02	AE0S-81802-RC137	AccessDefender 機能において、"packet-filter2 group <group>"コマン</group>
		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止し
8.18.02	AE0S-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"を実行するとエフーメッセーンが出る問題を
0 10 00	AFOS 91902 DC145	18止しました。
0.10.02	AEUS-81802-RC145	AccessDefender 仮能にのいて、TEEE002.1A 認証の設定変更を11つ場合、
		AccessDefender の設定を更かてきず、 Show Tulling-Contry に
8 18 02	AE05-81802-RC146	
0.10.02	AL03-01002-10140	
8 18 03	AF0S-81803-RC007	
0.10.00		ると"show access-defender client"の改行表示がずれる問題がありま
		たため、記載を削除いたします。
8.19.01	AE0S-81901-RC021	MMRP-Plus 機能の分散マスター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
		「た変更しました。
		• "[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"ssI 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	AEOS-81901-RC155	AEOS-81001-ER023 【AccessDefender 機能において、Class の値が4桁にな
8.19.03	AEOS-81903-RC004	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	AE0S-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	AE0S-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</port>
		vlan : uid= <user id=""> port=<port number=""> [new vid=<vid>]"</vid></port></user>
		• "A-Def : {web mac dot1x} : port <port number=""> has already been</port>
		assigned to another vlan : uid= <user id=""> mac=<mac address=""> ip=<ip< td=""></ip<></mac></user>
		address> port= <port number=""> vid=<vid> [new vid=<vid>]"</vid></vid></port>
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	AE0S-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	AE0S-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 name="action" type="submit" 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	AE0S-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	AE0S-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	AE0S-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</index></index>
		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</time>
		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) (Tag LAGRANGE) (mTag
8.24.01	AE0S-82401-RC088	AccessDefender 機能の DHCP Snooping 機能において、設定変更に作う
		"ancp-snooping mode timer"の起動時に、ト記ロクか出力されない場合が
		のる问想を修止しました。 • "A Def : dependencing : mode times started"
0.04.04		A-Def : ancpshooping : mode-timer started
0.24.01	AEUS-82401-KUU89	Accessperender 機能の DHCP Shooping 機能において、以下の手順で
		ancp-shooping statte-entry コマノトの設定、削除を実行しに俊に、 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 併用ボート
		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かロクアワトしない問題を修止しました。
8.25.01	AE0S-82501-RC063	AccessDefender 機能において、 "dhcp-snooping mode deny"コマンドか設
		定済みで"dhcp-snooping enable"設定時(無効から有効)に、以下のロクか
		出力されていなかった問題を修正しました。
0.00.04	4500 00004 00000	"A-Def : dncpsnooping : mode changed to deny manually"
8.26.01	AE0S-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	AE0S-82601-RC024	AccessDefender 機能において、IEEE802.1X 機能有効時、かつ FDB 登録数
0.00.04	4500 00004 00050	か多い場合における CPU 貝何を低減させよした。
8.26.01	AEUS-82601-RC056	AccessDefender 機能において、DHCP Snooping 登録端木数が装直の最大数
		古、以下に示9・表直の取入認証数によるログイノ不可」のログが出力さ
		1 いるい 川可思で 形正 しま した。 • "A Dof : dhopspooping : the number of terminals on emitted is full :"
0.00.04		 A-bei . uncpshooping . the number of terminals on switch is TUTL: AccesseDefender 地台に キロステーロ(OD Occession 落ちませーナボーボー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
0.20.01	AEUS-82001-KUUS/	Accessuerender (機能にのいて、Unor Snooping 豆球峏木数が max-client)
		フニッる场古、以下に小り イノグーノエー人の取人認証数によるログイ

Version	管理番号	内容
		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></portno>
		is full :"
		• "A-Def : dhcpsnooping : the number of terminals on port <lagno></lagno>
		is full :"
		• "A-Def : dhcpsnooping : the number of terminals on port MLAG
		<domain>/<mlag id=""> is full :"</mlag></domain>
8.26.01	AEOS-82601-RC058	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
8.26.01	AEOS-82601-RC059	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
8.26.01	AE0S-82601-RC060	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。
		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】
		(1) IEEE802.1X 機能有効時に、多数のサフリカントから EAP フレームを
		(3) (1)の状態にあいて、TEEE802.1X 認証ホート間で認証端末がローミン
		次・示け(2)対象コマンド 見
		mmrp.plus.ring master master port <portno> slave-port <portno.< td=""></portno.<></portno>
		mmrp plus ring master master log d ACNO, clove port (POPTNO)
		mmrp plue ring uplink port «POPTPANCE»
		interface part (DOPTRANCE)
		detty port - DODTDANCE, initializa
		dotty port -POPTPANCE, re outbontionto
		L po 1 dotty port «POPTPANCE»
		[no] wob authentication part (DODTRANCE) dotay
		[no] detty part (DOPTRANCE) timeout quiet period
		[no] dotty port <pontrainge> timeout ty ported</pontrainge>
		[no] dotty port <pre>CONTRAINCE> timeout to suther side</pre>
		[no] dotty port <portrainge> timeout curp timeout</portrainge>
		[no] dotty port <portrange> (Imeout supp-timeout</portrange>
		[no] dot1x port <purirange> reauthentication</purirange>

Version	管理番号	内容
		[no] dot1x port <portrange> ignore-eapol-start</portrange>
		show access-defender dot1x port <portrange></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、いりれのハーションにおいても IEEE802.1X 関連ログのタイムスタ
0.00.01	AFOS 83601 DC061	ノノか不止となることがのります。
0.20.01	AEUS-82601-RC061	Aprestatsooo シリースの Accessberender 機能にのいて、動的 VLAN の割 リップが 256 逆ままでしかできない問題を修正しました
		ゆ正前のバージョンでは、257個以上の端末に動的 VIAN 割1)当てを試み
		• 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
		ホートの設定において、エラーメッセージの一部が大又子になる問題を修
9 27 01	AEOS 92701 BC014	止しました。
0.27.01	AEUS-02701-RC014	
		ーロージョン 300 CM 2010Cのないの度を停止しなりた。停止後は、 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	AF0S-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	AE0S-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>"</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"
		オブションをサポートしました。
		• "aaa authentication web [<id>] <radius1> <local> <force></force></local></radius1></id>
		[port <portrange>]"</portrange>
		• "aaa authentication mac <radius1> <local> <force> [port</force></local></radius1>
		<portrange>]"</portrange>
		ローカル、 強制認証を設定 9 ることか 可能になります。
		本オノンョンは認証万式として Web 認証、MAC 認証を指定した際にのみ設

Version	管理番号	内容						
		定可能です。 IEEE802.1X は未サポートです。						
		本オプシ	ション設定	定時は、"aaa	authen	tication control"コマ	マンドとの併用	
		は未せた	は未サポートです。					
8.31.02	AEOS-83102-RC007	AccessD	AccessDefender 機能の"logout aging-time"コマンドにおいて、					
		"dhcp-s	noop i ng	"オプションな	をサポー	トしました。		
		• "logo	out aging	g-time <time< th=""><th>> dhcp-</th><th>snooping"</th><th></th></time<>	> dhcp-	snooping"		
		設定した	こ無通信	時間を経過9	ると、認	「証済み端末を自動的」の	ニロクアワトさ	
		せより。	せより。 毎通信防視対象となるパケットけりての通りです					
		無地						
		初記古式		毎通信				
		(1)	DHCP Sr	<u>~~</u> 100pingのみ	Ser	<u>血院/J3((ソット</u> nder IP が認証端末の	ARP パケッ	
					送	言元 IP が認証端末の	P パケット	
		(2)	2) DHCP Snooping と		DHCP S	DHCP Snooping と Web/IEEE802.1X 認証		
			Web/IEEE802.1X 認		(AND)	(AND)が独立して以下のパケットを監視		
			証(AND)を併用		DHCP Snooping			
			Sender IP が認証端末の		ARP パケッ			
			Web/IEEE802.1X 認証(AND))) 			
					达1 z	言元 MAC アトレスか認 ID パケット	証姉木でめ	
		(2)	DHCP Snoopina と		0 ПЦ(IF ハウット P Spooning で登録さ:	 hた坦스	
		(3)	(2) L	Mooping と 外の認証方	Ser	r Shooping C豆銀と der IP が認証端末の	いこ場合 ARP パケッ	
			(2) ダノ 式の併	用				
			2002 101		Web	o/MAC/IEEE802.1Xで認	証された場	
					合			
					送	言元 MAC アドレスが認	証端末であ	
					る	IP パケット		
8.31.02	AEOS-83102-RC009	SSL 機能	ミにおいて	て、デフォル	トのサー	・バー証明書、及び秘密	聲鍵を変更しま	
		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	艮が変更	になります。				
		тт		0 20 VV	いお	0.21.02.11.108	供老	
		归 Organi	<u>zation</u>	Hitachi Ca		Evample Domain	111115	
		organi	2011011	td.	1016, L			
		Organi	zation	Informatio	on Syst	Example Group.		
		Unit		ems Group	- j			
		Email		apresia@hi	tachi-	example@example.c		
		Addres	Address cable.co		р	om		
		有効期	限	2009/8/19-	~ 2029/	2017/1/25 ~ 2037/1	時刻情報は	
				8/14		/20	省略	

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止しました。
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"コマンドの設定かめる状態で、
		10 access-defender コマノトで設定を削除した後に TEEE002.1A 認証を (たうと、 JEEE002 1V/MAC 初証の動作が行われる問題を修正しました
0 21 02	AEOS 92102 PC020	1) クC、TEEE002.17/MAC 認証の動作が1)われる问題を修正しました。
8.31.02	AE05-83102-RC020	Accessberender 機能において、 aaa authentication dotix コマノトで "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 認証有効ボートで受信する自装置の
		UPU 宛てのフレーム、およびソフトワェア甲継されるフレームのうち、認
		証ハ1 ハスの対象ノレームの場合は MAC 認証を行わないようにする機能
		をリハートしました。 ・ "mac authorization hypers from check archie"
8 3/ 01	AE05-83401- PC005	- mac-authentication bypass-Itame-check elidole
0.04.01		nort"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>]"</portrange></id>
		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	AE0S-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)

Copyright(c) 2014 APRESIA Systems, Ltd. 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/