



第9版(Rev.2)

Copyright © 2007-2014, ALAXALA Networks Corporation. All rights reserved.



はじめに

本ガイドは、Microsoft 社の提唱する Network Access Protection(NAP)検疫システムをアラクサラネットワークス社の AX シリーズ(AX1200S / AX2400S / AX2200S / AX2500S / AX3600S)でサポートしている IEEE802.1X 認証機能を用いたシステム構築において、RADIUS サーバに Windows Server 2008 及び Windows Server 2008 R2、クライアント端末に Windows 7、Windows Vista 及び Windows XP を使用する場合の設定方法を示します

関連資料

・AX シリーズ認証ソリューションガイド

・AX シリーズ製品マニュアル (http://www.alaxala.com/jp/techinfo/manual/index.html)

本ガイド使用上の注意事項

本ガイドに記載の内容は、弊社が特定の環境において、基本動作や接続動作を確認したものであり、 すべての環境で機能・性能・信頼性を保証するものではありません。弊社製品を用いたシステム構築の 一助としていただくためのものとご理解いただけますようお願いいたします。

Windows 製品に関する詳細はマイクロソフト株式会社のドキュメント等を参照下さい。

本ガイド作成時の OS ソフトウエアバージョンは以下のようになっております。

AX1230S	Ver1.4.J
AX1240S	Ver2.2.F
AX2200S	Ver.2.4.D
AX2400S / AX3600S	Ver11.4.D
AX2500S	Ver3.0.B

本ガイドの内容は、改良のため予告なく変更する場合があります。

輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国輸出管理規制など外国 の関連法規をご確認の上、必要な手続きをお取り下さい。

なお、不明な場合は弊社営業担当にお問い合わせ下さい。

商標一覧

- ・Ethernetは、富士ゼロックス(株)の登録商標です。
- ・イーサネットは、富士ゼロックス(株)の登録商標です。
- ・Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- ・Windowsは、米国およびその他の国における米国Microsoft Corp. の登録商標です。
- ・そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

使用機器一覧

- AX1230S (Ver1.4.J)
- AX1240S (Ver2.2.F)
- AX2430S (Ver11.4.D)
- AX3630S (Ver11.4.D)
- AX2530S (Ver 3.0.B)
- Windows XP SP3
- Windows Vista SP1
- Windows 7
- Windows Server 2008 Standard
- Windows Server 2008 R2 Standard

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	_	2007.10.10	初版発行	_
第2版	_	2007.10.26	Windows Server 2008 (RC 版) の内容に差し替え	5.2.1
			検疫ネットワーク構成図に以下を追加	3.1.1
			・ 認証スイッチで VRRP をフィルタリング	3.1.2
			・ コアスイッチ間にリンクアグリゲーションを設定	3.1.3
				3.2.1 3.2.3
				5.2.5 付録 A
			▲X1230S に端支検出機能を停止するコンフィグレーショ	3131(3)
			いた12000に加水検出機能を停止するコンジャッレーンコーンを追加	付録 A
			Windows Server 2008 のデフォルトドメインポリシーの	43
			変更方法を追加	
			NAP クライアントのネットワークアクセス状態の確認方	5.3.2
			法を追加	
			誤記および表現を全体的に修正	_
第3版	_	2008.3.21	ドキュメント名変更	_
			サポート内容を更新	2章
			Windows Server 2008 (製品版)の内容に差し替え	3.1.4.1
		0000 5 04		3.2.4
第4版	_	2008.5.21	Windows Vista (SP1)に対応	_
			NAP クライアントに Windows XP SP3 を追加	3.6
			Active Directory との連携およひ特徴を新規追加	1.4 1.5
			認証前 VLAN から Windows ドメインにログオンできる構	3.2
			成に変更	3.3
				3.4
			NAP クライアント設定手順を自動設定に変更	3.5.2 3.6
			RADIUS サーバ冗長化に関する注意事項を「認証ソリュー	6章
			ションガイド」に移動	
			Windows XP SP3 に関する注意事項を追加	
			Windows の IEEE802.1X 認証に関する注意事項を追加	
第5版	_	2008.9.16	AX1200S(Ver1.4)でサポートされた内容を反映	2章
			・ IEEE802.1X 認証(動的 VLAN モード)の新コンフィグ	3.3.1
			レーションに変更	3.4.1
			・ 認証専用アクセスリストをサポート	4.4.1

第6版	_	2009.3.9	新規機種 AX1240S に対応	はじめに		
			・収容条件追加	2章		
			・ AX1230S との動作差分記載	3.3.1		
			システムファンクションリソース設定	3.4.1		
			フィルタのコンフィグレーションコマンド	6.3		
			NAP と連携可能な認証方式一覧を追加	2章		
			固定 VLAN モードでの NAP 連携サポートの内容を追加	1.3		
			・検疫ネットワークの構築(基本編)のタイトルを(固定	3章		
			VLAN 構成)に変更、(応用編)削除し(固定 VLAN 構成)を	4 章		
			新規追加	付録 A		
			グループポリシーの設定内容追記	3.5.2		
			IP アドレス切り替え問題の回避方法の説明追記	6.1.1		
第7版	_	2009.07.16	AX2400S/AX3600S でサポートされた内容を反映	1.3		
			・固定 VI AN モードの NAP 連携をサポート	2章		
			・IFFF8021X 認証の認証専用 IPv4 アクセスリストをサ	3.3		
			ポート	3.4		
				4章		
			IEEE802.1X 端末検出機能の AUTO サポートを反映	3.3		
				3.4		
				4.3		
				4.4		
			RADIUS サーバが 1 台で構成されるシステムでの	3.3		
			AX1200S を認証スイッチにした場合の構築ポイントを追	3.4		
			<u></u>			
			Windows Server のネットワークポリシーの構成で認証エ	3.5		
			ラーの最大値設定を追加			
			AX シリーズの運用コマンド表示例を更新	5.1		
第8版	—	2010.2.17	Windows Server 2008 R2 版の内容を追加	_		
			NAP クライアントに Windows 7 を追加			
			「1.6 オペレーションシステムによる差分について」を追	16		
			加	1.0		
			AX シリーズの構築ポイント(1)にレイヤ 2 ハードウェ	221		
			アテーブルの検索方式を追加	5.5.1		
			AX シリーズのコンフィグレーションを更新	3.4		
			・レイヤ2ハードウェアテーブルの検索方式を追加	4.4		
		注意事項を更新				
			6.2.1 の内容の一部を 8 章構築ノウハウ「8.2 コンピュー	8.2		
			タ認証について」に移動			
第9版	_	2011.1.28	収容条件に追加 AX2530S 追加	2		
				0.1.1		
			コンフィクレーションに AX2530S と AX1240S との差分	3.4.4		
				4.4.4		
			グループポリシーの設定時に gpupdate /force コマンドを	3.5.2(7)		
			追加し設定反映を即時に実施するよう変更			
				付録Δ		
				רי איי ניו		
	1	2014.9.18	収容条件に AX2230S および AX3650S 追加	2章		
			収容条件の認証モードについて、表現を修正			
	2	2014.10.22	AX2400S,AX3600S,AX6000S での固定 VLAN モードの表	1.3		
			記について明確化	4 草		
				5.1		

目次

1. NAP 検	疫概要	8
1.1 検兆	タネットワークとは	8
1.2 NA	P (Network Access Protection)	9
1.2.1	概要	9
1.2.2	NAP 実施オプション	9
1.2.3	NAP 構成要素とセキュリティ検査項目	10
1.3 AX	と NAP の連携	11
1.3.1	IEEE802.1X 動的 VLAN モード	12
1.3.2	IEEE802.1X 固定 VLAN モード	15
1.3.3	IEEE802.1X 動的 VLAN モードと固定 VLAN モードのまとめ	18
1.4 Act	ive Directory との連携	19
1.4.1	Windows ドメイン環境との共存	19
1.4.2	グループポリシーを用いた NAP クライアント自動設定	19
1.5 AX	と NAP 検疫の特徴	
1.5.1	NAP 検疫の特徴	
1.5.2	AX シリーズを用いた NAP 検疫システムの特徴	
1.6 才	ペレーションシステムによる差分について	22
1.6.1	Windows Server 2008 R2 と Windows Server 2008 の差分	
1.6.2	Windows 7、Windows Vista、Windows XP(SP3)の差分	
2. AX シリ	ーズの収容条件	23
3. 検疫ネッ	ットワークの構築(動的 VLAN 構成)	
		2 (
3.1 概要	安	
3.2 快渡	ダイットワーク 構成凶	
3.3 1件5	≈ ^ Y / - 関する構筑ポイント	21 27
333	AAに関する構築ホイント Windows Server 2008 に関する構筑ポイント	21
3.4 ΔX	の設定	29 30
341	AX1200Sのコンフィグレーション	
3.4.2	AX2400S のコンフィグレーション	
3.4.3	AX3600S のコンフィグレーション	
3.4.4	AX2500S のコンフィグレーション	
3.5 Wi	ndows Server 2008 の設定	
3.5.1.	事前準備	40
3.5.2.	グループポリシーの設定	41
3.5.3.	ユーザ、グループの作成	
354	RADIUS クライアントの設定	

	3.5.5.	接続要求ポリシーの設定	53
	3.5.6.	システム正常性検証ツール(SHV)の設定	
	3.5.7.	正常性ポリシーの設定	
	3.5.8.	ネットワークポリシーの設定	61
	3.5.9.	DHCP サーバの設定	
3.	6 NA	P クライアントの設定	
	3.6.1.	導入ステップ	
	3.6.2.	Windows ドメイン参加の設定	70
	3.6.3.	設定の確認	73
4.	検疫ネ	ットワークの構築(固定 VLAN(ポート単位)構成)	74
4	1 根耳	要	74
4	2 検	≪	75
4.:	- 穴	~ / / / / / / / / / / / / / / / / / / /	
	4.3.1		
4.	4 AX	の設定	
	4.4.1	AX1240S のコンフィグレーション	
	4.4.2	AX2400S のコンフィグレーション	81
	4.4.3	AX3600S のコンフィグレーション	83
	4.4.4	AX2500S のコンフィグレーション	85
4.	5 Wi	ndows Server 2008 の設定	
	4.5.1	ネットワークポリシーの設定	
5.	動作確認	認	
5	1 1	シリーブの運用コマンド	02
5.	511	- シリースの定用コマンド	92 02
	512	show dot1x logging	عد مر
	513	clear dot1x auth-state	بەت مە
5	2 NF	いては、ACCAL ACCAL	
0.	5.2.1	イベントビューアー	
5.3	3 NA	P クライアントの運用ツール	
	5.3.1	netsh nap client show state	
	5.3.2	ネットワークアクセス状態の確認	
6	注音車1	۲	100
0.	江志寺		
6.	1 動	約 VLAN 使用時の注意争項	
	б.1.1 о.с.с	WINDOWS XP のIP アトレス切り替え問題	
-	б.1.2	IP アトレス切り替え問題の詳細解説	
6.	2 VL	AN モート共通(動的 VLAN、固定 VLAN)の注意事項	
	6.2.1	非認証状態保持時間の設定について	105
7.	トラブ	ルシューティング	106

7.1	Windows ドメインに参加できない	
7.2	検疫に成功しない	
7.3	IEEE802.1X 認証動作を行わない	
8. 設	定ノウハウ集	
8.1	手動による NAP クライアント設定	
8.1	1.1 Windows 7、Windows Vista の設定	
8.1	1.2 Windows XP SP3 の設定	112
8.2	コンピュータ認証について	117
付録 A.	. コンフィグレーション	118

1.NAP 検疫概要

1.1 検疫ネットワークとは

検疫ネットワークとは、社内 LAN に接続するコンピュータにセキュリティコンプライアンスに沿っ た検査を行い、問題があると判断されたコンピュータを社内 LAN から隔離されたネットワークに収容 し、問題が無いと判断されたコンピュータのみ社内のネットワークやリソースへの接続を許可する仕組 みのことです。

検疫ネットワークは主に以下の3要素で構成されます。

·検疫機能:

ネットワークに接続しようとしている端末についてのセキュリティ状態を検査する機能。

·隔離機能:

検疫によって不合格とされた端末について、基幹のネットワークと分離させる機能。

·治療機能:

隔離された端末に対して治療を施しセキュリティ状態を正常に回復させる機能。

検疫ネットワークにより、社外から持ち込まれたウイルスに感染したノート PC や最新のセキュリティパッチ未対応などによるセキュリティ対策が不十分な端末等は、対策を施さない限り社内のネットワ ークに接続できないため、社内 LAN のセキュリティを強化する事ができます。



図 1.1-1 検疫ネットワークの要素

1.2 NAP (Network Access Protection)

1.2.1 概要

Network Access Protection (以下 NAP) とは、Windows 7、Windows Vista、Windows XP SP3 およ び Windows Server 2008の各オペレーティングシステムに組み込まれたポリシーベースの検疫プラッ トフォームです。NAP では、ネットワークに接続する前のコンピュータに対し、システム正常性を検証 することによって、セキュリティポリシーに準拠していないコンピュータをアクセス制限付きネットワ ークに隔離する事ができます。また、セキュリティポリシーの準拠を強制することで、社内 LAN やネ ットワークリソースの保護を強化します。

1.2.2 NAP 実施オプション

NAP を実現する方法として、5 つのオプションが用意されています。これを NAP 実施オプションと いい、いずれか 1 つを選択する必要があります。また、複数の組み合わせも可能です。NAP 実施オプシ ョンのセキュリティレベルや保護方法はそれぞれ異なり、NAP を導入する環境に合わせて選択します。 NAP 実施オプションを以下に示します。

項 番	実施オプション	実施ポイント	アクセス制限・許可の方式
1	DHCP (動的ホスト構成プロ	DHCP サーバ	検証結果に応じて、IP アドレスを割り
	トコル)		当てる。
2	インターネットプロトコル	正常性登録機関 Web サイト	検証結果に応じて、証明書を発行する。
	セキュリティ(IPsec)		
3	IEEE802.1X 認証	IEEE802.1X ネットワーク	検証結果に応じて、接続ポートへ動的
		機器	な VLAN を割り当てる。
4	仮想プライベートネットワ	VPN サーバ	検証結果に応じて、パケットフィルタ
	ーク(VPN)		リングを行う。
5	ターミナルサービスゲート	ターミナルサービスゲート	検証結果に応じて、ターミナルサーバ
	ウェイ	ウェイサーバ	への中継を行う。

表 1.2-1 NAP 実施オプション

アラクサラネットワークスでは、IEEE802.1X 実施オプションの NAP を推奨しています。

1.2.3 NAP 構成要素とセキュリティ検査項目

(1) NAP 構成要素

NAP は以下の機器により構成されます。

- ネットワークポリシーサーバ(NPS)
 - ▶ NAP クライアントのセキュリティ状態を検証し、セキュリティポリシーに準拠していない 場合は、制限されたネットワークアクセスを適用する。
- NAP クライアント
 ➢ IPsec や IEEE802.1X 認証などを使用したセキュアな通信をサポートするコンピュータ。
- (2) システム正常性コンポーネント

NAP は以下 2 つのシステム正常性コンポーネントにより、アクセス端末に対してセキュリティポリシーに準拠しているかどうかを確認します。

- システム正常性エージェント(SHA)
 > Windows 7、Windows Vista、Windows XP SP3 に搭載
- システム正常性検証ツール(SHV)
 > Windows Server 2008 に搭載
- (3) セキュリティ検査項目

Windows Server 2008 に標準搭載されている SHV(Windows セキュリティ正常性検証ツール)では、以下の正常性ポリシーを設定することができます。

- Windows ファイアウォール有効の準拠
- 自動更新有効の準拠
- セキュリティ更新プログラムの適用状況の準拠
- ウイルス対策の準拠
- スパイウェア対策の準拠

SHV および SHA については、公開済みの API セットを認識するサードパーティ製のソフトウェアと 相互運用することにより、正常性ポリシーの拡張を可能にしています。 本ガイドでは、Windows Server 2008 標準の SHV を対象にシステム構築をしています。 詳細につきましては、下記 Microsoft のホームページを参照して下さい。

- Windows Server 2008 のネットワークアクセスプロテクション(NAP)
 http://www.microsoft.com/japan/windowsserver2008/network-access-protection.mspx
- Microsoft TechNet Network Access Protection(英語) <u>http://technet.microsoft.com/en-us/network/bb545879.aspx</u>

1.3 AX と NAP の連携

AX シリーズの IEEE802.1X 認証と NAP を連携する事で、社内 LAN に接続する端末の認証および検 疫が可能です。AX シリーズは、NAP と連携可能な IEEE802.1X 動的 VLAN モードおよび IEEE802.1x 固定 VLAN モードをサポートしています。

認証モードの表記については、マニュアルでは AX シリーズ毎に若干の違いがありますが、本ガイド 上ではシリーズ毎に依存しない表記としています。本ガイドと製品マニュアルでの認証モード表記の対 応について以下の表に示します。

本ガイド上の モード表記			製品マニュアル上の表記			
		認証方式	AX1200S AX2200S AX2500S	AX2400S AX3600S	AX6000S	
	固定 VLAN (ポート単位)	IEEE802.1X 認証 ポート単位	ポート単位認証 (静的)	ポート単位認証	ポート単位認証	
	固定 VLAN (VLAN 単位)	IEEE802.1X 認証 VLAN 単位	_	VLAN 単位認証 (静的)	VLAN 単位認証 (静的)	
固定 VLAN (*3)		Web 認証	固定 VLAN モード	固定 VLAN モード	固定 VLAN モード	
		MAC 認証	固定 VLAN モード	固定 VLAN モード	固定 VLAN モード	
動的 VLAN		IEEE802.1X 認証	ポート単位認証 (動的)	VLAN 単位認証 (動的) ^(*1)	VLAN 単位認証 (動的) ^(*1)	
		Web 認証	ダイナミック VLAN モード	ダイナミック VLAN モード	ダイナミック VLAN モード	
		MAC 認証	ダイナミック VLAN モード	ダイナミック VLAN モード	ダイナミック VLAN モード	
		IEEE802.1X 認証	VLAN 単位認証 (動的) ^(*2)	VLAN 単位認証 (動的) ^(*1)	VLAN 単位認証 (動的) ^(*1)	
レガ	ッガシーモード	Web 認証	レガシーモード ^(*2)	レガシーモード	レガシーモード	
		MAC 認証	レガシーモード ^(*2)	—	—	

表1-1 認証モードの表記

- : 未サポート

(*1) AX2400S、AX3600S、AX6000S の IEEE802.1X 認証(VLAN 単位認証(動的))は同一装置内で Web 認証または MAC 認証の動的 VLAN と併用した場合、動的 VLAN として動作します。 また装置で IEEE802.1X 認証(VLAN 単 位認証(動的))を単独で用いた場合、レガシーモードとして動作します。

(*2) AX2530S では未サポートです。

(*3) 本ガイドでの IEEE802.1X 認証における「固定 VLAN」のみの表記は、固定 VLAN(ポート単位)と固定 VLAN(VLAN 単位)の双方を含むものとします。

IEEE802.1X 動的 VLAN モードでは、ユーザ毎に VLAN の設定が可能で、所属する VLAN 毎にアクセ ス許可・遮断が可能なシステムが可能です。また、IEEE802.1X 固定 VLAN モードでは、既存システム の VLAN 構成を変更することなく、固定 IP 環境で検疫システムを構築することが可能です。

1.3.1 IEEE802.1X 動的 VLAN モード

(1) 概要

IEEE802.1X 動的 VLAN モードではその検疫結果により端末が所属する VLAN を動的に割り当てる事ができます。AX シリーズと NAP システムにおける検疫および隔離動作の概要を下図に示します。



図 1.3-1 AX シリーズとNAP システムによる検疫動作(動的 VLAN モード)

AX シリーズのサポートする IEEE802.1X 認証と NAP により、検疫ネットワークの要素は以下の様になります。

·認証機能: IEEE802.1X 認証によるユーザ認証(EAP-PEAP)を行う。

・検疫機能:NPSのSHVとNAPクライアントのSHAによるシステム正常性の確認を行う。

·隔離機能:検疫結果と連動し、動的に端末を検疫 VLAN へ所属させる。

·治療機能:隔離された端末に対し、NPSの自動修復機能による治療を行う。

(2) 検疫シーケンス

IEEE802.1X 認証を使用した NAP では、NAP クライアントの検疫情報を認証シーケンス中の EAP パ ケット(PEAP の TLV メッセージ)にてサーバと交換します。そのため、認証・検疫の連続動作が可能 です。

以下に一連の認証・検疫シーケンスの例と、検疫要素の機能を示します。



図 1.3-2 NAP シーケンス(動的 VLAN モード)

A) 認証機能:

フェーズ①、②、③全てで実施。

IEEE802.1X 認証(EAP-PEAP)により、ネットワークにアクセスするユーザの認証を行う。 フェーズ①ではネットワーク接続時に NAP クライアントから EAPOL-Start が送信され、認証 シーケンスを開始する。

B) 検疫機能:

フェーズ①、②、③全てで実施。

NAP クライアントは IEEE802.1X 認証時、PEAP の TLV メッセージ内に検疫情報を入れて送 信する。NPS はセキュリティポリシーに合致しているかを確認する。

C) 隔離機能:

フェーズ②にて実施。

NAP クライアントでセキュリティ状態が変化した場合、NAP クライアントはすぐに認証シー ケンスを開始し、現在のセキュリティ状態を NPS に伝える。 NPS はセキュリティポリシーに合致しているかを確認し、セキュリティポリシーを満たしてい ない場合は、その NAP クライアントを検疫 VLAN (VLAN30) に所属させる。

D) 治療機能

フェーズ③にて実施。

NPS にて自動修復機能が有効な場合、セキュリティポリシーを満たさない NAP クライアントのセキュリティ状態を強制的に修復させることができる。

フェーズ③の NAP クライアントでは強制的にセキュリティ状態が変更され、再度認証シーケンスを開始する。認証が成功すると、認証後 VLAN に切り替わる。

1.3.2 IEEE802.1X 固定 VLAN モード

(1) 概要

IEEE802.1x 固定 VLAN モードでは、検疫機能でポリシーに合致した端末のみフルアクセス通信を許可し、違反を検出した端末は、認証専用 IPv4 アクセスリストで設定した範囲のみアクセスを許可します。

AX シリーズと NAP システムにおける検疫および隔離動作の概要を下図に示します。



図 1.3-3 AX シリーズと NAP システムによる検疫動作(固定 VLAN モード

AX シリーズのサポートする IEEE802.1X 認証と NAP により、検疫ネットワークの要素は以下の様になります。

·認証機能: IEEE802.1X 認証によるユーザ認証(EAP-PEAP)を行う。

·検疫機能:NPSのSHVとNAPクライアントのSHAによるシステム正常性の確認を行う。

·隔離機能:検疫結果と連動し、アクセス範囲を制限する。

·治療機能:隔離された端末に対し、NPSの自動修復機能による治療を行う。

(2) 検疫シーケンス

IEEE802.1x 固定 VLAN を使用する場合、NPS に検疫不合格時に通知する Filter-Id 属性に認証専用 IPv4 アクセスリスト名を設定します。AX は NPS から通知される RADIUS Accept メッセージ内の Filter-Id 属性を判断し NAP クライアントに許可するアクセス範囲を制御します。以下に一連の認証・検疫シー ケンスの例と検疫要素の機能を示します。



※シーケンスは一部省略されています。

図 1.3-4 NAP シーケンス(固定 VLAN モード)

A) 認証機能:

フェーズ①、②、③全てで実施。

IEEE802.1X 認証(EAP-PEAP)により、ネットワークにアクセスするユーザの認証を行う。 フェーズ①ではネットワーク接続時に NAP クライアントから EAPOL-Start が送信され、認証 シーケンスを開始する。

B) 検疫機能:

フェーズ①、②、③全てで実施。

NAP クライアントは IEEE802.1X 認証時、PEAP の TLV メッセージ内に検疫情報を入れて送 信する。NPS はセキュリティポリシーに合致しているかを確認する。

C) 隔離機能:

フェーズ2にて実施。

NAP クライアントでセキュリティ状態が変化した場合、NAP クライアントはすぐに認証シー ケンスを開始し、現在のセキュリティ状態を NPS に伝える。 NPS はセキュリティポリシーに合致しているかを確認し、セキュリティポリシーを満たしてい ない場合は、その NAP クライアントに認証専用 IPv4 アクセスリストを通知し、AX はアクセ ス範囲を制限する。

D) 治療機能

フェーズ③にて実施。

NPS にて自動修復機能が有効な場合、セキュリティポリシーを満たさない NAP クライアントのセキュリティ状態を強制的に修復させることができる。

フェーズ③の NAP クライアントでは強制的にセキュリティ状態が変更され、再度認証シーケンスを開始する。認証が成功すると、認証後フルアクセスを許可する。

1.3.3 IEEE802.1X 動的 VLAN モードと固定 VLAN モードのまとめ

NAP 連携時の IEEE802.1x 動的 VLAN モードと固定 VLAN モードそれぞれの機能を下表に示します。

項目	動的 LAN モード	固定 VLAN モード
VLAN 種別	MAC VLAN	ポート VLAN
認証および検疫の	NAP クライアント端末の所属する VLAN	NAP クライアント端末のアクセス
各状態の切り替え	を切り替える。	範囲を切り替える。
方法		
RADIUS からの検疫	VLAN ID	認証専用 IPv4 アクセスリスト名
結果通知	(Tunnel-Pvt-Group-Id)	(Filter-Id)
DHCP との連携	必須	任意(固定 IP でも可)
サポート機種	AX1200S/AX2200S/AX2400S/AX2500S/	AX1240S/AX2200S/AX2400S
	AX3600S/AX6300S/AX6700S	AX2500S/AX3600S

表 1-2 動的 VLAN モードと固定 VLAN モードの NAP 連携機能

各状態での NAP クライアント端末の所属 VLAN およびアクセス可能範囲を下表に示します。

表 1-3 各状態での NAP クライアント端末の所属 VLAN およびアクセス可能範囲

NAP クライアント	動的 VLAN -	モード	固定 VLAN モード		
端末の状態	所属 VLAN	アクセス可能範囲	所属 VLAN	アクセス可能範囲	
認証 NG	認証前	認証専用 IPv4 アクセス		認証専用 IPv4 アクセス	
	VLAN	リストの設定範囲		リストの設定範囲	
検疫 NG	検疫 VLAN	検疫 VLAN の設定範囲	技術化 トク	認証専用 IPv4 アクセス	
				リストの設定範囲	
検疫 OK	ユーザ毎	フルアクセス可能(*1)	VLAN	フルアクセス可能(*1)	
	の認証				
	VLAN				

(*1):所属する VLAN にフィルタ設定している場合は、そのフィルタ条件に従います。

1.4 Active Directory との連携

1.4.1 Windows ドメイン環境との共存

(1) 従来の Windows ドメイン参加のしくみ

Active Directory の Windows ドメインに参加しているコンピュータは、OS を起動すると、Windows ドメインリソースへのアクセス認証を行い、Windows ドメインヘログオンすることができるように なります。Windows ドメインにログオンすると、Windows ドメイン内のリソースへのアクセスが可 能になります。また、複数のユーザやコンピュータに共通の設定を行うことができるグループポリシ ーを適用することができます。

(2) IEEE802.1X 認証を使う場合の Windows ドメイン連携

通常、Active Directory のドメインコントローラとクライアント端末との間には、数台のスイッチ が接続されますが、そのうちの1台を IEEE802.1X 認証スイッチとして設定します。

Windows ドメイン環境と IEEE802.1X 認証環境を共存させる場合、ユーザがログオンする前に、 コンピュータのレベルでドメインコントローラと通信ができる必要があります。事前にドメインコン トローラと通信ができないと、以下の現象が発生します。

- ・ コンピュータに適用されるグループポリシー情報(<u>1.4.2</u>参照)を、起動の時点で適用することができない
- 一度も該当コンピュータにログオンしたことがなく、また認証情報がコンピュータにキャッシュされていないユーザアカウントでのログオンができない
- ・ 新しいコンピュータを Windows ドメインに参加させることができない

AX シリーズでは、認証前 VLAN を用いることで、ドメインコントローラとの接続性を確保することができます。

1.4.2 グループポリシーを用いた NAP クライアント自動設定

Active Directory のグループポリシーを用いると、認証・検疫を行う前のコンピュータへ NAP クライ アント設定を一括して行うことができます。これにより、NAP 初期導入が容易になります。

Windows 7、Windows Vista では GUI を使って NAP 設定を行いますが、Windows XP SP3 では NAP 設定をするための GUI が用意されていません。(8.1参照) このため、NAP の初期設定をするにはコマ ンドラインからの設定が必要になり、ユーザの設定コストが大きくなります。Active Directory のグルー プポリシーを用いると、管理者が一律に NAP クライアントの設定を行うことができ、ユーザの設定コ ストを低減できます。

1.5 AX と NAP 検疫の特徴

1.5.1 NAP 検疫の特徴

NAP 検疫の特徴を以下に示します。

(1) シングルサインオンが可能

Windows へのログオン情報、Windows ドメインへのログオン情報およびネットワーク認証情報を 共通化できるので、ユーザ ID とパスワードを1回入力するだけで、認証・検疫まで自動制御が可能 になります。

(2) 隔離機能の安定性

IEEE802.1x 動的 VLAN モードでは、DHCP クライアント機能と連動するため、検疫時の動的 VLAN 切替にも IP アドレスの切替が安定して動作します。(図 1.3-2参照)

(3) 初期導入が容易

Active Directory による Windows ドメイン管理と併用することで、NAP クライアント設定を一括して行うことができます。

1.5.2 AX シリーズを用いた NAP 検疫システムの特徴

AX シリーズと NAP 検疫の特徴を以下に示します。

(1) IEEE802.1X 認証を契機とした検疫による、ユーザ毎のセキュリティ管理

1ポートに複数の端末が接続されている環境でも、PC単位の制御が可能になります。

(2) 認証・検疫ネットワークへの移行環境の提供

AX シリーズでは、IEEE802.1X 認証端末、Web 認証端末および MAC 認証端末をポート内又はポ ート単位で混在できるので、NAP に対応している端末と認証のみの端末との混在が可能です。これ により、例えば、部署単位での NAP 検疫システムの導入が可能になります。

(3) アラクサラのシングルサインオンソリューション

AX シリーズがサポートしている認証前 VLAN を用いることにより、IEEE802.1X 認証によるネットワーク認証の前に、ドメインコントローラによるアクセス認証を行うことができます。(<u>1.4.1</u>参照)

(4) 動的 VLAN モードと固定 VLAN モードの両方式を提供

AX シリーズは、従来の動的 VLAN モードに加えて固定 VLAN モードをサポートしました。 各方式の適用

> ・動的 VLAN モード:ユーザ毎に個別に VLAN の設定が可能で、所属する VLAN 毎に サーバへのアクセス許可・遮断設定ができます。

> > 例えばアクセス権限の違うユーザが混在する環境下で有効な方式 です。

・固定 VLAN モード: 既存システムの VLAN 構成を変更することなく検疫システムの構築ができます。また、固定 IP 環境で利用可能です。

例えばフロア毎にアクセス制御が異なる環境下で有効な方式です。

これによりお客様ニーズに合わせた検疫システムを柔軟に構築することができます。

1.6 オペレーションシステムによる差分について

ここでは本ガイドで作成するNAP検疫システムにてオペレーションシステムによる設定手順や設 定内容に差分がある箇所を一覧にして示します。

1.6.1 Windows Server 2008 R2 と Windows Server 2008 の差分

Windows Server 2008 R2 と Windows Server 2008 では設定画面のデザインや設定方法が一部異 なります。本ガイドは Windows Server 2008 R2 ベースで記述し設定画面や設定内容に差分がある箇 所については両方の設定方法を記述しています。以下に本ガイド内で設定に差分がある箇所を示し ます。

- <u>「3.5.2 グループポリシーの設定」</u>の(3)、(4)、(5)の設定画面
- <u>「3.5.4 RADIUS クライアントの設定」</u>の設定画面
- <u>「3.5.5 接続要求ポリシーの設定」</u>の⑨処理順序の変更
- <u>「3.5.6 システム正常性検証ツール(SHV)の設定」</u>の設定画面
- <u>「3.5.7 正常性ポリシーの設定」</u>の設定画面

1.6.2 Windows 7、Windows Vista、Windows XP(SP3)の差分

本ガイドでは NAP クライアントとして Windows 7、Windows Vista、Windows XP(SP3)の設定 手順を示しています。本ガイド内で各クライアントのオペレーションシステムによる設定画面や 設定内容及び動作に差分がある箇所を以下に示します。

- 「3.5.6 システム正常性検証ツール(SHV)の設定」のWindows セキュリティ正常性検証ツールにて Windows XP(SP3)のみ「スパイウェア対策」のチェックをサポートしていません。
 Windows 7 と Windows Vista は「スパイウェア対策」のチェックをサポートしています。
- 「1.1.3.6.2 Windows ドメイン参加の設定」にて Windows XP(SP3)のみドメイン参加時再起 動が 2 回必要です。Windows 7 と Windows Vista は 1 回の再起動で設定が完了します。
- <u>「6.1.1 Windows XP の IP アドレス切り替え問題」</u>にて Windows XP(SP3)のみ IP アドレス 切り替えの契機が異なるため対策が必要です。なお Windows 7 と Windows Vista は同じ仕様 でありこの対策を行う必要はありません。
- 「8.1 手動による NAP クライアント設定」にて Windows XP(SP3)のみ GUI の設定に加えコ マンドプロンプトでのコマンド投入が必要です。Windows 7 と Windows Vista は GUI のみで 本設定を完了できます。
- 「8.2 コンピュータ認証について」にてクライアント端末からコンピュータ認証を停止する 場合、Windows 7 のみコンピュータ認証の停止を GUI で設定することが可能です。Windows Vista と Windows XP(SP3)は設定ファイルのインポートを行う必要があります。

2. AX シリーズの収容条件

本ガイドの検疫ネットワークでは、AX シリーズの IEEE802.1X 認証方式を使用しています。AX シリーズのサポートする認証モード毎の最大認証端末数を以下に示します。なお認証モードの表記については 1.3 も合わせて参照下さい。

NAPと連携可能な AX シリーズの認証方式を以下に示します。

表 2-1 NAPと連携可能な認証方式

認証方式	認証モード	AX1230S	AX1240S AX2200S AX2500S	AX2400S AX3600S	AX6300S AX6700S
IEEE802.1X	固定 VLAN	—	0	0	—
認証	動的 VLAN	0	0	0	0
\//。。 =刃 =正	固定 VLAN	—	—	—	—
VVED 認証	動的 VLAN	—	—	—	—
	固定 VLAN	_	_	—	_
IVIAC 認証	動的 VLAN	—	—	—	—

(凡例) 〇:検疫連携可能 △:検疫連携可能予定 -:検疫連携不可

検疫ネットワークのみを構成する場合は、太枠で示した数値まで端末を収容することができます。

認証方式	認証 モード	AX1200S AX2200S		AX2500S		AX2400S AX3600S		AX6300S AX6700S	
IEEE802.1X 認証	固定 VLAN (ポート単位)	64/ ポート ^(*2)	合計 256/	1024/ ポート	合計 1024/	64/ ポート	合計 1024/	256/ ポート	合計
	固定 VLAN (VLAN 単位)	×	之50/ 装置 ^(*2)	×	1024/ 装置	256/ VLAN	1024/ 装置	256/ VLAN	4090/ 装置
	動的 VLAN	256/	装置	1000/装置		1024/装	置 ^(*1)	4096/装	置
MAC 認証	固定 VLAN	1024/装置		1024/装置		1024/装置		4096/装置	
	動的 VLAN	256/装置		1000/装置		×		×	
Web 認証	固定 VLAN	1024/	'装置	1024/	 	1024/装置		4096/装置	
	動的 VLAN	256/	6/装置 1000		接置 1024/装置 ^(*1)		4096/装置		

表 2-2 認証モード毎の最大認証端末数

(凡例) ×: 未サポート

(^{*1)}AX3630Sでは256/装置となります。

^(*2)AX1230S では固定 VLAN の NAP 連携は未サポートです。

3. *検疫ネットワークの構築(動的 VLAN 構成)*

本章では、AX シリーズを用いた検疫ネットワークの構築例を示します。

3.1 概要

検疫ネットワークの動的 VLAN 構成を、以下のように定義します。



図 3.1-1 検疫ネットワークの構成(動的 VLAN 構成)

コアスイッチには AX3600S を配置し、VRRP を用いて装置を冗長化します。また、装置間はリンク アグリゲーションを用いて回線を冗長化します。

NPS として稼動する Windows Server 2008、検疫により隔離された端末を治療する修復サーバ、および検疫後にアクセス可能な業務サーバは、コアスイッチ配下に接続します。コアスイッチ同士の経路交換には、OSPF 等のルーティングプロトコルを使用します。

認証スイッチにはAX2400SおよびAX1200Sを配置し、IEEE802.1x動的VLANモードで認証を行い、 スパニングツリーを用いて冗長化します。

検疫を行う端末は、認証スイッチに直接またはハブを介して接続します。

本ガイドで使用したサーバとクライアント端末を以下に示します。

表 3-1 サーバとクライアント一覧

Windows Server 2008	NAP クライアント 端末	修復サーバ	業務サーバ
 ・ドメインコントローラ •DNS サーバ •DHCP サーバ •NPS (Network Policy Server) 	Windows 7 Windows Vista Windows XP SP3	ウイルス対策ソフト のダウンロード用 サーバ	ファイル共有 サーバ

3.2 検疫ネットワーク構成図





図 3.2-1 検疫ネットワーク構成図(動的 VLAN 構成)

ここで、認証スイッチのポートを以下のように設定します。

表 3-2 認証スイッチのポート設定

認証 スイッチ	用途	ポート番号	ポート種別	認証方式	認証前 VLAN	検疫 VLAN	認証後 VLAN
A V 2400S	認証用	0/1~0/10	MAC VLAN ポート	IEEE802.1X 認証 (動的 VLAN)	10	30	100
AX24005 上 2	上位スイッチ との通信用	0/47~0/48	トランク ポート	_			
A V1200S	認証用	0/1~0/10	MAC VLAN ポート	IEEE802.1X 認証 (動的 VLAN)	10	30	100
AA12003	上位スイッチ との通信用	0/25~0/26	トランク ポート				

各 VLAN の定義および VLAN とサーバ間通信の可否を以下の表に示します。

表 3-3 VLAN の定義

VLAN 名	VLAN ID	ネットワーク IP アドレス	用途	設置サーバ
業務サーバ用	50	10.50.0.0/24	検疫後に通信可能なサーバが所属する	業務サーバ
VLAN			VLAN。	
Windows Server	51	10.51.0.0/24	NPS、ドメインコントローラ、DHCP な	Windows
2008 用 VLAN			どのサービスが稼動している Windows	Server 2008
			Server 2008 が所属する VLAN。	
修復サーバ用	52	10.52.0.0/24	検疫により隔離された端末を修復する	修復サーバ
VLAN			ためのサーバが所属する VLAN。	
認証前 VLAN	10	192.168.10.0/24	端末がネットワーク認証を行う前に所	_
			属する VLAN。認証に失敗した場合も本	
			VLAN に所属する。	
検疫 VLAN	30	192.168.30.0/24	認証は成功したが、検疫により隔離され	_
			た端末が所属する VLAN。	
			修復サーバのみと通信可能。	
認証後 VLAN	100	192.168.100.0/24	認証および検疫が成功した端末が所属	—
			するVLAN。	
管理用 VLAN	1000	172.16.0.0/24	各装置を管理するための VLAN。	

表 3-4 VLAN-サーバ間通信の可否

送信元	送信先	業務サーバ	Windows Server 2008	修復サーバ
認証前 VLAN	10	×	0	×
検疫 VLAN	30	×	0	0
認証後 VLAN	100	0	0	0

Windows ドメイン名と、そのドメインに適用するグループポリシーを以下の表に示します。

表 3-5 Windows ドメイン名とグループポリシー

W	indows ドメイン名	
ex	ample.co.jp	
グ	゚ループポリシー	
1	システムサービスの構成	NAP クライアントとして必要なサービスを自動起動させる。
2	ネットワークポリシーの構成	EAP の構成やシングルサインオンの設定を構成する。
3	NAP クライアントの構成	NAP クライアントが実施する検疫方法を IEEE802.1X 認証に
		指定する。
4	セキュリティセンターの構成	セキュリティセンターを有効にする。

3.3 構築ポイント

図 3.2-1の検疫ネットワーク構成図について、構築のポイントを以下に示します。

3.3.1 AX に関する構築ポイント

認証スイッチおよびコアスイッチの設定について、必須項目と推奨項目を示します。必須項目は検疫 を行う上で必要な項目、推奨項目はネットワークを構築する上で注意すべき項目となっています。

必須項目

(1) 運用前の事前設定を行う。

・AX1230S のみ

運用前にシステムファンクションリソース配分を変更してフィルタ機能と拡張認証機能を有効 にします。設定変更後は装置の再起動が必要です。

·AX1200S

MACVLAN を使用する認証スイッチにレイヤ2ハードウェアテーブルの検索方式をオートに設定します。設定変更後は装置の再起動が必要です。

·AX2400S

MACVLAN を使用する認証スイッチにレイヤ2ハードウェアテーブルの検索方式をオートに設定します。設定変更後は VLAN プログラムの再起動が必要です。

(2) 認証前 VLAN をアップリンク側のポートに追加する。

ユーザ認証前に Windows ドメインヘログオンするため、認証前 VLAN から Windows Server 2008(ドメインコントローラ)へ通信ができるよう、認証前 VLAN をアップリンク側のポートに追加します。

(3) 認証ポートにフィルタを設定する。

認証の設定を行ったポートは、認証前のすべての通信が遮断されます。認証前に通信を行いた い場合は、認証専用アクセスリストを作成してポートに適用します。また、ARP リレーの設定も 必要です。

本ガイドでは、<u>表 3.2-3</u>に示す通信が可能な認証専用アクセスリストを作成して、認証ポートに 適用しています。

- (a) Windows Server 2008「10.51.0.1」への通信を許可する
- (b) DHCP 通信を許可する

(4) 検疫 VLAN を決める。

検疫 VLAN は、IEEE802.1X 認証で動的に切り替わる VLAN になります。認証後 VLAN も動的に 切り替わる VLAN ですが、検疫 VLAN にフィルタを設定することで認証後 VLAN と区別します。 本ガイドでは、VLAN30 を検疫 VLAN としています。 (5) 検疫 VLAN にフィルタを設定する。

表 3.2-3 に示すように、検疫 VLAN に所属する端末は Windows Server 2008(ドメインコントローラ)および修復サーバと通信可能です。この他に、IP アドレスを取得するため DHCP 通信を許可する必要があります。

本ガイドでは、次のアクセスリストを作成して、認証スイッチの検疫 VLAN30 に適用しています。

- (a) Windows Server 2008「10.51.0.1」との通信を許可する
- (b) 修復サーバ「10.52.0.1」との通信を許可する
- (c) DHCP 通信を許可する
- (6) 認証スイッチと端末との間にハブを設置する場合、EAPOL フォワーディング機能のあるハブ を用いる。

IEEE802.1X 認証を行うため、認証スイッチと端末との間に設置するハブには EAPOL フォワー ディング機能が必要です。AX1200S には EAPOL フォワーディング機能が実装されています。

(7) デフォルトルートを設定する。

Windows Server 2008 と通信を行うため、認証スイッチにデフォルトルートを設定します。

推奨項目

(8) 認証スイッチの IEEE802.1X 端末検出機能を auto に設定する。

認証スイッチの IEEE802.1X 端末検出機能 auto に設定します。ただし、AX1230S の場合、auto 機能未サポートのため disable(停止)と設定して下さい。(詳細は、「認証ソリューションガイド」 を参照して下さい。)

(9) 認証スイッチの非認証状態保持時間を調整する。

IEEE802.1X 認証機能を有効に設定した Windows 端末は、起動時にコンピュータの IEEE802.1X 認証を行い、ユーザログオン時にユーザの IEEE802.1X 認証を行います。本ガイドの検疫ネット ワークでは、コンピュータの認証が失敗する構成のため、次のユーザ認証が行えるようになるま で非認証状態保持時間(デフォルト値:60秒)かかります。デフォルト値のままではユーザ認証 が失敗する場合があるので、短い値に設定します。本ガイドでは、非認証状態保持時間を5秒に 設定しています。(詳細は注意事項「6.2.1非認証状態保持時間の設定について」を参照)

(10) RADIUS サーバ通信 dead interval 時間を調整する。(AX1200S)

RADIUS サーバへの認証がタイムアウトした場合、2 台目以降に設定された RADIUS サーバへ 切替えます。その後再び1 台目の RADIUS サーバを選択するまでの時間(dead interval)のデフォ ルト値は10 分です。RADIUS サーバが1 台のみで構成されるシステムにおいて、RADIUS サー バのタイムアウトを検出すると dead interval に設定された時間 RADIUS サーバへのアクセスを行 いません。RADIUS サーバが1 台で構成される場合、dead interval を短い値に設定してください。 本ガイドでは dead interval を0 分に設定しています。なお、AX2400S/AX3600S の IEEE802.1X 認証では常に1 台目に設定した RADIUS サーバより認証を始めます。 (11) コアスイッチ間の回線にリンクアグリゲーションを設定する。 コアスイッチ間の回線を冗長化するため、リンクアグリゲーションを設定します。本ガイドで はスタティックモードを用いています。

(12) マルチプルスパニングツリーを使用する。

AX シリーズではデフォルトで PVST+が動作していますが、MAC VLAN では PVST+を使用する ことができないため、シングルスパニングツリーもしくはマルチプルスパニングツリーを使用し ます。本ガイドでは、VLAN 数が増加した時に柔軟性が高いマルチプルスパニングツリーを使用 しています。また、認証スイッチの認証用ポートは、スパニングツリー対象外とします。

(13) VRRP のマスタ、STP のルートブリッジを設定する。

本ガイドでは、core#1の仮想ルータ優先度を「200」、core#2の優先度を「100」として、core#1 をマスタに設定しています。また、core#1のブリッジ優先度を「4096」、core#2のブリッジ優先 度を「8192」として、core#1をルートブリッジに設定しています。

(14) 認証後の DHCP の設定をする。

認証後、DHCP サーバから IP アドレスを取得するため、コアスイッチに DHCP リレーエージ ェントによる転送先アドレスの設定をします。また、DHCP サーバ側の設定で、配布するデフォ ルトゲートウェイを VRRP の仮想ルータアドレスに設定する必要があります。

3.3.2 Windows Server 2008 に関する構築ポイント

Windows Server 2008 の設定について、注意すべき項目を示します。

推奨項目

(1) グループポリシーを作成する。

NAP クライアント設定を一括して行うために、グループポリシーを使用します。設定方法は後述の「3.5.2グループポリシーの設定」を参照してください。

3.4 AX の設定

3.4.1 AX1200S のコンフィグレーション

AX1200S シリーズの設定例を示します。

(1) 事前設定

AX1230S のみ設定	
システムファンクションリソース配分の設定	
(config)# system function filter extended-authentication	フィルタ機能と拡張認証機能を使用するため、システ ムファンクションリソース配分を変更します。 ※本設定は AX1230S のみ必要で設定後は、装置の再 起動が必要です。
AX1200S シリーズの設定	
レイヤ2ハードウェアテーブルの設定	
(config)# system l2-table mode auto	レイヤ2ハードウェアテーブルの検索方式をオートに 設定します。※設定後は、装置の再起動が必要です。

(2) 基本設定

AX1200S シリーズの設定	
ポート VLAN の設定	
(config)#vlan 1	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config-ylan)# name BeforeAuthVIAN	認証前 VLAN として VLAN10 を、管理用 VLAN として
(config)# vlan 1000	VLAN1000 を作成します。
(config-vlan)# name ManagedVLAN	
MAC VLAN の設定	
(contig)# vlan 30 mac-based	検疫 VLAN として MAC VLAN30 を、認証後 VLAN とし
(config) # vlan 100 mac-based	て MAC VLAN100 を作成します。
(config-vlan)# name OkVLAN	▶ 構築ポイント <u>(4)</u>
スパニングツリーの設定	
(contig) # spanning-tree mode mst	マルチプルスパニングツリーを有効にし、リージョン、
(config)# spanning-tree mode mst (config)# spanning-tree mst configuration	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1
<pre>(config) # spanning-tree mode mst (config) # spanning-tree mst configuration (config-mst) # name NAP (config-mst) # revision 1 (config-mst) # instance 1 vlans 100, 1000</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 2 vlans 30</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30 MST インスタンス3:VLAN10
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30 MST インスタンス3:VLAN10
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config)# interface range fastethernet 0/1-10</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30 MST インスタンス3:VLAN10 認証用ポート 0/1~0/10 に対して、スパニングツリーの
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config)# interface range fastethernet 0/1-10 (config-if-range)# spanning-tree portfast</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1: VLAN100、1000 MST インスタンス2: VLAN30 MST インスタンス3: VLAN10 認証用ポート 0/1~0/10 に対して、スパニングツリーの PortFast 機能を適用し、スパニングツリー対象外としま
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config)# interface range fastethernet 0/1-10 (config-if-range)# spanning-tree portfast</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30 MST インスタンス3:VLAN10 認証用ポート 0/1~0/10 に対して、スパニングツリーの PortFast 機能を適用し、スパニングツリー対象外としま す。
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# name NAP (config-mst)# revision 1 (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config)# interface range fastethernet 0/1-10 (config-if-range)# spanning-tree portfast</pre>	 マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名: NAP リビジョン番号: 1 MST インスタンス 1: VLAN100、1000 MST インスタンス 2: VLAN30 MST インスタンス 3: VLAN10 認証用ポート 0/1~0/10 に対して、スパニングツリーの PortFast 機能を適用し、スパニングツリー対象外とします。 構築ポイント(12)

物理ポートの設定		
●認証用 (config)# interface range fastethernet 0/1-10 (config-if-range)# switchport mode mac-vlan (config-if-range)# switchport mac vlan 30,100 (config-if-range)# switchport mac native vlan 10	ポート 0/1~0/10 を、MAC VLAN ポートとして設定しま す。 MAC VLAN ポートに VLAN30 および 100 を、Native VLAN として VLAN10 を設定します。 ▶ 構築ポイント <u>(4)</u>	
●上位スイッチとの通信用 (config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 10, 30, 100, 10	 ポート 0/25~0/26 を、上位スイッチと通信するトランクポートとして設定します。 トランクポートに VLAN10、30、100 および 1000 を設定します。 ▶ 構築ポイント(2) 	
インタフェースの設定		
(config)# interface vlan 1000 (config-if)# ip address 172.16.0.12 255.255.255.0	管理用 VLAN1000 にインタフェース IP アドレスを設定 します。	
RADIUS サーバの設定		
(config)# radius-server host 10.51.0.1 key alaxala (config)# radius-server dead-interval 0	RADIUS サーバの IP アドレスおよびキーを設定します。 本ガイドではキーを「alaxala」としています。 RADIUS サーバの dead interval を 0 に設定します。 構築ポイント<u>(10)</u>	
スタティックルートの設定		
(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254	Windows Server 2008 と通信を行うため、デフォルトル ートを設定します。 ▶ 構築ポイント<u>(7)</u>	

(3) アクセスリストの設定

AX1200S の設定				
認証専用アクセスリストの設定				
<pre>(config)# ip access-list extended JoinDomain AX1230Sの場合 (config-ext-nacl)# permit protocol ip src 192.168.10.0 0.0.0.255 dst 10.51.0.1 0.0.0.0 (config-ext-nacl)# permit udp src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps AX1240Sの場合 (config-ext-nacl)# 10 permit ip 192.168.10.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# 20 permit udp any any eq bootps</pre>	 アクセスリスト「JoinDomain」を作成します。 AX1230Sの場合 ・認証前 VLAN10 から Windows Server 2008 「10.51.0.1」への通信を許可します。 ・DHCP サーバ通信を許可します。 AX1240S の場合 ・認証前 VLAN10 から Windows Server 2008 「10.51.0.1」への通信を許可します。 ・DHCP サーバ通信を許可します。 ・DHCP サーバ通信を許可します。 ▶ 構築ポイント(3) (3) 			
検疫 VLAN 用アクセスリストの設定				
<pre>(config)# ip access-list extended Quarantine AX1230Sの場合 (config-ext-nacl)# permit protocol ip src 192.168.30.0 0.0.0.255 dst 10.51.0.1 0.0.0.0 (config-ext-nacl)# permit protocol ip src 10.51.0.1 0.0.0.0 dst 192.168.30.0 0.0.0.255 (config-ext-nacl)# permit protocol ip src 192.168.30.0 0.0.0.255 dst 10.52.0.1 0.0.0 (config-ext-nacl)# permit protocol ip src 10.52.0.1 0.0.0 dst 192.168.30.0 0.0.0.255 (config-ext-nacl)# permit udp src 0.0.0.0 255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps (config-ext-nacl)# permit udp src 0.0.0.255 ast 255.255 dst</pre>	 アクセスリスト「Quarantine」を作成します。 ・検疫 VLAN30 から Windows Server 2008「10.51.0.1」 への通信を許可します。 ・Windows Server 2008「10.51.0.1」から検疫 VLAN30 への通信を許可します。 ・検疫 VLAN30 から修復サーバ「10.52.0.1」への通信 を許可します。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信 を許可します。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信 を許可します。 ・DHCP サーバ通信を許可します。 ・DHCP クライアント通信を許可します。 			
(config-ext-nacl)# permit ddp src 0.0.0.0255.255.255.255 dst 0.0.0.0255.255.255.255 eq bootpc AX1240Sの場合 (config-ext-nacl)# 10 permit ip 192.168.30.00.0.0.255 host 10.51.0.1 (config-ext-nacl)# 20 permit ip host 10.51.0.1 192.168.30.0	AX1240S の場合 ・検疫 VLAN30 から Windows Server 2008「10.51.0.1」 への通信を許可します。 ・Windows Server 2008「10.51.0.1」から検疫 VLAN30			

AX1200S の設定	
AX1200S の設定 0.0.0.255 (config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 host 10.52.0.1 (config-ext-nacl)# 40 permit ip host 10.52.0.1 192.168.30.0 0.0.0.255 (config-ext-nacl)# 50 permit udp any any eq bootps (config-ext-nacl)# 60 permit udp any any eq bootpc AX1200S共通 (config)# interface vlan 30 (config-if)# ip access-group Quarantine in	 への通信を許可します。 ・検疫 VLAN30 から修復サーバ「10.52.0.1」への通信 を許可します。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信 を許可します。 ・DHCP サーバ通信を許可します。 ・DHCP クライアント通信を許可します。
	検疫 VLAN30 にアクセスリストを適用します。 ▶ 横築ポイント(5)

(4) IEEE802.1X 認証の設定

AX1200S の設定	
RADIUS の設定	
(config)# aaa authentication dot1x default group radius	RADIUS サーバで IEEE802.1X 認証を行うことを設定
	します。
IEEE802.1X 認証の設定	
(config)# interface range fastethernet 0/1-10	ポート 0/1~0/10 に対して、IEEE802.1X 認証を有
(config-if-range)# dot1x port-control auto	効にします。
	認証サブモードを端末認証モードにします。
(config-if-range)# dot1x reauthentication	サプリカントの再認証を有効にし、その周期を
(config-if-range)# dot1x timeout reauth-period 3600	3600 秒に設定します。
(config_if_range) # dat1x timeout quiat_paried 5	
(config=11=fange)# doctx climeour quiet=period 5	非認証状態保持時間を5秒に設定します。
	▶ 構築ボイント <u>(9)</u>
(config-if-range)# dot1x supplicant-detection disable	端 末 検 出 モ ー ト を disable に し て 、
	EAP-Request/Identity の达信を抑止します。
	AX1240S を使用9 る場合は auto に設定して下さ
	い。 横築ポイント (9)
(config-it-range)# authentication ip access-group JoinDomai	□ 認証用ポート 0/1~0/10 に認証専用アクセスリス
	ト [.loinDomain」を適用します。
(config-if-range)# authentication arp-relay	認証前の ARP リレーを設定します。
	▶ 構築ポイント(3)
(config)# dot1x system-auth-control	
	IEEE802.1X 認証を有効にします。

3.4.2 AX2400S のコンフィグレーション

AX2400Sの設定例を示します。

レイヤ2ハードウェアテーブルを検索方式をオートに
設定します。 ※設定後は、VLAN プログラムの再起動
が必要です。
▶ 構築ポイント <u>(1)</u>
VLAN1 は使用しないため、無効にします。
認証前 VLAN として VLAN10 を、管理用 VLAN として
VLAN1000 を作成します。
使役 VLAN として MAC VLAN3U を、認証彼 VLAN と
して MAC VLANTOU をIF成します。
マルチブルスパニングツリーを有効にし、リージョン、
インスタンスを設定します。
リーション名:NAP
リビンヨン奋号:1 MCT インスカンスオーバ(AN1400 - 4000
NIST インスタンス I: VLAINTUU、TUUU MST インスタンス 2: VLAN20
NGT インスタンス 2:VLANOU MST インスタンス 3・VI AN10

(config)# interface range gigabitethernet 0/1-10
(config-if-range)# spanning-tree portfast

	します。	
<u>物理ポートの設定</u>		
●IEEE802.1X 認証(動的 VLAN)用 (config) # interface range gigabitethernet 0/1-10 (config-if-range) # switchport mode mac-vlan (config-if-range) # switchport mac vlan 30,100 (config-if-range) # switchport mac native vlan 10	ポート 0/1∼0/10 を、MAC VLAN ポートとして設定し ます。 MAC VLAN ポートに VLAN30 および 100 を、Native VLAN として VLAN10 を設定します。 ▶ 構築ポイント <u>(4)</u>	
 上位スイッチとの通信用 (config)# interface range gigabitethernet 0/47-48 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 10, 30, 100, 10 	ポート 0/47~0/48 を、上位スイッチと通信するト ランクポートとして設定します。 トランクポートに VLAN10、30、100 および 1000 を設定します。	

MST インスタンス 2: VLAN30 MST インスタンス 3: VLAN10

認証用ポート 0/1~0/10 に対して、スパニングツリー の PortFast 機能を適用し、スパニングツリー対象外と

インタフェースの設定		
(config)# interface vlan 1000 (config-if)# ip address 172.16.0.11 255.255.255.0	管理用 VLAN1000 にインタフェース IP アドレスを設 ニュキオ	
	たしより。	
RADIUS サーバの設定		
(config)# radius-server host 10.51.0.1 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定しま す。本ガイドではキーを「alaxala」としています。	
デフォルトルートの設定		
(config)# ip default-gateway 172.16.0.254	Windows Server 2008 と通信を行うため、デフォルト ルートを設定します。 ▶ 構築ポイント<u>(7)</u>	

(3) アクセスリストの設定

AX2400S の設定		
アクセスリストの設定		
 認証前 VLAN 用 (config)# ip access-list extended JoinDomain	 アクセスリスト「JoinDomain」を作成します。 ・認証前 VLAN10 から Windows Server 2008 「10.51.0.1」への通信を許可します。 ・Windows Server 2008「10.51.0.1」から認証前 VLAN10への通信を許可します。 ・DHCPサーバ通信を許可します。 ・DHCP クライアント通信を許可します。 	
 ●検疫 VLAN 用 (config)# ip access-list extended Quarantine	 アクセスリスト「Quarantine」を作成します。 ・検疫 VLAN30 から Windows Server 2008「10.51.0.1」 への通信を許可します。 ・Windows Server 2008「10.51.0.1」から検疫 VLAN30 への通信を許可します。 ・検疫 VLAN30 から修復サーバ「10.52.0.1」への通信 を許可します。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信 を許可します。 ・BHCP サーバ通信を許可します。 ・DHCP クライアント通信を許可します。 	
(config)# interface vlan 30 (config-if)# ip access-group Quarantine in	検疫 VLAN30 にアクセスリストを適用します。 ▶ <mark>構築ポイント<u>(5)</u></mark>	

(4) IEEE802.1X 認証の設定

AX2400S の設定		
RADIUS の設定		
(config)# aaa authentication dot1x default group radius	RADIUS サーバで IEEE802.1X 認証を行うことを設定	
(config)# aaa authorization network default group radius	します。 RADIUSサーバで IEEE802.1X 認証(動的 VLAN)を行う	
	ことを設定します。	
 IEEE802.1X 認証の設定		
(config)# interface range gigabitethernet 0/1-10	ポート 0/1~0/10 に対して、認証専用アクセスリス	
(config-if-range)# authentication ip access-group JoinDoma	ⁱⁿ ト「JoinDomain」を適用します。	
(config) # dot1x ylon dynamia radius ylon 20,100	▶ 構築ポイント(3)	
(coning)# dotix vian dynamic radius=vian 30,100	認証後動的に切り替わる VLAN を、VLAN30 およ	
	び 100 とします。	
(config)# dot1x vlan dynamic enable	▶ 構築ポイント(4)	
	IEEE802.1X 認証(動的 VLAN)を有効にします。	
(config)# dot1x vlan dynamic reauthentication		
(config)# dot1x vlan dynamic timeout reauth-period 3600	サプリカントの再認証を有効にし、その周期を	
	3600 秒に設定します。	
(config)# dot1x vlan dynamic timeout quiet-period 5	非認証状能保持時間を5秒に設定します	
	→ 構築ポイント (9)	
(config)# dot1x vlan dynamic supplicant-detection auto	端末検出モードを auto にして	
	FAP-Request/Identityの送信を自動します。	
(config)# dot1x system-auth-control	▶ 構築ポイント(8)	
(config)# dot1x logging enable	IEEE802.1X 認証を有効にします。	
	IEEE802.1X 認証ログを syslog に出力します。	
syslog の設定		
(config)# logging host 192.168.0.1	syslog サーバの IP アドレスを設定します。	
(config) # logging event-kind err, evt, aut	syslog 出力条件に認証ログ aut を追加します。	

3.4.3 AX3600S のコンフィグレーション

AX3600S の設定例を示します。

(1) 共通の設定

AX3600S の設定		
ポート VLAN の設定		
(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 10	VLAN1 は使用しないため、無効にします。	
(config-vlan)# name BeforeAuthVLAN (config)# vlan 30 (config-vlan)# name QuarantineVLAN	認証前 VLAN として VLANIO を、検疫 VLAN として VLAN30 を、認証後 VLAN として VLAN100 を、管理 用 VLAN として VLAN1000 を作成します。	
(config)# vlan 100 (config-vlan)# name 0kVLAN (config=# vlan 1000		
(config-vlan)# name ManagedVLAN		
スパニングツリーの設定		
<pre>(config)# spanning-tree mode mst (config)# spanning-tree mst configuration (config-mst)# instance 1 vlans 100, 1000 (config-mst)# instance 2 vlans 30 (config-mst)# instance 3 vlans 10 (config-mst)# name NAP (config-mst)# revision 1</pre>	マルチプルスパニングツリーを有効にし、リージョン、 インスタンスを設定します。 リージョン名:NAP リビジョン番号:1 MST インスタンス1:VLAN100、1000 MST インスタンス2:VLAN30 MST インスタンス3:VLAN10 > 構築ポイント <u>(12)</u>	
<pre>(config)# spanning-tree mst 0 root priority 4096 (config)# spanning-tree mst 1 root priority 4096 (config)# spanning-tree mst 2 root priority 4096 (config)# spanning-tree mst 3 root priority 4096</pre>	ブリッジ優先度を設定します。 ▶ 構築ポイント<u>(13)</u>	
物理ポートの設定		
<pre>(config)# interface range gigabitethernet 0/1-4 (config-if-range)# media-type rj45 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 10,30,100,100</pre>	ポート 0/1~0/4 を、下位スイッチと通信するトラン クポートとして設定します。 トランクポートに VLAN10、30、100 および 1000 を設定します。	
リンクアグリゲーションの設定		
<pre>(config)# interface port-channel 1 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan 10,30,100,1000</pre>	ポートチャネルインタフェース 1 をトランクポートと して作成し、トランクポートに VLAN10、30、100 お よび 1000 を設定します。	
(config)# interface range gigabitethernet 0/3-4 (config-if-range)# channel-group 1 mode on	ポート 0/3~0/4 を、スタティックモードのチャネルグ ループ 1 に設定します。	
インタフェースの設定		
<pre>(config)# interface vlan 10 (config-if)# ip address 192.168.10.1 255.255.255.0 (config)# interface vlan 30 (config-if)# ip address 192.168.30.1 255.255.255.0 (config)# interface vlan 100 (config-if)# ip address 192.168.100.1 255.255.255.0 (config)# interface vlan 1000 (config-if)# ip address 172.16.0.1 255.255.255.0</pre>	VLAN10、30、100 および 1000 に、インタフェース IP アドレスをそれぞれ設定します。	
(2) VRRPの設定

AX3600S の設定	
VRRP の設定	
<pre>(config)# interface vlan 10 (config-if)# vrrp 10 ip 192.168.10.254 (config-if)# vrrp 10 priority 200 (config-if)# no vrrp 10 preempt (config-if)# vrrp 10 accept</pre>	VLAN10、30、100 および 1000 に対して、以下の設定 を行います。 ・仮想ルータの IP アドレスを設定します。 ・仮想ルータの優先度を設定します。 ・自動切り戻しを抑止します。
<pre>(config)# interface vlan 30 (config-if)# vrrp 30 ip 192.168.30.254 (config-if)# vrrp 30 priority 200 (config-if)# no vrrp 30 preempt (config-if)# vrrp 30 accept</pre>	 ・アクセプトモードを有効にします。 > 構築ポイント(13)
<pre>(config)# interface vlan 100 (config-if)# vrrp 100 ip 192.168.100.254 (config-if)# vrrp 100 priority 200 (config-if)# no vrrp 100 preempt (config-if)# vrrp 100 accept</pre>	
<pre>(config)# interface vlan 1000 (config-if)# vrrp 1 ip 172.16.0.254 (config-if)# vrrp 1 priority 200 (config-if)# no vrrp 1 preempt (config-if)# vrrp 1 accept</pre>	

(3) DHCP リレーの設定

AX3600S の設定	
DHCP リレーの設定	
(config)# interface vlan 10 (config-if)# ip helper-address 10.51.0.1	VLAN10、30 および 100 に対して、DHCP リレーエー ジェントによる転送先アドレスを設定します。
(config)# interface vlan 30 (config-if)# ip helper-address 10.51.0.1	▶ 構築ポイント <u>(14)</u>
(config)# interface vlan 100 (config-if)# ip helper-address 10.51.0.1	

(4) OSPF の設定

AX3600S の設定	
ポート VLAN の設定	
<pre>(config)# vlan 5 (config-vlan)# name OSPF (config)# vlan 15 (config-vlan)# name OSPF</pre>	OSPF 通信用に、ポート VLAN5 および 15 を作成します。
物理ポートの設定	
<pre>(config)# interface gigabitethernet 0/24 (config-if)# switchport mode access (config-if)# switchport access vlan 15 (config-if)# spanning-tree portfast</pre>	ポート 0/24 をアクセスポートとして設定します。 アクセスポートに VLAN15 を設定します。 スパニングツリーの PortFast 機能を適用し、スパニン グツリー対象外とします。
リンクアグリゲーションの設定	
<pre>(config)# interface port-channel 1 (config-if)# switchport trunk allowed vlan add 5</pre>	ポートチャネルインタフェース 1 で VLAN5 を追加し ます。
インタフェースの設定	
(config)# interface vlan 5 (config-if)# ip address 10.5.0.1 255.255.255.0 (config)# interface vlan 15 (config-if)# ip address 10.15.0.1 255.255.255.0	VLAN5 および 15 に、インタフェース IP アドレスを設 定します。
OSPF の設定	
<pre>(config)# router ospf 1 (config-router)# router-id 10.5.0.1 (config-router)# maximum-paths 4 (config-router)# network 10.5.0.0 0.0.0.255 area 0 (config-router)# network 10.15.0.0 0.0.0.255 area 0 (config-router)# redistribute connected</pre>	OSPF を起動します。 ルータ ID を設定します。 OSPF が動作するネットワークを設定します。 connected 経路を再配送します。

3.4.4 AX2500S のコンフィグレーション

AX2500SシリーズのコンフィグレーションはAX1200Sシリーズに比べて、インタフェース種別以外の認 証関連のコンフィグレーションコマンドは基本的に共通です。

ただし、認証関連では、次に示す機能追加とコンフィグレーションの追加があります。機能としては、 リンクアグリゲーションポートの認証機能が追加され、コンフィグレーションとしては、認証ログを syslog採取する場合にlogging event-kind autを追加設定する必要があります。

付録 A.コンフィグレーションに AX1240S を AX2530S に置き換えた場合の完成コンフィグレーショ ンファイルを添付しましたので参考にしてください。

3.5 Windows Server 2008 の設定

本章では、NAP に必要なコンポーネントを1台の Windows Server 2008 に全て構築しているものと して、本環境用のグループポリシーの作成手順や Network Policy Server (以下 NPS)の設定方法を示し ます。各コンポーネントは、それぞれ別のサーバマシンで構成して連携させる事で NAP 検疫システム を構築する事も可能です。

設定に必要な各コンポーネントは既にインストール済みであることが前提です。OS ならびに必要機能に関してのインストール手順等は Microsoft のホームページを参照して下さい。

本ガイドでは Windows Server 2008 R2 ベースで記述しています。本章では Windows Server 2008 と Windows Server 2008 R2 で設定に違いがある場合、設定画面や設定手順の差分箇所について両方の 設定方法を記述しています。

また NPS の設定は IAS (Windows Server 2003)の構築知識や経験がある方を対象としています。

以下に Windows Server 2008 の構成ステップを記載します。

(1) <u>事前準備</u>

本ガイドにて設定を実施する前に必要な役割を示します。

- (2) <u>グループポリシーの設定</u>(Active Directory)
 本環境用のグループポリシーを作成します。
- ユーザ、グループの作成 (Active Directory)
 認証するユーザやグループの登録を行います。
- (4) RADIUS クライアントの設定 (NPS)

NPS に Authenticator (認証スイッチ)の IP アドレスを登録します。

(5) <u>接続要求ポリシーの設定</u>(NPS)

NPS が RADIUS リクエストを受信した場合の処理を定義します。

- (6) <u>システム正常性検証ツール(SHV)の設定</u>(NPS) NPS にシステムのセキュリティポリシーを定義します。
- (7) 正常性ポリシーの設定 (NPS)

セキュリティポリシーに対する判定基準を定義します。

(8) <u>ネットワークポリシーの設定</u>(NPS)

RADIUS リクエストの内容に一致する条件や接続設定などのセットを作成します。

(9) <u>DHCP サーバの設定</u>(DHCP)

各 VLAN に対応する DHCP スコープを作成します。

3.5.1. 事前準備

本ガイドでは、Windows Server 2008 にて下記の役割を使用します。 Windows Server 2008 に以下の役割が構成されているかを確認し、必要に応じて追加インストールを行って下さい。

役割

1. Active Directory ドメインサービス

本ガイドではドメインにて最初のドメインコントローラとして構成しています。 本章にてグループポリシーの設定内容を示します。

2. Active Directory 証明書サービス

本ガイドではエンタープライズのルート CA として構成しています。

3. DNS サーバ

このサーバをプライマリ DNS として設定します。

4. NPS

本章にて設定内容を示します。

5. DHCP サーバ

本章にて設定内容を示します。

3.5.2. グループポリシーの設定

本ガイドでは、Active Directory のグループポリシーを用いて、組織内のコンピュータを一括管理して います。これにより、Windows ドメインに参加した端末に、NAP クライアントとしての構成や IEEE802.1X 認証の設定を自動的に適用させることで、初期導入時の負担を軽減することができます。

グループポリシーの設定を行わない場合、コンピュータ毎に NAP クライアントとしての構成や IEEE802.1X 認証の設定を手動で構成する必要があります。グループポリシーの設定を行わない場合は、 8.1章を参照して下さい。

グループポリシーの設定内容や適応範囲はシステム全体のセキュリティに大きく影響を与えますの で、導入環境のセキュリティポリシーに応じて適切な設定を行って下さい。なお、セキュリティフィル タ処理を構成することで、特定のコンピュータのみに適用対象を絞り込むこともできます。

本ガイドで設定するグループポリシーの内容を以下に示します。

項 番	ポリシー名	設定内容	説明
1	Network Access Protection Agent	自動開始	クライアントコンピュータ上のネットワーク アクセス保護(NAP)機能を有効にします。
2	Wired AutoConfig	自動開始	イーサネットインタフェース上で IEEE802.1X 認証を実行します。
3	新しい Vista ワイヤード(有線) ネットワークポリシー	有効	クライアントコンピュータ上の EAP 設定を構 成します。
4	EAP 検疫強制クライアント	有効	EAP ベースの強制を NAP に提供します。
5	セキュリティセンターをオンにする (ドメイン上のコンピュータのみ)	有効	ドメイン上のコンピュータにてセキュリティ センターを自動開始させます。

表 3-6 グループポリシーの設定内容

以下にグループポリシーの作成ステップを記載します。

- (1) 新しいグループポリシーオブジェクトの作成
- (2) <u>システムサービスの構成</u>
- (3) <u>ネットワークポリシーの構成</u>
- (4) <u>NAP クライアントの構成</u>
- (5) <u>セキュリティセンターの構成</u>
- (6) <u>グループポリシーの優先度の変更</u>
- (7) <u>グループポリシーの反映</u>

(1) 新しいグループポリシーオブジェクトの作成

本ガイドで使用するグループポリシーオブジェクトを作成する手順を示します。

 「スタート」→「検索の開始」に「mmc」と入力して MMC (Microsoft Management Consol)を起 動する。

コンソール1の画面にて、「ファイル」→「スナップインの追加と削除」をクリックする。

スナップインの追加と削除画面にて、
 「グループポリシー管理エディタ」を選択し「追加」をクリックする。

ナップイン	10/9 .	コンソール ルート	103系の編集(公)
NAP クライアントの構成	Microsoft Co		荆臣松书)
Web アドレスへのリンク	Microsoft Co		and the second s
Windows Server KobPod	Microsoft Co		上へ移動(U)
WMI בבידם - אר	Microsoft Co-		(FAISab(D)
イベントビューア	Microsoft Co		1.04690040
エンターフライス PKI	Microsoft Co		
クルーフ ポリシー オフジェクト エティー ブループ ポリシー スカーカー OPO	Microsoft Co		
グルーナ ホリシーの管理	Microsoft Co		
グループ ポリシー管理エティタ	Microsoft Co		
コンピュータの管理	Microsoft Co		IFFERENCE (N)-
4			
スナップインでは、Active Directory の	りサイト、ドメイン、細菌単位(0	U) にリンクされた、またはコンピュータに格納され	たグルーフ ポリシー オブジェクトを編集
0			

- 図 3.5-1 新しいグループポリシーオブジェクトの作成①
- グループポリシーオブジェクトの選択画 面にて「参照」をクリックし、「ドメイン /OU」タブの「新しいグループポリシー オブジェクトの作成」アイコンをクリッ クして「新しいグループポリシーオブジ ェクト」を作成する。

グルーナ ポリシー オブジェクトの参照	<u>? ×</u>
ドメイン/OU サイト すべて	
場所①: 🚔 example.co.jp 🔹 🖄 🔛 🔹 ドメイン、OLL およびリンクされたグループ ポリシー オブジェクド(型):	
■ Domain Controllers.example.co.jp ■ Default Domain Policy ■ 新しいヴルーラ ポリシー オブジェクト	
OK *-	トンセル

図 3.5-2 新しいグループポリシーオブジェクトの作成②

- ④ 新しく作成したグループポリシーオブジェクトの名前を変更し、「OK」をクリックする。
 (本ガイドでは「Nap Test Policy」)
 グループポリシーオブジェクトの選択画面にて「完了」をクリックして画面を閉じる。
- ⑤ スナップインの追加と削除画面にて、選択されたスナップインの中に作成したグループポリシーオブジェクトが存在する事を確認し「OK」をクリックして画面を閉じる。

ップイン	-	ニコンソール ルート	_	拡張の編集(2)-
TPM 管理 Neb アドレスへのリンク		Nap Test Policy (DC example	(d) (0)	首項於(<u>R</u>)
Nindows Server バックアップ NML コントロール				上小明的山
(ペント ビューア ビンターブライズ PKI	- Intervals	r.		下八年時(10)
ダループ ポリシー オブジェクト エディタ ダループ ポドシー スカーター CPO エディタ		1		
グループ ポリシーの管理				
リルーファルリンー管理エティター エンピュータの管理	22			
シボーネント サービス	<u> </u>		2	IT48的定(1/)_
ナップインでは、Active Directory のサイト、ドメ	イン、秘密単位(00)(コンクされた、またはコンピュータに格納されば	とグルーフ 木り	シーオブジェクトを編集で

図 3.5-3 新しいグループポリシーオブジェクトの作成③

(2) システムサービスの構成

NAP クライアントの構成として必要な下記 2 つのサービスについて、クライアント端末起動時に自 動的に開始状態となるよう設定する手順を示します。

- 「Network Access Protection Agent」
- Wired Auto Config_
- ① コンソール 1 の左画面にて、「コンソー $\mathcal{W} \to [\mathsf{Nap Test Policy}] \to [\exists$ ンピュータの構成」→「ポリシー」→ 「Windows の設定」→「セキュリティの 設定」→「システムサービス」を選択す る。右画面の「Network Access Protection Agent」を右クリックしてプロパティを 開く。

② Network Access Protection Agent のプロ パティ画面にて、サービスのスタートア ップモードを「自動」に設定し、「OK」 をクリックして画面を閉じる。



図 3.5-4 システムサービスの構成①



図 3.5-5 システムサービスの構成②

③ ①の右画面より「Wired AutoConfig」を 右クリックして「プロパティ」を開き、 サービスのスタートアップモードを「自 動」に設定する。最後に「OK」をクリッ クして画面を閉じる。



図 3.5-6 システムサービスの構成③

(3) ネットワークポリシーの構成

クライアント端末の IEEE802.1X 認証やシングルサインオンを設定する手順を示します。Windows Server 2008 R2 と Windows Server 2008 で差分がある箇所については下線で示しています。

① 「ワイヤード(有線)ネットワーク(IEEE802.3)ポリシー」

Windows Server 2008 R2 の場合

コンソール 1 の左画面にて、「コンソー ルルート」→「Nap Test Policy」→「コン ピュータの構成」→「ポリシー」→ 「Windows の設定」→「セキュリティの設 定」→「ワイヤード(有線)ネットワーク (IEEE802.3)ポリシー」を右クリックし て<u>「Windows Vista 以降のリリース用の新</u> しいワイヤード(有線)ネットワークポリシ <u>一の作成」を選択する。</u>

💴 エンソール ルート	名前 說明	10ft
■ Test poly (Sociample co.p.) ポリシー ■ エントークーの構成 ■ エントークーク・ロットボック・ ■ ローカル ボリンー ■ ローカル ボリン ■ ローカル ボリン ■ ローカル ボリン ■ ローカル ■ ローカル	このビューに表示する項目はよりません。	9-fヤード (前級) ネットワー 他の時間 ポリーの行成
11 2 2間キーのポリシー	新しいタスクパッド表示(1)_	
 ラフトウェアの事件ののパワラー ネットワークアクセス(名) アアリケーション制造ポリシー 	最新の情報に更新(F) 一覧のエクスポード(L)	
 ※ 15歳かど)-の21482485、 ※ 通りシントベス20 GoS ※ 12税約270とトローカル・エンビューターから取得して ※ 4532 ※ 4532 ※ 4532 	AU7040 1999-	

図 3.5-7 ネットワークポリシーの構成(Windows Server 2008 R2)①

Windows Server 2008 の場合

コンソール 1 の左画面にて、「コンソ ールルート」→「Nap Test Policy」→「コ ンピュータの構成」→「ポリシー」→ 「Windows の設定」→「セキュリティの 設定」→「ワイヤード(有線)ネットワ ーク(IEEE802.3)ポリシー」を右クリ ックして<u>「新しい Windows Vista ポリシ</u> <u>一の作成」を選択する。</u>

コンソール みート	名前	1248	1911
日 副 Nap Test Policy [DClexample.co.jp] ポリシー	ະຫ	ピューに表示する項目はありません。	ワイヤード(有線)
			80:01 9 (1)
 アイヤード(46年)ネットワーク(IEEE 8023)ポリシー ビキュリティが強化された Windowe ファイアウォール 	IfLC: Windows Vista #0	シーの作成	
ネットワークリストマネージャオリシー 田 マクイヤレスネットワーク (IEEE 00211) ポリシー	表示(V) ここから新しいウィンドウ(W)		
田 ジフトウェアの単語のポリシー	新しいタスクパッド表示(T)_		
 ■ Network Access Protection ■ ■ P セキュリティ カリシー (Active Directory (example ■ ■ セリュー ペースの QoS 	最新の情報に更新(F) 一覧のエクスポート(L)。		
回 🧰 管理用テンプレート ローカル コンピュータから取得したポパシー	へルプ(H)		
 □ 読_2			

図 3.5-8 ネットワークポリシーの構成(Windows Server 2008)①

② IEEE802.1X 認証の設定

新しい Vista ワイヤード(有線)ネットワークポリシー画面にて、「セキュリティ」タブを選択し 「プロパティ」をクリックする。

保護された EAP のプロパティ画面にて、信頼されたルート証明機関一覧にインストールした CA の名前がある事を確認してチェックする。(本ガイドでは「example-DC-CA」)

Windows Server 2008 R2 の場合

次に、<u>「ネットワークアクセス保護を強</u> <u>制する」にチェックする。</u> 最後に、認証方法として「セキュリティで 保 護 さ れ た パ ス ワ ー ド (EAP-MSCHAPv2)」が選択されている 事を確認し、「構成」をクリックする。

新しいワイヤード (有線) ネットワーク ポリシー Properties ? 🛛 🗙	保護された EAP のプロパティ 🛛 🗵
全校 セキュリティ マ ネットワーク アリセスのために IFFE 802 /X 記録を使用可能による(F) ネットワークの認知方法の達解(1) Microsoft [2扱え?1/2 EAP (PEAP)	現代のための総論ま方法 「サーバーの運動用を検護する(い) 「大切サーバー(建設する(o): 「信頼されたルート注意可規規模(R) 「信頼されたルート注意可規規模(R) 「信頼されたルート注意可規規模(R) 「信頼された」レード注意可規規模(R) 「信頼された」の一CA = scample-DC-CA = scample-D
	は話よ方法を確認する(S): [セキュリチィで保護されなけなリード (EAP-MSCHAP v2) ・ 構成(C)_ 「 必須有時続を有効にする(F) 「 ネットラーク アクセス保護を証明する(N) 「 サーバーに暗号化 バインドの TLV がない場合はな助所する(D) 「 D フライバシーを有効にする(D)

図 3.5-9 ネットワークポリシーの構成(Windows Server 2008 R2)2

Windows Server 2008 の場合

次に、「検疫のチェックを有効にする」 <u>がチェックされている事を確認する。</u> 最後に、認証方法として「セキュリティで 保 護 さ れ た パ ス ワ ー ド (EAP-MSCHAPv2)」が選択されている 事を確認し、「構成」をクリックする。

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 ネットワークの認証方法の選択(T).	.∮&(E)	マ サーバーの証明者を検証する(V) 「 次のサーバー(:1種語する(0):
Microsoft 保護された EAP (PEAP) 初日チード(A)		 (食養的でおした ルート主人専門研究論N (R):
コーザーの再設設 設設エスーの最大数(1) ア このそうトワークへの今後の接続のため、ユーザー情報を行 ユオる(0)	▼ 「 」 】 】 】 】 】 】 】 】 】 】 】 】 】	Class 3 Public Filmary Certification Authority @ example-DO-CA = resemple-DO-CA @ OTE Cyber Trust Global Root http://www.scot.n// Microsoft Root Authority @ university filmation Automic 新しょいヤーバー表たは容易なりた話が時期開始が追加するようフーザーに次の ない(P) 記録が方法素減的で考えGS.

図 3.5-10 ネットワークポリシーの構成(Windows Server 2008)②

注意:「Windows Vista 以降のリリース用の新しいワイヤード(有線)ネットワークポリシー」と「新しい Vista ワイヤード (有線) ネットワークポリシー」は Windows XP SP3 にも適用されます。

- ③ EAP-MSCHAPv2 のプロパティ画面にて、 「Windows のログオンとパスワード(お よびドメインがある場合はドメイン)を 自動的に使う」がチェックされている事 を確認し、「OK」をクリックして画面を 閉じる。さらに「OK」をクリックし保護 された EAP のプロパティ画面を閉じる。
- ② 認証エラーの最大値の初期値は1です。
 RADIUS サーバ,認証スイッチおよび端末への負荷などでパケットロスが発生した場合を考慮し、本ガイドでは「5」としています。また、「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ッシュする」にチェックする。

⑤ 「詳細設定」をクリックし詳細なセキュ リティ設定画面のシングル サイオンの 「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」をチェックし、 「OK」をクリックして画面を閉じる。



図 3.5-11 ネットワークポリシーの構成③



図 3.5-12 ネットワークポリシーの構成④

F 80	2.1×の詳細設	定を強制する(<u>E</u>)				
E	APOL 開始メッ	セージの最大数(工):	保持期間((秒)(日):		
la la						
開	1始期間(秒)(<u>[</u>	<u>)):</u>	認証期間((秒)(山):		
Į8			118			
E	apol 開始メッセ	ージ(<u>0</u>):				
I	EEE 802.1X を	とおして送信する		-		
(行 招	・ユーザー ログ シューザー ログ 競売の最大遅延	オンの直前に美行す オンの直後に実行す . (秒):	ବ ବି		10	
F	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		
	- መልካትወት	クでは、コンピュ <u>ー</u> タと	ユーザーの資	格情報を使	開し	

図 3.5-13 ネットワークポリシーの構成⑤

(4) NAP クライアントの構成

NAP 実施オプションを指定します。本ガイドでは、IEEE802.1X 認証のみを構成します。Windows Server 2008 R2 と Windows Server 2008 で差分がある箇所については下線で示しています。

① NAP クライアントの構成

Windows Server 2008 R2 の場合

コンソール 1 の左画面にて、「コンソ ールルート」→「Nap Test Policy」→「コ ンピュータの構成」→「ポリシー」→ 「Windows の設定」→「セキュリティの 設定」→「Network Access Protection」 →「NAP クライアントの構成」→<u>「強制</u> クライアント」を選択し、右画面の「EAP 検疫強制クライアント」を右クリックし て「有効」にする。



図 3.5-14 NAP クライアントの構成(Windows Server 2008 R2)①

Windows Server 2008 の場合

コンソール1の左画面にて、「コンソー ルルート」→「Nap Test Policy」→「コン ピュータの構成」→「ポリシー」→ 「Windows の設定」→「セキュリティの 設定」→「Network Access Protection」→ 「NAP クライアントの構成」→<u>「実施ク</u> <u>ライアント」を選択し、右画面の「EAP</u> 検疫強制クライアント」を右クリックして 「有効」にする。

コンソール ルート	宇協クライアント			121	ት	
Nap Test Policy [DC example co.jp] ポリシー 同 4年 プンピュータの種類	名前	秋藤		実	塗クライアント	14
 ■ オリシー ■ メリシーンFの最初定 ■ ジントウェアの最初定 ■ Windows の最初定 	DHOP 検疫強制クライアント リモート アクセス検疫強制クライアント IPSec 証明書利用者	無(3)) - 第(3)) 第(3))			表示 ここから新しいウ	20
スタリプト (スタートアップ/シャットダウン)	NTS ゲートウェイ検疫法制クライアント	無効	相约)(E)		教育を行われる 単語に	
日 時 アカアント ポリシー		無効	最新の情報に更新	f(F)	11.7	
田 🧃 ローカル ポリシー		_	プロパティ(R)		検疫強制クラ	
田 通 イベント ロク 田 の 御膳されたグループ			~x7(H)		电学力	
田 🙀 システム サービス		<u></u>		i di	最新の情報	
第二番 レジスドリ 第二番 ファイル システム				103	70/5+	
	* () •			
※ ご 実施254アンド ※ ご ユーザー インターフェイスの設定	ID: 79623					
 E ご 正常性登録の設定 E P とたっと見て、世紀に、 Active Directory (avagely no in) 	名前: EAP 相	相互強制カライアント				
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1號8月 EAP A	一天の強制在 NAP	に提供します。			
B 管理用テンプレード ローカル コンピューダがら取得したポリシー定義 ア ボネ おま 市 ホー ホ	パージョン: 10					
三 18 ユーザーの構成	ペンダ: Micros	oft Corporation		L		
 田 (二) ボリシー 田 (二) 基本設定 	₩\$\$ ●			L		

図 3.5-15 NAP クライアントの構成(Windows Server 2008)①

(5) セキュリティセンターの構成

Windows ドメインに所属している端末のセキュリティセンターを有効にする手順を以下に示します。 この設定が未構成の場合、Windows ドメインに所属している端末のセキュリティセンターは無効に なります。Windows Server 2008 R2 と Windows Server 2008 で差分がある箇所については下線で示 しています。

① セキュリティセンターの構成

Windows Server 2008 R2 の場合

コンソール1の左画面にて、「コンソー ルルート」→「Nap Test Policy」→「コン ピュータの構成」→「ポリシー」→「管理 用テンプレート」→「Windows コンポー ネント」→「セキュリティーセンター」を 選択する。右画面の「セキュリティセンタ ーをオンにする(ドメイン上のコンピュー タのみ)」を右クリックして<u>「編集」を選</u> <u>択、新しく表示された「セキュリティ セ</u> <u>ンターをオンにする(ドメイン上のコンピ</u> <u>ユータのみ)」画面の「有効」にチェック</u> <u>する。</u>



図 3.5-16 セキュリティセンターの構成(Windows Server 2008 R2)①

Windows Server 2008 の場合

コンソール1の左画面にて、「コンソー ルルート」→「Nap Test Policy」→「コン ピュータの構成」→「ポリシー」→「管理 用テンプレート」→「Windows コンポー ネント」→「セキュリティーセンター」を 選択する。右画面の「セキュリティセンタ ーをオンにする(ドメイン上のコンピュー タのみ)」を右クリックして<u>「プロパティ」</u> を開き、「有効」をチェックする。



図 3.5-17 セキュリティセンターの構成(Windows Server 2008)①

② 「OK」をクリックし画面を閉じる。コンソール1画面も閉じる。

Windows Server 2008 の場合

その後表示される「NAP クライアントの 構成」画面にて「はい」をクリックして NAP クライアントの構成をグループポリ シーオブジェクトに適用させて下さい。

NAP クライアントの構成		×
現在のグループ ポリシー オブジェクト (GPO) I しか?	に設定が適用されていません。言	没定を適用しま
	(t)(Y)	いいえ(N)

(6) グループポリシーの優先度の変更

作成したグループポリシーオブジェクト(Nap Test Policy)をWindows ドメイン「example.co.jp」 にリンクさせる方法を示します。

Windows ドメイン「example.co.jp」には既存のグループポリシーオブジェクト(Default Domain Policy)がリンクされていますので、優先度の入れ替えを行います。

- ① 「スタート」→「検索の開始」に「gpmc.msc」と入力してグループポリシー管理コンソールを起 動する。
- グループポリシーの管理の左画面にて、
 「グループポリシーの管理」→「フォレスト」→「ドメイン」→「example.co.jp」
 を選択する。

屋グルーフ ポリシーの管理							_101
ファイル(E) 操作(A) 表示(U) ウインドウ	X999 ~11-7KB9						<u>_101</u> 2
ダループ ポリシーの管理 S 入 フォレスト example co.jp マットント example co.jp マットント example co.jp マットント S ムイン	example.co.jp リンクされたグループ	ip フ ポリシー オブジェクト グルーフ ポリシ	-0继承 委任				
 ■ トキシンション ● トキシンション ● トキシンション ● トキシンション ● トキンション ●		ates Ooro 1 jii Defaut Donain Pol. 2 jii Nap Test Policy	3440 192-50540346_ (A) (BA) (A) (BA)	<u>ロPO のお代報</u> 有効 有効	<u>WMM フィルク</u> なし なし	2008/04. 2008/04. 2008/04.	B34(2) examplec examplec

図 3.5-19 グループポリシーの優先度の変更①

 グループポリシーの管理の右画面にて 「リンクの順序」の上下矢印を操作し、 新しく作成した Nap Test Policy の順序 が「1」、Default Domain Policy が「2」 となるように設定する。

<u>鳥</u> グルーナ ポリシーの管理								<u>_ 0 ×</u>	
□ 7rイル(E) 操作(A) 表示(U) ウルンド穴(W) ヘルプ(E)									
(= =) 🖄 🖬 🙆 🖬									
▲ グループ ポリシーの管理 □ A フォレスト: example.co.jp □ 品 ドメイン	examp りンが	ole.co.jp れたグループ ポリシー	オブジェクト グルーフ ポリ・	シーの維	承 委任				
🗄 🚔 example.co.jp	[リンクの順序 ^	GPO	強制	リンクの有効化	GPOの状態	WML 7r/ly	更新日時	15X/2
🛒 Default Domain Policy 🔟	会	1	Nap Test Policy	<i>р_</i>	(th	有効	なし	2008/04	exampl
🚮 Nap Test Policy		2	🛒 Default Domain Pol.	. ()_	(ti)	有効	なし	2008/04	exampl
🕀 🗊 Domain Controllers	Δ								
🗉 📴 グループ ポリシー オブジェジー	_	4							- F
									_

図 3.5-20 グループポリシーの優先度の変更②

④ リンクの順序を変更後、グループポリシーの管理画面を閉じる。
 以上で本ガイド用のグループポリシーの設定は終了です。

図 3.5-18 セキュリティセンターの構成②

(7) グループポリシーの反映

サーバのコマンドプロンプトより「gpupdate /force」 コマンドを実行し、(1)~(6)で作成した全てのグループポリシー情報の更新を実行します。これにより、以降ドメイン参加した端末には NAPクライアントとしての構成やIEEE802.1X認証の設定が自動的に適用されます。

すでにドメイン参加済みの端末はポリシー更新周期(初期値90分周期)及び再起動時にポリシーが更 新します。

3.5.3. ユーザ、グループの作成

Active Directory に認証するユーザとグループを作成する手順を以下に示します。 本ガイドでは、ユーザ ID: user01、グループ: Sales としています。

 「スタート」→「管理ツール」→「Active Directory ユーザーとコンピュータ」を開 く。
 左画面から該当ドメインを展開し、
 「Users」を右クリックして「新規作成」
 →「ユーザー」を選択すると、ウィザー ドが開始される。



図 3.5-21 ユーザ、グループの作成①

- ② ウィザードが開始されたら、ユーザ ID およびパスワードを指定してユーザを作成する。
- ③ 「スタート」→「管理ツール」→「Active Directory ユーザーとコンピュータ」を開 く。
 左画 面から該当ドメインを展開し、
 「Users」を右クリックして「新規作成」
 →「グループ」を選択すると、ウィザー
 ドが開始される。

/ァイル(ト) 探作(A) 表示(V) ヘ	ルブ(H)		
• 🔿 🖄 🚾 🖌 🗋 🗙 🛙	🗐 💁 📴 🖬 🔧 📚 🖆 🎙	7 🗾 🤽	
	この こ		
	怒 Schema Admi セキュリティ グル Suser01 ユーザー	スキーマの指定された管理者	

図 3.5-22 ユーザ、グループの作成②

④ ウィザードが開始されたら、グループ名を入力してグループを作成する。

(5) 作成したユーザをグループに参加させる。
 (2)にて作成したユーザ(本ガイドでは「user01」)を右クリックしてプロパティを開き、プロパティ画面にて「所属するグループ」タグを選択し、④にて作成したグループを追加する。



⑥ 「OK」をクリックして画面を閉じる。

3.5.4. RADIUS クライアントの設定

NPS に認証スイッチを登録する手順を以下に示します。

- 「スタート」→「管理ツール」→「ネットワークポリシーサーバー」を開く。
 左画面の「RADIUS クライアントとサーバー」を展開し、「RADIUS クライアント」を右クリックして「新規」を選択する。
- ② 新規 RADIUS クライアント画面にて、下記3項目を入力して「OK」をクリックする。
 ・フレンドリ名:任意(本ガイドでは「AX2430S」)
 ・アドレス:認証スイッチの IP アドレス(本ガイドでは「172.16.0.11」)
 ・共有シークレット:認証スイッチにて設定したシークレットキー(本ガイドでは「alaxala」)

・Windows Server 2008 R2 の設定画面



図 3.5-24 RADIUS クライアントの設定(Windows Server 2008 R2)①

・Windows Server 2008 の設定画面

💖 ネットワーク ポリシー サーバー	所規 RADIUS クライアント	×	
アイル(F) 操作(A) 表示(V) マーク・(A) ます(V) マーク・(A) ます(V)	A MUNDO シライアントを有効にする(E) 名(E) 名(E) 名(E) 名(E) 名(E) ス(E) ス(E		ーバーを指定できます。
1			

図 3.5-25 RADIUS クライアントの設定(Windows Server 2008)①

- 注意:追加オプションの「RADIUS クライアントが NAP に対応している」は VPN 方式関連設定 のため、チェックする必要はありません。
- ③ 登録する RADIUS クライアント(認証スイッチ)全てに対して同上の設定を行う。
- ④ RADIUS クライアントの確認
 NPS の右画面に、作成した RADIUS ク ライアントが存在する事を確認する。

💖ネットワーク ポリシー サーバー					
ファイル(E) 操作(<u>A</u>) 表示(V) /	シレプ(圧)				
🗢 🔿 🖄 🖬 🚺 🖬					
🚯 NPS (ローカル)	RADIUS クライアント				
RADIUS クライアントとサーバー RADIUS クライアント RADIUS クライアント IN ADIUS クライアント	RADIUS クライアント(こは、ネットワークへのア	りセスを提供す	するネットワーク アクセス・	サーバーを指定できます。
Ⅲ 川 ボリシー		「デバノフの御坊告示」	MAR SHIT	小七年時	
·····································	AX2430S 172.16.0.11	RADIUS Standard	No	有効	
🗉 🜉 テンプレートの管理	📱 AX1240S 172.16.0.11	RADIUS Standard	No	有効	
•					

図 3.5-26 RADIUS クライアントの設定②

3.5.5. 接続要求ポリシーの設定

NPS に RADIUS リクエストを受信した場合の処理を設定する手順を以下に示します。

- ネットワークポリシーサーバー画面にて、左画面の中の「ポリシー」を展開し「接続要求ポリシー」
 を右クリックして「新規」を選択すると、ウィザードが開始される。
- 新しい接続要求ポリシー画面にて、ポリシー名(本ガイドでは「NAP 検疫」)を 入力し「次へ」をクリックする。



図 3.5-27 接続要求ポリシーの設定①

3 条件の指定

新しい接続要求ポリシー画面にて「追加」 をクリックする。 条件の選択画面にて「NAS ポートの種 類」を選択して「追加」をクリックする。 最後に NAS ポートの種類画面にて 「Ethernet」をチェックして「OK」をク

リックし、次へ進む。

新しい接続要求ポリシー x 条件の指定 接続要求についてこの接続要求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 NAS ボートの種類 x x 条件の選択 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。 条件を選択し、「追加」 一般的なダイヤルアップおよび VPN トンネルの種類(D) **?**} NAS ID Async (Modem) 構文を使用し NAS ID の条 て NAS 名を ISDN Sync Sync (T1 Line) NAS IPv4 7 Virtual (VPN) **?**] NAS IP アド| を指定できま Ρ ネットワーク ・般的な 802.1X 接続トンネルの種類(X) 🔽 Ethernet NAS IPv6 7 FDDI **7** |Token Ring |Wireless - IEEE 802.11 って IPv6 ネッ NAS IPv6 ア トワークを指定 NAS ポート0 その他(T) 802.11 ワイヤ ボート および ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation 🗌 Async (Modem) • . キャンセル OK キャンセル

図 3.5-28 接続要求ポリシーの設定②

後続要求転送の指定

「次へ」をクリックして進む。

⑤ 認証方法の指定

新しい接続要求ポリシー画面にて、「ネ ットワークポリシーの認証設定よりも優 先する」をチェックし、EAP の種類に 「Microsoft: 保護された EAP (PEAP)」 を追加する。



図 3.5-29 接続要求ポリシーの設定③

⑥ PEAP のプロパティ

EAP の種類に追加した「Microsoft 保護 された EAP (PEAP)」を選択し、「編集」 をクリックする。保護された EAP のプロ パティの構成画面にて、証明書の発行先 と「検疫のチェックを有効にする」がチ ェックされていることを確認して「OK」 をクリックする。

保護された EAP のプロ/	パティの構成	X
クライアントに対して、サ・ 明書はリモート アクセス されます。	ーバーがその ID の証明をするための証明書を選択し ポリシーにおいて、 保護された EAP のために選択した	てください。この証 証明書より優先
証明書の発行先(1):	dc.example.co.jp	
フレンドリ名:		
発行者:	example-DC-CA	
有効期限:	2011/01/22 9:46:32	
 ○ 高速再接続を有効() ○ 暗号化バインドがな() ○ ネットワーク アクセス(: EAP の種類(T) 	こする(E) 、ウライアントとの接続を切断する(©) 呆護を強制する(<u>N</u>)	
セキュリティで保護された	パスワード (EAP-MSCHAP ∨2)	<u>L</u> A(U) FA(D)
道加(<u>A</u>)	編集(<u>E)</u> 削除(<u>R)</u> OK	キャンセル

図 3.5-30 接続要求ポリシーの設定④

- ⑦ 設定の構成、「次へ」をクリックして進む。
- ⑧ 「完了」ボタンをクリックし、ウィザードを終了する。
- 9 処理順序の変更

Winodows Server 2008 R2 の場合

Windows Server 2008 R2 では新規で作成したポリシーがデフォルトで処理順序「1」となります。

Winodows Server 2008 の場合

作成したポリシー(NAP 検疫)を右クリックして「上へ移動」を選択し、処理順序が「1」となる ように操作する。

🞭ネットワーク ポリシー サーバー	The second s		
ファイル(F) 操作(A) 表示(V) ヘルプ	?(H)		
 NPS (ローカル) ■ RADIUS ウライアントとサーバー ■ RADIUS ウライアントとサーバー ■ RADIUS ウライアント ■ リモート RADIUS サーバー グル ■ リモート RADIUS サーバー グル ■ リモート RADIUS サーバー グル ■ ボウンク ■ ボウンク ポリシー ■ 茶ットワーク ポリシー ■ 茶ットワーク ポリシー ■ 茶ットワーク オリシー ■ ホットワーク アクセス/保護 ■ アカウンティング 	接続要求ポリシーでは、接続要求をロ VPN または 802.1X の場合、接続要 ポリシー名 NAP検疫 ダベてのユーザーに Windows 認証を使用	1. たれにで処理するか 11 上へ移動(0) 無効(する(D) 削除(1) 名前の変更(M) ポリシーの検製(C) プロパティ(R) ヘルプ(H)	王- ト RADIUS サーバーに転送するかを指定できます。NAP 構成する必要があります。 ース 行定なし 5定なし

図 3.5-31 接続要求ポリシーの設定⑤

3.5.6. システム正常性検証ツール(SHV)の設定

NPS にシステムのセキュリティポリシーを設定する手順を以下に示します。Windows Server 2008 R2 と Windows Server 2008 で差分がある箇所については下線で示しています。

① セキュリティ正常性検証ツール

Windows Server 2008 R2 の場合

Windows セキュリティ正常性検証ツール

ネットワークポリシーサーバー画面にて、左画面の中の「ネットワークアクセス保護」→「システ ム正常性検証ツール」→「Windows セキュリティ正常性検証ツール」と展開して「設定」を選択し、 <u>右画面に現れた「規定の構成」を右クリックしてプロパティを開く。</u>



図 3.5-32 システム正常性検証ツール(SHV)の設定(Windows Server 2008 R2)①

Windows Server 2008 の場合

Windows セキュリティ正常性検証ツール

ネットワークポリシーサーバー画面にて、左画面の中の「ネットワークアクセス保護」を展開して 「システム正常性検証ツール」を選択し、<u>右画面に現れた「Windows セキュリティ正常性検証ツー</u> <u>ル」を右クリックしてプロパティを選択、Windows セキュリティ正常性検証ツールのプロパティ画</u> 面にて、「構成」をクリックする。

🦻ネットワーク ポリシー サーバー		_ 0 ×
ファイル(F) 操作(A) 表示(V) ヘル	⊅(H)	
🗢 🔿 🛛 🚾 🛛 🖬		
 ● NPS (ローカル) ● ○ RADIUS クライアントとサーバー ● ○ ポリシー 	システム正常性検証ツール (SHV) では、NAP 対応クライアントコン しては、SHV を構成して正常性ポリシーにキュレビになる。 フロパティ(R)	ピュータに必要な設定を指定できます。SHV を使用する
□ 50 ネットリーク アクセスは譲 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	名前 ヘルプ(H)	
■ 修復サーバー グループ ■ アカウンティング		
	Windows セキュリティ正常性検証ツール	

図 3.5-33 システム正常性検証ツール(SHV)の設定(Windows Server 2008)①

Windows セキュリティ正常性検証ツールのブロノ	१न्न 🛛 🗙
設定	
システム正常性検証ツールを開いて構成するには	、 [構成] をクリックします。
構成(C)	
第二日 クライアントがネットワーク_アクセスを要求したとき(2	、このシステム正常性検証
ッールおよび関連するシステム正常性エーシェント ある次のエラー コードの解決方法を選択します。	について返される可能性か
SHV が必要なサービスに接続できません(S)	非準拠 ▼
SHA が必要なサービスに接続できません(H)	非準拠 💌
SHA が NAP クライアントに応答していません(N)	非進枷
SHV か心合していません(U)	非準拠
ベンダ固有のエラー コードを受信しました(R)	非準拠 ▼
OK	ンセル 適用(A)

図 3.5-34 システム正常性検証ツール(SHV)の設定②

② Windows セキュリティ正常性検証ツール

本設定が検疫チェック項目の設定となります。クライアントの環境に合わせて適切な設定を行って ください。なお本ガイドでは全ての項目をチェックする例を示しています。

Windows Server 2008 R2 の場合

左画面にて、「Windows 7/Windows Vista」を選択し画面右の詳細情報にチェックが入っていることを確認する。同様に「Windows XP」にも詳細情報にチェックが入っていることを確認する。

Windows セキュリティ正常性検討	ヨッール	Windows 7, Windows Vista	_	X	Windows セキュリティ正常性検討	Eツール	Windows XP	_
Windows 7/Windows Vista Windows XP	•	Windows セキュリティ正常性検証ツールのポリシー設定	の選択		Windows 7/Windows Vista Windows XP	💮 Wir	ndows セキュリティ正常性検証ツ・	-ルのボリシー設定の選択
	以下のした内	D設定を使用して、Windows セキュリティ正常性検証ッールのポリシーを定義し、 容によって、ネットワークに接続するクライアント コンピューターの要件が定義され	ます。 選択 ます。	•		以下の設定を付 した内容によって	使用して、Windows セキュリティ正常性検証り こ、ネットワークに接続するクライアント コンピュ	ノールのポリシーを定義します。選択 ーターの要件が定義されます。
	セキュ	リティ正常性ポリシーを構成する方法				セキュリティ正常	曾社ポリシーを構成する方法	
	77.	イアウォール設定				ファイアウォ	ール設定	
		「ネットワーク接続に対してファイアウォールが有効(E)				▼ ネットワ	ーク接続に対してファイアウォールが有効(E)	
	<u> 91)</u>							
		!ウイルス対策ソフトウェアが有効(⊻) 「ウイルス対策が最新の状態(T)				■ 01ルス ■ 01ルス	対策ダンドウェアが有効(型) 対策が最新の状態(T)	_
	スパー	イウェア対策の設定				自動更新の設	 定	
		「スパイウェア対策アプリケーションが有効(S)				☑ 自動更	新が有効(<u>U)</u>	
		スパイウェア対策が最新の状態(D)				セキュリティ	更新プログラムの設定	
۲ () () () () () () () () () (自動	更新の設定	<u></u>	•	4 F	🗆 🗆 🗆	ティ更新ブログラムのインストールが不十分な	クライアントのアクセスを制限する(<u>R)</u> ▼
		ОК	キャンセル					OK キャンセル

図 3.5-35 システム正常性検証ツール(SHV)の設定(Windows Server 2008 R2)③

Windows Server 2008 の場合

「Windows Vista」タブの詳細情報にチェックが入っていることを確認する。同様に Windows XP」 タブも詳細情報にチェックが入っていることを確認する。

※Windows 7 は「Windows vista」のタブの内容で動作します。

Windows セキュリティ正常性後証ツール	Windows 7, Windows Vista	<u>?1×</u>	Windows セキュリティ正常性教証ツール	Windows XP	<u>2 X</u>
Windows Vista Windows XP			Windows Vista Windows XP		
い下の設定を使用して、Windows セキュリ ます。 <u>詳細情報</u> - ファイアウォール - フィイアウォール	ティ正常性検証シール・ポリンーを定置します。ここで連択した内容により、ネットワークに接続するウライアント: - 小が有効(E)	コンピュータの要件が定義され	以下の設定を使用して、Windows セキュリティ正常性体証シール。 ます。	わシーを定義します。ここで選択した内容により、ネットワーク	こ接続するクライアントコンピュータの要件が定義され
ウイルス対策 マウイルス対策ソフトウェアが有効(少	F ウイルス対策が最新の状態D		ウイルス対策 ↓ ウイルス対策ソフトウェアが有効\少	▶ ウイルス対策が最新の状態(1)	
スパイウェア対策 ▼ スパイウェア対策アプリケーションが有効	があ) マンパウェア対策が最新の状態(1)		自動更新 「F 自動更新が有効(」)		
自動更新 ▽ 自動更新が有効(以)			- セキュリティ更新プログラムによる保護 「 セキュリティ更新プログラムのインストールが不十分なクライアン	ットのアクセスを制限する(R)	
セキュリティ更新プログラムによる保護 ビセキュリティ更新プログラムのインストー 重要およびそれ以上上	スポポイト分なガライアントのアクセスを制限する(E) ■		「重要およびそれは人上 クライアントによる最新のセキュリティ更新プログラムのチェックが	1.6要な響味(0時開放(5)	<u>127</u>
クライアントによる最新のセキュリティア	(新力ログラムのチェックが必要な環境の時間的(5) [22]		見定では、クライアントは Microsoft Update からセキュリティ 両方を選択してください。	更新プログラムを取得できます。展開に適加のプログラム取得	先が必要な場合は、次のいずれか1つまたは
既定では、クライアントは Microsoft I を選択してください。	Update からセキュリティ更新プログラムを取得できます。原間に適加のプログラム取得先が必要な場合は、パ	たのいずれか 1 つまたは南方	Windows Server Update Services	🔽 Windows Update	
☐ Windows Server Update Serv	vices 🔽 Windows Update				
	OK	キャンセル 適用(A)		[0K キャンセル 適用(A)

図 3.5-36 システム正常性検証ツール(SHV)の設定③

3.5.7. 正常性ポリシーの設定

NPS にセキュリティポリシーに対する判定基準を設定する手順を以下に示します。本ガイドでは、 検疫合格時のポリシーと検疫失敗時のポリシーを作成しています。Windows Server 2008 R2 と Windows Server 2008 で差分がある箇所については下線で示しています。

① 新しい正常性ポリシーの作成(検疫合格)

ネットワークポリシーサーバー画面にて、左画面の中の「ポリシー」を展開して「正常性ポリ シー」を右クリックし「新規」を選択する。新しい正常性ポリシーの作成画面にて、次の3項 目を設定して「OK」をクリックする。

Windows Server 2008 R2 の場合	ファイル(F) 操作(A) 表示(V) /	√ルプ(H)
・ ポリシー名 :任意(本ガイドでは「OK」)	 NPS (ローカル) RADIUS クライアントとサーバー ポリシー 	正常性ポリシー 正常性ポリシーはネット
・クライアント SHV のチェック対象:	 □ 102 (まへのクラ □ ネットワーク ポリシー ○ 正常性ポリシー □ 素 ネットワーク アクセス保護 	
すべての SHV チェックにパスしたクライ	 ■ アカウンティング ■ ● テンブレートの管理 	
アント		
・この正常性ポリシーで使用されている		」 い下のすべての SHV をパフ
SHV :		
Windows セキュリティ正常性検証ツール		
「既定の構成」を選択		
	▶ 操作: 進行中]

 アノリルフ
 第1日の
 またいの
 シスノホリ

 ●
 ●
 ●
 ●

 ●
 NPS
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●
 ●
 ●

 ●
 ●

図 3.5-37 正常性ポリシーの設定(Windows Server 2008 R2)①

<u>- | | ×</u>

ふネットワーク ポリシー サーバー Windows Server 2008 の場合 ファイル(F) 操作(A) 表示(V) ヘルプ(H) 2 🗖 🖬 🖬 **|** ポリシー名:任意(本ガイドでは「OK」) 💊 NPS (ローカル) Ⅲ 🧰 RADIUS クライアントとサーバ 正常性ポリシーはネットワークアクセス保護(NAP)で使用されます。正常性オ コンピュータがネットワークにアクセスするために必要な構成を指定できます。 E Control Contr ・クライアント SHV のチェック対象: 新しい正常性ポリシーの作成 ■ 1900年36072
 ● ネットワーク ポリシー
 ● 正常性ポリシー
 ■ ネットワーク アクセス保護
 ■ アカウンティング すべての SHV チェックにパスしたクライア 設定 正常性ポリシー設定を構成します。正常性ポリシーを強制するには、1 つ以 上のネットワーク ポリシーの正常性ポリシー条件に、その正常性ポリシーを追 加します。 ント ポリシー名(N) ・この正常性ポリシーで使用されている 0 クライアント SHV のチェック対象(L): すべての SHV チェックにパスしたクライアン SHV: -この正常性ポリシーで使用されている SHV(V): Windows セキュリティ正常性検証ツール Τ 名前 Windows セキュリティ正常性検証ツール • キャンセル 適用(A)

図 3.5-38 正常性ポリシーの設定(Windows Server 2008)①

OK

新しい正常性ポリシーの作成(検疫失敗)

①と同様にポリシーを新規作成し、下記3項目を設定して「OK」をクリックする。

Windows Server 2008 R2 の場合

- ・ポリシー名:任意(本ガイドでは「NGI)
- ・クライアント SHV のチェック対象: 1つ以上のSHV チェックに失敗したクライ
- アント
- ・この正常性ポリシーで使用されている SHV :

Windows セキュリティ正常性検証ツール 「既定の構成」を選択



図 3.5-39 正常性ポリシーの設定(Windows Server 2008 R2)②

Windows Server 2008 の場合

- ・ポリシー名:任意(本ガイドでは「NG」)
- ・クライアント SHV のチェック対象:
 1つ以上の SHV チェックに失敗したクライアント
- ・この正常性ポリシーで使用されている SHV :

Windows セキュリティ正常性検証ツール



図 3.5-40 正常性ポリシーの設定(Windows Server 2008)2

③ 正常性ポリシーの確認
 NPSの右画面にて、作成した2つのポリ
 シーが存在する事を確認する。

🛸 ネットワーク ポリシー サーバー	
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	
🧢 🔿 🖄 📧 🖬	
	性ポリシーにはネットワーク アウセス保護(NAP) で使用されます。正常性ポリシーを使用すると、NAP ウライアント コンピューゲがネットワーグ、アウセスするため、必要な構成を指定できます。 の少なくとも 1 つが失敗した場合、クライアントはこのポリシーの条件を満たします。 5 セキュリティ正常性検証ツール

図 3.5-41 正常性ポリシーの設定③

3.5.8. ネットワークポリシーの設定

認証後 VLAN と検疫 VLAN のポリシーを作成する手順を以下に示します。

(1) 認証後 VLAN のポリシー作成

- ネットワークポリシーサーバー画面にて、 左画面の中の「ポリシー」を展開し「ネ ットワークポリシー」を右クリックして 「新規」を選択すると、ウィザードが開 始される。
- 第しいネットワークポリシー画面にて、 ポリシー名(本ガイドでは「認証後 VLAN100」)を入力して「次へ」をクリ ックする。
- 条件の追加(ユーザーグループ)
 新しいネットワークポリシー画面にて「追加」をクリックする。
 条件の選択画面にて「ユーザーグループ」
 を選択し「追加」をクリックする。

iしいネットワ-	-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。
200	
	N
ボリシー名(音	y): utoni
leven i & cui	100
ネットワーク接	続の方法
NPS (ご接続要 べ) 次固有] を	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するか、[『指定する』とができます。
· ネットワー	ケアクセス サーバーの種業買(S):
指定なし	
Thateore	
○ べンダ固有	¶(<u>V</u>):
10	
	前へ(P) 次へ(N) 完了(E) キャンセル

図 3.5-42 認証後 VLAN のポリシー作成①

	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 要です。
の選択	
件を選択し、	[追加]をクリックします。
ルーン Windo あること しいビュ	ws グループ ws 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がに所属している必要が こを指定します。 コータ グループ 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
ユーサ ユーザ	۲ーヴループ 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すれかに所属している必要があることを指定します。
UAF しかー HCAP Protoc サーバ	ション グループ ・ロケーション グループの条件には、このボリシーに一致するために必要な HGAP (Host Gredential Authorization 20)ロケーション グループを指定します。HGAP プロトコルは、NPS と一部のサード パーティ製ネットワーン アクセス - (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 3.5-43 認証後 VLAN のポリシー作成②

④ ユーザーグループ画面にて「グループの 追加」をクリックする。

///	

図 3.5-44 認証後 VLAN のポリシー作成③

 ⑤ グループの選択画面にて、場所の指定が 該当ドメインである事を確認し、<u>3.5.3</u>に て作成したグループ名(本ガイドでは 「Sales」)を入力する。「OK」をクリッ クして画面を閉じる。

ヴループ 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> : レグルーマ	オゴミニークトの5番番(の)
リンパーン 場所を指定してください(E):	
example.co.jp	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</u>)(<u>E</u>):	
Sales	名前の確認(<u>C</u>)
図 3.5-45 認証後 VLAN のポリシー	·作成④

⑥ 条件の追加(正常性ポリシー)
 新しいネットワークポリシー画面にて「追加」をクリックする。
 条件の選択画面にて「正常性ポリシー」
 を選択し「追加」をクリックする。
 正常性ポリシー画面にて、3.5.7で作成した検疫合格時のポリシー(本ガイドでは「OK」)を選択し、「OK」をクリックする。

新しいネットワー	-ク ポリシー	×
	条件の指定	
	接続要求につい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。	
条件の選択		×
条件を選択し、	「追加」をクリックします。	
日の相 日の相 日の相 す。	2月 第90条件は、NAP 正常性ステートメント (SoH) などの指定した機構で識別できるクライアントだけにポリシーを刺取しま	4
MS-Se MS-サ を取得	arvice グラス ービス クラスの条件は、接続するコンピュータが、選択したプロファイル名に一致する DHCP スコープから IP アドレス リース している必要があることを指定します。	
₩ 王業福	は <mark>わ</mark> ター ポリシーの条件は、正常性ポリシーで指定された正常性条件に適合するクライアントだけにポリシーを適用します。	1
אר א ארא ארא ארא ארא ארא ארא ארא ארא אר	城ごコンピュータ す応コンピュータの条件は、接続するコンピュータが NAP に参加できるかどうかを指定します。この機能は、クライアント コン が NPらに正常性えテートメントを送信するかどうかによって決まります。	
かい オペレー オペレー オペレー オペレー オペレー	ー ティングシステム ティングシステムの条件は、クライアントコンピューダ構成がこのポリシーに一致するために必要なオペレーティングシステ 期、およびアーキテクチャを指定します。	
	正常性ポリシー	×
	適用する正常性ポリシーを選択します。新しい正常性ポリシーを作成するには、 (新規) をグリックします。	
	正常性ポリシー(日):	
	<mark>⊙K</mark>	
	OK ++)72/	1
		_

図 3.5-46 認証後 VLAN のポリシー作成⑤

アクセス許可の指定
 「次へ」をクリックして進む。



図 3.5-47 認証後 VLAN のポリシー作成⑥

⑧ 認証方法の構成

「次へ」をクリックして進む。

新しいネットリー	-0 #J9-
	認証方法の構成 接続要求がに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、ネッドワーク 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ェートされます。
EAP の種類(P): 上へ称動(U) 下へ称動(U) 下へ称動(U)
〕 	<u>編集(E)</u> 前邸余(R)
セキュリティレ ▼ Microsoft ▼ パスワー 「 パスワー 「 晴号化認識 「 晴号化認識 「 暗号化認識 「 記証方法を 「 コンピュータ	べみの低い認証方法: 暗号化記録IJバージョン 2 (MS-CHAP v2)(V) ドの期間が以れた後も、ユーザー(J/12ワードの変更を許可する(H) 暗号化記録I (MS-CHAP)(Y) ドの期間が以れた後も、ユーザー(J/12ワードの変更を許可する(X) 証 (CHAP)(U) 17(1/42) 記録I (PAP、SPAP)(T) をオジュートせずにジライアント(法務会許可する(L) 20正常性チェックのみを実行する(F)
	前へ(P) 洗へ(N) 完了(F) キャンセル
	図 3.5-48 認証後 VLAN のポリシー作成⑦

9 制約の構成

「次へ」をクリックして進む。

新しいネットワーク ポリシー 🛛 🛛 🛛 🔺
お終うの構成 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。接続要求が削約と一致しない場合 合、NFS は接続要求を自動的に拒否します。刺約りはオブションです。制約を構成しない場合は、じたく1をジリックしてだ さい。
Cのスットワーク・ガルシ・クロ総合権機長はます。 マイたの制造が接続要素に一致じない場合、ネットワーク アクセスは描言されます。 1495(5) マション タイムアウト Called-Station=D Gald-Station=D G 日だは時以の制限 ア NAS ポートの種類
<u> 前へ(P)</u> <u> 流へ(N)</u> <u> </u> 売了(F) <u></u> <u></u> キャンセル

図 3.5-49 認証後 VLAN のポリシー作成⑧

⑩ 設定の構成(属性追加)
 新しいネットワークポリシー画面にて、
 左画面の中の「標準」を選択し、右画面の「追加」をクリックする。



図 3.5-50 認証後 VLAN のポリシー作成⑨

- 標準 RADIUS 属性の追加画面にて、アクセスの種類を「802.1X」に設定し、下記3つの属性を追加する。
 ・Tunnel-Medium-Type = "802"
 ・Tunnel-Type = "VLAN"
 ・Tunnel-Pvt-Group-Id = "100" (所属す
 - る VLAN ID)



図 3.5-51 認証後 VLAN のポリシー作成①

 追加属性の確認
 認証成功時に返す属性を確認し、「次へ」 をクリックする。
 ここで、「Framed-Protocol」と 「Service-Type」は削除しても良い。

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	ソワーク ボリシー条件わよび制料3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 設定(S):	ます。 2スが44可される場合、この設定が適用されます。
RADIS 時代 ● 経営 ● パング回有 ▲ 21ワークアクセス保護 ● NAP 法制 ● 松泉水園 ● ベング回右 ● パングの2015 ● パングの2015 ● アンパンクあよび帯 熱情 ● ドランパンタ ● 「日本 ● 「日本 <tr< th=""><th>ちの管性を APOLIS シティアントに送けまたには 建築 PADILS 開せた発行し、[編集] クリックします。最終を執続したと、書件は APOLIS シライアントに送信されません。必要 た間性については、RADIUS タライアントのドキュメントを参照してくだとい。 著性(7) 名前 「Frandes-Protocol PPP Service-Type Franed Turnel-Medium-Type Franed Turnel-Medium-Type Virtual LANs (VLAN) Turnel-Medium-Type 100 这世か(D)_ 編集(E)_ 影励(F)</th></tr<>	ちの管性を APOLIS シティアントに送けまたには 建築 PADILS 開せた発行し、[編集] クリックします。最終を執続したと、書件は APOLIS シライアントに送信されません。必要 た間性については、RADIUS タライアントのドキュメントを参照してくだとい。 著性(7) 名前 「Frandes-Protocol PPP Service-Type Franed Turnel-Medium-Type Franed Turnel-Medium-Type Virtual LANs (VLAN) Turnel-Medium-Type 100 这世か(D)_ 編集(E)_ 影励(F)
	前へ(P) 次へ(N) 完了(F) キャンセル

図 3.5-52 認証後 VLAN のポリシー作成①

🚯 「完了」をクリックして画面を閉じる。

(2) 検疫 VLAN のポリシー作成

- ネットワークポリシーサーバーの画面に て、左画面の中の「ポリシー」を展開し 「ネットワークポリシー」を右クリック して「新規」を選択すると、ウィザード が開始される。
- 新しいネットワークポリシー画面にて、 ポリシー名(本ガイドでは「検疫 VLAN30」)を入力して「次へ」をクリッ クする。



図 3.5-53 検疫 VLAN のポリシー作成①

③ 条件の指定

(1)の③~6と同様に「ユーザーグル ープ」と「正常性ポリシー」を追加する。 「正常性ポリシー」については、<u>3.5.7</u>で 作成した検疫失敗時のポリシー(本ガイ ドでは「NG」)を選択する。最後に「次 へ」をクリックして進む。

新しいネットワー	ر المراجع
	条件の指定 接続要求につい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。
条件の選択	X
条件を選択し、	「追加」をクリックします。
ネットワーク アク	セス保護
D 01	25 類の条件は、NAP 正常性ステートメント (SoH) などの指定した機構で識別できるクライアントだけにポリシーを制限しま
MS-Se MS-5e MS-サ を取得	wrize <u>757</u> ービス クラスの条件は、接続するコンピュータが、選択したプロファイル・名に一致する DHOP スコープから IP アドレス リース している必要があることを指定します。
	#05~ ポリシーの条件は、正常性ポリシーで指定された正常性条件に適合するクライアントだけにポリシーを適用します。
NAP # NAP # ピュータ	は(ニンピュータ) ガロコンピュータの条件は、接続するコンピュータが NAP に参加できるかどうかを指定します。この機能は、クライアント コン が NPS に正常性ステートソントを送信するかどうかによって決まります。
きょう オペレー	ティングシステム
正常性ホリソー	
適用する正常 [新規] をクリッ	性ポリシーを選択します。新しい正常性ポリシーを作成するには、 道加(D) キャンセル / します。
正常性ポリシ NG	(H): 新規(W)編集(E)削除(R)
	OK キャンセル 法へ(N) 完了(F) キャンセル

図 3.5-54 検疫 VLAN のポリシー作成②

- ④ アクセス許可の指定、認証方法の構成、制約の構成をそれぞれ「次へ」で進める。
- ⑤ 設定の構成(属性追加) 新しいネットワークポリシー画面にて、 左画面の中の「標準」を選択し、右画面 の「追加」をクリックする。標準 RADIUS 属性の追加画面にて、アクセスの種類を 「802.1X」に設定し、下記3つの属性を 追加する。
- •Tunnel-Medium-Type = "802"
- •Tunnel-Type = "VLAN"

・Tunnel-Pvt-Group-Id = "30"(所属する VLAN ID)

⑥ NAP 強制(自動修復無し) 新しいネットワークポリシー画面にて、 左画面の中の「NAP 強制」を選択する。 右画面にて「制限付きアクセスを許可す る」をチェックし、「自動修復」のチェッ クを外して「次へ」をクリックする。



図 3.5-55 検疫 VLAN のポリシー作成③

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	区
このネットワークボ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 設定(S): RADLIS 国性	ます。 とスが許可される場合、この設定が適用されます。 C 時間を見てに完全なスキットワーク アクセス 数件可する(N) 第二字 からりまますが明 ターレック リーク かられるままでは、また、またのであた 日本をは、第二
 ● 標準 ✓ ✓ ジョンクアクセス(保護 ▲ 201-ワアクセス(保護 ▲ NAP 強制 	指定した日本代を知識のがイッシーク・クランスを計りします。信定した日本代題 また、本行サークの場合は、単純していないとし、シックランにより、 されたトリークのはないます。 日代の 007/09/14 - ・ はれい 00035 - ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
● 拡張状態 ルーライングとリモート アクセ 入 ● マルチリンクおよび帯域幅 作品の 日本	(単規していないクライアントがアクセスできるのは、更新プログラム用に制限されたネットワークのみです。 クのみです。 のした、フループとトラブルシューティングの URL 修能サーバ、クループ、トラブルシューティングの URL、または両方を構成するには、(構成) を切っかして(だだい)。 構成(M)。
● IP フィルタ 桑 暗号化 ✓ IP 設定	自動解資 □ シライアントコンピューシの自動修復を有効にする(U) このポリシーで完美されている正常性の要件を満たしていないコンピュータを自動 時気(感覚します。 ▼
	前へ(P) 次へ(N) 売了(F) <u>キャンセル</u>

図 3.5-56 検疫 VLAN のポリシー作成④

- 注意:NPS はデフォルトで自動修復が有効となっていますが、本ガイドでは検疫 VLAN に隔離 された NAP クライアントが手動で修復を行うことを想定しているので無効にしています。 自動修復機能を有効のまま構築する場合は、この手順を省略して下さい。
- ⑦ 「完了」をクリックして画面を閉じる。以上で NPS の設定は終了です。

3.5.9. DHCP サーバの設定

認証後 VLAN、検疫 VLAN および認証前 VLAN のネットワーク IP アドレスを配布する DHCP サーバの設定手順を示します。本ガイドで設定する値を以下の表に示します。

認証後 VLAN100		
アドレス範囲	192.168.100.50~192.168.100.100	
サブネットマスク	255.255.255.0	
デフォルト	192 168 100 254	
ゲートウェイ	192.100.100.234	
検疫 VLAN30		
アドレス範囲	192.168.30.50~192.168.30.100	
サブネットマスク	255.255.255.0	
デフォルト	102 168 30 254	
ゲートウェイ	192.108.30.234	
認証前 VLAN10		
アドレス範囲	192.168.10.50~192.168.10.100	
サブネットマスク	255.255.255.0	
デフォルト	102 169 10 254	
ゲートウェイ	192.108.10.234	
DNS サーバ		
10.51.0.1		

表 3-7 DHCP の設定内容

① 「スタート」→「管理ツール」→「DHCP」 を開く。

左画面から該当ドメインを展開し、 「IPv4」を右クリックして「新しいスコ ープ」を選択するとウィザードが開始さ れる。



図 3.5-57 DHCP サーバの設定①

 ウィザードが開始されたら、スコープ名 (本ガイドでは「認証後 VLAN100」)を 入力し「次へ」をクリックする。

コープ名 識別するための:	しコーフ名を指定する必要があります。1月8月6週加することができます。
このスコープのゴのように使用さ	。 前と説明を入力してください。この情報版を入力することで、ネットワークでこのスコープがど しるかをすばやく判測所することができます。
名前(<u>A</u>):	ISIE住VLAN100
1说8月(<u>D</u>):	
	< 戻る(B) (次へ(N)) キャン

図 3.5-58 DHCP サーバの設定②

 ③ IP アドレスの範囲 新しいスコープウィザード画面にて「認 証後 VLAN100」に配布する IP アドレス の範囲(<u>表 3.5-2</u>)を入力し「次へ」を クリックする。

スコープが割り当てるアドレス	の範囲を指定してください。	
開始 IP アドレス(<u>S</u>):	192 . 168 . 100 . 10	
終了 IP アドレス(<u>E</u>):	192 . 168 . 100 . 210	
サブネット マスクは、IP アド ID に使うかを定義します。†	/スのビットのどれだけをネットワーク/サブネット ID に使い、どれだけす ナブネット マスクは、長さもしくは IP アドレスを使って指定できます。	ይホスト
長さ(」):	24	

図 3.5-59 DHCP サーバの設定③

- ④ 除外の追加「次へ」をクリックする。その後リース期間も「次へ」をクリックする。
- ⑤ DHCP オプションの構成
 「今すぐオプションを構成する」(デフォルト)を選択し「次へ」をクリックする。
- ⑥ ルーター(デフォルトゲートウェイ)
 デフォルトゲートウェイの IP アドレス
 (表 3.5-2)を入力し、「次へ」をクリックする。

クライアントが使用するルーク	ーの IP アドレスを追加するには、そのアドレスを下に入力して	ください。
	追加(D)	
192.168.100.254		
	TA(Q)	

図 3.5-60 DHCP サーバの設定④

⑦ ドメイン名および DNS サーバー
 DNS サーバの情報(表 3.5-2)を入力し
 「次へ」をクリックする。

新しいスコープ ウィザード		
ドメイン名および DNS サーバー ドメイン ネーム システム (DNS) は、ネットワーク上の 行います。	ウライアントが使用するドメイン名のマッフ	
ネットワーク上のクライアント コンピュータが DNS 名の解決	夫のために使う親ドメインを指定すること	ができます。
親ドメイン(<u>M</u>):		
ネットワーク上の DNS サーバーを使用するようにスコープ スを入力してください。	クライアントを構成するには、それらのサ	ーバーの IP アドレ
サーバー名(S):	IP アドレス(<u>P</u>):	
dc.example.co.jp		追加(<u>D</u>)
解決(E)	1051.0.1	育耶余(<u>E</u>)
		上へ(山)
		下へ(0)
	< 戻る(B) 次へ(N) >	キャンセル

図 3.5-61 DHCP サーバの設定⑤

- ⑧ WINS サーバの設定
 「次へ」をクリックする。
- ⑨ スコープのアクティブ化「今すぐアクティブにする」(デフォルト)を選択し「次へ」をクリックする。
- 10 「完了」をクリックして画面を閉じる。
- ① ①~⑩と同様に「検疫 VLAN」および「認証前 VLAN」のスコープを作成する。

CHCP			- D ×
ファイル(E) 操作(A) 表示(V) ヘルブ(H)			
🗢 🔿 🗡 📷 🖼 🖉 👘			
P DHCP	IPv4		
□ 🕞 dc.example.co.jp	DHCP サーバーの内容	状態	説明
□ ● ● 第二章 田 ● スコープ [192.168.10.0] 認証前VLAN10	📄 スコープ [192.168.10.0] 認証前VLAN10	** アクティブ **	
□ □ スコープ [192.168.30.0] 検疫 VLAN30	□ スコープ [192.168.30.0] 検疫 VLAN30	** アクティブ **	
🗉 🧰 スコープ [192.168.100.0] 認証後VLAN100	□ スコープ [192.168.100.0] 認証後VLAN100	** アクティブ **	
_ 📴 サーバー オプション	■ サーバー オブション		
		_	
	•		Þ

図 3.5-62 DHCP サーバの設定⑥

以上で DHCP サーバの設定は終了です。

3.6 NAP クライアントの設定

3.6.1. 導入ステップ

本ガイドにおける NAP クライアントの初期導入の流れを以下に示します。

ここで、クライアント端末は Windows 7、Windows Vista および Windows XP SP3 とします。

- (1) コンピュータの管理者権限のあるユーザで端末にログオンする。
- (2) 端末を Windows ドメイン参加させる。
- (3) 端末を再起動すると、グループポリシーにより、NAP クライアント設定が自動的に適用される。
- (4) Active Directory に登録したユーザで端末にログオンする。

初期導入時に上記ステップを実施したクライアント端末は、以降シングルサインオン構成の NAP クライアントとして利用することができます。

3.6.2. Windows ドメイン参加の設定

クライアント端末をWindows ドメインに参加させる手順を以下に示します。本ガイドではWindows 7 を使用した設定手順を示していますが、Windows Vista、Windows XP に関しても同等の手順で Windows ドメインに参加させることができます。

- Administrator もしくはコンピュータの 管理者権限のあるユーザにて端末にログ オンする。
- 端末を認証スイッチのポートに接続し、 コマンドプロンプトにて認証前 VLAN の IP アドレス(本ガイドでは 「192.168.10.0/24」)を取得しているこ と、ドメインコントローラへ PING を実 行して通信可能であることを確認する。 また、DNS の確認として、DNS に設定 されている Windows ドメイン内サーバ への PING も実行する。

🖬 בערד לערד 🔤	
C:¥>ipconfig	_
Windows IP 構成	
Wireless LAN adapter ワイヤレス ネットワーク接続:	
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス:	
イーサネット アダプタ ローカル エリア接続:	
接続固有の DNS サフィックス : example.co.jp IPv4 アドレス : 192.168.10.10 サブネット マスク : 255.255.255.0 デフォルト ゲートウェイ : 192.168.10.254	
Tunnel adapter ローカル エリア接続*:	
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス:	
Tunnel adapter ローカル エリア接続* 2:	
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス: example.co.jp	
Tunnel adapter ローカル エリア接続* 6:	
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス:	
C:¥>ping 10.51.0.1	
10.51.0.1 に ping を送信しています 32 バイトのデータ: 10.51.0.1 からの応答: バイト数 =32 時間 <1ms TTL=126 10.51.0.1 からの応答: バイト数 =32 時間 <1ms TTL=126	

図 3.6-1 Windows ドメイン参加の設定①

L

③ 端末が Windows 7 / Windows Vista の場合、「スタート」→「コントロールパネル」→「システム」 をクリックしてシステムの画面を開き、「コンピュータ名、ドメインおよびワークグループの設定」 にて、現在コンピュータがワークグループ構成である事を確認し「設定と変更」をクリックする。

ンピュータ名、ドメインお	よびワークグループの設定	+
コンピュータ名:	PC1	御設定と変更(C)
フル コンピュータ名:	PC1	
コンピュータの説明:		
ワークグループ:	WORKGROUP	

図 3.6-2 Windows ドメイン参加の設定②

④ 端末が Windows XP の場合、「スタート」→「コントロールパネル」→「システム」をクリックしてシステムのプロパティ画面を開き、「コンピュータ名」のタブにて、現在コンピュータがワークグループ構成である事を確認する。

システムのプロパティ画面にて、「変更」
 をクリックする。



図 3.6-3 Windows ドメイン参加の設定③

⑥ コンピュータ名/ドメイン名の変更画面にて、次のメンバに「ドメイン」を選択し、参加する Windows ドメイン名を入力する。(本ガイドでは「example.co.jp」)

次に、「詳細」をクリックし、DNS サフ ィックスと NetBIOS コンピュータ名画 面にて、「このコンピュータのプライマ リ DNS サフィックス」に DNS サーバ名 を入力する。(本ガイドでは 「example.co.jp」)

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。詳細面音報	われます。
コンピューター名(C): PC3	-9-"
フル コンピューター名: PC3	
[]][]][]][]][]][]][]][]][]][]][]][]][]]	7 ID(<u>N</u>)
所属するグループ ● ドメイン(D): example.co.jp	0
◎ ワークグループ(₩): ACC	
OK キャンセル	
DNS サフィックスと NetBIOS コンピューター名	×
このコンピューターのプライマリ DNS サフィックス(P): example.co.jp	
▼ドメインのメンバーシップが変更されるときにプライマリ DNS サフィックスを変更	€する(C)
NetBIOS コンピューター名(N): PC3	
この名前は、古いコンピューターやサービスとの相互運用に使用されます。	
ОК	キャンセル

図 3.6-4 Windows ドメイン参加の設定④

 「OK」をクリックして画面を閉じると、 ダイアログが表示される。
 <u>3.5.3</u>にて登録したユーザ名およびパス ワードを入力し、「OK」をクリックする。

Windows セキュリティ
コンピュータ名/ドメイン名の変更 ドメインに参加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 ワードを入力してください。
user01 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
OK キャンセル

図 3.6-5 Windows ドメイン参加の設定⑤

 Windows ドメインに参加されたことを 示すメッセージが表示される。



図 3.6-6 Windows ドメイン参加の設定⑥

注意:このメッセージが表示されない場合は、設定をもう一度見直して下さい。(7.1章参照)

- ⑨ 「OK」をクリックして画面を閉じ、端末を再起動する。
- 10 Windows ログオン画面にて、ログオン先が
 ②で入力したユーザでログオンする。(本ガイドでは「user01」)
- ※Windows XP を NAP クライアントとして構成した場合⑩の手順にてドメインログオンした後、再度 OS 再起動を行い⑩の手順を実施してください。
3.6.3. 設定の確認

NAP クライアントの設定が完了したことを確認する方法を以下に示します。

①コマンドプロンプトを開き、NAP クライアントステータスを確認するコマンドを実行する。

netsh nap client show state

EAP 検疫強制クライアントの状態で「初期化済み=はい」となっていること、Windows セキュリ ティ正常性エージェントの状態で「初期化済み=はい」となっていることを確認する。

ID	= 78623
名前	= EAP 検疫強制クライアント
説明	= EAP 検疫強制クライアント
バージョン	= 1.0
ベンダ名	= Microsoft Comporation
登録日	=
初期化済み	= (はい)
System Health Agent (S	(4) の状態:
ID	= 78744
名前	= Windows セキュリティ正常性エージェント
説明	= ₩indows セキュリティ正常性エージェントは、管理者が定象
したポリシーに、コンビ	ニータが準拠しているかどうかをチェックします。
バージョン	≓ 1.0
ベンダ名	= Microsoft Corporation
登録日	=
初期化済み	= はい
エラーのカテゴリ	= なし
修復の状態	= 成功
修復の割合	= 0
修正のメッセージ	= (\$2\$7937214) - Windows セキュリティ正常性エージェント
は、セキュリティ状態の	更新を終了しました。
確認の結果	=
修復の結果	=
0K	

図 3.6-7 設定の確認①

②コマンドプロンプトの ipconfig にて IP アドレスを確認する。

認証や検疫の結果に応じたネットワークにクライアント端末が所属している事を確認する。 (下図の場合、認証後 VLAN100:192.168.100.0/24 に所属している。)

ש איז לעד של גער של גער	X
接続固有の DNS サフィックス :	_
C:¥Users¥user01>ipconfig	
Windows IP 構成	
イーサネット アダブタ ローカル エリア接続:	
接続回有の DNS サフィックス : nap.alaxala.com IPv4 アドレス	
Tunnel adapter ローカル エリア接続*:	
メディアの状態メディアは接続されていません 接続固有の DNS サフィックス : nap.alaxala.com	
Tunnel adapter ローカル エリア接続* 6:	
メディアの状態メディアは接続されていません 接続回有の DNS サフィックス:	
C:¥Users¥user01>	-

図 3.6-8 設定の確認②

IP アドレスが認証前 VLAN のまま変更しない場合は、<u>7.3</u>の方法を試してみて下さい。

4. 検疫ネットワークの構築(固定 VLAN(ポート単位)構成)

4.1 概要

検疫ネットワークの固定 VLAN(ポート単位)構成を、以下のように定義します。



NAP クライアント端末

図 4.1-1 検疫ネットワークの基本構成(固定 VLAN(ポート単位)構成)

コアスイッチには AX3600S を配置し、VRRP を用いて装置を冗長化します。また、装置間はリンク アグリゲーションを用いて回線を冗長化します。

NPS として稼動する Windows Server 2008、検疫により隔離された端末を治療する修復サーバ、および検疫後にアクセス可能な業務サーバは、コアスイッチ配下に接続します。コアスイッチ同士の経路交換には、OSPF 等のルーティングプロトコルを使用します。

認証スイッチには AX2400S, AX1240S を配置し、IEEE802.1x 固定 VLAN(ポート単位)モードで認証を 行い、スパニングツリーを用いて冗長化します。

検疫を行う端末は、認証スイッチに直接またはハブを介して接続します。

また、ユーザ1とユーザ2に分け、認証および検疫成功後アクセス可能な業務サーバを分けます。

4.2 検疫ネットワーク構成図





図 4.2-1 ネットワーク構成図(固定 VLAN(ポート単位)構成)

ここで、認証スイッチのポートを以下のように設定します。

表 4-1 認証スイッチのポート設定

認証 スイッチ	用途	ポート番号	ポート種別	認証方式	VLAN
	認証用	0/1~0/10	アクセスポート	IEEE802.1X 認証 (固定 VLAN(ポート単位))	100
AX2400S		0/11~0/20	アクセスポート	IEEE802.1X 認証 (固定 VLAN(ポート単位))	200
	上位スイッチ との通信用	0/47~0/48	トランク ポート	_	_
	認証用	0/1~0/10	アクセスポート	IEEE802.1X 認証 (固定 VLAN(ポート単位))	100
AX1240S		0/11~0/20	アクセスポート	IEEE802.1X 認証 (固定 VLAN(ポート単位))	200
	上位スイッチ との通信用	0/25~0/26	トランク ポート		

各 VLAN の定義および VLAN とサーバ間通信の可否を以下の表に示します。

VLAN 名	VLAN ID	ネットワーク IP アドレス	用途	設置サーバ
業務サーバ用 VIAN	50	10.50.0.0/24	検疫後に通信可能なサーバが所属 オス VI AN	業務サーバ#1 業務サーバ#2
Windows Server 2008 用 VLAN	51	10.51.0.0/24	NPS、ドメインコントローラ、 DHCP などのサービスが稼動して いる Windows Server 2008 が所属 する VLAN。	Windows Server 2008
修 復 サ ー バ 用 VLAN	52	10.52.0.0/24	検疫により隔離された端末を修復 するためのサーバが所属する VLAN。	修復サーバ
クライアント用 VLAN 1	100	192.168.100.0/24	ユーザが所属する VLAN。	_
クライアント用 VLAN2	200	192.168.200.0/24		
管理用 VLAN	1000	172.16.0.0/24	各装置を管理するための VLAN。	—

表 4-2 VLAN の定義

表 4-3 VLAN-サーバ間通信の可否

		送信先	VL	AN	業務	業務	Windows	修復
送信元			100	200	サーバ#1	サーバ#2	Server 2008	サーバ
	100	認証失敗		×	×	×	0	0
		検疫失敗		×	×	×	0	0
		検疫成功		×	0	0	0	0
VLAN	200	認証失敗	×		×	×	0	0
		検疫失敗	×		×	×	0	0
		検疫成功	×		0	×	0	0

凡例: 〇 通信可 × 通信不可

ユーザ1とユーザ2でアクセス可能なネットワークを変更するには、ユーザ1とユーザ2が所属する 回線および VLAN を分けて、それぞれ所属する VLAN にフィルタを設定することで実現できます。

4.3 構築ポイント

図 4.2-1の検疫ネットワーク構成図について、構築ポイントを以下に示します。

4.3.1 AX に関する構築ポイント

認証スイッチおよびコアスイッチの設定について、必須項目と推奨項目を示します。必須項目は検疫 を行う上で必要な項目、推奨項目はネットワークを構築する上で注意すべき項目となっています。

必須項目

(1) クライアント用 VLAN をアップリンク側のポートに追加する。

ユーザ認証前に Windows ドメインヘログオンするため、クライアント用 VLAN から Windows Server 2008(ドメインコントローラ)へ通信ができるよう、クライアント用 VLAN をアップリンク 側のポートに追加します。

(2) 認証前および正常性ポリシー違反時にアクセス許可するフィルタ条件を設定する。

認証の設定を行ったポートは、認証前のすべての通信が遮断されます。表 4.2-3に示すように、 認証前および正常性ポリシー違反の端末は Windows Server 2008(ドメインコントローラ)と修復 サーバと通信可能とします。この設定は、認証専用 IPv4 アクセスリストを作成してポートに適用 します。また、ARP リレーの設定も必要です。この他に、DHCP を使用する場合は DHCP 通信を 許可する必要があります。

本ガイドでは、次のアクセスリストを作成して、認証スイッチに適用しています。

- (a) Windows Server 2008「10.51.0.1」との通信を許可する
- (b) 修復サーバ「10.52.0.1」との通信を許可する
- (c) DHCP 通信を許可する
- (3) 認証スイッチと端末との間にハブを設置する場合、EAPOL フォワーディング機能のあるハブ を用いる。

IEEE802.1X 認証を行うため、認証スイッチと端末との間に設置するハブには EAPOL フォワー ディング機能が必要です。AX1200S には EAPOL フォワーディング機能が実装されています。

(4) デフォルトルートを設定する。

Windows Server 2008 と通信を行うため、認証スイッチにデフォルトルートを設定します。

(5) VLAN にフィルタを設定する。

表 4.2-3に示す VLAN 間通信の可否を、フィルタを用いて実現します。

本ガイドでは、次の2つのアクセスリストを作成し、それぞれ認証専用 IPv4 アクセスリストおよび VLAN200 に適用することで実現しています。

<認証専用 IPv4 アクセスリスト>

- (a) DHCP 通信を許可する。
- (b) Windows SERVER2008「10.51.0.1/24」への通信を許可する。
- (c) 修復サーバ「10.52.0.1/24」への通信を許可する。

<VLAN200 用アクセスリスト>

- (a) VLAN100「192.168.100.0/24」への通信を拒否する
- (b) 業務サーバ#2「10.50.0.2」への通信を拒否する
- (c) すべての通信を許可する

推奨項目

(6) 認証スイッチの IEEE802.1X 端末検出機能を auto に設定する。

認証スイッチの IEEE802.1X 端末検出機能 auto に設定します。(詳細は、「認証ソリューション ガイド」を参照して下さい。)

(7) 認証スイッチの非認証状態保持時間を調整する。

IEEE802.1X 認証機能を有効に設定した Windows 端末は、起動時にコンピュータの IEEE802.1X 認証を行い、ユーザログオン時にユーザの IEEE802.1X 認証を行います。本ガイドの検疫ネット ワークでは、コンピュータの認証が失敗する構成のため、次のユーザ認証が行えるようになるま で非認証状態保持時間(デフォルト値:60秒)かかります。デフォルト値のままではユーザ認証 が失敗する場合があるので、短い値に設定します。本ガイドでは、非認証状態保持時間を5秒に 設定しています。(詳細は注意事項「6.2.1非認証状態保持時間の設定について」を参照)

(8) RADIUS サーバ通信 dead interval 時間を調整する。(AX1200S)

RADIUS サーバへの認証がタイムアウトした場合、2 台目以降に設定された RADIUS サーバへ 切替えます。その後再び 1 台目の RADIUS サーバを選択するまでの時間(dead interval)のデフォ ルト値は 10 分です。RADIUS サーバが 1 台のみで構成されるシステムにおいて、RADIUS サー バのタイムアウトを検出すると dead interval に設定された時間 RADIUS サーバへのアクセスを行 いません。RADIUS サーバが 1 台で構成される場合、dead interval を短い値に設定してください。 本ガイドでは dead interval を 0 分に設定しています。なお、AX2400S/AX3600S の IEEE802.1X 認証では常に 1 台目に設定した RADIUS サーバより認証を始めます。

(9) コアスイッチ間の回線にリンクアグリゲーションを設定する。

コアスイッチ間の回線を冗長化するため、リンクアグリゲーションを設定します。本ガイドで はスタティックモードを用いています。

(10) VRRP のマスタ、STP のルートブリッジを設定する。

本ガイドでは、core#1 の仮想ルータ優先度を「200」、core#2 の優先度を「100」として、core#1 をマスタに設定しています。また、core#1 のブリッジ優先度を「4096」、core#2 のブリッジ優先 度を「8192」として、core#1 をルートブリッジに設定しています。

4.4 AX の設定

4.4.1 AX1240S のコンフィグレーション

AX1240S の設定例を示します。

(1) 基本設定

AX1240S の設定				
ポート VLAN の設定				
<pre>(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 100 (config-vlan)# state active (config)# vlan 200 (config-vlan)# state active (config)# vlan 1000 (config-vlan)# state active</pre>	VLAN1 は使用しないため、無効にします。 クライアント用 VLAN として VLAN100、200 管理用 VLAN として VLAN1000 を作成します。			
スパニングツリーの設定				
<pre>(config)# spanning-tree single (config)# spanning-tree single mode rapid-stp (config)# spanning-tree mode pvst (config)# no spanning-tree vlan 100, 200, 1000 (config)# interface range fastethernet 0/1-20 (config-if-range)# spanning-tree portfast</pre>	シングルスパニングツリーを有効にします。 動作モードを高速 STP に設定します。 VLAN 1 0 0、2 0 0 および 1 0 0 0 をシングルスパ ニングツリー対象にします。 認証用ポート 0/1~0/20 に対して、スパニングツリー の PortFast 機能を適用し、スパニングツリー対象外に します。			
物理ポートの設定				
Image: Second	認証用ポート 0/1~0/10 に、VLAN100。0/11~0/20 に、 VLAN200 を設定します。			
 上位スイッチとの通信用 (config)# interface range gigabitethernet 0/25-26 (config-if-range)# switchport mode trunk (config-if-range)# switchport trunk allowed vlan 100 200 1000 	上位スイッチとの通信用ポート 0/25~0/26 に、クライ アント用 VLAN100、200 と管理用 VLAN1000 を設定 します。 ▶ 構築ポイント <u>(1)</u>			
インタフェースの設定				
(config)# interface vlan 1000 (config-if)# ip address 172.16.0.12 255.255.255.0	管理用 VLAN1000 にインタフェース IP アドレスを設 定します。			

RADIUS サーバの設定	
(config)# radius-server host 10.51.0.1 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定しま す。本ガイドではキーを「alaxala」としています。
(config)# radius-server dead-interval O	RADIUS サーバの dead interval を 0 に設定します。
スタティックルートの設定	
(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.254	WindowsServer 2008 と通信を行うためデフォルトル ートを設定します。 ▶ 構築ポイント<u>(4)</u>

(2) アクセスリストの設定

AX1240S の設定				
認証専用 IPv4 アクセスリストの設定				
(config)# ip access-list extended JoinDomain	認証専用 IPv4 アクセスリスト「JoinDomain」を作成 します。			
(config-ext-nacl)# 10 permit ip 192.168.100.0 0.0.0.255 host 10.51.0.1	 ・ VLAN100 から Windows Server 2008「10.51.0.1」 への通信を許可します。 、 VLAN100 から修復サーバ「10.52.0.1」 			
(config-ext-nacl)# 20 permit ip 192.168.100.0 0.0.0.255 host 10.52.0.1	・VLAN100 から修復り二八(10.52.0.1)への通信を 許可します。 ・VLAN200 から Windows Server 2008「10.51.0.1」			
(config-ext-nacl)# 30 permit ip 192.168.200.0 0.0.0.255 host 10.51.0.1	への通信を許可します。 ・VLAN200 から修復サーバ「10.52.0.1」への通信を			
(config-ext-nacl)# 40 permit ip 192.168.200.0 0.0.0.255 host 10.52.0.1	許可します。 ・DHCP サーバ通信を許可します。 ・DHCP クライアント通信を許可します。			
(config-ext-nacl)# 50 permit udp any any eq bootps (config-ext-nacl)# 60 permit udp any any eq bootpc	 構築ポイント(2) 認証用ポート 0/1~0/20 に対して、認証専用 IPv4 アクセスリストを適用します。 構築ポイント(5) 			
(config)# interface range fastethernet 0/1-20 (config-if-range)# authentication ip access-group JoinDomain				
VLAN200 用アクセスリストの設定				
<pre>(config)# ip access-list extended VLAN200 (config-ext-nacl)# deny ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 (config-ext-nacl)# deny ip 192.168.200.0 0.0.0.255 host 10.50.0.2 (config-ext-nacl)# permit ip any any</pre>	アクセスリスト「VLAN200」を作成します。 ・VLAN200 から VALN100 への通信を拒否します。 ・VLAN200 から業務サーバ2「10.50.0.2」への通信 を拒否します。 ・すべての通信を許可します。			
(config)# interface vlan 200 (config-if)# ip access-group VLAN200 in	VLAN200 にアクセスリストを適用します。 ▶ 構築ポイント(5)			

(3) IEEE802.1X 認証の設定

AX1240S の設定			
RADIUS の設定			
(config)# aaa authentication dot1x default group radius	RADIUS サーバで IEEE802.1X 認証を行うことを設定 します。		
IEEE802.1X 認証の設定			
<pre>(config)# interface range fastethernet 0/1-20 (config-if-range)# dot1x port-control auto (config-if-range)# dot1x multiple-authentication (config-if-range)# dot1x reauthentication (config-if-range)# dot1x timeout reauth-period 3600</pre>	ポート 0/1~0/20 に対して、IEEE802.1X 認証を有効 にします。 認証サブモードを端末認証モードにします。 サプリカントの再認証を有効にし、その周期を 3600 秒に設定します。		
(config-if-range)# dot1x timeout quiet-period 5	 非認証状態保持時間を5秒に設定します。 ▶ 構築ポイント(7)		
(config-if-range)# dot1x supplicant-detection disable	端 末 検 出 モ ー ド を disable に し て 、 EAP-Request/Identityの送信を抑止します。 ▶ <mark>構築ポイント<u>(6)</u></mark>		
(config-if-range)# authentication ip access-group JoinDomain	 認証用ポート 0/1~0/10 に認証専用アクセスリスト 「JoinDomain」を適用します。		
(config-if-range)# authentication arp-relay	認証前の ARP リレーを設定します。 ▶ 構築ポイント<u>(2)</u>		
(config)# dot1x system-auth-control	 IEEE802.1X 認証を有効にします。		
(config)# dot1x logging enable	 IEEE802.1X 認証ログを syslog へ通知します。		
syslog の設定			
(config)# logging host 10.51.0.1	syslog サーバの IP アドレスを設定します。 (logging event-kind evt が必要ではあるが、デフォル トで有効なため省略可)		

4.4.2 AX2400S のコンフィグレーション

AX2400S シリーズの設定例を示します。

(1) 基本設定

AX2400S の設定	
ポート VLAN の設定	
<pre>(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 100 (config-vlan)# state active (config)# vlan 200 (config-vlan)# state active (config)# vlan 1000 (config-vlan)# state active</pre>	VLAN1 は使用しないため、無効にします。 クライアント用 VLAN として VLAN100、200 管理用 VLAN として VLAN1000 を作成します。
スパニングツリーの設定	
<pre>(config) # spanning-tree single (config) # spanning-tree single mode rapid-stp (config) # spanning-tree mode pvst (config) # no spanning-tree vlan 100,200,1000 (config) # interface range fastethernet 0/1-20 (config-if-range) # spanning-tree portfast</pre>	シングルスパニングツリーを有効にします。 動作モードを高速 STP に設定します。 VLAN 1 0 0、2 0 0 および 1 0 0 0 をシングルスパ ニングツリー対象にします。 認証用ポート 0/1~0/20 に対して、スパニングツリー の PortFast 機能を適用し、スパニングツリー対象外に します。

AX2400S の設定	
物理ポートの設定	
●認証用 (config)# interface range gigabitethernet 0/1-10 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 100 (config)# interface range fastethernet 0/11-20 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 200 ●上位スイッチとの通信用 (config-if-range)# switchport mode trunk (config-if-range)# switchport mode trunk	認証用ポート 0/1~0/10 に、VLAN100 を、0/11~0/20 に、VLAN200 を設定します。 上位スイッチとの通信用ポート 0/47~0/48 に、クライ アント用 VLAN100、200 と管理用 VLAN1000 を設定 します。
	▶ 構築ボイント <u>(1)</u>
インタノエースの設定 (config)# interface vlan 100 (config-if)# ip address 192.168.100.11 255.255.255.0 (config)# interface vlan 200 (config-if)# ip address 192.168.200.11 255.255.255.0 (config)# interface vlan 1000 (config-if)# ip address 172.16.0.11 255.255.255.0	クライアント用 VLAN100、200 と管理用 VLAN1000 にインタフェース IP アドレスを設定します。
RADIUS サーバの設定	
(config)# radius-server host 10.51.0.1 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定しま す。本ガイドではキーを「alaxala」としています。
スタティックルートの設定	
(config)# ip default-gateway 172.16.0.254	WindowsServer 2008 と通信を行うためデフォルトル ートを設定します。 ▶ <mark>構築ポイント<u>(4)</u></mark>

(2) アクセスリストの設定

AX2400S の設定	
認証専用 IPv4 アクセスリストの設定	
(config)# ip access-list extended JoinDomain	認証専用 IPv4 アクセスリスト「JoinDomain」を作成 します。
(config-ext-nacl)#permit ip 192.168.100.00.0.0.255 host 10.51.0.1	・VLAN100 から Windows Server 2008「10.51.0.1」 への通信を許可します。
(config-ext-nacl)#permit ip 192.168.100.00.0.0.255 host 10.52.0.1	・VLAN100 から修復サーバ「10.52.0.1」への通信を 許可します。
(config-ext-nacl)#permit ip 192.168.200.00.0.0.255 host 10.51.0.1	・VLAN200 から Windows Server 2008「10.51.0.1」 への通信を許可します。
(config-ext-nacl)#permit ip 192.168.200.00.0.0.255 host 10.52.0.1	・VLAN200 から修復サーバ「10.52.0.1」への通信を 許可します。
(config-ext-nacl)# permit udp any any eq bootps (config-ext-nacl)# permit udp any any eq bootpc	・DHCP サーバ通信を許可します。 ・DHCP クライアント通信を許可します。 ▶ 構築ポイント<u>(2)</u>
(config)# interface range fastethernet 0/1-20 (config-if-range)# authentication ip access-group JoinDomain	認証用ポート 0/1~0/20 に対して、認証専用 IPv4 アク セスリストを適用します。 ▶ 構築ポイント<u>(5)</u>
VLAN200 用アクセスリストの設定	
<pre>(config)# ip access-list extended VLAN200 (config-ext-nacl)# deny ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255 (config-ext-nacl)# deny ip 192.168.200.0 0.0.0.255 host 10.50.0.2 (config-ext-nacl)# deny vrrp any host 224.0.0.18 (config-ext-nacl)# permit ip any any</pre>	 アクセスリスト「VLAN200」を作成します。 ・VLAN200 から VALN100 への通信を拒否します。 ・VLAN200 から業務サーバ2「10.50.0.2」への通信を拒否します。 ・「224.0.0.18」宛の VRRP 通信を拒否します。 ・すべての通信を許可します。
(config)# interface vlan 200 (config-if)# ip access-group VLAN200 in	VLAN200 にアクセスリストを適用します。 ▶ 構築ポイント(5)

VRRP フィルタリング用アクセスリストの設定	
(config)# ip access-list extended VRRPstop (config-ext-nacl)# deny vrrp any host 224.0.0.18 (config-ext-nacl)# permit ip any any	アクセスリスト「VRRPstop」を作成します。 ・「224.0.0.18」宛の VRRP 通信を拒否します。 ・すべての通信を許可します。
<pre>(config)# interface vlan 100 (config-if)# ip access-group "VRRPstop" in (config)# interface vlan 1000 (config-if)# ip access-group "VRRPstop" in</pre>	VLAN100、1000 にアクセスリストを適用します。

(3) IEEE802.1X 認証の設定

AX2400S の設定	
RADIUS の設定	
(config)# aaa authentication dot1x default group radius	RADIUS サーバで IEEE802.1X 認証を行うことを 設定します。
IEEE802.1X 認証の設定	
<pre>(config)# interface range gigabitethernet 0/1-20 (config-if-range)# dot1x port-control auto (config-if-range)# dot1x multiple-authentication (config-if-range)# dot1x reauthentication (config-if-range)# dot1x timeout reauth-period 3600</pre>	ポート 0/1~0/20 に対して、IEEE802.1X 認証を有 効にします。 認証サブモードを端末認証モードにします。 サプリカントの再認証を有効にし、その周期を 3600 秒に設定します。
(config-if-range)# dot1x timeout quiet-period 5	非認証状態保持時間を5秒に設定します。 ▶ <mark>構築ポイント<u>(7)</u></mark>
(config-if-range)# dot1x supplicant-detection disable	端 末 検 出 モ ー ド を disable に し て 、 EAP-Request/Identity の送信を抑止します。
(config-if-range)# authentication ip access-group JoinDomain	認証用ポート 0/1~0/20 に認証専用アクセスリス
(config-if-range)# authentication arp-relay	ト「JoinDomain」を適用します。 認証前の ARP リレーを設定します。
(config)# dot1x system-auth-control (config)# dot1x logging enable	ア 構築ホイント <u>(2)</u> IEEE802.1X 認証を有効にします。 IEEE802.1X 認証ログを syslog へ通知します。
syslog の設定	
(config)# logging host 10.51.0.1 (config)# logging event-kind err, evt, aut	syslog サーバの IP アドレスを設定します。 syslog 出力条件に認証ログ aut を追加します。

4.4.3 AX3600S のコンフィグレーション

AX3600S の設定例を示します。

(1) 共通の設定

AX3600S の設定	
ポート VLAN の設定	
<pre>(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 100 (config-vlan)# name userVLAN100 (config)# vlan 200 (config-vlan)# name userVLAN200 (config)# vlan 1000 (config-vlan)# name ManageVLAN</pre>	VLAN1 は使用しないため、無効にします。 クライアント用 VLAN として、VLAN100、200 管 理用 VLAN として VLAN1000 を作成します。

AX3600S の設定	
スパニングツリーの設定	
<pre>(config)# spanning-tree single (config)# spanning-tree single mode rapid-stp (config)# no spanning-tree vlan 100, 200, 1000</pre>	シングルスパニングツリーを有効にします。 動作モードを高速 STP に設定します。 VLAN 1 0 0 、2 0 0 および 1 0 0 0 をシングルス パニングツリー対象にします。
(config)# spanning-tree single priority 4096	ブリッジ優先度を設定します。
物理ポートの設定	
<pre>(config)# interface range gigabitethernet 0/1 (config-if)#media-type rj45 (config-if)#switchport mode trunk (config-if)# switchport trunk allowed vlan 100, 200, 1000 リンクアグリゲーションの設定 (config)# interface port-channel 1 (config-if)#switchport mode trunk (config-if)# switchport trunk allowed vlan 100, 200, 1000 (config)#interface range gigabitethernet 0/3-4 (config-if-range)#channel-group 1 mode on</pre>	 下位スイッチとの通信用ポート 0/1 をトランクポートとして設定します。 メディアタイプを設定します。 VLAN100、200 および 1000 を設定します。 ポートチャネルインタフェース1をトランクポートとして作成します。 VLAN100、200 および 1000 を追加します。 ポート 0/3~0/4 を、スタティックモードのチャネルグループ1に設定します。 ▶ 構築ポイント(9)
インタフェースの設定	
<pre>(config)# interface vlan 100 (config-if)# ip address 192.168.100.1 255.255.255.0 (config)# interface vlan 200 (config-if)# ip address 192.168.200.1 255.255.255.0 (config)# interface vlan 1000 (config-if)# ip address 172.16.0.1 255.255.255.0</pre>	VLAN5、100、200 および 1000 のインタフェース IP アドレスをそれぞれ設定します。

(2) VRRP の設定

AX3600S の設定	
VRRP の設定	
<pre>(config) # interface vlan 100 (config-if) # vrrp 100 ip 192.168.100.254 (config-if) # vrrp 100 priority 200 (config-if) # no vrrp 100 preempt (config-if) # vrrp 100 accept</pre>	VLAN100、200 および 1000 に対して、以下の設定を 行います。 ・仮想ルータの IP アドレスを設定します。 ・仮想ルータの優先度を設定します。 ・自動切り戻しを抑止します。
<pre>(config)# interface vian 200 (config-if)# vrrp 200 ip 192.168.200.254 (config-if)# vrrp 200 priority 200 (config-if)# no vrrp 200 preempt (config-if)# vrrp 200 accept</pre>	・アクセプトモードを有効にします。 ▶ <mark>構築ポイント<u>(10)</u></mark>
<pre>(config)# interface vlan 1000 (config-if)# vrrp 1 ip 172.16.0.254 (config-if)# vrrp 1 priority 200 (config-if)# no vrrp 1 preempt (config-if)# vrrp 1 accept</pre>	

(3) DHCP リレーの設定

AX3600S の設定	
DHCP リレーの設定	
(config)# interface vlan 100 (config-if)# ip helper-address 10.51.0.1	VLAN100 および 200 に対して、DHCP リレーエージ ェントによる転送先アドレスを設定します。
(config)# interface vlan 200 (config-if)# ip helper-address 10.51.0.1	

(4) OSPF の設定

AX3600S の設定	
ポート VLAN の設定	
<pre>(config)# vlan 5 (config-vlan)# name OSPF (config)# vlan 15 (config-vlan)# name OSPF</pre>	OSPF 通信用に、ポート VLAN5 および 15 を作成します。
物理ポートの設定	
<pre>(config)# interface gigabitethernet 0/24 (config-if)# switchport mode access (config-if)# switchport access vlan 15 (config-if)# spanning-tree portfast</pre>	ポート 0/24 をアクセスポートとして設定します。 アクセスポートに VLAN15 を設定します。 スパニングツリーの PortFast 機能を適用し、スパニン グツリー対象外とします。
リンクアグリゲーションの設定	
<pre>(config)# interface port-channel 1 (config-if)# switchport trunk allowed vlan add 5</pre>	ポートチャネルインタフェース 1 で VLAN5 を追加し ます。
インタフェースの設定	
(config)# interface vlan 5 (config-if)# ip address 10.5.0.1 255.255.255.0 (config)# interface vlan 15 (config-if)# ip address 10.15.0.1 255.255.255.0	VLAN5 および 15 に、インタフェース IP アドレスを設 定します。
OSPF の設定	
<pre>(config)# router ospf 1 (config-router)# router-id 10.5.0.1 (config-router)# maximum-paths 4 (config-router)# network 10.5.0.0 0.0.0.255 area 0 (config-router)# network 10.15.0.0 0.0.0.255 area 0 (config-router)# redistribute connected</pre>	OSPF を起動します。 ルータ ID を設定します。 OSPF が動作するネットワークを設定します。 connected 経路を再配送します。

4.4.4 AX2500S のコンフィグレーション

AX2500SシリーズのコンフィグレーションはAX1200Sシリーズに比べて、インタフェース種別以外の認 証関連のコンフィグレーションコマンドは基本的に共通です。

ただし、認証関連では、次に示す機能追加とコンフィグレーションの追加があります。機能としては、 リンクアグリゲーションポートの認証機能が追加され、コンフィグレーションとしては、認証ログを syslog採取する場合にlogging event-kind autを追加設定する必要があります。

付録 A.コンフィグレーションに AX1240S を AX2530S に置き換えた場合の完成コンフィグレーショ ンファイルを添付しましたので参考にしてください。

4.5 Windows Server 2008 の設定

固定 VLAN 構成における Windows Server 2008 の設定は、動的 VLAN 構成(<u>3.5</u>章)とほぼ同様です。 ここでは、変更する部分のみ示します。

4.5.1 ネットワークポリシーの設定

正常性ポリシーに合致(検疫 OK)した場合と違反(検疫 NG)した場合のポリシーを作成します。 各ポリシーを作成する手順を以下に示します。

- (1) 正常性ポリシーに合致した場合のポリシー作成
- ネットワークポリシーサーバー画面にて、 左画面の中の「ポリシー」を展開し「ネ ットワークポリシー」を右クリックして 「新規」を選択すると、ウィザードが開 始される。
- 第しいネットワークポリシー画面にて、 ポリシー名(本ガイドでは「検疫 OK」) を入力して「次へ」をクリックする。



図 4.5-1 正常性ポリシーに合致した場合のポリシー作成①

条件の追加(ユーザーグループ)
 新しいネットワークポリシー画面にて
 「追加」をクリックする。
 条件の選択画面にて「ユーザーグループ」
 を選択し「追加」をクリックする。



図 4.5-2 正常性ポリシーに合致した場合のポリシー作成②

④ ユーザーグループ画面にて「グループの 追加」をクリックする。



図 4.5-3 正常性ポリシーに合致した場合のポリシー作成③

⑤ グループの選択画面にて、場所の指定が該当ドメインである事を確認し、3.5.3にて作成したグループ名(本ガイドでは「Sales」)を入力する。「OK」をクリックして画面を閉じる。

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(E):	
example.co.jp	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</u>)(E):	
Sales	名前の確認(<u>C</u>)

図 4.5-4 正常性ポリシーに合致した場合のポリシー作成④

 ⑥ 条件の追加(正常性ポリシー)
 新しいネットワークポリシー画面にて
 「追加」をクリックする。
 条件の選択画面にて「正常性ポリシー」
 を選択し「追加」をクリックする。
 正常性ポリシー画面にて、3.5.7 で作成した検疫合格時のポリシー(本ガイドでは 「OK」)を選択し、「OK」をクリックする。

新しいネットワー	ク ポリシー
	条件の指定 接続要求につい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。
条件の選択	X
条件を選択し、	[j@bn] をクリックします。
D 0月 日の種 す。	★ 類の条件は、NAP 正常性ステートメント (SoH) などの指定した機構で識別できるクライアントだけにポリシーを制限しま
NS-Se MS-サ を取得	***12 グラス - ビス クラスの急作は、接続するコンピュータが、選択したプロファイル名に一致する DHCP スコープから IP アドレス リース している必要があることを指定します。
₩ 歪驚惶	1 70.9 ~ ポリシーの条件は、正常性ポリシーで指定された正常性条件に適合するクライアントだけにポリシーを適用します。
NAP あ NAP か ピュータ	はCコンピュータ の条件は、接続するコンピュータが NAP に参加できるかどうかを指定します。この機能は、クライアント コン が NPS に正常性ステートメントを送信するかどうかによって決まります。
おんし-	テ ク・グランテム テイング システムの条件は、クライアント コンピューダ構成がこのポリシーに一致するために必要なオペレーティング システ 駅、およびアーキテクチャを指定します。
	正市社ホリシー レ
	適用する正常性ポリシーを選択します。新しい正常性ポリシーを作成するには、 「新規」をクリックします。
	正常性ポリシー(H): OK 新規(W)
	OK キャンセル

図 4.5-5 正常性ポリシーに合致した場合のポリシー作成⑤

アクセス許可の指定
 「次へ」をクリックして進む。



⑧ 認証方法の構成

「次へ」をクリックして進む。

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、のかシーの条件を読むすために必要な認証方法を、1 つとし指定して代だい。EAP 認証には、EAA 描述者能容認な多数が必須す、NAP を使用する 8021X または VPN 実履関する場合は、接続要求ポロシーと[編 症』を経営する必要がめけます。接続要求ポロシーは、ネットワーク ポリシーの認証経営よりも優先されます。	Ø ∎ĕn
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(P): 上へ移動(U) 下へ移動(D)	
セキュリティレベルの低い認証方法:	
前へ(P) 法へ(N) 売了(F) 考せンセル	
図 4.5-7 正常性ポリシーに合致した場合のポリシー作成	Ø

⑨ 制約の構成

「次へ」をクリックして進む。



図 4.5-8 正常性ポリシーに合致した場合のポリシー作成⑧

① 設定の構成(属性追加)
 「次へ」をクリックして進む。
 固定 VLAN モードを使用する場合、属性を追加する必要はありません。また、
 「Framed-Protocol」と「Service-Type」
 は削除しても良いです。

新しいネットワーク ポリシー	X
設定の構成 ポリシーのすべてのネッ	・ワーク ポリシー条件および卸払が一致した場合、NPS は接続要求に対して設定を適用します。
このネットワークボリシーの設定を構成し 条件と制いが接続要求に一致してアクト 読定(S):	ます。 とスガトすされる場合、この設定が適用されます。
RADES Bitt 2 ペンダ回称 2 ペンダ回称 2 ペンダ回称 3 NAP 送明 2 ペンダ回称 3 NAP 送明 3 マルキソンウムシアレマン 3 マルキソンウムシアレボル(留 (GAP) 4 ローク・パクタ 4 ローク・パクタ 4 ローク・パクタ 4 昭令化 2 アト・パクタ	2010時代を PADUE クライアントに当けすたいは、構築 PADUE 発展を支援化し、編集) クリックします、加速を構成していて、解発は PADUE クリーアントできる 活動性については、PADUE クライアントのドキュスントを参照していただい。 滞性 7 滞性 7 「Framed Protocol PPP Service-Type Framed 2010(0)_ Nutlic(C)_ AUEN(70)
	_ 前へ(P) _ 次へ(N) 元子(F) _ キャンセル

図 4.5-9 正常性ポリシーに合致した場合のポリシー作成⑨

① 「完了」をクリックして画面を閉じる。

「「「」「」「」「」「」「」「」「」「」「」」「」「」」「」」「」」「」」「」	ークポリシーの完了
かのネットワーク ポリシーが正常に作	11成されました:
會疫OK	
 111-3	
	ч
	N EC
コーザー グループ EXAMPLE¥SA	9LEO
ユーザー グループ EXAMPLEXS: 正常性ポリシー OK	165
ユーザー グループ EXAMPLEWS 正常性ポリシー OK	115
ユーザー グループ EXAMPLEVS。 正常性ポリシー OK 切シー設定: タノチ	165
ユーザー グループ EXAMPLEVS。 正常性ポリシー OK 切シー設定: 条件 2月215年4	
ユーザー グループ EXAMPLENS 正常性ポリシー OK 切シー設定 : 条件 認証方法 マットロットコー	」値 MS-CHAP v1 または MS-CHAP v1 (パスワードの実現委が切れた後、ユーザーがパス… つわわつ Akk ard ま。
ユーザー グループ EXAMPLEWS 正常性ポリシー OK 切り - 設定: 条件 20日方法 アンセスド可 非違案からイア・人の軍所	値 MS-OHAP v1 または MS-OHAP v1 (パスワードの期限が切れた後、ユーザーがパス アックセスを計すする Ture
<u>ユーザー ガループ EXAMPLEVS</u> 正常性ポリシー OK 切りー設定: 条件 認証方法 アシセス許可 非単拠のライアントの更新 NAP	値 MS-OHAP v1または MS-OHAP v1 (パスワードの期間が切れた後、ユーザーがパス アクセス各計可する True 完全なネットワーク アクセス名計可する
<u>ユーザー グループ</u> EXAMPLEVS, 正常性ポリシー OK 数定: 条件 22証方法 アンセンドの更新 NAP 強制 Framed-Protocol	値 MS-CHAP v1 または MS-CHAP v1 (パスワードの期限が切れた後、ユーザーがパス アクセスを許可する True 完全なオットワーク アクセスを許可する PPP

図 4.5-10 正常性ポリシーに合致した場合のポリシー作成⑩

- (2) 正常性ポリシー違反のポリシー作成
- ネットワークポリシーサーバーの画面に て、左画面の中の「ポリシー」を展開し 「ネットワークポリシー」を右クリック して「新規」を選択すると、ウィザード が開始される。
- 新しいネットワークポリシー画面にて、 ポリシー名(本ガイドでは「検疫 NG」) を入力して「次へ」をクリックする。



図 4.5-11 正常性ポリシー違反のポリシー作成①

3 条件の指定

(1)の③~⑥と同様に「ユーザーグル ープ」と「正常性ポリシー」を追加する。 「正常性ポリシー」については、<u>3.5.7</u>で 作成した検疫失敗時のポリシー(本ガイ ドでは「NG」)を選択する。最後に「次 へ」をクリックして進む。

新しいネットワー	クポリシー 🛛
	条件の指定 接続要求につい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。
条件の選択	E Contraction of the second
条件を選択し、	G追加]をクリックします。
ネットワーク アク	セス保護
日本 しの種 す。	類 類の条件は、NAP 正常性ステートメント (SoH) などの指定した機構で識別できるクライアントだけにポリシーを制限しま
NS-Se MS-サ を取得	wize クラス ービス クラスの条件は、接続するコンピュータが、違択したプロファイル名に一致する DHOP スコーブから IP アドレス リース ている必要があることを指定します。
	<mark>ポラー</mark> ポリシーの条件は、正常性ポリシーで指定された正常性条件に適合するクライアントだけにポリシーを適用します。
NAP お NAP 対 ピュータ	応コンピュータ 広コンピュータの条件は、接続するコンピュータが NAP に参加できるかどうかを指定します。この機能は、クライアント コン が NPS に正常性ステートメントを送信するかどうかによって決まります。
	ティングシステム
止常性ポリシー	▲ 「に一致するためと必要なオペレーディング システ
適用する正常 [新規] をクリッ	性ポリシーを選択します。新しい正常性ポリシーを作成するには、 りします。
正常性ポリシー	-(H):
ING	▼ <u></u>
	OK キャンセル 」 次へ(N) 完了(F) キャンセル
	図 4.5-12 正常性ポリシー違反のポリシー作成②

- ④ アクセス許可の指定、認証方法の構成、制約の構成をそれぞれ「次へ」で進める。
- ⑤ 設定の構成(属性追加)
 新しいネットワークポリシー画面にて、
 左画面の中の「標準」を選択し、右画面の「追加」をクリックする。標準 RADIUS
 属性の追加画面にて、下記属性を追加する。
 ・Filter-Id = "JoinDomain"(認証専用)

IPv4 アクセスリスト名)

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 条件と制約が接続要求に一致して 時 定(S)	成します。 Pクセスが許可される場合、さ	この順定が適用されます。
RADILS 属性 ● 標準 マ ペンダ固有 ネットワークアクセス保護	追加爾性を RADIUS をりリックします。属性 な属性については、RA	クライアントに送信するには、標準 RADIUS 居性を提択し、[編集] 装積成しないと、居性は RADIUS クライアントに送信されません。必要 DOUS クライアントのドキュメントを参照してください。
NAP 注制 が最大状態 ルーティングとリモートアクセン ス ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	爾性(T): 名前 Framed-Protocol Service-Type Filter-Id	fē PPP Framed JoinDomain
▲ 暗号化 ☑ IP 設定		扁葉(E)

図 4.5-13 正常性ポリシー違反のポリシー作成③

⑥ NAP 強制(自動修復無し) 新しいネットワークポリシー画面にて、 左画面の中の「NAP 強制」を選択する。 右画面にて「制限付きアクセスを許可す る」をチェックし、「自動修復」のチェッ クを外して「次へ」をクリックする。

新しいネットワーク ポリシー	x
ジェク構成 ポリシーのすべてのネッ	トワーク ボジー条件および制約が一致した場合、NPS は揺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 設定(S):	します。 やスガはす可される場合、この設定が適用されます。
RADILS 周生 ● 標準 マ べ 次間有	○ 時間を限定して完全なネットワークアクセスを許可する(N) 指定された日時をで制限のないネットワークアクセスを許可します。指定された日時を過ぎると、正常性ポリシーが確制ない、準拠していないコンピュータがアクセスできるのは制限 されたネットワーンのみになります。
 ネットワークアクセス保護 NAP 強制 サジェリナ地 	日付(T): 2007/09/14 ・ 時刻(D): 2003/51
	うのみです。 「修復サーバー グループとトラブルシューティングの URL 修復サーバー グループ トラブルシューティングの URL、または両方を構成するには、[構 成]をかりのしてださい。
~ 割り当てフロトコル (BAP) 品 IP フィルタ	
♣ 暗专化 ☑ IP 設定	□ クライアントコンピュータの自動修復を有効にする(U) このポリシーで定義されている正常性の要件を満たしていないコンピュータを自動 的に修復します。 ▼
図 4 5	

- 注意:NPS はデフォルトで自動修復が有効となっていますが、本ガイドでは検疫 VLAN に隔離 された NAP クライアントが手動で修復を行うことを想定しているので無効にしています。 自動修復機能を有効のまま構築する場合は、この手順を省略して下さい。
- ⑦ 「完了」をクリックして画面を閉じる。

新しいネットワ・	ークポリシーの完了
かのえっしりーク おいシーガ正学に作り	ポン約 = 1 た-
	wet to over
LISE NG	
リシー条件:	
条件 值	
1ーザー グループ EXAMPLE¥SAL	ES
上市11王小リント NG	
1121、副台。	
リシー設定:	
リシー設定: 条件 2015年3年	値 MS-CHAP JJ またけ MS-CHAP JJ (パフワードの運転開始行動た後を ユーザーがパフ
リシー設定: 条件 認証方法 PD47344可	値 MS-CHAP v1 または MS-CHAP v1 (パスワードの期限が切れた後、ユーザーがパス アクトウスを注むする。
リシー設定: 条件 23証方法 ウクセスド可 12編約05イアントの更新	値 MS-CHAP v1 または MS-CHAP v1 リペスワードの期間数が切れた後、ユーザーがパス… アクセンを許可する False
リシー設定: 条件 辺証方法: アクセスド可 非準拠(55イアントの更新 NAP 発制)	値 MS-CHAP v1 または MS-CHAP v1 U1スワードの実際数が切れた後、ユーザーがパス… アクセスを計すする False 制限行きネットワーク アクセスを計可
切り 一読定: 条件 認証方法 アクセス4-0T 非単純シライアントの更新 NAP 達却 Frand-Protocol	値 MS-CHAP v1 または MS-CHAP v1 (パスワードの再駆動が切れた後、ユーザーがパス アクセスを計中する False 参調取代きネットワーク アクセスを計す可 PPP
リシー設定: 委件 設計方法 アクセンドロ「 非実地シライアントの更新 NAP 強制 Frand-Protocol Service-Type	値 MS-CHAP v1または MS-CHAP v1 リペスワードの専務政が切れた後、ユーザーがパス… Polse 制限付きネットワーク アクセスを許可 PPP Framed
切り一読定: 条件 認証方法 72位24年7年 #2種20ライアントの更新 #2種20ライアントの更新 Frand-Protocol Service-Type	値 MS-CHAP v1 または MS-CHAP v1 (パスワードの)期間が切れた後、ユーザーがパス アクセスを計すする False 制度付きネットワーク アクセスを計可 PPP Framed
リッー説定: 条件 辺証方法 アクセ21年可 非単地クライアントの更新 NAP 注制 Frand-Protocol Service-Type のナイードを開けるには、にて了 を	値 MS-CHAP v1または MS-CHAP v1 (パスワードの期限が切れた後、ユーザーがパス アクセンを許可する False 部隊民行きネットワーク アクセスを許可 PPP Framed グリックしてください。
リッー設定: 条件 認証方法 アクセスキャゴ 非単処フィアントの更新 ARP 強制 Francd-Protocol Service-Type のウィザードを閉じるには、DFC 7 を	値 MS-CHAP v1 または MS-CHAP v1 (パスワードの再卵数が切れた後、ユーザーがパス アクセスを計可する False 参 JIR(打きネットワーク アクセスを計可 PPP Framed グリックしてください。
リッー説定: 条件 辺証方法 アクセ24年可 非単地クライアントの更新 NAP 注制 Frand-Protocol Service-Type のウィザードを閉じるには、DFT 1を	値 MS-CHAP v1または MS-CHAP v1 (パスワードの期限が切れた後、ユーザーがパス アクセンを許可する False 部隊民だきネットワーク アクセスを許可 PPP Framed グリックしてください。
切り - 読定: 条件 辺証方法 アクセス許可 オギ型(シライワントの更新 NAP 強制 Framed-Protocol Service-Type のウィザードを閉じるには、「完了」を	値 MS-CHAP v1 または MS-CHAP v1 U1スワードの実際数が切れた後、ユーザーがパス アクセスを許可する False 事業取けきネットワーク アクセスを許可 PPP Framed グリックしてください。

図 4.5-15 正常性ポリシー違反のポリシー作成⑤

以上で設定は完了です。

5.動作確認

本章では、検疫ネットワークの認証スイッチ、NPS および NAP クライアントにおける検疫動作の確認 方法について示します。

5.1 AX シリーズの運用コマンド

5.1.1 show dot1x detail

AX シリーズ(認証スイッチ)での IEEE802.1X 認証方式の状態表示コマンドです。 NAP クライアントが認証成功しているかどうかを確認することができます。 また、その所属している VLAN 情報から、検疫成功しているかどうかを確認することができます。 AX1200S の場合は、show mac-address-table コマンドと併用してください。

edge#1# show dot1	x port O	/3 detail					
Date 2010/01/30 14 Port 0/3 (Dynamic) AccessControl : M Status : - Supplicants : T TxTimer : C ReAuthSuccess : SuppDetection : M VLAN(s): 10,30,100	4:00:07 Multiple 1 / 1 / 0 30 1 Auto 0	JST -Auth 64	P L R R R R	PortContro ast EAPOI ReAuthMode ReAuthTim ReAuthFai	ol L er I	: Auto : 0019.b : Enable : 300 : 0	97d. 46c7
Supplicants MAC [VLAN 100] 0019.b97d.46c7	F State Sess Port Autho 113	us ionTime(s) (Dynamic) orized	AuthStat Date/Tim Supplican Authenti 2009/06/	ie Ba ne nts:1 cated Id '22 13:58	ackEn dle :14	dState	ReAuthSuccess 1
edge#1# <mark>show mac-</mark> a	address-	table					
Date 2010/01/30 14 Aging time : 300	4:00:46	JST					
MAC address 0000. 5e00. 010a 0019. b97d. 46c7 0000. 5e00. 011e 0000. 5e00. 0164 0012. e228. f5fe 0012. e238. 2a68 0019. b97d. 46c7 0000. 5e00. 0101 0012. e228. cd62 0012. e228. f5fe 0012. e238. 2a68	VLAN 10 10 100 100 100 1000 1000 1000 1000	Type Dynamic Dynamic Dynamic Dynamic Dynamic Dot1x Dynamic Dynamic Dynamic Dynamic	Port-lis 0/26 0/3 0/26 0/26 0/26 0/26 0/26 0/26 0/26 0/26	t			

図 5.1-1 AX1200Sの状態表示例(動的 VLAN)

edge#1# show dot1x port 0/3 detail
Date 2010/01/30 16:11:40 JST Port 0/3PortControlAutoAccessControlMultiple-Auth StatusPortControl: AutoStatus: SupplicantsLast EAPOL: 0019. b97d. 46c7Supplicants: 1 / 1 / 64 ReAuthModeReAuthMode: EnableTxTimer: 30 ReAuthSuccess: 1 AutoReAuthFail: 0SuppDetection: AutoVLAN (s) : 100: 100: 100
Supplicants MAC F Status AuthState BackEndState ReAuthSuccess [VLAN 100] Port(Static) Supplicants : 1 Supplicants : 1 0019. b97d. 46c7 Authorized Authenticated Idle 101 2010/01/30 16:09:59 Full 7ルアクセス許可







dist#1# <mark>show dot1x v</mark> Date 2010/01/30 14:0 VLAN(Dvnamic)	ylan dynamic detail 02:39 JST			
AccessControl : Mul Status : Supplicants : 1 / TxTimer(s) : ReAuthSuccess : 0 SuppDetection : Aut VLAN(s): 30,100	tiple-Auth / 1 / 256 - / 30	PortCont Last EAF ReAuthMo ReAuthTi ReAuthFa	trol : Auto POL : 0019.b ode : Enable imer(s): 269 ail : 0	97d. 46c7 / 300
Supplicants MAC [VLAN 100] 0019.b97d.46c7 dist#1#	Status AuthS SessionTime(s) Date/ VLAN(Dynamic) Suppli Authorized Authe 33 2010/	State /Time cants : 1 enticated /01/30 14:0	BackEndState Idle 02:07	ReAuthSuccess O



dist#1# show dot1x por Date 2010/01/30 16:06:	r t <mark>0/5 detail</mark> :22 JST			
Fort 0/5AccessControl : MultiStatus :Supplicants : 1 / 1TxTimer(s) :ReAuthSuccess : 3SuppDetection : Auto	iple-Auth / 64 / 30	PortCont Last EAF ReAuthMc ReAuthTi ReAuthFa	rol : Auto POL : 0019.b ode : Enable mer(s): 178 , ail : 0	97d. 46c7 / 300
Supplicants MAC	Status SessionTime(s)	AuthState	BackEndState	ReAuthSuccess
019. b97d. 46c7	Authorized 122	Authenticated 2010/01/30 16:0	Idle)4:19	0
dist#1# 7ルアクセス許可	ſ			
[Supplicant	の MAC 7ト レスの)前に*が表示さ;	れない。]	

図 5.1-5 AX2400S/AX3600S の状態表示例(固定 VLAN(ポート単位))検疫 OK



図 5.1-6 AX2400S/AX3600Sの状態表示例(固定 VLAN(ポート単位))検疫 NG

5.1.2 show dot1x logging

IEEE802.1X 認証の動作ログ表示コマンドです。 NAP クライアントがいつログインしたか、いつ再認証を行ったか等を確認することができます。 また、認証失敗時の原因についても確認することができます。

5.1.3 clear dot1x auth-state

IEEE802.1X 認証状態を初期化するコマンドです。 NAP クライアントを強制的にログアウトさせる場合に使用します。

5.2 NPS の運用ツール

5.2.1 イベントビューアー

NPS による認証、検疫のログを表示します。

認証検疫合否ログ、認証失敗理由、システムの正常性結果、RADIUS リクエストパケットの内容など多 くの情報を確認することができます。

以下に、イベントビューアーの表示、確認方法を示します。

- 「スタート」→「管理ツール」→「イベントビューアー」をクリックする。イベントビューアーの左画面にて「カスタムビュー」→「サーバーの役割」→「ネットワークポリシーとアクセスサービス」を選択して、アクセスログを確認する。
- ② 検疫成功ログ表示画面を以下に示します。
 IEEE802.1X 認証方式の NAP では、検疫結果のログは必ず認証成功ログとペアになります。
 ・イベント ID: 6278 検疫成功
 - ・イベント ID: 6272 認証成功

🛃 イベント ይューアー						_ 🗆 ×
ファイル(F) 操作(A) 表示(V) /	ヘノレプ(H)					
🗢 🔿 🖄 📰 🚺						
🚺 イベント ビューアー (ローカル)	ネットワーク ポリシーとア	クセス サービス イベント数: 578	1			操作
日 📑 カスタム ビュー	マーイベント差折 573					ネットワーク 🔺
Active Directory ド≯	1 1.01 20.010		[), = [-80	🧉 保存され
Active Directory	レベル	<u> 日村と時刻 </u> 2010/01/27 12-25-07	Microsoft Windo	<u>イベント ID タスクのカナ</u> 6179 ウットローク	<u>コリ ▲</u> ポルシュ	→7月J
The phone and t	(14+1)	2010/01/27 13:25:07	Microsoft Windo	6272 ネットワーク	ポリシュー	Y 33774
	前情報	2010/01/27 13:24:22	Microsoft Windo	6278 ネットワーク	ポリシュ	
▼ web サーバー (LS) ▼ えットローク ポルシーと	() 情報	2010/01/27 13:24:22	Microsoft Windo	6272 ネットワーク	ポリシー	🝸 現在の力
マ 管理イベント	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2010/01/27 13:24:10	Microsoft Windo	6278 ネットワーク	ポリシ	□ プロパティ
🕀 🚉 Windows 🛛 グ	1 情報	2010/01/27 13:24:10	Microsoft Windo	6272 ネットワーク	ポリシニ	010 total
💷 🛅 アプリケーションとサービス ログ	(1) 情報	2010/01/27 13:23:26	Microsoft Windo	6276 ネットワーク	ポリシー	· · · · · · · · · · · · · · · · · · ·
📑 サブスクノプション		2010/01/27 13:23:26	Microsoft Windo	6272 ネットワーク	ポリシュ	אַגאַל 🛄 אַ
		2010/01/27 13:20:58	Microsoft Windo	0270 <u> </u>	· 赤小シ	<u> </u>
	🛃イベント プロパティー	イベント 6278, Microsoft Win	dows security auditing.		××	<u> </u>
	全般詳細					このカスタ
						—————————————————————————————————————
	認証の詳細	1910. A		_		301
		Rリシー名: NAP都 ましいこと: IDEEA IDEEA	現受 後\/L 4N 100			🞑 最新の
	マンクロバ 認証プロバ	パリシーム stater: イダー: Windows	g VEHN100			🛛 🛛 🖓 🕹 🕨
	認証サーバ	dcexample.co.jp)	-		(
	認証の種業	₫: PEAP				1/21 027 ▲
	EAP の種類	康: Micro:	soft: セキュリティで保護されたパスワ	~ド(EAP- ↓	T	🔄 🛅 イベント
	IMCOUND ION				<u> </u>	💿 201K
	ログの名前(M):	セキュリティ			. I I I I	B ⊐P- ►
	ソース(S):	Microsoft Windows secur	ity a ログの日付(D): 2010/01	1/27 18:25:07		
	イベント ID(E):	6278	タスクのカテゴリ(Y): ネットワー	-クポリシー サーバー		日 選択した
	ν.<	情報	キーワード(K): 成功の語	in in it is a state of the sta		🧟 最新の
	ユーザー(U):	N/A	コンピューター(R): dc.exam	ple.co.jp		2 ヘルプ →
	オペコード(0):	唐朝				-
	目羊糸肥(香寿局(1):	ፈለጉ/ት በグብላ ዜማ				
	BTOWINTING.					
	⊐ピ−(P)			閉じる(C)		
					-	

図 5.2-1 検疫結果成功のログ

③ 検疫失敗ログ表示画面を以下に示します。

IEEE802.1X 認証方式の NAP では、検疫結果のログは必ず認証成功ログとペアになります。

- ・イベント ID:6276 検疫失敗
- ・イベントID:6272 認証成功



図 5.2-2 検疫結果失敗のログ

④ 認証に失敗した(NPSのネットワークポリシーに一致しなかった)場合、検疫チェックは実施されず認証失敗ログのみ表示されます。

5.3 NAP クライアントの運用ツール

5.3.1 netsh nap client show state

NAP クライアントのステータスを表示するコマンドです。

NAP を実施する検疫方法のステータスや、SHA のバージョン情報、現状のセキュリティ状態を確認することができます。

コマンドプロンプトでコマンドを実行した結果例を以下に示します。

ID 名前 説明 バージョン ベンダ名 登録日 初期NY済み	= 78623 = EAP 検疫強制クライアント = EAP ベースの強制を NAP に提供します。 = 1.0 = Microsoft Corporation = = (すい)
System Health Agent (Sh	4)の状態:
ID 名前	= 78744 = Windows セキュリティ正常性エージェント
説明 したポリシーに、コンビ.	= Windows セキュリティ正常性エージェントは、管理者が定義 ニータが準拠しているかどうかをチェックします。
バージョン	≡01.0
ベンダ名	= Microsoft Corporation
登録日 初期化済み エラーのカテゴリ 修復の状態 修復の割合 修正のメッセージ は、セキュリティ状態の引	= = はい = なし = 成功 = 0 = (3237937214) - Windows セキュリティ正常性エージェント 更新を終了しました。
確認の結果 修復の結果	
0K	*

図 5.3-1 NAP クライアントステータス表示例

5.3.2 ネットワークアクセス状態の確認

NAP クライアントを認証スイッチに接続すると、ネットワークアクセス状態が Windows 画面のタス クバーに自動的に表示されます。

NAP クライアントが検疫に失敗した場合、以下のメッセージが表示されます。



図 5.3-2 検疫失敗時のメッセージ

メッセージをクリックすると、検疫結果を確認することができます。

コンピュータが更新されるまで、ネットワーク アクセスは制限されます。 試行] または [詳細情報] をクリックしてください。	[再
Windows セキュリティ正常性エージェント 失敗 Microsoft Corporation Windows セキュリティ正常性エージェントは、管理者が定義したポリシー に、コンピュータが準拠しているかどうかをチェックします。 バージョン: 1.0、ID 79744	
Windows セキュリティ正常性エージェントが、このコンピュータのセキュリ ティ状態の更新に失敗しました。	
	試行]または[詳細情報]をクリックしてください。 Windows セキュリティ正常性エージェント 失敗 Microsoft Corporation Windows セキュリティ正常性エージェントは、管理者が定義したポリシー (、コンピュータが準拠しているかどうかをチェックします。 パージョン:1.0、ID 79744 Windows セキュリティ正常性エージェントが、このコンピュータのセキュリティ状態の更新に失敗しました。 修復結果・

図 5.3-3 検疫失敗時の画面

ここで、NAP クライアント端末の設定を変更してネットワーク要件に準拠させると、再度検疫が実施 されます。NAP クライアントが検疫に成功した場合、以下のようなメッセージが Windows 画面のタ スクバーに表示されます。



図 5.3-4 検疫成功時のメッセージ

メッセージをクリックすると、検疫結果を確認することができます。

Window	vs セキュリティ正常性エージェント	更新完了100%
Microsof	t Corporation	
Windows	。セキュリティ正常性エージェントは、管	理者が定義したポリシーに、
コンピュ	ータが準拠しているかどうかをチェックし)ます。
バージョ	ン: 1.0、ID 79744	
Windows 了しまし	。セキュリティ正常性エージェントでは、 た。	セキュリティ状態の更新を終

図 5.3-5 検疫成功時の**画**面

6.注意事項

6.1 動的 VLAN 使用時の注意事項

6.1.1 Windows XP の IP アドレス切り替え問題

AX シリーズの MAC VLAN を用いた検疫ネットワークシステムにおいて、Windows XP を NAP クラ イアントとした場合、IP アドレスが切り替わらない問題が発生します。なお、Windows Vista では発生 しません。



図 6.1-1 IP アドレス切り替え問題の起こるネットワーク構成

図 6.1-1において、検疫済みの Windows XP が、セキュリティポリシー違反などにより所属する VLAN が切り替わると、Windows XP はまずデフォルトゲートウェイ宛てに PING (ICMP-Echo Request)を送信して到達可能性を確認します。デフォルトゲートウェイからの ICMP-Echo Reply は、AX (認証ス イッチ)の MAC VLAN の仕様により Windows XP へと転送されるため、Windows XP は DHCP パケットを送信せず、従って IP アドレスの切り替わりが発生しません。本問題の詳細については、6.1.2章を参照して下さい。

ここでは、本問題を回避する方法を3種類示します。以下何れかの回避方法を使用して下さい。

(1) デフォルトゲートウェイ(L3スイッチ)にて VRRP を構成する。

VRRP を設定すると VLAN 毎に異なった仮想 MAC アドレスが使用されるため、デフォルトゲート ウェイは Windows XP からの ICMP-Echo Request に応答しません。但し、この方法はデフォルトゲ ートウェイ冗長化構成に依存した回避方法です。

本ガイドでは、VRRP を使用した構成を用いているため、IP アドレス切り替わりの問題は起こり ません。VRRPの設定方法については<u>3</u>章を参照して下さい。

(2) デフォルトゲートウェイ(L3スイッチ)にて VLAN 毎に使用する MAC アドレスを変更する。

AX シリーズでは、コンフィグレーションコマンド(vlan-mac-prefix)を用いて VLAN 毎に異なる MAC アドレスを設定することができます。これにより、検疫 VLAN と認証後 VLAN で異なる MAC アドレスが使用されるため、デフォルトゲートウェイは Windows XP からの ICMP-Echo Request に 応答することはありません。

コンフィグレーションの参考例を次に示します。

表 6-1 VLAN 毎に使用する MAC アドレス設定例

AX3600S
vlan-mac-prefix 0012.e208.6277 ffff.fff.0000
vlan 10
vlan-mac
vlan 30
vlan-mac
vlan 100
vlan-mac

(3) 認証スイッチにフィルタを設定する。

認証スイッチにアクセスリストを適用して、VLAN 変更後に送信される Windows XP からのデフォ ルトゲートウェイ宛 ICMP-Echo Request をフィルタリングします。コンフィグレーションの参考例 とその解説を以下に示します。

表 6-2 ICMP フィルタ設定例

interface vlan 30
ip access-group "XP-ICMP30" in
interface when 100
in access-group "XP-ICMP100" in
ip access-list extended "XP-ICMP30"
seq 10 deny protocol icmp src 192.168.10.0 0.0.0.255 dst 192.168.10.254 0.0.0.0
seq 20 deny protocol icmp src 192.168.100.0 0.0.0.255 dst 192.168.100.254 0.0.0.0
seq 30 permit protocol ip src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 (% 1)
! in access-list extended "XP-ICMP100"
seg 10 deny protocol jemp src 192,168,10,0,0,0,255 dst 192,168,10,254,0,0,0,0
seq 20 deny protocol icmp src 192.168.30.0 0.0.255 dst 192.168.30.254 0.0.0
seq 30 permit protocol ip src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255
AX2400S
interface vlan 30
ip access-group XP-ICMP30 in
ip access-group XP-ICMP30 in
ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in
ip access-group XP-ICMP30 in ! interface vlan 100 ip access-group XP-ICMP100 in
ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in i ip access-list extended XP-ICMP30
<pre>incorrace vian co ip access-group XP-ICMP30 in interface vian 100 ip access-group XP-ICMP100 in ! ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254</pre>
<pre>ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in i ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.100.0 0.0.0.255 host 192.168.100.254</pre>
ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.100.0 0.0.0.255 host 192.168.100.254 30 permit ip any any (¥1)
<pre>ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.100.0 0.0.0.255 host 192.168.100.254 30 permit ip any any (%1) ip access-list extended XP-ICMP100</pre>
<pre>ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.100.0 0.0.0.255 host 192.168.100.254 30 permit ip any any (%1) ip access-list extended XP-ICMP100 10 deny icmp 192.168.10 0.0.0.255 host 192.168.10.254</pre>
<pre>ip access-group XP-ICMP30 in interface vlan 100 ip access-group XP-ICMP100 in ip access-list extended XP-ICMP30 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.100.0 0.0.0.255 host 192.168.100.254 30 permit ip any any (※1) ip access-list extended XP-ICMP100 10 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254 20 deny icmp 192.168.10.0 0.0.0.255 host 192.168.10.254</pre>

表 6-3 本参考例の各 VLAN について

VLAN-ID	VLAN	ネットワークアドレス	デフォルトゲートウェイ
10	認証前 VLAN	192.168.10.0/24	192.168.10.254
30	検疫 VLAN	192.168.30.0/24	192.168.30.254
100	認証後 VLAN	192.168.100.0/24	192.168.100.254

上記のアクセスリストでは認証前 VLAN と認証後 VLAN からそれぞれの VLAN のデフォルトゲー トウェイ「192.168.10.254」と「192.168.100.254」への PING を拒否するアクセスリスト「XP-ICMP30」 を作成し、検疫 VLAN30 に適用しています。同様に、認証前 VLAN と検疫 VLAN からそれぞれのデ フォルトゲートウェイ「192.168.10.254」と「192.168.30.254」への PING を拒否するアクセスリス ト「XP-ICMP100」を作成し、認証後 VLAN100 に適用しています。

注意…上記の参考例では本問題を回避するためのフィルタリング定義となっています、既に VLAN に対しアクセスリストが定義されている場合は既存のアクセスリストに追加して下さい。なお本参考 例では検疫 VLAN (VLAN30) にも全ての通信を許可する定義(※1)が含まれています、適応する 環境に応じて検疫 VLAN の通信可能範囲を正しく設定して下さい。

6.1.2 IP アドレス切り替え問題の詳細解説

Windows OS の端末は、IEEE802.1X 認証シーケンス完了後デフォルトゲートウェイへの通信確認を 行い、応答が無ければ DHCP パケットを送信して IP アドレスの再取得を行います。

Windows XP と Windows Vista ではデフォルトゲートウェイへの通信確認方法が異なるため、動作に 差分が生じています。それぞれの動作シーケンスについて次に示します。

(1) Windows XP の動作シーケンス

Windows XP は、IEEE802.1X 認証後 VLAN が切り替わると、ICMP-Echo Request をデフォルト ゲートウェイに送信して到達可能性を確認します。デフォルトゲートウェイは、既に Windows XP 端末の所属する VLAN が切り替わった後であっても、ICMP-Echo Reply を送信します。MAC VLAN を使用している認証スイッチ (AX2400S / AX1200S) では、その ICMP-Echo Reply を転送するため、 Windows XP はデフォルトゲートウェイに到達可能であると判断して DHCP パケットを送信しませ ん。

Windows XPの IP アドレス切り替えシーケンス図を以下に示します。



図 6.1-2 Windows XPの IP アドレス切り替えのシーケンス

(2) Windows 7 と Windows Vista の動作シーケンス

Windows 7 と Windows Vista は、IEEE802.1X 認証後 ARP-Request をデフォルトゲートウェイに 送信して到達可能性を確認します。ここで、認証スイッチでは VLAN が切り替わっているため、デ フォルトゲートウェイ (AX3600S) は ARP パケットを廃棄し応答しません。Windows 7 と Windows Vista はデフォルトゲートウェイに到達できないと判断して DHCP パケットを送信します。 Windows 7 と Windows Vista の IP アドレス切り替えシーケンス図を以下に示します。



図 6.1-3 Windows 7 と Windows Vista の IP アドレス切り替えのシーケンス

6.2 VLAN モード共通(動的 VLAN、固定 VLAN)の注意事項

6.2.1 非認証状態保持時間の設定について

IEEE802.1X 認証機能を有効に設定した Windows 端末は、起動時に「コンピュータ認証」を行い、 Windows ログオン時に「ユーザー認証」を行います。本ガイドではコンピュータの IEEE802.1X 認証用 のネットワークポリシーを設定していないためコンピュータ認証は失敗します。その後、ユーザー認証 が行われます。(図 6.2-1参照)

コンピュータ認証が失敗すると、AXスイッチの該当VLANインタフェースは非認証状態となります。 この状態は非認証状態保持時間(デフォルト値は 60 秒)続き、その間は認証処理を行いません。非認 証状態保持時間内に端末がユーザー認証を試みて失敗すると、その後認証処理を停止してしまう場合が あります。そのため、AX スイッチのコンフィグレーションコマンドを用いて非認証状態保持時間 (quiet-period)を短く設定して下さい。

一般的に、コンピュータ認証失敗からユーザ認証を開始するまで数秒~数十秒程度となるため、本ガ イドでは非認証状態保持時間を5秒に設定しています。(3.4章を参照)



図 6.2-1 Windows の IEEE802.1X 認証シーケンス

7. トラブルシューティング

本章では、検疫が正常に動作しないトラブルが発生した場合の対処方法を示します。

7.1 Windows ドメインに参加できない

3.6.2 章のNAPクライアントのWindowsドメイン参加ができない場合、以下を確認して下さい。

(1) ドメインコントローラと通信できていない。

クライアント端末からWindows Server 2008へのPING確認および名前解決ができていることを確認して下さい。名前解決に失敗する場合はWindows Server 2008にてDNSサーバのサービスが動作していることを確認してください。

(2) ユーザID、パスワードが間違っている。

3.5.3 章のActive Directoryにて作成したユーザIDおよびパスワードを入力して下さい。

(3) ネットワーク接続のプロパティに「Microsoft ネットワーク用クライアント」がない。
 接続のプロパティよりインストールし、チェックをつけ有効にして下さい。

7.2 検疫に成功しない

NAP クライアントが検疫に成功しない場合、以下を確認して下さい。

(1) NAP クライアントのセキュリティセンターが有効になっていない。

5.3.1の「netsh nap client show state」コマンドにて確認して下さい。セキュリティセンターが有効になっていない場合、8.1.1.(2)または8.1.2(2)の手順で有効にして下さい。

(2) NAP クライアントがセキュリティポリシーに準拠していない。

NAP クライアントが3.5.7章で設定したポリシーに準拠しているかどうか確認して下さい。

(3) システム正常性ツールの設定が間違っている。
 「3.5.6 システム正常性検証ツール(SHV)の設定」のシステム正常性検証ツール(SHV)の設定
 を確認して下さい。

7.3 IEEE802.1X 認証動作を行わない

ネットワーク障害や過負荷等により IEEE802.1X 認証が失敗してしまい、その後認証動作が停止して しまう事があります。(ネットワークアクセス状態の確認方法は<u>5.3.2</u>参照)

この場合、以下のいずれかの操作を実施して再認証を試みて下さい。

- (1) 通信インタフェースのリンクダウン・アップ
- (2) ユーザのログオフ・ログオン
- (3) 端末の再起動

8. 設定ノウハウ集

8.1 手動による NAP クライアント設定

本ガイドにおいて Windows ドメイン参加を行った Windows 端末は、グループポリシーにより自動的 に NAP クライアントの設定が行われています。(<u>3.5.2</u>章参照)

本章では、グループポリシーを用いずに、手動で NAP クライアント設定を行う方法を示します。

8.1.1 Windows 7、Windows Vista の設定

Windows 7、Windows Vista の NAP クライアント設定ステップを以下に示します。本章では Windows 7 と Windows Vista で設定に違いがある場合、設定画面や設定手順の差分箇所について両方の設定方法を記述しています。

- (1) NAP Agent と Wired Auto Config サービスの有効化
- (2) EAP 実施クライアントとセキュリティセンターの有効化
- (3) <u>認証方式の構成</u>

(1) NAP Agent と Wired Auto Config サービスの有効化

① NAP Agent の有効化

「スタート」→「コントロールパネル」 →「システムとメンテナンス」→「管理 ツール」→「サービス」をクリックする。 「Network Access Protection Agent」を 右クリックし、プロパティを選択する。 次に、スタートアップの種類を「自動」 に選択し、サービスの状態にて「開始」 をクリックする。最後に「OK」をクリッ クして画面を閉じる。

Network Access Protection	名前	説明	状態	スタートアップの種類	ログオン
Agent	🔍 Net.Tcp ポート	net		無効	Local Se
	🔍 Netlogon	그	開始	自動	Local Sy
サービスの停止	Retwork Access	クラ	開始	手動	Networ
説明: クライアント コンピュータ上のネッ トワーク アクセス保護 (NAP) 機能を 有効にします	(ローカル コンピュー 全般 ログオン 回 サービス名 表示名(N): 説明(D): 実行ファイルの/5ス(C*WindowsVsyst スタートアップの 種類(E): サービスの大歌: 問題(G) ここでサービス名問題	-タ) Netr 消度 依 napage Networ クライア 機能を H): em32¥svc 自動 シブオブシ 開始 (合するとき(a)	work Acc 字関係 ent k Access ントコンピ 有効にしま hostexe <u>コンの構成</u> 事上(T) i適用する制	ess Protection Agent のジ Protection Agent ユーラ上のネットワーク アクセス(す -k NetworkService の詳細を表示します ー時(停止(P) 開始パラメークを指定してください	ロバティ 健 (NAP) ・ ・
	開始台パラメータ(M):				

図 8.1-1 NAP Agent と Wired Auto Config サービスの有効化①

 ② Wired AutoConfig の有効化

 ①と同じように「Wired AutoConfig」を 右クリックし、プロパティを選択する。 次に、スタートアップの種類を「自動」
 に選択し、サービスの状態にて「開始」 をクリックする。最後に「OK」をクリッ クして画面を閉じる。

	(ローカル コンピュー	ータ) Wired AutoConfig のフロバティ	l.
Wired AutoConfig	全般 ログオン [回復 依存関係	
サービスの停止	サービス名:	dot3svc	
サービスの再起動	表示名(N):	Wired AutoConfig	
	[党8月(D):	イーサネット インターフェイス上で IEEE 8 す。	02.1X 認証を実行しま /
説明: イーサネット インターフェイス上で	実行ファイルのパス C:¥Windows¥sys		orkRestricted
IEEE 802.1X 認証を実行します。	スタートアップの 種類(E):	自動	
	サービスのスタート	<u>アップ オブションの構成の詳細</u> を表示します	
	サービスの状態	開始	
	[開始:(S)	停止(T) 一時停止(P)	再開(R)
	ここでサービスを開	始するときに適用する開始パラメータを指定し	てください。
	88%4 (2=1,		
	1#1XB/1/J/X-7/(19/		
		OK ¥	ッンセル 通用(れ
	WLAN AutoConfig	g この 開始 自動	Local Sy
	🖏 WMI Performan	Win 手動	Local Sy

図 8.1-2 NAP Agent と Wired Auto Config サービスの有効化②

③ サービスの画面を閉じる。

(2) EAP 実施クライアントとセキュリティセンターの有効化

① MMC スナップインの追加

「スタート」→「検索の開始」に「mmc」と入力して MMC(Microsft Management Consol)を起 動する。

コンソール1の画面にて、「ファイル」→「スナップインの追加と削除」をクリックする。

 スナップインの追加と削除画面にて、 「NAP クライアントの構成」と「グルー プポリシーオブジェクトエディタ」をロ ーカルのコンピュータで追加し、「OK」 をクリックする。



図 8.1-3 EAP 実施クライアントとセキュリティセンターの有効化①
③ コンソール 1 の左画面にて、「コンソー ルルート」→「NAP クライアントの構成」
 →「実施クライアント」を選択し、右画 面の「EAP 検疫強制クライアント」を右 クリックして「有効」にする。

パールルート 名前	Ĵ.	状態	操作
	HOP 核反弦動(シンパント Peec 延行者)(明若 K ジットウス 体気(ない)(シント AP 化気(ない)(シント (スク・)	2003 2005 至为 至为	 2000 クイアント 表示 ここから新しいウィン 会析の情報に更新 ヘルプ EAP 検護器物クライアント 有効 そ析の情報に更新 プロパティ へルプ
	EAP 検疫強制クライアント		
 ◎ コージーインターフェ ○ 正常性登録の設定 名称 [取明 バージュン、 ペンダー 状態 	79823 約 EAP 検 用 ネッドン・ -ジョン・ 1.0 パダー: Microso 酸 無効	病強制クライアント ーク アクセス環境の強制を SIZ.1X や VPN テクノロジで使用される EAP EZ ft Corporation	

図 8.1-4 EAP 実施クライアントとセキュリティセンターの有効化②

 ④ コンソール 1 の左画面にて、「コンソールルート」→「ローカルコンピュータポリシー」→「コン ピュータの構成」→「管理用テンプレート」→「Windows コンポーネント」→「セキュリティセン ター」を選択する。

・Windows 7 の場合

右画面の「セキュリティセンターをオンにする(ドメイン上のコンピュータのみ)」を右クリックして「編集」を選択し、「有効」をチェックする。

🖾 Windows +	2 セキュリティ センター		18/1
Windows Windows Windows Windows Windows アブリケ- イベント イベント イベント イベント マブリケ- マント マン マント マント	はキュリティ センターをオンにす。 ドメイン上のコンピューターのみ (リシー設立) (現在) (Indows XP Professional, Indows Server 2003 ファミ) 、または本れの語	 セキュリティ センターをオンにする セキュリティ センターをオンにす 未構成(C) コン ● 形効(E) ● 新効(D) サポートされる/(-3) 	8 (ドメイン上のコンピューターのみ) F8 (ドメイン上のコンピューターのみ) mの知道(P) 次の初期(メント: ジョン: Windows XP Professional, Windows Server 2003 ファミリ、8
ゴック・ション・レース 2 に 0 の 2 の 2 の 2 の 2 の 2 の 2 の 2 の 2 の 2 の	用: (30代シー協定は、Active (30代シー協定は、Active (30代シーンターででキュリティ シンターをマンにするかとちかど さなりにすると、重要なでキュ (まつま)でキュンリティ センター やイジにすると、重要なでキュ ・ディンシトロールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド(34代) (まつシールド) (まつシールド(34代) (まつシールド(34代) (まつシールド) (まつンルド) (まつント) (ま	775=5:	へして: このボリシー製液は、Active Directory ドメインに参加 さコボリシューターでセキュリディ センターをオンにするよう かを想定します。セキュリディ センターをオンにするよう かを想定します。セキュリディ センターをオンにするよう なせキュリディの起きを提供、コンピューターが効果 されている制能がある場合にユーダーに満知します。コ ロール/パル/のセキュリディ センターのチョンを表示プリ表示に 別感のセクションをあり、ユーザーはコンピューターのグ リディ センター・がドメインで有効になっていない場合。 セキュリディ センターの状態セクションを表示されません Windows ドメインに考加していない場合。 ボリン・提定は何の感覚のラスません。 この設定がを構成の場合は、ドメインのメンリ(~について)

図 8.1-5 EAP 実施クライアントとセキュリティセンターの有効化(Windows 7)③

·Windows Vista の場合

右画面の「セキュリティセンターをオンにする(ドメイン上のコンピュータのみ)」を右クリックして「プロパティ」を選択し、「有効」をチェックする。

📔 Windows 🔺	📋 セキュリティ センター		操作
🛗 Windows			セキュリティセン ・
📔 Windows	項目を選択すると説明が表示されま	設定	他の操作・
Windows	<u>र</u> .	目 セキュリティ センターをオンにする (ドメイン上のコンピ	5-0100000000000000000000000000000000000
🚞 Windows		-	
🛗 Windows		セキュリティ センターをオンにする (ドメイン上のコンピュータの	ゆみ) 🖞 🔜 💴
📑 アプリケ			
📋 イベント		a×AE aT0H	
▷ 🛄 イベント		📅 セキュリティ センターをオンにする (ドメイン上のコンピュータのみ)	
🧾 インター			
▶ 🧰 エクスプ		◎ 未構成(C)	
🧰 オンライ		 有効(E) 	
🧰 ゲーム エ		◎ 無効(D)	
🧮 サウンド			
ジャット			
スマート			
📑 セキュリ			
▶ 🛄 ターミナ.			
タスクス			
デジタル			
□ ネットワ			
▶ 🦰 バックア			
ビデオの		サポートされるバージョン	
☐ プレゼン		Microsoft Windows XP Professional, Windows Server 2003 77≷!	し、またはそれ以
	↓ \ 拡張 〈 標進 /	前の設定(P) 次の設定(N)	
		OK キャンセル	通用(A)

図 8.1-6 EAP 実施クライアントとセキュリティセンターの有効化(Windows Vista)③

⑤ 「OK」をクリックして画面を閉じる。

(3) 認証方式の構成

- ローカルエリア接続のプロパティを表示し、認証タブを選択する。「IEEE802.1X 認証を有効にする」をチェックし、ネットワーク認証方法に「保護された EAP(PEAP)」を選択する。最後に「設定」をクリックする。
- ② 保護された EAP のプロパティ画面にて、信頼されたルート証明機関に作成した CA 局の名前がある 事を確認し、チェックする。次に、「検疫のチェックを有効にする」をチェックする。最後に、認 証方法として「セキュリティで保護されたパスワード(EAP-MSCHAPv2)」を選択し、「構成」を クリックする。
- ③ 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(およびドメインがある場合はドメイン)を自動的に使う」をチェックする。

・Windows 7 の場合

	保護された EAP のプロパティ
ネットワーク 認証 このイーサネット アダプター(ご認証)済みのネットワーク アクセスを提供する(こ (よ、このオプションを選択してください。 ■ IEEE 802.1X 認証を有分にする(N) ネットワークの認証で方法の選択(M): Microsoft: 保護された EAP (PEAP) ■ 該定(S) ■ ログオンするたびに、この接続用の資格情報を使用する(R)	接続のための認証方法:
☑ 承認されていないネットワーク アクセスにフォールバックする(F) 追加の服作定(D)	 新しいサーバーまたは信頼された証明機関を承認するようユーザー(こ求めない、YP) 記証方法を選択する(S): セキュリティで保護されたパスワード (EAP-MSCHAP v2) ▼ 構成(C)_ マ高速再接続を有効にする(F) マネッドワーク アクセス保護を強制する(N) サービックス 保護を強ける(N)
OK キャンセル EAP MSCHAPv2 のプロパティ × 接続のための認証方法: Windows ののグランをとパスワード(およびドメインがある場合はドメイン)を自動的に使気A) OK キャンセル	● サーバーに増与けビイオンド心「LV かない場合はむ時するい」 ■ ID ブライバシーを有効にする(I) ● OK キャンセル

図 8.1-7 認証方式の構成(Windows 7)①

・Windows Vista の場合

<u> ローカル エリア接続のプロパティ X </u>	保護された EAP のプロパティ
ネットワーク 認証 共有 このイーサネット アダブタに、認証法済みのネットワーク アクセスを提供するに は、このオブションを選択してください。 ▼ IEEE 8021X 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): 「保護された EAP (PEAP) ▼ 設定(S) ▼ 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)	接続のたいの記記証方法: マ サーバーの言語明書を検証する(V) □ ンたのサーバーに接続する(C). 【信頼されたルート証明視閲(R): □ Class 3 Public Primary Certification Authority □ Class 3 Public Primary Certification Authority □ Microsoft Root Certificate Authority □ Microsoft Root Certificate Authority □ Microsoft Root Certificate Authority □ map-LH=9CDNNGSWRVHM-CA □ Thavte Timestamping CA □ 新し(z)サーバーまたは信頼された証明視閲を承認するようユーザー(こ求め) ない(P)
	認証方法を選択する(S):
EAP MSCHAPv2 のプロパティ	セキュリティで保護されたパスワード (EAP-MSCHAP v2) ▼ 構成(G)
接続のための認証方法:	 マ 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) □ サーパーに暗号(ヒバインドの TI V がない場合(は切断する(D) OK キャンセル

図 8.1-8 認証方式の構成(Windows Vista)①

④ 「OK」をクリックして画面を閉じる。以上で設定は完了です。

AX シリーズ NAP ソリューションガイド IEEE802.1X 認証編(第9版)

8.1.2 Windows XP SP3 の設定

Windows XP SP3の NAP クライアント設定ステップを以下に示します。

- (1) NAP Agent と Wired Auto Config サービスの有効化
- (2) EAP 実施クライアントとセキュリティセンターの有効化
- (3) <u>認証方式の構成</u>
- (1) NAP Agent と Wired Auto Config サービスの有効化
 - ① NAP Agent の有効化

「スタート」→「コントロールパネル」→「管理ツール」→「サービス」をクリックする。 「Network Access Protection Agent」を右クリックし、プロパティを選択する。次に、スター トアップの種類を「自動」に選択し、サービスの状態にて「開始」をクリックする。最後に「OK」 をクリックして画面を閉じる。

🍓 サービス (ローカル)				
Network Access Protection	名前 🛆	説明 状態	スタートアップ [コグオン
	Messenger MS Software Shadow Copy Provid	ネットワー ボリューム	無効 D 手動 D] ーカル] ーカル
<u>サービスの再起動</u>	Net Logon	ドメイン… 開始 権限を与	自動 D 手動 D	1ーカル 1ーカル
[兑 ¹¹ 月:	Network Access Protection Agent	Windows 開始	手動	1ーカル
Windows クライアントにネットワーク アクセス 保護への参加を許可します。	(ローカル コンピュータ) Network	Access Protection	n Agent のプロパ	? 🛛
	全般 ログオン 回復 依存関係			
	サービス名: NapAgent			
	表示名(N): Network Acc	ess Protection Agent		
	説明(<u>D</u>): Windows クラ 可します。	イアントにネットワーク アク	セス保護への参加を許	
	実行ファイルのパス(出):	ovo ek notouro		_
	D.≢wiNDOws≠systemsz≢svcriust	.exe -k netsvos		
	スタート/9700 自動 種類(E):			~
				-
	開始(S) 停止(T) 一時停止(日	?) 再開(R)	
	ここでサービスを開始するときに適用す	な開始パラメータを指定	してください。	
	開始パラメータ(M):			
	(OK *	テャンセル 適用	<u>=(A)</u>

図 8.1-9 NAP Agent と Wired Auto Config サービスの有効化(Windows XP)①

② Wired AutoConfig の有効化

①と同じように「Wired AutoConfig」を右クリックし、プロパティを選択する。次に、スター トアップの種類を「自動」に選択し、サービスの状態にて「開始」をクリックする。最後に「OK」 をクリックして画面を閉じる。

🍓 サービス(ローカル)		
Wired AutoConfig	名前 🛆	説明 状態 スタートアップ ログオン
サービスの停止	Security Center	システム… 開始 自動 ローカル…
サービスの再進動	(ローカル コンピュータ)Wired Au	itoConfig のプロパティ 🛛 🕐 🔀
説明: Dia convice performs IEEE 9021V	全般 ログオン 回復 依存関係	ξ.
authentication on Ethernet interfaces	サービス名: Dot3svc	
	表示名(<u>N</u>): Wired AutoC	Config
	説明(<u>D</u>): This service Ethernet int	e performs IEEE 802.1X authentication on
	実行ファイルのパス(H)・	
	C#WINDOWS¥System32¥svchos	stexe -k dot3svc
	スタートアップの 自動	▼
	1EXR (_).	
	サービスの状態: 開始	
	開始⑤ 停止(D _ 時停止(P) 再開(B)
	ここでサービスを開始するときに適用	する開始パラメータを指定してください。
	開始パラメータ(<u>M</u>):	
		OK キャンセル 適用(<u>A)</u>
	Wired AutoConfig	This ser 開始中 手動 ローカル

図 8.1-10 NAP Agent と Wired Auto Config サービスの有効化(Windows XP)2)

- ③ サービスの画面を閉じる。
- (2) EAP 実施クライアントとセキュリティセンターの有効化
 - ① MMC スナップインの追加

「スタート」→「ファイル名を指定して実行」を開き、「mmc」と入力して MMC (Microsoft Management Consol)を起動する。

コンソール1の画面にて、「ファイル」→「スナップインの追加と削除」をクリックする。

② スナップインの追加と削除の画面にて「追加」をクリックする。 スタンドアロン スナップインの追加画面にて「グループポリシー」を選択し、「追加」をクリ ックする。



図 8.1-11 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)③

③ グループポリシーオブジェクトの選択画面にて、「完了」をクリックする。



図 8.1-12 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)④

④ コンソール1の左画面にて、「コンソールルート」→「ローカルコンピュータポリシー」→「コンピュータの構成」→「管理用テンプレート」→「Windows コンポーネント」→「セキュリティセンター」を選択する。右画面の「セキュリティセンターを有効にする(ドメイン上のコンピュータのみ)」を右クリックしてプロパティを選択し、「有効」をチェックする。

コンソール ルート	💼 ヤキュリティ ヤンター		
🗈 😼 ローカル コンピュータ ポリシー		-	
□	セキュリティ センターを有効にする (ドメ	設定 状態	
田 🧰 Windows の設定	17101761-20007	🇊 セキュリティ センターを有効にする(ドメイン上のコンピュータのみ) 🛛 有効	
□ □ 管理用テンプレート □ □ □ Windows コンポーネント	<u>プロパティ</u> の表示	セキュリティ センターを有効にする (ドメイン上のコンピュータのみ)のブロ 🤶	X
NetMeeting	必要条件: Microsoft Windows XP	設定説明	
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Professional、Windows Server 2003 ファミリ、またはそれよび峰	🎒 セキュリティ センターを有効にする(ドメイン上のコンピュータのみ)	
	割時 Active Directory ドメインに参加して いるユーザーのコンとユーダでやキュリテ イセンターを有効にするがどうかを指定 します。セキュリティの設定の重要項目で イアンフォールのパンパンの構造で します。セキュリティの設定の重要項目で オークロンパンパンパンパン が市危険にさなれている可能性がある 場合にユーザー(ご通知します、セキュリ ディセンターのコントロール/ドメルのカテ コン表示には、状態のセクションも表示、 コンポーズは、大能のセクションも表示、 ことができます。セキュリティの同 上に役立つゴ格要とれるプロ実実を取得す なことができます。セキュリティレシターを 悪効にすると、通知をセキュリティレシターで 、の状態を見つきょりも表示ではません。	 未構成(Q) () · 酒坊(Q) () · 無効(Q) 	
☞ 🚜 ユーザーの構成	Windows ドメインに参加していないコン ピュータでは、セキュリティ センターを無 効にすることはできません。この場合、ポ リシーは何も影響がありません。	サポートされるバージョン: Microsoft Windows XP Professional, Windows Server 2003 ファミリ、またはそれ以… 前の設定(空) 次の設定(公)	
	この設定が未構成の場合は、ドメインの メンバについてはセキュリティセンターは 無効になります。	OK キャンセル 適用(A)	

図 8.1-13 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)⑤

⑤ 「OK」をクリックして画面を閉じる。

 ⑥ コマンドプロンプトを開き、「EAP Quarantine Enforcement Client」を有効化するコマンドを実 行する。

netsh nap client set enforcement ID = 79623 ADMIN = "ENABLE"

 ⑦ 以下のコマンドを実行して、「実施クライアントの状態」の中の「EAP Quarantine Enforcement Client」が「初期化済み = はい」となっている事を確認する。

netsh nap client show state

ID 名前 説明 バージョン ベンダ名 登録日 初期化済み System Health Agent (S	= 79623 = EAP Quarantine Enforcement Client = EAP ベースの強制を NAP に提供します。 = 1.0 = Microsoft Corporation = = (はい
ID 名前	= 78744 = Windows セキュリティ正常性エージェント
説明 したポリシーに、コンビ	= Windows セキュリティ正常性エージェントは、管理者が定義 ュータが準拠しているかどうかをチェックします。
バージョン	= 1.0
ベンダ名	= Microsoft Corporation
登録日 初期化済み エラーのカテゴリ 修復の割合 修正のメッセージ は、セキュリティ状態の	= = はい = なし = 成功 = 0 = (3237937214) - ₩indows セキュリティ正常性エージェントで 更新を終了しました。
確認の結果 修復の結果	=
OK	

図 8.1-14 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)⑥

(3) 認証方式の構成

- ローカルエリア接続のプロパティを開き、「認証」タブを選択する。「IEEE802.1X 認証を有効 にする」をチェックし、ネットワーク認証方法に「保護された EAP(PEAP)」を選択する。最 後に「設定」をクリックする。
- ② 保護された EAP のプロパティ画面にて、信頼されたルート証明機関に作成した CA 局の名前がある事を確認し、チェックする。次に、「検疫のチェックを有効にする」をチェックする。最後に、認証方法として「セキュリティで保護されたパスワード(EAP-MSCHAPv2)」を選択し、「構成」をクリックする。
- ③ 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(およびドメインがある場合はドメイン)を自動的に使う」をチェックする。



図 8.1-15 認証方式の構成(Windows XP)①

④ 「OK」をクリックして画面を閉じる。

以上で設定は完了です。

8.2 コンピュータ認証について

「6.2.1 非認証状態保持時間の設定について」で述べたとおり、本ガイドの検疫ネットワークでは、 コンピュータ認証が失敗する構成となっています。コンピュータ認証の扱いについて他の構成を以下に 紹介します。なお以下の設定は必須ではありません。

(1) コンピュータ認証が成功するようにネットワークポリシーを作成する

コンピュータ認証が成功した場合に所属する VLAN とネットワークポリシーを新たに追加作成し ます。この VLAN に所属する端末は、ドメインコントローラとのみ通信可能とします。この構成で は、認証スイッチの非認証状態保持時間を調整する必要はありませんが、各スイッチに対して、新し い VLAN およびその VLAN に適用するフィルタの設定が必要になります。また、NPS に対しても新 しいネットワークポリシーの設定が必要になります。

(2) クライアント端末のコンピュータ認証を停止させる

3.5.2.(3)の「新しい Vista ワイヤード(有線)ネットワークポリシー画面」にて、「セキュリティ」タブにある「認証モード」を「ユーザー認証」に設定することにより、コンピュータとしての IEEE802.1X 認証が行われなくなります。ただし、ユーザーがログオフした後、ユーザがログオンするまでは、前回ログオンしたユーザで認証は通ったままになります。

また、<u>3.5.2</u>のグループポリシーを用いずにクライアントで手動設定する場合は、クライアント OS 毎に設定方法が異なります。

・Windows 7 の場合

「8.1.1(3)認証方式の構成」の Windows 7 の「ローカルエリア接続のプロパティ」 内にある「追加の設定」をクリックし、認 証モードを「ユーザー認証」に変更するこ とで IEEE802.1X 認証のコンピュータ認証 は停止し、ユーザー認証のみ行うように構 成できます。

802.1×の設定	
 ✓ 認証モードを指定する(P) ユーザー認証 コペてのユーザーの資格情報を削除する(L) 	資格情報の保存(C)
◎ こっせい ログナンの支払(こ本)(こ本)	nc78(S)
 ユーザー ログオンの直接(ま実行する(E) ユーザー ログオンの直接(ま実行する(E) 最大待ち時間(秒)(M): ✓ シングル サインオン中に追加のダイアログの剥 □ このネットワークでは、コンピューターとユーザー □ LAN を使用する(Y) 	10 表示を許可する(D) の認証(こ別の仮想

図 8.2-1 コンピュータ認証の停止

·Windows Vista、Windows XP SP3 の場合

netsh コマンドによる設定のエクスポートと設定ファイルの編集、および設定ファイルのインポートが必要になります。手動設定の詳細については、下記 Microsoft の技術情報を参照して下さい。

 How to enable computer-only authentication for a 802.1X-based network in Windows Vista (英語) http://support.microsoft.com/kb/929847/en-us

付録A. コンフィグレーション

(1) AX シリーズのコンフィグレーションファイル

本ガイドにて紹介した構成のコンフィグレーション例です。

「<u>3章 検疫ネットワークの構築(動的 VLAN 構成)</u>」と「<u>4章 検疫ネットワークの構築(固定 VLAN(ポート単位)構成</u>」のネットワーク構成における各装置のコンフィグレーションをテキスト形式のファイルとして本ガイドに添付しております。(添付ファイルを抽出するには、Adobe Acrobat 5.0 以降もしくは Adobe Reader 6.0 以降が必要です。)

各コンフィグレーションについては、以下に示すファイル名と同じ名前の添付ファイルを参照下さい。

構築例	対象機器	装置名	対象ファイル
	認証スイッチ	edge#1(AX1240S)	edge#1d_config.txt
	認証スイッチ	edge#1(AX1230S)	edge#1d_AX1230_config.txt
	認証スイッチ	distr#1(AX2430S)	distr#1d_config.txt
構築例1	認証スイッチ	distr#2(AX2530S)	distr#2d_config.txt
	L3 スイッチ	core#1(AX3630S)	core#1d_config.txt
	L3 スイッチ	core#2(AX3630S)	core#2d_config.txt
	L3 スイッチ	core#3(AX3630S)	core#3d_config.txt
構築例 2	認証スイッチ	edge#1(AX1240S)	edge#1s_config.txt
	認証スイッチ	distr#1(AX2430S)	distr#1s_config.txt
	認証スイッチ	distr#2(AX2530S)	distr#2s_config.txt
	L3 スイッチ	core#1(AX3630S)	core#1s_config.txt
	L3 スイッチ	core#2(AX3630S)	core#2s_config.txt
	L3 スイッチ	core#3(AX3630S)	core#3s_config.txt

< 空白ページ >



2014 年 10 月 22 日 第9版 (Rev.2) 発行 資料 No. NTS-07-R-033

アラクサラネットワークス株式会社 ネットワークテクニカルサポート

〒212-0058

川崎市幸区鹿島田一丁目1番2号 新川崎三井ビル西棟 http://www.alaxala.com/