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

第 9 版 (Rev.2)

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 ・ 認証スイッチで VRRP をフィルタリング ・ コアスイッチ間にリンクアグリゲーションを設定	3.1.1 3.1.2 3.1.3 3.2.1 3.2.3 付録 A
			AX1230S に端末検出機能を停止するコンフィグレーションを追加	3.1.3.1(3) 付録 A
			Windows Server 2008 のデフォルトドメインポリシーの変更方法を追加	4.3
			NAP クライアントのネットワークアクセス状態の確認方法を追加	5.3.2
			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 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 との連携および特徴を新規追加	1.4 1.5
			認証前 VLAN から Windows ドメインにログオンできる構成に変更	3.2 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	6 章
第 5 版	―	2008.9.16	AX1200S(Ver1.4)でサポートされた内容を反映 ・ IEEE802.1X 認証(動的 VLAN モード)の新コンフィグレーションに変更 ・ 認証専用アクセスリストをサポート	2 章 3.3.1 3.4.1 4.4.1 5.1.1

第 6 版	―	2009.3.9	新規機種 AX1240S に対応 ・ 収容条件追加 ・ AX1230S との動作差分記載 システムファンクションリソース設定 フィルタのコンフィグレーションコマンド	はじめに 2 章 3.3.1 3.4.1 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 ・検疫ネットワークの構築(基本編)のタイトルを(固定 VLAN 構成)に変更、(応用編)削除し(固定 VLAN 構成)を新規追加	1.3 3 章 4 章 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 ・固定 VLAN モードの NAP 連携をサポート ・IEEE802.1X 認証の認証専用 IPv4 アクセスリストをサポート	1.3 2 章 3.3 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 AX1200S を認証スイッチにした場合の構築ポイントを追加	3.3 3.4
			Windows Server のネットワークポリシーの構成で認証エラーの最大値設定を追加	3.5
			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」を追加	1.6
			AX シリーズの構築ポイント（1）にレイヤ 2 ハードウェアテーブルの検索方式を追加	3.3.1
			AX シリーズのコンフィグレーションを更新 ・レイヤ 2 ハードウェアテーブルの検索方式を追加	3.4 4.4
			注意事項を更新	6
			6.2.1 の内容の一部を 8 章構築ノウハウ「8.2 コンピュータ認証について」に移動	8.2
第 9 版	―	2011.1.28	収容条件に追加 AX2530S 追加	2
			コンフィグレーションに AX2530S と AX1240S との差分として追加	3.4.4 4.4.4
			グループポリシーの設定時に gpupdate /force コマンドを追加し設定反映を即時に実施するよう変更	3.5.2(7)
			AX2530S のコンフィグレーション例追加	付録 A
	1	2014.9.18	収容条件に AX2230S および AX3650S 追加 収容条件の認証モードについて、表現を修正	2 章
	2	2014.10.22	AX2400S,AX3600S,AX6000S での固定 VLAN モードの表記について明確化	1.3 4 章 5.1

目次

1. NAP 検疫概要 8

1.1 検疫ネットワークとは 8
1.2 NAP (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 Active 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 20
1.5.1 NAP 検疫の特徴 20
1.5.2 AX シリーズを用いた NAP 検疫システムの特徴 20
1.6 オ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 22
1.6.2 Windows 7、Windows Vista、Windows XP(SP3)の差分 22

2. AX シリーズの収容条件 23

3. 検疫ネットワークの構築（動的 VLAN 構成） 24

3.1 概要 24
3.2 検疫ネットワーク構成図 25
3.3 構築ポイント 27
3.3.1 AX に関する構築ポイント 27
3.3.2 Windows Server 2008 に関する構築ポイント 29
3.4 AX の設定 30
3.4.1 AX1200S のコンフィグレーション 30
3.4.2 AX2400S のコンフィグレーション 33
3.4.3 AX3600S のコンフィグレーション 36
3.4.4 AX2500S のコンフィグレーション 38
3.5 Windows Server 2008 の設定 39
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 50
3.5.4. RADIUS クライアントの設定 52

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 56
3.5.7. 正常性ポリシーの設定 58
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 66
3.6 NAP クライアントの設定 69
3.6.1. 導入ステップ 69
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 概要 74
4.2 検疫ネットワーク構成図 75
4.3 構築ポイント 77
4.3.1 AX に関する構築ポイント 77
4.4 AX の設定 79
4.4.1 AX1240S のコンフィグレーション 79
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 Windows Server 2008 の設定 86
4.5.1 ネットワークポリシーの設定 86
5. 動作確認 92
5.1 AX シリーズの運用コマンド 92
5.1.1 show dot1x detail 92
5.1.2 show dot1x logging 94
5.1.3 clear dot1x auth-state 94
5.2 NPS の運用ツール 95
5.2.1 イベントビューアー 95
5.3 NAP クライアントの運用ツール 97
5.3.1 netsh nap client show state 97
5.3.2 ネットワークアクセス状態の確認 98
6. 注意事項 100
6.1 動的 VLAN 使用時の注意事項 100
6.1.1 Windows XP の IP アドレス切り替え問題 100
6.1.2 IP アドレス切り替え問題の詳細解説 103
6.2 VLAN モード共通（動的 VLAN、固定 VLAN）の注意事項 105
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 106
7.2 検疫に成功しない 106
7.3 IEEE802.1X 認証動作を行わない 106

8. 設定ノウハウ集 107

8.1 手動による NAP クライアント設定 107
8.1.1 Windows 7、Windows Vista の設定 107
8.1.2 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。

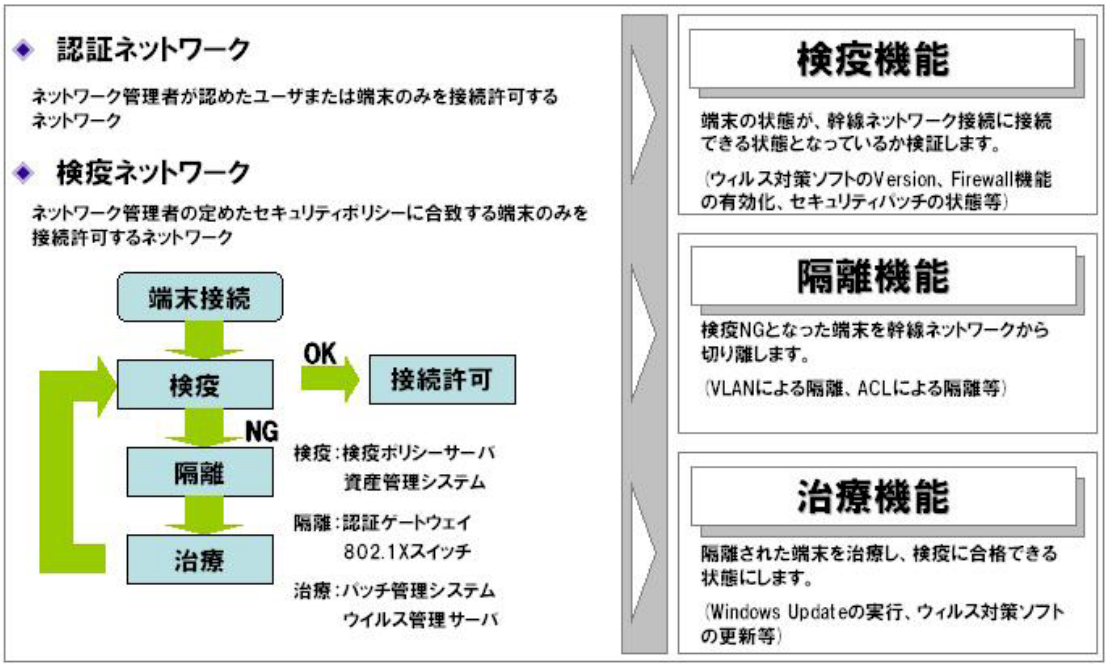


図 1.1-1 検疫ネットワークの要素

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。

表 1.2-1 NAP 実施オプション

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トコル)	DHCP サーバ	検証結果に応じて、IP アドレスを割り当てる。
2	インターネットプロトコルセキュリティ(IPsec)	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。
3	IEEE802.1X 認証	IEEE802.1X ネットワーク機器	検証結果に応じて、接続ポートへ動的な VLAN を割り当てる。
4	仮想プライベートネットワーク(VPN)	VPN サーバ	検証結果に応じて、パケットフィルタリングを行う。
5	ターミナルサービスゲートウェイ	ターミナルサービスゲートウェイサーバ	検証結果に応じて、ターミナルサーバへの中継を行う。

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）
  http://technet.microsoft.com/en-us/network/bb545879.aspx

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。

表1-1 認証モードの表記

本ガイド上のモード表記	認証方式	製品マニュアル上の表記		
		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
レガシーモード	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)
	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)	―	―

―：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。

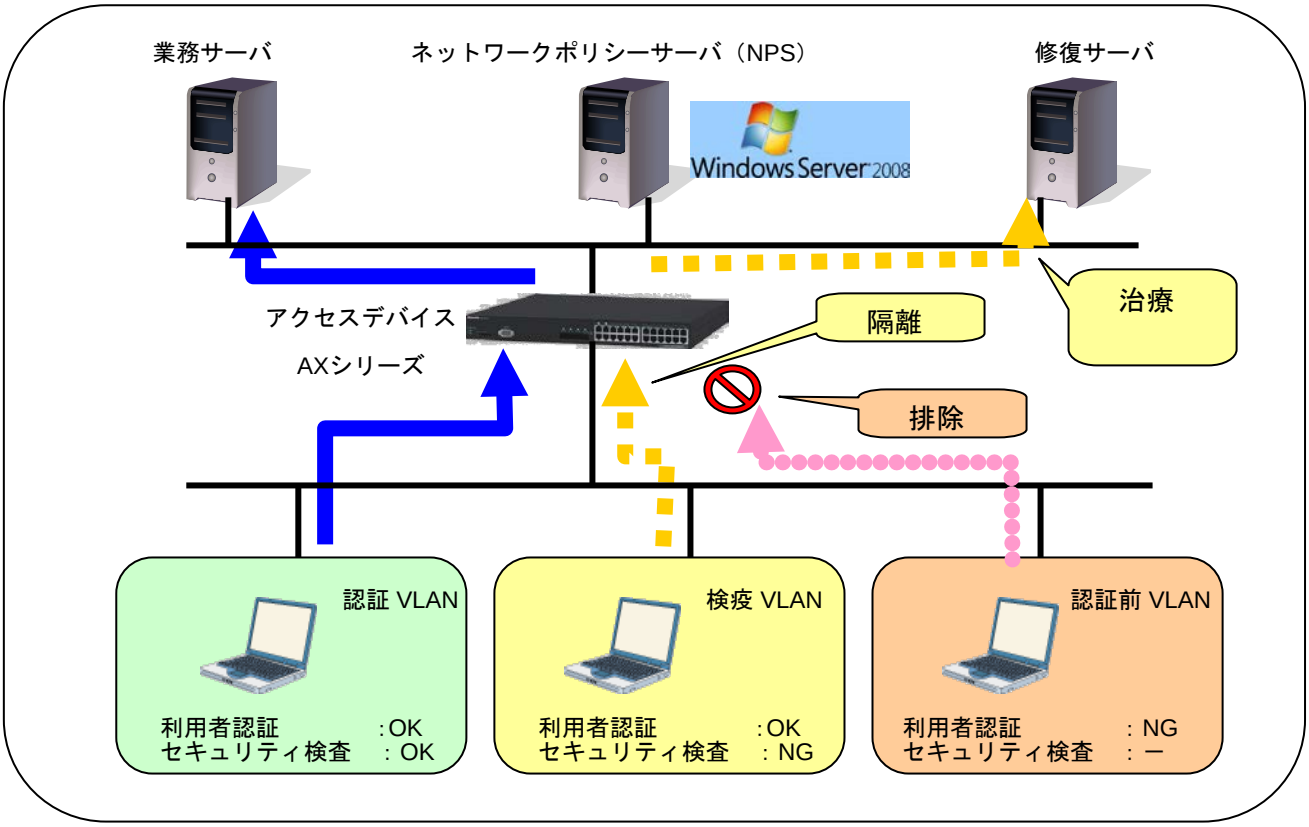


図 1.3-1 AX シリーズと NAP システムによる検疫動作(動的 VLAN モード)

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。

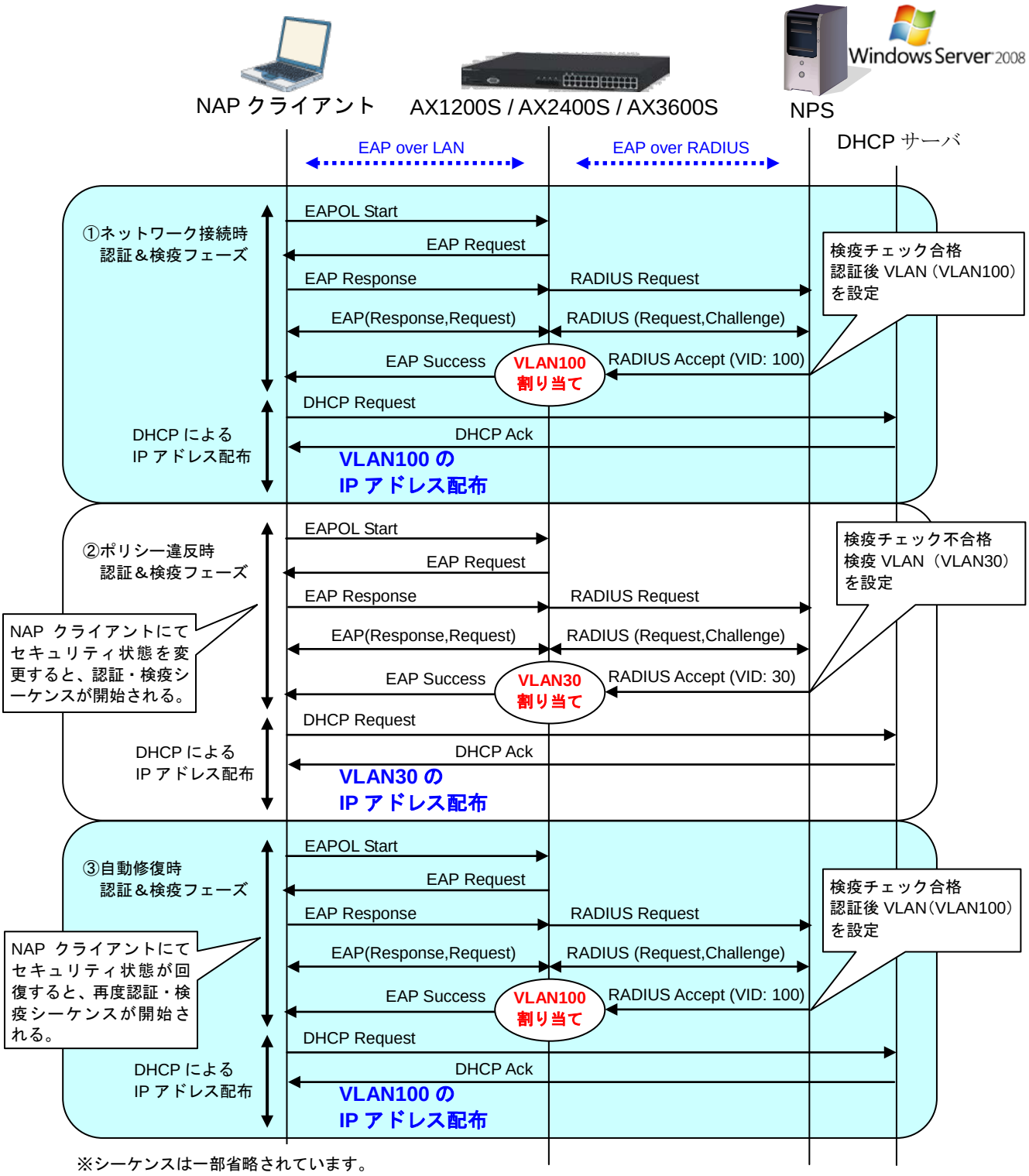


図 1.3-2 NAP シーケンス（動的 VLAN モード）

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。

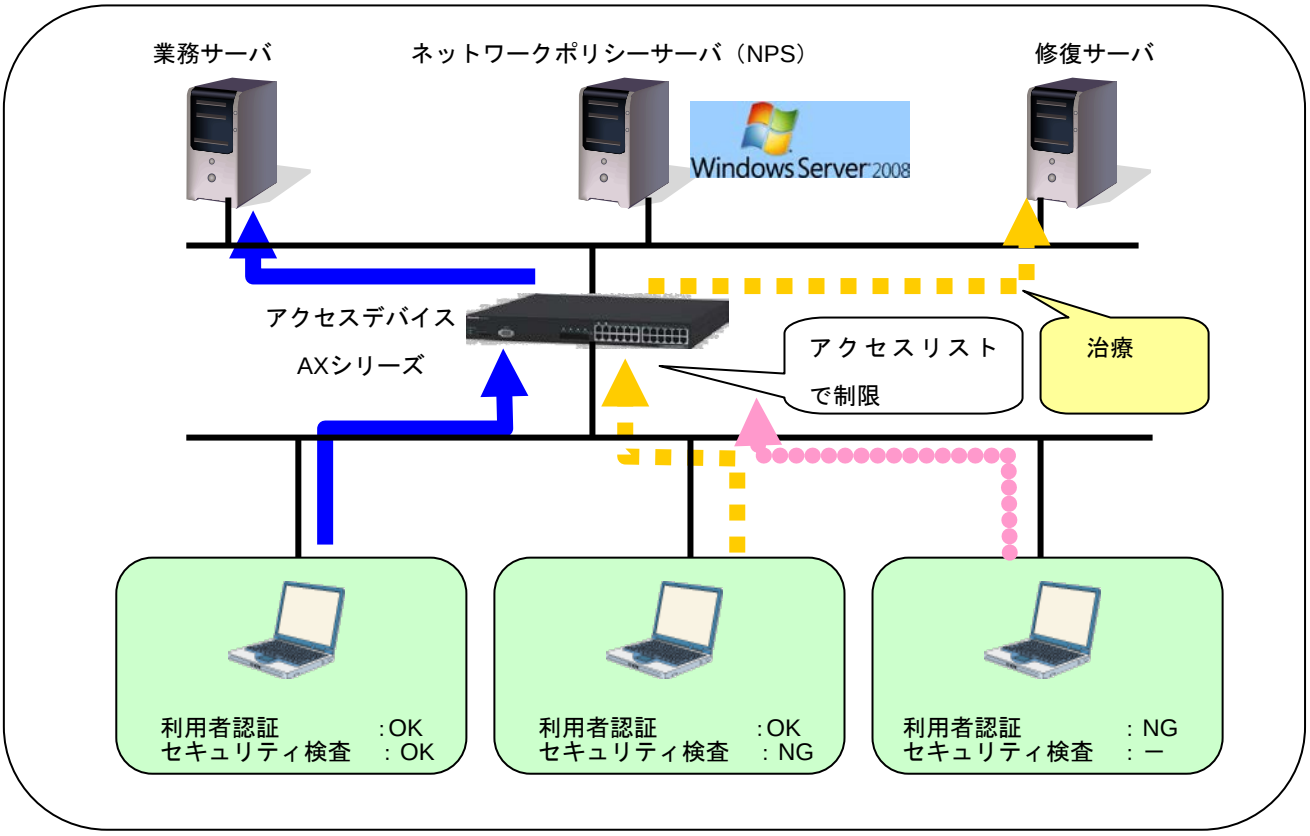


図 1.3-3 AX シリーズと NAP システムによる検疫動作(固定 VLAN モード

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。

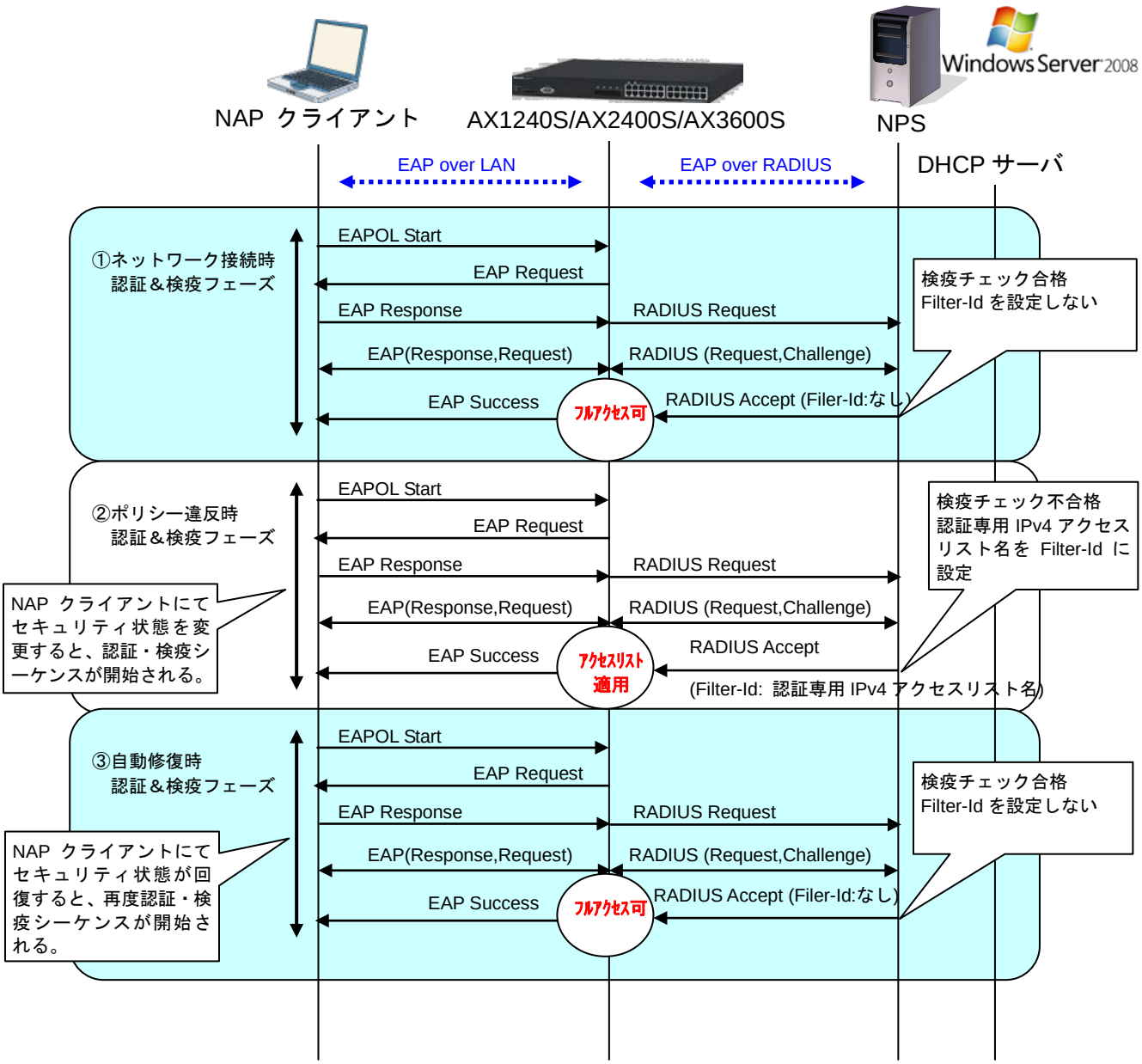
・検疫機能：NPS の SHV と NAP クライアントの SHA によるシステム正常性の確認を行う。

・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。

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

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

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 クライアント端末の状態	動的 VLAN モード		固定 VLAN モード	
	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 VLAN	認証専用 IPv4 アクセスリストの設定範囲	接続ポートの VLAN	認証専用 IPv4 アクセスリストの設定範囲
検疫 NG	検疫 VLAN	検疫 VLAN の設定範囲		認証専用 IPv4 アクセスリストの設定範囲
検疫 OK	ユーザ毎の認証 VLAN	フルアクセス可能(*1)		フルアクセス可能(*1)

（＊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 ドメインへ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（1.4.2参照）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。（1.4.1参照）

（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。

- 「3.5.2 グループポリシーの設定」の（３）、（４）、（５）の設定画面
- 「3.5.4 RADIUS クライアントの設定」の設定画面
- 「3.5.5 接続要求ポリシーの設定」の⑨処理順序の変更
- 「3.5.6 システム正常性検証ツール（SHV）の設定」の設定画面
- 「3.5.7 正常性ポリシーの設定」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。
- 「6.1.1 Windows XP の IP アドレス切り替え問題」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 認証	固定 VLAN	ー	○	○	ー
	動的 VLAN	○	○	○	○
Web 認証	固定 VLAN	ー	ー	ー	ー
	動的 VLAN	ー	ー	ー	ー
MAC 認証	固定 VLAN	ー	ー	ー	ー
	動的 VLAN	ー	ー	ー	ー

(凡例) ○：検疫連携可能　△：検疫連携可能予定　ー：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。

表 2-2 認証モード毎の最大認証端末数

認証方式	認証モード	AX1200S AX2200S		AX2500S		AX2400S AX3600S		AX6300S AX6700S	
IEEE802.1X 認証	固定 VLAN (ﾎﾟｰﾄ単位)	64/ポート(*2)	合計 256/装置(*2)	1024/ポート	合計 1024/装置	64/ポート	合計 1024/装置	256/ポート	合計 4096/装置
	固定 VLAN (VLAN 単位)	×		×		256/VLAN		256/VLAN	
	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/装置		1024/装置		4096/装置	
	動的 VLAN	256/装置		1000/装置		1024/装置(*1)		4096/装置	

(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。

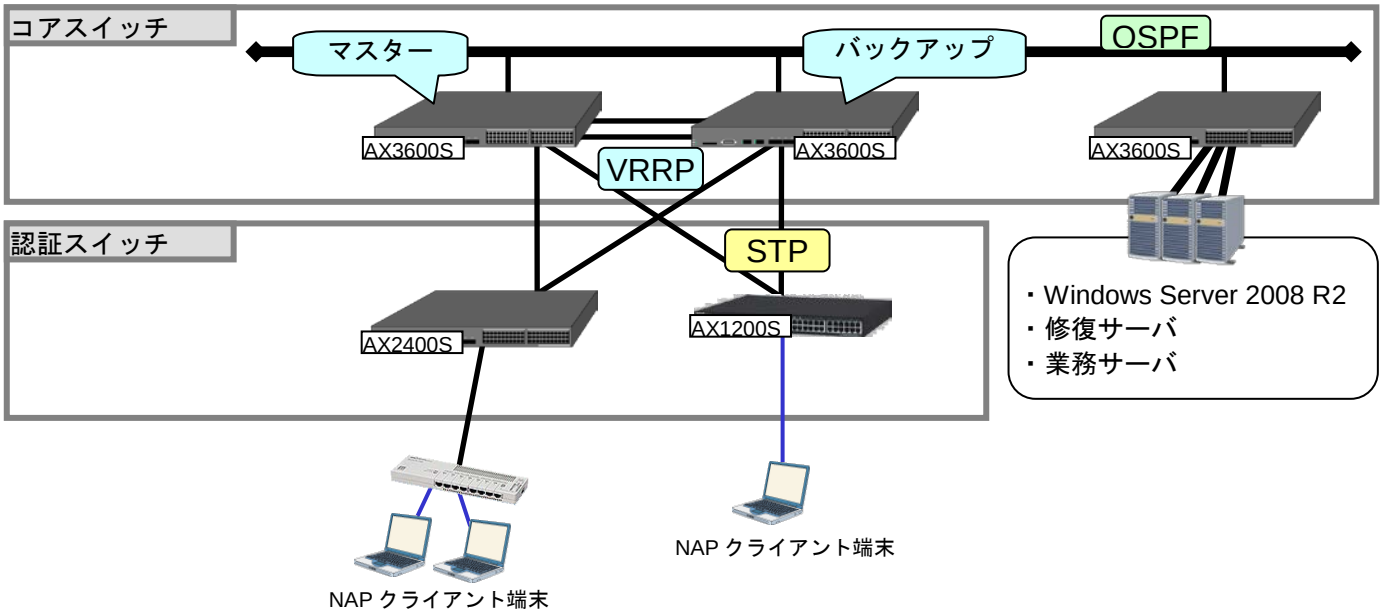


図 3.1-1 検疫ネットワークの構成(動的 VLAN 構成)

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

検疫ネットワーク構成図(動的 VLAN 構成)を以下に示します。

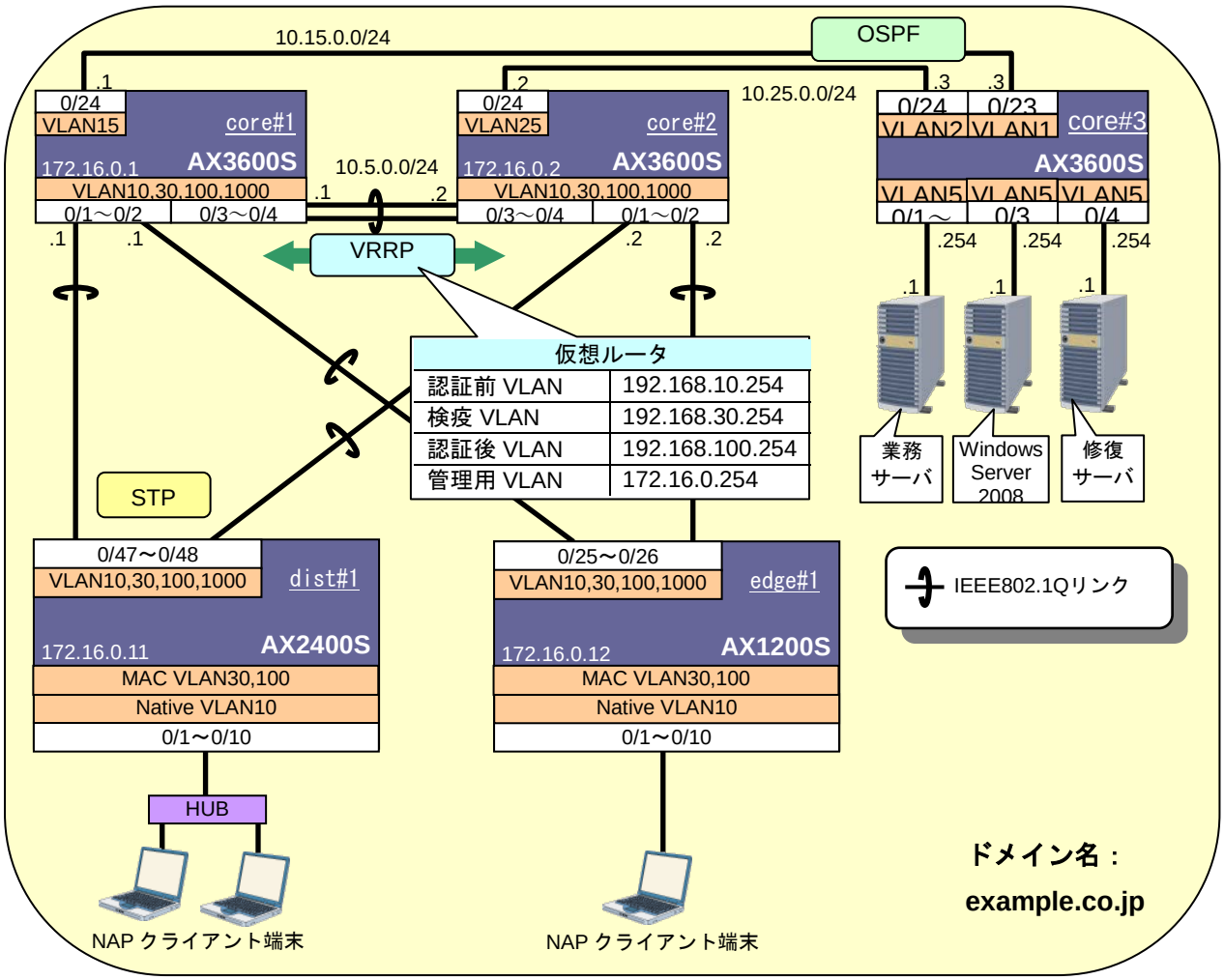


図 3.2-1 検疫ネットワーク構成図(動的 VLAN 構成)

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
AX2400S	認証用	0/1～0/10	MAC VLAN ポート	IEEE802.1X 認証 (動的 VLAN)	10	30	100
	上位スイッチとの通信用	0/47～0/48	トランクポート	—	—	—	—
AX1200S	認証用	0/1～0/10	MAC VLAN ポート	IEEE802.1X 認証 (動的 VLAN)	10	30	100
	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 VLAN	50	10.50.0.0/24	検疫後に通信可能なサーバが所属する VLAN。	業務サーバ
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
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	×	○	×
検疫 VLAN	30	×	○	○
認証後 VLAN	100	○	○	○

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

Windows ドメイン名		
example.co.jp		
グループポリシー		
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 ドメインへログオンするため、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、表 3.2-3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。** ➢ **構築ポイント（１）**
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。** ➢ **構築ポイント（１）**

（２） 基本設定

AX1200S シリーズの設定	
ポート VLAN の設定	
(config)# vlan 1 (config-vlan)# state suspend (config)# vlan 10 (config-vlan)# name BeforeAuthVLAN (config)# vlan 1000 (config-vlan)# name ManagedVLAN	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。
MAC VLAN の設定	
(config)# vlan 30 mac-based (config-vlan)# name QuarantineVLAN (config)# vlan 100 mac-based (config-vlan)# name OkVLAN	検疫 VLAN として MAC VLAN30 を、認証後 VLAN として MAC VLAN100 を作成します。 ➢ **構築ポイント（４）**
スパニングツリーの設定	
(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	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（４）**
●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 10,30,100,1000	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（１０）**
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（７）**

（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	
(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	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。 ➢ **構築ポイント（３）**
検疫 VLAN 用アクセスリストの設定	
(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 0.0.0.0 (config-ext-nacl)# permit protocol ip src 10.52.0.1 0.0.0.0 dst 192.168.30.0 0.0.0.255 (config-ext-nacl)# permit udp src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps (config-ext-nacl)# permit udp src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootpc --AX1240Sの場合-- (config-ext-nacl)# 10 permit ip 192.168.30.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# 20 permit ip host 10.51.0.1 192.168.30.0	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。 ・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。 ----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	
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。 ➢ **構築ポイント（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 (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 (config-if-range)# dot1x timeout quiet-period 5 (config-if-range)# dot1x supplicant-detection disable (config-if-range)# authentication ip access-group JoinDomain (config-if-range)# authentication arp-relay (config)# dot1x system-auth-control	ポート 0/1～0/10 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。 非認証状態保持時間を 5 秒に設定します。 ➢ **構築ポイント（９）** 端末検出モードを disable にして、EAP-Request/Identity の送信を抑止します。 AX1240S を使用する場合は auto に設定して下さい。 ➢ **構築ポイント（８）** 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。 認証前の ARP リレーを設定します。 ➢ **構築ポイント（３）** 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。

（1） 事前設定

AX2400S 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（1）**

（2） 基本設定

AX2400S の設定

ポート VLAN の設定

```
(config)# vlan 1
(config-vlan)# state suspend
(config)# vlan 10
(config-vlan)# name BeforeAuthVLAN
(config)# vlan 1000
(config-vlan)# name ManagedVLAN
```

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。

MAC VLAN の設定

```
(config)# vlan 30 mac-based
(config-vlan)# name QuarantineVLAN
(config)# vlan 100 mac-based
(config-vlan)# name OkVLAN
```

検疫 VLAN として MAC VLAN30 を、認証後 VLAN として MAC VLAN100 を作成します。

➢ **構築ポイント（4）**

スパニングツリーの設定

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

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

●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（4）**

●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 10,30,100,1000
```

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。

➢ **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 172.16.0.11 255.255.255.0	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。
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（７）**

（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 (config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# permit ip host 10.51.0.1 192.168.10.0 0.0.0.255 (config-ext-nacl)# permit udp any eq bootps any (config-ext-nacl)# permit udp any eq bootpc any	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 (config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# permit ip host 10.51.0.1 192.168.30.0 0.0.0.255 (config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 host 10.52.0.1 (config-ext-nacl)# permit ip host 10.52.0.1 192.168.30.0 0.0.0.255 (config-ext-nacl)# permit udp any eq bootps any (config-ext-nacl)# permit udp any eq bootpc any (config)# interface vlan 30 (config-if)# ip access-group Quarantine in	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。 ・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。 ➢ **構築ポイント（５）**

（４） IEEE802.1X 認証の設定

AX2400S の設定

RADIUS の設定

(config)# aaa authentication dot1x default group radius (config)# aaa authorization network default group radius	RADIUS サーバで IEEE802.1X 認証を行うことを設定します。 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 (config-if-range)# authentication ip access-group JoinDomain (config)# dot1x vlan dynamic radius-vlan 30,100 (config)# dot1x vlan dynamic enable (config)# dot1x vlan dynamic reauthentication (config)# dot1x vlan dynamic timeout reauth-period 3600 (config)# dot1x vlan dynamic timeout quiet-period 5 (config)# dot1x vlan dynamic supplicant-detection auto (config)# dot1x system-auth-control (config)# dot1x logging enable	ポート 0/1～0/10 に対して、認証専用アクセスリスト「JoinDomain」を適用します。 ➢ **構築ポイント（３）** 認証後動的に切り替わる VLAN を、VLAN30 および 100 とします。 ➢ **構築ポイント（４）** IEEE802.1X 認証(動的 VLAN)を有効にします。 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。 非認証状態保持時間を 5 秒に設定します。 ➢ **構築ポイント（９）** 端末検出モードを auto にして、EAP-Request/Identity の送信を自動します。 ➢ **構築ポイント（８）** 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 (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。

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
(config-vlan)# name BeforeAuthVLAN
(config)# vlan 30
(config-vlan)# name QuarantineVLAN
(config)# vlan 100
(config-vlan)# name OkVLAN
(config)# vlan 1000
(config-vlan)# name ManagedVLAN
```

VLAN1 は使用しないため、無効にします。

認証前 VLAN として VLAN10 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。

スパニングツリーの設定

```
(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
```

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（１２）**

```
(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
```

ブリッジ優先度を設定します。

➢ **構築ポイント（１３）**

物理ポートの設定

```
(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 10,30,100,1000
```

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

```
(config)# interface port-channel 1
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,30,100,1000
```

```
(config)# interface range gigabitethernet 0/3-4
(config-if-range)# channel-group 1 mode on
```

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。

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（１１）**

インタフェースの設定

```
(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
```

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	
(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 (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 (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 (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	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。 ・アクセプトモードを有効にします。 ➢ **構築ポイント（１３）**

（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 (config)# interface vlan 30 (config-if)# ip helper-address 10.51.0.1 (config)# interface vlan 100 (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。 ➢ **構築ポイント（１４）**

（4） OSPF の設定

AX3600S の設定	
ポート VLAN の設定	
(config)# vlan 5 (config-vlan)# name OSPF (config)# vlan 15 (config-vlan)# name OSPF	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	
(config)# interface gigabitethernet 0/24 (config-if)# switchport mode access (config-if)# switchport access vlan 15 (config-if)# spanning-tree portfast	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	
(config)# interface port-channel 1 (config-if)# switchport trunk allowed vlan add 5	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	
(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	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） 事前準備

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） グループポリシーの設定（Active Directory）

本環境用のグループポリシーを作成します。

（3） 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） 接続要求ポリシーの設定（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） システム正常性検証ツール（SHV）の設定（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） ネットワークポリシーの設定（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） DHCP サーバの設定（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。

表 3-6 グループポリシーの設定内容

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。

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） システムサービスの構成
（3） ネットワークポリシーの構成
（4） NAP クライアントの構成
（5） セキュリティセンターの構成
（6） グループポリシーの優先度の変更
（7） グループポリシーの反映

（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。

① 「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。

② 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。

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

③ 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。

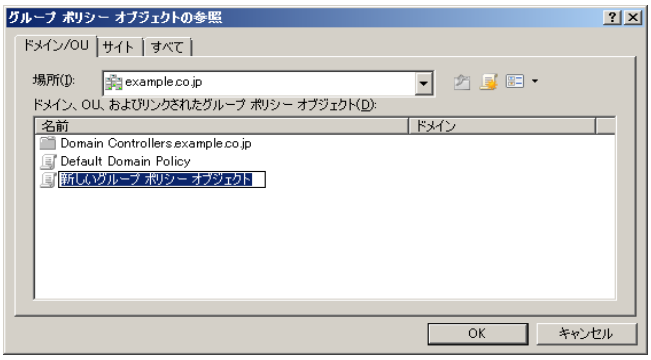


図 3.5-2 新しいグループポリシーオブジェクトの作成②

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。

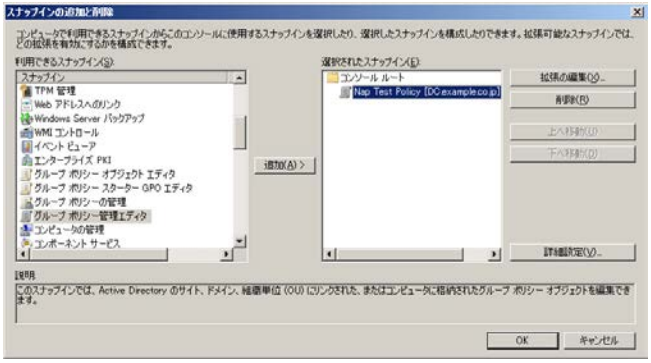


図 3.5-3 新しいグループポリシーオブジェクトの作成③

（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」→「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。

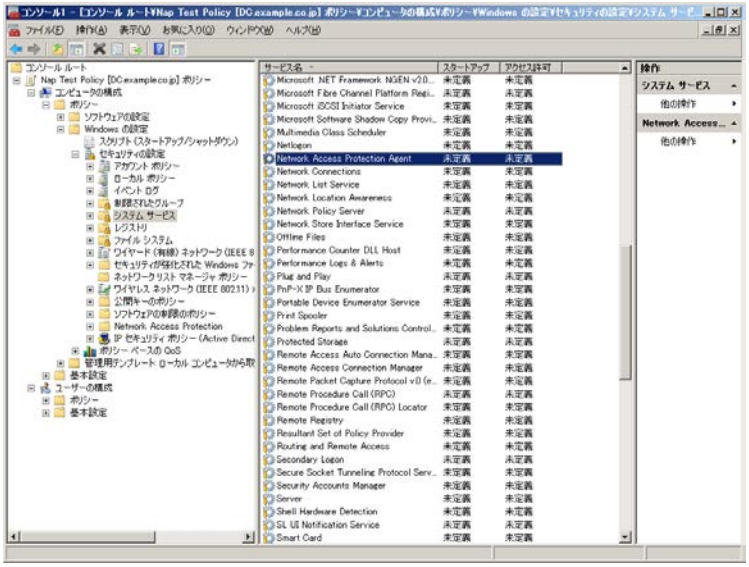


図 3.5-4 システムサービスの構成①

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 3.5-5 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「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の作成」を選択する。

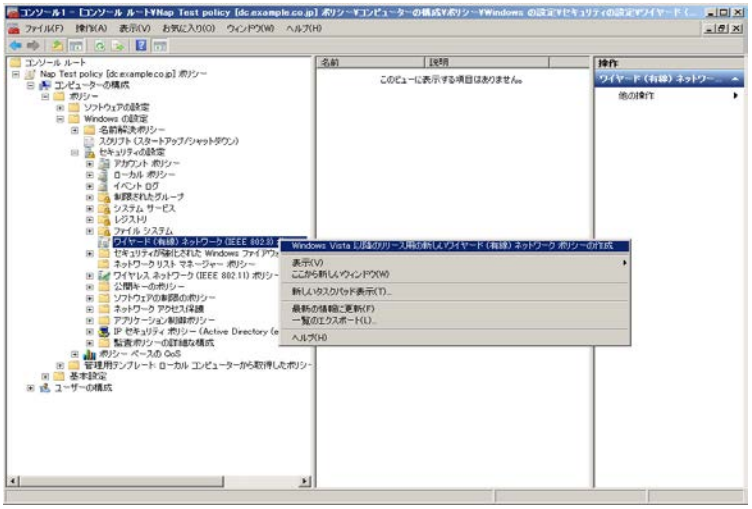


図 3.5-7 ネットワークポリシーの構成(Windows Server 2008 R2)①

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「新しい Windows Vista ポリシーの作成」を選択する。

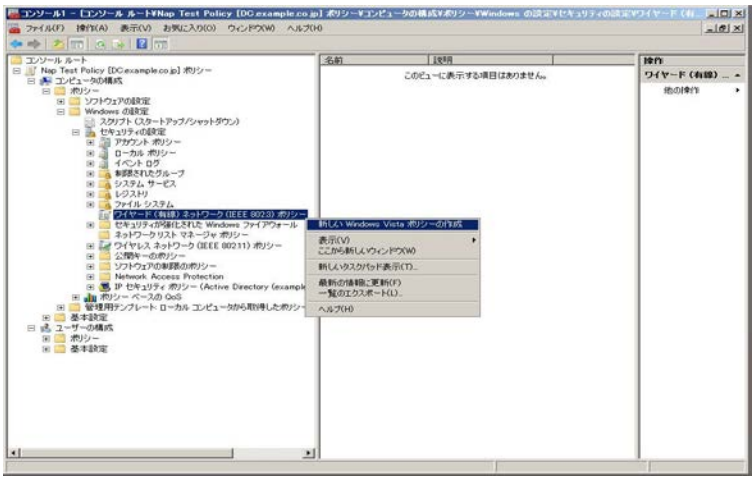


図 3.5-8 ネットワークポリシーの構成(Windows Server 2008)①

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、「ネットワークアクセス保護を強制する」にチェックする。

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）」が選択されている事を確認し、「構成」をクリックする。

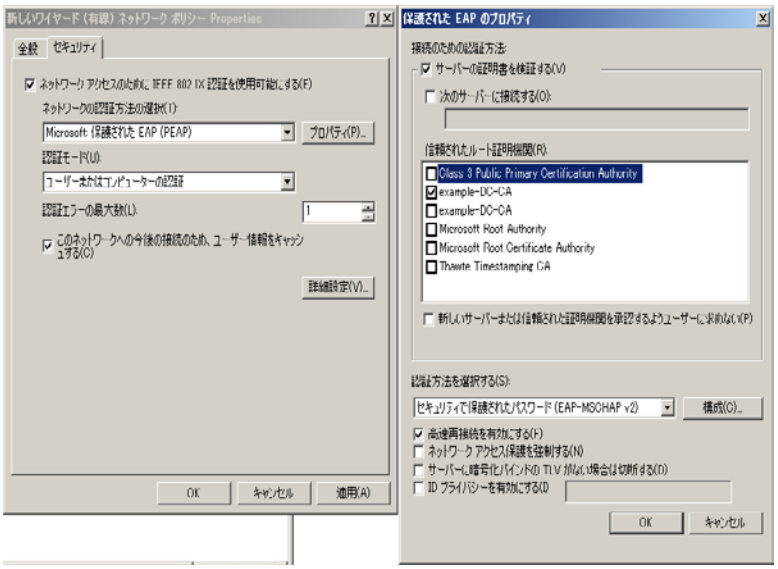


図 3.5-9 ネットワークポリシーの構成(Windows Server 2008 R2)②

Windows Server 2008 の場合

次に、「検疫のチェックを有効にする」がチェックされている事を確認する。

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）」が選択されている事を確認し、「構成」をクリックする。

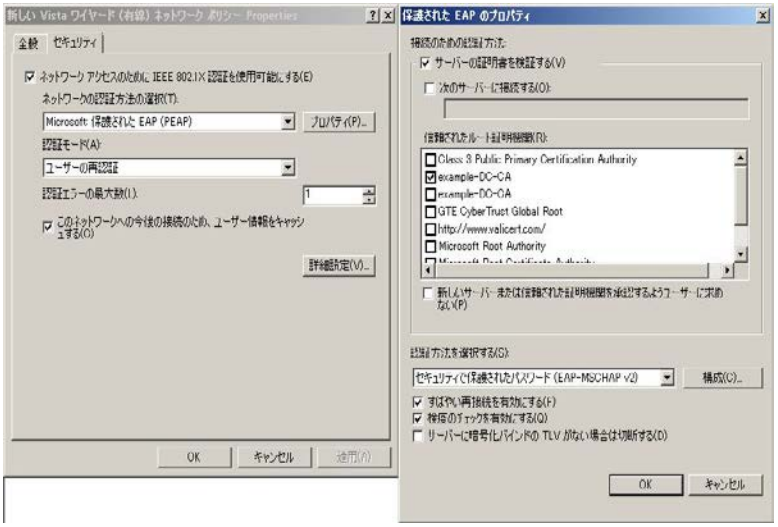


図 3.5-10 ネットワークポリシーの構成(Windows Server 2008)②

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。

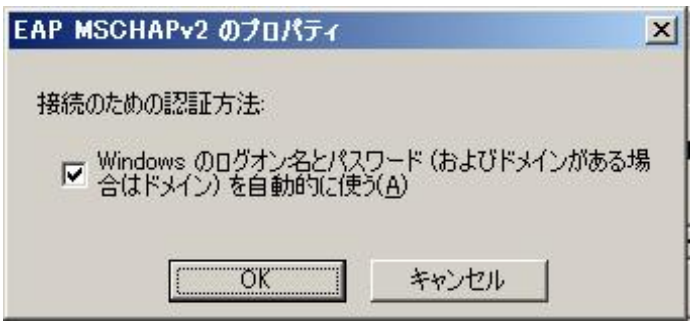


図 3.5-11 ネットワークポリシーの構成③

④ 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。

図 3.5-12 ネットワークポリシーの構成④

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 3.5-13 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」→「強制クライアント」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。

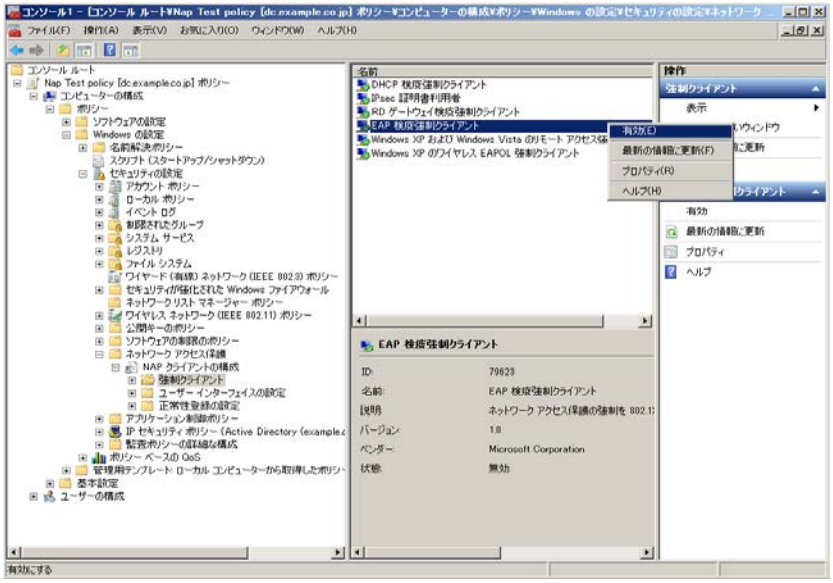


図 3.5-14 NAP クライアントの構成(Windows Server 2008 R2)①

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」→「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。

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「編集」を選択、新しく表示された「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)」画面の「有効」にチェックする。

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「プロパティ」を開き、「有効」をチェックする。

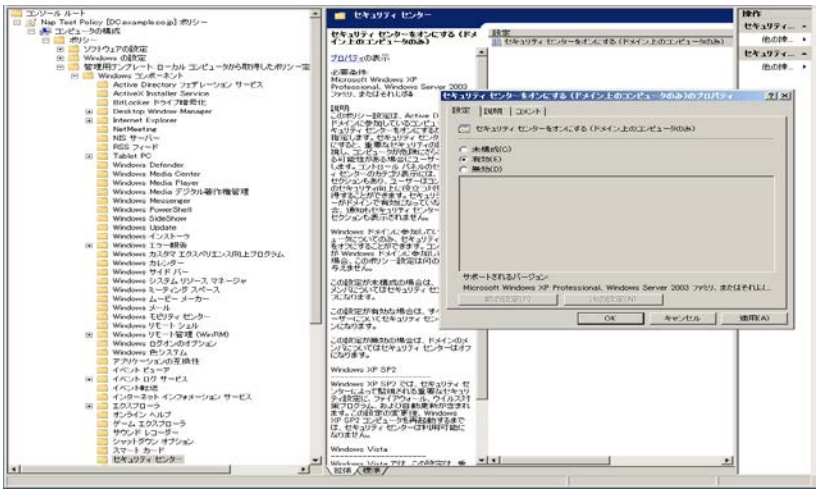


図 3.5-17 セキュリティセンターの構成(Windows Server 2008)①

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。

図 3.5-18 セキュリティセンターの構成②

（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。

② 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。

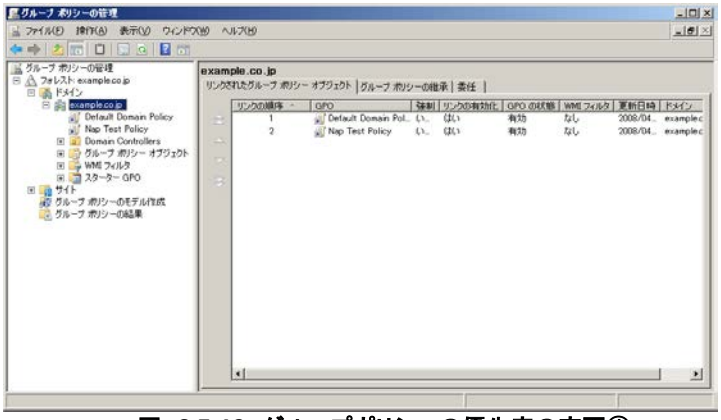


図 3.5-19 グループポリシーの優先度の変更①

③ 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。

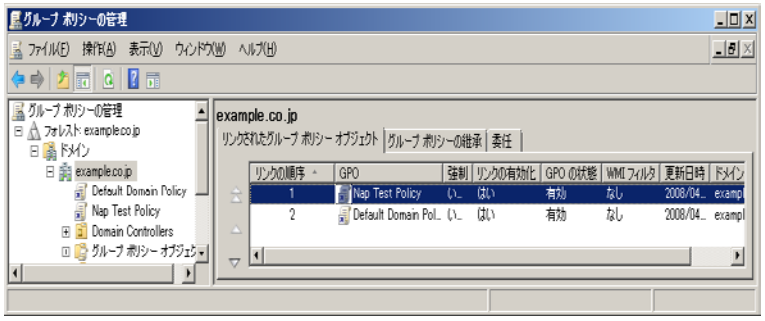


図 3.5-20 グループポリシーの優先度の変更②

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。

（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。

① 「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。

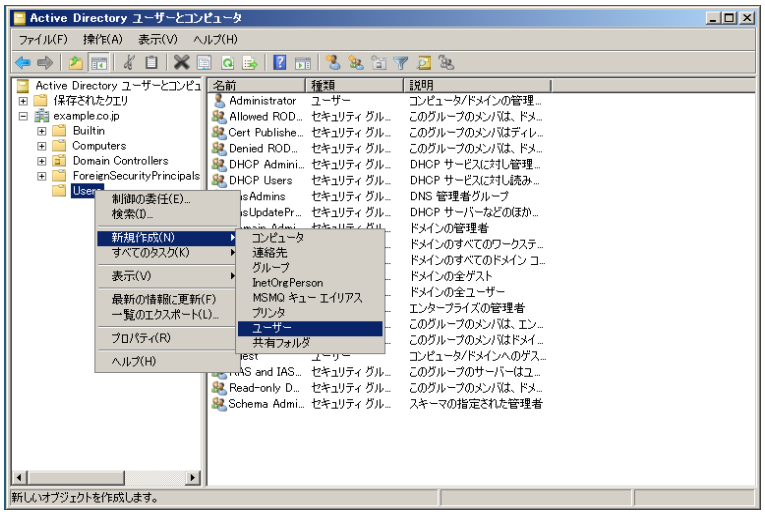


図 3.5-21 ユーザ、グループの作成①

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。

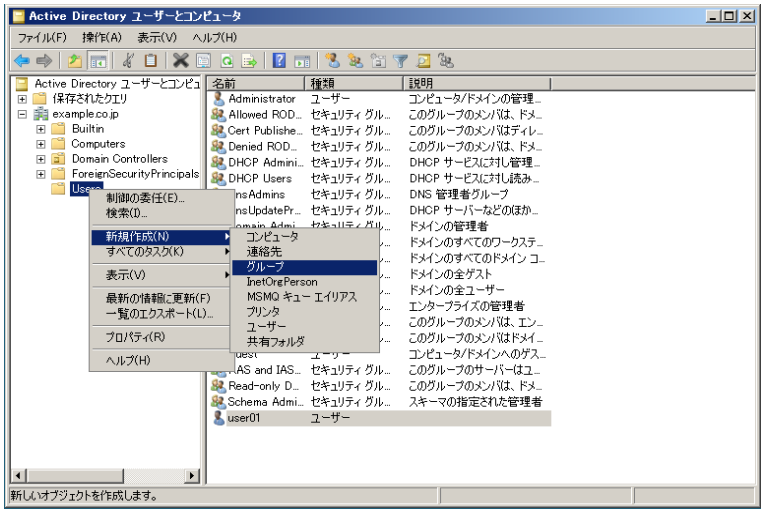


図 3.5-22 ユーザ、グループの作成②

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。

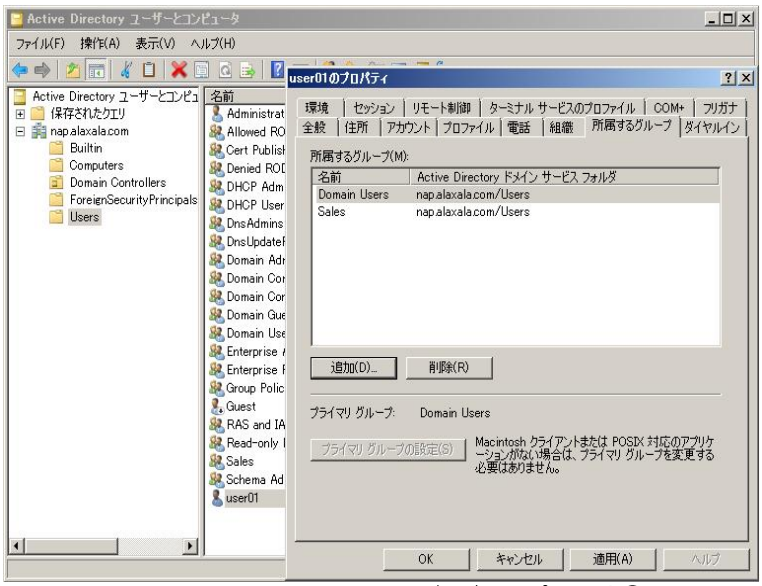


図 3.5-23 ユーザ、グループの作成③

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。

① 「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

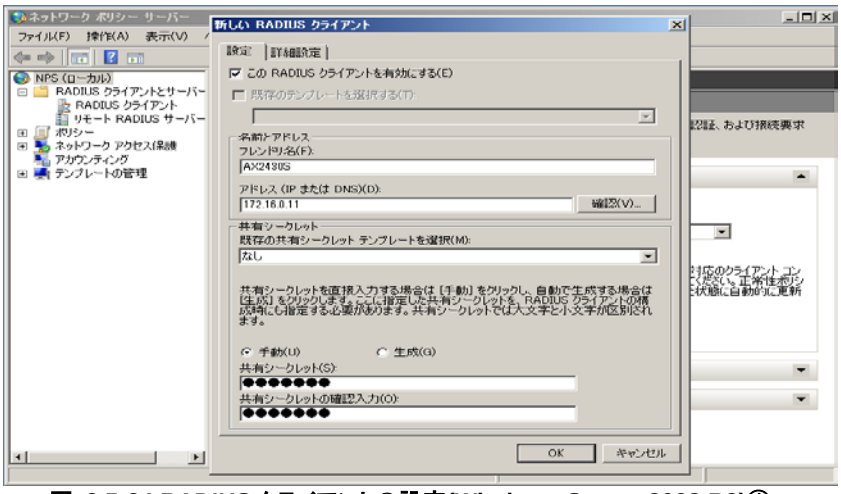


図 3.5-24 RADIUS クライアントの設定(Windows Server 2008 R2)①

・Windows Server 2008 の設定画面

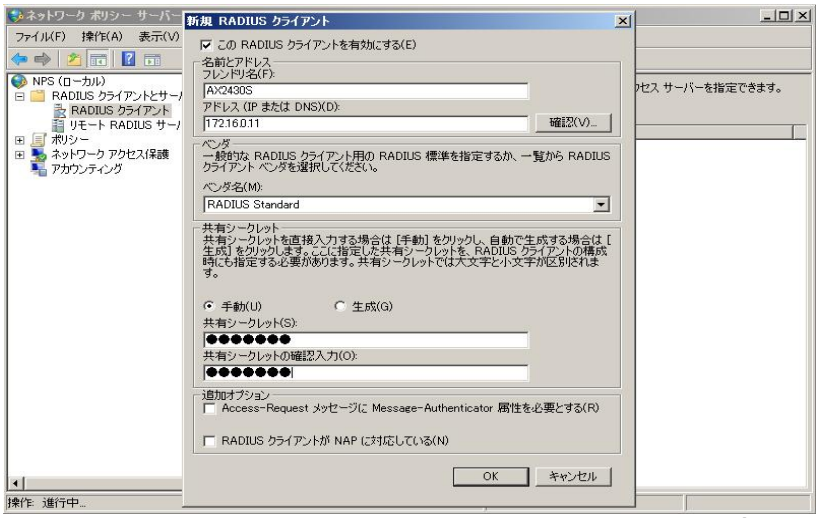


図 3.5-25 RADIUS クライアントの設定(Windows Server 2008)①

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。

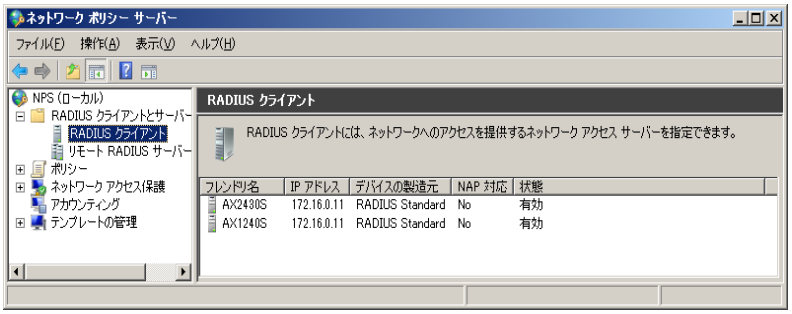


図 3.5-26 RADIUS クライアントの設定②

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。

① 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。

② 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。

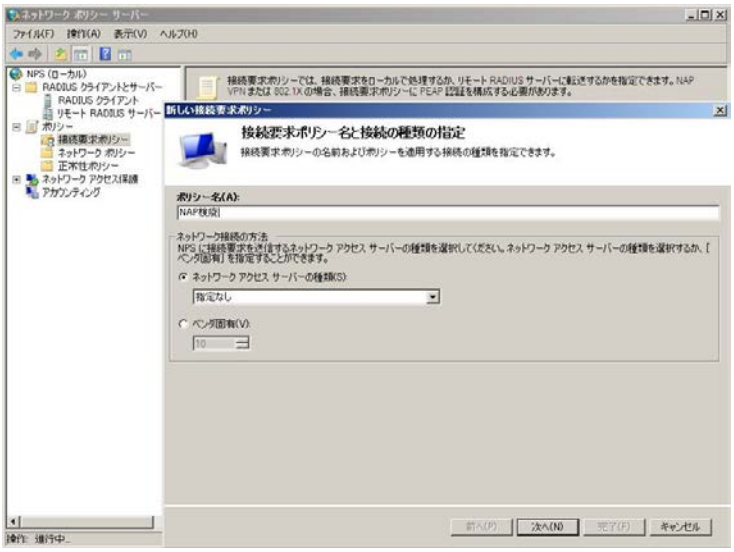


図 3.5-27 接続要求ポリシーの設定①

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。

図 3.5-28 接続要求ポリシーの設定②

④ 接続要求転送の指定

「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。

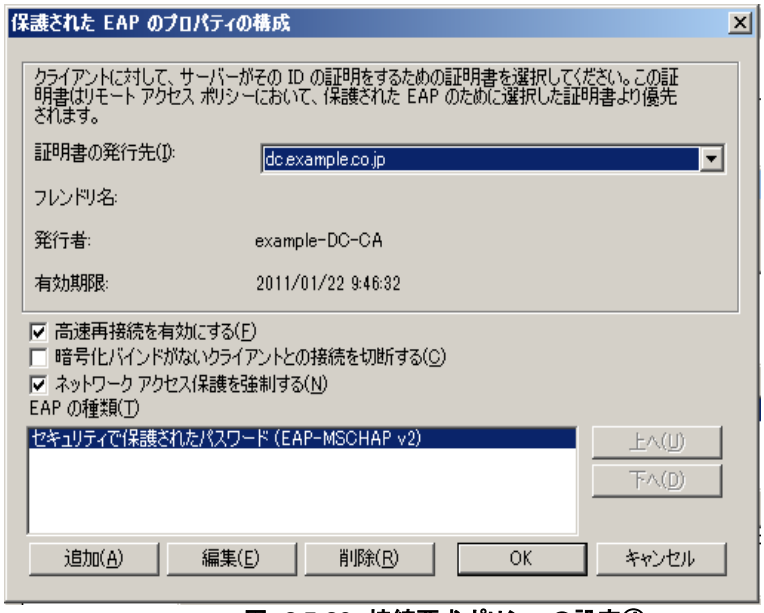


図 3.5-30 接続要求ポリシーの設定④

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。

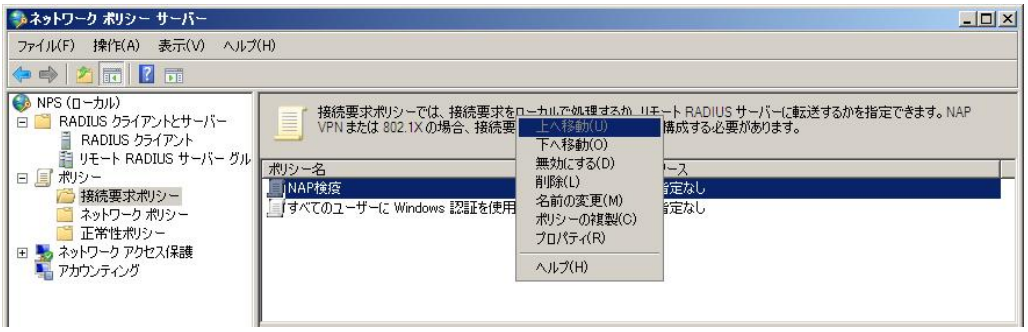


図 3.5-31 接続要求ポリシーの設定⑤

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、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。

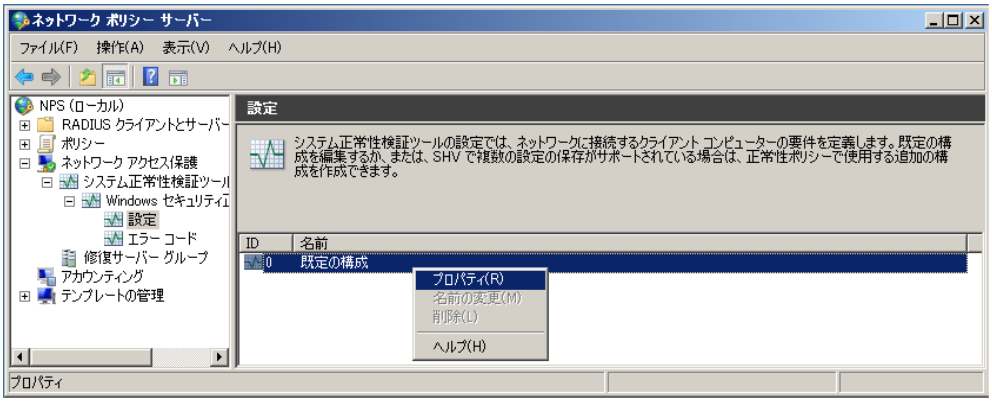


図 3.5-32 システム正常性検証ツール(SHV)の設定(Windows Server 2008 R2)①

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、右画面に現れた「Windows セキュリティ正常性検証ツール」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面にて、「構成」をクリックする。

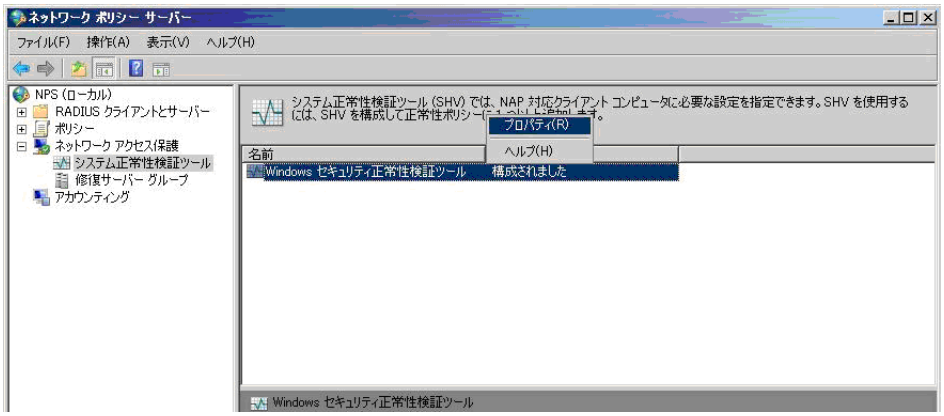


図 3.5-33 システム正常性検証ツール(SHV)の設定(Windows Server 2008)①

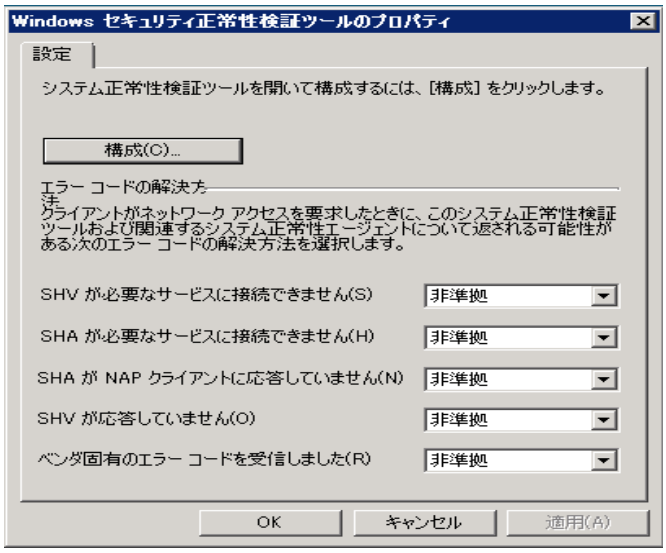


図 3.5-34 システム正常性検証ツール(SHV)の設定②

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。

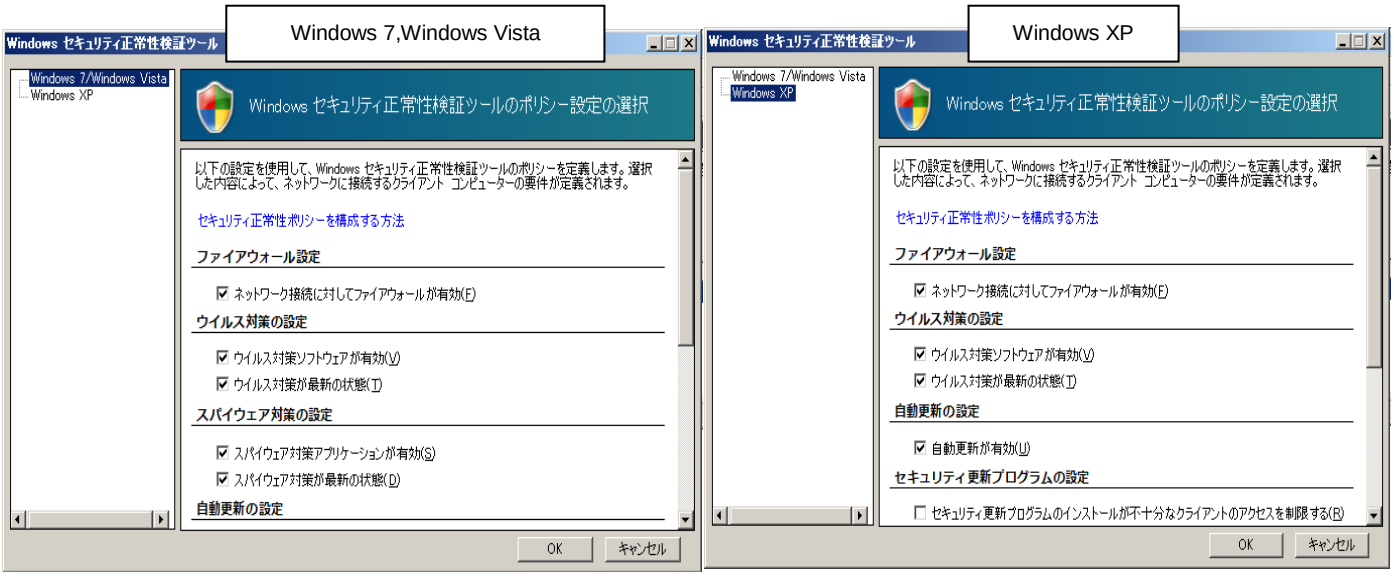


図 3.5-35 システム正常性検証ツール(SHV)の設定(Windows Server 2008 R2)③

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。

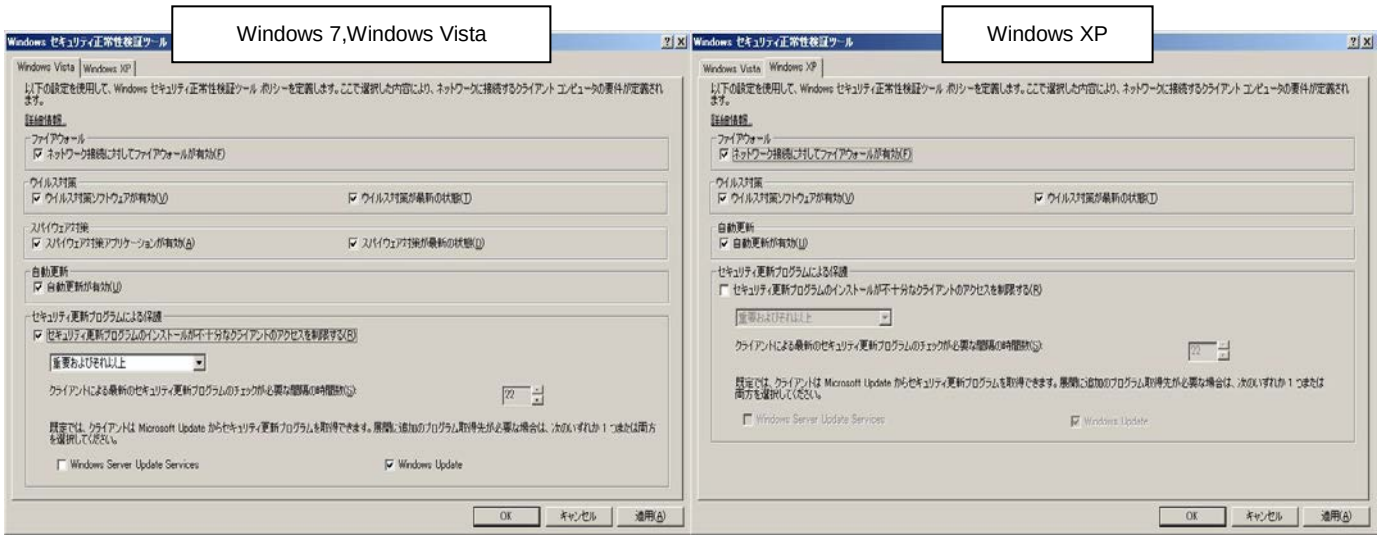


図 3.5-36 システム正常性検証ツール(SHV)の設定③

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

- **ポリシー名**：任意（本ガイドでは「OK」）
- **クライアント SHV のチェック対象**：
  すべての SHV チェックにパスしたクライアント
- **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

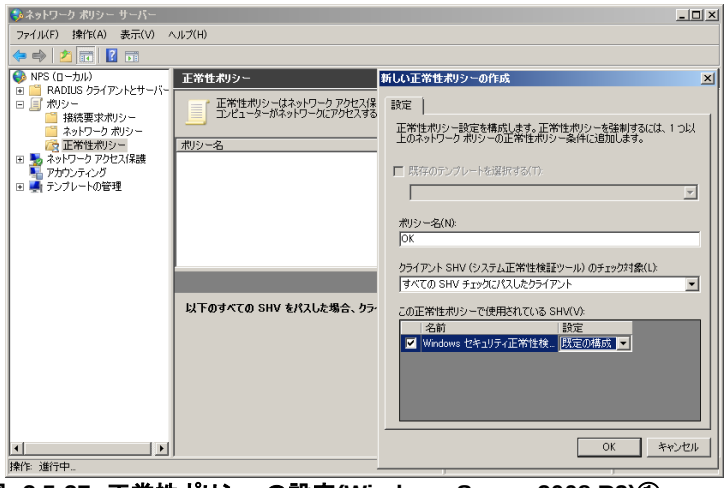


図 3.5-37 正常性ポリシーの設定(Windows Server 2008 R2)①

Windows Server 2008 の場合

・ポリシー名：任意（本ガイドでは「OK」）

・クライアント SHV のチェック対象：

すべての SHV チェックにパスしたクライアント

・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

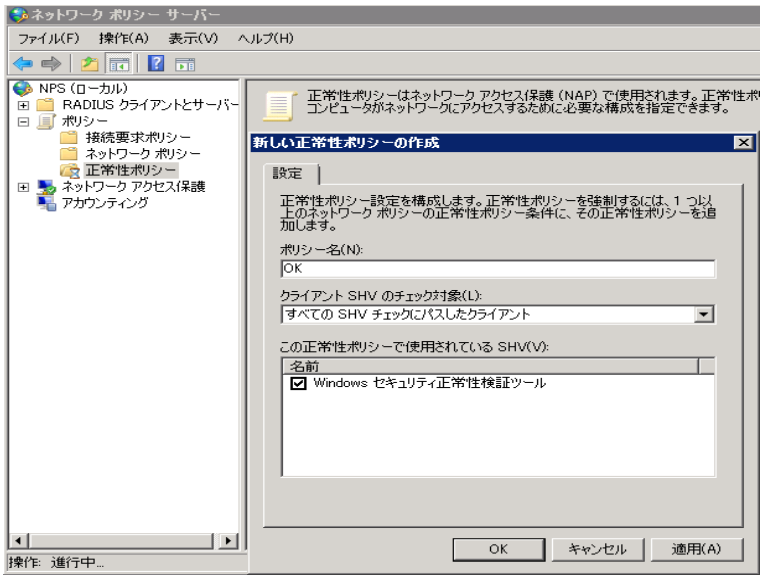


図 3.5-38 正常性ポリシーの設定(Windows Server 2008)①

② 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「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「既定の構成」を選択

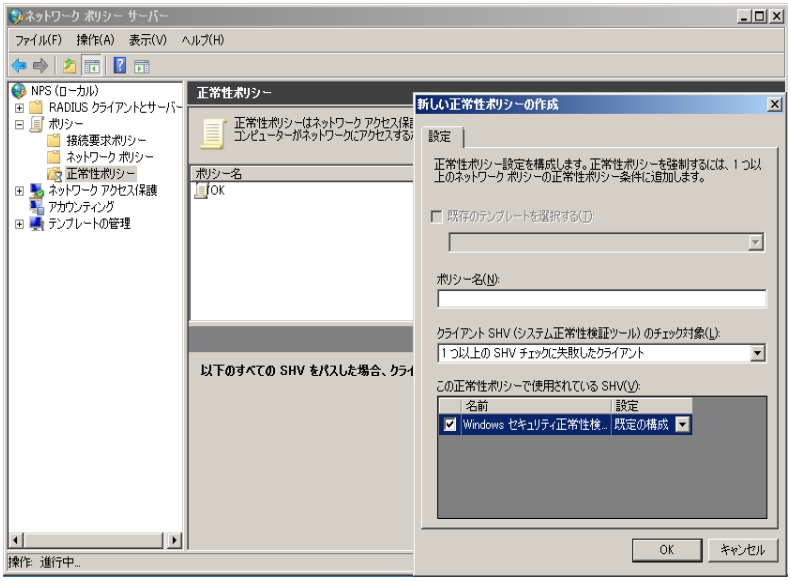


図 3.5-39 正常性ポリシーの設定(Windows Server 2008 R2)②

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

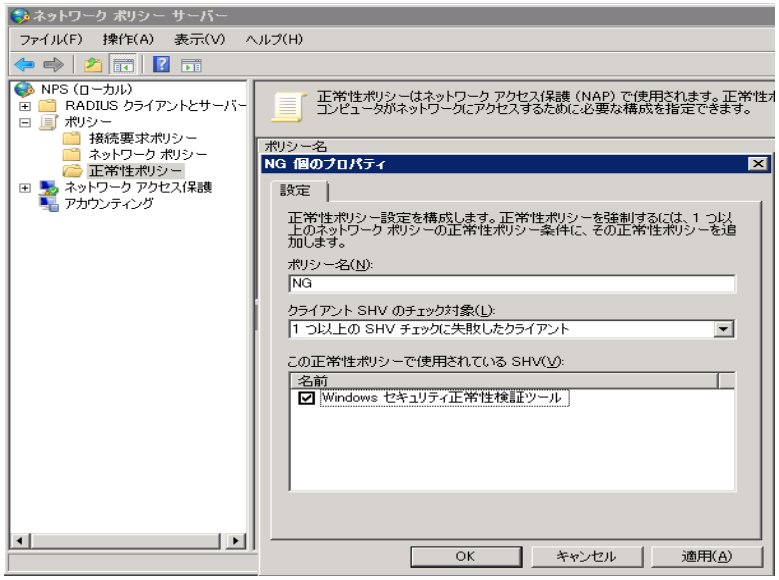


図 3.5-40 正常性ポリシーの設定(Windows Server 2008)②

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。

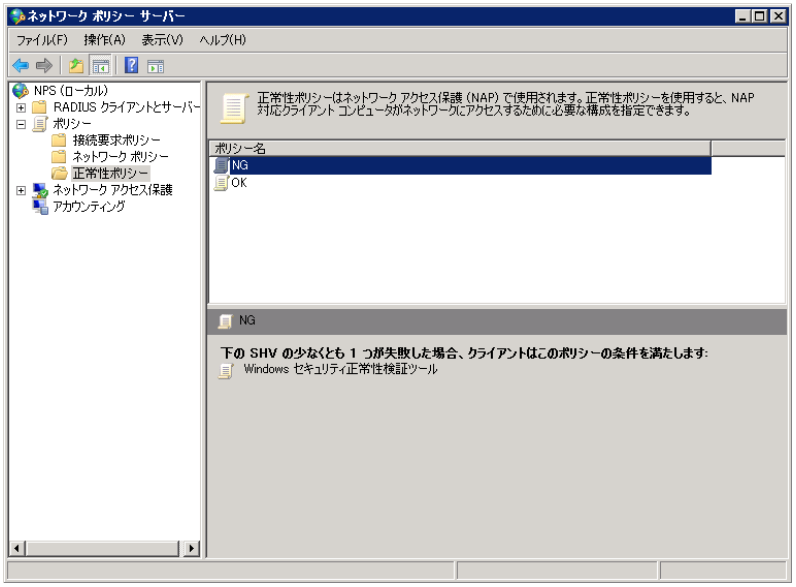


図 3.5-41 正常性ポリシーの設定③

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

① 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。

② 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「認証後 VLAN100」）を入力して「次へ」をクリックする。

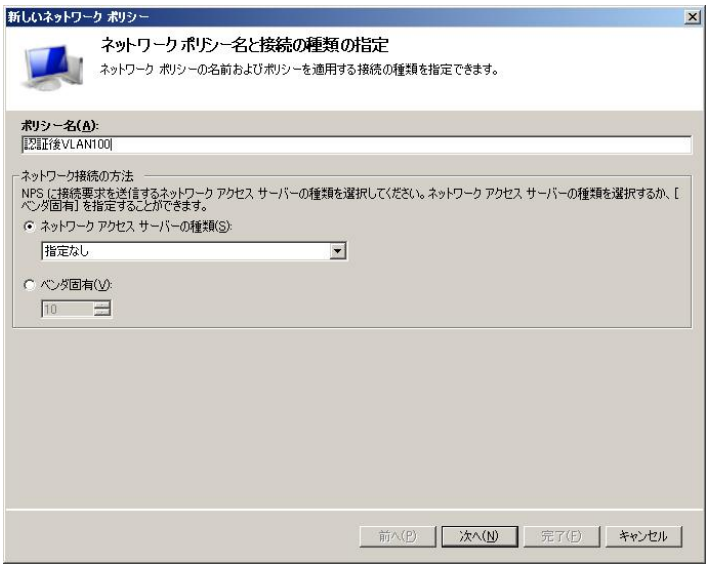


図 3.5-42 認証後 VLAN のポリシー作成①

③ 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。

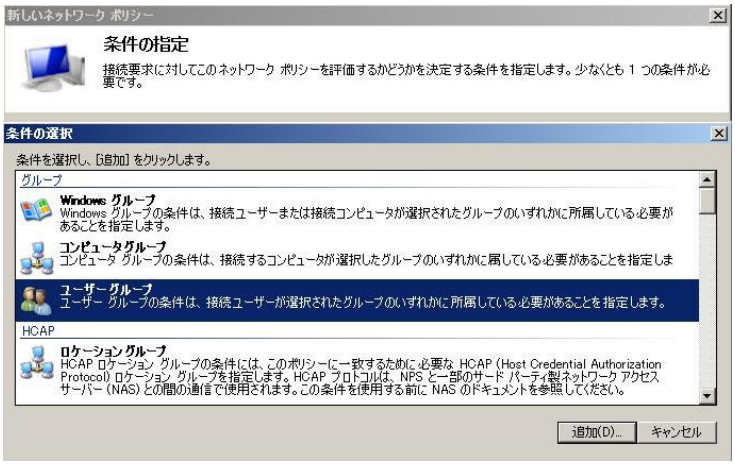


図 3.5-43 認証後 VLAN のポリシー作成②

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、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。

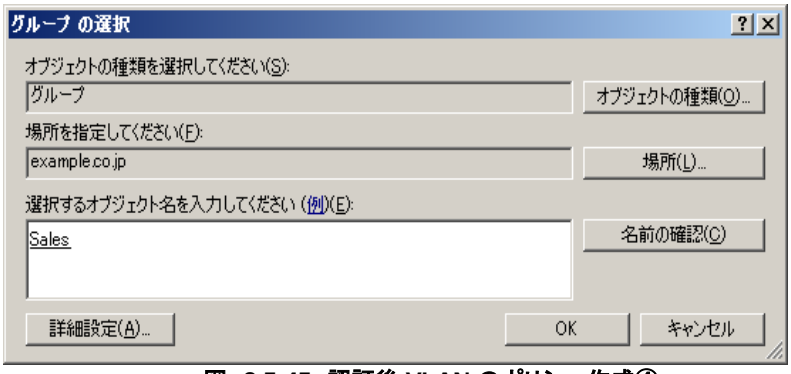


図 3.5-45 認証後 VLAN のポリシー作成④

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。最後に「次へ」をクリックして進む。

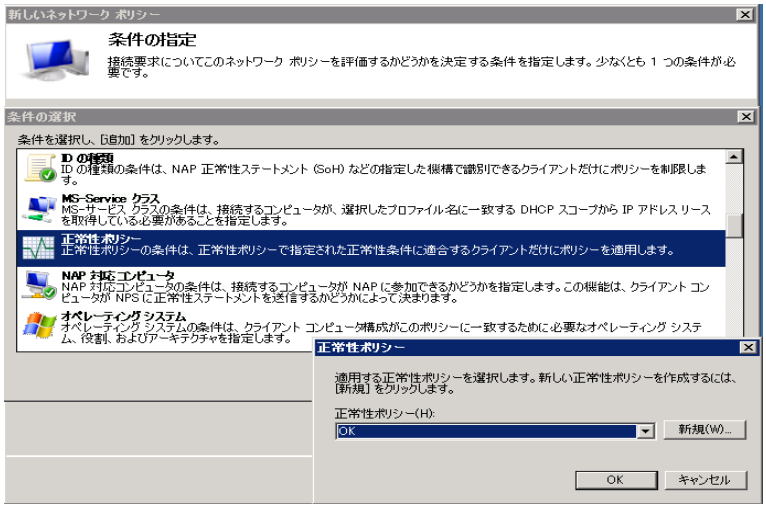


図 3.5-46 認証後 VLAN のポリシー作成⑤

⑦ アクセス許可の指定
「次へ」をクリックして進む。

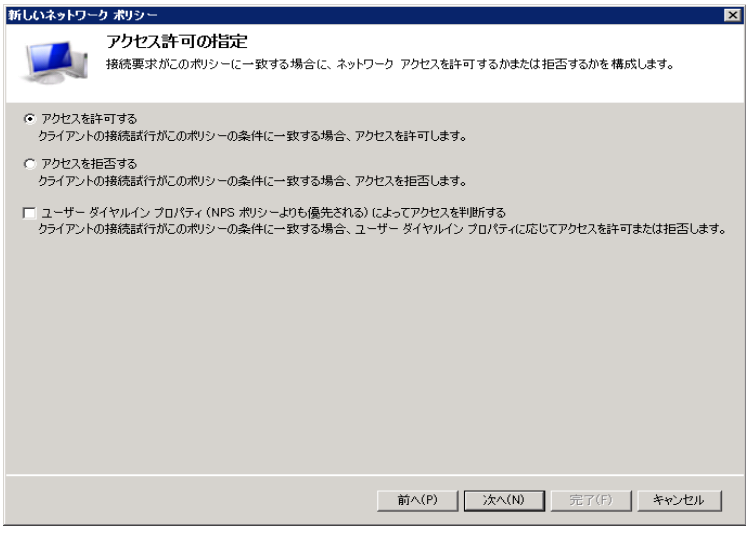


図 3.5-47 認証後 VLAN のポリシー作成⑥

⑧ 認証方法の構成

「次へ」をクリックして進む。

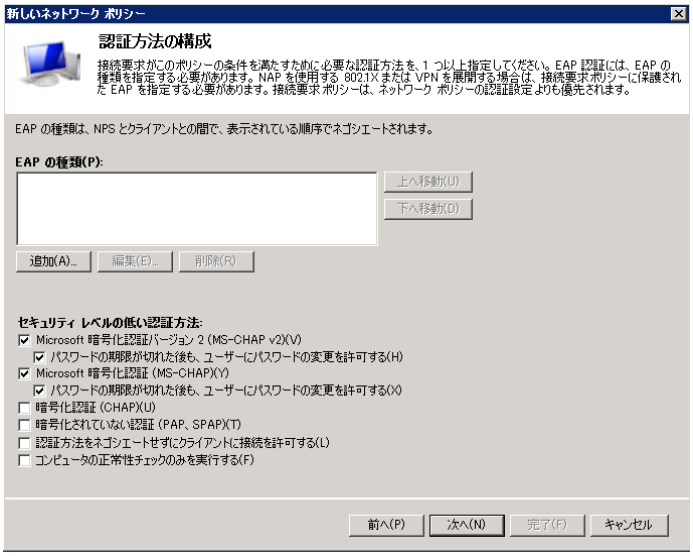


図 3.5-48 認証後 VLAN のポリシー作成⑦

⑨ 制約の構成

「次へ」をクリックして進む。

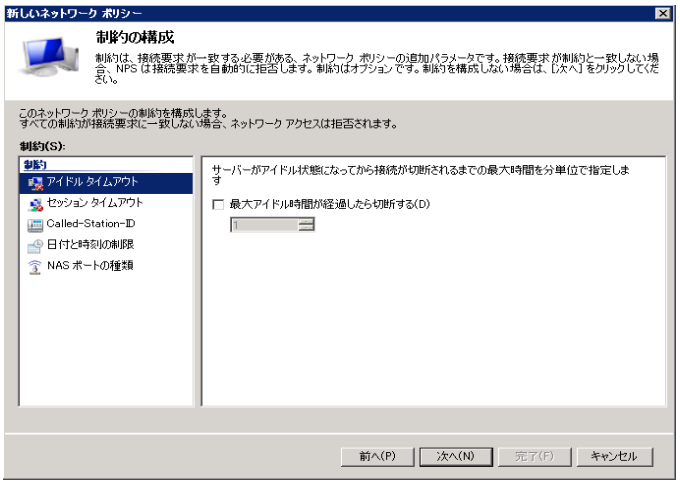


図 3.5-49 認証後 VLAN のポリシー作成⑧

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。

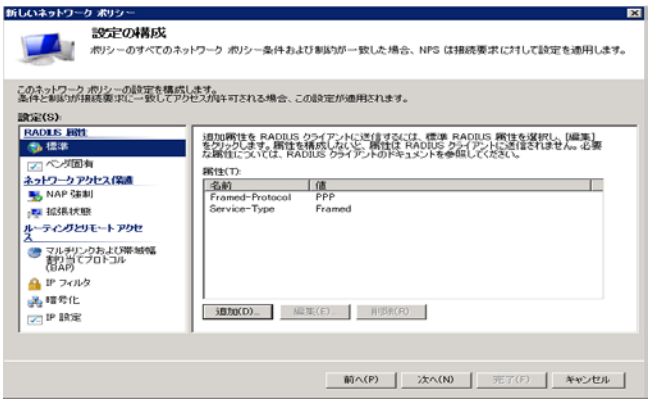


図 3.5-50 認証後 VLAN のポリシー作成⑨

⑪ 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)

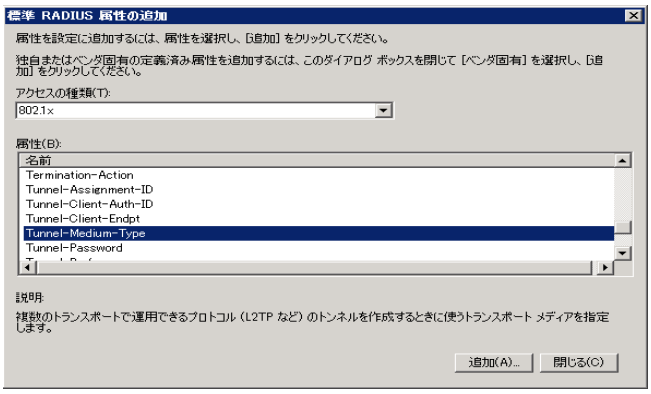


図 3.5-51 認証後 VLAN のポリシー作成⑩

⑫ 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。

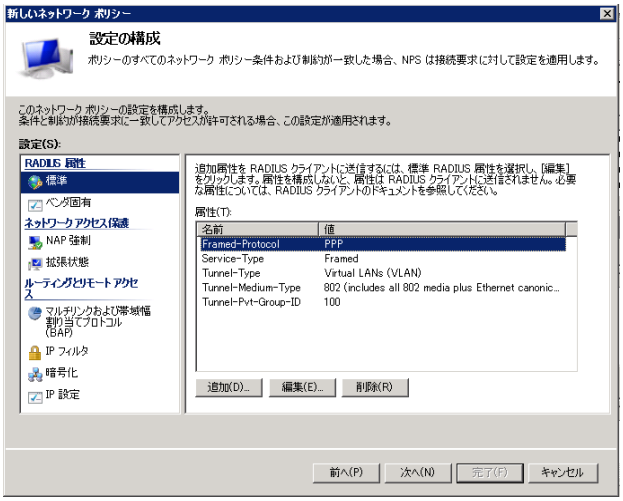


図 3.5-52 認証後 VLAN のポリシー作成⑪

⑬ 「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

① 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。

② 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。

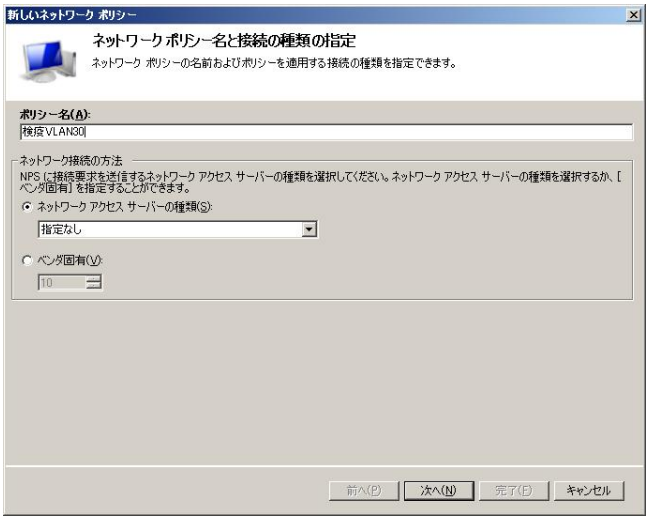


図 3.5-53 検疫 VLAN のポリシー作成①

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、3.5.7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。

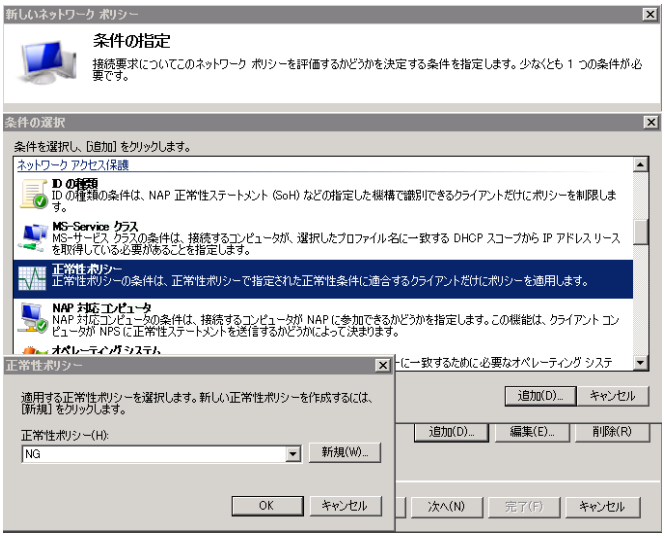


図 3.5-54 検疫 VLAN のポリシー作成②

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)

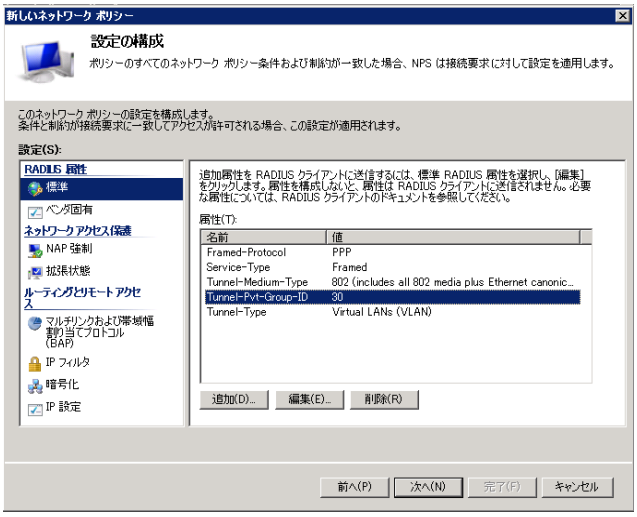


図 3.5-55 検疫 VLAN のポリシー作成③

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。

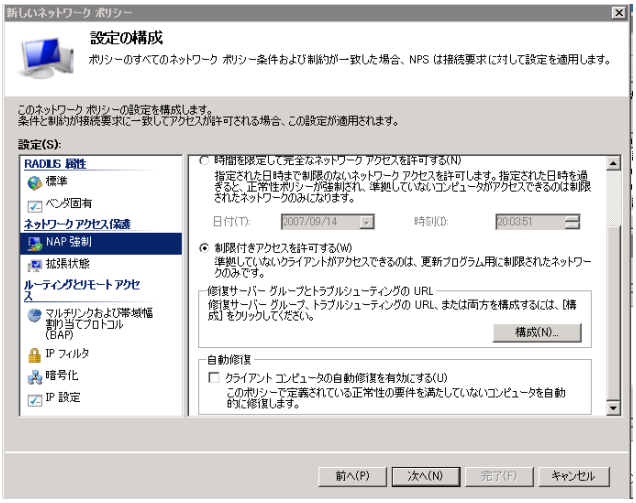


図 3.5-56 検疫 VLAN のポリシー作成④

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。

表 3-7 DHCP の設定内容

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 ゲートウェイ	192.168.100.254
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 ゲートウェイ	192.168.30.254
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 ゲートウェイ	192.168.10.254
DNS サーバ	
10.51.0.1	

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。

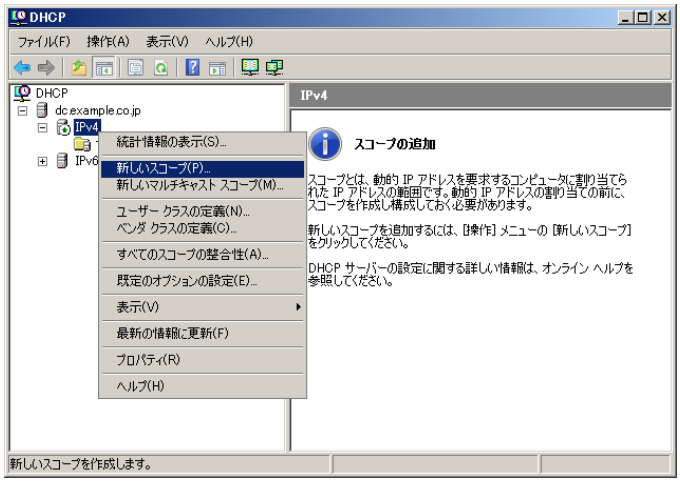


図 3.5-57 DHCP サーバの設定①

② 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。

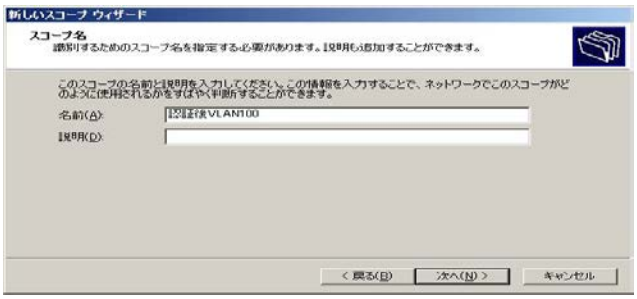


図 3.5-58 DHCP サーバの設定②

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（表 3.5-2）を入力し「次へ」をクリックする。

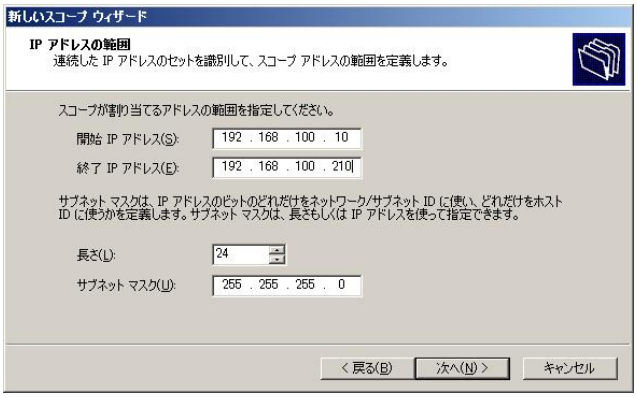


図 3.5-59 DHCP サーバの設定③

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。

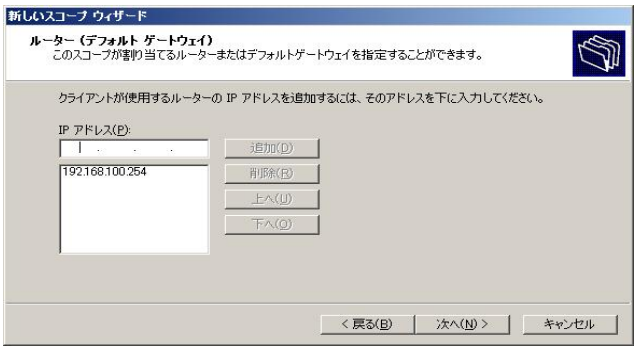


図 3.5-60 DHCP サーバの設定④

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。

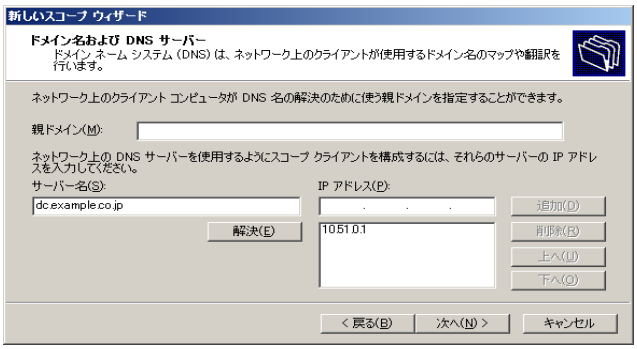


図 3.5-61 DHCP サーバの設定⑤

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。

⑪ 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。

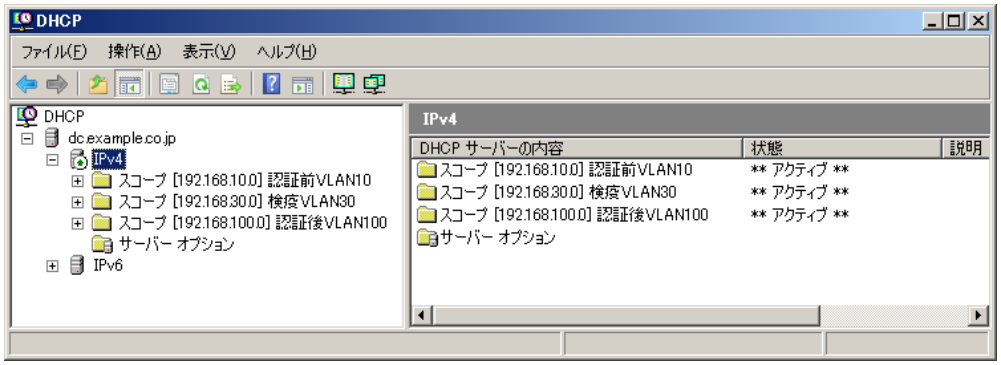


図 3.5-62 DHCP サーバの設定⑥

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。

① 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。

② 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。

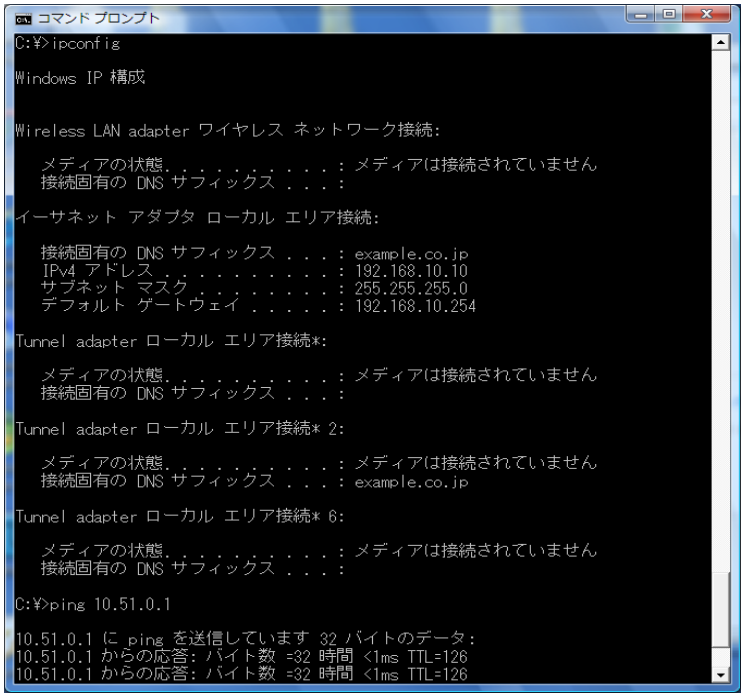


図 3.6-1 Windows ドメイン参加の設定①

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。

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。

⑤ システムのプロパティ画面にて、「変更」をクリックする。

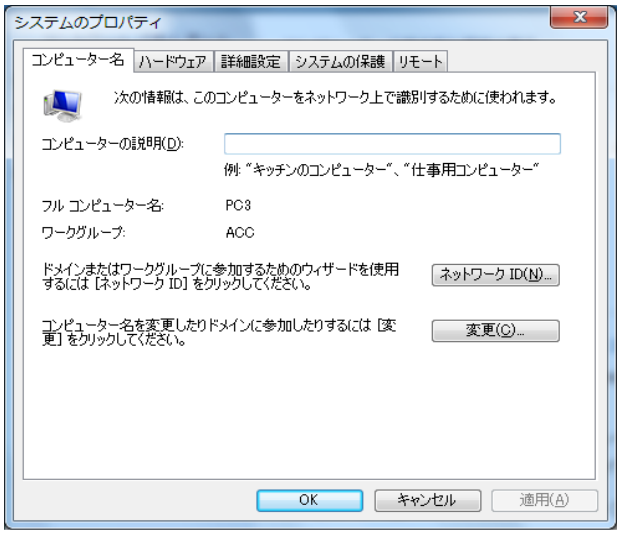


図 3.6-3 Windows ドメイン参加の設定③

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」）

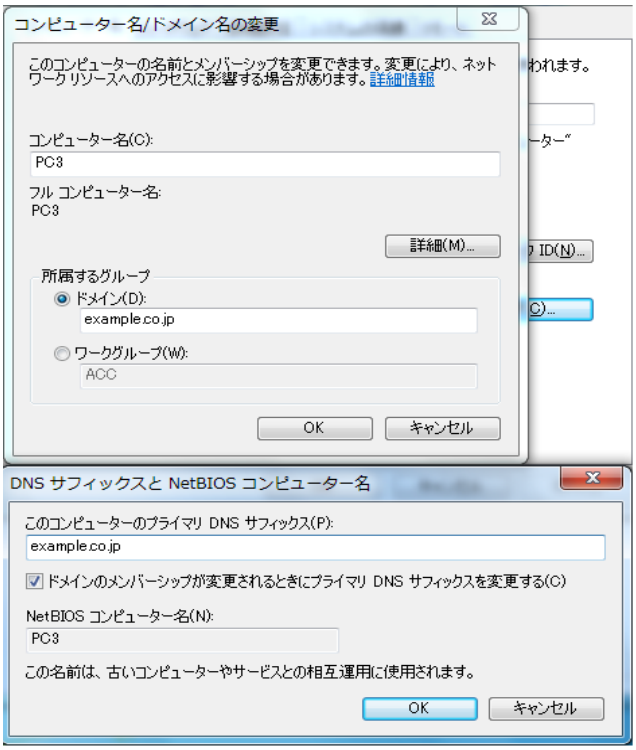


図 3.6-4 Windows ドメイン参加の設定④

⑦ 「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。
3.5.3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。

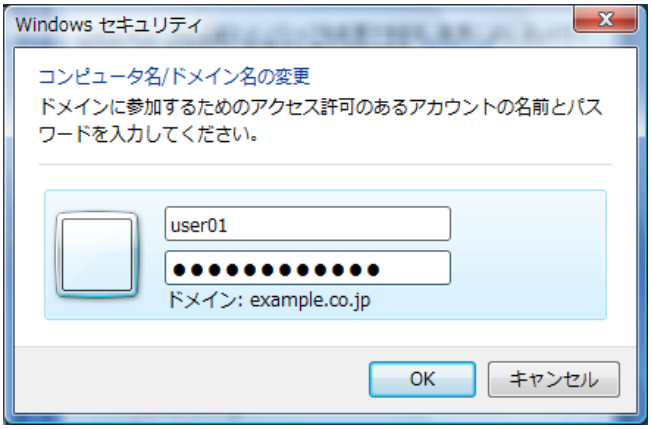


図 3.6-5 Windows ドメイン参加の設定⑤

⑧ 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。

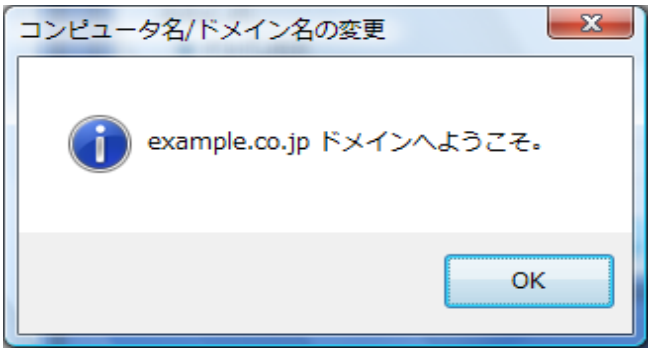


図 3.6-6 Windows ドメイン参加の設定⑥

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⑧で参加した Windows ドメイン名であることを確認し、⑦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。

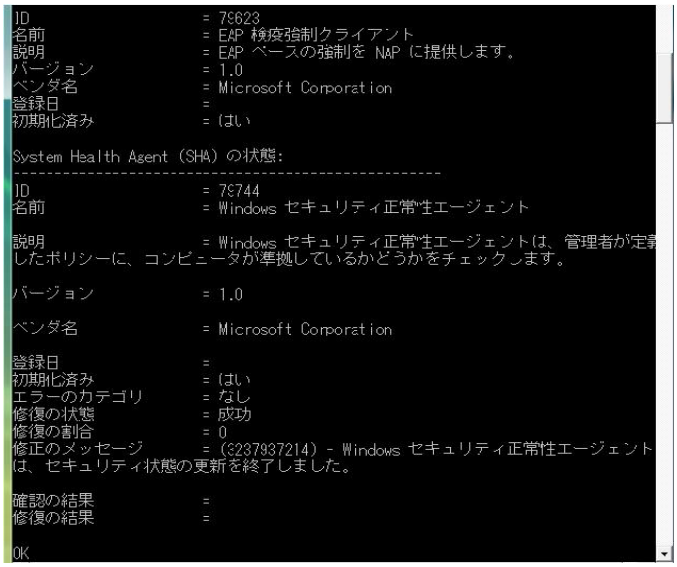


図 3.6-7 設定の確認①

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。）

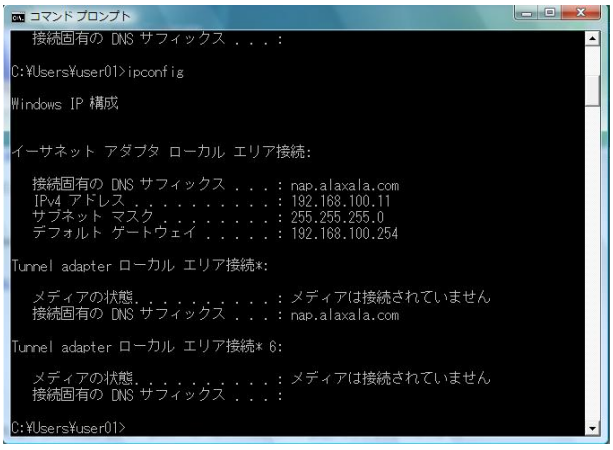


図 3.6-8 設定の確認②

IP アドレスが認証前 VLAN のまま変更しない場合は、7.3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。

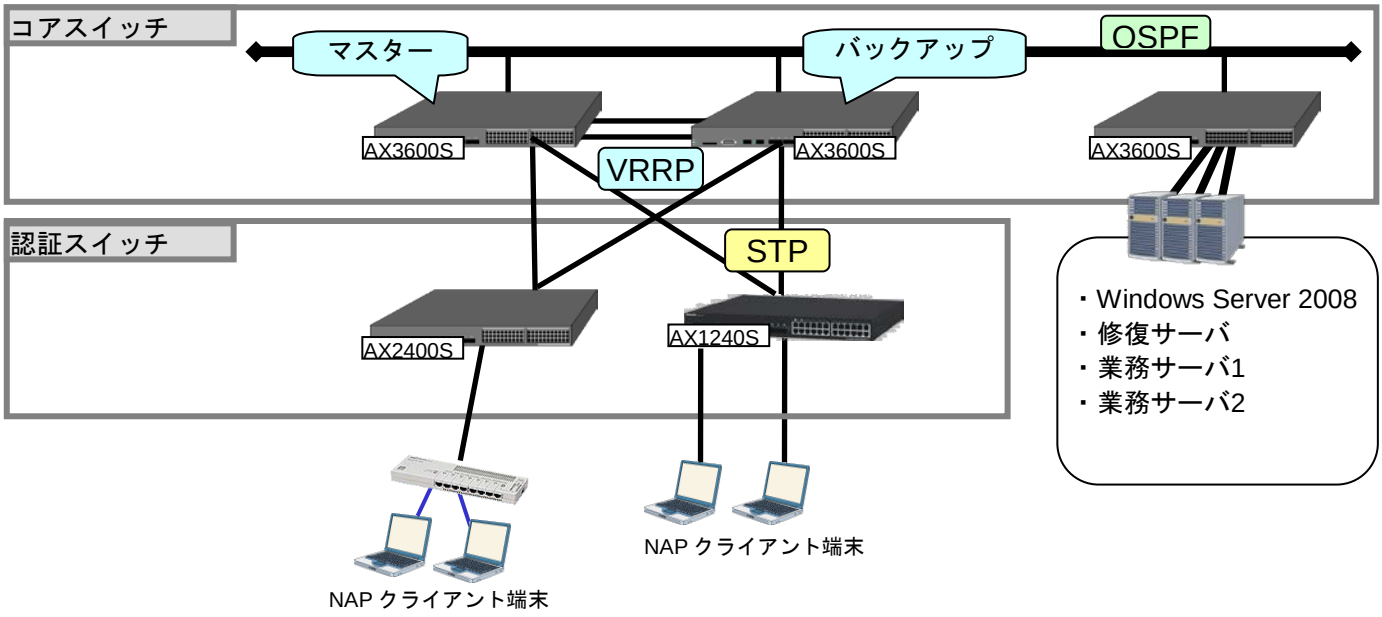


図 4.1-1 検疫ネットワークの基本構成(固定 VLAN(ポート単位)構成)

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

検疫ネットワーク構成図(固定 VLAN(ポート単位)構成)を以下に示します。

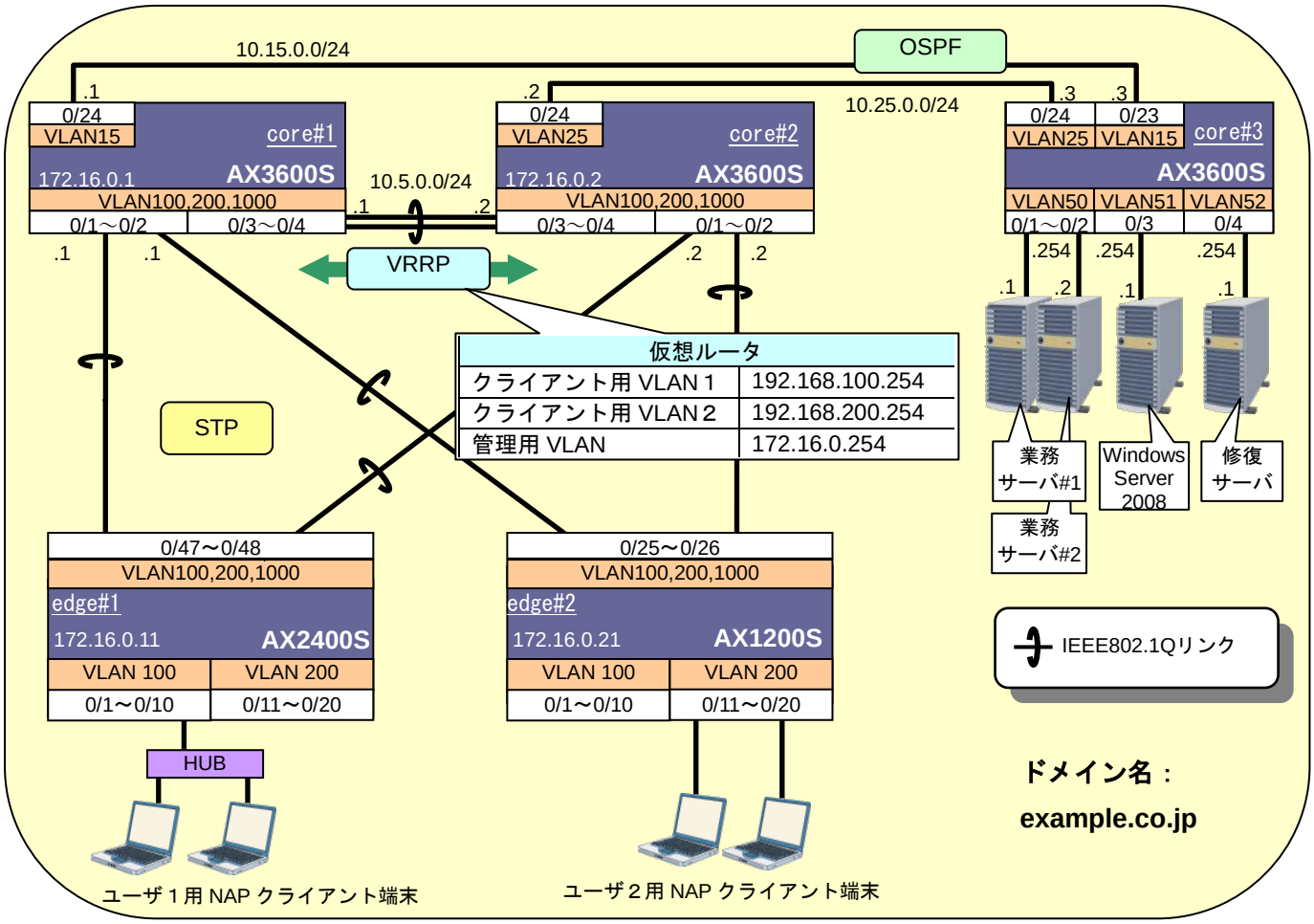


図 4.2-1 ネットワーク構成図(固定 VLAN(ポート単位)構成)

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
AX2400S	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
		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	—	—
AX1240S	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
		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。

表 4-2 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 VLAN	50	10.50.0.0/24	検疫後に通信可能なサーバが所属する VLAN。	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 VLAN１	100	192.168.100.0/24	ユーザが所属する VLAN。	ー
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。	ー

表 4-3 VLANーサーバ間通信の可否

送信元＼送信先			VLAN 100	VLAN 200	業務サーバ#1	業務サーバ#2	Windows Server 2008	修復サーバ
VLAN	100	認証失敗		×	×	×	○	○
		検疫失敗		×	×	×	○	○
		検疫成功		×	○	○	○	○
	200	認証失敗	×		×	×	○	○
		検疫失敗	×		×	×	○	○
		検疫成功	×		○	×	○	○

凡例：○ 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 ドメインへログオンするため、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	
(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	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	
(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	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。 VLAN１００、２００および１０００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	
●認証用 (config)# interface range fastethernet 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	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（1）**
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（8）**
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（4）**

（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

(config-ext-nacl)# 10 permit ip 192.168.100.0 0.0.0.255 host
10.51.0.1
(config-ext-nacl)# 20 permit ip 192.168.100.0 0.0.0.255 host
10.52.0.1
(config-ext-nacl)# 30 permit ip 192.168.200.0 0.0.0.255 host
10.51.0.1
(config-ext-nacl)# 40 permit ip 192.168.200.0 0.0.0.255 host
10.52.0.1

(config-ext-nacl)# 50 permit udp any any eq bootps
(config-ext-nacl)# 60 permit udp any any eq bootpc

(config)# interface range fastethernet 0/1-20
(config-if-range)# authentication ip access-group JoinDomain
```

認証専用 IPv4 アクセスリスト「JoinDomain」を作成します。
・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」への通信を許可します。
・VLAN200 から Windows Server 2008「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。

➢ **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）**

VLAN200 用アクセスリストの設定

```
(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

(config)# interface vlan 200
(config-if)# ip access-group VLAN200 in
```

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。

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	
(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 (config-if-range)# dot1x timeout quiet-period 5 (config-if-range)# dot1x supplicant-detection disable (config-if-range)# authentication ip access-group JoinDomain (config-if-range)# authentication arp-relay (config)# dot1x system-auth-control (config)# dot1x logging enable	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。 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）** 端末検出モードを disable にして、EAP-Request/Identity の送信を抑止します。 ➢ **構築ポイント（６）** 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。 認証前の ARP リレーを設定します。 ➢ **構築ポイント（２）** 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	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	
(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	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	
(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	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。 VLAN１００、２００および１０００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	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 (config)# interface range gigabitethernet 0/47-48 (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 0/47～0/48 に、クライアント用 VLAN100、200 と管理用 VLAN1000 を設定します。 ➢ **構築ポイント（１）**
インタフェースの設定	
(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。 ➢ **構築ポイント（４）**

（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 (config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 host 10.52.0.1 (config-ext-nacl)# permit ip 192.168.200.0 0.0.0.255 host 10.51.0.1 (config-ext-nacl)# permit ip 192.168.200.0 0.0.0.255 host 10.52.0.1 (config-ext-nacl)# permit udp any any eq bootps (config-ext-nacl)# permit udp any any eq bootpc (config)# interface range fastethernet 0/1-20 (config-if-range)# authentication ip access-group JoinDomain	認証専用 IPv4 アクセスリスト「JoinDomain」を作成します。 ・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」への通信を許可します。 ・VLAN200 から Windows Server 2008「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。 ➢ **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）**
VLAN200 用アクセスリストの設定	
(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 (config)# interface vlan 200 (config-if)# ip access-group VLAN200 in	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。 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 (config)# interface vlan 100 (config-if)# ip access-group "VRRPstop" in (config)# interface vlan 1000 (config-if)# ip access-group "VRRPstop" in	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。 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	
(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 (config-if-range)# dot1x timeout quiet-period 5 (config-if-range)# dot1x supplicant-detection disable (config-if-range)# authentication ip access-group JoinDomain (config-if-range)# authentication arp-relay (config)# dot1x system-auth-control (config)# dot1x logging enable	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。 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）** 端末検出モードを disable にして、EAP-Request/Identity の送信を抑止します。 ➢ **構築ポイント（6）** 認証用ポート 0/1～0/20 に認証専用アクセスリスト「JoinDomain」を適用します。 認証前の ARP リレーを設定します。 ➢ **構築ポイント（2）** 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	
(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	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	
(config)# spanning-tree single (config)# spanning-tree single mode rapid-stp (config)# no spanning-tree vlan 100,200,1000 (config)# spanning-tree single priority 4096	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。 VLAN１００、２００および１０００をシングルスパニングツリー対象にします。 ブリッジ優先度を設定します。
物理ポートの設定	
(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	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。
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	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	
(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	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	
(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 (config)# interface vlan 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 (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	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。 ・アクセプトモードを有効にします。 ➢ **構築ポイント（１０）**

（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 (config)# interface vlan 200 (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。

（4） OSPF の設定

AX3600S の設定	
ポート VLAN の設定	
(config)# vlan 5 (config-vlan)# name OSPF (config)# vlan 15 (config-vlan)# name OSPF	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	
(config)# interface gigabitethernet 0/24 (config-if)# switchport mode access (config-if)# switchport access vlan 15 (config-if)# spanning-tree portfast	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	
(config)# interface port-channel 1 (config-if)# switchport trunk allowed vlan add 5	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	
(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	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(3.5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

① 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。

② 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 OK」）を入力して「次へ」をクリックする。

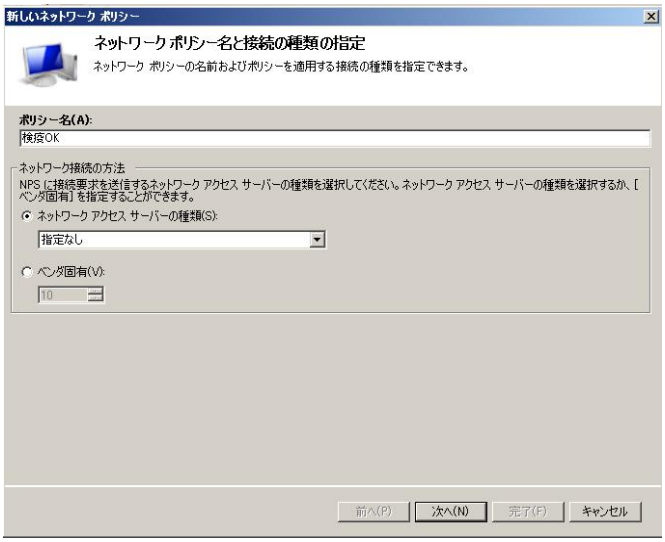


図 4.5-1 正常性ポリシーに合致した場合のポリシー作成①

③ 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。

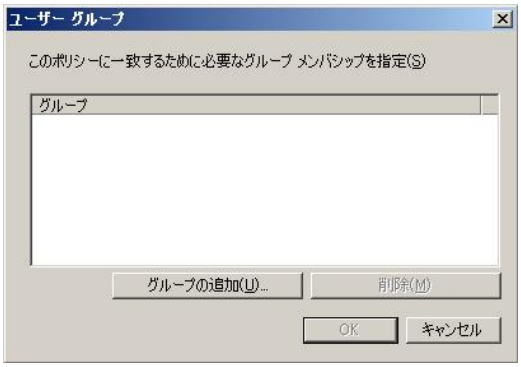


図 4.5-3 正常性ポリシーに合致した場合のポリシー作成③

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。

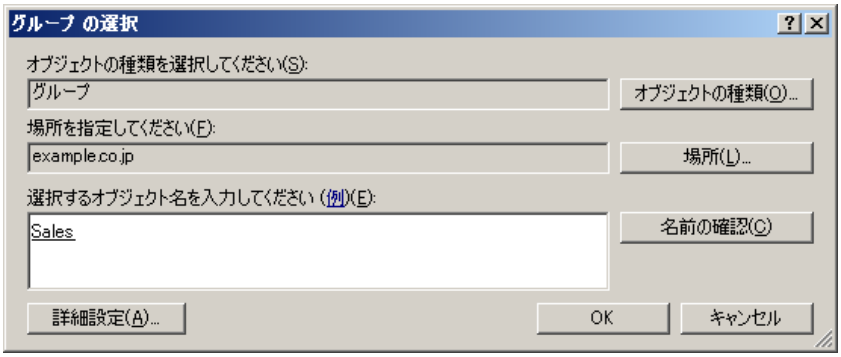


図 4.5-4 正常性ポリシーに合致した場合のポリシー作成④

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。最後に「次へ」をクリックして進む。

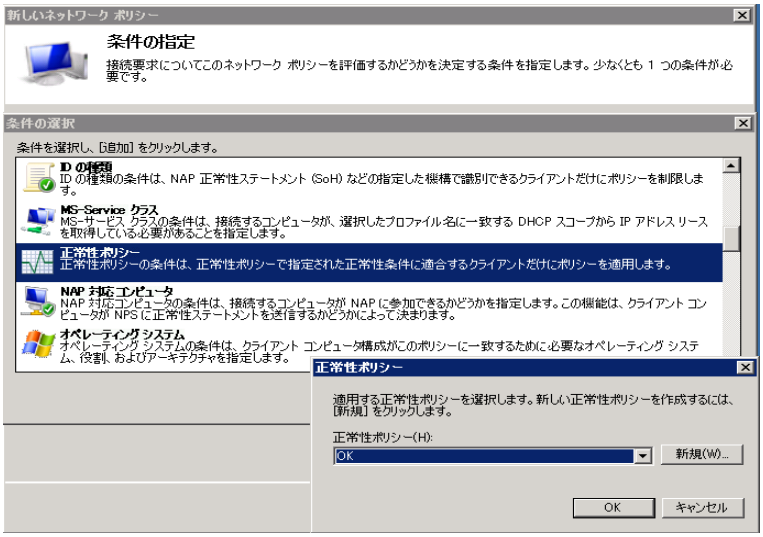


図 4.5-5 正常性ポリシーに合致した場合のポリシー作成⑤

⑦ アクセス許可の指定

「次へ」をクリックして進む。

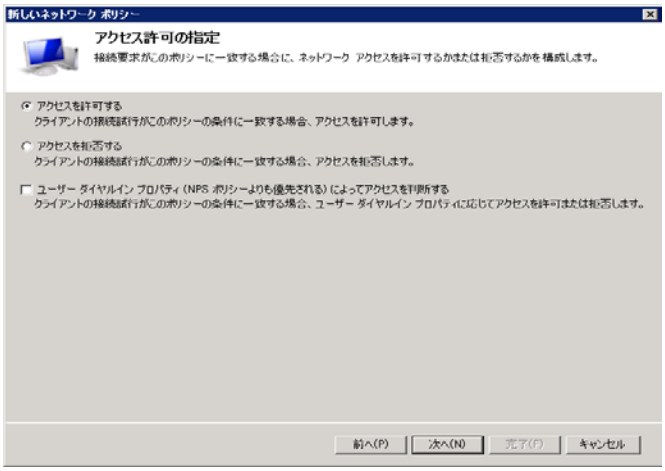


図 4.5-6 正常性ポリシーに合致した場合のポリシー作成⑥

⑧ 認証方法の構成

「次へ」をクリックして進む。

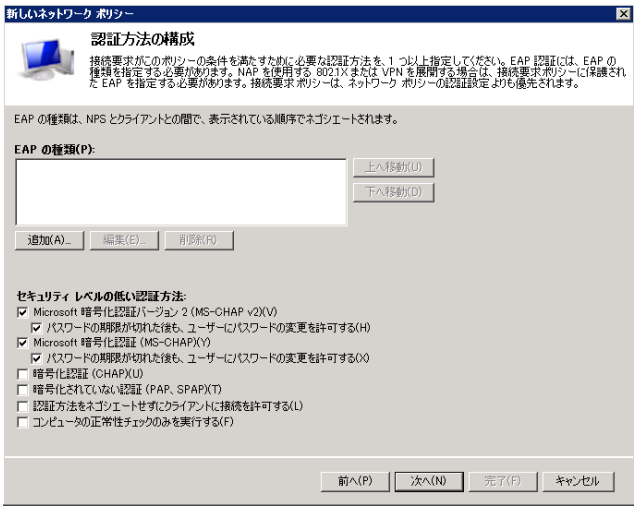


図 4.5-7 正常性ポリシーに合致した場合のポリシー作成⑦

⑨ 制約の構成

「次へ」をクリックして進む。

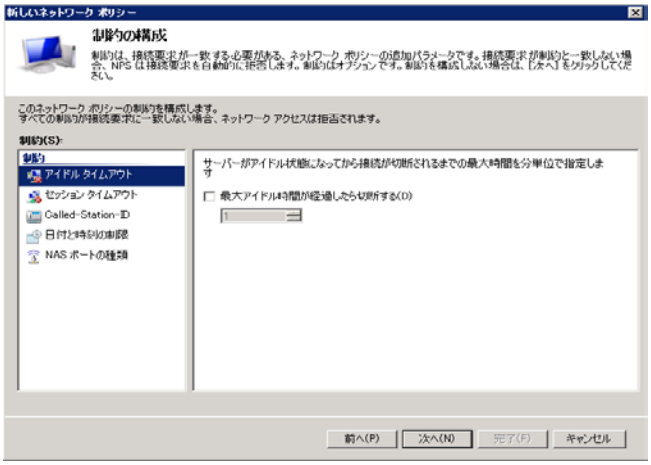


図 4.5-8 正常性ポリシーに合致した場合のポリシー作成⑧

⑩ 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。

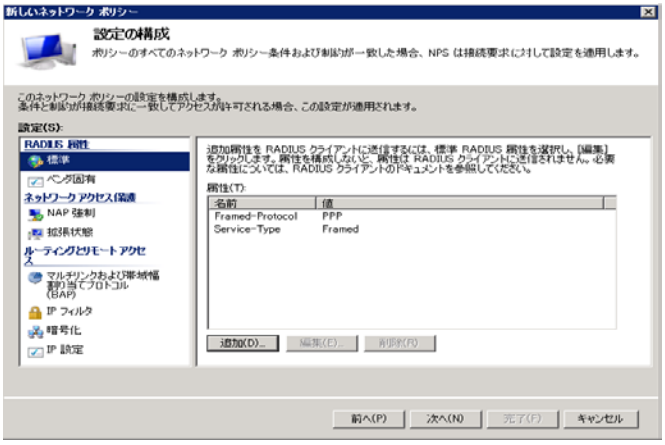


図 4.5-9 正常性ポリシーに合致した場合のポリシー作成⑨

⑪ 「完了」をクリックして画面を閉じる。

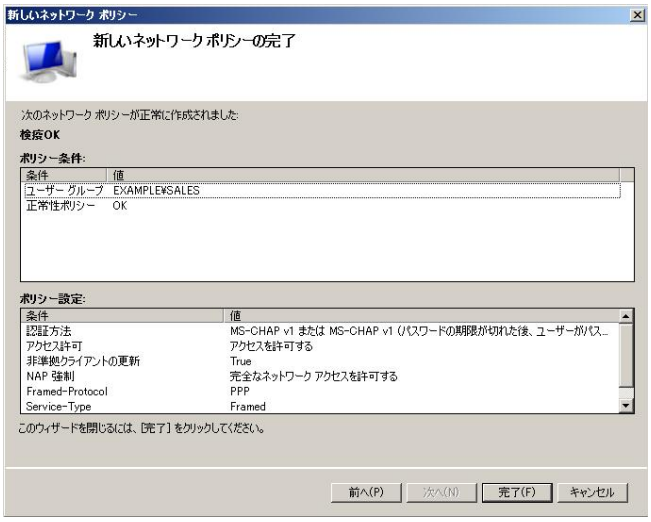


図 4.5-10 正常性ポリシーに合致した場合のポリシー作成⑩

（２） 正常性ポリシー違反のポリシー作成

① 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。

② 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。

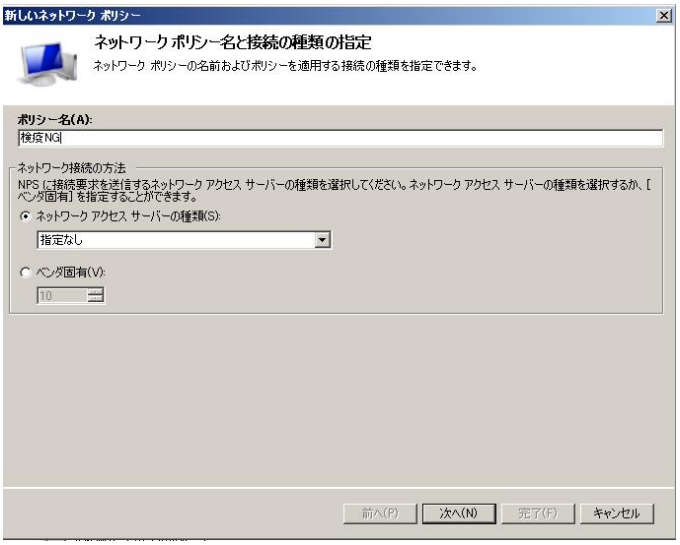


図 4.5-11 正常性ポリシー違反のポリシー作成①

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、3.5.7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。

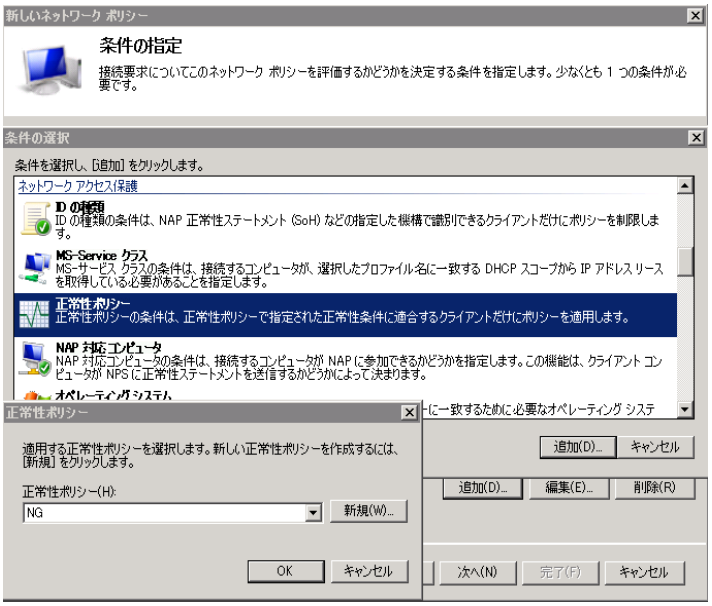


図 4.5-12 正常性ポリシー違反のポリシー作成②

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)

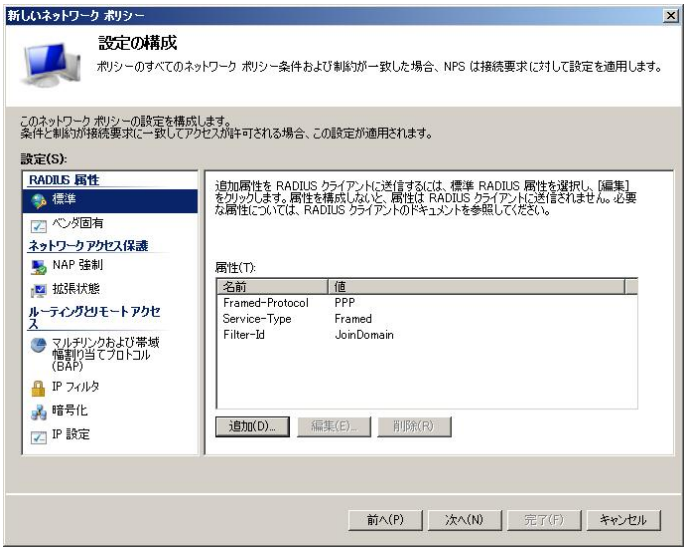


図 4.5-13 正常性ポリシー違反のポリシー作成③

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。

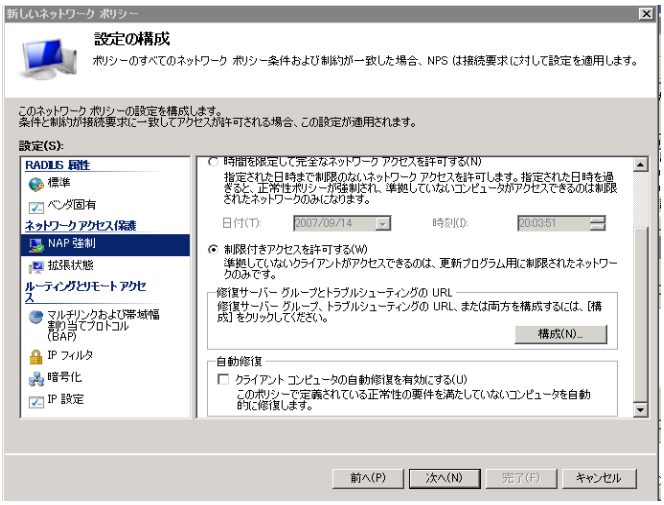


図 4.5-14 正常性ポリシー違反のポリシー作成④

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。

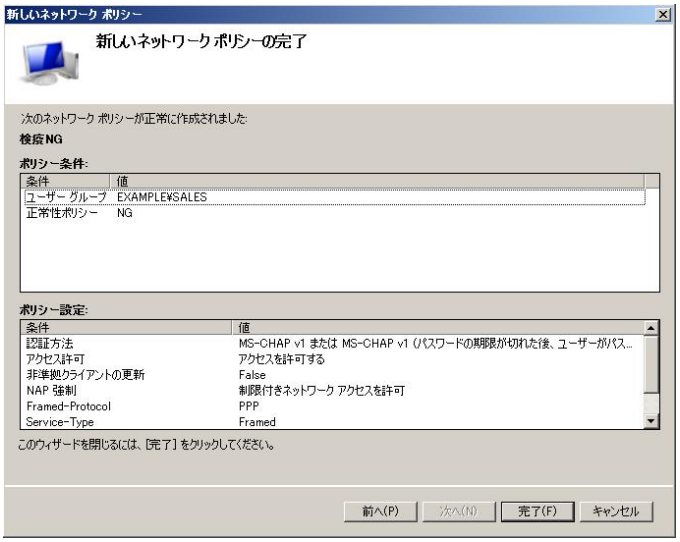


図 4.5-15 正常性ポリシー違反のポリシー作成⑤

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 dot1x port 0/3 detail

Date 2010/01/30 14:00:07 JST
Port 0/3 (Dynamic)
AccessControl   : Multiple-Auth             PortControl    : Auto
Status          : ---                       Last EAPOL     : 0019.b97d.46c7
Supplicants     : 1 / 1 / 64                ReAuthMode     : Enable
TxTimer         : 30                        ReAuthTimer    : 300
ReAuthSuccess   : 1                         ReAuthFail     : 0
SuppDetection   : Auto
VLAN(s): 10,30,100

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 100]          Port(Dynamic) Supplicants : 1
 0019.b97d.46c7      Authorized     Authenticated  Idle           1
                     113            2009/06/22 13:58:14

edge#1# show mac-address-table

Date 2010/01/30 14:00:46 JST
Aging time : 300
MAC address        VLAN    Type     Port-list
0000.5e00.010a       10    Dynamic  0/26
0019.b97d.46c7       10    Dynamic  0/3
0000.5e00.011e       30    Dynamic  0/26
0000.5e00.0164      100    Dynamic  0/26
0012.e228.f5fe      100    Dynamic  0/26
0012.e238.2a68      100    Dynamic  0/26
0019.b97d.46c7      100    Dot1x    0/3
0000.5e00.0101     1000    Dynamic  0/26
0012.e228.cd62     1000    Dynamic  0/26
0012.e228.f5fe     1000    Dynamic  0/26
0012.e238.2a68     1000    Dynamic  0/26
```

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 0/3
AccessControl   : Multiple-Auth             PortControl     : Auto
Status          : ---                       Last EAPOL      : 0019.b97d.46c7
Supplicants     : 1 / 1 / 64                ReAuthMode      : Enable
TxTimer         : 30                        ReAuthTimer     : 300
ReAuthSuccess   : 1                         ReAuthFail      : 0
SuppDetection   : Auto
VLAN(s): 100

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                     SubState
 [VLAN 100]          Port(Static)   Supplicants : 1
 0019.b97d.46c7      Authorized     Authenticated  Idle            1
                     101            2010/01/30 16:09:59          Full
```

フルアクセス許可

図 5.1-2 AX1240S の状態表示例(固定 VLAN)検疫 OK

```
edge#1# show dot1x port 0/3 detail

Date 2010/01/30 16:10:24 JST
Port 0/3
AccessControl   : Multiple-Auth             PortControl     : Auto
Status          : ---                       Last EAPOL      : 0019.b97d.46c7
Supplicants     : 1 / 1 / 64                ReAuthMode      : Enable
TxTimer         : 30                        ReAuthTimer     : 300
ReAuthSuccess   : 0                         ReAuthFail      : 0
SuppDetection   : Auto
VLAN(s): 100

 Supplicants MAC  F  Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time                     SubState
 [VLAN 100]          Port(Static)   Supplicants : 1
 0019.b97d.46c7      Authorized     Authenticated  Idle            0
                     26             2010/01/30 16:09:59          Protection
```

制限つき

アクセス許可

図 5.1-3 AX1240S の状態表示例(固定 VLAN)検疫 NG

```
dist#1# show dot1x vlan dynamic detail
Date 2010/01/30 14:02:39 JST
VLAN(Dynamic)
AccessControl   : Multiple-Auth             PortControl     : Auto
Status          : ---                       Last EAPOL      : 0019.b97d.46c7
Supplicants     : 1 / 1 / 256               ReAuthMode      : Enable
TxTimer(s)      : ---   / 30                ReAuthTimer(s): 269   / 300
ReAuthSuccess   : 0                         ReAuthFail      : 0
SuppDetection   : Auto
VLAN(s): 30,100

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 100]          VLAN(Dynamic)  Supplicants : 1
 0019.b97d.46c7      Authorized     Authenticated  Idle            0
                     33             2010/01/30 14:02:07
dist#1#
```

図 5.1-4 AX2400S/AX3600S の状態表示例(動的 VLAN)

```
dist#1# show dot1x port 0/5 detail
Date 2010/01/30 16:06:22 JST
Port  0/5
AccessControl  : Multiple-Auth             PortControl    : Auto
Status         : ---                       Last EAPOL     : 0019.b97d.46c7
Supplicants    : 1 / 1 / 64                ReAuthMode     : Enable
TxTimer(s)     : ---   / 30                ReAuthTimer(s): 178   / 300
ReAuthSuccess  : 3                         ReAuthFail     : 0
SuppDetection  : Auto

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 0019.b97d.46c7      Authorized     Authenticated  Idle           0
                     122            2010/01/30 16:04:19
dist#1#
```

フルアクセス許可

[Supplicant の MAC アドレスの前に＊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

```
dist#1# show dot1x port 0/5 detail
Date 2010/01/30 16:08:33 JST
Port  0/5
AccessControl  : Multiple-Auth             PortControl    : Auto
Status         : ---                       Last EAPOL     : 0019.b97d.46c7
Supplicants    : 1 / 1 / 64                ReAuthMode     : Enable
TxTimer(s)     : ---   / 30                ReAuthTimer(s): 48    / 300
ReAuthSuccess  : 4                         ReAuthFail     : 0
SuppDetection  : Auto

 Supplicants MAC     Status         AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
*0019.b97d.46c7      Authorized     Authenticated  Idle           1
                     254            2010/01/30 16:04:19
dist#1#
```

制限付きアクセス許可(検疫中)

[Supplicant の MAC アドレスの前に＊を表示する。]

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。

① 「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

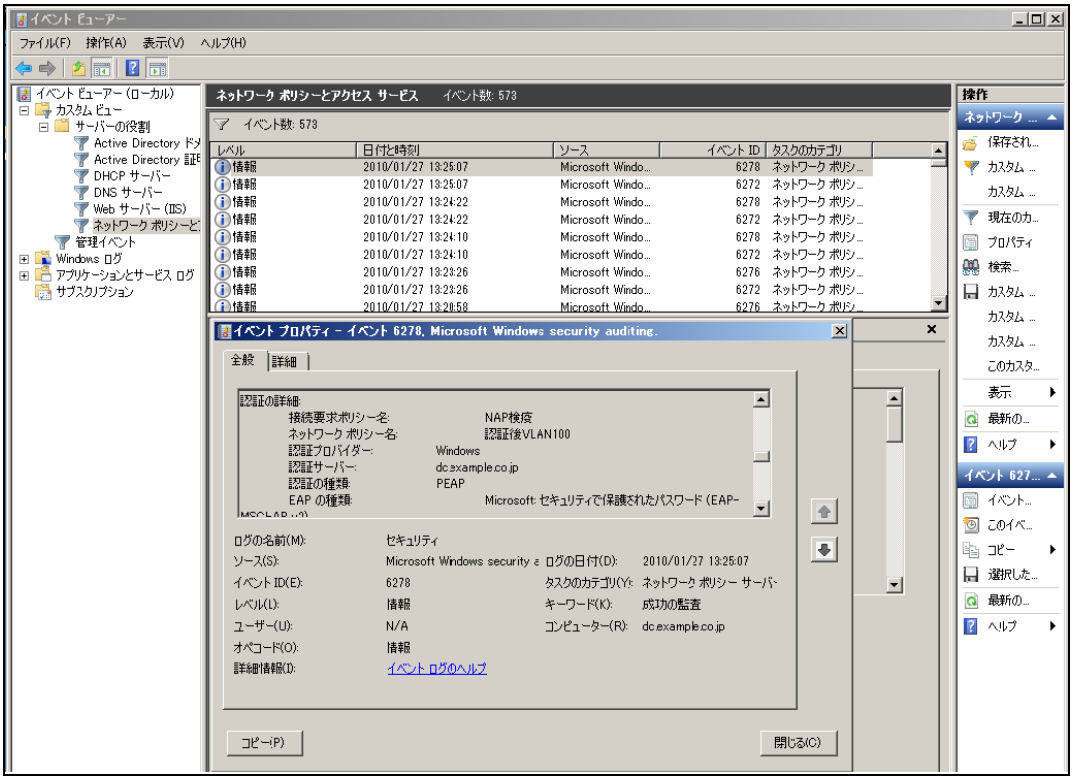


図 5.2-1 検疫結果成功のログ

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

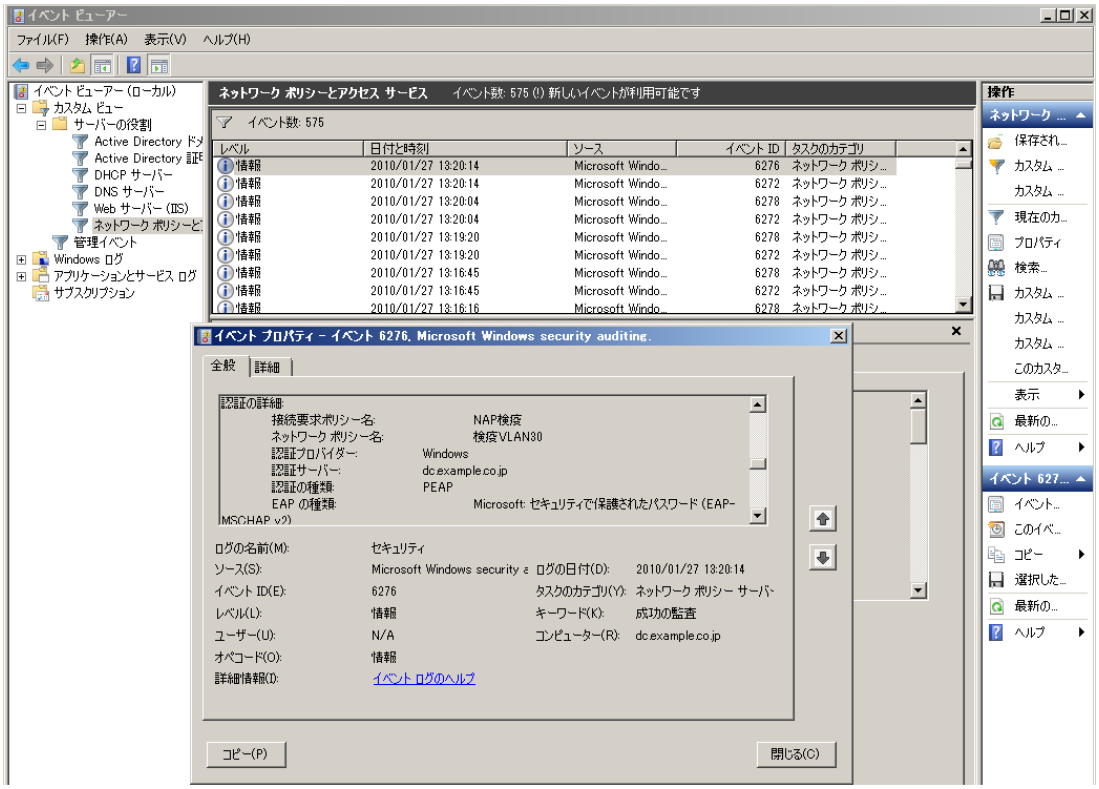


図 5.2-2 検疫結果失敗のログ

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。

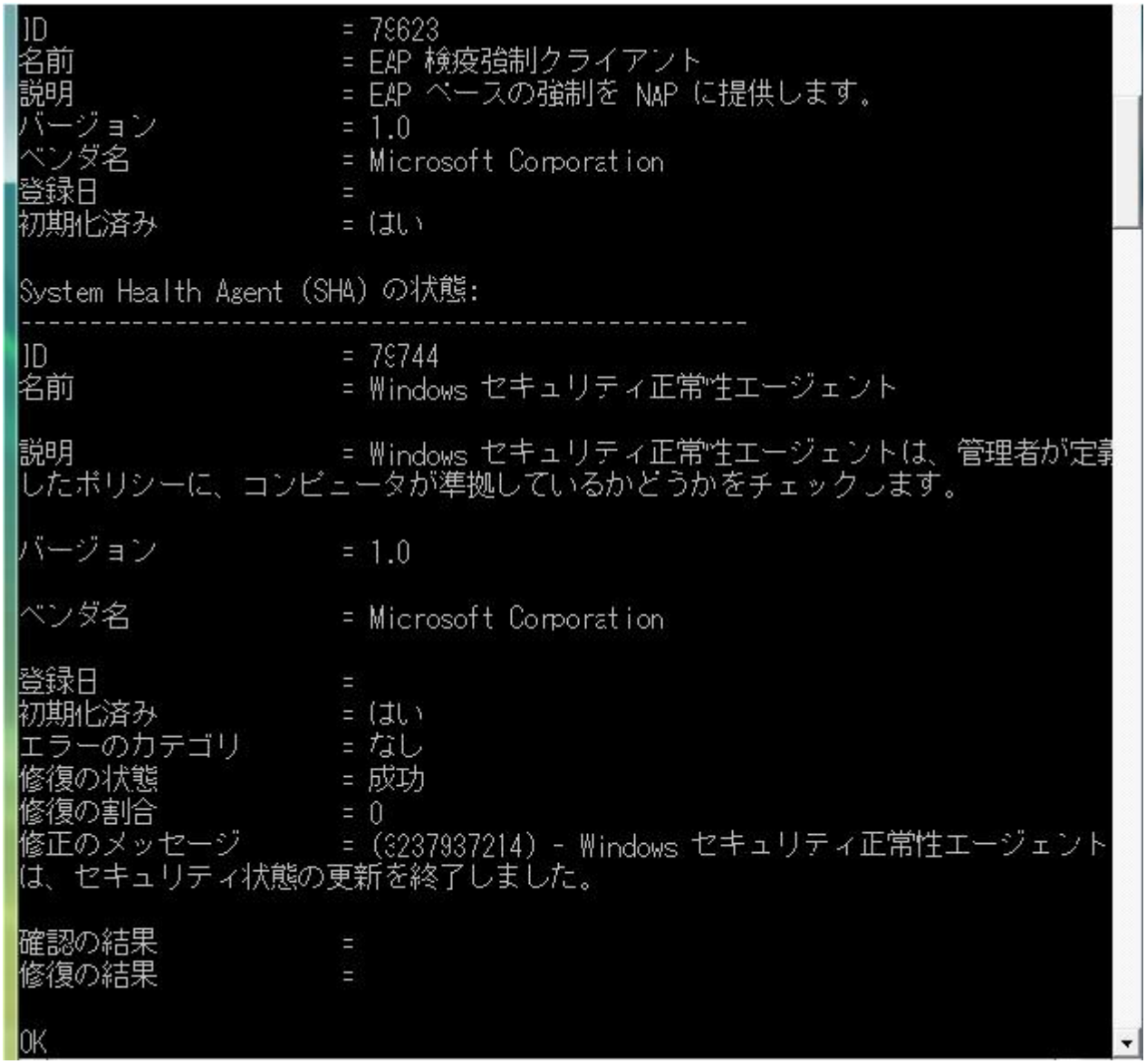


図 5.3-1 NAP クライアントステータス表示例

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。

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。

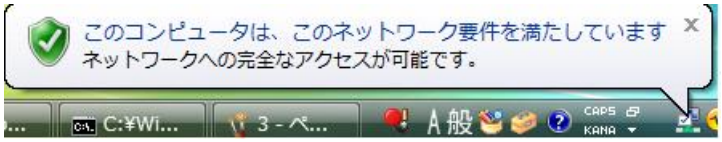


図 5.3-4 検疫成功時のメッセージ

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。

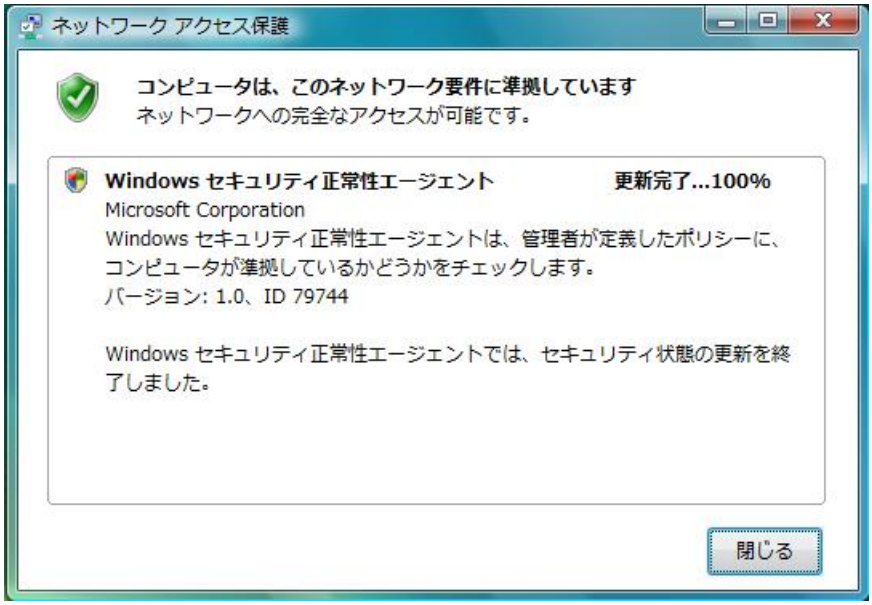


図 5.3-5 検疫成功時の画面

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。

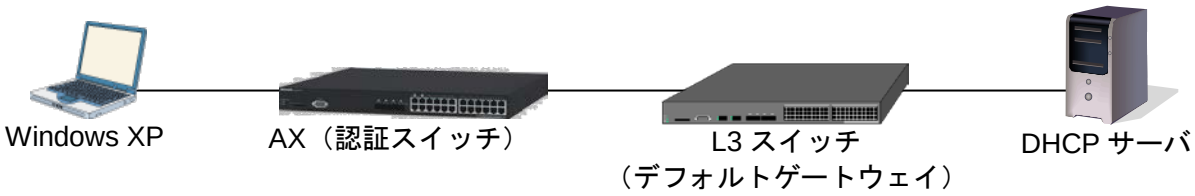


図 6.1-1 IP アドレス切り替え問題の起こるネットワーク構成

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3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.ffff.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

AX1200S

```
interface vlan 30
ip access-group "XP-ICMP30" in
!
interface vlan 100
ip 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)
!
ip access-list extended "XP-ICMP100"
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 192.168.30.0 0.0.0.255 dst 192.168.30.254 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
```

AX2400S

```
interface vlan 30
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 192.168.30.0 0.0.0.255 host 192.168.30.254
30 permit ip any any
```

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。

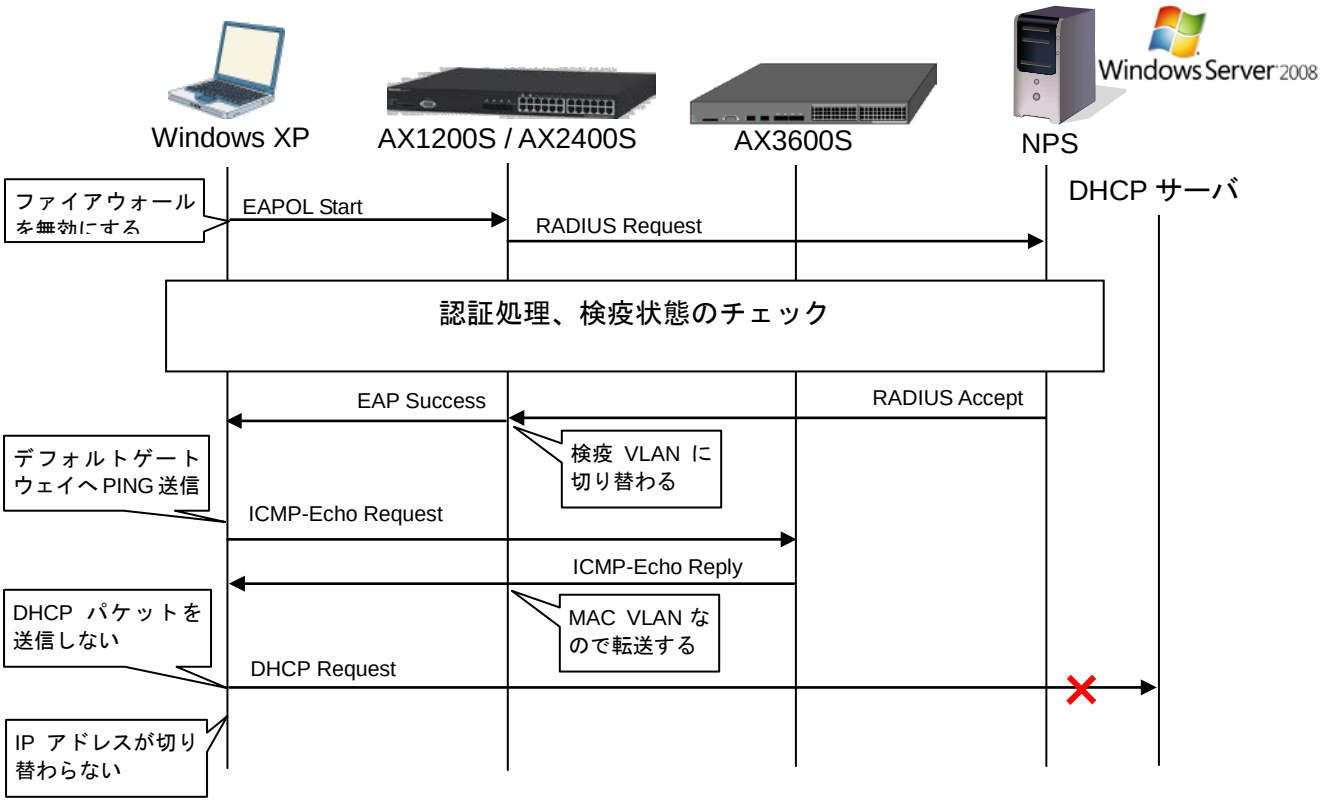


図 6.1-2 Windows XP の IP アドレス切り替えのシーケンス

（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。

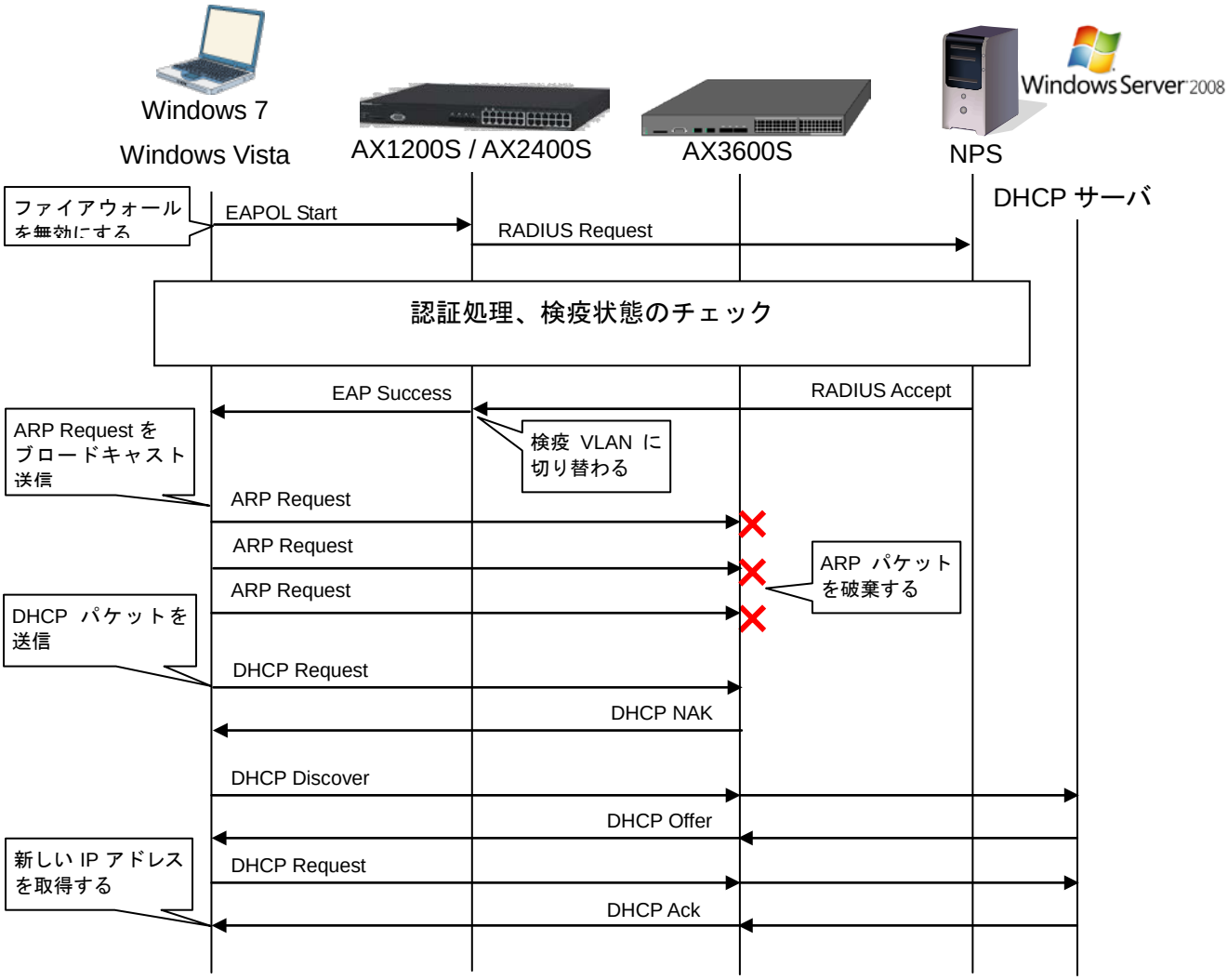


図 6.1-3 Windows 7 と Windows Vista の IP アドレス切り替えのシーケンス

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）

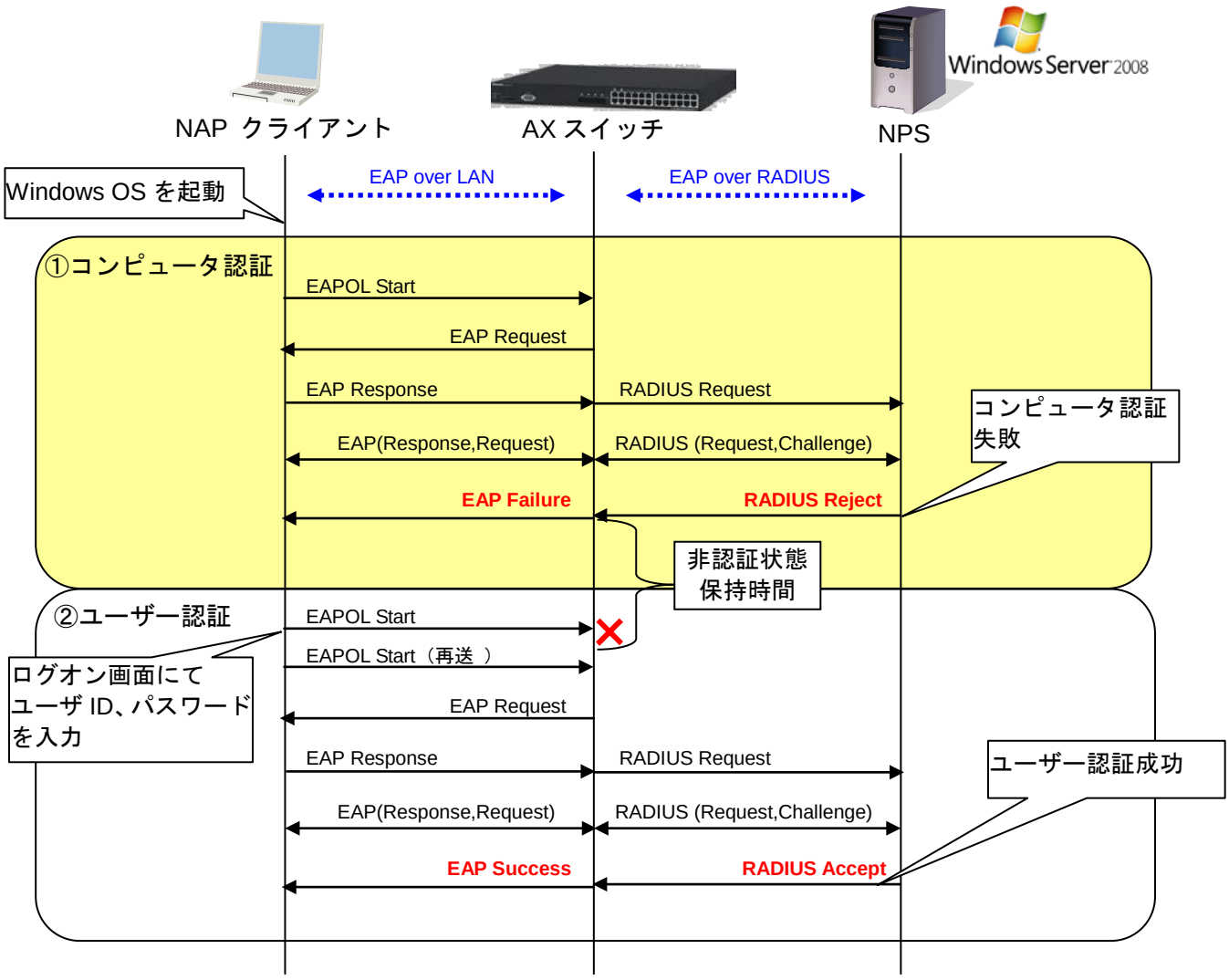


図 6.2-1 Windows の IEEE802.1X 認証シーケンス

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5.3.2参照)
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。（3.5.2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 Windows7 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） 認証方式の構成

（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。

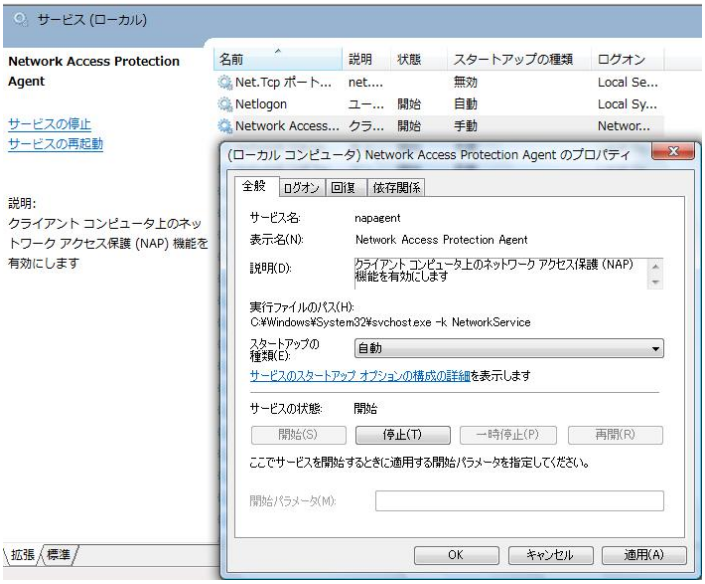


図 8.1-1 NAP Agent と Wired Auto Config サービスの有効化①

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。

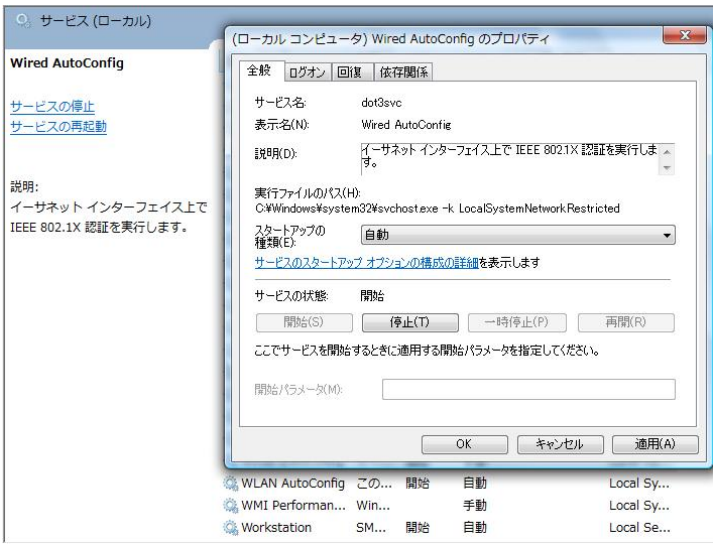


図 8.1-2 NAP Agent と Wired Auto Config サービスの有効化②

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。

② 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。

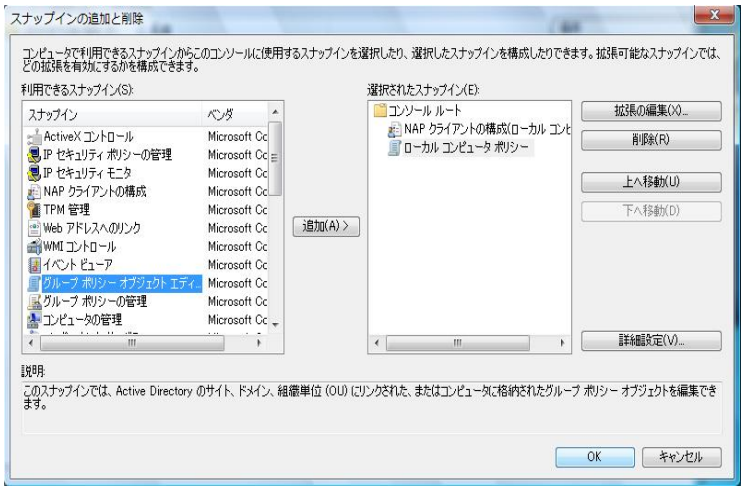


図 8.1-3 EAP 実施クライアントとセキュリティセンターの有効化①

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。

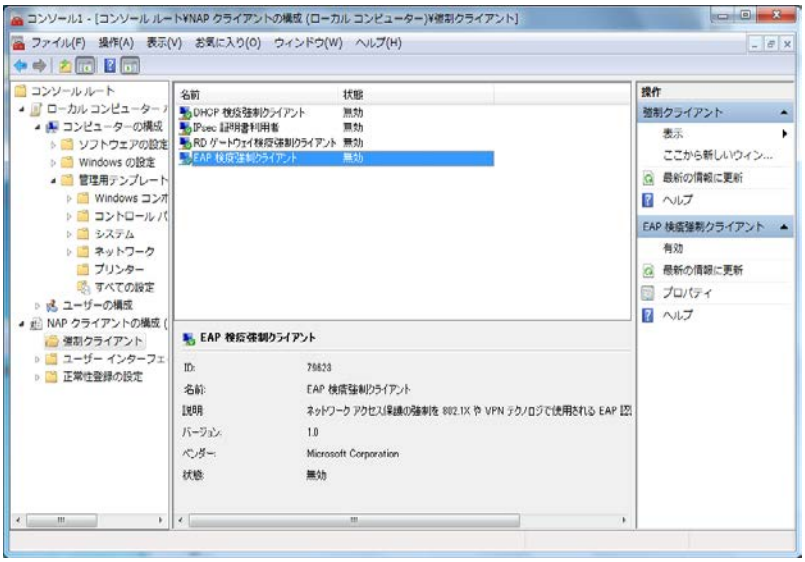


図 8.1-4 EAP 実施クライアントとセキュリティセンターの有効化②

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。

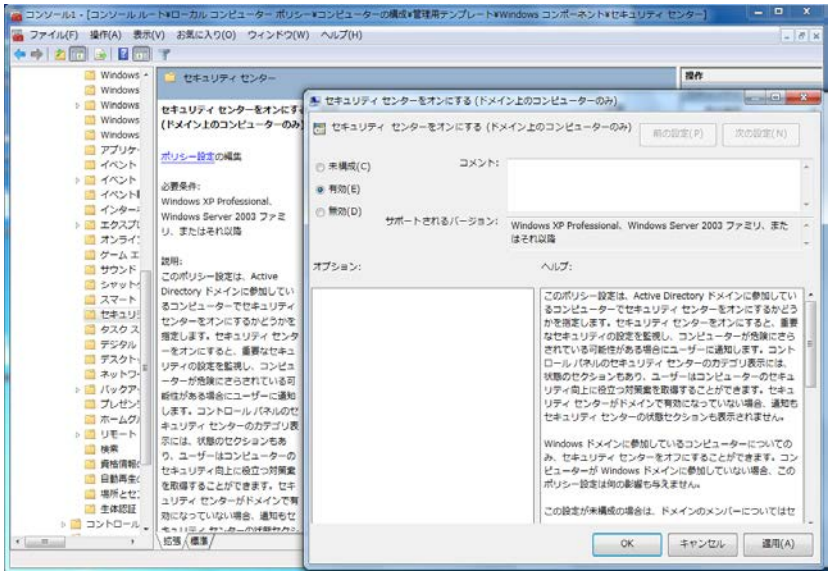


図 8.1-5 EAP 実施クライアントとセキュリティセンターの有効化(Windows 7)③

･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。

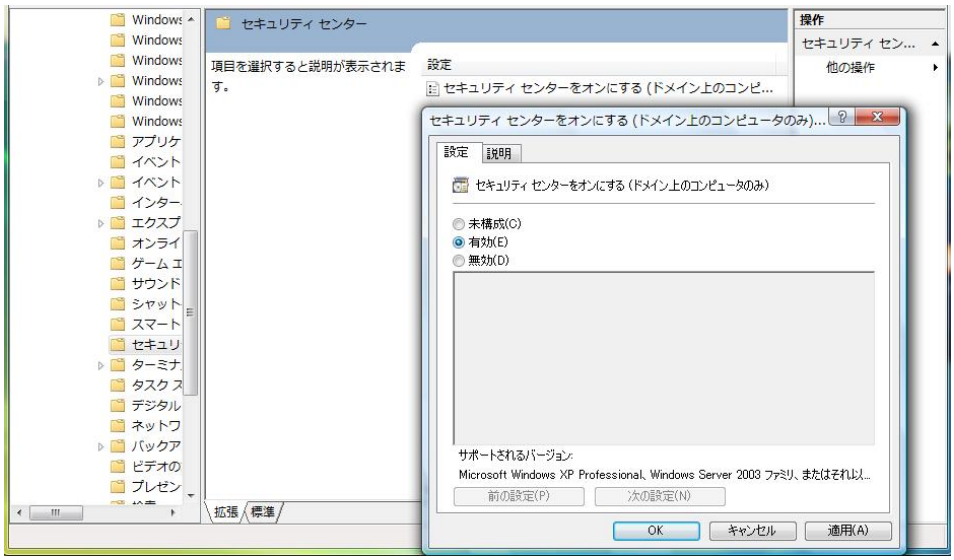


図 8.1-6 EAP 実施クライアントとセキュリティセンターの有効化(Windows Vista)③

⑤ 「OK」をクリックして画面を閉じる。

（３） 認証方式の構成

① 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

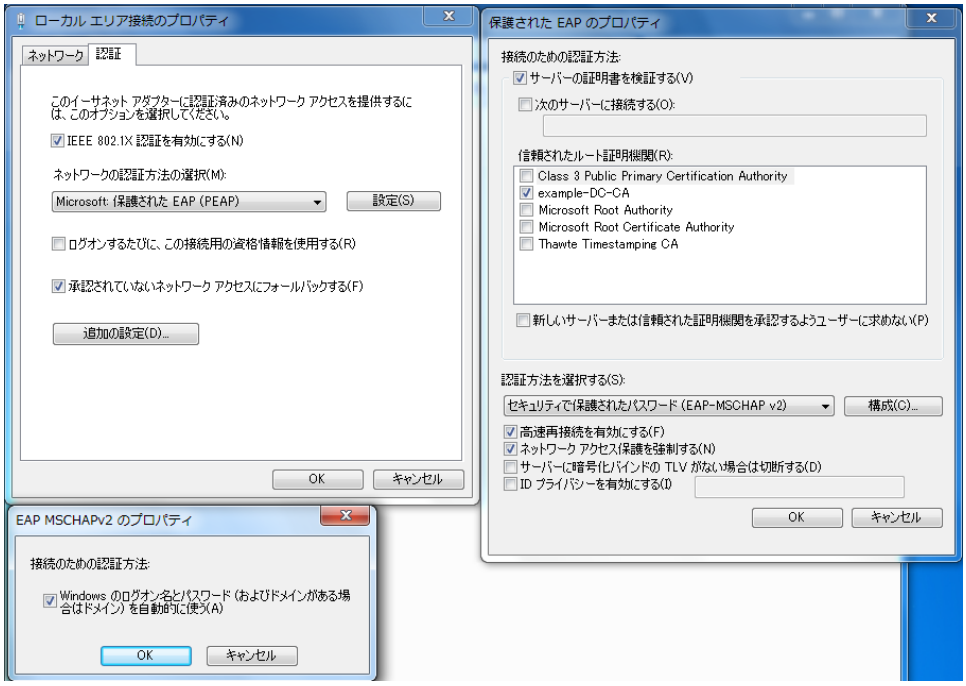


図 8.1-7 認証方式の構成(Windows 7)①

・Windows Vista の場合

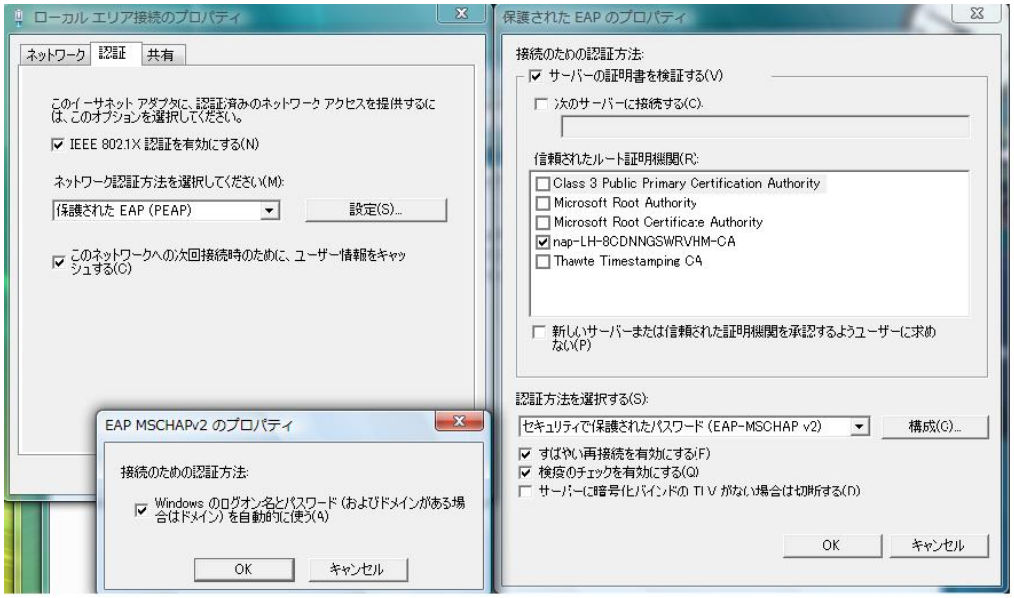


図 8.1-8 認証方式の構成(Windows Vista)①

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。

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） 認証方式の構成

（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。

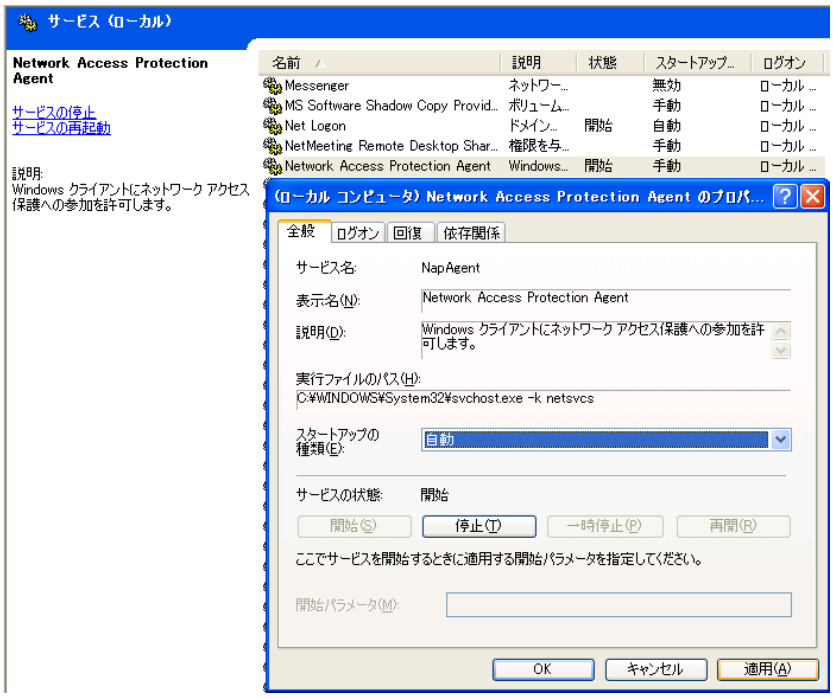


図 8.1-9 NAP Agent と Wired Auto Config サービスの有効化(Windows XP)①

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。

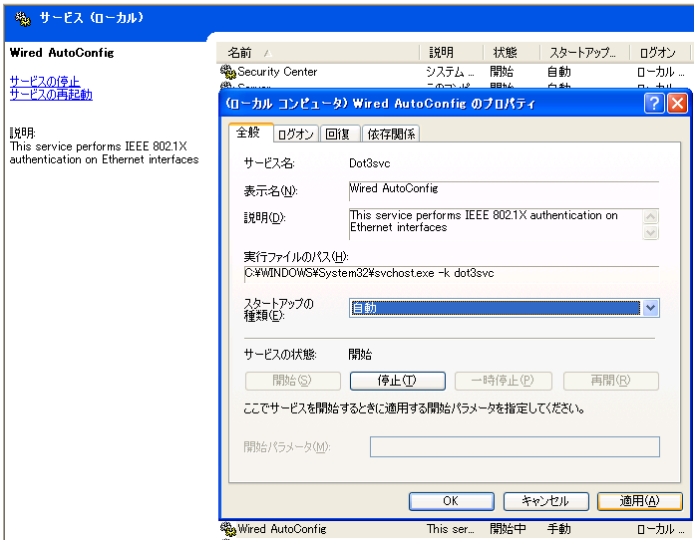


図 8.1-10 NAP Agent と Wired Auto Config サービスの有効化(Windows XP)②

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。

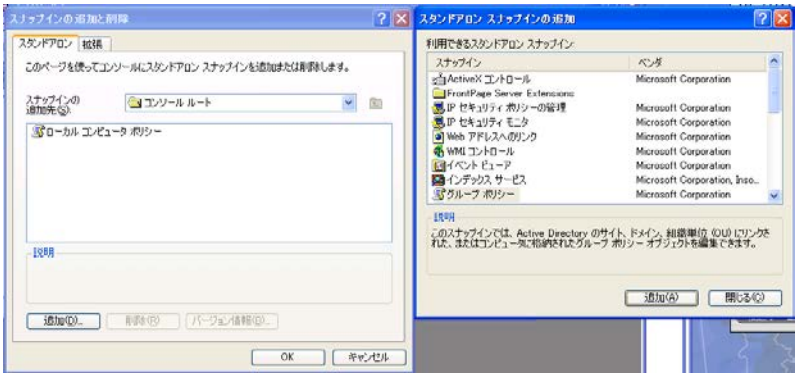


図 8.1-11 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)③

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。

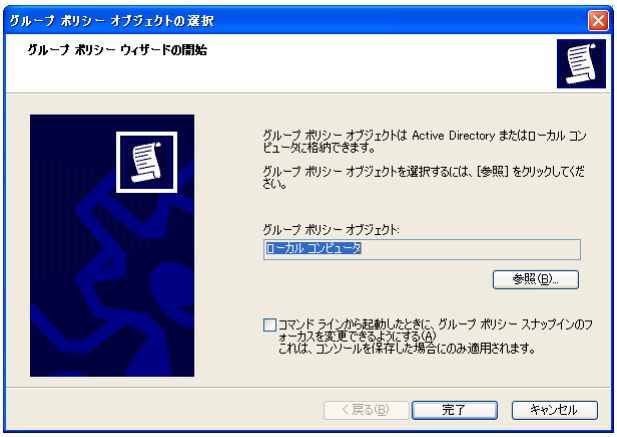


図 8.1-12 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)④

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。

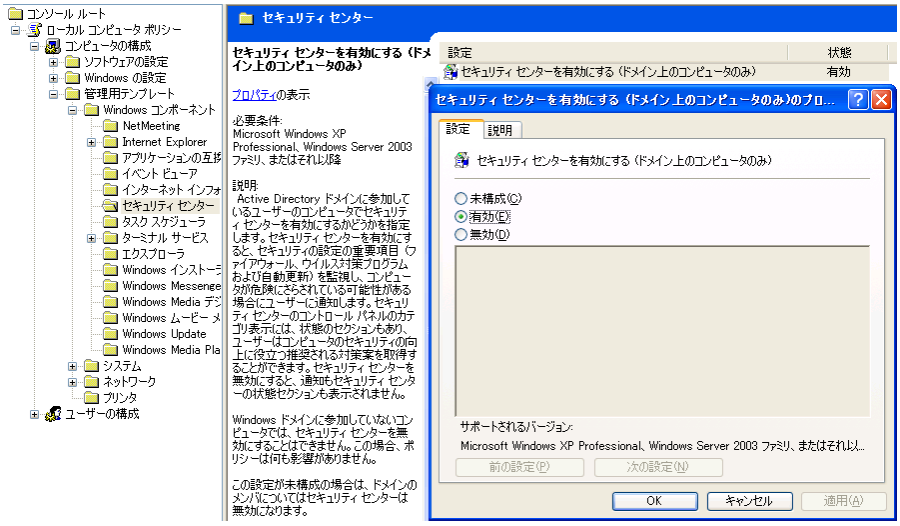


図 8.1-13 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)⑤

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
```

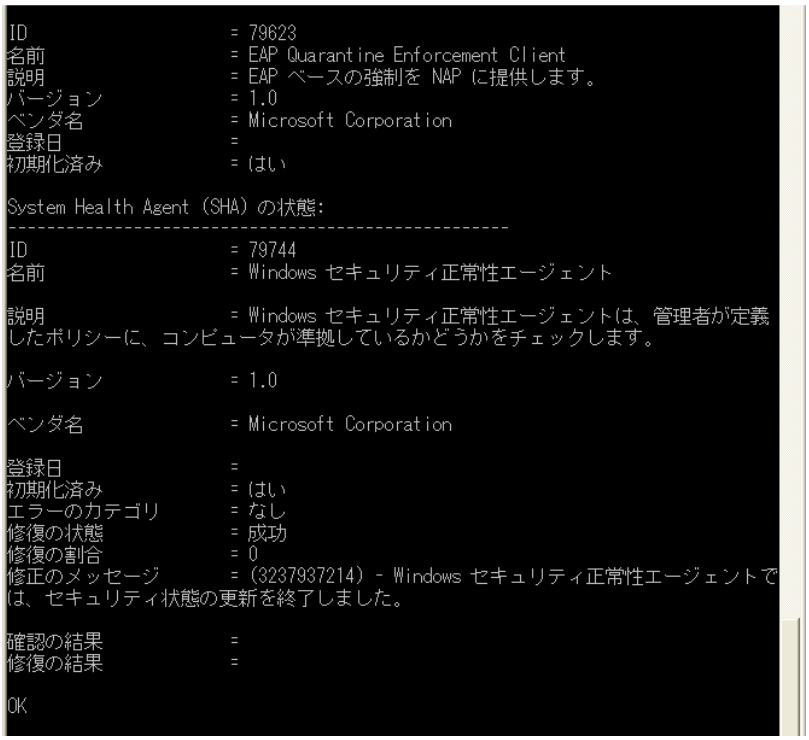


図 8.1-14 EAP 実施クライアントとセキュリティセンターの有効化(Windows XP)⑥

（3） 認証方式の構成

① 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。

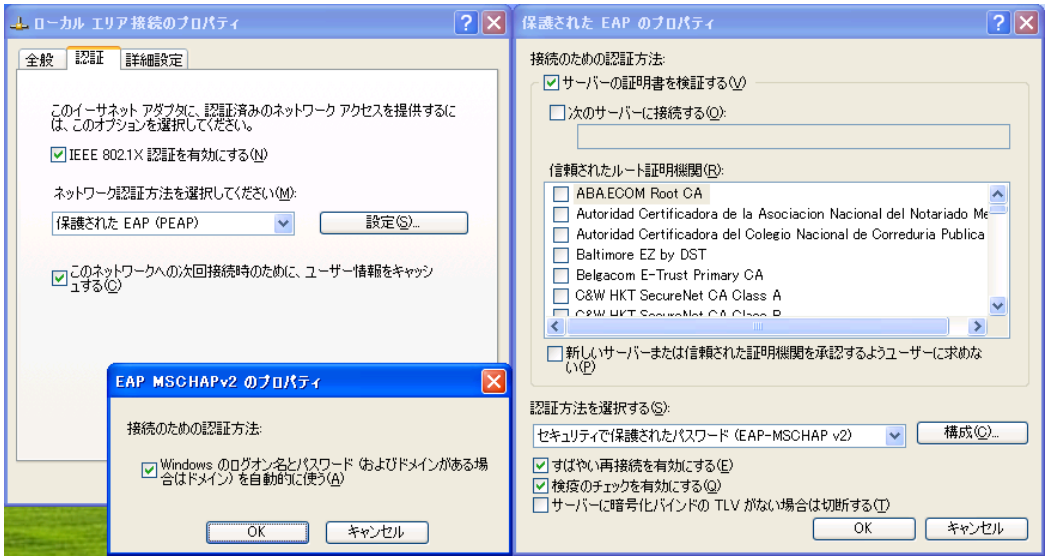


図 8.1-15 認証方式の構成(Windows XP)①

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、3.5.2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。

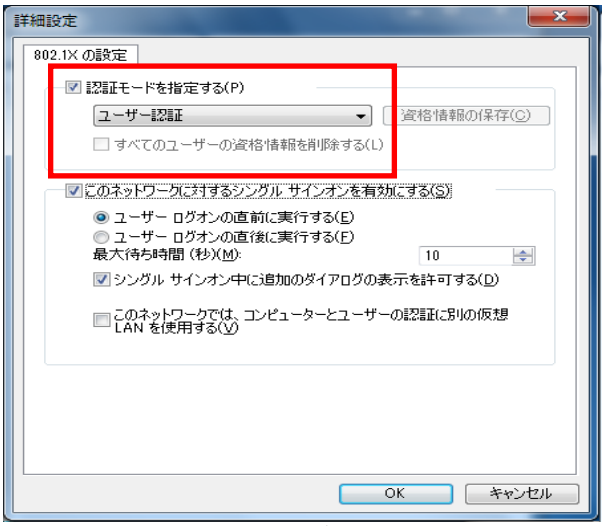


図 8.2-1 コンピュータ認証の停止

・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。

「3 章 検疫ネットワークの構築(動的 VLAN 構成)」と「4 章 検疫ネットワークの構築(固定 VLAN(ポート単位)構成」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
構築例1	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
	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/