AX シリーズ
NAP ソリューションガイド
(DHCP 編)

初版

はじめに

本ガイドは、Microsoft 社の提唱する Network Access Protection(NAP)検疫システムを構築するための技術情報をシステムエンジニアの方へ提供し、安全・安心な検疫システムの構築と安定稼動を目的として書かれています。

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 NAP ソリューションガイド（IEEE802.1X 認証編）
・AXシリーズ 製品マニュアル（http://www.alaxala.com/jp/support/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ください。

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	Ver1.3.D
AX3630S / AX3640S	Ver10.7

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

本ガイドを輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

商標一覧

・アラクサラの名称およびロゴマークは、アラクサラネットワークス株式会社の商標および登録商標です。
・Ethernetは、米国Xerox Corp.の商品名称です。
・イーサネットは、富士ゼロックス（株）の商品名称です。
・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 (Ver1.3.D)
- AX3630S (Ver10.7)
- Windows XP Professional SP3
- Windows Vista Ultimate SP1
- Windows Server 2008 Standard

目次

1. NAP 検疫概要

1.1. DHCP 方式の NAP 概要

1.1.1. 概要

Network Access Protection（以下 NAP）とは、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の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。

NAP を実現する方法として、5 つの方法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 1.1-1 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	IPsec（インターネットプロトコルセキュリティ）	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	VPN（仮想プライベートネットワーク）	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。

本ガイドでは、DHCP 方式の NAP 構築を紹介しています。

DHCP 方式の NAP は構築が最も容易であり、Windows Vista および Windows XP SP3 に DHCP で IP アドレスを配布している環境に初めて NAP を導入する場合に、サーバを Windows Server 2008 に置き換えるだけで実現することができます。また、ネットワーク認証と独立して検疫を行うため、ネットワーク構成に影響を与えず構築することができます。

DHCP 方式による検疫は、クライアント端末が DHCP サーバに対して IP アドレスを要求する時に、NAP クライアントの検疫情報を DHCP パケットに格納してサーバと交換することで実現しています。ネットワークポリシーサーバ（以下 NPS）は、受信した情報がセキュリティポリシーと合致しているか確認し、問題がなければ DHCP サーバが正規の IP アドレスを配布します。セキュリティポリシーに準拠していない端末には、修復作業のみに通信を制限したネットワーク接続を許可します。

DHCP 方式による検疫および隔離動作の概要を下図に示します。

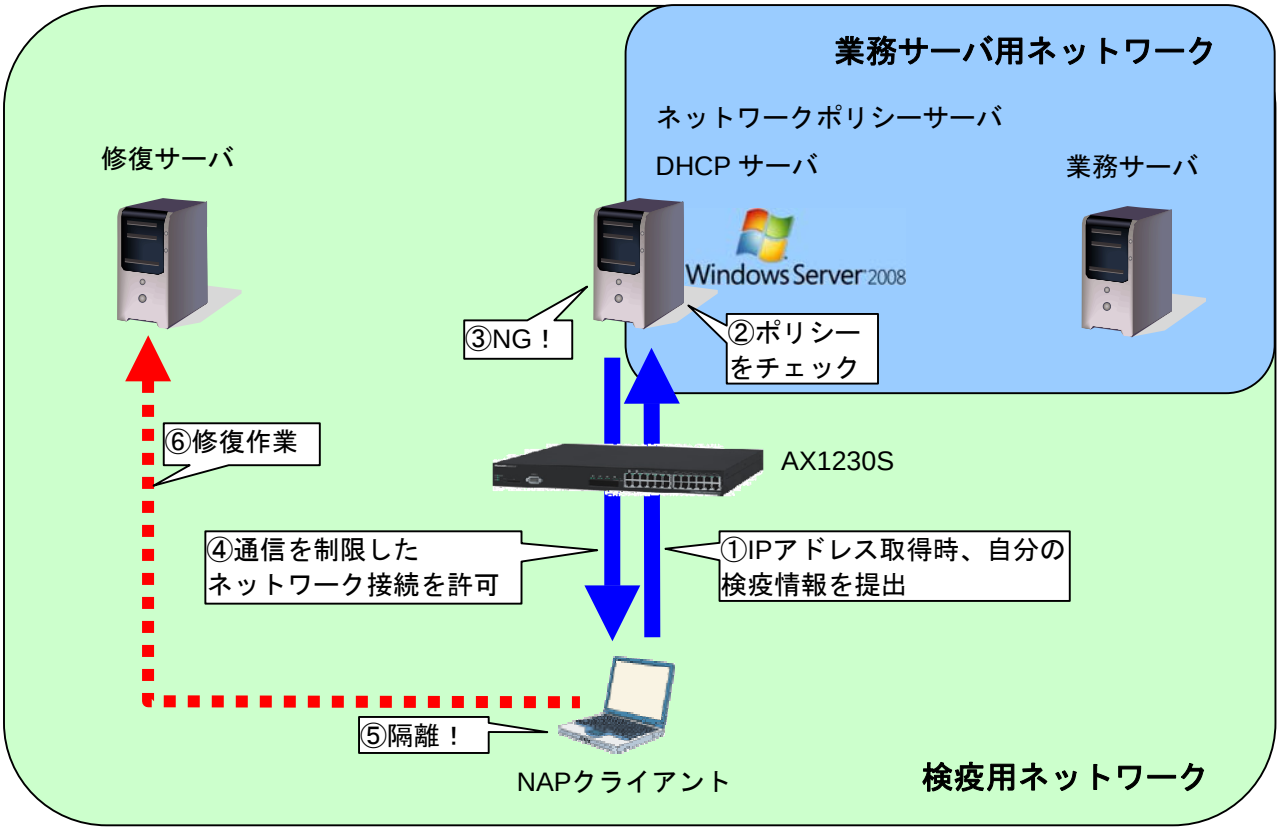


図 1.1-1　DHCP 方式の NAP 検疫動作

1.1.2. 検疫シーケンス

DHCP 方式の NAP では、NAP クライアントの検疫情報を DHCP リクエストパケットに格納してサーバと交換します。以下に、検疫シーケンスの例と、検疫動作について示します。

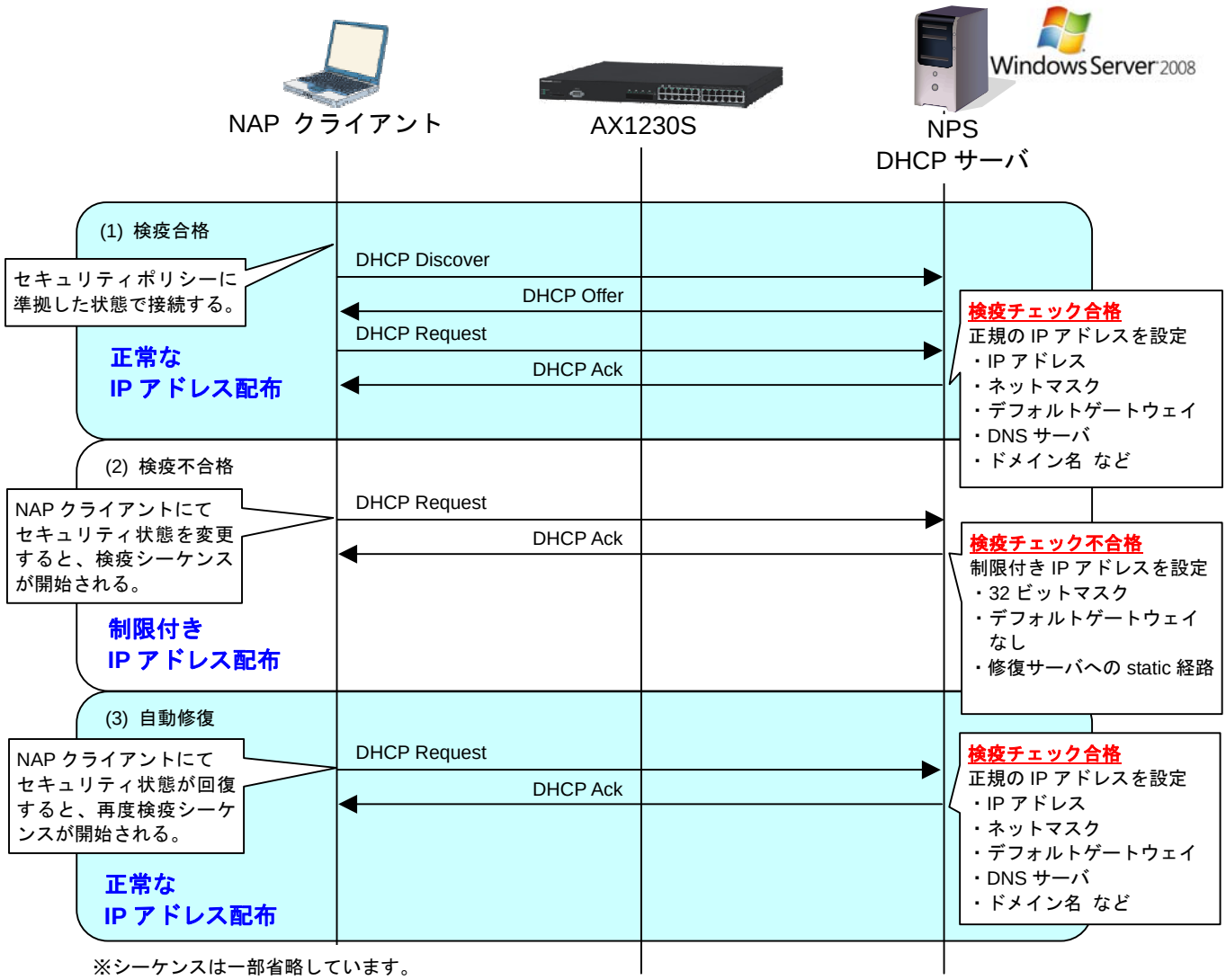


図 1.1-2 DHCP 方式の NAP シーケンス

（1） 検疫合格

NAP クライアント端末から DHCP リクエストパケットで送信された NAP クライアントの検疫情報について、セキュリティポリシーに合致しているか NPS で確認した結果、セキュリティポリシーを満たしている場合は DHCP サーバより正規の IP アドレスが配布されます。配布される情報は、IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバ、ドメイン名などです。

（2） 検疫不合格

ネットワーク接続時の DHCP リクエストパケットにより、NAP クライアントがセキュリティポリシーに合致しているか NPS で確認します。ネットワークに接続した後でも、NAP クライアントのセキュリティ状態が変化すると、NAP クライアントは即 DHCP リクエストパケットを送信し現在のセキュリティ状態を NPS に伝えます。NAP クライアントがセキュリティポリシーを満たしていない場合､DHCP サーバより通信を制限された IP アドレスが配布されます。配布される情報は、32 ビットマスク長の IP アドレス、修復サーバへの static 経路などです。デフォルトゲートウェイは配布されません。

（3） 自動修復

NPS で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していない NAP クライアントのセキュリティ状態は強制的に修復されます。

NAP クライアントのセキュリティ状態が強制的に変更されると、NAP クライアントは再度 DHCP リクエストパケットを送信して検疫シーケンスを開始します。検疫に合格すると、正規の IP アドレスが配布されます。

1.2. NAP と DHCP snooping 機能との併用

DHCP 方式による NAP は導入が容易な反面、固定 IP アドレスを持つクライアント端末は意図的に検疫を回避できてしまうという問題があります。この問題は、AX1200S のサポートする DHCP snooping 機能と併用することで抑止できます。

DHCP snooping 機能は、DHCP パケットを監視して、不正な DHCP サーバからの IP アドレス配布を抑止したり、正規の DHCP サーバから IP アドレスを配布されていない端末からの IP アドレス解放要求を抑止したりして、不正ユーザを排除する機能です。また、通信データの送信元 IP アドレスや送信元 MAC アドレスをチェックして、不正な端末の通信を制限することもできます。これにより、正規の DHCP サーバから IP アドレスを配布された端末のみ通信が可能となり、固定 IP アドレス端末は通信できなくなります。

プリンタなど固定IPアドレスを持つNAP非対応クライアントをネットワークに接続したい場合は、AX1200Sに端末情報を登録することにより、通信を許可することができます。(注意事項**5.1**を参照)

1.3. NAP のセキュリティリスク

DHCP 方式の NAP では、クライアント端末で IP アドレスを取得した後、その IP アドレスの値を使って手動で固定 IP アドレス設定に変更すると、以降の検疫を回避できてしまいます。これは、DHCP snooping 機能を併用している場合でも起こる問題です。DHCP snooping は DHCP パケットが通過する度にバインディングデータベースを更新しますが、そのエントリにおいて「IP アドレス」「MAC アドレス」「接続ポート」が一致するクライアント端末は、通信が許可されるためです。

本問題について、対策法を以下に示します。導入する環境に合わせて対処してください。

（１） DHCP のリース期間を短くする。

DHCP snooping のバインディングデータベースに登録されているエントリは、その IP アドレスのリース期間が過ぎるとバインディングデータベースから削除されます。これ以降、固定 IP アドレスに変更したクライアント端末は通信できなくなります。従って、DHCP サーバでリース期間を短く設定することで、不正なクライアント端末の通信を抑止することができます。

ただし、リース期間が短すぎるとトラフィックが増加するので、ネットワークの負荷、コアスイッチおよび DHCP サーバの負荷や運用方針を考慮して設定してください。例えば、クライアント端末に 1 日 1 回は必ず検疫を実施したいのであれば、リース期間を 1 日以内に設定してください。

（２） IEEE802.1X 認証方式を使う。

IEEE802.1X 認証方式の NAP は、より強固な検疫ネットワークを構築するのに適しています。詳細は「AX シリーズ NAP ソリューションガイド（IEEE802.1X 認証編）」をご参照ください。

2. AX1200S の DHCP snooping 収容条件

本ガイドの検疫ネットワークでは、AX1200S の DHCP snooping 機能を使用しています。AX1200S のサポートする DHCP snooping 機能の収容条件を以下に示します。

表 2-1 DHCP snooping 機能の収容条件

項番	項目	最大数
1	設定 VLAN 数	32
2	バインディングデータベースエントリ総数	246
3	バインディングデータベーススタティックエントリ数(*1)	64

(*1) スタティックエントリ数は、バインディングデータベースエントリ総数に含まれます。

3. 検疫ネットワークの構築

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

DHCP 方式検疫ネットワークの基本的な構成を、以下のように定義します。

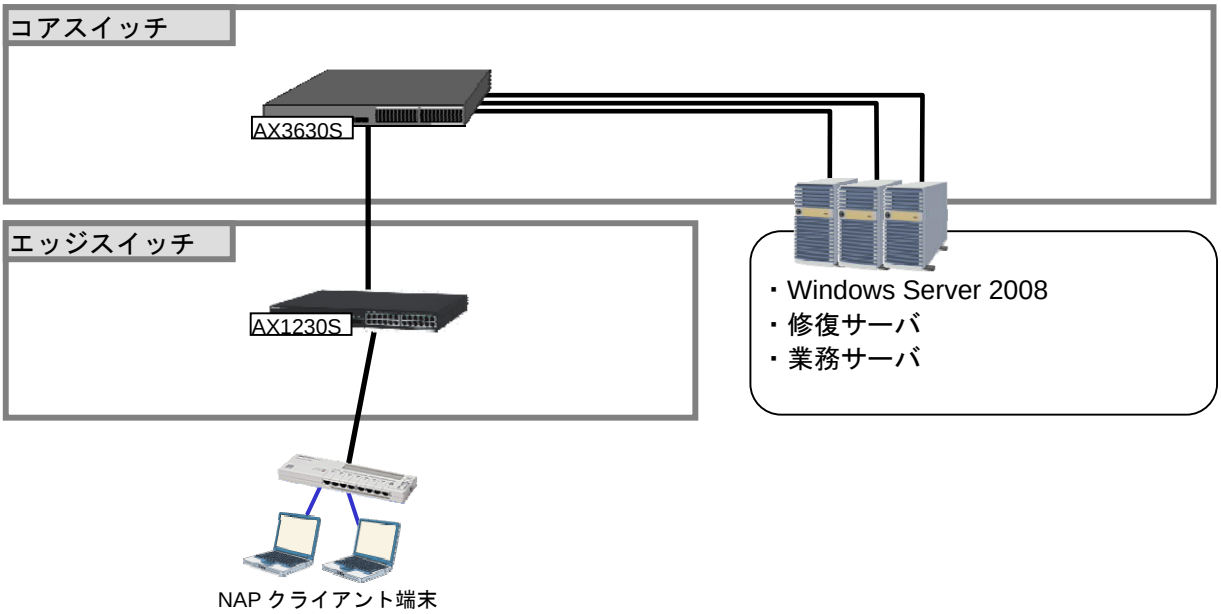


図 3.1-1 検疫ネットワークの基本構成

コアスイッチには AX3630S を配置します。NPS および DHCP サーバとして稼動する Windows Server 2008、検疫によりネットワークアクセスが制限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を、コアスイッチ配下に接続します。

エッジスイッチには AX1230S を配置し、検疫を行う端末をエッジ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 3.1-1 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
•DNS サーバ •DHCP サーバ •NPS	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

基本的な検疫ネットワーク構成例を以下に示します。

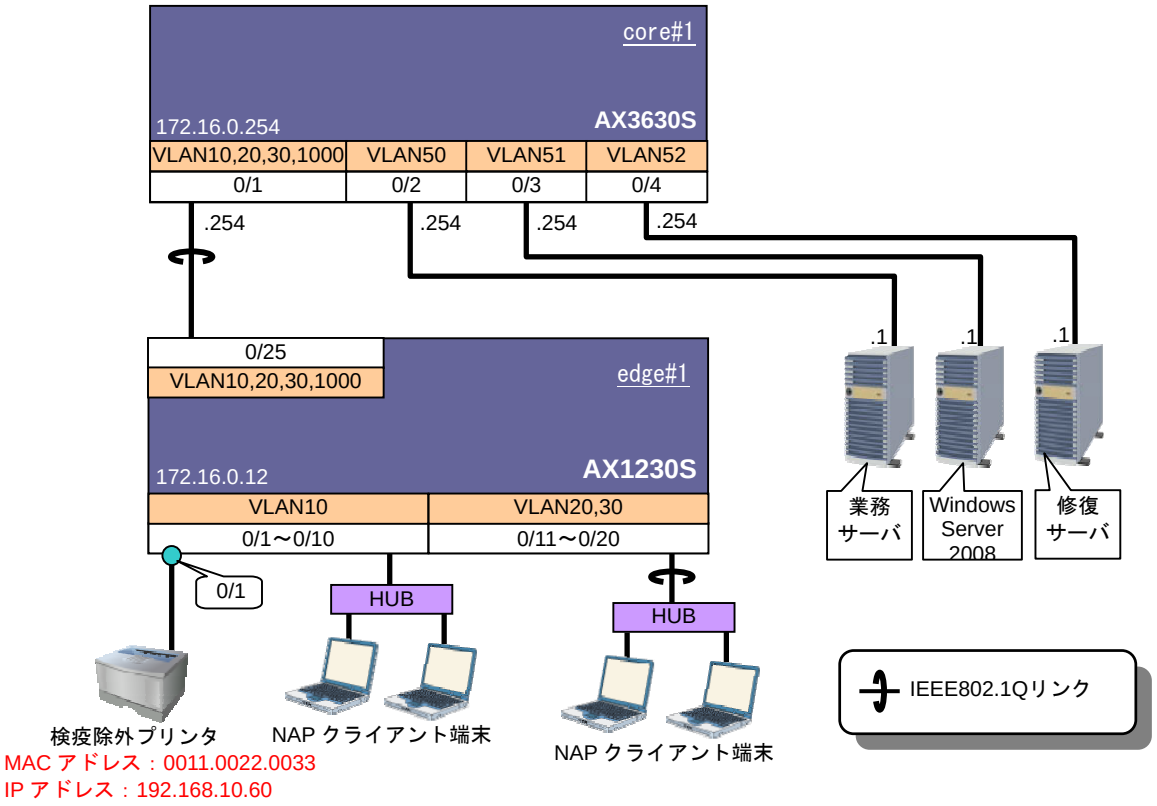


図 3.2-1 検疫ネットワーク構成図

各 VLAN の定義および端末とサーバ間通信の可否を以下の表に示します。

表 3.2-1 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、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	検疫により通信制限された端末を修復するためのサーバが所属する VLAN。	修復サーバ
クライアント用 VLAN	10	192.168.10.0/24	クライアント端末が所属する VLAN。	―
	20	192.168.20.0/24		
	30	192.168.30.0/24		
管理用 VLAN	1000	172.16.0.0/24	各装置を管理するための VLAN。	―

表 3.2-2 端末ーサーバ間通信の可否

	業務サーバ	Windows Server 2008	修復サーバ
検疫合格	○	○	○
検疫不合格	×	○	○

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

（１） 運用前にシステムファンクションリソースを設定する。

エッジスイッチの DHCP snooping 機能を使用する場合、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ます。設定変更後は装置の再起動が必要です。

（２） DHCP snooping を設定する。

不正な端末の通信を防ぐため、エッジスイッチの DHCP snooping 機能を有効にします。DHCP サーバと通信するポートを trust ポートとし、他のポートについては端末フィルタを実施します。

（３） DHCP snooping のバインディングデータベース保存先を指定する。

DHCP snooping機能が管理するバインディングデータベースの保存先を指定しておきます。本ガイドでは内蔵フラッシュメモリに指定しています。（注意事項5.3を参照）

（４） 検疫除外端末を登録する。

検疫を除外したい端末がある場合は、バインディングデータベースにstatic登録します。（注意事項5.1を参照）

（５） DHCP リレーの設定をする。

コアスイッチに Windows Server 2008（DHCP サーバ）の IP アドレスを設定をします。

3.3.2. Windows Server 2008 に関する構築ポイント

（１） 検疫不合格時に DHCP サーバへの static 経路を配布する。

検疫不合格時には、表 3.2-2に示すように、クライアントに対してWindows Server 2008（DHCP サーバ）への通信も許可する必要があります。DHCPサーバへの通信が許可されていない場合、セキュリティ状態が変化したときの検疫処理に時間がかかってしまいます。（注意事項5.2を参照）

3.4. AX の設定

3.4.1. AX1230S のコンフィグレーション

AX1230S の設定例を示します。

（1） 事前設定

AX1230S の設定	
システムファンクションリソース配分の設定	
(config)# system function filter dhcp-snooping	フィルタ機能と DHCP snooping 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。 **※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

AX1230S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 10,20,30,1000** **(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 VLAN10、20、30 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 disable	スパニングツリーを無効にします。
物理ポートの設定	
●クライアント側（アクセスポート） **(config)# interface range fastethernet 0/1-10** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 10**	ポート 0/1～0/10 を、アクセスポートとして設定します。 アクセスポートに VLAN10 を設定します。
●クライアント側（トランクポート） **(config)# interface range fastethernet 0/11-20** **(config-if-range)# switchport mode trunk** **(config-if-range)# switchport trunk allowed vlan 20,30**	ポート 0/11～0/20 を、トランクポートとして設定します。 トランクポートに VLAN20、30 を設定します。
●上位スイッチとの通信用 **(config)# interface gigabitethernet 0/25** **(config-if)# switchport mode trunk** **(config-if)# switchport trunk allowed vlan 10,20,30,1000**	ポート 0/25 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、20、30 および 1000 を設定します。
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。
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	デフォルトルートを設定します。

（３） DHCP snooping の設定

AX1230S の設定	
DHCP snooping の設定	
(config)# ip dhcp snooping vlan 10,20,30 **(config)# interface gigabitethernet 0/25** **(config-if)# ip dhcp snooping trust** **(config)# interface range fastethernet 0/1-20** **(config-if-range)# ip verify source port-security** **(config)# ip dhcp snooping** **(config)# ip dhcp snooping database url flash**	VLAN10、20、30 で DHCP snooping を有効にします。 上位スイッチとの通信用ポート 0/25 を、信頼されているポートとして設定します。 ポート 0/1～0/20 で、送信元 IP アドレスと送信元 MAC アドレスによる端末フィルタを実施します。 DHCP snooping 機能を有効にします。 ➢ **構築ポイント（２）** バインディングデータベースの保存先を内蔵フラッシュメモリに指定します。 ➢ **構築ポイント（３）**
●検疫除外端末の登録 **(config)# ip source binding 0011.0022.0033 vlan 10 192.168.10.60 interface fastethernet 0/1**	バインディングデータベースに static 登録します。 ➢ **構築ポイント（４）**

3.4.2. AX3630S のコンフィグレーション

AX3630S の設定例を示します。

（1） 基本設定

AX3630S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 10,20,30,1000** **(config-vlan)# state active** **(config)# vlan 50,51,52** **(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 VLAN10、20、30 を、管理用 VLAN として VLAN1000 を作成します。 サーバ用 VLAN として VLAN50、51、52 を作成します。
スパニングツリーの設定	
(config)# spanning-tree disable	スパニングツリーを無効にします。
物理ポートの設定	
(config)# interface gigabitethernet 0/1 **(config-if)# media-type rj45** **(config-if)# switchport mode trunk** **(config-if)# switchport trunk allowed vlan 10,20,30,1000** **(config)# interface gigabitethernet 0/2** **(config-if)# media-type rj45** **(config-if)# switchport mode access** **(config-if)# switchport access vlan 50** **(config)# interface gigabitethernet 0/3** **(config-if)# media-type rj45** **(config-if)# switchport mode access** **(config-if)# switchport access vlan 51** **(config)# interface gigabitethernet 0/4** **(config-if)# media-type rj45** **(config-if)# switchport mode access** **(config-if)# switchport access vlan 52**	ポート 0/1 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、20、30 および 1000 を設定します。 ポート 0/2 を、アクセスポートとして設定します。 アクセスポートに VLAN50 を設定します。 ポート 0/3 を、アクセスポートとして設定します。 アクセスポートに VLAN51 を設定します。 ポート 0/4 を、アクセスポートとして設定します。 アクセスポートに VLAN52 を設定します。
インタフェースの設定	
(config)# interface vlan 10 **(config-if)# ip address 192.168.10.254 255.255.255.0** **(config)# interface vlan 20** **(config-if)# ip address 192.168.20.254 255.255.255.0** **(config)# interface vlan 30** **(config-if)# ip address 192.168.30.254 255.255.255.0** **(config)# interface vlan 50** **(config-if)# ip address 10.50.0.254 255.255.255.0** **(config)# interface vlan 51** **(config-if)# ip address 10.51.0.254 255.255.255.0** **(config)# interface vlan 52** **(config-if)# ip address 10.52.0.254 255.255.255.0**	各 VLAN にインタフェース IP アドレスをそれぞれ設定します。

AX3630S の設定	
(config)# interface vlan 1000 **(config-if)# ip address 172.16.0.254 255.255.255.0**	

（２） DHCP リレーの設定

AX3630S 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 20** **(config-if)# ip helper-address 10.51.0.1** **(config)# interface vlan 30** **(config-if)# ip helper-address 10.51.0.1**	VLAN10、20 および 30 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（５）**

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、NPS および DHCP サーバ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ください。
なお、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） NPSの設定
DHCP 方式の NAP を構成します。
（３） DHCPサーバの設定
スコープの作成および NAP を使用するため必要な設定を行います。

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ください。

役割

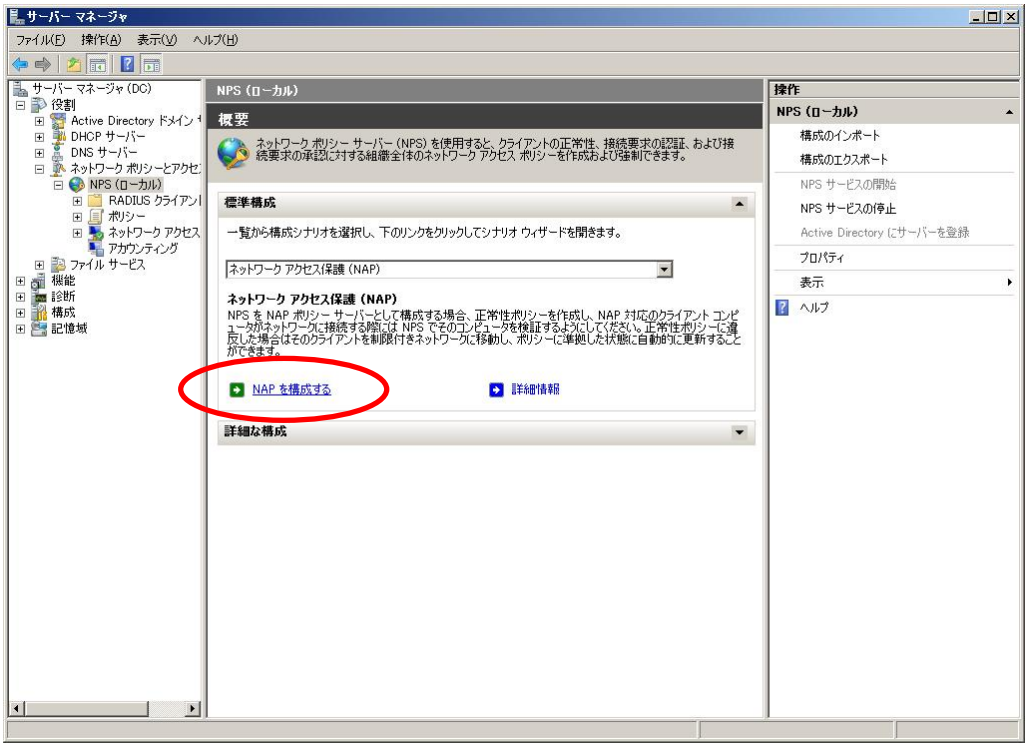
1. **DNS サーバ**
   このサーバをプライマリ DNS として設定します。
2. **NPS**
   本章にて設定内容を示します。
3. **DHCP サーバ**
   本章にて設定内容を示します。

3.5.2. NPS の設定

（1） NAP の構成

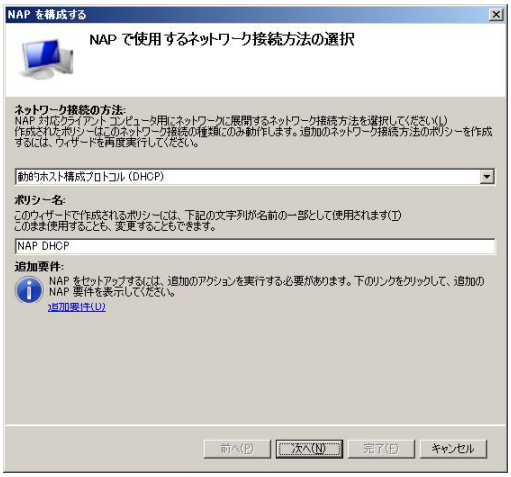
DHCP 方式の NAP を構成する手順を以下に示します。

① 「スタート」→「管理ツール」→「サーバーマネージャ」を開く。
サーバーマネージャ画面にて、左画面の中の「サーバーマネージャ」→「役割」→「ネットワークポリシーとアクセスサービス」→「NPS(ローカル)」を選択し、右画面の「NAP を構成する」をクリックすると、ウィザードが開始される。



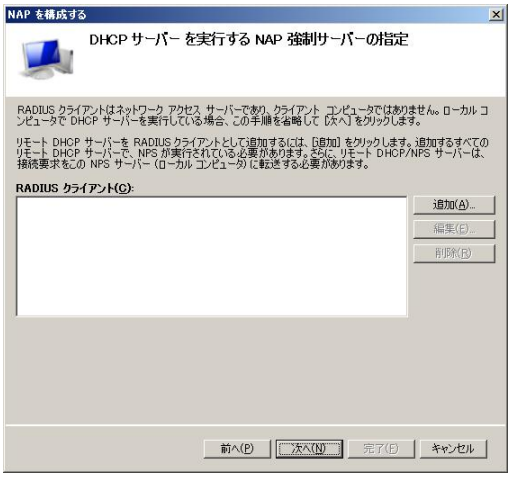
② NAP で使用するネットワーク接続方法の選択

ネットワーク接続の方法として「動的ホスト構成プロトコル(DHCP)」を選択し、「次へ」をクリックする。



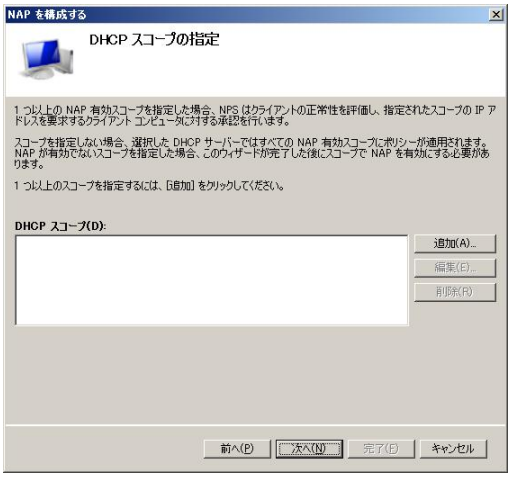
③ DHCP サーバーを実行する NAP 強制サーバーの指定

「次へ」をクリックする。



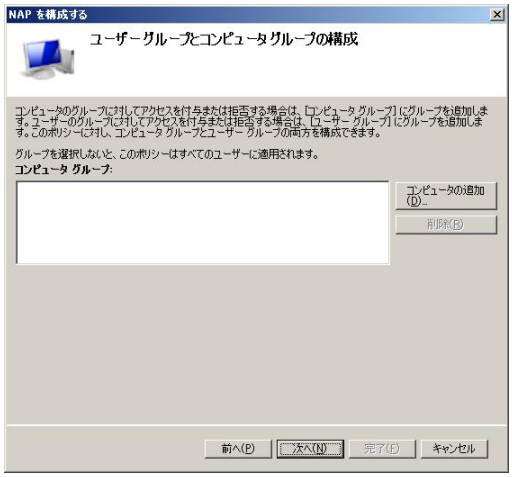
④ DHCP スコープの指定

「次へ」をクリックする。



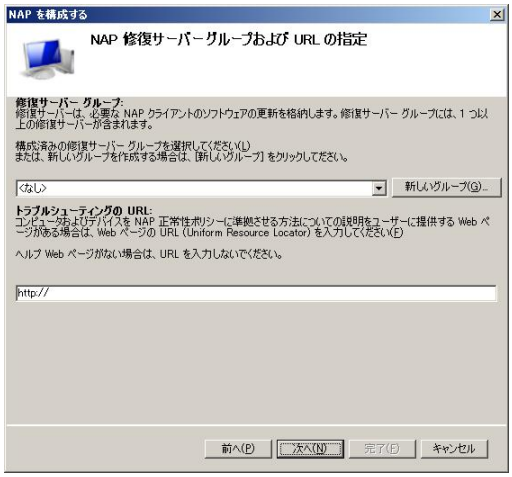
⑤ ユーザーグループとコンピュータグループの構成

「次へ」をクリックする。



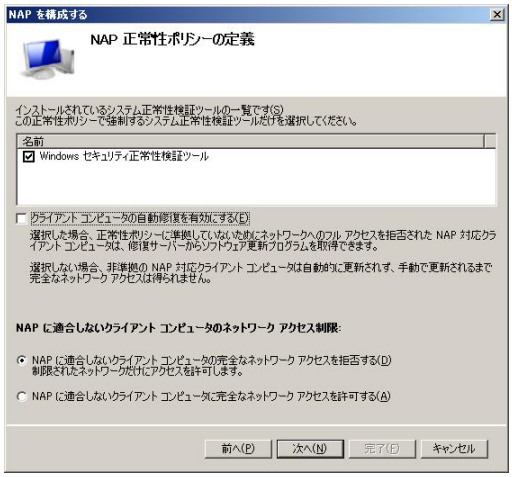
⑥ NAP 修復サーバーグループおよび URL の指定

「次へ」をクリックする。

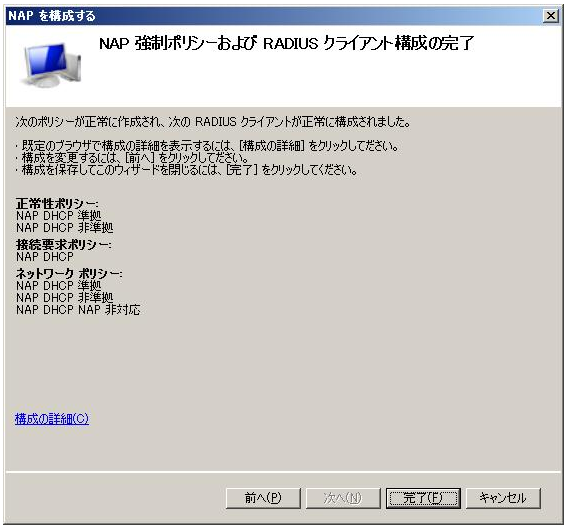


⑦ NAP 正常性ポリシーの定義

「クライアントコンピュータの自動修復を有効にする」のチェックを外す（自動修復機能を使用する場合は、本手順を省略）。「次へ」をクリックする。



⑧ 「完了」をクリックして画面を閉じる。



以上で、下記 6 つのポリシーが自動的に作成されます。

接続要求ポリシー

・NAP DHCP

ネットワークポリシー

・NAP DHCP 準拠

・NAP DHCP 非準拠

・NAP DHCP NAP 非対応

正常性ポリシー

・NAP DHCP 準拠

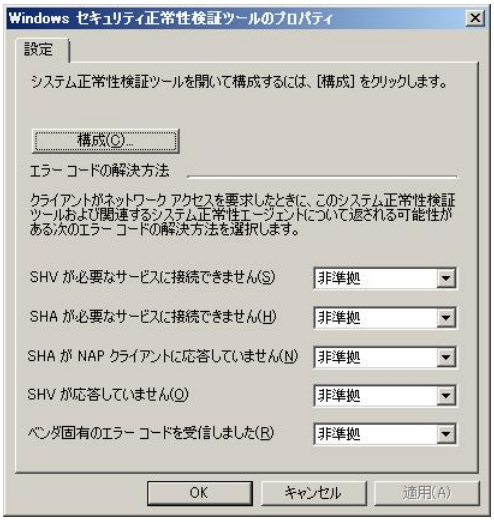
・NAP DHCP 非準拠

（２） システム正常性検証ツールの変更

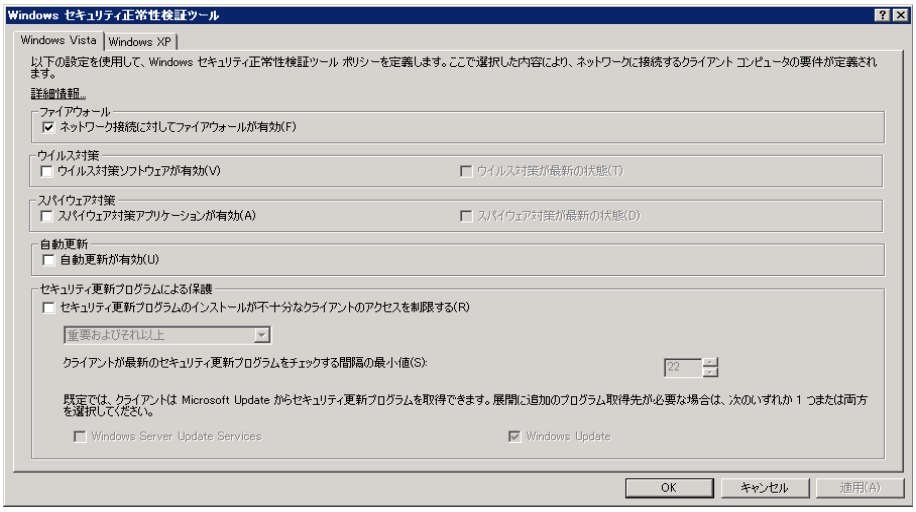
本ガイドでは、Windows ファイアウォールの有無のみを検疫判断基準としています。変更が必要でない場合は、本手順を省略してください。

① 「スタート」→「管理ツール」→「サーバーマネージャ」を開く。
サーバーマネージャ画面にて、左画面の中の「サーバーマネージャ」→「役割」→「ネットワークポリシーとアクセスサービス」→「NPS(ローカル)」→「ネットワークアクセス保護」→「システム正常性検証ツール」を展開し、右画面の「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開く。

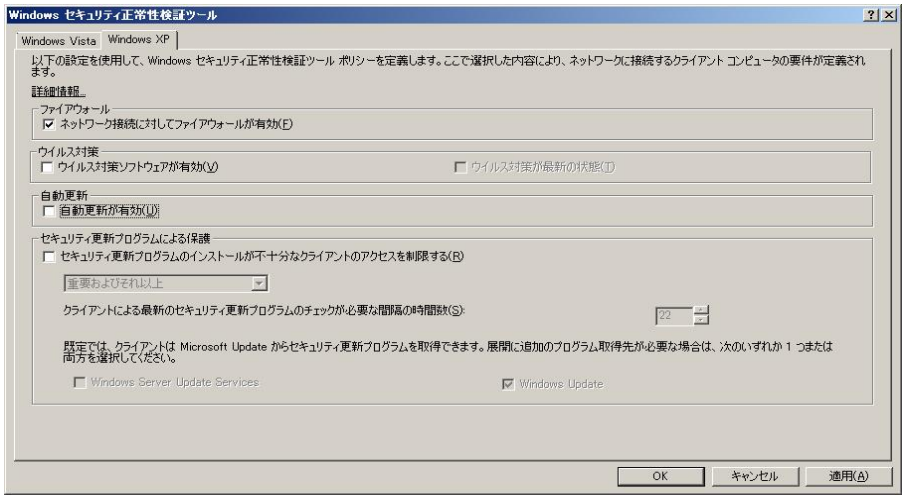
② Windows セキュリティ正常性検証ツールのプロパティ画面にて、「構成」をクリックする。



③ Windows セキュリティ正常性検証ツール画面にて、「Windows Vista」タブの「ファイアウォール」にのみチェックする。



④ 同様に「Windows XP」タブの「ファイアウォール」のみにチェックする。



以上で NPS の設定は終了です。

3.5.3. DHCP サーバの設定

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 3.5-1 DHCP の設定内容（検疫合格時）

	クライアント用 VLAN10	クライアント用 VLAN20	クライアント用 VLAN30
アドレス範囲	192.168.10.51～ 192.168.10.100	192.168.20.51～ 192.168.20.100	192.168.30.51～ 192.168.30.100
サブネット マスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルト ゲートウェイ	192.168.10.254	192.168.20.254	192.168.30.254
DNS サーバ	10.51.0.1		
ドメイン名	example.co.jp		

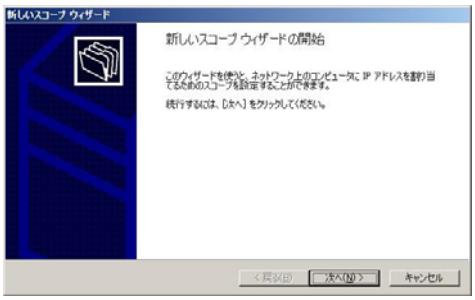
表 3.5-2 DHCP の設定内容（検疫不合格時）

		クライアント用 VLAN10	クライアント用 VLAN20	クライアント用 VLAN30
デフォルト ゲートウェイ		なし		
DNS サーバ		10.51.0.1		
ドメイン名		limit10.example.co.jp	limit20.example.co.jp	limit30.example.co.jp
DHCPサーバへのstatic経路(*1)	宛先	10.51.0.1/32	10.51.0.1/32	10.51.0.1/32
	nexthop	192.168.10.254	192.168.20.254	192.168.30.254
修復サーバへの static 経路	宛先	10.52.0.1/32	10.52.0.1/32	10.52.0.1/32
	nexthop	192.168.10.254	192.168.20.254	192.168.30.254

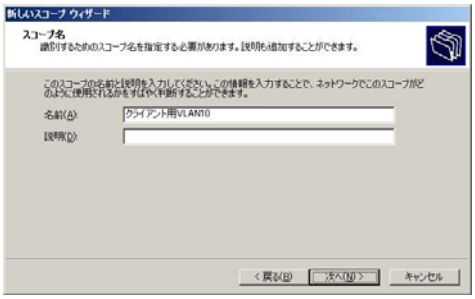
(*1) **構築ポイント（１）**

① 「スタート」→「管理ツール」→「サーバーマネージャ」を開く。
サーバーマネージャ画面にて、左画面の中の「サーバーマネージャ」→「役割」→「DHCP サーバー」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。

② 新しいスコープウィザード画面にて、「次へ」をクリックする。



③ スコープ名
任意の名前（本ガイドでは「クライアント用 VLAN10」）を入力し「次へ」をクリックする。

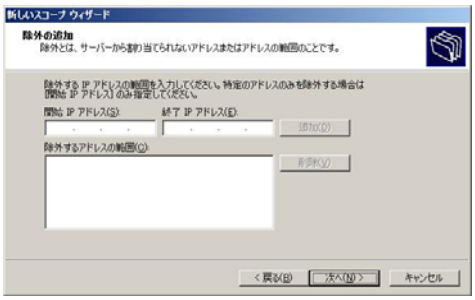


④ IPアドレスの範囲

配布するIPアドレスの範囲（表 3.5-1）を入力し「次へ」をクリックする。

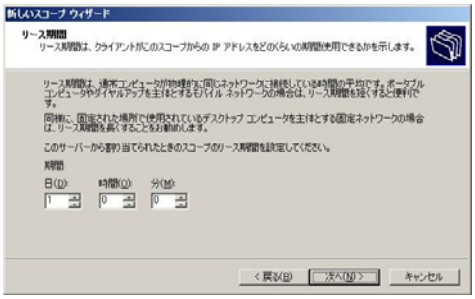
⑤ 除外の追加

「次へ」をクリックする。



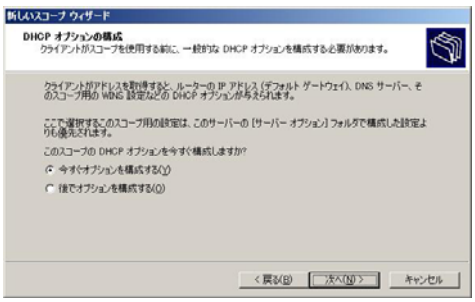
⑥ リース期間

IP アドレスの使用期間（本ガイドでは「1 日」）を入力し、「次へ」をクリックする。



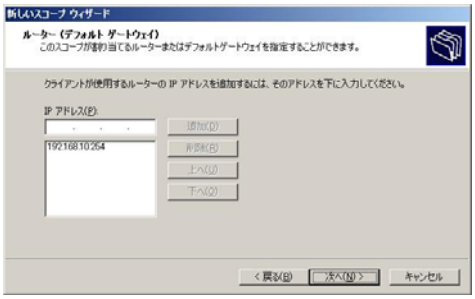
⑦ DHCP オプションの構成

「今すぐオプションを構成する」をチェックし「次へ」をクリックする。



⑧ 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 3.5-1）を入力して「追加」をクリックし、「次へ」をクリックする。

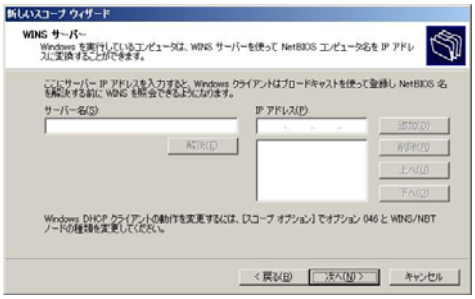


⑨ ドメイン名およびDNSサーバー

DNSサーバの情報（表 3.5-1）を入力し「次へ」をクリックする。

⑩ WINS サーバーの設定

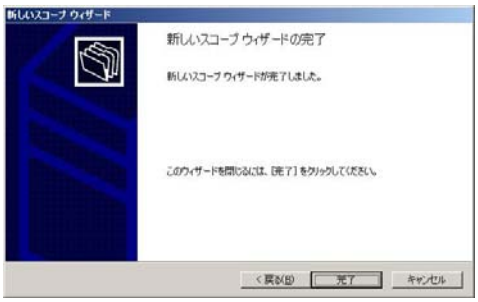
「次へ」をクリックする。



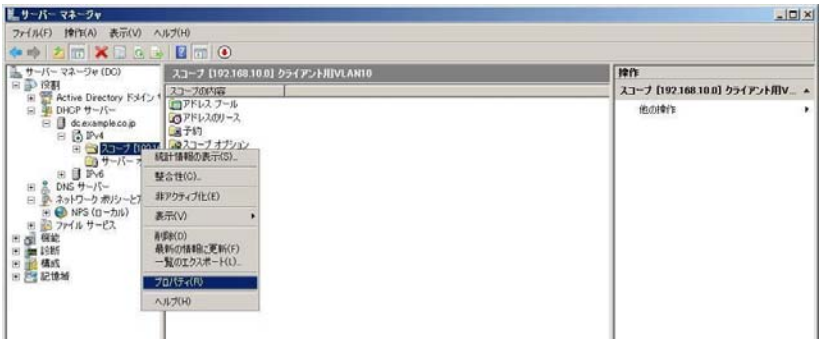
⑪ スコープのアクティブ化

「今すぐアクティブにする」をチェックし「次へ」をクリックする。

⑫ 「完了」をクリックして画面を閉じる。

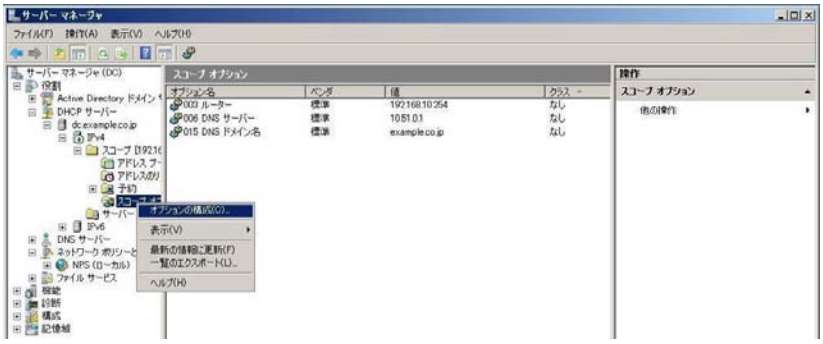


⑬ サーバーマネージャ画面にて、作成したスコープを右クリックしてプロパティを開く。

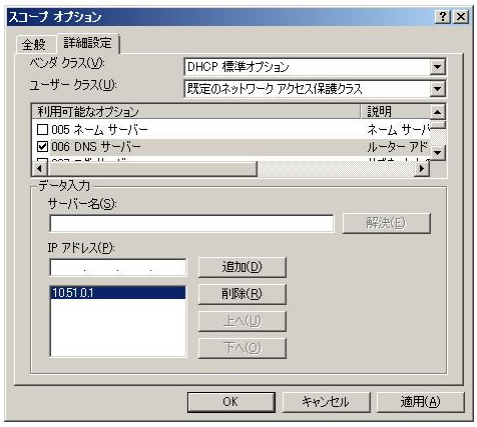


⑭ スコープのプロパティ画面にて「ネットワークアクセス保護」タブを選択し、ネットワークアクセス保護設定で「このスコープに対して有効にする」をチェックし、「OK」をクリックする。

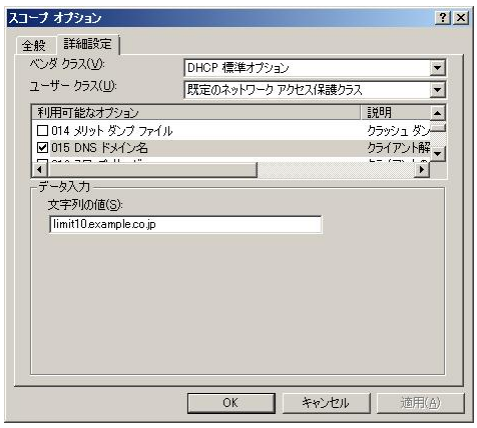
⑮ サーバーマネージャ画面にて、作成したスコープの「スコープオプション」を右クリックして「オプションの構成」を選択する。



⑯ スコープオプション画面にて「詳細設定」タブを選択し、ユーザークラスを「既定のネットワークアクセス保護クラス」に指定する。
利用可能なオプションの「006 DNSサーバー」をチェックし、DNSサーバのIPアドレス（表 3.5-2）を入力する。

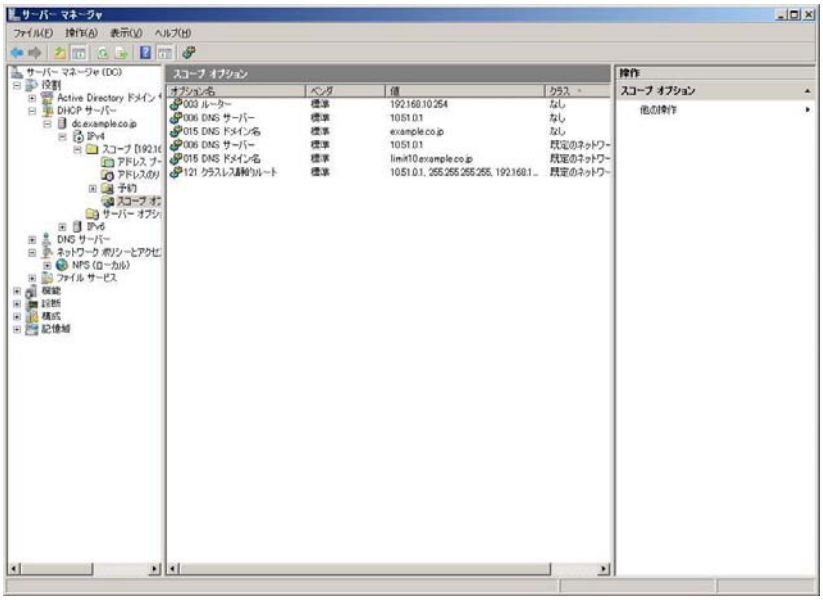


⑰ 「015 DNSドメイン名」をチェックし、ドメイン名（表 3.5-2）を入力する。

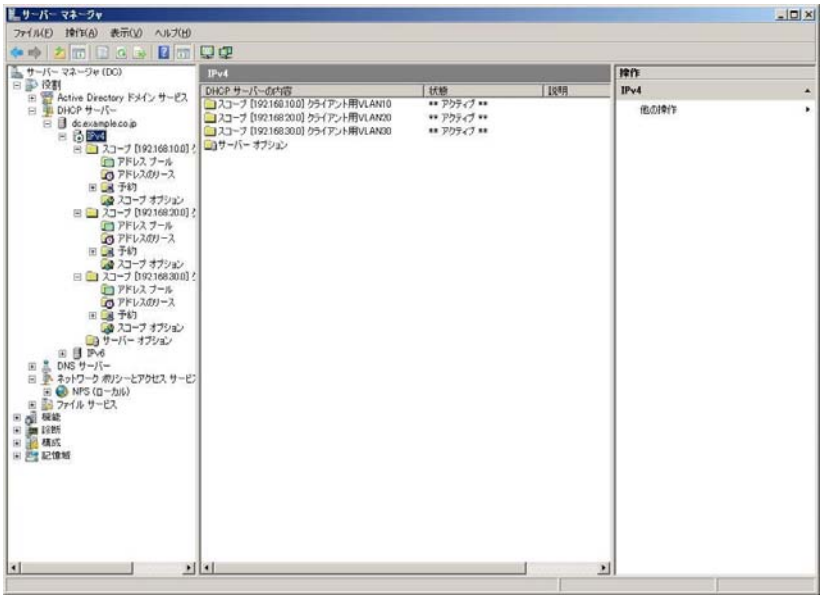


⑱ 「121 クラスレス静的ルート」をチェックし、「ルートの追加」をクリックしてstatic経路（表 3.5-2）を入力する。最後に「OK」をクリックして画面を閉じる。

⑲ サーバマネージャ画面にて、設定したスコープオプションを確認する。



⑳ ①～⑱と同様に「クライアント用VLAN20」および「クライアント用VLAN30」のスコープを作成する。



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

Windows Vista および Windows XP SP3 について、NAP クライアント設定を手動で行う方法を示します。なお、Active Directory のグループポリシーを用いると、サーバ側で NAP クライアント設定を一括して行うこともできます。グループポリシーの設定については、「AX シリーズ NAP ソリューションガイド（IEEE802.1X 認証編）」をご参照ください。

3.6.1. Windows Vista の設定

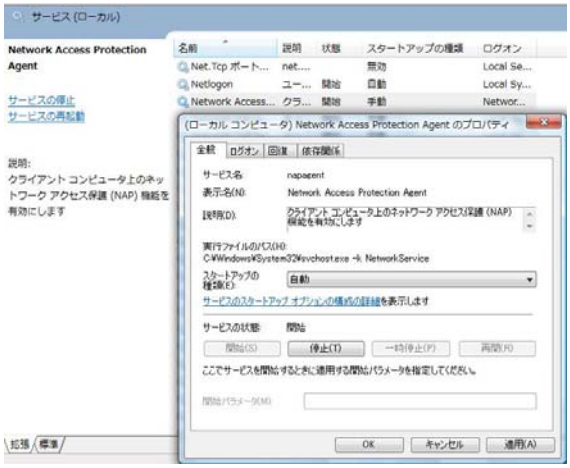
Windows Vista の NAP クライアント設定ステップを以下に示します。

（１） NAP Agentサービスの有効化
（２） セキュリティセンターとDHCP実施クライアントの有効化

なお、本設定はコンピュータの管理者権限のあるユーザで行ってください。

（１） NAP Agent サービスの有効化

① 「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」から「サービス」を開く。
「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。



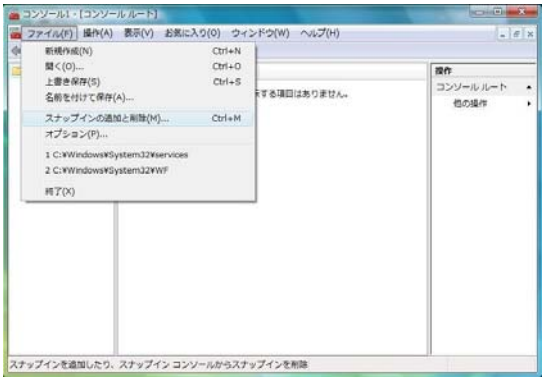
② サービスの画面を閉じる。

（2） セキュリティセンターと DHCP 実施クライアントの有効化

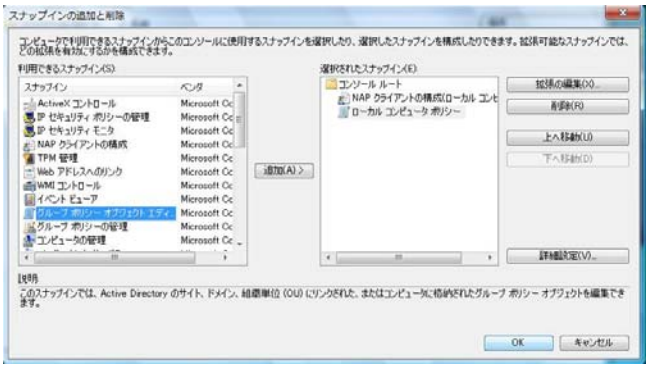
① MMC スナップインの追加

「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。

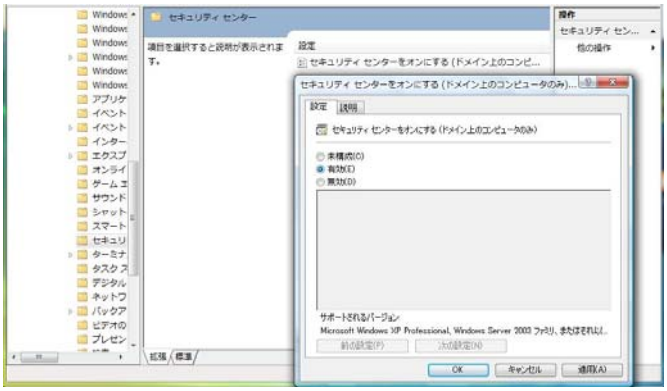
コンソール 1 の画面にて、「ファイル」→「スナップインの追加と削除」を選択する。



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。

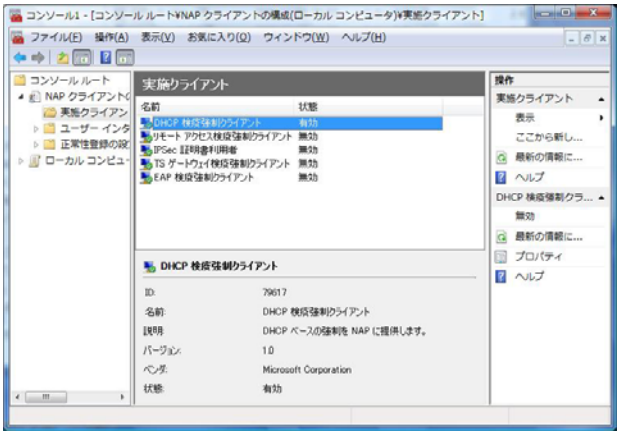


③ コンソール 1 の左画面にて、「コンソールルート」→「ローカルコンピュータポリシー」→「コンピュータの構成」→「管理用テンプレート」→「Windows コンポーネント」→「セキュリティセンター」を選択する。右画面の「セキュリティセンターをオンにする（ドメイン上のコンピュータのみ）」を右クリックしてプロパティを選択し、「有効」をチェックする。



④ 「OK」をクリックして画面を閉じる。

⑤ 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「DHCP 検疫強制クライアント」を右クリックして「有効」にする。



以上で設定は完了です。

3.6.2. Windows XP SP3 の設定

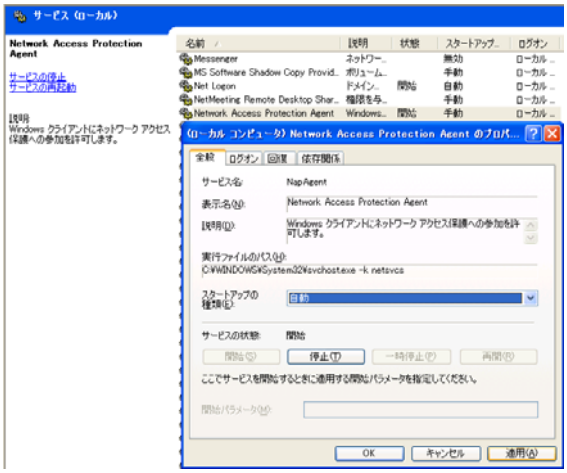
Windows XP SP3 の NAP クライアント設定ステップを以下に示します。

（１） NAP Agentサービスの有効化
（２） セキュリティセンターの有効化
（３） DHCP実施クライアントの有効化

なお、本設定はコンピュータの管理者権限のあるユーザで行ってください。

（１） NAP Agent サービスの有効化

① 「スタート」→「コントロールパネル」→「管理ツール」から「サービス」を開く。
「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。



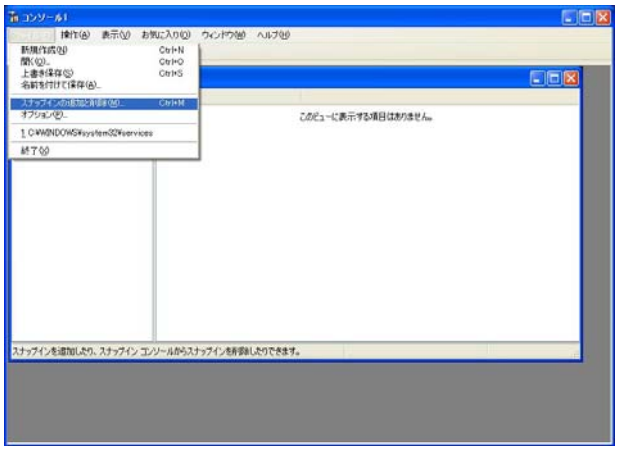
② サービスの画面を閉じる。

（２） 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

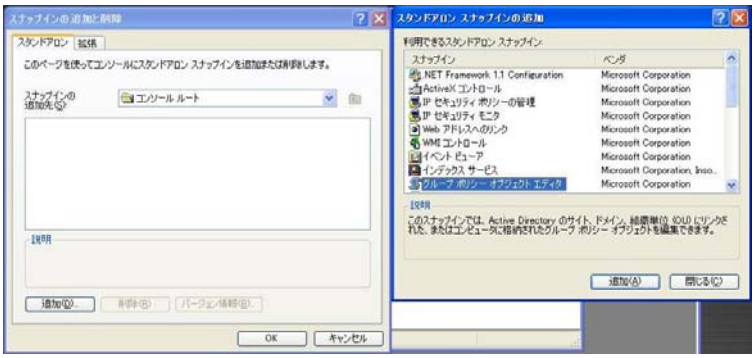
「スタート」→「ファイル名を指定して実行」を開き、「mmc」と入力して MMC（Microsoft Management Consol）を起動する。

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」を選択する。

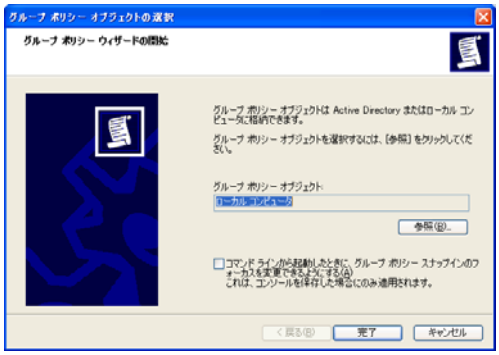


② スナップインの追加と削除の画面にて「追加」をクリックする。

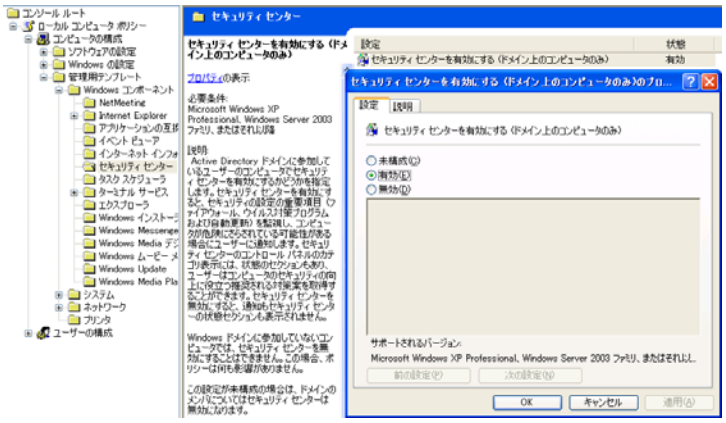
スタンドアロン スナップインの追加画面にて「グループポリシーオブジェクトエディタ」を選択し、「追加」をクリックする。



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。



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。



⑤ 「OK」をクリックして画面を閉じる。

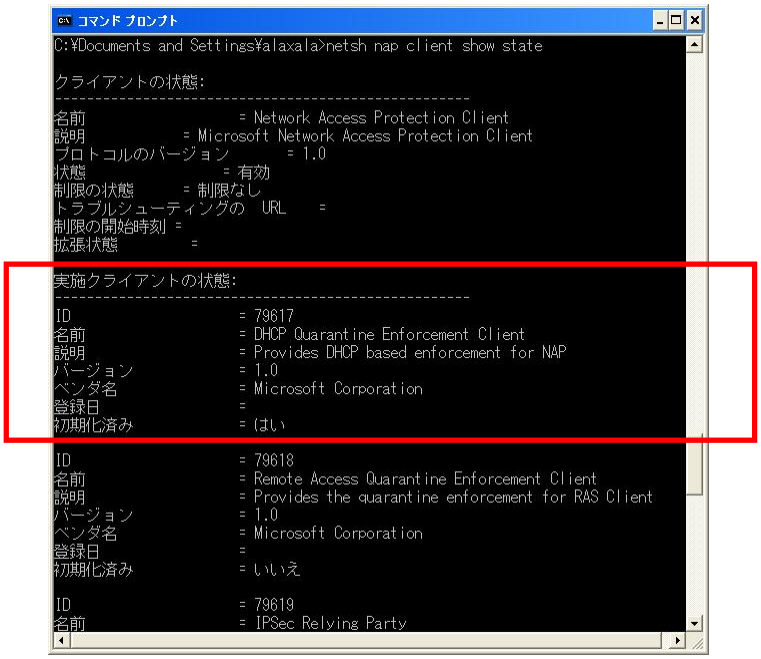
（3） DHCP 実施クライアントの有効化

① コマンドプロンプトを開き、DHCP 実施クライアントを有効化するコマンドを実行する。

```
netsh nap client set enforcement ID = 79617 ADMIN = “ENABLE”
```

② 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「DHCP 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
```



以上で設定は完了です。

3.6.3. 設定の確認

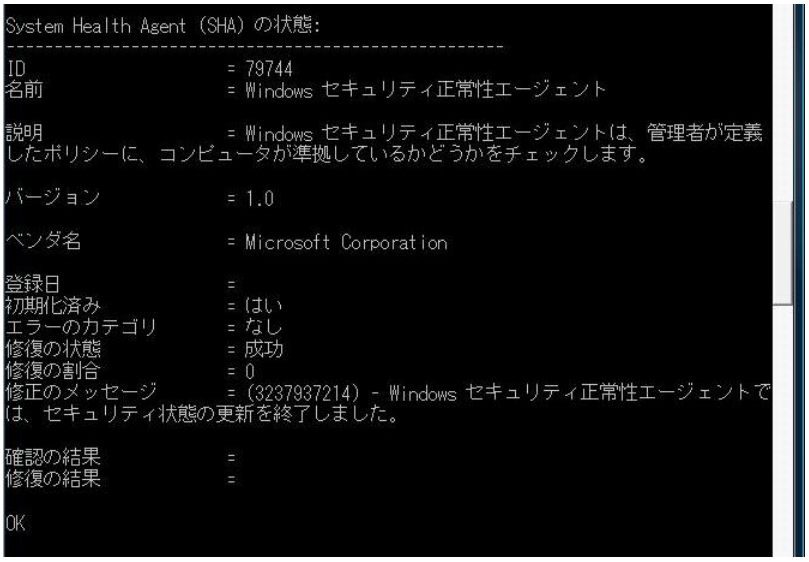
NAP クライアントの設定が完了したことを確認する方法を以下に示します。

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
```

② DHCP 検疫強制クライアントの状態で「初期化済み＝はい」となっていることを確認する。

③ 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。



4. 動作確認

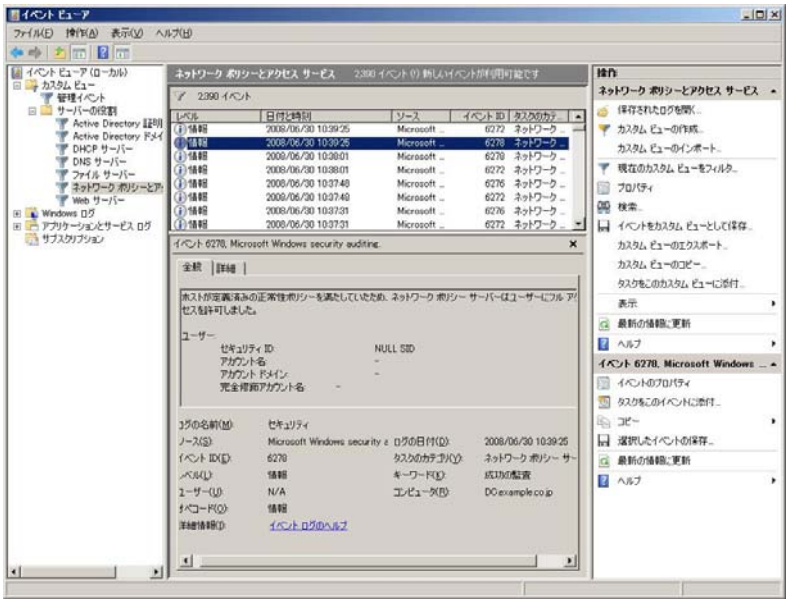
本章では、検疫ネットワークにおける検疫動作の確認方法について示します。

4.1. Windows Server 2008 での確認方法

4.1.1. イベントビューア

NPS による NAP 検疫のログ確認方法を示します。
検疫合否、システムの正常性結果など、多くの情報を確認することができます。

① 「スタート」→「管理ツール」→「イベントビューア」を開く。
イベントビューアの左画面にて「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、ログを確認する。



② 内容を確認したいイベントをダブルクリックして、詳細情報を確認する。

・イベント ID：6278　検疫合格

・イベント ID：6276　検疫不合格

4.2. NAP クライアントでの確認方法

4.2.1. 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不合格した場合、以下のメッセージが表示されます。

図 4.2-1 検疫不合格時のメッセージ

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。

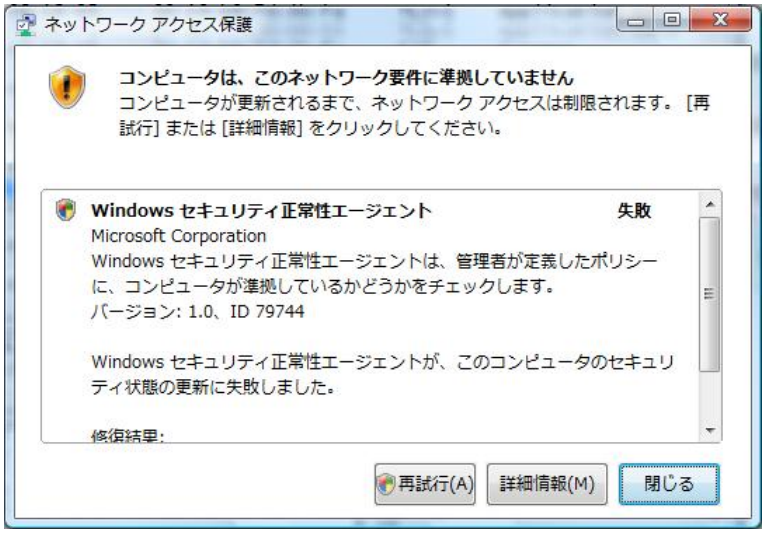


図 4.2-2 検疫不合格時の画面

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合格した場合、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。

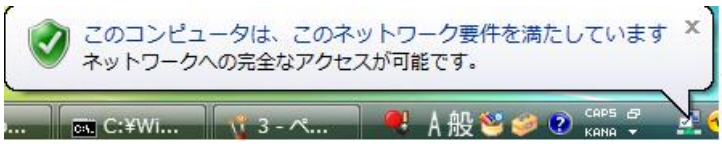


図 4.2-3 検疫合格時のメッセージ

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 4.2-4　検疫合格時の画面

4.2.2. Windows コマンドによる確認

（1） ipconfig

NAP クライアントの IP アドレス情報を表示するコマンドです。検疫の結果に応じた IP アドレスを取得しているかを確認することができます。「/all」オプションを付けると詳細情報が確認できます。

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。

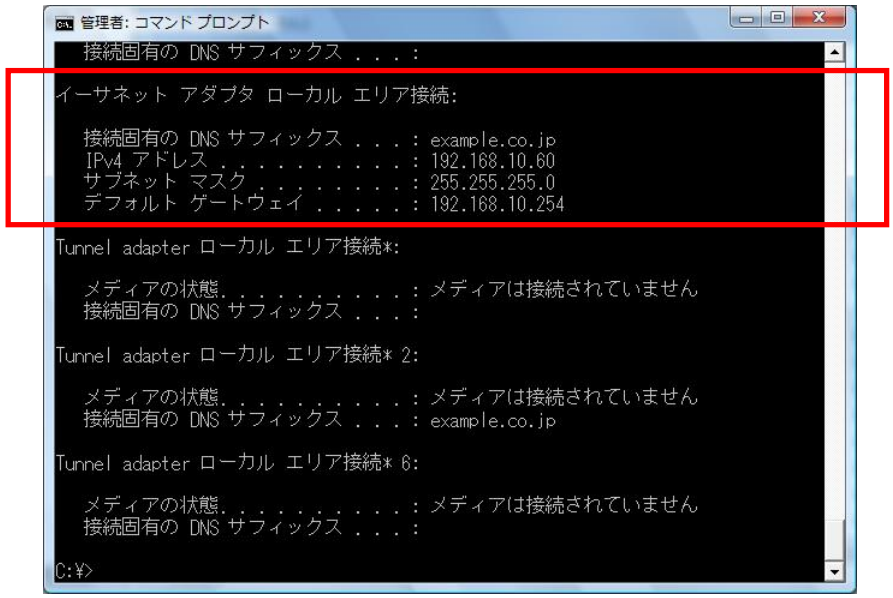


図 4.2-5 検疫合格時の ipconfig 結果

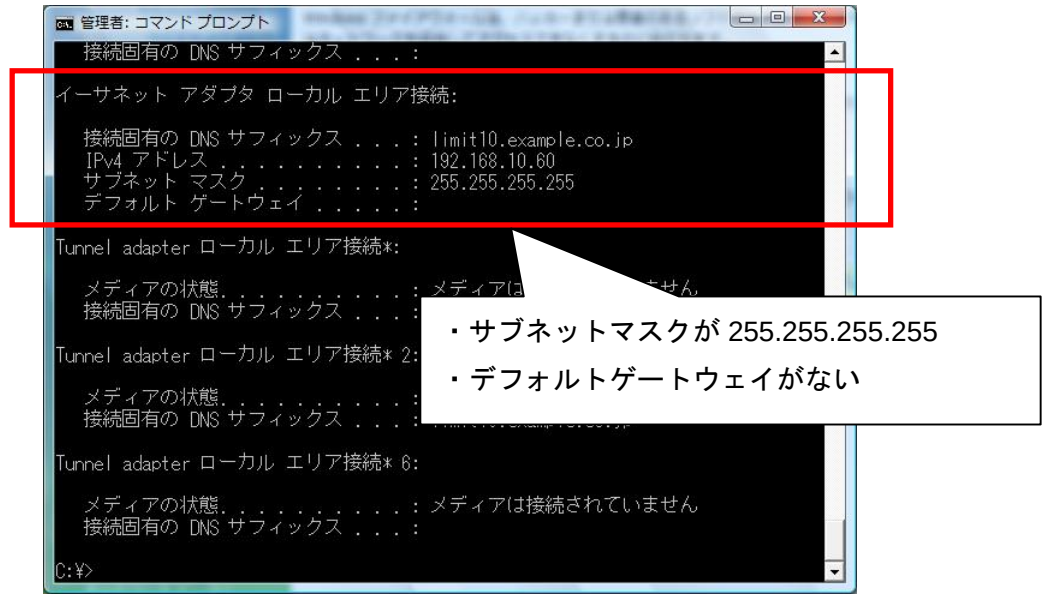


図 4.2-6 検疫不合格時の ipconfig 結果

（２） route print

NAP クライアントが保持する経路情報を表示するコマンドです。

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。

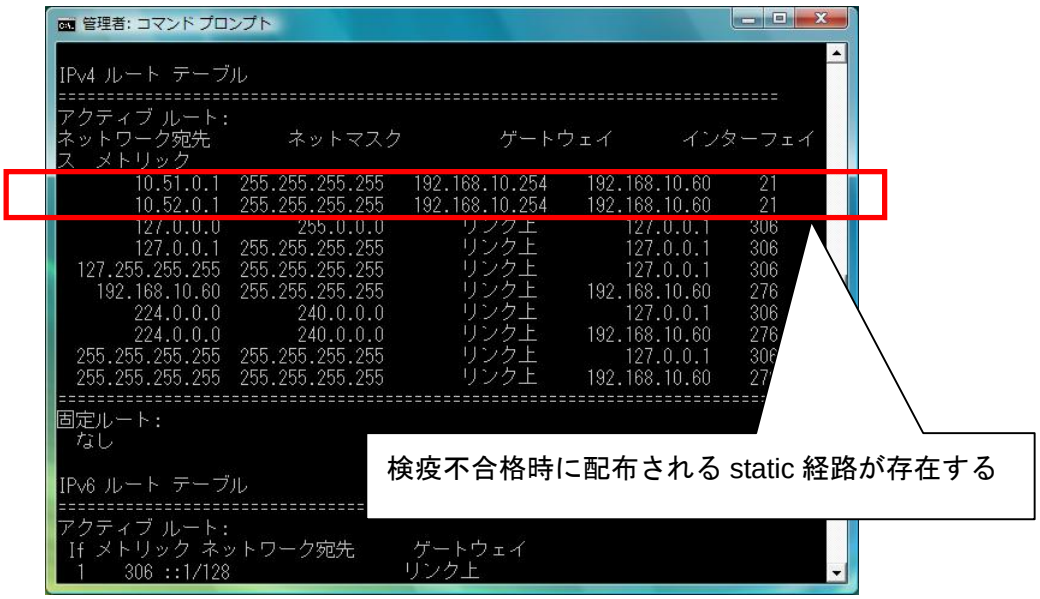


図 4.2-7 検疫不合格時の route print 結果

（３） 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。(コマンド実行例は3.6.3を参照)

4.3. AX シリーズの運用コマンド

4.3.1. show ip dhcp snooping binding

AX シリーズにおける DHCP snooping の状態表示コマンドです。
バインディングデータベースに登録されている端末を確認することができます。バインディングデータベースに登録されていない端末は通信ができません。

```
> sh ip dhcp snooping binding

Date 2008/06/09 19:22:13 JST

Agent URL: flash
Last succeeded time: -

Total Bindings: 2
MAC Address     IP Address      Expire(min) Type     VLAN  Interface
0019.b97d.46c7  192.168.20.51   11514       dynamic  20    fastethernet    0/13
001e.c965.cf5c  192.168.10.52   11520       dynamic  10    fastethernet    0/1
```

バインディングデータベースに端末が登録されていない場合、クライアント端末側で IP アドレスの再取得を行ってください。

5. 注意事項

5.1. 検疫除外端末を接続する場合

プリンタなどのNAP非対応クライアントを検疫ネットワークに接続する場合、AX1200Sのバインディングデータベースに端末のMACアドレス、IPアドレス、VLAN IDおよび接続するポート番号を登録することで、検疫を行わず通信できるようになります。（設定方法は3.4.1.（３）を参照）このとき、クライアントには必ず固定IPアドレスを設定してください。DHCP設定では通信できません。

検疫を除外したいDHCPクライアントを接続する場合は、DHCP方式のNAPを実施しない別のVLANを作成する必要があります。

5.2. 検疫不合格時に配布する static 経路について

検疫不合格時には、修復サーバへのstatic経路のほかに、DHCPサーバへのstatic経路を必ず配布してください。（設定方法は3.5.3を参照）

クライアントはセキュリティ状態が変化すると、検疫情報を格納した DHCP リクエストパケットを DHCP サーバへ送信しますが、DHCP サーバから応答がない場合、DHCP Discover パケットをブロードキャスト送信して DHCP シーケンスを最初から開始します。このため、検疫処理および IP アドレス再取得に時間がかかってしまいます。

5.3. DHCP snooping のバインディングデータベース保存について

DHCP snooping機能が管理するバインディングデータベースは、コンフィグレーションコマンドで保存先を指定しておいてください。デフォルト動作では、装置が再起動すると全データが消去されるので、既にIPアドレスを取得している端末は、再度IPアドレスを取得しない限り通信不可となってしまいます。設定方法は3.4.1（３）を参照してください。

付録A. コンフィグレーション

図 3.2-1のネットワーク構成図における各装置の全コンフィグレーションを、テキスト形式の添付ファイルで示します。各コンフィグレーションを参照する場合は、以下に示すファイル名と同じ名前の添付ファイルを開いてください。

A.1. AX1230S のコンフィグレーション

A-1_edge1_config.txt

A.2. AX3630S のコンフィグレーション

A-2_core1_config.txt

※ PDF 文書にて添付ファイルを開く場合は、Adobe Reader 7 以上を使用してください。Adobe Reader メニューバーの「表示」→「ナビゲーションパネル」→「添付ファイル」クリックで添付ファイル一覧が表示されます。

2008 年 7 月 18 日　初版発行

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 890 番地 新川崎三井ビル西棟
http://www.alaxala.com/