AX シリーズ
検疫ソリューションガイド
（JP1 編）

JP1 Version 9

第 2 版

はじめに

本ガイドは、株式会社 日立製作所製の JP1 と AX シリーズ（AX1200S / AX2400S / AX3600S）でサポートしている認証機能を用いた検疫ネットワーク構築の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 製品マニュアル（http://www.alaxala.com/jp/techinfo/manual/index.html）
- RADIUS サーバ設定ガイド（Windows Server 2003 編 及び Windows Server 2008 編）
- JP1Ver9 JP1/NETM/DM 構築ガイド
- JP1Ver9 JP1/NETM/DM 運用ガイド
- JP1Ver9 JP1/NETM/Asset Information Manager 運用ガイド
- JP1Ver9 JP1/NETM/Client Security Control 解説・手引・操作書

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 ソフトウェアバージョンは以下のようになっております。

AX1200S	Ver2.2.A
AX2400S / AX3600S	Ver11.4

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下さい。

商標一覧

- JP1 は、株式会社日立製作所の日本における商品名称(商標又は、登録商標)です。
- 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

- AX1240S (Ver2.2.C), AX2430S (Ver11.4) , AX3630S (Ver11.4)
- Windows Server 2003 , Windows Server 2008
- Windows XP(SP2,SP3),Windows Vista SP1, Windows 7

検疫ソフトウェア一覧

- JP1/NETM/DM Manager (Ver09-01)
- JP1/NETM/Asset Information Manager (Ver09-01) 本資料では JP1/NETM/AIM と表記
- JP1/NETM/Client Security Control - Manager (Ver09-01) 本資料では JP1/NETM/CSC-Manager と表記
- JP1/NETM/Client Security Control - Agent (Ver09-01) 本資料では JP1/NETM/CSC-Agent と表記
- JP1/NETM/DM Client (Ver09-01)

改訂履歴

版数	rev.	日付	変更内容	変更箇所
初版	―	2009.1.20.	初版発行	―
第 2 版	―	2010.7.2.	使用機器一覧更新	―
			検疫ソフトウェア Ver 更新	―
			対応クライアント追加	表 1.1-3
			対応 OS 情報追加	表 1.1-4
			AX スイッチ設定修正（AX1240S の設定追加および最新 OS への対応による見直し）	3.4

目次

1. JP1 の検疫システム概要 5

1.1. JP1 の検疫システムについて 5
1.1.1. JP1 の検疫システムの特徴 5
1.1.2. JP1 の検疫システム動作概要 5
1.1.3. JP1 の検疫関連機能 6
1.2. AXとJP1 の連携 8
1.2.1. AXスイッチとJP1 の連携概要 8
1.2.2. JP1/NETM/CSCとRADIUSサーバの連携動作 9
1.2.3. 連携するAXスイッチの認証方式ごとの特徴 10
1.2.4. 検疫時間について 10

2. JP1 と連携可能なAXシリーズの認証方式と収容条件 11

2.1. AXシリーズの最大認証端末数を以下に示します。 11

3. 検疫ネットワークの構築 12

3.1. 概要 12
3.2. 検疫ネットワーク構成図 13
3.3. 構築ポイント 15
3.4. AXの設定 16
3.4.1. AX1200Sのコンフィグレーション 16
3.4.2. AX2400Sのコンフィグレーション 19
3.4.3. AX3600Sのコンフィグレーション 22
3.5. サーバの設定 23
3.5.1. 事前準備 23
3.5.2. RADIUSサーバ連携設定 25
3.5.3. ポリシー管理設定 27
3.6. クライアントPCの設定 35
3.6.1. インストール時の設定 35
3.6.2. インストール後の設定 37
3.7. 検疫除外端末の接続方法 39

4. 動作確認方法 41

4.1. AXにおける動作確認 41
4.1.1. show dot1x detail 41
4.1.2. show dot1x logging 41
4.1.3. clear dot1x auth-state 41
4.1.4. show mac-authentication login 42
4.2. 検疫サーバにおける動作確認 43

5. 注意事項 46

5.1. 検疫ポリシーの設定について 46
5.2. RADIUSサーバ冗長化について 46
5.3. JP1/NETM/DM Clientの設定について 46
5.4. IEEE802.1X認証の再接続について 46
5.5. 認証スイッチの再認証時間の設定について 47

付録A. コンフィグレーション 47

A.1. AX1200Sのコンフィグレーション 47
A.2. AX2400Sのコンフィグレーション 47
A.3. AX3600Sのコンフィグレーション 47

1. JP1 の検疫システム概要

1.1. JP1 の検疫システムについて

1.1.1. JP1 の検疫システムの特徴

- JP1 の統制機能によりクライアント PC のセキュリティポリシーを強制的に設定できます。
- 資産管理･配布機能によるクライアントPCのハードウェア情報収集およびインストールされたソフトウェア情報の収集と配布ができます。
- 認証スイッチまたは JP1/NETM/Network Monitor と連携する事でポリシーに適合しないクライアント PC に対しネットワーク接続を制限できます。
- 認証スイッチまたは JP1/NETM/Network Monitor と連携する事で JP1/NETM/DM Client を導入しないクライアント PC の接続を制限できます。

1.1.2. JP1 の検疫システム動作概要

認証スイッチを用いた JP1 の検疫システムでは、JP1/NETM/DM Client 導入 PC の検疫と、未導入 PC の業務ネットワークへの接続を制限することができます。JP1 とアラクサラの AX シリーズ認証スイッチを連携した検疫システムの概要を図 1.1-1 に示し、クライアント PC の検疫から通信まで一連の流れを以下に示します。

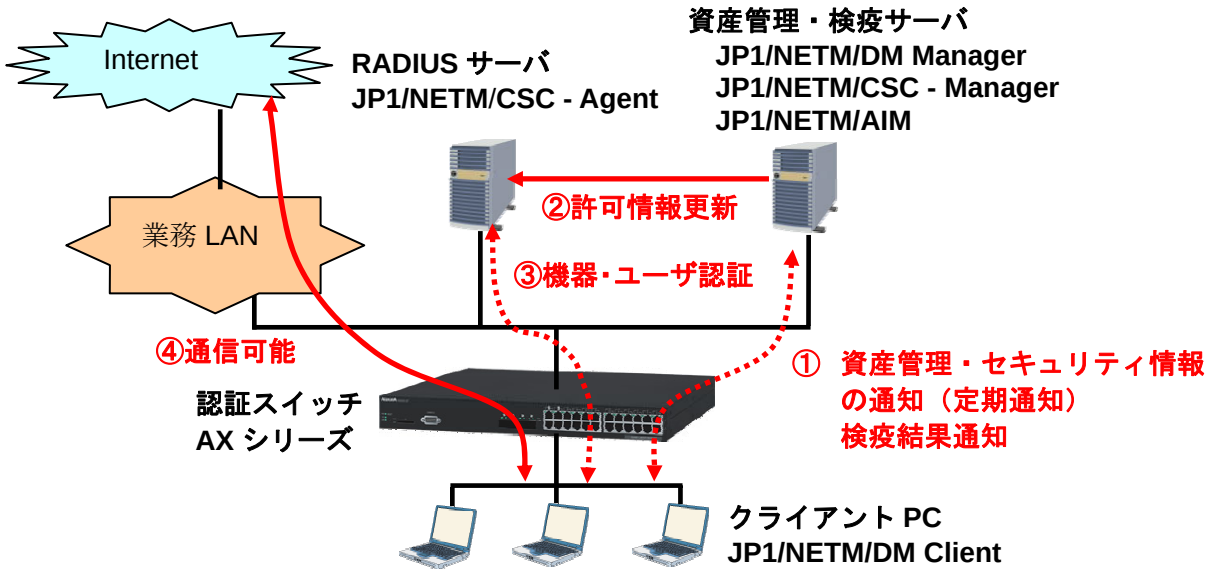

図 1.1-1 検疫システム概要

① JP1/NETM/DM Clientから資産管理・セキュリティ対策などの情報を収集し検疫を実行します。
② RADIUSサーバ上のJP1/NETM/CSC - Agentへ検疫結果を更新し認証を制御します。
③ ユーザまたは機器の認証を実施し検疫結果に応じたネットワーク制御を実行します。
④ 検疫に成功したクライアント PC のみ通信可能となります。

1.1.3. JP1 の検疫関連機能

JP1 で実施可能な検疫項目を表 1.1-1　検疫項目に示します。

表 1.1-1 検疫項目

機能名	機能詳細
Windows セキュリティパッチチェック	Windows セキュリティパッチが適用されているかチェックする機能
ウイルス対策ソフトチェック	ウイルス対策ソフトのインストールおよびパターンファイルをチェックする機能 ウイルス対策ソフトについては以下のベンダに対応 トレンドマイクロ、シマンテック、マカフィー、マイクロソフト
禁止ソフトチェック	クライアント PC に禁止ソフトがインストールされていないかチェックする機能
必須ソフトウェアチェック	必須ソフトが導入されているかチェックする機能
その他設定チェック	Windows　Firewall　適用、 Windows セキュリティパッチの自動更新、スクリーンセーバーのパスワード保護など

JP1 のセキュリティ関連機能を表 1.1-2　セキュリティ関連機能に示します。

表 1.1-2 セキュリティ関連機能

機能名	機能詳細
資産管理情報の収集と管理	資産管理情報として、H/W 情報、インストールソフトウェア、セキュリティ対策情報の収集し管理することが出来ます。
セキュリティ関連の設定	Windows アップデートや WSUS サーバグループの制御など
ソフトウェアの配布	ソフトウェアの配布機能

検疫対応クライアントを表 1.1-3　対応クライアント環境に示します

表 1.1-3 対応クライアント環境

項目	サポート OS
検疫可能クライアント OS	Windows　7 Windows　Vista Windows　XP Windows　2000　（IEEE802.1X 連携は SP4 以降） Windows　Server 2008 R2 Windows　Server 2008 Windows　Server 2003

認証スイッチと連携した JP1 の検疫システム構築に必要な JP1 コンポーネントを表 1.1-4　検疫システムに必要な JP1 コンポーネントに示します。

表 1.1-4 検疫システムに必要な JP1 コンポーネント

	コンポーネント名	機能
資産管理・検疫サーバ	JP1/NETM/DM Manager	資産管理ソフトウェア配布マネージャ
	JP1/NETM/AIMまたは JP1/NETM/AIM Limited	セキュリティ管理を含めた統合資産管理マネージャ
	JP1/NETM/CSC – Manager	クライアントセキュリティ管理マネージャ
RADIUSサーバ	JP1/NETM/CSC – Agent	RADIUSサーバと連携して認証を制御
クライアントPC	JP1/NETM/DM Client	資産管理ソフトウェア配布クライアント

※ RADIUS サーバは Windows Server 2003 および Windows Server 2008 に対応、但し x64 Edition には対応していません。

※ 資産管理・検疫サーバは Wendows Server 2003,Windows Server 2008,Winodows Server 2008 R2 で使用できます。

1.2. AX と JP1 の連携

1.2.1. AX スイッチと JP1 の連携概要

JP1/NETM/DM、JP1/NETM/CSC-Manager を導入すると PC に対して、資産管理情報の収集とセキュリティにかかわる設定を管理者から行うことが可能となり、セキュリティポリシーに適合しない PC に対して警告メッセージを強制的に表示することができますが、JP1/NETM/DM Client を導入していない PC の業務ネットワーク接続制御に関しては、JP1/NETM/Network Monitor を導入するか、JP1 と連携可能な認証スイッチを導入する必要があります。

AX スイッチの **IEEE802.1X 認証**または **MAC 認証**と JP1 が連携することで、JP1/NETM/DM Client を導入していないクライアント PC やセキュリティポリシーに違反しているクライアント PC に対して業務ネットワークへの接続を排除する検疫ネットワークを構築できます。

AX スイッチの認証機能との連携の概要を図 1.2-1 で説明します。JP1/NETM/DM Client 導入のクライアント PC は定期的に資産管理サーバへの資産管理情報を更新しており、通知された情報を元に JP1/NETM/CSC - Manager が検疫を実施して、安全な PC のみ RADIUS サーバ上で動作する JP1/NETM/CSC - Agent に許可情報を更新します。
RADIUS サーバは検疫成功したクライアント PC のみ認証を許可するため、AX スイッチの認証機能と連携することで JP1/NETM/CSC - Manager で検疫に成功した PC のみが業務ネットワークへ通信できるようになります。

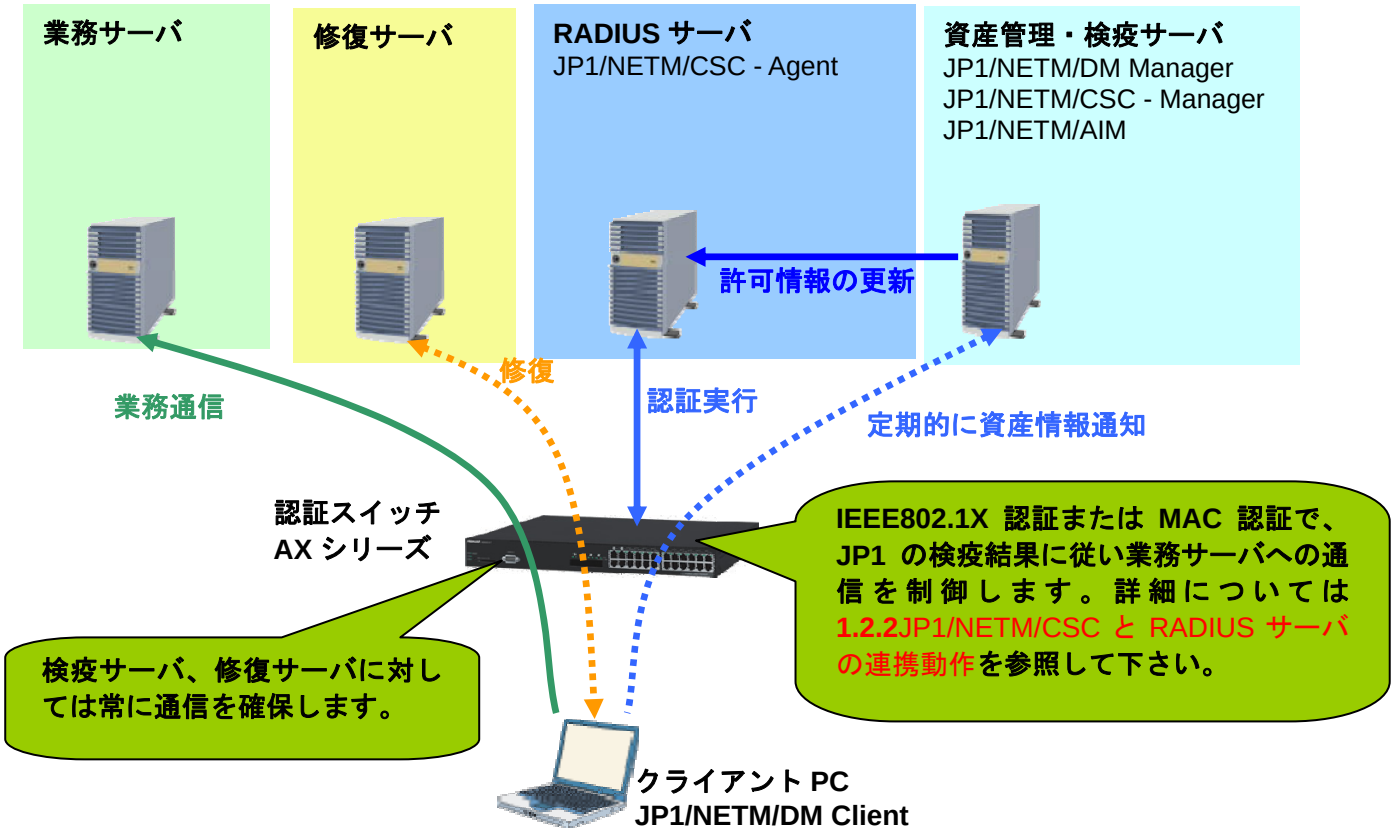

図 1.2-1 JP1 と AX の検疫連携のしくみ

ネットワーク認証（MAC 認証または IEEE802.1X 認証）の設定のほかに資産管理サーバへの認証前アクセスリストの設定を AX スイッチに行う必要があります。
また検疫に失敗したクライアント PC を修復するためのソフトウェアや Windows パッチを配布する WSUS サーバなどの修復サーバを用意する場合も AX スイッチの認証前アクセスリストに登録します。

1.2.2. JP1/NETM/CSC と RADIUS サーバの連携動作

JP1/NETM/CSC - Manager は JP1/NETM/DM Manager と連携して、クライアント PC から収集したインベントリ（資産管理情報）が設定されたセキュリティーポリシーに準拠しているか判定します。
その後 JP1/NETM/CSC-Manager はクライアント PC の判定結果を RADIUS サーバ上の JP1/NETM/CSC - Agent が持つ接続制御リスト（「図 1.2-2　接続制御」の太枠部分）に反映します。
接続制御リストにはクライアント PC の MAC アドレスをキー情報としたネットワーク接続の許可、拒否の情報が記載されていて、RADIUS サーバは接続制御リストの情報を元にクライアント PC からネットワーク認証に応答します。

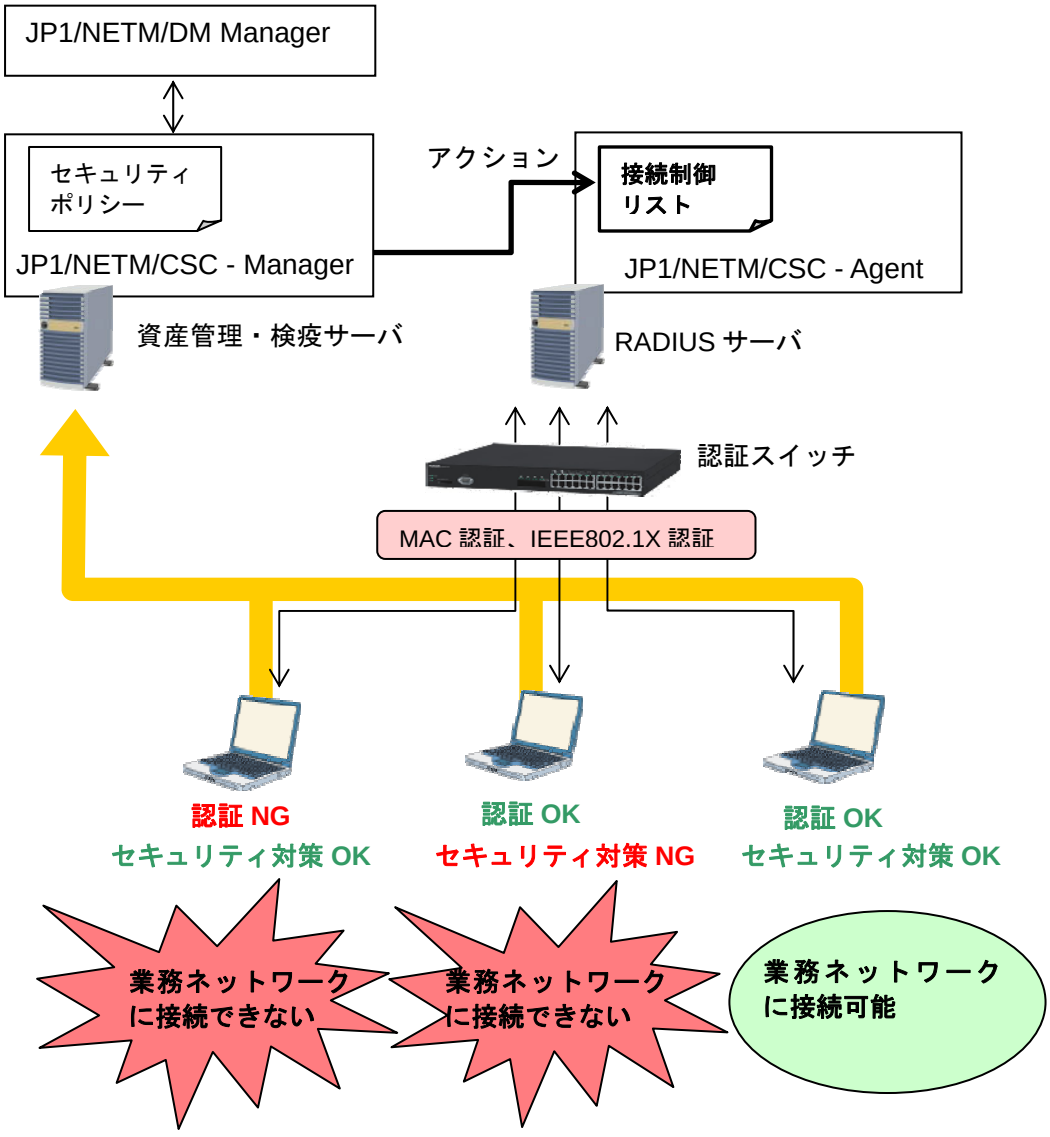

図 1.2-2 接続制御リスト

プリンタなど検疫除外したい端末を認証ポートに接続するには JP1/NETM/CSC - Agent の接続制御リストを手動で編集し登録することにより業務ネットワークへの接続が可能となります。
検疫除外端末の登録方法は 3.7検疫除外端末の接続方法を参照して下さい。

1.2.3. 連携する AX スイッチの認証方式ごとの特徴

AX スイッチが JP1 の検疫システムと連携できる認証方式には IEEE802.1X 認証と MAC 認証があり、それぞれの特徴を表 1.2-1　認証方式ごとの特徴に示します。

表 1.2-1 認証方式ごとの特徴

認証方式	JP1 の検疫システムと連携した際の特徴
IEEE802.1X 認証	・ユーザ ID とパスワードか証明書によるユーザ認証。 ・検疫とユーザ認証両方実施したい場合に選択します。 ・ユーザが認証の設定を行う必要があります。
MAC 認証	・登録された機器の MAC アドレスで認証。 ・ユーザ側で認証の設定を行う必要はありません。

利用者の認証とクライアント PC の検疫の両方を実施したい場合は IEEE802.1X 認証方式、機器認証のみ実施する場合は MAC 認証方式でシステムを導入できます、いずれの場合においても、JP1/NETM/DM Client を導入し検疫に成功したクライアント PC か、管理者が特別に許可したクライアント PC のみ業務ネットワークへの接続を許可します。

1.2.4. 検疫時間について

AX スイッチと JP1 の検疫システムの連携における検疫時間について以下に示します。

表 1.2-2 検疫に関わる時間

項目	時間と解説
検疫済み PC のネットワーク接続開始時間（通常運用時）	通常運用において前回接続時のセキュリティ対策 OK のクライアント PC は即座に業務ネットワークに接続可能です。
新規登録ＰＣのネットワーク接続開始時間	新規登録時には、JP1/NETM/DM Client をインストール後に再起してから約 20 分で業務ネットワークに接続可能となります。 （資産登録情報がサーバへ全て通知が完了し安全が確認されるまで約 20 分程度かかります、クライアント PC の性能やインストールされたソフトウェアの量でさらに長くなる場合があります。）
検疫時間 （前回接続時に検疫を通過した PC をセキュリティ対策 NG 状態で接続した場合に業務 LAN から排除されるまで）	一旦業務ネットワークに接続され、PC 起動から約 15 分で業務ネットワークから切り離されます。 （セキュリティ対策 NG の場合にメッセージが表示されます）
業務復帰時間 （セキュリティ対策 NG の PC が、修復後業務 LAN に復帰 するまで）	一旦業務ネットワーク接続を排除された PC は、対策後 PC 再起動から約 15 分で業務ネットワークに復帰できます。 （“安全になりました” が表示されます） IEEE802.1X 認証の場合手動で再接続を実施する必要があります。
接続許可 PC の有効期間	検疫安全を確認したクライアント PC は管理者が設定した期間接続がない場合に再度検疫しなければ接続を許可しないように出来ます。 設定により任意に指定可能です。

（表内で示す時間は 3検疫ネットワークの構築の設定条件に従い本システムを構築した場合の測定値です。）

新規登録時と検疫失敗になった場合、業務ネットワークへの接続に時間がかかるため注意が必要です。
5.1検疫ポリシーの設定についてを参照下さい。

2. JP1 と連携可能な AX シリーズの認証方式と収容条件

2.1. AX シリーズの最大認証端末数を以下に示します。

表 2.1-1 認証方式毎の最大認証端末数

<table>
<tr><th>認証方式</th><th colspan="2">AX1200S</th><th colspan="2">AX2400S
AX3600S</th></tr>
<tr><td rowspan="2">IEEE802.1X
認証</td><td>64／ポート</td><td rowspan="3">合計
1024／装置</td><td>64／ポート</td><td rowspan="3">合計
1024／装置</td></tr>
<tr><td>256／装置</td><td>256／VLAN</td></tr>
<tr><td>MAC 認証</td><td>1024／装置</td><td>1024／装置</td></tr>
</table>

3. 検疫ネットワークの構築

本ガイド **1.2.1**AXスイッチとJP1 の連携概要に記載のとおり、AXスイッチと連携するJP1 の検疫システムでは認証方式にIEEE802.1X認証方式、MAC認証方式のどちらでも構築することが可能です。

本ガイドの構築例では解説のため、認証スイッチに IEEE802.1X 認証ポート、MAC 認証ポート、IEEE802.1X 認証と MAC 認証の混在ポートの 3 パターンの設定例を示しています。
混在ポートについては、検疫を実施するクライアント PC は IEEE802.1X 認証を使用し、検疫除外端末は MAC 認証で登録する運用を想定しています。
5.1検疫ポリシーの設定についてを参照してユーザの環境に合わせた認証方式を選択し設定を行って下さい。また、認証除外端末の登録については **3.7**検疫除外端末の接続方法を参照して下さい。

3.1. 概要

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。

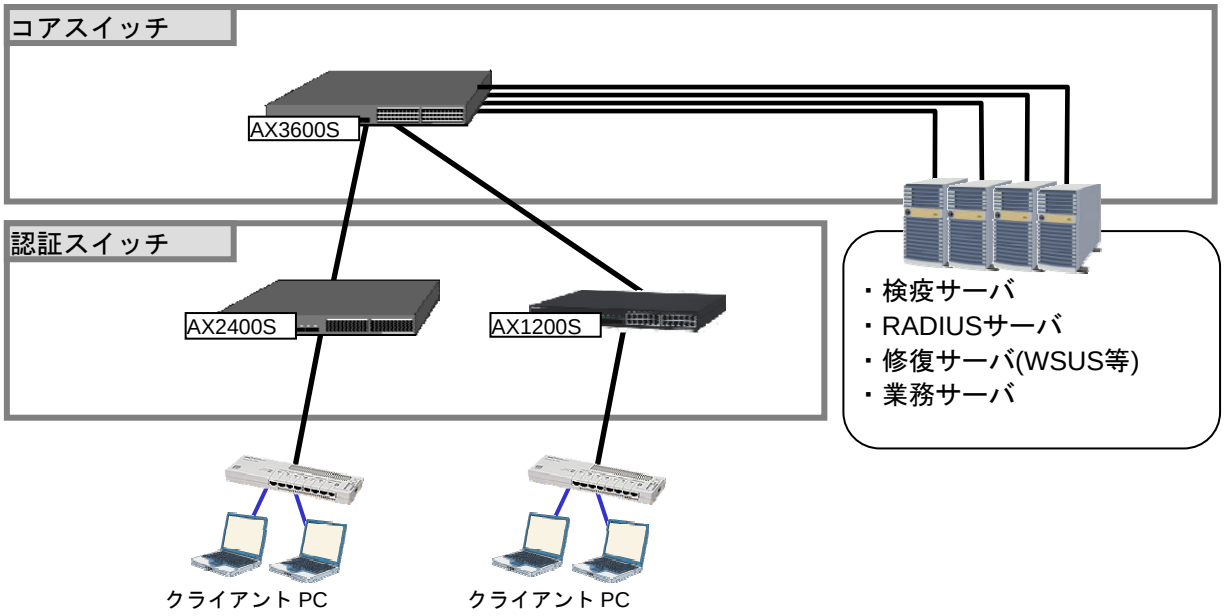

図 3.1-1 検疫ネットワークの基本構成

コアスイッチには AX3600S を配置し、各種サーバをコアスイッチ配下に接続します。
認証スイッチには AX2400S および AX1200S を配置し、検疫を行うクライアント PC を認証スイッチに直接またはハブを介して接続します。

本ガイドで使用するサーバとクライアント PC を以下に示します。

表 3.1-1 サーバとクライアント一覧

検疫サーバ	RADIUS サーバ	クライアント PC
Windows Server 2008 ・**JP1/NETM/DM Manager** ・**JP1/NETM/CSC - Manager** ・**JP1/NETM/AIM**	Windows Server 2008 ・**JP1/NETM/CSC - Agent** ・RADIUS サーバ(NPS) ・ActiveDirectory ドメインコントローラ ・DHCP サーバ	Windows XP ・**JP1/NETM/DM Client** Windows Vista ・**JP1/NETM/DM Client**

3.2. 検疫ネットワーク構成図

検疫ネットワーク構成図（詳細）を以下に示します。

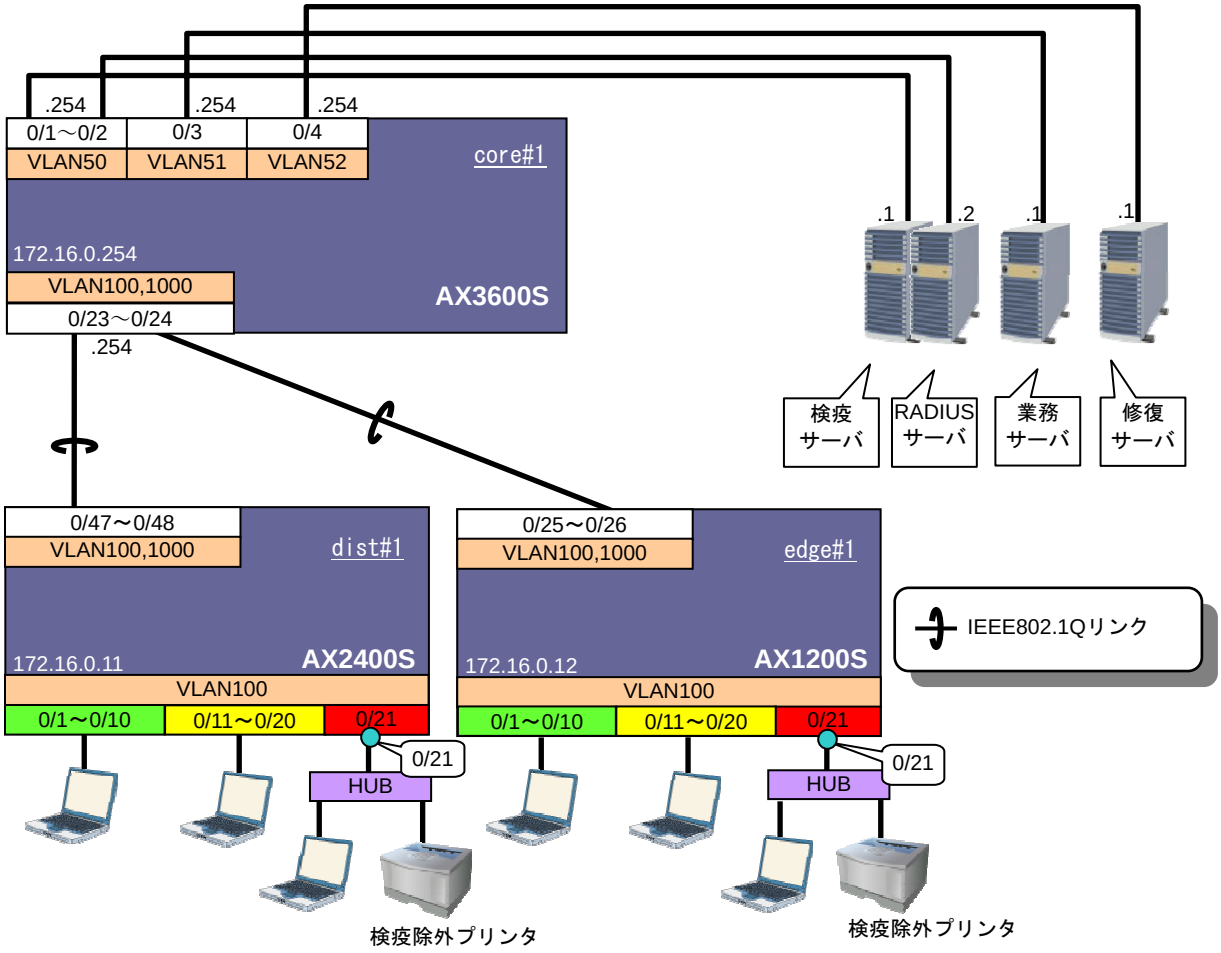

図 3.2-1 検疫ネットワーク構成図

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 3.2-1 認証スイッチのポート設定

認証スイッチ	VLAN モード	ポート種別	ポート番号	認証方式	用途	VLAN
AX2400S	固定 VLAN モード	アクセスポート	0/1～0/10	IEEE802.1X 認証	認証用	100
			0/11～0/20	MAC 認証		
			0/21	認証方式混在※1		
	—	トランクポート	0/47～0/48	—	上位スイッチとの通信用	100, 1000
AX1200S	固定 VLAN モード	アクセスポート	0/1～0/10	IEEE802.1X 認証	認証用	100
			0/11～0/20	MAC 認証		
			0/21	認証方式混在※1		
	—	トランクポート	0/25～0/26	—	上位スイッチとの通信用	100, 1000

※1…IEEE802.1X 認証と MAC 認証の混在ポート

各 VLAN の定義および VLAN 間通信の可否を以下の表に示します。

表 3.2-2　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
検疫・認証サーバ用 VLAN	50	10.50.0.0/24	検疫サーバおよび RADIUS サーバが所属する VLAN。	検疫サーバ RADIUS サーバ
業務サーバ用 VLAN	51	10.51.0.0/24	認証・検疫が成功したクライアント PC と通信可能なサーバが所属する VLAN。	業務サーバ
修復サーバ用 VLAN	52	10.52.0.0/24	検疫により隔離されたクライアント PC を修復するためのサーバが所属する VLAN。	修復サーバ
認証 VLAN	100	192.168.100.0/24	クライアント PC が所属する認証 VLAN。	
管理用 VLAN	1000	172.16.0.0/24	各装置を管理するための VLAN。	

表 3.2-3　検疫結果とサーバ間の通信可否

送信先 / 送信元	検疫サーバ	業務サーバ	修復サーバ
検疫失敗	○	×	○
検疫成功	○	○	○

本検疫システムで設定するセキュリティポリシーを以下に示します。

表 3.2-4 セキュリティポリシー

判定ポリシー	適用グループ	セキュリティポリシーの説明
ウイルス対策製品の判定	営業部	営業部に所属するPCは指定されたウイルス対策製品がインストールされていて、最新のウィルス定義ファイルを更新している必要があります。

※ウィルス対策製品の判定ポリシーを自動更新する場合はリモート管理サーバの設定が必要です。設定方法は「JP1/NETM/Client Security Control 解説・手引・操作書」の「6.4.6　ウィルス対策製品の判定ポリシーを自動・手動で更新する」を参照して下さい。

3.3. 構築ポイント

図 3.2-1の検疫ネットワークについて構築ポイントを以下に示します。

（１） 認証前アクセスリストを作成する。

クライアント PC の認証前及び認証失敗時に以下①～③の通信を許可するため、認証スイッチに認証前アクセスリストを定義します。

① JP1の検疫システムでは認証の可否に問わずクライアントPCと検疫サーバの接続性を確保する必要があります。クライアント PC と検疫サーバ間の通信許可の定義を行います。

② 検疫に失敗したクライアントPCが修復を行うためクライアントPCと修復サーバの接続性を確保する必要があります。クライアント PC と検疫サーバ間の通信許可の定義を行います。

③ 本ガイドではクライアント PC の IP アドレスを DHCP サーバより配布しています。そのためクライアント PC からの DHCP パケット通信許可の定義を行います。
（クライアント PC の IP アドレスを固定する環境では本定義は不要です。）

（２） IEEE802.1X 認証の再認証間隔を設定する。

IEEE802.1X 認証を使用した本検疫システムでは AX スイッチの IEEE802.1X 認証の再認証間隔毎にクライアント PC の検疫結果に応じた通信の可否を行います。本ガイドでは再認証間隔 5 分で設定しています。

（３） MAC 認証の最大接続時間を設定する。

MAC 認証を使用した本検疫システムでは AX スイッチの MAC 認証の最大接続時間毎にクライアント PC の検疫結果に応じた通信の可否を行います。本ガイドでは最大接続時間 10 分で設定しています。

3.4. AX の設定

3.4.1. AX1200S のコンフィグレーション

AX1200S の設定例を示します。

（１） 事前設定

AX1200S 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 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。(AX1230S の場合のみ) **※設定後は、装置の再起動が必要です。**

（２） 共通の設定

AX1200S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 100,1000** **(config-vlan)# state active**	VLAN1 は使用しないため、無効にします。 認証 VLAN として VLAN100 を、管理用 VLAN として VLAN1000 を作成します。
VLAN 名の設定	
(config)# vlan 100 **(config-vlan)# name AuthVLAN** **(config)# vlan 1000** **(config-vlan)# name ManagedVLAN**	VLAN100 に VLAN 名“AuthVLAN”を設定します。 VLAN1000 に VLAN 名“ManagedVLAN”を設定します。
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	
●認証用 **(config)# interface range fastethernet 0/1-21** **(config-if-range)# switchport access vlan 100**	ポート 0/1～0/21 を、アクセスポートとして VLAN100 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 100,1000**	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 VLAN100、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。
RADIUS サーバの設定	
(config)# radius-server host 10.50.0.2 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定します。本ガイドではシークレットキーを「alaxala」としています。
デフォルトルートの設定	
(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） 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)# dot1x system-auth-control **(config)# interface range fastethernet 0/1-10、0/21** **(config-if-range)# dot1x port-control auto** **(config-if-range)# dot1x multiple-authentication** **(config-if-range)# dot1x reauthentication** **(config-if-range)# dot1x supplicant-detection auto** **(config-if-range)# dot1x timeout reauth-period 300** 以下の設定は、環境に合わせて行います。 **(config-if-range)# dot1x timeout quiet-period 5**	IEEE802.1X 認証を有効にします。 ポート 0/1～0/10、0/21 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設定します。 サプリカントの再認証を有効にします。 端末検出モードを auto にします。 （AX1230S では disable にしてください） サプリカントの再認証周期を **300 秒(5 分)**に設定します。 ➢ **構築ポイント（２）** 認証失敗時の非認証状態保持時間を 5 秒に設定します。

（４） MAC 認証の設定

AX1200S の設定	
物理ポートの設定	
(config)# interface range fastethernet 0/11-0/21 **(config-if)# mac-authentication port**	ポート 0/11～0/21 を MAC 認証用ポートとして設定します。
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** **(config)# mac-authentication max-timer 10** 以下の設定は、環境に合わせて行います。 **(config)# mac-authentication id-format 1** **(config)# mac-authentication password macpass**	RADIUS サーバでユーザ認証を行うことを設定します。 MAC 認証機能を有効にします。 サプリカントの最大接続時間を **10 分**に設定します。 ➢ **構築ポイント（３）** RADIUS サーバへ認証要求する際の MAC アドレス形式を設定します。 MAC 認証のパスワードを統一する場合に設定します。この例では統一パスワードを「macpass」としています。

（５） 認証前アクセスリストの設定

AX1200S の設定	
認証前アクセスリストの設定	
(config)# ip access-list extended BeforeAuth **(config-ext-nacl)# permit protocol ip src 192.168.100.0 0.0.0.255 dst 10.50.0.1 0.0.0.0** **(config-ext-nacl)# permit protocol ip src 192.168.100.0 0.0.0.255 dst 10.52.0.1 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 bootpc** **(config-ext-nacl)# permit protocol ip src 192.168.100.0 0.0.0.255 dst 10.50.0.2 0.0.0.0**	以下条件の認証前アクセスリスト「BeforeAuth」を作成します。 ①認証 VLAN から検疫サーバ「10.50.0.1」への通信を許可する。 ②認証 VLAN から修復サーバ「10.52.0.1」への通信を許可する。 ③クライアントからの DHCP-Discover パケットを許可する。 認証 VLAN から DHCP サーバ「10.50.0.2」への通信を許可する。 ➢ **構築ポイント（１）**
(config)# interface range fastethernet 0/1-21 **(config-if-range)#authentication ip access-group "BeforeAuth"** **(config-if-range)# authentication arp-relay**	ポート 0/1-0/21 に認証前アクセスリストを適用します。 ポート 0/1-0/21 に arp-relay を適用します。

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） 共通の設定

AX2400S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 100,1000** **(config-vlan)# state active**	VLAN1 は使用しないため、無効にします。 認証前 VLAN として VLAN100 を、管理用 VLAN として VLAN1000 を作成します。
VLAN 名の設定	
(config)# vlan 100 **(config-vlan)# name AuthVLAN** **(config)# vlan 1000** **(config-vlan)# name MnagedVLAN**	VLAN100 に VLAN 名“AuthVLAN”を設定します。 VLAN1000 に VLAN 名“ManagedVLAN”を設定します。
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	
●認証用 **(config)# interface range gigabitethernet 0/1-21** **(config-if-range)# switchport access vlan 100**	ポート 0/1～0/21 を、アクセスポートとして VLAN100 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 100,1000**	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 VLAN100、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 172.16.0.11 255.255.255.0**	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 10.50.0.2 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定します。この例ではシークレットキーを「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	デフォルトルートを設定します。

（２） 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)# dot1x system-auth-control **(config)# interface range gigabitethernet 0/1-10、gigabitethernet 0/21** **(config-if-range)# dot1x port-control auto** **(config-if-range)# dot1x multiple-authentication** **(config-if-range)# dot1x reauthentication** **(config-if-range)# dot1x supplicant-detection auto** **(config-if-range)# dot1x timeout reauth-period 300** 以下の設定は、環境に合わせて行います。 **(config-if-range)# dot1x timeout quiet-period 5**	IEEE802.1X 認証を有効にします。 ポート 0/1～0/10、0/21 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設定します。 サプリカントの再認証を有効にします。 端末検出モード auto にします。 サプリカントの再認証周期を **300 秒(5 分)**に設定します。 ➢ **構築ポイント （２）** 認証失敗時の非認証状態保持時間を 5 秒に設定します。

（３） MAC 認証の設定

AX2400S の設定	
物理ポートの設定	
(config)# interface range gigabitethernet 0/11-21 **(config-if)# mac-authentication port**	ポート 0/11～0/21 を MAC 認証用ポートとして設定します。
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** **(config)# mac-authentication max-timer 10** 以下の設定は、環境に合わせて行います。 **(config)# mac-authentication password macpass**	RADIUS サーバでユーザ認証を行うことを設定します。 MAC 認証機能を有効にします。 サプリカントの最大接続時間を **10 分**に設定します。 ➢ **構築ポイント （３）** MAC 認証のパスワードを統一する場合に設定します。この例では統一パスワードを「macpass」としています。

（４） 認証前アクセスリストの設定

AX2400S の設定	
アクセスリストの設定	
(config)# ip access-list extended BeforeAuth **(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 host 10.50.0.1** **(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 host 10.52.0.1** **(config-ext-nacl)# permit udp any any eq bootpc** **(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255 host 10.50.0.2**	以下のアクセスリスト「BeforeAuth」を作成します。 ①認証 VLAN から検疫サーバ「10.50.0.1」への通信を許可する。 ②認証 VLAN から修復サーバ「10.52.0.1」への通信を許可する。 ③クライアントからの DHCP-Discover パケットを許可する。 認証 VLAN から DHCP サーバ「10.50.0.2」への通信を許可する。 ➢ **構築ポイント（１）**
(config)# interface range gigabitethernet 0/1-21 **(config-if-range)#authentication ip access-group "BeforeAuth"** **(config-if-range)# authentication arp-relay**	ポート 0/1-0/21 に認証前アクセスリストを適用します。 ポート 0/1-0/21 に arp-relay を適用します。

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。

AX3600S 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 50,51,52** **(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。 認証 VLAN として VLAN100 を作成します。 サーバ用 VLAN として VLAN50、51、52 を作成します。 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	
(config)# interface range gigabitethernet 0/1-2 **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 50** **(config)# interface range gigabitethernet 0/3** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 51** **(config)# interface range gigabitethernet 0/4** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 52** **(config)# interface range gigabitethernet 0/23-24** **(config-if-range)# switchport mode trunk** **(config-if-range)# switchport trunk allowed vlan 100,1000**	ポート 0/1～0/2 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。 ポート 0/23～0/24 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 VLAN100、1000 を設定します。
インタフェースの設定	
(config)# interface vlan 100 **(config-if)# ip address 192.168.100.254 255.255.255.0** **(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** **(config)# interface vlan 1000** **(config-if)# ip address 172.16.0.254 255.255.255.0**	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。
DHCP リレーの設定	
(config)# interface vlan 100 **(config-if)# ip helper-address 10.50.0.2**	VLAN100 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。

3.5. サーバの設定

本章では AX スイッチと連携した JP1 の検疫システムを構築する際に必要なサーバの設定にて重要なポイントをピックアップし設定方法を記載しています。
以下に本ガイドで記載しているサーバの設定を示します。

- **3.5.1事前準備**
  本ガイドに沿って JP1 の検疫システムを構築する際に事前に行っておく必要がある設定を示しています。

- **3.5.2RADIUSサーバ連携設定**
  RADIUS サーバがクライアント PC の検疫結果に応じた認証応答を行うための JP1/NETM/CSC - Agent への RADIUS サーバ連携の設定手順を示します。

- **3.5.3ポリシー管理設定**
  本検疫システムで使用するセキュリティポリシーを設定する JP1/NETM/CSC - Manager のポリシー管理画面の設定手順を示します。

3.5.1. 事前準備

本検疫システムを構築するために事前に行っておく必要がある設定を以下に示します。**3.5.2**RADIUS サーバ連携設定、**3.5.3**ポリシー管理設定を実施する前にサーバにて以下①～③の設定が完了していることを確認して下さい。

① サーバコンポーネントのインストール

本ガイドでは、検疫サーバと RADIUS サーバに以下の Windows Server コンポーネントと JP1 コンポーネントをインストールして JP1 の検疫システムを構築しています。
各サーバにて下記表のコンポーネントのインストールが完了していることを確認して下さい。

表 3.5-1 検疫サーバのコンポーネント表

検疫サーバ （Windows Server 2003 または Windows Server 2008）			
	コンポーネント名	役割	コンポーネント種別
1	IIS	Web サーバ（管理用）	Windows Server コンポーネント
2	JP1/NETM/DM Manager	ソフトウェア配布・資産管理	JP1 コンポーネント
3	JP1/NETM/AIM	統合資産管理	
4	JP1/NETM/CSC - Manager	クライアントセキュリティ管理	

表 3.5-2 RADIUS サーバのコンポーネント表

RADIUS サーバ （Windows Server 2003 または Windows Server 2008）			
	コンポーネント名	役割	コンポーネント種別
1	Active Directory	ディレクトリサービス	Windows server コンポーネント
2	Network Poricy Server 及び IAS	RADIUS サーバ	
3	DHCP	DHCP サーバ	
4	JP1/NETM/CSC - Agent	クライアントセキュリティ管理	JP1 コンポーネント

サーバインストール方法については以下の資料を参照して下さい。

・「JP1/NETM/Asset Information Manager 設定・構築ガイド」の「第 2 編 構築編」
・「JP1/NETM/DM 導入・設計ガイド(Windows(R)用)」の「3 導入から運用開始までの流れ」
・「JP1/NETM/Client Security Control解説・手引き・操作書」の「インストールとセットアップ」
・ Windows コンポーネントについては Microsoft のホームページや RADIUS サーバ設定ガイド
（Windows Server 2003 編、及び Windows Server 2008 編） をそれぞれ参照して下さい。

② 統合資産管理の設定

統合資産管理（JP1/NETM/AIM）にてクライアント PC が所属する部署情報の設定を行って下さい。
統合資産管理の設定や部署情報の作成、設定方法については以下の資料を参照して下さい。
本ガイドの例では「営業部」を登録して使用しています。

・「JP1/NETM/Asset Information Manager 運用ガイド」の「1.4 登録操作の流れ」

③ RADIUS サーバのセットアップ

AX スイッチのネットワーク認証を行うために RADIUS サーバのセットアップをして下さい。
必要な設定を以下の表に示します。

表 3.5-3 RADIUS サーバのセットアップ手順

RADIUS サーバ （Windows Server 2003 または Windows Server 2008）			
項番	設定内容	コンポーネント	RADIUS サーバ設定ガイドでの記載箇所
1	ユーザの作成	Active Directory	「2 章 Windows Server 2003 の構成」 「2 章 Windows Server 2008 の構成」
2	グループの作成		
3	RADIUS クライアントの設定	NPS 及び IAS	「3 章 IEEE802.1X 認証の設定」、 「5 章 MAC 認証の設定」
4	ネットワークポリシーの設定		

RADIUS サーバのセットアップ方法については以下の資料を参照し本検疫ネットワークの環境に合わせて設定を完了させて下さい。

・RADIUS サーバ設定ガイド（Windows Server 2003 編 及び Windows Server 2008 編）

3.5.2. RADIUS サーバ連携設定

RADIUS サーバがクライアント PC の検疫結果に応じた認証応答をするため“JP1/NETM/CSC - Agent ”のセットアップを行います。

（１）エージェントセットアップ

①「スタート」→「JP1/NETM/Client Security Control」→「エージェントセットアップ」をクリックし設定画面を表示します。

②基本設定タブの「マネージャー通信環境情報」を展開し「IP アドレス」を選択、画面下の入力欄に検疫サーバの IP アドレスを入力します。（本ガイドでは 10.50.0.1）
また「ネットワーク制御製品情報」の「名称」を「JP1/NETM/Network Monitor」から「Internet Authentication Service」に変更して下さい。

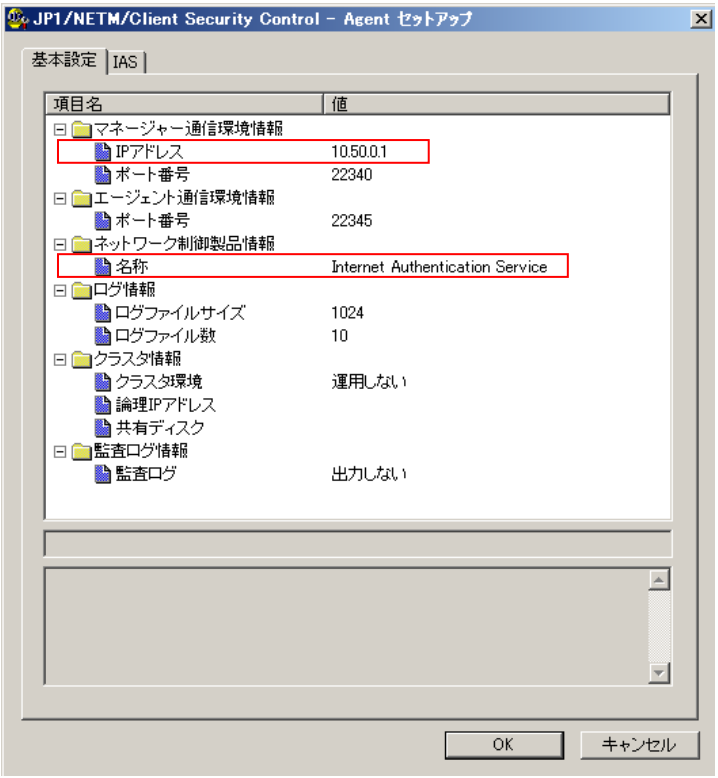

図 3.5-1 JP1/NETM/CSC - Agent 基本設定

③「IAS」タブを選択し「未登録資産の接続情報」と「拒否資産の接続情報」をそれぞれ「認証前」に選択します。
　　「IAS」タブのその他の設定は変更する必要はありません。

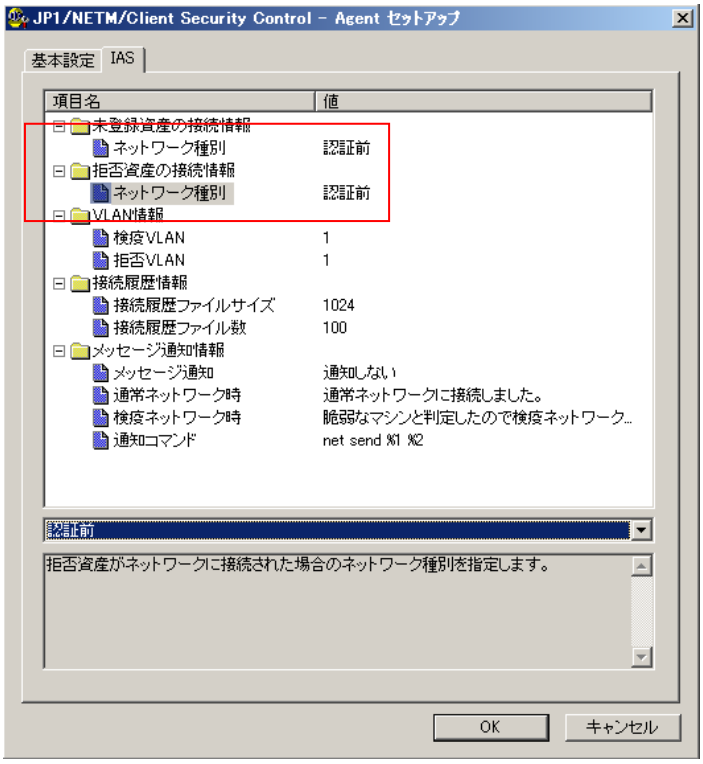

図 3.5-2 JP1/NETM/CSC - Agent IAS

※項目名 VLAN 情報については固定 VLAN 方式との連携の例であるため、本ガイドでは使用しません。
　値が入っていても問題はないのでデフォルトのままで問題ありません。

※Windows Server 2008 でもタブ名は「IAS」となります。

④画面右下「OK」をクリックして「JP1/NETM/Client Security Control – Agent セットアップ」画面を閉じます。

3.5.3. ポリシー管理設定

検疫サーバでは本検疫システムで使用するセキュリティポリシーの作成と設定を行います。
本設定例ではクライアント PC にセキュリティソフトがインストールされているかを判定し、
ネットワーク接続の制御を行うセキュリティポリシーを作成します。
（※構築の際は環境に合わせ適切なセキュリティーポリシーの作成、設定を行って下さい。）

JP1/NETM/CSC - Manager のポリシー管理画面を使用して以下の 2 つのセキュリティポリシーの作成と各ポリシーの割り当てを行います。

・判定ポリシー
クライアントの危険レベルを判定する条件および危険レベルの定義を行います。

・アクションポリシー
危険レベルに応じて実施するアクションを定義します。

ポリシー管理設定は以下の作業からなります。
（１）ポリシー管理画面の起動　手順番号①
（２）ポリシーの作成　　手順番号①～⑬
（３）ポリシーの割り当て　手順番号①～④

（１）ポリシー管理画面の起動

①「スタート」→「すべてのプログラム」→「JP1_NETM_Client Secrity Control 」→「ポリシー管理」をクリックしポリシー管理画面を起動する。

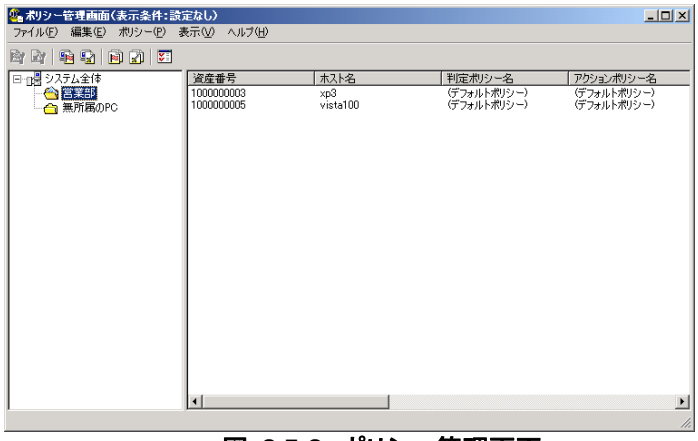

図 3.5-3 ポリシー管理画面

（２）ポリシーの作成

① ポリシー管理画面の左画面にて「営業部」フォルダを選択し、画面上段の「ポリシー」から「判定ポリシーの管理」をクリックして開く。

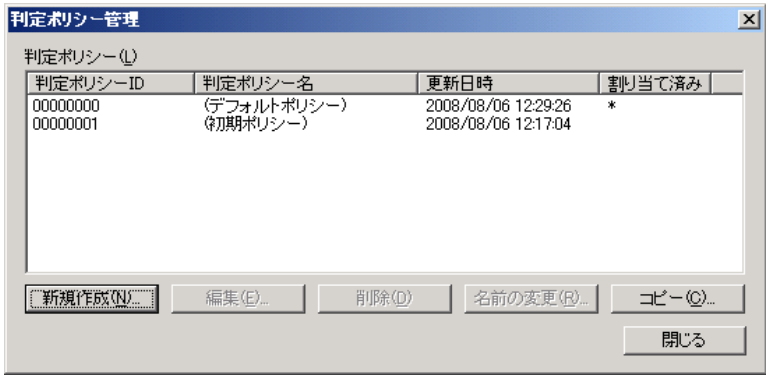

図 3.5-4 判定ポリシー管理

② 判定ポリシー管理画面の「新規作成」をクリックし判定ポリシー名を入力（ここでは営業部の判定ポリシーとする）「既存の判定ポリシーを指定してコピーを作成する」のチェックを確認し、画面下のデフォルトポリシーが選択されていること

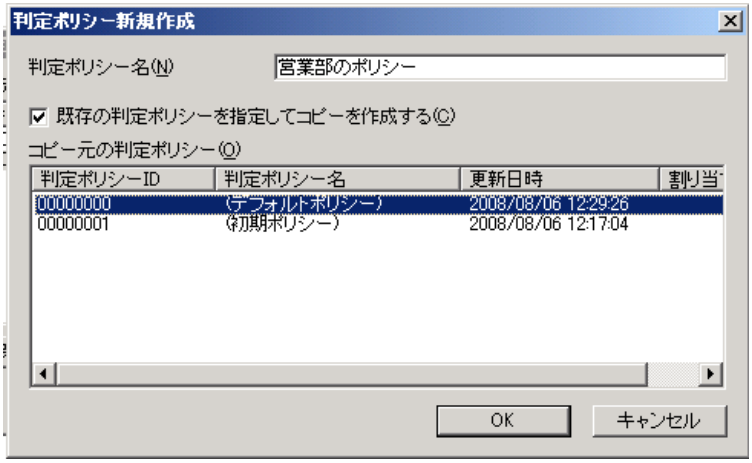

図 3.5-5 判定ポリシー新規作成

③「OK」ボタンをクリックして画面閉じ判定ポリシー画面に「営業部の判定ポリシー」が追加されている事を確認する。

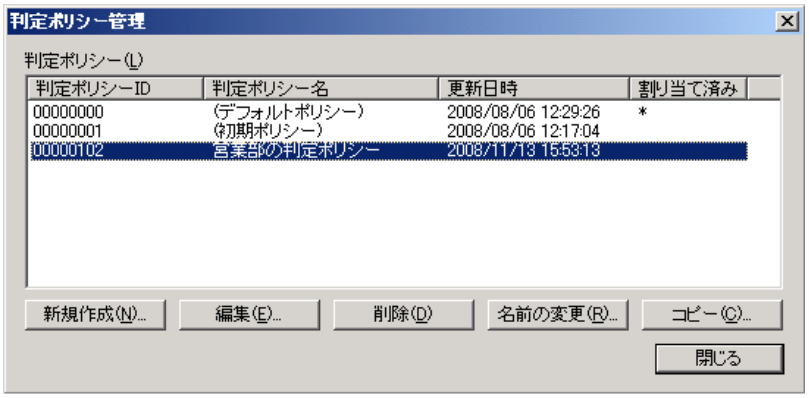

図 3.5-6 判定ポリシー管理 2

④判定ポリシー管理画面の「営業部の判定ポリシー」を選択し下の「編集」を
クリックし判定ポリシーの編集画面を表示、左画面「ウイルス対策製品」を選択、
右画面の「判定対象とする」にチェックする。そして下の「保存」をクリックした後
「閉じる」をクリックし画面を閉じる。

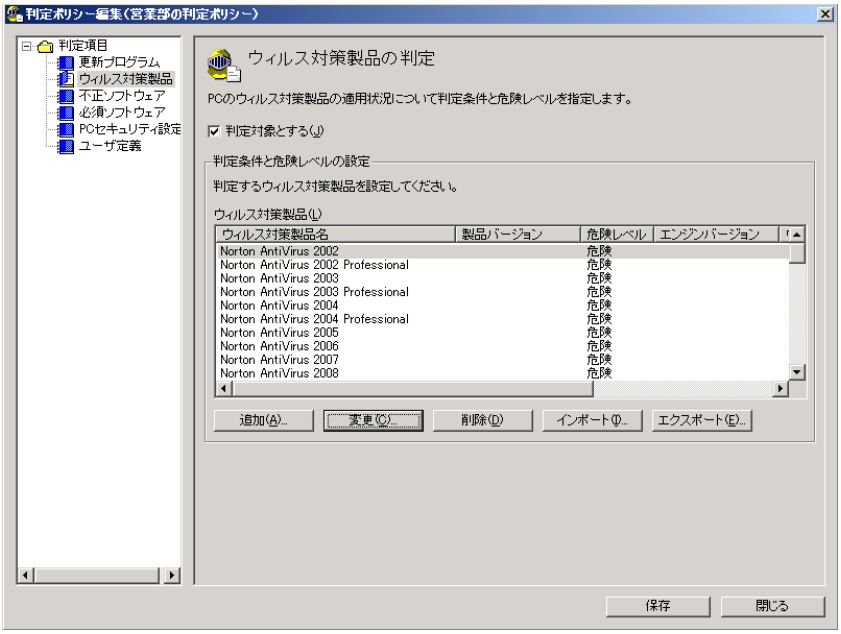

図 3.5-7 判定ポリシー編集

⑤判定ポリシー画面も「閉じる」をクリックし閉じる。

⑥ポリシー管理画面の「ポリシー」を選択し「アクションポリシーの管理」を開く。

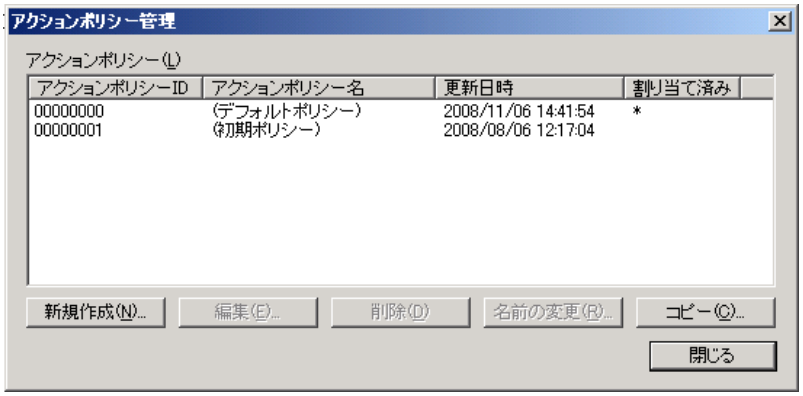

図 3.5-8 アクションポリシー管理

⑦画面下の「新規作成」をクリックしアクションポリシー名を入力（ここでは営業部のアクションポリシーとする）。
「既存のアクションポリシーを指定してコピーを作成する」のチェックを確認し、画面下のデフォルトポリシーが選択されていることを確認。

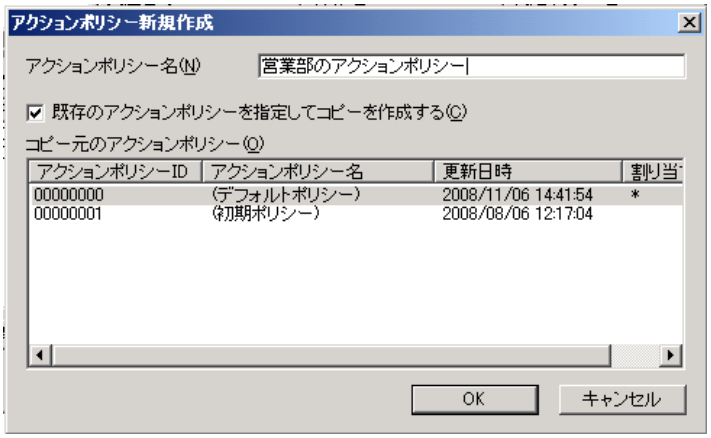

図 3.5-9 アクションポリシー新規作成

⑧「OK」ボタンで閉じアクションポリシー管理画面に「営業部のアクションポリシー」が追加されている事を確認する。

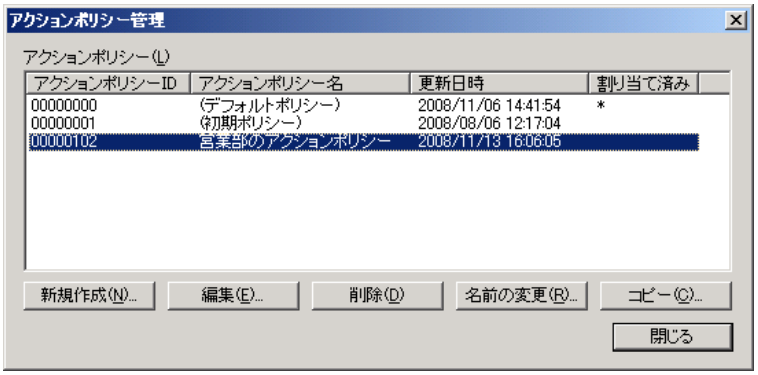

図 3.5-10 アクションポリシー管理 2

⑨アクションポリシー管理画面の「営業部のアクションポリシー」を選択し下の「編集」をクリック、アクションポリシーの編集画面を表示する。
左画面「アクション」を展開し「危険」を選択、メイン画面にて「PC 使用者への通知」の「使用者にメッセージ通知する」のチェックボックスにチェックを入れてください。
また「PC のネットワーク接続の制御」の「ネットワーク接続を制御する」と「接続を拒否する」にそれぞれチェックを入れてください。

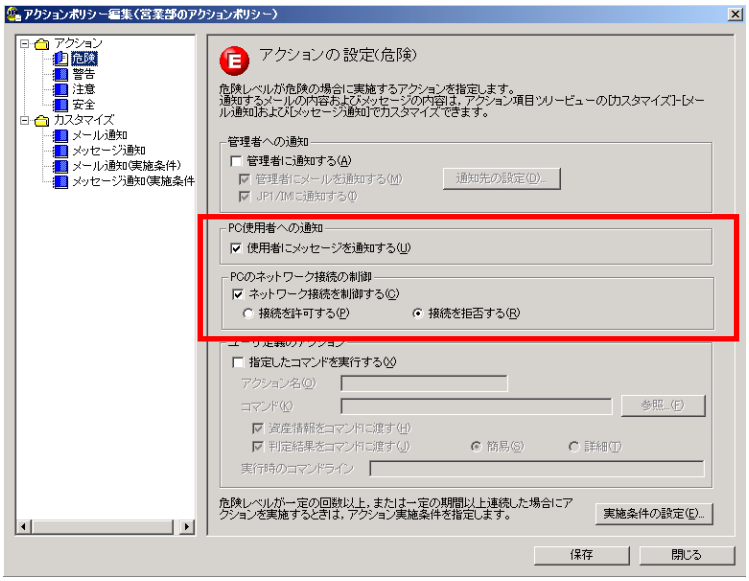

図 3.5-11 アクションの設定「危険」

⑩左画面「アクション」を展開し「安全」を選択、⑨の「危険」の設定と違う箇所は「PC のネットワーク接続の制御」にて「接続を許可する」をチェックしてください。

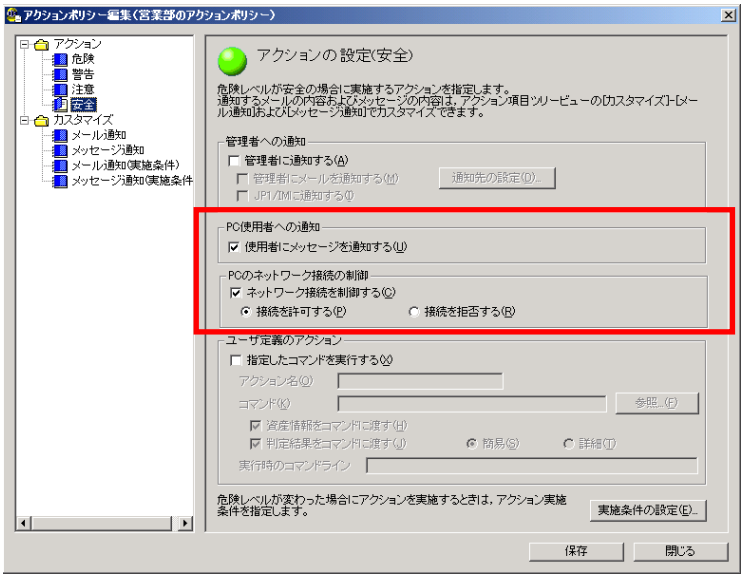

図 3.5-12 アクションの設定「安全」

※また左画面の「アクション」には「安全」、「危険」の他に「警告」、「注意」も存在します。本ガイドでは設定を省いていますが、構築する環境に応じて適切な設定を行ってください。

⑪左画面「カスタマイズ」を展開し「メッセージ通知」を選択し「危険」タブと「安全」タブのメッセージ内容を環境に応じて編集する。
本ガイドでは「危険」タブの通知するメッセージに”※修復を実施してサーバに反映されるまで時間がかかります。安全メッセージが表示されるまでお待ち下さい。”）とのメッセージを追加。

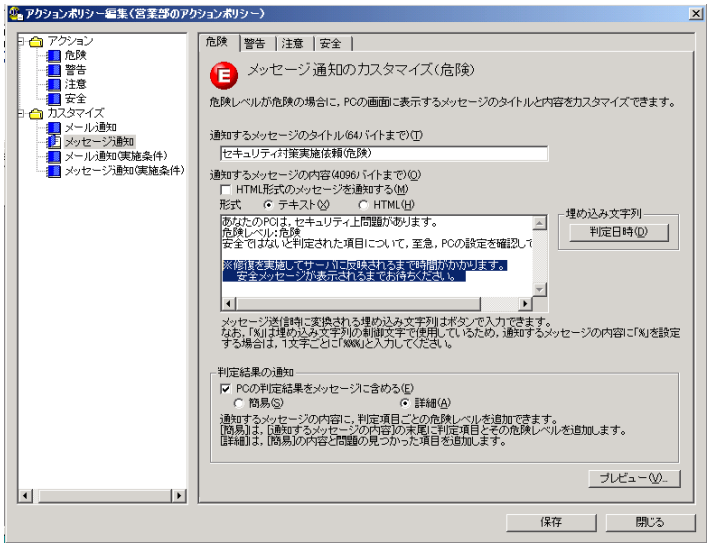

図 3.5-13 アクションポリシー編集

⑫本検疫システムに IEEE802.1X 認証を使用時はネットワーク再接続操作が必要のため「安全」タブの通知するメッセージに以下の内容を追加して下さい。
”通信が復旧していない場合、ネットワーク再接続のために以下の何れかの操作を行って下さい。
・PC に接続しているネットワークケーブルを抜き差しする。
・ネットワーク接続を一度無効にし再度有効にする。
・PC の再起動をする。”

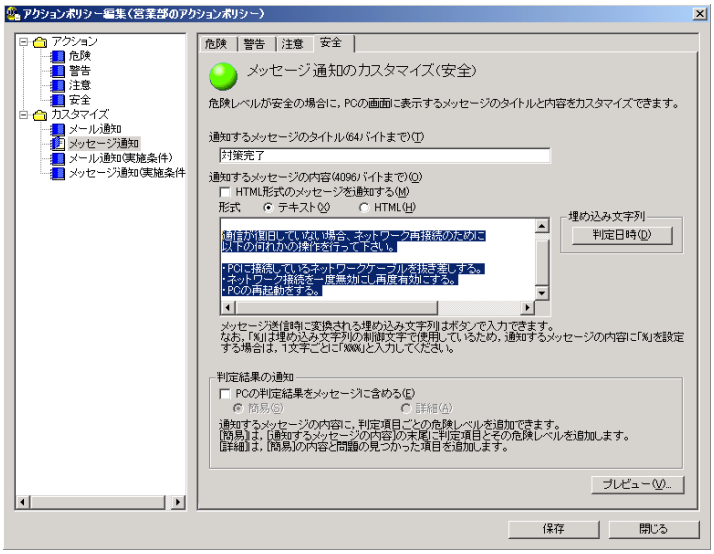

図 3.5-14 アクションポリシー編集 2

※MAC 認証使用時は自動的認証が行われるためネットワーク再接続操作は不要です。

⑬下の「保存」をクリックした後「閉じる」をクリックし画面を閉じます。
アクションポリシー画面も「閉じる」をクリックし閉じます。

（３）ポリシーの割り当て

①ポリシー管理画面の左画面の「営業部」フォルダを選択し「ポリシー」をクリック
「判定ポリシーの割り当て」をクリックし判定ポリシー割り当て画面を表示する。

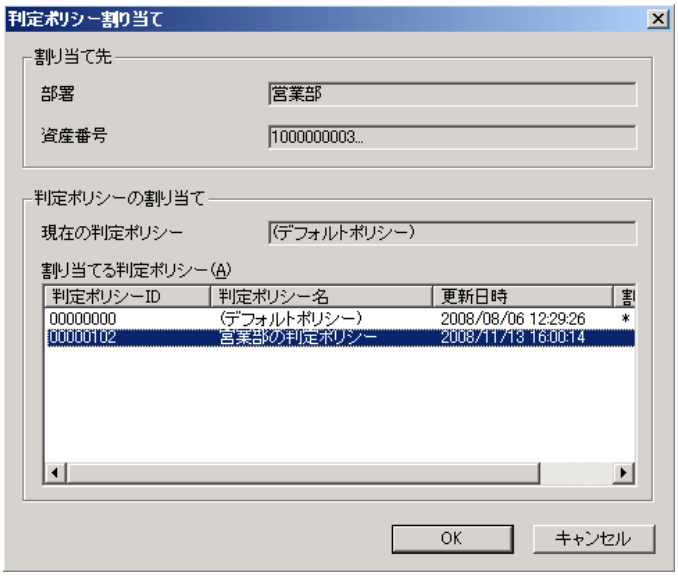

図 3.5-15 判定ポリシー割り当て

②「割り当てる判定ポリシー」の中で先程作成した「営業部の判定ポリシー」を選択し「OK」ボタンをクリックし閉じる。

③ポリシー管理画面の左画面の「営業部」フォルダを選択し「ポリシー」をクリック
「アクションポリシーの割り当て」をクリックしアクションポリシー割り当て画面を表示する。
「割り当てるアクションポリシー」の中で先程作成した「営業部のアクションポリシー」を選択し「OK」ボタンをクリックし閉じる。

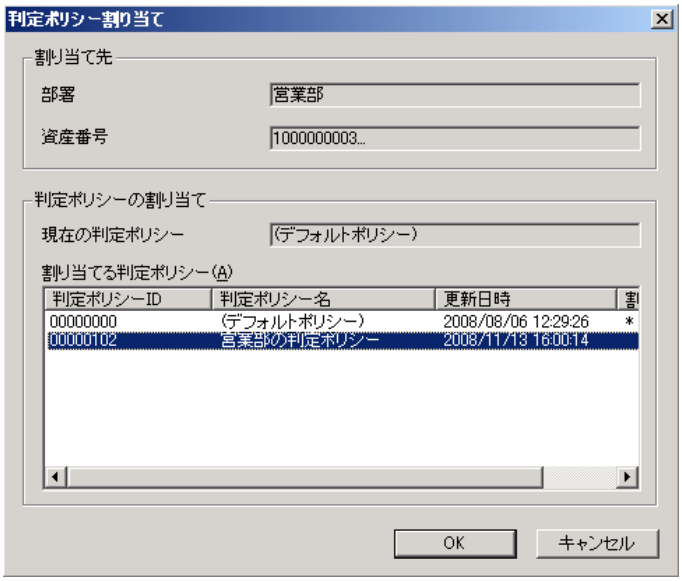

図 3.5-16 判定ポリシー割り当て 2

④最後にポリシー管理画面の左画面の「営業部」フォルダを選択し判定ポリシー名に「営業部の判定ポリシー」、アクションポリシー名に「営業部のアクションポリシー」が割り当てられていることを確認しポリシー管理画面を閉じる。

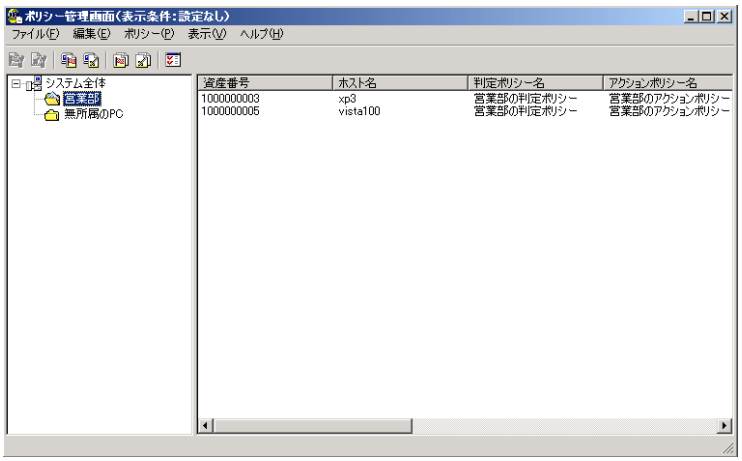

図 3.5-17 ポリシー管理画面 2

3.6. クライアント PC の設定

ここでは、本ガイドの検疫ネットワークの環境に合わせたクライアント PC（JP1/NETM/DM Client）のセットアップを行います。
※JP1/NETM/DM Clientの詳細につきましては「JP1/NETM/DM 構築ガイド」の「６章 JP1/NETM/DM Client（クライアント）をセットアップする」をご参照下さい。

3.6.1. インストール時の設定

①まずはクライアント PC に JP1/NETM/DM Client をインストールします。クライアント PC に管理者権限のユーザでログインしインストール CD を挿入して下さい。下記画面のインストールウィザードが開始します。

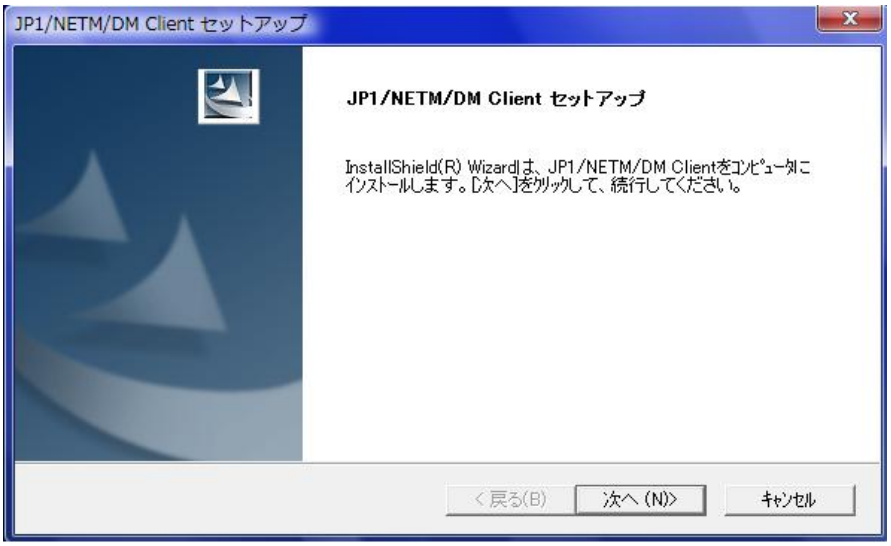

図 3.6-1 JP1/NETM/DM Client セットアップ

※本ガイドのインストールウィザードでは設定の必要が無いページの記載を省いています。本ガイドにて記載の無いインストールウィザードの画面はデフォルトのまま「次へ」をクリックして下さい。

②種別の選択では「クライアント」を選択して下さい。

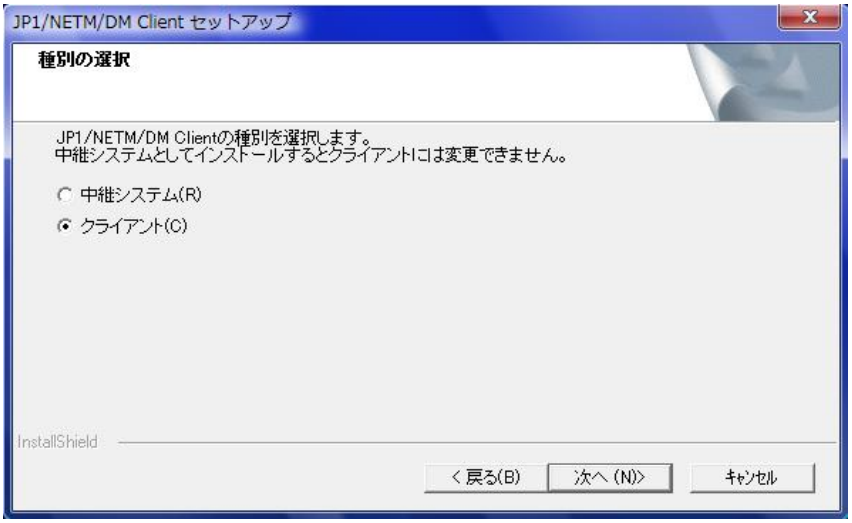

図 3.6-2 種別の選択

③接続先の設定では製品種別に「JP1/NETM/DM Manager」を選択して、接続先の「ホスト名または IP アドレス」の項目には検疫サーバの IP アドレス（本ガイドでは 10.50.0.1）を入力して下さい。

図 3.6-3 接続先の設定

④ネットワークの設定では「LAN」を選択して下さい。

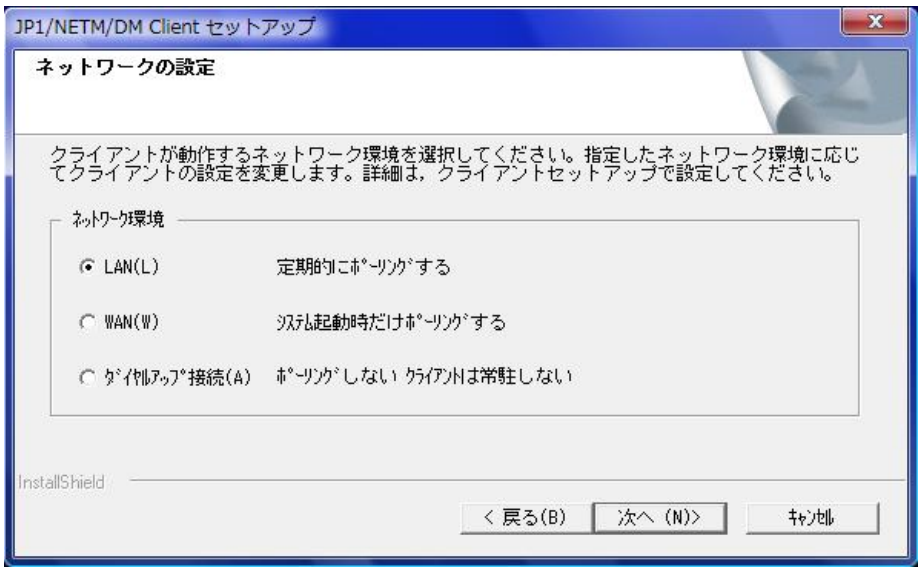

図 3.6-4 ネットワークの設定

⑤インストール完了後クライアント PC の再起動が必要です。

3.6.2. インストール後の設定

①クライアント PC にて「スタート」→「すべてのプログラム」をクリック、「JP1/NETM/DM Client」を展開「セットアップ」をクリックしてクライアントセットアップ画面を表示します。
「接続先」タブを選択し接続先に「JP1/NETM/DM Manager」のチェックと検疫サーバの IP アドレス（本ガイドでは 10.50.0.1）が正しいことを確認して下さい。

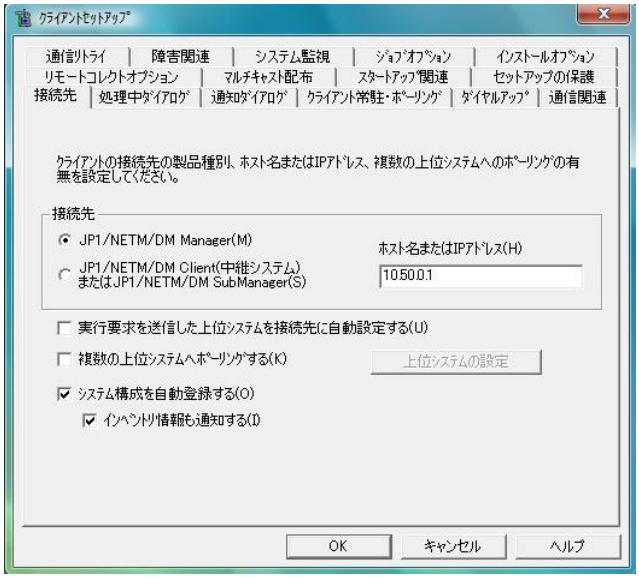

図 3.6-5 クライアントセットアップ 接続先

②「クライアント常駐・ポーリング」タブを選択しポーリングのタイミングにて「システム起動時から一定間隔」をデフォルトの 30 分を 10 分（本ガイドでの推奨値）に変更します。

図 3.6-6 クライアントセットアップ クライアント常駐・ポーリング

※クライアントPCのポーリング間隔の設定は本検疫システムを構築するうえで重要な設定となります。
5.3JP1/NETM/DM Clientの設定についてをご確認のうえ構築する環境に合わせて適切な値を設定して下さい。

③「システム監査」タブを選択しこのチェック項目全てにチェックをします。

図 3.6-7 クライアントセットアップ システム監視

④ 以上でクライアントセットアップは完了です。

※IEEE802.1X 認証で本検疫システムを構築する場合はクライアント PC にてサプリカントの設定が必要です。
設定方法は RADIUS サーバ設定ガイド（Windows Server 2003 編または Windows Server 2008 編）の「3 章 IEEE802.1X 認証の設定」を参照して下さい。

3.7. 検疫除外端末の接続方法

検疫除外端末を基幹ネットワークに接続するために接続制御リストの編集方法を示します。
接続制御リストの概要に関しては1.2.2JP1/NETM/CSCとRADIUSサーバの連携動作を参照して下さい。

ここでは既に検疫除外端末が登録されている接続制御リストをエクスポートし、ファイルの中身と書式を確認した後、新しく検疫除外端末を追加する手順を示しています。
接続制御リストの確認をする必要が無い場合は手順⑤のインポートから設定することで検疫除外端末の追加をする事ができます。

①AXスイッチのMAC認証の設定を行う。3検疫ネットワークの構築を参照して下さい。

②管理者権限のあるユーザで JP1/NETM/CSC - Agen t がインストールされた Windows Server にログインし「コマンドプロンプト」を起動します。

③cscrexport コマンドを実行して接続制御リストを CSV 形式のファイルにエクスポートします。
※JP1/NETM/CSC - Agent の各コマンドの格納先は“JP1/NETM/CSC - Agent のインストール先フォルダ¥radius¥bin”にあります。
※エクスポート先は“JP1/NETM/CSC - Agent のインストール先フォルダ¥radius¥dat”です。

④エクスポートした CSV ファイルを開き下記書体に従って検疫除外するクライアント PC の「MAC アドレス」と「接続状態」を追加して下さい。
※接続状態は 1＝拒否、２＝許可となります、２と追記して下さい。
※クライアント PC の IP アドレスが固定の場合 IP アドレスも追加して下さい。

接続制御リストの書式：MAC アドレス,IP アドレス,接続状態{ 1 | 2 }

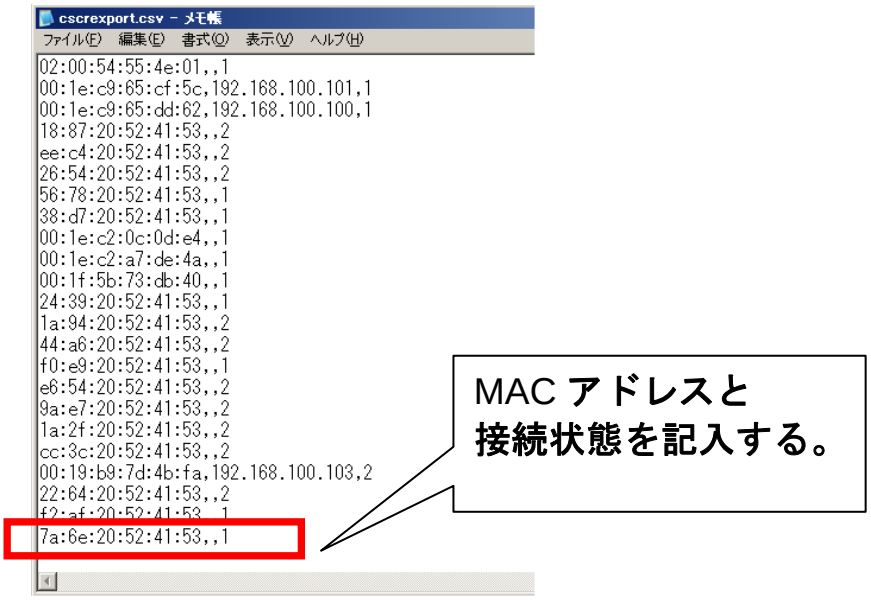

図 3.7-1 接続制御リスト書体

⑤cscrimport コマンドを実行し cscrexport コマンドでエクスポートし編集した接続制御リストを JP1/NETM/CSC - Agent にインポートします。

⑥JP1/NETM/CSC – Agent の設定は以上です。該当クライアント PC が AX スイッチの MAC 認証に成功することを確認して下さい。

接続制御リストの編集についての詳細は以下の資料に記載されています。

・JP1/NETM/Client Security Control 解説・手引・操作書」の「第 6 編 リファレンス編」

4. 動作確認方法

本章では、検疫システムにおける検疫動作の確認方法について示します。

4.1. AX における動作確認

4.1.1. show dot1x detail

IEEE802.1X 認証の状態表示コマンドです。クライアント PC が認証に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下さい。

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

Date 2008/11/04 16:35:03 JST
Port  0/1
AccessControl   : Multiple-Auth              PortControl     : Auto
Status          : ---                        Last EAPOL      : 0019.b97d.46c7
Supplicants     : 1 / 1 / 64                 ReAuthMode      : Enable
TxTimer(s)      : ---   / 30                 ReAuthTimer(s): 140   / 300
ReAuthSuccess   : 3                          ReAuthFail      : 1
SuppDetection   : Disable

 Supplicants MAC     Status          AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s)  Date/Time
 0019.b97d.46c7      Authorized      Authenticated  Idle           2
                     781             2008/11/04 16:22:02

edge#1> show mac-address-table

Date 2008/11/04 16:35:14 JST
MAC address         VLAN    Type     Port-list
0012.e208.4a71       100    Dynamic  0/48
0012.e208.4a71      1000    Dynamic  0/48
0019.b97d.46c7       100    Dot1x    0/1
```

図 4.1-1 AX1200S の状態表示例

4.1.2. show dot1x logging

IEEE802.1X 認証の動作ログ表示コマンドです。検疫エージェ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。

4.1.3. clear dot1x auth-state

IEEE802.1X 認証状態を初期化するコマンドです。検疫エージェントを強制的にログアウトさせる場合に使用します。

4.1.4. show mac-authentication login

MAC 認証の状態表示コマンドです。MAC 認証に成功したクライアント PC の認証状況を確認することができます。

```
edge#1# show mac-authentication login

Date 2008/11/04 18:58:58 JST
 Dynamic VLAN mode total client counts(Login/Max):   1 / 256
  Authenticating client counts :    0
  Hold down client counts      :    0
  Port roaming : Disable
   No F MAC address     Port VLAN  Login time            Limit     Reauth
    1   001e.c965.ea0c  0/1   100  2008/11/04 18:55:23   infinity    3384
```

図 4.1-2 AX1200S の状態表示例

4.2. 検疫サーバにおける動作確認

AIM にてクライアント PC の検疫結果とネットワーク接続状態を確認できます。またクライアント PC 単位で検疫結果の他に、検疫に失敗した際の原因や検疫結果の履歴などを確認することができます。

①ブラウザで「http:// “検疫サーバの IP アドレス” /jp1asset/login.htm」にアクセスすると下記画面が表示されます。
ユーザ ID、パスワードを入力しログインします。

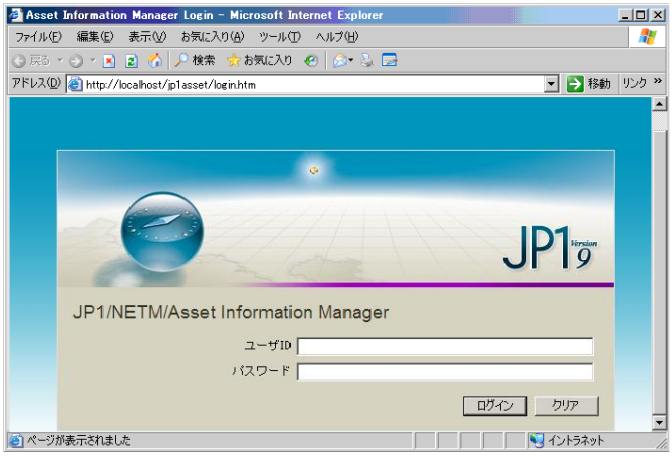

図 4.2-1 AIM ログイン画面

②ログイン後 AIM の操作画面左下の「管理業務」一覧から「クライアントセキュリティ」を展開し「PC 危険レベル管理」をクリックします。
メイン画面が以下の画面に遷移したら「検索」ボタンをクリックします。

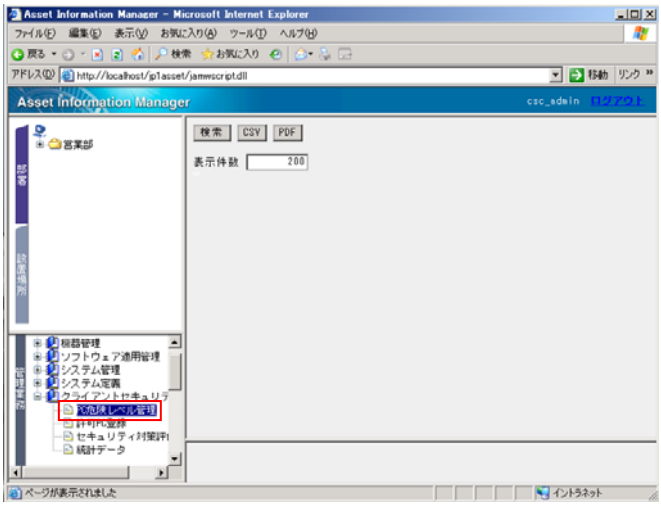

図 4.2-2 AIM 操作画面

③メイン画面に資産として管理されているクライアント PC の一覧が表示されます､クライアント PC の PC 危険レベル（検疫結果）とネットワーク接続状況を確認できます。

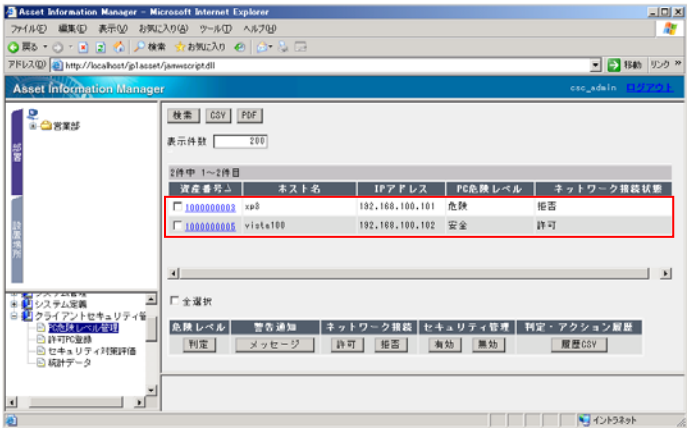

図 4.2-3 AIM PC 危険レベル管理画面

④またクライアント PC の詳細な情報を表示したい場合は該当するクライアント PC の資産番号をクリックすると詳細情報を表示する「PC 危険レベル詳細」画面となります。

図 4.2-4 AIM PC 危険レベル詳細画面

⑤「PC 危険レベル詳細」画面の「判定・アクション履歴」ボタンをクリックすると該当するクライアント PC の検疫結果の履歴を確認できます。

図 4.2-5 AIM 判定アクション履歴

⑥さらに「PC 危険レベル詳細」画面の「機器詳細」ボタンをクリックすると該当するクライアント PC の詳細情報を確認することができます。

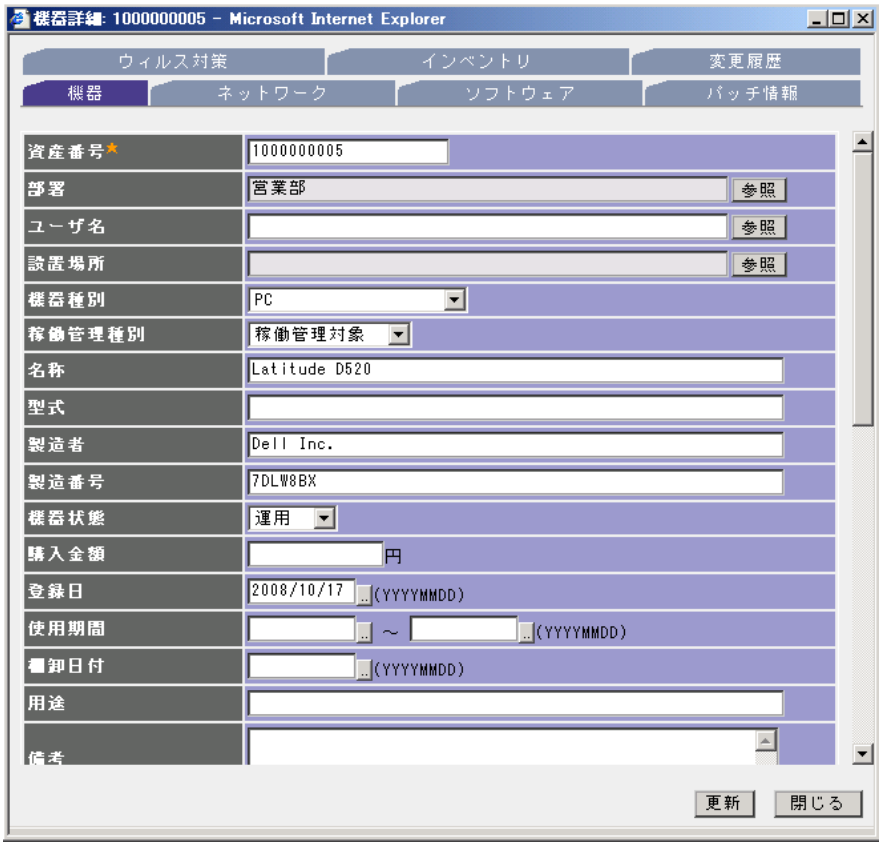

図 4.2-6 AIM 機器詳細

5. 注意事項

5.1. 検疫ポリシーの設定について

本検疫システムでは、一旦検疫失敗と判定されたクライアントPCが修復を行った後、業務ネットワークに復帰するには多少時間が掛かります。（詳細は 1.2.4検疫時間についてを参照）業務ネットワークへの接続を排除するセキュリティポリシー設定は、通常業務に支障が出ないようにセキュリティ上重大な項目のみで実施し、軽微な違反に関しては警告メッセージに留めた運用をお勧めします。

以下に検疫ポリシーの例を示します。

業務ネットワークへの接続を排除すべき検疫項目例

① ウイルス対策ソフトをインストールしていない場合
② 禁止ソフトの使用

警告に留める項目例

① ウイルスパターンの更新もれ
② セキュリティパッチの更新もれ

なお JP1/NETM/DM では Windows のセキュリティパッチに関しては管理者が強制的に自動更新を有効にする事も可能であり、WSUS サーバグループへ割り当ててパッチの配布をコントロールする事ができます。

5.2. RADIUS サーバ冗長化について

AXの構成定義にRADIUSサーバを複数定義する事で冗長化する事ができますが、**3.7検疫除外端末の接続方法**で記載した検疫除外端末の登録などはそれぞれのRADIUSサーバに手動で同期する必要があります。検疫・資産管理サーバの冗長化については、JP1 マニュアルで確認して下さい。

5.3. JP1/NETM/DM Client の設定について

ポーリング周期の推奨値は 10 分です。ポーリング周期が長すぎるとクライアント PC への検疫結果のメッセージ表示がポーリング周期時間分遅れることになります。またポーリング周期を 5 分以内に設定した場合サーバへの資産管理情報通知のため、クライアント PC の CPU 使用率が上がったり、かえって検疫時間が長くなるなど検疫の動作が不安定になる可能性があります。

5.4. IEEE802.1X 認証の再接続について

本検疫ネットワーク（固定 VLAN モード）では検疫に失敗したクライアント PC は AX スイッチの認証にも失敗します。再接続する場合は治療を行い検疫に成功し、その後ネットワーク認証に成功する必要があります。認証方式に MAC 認証を使用している場合は検疫成功後自動的に MAC 認証が実施され再接続されますが、IEEE802.1X 認証を使用したクライアント PC では検疫成功後、再度認証を実施するため以下の何れかの操作が必要です。

- PC に接続しているネットワークケーブルを抜き差しする。
- ネットワーク接続を一度無効にし再度有効にする。
- PC を再起動する。

※ 本ガイド **3.5.3**ポリシー管理設定の「メッセージ通知のカスタマイズ（安全）」設定では検疫成功後のメッセージにて上記何れかの操作をユーザに指示しています。

5.5. 認証スイッチの再認証時間の設定について

検疫に成功したクライアント PC にセキュリティ違反を発見した場合、ネットワーク接続から除外するために RADIUS サーバへの定期的な再認証を設定する必要があります。
再認証時間は短いほど不正ユーザの切り離しが早くなりセキュリティは高くなりますが、極端に短いと RASIUS サーバの負荷が上がってしまいますので、収容ユーザ数などを考慮して設定してください。
再認証時間の推奨値を以下に示します。

表 5.5-1 認証方式毎の再認証時間推奨値

認証方式	推奨値
IEEE802.1X 認証	5 分（300 秒） コンフィグレーションコマンド：dot1x timeout reauth-period 300
MAC 認証	10 分　（最小値 10 分のため） コンフィグレーションコマンド：mac-authentication max-timer 10

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下さい。

A.1. AX1200S のコンフィグレーション

AX1230S.txt
AX1240S.txt

A.2. AX2400S のコンフィグレーション

AX2400S.txt

A.3. AX3600S のコンフィグレーション

AX3600S.txt

※ PDF 文書にて添付ファイルを開く場合は、Adobe Reader 7 以上を使用して下さい。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。

2010 年 7 月 2 日　第2版

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