AX シリーズ
検疫ソリューションガイド
(iNetSec® Inspection Center 編)

第3版

はじめに

本ガイドは、株式会社 PFU 製の iNetSec Inspection Center 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システム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 認証ソリューションガイド補足資料
- AX シリーズ 製品マニュアル（http://www.alaxala.com/jp/techinfo/manual/index.html）
- iNetSec Inspection Center V5.0 L10 ユーザーズガイド
- iNetSec Inspection Center V5.0 L10 認証サーバ ユーザーズガイド
- iNetSec Inspection Center V5.0 L10 802.1X サプリカント ユーザーズガイド
- Web 認証方式認証機器連携導入設定手順書 第 1.0 版

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。

AX1230S	Ver1.4.D
AX1240S	Ver2.1
AX2400S / AX3600S	Ver11.1.A

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

- iNetSec は、株式会社 PFU の登録商標です。
- 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商標登録です。
- 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。
- ActiveX 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。
- Mac および Mac OS は米国およびその他の国における米国 Apple Computer, Inc の登録商標です。
- Red Hat は、米国およびその他の国における Red Hat, Inc. の登録商標または商標です。
- Linux は、Linus Torvalds の米国およびその他の国における登録商標あるいは商標です。
- 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.D)
- AX1240S (Ver2.1)
- AX2430S (Ver11.1.A)
- AX3630S (Ver11.1.A)
- Windows Server 2003
- Windows XP SP2
- Windows Vista SP1
- Red Hat Enterprise Linux Server release 5.1
- Mac OS X

検疫ソフトウェアー覧

- iNetSec Inspection Center V5.0L10A サーバパッケージ
- iNetSec Inspection Center V5.0 クライアントライセンス
- iNetSec Inspection Center V5.0L10A 認証機器拡充固有修正
- オプション：iNetSec Inspection Center V5.0 認証サーバパッケージ
- オプション：iNetSec Inspection Center V5.0 802.1X サプリカントライセンス

改訂履歴

版数	Rev.	日付	変更内容	変更箇所
初版	ー	2008.9.22	初版発行	ー
第 2 版	ー	2009.1.30	･ゲートウェイ方式を追加。 ･認証方式混在について注意事項を追加 ･AX シリーズのコンフィグレーション（ゲートウェイ方式）を付録として追加	･1.3 ･2 章 ･4 章 ･5.1.2 ･6.2 ･6.3 ･A.2
第 3 版	ー	2009.5.20	･検疫シーケンスを一部修正。 ･文中にユーザ認証が省略可能な旨を追加。 ･シーケンス図中の説明を一部修正。 ･その他誤字を修正。	･1.2.2 ･1.3.1 ･1.3.5 全体的

目次

1. iNetSec Inspection Center 検疫概要

1.1. iNetSec Inspection Center 検疫

1.1.1. iNetSec Inspection Center 検疫システム概要

iNetSec Inspection Center は、ネットワークに接続するクライアントのセキュリティ状態を調査し、ネットワーク認証機スイッチ AX シリーズと連携して、クライアントのネットワークへの接続を制御します。

不正な利用者や許可されていないクライアントがネットワーク接続しようとした場合、その接続を排除します。許可されたクライアントがセキュリティポリシーに適合していない場合は、そのクライアントをネットワークから隔離します。隔離したクライアントについては、セキュリティパッチ適用などを行う修復サーバへの通信を許可して、クライアントを安全な状態に誘導することで治療を行います。

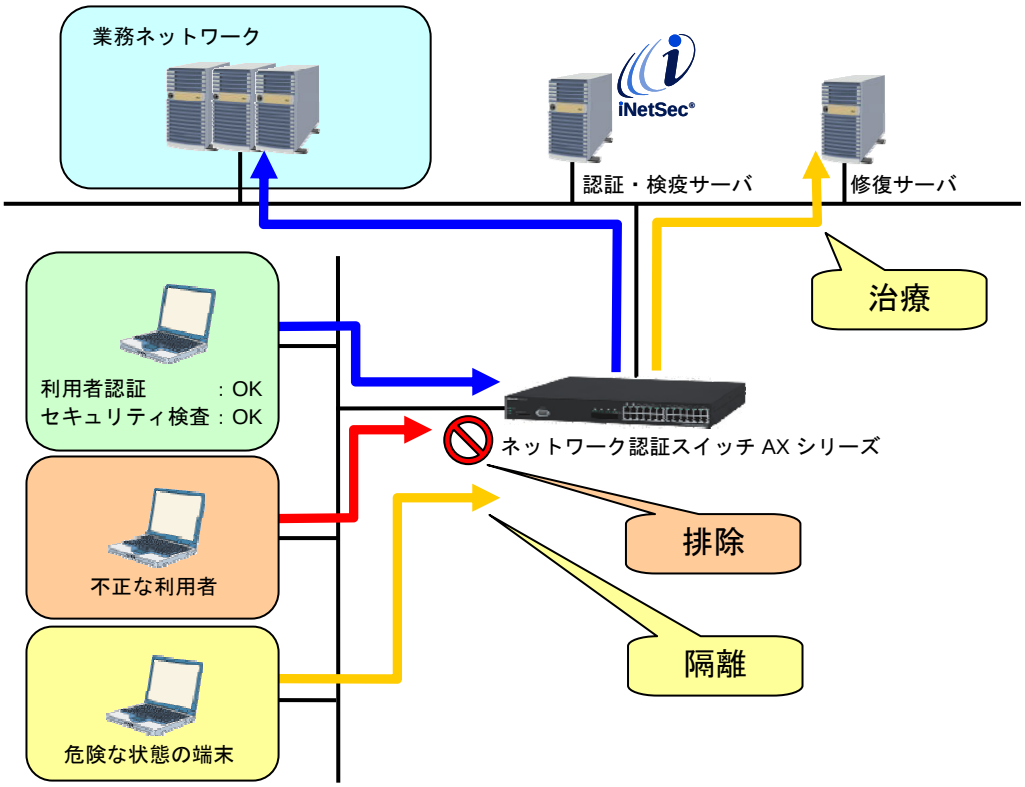


図 1.1-1 iNetSec Inspection Center 検疫システム概要

1.1.2. iNetSec Inspection Center サポート一覧

表 1.1-1 iNetSec Inspection Center の動作モード

分類	方式	特徴	AX シリーズとの連携
LAN 検疫	IEEE802.1X 認証 VLAN 方式	ユーザ単位にネットワーク（VLAN）を別けることにより、ユーザ単位の通信制御が可能	連携可能
	ゲートウェイ方式	クライアント端末に特別なソフトウェアをインストールする必要がなく、導入が容易	連携可能
リモートアクセス検疫	SSL-VPN 方式	リモートアクセス環境における検疫を実現する	認証スイッチとしての連携は不可。

表 1.1-2 iNetSec Inspection Center の主なセキュリティポリシー検査項目

項番	検査項目	詳細
1	セキュリティパッチ	Windows/Internet Explorer/Microsoft Office のセキュリティパッチ適用状況
2	ウイルス対策ソフト	主要ウイルス対策ソフトの導入状況､パターンファイル更新状況、リアルタイムスキャン設定状況
3	ソフトウェア導入	義務付けソフトウェア(セキュリティソフトウェア等)の導入状況
4	禁止ソフトウェア	ポリシーで使用を禁止するソフトウェア(例えば Winny 等の P2P ソフト)の未インストール状況
5	パスワード	Windows ログオン、スクリーンセーバーのパスワードの設定状況
6	ファイアウォール	パーソナルファイアウォール(Windows、ウイルス対策ソフト)の設定状況
7	MAC アドレス	端末の管理登録状況(管理外端末の不正接続排除)

表 1.1-3 iNetSec Inspection Center の動作環境

検疫サーバ	Red Hat Enterprise Linux 4.6、5.1(for x86)
認証サーバ	Red Hat Enterprise Linux 4.6、5.1(for x86)
クライアント端末 (IEEE802.1X 認証 VLAN 方式)	Windows 98SE(*1)、Windows Me(*1)、 Windows 2000、Windows XP、Windows Vista
クライアント端末 (ゲートウェイ方式)	Windows 98SE(*1)、Windows Me(*1)、 Windows NT4.0(*1)、Windows 2000、 Windows XP、Windows Vista、 Windows Server 2003(R2 含む)、 Windows Server 2008
	Mac OS(*1)、Red Hat Linux(*1)
クライアント端末 (SSL-VPN 方式)	Windows 2000、Windows XP、Windows Vista
	Mac OS(*1)

(*1) 検疫(セキュリティ監査)を実施せず、ユーザ認証による運用となります。

1.2. IEEE802.1X 認証 VLAN 方式による連携

表 1.1-1の 3 つのネットワーク認証方式のうち、IEEE802.1X認証VLAN方式を用いて、AXシリーズと連携した検疫システムの概要を説明します。

1.2.1. AX の IEEE802.1X 認証方式を用いた検疫概要

AX シリーズのサポートする IEEE802.1X 認証機能と iNetSec Inspection Center を連携した IEEE802.1X 認証 VLAN 方式による検疫ネットワークを構築します。
構築に必要なソフトウェアを表 1.2-1 に示します。

表 1.2-1 IEEE802.1X 認証方式の必須ソフトウェア構成

基本ソフトウェア	iNetSec Inspection Center V5.0 サーバパッケージ
	iNetSec Inspection Center V5.0 クライアントライセンス
オプション製品	iNetSec Inspection Center V5.0 認証サーバパッケージ
	iNetSec Inspection Center V5.0 802.1X サプリカントライセンス

検疫を行うクライアントには、オプション製品の iNetSec Inspection Center V5.0 802.1X サプリカントライセンスをインストールします。検疫を行うサーバには、iNetSec Inspection Center V5.0 サーバパッケージと iNetSec Inspection Center V5.0 認証サーバパッケージをインストールして、検疫サーバを構成します。
802.1X サプリカントが認証処理を開始すると、AX は検疫サーバと通信を行い、IEEE802.1X 認証を実施します。このとき、検疫サーバはセキュリティ検査を実行します。認証が成功すると、クライアントには検疫結果に対応した VLAN が動的に割り当てられ、クライアントは IP アドレスを DHCP サーバから取得して通信が可能になります。認証が失敗した場合は、IP アドレスが取得できず通信不可となります。

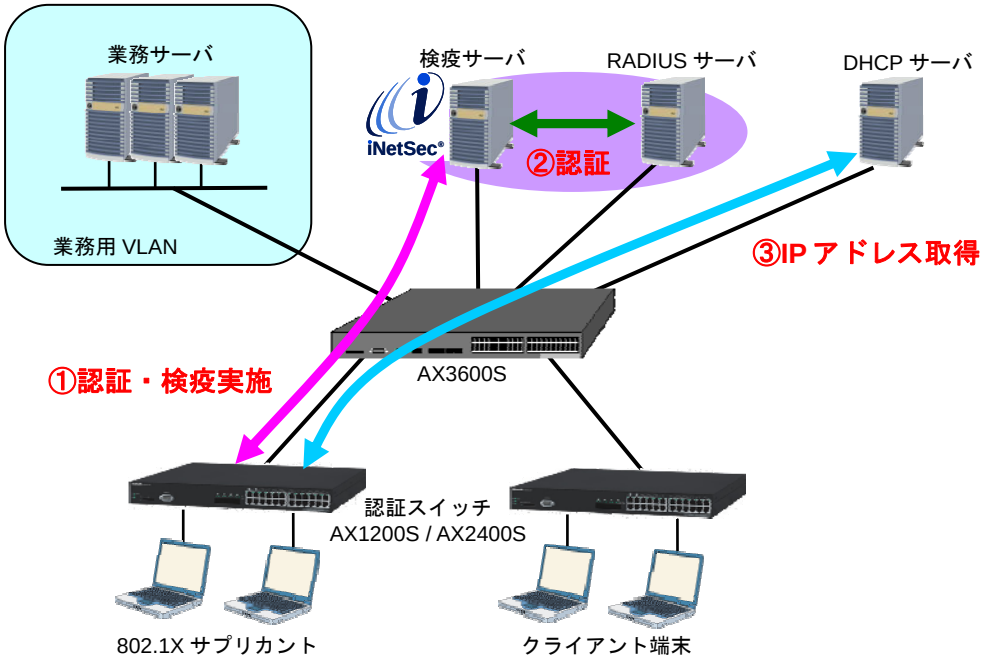


図 1.2-1 iNetSec Inspection Center と AX を用いた検疫ネットワーク概要

検疫サーバ 1 台でも検疫を行うことができますが、iNetSec Inspection Center の RADIUS プロキシ機能を用いて、外部 RADIUS サーバと連携した検疫を実施する事もできます。本ガイドでは、既存の RADIUS サーバを用いて検疫ネットワークシステムを構築する方法を示します。

1.2.2. 検疫シーケンス

IEEE802.1X 認証 VLAN 方式の検疫シーケンスを以下に示します。

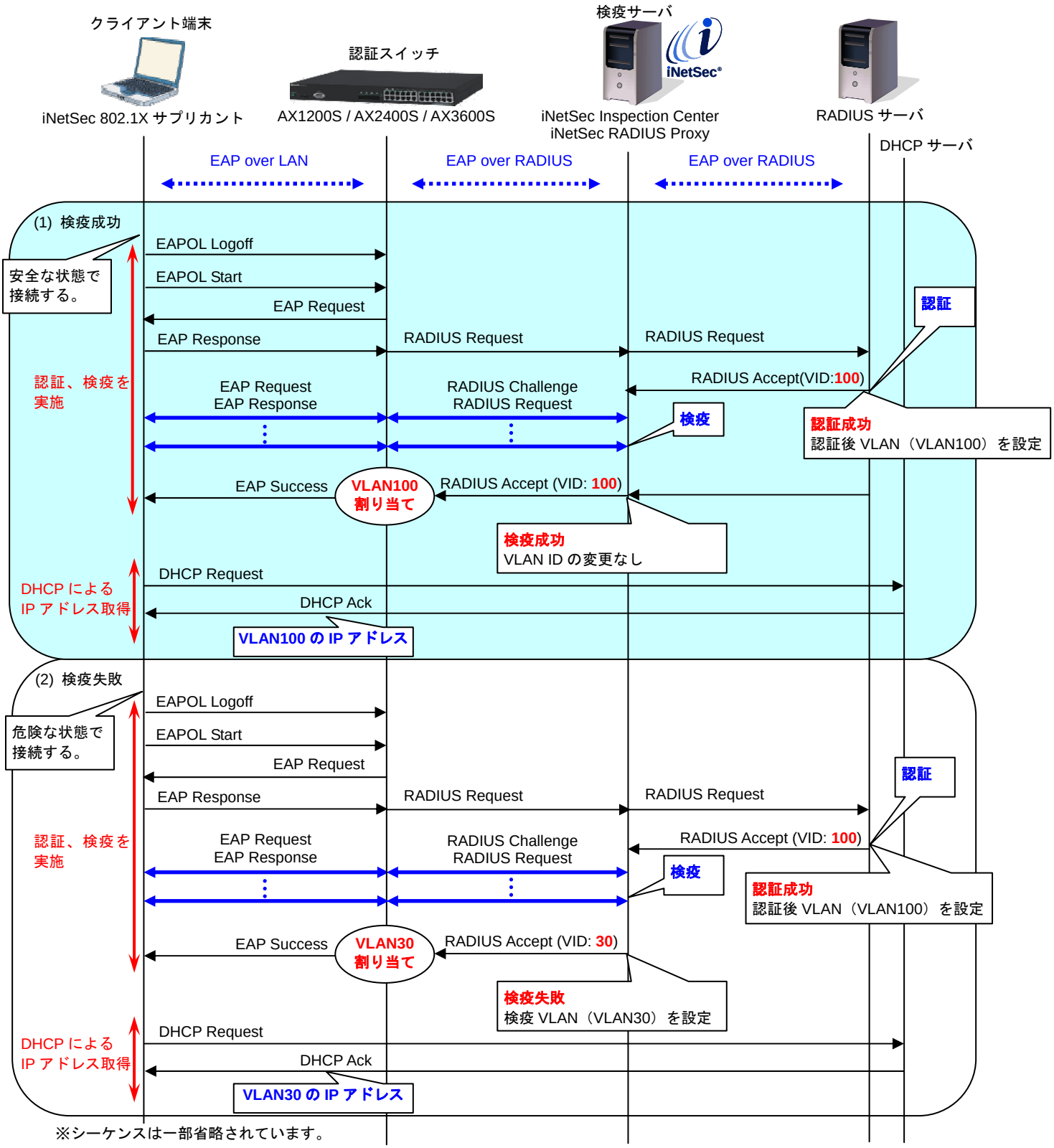


図 1.2-2 検疫認証シーケンス

検疫成功時と検疫失敗時の動作について、以下に示します。

(1) 検疫成功

端末をネットワークに接続すると、802.1X サプリカントは EAPOL-Logoff を送信してから IEEE802.1X 認証処理を開始します。RADIUS サーバはユーザ認証を行い、成功すると認証後 VLAN ID を送信します。検疫サーバはセキュリティポリシーに適合しているか検査を行います。検査時間は 10 秒程度になります。検査が成功すると、検疫サーバは RADIUS サーバから送られてきた VLAN ID をそのまま認証スイッチに送信します。

検疫完了した端末は DHCP サーバから IP アドレスを取得し、ネットワーク通信が可能となります。

(2) 検疫失敗

検疫サーバがセキュリティポリシーに不適合と判断した場合、RADIUS サーバから送られてきた VLAN ID を検疫 VLAN ID に書き換えて認証スイッチに送信します。

検疫完了した端末は、検疫 VLAN の IP アドレスを取得し、制限されたネットワーク通信が可能となります。

1.2.3. IEEE802.1X 認証 VLAN 方式による検疫の特徴

AX シリーズと iNetSec Inspection Centerによる検疫ネットワークシステム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、端末単位(VLAN 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またはポート単位で混在できるので、802.1X サプリカントをインストールできない端末でも認証のみの端末として混在することができます。これにより、例えば、部署単位での検疫システムの導入が可能になります。

1.3. ゲートウェイ方式による連携

表 1.1-1に示すiNetSecの 3 つの動作モードのうち、ゲートウェイ方式による検疫システムの連携の概要を説明します。

1.3.1. AX とゲートウェイ方式を用いた検疫概要

AX シリーズのサポートする Web 認証機能と iNetSec Inspection Center のゲートウェイ方式を連携した検疫ネットワークの構築概要を説明します。

構築に必要なソフトウェアを表 1.3-1 に示します。詳細に関しては iNetSec の「Web 認証方式認証機器連携導入設定手順書」を参照して下さい。

表 1.3-1 AX と連携する iNetSec ゲートウェイ方式のソフトウェア構成

基本ソフトウェア	iNetSec Inspection Center V5.0L10A　サーバパッケージ
	iNetSec Inspection Center V5.0 クライアントライセンス
	iNetSec Inspection Center V5.0L10A サーバパッケージ 認証機器拡充固有修正（AX と連携する場合に適用）
オプション製品	iNetSec Inspection Center V5.0 認証サーバパッケージ 外部 RADIUS を使用する場合は必須ではありません（任意）

※ゲートウェイ方式では検疫サーバ上に認証スイッチの切替用アカウント制御用として、サーバパッケージに含まれる認証機器連携アダプタをインストールするか、または同一検疫サーバ上にiNetSec Inspection Center V5.0認証サーバパッケージをインストールする必要があります。

次に表 1. 3–1 に示すソフトウェアをインストールする機器について説明します。iNetSec Inspection Center のゲートウェイ方式では、検疫を行うクライアントに特別なソフトウェアをインストールする必要はありません。Web ブラウザにて認証と検疫を実施します（Web ブラウザで ActiveX を有効にする必要があります）。

機器構成として図 1.3-1に示す検疫サーバにiNetSec Inspection Centerの基本ソフトウェアのサーバパッケージと認証機器拡充固有修正をインストールすることでAXシリーズのWeb認証と連携します。またユーザ認証サーバとして他社製の外部RADIUSサーバかiNetSec Inspection Center V5.0 認証サーバパッケージを使用します。

なお、クライアント端末の検疫のみを行う場合はユーザ認証は省略することが可能です。

1.3.2. 各装置の役割

図 1.3-1 に示す検疫システムを構成する各装置の役割を解説します。

（１）**検疫サーバ**

iNetSec Inspection Center をインストールした検疫サーバはクライアントへの ActiveX の配布と検疫の実施、認証スイッチから見た RADIUS サーバとして動作します、検疫成功時に一時的に切替用アカウントを有効化し認証スイッチからの認証に備えます。

（２）**RADIUS サーバ**

検疫サーバへアクセスしたユーザの認証行います。

（３）**認証スイッチ**

AX 認証スイッチの Web 認証機能を利用してネットワークのアクセス制御を担当します。認証前ユーザの検疫サーバや修復サーバへの限定した通信許可や業務サーバなどの機密性の高いサーバへの通信遮断等のネットワーク制御を行います。またリダイレクト機能により認証前クライアントの Web アクセスを検疫サーバに誘導します。

（４）**クライアント端末**

Webアクセスを行うと認証スイッチにより検疫サーバに誘導され、初回のみActiveXのダウンロードを行います。ActiveXダウンロード以降は、Web認証画面にてユーザID、パスワードを入力しユーザ認証を実施。認証成功後、検疫が実行されます。検疫に成功したクライアント端末は、ActiveXにより認証スイッチに対し切替用アカウントで再度認証が行われます。

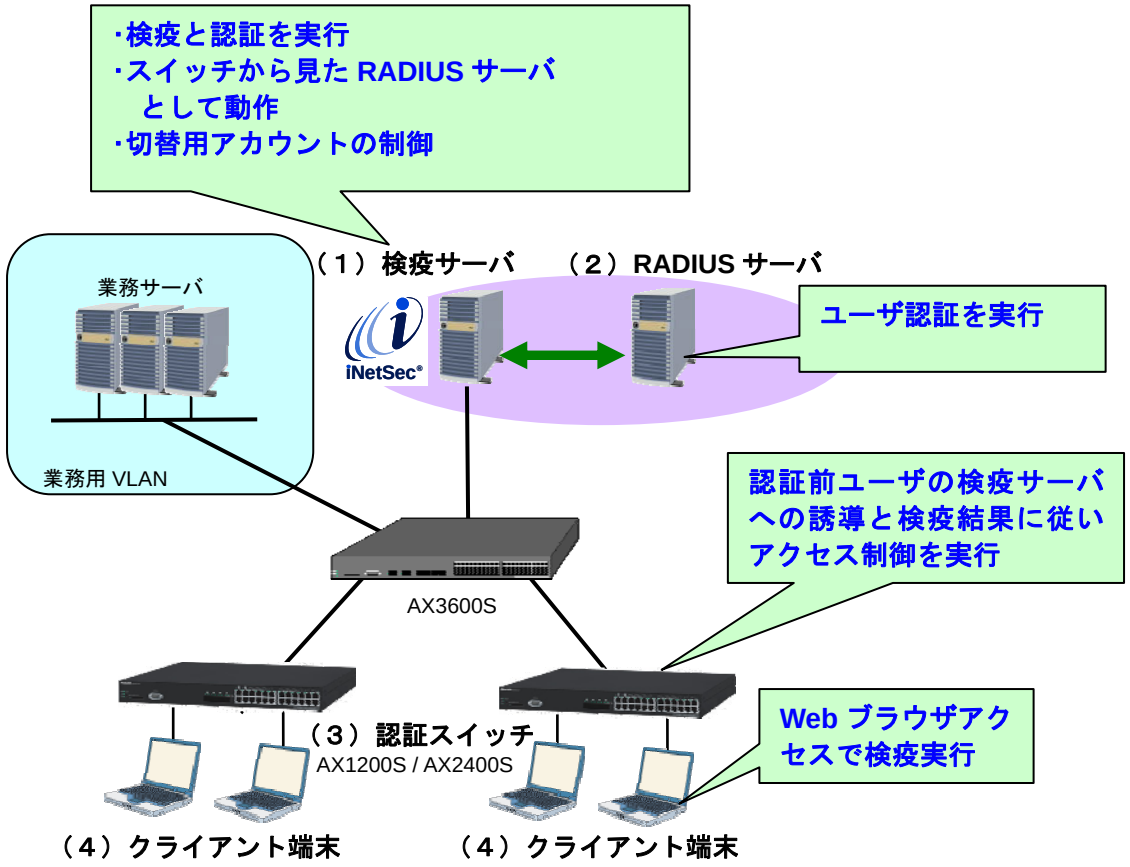
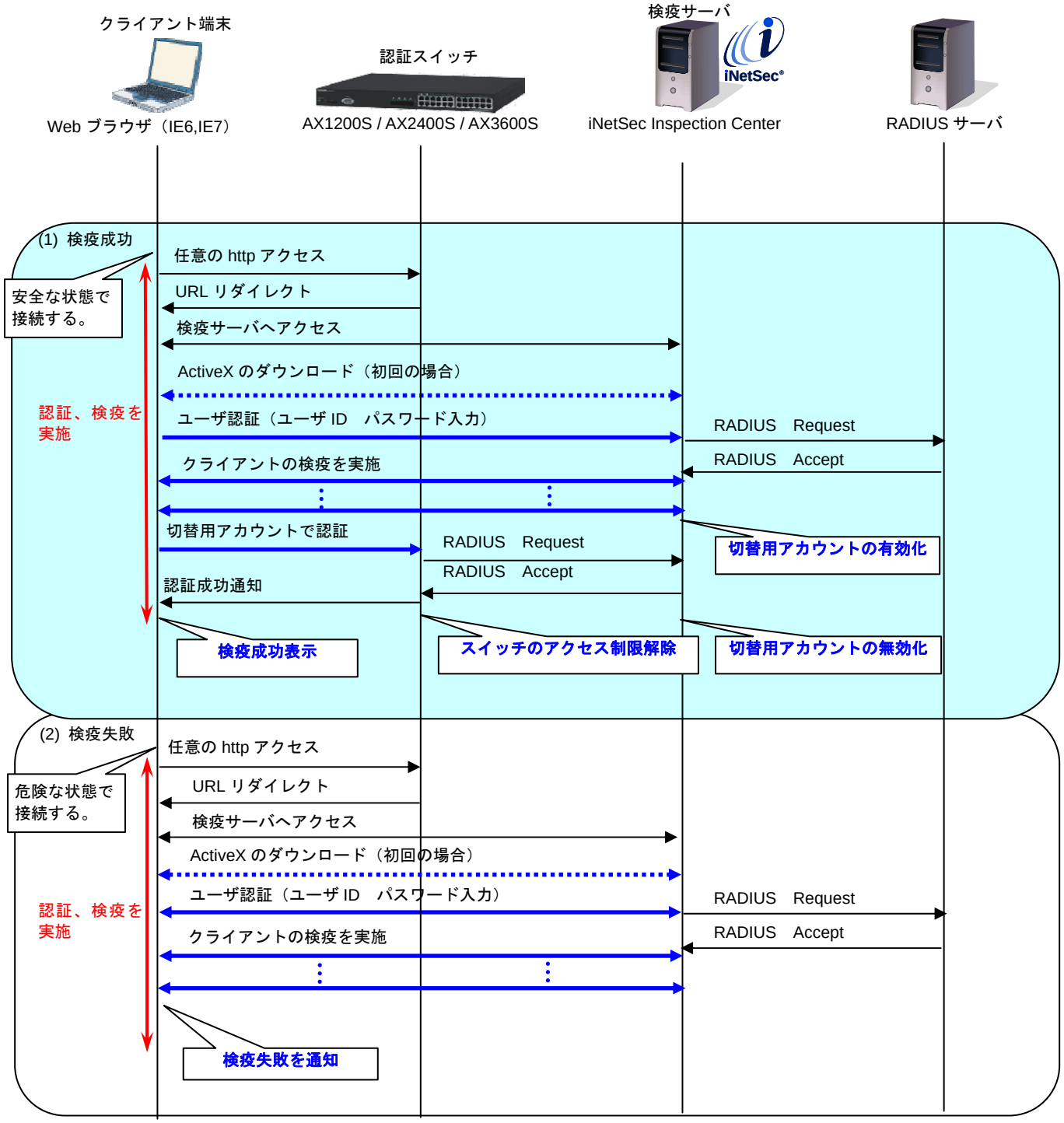


図 1.3-1 ゲートウェイ方式による検疫ネットワーク連携概要

1.3.3. 検疫シーケンス

ゲートウェイ方式の検疫シーケンスと検疫結果毎の動作説明を以下に示します。



※シーケンスは一部省略されています。

図 1.3-2 検疫認証シーケンス

検疫成功時と検疫失敗時の動作について、以下に示します。

（1） 検疫成功

認証前のクライアント端末からユーザがWebブラウザを使用して任意のURLへアクセスした場合、AX 認証スイッチの URL リダイレクト機能により検疫サーバの URL へリダイレクトされます。このとき初回の接続の端末は ActiveX のダウンロード要求へ遷移し、ActiveX ダウンロード済みの端末はログイン画面が開きます。

ユーザ ID とパスワードを入力すると検疫サーバから外部 RADIUS へユーザ認証を実施します。成功すると端末の検疫を実施します。検疫成功後に検疫サーバ上の切替用アカウントが活性化され、端末側から自動的に認証スイッチへ切替用アカウントで認証します。その後ログイン成功画面が表示され、業務ネットワークへの通信が可能となります。

（2） 検疫失敗

検疫に失敗した場合は、検疫サーバの切替用アカウントは活性化されず、クライアント端末からの認証も実施されません、Web ブラウザで認証スイッチに直接アクセスしても検疫サーバへリダイレクトされるため、通常 Web ブラウザから認証操作は不可能とります。たとえ直接認証パケットを送付しても切替用アカウントは非公開かつ非活性のため接続不可能となります。

1.3.4. ゲートウェイ方式を用いた検疫の特徴

AX シリーズと iNetSec Inspection Center によるゲートウェイ方式を用いた検疫ネットワークシステムの特徴を以下に示します。

（１） 未認証端末を自動的に検疫サーバへ誘導

AX シリーズがサポートする Web 認証の URL リダイレクト機能により認証前のクライアント端末を検疫サーバへ誘導します。また、ゲートウェイ方式はエージェントレスで検疫可能なため事前の端末へのソフト導入の手間が省けます。

（２） 検疫対象外端末を同一ポートに収容可能

プリンタなどの Web ブラウザ機能を持たない端末は AX シリーズがサポートする MAC 認証で検疫を除外する事が可能です。

iNetSec Inspection Center で MacOS や Linux などの検疫対象外端末を認証のみで接続可能とする設定ができますので、AX シリーズの同一ポートに検疫対象端末と検疫対象外端末の両方を収容できる OS 混在環境が容易に導入できます。

1.3.5. ゲートウェイ方式での検疫対象外端末について

iNetSec Inspection Center のゲートウェイ方式では、クライアント端末から検疫サーバへの Web アクセスの際にクライアント端末の OS を検査し検疫対象であるか判断します。Windows 系 OS であれば検疫を実施し、検疫対象外の MacOS や Linux などの OS は認証のみで接続するというシステムを構築する事ができます。

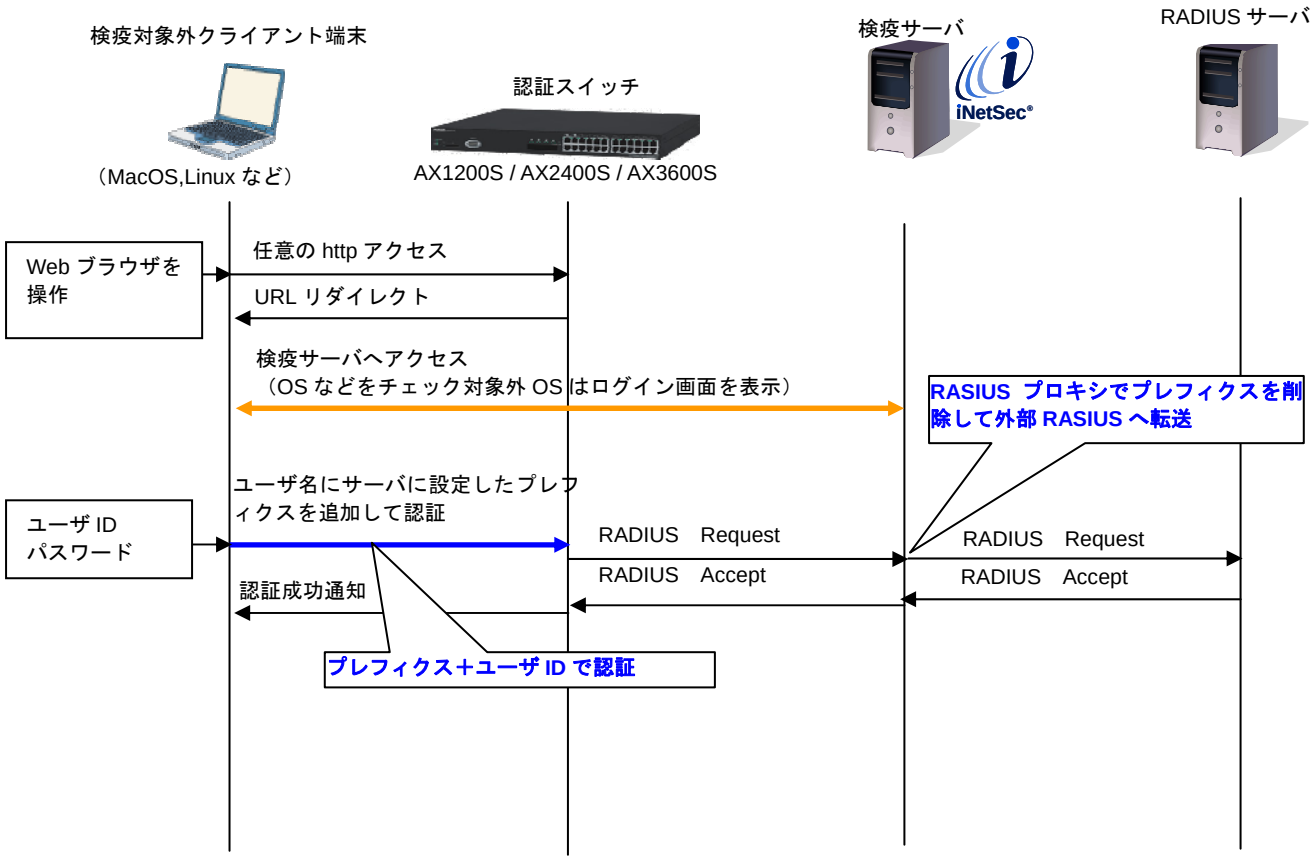


図 1.3-3 検疫対象外 OS の認証シーケンス

クライアント端末がウェブブラウザで任意のサイトにアクセス要求すると、認証スイッチは検疫サーバにリダイレクトします。このとき、検疫サーバはOS種別を判定し、認証画面を表示します。非Windowsからのアクセスの場合、ユーザが認証画面に入力したユーザIDに検疫対象外OS用のプレフィックス（※）が付加され認証スイッチに渡されます。認証スイッチはRADIUSサーバとして設定されている検疫サーバに認証要求を送信し、検疫サーバではユーザIDの検疫対象外OSのプレフィックスの有無を判定しプレフィックスがあった場合、登録された外部RADIUSサーバへプレフィックスを削除し転送します。この動作により、ユーザは検疫対象OSと検疫対象外OSを意識することなく混在することが可能となります。
※検疫対象外OS接続は検疫サーバに設定が必要です。設定方法は**4.8.1検疫対象外**を参照して下さい。

プリンタなどWeb機能を持たない機器を除外する場合はAXシリーズのサポートするMAC認証に検疫除外の設定を行ないます。設定方法は**4.8.2MAC認証の設定方法**を参照して下さい。

2. iNetSec Inspection Center と連携可能な AX シリーズの認証方式と収容条件

iNetSec Inspection Center 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 iNetSec Inspection Center と連携可能な認証方式

認証方式	認証モード	AX1200S	AX2400S AX3600S	AX6300S AX6700S
IEEE802.1X 認証	固定 VLAN	ー	ー	ー
	動的 VLAN	○	○	○
Web 認証	固定 VLAN	○	○	○
	動的 VLAN	ー	ー	ー
MAC 認証	固定 VLAN	ー	ー	ー
	動的 VLAN	ー	ー	ー

(凡例) ○：検疫連携可能　ー：検疫連携不可

AX シリーズの最大認証端末数を以下に示します。
なお、MAC認証は検疫未対応端末を接続するときに利用します。（3.8を参照）

表 2-2 認証方式毎の最大認証端末数

認証方式	認証モード	AX1200S		AX2400S AX3600S		AX6300S AX6700S	
IEEE802.1X 認証	動的 VLAN	256/装置	合計 256/装置	256/装置(*1)	合計 256/装置(*1)	4096/装置	合計 4096/装置
MAC 認証		256/装置		256/装置(*1)		×	
Web 認証	固定 VLAN	1024/装置	合計 1024/装置	1024/装置	合計 1024/装置	4096/装置	合計 4096/装置

(凡例) ×：未サポート
(*1) AX3640Sでは 1024/装置となります。

3. 検疫ネットワークの構築（IEEE802.1X 認証 VLAN 方式）

本章では、AXシリーズのIEEE802.1X認証方式（動的VLANモード）を用いた検疫ネットワークの構築例として、既に稼動中のIEEE802.1X認証ネットワークシステムに検疫サーバを増設して検疫ネットワークシステムを構築する場合を説明します。

3.1. 概要

検疫ネットワークの基本的な構成を図 3.1-1 に示します。

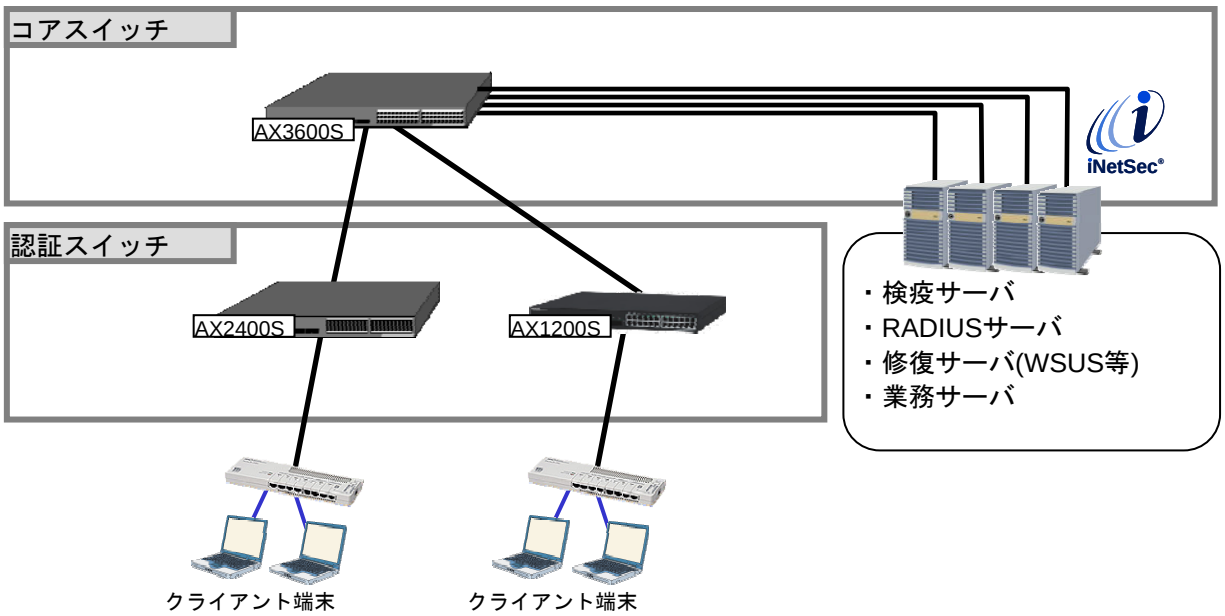


図 3.1-1 検疫ネットワークの基本構成(IEEE802.1X 認証 VLAN 方式)

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、検疫を行う端末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

検疫サーバ	RADIUS サーバ	クライアント端末
Red Hat Enterprise Linux Server release 5 ・iNetSec Inspection Center サーバパッケージ ・iNetSecInspection Center 認証サーバパッケージ	Windows Server 2003 ・ActiveDirectory ドメインコントローラ ・RADIUS サーバ(IAS)	Windows XP ・iNetSec Inspection Center 802.1X サプリカント Windows Vista ・iNetSec Inspection Center 802.1X サプリカント

3.2. 検疫ネットワーク構成図

検疫ネットワークの基本構成（IEEE802.1X 認証 VLAN 方式）を、具体的な構成例で示したものを以下に示します。

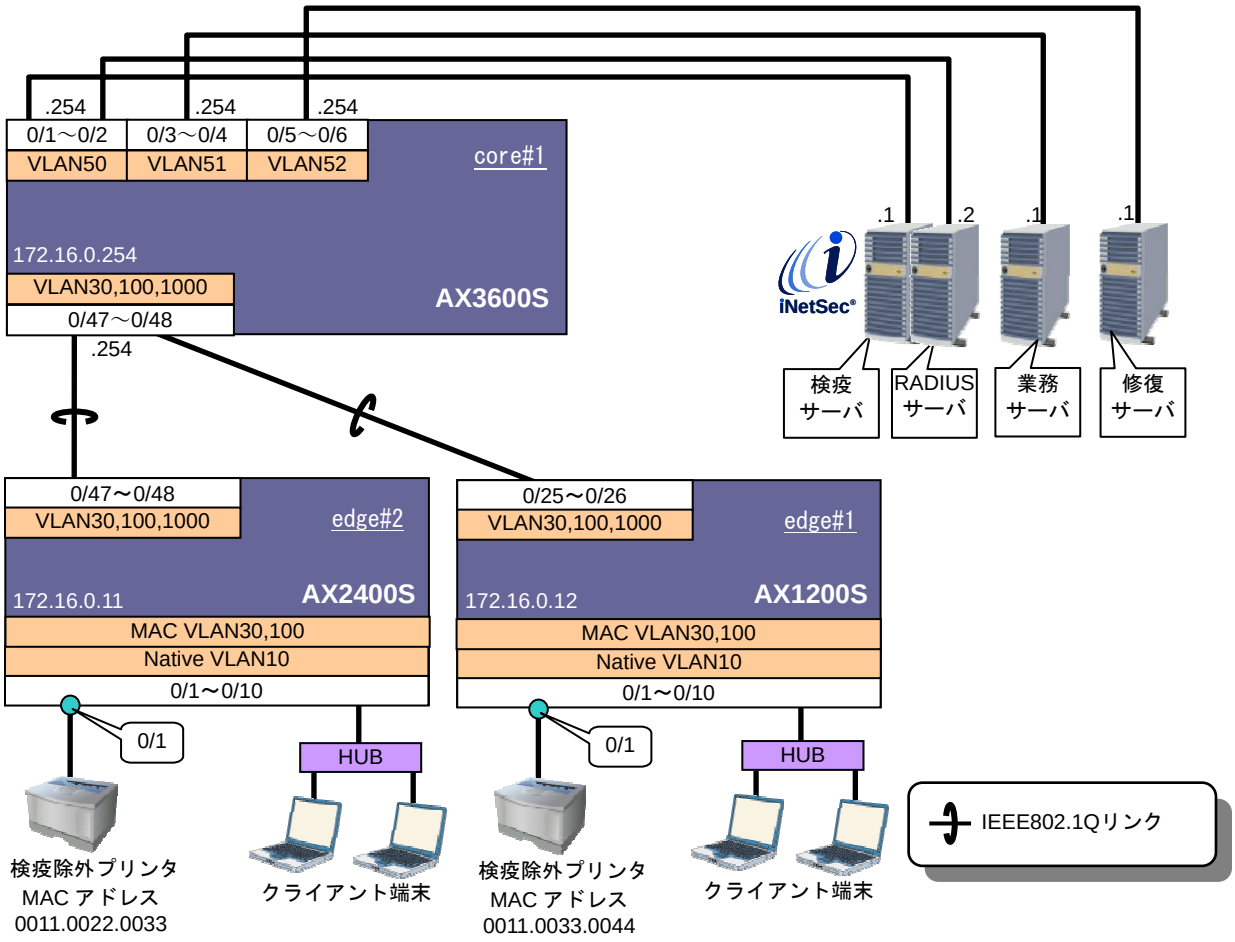


図 3.2-1 検疫ネットワーク構成図

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	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	MAC VLAN ポート	MAC 認証 (動的 VLAN)	10	30	100
		0/1～0/10		IEEE802.1X 認証 (動的 VLAN)			
	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	MAC VLAN ポート	MAC 認証 (動的 VLAN)	10	30	100
		0/1～0/10		IEEE802.1X 認証 (動的 VLAN)			
	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 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･検疫が成功した端末と通信可能なサーバが所属する VLAN。(社内ネットワーク)	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	192.18.100.0/24	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。	

クライアント端末の所属する VLAN に応じた各サーバへのアクセス制御を以下に示します。

表 3.2-3　VLANーサーバ間通信の可否

送信元 ＼ 送信先		検疫サーバ RADIUS サーバ	業務サーバ	修復サーバ
認証前 VLAN	10	×	×	×
検疫 VLAN	30	×	×	○
認証後 VLAN	100	○	○	○

表 3.2-4　本ガイドの構築例（IEEE802.1X 認証 VLAN 方式）で設定する ID、パスワード一覧

項番	設定先	項目名	値	説明	本ガイド内の設定箇所
1	AX 認証スイッチ	radius key	alaxala	RADIUS シークレット	3.4.1 の（2）、 3.4.2 の（1）
2		mac-authentication	macpass	MAC 認証用パスワード	3.4.1 の（5）、 3.4.2 の（4）
3	検疫サーバ	PrimaryAuthSecret	alaxala	RADIUS シークレット	3.6.1の②
4	外部 RADIUS サーバ	共有シークレット	alaxala	RADIUS シークレット	3.5.1の③

※表 3.2-4 で示す値は構築する環境に合わせて任意に変更して下さい。但し項番 1,3,4,7 の RADIUS シークレットにはそれぞれ同じ値を使用して下さい。

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、既に稼動中のIEEE802.1X認証ネットワークから検疫ネットワークへ移行する場合の構築ポイントを以下に示します。

（１） 検疫 VLAN ID を決める。

検疫 VLAN は、検疫サーバによって検疫失敗と判断された端末に対して、動的に割り当てられる VLAN です。IEEE802.1X 認証の認証後 VLAN とは異なる VLAN ID を設定してください。本ガイドでは、VLAN30 を検疫 VLAN としています。

検疫 VLAN を設定する機器は、認証スイッチ、コアスイッチおよび検疫サーバとなります。

（２） 検疫 VLAN にフィルタを設定する。

表 3.2-3に示すように、検疫失敗した端末は修復サーバのみと通信可能です。この他に、端末が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 VLAN に適用しています。

(a) 修復サーバ「10.51.0.1」との通信を許可する
(b) DHCP 通信を許可する

検疫サーバに対して ping 導通確認などを行いたい場合は、適宜アクセスリストを追加して下さい。

（３） 検疫サーバを RADIUS サーバとして設定する。

本ガイドでは、既存の RADIUS サーバを利用するため、認証機器連携アダプターを RADIUS プロキシサーバとしています。認証スイッチには検疫サーバを RADIUS サーバとして設定して下さい。

（４） 検疫除外端末を接続するポートに MAC 認証を設定する。

プリンタなどの検疫が実施できない端末を接続する場合、接続するポートにMAC認証を設定します。(詳細は3.8を参照)

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。 **※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 10,1000** **(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 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 を作成します。 ➢ **構築ポイント（１）** 認証後 VLAN として MAC VLAN100 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	
●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（１）**
●上位スイッチとの通信用 **(config)# interface rqnge gigabitethernet 0/25-26** **(config-if-range)# switchport mode trunk** **(config-if-range)# switchport trunk allowed vlan 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 VLAN30、100 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。
RADIUS サーバの設定	
(config)# radius-server host 10.50.0.1 key alaxala	検疫サーバの 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。 ➢ **構築ポイント（３）**
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） 検疫 VLAN 用アクセスリストの設定

AX1200S の設定	
アクセスリストの設定	
(config)# ip access-list extended Quarantine **(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** **(config)# interface vlan 30** **(config-if)# ip access-group Quarantine in**	以下のアクセスリスト「Quarantine」を作成します。 ・検疫 VLAN30 から修復サーバ「10.52.0.1」への通信を許可する。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信を許可する。 ・DHCP サーバ通信を許可する。 ・DHCP クライアント通信を許可する。 検疫 VLAN30 にアクセスリストを適用します。 ➢ **構築ポイント（２）**

（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 supplicant-detection disable** **(config)# dot1x system-auth-control** 以下の設定は、環境に合わせて行います。 **(config-if-range)# dot1x timeout reauth-period 600**	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 disable にして、EAP-Request/Identity の送信を抑止します。 IEEE802.1X 認証を有効にします。 サプリカントの再認証周期を **600 秒(10 分)**に設定します。

（５） MAC 認証の設定

AX1200S の設定	
物理ポートの設定	
(config)# interface fastethernet 0/1 **(config-if)# mac-authentication port**	ポート 0/1 を MAC 認証用ポートとして設定します。 ➢ **構築ポイント（４）**
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** 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。 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。

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 10,1000** **(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 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 を作成します。 ➢ **構築ポイント（１）** 認証後 VLAN として MAC VLAN100 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	
●認証用 **(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（１）**
●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 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 VLAN30、100 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 172.16.0.11 255.255.255.0**	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 10.50.0.1 key alaxala	検疫サーバの IP アドレスおよびキーを設定します。この例ではキーを「alaxala」としています。 ➢ **構築ポイント（３）**
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） 検疫 VLAN 用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 Quarantine **(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 any eq bootps** **(config-ext-nacl)# permit udp any any eq bootpc** **(config)# interface vlan 30** **(config-if)# ip access-group Quarantine in**	以下のアクセスリスト「Quarantine」を作成します。 ・検疫 VLAN30 から修復サーバ「10.52.0.1」への通信を許可する。 ・修復サーバ「10.52.0.1」から検疫 VLAN30 への通信を許可する。 ・DHCP サーバ通信を許可する。 ・DHCP クライアント通信を許可する。 検疫 VLAN30 にアクセスリストを適用します。 ➢ **構築ポイント（２）**

（３） 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)# dot1x vlan dynamic radius-vlan 30,100 **(config)# dot1x vlan dynamic enable** **(config)# dot1x vlan dynamic reauthentication** **(config)# dot1x vlan dynamic supplicant-detection disable** **(config)# dot1x system-auth-control** 以下の設定は、環境に合わせて行います。 **(config)# dot1x vlan dynamic timeout reauth-period 600**	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（１）** IEEE802.1X 認証を有効にします。 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 disable にして、EAP-Request/Identity の送信を抑止します。 IEEE802.1X 認証を有効にします。 サプリカントの再認証周期を **600 秒(10 分)**に設定します。

（４） MAC 認証の設定

AX2400S の設定	
物理ポートの設定	
(config)# interface gigabitethernet 0/1 **(config-if)# mac-authentication port**	ポート 0/1 を MAC 認証用ポートとして設定します。 ➢ **構築ポイント（４）**
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** 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。 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。

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 30,100** **(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。 検疫 VLAN として VLAN30 を、認証後 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 0/3-4** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 51** **(config)# interface range gigabitethernet 0/5-6** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 52** **(config)# interface range gigabitethernet 0/47-48** **(config-if-range)# switchport mode trunk** **(config-if-range)# switchport trunk allowed vlan 30,100,1000**	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 0/3～0/4 を、アクセスポートとして設定します。 アクセスポートに VLAN51 を設定します。 ポート 0/5～0/6 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 0/47～0/48 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 VLAN30、100 および 1000 を設定します。
インタフェースの設定	
(config)# interface vlan 30 **(config-if)# ip address 192.168.30.254 255.255.255.0** **(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 30 **(config-if)# ip helper-address 10.50.0.2** **(config)# interface vlan 100** **(config-if)# ip helper-address 10.50.0.2**	VLAN30 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。

3.5. 外部 RADIUS サーバの設定

本ガイドでは、Windows Server 2003 の IAS を RADIUS サーバとして用いています。システムを利用するユーザやグループなどは、既に設定済みであるものとします。

3.5.1. RADIUS クライアントの設定

既存の RADIUS サーバを用いて検疫ネットワークを構築するには、検疫サーバを RADIUS クライアントとして新たに登録する必要があります。本ガイドでは、Windows Server 2003 の IAS における RADIUS クライアントの設定方法について示します。

① 「スタート」→「管理ツール」→「インターネット認証サービス」を開き、左画面の中の「RADIUS クライアント」を右クリックして「新しい RADIUS クライアント」をクリックする。

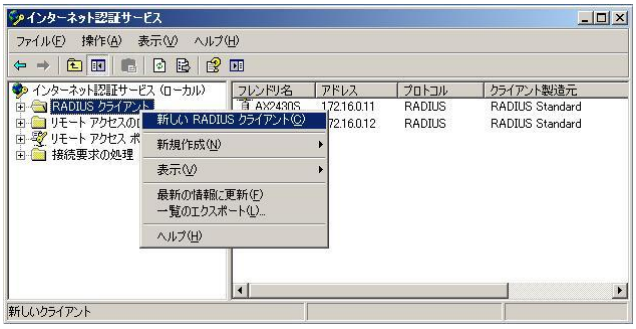


図 3.5-1 RADIUS クライアント設定1

② 新しいクライアント画面にて、下記 2 項目を入力し「次へ」をクリックする。
- **フレンドリ名**：任意（本ガイドでは「iNetSec」）
- **クライアントのアドレス**：検疫サーバの IP アドレス（本ガイドでは「10.50.0.1」）

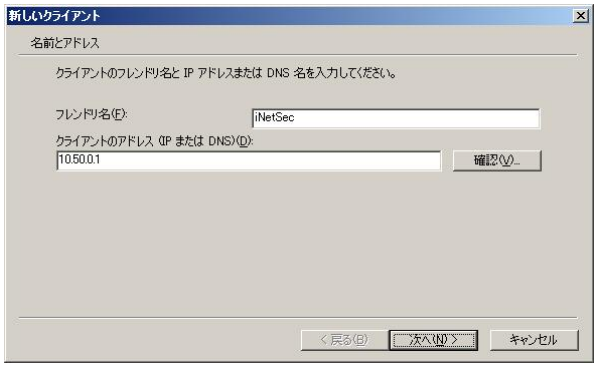


図 3.5-2 RADIUS クライアント設定 2

③ 新しい RAIDUS クライアント画面にて共有シークレットを入力し、「完了」をクリックする。

図 3.5-3 RADIUS クライアント設定 3

3.6. 検疫サーバの設定

本ガイドでは、1 台のマシンに iNetSec Inspection Center V5.0 サーバパッケージと iNetSec Inspection Center V5.0 認証サーバパッケージをインストールして検疫サーバを構成しているものとします。インストール方法および初期設定については、「iNetSec Inspection Center V5.0 L10 ユーザーズガイド」および「iNetSec Inspection Center V5.0 L10 認証サーバ ユーザーズガイド」をご参照ください。

3.6.1. iNetSec 認証サーバの設定

iNetSec 認証サーバの設定方法について示します。

① Web ブラウザで「http:// “検疫サーバの IP アドレス：運用管理 Web サーバのポート番号” /」にアクセスし、「環境設定」をクリックする。

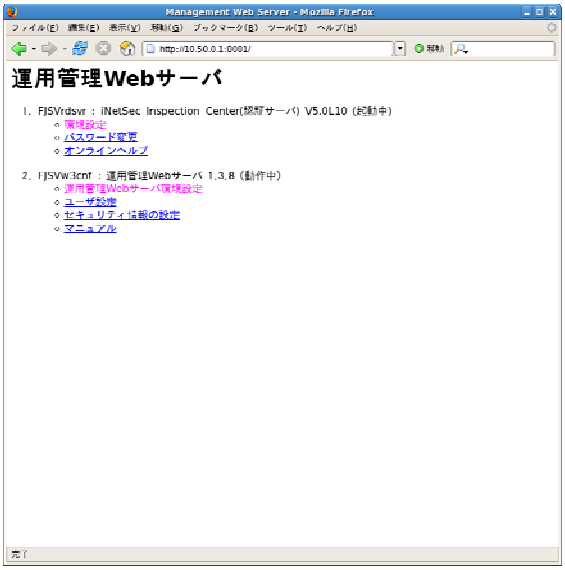


図 3.6-1 認証サーバ 1

② クライアント設定
左画面の中の「クライアント設定」をクリックし、右画面にて下記 2 項目を入力して「追加」をクリックする。

- **クライアントアドレス**：認証スイッチのIPアドレス
- **クライアント認証キー**：3.4で認証スイッチに設定した認証キー

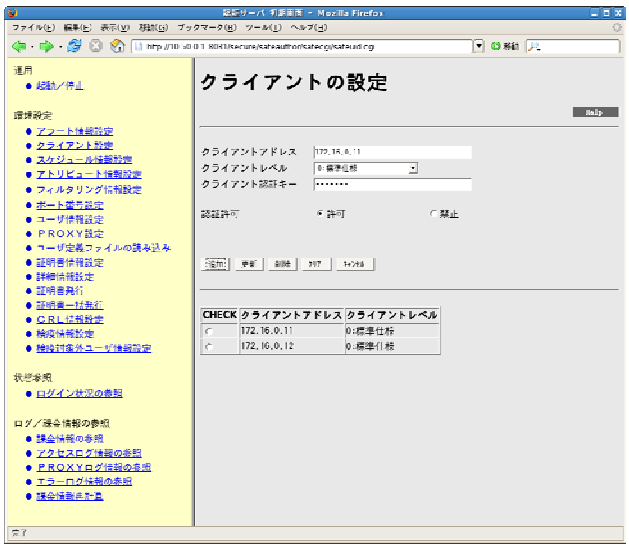


図 3.6-2 認証サーバ 2

③ アトリビュート情報設定
左画面の中の「アトリビュート情報設定」をクリックし、右画面にて検疫失敗時のアトリビュートを設定する。(設定値は表 3.6-1 参照) なお、本ガイドでは「サービスグループ」を「NG」としている。

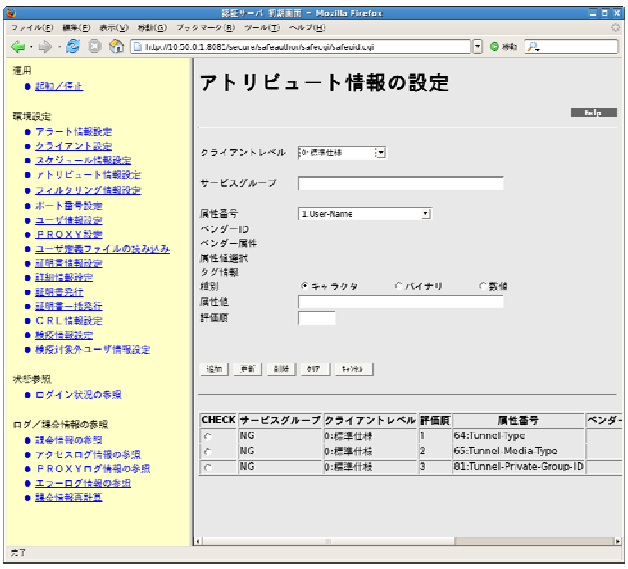
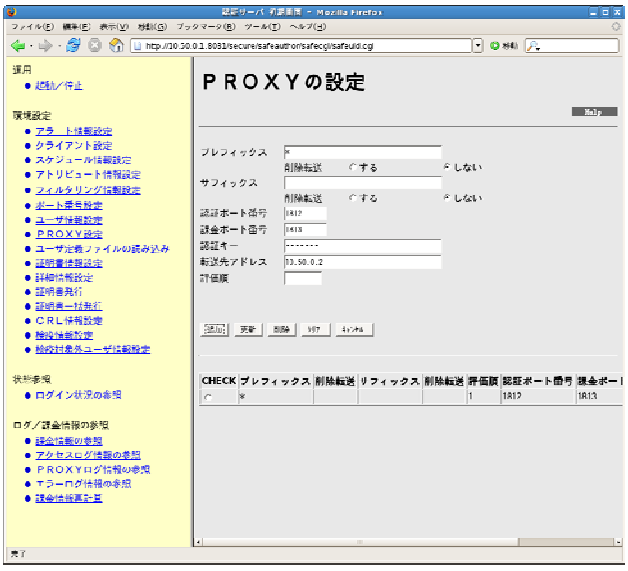


図 3.6-3 認証サーバ 3

表 3.6-1 検疫失敗時のアトリビュート情報

サービスグループ	属性番号	種別	属性値	評価順
NG	64:Tunnel-Type	数値	13	1
NG	65:Tunnel-Media-Type	数値	6	2
NG	81:Tunnel-Private-Group-ID	キャラクタ	**30（検疫 VLAN ID）**	3

④ PROXY設定
左画面の中の「PROXY設定」をクリックし、右画面にて下記 3 項目を入力して「追加」をクリックする。
- **プレフィックス**：「*」
- **認証キー**： 3.5.1でRADIUSサーバに設定した共有シークレット
- **転送先アドレス**：RADIUSサーバのIPアドレス



本例は全て同一サーバへプロキシする設定例となっています

図 3.6-4 認証サーバ 4

⑤ ターミナルウインドウを開き、「/opt/FJSVrdsvr/raddb/radius.conf」に以下の 1 行を追加する。

```
PROXY-OTHER-USER        *
```

⑥ 検疫情報設定
左画面の中の「検疫情報設定」をクリックし、右画面にて下記 3 項目を入力して「設定」をクリックする。

- **検疫サーバ連携指定**：「連携する」
- **RADIUS-PROXY 検疫指定**：「連携する」
- **検疫サーバアドレス**：「http://10.50.0.1/」
- **検疫失敗サービスグループ**：「NG」

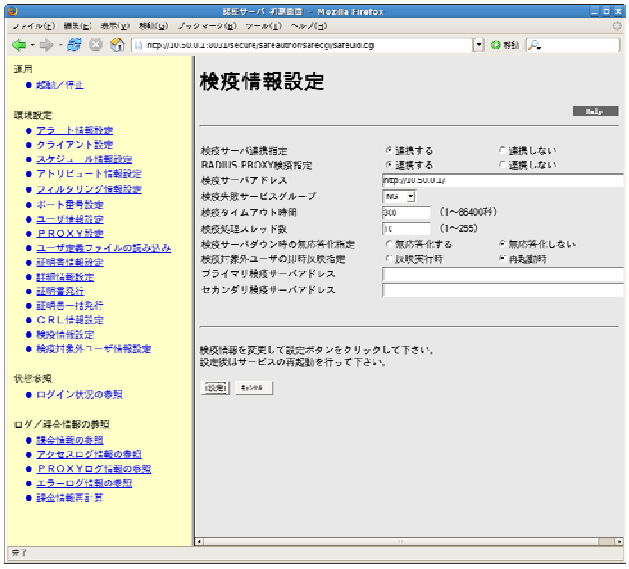


図 3.6-5 認証サーバ 5

⑦ サービスの再起動
左画面の中の「起動／停止」をクリックし、右画面にて「停止」をクリックして認証サーバ状態が「未起動」に変わったことを確認してから「起動」をクリックする。

図 3.6-6 認証サーバ 6

3.6.2. iNetSec Inspection Center の設定

検疫のセキュリティポリシーとして、Windows ファイアウォールが有効になっているかどうかを検査する設定方法を示します。

① 管理者ログイン
Web ブラウザで「https://“検疫サーバの IP アドレス”/quarantine/admin/Login.jsp/」にアクセスする。
検疫ネットワークシステム管理者ログイン画面にて管理者アカウントでログインする。

図 3.6-7 iNetSec Inspection Center の設定 1

② 左画面のメニューより「ファイアウォール」をクリックし、右画面の「選択したファイアウォールが必ず 1 つは入っており、有効になっていることを要求する」を選択し「Microsoft Windows ファイアウォール」にチェックして「反映」をクリックする。

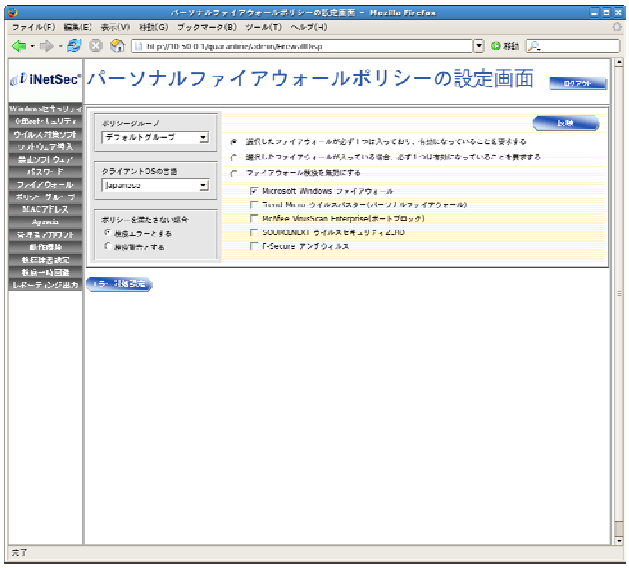


図 3.6-8 iNetSec Inspection Center の設定 2

3.7. 検疫クライアントの設定

iNetSec 802.1X サプリカントのユーザ認証モード設定方法を示します。
詳細は「iNetSec Inspection Center V5.0 L10 802.1X サプリカント ユーザーズガイド」をご参照ください。

3.7.1. インストール時の設定

① ユーザ認証方式の選択
「Windows ログオン後に認証する」にチェックする。

図 3.7-1 クライアントの設定 1

② クライアントアップデートサーバの指定
検疫サーバ（本ガイドでは「http://10.50.0.1/」）を入力する。

図 3.7-2 クライアントの設定 2

3.7.2. インストール後の設定

① Windows のタスクトレイに表示されているアイコンをクリックし、「設定」を選択する。

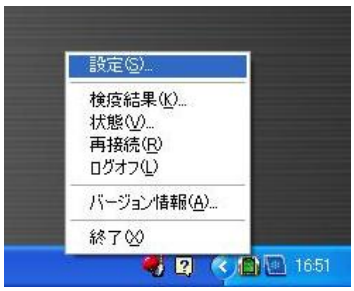


図 3.7-3 クライアントの設定 3

② 設定画面にて「ユーザー設定」タブを選択し、「アダプター一覧」の使用するインタフェースにチェックして「追加」をクリックする。

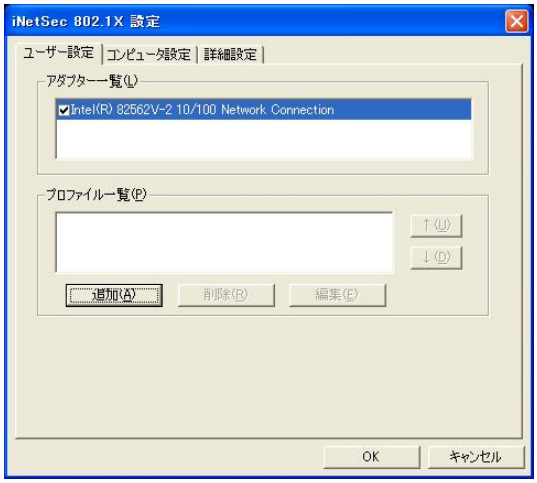


図 3.7-4 クライアントの設定 4

③ プロファイル画面にて以下 3 項目を入力し、「プロパティ」をクリックする。
- **プロファイル名**：任意（本ガイドでは「alaxala」）
- **EAP の種類**：「PEAP v0/EAP-MS-CHAP-V2」
- **「IP アドレスを更新する」にチェック**

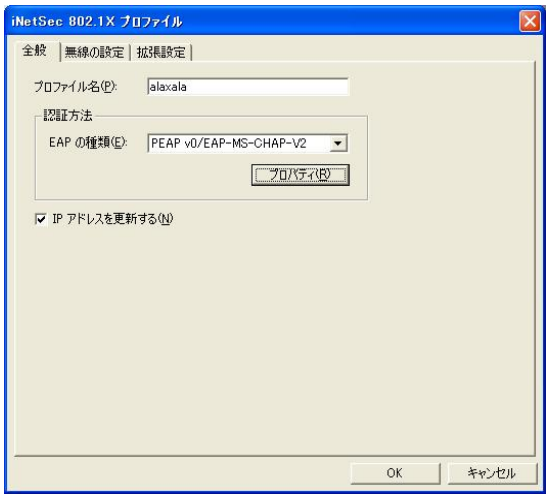


図 3.7-5 クライアントの設定 5

④ プロパティ画面にて RADIUS サーバに登録済みユーザの「ユーザー名」と「パスワード」を入力し「OK」をクリックして画面を閉じる。

図 3.7-6 クライアントの設定 6

⑤ 設定画面にて作成したプロファイルにチェックし、「OK」をクリックして画面を閉じる。

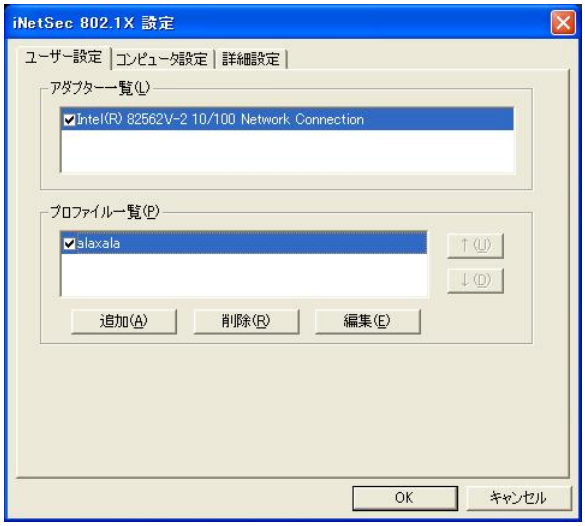


図 3.7-7 クライアントの設定 7

3.8. 検疫未対応端末の接続方法

IEEE802.1X 認証 VLAN 方式の検疫ネットワークシステムにおいて、検疫未対応端末を接続する方法は 2 通りあります。

（1） 検疫対象外ユーザを設定する。

検疫をパスするユーザを登録し、IEEE802.1X 認証のみ行います。
Mac OS や Linux など、クライアントソフトはインストールできないが IEEE802.1X 認証は可能な端末向きです。

（2） MAC 認証を設定する。

端末の MAC アドレスを用いて MAC 認証を行います。認証スイッチ、RADIUS サーバ、および検疫サーバに、新しく MAC 認証の設定をする必要があります。
プリンタなど、IEEE802.1X 認証が行えない端末向きです。

以下、それぞれの設定方法について示します。

3.8.1. 検疫対象外ユーザの設定

検疫サーバで、検疫を実施しないユーザを登録する方法を以下に示します。

① Web ブラウザで「http:// “検疫サーバの IP アドレス：運用管理 Web サーバのポート番号” /」にアクセスし、「環境設定」をクリックする。

② 検疫対象外ユーザ情報の設定
左画面の中の「検疫対象外ユーザ情報設定」をクリックし、右画面にて「検疫対象外ユーザ ID」にユーザ名を入力して「追加」をクリックする。

図 3.8-1 検疫対象外ユーザの設定 1

3.8.2. MAC 認証の設定

検疫を行わず、MAC 認証のみ行う方法を以下に示します。

（１） AX の設定

端末を接続するポートに対してMAC認証の設定を行います。詳細は3.4を参照して下さい。

（２） RADIUS サーバの設定

検疫を実施しない端末の MAC アドレスをユーザ名としてユーザ登録します。

（３） 検疫サーバの設定

AX2400S では MAC 認証に使用する RADIUS サーバは別に設定できますので、個別に管理する方法を推奨します。

AX1200SではMAC認証に使用するRADIUSサーバを別けることができませんので、検疫サーバのRADIUSプロキシ設定にて外部RADIUSサーバに転送する必要があります。3.6.1④を参照してください。

※AX1240S では Ver2.1 にて MAC 認証の RADIUS サーバの個別設定をサポート予定です。

（４） 動作確認方法

AXで認証状態を確認するには、show mac-authentication loginコマンドを実行します。コマンドについては5.1.3を参照してください。
検疫サーバにおける確認方法は5.2を参照してください。

4. 検疫ネットワークの構築（ゲートウェイ方式）

本章では、AXシリーズのWeb認証（固定VLANモード）を用いた検疫ネットワークの構築例を説明します。

4.1. 概要

検疫ネットワークの基本的な構成を図 4.1-1 に示します。

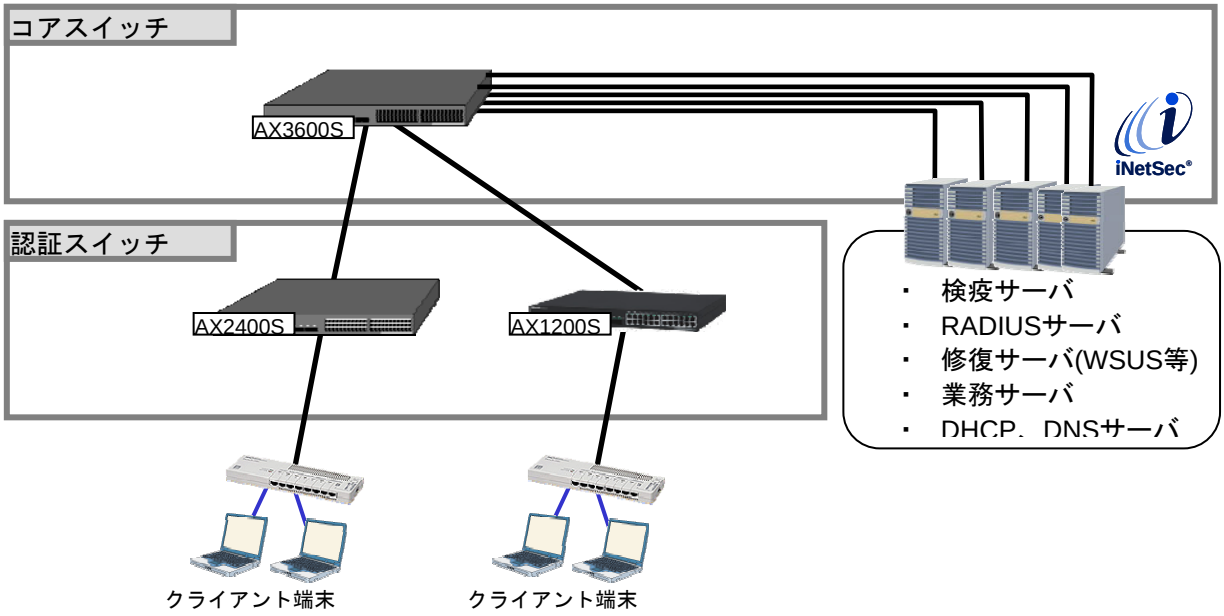


図 4.1-1 検疫ネットワークの基本構成（ゲートウェイ方式）

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、検疫を行う端末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端末を以下に示します。

表 4.1-1 サーバとクライアント一覧

検疫サーバ	RADIUS サーバ	クライアント端末
Red Hat Enterprise Linux Server release 5.1 ・iNetSec Inspection Center サーバパッケージ ・iNetSec Inspection Center V5.0L10A 認証機器拡充固有修正	Windows Server 2003 ・ActiveDirectory ドメインコントローラ ・RADIUS サーバ(IAS)	Windows XP InternetExplorer 6 Windows Vista InternetExplorer 7 Mac OSX Safari3.11

4.2. 検疫ネットワーク構成図

検疫ネットワークの基本構成（ゲートウェイ方式）を、具体的な構成例で示したものを以下に示します。

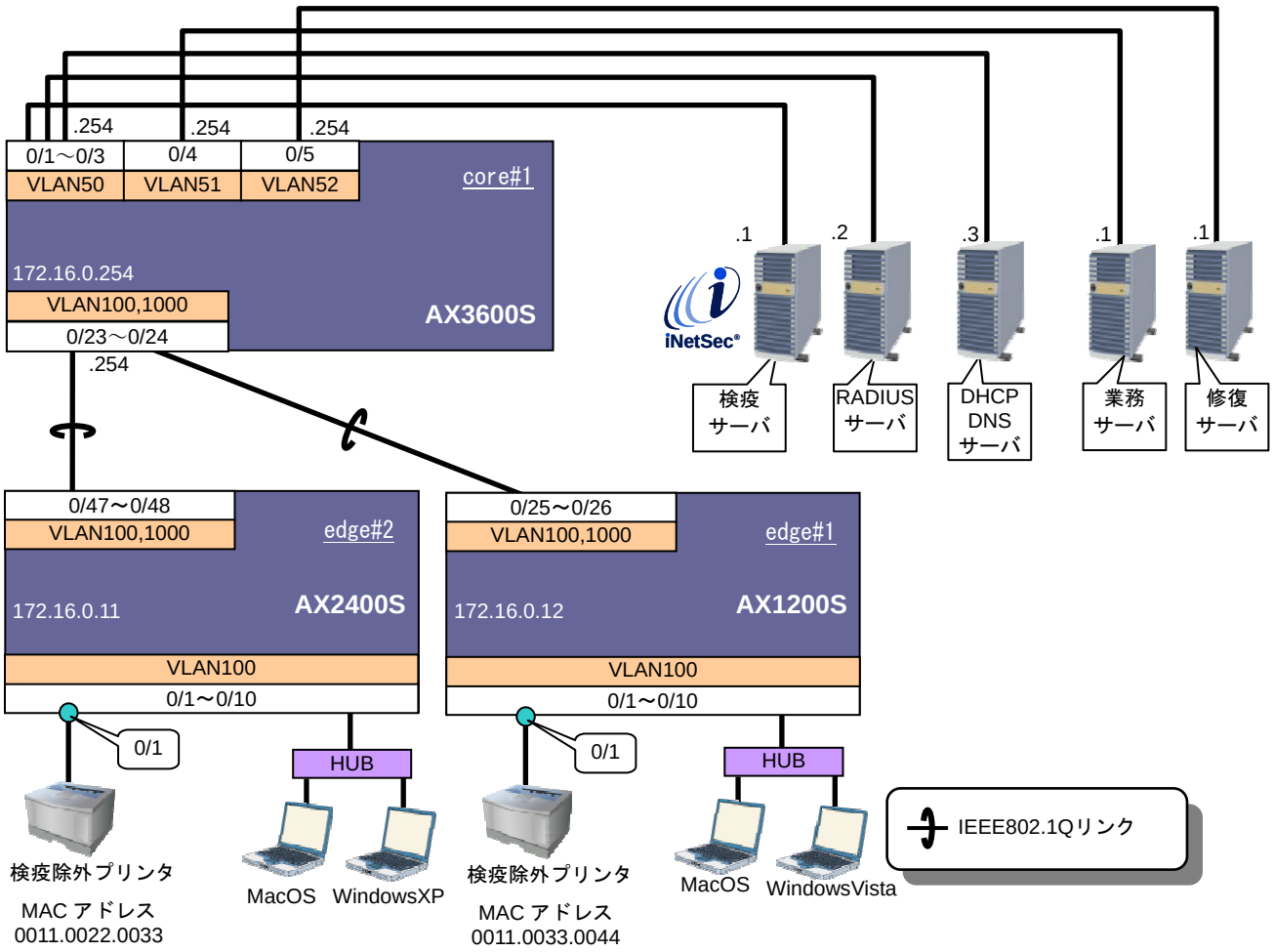


図 4.2-1 検疫ネットワーク構成図

認証スイッチのポートを以下の表のように設定します。

表 4.2-1 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	認証 VLAN	トランク VLAN
AX2400S	認証用	0/1	アクセス VLAN ポート	MAC 認証 (固定 VLAN)	100	—
		0/1～0/10		Web 認証 (固定 VLAN)		
	上位スイッチとの通信用	0/47～0/48	トランクポート	—	—	100,1000
AX1200S	認証用	0/1	アクセス VLAN ポート	MAC 認証 (固定 VLAN)	100	—
		0/1～0/10		Web 認証 (固定 VLAN)		
	上位スイッチとの通信用	0/25～0/26	トランクポート	—	—	100,1000

クライアント端末の検疫結果に応じた各サーバへの通信制御を以下に示します。

表 4.2-2 端末の検疫結果による通信制御

	検疫サーバ	DHCP、DNS サーバ	業務サーバ	修復サーバ
検疫成功端末	○	△	○	○
検疫失敗端末	○	△	×	○

※表中の○は端末から通信可能、×は通信不可、△は一部プロトコル（DHCP、DNS）のみ通信可能

本ガイドの構築例で設定する ID、パスワードの一覧を以下に示します。

表 4.2-3 本ガイドの構築例（ゲートウェイ方式）で設定する ID、パスワード一覧

項番	設定先	項目名	値	説明	本ガイド内の設定箇所
1	AX 認証スイッチ	radius key	alaxala	RADIUS シークレット	4.4.2 の（2）、4.4.3 の（1）
2		mac-authentication	macpass	MAC 認証用パスワード	4.4.2 の（5）、4.4.3 の（4）
3	検疫サーバ	クライアント認証キー	alaxala	RADIUS シークレット	4.6.2の②
4		PrimaryAuthSecret	alaxala	RADIUS シークレット	4.6.2の⑥
5		切替用アカウント KeyName	tmp01～tmp10	切替用アカウントのユーザ ID	4.6.2の③
6		切替用アカウント Password	tmppass	切替用アカウントのパスワード	4.6.2の③
7	外部 RADIUS サーバ	共有シークレット	alaxala	RADIUS シークレット	4.5

※表 4.2-3 で示す値は構築する環境に合わせて任意に変更して下さい。但し項番 1,3,4,7 の RADIUS シークレットにはそれぞれ同じ値を使用して下さい。

4.3. 構築ポイント

図 4.2-1のゲートウェイ方式の検疫ネットワークの構築ポイントを以下に示します。

(1) Web 認証用の画面を入れ替える。

AXスイッチのWeb認証画面(login.html)ファイルを入れ替えることで端末からのWebアクセスを検疫サーバにリダイレクトさせます。（詳細は4.4.1 Web認証画面入れ替え手順を参照）

(2) 認証前 ACL を作成する。

クライアント端末の認証前及び認証失敗時に以下①～④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 本ガイドではクライアント端末の 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端末からの DHCP パケットを許可します。
（クライアント端末の IP アドレスを固定する環境では本定義は不要です。）

② 認証前にクライアント端末からの名前解決を可能にします。
クライアント端末から DNS サーバ宛、DNS クエリパケットを許可します。

③ 本検疫システムではクライアント端末は Web ブラウザにて検疫サーバにアクセスし検疫を実施します。クライアント端末と検疫サーバ間の IP 通信を許可します。

④ 検疫に失敗したクライアント端末が修復を行うためクライアント端末と修復サーバの接続性を確保する必要があります。クライアント端末と修復サーバ間の IP 通信を許可します。

(3) 検疫サーバを RADIUS サーバとして設定する。

AX シリーズの認証スイッチに設定する RADIUS サーバは検疫サーバの IP アドレスを指定します。

(4) 検疫除外端末を接続するポートに MAC 認証を設定する。

プリンタなどの検疫が実施できない端末を接続する場合、接続するポートにMAC認証を設定します。詳細は**4.8.2MAC認証の設定方法**を参照して下さい。

4.4. AX の設定

4.4.1. Web 認証画面入れ替え手順

本検疫システムでは検疫サーバと連携するため AX スイッチの認証画面（login.html）を入替えます。検疫サーバへリダイレクトするように設定したHTMLファイルをスイッチのlogin.htmlファイルと入替えます。本ガイドでは設定例として本ガイド**B付録　Web認証画面入れ替え用ファイル**を編集して適用する例を示します。

①添付のファイル（はクリップマークを右クリックして「埋め込みファイルをディスクに保存」をクリックして下さい。

②保存されたファイルをエディタ等で開き“xx.xx.xx.xx”の部分を検疫サーバの IP アドレス（本ガイドでは 10.50.0.1 です。）に変更して下さい。編集後は保存して閉じてください。

③SD または FTP にて認証スイッチにファイルを転送。

④認証スイッチにて　set web-authentication html-files <directory> -f　コマンドを投入し転送したファイルを適用します。
※ただし、本コマンドはディレクトリ指定のため下記コマンドでディレクトリ作成してファイル移動後に set コマンドを実行してください。

AX2400S、AX3600S
mkdir <directory name>

AX1200S
mkdir ramdisk <directory name>

4.4.2. 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。 **※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。
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 0/1-10** **(config-if-range)# switchport access vlan 100**	ポート 0/1～0/10 を、アクセスポートの VLAN100 に設定します。
●上位スイッチとの通信用 **(config)# interface rqnge 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 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** **(config)# interface vlan 100** **(config-if)# ip address 192.168.100.12 255.255.255.0**	管理用 VLAN1000 にインタフェース IP アドレスを設定します。 認証用 VLAN100 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 10.50.0.1 key alaxala	検疫サーバの 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。 ➢ **構築ポイント（３）**
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） 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 WEBAUTH **(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 192.168.100.0 0.0.0.255 dst 10.50.0.3 0.0.0.0 eq bootpc** **(config-ext-nacl)# permit udp src 192.168.100.0 0.0.0.255 dst 10.50.0.3 0.0.0.0 eq domain** **(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**	以下のアクセスリスト「WEBAUTH」を作成します。 ①クライアント端末からの DHCP パケットを許可します。 ②クライアント端末からの DNS パケットを許可します。 ③クライアント端末から検疫サーバ宛の通信を許可します。 ④クライアント端末から修復サーバ宛の通信を許可します。 ➢ **構築ポイント（２）**

（４） Web 認証の設定

AX1200S の設定	
Web 認証の設定	
(config)# web-authentication system-auth-control **(config)# web-authentication ip address 1.1.1.1** **(config)# web-authentication redirect-mode http**	Web 認証を有効にします。 Web 認証専用 IP アドレスを設定します。 Web 認証のリダイレクトモードを HTTP にします。
物理ポートの設定	
(config)# interface range fastethernet 0/1-10 **(config-if-range)# web-authentication port** **(config-if-range)# authentication ip access-group “WEBAUTH”** **(config-if-range)# authentication arp-relay**	ポート 0/1～0/10 に対して、Web 認証を有効にします。 認証前アクセスリスト “WEBAUTH” を有効にします。 認証前ポートでの arp リレーを有効にします。
RADIUS の設定	
(config)# aaa authentication web-authentication default group radius	RADIUS サーバで Web 認証を行うことを設定します。

（５） MAC 認証の設定

AX1200S の設定	
物理ポートの設定	
(config)# interface fastethernet 0/1 **(config-if)# mac-authentication port**	ポート 0/1 を MAC 認証用ポートとして設定します。 ➢ **構築ポイント（４）**
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** 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。 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。

4.4.3. 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 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 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 0/1-10** **(config-if-range)# switchport access vlan 100**	ポート 0/1～0/10 を、アクセスポートの VLAN100 に設定します。
●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 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 172.16.0.11 255.255.255.0** **(config)# interface vlan 100** **(config-if)# ip address 192.168.100.11 255.255.255.0**	管理用 VLAN1000 にインタフェース IP アドレスを設定します。 認証用 VLAN100 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 10.50.0.1 key alaxala	検疫サーバの IP アドレスおよびキーを設定します。この例ではキーを「alaxala」としています。 ➢ **構築ポイント（３）**
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） 検疫 VLAN 用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 WEBAUTH **(config-ext-nacl)# permit udp any any eq bootps** **(config-ext-nacl)# permit udp any host 10.50.0.3 eq bootpc** **(config-ext-nacl)# permit udp 192.168.100.0 0.0.0.255 host 10.50.0.3 eq domain** **(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**	以下のアクセスリスト「WEBAUTH」を作成します。 ①クライアント端末からの DHCP パケットを許可します。 ②クライアント端末からの DNS パケットを許可します。 ③クライアント端末から検疫サーバ宛の　信を許可します。 ④クライアント端末から修復サーバ宛の通信を許可します。 **構築ポイント（２）**

（３） Web 認証の設定

AX2400S の設定	
Web 認証の設定	
(config)# web-authentication system-auth-control **(config)# web-authentication ip address 1.1.1.1** **(config)# web-authentication redirect-mode http**	Web 認証を有効にします。 Web 認証専用 IP アドレスを設定します。 Web 認証のリダイレクトモードを HTTP にします。
物理ポートの設定	
(config)# interface range gigabitethernet 0/1-10 **(config-if-range)# web-authentication port** **(config-if-range)# authentication ip access-group “WEBAUTH”** **(config-if-range)# authentication arp-relay**	ポート 0/1～0/10 に対して、Web 認証を有効にします。 認証前アクセスリスト “WEBAUTH” を有効にします。 認証前に arp リレーを有効にします。
RADIUS の設定	
(config)# aaa authentication web-authentication default group radius	RADIUS サーバで Web 認証を行うことを設定します。

（４） MAC 認証の設定

AX2400S の設定	
物理ポートの設定	
(config)# interface gigabitethernet 0/1 **(config-if)# mac-authentication port**	ポート 0/1 を MAC 認証用ポートとして設定します。 ➢ **構築ポイント（４）**
MAC 認証の設定	
(config)# aaa authentication mac-authentication default group radius **(config)# mac-authentication system-auth-control** 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。 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。

4.4.4. 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 100,1000** **(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。 認証 VLAN として VLAN100 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 range gigabitethernet 0/1-3 **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 50** **(config)# interface gigabitethernet 0/4** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 51** **(config)# interface gigabitethernet 0/5** **(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 0/1～0/3 を、アクセスポートとして設定します。 アクセスポートに VLAN50 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 VLAN51 を設定します。 ポート 0/5 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 および 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。

4.5. 外部 RADIUS サーバの設定

外部RADIUSサーバの設定に関してはIEEE802.1X認証VLAN方式と同じです。**3.5外部RADIUSサーバの設定**を参照して下さい。

4.6. 検疫サーバの設定

本ガイドの環境に合わせた検疫サーバの設定を紹介します。
基本サーバコンポーネントや機能追加パッケージ「iNetSec Inspection Center V5.0L10A 認証機器拡充固有修正」が既にインストールされていることを前提としています。インストール方法および初期設定については以下のマニュアルを参照して下さい。

- 「Web 認証方式認証機器連携導入設定手順書」
- 「iNetSec Inspection Center V5.0 L10 認証サーバ ユーザーズガイド」
- 「iNetSec Inspection Center V5.0 L10 ユーザーズガイド」

4.6.1. 検疫サーバの構成

本検疫システムにて検疫サーバの構成は大きく別けて二つあります。
・検疫サーバと RADIUS サーバがそれぞれ別のサーバで構成する**基本構成**。
・検疫サーバと RADIUS サーバを 1 台にまとめた**オールインワン構成**。
詳細は「Web 認証方式認証機器連携導入設定手順書」の Web 認証方式認証機器連携の項目を参照して下さい。

本ガイドでは“基本構成”で構築し、切替用アカウントを制御する“認証機器連携アダプター”をインストールした検疫サーバの設定を紹介しています。図 4.6-1 を参照。

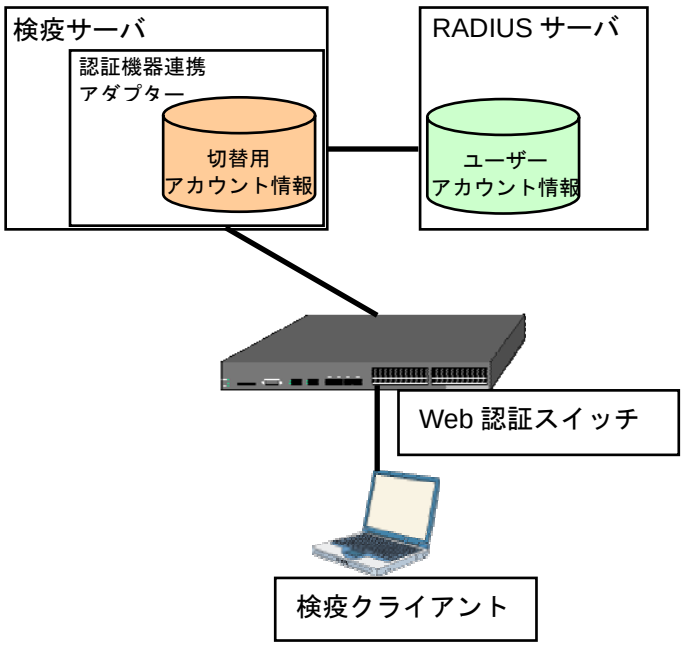


図 4.6-1 基本構成

4.6.2. 認証機器連携アダプターの設定

本検疫ネットワークでの認証機器連携アダプターの設定を示します。

①クライアント設定

認証機器連携アダプターに、RADIUS クライアント情報を登録します。Root 権限にて以下の radclient コマンドを実行してください。詳細は「iNetSec Inspection Center V5.0L10 ユーザーズガイド」の“4.5.2.3 RADIUS クライアント情報の登録”を参照してください。

```
[root]# /opt/FJSVrdsvr/bin/radclient -A -i 172.16.0.11 -k alaxala -v 0 -U root -P root
[root]# /opt/FJSVrdsvr/bin/radclient -A -i 172.16.0.12 -k alaxala -v 0 -U root -P root
```

・**クライアントアドレス**：認証スイッチの IP アドレス
本ガイドでは AX2400S（172.16.0.11）、AX1200S（172.16.0.12）

・**クライアント認証キー**：**4.4**で認証スイッチに設定した認証キー
本ガイドでは“alaxala”で共通

②切替用アカウントの設定確認

切替用アカウントの共通管理情報の確認、編集を行います。本ガイドでは以下の設定で tmp01～tmp10 という切替用アカウントの使用を定義しています。
ファイルの場所（$QUARANTINE_CONF_DIR/quarantine/base/conf/SwitchAccount.conf）

- KeyName= に切替用アカウントのキーを設定します。（本ガイドでは tmp としています。）
- GenerateNumber= に切替用アカウントの生成数を設定します。（本ガイドでは 10 としています。）
- Password= に切替用アカウントのパスワードを設定します。（本ガイドでは tmppass としています。）

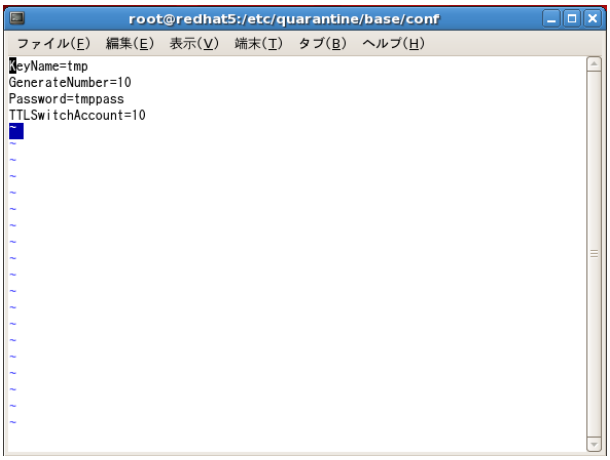


図 4.6-2 SwitchAccount.conf

③切替用アカウントの登録作業

②の設定後に SwitchAccount.conf の設定内容にあわせた共通切替用アカウントの登録作業が必要です。詳細は「iNetSec Inspection Center V5.0L10 ユーザーズガイド」の“4.5.2.4 切替用アカウントの登録”を参照してください。

④IPModeTable.csv ファイルの確認

クライアントの接続するネットワーク（IP アドレス）と、検疫方式を対応付けするための設定を行います。ファイルの場所（$QUARANTINE_CONF_DIR/quarantine/share/conf/IPModeTable.csv）
（本ガイドでは全てのクライアントを検疫対象とする設定になっています。）

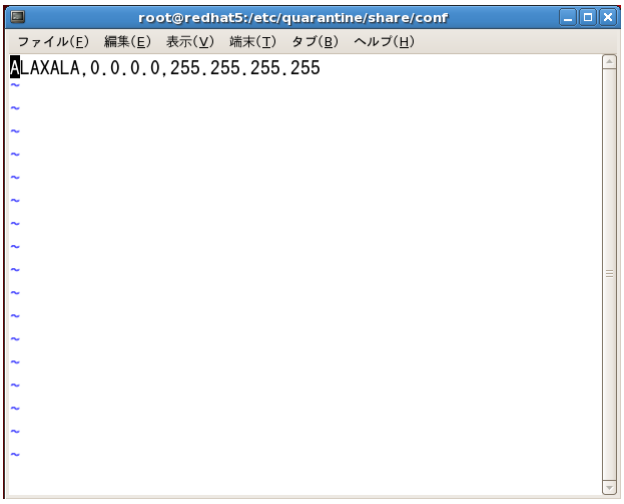


図 4.6-3 IPModeTable.csv

⑤認証サーバ情報の設定

ユーザ認証を行うサーバの指定を行います。本ガイドでは基本構成で構築していますので認証サーバに外部 RADIUS サーバを指定しています。以下の設定を確認して下さい。
ファイルの場所（$QUARANTINE_CONF_DIR/quarantine/share/conf/AlaxalAPlugin.conf）

- Plugin = ON （プラグインを有効にします）
- PrimaryAuthServer = 10.50.0.2 （本ガイドでは外部 RADIUS サーバ“10.50.0.2”を指定）
- PrimaryAuthPort = 1812 （本ガイドでは RADIUS 使用ポートに“1812”を指定）
- PrimaryAuthSecret = alaxala （本ガイドでは RADIUS シークレットを“alaxala”を指定）

※その他の設定に関しては構築する環境に合わせて変更して下さい。

図 4.6-4 AlaxalAPlugin.conf

⑥認証機器 CGI 情報の確認

認証機器環境に合わせて、CGI 情報を確認、編集を行います。

ファイルの場所（$QUARANTINE_CONF_DIR/quarantine/base/conf/AlaxalAAuthentication.conf）

- AuthCGIHost=1.1.1.1　（認証スイッチの Web 認証専用 IP アドレスを指定）
- AuthCGIProtocol=https　（Web 認証時の使用プロトコルに HTTPS を指定）
- AuthCGIPort=443　（HTTPS 使用時のポート番号を指定）

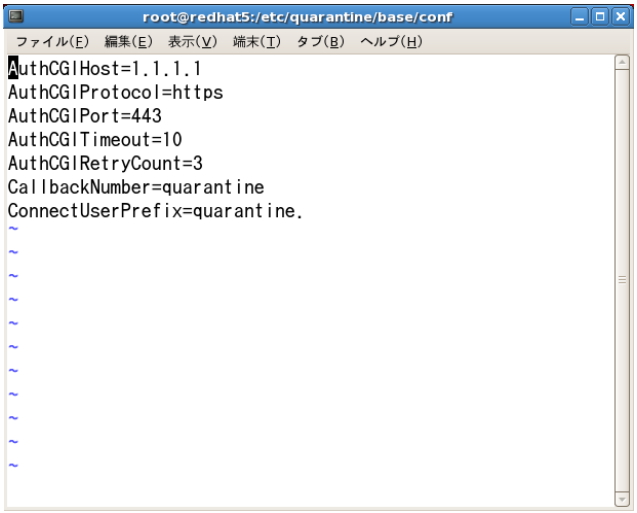


図 4.6-5 AlaxalAAuthentication.conf

4.6.3. iNetSec Inspection Center の設定

iNetSec Inspection Centerの設定に関してはIEEE802.1X認証VLAN方式と同じです。**3.6.2iNetSec Inspection Centerの設定**を参照して下さい。

4.7. 検疫クライアントの設定と操作

ゲートウェイ方式のクライアント設定方法と検疫操作手順を示します。
詳細は「iNetSec Inspection Center V5.0 L10 ユーザーズガイド」をご参照ください。

4.7.1. 設定方法

①クライアント端末の Internet Explorer にて“ActiveX”を有効にする設定を行って下さい。
詳細は「iNetSec Inspection Center V5.0L10 ユーザーズガイド」の“5.2.1 Web ブラウザ型クライアントのインストール”を参照してください。

クライアント端末にて事前に行う設定は以上です。

4.7.2. 検疫操作手順

①クライアント端末を認証スイッチに接続し、クライアントの Web ブラウザから任意の URL にアクセスすると検疫サーバのログイン画面にリダイレクトされます。（証明書エラーが表示される場合があります。証明書に関しての注意事項は「認証ソリューションガイド補足資料」を参照して下さい。）
下記画面上段の情報バーをクリックして「ActiveX コントロールの実行」をクリックして下さい。

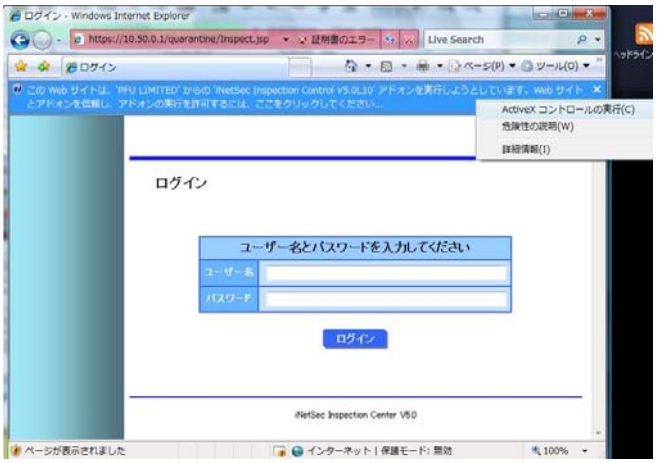


図 4.7-1 ActiveX コントロールの実行

②下記セキュリティ警告が表示されます。「実行する」をクリックして下さい。

図 4.7-2 セキュリティ警告

③ActiveX コントロールのインストール後ログイン画面にて RADIUS サーバで登録したユーザー名とパスワードを入力し「ログイン」ボタンをクリックして下さい。

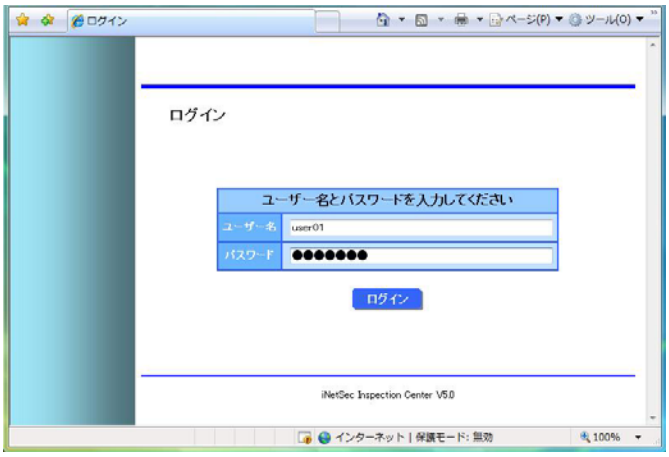


図 4.7-3 ログイン画面

④クライアント端末の認証と検疫が実施されます。

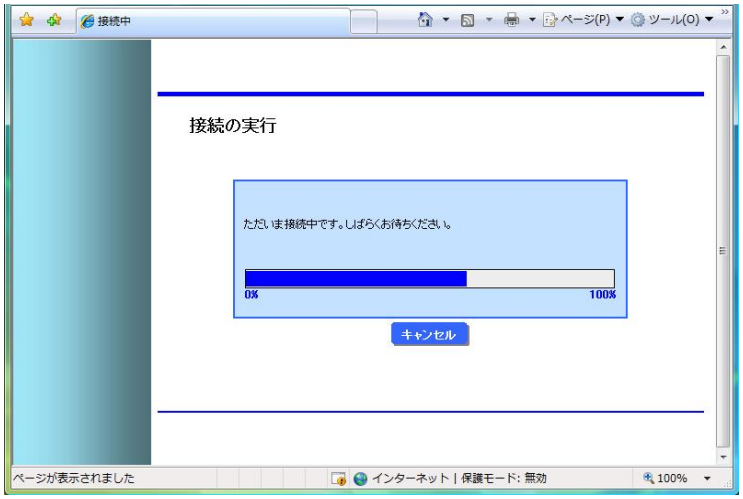


図 4.7-4 検疫実施画面

⑤ログインの成功画面が表示され、業務サーバへの通信が可能となります。

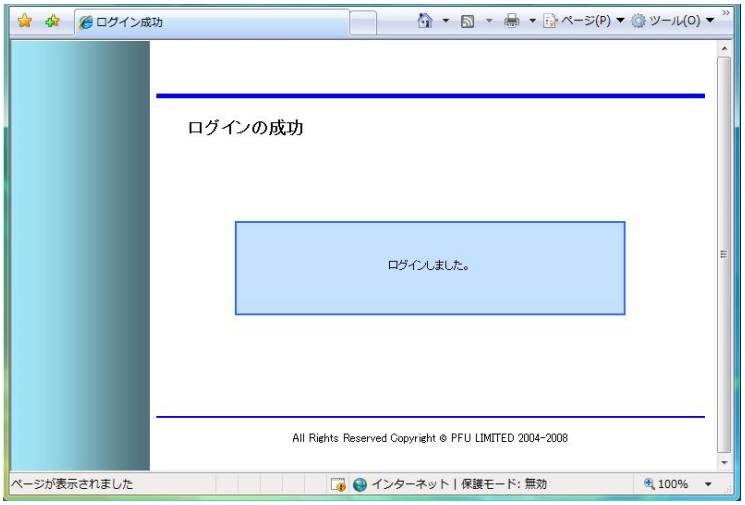


図 4.7-5 ログインの成功画面

4.8. 検疫未対応端末の接続方法

ゲートウェイ方式の検疫ネットワークシステムにおいて、検疫未対応端末を接続する方法は 2 通りあります。

（1） 検疫対象外 OS の接続

検疫を行わず、Web 認証のみ行います。
Mac OS や Linux など、ActiveX コントロールはインストールできないが Web ブラウザにて Web 認証が可能な端末向きです。4.8.1.にて設定方法を示します。

※本構成を構築する場合は iNetSec 認証サーバ（オプション）のインストールが必要です。詳細は「Web 認証方式認証機器連携導入設定手順書」の Web 認証方式認証機器連携の項目を参照して下さい。

（2） MAC 認証端末の接続

端末の MAC アドレスを用いて AX シリーズがサポートする MAC 認証を行います。認証スイッチ、RADIUS サーバ、および検疫サーバに、新しく MAC 認証の設定をする必要があります。
プリンタなど、Web ブラウザを使って Web 認証が行えない端末向きです。
4.8.2.にて設定方法を示します。

以下、それぞれの設定方法について示します。

4.8.1. 検疫対象外 OS の接続設定と確認

iNetSec認証サーバの検疫対象外OS用のプレフィックスの設定方法と検疫対象外OSとしてMacOS端末の接続操作方法を紹介します。概要については**1.3.5ゲートウェイ方式での検疫対象外端末について**を確認してください。

(1) PROXY の設定

①iNetSec 認証サーバの設定画面を開き、左画「PROXY 設定」をクリックする。
メイン画面の下に iNetSec 認証サーバのプロキシ設定が表示されていることを確認する。
（本ガイドでは全てのリクエストを外部 RADIUS サーバに転送する設定となっています）
ここで以下の検疫除外端末用のプロキシ条件を 1 つ追加します。

- プレフィックス ：（quarantine.） 削除転送する。
- 認証キー ：alaxala
- 転送先アドレス ：10.50.0.2
- 評価順 ：1

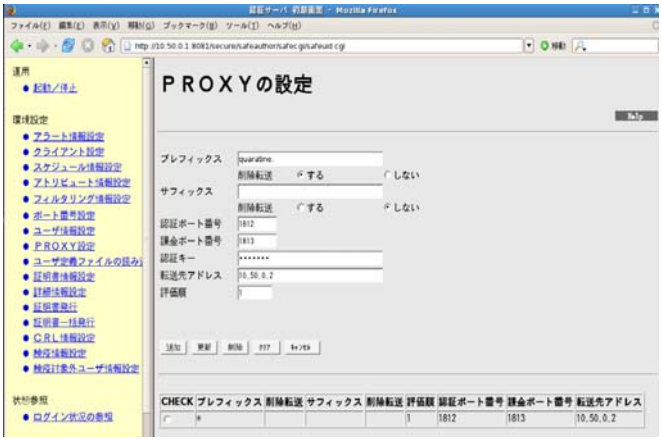


図 4.8-1 proxy 設定 1

②プロキシの条件を正しく追加するとメイン画面の下に以下図のように表示されます。
RADIUS サーバでは既存ユーザの認証となりますので設定は以上です。

CHECK	プレフィックス	削除転送	サフィックス	削除転送	評価順	認証ポート番号	課金ポート番号	転送先アドレス
○	quaratine.	する			1	1812	1813	10.50.0.2
○	*				2	1812	1813	10.50.0.2

図 4.8-2 proxy 設定 2

(2) MacOS で認証

本ガイドでは実際に MacOS にて検疫除外の接続を行う手順を示します。使用した端末は MacOSX、Web ブラウザは Safari（Ver3.1.1）です。事前に Web ブラウザの設定にて“JAVA”を有効にして下さい。

①MacOS を認証スイッチに接続し Web ブラウザ（Safari）を立ち上げる。任意の URL を入力したところ検疫サーバのログイン画面にリダイレクトされていることを確認し以下を入力、「ログイン」ボタンをクリックする。

ユーザー名：外部 RADIUS で登録されたユーザ ID を入力（本ガイドでは“user01”を使用）
パスワード：ユーザー名に記入したユーザ ID のパスワードを入力

図 4.8-3 Safari1

②認証に成功すると、以下の AX シリーズの認証成功画面が表示されます。
（本画面は AX シリーズの認証画面入れ替えによりカスタマイズ可能です。）

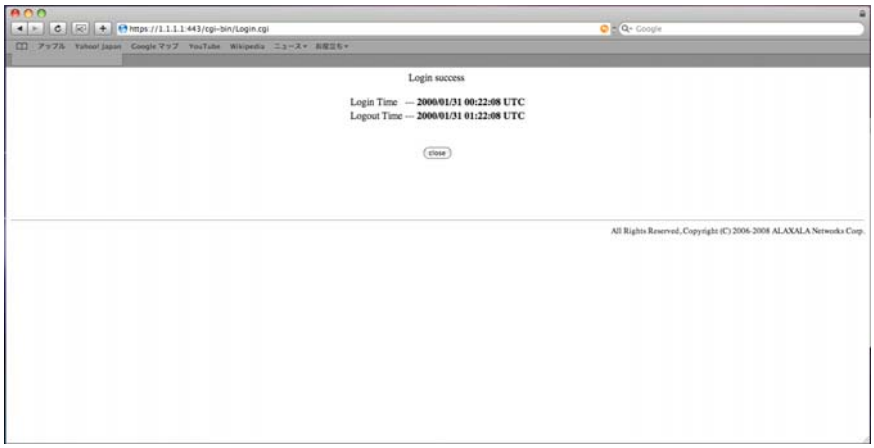


図 4.8-4 Safari2

(3) 認証スイッチで確認

AX シリーズの運用コマンド（show web-authentication login）にて検疫除外端末としてプレフィックスが追加されたユーザ（quarantine.user01）からの認証であることを確認する。

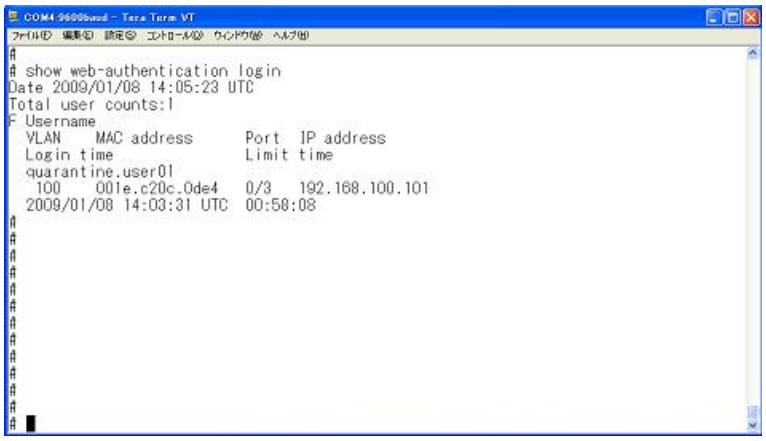


図 4.8-5 show web-authentication login

4.8.2. MAC 認証の設定方法

検疫を行わず、MAC 認証のみ行う方法を以下に示します。

(1) AX の設定

端末を接続するポートに対してMAC認証の設定を行います。詳細は**4.4AXの設定**を参照して下さい。

(2) RADIUS サーバの設定

検疫を実施しない端末の MAC アドレスをユーザ名としてユーザ登録します。

(3) 検疫サーバの設定

AX2400S では MAC 認証で使用する RADIUS サーバは別に設定できますので、個別に管理する方法を推奨します。

AX1200S では MAC 認証で使用する RADIUS サーバを別けることができませんので、検疫サーバの RADIUS プロキシ設定にて外部 RADIUS サーバに転送する必要があります。

図 4.8-1 proxy設定 1を参照して下さい。

※　AX1240S では Ver2.1 にて MAC 認証の RADIUS サーバの個別設定をサポート予定です。

(4) 動作確認方法

AXで認証状態を確認するには、show mac-authentication loginコマンドを実行します。コマンドについては**5.1.3**を参照してください。
検疫サーバにおける確認方法は**5.2**を参照してください。

5. 動作確認方法

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説明します。

5.1. AX における動作確認

5.1.1. IEEE802.1X 認証 VLAN 方式

①show dot1x detail

IEEE802.1X 認証の状態表示コマンドです。検疫クライアント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。また、その所属している VLAN 情報から、検疫に成功しているかどうかも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 0/1 detail

Date 2008/08/27 19:14:51 JST

Port 0/1(Dynamic)
AccessControl   : Multiple-Auth              PortControl    : Auto
Status          : ---                        Last EAPOL     : 0019.b97d.4bfa
Supplicants     : 2 / 2 / 64                 ReAuthMode     : Enable
TxTimer         : 30                         ReAuthTimer    : 600
ReAuthSuccess   : 54                         ReAuthFail     : 3
SuppDetection   : Disable

 Supplicants MAC  F  Status          AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s)  Date/Time
 001e.c965.dd62      Authorized      Authenticated  Idle           2
                     1408            2008/08/27 18:51:21
 0019.b97d.4bfa      Authorized      Authenticated  Idle           0
                     103             2008/08/27 19:13:08

edge#1> show mac-address-table

Date 2008/08/27 19:15:03 JST
Aging time : 300
No     MAC address       VLAN     Type     Port      ChGrp     MCast
1      0019.b97d.4bfa      10     Dynamic  0/1       -         -
2      001e.c965.dd62      30     Dot1x    0/1       -         -
3      0012.e248.4220     100     Dynamic  0/25      -         -
4      0019.b97d.4bfa     100     Dot1x    0/1       -         -
5      0012.e248.4220    1000     Dynamic  0/25      -         -
```

図 5.1-1 AX1200S の状態表示例

```
edge#2> show dot1x vlan dynamic detail
Date 2008/08/27 19:26:04 JST
VLAN(Dynamic)
AccessControl   : Multiple-Auth            PortControl    : Auto
Status          : ---                      Last EAPOL     : 001e.c965.dd62
Supplicants     : 2 / 2 / 256              ReAuthMode     : Enable
TxTimer(s)      : ---   / 30               ReAuthTimer(s): 556   / 600
ReAuthSuccess   : 1                        ReAuthFail     : 0
SuppDetection   : Disable
VLAN(s): 30,100

 Supplicants MAC     Status          AuthState      BackEndState   ReAuthSuccess
                     SessionTime(s) Date/Time
 [VLAN 30]           VLAN(Dynamic) Supplicants : 1
 001e.c965.dd62      Authorized      Authenticated  Idle           0
                     45              2008/08/27 19:25:19
 [VLAN 100]          VLAN(Dynamic) Supplicants : 1
 0019.b97d.4bfa      Authorized      Authenticated  Idle           0
                     56              2008/08/27 19:25:08
```

図 5.1-2 AX2400S/AX3600S の状態表示例

②show dot1x logging

IEEE802.1X 認証の動作ログ表示コマンドです。検疫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。

③clear dot1x auth-state

IEEE802.1X認証状態を初期化するコマンドです。検疫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。

5.1.2. ゲートウェイ方式

①show web-authentication login

Web 認証の認証状態表示コマンドです。現在ログイン中（認証済み）のユーザを，ログイン日時の昇順に表示します。

```
edge#2>show web-authentication login
Date 2009/1/9 10:52:49 UTC
Total user counts:2
F Username
VLAN    MAC address      Port  IP address
Login time               Limit time
User01
3    0012.e2e3.9166   0/5   192.168.0.1
2009/1/9 09:58:04 UTC  00:10:20
```

図 5.1-3 AX2400S/AX3600S の状態表示例

②show web-authentication logging

Web 認証の動作ログ表示コマンドです。検疫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。

③clear web-authentication auth-state

Web認証状態を初期化するコマンドです。検疫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。

5.1.3. show mac-authentication login

MAC 認証の状態表示コマンドです。検疫を行わず、MAC 認証を行っている端末の認証状況を確認することができます。

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

Date 2008/09/04 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  2008/09/04 18:55:23   infinity    3384
```

図 5.1-4 AX1200S の状態表示例

5.2. 検疫サーバにおける動作確認

5.2.1. レポーティング出力

検疫結果のログを表示します。検疫結果の他に、検疫失敗の原因などを確認することができます。

① Web ブラウザで「https://“検疫サーバの IP アドレス”/quarantine/admin/Login.jsp/」にアクセスする。
検疫ネットワークシステム管理者ログイン画面にて管理者アカウントでログインする。
② 左画面のメニューより「レポーティング出力」をクリックし、右画面の「時系列検疫状況」の「出力」をクリックする。

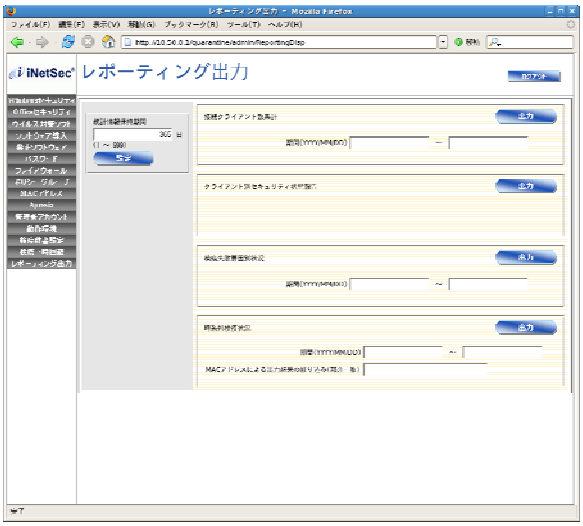


図 5.2-1 レポーティング出力

5.2.2. PROXY ログ情報の参照

RADIUS プロキシのログを表示します。検疫サーバと RADIUS サーバとの間の通信に問題がないか確認することができます。

① Web ブラウザで「http://“検疫サーバの IP アドレス：運用管理 Web サーバのポート番号”/」にアクセスし、「環境設定」をクリックする。
② 左画面の中の「ログ／課金情報の参照」にある「PROXY ログ情報の参照」をクリックする。

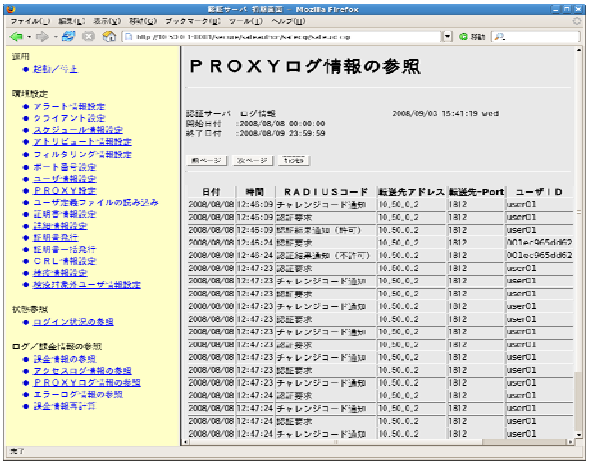


図 5.2-2 プロキシログ出力

※認証結果の確認については、各 RADIUS サーバのイベントログを確認してください。

5.3. 検疫クライアントにおける動作確認

5.3.1. IEEE802.1X 認証 VLAN 方式

Windows のタスクトレイに表示されているアイコンで、検疫状態を確認することができます。

検疫クライアントが検疫に失敗した場合は、検疫結果画面が表示されます。検疫失敗画面例を図 5.3-1 に示します。

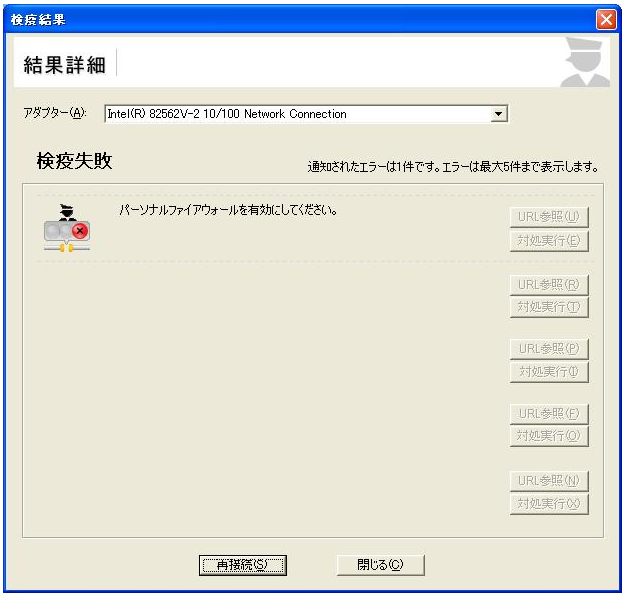


図 5.3-1 検疫失敗画面

ここで、検疫クライアント端末のセキュリティポリシーを変更して安全な状態にした後「再接続」をクリックすると、再度検疫が実施されます。検疫クライアントが検疫に成功すると、図 5.3-2 に示す画面が表示されます。

図 5.3-2 検疫成功画面

画面を閉じてしまった場合は、Windows タスクトレイに表示されているアイコンをクリックして、ポップアップメニューから「検疫結果」を選択すると、上記の画面を表示することができます。

6. 注意事項

6.1. 検疫方式を混在するときの注意事項

一台の AX 認証スイッチで IEEE802.1X 認証 VLAN 方式とゲートウェイ方式を混在する場合の注意事項を説明します。

6.1.1. AX の設定に関する注意事項

（１） AX では同一ポートで IEEE802.1X 認証 VLAN 方式とゲートウェイ方式（Web 認証連携）方式の混在ができません、同一スイッチ内で混在する場合は別ポートで設定してください。

（２） 現在の AX の仕様では IEEE802.1X 認証と Web 認証で使用する RADIUS サーバは共通となります。そのため 6.3.2 の注意事項に従い検疫サーバを構築してください

6.1.2. iNetSec Inspection Center の設定に関する注意事項

一台の検疫サーバでゲートウェイ方式と IEEE802.1X 認証 VLAN 方式を混在する必要がありますので IEEE802.1X 認証 VLAN 方式で設定する RADIUS プロキシの設定に注意が必要です。

（１） IEEE802.1X 認証 VLAN 方式とゲートウェイ方式を共存させる場合は検疫サーバ上の認証機器連携アダプターに Web 認証連携で使用する切替用アカウントを RADIUS プロキシされるより先に認証する必要があります。

設定方法
/opt/FJSVrdsvr/raddb/radius.conf ファイルに PRX-LOCAL-USER-CHECKを
1行追加してください。

（２） RADIUS プロキシの条件について、全てのユーザ名をプロキシする条件とせず、IEEE802.1X 認証 VLAN 方式で使用するユーザのみプロキシするようにユーザ名にルールを決めて適用する方がセキュリティ性が向上します。

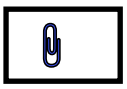
A. 付録　コンフィグレーション

3.4と4.4で示したAXのコンフィグレーションをテキスト形式のファイルで添付しています。
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. 802.1X 認証 VLAN 方式

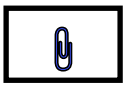
図 3.2-1のネットワーク構成図における各装置の全コンフィグレーションです。

A.1.1. AX1200S のコンフィグレーション



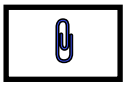
A-1_edge1_config.txt

A.1.2. AX2400S のコンフィグレーション



A-1_edge2_config.txt

A.1.3. AX3600S のコンフィグレーション

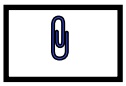


A-1_core1_config.txt

A.2. ゲートウェイ方式

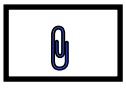
図 4.2-1のネットワーク構成図における各装置の全コンフィグレーションです。

A.2.1. AX1200S のコンフィグレーション



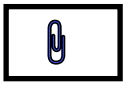
A-2_edge1_config.txt

A.2.2. AX2400S のコンフィグレーション



A-2_edge2_config.txt

A.2.3. AX3600S のコンフィグレーション



A-2_core1_config.txt

B. 付録　Web 認証画面入れ替え用ファイル

4.4.1Web認証画面入れ替え手順にて使用するhtmlファイルを添付しています。

A.1. ゲートウェイ方式

A.1.1. login.html

※ 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。

2009 年 5 月 22 日　第 3 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