

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



第3版



Copyright © 2008,2009, ALAXALA Networks Corporation. All rights reserved.

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

検疫ソフトウェア一覧

- 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	—	2008. 9. 22	初版発行	-
第2版	—	2009. 1. 30	・ゲートウェイ方式を追加。	•1.3
				·2章
				•4章
				•5. 1. 2
				·6.2
			・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	·6.3
			イ方式)を付録として追加	•A. 2
第3版	—	2009. 5. 20	・検疫シーケンスを一部修正。	•1.2.2
			 ・文中にユーザ認証が省略可能な旨を追加。 	•1.3.1
			・シーケンス図中の説明を一部修正。	•1.3.5
			・その他誤字を修正。	全体的

目次

1.	iNetS	ec Inspection Center検疫概要	6
	1.1. iN	etSec Inspection Center検疫	6
	1.1.1.	iNetSec Inspection Center検疫システム概要	6
	1.1.2.	iNetSec Inspection Centerサポート一覧	7
	1.2. IE	EEE802.1X認証VLAN方式による連携	8
	1.2.1.	AXのIEEE802.1X認証方式を用いた検疫概要	8
	1.2.2.	検疫シーケンス	9
	1.2.3.	IEEE802.1X認証VLAN方式による検疫の特徴	10
	1.3. ゲ	ーー	.11
	1.3.1.	AXとゲートウェイ方式を用いた検疫概要	11
	1.3.2.	各装置の役割	12
	1.3.3.	検疫シーケンス	13
	1.3.4.	ゲートウェイ方式を用いた検疫の特徴	14
	1.3.5.	ゲートウェイ方式での検疫対象外端末について	15
2	iNotS	oc Inspection Contorと海堆可能たAVシリーブの認証方式と収容冬代	16
۷.	meto	et inspection center と 定張可能な AX クリースの 認証 力式 C 私 在 本 IT	10
3.	検疫さ	[、] ットワークの構築(IEEE802.1X認証VLAN方式)	17
	3.1 概	要	17
	3.2 検		18
	3.3 構	※ ディーシーシーション (1973) 日	20
	3.4. A	Xの設定	21
	3.4.1.	AX1200Sのコンフィグレーション	21
	3.4.2.	AX2400Sのコンフィグレーション	23
	3.4.3.	AX3600Sのコンフィグレーション	25
	3.5. 外	部RADIUSサーバの設定	26
	3.5.1.	RADIUSクライアントの設定	26
	3.6. 検	った。 一般の一般ので、 一ので、 一般ので、 一のので、 一のので、 一のので、 一のので、 一のので、 一のので、 一のので、 一のので、 一ののので、 一のので、 一ののので、 一ののので、 一ののので、 一ののので、 一ののので、 一ののので、 一のののので、 一のののので、 一のののので、 一のののので、 一ののののので、 一ののののので、 一のののので、 一ののののののののので、 一のののののののののののののののののののののののののののののののののののの	27
	3.6.1.	iNetSec認証サーバの設定	27
	3.6.2.	iNetSec Inspection Centerの設定	30
	3.7. 検	疫クライアントの設定	31
	3.7.1.	インストール時の設定	31
	3.7.2.	インストール後の設定	32
	3.8. 検	疫未対応端末の接続方法	34
	3.8.1.	検疫対象外ユーザの設定	34
	3.8.2.	MAC認証の設定	35
1	烩疓;	なットロークの構築(ゲートウェイ方ギ)	36
	1,5,2,5		
	4.1. 砌		36
	4.2. 検	没 イットリーク	37
	4.3. 桶	·梁 ホイント	38
	4.4. A		39
	4.4.1.	Web認証画面人れ替え手順	39
	4.4.2.	AX12005のコンノイクレーション	40
	4.4.3.		42
	4.4.4.	AX36005のコンノイクレーンヨン	44
	4.5. 外	部KADIUSサーハの設定 v在共一、Mの記白	45
	4.6. (後サーハの設定	45
	4.6.1.	夜没サーハの 構成	45

4.6.2.	認証機器連携アダプターの設定	46
4.6.3.	iNetSec Inspection Centerの設定	
4.7. 検	€疫クライアントの設定と操作	
4.7.1.	設定方法	
4.7.2.	検疫操作手順	
4.8. 検	€疫未対応端末の接続方法	51
4.8.1.	検疫対象外OSの接続設定と確認	51
4.8.2.	MAC認証の設定方法	53
5. 動作码	灌認方法	55
5.1. A	Xにおける動作確認	
5.1.1.	IEEE802.1X認証VLAN方式	
5.1.2.	ゲートウェイ方式	
5.1.3.	show mac-authentication login	57
5.2. 検	減疫サーバにおける動作確認	58
5.2.1.	レポーティング出力	58
5.2.2.	PROXYログ情報の参照	58
5.3. 検	酸クライアントにおける動作確認	59
5.3.1.	IEEE802.1X認証VLAN方式	59
6. 注意	事項	60
6. 注意 6.1. 検	事項 〕疫方式を混在するときの注意事項	60
6. 注意 6.1. 検 6.1.1.	事項 衰方式を混在するときの注意事項 AXの設定に関する注意事項	60 60
6. 注意 6.1. 検 6.1.1. 6.1.2.	事項 酸疫方式を混在するときの注意事項	60
 6. 注意 第 6.1. 検 6.1.1. 6.1.2. A. 付銀 	事項 ●疫方式を混在するときの注意事項	
 注意到 6.1. 検 6.1.1. 6.1.2. A. 付銀 A.1. 80 	事項	
 6.1. 検 6.1. 検 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1.1. 	事項	
 注意到 6.1. 検 6.1.1. 6.1.2. A. 付留 A.1. 80 A.1.1. A.1.2. 	事項	
 注意到 6.1. 検 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1.1. A.1.2. A.1.3. 	事項	
 6. 注意 6.1. 検 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1.1. A.1.2. A.1.3. A.2. グ 	 事項	
 注意到 6.1. 核 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1. 80 A.1.1. A.1.2. A.1.3. A.2. 7 A.2.1. 	 事項	
 注意 6.1. 検 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1.2. A.1.3. A.2. ゲ A.2.1. 	 事項	60
 注意型 6.1. 検 6.1.1. 6.1.2. A. 付望 A.1. 80 A.1. 80 A.1. 80 A.1. 80 A.1.1. A.1.2. A.1.3. A.2. 7 A.2.1. A.2.3. 	 事項	
 注意到 6.1. 核 6.1.1. 6.1.2. A. 付銀 A.1. 80 A.1.	 事項	
 注意型 6.1. 検 6.1.1. 6.1.2. A. 付望 A.1. 80 A.1.2. A.1.3. A.2. ゲ A.2.1. A.2.1. A.2.3. B. 付望 A.1. ゲ 	 事項	60

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

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

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

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	Windows 98SE ^(*1) 、Windows Me ^(*1) 、		
(IEEE802.1X 認証 VLAN 方式)	Windows 2000、Windows XP、Windows Vista		
クライアント端末	Windows 98SE ^(*1) 、Windows Me ^(*1) 、		
(ゲートウェイ方式)	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	Windows 2000、Windows XP、Windows Vista		
(SSL-VPN 方式)	Mac OS ⁽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

<u>表 1.1-1</u>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。

甘木いつトウェマ	iNetSec Inspection Center V5.0 サーバパッケージ
本中 ノノトウェブ	iNetSec Inspection Center V5.0 クライアントライセンス
ナリション世口	iNetSec Inspection Center V5.0 認証サーバパッケージ
オフション表品	iNetSec Inspection Center V5.0 802.1X サプリカントライセンス

表 1.2-1 IEEE802.1X 認証方式の必須ソフトウェア構成

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

<u>表 1.1-1</u>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。

	iNetSec Inspection Center V5.0L10A サーバパッケージ
基本ソフトウェア	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)

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

※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 ヘ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 ヘ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ヘリダイレク 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。

認証方式	認証モード	AX1200S	AX2400S AX3600S	AX6300S AX6700S
IEEE802.1X	固定 VLAN	—	—	—
認証	動的 VLAN	0	0	0
10/06 認証	固定 VLAN	0	0	0
	動的 VLAN	—	—	—
いん う 認証	固定 VLAN	—	—	—
	動的 VLAN	_	_	_

表 2-1 iNetSec Inspection Center と連携可能な認証方式

(凡例) 〇:検疫連携可能 一: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		AX2 AX3	400S 600S	AX630 AX670	00S 00S
IEEE802.1X 認証	動的 \/I AN I	256/装置	合計	256/装置 ^(*1)	合計	4096/装置	合計
MAC 認証	到的 VLAN	256/装置	256/装置	256/装置 ^(*1)	256/装置 ^(*1)	×	4096/装置
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	Windows Server 2003	Windows XP
release 5	・ActiveDirectory ドメインコント	 iNetSec Inspection Center
・iNetSec Inspection Center サー	ローラ	802.1X サプリカント
バパッケージ	・RADIUS サーバ(IAS)	Windows Vista
・iNetSecInspection Center 認証		iNetSec Inspection Center
サーバパッケージ		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
	認証用	0/1	MAC VLAN	MAC 認証 (動的 VLAN)	10	30	100
AX2400S		0/1~0/10	ポート	IEEE802.1X 認証 (動的 VLAN)	10	- 50	100
	上位スイッチ との通信用	0/47~0/48	トランク ポート	—	—	—	—
AX1200S	認証用	0/1	MAC VLAN	MAC 認証 (動的 VLAN)	10	30	100
		0/1~0/10	ポート	IEEE802.1X 認証 (動的 VLAN)	10	30	100
	上位スイッチ との通信用	0/25~0/26	トランク ポート				

各 VLAN の定義および VLAN 間通信の可否を以下の表に示します。

VLAN 名	VLAN ID	ネットワーク IP アドレス	用途	設置サーバ
検疫・認証サー	50	10.50.0.0/24	検疫サーバおよび RADIUS サーバが	検疫サーバ
バ用 VLAN			所属する VLAN。	RADIUS サーバ
業務サーバ用	51	10.51.0.0/24	認証・検疫が成功した端末と通信可能	業務サーバ
VLAN			なサーバが所属する VLAN。(社内ネッ	
			トワーク)	
修復サーバ用	52	10.52.0.0/24	検疫により隔離された端末を修復す	修復サーバ
VLAN			るためのサーバが所属する VLAN。	
認証前 VLAN	10	192.168.10.0/24	端末が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。	

表 3.2-2 VLAN の定義

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-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	×	×	0
認証後 VLAN	100	0	0	0

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、パスワードー覧

項番	設定先	項目名	値	説明	本ガイド内の 設定箇所
1	^ > ㅋㅋㅋㅋ ㅋ ㅋ ㅋ	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	<mark>3.6.1</mark> 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	<mark>3.5.1</mark> 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<u>3.8</u>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	フィルタ機能と拡張認証機能を使用するため、
extended-authentication	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	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config)# vlan 10,1000	認証前 VLAN として VLAN10 を、管理用 VLAN
(config-vlan)# state active	として VLAN1000 を作成します。
MAC VLAN の設定	
(config)# vlan 30 mac-based	検疫 VLAN として MAC VLAN30 を作成しま
(config-vlan)# name QuarantineVLAN	
(config)# ylon 100 maa baaad	▶ 博架ホイント<u>(Ⅰ)</u> 認証後 \// AN トレズ MAC \// AN100 た作式
(config-vlan)# name OkVLAN	認証後 VLAN として MAC VLAN 100 を作成し ます
	<u>ራ ሃ 0</u>
ベハーンゲンリーの設定 (config)# spanning tree disable	フパニングツリーを無効にします
(comg)# spanning-nee disable	スパーンゲンゲーを無効にしより。
物理ポートの設定	
●認証用	
(config)# interface range fastethernet 0/1-10	ポート 0/1~0/10 を、MAC VLAN ポートとし
(config-if-range)# switchport mode mac-vlan	て設定します。
(config-if-range)# switchport mac vlan 30,100	MAC VLAN ポートに VLAN30 および 100 を、
(config-if-range)# switchport mac native vlan 10	Native VLAN として VLAN10 を設定します。
● トルフノルエレのほた田	▶ 構架ホイント <u>(1)</u>
●エゼス1ッテとの通信用 (config)# interface range gigsbitetbernet 0/25-26	ポート 0/25~0/26 た ト位フィッチャ通信す
(config-if-range)# switchport mode trunk	ホートの25%の20を、エロスイッチを通信す ストランクポートとして設定します
(config-if-range)# switchport trunk allowed vlan	トランクポートに VI AN30、100 および 1000
30,100,1000	を設定します。
インタフェースの設定	
(config)# interface vlan 1000	管理用 VLAN1000 にインタフェース IP アドレ
(config-if)# ip address 172.16.0.12 255.255.255.0	スを設定します。
RADIUS サーバの設定	
(contig)# radius-server host 10.50.0.1 key alaxala	検疫サーハの IP アドレスおよびキーを設定し
	まり。平川1Fビは十一を「alaxala」として います
	いみり。 > 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	以下のアクセスリスト「Quarantine」を作成 します。
(config-ext-nacl)# permit protocol ip src 192.168.30.0 0.0.255 dst 10.52.0.1 0.0.0 (config-ext-nacl)# permit protocol ip src 10.52.0.1 0.0.0 dst 192.168.30.0 0.0.255 (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	 ・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。
(config)# interface vlan 30 (config-if)# ip access-group Quarantine in	検疫 VLAN30 にアクセスリストを適用しま す。 ▶ 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	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。
(config-if-range)# dot1x reauthentication (config-if-range)# dot1x supplicant-detection disable (config)# dot1x system-auth-control	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。
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	サプリカントの再認証周期を <mark>600 秒(10 分)</mark> 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	ポート 0/1 を MAC 認証用ポートとして設定し
(config-if)# mac-authentication port	ます。
	▶ 構築ポイント <u>(4)</u>
MAC 認証の設定	
(config)# aaa authentication mac-authentication	RADIUS サーバでユーザ認証を行うことを設
default group radius	定します。
(config)# mac-authentication system-auth-control	MAC 認証機能を有効にします。
以下の設定は、環境に合わせて行います。	
(config)# mac-authentication id-format 1	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。
(config)# mac-authentication password macpass	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
	1	一大垣り以た

AX2400S の設定	
ポート VLAN の設定	
(config)# vlan 1	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config)# vlan 10,1000	認証前 VLAN として VLAN10 を、管理用 VLAN
(config-vlan)# state active	として VLAN1000 を作成します。
MAC VLAN の設定	
(config)# vlan 30 mac-based	検疫 VLAN として MAC VLAN30 を作成しま
(config-vlan)# name QuarantineVLAN	す。
	▶ 構築ポイント <u>(1)</u>
(config)# vlan 100 mac-based	認証後 VLAN として MAC VLAN100 を作成し
(config-vlan)# name OkVLAN	ます。
スパニンクツリーの設定	
(config)# spanning-tree disable	スハニンクツリーを無効にします。
物理ホートの設定	
●認証用	
(config)# interface range gigabitethernet 0/1-10	ホート 0/1~0/10 を、MAC VLAN ホートとし エ記ロレナナ
(config-if-range)# switchport mode mac-vian	して設たしまり。 MAC VI AN ポートに VI AN20 たたが 100 た
(configuit-range)# switchport mac vian 50,100	MAC VLAN 小一下に VLAN30 のよい 100 ぞ、 Notivo VLAN トレイ VLAN10 た設空します
(comg-n-range)# switchport mac halive vian to	Native VLAN として VLAN TO を設定しより。 参構築ポイント(1)
●上位スイッチとの通信用	
(config)# interface range gigabitethernet 0/47-48	ポート 0/47~0/48 を、上位スイッチと通信す
(config-if-range)# switchport mode trunk	るトランクポートとして設定します。
(config-if-range)# switchport trunk allowed vlan	トランクポートに VLAN30、100 および 1000
30,100,1000	を設定します。
インタフェースの設定	
(config)# interface vlan 1000	管理用 VLAN1000 にインタフェース IP アドレ
(config-if)# ip address 172.16.0.11 255.255.255.0	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9。
	/ 悟采小1 ノ Γ <u>(3)</u>
TJTルトルートの改正	ニュートリート たいウレナナ
(conny)# ip default-gateway 172.16.0.254	テノオルトルートを改正しまり。

(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	以下のアクセスリスト「Quarantine」を作成し ます
(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	 ・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。
(config)# interface vlan 30 (config-if)# ip access-group Quarantine in	検疫 VLAN30 にアクセスリストを適用します。 ▶ 構築ポイント<u>(2)</u>

(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	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)
(config)# dot1x vlan dynamic enable	IEEE802.1X 認証を有効にします。
(config)# dot1x vlan dynamic reauthentication (config)# dot1x vlan dynamic supplicant-detection disable (config)# dot1x system-auth-control	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。
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	サプリカントの再認証周期を <mark>600 秒(10 分)</mark> 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	ポート 0/1 を MAC 認証用ポートとして設定し
(config-if)# mac-authentication port	ます。
	構築ポイント <u>(4)</u>
MAC 認証の設定	
(config)# aaa authentication mac-authentication	RADIUS サーバでユーザ認証を行うことを設
default group radius	定します。
(config)# mac-authentication system-auth-control	MAC 認証機能を有効にします。
以下の設定は、環境に合わせて行います。	
(config)# mac-authentication password macpass	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	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config)# vlan 30,100	検疫 VLAN として VLAN30 を、認証後 VLAN
(config-vlan)# state active	として VLAN100 を作成します。
(config)# vlan 50,51,52	サーバ用 VLAN として VLAN50、51、52 を作
(config-vlan)# state active	成します。
(config)# vlan 1000	管理用 VLAN として VLAN1000 を作成します。
(config-vlan)# state active	
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	ポート 0/1~0/2 を、アクセスポートとして設
(config-if-range)# switchport mode access	定します。
(config-if-range)# switchport access vlan 50	アクセスポートに VLAN50 を設定します。
(config)# interface range gigabitethernet 0/3-4	ポート 0/3~0/4 を、アクセスポートとして設
(config-if-range)# switchport mode access	
(config-if-range)# switchport access vian 51	アクセスホートに VLAN51 を設定します。
(config)# interface range significations 0/5 6	ポート 0/5~0/6 ち、マクセスポートトレイジ
(config_if_range)# switchport mode access	ホート 0/5~0/6 を、アクセスホートとして設 テレキオ
(config-if-range)# switchport access vian 52	」たしより。 アクセスポートに \/I_ANI52 を設定します
	ノノビス小一FIC VLANSZ を設定しより。
(config)# interface range gigabitethernet 0/47-48	ポート 0/47~0/48 を 下位スイッチと通信す
(config-if-range)# switchport mode trunk	ふトランクポートとして設定します。
(config-if-range)# switchport trunk allowed vlan	トランクポートに VLAN30, 100 および 1000
30,100,1000	を設定します。
インタフェースの設定	
(config)# interface vlan 30	各 VLAN にインタフェース IP アドレスをそれ
(config-if)# ip address 192.168.30.254 255.255.255.0	ぞれ設定します。
(config)# interface vlan 100	
(config-if)# ip address 192.168.100.254 255.255.255.0	
(config)# interface vian 50	
(config-if)# ip address 10.50.0.254 255.255.255.0	
(config)# interface vian 51	
(config)# interface view 52	
(config_if)# in address 10.52 0.254.255.255.0	
(comg-n)# ip address 10.52.0.254 255.255.255.0	
(config)# interface vlan 1000	
(config-if)# in address 172 16 0 254 255 255 255 0	
DHCP リレーの設定	
(config)# interface vlan 30	VLAN30 および 100 に対して、DHCP リレー
(config-if)# ip helper-address 10.50.0.2	エージェントによる転送先アドレスを設定し
	ます。
(config)# interface vlan 100	
(config-if)# ip helper-address 10.50.0.2	

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。

 「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。

ファイル(E) 操作(A) 表	示② ヘルプ④			
🗢 🔿 🔁 💽 🖷				
 クインターネットIZIEサービ RADIUS クライアンメ リモート アクセスの(ジリモート アクセス ボ 接続要求の処理 	ス(ローカル) するX24305 新しい RADIUS クライアント(①) 新規作成(①) まこ0.0	アドレス 172.16.0.11 72.16.0.12	プロトコル RADIUS RADIUS	クライアント製造元 RADIUS Standard RADIUS Standard
-	最新の情報に更新(F) 一覧のエクスポート(L)… ヘルプ(L)			
-	I	72		

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」)

クライアントのフレンドリ名と I	P アドレスまたは DNS 名を入力してください	lo
フレンドリ名(圧):	iNetSec	
クライアントのアドレス (IP ま)	E(J DNS)(D):	
10.50.0.1		確認(⊻)

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。

ライアント ペンダの開始に基づいモート アクセス ポリシーを使用している場合、RADIUS クライアントのペンダ 指定してださい。 クライアント ペンダ(2): [RADIUS Standard 共有シークレット(2): ####### 共有シークレットの確認入力(2): #######		
クライアント ペンダ(©): 「RADIUS Standard 共有シークレット⑤: #****** 共有シークレットの確認入力(©): #******	ライアントベンダの属性に基づくリモート 指定してください。	アクセスポリシーを使用している場合、RADIUS クライアントのベンダ
RADIUS Standard ▼ 共有シークレット⑤: ******* 共有シークレット⑤: *******	クライアント ベンダ(<u>©</u>):	
共有シークレット©: ****** 共有シークレットの確認入力(Q): ******	RADIUS Standard	×
共有シークレットの確認入力(2): *******	共有シークレット(<u>S</u>):	жыскоюк
	共有シークレットの確認入力(@):	*****

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。

 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

8	転転サーバ 初調面間	i - Mozilia Firefox		_ _ _ ×
ファイル(上) 編集(上) 表示(型) 税額(広) ブッ	24-2(E) λ-M(T) √	%7(<u>⊣</u>)		0
🦛 - 🏟 - 🍠 💿 🚷 🕕 ктр уло за	0.1 8081/Secure/sateauthor	/satecgi/sateud.cg		9 860 🔎
通用 ● 総動/符上	クライアン	トの設定		
環境設定				Balp
 <u>ノフートは数点に</u> <u>クライアント数度</u> <u>スケジュール性報設定</u> <u>フトリビュート情報設定</u> フィルタリング福和設定 	クライアントアドレス クライアントレベル クライアントは新キー	177, 16, 0, 11 0: 標準但想	2	
 <u>ポート番号設定</u> ユーザ借税設定 PROXY設定 コーザ定義ファイルの読み込み 	認証許可	6 許可	⊂禁止	
● 証明書情報設定 ● 詳細情報設定 ● 証明書発行	<u></u>	317 H-248		
● <u>邮用量一括共任</u> ● <u>CRL结報設定</u>	CHECK クライアント	アドレス クライアント	1.~JF	
 ● 検疫情報設定 ● 検疫情報設定 	C 172.16.0.11 C 172,16,0,12	0:標準仕校 0:標準任校		
状 ^技 参照 ● <u>ログイン状況の泰明</u>				
ロダノほ合情報の参照 ● 課金情報の参照 ● <u>アクセスログ情報の参照</u> ● ROXY21000000000				
 エラーログ体制の条照 エラーログ体制の条照 課会活動点計算 				
27				

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。

(V	認証サーバ 初期画面 -)	dozilla Firefox			_ 0 ×
ファイル(E) 編集(E) 表示(型) 粉掛(G) ブラ	$g = g = g(\underline{\mathbf{R}}) - g(\underline{\mathbf{r}}) - g(\underline{\mathbf{r}}) = -g(\underline{\mathbf{r}})$	0			0
🖕 • 🍦 - 💋 💿 🏠 🗋 НЦжиго 50.	0.1.8081/Secure/Safeauthon/Safe	ugi/Safeuid.ugi		🕘 🕲 ##1 🔑	
運用		1.1++0			
• <u>#280 / 17 il-</u>	アトリヒュー	ト情報の話	定		
環境設定				-	is la
● アラート情報設定					
 クライアント設定 スケジュール情報設定 	クライアントレベル [018	第位师 : -			
 アトリビュート情報設定 フィルタリング情報設定 	サービスグループ				
■ ボート番号設定	居住茶 会 118	er.Nome	-		
 <u>ユーザ情報設定</u> BROXXS 	ベンダーID	e manne	-		
 コーデ索素ファイムのはわけみ 	ベンダー属性				
 新期書情報設定 	属性促进状				
• 詳細情報決定	タグ情報				
■ 証明書発行	相別 (* +	ッラクタ C/S4	ナリ	○ 數値	
 <u>証明書―括発行</u> 	属性能				
■ C R L 情報設定	評価原				
● <u>教授情報院定</u>					
● 検疫対象外ユーザ情報設定					
	· 运加 · 更新 · 自然 · 017	1+783			
状態要照					
● ログイン状況の参照					
ログノ弾会情報の素昭	CHECK サービスグループ	クライアントレベル	評価原	属性番号	ペンダー
■ 課会情報の条約	C NG	0:標準仕株	1	64:Tunnel-Type	
 アクセスログ情報の参照 	c NG	0:標準什樣 2	2	65:Tunnel-Media-Type	
 PROXYIDダ情報の参照 	C NG	0:標準什极 3	3	81:Tunnel-Private-Group-ID	
 エラーログ情報の参照 	-				
 課金信報再計算 					
=7	x				۲
241					

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	数值	13	1
NG	65:Tunnel-Media-Type	数值	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

¥	認証サーバ 引渡画面 - Mozilla Firefox	
ファイル(E) 編集(E) 表示(V) 移動(G) ブラ	$\mathcal{D} = \mathcal{D}(\underline{B}) \mathcal{D} = \mathcal{D}(\underline{\Gamma}) \sim \mathcal{D} = \mathcal{D}(\underline{\Gamma})$	0
🖕 - 🍌 - 🍠 💿 🏠 📋 нер.//30.50.	0.1.8081/secure/safeauthor/safecgl/safeuid.cgl	- O 840 🔎
運用 ● 起動/符止	PROXYの設定	
環境設定		Halp
	ブレライックス 利用本述 ・ する サフィックス 利用本述 ・ する 道家本・ト語号 10 ・ する 道家本・ト語号 101 ・ ・ ・ ・ ・ 東北キ・ト語号 10.50.0.2 ・ ・ ・ ・ ・ 市営長 10.50.0.2 ・ ・ ・ ・ 丁信順 ・ ・ ・ ・ ・ ・ ・ ・ ・ 三匹ご 天野 10.50.1 10.764	- L-Qui - L-Qui - L-Qui
状形表现	CHECK ブレフィックス 削除転送 リフィックス 削除	転送 評価膜 認証ボート番号 課金ボート
 ログイン状況の参照 	c *	1 1812 1813
 ログノ資金価格の時間 <u>認合性能の時間</u> <u>アクセスとグ性能の原則</u> PROXYTP21合相の原則 アラーログ体現の原則 <u>認合性作業に並</u> 		

本例は全て同一サーバ
ヘ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」

8	認証サーバ 将原自己 - Mozila Firefo	x X
ファイル(王) 福泉(王) 表示(王) 材料(日) プッ	$\delta \prec - \delta(\overline{\mathbf{R}}) = \Delta - \Psi(\overline{\mathbf{T}}) = - \nabla \delta(\overline{\mathbf{T}})$	0
🖕 - 🧼 - 🎒 🖸 🚷 🛄 nepyto so	u 1:0031/secure/sareautron/sarecgi/sareuro.cg]] 🛛 🕬 [,P.,]
通用 ● 起動/存止	検疫情報設定	
環境設定		Ralp
 アラートは報報度 		
 ● クライアント設定 ● フライアント設定 	検疫サーバ連携指定	◎ 連携する ○ 連携しない
 ・ アトリビュート情報設定 	RADIUS-PROXY模模指定	● 道携する ○ 道携しない
 フィルタリング情報設置 	検疫サーハナトレス 結約生態サービッグループ	NEP-00 50.01/
 ボート世号設定 	林校タイムアウト時間	300 (1~86400F9)
	被疫処理スレッド数	10 (1~255)
 ユーザ定義ファイルの読み込み 	検疫サーバダウン時の気応等化指定	○ 無応答化する ◇ 無応答化しない
 ■ Ⅲ雪信報設定 	検疫対象外ユーザの即時反映指定	() 以映実行時 () 再動動時
	フライマリ教授サーバアドレス セカンダリ輪続サーバアドレス	·
 ■ 証明書→括発行 		
● C R L 借報設定		
 ● 検疫情報設定 		
● 税役河家外ワーサ情報設定	秩校情報を変更して設定ボタンをクリック 設定後はサービスの再起動を行って下さい	れして下さい。 ^
状態参照	STORE AND A	
 ログイン状況の参照 	Trees Trees	
ロダノ連合性部の兼約		
 課金情報の参照 		
 アクセスログ情報の参照 		
 <u>PROXYログ情報の参照</u> 		
 エラーロクは朝の地獄 課会は範囲計算 		
完7	•	

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。

2	防田サーバ 羽馬田田 - Mozi	la Firefox		
ファイル(E) 編集(E) 表示(Y) 税額(G) ブッ	$2\Delta - 2(\overline{B}) \Delta - \Psi(\overline{T}) \nabla \Psi \Delta(\overline{T})$			
🐗 - 👘 - 🍠 🕄 🚷 🗋 верило на	0.1.8031Kecure/sateauthor/satecg//S	teuding	💽 🛛 Sốn 🔎	
運用 ● 起動/停止	認証サーバの起	動・停止		
釀境設定				Halp
 アラート情報設定 				
 クライアント設定 	物気サーベ分解・ 記動す	,		
● スケジュール情報設定	NUMBER OF THE OWNER			
● アトリビュート情報設定				
 <u>フィルタリング情報設定</u> 	<u></u> 送用環境への反映	(FE 1996)		
PROXYNS				
 ユーザ定義ファイルの読み込み 				
 証明書信報設定 	現在、認証サーバは以下	の環境で動作している	K 97	
● 詳細情報設定	- 金字田是将官法法职。	0000 (00 (00 14-01-0		
 証明書発行 	東谷理用環境区区时间:	2008/08/08 14:31:2	2	
● 証明書一括発行	La manager a second	lavas na na ca ar ar l		
● <u>CRL性報務定</u> ▲ 50/05/1±105/08	クライアント情報	2008/07/29 17:31:33		
 Mean Provide Line	ユーザ情報	2008/08/08 14:31:21		
	アトリビュート情報	2008/07/30 19:34:36		
状態接触	スケジュール情報(週間)	2003/07/23 10:57:08		
 ログイン状況の参照 	スケジュール情報(特異日)	2003/07/23 10:58:40		
	アラート情報	2003/07/23 10:55:32		
ログ/課金情報の参照	ボート情報	2003/07/23 10:58:22		
 課金情報の参照 	PROXY储報	2008/08/05 19:05:24		
● アクセスログ情報の参照		·		
 <u>PROXYログ情報の零度</u> 				
 エンーロン(mittooke)3(
• arazimintra 👫				
<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>				

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

 を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。

🙀 iNetSec Inspection Center 80	02.1X Suppli	cant	
ユーザー認証方式の選択			
使用するユーザー認証方式を選択します	ਰ 。		
● Windows□グオン後(ご認証する(A)			
○ Windowsログオン前(ご認証する(E)			
InstallShield			
	< 戻る(B)) 次へ(N) >	キャンセル

図 3.7-1 クライアントの設定1

 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。

iNetSec Inspection Ce クライアントアップデートサール	nter 802.1X Supplicant の指定	
クライアントアップデートサーバを	以下の形式で指定して下さい。	
http://サーバアドレス:ボート番	号	
https://サーバアドレス:ボート看	持/	
ポート番号を省略した場合、h	:tpは80、httpsは443になります。	
クライアントアップデートサーバ (複数指定時は、セミコロン";"[2 http://10.50.0.1/	〔切りでエントリを分けて(ださい。)	
http://10.00.0.1/		
tallShield		
	く 戻る(目)次へ()	V)> キャンセル

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。

iNetSec 802.1X 設定	×
ユーザー設定 コンピュータ設定 詳細設定 - アダプター - 覧 ① ✓Intel(R) 82562V-2 10/100 Network Connection	
プロファイルー覧(2) 「 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
OK	

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

王取 黒線の設定	孤張載定		
プロファイル名(<u>P</u>):	alaxala		
- 認証方法			
EAP の種類(<u>E</u>):	PEAP v0/EAP-MS-CHAP-V2		
	(
☑ TP アドレスを更ま	543.(N)		
☞ IP アドレスを更新	<u></u>		
☞ IP アドレスを更新	<u></u>		
IP アドレスを更来			
▼ IP アドレスを更新	<u></u>		
▼ IP アドレスを更素			
☞ IP アドレスを更新			
IP アドレスを更新			

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。

PEAP ወታወለታィ	
第1段階 「第1段階での Identityの 「サーバ証明書 ルート証明相	I Identity を指定する(1) 「 を検証する(D)
- 第2段階	
ユーザー名(山):	user01
パスワード(<u>P</u>):	******** ✓ パスワードを保存する(S)

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。

iNetSec 802.1X 設定	×
ユーザー設定 コンピュータ設定 詳細設定 アダプター→覧① ✓Intel(R) 82562V-2 10/100 Network Connection	
プロファイルー覧(P) ✓slaxela ↓①	
OKキャンセル	

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。

- 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。
- 後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。

	発展サーバ 引見目目 - Mozna Hirerox	
ファイル(E) 編集(E) 表示(E) 移動(<u>6</u>) ブッ	$Q \Delta - Q(\overline{E}) = \Delta - 2^{\mu}(\overline{T}) = \sqrt{2^{\mu}\Delta_{\mu}(\overline{E})}$	0
🛊 • 🛶 - 👙 🕲 🚷 🗈 http://10.50	0.1.8061/secure/satesuthor/satesg/sateud.cg]
運用 ● <u>起動/存止</u>	検疫対象外ユーザ情報の設定	
	検疫対象染ユーザD periq 検疫対象染ユーザDを指定して進加ポタンはとは判除ポタンをクリックして下さい。 ま変なはアービスの再起相互には進用環境への反映を行って下さい。	2017
1.00		

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<u>3.4</u>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<u>5.1.3</u>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	Windows Server 2003	Windows XP
release 5.1	・ActiveDirectory ドメインコン	InternetExplorer 6
・iNetSec Inspection Center サーバ	トローラ	
パッケージ	・RADIUS サーバ(IAS)	Windows Vista
 iNetSec Inspection Center 		InternetExplorer 7
V5.0L10A 認証機器拡充固有修正		
		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
=1)=7 CD	0/1	アクセス	MAC 認証 (固定 VLAN)	100		
AX2400S	品公司上773	0/1~0/10	ポート	Web 認証 (固定 VLAN)	100	
	上位スイッチ との通信用	0/47~0/48	トランク ポート	—	—	100,1000
	≣刃≣∓ 用	0/1	アクセス	MAC 認証 (固定 VLAN)	100	
AX1200S	品公司上7日	0/1~0/10	ポート	Web 認証 (固定 VLAN)	100	_
	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	0	Δ	0	0
検疫失敗端末	0	Δ	×	0

※表中の〇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、パスワードー覧

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 Ø (5)
2		カニノマント初証と	olovolo		4.4.3 () (4)
3	 検疫サーバ 	クライアント認証キー	alaxala	RADIUS 9-9 D9F	4.0.20)2
4		PrimaryAuthSecret	alaxala	RADIUS シークレット	<mark>4.6.2</mark> の⑥
5		切替用アカウント	tmp01~	切替用アカウントの	16202
		KeyName	tmp10	ユーザ ID	4.0.2003
6		切替用アカウント	tmppace	切替用アカウントの	16203
0		Password	Password	パスワード	4.0.2003
7		サカシ カレット	alayala		4 5

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。

- 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。 検疫サーバヘ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"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	フィルタ機能と拡張認証機能を使用するため、
extended-authentication	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	VLAN1 は使用しないため、無効にします。	
(config-vlan)# state suspend		
(config)# vlan 100,1000	認証 VLAN として VLAN100 を、管理用 VLAN	
(config-vlan)# state active	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	ポート 0/1~0/10 を、アクセスポートの	
(config-if-range)# switchport access vlan 100	VLAN100 に設定します。	
● したっ くってし かぼた田		
●上位入イッナとの通信用		
(config)# interface rqnge gigabitetnernet 0/25-26	ホート 0/25~0/26 を、上位スイツナと通信 9	
(config-if-range)# switchport mode trunk	るトフノグホートとして設定しまり。	
(config-in-range)# switchport trunk allowed vian	トラフクホートに VLAIN100 および 1000 を設 空」ます	
	たしより。	
インメンエースの設定 (config)# interface vian 1000	答理田 \/ AN1000 にくいタフェース IR スドレ	
(config_if)# in address 172 16 0 12 255 255 255 0	官理用 VLANTOOD にインテンエース IF ノドレ スを設定します	
(comig-in)# ip address 172.10.0.12 235.255.255.0	へを成だしより。	
(config)# interface vlan 100	認証用 VLAN100 にインタフェース IP アドレ	
(config-if)# ip address 192.168.100.12 255.255.255.0	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	以下のアクセスリスト「WEBAUTH」を作成
	します。
(config-ext-nacl)# permit udp src 0.0.0.0	①クライアント端末からの DHCP パケット
255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps	を許可します。
(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	②クライアント端末からの DNS パケットを
0.0.0.255 dst 10.50.0.3 0.0.0.0 eq domain	許可します。
(config-ext-nacl)# permit protocol ip src 192.168.100.0	③クライアント端末から検疫サーバ宛の
0.0.0.255 dst 10.50.0.1 0.0.0.0	信を許可します。
(config-ext-nacl)# permit protocol ip src 192.168.100.0	④クライアント端末から修復サーバ宛の通
0.0.0.255 dst 10.52.0.1 0.0.0.0	信を許可します。
	▶ 構築ポイント <u>(2)</u>

(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	ポート 0/1 を MAC 認証用ポートとして設定し
(config-if)# mac-authentication port	ます。
	▶ 構築ポイント <u>(4)</u>
MAC 認証の設定	
(config)# aaa authentication mac-authentication	RADIUS サーバでユーザ認証を行うことを設
default group radius	定します。
(config)# mac-authentication system-auth-control	MAC 認証機能を有効にします。
以下の設定は、境境に合わせて行います。	
(config)# mac-authentication id-format 1	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。
(config)# mac-authentication password macpass	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) 共通の詞

AX2400S の設定		
ポート VLAN の設定		
(config)# vlan 1	VLAN1 は使用しないため、無効にします。	
(config-vlan)# state suspend		
(config)# vlan 100,1000	認証 VLAN として VLAN100 を、管理用 VLAN	
(config-vlan)# state active	として VLAN1000 を作成します。	
スハ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。	
●割計用		
●認証用 (config)# interface range gigsbitetbernet 0/1 10	ポート 0/1~0/10 た アクセスポートの	
(config-if-range)# switchport access vian 100	バードの100010 を、アクセスホードの VLAN100 に設定します	
(comig in range)# switchport access vian roo		
●上位スイッチとの通信用		
(config)# interface range gigabitethernet 0/47-48	ポート 0/47~0/48 を、上位スイッチと通信す	
(config-if-range)# switchport mode trunk	るトランクポートとして設定します。	
(config-if-range)# switchport trunk allowed vlan	トランクポートに VLAN100 および 1000 を設	
100,1000	定します。	
インダノェー人の設定		
(config)# interface vian 1000	官理用 VLAN1000 にインタフェース IP アトレ スチ乳ウレキナ	
(config-if)# ip address 172.16.0.11 255.255.255.0	人を設定しまり。	
(config)# interface vlan 100	 	
(config-if)# ip address 192.168.100.11 255.255.255.0	ふ 証別 いしんいの に イングン エーバー グイン	
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	以下のアクセスリスト「WEBAUTH」を作成し
	ます。
(config-ext-nacl)# permit udp any any eq bootps	①クライアント端末からの DHCP パケットを
(config-ext-nacl)# permit udp any host 10.50.0.3 eq	許可します。
bootpc	
(config-ext-nacl)# permit udp 192.168.100.0	②クライアント端末からの DNS パケットを許
0.0.0.255 host 10.50.0.3 eq domain	可します。
(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255	③クライアント端末から検疫サーバ宛の 信
host 10.50.0.1	を許可します。
(config-ext-nacl)# permit ip 192.168.100.0 0.0.0.255	④クライアント端末から修復サーバ宛の通信
host 10.52.0.1	を許可します。
	構築ポイント <u>(2)</u>

(3) Web 認証の設定

AX2400S の設定		
Web 認証の設定		
(config)# web-authentication system-auth-control	Web 認証を有効にします。	
(config)# web-authentication ip address 1.1.1.1	Web 認証専用 IP アドレスを設定します。	
(config)# web-authentication redirect-mode http	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	ポート 0/1~0/10 に対して、Web 認証を有効	
(config-if-range)# web-authentication port	にします。	
(config-if-range)# authentication ip access-group	認証前アクセスリスト "WEBAUTH" を有効に	
"WEBAUTH"	します。	
(config-if-range)# authentication arp-relay	認証前に arp リレーを有効にします。	
RADIUS の設定		
(config)# aaa authentication web-authentication	RADIUS サーバで Web 認証を行うことを設定	
default group radius	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	ポート 0/1 を MAC 認証用ポートとして設定し	
(config-if)# mac-authentication port	ます。	
	▶ 構築ポイント(4)	
MAC 認証の設定		
(config)# aaa authentication mac-authentication	RADIUS サーバでユーザ認証を行うことを設	
default group radius	定します。	
(config)# mac-authentication system-auth-control	MAC 認証機能を有効にします。	
以下の設定は、環境に合わせて行います。		
(config)# mac-authentication password macpass	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	VLAN1 は使用しないため、無効にします。	
(config-vlan)# state suspend		
(config)# vlan 100,1000	認証 VLAN として VLAN100 を、管理用 VLAN	
(config-vlan)# state active	として VLAN1000 を作成します。	
(config)# vlan 50,51,52	サーバ用 VLAN として VLAN50、51、52 を作	
(config-vlan)# state active	反します。	
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。	
物理ホートの設定		
(config)# interface range gigabitethernet 0/1-3	ホート 0/1~0/3 を、アクセスホートとして設	
(config-if-range)# switchport mode access		
(config-if-range)# switchport access vian 50	アクセスホートに VLAN50 を設定します。	
(config)# interface gigabitethernet 0/4	 ポート 0/1 を アクセスポートと て設守 ま	
(config_if_range)# switchport mode access	ホートのキを、アノビスホートとして設定しよ	
(config-if-range)# switchport access vian 51	ッ。 アクセスポートに VI AN51 を設定します。	
(config)# interface gigabitethernet 0/5	ポート 0/5 を、アクセスポートとして設定しま	
(config-if-range)# switchport mode access	す。	
(config-if-range)# switchport access vlan 52	アクセスポートに VLAN52 を設定します。	
(config)# interface range gigabitethernet 0/23-24	ポート 0/23~0/24 を、下位スイッチと通信す	
(config-if-range)# switchport mode trunk	るトランクボートとして設定します。	
(config-if-range)# switchport trunk allowed vian	トランクホートに VLAN100 およひ 1000 を設	
100,1000	正しま9。	
インタフェースの設定		
(config)# interface vlan 100	冬 VI AN にインタフェース IP アドレスをそれ	
(config-if)# ip address 192.168.100.254 255.255.255.0	それ設定します。	
(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 view 1000		
(conny)# Interface vian 1000 (config if)# in address 172.16.0.254.255.255.255.0		
(conny-n)# ip address 172.10.0.234 235.235.235.0		
(config)# interface vian 100	VLAN100に対して、DHCPULLーエージェン	
(config.if)# in helper-address 10 50 0 2	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。)

	root	@redhat	5:/etc/qu	arantine	e/base/conf	
ファイル(<u>E</u>)	編集(<u>E</u>)	表示(⊻)	端末(<u>T</u>)	タブ(<u>B</u>)	ヘルプ(<u>H</u>)	
VeyName=tmp GenerateNumb Password=tmp TTLSwitchAcc	er=10 pass ount=10					4
~						=
~						
~						
~						
2						
~						
~						
~						
~						~

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。)

root@redhat5:/etc/quarantine/share/conf	
ファイル(<u>E</u>) 編集(<u>E</u>) 表示(<u>V</u>) 端末(<u>T</u>) タブ(<u>B</u>) ヘルプ(<u>H</u>)	
ALAXALA, 0. 0. 0. 0, 255. 255. 255. 255	<u></u>
~	
~	
~	
~	
~	
~	
~	
~	
~	=
~	
~	
~	
~	
~	
~	
~	
~	
	T

☑ 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
- PrimaryAuthPort = 1812 •

(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)
 - (本ガイドでは RADIUS 使用ポートに"1812"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。

💷 ro	ot@r	edhat5:	/etc/quai	rantine/s	hare/cor	11 ⁷ – 🗆 🗙
ファイノ	ν(<u>F</u>)	編集(<u>E</u>)	表示(<u>V</u>)	端末(<u>T</u>)	タブ(<u>B</u>)	ヘルプ(<u>H</u>)
Iugin=(AuthSkip Primary) Primary) Secondai Secondai Secondai AuthTima AuthRet ChangeT	DN p=OFF AuthSe AuthSe ryAuth ryAuth ryAuth ryAuth ryAuth ry=3 ime=30	erver=10.1 prt=1812 ecret=ala: nServer= nPort= nSecret= 3	50.0.2 xala			

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 •

•

AuthCGIProtocol=https • AuthCGIPort=443

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



X 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。

👷 🕸 🏀 Dダイン		} ベージ(P) ▼ () ▼ //(O) ▼ "
2 この Web 54 FEL F とアドインを住職し、3	りしいTEL からの Recisio Impedian Canad Vacual アトメンをあましょ やまとめ第六を計画するには、ここをクリックしてくとさい…	ActiveX コントロールの実行(C) 危険性の説明(W) 詳細情報(I)
	ログイン ユーザー名とバスワードを入力してくださ ユーザーち バスワード	U
	ロダイン	

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。



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。

🚖 🎕 🍘 🖉 🖉 🖗	⁽¹⁾ ▼ ⁽²⁾	▼ ③ ツール(0) ▼ "
	ログイン	_
	ユーザー名とバスワードを入力してください ユーザー名 user01	
	1829-F	
	iNetSec Inspection Center V50	
	🍙 😜 インターネット 保護モード: 無効	€ 100% -

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。

😭 🏟 🏈 接続中	<u></u>	© ツール(0) ▼ [»]
	接続の実行	
	ただいは接続中です。しばらくお待ちください。	E
	US 1005 年4ンセル	
ページが表示されました	😱 🔮 インターネット 保護モード: 無効	•

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。

😭 🍄 🌈 ログイン成	あ ▼ <u>□</u> ▼ <u>□</u> ▼ <u>□</u> ページ(P) ▼ ③ ツール(0) ▼ [※]
	ロウインしました。
	All Rights Reserved Copyright @ PFU LIMITED 2004-2008
ページが表示されました	🕞 🔮 インターネット 保護モード: 無効 🔍 100% 🔻

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。

: 1

- 認証キー : alaxala
- 転送先アドレス : 10.50.0.2
- 評価順

9 ·		開ビサー	《 初期義武 - Mo.	illia Firefox			1.0
ファイル(2) 編集(2) 表示(文) 制約(2) (4) (2) (4) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	() ブックマーク(田) //10 50 0 1 8081/secu	v=a(I) ~a	카(H) 카ecginateust.cgi			• •	MR (A.
運用 ● <u>起動/得止</u> 環境設定	PROX	(Yの)	设定				56.1p
2.2.1.は単語空 2.5.47.2.1.2 2.5.47.2.1.2 2.4.75.1.2.1.2 2.4.75.1.2.1.2.2 2.4.75.1.2.2.2 2.4.75.1.2.2.1.2.2 2.4.75.1.2.2.2 2.4.75.1.2.2.1.2.2 2.4.75.1.2.2.2 2.4.75.1.2.2.2.2.2 2.4.75.1.2.2.2 2.4.75.1.2.2.2.2.2.2 2.4.75.1.2.2.2.2 2.4.75.1.2.2.2.2.2.2.2.2.2 2.4.75.1.2.2.2.2.2 2.4.75.1.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.	プレフィックス サフィックス 認証ボート番号 講座ホー 転送キー 転送先アドレス 評価原	Poarstine. (1)(1)(4)(4)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)	 с т 5 с т 5 т т 5 				
★50参照 ● ログイン状況の参照	CHECK 717	ィックス NN	転送 サフィック	ス 削除転送 評価 1	取 綿証ボー 1812	ト書号 課会ボート 1813	番号 転送先アドレス 10.50.0.2

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
0	quaratine.	する			1	1812	1813	10.50.0.2
0	*				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



🗵 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。)



🗵 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。

🚆 COM4-96005aud - Tera Term VT		
アイルロ 編集句 脱毛の 立トロールの ウル 育 者 show web-authentication Date 2009/01/08 14:05:23 U Total user counts:1	നയം സംഗയ login TC	~
F Username VLAN MAC address Login time quarantine user01	Port IP address Limit time	
100 001e.c20c.Ode4 2009/01/08 14:03:31 UTC 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	0/3 192.168.100.101 00:58:08	
å I		2

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<u>5.1.3</u>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	edge#1> show dot1x port 0/1 detail						
Date 2008/08/27 19:14:51 JST							
Port 0/1(Dynamic)							
AccessControl : Multiple	le-Auth	PortC	ontrol	: Auto			
Status :		Last	EAPOL	: 0019.bs	97d. 4bfa		
Supplicants : 2 / 2 /	/ 64	ReAut	hMode	: Enable			
TxTimer : 30		ReAut	hTimer	: 600			
ReAuthSuccess : 54		ReAut	hFail	: 3			
SuppDetection : Disable	e						
Supplicants MAC F Sta	atus /	AuthState	BackEr	ndState	ReAuthSuccess		
Ses	ssionTime(s) [Date/Time					
001e.c965.dd62 Aut	thorized /	Authenticate	d Idle		2		
140)8	2008/08/27 1	8:51:21				
0019.b97d.4bfa Aut	thorized I	Authenticate	d Idle		0		
103	3	2008/08/27 1	9:13:08				
edge#1> show mac-address	s-table						
Date 2008/08/27 19:15:03	3 121						
Aging time : 300			01.0	NO 1			
No MAC address V	/LAN Type	Port	Churp	MCast			
1 UU19. b9/d. 4bfa	IU Dynam		-	-			
2 UUTE. C965. dd62	JU DOTIX	U/ I	-	-			
3 0012. e248. 4220	100 Dynam	10 0/25	-	-			
4 0019. b9/d. 4bta	IUU Dot1x	0/1	-	-			
5 0012. e248. 4220 1	1000 Dynam	ıc 0/25	-	-			

図 5.1-1 AX1200Sの状態表示例

edge#2> show dot1x v	lan dynamic detai	i I		
Date 2008/08/27 19:20	6:04 JST			
VLAN(Dynamic)				
AccessControl : Mul	tiple-Auth	PortCon	trol : Auto	
Status :		Last EA	POL : 001e.	c965. dd62
Supplicants : 2 /	2 / 256	ReAuthM	ode : Enabl	e
TxTimer(s) :	/ 30	ReAuthT	imer(s): 556	/ 600
ReAuthSuccess : 1		ReAuthF	ail : O	
SuppDetection : Disa	able			
VLAN(s): 30,100				
Supplicants MAC	Status A	luthState	BackEndState	ReAuthSuccess
	SessionTime(s) D	Date/Time		
[VLAN 30]	VLAN(Dynamic) Su	upplicants : 1		
001e.c965.dd62	Authorized A	Authenticated	ldle	0
	45 2	2008/08/27 19:	25:19	
[VLAN 100]	VLAN(Dynamic) Su	upplicants : 1		
0019. b97d. 4bfa	Authorized A	Authenticated	ldle	0
	56 2	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

(1)show 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

(2)show 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 001e. c965. ea0c 0/1 100 2008/09/04 18:55:23 3384 1 infinity

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。

 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。

🕒 DA-Fx 20137) - Mozila Firefox 📃 न 🗵							
ファイル(F) 議員(F) 務局(G) ブックマーク(R) ツール(T) ヘルプ(H) ○							
🜾 - 🎲 - 😼 🕄 🏠 🗋 http://2015/0.0.2/guaranthre/admin/ReportingDisp. 🕒 🛛 891 🖉							
<i>∉i</i> iNetSec*	レポーティン	グ出力	n2754				
11回後の部分キムリア々 10日から生きりフォ 10日から生きりフォ 20日からアプロ入 またジフトクマアロ入 12人でひった 20人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が分かった 30人が	15月2 ライアントDAH 第四(YYYY)H46の)	<u></u>					
FUY- 51レ J MAC / PLX Appels 東京会7内ウント 動作環境 和に計畫型会		クライアント語とキュリティ状態面で	<u></u>				
住店・時間語 レポー」∢ング出力		(444年)計算至約442 (2577)(2577)(2574)(2523)	~ [
		時後の時代 外記 期間(1997)MACD) MAC2 ドレスによる二の時代の例りとか(12.0 - 10.)					
₩7							

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。

- 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。

BEサーバ 新聞画面 - Mozilia Firefox - 一回						
$\tau \prec A^{(-)}$ 編集(L) 表示(<u>V</u>) 初時(<u>G</u>) プ	ックマーク(型) つ	$\gamma = M(\overline{1})$	~~~~(円)			
a = 🕪 = 💋 💿 🚷 🗋 may yao s	2011-0000/secto	e/aleath	n/wiecg/stead op	1	🚽 🥨 Siki 🔎	
/用 ● 超動/帝王	PRO	οхı	(ログ情報の	O参照		
 ● グラートは無路定 ● グラートは無路定 ● クライアント設定 ● <u>2クジュール連携</u>協定 ● <u>2トリビュートは無路定</u> ● フィルタリングは無数定 ● オート書目設定 	記証サーバ 開始日付 終了日付 <u>第ページ</u>	0 %155 :2008/08, :2008/08, :2008/08,	8 108 00:00:00 109 23:59:59	2008/09/03 1	15:41:19 wed	
 ■ <u>コーザ後報設定</u> ● PROXY設定 	日付	建制	RADIUSD-F	販業先アドレス	転送先-Port	a- ∜ ∣D
● ユーザ定義ファイルの読み込み	2008/08/08	12:46:09	チャレンジュード通知	10.50.0.2	1812	user01
● 証明書情報設定:	2008/08/08	12:45:09	認証要求	10,50,0,2	1812	user01
◆ 注册通報设定	2008/08/08	12:45:09	認証結束通知 (許可)	10.50.0.2	1812	user01
● <u>新期書発行</u>	2008/08/08	12:46:24	統訂要求	10,50,0,2	1812	001er965dd62
● 証明書一洁発行	2008/08/08	12-46-24	認証結果通知 (不許可)	10.50.0.2	1812	001ec965dd62
● CKL情報設定	2008/08/08	12:47:23	認証要求	10.50.0.2	1812	user01
▲ 始始对意识□	2008/08/08	12:47:23	チャレンジョード追加	10,50,0,2	1812	user01
	2008/08/08	12:47:23	認証要求	10,50,0,2	1812	user01
194 201 10	2008/08/08	12:47:23	チャレンジョード通知	10.50.0.2	1312	user01
● ログイン建況の参照	2008/08/08	12:47:23	認証要求	10.50.0.2	1812	user 01
	2008/08/08	12:47:23	チャレンジョード連知	10,50,0,2	1812	user01
ヴノ課会情報の参照	2008/08/08	12:4/:23	認計要求	10,50,0,2	1812	user01
 決会情報の参照 	2008/08/08	12:47:23	チャレンジコード通知	10,50,0,2	1812	user01
● アクセスログ情報の表現	2008/08/08	12:47:23	認証要求	10.50.0.2	1812	user01
 <u>PROXYログ協報の参照</u> 	2008/08/08	12:47:23	チャレンジョード通知	10.50.0.2	1812	user01
● エラーログ情報の参照	2008/08/08	12:47:24	認証要求	10,50,0,2	1812	user01
● 決金情報再計算	2008/08/08	12:47:24	チャレンジコード通知	10,50,0,2	1812	usor01
	2008/08/08	12:47:24	認証要求	10.50.0.2	1812	user01
	2008/08/08	12:47:24	チャレンジコード通知	10.50.0.2	1812	user01
7	•					

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。

0/100 Natwork Connection	2
しか TOU NetWOrk Connection 通知されたエラーは1件	♪」 です。エラーは最大5件まで表示しま
ォールを有効にしてください。	URL参照(U) 対処実行任
	URL参照(R) 対処実行(I
	山和参照化
	URL参照(E) 対処実行(<u>0</u>)
	URL参照(<u>k</u>) 対処実行(X
	0/100 Network Connection 道数なされたエラー(ま1件 はールを有効にしてください。

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。

検疫結果	X
結果詳細	
アダプター(<u>A</u>): Intel(R) 82562V-2 10	1/100 Network Connection
検疫成功	通知されたエラーは0件です。エラーは最大5件まで表示します。
	URL参照(U) 対処実行(E)
	URL参照(R) 対処実行(D)
	URL参照(P) 対処実行①
	URL参照(C) 対処実行(Q)
	URL参照(位) 対処実行⊗
	再接続(5) 閉じる(2)

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

ー台の 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

ー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.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.2.2. 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ー 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