資料No. NTS-08-R-064
（Rev.0 ）

PFU検疫システム

iNetSec® Inspection Center

評価報告書

iNetSec®

2009年1月30日

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

はじめに

■注意事項

本資料に記載の内容は、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。

■商標一覧

「iNetSec」は株式会社PFU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。
Red Hat は、Red Hat, Inc.の登録商標です。
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。
その他記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

■関連資料

AXシリーズ製品マニュアル
AXシリーズ認証ソリューションガイド

目次

1-1. 評価対象機器と検疫方式

■評価対象機器

本検証にて使用した機器及びソフトウェアのバージョンを以下の表に記載します。

●端末およびサーバとシステムコンポーネント

用途	OS	コンポーネント	
検疫サーバ	RedHat Enterprise Linux 5.1	iNetSec Inspection Center サーバパッケージ	V5.0L10A
		iNetSec Inspection Center 認証サーバパッケージ	V5.0L10
		iNetSec Inspection Center 認証機器拡充固有修正	PL00059-01
外部RADIUSサーバ	Windows Server 2003	Active Directory IAS	SP1
クライアントPC①	Windows Vista SP1	iNetSec Inspection Center IEEE802.1Xサプリカント (IEEE802.1X連携時に使用)	V5.0L10
クライアントPC②	Windows XP SP2		

●認証スイッチ(AXシリーズ)

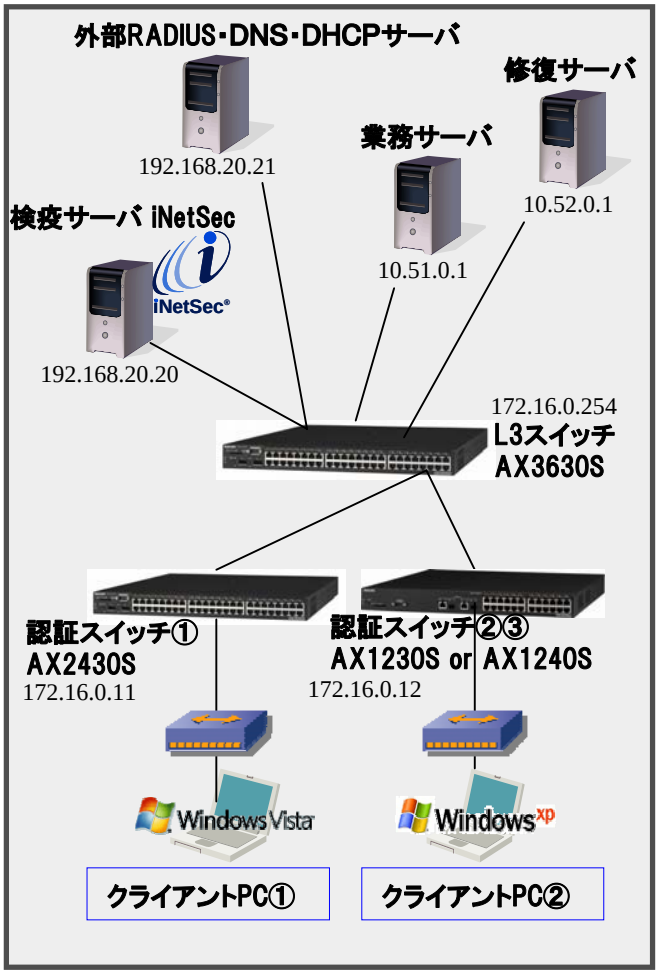
用途	機器名	バージョン
L3スイッチ	AX3630S	11.0
認証スイッチ①	AX2430S	11.0
認証スイッチ②	AX1240S	1.4.B
認証スイッチ③	AX1230S	2.0

1-2. 評価構成

■評価構成図

本検証は以下のネットワーク構成にて実施しました。クライアントPCは検疫と認証を行う前は認証スイッチの認証前アクセスリストにて通信を制限しています。

●構成図



●ネットワーク体系

用途	VLANID	ネットワークアドレス	備考
検疫サーバ用VLAN	50	192.168.20.0/24	
業務サーバ用VLAN	51	10.51.0.0/24	
修復サーバ用VLAN	52	10.52.0.0/24	SUS等を想定、本検証ではPING通信用
管理用VLAN	1000	172.16.0.0/24	
認証後VLAN	100	192.168.100.0/24	（検疫成功後に所属するVLAN）
検疫VLAN	30	192.168.30.0/24	（ゲートウェイ方式では使用しません）
認証前VLAN	10	192.168.10.0/24	（ゲートウェイ方式では使用しません）

●連携する認証方式

iNetSec検疫方式	対応するAXの認証方式
IEEE802.1X認証VLAN方式	IEEE802.1X認証 （ダイナミックVLAN）
ゲートウェイ方式	Web認証 （固定VLAN）

1-3. 動作条件

■検疫結果によるネットワーク制御

本検疫システムではクライアントPCがネットワークに接続した時の認証と検疫の合否の組み合わせにより許可されるアクセス権限が変化します。以下にIEEE802.1X認証VLAN方式とゲートウェイ方式のネットワーク制御の一覧を示します。

（表中の○は通信可能、×は通信不可を示します）

●IEEE802.1X認証VLAN方式使用時の本検疫システムのネットワーク制御を以下の表に示します.

条件	組み合わせ		ネットワーク制御	VLAN-ID	通信許可サーバ		
					検疫	修復	業務
①	認証成功	検疫成功	フルアクセス許可	100	○	○	○
②	認証成功	検疫失敗	検疫VLANによるアクセス制限	30	○	○	×
③	認証失敗	―	認証前アクセスリストによるアクセス制限	10	×	×	×

●ゲートウェイ方式使用時の本検疫システムのネットワーク制御を以下の表に示します.

条件	組み合わせ		ネットワーク制御	通信許可サーバ		
				検疫	修復	業務
①	認証成功	検疫成功	フルアクセス許可	○	○	○
②	認証成功	検疫失敗	認証前アクセスリストによるアクセス制限	○	○	×
③	認証失敗	―	認証前アクセスリストによるアクセス制限	○	○	×

2-1. iNetSec Inspection Center の検証結果

■検証結果一覧

iNetSec検疫とAXシリーズの各認証機能を用いて、検疫システムが構築可能かを検証し、その結果一覧を以下に示します。

検証結果				
iNetSec検疫方式	AX認証方式	AX2400S	AX1200S	備考
IEEE802.1X認証VLAN方式	IEEE802.1X認証 （ダイナミックVLAN）	○	○	2-2. 判断基準と見解 （IEEE802.1X認証方式）
ゲートウェイ方式	Web認証 （固定VLAN）	○	○	2-3. 判断基準と見解 （ゲートウェイ方式）

※表中の○は連携動作の判断基準を満たしていることを示します。

2-2. 判断基準と見解(IEEE802.1X認証VLAN方式)

■ 判断基準

1. 正常端末は、基幹ネットワークに接続できる
2. ポリシー違反した端末は、検疫ネットワークに隔離される
3. 隔離された端末を治療した後は、基幹ネットワークに接続できる
4. 基幹ネットワークに接続した端末がポリシー違反をした場合は、自動的に検疫ネットワークに隔離される
5. MAC認証登録した検疫除外端末が同一ポートで混在可能であること。

■ 見解

iNetSec Inspection CenterのIEEE802.1X認証VLAN方式とAXのIEEE802.1X認証(ダイナミックVLAN方式)の連動試験を実施し連携動作に問題がないことを確認しました。

2-3. 判断基準と見解(ゲートウェイ方式)

■ 判断基準

1. 正常端末は、基幹ネットワークに接続できる
2. ポリシー違反した端末は、基幹ネットワークに接続できない。
3. 隔離された端末を治療した後は、基幹ネットワークに接続できる
4. 同一ポート上で検疫対象外OS端末が認証のみで接続可能であること。
5. 認証前の端末に対してURLリダイレクトで検疫サーバへ自動的に誘導できること。

■ 見解

iNetSec Inspection Centerのゲートウェイ方式証とAXのWeb認証(固定VLAN方式)との連動試験を実施し連携動作に問題がないことを確認しました。