InfoCage PC検疫 および UNIVERGE RD1000

評価報告書

2008年12月4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

「InfoCage」、「UNIVERGE」は日本電気株式会社の登録商標です。
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(AX1200S/AX2400S)
AXシリーズ認証ソリューションガイド

目次

1-1. InfoCage PC検疫の検証結果

■概要

本資料は、日本電気株式会社製品「 InfoCage PC検疫」と、AXシリーズの認証機能を用いたシステム構築が可能かを検証し、その結果と見解及び構築のポイントを報告しています。

■検証結果一覧

InfoCage PC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				
VLANモード	認証方式	AX2430S	AX1230S	備考
固定 VLANモード	IEEE802.1X	◎	◎	1-3. 結果に対する見解① 連携動作(固定VLANモード) の判断基準を参照して下さい。
	Web認証	○	○	
	MAC認証	◎	◎	
ダイナミック VLANモード	IEEE802.1X	◎	◎	1-3. 結果に対する見解② 連携動作(ダイナミックVLANモード) の判断基準を参照して下さい。
	Web認証	○	○	
	MAC認証	○	○	

※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。
※表中の○は連係が可能ですが、一部判断基準に満たないこと示します。

1-2. UNIVERGE RD1000相互接続検証結果

■ UNIVERGE RD1000相互接続検証結果

AXシリーズがサポートしている認証方式とRADIUSサーバUNIVERGE RD1000の相互接続検証の結果一覧を以下の表に示します。

なお本検証結果はInfoCage PC検疫とは別に認証機能のみの検証を実施した結果を示します。

認証スイッチ	認証方式		VLANモード	結果
AX1230S(Ver1.4) AX2430S(Ver10.7.C)	IEEE802.1X認証 (EAP)	EAP-MD5	固定VLANモード	○
			ダイナミックVLANモード	○
		EAP-PEAP	固定VLANモード	○
			ダイナミックVLANモード	○
		EAP-TLS	固定VLANモード	○
			ダイナミックVLANモード	○
	Web認証 (PAP)		固定VLANモード	○
			ダイナミックVLANモード	○
	MAC認証 (PAP)		固定VLANモード	○
			ダイナミックVLANモード	○

※表中の○は連携動作が可能であることを示します。

※ダイナミックVLANモードではAXシリーズで使用する以下3つのRADIUSアトリビュートをUNIVERGE RD1000のリターンアトリビュートに設定しています。

- Tunnel-Private-Group-ID = VLAN番号
- Tunnel-Type = VLAN
- Tunnel-Medium-Type = 802

1-3. InfoCage PC検疫の結果に対する見解①

■ 連携動作(固定VLANモード)の判断基準

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. 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、自動的に基幹ネットワークから隔離される

■ 見解

・IEEE802.1X認証

InfoCage PC検疫との連携動作に問題が無いことを確認しました。

・Web認証

InfoCage PC検疫との連携動作の確認は出来ましたが、Web認証では定期的に再認証を行うことができないため、一度許可された端末が検疫ポリシーに違反した場合ネットワークからの排除が次回認証時となります。

・MAC認証

InfoCage PC検疫との連携動作に問題がないことを確認しました。
検疫PCのネットワーク接続排除は自動的に実施されますが、最短でAXのMAC認証最大接続時間10分となります。

1-3. InfoCage PC検疫の結果に対する見解②

■ 連携動作(ダイナミックVLANモード)の判断基準

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

■ 見解

・IEEE802.1X認証

InfoCage PC検疫との連携動作に問題が無いことを確認しました。

・Web認証

InfoCage PC検疫との連携動作の確認は出来ましたが、Web認証では定期的に再認証を行うことができないため、一度許可された端末が検疫ポリシーに違反した場合ネットワークからの排除が次回認証時となります。

またDHCP環境下ではネットワーク切り替え時に端末のIPアドレスを手動で再取得する必要があります。※1

※1…但し検疫および認証前ネットワークのDHCPサーバでIPアドレスのリース時間を短く設定すれば、検疫失敗から検疫成功時には自動的にIPアドレスの再取得を行う事が可能です。

・MAC認証

InfoCage PC検疫との連携動作の確認は出来ましたが、DHCP環境下ではネットワーク切り替え時にIPアドレスの手動切り替えが必要です。

2-1. 評価対象機器

■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。

●InfoCage PC検疫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	Windows Sever 2003	InfoCage PC検疫 検疫ポリシ管理サーバ	Ver 5.3.0.200
		InfoCage PC検疫 検疫ポリシ管理コンソール	Ver5.3.0.0
		InfoCage PC検疫 検疫コネクタ	Ver1.02.0
RADIUSサーバ	RedHat Enterprise Linux Ver4.0	UNIVERGE RD1000	Ver4.04-00. ES4
クライアントPC①	Windows Vista SP1	InfoCage PC検疫 検疫エージェント	Ver5.3.0
クライアントPC②	Windows XP SP2		

●認証スイッチ(AXシリーズ)

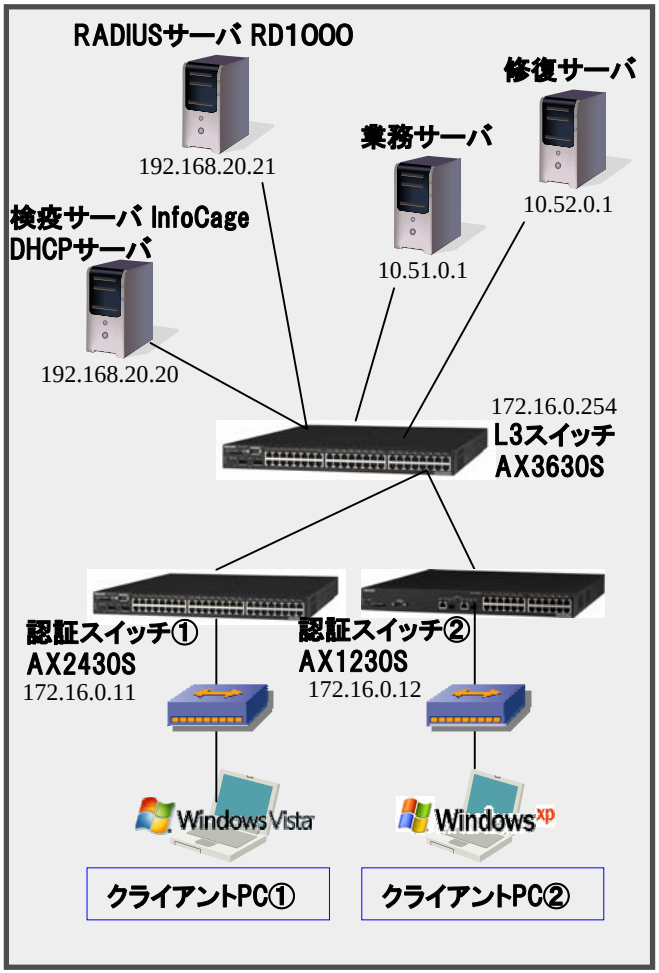
用途	機器名	バージョン
L3スイッチ	AX3630S	10.7.C
認証スイッチ①	AX2430S	10.7.C
認証スイッチ②	AX1230S	1.4

2-2. 評価構成図

■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VLAN	30	192.168.30.0/24	固定VLANモードでは使用しません。
認証前VLAN	10	192.168.10.0/24	固定VLANモードでは使用しません。

●認証前のアクセスリスト

本検証にて認証スイッチに設定する認証前アクセスリストを以下に示します。

	認証前アクセスリスト
①	permit udp src 0.0.0.0 255.255.255.255 dst 0.0.0.0 255.255.255.255 eq bootps
	クライアントPCにてIPアドレスを取得するためのDHCPパケットの通信許可。
②	permit protocol ip src 192.168.0.0 0.0.255.255 dst 192.168.20.20 0.0.0.0
	クライアントPCにて検疫を実施するための検疫サーバへのIPパケットの通信許可。
③	permit protocol ip src 192.168.0.0 0.0.255.255 dst 10.52.0.1 0.0.0.0
	クライアントPCにて修復を実施するための修復サーバへのIPパケットの通信許可。

2-3. 検疫結果によるネットワーク制御

■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。以下に固定VLANモードとダイナミックVLANモード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）

●固定VLANモード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	検疫成功	認証前アクセスリストによるアクセス制限	○	○	×
④	認証失敗	検疫失敗	認証前アクセスリストによるアクセス制限	○	○	×

●ダイナミックVLANモード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	検疫成功※1	認証前アクセスリストによるアクセス制限	10	×	×	×
④	認証失敗	検疫失敗※1	認証前アクセスリストによるアクセス制限	10	×	×	×

※1認証失敗時は検疫を実施しません。

3-1. RD1000設定のポイント(1/3)

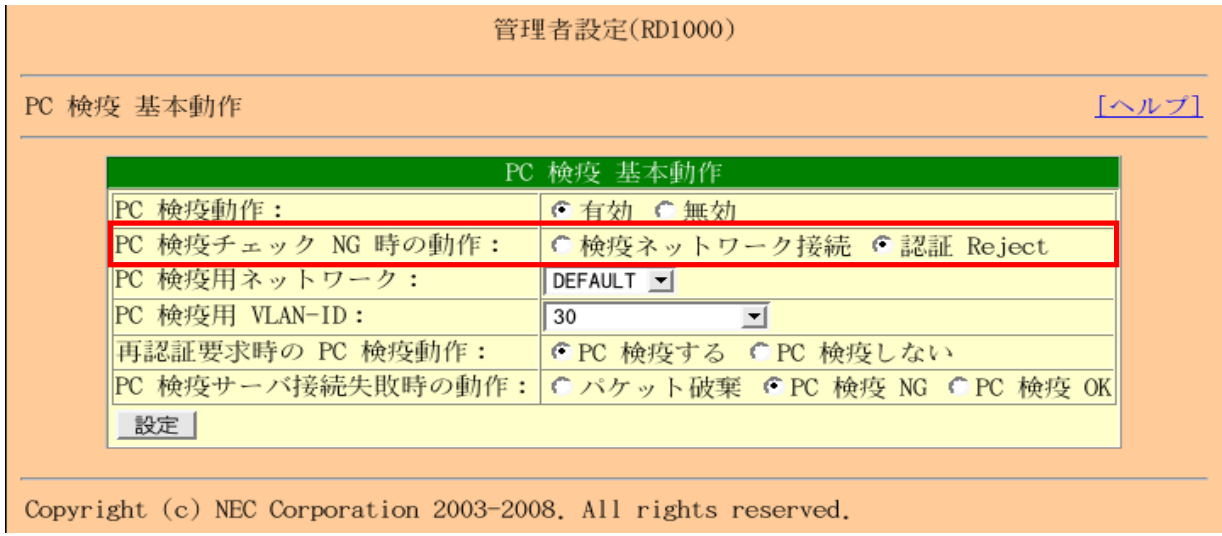
■RD1000の設定

本検疫システム(InfoCage PC検疫＋AXシリーズ)を構築する際にRD1000にて必要な設定ポイントをVLANモード毎(固定VLANモード、ダイナミックVLANモード)に示します。
なおRD1000では通常のRADIUSとして動作する設定が完了していることを前提としています。

■固定VLANモード

①PC検疫設定:基本動作

設定メニューから「PC検疫設定」→「基本動作」と展開し下記画面を表示します。
●「PC検疫動作」の項目で有効を選択し検疫を有効にします。
●下記画面赤枠内の「検疫チェックNG時の動作」項目に**「認証Reject」**を選択して下さい。



3-1. RD1000設定のポイント(2/3)

■ダイナミックVLANモード

①PC検疫設定:PC検疫用 VLAN-ID 設定

設定メニューから「PC検疫設定」→「 PC検疫用 VLAN-ID 設定」と展開し設定画面を表示します。

●認証スイッチで設定された検疫VLANの**VLAN-ID**を追加します。

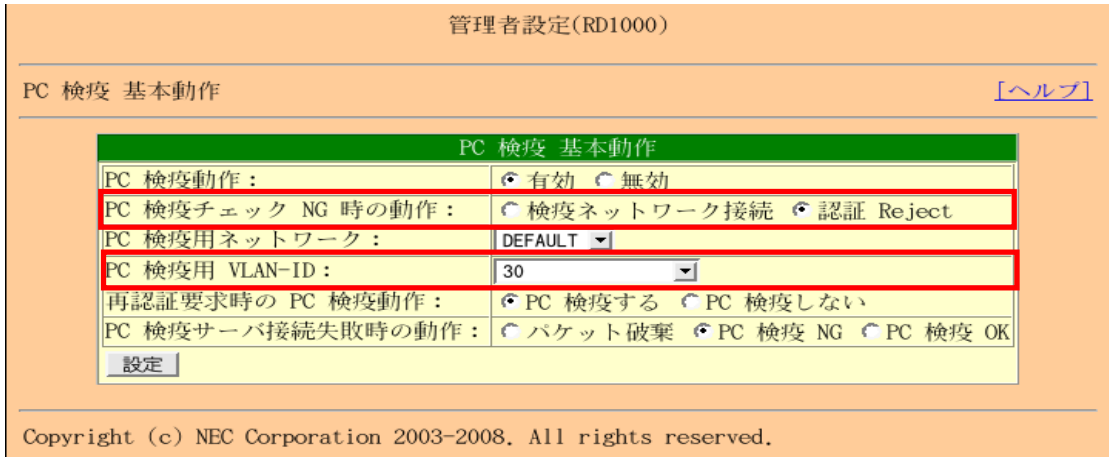
②PC検疫設定:基本動作

設定メニューから「PC検疫設定」→「基本動作」と展開し下記画面を表示します。

●「PC検疫動作」の項目で有効を選択し検疫を有効にします。

●下記画面赤枠内の「検疫チェックNG時の動作」項目に**「検疫ネットワーク接続」**を選択して下さい。

●下記画面赤枠内の「PC検疫用 VLAN-ID」項目から**「検疫VLANのID」**を選択して下さい。

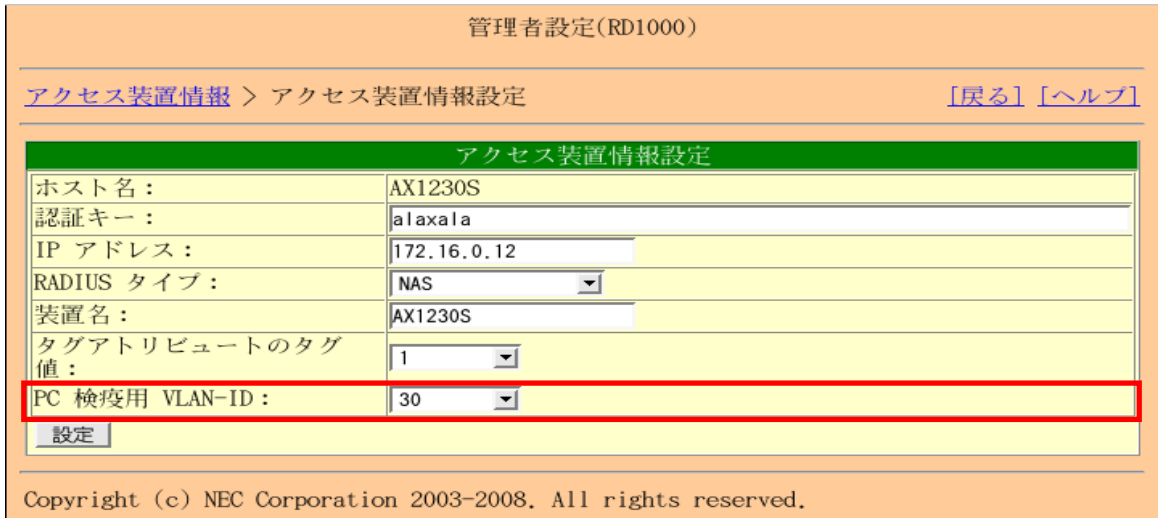


3-1. RD1000設定のポイント(3/3)

③アクセス装置情報:アクセス装置情報設定

ダイナミックVLANモードを使用した検疫システム検証の際、本構成では検疫用VLAN-IDの設定をアクセス装置（認証スイッチ）単位で設定しています。

設定メニューから「アクセス装置情報」→「アクセス装置情報設定」を展開し以下の画面を表示します。
●画面赤枠内の「PC検疫用VLAN-ID」の設定を行って下さい。



※ダイナミックVLANモード使用時の検疫VLAN-IDの指定方法について
本検証環境では③アクセス装置情報:アクセス装置情報設定のとおり、アクセス装置単位で設定しましたが、検疫VLAN-IDの指定方法は以下の2種類から選択となります。
・RADIUS単位
・アクセス装置単位（認証スイッチ）

3-2. InfoCage 設定のポイント(1/3)

■InfoCageポリシ管理サーバの設定

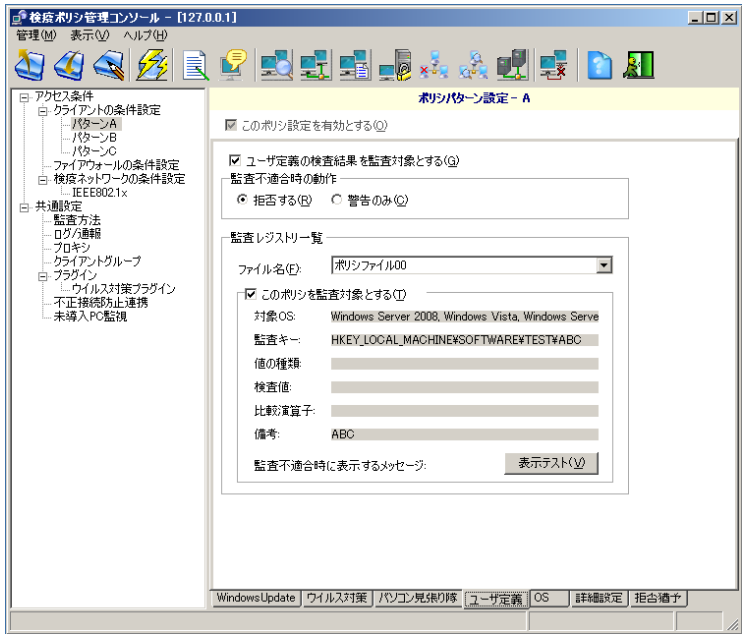
本検疫システム(InfoCage PC検疫＋AXシリーズ)を構築する際にInfoCageポリシ管理サーバにて必要な設定ポイントを以下に示します。なおInfoCageポリシ管理サーバはインストール、初期設定で完了していることが前提としています。

①ポリシーパターン設定

画面左の設定メニューから「アクセス条件」→「クライアントの条件設定」→パターンA※1を展開し下記設定画面を表示します。

(※1・・・IEEE802.1X認証使用時はパターンAのみ使用可能)

ここではクライアントを検疫する際のセキュリティポリシーを作成します。本検証では「ユーザー定義」項目にてレジストリ特定箇所のチェックを行うポリシーを作成しています。



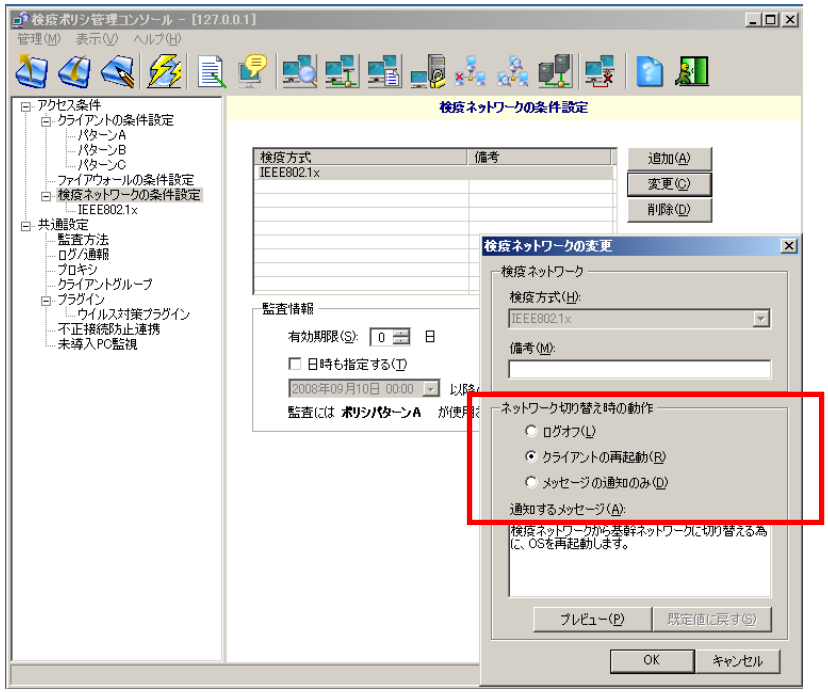
3-2. InfoCage 設定のポイント(2/3)

②ネットワーク切り替え動作の設定

ダイナミックVLANモード使用時にクライアントPCのセキュリティ状態の変化に応じて早期のネットワーク切り替えを促がす機能の設定を行います。

画面左の設定メニューから「アクセス条件」→「検疫ネットワークの条件設定」の画面にて検疫方式「IEEE802.1X」を追加し下記設定画面を表示します。

赤枠内のネットワーク切り替え時の動作を環境に応じて設定します。



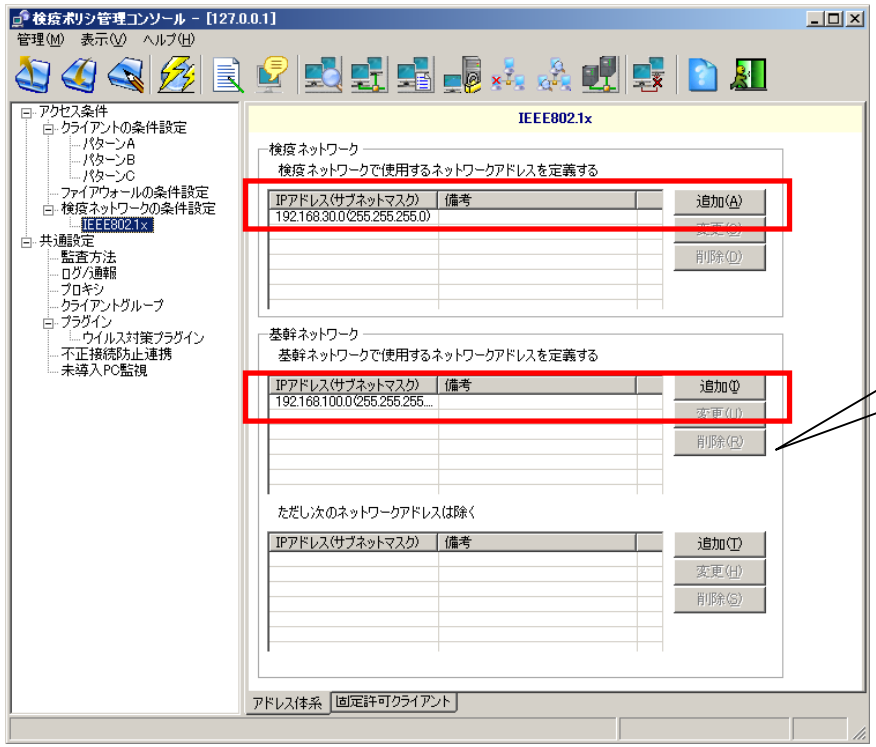
3-2. InfoCage 設定のポイント(3/3)

③ネットワークアドレスの定義

ダイナミックVLANモード使用時にクライアントPCの所属するネットワークアドレスを定義する事により検疫サーバがクライアントPCの所属ネットワークの移動を検知することができます。本設定は固定VLANモード使用時は設定しません。

場面左の設定メニューから「アクセス条件」→「検疫ネットワークの条件設定」→IEEE802.1X選択し下記の設定画面を表示して下さい。にて検疫方式「IEEE802.1X」を追加し下記設定画面を表示します。

赤枠内の設定欄に環境に応じたネットワークアドレスを設定してください。



本設定は固定VLANモード使用時は設定しません。

■AXコンフィグレーションファイル

評価に使用した各認証スイッチのコンフィグレーションファイルは以下の通りです。
AX1230Sにつきましては装置内で固定VLANモード、ダイナミックVLANモード共存可能であるためコンフィグレーションファイルは1つになります。

認証スイッチ	認証方式	コンフィグレーションファイル
AX2430S	固定VLANモード	InfoCage_AX2430S_static.txt
	ダイナミックVLANモード	InfoCage_AX2430S_dynamic.txt
AX1230S	固定VLANモード	InfoCage_AX1230S_static.txt
	ダイナミックVLANモード	InfoCage _AX1230S_dynamic.txt

※ファイル名の下のクリップをクリックするとコンフィグレーションファイルが開きます。