AX シリーズ
検疫ソリューションガイド
（QuOLA@Adapter 編）

for the Guaranteed Network

初版

はじめに

本ガイドは、日立電線ネットワークス株式会社製の QuOLA@Adapter と AX シリーズ（AX1230S / AX2430S / AX3630S / AX3640S）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シリーズ製品マニュアル（http://www.alaxala.com/jp/support/manual/index.html）
・QuOLA@Adapter マニュアル

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	Ver1.3.F
AX2430S / AX3630S / AX3640S	Ver10.7.B

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

・QuOLA@Adapterは、日立電線ネットワークス株式会社の登録商標です。
・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。
・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

- QuOLA@Adapter (Ver 1.05)
- AX1230S (Ver1.3.F)
- AX2430S (Ver10.7.B)
- AX3630S (Ver10.7.B)
- Windows XP (SP2)
- Windows Vista (SP1)
- Windows Server 2008 Standard

目次

1. QuOLA@Adapter 検疫概要

1.1. QuOLA@Adapter 検疫について

1.1.1. QuOLA@Adapter の特徴

- 検疫に特化した専用アプライアンス化で導入が容易
- Windowsセキュリティパッチリスト自動配布サービスで運用が簡単
- クライアントPCに事前の検疫エージェント（検疫ソフト）のインストール不要

1.1.2. 検疫動作概要

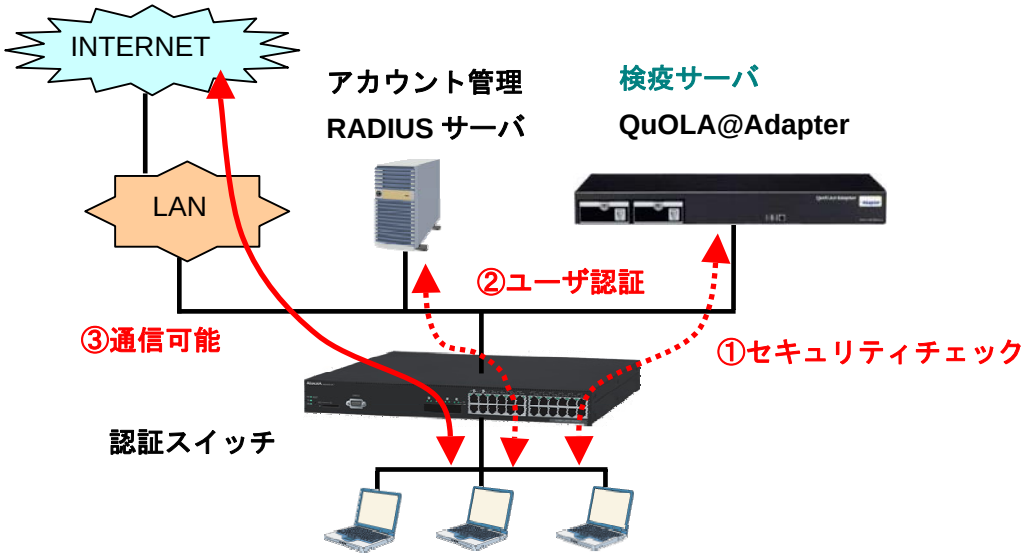


図 1.1-1 検疫システム概要

QuOLA@Adapterは検疫を行うアプライアンスサーバであり、図1.1-1で示すように認証スイッチと連携する事で、クライアントPCにソフトウエアインストール不要で検疫ネットワークを構築する事ができます。
検疫～通信の一連の流れを以下にしめします。

① セキュリティチェックはQuOLA@Adapterから検疫ソフトをダウンロードして実行
② 検疫成功後ユーザIDとパスワードを入力しユーザ認証を実施
③ 通信可能となります

検疫ソフトは検疫サーバからダウンロード時に保存することで、次回以降はQuOLA@AdapterへのWebアクセスを省略できます。また、PCのスタートアップからの実行する事ができます。検疫ソフトをWindows　ドメイン環境を利用し、ログオンスクリプトに登録することでWindowsログオン時に自動的に検疫する事も可能です。

1.1.3. QuOLA@Adapter のサポート機能

表 1.1-1 検疫機能

機能名	機能詳細
Windows セキュリティパッチチェック	Windows セキュリティパッチが適用されているかチェックする機能
ウイルス対策ソフトチェック	ウイルス対策ソフトがインストールされているかチェックする機能 パターンファイル番号がセキュリティポリシー以上かチェックする機能 ＜対応アンチウイルスソフトベンダ＞ ・TrendMicro　・Symantec　・McAfee　・F-Secure 10 世代まで遡って猶予期間を設定可能
Windows　Firewall チェック	Windows　Firewall が稼動しているかチェックする機能 ＊他ベンダー製は対象外
資産管理台帳チェック	端末が資産管理台帳登録されているかチェックする機能 （IP アドレス、MAC アドレス、コンピュータ名）
禁止ソフトチェック	端末に禁止ソフトがインストールされていないかチェックする機能

表 1.1-2 運用サポート機能

機能名	機能詳細
アンチウイルスソフトパターン番号自動更新機能	アンチウイルスソフトベンダから最新パターンファイル番号の情報を自動取得する機能 Ver2.0　より　日立電線ネットワーク（株）データセンタより配信に変更　＊）無償
Windows セキュリティパッチリスト自動取得機能	日立電線ネットワーク（株）データセンタより Windows パッチ情報を取得する機能 ＊）別途パッチリスト自動配布契約（有償）を締結する必要があります。

表 1.1-3 対応クライアント環境

項目	機能詳細
検疫可能クライアント OS	Windwos2000 Professional　SP4 以降 Windwos XP Home Editon SP2 以降 Windows XP Professional SP2 以降 Windows Vista Home Basic Windows Vista Home Premium Windows Vista Business Windows Vista Ultimate Windows Vista Enterprise
Web ブラウザ	Internet Explorer6 (Windows 2000, XP) Internet Explorer7 (Windows XP, Vista)

＊）検疫可能クライアントOSの情報はVer2.0の情報となります。

1.2. QuOLA@Adapter と AX の連携

1.2.1. QuOLA@Adapter と AX スイッチによる検疫ソリューションの特徴

（１） クライアント PC を自動的に検疫実行画面に誘導

初めてブラウザをアクセスした時に、AX スイッチの URL リダイレクト機能で自動的に検疫サーバの検疫実行画面（検疫ソフトダウンロード画面）へ誘導します。

（２） PC の検疫とユーザ認証ができる

検疫成功後にユーザ ID とパスワードを入力することで検疫とユーザ認証ができます。またはユーザ認証を行なわず検疫可否のみでアクセス制御する事も可能です。

（**ユーザ認証方式の選択**）

（３） AX スイッチの Web 認証導入済みユーザに導入が容易

AX の Web 認証と連携する場合に使用する RADIUS サーバ（認証サーバ）は、スイッチ内蔵 Web 認証データベースを含め AX の Web 認証と連携可能であれば使用可能です。

RADIUS サーバを選ばないため、QuOLA@Adapter を AX の Web 認証システムに増設するだけで簡単に既存の Web 認証システムへの検疫システムの導入が可能です。

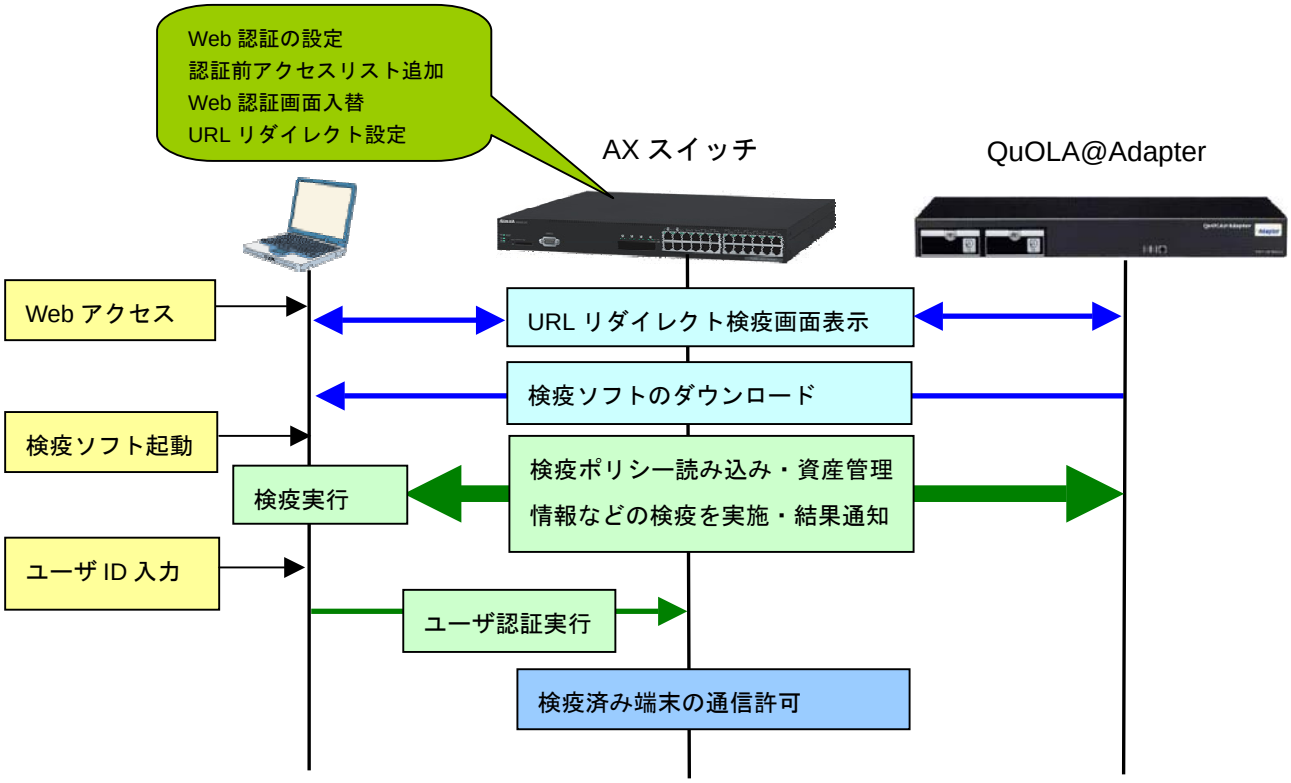
1.2.2. QuOLA@Adapter と AX スイッチの検疫動作概要

QuOLA@Adapter と AX スイッチの **Web 認証機能**を連携することで、簡単に検疫システムが構築できます。

AXスイッチには、認証前ユーザが検疫・修復するために検疫サーバと修復サーバへの認証前アクセスリストと、ユーザに事前設定無しでQuOLA@Adapter検疫画面に誘導するためにAXスイッチの認証画面入替えおよびURLリダイレクトを設定します。（詳細は 3 章を参照）

検疫前のユーザは Web ブラウザ使用時に AX の URL リダイレクト機能で QuOLA@Adapter の検疫ソフトのダウンロード画面へ自動的に誘導され、検疫ソフトをダウンロードし実行する事で検疫します。検疫成功後、ユーザ ID およびパスワードを入力すると、検疫ソフトは AX へ認証処理を開始します。

連携のシーケンスを以下に示します。



＊）ユーザの検疫ソフトのダウンロードは初回のみで次回より省略可能

図 1.2-1 QuOLA@Adapter と AX の検疫連携のしくみ

2. QuOLA@Adapter と AX シリーズの連携機能と収容条件

QuOLA@Adapter と AX シリーズで連携可能な認証方式と収容条件を示します。
本ガイドで解説している方式を赤文字で示しています。

表 2-1 連携可能なスイッチと認証方式

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

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
Web 認証	固定 VLAN	1024/装置	1024/装置
	動的 VLAN	256/装置	256/装置(*1)

(*1)AX3640Sでは 1024/装置となります。

3. 検疫ネットワークの構築

本章では、QuOLA@Adapter 検疫サーバと AX シリーズを用いた検疫ネットワークの構築例を示します。 QuOLA@Adapter 検疫と連携可能な認証方式は Web 認証方式で本例では固定 VLAN モードとの連携の例を解説します。

3.1. 概要

検疫ネットワークの基本的な構成を、以下のように定義します。

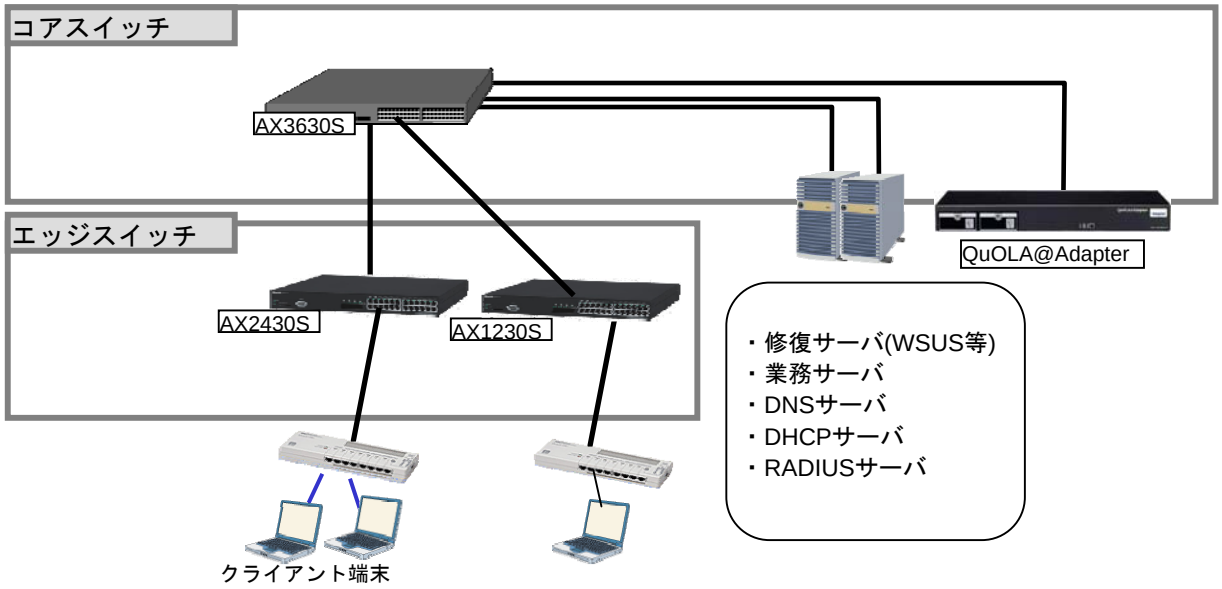


図 3.1-1 検疫ネットワークの基本構成

コアスイッチには AX3630S を配置します。QuOLA@Adapter および DNS サーバ RADIUS サーバ、検疫によりネットワークアクセスが制限された端末を治療する修復サーバ、および検疫後にアクセス可能な業務サーバを、コアスイッチ配下に接続します。

エッジスイッチには AX1230S,AX2430S を配置し、検疫を行う端末をエッジスイッチに直接またはハブを介して接続します。

本ガイドで使用した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

サーバ・端末など	詳細・アクセス制御など	IP アドレス
検疫サーバ　QuOLA@Adapter	検疫サーバのため常に通信許可とします。	192.168.1.102
RADIUS サーバ	AX スイッチと接続可能な RADIUS サーバであれば連携可能。	192.168.1.10
DNS サーバ	名前解決するため DNS の通信を許可します。	192.168.1.11
DHCP サーバ	DHCP で IP アドレス配布を行います。	192.168.1.12
修復サーバ	ウイルス対策ソフト等のダウンロード用サーバであり常に通信可能とします。	192.168.1.103
業務サーバ	ファイル共有サーバ等	192.168.200.1
クライアント端末	Windows XP Windows Vista	DHCP

3.2. 認証ネットワーク構成図

基本的な検疫ネットワーク構成例を以下に示します。

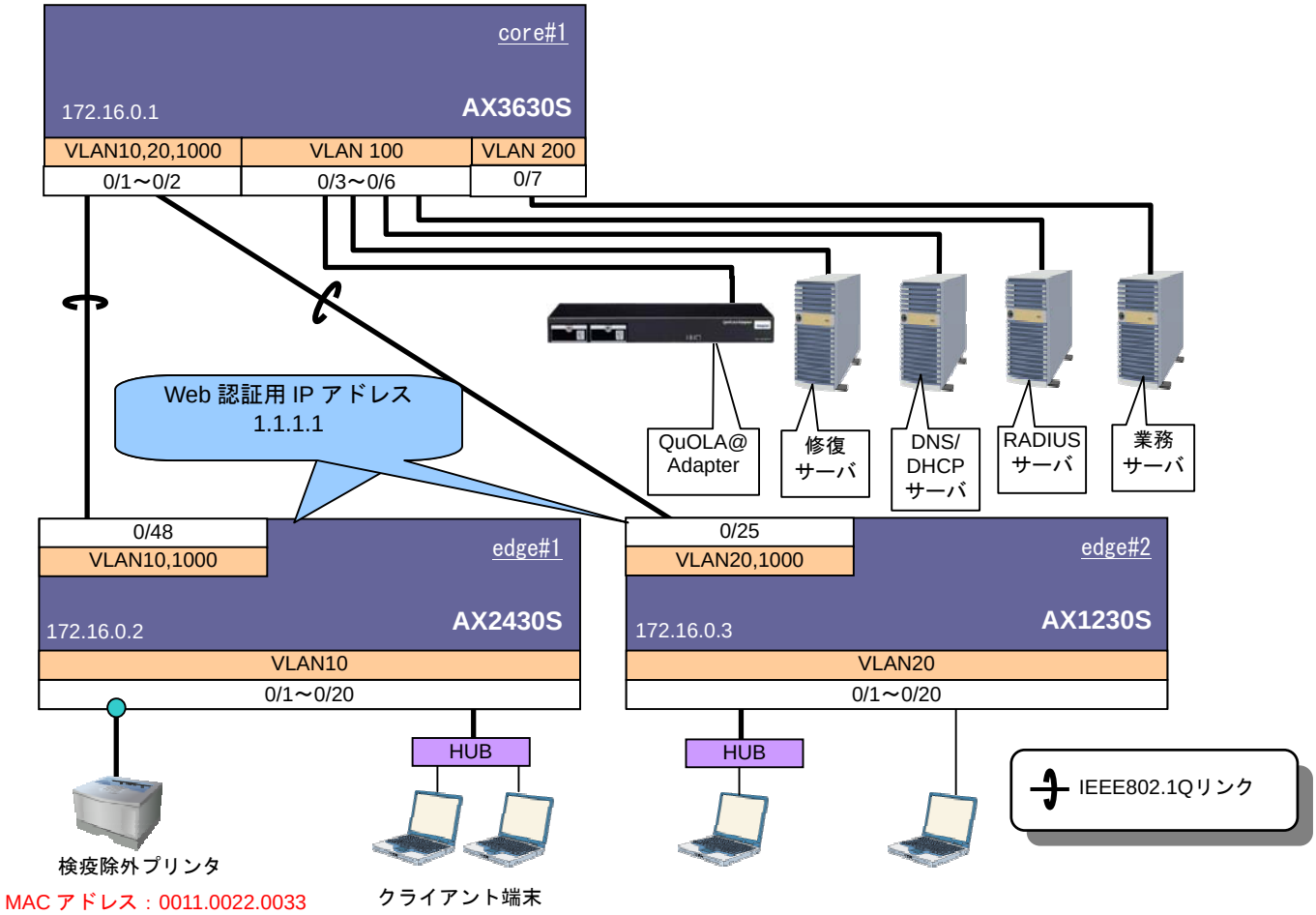


図 3.2-1 検疫ネットワーク構成図

各 VLAN の定義および端末とサーバ間通信の可否を以下の表に示します。

表 3.2-1 VLAN の定義

VLAN 名	VLAN ID	ネットワーク IP アドレス	用途
ネットワーク管理サーバ用 VLAN (ネットワーク管理)	100	192.168.1.0/24	ネットワーク管理用のサーバとして検疫サーバ等を配置する VLAN
業務用サーバ VLAN	200	192.168.200.0/24	業務用のサーバを配置する VLAN
ユーザが所属する VLAN1（AX2430S）	10	192.168.10.0/24	AX2430S 配下の端末が所属する VLAN
ユーザが所属する VLAN2（AX1230S）	20	192.168.20.0/24	AX1230S 配下の端末が所属する 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 端末ーサーバ間通信の可否

	業務サーバ	DNS サーバ	修復サーバ	検疫サーバ
検疫成功	○	○	○	○
検疫失敗	×	○	○	○

3.3. 構築ポイント

QuOLA@Adapter 検疫と AX の Web 認証方式（固定 VLAN モード）との連携において、構築の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、直接クライアント端末からスイッチへの Web 認証操作をできないようにします。

スイッチへの認証は QuOLA@Adapter の検疫ソフトが検疫チェックで成功した場合に自動的に実行されユーザは意識しません。

画面入れ替えに関しては　（画面入替え詳細は**3.5**章参照）

（２） URL リダイレクト機能を有効にする

（１）で示す画面入れ替えと URL リダイレクト機能を併用する事で検疫前のクライアントが http アクセスを実行した場合自動的に下記に示す QuOLA@Adapter の検疫ソフトのダウンロード画面へジャンプするようにします。

デフォルトの https モードでは証明書エラーが出ますので、リダイレクトモードを http に変更します。

（３） Web 認証用ポートにフィルタを設定する。

ポートに Web 認証の設定を行うと、そのポートでは認証前のすべての通信を遮断します。認証（検疫）前に通信を行いたい場合は、アクセスリストを作成してポートに適用する必要があります。また、ARP リレーの設定も必要です。

本ガイドでは、次のアクセスリストを作成して、Web 認証ポートに適用しています。

(a) DHCP 通信を許可する

(b) DNS サーバ「192.168.1.11」への DNS 通信を許可する

(c)検疫サーバ(QuOLA@Adapter)「192.168.1.102」への通信を許可する

(d)修復サーバ「192.168.1.103」への通信を許可する

（４） Web 認証専用 IP アドレスを設定する。

Web 認証用の IP アドレスを設定します。この IP アドレスは同一の検疫サーバ（QuOLA@Adapter）配下で動作する AX 全認証スイッチで共通の IP アドレスを設定して下さい。この例では、「1.1.1.1」としています。

また、クライアント用 VLAN のインタフェース IP アドレス設定が必要です。この例では、クライアント用 VLAN の IP アドレスをそれぞれ以下のように設定しています。

VLAN10：192.168.10.3　（AX2430S）

VLAN20：192.168.20.3　（AX1230S）

（５） 検疫未対応端末への対応

QuOLA@Adapter で検疫できない端末、例えばプリンタや Linux 端末等を接続する場合は MAC 認証を設定するかスイッチに端末の MAC アドレスを登録してください。

（６） デフォルトルートを設定する。

認証スイッチが RADIUS サーバ等と通信できるようにするためにデフォルトルートを設定します。

（７） RADIUS サーバを設定する。

認証スイッチが使用する RADIUS サーバを設定します。複数指定で RADIUS サーバを冗長化する事も可能です複数指定した場合は設定順に優先されます。

QuOLA@Adapter の検疫との連動では内蔵データベースでも可能ですが本例では RADIUS を用います。

（８） 最大接続時間を設定する。

Web 認証の最大接続時間はデフォルト 1 時間となっていますので、通信中であっても最大接続時間経過後に認証が解除されてしまいますので変更が必要です。少なくともユーザに 1 日 1 回は検疫を実行するポリシーとするため、最大接続時間を 1 日（1440 分）に変更します。

3.4. AX の設定

3.4.1. AX1230S のコンフィグレーション

AX1230S の設定例を示します。

（１） 事前設定

AX1230S 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	フィルタ機能と固定 VLAN モードを使用するため、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） 基本設定

AX1230S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 20,1000** **(config-vlan)# state active**	VLAN1 は使用しないため、無効にします。 クライアント用 VLAN として VLAN20 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	
●クライアント側 **(config)# interface range fastethernet 0/1-20** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 20**	ポート 0/1～0/20 を、アクセスポートとして設定します。 アクセスポートに VLAN20 を設定します。
●上位スイッチとの通信用 **(config)# interface gigabitethernet 0/25** **(config-if)# switchport mode trunk** **(config-if)# switchport trunk allowed vlan 20,1000**	ポート 0/25 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 VLAN20 および 1000 を設定します。
インタフェースの設定	
(config)# interface vlan 20 **(config-if)# ip address 192.168.20.3 255.255.255.0** **(config)# interface vlan 1000** **(config-if)# ip address 172.16.0.3 255.255.255.0**	VLAN20 および 1000 にインタフェース IP アドレスを設定します。
デフォルトルートの設定	
(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.1	検疫用 VLAN と通信を行うため、デフォルトルートを設定します。 ➢ **構築ポイント（６）**
RADIUS サーバの設定	
(config)# radius-server host 192.168.1.10 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定します。この例ではキーを「alaxala」としています。

（３） Web 認証の設定

AX1230S の設定	
Web 認証用アクセスリストの設定	
(config)# ip access-list extended web-auth **(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 192.168.1.11 0.0.0.0 eq domain** **(config-ext-nacl)# permit protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.1.102 0.0.0.0** **(config-ext-nacl)# permit protocol ip src 0.0.0.0 255.255.255.255 dst 192.168.1.103 0.0.0.0**	以下のアクセスリストを作成します。 ・DHCP通信を許可する。 ・DNSサーバ「192.168.1.11」へのDNS通信を許可する。 ・検疫サーバ「192.168.1.102」との通信を許可する。 ・修復サーバ「192.168.1.103」との通信を許可する。 ➢ **構築ポイント（３）**
物理ポートの設定	
(config)# interface range fastethernet 0/1-20 **(config-if-range)# web-authentication port** **(config-if-range)# authentication arp-relay** **(config-if-range)# authentication ip access-group web-auth**	ポート 0/1～0/20 を Web 認証対象ポートとして設定します。 認証前の端末から送信される他宛て ARP パケットを認証対象外のポートへ出力させます。 認証用アクセスリストを適用します。 ➢ **構築ポイント（３）**
RADIUS の設定	
(config)# aaa authentication web-authentication default group radius	RADIUS サーバでユーザ認証を行うことを設定します。
Web 認証(固定 VLAN)の設定	
(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。本ガイドでは「1.1.1.1」としています。 ➢ **構築ポイント（４）**
(config)# web-authentication redirect-mode http	リダイレクトモードを「http」に指定します。 ➢ **構築ポイント（２）**
(config)# web-authentication system-auth-control	Web 認証を有効にします。
(config)# web-authentication max-timer 1440	認証成功後の最大接続時間を **1440 分(1 日)**に設定します。 ➢ **構築ポイント（８）**

3.4.2. AX2430S のコンフィグレーション

AX2430S の設定例を示します。

（１） 基本設定

AX2430S 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。 クライアント用 VLAN として VLAN10 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	
●クライアント側 **(config)# interface range gigabitethernet 0/1-20** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 10**	ポート 0/1～0/20 を、アクセスポートとして設定します。 アクセスポートに VLAN10 を設定します。
●上位スイッチとの通信用 **(config)# interface gigabitethernet 0/48** **(config-if)# switchport mode trunk** **(config-if)# switchport trunk allowed vlan 10,1000**	ポート 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 VLAN10 および 1000 を設定します。
インタフェースの設定	
(config)# interface vlan 10 **(config-if)# ip address 192.168.10.3 255.255.255.0** **(config)# interface vlan 1000** **(config-if)# ip address 172.16.0.2 255.255.255.0**	VLAN10 および 1000 にインタフェース IP アドレスを設定します。
デフォルトルートの設定	
(config)# ip default-gateway 172.16.0.1	検疫用 VLAN と通信を行うため、デフォルトルートを設定します。 ➢ **構築ポイント（６）**
RADIUS サーバの設定	
(config)# radius-server host 192.168.1.10 key alaxala	RADIUS サーバの IP アドレスおよびキーを設定します。この例ではキーを「alaxala」としています。

（２） Web 認証の設定

AX2430S の設定	
Web 認証用アクセスリストの設定	
(config)# ip access-list extended web-auth **(config-ext-nacl)# permit udp any any eq bootps** **(config-ext-nacl)# permit udp any host 192.168.1.11 eq domain** **(config-ext-nacl)# permit ip any host 192.168.1.102** **(config-ext-nacl)# permit ip any host 192.168.1.103**	以下のアクセスリストを作成します。 ・DHCP通信を許可する。 ・DNSサーバ「192.168.1.11」へのDNS通信を許可する。 ・検疫サーバ「192.168.1.102」への通信を許可する。 ・修復サーバ「192.168.1.103」への通信を許可する。 ➢ **構築ポイント（３）**
物理ポートの設定	
(config)# interface range gigabitethernet 0/1-20 **(config-if-range)# web-authentication port** **(config-if-range)# authentication arp-relay** **(config-if-range)# authentication ip access-group web-auth**	ポート 0/1～0/20 を Web 認証対象ポートとして設定します。 認証前の端末から送信される他宛て ARP パケットを認証対象外のポートへ出力させます。 認証用アクセスリストを適用します。 ➢ **構築ポイント（３）**
RADIUS の設定	
(config)# aaa authentication web-authentication default group radius	RADIUS サーバでユーザ認証を行うことを設定します。
Web 認証(固定 VLAN)の設定	
(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。本ガイドでは「1.1.1.1」としています。 ➢ **構築ポイント（４）**
(config)# web-authentication redirect-mode http	リダイレクトモードを「http」に指定します。 ➢ **構築ポイント（２）**
(config)# web-authentication system-auth-control	Web 認証を有効にします。
(config)# web-authentication max-timer 1440	認証成功後の最大接続時間を **1440 分(1 日)**に設定します。 ➢ **構築ポイント（８）**

3.4.3. AX3630S のコンフィグレーション

AX3630S の設定例を示します。

（1） 基本設定

AX3630S の設定	
ポート VLAN の設定	
(config)# vlan 1 **(config-vlan)# state suspend** **(config)# vlan 10,20,1000** **(config-vlan)# state active** **(config)# vlan 100,200** **(config-vlan)# state active**	VLAN1 は使用しないため、無効にします。 クライアント用 VLAN として VLAN10 および 20 を、管理用 VLAN として VLAN1000 を作成します。 サーバ用 VLAN として VLAN100 および 200 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 trunk** **(config-if-range)# switchport trunk allowed vlan 10,20,1000** **(config)# interface range gigabitethernet 0/3-6** **(config-if-range)# switchport mode access** **(config-if-range)# switchport access vlan 100** **(config)# interface gigabitethernet 0/7** **(config-if)# switchport mode access** **(config-if)# switchport access vlan 200** **(config)# interface range gigabitethernet 0/1-4** **(config-if-range)# media-type rj45**	ポート 0/1～0/2 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 VLAN10、20 および 1000 を設定します。 ポート 0/3～0/6 を、アクセスポートとして設定します。 アクセスポートに VLAN100 を設定します。 ポート 0/7 を、アクセスポートとして設定します。 アクセスポートに VLAN200 を設定します。 ポート 0/1～0/4 にメディアタイプを設定します。
インタフェースの設定	
(config)# interface vlan 10 **(config-if)# ip address 192.168.10.254 255.255.255.0** **(config)# interface vlan 20** **(config-if)# ip address 192.168.20.254 255.255.255.0** **(config)# interface vlan 100** **(config-if)# ip address 192.168.1.254 255.255.255.0** **(config)# interface vlan 200** **(config-if)# ip address 192.168.200.254 255.255.255.0** **(config)# interface vlan 1000** **(config-if)# ip address 172.16.0.1 255.255.255.0**	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。

（２） DHCP リレーの設定

AX3630S の設定	
DHCP リレーの設定	
(config)# interface vlan 10 **(config-if)# ip helper-address 192.168.1.12** **(config)# interface vlan 20** **(config-if)# ip helper-address 192.168.1.12**	VLAN10 および 20 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. 認証画面入替え

QuOLA@Adapter と連携する場合は AX スイッチの認証画面（login.html）を入替えます。

認証用の HTML ファイルには QuOLA@Adapter の検疫画面への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。


login.html

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」して編集してください。

編集個所は、添付ファイルの“xx.xx.xx.xx”と書いてある部分をエディタ等で検疫サーバの IP アドレスに書換えて SD または FTP でスイッチへファイル転送後に以下のコマンドで適用して下さい。

```
set web-authentication html-files <directory> -f
```

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。

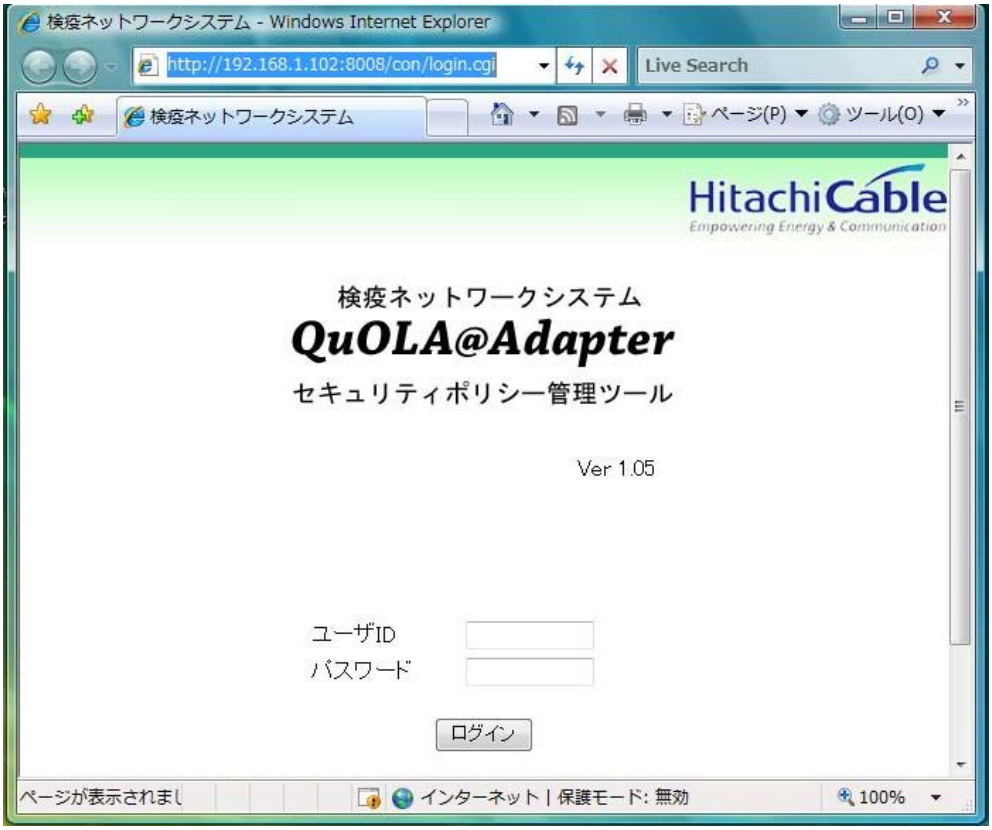
AX2400S、AX3600S
mkdir　<directory name>

AX1200S
mkdir ramdisk <directory name>

3.6. QuOLA@Adapter の設定

3.6.1. QuOLA@Adapter へのログイン

QuOLA@Adapter へログインする場合は http://QuOLA@Adapter の IP 又は HOST 名 /con/login.html にアクセスします。



3.6.2. 認証スイッチの設定

QuOLA@Adapter と連携するスイッチの設定をします。

（１） ユーザ認証方式の選択

認証スイッチの共通設定

共通 ID　：　QuOLA@Adapter の検疫のみでネットワークアクセス制御する場合に選択します。システムとする場合スイッチに**共通 ID** で認証します。
共通 ID 選択時は**共通ユーザ名**及び**パスワード**を設定します。

個別 ID　：　QuOLA@Adapter の検疫とユーザ認証を組み合わせて実施したい場合は**個別 ID** を選択します。検疫成功後にユーザ ID、パスワード入力を求めます。

（２） 使用スイッチの設定

使用スイッチに AlaxalA を選択します。

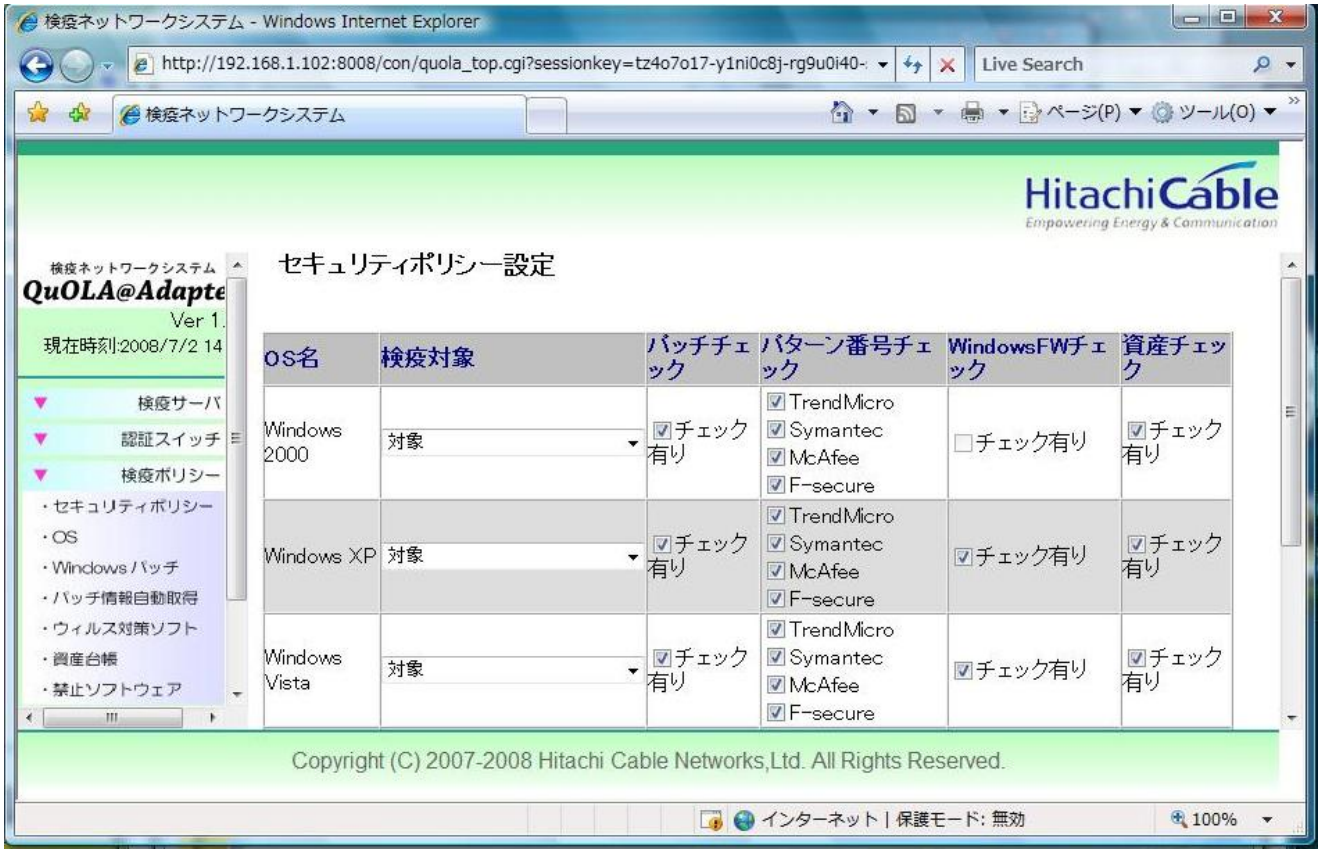
（３） AX スイッチの設定

AX スイッチの認証の設定は以下を設定します。

認証解除 URL： http:/1.1.1.1/cgi-bin/Login.cgi (認証 IP が 1.1.1.1 の場合)
認証成功文字列： Login success
認証失敗文字列： Authentication reject

3.6.3. 検疫項目の設定

検疫ポリシーからセキュリティポリシーを選択し、検疫対象とする項目をチェックします。



その他に　資産登録、禁止ソフトの登録、ウイルス対策ソフトの設定、OS セキュリティパッチ登録、することができます詳細は QuOLA@Adapter のマニュアルで確認して下さい。

4. ユーザの検疫実施方法

（1） 検疫実行 URL にアクセスする。

URL ： http://**QuOLA@Adapter 検疫サーバ名または IP アドレス**/sec/download.cgi

＊ AX スイッチで URL リダイレクトを設定している場合は検疫前のユーザを自動的に QuOLA@Adapter の検疫 URL へ誘導します。

（２） 検疫ソフトのダウンロード

開始をクリックするとアプリケーションのダウンロード又は実行を聞いてきます
実行するか保存して実行してください。

＊１） 「保存する」を選択した場合ファイル名の変更はしないで下さい。
変更した場合検疫サーバへ接続できなくなります。

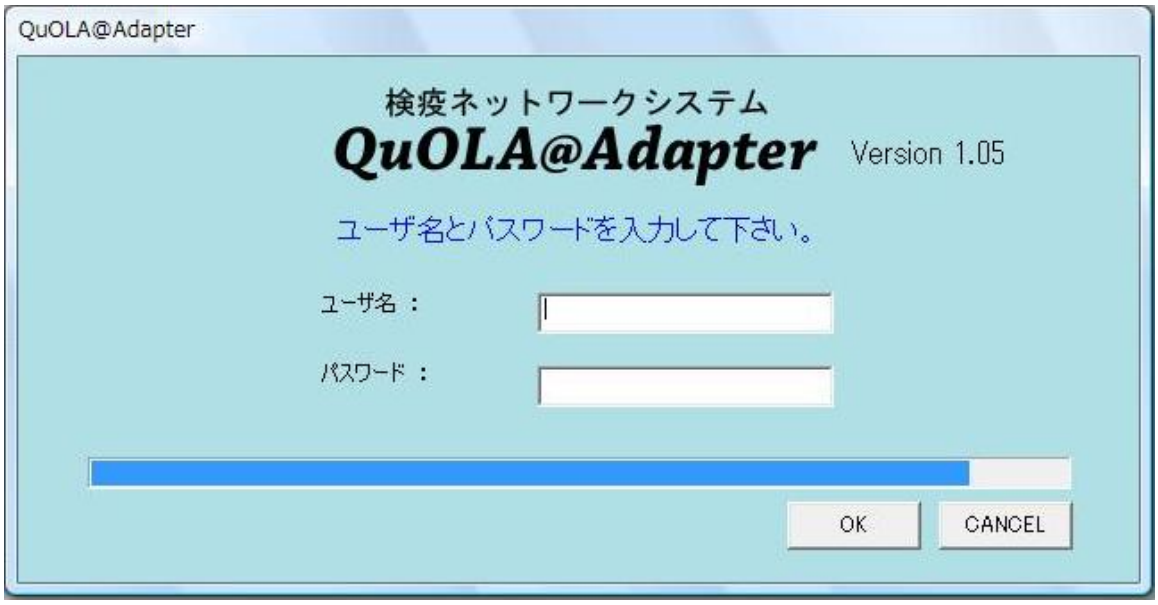
＊２） 保存を選んだ場合ダウンロードは毎回実施する必要はありません。

（３） 検疫実行

ダウンロードした検疫アプリケーションを実行します。

（４） 検疫実行

ダウンロードしたファイルを実行すると検疫実行中の表示後、検疫が合格すると、個別 ID でユーザ認証する場合にはユーザ名、パスワードを求めてきます。
入力後 AX スイッチへ認証が実行されネットワークが使用可能となります。
（共通 ID で認証する場合はユーザ名と入力は省略されネットワーク使用可能となります）



（５） 検疫失敗

検疫失敗時の例を下記に示します。

セキュリティ違反時は対策後　検疫アプリケーションを再起動してください。

5. 注意事項

5.1. 検疫除外端末

検疫サポート外の機器を接続する場合には、AX スイッチの検疫実施ポートに MAC 認証を設定するか、コンフィグレーションで MAC アドレスを登録して通信許可してください。

5.2. ログアウトに関する注意事項

認証モードによりログアウト条件が異なるため注意下さい。

5.2.1. 固定 VLAN モードの Web 認証のログアウト条件

固定 VLAN モードで Web 認証した端末は、以下のいずれかの条件に一致した場合、ログアウト（通信非許可状態）します。

条件１：ログイン画面からログアウトした場合。（QuOLA@Adapter 連携では使用不可）
条件２：最大接続時間を超えた場合。（デフォルト 3600 秒）
　　コンフィグレーションによって時間と機能の有効無効化ができます。
条件３：認証済み端末の接続監視機能によるログアウト
　　ARP パケットを用いて ARP 返答パケットを受信することにより接続監視を行ないます。
　　コンフィグレーションによって監視時間の設定変更が可能です。
　　監視時間の初期値は 5 分ごとに監視を行い、無応答の場合 1 秒×3 回リトライし、
　　無応答の場合切断します。
条件４：認証ポートのリンクダウン
条件５：強制ログアウトコマンドによるログアウト
条件６：特殊 ping によるログアウト
　　（認証用 IP アドレス宛て、コンフィグレーションで指定した TOS、TTL 値の ping）

5.2.2. 動的 VLAN モードの Web 認証のログアウト条件

動的 VLAN モードで Web 認証した端末は、以下のいずれかの条件に一致した場合、ログアウト（通信非許可状態）します。

条件１：ログイン画面からログアウトした場合。（QuOLA@Adapter 連携では使用不可）
条件２：端末の MAC アドレスが MAC アドレステーブルから削除されて約 10 分経過した場合。
（コンフィグレーションで監視機能を無効にする事が可能）

MAC アドレステーブルクリア条件
1．MAC アドレステーブルのエージング時間（デフォルト 300 秒）にパケット通信が無い時
2．学習インタフェースのリンクダウン時
3．スパニングツリーやリングのトポロジーチェンジ時

条件３：最大接続時間を超えた場合。
ログインしてから強制ログアウトされる時間のデフォルト値は 3600 秒です。
本機能はコンフィグレーションコマンドにて無効にすることができます。
条件４：強制ログアウトコマンドによるログアウト

付録A. コンフィグレーション

3.2のネットワーク構成図における各装置の全コンフィグレーションを、テキスト形式の添付ファイルで示します。各コンフィグレーションを参照する場合は、以下に示すファイル名と同じ名前の添付ファイルを開いてください。

A.1. AX3630S のコンフィグレーション

core1-AX3630S.txt

A.2. AX2430S のコンフィグレーション

edge1-AX2430S.txt

A.3. AX1230S のコンフィグレーション

edge2-AX1230S.txt

2008 年 9 月 3 日　初版発行

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
http://www.alaxala.com/