



初版

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



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(<u>http://www.alaxala.com/jp/support/manual/index.html</u>)
- ・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.	QuOL	A@Adapter検疫概要	5
	1.1. Qi	uOLA@Adapter検疫について	5
	1.1.1.	QuOLA@Adapterの特徴	5
	1.1.2.		5
	1.1.3.	QuOLA@Adapterのサポート機能	6
	1.2. Qu	uOLA@AdapterとAXの連携	7
	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	7
	1.2.2.	QuOLA@AdapterとAXスイッチの検疫動作概要	8
2.	QuOL	A@Adapter とAXシリーズの連携機能と収容条件	9
3.	検疫ネ	ットワークの構築	10
:	3.1. 概	要	10
	3.2. 認	証ネットワーク構成図	12
	3.3. 構	築ポイント	13
	3.4. AX	〈の設定	15
	3.4.1.	AX1230Sのコンフィグレーション	15
	3.4.2.	AX2430Sのコンフィグレーション	17
	3.4.3.	AX3630Sのコンフィグレーション	19
	3.5. 認	証画面入替え	21
	3.6. Qi	uOLA@Adapterの設定	22
	3.6.1.	QuOLA@Adapterへのログイン	22
	3.6.2.	認証スイッチの設定	22
	3.6.3.	検疫項目の設定	25
4.	ユーザ	の検疫実施方法	26
5.	注意事	項	29
į	5.1. 検	疫除外端末	29
ļ	5.2. 🗆	グアウトに関する注意事項	29
	5.2.1.	固定VLANモードのWeb認証のログアウト条件	
	5.2.2.	動的VLANモードのWeb認証のログアウト条件	
付	禄A.	コンフィグレーション	31
	ዓ.1. Aን	X3630Sのコンフィグレーション	31
1	Α.2. A>	×2430Sのコンフィグレーション	31
	4.3. AX	×1230Sのコンフィグレーション	31

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	固定 VLAN	—	—	—
認証	動的 VLAN	—	—	—
MAC 認証	固定 VLAN	—	—	—
	動的 VLAN	—	—	—
Web 認証	固定 VLAN	0	0	
	動的 VLAN	0	0	

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 1	サーバとク	ライア	ントー	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	192.168.1.10
	であれば連携可能。	
DNS サーバ	名前解決するため DNS の通信を許可しま	192.168.1.11
	す。	
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	192.168.1.103
	ーバであり常に通信可能とします。	
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	DHCP
	Windows Vista	

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	100	192.168.1.0/24	ネットワーク管理用のサーバと
サーバ用 VLAN			して検疫サーバ等を配置する
(ネットワーク管理)			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	10	192.168.10.0/24	AX2430S 配下の端末が所属する
VLAN1 (AX2430S)			VLAN
ユーザが所属する	20	192.168.20.0/24	AX1230S 配下の端末が所属する
VLAN2 (AX1230S)			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-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	0	0	0	0
検疫失敗	×	0	0	0

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。

後疫ネットワークシステム - Windows Internet Explorer		
C C C A thtp://192.168.1.102:8008/sec/download.cgi	• 47 X Live Search	₽ • »
☆ ☆	û ▼ ⊠ * ₩ * ⊡ ページ(P) ▼ (》ツール(0) ▼
	HitachiC Empowering Energy & U	Communication
検疫ネット5 QuOLA @	o-99274 Adapter	E
下記のボタンをクリックし、セキ:	ュリティチェックを実行して下さい	
セキュリティチェ 開始	99 	
<mark>管理者からのメッセージ</mark> セキュリティチェックを実行しなければネットワ	ークに接続することは出来ません。	
【********グルーフからのメッセージ】 ウィルス対策ソフトのパターンファイルの更新	(はこまめに!	-
	インターネット 保護モード: 無効	€ 100% ▼

(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	フィルタ機能と固定 VLAN モードを使用する
extended-authentication	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	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config)# vlan 20,1000	クライアント用 VLAN として VLAN20 を、管
(config-vlan)# state active	理用 VLAN として VLAN1000 を作成します。
スパニンクツリーの設定	
(config)# spanning-tree disable	スパニングツリーを無効にします。
●ソフコブノド側 (config)# interface range fastethernet 0/1-20	ポート 0/1~0/20 を アクセスポートとして設
(config_if_range)# switchport mode access	ホートの100/20 を、アノビスホートとして設
(config-if-range)# switchport access vian 20	アクセスポートに VIAN20 を設定します。
●上位スイッチとの通信用	
(config)# interface gigabitethernet 0/25	ポート 0/25 を、上位スイッチと通信するトラ
(config-if)# switchport mode trunk	ンクポートとして設定します。
(config-if)# switchport trunk allowed vlan 20,1000	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 vian 20	VLAN20 およひ 1000 にインタフェース IP ア
(config-if)# ip address 192.168.20.3 255.255.255.0	トレスを設定します。
(config)# interface vian 1000	
(conng-n)# ip address 172.10.0.5 255.255.255.0	
デフォルトルートの設定	
(config)# in route 0.0.0.0.0.0.0.172.16.0.1	検疫田 VIAN 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	RADIUS サーバの IP アドレスおよびキーを設
alaxala	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	以下のアクセスリストを作成します。
(config-ext-nacl)#permit udp src 0.0.0.0	・DHCP通信を許可する。
255.255.255.255 dst 0.0.0.0 255.255.255.255 eq	・DNSサーバ「192.168.1.11」へのDNS通信を
bootps	許可する。
(config-ext-nacl)# permit udp src 0.0.0.0	・検疫サーバ「192.168.1.102」との通信を許
255.255.255.255 dst 192.168.1.11 0.0.0.0 eq domain	可する。
(config-ext-nacl)# permit protocol ip src 0.0.0.0	・修復サーバ「192.168.1.103」との通信を許
255.255.255.255 dst 192.168.1.102 0.0.0	可する。
(config-ext-nacl)# permit protocol ip src 0.0.0.0	▶ 構築ボイント(3)
255.255.255.255 dst 192.168.1.103 0.0.0.0	
物理ボートの設定	
(config)# interface range fastethernet 0/1-20	ポート 0/1~0/20 を Web 認証対象ポートとし
(config-if-range)# web-authentication port	て設定します。
(config-if-range)# authentication arp-relay	認証前の端末から送信される他宛て ARP バ
	ケットを認証対家外のホートへ出力させます。
(config-if-range)# authentication ip access-group	認証用アクセスリストを適用します。
web-auth	> 博楽小1 ノト (3)
RADIUS の設定	
(config)# aga authentication web-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
deladit group facius	定します。
Web 認証(固定 VLAN)の設定	定します。
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1	定します。 Web 認証専用 IP アドレスを設定します。本ガ
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1	定します。
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1	定します。 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」としています。 ▶ 構築ポイント(4)
web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http	定します。 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」としています。 ▶ 構築ポイント(4) リダイレクトモードを「http」に指定します。
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http	定します。 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」としています。 ▶ 構築ポイント(4) リダイレクトモードを「http」に指定します。 ▶ 構築ポイント(2)
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http (config)# web-authentication system-auth-control	 定します。 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」としています。 構築ポイント(4) リダイレクトモードを「http」に指定します。 構築ポイント(2) Web 認証を有効にします。
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http (config)# web-authentication system-auth-control	定します。 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」としています。 > 構築ポイント(4) リダイレクトモードを「http」に指定します。 > 構築ポイント(2) Web 認証を有効にします。
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http (config)# web-authentication system-auth-control (config)# web-authentication max-timer 1440	 定します。 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」としています。 構築ポイント(4) リダイレクトモードを「http」に指定します。 構築ポイント(2) Web 認証を有効にします。 認証成功後の最大接続時間を 1440 分(1 日)に
Web 認証(固定 VLAN)の設定 (config)# web-authentication ip address 1.1.1.1 (config)# web-authentication redirect-mode http (config)# web-authentication system-auth-control (config)# web-authentication max-timer 1440	 定します。 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」としています。 構築ポイント(4) リダイレクトモードを「http」に指定します。 構築ポイント(2) Web 認証を有効にします。 認証成功後の最大接続時間を 1440 分(1 日)に 設定します。

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	VLAN1 は使用しないため、無効にします。
(config-vlan)# state suspend	
(config)# vlan 10,1000	クライアント用 VLAN として VLAN10 を、管
(config-vlan)# state active	理用 VLAN として VLAN1000 を作成します。
フパニングッリーの設定	
<u> へハーンゲンゲーの設定</u> (config)# spanning tree disable	フパニングツリーを無効にします
(conng)# spanning-tree disable	スパーンググ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	ポート 0/1~0/20 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 10	アクセスポートに VLAN10 を設定します。
●上位フィッチトの運信田	
●エゼスイッチとの通信用 (config)# interface gigsbitethernet 0/48	ポート 0/48 を 上位スイッチと通信するトラ
(config-if)# switchport mode trunk	ハードのもので、エロハイノアと通信するトノ ンクポートとして設定します。
(config-if)# switchport trunk allowed vlan 10.1000	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	VLAN10 および 1000 にインタフェース IP ア
(config-if)# ip address 192.168.10.3 255.255.255.0	ドレスを設定します。
(config)# interface vian 1000	
(coning-in)# ip address 172.16.0.2 255.255.255.0	
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	RADIUS サーバの IP アドレスおよびキーを設
alaxala	定します。この例ではキーを「alaxala」とし
	しいより。

(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	以下のアクセスリストを作成します。
(config-ext-nacl)# permit udp any any eq bootps	・DHCP通信を許可する。
(config-ext-nacl)# permit udp any host 192.168.1.11	・DNSサーバ「192.168.1.11」へのDNS通信を
eq domain	許可する。
(config-ext-nacl)# permit ip any host 192.168.1.102	・検疫サーバ「192.168.1.102」への通信を許
(config-ext-nacl)# permit ip any host 192.168.1.103	可する。
	・修復サーバ「192.168.1.103」への通信を許
	リする。
	> 構架ホイント(3)
物理ホートの設定	
(config)# interface range gigabitethernet 0/1-20	ボート 0/1~0/20 を Web 認証対象ボートとし
(config-if-range)# web-authentication port	て設定します。
(config-if-range)# authentication arp-relay	認証則の姉木から达信される他死て ARP ハ
(configuit renge)# outboution in concern	ケットを認証対象外のホートへ四力させます。 認証用マクセスリストを適用します
wob-auth	認証用プラセスリストを適用します。
RADIUS の設定	
(config)# aga authentication web-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。
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。
	▶ 構築ボイント(2)
(config)# web-authentication system-auth-control	Web 認証を有効にします。
(config)# web outbontion may timer 1110	
(comy)# web-authentication max-timer 1440	認証 以り夜の取入技院时间で 440 万(口) - 設宁 ます
	□ x z u c c c c c c c c c c c c c c c c c c

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-vlap)# state suspend	VLAN1 は使用しないため、無効にします。
(config)# vlan 10,20,1000 (config)# vlan 10,20,1000 (config-vlan)# state active	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
(config)# vlan 100,200	します。
(config-vlan)# state active	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	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。
(config)# interface range gigabitethernet 0/3-6 (config-if-range)# switchport mode access (config-if-range)# switchport access vlan 100	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。
(config)# interface gigabitethernet 0/7 (config-if)# switchport mode access (config-if)# switchport access vlan 200	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。
(config)# interface range gigabitethernet 0/1-4 (config-if-range)# media-type rj45	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	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。
(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	

(2) DHCP リレーの設定

AX3630S の設定	
DHCP リレーの設定	
(config)# interface vlan 10	VLAN10 および 20 に対して、DHCP リレーエ
(config-if)# ip helper-address 192.168.1.12	ージェントによる転送先アドレスを設定しま
	す。
(config)# interface vlan 20	
(config-if)# ip helper-address 192.168.1.12	

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。



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"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 ヘ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。

後疫ネットワークシステム - Windows Internet Explorer	
O → Ittp://192.168.1.102:8008/con/login.cgi	۰ م
😪 🍪 🏉 検疫ネットワークシステム 🍡 🏠 🔹 🗟 🔹 💀 ページ(P)	▼ ② ツール(0) ▼ [≫]
	-
Hitac	hiCáble
Empowering E	nergy & Communication
検疫ネットワークシステム	
OuOLA@Adapter	
セキュリティポリシー管理ツール	
ビモエリアイホリン「自生ノール	E
Ver 1.05	
ユーザID	الشنا
バスワード	
	τ.
ページが表示されまし 🛛 🕞 インターネット 保護モード: 無効	🔍 100% 🔻

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。

 	x
 金 後 検 タ マ トワークシステム	•
・ ・ ・	*
検皮ネットワークシステム 認証スイッチ共通設定 QuOLA@Adapter Ver 1.05 現在時刻:2008/6/30 11:30 1.ユーザ認証方式選択	2
	*
★検疫サーバ ユーザ認証方式 ◎ 共通ID ◎ 個別ID ◎ WindowsログインID	
認証スイッチ 共通ユーザ名 Juser01 ・認証スイッチ共通 バスワード ※1	
· Apresia A-Def ※1エーリ認証方式を変更される場合は必ずバスワートを入力して下さ · AlaxalA い。	H
▼ 検疫ボリシー 設定	
× メンテナンス	
▼ サポートセンター 2.使用スイッチ	
▼ ログアウト 優先順位 1 AlaxalA ▼	
優先順位 2 ▼ 優先順位 3 ▼	
設定	

(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

	ベットワークシステム -	Windows Internet Explorer		
C) - 🙋 http://192.1	68.1.102:8008/con/quola_top.cgi	i?sessionkey=pmdkjvy 👻 44 X Live Search	Q
🚖 🏟	🏉 検疫ネットワー	クシステム) •
			Hitachi C ab	le
_{検疫} ネ の 	vyhy-þýzfu L A@Adanter	AlaxalA設定	Empowering Energy & Communic	ation
現在時	Ver 1.05 刻:2008/6/30 11:34	1.認証解除情報		
		認証解除 URL	http://1.1.1.1/cgi-bin/Login.cgi	
	検疫サーバ	認証成功文字列	Login success	
	認証スイッチ	認証失敗文字列	Authentication reject	
· 5251E	スイッチ共通			
• Apre	isia NA		設定	
• Apre	sia A-Det			
V	検疫ポリシー			
	メンテナンス			
	サポートセンター			

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。

🚱 🏈 検疫ネットワ	ークシステム			☆ • ■	▼ 🖶 ▼ 🔂 ページ(F	P) ▼ (③ ツール(0
					Hita	chiCab
疲ネットワークシステム 🔶	セキュリテ	ティポリシー設定			Empowering	Energy & Communic
OLA@Adapte Ver 1.						
在時刻:2008/7/2 14	os名	検疫対象	バッチチェ ック	バターン番号チュック	: WindowsFWチェ ック	貸産チェッ ク
検疫サーバ 認証スイッチ 検疫ボリシー	Windows 2000	対象	▼ 『チェック 有り	 ✓ TrendMicro ✓ Symantec ✓ McAfee ✓ F=secure 	□チェック有り	■チェック 有り
キュリティポリシー S Inclows バッチ ッチ情報自動取得	Windows XP	対象	▼ ▼ 有り	 ✓ TrendMicro ✓ Symantec ✓ McAfee ✓ F-secure 	☑チェック有り	◎チェック 有り
ィルス対策ソフト 産台帳 止ソフトウェア -	Windows Vista	対象	▼ ■チェック 有り	 ✓ TrendMicro ✓ Symantec ✓ McAfee ✓ F−secure 	☑チェック有り	■チェック 有り

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

検疫ネットワークシステム - Windows Internet Explorer	
C v ktp://192.168.1.102:8008/sec/download.cgi	 t_f × Live Search
🚖 🏟 🧶 検疫ネットワークシステム	
	HitachiCable Empowering Energy & Communication
検疫ネットワー QuOLA@A	クシステム A dapter
下記のボタンをクリックし、セキュリテ セキュリティチェック 開始	- イチェックを実行して下さい
<mark>管理者からのメッセージ</mark> セキュリティチェックを実行しなければネットワーク 【******ガループからのメッセージ】 ウィルス対策ソフトのパターンファイルの更新はこ	7に接続することは出来ません。 こまめに!
	ターネット 保護モード: 無効 🔍 100% 🔻

* 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。

後庭ネットワークシステム - Windows Internet Explorer	
Composition Composition <thcomposition< th=""> <thcomposition< th=""></thcomposition<></thcomposition<>	ρ -
☆ ☆ 愛検疫ネットワークシステム ☆ マ 回 マ 一 ジ ページ(P) マ ()	🎒 ツール(0) 🔻 🤌
Hitachi Empowering Energy & ファイルのダウンロード - セキュリティの警告	
このファイルを実行または保存しますか? 名前: quolaNCOA801665008.exe 種類: アブリケーション, 568 KB 発信元: 192.168.1.102 下記の: 実行(R) (保存(S))	E
インターネットのファイルは役に立ちますが、このファイルの種類はコンピュータに問題 を起こす可能性があります。発信元が(言語できないは易合は、このソフトウェアを実 行したり(保存したりしないでくだとい。一位受性の説明)	
管理者からのメッセージ セキュリティチェックを実行しなければネットワークに接続することは出来ません。 【*******グループからのメッセージ】 ウィルス対策ソフトのパターンファイルの更新はこまめに!	-
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	a 100% 👻

- *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)

検疫ネ QuO	ットワーク LA@A	فمج⊥ dapt e	27 Versio	n 1.05
ユーザ名と/ ユーザ名 :	(スワードを入 「	、カレて下さ	L Y.	
パスワード :				

(5) 検疫失敗

検疫失敗時の例を下記に示します。

QuOLA@Adapter	
	検疫ネットワークシステム QuOLA@Adapter Version 1.05
下記のセキュリ ・WindowsFireW	ティポリシー違反のためネットワークへ接続できません。 all機能が無効です。

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



A.2. AX24308 のコンフィグレーション



A.3. AX12308 のコンフィグレーション





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/