

オープンネット・ガード評価報告書

2009年3月25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

■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

「オープンネット・ガード」は株式会社日立システムアンドサービスの登録商標です。
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
オープンネット・ガード インストールマニュアル
オープンネット・ガード 運用マニュアル

目次

1. オープンネット・ガードとAXシリーズの連携概要
2. 評価構成
 - 2-1. 評価対象機器
 - 2-2. 評価構成図
3. 検証結果
 - 3-1. 認証機能評価結果
 - 3-2. MAC認証ログ評価結果
 - 3-3. Web認証ログ評価結果
4. オープンネットガード・設定
 - 4-1. 認証設定
 - 4-2. 認証ログの設定
5. 認証ログ表示例
 - 5-1. MAC認証ログの表示例
 - 5-2. Web認証ログの表示例

1. オープンネット・ガードとAXシリーズの連携概要

■AX認証機能とオープンネット・ガードの連携の特徴

1. オープンネット・ガードのRADIUS連携機能で、AXシリーズのMAC認証およびWeb認証の認証サーバとして連携可能です。
2. AXシリーズの認証ログと連携して、不正端末の接続および、登録ユーザまたは端末ごとに認証スイッチの接続ポートまで追跡可能です。
(ログはオープンネット・ガードのデータベースよりMACアドレスからユーザIDを検索して表示され検索が便利です。)
3. AXシリーズのWeb認証とオープンネット・ガードのDHCP機能と連携することで、Web認証によるユーザ認証とDHCPサーバによる端末認証でネットワークへの不正接続をガードします。

■評価試験結果

AXシリーズの認証機能とオープンネット・ガードのRADIUS連携機能および認証ログ連携機能の評価試験を実施して問題なく動作する事を確認しました。

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。

● 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	
管理サーバ RADIUSサーバ DHCPサーバ syslogサーバ	RedHat Enterprise Linux 5	オープンネット・ガード (エンタープライズ版)	Ver4.0
		前提プログラム(注)	
端末	OSは問わないが本試験では Windows XPを使用	—	SP2

(注)オープンネット・ガードのインストールマニュアルに従い、Webサーバ、DHCPサーバ、RADIUSサーバなどのRed Hat Linux上で動作する各種前提プログラムを使用しました。

● 認証スイッチ(AXシリーズ)

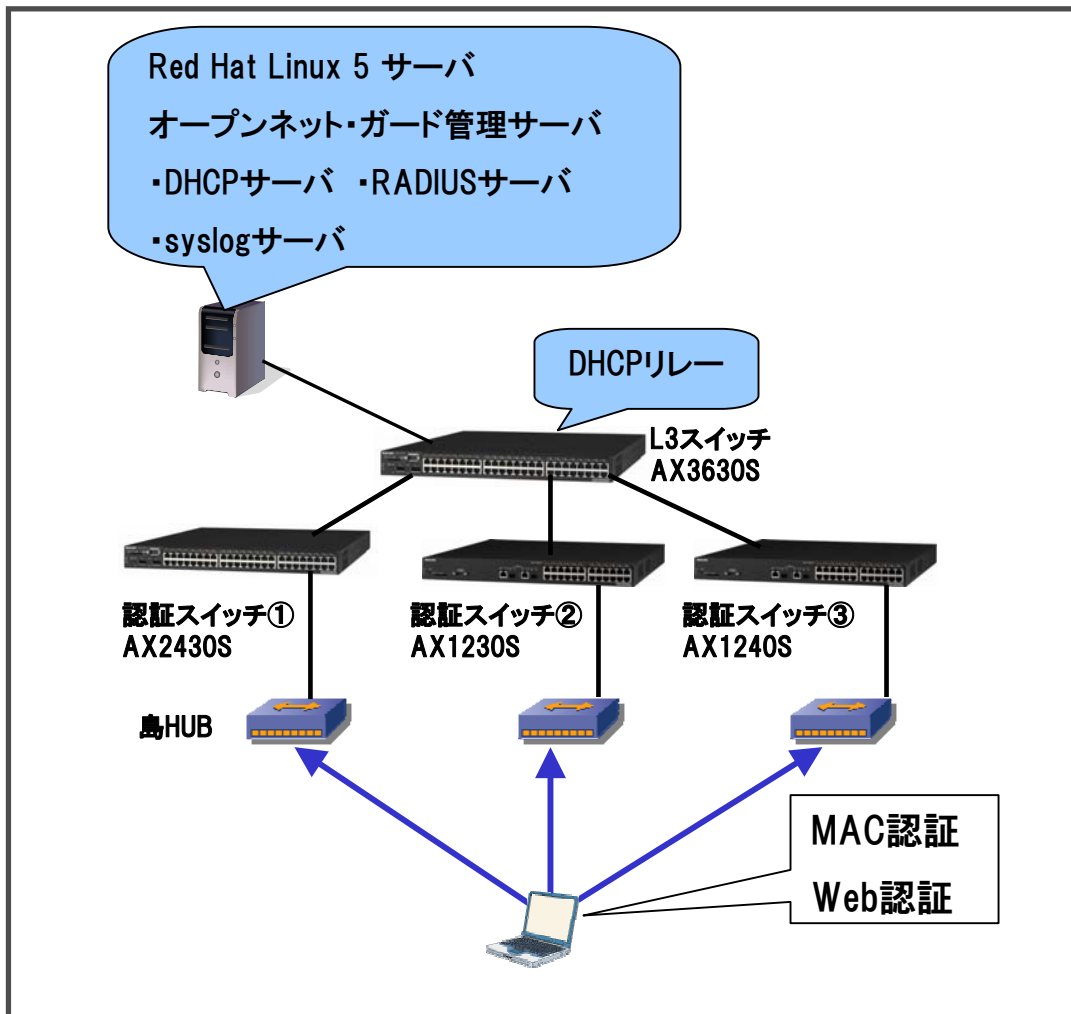
用途	機器名	バージョン
L3スイッチ	AX3630S	11.0
認証スイッチ①	AX2430S	11.0
認証スイッチ②	AX1230S	1.4.B
認証スイッチ③	AX1240S	2.0

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。

● 構成図



● 試験概要

1台のRed Hat Linux 5サーバ上にオープンネット・ガード管理サーバとオープンネット・ガードで連携する、DHCPサーバ、RADIUSサーバ、syslogサーバを構築し配下にAXシリーズ認証スイッチを配置して以下の動作を確認

- ・MAC認証の連携
- ・Web認証の連携
- ・DHCPサーバ連携(登録端末のみに配布)
- ・AlaxaIA認証ログの確認

● 認証スイッチの設定概要

認証スイッチにMAC認証(固定VLAN、動的LAN)とWeb認証(固定VLAN、動的VLAN)を設定して、合計4種類の認証を定義。

● オープンネット・ガードの設定概要

試験対象ユーザの登録とユーザの使用端末を登録し、DHCPサーバRADIUSサーバ、syslogサーバと連携。

3-1. 認証機能評価結果

■ AXスイッチの認証機能とオープンネット・ガード連携の評価結果

試験対象機器	認証方式	認証モード	認証連携試験結果
AX2430S	MAC認証	固定VLAN	○
		動的VLAN	○
	Web認証	固定VLAN	○
		動的VLAN	○
AX1230S	MAC認証	固定VLAN	○
		動的VLAN	○
	Web認証	固定VLAN	○
		動的VLAN	○
AX1240S	MAC認証	固定VLAN	○
		動的VLAN	○
	Web認証	固定VLAN	○
		動的VLAN	○

※表中の○は認証機能および登録MACアドレスによるDHCP連携動作が可能であることを示します。

動的VLAN時の応答定義は 以下を使用

Tunnel-Type = 13 , Tunnel-Medium-Type = 6, Tunnel-Private-Group-ID = VLAN番号(VLAN名称でも可)

3-2. MAC認証ログ確認結果

■MAC認証ログの確認項目と結果

試験項目	確認項目	AX1230S、AX1240S		AX2400S、AX3600S	
		固定VLAN	動的VLAN	固定VLAN	動的VLAN
ログイン成功	ログイン成功	○	○	○	○
ログイン失敗	未登録端末の接続	○	○	○	○
	VLAN番号不正	—	○	—	○
ログアウト	最大接続時間	○	○	○	○
	無通信監視	○	○	○	○
	リンクダウン	○	○	○	—
システムメッセージ	ログアウトコマンド	○	○	○	○
	認証開始	○	○	○	○
	再認証	—	○	—	—
ログ内の表示確認	時刻表示	○	○	○	○
	認証スイッチ	○	○	○	○
	認証ポート	○	○	○	○
	MACアドレス	○	○	○	○
	ユーザID(※2)	○	○	○	○

※ 表中の○はログ連携が正しく動作している事を示します。—は当該機能のログをAX未サポートのログであることを示します。

試験結果について、運用上主要なログについて問題なく連携できる事を確認しました。

※2 ユーザIDはオープンネット・ガードのデータベースより認証機器のMACアドレスから検索され表示されます。

3-3. Web認証ログ確認結果

■ Web認証ログの確認項目と結果

試験項目	確認項目	AX1230S、AX1240S		AX2400S、AX3600S	
		固定VLAN	動的VLAN	固定VLAN	動的VLAN
ログイン成功	ログイン成功	○	○	○	○
ログイン失敗	未登録端末の接続	○	○	○	○
	VLAN番号不正	—	○	—	○
ログアウト	最大接続時間	○	○	○	○
	無通信監視	○	○	○	○
	リンクダウン	○	○	○	—
	ユーザ操作	○	○	○	○
システムメッセージ	ログアウトコマンド	○	○	○	○
	認証開始	○	○	○	○
ログ内の表示確認	時刻表示	○	○	○	○
	認証スイッチ	○	○	○	○
	認証ポート	○	○	○	○
	MACアドレス	○	○	○	○
	認証ユーザ名	○	○	○	○
	ユーザID(※2)	○	○	○	○
	IPアドレス	○	○	○	○

※ 表中の○はログ連携が正しく動作している事を示します。—は当該機能のログをAX未サポートのログであることを示します。

試験結果について、運用上主要なログについて問題なく連携できる事を確認しました。

※ 2 ユーザIDはオープンネット・ガードのデータベースより認証機器のMACアドレスから検索され表示されます。

4-1. 認証設定

■オープンネット・ガードの設定に関して

インストールマニュアルに従い各種前提プログラムとともに、オープンネット・ガード管理サーバをセットアップしAXの認証とログ連携に必要な設定をWeb画面から実施しました。

本章ではAXと相互接続確認でを使用した認証関連の設定のポイント部分を抜粋して紹介します。

ユーザの登録や端末の登録作業などの共通操作は省略おり、作業ポイント部分のみを抜粋しています。詳細な設定に関してはオープンネット・ガード 運用マニュアルを参照してください。

■AXシリーズの認証に関する設定

AX認証スイッチの設定に関しては「AXシリーズ認証ソリューションガイド」を参照してください。オープンネット・ガードとの連携に関して、syslogサーバとRADIUSサーバをオープンネット・ガードの管理するサーバに設定する以外の特別な設定は必要ありません。

4-1. 認証設定

■(1) 認証スイッチの登録

OpenNET・Guard コントローラのURL: http://サーバ名/ctl/ctl_frame.php

OpenNET・Guard コントローラ

サーバ管理 - RADIUSサーバ編集

RADIUSサーバ情報

RADIUSサーバ名: ONG_ALAXALA_RADIUSD

RADIUSサーバ

#	IPアドレス	ONG制御ポート
1	10.50.0.3	1097
2		1097
3		1097
		1097

②

認証クライアント設定

認証クライアント名: AX1230S-2

コメント: AX1230S-2

IPアドレス: 172.16.0.16

共有鍵(secret): alaxala

略称(shortname): AX1230S-2

機種タイプ(nastype): other

③

3件の登録があります

④ クライアント追加

選択	▲認証クライアント名	コメント	IPアドレス	共有鍵	略称	機種タイプ	使用
<input type="checkbox"/>	AX1230S	AX1230S	172.16.0.13	alaxala	AX1230	other	する
<input type="checkbox"/>	AX1240S	AX1240S	172.16.0.15	alaxala	AX1240	other	する
<input type="checkbox"/>	AX2430S	AX2400S	172.16.0.14	alaxala	AX2400	other	する

⑤

保存 戻る

試用版(有効期限:2009/04/30) 30 クライアントライセンス

All Rights Reserved. Copyright (C) 2004,2008, Hitachi Systems & Se

認証スイッチの登録は
 ①RADIUSサーバー一覧を開き、②認証クライアント情報を選択して、③の各種項目を入力後、④追加を行ない画面下の⑤保存を実行してください。

ここで設定された、認証クライアント名やコメントが認証ログに表示されます。

4-1. 認証設定

■(2) RADIUS設定情報の反映

OpenNET・Guard コントローラ

利用状況モニター 運用・保守 - 起動/停止

利用IP検索
端末情報配信

不正接続モニター
不正接続IP一覧
遮断IP一覧

端末情報管理
端末情報検索
新規登録
監査情報検索
Infoblox連携

ユーザ情報管理
ユーザ情報検索
新規登録

サーバ管理
DHCPサーバ一覧
不正接続監視
RADIUSサーバ一覧

システム定義
コントローラ定義
レジストラ定義
ルータ定義
遮断装置定義
Infoblox定義
認証情報定義

運用・保守
起動/停止
メンテナンス
ログ参照
Alaxala認証ログ
MAC収集

登録管理サーバ

状態 ONG 操作
正常 [v] 実行

ONGサーバ
最新の状態に更新

サーバ名	種別	サーバ設定			サーバ情報					
		状態	サーバ操作	冗長化	IPアドレス	構成	状態	サーバ操作	ONG	操作
ONG_ALAXALA_DHCPD	DHCP	登録済	[v]	なし	10.50.0.3	-	正常	[v]	[v]	状態更新
ONG_ALAXALA_RADIUSD	RADIUS	登録済	登録 [v]	なし	10.50.0.3	-	正常	[v]	[v]	実行

① 起動/停止

② 登録を選択して実行

③ 再起動を選択して実行

(1)のRADIUS設定に関する情報の変更をした場合は、①「起動/停止」から、RADIUSサーバへ情報の②「登録」と③「再起動」を実行します。

4-1. 認証設定

■(3) 認証情報の登録(MAC認証)

OpenNET・Guard コントローラ

システム定義 - 認証情報定義編集

利用状況モニター
利用IP検索
端末情報配信

不正接続モニター
不正接続IP一覧
遮断IP一覧

端末情報管理
端末情報検索
新規登録
監査情報検索
Infoblox連携

ユーザ情報管理
ユーザ情報検索
新規登録

サーバ管理
DHCPサーバ一覧
不正接続監視
RADIUSサーバ一覧

システム定義
コントローラ定義
レジスタ定義
ルータ定義
遮断装置定義
Infoblox定義
① 認証情報定義

運用・保守
起動/停止
メンテナンス
ログ参照
Alaxala認証ログ
MAC収集

認証情報

グループ名: MAC-VLAN200

認証名: MAC

コメント: MAC認証 VLAN200

③ 認証種別: 端末用

④ 認証定義: ##MACADDRESS10## Auth-Type=Local, User-Password="" ##MACADDRESS10##

⑤ 応答定義: Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-Id = 200

MACアドレスの変換パターン

##MACADDRESS00##	→ 00-11-22-33-aa-bb
##MACADDRESS01##	→ 00-11-22-33-AA-BB
##MACADDRESS10##	→ 00112233aabb
##MACADDRESS11##	→ 00112233AABB
##MACADDRESS20##	→ 0011.2233.aabb
##MACADDRESS21##	→ 0011.2233.AABB
##MACADDRESS30##	→ 00:11:22:33:aabb
##MACADDRESS31##	→ 00:11:22:33:AA:BB

ユーザIDの変換パターン

##USER00##	→ 変換しない (Admin→Admin)
##USER01##	→ 英大文字に変換 (Admin→ADMIN)
##USER02##	→ 英小文字に変換 (Admin→admin)

⑥ 更新

⑦

リセット

デフォルト値設定

戻る

MAC認証の場合は端末用を選択してください

VLAN番号またはVLAN名称を指定します

MAC認証を行なう場合は
①「認証情報定義」より本画面を表示して②に示すように任意の認証グループ名、認証名、コメント、を入力し、③「認証種別」を端末用に入します。

④「認証定義」にユーザ名、パスワードともにMACアドレスの場合は、認証定義を左記のように入力します。
(⑦のプルダウンメニューで「MACアドレス認証」を選択し、「デフォルト値設定」ボタン押下で入力が可能。) MAC認証のパスワードを認証スイッチのConfigで指定する場合は、Password=""にMAC認証のパスワードを入力してください。

⑤「応答定義」は動的VLAN認証の場合にのみ必要です。

⑥「更新」ボタンで登録後に(5)の端末情報と関連付けを行ないます。

4-1. 認証設定

■(4) 認証情報の登録(Web認証)

OpenNET・Guard コントローラ

システム定義 - 認証情報定義編集

利用状況モニター
利用IP検索
端末情報配信

不正接続モニター
不正接続IP一覧
遮断IP一覧

端末情報管理
端末情報検索
新規登録
監査情報検索
Infoblox連携

ユーザ情報管理
ユーザ情報検索
新規登録

サーバ管理
DHCPサーバー一覧
不正接続監視
RADIUSサーバー一覧

システム定義
コントローラ定義
レジスタ定義
ルータ定義
遮断装置定義
Infoblox定義
① 認証情報定義

運用・保守
起動/停止
メンテナンス
ログ参照
Alaxala認証ログ
MAC収集

認証情報

グループ名: Web-VLAN200

②

認証名: Web

コメント: Web認証 VLAN200

③ 認証種別: ユーザ用 ← Web認証の場合はユーザ用を選択してください

④

認証定義: ##USER00## Auth-Type:=ONGAUTH

⑤

⑦ 応答定義: Tunnel-Type = 13,
Tunnel-Medium-Type = 6,
Tunnel-Private-Group-Id = 200
← VLAN番号またはVLAN名称を指定します

MACアドレスの変換パターン

##MACADDRESS00##	→ 00-11-22-33-aa-bb
##MACADDRESS01##	→ 00-11-22-33-AA-BB
##MACADDRESS10##	→ 00112233aabb
##MACADDRESS11##	→ 00112233AABB
##MACADDRESS20##	→ 0011.2233.aabb
##MACADDRESS21##	→ 0011.2233.AABB
##MACADDRESS30##	→ 00:11:22:33:aa:bb
##MACADDRESS31##	→ 00:11:22:33:AA:BB

ユーザIDの変換パターン

##USER00##	→ 変換しない(Admin→Admin)
##USER01##	→ 英大文字に変換(Admin→ADMIN)
##USER02##	→ 英小文字に変換(Admin→admin)

⑥

更新 リセット ONGユーザ認証 デフォルト値設定 戻る

Web認証を行なう場合は ①「認証情報定義」より本画面を表示して②で任意の認証グループ名、認証名、コメント、を入力し③「認証種別」をユーザ用にします。

④「認証定義」をWeb認証の場合は左記のように入力します。

(⑦のプルダウンメニューで「ONGユーザ認証」を選択し、「デフォルト値設定」ボタン押下で入力が可能。)

⑤「応答定義」は動的VLAN認証の場合のみ必要です。

⑥「更新」ボタンで登録後(6)のユーザ情報に関連付けを行ないます。

4-1. 認証設定

■(5) 端末情報と認証情報の関連付け(MAC認証)

OpenNET・Guard コントローラ

利用状況モニター

利用IP検索
端末情報配信

不正接続モニター

不正接続IP一覧
遮断IP一覧

① 端末情報管理

端末情報検索
新規登録
監査情報検索
Infoblox連携

ユーザ情報管理

ユーザ情報検索
新規登録

サーバ管理

DHCPサーバ一覧
不正接続監視
RADIUSサーバ一覧

システム定義

コントローラ定義
レジスタ定義
ルータ定義
遮断装置定義
Infoblox定義
認証情報定義

運用・保守

起動/停止
メンテナンス
ログ参照
Alaxala認証ログ
MAC収集

端末情報管理 - 端末情報・変更

ハードウェア情報

MACアドレス: 00:1a:4b:60:c3:83 Hewlett Packard

リース: 無効

ARP不正接続監視: 対象外

固定IPアドレス: 登録なし

MACグループ: 登録なし

RADIUS認証設定
MAC-VLAN200:MAC

②

ユーザ情報

ユーザID: user01

ユーザ名: user01

組織名: alaxala

ユーザ確認

RADIUS認証設定で(2)で登録した認証情報と関連付けします。

コンピュータ情報

ホスト名: HP_NOTE

OS種別: Windows XP Professional

管理番号:

備考:

利用期間

利用期間(開始): 2008-01-01

利用期間(終了): 2008-01-01 無期限

利用時間(開始): 00 時 00 分

利用時間(終了): 00 時 00 分 全時間帯

監査結果による有効期限: 2008-12-16 無効

③

更新 監査情報 リセット 削除 戻る

MAC認証を行なう場合、登録済み端末情報と(3)の認証情報の関連付けを行なう必要があります。端末の登録に関しては省略しています。

①「端末情報検索」から登録済み端末を検索して②「RADIUS認証設定」で(3)にて設定済みの認証情報と関連付けします。

③「更新」で入力情報を反映します。

4-1. 認証設定

■(6) ユーザ情報と認証情報の関連付け(Web認証)

OpenNET Guard コントローラ

ユーザ情報管理 - ユーザ情報・変更

ユーザ情報

ユーザID : user01

ユーザ状態: ユーザを無効にする

パスワード: 再入力:

ユーザ名: user01 権限: User WF管理者

組織名1: alaxala 管理組織: 組織1

組織名2: _____

組織名3: _____

メールアドレス: _____

電話番号: _____

備考: _____

RADIUS認証設定

Web-VLAN200:Web

RADIUS認証設定で(3)で登録した認証情報と関連付けします。

更新 リセット 削除 戻る

Web認証を行なう場合は、登録済みユーザ情報を(3)で登録した認証情報と関連付けします。

①「ユーザ情報検索」から登録済みユーザ情報を検索して
②「RADIUS認証設定」で(3)で登録した認証設定を関連付けしてします。

③「更新」で入力情報を反映します。

4-1. 認証設定

■(7) ユーザ情報および認証情報の反映

利用状況モニター — 端末情報配信」

OpenNET・Guard コントローラ Version 4.0

利用状況モニター — 端末情報配信

状態更新  (*)全端末情報登録は、端末情報が多い場合、処理に時間がかかる場合があります。

■MACアドレス数(リース有効):450件 ■消費ライセンス数:427件(Infoblox登録対象:13件)

▲サーバ名	種別	冗長化	IPアドレス	状態	端末情報更新	全端末情報更新(*)
OA認証サーバ	RADIUS	<使用しない>				
なんぼパークス21F	DHCP	なし	10.211.226.199	正常運転	<input type="button" value="登録"/>	<input type="button" value="登録"/>
ローカルサーバ	RADIUS	なし	10.211.226.199	正常運転	<input type="button" value="登録"/>	<input type="button" value="登録"/>

(3)~(6)の認証情報およびユーザや端末情報の追加や変更をした場合は

「利用状況モニター — 端末情報配信」から端末情報更新「登録」ボタンを押下するか、

「システム定義 — コントローラ定義」のコントローラ設定「端末情報更新間隔」経過時、自動更新します。この場合、ファイル更新後、RADIUSサーバサービスを自動的に再起動します。

OpenNET・Guard コントローラ

システム定義 — コントローラ定義

コントローラ設定

検索結果最大表示件数: 1000 件(100~1000000)

端末情報更新間隔: 10 分(5~720) Infoblox自動更新: しない する

全端末情報更新時刻: 00 時 00 分 全端末情報更新: しない する

利用状況情報取込間隔: 10 分(5~60) Infoblox利用状況取得: しない する

DHCPサーバステータスチェック間隔: 10 分(5~60)

モニター画面更新間隔: 30 秒(10~180)

不正接続監視設定

不正接続監視する

4-2. 認証ログの設定

■ 認証ログの設定

OpenNET・Guard 設定のURL: <http://サーバ名/setup/index.php>

OpenNET・Guard 設定

権限管理
[ユーザ権限検索](#)
[メニュー表示設定](#)
[一覧表示設定](#)

ログ管理
[認証ログ定義](#)

ログ管理 - 認証ログ定義

ログ参照名称: ログ種別選択: [追加] [更新] [削除] [↑] [↓]

9件の登録があります

選択	ログ参照名称	ログ種別名称	ファイル定義	使用
<input type="checkbox"/>	認証ログ	アラクサラ認証詳細ログ	3件登録	する
<input type="checkbox"/>	MAC認証ログ	アラクサラMAC認証詳細ログ	3件登録	する
<input type="checkbox"/>	WEB認証ログ	アラクサラWEB認証詳細ログ	3件登録	する
<input type="checkbox"/>	システムログ	システムログ	1件登録	する

①

② 認証ログ定義したい項目を選択してファイルを追加してください。

OpenNET・Guard 設定

権限管理
[ユーザ権限検索](#)
[メニュー表示設定](#)
[一覧表示設定](#)

ログ管理
[認証ログ定義](#)

ログ管理 - 認証ログ定義・ファイル定義

ログ参照名称: MAC認証ログ ファイル名: /var/log/messages.3 読込行数: [追加] [更新] [削除] [↑] [↓] [戻る]

4件の登録があります

選択	ファイル名	読込行数
<input checked="" type="checkbox"/>	/var/log/messages.3	指定なし
<input type="checkbox"/>	/var/log/messages.2	指定なし
<input type="checkbox"/>	/var/log/messages.1	指定なし
<input type="checkbox"/>	/var/log/messages	指定なし

③ 認証ログのファイルの順序に注意してください。古いものから新しい順に設定する必要があり↑↓で追加後並べ替えてください。

認証ログの設定は、<http://サーバ名/setup/index.php>の①「認証ログ定義」から行ないます。

② 認証ログ、MAC認証ログ、Web認証を選択して読み込むログファイルを指定します。

③ この時ログファイルを複数指定する場合は古いものから順に設定する必要があります。

(初期値)

syslogサーバ設定の初期値では認証のログ含めて全ログが/var/log/messagesに格納されファイル容量が制限を超えるかまたは1週間ごとに古いものをmessages.1, messages.2とリネームしてログファイルのローテーションをします。

ログの採取ファイル名の変更等syslogの詳細な設定が必要です、オープンネット・ガードのマニュアル等を参照してsyslog.confなどの設定ファイルを変更する必要があります。

5-1. MAC認証ログの表示例

■MAC認証ログ表示例(1)

OpenNET・Guard コントローラ Version 4.0

運用・保守 - AlaxalA認証ログ

MAC認証ログを選択し、検索条件クリア、MACアドレス毎に最新のみ表示、自動表示更新、CSV出力

MACアドレスでフィルタすることができます。

135件見つかりました

▼日付	機器IP	機器名	コメント	装置日付	ログ種別	ログ種別	状態	MACアドレス	ホスト名	ユーザID	ユーザ名	IPアド
02-13 11:40:17	172.16.0.15	AX12405	AX12405	02-13 10:46:03	標準	ログアウト	認証解除	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-13 11:39:04	172.16.0.15	AX12405	AX12405	02-13 10:44:50	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-13 11:39:04	172.16.0.15	AX12405	AX12405	02-13 10:44:50	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-13 11:29:01	172.16.0.15	AX12405	AX12405	02-13 10:34:48	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-13 11:29:01	172.16.0.15	AX12405	AX12405	02-13 10:34:48	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:52:51	172.16.0.15	AX12405	AX12405	02-12 17:58:37	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:52:51	172.16.0.15	AX12405	AX12405	02-12 17:58:37	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:42:50	172.16.0.15	AX12405	AX12405	02-12 17:48:37	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:42:50	172.16.0.15	AX12405	AX12405	02-12 17:48:37	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:32:50	172.16.0.15	AX12405	AX12405	02-12 17:38:36	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:32:50	172.16.0.15	AX12405	AX12405	02-12 17:38:36	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:22:49	172.16.0.15	AX12405	AX12405	02-12 17:28:35	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:22:49	172.16.0.15	AX12405	AX12405	02-12 17:28:35	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:12:48	172.16.0.15	AX12405	AX12405	02-12 17:18:34	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:12:48	172.16.0.15	AX12405	AX12405	02-12 17:18:34	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:02:47	172.16.0.15	AX12405	AX12405	02-12 17:08:33	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 18:02:47	172.16.0.15	AX12405	AX12405	02-12 17:08:33	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:52:47	172.16.0.15	AX12405	AX12405	02-12 16:58:33	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:52:47	172.16.0.15	AX12405	AX12405	02-12 16:58:33	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:41:20	172.16.0.15	AX12405	AX12405	02-12 16:47:06	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:41:20	172.16.0.15	AX12405	AX12405	02-12 16:47:06	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:35:33	172.16.0.15	AX12405	AX12405	02-12 16:41:19	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:35:33	172.16.0.15	AX12405	AX12405	02-12 16:41:19	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:35:30	172.16.0.15	AX12405	AX12405	02-12 16:41:16	標準	ログアウト	認証解除	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:35:13	172.16.0.15	AX12405	AX12405	02-12 16:40:59	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:35:13	172.16.0.15	AX12405	AX12405	02-12 16:40:58	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:33:45	172.16.0.15	AX12405	AX12405	02-12 16:39:31	標準	ログアウト	認証解除	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:27:37	172.16.0.15	AX12405	AX12405	02-12 16:33:23	標準	ログイン	成功	00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:27:37	172.16.0.15	AX12405	AX12405	02-12 16:33:23	標準	システム		00:1a:4b:60:ce:83	HP_NOTE	user01	user01	
02-12 17:25:30	172.16.0.15	AX12405	AX12405	02-12 16:31:16	標準	システム						
02-12 17:10:43	172.16.0.15	AX12405	AX12405	02-12 16:16:30	通知	ログイン	失敗	00:00:11:11:11:11				

試用版(有効期限:2009/04/30) 30 クライアントライセンス All Rights Reserved. Copyright (C) 2004,2008. Hitachi Systems & Services, Ltd.

MAC認証ログを表示するためには①「AlaxalA認証ログ」を選択して、②「MAC認証ログ」を選択します。

日付の▼をクリックすると新⇄旧の並べ替えができます。

また、各表示項目をキーとしてログ表示のフィルタができます。

認証スイッチの機種名やユーザ名をオープンネット・ガードのデータベースに登録された情報と紐付けして表示するため追跡が容易です。

次のページに同一ログの右側部分を表示しています

5-1. MAC認証ログの表示例

■MAC認証ログ表示例(2)

OpenNET・Guard コントローラ Version 4.0

利用状況モニター 運用・保守 - AlaxaIA認証ログ

MAC認証ログ: 検索 検索条件クリア MACアドレス箱に最新のみ表示 自動表示更新 CSV出力

不正接続モニター 135件見つかりました

	ホスト名	ユーザID	ユーザ名	IPアドレス	ポート	VLAN	番号	メッセージ
83	HP_NOTE	user01	user01		0/3	200	2	認証対象ポートがリンクダウンしたため、該当ポートでログインしていたすべてのユーザ認証を解除しました。
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	1	クライアントは認証に成功しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	256	再認証されました。
83	HP_NOTE	user01	user01				266	Restart authenticating for MAC address.
83	HP_NOTE	user01	user01		0/3	200	1	クライアントは認証に成功しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01		0/3	200	1	クライアントは認証に成功しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01		0/3	200	30	MACアドレスエージングによって、MACアドレスが削除されたため、認証を解除しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01				82	clear mac-authentication auth-stateコマンドを受けました。
83	HP_NOTE	user01	user01		0/3	200	1	クライアントは認証に成功しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01		0/3	200	1	クライアントは認証に成功しました。
83	HP_NOTE	user01	user01				265	MACアドレス認証を開始しました。
83	HP_NOTE	user01	user01				82	clear mac-authentication auth-stateコマンドを受けました。

試用版(有効期限:2009/04/30) 30 クライアントライセンス All Rights Reserved. Copyright (C) 2004,2008, Hitachi Systems & Services, Ltd.

一部のログを除き、ログインやログアウト要因などを、日本語に変換して表示します。

ポート番号やVLAN番号が付いたログはポート番号とVLAN番号を表示します。

一部ログを除き日本語変換されます。

5-2. Web認証ログの表示例

■ Web認証ログ表示例(1)

OpenNET・Guard コントローラ Version 4.0

利用状況モニター 運用・保守 - Alaxala認証ログ

利用IP検査 ② Web認証ログ 検索 検索条件クリア MACアドレス毎に最新のみ表示 自動表示更新 CSV出力

不正接続モニター 191件見つかりました

ユーザ名でフィルタできます

▼日付	機器IP	機器名	コメント	装置日付	ログ識別	ログ種別	状態	認証ユーザ	MACアドレス	ホスト名	ユーザID	ユーザ名
02-13 16:44:25	172.16.0.15	AX1240S	AX1240S	02-13 15:50:14	標準	ログアウト	認証解除	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 15:47:21	172.16.0.15	AX1240S	AX1240S	02-13 14:53:10	標準	ログアウト	認証解除	user02	00:0a:e4:4d:55:92		user02	user02
02-13 15:43:41	172.16.0.15	AX1240S	AX1240S	02-13 14:49:29	標準	ログイン	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 15:40:44	172.16.0.15	AX1240S	AX1240S	02-13 14:49:29	標準	システム		user01				
02-13 15:40:44	172.16.0.15	AX1240S	AX1240S	02-13 14:46:32	標準	ログアウト	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 15:40:44	172.16.0.15	AX1240S	AX1240S	02-13 14:46:32	標準	システム						
02-13 15:08:37	172.16.0.15	AX1240S	AX1240S	02-13 14:14:25	標準	ログイン	成功	user02	00:0a:e4:4d:55:92		user02	user02
02-13 15:08:37	172.16.0.15	AX1240S	AX1240S	02-13 14:14:25	標準	システム		user02				
02-13 15:03:52	172.16.0.15	AX1240S	AX1240S	02-13 14:09:40	通知	ログイン	失敗	user02	00:0a:e4:4d:55:92		user02	user02
02-13 15:03:52	172.16.0.15	AX1240S	AX1240S	02-13 14:09:40	標準	システム		user02				
02-13 15:02:40	172.16.0.15	AX1240S	AX1240S	02-13 14:08:28	通知	ログイン	失敗	user02	00:0a:e4:4d:55:92		user02	user02
02-13 15:02:40	172.16.0.15	AX1240S	AX1240S	02-13 14:08:28	標準	システム		user02				
02-13 15:01:00	172.16.0.15	AX1240S	AX1240S	02-13 14:06:49	通知	ログイン	失敗	user02	00:0a:e4:4d:55:92		user02	user02
02-13 15:01:00	172.16.0.15	AX1240S	AX1240S	02-13 14:06:49	標準	システム		user02				
02-13 14:57:29	172.16.0.15	AX1240S	AX1240S	02-13 14:03:17	標準	ログイン	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:57:29	172.16.0.15	AX1240S	AX1240S	02-13 14:03:17	標準	システム		user01				
02-13 14:56:49	172.16.0.15	AX1240S	AX1240S	02-13 14:02:37	標準	ログアウト	認証解除	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:42:24	172.16.0.15	AX1240S	AX1240S	02-13 13:48:12	標準	ログイン	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:42:24	172.16.0.15	AX1240S	AX1240S	02-13 13:48:12	標準	システム		user01				
02-13 14:42:13	172.16.0.15	AX1240S	AX1240S	02-13 13:48:01	通知	ログイン	失敗	user02	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:42:13	172.16.0.15	AX1240S	AX1240S	02-13 13:48:01	標準	システム		user02				
02-13 14:41:49	172.16.0.15	AX1240S	AX1240S	02-13 13:47:37	通知	ログイン	失敗	user02	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:41:49	172.16.0.15	AX1240S	AX1240S	02-13 13:47:37	標準	システム		user02				
02-13 14:41:35	172.16.0.15	AX1240S	AX1240S	02-13 13:47:23	通知	ログイン	失敗	user03	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:41:35	172.16.0.15	AX1240S	AX1240S	02-13 13:47:23	標準	システム		user03				
02-13 14:31:52	172.16.0.15	AX1240S	AX1240S	02-13 13:37:39	標準	ログアウト	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:31:52	172.16.0.15	AX1240S	AX1240S	02-13 13:37:39	標準	システム						
02-13 14:10:30	172.16.0.15	AX1240S	AX1240S	02-13 13:16:18	標準	ログイン	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 14:10:30	172.16.0.15	AX1240S	AX1240S	02-13 13:16:18	標準	システム		user01				
02-13 12:41:09	172.16.0.15	AX1240S	AX1240S	02-13 11:46:56	標準	ログアウト	認証解除	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 11:41:07	172.16.0.15	AX1240S	AX1240S	02-13 10:46:54	標準	ログイン	成功	user01	00:1a:4b:60:ce:83	HP_NOTE	user01	user01
02-13 11:41:07	172.16.0.15	AX1240S	AX1240S	02-13 10:46:54	標準	システム		user01				

① Alaxala認証ログ
MAC収集

Web認証ログを表示するためには①「Alaxala認証ログ」を選択して、②「Web認証ログ」を選択します。

日付の▼をクリックすると新⇄旧の並べ替えができます。

各表示項目をキーとしてログ表示のフィルタができます。

認証スイッチの機種名やユーザ名をオープンネット・ガードのデータベースに登録された情報と紐付けして表示するため追跡が容易です。

次のページに同一ログの右側部分を表示しています

5-2. Web認証ログの表示例

■ Web認証ログ表示例(2)

OpenNET・Guard コントローラ Version 4.0

運用・保守 - Alaxala認証ログ

WEB認証ログ 検索 検索条件クリア MACアドレス毎に最新のみ表示 自動表示更新 CSV出力

191件見つかりました

	ホスト名	ユーザID	ユーザ名	IPアドレス	ポート	VLAN	番号	メッセージ
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	5	最大接続時間を超えたので、認証を解除しました。
92		user02	user02	192.168.1.1	0/4	200	6	MACアドレスエージングによって、MACアドレスが削除されたため、認証を解除しました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.200.1	0/4	200	2	クライアントは認証解除に成功しました。
				192.168.200.1			265	ログアウト要求を受け取りました。
92		user02	user02	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。
92		user02	user02	192.168.1.1	0/4	256	256	RADIUSサーバから受信したAcceptバケットのAttribute内容が解析できないため、ログインに失敗しました。
				192.168.1.1			264	ログイン要求を受け取りました。
92		user02	user02	192.168.1.1	0/4	256	256	RADIUSサーバから受信したAcceptバケットのAttribute内容が解析できないため、ログインに失敗しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	33	認証対象ポートがリンクダウンしたため、該当ポートでログインしていたすべてのユーザ認証を解除しました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	256	256	RADIUSサーバから受信したAcceptバケットのAttribute内容が解析できないため、ログインに失敗しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	20	RADIUS認証に失敗したため、認証できません。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.200.1	0/4	200	2	クライアントは認証解除に成功しました。
				192.168.200.1			265	ログアウト要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	5	最大接続時間を超えたので、認証を解除しました。
83	HP_NOTE	user01	user01	192.168.1.1	0/4	200	1	クライアントは認証に成功しました。
				192.168.1.1			264	ログイン要求を受け取りました。

ポート番号やVLAN番号が付いたログはポート番号およびVLAN番号を表示します。

一部ログを除き日本語日本語に変換され表示されます。

IPアドレスに関しては、認証時のIPアドレスが表示されませんので動的VLANの場合認証前のIPアドレスになるため注意してください。

※「認証ログ」を選んだ場合は、MAC認証とWeb認証をマージして表示します。

一部ログを除き日本語変換されます。