# 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

# 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

「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<br>RADIUSサーバ<br>DHCPサーバ<br>syslogサーバ | RedHat Enterprise Linux 5 | オープンネット・ガード<br>（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<br>Windows XPを使用 | ー | 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）

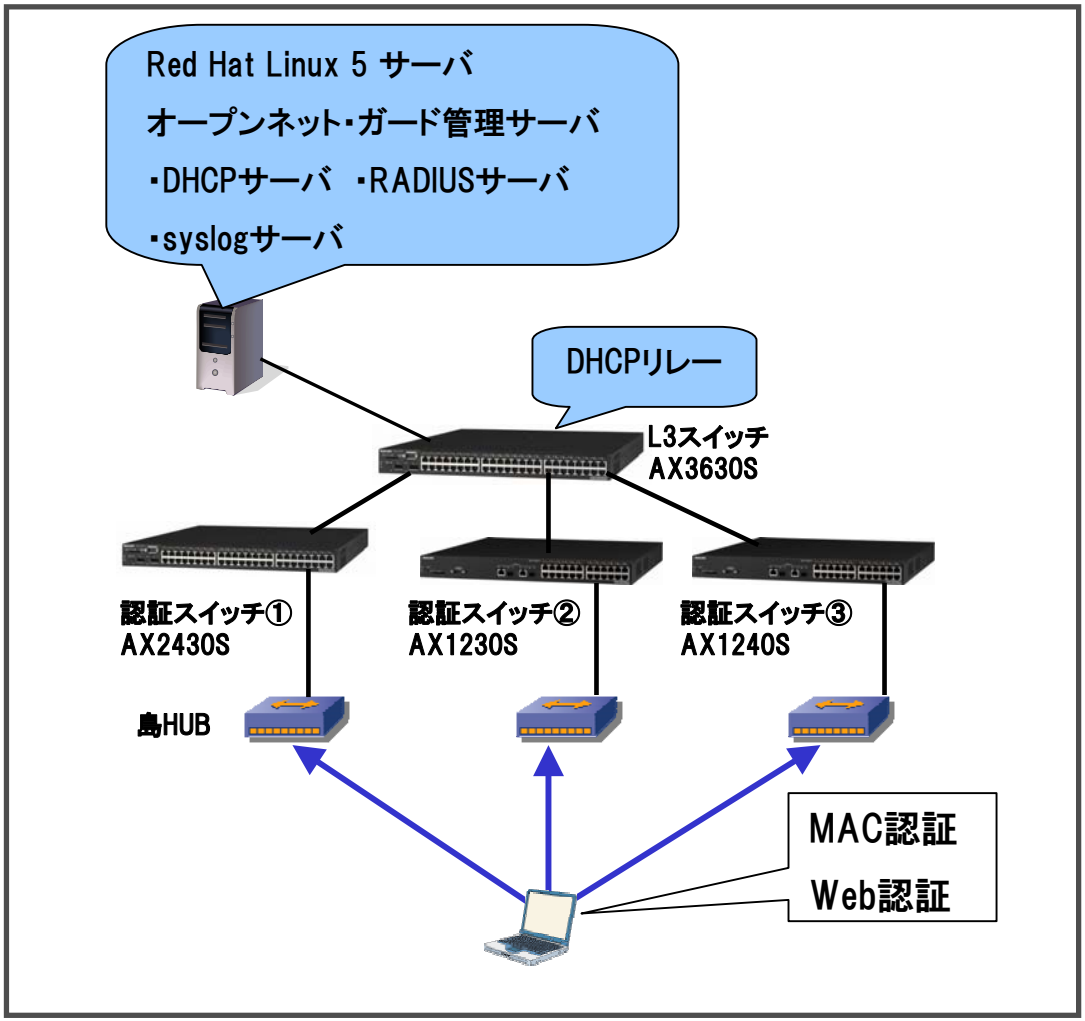
| 用途 | 機器名 | バージョン |
|---|---|---|
| L3スイッチ | AX3630S | 11.0 |
| 認証スイッチ① | AX2430S | 11.0 |
| 認証スイッチ② | AX1230S | 1.4.B |
| 認証スイッチ③ | AX1240S | 2.0 |

# 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)

・AlaxalA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事を示します。

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。

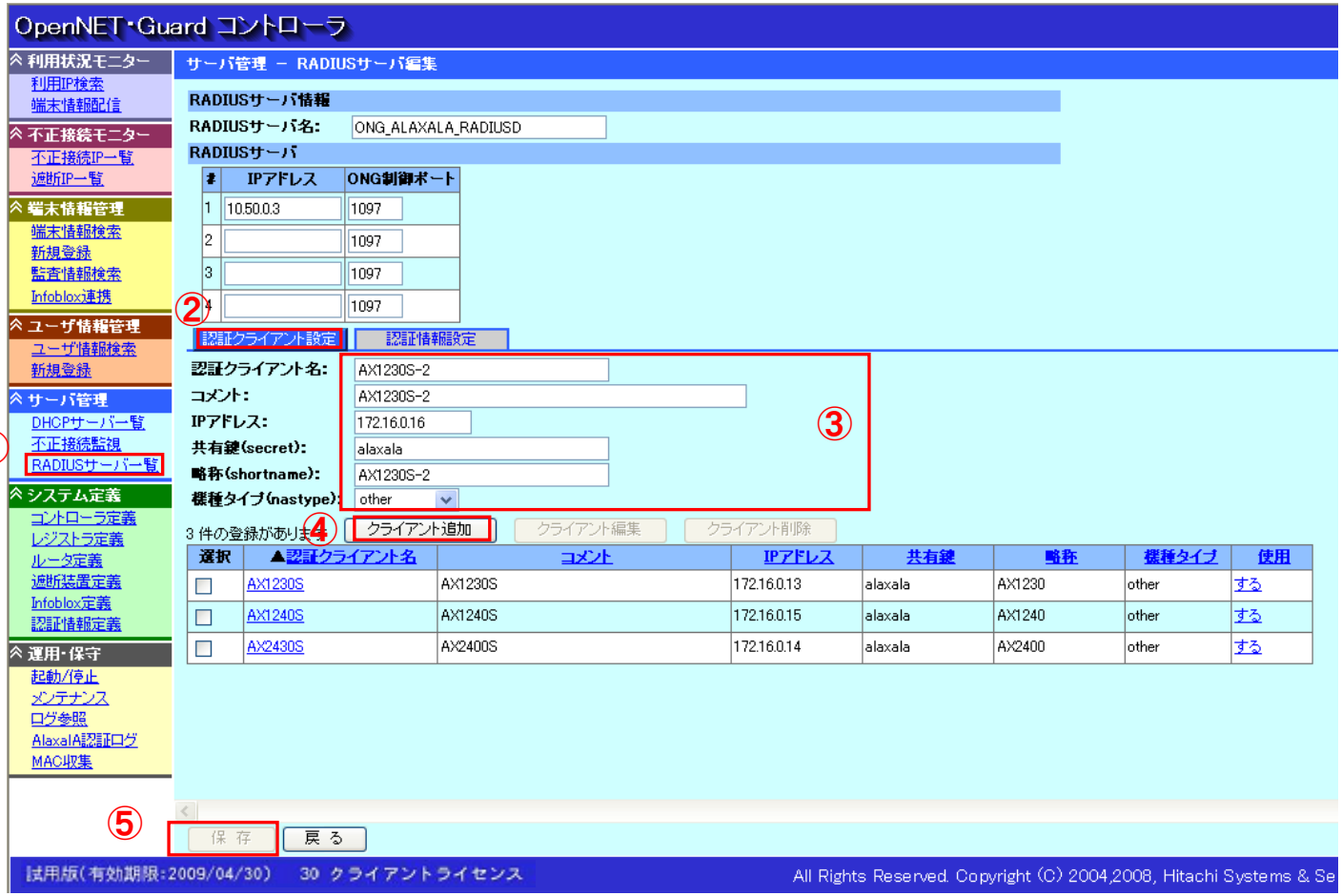
■AXシリーズの認証に関する設定

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/cntl/cntl_frame.php

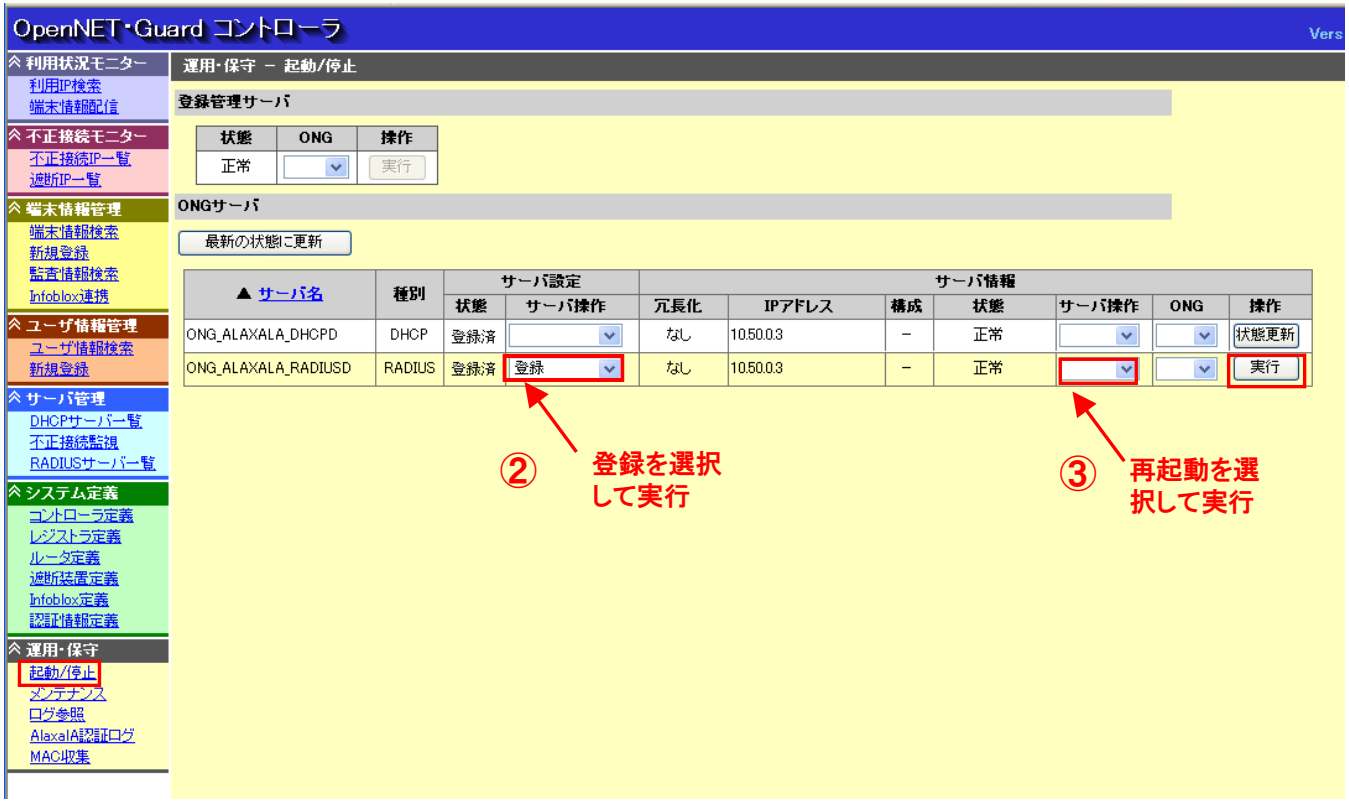



認証スイッチの登録は①RADIUSサーバー覧を開き、②認証クライアント情報を選択して、③の各種項目を入力後、④追加を行ない画面下の⑤保存を実行してください。

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

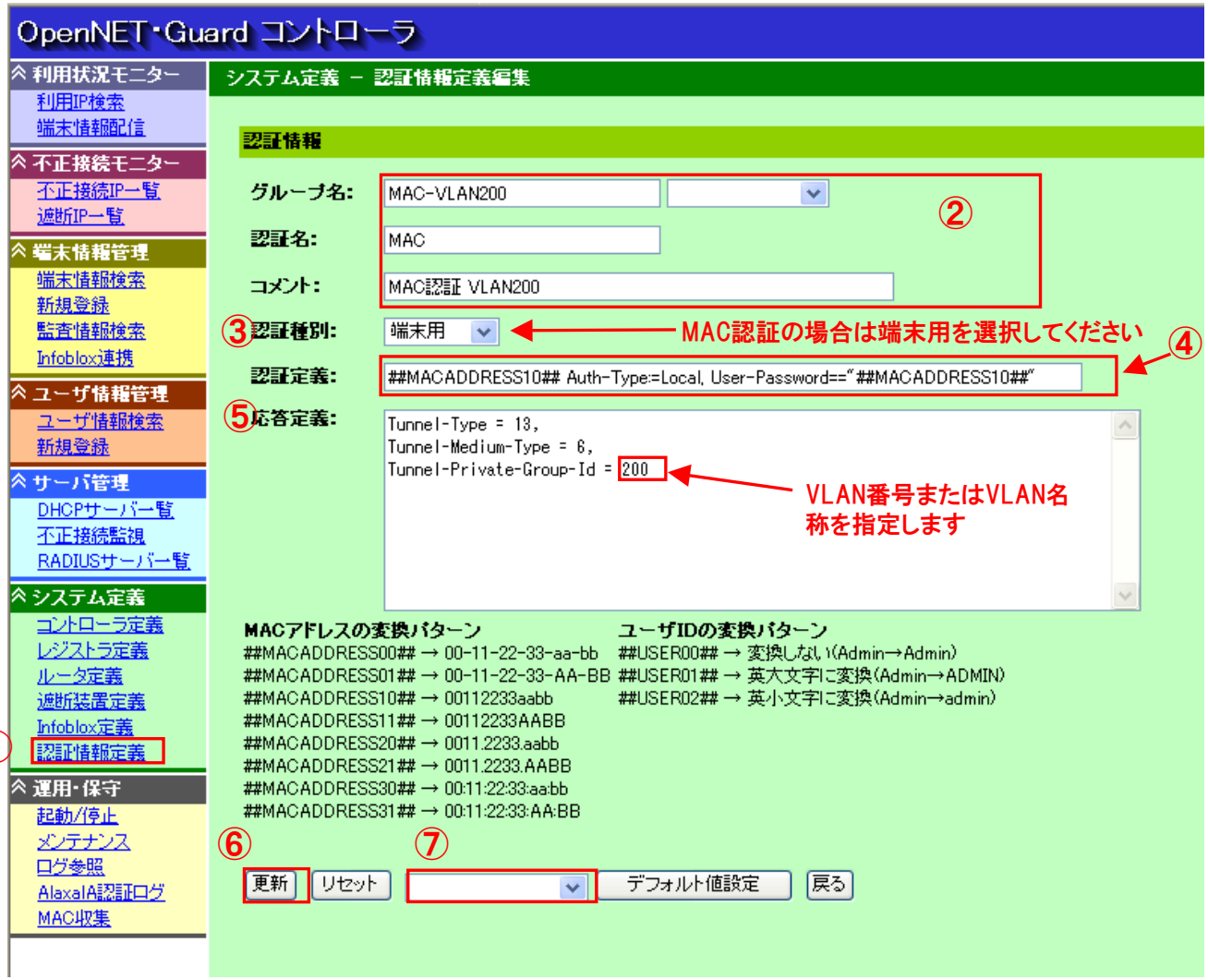
## ■(2) RADIUS設定情報の反映




(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)




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。

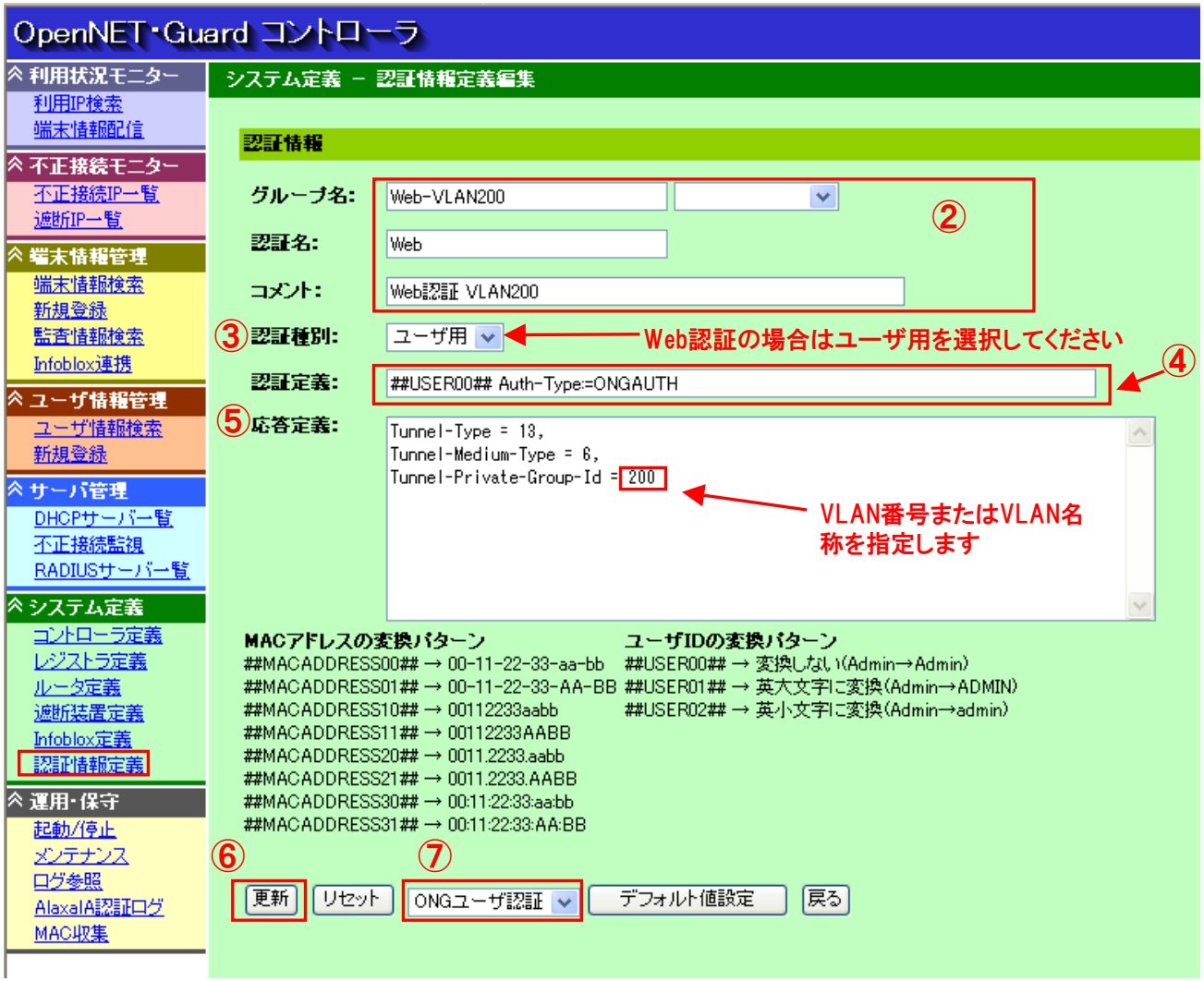
④「認証定義」にユーザ名、パスワードともにMACアドレスの場合は、認証定義を左記のように入力します。(⑦のプルダウンメニューで「MACアドレス認証」を選択し、「デフォルト値設定」ボタン押下で入力が可能。)
MAC認証のパスワードを認証スイッチのConfigで指定する場合は、Password=””にMAC認証のパスワードを入力してください。

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)




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)


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)


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 」



(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

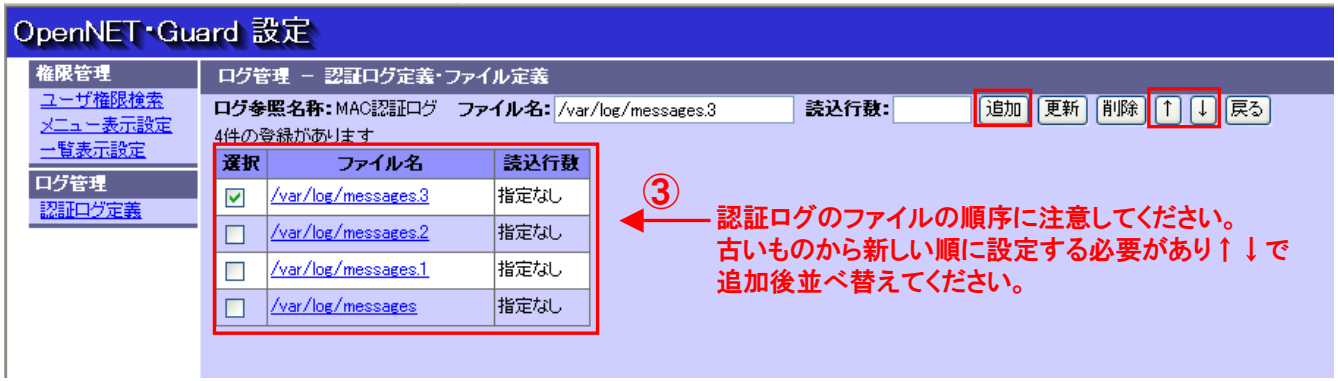
「利用状況モニター ― 端末情報配信 」から端末情報更新「登録」ボタンを押下するか、

「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。

# 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


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。

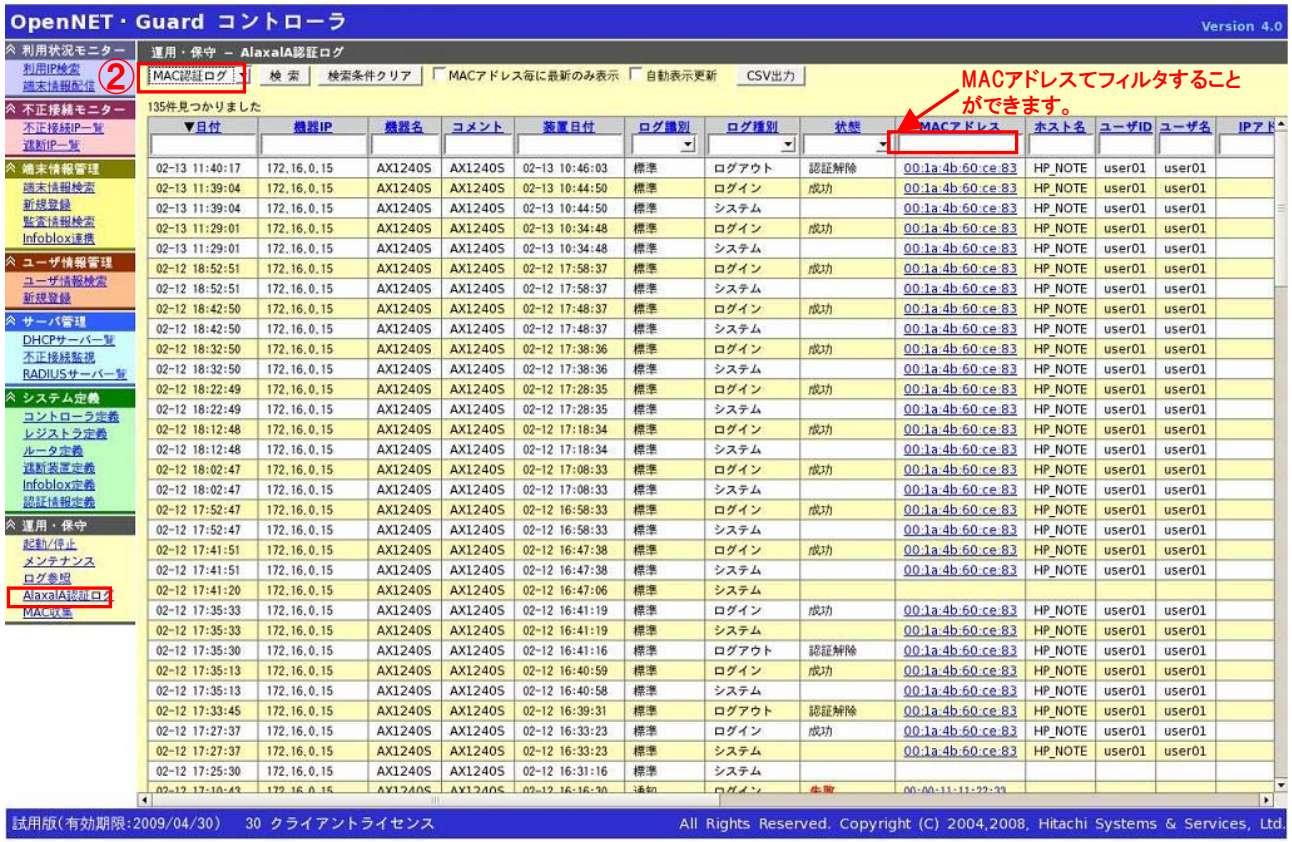
（初期値）

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)




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。

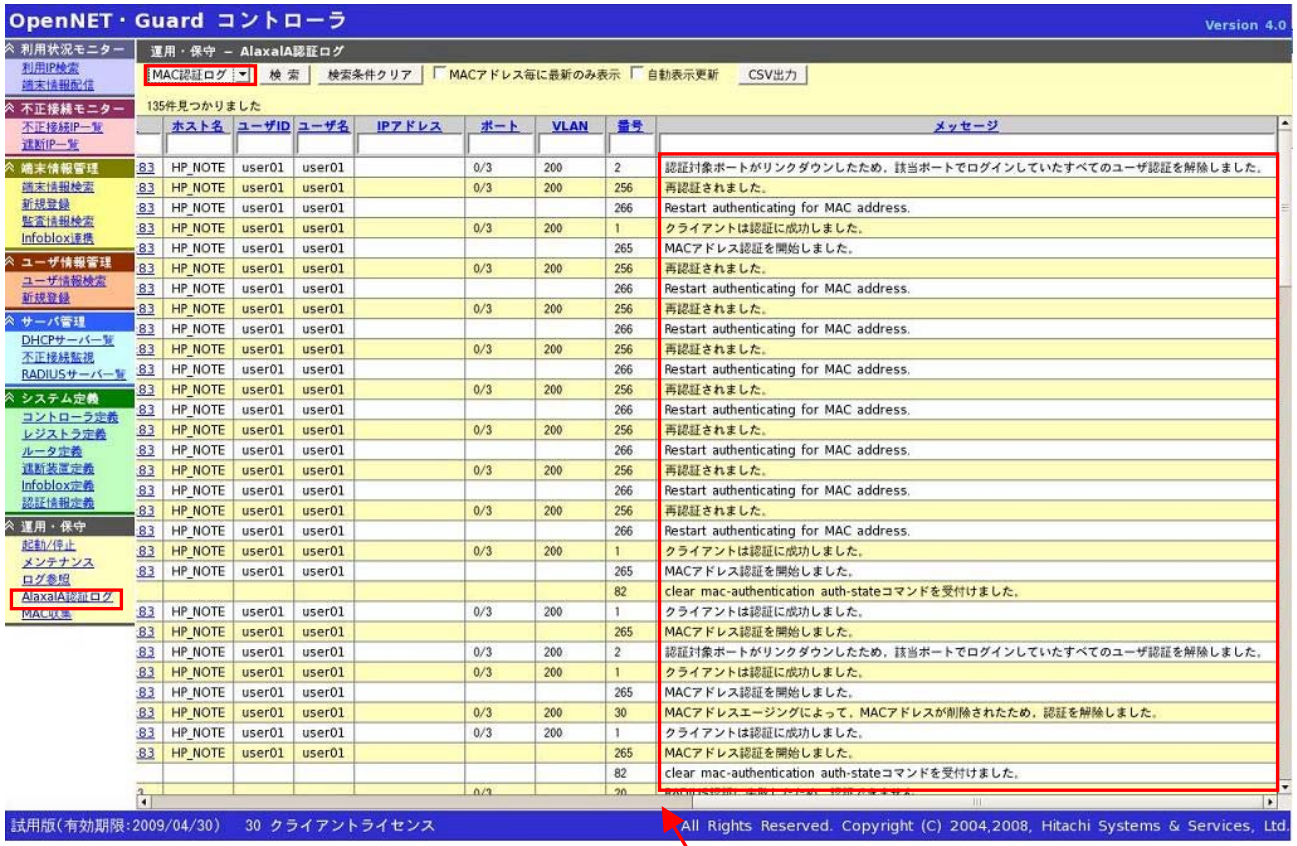
また、各表示項目をキーとしてログ表示のフィルタができます。

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)



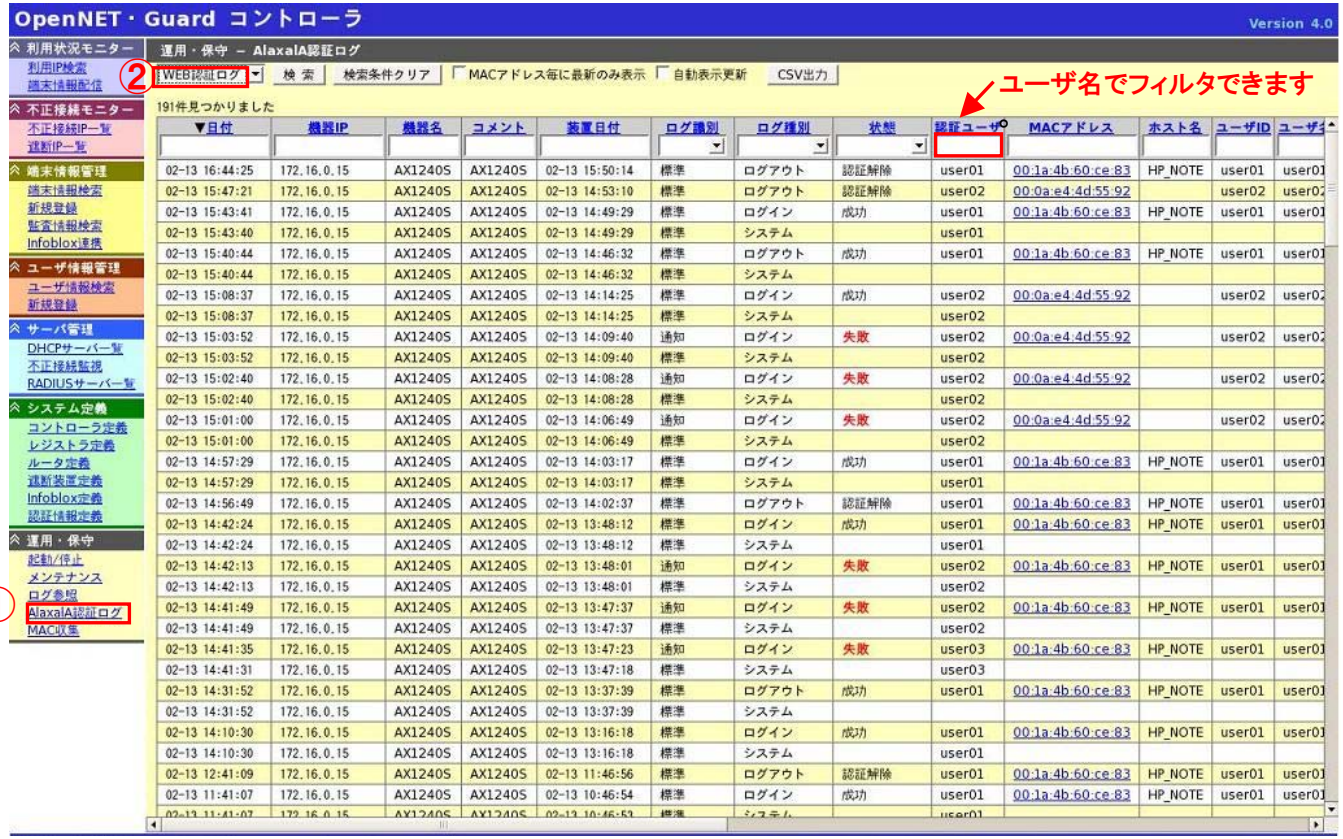

一部のログを除き、ログインやログアウト要因などを、日本語に変換して表示します。

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)




次のページに同一ログの右側部分を表示しています

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。

# 5-2. Web認証ログの表示例

## ■Web認証ログ表示例(2)


ポート番号やVLAN番号が付いたログはボート番号および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すので動的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。