RADIUS サーバ設定ガイド
オープンネット・ガード編

初版

はじめに

本ガイドは、AX シリーズでサポートしている認証機能を用いたシステム構築において、RADIUS サーバに株式会社日立システムアンドサービス製のオープンネット・ガードを使用する場合の設定方法を示します。

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/techinfo/manual/index.html）
・オープンネット・ガード　インストールマニュアル　V4.0　SAS-M-ONGISM-40
・オープンネット・ガード　運用マニュアル　V4.0　SAS-M-ONGOPM-40
・オープンネット・ガード　ユーザーズマニュアル　V4.0　SAS-M-ONGUSM-40
・オープンネット・ガードのウェブサイト（http://www.hitachi-system.co.jp/ong/index.html）

本ガイド使用上の注意事項

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。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。
Red Hat製品に関する詳細はRed Hat社のHP等をご参照下さい。
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ご参照下さい。
本資料の内容は、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

・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。
・Linuxは、Linus Torvaldsの米国およびその他の国における登録商標または商標です。
・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。
・Red Hatは、米国およびその他の国における米国Red Hat, Incの登録商標または商標です。
・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

- AX1230S (Ver1.4.D)
- AX1240S (Ver2.1)
- AX2430S (Ver11.1.A)
- AX3630S (Ver11.1.A)
- Windows XP SP2

目次

1. 概要

1.1 概要

本資料では認証スイッチに AX シリーズ、認証端末に Windows XP を使用し、オープンネット・ガードを RADIUS、ユーザデータベースとして下記認証方式を使用したシステムを構築するための設定方法を記載しています。

認証方式

- Web 認証
- MAC 認証
- ログイン認証（装置ログイン）

使用方法

本資料は、認証方式毎に設定方法を記載しています。目次を参照して構成する認証方式の項目から設定してください。

AX のコンフィグレーションに関して本資料では詳細な説明は記載していません。AX の設定は完了している事を前提にサーバ、認証端末の設定方法を記載しています。各認証方式に関連するコンフィグレーションは AX のマニュアルや認証ソリューションガイド_3 章(認証ネットワークの構築)を参照してください。

1.2　設定例環境

1.2.1　使用機器一覧と AX コンフィグレーション

使用機器一覧

RADIUS：オープンネット・ガード　V4.0

Client：Windows XP

Authenticator：AX1240S(Ver2.1) / AX2430S(Ver11.1.A)

L3switch：AX3630S（Ver11.1.A）

AX コンフィグレーション設定例

AX1240S のコンフィグレーション

```
hostname "AX1240S"
!
vlan 1
   name "VLAN0001"
!
vlan 30 mac-based
!
vlan 31 mac-based
!
vlan 100
!
vlan 200
!
spanning-tree disable
spanning-tree mode pvst
!
interface fastethernet 0/24
   switchport mode mac-vlan
   switchport mac vlan 30-31
   switchport mac native vlan 100
   web-authentication port
   mac-authentication port
   authentication ip access-group Auth
   authentication arp-relay
!
interface gigabitethernet 0/25
   media-type auto
   switchport mode trunk
   switchport trunk allowed vlan 30,31,100,200
!
interface vlan 1
!
interface vlan 30
   ip address 192.168.30.253 255.255.255.0
!
interface vlan 31
   ip address 192.168.31.253 255.255.255.0
!
interface vlan 100
ip address 192.168.100.253 255.255.255.0
!
interface vlan 200
ip address 192.168.200.253 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.200.254
!
▲mac-authentication system-auth-control
▲mac-authentication id-format 1
!
■   web-authentication system-auth-control
■   web-authentication ip address 10.10.10.10
!
service dhcp vlan 100
!
ip dhcp pool "VLAN100"
   network 192.168.100.0/24
   lease 0 0 0 10
   default-router 192.168.100.254
   dns-server 192.168.10.1
!
▼logging host 192.168.10.1
★radius-server host 192.168.10.1 key "alaxala"
◆aaa authentication login default group radius local
▲aaa authentication mac-authentication default group radius
■aaa authentication web-authentication default group radius
!
line vty 0 0
!
```

■Web 認証を行うためのコンフィグレーション

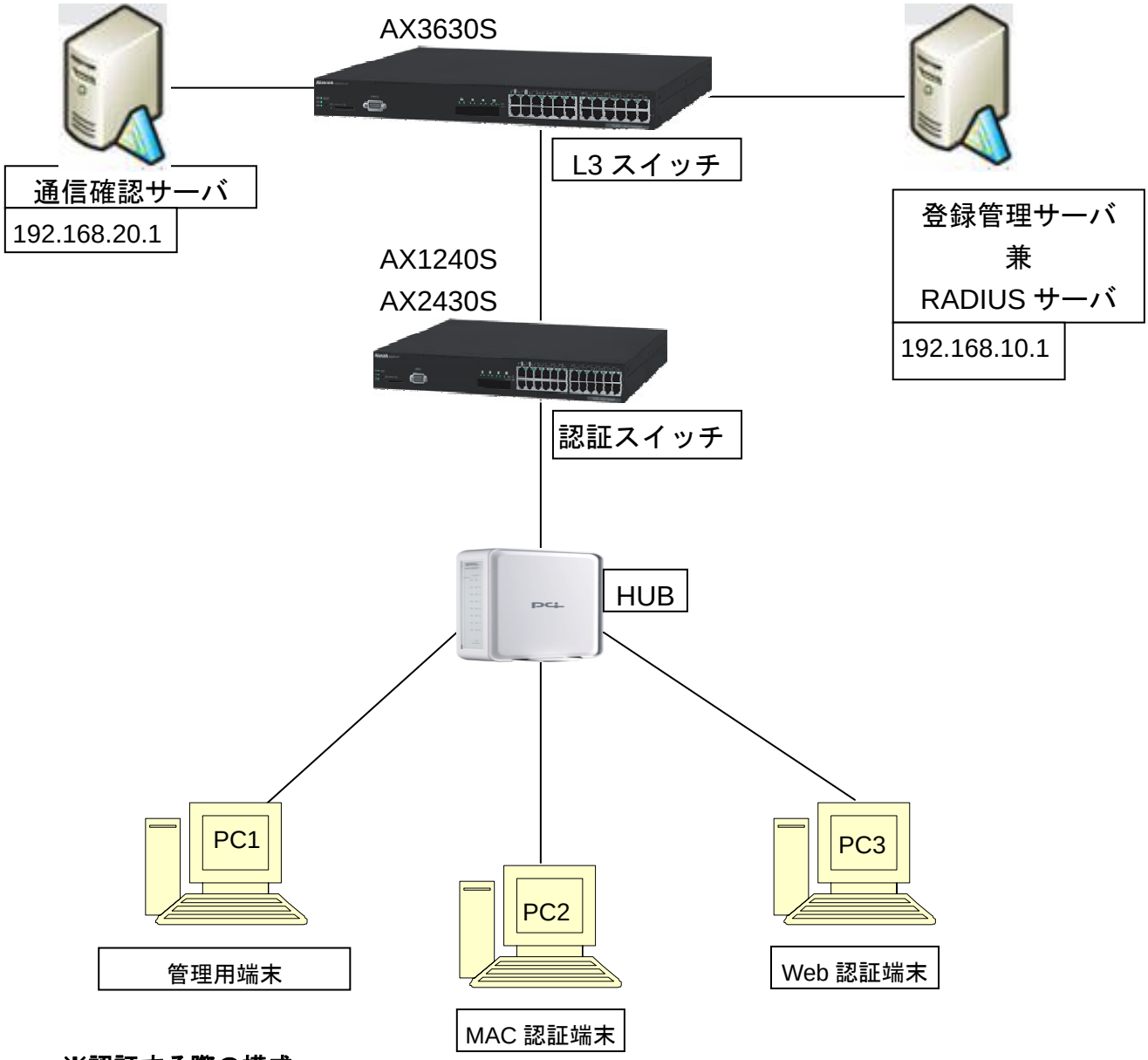
▲MAC 認証を行うためのコンフィグレーション

◆ログイン認証を行うためのコンフィグレーション

★RADIUS サーバ関連のコンフィグレーション（各認証方式共通）

▼Syslog サーバへログ情報を転送するためのコンフィグレーション

1.2.2　設定例のネットワーク構成図



※認証する際の構成

ユーザ名：user01・user02

認証後の VLAN：VLAN30、31

Windows XP SP2

2. オープンネット・ガードの構成

2.1 準備

インストールするサーバを用意してください。
なお、オープンネット・ガードの前提OSは以下となっております。

No.	OS
1	RedHat Enterprise Linux ES 4.5 (ES 4 Update 5) ,4.7 (ES 4 Update 7)
2	RedHat Enterprise Linux 5.1,5.2,5.3

上記OSのメーカサポートがあるハードウェアを選定ください。
ハードウェアの前提スペックは以下になります。

	前提スペック
CPU	Pentium4以上
メモリ	1GB以上
HDD	40GB以上

2.2 サーバへのインストール

インストール方法については、オープンネット・ガードのインストールマニュアルをご参照下さい。

3. オープンネット・ガードの設定

3.1 ユーザの登録

オープンネット･ガードのコントローラにログインします。

（1）Web ブラウザを起動してアドレス欄に
「http://192.168.10.1/cntl/cntl_frame.php」
を入力します。

（2）ユーザ ID とパスワードを入力してログインします。
「Admin」権限を持っているユーザのみログインすることができます。

ディフォルトでは、ユーザＩＤ：admin、パスワード：admin が「Admin」権限ユーザとして設定されています。ログイン後、パスワードを変更する等のセキュリティ対策を実施してください。

（3）ユーザの新規登録を行います。

「ユーザ情報管理」－「新規登録」メニューをクリックしますと、以下の画面を表示します。ここで登録するユーザは、MAC アドレスの登録する際や、Web 認証を使用する際に使用します。

また、ユーザ情報は、CSV ファイルからの一括登録を行うことが出来ます。

「ユーザ情報管理」－「ユーザ情報検索」メニューをクリックしますと、以下の画面を表示します。

「登録用ファイル：」の項目に CSV ファイル名を指定します。（「参照」ボタンをクリックして、指定することも可能です）

登録情報種別選択欄に「ユーザ情報」を指定します。

注）CSVの形式については、「オープンネット・ガード　ユーザーズマニュアル
4.1.1 ユーザ情報 (1) ユーザ情報一括登録」 をご参照下さい。

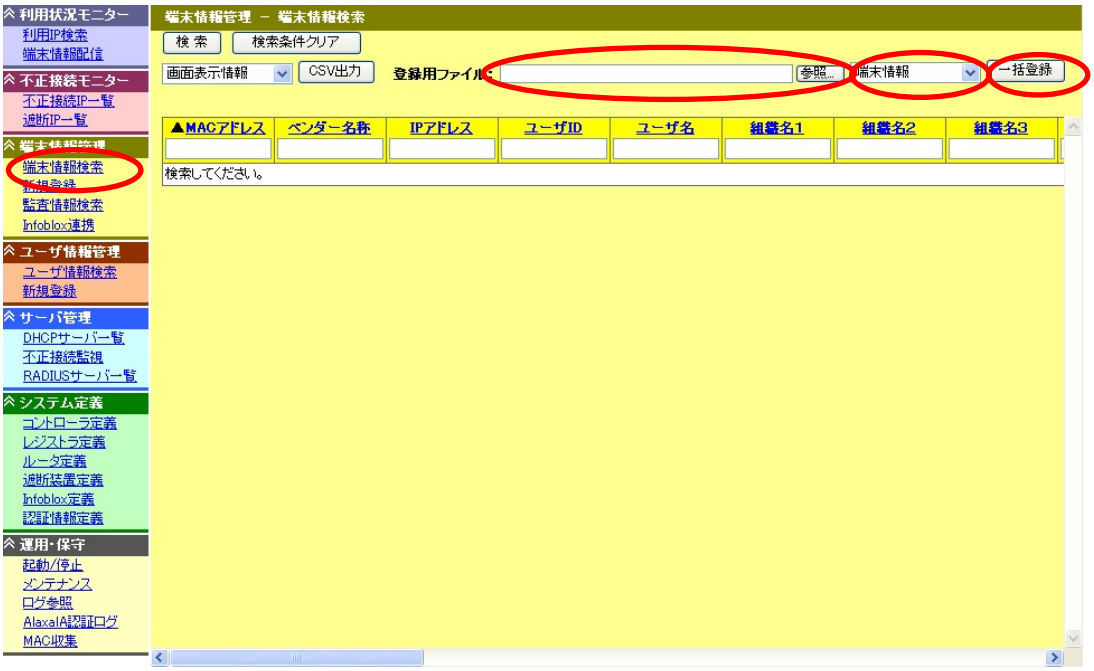
CSV ファイルを指定後、「一括登録」ボタンをクリックします。

3.2 MAC アドレスの登録

「端末情報管理」－「新規登録」メニューをクリックしますと、以下の画面を表示します。ここで AX にて認証を行う MAC アドレスを登録します。

また、MAC アドレス情報は、CSV ファイルからの一括登録を行うことが出来ます。

「端末情報管理」－「端末情報検索」メニューをクリックしますと、以下の画面を表示します。



「登録用ファイル：」の項目に CSV ファイルを指定します。（「参照」ボタンをクリックして、指定することも可能です）

登録情報種別選択欄に「端末情報」を指定します。

注）CSV ファイルは、MAC 収集機能を使用して作成することも可能です。
MAC収集機能については、「8.2 MAC収集機能」をご参照下さい。

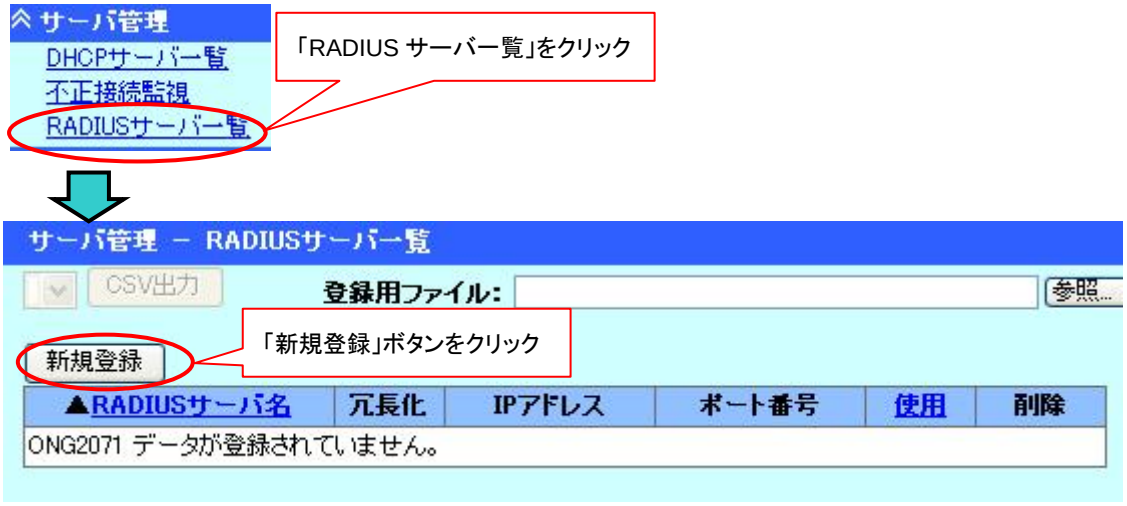
注）CSVの形式については、「オープンネット・ガード　ユーザーズマニュアル
4.1.2 端末情報 (2) 端末情報」 をご参照下さい。

CSV ファイルを指定後、「一括登録」ボタンをクリックします。

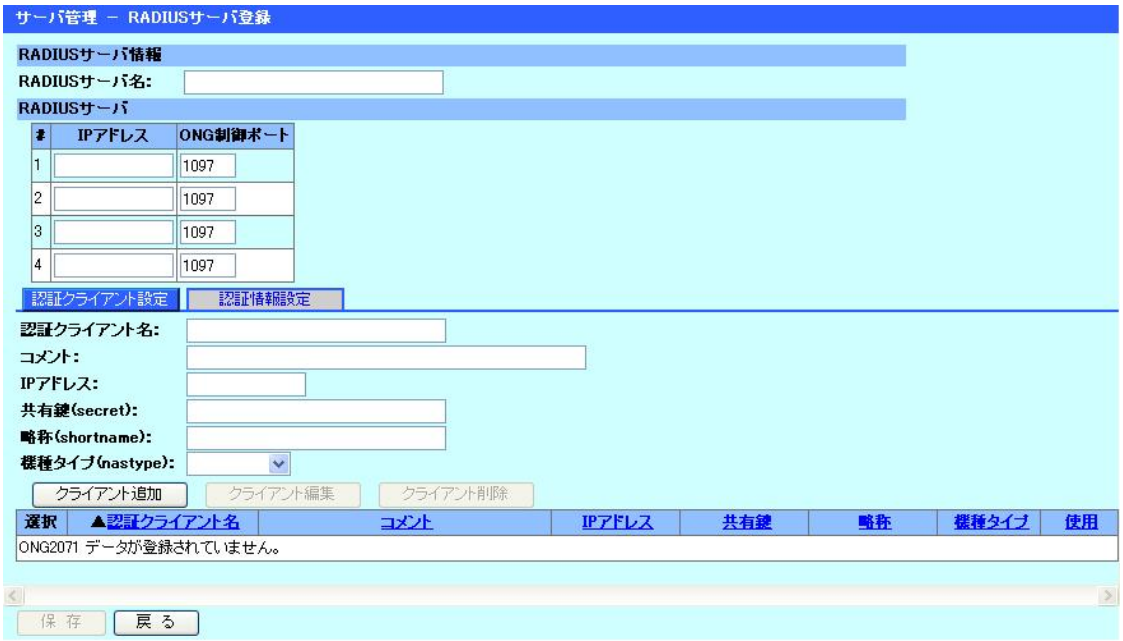
3.3 認証スイッチの登録

左のメニューから「RADIUS サーバー覧」をクリックし、「RADIUS サーバー覧」画面を開きます。

画面左上の「新規登録」ボタンをクリックしてください。



「RADIUS サーバ登録」画面が開きます。RADIUS サーバ情報、認証クライアント情報を入力します。各入力項目の詳細は「オープンネット・ガード　ユーザーズマニュアル　2.1.6 サーバ管理」をご参照下さい。



(1) RADIUS サーバ情報設定

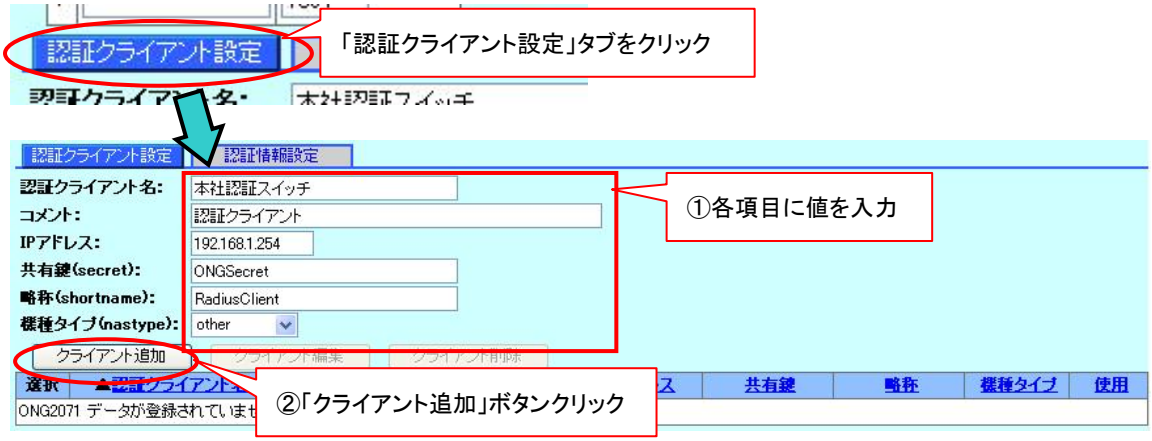
RADIUS サーバ情報の設定を行います。RADIUS サーバ名に設定する名称を指定してください。

(2) RADIUS サーバ設定

RADIUS サーバの設定を行います。IP アドレスおよび ONG 制御ポートに適宜値を入力してください。

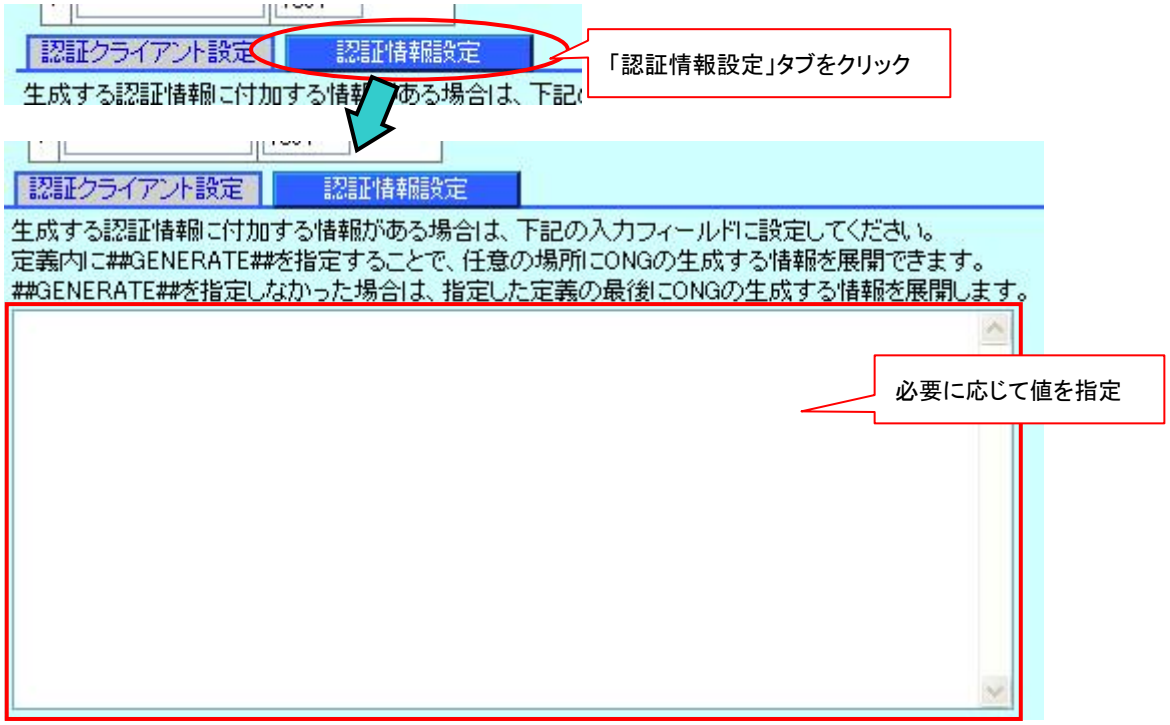
(3) 認証クライアント設定

認証クライアントの設定を行います。「認証クライアント設定」タブをクリックしタブをアクティブにします。
各入力欄に適宜値を指定し、「クライアント追加」ボタンをクリックしてください。



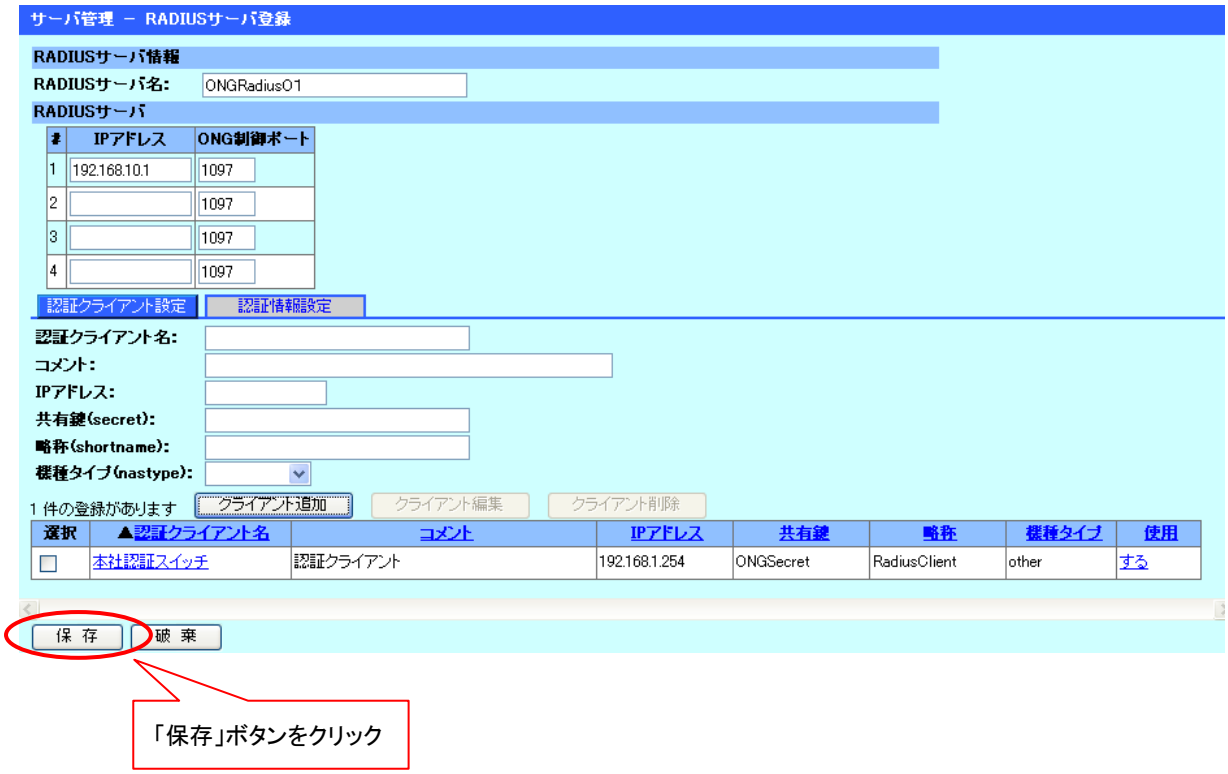
(4) 認証情報設定

認証情報の設定を行います。生成する認証情報に付加する情報がある場合は適宜値を指定してください。

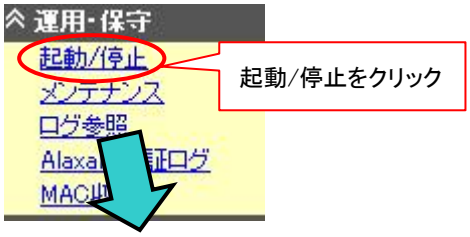


(5) RADIUS サーバの登録

全ての設定が完了したら「保存」ボタンをクリックし、RADIUS サーバ情報を登録してください。



RADIUS サーバ情報の設定変更を行った場合、RADIUS 設定の登録および RADIUS サービスの再起動を行う必要があります。
左のメニューから「起動/停止」をクリックし、「起動/停止」画面を開いてください。

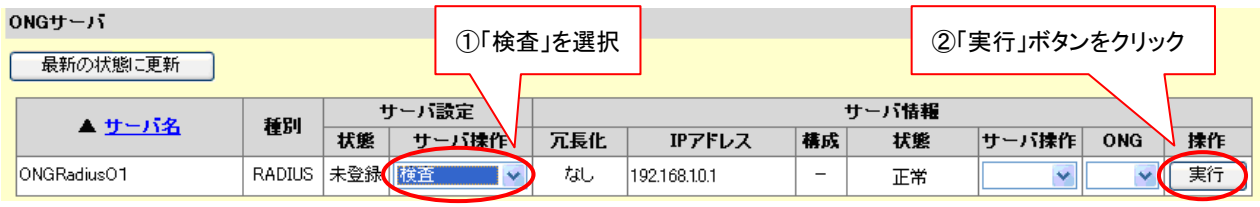


RADIUS サーバに関連するサービスの再起動を行います。
FreeRADIUS サービスを停止した場合、RADIUS 認証ができません。
オープンネット・ガード（RADIUS サーバ）のサービスを停止した場合、RADIUS 情報の登録、認証情報の配信などができません。

RADIUS サーバを登録した直後に本画面を表示すると、RADIUS サーバの状態が、「不明」となります。その場合、「最新の状態に更新」ボタンをクリックして、状態が「正常」になることを確認してください。

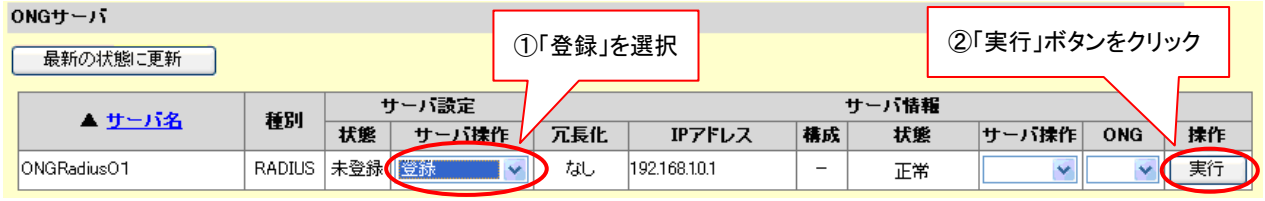
(6) RADIUS 設定ファイル検査

まず、設定内容の妥当性チェックを行います。「サーバ設定」－「サーバ操作」欄のプルダウンから「検査」を選択してください。選択すると「状態更新」ボタンが「実行」ボタンに変わります。「実行」ボタンをクリックしてください。



(7) RADIUS 設定ファイル登録

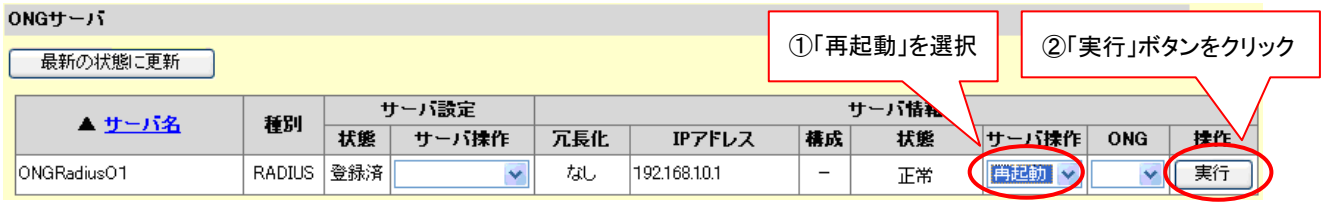
検査が正常終了した後、RADIUS への登録作業を行います。「サーバ設定」－「サーバ操作」欄のプルダウンから「登録」を選択します。選択すると「状態更新」ボタンが「実行」ボタンに変わります。「実行」ボタンをクリックしてください。



登録処理が完了すると、「サーバ設定」欄の「状態」項目が「登録済」となります。

(8) FreeRADIUS サービスの再起動

FreeRADIUS サービスの再起動を行います。
「サーバ情報」－「サーバ操作」欄のプルダウンから「再起動」を選択します。選択すると「状態更新」ボタンが「実行」ボタンに変わります。「実行」ボタンをクリックします。



検査・登録および、再起動時にエラーが発生すると以下のような実行結果画面が表示されますので、エラー内容を確認してください。また、冗長化構成時にどちらかのサーバがダウンしている場合や、通信できない場合はエラーとなりますので、両サーバの状態を確認して処理を行ってください。

3.4　認証ログの登録

認証ログを登録することにより、AlaxalA ログを一覧表形式で参照することができます。なお、前提として、以下の設定が必要となります。

(1)AX 側

・syslog サーバとして、ONG サーバを指定

詳細は、「1.2.1 使用機器一覧と AX コンフィグレーション」の「Syslog サーバへログ情報を転送するためのコンフィグレーション」をご参照下さい。

(2)ONG サーバ側

・AX から syslog を受信するように設定。

詳細は、「オープンネット・ガード　インストールマニュアル　5.2.2 Syslog に出力する方法」をご参照下さい。

・AX の最終認証日を、オープンネット・ガードのデータベースに反映する設定。

詳細は、「オープンネット・ガード　運用マニュアル　4.2 CRON の設定」をご参照下さい。

3.4.1　認証ログの追加・編集・削除

ONG 設定画面にログインします。

（１） Web ブラウザを立ち上げ、アドレス欄に
「http://192.168.10.1/setup/」を入力します。

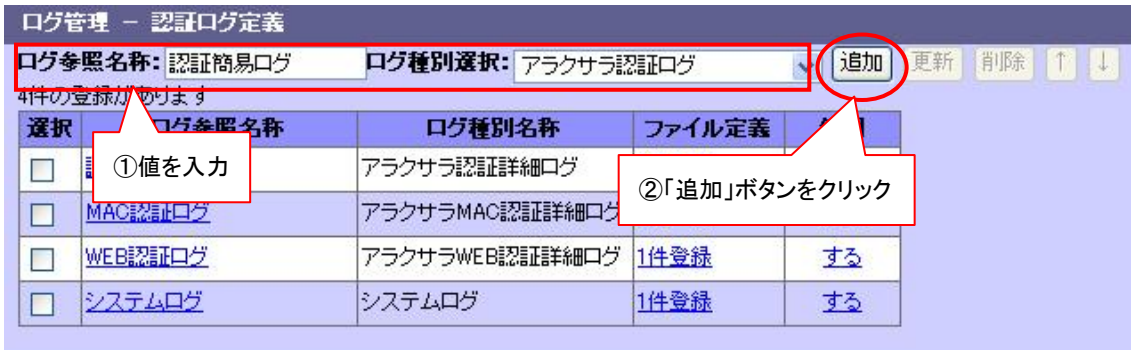
（２） ユーザ ID とパスワードを入力しログインします。
インストール時に Apache 認証設定で指定したユーザ ID、パスワードを入力します。

ユーザ権限設定は、ONG 設定より行います。項目の詳細については「オープンネット・ガード ユーザーズマニュアル 2.3　ONG 設定」をご参照下さい。

ログイン後、「認証ログ定義」をクリックします。

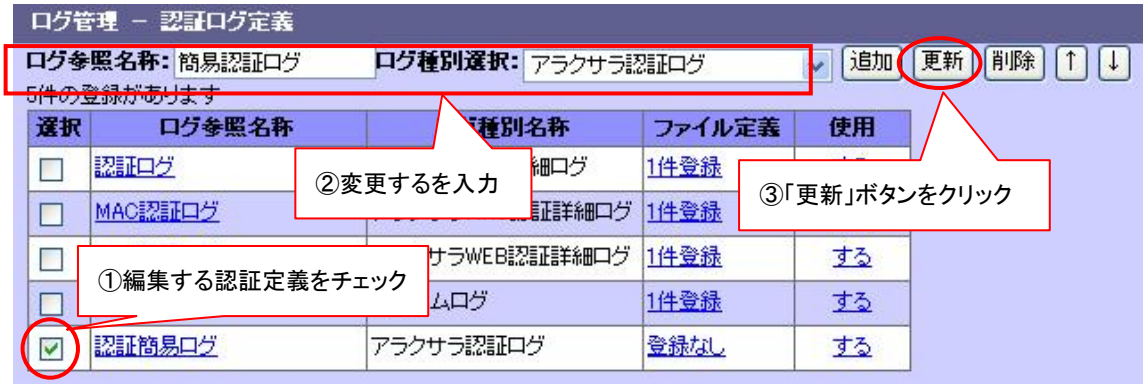
(1)　　認証ログ定義の追加

「認証ログ定義」画面のログ参照名称、ログ種別選択に適宜値を指定し、「追加」ボタンをクリックします。



(2)　　認証ログ定義の編集

「認証ログ定義」画面の認証ログ定義一覧から、編集したい認証ログ定義の選択項目を有効にします。ログ参照名称、ログ種別選択に変更後の値を指定し、「更新」ボタンをクリックします。



認証ログ定義の削除

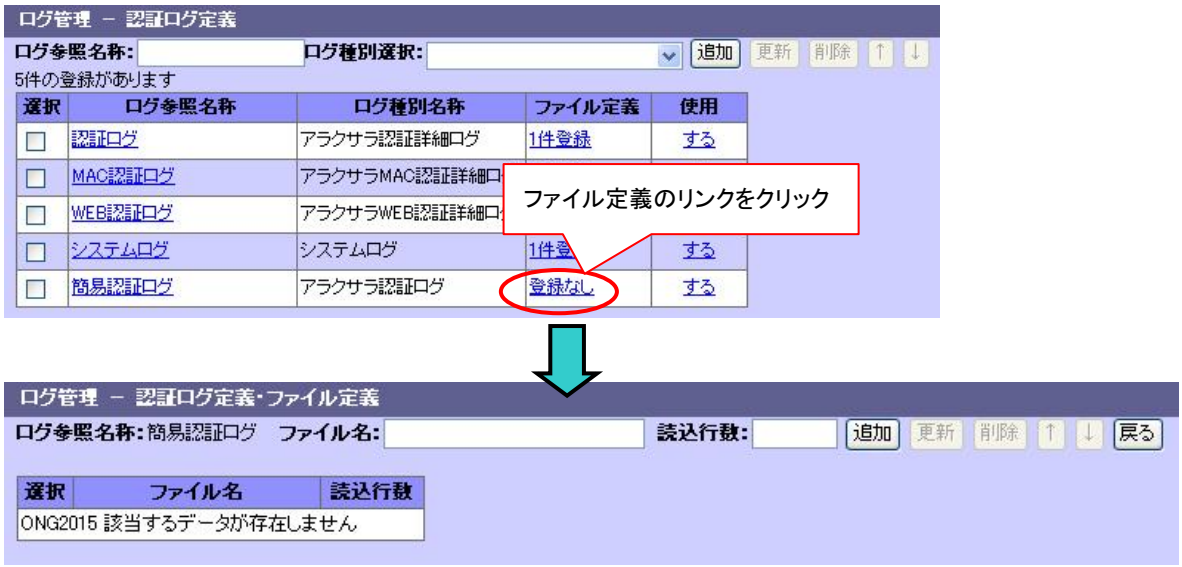
「認証ログ定義」画面の認証ログ定義一覧から、削除したい認証ログ定義の選択項目を有効にし、削除ボタンをクリックします。

3.4.2　ファイル定義の追加・編集・削除

認証ログ定義にファイル定義の追加・編集・削除を行います。認証ログ定義にファイル定義を追加することで、ログを検索するファイルを指定します。

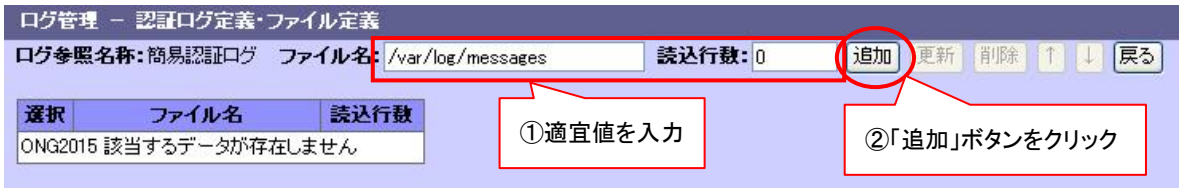
「認証ログ定義」の認証ログ定義一覧からファイル定義を追加・編集・削除を行う認証ログ定義のファイル定義項目のリンクをクリックし、「ファイル定義」画面を表示します。

項目の詳細については「オープンネット・ガード　ユーザーズマニュアル 2.3.3 ログ管理」をご参照下さい。



(1)　　ファイル定義の追加

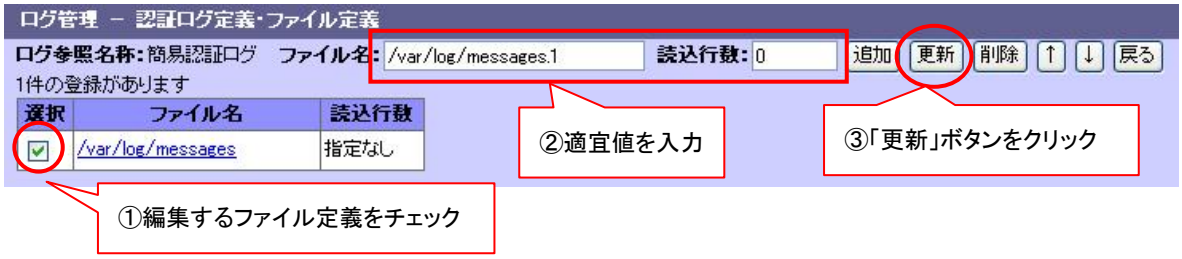
「認証ログ定義・ファイル定義」画面のファイル名および読込行数に適宜値を指定し、「追加」ボタンをクリックします。



注）認証ログファイルは、古いものから順に追加する必要があります。追加後も「↑↓」ボタンで並べ替えすることが可能です。

(2) ファイル定義の編集

「認証ログ定義・ファイル定義」画面のファイル定義一覧から編集するファイル定義の選択項目をチェックします。ファイル名および読込行数に変更する値を指定し、「更新」ボタンをクリックしてください。



(3) ファイル定義の削除

「認証ログ定義・ファイル定義」画面のファイル定義一覧から削除するファイル定義の選択項目をチェックし、「削除」ボタンをクリックします。

4. MAC 認証の設定

4.1 認証情報の設定

MAC 認証を実施する際の認証情報の設定について以下に示します。

4.1.1 認証情報定義作成

オープンネット･ガードのコントローラにログインします。

（１）Web ブラウザを起動してアドレス欄に
「http://192.168.10.1/cntl/cntl_frame.php」
を入力します。

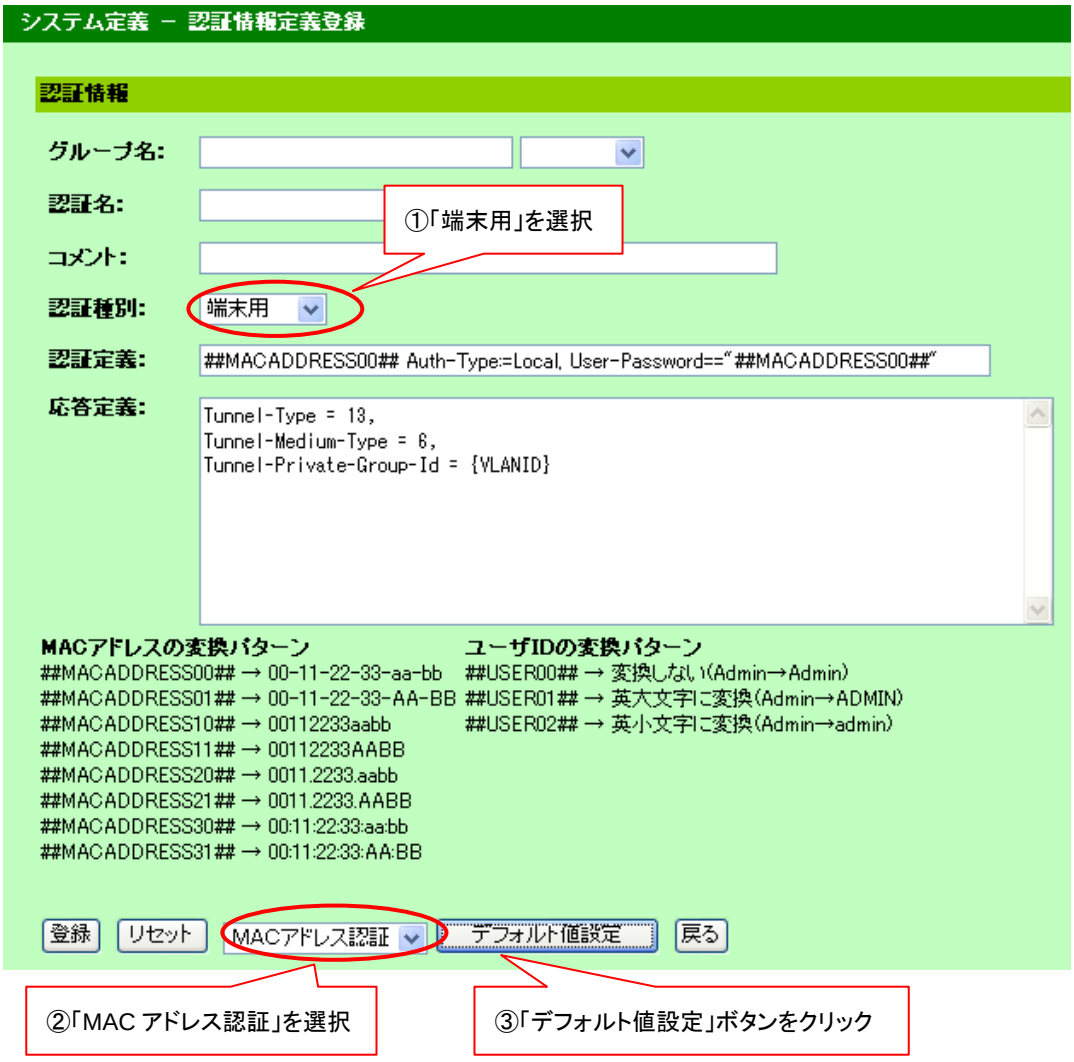
（２）ユーザ ID とパスワードを入力してログインします。
「Admin」権限を持っているユーザのみログインすることができます。

（３）RADIUS 認証で使用する認証情報定義を追加します。
左のメニューから「認証情報定義」をクリックし、「認証情報定義」画面を表示してください。
画面左上の「新規登録」ボタンをクリックし、「認証情報定義登録」画面を表示します。

RADIUS サーバで使用する認証用データベースファイルの記述方式を定義します。
導入環境に合わせて認証定義および応答定義項目に適宜値を指定してください。その他各項目に適宜値を指定し、「登録」ボタンをクリックします。

デフォルト値を自動入力するには、認証種別に「端末用」、画面下部の選択欄に「MAC アドレス認証」を選択し、「デフォルト値設定」をクリックします。

項目の詳細については「オープンネット・ガード　ユーザーズマニュアル　2.1.7 システム定義」をご参照下さい。



●固定 VLAN 環境での MAC 認証定義　例

※デフォルト値を利用する際は、自動入力された以下の値を修正してください。
- 認証定義：”##～##”で記述されている変換パターン
- 応答定義：削除してください。

認証定義について AX2400S/AX3600S シリーズの変換パターンは##MACADDRESS10##となっており変更不可であるため、AX1200S のシリーズのコンフィグレーションで下記コマンドを投入して統一する事をお勧めします。

(config): mac-authentication id-format 1

●動的 VLAN 環境での MAC 認証定義　例

※デフォルト値を利用する際は、上記画面を参考に自動入力された以下の値を修正してください。

・認証定義：”##～##”で記述されている変換パターン
・応答定義：”Tunnel-Private-Group-Id”の値

認証定義について AX2400S/AX3600S シリーズの変換パターンは##MACADDRESS10##となっており変更不可であるため、AX1200S のシリーズのコンフィグレーションで下記コマンドを投入して統一する事をお勧めします。

(config): mac-authentication id-format 1

●動的 VLAN 環境での MAC 認証定義（マルチステップ認証）例

※デフォルト値を利用する際は、上記画面を参考に自動入力された以下の値を修正してください。
・認証定義：”##～##”で記述されている変換パターン
・応答定義：”Tunnel-Private-Group-Id”の値（行末に”,”も追加ください。）

また、応答定義に“Filter-ID”を追加し、以下を設定してください。
- IEEE802.1X 認証の場合：“@@1X-Auth@@”
- Web 認証の場合：“@@Web-Auth@@”
- IEEE802.1X 認証もしくは、Web 認証の場合：“@@MultiStep@@”

ただし、オープンネット・ガードを、ユーザ認証の際の RADIUS サーバとして使用する場合は、Web 認証のみ使用可能です。IEEE802.1X 認証を使用する場合はオープンネット･ガードとは別の RADIUS サーバを用意してください。

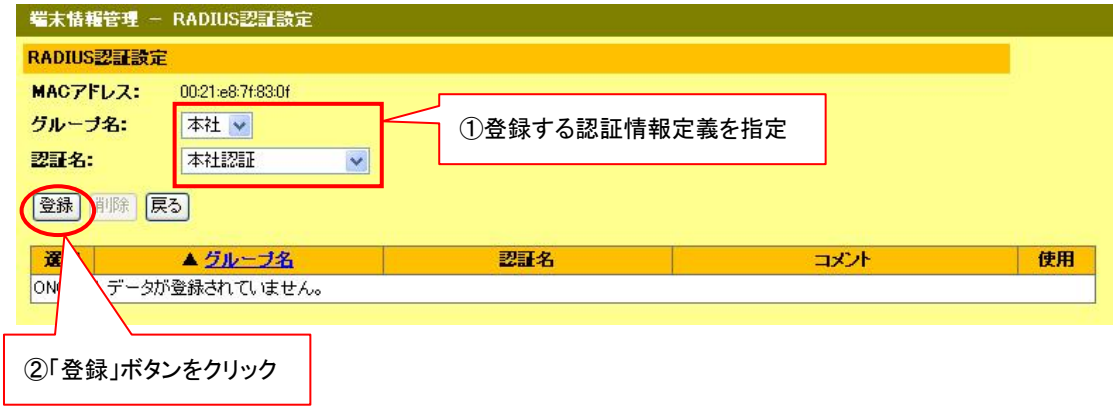
4.1.2 MAC アドレスと認証情報の関連付け

MAC 認証を行う MAC アドレスと、認証情報の関連付けを行います。

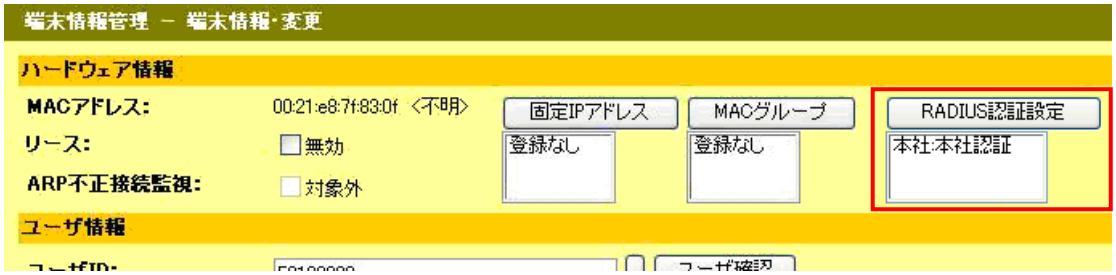
左のメニューから「端末情報検索」をクリックし、「端末情報検索」画面を表示します。端末情報一覧からRADIUS認証設定を登録する端末のMACアドレスをクリックし、「端末情報･変更」画面を表示します。

「端末情報・変更」画面右上部分の「RADIUS 認証設定」ボタンをクリックし、「RADIUS 認証設定」画面を表示します。

「グループ名」、「認証名」項目に登録する「認証情報定義」を指定し、「登録」ボタンをクリックします。

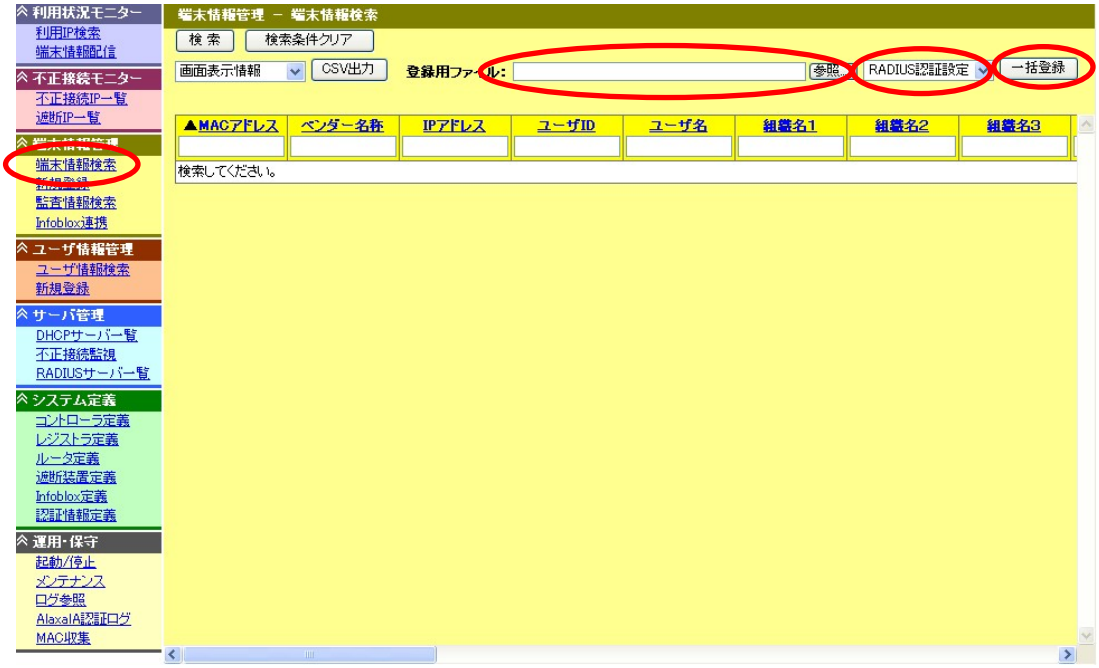


「戻る」ボタンをクリックすると、「RADIUS 認証設定」が追加されたことが確認できます。



また、CSV ファイルからの一括登録を行うことが出来ます。

「端末情報管理」－「端末情報検索」メニューをクリックしますと以下の画面を表示します。



「登録用ファイル：」の項目に CSV ファイルを指定します。（「参照」ボタンをクリックして、指定することも可能です）

登録情報種別選択欄に「RADIUS 認証設定」を指定します。

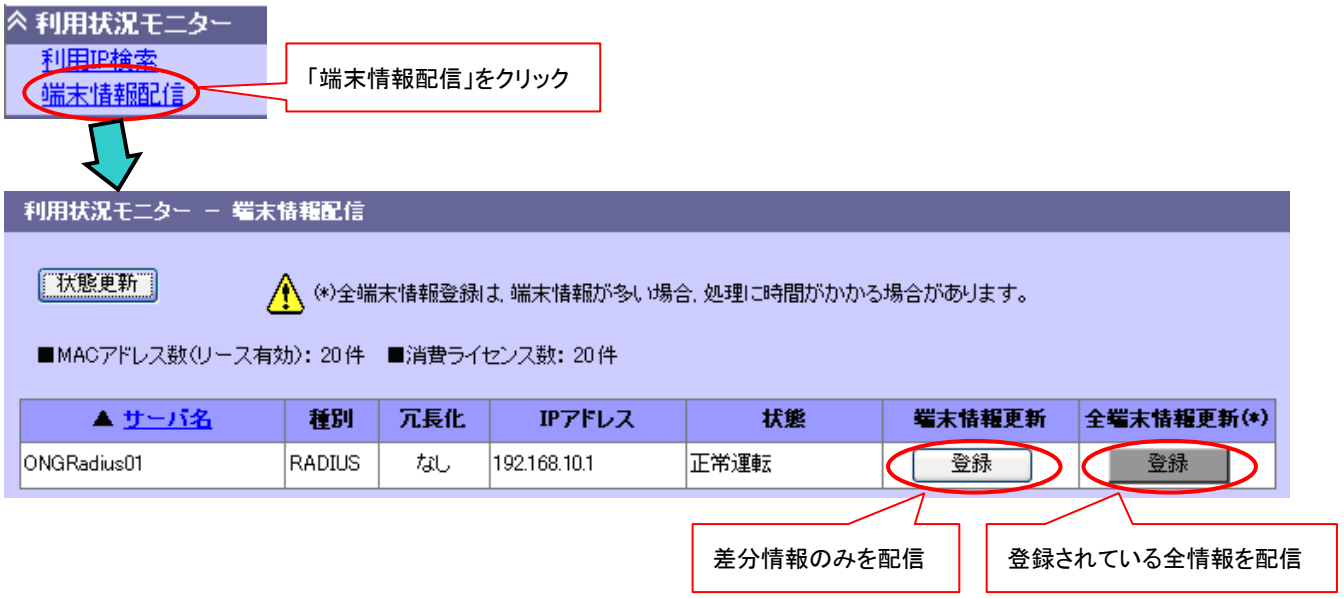
注）CSVの形式については、「オープンネット・ガード　ユーザーズマニュアル
4.1.2 端末情報 (5) RADIUS認証設定」 をご参照下さい。

CSV ファイルを指定後、「一括登録」ボタンをクリックします。

4.2 認証情報の配信

設定した認証情報を RADIUS サーバに配信します。配信作業が完了した時点で、登録した端末情報が有効になります。

左のメニューから「端末情報配信」をクリックし、「端末情報配信」画面を表示してください。
差分情報のみを配信する場合は「端末情報更新」欄の「登録」ボタンをクリックしてください。
また、登録されている全情報を再配信する場合は「全端末情報更新」欄の「登録」ボタンをクリックしてください。



5. Web 認証の設定

5.1 認証情報の設定

Web 認証を実施する際の認証情報の設定について以下に示します。

5.1.1 認証情報定義作成

オープンネット･ガードのコントローラにログインします。

（１）Web ブラウザを起動してアドレス欄に
「http://192.168.10.1/cntl/cntl_frame.php」
を入力します。

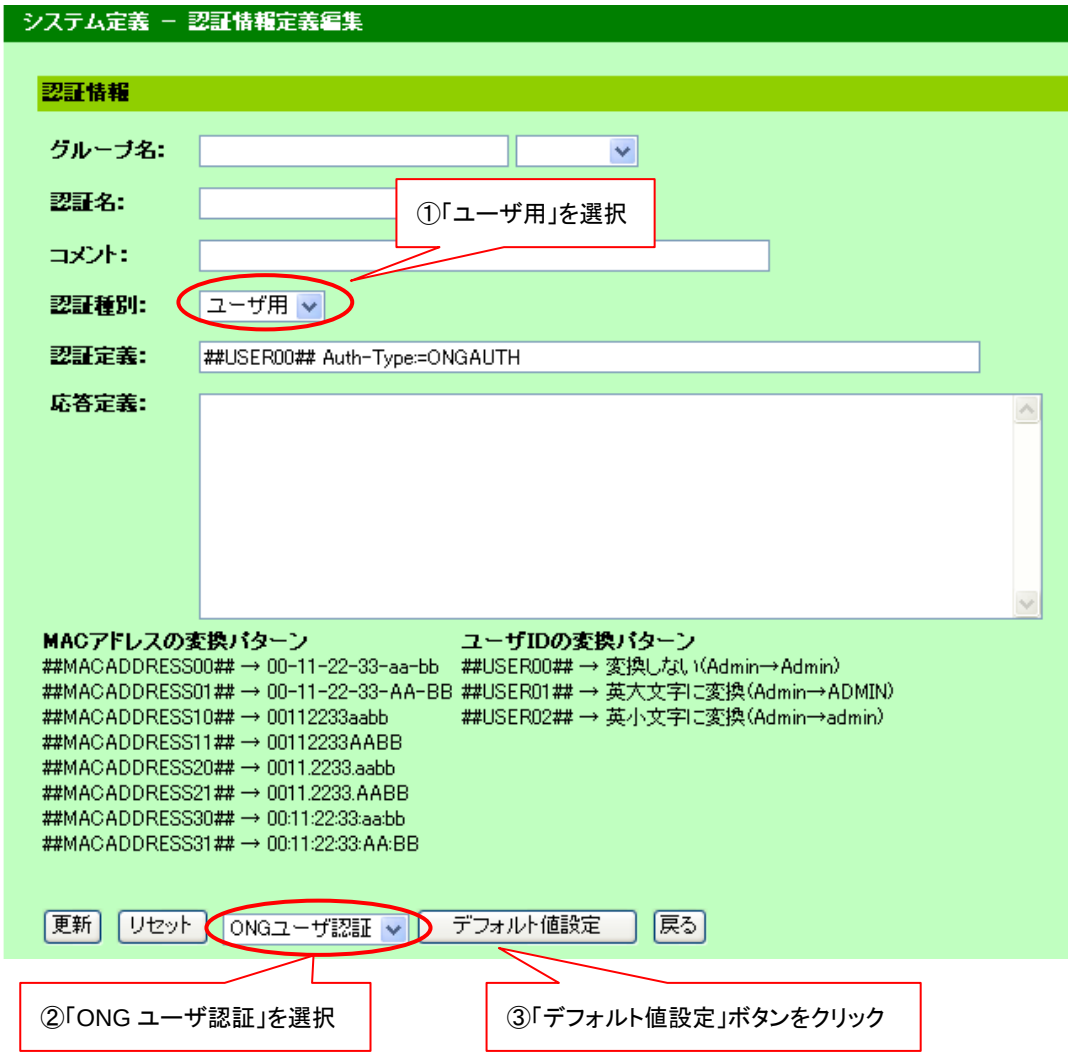
（２）ユーザ ID とパスワードを入力してログインします。
「Admin」権限を持っているユーザのみログインすることができます。

（３）RADIUS 認証で使用する認証情報定義を追加します。
左のメニューから「認証情報定義」をクリックし、「認証情報定義」画面を表示してください。
画面左上の「新規登録」ボタンをクリックし、「認証情報定義登録」画面を表示します。

RADIUS サーバで使用する認証用データベースファイルの記述方式を定義します。
導入環境に合わせて認証定義および応答定義項目に適宜値を指定してください。その他各項目に適宜値を指定し、「登録」ボタンをクリックします。

デフォルト値を自動入力するには、認証種別に「ユーザ用」、画面下部の選択欄に「ONG ユーザ認証」を選択し、「デフォルト値設定」をクリックします。

項目の詳細については「オープンネット・ガード　ユーザーズマニュアル　2.1.7 システム定義」をご参照下さい。



●固定 VLAN 環境および、ログイン認証での Web 認証定義　例

※デフォルト値を利用する際は、自動入力された以下の値を修正してください。
・認証定義：”##～##”で記述されている変換パターン

●動的 VLAN 環境での Web 認証定義　例

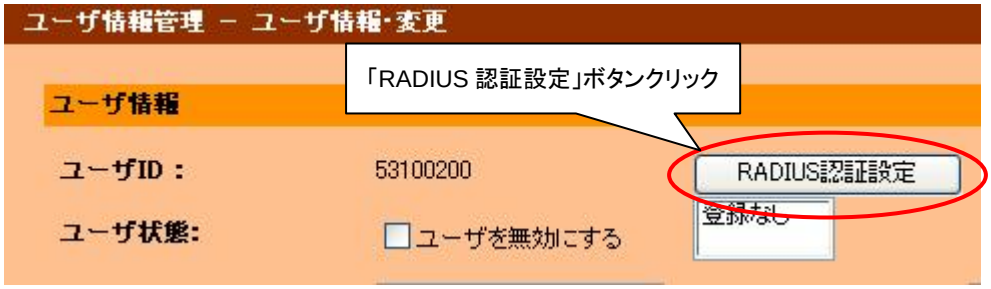
※デフォルト値を利用する際は、自動入力された以下の値を修正してください。
　・認証定義：”##～##”で記述されている変換パターン
また、応答定義は自動入力されませんので、上記画面例を参照して、入力してください。

5.1.2　ユーザと認証情報の関連付け

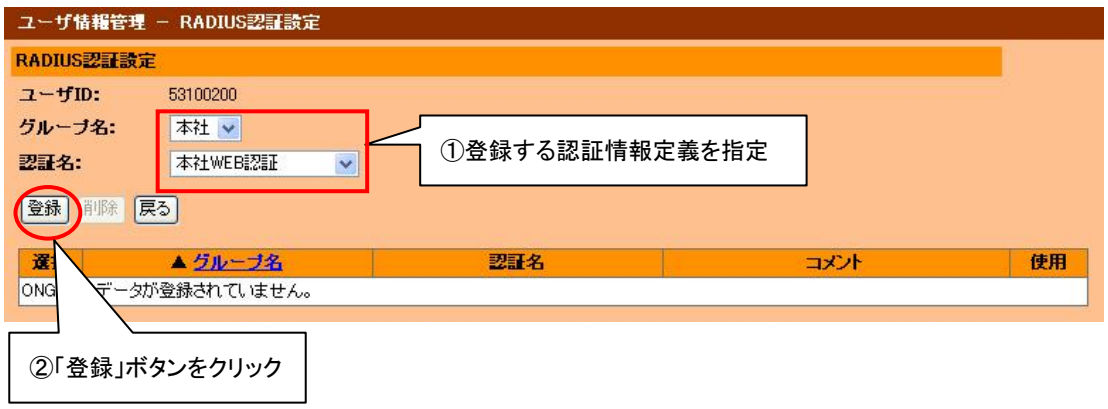
Web 認証を行うユーザと、認証情報の関連付けを行います。

左のメニューから「ユーザ情報検索」をクリックし、「ユーザ情報検索」画面を表示します。ユーザ情報一覧から RADIUS 認証設定登録を行うユーザのユーザ ID をクリックし、「ユーザ情報・変更」画面を表示します。

「ユーザ情報・変更」画面右上部の「RADIUS 認証設定」ボタンをクリックし、「RADIUS 認証設定」画面を表示します。



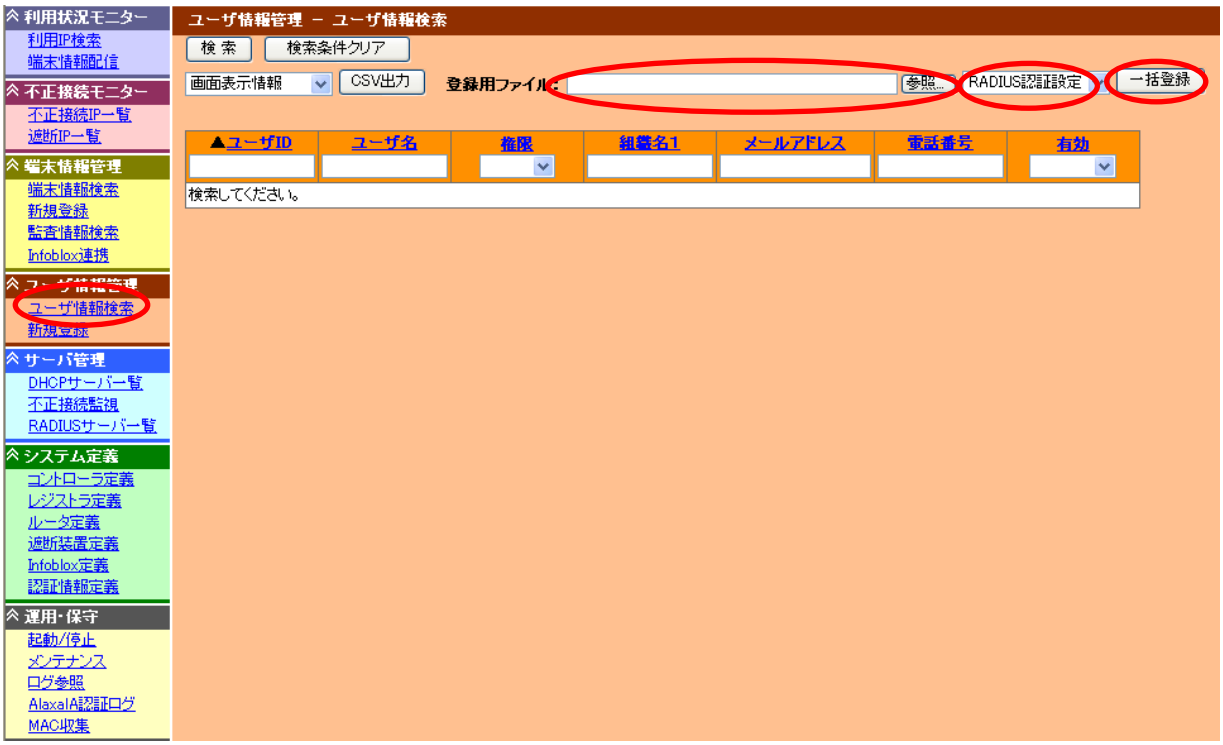
「グループ名」、「認証名」項目に登録する「認証情報定義」を指定し、「登録」ボタンをクリックします。



「戻る」ボタンをクリックすると、「RADIUS 認証設定」が追加されたことが確認できます。

また、CSV ファイルからの一括登録を行うことが出来ます。

「ユーザ情報管理」－「ユーザ情報検索」メニューをクリックしますと以下の画面を表示します。



「登録用ファイル：」の項目に CSV ファイルを指定します。（「参照」ボタンをクリックして、指定することも可能です）

登録情報種別選択欄に「RADIUS 認証設定」を指定します。

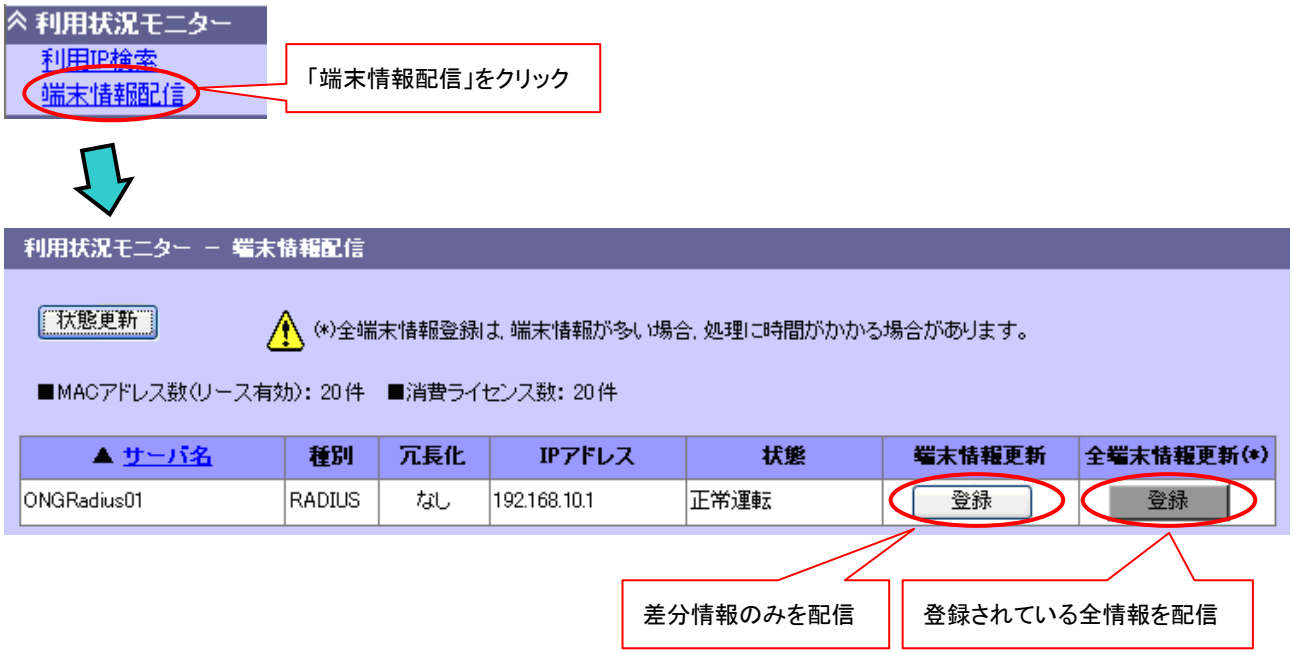
注）CSVの形式については、「オープンネット・ガード　ユーザーズマニュアル
4.1.2 端末情報 (5) RADIUS認証設定」 をご参照下さい。

CSV ファイルを指定後、「一括登録」ボタンをクリックします。

5.2 認証情報の配信

設定した認証情報を RADIUS サーバに配信します。配信作業が完了した時点で、登録した端末情報が有効になります。

左のメニューから「利用状況モニター」をクリックし、「端末情報配信」画面を表示してください。差分情報のみを配信する場合は「端末情報更新」欄の「登録」ボタンをクリックしてください。また、登録されている全情報を再配信する場合は「全端末情報更新」欄の「登録」ボタンをクリックしてください。



6. ログイン認証

6.1 RADIUS サーバによる認証の設定

［設定のポイント］

RADIUS サーバ、およびローカル認証を行う設定例を示します。RADIUS 認証に失敗した場合には、本装置によるローカル認証を行うように設定します。

あらかじめ、通常のリモートアクセスに必要な設定を行っておく必要があります。

［AXでの設定］

① **(config)# aaa authentication login default group radius local**

使用するログイン認証方式をRADIUS 認証、ローカル認証の順に設定します。

② **(config)# radius-server host 192.168.10.1 key "alaxala"**

RADIUS 認証に使用するサーバのIP アドレス（192.168.10.1）と共有鍵（alaxala）を設定します。

［オープンネット・ガードでの設定］

① ログイン認証用のユーザ情報をオープンネット・ガードに登録します。
　手順は、「3.1 ユーザの登録」をご参照下さい。

② 認証情報を設定します。手順は、「5.1 認証情報の設定」をご参照下さい。

③ RADIUSサーバへ認証情報を配信してください。
　手順は、「5.2 認証情報の配信」をご参照下さい。

詳細は、AX1200S装置のソフトウェアマニュアルのコンフィグレーションガイドVol. 1
「第8章 ログインセキュリティとRADIUS」をご参照下さい。

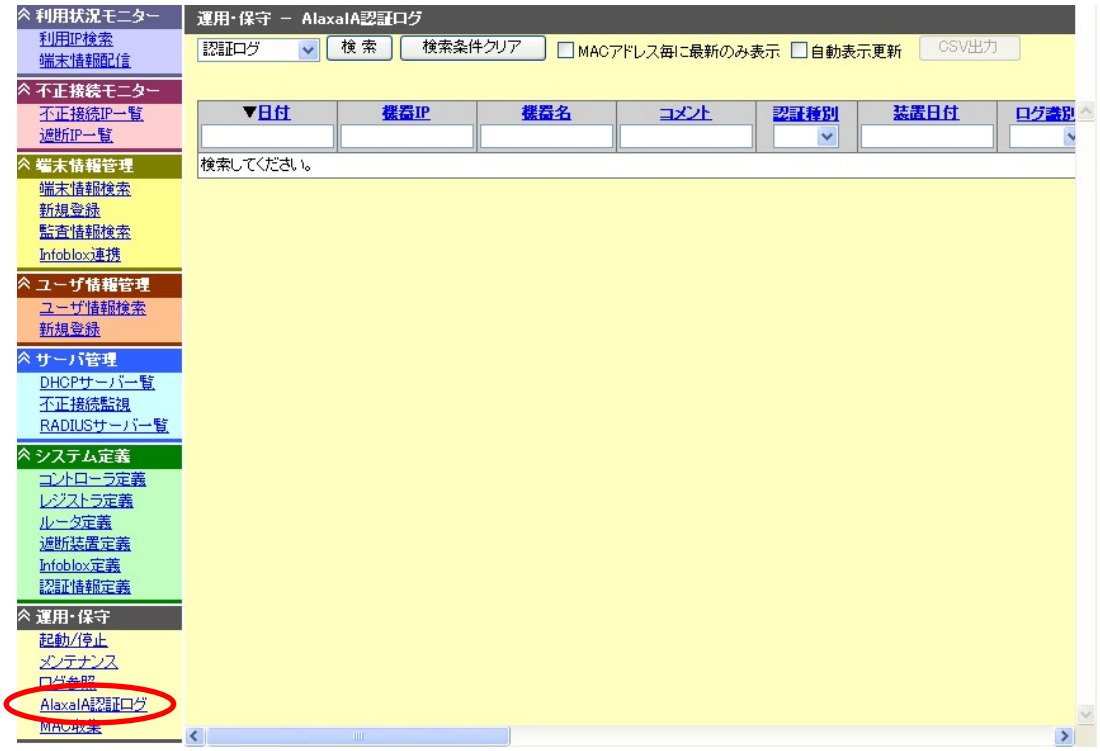
7. ログ確認

7.1 AlaxalA 認証ログの確認方法

syslog に出力されている AlaxalA 認証ログの参照を行うことが出来ます。

「運用・保守」－「AlaxalA 認証ログ」メニューを選択しますと以下の画面を表示します。

検索ボタン左横のプルダウンで表示する認証ログを切り替えます。



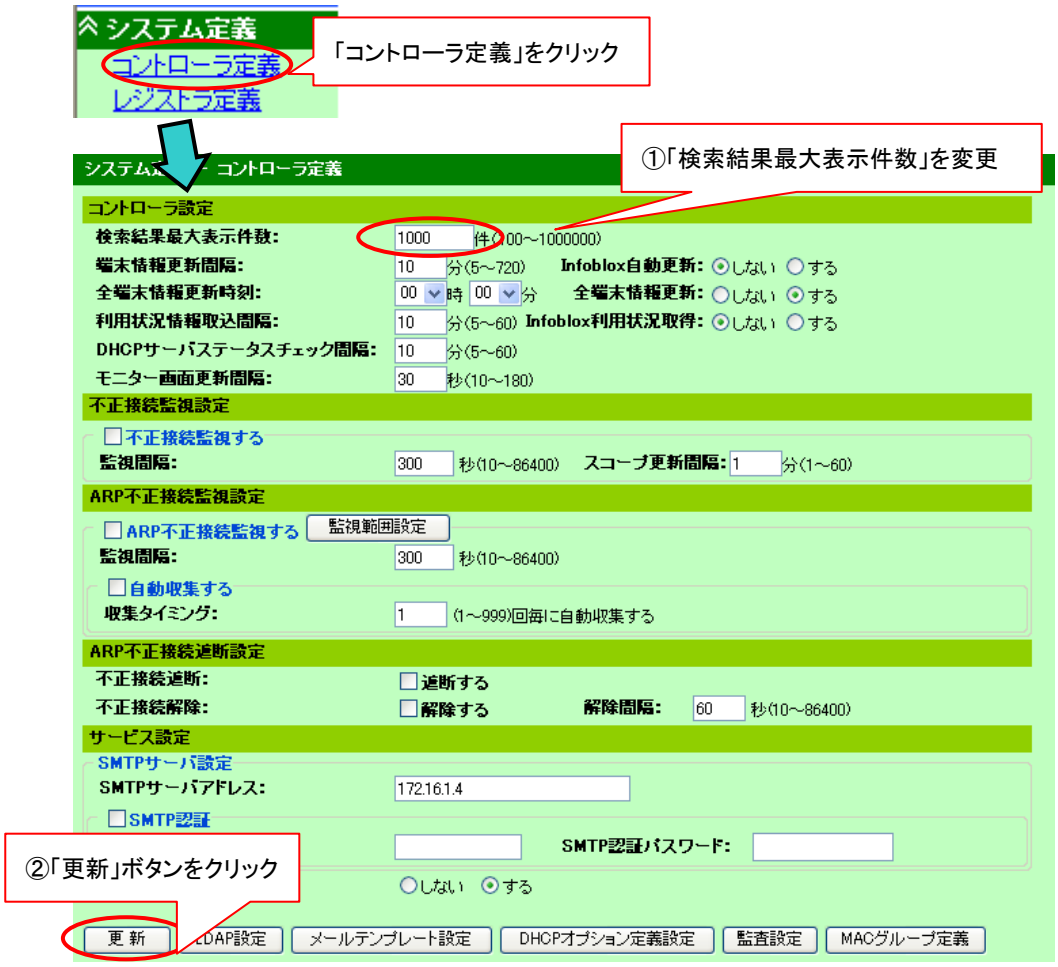
（１）認証ログ全検索

検索欄に何も指定せずに「検索」ボタンをクリックしますと、全てのログを認証ログ一覧に表示します。

※検索結果件数が多量な場合、検索結果の表示に時間がかかります。また、1000 件を超過した検索結果は画面に表示しません。検索結果が 1000 件を超過する場合は、検索結果が 1000 件以下になるように絞込み検索を行うか、以下の手順にて検索結果最大表示件数を変更して下さい。

(1)「システム定義」－「コントローラ定義」メニューを選択する。

(2)「検索結果最大表示件数」を変更後、「更新」ボタンをクリックする。



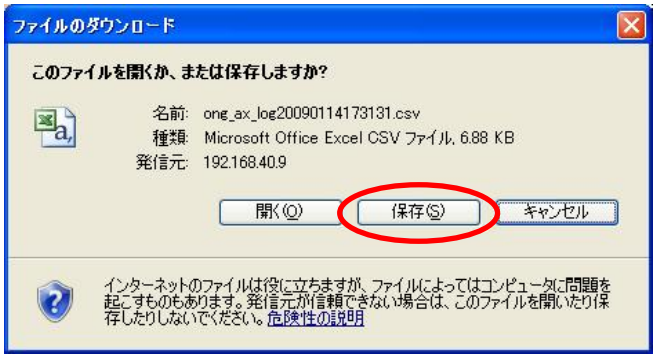
（２）絞込み検索

認証ログ一覧の検索欄に値を入力し、「検索」ボタンをクリックしますと、指定した検索条件で検索した認証ログを認証ログ一覧に表示します。

（３）CSV 出力

「CSV 出力」ボタンをクリックします。

「CSV 出力」ボタンをクリックしますと、以下のようなファイルのダウンロードを促す画面を表示します。



「保存」ボタンをクリック後、保存先を指定してファイルに保存します。

出力する CSV ファイル名は以下となります。

・ong_ax_log[日時].csv

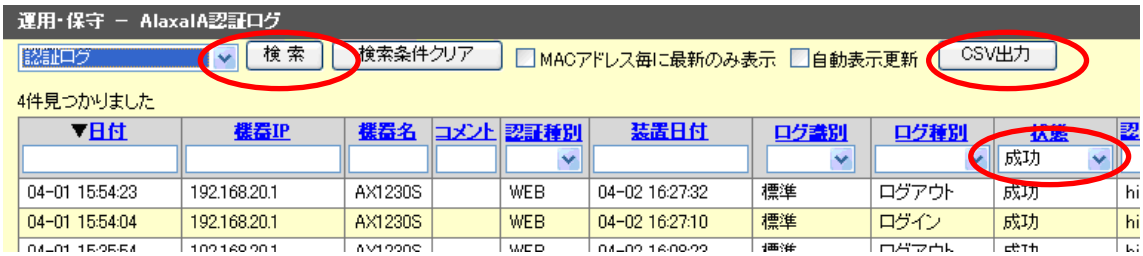
（例）2009 年 1 月 14 日、17 時 31 分 31 秒に出力したファイル：

ong_ax_log20090114173131.csv

7.2 AlaxalA 認証ログの利用例

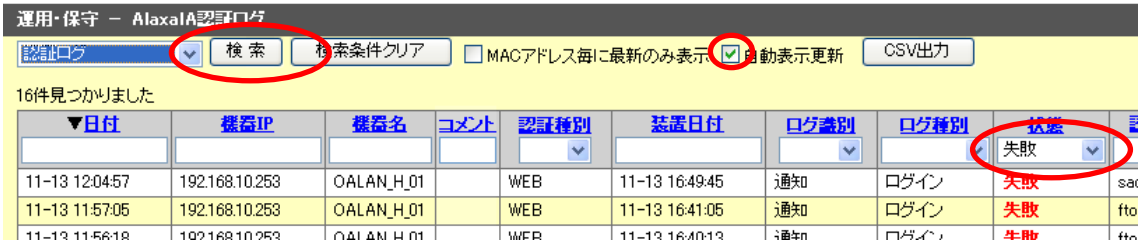
(1)成功ログの出力（MAC 認証ログ、Web 認証ログ）

「状態」のプルダウンで「成功」を選択し、「検索」ボタンをクリックします。認証に成功したログを表示できます。また、「CSV 出力」ボタンをクリックすることで CSV 形式ファイルに出力でき、認証に成功したポートの一覧ファイル等の作成が可能です。



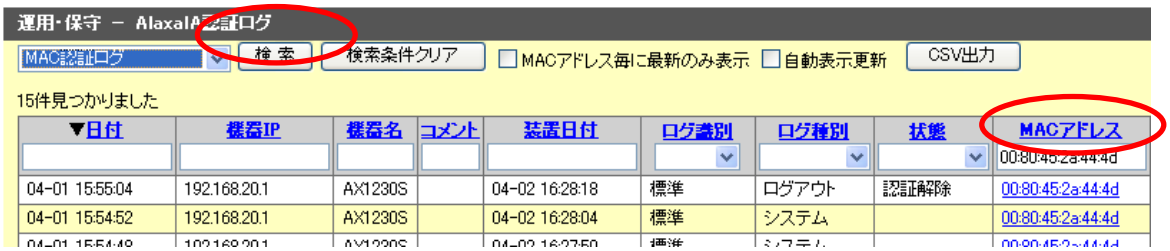
(2)不正ログの継続表示(MAC 認証ログ、Web 認証ログ)

「状態」のプルダウンで「失敗」を選択、「自動表示更新」にチェックを入れて、検索ボタンをクリックします。認証に失敗したログが継続的に表示できます。



(3)各端末の認証履歴確認（MAC 認証ログ）

「MAC アドレス」に認証履歴を確認したい MAC アドレスを入力し、「検索」ボタンをクリックします。認証に成功/失敗したログを表示できます。



(4)各ユーザの認証履歴確認（Web 認証ログ）

「認証ユーザ」に認証履歴を確認したいユーザ ID を入力し、「検索」ボタンをクリックします。認証に成功/失敗したログを表示できます。

8. 付加機能

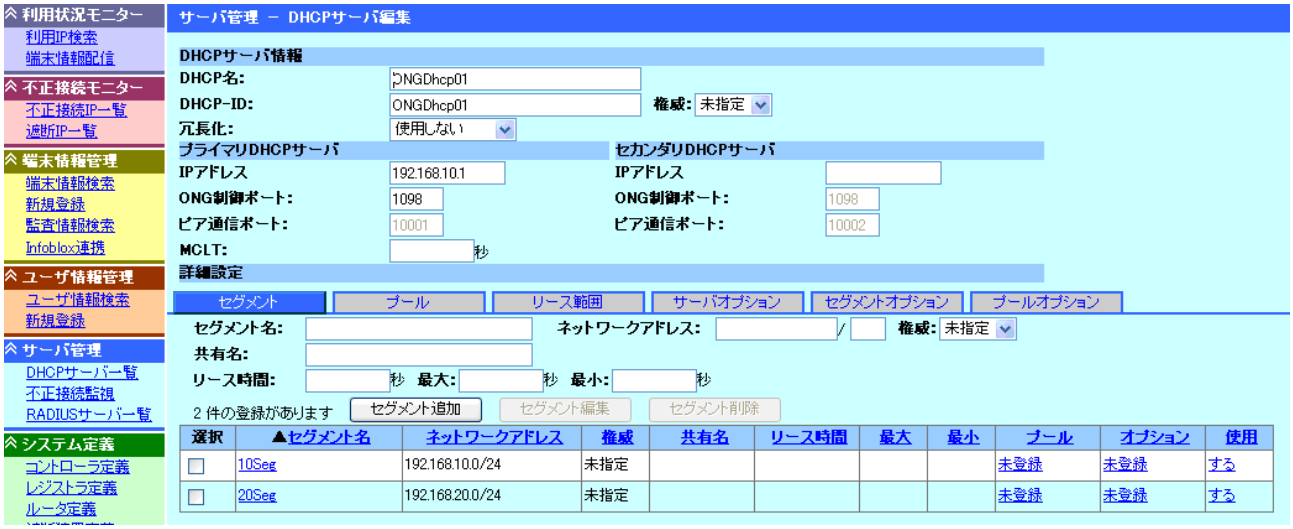
8.1 DHCP 機能

オープンネット･ガードの DHCP 機能を使用することで登録された MAC アドレスの端末のみ IP アドレスを割り振ることが可能です。

「サーバ管理」－「DHCP サーバー覧」メニューを選択すると以下の画面を表示します。

「新規登録」ボタンをクリックしてください。

DHCP サーバ登録画面にて、情報を入力します。項目の詳細および、設定・操作方法については「オープンネット・ガード　運用マニュアル　2.1 DHCP 設定」をご参照下さい。



8.2 MAC 収集機能

３．２で登録する MAC アドレスを､指定したルータの ARP 情報から収集することが出来ます。

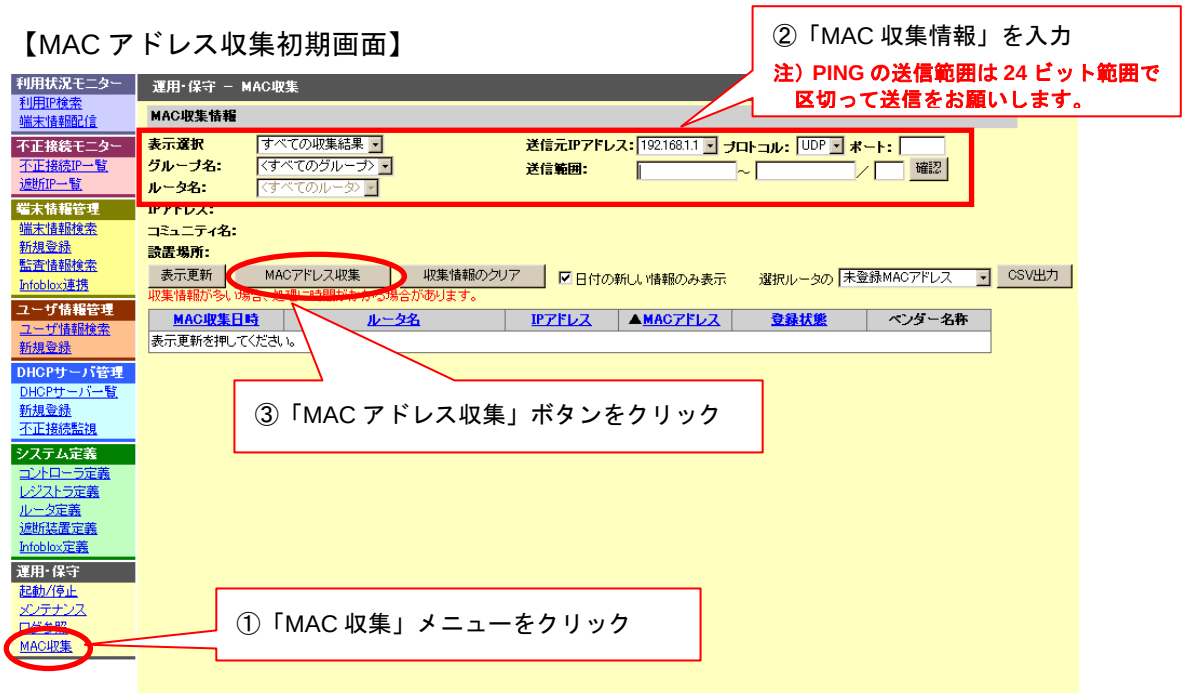
「運用・保守」－「MAC 収集」メニューを選択すると以下の画面を表示します。

注）事前に、ARP情報を収集するルータを定義する必要があります。

ルータの定義方法については、「オープンネット・ガード　ユーザーズマニュアル

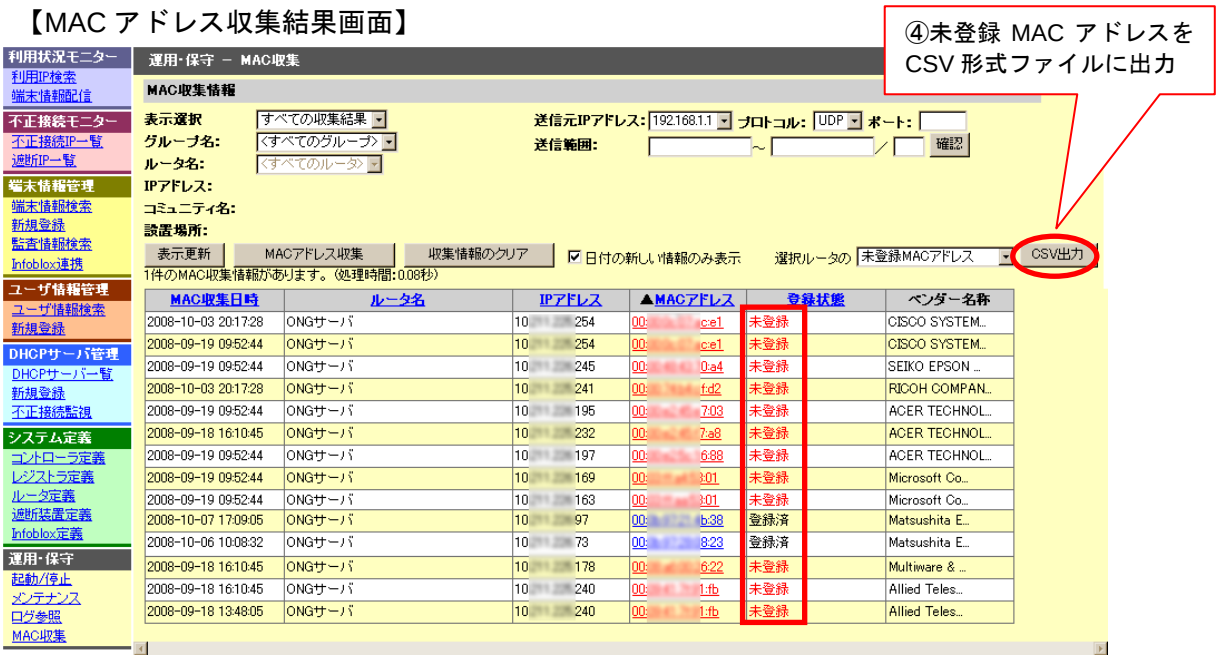
2.1.7 システム定義　(10) ルータ定義　(11)ルータ定義登録（更新）」 をご参照下さい。

【MAC アドレス収集初期画面】



MAC 収集情報を入力し「MAC アドレス収集」ボタンをクリックして MAC アドレスを収集します。

【MAC アドレス収集結果画面】



未登録 MAC アドレスを CSV 形式ファイルに出力し、MAC アドレスの精査を実施します。
（MAC アドレス収集時に出力した CSV 形式ファイルのまま、一括登録可能）
CSV 形式ファイルの登録方法に関しては、「3.2 MAC アドレスの登録」をご参照下さい。

2009 年 5 月 22 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