

RADIUS サーバ設定ガイド オープンネット・ガード編

初版

Copyright © 2009, ALAXALA Networks Corporation. All rights reserved.



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(<u>http://www.alaxala.com/jp/techinfo/manual/index.html</u>)
- ・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(<u>http://www.hitachi-system.co.jp/ong/index.html</u>)

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	Ę	5
1.1	概要	5
1.2	設定例環境	6
1.2.	1 使用機器一覧とAXコンフィグレーション	6
1.2.	2 設定例のネットワーク構成図	7
2. オー	- プンネット・ガードの構成	B
21	進備	8
2.2	サーバへのインストール	8
2 + _	_ プンナット・ギー じつむウ	•
J. /] –	- ノノイット・リートの設定	"
3.1	ユーザの登録	9
3.2	MACアドレスの登録11	2
3.3	認証スイッチの登録1- 	4
(1	1) RADIUSサーバ情報設定1	4
(2	2) RADIUSサーバ設定	5 -
(3	3) 認証クライアント設定	с С
(2		с С
(5	5) RADIUSサーバの登録	2 7
(6	5) RADIOS設定ファイル検査I	r Q
(7	r_{1} RADIOS設定ファイル登録	с Q
34		a
3.4	1 認証ログの追加・編集・削除 1/	a
(1	1) 認証ログ定義の追加	0
(2	//	0
(3	/	1
3.4.	, 2 ファイル定義の追加・編集・削除	2
(1	1) ファイル定義の追加	2
(2		3
(3	3) ファイル定義の削除2	3
4. MA	C認証の設定2	4
4.1	認証情報の設定	4
4.1.	1 認証情報定義作成	4
4.1.	2 MACアドレスと認証情報の関連付け2	9
4.2	認証情報の配信	1

RADIUS サーバ設定ガイド オープンネット・ガード編(初版)

5.	We	əb認証の設定	.32
Į	5.1	認証情報の設定	.32
	5.1	l.1 認証情報定義作成	.32
	5.1	Ⅰ.2 ユーザと認証情報の関連付け	.36
į	5.2	認証情報の配信	.38
6.		グイン認証	.39
(6.1	RADIUSサーバによる認証の設定	.39
7.	¤ ?	グ確認	.40
-	7.1	AlaxalA認証ログの確認方法	.40
-	7.2	AlaxalA認証ログの利用例	.43
8.	付加	加機能	.45
8	3.1	DHCP機能	.45
8	3.2	MAC収集機能	.46

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

- 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。

ロダイン ユーザID:
ユーザID:
ユーザID:
パスワード:
クライマンルライヤンフ All Pickte Received Convicts (0) 2004 2008. Hitschi Systems & Services Ltd

ディフォルトでは、ユーザ I D: 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。

◇ 利用状況モニター	ユーザ情報管理 - 新規登録				①各7	項目に値を入	л
<u>利用印候祭</u> <u>端末情報配信</u>	ユーザ情報						
ペ 不正接続モニター <u>不正接続IPー覧</u>	ユーザID:				V		_
	ユーザ状態:	□ユーザを無効にする					
	パスワード:]	再入力:			
<u>新規登録</u> 監査情報検索	ユーザ名:			権限:	User 🔽	WF管理者	
<u>Infoblox連携</u>	組織名1:		i	管理組織:	組織1 🗸		
ユーザ情報検索	組織名2:						
利規豆球 ペ サーバ管理	組織名3:						
<u>DHCPサーバー覧</u> 不正接続監視	メールアドレス:						
RADIUSサーバー覧	電話番号:						
ペ システム定義 <u>コントローラ定義</u>	備考:						
レジストラ定義 ルータ定義							
<u>遮断装置定義</u> Infoblox定義							
≪ 運用・保守 起動/停止							
メ <u>ンテナンス</u> ロ <u>グ参照</u>							
<u>AlaxalA認証ログ</u> <u>MAC収集</u>							

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。

◇ 利用状況モニター	ユーザ情報管理 -	ユーザ情報検索	R.						
利用IP検索	検索 検索	条件クリア							
端末情報配信						CARD	+	一样弯	4
◇ 不正接続モニター	■田表示情報 ▶		登録用ファイル			李照	ユーリー育業限		10K
不正接続IP一覧									
<u>通断IP一覧</u>	▲ <u>ユーザID</u>	<u>ユーザ名</u>	<u>ユーザ種別</u>	<u>組織名1</u>	組織名2	<u>組織名3</u>	<u>備考</u>	メモ	<u>^</u>
◇ 端末情報管理			~		and the second second	1. Sec. 1. Sec. 1.			
端末情報検索	検索してください。								
<u> </u>									
<u>一旦 IIIII 表示</u> Infobloxi事携									
ヘユーリ商報管理									
「「日田田田田本	2								
◇ サーバ管理									
DHCPサーバー覧									
不正接続監視									
<u>RADIUSサーバー覧</u>									
◇ 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									
<u>過期表面進載</u> Infoblox定義									
認証情報定義									
☆ 運用・保守									
記動/停止									
メンテナンス									
<u>ログ参照</u>									
<u>AlaxalA認証ログ</u>									~
<u>MAC収集</u>	<								>

「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。

Г

				①各項目に値	を入力	
◇ 利用状況モニター	端末情報管理 — 新規登錄	k				
<u>利用坦爾索</u> <u>端末情報配信</u>	ハードウェア情報					
◇ 不正接続モニター	MACアドレス:					
<u>不正接続IP一覧</u>	リース:	□無効				
	ARP不正接続監視:	■対象外				
^人 電木	ユーザ情報					
新規登録	ユーザID:		ユーザ確認	3		
<u>一旦日午的東京</u> Infobloy演進	ユーザ名:			_		
<u>modiox連携</u> ◇ つーザは超等理	組織名:					
<u>ユーザ情報検索</u>	コンピュータ情報					
新規登録	ホスト名:					
冬 サーバ管理	OS種別:	指定しない	~			
<u>DHOPサーバー覧</u> 不正接続監視	管理番号:					
<u>RADIUSサーバー覧</u>	備考:					
冬 システム定義	利用期間					
<u>コントローラ定義</u> レジストラ定義	利用期間(開始):	2008-01-01				
ルータ定義	利用期間(終了):					
<u>遮断装置定義</u>						
認証情報定義	利用時間(開始):					
≪ 運用∙保守	利用時間(終了):	時分 ⊻全時間帯				
起動/停止	監査結果による有効期限:	2009-02-06 🖳 🗹 無効				
メ <u>ンテナンス</u> ログ参照						
<u>AlaxalA認証ログ</u>						
<u>MAC収集</u>						

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。

◇利用状況モニター	端末情報管理 - 端末情報検索					
利用理検索	検索 検索条件クリア					
◇ 不正接結エニター	画面表示情報 🗸 CSV出力	登録用ファイル、		参照	端末情報	✓ 一括登録
不正接続アー覧						
<u>遮断IP一覧</u>	▲MACアドレス ベンダー名称	IPアドレス ユーザID	ユーザ名	組織名1	組織名2	組織名3 ^
☆ 端末快報等理						
端末情報検索	検索してください。					
<u>和担</u> 学转 壓害情報檢索	8					
Infoblox 連携						
ペ ユーザ情報管理						
ユーザ情報検索						
新規登録						
≪ サーバ管理						
<u>DHCPサーバー覧</u> 不正接結時短						
RADIUSサーバー覧						
◇ システム定義						
コントローラ定義						
レジストラ定義						
ルニシ定義						
Infoblox定義						
認証情報定義						
≪ 運用・保守						
<u>起動/停止</u>						
ログ参照						
AlaxalA認証ログ						
<u>MAC収集</u>						~

「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。

ペ サーバ管理 DHCPサーバー覧 不正接続監視 RADIUSサーバー覧	「RADIUS サー	バー覧」をクリック]		
サーバ管理 - RAI)IUSサーバー覧 登録用ファイ	(Jb:			参照
新規登録 ▲RADIUSサーノ	「新規登録」ボタンを	- クリック IPアドレス	ポート番号	使用	削除
ONG2071 データが登	録されていません。				

「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。

サーバ管理 - RADIU	Sサーバ登録						
RADIUSサーバ情報							
RADIUSサーバ名:							
RADIUSサーバ							
ま IPアドレス	ONG制御ボート						
1	1097						
2	1097						
3	1097						
4	1097						
認証クライアント設定	認証情報服役	定					
認証クライアント名:							
コメント:							
IPアドレス:							
共有鍵(secret):							
略称(shortname):							
機種タイブ(nastype):	*						
クライアント追加] [クライアン	ト編集 クライアント削除					
選択 ▲ <mark>認証クライ</mark>	(アント名		IP7FLZ	共有鍵	略称	機種タイプ	使用
ONG2071 データが登録る	もれていません。						
2							
保存反る							1

(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。

RADIUSサーハ情報		
RADIUSサーバ名:	ONGRadius01	項目に値を入力

(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。

z	IPアドレス	ONG創資	ボート	
1	192.168.10.1	1097		
2		1097		百日に値を入力
з		1097		項日に値を八刀
4		1097	2	

(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。

認証クライア.	ト設定 「認証クライアント設定」タブをクリック タ・ ホ2+IPPETマイッチ
認証クライアント設定	記言証情報顧設定
認証クライアント名:	本社認証スイッチ
コメント:	認証クライアント ①各項目に値を入力
IPアドレス:	192.168.1.254
共有鍵(secret):	ONGSecret
略称(shortname):	RadiusClient
機種タイブ(nastype):	other 🔽
クライアント追加	クライアン作品来 クライアン作用 味
達択 <u>▲認識</u>の ONG2071 データが登録る	アント ないています ②「クライアント追加」ボタンクリック ス 共有鍵 略称 様種 な な な な な な な な な な な な な

(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。

認証クライアント設定 認証情報設定」タブをクリック 生成する認証情報は「加する情報」ある場合は、下記 認証クライアント設定 認証情報設定 認証力ライアント設定 認証情報設定 生成する認証情報に付加する情報がある場合は、下記の入力フィールドに設定してください。 定義内に##3GENERATE##を指定することで、任意の場所にONGの生成する情報を展開できます。 ##3GENERATE##を指定しなかった場合は、指定した定義の最後にONGの生成する情報を展開します。 必要に応じて値を指定		
生成する認証情報に付加する情報 ある場合は、下記 記証クライアント設定 認証情報設定 生成する認証情報のに付加する情報がある場合は、下記の入力フィールドに設定してください。 定義内に##GENERATE##を指定することで、任意の場所にONGの生成する情報を展開できます。 ##GENERATE##を指定しなかった場合は、指定した定義の最後にONGの生成する情報を展開します。 必要に応じて値を指定	認証クライアント設定 認証情報設定 「認証情報設定」タブをクリッ	ック
記証クライアント設定 認証情報設定 生成する認証情報に付加する情報がある場合は、下記の入力フィールドに設定してください。 定義内に##GENERATE##を指定することで、任意の場所にONGの生成する情報を展開できます。 ##GENERATE##を指定しなかった場合は、指定した定義の最後にONGの生成する情報を展開します。 必要に応じて値を指定	生成する認証情報に付加する情報のある場合は、下記に	
認証15日2000000000000000000000000000000000000		
生成する認証情報に付加する情報がある場合は、下記の入力フィールドに設定してください。 定義内に##GENERATE##を指定することで、任意の場所にONGの生成する情報を展開できます。 ##GENERATE##を指定しなかった場合は、指定した定義の最後にONGの生成する情報を展開します。 必要に応じて値を指定	認証クライアント設定 認証情報設定	
定義内に##GENERATE##を指定することで、任意の場所にONGの生成する情報を展開できます。 ##GENERATE##を指定しなかった場合は、指定した定義の最後にONGの生成する情報を展開します。 必要に応じて値を指定	生成する認証情報に付加する情報がある場合は、下記の入力フィールドに設定してくだ	さい。
##GLINETHTE##2182030175538113、1820722305度181201439531141822度1910349。 必要に応じて値を指定	定義内に##GENERATE##を指定することで、任意の場所にONGの生成する情報を展開 ##GENERATE##を指定したかった提合は、指定した定義の最後にONGの生成する情報	できます。 茨展明 ます
必要に応じて値を指定		
必要に応じて値を指定	r	
		必要に応じて値を指定
		and a

(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。

サーバ管理 - RADIUS	サーバ登録						
RADIUSサーバ情報							
RADIUSサーバ名:	ONGRadius01						
RADIUSサーバ							
≇ IPアドレス C	DNG制御ボート						
1 192.168.10.1	1097						
2	1097						
3	1097						
4	1097						
認証クライアント設定		1					
認証クライアント名:							
コメント:							
IPアドレス:							
共有鏈(secret):							
略称(shortname):							
催檀タイブ(nastype):	×						
1件の登録があります	クライアント追加	クライアント編集	クライアント削除	11-1-00	-10		-
「度訳 ▲2211/2-1	(<u>72h%</u>		ΨΥΈνλ	王有選		<u> 獲種タイプ</u>	12日
▲ 本社認証スイッチ	認証クライ	アント	192.168.1.254	ONGSecret	RadiusClient	other	<u>রু</u>
2							
保存 破棄							
	<u> </u>						
「保存	ミュボタンをクリッ	4					

Copyright (c) 2009 ALAXALA Networks Corporation. All rights reserved.

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	こください

≪ 運用・保守	
起動/停止 メンテナンス	起動/停止をクリック
ログ参照 Alaxa MAC地 IIログ	

運用•保守 – 起動/停止												
登録管理サーバ												
状態 ONG 正常 Image: Constraint of the second secon	操作 実行											
ONGサーバ 「状態」が「不明」となる 最新の状態に更新 「												
▲ サーバ名	種別	<u>t</u>	ナーバ設定		1	サー	バ情報					
	E.	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		
ONGRadius01	RADIUS	未登録	~	なし	192.168.1.0.1	- <	不明		*	状態更新		

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。

		①「最新の	状態に	更新」ボタンを				তা	「小牛台に」よく「こ	て 尚 」 し #	- Z	
4		2			-				1人態」が1	「吊」こん	10	
	A ++- 15-7	## Pil	ť	トーバ設定	サーバ情報							
	■ <u>9 = /14</u>	1 <u>E</u> 51	状態	サーバ操作	冗長化	IPアドレス	構成	状態	1	サーバ操作	ONG	操作
	ONGRadius01	RADIUS	未登録	*	なし	192.168.1.0.1	-	<u> </u>	-	~	*	状態更新

(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。

C	DNGサーバ			÷۲	۵ ж						.+ 511	ь	
(最新の状態に更新		史宜	「」を迭択		アをクリッ	9						
	▲ #+_154 新型						サーバ情報						
	= <u>5 7141</u>	12.01	状態	サーバ操作	N	冗長化	IPアドレス	構成	状態	サーバ操作	ONG	抹ſ	F
	ONGRadius01	RADIUS	未登録	検査	$\overline{}$	なし	192.168.1.0.1	-	正常	×	~	実行	ī)

(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。

ONGサーバ		_						<u>م</u>						
最新の状態に更新					①「登録」を選択					(2)実行」ホタンをクリック				
▲ # ~ バタ 新四 サーバ設定									サーバ情報					
▲ <u>リーパ名</u> 僅刻 状態 サー		サーバ操作	И	冗長化	IP7	ペレス	構成	状態	ť	トーバ操作	ONG	操作		
ONGRadius01	RADIUS	未登録	登録 🗸		ಸ ರಿ	192.168.1.	0.1	-	正常		*	~	実行	\supset

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。

ONGサーバ				. .							
最新の状態に更新				①「再	起動」を選択	2	②「実行」ボタンをクリック				
▲ #t=15-2	34 Pil	t	トーバ設定				サーバ情報				
▲ <u>9 - 714</u>	4 <u>E</u> 01	状態	サーバ操作	冗長化	IPアドレス	構成	状態	サーバ抹	ť≇ ONG	操作	
ONGRadius01	RADIUS	登録済	×	なし	192.168.1.0.1	-	正常	再起動	>	実行)

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 サーバヘ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。

- 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。

192.168.10.1 へ接続	ŧ ? 🗙
	Ger
OpenNETGuard Setup (ードが必要です。	Dサーバー 192.168.10.1 (こはユーザー名とパスワ
ユーザー名(山):	
バスワード(<u>P</u>):	
	パスワードを記憶する(<u>R</u>)
	OK キャンセル

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。

	ログ管線加速	理 「認証ログ 「認証ログ 理 認証ログ	定義」をクリック			
I	コグ参	照名称:	ログ種別選択:		🖌 追加	更新 削除 ↑ ↓
4	件の	登録があります				
	選択	ログ参照名称	口グ種別名称	ファイル定義	使用	
		認証ログ	アラクサラ認証詳細ログ	<u>1件登録</u>	する	
		<u>MAC認証ログ</u>	アラクサラMAC認証詳細ログ	<u>1件登録</u>	する	
		<u>WEB認証ログ</u>	アラクサラWEB認証詳細ログ 1件登録		する	
		システムログ	システムログ	<u>1件登録</u>	する	

(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。

口グ	ログ管理 - 認証ログ定義							
ログ	参照名称:認証簡易ログ	更新│削除│↑↓↓						
4140	の登録があります							
選拔	R	ログ種別名称	ファイル定義					
	1 ①値を入力	アラクサラ認証詳細ログ	の「追加」ボタ]			
	MAC	アラクサラMAC認証詳細ログ		287999				
	WEB認証ログ	アラクサラWEB認証詳細ログ	<u>1件登録</u>	する				
	<u>システムログ</u>	システムログ	<u>1件登録</u>	する				

(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。

	口夕管	辞理 - 認証ロク定義							\sim	
	5 (4 :0)	登録があります	1.1				-	_	$\overline{\wedge}$	
	選択	ログ参照名称		種別	名称	ファイル	定義	使用	$ / \rangle$	
		200 <u>7</u>	②変更する	- 5を入力	細口グ	<u>1件登録</u>]
		MAC認証ログ		正詳細ログ		1件登録 (3)		③「更新」ホタンをクリック		
			ミナ イー・ハク	サラWEB	忍証詳細ログ	<u>1件登録</u>		する		
		①編集する認証定義をナエツ		1 7 ムログ		<u>1件登録</u>		する		
(認証簡易ログ	アラク	サラ認証	コグ	登録なし		する	-	

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。

	口グ管	理 - 認証ログ定義					
ļ	ログ参	照名称:	ログ種別選択:		- 追加	更新(削除)↑	†
1	5件の3	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		
		認証ログ	アラクサラ認証詳細ログ	<u>1件登録</u>			
	MAC認証ログ		アラクサラMAC認証詳細ログ 1件登録		(2)「削除」ボタンをクリック		
	①肖	削除する認証定義をチェック	?ラクサラWEB認証詳細ログ	<u>1件登録</u>	する		
		402	システムログ	<u>1件登録</u>	する		
(簡易認証ログ	アラクサラ認証ログ	登録なし	する		
1	_		e onder westers dar in De 19 Bi				

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。

ログも	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	\uparrow \downarrow		
5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				
	認証ログ	アラクサラ認証詳細ログ	<u>1件登録</u>	する				
	MAC認証ログ	アラクサラMAC認証詳細ロ		ALL				
	<u>WEB認証ログ</u>	アラクサラWEB認証詳細ロ	ノアイル正義	のリンクを	トクリック			
	<u>システムログ</u>	システムログ	1件登	する				
	簡易認証ログ	アラクサラ認証ログ	<u>登録なし</u>	する				
			Ţ					
口グ	管理 - 認証ログ定義・コ	ファイル定義	\sim					
ログき	多照名称: 簡易認証ログ	ファイル名:		読込行数:	6	追加更新	削除 ↑	↓ 戻る
選択 ONG	く ファイル名 2015 該当するデータが存れ	読込行数 狂しません						

(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。

口グ管理	- 認証ログ定義・	ファイル定義				
ログ参照名	5年:簡易認証ログ	ファイル名: /var/log/	/messages 読込	行数:0	追加」更新「削除」↑↓↓ 戻る	3
選択	ファイル名	読込行数]
ONG2015	該当するデータが存	在しません	①適宜値を入力		②「追加」ボタンをクリック	

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。
-------------	-------------

			7定義・	ファイル定義			
①並べ替えするフ	アイル	をチェック	証ログ	ファイル名: /var.	/log/messages.3	読込行数: 0	追加 更新 削除 ↑ ↓ 戻る
	47	5,500					
	選択	77	(ル名	読込行数			
(/var/log/mes:	sages.3	指定なし			
		/var/log/mes:	sages.2	指定なし			(2)「↓」ホタンをクリック
		/var/log/mes:	sages.1	指定なし			
		/var/log/mes:	sages	指定なし			

(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。

口グ管理	- 認証ログ定義・	ファイル定義					
ログ参照: 1件の登録	名称: 簡易認証ログ 紡あります	ファイル名: /var/log/n	nessages.1	読込行	b: 0	追加 更新 削除 ↑ ↓ 戻	3
	ファイル名 ar/log/messages	読込行数 指定なし	2適宜	値を入力		③「更新」ボタンをクリック]
	①編集するファ	イル定義をチェック					

(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。

ログ管理 - ログ参照名称: 1/4の登録があり	2011ログ定義・フ 簡易認証ログ :	ァイル定義 ファイル名:	読込行数:	追加」更新(削除)↑)↓ <u>戻</u> る
####################################	Dます ファイル名 /messages.1	読込行数 指定なし		②「削除」ボタンをクリック]
)削除するファー	イル定義をチェック]		

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。

- 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。

≪ 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	「認証情報定義」をクリック				
進助装置定義					
Inteblex元素					
認証值報定義					
Ţ					
システム定義 - 翌	証情報定義				
CSV出力	登録用ファイル:		参照		禄
新規登録 219の	登録があります				
▲クルトブ名	認証名	コメント	認正種別	使用	削除
default	<u>default</u>		端末用	Utal 1	
default	default		ユーザ用	Utal 1	
「新規	見登録」ボタンをクリック				

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。

システム定義 -	忍証情報定義登録
認証情報	
グループ名:	
認証名:	①「端末用」を選択
コメント:	
認証種別: (端末用 🔽
認証定義:	##MACADDRESS00## Auth-Type:=Local, User-Password=="##MACADDRESS00##"
応答定義:	Tunnel-Type = 13, Tunnel-Medium-Type = 6, Tunnel-Private-Group-Id = {VLANID}
MACアドレスの3 ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS	E換バターン ユーザIDの変換バターン 10## → 00-11-22-33-aa-bb ##USER00## → 変換しない(Admin→Admin) 11## → 00-11-22-33-AA-BB ##USER01## → 英大文字に変換(Admin→ADMIN) 10## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin) 11## → 00112233.aabb ##USER02## → 英小文字に変換(Admin→admin) 20## → 0011.2233.aabb ##USER02## → 英小文字に変換(Admin→admin) 21## → 0011.2233.aabb ##USER02## → 英小文字に変換(Admin→admin) 21## → 0011.2233.aABB ##USER02## → 英小文字に変換(Admin→admin) 30## → 0011.2233.AABB ##USER02## → 英小文字に変換(Admin→admin) 11## → 0011.2233.AABB ##USER02## → 英小文字に変換(Admin→admin) 21## → 0011.2233.AABB ##USER02## → Example 21## → 0011.2233.AABB ##USER02## → Example
②「MAC アドレ	マス認証」を選択 ③「デフォルト値設定」ボタンをクリック



- ・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 (証定義 例
--------------------------	-------

システム定義 -	認証情報定義編集
-0-744 #P	
認識情報	
グループ名:	本社
認証名:	本社認証
コメント:	
認証種別:	端末用 🖌
認証定義:	##MACADDRESS10## Auth-Type:=Local, User-Password=="##MACADDRESS10##"
応答定義: MACアドレスの ##MACADDRES ##MACADDRES ##MACADDRES ##MACADDRES	Tunnel-Type = 13, ← VPNトンネルのタイプ指定 Tunnel-Medium-Type = 6, ← トンネルを作成する際のプロトコル Tunnel-Private-Group-Id = 20 ← 認証済みの端末に割り当てるVLANID 変換パターン ユーザIDの変換パターン S00## → 00-11-22-33-aa-bb ##USER00## → 変換しない(Admin→Admin) S01## → 00-11-22-33-AA-BB ##USER01## → 英大文字に変換(Admin→ADMIN) S10## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin) S11## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin)
##MACADDRES	S21## → 0011.2233.AABB
##MACADDRES	300##→00:11:22:33:AA:BB ③1件 → 00:11:22:33:AA:BB
登録したり	ト MACアドレス認証 🗸 デフォルト値設定 戻る
	②「登録」ボタンをクリック

※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 VI AN 環境での MAC 認証定義 (マルチステップ認証)	例
	15.1

システム定義 -	認証情報定義編集
_	
認証情報	
グループ名:	本社
認証名:	本社認証
コメント:	
認証種別:	端末用 🔽
認証定義:	##MACADDRESS10## Auth-Type:=Local, User-Password=="##MACADDRESS10##"
応答定義: MACアドレスの ##MACADDRES ##MACADDRES ##MACADDRES ##MACADDRES	Tunnel-Type = 13, ← VPNトンネルのタイプ指定 Tunnel-Medium-Type = 6, ← トンネルを作成する際のプロトコル Tunnel-Private-Group-Id = 20, ← 認証済みの端末に割り当てるVLANID Filter-ID = 00Web-Auth80 ← MAC 認証後に使用する認証方式指定 S00## → 00-11-22-33-aa-bb ##USER00## → 変換しない(Admin→Admin) S01## → 00-11-22-33-AA-BB ##USER01## → 英大文字に変換(Admin→ADMIN) S11## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin) S11## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin)
##MACADDRES	S21## → 0011.2233.AABB
##MACADDRES	S30##→0001122333aabb S31##→00:11:2233:AA:BB ①各項目に値を入力
登録リセッ	ト MACアドレス認証 🗸 デフォルト値設定 戻る
	②「登録」ボタンをクリック

※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。

端末情報管理 -	端末情報検索								
検索 検索条件クリア 画面表示情報 ▼ CSV出力 登録用ファイル: 参照 20件見つかりました									
▲ <u>MACグループ</u>	MACTEUZ	IPアドレス	木スト名	<u>ユーザID</u>	権限	<u>ユーザ名</u>	組織名		
ong	00:21:e8:7f:83:0f	>	nomura-pc	53100200	User	野村 幸久	営業部		
ong	00:21:e8:71:83:10		kawaguchi-pc	53291084	User	川口 頼子	営業部		
ong	00:21:e8:7f:83:22		uchida-pc	53200024	User	内田 理佳子	開発部		
ong	00:21:e8:7 MAC	こアドレスの	リンクをクリック	3293097	User	細川 一絵	総務部B		

「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。

端末情報管理 - 端末情	٢RAD	IUS 認証設定」ボタ	マンをクリック		
ハードウェア情報					
MACアドレス:	00:21:e8:7f:83:0f	〈不明〉	固定IPアドレス	MACグループ	RADIUS認証設定
リース:	□無効		登録なし	登録なし	登録41.
ARP不正接続監視:	□対象外				
ユーザ情報					
⊐ _tfm.	[T0100000]		וחר	フーザ確認	

「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。

端末情報管理 -	RADIUS認証設定			
RADIUS認証設定				
MAC7Fレス:	00:21:e8:7f:83:0f			
グループ名:	本社 🗸	🦳 ①登録する認証情報定調	義を指定	
翌証名:	本社認証 🗸			
	3			
選	▲ <u>グループ名</u>	認証名	コメント	使用
ON データが	登録されていません。			
②「登録」ボタン	ン をクリック			

「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。

端末情報管理 - 端末情	翡 ₩•変更	
ハードウェア情報		
MAC7FUZ:	00:21:e8:7f:83:0f 〈不明〉	固定IPアドレス MACグループ RADIUS認証設定
リース:	一無効	登録なし 登録なし 本社:本社認証
ARP不正接続監視:	一対象外	
ユーザ情報		
⊐'=+fID+	F010000	

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。

◇利用状況モニター	端末情報管理 - 端末1	情報検索					
利用理検索	検索 検索条件	707					
	画面表示情報 🗸 🔽	CSV出力 登録用ファイル			参照 。	RADIUS 記書	〒 ◇ ●括登録
へ 不正接続モニター 不正接続IP一覧							
遮断IP一覧			⊐ – tf ID	コードタ	細葉之1	組織をつ	組織をつ
			1 210		GILLION I		
端末情報検索	検索してください。			L]			
	bond c acci o						
<u>転首情報映来</u> Infobloxi東雄							
ハユーリ情報管理							
新規登録							
≪ サーバ管理							
<u>DHCPサーバー覧</u>							
RADIUS							
◇ システム定義							
レジストラ定義							
ルータ定義							
<u>遮断装置定義</u>							
Intoblox 正義 認証法報定業							
会 運用・保全							
記動/停止							
メンテナンス							
ログ参照							
<u>AlaxalA認証ログ</u> MACID集							
PROPAGE	<						>

「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。

ペ利用状況モニター 利用理検索 端末情報配信		青報配信」を	モクリック			
利用状況モニター - 端末	情報配信					
秋態更新 人 「 秋態更新 」 日 MACアドレス数(リース有多 日本) 日本 日本	<mark>介</mark> ㈱全端 助): 20件	末情報登録 ■消費ライ・	ま,端末情報が多い場合 センス数: 20件	合、処理に時間がかかる	場合があります。	
▲ <u>サーバ名</u>	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(*)
ONGRadius01	RADIUS	なし	192.168.10.1	正常運転	登録	登録
				差分情報のみを	配信登録さ	れている全情報を配信

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。

- 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。

≪ 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		1			
遮断装置定義	認証情報定義」をクリック				
Infoblex定差		J			
認証情報定義					
	* *0-5-**				
システム定義 - 認証情	青報正義				
CSV出力 登録	用ファイル:		参照] 一括登約	禄
新規登録 件の登録	があります				
▲グループ名	認証名	コメント	認証種別	使用	削除
defat	default		端末用	Utal 1	
defau	default		ユーザ用	Utali	
「新規登録」ボタンを	クリック				

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。

システム定義 - 📲	2証情報定義編集
認証情報	
グルーブ名:	
認証名:	①「ユーザ用」を選択
コメント:	
認証種別: 🤇	ユーザ用 🗸
認証定義:	##USER00## Auth-Type=ONGAUTH
応答定義:	
MAC7FL203 ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS ##MACADDRESS	「換パターン ユーザIDの変換パターン 10## → 00-11-22-33-aa-bb ##USER00## → 変換しない(Admin→Admin) 11## → 00-11-22-33-AA-BB ##USER01## → 英大文字に変換(Admin→ADMIN) 0## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin) 1## → 00112233.aABB 10## → 0011.2233.aABB 10## → 00:11:22:33:aA:BB 1## → 00:11:22:33:AA:BB
更新 リセット	ONGユーザ認証 V デフォルト値設定 戻る
②「ONG ユーサ	「認証」を選択 ③「デフォルト値設定」ボタンをクリック



●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 W	əb 認証定義 例
-----------------	-----------

システム定義 -	認証情報定義編集						
=31=744 #2							
225E TA 42							
グルーブ名:	本社 ▼						
認証名:	本社認証						
コメント:							
認証種別:	ユーザ用 💌						
認証定義:	##USER00## Auth-Type=ONGAUTH						
応答定義:	Tunnel-Type = 13, ← VPNトンネルのタイプ指定 Tunnel-Medium-Type = 6, ←トンネルを作成する際のプロトコル Tunnel-Private-Group-Id = 20 ← 認証済みの端末に割り当てるVLANID						
MACアドレスの変換パターン ユーザIDの変換パターン ##MACADDRESS00## → 00-11-22-33-aa-bb ##USER00## → 変換しない(Admin→Admin) ##MACADDRESS01## → 00-11-22-33-AA-BB ##USER01## → 英大文字に変換(Admin→ADMIN) ##MACADDRESS10## → 00112233aabb ##USER02## → 英小文字に変換(Admin→admin) ##MACADDRESS11## → 00112233AABB ##USER02## → 英小文字に変換(Admin→admin) ##MACADDRESS20## → 00112233.aabb ##USER02## → 英小文字に変換(Admin→admin)							
##MACADDRES ##MACADDRES ##MACADDRES	S21##→0011.2233.AABB S30##→00:11:22:33:aa:bb S31##→00:11:22:33:AA:BB						
	ト ONGユーザ認証 デフォルト値設定 戻る ②「登録」ボタンをクリック						

※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	管理 - ユーザ情	報検索							
検索	検索条件クリア]							
画面表示情報 V CSV出力 登録用ファイル:									
21件見つかりま	ました								
▲ <u>ユーザID</u>	<u>ユーザ名</u>	権限	組織名1	メールアドレス	重話				
	100 Martin	~							
53100200	野村 幸久	User	営業部	y-nomura@xxx.yy.zz	432-{				
53101167	朝永 祐介	User	営業部	y-asanaga@xxx.yy.zz	432-5				
53179065		User	人事部	k-hirata@xxx.yy.zz	432-{				
E0100100	-ーザ ID をクリック	11	守幸立の	1	400.6				

「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。

ユーザ情報管理 - ユーザ情報・変更							
ユーザ情報	「RADIUS 認証設定」ボタンクリッ	<i>⁷</i>					
ユーザID:	53100200	RADIUS認証設定					
ユーザ 状態:	□ユーザを無効にする	登録起					

「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。

ユーザ情報管理	- RADIUS認証設定			
RADIUS認証設定				
ユーザID:	53100200			
グルーブ名: 認証名:	本社 ♥ 本社WEB認証 ♥	①登録する認証情報定	義を指定	
登録 削除 戻	3			
2	▲ <u>グループ名</u>	認証名	コメント	使用
ONG データが	登録されていません。			
②「登録」ボタ	マンをクリック			

「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。

ユーザ情報管理 - ユ、	- ザ情報·変更	
ユーザ情報		
ユーザID:	53100200	RADIUS認証設定
ユーザ状態:	□ユーザを無効にする	本社:本社WEB認証

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。

◇利用状況モニター	ユーザ情報管理 - ユーザ情報検索
利用PP検索	検索 検索条件クリア
	画面表示情報 ▼ CSV出力 登録用ファイルC ●登録 RADIUS認識正設定 一括登録
へ 不止接続モニター 不正接続IP→階	
<u>→ 正面にい し</u> <u>遮断IP一覧</u>	▲フーザID フーザタ 線線 保健な1 ノールフロルフ 泰計連ジ ため
≪ 端末情報管理	
<u>端末情報検索</u>	検索してください。
<u>新規登録</u>	
<u>監査情報検索</u> Totoblovi声堆	
新規支尿	
≪ サーバ管理	
<u>DHCPサーバー覧</u>	
不正接続監視	
<u>RADIUSサーバー管</u>	
≪ システム定義	
<u>コンドロニフ定義</u> レジストラ定義	
ルータ定義	
遮斯装置定義	
Intoblox定義 認証法報定差	
▲ 運用。保空	
へ 建用 体寸 記動/停止	
メンテナンス	
口グ参照	
<u>AlaxalA認証ログ</u> MACI取集	
MICHAR	

「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。

利用理検索 端末情報配信	「端末怕 	青報配信」を	ミクリック				
\mathbf{r}							
利用状況モニター - 端末	情報配信						
秋態更新 ★ ★ ★	⚠️ ^(*) 全端 劾): 20件	末情報登録 ■消費ライ†	ま,端末情報が [:] センス数: 20件	多U 1場台	3、処理に時間がかか	る場合があります。	
▲ <u>サーバ名</u>	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(
ONGRadius01	RADIUS	なし	192.168.10.1		正常運転	登録	登録
						1	\wedge

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]

- 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。

運用・保守 - AlaxalAIIIログ									
21 Iログ 🔽 🚺	検索 検索条	ミ件クリア) 🗆 м#	ACアドレス毎に	最新のみ表示 🗌 自日	动表示更新 🗌	CSV出力		
35件見つかりました。 35 年 見つかりました。									
▼日付	<u>機器IP</u>	【 【 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	コメント	忍証種別	装置日付	口グ書別	口乞種別	1	
				~		×	×		
11-05 17:14:55	alaxala			MAC	11-05 17:18:39	標準	ログイン	成功	
11-05 17:14:35	alaxala			MAC	11-05 17:18:19	標準	システム		
11-04 18:26:43	alaxala			MAC	11-04 18:30:25	標準	ログアウト	認証	
11-04 18:25:40	alaxala			MAC	11-04 18:29:22	標準	ロダイン	成功	
11-04 18:25:40	alaxala			MAC	11-04 18:29:22	標準	システム		
11-04 18:25:21	alaxala			MAC	11-04 18:29:03	標準	ログアウト	認証	
11-04 18:25:21	alaxala			MAC	11-04 18:29:03	標準	ログアウト	1211	
11-04 18:25:21	alaxala			MAC	11-04 18:29:03	標準	ログアウト	認証	
11-04 18:25:21	alaxala			MAC	11-04 18:29:03	標準	ログアウト	1211	

※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。

ペシステム定義 「♪」」・「□」・「□」	コントローラ定義」をクリック
レジストラ定義	
システムズ・コントローラ定義	①「検索結果最大表示件数」を変更
コントローラ設定	
検索結果最大表示件数: (1000 件()00~1000000)
端末情報更新問隔:	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: ④しない ○する
DHCPサーバステータスチェック間隔	品: 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	
監視間隔:	300 秒(10~86400) スコーブ更新間隔:1 分(1~60)
ARP不正接続監視設定	
○ ■ ARP不正接続監視する	範囲設定
監視間隔:	300 秒(10~86400)
○□自動収集する	
収集タイミング:	1 (1~999)回毎に自動収集する
ARP不正接続這断設定	4
不正接続這断:	□ 追断する
不正接続解除:	解除する 解除間隔: 60 秒(10~86400)
サービス設定	
─ SMTPサーバ設定	
SMTPサーバアドレス:	172.16.1.4
「更新」ボタンをクリック	SMTP認証パスワード: ○しない ⊙する
更新 DAP設定 メール5	テンプレート設定 DHCPオブション定義設定 監査設定 MACグループ定義

(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。

	運用·保守 - A/ax	alA認証プ				and the second		and the second secon		
	認証ログ V 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									
	2 2 住国つかりました									
(▼日付	<u>機器IP</u>	機器名	コメント	認証種別	装置日付	口グ識別	口乞種別	拔算	
	11-05 17:14	1			~			~		
	11-05 17:14:55	alaxala			MAC	11-05 17:18:39	標準	ログイン	成功	
	11-05 17:14:35	alaxala			MAC	11-05 17:18:19	標準	システム		

(3) CSV 出力

「CSV 出力」ボタンをクリックします。

運用・保守 - AlaxalA認証ログ											
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											
▼ <u>日付</u>	<u>機器IP</u>	機器名 コメント	認証種別	装置日付	口グ書別	<u>口グ種別</u>					
			~			~					
11-05 17:14:55	alaxala		MAC	11-05 17:18:39	標準	ログイン					
11-05 17:14:35	alaxala		MAC	11-05 17:18:19	標準	システム					
11-04 18:26:43	alaxala		MAC	11-04 18:30:25	標準	ログアウト					
11-04 18:25:40	alaxala		MAC	11-04 18:29:22	標準	ログイン					
11-04 18:25:40	alaxala		MAC	11-04 18:29:22	標準	システム					
11-04 18:25:21	alaxala		MAC	11-04 18:29:03	標準	ログアウト					
11-04 18:25:21	alaxala		MAC	11-04 18:29:03	標準	ログアウト					

「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。

ファイルのダ	۴ – ۵۷
20771/	レを聞くか、または保存しますか?
a,	名前: ong_ax_log20090114173131.csv 種類: Microsoft Office Excel CSV ファイル, 6.88 KB 発信元: 192.168.40.9 開(の) 保存の キャンセル
0	インターネットのファイルは役(こ立ちますが、ファイルによってはコンピュータに問題を 起こすものもあります。発信元が信頼できない場合は、このファイルを開いたり保 存したりしないでください。 <u>危険性の説明</u>

「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。

運用	運用・保守 — AlaxalA認証ログ												
総計ログ 検索 検索 検索 検索 CSV出力 CSV出力 CSV出力 CSV出力 CSV出力 CSV出力													
4件見	見つかりました												
	▼ <mark>日付</mark>	住 機器正 機器名 コメント 認証種別 装置日付 ログ巻別 ログ種別 抜								큀			
					~		×		成功 🔻				
04-	01 15:54:23	192.168.20.1	AX1230S		WEB	04-02 16:27:32	標準	ログアウト	成功	hi			
04-	01 15:54:04	192.168.20.1	AX1230S		WEB	04-02 16:27:10	標準	ログイン	成功	hi			
04-	01-15-25-54	100160001	000 PV4		WED	04_02 16:00:22	1曲 注于	ロバマウト	c€⊺th	hi			

(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。

運用·保守 - AlaxalA認証ログ											
認識ログ 検索 検索 MACアドレス毎に最新のみ表示 の 動表示更新 CSV出力 CSV出力											
16件見つかりました 16件見つかりました											
▼ <mark>日付</mark>	<u>機器IP</u>	機器名	コメント	認証績別	装置日付	口方嘗別	口与種別	14.25			
				*		×		失敗 🔽	D		
11-13 12:04:57	192.168.10.253	OALAN_H_01		WEB	11-13 16:49:45	通知	ログイン	天殿	sac		
11-13 11:57:05	192.168.10.253	OALAN_H_01		WEB	11-13 16:41:05	通知	ログイン	失敗	fto		
11-13 11-56-18	10216910253	∩∆L∆N H 01		WER	11-13 16/013	i面车n	ロダイン	牛肋	fto		

(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。

運用・保守 - AlaxalAZ語ログ											
MAC認識ログ 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											
▼ <mark>日付</mark>	<u>機器IP</u>	機器名	コメント	装置日付	口方营制	口与種別	状態	MAC7FUZ			
					×	~	~	00:80:45:28:44:40			
04-01 15:55:04	192.168.20.1	AX1230S		04-02 16:28:18	標準	ログアウト	認証解除	00:80:45:2a:44:4d			
04-01 15:54:52	192.168.20.1	AX1230S		04-02 16:28:04	標準	システム		00:80:45:2a:44:4d			
04_01_15/54-40	100160001	V/1000C		04_02 16/27/50	1里洪中	ミッフティー		00-00-45-244-4-4			

(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。

運用・保守 — AlaxalA認証ログ												
WEB認識ログ 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												
2件見つかりました	2件見つかりました											
▼ <mark>日付</mark>	<u>機器IP</u>	機器名	装置日付	口方营制	<u>ログ種別</u>	状態	<u>※目上一丁</u>					
				×	*		admin					
11-13 11:47:27	192.168.10.253	OALAN_H_01	11-13 16:30:23	通知	ログイン	失敗	admin	00:				
11-13 11:47:27	192.168.10.253	OALAN_H_01	11-13 16:30:23	標準	システム		admin					

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。

◇利用状況モニタ	-	サーパ管理 - DHCPサーパ編集												
<u>利用IP検索</u>		DUOD	+									_		
<u>「端末」「清辛饭吧」「言</u>		DHCP	ノーハ液種		5NODI 01									
◇ 不正接続モニタ	-	DHCP3	6:		JNGDhcpUI									
不正接続IP一覧		DHCP-	ID:		ONGDhcp01	_		権威: 未指定	*					
<u>遮断IP一覧</u>		冗長化:	:		使用しない	*								
◇ 農士快超管理		ブライマ	7UDHCPサ	ーバ			セカ	ンタリDHCPサー	-バ					
~ 雪不旧我自在		IPアドレ	ス		192.168.10.1		IP7	ドレス						
·····································		ONG制	御ボート:		1098		ONG	制御ボート:	1098					
監査情報検索		ピア通信	言ポート:		10001		Ľ7;	通信ボート:	1000	2				
Infoblox <u>連携</u>		MCLT:			秒									
◇ ユーザ情報管理		詳細設)	定											
<u>ユーザ情報検索</u>		tz	:グメント		プール	リース	範囲	サーバオプシ	個ン セグス	(ントオプシ)	シ ー	ブールオブション	/	
<u>新規登録</u>		セグン	())ト名:			ネッ	トワークア	パレス:	/	権威	未指定	*		
≪ サーパ管理		共有:	名:			_								
<u>DHCPサーバー間</u> オエキが#FEChe	Ľ.	リーフ	く時間:		秒 最大:	秒 日	赴小:	秒						
<u>小正接続電視</u> RADIUSサーバー	-暫	2 件の)登録があり	ます セ ク	ブメント追加	セグメント	編集	セグメント削除	ŧ					
◇ シフテム 完美	- W .	選択	▲tz	ラメント名	ネットワーク	アドレス	権威	共有名	リース時間	最大	最小	ブール	オプション	使用
へ システム定義			10Seg		192.168.10.0/24		未指定					未登録	未登録	する
 <u>コントローン</u>/2 レジストラ定差 							1.11.11					1.70.67	1.70.47	
ルータ定義			20Seg		192.168.20.0/24		未指定					未登録	未登録	<u>রু</u> হু

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。

E.

【MAC ア	ドレス収集初期画面】	②「MAC 収集情報」を入力
利用状況モニター 利用正検索	運用·保守 - MAC収集 MACUNE444	[/] 注)PING の送信範囲は 24 ビット範囲で 区切って送信をお願いします。
<u>端末情報配信</u> 不正接続モニター 不正接続IP一覧 <u>通断IP一覧</u>	mov理集論理 送信元IPアドレス: 192108.11 ・ ブロ ちルーブ名: マオペての切りーづり・ 送信範囲: ~ ルータ名: マオペてのリレージ・ ど信範囲: ~	▶コル: UDP ▼ ポート: [確認]
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	ドアドレス: コミュニティ名: 読置場所: 表示 MACアドレス収集 収集情報のクリア	<u> 選択ルータの 未登録MACアドレス ・</u> CSV出力
ユーザ情報管理 ユーザ情報検索 <u>新規登録</u> DHCPサーバ管理	W集情報が多い場合でも知道するのであるかのります。 <u>MACW集目時</u> <u>ルータ名</u> <u>IPアドレス</u> ▲ <u>MACアドレス</u> 表示更新を押してください。	<u>登録状態</u> ベンダー名称
<u>DHCPサーバー覧</u> <u>新規登録</u> <u>不正接続監視</u> システム定義	③「MAC アドレス収集」ボタンをクリック	
コントローラ定義 レジストラ定義 ルータ定義 追断装置定義 Infoblox定義		
選用・保守 起動/停止 メンテナンス ログキャ MAC収集	①「MAC 収集」メニューをクリック	

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】				④未登録	MAC アドレスを
利用状況モニター	運用・保守 — MAC4	皮集	CSV 形式	ファイルに出力			
端末情報配信	MAC収集情報						
不正接続モニター	表示選択 すべ	べての収集結果 🔹	送信元IPアドL	· ス: 192.168.1.1 .		-h:	
不正接続IP一覧	グループ名: くす	べてのグループ> -	送信範囲:		~	確認	
<u>遮断IP一覧</u>	ルータ名: <す	べてのルータ> 🔽					
端末情報管理	IPアドレス:						
端末情報検索	コミュニティ名:						
新規登録	設置場所:						
西 <u>且間部別思熱</u> Infobloxi庫携	表示更新 Mr	ACアドレス収集 収集情報のク	リア 🛛 🔽 日付の	新しい情報のみ表示	選択ルータの 未	登録MACアドレス 💽	CSV出力
コーザは起答理	1件のMAC収集情報があ	あります。(処理時間:0.08秒)					
ユージョ報日生	<u>MAC収集日時</u>	ルータ名	<u>IPアドレス</u>	▲ <u>MAC7ドレス</u>	登録状態	ベンダー名称	
新規登録	2008-10-03 20:17:28	ONGサーバ	10 254	<u>00: c:e1</u>	未登録	CISCO SYSTEM	
DHCPサーバ管理	2008-09-19 09:52:44	ONGサーバ	10 254	<u>00: c:e1</u>	未登録	CISCO SYSTEM	
DHCPサーバー覧	2008-09-19 09:52:44	ONGサーバ	10 245	<u>00:</u> 0:a4	未登録	SEIKO EPSON	
<u>新規登録</u>	2008-10-03 20:17:28	ONGサーバ	10 241	<u>00:</u> <u>f:d2</u>	未登録	RICOH COMPAN	
不正接続監視	2008-09-19 09:52:44	ONGサーバ	10 195	<u>00:</u> <u>7:03</u>	未登録	ACER TECHNOL	
システム定義	2008-09-18 16:10:45	ONGサーバ	10 232	<u>00:</u> <u>7:a8</u>	未登録	ACER TECHNOL	
コントローラ定義	2008-09-19 09:52:44	ONGサーバ	10 197	<u>00:</u> 6:88	未登録	ACER TECHNOL	
レジストラ定義	2008-09-19 09:52:44	ONGサーバ	10 169	<u>00: 3:01</u>	未登録	Microsoft Co	
<u>ルータ定義</u> 遠期がまま	2008-09-19 09:52:44	ONGサーバ	10 163	<u>00:</u> <u>3:01</u>	未登録	Microsoft Co	
Infoblox定義	2008-10-07 17:09:05	ONGサーバ	10 97	<u>00:</u> <u>b:38</u>	登録済	Matsushita E	
渡田- 保守	2008-10-06 10:08:32	ONGサーバ	10 73	<u>00: 8:23</u>	登録済	Matsushita E	
起動/停止	2008-09-18 16:10:45	ONGサーバ	10 178	<u>00: 6:22</u>	未登録	Multiware &	
メンテナンス	2008-09-18 16:10:45	ONGサーバ	10 240	<u>00: 1:fb</u>	未登録	Allied Teles	
ログ参照	2008-09-18 13:48:05	ONGサーバ	10 240	<u>00: 1:fb</u>	未登録	Allied Teles	
<u>MAC収集</u>	3						

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