

# リファレンスマニュアル





コンセントや配線器具の定格を超える使い方はしない たこ足配線などで定格を超えると発熱による火災の原因となります。



設置・移動のときは電源プラグを抜く

感電の原因となります。



# ご使用にあたってのお願い

# 次のような場所での使用や保管はしないでください。

- ・直射日光の当たる場所
- ・暖房器具の近くなどの高温になる場所
- ・急激な温度変化のある場所(結露するような場所)
- ・湿気の多い場所や、水などの液体がかかる場所(湿度80%以下の環境でご使用ください)
- ・振動の激しい場所
- ・ほこりの多い場所や、ジュータンを敷いた場所(静電気障害の原因になります) ・腐食性ガスの発生する場所



## 静電気注意

本製品は、静電気に敏感な部品を使用しています。 部品が静電破壊する恐れがありますので、コネクターの接点部分、ポート、 部品などに素手で触れないで下さい。

# 取り扱いはていねいに

落としたり、ぶつけたり、強いショックを与えないでください。





# 清掃するときは電源を切った状態で

誤動作の原因になります。

# 機器は、乾いた柔らかい布で拭く

汚れがひどい場合は、柔らかい布に薄めた台所用洗剤(中性)をしみこ ませ、堅く絞ったものでふき、乾いた柔らかい布で仕上げてください。



# お手入れには次のものは使わないでください

石油・みがき粉・シンナー・ベンジン・ワックス・熱湯・粉せっけん (化学ぞうきんをご使用のときは、その注意書に従ってください。)



# はじめに

このたびは、CentreCOM AR260S をお買い上げいただき、誠にありがとうございます。

CentreCOM AR260S は、IPSec に準拠した高速 VPN ルーターです。

本リファレンスマニュアルでは、CentreCOM AR260S の GUI 設定について解説しています。本製品を活用するための参考資料としてご利用ください。

なお、設定を行う前に必要なこと、たとえばルーターや LAN/WAN の配線、インターネットへの接続などについては説明しておりません。これらに関しては、製品付属の冊子「取扱説明書」をご覧ください。

# 本書の構成

#### 章構成

本書は大きな機能ごとに、以下のような章構成になっています。また、各章では一部を除き、「機能の概要」、「設定手順」、「設定画面の解説」の流れになっています。

#### 「1 運用・管理」では

本製品の運用・管理に関する以下の設定について説明します。

- · ログイン / ログオフ
- · 再起動
- 設定内容の初期化 / バックアップ / 復元
- · ファームウェアの更新
- · 設定管理クライアント / パスワードの設定
- · SNMP エージェントの設定
- ・ システム情報の設定
- ・ システム情報の確認
- · システム時刻 /SNTP サーバーの設定
- · ファイアウォール、VPN など各機能の有効化 / 無効化
- ・ ログの記録

#### 「2 LAN 側インターフェースの設定」では

LAN 側インターフェースの IP 情報や DHCP サーバー機能に関する設定について説明します。

#### 「3 WAN 側インターフェースの設定」では

WAN 側の接続形態別(DHCP、PPPoE、固定 IP)に WAN 側インターフェースに関する設定について説明します。

#### 「4 ルーティングの設定」では

ルーティングに関する設定について説明します。本製品では、スタティックルーティングをサポートしています。

#### 「5 ファイアウォールの設定」では

ファイアウォール機能に関する設定について説明します。本製品のファイアウォール機能は大きくわけて以下の 6 つになります。

- ・ Inbound アクセス
- ・ Outbound アクセス
- · ステルスモード
- ・ セルフアクセス
- ・ URL フィルター
- ・ DoS アタックプロテクト

#### 「6 各種ポリシーとサービスの設定」では

「5 ファイアウォールの設定」で使用する各種ポリシー(IP プール、NAT プール)とサービスに関する設定について説明 します。

「7 VPN の設定」では

VPN 機能に関する設定について説明します。本製品の VPN 機能は IPSec に準拠しています。

# 表記上の注意

本書で使用しているアイコンは次の意味で使用しています。

アイコン	意味	説明	
シント       知っていると便利な情報、操作の手助けになる情報を示していていた。                 注意             注意		知っていると便利な情報、操作の手助けになる情報を示しています。	
		物的損害や使用者が傷害を負うことが想定される内容を示しています。	
		使用者が死亡または重傷を負うことが想定される内容を示しています。	
		関連する情報が書かれているところを示しています。	

# 例について

本書では、設定画面に数多くの入力例を使用しています。電話番号、IP アドレス、ドメイン名、ログイン名、パスワードなどに具体的な文字列や値を使用していますが、これらは例として挙げただけの架空のものです。実際に運用を行う場合は、お客様の環境におけるものをご使用ください。

# 最新情報

製品の出荷後は、弊社 Web サイトでマニュアル等の正誤情報や改版されたマニュアル、アップデートされたファームウェアな どの最新の情報を公開しています。

http://www.allied-telesis.co.jp/

# 目次

は	じめに.				5
本	書の構成	戓			5
表	記上のシ	注意			6
例	につい	τ			7
最	新情報.				7
1	運用·	管理.			15
		1.1	ログイ		15
		1 2	<b>五記</b> 動		16
		1.2			17
		1.3			17
		1.4	機能の	有効化 / 無効化の設定	18
			1.4.1	概要	. 18 10
			1.4.2	做能の有効化 / 無効化 · · · · · · · · · · · · · · · · · · ·	20
			1.4.4	「サービスの有効 / 無効」ページの解説	. 20
		15	設定管	理クライアント / ログインパスワードの設定	22
		1.0	151		22
			1.5.2	設定管理クライアントの設定	22
				1.5.2.1 設定管理クライアントの作成	. 22
				1.5.2.2 設定管理クライアントの変更	. 24
				1.5.2.3 設定管理クライアントの削除	. 24
				1.5.2.4 設定管理クライアントの確認	. 24
			1. 5. 3	パスワードの設定	. 25
			1. 5. 4	「設定管理クライアント / パスワード」ページの解説	. 26
				1.5.4.1 設定管理クライアント	. 26
				1.5.4.2 パスワード	. 28
				1.5.4.3 設定管理クライアントリスト	. 29
		1.6	システ	ム情報の設定	30
			1. 6. 1	概要	. 30
			1.6.2	設定	. 30
			1.6.3	確認	. 31
			1.6.4	「システム情報」ページの解説	. 32
		1.7	システ	ム時刻の設定	33
			1. 7. 1	概要	. 33
			1. 7. 2	システム時刻の設定	. 33
			1.7.3	システム時刻の確認	. 34
			1.7.4	SNIP サーハーの設定	. 35
			1. /. 5	「ダイムソーン設定」へーンの解説	30 26
				1.7.5.1 ライムノーン設定	. JU 27
				I. /. J. Z SNIF リーヒスの設定	. 37

	1.8	3 SNMP I	ージェントの設定	38
		1. 8. 1	概要	38
		1. 8. 2	SNMP エージェントの設定	38
		1.8.3	SNMP 設定情報の確認	39
		1. 8. 4	「SNMP」ページの解説	39
			1.8.4.1 SNMP 設定	39
			1.8.4.2 SNMP 設定情報	40
	1.9	9 ログの	記録	41
		1. 9. 1	概要	41
		1. 9. 2	ログの設定	41
		1.9.3	ログの確認	42
		1. 9. 4	「ログ」ページの解説	42
			1.9.4.1 システムロク設定	42
			1.9.4.2 ログリスト	43
	1. 1	10 設定の	初期化	44
		1. 10. 1	GUI 設定画面からの初期化	44
		1. 10. 2	リセットスイッチによる初期化	45
	1. 1	11 設定内	容のバックアップ	46
	1. 1	12 バック	アップファイルの復元	48
	1	13 77-	ムウェアの面新	50
				00
2	LAN 側イン	ノターフェ	.ースの設定	53
	2	1 概要		53
	2.	י איבעייי	、	E0
	Ζ. 4			53
		2.2.1	設定	53
		Z. Z. Z 2 2 2	催認	54
		Z. Z. J	「N」、「ノの解説	55
			2.2.3.1 日本の設定	55
	o <i>4</i>			56
	Ζ			50
		2.3.1	テノオルト設定	50
		2.3.2 2.2.2	設正	57
		2.3.3	催認 「DHCP」ページの磁話	60
		2. 0. 4	2 3 4 1 DHCP サーバー設定	60
			2.3.4.2 現在の設定	61
			2.3.4.3 クライアントー管	62
	2.4	4 IPアド	レスの静的割り当ての設定	63
		2. 4. 1	設定	63
		2. 4. 2	固定 DHCP クライアントの削除	63
		2.4.3	確認	64
		2. 4. 4	「固定 DHCP クライアント」ページの解説	64
		2. 4. 5	固定 DHCP クライアント設定	64
		2. 4. 6	固定 DHCP クライアントー覧	65
	2. 5	5 トラフ	ィックの確認	66
		2. 5. 1	確認	66
		2. 5. 2	「統計情報」ページの解説	67

3	WAN 側インタ	マーフェースの設定	69
	3. 1	概要	69
	3. 2	DHCP を使用した WAN 側ネットワークへの接続	69
		3.2.1 設定	69
		 3.2.2 設定の確認	70
	3.3	PPPoE を使用した WAN 側ネットワークへの接続	71
		3.3.1 設定	
		3.3.2 設定の確認	73
		3.3.3 PPPoE セッションの切断 / 接続	73
	3.4	固定 IP アドレスを使用した WAN 側ネットワークへの接続	74
		3.4.1 設定	74
		3.4.2 設定の確認	76
	3.5	「WAN」ページの解説	76
		3.5.1 WAN 設定	76
		3.5.1.1 接続モードに「DHCP」を選択した場合	77
		3.5.1.2 接続モードに「PPPoE」を選択した場合	79
		3.5.1.3 接続モードに「固定 IP」を選択した場合	83
	3.6	トラフィックの確認	85
		3.6.1 確認	85
		3.6.2 「統計情報」ページの解説	86
4	ルーティング	クの設定	87
	4. 1	概要	87
	4. 2	スタティックルーティング	87
		4.2.1 設定	87
		4.2.2 設定の確認	89
		4.2.3 スタティックルーティングの変更	89
		4.2.4 スタティックルーティングの削除	89
	4.3	「ルーティング」ページの解説	90
		4.3.1 スタティックルーティング設定	90
		4.3.2 ルーティングテーブル	91
F	<b>フ</b> _ / <b>フ</b> +		00
5	ノアイアリテ	オールの設定	93
	5. 1	概要	93
	5.2	Inbound アクセスルールの設定	93
		5.2.1 ルールの作成	93
		5.2.2 ルールの変更	95
		5.2.3 ルールの削除	95
		5.2.4 ルールの確認	
		5.2.5 IIDDOUND アクセス」へーンの解説 5.9.5.1 Inbound アクセス型御設ティーブル	
		5.2.5.1 Inbound アクセス制御以たデーフル 5.2.5.2 Inbound アクセス制御リスト	101
	E O	0.2.0.2 modula アクセスリールの恐宁	100
	5.3	Outpound アクセムルールの設定	102
		5.3.I テノオルトホリン一	102
		5.3.2 ルールの変更	103
		5.3.4 ルールの削除	105

		5.3.5	ルールの確認	105
		5.3.6	「Outbound アクセス」ページの解説	105
			5.3.6.1 Outbound アクセス制御設定	105
			5.3.6.2 Outbound アクセス制御リスト	110
	54	ステル	スモードの設定 1	11
	0.4	5 1 1		111
		J. 4. 1		111
	5.5	セルノ	アクセスルールの設定・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ΤZ
		5.5.1	デフォルト設定	112
		5.5.2	ルールの作成	113
		5.5.3	ルールの変更	114
		5.5.4	ルールの削除・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	114
		5.5.5		114
		5.5.6	「セルノアクセス」ヘーンの解説	115
			5.5.6.1 セルノアクセス設定	115
			5.5.6.2 セルフアクセスルール	116
	5.6 l	JRLフィ	ィルターの設定 1	17
		5.6.1	URL フィルターの有効 / 無効	117
		5.6.2	キーワードの追加	117
		5.6.3	プロキシーポートの変更	118
		5.6.4	キーワードの削除	118
		5.6.5	キーワードの確認	118
		5.6.6	「URL フィルター」ページの解説	119
			5.6.6.1 URL フィルター設定 /URL フィルターテーブル	119
			5.6.6.2 現在のフィルター設定	120
	5.7 E	DoSアク	タックプロテクトの設定 1	21
		5. 7. 1	デフォルト設定	121
		5.7.2	DoS アタックプロテクトの有効 / 無効	121
		5.7.3	DoS アタックプロテクトリストの確認	122
		5.7.4	「DoS」ページの解説	123
			5.7.4.1 DoS アタックフィルター設定	123
			5.7.4.2 DoS アタックプロテクトリスト	124
	58	トラフ	イックの確認 1	25
	0.0	5 9 1		125
		582	11年記	125
		J. 0. Z	「Null       和山 ( ) の時前	120
			5. 8. 2. 2 Total Connections Count	120
				120
6	久毎ポリシー	レ++-	- ビスの設定 1	20
U	古性ハリノ	2.9		ΖĴ
	6.1	概要	1	29
	6. 2	IP プー	・ルの設定	29
		621	IP プールの追加	129
		622	Pプールの変更	130
		6. 2. 3	IP プールの削除	130
		6. 2. 4	IP プールの確認	131
		6. 2. 5	「IP プール」ページの解説	132
			6.2.5.1 IP プール設定	132
			6.2.5.2 IP プールリスト	133
	6.3 M	VAT プ-	ールの設定 1	34
	0.0 1	6 2 1	// // // // // // // // // // // // //	124
		U. U. I		104

		6.3.2	NAT プールの変更	135
		6.3.3	NAT プールの削除	135
		6.3.4	NAT プールの確認	136
		6.3.5	「NAT プール」ページの解説	136
			6.3.5.1 NAT プール設定	136
			6.3.5.2 NAT プールリスト	138
	6.4 サ	ナービス	への設定	139
		6.4.1	サービスの作成	139
		6.4.2	サービスの変更	140
		6.4.3	サービスの削除	140
		6.4.4	サービスの確認	141
		6.4.5	「サービス」ページの解説	142
			6.4.5.1 サービス設定	142
			6.4.5.2 サービスリスト	143
7	VPNの設定			. 145
	7.1 根	既要		. 145
	7 0 VI	// DN のヺ	ι <u>⇔</u>	145
	1. Z VI			140
		7.2.1	ホリシーの作成	145
		7.2.2	ホリンーの変更	148
		1.2.3	ホリンーの削除	149
		1. 2. 4 7 9 5	小リンーの確認	149
		1. 2. 5	│VIN	149
			7. 2. 5. Ⅰ VFN 接枕設と	150
			/. Z. J. Z INE 設定	153
			7.2.5.3 IPSec 設定	154
		7.2.6	サイト間アクセスルール	155
	7.3 VI	PN トラ	ラフィックの確認	156
		7.3.1	確認	156
		7.3.2	「統計情報」ページの解説	158
			7.3.2.1 VPN Statistics	158
			7.3.2.2 IKE SA	160
			7.3.2.3 IPSec SA	160
0	/ 43			1.01
8	1寸琢			. 101
	8.1 <del>7</del>	デフォノ	レト設定	161
	:	8. 1. 1	ユーザー名 / パスワードのデフォルト設定	161
	1	8. 1. 2	設定ページ別のデフォルト設定	161
	82 N/	AT 1		163
	0.2 1	8 2 1	マタテノック NAT	163
		822	ベテリュ ジン NAT	164
		823	FNAT	164
		8. 2. 4		165
	83 4	トラブリ	レシューティング	165
	0.0 1	021	マン ユー リー 1 イン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	165
	· · · · · · · · · · · · · · · · · · ·	U. J. I	LLU に因うのドノノル	165
			o. v. i ・ 电标で a イン C C C I OTELL LLD A 古方 J C G V' ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	100
			0. 0. 1. 2 011 ノーフルで12 10/10 して 0 11/11 LLD が出対しない	160
		0 0 0	0. 3. 1. 3 UIF ゲーノルを按続しても LAN LEU か品灯 しない	100
		ö. 3. 2	1 ンダーネットへのアクセスに関するトフフル	166

	8.3.2.1 インターネットにアクセスできない1	66
	8.3.2.2 Web ページを表示できない1	66
8.3.3	GUI 設定に関するトラブル1	67
	8.3.3.1 ログインバスワートを忘れた	07
	8.3.3.2 設定回面が表示されない	07
ご注意		39
商標について		39
マニュアルバージョン	,	39

# 1 運用·管理

本章では、本製品の運用・管理に関する以下の設定について説明します。

- ・ ログイン
- · 再起動
- ・ ログアウト
- 機能の有効化 / 無効化
- · 設定管理クライアント / パスワードの設定
- ・ システム情報の設定
- ・ システム時刻の設定
- · SNMP エージェントの設定
- 設定の初期化
- ・ 設定内容のバックアップ
- · 設定内容の復元
- · ファームウェアの更新
- ・ ログの記録
- ・ システム情報の確認

### 1.1 ログイン

本製品にログインするには以下の手順を実行します。



ここでは、本製品の LAN 側インターフェースの IP アドレスがデフォルト設定 (192.168.1.1) であるものとします。

1. Web ブラウザーを起動後、アドレス欄に「192.168.1.1」を指定してアクセスします。

ダイアログで「ユーザー名」と「パスワード」を入力し「OK」ボタンをクリックします。本製品のデフォルトではユーザー名「manager」、パスワード「friend」です。

192.168.1.1 に接続	? 🛛
	ALL ARE
AR260S	
ユーザー名(山):	🖸 manager 💌
パスワード( <u>P</u> ):	*****
	□パスワードを記憶する(R)
	OK ++>>tz/

3. 本製品の設定画面が表示されたらログインは完了です。

### 1.2 再起動

#### 本製品を再起動するには以下の手順を実行します。

1. メニューから「再起動」をクリックします。



2.「適用」ボタンをクリックします。

tmi	
	Allied Telesis
再起動	
再起動完了後、ブラウザを	更新してください
(通用)	
Ū	

以下の画面が表示され、再起動に必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。

	📣 🖉 Allied Telesis
システムが再起動されました。	
再起動が完了するまであと 53 秒です。再起動完了後、自動的に本製品に再接続されます。	

4. カウントダウンが終了すると、以下のダイアログが表示されます。

Microso	ft Internet Explorer 🛛 🗙
?	IPアドレス 1921681.1. で本製品に再接続する場合は「OK」、それ以外の場合は「キャンセル」をクリックしてください。デフォ ルトのIPアドレスを変更した場合は「キャンセル」をクリックし、変更後のIPアドレスで再接続してください。
	OK キャンセル

本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

5.以上で再起動は完了です。

# 1.3 ログアウト

本製品からログアウトするには以下の手順を実行します。

1. メニューから「ログアウト」をクリックします。



2.「適用」ボタンをクリックします。

	Allied Telesis
ログアウト	
ログアウトするには「適用」ボタンをクリックしてください	
「適界」	
V	

3. 以下のダイアログが表示されたら「はい」ボタンをクリックします。



4. 以上でログアウトは完了です。

# 1.4 機能の有効化 / 無効化の設定

#### 1.4.1 概要

本製品では、以下の各種機能を「サービスの有効/無効」ページで有効化/無効化することができます。

- ファイアウォール機能
- · VPN 機能
- ・ DNS リレー機能
- ・ DHCP サーバー機能
- · SNTP 機能
- ・ リセットスイッチによる初期化機能

#### 1.4.2 機能の有効化 / 無効化

各機能を有効化 / 無効化するには以下の手順を実行します。

1.メニューから「システム管理」->「サービスの有効/無効」の順にクリックします。

CentreCOM AR260S - Microsoft 1	Internet Explorer			🗖 🗗 🔽
ファイル(E) 編集(E) 表示(V) お気に入り	)(A) ツール(D) ヘルプ(H) 🛛 🏹	🌶 🖉 • त्रेत्रक्रेप्र	検索 🔹 Yahoo! JAPANに接続中	<b>A</b> *
VPN Router				Allied Telesis
		サービス	の有効/無効	
	ファイアウォール	◎有効 ○無効		
Ē	VPN	◎有効 ○無効		
	DNSUL-	◎有効 ○無効		
CentreCOM AR260S	DHCP	◎有効 ○無効		
セットアップウィザード	SNTP	○有効 ⊙無効		
	リセットスイッチによる初期化	◎有効 ◎無効		
🕀 🦲 WAN			適用	(ヘルプ)
ー D ルーティング 中 つ ファイアウォール				
- 日ク				
サービスの有効/無効				
- 再起動				

2. 機能の有効 / 無効を選択し、「適用」ボタンをクリックします。ここでは、以下の機能を無効にしています。

- · VPN
- · SNTP
- ・ リセットスイッチによる初期化

ファイアウォール	◎有効 ○無効	
VPN	○有効 ◎無効	
DNSリレー	◎有効 ○無効	
DHCP	◎有効 ○無効	
SNTP	○有効 ◎無効	
リセットスイッチによる初期化	○有効 ⊙無効	

3.以上で設定は完了です。

#### 1.4.3 機能の有効 / 無効の確認

#### 機能の有効 / 無効を確認するには以下の手順を実行します。

1. メニューから「システム情報」をクリックします。

2.「システムサービス」に機能の有効/無効が一覧表示されます。

	システムサービス	
ファイアウォール	有効	
VPN	無効	
DHCP	有効	
DNSリレー	有効	
SNTP	無効	
リセットスイッチによる初期化	有効	

#### 1.4.4 「サービスの有効 / 無効」ページの解説

サービスの有効 / 無効ページについて解説します。「サービスの有効 / 無効」ページでは、サービスを有効 / 無効にする ことができます。

メニューから「システム管理」->「サービスの有効/無効」の順にクリックすると設定画面が表示されます。

ファイアウォール	◉有効	○無効	
VPN	○有効	⊙ 無効	
DNSリレー	⊙有効	○無効	
DHCP	⊙有効	○無効	
SNTP	○有効	⊙ 無効	
リセットスイッチによる初期化	◎有効	○無効	

パラメーター	オプション	説明
ファイアウォール	有効 / 無効	ファイアウォール機能を有効にする場合 は「有効」、無効にする場合は「無効」 ラジオボタンをクリックします。ファイ アウォールを無効にした場合、外部から のアクセスが容易になりますのでご注意 ください。ファイアウォールの設定につ いては「P.93 ファイアウォールの設定」 を参照してください。デフォルトは「有 効」です。
VPN	有効 / 無効	VPN サービスを有効にする場合は「有 効」、無効にする場合は「無効」ラジオ ボタンをクリックします。「P.145 VPN の設定」の設定を行う場合は、あらかじ め VPN サービスを有効にしてください。 デフォルトは「無効」です。
DNS リレー	有効 / 無効	DNS リレー機能を有効にする場合は「有 効」、無効にする場合は「無効」ラジオ ボタンをクリックします。デフォルトは 「有効」です。
DHCP	有効 / 無効	DHCP サーバー機能を有効にする場合は 「有効」、無効にする場合は「無効」ラジ オボタンをクリックします。無効にした 場合は、LAN 内のコンピューターの IP 設定を正確に行ってください。DHCP サーバー機能の詳細については「P.56

		DHCP サーバーの設定」を参照してくだ さい。デフォルトは「有効」です。
SNTP	有効 / 無効	外部 SNTP サーバーから時刻情報を取得 する場合は「有効」、取得しない場合は 「無効」ラジオボタンをクリックします。 SNTP サーバーの詳細については「P.33 システム時刻の設定」を参照してくださ い。デフォルトは「無効」です。
リセットスイッチによる初期化	有効 / 無効	リセットスイッチを押した場合に、本製 品の設定をデフォルト値に戻す機能を有 効にする場合は「有効」、リブートのみ 行う場合は「無効」ラジオボタンを選択 します。デフォルトは「有効」です。 「リセットスイッチによる初期化」を無 効にした状態で、管理者パスワードを忘 れた場合、本製品の設定を初期化するこ とができなくなりますのでご注意ください。
「適用」ボタン		設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

### 1.5 設定管理クライアント / ログインパスワードの設定

#### 1.5.1 概要

本製品では、「設定管理 / パスワード」ページで、クライアントに対して本製品の設定権限を付与し、設定管理クライア ントとして登録することができます。また、ログインパスワードは管理者レベルのユーザーとユーザーレベルのユーザー に対してそれぞれパスワードが設定されています。ここでは、設定管理クライアントとパスワードに関して説明します。

#### 1.5.2 設定管理クライアントの設定

ここでは、設定管理クライアントの設定方法について説明します。

#### 1.5.2.1 設定管理クライアントの作成

設定管理クライアントを作成するには以下の手順を実行します。



設定管理クライアントを設定した場合、設定されたクライアント以外からは本製品の設定ができませんのでご注意く ださい。

1.メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。

PN Router			Alleo le
		設定管理クライアント	
	ID 新規追加 🗸		
C	グループ形式	<ul> <li>● IPアドレス ○ 範囲指定 ○ サ</li> </ul>	ブネット
	IPアドレス		
entreCOM AR260S		追加 変更 削	除 ヘルプ
] セットアッブウィザード ] システム情報			
LAN		パスワード	
】WAN 】ルーティング	現在の管理者バスワード		
ファイアウォール		新しいパスワード	]
」VPN ]ログ	管理者バスリード	バスワードの確認	Ĩ
】システム管理 	ere solo concolo mar	新しいパスワード	1
設定管理ルイスワード	ユーザーバスワード	バスワードの確認	1
		通用	(ヘルノ
→ → ンステムの設定 → → ファームウェアの更新 → 再記動		設定管理クライアントリス	F
ログアウト	ID	グループ形式	グループアドレス

2.「設定管理クライアント」テーブルの ID ドロップダウンリストから「新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のように設定するものとします。

グループ形式	範囲指定
始点 IP アドレス	192.168.1.10
終点 IP アドレス	192.168.1.13

ID 新規追加 🖌		
グループ形式	○ IPアドレス ③ 範囲指定 ○ サブネット	
始点IPアドレス	192.168.1.10	
終点IPアドレス	192.168.1.13	
	(10+10) 水西 (11)除	



WAN 側のクライアントを設定管理クライアントとして追加した場合、セルフアクセスルールで WAN 側からのアクセ スについて HTTP の 80 番ポートをオープンする必要があります。セルフアクセスルールについては「P.112 セルフア クセスルールの設定」を参照してください。

4. 以上で設定は完了です。

#### 1.5.2.2 設定管理クライアントの変更

#### 設定管理クライアントを変更するには以下の手順を実行します。

- 1.メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
- 2. ID ドロップダウンリストから変更するクライアントの ID を選択します。または、「設定管理クライアントリスト」テーブルの該当クライアント左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

#### 1.5.2.3 設定管理クライアントの削除

- 1.メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
- 2. ID ドロップダウンリストから削除するクライアントの ID を選択し「削除」ボタンをクリックします。または、「設定管理ク ライアントリスト」テーブルの該当クライアント左部にある「ごみ箱」アイコンをクリックします。
- 3. 以上で設定は完了です。

#### 1.5.2.4 設定管理クライアントの確認

1.メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。

2.「設定管理クライアントリスト」テーブルにクライアントが一覧表示されます

		設定管理クライアントリスト	
	ID	グループ形式	グループアドレス
/ 🖻	1	範囲指定	192.168.1.10~192.168.1.13

### 1.5.3 パスワードの設定

本製品に設定されている管理者レベル / ユーザーレベルのパスワードは以下のとおりです。ここでは、パスワードの設定について説明します。

ユーザー名	レベル	パスワード
manager	管理者	friend
guest	ユーザー	guest

#### 1.メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。

アドレス(1)) 🍓 http://192.168.1.1/index.h	tml		💌 🔁 移動
VPN Router			Allied Telesis
		設定管理クライアント	
	ID 新規追加 🔽		
C	グループ形式	<ul> <li>● IPアドレス ○ 範囲指定 ○</li> </ul>	サブネット
	IPアドレス		
CentreCOM AR260S		追加 変更	削除 ヘルプ
── <b>─</b> ─ <b>─</b> セットアップウィザード ── <b>─</b> システム情報			
E LAN		パスワード	
WAN	現在の管理者バスワード		
□ ファイアウォール	倍理者パラワーに	新しいパスワード	
- <b>0</b> 09	Even (XXX)	バスワードの確認	
□□□ システム管理 □□□□ サービスの有効/筆効		新しいバスワード	
設定管理パスワード	ユーザーパスワード	バスワードの確認	=
		通用	
		設定管理クライアントリ	71
	ID	グループ形式	グループアドレス

2.「パスワード」テーブルで各パラメーターを入力し、「適用」ボタンをクリックします。ここでは、現在の管理者レベルのログ インパスワード「friend」を「ar260s」に変更するものとします。

••••••
2



「現在の管理者パスワード」には、現在設定されている管理者レベルのパスワードを入力してください。

3. ログイン画面が表示されますので、「パスワード」に新しく設定したパスワードを入力して「OK」ボタンをクリックします。

192.168.1.1 に接続	? 🔀
AR260S	
ユーザー名(山):	🖸 manager 💌
パスワード( <u>P</u> ):	*****
	□パスワードを記憶する( <u>R</u> )

4. 以上で設定は完了です。

1. 5. 4 「設定管理クライアント / パスワード」ページの解説

「設定管理クライアント / パスワード」ページについて解説します。

#### 1.5.4.1 設定管理クライアント

設定管理クライアントとは、本製品の設定権限をもつクライアントです。「設定管理クライアント」テーブルでは、クラ イアントを IP アドレスで指定して、本製品の設定権限を付与することができます。

設定管理クライアント		
ID 新規追加 🖌		
グループ形式	● IPアドレス ○ 範囲指定 ○ サブネット	
IPアドレス		
	追加 変更 削除	ヘルプ



パラメーター	オプション	説明
IDドロップダウンリ	Z F	設定管理クライアントを新規に追加する 場合は「新規追加」、既存のクライアン トの設定を変更 / 削除する場合は該当の ID 番号を選択します。
グループ形式		クライアントの指定方法を選択します。
	IPアドレス	クライアントを IP アドレスで指定する 場合に選択します。
	範囲指定	クライアントを IP アドレスの範囲で指 定する場合に選択します。

サブネット	クライアントをサブネットで指定する場 合に選択します。
IP アドレス	グループ形式に「IP アドレス」を選択し た場合にのみ表示されます。クライアン トの IP アドレスを入力します。
始点 IP アドレス / 終点 IP アドレス	グループ形式に「範囲指定」を選択した 場合にのみ表示されます。指定する IP アドレスの範囲の始点 / 終点 IP アドレ スを入力します。
ネットワークアドレス	グループ形式に「サブネット」を選択し た場合にのみ表示されます。指定するク ライアントのネットワークアドレスを入 力します。
サブネットマスク	グループ形式に「サブネット」を選択し た場合にのみ表示されます。指定するク ライアントのサブネットマスクを入力し ます。
「追加」ボタン	ドロップダウンリストで「新規追加」を 選択した場合にアクティブになります。 クライアントを追加登録します。8件ま でのエントリーを追加することができま す。ボタンをクリックすると設定内容が 即時に反映されます。
「変更」ボタン	ドロップダウンリストで既存のクライア ントの ID 番号を選択した場合にアク ティブになります。設定内容の変更を保 存します。ボタンをクリックすると設定 内容が即時に反映されます。
「削除」ボタン	ドロップダウンリストで既存のクライア ントの ID 番号を選択した場合にアク ティブになります。選択したクライアン トを削除します。ボタンをクリックする と設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

### 1.5.4.2 パスワード

#### 本製品には以下の2種類のユーザー名/パスワードがあります。

ユーザー名	パスワード	説明
manager	friend	管理者レベルのユーザー名とパスワード です。管理者には設定変更の権限があり ます。パスワードは変更することができ ますが、ユーザー名を変更することはで きません。
guest	guest	ユーザーレベルのユーザー名とパスワー ドです。設定を参照することはできます が、変更する権限はありません。パス ワードは変更することができますが、 ユーザー名を変更することはできません。

#### 「パスワード」テーブルでは、本製品のユーザー(manager/guest)に対してパスワードを設定します。

			パスワー	-F	
	現在の管理者バス	マワード			
	管理者バフワード		新しいパスワード		
	64±181/2271		バスワードの確認		
		1	新しいパスワード		
		T.	バスワードの確認		
			通用		
パラ	パラメーター オプション 説明				
現在	の管理者パスワ-	- F			「管理者パスワード」、「ユーザーパス ワード」を設定する前に現在の管理者 スワードを入力します。ここに誤った スワードを入力した場合、以下のパス ワードの設定ができません。
管理	者パスワード				「manager」に対するパスワードを設定! 更します。
	_	新しいパスワー	۲		新しく設定するパスワードを入力しま す。半角英数字で 16 文字以内で入力し てください。
		パスワードの確	認		確認のために、再度同じパスワードを, カします。
<u>–</u> ـ	ザーパスワード				「guest」に対するパスワードを設定変更 します。
	_	新しいパスワー	۴		新しく設定するパスワードを入力しま す。半角英数字で 16 文字以内で入力し てください。
	_	パスワードの確	<b>認</b>		確認のために、再度同じパスワードを, 力します。

「適用」ボタン	設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

#### 1.5.4.3 設定管理クライアントリスト

「設定管理クライアントリスト」テーブルには、「設定管理クライアント」で設定したクライアントが一覧表示されます。

	設定管理クライアントリスト	
ID	グループ形式	グループアドレス
1 📅 🖉	範囲指定	192.168.1.10~192.168.1.13

パラメーター	説明
ID	クライアントの ID が表示されます。
グループ形式	クライアントの指定形式が表示されま す。
グループアドレス	クライアントの IP 情報が表示されます。
「えんぴつ」アイコン	クリックすると「設定管理クライアント リスト」の該当クライアントの設定内容 を変更することができます。
「ごみ箱」アイコン	クリックすると「設定管理クライアント リスト」から該当クライアントを削除し ます。



設定管理クライアントリストに表示されたクライアント以外からは本製品にアクセスできませんのでご注意ください。

### 1.6 システム情報の設定

#### 1.6.1 概要

本製品では「システム情報」ページで「システム名 (SysName)」、「システムロケーション (SysLocation)」、「連絡先 (SysContact)」を設定することができます。ここでは、システム情報の設定について説明します。

#### 1.6.2 設定

システム情報を設定するには以下の手順を実行します。

1.メニューから「システム管理」->「システム情報」の順にクリックします。

アドレス(D) 🍓 http://192.168.1.1/index.html			💙 🄁 移動
VPN Router			Allied Telesis
	システム情報		
	システム名(SysName)	AR260S	(オプション)
-	システムロケーション(SysLocation)		(オプション)
	連絡先(SysContact)		(オプション)
CentreCOM AR260S			用 へルプ
サービスの有効/無効			
タイムソージ設定			
□ SNMP □ □ システムの設定			
ログアウト			

2. 各パラメーターを入力し「適用」ボタンをクリックします。ここでは、以下のように設定するものとします。

システム名(SysName)	AR260S
システムロケーション (SysLocation)	tokyo
連絡先(SysContact)	03-1111-2222

			Allied lelesi
	<b>シ</b>	ステム情報	
システム名(SysName)	AR260S	(オプション)	
システムロケーション(SysLocation)	tokyo	(オプション)	
連絡先(SysContact)	03-1111-2222	(オプション)	
		<u>la</u> p	ヘルプ

3.以上で設定は完了です。

### 1.6.3 確認

#### システム情報を確認するには以下の手順を実行します。

#### 1. メニューから「システム情報」をクリックします。

: ファイル(E) 編集(E) 表示(V) お気に人	り(A) ツール(エ) ヘルプ(H)	1 X? » 🧃
: アドレス① 🥘 http://192.168.1.1/index.html		💌 🔁 🕅
VPN Router		Allied Telesi
		システム情報
	ファームウェアバージョン	AR260S.1.1.XXx.410, May 31 2004, 18:11:38
-	LAN側IPアドレス	192.168.1.1
	WAN側MACアドレス	00:09:41:7e:e0:0b
	LAN側MACアドレス	00:09:41:7e:e0:0c
CentreCOM AR260S	システム起動時間	3日23時間29分52秒
	システム名(SysName)	AR260S
システム 精報	システムロケーション(SysLocation)	
	連絡先(SysContact)	
		LAN側設定
□ ルーナインシ  〒- <mark>□ ファイアウォール</mark>	LAN側IPアドレス	192.168.1.1
	LAN側サブネットマスク	255.255.255.0
<b>  - - - - - - -</b>		WAN側設定
□□システム管理	WAN側接続モード	固定IP
	WAN側接続状況	接続
	WAN側IPアドレス	200.100.10.54
	WAN側サブネットマスク	255.255.255.0
	デフォルトゲートウェイアドレス	200.100.10.1
	プライマリDNSサーバー	200.100.10.32
	セカンダリDNSサーバー	
		システムサービス
	ファイアウォール	有効
	VPN	有効
	DHCP	有効
	DNSリレー	有効
	SNTP	無効
	UPnP	有効
	リセットスイッチによる初期化	有効

#### 2.「システム情報」に設定したシステム情報が表示されます。

	システム情報	
ファームウェアバージョン	AR260S.1.1.XXx.410, May 26 200	04, 19:16:48
LAN側IPアドレス	192.168.1.1	
WAN側MACアドレス	00:09:41:7e:e0:0b	
LAN側MACアドレス	00:09:41:7e:e0:0c	
システム起動時間	0日2時間2分49秒	
システム名(SysName)	AR260S	
システムロケーション(SysLoca	tion) tokyo	
連絡先(SysContact)	03-1111-2222	
	LANの開始空	
パラメーター		説明
ファームウェアバージョン		本製品のファームウェアのバージョンが 「1.1.XXx.410」のように表示されます。 「XX」の部分には数字、「x」には小文字 の英字が表示されます。
LAN 側 IP アドレス		本製品の LAN 側インターフェースの IP アドレスが表示されます。
WAN 側 MAC アドレス		本製品の WAN 側の MAC アドレスが表示 されます。プロバイダーに本製品の MAC アドレスを通知する場合は、この MAC アドレスを通知してください。
LAN 側 MAC アドレス		本製品の LAN 側の MAC アドレスが表示 されます。
システム起動時間		本製品が起動してから経過した時間が表 示されます。
システム名 (SysName)		「システム管理」の「システム情報」 ページで設定した「システム名 (SysName)」が表示されます。

システムロケーション (SysLocation)	「システム管理」の「システム情報」 ページで設定した「システムロケーショ ン (SysLocation)」が表示されます。
連絡先(SysContact)	「システム管理」の「システム情報」 ページで設定した「連絡先 (SysContact)」が表示されます。

# 1.6.4 「システム情報」ページの解説

「システム情報」ページについて解説します。

		システム情報		
	システム名(SysName)	AR260S	(オプション)	
	システムロケーション(SysLocation)		(オプション)	
	連絡先(SysContact)		(オプション)	
		適別	1	
パラメ	-9-			説明
システ.	ム名 (SysName)			本製品のシステム名を入力します。デ フォルトは「AR260S」です。半角英数 字で 63 文字以内で入力してください。 入力は任意です。
システ.	ムロケーション (SysLocation)			本製品の設置場所を入力します。半角英 数字で 31 文字以内で入力してください。 入力は任意です。
連絡先	(SysContact)			連絡先を入力します。半角英数字で 31 文字以内で入力してください。入力は任 意です。
「適用」	ボタン			ーーーーーーーーーーーーーーーーーーーーーー 設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルブ	゚」ボタン			操作のヒントを参照することができま す。

### 1.7 システム時刻の設定

#### 1.7.1 概要

本製品ではシステム時刻を「タイムゾーン設定」ページで設定します。本製品は SNTP クライアント機能をもつため、時 刻を一度設定すると、その後は外部の SNTP サーバーとの通信により、時刻を同期します。ここでは、時刻を同期するた めの外部 SNTP サーバーを本製品に設定する方法についても説明します。

#### 1.7.2 システム時刻の設定

システム時刻を設定するには以下の手順を実行します。

1.メニューから「システム管理」->「タイムゾーン設定」の順にクリックします。

S - S - 🛛 🖉 🏠 🏸	' 🛠 😵 🥴 🖾 · 👹 · 🛛	😼 🖏	
:アドレス(D) @ http://192.168.1.1/index.html			✔ 🔁 移動
VPN Router			Allied Telesis
		タイムゾーン設定	
	日付	1 1 2000 (mm 月: dd 日: yyyy 西暦)	
1	時刻	1 6 2 (hh時: mm分: ss秒)	
	タイムゾーン	GMT+9:00 V	
CentreCOM AR260S		SNTPサービスの設定	
	SNTPサーバー1	133.100.9.2	
	SNTPサーバー2	133.100.11.8	
⊕ → WAN	SNTPサーバー3	133.40.41.175	
■ □ ファイアウォール	SNTPサーバー4	130.69.251.23	
E-■VPN	SNTPサーバー5	128.105.39.11	
日日システム管理	更新聞隔	60 分	
		適用	「ヘルプ
シイムボーン設定			

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは、「2004 年 4 月 22 日 19 時 30 分 00 秒」に設定し、タイムゾーンは「GMT+9:00」を選択するものとします。

	タイムゾーン設定
日付	4 22 2004 (mm 月: dd 日: yyyy 西暦)
時刻	19 30 00 (hh時: mm分: ss秒)
タイムゾーン	GMT+9:00 💌
	SNTPサービスの設定
SNTPサーバー1	133.100.9.2
SNTPサーバー2	133.100.11.8
SNTPサーバー3	133.40.41.175
SNTPサーバー4	130.69.251.23
SNTPサーバー5	128.105.39.11
更新間隔	60 分

<sup>3.</sup>以上で設定は完了です。

### 1.7.3 システム時刻の確認

#### システム時刻を確認するには以下の手順を実行します。

1. メニューから「システム管理」->「タイムゾーン設定」をクリックします。

アドレス(D) 🥘 http://192.168.1.1/index.htm	nl	💌 🔁 移動
VPN Router		Allied Telesis
		タイムゾーン設定
	日付	1 4 2000 (mm 月: dd 日: yyyy 西暦)
1	時刻	5 0 47 (hh時: mm分: ss秒)
	タイムゾーン	GMT+9:00 V
CentreCOM AR260S		SNTPサービスの設定
	SNTPサーバー1	133.100.9.2
一日 システム 南韓 田 🌐 LAN	SNTPサーバー2	133.100.11.8
	SNTPサーバー3	133.40.41.175
□ <i>ル</i> ファイアウォール	SNTPサーバー4	130.69.251.23
	SNTPサーバー5	128.105.39.11
日日システム管理	更新間隔	60 分
		道用
タイムドジーン設定		
田 システムの設定		
□ □ ファームウェアの更新		

2.「タイムゾーン設定」テーブルに現在の時刻が表示されます。

タイムゾーン設定				
日付	4 22 2004 (mm 月: dd 日: yyyy 西暦)			
時刻	19 30 18 (hh時: mm分: ss秒)			
タイムゾーン	GMT+9:00 🗸			

#### 1.7.4 SNTP サーバーの設定

SNTP サーバーとは、時刻情報サーバーを階層的に構成し、時刻を同期するサーバーです。本製品は SNTP クライアント機 能をもつため、外部 SNTP サーバーの IP アドレスを指定し、時刻を同期することができます。SNTP サーバーの IP アドレ スを指定するには以下の手順を実行します。

1.メニューから「システム管理」->「タイムゾーン設定」をクリックします。

: アドレス(D) (2) http://192.168.1.1/index.html						▶ ▶ 移動
VPN Router						Allied lelesis
				タイム	ゾーン設定	
	日付	1	1	2000	(mm 月: dd 日: yyyy 西暦)	
-	時刻	1	6	2	(hh 時: mm 分: ss 秒)	
	タイムゾーン	GMT+9	00 🗸			
CentreCOM AR260S			S	ITPサ	ービスの設定	
	SNTPサーバー1	133.10	0.9.2			
日 ・ ・ こ レAN	SNTPサーバー2	133.10	0.11.8			
	SNTPサーバー3	133.40	.41.175			
□ □ ファイアウォール	SNTPサーバー4	130.69	.251.23			
	SNTPサーバー5	128.10	5.39.11			
日日システム管理	更新間隔	60	分			
					適用	(ヘルプ)
タイムパーン設定						
□ SNMP↓/ □ □ □ システムの設定						
ファームウェアの更新						

2. 「SNTP サービスの設定」テーブルの各パラメーターを設定し「適用」ボタンをクリックします。ここでは、SNTP サーバー1~5をそれぞれ「192.168.10.5」、「133.100.11.8」、「133.40.41.175」、「130.69.251.23」、「128.105.39.11」、更新間隔を「1分」に設定するものとします。

	SNTPサービスの設定			
SNTPサーバー1	192.168.10.5			
SNTPサーバー2	133.100.11.8			
SNTPサーバー3	133.40.41.175			
SNTPサーバー4	130.69.251.23			
SNTPサーバー5	128.105.39.11			
更新間隔	1 分			
		ヘルプ		

3.以上で設定は完了です。

### 1.7.5 「タイムゾーン設定」ページの解説

「タイムゾーン設定」ページについて解説します。「タイムゾーン設定」ページでは、本製品のシステム時刻や外部 SNTP サーバーを設定します。

#### 1.7.5.1 タイムゾーン設定

「タイムゾーン設定」テーブルでは、システム時刻とタイムゾーンを設定します。

タイムゾーン設定				
日付	1 2000 (mm 月: dd 日: yyyy 西暦)			
時刻	1 32 34 (hh 時: mm 分: ss 秒)			
タイムゾーン	GMT+9:00 🔽			

パラメーター	説明
日付	日付を入力します。入力形式は「月 : 日 : 西暦年」です。
時刻	ー 時刻を入力します。入力形式は「時 : 分 : 秒」です。
タイムゾーン	タイムゾーンを選択します。


# 1.7.5.2 SNTP サービスの設定

	OM110.00	
	SNTPサービスの設定	
SNTPサーバー1	133.100.9.2	
SNTPサーバー2	133.100.11.8	
SNTPサーバー3	133.40.41.175	
SNTPサーバー4	130.69.251.23	
SNTPサーバー5	128.105.39.11	
更新間隔	60 分	
		(ヘルプ)
SNTP サーバー 1 ~ 5		
		べて異なる IP アドレスを入力する があります。
更新間隔		SNTP サーバーと同期を行う間隔 位で入力します。1 分〜 99 分の範 入力してください。
		設定した内容を本製品の設定に適
「適用」ボタン		す。ホスシェクリックすると設定 即時に反映されます。

# 1.8 SNMP エージェントの設定

#### 1.8.1 概要

本製品では SNMP エージェント機能をサポートしています。「SNMP」ページで SNMP エージェントを設定し、有効にすると SNMP マネージャーから本製品の設定を参照したり、変更することができます。ここでは、SNMP エージェントの設定につ いて説明します。

### 1.8.2 SNMP エージェントの設定

SNMP エージェントの設定を行うには以下の手順を実行します。

1.メニューから「システム管理」->「SNMP」の順にクリックします。

アドレス(D) 🍯 http://192.168.1.1/index.htt	ml		💙 🄁 移動
VPN Router			Allied Telesis
		SNMP設定	
	SNMP	○ 有効 ⊙ 無効	
-	ROコミュニティー名	public	
	RWコミュニティー名	private	
CentreCOM AR260S	通知先アドレス		
<ul> <li>□ セットアップウィザード</li> <li>□ システム情報</li> <li>□ L AN</li> </ul>		適用	(ヘルプ)
● ● WAN ● ● ルーティング		SNMP設定情報	
■ □ ファイアウォール	SNMP	無効	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	RUコミュニティー石 RWコミュニティー名 通知先マドレフ	private	
- 〕サービスの有効無効 - 〕サービスの有効無効 システム情報 - 〕システム情報 - 〕シイムワーン調定 - 〕SMAP 0 〕システムの設定 - 〕SMAP - 〕システムの設定 - 〕アークッエアの更新 - 〕再起動 - 〕ログアウト			

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

SNMP	有効
RO コミュニティー名	viewer
- RW コミュニティー名	secret
通知先アドレス	192.168.10.5

<sup>3.</sup>以上で設定は完了です。

### 1.8.3 SNMP 設定情報の確認

### 設定した SNMP 情報を確認するには以下の手順を実行します。

1.メニューから「システム管理」->「SNMP」の順にクリックします。

2.「SNMP 設定」テーブルに設定された情報が表示されます。

	SNMP設定	
SNMP	有効	
ROコミュニティー名	viewer	
RWコミュニティー名	secret	
通知先アドレス	192.168.10.5	

### 1.8.4 「SNMP」ページの解説

「SNMP ページ」について解説します。「SNMP」ページでは、本製品が SNMP エージェントとして動作する場合の設定を行います。

#### 1.8.4.1 SNMP 設定

SNMP 設定テーブルでは、SNMP エージェントの設定を行います。

				SNMP設定			
	SNMP		○ 有効 ⊙ 無効				
	ROコミュニティー名		public				
	RWコミュニティー名		private				
	通知先アドレス						
				適用		ヘルプ	
パラ	ラメーター	オプション			説明		
SNM	ИР	有効 / 無効			SNMP を有効 効にする場合 クリックしま	にする場合は「有効」 は「無効」ラジオボ す。	、無 タンを
RO	コミュニティー名				SNMP 管理ホ 出す場合に使 ワードを入力 文字以内で入 トは「public」	ストが本製品の情報る 用する平文テキスト( します。半角英数字 カしてください。デ です。	を読み のパス で 15 フォル
RW	コミュニティー名				SNMP 管理ホ 出す場合、お 使用する平文 力します。半 入力してくだ 「private」です	ストが本製品の情報衣 よび設定を書き込む テキストのパスワー 角英数字で 15 文字以 さい。デフォルトは -。	を読み 場合に ドを入 L内で
通知	ロ先アドレス				SNMP 管理ホ ます。	ストの IP アドレスを	入力し
「適	用」ボタン				設定した内容 す。ボタンを 即時に反映さ	を本製品の設定に適り クリックすると設定で れます。	用しま 内容が
^ آ	ルプ」ボタン				操作のヒント す。	を参照することができ	きま

# 1.8.4.2 SNMP 設定情報

「SNMP 設定情報」テーブルでは、「SNMP 設定」テーブルで設定した内容が一覧表示されます。

SNMP	
ROコミュニティー名	public
RWコミュニティー名	private
通知先アドレス	

パラメーター	説明
SNMP	SNMP の有効 / 無効が表示されます。
RO コミュニティー名	本製品の情報を読み出す場合のパスワー ドが表示されます。
RW コミュニティー名	本製品の情報を読み出す場合、および設 定を書き込む場合のパスワードが表示さ れます。
通知先アドレス	SNMP 管理ホストの IP アドレスが表示さ れます。

# 1.9 ログの記録

#### 1.9.1 概要

本製品では「アクセス」、「システム」、「ファイアウォール」、「VPN」の4種類の各ログを「ログ」ページで選択して記録 することができます。また、記録したログはログリストに表示したり、Syslogサーバーに送信することもできます。こ こでは、ログ機能の設定について説明します。

#### 1.9.2 ログの設定

ログ機能を設定するには以下の手順を実行します。

1. メニューから「ログ」をクリックします。

: アドレス(型) 🥘 http://192.168.1.1/index.html					
VPN Router					
			システ	・ムログ設定	
	ログの種類	アクセス	システム	ファイアウォー	-JU VPN
	ファイル		<b>~</b>	<b></b>	
	Syslog				
<ul> <li>CentreCOM AR260S</li> <li>□ セットアップウィザード</li> <li>□ システム 情報</li> <li>□ LAN</li> <li>□ WAN</li> <li>□ W-7 アウォール</li> <li>□ WPN</li> </ul>			(	適用	
			L	ダリスト	
	Jan 1 00:00:20 (none) syste Jan 1 00:00:20 (none) syste shanged the ID address of	ogd 1.3-3: restart og: id=CONFIG tir br0 interface to 1	ne="2000- 70 16 17 1	01-01 00:00	:20" fw=AR260S pri=5 msg="Suc
	Jan 1 00:00:20 (none) syste changed the IP address of	og: id=CONFIG tir eth1 interface to	ne="2000- 192.168.1.	0 01-01 00:00 1"	:20" fw=AR260S pri=5 msg="Suc
	Jan 1 00:00:20 (none) syste initialised"	og: id=SYSTEM ti	me="2000-	01-01 00:00	0:20" fw=AR260S pri=5 msg="CPI
日のシステム管理	Jan 1 00:00:20 (none) syste changed the state of eth1 in	og: id=CONFIG tir nterface to UP "	ne="2000-	01-01 00:00	:20" fw=AR260S pri=5 msg="Suc
	Jan 1 00:00:20 (none) syste the Bridge"	og: id=BRIDGE tir	ne="2000-i	01-01 00:00	:20" fw=AR260S pri=5 msg="Suc

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

アクセス	ファイル
システム	Syslog
ファイアウォール	ファイル
VPN	Syslog、ファイル
ログサーバー IP アドレス	192.168.10.54

			テムログ設定		
ログの種類	アクセス	、システム	ファイアウォール	U VPN	
ファイル			<b>V</b>	<b>V</b>	
Syslog		<b>V</b>		<b>V</b>	
ログサーバーIPアドレス	192.168	.10.54			
			(in the second s		(ヘルプ

<sup>3.</sup>以上で設定は完了です。

### 1.9.3 ログの確認

#### ログをファイルで確認するには以下の手順を実行します。

1. メニューから「ログ」をクリックします。

2.「ログリスト」にログが表示されます。また「更新」ボタンをクリックすると表示内容が更新されます。



### 1.9.4 「ログ」ページの解説

「ログ」ページについて解説します。「ログ」ページでは、ログの設定を行います。

#### 1.9.4.1 システムログ設定

メニューから「ログ」をクリックすると設定画面が表示されます。

		シス	テムログ設定	
ロクの種類 ファイル	アクt	2ス システム <b>マ</b>	ファイアワォー	
Syslog				
			適用	ヘルプ
			าธีแรง	
パラメーター	オプション			説明
ログの種類				アクセス、システム、ファイアウォー ル、VPN の 4 種類のログを記録すること ができます。
	アクセス			本製品へのアクセスに関するログです。
	システム			本製品のシステムに関するログです。
	ファイアウォール			ファイアウォールを経由した通信のログ です。
	VPN			VPN 通信に関するログです。
ファイル				ログを「ログリスト」テーブルに表示す る場合にチェックを入れます。チェック は、ログの種類ごとに入れます。ログの サイズは 64Kbyte を超えると(およそ 450 件分)古い順から上書きされます。
Syslog				ログをリモート syslog サーバーに送信す る場合にチェックを入れます。ログのサ イズが 64Kbyte を超えると自動的にサー バーに送信されます。チェックは、ログ の種類ごとに入れます。Syslog のログ送 出の出力監視レベルは PRI に対応してい ます。

-	ログサーバー IP アドレス	「Syslog」にチェックを入れた場合にのみ 表示されます。ログを送信する syslog サーバーの IP アドレスを入力します。
「適用」ボタン		設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

# 1.9.4.2 ログリスト

ログリストには、「システムログ設定」でファイルにチェックを入れた場合に、ログが記録されます。

	ログリスト		
Jan 1 00:00:48 (none) syslog: id=OAM time="2000-0 logged in"	Jan 1 00:00:48 (none) syslog: id=OAM time="2000-01-01 00:00:48" fw=AR260S pri=6 msg="HTTP- User: manager logged in"		
	更新		
ラメーター	説明		
「新」ボタン	クリックすると、ログの表示が更新 ます。		

# 1.10 設定の初期化

本製品に設定した内容を初期化(デフォルト設定に戻す)する手順を説明します。



#### 1.10.1 GUI 設定画面からの初期化

1.メニューから「システム管理」->「システムの設定」->「デフォルト設定」の順にクリックします。



2.「適用」ボタンをクリックします。

awaa 1000	
	Allied Telesis
	デフォルト設定
	注意:「適用」ボタンをクリックすると、システム設定がすべて工場出荷時の値に戻ります。 「適用」ボタンをクリックする前に設定をバックアップしておくことをお勧めします。
	5

3. 以下の画面が表示され、必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。



4. カウントダウンが終了すると、以下のダイアログが表示されます。

Microso	ft Internet Explorer 🛛 🗙
2	IPアドレス 19216811.1 で本製品に再接続する場合は「OK」、それ以外の場合は「キャンセル」をクリックしてください。デフォ ルトのIPアドレスを変更した場合は「キャンセル」をクリックし、変更後のIPアドレスで再接続してください。
	<b>OK</b> キャンセル

本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

5.以上で完了です。

### 1.10.2 リセットスイッチによる初期化



1. 本製品の電源をオフにして、5 秒以上待ちます。

2. 本製品の電源をオンにして5秒以上経過したらリセットスイッチを短く押します。

3. しばらくすると ALARM LED が一瞬消灯しますので、消灯している間にリセットスイッチをもう一度短く押します。

4. 以上で完了です。

# 1.11 設定内容のバックアップ

#### 本製品で設定した内容をコンピューターにバックアップする手順を説明します。

1.メニューから「システム管理」->「システムの設定」->「バックアップ」の順にクリックします。



2.「適用」ボタンをクリックします。

-

Allied Te
設定内容のバックアップ
設定内容をコンピューターにバックアップするには「適用」ボタンをクリックしてください
(適時)

以下の画面が表示されたら「保存」ボタンをクリックして、バックアップファイルの保存場所を指定し、ダイアログの「保存」ボタンをクリックします。

ファイルのダウンロー	F			
? 27イルに 以下のフ きない場	はっては、コンピュータボ アイル情報のに関して紛れ 合は、このファイルを開い	問題を起こす可能性があります。 しい点がある場合や、発信元が完全に信用で たり保存したりしないでください。		
77	イル名: bkupcfe	b4eef8cc		
77	ペイルの種類 信元: 192.168			
ファイルあ	問(カカ ファイルをついど・	ーカに保存するが遅択してください。		
開	( <sup>(())</sup> ) 保存和	シート キャンセル 詳細情報(10)		
☑ 208	i類のファイルであれば常	(ご警告する(W)		
名前友付け了保存				2
(保存する場所の)	C backup	~	0 A P	
in y warn y	- Duonap			
- 1000000000000000000000000000000000000				
18./LIX5/C7717/				
<u>1</u> 7271-107				
71 FF1X2F				
₹1 <u>1</u> ),ピュータ				
<b>(</b> )				
マイ ネットワーク	ファイル名(N):	bkupcfgb4eef8cc	~	保存(S)
		۲ بربر ا	~	キャンセル

4.「ダウンロードの完了」ダイアログが表示されたら「閉じる」をクリックします。

ダウンロードの完了	
يري 🔁	ロードの完了
保存しました	
192.168.1.1 - bkup	cfgb4eef8cc
ダウンロード:	834 バイトを1 秒
ダウンロード先:	C:¥Documents and¥bkupcfgb4eef8cc
転送率:	834 バイト/秒
■ダウンロードの完	了後、このダイアログ ボックスを閉じる(C)
	ファイルを開く(①) フォルダを開く(E) 開じる

5.以上で完了です。





# 1.12 バックアップファイルの復元

#### バックアップした本製品の設定ファイルを復元する手順を説明します。

1.メニューから「システム管理」->「システムの設定」->「システムの復元」の順にクリックします。



2.「参照」ボタンをクリックして、バックアップファイルを指定し「開く」ボタンをクリックします。

		Allied Te
	システムの復元	
設定ファイル名		参照
	適用	ki ki

ファイルの選択					? 🔀
ファイルの場所の:	ackup 🔁		• 3 🕫	۳ 🔁	
	bkupcfeb4eef8co	•			
最近使ったファイル					
デスクトップ					
کر الج					
ر ¢− 2221 - ¢					
マイ ネットワーク					
	ファイル名(N):	bkupcfgb4eef8cc		•	Ŋ\$K(©)
	ファイルの種類①	すべてのファイル (*.*)		-	キャンセル

3.「適用」ボタンをクリックします。

		Allied leies
	いった」の海二	
	ンステムの仮元	
設定ファイル名	C:\Documents and Settings\backup\bkupcfgb4eef8cc	参照
	(適用 <sub>m</sub> )	
	0	

4. 以下の画面が表示され、必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。



5. カウントダウンが終了すると、以下のダイアログが表示されます。

Ì	Microso	ft Internet Explorer 🛛 🗙
	?	IPアドレス 1921681.1. で本製品に再接続する場合は「OK」、それ以外の場合は「キャンセル」をクリックしてください。デフォ ルトのIPアドレスを変更した場合は「キャンセル」をクリックし、変更後のIPアドレスで再接続してください。
		OK キャンセル

本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

6.以上で完了です。

# 1.13 ファームウェアの更新

「ファームウェアの更新」ページでは、本製品のファームウェアを新しいバージョンのファームウェアに更新することが できます。

1.メニューから「システム管理」→>「ファームウェアの更新」の順にクリックします。

Ē	
Ē	B 🗀 VPN
	💼 ログ
Ė	- 🔁 システム管理
	🔤 サービスの有効/無効
	- SNMP
	🕀 🗋 システムの設定
	 ファ <u> に</u> ムウェアの更新

2.「参照」ボタンをクリックして、ファームウェアファイルを指定し「開く」ボタンをクリックします。

	-						AVZ A	llied Telesis
				ファームウェア	の更新			
ファーム	ウェア					3	<u>参照</u>	
				適用			43	
					-			
ファイルの選択				? 🛛	1			
ファイルの場所の: 「	🗀 firmware		🔹 🔾 🕸 🖻					
	a AF260S_firmwar	ebin						
最近使ったファイル								
デスクトップ								
6								
71 F#13/2F								
71 J)L1-9								
マイ ネットワーク								
-	ファイル名( <u>N</u> ): ファイルの種類(T)	AR260S_firmware.bin						
	A DRAVENCY	12:10/02/11/07/09/	2		4			

3.「適用」ボタンをクリックします。

	ファームウェアの更新
ファームウェア	C:\Documents and Settings\sshimizu\firmware\AR260S_firm
	適用

4. 以下の画面が表示され、必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。



ファームウェア更新中にリセットボタンを押さないでください。また、電源をオフにすることやケーブルの抜き差し ヒント もしないでください。

#### 5. カウントダウンが終了すると、以下のダイアログが表示されます。

Micros	oft Internet Explorer 🛛 🗙
2	IPアドレス192168.11で本製品に再接続する場合は「OK」、それ以外の場合は「キャンセル」をクリックしてください。デフォル ドのIPアドレスを変更した場合は「キャンセル」をクリックし、変更後のIPアドレスで再接続してください。
	OK キャンセル

本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場 合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

6.以上で完了です。

マテームウェアの更新中、本製品の通信は停止しますので、運用中にファームウェアの更新を実行しないようご注意 ビント ください。



# 2 LAN 側インターフェースの設定

# 2.1 概要

本章では、本製品のLAN 側インターフェースに関する設定の手順について説明します。本製品のLAN 側インターフェースに関する設定は以下のとおりです。

- ・ IP アドレスの設定
- ・ DHCP サーバーの設定
- IP アドレスの静的割り当ての設定
- ・ LAN 側インターフェースのトラフィック確認

# 2.2 IP アドレスの設定

LAN 側インターフェースの IP アドレスの設定は「IP」ページで行います。ログイン時には、ここで設定した IP アドレス を使用します。

### 2.2.1 設定

LAN 側インターフェースに IP アドレスを割り当てるには以下の手順を実行します。



1.メニューから「LAN」->「IP」の順にクリックします。

アドレス(D) 🍯 http://192.168.1.1/index.ht	iml		🗸 🄁 移動
VPN Router			Allied Telesi
		LAN側IP設定	
	IPアドレス	192.168.1.1	
C	サブネットマスク	255.255.255.0	
		適用	(ヘルプ)
CentreCOM AR260S			
		現在の設定	
	IPアドレス	192.168.1.1	
	サブネットマスク	255.255.255.0	
□ 固定UHUPクライアント			
ー 📄 ルーティング			
<b>→</b> □ファイアウォール			
□□□-□			

2. IP アドレスに「192.168.10.1」、サブネットマスクに「255.255.255.0」を入力し「適用」ボタンをクリックします。

		Allied Telesis
	LAN側IP設定	
IPアドレス	192.168.10 1	
サブネットマスク	255.255.255.0	
	(適用)	
	現在の設定	
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	

3. 以下のメッセージが表示されますので「OK」ボタンをクリックします。

Microso	oft Internet Explorer 🛛 🗙
⚠	LAN側IPアドレスまたはサブネットマスクが変更されています。変更後のLAN側IPアドレスで再接続してください

4. これで設定は完了です。



次回、本製品の設定を行う場合は変更後の № アドレスでアクセスしてください。

#### 2.2.2 確認

LAN 側インターフェースに割り当てた IP アドレスは以下の手順で確認します。

1.メニューから「LAN」->「IP」の順にクリックします。

2.「現在の設定」テーブルに、現在の IP アドレスとサブネットマスクが表示されます。

	現在の設定
IPアドレス	192.168.10.1
サブネットマスク	255.255.255.0

# 2.2.3 「IP」ページの解説

「IP」ページについて解説します。「IP」ページでは本製品の LAN 側に関する設定を行います。

## 2.2.3.1 LAN 側 IP 設定

メニューから「LAN」->「IP」の順にクリックすると以下の画面が表示されます。

		Allied Telesis
	LAN側IP設定	
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	
	適用	
パラメーター		説明
IPアドレス		本製品の LAN 側 IP アドレスを入力しま す。デフォルトでは「192.168.1.1」です。 ここで設定した IP アドレスを使用して 本製品の設定画面にアクセスします。
サブネットマスク		LAN 側サブネットマスクを入力します。
「適用」ボタン		入力した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

# 2.2.3.2 現在の設定

	現在の設定	
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	

パラメーター	説明
アアドレス	現在本製品の LAN 側インターフェース に設定されている IP アドレスが表示さ れます。
サブネットマスク	現在本製品の LAN 側インターフェース に設定されているサブネットマスクが表 示されます。

# 2.3 DHCP サーバーの設定

DHCP (Dynamic Host Configuration Protocol) は、クライアントに対して動的に IP アドレスを提供する機能です。DHCP サーバーは、クライアントの要求に対して、あらかじめプールされた IP アドレスの中から使用されていないアドレスを 選び、一定期間クライアントに割り当てます。本製品の DHCP サーバーの設定は「DHCP」ページで行います。

#### 2.3.1 デフォルト設定

DHCP サーバーに関するデフォルト設定は以下のとおりです。

パラメーター		デフォルト値
DHCP サーバー		有効
IP アドレスプール		
-	始点 IP アドレス	192.168.1.10
-	終点 IP アドレス	192.168.1.200
サブネットマスク		255.255.255.0
リース期限		14日
デフォルトゲートウ	?ェイ	192.168.1.1
プライマリ DNS サ-	-, <sup>x</sup> -	192.168.1.1

# 2.3.2 設定

DHCP サーバーの設定を行うには以下の手順を実行します。

1.メニューから「LAN」->「DHCP」の順にクリックします。

				Allied Teles
VPN Router				ZAZS AIIEU IEIES
		Di	ICPサーバー設定	
	יון ביב די געדיר	始点IPアドレス	192.168.1.10	
		終点IPアドレス	192.168.1.200	
	サブネットマスク	255.255.255.0		
CentreCOM AR260S	リース期限	14:00:00 (dd	日: hh 時間: mm 分)	
システム情報	デフォルトゲートウェイ	192.168.1.1		
	プライマリDNSサーバー	192.168.1.1	(オブション)	
	セカンダリDNSサーバー		(オプション)	
	プライマリWINSサーバー		(オブション)	
	セカンダリWINSサーバー		(オプション)	
			適用	(ヘルプ)
- <u>0</u> 07			_	_
- □ システム管理 				
			現在の設定	

2. 各パラメーターの値を入力し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

IP アドレスプール		
	始点 IP アドレス	192.168.1.200
	終点 IP アドレス	192.168.1.240
サブネットマスク		255.255.255.0
リース期限		14 日
デフォルトゲート	זבל	192.168.1.1
プライマリ DNS サ	- <i>i</i> \	192.168.1.10
セカンダリ DNS サ	-バー	192.168.1.12

	DHCPサーバー設定
IPアドレスプール	始点IPアドレス 192.168.1.200 終点IPアドレス 192.168.1.240
サブネットマスク	255.255.255.0
リース期限	14:00:00 (dd 日: hh 時間: mm 分)
デフォルトゲートウェイ	192.168.1.1
プライマリDNSサーバー	192.168.1.10 (オプション)
セカンダリDNSサーバー	192.168.1.12 (オプション)
プライマリWINSサーバー	(オプション)
セカンダリWINSサーバー	(オプション)

3.以上で設定は完了です。



DHCP サーバーの起動と停止については「P.18 機能の有効化 / 無効化の設定」を参照してください。

### 2.3.3 確認

DHCP サーバーの設定は以下の手順で確認します。

1.メニューから「LAN」->「DHCP」の順にクリックします。

2.「現在の設定」テーブルに、DHCP サーバーの設定が表示されます。その下の「クライアントー覧」テーブルには本製品が IP アドレスを割り当てた DHCP クライアントの一覧が表示されます。「更新」ボタンをクリックすると表示内容が更新されます。

	現在の設定		
Pアドレスブール	192.168.1.200 ~ 192.168.1.240	0	
サブネットマスク	255.255.255.0		
リース期限	14:00:00 (dd 日: hh 時間: mm 🤊	<del>ن</del> )	
デフォルトゲートウェイ	192.168.1.1		
プライマリDNSサーバー	192.168.1.10		
セカンダリDNSサーバー	192.168.1.12	192.168.1.12	
プライマリWINSサーバー			
セカンダリWINSサーバー			
	クライアント一覧		
MACアドレス	割り当てIPアドレス	リース期限	
00:00:e2:59:56:48	192.168.1.200	16:14:56 1/15/2000	
	(東新)		

## 2.3.4 「DHCP」ページの解説

「DHCP」ページについて解説します。「DHCP」ページでは、本製品の DHCP サーバー機能についての設定を行います。

### 2.3.4.1 DHCP サーバー設定

メニューから「LAN」->「DHCP」の順にクリックすると以下の画面が表示されます。

	DHCPサーバー設定
IPアドレスプール	始点IPアドレス 192.168.1.10 終点IPアドレス 192.168.1.200
サブネットマスク	255.255.255.0
リース期限	14:00:00 (dd 日: hh 時間: mm 分)
デフォルトゲートウェイ	192.168.1.1
プライマリDNSサーバー	192.168.1.1 (オプション)
セカンダリDNSサーバー	(オプション)
プライマリWINSサーバー	(オプション)
セカンダリWINSサーバー	(オプション)
	(適用) (ヘルプ)

パラメーター

オプション

説明

IP アドレスプール

	始点 IP アドレス	DHCP サーバー機能によって割り当てる IP アドレスの始点 IP アドレスを入力し ます。
	終点 IP アドレス	DHCP サーバー機能によって割り当てる IP アドレスの終点 IP アドレスを入力し ます。
サブネットマスク		IP アドレスプールのサブネットマスクを 入力します。
リース期限		クライアントに割り当てる IP アドレス のリース期限を入力します。1 分~ 99 日 23 時間 59 分の範囲で入力してくださ い。
デフォルトゲートウェイ		デフォルトゲートウェイの IP アドレス を入力します。通常は、本製品の LAN 側の IP アドレスです。
プライマリDNS サーバー		プライマリ DNS サーバーの IP アドレス を入力します。通常は、本製品の LAN 側の IP アドレスです。入力は任意です。
セカンダリDNS サーバー		セカンダリ DNS サーバーの IP アドレス を入力します。入力は任意です。
プライマリ WINS サーバー		プライマリ WINS サーバーの IP アドレス を入力します。入力は任意です。
セカンダリWINS サーバー		セカンダリ WINS サーバーの IP アドレス を入力します。入力は任意です。

「適用」ボタン	入力した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

# 2.3.4.2 現在の設定

	現在の設定	
IPアドレスブール	192.168.1.10 ~ 192.168.1.200	
サブネットマスク	255.255.255.0	
リース期限	14:00:00 (dd 日: hh 時間: mm 分)	
デフォルトゲートウェイ	192.168.1.1	
プライマリDNSサーバー	192.168.1.1	
セカンダリDNSサーバー		
プライマリWINSサーバー		
セカンダリWINSサーバー		

パラメーター	説明
IP アドレスプール	本製品に設定された IP アドレスプール が表示されます。
サブネットマスク	IP アドレスプールのサブネットマスクが 表示されます。
リース期限	クライアントに割り当てた IP アドレス のリース期限が表示されます。
デフォルトゲートウェイ	デフォルトゲートウェイのアドレスが表 示されます。
プライマリDNS サーバー	プライマリ DNS サーバーの IP アドレス が表示されます。
セカンダリDNS サーバー	セカンダリ DNS サーバーの IP アドレス が表示されます。
プライマリWINS サーバー	プライマリ WINS サーバーの IP アドレス が表示されます。
セカンダリWINS サーバー	セカンダリ WINS サーバーの IP アドレス が表示されます。

# 2.3.4.3 クライアント一覧



パラメーター	説明
MACアドレス	IP アドレスを割り当てたクライアントの MAC アドレスが表示されます。
割り当て IP アドレス	クライアントに割り当てた IP アドレス が表示されます。
リース期限	IP アドレスを割り当ててから経過した時 間が表示されます。
「更新」ボタン	クリックすると「クライアントー覧」の 表示内容を更新することができます。

# 2.4 IP アドレスの静的割り当ての設定

本製品では、DHCP サーバー機能の一部として、IP アドレスをクライアントに固定的に割り当てる機能(固定 DHCP クライ アント機能)があります。固定 DHCP クライアント機能の設定は「固定 DHCP クライアント」ページで行います。

#### 2.4.1 設定

固定 DHCP クライアントを追加するには以下の手順を実行します。

1. メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

,	~~ ~ ~ <u>~</u> <u>~</u> <u>~</u> <u>~</u>			
アドレス(D) 🍯 http://192.168.1.1/index.html				🔽 🔁 移動
VPN Router				Allied Telesis
		固定DHCPクライ	アント設定	
	DHCPクライアントのMACアドレス			
-	固定DHCPアドレス			
		〔追加		(ヘルプ)
CentreCOM AR260S				
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>		固定DHCPクライ	アントー覧	
	DHCPクライアントのM/	ACTFUR	固定DHCPアドレス	
ー P DHCP 一 固定DHCPクライアント				
E- WAN				
ー 🛄 ルーティング				
□ ファイアウォール				
□□□♡ 用-□システム管理				
一 再起動				
<sup></sup> <mark>] ログアウト</mark>				

2. 各パラメーターに値を入力し「追加」ボタンをクリックします。ここでは、MAC アドレス「00-00-f4-11-22-33」のクライア ントに固定 DHCP アドレスとして「192.168.1.250」を割り当てるものとします。

	Allied Telesi
固定DHCPクライアント設定	
00 : 00 : f4 : 11 : 22 : 33	
192.168.1.250	
	ヘルプ
	固定DHCPクライアント設定 00 : 00 : 14 : 11 : 22 : 33 192.168.1.250

3.以上で設定は完了です。

#### 2.4.2 固定 DHCP クライアントの削除

追加した固定 DHCP クライアントを削除するには以下の手順を実行します。

1. メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

2.「固定 DHCP クライアント一覧」で、削除するクライアント左部の「ごみ箱」アイコンをクリックします。

3. 以上で設定は完了です。

#### 2.4.3 確認

#### 追加された固定 DHCP クライアントを確認するには以下の手順を実行します。

1.メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

2.「固定 DHCP クライアントー覧」テーブルに固定 DHCP クライアントの一覧が表示されます。

	固定DH(	CPクライアント一覧	
	DHCPクライアントのMACアドレス	固定DHCPアドレス	
Ē	00:00:f4:11:22:33	192.168.1.250	

#### 2.4.4 「固定 DHCP クライアント」ページの解説

「固定 DHCP クライアント」ページについて解説します。「固定 DHCP クライアント」ページでは、本製品の DHCP サーバー 機能で固定的に IP アドレスを割り当てるクライアントを登録します。

### 2.4.5 固定 DHCP クライアント設定

メニューから「LAN」->「固定 DHCP クライアント」の順にクリックすると以下の画面が表示されます。

固定DHCPクライアント設定			
DHCPクライアントのMACアドレス			
固定DHCPアドレス			
追加 ヘルプ			

パラメーター	説明
DHCP クライアントの MAC アドレス	IP アドレスを固定的に割り当てるクライ アントの MAC アドレスを入力します。
固定 DHCP アドレス	クライアントに固定的に割り当てる IP アドレスを入力します。
「追加」ボタン	クライアントを追加登録します。追加で きるクライアントは 10 台までです。ボ タンをクリックすると設定内容が即時に 反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

# 2.4.6 固定 DHCP クライアント一覧

	固定DH	HCPクライアント一覧	
	DHCPクライアントのMACアドレス	固定DHCPアドレス	
<b>1</b>	00:00:f4:11:22:33	192.168.1.250	

パラメーター	説明
DHCP クライアントの MAC アドレス	IP アドレスが固定的に割り当てられてい るクライアントの MAC アドレスが表示 されます。
固定 DHCP アドレス	クライアントに固定的に割り当てられて いる IP アドレスが表示されます。
「ごみ箱」アイコン	クリックすると「固定 DHCP クライアン ト一覧」から該当クライアントを削除し ます。

# <u>2.5 トラフィックの確認</u>

本製品では、LAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。LAN 側 インターフェースの送受信トラフィックは「統計情報」ページで確認します。

#### 2.5.1 確認

#### 1.メニューから「LAN」->「統計情報」をクリックします。

アドレス(1) @ http://192168.1.1/index.html			✔ 🄁 移動
VPN Router			Allied Telesis
		LAN Statistics	
		Ethernet Statistics	
-	Total Bytes Received	38741	
	Unicast Packets Received	333	
	Multicast Packets Recieved	0	
CentreCOM AR260S	Packets Received and Discarded	0	
	Packets Received with Errors	0	
	Packets Received with unknown Protocols	0	
I	Total Bytes Transmitted	137039	
- DHCP	Unicast Packets Transmitted	317	
	Multicast Packets Transmitted	2	
	Packets Discarded while Transmission	0	
ー ロルーティング	Packets Sent with Errors	0	
🖻 🧰 ファイアウォール		更新	
		2.41	
- 再起動			
ーログアウト			

2.「LAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。

	Ethernet Statistics	
Total Bytes Received	78149	
Unicast Packets Received	386	
Multicast Packets Recieved	0	
Packets Received and Discarded	0	
Packets Received with Errors	0	
Packets Received with unknown Protocols	0	
Total Bytes Transmitted	125563	
Unicast Packets Transmitted	330	
Multicast Packets Transmitted	0	
Packets Discarded while Transmission	0	
Packets Sent with Errors	0	

# 2.5.2 「統計情報」ページの解説

#### 「統計情報」ページでは、本製品のLAN 側インターフェースのパケット転送に関する統計を参照することができます。

#### メニューから「LAN」->「統計情報」の順にクリックすると以下の画面が表示されます。

LAN Statistics				
		Ethernet Statistics		
	Total Bytes Received	61834		
	Unicast Packets Received	377		
	Multicast Packets Recieved	0		
	Packets Received and Discarded	0		
	Packets Received with Errors	0		
	Packets Received with unknown Protocols	0		
	Total Bytes Transmitted	136882		
	Unicast Packets Transmitted	351		
	Multicast Packets Transmitted	0		
	Packets Discarded while Transmission	0		
	Packets Sent with Errors	0		
		更新		
パラメ	-9-		説明	
Total B	lytes Received		受信パケットの総バイト数がカウントさ れます。	
Unicast	t Packets Received		受信ユニキャストパケットの総数がカウ ントされます。	
Multicast Packets Received		受信マルチキャストパケットの総数がカ ウントされます。		
Packets Received and Discarded			破棄されたパケット数がカウントされま す。	
Packet Received with Errors			エラーパケット数がカウントされます。	
Packets Received with unknown Protocols キサポートプロトコルの ウントされます。		未サポートプロトコルのパケット数がカ ウントされます。		
Total Bytes Transmitted     転送パケットの       れます。     1		転送パケットの総バイト数がカウントさ れます。		
Unicast Packets Transmitted			転送ユニキャストパケット数がカウント されます。	
Multicast Packets Transmitted			転送マルチキャストパケット数がカウン トされます。	
Packet	s Discarded while Transmission		転送中に破棄されたパケット数がカウン トされます。	
Packet	s Sent with Errors		転送されたエラーパケット数がカウント されます。	
「更新」	ボタン		統計情報の表示内容を更新します。	

# 3 WAN 側インターフェースの設定

# 3.1 概要

本章では、本製品の WAN 側インターフェースに関する設定を「WAN」ページで行う手順について説明します。本製品の WAN 側イ ンターフェースに関する設定は以下のとおりです。

- DHCP を使用した WAN 側ネットワークへの接続設定
- ・ PPPoE を使用した WAN 側ネットワークへの接続設定
- ・ 固定 IP を使用した WAN 側ネットワークへの接続設定
- · WAN 側インターフェースのトラフィック確認

## 3.2 DHCP を使用した WAN 側ネットワークへの接続

WAN 側インターフェースを DHCP で接続する場合の手順について説明します。おもに CATV のインターネット接続サービス などで多く使用される接続形態です。

### 3.2.1 設定

WAN 側インターフェースを DHCP で接続するには以下の手順を実行します。



インターネット接続サービスを提供するサービスプロバイダーから、設定に必要な情報を提供されている場合は事前 ント にご用意ください。詳細についてはプロバイダーにお問い合わせください。

1.メニューから「WAN」->「WAN」の順にクリックします。

アドレス(D) 🍯 http://192.168.1.1/index.html			💙 🄁 移動
VPN Router			Allied Telesis
		W	/AN設定
	接続モード	PPPoE 💌	
	セッションID	PPPoE:0 🖌 接続	]
CentreCOM AR260S	デフォルトゲートウェイ	PPPoE:0 🗸	
	Unnumbered PPPoE	○有効 ⊙無効	
	ホスト名	AR260S	(オプション)
- WAN	ユーザー名		
	パスワード		
	サービス名		(オプション)
□□ ロク □□ システム管理	AC(アクセスコンセントレーター)名		(オプション)
- 日本記動	DNSオプション	○固定設定 ⊙自動	加取得
	プライマリDNSサーバー		(オプション)
	セカンダリDNSサーバー		(オプション)
	MSSクランプ	<ul> <li>○無効 ●有効</li> <li>MSSの値: 40</li> </ul>	Bytes
	接続オプション	○ダイアルオンデマ エコー送信間隔 60	rンド ●キーブアライブ ○無効 秒
			適用 (ヘルプ)
A have ( (100 100 11 / h)) / how one	サージルウンドウィーナーナー 相大不乱	現: CHENTA VENUSA	在の設定 - ● ひた ★u

2.接続モードに「DHCP」を選択します。

	WAN設定
接続モード	
ホフトタ(オポション)	ADJene W

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

ホスト名	mycomputer(プロバイダーから提供されたと仮定します)
DNS オプション	自動取得
MAC クローニング	有効、「00:00:f4:11:22:33」に設定する

接続モード		
ホスト名	mycomputer (オプション)	
DNSオプション	○固定設定 ◎自動取得	
プライマリDNSサーバー	(オプション)	
セカンダリDNSサーバー	(オプション)	
☑ MACクローニング	00 - 00 - 14 - 11 - 22 - 33	

~

4.以上で設定は完了です。

#### 3.2.2 設定の確認

#### WAN 側の設定は以下の手順で確認します。

1.メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。

現在の設定		
基本設定が完了しました。現在の設定は以下のとおりです。		
LAN設定		
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	
DHCP	有効	
WAN設定		
接続モード	DHCP	
デフォルトゲートウェイアドレス	10.10.31.1	
ブライマリDNSサーバー	10.10.31.2	
セカンダリDNSサーバー		
接続状況	接続	
IPアドレス	10.10.31.45	
サブネットマスク	255.255.255.0	
MACクローニング	00:00:14:11:22:33	

# 3.3 PPPoE を使用した WAN 側ネットワークへの接続

WAN 側インターフェースを PPPoE で接続する場合の手順について説明します。おもに x DSL などのインターネット接続 サービスなどで多く使用される接続形態です。

#### 3.3.1 設定

WAN 側インターフェースを PPPoE で接続するには以下の手順を実行します。

インターネット接続サービスを提供するサービスプロバイダーから、設定に必要な情報を提供されている場合は事前 ヒント にご用意ください。詳細についてはプロバイダーにお問い合わせください。

1.メニューから「WAN」->「WAN」の順にクリックします。

VPN Router       WANUGE         CentreCOM AR260S       超数モード         ビックアップウ・ガード       ワPP0E 0         ジステム 物理       デフォルトゲートウェイ         ビックスの かした       ロハロのかしていたい         ジステム 物理       ホスト名         AR260S       (オフション)         レード マック       ロバロのかしていたい         レード マック       (オフション)         レード マック       (オフション)         レード マック       (オフション)         レード マック       (オフション)         ログ       AC(アクセスコンセントレーター)名         ログ マット       (オフション)         (基数オブション)       (クレア	- アドレス(D) (値) http://192.168.1.1/index.html			多動
WANBER         CentreCOM AR260S         ビッカアップウ・ガード         ジンステムな場合         ロハ         レカトアップウ・ガード         ジンステムな場合         レハ         レカ         レカ         レカ         レカ         レカ         レカ<	VPN Router		¥ ● 務約 ▲ WAN設定 PPPoE ▼ PPPoE 0	
接続モード       PPPoE         セッションD       PPPoE         セッションD       PPPoE         セッションD       PPPoE         ジステム協能       ボスト名         ホスト名       AP260S         レーレームA       AP260S         レーレームA       バスワード         コンパードウリ       レーレームA         ログログ       レーレームA         マアパアウォール       ワービス名         マノード       ローログ         ログアウト       レービス名         ログアウト       ログワセスコンセントレーター/名         ログアウト       ログフレン         マノマト       ログフション)         ログアウト       ログフレーン         マノマト       ログフレーン         ログアウト       ログフレーン         ログアウリ       レーン         ログアウリ       ログワーン         ログワーン       ログワーン         ログワーン       ログワーン         ログワーン       ログワーン         ログワーン       ログログ         ログログ       ログワーン         ログログ       ログログ     <			WAN設定	Î
ビッションID         PPPoE0 、 地路           ビットコック・グザー・ウェイ         PPPoE0 、           ビットフック・グザー・ウェイ         PPPoE0 、           レロロumbered PPPoE         ○有効 ○無効           ホスト名         AP260S (オブション)           エーザー名         □           エーザー名         □           アナイアウォール         サービス名           サービス名         □           ログ         ステンセンドレーター名           ログ         マングンドンシンテム管理           ログ         ステンセンドレーター名           ログ         ステンセンドレーター名           ログ         マングンドンシンシン           ログ         ログ		接続モード	PPPoE 🗸	
CentreCOM AR280S       デフォルゲー・ウェイ       PPP6E0 ▼         ● クステム情報       ハロルのbered PPP0E       ○有効 ○無効         ● レムハ       ホスト名       AR260S (オブション)         ▲ レイ情報       スレイー名       □         ● レムハ       オスト名       AR260S (オブション)         ● レムハ       オスト名       AR260S (オブション)         ● レイオ       バスワード       □         ● レイオ       パスワード       □         ● レスス 各       □       (オブション)         ● レス ス ム 管理       ○       (オブション)         ● レス ク 合数       ○       (オブション)         ● レス ク 合数       ○       (オブション)         ● ログアウト       ○       (オブション)         ● ログアウト       ○       (オブション)       ●         ● ログアウト       ○       (オブション)       ●         ● ログアウト       ○       (カー       ●         ● ログアウト       ○       ●       ●         ● ログアウト       ○       ●       ●         ● ログアウト       ○       ●       ●		セッションID	PPPoE:0 🗸 接続	
セットアップウィヴード システム情報 レスト報告         Unnumbered PPPoE         ○有効 ○無効           レスト報告         AR260S         (オブション)           エーザー名	CentreCOM AR260S	デフォルトゲートウェイ	PPPoE:0 V	
		Unnumbered PPPoE	○有効 ●無効	
ユーザー名       1/1/14         レルキャンク       1/1/27         マンオイワオール       1/1/24         レノオキャンク       1/1/27         マンオイワオール       ワービス名         レノオキャンク       1/1/27         マンオンクション       ロ(オブション)         ログ       DNSオブション         ログアウト       1/1/27         道銀ブション       1/1/27         道銀ブション       1/1/27         道銀ブ       1/1/27         道銀ブ       1/1/27         1/1/27       1/1/27         1/1/27		ホスト名	AR260S (オブション)	
・ハーディグラ       バスワード         ・ハーディグラ       ワーイ         ・ファイアウォール       ワービス名         ・ログ       ログ         ・ログ       ログ         ・ログ       ハ         ・ログ       ・ログ         ・ログ       ・		ユーザー名		
サービス名     サービス名     「(オジョン)     サービス名     「(オジョン)     ログ     ログ     マンスム管理     ハンアウト     ログ     ログアウト     ログ     ログアウト     ログアウト     ログ     ログアウト     ログ     ロ     ログ     ログ     ログ     ロ     ログ     ロ     ロ     ロ     ログ     ログ     ロ     ロ     ログ     ロ     ロ     ロ     ログ     ロ     ロ     ログ     ロ     ロ     ロ     ロ     ロ     ログ     ロ		パスワード		
P ・ 22 テム管理 ・ 22 FA 管理 ・ 22 FA EA		サービス名	(オプション)	
DNSオブション       ○固定設定 ©自動取得         ブライマリDNSサーバー       (オブション)         セカンダリDNSサーバー       (オブション)         セカンダリDNSサーバー       (オブション)         MSSクランブ       〇無効 ●有効 MSSの値 40 Bytes         接続オブション       〇ダイアルオンデマンド ●キーブアライブ ○無効 エコー送信間隔 60 秒         近日の設定         現在の設定	□□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	AC(アクセスコンセントレーター)名	(オプション)	
ブライマリDNSサーバー     (オブション)       セカンダリDNSサーバー     (オブション)       MSSグランブ     ○無効 ○有効 MSSの値: 40 Bytes       超線オブション     〇ダイアルオンデマンド ○キーブアライブ ○無効 エコー送信間隔 60 秒       近年間隔 60 秒	□ 冉起動 □ ログアウト	DNSオプション	○固定設定 ⊙自動取得	
セカンダリDNSサーバー     (オブション)       MSSクランブ     〇無効 ©有効 MSSの値: 40 Bytes       提続オブション     〇ダイアルオンデマンド ③キーブアライブ 〇無効 エコー送信間隔 60 秒       現在の設定       現在の設定		プライマリDNSサーバー		
MSSクランブ     〇無効 ●有効 MSSの値 40 Bytes       投続オブション     〇ダイアルオンデマンド ●キーブアライブ ○無効 エコー送信開隔 60 秒       通用       現在の設定       現在の設定		セカンダリDNSサーバー	(オブション)	
日本部でははファーオーナープロテライブ ○無効     エコー送信間隔 60 秒     ひゅり ひゅう		MSSクランプ	○ 無効	● ● 秋和
道用 (ルフ) 現在の設定 オ+キがつよなフィット・・100000000000000000000000000000000000		接続オプション	<ul> <li>○ダイアルオンデマンド ●キーブアライブ ○無効</li> <li>エコー送信問題 60 秒</li> </ul>	
現在の設定				
		サージーン ロチへが	現在の設定	~

2. 接続モードに「PPPoE」を選択します。

	WAN設定
接続モード	PPPoE Y
	WE

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは、セッション ID「PPPoE:0」に以下のように設定す るものとします。

Unnumbered PPPoE	無効
ホスト名	mycomputer(プロバイダーから提供されたと仮定します)
ユーザー名	user@isp.ne.jp(プロバイダーから提供されたと仮定します)
パスワード	isppassword(プロバイダーから提供されたと仮定します)
DNS オプション	自動取得
MSS クランプ	有効、40Bytes
接続オプション	ダイアルオンデマンド、タイムアウトまでの時間 60 秒

PPPoE V	
PPPoE:0 🗸 接続	
PPPoE:0 V	
○有効 ◎無効	
mycomputer (オプション)	
user@isp.ne.jp	
•••••	
(オブション)	
(オブション)	
○固定設定 ⊙自動取得	
(オプション)	
(オブション)	
○無効 ◎有効	
MSSの値: 40 Bytes	
●ダイアルオンデマンド ○キーブアライブ ○無効	
タイムアウトまでの時間 60 秒	

4. 以上で設定は完了です。
## 3.3.2 設定の確認

#### WAN 側の設定は以下の手順で確認します。

1.メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。マルチセッションで接続している場合は、セッションごとに設定の 詳細が表示されます。

	現在の設定
基本設定が完了しました。現在の設	定は以下のとおりです。
LAN設定	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
DHCP	有効
WAN設定	
接続モード	PPPoE
デフォルトゲートウェイアドレス	10.10.31.32
セッションID	PPPoE:0
接続状況	接続
IPアドレス	10.10.31.25
PEERのアドレス	10.10.31.32
プライマリDNSサーバー	10.10.31.2
セカンダリDNSサーバー	
サブネットマスク	255.255.255.255
接続オブション	ダイアルオンデマンド
	タイムアウトまでの時間: 60 秒
17พกับสไปID	PPPoF-1
接続状況	未接続
IPアドレス	
PEERのアドレス	0.0.0.0
ブライマリDNSサーバー	
セカンダリDNSサーバー	
サブネットマスク	
接续才学的小学,	キープアライブ
1950和バイリンヨン	エコー送信間隔:60 秒

## 3.3.3 PPPoE セッションの切断 / 接続

PPPoE セッションを手動で切断 / 接続するには以下の手順を実行します。

1.メニューから「WAN」->「WAN」の順にクリックします。

2. 切断 / 接続するセッションを選択します。ここでは「PPPoE:0」を選択するものとします。

	WAN設定	
接続モード	PPPoE 🗸	
セッションID	PPPoE:0 x 接続	
デフォルルゲートウェイ		

3.「切断 / 接続」ボタンをクリックします。ここでは切断されたセッションを「接続」するものとします。

接続モード	PPPoE 🗸
セッションID	PPPoE:0 V HAG
ギウュルルゲニレウンス	

4. 以上で設定は完了です。

## 3.4 固定 IP アドレスを使用した WAN 側ネットワークへの接続

WAN 側インターフェースを固定 IP アドレスで接続する場合の手順について説明します。おもに PPPoE 接続サービス以外 で固定 IP アドレスを割り当てられているサービスで使用します。

### 3.4.1 設定

WAN 側インターフェースを固定 IP アドレスで接続するには以下の手順を実行します。

1.メニューから「WAN」->「WAN」の順にクリックします。

: アドレス(D) 🍓 http://192.168.1.1/index.html		💌 🔁 移動			
VPN Router		Allied Telesis			
	WAN設定				
	接続モード	PPPoE V			
	セッションID	PPPoE:0 V 接続			
CentreCOM AR260S	デフォルトゲートウェイ	PPPoE:0			
	Unnumbered PPPoE	○有効 ◎無効			
	ホスト名	AR260S (オブション)			
- WAN	ユーザー名				
	パスワード				
	サービス名	(オプション)			
─□  リク  □  <mark> □  システム管理</mark>	AC(アクセスコンセントレーター)名	(オプション)			
□ 冉起動 □ ログアウト	DNSオプション	○固定設定 ●自動取得			
	プライマリDNSサーバー	(オプション)			
	セカンダリDNSサーバー	(オブション)			
	MSSクランブ	○ 無効			
	接続オプション	○ダイアルオンデマンド ◎ キーブアライブ ○ 無効 エコー送信間隔 60 秒			
		( 適用 ) (ヘルプ)			
		現在の設定			

2. 接続モードに「固定 IP」を選択します。

	WAN設定
接続モード	
געואקפו	

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは、以下のように設定するものとします。

IPアドレス	200.100.10.54
サブネットマスク	255.255.255.0
ゲートウェイアドレス	200.100.10.1
プライマリ DNS サーバー	200.100.10.32

	WAN設定	
接続モード	固定IP 🗸	
IPアドレス	200.100.10.54	
サブネットマスク	255.255.255.0	
ゲートウェイアドレス	200.100.10.1	
プライマリDNSサーバー	200.100.10.32	
セカンダリDNSサーバー	(オプション)	
		レフ

4. 以上で設定は完了です。

## 3.4.2 設定の確認

#### WAN 側の設定は以下の手順で確認します。

1.メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。

	現在の設定	
基本設定が完了しました。現在の	設定は以下のとおりです。	
LAN設定		
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	
DHCP	有効	
WAN設定		
接続モード	面定IP 固定IP	
デフォルトゲートウェイアドレス	200.100.10.1	
プライマリDNSサーバー	200.100.10.32	
セカンダリDNSサーバー		
接続状況	接続	
IPアドレス	200.100.10.54	
サブネットマスク	255,255,255,0	

# 3.5 「WAN」ページの解説

「WAN」ページについて解説します。「WAN」ページでは本製品の WAN 側に関する設定を行います。

#### 3.5.1 WAN 設定

メニューから「WAN」->「WAN」の順にクリックすると以下の画面が表示されます。

	WAN設定
接続モード	固定IP 📉
IPアドレス	DHCP VS PPPoE 1
サブネットマスク	固定P 255.255.255.0

パラメーター	説明
接続モード	WANポートの接続モードを「DHCP」、 「PPPoE」、「固定 IP」の3つのオプショ ンから選択します。選択するオプション によって、設定画面に表示されるパラ メーターが異なります。



## 3.5.1.1 接続モードに「DHCP」を選択した場合

#### 接続モードに「DHCP」を選択すると、以下の画面が表示されます。

WAN設定			
接続モード	DHCP V		
ホスト名	AR260S (オプション)		
DNSオプション	○固定設定 ⊙自動取得		
プライマリDNSサーバー	(オブション)		
セカンダリDNSサーバー	(オプション)		
□ MACクローニング	00 - 00 - 00 - 00 - 00 - 00		
	(適用)	(ヘルプ)	



ご契約の ISP が DHCP をサポートしている場合に選択します。CATV のインターネット接続サービスなどは通常 DHCP 接続になります。

パラメーター	オプション	説明	
ホスト名			本製品のホスト名を入力します。半角英 数字で 63 文字以内で入力してください。 プロバイダーに指定されていない場合は 入力しないでください。
DNS オプション	固定設定 / 自動取得		プライマリ DNS サーバー、セカンダリ DNS サーバーを手動で入力する場合は 「固定設定」、自動で取得する場合は「自 動取得」ラジオボタンを選択します。
プライマリ DNS サーバー			ISP から DNS の情報が提供されている場 合に入力します。指定されていない場合 は入力しないでください。
セカンダリ DNS サーバー			ISP から DNS の情報が提供されている場 合に入力します。指定されていない場合 は入力しないでください。
MAC クローニング			本製品のWAN側のMACアドレスを、こ こで指定したMACアドレスに見せかけ る機能です。チェックボックスにチェッ クを入れるとMACクローニング機能が 有効になります。また、有効にした場合 は本製品に擬似的に割り当てるMACア ドレスを入力します。
「適用」ボタン			入力した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができま す。

\_\_\_\_\_

	現在の設定	
基本設定が完了し	しました。現在の設定は以下のとおりです。	
LAN設定		
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	
DHCP	有効	
WAN設定		
接続モード	DHCP	
デフォルトゲートウ	リェイアドレス	
プライマリDNSサ	ーバー 192.168.2.32	
セカンダリDNSサ	/ Ň	
接続状況	接続	
IPアドレス	192.168.2.1	
サブネットマスク	255.255.255.0	
MACクローニング	無効	
パラメーター	+	
~~~~~	17937	武 明
LAN 設定		本製品の LAN 側インターフェースに関 する情報が表示されます。
-	IPアドレス	現在本製品の LAN 側インターフェース に設定されている IP アドレスが表示さ れます。
-	サブネットマスク	現在本製品の LAN 側インターフェース に設定されているサブネットマスクが表 示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示 されます。
WAN 設定		本製品の WAN 側インターフェースに関 する情報が表示されます。
-	接続モード	現在の接続モードが表示されます。
-	デフォルトゲートウェイアドレス	デフォルトゲートウェイのアドレスが表 示されます。
-	プライマリ DNS サーバー	プライマリ DNS サーバーのアドレスが 表示されます。
-	セカンダリ DNS サーバー	セカンダリ DNS サーバーのアドレスが 表示されます。
-	接続状況	接続状況が表示されます。
-	旧アドレス	WAN 側インターフェースに設定されて いる IP アドレスが表示されます。
-	サブネットマスク	WAN 側インターフェースに設定されて いるサブネットマスクが表示されます。
-	MAC クローニング	MAC クローニングの有効 / 無効が表示 されます。

## 3.5.1.2 接続モードに「PPPoE」を選択した場合

### 接続モードに「PPPoE」を選択すると、以下の画面が表示されます。

	WAN設定
接続モード	PPPoE 🗸
セッションID	PPPoE:0 🗸 接続
デフォルトゲートウェイ	PPPoE:0 🗸
Unnumbered PPPoE	○有効 ④無効
ホスト名	AR260S (オブション)
ユーザー名	
パスワード	
サービス名	(オプション)
AC(アクセスコンセントレーター)名	(オブション)
DNSオブション	○固定設定 ⊙自動取得
プライマリDNSサーバー	(オブション)
セカンダリDNSサーバー	(オブション)
MSSクランプ	〇無効
接続オプション	<ul> <li>○ダイアルオンデマンド ● キープアライブ ○ 無効</li> <li>エコー送信間隔 60 秒</li> </ul>
	適用         ヘルプ

	こ契約の ISP が PPPoE をサポートしている場合に選択します。xDSL 回線を	利用する ISP では通常 PPPoE 接続になり
ヒント	、 ます。	

パラメーター	オプション	説明
セッション ID		確立するセッションの ID を選択します。
	PPPoE:0	1 つ目のセッションを設定、表示する場 合に選択します。
	PPPoE:1	2 つ目のセッションを設定、表示する場 合に選択します。
	「接続 / 切断」ボタン	選択したセッションを接続、切断する場 合にクリックします。
デフォルトゲートウ	7ェイ	デフォルトゲートウェイを選択します。
	PPPoE:0	pppoe0 のゲートウェイをデフォルト ゲートウェイに設定する場合に選択しま す。
	PPPoE:1	pppoe1 のゲートウェイをデフォルト ゲートウェイに設定する場合に選択しま す。

Unnumbered PPPoE	有効/無効	Unnumbered PPPoE を有効にする場合は 「有効」、無効にする場合は「無効」ラジ オボタンを選択します。
ホスト名		本製品のホスト名を入力します。半角英 数字で 63 文字以内で入力してください。 指定されていない場合は入力しないでく ださい。
ユーザー名		ISP から提供された PPP₀E 接続に使用す るユーザー名を入力します。半角英数字 で 63 文字以内で入力してください。
パスワード		ISP から提供された PPPoE 接続に使用す るパスワードを入力します。半角英数字 で 63 文字以内で入力してください。
サービス名		ISP から提供された PPPoE サービス名を 入力します。半角英数字で 80 文字以内 で入力してください。指定されていない 場合は入力しないでください。
AC(アクセスコンヤ	エントレーター) 名	ISP から提供された PPPoE AC(アクセ スコンセントレーター)名を入力しま す。半角英数字で 15 文字以内で入力し てください。指定されていない場合は入 力しないでください。
DNS オプション	固定設定 / 自動取得	プライマリ DNS サーバー、セカンダリ DNS サーバーを手動で入力する場合は 「固定設定」、自動で取得する場合は「自 動取得」ラジオボタンを選択します。
プライマリ DNS サ-	-/-	ISP から DNS の情報が提供されている場 合に入力します。指定されていない場合 は入力しないでください。
セカンダリ DNS サ-	-/\$	ISP から DNS の情報が提供されている場 合に入力します。指定されていない場合 は入力しないでください。
MSS クランプ	有効/無効	MSS の値を設定する場合は「有効」、設 定しない場合は「無効」ラジオボタンを 選択します。
	MSS の値	MSS クランプを有効にした場合に、MSS (Maximum Segment Size) の値を入力し ます。40 ~ 120bytes の範囲で入力して ください。
接続オプション		接続する際のオプションを選択します。
-	ダイアルオンデマンド	ダイアルオンデマンドを有効にする場合 に選択します。
-	タイムアウトまでの時間	「ダイアルオンデマンド」を有効にした 場合にのみ表示されます。無通信時にイ ンターネット接続を切断するまでの時間 を入力します。60 秒~ 600 秒の範囲で 入力してください。
-	キープアライブ	キープアライブを有効にする場合に選択 します。
-	エコー送信間隔	「キープアライブ」を有効にした場合に のみ表示されます。無通信時でもイン ターネット接続を切断しないために送る

		エコーの送信間隔を入力します。60 秒 ~ 600 秒の範囲で入力してください。
	無効	接続オプションを使用しない場合に選択 します。
「適用」ボタン		入力した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

	現在の設定	
基本設定が完了しました。現在	主の設定は以下のとおりです。	
LAN設定		
IPアドレス	192.168.1.1	
サブネットマスク	255.255.255.0	
DHCP	有効	
WAN設定		
接続モード	PPPoE	
デフォルトゲートウェイアドレス	10.10.31.32	
セッションID	PPPoE:0	
接続状況	接続	
IPアドレス	10.10.31.25	
PEERのアドレス	10.10.31.32	
プライマリDNSサーバー	10.10.31.2	
セカンダリDNSサーバー		
サブネットマスク	255.255.255.255	
接続オプション	タイアルオンテマンド タイムアウトまでの時間: 60 秒	
セッジノコンノロ	PPPoE-1	
接続状況	未接続	
IPアドレス	- 1 - 126000 M	
PEERのアドレス	0000	
プライマリDNSサーバー		
セカンダリDNSサーバー		
サブネットマスク		
接続オポット	キープアライブ	
1200/0-0 2 2 4 2	エコー送信間隔:60 秒	
パラメーター	オプション	説明
I AN 設定		大制品の I AN 側インターフェースに閉
		する情報が表示されます。
		現在本製品の I AN 側インターフェース
		に設定されている IP アドレスが表示さ れます。
	サブネットマスク	現在本製品の I AN 側インターフェース
		に設定されているサブネットマスクが表 示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示 されます。
WAN 設定		本製品の WAN 側インターフェースに関 する情報が表示されます。
	接続モード	現在の接続モードが表示されます。

デフォルトゲートウェイアドレス	デフォルトゲートウェイアドレスが表示 されます。
セッション ID	情報が表示されているセッション ID が 表示されます。
接続状況	セッションの接続状況が表示されます。
IPアドレス	セッションで割り当てられた WAN 側の IP アドレスが表示されます。
PEER のアドレス	接続された PPPoE サーバーのアドレス が表示されます。
プライマリ DNS サーバー	プライマリ DNS サーバーのアドレスが 表示されます。
セカンダリ DNS サーバー	セカンダリ DNS サーバーのアドレスが 表示されます。
サブネットマスク	セッションで割り当てられた WAN 側の サブネットマスクが表示されます。
接続オプション	セッションに設定された接続オプション が表示されます。

## 3.5.1.3 接続モードに「固定 IP」を選択した場合

#### 接続モードに「固定 IP」を選択すると、以下の画面が表示されます。

	WAN設定
接続モード	固定IP 🗸
IPアドレス	
サブネットマスク	
ゲートウェイアドレス	
プライマリDNSサーバー	
セカンダリDNSサーバー	(オプション)
	(適用) (ヘルプ)



固定IPアドレスを使用して接続する場合に選択します。

パラメーター	説明
IPアドレス	ISP から提供された IP アドレスを入力し ます。インターネット側から本製品への アクセスにはこの IP アドレスが使用さ れます。
サブネットマスク	ISP から提供されたサブネットマスクを 入力します。
ゲートウェイアドレス	ISP から提供されたゲートウェイの IP ア ドレスを入力します。
プライマリ / セカンダリ DNS サーバー	ISP から提供されたプライマリ / セカン ダリ DNS サーバーの IP アドレスを入力 します。指定されていない場合は入力し ないでください。

	現在の設定	
基本設定が	完了しました。現在の設定は以下のとおりです。	
LAN設定		
IPアドレス	192.168.1.1	
サブネットマ	マスク 255,255,255,0	
DHCP	有効	
AVANES:		
1327%で一下		
テノオルトク	ードウェイアドレス 200.100.10.1	
ブライマリロ	NSサーバー 200.100.10.32	
セカンダリロ	)NSサーバー	
接続状況	接続	
IPアドレス	200.100.10.54	
サブネットマ	マスク 255,255,255,0	
パラメーター	オプション	説明
		100 F3
LAN 設定		本製品の LAN 側インターフェースに関 する情報が表示されます。
-	IPアドレス	現在本製品の LAN 側インターフェース に設定されている IP アドレスが表示さ れます。
-	サブネットマスク	現在本製品の LAN 側インターフェース に設定されているサブネットマスクが 示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示 されます。
WAN 設定		本製品の WAN 側インターフェースに関 する情報が表示されます。
-	接続モード	現在の接続モードが表示されます。
-	デフォルトゲートウェイアドレス	デフォルトゲートウェイアドレスが表: されます。
-	プライマリ DNS サーバー	プライマリ DNS サーバーのアドレスが 表示されます。
-	セカンダリ DNS サーバー	セカンダリ DNS サーバーのアドレスが 表示されます。
-	接続状況	接続状況が表示されます。
-	IPアドレス	WAN 側の IP アドレスが表示されます。
-	サブネットマスク	WAN 側のサブネットマスクが表示され ます

## 3.6 トラフィックの確認

本製品では、WAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。WAN 側 インターフェースの送受信トラフィックは「統計情報」ページで確認します。

## 3.6.1 確認

1.メニューから「WAN」->「統計情報」をクリックします。

WAN Statistics	
ernet Statistics	
0	
2	
0	
0	
0	
0	
21300	
0	
25	
18	
0	
	nernet Statistics 0 2 0 0 0 0 21300 0 25 18 0

2.「WAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。

	WAN Statistics	
E	thernet Statistics	
Total Bytes Received	0	
Unicast Packets Received	0	
Multicast Packets Recieved	0	
Packets Received and Discarded	0	
Packets Received with Errors	0	
Packets Received with unknown Protocols	0	
Total Bytes Transmitted	0	
Unicast Packets Transmitted	0	
Multicast Packets Transmitted	0	
Packets Discarded while Transmission	0	
Packets Sent with Errors	0	
	西共	

## 3.6.2 「統計情報」ページの解説

# 「統計情報」ページについて解説します。「統計情報」ページでは、本製品の WAN 側インターフェースのパケット転送に関する統計を参照することができます。

メニューから「WAN」->「統計情報」の順にクリックすると以下の画面が表示されます。

	WAN Statistics	
E	thernet Statistics	
Total Bytes Received	0	
Unicast Packets Received	0	
Multicast Packets Recieved	0	
Packets Received and Discarded	0	
Packets Received with Errors	0	
Packets Received with unknown Protocols	0	
Total Bytes Transmitted	12798	
Unicast Packets Transmitted	Π	
Multicast Packets Transmitted	0	
Packets Discarded while Transmission	0	
Packets Sent with Errors	ő	
	更新	
パラメーター	_	説明
		we 73
Total Bytes Received		受信パケットの総バイト数がカウントさ れます。
Unicast Packets Received		受信ユニキャストパケットの総数がカウ ントされます。
Multicast Packets Received		受信マルチキャストパケットの総数がカ ウントされます。
Packets Received and Discarded		破棄されたパケット数がカウントされま す。
Packet Received with Errors		エラーパケット数がカウントされます。
Packets Received with unknown Protocols		未サポートプロトコルのパケット数がカ ウントされます。
Total Bytes Transmitted		転送パケットの総バイト数がカウントさ れます。
Unicast Packets Transmitted		転送ユニキャストパケット数がカウント されます。
Multicast Packets Transmitted		転送マルチキャストパケット数がカウン トされます。
Packets Discarded while Transmission		転送中に破棄されたパケット数がカウン トされます。
Packets Sent with Errors		転送されたエラーパケット数がカウント されます。
「更新」ボタン		統計情報の表示内容を更新します。

# 4 ルーティングの設定

## 4.1 概要

ルーティングには、RIP(Routing Information Protocol) などのプロトコルを使用して行うダイナミックルーティングと、スタ ティックルートを手動で設定してルーティングを行うスタティックルーティングがありますが、本製品では、スタティック ルーティングのみサポートしています。本章では、本製品のルーティング機能を「ルーティング」ページで設定する手順を説 明します。

## 4.2 スタティックルーティング

スタティックルーティングを設定する手順について説明します。

## 4.2.1 設定

スタティックルーティングを設定するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

ファイル(ヒ) 編集(ヒ) 表示(W) お気に入 アドレス(D) @ http://192168.1.1/index.html	ወው ማ	-nO	ヘルブ(円)			X * * * * * * * * * * * * * * * * * * *
VPN Router						Allied Telesis
	新規	追加		スタティックルーティ	ンク設定	
	宛先:	ネットワ	フークアドレス			
CentreCOM AR260S	ッセナム- ゲート	イット・ ・ウェ1	(アドレス			
				追加 変更		(ヘルフ)
$= \frac{1}{2} $				ルーティングテー	ーブル	
● <u>○</u> VPN - □ ログ	/	Ē	<mark>宛先ネットワークアドレス</mark> 0.0.0.0	<mark>宛先ネットマスク</mark> 0.0.0.0	<mark>ゲートウェイアドレス</mark> 200.100.10.1	<b>種類</b> スタティック
□ · · · · · · · · · · · · · · · · · · ·						

2. ドロップダウンリストから「新規追加」を選択します。

3. 各パラメーターに値を入力し「追加」ボタンをクリックします。ここでは、以下のように設定するものとします。

宛先ネットワークアドレス	192.168.2.0
宛先ネットマスク	255.255.255.0
ゲートウェイアドレス	192.168.1.1

新規追加 🖌	
宛先ネットワークアドレス	192.168.2.0
宛先ネットマスク	255.255.255.0
ゲートウェイアドレス	192.168.1.1

4. 以上で設定は完了です。

## 4.2.2 設定の確認

#### スタティックルーティングの設定は以下の手順で確認します。

1. メニューから「ルーティング」をクリックします。

2.「ルーティングテーブル」に、現在のルーティング設定が表示されます。

ルーティングテーブル					
		宛先ネットワークアドレス	宛先ネットマスク	ゲートウェイアドレス	種類
de la compañía de la		192.168.2.0	255.255.255.0	192.168.1.1	スタティック

#### 4.2.3 スタティックルーティングの変更

スタティックルーティングを変更するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

- 2.「スタティックルーティング設定」テーブルのドロップダウンリストから変更するルートを選択します。または、「ルーティン グテーブル」の該当ルート左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターの値を変更し「変更」ボタンをクリックします。

4. 以上で設定は完了です。

## 4.2.4 スタティックルーティングの削除

スタティックルーティングを削除するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

スタティックルーティング設定」テーブルのドロップダウンリストから削除するルートを選択し「削除」ボタンをクリックします。または、「ルーティングテーブル」の該当ルート左部にある「ごみ箱」アイコンをクリックします。

3.以上で設定は完了です。

# 4.3 「ルーティング」ページの解説

「ルーティング」ページについて解説します。「ルーティング」ページでは本製品のルーティングに関する設定を行いま す。

## 4.3.1 スタティックルーティング設定

スタティックルーティング設定	
新規追加 🗸	
宛先ネットワークアドレス	
宛先ネットマスク	
ゲートウェイアドレス	
〔追加〕 変更 〕 削除 〕	
パラメーター	説明
ドロップダウンリスト	ルートを新規追加する場合は「新規追 加」、既存のルートを変更 / 削除する場 合は、該当のルートの宛先ネットワーク アドレスを選択します。
宛先ネットワークアドレス	ルーティングの宛先ホスト、またはネッ トワークアドレスを入力します。
宛先ネットマスク	宛先ホスト、またはネットワークのネッ トマスクを入力します。
ゲートウェイアドレス	宛先ホスト、またはネットワークヘパ ケットを転送するゲートウェイの IP ア ドレスを入力します。
「追加」ボタン	ドロップダウンリストで「新規追加」を 選択した場合にアクティブになります。 ルーティングを追加登録します。15件 までのルーティングを追加することがで きます。ボタンをクリックすると設定内 容が即時に反映されます。
「変更」ボタン	ドロップダウンリストで既存のルートを 選択した場合にアクティブになります。 設定内容の変更を保存します。ボタンを クリックすると設定内容が即時に反映さ れます。
「削除」ボタン	ドロップダウンリストで既存のルートを 選択した場合にアクティブになります。 選択したルートを削除します。ボタンを クリックすると設定内容が即時に反映さ れます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

## 4.3.2 ルーティングテーブル

		ルーティングテー	ブル	
	宛先ネットワークアドレス	宛先ネットマスク	ゲートウェイアドレス	種類
d de la constante de la consta	192.168.2.0	255.255.255.0	192.168.1.1	スタティック

パラメーター	説明
宛先ネットワークアドレス	登録されたルートの宛先ネットワークア ドレスが表示されます。
宛先ネットマスク	登録されたルートの宛先ネットマスクが 表示されます。
ゲートウェイアドレス	登録されたルートのゲートウェイアドレ スが表示されます。
種類	ルーティングの種類が表示されます。
「えんぴつ」アイコン	クリックすると「ルーティングテーブ ル」の該当ルートの設定内容を変更する ことができます。
「ごみ箱」アイコン	クリックすると「ルーティングテーブ ル」から該当ルートを削除します。

# 5 ファイアウォールの設定

## 5.1 概要

ファイアウォールは、ポリシーを作成し、そのポリシーにマッチするパケットの通過を許可/拒否する機能です。本製品はス テートフルインスペクション型ファイアウォール機能を搭載しており、WAN 側からのパケットはデフォルトですべて破棄しま す(ファイアウォールを無効に設定した場合は無効になります)。また、NAT は WAN 側へ向けたパケットに対してインター フェース NAT が有効に設定されています(Outbound アクセスルール)。本章では、本製品の以下の 6 つのファイアウォール機 能について説明します。

- ・ Inbound アクセスルール
- ・ Outbound アクセスルール
- · ステルスモード
- ・ セルフアクセス
- ・ URL フィルター
- ・ DoS アタックプロテクト

## 5.2 Inbound アクセスルールの設定

Inbound ルールは、本製品を経由する WAN 側から LAN 側へ向けたトラフィックを制御するルールです。Inbound アクセス ルールは「Inbound アクセス」ページで作成します。

### 5.2.1 ルールの作成

ルールを作成するには以下の手順を実行します。



1. メニューから「ファイアウォール」->「Inbound アクセス」の順にクリックします。

- ファイル(E) 編集(E) 表示(V) お気に入	(り(合) ツール(田) ヘルプ(出)				🗙 🕺 🏹 🕺
アドレス(D) (創 http://192.168.1.1/index.htm)					▶ 🔁 移動
VPN Router					Allied Telesis
		Inboundアクt	zス制御設定		
	ID 新規追加 💌 アクシ	ョン 通過 💙 🛛 優先度 1 🗸	]		
	送信元	タイプ全て 🔽			
CentreCOM AR260S	宛先	タイプ全て 🗸			
	送信元ポート	タイプ全て 💌			
ーロンステム 暗難 田一山 LAN	宛先ポート	タイプ全て 🗸			
■ WAN	プロトコル	全て 💙			
	NAT	未定義 🗸			
- Inboundアクセス	ログ	○有効 ⊙無効			
URLフィルター	VPN	○有効 ⊙無効			
□-□ アドバンスト設定 □-□ ポリシーリスト		追加			ヘルプ
□ ● 統計情報 □ ● ● VPN		Inboundアクセ	ス制御リスト		
── □ ロク   ── □ システム管理	ID 送信元	宛先	プロトコル	NAT	アクション
一百起動					

2. ID ドロップダウンリストから「新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のポリシーでルールを設定するものとします。

アクション		通過
優先度		1
送信元		全て
宛先		全て
送信元ポート		全て
宛先ポート		サービス
	サービス	HTTP
NAT		IPアドレス
	IP アドレス	192.168.1.200
ログ		無効
VPN		無効

	Inboundアクセス制御設定
ID 新規追加 🔽 アクシ	ョン 通過 👻 優先度 1 🐱
送信元	タイブ 全て 🗸
宛先	タイプ 全て 🔍
送信元ポート	タイプ 全て 🔍
宛先ポート	タイブ サービス <b>マ</b> サービス HTTP <b>マ</b>
NAT	IPアドレス ▼ IPアドレス 192.168.1.200
ログ	○有効 ◎無効
VPN	○有効   ●   無効
	(派加) 変更   削除   ヘルプ



「送信元」、「宛先」で「IP プール」を選択する場合、「宛先ポート」で定義されていない「サービス」を選択する場合、 「NAT」で「NAT プール」を選択する場合は、各設定をあらかじめ行っておく必要があります。「IP プール」、「NAT プール」、「サービス」の設定方法の詳細については「P.129 各種ポリシーとサービスの設定」を参照してください。

4. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。

5.以上で設定は完了です。

#### 5.2.2 ルールの変更

ルールを変更するには以下の手順を実行します。

- 1. メニューから「ファイアウォール」->「Inbound アクセス」の順にクリックします。
- 2. ID ドロップダウンリストから変更するルールの ID を選択します。または、「Inbound アクセス制御リスト」テーブルの該当 ルール左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。
- 6. 以上で設定は完了です。

### 5.2.3 ルールの削除

#### ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「Inbound アクセス」の順にクリックします。

- ID ドロップダウンリストから削除するルールの ID を選択し「削除」ボタンをクリックします。または、「Inbound アクセス制 御リスト」テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。
- 3. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。
- 4. 以上で設定は完了です。

## 5.2.4 ルールの確認

#### ルールを確認するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「Inbound アクセス」の順にクリックします。

2.「Inbound アクセス制御リスト」テーブルにルールが一覧表示されます。

 Inboundアクセス制御リスト						
	ID	送信元	宛先	ブロトコル	NAT	アクション
/ 🗇	1	全て	全て	HTTP(TCP,80)	192.168.1.200	通過

### 5.2.5 「Inbound アクセス」ページの解説

「Inbound アクセス」ページについて解説します。「Inbound アクセス」ページでは本製品の受信トラフィックに関するア クセス制御の設定を行い、ファイアウォールのルールを設定します。

#### 5.2.5.1 Inbound アクセス制御設定テーブル

メニューから「ファイアウォール」->「Inbound アクセス」の順にクリックすると以下の画面が表示されます。

Inboundアクセス制御設定			
□ 新規追加 、	<ul> <li>アクション 1</li> </ul>	🍓 🖌 🥂 優先度 1 🖌	
送信元		タイプ全て 💌	
宛先		タイプ全て 💌	
送信元ポート		タイプ全て 🗸	
宛先ボート		タイプ全て 🗸	
プロトコル		全て V	
NAT		未定義	
ログ		○有効 ④無効	
VPN		○有効 ⊙無効	
		追加 変更 削除	
パラメーター	オプション		説明
IDドロップダウンリス	< Η		ファイアウォールのルールを新規追加す る場合は「新規追加」、既存のルールを 変更 / 削除する場合は該当の ID 番号を 選択します。
アクション	通過 / 破棄		ルールにマッチしたパケットに対するア クションを選択します。マッチしたパ ケットを転送する場合は「通過」、破棄 する場合は「破棄」を選択します。
優先度			ルールの優先度を選択します。数字が小 さくなると優先度が高くなります。ルー ルが複数存在する場合、優先度が高い順 にパケットにマッチングされます。
送信元			ルールを適用する送信元ネットワークの 指定方法を選択します。
	全て		送信元のすべてのコンピューターにルー ルを適用する場合に選択します。

IPアドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
	IP アドレス	タイプに「IP アドレス」を選択した場合 にのみ表示されます。ルールを適用する コンピューターの IP アドレスを入力し ます。
サブネット		ルールを適用するコンピューターをサブ ネット単位で指定する場合に選択しま す。
	アドレス	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットアドレスを 入力します。
	マスク	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットマスクを入 力します。
 範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
	始点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の始点 IP アドレスを入力します。
	終点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の終点 IP アドレスを入力します。
IP プール		ルールを適用するコンピューターをあら かじめ設定した IP プールで指定する場 合に選択します。IP プールの設定方法に ついては「P.129 IP プールの設定」を参 照してください。
	IP プール	タイプに「IP プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の IP ブール名をドロップダ ウンリストから選択します。
		ルールを適用する宛先ネットワークの指 定方法を選択します。
<b>全</b> て		宛先のすべてのコンピューターにルール を適用する場合に選択します。
IPアドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
	IPアドレス	タイプに「IP アドレス」を選択した場合 にのみ表示されます。ルールを適用する コンピューターの IP アドレスを入力し ます。

宛先

	サブネット		ルールを適用するコンピューターをサブ ネット単位で指定する場合に選択しま す。
		アドレス	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットアドレスを 入力します。
		マスク	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットマスクを入 力します。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあら かじめ設定した IP プールで指定する場 合に選択します。IP プールの設定方法に ついては「P.129 IP プールの設定」を参 照してください。
		IP プール	タイプに「IP プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の IP プール名をドロップダ ウンリストから選択します。
送信元ポート			ルールを適用する送信元ポートの指定方 法を選択します。
	全て		すべてのアプリケーションにルールを適 用する場合に選択します。
	ポート指定		特定のポートを使用するアプリケーショ ンにルールを適用する場合に選択しま す。
		ポート番号	タイプに「ポート指定」を選択した場合 にのみ表示されます。ルールを適用する アブリケーションで使用するポート番号 を入力します。ポート番号は1~65535 の範囲で入力してください。
	範囲指定		特定の範囲のポートを使用するアプリ ケーションにルールを適用する場合に選 択します。
		始点ポート	タイプに「範囲指定」を選択した場合に のみ表示されます。ポートを指定する範 囲の始点ポート番号を入力します。ポー

			ト番号は 1 ~ 65535 の範囲で入力してく ださい。
		終点ポート	タイプに「範囲指定」を選択した場合に のみ表示されます。ポートを指定する範 囲の終点ポート番号を入力します。ポー ト番号は1~ 65535 の範囲で入力してく ださい。
宛先ポート			ルールを適用する宛先ポートの指定方法 を選択します。
	 全て		すべてのアプリケーションにルールを適 用する場合に選択します。
	ポート指定		特定のポートを使用するアプリケーショ ンにルールを適用する場合に選択しま す。
		ポート番号	種類に「ポート指定」を選択した場合に のみ表示されます。ルールを適用するア プリケーションで使用するポート番号を 入力します。ポート番号は1~65535の 範囲で入力してください。
	範囲指定		特定の範囲のポートを使用するアプリ ケーションにルールを適用する場合に選 択します。
		始点ポート	種類に「範囲指定」を選択した場合にの み表示されます。ポートを指定する範囲 の始点ポート番号を入力します。ポート 番号は1~65535の範囲で入力してくだ さい。
		終点ポート	種類に「範囲指定」を選択した場合にの み表示されます。ポートを指定する範囲 の終点ポート番号を入力します。ポート 番号は1~65535の範囲で入力してくだ さい。
	サービス		ポートを指定せずに、あらかじめ定義さ れたサービスにルールを適用する場合に 選択します。
		サービス	タイプに「サービス」を選択した場合に のみ表示されます。ドロップダウンリス トからルールを適用するサービスを選択 します。リストにないサービスを指定す る場合は、あらかじめ定義しておいてく ださい。サービスの設定方法については 「P.139 サービスの設定」を参照してくだ さい。
プロトコル			宛先ポートパラメーターに「全て」、 「ポート指定」、「範囲指定」を選択した 場合に表示されます。サービスを選択し た場合には表示されません。ルールを適 用するプロトコルをドロップダウンリス トから選択します。
NAT			ルールに設定する NAT の種類を選択し ます。

	未定義		ルールに NAT を設定しない場合に選択 します。
	IP アドレス		IP アドレスを指定してルールに NAT を 設定する場合に選択します。
		IP アドレス	NAT に「IP アドレス」を選択した場合に のみ表示されます。本製品で受信したパ ケットの転送先コンピューターの IP ア ドレスを指定します。この機能は DMZ、 またはパーチャルサーバー機能と呼ばれ ます。
	NAT プール		ルールに設定する NAT をあらかじめ作 成した NAT プールで指定する場合に選 択します。DMZ、またはバーチャルサー バー機能の動作をするプールのみ選択可 能です。NAT プールの作成方法について は「P.134 NAT プールの設定」を参照し てください。
		プール	NAT に「NAT プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の NAT プールから選択しま す。
ログ	有効 / 無効		ルールのログを記録する場合は「有効」、 記録しない場合は「無効」ラジオボタン を選択します。
VPN	有効 / 無効		VPN 通信を使用する場合は「有効」、使 用しない場合は「無効」を選択します。
「追加」ボタン			IDドロップダウンリストで「新規追加」 を選択した場合にアクティブになりま す。ルールを追加登録します。Inbound/ Outbound アクセスを合わせて 150 件ま でのルールを追加することができます。 ボタンをクリックしても、本製品を再起 動するまで設定内容は反映されません。
「変更」ボタン			ID ドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。設定内容の変更を保存しま す。ボタンをクリックしても、本製品を 再起動するまで設定内容は反映されませ ん。
「削除」ボタン			IDドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。選択したルールを削除しま す。ボタンをクリックしても、本製品を 再起動するまで設定内容は反映されませ ん。
「ヘルプ」ボタン			操作のヒントを参照することができま す。

## 5.2.5.2 Inbound アクセス制御リスト

Inboundアクセス制御リスト							
		ID	送信元	宛先	プロトコル	NAT	アクション
ø	Ē	1	全て	全て	HTTP(TCP,80)	192.168.1.200	通過

パラメーター	説明
ID	ルールの ID 番号が表示されます。
送信元	ルールが適用される送信元コンピュー ターの IP アドレスが表示されます。
 宛先	ルールが適用される宛先コンピューター の IP アドレスが表示されます。
プロトコル	ルールが適用されるプロトコル、サービ ス名、ポート番号が表示されます。
NAT	ルールに設定された NAT の内容が表示 されます。
アクション	ルールに設定されたアクションです。通 過 / 破棄のいずれかが表示されます。
「えんぴつ」アイコン	クリックすると「Inbound アクセス制御 リスト」の該当ルールの設定内容を変更 することができます。
「ごみ箱」アイコン	クリックすると「Inbound アクセス制御 リスト」から該当ルールを削除します。

# 5.3 Outbound アクセスルールの設定

Outbound アクセスルールは、本製品を経由する LAN 側から WAN 側へ向けたトラフィックを制御するルールです。 Outbound アクセスルールは「Outbound アクセス」ページで作成します。

### 5.3.1 デフォルトポリシー

Outbound アクセスルールにはデフォルトでポリシーが設定されています。ポリシーの内容は下記のとおりです。このポ リシーが設定されていることで、LAN 側からインターネットへ向けたパケットの IP アドレスは全て pppoe0 インター フェースの IP アドレスに変換され、インターネット通信が可能になります。

通過
1
全て
インターフェース NAT(pppoe0)
無効
無効



デフォルトのポリシーの優先度を変更したり、他に Outbound アクセスルールを追加した場合、インターネットへの通 信ができなくなることもありますので、ルールを追加する場合は正確に設定してください。

## 5.3.2 ルールの作成

ルールを作成するには以下の手順を実行します。



1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。

アドレス(D) 🕘 http://192.168.1.1/index	html				✓ →
VPN Router					Allied Tele
		Outboundアク	セス制御設定		
	ID 新規追加 🔽 アク	ンョン 通過 🖌 🦷 優先度 1 🔹	•		
	送信元	タイプ全て 🗸			
	宛先	タイプ全て 🔽			
・ セットアップウィザード	送信元ポート	タイプ 全て 🗸			
- 📑 システム 情報 - 🎦 LAN	宛先ボート	タイプ 全て 🗸			
WAN	プロトコル	全て V			
ーコルーフィンシ ーコーファイアウォール	NAT	未定義			
Inboundアクセス Outhoundアクセス	ログ	○有効 ⊙無効			
- Unit Jink Jink	VPN	○有効 ⊙無効			
申 □ アドバンスト設定 □ ポリシーリスト □ 統計情報		追加			ヘルプ
		Outboundアク	セス制御リスト		
□□□ □システム管理	ID 送信元	宛先	プロトコル	NAT	アクション
·	☆ 〒 1 全て     ☆      ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆     ☆	200.100.20.1	全て,全て,全て	pppoe0	破棄
	❷ Ⅲ 2 至℃	主て	主(主(主)	ethu	進迴

2. ID ドロップダウンリストから「新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のポリシーでルールを設定するものとします。

アクション	破棄
優先度	1
送信元	全て
	IPアドレス

	IPアドレス	200.100.20.1
送信元ポート		全て
宛先ポート		全て
プロトコル		全て
NAT		インターフェース NAT
	インターフェース	ррроеО
ログ 		無効
VPN		無効

□ 新規追加 🎽 ア	ブション [ 繊栗 ▼ ]
送信元	タイプ 全て 💌
宛先	タイプ IPアドレス ▼ IPアドレス 200.100.20.1
送信元ポート	タイプ 全て 🗸
宛先ポート	タイプ 全て 🗸
プロトコル	全て
NAT	インタフェースNAT ▼ インターフェース pppce0 ▼
ログ	○有効
VPN	○有効 ④無効

「送信元」、「宛先」で「IP ブール」を選択する場合、「宛先ポート」で定義されていない「サービス」を選択する場合、 ヒント 「NAT」で「NAT プール」を選択する場合は、各設定をあらかじめ行っておく必要があります。「IP プール」、「NAT プール」、「サービス」の設定方法の詳細については「P.129 各種ポリシーとサービスの設定」を参照してください。

4. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。

5.以上で設定は完了です。

#### 5.3.3 ルールの変更

#### ルールを変更するには以下の手順を実行します。

- 1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。
- 2. ID ドロップダウンリストから変更するルールの ID を選択します。または、「Outbound アクセス制御リスト」テーブルの該当 ルール左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。

6.以上で設定は完了です。

#### 5.3.4 ルールの削除

ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。

 ID ドロップダウンリストから削除するルールの ID を選択し「削除」ボタンをクリックします。または、「Outbound アクセス 制御リスト」テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。

3. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。

4. 以上で設定は完了です。

#### 5.3.5 ルールの確認

#### ルールを確認するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。

2.「Outbound アクセス制御リスト」テーブルにルールが一覧表示されます。

Outboundアクセス制御リスト							
		ID	送信元	宛先	プロトコル	NAT	アクション
J	団	1	全て	200.100.20.1	全て,全て,全て	pppoe0	破棄
1	亩	2	全て	全て	全て,全て,全て	eth0	通過

## 5.3.6 「Outbound アクセス」ページの解説

「Outbound アクセス」ページについて解説します。「Outbound アクセス」ページでは本製品の送信トラフィックに関する アクセス制御の設定を行い、ファイアウォールのルールを設定します。

#### 5.3.6.1 Outbound アクセス制御設定

メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックすると以下の画面が表示されます。

	Outboundアクセス制御設定				
ID 新規追加 🔽 アク	ション 通過 🗸 🦷 優先度 1 🗸				
送信元	タイプ 全て 🔍				
宛先	タイプ 全て 🔍				
送信元ポート	タイプ 全て 🔍				
宛先ボート	タイプ 全て 🔍				
プロトコル	全て 🖌				
NAT	未定義				
ログ	○有効 ◎無効				
VPN	○有効 ◎無効				
	追加 変更 削除 ヘルフ				

パラメーター	オプション		説明
IDドロップダウン	ンリスト		ファイアウォールのルールを新規追加す る場合は「新規追加」、既存のルールを 変更 / 削除する場合は該当の ID 番号を 選択します。
アクション	通過 / 破棄		ルールにマッチしたパケットに対するア クションを選択します。マッチしたパ ケットを転送する場合は「通過」、破棄 する場合は「破棄」を選択します。
優先度			ルールの優先度を選択します。数字が小 さくなると優先度が高くなります。ルー ルが複数存在する場合、優先度が高い順 にパケットにマッチングされます。
送信元			ルールを適用する送信元ネットワークの 指定方法を選択します。
	 全て		送信元のすべてのコンピューターにルー ルを適用する場合に選択します。
	IPアドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
		IPアドレス	タイプに「IP アドレス」を選択した場合 にのみ表示されます。ルールを適用する コンピューターの IP アドレスを入力し ます。
	サブネット		ルールを適用するコンピューターをサブ ネット単位で指定する場合に選択しま す。
		アドレス	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットアドレスを 入力します。
		マスク	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットマスクを入 力します。
	 範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあら かじめ設定した IP ブールで指定する場 合に選択します。IP プールの設定方法に ついては「P.129 IP プールの設定」を参 照してください。

		IP プール	タイプに「IP プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の IP プール名をドロップダ ウンリストから選択します。
宛先			ルールを適用する宛先ネットワークの指 定方法を選択します。
	 全て		宛先のすべてのコンピューターにルール を適用する場合に選択します。
	IPアドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
		IPアドレス	タイプに「IP アドレス」を選択した場合 にのみ表示されます。ルールを適用する コンピューターの IP アドレスを入力し ます。
	サブネット		ルールを適用するコンピューターをサブ ネット単位で指定する場合に選択しま す。
		アドレス	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットアドレスを 入力します。
		マスク	タイプに「サブネット」を選択した場合 にのみ表示されます。ルールを適用する コンピューターのサブネットマスクを入 カします。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	タイプに「範囲指定」を選択した場合に のみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあら かじめ設定した IP プールで指定する場 合に選択します。IP プールの設定方法に ついては「P.129 IP プールの設定」を参 照してください。
		IP プール	タイプに「IP プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の IP プール名をドロップダ ウンリストから選択します。
送信元ポート			ルールを適用する送信元ポートの指定方 法を選択します。

宛先ポート

 全て		すべてのアプリケーションにルールを適 用する場合に選択します。	
ポート指定		特定のポートを使用するアプリケーショ ンにルールを適用する場合に選択しま す。	
	ポート番号	タイプに「ポート指定」を選択した場合 にのみ表示されます。ルールを適用する アプリケーションで使用するポート番号 を入力します。ポート番号は1~65535 の範囲で入力してください。	
範囲指定		特定の範囲のポートを使用するアプリ ケーションにルールを適用する場合に選 択します。	
	始点ポート	タイプに「範囲指定」を選択した場合に のみ表示されます。ポートを指定する範 囲の始点ポート番号を入力します。ポー ト番号は1~65535の範囲で入力してく ださい。	
	終点ポート	タイプに「範囲指定」を選択した場合に のみ表示されます。ポートを指定する範 囲の終点ポート番号を入力します。ポー ト番号は1~ 65535 の範囲で入力してく ださい。	
		ルールを適用する宛先ポートの指定方法 を選択します。	
全て		すべてのアプリケーションにルールを適 用する場合に選択します。	
ポート指定		特定のポートを使用するアプリケーショ ンにルールを適用する場合に選択しま す。	
	ポート番号	種類に「ポート指定」を選択した場合に のみ表示されます。ルールを適用するア プリケーションで使用するポート番号を 入力します。ポート番号は1~65535の 範囲で入力してください。	
範囲指定		特定の範囲のポートを使用するアプリ ケーションにルールを適用する場合に選 択します。	
	始点ポート	種類に「範囲指定」を選択した場合にの み表示されます。ポートを指定する範囲 の始点ボート番号を入力します。ボート 番号は1~65535の範囲で入力してくだ さい。	
	終点ポート	種類に「範囲指定」を選択した場合にの み表示されます。ポートを指定する範囲 の終点ポート番号を入力します。ポート 番号は1~65535の範囲で入力してくだ さい。	
	サービス		ポートを指定せずに、あらかじめ定義さ れたサービスにルールを適用する場合に 選択します。
---------	---------	---------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------
		サービス	タイプに「サービス」を選択した場合に のみ表示されます。ドロップダウンリス トからルールを適用するサービスを選択 します。サービスの設定方法については 「P.139 サービスの設定」を参照してくだ さい。
プロトコル			宛先ポートパラメーターに「全て」、 「ポート指定」、「範囲指定」を選択した 場合に表示されます。「サービス」を選 択した場合には表示されません。ルール を適用するプロトコルをドロップダウン リストから選択します。
NAT			ルールに設定する NAT の種類を選択し ます。
	未定義		ルールに NAT を設定しない場合に選択 します。
	IPアドレス		IP アドレスを指定してルールに NAT を 設定する場合に選択します。
		IP アドレス	NAT に「IP アドレス」を選択した場合に のみ表示されます。本製品で受信したパ ケットの転送先コンピューターの IP ア ドレスを指定します。
	NAT プール		ルールに設定する NAT をあらかじめ作 成した NAT プールで指定する場合に選 択します。NAT プールの作成方法につい ては「P.134 NAT プールの設定」を参照 してください。
		プール	NAT に「NAT プール」を選択した場合に のみ表示されます。あらかじめ設定され ている既存の NAT プールから選択しま す。
ログ	有効 / 無効		ルールのログを記録する場合は「有効」、 記録しない場合は「無効」ラジオボタン を選択します。
VPN	有効 / 無効		VPN 通信を使用する場合は「有効」、使 用しない場合は「無効」を選択します。
「追加」ボタン			ID ドロップダウンリストで「新規追加」 を選択した場合にアクティブになりま す。ルールを追加登録します。Inbound/ Outbound アクセスを合わせて 150 件ま でのルールを追加することができます。 ボタンをクリックしても、本製品を再起 動するまで設定内容は反映されません。
「変更」ボタン			ID ドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。設定内容の変更を保存しま す。ボタンをクリックしても、本製品を 再起動するまで設定内容は反映されませ ん。

「削除」ボタン	IDドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。選択したルールを削除しま す。ボタンをクリックしても、本製品を 再起動するまで設定内容は反映されませ ん。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

# 5.3.6.2 Outbound アクセス制御リスト

	Outboundア	クセス制御リスト			
ID 送信元	宛先	プロトコル	NAT	アクション	
🖉 💼 1 全て	全て	全て,全て,全て	eth0	通過	
パラメーター			説明		
ID			ルールの ID 番	号が表示されます	•
送信元			ルールが適用さ ターの IP アド	きれる送信元コン レスが表示されま	ピュー す。
宛先			ルールが適用さ の IP アドレス:	きれる宛先コンピ が表示されます。	ューター
プロトコル			ルールが適用さ ス名、ポート者	れるプロトコル 号が表示されま	、サービ す。
NAT			ルールに設定さ されます。	sれた NAT の内容	が表示
アクション			ルールに設定さ 過 / 破棄のいす	れたアクション 「れかが表示され	です。通 ます。
「えんぴつ」アイコン			クリックすると 御リスト」の調 更することがで	: 「Outbound アク 核当ルールの設定  『きます。	セス制 内容を変
「ごみ箱」アイコン			クリックすると 御リスト」から す。	- 「Outbound アク b該当ルールを削	セス制 除しま

# 5.4 ステルスモードの設定

ステルスモードは、本製品に対する外部からのポートスキャンなどに対して本製品からの応答を返さないようにする機能 です。ただし、セルフアクセスルールで特定のポートをオープンしている場合は、そのポートに対しての応答を返しま す。セルフアクセスルールについては「P.112 セルフアクセスルールの設定」を参照してください。

### 5.4.1 ステルスモード

ステルスモードの設定について説明します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

ファイル(E) 編集(E) 表示(V) お気(2	(人り(色) ツール(① ヘルブ(世)		¥? » 🦓
アドレス(D) 🧃 http://192.168.1.1/index.ht	ml		ど 🔁 移動
VPN Router			Allied Telesis
		ステルスモード設計	Ê
	ステルスモード	○ 有効 ④ 無効	
E		適用	
CentreCOM AR260S		セルフアクセス設計	Ê
	新規追加 🖌		
	プロトコル	TCP 🗸	
🕀 🦲 WAN	ボート		
ー <u>□</u> ルーティング □- <u>□</u> ファイアウォール	LAN側からのアクセス	○有効 ⊙無効	
Inboundアクセス	WAN側からのアクセス	○有効 ⊙無効	
		追加 麥更	削除
ローコアドバンスト設定			
<u>サービ</u> DoS		セルフアクセスルー	JL
□ □ ポリシーリスト	プロトコル	ボート	方向
	/ 📅 ICMP	0	LAN
		80	LAN
田 システム管理		161	LAN
一日クアウト		162	LAN
		03	LAN
		500	WAN
	·	000	
			Allied lelesi
		ステルスモード設定	
ステルスモード	○ 有效	九 💿 無効	
	O HX		
		適用	
パラメーター オ	プション		説明
ステルスモード 有	効 / 無効		ステルスモードを有効にする場合は「有 効」、無効にする場合は「無効」ラジオ ボタンを選択します。デフォルト設定は 「無効」です。
「適用」ボタン			設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができま す。

# 5.5 セルフアクセスルールの設定

セルフアクセスルールは、本製品本体へ向けたアクセスを制御するルールです。セルフアクセスルールは「セルフアクセス」ページで設定します。

### 5.5.1 デフォルト設定

本製品では、デフォルトで以下のセルフアクセスルールが設定されています。

プロトコル	ポート	方向
ICMP	0	LAN からのアクセス
ТСР	80	LAN からのアクセス
UDP	161	LAN からのアクセス
UDP	162	LAN からのアクセス
UDP	53	LAN からのアクセス
ТСР	10081	LAN からのアクセス
UDP	500	WAN からのアクセス

デフォルトのルールを削除、変更しないでください。削除や変更をおこなった場合、正常な通信ができなくなる場合 ント があります。



TCP の 80 番ポートは LAN 側コンピューターから本製品を設定する際に使用します。また、TCP の 10081 番ポートは ファームウェアの更新をおこなう際に使用します。

# 5.5.2 ルールの作成

### ルールを作成するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

ファイル(E) 編集(E) 表示(V) お気	に入り( <u>A</u> ) ツール	う くこう (日)		<b>Y</b> ? »	
: アドレス(D) 🧃 http://192.168.1.1/index.	ntml				移動
VPN Router				Allied Tele	esi
				,	
	フテルフ	7モード			٩.
					-
			()		1
CentreCOM AR260S			セルフアクセス設定	2	
ー ロットアップウィザード	新規追加	n 🗸			
	プロトコ	μ μ	TCP V		
	ポート				-
ーコルーティング	L a NI/BUA				-
□ □ ファイアウォール		からのアクビス			-
	VVAN(R)	からのアクセス	○有効◎無効		_
	追加 変更 削除 ヘルプ				
P コアドバンスト設定 アドバンスト設定					
- <u><u></u> + </u>			セルファカセス ルー	1.	
一日 105		プロトコル	ボート	方向	
	1		0	LAN	
B-COVPN	/ 1	TCP	80	LAN	
□□□2 田□システム管理	1	UDP	161	LAN	
再起動	1	UDP	162	LAN	
ーコログアウト	1	UDP	53	LAN	
	1	TCP	10081	LAN	
	1	UDP	500	WAN	

2. ドロップダウンリストから「新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のポリシーでルールを設定するものとします。

プロトコル	ТСР
ポート	21
LAN 側からのアクセス	有効
- WAN 側からのアクセス	無効

		the second se
	セルフアクセス設定	
新規追加 🖌		
プロトコル	TCP 💌	
ポート	21	
LAN側からのアクセス	◎有効 ○無効	
WAN側からのアクセス	○有効 ④無効	
	<b>追帜</b> 変更 削除	ヘルプ



4. 以上で設定は完了です。

### 5.5.3 ルールの変更

#### ルールを変更するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

- ドロップダウンリストから変更するルールを選択します。または、「セルフアクセスルール」テーブルの該当ルール左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。



アクセスの方向(「LAN 側からのアクセス」、「WAN 側からのアクセス」)のみ変更可能です。

- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

#### 5.5.4 ルールの削除

#### ルールを削除するには以下の手順を実行します。

- 1.メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。
- 2. ドロップダウンリストから削除するルールを選択し「削除」ボタンをクリックします。または、「セルフアクセスルール」 テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。
- 3.以上で設定は完了です。

### 5.5.5 ルールの確認

#### ルールを確認するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

2.「セルフアクセスルール」テーブルにルールが一覧表示されます。

			セルファクセスルート	لم ا
		ブロトコル	ポート	方向
P	Ē	ICMP	0	LAN
1		TCP	80	LAN
1		UDP	161	LAN
s/P		UDP	162	LAN
Ø	Ē	UDP	53	LAN
s/P		TCP	10081	LAN
s and a second s	Ē	UDP	500	WAN
1		TCP	21	LAN

# 5.5.6 「セルフアクセス」ページの解説

「セルフアクセス」ページについて解説します。「セルフアクセス」ページでは、本製品本体に着信したパケットの処理 ルールについて設定します。

# 5.5.6.1 セルフアクセス設定

メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックすると以下の画面が表示され ます。

		セルコ	ファクセス設定	
	新規追加 🗸			
	プロトコル	тср 🗸		
	ポート			
	LAN側からのアクセス	◎有効 ◎無効		
	WAN側からのアクセス	○有効 ⊙無効		
		追加	変更削除	ヘルプ
パラ	メーター		オプション	説明
ドロ	ップダウンリスト			セルフアクセスルールを新規に追加する 場合は「新規追加」、既存のルールを変 更 / 削除する場合は該当のルールを選択 します。
プロ	トコル			ルールを適用するプロトコルを選択しま す。
ポー	۲			プロトコルに「TCP」、「UDP」を選択し た場合にのみ表示されます。ルールを適 用するプロトコルで使用するポート番号 を入力します。
LAN	側からのアクセス		有効 / 無効	LAN 側からの本製品へのアクセスを有効 にするルールを作成する場合は「有効」、 無効にするルールを作成する場合は「無 効」ラジオボタンを選択します。本パラ メーターを無効にした場合は、「WAN 側 からのアクセス」を有効にする必要があ ります。
WAN	側からのアクセス		有効 / 無効	WAN 側からの本製品へのアクセスを有 効にするルールを作成する場合は「有 効」、無効にするルールを作成する場合 は「無効」ラジオボタンを選択します。 本パラメーターを無効にした場合は、 「LAN 側からのアクセス」を有効にする 必要があります。
「追加	ロ」ボタン			ドロップダウンリストで「新規追加」を 選択した場合にアクティブになります。 ルールを追加登録します。50件までの ルールを追加することができます。ボタ ンをクリックすると設定内容が即時に反 映されます。
「変す	更」ボタン			ドロップダウンリストで既存のルールを 選択した場合にアクティブになります。 設定内容の変更を保存します。ボタンを クリックすると設定内容が即時に反映さ れます。
「削除	 余」ボタン			ドロップダウンリストで既存ルールを選 択した場合にアクティブになります。選 択したルールを削除します。ボタンをク

リックすると設定内容が即時に反映され ます。

「ヘルプ」ボタン	操作のヒントを参照することができま す。

### 5.5.6.2 セルフアクセスルール

現在設定されているセルフアクセスルールが一覧表示されます。

		セルフアクセスルー	IL
	プロトコル	ボート	方向
/ 💼	ICMP	0	LAN
/ 🗇	TCP	80	LAN
/ 🗇	UDP	161	LAN
/ 🖻	UDP	162	LAN
/ 🗇	UDP	53	LAN
/ 🗇	TCP	10081	LAN
1 🗇	UDP	500	WAN
パラメータ	r —		説明
プロトコル	,		ルールが適用されるプロトコルが表示さ れます。
ポート			ルールが適用されるポートの番号が表示 されます。ポート番号が指定されないブ ロトコルについては、「0」と表示されま す。
方向			有効なアクセスの方向が LAN/WAN のい ずれかで表示されます。

# 5.6 URL フィルターの設定

URL フィルターは、指定したキーワードを URL に含む Web サイトへのアクセスを制限する機能です。ここでは、URL フィ ルターの有効 / 無効、キーワードの追加方法、フィルターの確認を「URL フィルター」ページで行う手順について説明し ます。

### 5.6.1 URL フィルターの有効 / 無効

URL フィルターを有効 / 無効にするには以下の手順を実行します。また、コンピューターで使用しているプロキシーポートも指定します。

1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。

ファイル(E) 編集(E) 表示(V) お気に入	い(A) ツール(① ヘルプ(H)		🍸 » 🦧
: アドレス(D) 🕘 http://192.168.1.1/index.html	I		🐱 🔁 移動
VPN Router	^		Allied Telesis
		URLフィルター設定	
-	URLフィルター	◎ 有効 ○ 無効	
		URLフィルターテーブル	
CentreCOM AR260S	D 新規追加 🗸		
ー ヨセットアップウィザード ー ヨシステム情報	+-ワド		
		(追加)(削除)	
- DHCP - 同面定DHCPクライアント		現在のURLフィルター設定	
→ 🗍 統計情報	ID キーワード		
ー D ルーティング ローマイアウォール			
セルフアクセス			
DoS			
□- <b>□</b> #リシーリスト <b>〕</b> IPナール			
⊟-·⊒ VPN 			

 IURL フィルター設定」テーブルで各パラメーターを設定し「追加」ボタンをクリックします。ここでは URL フィルターを 「有効」、プロキシーポートを「1080」に設定するものとします。

		Allied le
	URLフィルター設定	
URLフィルター	◎ 有効 ○ 無効	
ブロキシーボート	1080	
	URLフィルターテーブル	
ID 新規追加 🗸		
キーワード		
	(真如) 削除	(ヘルプ

3.以上で設定は完了です。

### 5.6.2 キーワードの追加

URL フィルターを有効にしたら、キーワードを追加します。キーワードを追加すると、そのキーワードを URL に含む Web サイトへのアクセスが制限されます。

1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。

2.「URL フィルターテーブル」の ID ドロップダウンリストから「新規追加」を選択します。

117

3. キーワードを入力し「追加」ボタンをクリックします。ここでは、キーワードに「abcnews」を指定するものとします。

ZHIZ ZP I	1000	
	URLフィルターテーブル	
ID 新規追加 🖌		
キーワード	abcnews	
	(追加)。 削除	ヘルプ

4. 以上で設定は完了です。

### 5.6.3 プロキシーポートの変更

プロキシーポートを変更するには以下の手順を実行します。

- 1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。
- 2.「現在の URL フィルター設定」テーブルの該当キーワード左部にある「えんぴつ」アイコンをクリックします。
- 3. プロキシーポートの値を変更します。
- 4.「追加」ボタンをクリックします。
- 5.以上で設定は完了です。

### 5.6.4 キーワードの削除

キーワードを削除するには以下の手順を実行します。

- 1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。
- 2.「現在の URL フィルター設定」テーブルの該当キーワード左部にある「ごみ箱」アイコンをクリックします。または、「URL フィルターテーブル」の ID ドロップダウンリストから該当のキーワードを選択し「削除」ボタンをクリックします。

3. 以上で設定は完了です。

### 5.6.5 キーワードの確認

1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。

2.「現在のフィルター設定」テーブルにキーワードが一覧表示されます。

5				現在のURLフィルター設定
			ID	+-ワ- <b>ŀ</b>
	di Barris	Ē	1	abonews

# 5.6.6 「URL フィルター」ページの解説

「URL フィルター」ページについて解説します。「URL フィルター」ページでは、キーワードを指定して特定の Web サイト へのアクセスを制限できる URL フィルター機能に関する設定をします。

### 5.6.6.1 URL フィルター設定 /URL フィルターテーブル

URL フィルターの有効 / 無効を設定するテーブルです。メニューから「ファイアウォール」->「URL フィルター」の順にクリック すると以下の画面が表示されます。

URI フィルター			
ブロキシーボー	<u>ا</u>	80	
2 H 12 H	'	URLフィルターテーブル	
ID 新規追加 ∨			
キーワード			
		追加削除	
パラメーター	オプション		説明
URL フィルター	有効 / 無効		URL フィルターを有効にする場合は「有 効」、無効にする場合は「無効」ラジオ ボタンを選択します。
プロキシーポート			コンピューターの Web ブラウザーに設 定したプロキシーポートの番号を入力し ます。ここでプロキシーボートを設定し た場合でも、コンピューター側のブラウ ザーにもプロキシー設定をおこなってく ださい。
ID			キーワードを新規に追加する場合は「新 規追加」、既存のキーワードを削除する 場合は該当のキーワードを選択します。
キーワード			URL フィルターに指定するキーワードを 入力します。半角英数字で 15 文字以内 で入力してください。
「追加」ボタン			ID ドロップダウンリストで「新規追加」 を選択した場合にアクティブになりま す。キーワードを追加登録します。10 件までのキーワードを追加することがで きます。ボタンをクリックすると設定内 容が即時に反映されます。
「削除」ボタン			ID ドロップダウンリストで既存のキー ワードを選択した場合にアクティブにな ります。選択したキーワードを削除しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができま す。

# 5.6.6.2 現在のフィルター設定

現在設定されている URL フィルターが一覧表示されます。

パラメーター	説明
ID	キーワードの ID 番号が表示されます。
キーワード	指定されているキーワードが表示されま す。
「えんぴつ」アイコン	クリックすると「現在の URL フィル ター設定」の該当キーワードの設定内容 を変更することができます。
「ごみ箱」アイコン	クリックすると「現在の URL フィル ター設定」から該当キーワードを削除し ます。

# 5.7 DoS アタックプロテクトの設定

DoS アタックとは、ネットワークのルーターなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大 させて相手のネットワークを麻痺させる攻撃です。本製品には、有効/無効を設定できる DoS アタックプロテクトと、無 条件に有効に設定されたプロテクトがあります。DoS アタックプロテクトの設定は「DoS」ページで行います。



無条件に設定されたプロテクトについては、プロテクトを無効にすることはできません。

### 5.7.1 デフォルト設定

本製品では、「SYN Flooding」、「ICMP Verbose」に対してプロテクトが有効に設定されています。

### 5.7.2 DoS アタックプロテクトの有効 / 無効

DoS アタックプロテクトを有効/無効にするには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「DoS」の順にクリックします。

アドレス(D) 🍓 http://192.168.1.1/index.html			15	🖌 🄁 移動
VPN Router			Allie	ed Telesis
		DoSアタッ	クフィルター設定	
	SYN Flooding			
	Winnuke			
	MIME Flood			
CentreCOM AR260S	FTP Bounce			
- セットアップウィザード	IP Unaligned Time-stamp			
────────────────────────────────────	Sequence Number Prediction Check			
	Sequence Number Out-of-range Check			
● 固定のにワジュアンド	ICMP Verbose			
🖻 🔄 WAN	Max IP Fragment Count	45		
WAN 经計售報	Minimum IP Fragment Size	512		
ー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・				
□ □ ファイアウォール		(	四用	
- Inboundアクセス - Outhoundアクセス				
□ □ □ アドバンスト設定		DoSアダッ	クフロテクトリスト	
ー ー セルフアクセス	IP Reassembly Attacks:	Bonk, Boink, Teard	rop(New Tear), Overdrop, Opentear, Syndrop, Jolt	
	ICMP Attacks:	Ping of Death, Smu	rf, Twinge	
	Flooders:	ICMP Flooder, UDP	Flooder	
	Port Scans:	TCP XMAS Scan, T	CP Null Scan, TCP SYN Scan, TCP Stealth Scan	
	Protection with PF Rules: Echo-Chargen, Ascend Kill			
	Miscellaneous Attacks:	IP Spoofing, LAND.	Targa, Tentacle	

 プロテクトを有効にする DoS アタックにチェックを入れ「適用」ボタンをクリックします。ここでは、「SYN Flooding」、 「Winnuke」、「ICMP Verbose」に対するプロテクトを有効にするものとします。

	DoSアタックフィルター設定
SYN Flooding	
Winnuke	
MIME Flood	
FTP Bounce	
IP Unaligned Time-stamp	
Sequence Number Prediction Check	
Sequence Number Out-of-range Check	
ICMP Verbose	
Max IP Fragment Count	45
Minimum IP Fragment Size	512

3.以上で設定は完了です。

### 5.7.3 DoS アタックプロテクトリストの確認

無条件にプロテクトを有効に設定されたアタックのリストを確認するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「DoS」の順にクリックします。

2. 「DoS アタックプロテクトリスト」に無条件に有効な DoS アタックプロテクトの一覧が表示されます。

		DoSアタックブロテクトリスト
	IP Reassembly Attacks:	Bonk, Boink, Teardrop(New Tear), Overdrop, Opentear, Syndrop, Jolt
	ICMP Attacks:	Ping of Death, Smurf, Twinge
13-	Flooders:	ICMP Flooder, UDP Flooder
	Port Scans:	TCP XMAS Scan, TCP Null Scan, TCP SYN Scan, TCP Stealth Scan
	Protection with PF Rules:	Echo-Chargen, Ascend Kill
	Miscellaneous Attacks:	IP Spoofing, LAND, Targa, Tentacle

# 5.7.4 「DoS」ページの解説

「DoS」ページについて解説します。「DoS」ページでは、DoS アタックに対するプロテクトの有効/無効を設定します。

# 5.7.4.1 DoS アタックフィルター設定

メニューから「ファイアウォール」->「アドバンスト設定」->「DoS」の順にクリックすると以下の画面が表示されます。

	DoSアタックフィル	ター設定
SYN Flooding		
Winnuke		
MIME Flood		
FTP Bounce		
IP Unaligned Time-stamp		
Sequence Number Prediction Check		
Sequence Number Out-of-range Check		
ICMP Verbose		
Max IP Fragment Count	45	
Minimum IP Fragment Size	512	
	適用	
パラメーター		説明
SYN Flooding		SYN Flooding に対するプロテクトを有効 にする場合はチェックを入れます。デ フォルトは有効です。
Winnuke		Winnuke に対するプロテクトを有効にす る場合はチェックを入れます。デフォル トは無効です。
MIME Flood		MIME Flood に対するプロテクトを有効に する場合はチェックを入れます。デフォ ルトは無効です。
FTP Bounce		FTP Bounce に対するプロテクトを有効 にする場合はチェックを入れます。デ フォルトは無効です。
P Unaligned Time-stamp		IP Unaligned Time-stamp に対するプロテ クトを有効にする場合はチェックを入れ ます。デフォルトは無効です。
Sequence Number Prediction Check		Sequence Number Prediction Check に対 するプロテクトを有効にする場合は チェックを入れます。デフォルトは無効 です。
Sequence Number Out of Range Check		Sequence Number Out of Range Check に 対するプロテクトを有効にする場合は チェックを入れます。デフォルトは無効 です。
CMP Verbose		ICMP Verbose に対するプロテクトを有 効にする場合はチェックを入れます。デ フォルトは有効です。
IAX IP Fragment Count		ファイアウォールを通過させるパケット のフラグメントサイズの最大しきい値を 入力します。PPPoE で接続している場合 には必ず入力してください。0 ~ 90 の

	範囲で入力してください。デフォルトは 45 です。
Minimum IP Fragment Size	ファイアウォールを通過させるパケット のフラグメントサイズの最小しきい値を 入力します。1 ~ 65534 の範囲で入力し てください。デフォルトは 512 です。
「適用」ボタン	設定した内容を本製品の設定に適用しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

### 5.7.4.2 DoS アタックプロテクトリスト

本製品でプロテクトが有効になっているアタックが一覧表示されます。DoS アタックフィルター設定テーブルで設定した内容は 反映されません。

	DoSアダックフロテクトリスト		
IP Reassembly Attacks:	Bonk, Boink, Teardrop(New Tear), Overdrop, Opentear, Syndrop, Jolt		
ICMP Attacks:	Ping of Death, Smurf, Twinge		
Flooders:	ICMP Flooder, UDP Flooder		
Port Scans:	TCP XMAS Scan, TCP Null Scan, TCP SYN	Scan, TCP Stealth Scan	
Protection with PF Rules:	Echo-Chargen, Ascend Kill		
Miscellaneous Attacks:	IP Spoofing, LAND, Targa, Tentacle		
パラメーター		説明	
IP Reassembly Attacks		本製品でプロテクトが有効になっている IP Reassembly Attack の一覧が表示され ます。	
ICMP Attacks		本製品でプロテクトが有効になっている ICMP Attack の一覧が表示されます。	
Flooders		本製品でプロテクトが有効になっている Flooder の一覧が表示されます。	
Port Scans		本製品でプロテクトが有効になっている Port Scan の一覧が表示されます。	
Protection with PF Rules		本製品でプロテクトが有効になっている Protection with PF Rule の一覧が表示され ます。	
Miscellaneous Attacks		本製品でプロテクトが有効になっている Miscellaneous Attack の一覧が表示されま す。	

# 5.8 トラフィックの確認

本製品では、ファイアウォールの統計を「統計情報」ページで一覧表示できます。

### 5.8.1 確認

統計情報を確認するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「統計情報」の順にクリックします。

ドレス(D) 🍓 http://192.168.1.1/index.html								🖌 🄁 移
PN Router	<u>`</u>					2	1 <b>729</b> A	llied Teles
				Active Connecti	ions			
	Source Network	k Protoco	I Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
	LAN	TCP	192.168.1.200 - 1	132 192.168.1.1 - 49200	0.0.0.0 - 0	12	0	0
	LAN	TCP	192.168.1.200 - 1	141 192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
CentreCOM AR260S				Total Compositions	Count			
システム情報				Total Connections	Count			
LAN		ICP		UDP	ICMP		Others	
		2		U	U		U	
				更新				
自定のにアンチアンド								
WAN								
- 🗎 WAN								
ルーティング								
アドバンスト設定								
統計情報								
VPN ()								
■ VPN接続								

2. ファイアウォールの統計情報が一覧表示されます。「更新」ボタンをクリックすると、表示内容を更新することができます。

			Active Connecti				
Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	TCP	192.168.1.200 - 1213	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
LAN	TCP	192.168.1.200 - 1212	192.168.1.1 - 80	0.0.0.0 - 0	20	0	0
			Total Connections	Count			
	TCP	U	IDP	ICMP		Others	
	2		0	0		0	
			「東新				

# 5.8.2 「統計情報」ページの解説

「統計情報」ページについて解説します。「統計情報」ページでは、ファイアウォールに関する統計情報を参照できます。

# 5.8.2.1 Active Connections

ファイアウォールを経由したセッションに関する情報が一覧表示されます。

				Active Connecti	ons				
	Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In	
	LAN	UDP	192.168.1.10 - 1029	192.168.1.1 - 53	0.0.0.0 - 0	48	0	0	
	LAN	UDP	192.168.1.10 - 1027	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0	
	LAN	TCP	192.168.1.10 - 1328	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0	
	Local	UDP	192.168.2.1 - 520	224.0.0.9 - 520	0.0.0.0 - 0	36	0	0	
	Local	UDP	192.168.1.1 - 520	224.0.0.9 - 520	0.0.0.0 - 0	36	0	0	
パラ	メーター					説明			
Souce Network						送信元のネ	・ットワ-	- クが表示	されます。
Prot	ocol					通信プロトコルが表示されます。			
Sour	rce IP-Po	rt				送信元の II 示されます	Pアドレ. -₀	スとポート	、番号が表
Dest	ination IP	-Port				宛先の IP つ されます。	アドレス	とポート者	<b>昏</b> 号が表示
NAT	IP-Port					NAT が使用 IP アドレス す。	目されたは くとポート	昜合、変換 ト番号が表	後の NAT 示されま
Life(	Secs)					セッション で表示され	vが切れる Lます。	るまでの時	間が秒単
Byte	s Out					送信元から バイト数か	宛先へ車 「表示され	云送された ぃます。	パケット(
Byte	es In					宛先から送 バイト数か	信元へ 転示され	⊼送された ヽます。	パケット(

### 5.8.2.2 Total Connections Count

現在通信中のセッション数が一覧表示されます。



UDP	UDP を使用したセッション数が表示され ます。
ICMP	ICMP を使用したセッション数が表示さ れます。
Others	TCP/UDP/ICMP 以外のプロトコルを使 用したセッション数が表示されます。
「更新」ボタン	クリックすると表示内容を更新します。

# 6 各種ポリシーとサービスの設定

# 6.1 概要

本製品では、ファイアウォールのInbound/Outbound アクセスルールを作成する際の送信元、宛先、宛先ポート、NAT パラメー ターに、あらかじめ作成したポリシー(IP プール、NAT プール)やサービスを指定することができます。ファイアウォールの 設定内容によっては、パラメーターに指定するポリシーやサービスをあらかじめ作成しておくことで設定を容易にすることが できます。本章では、以下のポリシーとサービスの設定について説明します。

- · IPプール
- ・ NAT プール
- ・ サービス

# 6.2 IP プールの設定

IP プールは、複数の IP アドレスをプール (グループ) として命名し、ファイアウォール設定時のパラメーター指定を容易にするものです。ファイアウォール (Inbound/Outbound アクセス)の設定で、送信元または宛先パラメーターに使用 します。IP プールの設定は「IP プール」ページで行います。

### 6.2.1 IP プールの追加

IP プールを追加するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。

アドレス(D) 🕘 http://192.168.1.1/index.html				🔺 🄁 移動
VPN Router				Allied Telesis
			IPブール設定	
	ブールの新規追加 🖌			
1	ブール名			
	種類	範	囲指定 🔽	
CentreCOM AR260S	始点IPアドレス			
	終点IPアドレス			
			追加 変更 削除	(ヘルプ)
ー ルーティング ローコファイアウォール				
- Inboundアクセス			IPブールリスト	
	ブール名	種類	始点/サブネットIPアドレス	終点/サブネットIPアドレス

2. ドロップダウンリストから「プールの新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のように IP プールを設定するものとします。

プール名	group1
	範囲指定
始点 IP アドレス	192.168.1.10
終点 IP アドレス	192.168.1.20

	IPブール設定
ブールの新規追加 🔽	
ブール名	group1
種類	範囲指定 🗸
始点IPアドレス	192.168.1.10
終点IPアドレス	192.168.1.20
	道加、変更)削除

4. 以上で設定は完了です。

#### 6.2.2 IP プールの変更

### IP プールを変更するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。

- ドロップダウンリストから変更する IP プールを選択します。または、「IP プールリスト」テーブルの該当プール左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

#### 6.2.3 IP プールの削除

IP プールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。

2. ドロップダウンリストから削除する IP プールを選択し、「削除」ボタンをクリックします。または、「IP プールリスト」テーブルの該当プール左部にある「ごみ箱」アイコンをクリックします。

3. 以上で設定は完了です。

# 6.2.4 IP プールの確認

### IP プールを確認するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。

2.「IP プールリスト」テーブルに IP プールが一覧表示されます。

			IPブールリスト	
<b>±</b>	ブール名 group1	<b>種類</b> 範囲指定	<mark>始点/サブネットIPアドレス</mark> 192.168.1.10	<mark>終点/サブネットIPアドレス</mark> 192.168.1.20

#### 6. 2. 5 「IP プール」ページの解説

「IP プール」ページについて解説します。「IP プール」ページでは、IP プールを定義します。定義した IP プールは、 Inbound/Outbound アクセスルールを設定する場合に使用します。

# 6.2.5.1 IP プール設定

\_\_\_\_\_

IP プールを定義するテーブルです。メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリック すると以下の画面が表示されます。

		IPC	ラール設定	
ブールの新規追加	<b>~</b>			
ブール名				
種類		範囲指定 🗸		
始点IPアドレス				
終点IPアドレス				
		〔追加〕	(	
パラメーター	オプション			説明
ドロップダウンリス	<			IP プールを新規に追加する場合は「プー ルの新規追加」、既存の IP プールを変更 / 削除する場合は該当プールを選択しま す。
プール名				プール名を入力します。半角英数字で 15 文字以内で入力してください。
種類				プールの種類を選択します。
	範囲指定			IP アドレスの範囲を指定して IP プール を定義する場合に選択します。
			始点 IP アドレス	種類パラメーターに「範囲指定」を選択 した場合にのみ表示されます。範囲を指 定する IP アドレスの始点 IP アドレスを 入力します。
			終点 IP アドレス	種類パラメーターに「範囲指定」を選択 した場合にのみ表示されます。範囲を指 定する IP アドレスの終点 IP アドレスを 入力します。
	サブネット			サブネットを指定して IP プールを定義 する場合に選択します。
			サブネットアドレス	種類パラメーターに「サブネット」を選 択した場合にのみ表示されます。IP プー ルに指定するサブネットのサブネットア ドレスを入力します。
			サブネットマスク	種類パラメーターに「サブネット」を選 択した場合にのみ表示されます。P プー ルに指定するサブネットのサブネットマ スクを入力します。
	IP アドレス			IP アドレスを指定して IP プールを定義 する場合に選択します。

	ゆ アドレス	種類パラメーターに「IP アドレス」を選 択した場合にのみ表示されます。IP プー ルに指定する IP アドレスを入力します。
「追加」ボタン		ドロップダウンリストで「プールの新規 追加」を選択した場合にアクティブにな ります。IP プールを追加登録します。50 件までのプールを追加することができま す。ボタンをクリックすると設定内容が 即時に反映されます。
「変更」ボタン		ドロップダウンリストで既存の IP プー ルを選択した場合にアクティブになりま す。設定内容の変更を保存します。ボタ ンをクリックすると設定内容が即時に反 映されます。
「削除」ボタン		ドロップダウンリストで既存の IP プー ルを選択した場合にアクティブになりま す。選択した IP プールを削除します。 ボタンをクリックすると設定内容が即時 に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

# 6.2.5.2 IP プールリスト

設定された IP プールが一覧表示されます。

			IPブールリスト	
	ブール名	種類	始点/サブネットIPアドレス	終点/サブネットIPアドレス
ø	group1	範囲指定	192.168.1.10	192.168.1.20

パラメーター	説明
プール名	IP プール名が表示されます。
▲ 種類	IP プールの種類 (IP アドレス / 範囲指定 / サブネット ) が表示されます。
始点 / サブネット IP アドレス	IP プールの種類が範囲指定の場合は始点 IP アドレス、サブネットの場合はサブ ネットアドレス、IP アドレスの場合は IP アドレスが表示されます。
終点 / サブネット IP アドレス	IP プールの種類が範囲指定の場合は終点 IP アドレス、サブネットの場合はサブ ネットアドレスが表示されます。種類が IP アドレスの場合は何も表示されませ ん。
「えんぴつ」アイコン	クリックすると「IP プールリスト」の該 当プールの設定内容を変更することがで きます。
「ごみ箱」アイコン	クリックすると「IP プールリスト」から 該当プールを削除します。

# 6.3 NAT プールの設定

NAT プールは、NAT タイプを指定して NAT を定義し、ファイアウォールポリシー(Inbound/Outbound アクセス)作成時に 使用するための NAT のグループです。Inbound アクセスでは、スタティック / ダイナミック NAT、ENAT, インターフェー ス NAT、Outbound アクセスではスタティック / ダイナミック NAT、ENAT をポリシーに設定する場合は、あらかじめ NAT プールを作成する必要があります。NAT プールの設定は「NAT プール」ページで行います。本製品で設定できる NAT プー ルは以下のとおりです。

- ・ スタティック NAT プール
- ・ ダイナミック NAT プール
- ・ ENAT プール
- ・ インターフェース NAT プール

### 6.3.1 NAT プールの追加

#### NAT プールを追加するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。

VPN Router				Allied Tele
S COMPANY		NA	プール設定	
	ブールの新規追加 🐱			
	ブール名			
	ブールタイプ	スタティックNAT 🔹	•	
CentreCOM AR260S		始点IPアドレス		
セットアップウィザード システム情報	変換前のIPアドレス	終点IPアドレス		
		始点NAT IPアドレス	2	
■ ルーティング コーイスウィール	NAT IPアドレス	終点NAT IPアドレン	2	
		〔追加	変更)削除	(ヘルプ)
□ - □ アドハンスト設定 □ - □ ポリシーリスト		NA	エブールリスト	
IPナール NATISール	ブール名	NATタイプ NAT IPアドレス	インターフェース	範囲指定 NAT範囲指定
— □ 統計情報 — VPN	🖋 💼 sta	スタティック NAT		192.168.10.20 - 192.168.20.20 - 192.168.10.26 192.168.20.26
<ul> <li>ログ</li> <li>システム管理</li> </ul>	🖋 📅 dyn	ダイナミック NAT		192.168.10.30 - 192.168.20.30 - 192.168.10.32 192.168.20.30
■ 再起動 ■ ログアウト	🖋 💼 enat	ENAT 192.168.20.50		
	🖋 💼 int	インターフェ ースNAT	eth0	

2. ドロップダウンリストから「プールの新規追加」を選択します。

3. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のように NAT プールを設定するものとします。

プール名	enat1
プールタイプ	ENAT
NAT IP アドレス	1.1.1.1

ブールの新規追加 🖌	
ブール名	enat1
プールタイプ	ENAT
NAT IPアドレス	1.1.1.1

4. 以上で設定は完了です。

# 6.3.2 NAT プールの変更

NAT プールを変更するには以下の手順を実行します。

- 1.メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。
- ドロップダウンリストから変更する NAT プールを選択します。または、「NAT プールリスト」テーブルの該当プール左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

### 6.3.3 NAT プールの削除

NAT プールを削除するには以下の手順を実行します。

- 1.メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。
- ドロップダウンリストから削除する NAT プールを選択し、「削除」ボタンをクリックします。または、「NAT プールリスト」 テーブルの該当プール左部にある「ごみ箱」アイコンをクリックします。

3. 以上で設定は完了です。

# 6.3.4 NAT プールの確認

### NAT プールを確認するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。

2.「NAT プールリスト」テーブルに NAT プールが一覧表示されます。

	NATブールリスト						
		ブール名	NATタイプ NAT IPアドレス	インターフェース	範囲指定	NAT範囲指定	
s	<b></b>	enat1	ENAT 1.1.1.1				
ø	Ē	static	スタティック NAT		192.168.1.10 - 192.168.1.12	200.100.10.10 - 200.100.10.12	
s/P	<b></b>	dynamic	ダイナミック NAT		192.168.1.20 - 192.168.1.40	200.100.1.20 - 200.100.1.30	
e/P	<b></b>	int	インターフェ ースNAT	eth0			

### 6.3.5 「NAT プール」ページの解説

「NAT プール」ページについて解説します。「NAT プール」ページでは、NAT プールを定義します。定義した NAT プールは、 Inbound/Outbound アクセスルールを設定する場合に使用します。

# 6.3.5.1 NAT プール設定

NAT プールを設定するテーブルです。メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックすると以下の画面が表示されます。

	NATブール設定	
ブールの新規追加 🔽		
ブール名		
ブールタイプ	スタティックNAT 🗸	
- 赤橋会へのつい コー	始点IPアドレス	
変換的のPアトレス	終点IPアドレス	
	始点NAT IPアドレス	
NATIPYEDX	終点NAT IPアドレス	
	追加 変更 削除	
パラメーター オブ	ジョン	説明
<sup>、</sup> ロップダウンリスト		NAT プールを新規に追加する場合は 「プールの新規追加」、既存のプールを変 更 / 削除する場合は該当プールを選択し ます。
パール名		プール名を入力します。半角英数字で 15 文字以内で入力してください。
パールタイプ		NAT プールの指定方法を選択します。
 スタ	ティック NAT	プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で変換する場合に選 択します。ポート変換は行いません。1 対 1 で変換するため、グローバル IP ア ドレスはプライベート IP アドレスと同 じ数にしてください。

_	ダイナミック NAT	複数のプライベート IP アドレスを、複数のグローバル IP アドレスに変換する 場合に選択します。ポート変換は行いま せん。動的に変換するため、グローバル IP アドレスはプライベート IP アドレス の数と同じである必要はありませんが、 変換時に使用可能なグローバル IP アド レスがない場合にはパケットは破棄され ます。
	ENAT	NAPT とも呼ばれます。複数のプライ ベート IP アドレスを、ポートを変換し て 1 つのグローバル IP アドレスに変換 する場合に選択します。
	インターフェース NAT	複数のプライベート IP アドレスを、 ポートを変換して、WAN 側インター フェースのグローバル IP アドレスに変 換する場合に選択します。
変換前の IP アドレ <i>ス</i>	ζ	プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。プライベート IP ア ドレスを指定します。
-	始点 IP アドレス	プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。スタティック NAT/ ダイナミック NAT に指定する始点 IP ア ドレスを入力します。
	終点 IP アドレス	プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。スタティック NAT/ ダイナミック NAT に指定する終点 IP ア ドレスを入力します。
NAT IP アドレス		プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。グローバル IP アド レスを指定します。
-	始点 NAT IP アドレス	プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。スタティック NAT/ ダイナミック NAT に指定する始点 NAT IP アドレスを入力します。
	終点 NAT IP アドレス	プールタイプに「スタティック NAT」、 「ダイナミック NAT」を選択した場合に のみ表示されます。スタティック NAT/ ダイナミック NAT に指定する終点 NAT IP アドレスを入力します。
NAT IP アドレス		ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
NAT インターフェー	-ス	プールタイプに「インターフェース NAT」を選択した場合にのみ表示されま す。インターフェース NAT に指定する インターフェースを eth0/pppoe0/pppoe1 から選択します。

「追加」ボタン	ドロップダウンリストで「プールの新規 追加」を選択した場合にアクティブにな ります。IP プールを追加登録します。31 件までのプールを追加することができま す。ボタンをクリックすると設定内容が 即時に反映されます。
「変更」ボタン	ドロップダウンリストで既存の NAT プールを選択した場合にアクティブにな ります。設定内容の変更を保存します。 ボタンをクリックすると設定内容が即時 に反映されます。
「削除」ボタン	ドロップダウンリストで既存の NAT プールを選択した場合にアクティブにな ります。選択した NAT プールを削除し ます。ボタンをクリックすると設定内容 が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

# 6.3.5.2 NAT プールリスト

設定した NAT プールが一覧表示されます。

				NATO	ノールリスト		
		ブール名	NATタイプ NAT IF	アドレス	インターフェース	範囲指定	NAT範囲指定
I	Ē	enat1	ENAT 1.1.1.1				
I		static	スタティック NAT			192.168.1.10 -	200.100.10.10 -
			ダイナミック			192,168,1,20 -	200.100.10.12
6	Ш	dynamic	NAT			192.168.1.40	200.100.1.30
ø	Ē	int	インターフェ ースNAT		eth0		
パラメ	-9-					説明	1
パール	名					プー	-ル名が表示されます。
IAT タ	イプ					NAT	- プールの種類が表示されます
IAT IP	アドレ	レス				NAT ドレ	「タイプが ENAT の場合に NA <sup>-</sup> シスが表示されます。
インタ	ーフェ	ニース				イン され す。	ッターフェース NAT の場合に、 いたインターフェースが表示さ
<b>范囲指</b>	定					スタ 合に スの	『ティック / ダイナミック NAT こ、指定したプライベート IP つ 〕範囲が表示されます。
IAT 範	囲指定	2				ス ら 合に の 範	マティック / ダイナミック NAT 、指定したグローバル IP アト 随 が表示されます。

# 6.4 サービスの設定

サービスは、特定ポートを使用するアプリケーションです。ファイアウォールを設定する場合に宛先ポートパラメーター でサービスを選択する場合に使用します。本製品に既に登録されているサービス以外のサービスを指定する場合に、 「サービス」ページで新たにサービスを定義して追加することができます。

### 6.4.1 サービスの作成

#### サービスを作成するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」の順にクリックします。

PN Router				Allied T
			サービス設定	
	新規追	ta 🗸		
	サービ			
	15-511-5			
	1205	/2/w=r		
ntreCOM AR260S	フロトコ	UL	TCP 💌	
セットアップウィザード			追加 変更 詳	川除し、「ヘルス
ンスリム mista IAN				
WAN			サービフリフト	
ルーティング		サービフタ		パブリックポート
ファイアワオール	<i>A</i> 5			00 00
Outboundアクセス	-		LIDD	20
URLフィルター	-		TOP	101
アドバンスト設定	-		ICP	20
セルフアクセス	<i>•</i>		TOP	3050
	-		TOP	1010
□ ポリシーリスト	-	□ RISPU04	I CP	004
📄 統計情報	-		UDP	27010
VPN			UDP	27910
ロクシステム管理			TOP	1723
再起動			TCP	110
	1	PC-ANYWHERE	UDP	22
ログアウト		The Address of the Ad	TOD	110
ロ <b>グアウト</b>	1	MNTP	TCP	119

### 2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のように設定するものとします。

サービス名	service1
パブリックポート	1080
プロトコル	TCP

	サービス設定			
新規追加 💙				
サービス名	service1			
パブリックポート	1080			
プロトコル	TCP 🗸			
追加 変更 削除 ヘルプ				

3. 以上で設定は完了です。

### 6.4.2 サービスの変更

#### サービスを変更するには以下の手順を実行します。

- 1. メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」の順にクリックします。
- 2. ドロップダウンリストから変更するサービスを選択します。または、「サービスリスト」テーブルの該当サービス左部にある 「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

#### 6.4.3 サービスの削除

#### サービスを削除するには以下の手順を実行します。

- 1.メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」の順にクリックします。
- 2. ドロップダウンリストから削除するサービスを選択し、「削除」ボタンをクリックします。または、「サービスリスト」テーブ ルの該当サービス左部にある「ごみ箱」アイコンをクリックします。

3.以上で設定は完了です。

### 6.4.4 サービスの確認

### サービスを確認するには以下の手順を実行します。

1.メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」の順にクリックします。

2.「サービスリスト」テーブルにサービスが一覧表示されます。

		サービス名	プロトコル	バブリックボート
5.A	Ē	TELNET	TCP	23
<b>6</b>	Ē	SNMP	UDP	161
e de la companya de l	Ē	SMTP	TCP	25
6.	Ē	SIP	UDP	5060
di kana kana kana kana kana kana kana kan	Ē	RTSP7070	TCP	7070
5.00	Ē	RTSP554	TCP	554
a de la calegaria de la calega	Ē	RPC	UDP	111
e de la calegaria de la calega	Ē	QUAKE-II	UDP	27910
set i	÷.	PPTP	TCP	1723
ø	Ē	POP3	TCP	110
ø	Ē	PC-ANYWHERE	UDP	22
6	Ē	NNTP	TCP	119
al an	Ē	N2P	UDP	6801
6 <sup>10</sup>	tin and a second	MSN-ZONE	TCP	28801
ø	Ē	MSN	TCP	1863
e de la companya de l	$\Box$	MSG2	UDP	47624
sa the second se	Ē	MSG1	TCP	47624
<b>6</b> 29	Ē	L2TP	UDP	1701
Sentir Contraction	Ī	IRC	TCP	6667
sa the second	Ē	IMAP4	TCP	143
e de la companya de l	Ē	ILS	TCP	389
6.0	Ē	IKE	UDP	500
di kana kana kana kana kana kana kana kan	Ē	ICQ-2002	TCP	5190
6 <b>-</b> 2		ICQ-2000	TCP	5191
e de la companya de la company	Ē	HTTPS	TCP	443
6 <b>1</b> 9		HTTP	TCP	80
5.00	Ē	H323GK	UDP	1719
6 <b>1</b> 9	Ē	H323	TCP	1720
e de la compañía de la	Ē	FTP	TCP	21
5.00	Ē	FINGER	TCP	79
<i>.</i>		DNS	UDP	53
6 M	Ē	DIABLO-II	TCP	4000
4	Ē	CUSEEME	TCP	7648
e de la compañía de la compa		BATTLE-NET-UDP	UDP	6112
6	Ē	BATTLE-NET-TCP	TCP	6112
ø	Ē	AOL	TCP	5190

### 6.4.5 「サービス」ページの解説

「サービス」ページについて解説します。「サービス」ページでは、既存のサービスの変更 / 削除、サービスの新規登録を 行います。

### 6.4.5.1 サービス設定

メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」の順にクリックすると以下の画面が表示されます。

サービッシウ	^
5 - □ ス 100 上 新規追加 ◆	
サービス名	
パブリックポート	
プロトコル TCP 🗸	
追加 変更 削除	
バラメーター	説明
ドロップダウンリスト	サービスを新規に追加する場合は「新規 追加」、既存のサービスを変更 / 削除す る場合は、該当サービスを選択します。
サービス名	サービス名を入力します。半角英数字で 15 文字以内で入力します。
パブリックポート	サービスで使用するポートの番号を入力 します。
プロトコル	サービスで使用するプロトコルを選択し ます。
「追加」ボタン	ドロップダウンリストで「新規追加」を 選択した場合にアクティブになります。 サービスを追加登録します。50件まで のサービスを追加することができます。 ボタンをクリックすると設定内容が即時 に反映されます。
「変更」ボタン	ドロップダウンリストで既存のサービス を選択した場合にアクティブになりま す。設定内容の変更を保存します。ボタ ンをクリックすると設定内容が即時に反 映されます。
 「削除」ボタン	ドロップダウンリストで既存のサービス を選択した場合にアクティブになりま す。選択したサービスを削除します。ボ タンをクリックすると設定内容が即時に 反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができま す。

# 6.4.5.2 サービスリスト

現在設定されているサービスが一覧表示されます。

サービスリスト					
		サービス名	プロトコル	バブリックボート	
6 <b>-</b> 2		TELNET	TCP	23	
ø	Ē	SNMP	UDP	161	
ø	Ē	SMTP	TCP	25	
ø	Ē	SIP	UDP	5060	
ø	Ē	RTSP7070	TCP	7070	
5-12	Ē	RTSP554	TCP	554	
ø	Ē	RPC	UDP	111	
e de la calegaria de la calega	Ē	QUAKE-II	UDP	27910	
ø	Ξ.	PPTP	TCP	1723	
Ø	Ē	POP3	TCP	110	
ø	Ē	PC-ANYWHERE	UDP	22	
sa the second se	Ē	NNTP	TCP	119	
d de la companya de l		N2P	UDP	6801	
set.	Ē	MSN-ZONE	TCP	28801	
di kana kana kana kana kana kana kana kan	Ē	MSN	TCP	1863	
ø	Ē	MSG2	UDP	47624	
6	Ē	MSG1	TCP	47624	
ø	Ē	L2TP	UDP	1701	
set.	Ī	IRC	TCP	6667	
6.1	Ē	IMAP4	TCP	143	
ø	Ē	ILS	TCP	389	
6	Ē	IKE	UDP	500	
ø	Ē	ICQ-2002	TCP	5190	
6 <sup>2</sup>		ICQ-2000	TCP	5191	
s de la constante de la consta	Ē	HTTPS	TCP	443	
6.19	Ē	HTTP	TCP	80	
5.	Ē	H323GK	UDP	1719	
ø	Ē	H323	TCP	1720	
6	Ē	FTP	TCP	21	
6		FINGER	TCP	79	
<b>1</b> 2		DNS	UDP	53	
6 M	Ē	DIABLO-II	TCP	4000	
<i>6</i>	Ē	CUSEEME	TCP	7648	
e de la companya de la compa	Ē	BATTLE-NET-UDP	UDP	6112	
6	Ē	BATTLE-NET-TCP	TCP	6112	
ø	Ē	AOL	TCP	5190	

パラメーター	説明
サービス名	サービス名が表示されます。
プロトコル	サービスで使用されるプロトコルが表示 されます。
パブリックポート	サービスで使用されるポートの番号が表 示されます。
「えんぴつ」アイコン	クリックすると「サービスリスト」の該 当サービスの設定内容を変更することが できます。
「ごみ箱」アイコン	クリックすると「サービスリスト」から 該当サービスを削除します。
# 7 VPN の設定

# 7.1 概要

VPN (Virtual Private Network) は、ネットワーク間に仮想的なトンネルを構築し、パケットを暗号化して通信を行い、ネットワーク間の通信のセキュリティーを低コストで実現する機能です。本製品の VPN は IPSec (IP Security) に準拠していま す。IPSec とは、IP に暗号化や認証などのセキュリティー機能を付加する一連のプロトコル群です。本製品では「VPN 接続」 ページで VPN を構築することができます。

# 7.2 VPNの設定

VPN トンネルでネットワーク間を接続するなど、VPN ゲートウェイ間で接続する場合に使用します。

# 7.2.1 ポリシーの作成

ポリシーを作成するには以下の手順を実行します。

ここでは、下図のようなネットワーク構成でルーター A のポリシーを作成するものとします。



】 ポリシーを作成する前に、あらかじめ VPN サービスを有効にしておいてください。サービスを有効にする方法につい ・ ては「P.18 機能の有効化 / 無効化の設定」を参照してください。



1.メニューから「VPN」->「VPN 接続」の順にクリックします。

アドレス(D) 🥘 http://192.168.1.1/index.	html			
VPN Router				🗤 Allied Tele
		VPN接続設定		
	ID 新規追加 👻 ポリ	シー名	◎有効 ○無効	優先度 1 🗸
	VPN無通信監視	◎ 有効 ◎ 無効		
Contra COM AD2000	ローカルセキュアグループ	種類 全て 💌		
・ セットアップウィザード	リモート セキュアグループ	種類 全て ✔		
·Ⅲ システム情報 └── LAN	ローカルゲートウェイ	インターフェース eth0 💌		
□ WAN □ ルーティング	リモートゲートウェイ	種類 全て ✔		
ロファイアウォール		IKE設定		
VPN VPN複続	IKE交換モード	Main ○ Aggressive		
	事前共有鍵			
□ µク □ システム管理	IKE暗号化認証アルゴリズム	全て <b>マ</b>		
再起動	有効期限	3600 10 🗸		
		IPSec設定		
	IPSec暗号化認証アルゴリズム	全て	*	
	PFSグループ	未定義 🗸		
	有効期限	3600 秒 🖌 または 75000	KByte	
		追加变更		ヘルプ
		サイト間アクセスルー	JL	
	ID ポリシー名	ローカル/リモートネットワーク	トンネル終端 鍵管理方	式 IPSec 状況

2. ID ドロップダウンリストから「新規追加」を選択します。

<sup>3.</sup> 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のようにポリシーを設定するものとします。

ポリシー名		АТОВ
VPN		有効
優先度		1
VPN 無通信監視		有効
無通信時間		60 秒
ローカルセキュアグループ	種類	サブネット
	アドレス	192.168.1.0
	マスク	255.255.255.0
リモートセキュアグループ	種類	サブネット
	アドレス	192.168.2.0
	マスク	255.255.255.0
ローカルゲートウェイ	インターフェース	ррроеО
リモートゲートウェイ	種類	IP アドレス
	IPアドレス	2.2.2.2

## VPN 接続設定テーブル

I KE	设定
------	----

	Main
事前共有鍵	atobkey
	全て

#### IPSec 設定

IPSec 暗号化 / 認証アルゴリズム	全て
PFS グループ	DH-2
有効期限	3600 秒 /75000KByte

				Allied leles
		VPN接続設定		
ID 新規追加 🔽 ポリ	シー名 ATOB		⊙有効 ○無効	優先度 1 🗸
/PN無通信監視	<ul><li>●有効</li><li>無通信時間</li></ul>	○無効 60	秒	
コーカルセキュアグループ	種類 アドレス マスク	サブネット <b>マ</b> 192.168.1.0 255.255.255.0		
リモート セキュアグループ	種類 アドレス マスク	サブネット <b>マ</b> 192.168.2.0 255.255.255.0		
コーカルゲートウェイ	インターフェース	pppoe0 🗸		
リモートゲートウェイ	種類 IPアドレス	IPアドレス 💌 2.2.2.2		
		IKE設定		
KE交換モード	⊙ Main (	DAggressive		
事前共有鍵	•••••			
KE暗号化/認証アルゴリズム	全て	*		
有効期限	3600 秒	~		
		IPSec設定		
PSec暗号化/認証アルゴリズム	全て		~	
PFSグループ	DH-2 🗸			
有効期限	3600 秒	✓または 75000 KB	,⁄te	
	〕	なり 一変更 削除		「ヘルプ

ファイアウォールを有効にしている場合は、ファイアウォールで ISAKMP/IPSec のパケットが遮断されないように、以下の設定を含めた Outbound/Inbound アクセスのルールを追加します。Outbound/Inbound アクセスのルールの作成については「P.93 ファイアウォールの設定」を参照してください。

アクション		通過
送信元	タイプ	サブネット
	アドレス	192168.1.0
	マスク	255.255.255.0

Outbound アクセスのルール

宛先		タイプ	サブネット
		アドレス	192.168.2.0
		マスク	255.255.255.0
NAT			未定義
VPN			有効
Inbound アクセスの	)ルール		
アクション			通過
送信元		タイプ	サブネット
		アドレス	192.168.2.0
		マスク	255.255.255.0
宛先		タイプ	サブネット
		アドレス	192.168.1.0
		マスク	255.255.255.0
NAT			未定義
VPN			有効

5.以上で設定は完了です。

### 7.2.2 ポリシーの変更

ポリシーを変更するには以下の手順を実行します。

- 1.メニューから「VPN」->「VPN 接続」の順にクリックします。
- ID ドロップダウンリストから変更するポリシーを選択します。または、「サイト間アクセスルール」テーブルの該当ポリシー 左部にある「えんぴつ」アイコンをクリックします。
- 3. 各パラメーターを変更します。
- 4.「変更」ボタンをクリックします。
- 5.以上で設定は完了です。

## 7.2.3 ポリシーの削除

ポリシーを削除するには以下の手順を実行します。

- 1.メニューから「VPN」->「VPN 接続」の順にクリックします。
- 2. ID ドロップダウンリストから削除するポリシーの ID を選択し「削除」ボタンをクリックします。または、「サイト間アクセ スルール」テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。

3.以上で設定は完了です。

## 7.2.4 ポリシーの確認

1.メニューから「VPN」->「VPN 接続」の順にクリックします。

2.「サイト間アクセスルール」テーブルにポリシーが一覧表示されます。

				サイト間アクセスル	ール		
		ID	ポリシー名	ローカル/リモートネットワーク	トンネル終端	鍵管理方式	IPSec 状況
ı	Ē	1	ATOB	192.168.1.0/24 192.168.2.0/24	2.2.2.2	事前共有鍵	トンネ ル ル

### 7.2.5 「VPN 接続」ページの解説

「VPN 接続」ページについて解説します。

# 7.2.5.1 VPN 接続設定

メニューから「VPN」->「VPN 接続」の順にクリックすると以下の画面が表示されます。

	VPN接続設定	
ID 新規追加 🖌 ポリ	シー名	◎有効 ○無効 優先度 1 🖌
VPN無通信監視	◎有効 ◎無効	
ローカルセキュアグループ	種類 全て 🗸	
リモートセキュアグループ	種類 全て 🗸	
ローカルゲートウェイ	インターフェース eth0 💌	
リモートゲートウェイ	種類 全て 🗸	
	IKE設空	
パラメーター オプション		説明
ID		VPN 接続ポリシーを新規に追加する場 は「新規追加」、既存のポリシーを変! / 削除する場合は該当ポリシーの ID 覆 を選択します。
ポリシー名		ポリシー名を入力します。半角英数字 31 文字以内で入力してください。
有効 / 無効		ーーーーーーーーーーーーーーーーーーーーーーー 作成したポリシーを有効にする場合は 「有効」、無効にする場合は「無効」ラ オボタンを選択します。
優先度		ポリシーの優先度を選択します。数字 小さくなると優先度が高くなります。

			リシーが複数存在する場合、優先度が高 い順にパケットにマッチングされます。
VPN 無通信監視	有効 / 無効		VPN の通信が「無通信時間」で指定した 時間発生しなかった場合に、IPSec SA を 削除する機能です。VPN 無通信監視を有 効にする場合は「有効」、無効にする場 合は「無効」ラジオボタンを選択しま す。
		無通信時間	VPN 無通信監視で「有効」を選択した場 合にのみ表示されます。無通信時に IPSec SA を消去するまでの時間を 60 秒 ~ 600 秒の範囲で指定します。
ローカルセキュアク	゛ループ		VPN ポリシーを適用するローカルセキュ アグループの指定方法を選択します。
-	全て		LAN 側のすべてのコンピューターにポリ シーを適用する場合に選択します。
	IP アドレス		ポリシーを適用するコンピューターを IP アドレスで 1 台指定する場合に選択しま す。
		IP アドレス	ローカルセキュアグループの種類に「IP アドレス」を選択した場合にのみ表示さ れます。ポリシーを適用するコンピュー ターの IP アドレスを入力します。
	サブネット		ポリシーを適用するコンピューターをサ ブネットで指定する場合に選択します。
		アドレス	ローカルセキュアグループの種類に「サ ブネット」を選択した場合にのみ表示さ れます。ポリシーを適用するグループの サブネットアドレスを入力します。
		マスク	ローカルセキュアグループの種類に「サ ブネット」を選択した場合にのみ表示さ れます。ポリシーを適用するグループの サブネットマスクを入力します。
	範囲指定		ポリシーを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
		始点 IP アドレス	ローカルセキュアグループの種類に「範 囲指定」を選択した場合にのみ表示され ます。ポリシーを適用する IP アドレス の範囲の始点 IP アドレスを入力します。
-		終点 IP アドレス	ローカルセキュアグループの種類に「範 囲指定」を選択した場合にのみ表示され ます。ポリシーを適用する IP アドレス の範囲の終点 IP アドレスを入力します。

リモートセキュアグループ

VPN ポリシーを適用するリモートセキュ アグループの指定方法を選択します。

	全て		リモートのすべてのコンピューターにポ リシーを適用する場合に選択します。
	IP アドレス		ポリシーを適用するコンピューターを IP アドレスで 1 台指定する場合に選択しま す。
		IP アドレス	リモートセキュアグループの種類に IP アドレスを選択した場合にのみ表示され ます。ポリシーを適用するコンピュー ターの IP アドレスを入力します。
	サブネット		ポリシーを適用するコンピューターをサ ブネットで指定する場合に選択します。
		アドレス	リモートセキュアグループの種類に「サ ブネット」を選択した場合にのみ表示さ れます。ポリシーを適用するグループの サブネットアドレスを入力します。
		マスク	リモートセキュアグループの種類に「サ ブネット」を選択した場合にのみ表示さ れます。ポリシーを適用するグループの サブネットマスクを入力します。
	範囲指定		ポリシーを適用するコンピューターを IP アドレスの範囲で指定する場合に選択し ます。
		始点 IP アドレス	リモートセキュアグループの種類に「範 囲指定」を選択した場合にのみ表示され ます。ポリシーを適用する IP アドレス の範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	リモートセキュアグループの種類に「範 囲指定」を選択した場合にのみ表示され ます。ポリシーを適用する IP アドレス の範囲の終点 IP アドレスを入力します。
ローカルゲートウ:	۲. T		VPN 通信パケットを送受信するローカル のインターフェース(eth0/pppoe0/ pppoe1)をドロップダウンリストから選 択します。
リモートゲートウェ	r ٦		VPN ポリシーを適用するリモートゲート ウェイの指定方法を選択します。
	全て		VPN 接続のピアが AR260S の場合で、IP アドレスが固定されていない場合に選択 します。「全て」を選択した場合「ロー カル ID」と「リモート ID」を指定して ください。
	IPアドレス		リモートゲートウェイを IP アドレスで 指定する場合に選択します。
		IPアドレス	リモートゲートウェイの種類に「IP アド レス」を選択した場合にのみ表示されま す。リモートゲートウェイの IP アドレ スを入力します。

ローカル ID			ISAKMP フェーズ 1 でリモートゲート ウェイに送信する ID ペイロードの内容 を指定します。IKE 設定の「IKE 交換 モード」で「Aggressive」を選択した場 合にのみ表示されます。おもに、本製品 の IP アドレスが不定の場合に設定しま す。
	未定義		ID ペイロードの内容を指定しない場合に 選択します。「未定義」を選択した場合、 「リモートゲートウェイ」で指定した IP アドレスが ID ペイロードに使用されま す。
	IPアドレス		ID ペイロードの内容を IP アドレスで指 定する場合に選択します。
		IP アドレス	「ローカル ID」で「IP アドレス」を選択 した場合にのみ表示されます。ID ペイ ロードに指定する IP アドレスを入力し ます。
	FQDN		ID ペイロードの内容を FQDN(Fully Quali- fied Domain Name) で指定する場合に選択 します。
		FQDN	「ローカル ID」で「FQDN」を選択した場 合にのみ表示されます。ID ペイロードに 指定する FQDN を入力します。
	E-mail		ID ペイロードの内容を E-mail アドレス で指定する場合に選択します。
		E-mail	「ローカル ID」で「E-mail」を選択した 場合にのみ表示されます。ID ペイロード に指定する E-mail アドレスを入力しま す。
リモートロ			ISAKMP フェーズ 1 でリモートゲート ウェイから受信する ID ペイロードの内 容を指定します。IKE 設定の「IKE 交換 モード」で「Aggressive」を選択した場 合にのみ表示されます。おもに、リモー トゲートウェイの IP アドレスが不定の 場合に設定します。
	未定義		ID ペイロードの内容を指定しない場合に 選択します。「未定義」を選択した場合、 「リモートゲートウェイ」で指定した IP アドレスが ID ペイロードに使用されま す。
	IP アドレス		ID ペイロードの内容を IP アドレスで指 定する場合に選択します。
		₽ アドレス	「ローカル ID」で「IP アドレス」を選択 した場合にのみ表示されます。ID ペイ ロードに指定する IP アドレスを入力し ます。
	FQDN		ID ペイロードの内容を FQDN(Fully Quali- fied Domain Name) で指定する場合に選択 します。

	FQDN	「ローカル ID」で「FQDN」を選択した場 合にのみ表示されます。ID ペイロードに 指定する FQDN を入力します。
E-mail		ID ペイロードの内容を E-mail アドレス で指定する場合に選択します。
	E-mail	「ローカル ID」で「E-mail」を選択した 場合にのみ表示されます。ID ペイロード に指定する E-mail アドレスを入力しま す。

# 7.2.5.2 IKE 設定

奥生 日本主ノリキン		━━−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−	
		IKE設定	
IKE交換モー	-F	Main ○ Aggressive	
事前共有鍵			
IKE暗号化/	認証アルゴリズム	全て 🗸	
有効期限		3600 秒 💙	
		IBBao翻字	
パラメーター			説明
IKE 交換モード			IKE 交換フェーズのモードを選択します。
	Main		Main モードを使用する場合に選択しま す。Main モードではネゴシエーション中 の ID 情報を保護します。
	Aggressive		Aggressive モードを使用する場合に選択 します。Aggressive モードではネゴシ エーション中に ID 情報を保護しません。 Main モードに比べて IKE トンネルの交換 プロセスが少ないので処理が高速です。
事前共有鍵			事前共有鍵を入力します。半角英数字で 50 文字以内で入力してください。
IKE 暗号化 / 認証;	アルゴリズム		ドロップダウンリストから使用する暗号 化 / 認証アルゴリズムの組み合わせを選 択します。VPN 機器間の通信で双方がサ ポートするアルゴリズムの組み合わせを 適用する場合は「全て」を選択してくだ さい。
有効期限			鍵の有効期限を設定します。単位は 「秒」、「分」、「時間」、「日」から選択で きます。IKE 暗号化 / 認証アルゴリズム に「全て」を選択した場合は設定できま せん。600 秒~ 30 日の範囲で設定して ください。

# 7.2.5.3 IPSec 設定

何知思知	3000 179 💙	
	IPSec設定	
IPSec暗号化/認証アルゴリズム	全て	~
PFSグループ	未定義 🗸	
有効期限	3600 秒 🗸 または 75000 KByte	
	<u>追加</u> 変更 削除	ヘルプ
パラメーター		説明
IPSec 暗号化 / 認証アルゴリズム		ドロップダウンリストから使用する暗号 化 / 認証アルゴリズムの組み合わせを選 択します。VPN 機器間の通信で双方がサ ポートするアルゴリズムの組み合わせを 適用する場合は「全て」を選択してくだ さい。
PFS グループ		「DH–1」、「DH–2」、「DH–5」から選択し ます。PFS グループを指定しない場合は 「未定義」を選択します。
有効期限		IPSec 暗号化 / 認証アルゴリズムにすべ てを選択した場合は設定できません。単 位を「秒」、「分」、「時間」、「日」または 「Kbyte」から選択できます。300 秒~30 日、または 1000KBytes ~ 1000000KBytes の範囲で設定してくださ い。
「追加」ボタン		ID ドロップダウンリストで「新規追加」 を選択した場合にアクティブになりま す。VPN ポリシーを追加登録します。10 件までのポリシーを追加することができ ます。ボタンをクリックすると設定内容 が即時に反映されます。
「変更」ボタン		ID ドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。設定内容の変更を保存しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「削除」ボタン		ID ドロップダウンリストで既存のルール の ID 番号を選択した場合にアクティブ になります。選択したルールを削除しま す。ボタンをクリックすると設定内容が 即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができま す。

# 7.2.6 サイト間アクセスルール

VPN ポリシーが一覧表示されます。

サイト間アクセスルール ID ポリシー名 ローカル/リモートネットワーク トンネル終端 鍵管理方式 IPSec 状況

パラメーター	説明
ID	ポリシーの ID 番号が表示されます。
ポリシー名	ポリシー名が表示されます。
ローカル / リモートネットワーク	ローカル / リモートセキュアグループに 関する情報が表示されます。
トンネル終端	リモートゲートウェイの IP アドレスが 表示されます。
鍵管理方式	鍵管理方式が表示されます。
IPSec	IPSec の動作モードが表示されます。
状況	VPN の有効 / 無効が表示されます。

# 7.3 VPN トラフィックの確認

「統計情報」ページでは、本製品の VPN に関するパケット転送の統計を参照することができます。

# 7.3.1 確認

VPN トラフィックの状況を確認するには以下の手順を実行します。

1.メニューから「VPN」->「統計情報」をクリックします。

アドレス(D) 🕘 http://192.168.1.1/index.html								💌 🔁 i
VPN Router								Allied Tele
				VPN Stat	istics			
				Global IPSec S	A Statistics			
-	AH Packet	s		0				
	ESP Pack	ets		0				
	Triggers			0				
CentreCOM AR260S	Packets D	ropped		0				
──■ セットアップワイサード ──■ システム 情報	Packets P	assed		0				
				IKE Stati	stics			
H WAN	IKE Phase	1 Negotiations	Done	0				
… <u>■</u> ルーナインク ト <mark>←</mark> ]ファイアウォール	Failed IKE	Negotiations D	one	0				
- Inboundアクセス	Quick Mod	le Negotiations	Performed	0				
- Outboundアクセス	Number of	ISAKMP SAs		0				
一回 URLフィルター 日一回 アドバンスト語定				ESP Stat	stics			
セルフアクセス	Active Inbo	ound ESP SAs		0				
	Active Out	bound ESP SA	s	0				
	Total Inbo	und ESP SAs		0				
	Total Outt	ound ESP SAs		0				
				AH Stati	stics			
VPN 接続 1 经手续超	Active Inbo	ound AH SAs		0				
	Active Out	bound AH SAs		0				
システム管理	Total Inbo	und AH SAs		0				
	Total Outb	ound AH SAs		0				
				IKE S	A			
	Loc	al ID	Remote ID	Local Port	Remote Port	Phase1 Status	Exchange Type	Initiator
				IPSec	SA			
	SPI	Protocol		Source IP		Destination IP		
				更新				

		Global IPSec S	A Statistic	S		
AH Packets		0				
ESP Packets		0				
Triggers		0				
Packets Dropped		0				
Packets Passed		0				
		IKE Stati	stics			
IKE Phase1 Negotiations (	Done	0				
Failed IKE Negotiations D	one	0				
Quick Mode Negotiations	Performed	0				
Number of ISAKMP SAs		0				
		ESP Stati	stics			
Active Inbound ESP SAs		0				
Active Outbound ESP SAs	5	0				
Total Inbound ESP SAs		0				
Total Outbound ESP SAs		0				
		AH Statis	stics			
Active Inbound AH SAs		0				
Active Outbound AH SAs		0				
Total Inbound AH SAs		0				
Total Outbound AH SAs		0				
		IKE S	A			
Local ID	Remote ID	Local Port	Remote Port	Phase1 Status	Exchange Type	Initiator
		IPSec	SA			
SPI Protocol		Source IP		<b>Destination IP</b>		

2.「VPN Statistics」、「IKE SA」、「IPSec SA」が表示されます。表示を更新するには「更新」ボタンをクリックします。

# 7.3.2 「統計情報」ページの解説

「統計情報」ページでは、VPN 接続に関する統計情報を参照できます。

# 7.3.2.1 VPN Statistics

メニューから「VPN」->「統計情報」の順にクリックすると以下の画面が表示されます。

	VPN Statistics	
	Olehel IPRes CA Statistics	
ALL Deal/ata	Global IPSec SA Statistics	
AR Paukets	U	
ESP Packets	U	
Triggers Desires	U	
Packets Dropped	U	
Packets Passed	U	
	IKE Statistics	
IKE Phase1 Negotiations Done	0	
Failed IKE Negotiations Done	D	
Quick Mode Negotiations Performed	0	
Number of ISAKMP SAs	0	
	ESP Statistics	
Active Inbound ESP SAs	0	
Active Outbound ESP SAs	0	
Total Inbound ESP SAs	0	
Total Outbound ESP SAs	0	
	AH Statistics	
Active Inbound AH SAs	0	
Active Outbound AH SAs	0	
Total Inbound AH SAs	0	
Total Outbound AH SAs	0	
	WE CA	
メーター オプション		説明
IPSec SA Statistics		IPSec SA のパケットの統計情報が- 示されます

	AH Packets	AH パケット数がカウントされます。
	ESP Packets	ESP パケット数がカウントされます。
	Triggers	LAN 側から IPSec パケット送信時、VPN トンネルを新規に作成する場合にカウン トされます。
	Packets Dropped	破棄されたパケット数がカウントされま す。
	Packets Passed	転送されたパケット数がカウントされま す。
IKE Statistics		IKE のネゴシエーションの情報が一覧表 示されます。
	IKE Phase1 Negotiations Done	完了した IKE フェーズ 1 のネゴシエー ション数がカウントされます。

	Failed IKE Negotiations Done	失敗した IKE フェーズ 1 のネゴシエー ション数がカウントされます。
	Quick Mode Negotiations Performed	完了したクイックモードでのネゴシエー ション数がカウントされます。
	Number of ISAKMP SAs	フェーズ 1 の SA の数がカウントされま す。
ESP Statistics		ESP に関する情報が一覧表示されます。
	Active Inbound ESP SAs	有効な Inbound ESP SA の数がカウント されます。
	Active Outbound ESP SAs	有効な Outbound ESP SA の数がカウント されます。
	Total Inbound ESP SAs	IKE SA が確立してからの Inbound ESP SA の総数がカウントされます。
	Total Outbound ESP SAs	IKE SA が確立してからの Outbound ESP SA の総数がカウントされます。
AH Statistics		AH に関する情報が一覧表示されます。
	Active Inbound AH SAs	有効な Inbound AH SA の数がカウントさ れます。
	Active Outbound AH SAs	有効な Outbound AH SA の数がカウント されます。
	Total Inbound AH SAs	IKE SA が確立してからの Inbound AH SA の総数がカウントされます。
	Total Outbound AH SAs	IKE SA が確立してからの Outbound AH SA の総数がカウントされます。

# 7.3.2.2 IKE SA

Total Outb	ound AH SAs		0			
		IKE	SA			
Loca	ıl ID Remot	e ID Local Po	rt Remote Port	Phase1 Status	Exchange Type	Initiator

パラメーター	説明
Local ID	IKE SA 確立時のローカル ID が表示され ます。
Remote ID	IKE SA 確立時のリモート ID が表示され ます。
Local Port	IKE SA 確立時に使用するローカルポート の番号が表示されます。
Remote Port	IKE SA 確立時に使用するリモートポート の番号が表示されます。
Phase1 Status	フェーズ 1 のステータスが表示されま す。
Exchange Type	IKE 交換モードが表示されます。
Initiator	本製品がイニシエーターとして動作して いる場合に「Yes」、レスポンダーとして 動作している場合に「No」が表示されま す。

# 7.3.2.3 IPSec SA

		IPSec S		
SPI	Protocol	Source IP	Destination IP	
		西北		

パラメーター	説明
SPI	SPI(Security Parameter Index)が表示さ れます。
Protocol	VPN トンネルで使用されているプロトコ ルが表示されます。
Source IP	VPN トンネルのローカルゲートウェイの IP アドレスが表示されます。
Destination IP	VPN トンネルのリモートゲートウェイの IP アドレスが表示されます。
「更新」ボタン	クリックすると表示内容を更新します。

# 8 付録

# 8.1 デフォルト設定

本製品のデフォルト設定は以下のとおりです。

## 8.1.1 ユーザー名 / パスワードのデフォルト設定

ユーザー名	レベル	パスワード
manager	管理者	friend
guest	ユーザー	guest



# 8.1.2 設定ページ別のデフォルト設定

「LAN」/「IP」		
	IP アドレス	192.168.1.1
	サブネットマスク	255.255.255.0
「LAN」/「DHCP」		
	IP アドレスプール	192.168.1.10 ~ 192.168.1.200
	サブネットマスク	255.255.255.0
	リース期限	14 日
	デフォルトゲートウェイ	192.168.1.1
	プライマリ DNS サーバー	192.168.1.1
「WAN」/「WAN」		
	接続モード	PPPoE
	Unnumbered PPPoE	無効
	ホスト名	AR260S
	DNS オプション	自動取得
	MSS クランプ	有効
	MSS の値	40Bytes
	接続オプション	キープアライブ
	エコー送信間隔	60 秒

「ファイアウォール」	/「アドバンスト設定」	/「セルフアクセス」
------------	-------------	------------

	ステルスモード	無効
	セルフアクセスルール	ICMP(LAN 側)、TCP(80 番、LAN 側)、UDP(161 番、LAN 側)、 UDP(162 番、LAN 側)、UDP(53 番、LAN 側)、TCP(10081 番、 LAN 側)、UDP(500 番、WAN 側)
「ファイアウォール」	/「アドバンスト設定」/「DoS」	
	DoS アタックフィルター設定	SYN Flooding(有効)、Winnuke(無効)、MIME Flood(無効)、FTP Bounce(無効)、IP Unaligned Time-stamp(無効)、Sequence Num- ber Prediction Check(無効)、Sequence Number Out-of-range Check (無効)、ICMP Verbose(有効)
_		MAX IP Fragment Count: 45
		Minimum IP Fragment Size: 512
「システム管理」/「サ	・ービスの有効/無効」	
	ファイアウォール	有効
	VPN	無効
	DNSリレー	有効
	DHCP	有効
	SNTP	無効
	リセットスイッチによる初期化	有効
「システム管理」/「設	定管理 / パスワード」	
	管理者パスワード	friend(ユーザー名 :manager)
	ユーザーパスワード	guest (ユーザー名 :guest)
「システム管理」/「シ	マステム情報」	
	システム名(SysName)	AR260S
「システム管理」/「タ	イムゾーン設定」	
	日付	2000 年 1 月 1 日
	時刻	0時0分0秒
	タイムゾーン	GMT+9:00
	SNTP サーバー 1	133.100.9.2
	SNTP サーバー 2	133.100.11.8
	SNTP サーバー 3	133.40.41.175
	SNTP サーバー 4	130.69.251.23
	SNTP サーバー 5	128.105.39.11
	更新間隔	60 分

「システム管理」/「SNMP」

SNMP	無効
RO コミュニティー名	public
RW コミュニティー名	private

# 8.2 NAT について

NAT (Network Address Translation) とは、ローカルネットワーク内のみで使用するプライベート IP アドレスとグローバ ル IP アドレスを相互に変換し、プライベート IP アドレスを使用するローカルネットワーク内のクライアントからイン ターネットにアクセスできるようにする仕組みです。本製品ではスタティック NAT、ダイナミック NAT、ENAT、インター フェース NAT を使用することができます。

#### 8.2.1 スタティック NAT

スタティック NAT では、プライベート IP アドレスをグローバル IP アドレスに1対1で固定的にマッピングします。管理 者が意図的に変更しない限りマッピングは固定的に行われます。つまり、1 台のクライアントのプライベート IP アドレ スに対して、常に同じグローバル IP アドレスがマッピングされます。グローバル IP アドレスはプライベート IP アドレ スと同じ数必要です。



GBLIP=グローバルIPアドレス PVTIP=プライベートIPアドレス

# 8.2.2 ダイナミック NAT

ダイナミック NAT では、プライベート IP アドレスをグローバル IP アドレスに1対1で動的にマッピングします。動的に マッピングするため、グローバル IP アドレスとプライベート IP アドレスの数は同じである必要はありませんが、使用で きるグローバル IP アドレスがない場合、クライアントの送出したパケットは破棄されます。



GBLIP=グローバルIPアドレス PVTIP=プライベートIPアドレス

#### 8. 2. 3 ENAT

NAPT (Network Address and Port Translation)、または IP マスカレードとも呼ばれます。ENAT では、複数のプライベート IP アドレスに 1 つのグローバル IP アドレスと複数のポートをマッピングします。グローバル IP アドレスが 1 つのみの場合でも、異なるポートを使用して複数のクライアントからインターネットに接続することができます。



GBLIP=グローバルIPアドレス PVTIP=プライベートIPアドレス

#### 8.2.4 インターフェース NAT

インターフェース NAT は ENAT と同じ仕組みです。ただし、使用するグローバル IP アドレスは、本製品の WAN 側インター フェースに割り当てられたグローバル IP アドレスです。



GBLIP=グローバルIPアドレス PVTIP=プライベートIPアドレス

# 8.3 トラブルシューティング

ここでは、本製品使用中のトラブルの代表的な例と、その対応方法について説明します。

#### 8.3.1 LED に関するトラブル

LED に関するトラブルについて説明します。

#### 8.3.1.1 電源をオンにしても POWER LED が点灯しない

#### 以下の事項を確認してください。

1. 本製品付属の AC アダプターを使用していますか?電源アダプターは付属のものをご使用ください。

2. AC アダプターの出力プラグは本製品にきちんと接続されていますか?接続されていないと電源が供給されません。

3. AC アダプターの AC プラグは電源コンセントにきちんと差し込まれていますか?接続されていないと電源が供給されません。

### 8.3.1.2 UTP ケーブルを接続しても WAN LED が点灯しない

#### 以下の事項を確認してください。

- 1. UTP ケーブルはそれぞれ本製品の WAN ポート、モデムのポートにきちんと接続されていますか?接続されていないとリンクが 確立しないため WAN LED が点灯しません。
- 2. モデムの電源はオンになっていますか?モデムの電源がオンになっていないとリンクが確立しないため WAN LED が点灯しません。
- 3. 本製品の電源をオンにしてモデムに接続してから 30 秒以上経過していますか?本製品の起動には 30 秒ほどかかります。
- 4. 本製品とモデムの接続にはストレートケーブルを使用していますか?モデムとの接続にはストレートケーブルを使用してください。

### 8.3.1.3 UTP ケーブルを接続しても LAN LED が点灯しない

#### 以下の事項を確認してください。

- 1. UTP ケーブルはそれぞれ本製品の LAN ポート、対向のハブ、コンピューターにきちんと接続されていますか?接続されていな いとリンクが確立しないため、LAN LED が点灯しません。
- 2. ハブやコンピューターの電源はオンになっていますか? 電源がオンになっていないとリンクが確立しないため、LAN LED が点 灯しません。
- 3. 適切な UTP ケーブルを使用していますか? 100BASE-TX で通信する場合はカテゴリー 5、10BASE-T で通信する場合はカテゴ リー3以上のケーブルを使用してください。

#### 8.3.2 インターネットへのアクセスに関するトラブル

インターネットへのアクセスに関するトラブルについて説明します。

#### 8.3.2.1 インターネットにアクセスできない

#### 以下の事項を確認してください。

- 1. 本製品に対して Ping コマンドを実行した場合に、正しく応答がありますか?応答がない場合、本製品との通信ができていません。
- 2. コンピューターに IP アドレスを手動で割り当てている場合、デフォルトゲートウェイの IP アドレスは正しく設定されていますか?設定されていない場合は、再度正しく設定を行ってください。
- コンピューターに IP アドレスを手動で割り当てている場合、DNS サーバーの IP アドレスは正しく設定されていますか? DNS サーバーの IP アドレスはご契約のプロバイダーから指定されている場合があります。詳細については、ご契約のプロバイ ダーにお問い合わせください。
- A. NAT は正しく設定されていますか?プライベートネットワークからインターネットにアクセスするには、プライベート IP ア ドレスをグローバル IP アドレスに NAT 変換する設定が必要です。デフォルト設定では、インターフェース NAT が設定されて います。

#### 8.3.2.2 Web ページを表示できない

#### 以下の事項を確認してください。

- 1. コンピューターに IP アドレスを手動で割り当てている場合、DNS サーバーの IP アドレスは正しく設定されていますか? DNS サーバーの IP アドレスはご契約のプロバイダーから指定されている場合があります。詳細については、ご契約のプロバイ ダーにお問い合わせください。
- 2. DNS サーバーに対して Ping コマンドを実行した場合に、正しく応答がありますか?応答がない場合、DNS サーバーとの通信ができていません。

### 8.3.3 GUI 設定に関するトラブル

GUI設定に関するトラブルについて説明します。

### 8.3.3.1 ログインパスワードを忘れた

以下の事項を確認してください。

1. デフォルトのパスワードを変更していますか?変更していない場合はユーザー名「manager」、パスワード「friend」でログイ ンすることができます。デフォルトのユーザー名とパスワードでログインできない場合は「P.45 リセットスイッチによる初 期化」を実行してください。初期化が完了したら再度デフォルトのユーザー名とパスワードでログインします。



│ 「リセットスイッチによる初期化」機能を無効にしている場合、リセットスイッチを使用した初期化はおこなえませ ・ ん。



初期化の手順を実行すると、現在の設定内容はすべて消去されますのであらかじめご注意ください。

#### 8.3.3.2 設定画面が表示されない

以下の事項を確認してください。

- 1. ご使用の Web ブラウザーのバージョンは Internet Explorer6 以降ですか?本製品でサポートするバージョンは Internet Explorer6 以上です。
- 2. Web ブラウザーのプロキシー設定がオンになっていませんか?本製品の設定画面にアクセスする場合は、プロキシー設定をオフにしてください。
- 3. Web ブラウザーの JavaScript が無効になっていませんか?本製品の設定画面を表示するには JavaScript を有効にしてください。
- 4. 本製品とコンピューターのサブネットマスクが異なっていませんか?本製品の設定画面にアクセスする場合は、本製品とコン ピューターは同じネットワークに属する必要があります。

# ご注意

- 本マニュアルは、アライドテレシス株式会社が作成したもので、すべての権利をアライドテレシス株式会社が保有しています。本 書の全部または一部を弊社の同意なしにコピーまたは転載することを固くお断りいたします。
- アライドテレシス株式会社は、予告なく本マニュアルの一部または全体を修正、変更することがありますのでご了承ください。
- アライドテレシス株式会社は、改良のため予告なく製品の仕様を変更することがありますのでご了承ください。
- 本マニュアルについて、万一記載漏れ、誤りや不審な点等がございましたらご連絡ください。
- 本製品を運用して発生した結果については、上記の各項にかかわらず責任を負いかねますのでご了承ください。

Copyright (C) 2004 アライドテレシス株式会社

# 商標について

- ・ CentreCOM はアライドテレシス株式会社の登録商標です。
- Windows、MS-DOS、Windows NT は、米国 Microsoft Corporationの米国およびその他の国における登録商標です。
- その他、この文書に記載されているソフトウェアおよび周辺機器の名称は各メーカーの商標または登録商標です。

マニュアルバージョン

2004 年 7 月 5 日 Rev. A 初校

アライドテレシス株式会社 PN J613-M0099-11 Rev.A 040705