4. 本機へのアクセスを管理する

機器設定の変更を防止する

本機の各種機能の設定項目は、管理者の種類によって設定できる項目が異なります。管理者が管理する項目はユーザーによる設定の変更を禁止することができます。
管理者を登録して本機を運用します。

♦ 管理者の種類

本機に管理者を登録し、管理者のログインユーザー名とログインパスワードで管理者を認証します。管理者の種類によって設定できる項目が異なります。本機を運用する上で、次の管理者を定義しています。

・ユーザー管理者
・機器管理者
・ネットワーク管理者
・文書管理者

管理者の適用設定項目については、各管理者の設定可能項目一覧を参照してください。

♦ メニュープロテクト機能

本機を使用する上で、管理者以外のユーザーでも設定を変更できる機能があります。この機能に対してユーザーのアクセス権のレベルを設定します。

参照

・P.141 「機器管理者設定可能項目一覧」
・P.145 「ネットワーク管理者設定可能項目一覧」
・P.148 「文書管理者設定可能項目一覧」
・P.149 「ユーザー管理者設定可能項目一覧」
・P.152 「ユーザー設定可能項目一覧」

メニュープロテクトについて

管理者は、本機の設定項目に対するユーザーのアクセス権を制限することもできます。本機に搭載されている機能の初期設定メニューやプリンターの通常メニューが変更できないようにロックします。この機能は、ユーザー認証による管理を行わない場合にも有効です。メニュープロテクトの設定を変更する場合は、事前に管理者認証を有効にする必要があります。管理者認証の設定方法については、「管理者認証を設定する」を参照してください。メニュープロテクトのレベルとユーザー権限の関係については、「ユーザー設定可能項目一覧」を参照してください。

参照

・P.23 「管理者認証を設定する」
・P.152 「ユーザー設定可能項目一覧」

メニュープロテクトを設定する

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
メニュープロテクトは［しない］、［レベル 1］、［レベル 2］から設定することができます。［しない］を設定した場合はメニュープロテクトによる制限はありません。アクセス権の制限をより強くする場合は、［レベル 2］に設定してください。

1 ［メニュー］キーを押します。

2 ［▲］［▼］キーを押して［調整 / 管理］を選択し、［OK］キーを押します。

3 ［▲］［▼］キーを押して［一般管理］を選択し、［OK］キーを押します。

4 ［▲］［▼］キーを押して［メニュープロテクト］を選択し、［OK］キーを押します。

5 ［▲］［▼］キーを押して設定するメニュープロテクトのレベルを選択し、［OK］キーを押します。

6 ［メニュー］キーを押します。

補足

・各機能のメニュープロテクトのレベルについては、「ユーザー設定可能項目一覧」を参照してください。

参照

・P.152 「ユーザー設定可能項目一覧」
・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

機能の使用を制限する

本機の各種機能に対してユーザーのアクセス権を設定し、第三者による不正操作の介入を防止することができます。

使用できる機能を設定する

ユーザー管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
登録されたユーザーに対して、使用できる機能を設定します。この設定により、ユーザーの使用できる機能を制限することができます。

1. Web Image Monitor を起動し、ユーザー管理者モードにログインします。
2. [アドレス帳] をクリックします。
3. 設定したいユーザーをクリックし、[変更] をクリックします。
   [検索] をクリックすると、名称、リスト表示、登録番号、ユーザーコードから検索することができます。
4. 利用を可能とする機能を選択し、[OK] キーをクリックします。
5. 管理者モードからログアウトします。
6. Web Image Monitor を終了します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

ログ情報の管理

1) ログについて
本機は以下のログ情報の蓄積をメモリーやハードディスクに行います。
ログ情報を確認するためには、Ridoc IO OperationServer が必要です。
・ジョブログ
ユーザーの文書に関わるワークフロー全てのログ情報
・アクセスログ
ログイン / ログアウト / 文書生成 / 文書削除 / 文書自動削除 / 文書一括削除 / 不正コピーガード文書読み取り / 管理者操作 *1 / カスタマーエンジニア操作 *2
*1 管理者操作 : ジョブログ機能設定変更 / アクセスログ機能設定変更 / ログ情報一括削除 / ログ暗号化設定変更
*2 カスタマーエンジニア操作 : ハードディスク初期化

2) ログ消去について
本機に記録されたログを消去することで、ハードディスクの容量を空けることができます。

3) ログ転送について
転送されるログはジョブログ、アクセスログ、不正読み取りの事実、読み取り者、読み取り時刻です。
ログを転送することで、不正読み取り履歴や読み取り者の確認ができます。

ログ消去の設定

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
本機に記憶されたログをまとめて消去することができます。本機に記録されたログを消去することで、ハードディスクの容量を空けることができます。

1 Web Image Monitor を起動し、機器管理者モードにログインします。

2 [設定] をクリックします。

3 [機器] メニューの [ログ] をクリックします。

4 [ログ一括消去] で [実行] をクリックします。
確認のメッセージが表示されます。

5 [OK] をクリックします。
[ログ] メニューに戻ります。

6 [OK] をクリックします。

7 [ログアウト] をクリックします。

8 Web Image Monitor を終了します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

ログ転送の設定

機器管理者は、Ridoc IO OperationServer からのみ［する］に設定できます。本機からは［する］に設定されている場合のみ［しない］に設定の変更ができます。本機への管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
ログ転送設定の設定値の確認や変更ができます。この設定により Ridoc IO OperationServer へログを転送し、不正読み取り履歴や読み取り者の確認ができます。
Ridoc IO OperationServer については、販売店にお問い合わせください。
ログ転送の設定については Ridoc IO OperationServer の使用説明書を参照してください。

1 ［メニュー］キーを押します。

2 ［▲］［▼］キーを押して［セキュリティー管理］を選択し、［OK］キーを押します。

3 ［▲］［▼］キーを押して［ログ転送設定］を選択し、［OK］キーを押します。

4 ［▲］［▼］キーを押して［しない］を選択し、［OK］キーを押します。

5 ［メニュー］キーを押します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

5. ネットワークのセキュリティー強化

不正なアクセスを防止する

IPアドレスに制限をかけたり、ポートやプロトコルを無効に設定したり、Web Image Monitorからネットワークセキュリティーレベルの設定をすることによって、ネットワーク上での不正アクセスを防止し、アドレス帳や蓄積文書、初期設定のデータなどを保護することができます。

アクセスコントロールの設定

ネットワーク管理者が設定します。
本機はTCP/IP通信を使ったアクセスに対し、アクセスコントロールを行うことができます。アクセスを許可するIPアドレスを範囲指定により制限します。
たとえば、アクセスコントロール範囲を［192.168.15.16］-［192.168.15.20］のように設定した場合は、アクセス可能なPCのIPアドレスは、192.168.15.16～192.168.15.20になります。

重要

- アクセスコントロールはLPR、RSH/RCP、FTP、SFTP、IPP、Web Image Monitor、Ridoc IO Navi、Ridoc Desk Navigator、Ridoc Document Routerからの利用を制限することができます。Ridoc IO Naviの監視機能を制限することはできません。
- telnetからの利用を制限することはできません。

1 **Webブラウザーを起動します。**

2 **Webブラウザーのアドレスバーに「http://（本機のIPアドレス、またはホスト名）/」と入力し、本機にアクセスします。**
IPv4アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 **［ログイン］をクリックします。**
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 **［設定］をクリックし、「セキュリティー」の［アクセスコントロール］をクリックします。**
「アクセスコントロール」エリアが表示されます。

5 IPv4 アドレスの設定の場合は、本機にアクセスを許可する IP アドレスの数値を「アクセスコントロール範囲」に入力します。

IPv6 アドレスの設定の場合は、本機にアクセスを許可する IP アドレスの数値を「アクセスコントロール範囲」の「範囲指定」に入力するか、本機にアクセスを許可する IP アドレスの数値を「マスク指定」に入力し、「マスク長」を入力します。

6 [OK] をクリックします。

アクセスコントロールが設定されます。

7 [OK] をクリックします。

8 [ログアウト] をクリックします。

プロトコル有効／無効の設定

ネットワーク管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

プロトコルごとに、有効にするか、無効にするかを設定します。この設定により、プロトコルを限定し、不正なアクセスを制限します。

プロトコル有効／無効の切り替えは、操作部、Web Image Monitor、telnet、Ridoc IO Admin、またはRidoc IO OperationServerで設定できます。ただし設定対象プロトコルが異なります。

プロトコル	ポート	設定手段	無効時の状態
TCP/IP	-	・操作部 ・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	IPv4上で動作するすべてのアプリケーションが使用できなくなります。 IPv4通信しているときにWeb Image Monitor で IPv4 を無効化することはできません。
IPv6	-	・操作部 ・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	IPv6上で動作するすべてのアプリケーションが使用できなくなります。
IPsec	-	・操作部 ・Web Image Monitor ・telnet	IPsec による暗号化通信ができなくなります。
FTP	TCP:21	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	FTP の機能が使用できなくなります。 操作部からの設定で個人情報のみを表示禁止することもできます。

プロトコル	ポート	設定手段	無効時の状態
sshd/sftpd	TCP:22	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	sftp の機能が使用できなくなります。 操作部からの設定で個人情報のみを表示禁止することもできます。 表示禁止の設定については、P.129 「セキュリティー強化機能を設定する」を参照してください。
telnet	TCP:23	・Web Image Monitor	telnet の機能が使用できなくなります。
SMTP	TCP:25 （可変）	・操作部 ・Web Image Monitor ・Ridoc IO Admin ・Ridoc IO OperationServer	メール通知機能の SMTP 受信が使用できなくなります。
HTTP	TCP:80	・Web Image Monitor ・telnet	HTTP の機能が使用できなくなります。 IPP による 80 ポートでの印刷ができなくなります。
HTTPS	TCP:443	・Web Image Monitor ・telnet	HTTPS の機能が使用できなくなります。 @Remote が使用できなくなります。 尚、操作部、Web Image Monitor からの設定で SSL 通信のみを許可し、非 SSL 通信を禁止することもできます。
SMB	TCP:139	・操作部 ・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	SMB の機能が使用できなくなります。
NBT （NetBIOS over TCP/IPv4)	UDP:137 UDP:138	・Web Image Monitor ・telnet	TCP/IP 経由での SMB 印刷の機能、および WINS サーバーによる NetBIOS 名解決機能が使用できなくなります。

プロトコル	ポート	設定手段	無効時の状態
SNMPv1,v2	UDP:161	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	SNMPv1,v2 の機能が使用できなくなります。 操作部、Web Image Monitor、telnet で SNMPv1,v2 による設定のみを禁止し、参照を許可することもできます。
SNMPv3	UDP:161	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	SNMPv3 の機能が使用できなくなります。 操作部、Web Image Monitor、telnet からの設定で SNMPv3 暗号通信のみ許可し、非 SNMPv3 暗号通信を禁止することもできます。
RSH/RCP	TCP:514	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	RSH の機能、ネットワーク TWAIN 機能が使用できなくなります。 操作パネルからの設定で個人情報のみを表示禁止することもできます。
LPR	TCP:515	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	LPR の機能が使用できなくなります。 操作パネルからの設定で個人情報のみを表示禁止することもできます。 表示禁止の設定については、P.129 「セキュリティー強化機能を設定する」を参照してください。
IPP	TCP:631	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	IPP の機能が使用できなくなります。
SSDP	UDP:1900	・Web Image Monitor ・telnet	Windows からの UPnP による機器検索および BMLinkS からの機器検索ができなくなります。
BMLinkS	TCP:52000 （可変）	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	BMLinkS の機能が使用できなくなります。

プロトコル	ポート	設定手段	無効時の状態
BMLinkS over SSL	TCP:52001 （可変）	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	BMLinkSの機能が使用できなくなります。
Bonjour	UDP:5353	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	Bonjour の機能が使用できなくなります。
@Remote	TCP:7443 TCP:7444	・telnet	@Remote が使用できなくなります。
DIPRINT	TCP:9100	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	DIPRINT の機能が使用できなくなります。
RFU	TCP:10021	・telnet	FTP 経由でリモートファームウェア更新を試みます。
AppleTalk	(PAP)	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	AppleTalk 印刷が使用できなくなります。
WS-Device	TCP:53000 （可変） UDP/TCP:3702	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	WS-Device の機能が使用できなくなります。
WS-Printer	TCP:53001 （可変）	・Web Image Monitor ・telnet ・Ridoc IO Admin ・Ridoc IO OperationServer	WS-Printer の機能が使用できなくなります。
RHPP	TCP:59100	・Web Image Monitor ・telnet	RHPP を用いた印刷ができなくなります。

補足

・「無効時の状態欄」に記載されている操作部からの設定で個人情報のみを表示禁止する方法については、「個人情報表示制限」を参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」
・P.130 「個人情報表示制限」

操作部による設定

1 [メニュー] キーを押します。

2 [▲] [▼] キーを押して [インターフェース設定] を選択し、[OK] キーを押します。

3 [▲] [▼] キーを押して [ネットワーク設定] を選択し、[OK] キーを押します。

4 [▲] [▼] キーを押して [有効プロトコル] を選択し、[OK] キーを押します。

5 [▲] [▼] キーを押して設定をしたいプロトコルを選択し、[OK] キーを押します。

6 [▲] [▼] キーを押して [無効] を選択し、[OK] キーを押します。

7 [メニュー] キーを押します。

Web Image Monitor による設定

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http:// (本機の IP アドレス、またはホスト名) /」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [ネットワークセキュリティー] をクリックします。
「ネットワークセキュリティーレベル設定」エリアが表示されます。

5 設定するプロトコルの有効 / 無効 (または、Open/Close) を選択します。

6 [OK] をクリックします。

7 [OK] をクリックします。

8 [ログアウト] をクリックします。

補足

・Web Image Monitor で SMTP を無効にするには、メール設定で受信プロトコルを SMTP 以外に設定します。設定方法は、Web Image Monitor のヘルプを参照してください。
・telnet での設定方法は、『ソフトウエアガイド』「機器の監視」を参照してください。Ridoc IO Admin での設定方法は、Ridoc IO Admin のヘルプを参照してください。Ridoc IO OperationServer の設定方法は、Ridoc IO OperationServer の使用説明書を参照してください。

ネットワークセキュリティーレベル設定

ネットワーク管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
プロトコルの有効／無効を 3 段階のレベルで自動的に設定し、セキュリティーの強度を変更できます。
この設定により不正なアクセスを制限できます。
ネットワークセキュリティーレベル設定は、操作部、または Web Image Monitor で設定できます。ただし設定対象プロトコルが異なります。
セキュリティーレベルは［レベル 0］、［レベル 1］、［レベル 2］から選択します。
［レベル 2］に設定すると、最高度のセキュリティー強度を持ちます。脅威から守るべき情報が極めて重要なときに設定します。
［レベル 1］に設定すると、適切なセキュリティー強度を持ちます。例えば社内 LAN に接続するときなどに設定します。
［レベル 0］に設定すると、全機能を最も容易に利用できます。脅威から守るべき情報がないときに設定します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

操作部による設定

1 ［メニュー］キーを押します。

2 ［▲］［▼］キーを押して［セキュリティー管理］を選択し、［OK］キーを押します。

3 ［▲］［▼］キーを押して［ネットワークセキュリティレベル］を選択し、［OK］キーを押します。

4 ［▲］［▼］キーを押してネットワークのセキュリティレベルを選択し、［OK］キーを押します。

5 ［メニュー］キーを押します。

Web Image Monitor による設定

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [ネットワークセキュリティ] をクリックします。
「ネットワークセキュリティーレベル設定」エリアが表示されます。

5 「セキュリティーレベル詳細」で設定するレベルを選択します。

6 [OK] をクリックします。

7 [OK] をクリックします。

8 [ログアウト] をクリックします。

各機能とセキュリティーモードレベルの関係

◯= 使用可能です。
- = 使用不可です。
▲= ポートが開いています。
■ = ポートが閉じています。
☆= 自動
★ = 必ず暗号
×= 暗号化優先

	機能		セキュリティーモードレベル		
			レベル 0	レベル 1	レベル 2
TCP/IP *1	HTTP	80 ポート	▲	▲	▲
		443 ポート	▲	▲	▲
		631 ポート	▲	▲	■
	IPP	80 ポート	▲	▲	▲
		631 ポート	▲	▲	■
		443 ポート	▲	▲	▲
	DIPRINT		◯	◯	-
	LPR		◯	◯	-
	FTP		◯	◯	◯
	ssh		◯	◯	◯
	sftp		◯	◯	◯
	RSH/RCP		◯	◯	-
	SNMP		◯	◯	◯
	SNMPv1,v2	設定	◯	-	-
		参照	◯	◯	-
	SNMPv3		◯	◯	◯
		SNMP 暗号	☆	☆	★
	telnet		◯	-	-
	SSDP		◯	◯	-
	NBT (NetBIOS over TCP/IPv4)		◯	◯	-
	SSL	443 ポート	▲	▲	▲
		SSL/TLS 暗号設定	×	×	★
	Bonjour		◯	◯	-
	SMB		◯	◯	-
	WS-MFP(WS-Device, WS-Printer)		◯	◯	-
	RHPP		◯	◯	-
AppleTalk *2	AppleTalk		◯	◯	-

*1 IPv4、IPv6 共通です。
*2 AppleTalk、および PS3 カードかマルチエミュレーションカードのどちらかが搭載されていない場合、◯であっても利用できません。

パスワードを暗号化通信する

ログインパスワード、PDF 文書のグループパスワード、および IPP 認証のパスワードを暗号化通信し、パスワードを解析される脅威から保護することができます。また管理者認証、ユーザー認証時のログインパスワードも暗号化します。

♦ **ドライバー暗号鍵について**
ユーザー認証を設定しているときに送信するパスワードの暗号化を行います。
ログインパスワードを暗号化するためには、本機とユーザーの PC で使用するドライバーにドライバー暗号鍵を設定します。

♦ **PDF 文書のグループパスワードについて**
Ridoc Desk Navigator の PDF ダイレクトプリント機能では、セキュリティーを強化するために PDF グループパスワードを設定することができます。本機の「プリンター初期設定」にある「PDF 設定」の「PDF グループパスワード」と同じパスワードに設定してください。

♦ **IPP 認証のパスワードについて**
IPP 認証のパスワードを暗号化するためには、Web Image Monitor を使用し、認証方法で［DIGEST］を選択し、本機に IPP 認証のパスワードを設定します。

補足

・PDF ダイレクトプリントを使用するためには、オプションの PS3 カード、またはマルチエミュレーションカードが必要です。
・IPP 認証のパスワードは、telnet や FTP で操作できますが、推奨はしません。

ドライバー暗号鍵の設定

ネットワーク管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
本機にドライバー暗号鍵を設定します。
この設定により、ログインパスワードを暗号化通信し、パスワードを解析される脅威から保護することができます。

1. ［メニュー］キーを押します。
2. ［▲］［▼］キーを押して［セキュリティー管理］を選択し、［OK］キーを押します。
3. ［▲］［▼］キーを押して［セキュリティー強化］を選択し、［OK］キーを押します。
4. ［▲］［▼］キーを押して［ドライバー暗号鍵］を選択し、［OK］キーを押します。
5. メッセージを確認し、［入力］を押します。

6 スクロールキーと［OK］キーでドライバー暗号鍵を入力し、［OK］キーを押します。

ドライバー暗号鍵は、半角英数字 32 文字以内で入力します。
本機に設定したドライバー暗号鍵は、ネットワーク管理者からユーザーに伝え、各ユーザーは、使用しているパソコンのドライバーに登録します。必ず本機に設定したドライバー暗号鍵と同じ文字列を入力してください。

7 ［メニュー］キーを押します。

補足

・プリンタードライバーの暗号鍵設定については、プリンタードライバーのヘルプを参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

5

PDF グループパスワードの設定

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
本機に PDF グループパスワードを設定します。
PDF グループパスワードを使用することにより、セキュリティーを強化し、PDF に設定されている PDF パスワードを解析される脅威から保護することができます。

重要

・本機に設定した PDF グループパスワードは、ネットワーク管理者からユーザーに伝え、各ユーザーは、使用している PC の Ridoc Desk Navigator に登録します。必ず本機に設定した PDF グループパスワードと同じ文字列を入力してください。登録方法は Ridoc Desk Navigator のヘルプを参照してください。

1 Web Image Monitor を起動し、ネットワーク管理者モードにログインします。

2 ［設定］をクリックします。

3 「プリンター」の［PDF グループパスワード］をクリックします。

4 「新 PDF グループパスワード」と「新 PDF グループパスワード（確認）」に同じパスワードを入力し、［OK］をクリックします。

5 管理者モードからログアウトします。

6 Web Image Monitor を終了します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

IPP 認証のパスワードの設定

ネットワーク管理者が設定します。
Web Image Monitor を使用し、本機に IPP 認証のパスワードを設定します。
以下の設定により、IPP 認証のパスワードを暗号化通信し、パスワードを解析される脅威から保護することができます。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http:// (本機の IP アドレス、またはホスト名) /」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [IPP 認証] をクリックします。
「IPP 認証」エリアが表示されます。

5 「認証 :」のドロップダウンメニューから［DIGEST］を選択します。

6 ユーザー名を「ユーザー名 :」ボックスに入力します。

7 パスワードを「パスワード :」ボックスに入力します。

8 [OK] をクリックします。
IPP 認証が設定されます。

9 [OK] をクリックします。

10 [ログアウト] をクリックします。

補足

・Windows XP、Windows Server 2003 で IPP ポートを使用する場合、OS の標準 IPP ポートを使用できます。

通信経路の保護と暗号化通信

本機では SSL、SNMPv3、IPsec を使用して暗号化通信を確立することができます。通信経路の保護や通信データの暗号化を行うことで、通信途中でのデータの盗聴、内容の解析、改ざんを防止することができます。

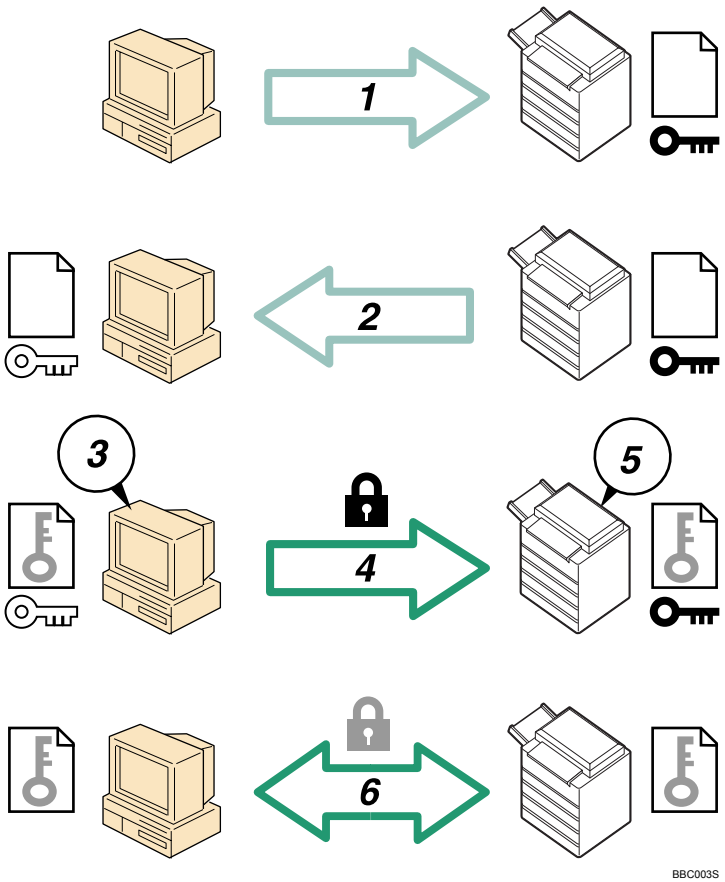
SSL（暗号化通信）の設定

ネットワーク管理者が設定します。
通信経路の保護と暗号化通信ができるように、機器証明書を作成、導入します。
機器証明書は、機器自身で作成、導入する自己証明書と、任意の認証局に証明書を申請し機器に導入する 2 つの運用形態があります。

重要

・SSL の設定には、ハードディスクもしくは保存用 SD カードが必要です。

♦ SSL（暗号化通信）について



1) ユーザーの PC から本機へアクセスするとき、SSL の機器証明書と公開鍵を要求します。

2) 本機からユーザーの PC へ機器証明書と公開鍵が送られます。
3) PC で共通鍵を生成し、公開鍵を使用して暗号化します。
4) 暗号化された共通鍵が本機に送られます。
5) 本機で秘密鍵を使用し、暗号化された共通鍵が復号されます。
6) 共通鍵を使用してデータを暗号化し、相手側で復号する安全な通信を実現します。

♦ 設定の流れ（自己証明書）

1) 機器証明書の作成と導入
Web Image Monitor を使用して機器証明書を作成、導入します。
2) SSL を有効にする
Web Image Monitor を使用し、［SSL/TLS］の設定を有効にします。

♦ 設定の流れ（認証局証明書）

1) 機器証明書の作成
Web Image Monitor を使用し、機器証明書を作成します。
証明書の作成後の申請や内容は認証局によって異なるため、認証局の要求する申請方法にしたがって手続きします。
2) 機器証明書の導入
Web Image Monitor を使用し、機器証明書を導入します。
3) SSL を有効にする
Web Image Monitor を使用し、［SSL/TLS］の設定を有効にします。

5

補足

・SSLの設定が有効になっているかどうかを確認するには､Webブラウザーのアドレスバーに「https://（本機の IP アドレス、またはホスト名）/」と入力し本機へのアクセスを行ってください。「ページを表示できません」と表示された場合は、SSL の設定が無効となっていますので、設定の内容を確認してください。

機器証明書の作成と導入（自己証明書）

Web Image Monitor を使用し、機器証明書を作成、導入します。
機器証明書に、自己証明書を利用する場合の説明です。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。

IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 ［ログイン］をクリックします。

ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 ［設定］をクリックし、「セキュリティー」の［機器証明書］をクリックします。

「機器証明書」エリアが表示されます。

5 作成する証明書番号を選択します。

6 [作成] をクリックします。

7 必要な設定項目を入力します。
表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。

8 [OK] をクリックします。
設定が書き換えられます。

9 [OK] をクリックします。
セキュリティーの警告に関するダイアログが表示されます。

10 内容を確認して [はい] をクリックします。
「証明書状態」に「導入済」が表示され、本機に機器証明書が導入されます。

11 [ログアウト] をクリックします。

補足

・本機から機器証明書を削除する場合は、[削除] をクリックします。

機器証明書の作成（認証局証明書）

Web Image Monitor を使用し、機器証明書を作成します。
機器証明書に、認証局証明書を利用する場合の説明です。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [機器証明書] をクリックします。
「機器証明書」エリアが表示されます。

5 作成する証明書番号を選択します。

6 [要求] をクリックします。

7 必要な設定項目を入力します。
表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。

8 [OK] をクリックします。
「機器証明書」エリアの「証明書状態」に「要求中」が表示されます。

9 [ログアウト] をクリックします。

10 機器証明書を認証局に申請します。
申請方法は、認証局により異なります。申請先の認証局に確認してください。
また、申請に必要な情報は、Web Image Monitor の詳細アイコンをクリックして表示される「証明書詳細」の内容を利用してください。

補足

- 2 つの証明書の申請を同時に行うと証明書の発行先が表示されないときがあります。導入する際に証明書の目的と導入順について確認してください。
- Web Image Monitor を使用して機器証明書を作成することができますが、申請できるものではありません。
- 機器証明書の要求を取りやめる場合は、[取りやめ要求] をクリックします。

5

機器証明書の導入（認証局証明書）

Web Image Monitor を使用し、機器証明書を導入します。
機器証明書に、認証局証明書を利用する場合の説明です。認証局から送られてきた機器証明書の内容を導入します。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [機器証明書] をクリックします。
「機器証明書」エリアが表示されます。

5 導入する証明書番号を選択します。

6 [導入] をクリックします。

7 機器証明書の内容を入力します。
「証明書要求」の入力ボックスに認証局から送られてきた機器証明書の内容を入力します。
表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。

8 [OK] をクリックします。
「証明書状態」に「導入済み」が表示され、本機に機器証明書が導入されます。

9 [ログアウト] をクリックします。

SSL を有効にする

本機に機器証明書を導入後、SSL の設定を有効にします。
この設定は、機器証明書が自己証明書を利用する場合、または認証局証明書を利用する場合のどちらにも共通の設定方法です。Web Image Monitor を使用し、管理者モードで設定します。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [SSL/TLS] をクリックします。
「SSL/TLS」エリアが表示されます。

5 「SSL/TLS」でご使用になるインターネットプロトコルのバージョンを [有効] に設定します。

6 「SSL/TLS 通信許可設定」から暗号化通信モードを選択します。

7 [OK] をクリックします。
SSL の設定が有効になります。

8 [OK] をクリックします。

9 [ログアウト] をクリックします。

補足

・「SSL/TLS 通信許可設定」を［暗号化のみ］に設定した場合、本機にアクセスするときは、「https://（本機の IP アドレス、またはホスト名）/」と入力します。

SSL（暗号化通信）のユーザーの設定

本機に機器証明書を導入し、SSL（暗号化通信）の設定を有効にしている場合、ユーザーの PC に証明書をインストールする必要があります。ネットワーク管理者から証明書のインストールについて、各ユーザーに伝えてください。
Web Image Monitor や IPP で本機にアクセスするとき、セキュリティーに関する警告ダイアログが表示された場合、各ブラウザーの操作にしたがって、証明書をインストールしてください。

補足

- 証明書の有効期限が切れているなどの問題でユーザーから問い合わせがある場合は、適切な対応をしてください。
- 本機に導入している機器証明書が認証局証明書の場合は、認証局に証明書ストアの場所を確認してください。
- IPP で本機にアクセスするときの証明書ストアの場所は、Web Image Monitor のヘルプを参照してください。

5

SSL/TLS 通信許可設定

SSL/TLS の暗号化通信モードを設定し、セキュリティーの強度を変更することができます。

♦ **暗号化通信モードについて**
暗号化通信モードによって暗号化通信を設定することができます。

暗号文のみ	暗号化通信のみを許可します。 暗号化できない場合は、通信できません。
暗号文優先	暗号化できる場合は、暗号化通信します。 暗号化できない場合は、平文で通信します。
暗号文／平文	暗号化、または平文の指定された方法で通信します。

暗号化通信モードの設定

ネットワーク管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
機器証明書を導入後、SSL/TLS の暗号化通信モードを設定します。
この設定により、セキュリティーの強度を変更することができます。

1. Web Image Monitorを起動し、ネットワーク管理者モードにログインします。
2. ［設定］をクリックします。
3. 「セキュリティー」の［SSL/TLS］をクリックします。

4 「SSL/TLS 通信許可設定」のドロップダウンメニューから暗号化通信モードを選択し、[OK] をクリックします。
暗号化通信モードは、[暗号文のみ]、[暗号文優先]、[暗号文 / 平文] のいずれかを選択します。

5 管理者モードからログアウトします。

6 Web Image Monitor を終了します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

SNMPv3 暗号化通信の設定

ネットワーク管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
Ridoc IO Admin などを使用し、各種の設定を行うときの通信データを暗号化通信することができます。
この設定により、通信データの改ざんを防止することができます。

1 Web Image Monitor を起動し、ネットワーク管理者モードにログインします。

2 [設定] をクリックします。

3 「ネットワーク」の [SNMPv3] をクリックします。

4 「SNMPv3 設定」の [SNMPv3 通信許可設定] から [暗号化のみ] を選択し、[OK] をクリックします。

5 管理者モードからログアウトします。

6 Web Image Monitor を終了します。

補足

・Ridoc IO Admin を使用し、各種の設定を行うときの通信データを暗号化するためには、本機の「SNMPv3 通信許可設定」の設定以外にネットワーク管理者の暗号パスワードの設定と Ridoc IO Admin の「SNMPv3 認証情報の入力」の暗号鍵の設定が必要です。
・ネットワーク管理者の暗号パスワードが設定されていない場合、通信データが暗号化されないことや、通信できないことがあります。
・ネットワーク管理者の暗号パスワードの設定については、「管理者を登録する」を参照してください。
・Ridoc IO Admin の暗号鍵の設定は、Ridoc IO Admin のヘルプを参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

・P.26 「管理者を登録する」

IPsec を使用して通信する

ネットワーク管理者が設定します。
本機には IPsec 機能が搭載されています。IPsec は IP プロトコルのレベルで、セキュアなパケット単位の通信を行います。暗号化には送信者、受信者が同じ鍵を保有する共通鍵暗号方式を使用します。本機は通信者双方に共通鍵を設定する方法として、手動鍵設定方式と自動鍵設定方式を搭載しています。自動鍵設定を使用すると、IPsec の共有鍵を設定した時間で更新し、よりセキュリティー強度の高い通信を行うことができます。

重要

- 「HTTPS 通信の除外」で［無効］を選択しているとき、誤った鍵設定を行うと、Web Image Monitor にアクセスすることができなくなります。アクセス不能となることを防ぐために HTTPS 通信を IPsec の除外対象に設定することができます。HTTPS 通信も IPsec の対象とする場合は、IPsec 機能が正しく設定されたことを確認したあとに、「HTTPS 通信の除外」で［無効］を選択することをお勧めします。「HTTPS 通信の除外」で［有効］を選択し、HTTPS 通信を IPsec の対象から外していても、PC 側で TCP が IPsec の対象となっているときは Web Image Monitor を使用できません。Web Image Monitor にアクセスできないときは、本体操作部の初期設定で IPsec 設定を無効に設定してからアクセスしてください。本体操作部による IPsec 無効設定の切り替え方法については、「操作部から IPsec を無効に設定す」を参照してください。
- DHCP、DNS、WINS で取得する情報、およびパケットについては、IPsec の対象にならないものがあります。
- IPsec に対応している OS は Windows XP SP2、Windows Vista、Mac OS X 10.4 以降、RedHat Linux Enterprise WS 4.0、Solaris 10 です。ただし、OS によって対応していない設定項目があります。IPsec の設定を行うときは、かならず OS 側の IPsec 設定内容を確認し、同一の設定を行ってください。

参照

・P.127 「操作部から IPsec を無効に設定する」

IPsec が実現する通信データの暗号化と認証

IPsec には、データの機密性を確保する「暗号化」機能と、データ送信者が正しいこと、またデータが改ざんされていないことを証明する「認証」機能の 2 つの機能が存在します。本機の IPsec 機能は、2 つの機能を同時に有効にする ESP プロトコルと認証のみの機能を有効にする AH プロトコルの 2 つのセキュリティープロトコルに対応しています。

♦ ESP プロトコル

データの暗号化と認証の両方に対応したセキュリティー通信を行います。

- 暗号化を行うためには送信側、受信側ともに同一の暗号化アルゴリズムと暗号鍵を設定する必要があります。自動鍵設定のとき、暗号化アルゴリズムと暗号鍵は自動的に設定されます。

・認証を行うためには送信側、受信側ともに同一の認証アルゴリズムと認証鍵を設定する必要があります。自動鍵設定のとき、認証アルゴリズムと認証鍵は自動的に設定されます。

♦ AH プロトコル

認証のみに対応したセキュリティー通信を行います。

・認証を行うためには送信側、受信側ともに同一の認証アルゴリズムと認証鍵を設定する必要があります。自動鍵設定のとき、認証アルゴリズムと認証鍵は自動的に設定されます。

補足

・お使いの OS によっては、「認証」は「整合性」という名称を使用していることがあります。

自動鍵設定と手動鍵設定

本機は鍵の設定方式として、自動鍵設定、手動鍵設定の 2 種類に対応しています。鍵設定によって、IPsec 通信に使用するアルゴリズムや鍵などの約束事を送信者、受信者双方に設定します。この約束事を SA(Security Association) と呼びます。送信者、受信者で SA 設定内容が一致していないと IPsec 通信を行うことができません。

自動鍵設定方式では、SA の設定が自動的に行われますが、最初に ISAKMP SA が自動設定（フェーズ 1）され、続いて IPsec 通信のための IPsec SA が自動設定（フェーズ 2）されます。また、より高いセキュリティーを確保した通信を行うために、設定の有効期間を定めることで SA の定期的な自動更新を可能にします。本機の自動鍵設定方式は IKEv1 のみ対応しています。

手動鍵設定方式では、事前に送信者、受信者で IPsec 通信のための IPsec SA 情報を共有しそれぞれに設定します。この場合、鍵情報の漏洩を防ぐために、情報の交換はネットワークを使用せずに行うことをお勧めします。

自動鍵設定、手動鍵設定ともに、SA の設定を複数設定することができます。

♦ 個別設定とデフォルト設定

自動鍵設定、手動鍵設定ともに、IPsec で使用するアルゴリズムや鍵などの SA 設定を個別に 4 種類設定することができます。また個別設定に含まれない通信相手を対象としたデフォルト設定を別途設定することも可能です。個別設定の優先度は 1 が最も高く 4 が最も低くなります。優先度の低い個別設定で設定対象となる IP アドレス範囲を指定し、その範囲内の特定の通信者のみを対象とした個別設定を行いたいときは、上位の個別設定でその通信者のみを指定して設定を行うと上位の設定が有効になります。

IPsec 設定の設定項目

本機での IPsec 設定は Web Image Monitor を使用して行います。ここでは設定項目について説明します。

♦ 自動鍵設定／手動鍵設定共通設定項目

設定項目	設定内容	設定値
IPsec	IPsec 機能を有効にするか無効にするか設定します。	・有効 ・無効

設定項目	設定内容	設定値
HTTPS 通信の除外	HTTPS 通信を IPsec から除外するかしないかを設定します。	・有効 ・無効 HTTPS通信をIPsecの対象から外す場合は有効を選択します。
手動鍵設定	手動鍵設定を有効にするか無効にするか設定します。	・有効 ・無効 手動鍵設定を使用する場合は有効を選択します。

♦ 自動鍵設定のセキュリティーレベル

自動鍵設定では、セキュリティーレベルの項目を選択すると、セキュリティー詳細項目はレベルに応じて自動設定されます。
各セキュリティーレベルの特徴は以下のとおりです。

セキュリティーレベル	セキュリティーレベルの特徴
認証のみ	パケットデータの暗号化は行わず、通信相手の認証とデータの改ざん防止のみを行うときに選択します。パケット単位のデータは平文のままネットワークを流れるため、盗聴される危険性があります。
認証と暗号化（低）	通信相手の認証と改ざん防止に加え、パケットデータの暗号化を行うときに選択します。「認証と暗号化（高）」よりもセキュリティーの強度は低い設定になります。
認証と暗号化（高）	通信相手の認証と改ざん防止に加え、パケットデータの暗号化を行うときに選択します。「認証と暗号化（低）」よりもセキュリティー強度の高い設定になります。

セキュリティーレベル選択時の自動設定値は以下のとおりです。

設定項目	各セキュリティーレベル選択時の設定値		
	認証のみ	認証と暗号化（低）	認証と暗号化（高）
処理方法	apply	apply	apply
カプセル化モード	トランスポートモード	トランスポートモード	トランスポートモード
IPsec 要求レベル	可能な場合に使用する	可能な場合に使用する	必須
認証方式	PSK	PSK	PSK
フェーズ 1 ハッシュアルゴリズム	MD5	SHA1	SHA1
フェーズ 1 暗号化アルゴリズム	DES	3DES	3DES
フェーズ 1 Diffie-Hellmanグループ	2	2	2
フェーズ 2 セキュリティープロトコル	AH	ESP	ESP

設定項目	各セキュリティーレベル選択時の設定値		
	認証のみ	認証と暗号化（低）	認証と暗号化（高）
フェーズ 2 認証アルゴリズム	HMAC-MD5-96 ／ HMAC-SHA1-96	HMAC-MD5-96 ／ HMAC-SHA1-96	HMAC-SHA1-96
フェーズ 2 暗号化アルゴリズム	平文（NULL 暗号）	DES ／ 3DES ／ AES-128 ／ AES-192 ／ AES-256	3DES ／ AES-128 ／ AES-192 ／ AES-256
フェーズ 2 PFS	無効	無効	2

♦ 自動鍵設定の設定項目

セキュリティーレベルの項目を選択することで、セキュリティー詳細項目は自動設定されますが、アドレスタイプや、ローカルアドレス、リモートアドレスの入力は必須です。認証にまたセキュリティーレベルの項目を選択することで自動設定される設定内容を部分的に手動で変更することも可能です。自動設定された内容を変更した場合、セキュリティーレベルは自動的に「ユーザー設定」の表示に切り替わります。

設定項目	設定内容	設定値
アドレスタイプ	IPsec の対象とする IP アドレスのタイプを選択します。	・無効 ・IPv4 ・IPv6
ローカルアドレス	機器のアドレスを設定します。IPv6 で複数のアドレスを使用しているときには、範囲指定することもできます。	機器の IPv4、または IPv6 のアドレス 範囲指定設定しない場合、IPv4 アドレスはアドレスの後に 32 を入力し、IPv6 アドレスはアドレスの後に 128 を入力します。
リモートアドレス	IPsec 通信対象となる相手先のアドレスを指定します。範囲を指定することもできます。	通信相手の IPv4、または IPv6 のアドレス 範囲指定設定しない場合、IPv4 アドレスはアドレスの後に 32 を入力し、IPv6 アドレスはアドレスの後に 128 を入力します。

設定項目	設定内容	設定値
カプセル化モード	カプセル化モードを選択します。 （自動設定対象項目）	・トランスポート ・トンネル （トンネル始点 IP アドレス－トンネル終点 IP アドレス） セキュリティーレベルに関係なくトランスポートモードが選択されます。 トンネルモードを選択したときは、トンネルエンドポイントで始点 IP アドレスと終点 IP アドレスを指定します。 トンネルエンドポイントの始点 IP アドレスとローカルアドレスは同一の値を設定します。
IPsec 要求レベル	通信相手と IPsec による通信のみを行うか、IPsec が確立できない場合、平文による通信を行うかを選択します。 （自動設定対象項目）	・可能な場合に使用する ・必須
認証方式	通信相手の認証を行う方式を選択します。 （自動設定対象項目）	・PSK ・証明書 セキュリティーレベルに関係なく「PSK」方式が選択されます。 「PSK」を使用する場合は PSK の文字列（アスキー文字列で 32 文字以内）を設定します。 「証明書」を選択する場合は、事前に機器証明書を導入し、IPsec 用の証明書を割り当てておく必要があります。
フェーズ 1 ハッシュアルゴリズム	フェーズ1で使用するハッシュアルゴリズムを選択します。 （自動設定対象項目）	・MD5 ・SHA1
フェーズ 1 暗号化アルゴリズム	フェーズ1で使用する暗号化アルゴリズムを選択します。 （自動設定対象項目）	・DES ・3DES
フェーズ 1 Diffie-Hellman グループ	Diffie-Hellman グループ番号を選択します。 （自動設定対象項目）	・1 ・2
フェーズ 1 有効期間	フェーズ 1 で使用する SA の有効期間を設定します。	300 秒（5 分）～ 172800 秒（48 時間）の間で秒単位で設定します。

設定項目	設定内容	設定値
フェーズ 2 セキュリティープロトコル	フェーズ 2 で使用するセキュリティープロトコルを選択します。 （自動設定対象項目）	・AH ・ESP ・AH ＋ ESP
フェーズ 2 認証アルゴリズム	フェーズ2で使用する認証アルゴリズムを選択します。 （自動設定対象項目）	・HMAC-MD5-96 ・HMAC-SHA1-96
フェーズ 2 暗号化アルゴリズム	フェーズ2で使用する暗号化アルゴリズムを選択します。 （自動設定対象項目）	・平文（NULL 暗号） ・DES ・3DES ・AES-128 ・AES-192 ・AES-256
フェーズ 2 PFS	PFS の有効 / 無効と有効時の Diffie-Hellman グループ番号を選択します。 （自動設定対象項目）	・無効 ・1 ・2 ・14
フェーズ 2 有効期間	フェーズ 2 で使用する SA の有効期間を設定します。	300 秒（5 分）～ 172800 秒（48 時間）の間で秒単位で設定します。

♦ 手動鍵設定の設定項目

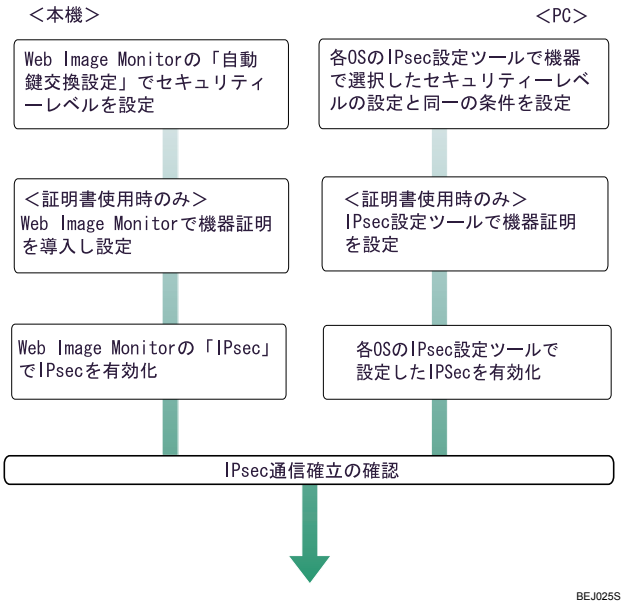
設定項目	設定内容	設定値
アドレスタイプ	IPsec の対象とする IP アドレスのタイプを選択します。	・無効 ・IPv4 ・IPv6
ローカルアドレス	機器のアドレスを設定します。IPv6 で複数のアドレスを使用しているとき、範囲指定することもできます。	機器の IPv4、または IPv6 のアドレス 範囲指定設定しない場合、IPv4 アドレスはアドレスの後に 32 を入力し、IPv6 アドレスはアドレスの後に 128 を入力します。
リモートアドレス	IPsec 通信対象となる相手先のアドレスを指定します。範囲を指定することもできます。	通信相手の IPv4、または IPv6 のアドレス 範囲指定設定しない場合、IPv4 アドレスはアドレスの後に 32 を入力し、IPv6 アドレスはアドレスの後に 128 を入力します。

設定項目	設定内容	設定値
カプセル化モード	カプセル化モードを選択します。	・トランスポート ・トンネル （トンネル始点IPアドレスートンネル終点 IP アドレス） トンネルモードを選択したときは、トンネルエンドポイントで始点 IP アドレスと終点IPアドレスを指定します。トンネルエンドポイントの始点IPアドレスとローカルアドレスは同一の値を設定します。
SPI 値（出力）	通信相手先の入力の SPI 値と同一の値を設定します。	256 ～ 4095 の間の任意の整数値
SPI 値（入力）	通信相手先の出力の SPI 値と同一の値を設定します。	256 ～ 4095 の間の任意の整数値
セキュリティープロトコル	暗号化と認証を同時に行う場合は ESP を、認証のみを行う場合は AH を選択します。	・ESP ・AH
認証アルゴリズム	認証に使用するアルゴリズムを選択します。	・HMAC-MD5-96 ・HMAC-SHA1-96
認証鍵	認証アルゴリズムの鍵を設定します。	認証アルゴリズムによって以下の長さの任意の値を設定します。 ＜ 16 進数の場合＞ 半角の 0 ～ 9、a ～ f、A ～ F ・HMAC-MD5-96 選択時 32 桁 ・HMAC-SHA1-96 選択時 40 桁 ＜アスキー文字列の場合＞ ・HMAC-MD5-96 選択時 16 文字 ・HMAC-SHA1-96 選択時 20 文字
暗号化アルゴリズム	暗号化に使用するアルゴリズムを選択します。	・平文（NULL 暗号） ・DES ・3DES ・AES-128 ・AES-192 ・AES-256

設定項目	設定内容	設定値
暗号鍵	暗号化アルゴリズムの鍵を指定します。	認証アルゴリズムによって以下の長さの任意の値を設定します。 ＜16 進数の場合＞ 半角の 0 ～ 9、a ～ f、A ～ F ・DES 選択時 16 桁 ・3DES 選択時 48 桁 ・AES-128 選択時 32 桁 ・AES-192 選択時 48 桁 ・AES-256 選択時 64 桁 ＜アスキー文字列の場合＞ ・DES 選択時 8 文字 ・3DES 選択時 24 文字 ・AES-128 選択時 16 文字 ・AES-192 選択時 24 文字 ・AES-256 選択時 32 文字

自動鍵設定のながれ

自動鍵設定の設定手順を説明します。ネットワーク管理者が設定します。



重要

・自動鍵設定で通信相手の認証方法に証明書を使用する場合は、機器証明書の導入が必要です。

・IPsec 設定後、正しく通信が確立されているかどうかの確認は Ping コマンドを使用して確認することができます。ただし、ICMP が IPsec の除外対象になっているときは Ping コマンドを使用できません。また、鍵交換設定中は応答がないため、通信確立の確認に時間がかかることがあります。

■自動鍵設定の設定手順

Web Image Monitor を使用して設定します。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [IPsec] をクリックします。
「IPsec」エリアが表示されます。

5 「自動鍵設定」の [編集] をクリックします。

6 「個別設定 1」で自動鍵設定の条件を設定します。
複数の個別設定条件を設定する場合は、個別設定番号を切り替えて追加設定します。

7 [OK] をクリックします。

8 「IPsec」の「IPsec:」で [有効] を選択します。

9 「HTTPS通信の除外:」でHTTPS通信をIPsecの除外対象とするときは[有効] を選択します。

10 [OK] をクリックします。

11 [ログアウト] をクリックします。

補足

・自動鍵設定の条件設定で送信相手の認証方式を「証明書」に変更する場合、事前に証明書の導入と割り当てを行ってください。証明書の作成・導入については、「S/MIME を利用してメール送信を保護する」の機器証明書の作成方法、導入方法を参照してください。導入した証明書を IPsec に割り当てる方法については、「証明書を選択する」を参照してください。

参照

・P.117 「証明書を選択する」

■証明書を選択する

Web Image Monitor を使用し、IPsec で使用する証明書を設定します。

1 Web ブラウザーを起動します。

2 Web ブラウザーのアドレスバーに「http://（本機の IP アドレス、またはホスト名）/」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティー」の [機器証明書] をクリックします。
「機器証明書」エリアが表示されます。

5 「利用する証明書」の「IPsec」の欄で、使用する証明書を選択します。

6 [OK] を 2 回クリックします。

7 [ログアウト] をクリックします。

■PC で IPsec の条件を設定する

機器で選択したセキュリティーレベルの IPsec SA 設定と同一の条件を PC 側で設定します。設定方法は OS によって異なります。ここではセキュリティーレベルで「認証と暗号化（低）」を選択したときの Windows XP 側の設定を例に説明します。

1 [スタート] メニューから [コントロールパネル] ー [パフォーマンスとメンテナンス] ー [管理ツール] をクリックします。

2 [ローカルセキュリティポリシー] をダブルクリックします。

3 [ローカルコンピュータの IP セキュリティポリシー] をクリックします。

4 [操作]メニューから[IP セキュリティポリシーの作成]をクリックします。
「IP セキュリティポリシーウィザード」が表示されます。

5 [次へ] をクリックします。

6 任意の IP セキュリティポリシー名を入力し、[次へ] をクリックします。

7 「既定の応答規則をアクティブにする」のチェックを外し、[次へ] をクリックします。

8 「プロパティを編集する」にチェックを入れ、[完了] をクリックします。

9 ［全般］タブを選択し、［詳細設定］をクリックします。

10 「新しいキーを認証して生成する間隔」に機器の自動鍵設定のフェーズ 1 で設定した有効期間を分単位で入力し、［メソッド］をクリックします。

11 機器の自動鍵設定のフェーズ 1 で選択されているハッシュアルゴリズム（Windows XP では整合性）、暗号化アルゴリズム（Windows XP では暗号化）、Diffie-Hellman グループの組み合わせが「キー交換のセキュリティメソッド」に存在しているか確認します。
存在しない場合は［追加］をクリックし作成します。

12 ［OK］を 2 回クリックします。

13 ［規則］タブを選択し、［追加］をクリックします。
「セキュリティーの規則ウィザード」が表示されます。

14 ［次へ］をクリックします。

15 「この規則ではトンネルを使用しない」にチェックを入れ、［次へ］をクリックします。

16 IPsec を適用するネットワークの種類を選択し、［次へ］をクリックします。

17 認証方法を選択して［次へ］をクリックします。
機器の自動鍵設定の認証方法で証明書を選択している場合は、機器証明書を設定します。PSK を選択している場合は、事前共有キーとして機器で設定した PSK と同じ文字列を入力します。

18 IP フィルター一覧で［追加］をクリックします。

19 「名前」に任意の IP フィルタ名を入力し、［追加］をクリックします。
「IP フィルタウィザード」が表示されます。

20 ［次へ］をクリックします。

21 「発信元アドレス」で「このコンピュータの IP アドレス」を選択し、［次へ］をクリックします。

22 「宛先アドレス」で「特定の IP アドレス」を選択し、機器の IP アドレスを入力して［次へ］をクリックします。

23 IPsec の対象とするプロトコルを選択し、［次へ］をクリックします。

24 ［完了］をクリックします。

25 ［OK］をクリックします。

26 設定した IP フィルタを選択し、［次へ］をクリックします。

27 フィルタ操作の種類を選択し、[編集] をクリックします。

28 [追加] をクリックし、「カスタム」にチェックを入れて [設定] をクリックします。

29 「整合性アルゴリズム」で機器の自動鍵設定のフェーズ 2 で選択されている認証アルゴリズムを選択します。

30 「暗号化アルゴリズム」で機器の自動鍵設定のフェーズ 2 で選択されている暗号化アルゴリズムを選択します。

31 「セッションのキーの設定」で「新しいキーの生成間隔（R)」にチェックを入れ、機器の自動鍵設定のフェーズ 2 で設定した有効期間を秒単位で入力します。

32 [OK] を 3 回クリックします。

33 [次へ] をクリックします。

34 [完了] をクリックします。

35 [閉じる] をクリックします。
新しい IP セキュリティーポリシー（IPsec 設定）が設定されます。

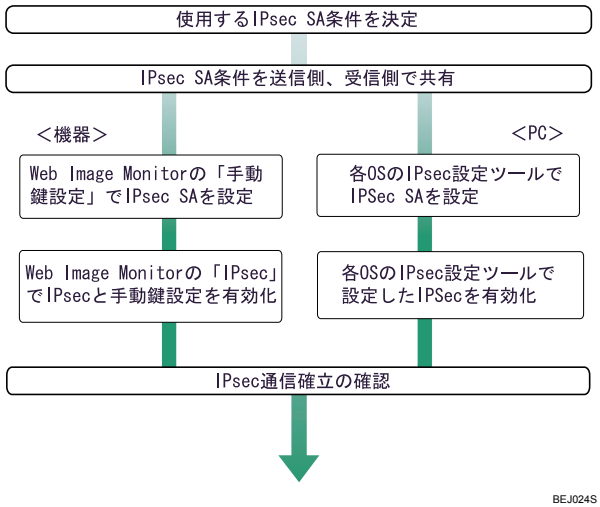
36 設定したセキュリティーポリシー名を選択し、右クリックして [割り当て] をクリックします。
PC の IPsec 設定が有効になります。

補足

・PC の IPsec を無効にするときは、設定したセキュリティーポリシー名を選択し、右クリックして [割り当ての解除] をクリックします。

手動鍵設定のながれ

手動鍵設定の設定手順を説明します。ネットワーク管理者が設定します。



重要

- 事前に送信者、受信者で IPsec 通信のための IPsec SA 情報を共有しそれぞれに設定します。この場合、IPsec SA の漏洩を防ぐために、情報の交換はネットワークを使用せずに行うことをお勧めします。
- IPsec 設定後、正しく通信が確立されているかどうかの確認は Ping コマンドを使用して確認することができます。ただし、ICMP が IPsec の除外対象になっているときは Ping コマンドを使用できません。また、鍵交換設定中は応答がないため、通信確立の確認に時間がかかることがあります。

■手動鍵設定の設定手順

Web Image Monitor を使用して設定します。

1 **Web ブラウザーを起動します。**

2 **Web ブラウザーのアドレスバーに「http:// (本機の IP アドレス、またはホスト名) /」と入力し、本機にアクセスします。**

IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。「192.168.001.010」と入力すると、本機に接続できません。

3 **[ログイン] をクリックします。**

ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 **[設定] をクリックし、「セキュリティー」の [IPsec] をクリックします。**

「IPsec」エリアが表示されます。

5 **「手動鍵設定 :」で [有効] を選択します。**

6 「手動鍵設定」の［編集］をクリックします。

7 「個別設定 1」で手動鍵設定の条件を設定します。
複数の個別設定条件を設定する場合は、個別設定番号を切り替えて追加設定します。

8 ［OK］をクリックします。

9 「IPsec」の「IPsec:」で［有効］を選択します。

10 「HTTPS通信の除外:」でHTTPS通信をIPsecの除外対象とするときは[有効］を選択します。

11 ［OK］をクリックします。

12 ［ログアウト］をクリックします。

telnet で IPsec を設定する

本機では、Web Image Monitor のほかに、telnet を使用して IPsec 設定の内容確認、設定変更を行うことができます。ここでは IPsec に関連するコマンドを説明します。telnet を使用するとき、管理者としてログインする場合のユーザー名の初期値は admin、パスワードの初期値は空です。telnet のログイン方法、操作方法については、『ソフトウエアガイド』「機器の監視」を参照してください。

重要

・自動鍵設定（IKE）で認証方式に証明書を使用するときは、Web Image Monitor で証明書の導入設定を行ってください。telnet は証明書の導入に対応していません。

IPsec 関連の設定情報を表示するときは、「ipsec」コマンドを使用します。

♦ **現在の設定の表示**
msh> ipsec
・以下の IPsec 関連の設定情報がすべて表示されます。
IPsec 共通設定の設定値
手動鍵設定の個別 SA 設定値
手動鍵設定のデフォルト SA 設定値
自動鍵設定の個別 IKE 設定値
自動鍵設定のデフォルト IKE 設定値

♦ **現在の設定の分割表示**
msh> ipsec -p
・IPsec 関連の設定情報を分割して表示します。

手動鍵設定の表示・設定は、「ipsec manual_mode」コマンドを使用します。

♦ **現在の設定の表示**
msh> ipsec manual_mode
・手動鍵設定の設定情報が表示されます。

♦ 手動鍵設定の設定

msh> ipsec manual_mode {on|off}

・手動鍵設定を有効にするには「on」を、無効にするには「off」を指定します。

IPsec 除外対象プロトコルの表示・設定は、「ipsec exclude」コマンドを使用します。

♦ 現在の設定の表示

msh> ipsec exclude

・現在の除外対象プロトコルが表示されます。

♦ 除外対象プロトコルの設定

msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}

・設定するプロトコルを指定し、除外対象とするときは「on」を、除外対象にしないときは「off」を指定します。プロトコルで「all」を指定するとすべてのプロトコルの設定が一括で行えます。

手動鍵設定の SA 設定の表示・設定は、「ipsec manual」コマンドを使用します。

♦ 現在の設定の表示

msh> ipsec manual {1|2|3|4|default}

・個別設定の設定内容を表示するときは個別設定番号「1 ～ 4」を指定します。
・デフォルト設定の設定内容を表示するときは「default」を指定します。
・設定値を省略した場合、個別設定 1 ～ 4 とデフォルト設定の設定情報がすべて表示されます。

♦ 設定の無効化

msh> ipsec manual {1|2|3|4|default} disable

・設定を無効化する個別設定番号「1 ～ 4」を指定します。
・デフォルト設定を無効に設定するときは「default」を指定します。

♦ 個別設定のローカル／リモートアドレスの設定

msh> ipsec manual {1|2|3|4} {ipv4|ipv6} ローカルアドレス リモートアドレス

・個別設定番号を指定し、使用するアドレスタイプを指定した上で、ローカルアドレスとリモートアドレスを指定します。
・ローカルアドレス、リモートアドレスの値は、アドレスタイプが IPv4 の場合、アドレスの後に「/」を入れて 0-32 の整数値で「masklen」を指定します。アドレスタイプが IPv6 の場合、アドレスの後に「/」を入れて 0-128 の整数値で「masklen」を指定します。
・アドレスの指定値を省略したときは、現在の設定が表示されます。

♦ デフォルト設定のアドレスタイプの設定

msh> ipsec manual default {ipv4|ipv6|any}

・デフォルト設定のアドレスタイプを指定します。
・IPv4 と IPv6 の両方のアドレスタイプを指定する場合は「any」を指定します。

♦ セキュリティープロトコルの設定

msh> ipsec manual {1|2|3|4|default} proto {ah|esp|dual}

・個別設定番号、またはデフォルト設定を指定し、使用するセキュリティープロトコルを指定します。
・AH を使用するときは「ah」、ESP を使用するときは「esp」、AH ＋ ESP を使用するときは「dual」を指定します。
・セキュリティープロトコルの指定値を省略したときは、現在の設定が表示されます。

♦ SPI 値の設定

msh> ipsec manual {1|2|3|4|default} spi 出力方向の SPI 値 入力方向の SPI 値

・個別設定番号、またはデフォルト設定を指定し、出力方向 / 入力方向の SPI 値を指定します。
・出力方向、入力方向ともに、SPI 値は 256 ～ 4095 の間の 10 進数で指定します。
・SPI 値の指定を省略したときは、現在の設定が表示されます。

♦ カプセル化モードの設定

msh> ipsec manual {1|2|3|4|default} mode {transport|tunnel}

・個別設定番号、またはデフォルト設定を指定し、カプセル化モードを設定します。
・トランスポートモードを使用するときは「transport」、トンネルモードを使用するときは「tunnel」を指定します。
・デフォルト設定のアドレスタイプで「any」を指定しているときは、カプセル化モードに「tunnel」を指定することはできません。

♦ トンネルモードの始点 / 終点 IP アドレスの設定

msh> ipsec manual {1|2|3|4|default} tunneladdar 始点 IP アドレス 終点 IP アドレス

・個別設定番号、またはデフォルト設定を指定し、トンネルモードの始点 IP アドレスと終点 IP アドレスを指定します。
・始点 / 終点 IP アドレスの両方の指定値を省略したときは、現在の設定が表示されます。

♦ 認証アルゴリズムと認証鍵の設定

msh> ipsec manual {1|2|3|4|default} auth {hmac-md5|hmac-sha1} 認証鍵

・個別設定番号、またはデフォルト設定を指定し、認証アルゴリズムを指定した上で、認証鍵を指定します。
・認証鍵を 16 進数で設定するときは、先頭に 0x を付加して指定します。
・認証鍵をアスキー文字列で指定するときは、そのまま指定します。
・認証アルゴリズムと認証鍵の両方の指定値を省略したときは、現在の設定が表示されます。（認証鍵は非表示）

♦ 暗号アルゴリズムと暗号鍵の設定

msh> ipsec manual {1|2|3|4|default} encrypt {null|des|3des|aes128|aes192|aes256} 暗号鍵

・個別設定番号、またはデフォルト設定を指定し、暗号アルゴリズムを指定した上で、暗号鍵を指定します。
・暗号鍵を 16 進数で設定するときは、先頭に 0x を付加して指定します。暗号アルゴリズムで「null」を選択した場合は、2 ～ 64 桁の任意の長さの暗号鍵を指定してください。
・暗号鍵をアスキー文字列で指定するときは、そのまま指定します。暗号アルゴリズムで「null」を選択した場合は、1 ～ 32 文字の任意の長さの暗号鍵を指定してください。
・暗号アルゴリズムと暗号鍵の両方の指定値を省略したときは、現在の設定が表示されます。（暗号鍵は非表示）

♦ **手動鍵（manual）設定値の初期化**

msh> ipsec manual {1|2|3|4|default|all} clear

・設定値を初期化する個別設定番号、またはデフォルト設定を指定します。「all」を指定するとすべての個別設定とデフォルト設定を初期化します。

自動鍵設定の SA 設定の表示・設定は、ipsec ike コマンドを使用します。

♦ **現在の設定の表示**

msh> ipsec ike {1|2|3|4|default}

・個別設定の設定内容を表示するときは個別設定番号「1 ～ 4」を指定します。
・デフォルト設定の設定内容を表示するときは「default」を指定します。
・設定値を省略した場合、個別設定 1 ～ 4 とデフォルト設定の設定情報がすべて表示されます。

♦ **設定の無効化**

msh> ipsec ike {1|2|3|4|default} disable

・設定を無効化する個別設定番号「1 ～ 4」を指定します。
・デフォルト設定を無効に設定するときは「default」を指定します。

♦ **個別設定のローカル／リモートアドレスの設定**

msh> ipsec ike {1|2|3|4} {ipv4|ipv6} ローカルアドレス リモートアドレス

・個別設定番号を指定し、使用するアドレスタイプを指定した上で、ローカルアドレスとリモートアドレスを指定します。
・ローカルアドレス、リモートアドレスの値は、アドレスタイプが IPv4 の場合、アドレスの後に「/」を入れて 0-32 の整数値で「masklen」を指定します。アドレスタイプが IPv6 の場合、アドレスの後に「/」を入れて 0-128 の整数値で「masklen」を指定します。
・アドレスの指定値を省略したときは、現在の設定が表示されます。

♦ **デフォルト設定のアドレスタイプの設定**

msh> ipsec ike default {ipv4|ipv6|any}

・デフォルト設定のアドレスタイプを指定します。
・IPv4 と IPv6 の両方のアドレスタイプを指定する場合は「any」を指定します。

♦ **処理方法の設定**

msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}

・個別設定番号、またはデフォルト設定を指定し、指定したアドレスに該当するパケットの処理方法を指定します。
・該当するパケットに対して IPsec を適用するときは、「apply」を指定し、IPsec を適用しないときは、「bypass」を指定します。
・該当するパケットを破棄するときは、「discard」を指定します。
・処理方法の指定値を省略したときは、現在の設定が表示されます。

♦ **セキュリティープロトコルの指定**

msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}

・個別設定番号、またはデフォルト設定を指定し、使用するセキュリティープロトコルを指定します。
・AH を使用するときは「ah」、ESP を使用するときは「esp」、AH ＋ ESP を使用するときは「dual」を指定します。
・セキュリティープロトコルの指定値を省略したときは、現在の設定が表示されます。

♦ 要求レベルの設定

msh> ipsec ike {1|2|3|4|default} level {require|use}

・個別設定番号、またはデフォルト設定を指定し、IPsec の要求レベルを指定します。
・「require」を指定すると、IPsec が利用できないときには通信ができません。「use」を指定すると、IPsec が利用できないときには通常の通信を行い、IPsec が利用可能なときには IPsec 通信を行います。
・要求レベルの指定値を省略したときは、現在の設定が表示されます。

♦ カプセル化モードの設定

msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}

・個別設定番号、またはデフォルト設定を指定し、カプセル化モードを設定します。
・トランスポートモードを使用するときは「transport」、トンネルモードを使用するときは「tunnel」を指定します。
・デフォルト設定のアドレスタイプで「any」を指定しているときは、カプセル化モードに「tunnel」を指定することはできません。
・カプセル化モードの指定値を省略したときは、現在の設定が表示されます。

♦ トンネルモードの始点 / 終点 IP アドレスの設定

msh> ipsec ike {1|2|3|4|default} tunneladdar 始点 IP アドレス 終点 IP アドレス

・個別設定番号、またはデフォルト設定を指定し、トンネルモードの始点 IP アドレスと終点 IP アドレスを指定します。
・始点 / 終点 IP アドレスの指定値を省略したときは、現在の設定が表示されます。

♦ IKE の相手認証方式の設定

msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}

・個別設定番号、またはデフォルト設定を指定し、相手認証方式を指定します。
・事前共有鍵による認証方式を使用するときは「psk」を指定し、証明書による認証方式を使用するときは「rsasig」を指定します。
証明書による認証方式を使用するときは、事前に機器証明書を導入し、IPsec 用の証明書を割り当てておく必要があります。機器証明書の導入は Web Image Monitor を使用して設定します。
・「psk」を指定したときは、PSK 文字列の設定が必要です。

♦ PSK 文字列の設定

msh> ipsec ike {1|2|3|4|default} psk PSK 文字列

・相手認証方式で PSK を選択しているとき、個別設定番号またはデフォルト設定を指定し、PSK 文字列を指定します。
・PSK 文字列はアスキー文字（32 文字以内）で指定します。省略することはできません。

♦ ISAKMP SA（フェーズ 1）のハッシュアルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1}

・個別設定番号、またはデフォルト設定を指定し、ISAKMP SA（フェーズ 1）で使用するハッシュアルゴリズムを指定します。
・MD5 を使用するときは「md5」を指定し、SHA1 を使用するときは「sha1」を指定します。
・ハッシュアルゴリズムの指定値を省略したときは、現在の設定が表示されます。

♦ ISAKMP SA（フェーズ 1）の暗号アルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des}

・個別設定番号、またはデフォルト設定を指定し、ISAKMP SA（フェーズ 1）で使用する暗号アルゴリズムを指定します。
・DES を使用するときは「des」を指定し、3DES を使用するときは「3des」を指定します。
・暗号アルゴリズムの指定値を省略したときは、現在の設定が表示されます。

♦ ISAKMP SA（フェーズ 1）の Diffie-Hellman グループ番号の設定

msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}

・個別設定番号、またはデフォルト設定を指定し、ISAKMP SA（フェーズ 1）で使用する Diffie-Hellman グループ番号を指定します。
・使用するグループ番号を番号数値で指定します。
・グループ番号の指定値を省略したときは、現在の設定が表示されます。

♦ ISAKMP SA（フェーズ 1）の有効期間の設定

msh> ipsec ike {1|2|3|4|default} ph1 lifetime 有効期間

・個別設定番号、またはデフォルト設定を指定し、ISAKMP SA（フェーズ 1）の有効期間を指定します。
・有効期間は秒単位で 300 ～ 172800 の間の整数値で指定します。
・有効期間の指定値を省略したときは、現在の設定が表示されます。

♦ IPsec SA（フェーズ 2）の認証アルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1}

・個別設定番号、またはデフォルト設定を指定し、IPsec SA（フェーズ 2）で使用する認証アルゴリズムを指定します。
・複数の認証アルゴリズムを指定するときは（,）で区切って指定します。このとき、現在の設定値表示は優先順位の高いアルゴリズムから表示されます。
・認証アルゴリズムの指定値を省略したときは、現在の設定が表示されます。

♦ IPsec SA（フェーズ 2）の暗号アルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|aes256}

・個別設定番号、またはデフォルト設定を指定し、IPsec SA（フェーズ 2）で使用する暗号アルゴリズムを指定します。
・複数の暗号アルゴリズムを指定するときは（,）で区切って指定します。このとき、現在の設定値表示は優先順位の高いアルゴリズムから表示されます。
・暗号アルゴリズムの指定値を省略したときは、現在の設定が表示されます。

♦ IPsec SA（フェーズ 2）の PFS の設定

msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}

・個別設定番号、またはデフォルト設定を指定し、IPsec SA（フェーズ 2）の PFS で使用する Diffie-Hellman グループ番号を指定します。
・使用するグループ番号を番号数値で指定します。
・グループ番号の指定値を省略したときは、現在の設定が表示されます。

♦ IPsec SA（フェーズ 2）の有効期間の設定

msh> ipsec ike {1|2|3|4|default} ph2 lifetime 有効期間

・個別設定番号、またはデフォルト設定を指定し、IPsec SA（フェーズ 2）の有効期間を指定します。
・有効期間は秒単位で 300 ～ 172800 の間の整数値で指定します。
・有効期間の指定値を省略したときは、現在の設定が表示されます。

♦ 自動鍵（ike）設定値の初期化

msh> ipsec ike {1|2|3|4|default|all} clear

・設定値を初期化する個別設定番号、またはデフォルト設定を指定します。「all」を指定するとすべての個別設定とデフォルト設定を初期化します。

操作部から IPsec を無効に設定する

1 ［メニュー］キーを押します。

2 ［▲］［▼］キーを押して［インターフェース設定］を選択し、［OK］キーを押します。

3 ［▲］［▼］キーを押して［ネットワーク設定］を選択し、［OK］キーを押します。

4 ［▲］［▼］キーを押して［IPsec］を選択し、［OK］キーを押します。

5 ［▲］［▼］キーを押して［無効］を選択し、［OK］キーを押します。

telnet 接続時の認証について

telnet を使用するとき、管理者としてログインする場合のユーザー名の初期値は admin、パスワードの初期値は空です。telnet のログイン方法、操作方法については、『ソフトウエアガイド』「機器の監視」を参照してください。

authfree コマンドについて

telnet で authfree コマンドを使用すると、プリンタージョブ認証時の認証を除外する IP アドレス範囲設定を行うことができます。認証除外制御の表示と設定方法は以下のとおりです。

♦ 現在の設定の表示

msh> authfree

・プリンタージョブ認証が認証除外に設定されていない場合、認証除外制御の情報は表示できません。

♦ IPv4 アドレスの設定

msh> authfree 対象 ID range_addr1 range_addr2

♦ IPv6 アドレスのレンジでの設定

msh> authfree 対象 ID range6_addr1 range6_addr2

♦ IPv6 アドレスのマスクでの設定

msh> authfree 対象 ID mask6_addr1 masklen

♦ IEEE 1284/USB の設定

msh> authfree [parallel|usb] [on|off]

・authfree 機能を有効するには「on」を、無効にするときは「off」を指定します。

・インターフェースを必ず指定してください。

♦ 設定を工場出荷値に戻す

msh> authfree flush

補足

・IPv4 と IPv6 の対象 ID は、それぞれ 1~5 の 5 件が設定できます。