

**SPEEDIA**

# B9500シリーズ セキュリティーガイド

本機のセキュリティー機能に関する説明を  
記載しています。セキュリティー強化の  
ために最初に設定をすることをお勧めします。

品種コード B1-EJ1C

プリンターをご使用になる前に必ずお読みください。

**CASIO**®

# 目次

目次	2
はじめに	
セキュリティ機能を設定する前に	6
本機の運用を開始する前に	7
管理者とは	8
管理者認証を設定する	9
管理者権限を設定する	10
管理者を登録、変更する	11
管理者のログイン方法	13
操作部からログインする	13
Web Image Monitorからログインする	14
管理者のログアウト方法	15
操作部からログアウトする	15
Web Image Monitorからログアウトする	15
スーパーバイザーとは	16
管理者のパスワードを再設定する	16
スーパーバイザーを変更する	17
ユーザー認証を設定する	
ユーザーとは	18
ユーザー認証の概念	19
ユーザー認証を設定する	20
ユーザーコード認証	22
ユーザーコード認証を設定する	22
ベーシック認証	23
ベーシック認証を設定する	23
アドレス帳の認証情報	23
ログインユーザー名とログインパスワードを設定する	24
Windows 認証	25
Windows 認証を設定する	26
「Webサーバー (ISS)」と「Active Directory 証明書サービス」を インストールする	28
サーバー証明書を作成する	30
LDAP 認証	31
プリンタージョブ認証	34
プリンタージョブ認証のレベル	34
プリンタージョブの種類	34
authfree コマンド	36
ロックアウト機能	37
パスワードロックアウト設定	38
パスワードロックアウト解除	38
オートログアウト時間設定	40
機器の利用を制限する	
管理者設定項目の変更を防止する	41
ユーザーによる設定の変更を禁止する	41
メニュープロテクトを設定する	42
機器の利用を制限する	43
ユーザーの印刷利用量を制限する	44
利用量制限を設定する	45
ユーザーごとに利用量上限を設定する	46
ユーザーの利用量を確認する	46
利用量カウンターをクリアする	46
自動リセット機能を設定する	47

## 目次

機器情報の漏洩を防止する	
アドレス帳の登録情報を保護する	49
アドレス帳にアクセス権を設定する	49
アドレス帳を暗号化する	50
機器のデータを暗号化する	52
暗号化設定を有効にする	54
暗号鍵をバックアップする	55
暗号鍵を更新する	56
暗号化を解除する	57
データを上書き消去する	59
使用環境	59
使用上のご注意	59
メモリー全消去	61
ネットワークセキュリティを強化する	64
アクセスコントロールを設定する	64
プロトコルの有効／無効を設定する	66
操作部から設定する	69
Web Image Monitorから設定する	70
ネットワークセキュリティレベルを設定する	71
操作部から設定する	71
Web Image Monitorから設定する	72
各機能とネットワークセキュリティレベルの関係	72
機器証明書による通信経路の保護	76
Web Image Monitorから機器証明書を作成、導入する（自己証明書）	76
機器証明書を作成、申請する（認証局証明書）	77
機器証明書を導入する（認証局証明書）	78
中間証明書を導入する（認証局証明書）	78
SSL／TLSを設定する	80
SSL／TLSを有効にする	81
SSL／TLSのユーザー設定	82
SSL／TLS暗号化通信モードを設定する	83
SMTP通信のSSLを設定する	84
IPsecを設定する	85
通信データの暗号化と認証	85
自動鍵交換設定	86
IPsec設定項目	87
自動鍵交換設定の流れ	93
telnetでIPsecを設定する	97
IEEE802.1X認証を設定する	102
サイト証明書を導入する	102
機器証明書を選択する	103
イーサネットでIEEE802.1Xを使用する	103
パスワードを暗号化する	105
ドライバー暗号鍵を設定する	106
IPP認証のパスワードを設定する	107
Kerberos認証の暗号化設定	108
本機を管理する	110
ログを管理する	110
Web Image Monitorからログを管理する	111
Web Image Monitorで管理できるログ項目	111
ダウンロードできるログ情報の属性一覧	116
収集するログを設定する	136
ログを暗号化する	137
ログをダウンロードする	137
本機に保持できるログ件数	138
ログフル時の注意事項	139

## 目次

プリンター印刷時のログ	141
ログを一括消去する	142
ログ収集サーバーへのログ転送を無効にする	142
本機からログを管理する	144
収集するログを設定する	144
ログ収集サーバーへのログ転送を無効にする	144
ログ収集サーバーからログを管理する	145
機器情報を管理する	146
SDカードを取り付ける	147
機器情報をエクスポートする	148
機器情報をインポートする	149
サーバーの機器情報を手動でインポートする	150
こんなときには	151
アドレス帳を管理する	154
アドレス帳の自動消去を設定する	154
セキュリティー強化機能を設定する	154
セキュリティー強化機能の設定項目	155
その他のセキュリティー機能	162
システム状態	162
ファームウェアの正当性確認	162
カスタマーエンジニアの操作を制限する	163
サービスモード移行禁止設定を有効にする	163
こんなときには	
メッセージが表示されたとき	164
エラーコードが表示されたとき	166
ベーシック認証時のエラーコード	166
Windows 認証時のエラーコード	167
LDAP 認証時のエラーコード	170
操作ができないとき	174
設定項目の操作権限一覧	176
表の見かた	176
[メニュー] キー項目の操作権限一覧	177
プリンター通常画面	177
用紙設定	177
調整/管理	178
テスト印刷	180
システム設定	180
印刷設定	182
セキュリティー管理	182
機器設定情報	183
インターフェース設定	183
表示言語切替	185
拡張機能初期設定	185
Web Image Monitor 設定項目の操作権限一覧	186
構成	186
状態	186
消耗品	186
カウンター	187
ユーザー別カウンター	187
ジョブ	187
設定	188
プリンター	197
インターフェース	199
ネットワーク	199
セキュリティー	205
Web page 設定	212

## 目次

---

拡張機能初期設定	213
アドレス帳	213
印刷取消	214
機器のリセット	214
アドレス帳の操作権限一覧	214

## はじめに

セキュリティー機能を使用するときの注意点と、管理者の設定について説明します。

---

### セキュリティー機能を設定する前に

---

**★重要**

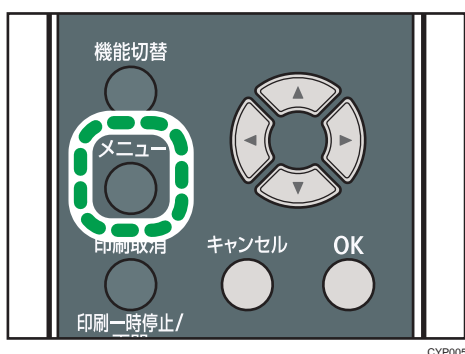
- 本機のセキュリティー設定をしないときは、悪意を持った攻撃者により被害を受けることがあります。
- 本機が持ち出されたり壊されたりしないように、セキュリティー管理の行き届いた環境に本機を設置してください。
- 本機購入者は、本機を適切に運用して頂ける方を、管理者とスーパーバイザーとして選定し、その方の管理下で運用してください。管理者とスーパーバイザーが適切な運用をしないときは、ユーザーにセキュリティー上の被害が発生する恐れがあります。
- 管理者の方はセキュリティー機能を使用する前に、本書を最後までよくお読みのうえ、正しく使用してください。特に、本項はよく読んでご理解ください。
- 管理者の方は、ユーザーがセキュリティー機能を正しく使用するように指導してください。
- 例外や異常な動作を確認するために、定期的なログ情報の監査をお勧めします。
- 本機をネットワークに接続するときは、ファイアウォールなどによって保護された環境で使用してください。
- 通信中のデータを守るために、本機でセキュリティー通信機能を利用するときは、暗号化通信などのセキュリティー通信機能に対応した接続機器をお選びください。

## 本機の運用を開始する前に

高度なセキュリティーを希望するときは、本機を使用する前に次の設定をしてください。情報の暗号化通信を有効にし、管理者アカウントを設定します。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 本機の電源を入れます。
2. [メニュー] キーを押します。



3. 本機の IPv4 アドレスを設定します。

[インターフェース設定] ▶ [OK] ▶ [ネットワーク設定] ▶ [OK] ▶ [本体 IPv4 アドレス] ▶ [OK] ▶ IP アドレスを設定

4. 本機を管理者だけがアクセスできるネットワークに接続します。
5. Web Image Monitor を起動し、管理者としてログインします。
6. 本機の管理者のメールアドレスを設定します。

[機器の管理] ▶ [設定] ▶ [機器] ▶ [メール] ▶ 「管理者メールアドレス」に入力 ▶ [OK]

7. 操作部から機器証明書の作成と導入をします。  
メールアドレス項目に、手順 6 で入力した管理者メールアドレスを設定してください。
8. 管理者のユーザー名、パスワードを変更します。
9. ログアウトします。
10. 本機を管理者だけがアクセスできるネットワークから外して、運用環境で使用するネットワークに接続します。

## はじめに

---

### ↓ 補足

- ・ IPv4 アドレスの設定方法は、『使用説明書』「ネットワークの設定」を参照してください。
- ・ Web Image Monitor のログイン方法は、P. 13 「管理者のログイン方法」を参照してください。
- ・ 機器証明書の導入方法は、P. 76 「機器証明書による通信経路の保護」を参照してください。
- ・ 管理者のユーザー名、パスワードの設定については、P. 11 「管理者を登録、変更する」を参照してください。

---

## 管理者とは

---

管理者とは、本機を使用するユーザーのアクセス制限をしたり、本機の各種機能・設定を管理する人のことです。

管理者がアクセス制限や設定項目を管理するときは、まず本機の管理者を決定し、認証機能を有効にします。認証機能を有効にすると、本機を使用するにはログインユーザー名とログインパスワードが必要です。

本機の管理者は担当する機能によってユーザー管理者、機器管理者、ネットワーク管理者、文書管理者の4つのカテゴリーに分かれます。管理者の役割を分担すると、1人の管理者の負担を軽減すると同時に、管理者による不正操作も制限できます。複数の管理者を1人で兼務したり、1つの管理者を複数人で担当したりできます。また、管理者のパスワードを変更できるスーパーバイザーを設定できます。

管理者は本機のアクセス制限や設定項目を管理するために設定されるものであるため、管理者ログイン名で文書印刷などのユーザー機能は使用できません。別途、ユーザー認証が必要です。

管理者の登録方法はP. 11 「管理者を登録、変更する」、スーパーバイザーについてはP. 16 「スーパーバイザーとは」、ユーザーについてはP. 18 「ユーザーとは」を参照してください。

### ★ 重要

- ネットワークのトラブルなどで、ユーザー認証ができないときは、管理者認証でアクセスして、ユーザー認証を無効に設定すれば使用できます。緊急のときに使用してください。

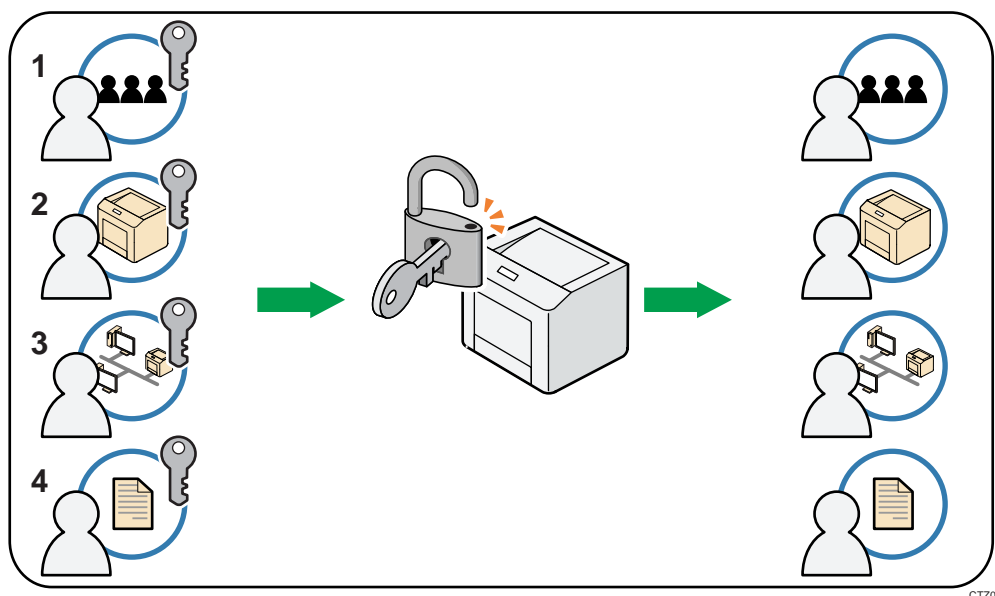


## 管理者認証を設定する

管理者認証とは、管理者が本機の各種設定を開始するとき、またはネットワークから本機にアクセスするとき、ログインユーザー名とログインパスワードによって確認する仕組みです。管理者はアドレス帳に登録されるユーザーとは区別されます。管理者を登録するときに、すでにアドレス帳に登録されているログインユーザー名は使用できません。各管理者はログインユーザー名でそれぞれ区別されますが、1つのログインユーザー名に異なる管理者の権限を与えると、複数の管理者を兼務できます。管理者の登録方法は、P.11「管理者を登録、変更する」を参照してください。

各管理者に設定できる項目は、ログインユーザー名、ログインパスワードです。管理者は本機のアクセス制限や設定項目を管理するために設定されるものであるため、管理者ログイン名で文書印刷などのユーザー機能は使用できません。ユーザー機能を使用するときは、アドレス帳にユーザーを新規に作成し、ユーザーとしての認証が必要です。管理者認証を設定してからユーザー認証を設定します。

### 各管理者の役割



#### 1. ユーザー管理者

アドレス帳の個人情報进行管理します。ユーザー管理者は、アドレス帳へユーザーを登録・削除したり、ユーザーの個人情報を変更できます。アドレス帳に登録されたユーザー自身も自分の情報を変更、削除できます。ユーザー管理者はユーザーが自分のパスワードを忘れたときに削除したり、新規に設定でき、ユーザーが操作できなくなることを防止できます。

## はじめに

---

### 2. 機器管理者

おもに本機の初期設定を管理します。各機能の初期設定を機器管理者だけが設定できるようにできます。それにより、不特定のユーザーが設定を変更することを防止できます。

### 3. ネットワーク管理者

ネットワークに接続するための設定を管理します。ネットワークに接続するための IP アドレスの設定や、メールを送受信するための設定をネットワーク管理者だけが設定できるようにできます。これにより、不特定のユーザーが設定を変更し、本機を使用できなくすることを防止し、適切なネットワーク設定ができるようにします。

### 4. 文書管理者

蓄積した文書のアクセス権を管理します。本機に蓄積した文書に、登録したユーザーや許可したユーザーだけが閲覧、編集できるように設定できます。これにより、登録した文書を不特定のユーザーが閲覧したり、操作したりすることで起こる情報漏洩や改ざんを防止できます。

#### 補足

- ユーザーコード認証を設定するときは、管理者認証を設定しないで、ユーザー認証の設定ができます。

---

## 管理者の権限を設定する

---

管理者認証を有効にするには、管理者認証管理の設定で [する] を選択します。設定を有効にすると、各管理者に割り当てられている初期設定項目が管理項目になります。

管理者認証のログイン、ログアウトの方法は、P. 13 「管理者のログイン方法」、P. 15 「管理者のログアウト方法」を参照してください。

#### 重要

- 管理者認証を有効にしたときは、管理者のログインユーザー名とログインパスワードを絶対に忘れないようにしてください。万一忘れてしまったときは、スーパーバイザーの権限でパスワードを新しく設定します。スーパーバイザーの権限については、P. 16 「スーパーバイザーとは」を参照してください。
- スーパーバイザーのログインユーザー名とログインパスワードは、絶対に忘れないようにしてください。万一忘れてしまったときは、サービス実施店に連絡し、工場出荷時の値に戻してください。このとき、本機のデータや設定が失われるのでご了承ください。

1. Web Image Monitor から管理者がログインします。
2. 設定する管理者認証を選択します。

## はじめに

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [管理者認証管理] ▶ [ユーザー管理者認証]、[機器管理者認証]、[ネットワーク管理者認証]、[文書管理者認証]のうち、有効にする管理者認証を選択

3. [OK] をクリックします。
4. ログアウトします。

## 管理者を登録、変更する

管理者認証を設定するときは、1人の管理者が1つの管理者の役割を担当されることをお勧めします。管理者の役割を分担すると、1人の管理者の負担を軽減すると同時に管理者による不正操作も制限できます。管理者の権限を与えることができるログインユーザー名は管理者1～4の4件まで登録できます。

管理者認証のログイン、ログアウトの方法は、P. 13「管理者のログイン方法」、P. 15「管理者のログアウト方法」を参照してください。

1. Web Image Monitor から管理者がログインします。
2. [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] に割り当てる管理者の番号を選択します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [管理者登録/変更] ▶ 各カテゴリで管理者1～4を選択

各管理者の権限を1人ずつに割り当てるときは、各カテゴリで別の管理者の番号を設定します。たとえば、[ユーザー管理者] で [管理者1] を設定したら、[機器管理者] では [管理者2] を設定します。

複数の管理者の権限をまとめるときは、ひとつの管理者の番号に複数の権限を割り当てます。たとえば、ユーザー管理者と機器管理者の権限を [管理者1] にまとめたいときは、[ユーザー管理者] と [機器管理者] の両方で [管理者1] を設定します。

3. 「ログインユーザー名」を入力します。
4. 「ログインパスワード」を入力します。

[変更] ▶ ログインパスワードを入力 ▶ 確認用のログインパスワードを入力 ▶ [OK]

## はじめに

---

他人に容易に推測されないように、ログインパスワードはパスワードポリシーにしたがって設定されることを強くお勧めします。パスワードポリシーについては、P. 154「セキュリティ強化機能を設定する」の「パスワードポリシー」を参照してください。

### 5. 「暗号パスワード」を入力します。

[変更] ▶ 暗号パスワードを入力 ▶ 確認用の暗号パスワードを入力 ▶ [OK]

### 6. [OK] をクリックします。

### 7. ログアウトします。

#### ↓ 補足

- 各管理者の権限は、その管理者権限を持つ管理者だけが変更できます。
- 各管理者権限には、必ず1人以上の管理者を割り当ててください。

## ユーザー名、パスワードに使用できる文字

---

ログインユーザー名とログインパスワードには、次の文字を使用します。アルファベットは大文字、小文字を区別して登録してください。

- 英大文字：[A-Z] (26 文字)
- 英小文字：[a-z] (26 文字)
- 数字：[0-9] (10 文字)
- 記号：(スペース) ! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ ¥ ] ^ \_ ` { | } ~ (33 文字)

### ログインユーザー名

- スペース、「:」、「"」を使用できません。
- 数字だけや、空白にはできません。
- 最大文字数は、32 文字です。

### ログインパスワード

- 最大文字数は管理者とスーパーバイザーは 32 文字、ユーザーは 128 文字です。
- アルファベットの大文字、小文字、数字、記号を組み合わせで作成してください。文字数が多いほど第三者に推測されにくくなります。
- [セキュリティ強化] の [パスワードポリシー] で、パスワードの複雑さと最小文字数を設定すると、条件を満たしたパスワードだけを設定できます。パスワードポリシーの設定方法は、P. 154「セキュリティ強化機能を設定する」の「パスワードポリシー」を参照してください。

## 管理者のログイン方法

---

管理者認証が設定されているときは、管理者のユーザー名とパスワードでログインします。スーパーバイザーも同じ方法でログインします。管理者とスーパーバイザーのログインユーザー名、ログインパスワードについては管理者へ問い合わせてください。

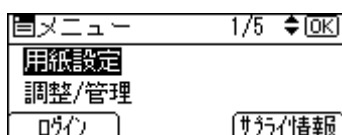
### 操作部からログインする

---

**★重要**

- [ログイン] 表示は、Web Image Monitor から機器管理者認証を有効にしたときに表示されます。

1. [メニュー] キー ▶ [ログイン]



2. 管理者のログインユーザー名を入力します。

[入力] ▶ ログインユーザー名を入力 ▶ [入力終了]

3. 管理者のログインパスワードを入力します。

[入力] ▶ ログインパスワードを入力 ▶ [入力終了]

**↓補足**

- すでにユーザー認証が設定されているときは、認証画面が表示されます。管理者としてログインするときは、管理者のログインユーザー名とログインパスワードを入力します。

## Web Image Monitor からログインする

---

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ときは、各セグメントの先頭につく「0」は入力しないでください。たとえば「192.168.001.010」のときは、「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。  
IPv6 アドレスは [2001:db8::9abc] のように、前後に [ ] をつけて入力してください。
3. [ログイン] をクリックします。
4. 管理者の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] をクリックします。

### ↓ 補足

- 使用している Web ブラウザーの設定により、ログインユーザー名とログインパスワードが Web ブラウザーに保存されることがあります。これを防止するためには Web ブラウザーでログインユーザー名とログインパスワードを保存しないように設定してください。

---

## 管理者のログアウト方法

---

管理者認証が設定されているときは、各種設定が終了したあとに、必ずログアウトしてください。スーパーバイザーも同じ方法でログアウトします。

---

### 操作部からログアウトする

---

1. **【ログアウト】**を押します。  
【ログアウト】が表示されていないときは、**【メニュー】**キーを押します。
2. **【する】**を押します。

---

### Web Image Monitor からログアウトする

---

1. **【ログアウト】**をクリックします。

 補足

- ログアウト後は、Web ブラウザーのキャッシュを削除してください。

## スーパーバイザーとは

---

スーパーバイザーは各管理者のパスワードを削除したり、新しく設定できます。たとえば、各管理者がパスワードを忘れたときや、管理者が交代したときなどにスーパーバイザーがパスワードを再設定します。

スーパーバイザーでログインしたときは、各機能や初期設定の操作はできません。管理者のパスワードを新しく設定するときだけログインしてください。

ログイン、ログアウトの方法は管理者と同様です。P. 13「管理者のログイン方法」、P. 15「管理者のログアウト方法」を参照してください。

### ★重要

- スーパーバイザーのログインユーザー名とログインパスワードは、絶対に忘れないようにしてください。万一忘れてしまったときは、サービス実施店に連絡し、工場出荷時の値に戻してください。このとき、本機の設定やカウンター、ログなどのデータが失われるのでご了承ください。

### ↓補足

- ログインユーザー名、ログインパスワードに使用できる文字は、P. 12「ユーザー名、パスワードに使用できる文字」を参照してください。
- スーパーバイザーと各管理者は同じログインユーザー名にできません。

## 管理者のパスワードを再設定する

---

1. Web Image Monitor からスーパーバイザーがログインします。  
ログイン方法は、P. 13「管理者のログイン方法」を参照してください。
2. パスワードを再設定する管理者を選択します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [管理者登録/変更] ▶ パスワードを再設定する管理者の [変更] を選択

3. ログインパスワードを入力します。

ログインパスワードを入力 ▶ 確認用のログインパスワードを入力 ▶ [OK]

4. [OK] をクリックします。
5. ログアウトします。

### ↓補足



はじめに

---

- スーパーバイザーが変更できるのはログインパスワードだけです。管理者のログインユーザー名は変更できません。

---

## スーパーバイザーを変更する

---

スーパーバイザーのログイン名やパスワードを変更します。

「管理者認証管理」の設定で[ユーザー管理]を[する]に設定してから操作してください。詳しくはP.10「管理者の権限を設定する」を参照してください。

1. Web Image Monitor からスーパーバイザーがログインします。  
ログイン方法は、P.13「管理者のログイン方法」を参照してください。
2. スーパーバイザーのログインユーザー名を変更します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [管理者登録/変更] ▶ スーパーバイザーのログインユーザー名を入力

3. 「ログインパスワード」を変更します。

[変更] ▶ ログインパスワードを入力 ▶ 確認用のログインパスワードを入力 ▶ [OK]

4. [OK] をクリックします。
5. ログアウトします。

## ユーザー認証を設定する

ユーザー認証の設定方法と、ユーザー認証によって有効になる機能について説明します。

---

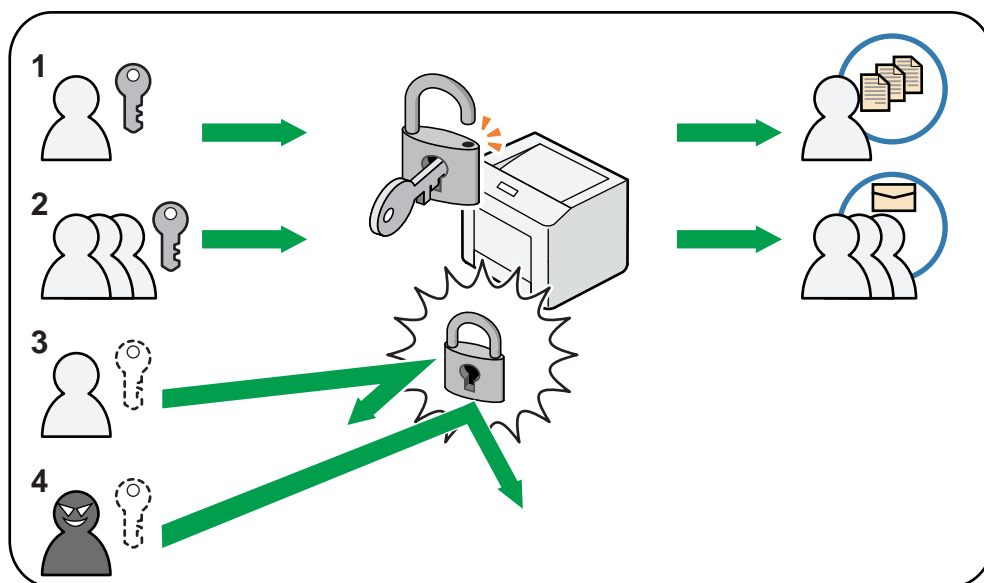
### ユーザーとは

---

ユーザーとは、文書印刷など、本機の機能を使用している個人のことです。ユーザーは本機のアドレス帳に登録された個人情報によって管理され、管理者によってアクセス権を与えられた機能だけを使用できます。また、ユーザー認証を有効に設定すると、アドレス帳に登録されたユーザーだけを本機の利用者として設定できます。ユーザー管理者がアドレス帳へのユーザー登録をします。管理者については、P.8「管理者とは」を参照してください。アドレス帳へのユーザーの登録方法は、Web Image Monitor のヘルプを参照してください。

## ユーザー認証の概念

ユーザー認証とはユーザーが本機の使用を開始するとき、またはネットワークから本機にアクセスするとき、ログインユーザー名とログインパスワードでユーザーを確認する仕組みです。個人やグループ単位でのアクセス制限ができます。



1. ユーザー  
文書印刷など通常の機能として本機を使用する個人です。
2. グループ  
文書印刷など通常の機能として本機を使用するグループです。
3. アクセスを許可されていないユーザー
4. 不正アクセス者

## ユーザー認証を設定する

ユーザー認証にはユーザーコード認証、ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証の 5 つの認証方法があります。操作部でどれか 1 つの認証を選択し、必要な設定をします。設定項目は認証方法によって異なります。管理者認証を設定してから、ユーザー認証を設定します。

### ★重要

- 統合サーバー認証は使用できません。
- ネットワークのトラブルなど、ユーザー認証できないときは、管理者認証でアクセスして、ユーザー認証を無効に設定すれば使用できます。緊急のときに使用してください。

### ユーザー認証設定の流れ

設定の順序	詳細
管理者認証を設定する	P. 10 「管理者の権限を設定する」 P. 11 「管理者を登録、変更する」
ユーザー認証を設定する	ユーザー認証には次の方法があります。 <ul style="list-style-type: none"><li>▪ P. 22 「ユーザーコード認証」</li><li>▪ P. 23 「ベーシック認証」</li><li>▪ P. 25 「Windows 認証」</li><li>▪ P. 31 「LDAP 認証」</li><li>▪ 「統合サーバー認証」(使用できません)</li></ul>

### ↓補足

- ベーシック認証、Windows 認証、LDAP 認証を設定するときは、管理者認証管理の設定でユーザー管理者を [する] に設定してください。
- ユーザーコード認証を設定するときは、管理者認証を設定しなくても、ユーザー認証の設定ができます。
- ユーザーコード認証は個人単位ではなくユーザーコードごとの認証をするときに使用します。ベーシック認証、Windows 認証、LDAP 認証は個人単位の認証をするときに使用します。
- ユーザーコード認証で使用する 8 桁以内のユーザーコードアカウントは、認証方式をユーザーコード認証からベーシック認証、Windows 認証、LDAP 認証に切り替えた

## ユーザー認証を設定する

---

あとでも、ログインユーザー名として引き継がれ使用できます。このとき、ユーザーコード認証にパスワードはないため、ログインパスワードが空のアカウントとして設定されます。

- 外部の認証（Windows 認証、LDAP 認証）に切り替えたときは、引き継がれたユーザーコードアカウントが外部の認証機器に登録されていないと認証はされず、本機を利用できません。ただし、認証できなくても本機のアドレス帳にはユーザーコードアカウントが残ります。
- ユーザーコード認証からほかの認証方式に切り替えたときは、セキュリティの観点から、使用しないアカウントを削除するか、パスワードを設定することをお勧めします。同時に2つ以上の認証方法は設定できません。
- 電源を入れた直後は、ユーザー認証管理画面の認証対象に拡張機能が表示されないことがあります。そのときは、しばらく待ってからユーザー認証管理画面を開き直してください。

## ユーザーコード認証

---

ユーザーコードごとに機能のアクセス制限をするときに設定します。複数のユーザーが同一のユーザーコードを使用できます。

ユーザーコードの設定については Web Image Monitor で設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

プリンタードライバーのユーザーコード設定については、プリンタードライバーのヘルプを参照してください。

### ユーザーコード認証を設定する

---

1. Web Image Monitor から機器管理者がログインします。
2. ユーザーコード認証を設定します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ユーザー認証管理] ▶ 「ユーザー認証管理」 ▶ [ユーザーコード]

3. ユーザーの利用を制限する機能を選択します。

「ユーザーコード設定」 ▶ 「制限する機能」 ▶ 制限する機能を選択

プリンタージョブ認証を設定するときは、[自動登録] 以外を選択します。

4. プリンタージョブ認証を使用するときは、[プリンタージョブ認証] のレベルを設定します。

プリンタージョブ認証については、P. 34「プリンタージョブ認証」を参照してください。

[簡易 (限定)] を選択したときは、プリンタージョブ認証を簡易として扱う対象範囲を限定します。

IPv4 アドレスの範囲と、パラレル接続、USB 接続を対象とするかを設定できます。

5. [OK] をクリックします。
6. ログアウトします。

## ベーシック認証

---

本機のアドレス帳を使用して個人単位の認証をするときに設定します。個人単位で使用できる機能を設定したり、アドレス帳や保存文書などの個人データへのアクセスに、制限をかけられます。

ベーシック認証では認証を設定したあとに、管理者がアドレス帳に登録されたユーザーごとに本機の利用制限を設定します。利用制限の設定については、P. 23「アドレス帳の認証情報」を参照してください。

### ベーシック認証を設定する

---

管理者認証が設定されていることを確認してから、設定してください。

1. Web Image Monitor から機器管理者がログインします。
2. ベーシック認証を設定します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ユーザー認証管理] ▶ 「ユーザー認証管理」 ▶ [ベーシック認証]

3. [プリンタージョブ認証] のレベルを選択します。

プリンタージョブ認証については、P. 34「プリンタージョブ認証」を参照してください。

[簡易（限定）] を選択したときは、プリンタージョブ認証を簡易として扱う対象範囲を限定します。

IPv4 アドレスの範囲と、パラレル接続、USB 接続を対象とするかを設定できます。

4. ユーザーに使用を許可する機能を選択します。

「ベーシック認証設定」 ▶ 「使用できる機能」 ▶ 使用を許可する機能を選択

5. [OK] をクリックします。
6. ログアウトします。

### アドレス帳の認証情報

---

「ユーザー認証管理」を設定すると、個人やグループ単位でのアクセス制限、本機の利用制限を設定できます。本機の利用制限は、P. 20「ユーザー認証を設定する」を参照してください。

ユーザーが正しく本機を利用できるように、アドレス帳でユーザーごとの設定をします。事

## ユーザー認証を設定する

---

前にユーザーをアドレス帳に登録してください。アドレス帳については、Web Image Monitorのヘルプを参照してください。

---

## ログインユーザー名とログインパスワードを設定する

---

ユーザー認証で使用するログインユーザー名とログインパスワードを設定します。ログインユーザー名、ログインパスワードに使用できる文字は、P. 12「ユーザー名、パスワードに使用できる文字」を参照してください。

1. Web Image Monitor からユーザー管理者がログインします。
2. 設定するユーザーを選択します。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. 「ログインユーザー名」を変更します。

[詳細入力] ▶ [変更] ▶ ログインユーザー名を入力

4. 「ログインパスワード」を変更します。

「ログインパスワード」 ▶ [変更] ▶ ログインパスワードを入力 ▶ 確認用のログインパスワードを入力 ▶ [OK]

5. [OK] をクリックします。
6. ログアウトします。



## Windows 認証

---

Windows のドメインコントローラを使用して、ディレクトリサーバーにアカウントを持つユーザーの認証をするときに設定します。ディレクトリサーバーにアカウントがないユーザーは認証を受けることができません。Windows 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定できます。ディレクトリサーバーに登録されているアドレス帳を本機に自動で登録できるため、本機でアドレス帳の個人設定を登録しなくてもユーザー認証ができます。

はじめて利用するときは、所属するグループに割り当てられている機能を利用できます。グループに登録されていないときは [ \*Default Group ] に設定されている機能を利用できません。ユーザーごとに機能の制限をするときは事前にアドレス帳で設定してください。

Windows 認証でユーザー情報を自動登録するときは、本機とドメインコントローラが SSL/TLS による暗号化された通信をすることをお勧めします。そのときは事前にドメインコントローラのサーバー証明書を作成します。証明書の作成方法は、P. 30「サーバー証明書を作成する」を参照してください。

### ★重要

- Windows 認証を設定しているときは、認証のときに、ディレクトリサーバーに登録されているユーザー情報が自動登録されます。ディレクトリサーバーのユーザー情報を編集したあとに認証をすると、編集した情報が上書きされることがあります。
- 別のドメインで管理されているユーザーは、ユーザー認証を使用できますが、ユーザー情報は取得できません。
- ドメインコントローラに新規ユーザーを作成し、パスワード設定で「次回ログオン時にパスワード変更が必要」を選択したときは、先にパソコンよりログオンしてパスワードの変更をしてください。
- Kerberos 認証が選択されていても、認証先のサーバーが NTLM 認証だけに対応しているときは自動的に NTLM 認証に切り替わり認証動作が実行されます。
- Windows サーバーで「Guest」アカウントが有効に設定されているときは、ドメインコントローラに存在しないユーザーでも認証できます。そのときはユーザーはアドレス帳に登録され、[ \*Default Group ] に設定されている機能を利用できます。

本機の Windows 認証機能は、NTLM 認証と Kerberos 認証の 2 つの方式に対応しています。各認証の使用条件は次のとおりです。

### NTLM 認証の使用条件

- NTLMv1 認証および NTLMv2 認証に対応しています。
- NTLM 認証を設定するときは、指定したドメイン内にドメインコントローラが必要です。

## ユーザー認証を設定する

---

- 次の OS が対応しています。
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2
- ActiveDirectory 動作時のユーザー情報の取得には LDAP を利用します。そのとき、本機と LDAP サーバーが SSL/TLS による暗号化通信をすることをお勧めします。SSL/TLS を利用するときは、TLSv1 または SSLv3 がサーバーで動作することが必要です。

### Kerberos 認証の使用条件

- Kerberos 認証を設定するときは、指定したドメイン内にドメインコントローラが必要です。
- Kerberos 認証を使用するには、KDC（キー配布センター）に対応した OS が必要です。
- 次の OS が対応しています。
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

Windows Server 2008 で Kerberos 認証を使用するには、Service Pack 2 以降の導入が必要です。

- ActiveDirectory 動作時のユーザー情報の取得には LDAP を利用します。そのとき、本機と LDAP サーバーが SSL/TLS による暗号化通信をすることをお勧めします。SSL/TLS を利用するときは、TLSv1 または SSLv3 がサーバーで動作することが必要です。
- Kerberos 認証では、本機と KDC サーバーの間で暗号化通信をします。暗号化通信の設定は、P. 108 「Kerberos 認証の暗号化設定」を参照してください。

#### ↓ 補足

- ログインユーザー名、ログインパスワードに使用できる文字は、P. 12「ユーザー名、パスワードに使用できる文字」を参照してください。
- 複数のグループに登録されているユーザーは、複数のグループに割り当てられている機能のすべてを利用できます。
- 2 度目以降に利用するときは、ユーザーごとに割り当てられた機能と、所属するグループに割り当てられた機能を利用できます。
- Windows 認証では、認証時に SSL/TLS を利用するか、しないかの選択ができます。

---

## Windows 認証を設定する

---

管理者認証が設定されていることを確認してから、設定してください。

## ユーザー認証を設定する

---

1. Web Image Monitor から機器管理者がログインします。
2. [Windows 認証] を設定します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ユーザー認証管理] ▶ 「ユーザー認証管理」 ▶ [Windows 認証]

3. [プリンタージョブ認証] のレベルを選択します。

プリンタージョブ認証については、P. 34「プリンタージョブ認証」を参照してください。

[簡易 (限定)] を選択したときは、プリンタージョブ認証を簡易として扱う対象範囲を限定します。

IPv4 アドレスの範囲と、パラレル接続、USB 接続を対象とするかを設定できます。

4. 認証方式を選択します。

- Kerberos 認証

Kerberos 認証を [する] ▶ Kerberos 認証で使用するレルムを選択

Kerberos 認証を有効にするには、レルムの登録が必要です。

レルム名は半角大文字で登録します。レルムの登録は、Web Image Monitor のヘルプを参照してください。

- NTLM 認証

Kerberos 認証を [しない] ▶ 認証するドメイン名を入力

ドメイン名を [DNS 完全修飾ドメイン] 形式で指定するときは、文字列の最後に「.」を付加してください (ドメイン名が「abcd.com」のときは、「abcd.com.」と指定します)。

また、利用している環境に合わせて、「グループ設定 (Windows 認証)」メニューでグループ名を入力し、利用できる機能を選択します。

5. SSL を利用するときは、[する] をクリックします。
6. グローバルグループを使用するときは、グローバルグループを設定します。

「グループ設定 (Windows 認証)」 ▶ 「グループ名」 ▶ サーバーで登録されているグループ名を入力

## ユーザー認証を設定する

---

グループ名は、大文字、小文字を区別して入力してください。

選択した機能がWindows 認証の対象となります。選択していない機能は、ユーザーは使用できません。

機能の利用制限については、P. 43「機能の利用を制限する」を参照してください。

Windows サーバーでグローバルグループを登録していれば、グローバルグループごとに機能の利用制限ができます。あらかじめWindows サーバー側でグローバルグループを作成し、そのグループに認証するユーザーの登録が必要です。本機ではそのグローバルグループメンバーに許可する機能の登録が必要です。

Windows サーバーに登録したグループと同じ名前で、本機に大文字、小文字を区別して入力してグループを作成してください。作成したグループごとに、本機の機能の利用制限を設定します。初めて利用したとき、ユーザーは、[\*Default Group] に設定されている機能が利用できます。[\*Default Group] は、工場出荷時にすべての機能が利用できるように設定されています。運用にあわせて機能の利用制限を設定します。

### 7. 「使用できる機能」でグループに使用を許可する機能を選択します。

選択した機能がWindows 認証の対象となります。選択していない機能は、ユーザーは使用できません。

機能の利用制限については、P. 43「機能の利用を制限する」を参照してください。

### 8. [OK] をクリックします。

### 9. ログアウトします。

---

## 「Web サーバー (IIS)」と「Active Directory 証明書サービス」をインストールする

---

Active Directory に登録されているメールアドレスを、本機に自動で取得するときに設定します。

Windows のコンポーネントとして「Web サーバー (IIS)」と「Active Directory 証明書サービス」を下記の手順でインストールします。

すでにインストールされているときは、サーバー証明書の作成をしてください。

### Windows Server 2008 R2 での設定

---

1. [スタート] メニューから、[管理ツール] をポイントし、[サーバーマネージャー] をクリックします。
2. 左枠の [役割] をクリックし、[操作] メニューから [役割の追加] をクリックします。
3. [次へ] をクリックします。
4. [Web サーバー (IIS)] と [Active Directory 証明書サービス] のチェックボックスにチェックをつけ、[次へ] をクリックします。確認メッセージが表示されたときは [機能の追加] をクリックします。

## ユーザー認証を設定する

---

5. 表示された内容を確認したあと、[次へ] をクリックします。
6. [証明機関] にチェックが付いていることを確認し、[次へ] をクリックします。
7. [エンタープライズ] を選択し、[次へ] をクリックします。
8. [ルート CA] を選択し、[次へ] をクリックします。
9. [新しい秘密キーを作成する] を選択し、[次へ] をクリックします。
10. 秘密キーを作成するため、暗号化サービスプロバイダー、キーの長さ、ハッシュアルゴリズムを選択し、[次へ] をクリックします。
11. 「この CA の共通名:」に CA の名前を入力し、[次へ] をクリックします。
12. 証明書の有効期間を選択し、[次へ] をクリックします。
13. 「証明書データベースの場所:」と「証明書データベース ログの場所:」は変更しないで、[次へ] をクリックします。
14. 注意事項などを確認したら、[次へ] をクリックします。
15. インストールする役割サービスにチェックをつけ、[次へ] をクリックします。
16. [インストール] をクリックします。
17. インストールが完了したというメッセージが表示されたら、[閉じる] をクリックします。
18. サーバーマネージャーを終了します。

## Windows Server 2012 での設定

---

1. [スタート] メニューから、[サーバーマネージャー] をクリックします。
2. [管理] メニューから [役割と機能の追加] をクリックします。
3. [次へ] をクリックします。
4. [役割ベースまたは機能ベースのインストール] を選択し、[次へ] をクリックします。
5. サーバーを選択し、[次へ] をクリックします。
6. [Active Directory 証明書サービス] と [Web サーバー (IIS)] のチェックボックスにチェックを付け、[次へ] をクリックします。確認メッセージが表示されたときは、[機能の追加] をクリックします。
7. インストールする機能にチェックを付け、[次へ] をクリックします。
8. 表示された内容を確認したあと、[次へ] をクリックします。
9. Active Directory 証明書サービスのインストールする役割サービスで、[証明機関] にチェックが付いていることを確認し、[次へ] をクリックします。
10. 表示された内容を確認したあと、[次へ] をクリックします。
11. Web サーバー (IIS) のインストールする役割サービスにチェックを付け、[次へ] をクリックします。
12. [インストール] をクリックします。
13. インストールの終了後、サーバーマネージャーの通知アイコンをクリックし、[対象サ

## ユーザー認証を設定する

---

- サーバーに Active Directory 証明書サービスを構成する] をクリックします。
14. [次へ] をクリックします。
  15. 役割サービスで [証明機関] にチェックを付けて、[次へ] をクリックします。
  16. [エンタープライズ CA] を選択し、[次へ] をクリックします。
  17. [ルート CA] を選択し、[次へ] をクリックします。
  18. [新しい秘密キーを作成する] を選択し、[次へ] をクリックします。
  19. 秘密キーを作成するため、暗号化プロバイダー、キー長、ハッシュアルゴリズムを選択し、[次へ] をクリックします。
  20. 「この CA の共通名:」に CA の名前を入力し、[次へ] をクリックします。
  21. 証明書の有効期間を選択し、[次へ] をクリックします。
  22. 「証明書データベースの場所:」と「証明書データベース ログの場所:」は変更しないで [次へ] をクリックします。
  23. [構成] をクリックします。
  24. 構成に成功しましたというメッセージが表示されたら、[閉じる] をクリックします。

---

## サーバー証明書を作成する

---

「Web サーバー (IIS)」と「Active Directory 証明書サービス」のインストール後に次の手順でサーバー証明書を作成します。

ここでは Windows Server 2008 R2 を例に手順を説明します。

1. [スタート] メニューから、[管理ツール] をポイントし、[インターネットインフォメーションサービス (IIS) マネージャー] をクリックします。
2. 左枠の [サーバー名] をクリックして選択し、[サーバー証明書] をダブルクリックします。
3. 右枠の [証明書の要求の作成...] をクリックします。
4. すべての情報を入力して [次へ] をクリックします。
5. 「暗号化サービスプロバイダー:」でプロバイダーを選択し、[次へ] をクリックします。
6. [...] をクリックし、証明書を要求するためのファイル名を指定します。
7. ファイルを保存する場所を指定し、[開く] をクリックします。
8. [終了] をクリックし、インターネットインフォメーションサービス (IIS) マネージャーを終了します。

## LDAP 認証

---

LDAP サーバーを使用して、LDAP サーバーにアカウントを持つユーザーの認証をするときに設定します。LDAP サーバーにアカウントがないユーザーは認証を受けることができません。LDAP サーバーに登録されているアドレス帳を本機に自動で登録できるため、本機でアドレス帳の個人設定登録をしなくてもユーザー認証ができます。

LDAP 認証時にユーザー名、パスワードがネットワークに平文で流れるのを防止するために、本機と LDAP サーバー間で SSL による暗号化された通信をすることをお勧めします。そのときは事前に LDAP サーバーのサーバー証明書の作成が必要です。証明書の作成方法は、P. 30 「サーバー証明書を作成する」を参照してください。SSL の利用設定は LDAP サーバーで設定します。

接続する SSL サーバーが信頼できるかをチェックするには、サイト証明書のチェック機能を使用します。詳しくは Web Image Monitor のヘルプを参照してください。

認証方式で「平文認証」を選択していると LDAP 簡易認証が有効となり、DN ではなく、ユーザーの属性 (cn, uid など) により簡略化した認証ができます。

LDAP の認証方式で Kerberos 認証を選択するには、事前にレルムの登録が必要です。レルム名は必ず大文字で登録してください。レルムの登録方法は、Web Image Monitor のヘルプを参照してください。

### ★重要

- LDAP 認証を運用するとき、認証成功後に自動登録した認証済みユーザーのユーザー情報を本機で編集したときは、続く認証時の再取得により、ユーザー情報が書き換えられてしまうことがあるので注意してください。
- LDAP 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定できません。
- LDAP 認証を使用するときは、LDAP 検索時に SSL 設定されたサーバーには、参照機能が利用できません。
- Active Directory を使用して LDAP 認証をするときは、LDAP の認証種別で Kerberos 認証を選択し、同時に SSL を設定するとメールアドレスは取得できません。
- LDAP 認証を使用するとき、LDAP サーバーの設定で匿名認証を禁止にしていなかった場合は、LDAP サーバーにアカウントのないユーザーでも認証できることがあります。
- LDAP サーバーが Windows ActiveDirectory で構成されているときは、匿名認証が許可される場合があります。このような環境で使用するときは Windows 認証の利用をお勧めします。

### LDAP 認証の使用条件

LDAP 認証を設定するときは、次の条件が必要です。

## ユーザー認証を設定する

- 本機が LDAP サーバーを認識できる環境に接続されている
- SSL 使用時には、TLSv1 または SSLv3 が LDAP サーバーで動作する
- 本機に LDAP サーバーが登録されており、次の項目がすべて設定されている
  - 名前
  - サーバー名
  - 検索開始位置
  - ポート番号
  - SSL
  - 認証\*1
  - ユーザー名
  - パスワード
  - 日本語文字コード

\*1 認証は [Kerberos 認証]、[ダイジェスト認証]、[平文認証] のどれかに設定してください。

LDAP サーバーの登録方法は、Web Image Monitor のヘルプを参照してください。

### 補足

- ログインユーザー名、ログインパスワードに使用できる文字は、P. 12「ユーザー名、パスワードに使用できる文字」を参照してください。
- LDAP 簡易認証時に空パスワードでログインすると、認証に失敗します。空パスワードを許可するときは、サービス実施店にお問い合わせください。
- 設定後に未登録のユーザーが初めて本機を利用したときは、本機にユーザーが新規登録され、LDAP 認証設定時に「使用できる機能」で設定した機能が使用できます。ユーザーごとに利用できる機能を制限するには、あらかじめユーザーと「使用できる機能」の設定をアドレス帳に登録しておくか、新規登録したあと、ユーザーごとに「使用できる機能」を変更してください。2 回目以降の利用時には、ユーザーごとの「使用できる機能」の設定は維持されます。
- Kerberos 認証では、本機と KDC サーバーの間で暗号化通信をします。暗号化通信の設定は、P. 108「Kerberos 認証の暗号化設定」を参照してください。

管理者認証が設定されていることを確認してから設定してください。

1. Web Image Monitor から機器管理者がログインします。
2. [LDAP 認証] を設定します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ユーザー認証管理] ▶ 「ユーザー認証管理」 ▶ [LDAP 認証]

3. [プリンタージョブ認証] のレベルを選択します。



## ユーザー認証を設定する

---

プリンタージョブ認証については、P. 34「プリンタージョブ認証」を参照してください。

〔簡易（限定）〕を選択したときは、プリンタージョブ認証を簡易として扱う対象範囲を限定します。

IPv4 アドレスの範囲と、パラレル接続、USB 接続を対象とするかを設定できます。

### 4. 認証に使用する LDAP サーバーを選択します。

「LDAP 認証設定」 ▶ 「LDAP 認証」 ▶ 使用するサーバーを選択

### 5. ログイン名属性を入力します。

ログイン名属性は、認証ユーザーの情報取得のための検索条件として利用します。ログイン名属性で検索フィルターを作成して、ユーザーを特定してそのユーザーの情報を LDAP サーバーから本機のアドレス帳へ取得します。

ログイン名属性を（,）で区切って複数指定しているとき、ログイン名を1つ入力すると、指定した属性のどちらかでログイン名が一致したときに検索が成功します。また、ログイン名に（=）をつけて入力すると（例:cn=abcde, uid=xyz）、両方の属性が一致したときに検索が成功します。本機能は認証方式で「平文認証」を選択しているときに利用できません。

DN 形式で認証するときは、ログイン名属性を登録する必要はありません。

使用しているサーバー環境によりユーザー名の指定方法は異なります。使用しているサーバー環境を確認して入力してください。

### 6. 一意属性を入力します。

一意属性は、LDAP サーバーと本機のユーザー情報を対応させるために設定します。

一意属性を本機で設定すると、LDAP サーバーで一意属性が同じユーザー情報は、本機でも単一ユーザーとして扱えます。一意属性にはサーバーで一意な情報の管理に使用している属性を指定します。serialNumber、uidなどで、一意であればcnやemployeeNumberでも指定できます。

### 7. 「使用できる機能」でユーザーに使用を許可する機能を選択します。

選択した機能が LDAP 認証の対象となります。選択していない機能は、ユーザーは使用できません。

### 8. [OK] をクリックします。

### 9. ログアウトします。

## プリンタージョブ認証

---

プリンタージョブ認証とは、本機のジョブにユーザー認証をする機能です。

---

### プリンタージョブ認証のレベル

---

#### [すべて]

すべてのプリンタージョブ、およびリモートからの設定に認証チェックをするときに選択します。

ユーザー認証に対応していないプリンタードライバー、および装置からは印刷できません。

認証機能に対応していない環境からも印刷するときは、[簡易 (限定)] または [簡易] を選択してください。

#### [簡易 (限定)]

[簡易] の範囲を限定するときに選択します。

設定した範囲は認証機能に対応していなくても印刷できます。それ以外は認証機能への対応が必要です。

[簡易] の範囲を、パラレル接続、USB 接続、およびユーザーの IPv4 アドレスで設定できます。また、IPv6 アドレスの範囲は Web Image Monitor から設定できます。

#### [簡易]

印刷を指示するプリンタードライバーが装置が特定できないときや、本機の印刷に認証を必要としないときに選択します。

ユーザー認証に対応していないプリンタードライバーからのジョブ、および認証情報がないリモート設定は、認証チェックをしないで処理します。

ユーザー認証に対応したプリンタードライバーからのジョブ、および認証情報があるリモート設定に、認証チェックをします。

ユーザー認証をしなくても印刷できるため、想定外のユーザーに不正に使用されることがあるので注意してください。

---

### プリンタージョブの種類

---

プリンタージョブ認証のレベルとプリンタージョブの種類の間組み合わせによっては、正しく印刷されないことがあります。使用している環境に合わせて設定してください。

ユーザー認証を設定していないときは、すべての種類のプリンタージョブで印刷できます。

#### プリンタージョブの種類

1. 本機用のプリンタードライバーの設定で、「ユーザー認証」をチェックしたとき
2. 機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックし、さら

## ユーザー認証を設定する

に「暗号化する」をチェックしたとき

3. 機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックしたとき
4. 本機用のプリンタードライバーまたは、機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックしないとき

### プリンタージョブの種類

- a. プリンタードライバーから印刷したときです。ユーザー認証はユーザーコード認証です。

### 組み合わせ一覧

プリンタージョブ認証	簡易	簡易	簡易	すべて	すべて	すべて
ドライバー暗号鍵：暗号強度設定	簡易暗号	DES	AES	簡易暗号	DES	AES
プリンタージョブの種類 1	C*1	C*1	C*1	C*1	C*1	C*1
プリンタージョブの種類 2	C*1	C*1	X*1	C*1	C*1	X*1
プリンタージョブの種類 3	B	X*1	X*1	B	X*1	X*1
プリンタージョブの種類 4	X	X	X	X	X	X
プリンタージョブの種類 5	A	A	A	B	B	B
プリンタージョブの種類 6	A	A	A	X	X	X
プリンタージョブの種類 7	A	A	A	X	X	X
プリンタージョブの種類 8	B	B	B	B	B	B
プリンタージョブの種類 9	A	A	A	X	X	X
プリンタージョブの種類 10	C*1	C*1	C*1	C*1	C*1	C*1
プリンタージョブの種類 a	B	B	B	B	B	B

\*1 ユーザーコード認証時は B になります。

A：ユーザー認証に関係なく印刷できます。

B：ユーザー認証が通れば印刷できます。ユーザー認証が通らなければ印刷できません。ジョブがリセットされます。

## ユーザー認証を設定する

---

C : ユーザー認証が通り、プリンタードライバーと本機の [ドライバー暗号鍵] が一致すれば印刷できます。一致しなければ、ジョブがリセットされます。

× : ユーザー認証に関係なく印刷できません。ジョブがリセットされます。

### 補足

- 「ドライバー暗号鍵 : 暗号強度設定」については、P. 154 「セキュリティ強化機能を設定する」を参照してください。

## authfree コマンド

---

プリンタージョブ認証で [簡易 (限定)] を選択しているとき、telnet の authfree コマンドでプリンタージョブ認証から除外する対象を設定できます。

telnet にログインするときのログインユーザー名とログインパスワードについては管理者へ問い合わせてください。

### 現在の設定の表示

```
msh> authfree
```

- プリンタージョブ認証が [簡易 (限定)] に設定されているときに表示できます。

### IPv4 アドレスの設定

```
msh> authfree "対象 ID" range "始点アドレス" "終点アドレス"
```

### IPv6 アドレスのレンジでの設定

```
msh> authfree "対象 ID" range6 "始点アドレス" "終点アドレス"
```

### IPv6 アドレスのマスクでの設定

```
msh> authfree "対象 ID" mask6 "基準アドレス" "マスク長"
```

### パラレル/USB の設定

```
msh> authfree {parallel|usb} {on|off}
```

- パラレル接続、USB 接続をプリンタージョブ認証から除外するときに「on」にします。工場出荷時の設定は「off」です。

### 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。

## ロックアウト機能

ログイン時にパスワードを連続して間違えて入力すると、ロックアウト機能が働き、そのユーザー名でのログインが禁止されます。ロックアウトされたユーザーは、正しいパスワードを入力したときも認証失敗となり、一定時間が経過してロックアウトが解除されるか、管理者またはスーパーバイザーがロックアウト機能を解除するまで、本機を利用できません。ユーザーコード認証では、スーパーバイザーと各管理者だけがロックアウトの対象となり、ユーザーには機能しません。

### パスワードロックアウト機能の設定項目

ロックアウト機能は Web Image Monitor で設定します。

設定項目	設定内容	設定値	工場出荷時の設定値
ロックアウト	ロックアウト機能を有効にするかしないかを設定します。	<ul style="list-style-type: none"> <li>▪ 有効</li> <li>▪ 無効</li> </ul>	無効
ログインパスワード入力許容回数	パスワードの入力ミスを許容する回数を指定します。	1-10	5
ロックアウト解除タイマー	一定時間経過後のロックアウト解除を有効にするかしないかを設定します。	<ul style="list-style-type: none"> <li>▪ 有効</li> <li>▪ 無効</li> </ul>	無効
ロックアウト解除までの時間	ロックアウトを解除するまでの時間を設定します。	1-9999 分	60 分

### ロックアウト解除の関係

ロックアウト対象者によって解除できる管理者が異なります。

## ユーザー認証を設定する

ロックアウト対象者	解除者
ユーザー	ユーザー管理者
ユーザー管理者、ネットワーク管理者、 文書管理者、機器管理者	スーパーバイザー
スーパーバイザー	機器管理者

## パスワードロックアウト設定

1. Web Image Monitor から機器管理者がログインします。
2. ユーザーロックアウト機能を有効にします。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [ユーザーロックアウト]  
▶ 「ロックアウト」 ▶ [有効]

3. ログインパスワードの入力許容回数を設定します。

「ログインパスワード入力許容回数」 ▶ 許容回数を選択

4. 一定時間でロックアウトを解除するときは、タイマーを有効にします。

「ロックアウト解除タイマー」 ▶ [有効] ▶ 「ロックアウト解除までの時間」 ▶  
時間を分単位で入力

5. [OK] をクリックします。  
パスワードロックアウトが設定されます。
6. ログアウトします。

## パスワードロックアウト解除

1. Web Image Monitor からユーザー管理者がログインします。
2. ロックアウトを解除するユーザーを選択します。

## ユーザー認証を設定する

---

[機器の管理] ▶ [アドレス帳] ▶ ロックアウトを解除するユーザーを選択

### 3. ロックアウトを解除します。

[詳細入力] ▶ [変更] ▶ 「ロックアウト」 ▶ [無効]

### 4. [OK] をクリックします。

### 5. ログアウトします。

#### ↓ 補足

- 管理者とスーパーバイザーのパスワードロックアウトは、電源を一度切ってから再び入れるか、Web Image Monitor の [設定] ▶ [管理者登録/変更] で解除できません。

## オートログアウト時間設定

---

ログインした状態で一定時間、画面の操作をしないときに、自動でログアウトすることを「オートログアウト」と言います。

オートログアウト機能が働くまでの時間を設定します。

1. Web Image Monitor から機器管理者がログインします。
2. 「オートログアウト時間設定」を有効にします。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [タイマー] ▶ 「オートログアウト時間設定」 ▶ [する]

3. 「60～999」（1 秒単位）の範囲で時間を入力します。
4. [OK] をクリックします。
5. ログアウトします。

↓ 補足

- 紙づまりやトナー切れなどのときは、オートログアウトが働かないことがあります。



## 機器の利用を制限する

ユーザーの本機の利用を制限する方法を説明します。

---

### 管理者設定項目の変更を防止する

---

本機の設定項目は、管理者の種類によって設定できる項目が異なり、管理者を分けることで操作できる範囲を制限できます。

本機では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」を参照してください。

管理者の登録方法は、P. 11「管理者を登録、変更する」を参照してください。

---

### ユーザーによる設定の変更を禁止する

---

管理者設定項目をユーザーが変更することを禁止できます。

管理者認証を有効にした管理者の設定項目は、ユーザーによる変更ができません。

管理者認証の設定については、P. 9「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を設定する

---

システム初期設定以外の各機能の初期設定メニューに対するユーザーのアクセス権を制限します。この機能は、ユーザー認証による管理をしないときも有効です。

メニュープロテクトの設定を変更するには、事前に管理者認証を有効にします。管理者認証の設定方法は、P. 9「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は2段階のレベルで操作権限を変更できます。レベルごとの初期設定項目の操作権限は、P. 176「設定項目の操作権限一覧」を参照してください。

[レベル1] [レベル2] [しない]から選択します。[レベル1]よりも [レベル2] のほうが制限が強くなります。[しない]を選択するとメニュープロテクトが無効になります。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. メニュープロテクトを設定します。

[調整/管理] ▶ [OK] ▶ [一般管理] ▶ [OK] ▶ [メニュープロテクト] ▶ [OK]

3. メニュープロテクトのレベルを設定します。

レベルを選択 ▶ [OK]

4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

## 機能の利用を制限する

---

本機の各種機能にユーザーのアクセス権を設定し、第三者による不正操作を防止できます。アドレス帳に登録されたユーザーに、そのユーザーがログインしたときに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できます。

### 使用できる機能

- プリンター
- 拡張機能

1. Web Image Monitor からユーザー管理者がログインします。
2. ユーザーを選択します。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. ユーザーに使用を許可する機能を選択します。

[詳細入力] ▶ [変更] ▶ 「使用できる機能」 ▶ 使用を許可する機能を選択

4. [OK] をクリックします。
5. ログアウトします。

## ユーザーの印刷利用量を制限する

ユーザーごとに印刷利用量を制限できます。利用量が上限に達すると、ジョブをキャンセルし、メッセージを表示します。

ユーザーごとの印刷利用量は、ユーザー管理者、または機器管理者が設定します。

### 印刷利用量

印刷利用量は「印刷ページ数×度数」という計算方法でカウントされます。

度数とは、印刷条件ごとに重みを付ける値です。たとえば、度数 10 の条件で 1 ページ印刷すると、印刷利用量は 10 です。

印刷利用量は、ユーザーごとにカウントされます。

### 設定項目

項目名	説明	設定値
上限到達時動作設定	<p>利用量制限をするかしないか、および制限の方法を選択します。</p> <ul style="list-style-type: none"> <li>▪ ジョブ中断 上限に達すると、実行中のジョブ、および実行待ちのジョブがキャンセルされます。</li> <li>▪ ジョブ終了後制限 上限に達すると、実行中のジョブは継続されますが、実行待ちのジョブはキャンセルされます。</li> <li>▪ 継続利用許可 利用量を制限しません。</li> </ul>	<ul style="list-style-type: none"> <li>▪ 継続利用許可（工場出荷時の設定）</li> <li>▪ ジョブ終了後制限</li> <li>▪ ジョブ中断</li> </ul>
印刷利用量制限度数設定	<p>印刷条件ごとに 0~200 で度数を設定します。 それぞれの項目の工場出荷時の度数は、1 です。</p>	<ul style="list-style-type: none"> <li>▪ プリンター：A3/DLT</li> <li>▪ プリンター：その他</li> </ul>

## 機器の利用を制限する

---

### 利用量制限を設定したときの注意事項

次の操作をしたときは、印刷ができません。

- 認証済みユーザーのログイン中に、アドレス帳に登録されたそのユーザーのログインユーザー名またはユーザーコードを変更したとき

次の条件のときは、利用量制限の対象外です。

- 使用中の認証方式に対応していない OS からの印刷

---

### 利用量制限を設定する

---

1. Web Image Monitor から機器管理者がログインします。
2. 利用量が上限に到達したときの動作を設定します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [印刷利用量制限] ▶ 「上限到達時動作」 ▶ [ジョブ中断]、または [ジョブ終了後制限]

3. 印刷利用量の制限度数を入力します。

「印刷利用量制限度数設定」 ▶ 印刷条件を選択 ▶ 「0~200」の範囲で度数を入力

0 を設定すると利用量は制限されません。

4. [OK] をクリックします。
5. ログアウトします。

### ユーザーコード認証時の制限事項

---

ユーザーコード認証有効時に、利用量制限を設定したときは、次の制限事項があります。

- 「ユーザー認証管理」でプリンター機能の自動登録が有効になっていると、設定した利用量制限の度数がユーザーのカウンターに反映されないことがあります。  
ユーザーコード認証有効時に利用量を制限するときは、自動登録を設定しないでください。
- 利用量制限のログは、ジョブログやアクセスログとして記録されません。
- ユーザーコード認証の設定によっては、利用量制限の設定にかかわらず、ログインをしていないユーザーによる印刷ができます。[ユーザー認証管理] の [ユーザーコード認証] の「制限する機能」ですべての機能を制限してください。

## 機器の利用を制限する

---

### ユーザーごとに利用量上限を設定する

---

1. Web Image Monitor からユーザー管理者がログインします。
2. 設定するユーザーを選択します。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. 「印刷利用量制限」を有効にします。

[詳細入力] ▶ [変更] ▶ 「印刷利用量制限」 ▶ [する]

4. 「0~999,999」の範囲で上限値を入力します。
5. [OK] をクリックします。
6. ログアウトします。

---

### ユーザーの利用量を確認する

---

1. Web Image Monitor から管理者がログインします。
2. ユーザー一覧に確認するユーザーを表示させます。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. [利用量] と [上限値] の数値を確認します。
4. 確認が終了したらログアウトします。

---

### 利用量カウンターをクリアする

---

利用量カウンターが上限に達したときは、該当するユーザーのカウンターをクリアするか、上限度数の設定値を上げると、印刷を再開できます。

1. Web Image Monitor からユーザー管理者がログインします。
2. カウンターをクリアするユーザーを選択します。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. カウンターをクリアします。

[詳細入力] ▶ [変更] ▶ 「利用量」 ▶ [クリア] ▶ [OK]

4. [OK] をクリックします。
5. ログアウトします。

---

### 自動リセット機能を設定する

---

設定したタイミングで利用量カウンターをリセットできます。

選択項目	詳細
月ごと	毎月決まった日にち・時刻にリセットします
日時を指定	指定した年月日・時刻にリセットします。1度だけ実施されます
指定日数ごと	基準の年月日から設定した間隔が経つとリセットされ、以降は同じ間隔でリセットされます

1. Web Image Monitor から機器管理者がログインします。
2. 自動リセットを実施するタイミングを選択します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [印刷利用量制限] ▶ 「利用量カウンター定期/指定リセット設定」 ▶ [しない]、[日時を指定]、[指定日数ごと]、[月ごと] のどれかを選択

3. 条件を設定します。

条件を入力 ▶ [OK]

4. ログアウトします。

#### 補足

- 指定した日時に本機の電源が入っていないときは、電源を入れたときにリセットされます。
- [月ごと] で、31日など日付がカレンダーにないときは、翌月1日の0:00にリセ

## 機器の利用を制限する

---

ットされます。

- 使用できる機能の設定は Web Image Monitor からできます。



## 機器情報の漏洩を防止する

本機のメモリーに保存された情報を保護する方法を説明します。

---

### アドレス帳の登録情報を保護する

---

アドレス帳のデータに、ユーザーごとにアクセス権を設定したり、アドレス帳のデータを暗号化して、個人情報の漏洩を防止できます。

---

#### アドレス帳にアクセス権を設定する

---

アドレス帳登録者、フルコントロール権限のあるユーザー、およびユーザー管理者が設定します。

1. Web Image Monitor からユーザー管理者がログインします。
2. アクセス権を変更するユーザーを選択します。

[機器の管理] ▶ [アドレス帳] ▶ ユーザーを選択

3. アクセス許可の設定画面を表示します。

[詳細入力] ▶ [変更] ▶ 「認証保護」 ▶ 「あて先保護」 ▶ 「アクセス権」 ▶ [変更]

4. アクセス権を付与するユーザーを表示し、アクセス権を設定してから、[OK] をクリックします。

「全員に公開」で設定すると、すべてのユーザーにアクセス権が設定されます。

5. [OK] をクリックします。
6. ログアウトします。

#### ↓ 補足

- 本機を安全に使用するために、認証ユーザーにも [編集]、[編集/削除]、[フルコントロール] の権限を与えないで運用することをお勧めします。

## 機器情報の漏洩を防止する

### アドレス帳を暗号化する

アドレス帳のデータを暗号化します。この設定により、アドレス帳データの読み取りを防止できます。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部からユーザー管理者がログインします。
2. [アドレス帳暗号化] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [セキュリティ強化] ▶ [OK] ▶ [アドレス帳暗号化] ▶ [OK]

3. 暗号鍵を入力します。

[する] ▶ [暗号鍵] ▶ [入力] ▶ 暗号鍵を入力 ▶ [入力終了]

暗号鍵は、半角英数字 32 文字以内で入力してください。

4. 確認のための暗号鍵を再入力します。

[入力] ▶ 暗号鍵を再入力 ▶ [入力終了]

5. 暗号化を実行します。

[する] ▶ メッセージを確認し、[実行する]

暗号化/復号化中に電源スイッチを切らないでください。実行中に電源スイッチを切ると、データが壊れることがあります。

アドレス帳の暗号化処理の実行は、時間がかかることがあります。

アドレス帳の暗号化の処理時間は、ユーザー数の登録件数によって処理時間が異なります。また、処理実行中は、本機を使用できません。

暗号化中に [中止] を押しと、データは暗号化されません。

復号化中に [中止] を押しと、データは暗号化されたままです。

暗号化が終了すると「暗号（復号）化を完了しました。 [確認] を押してください。」が表示されます。

6. [確認] を押します。
7. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

↓ 補足

- アドレス帳の暗号化をしたあとに追加したユーザーも暗号化されます。
- SD カードまたは、Web Image Monitor でバックアップされたアドレス帳は暗号化されています。

## 機器のデータを暗号化する

---

### ⚠ 注意



- SD カードは、子供の手に触れないようにしてください。もし子供が誤って SD カードを飲み込んだときは、直ちに医師の診断を受けてください。

本機に蓄積されるアドレス帳データ、認証情報、蓄積文書などをデータの記録時に暗号化して、情報の漏洩を防止します。

暗号化されたデータの復元には、データ暗号化設定時に生成される暗号鍵を使用します。暗号鍵は途中で変更できます。

### 暗号化の対象となるデータ

電源を切ってもデータを保持する本機搭載メモリーに蓄積される次のデータが暗号化されます。

- アドレス帳
- ユーザー認証データ
- 一時保存されている文書データ
- ログ
- ネットワーク I/F 設定情報
- 機器設定情報

#### ↓ 補足

- 本機の入替え時に既存のデータを引き継ぐときは、データが暗号化されていても新しい機器に引き継ぐことができます。データの引継ぎはサービス実施店に依頼してください。

### 暗号化設定の所要時間

暗号化を設定するときは、データを消去（初期化）してから暗号化を始めるか、すでにあるデータを暗号化して残すかを選択します。残すデータがあると、暗号化設定に時間がかかります。

機器情報の漏洩を防止する

設定	暗号化して残すデータ	初期化するデータ	所要時間の目安
[ファイルシステムデータのみ] / [ファイルシステムデータのみ引き継ぎ]	<ul style="list-style-type: none"> <li>▪ Embedded Software Architecture アプリケーションプログラム/ログ</li> <li>▪ アドレス帳</li> <li>▪ 登録したフォント</li> <li>▪ ジョブログ/アクセスログ</li> <li>▪ スプールされたジョブ</li> </ul>	<ul style="list-style-type: none"> <li>▪ 蓄積文書（機密印刷/試し印刷/保存印刷/保留印刷関連）</li> </ul>	約 1 時間
[全データ] / [全データ引き継ぎ]	全データ： [ファイルシステムデータのみ] / [ファイルシステムデータのみ引き継ぎ] で暗号化して残すデータと、初期化するデータの両方	なし	約 2 時間
[全データ初期化]	なし	全データ： [ファイルシステムデータのみ] / [ファイルシステムデータのみ引き継ぎ] で暗号化して残すデータと、初期化するデータの両方	数分

暗号化設定を有効にするときの注意事項

- Embedded Software Architecture アプリケーションを使用するときは、必ず [ファイルシステムデータのみ] / [ファイルシステムデータのみ引き継ぎ] または [全データ] / [全データ引き継ぎ] を選択してください。
- [全データ初期化]、[ファイルシステムデータのみ] / [ファイルシステムデータ

## 機器情報の漏洩を防止する

のみ引き継ぎ]、[全データ] / [全データ引き継ぎ] のどれを選択しても、本機の初期設定は初期化されません。

## 暗号化設定を有効にする

### ★重要

- 暗号化設定の実行時は本機の操作はできません。
- 暗号化設定を一度実行すると、途中で中止できません。また、暗号化設定の実行中に電源が切られないよう必ず確認をしてください。
- 暗号鍵は、障害時のデータリカバリーなどに必要です。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号化の設定は、操作部での設定手順を完了し、電源を一度切ってから再び入れて本機が再起動されたあとに有効になります。
- [全データ初期化] を選択して暗号化を設定すると、再起動後の時間が短くなりますが、すべてのデータが初期化されます。また、再起動後に暗号化が実行されている途中で再度電源を切ったときにもすべてのデータが初期化されます。アドレス帳など、重要なデータは暗号化の前にバックアップを取っておくことをお勧めします。
- 暗号鍵の更新が正常に終了しなかったときは、印刷された暗号鍵は無効です。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. [暗号化] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [機器データ暗号化設定] ▶ [OK] ▶ [暗号化] が表示されていることを確認 ▶ [OK]

3. 初期化しないで残すデータを選択します。

残すデータを選択 ▶ [OK]

すべてのデータを残すときは [全データ引き継ぎ]、本機の設定データだけを残すときは [ファイルシステムデータのみ引き継ぎ] を選択します。すべてのデータを初期化するときは [全データ初期化] を選択します。

4. 初期化しないで残すデータを選択します。

## 機器情報の漏洩を防止する

残すデータを選択 ▶ [OK]

すべてのデータを残すときは [全データ引き継ぎ]、本機の設定データだけを残すときは [ファイルシステムデータのみ引き継ぎ] を選択します。すべてのデータを初期化するときは [全データ初期化] を選択します。

### 5. 暗号鍵をバックアップします。

[紙に印刷] ▶ [印刷] ▶ [実行]

### 6. [確認] を選択します。

### 7. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

### 8. 本機の電源を切り、再度、電源を入れます。

本機の電源を入れると、メモリー変換が実行されます。「メモリー変換を完了しました。電源を切ってください。」のメッセージが表示されるまで待ってください。

メッセージが表示されたら再度本機の電源を切ってください。

電源の入れかた、切りかたは、『使用説明書』「電源の入れかた、切りかた」を参照してください。

## 暗号鍵をバックアップする

暗号鍵のバックアップができます。



重要

- 暗号鍵は、障害時のデータリカバリーなどに必要です。出力されるバックアップ用データ暗号鍵は大切に保管してください。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

### 1. 操作部から機器管理者がログインします。

### 2. [機器データ暗号鍵バックアップ] を選択します。

[セキュリティー管理] ▶ [OK] ▶ [機器データ暗号化設定] ▶ [OK] ▶ [機器データ暗号鍵バックアップ] ▶ [OK]

## 機器情報の漏洩を防止する

---

### 3. 暗号鍵をバックアップします。

[紙に印刷] ▶ [印刷]

### 4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

---

## 暗号鍵を更新する

---

暗号鍵を新しいものに変更します。本機が正常に動作している状態で、機器データ暗号化が設定されているときに変更できます。

#### ★重要

- 暗号鍵は、障害時のデータリカバリーなどに必要です。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号鍵の更新をすると、新しい暗号鍵を使用して暗号化します。新しい暗号鍵での暗号化設定は、操作部での設定手順を完了し、電源を一度切ってから再び入れて本機が再起動したあとに有効になります。
- 暗号鍵の更新が正常に終了しなかったときは、印刷された暗号鍵は無効です。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. [機器データ暗号鍵更新] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [機器データ暗号化設定] ▶ [OK] ▶ [機器データ暗号鍵更新] ▶ [OK]

### 3. 初期化しないで残すデータを選択します。

残すデータを選択 ▶ [OK]

すべてのデータを残すときは [全データ引き継ぎ]、本機の設定データだけを残すときは [ファイルシステムデータのみ引き継ぎ] を選択します。すべてのデータを初期化するときには [全データ初期化] を選択します。



4. 更新した暗号鍵をバックアップします。

[紙に印刷] ▶ [印刷] ▶ [実行]

5. [確認] を選択します。

6. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

7. 本機の電源を切り、再度、電源を入れます。

本機の電源を入れると、メモリー変換が実行されます。「メモリー変換を完了しました。電源を切ってください。」のメッセージが表示されるまで待ってください。

メッセージが表示されたら再度本機の電源を切ってください。

電源の入れかた、切りかたは、『使用説明書』「電源の入れかた、切りかた」を参照してください。

---

## 暗号化を解除する

---

データの暗号化が不要になったとき、暗号化の設定を解除できます。

**★重要**

- 暗号化の解除は、操作部での設定手順を完了し、電源を一度切ってから再び入れて本機が再起動したあとに有効になります。
- 本機を廃棄するときはメモリー全消去をしてください。メモリー全消去については、P.59「データを上書き消去する」を参照してください。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。

2. [暗号化解除] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [機器データ暗号化設定] ▶ [OK] ▶ [暗号化解除] ▶ [OK]

3. 初期化しないで残すデータを選択します。

残すデータを選択 ▶ [OK]

## 機器情報の漏洩を防止する

---

すべてのデータを残すときは [全データ引き継ぎ]、本機の設定データだけを残すときは [ファイルシステムデータのみ引き継ぎ] を選択します。すべてのデータを初期化するときは [全データ初期化] を選択します。

### 4. 暗号化解除を実行します。

[実行] ▶ [確認]

### 5. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

### 6. 本機の電源を切り、再度、電源を入れます。

電源の入れかた、切りかたは、『使用説明書』「電源の入れかた、切りかた」を参照してください。

## データを上書き消去する

---

一時的に保存されたジョブのデータを自動で上書き消去（メモリー自動消去）したり、本機を廃棄するときに、蓄積されているすべてのデータを上書き消去（メモリー全消去）すると、データの漏洩を防止できます。

本機は、本機メモリーの上書き消去（メモリー全消去）だけできます。

---

### 使用環境

---

- 本機が正常な状態（壊れていたり、改造されたり、本機の一部を取り除かれていない状態）で使用されている。
  - 本書をよく読んでその内容を十分に理解し、一般の使用者が本製品を正しく使用できるように対応がとれる担当者によって管理されている。
- 

### 使用上のご注意

---

メモリー自動消去、メモリー全消去は、機器管理者が設定してください。

- 本機の電源を切るときは上書き消去アイコン、またはメモリー内残存データ状態が「残存データ無し」と表示されていることを確認し、残存データがない状態であることを必ず確認してください。
  - 上書き消去中は、[スリープモード移行時間設定]を設定していても、スリープモードには移行しません。上書き処理が完了した時点で移行します。
  - 上書き消去の対象となるデータが残っていないにもかかわらず上書き消去アイコン、またはメモリー内残存データ状態が「残存データ有り」と表示されるときは、本機の電源を一度切り、再び電源を入れて、「残存データ無し」と表示されるかを確認してください。表示が変更されないときはサービス実施店に連絡してください。
- 

### メモリー自動消去を設定する

---

#### ★重要

- メモリー自動消去が完了する前に電源を切ると、上書き消去は一時中断されます。
  - 万一、メモリー自動消去が完了する前に電源を切ったときは、電源を再び入れたときに、メモリー自動消去を続きから設定します。
  - 上書き消去中にエラーが発生したときは、電源を一度切ってください。再び電源を入れて、手順をやり直してください。
- 

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
-

2. [メモリー自動消去設定] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [メモリー自動消去設定] ▶ [OK] ▶ [する]

3. 消去方式を選択します。

- NSA 方式

[消去方式] ▶ [NSA 方式] ▶ [OK]

- DoD 方式

[消去方式] ▶ [DoD 方式] ▶ [OK]

- 乱数方式

[消去方式] ▶ [乱数方式] ▶ 消去回数を入力 ▶ [OK]

4. [OK] キーを押します。

5. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

↓ 補足

- メモリー自動消去と暗号化機能を組み合わせて設定したときは、上書き消去で書き込むデータも暗号化されます。

メモリー自動消去設定を解除する

---

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. [メモリー自動消去設定] を選択します。

## 機器情報の漏洩を防止する

---

[セキュリティ管理] ▶ [OK] ▶ [メモリー自動消去設定] ▶ [OK]

### 3. [しない] を選択します。

[しない] ▶ [OK]

### 4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

## 上書き消去できるデータ／できないデータ

---

上書き消去できるデータと、上書き消去できないデータは次のとおりです。

### 上書き消去できるデータ

- 印刷のデータ
- 機密印刷/試し印刷/保留印刷/保存文書（プリンターに保存）のデータ  
機密印刷/試し印刷/保留印刷のデータは、印刷されてはじめて上書き消去の対象となります。保存文書のデータは、削除されてはじめて上書き消去の対象となります。
- スプール印刷のデータ

### 上書き消去できないデータ

- アドレス帳に登録されているデータ  
アドレス帳に登録されているデータの不正利用を防止するために暗号化ができません。詳しくは、P. 49「アドレス帳の登録情報を保護する」を参照してください。
- ユーザーコード別カウンター
- イメージオーバーレイデータ  
イメージオーバーレイデータは、削除されてはじめて上書き消去の対象となります。

## メモリー全消去

---

本機を移設または廃棄するときに、すべてのデータを一括して上書き消去できます。

次の情報もメモリー全消去の対象です。メモリー全消去後に本機を使用するときは、サービス実施店に相談してください。

- ユーザーコード
- ユーザーコード別カウンター
- アドレス帳

## 機器情報の漏洩を防止する

---

- ユーザーがダウンロードしたプリンターフォント
- Embedded Software Architecture アプリケーション
- SSL 機器証明書
- 本機のネットワーク設定

### ★重要

- メモリー全消去を実行している間は、本機の操作はできません。メモリー全消去の一時停止の操作だけできます。乱数方式を選択して書き込み回数を3回に設定したときは、最大約5時間45分かかります。
- メモリー全消去が完了すると、本機のセキュリティー設定も消去され、本機の管理やユーザーの管理ができなくなります。メモリー全消去後に再度データが不特定ユーザーに書き込まれないように取り扱いに注意してください。

## メモリー全消去を使用する

---

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 本機に接続されているケーブルをすべて取り外します。
2. 操作部から機器管理者がログインします。
3. [メモリー全消去] を選択します。

[セキュリティー管理] ▶ [OK] ▶ [メモリー全消去] ▶ [OK]

4. 消去方式を選択します。

- NSA 方式

[NSA 方式] ▶ [OK]

- DoD 方式

[DoD 方式] ▶ [OK]

- 乱数方式

[乱数方式] ▶ 消去回数を入力 ▶ [OK]

5. [消去する] を押します。

## 機器情報の漏洩を防止する

---

本機が自動的に再起動し、メモリー全消去を開始します。

### 6. メモリー全消去が完了したら【確認】を押して電源を切ります。

電源の切りかたは、『使用説明書』「電源の入れかた、切りかた」を参照してください。

#### 補足

- 万一、メモリー全消去が完了する前に電源スイッチを切ったときは、電源を再び入れたときに、メモリー全消去を最初から設定します。
- メモリー全消去中にエラーが発生したときは、電源スイッチを一度切り、再び電源を入れて、手順 2 から設定し直してください。

## メモリー全消去を一時停止する

---

メモリー全消去中に本機の電源を切りたいときは、一時停止すると電源を切ることができます。

電源を再び入れるとメモリー全消去が再開されます。

1. メモリー全消去処理中に【一時停止】を押します。
2. 【停止する】を押します。
3. 電源を切ります。

電源の切りかたは、『使用説明書』「電源の入れかた、切りかた」を参照してください。

## ネットワークセキュリティを強化する

本機をネットワークに接続して使用するとき、セキュリティを高める機能について説明します。

---

### アクセスコントロールを設定する

---

本機は TCP/IP 通信を使ったアクセスに、アクセスコントロールができます。

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] に設定すると、アクセスできるパソコンの IP アドレスは、192.168.15.16~192.168.15.20 です。

**★重要**

- アクセスコントロールは LPR、RCP/RSH、FTP、SSH/SFTP、Bonjour、SMB、WSD (Device)、WSD (Printer)、IPP、DIPRINT、RHPP、Web Image Monitor からの利用を制限できません。
  - telnet、SNMP からの利用は制限できません。
1. Web Image Monitor からネットワーク管理者がログインします。
  2. [アクセスコントロール] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティ」 ▶ [アクセスコントロール]

3. アクセスコントロールの範囲を指定します。

- IPv4 のとき

「アクセスコントロール範囲」 ▶ 本機にアクセスを許可する IP アドレスの数値を入力

- IPv6 のとき（範囲指定、マスク指定のどちらかで設定）

- 「範囲指定」 ▶ 本機にアクセスを許可する IP アドレスの数値を入力
- 「マスク指定」 ▶ 本機にアクセスを許可する IP アドレスの基準アドレスを入力 ▶ 「マスク長」を入力



4. [OK] をクリックします。
5. 「設定の書き換え中」画面が表示されます。1~2分経過してから [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。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
6. ログアウトします。

## プロトコルの有効／無効を設定する

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 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
IPv4	-	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	<p>IPv4 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。</p> <p>IPv4 通信しているときに Web Image Monitor で IPv4 の無効化はできません。</p>
IPv6	-	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	<p>IPv6 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。</p>
IPsec	-	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	<p>IPsec による暗号化通信ができなくなります。</p>
FTP	TCP:21	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	<p>FTP の機能が使用できなくなります。</p> <p>操作部からの設定で個人情報の表示だけを禁止できます。</p>
ssh/sftp	TCP:22	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	<p>sftp の機能が使用できなくなります。</p> <p>操作部からの設定で個人情報の表示だけを禁止できます。</p>

ネットワークセキュリティを強化する

プロトコル	ポート	設定手段	無効時の状態
telnet	TCP:23	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> </ul>	telnet の機能が使用できなくなります。
SMTP	TCP:25 (可変)	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ Web Image Monitor</li> </ul>	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	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	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	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	HTTPS の機能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 通信だけを許可し、非 SSL 通信を禁止できます。
SMB	TCP:139	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	SMB の機能が使用できなくなります。
NBT	UDP:137 UDP:138	<ul style="list-style-type: none"> <li>▪ telnet</li> </ul>	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。
SNMPv1/v2	UDP:161	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	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 による設定だけを禁止し、参照は許可できます。

ネットワークセキュリティを強化する

プロトコル	ポート	設定手段	無効時の状態
SNMPv3	UDP:161	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	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 暗号通信だけ許可し、非 SNMPv3 暗号通信は禁止できます。
RSH/RCP	TCP:514	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	RSH の機能、ネットワーク TWAIN 機能が使用できなくなります。 操作部からの設定で個人情報の表示だけを禁止できます。
LPR	TCP:515	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	LPR 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表示だけを禁止できます。
IPP	TCP:631	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	IPP の機能が使用できなくなります。
SSDP	UDP:1900	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	Windows からの UPnP による機器検索ができなくなります。
Bonjour	UDP:5353	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	Bonjour の機能が使用できなくなります。
DIPRINT	TCP:9100	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	DIPRINT の機能が使用できなくなります。
RFU	TCP:10021	<ul style="list-style-type: none"> <li>▪ 操作部</li> <li>▪ telnet</li> </ul>	FTP 経由でリモートファームウェア更新を試みます。

## ネットワークセキュリティを強化する

プロトコル	ポート	設定手段	無効時の状態
WSD (Device)	TCP:53000 (可変)	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	WSD (Device)の機能が使用できなくなります
WSD (Printer)	TCP:53001 (可変)	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	WSD (Printer)の機能が使用できなくなります。
WS-Discovery	TCP:3702 UDP:3702	<ul style="list-style-type: none"> <li>▪ telnet</li> </ul>	WSD (Device/Printer)の機器検索ができなくなります。
RHPP	TCP:59100	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	RHPPで印刷ができなくなります。
LLTD	-	<ul style="list-style-type: none"> <li>▪ telnet</li> </ul>	LLTDによる機器検索ができなくなります。
LLMNR	UDP:5355	<ul style="list-style-type: none"> <li>▪ Web Image Monitor</li> <li>▪ telnet</li> </ul>	LLMNRによる名前解決要求に応答できなくなります。

### 補足

- 「無効時の状態」欄に記載されている個人情報の表示禁止は、操作部の「個人情報表示制限」で設定できます。詳しくは、P.154「セキュリティ強化機能を設定する」を参照してください。

## 操作部から設定する

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部からネットワーク管理者がログインします。
2. [有効プロトコル] を選択します。

[インターフェース設定] ▶ [OK] ▶ [ネットワーク設定] ▶ [OK] ▶ [有効プロトコル] ▶ [OK]

3. 設定するプロトコルの有効/無効を選択します。

プロトコルを選択 ▶ [OK] ▶ 有効/無効を選択 ▶ [OK]

4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

---

Web Image Monitor から設定する

---

1. Web Image Monitor からネットワーク管理者がログインします。
2. [ネットワークセキュリティ] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティ」 ▶ [ネットワークセキュリティ]

3. 設定するプロトコルの有効/無効（または、オープン/クローズ）を選択します。
4. [OK] をクリックします。
5. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
6. ログアウトします。

## ネットワークセキュリティレベルを設定する

プロトコルの有効／無効を4段階のレベルで自動的に設定し、セキュリティ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。

**★重要**

- ネットワークセキュリティレベルによっては一部のユーティリティで通信ができない、またはログインに失敗することがあります。

セキュリティレベル	説明
[レベル0]	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。
[レベル1]	適切なセキュリティ強度を持ちます。たとえば社内LANに接続するときなどに設定します。
[FIPS140]	[レベル1]と[レベル2]の中間のセキュリティ強度を持ちます。 暗号/認証アルゴリズムとして、米国政府の推奨暗号だけを使用します。 アルゴリズム以外の設定値は、[レベル2]と同等です。
[レベル2]	最高度のセキュリティ強度を持ちます。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。
[カスタム]	上記レベル以外の状態です。Web Image Monitorで設定します。

### 操作部から設定する

操作部の[メニュー]キーを押し、[▼]または[▲]キーを使用して操作してください。

1. 操作部からネットワーク管理者がログインします。
2. [セキュリティ管理]から[ネットワークセキュリティレベル]を選択します。

## ネットワークセキュリティを強化する

[セキュリティ管理] ▶ [OK] ▶ [ネットワークセキュリティレベル] ▶ [OK]

確認メッセージが表示されたときは、[確認] を押します。

3. ネットワークのセキュリティレベルを選択します。

レベル 0、レベル 1、レベル 2、FIPS140 のどれかを選択 ▶ [OK]

4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

## Web Image Monitor から設定する

1. Web Image Monitor からネットワーク管理者がログインします。
2. [ネットワークセキュリティ] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティ」 ▶ [ネットワークセキュリティ]

3. 「セキュリティレベル」で設定するレベルを選択します。
4. [OK] をクリックします。
5. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
6. ログアウトします。

## 各機能とネットワークセキュリティレベルの関係

○=使用できます。

- =使用できません。

▲=使用できます。ポートが開いています。

■=使用できません。ポートが閉じています。

TCP/IP\*1



ネットワークセキュリティを強化する

機能	レベル0	レベル1	FIPS 140	レベル2
TCP/IP*2	○	○	○	○
HTTP > ポート 80	▲	▲	▲	▲
IPP > ポート 80	▲	▲	▲	▲
IPP > ポート 631	▲	▲	■	■
SSL/TLS > ポート 443	▲	▲	▲	▲
SSL/TLS > SSL/TLS 通信許可設定	暗号文優先	暗号文優先	暗号文のみ	暗号文のみ
SSL/TLS バージョン > TLS1.2	○	○	○	○
SSL/TLS バージョン > TLS1.1	○	○	○	○
SSL/TLS バージョン > TLS1.0	○	○	○	○
SSL/TLS バージョン > SSL3.0	○	○	-	-
暗号強度設定 > AES	128ビット /256ビット	128ビット /256ビット	128ビット /256ビット	128ビット /256ビット
暗号強度設定 > 3DES	168ビット	168ビット	168ビット	-
暗号強度設定 > RC4	-	-	-	-
DIPRINT	○	○	-	-
LPR	○	○	-	-
FTP	○	○	○	○
sftp	○	○	○	○
ssh	○	○	○	○
RSH/RCP	○	○	-	-
TELNET	○	-	-	-

## ネットワークセキュリティを強化する

機能	レベル 0	レベル 1	FIPS 140	レベル 2
Bonjour	○	○	-	-
SSDP	○	○	-	-
SMB	○	○	-	-
NetBIOS over TCP/IPv4	○	○	-	-
WSD (Device)	○	○	○	○
WSD (Printer)	○	○	○	○
WSD (機器の暗号化通信)	-	-	○	○
RHPP	○	○	-	-

\*1 IPv4、IPv6 共通です。

\*2 セキュリティレベルとは連動していません。個別に有効/無効を設定してください。

## SNMP

機能	レベル 0	レベル 1	FIPS 140	レベル 2
SNMP	○	○	○	○
SNMPv1, v2 による設定許可	○	-	-	-
SNMPv1, v2 機能	○	○	-	-
SNMPv3 機能	○	○	○	○
SNMPv3 通信許可設定	暗号文/平文	暗号文/平文	暗号文のみ	暗号文のみ

## TCP/IP 暗号強度設定

ネットワークセキュリティを強化する

機能	レベル 0	レベル 1	FIPS 140	レベル 2
ssh > 暗号化アルゴリズム	DES/3DES/AES-128/AES-192/AES-256/Blowfish/Arcfour	3DES/AES-128/AES-192/AES-256/Arcfour	3DES/AES-128/AES-192/AES-256	3DES/AES-128/AES-192/AES-256
SNMPv3 > 認証アルゴリズム	MD5	SHA1	SHA1	SHA1
SNMPv3 > 暗号化アルゴリズム	DES	DES	AES128	AES128
Kerberos 認証 > 暗号化アルゴリズム	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC/DES-CBC-MD5	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1/RC4-HMAC	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96/DES3-CBC-SHA1	AES256-CTS-HMAC-SHA1-96/AES128-CTS-HMAC-SHA1-96
ドライバー暗号鍵 > 暗号強度設定	簡易暗号	DES	AES	AES

## 機器証明書による通信経路の保護

本機では SSL/TLS、IPsec、または IEEE 802.1X などを使用して、通信経路の保護と暗号化通信を確立できます。

これらを使用するには、事前に本機に機器証明書を作成、導入します。

機器証明書には、次の 2 つがあります。

- 機器自身で作成する自己証明書
- 認証局に申請して発行された認証局証明書

### ★重要

- 管理者の方は、証明書の期限を管理し、期限が切れる前に証明書の更新をしてください。
- 管理者の方は、証明書の発行元が適切であることを確認してください。
- 機器証明書の署名アルゴリズムに SHA256、SHA512 を設定したときは、Internet Explorer 6.0 で接続するには、Windows XP SP3 以降が必要です。

## Web Image Monitor から機器証明書を作成、導入する（自己証明書）

Web Image Monitor で機器証明書を作成、導入します。

機器証明書に、自己証明書を利用するときの説明です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 機器証明書を作成します。

作成する証明書番号を選択 ▶ [作成] ▶ 必要な設定項目を入力

SSL/TLS に使用するときには [証明書 1] を選択します。その他で使用するときには任意の証明書番号を選択します。

本機から機器証明書を削除するときは、[削除] をクリックします。

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。

4. [OK] をクリックします。  
設定が書き換えられます。
5. [OK] をクリックします。

## ネットワークセキュリティーを強化する

6. セキュリティーの警告ダイアログが表示されたときは、内容を確認して [はい] をクリックします。

「証明書状態」に「導入済み」が表示され、本機に機器証明書が導入されます。

7. ログアウトします。

## 機器証明書を作成、申請する（認証局証明書）

Web Image Monitor で機器証明書を作成し、認証局に申請します。

機器証明書に、認証局証明書を利用するときの説明です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 機器証明書を作成します。

作成する証明書番号を選択 ▶ [要求] ▶ 必要な設定項目を入力

SSL/TLS に使用するときには [証明書 1] を選択します。その他で使用するときは任意の証明書番号を選択します。


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。

4. [OK] をクリックします。
5. [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。

6. ログアウトします。
7. 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「証明書詳細情報」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すると、証明書の発行先が表示されないことがあります。導入するとき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 で機器証明書を作成できますが、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ときは、[取りやめ要求] をクリックします。

## ネットワークセキュリティーを強化する

### 機器証明書を導入する（認証局証明書）

Web Image Monitor で、認証局から発行された機器証明書の内容を導入します。  
機器証明書に、認証局証明書を利用するときの説明です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 機器証明書を導入します。

導入する証明書番号を選択 ▶ [導入] ▶ 機器証明書の内容を入力

SSL/TLS に使用するときには [証明書 1] を選択します。その他で使用するときは任意の証明書番号を選択します。

証明書の入力ボックスに認証局から発行された機器証明書の内容を入力します。

中間証明書も併せて導入するときは、中間証明書の内容も入力してください。

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。

4. [OK] をクリックします。
5. 1~2分待ってから、[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。
6. ログアウトします。

### 中間証明書を導入する（認証局証明書）

Web Image Monitor で、認証局から発行された中間証明書の内容を導入します。

認証局から発行された中間証明書がないと、ネットワーク通信時に警告画面がでます。

認証局から中間証明書が発行されているときは、中間証明書を導入しておくことをお勧めします。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 中間証明書を導入します。

導入する証明書番号を選択 ▶ [中間証明書導入] ▶ 中間証明書の内容を入力

証明書の入力ボックスに認証局から発行された中間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。

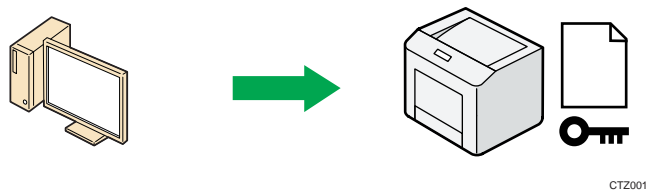
4. [OK] をクリックします。
5. 1~2分待ってから、[OK] をクリックします。  
本機に中間証明書が導入されます。中間証明書が導入されたかについては、「証明書詳細情報」から確認できます。「証明書詳細情報」は、Web Image Monitor のヘルプを参照してください。
6. ログアウトします。

## SSL/TLS を設定する

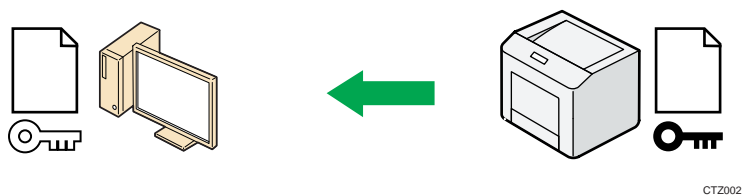
SSL/TLS を設定すると、暗号化通信ができます。これにより、通信途中でのデータの盗聴、内容の解析、改ざんを防止できます。

### SSL/TLS による暗号化通信の流れ

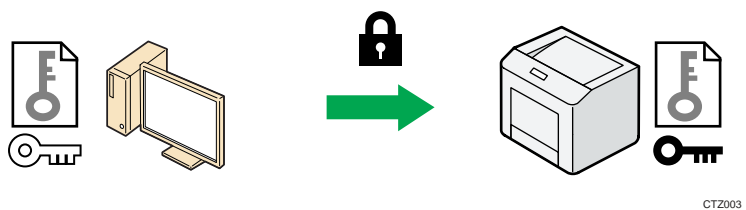
1. ユーザーのパソコンから本機へアクセスするとき、SSL/TLS の機器証明書と公開鍵を要求します。



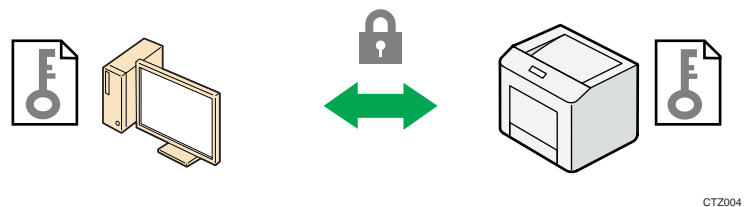
2. 本機からユーザーのパソコンへ機器証明書と公開鍵が送られます。



3. パソコンで生成した共通鍵は、公開鍵によって暗号化されて本機に送られ、本機の秘密鍵で復号されます。



4. 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。



### 自己証明書利用時の設定の流れ

1. 機器証明書の作成と導入  
操作部または、Web Image Monitor で機器証明書を作成、導入します。
2. SSL/TLS を有効にする



## ネットワークセキュリティーを強化する

---

Web Image Monitor で、SSL/TLS の設定を有効にします。

### 認証局証明書利用時の設定の流れ

1. 機器証明書の作成と認証局への申請

Web Image Monitor で機器証明書を作成したのち認証局に申請します。申請の内容は認証局によって異なるため認証局の要求する方法にしたがって手続きします。

2. 機器証明書を導入する

Web Image Monitor で、認証局から発行された機器証明書を導入します。

3. SSL/TLS を有効にする

Web Image Monitor で、SSL/TLS の設定をします。

↓ 補足

- SSL/TLS 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) /」と入力し本機にアクセスしてください。「ページを表示できません」と表示されたときは、SSL/TLS の設定が無効です。設定の内容を確認してください。
- SSL/TLS (暗号化通信) の設定を有効にした状態で IPP を使用してプリンター機能を運用すると、経路を暗号化し、通信途中でのデータの盗聴、内容の解析、改ざんを防止できます。

---

## SSL/TLS を有効にする

---

機器証明書を導入後、SSL/TLS 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とき、または認証局証明書を利用するときのどちらにも共通の設定方法です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [SSL/TLS] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [SSL/TLS]

3. 「SSL/TLS」を設定します。

IPv4、IPv6 のうち使用するものを [有効] に設定します。

4. 「SSL/TLS 通信許可設定」を設定します。

暗号化の通信モードを選択します。

5. 「SSL/TLS バージョン」を設定します。

TLS1.2、TLS1.1、TLS1.0、SSL3.0 のどれかを無効にするときは、[無効] を選択します。

少なくとも 1 つは有効にしておきます。

## ネットワークセキュリティーを強化する

---

### 6. 「暗号強度設定」を設定します。

AES、3DES、RC4 それぞれで使用する暗号強度をチェックします。少なくとも1項目のチェックが必要です。

TLS1.2、TLS1.1、TLS1.0、SSL3.0の[有効][無効]の選択によりチェックできる項目が異なります。

### 7. [OK] をクリックします。

### 8. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。

[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの[更新] ボタンをクリックします。

### 9. ログアウトします。

#### ↓ 補足

- 「SSL/TLS 通信許可設定」が [暗号文のみ] になっているときに、Web ブラウザーの対応していないプロトコルまたは暗号化強度だけを選択すると、通信できなくなります。そのときは、操作部から [SSL/TLS 通信許可設定] を [暗号文/平文] に設定すると通信ができるので、適切なプロトコルと暗号化強度に設定し直してください。
- SSL/TLS バージョンと暗号強度設定は、[ネットワークセキュリティー] でも変更できます。
- TLS1.2、TLS1.1、TLS1.0、SSL3.0の有効または無効の設定により、LDAP サーバーに接続できないことがあります。
- TLS1.2 と TLS1.1 だけを有効にしたときは、統合サーバー認証ができません。

---

## SSL/TLS のユーザー設定

---

本機に自己証明書あるいはプライベート CA 局による機器証明書を導入し、SSL/TLS の設定を有効にしているときは、ユーザーのパソコンに証明書をインストールすることをお勧めします。特に Windows Vista/7/8/8.1、Windows Server 2008/2008 R2/2012/2012 R2 で IPP-SSL を利用して本機で印刷するときは、証明書のインストールが必要です。証明書のインストールについては、ネットワーク管理者から、各ユーザーにお伝えください。

IPP で本機にアクセスするときの証明書ストアの場所は、「信頼されたルート証明機関」を選択してください。

#### ↓ 補足

- 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。
- Windows Vista/7/8/8.1、Windows Server 2008/2008 R2/2012/2012 R2 で OS 標準の IPP ポートを使っているときに、機器証明書の [共通名称] のホスト名や IP ア

## ネットワークセキュリティを強化する

ドレスを変更する場合は、先にパソコンの本機を削除し、[共通名称] の変更後に本機を再インストールしてください。またユーザー認証の設定（ログインユーザー名とログインパスワード）を変更するときも、本機を削除してユーザー認証の設定を変更後、本機を再インストールしてください。

## SSL/TLS 暗号化通信モードを設定する

SSL/TLS の暗号化通信モードを設定し、セキュリティの強度を変更できます。

暗号化通信モード	説明
暗号文のみ	暗号化通信だけを許可します。 暗号化できないときは、通信できません。
暗号文優先	暗号化できるときは、暗号化通信します。 暗号化できないときは、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。

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。

1. 操作部からネットワーク管理者がログインします。
2. [SSL/TLS 通信許可設定] を選択します。

[インターフェース設定] ▶ [OK] ▶ [ネットワーク設定] ▶ [OK] ▶ [SSL/TLS 通信許可設定] ▶ [OK]

3. 暗号化通信モードを選択します。

[暗号文のみ]、[暗号文優先]、[暗号文/平文] のどれかを選択 ▶ [OK]

確認メッセージが表示されたときは、[確認] を押します。

4. ログアウトします。

↓ 補足

- Web Image Monitor から SSL/TLS の暗号化通信モードを設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

## ネットワークセキュリティーを強化する

---

### SMTP 通信の SSL を設定する

---

1. Web Image Monitor からネットワーク管理者がログインします。
2. [メール] を選択します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [メール]

3. 「SSL」を設定します。

「SMTP」 ▶ 「SSL」 ▶ [利用する] ▶ [OK]

SMTP 通信で SSL を設定しないときは、[利用しない] をクリックします。

4. [OK] をクリックします。
5. ログアウトします。

## IPsec を設定する

---

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します。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、自動鍵交換設定方式を搭載しています。自動鍵交換設定を使用すると、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、誤った鍵設定をすると、Web Image Monitor にアクセスできなくなります。アクセス不能となることを防止するために HTTPS 通信を IPsec の除外対象に設定できます。HTTPS 通信も IPsec の対象とするときは、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、パソコン側で TCP が IPsec の対象になっていると 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、操作部の初期設定で IPsec を無効にしてからアクセスしてください。操作部による IPsec 有効/無効設定の切り替え方法は、『使用説明書』「システム初期設定」、「インターフェース設定」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 は次のとおりです。
  - Windows Server 2003/2003 R2\*1
  - Windows Vista/7/8/8.1
  - Windows Server 2008/2008 R2/2012/2012 R2
- 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 の設定をするときは、必ず OS 側の IPsec 設定内容を確認し、同一の設定をしてください。

---

## 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 プロトコルと認証だけ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、ヘッダ以外のパケットの認証の両方に対応したセキュリティー通信

## ネットワークセキュリティーを強化する

---

をします。

- 暗号化するには送信側、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します。自動鍵交換設定では、暗号化アルゴリズムと暗号鍵は自動的に設定されます。
- 認証をするには送信側、受信側ともに同一の認証アルゴリズムと認証鍵を設定します。自動鍵交換設定では、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

ヘッダーを含むパケットの認証だけに対応したセキュリティー通信をします。

- 認証をするには送信側、受信側ともに同一の認証アルゴリズムと認証鍵を設定します。自動鍵交換設定では、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 + ESP プロトコル

データの暗号化と、ヘッダーを含むパケットの認証の両方に対応したセキュリティー通信をします。

- 暗号化をするには送信側、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します。自動鍵交換設定では、暗号化アルゴリズムと暗号鍵は自動的に設定されます。
- 認証をするには送信側、受信側ともに同一の認証アルゴリズムと認証鍵を設定します。自動鍵交換設定では、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

- 使用している 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。

---

## 自動鍵交換設定

---

本機は鍵の設定方式として、自動鍵交換設定に対応しています。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 通信ができません。

自動鍵交換設定方式では、SA が自動的に設定されますが、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するために、設定の有効期間を定めることで SA の定期的な自動更新ができます。本機の自動鍵交換設定方式は IKEv1 だけ対応しています。SA の設定は、複数設定できます。

### 個別設定とデフォルト設定

自動鍵交換設定は、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できます。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 IP アドレス範囲を指定し、優先度の高い個別設定でその範囲内の特定の通

## ネットワークセキュリティーを強化する

信者を指定した設定ができます。

## IPsec 設定項目

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

### IPsec の設定項目

設定項目	設定内容	設定値
IPsec*1	IPsec 機能を有効にするか無効にするか設定します。	<ul style="list-style-type: none"><li>有効</li><li>無効</li></ul>
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。	<ul style="list-style-type: none"><li>有効</li><li>無効</li></ul> HTTPS 通信を IPsec の対象から外すときは有効を選択します。

\*1 「IPsec」の設定は操作部からもできます。

### 自動鍵交換設定のセキュリティーレベル

自動鍵交換設定では、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次のとおりです。

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しないで、通信相手の認証とデータの改ざん防止だけをするときに選択します。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ので、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、パケットデータを暗号化するときに選択します。「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です。

## ネットワークセキュリティを強化する

セキュリティレベル	セキュリティレベルの特徴
認証と暗号化（高）	通信相手の認証と改ざん防止に加え、パケットデータを暗号化をするときに選択します。「認証と暗号化（低）」よりもセキュリティ強度の高い設定です。

各セキュリティレベル選択時の自動設定値は次のとおりです。

設定項目	各セキュリティ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）
セキュリティポリシー	apply	apply	apply
カプセル化モード	トランスポート	トランスポート	トランスポート
IPsec 要求レベル	可能な場合使用する	可能な場合使用する	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	SHA256
フェーズ1 暗号化アルゴリズム	DES	3DES	AES-128-CBC
フェーズ1 Diffie-Hellman グループ	2	2	2
フェーズ2 セキュリティプロトコル	AH	ESP	ESP



ネットワークセキュリティを強化する

設定項目	各セキュリティ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-SHA512-256／ HMAC-SHA384-192／ HMAC-SHA256-128／ HMAC-SHA1-96	HMAC-SHA512-256／ HMAC-SHA384-192／ HMAC-SHA256-128／ HMAC-SHA1-96	HMAC-SHA512-256／ HMAC-SHA384-192／ HMAC-SHA256-128
フェーズ 2 暗号化アルゴリズム 使用許可	平文（NULL 暗号）	3DES／AES-128／ AES-192／AES-256	AES-128／AES-192 ／AES-256
フェーズ 2 PFS	無効	無効	2

自動鍵交換設定の設定項目

セキュリティレベルを選択すると、セキュリティ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、リモートアドレスは手動での入力が必要です。また自動設定された内容を手動で変更すると、セキュリティレベルの表示は自動的に「ユーザー設定」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。	<ul style="list-style-type: none"> <li>・ 無効</li> <li>・ IPv4</li> <li>・ IPv6</li> <li>・ IPv4/IPv6（デフォルト設定のみ）</li> </ul>
ローカルアドレス	本機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は、範囲の指定もできます。	<ul style="list-style-type: none"> <li>・ 本機のIPv4アドレス、またはIPv6アドレス範囲で指定しないときは、IPv4はアドレスのあとに32を入力し、IPv6はアドレスのあとに128を入力します。</li> </ul>

ネットワークセキュリティを強化する

設定項目	設定内容	設定値
リモートアドレス	IPsec の通信対象となる相手先のアドレスを指定します。範囲の指定もできます。	<ul style="list-style-type: none"> <li>・ 通信相手の IPv4 アドレス、または IPv6 アドレス範囲で指定しないときは、IPv4 はアドレスのあとに 32 を入力し、IPv6 はアドレスのあとに 128 を入力します。</li> </ul>
セキュリティポリシー	IPsec の処理方法を設定します。	<ul style="list-style-type: none"> <li>・ IPsec を適用して送受信する (Apply)</li> <li>・ IPsec を適用しないで送受信する (Bypass)</li> <li>・ パケットを破棄する (Discard)</li> </ul>
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)	<ul style="list-style-type: none"> <li>・ トランスポート</li> <li>・ 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)</li> </ul> <p>セキュリティ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。</p> <p>トンネルエンドポイントの始点 IP アドレスにはローカルアドレスと同じ値を設定します。</p>

ネットワークセキュリティを強化する

設定項目	設定内容	設定値
IPsec 要求レベル	通信相手と IPsec だけで通信するか、IPsec が確立できないときは平文で通信するかを選択します。 (自動設定対象項目)	<ul style="list-style-type: none"> <li>・ 可能な場合使用する</li> <li>・ 必須</li> </ul>
認証方法	通信相手の認証をする方式を選択します。 (自動設定対象項目)	<ul style="list-style-type: none"> <li>・ PSK</li> <li>・ 証明書</li> </ul> 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」を使用するときは、PSK の文字列を設定します。「証明書」を選択するときは、事前に機器証明書を導入して、IPsec 用の証明書を割り当てておきます。
PSK 文字列	自動鍵交換で使用する PSK 文字列を設定します。	認証方式が PSK のときに、アスキー文字列で 32 文字以内の文字列を入力します。
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)	<ul style="list-style-type: none"> <li>・ MD5</li> <li>・ SHA1</li> <li>・ SHA256</li> <li>・ SHA384</li> <li>・ SHA512</li> </ul>
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)	<ul style="list-style-type: none"> <li>・ DES</li> <li>・ 3DES</li> <li>・ AES-128-CBC</li> <li>・ AES-192-CBC</li> <li>・ AES-256-CBC</li> </ul>

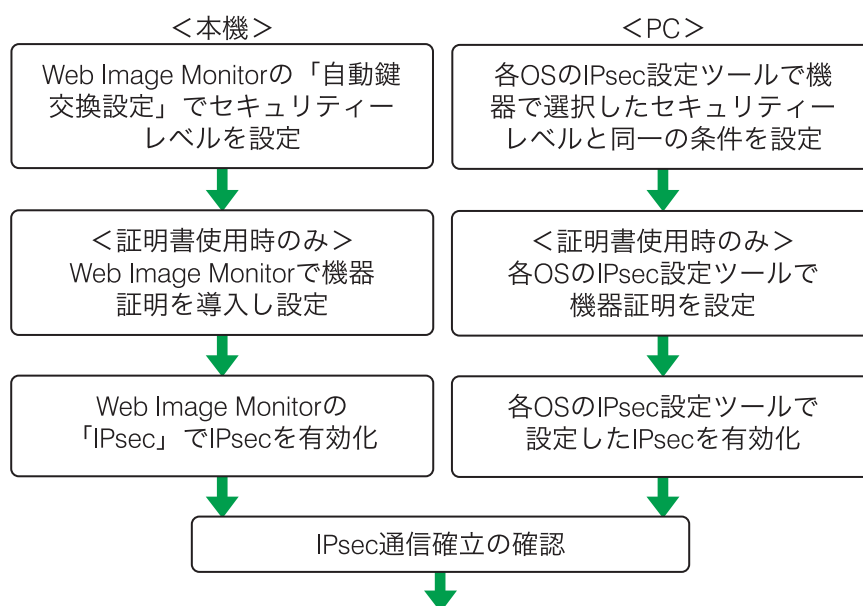
ネットワークセキュリティを強化する

設定項目	設定内容	設定値
フェーズ1 Diffie-Hellman グループ	IKE の暗号鍵生成に使用する Diffie-Hellman グループ番号を選択します。 (自動設定対象項目)	<ul style="list-style-type: none"> <li>・ 1</li> <li>・ 2</li> <li>・ 14</li> </ul>
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。
フェーズ2 セキュリティプロトコル	フェーズ2 で使用するセキュリティプロトコルを選択します。 暗号化と認証を同時にするときは ESP もしくは AH +ESP を、認証だけをするときは AH を選択します。 (自動設定対象項目)	<ul style="list-style-type: none"> <li>・ ESP</li> <li>・ AH</li> <li>・ ESP+AH</li> </ul>
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)	<ul style="list-style-type: none"> <li>・ HMAC-MD5-96</li> <li>・ HMAC-SHA1-96</li> <li>・ HMAC-SHA256-128</li> <li>・ HMAC-SHA384-192</li> <li>・ HMAC-SHA512-256</li> </ul>
フェーズ2 暗号化アルゴリズム使用許可	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)	<ul style="list-style-type: none"> <li>・ 平文 (NULL 暗号)</li> <li>・ DES</li> <li>・ 3DES</li> <li>・ AES-128</li> <li>・ AES-192</li> <li>・ AES-256</li> </ul>
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)	<ul style="list-style-type: none"> <li>・ 無効</li> <li>・ 1</li> <li>・ 2</li> <li>・ 14</li> </ul>

## ネットワークセキュリティを強化する

設定項目	設定内容	設定値
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。

## 自動鍵交換設定の流れ



CJC015

### ★重要

- 自動鍵交換設定で通信相手の認証方法に証明書を使用するときは、機器証明書の導入が必要です。
- IPsec の設定後、正しく通信が確立されているかどうかは Ping コマンドで確認できます。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。

## 自動鍵交換設定をする

1. Web Image Monitor からネットワーク管理者がログインします。
2. [IPsec] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティ」 ▶ [IPsec]

3. 自動鍵交換設定の条件を設定します。

[編集] ▶ 「個別設定 1」の条件を設定 ▶ [OK]

複数の個別設定条件を設定するときは、個別設定番号を切り替えて追加設定します。

4. 「IPsec」の「IPsec:」で [有効] を選択します。
5. 「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。
6. [OK] をクリックします。
7. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。

[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。

8. ログアウトします。

↓ 補足

- 自動鍵交換設定の条件設定で送信相手の認証方式を「証明書」に変更するときは、事前に証明書の導入と割り当てをしてください。証明書の作成・導入については、P. 76「機器証明書による通信経路の保護」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 に割り当てる方法は、「証明書を選択する」を参照してください。

証明書を選択する

---

あらかじめ本機で作成、導入した機器証明書から IPsec で使用する証明書を選択します。機器証明書の作成、導入については P. 76「機器証明書による通信経路の保護」を参照してください。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 「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。
4. [OK] をクリックします。
5. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。

## ネットワークセキュリティーを強化する

---

[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。

### 6. ログアウトします。

## パソコンで IPsec の条件を設定する

---

本機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パソコン側で設定します。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 7 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] - [システムとセキュリティー] - [管理ツール] をクリックします。

Windows 8 のときは、画面の右上端または、右下端をポイントし [設定] - [コントロールパネル] - [システムとセキュリティー] - [管理ツール] をクリックします。

2. [ローカルセキュリティーポリシー] をダブルクリックします。
3. [IP セキュリティポリシー（ローカルコンピューター）] 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、[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」に本機の自動鍵交換設定のフェーズ 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. 本機の自動鍵交換設定のフェーズ 1 で選択されている「暗号化」(暗号化アルゴリズム)、「整合性」(ハッシュアルゴリズム)、「Diffie-Hellman グループ」の組み合わせが [セキュリティーメソッドの優先順位] に存在しているか確認します。  
存在しないときは [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指定しない」を選択し、[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。  
本機の自動鍵交換設定の認証方法で証明書を選択しているときは、機器証明書を設定します。PSK を選択しているときは、事前共有キーとして本機で設定した PSK と同じ文字列を入力します。

17. 「IP フィルター一覧」で [追加] をクリックします。
18. 「名前」に任意の IP フィルター名を入力し、[追加] をクリックします。  
「IP フィルターウィザード」が表示されます。
19. [次へ] をクリックします。
20. 必要に応じて IP フィルターの説明を入力し、[次へ] をクリックします。
21. 「宛先アドレス」で「特定の IP アドレスまたはサブネット」を選択し、本機の IP アドレスを入力して [次へ] をクリックします。
22. 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。  
IPv6 で IPsec を使用するときには、対象プロトコルで [その他] のプロトコル番号 [58] を選択します。
23. [完了] をクリックします。
24. [OK] をクリックします。
25. 設定した IP フィルターを選択し、[次へ] をクリックします。
26. [追加] をクリックします。  
「フィルター操作ウィザード」が表示されます。
27. [次へ] をクリックします。
28. 任意のフィルター操作名を入力し、[次へ] をクリックします。
29. [セキュリティのネゴシエート] を選択し、[次へ] をクリックします。
30. [セキュリティで保護された接続が確立できないときは、保護されていない通信を許可する] を選択し、[次へ] をクリックします。
31. 「カスタム」を選択し、[設定] をクリックします。
32. 「整合性アルゴリズム」で本機の自動鍵交換設定のフェーズ 2 で選択されている認証アルゴリズムを選択します。
33. 「暗号化アルゴリズム」で本機の自動鍵交換設定のフェーズ 2 で選択されている暗号化アルゴリズムを選択します。
34. 「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、本機の自動鍵交換設定のフェーズ 2 で設定した有効期間を秒単位で入力します。
35. [OK] をクリックします。
36. [次へ] をクリックします。
37. [完了] をクリックします。
38. 作成したフィルター操作を選択し、[次へ] をクリックします。
39. 認証方法を選択して [次へ] をクリックします。  
本機の自動鍵交換設定の認証方法で証明書を選択しているときは、機器証明書を設定します。PSK を選択しているときは、事前共有キーとして本機で設定した PSK と同じ文字列を入力します。
40. [完了] をクリックします。



## ネットワークセキュリティを強化する

---

### 41. [OK] をクリックします。

新しい IP セキュリティポリシー (IPsec 設定) が設定されます。

### 42. 設定したセキュリティ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。

パソコンの IPsec 設定が有効になります。

#### ↓ 補足

- パソコンの IPsec を無効にするときは、設定したセキュリティ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。
- 自動鍵交換設定でセキュリティレベルを「認証と暗号化 (高)」に指定するときは、フィルター操作のプロパティ画面で [セッションキーの PFS (Perfect Forward Secrecy) を使う] をチェックします。Windows で PFS を使用するときは、自動鍵交換設定のフェーズ 2 で使用される PFS グループ番号は、ステップ 11 にある Diffie-Hellman グループ番号から自動的に変換されます。このため、本機の自動鍵交換設定で指定されたセキュリティレベルを変更し、「ユーザー設定」が表示される状況で IPsec を有効にするには、本機の「Diffie-Hellman グループフェーズ 1」と「PFS フェーズ 2」のグループ番号を同じにします。

## telnet で IPsec を設定する

---

本機では、telnet から IPsec 設定の確認、変更ができます。telnet にログインするときのログインユーザー名とログインパスワードについては管理者へ問い合わせてください。

#### ★ 重要

- 自動鍵交換設定 (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してください。telnet は証明書の導入に対応していません。

## ipsec

---

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

### 現在の設定の表示

```
msh> ipsec
```

- 次の IPsec 関連の設定情報がすべて表示されます。
  - IPsec 設定の設定値
  - 自動鍵交換設定の個別 IKE 設定値
  - 自動鍵交換設定のデフォルト 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。

## ネットワークセキュリティを強化する

---

### ipsec exclude

---

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を一括して設定できます。

### ipsec ike

---

自動鍵交換設定の 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。
- 設定値を省略したときは、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てから、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 のときは、アドレスのあとに「/」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 のときは、アドレスのあとに「/」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。

## ネットワークセキュリティを強化する

---

- IPv4 と IPv6 の両方のアドレスタイプを指定するときは「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 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は通常の通信をし、IPsec が利用できるときは IPsec 通信をします。
- 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} tunneladdr "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。

## ネットワークセキュリティを強化する

---

- 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きます。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|sha256|sha384|sha512}
```

- 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。
- 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|aes128|aes192|aes256}
```

- 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。
- 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

## ネットワークセキュリティを強化する

---

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|hmac-sha256|hmac-sha384|hmac-sha512}
```

- 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。

## IEEE 802.1X 認証を設定する

IEEE 802.1X 認証は、有線/無線の両方で利用できる認証機能です。認証サーバー（RADIUS サーバー）で認証をします。

EAP タイプ（認証方式）は、EAP-TLS、LEAP、EAP-TTLS、PEAP の 4 種類から選択できます。各 EAP タイプで必要な証明書は次のとおりです。

EAP タイプ	必要な証明書
EAP-TLS	サイト証明書、機器証明書（IEEE 802.1X クライアント証明書）
LEAP	-
EAP-TTLS	サイト証明書
PEAP	サイト証明書
PEAP（フェーズ 2 メソッドで TLS 選択時）	サイト証明書、機器証明書（IEEE 802.1X クライアント証明書）

### サイト証明書を導入する

認証サーバーの信頼性をチェックするための、サイト証明書（ルート CA 証明書）を導入します。サーバー証明書に署名した認証局の証明書か、その上位の認証局の証明書を入手しておきます。

証明書の入手方法は、使用している環境により異なります。

インポートできるサイト証明書の形式は、PEM（Base64 Encoded X.509）です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [サイト証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティ」 ▶ [サイト証明書]

3. 証明書をインポートします。

## ネットワークセキュリティーを強化する

「インポートするサイト証明書」 ▶ [参照] ▶ 入手した「CA 証明書」を選択 ▶ [開く] ▶ [インポート]

4. インポートした証明書の状態が「信頼できる」であることを確認します。  
「サイト証明書チェック機能」が [有効] になっていて、証明書の状態が「信頼できない」のときは、通信できなくなることがあります。
5. [OK] をクリックします。
6. ログアウトします。

## 機器証明書を選択する

あらかじめ本機で作成、導入した機器証明書から、IEEE 802.1X で使用する証明書を選択します。機器証明書の作成、導入については P. 76 「機器証明書による通信経路の保護」を参照してください。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器証明書] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [機器証明書]

3. 「利用する証明書」の「IEEE 802.1X」で、使用する証明書を選択します。
4. [OK] をクリックします。
5. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
6. ログアウトします。

## イーサネットで IEEE 802.1X を使用する

1. Web Image Monitor からネットワーク管理者がログインします。
2. [IEEE 802.1X] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [IEEE 802.1X]

3. 「ユーザー名」に、RADIUS サーバーに設定されているユーザー名を入力します。
4. 「ドメイン名」に、利用している環境のドメイン名を入力します。

5. 「EAP タイプ」を選択します。EAP タイプによって設定項目が異なります。

EAP-TLS

- 使用している環境に合わせて設定してください。
  - 「サーバー証明書の認証」を選択します。
  - 「中間認証局の信頼」を選択します。
  - 「サーバーID」に、RADIUS サーバーのホスト名を入力します。
  - 「サブドメイン許可」を選択します。

LEAP

- 「パスワード」の [変更] をクリックして、RADIUS サーバーに設定されているパスワードを入力します。

EAP-TTLS

- 「パスワード」の [変更] をクリックして、RADIUS サーバーに設定されているパスワードを入力します。
- 「フェーズ 2 ユーザー名」に、RADIUS サーバーに設定されているユーザー名を入力します。
- 「フェーズ 2 メソッド」の「EAP-TTLS」を選択します。

使用している RADIUS サーバーにより、使用できないメソッドがあります。

- 以降の項目は使用している環境に合わせて設定してください。
  - 「サーバー証明書の認証」を選択します。
  - 「中間認証局の信頼」を選択します。
  - 「サーバーID」に、RADIUS サーバーのホスト名を入力します。
  - 「サブドメイン許可」を選択します。

PEAP

- 「パスワード」の [変更] をクリックして、RADIUS サーバーに設定されているパスワードを入力します。
- 「フェーズ 2 メソッド」で [TLS] を選択するときは、パスワードの設定は不要です。
- 「フェーズ 2 ユーザー名」に、RADIUS サーバーに設定されているユーザー名を入力します。
- 「フェーズ 2 メソッド」の「PEAP」を選択します。
- メソッドに [TLS] を選択するときは、「IEEE 802.1X クライアント証明書」が必要です。
- 以降の項目は、使用している環境に合わせて設定してください。
  - 「サーバー証明書の認証」を選択します。
  - 「中間認証局の信頼」を選択します。
  - 「サーバーID」に、RADIUS サーバーのホスト名を入力します。



## ネットワークセキュリティを強化する

---

- 「サブドメイン許可」を選択します。
6. [OK] をクリックします。
  7. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
  8. 「インターフェース」の [インターフェース設定] をクリックします。
  9. 「イーサネット」の「セキュリティ (802.1X)」で [有効] を選択します。
  10. [OK] をクリックします。
  11. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
  12. ログアウトします。

### 補足

- 設定の不具合により、本機と通信できなくなることがあります。このようなときは、操作部から次の方法でネットワークサマリーを印刷して状況を確認できます。
  - [テスト印刷] の [ネットワークサマリー]
- 原因が特定できないときは、操作部の [インターフェース設定] の [ネットワーク] (ネットワーク設定) の [IEEE 802.1X 認証初期化] で設定を初期化してから、手順をやり直してください。

---

## パスワードを暗号化する

---

ドライバー暗号鍵、および IPP 認証のパスワード暗号化を設定すると、パスワードを暗号化通信でき、パスワード解析に対する安全性を強化できます。安全性をより強化するためには、IPsec、SNMPv3、SSL/TLS を併せて使用することをお勧めします。また管理者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

ユーザー認証を設定しているときに、各種ドライバーから送信するログインパスワードや、文書パスワードを暗号化するためのキー文字列です。

本機とユーザーのパソコンで使用するドライバーに、同じドライバー暗号鍵を設定します。

### IPP 認証のパスワード

IPP 認証のパスワードを暗号化するには、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。

## ネットワークセキュリティを強化する

### 補足

- 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。

## ドライバー暗号鍵を設定する

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、パスワード解析に対する安全性を強化できます。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部からネットワーク管理者がログインします。
2. [ドライバー暗号鍵] を選択します。

[セキュリティ管理] ▶ [OK] ▶ [セキュリティ強化] ▶ [OK] ▶ [ドライバー暗号鍵] ▶ [OK]

3. ドライバー暗号鍵を入力します。

[入力] ▶ 暗号鍵を入力 ▶ [入力終了]

4. ドライバー暗号鍵を再入力します。

[入力] ▶ 暗号鍵を再入力 ▶ [入力終了]

5. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

### 補足

- セキュリティ強化は Web Image Monitor でも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。
- 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。
-

## ネットワークセキュリティーを強化する

---

### IPP 認証のパスワードを設定する

---

本機に IPP 認証のパスワードを設定します。また、IPP 認証のパスワードを暗号化通信し、パスワード解析に対する安全性を強化できます。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [IPP 認証] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「セキュリティー」 ▶ [IPP 認証]

3. 「認証:」のドロップダウンメニューから [DIGEST] を選択します。
4. ユーザー名を「ユーザー名」ボックスに入力します。
5. パスワードを「パスワード」ボックスに入力します。
6. [OK] をクリックします。
7. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。  
[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。
8. ログアウトします。

## Kerberos 認証の暗号化設定

Kerberos 認証時の、本機と KDC サーバー間の暗号化通信を設定します。

Windows 認証、LDAP 認証、LDAP 検索などで Kerberos 認証を使用するときに、安全な通信ができます。

KDC サーバーの種類によって、サポートする暗号化アルゴリズムが異なるので、使用する環境に合わせて選択してください。

KDC サーバー	サポートする暗号化アルゴリズム
Windows Server 2003 Active Directory	<ul style="list-style-type: none"><li>RC4-HMAC (ARCFOUR-HMAC-MD5)</li><li>DES-CBC-MD5</li></ul>
Windows Server 2008	<ul style="list-style-type: none"><li>AES256-CTS-HMAC-SHA1-96</li><li>AES128-CTS-HMAC-SHA1-96</li><li>RC4-HMAC (ARCFOUR-HMAC-MD5)</li><li>DES-CBC-MD5</li></ul>
Windows Server 2008 R2/2012/2012 R2	<ul style="list-style-type: none"><li>AES256-CTS-HMAC-SHA1-96</li><li>AES128-CTS-HMAC-SHA1-96</li><li>RC4-HMAC (ARCFOUR-HMAC-MD5)</li><li>DES-CBC-MD5*</li></ul>
Heimdal	<ul style="list-style-type: none"><li>AES256-CTS-HMAC-SHA1-96</li><li>AES128-CTS-HMAC-SHA1-96</li><li>DES3-CBC-SHA1</li><li>RC4-HMAC (ARCFOUR-HMAC-MD5)</li><li>DES-CBC-MD5</li></ul>

\* OS の設定で有効にすると使用できます。

1. Web Image Monitor から機器管理者がログインします。
2. [Kerberos 認証] 設定を選択します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [Kerberos 認証]

3. 有効にする暗号化アルゴリズムを選択します。

## ネットワークセキュリティを強化する

---

少なくとも1つを有効にします。

4. [OK] をクリックします。
5. ログアウトします。

## 本機を管理する

本機の安全性を高め、効果的に運用するための機能を説明します。

---

### ログを管理する

---

本機に蓄積されたログを収集すると、各機能の使用履歴、エラー履歴、本機へのアクセス状況やアクセス者の詳細情報を確認できます。

また、暗号化してログの漏洩を防止できます。

ログは Web Image Monitor、またはログ収集サーバーを使用して確認します。収集したログは GSV ファイルに変換して一括ダウンロードできます。ハードディスクから直接読み出すことはできません。

#### ログの種類

本機に蓄積されるログは、ジョブログ、アクセスログ、eco ログがあります。

- ジョブログ  
印刷などのユーザーの文書にかかわるワークフローすべてのログ情報/操作部から印刷するシステム設定リストなどのレポート印刷
- アクセスログ  
ログイン、ログアウトなどの認証/ハードディスク初期化などのサービスエンジニア操作/ログ転送結果などのシステム動作/暗号化通信、アクセス攻撃、ロックアウト、ファームウェアの正当性確認などのセキュリティー動作
- eco ログ  
電源の入り、切り/電カステータスの遷移/ジョブの実行時間やジョブとジョブの時間間隔/1 時間ごとの用紙消費量/本機の消費電力量

#### ↓ 補足

- ログ収集サーバーについては、ログ収集サーバーの使用説明書を参照してください。
- ログ収集サーバーを使用するときは、ログ収集サーバーでログの転送設定が必要です。

## Web Image Monitor からログを管理する

本機で記録するログの種類、収集レベルを設定できます。また、ログの暗号化、一括消去を実施できます。

### Web Image Monitor で管理できるログ項目

Web Image Monitor でログを収集する機能を有効にすると、本機にログが蓄積されます。収集できるログは次のとおりです。Web Image Monitor の [設定] の [ログ] で設定できます。詳しくは Web Image Monitor のヘルプを参照してください。収集したログは、Web Image Monitor を使用してダウンロードできます。

使用している機種によって、収集できるログ項目は異なります。

#### ジョブログ

設定項目	Log Type の属性値	収集するログ
プリンター：印刷	Printer: Printing	通常のプリンター印刷のログ
プリンター：機密印刷（印刷未完）	Printer: Locked Print (Incomplete)	機密印刷で本機に文書を一時蓄積したときのログ
プリンター：機密印刷	Printer: Locked Print	本機に一時蓄積された機密印刷文書を操作部、または Web Image Monitor から印刷したときのログ
プリンター：試し印刷（印刷未完）	Printer: Sample Print (Incomplete)	試し印刷で本機に文書を一時蓄積したときのログ
プリンター：試し印刷	Printer: Sample Print	本機に一時蓄積された試し印刷文書を操作部、または Web Image Monitor から印刷したときのログ
プリンター：保留印刷（印刷未完）	Printer: Hold Print (Incomplete)	保留印刷で本機に文書を一時蓄積したときのログ

## 本機を管理する

設定項目	Log Type の属性値	収集するログ
プリンター：保留印刷	Printer: Hold Print	本機に一時蓄積された保留印刷文書を操作部、または Web Image Monitor から印刷したときのログ
プリンター：保存	Printer: Stored Print	保存印刷で本機に文書を蓄積したときのログ
プリンター：保存して印刷	Printer: Store and Normal Print	保存印刷で本機に文書を蓄積しながら印刷をしたときのログ プリンタードライバーの設定で印刷方法を [保存して印刷] に選択したとき
プリンター：保存文書印刷	Printer: Stored File Printing	本機に蓄積された保存文書を操作部、または Web Image Monitor から印刷したときのログ
レポート印刷	Report Printing	操作部からレポートを印刷したときのログ
プリンター：保留印刷文書印刷	Printer: Hold Print File Printing	本機に一時蓄積された保留印刷文書を操作部、または Web Image Monitor から時刻を指定して印刷したときのログ

## アクセスログ

設定項目	Log Type の属性値	収集するログ
ログイン*1	Login	ログインしたときのログ
ログアウト	Logout	ログアウトしたときのログ
文書蓄積	File Storing	本機に文書を蓄積したときのログ
蓄積文書印刷	Stored File Deletion	本機に蓄積した文書を削除したときのログ
蓄積文書一括削除	All Stored Files Deletion	本機に蓄積した文書を一括削除したときのログ



本機を管理する

設定項目	Log Type の属性値	収集するログ
ログ一括削除	All Logs Deletion	ログを一括削除したときのログ
ログ設定変更	Log Setting Change	ログの設定を変更したときのログ
ログ転送結果	Transfer Log Result	ログ転送結果のログ
ログ収集項目変更	Log Collection Item Change	ジョブログ収集レベル、アクセスログ収集レベル、収集する項目を変更したときのログ
暗号化通信ログ収集	Collect Encrypted Communication Logs	ユーティリティー、Web Image Monitor、または外部機器との間で暗号化通信をするときのログ
アクセス攻撃 <sup>*3</sup>	Access Violation	不正な高頻度のログイン要求を検知したときのログ
ロックアウト操作	Lockout	ロックアウト機能が働いたときのログ
ファームウェア: アップデート	Firmware: Update	ファームウェアをアップデートしたときのログ
ファームウェア: 構成変更	Firmware: Structure Change	SD カードの抜き差し、および異なった SD カード挿入など、構成変更を検知したときのログ
ファームウェア: 構成	Firmware: Structure	本機の電源投入時など、ファームウェアのモジュール構成を確認したときのログ
機器データ暗号鍵変更	Machine Data Encryption Key Change	機器データ暗号化設定の暗号鍵を変更したときのログ
ファームウェア: 正当性エラー	Firmware: Invalid	本機の電源投入時など、ファームウェアの正当性を確認したときのログ
日付・時刻設定変更	Date/Time Change	日付、時刻を変更したときのログ

本機を管理する

設定項目	Log Type の属性値	収集するログ
文書アクセス権変更	File Access Privilege Change	保存文書のアクセス権を変更したときのログ
パスワード変更	Password Change	ログインパスワードを変更したときのログ
管理者変更	Administrator Change	管理者を変更したときのログ
アドレス帳変更	Address Book Change	アドレス帳が変更されたときのログ
機器設定	Machine Configuration	本機の設定値を変更したときのログ
アドレス帳情報バックアップ	Back Up Address Book	アドレス帳の情報をバックアップしたときのログ
アドレス帳リストア	Restore Address Book	アドレス帳の情報をリストアしたときのログ
拡張印刷利用量制限:トラッキング許可結果	Enhanced Print Volume Use Limitation: Tracking Permission Result	アプリケーションによるトラッキングを保存したときのログ
ユーザ別カウンタークリア結果	Counter Clear Result: Selected User(s)	ユーザー別のカウンターをクリアしたときのログ
全ユーザカウンタークリア結果	Counter Clear Result: All Users	全ユーザーのカウンターをクリアしたときのログ
機器設定情報のインポート	Import Device Setting Information	本機の設定情報ファイルをインポートしたときのログ

## 本機を管理する

設定項目	Log Type の属性値	収集するログ
機器設定情報のエクスポート	Export Device Setting Information	本機の設定情報ファイルをエクスポートしたときのログ

\*1 SNMPv3 の「ログイン」のログは記録されません。

\*2 ハードディスクのフォーマット時は、それまでのログが消去され、フォーマットされたというログが記録されます。

\*3 頻繁なりモートログインによるユーザ認証 DoS 攻撃をアクセス攻撃と呼びます。

## eco ログ

設定項目	Log Type の属性値	収集するログ
主電源 ON	Main Power On	電源を入れたときのログ
主電源 OFF	Main Power Off	電源を切ったときのログ
電源ステータス移行結果	Power Status Transition Result	電源ステータス移行結果のログ
ジョブ関連情報	Job Related Information	ジョブ関連情報のログ
用紙使用量	Paper Usage	用紙使用量のログ
消費電力量	Power Consumption	消費電力量のログ

### 補足

- ジョブログ収集レベルを [レベル 1] に設定すると、すべてのジョブログが収集されます。
- アクセスログ収集レベルを [レベル 1] に設定すると、次の項目のログが収集されます。
  - ログ一括削除
  - ログ設定変更
  - ログ収集項目変更
- アクセスログ収集レベルを [レベル 2] に設定すると、すべてのアクセスログが収集されます。

## 本機を管理する

- 「ファームウェア:構成」のログは本機の電源投入後、最初に記録されるログです。
- eco ログ収集レベルを [レベル 1] に設定すると、eco ログは収集されません。
- eco ログ収集レベルを [レベル 2] に設定すると、すべての項目の eco ログが収集されます。

## ダウンロードできるログ情報の属性一覧

Web Image Monitor を使ってログをダウンロードすると、それぞれのログに、次の詳細情報が記録された Comma Separated Values (CSV) 形式のファイルが出力されます。タイトル名は、CSV ファイルに表示される文字列です。

ログに該当する詳細情報がないときは、その欄は空白で出力されます。

### ファイルの出力形式

- 文字コードセット : UTF-8
- 出力形式 : CSV (カンマ区切り) 形式
- ジョブログ、アクセスログのファイル名 : “機器名+\_log.csv”
- eco ログのファイル名 : “機器名+\_ecolog.csv”

### ログの並びかた

ログは「Log ID」で昇順して出力されます。

### ファイルの構成

ファイルの 1 行目 (ヘッダー行) に各データのタイトルが出力されます。

### ログのデータ形式

- ジョブログのとき

全体 (一般情報)、ソース (ジョブの入力情報)、ターゲット (ジョブの出力情報) の順に複数行が出力されます。それらは共通のログ ID を持ちます。

全体 (一般情報)				ソース			ターゲット			
Start Date/Time	...	Result	...	Access Result	Source	...	Print File Name	Target	...	Stored File Name
2011-03-03T15:43:03.0	...	Completed	...			...			...	
	...	Completed	...		Report	...			...	
	...	Completed	...			...	Print		...	

CJIC001

- 全体  
表中の共通項目が 1 行で出力されます。
- ソース  
表中の共通項目の「Result」、「Status」、およびジョブログの入力情報を出力します。複数のソースがあるときは、複数行が出力されます。
- ターゲット  
表中の共通項目の「Result」、「Status」、およびジョブログの出力情報が出力されます。複数のターゲットがあるときは、複数行が出力されます。
- アクセスログのとき

## 本機を管理する

---

表中の共通項目、およびアクセスログ情報が1行で出力されます。

- eco ログのとき

表中の共通項目、および eco ログ情報が1行で出力されます。

## 共通項目

---

### Start Date/Time

ジョブログでは、ジョブの開始日時が記録されます。

ジョブが終了していないときは、空欄になります。

アクセスログでは、End Date/Time と同じ日時が記録されます。

CSV ファイルの1番目の項目に記録されます。

### End Date/Time

ジョブログでは、ジョブの終了日時が記録されます。

ジョブが終了していないときは、空欄になります。

アクセスログでは、事象の発生日時が記録されます。Result 発生時刻に対応します。

CSV ファイルの2番目の項目に記録されます。

### Log Type

ログの種類が記録されます。アクセスログでは、「Access Log Type」でログが種類分けされます。

ログの種類は、P. 136「収集するログを設定する」を参照してください。

CSV ファイルの3番目の項目に記録されます。

### Result

操作、または事象の結果が記録されます。

ジョブログの「プリンター：保存文書印刷」は、その事象が成功したときだけログを記録します。

値	説明
Succeeded	操作または事象が正常終了した。
Failed	操作または事象が異常終了した。
<空欄>	操作または事象が進行中である。

- ジョブログでは、すると「」、異常終了すると、「Failed」と記録されます。終了していないジョブは、空欄になります。
- アクセスログでは、事象が成功のときは「Succeeded」、失敗のときは「Failed」と記録されます。

### Operation Method

操作の手段が記録されます。

値	説明
Control Panel	操作部
Driver	ドライバー
Utility	ユーティリティー
Web	Web
Email	Eメール

### Status

操作、または事象の状態が記録されます。

値	説明
Completed	正常終了
Failed	異常終了
Processing	進行中
Error	エラー発生
Suspended	中断
Succeeded	成功
Password Mismatch	パスワード不一致
User Not Programmed	ユーザー未登録
Other Failures	その他の失敗
User Locked Out	ユーザーロックアウト中
File Limit Exceeded	リクエストフルによるキャプチャー失敗
Transfer Cancelled	キャプチャー転送のキャンセルによる失敗

## 本機を管理する

値	説明
Power Failure	電源断によるキャプチャー失敗
Lost File	文書喪失によるキャプチャー失敗
Functional Problem	デバイス不良によるキャプチャー失敗
Communication Failure	通信失敗
Communication Result Unknown	通信結果判定不能

### Cancelled: Details

ログの状態が異常終了 (Failed) したときに記録されます。  
異常終了しなかったときは、何も記録されません。

値	説明
Cancelled by User	ユーザーによるキャンセル
Input Failure	入力中の異常終了
Output Failure	出力中の異常終了
Other Error	ジョブの実行前に検知したエラー、もしくはその他のエラー
Power Failure	電源断

### Cancelled: Details (Source が Stored File のとき)

ログの状態が異常終了 (Failed) したときに記録されます。  
異常終了しなかったときは、何も記録されません。

値	説明
Memory Full	データを処理するためのメモリー領域がいっぱいになった

## 本機を管理する

値	説明
Print Data Error	本機に搭載されていないPDL、もしくはポートを利用した
Data Transfer Interrupted	次のときに記録されます。 <ul style="list-style-type: none"><li>異なる機種ドライバーを利用した</li><li>ネットワーク障害が発生した</li></ul>
Other Error	その他のエラー

### Cancelled: Details (SourceがPrinterのとき)

ログの状態が異常終了 (Failed) したときに記録されます。  
異常終了しなかったときは、何も記録されません。

値	説明
Over Job Limit	受付できるジョブ数を超えた
Memory Full	データを処理するためのメモリー領域がいっぱいになった
Authentication Failed (Access Restricted)	本機の認証に失敗した
Data Transfer Interrupted	次のときに記録されます。 <ul style="list-style-type: none"><li>異なる機種ドライバーを利用した</li><li>ネットワーク障害が発生した</li></ul>
Print Data Error	本機に搭載されていないPDL、もしくはポートを利用した
Other Error	その他のエラー

### Cancelled: Details (SourceがReportのとき)

本機がシステムの異常を検知したときは、「Other Error」と記録されます。

### Cancelled: Details (TargetがStoreのとき)

ログの状態が異常終了 (Failed) したときに記録されます。  
異常終了しなかったときは、何も記録されません。



値	説明
Exceeded Print Volume Use Limitation	ログインしたユーザーの利用量制限枚数を越えた
Timeout	タイムアウトが発生した
No Privilege	文書や機能の利用権限がなかった
Unavailable Size to Store	指定の用紙サイズ（不定形も含む）が蓄積できないサイズだった
Other Error	その他のエラー

### User Entry ID

エントリーIDが記録されます。

ジョブログ、アクセスログの操作要求をしたユーザーを一意に指すIDです。16進数で出力されます。

値	説明
0x00000000	システム操作、未認証利用者の操作
0x00000001~0xfffffeff	ユーザーやユーザーコード
0xffffffff80	システム操作
0xffffffff81	システム操作、未認証利用者の操作
0xffffffff86	スーパーバイザー
0xffffffff87	管理者
0xffffffff88	管理者 1
0xffffffff89	管理者 2
0xffffffff8a	管理者 3
0xffffffff8b	管理者 4

## 本機を管理する

---

### User Code/User Name

ユーザーの操作では、ユーザーコードまたはユーザー名が記録されます。

管理者では、管理者のログインユーザー名が記録されます。

### Log ID

ログに ID が記録されます。

ログを一意に指す ID で、16 進数で出力されます。

## アクセスログに記録される情報

---

### Access Log Type

アクセスログの種類が記録されます。

値	説明
Authentication	ユーザー認証
System	システム
Stored File	文書
Network Attack Detection/Encrypted Communication	ネットワーク攻撃/暗号化通信
Firmware	ファームウェアの正当性確認
Address Book	アドレス帳
Device Settings	初期設定の設定を変更

### Authentication Server Name

最後に認証を試みたサーバー名が記録されます。

### No. of Authentication Server Switches

認証サーバーがダウンしたときにサーバーを切り替えた回数が記録されます。

サーバーダウンを検出したかどうかを判断できます。

サーバー切り替え回数は、0~4 回です。

0 のとき、サーバーダウンしていません。

### Logout Mode

ログアウト方法が記録されます。

## 本機を管理する

値	説明
by User's Operation	ユーザーのログアウト操作
by Auto Logout Timer	時間経過による自動ログアウト

## Login Method

認証要求を受けた経路が記録されます。

値	説明
Control Panel	操作部からの操作
via Network	ネットワークを介した操作
Others	その他からの要求

## Login User Type

ログインユーザーの種別が記録されます。

値	説明
User	認証ユーザー
Guest	ゲスト
User Administrator	ユーザー管理者
File Administrator	文書管理者
Machine Administrator	機器管理者
Network Administrator	ネットワーク管理者
Supervisor	スーパーバイザー
Customer Engineer (Service Mode)	カスタマーエンジニア
Others	上記以外のユーザーのログイン

#### Target User Entry ID

対象者にエントリーIDが記録されます。

次の操作で対象となったユーザーを一意に指す ID で、16 進数で出力されます。

- ロックアウト操作
- パスワード変更

#### Target User Code/User Name

対象者のユーザーコードまたはユーザー名が記録されます。

管理者のときは、管理者のログインユーザー名が記録されます。

#### Address Book Registration No.

操作したユーザーの登録番号が記録されます。

#### Address Book Operation Mode

アドレス帳の変更をどのように実施したか記録されます。

#### Address Book Change Item

アドレス帳のどの内容を変更したか記録されます。

#### Address Book Change Request IP Address

アドレス帳を操作したユーザーの IP アドレス情報 (IPV4/IPV6) が記録されます。

#### Lockout/Release

ロックアウト状態が記録されます。

値	説明
Lockout	パスワードがロックされた
Release	ロックが解除された

#### Lockout Release Method

ロックアウトを解除した方法が記録されます。

値	説明
Manual	手動によるロックアウト解除
Auto	解除タイマーによるロックアウト解除
Not Set	プリンターは lockout が未設定です。

#### Lockout Release Target Administrator

## 本機を管理する

---

ロックアウト解除のとき、対象となる管理者が記録されます。

### Counter to Clear

ユーザーごとにどのカウンターをクリアしたかが記録されます。

### Export Target

機器情報のエクスポートの対象となる設定情報が記録されます。

値	説明
System Settings	システム初期設定
Printer Features	プリンター初期設定
Web Image Monitor Setting	Web Image Monitor 設定
Web Service Settings	Web サービス設定
System SP	システム SP
Printer SP	プリンター SP

### Target File Name

機器情報のインポート・エクスポート対象となるファイル名が記録されます。

### Stored File ID

作成または削除された文書に ID が記録されます。

作成、または削除要求された文書を一意に指す ID で、10 進数で出力されます。

### Stored File Name

作成または削除された文書のファイル名が記録されます。

### Collect Job Logs

ジョブログ収集の設定を変更したかが記録されます。

値	説明
Active	有効に変更した
Inactive	無効に変更した
Not Changed	変更していない

### Collect Access Logs

## 本機を管理する

---

アクセスログ収集の設定を変更したかどうか記録されます。

値	説明
Active	有効に変更した
Inactive	無効に変更した
Not Changed	変更していない

## Collect Eco-friendly Logs

eco ログ収集の設定を変更したかどうか記録されます。

値	説明
Active	有効に変更した
Inactive	無効に変更した
Not Changed	変更していない

## Transfer Logs

ログ転送機能の設定を変更したかどうか記録されます。

値	説明
Active	有効に変更した
Inactive	無効に変更した
Not Changed	変更していない

## Encrypt Logs

ログ暗号化機能の設定を変更したかどうか記録されます。

値	説明
Active	有効に変更した

## 本機を管理する

値	説明
Inactive	無効に変更した
Not Changed	変更していない

## Log Type

ログ収集状態の変更で対象となるログタイプの種別が記録されます。

値	説明
Job Log	ジョブログ
Access Log	アクセスログ
Eco-friendly Log	eco ログ
Level 1	レベル 1
Level 2	レベル 2
User Settings	ユーザー設定

## Log Collect Level

ログレベル設定値が記録されます。

レベル 1 のときは「Level 1」、レベル 2 のときは「Level 2」、ユーザー設定のときは「User Settings」と記録されます。

## Encryption/Cleartext

暗号化通信か、非暗号化通信かの状態が記録されます。

値	説明
Encryption Communication	暗号化通信
Cleartext Communication	平文通信

## Machine Port No.

本機のポート番号が記録されます。

## Protocol

## 本機を管理する

---

通信先のプロトコルが記録されます。

TCP のときは「TCP」、UDP のときは「UDP」、プロトコルが特定できないときは「Unknown」と記録されます。

### IP Address

通信先の IP アドレスが記録されます。

### Port No.

通信先のポート番号が記録されます。

10 進数で出力されます。

### MAC Address

通信先の物理アドレスが記録されます。

### Primary Communication Protocol

第一階層の通信プロトコル名が記録されます。

### Secondary Communication Protocol

第二階層の通信プロトコル名が記録されます。

### Encryption Protocol

暗号化プロトコル名が記録されます。

### Communication Direction

通信方向が記録されます。

値	説明
Communication Start Request Receiver (In)	通信開始要求を受ける側 (IN)
Communication Start Request Sender (Out)	通信開始要求を出す側 (OUT)

### Communication Start Log ID

通信開始時のログ ID が記録されます。

通信開始時のログを一意に指す ID で、16 進数で出力されます。

### Communication Start/End

通信開始／終了を判断するための識別子が記録されます。

### Network Attack Status

攻撃検出の状態が記録されます。



## 本機を管理する

値	説明
Violation Detected	ネットワーク攻撃を検知した
Recovered from Violation	ネットワーク攻撃収束を検知した
Max. Host Capacity Reached	ホスト数上限に到達して管理不能になった
Recovered from Max. Host Capacity	ホスト管理不能から復帰した

### Network Attack Type

攻撃の種別が記録されます。

パスワード攻撃のときは「Password Entry Violation」、アクセス攻撃のときは「Device Access Violation」と記録されます。

### Network Attack Type Details

攻撃種別の詳細が記録されます。

認証エラーのときは「Authentication Error」、暗号エラーのときは「Encryption Error」と記録されます。

### Network Attack Route

攻撃経路が記録されます。

操作部からの攻撃を受けたときは「Attack from Control Panel」、操作部以外からの攻撃を受けたときは「Attack from Other than Control Panel」と記録されます。

### Login User Name used for Network Attack

ネットワーク攻撃に使用されたログインユーザー名が記録されます。

### Add/Update/Delete Firmware

ファームウェア変更の方式が記録されます。

値	説明
Updated with SD Card	SDカードによる更新
Added with SD Card	SDカードによる追加
Deleted with SD Card	SDカードによる削除
Moved to Another SD Card	別のSDカードへの移動

## 本機を管理する

値	説明
Updated via Remote	リモートによる更新
Updated for Other Reasons	その他の理由による更新

### Module Name

ファームウェアのモジュール名が記録されます。

### Parts Number

ファームウェアの部番が記録されます。

### Version

ファームウェアのバージョンが記録されます。

### Machine Data Encryption Key Operation

暗号鍵の操作の種別が記録されます。

値	説明
Back Up Machine Data Encryption Key	暗号鍵をバックアップした
Restore Machine Data Encryption Key	暗号鍵をリストアした
Clear NVRAM	NVRAM をクリアした
Start Updating Machine Data Encryption Key	暗号鍵更新を開始した
Finish Updating Machine Data Encryption Key	暗号鍵更新を終了した

### Machine Data Encryption Key Type

暗号鍵の種別が記録されます。

HDD 暗号鍵のときは「Encryption Key for Hard Disk」、NVRAM 暗号鍵のときは「Encryption Key for NVRAM」、機器証明書の場合は「Device Certificate」と記録されます。

### Validity Error File Name

正当性検証エラーが発生したときのエラーを検出したファイル名が記録されます。

### Configuration Category

## 本機を管理する

---

設定変更をしたカテゴリーが記録されます。

詳しくは、P. 134「カテゴリー／属性一覧」を参照してください。

### Configuration Name

カテゴリーの属性が記録されます。

詳しくは、P. 134「カテゴリー／属性一覧」を参照してください。

### Configuration Value

属性の値が記録されます。

詳しくは、P. 134「カテゴリー／属性一覧」を参照してください。

### Destination Server Name

ログタイプが「Enhanced Print Volume Use Limitation: Tracking Permission Result」のときは、トラッキングの情報送信に失敗した送信先のサーバー名が記録されます。

ログタイプがプリファレンス情報のインポートかエクスポートのときは、インポートの要求元、エクスポートの要求元のサーバー名が記録されます。

### HDD Format Partition

ハードディスクの初期時のパーティションごとの状態が記録されます。

### Access Result

ログが発生した操作の結果が記録されます。

正常に終了したときは「Completed」、異常終了したときは「Failed」と記録されます。

## ジョブログに記録される情報：入力情報

---

### Source

ジョブログの入力情報が記録されます。

値	説明
Stored File	文書蓄積
Printer	プリンタードライバーからの印刷指示
Report	レポート印刷

### Start Date/Time

入力情報が「Printer」のとき、入力情報の開始日時が記録されます。

### End Date/Time

入力情報が「Printer」のとき、入力情報の終了日時が記録されます。

### Stored File ID

入力情報が「Stored File」のとき、IDが記録されます。

## 本機を管理する

---

文書を一意に指す ID で、10 進数で出力されます。

### Stored File Name

入力情報が「Stored File」のとき、文書名が記録されます。

### Print File Name

入力情報が「Printer」のとき、印刷する文書のファイル名が記録されます。

## ジョブログに記録される情報：出力情報

---

### Target

ジョブログの出力情報が記録されます。

文書が印刷されると「Print」、蓄積されると「Store」と記録されます。

### Start Date/Time

文書の印刷、蓄積の開始日時が送信されます。

### End Date/Time

文書の印刷、蓄積の終了日時が送信されます。

### Stored File ID

出力情報が「Store」のとき、ID が付加されます。

文書を一意に指す ID で、10 進数で出力されます。

### Stored File Name

出力情報が「Store」のとき、蓄積される文書のファイル名が記録されます。

## eco ログに記載される情報

---

### Start Date/Time

イベントの開始日時が記録されます。

### End Date/Time

イベントの終了日時が記録されます。

### Log Type

eco ログのログの種類が記録されます。

Power ON、Power OFF、Status of Power、Job Information、Consumption of paper のいずれかが記録されます。

### Log Result

イベントが終了しているかどうかを表します。

正常に終了したときは、「Completed」、正常に終了しなかったときは、「Failed」と記録されます。

### Result

イベントの結果が記録されます。

成功したときは、「Succeeded」、失敗したときは「Failed」と記録されます。

## 本機を管理する

---

### Log ID

ログを特定する ID が記録されます。16 進の ID です。

### Power Mode

本機の電源状態（移行後）がログとして記録されます。

値	説明
Standby	待機状態
Low Power	低電力状態
Silent	静音状態
HDD On	HDD オン状態
Engine Off	エンジン停止の状態
Controller Off	コントローラー停止の状態
STR	STR (Suspend To RAM) 状態
Silent Print	静音印刷状態
Low Power Print	低電力印刷状態
Fusing Unit Off	待機定着オフ状態

### Log Type

ジョブログのログの種類が記録されます。

#### Job Interval (seconds)

前回のジョブ開始から該当ジョブ開始までの経過時間が記録されます。

#### Job Duration (seconds)

該当ジョブの開始から終了までの経過時間が記録されます。

#### Paper Usage (Large Size)

1 時間ごとの大サイズの紙の使用量が記録されます。

大サイズは、A3 または、11 × 17 インチ以上の用紙です。

#### Paper Usage (Small Size)

1 時間ごとの小サイズの紙の使用量が記録されます。

小サイズは、A3 または、11 × 17 インチ未満の用紙です。

#### Paper Usage (2 Sided: Large Size)

## 本機を管理する

---

1時間ごとの両面大サイズの紙の使用量が記録されます。  
大サイズは、A3または、11 × 17 インチ以上の用紙です。

### Paper Usage (2 Sided: Small Size)

1時間ごとの両面小サイズの紙の使用量が記録されます。  
小サイズは、A3または、11 × 17 インチ未満の用紙です。

### Detected Power

消費電力量計測時の電源状態が記録されます。

値	説明
Controller Standby	コントローラー待機状態
STR	STR (Suspend To RAM) 状態
Main Power Off	電源が切れている状態
Printing	プリンター動作中
Engine Standby	エンジン待機状態
Engine Low	エンジン低電力状態
Engine Night	エンジン静音状態
Engine Total	機器全体の状態
Fusing Unit Off	エンジン待機定着オフ状態

### Power Consumption(Wh)

各電源状態別の消費電力量が記録されます。

## カテゴリー／属性一覧

---

### User Lockout Policy

1. Lockout  
ロックアウトの有効 (Active)、無効 (Inactive) が記録されます。
2. Number of Attempts before Lockout  
ログインパスワード入力許容回数 (回) が記録されます。
3. Lockout Release Timer  
ロックアウト解除タイマーの有効 (Active)、無効 (Inactive) が記録されます。
4. Lock Out User for

ロックアウト解除までの時間が記録されます。

#### Auto Logout Timer

1. Auto Logout Timer  
オートログアウト時間設定のする (On)、しない (Off) が記録されます。
2. Auto Logout Time (seconds)  
オートログアウトが働くまでの時間が記録されます。

#### Device Certificate

1. Operation Mode  
操作の種類が記録されます。  
証明書を作成したときは「Create」と記録されます。  
証明書を削除したときは「Delete」と記録されます。  
証明書を導入したときは「Install」と記録されます。  
利用する証明書を変更したときは「Change Application to Use Certificate」と記録されます。  
中間証明書を導入したときは「Install Intermediate Certificate」と記録され  
ます。  
中間証明書を削除したときは「Delete Intermediate Certificate」と記録され  
ます。
2. Certificate No.  
操作対象の証明書の番号が記録されます。
3. Certificate No. (XXX)  
「XXX」には、次のいずれかが入ります。
  - IEEE 802.1X (WPA/WPA2)
  - IPsecアプリケーションの利用する証明書の番号が記録されます。証明書を利用しなかつたときは「Do not Use」と記録されます。

#### IPsec

1. IPsec  
IPsecの有効 (Active)、無効 (Inactive) が記録されます。
2. Encryption Key Auto Exchange: Setting 1-4: Remote Address  
リモートアドレスが記録されます。
3. Encryption Key Auto Exchange: Setting 1-4, Default): Security Level  
セキュリティーレベルが記録されます。「認証のみ」を選択したときは「Authentication Only」と記録されます。「認証と暗号化 (低)」を選択したときは「Authentication and Low Level Encryption」と記録されます。「認証と暗号化 (高)」を選択したときは「Authentication and High Level Encryption」と記録

## 本機を管理する

---

されます。「ユーザー設定」を選択したときは「User Settings」と記録されます。

4. Encryption Key Auto Exchange: Setting1-4, Default): Authentication Method  
自動鍵交換方式の認証方法が記録されます。「PSK」、または「Certificate」が記録されます。

### Compulsory Security Stamp

Compulsory Security Stamp

強制セキュリティー印字のする (On)、しない (Off) が記録されます。

### WIM Auto Logout Timer (minutes)

Web Image Monitor のオートログアウトが働くまでの時間が記録されます。

---

## 収集するログを設定する

---

ログの種類ごとに収集設定を有効にし、収集レベルを設定します。

- ジョブログ収集レベル  
レベル 1  
ユーザー設定
- アクセスログ収集レベル  
レベル 1  
レベル 2  
ユーザー設定
- eco ログ収集レベル  
レベル 1  
レベル 2  
ユーザー設定

1. Web Image Monitor から機器管理者がログインします。
2. ログ設定画面を表示します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ログ]

3. 収集するログを選択します。

「ジョブログ収集」、「アクセスログ収集」、「eco ログ収集」のうち、収集するログは [有効] を選択します。

4. 収集レベルを設定します。

「ジョブログ収集レベル」、「アクセスログ収集レベル」、「eco ログ収集レベル」で、それぞれ収集レベルを設定します。

レベルを変更すると、ログ詳細項目がレベルに応じた選択状態に変更されます。



## 本機を管理する

---

ログ詳細項目を個別に変更するときは、各項目で設定してください。収集レベルを [レベル 1] または [レベル 2] に選択しても、ログ詳細項目を個別に変更するとレベルが [ユーザー設定] に変更されます。

5. [OK] をクリックします。
6. 「設定の書き換え中」画面が表示されます。1~2分経過してから [OK] をクリックします。

[OK] をクリックしても画面が表示されないときは、しばらく待ってから Web ブラウザーの [更新] ボタンをクリックします。

7. ログアウトします。



補足

- 「アクセスログ収集レベル」はレベル値が大きいほど多くのログを収集します。

---

## ログを暗号化する

---

ログの暗号化を有効にするか無効にするかを選択します。

1. Web Image Monitor から機器管理者がログインします。
2. ログ設定画面を表示します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ログ]

3. ログの暗号化を有効にします。

「共通設定」 ▶ 「ログ暗号化」 ▶ [有効] ▶ [OK]

確認画面が表示されます。

4. [OK] をクリックします。
5. ログアウトします。



補足

- ログを暗号化するには、ジョブログ、アクセスログ、eco ログのいずれかの収集設定が有効に設定されていることが必要です。
- 本機に蓄積されたデータを暗号化すると、本設定に関係なくログは暗号化されます。

---

## ログをダウンロードする

---

本機が記録しているログを CSV ファイルに変換し、一括してダウンロードできます。

1. Web Image Monitor から機器管理者がログインします。
2. ログダウンロード画面を表示します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ログダウンロード]

3. ダウンロードするログの種類を選択します。

「ダウンロードするログ」 ▶ ログの種類を選択

セキュリティーログには、ジョブログ、アクセスログの2種類が含まれます。

4. ダウンロードします。

[ダウンロード] ▶ 保存場所を指定して保存

5. [戻る] をクリックします。

6. ログアウトします。

↓ 補足

- ログの取得範囲は、[ダウンロード] をクリックした時刻以前に終了しているオペレーションのログを対象とします。終了していないジョブはログの Result 列が空欄になります。
- ログの件数が多いとき、ダウンロードに時間がかかります。
- ログのダウンロードが実行され、ファイル書き込み開始時にエラーが発生したとき、そのエラーログはダウンロードされたファイルの最終行に記録され、ダウンロード処理は中止されます。
- ダウンロードが正常に終了したときは、ファイルの最終行に「Download completed.」と記録されます。
- ログファイルの保存方法は、使用している Web ブラウザーのヘルプを参照してください。
- ダウンロードしたファイルの文字コードは、UTF-8 です。内容の閲覧には、UTF-8 に対応したアプリケーションを使用してください。
- ログを収集するにはジョブログ、アクセスログ、eco ログの収集設定を有効にしてください。Web Image Monitor の [設定] の [ログ] で設定できます。
- ログで取得できる情報は、P. 136「収集するログを設定する」を参照してください。

---

## 本機に保持できるログ件数

---

ジョブログ、アクセスログ、および eco ログで、本機に保持できる最大件数を超過して新しい

## 本機を管理する

ログが発生すると、古いログが新しいログで上書きされます。定期的にログのダウンロードを実施しないと、ファイルに古いログが記録されないことがあります。

Web Image Monitor を使ってログを管理するとき、ログのダウンロードは、表の条件を参考に定期的に実施してください。

### 本機に保持できるログの最大件数

ログの種類	最大件数
ジョブログ	500
アクセスログ	500
eco ログ	500

### ログ発生量の目安

ログの種類	ログ発生量（件/1日あたり）
ジョブログ	100
アクセスログ	300 ジョブにともなうログイン／ログアウト（200件）と初期設定の操作や Web からのアクセスなど（100件）の合計
eco ログ	100

ダウンロードしたファイルは、機器管理者の責任で適切に管理してください。

#### 補足

- ログを [収集する] / [収集しない] の設定を変更したときは、ログを一括消去してください。
- ログをダウンロードしたあとは、ログを一括消去してください。
- ログのダウンロード中に動作したログは記録されないことがあるので、ログのダウンロード中はほかの動作をさせないでください。
- ログの一括消去は Web Image Monitor からできます。

### ログフル時の注意事項

本機は、ログが保持できる最大件数を超えると、古いログを消去して新しいログを上書きし

## 本機を管理する

まず、ログが保持できる最大件数を超えるかどうかは、ジョブログ、アクセスログ、eco ログのそれぞれで判定しています。

ジョブログとアクセスログは、1つのファイルとしてダウンロードされます。

図の「上書きが発生していないとき」は、ダウンロード後にジョブログとアクセスログが混在していることを示します。

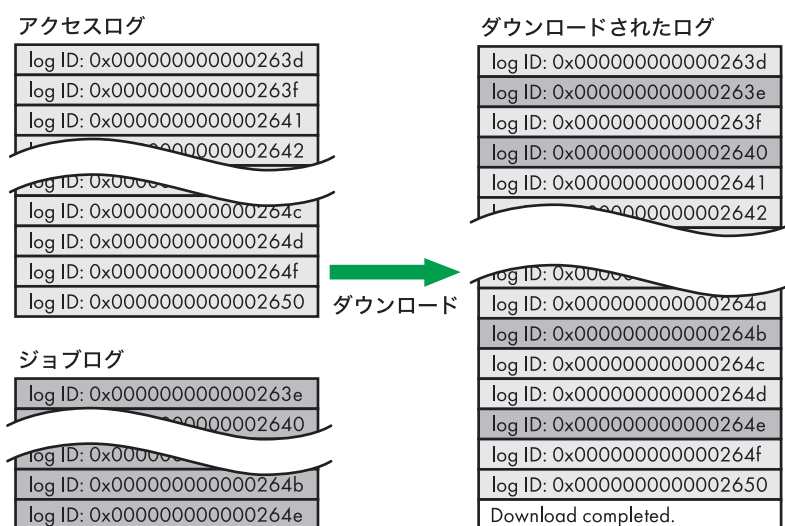
図の「上書きが発生しているとき」は、アクセスログで上書きが発生したときの例を示します。

この例では、ダウンロードされたログで、アクセスログの一部が上書きによって抜けた状態になっています。

eco ログは、単独のファイルとしてダウンロードされます。

ログが上書きされるときは、優先順位にしたがって上書きされるため、優先順位の高いログは上書きされずに残ります。

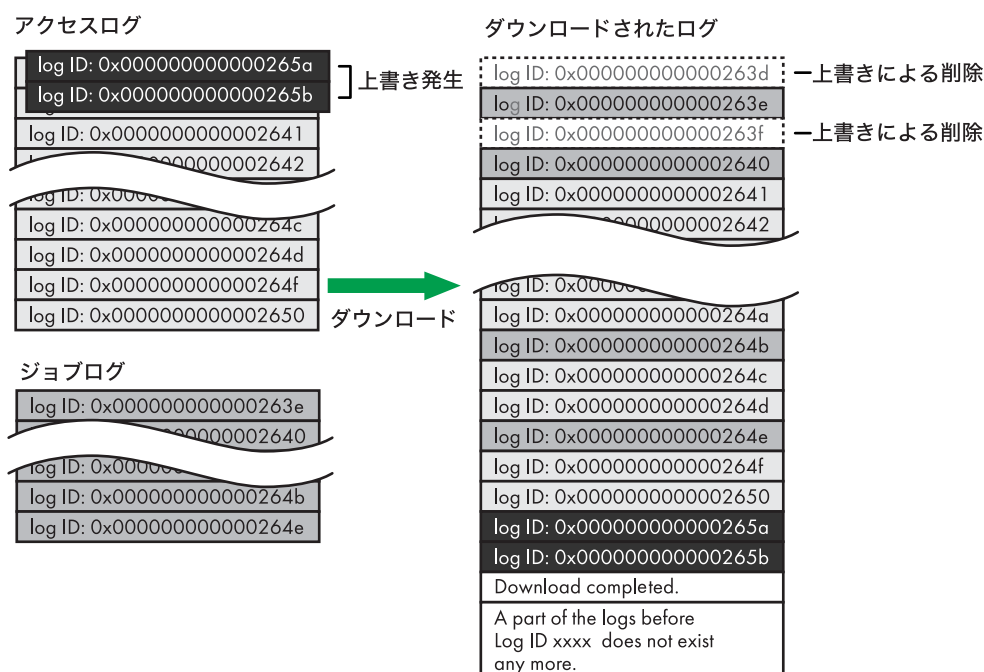
### 上書きが発生していないとき



CJC006

### 上書きが発生しているとき

## 本機を管理する



CJ0007

上書きが発生しているかどうかはダウンロードしたログの最終行に、次の文言があることで確認できます。

- 上書きが発生していないとき  
Download completed.
- 上書きが発生しているとき  
Download completed.  
A part of the logs before Log ID xxxx does not exist any more.

### 補足

- 「Log ID xxxx」以降のログを監査対象としてください。

## プリンター印刷時のログ

プリントジョブのログは、ログインのアクセスログの前にジョブログが記録されます。

プリントジョブのログは、データを受信して処理して出力するまでの一連のジョブを一つのジョブログに記録しています。

まずジョブデータを受信したときにジョブログのログ ID が採番され、それまでの情報をジョブログの一部として記録されます。

その後、認証情報を受けてログインのアクセスログが記録されます。

次にジョブデータを処理し、出力したログを先ほどのジョブログに追記します（ログ ID は同一）。

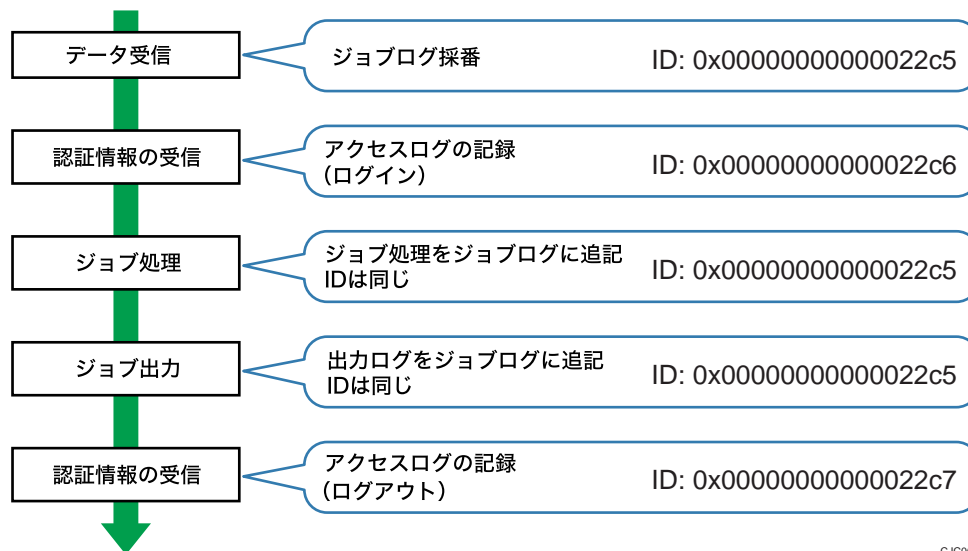
その後ログアウトのアクセスログが記録されます。

結果として、データを受信して処理して出力するまでの一連のジョブを記録した一つのジョ

## 本機を管理する

ブログを先頭に記録し、その後が続いてログイン、ログアウトのアクセスログを記録している状態になります。

### プリントジョブの流れ



## ログを一括消去する

本機に記録されたログをまとめて消去できます。

1. Web Image Monitor から機器管理者がログインします。
2. ログ設定画面を表示します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ログ]

3. ログ一括消去を実行します。

「ログ一括消去」 ▶ [削除] ▶ [OK]

4. ログアウトします。

#### 補足

- ログ設定画面読み込み時に、ジョブログ、アクセスログ、eco ログのいずれかの収集設定が [有効] でないと、「ログ一括消去」は表示されません。

## ログ収集サーバーへのログ転送を無効にする

ログ収集サーバーへのログ転送を無効にできます。

ログ転送は、ログ収集サーバーから有効に設定でき、[有効] に設定されているときだけ、

## 本機を管理する

---

[無効] の設定に変更できます。

1. Web Image Monitor から機器管理者がログインします。
2. ログ設定画面を表示します。

[機器の管理] ▶ [設定] ▶ 「機器」 ▶ [ログ]

3. ログ転送を無効にします。

「共通設定」 ▶ 「ログ転送」 ▶ [無効]

4. [OK] をクリックします。
5. ログアウトします。

## 本機からログを管理する

---

ログの収集設定、ログ収集サーバーへのログ転送設定ができます。

### 収集するログを設定する

---

ログの種類ごとに収集設定を有効にします。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. 「ログ収集」の画面を表示します。

[セキュリティ管理] ▶ [OK] ▶ [ログ収集設定] ▶ [OK]

3. 収集するログの種類を設定します。

「ジョブログ」、「アクセスログ」、「eco ログ」で、それぞれ [有効] を選択 ▶ [OK]  
▶ [確認]

4. ログアウトします。

### ログ収集サーバーへのログ転送を無効にする

---

本機のログ転送設定からログ収集サーバーへのログ転送を無効にできます。ログ転送が [する] に設定されているときだけ [しない] の設定に変更できます。

ログ収集サーバーについては、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ログ収集サーバーの使用説明書を参照してください。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. ログ転送を無効にします。

[セキュリティ管理] ▶ [OK] ▶ [ログ転送設定] ▶ [OK] ▶ [しない] ▶ [OK]



本機を管理する

---

**3. ログアウトします。**

ログ収集サーバーからログを管理する

---

ログ収集サーバーを使用したログ管理の方法は、ログ収集サーバーの使用説明書を参照してください。

## 機器情報を管理する

---

### ⚠ 注意



- SD カードは、子供の手に触れないようにしてください。もし子供が誤って SD カードを飲み込んだときは、直ちに医師の診断を受けてください。

機器管理、ユーザー管理、ネットワーク管理、文書管理のすべての権限を持つ管理者が設定します。

本機の機器情報は、設定情報ファイルとして外部機器にエクスポートできます。エクスポートした設定情報ファイルを本機にインポートすると、変更した設定を戻すことができるのでバックアップとして利用できます。

また、機器管理サーバーで設定情報ファイルを管理することで、機器の起動時や指定した日時で、定期的に設定情報ファイルをインポートできます。

#### インポート・エクスポートできるデータ

- 用紙設定
- 調整/管理
- システム設定
- 印刷設定
- セキュリティー管理
- リモートサービス
- インターフェース設定
- Web Image Monitor 設定
- Web サービス設定

#### インポート・エクスポートできないデータ

- アドレス帳
- プログラム（プリンター機能）
- telnet から設定する設定
- カウンター情報
- Web Image Monitor あるいは Web Service だけで設定できる項目（例：Bonjour、SSDP 設定）
- 本機の設定のうち次の項目
  - 年月日、時刻の設定
  - 機器証明書が必要な設定

## 本機を管理する

- 画像の補正值など機体ごとに調整する項目
- 実行するだけの項目と閲覧するだけの項目

### 補足

- エクスポートされるファイル形式は、CSV 形式です。
- 操作部からインポートする設定情報ファイルは、エクスポートしたときの設定情報ファイルと同じ機器構成である必要があります。機器構成の異なる設定情報ファイルは、インポートできません。
- 機種・モデル・仕向け地（国）が同一であり、かつ次のオプション構成が同一なときだけ、インポート/エクスポートができます。
  - 給紙トレイ
- 機器構成を変更したときは、エクスポートし、設定情報ファイルを更新してください。
- 複数の同じ機器構成の機器があるとき、設定情報ファイルをインポートすると、同じ設定にできます。
- ユーザーが本機を操作中のときは、その操作が終了するまではエクスポート・インポートできません。
- エクスポート・インポート中は、本機の操作はできません。

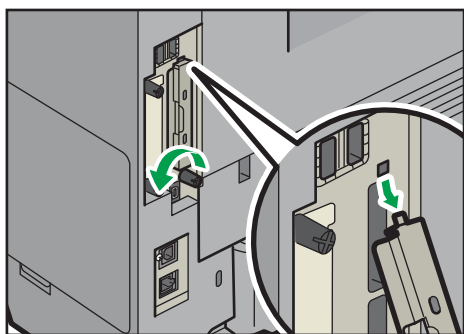
## SD カードを取り付ける

### 注意



- SD カードは、子供の手に触れないようにしてください。もし子供が誤って SD カードを飲み込んだ場合は、直ちに医師の診断を受けてください。

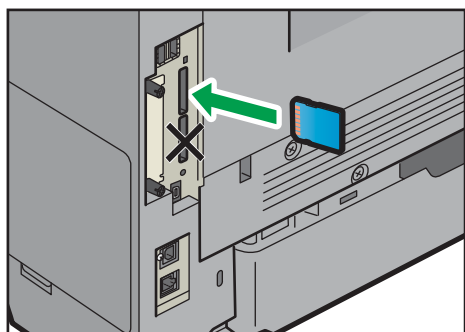
4. 同梱品を確認します。
5. 本機の電源を切り、電源プラグをコンセントから抜きます。
6. コインねじを外し、拡張 SD カード用のスロットカバーを傾けながら取り外します。



DBQ048

## 本機を管理する

7. カチッと音がするまで、拡張 SD カードをスロット 1（上段）に差し込みます。



## 機器情報をエクスポートする

操作部から機器情報をエクスポートするときは、SD カードに保存されます。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 本機に SD カードを装着します。

本機の電源を切る ▶ SD カードを本体背面の SD カードスロットに挿入 ▶ 本機の電源を入れる

2. 操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。
3. [機器設定情報：エクスポート（メディア）] を選択します。

[機器設定情報] ▶ [OK] ▶ [機器設定情報：エクスポート（メディア）] ▶ [OK]

4. 機器固有情報をエクスポートするかしないかを設定します。

[機器固有情報] ▶ [OK] ▶ [含む]、[含まない] を選択 ▶ [OK]

機器固有情報とは、IP アドレス、ホスト名などです。

5. 暗号鍵を入力します。

[暗号鍵入力] ▶ [OK] ▶ [入力する] ▶ [OK] ▶ [入力] ▶ 暗号鍵を入力  
▶ [入力終了] ▶ [入力] ▶ もう一度暗号鍵を入力 ▶ [入力終了]

6. エクスポートを実行します。

[エクスポート] ▶ [エクスポート]

7. [確認] を押します。

8. 電源を切り、SD カードを取り外します。



- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。

---

### 機器情報をインポートする

---

SD カードに保存された機器情報をインポートします。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 本機に SD カードを装着します。

本機の電源を切る ▶ SD カードを本体背面の SD カードスロットに挿入 ▶ 本機の電源を入れる

2. 操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。
3. [機器設定情報：インポート（メディア）] を選択します。

[機器設定情報] ▶ [OK] ▶ [機器設定情報：インポート（メディア）] ▶ [OK]

4. 機器設定情報ファイルを選択します。

[機器設定情報ファイルの選択] ▶ [OK] ▶ ファイルを選択 ▶ [OK]

5. 機器固有情報をインポートするかしないかを設定します。

[機器固有情報] ▶ [OK] ▶ [含む]、[含まない] を選択 ▶ [OK]

機器固有情報とは、IP アドレス、ホスト名などです。

6. エクスポート時に設定した暗号鍵を入力します。

[暗号鍵入力] ▶ [OK] ▶ [入力] ▶ 暗号鍵を入力 ▶ [入力終了]

7. インポートを実行します。

[インポート] ▶ [インポート]

8. [確認] を押します。

本機が再起動されます。

9. 電源を切り、SD カードを取り外します。



補足

- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。

---

## サーバーの機器情報を手動でインポートする

---

サーバーに格納された機器情報をインポートします。

1. Web Image Monitor からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。
2. [機器設定情報のインポート設定 (サーバー)] を選択します。

[機器の管理] ▶ [設定] ▶ [機器] ▶ [機器設定情報のインポート設定 (サーバー)]

3. 機器情報のインポート条件を設定します。

- ファイルのインポート元  
機器情報をインポートするサーバーを選択します。サーバー設定で、URL、ユーザー名、パスワードなどを設定します。
- 指定時刻での定期インポート  
機器情報をインポートする頻度を選択し、時刻を設定します。
- 前回のインポートファイルとの比較  
前回インポートした機器情報と比較し、機器情報が同じときにインポートするか、

## 本機を管理する

しないかを選択します。

- 再試行回数  
インポートに失敗したときに再試行する回数を 0~30 回の間で設定します。
- 再試行間隔  
インポートに失敗したときに再試行する間隔を 5~300 秒の間で設定します。
- メール通知  
インポートに失敗したとき、機器管理者にメールを通知するか、しないかを選択します。
- 暗号鍵  
暗号鍵を設定します。

4. [OK] をクリックします。

5. ログアウトします。

### 補足

- 機器管理サーバーを使用すると、より詳細なインポート設定ができます。詳しくは、機器管理サーバーの使用説明書を参照してください。
- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。

## こんなときには

エラーが発生したときは、最初にログの ResultCode を確認してください。0 以外の数値はエラーが発生しています。ResultCode は図の枠内に表示されています。

### ログファイルの例

```
"1.0.0"  
"ExecType", "Date", "SerialNo", "PnP", "Model", "Destinaion", "IP", "Host", "Storage", "FileNam  
e", "FileID", "TotalItem", "NumOfOkItem", "ResultCode", "ResultName", "Identifier"  
"IMPORT"  
"2012-07-05T15:29:16+09:00"  
"3C35-7M0014"  
"Brand Name"  
"Product Name"  
"0"  
"10"  
"10.250.155.125"  
"RNP00267332582D"  
"SD"  
"201207051519563C35-710220.csv"  
"201207051519563C35-710220"  
" 0"  
" 2"  
"..... REQUEST"  
"TargetID", "ModuleID", "PrefID", "Item", "NqCode", "NqName"
```

CJD021

内容を確認して解決しないとき、もしくは対処方法がわからないときは、エラーログを保存してサービス実施店にお問い合わせください。

ResultCode	原因	対処方法
2 (INVALID REQUEST)	異なるモデル、もしくは異なるオプション構成のモデルのファイルでインポートを実行しました。	同一モデルでエクスポートしたファイルをインポートしてください。
4 (INVALID OUTPUT DIR)	出力先に機器情報を書き込むことができません。	出力先が正常に動作しているか確認してください。
7 (MODULE ERROR)	インポート・エクスポート処理時に予期せぬエラーが発生しました。	電源を再投入して再度、実行してください。それでも同じエラーが発生するときは、サービス実施店に問い合わせてください。
8 (DISK FULL)	外部メディアの保存領域が不足しています。	十分な空き容量を確保してから実行してください。
9 (DEVICE ERROR)	ログファイルの書き込み、読み込みに失敗しました。	保存先・格納先のパスが存在するかどうか確認してください。
10 (LOG ERROR)	ログファイルの書き込みに失敗しました。	サービス実施店に問い合わせてください。



本機を管理する

ResultCode	原因	対処方法
20 (PART FAILED)	一部の設定項目の設定値をインポートできませんでした。	失敗した理由が NgName に記録されます。内容を確認してください。 <b>失敗理由 (NgName)</b> 2 INVALID VALUE 設定値が項目の許容範囲外 3 PERMISSION ERROR 項目の編集権限がない 4 NOT EXIST 項目がシステムに存在しない 5 INTERLOCK ERROR システムの状態または、ほかの設定値との連動により項目の変更ができない 6 OTHER ERROR その他の理由により、項目の変更ができない
21 (INVALID FILE)	メディアに保存されているデータが正しくないため、データがインポートできません。	適切なデータが使用されているか確認してください。データのフォーマットは GSV 形式です。
22 (INVALID KEY)	暗号鍵が不正です。	正しい暗号鍵を使用してください。

---

## アドレス帳を管理する

---

### アドレス帳の自動消去を設定する

---

アドレス帳の登録件数が上限のときに、自動登録の要求があった場合の動作を設定します。

[する]を選択すると、古いユーザーを自動で消去して新しいユーザーを追加します。自動で消去されるのは、前回のユーザー認証からもっとも時間が経っているユーザーです。

[しない]にすると、古いユーザーが消去されないで、新しいユーザーも追加されません。

1. Web Image Monitor からユーザー管理者がログインします。
2. アドレス帳の自動消去を有効にします。

[機器の管理] ▶ [アドレス帳] ▶ [メンテナンス] ▶ 「自動消去」 ▶ [する]  
▶ [OK]

3. ログアウトします。

↓ 補足

- 自動で消去されるのは、自動登録の要求があったときだけです。
- ユーザーコード、もしくはログインユーザー名とログインパスワードが入っているものが自動消去の対象です。
- 手動でユーザーを追加するときは、先にユーザーを消去してください。

---

## セキュリティー強化機能を設定する

---

ユーザー認証や、管理者による本機の利用制限だけではなく、本機が通信する情報やアドレス帳などのデータを暗号化し、セキュリティーを強化できます。

セキュリティー強化はWeb Image Monitor でも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から操作権限を持つ管理者がログインします。
2. [セキュリティー強化] を選択します。

[セキュリティー管理] ▶ [OK] ▶ [セキュリティー強化] ▶ [OK]

3. 設定を変更する項目を選択します。

設定を変更する項目を選択 ▶ [OK]

4. 設定を変更します。

設定を変更 ▶ [OK]

5. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

↓ 補足

- 設定項目によって、操作権限を持つ管理者が異なります。

---

## セキュリティ強化機能の設定項目

---

### ドライバー暗号鍵

ネットワーク管理者が設定します。

ユーザー認証を設定しているときに、各ドライバーから送信されたログインパスワードや文書パスワードを復号するためのキー文字列を設定します。ドライバー暗号鍵を設定するときは本機で設定した暗号鍵をドライバーに入力してください。

設定方法は、P. 106「ドライバー暗号鍵を設定する」を参照してください。

### ドライバー暗号鍵：暗号強度設定

ネットワーク管理者が設定します。

ドライバーから本機へジョブを送信するときの暗号強度を設定します。

本機がジョブに付加されているパスワードの暗号強度を確認し、ジョブを処理します。

[簡易暗号] に設定したときは、ユーザー認証に対応しているすべてのジョブを受け付けます。

[DES] に設定したときは、DES、もしくはAESで暗号化されたジョブを受け付けます。

[AES] に設定したときは、AESで暗号化されたジョブを受け付けます。

[AES] または [DES] に設定したときは、プリンタードライバーで暗号化を設定します。プリンタードライバーの設定については、プリンタードライバーのヘルプを参照してください。

- AES

## 本機を管理する

---

- DES
- 簡易暗号

工場出荷時の設定：簡易暗号

### 個人情報表示制限

機器管理者が設定します。

ユーザー認証を設定しているときに設定できます。個人認証ができない接続方法でジョブ履歴を確認するとき、個人情報をすべて「\*\*\*\*\*」表示できます。登録者の情報がわからないため、不特定のユーザーに登録した文書の情報が漏れることを防止できます。

- する
- しない

工場出荷時の設定：しない

### アドレス帳暗号化

ユーザー管理者が設定します。

本機のアドレス帳情報を暗号化します。

内部の部品が流出したときでも、暗号化によりアドレス帳の情報を読み取ることはできません。

設定方法は、P. 49「アドレス帳の登録情報を保護する」を参照してください。

- する（暗号鍵の入力）
- しない

工場出荷時の設定：しない

### 文書保護強化

文書管理者が設定します。

パスワード設定によって、文書の印刷、消去、配信などの操作が制限され、不特定の人による文書アクセスは避けられますが、パスワードが破られることもあります。

文書保護強化を設定したとき、誤ったパスワードを10回入力すると文書はロックされ、アクセスできなくなります。何度もパスワードを入力して、パスワードを解除しようとする不正なアクセスから文書を保護できます。

文書管理者だけ、ロックされた文書のロックを解除できます。

文書がロックされるとそれ以降は正しいパスワードを入力しても照合は失敗します。

- する
- しない

工場出荷時の設定：しない

### 実行中ジョブへの認証の実施

機器管理者が設定します。

本機のジョブキャンセルなどの操作に認証を必要とするか、不要とするか設定できます。

[ログイン権限]に設定すると認証の許可があるユーザー、および機器管理者が操作で

## 本機を管理する

---

きます。[ログイン権限] の設定が有効で、すでにユーザーが本機にログイン中のときは認証の要求はされません。

[アクセス権限] に設定すると印刷をしたユーザー、および機器管理者が操作できます。

[ログイン権限] に設定し、ユーザーが本機にログインできるときでも、プリンター機能の操作権限がユーザーになければ、本機のジョブキャンセルはできません。

「ユーザー認証管理」を設定しているときだけ、「実行中ジョブへの認証」の実施の設定ができます。

- ログイン権限
- アクセス権限
- しない

工場出荷時の設定：しない

### ファームウェアアップデート

機器管理者が設定します。

ファームウェアアップデートを許可するかしないかを設定します。ファームウェアアップデートとは、カスタマーエンジニアによる本機のファームウェア更新、また、ネットワーク経由でのファームウェア更新を意味します。

[禁止する] を選択すると、ファームウェアアップデートを実行できません。

[禁止しない] を選択したとき、ファームウェアアップデートの制限は無効になり、アップデートを実行できます。

- 禁止する
- 禁止しない

工場出荷時の設定：禁止しない

### 構成変更

機器管理者が設定します。

ファームウェア構成変更を監視するかしないかを設定します。ファームウェア構成変更とは SD カードの抜き差し、または異なった機種種の SD カードの挿入を意味します。

[禁止する] を選択すると、ファームウェアの構成変更があったとき、本機は起動時に構成変更を検知して停止し、管理者のログインを要求するメッセージが表示されます。機器管理者でログインすると、更新されたファームウェアで本機が起動します。画面に変更されたファームウェアのバージョンが表示され、管理者は構成変更が正当なものか不正なものかを確認できます。不正な構成変更のときは、サービス実施店に連絡してください。

ファームウェア構成変更を [禁止する] に設定するときは、「管理者認証管理」を有効に設定しておく必要があります。

[禁止する] に設定したあとに、「管理者認証管理」を一度無効にし、再度「管理者認証管理」を有効に設定したとき、ファームウェア構成変更の設定は初期値の [禁止しない]

い] に戻ります。

[禁止しない] に設定したとき、構成変更の検知は無効です。

- 禁止する
- 禁止しない

工場出荷時の設定：禁止しない

#### パスワードポリシー

ユーザー管理者が設定します。

パスワードの複雑度と使用できる最小文字数を設定できます。複雑度と最小文字数の両方の条件をみたすパスワードだけ設定できます。

[複雑度 1] に設定したとき、英大文字、英小文字、10 進数の数字、記号（#など）から 2 種類以上を組み合わせてパスワードを設定します。

[複雑度 2] に設定したとき、英大文字、英小文字、10 進数の数字、記号（#など）から 3 種類以上を組み合わせてパスワードを設定します。

- 複雑度 1
- 複雑度 2
- 制限しない

工場出荷時の設定：制限しない、最小文字数なし

#### SNMPv1, v2 による設定

ネットワーク管理者が設定します。

SNMPv1、v2 プロトコルでアクセスしたときは、個人認証ができないため、用紙設定など機器管理者が管理する項目の設定が変更されることがあります。[禁止する] に設定すると、SNMPv1、v2 を使った設定はできません。確認だけできます。

- 禁止する
- 禁止しない

工場出荷時の設定：禁止しない

#### アクセスセキュリティー設定

機器管理者が設定します。

ネットワーク接続を使用したアプリケーションで本機にログインしようとしたとき、ユーザーの認証操作と本機内部の認証動作の回数が揃わず、そのユーザー名でのログインが禁止されることがあります。

たとえば、アプリケーションから複数部数の印刷指示をするときなどにログインできないことがあります。

「アクセスセキュリティー設定」を有効にすると、そのような誤ったロックアウトを回避できます。

- 設定する
  - 攻撃拒否時間

同一のユーザーID とパスワードによる連続アクセスを除外拒否する時間を設定します。

「0-60」分の範囲で設定します。

工場出荷時の設定：15分

- ユーザー管理対象数

「アクセスセキュリティ設定」で管理できるユーザー情報の管理件数を設定します。

「50-200」件の範囲で設定します。

工場出荷時の設定：200件

- パスワード管理対象数

「アクセスセキュリティ設定」で管理できるパスワード情報の管理件数を設定します。

「50-200」件の範囲で設定します。

工場出荷時の設定：200件

- 状態監視間隔

「ユーザー管理対象数」と「パスワード管理対象数」を監視する処理の間隔を設定します。

「1-10」秒の範囲で設定します。

工場出荷時の設定：3秒

- 設定しない

工場出荷時の設定：設定しない

### パスワード攻撃検知

機器管理者が設定します。

設定した測定時間内に許容回数を超えるパスワードの認証失敗が発生したとき、パスワード攻撃と判定します。アクセスログを残すとともに、メールで機器管理者に通知します。

許容回数を「0」に設定したときは、パスワード攻撃を検知しません。

- 許容回数

連続したパスワードの認証失敗数をパスワード攻撃として検知しない最大許容回数を設定します。

「0-100」回の範囲で設定します。

工場出荷時の設定：30回

- 測定時間

連続したパスワードの認証失敗数をカウントする間隔を設定します。

測定時間を超えると、累積されたパスワードの認証失敗回数はクリアされます。

「1-10」秒の範囲で設定します。

工場出荷時の設定：5秒

↓ 補足

- 「許容回数」や「測定時間」の設定の値により、頻繁に検出メールを受信することがあります。
- メールを受信が頻繁に発生するときは、内容を確認し、設定値を見直してください。

### アクセス攻撃検知

機器管理者が設定します。

設定した測定時間内に許容回数を超えるログイン要求が発生したとき、アクセス攻撃と判定します。アクセスログを残すとともにメールにて機器管理者に通知します。操作部、および Web Image Monitor にメッセージが表示されます。

許容回数を「0」に設定したときは、アクセス攻撃を検知しません。

また、「認証遅延処理時間」を設定すると、アクセス攻撃検出時のログイン要求への応答時間を遅らせ、アクセス攻撃によるシステムダウンを防止できます。

「認証遅延処理時間」の設定時に、「同時アクセス管理対象数」を超えるホストからアクセスがあったときは、監視不能となり監視不能検出ログが残されます。

- 許容回数  
過剰なアクセス回数をアクセス攻撃として検知しない最大許容回数を設定します。  
「0-500」回の範囲で設定します。  
工場出荷時の設定：100回
- 測定時間  
過剰なアクセス回数をカウントする間隔を設定します。  
測定時間を超えると累積されたアクセス回数はクリアされます。  
「10-30」秒の範囲で設定します。  
工場出荷時の設定：10秒
- 認証遅延処理時間  
アクセス攻撃を検出したときに、ログイン要求への応答を遅らせる時間を設定します。  
「0-9」秒の範囲で設定します。  
工場出荷時の設定：3秒
- 同時アクセス管理対象数  
アクセス攻撃を検出して応答時間を遅らせたとき、受け付ける認証要求の件数を設定します。  
「50-200」件の範囲で設定します。  
工場出荷時の設定：200件

↓ 補足

- 「許容回数」や「測定時間」の設定の値により、頻繁に検出メールを受信すること



## 本機を管理する

---

があります。

- メールの受信が頻繁に発生するときは、内容を確認し、設定値を見直してください。

---

## その他のセキュリティ機能

---

### システム状態

---

Web Image Monitor のトップ画面の [警告] エリアと [状態] エリアで本機の状態を確認できます。

---

### ファームウェアの正当性確認

---

本機の起動時にファームウェアの正当性の検証が実行されます。

検証にエラーがあったときは、操作部に検証エラーが表示されます。

また、本機の起動後、Web Image Monitor でも確認できます。Web Image Monitor 自体の検証にエラーがあったときは、Web Image Monitor は利用できませんので、操作部の表示を確認してください。

検証エラーが表示されたときは、サービス実施店に連絡してください。

## カスタマーエンジニアの操作を制限する

---

カスタマーエンジニアによるサービスモードの操作を制限できます。

サービスモードは、カスタマーエンジニアが点検や修理をするときに使用する設定です。「サービスモード移行禁止設定」を「禁止する」に設定すると、機器管理者が「サービスモード移行禁止設定」を解除しないと、カスタマーエンジニアはサービスモードを使用できません。機器管理者が確認した状態で、カスタマーエンジニアは点検や修理をします。

### サービスモード移行禁止設定を有効にする

---

操作部の [メニュー] キーを押し、[▼] または [▲] キーを使用して操作してください。

1. 操作部から機器管理者がログインします。
2. 「サービスモード移行禁止設定」を選択します。

[セキュリティ管理] ▶ [OK] ▶ [サービスモード移行禁止設定] ▶ [OK]

3. 有効にします。

[する] ▶ [OK] ▶ [禁止する]

4. ログアウトします。

[メニュー] ▶ [メニュー] ▶ ログアウト

## こんなときには

本機がうまく操作ができないときの対処方法を説明します。

---

### メッセージが表示されたとき

---

ユーザー認証を使用しているときに画面にメッセージが表示されたときの対処方法を説明します。

ここに記載されていないメッセージが表示されたときは、メッセージにしたがって対処してください。

この機能を利用する権限がありません。

機能を使用する権限が設定されていません。

各機能を使用しようとして表示されたとき

- アドレス帳の認証情報で、機能を使用できるように設定されていません。
- 管理者が使用権限の追加を検討してください。

初期設定をしようとして表示されたとき

- 設定しようとした初期設定によって、管理者が異なります。」を参照してください。
- 設定項目一覧表を元に、該当する管理者が使用権限の追加を検討してください。詳しくは、P. 177 「[メニュー]キー項目の操作権限一覧」を参照してください。

認証に失敗しました。

エラーコード番号によって原因が異なります。

P. 166 「エラーコードが表示されたとき」を参照してください。

ユーザー管理者認証が無効のため設定できません。

管理者認証管理でユーザー管理者の権限が設定されていません。

ベーシック認証、Windows 認証、LDAP 認証を設定するときは、事前に管理者認証管理でユーザー管理者の権限を設定してください。

詳しくは、P. 9 「管理者認証を設定する」を参照してください。

URL の取得に失敗しました。

サーバーに到達できないか、通信が確立できません。

本機に設定されているサーバーの IP アドレス、ホスト名などの設定値を確認してください。

UA サーバー（統合サーバー）のホスト名の設定を確認してください。

URL の取得に失敗しました。

サーバーと接続されているが、ユーザー認証サービスが適切な返答を返していません。

ユーザー認証サービスが正しく設定されているか確認してください。

URL の取得に失敗しました。

こんなときには

---

サーバーで SSL が正しく設定されていません。

認証管理ツールを使用して、SSL を正しく設定してください。

URL の取得に失敗しました。

サーバー認証に失敗しています。

本機のサーバー認証の設定が正しいか確認してください。

選択された文書にアクセス権のない文書が含まれていました。アクセス権のある文書だけ消去されます。

削除する権限のない文書を削除しようとしてしました。

文書作成者（オーナー）、または文書管理者が削除できます。削除する権限のない文書を削除するときは、文書作成者（オーナー）に確認してください。

補足

- サービスコールのメッセージが表示されたときは、サービス実施店に連絡してください。

---

## エラーコードが表示されたとき

---

認証機能設定時にエラーメッセージが表示されたとき、システムログにエラーコードが記録されます。エラーコードごとに異なる対処方法を説明します。一覧にないエラーコードが記録されたときは、エラーコードを控えて、サービス実施店に連絡してください。システムログは Web Image Monitor の [設定] の「ネットワーク」で確認できます。

---

### ベーシック認証時のエラーコード

---

#### B0104-000

パスワード復号処理に失敗しました。

- パスワードに誤りがあります。パスワードが正しく入力されているか確認してください。
- 「ドライバー暗号鍵：暗号強度設定」で、[DES] または [AES] が選択されています。ドライバー暗号鍵を設定すると使用できます。
- ドライバー暗号鍵に誤りがあります。ドライバー暗号鍵が正しく入力されているか確認してください。

#### B0206-002: ケース 1

ログインユーザー名かパスワードに誤りがあります。

- ログインユーザー名とパスワードを正しく入力してログインしてください。

#### B0206-002: ケース 2

アプリケーション別個人認証機能を利用している環境で、初期設定など管理者だけがアクセスを許可される機能に、ユーザーのアカウントでログインしようとしてしました。

- 管理者しかログインできない仕様です。ユーザーでログインするときは、アプリケーションのログイン画面から認証を実行してください。

#### B0206-003

ログインユーザー名にスペース、「:」、「”」が含まれているため、認証に失敗しています。

- 禁則文字入りアカウントであるときは、アカウントを作成し直してください。
- 誤って禁則文字を入力したときは、正しく入力してログインしてください。

#### B0207-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

#### B0208-000 / B0208-002

認証に失敗した回数が、設定値を超えたため、アカウントがロックされました。

- アカウントを確認し、ロックを解除してください。

こんなときには

---

## Windows 認証時のエラーコード

---

### W0104-000

パスワード復号処理に失敗しました。

- パスワードに誤りがあります。パスワードが正しく入力されているか確認してください。
- 「ドライバー暗号鍵：暗号強度設定」で、[DES] または [AES] が選択されています。ドライバー暗号鍵を設定すると使用できます。
- ドライバー暗号鍵に誤りがあります。ドライバー暗号鍵が正しく入力されているか確認してください。

### W0206-002

アプリケーション別個人認証機能を利用している環境で、初期設定など管理者だけがアクセスを許可される機能に、ユーザーのアカウントでログインしようとした。

- 管理者しかログインできない仕様です。ユーザーでログインするときは、アプリケーションのログイン画面から認証を実行してください。

### W0206-003

ログインユーザー名にスペース、「:」、「"」が含まれているため、認証に失敗しています。禁則文字入りアカウントであるときは、アカウントを作成し直してください。

- 誤って禁則文字を入力したときは、正しく入力してログインしてください。

### W0207-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

### W0208-000 / W0208-002

認証に失敗した回数が、設定値を超えたため、アカウントがロックされました。

- アカウントを確認し、ロックを解除してください。

### W0400-102

サーバーが動作していないため、Kerberos 認証に失敗しました。

- サーバーが動作しているか確認してください。

### W0400-107: ケース 1

ログインユーザー名として UserPrincipalName (user@domain.xxx.co.jp) 形式を使用しています。

- ログインユーザー名で UserPrincipalName (user@domain.xxx.co.jp) を使用しているとき、ユーザーグループ取得はできません。ユーザーグループ取得できるアカウントは、sAMAccountName (user) になっているので、sAMAccountName でログインしてください。

### W0400-107: ケース 2

ユーザーグループが取得できるように設定されていません。

- DC (ドメインコントローラ) に作成したユーザーグループのプロパティ内グループのスコープは、「グローバルグループ」かつグループの種類は「セキュリティ」としている

こんなときには

---

か確認してください。

- 作成したユーザーグループにアカウントは追加されているか確認してください。
- 本機へ登録したユーザーグループ名と DC のユーザーグループ名は「全角半角・大文字小文字」も区別し全く同一の文字列か確認してください。
- DC が複数存在しているとき、DC 間の信頼関係は設定されているか確認してください。

#### W0400-107: ケース 3

ドメイン名の名前解決ができていません。

- 「インターフェース設定」のドメイン名、DNS/WINS の設定を確認してください。

#### W0400-200

認証数が多いため、リソースを使い果たしました。

- しばらく経ってからログインしてください。

#### W0400-202

認証サーバーと本機の SSL 設定が合っていません。

- 認証サーバーと本機の SSL 設定が合っているか確認してください。

ログインユーザー名に sAMAccountName を使用してログインを実行しています。

- 親子ドメイン環境で、子ドメインユーザーがログインするとき、ログインユーザー名に sAMAccountName を使用すると、ldap\_bind に失敗します。ログインユーザー名として、UserPrincipalName でログインをしてください。

#### W0406-003

ログインユーザー名にスペース、「:」、「/」が含まれているため、認証に失敗しています。

- 禁則文字入りアカウントであるときは、アカウントを作成し直してください。
- 誤って禁則文字を入力したときは、正しく入力してログインしてください。

#### W0406-101

同時に大量の認証が発生しているためログインできません。

- しばらく経ってからログインしてください。
- 復旧しないときは、認証の攻撃を受けていないか確認してください。
- 攻撃の状態は、画面メッセージ、管理者へのメール通知、システムログにて確認できません。

#### W0406-107: ケース 1

認証サーバーと通信できていません。

- サーバーと通信できることを確認してください。
- 「インターフェース設定」の「Ping コマンド実行」で接続の確認ができます。
- ほかのパソコンからも認証できるか確認してください。

#### W0406-107: ケース 2

ログインユーザー名かパスワードに誤りがあります。

- サーバーにユーザーが登録されているか確認してください。



こんなときには

- 登録されているログインユーザー名とパスワードを使用してログインしてください。

W0406-107: ケース 3

ドメイン名に誤りがあります。

- Windows 認証のドメイン名を正しく設定しているか確認してください。

W0406-107: ケース 4

ドメイン名の名前解決ができません。

ドメイン名に IP アドレスを設定して、認証に成功するか確認してください。

<成功するとき>

2. ドメイン名に階層ドメイン名 (domainname.xxx.co.jp) を指定するとき、「インターフェース設定」の DNS を設定しているか確認してください。
3. ドメイン名に NetBIOS ドメイン名 (DOMAINNAME) を指定するとき、「インターフェース設定」の WINS を設定しているか確認してください。

<失敗するとき>

4. ドメインコントローラセキュリティポリシー、またはドメインセキュリティポリシーで LM/NTLM を拒否する設定となっていないか確認してください。
  5. 本機からドメインコントローラの接続経路のファイアウォール、またはドメインコントローラのファイアウォール設定などでポートをクローズしていないか確認してください。
- Windows Vista/7/8/8.1 で、Windows ファイアウォールを有効にしているときは、「システムとセキュリティ」コントロールパネルの「Advanced settings」でファイアウォールルールを作成し、137 番と 139 番のポートを許可します。
  - Windows XP で、Windows ファイアウォールを有効にしているときは、ネットワーク接続のプロパティを開き、[詳細設定] タブの [設定] をクリックします。[例外] タブで 137 番/139 番を例外設定としてください。
  - ネットワーク接続のプロパティを開き、TCP/IP のプロパティを開きます。[詳細設定] をクリックします。[WINS] タブの「NetBIOS over TCP/IP を有効にする」にチェックすると、137 番が OPEN します。

W0406-107: ケース 5

Kerberos 認証に失敗しています。

- Kerberos 設定が正しく設定されていません。  
レルム名、KDC (キー配布センター) 名、対応ドメイン名を正しく設定しているか確認してください。
- KDC (キー配布センター) と本機の時刻が合っていません。  
KDC (キー配布センター) と本機との間に 5 分以上の時刻差があるときは、認証に失敗します。  
時刻が合っているか確認してください。

## こんなときには

---

- レルム名を小文字で設定しているとき、Kerberos 認証に失敗します。  
レルム名が小文字になっていないか確認してください。
- KDC（キー配布センター）の自動取得に失敗するとき、Kerberos 認証に失敗します。  
KDC（キー配布センター）取得設定が自動取得になっているかサービス実施店に確認を依頼してください。  
自動取得が上手く動作しないときは、手動設定に切り替えて使用してください。

### W0409-000

認証サーバーからの応答が返らないため、認証タイムアウトが発生しました。

- ネットワーク環境、および認証に使用するサーバーを確認してください。

### W0511-000

本機にすでに登録されているユーザーと、認証サーバーの一意属性で区別される別ユーザーのログイン名が重複しています。（一意属性は LDAP 認証設定で指定）

- 重複する古いユーザーを削除するか、ログイン名を変更してください。
- 認証サーバーを切り替えたあとのときは、古いサーバー側のユーザーを削除してください。

### W0606-004

ユーザーのログインユーザー名には指定できないユーザー名を指定したため、認証に失敗しました。

- ユーザーのアカウントとして、「other」「admin」「supervisor」「HIDE\*」は使用しないでください。

### W0607-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

### W0612-005

アドレス帳の登録数が上限に達し、ユーザー自動登録に失敗したため、認証に失敗しました。

- ユーザー登録件数が最大件数に達しているため、認証に失敗しました。
- ユーザー管理者がアドレス帳内に登録された不要なユーザーを削除してください。

### W0707-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

---

## LDAP 認証時のエラーコード

---

### L0104-000

パスワード復号処理に失敗しました。

- パスワードに誤りがあります。パスワードが正しく入力されているか確認してください。
- 「ドライバー暗号鍵：暗号強度設定」で、[DES] または [AES] が選択されています。

こんなときには

---

ドライバー暗号鍵を設定すると使用できます。

- ドライバー暗号鍵に誤りがあります。ドライバー暗号鍵が正しく入力されているか確認してください。

#### L0206-002

アプリケーション別個人認証機能を利用している環境で、初期設定など管理者だけがアクセスを許可される機能に、ユーザーのアカウントでログインしようとした。

- 管理者しかログインできない仕様です。ユーザーでログインするときは、アプリケーションのログイン画面から認証を実行してください。

#### L0206-003

ログインユーザー名にスペース、「:」、「"」が含まれているため、認証に失敗しています。

- 禁則文字入りアカウントであるときは、アカウントを作成し直してください。
- 誤って禁則文字を入力したときは、正しく入力してログインしてください。

#### L0207-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

#### L0208-000 / L0208-002

認証に失敗した回数が、設定値を超えたため、アカウントがロックされました。

- アカウントを確認し、ロックを解除してください。

#### L0306-018

LDAP サーバーの設定が正しくされていません。

- LDAP サーバー設定が代表者アカウントを正しく設定し、接続テストで成功できることを確認してください。

#### L0307-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

#### L0400-210

LDAP 検索結果を表示・記録するコードです。

- 検索条件となるログイン名属性が設定されていないか、情報が取得できない属性が指定されていることがあります。
- LDAP 認証の設定でログイン名属性が正しく設定されているか確認してください。

#### L0406-003

ログインユーザー名にスペース、「:」、「"」が含まれているため、認証に失敗しています。

- 禁則文字入りアカウントであるときは、アカウントを作成し直してください。
- 誤って禁則文字を入力したときは、正しく入力してログインしてください。

#### L0406-200

同時に大量の認証が発生しているためログインできません。

こんなときには

---

- しばらく経ってからログインしてください。
- 復旧しないときは、認証の攻撃を受けていないか確認してください。
- 攻撃の状態は、画面メッセージ、管理者へのメール通知、システムログにて確認できません。

#### L0406-201

LDAP サーバーの認証設定で [しない] が選択されています。

- 「LDAP サーバー登録／変更／消去」の「認証」設定を [しない] 以外に変更してください。

#### L0406-202 / L0406-203: ケース 1

LDAP 認証設定、LDAP サーバー設定、ネットワーク設定に誤りがあります。

- LDAP サーバー設定が代表者アカウントを正しく設定し、接続テストで成功することを確認してください。  
これに成功しないときは、ネットワーク設定に誤りがあることがあります。  
インターフェース設定のドメイン名や DNS 設定を確認してください。
- LDAP 認証設定で LDAP サーバーが正しく選択されていることを確認してください。
- LDAP 認証設定でログイン名属性が正しく入力されていることを確認してください。
- SSL 設定が LDAP サーバーでサポートされているか確認してください。

#### L0406-202 / L0406-203: ケース 2

ログインユーザー名かパスワードに誤りがあります。

- ログインユーザー名とパスワードが正しく入力されているか確認してください。
- 本機で使用できるログインユーザー名であることを確認してください。
- 以下に当てはまるときは、認証に失敗します。
  - スペース、「:」、「”」の禁則文字を使用しています。
  - ログインユーザー名が 128 バイトを超えています。

#### L0406-202 / L0406-203: ケース 3

簡易認証モードの使用方法に誤りがあります。

- 簡易認証モードでは空パスワードでは認証に失敗します。  
空パスワードを許可するときは、サービス実施店に連絡してください。
- 簡易認証モードでは代表者アカウントでログインユーザー名の DN を取得します。この取得に失敗したときも認証に失敗します。  
サーバー名、ログインユーザー名／パスワードや検索フィルターの入力情報に誤りがなければ確認してください。

#### L0406-204

Kerberos 認証で失敗しました。

- Kerberos 設定が正しく設定されていません。  
レルム名、KDC (キー配布センター) 名、対応ドメイン名を正しく設定しているか確認

こんなときには

---

してください。

- KDC（キー配布センター）と本機の時刻が合っていません。  
KDC（キー配布センター）と本機との間に5分以上の時刻差があるときは、認証に失敗します。  
時刻が合っているか確認してください。
- レルム名を小文字で設定しているとき、Kerberos 認証に失敗します。  
レルム名が小文字になっていないか確認してください。

#### L0409-000

認証サーバーからの応答が返らないため、認証タイムアウトが発生しました。

- ネットワーク環境、および認証に使用するサーバーを確認してください。

#### L0511-000

本機にすでに登録されているユーザーと、認証サーバーの一意属性で区別される別ユーザーのログイン名が重複しています。（一意属性はLDAP 認証設定で指定）

- 重複する古いユーザーを削除するか、ログイン名を変更してください。
- 認証サーバーを切り替えたあとであるときは、古いサーバー側のユーザーを削除してください。

#### L0606-004

ユーザーのログインユーザー名には指定できないユーザー名を指定したため、認証に失敗しました。

- ユーザーのアカウントとして、「other」「admin」「supervisor」「HIDE\*」は使用しないでください。

#### L0607-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

#### L0612-005

アドレス帳の登録数が上限に達し、ユーザー自動登録に失敗したため、認証に失敗しました。

- ユーザー登録件数が最大件数に達しているため、認証に失敗しました。
- ユーザー管理者がアドレス帳内に登録された不要なユーザーを削除してください。

#### L0707-001

アドレス帳が使用中の状態のため、認証に失敗しました。

しばらく経ってから操作してください。

## 操作ができないとき

ユーザーが操作しているときに次のような状態になったときは、対処方法を指示してください。

状態	原因	対処方法
プリンタードライバーから印刷できない。	ユーザー認証が拒否されました。	プリンタードライバーにログインユーザー名とログインパスワードを入力してください。Windows 認証、LDAP 認証を使用しているときは、利用しているネットワークの管理者にログインユーザー名とログインパスワードを確認してください。ベーシック認証のときは、ユーザー管理者に確認してください。
	ドライバーで暗号化を設定しているときに、ドライバー暗号鍵が本機と一致しませんでした。	本機に登録されているドライバー暗号鍵をドライバーに正しく設定してください。詳しくは、P. 106「ドライバー暗号鍵を設定する」を参照してください。
ユーザー認証を無効にしているのに本機で設定したアドレス帳の宛先が表示されない。	[すべてのユーザー]が設定されていない状態で、ユーザー認証の設定を無効にしました。	ユーザー認証の設定を再び有効にし、表示されていない宛先に [すべてのユーザー] の設定を有効にしてください。詳しくは、P. 49「アドレス帳の登録情報を保護する」を参照してください。

こんなときには

状態	原因	対処方法
ユーザー認証を設定しているときに、本機から印刷できない。	プリンタードライバー側にユーザー認証が設定されていません。	プリンタードライバーにユーザー認証の設定をしてください。 プリンタードライバーのヘルプを参照してください。
「上限到達時動作設定」を [ジョブ終了後制限] に設定しているが、印刷が終了する前にジョブがキャンセルされた。	使用しているアプリケーションによっては、本機が単一のジョブを複数のジョブと判断し、印刷中にジョブをキャンセルしてしまうことがあります。	ジョブがキャンセルされたユーザーの利用量カウンターをクリアするなどし、印刷利用量制限の設定を変更してください。利用量カウンターをクリアする方法は、P. 44 「ユーザーの印刷利用量を制限する」を参照してください。
ユーザー個別設定・アドレス帳の暗号化を実行し、しばらく待ったが終了が表示されない。	アドレス帳の件数が多く暗号化に時間がかかっています。もしくは、ファイルが破損しています。	P. 52「機器のデータを暗号化する」の [ファイルシステムデータのみ] / [ファイルシステムデータのみ引き継ぎ] の所要時間を過ぎても画面が更新されないときは、サービス実施店に連絡してください。

## 設定項目の操作権限一覧

管理者認証、ユーザー認証を実施しているときの本機の設定項目について、管理者やユーザーの操作権限をまとめています。

---

### 表の見かた

---

#### ヘッダーの見かた

- User  
ユーザー管理者の操作権限です。
- 機器  
機器管理者の操作権限です。
- N/W  
ネットワーク管理者の操作権限です。
- 文書  
文書管理者の操作権限です。
- あり  
ログインユーザーの操作権限です。  
「管理者認証管理」で管理者認証が有効になっているときの状態です。
- Lv.1  
メニュープロテクトが [レベル 1] に設定されている状態です。
- Lv.2  
メニュープロテクトが [レベル 2] に設定されている状態です。

#### マークの見かた

R/W：実行、変更、閲覧ができます。

R：閲覧ができます。

—：実行、変更、閲覧ができません。

#### ↓ 補足

- メニュープロテクトを [しない] に設定したとき、ユーザーは各機能の設定項目すべてを実行、変更、閲覧できます。



## [メニュー] キー項目の操作権限一覧

### プリンター通常画面

本機の通常の機能画面の項目です。

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

#### 補助メニュー

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
強制排紙	R/W	R/W	R/W	R/W	R/W	R/W
エラー履歴表示	—	R	—	—	R	R
エミュレーション呼び出し	R/W	R/W	R/W	R/W	R/W	R/W

### サプライ情報

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
サプライ情報	R	R	R	R	R	R

### 用紙設定

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
用紙サイズ設定：手差しトレイ	R	R/W	R	R	R/W	R
用紙サイズ設定：トレイ 1~4	R	R/W	R	R	R/W	R
用紙種類設定：手差しトレイ	R	R/W	R	R	R/W	R
用紙種類設定：トレイ 1~4	R	R/W	R	R	R/W	R

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
両面印刷トレイ	R	R/W	R	R	R/W	R
自動トレイ選択	R	R/W	R	R	R/W	R
優先給紙トレイ	R	R/W	R	R	R/W	R

## 調整／管理

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

### 品質調整

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
濃度調整	R	R/W	R	R	R	R
印刷位置調整	R	R/W	R	R	R/W	R
カール低減	R	R/W	R	R	R/W	R
手動ドラム回転	R	R/W	R	R	R	R
低温モード	R	R/W	R	R	R	R
定着クリーニング	R	R/W	R	R	R/W	R

### 一般管理

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
再生紙設定	R	R/W	R	R	R/W	R
色紙設定	R	R/W	R	R	R/W	R
レターヘッド紙設定	R	R/W	R	R	R/W	R
ラベル紙設定	R	R/W	R	R	R/W	R
封筒設定	R	R/W	R	R	R/W	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
印刷済み紙設定	R	R/W	R	R	R/W	R
サプライ交換通知時期設定	R	R/W	R	R	R	R
・トナー	R	R/W	R	R	R	R
・ドラムユニット	R	R/W	R	R	R	R
サプライエンド時動作	R	R/W	R	R	R	R
サプライ残量表示	R	R/W	R	R	R	R
封筒レバーメッセージ	R	R/W	R	R	R	R
メニュープロテクト	R	R/W	R	R	—	—
テスト印刷禁止	R	R/W	R	R	—	—
ブザー音	R	R/W	R	R	R	R
画面コントラスト調整	R	R/W	R	R	R	R
キーリピート設定	R	R/W	R	R	R	R
Compatible ID	R	R/W	R	R	R/W	R

時刻タイマー設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
オートリセット時間設定	R	R/W	R	R	R	R
年月日設定	R	R/W	R	R	R	R
時刻設定	R	R/W	R	R	R	R

機器設定値エクスポート

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
機器設定値エクスポート	—	—	—	R/W	—	—

## テスト印刷

設定項目	User	機器	N/W	文書	あり
一括リスト印刷	—	R/W	—	—	R/W
システム設定リスト	—	R/W	—	—	R/W
エラー履歴	—	R/W	—	—	R/W
ネットワークサマリー	—	R/W	—	—	R/W
サプライ情報リスト	—	R/W	—	—	R/W
メニューリスト	—	R/W	—	—	R/W
ヘキサダンプ	—	R/W	—	—	R/W

## システム設定

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
エラーレポート印刷	R	R/W	R	R	R	R
エラースキップ	R	R/W	R	R	R	R
画像エラー処理	R	R/W	R	R	R	R
エラー表示設定	R	R/W	R	R	R	R
エラー発生時のジョブ自動取消	R	R/W	R	R	R	R
補助用紙サイズ	R	R/W	R	R	R	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
低電力モード移行時間設定	R	R/W	R	R	R	R
・低電力モード移行設定	R	R/W	R	R	R	R
・低電力モード移行時間	R	R/W	R	R	R	R
スリープモード設定	R	R/W	R	R	R	R
・スリープモード移行設定	R	R/W	R	R	R	R
・スリープモード移行時間	R	R/W	R	R	R	R
定着部オフモード(省エネ)移行設定	R	R/W	R	R	R	R
・定着部オフモード(省エネ)移行設定	R	R/W	R	R	R	R
・定着部オフモード解除設定	R	R/W	R	R	R	R
・定着部オフモード(省エネ)移行時間	R	R/W	R	R	R	R
ウィークリータイマー	R	R/W	R	R	R	R
オフ解除コード設定	R	R/W	R	R	R	R
明るさ検知自動電源オフ	R	R/W	R	R	R	R
・モード設定	R	R/W	R	R	R	R
・オフ移行時間	R	R/W	R	R	R	R
・オン移行時間	R	R/W	R	R	R	R
・センサー感度	R	R/W	R	R	R	R
待機時定着ヒーターオフ	R	R/W	R	R	R	R
プリントサーバー使用不可な省エネモード	R	R/W	R	R	R	R
印刷後待機状態	R	R/W	R	R	R	R
エミュレーション検知	R	R/W	R	R	R	R
圧縮データの解凍印刷	R	R/W	R/W	R	R	R

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
優先エミュレーション/プログラム	R	R/W	R	R	R	R
優先メモリー	R	R/W	R	R	R	R
RAM ディスク	R	R/W	R	R	R	R
自動メール通知	R	R/W	R	R	R	R
機械番号	R	R	R	R	R	R

## 印刷設定

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

### 一般設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
180 度回転	R	R/W	R	R	R	R
レターヘッド紙使用設定	R	R/W	R	R	R	R
トレイ設定選択	R	R/W	R	R	R	R
拡張リミットレス給紙	R	R/W	R	R	R	R

## セキュリティー管理

設定項目	User	機器	N/W	文書	あり
セキュリティー強化					
・ SNMPv1, v2 による設定	R	R	R/W	R	R
・ ドライバー暗号鍵：暗号強度設定	R	R	R/W	R	R
・ パスワード攻撃検知	—	R/W	—	—	—

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	あり
・アクセスセキュリティー設定	—	R/W	—	—	—
・アクセス攻撃検知	—	R/W	—	—	—
サービスモード移行禁止設定	R	R/W	R	R	R
ファームウェアバージョン表示	R	R/W	R	R	R
ネットワークセキュリティーレベル	R	R/W	R	R	—
ログ転送設定 <sup>*1</sup>	R	R/W	R	R	R
機器データ暗号化設定	—	R/W	—	—	—
ログ収集設定	R	R/W	R	R	R
・ジョブログ	R	R/W	R	R	R
・アクセスログ	R	R/W	R	R	R
・eco ログ	R	R/W	R	R	R

\*1 [しない] への変更だけです。

## 機器設定情報

設定項目	User	機器	N/W	文書	あり
機器設定情報:エクスポート(メディア) <sup>*1</sup>	—	—	—	—	—
機器設定情報インポート(メディア) <sup>*1</sup>	—	—	—	—	—

\*1 ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が実行、変更、閲覧できます。

## インターフェース設定

管理者認証を設定しているときは、メニュープロテクトの設定によって、ユーザーの操作権限は異なります。

### 受信バッファ

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
受信バッファ	R	R/W	R	R	R	R

## インターフェース切り替え時間

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
インターフェース切り替え時間	R	R/W	R	R	R	R

## ネットワーク設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
本体 IPv4 アドレス*1	R	R	R/W	R	R	R
・ 自動的に取得 (DHCP)	R	R	R/W	R	R	R
・ 指定	R	R	R/W	R	R	R
IPv6 ステータス設定	R	R	R/W	R	R	R
DHCPv6	R	R	R/W	R	R	R
・ DHCPv6 設定	R	R	R/W	R	R	R
・ 動作モード	R	R	R/W	R	R	R
・ DNS サーバーアドレス	R	R	R/W	R	R	R
IPsec	R	R	R/W	R	R	R
有効プロトコル	R	R	R/W	R	R	R
・ IPv4	R	R	R/W	R	R	R
・ IPv6	R	R	R/W	R	R	R
・ SMB	R	R	R/W	R	R	R
・ ファームウェアアップデート (IPv4)	R	R	R/W	R	R	R



## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
・ファームウェアアップデート (IPv6)	R	R	R/W	R	R	R
イーサネット速度	R	R	R/W	R	R	R
イーサネット用 IEEE 802.1X 認証	R	R	R/W	R	R	R
IEEE 802.1X 認証初期化	R	R	R/W	R	R	R
SSL/TLS 通信許可設定	R	R	R/W	R	R	R

\*1 自動取得に設定したときは、閲覧だけです。

## USB 設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
USB 速度	R	R/W	R	R	R	R
USB ポート固定	R	R/W	R	R	R	R

## 表示言語切替

すべての管理者、ユーザーが実行、変更、閲覧できます。

## 拡張機能初期設定

このメニューは操作部から設定できません。Web Image Monitor から設定します。

## Web Image Monitor 設定項目の操作権限一覧

### 構成

[機器の情報] 中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
機器	R	R	R	R	R	R
システム	R	R	R	R	R	R
バージョン	R	R	R	R	R	R
エミュレーション	R	R	R	R	R	R

### 状態

[機器の情報] 中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
警告	R	R	R	R	R	R
状態	R	R	R	R	R	R

### 消耗品

[機器の情報] 中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
トナー	R	R	R	R	R	R
ドラムユニット	R	R	R	R	R	R
その他	R	R	R	R	R	R

## 設定項目の操作権限一覧

### カウンター

[機器の情報] の中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
トータル	R	R	R	R	R	R
プリンター	R	R	R	R	R	R
カバレッジ	R	R	R	R	R	R
その他の機器	R	R	R	R	R	R

### ユーザー別カウンター

[機器の情報] の中の項目です。

全ユーザーのカウンター情報を GSV ファイルでダウンロードできます。

### ジョブ

[機器の情報] の中の項目です。

ユーザーは、ユーザー自身が実行したジョブだけを操作できます。

### ジョブリスト

設定項目	User	機器	N/W	文書	なし	あり
実行中/待機中ジョブ一覧：予約削除	—	R/W	—	—	—	R/W
実行中/待機中ジョブ一覧：印刷保留/印刷再開	—	R/W	—	—	—	—
実行中/待機中ジョブ一覧：順序入れ替え	—	R/W	—	—	—	—
ジョブ履歴	—	R	—	—	—	R*1

\*1 ユーザー認証方式が、[ユーザーコード認証] のときに閲覧できます。

### プリンター

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
ジョブ履歴	R	R/W	R	R	R	R
エラー履歴	—	R	—	—	—	R

## 設定

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

## 機器

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

## システム

設定項目	User	機器	N/W	文書	なし	あり
基本設定	—	—	—	—	—	—
・名前	R	R	R/W	R	R/W	R
・コメント	R	R	R/W	R	R/W	R
・設置場所	R	R	R/W	R	R/W	R
・機器側プリンター操作部のメニュープロテクト	R	R/W	R	R	—	—
・機器側操作部の表示言語	R	R/W	R	R	R/W	R
・ファームウェアアップデート許可	R	R/W	R	R	—	—
・IP アドレス機器画面表示	R	R/W	R	R	—	—
・Compatible ID	R	R/W	R	R	R/W	R
優先給紙トレイ プリンター	R	R/W	R	R	R/W	R

設定項目の操作権限一覧

用紙

設定項目	User	機器	N/W	文書	なし	あり
トレイ 1~4*1、手差しトレイ	—	—	—	—	—	—
・用紙サイズ	R	R/W	R	R	R/W	R
・不定形用紙サイズ	R	R/W	R	R	R/W	R
・用紙種類	R	R/W	R	R	R/W	R
・自動用紙選択の対象	R	R/W	R	R	R/W	R
・両面印刷の対象	R	R/W	R	R	R/W	R

\*1 装着された増設トレイが表示されます。

ユーザー用紙種類

設定項目	User	機器	N/W	文書	なし	あり
ユーザー用紙種類 1~8	—	—	—	—	—	—
・用紙名称	R	R/W	R	R	R	R
・用紙種類	R	R/W	R	R	R	R

日付・時刻

設定項目	User	機器	N/W	文書	なし	あり
年月日設定	R	R/W	R	R	R/W	R
時刻設定	R	R/W	R	R	R/W	R
SNTP サーバー名	R	R/W	R	R	R/W	R
SNTP ポーリング間隔	R	R/W	R	R	R/W	R
タイムゾーン	R	R/W	R	R	R/W	R

設定項目の操作権限一覧

タイマー

設定項目	User	機器	N/W	文書	なし	あり
低電力モード移行時間設定	R	R/W	R	R	R/W	R
スリープモード移行時間設定	R	R/W	R	R	R/W	R
オートリセット時間設定	R	R/W	R	R	R/W	R
オートログアウト時間設定	R	R/W	R	R	R/W	R
定着部オフモード移行設定	R	R/W	R	R	R/W	R
・定着部オフモード移行時間	R	R/W	R	R	R/W	R
・定着部オフモード解除設定	R	R/W	R	R	R/W	R
明るさ検知オフ設定	—	—	—	—	—	—
・明るさ検知オフ	R	R/W	R	R	R/W	R
・オフ移行時間	R	R/W	R	R	R/W	R
・オン移行時間	R	R/W	R	R	R/W	R
・オフセンサー感度	R	R/W	R	R	R/W	R
・オンセンサー感度	R	R/W	R	R	R/W	R
ウィークリータイマー	—	—	—	—	—	—
・ウィークリータイマー設定	R	R/W	R	R	R/W	R
・毎日、月曜日～日曜日	R	R/W	R	R	R/W	R
・主電源オンタイマー停止期間	R	R/W	R	R	R/W	R
・オフ解除コード設定	R	R/W	R	R	R/W	R

ログ

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
ジョブログ	—	—	—	—	—	—
・ジョブログ収集	R	R/W	R	R	R/W	R
・ジョブログ収集レベル	R	R/W	R	R	R/W	R
アクセスログ	—	—	—	—	—	—
・アクセスログ収集	R	R/W	R	R	R/W	R
・アクセスログ収集レベル	R	R/W	R	R	R/W	R
eco ログ	—	—	—	—	—	—
・eco ログ収集	R	R/W	R	R	R/W	R
・eco ログ収集レベル	R	R/W	R	R	R/W	R
共通設定	—	—	—	—	—	—
・ログ転送 <sup>*1</sup>	R	R/W	R	R	R/W	R
・ログ暗号化	R	R/W	R	R	R/W	R
・分類コード	R	R/W	R	R	R/W	R

<sup>\*1</sup> [無効] への変更だけです。

## ログダウンロード

設定項目	User	機器	N/W	文書	なし	あり
ダウンロードするログ	—	R/W	—	—	—	—
ダウンロード	—	R/W	—	—	—	—

## メール

設定項目	User	機器	N/W	文書	なし	あり
管理者メールアドレス	—	R/W	—	—	R/W	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
受信	—	—	—	—	—	—
・受信プロトコル	—	R/W	—	—	R/W	R
・受信間隔設定	—	—	R/W	—	R/W	R
・サーバー側メール保持	—	—	R/W	—	R/W	R
SMTP	—	—	—	—	—	—
・SMTP サーバー名	—	—	R/W	—	R/W	R
・SMTP ポート番号	—	—	R/W	—	R/W	R
・SSL	—	—	R/W	—	R	—
・SMTP 認証	—	R/W	—	—	R/W	R
・SMTP 認証メールアドレス	—	R/W	—	—	R/W	R
・SMTP 認証ユーザー名	—	R/W	—	—	R/W	—
・SMTP 認証パスワード*1	—	R/W	—	—	R/W	—
・SMTP 認証暗号化	—	R/W	—	—	R/W	R
POP before SMTP	—	R/W	—	—	R/W	R
・POP メールアドレス	—	R/W	—	—	R/W	R
・POP ユーザー名	—	R/W	—	—	R/W	—
・POP パスワード*1	—	R/W	—	—	R/W	—
・POP 認証後待機時間	—	R/W	—	—	R/W	R
POP3/IMAP4	—	—	—	—	—	—
・POP3/IMAP4 サーバー名	—	R/W	—	—	R/W	R
・POP3/IMAP4 暗号化	—	R/W	—	—	R/W	R
メール通信ポート	—	—	—	—	—	—



設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・ POP3 受信ポート番号	—	—	R/W	—	R/W	R
・ IMAP4 受信ポート番号	—	—	R/W	—	R/W	R
メール通知アカウント	—	—	—	—	—	—
・ メール通知用メールアドレス	—	—	R/W	—	R/W	R
・ メール通知の受信	—	R/W	—	—	R/W	—
・ メール通知ユーザー名	—	R/W	—	—	R/W	—
・ メール通知パスワード*1	—	R/W	—	—	R/W	—

\*1 パスワードは閲覧できません。

自動メール通知

設定項目	User	機器	N/W	文書	なし	あり
共通本文	R	R/W	R	R	R	R
通知先グループ グループ1~4	—	—	—	—	—	—
・ 名称	R	R/W	R	R	R	R
・ 通知先リスト	R	R/W	R	R	R	R
項目ごとの通知先	—	—	—	—	—	—
・ サービスコール	R	R/W	R	R	R	R
・ トナーなし	R	R/W	R	R	R	R
・ トナー残りわずか	R	R/W	R	R	R	R
・ 用紙つまり	R	R/W	R	R	R	R
・ カバーオープン	R	R/W	R	R	R	R
・ 用紙なし	R	R/W	R	R	R	R
・ 給紙トレイエラー	R	R/W	R	R	R	R

### 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・ 排紙先満杯	R	R/W	R	R	R	R
・ ユニット接続エラー	R	R/W	R	R	R	R
・ 廃トナー満杯	R	R/W	R	R	R	R
・ 廃トナーもうすぐ満杯	R	R/W	R	R	R	R
・ 文書保存領域もうすぐ満杯	R	R/W	R	R	R	R
・ アクセス攻撃検知	R	R/W	R	R	R	R
・ ユニット交換時期	R	R/W	R	R	R	R
・ ユニット交換間近	R	R/W	R	R	R	R
・ トナー残りわずか（残量レベル選択）	R	R/W	R	R	R	R
各項目の詳細設定	R	R/W	R	R	R	R

### 要求時メール通知

設定項目	User	機器	N/W	文書	なし	あり
共通件名	R	R/W	R	R	R	R
共通本文	R	R/W	R	R	R	R
要求時メール通知のアクセス制限	—	—	—	—	—	—
・ 機器状態情報通知の制限	R	R/W	R	R	R	R
受信可能メールアドレス/ドメイン設定	R	R/W	R	R	R	R

### ユーザー認証管理

設定項目	User	機器	N/W	文書	なし	あり
ユーザー認証管理	R	R/W	R	R	R/W	R

## 設定項目の操作権限一覧

### 管理者認証管理

設定項目	User	機器	N/W	文書	なし	あり
ユーザー管理者認証	R/W	R	R	R	R	R
機器管理者認証	R	R/W	R	R	R	R
ネットワーク管理者認証	R	R	R/W	R	R	R
文書管理者認証	R	R	R	R/W	R	R

### 管理者登録/変更

設定項目	User	機器	N/W	文書	なし	あり
ユーザー管理者	R/W	R	R	R	—	—
機器管理者	R	R/W	R	R	—	—
ネットワーク管理者	R	R	R/W	R	—	—
文書管理者	R	R	R	R/W	—	—
管理者 1~4	—	—	—	—	—	—
・ログインユーザー名* <sup>1</sup>	R/W	R/W	R/W	R/W	—	—
・ログインパスワード* <sup>1</sup>	R/W	R/W	R/W	R/W	—	—
・暗号パスワード* <sup>1</sup>	R/W	R/W	R/W	R/W	—	—

\*<sup>1</sup> 管理者が管理者自身のアカウントだけを変更できます。

### 印刷利用量制限

設定項目	User	機器	N/W	文書	なし	あり
上限到達時動作	R	R/W	R	R	R	R
印刷利用量制限度数設定	R	R/W	R	R	R	R

### 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
利用量カウンター定期/指定リセット設定	R	R/W	R	R	R	R

### LDAP サーバー

設定項目	User	機器	N/W	文書	なし	あり
登録	—	R/W	—	—	R/W	—
変更	—	R/W	—	—	R/W	—
消去	—	R/W	—	—	R/W	—

### ファームウェアアップデート

設定項目	User	機器	N/W	文書	なし	あり
ファームウェアファイル名	—	R/W	—	—	—	—
・アップデート	—	R/W	—	—	—	—
ファームウェアバージョン	—	R	—	—	—	—

### Kerberos 認証

設定項目	User	機器	N/W	文書	なし	あり
暗号化アルゴリズム	—	R/W	—	—	—	—
レルム 1~5	—	—	—	—	—	—
・レルム名	—	R/W	—	—	—	—
・KDC サーバー名	—	R/W	—	—	—	—
・ドメイン名	—	R/W	—	—	—	—

### 機器設定情報のインポート設定 (サーバー)

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
ファイルのインポート元* <sup>1</sup>	—	—	—	—	—	—
・ URL	—	—	—	—	—	—
・ ユーザー名	—	—	—	—	—	—
・ パスワード	—	—	—	—	—	—
指定時刻での定期インポート* <sup>1</sup>	—	—	—	—	—	—
・ 指定時刻 1~2						
前回のインポートファイルとの比較* <sup>1</sup>	—	—	—	—	—	—
失敗時のメール通知* <sup>1</sup>	—	—	—	—	—	—
再試行回数* <sup>1</sup>	—	—	—	—	—	—
再試行間隔* <sup>1</sup>	—	—	—	—	—	—
暗号鍵* <sup>1</sup>	—	—	—	—	—	—

\*<sup>1</sup> ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が実行、変更、閲覧できます。

## インポートテスト

設定項目	User	機器	N/W	文書	なし	あり
インポートテスト* <sup>1</sup>	—	—	—	—	—	—

\*<sup>1</sup> ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が実行、変更、閲覧できます。

## プリンター

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、「メニュープロテクト」の設定によって、ユーザーの操作権限は異なります。

基本設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
システム設定	—	—	—	—	—	—
・エラーレポート印刷	R	R/W	R	R	R	R
・エラースキップ	R	R/W	R	R	R	R
・画像エラー処理	R	R/W	R	R	R	R
・エラー表示設定	R	R/W	R	R	R	R
・エラー発生時のジョブ自動取消	R	R/W	R	R	R	R
・180度回転	R	R/W	R	R	R	R
・圧縮データの解凍印刷	R	R/W	R/W	R	R	R
・優先メモリー	R	R/W	R	R	R	R
・補助用紙サイズ	R	R/W	R	R	R	R
・レターヘッド紙使用設定	R	R/W	R	R	R	R
・トレイ設定選択	R	R/W	R	R	R	R
・拡張リミットレス給紙	R	R/W	R	R	R	R
・仮想プリンター	R	R/W	R	R	R	R
インターフェース設定	R	R/W	R	R	R	R
・受信バッファ	R	R/W	R	R	R	R
・インターフェイス切り替え時間	R	R/W	R	R	R	R

仮想プリンター設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
仮想プリンター名	R	R/W	R	R	R	R

プリンター言語のファイルシステム操作許可設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
PJL	R	R/W	R	R	R	R

インターフェース

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

インターフェース設定

設定項目	User	機器	N/W	文書	なし	あり
イーサネット	—	—	—	—	—	—
・ネットワーク	R	R	R	R	R	R
・物理アドレス	R	R	R	R	R	R
・セキュリティ (802.1X)	R	R	R/W	R	R	R
・イーサネット速度	R	R	R/W	R	R	R
USB	R	R/W	R	R	R	R
USB ホスト	R	R	R	R	R	R

ネットワーク

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

設定項目の操作権限一覧

IPv4

設定項目	User	機器	N/W	文書	なし	あり
IPv4	—	—	—	—	—	—
イーサネット	—	—	—	—	—	—
・ ホスト名	R	R	R/W	R	R	R
・ DHCP	R	R	R/W	R	R	R
・ ドメイン名	R	R	R/W	R	R	R
・ IPv4 アドレス	R	R	R/W	R	R	R
・ サブネットマスク	R	R	R/W	R	R	R
・ DDNS	R	R	R/W	R	R	R
・ WINS	R	R	R/W	R	R	R
・ プライマリー-WINS サーバー	R	R	R/W	R	R	R
・ セカンダリー-WINS サーバー	R	R	R/W	R	R	R
・ LLMNR	R	R	R/W	R	R	R
・ スコープ ID	R	R	R/W	R	R	R
詳細情報	—	—	—	—	—	—
・ デフォルトゲートウェイ	R	R	R/W	R	R	R
・ DNS サーバー	R	R	R/W	R	R	R
・ LPR	R	R	R/W	R	R	R
・ RSH/RCP	R	R	R/W	R	R	R
・ DIPRINT	R	R	R/W	R	R	R
・ FTP	R	R	R/W	R	R	R
・ sftp	R	R	R/W	R	R	R



設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・ WSD (Device)	R	R	R/W	R	R	R
・ WSD (Printer)	R	R	R/W	R	R	R
・ WSD (機器の暗号化通信)	R	R	R/W	R	R	R
・ IPP	R	R	R/W	R	R	R
・ WSD (Printer) /IPP タイムアウト	R	R	R/W	R	R	R
・ RHPP	R	R	R/W	R	R	R

IPv6

設定項目	User	機器	N/W	文書	なし	あり
IPv6	R	R	R/W	R	R	R
イーサネット	—	—	—	—	—	—
・ ホスト名	R	R	R/W	R	R	R
・ ドメイン名	R	R	R/W	R	R	R
・ リンクローカルアドレス	R	R	R	R	R	R
・ ステートレスアドレス	R	R	R/W	R	R	R
・ 手動設定アドレス	R	R	R/W	R	R	R
・ DHCPv6	R	R	R/W	R	R	R
・ DHCPv6 アドレス	R	R	R	R	R	R
・ DDNS	R	R	R/W	R	R	R
・ LLMNR	R	R	R/W	R	R	R
詳細情報	—	—	—	—	—	—
・ デフォルトゲートウェイ	R	R	R/W	R	R	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・ DNS サーバー	R	R	R/W	R	R	R
・ DHCPv6 動作モード	R	R	R/W	R	R	R
・ DUID	R	R	R	R	R	R
・ LPR	R	R	R/W	R	R	R
・ RSH/RCP	R	R	R/W	R	R	R
・ DIPRINT	R	R	R/W	R	R	R
・ FTP	R	R	R/W	R	R	R
・ sftp	R	R	R/W	R	R	R
・ WSD (Device)	R	R	R/W	R	R	R
・ WSD (Printer)	R	R	R/W	R	R	R
・ WSD (機器の暗号化通信)	R	R	R/W	R	R	R
・ IPP	R	R	R/W	R	R	R
・ WSD (Printer) /IPP タイムアウト	R	R	R/W	R	R	R
・ RHPP	R	R	R/W	R	R	R

SMB

設定項目	User	機器	N/W	文書	なし	あり
SMB	R	R	R/W	R	R	R
基本設定	—	—	—	—	—	—
・ プロトコル	R	R	R	R	R	R
・ ワークグループ名	R	R	R/W	R	R	R
・ コンピュータ名	R	R	R/W	R	R	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・コメント	R	R	R/W	R	R	R
・共有名	R	R	R	R	R	R
・印刷完了通知	R	R	R/W	R	R	R

SNMP

設定項目	User	機器	N/W	文書	なし	あり
SNMP	—	—	R/W	—	R	R
プロトコル	—	—	—	—	—	—
・IPv4	—	—	R/W	—	R	R
・IPv6	—	—	R/W	—	R	R
SNMPv1, v2 共通設定	—	—	—	—	—	—
・SNMPv1, v2 機能	—	—	R/W	—	R	R
・SNMPv1Trap 送信	—	—	R/W	—	R	R
・SNMPv2Trap 送信	—	—	R/W	—	R	R
・SNMPv1, v2 による設定許可	—	—	R/W	—	R	R
コミュニティ	—	—	R/W	—	R	R

SNMPv3

設定項目	User	機器	N/W	文書	なし	あり
SNMP	—	—	R/W	—	R	R
プロトコル	—	—	—	—	—	—
・IPv4	—	—	R/W	—	R	R

設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
・ IPv6	—	—	R/W	—	R	R
SNMPv3 設定	—	—	—	—	—	—
・ SNMPv3 機能	—	—	R/W	—	R	R
・ SNMPv3Trap 送信	—	—	R/W	—	R	R
・ コンテキスト名	—	—	R	—	R	R
・ 認証アルゴリズム	—	—	R/W	—	R	R
・ 暗号化アルゴリズム	—	—	R/W	—	R	R
・ SNMPv3 通信許可設定	—	—	R/W	—	R	R
SNMPv3 Trap 送信設定	—	—	R/W	—	R	R
アカウント(一般)	—	—	—	—	—	—
・ アカウント名 (一般)	—	—	R/W	—	R	R
・ 認証パスワード (一般)	—	—	R/W	—	R	R
・ 暗号パスワード (一般)	—	—	R/W	—	R	R
・ アクセスタイプ (一般)	—	—	R/W	—	R	R
アカウント(ネットワーク管理者)	—	—	R/W	—	R	R
アカウント(機器管理者)	—	R/W	—	—	R	R

SSDP

設定項目	User	機器	N/W	文書	なし	あり
SSDP	—	—	R/W	—	R	R
UUID	—	—	R	—	R	R
プロファイル有効期限	—	—	R/W	—	R	R

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	なし	あり
TTL	—	—	R/W	—	R	R

## Bonjour

設定項目	User	機器	N/W	文書	なし	あり
Bonjour	—	—	—	—	—	—
・ IPv4	R	R	R/W	R	R	R
・ IPv6	R	R	R/W	R	R	R
イーサネット	—	—	—	—	—	—
・ ローカルホスト名	R	R	R	R	R	R
詳細情報	—	—	—	—	—	—
・ コンピュータ名	R	R	R/W	R	R	R
・ 設置場所	R	R	R/W	R	R	R
印刷優先順位	—	—	—	—	—	—
・ DIPRINT	R	R	R/W	R	R	R
・ LPR	R	R	R/W	R	R	R
・ IPP	R	R	R/W	R	R	R

## システムログ

設定項目	User	機器	N/W	文書	なし	あり
システムログ	R	R	R	R	R	R

## セキュリティー

[機器の管理] の [設定] の項目です。

ネットワークセキュリティー

設定項目	User	機器	N/W	文書	あり
セキュリティーレベル	—	—	R/W	—	—
TCP/IP	—	—	—	—	—
・ TCP/IP	—	—	R/W	—	—
・ HTTP	—	—	R/W	—	—
・ IPP	—	—	R/W	—	—
・ SSL/TLS	—	—	R/W	—	—
・ SSL/TLS バージョン	—	—	R/W	—	—
・ 暗号強度設定	—	—	R/W	—	—
・ DIPRINT	—	—	R/W	—	—
・ LPR	—	—	R/W	—	—
・ FTP	—	—	R/W	—	—
・ sftp	—	—	R/W	—	—
・ ssh	—	—	R/W	—	—
・ RSH/RCP	—	—	R/W	—	—
・ TELNET	—	—	R/W	—	—
・ Bonjour	—	—	R/W	—	—
・ SSDP	—	—	R/W	—	—
・ SMB	—	—	R/W	—	—
・ NetBIOS over TCP/IPv4	—	—	R/W	—	—
・ WSD (Device)	—	—	R/W	—	—

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	あり
・ WSD (Printer)	—	—	R/W	—	—
・ WSD (機器の暗号化通信)	—	—	R/W	—	—
・ RHPP	—	—	R/W	—	—
SNMP	—	—	R/W	—	—
・ SNMPv1, v2 による設定許可	—	—	R/W	—	—
・ SNMPv1, v2 機能	—	—	R/W	—	—
・ SNMPv3 機能	—	—	R/W	—	—
・ SNMPv3 通信許可設定	—	—	R/W	—	—
TCP/IP 暗号強度設定	—	—	—	—	—
・ ssh	—	—	R/W	—	—
・ IPsec	—	—	R/W	—	—
・ IEEE802.1X (有線)	—	—	R/W	—	—
・ SNMPv3	—	—	R/W	—	—
・ Kerberos 認証	—	—	R/W	—	—
・ ドライバー暗号鍵	—	—	R/W	—	—

## アクセスコントロール

設定項目	User	機器	N/W	文書	あり
IPv4	—	—	—	—	—
・ アクセスコントロール範囲 1~5	—	—	R/W	—	—
IPv6	—	—	—	—	—
・ アクセスコントロール範囲 1~5	—	—	R/W	—	—

## 設定項目の操作権限一覧

### IPP 認証

設定項目	User	機器	N/W	文書	あり
認証	—	—	R/W	—	—
・ ユーザー名 1~10	—	—	R/W	—	—
・ パスワード 1~10	—	—	R/W	—	—

### SSL/TLS

設定項目	User	機器	N/W	文書	あり
SSL/TLS	—	—	—	—	—
・ IPv4	—	—	R/W	—	—
・ IPv6	—	—	R/W	—	—
SSL/TLS 通信許可設定	—	—	R/W	—	—
証明書状態	—	—	R	—	—
SSL/TLS バージョン	—	—	—	—	—
・ TLS1.2	—	—	R/W	—	—
・ TLS1.1	—	—	R/W	—	—
・ TLS1.0	—	—	R/W	—	—
・ SSL3.0	—	—	R/W	—	—
暗号強度設定	—	—	—	—	—
・ AES	—	—	R/W	—	—
・ 3DES	—	—	R/W	—	—
・ RC4	—	—	R/W	—	—



## 設定項目の操作権限一覧

### ssh

設定項目	User	機器	N/W	文書	あり
ssh	—	—	R/W	—	R
ssh 設定	—	—	—	—	—
・ 圧縮転送	—	—	R/W	—	R
・ ポート番号	—	—	R/W	—	R
・ タイムアウト	—	—	R/W	—	R
・ ログインタイムアウト	—	—	R/W	—	R
・ 暗号化アルゴリズム	—	—	R/W	—	R
・ 公開鍵	—	—	R/W	—	R

### サイト証明書

設定項目	User	機器	N/W	文書	あり
サイト証明書チェック機能	—	—	R/W	—	—
インポート済みのサイト証明書	—	—	R/W	—	—
サイト証明書のインポート	—	—	R/W	—	—

### 機器証明書

設定項目	User	機器	N/W	文書	あり
証明書 1~6	—	—	R/W	—	—
利用する証明書	—	—	—	—	—
・ SSL/TLS	—	—	R/W	—	—
・ IEEE802.1X	—	—	R/W	—	—

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	あり
・ IPsec	—	—	R/W	—	—

## IPsec

設定項目	User	機器	N/W	文書	あり
IPsec	—	—	—	—	—
・ IPsec	—	—	R/W	—	—
・ HTTPS 通信の除外	—	—	R/W	—	—
自動鍵交換設定	—	—	R/W	—	—

## ユーザーロックアウト

設定項目	User	機器	N/W	文書	あり
ロックアウト	—	R/W	—	—	—
ログインパスワード入力許容回数	—	R/W	—	—	—
ロックアウト解除タイマー	—	R/W	—	—	—
ロックアウト解除までの時間	—	R/W	—	—	—

## IEEE802. 1X

設定項目	User	機器	N/W	文書	あり
ユーザー名	—	—	R/W	—	—
ドメイン名	—	—	R/W	—	—
EAP タイプ	—	—	R/W	—	—
IEEE802. 1X クライアント証明書状態	—	—	R/W	—	—

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	あり
パスワード	—	—	R/W	—	—
フェーズ2 ユーザー名	—	—	R/W	—	—
フェーズ2 メソッド	—	—	R/W	—	—
・ EAP-TTLS	—	—	R/W	—	—
・ PEAP	—	—	R/W	—	—
サーバー証明書の認証	—	—	R/W	—	—
中間認証局の信頼	—	—	R/W	—	—
サーバーID	—	—	R/W	—	—
サブドメイン許可	—	—	R/W	—	—

## セキュリティ強化

設定項目	User	機器	N/W	文書	あり
ドライバー暗号鍵：暗号強度設定	R	R	R/W	R	R
ファームウェアアップデート	R	R/W	R	R	—
ファームウェア構成変更	R	R/W	R	R	—
SNMPv1, v2 による設定	R	R	R/W	R	R
アクセスセキュリティ設定	—	R/W	—	—	—
・ 攻撃拒否時間	—	R/W	—	—	—
・ ユーザー管理対象数	—	R/W	—	—	—
・ パスワード管理対象数	—	R/W	—	—	—
・ 状態監視間隔	—	R/W	—	—	—
パスワード攻撃検知	—	—	—	—	—

## 設定項目の操作権限一覧

設定項目	User	機器	N/W	文書	あり
・ 許容回数	—	R/W	—	—	—
・ 測定時間	—	R/W	—	—	—
アクセス攻撃検知	—	—	—	—	—
・ 許容回数	—	R/W	—	—	—
・ 測定時間	—	R/W	—	—	—
・ 認証遅延処理時間	—	R/W	—	—	—
・ 同時アクセス管理対象数	—	R/W	—	—	—

## Webpage 設定

[機器の管理] の [設定] の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

設定項目	User	機器	N/W	文書	なし	あり
Web Image Monitor オートログアウト	—	—	—	—	—	—
・ Web Image Monitor オートログアウト設定時間	R	R	R/W	R	R/W	R
リンクページのリンク先設定	—	—	—	—	—	—
・ URL1	R	R	R/W	R	R/W	R
・ URL2	R	R	R/W	R	R/W	R
ヘルプリンク先設定	R	R	R/W	R	R/W	R
WSD/UPnP 設定	R	R	R/W	R	R/W	R

## 設定項目の操作権限一覧

### 拡張機能初期設定

[機器の管理] の [設定] の項目です。

設定項目	User	機器	N/W	文書	なし	あり
起動設定	—	R/W	—	—	—	—
拡張機能情報	R	R	R	R	R	R
インストール	—	R/W	—	—	—	—
アンインストール	—	R/W	—	—	—	—
管理者用設定	—	R/W	—	—	—	—
追加プログラム起動設定	—	R/W	—	—	—	—
追加プログラムインストール	—	R/W	—	—	—	—
追加プログラムアンインストール	—	R/W	—	—	—	—
拡張機能複製	—	R/W	—	—	—	—
カードセーブデータ複製	—	R/W	—	—	—	—

### アドレス帳

[機器の管理] の中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
ユーザー追加	R/W	—	—	—	R/W	R/W
変更	R/W	—	—	—	R/W	R/W
削除	R/W	—	—	—	R/W	R/W
グループ追加	R/W	—	—	—	R/W	R/W
メンテナンス	R/W	—	—	—	R/W	R/W

## 設定項目の操作権限一覧

### 印刷取消

[機器の管理] の中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
印刷中ジョブ消去	—	R/W	—	—	—	—
全ジョブ消去	—	R/W	—	—	—	—

### 機器のリセット

[機器の管理] の中の項目です。

管理者認証を設定しているときは、[管理者認証管理] の適用初期設定項目によって、ユーザーの操作権限は異なります。

設定項目	User	機器	N/W	文書	なし	あり
機器のリセット	—	R/W	—	—	R/W	—

## アドレス帳の操作権限一覧

### ヘッダーの見かた

- 閲覧  
「閲覧」権限が設定されているユーザーです。
- 編集  
「編集」権限が設定されているユーザーです。
- 編/削  
「編集／削除」権限が設定されているユーザーです。
- フル  
「フルコントロール」権限が設定されているユーザーです。
- 登録者  
アドレス帳に個人情報を登録されたユーザーです。ユーザーのログインユーザー名とログインパスワードを認知している本人です。
- User  
ユーザー管理者です。

### マークの見かた

R/W : 実行、変更、閲覧ができます。

## 設定項目の操作権限一覧

---

R：閲覧ができます。

－：実行、変更、閲覧ができません。

### 登録情報

設定項目	閲覧	編集	編/削	フル	登録者	User
登録番号	R	R/W	R/W	R/W	R/W	R/W
名前	R	R/W	R/W	R/W	R/W	R/W
ヨミガナ	R	R/W	R/W	R/W	R/W	R/W

### 認証情報

設定項目	閲覧	編集	編/削	フル	登録者	User
ユーザーコード	－	－	－	－	－	R/W
ログインユーザー名	－	－	－	－	R	R/W
ログインパスワード	－	－	－	－	R/W*1	R/W*1
使用できる機能	－	－	－	－	R	R/W
印刷利用量制限	－	－	－	－	R	R/W

\*1 パスワードは閲覧できません。

### 認証保護

設定項目	閲覧	編集	編/削	フル	登録者	User
宛先保護: アクセス許可ユーザー/グループ	－	－	－	R/W	R/W	R/W

### 登録先グループ

---

設定項目	閲覧	編集	編/削	フル	登録者	User
登録番号指定	R	R/W	R/W	R/W	R/W	R/W
検索	—	R/W	R/W	R/W	R/W	R/W



***SPEEDIA*** B9500シリーズ  
**セキュリティーガイド**

2015年1月5日 第1版発行

カシオ計算機株式会社  
〒151-8543 東京都渋谷区本町 1-6-2  
カシオ電子工業株式会社