



使用説明書

セキュリティガイド

はじめに	7
セキュリティ機能を設定する前に.....	7
本機の運用を開始する前に.....	8
管理者とは	9
管理者認証を設定する.....	10
管理者の権限を設定する.....	11
管理者を登録、変更する.....	12
Web Image Monitorを使用して管理者認証を設定する.....	15
管理者のログイン方法.....	16
操作部からログインする.....	16
Web Image Monitorからログインする.....	17
管理者のログアウト方法.....	18
操作部からログアウトする.....	18
Web Image Monitorからログアウトする.....	18
スーパーバイザーとは.....	19
管理者のパスワードを再設定する.....	19
スーパーバイザーを変更する.....	20
ユーザー認証を設定する.....	22
ユーザーとは	22
ユーザー認証の概念.....	23
ユーザー認証を設定する.....	24
ユーザーコード認証.....	26
ユーザーコード認証を設定する.....	26

ベーシック認証	28
ベーシック認証を設定する	28
アドレス帳の認証情報	29
ログインユーザー名とログインパスワードを設定する	30
ログイン用認証情報を設定する	30
Windows認証	32
Windows認証を設定する	34
「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	37
サーバー証明書を作成する	38
ファクス情報を取得できなかったとき	38
LDAP認証	40
LDAP認証を設定する	41
プリンタジョブ認証	45
プリンタジョブ認証のレベル	45
プリンタジョブの種類	45
authfreeコマンド	47
アドレス帳の自動登録	49
アドレス帳自動登録時データ利用設定	49
ロックアウト機能	51
パスワードロックアウト設定	52
パスワードロックアウト解除	52
オートログアウト時間設定	54
機器の利用を制限する	55
宛先表の利用を制限する	55
宛先利用制限／個人宛先登録制限	55
管理者設定項目の変更を防止する	57
ユーザーによる設定の変更を禁止する	57
メニュープロテクト	58
メニュープロテクトを設定する	58
機能の利用を制限する	60
使用できる機能を設定する	60
メディアスロットへのアクセスを制限する	61
ユーザーの印刷利用量を制限する	62
利用量制限を設定する	63
利用量上限の初期値を設定する	65
ユーザーごとに利用量上限を設定する	65

ユーザーの利用量を確認する.....	67
ユーザーの利用量カウンターを印刷する.....	68
利用量カウンターをクリアする.....	69
自動リセット機能を設定する.....	70
機器情報の漏洩を防止する.....	72
アドレス帳の登録情報を保護する.....	72
アドレス帳にアクセス権を設定する.....	72
アドレス帳を暗号化する.....	73
機器のデータを暗号化する.....	76
暗号化設定を有効にする.....	77
暗号鍵をバックアップする.....	79
暗号鍵を更新する.....	80
暗号化を解除する.....	81
ハードディスクのデータを上書き消去する.....	83
使用環境.....	83
使用上のご注意.....	83
メモリー自動消去設定.....	83
メモリー全消去.....	88
ネットワークセキュリティーを強化する.....	91
アクセスコントロールを設定する.....	91
プロトコルの有効／無効を設定する.....	92
操作部から設定する.....	96
Web Image Monitorから設定する.....	97
ネットワークセキュリティーレベルを設定する.....	98
操作部から設定する.....	98
Web Image Monitorから設定する.....	99
各機能とネットワークセキュリティーレベルの関係.....	99
機器証明書による通信経路の保護.....	106
操作部から機器証明書を作成、導入する（自己証明書）.....	106
Web Image Monitorから機器証明書を作成、導入する（自己証明書）.....	107
機器証明書を作成、申請する（認証局証明書）.....	107
機器証明書を導入する（認証局証明書）.....	108
中間証明書を導入する（認証局証明書）.....	109
SSL/TLSを設定する.....	110
SSL/TLSを有効にする.....	111
SSL/TLSのユーザー設定.....	112

SSL/TLS暗号化通信モードを設定する.....	113
SMTP通信のSSLを設定する.....	114
S/MIMEを設定する.....	115
メッセージを暗号化する.....	115
署名を添付する.....	117
証明書の有効期限チェックを設定する.....	119
電子署名付きPDFの設定をする.....	121
証明書を選択する.....	121
IPsecを設定する.....	123
通信データの暗号化と認証.....	123
自動鍵交換設定と手動鍵設定.....	124
IPsec設定項目.....	125
自動鍵交換設定の流れ.....	135
手動鍵設定の流れ.....	139
telnetでIPsecを設定する.....	140
IEEE 802.1X認証を設定する.....	148
サイト証明書を導入する.....	148
機器証明書を選択する.....	149
イーサネットでIEEE 802.1Xを使用する.....	149
無線LANでIEEE 802.1Xを使用する.....	151
SNMPv3 暗号化通信を設定する.....	154
パスワードを暗号化する.....	156
ドライバー暗号鍵を設定する.....	156
IPP認証のパスワードを設定する.....	157
Kerberos認証の暗号化設定.....	158
文書の漏洩を防止する.....	159
蓄積文書にアクセス権を設定する.....	159
蓄積文書ごとにアクセス権を設定する.....	160
蓄積文書のオーナーを変更する.....	163
ユーザーごとに蓄積文書に対するアクセス権を設定する.....	163
蓄積文書にパスワードを設定する.....	165
蓄積文書のロックを解除する.....	166
不正コピー抑止機能.....	168
地紋印刷を有効にする.....	168
印刷紙にユーザー情報を印字する.....	170
機密印刷文書を管理する.....	173

機密印刷文書を消去する.....	173
機密印刷文書のパスワードを変更する.....	174
機密印刷文書のロックを解除する.....	176
プリンターの印刷文書を強制的に蓄積する.....	177
本機を管理する	178
ログを管理する	178
本機からログを管理する.....	178
Web Image Monitorからログを管理する.....	179
Web Image Monitorで管理できるログ項目.....	185
操作部をカスタマイズする.....	221
ユーザー別ホームを設定する.....	221
機器情報を管理する.....	223
機器情報をエクスポートする.....	224
機器情報をインポートする.....	225
eco指数カウンターを管理する.....	227
eco指数カウンターの表示を設定する.....	227
機器のeco指数カウンターをクリアする.....	228
ユーザー別のeco指数カウンターをクリアする.....	228
セキュリティー強化機能を設定する.....	230
セキュリティー強化機能の設定項目.....	230
その他のセキュリティー機能.....	238
ファクス機能	238
スキャナー機能	239
システム状態	239
ファームウェアの正当性確認.....	239
機器の操作をお客様に限定する.....	240
設定項目	240
より安全にお使いいただくために.....	242
操作部から設定する項目.....	242
Web Image Monitorから設定する項目.....	245
IPsec有効/無効時の設定.....	247
こんなときには	250
認証がうまくいかなかったとき.....	250
メッセージが表示されたとき.....	250
エラーコードが表示されたとき.....	252
操作ができないとき.....	267

操作権限を確認する	274
設定項目の操作権限一覧.....	274
システム初期設定	276
ホーム編集	286
コピー／ドキュメントボックス初期設定.....	287
ファクス初期設定	293
プリンター通常画面.....	297
プリンター初期設定.....	298
スキャナー初期設定.....	303
Web Image Monitor：eco指数カウンター表示.....	305
Web Image Monitor：ジョブ.....	306
Web Image Monitor：機器.....	308
Web Image Monitor：プリンター.....	317
Web Image Monitor：ファクス.....	321
Web Image Monitor：スキャナー.....	324
Web Image Monitor：インターフェース.....	327
Web Image Monitor：ネットワーク.....	329
Web Image Monitor：セキュリティー.....	333
Web Image Monitor：Webpage.....	334
Web Image Monitor：アドレス帳.....	335
Web Image Monitor：印刷取消.....	336
Web Image Monitor：機器のリセット.....	337
Web Image Monitor：機器のホーム画面の管理.....	338
Web Image Monitor：ユーザーカスタマイズ.....	339
Web Image Monitor：ドキュメントボックス.....	340
Web Image Monitor：ファクス蓄積受信文書.....	341
Web Image Monitor：プリンター文書印刷.....	342
蓄積文書の操作権限一覧.....	343
アドレス帳の操作権限一覧.....	345
商標	349
索引	351

はじめに

セキュリティー機能を使用する場合の注意点と、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

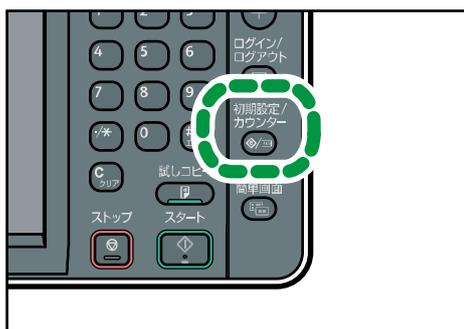
★重要

- **機器のセキュリティー設定を行わないときには、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。**
1. 本機が持ち出されたり壊されたりすることなどがないように、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。
 2. 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行わないときは、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。
 3. 管理者の方はセキュリティー機能をご使用になる前に、この使用説明書『セキュリティーガイド』を最後までよくお読みのうえ、正しくお使いください。特に、「セキュリティー機能を設定する前に」はよく読んでご理解ください。
 4. 管理者の方は、ユーザーがセキュリティー機能を正しくお使いいただけるように、利用方法をご指導ください。
 5. 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。
 6. 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お使いください。
 7. 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以下の設定をすみやかに行ってください。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。

1. 本機の主電源を入れます。
2. [初期設定/カウンター] キーを押します。



CJR003

3. [システム初期設定] を押します。
4. [インターフェース設定] を押します。
5. 本体 IPv4 アドレスを設定します。
IPv4 アドレスの設定方法は、『ネットワークの接続/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。
6. [システム初期設定] の [ファイル転送設定] を押します。
7. [管理者メールアドレス] を押し、本機の管理者のメールアドレスを設定します。
8. 操作部から機器証明書の作成と導入をします。
機器証明書の導入方法は、P. 106「機器証明書による通信経路の保護」を参照してください。
設定項目のメールアドレスに、手順 7 で入力した管理者メールアドレスを設定してください。
9. 管理者のユーザー名、パスワードを変更します。
管理者のユーザー名、パスワードの設定については、P. 12「管理者を登録、変更する」を参照してください。
10. 本機を運用環境で使用するネットワークに接続してください。

↓ 補足

- より高度なセキュリティーを希望するときは、P. 242「より安全にお使いいただくために」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、認証機能を有効にする必要があります。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になります。

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ことで、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人で兼務することや、1つの管理者を複数人で担当することもできます。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。

管理者は機器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コピーやプリンター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. 12「管理者を登録、変更する」、スーパーバイザーについてはP. 19「スーパーバイザーとは」、ユーザーについてはP. 22「ユーザーとは」を参照してください。

★重要

- ハードディスクの故障や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。緊急で本機を使用する必要があるときに使用してください。

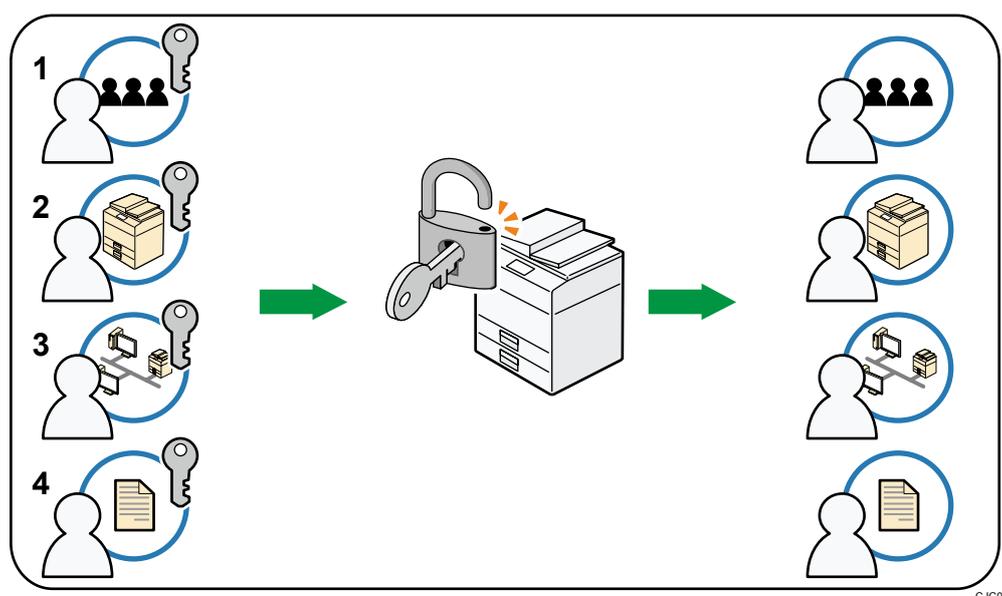
管理者認証を設定する

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、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。また、Windows 認証、LDAP 認証の対象とはならないため、ネットワーク環境で障害が起き、サーバーに接続できないときでもログインできます。

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. 12 「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、暗号パスワードです。暗号パスワードとは、SNMPv3 で暗号化するときのパスワードです。Network Monitor for Admin など SNMPv3 に対応したソフトウェアで使用します。管理者は機器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コピーやプリンター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。ユーザー認証の設定は、管理者認証を設定してから行ってください。ユーザー認証の設定の流れは P. 24 「ユーザー認証を設定する」を参照してください。

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

はじめに

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場合に削除したり、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。

2. 機器管理者

おもに機器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、機器を使用できなくすることを防止したり、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。ドキュメントボックスに蓄積した文書に、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、操作することで起こる情報漏洩や改ざんを防止できます。

★重要

- 管理者認証は、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。
- 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。

はじめて管理者としてログインするときは、工場出荷時のログインユーザー名、ログインパスワードでログインします。工場出荷時の、管理者のログインユーザー名は「admin」です。ログインパスワードは設定されていません。

管理者認証のログイン、ログアウトの方法は、P. 16「管理者のログイン方法」、P. 18「管理者のログアウト方法」を参照してください。

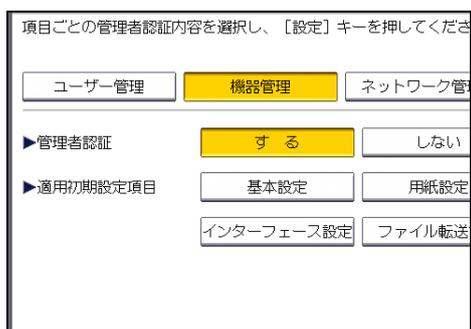
★重要

- 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. 19「スーパーバイザーとは」を参照してください。

はじめに

- 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場合は、サービス実施店に連絡し、工場出荷時の値に戻すこととなります。本機のデータや設定が失われますのでご了承ください。

1. [初期設定/カウンター] キーを押します。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [管理者認証管理] を押します。
6. [ユーザー管理]、[機器管理]、[ネットワーク管理]、[文書管理] のどれかを押して管理する項目を選択します。
7. 「管理者認証」で [する] を選択します。
8. 「適用初期設定項目」で管理する設定項目を選択します。



適用初期設定項目として選択した項目は、ユーザーによる設定ができなくなります。

適用初期設定項目は各管理者により異なります。

複数のカテゴリーに管理者認証を設定するときは、手順 6 から 8 を繰り返します。

9. [設定] を押します。
10. [初期設定/カウンター] キーを押します。

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ことで、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. 16「管理者のログイン方法」、P. 18「管理者のログアウト方法」を参照してください。

1. 操作部から管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。

はじめに

4. [▼次へ] を押します。
5. [管理者登録／変更] を押します。
6. 権限を設定する管理者の行の [管理者 1]、[管理者 2]、[管理者 3]、[管理者 4] のどれかを押して、[変更] を押します。

システム初期設定	
管理者登録／変更	
スルホ付	管理者 1 管理者 2 管理者 3
	<input type="button" value="変更"/> <input type="button" value="変更"/> <input type="button" value="変更"/> <input type="button" value="変更"/>
▶ユーザー管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶機器管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶ネットワーク管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶文書管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>

各管理者の権限を 1 人ずつに割り当てるときは下の図のように、1 カテゴリーに 1 人の管理者を選択します。

システム初期設定	
管理者登録／変更	
スルホ付	管理者 1 管理者 2 管理者 3
	<input type="button" value="変更"/> <input type="button" value="変更"/> <input type="button" value="変更"/> <input type="button" value="変更"/>
▶ユーザー管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶機器管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶ネットワーク管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>
▶文書管理者	<input type="button" value="管理者 1"/> <input type="button" value="管理者 2"/> <input type="button" value="管理者 3"/>

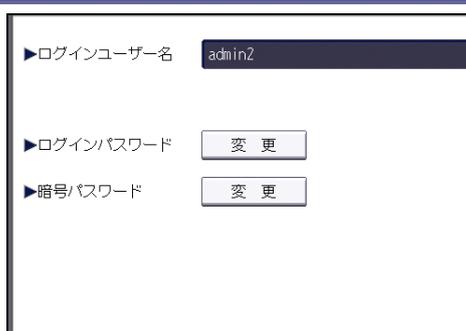
複数の管理者の権限をまとめるときは、1 人の管理者に複数の管理者を割り当てます。たとえば、機器管理者とユーザー管理者を [管理者 1] にまとめたいときは、機器管理者とユーザー管理者の行の [管理者 1] を押して、選択します。

7. 「ログインユーザー名」の [変更] を押します。

ログインユーザー名	
	<input type="button" value="終了"/>
	<input type="button" value="取消"/> <input type="button" value="設定"/>
	<input type="button" value="変更"/>

8. ログインユーザー名を入力し、[OK] を押します。
9. 「ログインパスワード」の [変更] を押します。

はじめに



10. ログインパスワードを入力し、[OK] を押します。

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. 230「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。

11. 確認のためにもう一度ログインパスワードを入力し、[OK] を押します。

12. 「暗号パスワード」の [変更] を押します。

13. 暗号パスワードを入力し、[OK] を押します。

14. 確認のためにもう一度暗号パスワードを入力し、[OK] を押します。

15. [設定] を 2 回押します。

自動的にログアウトされます。

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. 14「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。
- 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る必要があります。

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、以下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

はじめに

- 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るようになります。パスワードポリシーの設定方法は、P. 230「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。

Web Image Monitor を使用して管理者認証を設定する

Web Image Monitor を使用して本機にログインし、管理者認証の設定、変更ができます。管理者認証のログイン、ログアウトの方法は、P. 16「管理者のログイン方法」、P. 18「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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「機器」の [管理者認証管理] または、[管理者登録/変更] をクリックします。
4. 管理者認証の設定をします。
5. ログアウトします。

↓ 補足

- Web Image Monitor の詳細については Web Image Monitor のヘルプ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。

操作部からログインする

1. [初期設定/カウンター] キーを押します。
2. [ログイン/ログアウト] キーを押します。

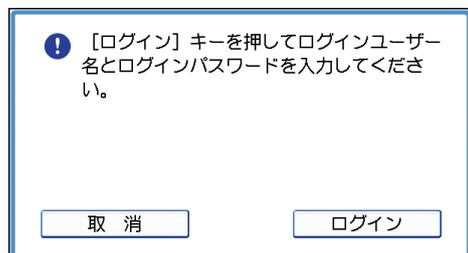


CJR004

初期設定画面の [ログイン] を押してもログイン画面に切り替わります。



3. [ログイン] を押します。



ログインしないときは、[取消] を押します。

4. 管理者のログインユーザー名を入力し、[OK] を押します。
工場出荷時は、管理者のログインユーザー名は「admin」、スーパーバイザーのログインユーザー名は「supervisor」です。

はじめに

5. 管理者のログインパスワードを入力し、[OK] を押します。

工場出荷時は、管理者とスーパーバイザーのパスワードは設定されていません。この場合は、パスワードを入力しないで、[OK] を押します。

「認証中です。しばらくおまちください。」というメッセージが表示され、初期設定の画面が表示されます。

↓ 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。
- 管理者権限でログインしたときは、ログインしている管理者名が表示されます。複数の管理者権限をもつログインユーザー名でログインしたときは、管理者権限をもついずれかの管理者名が表示されます。
- 各機能の操作画面でログインしたときは、「この機能を利用する権限はありません。管理者として設定変更はできます。」と表示されます。そのまま、[初期設定/カウンター] キーを押して、初期設定を変更します。

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場合、各セグメントの先頭につく「0」は入力しないでください。たとえば「192.168.001.010」の場合は、「192.168.1.10」と入力します。

「192.168.001.010」と入力すると、本機に接続できません。

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. 管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。

工場出荷時の、管理者のログインユーザー名は「admin」、スーパーバイザーは「supervisor」です。ログインパスワードは設定されていません。

↓ 補足

- 使用している Web ブラウザーの設定により、ログイン名、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名、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後に、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. [ログイン/ログアウト] キーを押します。
2. [ログアウトする] を押します。

 補足

- 次の方法でもログアウトできます。
 - ジョブが終了した後に [省エネ] キーを押す。

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。
- Web Image Monitor は 30 分間操作しないと、自動でログアウトされます。

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. 16「管理者のログイン方法」、P. 18「管理者のログアウト方法」を参照してください。

★重要

- 工場出荷時のログインユーザー名は「supervisor」です。ログインパスワードは設定されていません。ログインユーザー名とログインパスワードは変更することをお勧めします。
- 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. 14「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場合は、サービス実施店に連絡し、工場出荷時の値に戻すこととなります。本機のデータが失われますのでご了承ください。

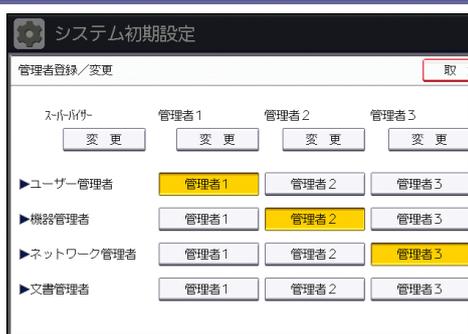
↓補足

- 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。
- Web Image Monitor からスーパーバイザーとしてログインし、管理者のパスワードを削除したり、新しく設定できます。

管理者のパスワードを再設定する

1. 操作部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. 16「管理者のログイン方法」を参照してください。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [管理者登録／変更] を押します。
6. 再設定する管理者の [変更] を押します。

はじめに



7. 「ログインパスワード」の[変更]を押します。



8. ログインパスワードを入力し、[OK] を押します。
9. 確認のためにもう一度ログインパスワードを入力し、[OK] を押します。
10. [設定] を 2 回押します。
自動的にログアウトされます。

補足

- 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. 11「管理者の権限を設定する」を参照してください。

1. 操作部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. 16「管理者のログイン方法」を参照してください。
2. [システム初期設定]を押します。
3. [管理者用設定]を押します。
4. [管理者登録/変更]を押します。
項目が表示されていない場合は、[▼次へ]を押します。
5. 「スーパーバイザー」の[変更]を押します。
6. 「ログインユーザー名」の[変更]を押します。
7. ログインユーザー名を入力し、[OK] を押します。

はじめに

8. 「ログインパスワード」の [変更] を押します。
9. ログインパスワードを入力し、[OK] を押します。
10. 確認のためにもう一度ログインパスワードを入力し、[OK] を押します。
11. [設定] を 2 回押します。
自動的にログアウトされます。

ユーザー認証を設定する

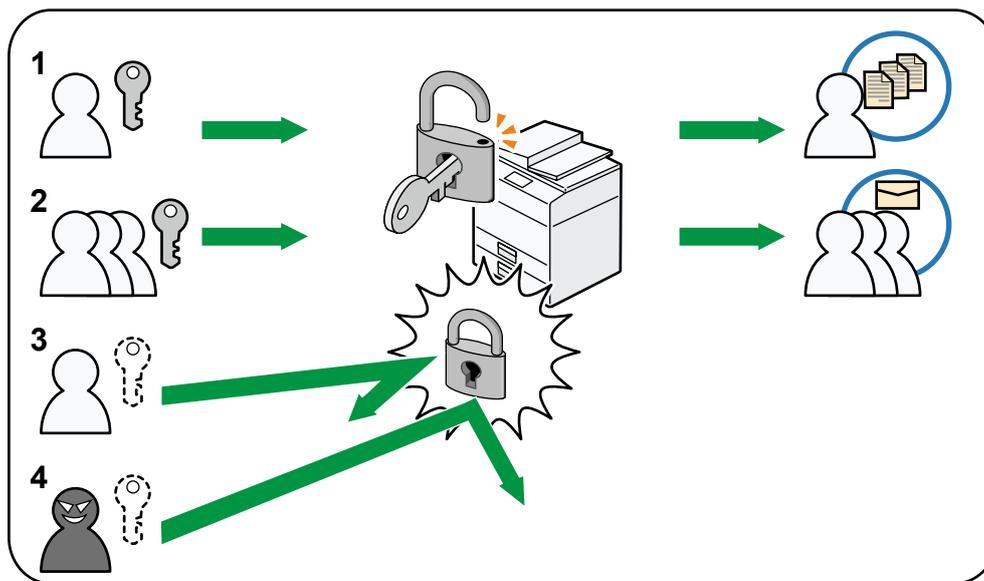
ユーザー認証の設定方法と、ユーザー認証によって有効になる機能について説明します。

ユーザーとは

ユーザーとは、文書のコピーやプリントなど、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機器の利用者として設定できます。アドレス帳へのユーザーの登録は、ユーザー管理者が行います。管理者については、P.9「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『ネットワークの接続/システム初期設定』「ユーザー情報の登録」、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
文書のコピーや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
文書のコピーや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 認証の 4 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

- ハードディスクの故障やネットワークのトラブルなどで、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。緊急で本機を使用する必要がある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. 11 「管理者の権限を設定する」 P. 12 「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">P. 26 「ユーザーコード認証」P. 28 「ベーシック認証」P. 32 「Windows 認証」P. 40 「LDAP 認証」

↓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 認証に切り替えた後でも、ログインユーザー名として引き継がれ使用できます。この場合、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。

ユーザー認証を設定する

- 外部の認証（Windows 認証、LDAP 認証）に切り替えた場合、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他の認証方式に切り替えたときは、セキュリティーの観点から、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。アカウントの削除方法は、『ネットワークの接続/システム初期設定』「ユーザーを消去する」、パスワードの設定方法は、P. 30「ログインユーザー名とログインパスワードを設定する」を参照してください。
- 同時に 2 つ以上の認証方法は設定できません。
- Windows 認証、LDAP 認証でユーザーのメールアドレスを取得できたときは、スキャナーのメール送信時、また受信ファクスのメール転送時に送信者（From）のアドレスが固定され、成りすましを防止できます。
- ユーザー認証は、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。
- 主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。
- 「統合サーバー認証」キーは使用できません。

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。

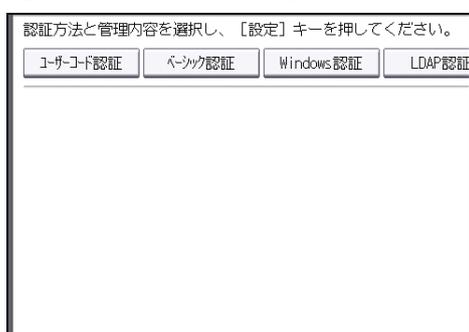
ユーザーコードの設定については『ネットワークの接続/システム初期設定』「ユーザーコードを登録する」を参照してください。

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』、またはプリンタードライバーのヘルプを参照してください。

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

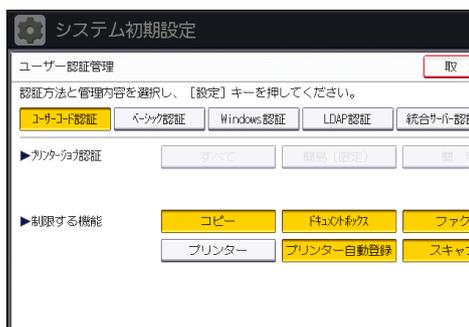
ユーザーコード認証を設定する

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [ユーザー認証管理] を押します。
6. [ユーザーコード認証] を選択します。



ユーザー認証管理を使用しないときは、[認証しない] を選択します。

7. 「制限する機能」で利用を制限する本機の機能を選択します。



選択した機能がユーザーコード認証の対象になります。選択していない機能はユーザー

ユーザー認証を設定する

コード認証をしません。

機能の利用制限については、P. 60「機能の利用を制限する」を参照してください。

プリンタージョブ認証を設定しないときは、手順 13 に進みます。

8. 「制限する機能」で [プリンター自動登録] の選択を外すか、[プリンター] を選択します。
9. 「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. 45「プリンタージョブ認証」を参照してください。
[簡易]、[すべて] を選択したときは、手順 13 へ進んでください。
[簡易 (限定)] を選択したときは、手順 10 へ進んでください。
10. 「限定対象」の [変更] を押します。
11. 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。

システム初期設定	
プリンタージョブ認証：限定対象	
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てください。	
▶IPv4アドレス1	0.0.0.0 - 0.0.0.0 変更
▶IPv4アドレス2	0.0.0.0 - 0.0.0.0 変更
▶IPv4アドレス3	0.0.0.0 - 0.0.0.0 変更
▶IPv4アドレス4	0.0.0.0 - 0.0.0.0 変更
▶IPv4アドレス5	0.0.0.0 - 0.0.0.0 変更
▶IPv6/ルーターフェース (簡易)	対象とする 対象としない
▶USB (簡易)	対象とする 対象としない

IPv4 アドレスの範囲、パラレル接続、USB 接続を設定できます。

12. [閉じる] を押します。
13. [設定] を押します。
14. [ログイン/ログアウト] キーを押します。

確認画面が表示されます。

[終了する] を押すと自動的にログアウトされます。

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、アドレス帳や蓄積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後に、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の設定をする必要があります。利用制限の設定については、P. 29「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

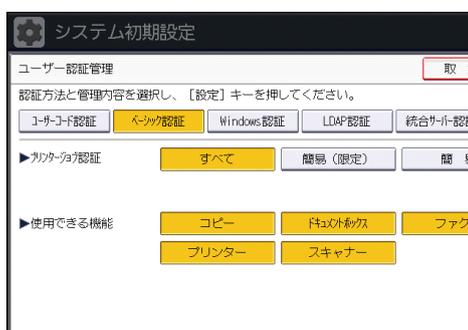
管理者認証が設定されていることを確認してから、設定してください。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [ユーザー認証管理] を押します。
6. [ベーシック認証] を選択します。



ユーザー認証管理を使用しないときは、[認証しない] を選択します。

7. 「プリンタージョブ認証」のレベルを選択します。



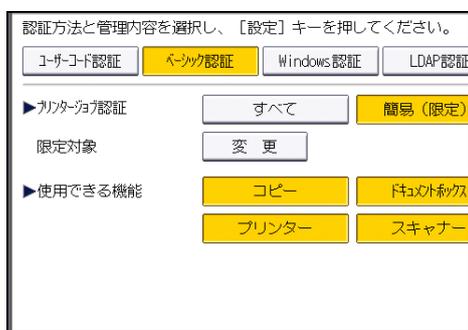
プリンタージョブ認証については、P. 45「プリンタージョブ認証」を参照してください。

[簡易]、[すべて] を選択したときは、手順 11 へ進みます。

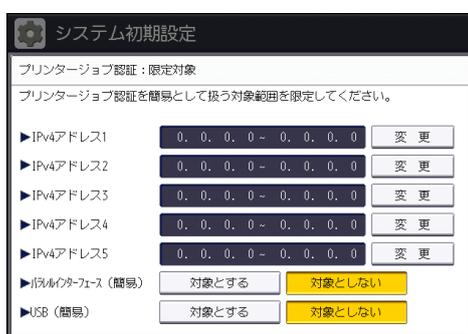
ユーザー認証を設定する

[簡易 (限定)] を選択したときは、手順 8 へ進みます。

8. 「限定対象」の[変更]を押します。



9. 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、パラレル接続、USB 接続を設定できます。

10. [閉じる]を押します。

11. 「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。

選択した機能がアドレス帳にユーザーを新規登録したときの、ベーシック認証の初期設定となります。

機能の利用制限については、P. 60「機能の利用を制限する」を参照してください。

12. [設定]を押します。

13. [ログイン/ログアウト] キーを押します。

確認画面が表示されます。

[終了する] を押すと自動的にログアウトされます。

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。機器の利用制限は、P. 60「機能の利用を制限する」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。事前にユーザーをアドレス帳に登録する必要があります。アドレス帳については、『ネットワークの接続/システム初期設定』『宛先・ユーザーを登録する』を参照してください。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。

ユーザー認証を設定する

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. 14「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. 操作部からユーザー管理者がログインします。
2. 「アドレス帳管理」を押します。
3. ユーザーを選択します。

【00001】 赤坂支店	【00002】 横浜事業所	【00003】 企画課	【00004】 ロサンゼルス支店	【00005】 営業課
【00007】 沼津ショールーム	【00008】 鹿児島事業所	【00010】 上海工場	【00011】 香港オフィス	【00009】 Folder01

4. 「認証情報」を押します。

名前: 赤坂支店 [変更]

キー表示名: 赤坂支店 [変更]

見出し選択

見出し1: 常用 AB CD EF GH IJK

見出し2: 常用 1 2 3 4 5

見出し3: 常用 1 2

5. 「ログインユーザー名」の「変更」を押します。
6. ログインユーザー名を入力し、「OK」を押します。
7. 「ログインパスワード」の「変更」を押します。
8. ログインパスワードを入力し、「OK」を押します。
9. 確認のためにもう一度ログインパスワードを入力し、「OK」を押します。
10. 「設定」を押します。
11. 「閉じる」を押します。
12. ログアウトします。

ログイン用認証情報を設定する

アドレス帳登録/変更/消去で設定したログインユーザー名とログインパスワードを、「SMTP 認証」、「フォルダー認証」、「LDAP 認証」の認証情報として使用します。
「SMTP 認証」、「フォルダー認証」、「LDAP 認証」で、別のログインユーザー名とログインパスワードを使用するときは『ネットワークの接続/システム初期設定』「共有フォルダーを登

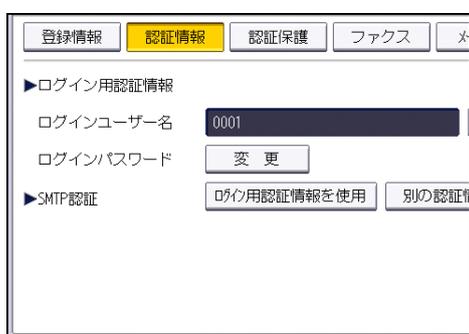
ユーザー認証を設定する

録する」「アドレス帳の認証情報」を参照してください。

★重要

- 「SMTP 認証」、「フォルダー認証」、「LDAP 認証」で [ログイン用認証情報を使用] を選択したときのユーザー名は、「other」、「admin」、「supervisor」および「HIDE***」以外の名前に設定されている必要があります。「***」は任意の文字列です。

1. 操作部からユーザー管理者がログインします。
2. [アドレス帳管理] を押します。
3. ユーザーを選択します。
4. [認証情報] を押します。
5. 「SMTP 認証」の [ログイン用認証情報を使用] を選択します。



フォルダー認証のときは、「フォルダー認証」の [ログイン用認証情報を使用] を選択します

LDAP 認証のときは、「LDAP 認証」の [ログイン用認証情報を使用] を選択します。

選択したい機能が表示されていないときは、[▼次へ] を押します。

6. [設定] を押します。
7. [閉じる] を押します。
8. 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。

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以下のとおりです。

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設置されている必要があります。
- 以下の OS が対応しています。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 を利用する場合は、TLSv1 または SSLv3 がサーバー上で動作することが必要です。
 - Windows Server 2003/2003 R2
 - Windows Server 2008/2008 R2

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設置されている必要があります。
- 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。以下の OS が対応しています。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 がサーバー上で動作することが必要です。
 - Windows Server 2003/2003 R2
 - Windows Server 2008/2008 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。

- 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. 158 「Kerberos 認証の暗号化設定」を参照してください。



ユーザー認証を設定する

- Windows 認証を設定しているときは、認証の際に、ディレクトリサーバーに登録されているユーザーのメールアドレスなどの情報が自動登録されます。ディレクトリサーバーのメールアドレスなどの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、メールアドレスなどは取得できません。
- Kerberos 認証を選択しているとき、SSL/TLS を設定していると、メールアドレスは取得できません。
- 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」を選択した場合は、先にコンピューター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。

↓ 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. 14「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。
- 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す。ユーザーごとに機能の制限をする場合は事前にアドレス帳を設定してください。
- 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 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上に存在しないユーザーでも認証できます。その際に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。
- 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 認証でファクス番号やメールアドレスなどの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。その場合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する必要があります。証明書の作成方法は、P. 38「サーバー証明書を作成する」を参照してください。
- Windows 認証でファクス番号やメールアドレスなどのユーザー情報を SSL/TLS による通信を利用しないで自動登録するとき、または自動登録を利用しないときは、証明書の作成は必要ありません。

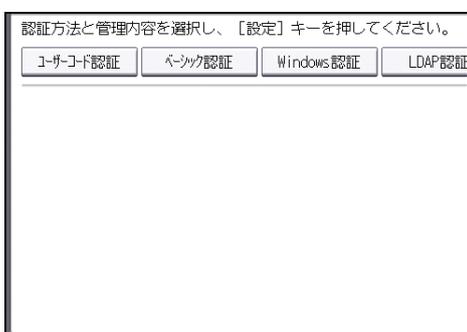
ユーザー認証を設定する

- 認証時にファクス情報取得に失敗するときは、P. 38「ファクス情報を取得できなかったとき」を参照してください。

Windows 認証を設定する

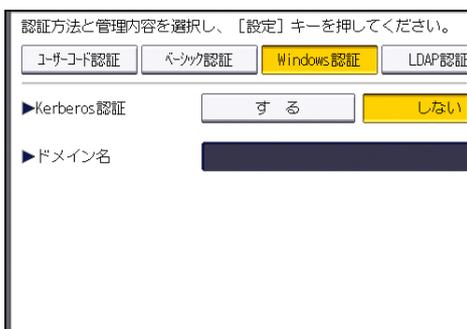
管理者認証が設定されていることを確認してから、設定してください。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [ユーザー認証管理] を押します。
6. [Windows 認証] を選択します。



ユーザー認証管理を使用しないときは、[認証しない] を選択します。

7. Kerberos 認証を使用する場合は「Kerberos 認証」の [する] を押します。



Kerberos 認証を使用しないときは、手順 9 へ進みます。

8. Kerberos 認証で使用するレルムを選択し、手順 10 へ進みます。



ユーザー認証を設定する

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、『ネットワークの接続/システム初期設定』「レルムを設定する」を参照してください。

レルムは5つまで登録できます。

9. 「ドメイン名」の [変更] を押し、認証を行うドメイン名を入力して [OK] を押し



10. [▼次へ] を押します。
11. 「プリンタージョブ認証」のレベルを選択します。

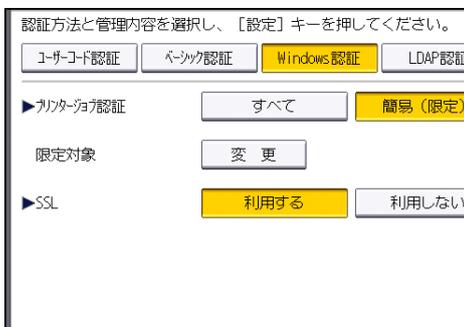


プリンタージョブ認証については、P. 45「プリンタージョブ認証」を参照してください。

[簡易]、[すべて] を選択したときは、手順 15 へ進みます。

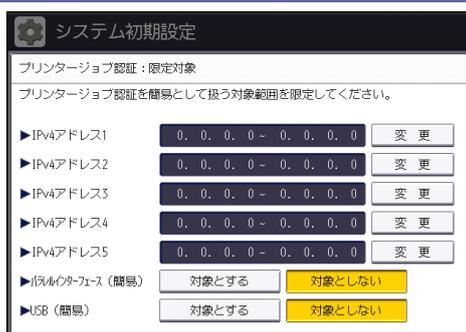
[簡易 (限定)] を選択したときは、手順 12 へ進みます。

12. 「限定対象」の [変更] を押します。



13. 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。

ユーザー認証を設定する



IPv4 アドレスの範囲、パラレル接続、USB 接続を設定できます。

14. 「閉じる」を押します。
15. 「SSL」の「利用する」を押します。

認証時に SSL を利用しないときは、「利用しない」を押します。

グローバルグループを登録していないときは、手順 22 へ進みます。

グローバルグループを登録しているときは、手順 17 へ進みます。

Windows サーバー上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を登録しておく必要があります。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を登録しておく必要があります。

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。初めて利用した場合、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可能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。

16. 「▼次へ」を押します。
17. 「グループ」の「登録／変更」を押し、「*未登録」を押します。



項目が表示されていないときは、「▼次へ」を押します。

18. 「グループ名」の「変更」を押します。
19. サーバー上で登録されているグループ名を入力し、「[OK]」を押します。
大文字、小文字は区別して入力してください。
20. 「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。

ユーザー認証を設定する

グループ名を入力し、利用する機能を選択してください。

▶グループ名	group1	
▶使用できる機能	<input type="checkbox"/> コピー	<input type="checkbox"/> ファクシ/紙おろし
	<input type="checkbox"/> プリンター	<input type="checkbox"/> スキャナー

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. 60「機能の利用を制限する」を参照してください。

21. [設定] を押します。
22. [設定] を押します。
23. [ログイン/ログアウト] キーを押します。

確認のメッセージが表示されます。

[終了する] を押すと、自動的にログアウトされます。

「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を設定します。

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。

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、[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。
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

ユーザー認証を設定する

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。

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以下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。

ファクス情報を取得できなかったとき

認証時にファクス情報の取得に失敗するときは、以下の設定を実施します。

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

1. コマンドプロンプトを開き、「regsvr32 schmmgmt.dll」を入力し [Enter] キーを押します。
2. [OK] をクリックし、コマンドプロンプトを閉じます。
3. [スタート] メニューから、[ファイル名を指定して実行...] をクリックします。

ユーザー認証を設定する

4. 「mmc」を入力し、[OK] をクリックします。
5. [ファイル] メニューから、[スナップインの追加と削除...] をクリックします。
6. [Active Directory スキーマ] を選択し、[追加>] をクリックします。
7. [OK] をクリックします。
8. 左枠の [Active Directory スキーマ] をクリックし、[属性] フォルダを開きます。
9. [facsimileTelephoneNumber] を右クリックし、[プロパティ] をクリックします。
10. [グローバルカタログにこの属性をレプリケートする] のチェックボックスをチェックし、[適用] をクリックします。
11. [OK] をクリックします。
12. [ファイル] メニューから [名前を付けて保存] をクリックします。
13. ファイル名とファイルを保存する場所を指定し、[保存] をクリックします。
14. コンソールダイアログボックスを閉じます。

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上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. 38「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サーバーの設定で行います。

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。

★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メールアドレスなどを本機で編集したときは、続く認証時の再取得により、メールアドレスなどが上書きさ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することはできません。
- 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対しては、参照機能の利用ができません。
- 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 認証の使用条件

LDAP 認証を設定するときは、以下の条件が必要です。

- 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 サーバー上で動作する
- 本機に LDAP サーバーが登録されており、以下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

ユーザー認証を設定する

- 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、『ネットワークの接続/システム初期設定』「LDAP サーバーを設定する」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. 14「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。
- 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 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したいときは、サービス実施店にお問い合わせください。
- LDAP 認証を使用する場合、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。
- 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可能になります。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 度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。
- 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する必要があります。レルムの登録方法は、『ネットワークの接続/システム初期設定』「レルムを設定する」を参照してください。
- 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. 158「Kerberos 認証の暗号化設定」を参照してください。

LDAP 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. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。

ユーザー認証を設定する

5. 「ユーザー認証管理」を押します。

6. 「LDAP 認証」を選択します。

ユーザー認証管理を使用しないときは、「認証しない」を選択してください。

7. 「認証 LDAP」で認証に使用する LDAP サーバーを選択します。

認証方法と管理内容を選択し、【設定】キーを押してください。

ユーザーコード認証 パスワード認証 Windows 認証 **LDAP 認証**

▶ 認証LDAP

1: ABCDSERVER	2: *
3: *未登録	4: *
5: *未登録	

SSL (暗号通信) 設定は、LDAPサーバー登録/変更画面にて変更し

▶ プリンタージョブ認証

すべて 簡易 (限定)

8. 「プリンタージョブ認証」のレベルを選択します。

システム初期設定

ユーザー認証管理

認証方法と管理内容を選択し、【設定】キーを押してください。

ユーザーコード認証 パスワード認証 Windows 認証 **LDAP 認証** 統合サーバ認証

▶ 認証LDAP

1: ABCDSERVER	2: *未登録
3: *未登録	4: *未登録
5: *未登録	

SSL (暗号通信) 設定は、LDAPサーバー登録/変更画面にて変更してください。

▶ プリンタージョブ認証

すべて 簡易 (限定) 簡易

プリンタージョブ認証については、P. 45「プリンタージョブ認証」を参照してください。

「簡易」、「すべて」を選択したときは、手順 12 へ進みます。

「簡易 (限定)」を選択したときは、手順 9 へ進みます。

9. 「限定対象」の「変更」を押します。

認証方法と管理内容を選択し、【設定】キーを押してください。

ユーザーコード認証 パスワード認証 Windows 認証 **LDAP 認証**

▶ 認証LDAP

1: ABCDSERVER	2: *
3: *未登録	4: *
5: *未登録	

SSL (暗号通信) 設定は、LDAPサーバー登録/変更画面にて変更し

▶ プリンタージョブ認証

すべて 簡易 (限定)

限定対象

変更

10. 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。

ユーザー認証を設定する

システム初期設定

プリンタージョブ認証：限定対象
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てください。

▶IPv4アドレス1 0.0.0.0 ~ 0.0.0.0 変更

▶IPv4アドレス2 0.0.0.0 ~ 0.0.0.0 変更

▶IPv4アドレス3 0.0.0.0 ~ 0.0.0.0 変更

▶IPv4アドレス4 0.0.0.0 ~ 0.0.0.0 変更

▶IPv4アドレス5 0.0.0.0 ~ 0.0.0.0 変更

▶iPrintのファクス (簡易) 対象とする 対象としない

▶USB (簡易) 対象とする 対象としない

IPv4 アドレスの範囲、パラレル接続、USB 接続を設定できます。

11. [閉じる] を押します。
12. [▼次へ] を押します。
13. 「ログイン名属性」の [変更] を押します。
14. ログイン名属性を入力し、[OK] を押します。

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成功となります。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成功となります。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。

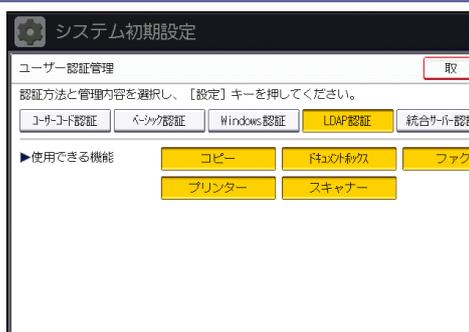
DN 形式で認証する場合は、ログイン名属性を登録する必要はありません。

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。

15. 「一意属性」の [変更] を押します。
16. 一意属性を入力し、[OK] を押します。

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ことで、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でも可能です。
17. [▼次へ] を押します。
18. 「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。

ユーザー認証を設定する



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。

機能の利用制限については、P. 60「機能の利用を制限する」を参照してください。

19. **【設定】**を押します。
20. **【ログイン/ログアウト】**キーを押します。

確認のメッセージが表示されます。

【終了する】を押すと、自動的にログアウトされます。

プリンタージョブ認証

プリンタージョブ認証とは、プリンターのジョブにユーザー認証をする機能です。ユーザー認証に対応しているプリンタードライバーはRPCS、RP-GL/2、PostScript 3です。PostScript 3はユーザーコード認証だけ対応しています。

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した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、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]

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、プリンターの印刷に対して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、想定外のユーザーから不正に使われてしまうことがあるので注意してください。

[簡易（限定）]

[簡易] の範囲を限定したいときに選択します。

[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。

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に対応している必要があります。

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組み合わせによっては、正しく印刷されない場合があります。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

ユーザー認証を設定する

1. 本機用の RPCS、RP-GL/2 プリンタードライバーの設定で、「印刷時に認証情報を確認する」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、「印刷時に認証情報を確認する」をチェックし、さらに「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、「印刷時に認証情報を確認する」をチェックしたとき
4. 本機用の RPCS、RP-GL/2 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、「印刷時に認証情報を確認する」をチェックしないとき
5. PostScript 3 プリンタードライバーでユーザーコードを入力したとき
他機種のユーザー認証に対応していない RPCS プリンタードライバーから、本機で代行印刷をした場合も同様です。
6. PostScript 3 プリンタードライバーでユーザーコードを入力しないとき
他機種のユーザー認証に対応していない RPCS プリンタードライバーから、本機で代行印刷をした場合も同様です。
7. RTIFF などのプリンタードライバーを使用しないプリンタージョブ、PDF を LPR 印刷したとき、Mail to Print のときです。Mail to Print については、『ファクス』「インターネットファクス/Mail to Print でメールを受信する」を参照してください。
8. PDF を ftp 印刷したときです。ftp でログインしたユーザーID とパスワードで個人認証されます。ただし、ユーザーID とパスワードは暗号化されません。

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

ユーザー認証を設定する

プリンタジョブ認証	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
プリンタジョブの種類 5	A	A	A	B	B	B
プリンタジョブの種類 6	A	A	A	X	X	X
プリンタジョブの種類 7	A	A	A	X	X	X
プリンタジョブの種類 8	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。

C：ユーザー認証が通り、プリンタ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。

X：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. 230「セキュリティー強化機能を設定する」を参照してください。

authfree コマンド

プリンタジョブ認証で [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 にログインする場合のユーザー名の初期値は「admin」です。パスワードは設定されていません。telnet のログイン方法、操作方法については、『ネットワークの接続/システム初期設定』「telnet を使う」を参照してください。

現在の設定の表示

```
msh> authfree
```

- プリンタジョブ認証が [簡易 (限定)] に設定されていないと表示できません。

IPv4 アドレスの設定

```
msh> authfree 対象 ID range アドレス 1 アドレス 2
```

IPv6 アドレスのレンジでの設定

```
msh> authfree 対象 ID range6 アドレス 1 アドレス 2
```

ユーザー認証を設定する

IPv6 アドレスのマスクでの設定

```
msh> authfree 対象 ID mask6 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。
- 「parallel」、「usb」のどちらかを必ず指定してください。
「parallel」はオプションの拡張 1284 ボード装着時に指定できます。

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。

アドレス帳の自動登録

Windows 認証、LDAP 認証の認証でログインしたユーザーは、個人情報がアドレス帳に自動登録されます。これ以外の情報は、別の登録済みユーザーからコピーするように設定できます。

自動登録されるアドレス帳の項目

- ログインユーザー名
- ログインパスワード
- 登録番号
- 名前*1
- キー表示名*1
- メールアドレス*2
- 文書保護 アクセス許可ユーザー/グループ*3

*1 情報を取得できないときはログインユーザー名が登録されます。

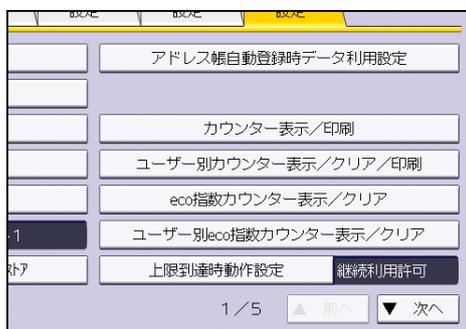
*2 情報を取得できないときは自動登録されません。

*3 [アドレス帳自動登録時データ利用設定] で [データを利用する] にしたときは、そちらが優先されます。

アドレス帳自動登録時データ利用設定

アドレス帳に自動登録されない情報を、すでに登録済みのユーザーからコピーして登録できます。

1. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [アドレス帳自動登録時データ利用設定] を押します。



5. [データを利用する] を押します。
6. 設定内容を利用するアドレス帳の登録番号をテンキーで入力し、[#] を押します。
7. [設定] を押します。
8. [ログイン/ログアウト] キーを押します。

ユーザー認証を設定する

確認のメッセージが表示されます。

[終了する] を押すと、自動的にログアウトされます。

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場合も認証失敗となり、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、機器を利用できなくなります。

ユーザー認証でロックアウト機能を使用するには、認証方法がベーシック認証に設定されている必要があります。他の認証選択時では、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

ロックアウト機能の設定は Web Image Monitor で行います。

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"> ▪ 有効 ▪ 無効 	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"> ▪ 有効 ▪ 無効 	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

ユーザー認証を設定する

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。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [ユーザーロックアウト] をクリックします。
4. 「ロックアウト」で [有効] を選択します。
5. 「ログインパスワード入力許容回数」でドロップダウンメニューから許容回数を選択します。
6. ロックアウト後、一定時間で解除したいときは「ロックアウト解除タイマー」で [有効] を選択します。
7. 「ロックアウト解除までの時間」に時間を分単位で入力します。
8. [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。
9. 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. [機器の管理] をポイントし、[アドレス帳] をクリックします。
3. ロックアウトを解除するユーザーを選択します。
4. [通常入力] をクリックし、[変更] をクリックします。
5. 「認証情報」の「ロックアウト」の [無効] にチェックを入れます。
6. [OK] をクリックします。
7. 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、主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

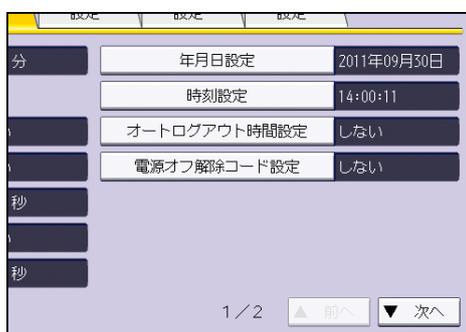
ユーザー認証を設定する

す。

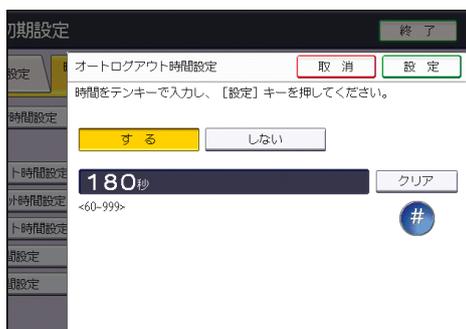
オートログアウト時間設定

ベーシック認証、Windows 認証、LDAP 認証のどれかを使用しているときに一定時間、画面の操作をしないと、自動的にログアウトします。これを「オートログアウト」といいます。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. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [時刻タイマー設定] を押します。
4. [オートログアウト時間設定] を押します。



5. [する] を選択します。
オートログアウトタイマー時間設定を設定しないときは、[しない] を選択します。
6. 「60～999」（1 秒単位）の範囲でテンキーで入力し、[#] を押します。



秒数を間違えたときは [クリア] を押して入力し直します。

7. [ログイン/ログアウト] キーを押します。
確認のメッセージが表示されます。
[終了する] を押すと、自動的にログアウトされます。

補足

- 紙づまりやトナー切れなどのときには、オートログアウトが働かないことがあります。
- Web Image Monitor のオートログアウト時間は 30 分で固定です。

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。

宛先表の利用を制限する

ファクス、スキャナー文書の送信先を、アドレス帳に登録された宛先だけに制限できます。また、送信先を直接入力できるときに、アドレス帳への登録を禁止できます。

宛先利用制限／個人宛先登録制限

ファクス機能と、スキャナー機能それぞれで宛先表の利用を制限できます。

宛先利用制限（ファクス）、宛先利用制限（スキャナー）

ファクスまたはスキャナーの送信先を、アドレス帳に登録された宛先だけに限定します。ユーザーが送信時に相手先のダイヤル番号やメールアドレス、フォルダー宛先を入力できなくなります。

個人宛先登録制限（ファクス）、個人宛先登録制限（スキャナー）

ファクスまたはスキャナーの送信時に直接入力した宛先を [宛先登録] でアドレス帳に登録することを禁止します。また、ユーザー管理者以外は、アドレス帳へのユーザーの新規登録や、登録済みユーザーのパスワードなどのユーザー情報の変更ができなくなります。個人宛先登録制限が設定されているときでも、宛先に登録されているユーザーは、パスワードを変更できます。パスワード以外の項目は、ユーザー管理者だけが変更できます。

1. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [セキュリティ強化] を押します。
6. [▼次へ] を押します。
7. 宛先利用制限と、個人宛先登録制限をファクスとスキャナーそれぞれで選択します。

機器の利用を制限する

機能を選択してください。

▶宛先利用制限 (ファクス)	▶受信指定先への転送
<input type="button" value="する"/> <input checked="" type="button" value="しない"/>	<input type="button" value="禁止する"/>
▶個人宛先登録制限 (ファクス)	
<input type="button" value="する"/> <input checked="" type="button" value="しない"/>	
▶宛先利用制限 (スキャナー)	▶実行中ジョブへの操作
<input type="button" value="する"/> <input checked="" type="button" value="しない"/>	<input type="button" value="ログイン権限"/>
▶個人宛先登録制限 (スキャナー)	<input checked="" type="button" value="しない"/>
<input type="button" value="する"/> <input checked="" type="button" value="しない"/>	

「宛先利用制限 (ファクス)」を [する] に設定すると、「個人宛先登録制限 (ファクス)」は表示されません。同様に、「宛先利用制限 (スキャナー)」を [する] に設定すると、「個人宛先登録制限 (スキャナー)」は表示されません。

8. **【設定】** を押します。
9. **【ログイン/ログアウト】** キーを押します。

確認のメッセージが表示されます。

[終了する] を押すと、自動的にログアウトされます。

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

各管理者の設定できる項目は、P. 274「設定項目の操作権限一覧」を参照してください。

管理者の登録方法は、P. 12「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。

管理者認証の適用初期設定項目で、変更を禁止する項目を選択します。

適用初期設定項目の選択については、P. 10「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

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. 10「管理者認証を設定する」を参照してください。

メニュープロテクトのレベルとユーザー権限の関係については、P. 274「設定項目の操作権限一覧」を参照してください。

メニュープロテクトを設定する

メニュープロテクトを有効にするには、[メニュープロテクト設定] を [レベル 1] か [レベル 2] に設定します。[レベル 2] のほうが制限が強くなります。

メニュープロテクトを無効にするには、[メニュープロテクト設定] を [しない] に設定します。

補足

- メニュープロテクトを [レベル 1] か [レベル 2] に設定した機能は、ユーザーによるプログラムの登録ができなくなります。

コピー機能

1. 操作部から機器管理者がログインします。
2. [コピー/ドキュメントボックス初期設定] を押します。
3. [管理者用設定] を押します。
4. [メニュープロテクト設定] を押します。
5. 設定するメニュープロテクトのレベルを選択し、[設定] を押します。
6. ログアウトします。

ファクス機能

1. 操作部から機器管理者がログインします。
2. [ファクス初期設定] を押します。
3. [導入設定] を押します。
4. [▼次へ] を押します。
5. [メニュープロテクト設定] を押します。
6. 設定するメニュープロテクトのレベルを選択し、[設定] を押します。
7. ログアウトします。

機器の利用を制限する

プリンター機能

1. 操作部から機器管理者がログインします。
2. [プリンター初期設定] を押します。
3. [調整／管理] を押します。
4. [メニュープロテクト] を押します。
5. 設定するメニュープロテクトのレベルを選択し、[設定] を押します。
6. ログアウトします。

スキャナー機能

1. 操作部から機器管理者がログインします。
2. [スキャナー初期設定] を押します。
3. [導入設定] を押します。
4. [メニュープロテクト設定] を押します。
5. 設定するメニュープロテクトのレベルを選択し、[設定] を押します。
6. ログアウトします。

機能の利用を制限する

本機の各種機能に対してユーザーのアクセス権を設定し、第三者による不正操作を防止できます。

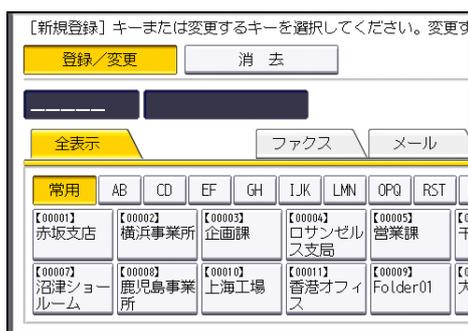
使用できる機能

コピー／ドキュメントボックス、プリンター、スキャナー、ファクス、ブラウザーで使用できる機能を設定します。

使用できる機能を設定する

アドレス帳に登録されたユーザーに対して、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。

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



4. [認証情報] を押します。

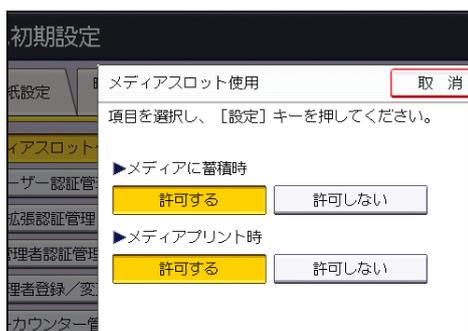


5. [▼次へ] を 2 回押します。
6. 「使用できる機能」で設定する機能を選択します。
7. [設定] を押します。
8. ログアウトします。

メディアスロットへのアクセスを制限する

メディアスロットの使用を許可するかしないか、操作部から設定します。この設定により、スキャナーで読み取った文書の外部メディア（USB メモリーか SD カード）への保存、および外部メディアに保存された文書の印刷を制限できます。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [メディアスロット使用] を押します。
6. 外部メディアへの文書の保存を制限するときは、「メディアに蓄積時」の [許可しない] を押します。



7. 外部メディアに保存された文書の印刷を制限するときは、「メディアプリント時」の [許可しない] を押します。
8. [設定] を押します。
9. ログアウトします。

↓ 補足

- 「メディアに蓄積時」で [許可しない] を選択すると、スキャナーの文書蓄積画面に [メディアに蓄積] は表示されません。
- 「メディアプリント時」で [許可しない] を選択すると、プリンターの初期画面に [メディアプリント] は表示されません。

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たり、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 になります。

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">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。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。継続利用許可 利用量を制限しません。	<ul style="list-style-type: none">ジョブ中断ジョブ終了後制限継続利用許可（工場出荷時の設定）

機器の利用を制限する

項目名	説明	設定値
印刷利用量制限度数設定	用紙サイズ、機能の組み合わせの4つの印刷条件ごとに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。 用紙サイズの「その他」は、A3または、DLT（11 × 17）以外の用紙サイズを表します。	<ul style="list-style-type: none">▪ コピー：A2▪ プリンター：A2▪ コピー：その他▪ プリンター：その他

利用量制限を設定したときの注意事項

以下の操作をした場合は、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場合

以下の場合は、利用量制限が適切にされません。

- Windows 認証、またはLDAP 認証時に、同一ユーザーとして複数のログイン名でログインし、別々のユーザーとしてアドレス帳に登録された場合

以下の場合は、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
- Mail to Print 機能を使用した印刷、ファクス機能を使用して本機に蓄積した文書、受信したファクス、およびPC FAX データの印刷

利用量制限を設定する

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [上限到達時動作設定] を押します。

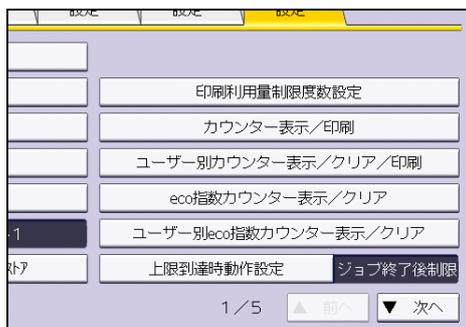


5. [ジョブ中断] または [ジョブ終了後制限] を選択し、[設定] を押します。

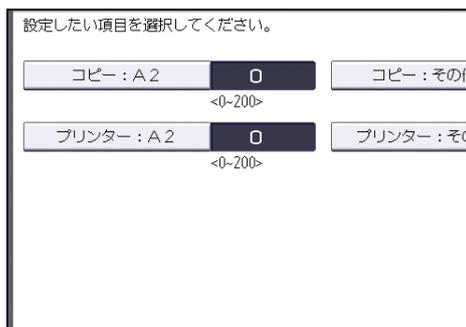
機器の利用を制限する

利用量の制限をしないときは、[継続利用許可] を選択してください。

6. [終了] を押します。
7. [システム初期設定] を押します。
8. [管理者用設定] を押します。
9. [印刷利用量制限度数設定] を押します。



10. 印刷条件を選択します。



11. テンキーを使って「0~200」の範囲で度数を入力し、[#] を押します。
0を設定すると、印刷の制限がされなくなります。
12. [設定] を押します。
13. ログアウトします。

補足

- 利用量の制限は、Web Image Monitor の [設定] の [印刷利用量制限] でも設定できます。

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、以下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場合は、自動登録を設定しないでください。
- ベーシック認証、Windows 認証、LDAP 認証が設定されているときは、画面左下にユーザーの利用上限度数と利用済みの度数が表示されますが、ユーザーコード認証では表示

機器の利用を制限する

されません。ユーザーコード認証有効時は、管理者がユーザーに利用度数を伝えてください。

- 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可能になることがあります。[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。

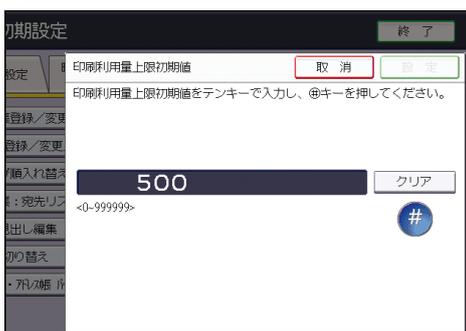
利用量上限の初期値を設定する

1. 操作部からユーザー管理者がログインします。
2. [システム初期設定]を押します。
3. [管理者用設定]を押します。
4. [▼次へ]を2回押します。
5. [印刷利用量上限初期値]を押します。



「上限到達時動作設定」で[継続利用許可]が選択されているときは、[印刷利用量上限初期値]は選択できません。

6. テンキーを使って「0~999,999」の範囲で度数を入力し、[#]を押します。



7. [設定]を押します。
8. ログアウトします。

ユーザーごとに利用量上限を設定する

1. 操作部からユーザー管理者がログインします。
2. [アドレス帳管理]を押します。

機器の利用を制限する

3. 利用量を設定するユーザーを選択します。

【新規登録】 キーまたは変更するキーを選択してください。変更する

登録/変更 消去

全表示 ファクス メール

常用	AB	CD	EF	GH	IJK	LMN	OPQ	RST
【00001】赤坂支店	【00002】横浜事業所	【00003】企画課	【00004】ロサンゼルス支局	【00005】営業課	【00006】	【00007】	【00008】	【00009】
【00007】沼津ショールーム	【00008】鹿児島事業所	【00010】上海工場	【00011】香港オフィス	【00009】Folder01	【00012】	【00013】	【00014】	【00015】

4. 「認証情報」を押します。

登録情報 認証情報 認証保護 ファクス メール

名前 赤坂支店 ▶ヨミカ
変更

キー表示名 赤坂支店 ▶登録番
変更

見出し選択

見出し1 常用 AB CD EF GH IJK

見出し2 常用 1 2 3 4 5

見出し3 常用 1 2

5. 「▼次へ」を2回押します。

6. 「印刷利用量制限」の「制限する」を選択し、「変更」を押します。

登録情報 認証情報 認証保護 ファクス メール

印刷利用量制限 制限する 制限しない

使用できる機能 コピー ファクス
プリンター スキャナー

「上限到達時動作設定」で「継続利用許可」が選択されているときは、「印刷利用量制限」は表示されません。

該当のユーザーの利用量制限をしないときは、「制限しない」を選択します。

7. テンキーを使って「0~999,999」の範囲で度数を入力し、「#」を押します。

認証情報 認証保護 ファクス メールアドレス フォルダ

制限する 制限しない

500 クリア #

コピー ファクス
プリンター スキャナー ブラウザー

機器の利用を制限する

ユーザーの上限度数を0に設定しても、印刷条件の度数が「0」の項目は印刷できます。

8. **【設定】**を押します。

9. **ログアウト**します。

補足

- 利用量の制限は、Web Image Monitor の [アドレス帳] でも設定できます。
- 操作部の [アドレス帳管理] の [検索] からユーザーを検索できます。
- ユーザーごとの上限度数は、500 件まで登録できます。

ユーザーの利用量を確認する

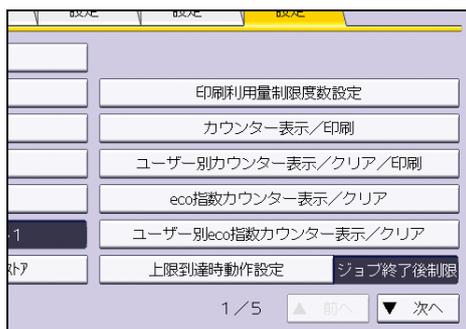
利用量はどの管理者でも確認できます。

1. **操作部から管理者がログイン**します。

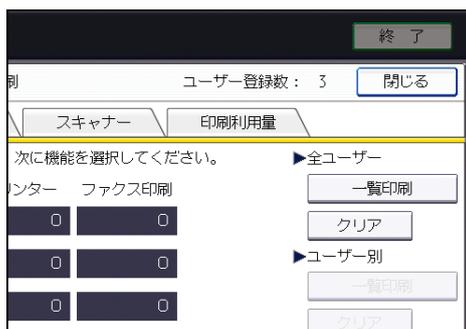
2. **【システム初期設定】**を押します。

3. **【管理者用設定】**を押します。

4. **【ユーザー別カウンター表示／クリア／印刷】**を押します。



5. **【印刷利用量】**を押します。



ユーザーごとの利用上限度数と、利用済みの度数が表示されます。

6. **確認が終了したらログアウト**します。

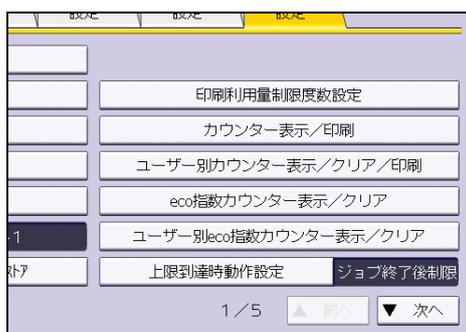
補足

- ユーザー管理者および認証済みユーザーは、Web Image Monitor の [アドレス帳] でも利用量を確認できます。

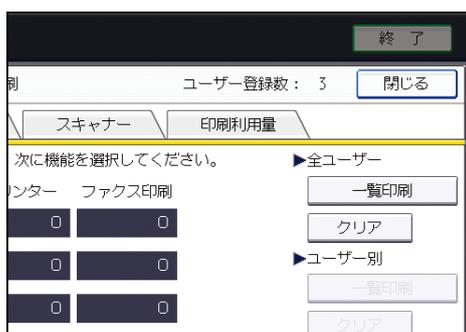
機器の利用を制限する

ユーザーの利用量カウンターを印刷する

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [ユーザー別カウンター表示/クリア/印刷] を押します。



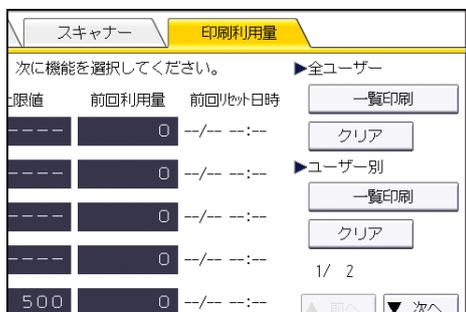
5. [印刷利用量] を押します。



ユーザーごとのカウンターが表示されます。

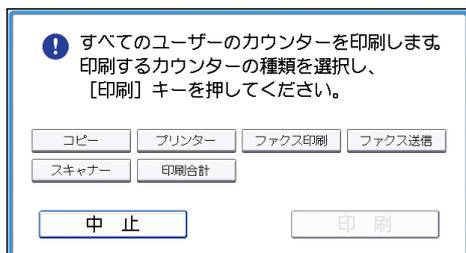
ページに表示されているユーザーをすべて選択するときは、[ページ内全選択] を押します。

6. ユーザーごとの利用量カウンターを印刷するときは、ユーザーを選択して「ユーザー別」の [一覧印刷] を押します。すべてのユーザーの利用量カウンターを印刷するときは、「全ユーザー」の [一覧印刷] を押します。



7. 印刷するカウンターを選択し、[印刷] を押します。

機器の利用を制限する



8. ログアウトします。



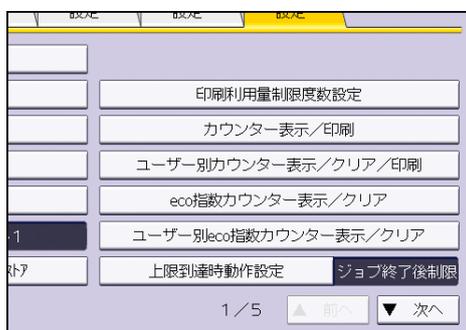
補足

- 利用量カウンターを印刷するときは、A4、 $8\frac{1}{2} \times 11$ 、B4、 $8\frac{1}{2} \times 14$ 、A3、または 11×17 のどれかのサイズの用紙を給紙トレイにセットしてください。

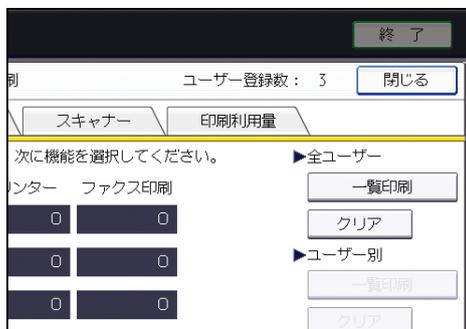
利用量カウンターをクリアする

利用量カウンターが上限に達した場合、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. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [ユーザー別カウンター表示/クリア/印刷] を押します。



5. [印刷利用量] を押します。



ユーザーごとのカウンターが表示されます。

6. ユーザーごとの利用量カウンターをクリアするときは、ユーザーを選択して「ユーザー別」の [クリア] を押します。すべてのユーザーの利用量カウンターをクリアする

機器の利用を制限する

ときは、「全ユーザー」の [クリア] を押します。

ページに表示されているユーザーをすべて選択するときは、[ページ内全選択] を押します。

7. [印刷利用量] を押し、[実行] を押します。

8. ログアウトします。

↓ 補足

- 個別のユーザーの利用量カウンターは、Web Image Monitor の [アドレス帳] でもクリアできます。すべてのユーザーの利用量カウンターを一括でクリアする場合は、操作部で行ってください。

自動リセット機能を設定する

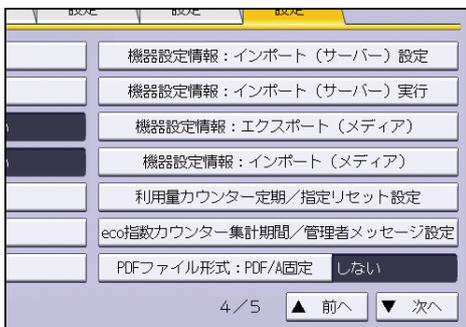
設定したタイミングで利用量カウンターをリセットできます。

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

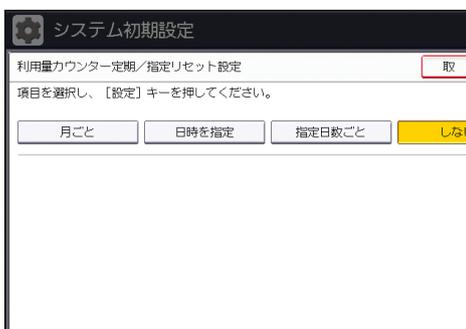
1. 操作部から機器管理者がログインします。

機器の利用を制限する

2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 3 回押します。
5. [利用量カウンター定期/指定リセット設定] を押します。



6. [月ごと]、[日時を指定]、[指定日数ごと] のどれかを選択します。



7. 条件を設定します。
8. [設定内容を反映] を押します。
9. [設定] を押します。
10. ログアウトします。

補足

- 指定した時間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 にリセットされます。

機器情報の漏洩を防止する

本機のメモリーや、ハードディスクに保存された情報を保護する方法を説明します。

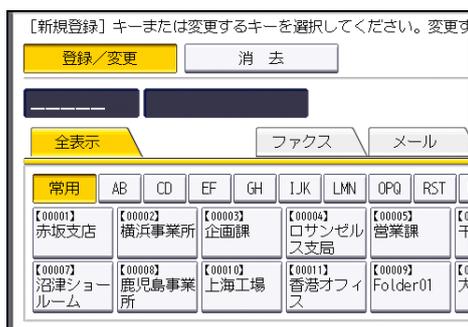
アドレス帳の登録情報を保護する

アドレス帳のデータに対して、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. 操作部からユーザー管理者がログインします。
2. [アドレス帳管理] を押します。
3. ユーザーを選択します。

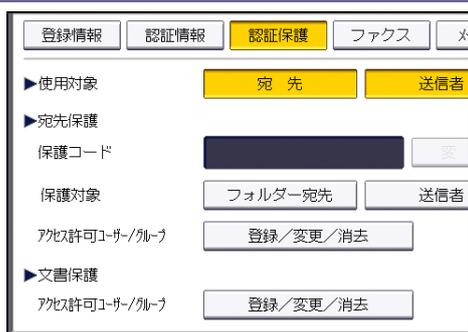


4. [認証保護] を押します。

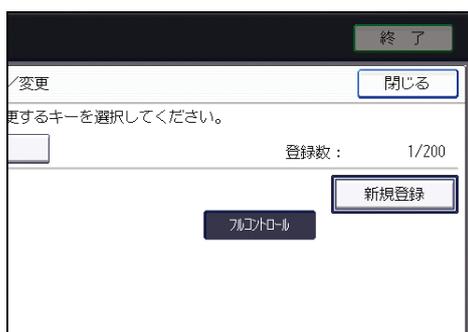


5. 「宛先保護」、「アクセス許可ユーザー/グループ」の [登録/変更/消去] を押します。

機器情報の漏洩を防止する



6. [新規登録] を押します。



7. 登録するユーザーまたはグループを選択します。

複数のユーザーを選択できます。

[すべてのユーザー] を押すと全ユーザーを選択できます。

8. [閉じる] を押します。

9. アクセス権を設定するユーザーを選択し、アクセス権を選択します。

アクセス権は、[閲覧]、[編集]、[編集/削除]、[フルコントロール] のどれかを選択します。

10. [閉じる] を押します。

11. [設定] を押します。

12. 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。

アドレス帳を暗号化する

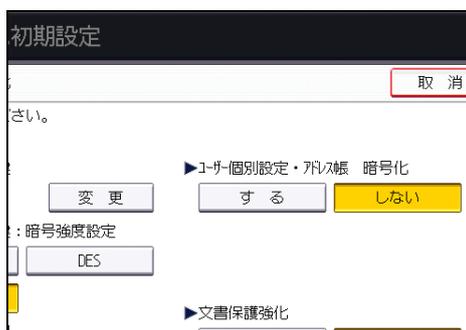
アドレス帳のデータを暗号化します。この設定により、アドレス帳データの読み取りを防止できます。

1. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。

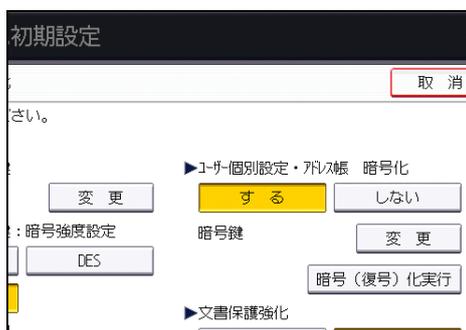
5. 「セキュリティ強化」を押します。



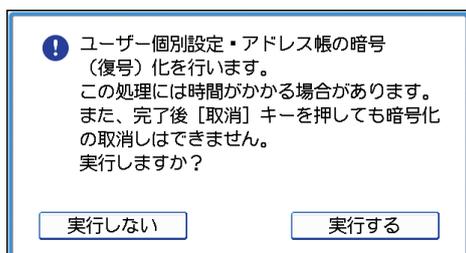
6. 「ユーザー個別設定・アドレス帳 暗号化」の「する」を押します。



7. 「暗号鍵」の「変更」を押します。



8. 暗号鍵を入力し、[OK] を押します。
暗号鍵は、半角英数字 32 文字以内で入力してください。
9. 「暗号（復号）化実行」を押します。
10. 「実行する」を押します。



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

機器情報の漏洩を防止する

アドレス帳の暗号化処理の実行は、時間がかかる場合があります。

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〕を押すと、データは暗号化されません。

復号化中に〔中止〕を押すと、データは暗号化されたままです。

暗号化が終了すると「アドレス帳暗号（復号）化を完了しました。〔確認〕キーを押してください。」が表示されます。

11. 〔確認〕を押します。

12. 〔設定〕を押します。

13. ログアウトします。

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 カードにバックアップされたアドレス帳は暗号化されています。SD カードにアドレス帳をバックアップ・リストアする方法は、『ネットワークの接続/システム初期設定』「管理者用設定」を参照してください。

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することもできます。

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体搭載メモリー、またはハードディスクに蓄積される以下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
- 蓄積文書データ
- 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

- 機器の故障時、機器の入れ替え時などに既存のデータを引き継ぐ場合、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。
- 使用できる外部メディアは SD カードです。ただし、すべての SD カードで動作を保証するものではありません。推奨する外部メディアについては販売店にご確認ください。
- 使用できる SD カードの容量は 32GB までです。

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]	<ul style="list-style-type: none"> ▪ アドレス帳 ▪ 登録したフォント ▪ ジョブログ/アクセスログ ▪ 蓄積した文書のサムネイル画像 ▪ 送受信メール ▪ Mail to Print で受信したファイル ▪ スプールされたジョブ 	<ul style="list-style-type: none"> ▪ 蓄積文書(ドキュメントボックス蓄積文書、機密印刷/試し印刷/保存印刷/保留印刷関連、ファクス蓄積受信文書) ▪ 登録したデータ(スタンプ、フォーム) 	1 時間程度
[全データ]	全データ： [ファイルシステムデータのみ] 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	4 時間程度
[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] 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際の注意事項

- [全データ初期化]、[ファイルシステムデータのみ]、[全データ] のどれを選択しても、機器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

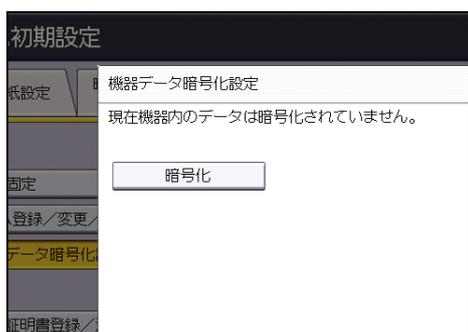
- 暗号化設定の実行時は本機の操作はできません。
- 暗号化設定を一度実行すると、途中で中止できません。また、暗号化設定の実行中に主電源が切られないよう必ず確認をしてください。実行中に電源が切られるとハ

機器情報の漏洩を防止する

ードディスクが破損しすべてのデータが使えなくなります。

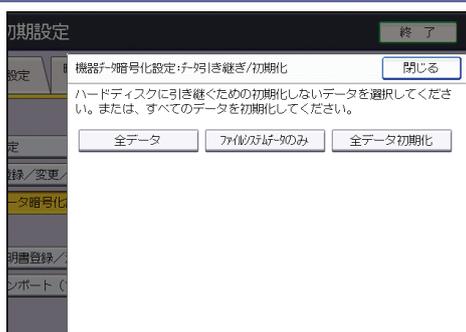
- 暗号鍵は、障害時のデータリカバリーなどに必要になります。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号化の設定は、操作部での設定手順を完了し、電源を一度切ってから再び入れて本機が再起動された後に有効になります。ハードディスク上書き消去機能と暗号化機能を同時に設定していると、ハードディスク上書き消去機能が実行された後、電源を切ってから再び入れた段階で暗号化が開始されます。
- ハードディスク上書き消去機能と暗号化機能を同時に設定すると、未暗号化状態から暗号化すると合わせて、ハードディスク上書き消去で乱数方式の3回書き込みを選択したときは、両機能が完了するまでに最大約8時間かかります。また、暗号化済み状態から再暗号化するときも、両機能が完了するまでに同じ時間がかかります。
- [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。アドレス帳やドキュメントボックスに保存されているデータなど、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。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を3回押します。
5. [機器データ暗号化設定] を押します。
6. [暗号化] を押します。



7. 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



すべてのデータを残すときは [全データ]、機器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] 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。

8. バックアップの方法を選択します。

[SD カードに保存] を選択したときは、操作部側面のメディアスロットに SD カードを挿入し、[実行] を押して機器データ暗号鍵のバックアップをします。

[紙に印刷] を選択したときは、[スタート] キーを押して機器データ暗号鍵を印刷します。

9. [実行] を押します。

10. [確認] を押します。

11. [終了] を押します。

12. ログアウトします。

13. 本機の主電源を切り、再度、主電源を入れます。

本機の主電源を入れると、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。主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主電源を切ってください。

電源の入れかた、切りかたは、『本機のご利用にあたって』『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。SD カードに保存するか、印刷するかのどちらかを選択します。

★重要

- 暗号鍵は、障害時のデータリカバリーなどに必要になります。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。

1. 操作部から機器管理者がログインします。

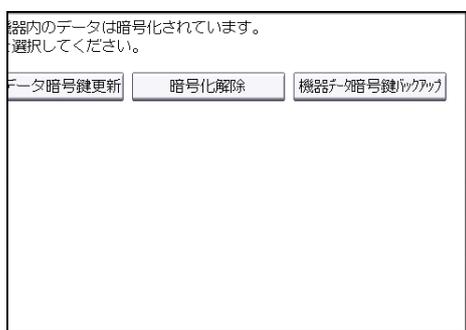
2. [システム初期設定] を押します。

3. [管理者用設定] を押します。

4. [▼次へ] を 3 回押します。

機器情報の漏洩を防止する

5. [機器データ暗号化設定] を押します。
6. [機器データ暗号鍵バックアップ] を押します。



7. バックアップの方法を選択します。
[SD カードに保存] を選択したときは、操作部側面のメディアスロットに SD カードを挿入し、[実行] を押して機器データ暗号鍵のバックアップ後に、[確認] を押します。
[紙に印刷] を選択したときは、[スタート] キーを押して機器データ暗号鍵を印刷します。
8. [閉じる] を押します。
9. ログアウトします。

暗号鍵を更新する

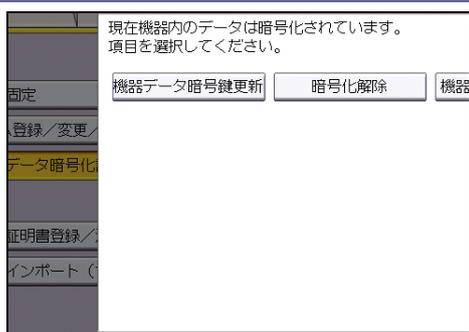
暗号鍵を新しいものに変更します。機器が正常に動作している状態で、機器データ暗号化が設定されているときに変更できます。

★重要

- 暗号鍵は、障害時のデータリカバリーなどに必要になります。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後に有効になります。ハードディスクに残すデータがあるときは、再起動に時間がかかります。
- 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。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 3 回押します。
5. [機器データ暗号化設定] を押します。
6. [機器データ暗号鍵更新] を押します。

機器情報の漏洩を防止する



7. 初期化しないで残すデータを選択します。

すべてのデータをハードディスクに残すときは [全データ]、機器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] 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。

8. 更新した暗号鍵のバックアップ方法を選択します。

[SD カードに保存] を選択したときは、操作部側面のメディアスロットに SD カードを挿入し、[実行] を押してバックアップをします。

[紙に印刷] を選択したときは、[スタート] キーを押して機器データ暗号鍵を印刷します。

9. [実行] を押します。

10. [確認] を押します。

11. [終了] を押します。

12. ログアウトします。

13. 本機の主電源を切り、再度、主電源を入れます。

本機の主電源を入れると、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。主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主電源を切ってください。

電源の入れかた、切りかたは、『本機のご利用にあたって』「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後に有効になります。ハードディスクに残すデータがあるときは、再起動に時間がかかります。
- 暗号化解除の設定で [全データ初期化] を選択しても、データはハードディスクから消去されません。機器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. 83 「ハードディスクのデータを上書き消去する」を参照し

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. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を3回押します。
5. [機器データ暗号化設定] を押します。
6. [暗号化解除] を押します。
7. 初期化しないで残すデータを選択します。

すべてのデータをハードディスクに残すときは [全データ]、機器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] 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。

8. [実行] を押します。
9. [確認] を押します。
10. [終了] を押します。
11. ログアウトします。
12. 本機の主電源を切り、再度、主電源を入れます。

電源の入れかた、切りかたは、『本機のご利用にあたって』「電源の入れかた、切りかた」を参照してください。

ハードディスクのデータを上書き消去する

本機に搭載されたハードディスクには、コピー、プリンター、ファクス、スキャナーのデータ、ユーザーによってドキュメントボックスに蓄積された文書、アドレス帳、ユーザーコード別カウンターを記録します。

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、ハードディスク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）することで、データの漏洩を防止できます。

使用環境

- 本体が正常な状態（壊れていたり、改造されたり、本体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えるように対応がとれる担当者によって管理されている。

補足

- 当社および当社の関連会社が派遣するカスタマーエンジニアは、本製品を扱うために教育されています。

使用上のご注意

メモリー自動消去、メモリー全消去の設定は、機器管理者が行ってください。

- 本機の主電源スイッチを切るときは、必ず上書き消去アイコンが「残存データ無し」表示に変わっていることを確認し、残存データがない状態で行ってください。
- 上書き消去中に低電力モードに移行して画面が暗くなっているときは、いったん画面を表示させ上書き消去アイコンを確認してください。
- 上書き消去中は、[オートオフ時間設定]を設定していても、オフモード（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が「残存データ有り」と表示されるときは、本機の主電源スイッチをいったん切ってください。再び主電源スイッチを入れて、アイコンが「残存データ無し」表示に変わったかどうかを確認してください。それでも表示が変わらなかったときはサービス実施店に連絡してください。

メモリー自動消去設定

コピー、スキャナーで原稿を読み取ったとき、あるいはPCから本機に出力されたデータは、ハードディスクに一時的に保存されます。メモリー自動消去設定を使用すると、これらのハ

機器情報の漏洩を防止する

ハードディスク内のデータを自動的に上書き消去できます。

上書き消去は、ジョブごとに自動的に行われます。

コピー、ファクス、プリンターの動作が優先され、上書き処理はこれらのジョブが終わった後に開始されます。

上書き消去アイコン

メモリー自動消去が設定されているとき、操作部の画面右下に状態を示すアイコンが表示されます。



アイコン	アイコン名	説明
	残存データ有り表示	残存データがハードディスクに残っているときに点灯します。 残存データの上書き動作中は点滅します。
	残存データ無し表示	残存データがなくなると点灯します。

★重要

- 保留印刷／保存印刷／機密印刷／試し印刷のデータがハードディスク内に残っている状態でも、上書き消去アイコンは「残存データ無し」と表示されます。

↓補足

- 上書き消去アイコンが画面に表示されないときは、メモリー自動消去設定が「しない」になっていないか確認してください。メモリー自動消去設定が「する」になっていてもアイコンが表示されないときは、サービス実施店に連絡してください。

消去方式

消去方式は次の中から選択できます。

機器情報の漏洩を防止する

NSA*1 方式

データを乱数 2 回、ゼロ 1 回で上書きします。

DoD*2 方式

データを固定値、固定値の補数、乱数で上書きし、検証処理を行います。

乱数方式

データを指定された回数の乱数で上書きします。乱数の書き込み回数は 1~9 回まで選択できます。

*1 National Security Agency (米) 国家安全保障局

*2 Department of Defense (米) 国防総省

補足

- 工場出荷時は「乱数方式」で、書き込み回数は 3 回に設定されています。

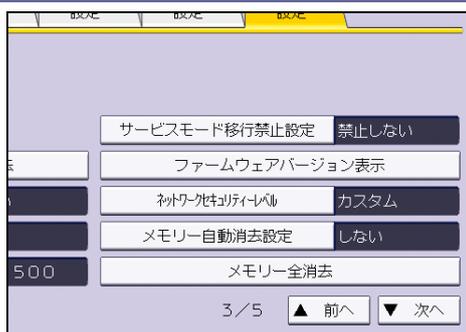
メモリー自動消去を設定する

重要

- メモリー自動消去設定を「しない」に設定されていたときのハードディスク使用領域は、メモリー自動消去設定を「する」に設定した後も残存データが上書きされないことがあります。
- メモリー自動消去が完了する前に主電源スイッチを切ると、上書き消去は一時中断され、データはハードディスク内に残ったままとなります。途中で中止はできません。また、ハードディスクが壊れることがあるので、上書き処理中に主電源を切られないように必ず確認してください。
- 万一、メモリー自動消去が完了する前に主電源スイッチを切った場合は、主電源スイッチを再び入れたときに、メモリー自動消去を続きから行います。
- 上書き消去中にエラーが発生したときは、主電源スイッチを一度切ってください。再び主電源スイッチを入れて、手順をやり直してください。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 2 回押します。
5. [メモリー自動消去設定] を押します。

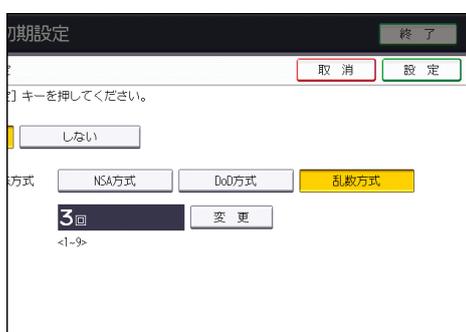
機器情報の漏洩を防止する



6. **【する】**を押します。

7. **消去方式を選択**します。

消去方式は、**【NSA方式】**、**【DoD方式】**、**【乱数方式】**のどれかを選択します。



【NSA方式】、**【DoD方式】**を選択した場合は、手順10へ進みます。**【乱数方式】**を設定する場合は手順8へ進みます。

8. **【変更】**を押します。

9. テンキーで消去の回数を入力し、**【#】**を押します。

10. **【設定】**を押します。

11. **ログアウト**します。

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

1. 「メモリー自動消去設定を使用する」の手順1~5と同様に操作します。

2. **【しない】**を押します。

3. **【設定】**を押します。

4. **【終了】**を押します。

5. **ログアウト**します。

補足

- メモリー自動消去設定を再度実行するときは、「メモリー自動消去設定を使用する」の手順をやり直してください。

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以下のとおりです。

上書き消去できるデータ

- コピー
 - コピーのデータ
- プリンター
 - 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、出力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
 - RTIFF エミュレーションの印刷データ
- ファクス
 - PC ファクスの印刷データ
本機で直接ファクス送受信したデータや登録されているファクス番号は、ハードディスクを使用していないため上書き消去の対象となりません。
- スキャナー
 - メール送信
 - フォルダ送信
 - ネットワーク TWAIN スキャナー
ネットワーク TWAIN スキャナーは、ハードディスクを使用していないため上書き消去の対象となりません。ただし、TWAIN ドライバーの先読みモードにチェックをつけてスキャンしたデータは、ハードディスクに蓄積されるので上書き消去の対象になります。

上書き消去できないデータ

- ユーザーによってドキュメントボックスに蓄積された文書
ドキュメントボックスに蓄積された文書は、ドキュメントボックスから削除されてはじめて上書き消去の対象となります。
- 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. 73「アドレス帳を暗号化する」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、ハードディスクに蓄積されているすべてのデータを一括して上書き消去できます。

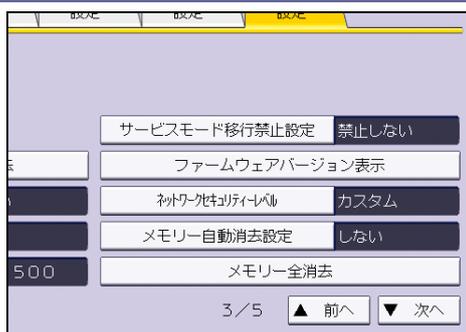
★重要

- 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、ユーザースタンプ、ユーザーがダウンロードしたプリンターフォント、SSL 機器証明書、および複合機本体のネットワーク設定もメモリー全消去の対象です。メモリー全消去後に使用する場合はサービス実施店に相談してください。
- メモリー全消去が完了する前に主電源スイッチを切ると、上書き消去は一時中断され、データはハードディスク内に残ったままとなります。途中で中止はできません。また、ハードディスクが壊れることがあるので、上書き処理中に主電源を切られないように必ず確認してください。
- メモリー全消去をする前に、Network Monitor for Admin を利用して、ユーザーコード、ユーザーコード別カウンター、アドレス帳のデータをバックアップすることをお勧めします。アドレス帳のバックアップは Web Image Monitor でもできます。詳細は、Network Monitor for Admin または Web Image Monitor のヘルプを参照してください。
- 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 回に設定した場合、最大約 4 時間かかります。
- 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、機器の管理やユーザーの管理が行われません。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

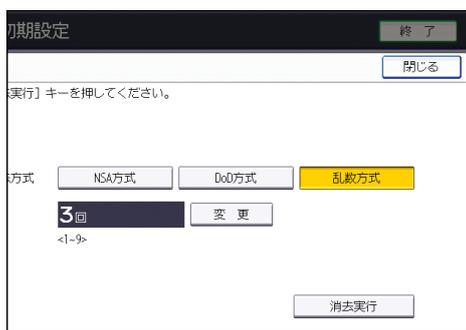
1. 本機に接続されているケーブルをすべて取り外します。
2. 操作部から機器管理者がログインします。
3. [システム初期設定] を押します。
4. [管理者用設定] を押します。
5. [▼次へ] を 2 回押します。
6. [メモリー全消去] を押します。

機器情報の漏洩を防止する



7. 消去方式を選択します。

消去方式は、[NSA方式]、[DoD方式]、[乱数方式] のどれかを選択します。



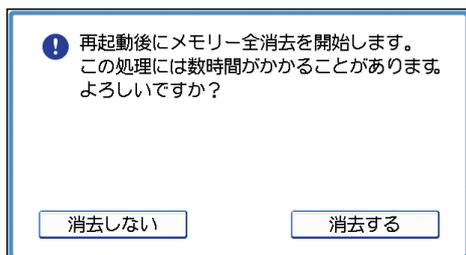
[NSA方式]、[DoD方式] を選択した場合は、手順 10 へ進みます。[乱数方式] を設定するときは手順 8 へ進みます。

8. [変更] を押します。

9. テンキーで消去の回数を入力し、[#] を押します。

10. [消去実行] を押します。

11. [消去する] を押します。



本機が自動的に再起動し、メモリ全消去を開始します。

12. メモリー全消去が完了したら [確認] を押して主電源を切ります。

電源の切りかたは、『本機のご利用にあたって』「電源の入れかた、切りかた」を参照してください。

↓ 補足

- 万一、メモリ全消去が完了する前に主電源スイッチを切った場合は、主電源スイッチを再び入れたときに、メモリ全消去を最初から行います。
- メモリー全消去中にエラーが発生したときは、主電源スイッチを一度切り、再び主

機器情報の漏洩を防止する

電源スイッチを入れて、手順 2 から行ってください。

メモリー全消去を一時停止する

★重要

- **メモリー全消去は中止できません。**

1. メモリー全消去処理中に [一時停止] を押します。
2. [一時停止する] を押します。
メモリー全消去は一時停止されます。
3. 主電源を切ります。

↓補足

- 主電源スイッチを再び入れるとメモリー全消去が再開されます。

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対して、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、アクセス可能な PC の IP アドレスは、192.168.15.16~192.168.15.20 になります。

★重要

- アクセスコントロールは LPR、RCP/RSH、FTP、SSH/SFTP、Bonjour、SMB、WSD (Device)、WSD (Printer)、IPP、DIPRINT、Web Image Monitor からの利用を制限できます。Network Monitor for Client の監視機能は制限できません。
- 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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [アクセスコントロール] をクリックします。
4. IPv4 アドレスで設定するときは、本機にアクセスを許可する IP アドレスの数値を「アクセスコントロール範囲」に入力します。
IPv6 アドレスで設定するときは、本機にアクセスを許可する IP アドレスの数値を「アクセスコントロール範囲」の「範囲指定」に入力するか、本機にアクセスを許可する IP アドレスの数値を「マスク指定」に入力し、「マスク長」を入力します。
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。
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。
7. 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、Network Monitor for Admin 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。Network Monitor for Admin から設定するときは、Web Image Monitor が起動します。

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"> ▪ 操作部 ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<p>IPv4 上で動作するすべてのアプリケーションが使用できなくなります。</p> <p>IPv4 通信しているときに Web Image Monitor で IPv4 を無効化することはできません。</p>
IPv6	-	<ul style="list-style-type: none"> ▪ 操作部 ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<p>IPv6 上で動作するすべてのアプリケーションが使用できなくなります。</p>
IPsec	-	<ul style="list-style-type: none"> ▪ 操作部 ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<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"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<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することもできます。</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
ssh/sftp	TCP:22	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<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することもできます。</p>
telnet	TCP:23	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ Network Monitor for Admin 	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"> ▪ 操作部 ▪ Web Image Monitor ▪ Network Monitor for Admin 	インターネットファクスおよびメール通知機能の SMTP 受信が使用できなくなります。
HTTP	TCP:80	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<p>HTTP の機能が使用できなくなります。</p> <p>IPP による 80 ポートでの印刷ができなくなります。</p>
HTTPS	TCP:443	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	<p>HTTPS の機能が使用できなくなります。</p> <p>尚、操作部、Web Image Monitor からの設定で SSL 通信だけを許可し、非 SSL 通信を禁止することもできます。</p>
SMB	TCP:139	<ul style="list-style-type: none"> ▪ 操作部 ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	SMB の機能が使用できなくなります。

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
NBT	UDP:137 UDP:138	<ul style="list-style-type: none"> ▪ telnet 	TCP/IP 経由での SMB 印刷の機能、および WINS サーバーによる NetBIOS 名解決機能が使用できなくなります。
SNMPv1/v2	UDP:161	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	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、参照は許可することもできます。
SNMPv3	UDP:161	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	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 暗号通信は禁止することもできます。
RSH/RCP	TCP:514	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	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することもできます。
LPR	TCP:515	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	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することもできます。

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
IPP	TCP:631	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	IPP の機能が使用できなくなります。
IP-ファクス	TCP:1720 (H. 323) UDP:1719 (Gatekeeper) TCP/UDP:5060 (SIP) TCP:5000 (H. 245) UPD5004, 5005 (Voice) TCP/UDP:49152 (T. 38)	<ul style="list-style-type: none"> ▪ 操作部 ▪ Web Image Monitor ▪ Network Monitor for Admin 	IP-ファクス接続の H. 323/SIP/T. 38 接続機能が使用できなくなります。
SSDP	UDP:1900	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	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"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	Bonjour の機能が使用できなくなります。
DIPRINT	TCP:9100	<ul style="list-style-type: none"> ▪ Web Image Monitor ▪ telnet ▪ Network Monitor for Admin 	DIPRINT の機能が使用できなくなります。
RFU	TCP:10021	<ul style="list-style-type: none"> ▪ 操作部 ▪ telnet 	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
AppleTalk	(PAP)	<ul style="list-style-type: none">操作部Web Image MonitortelnetNetwork Monitor for Admin	AppleTalk 印刷が使用できなくなります。
WSD (Device)	TCP:53000 (可変)	<ul style="list-style-type: none">Web Image MonitortelnetNetwork Monitor for Admin	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">Web Image MonitortelnetNetwork Monitor for Admin	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">telnet	WSD (Device/Printer)の機器検索ができなくなります。
LLTD	-	<ul style="list-style-type: none">telnet	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">Web Image Monitortelnet	LLMNRによる名前解決要求に応答できなくなります。

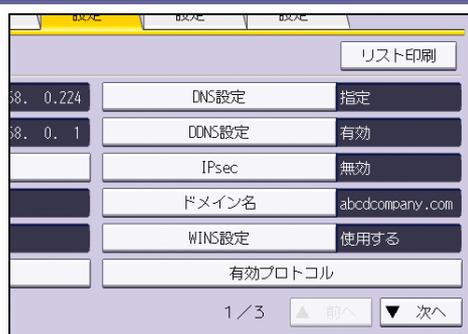
補足

- 「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.230「セキュリティ強化機能を設定する」を参照してください。

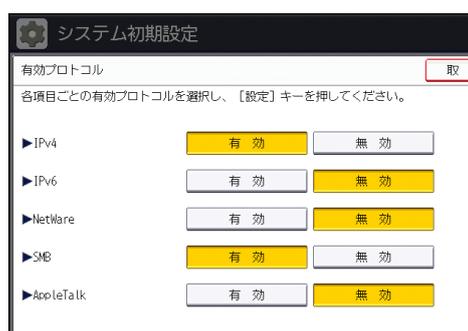
操作部から設定する

1. 操作部からネットワーク管理者がログインします。
2. [システム初期設定] を押します。
3. [インターフェース設定] を押します。
4. [ネットワーク] の [有効プロトコル] を押します。

ネットワークセキュリティを強化する



5. 設定するプロトコルの有効/無効を選択します。



6. [設定] を押します。
7. ログアウトします。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [ネットワークセキュリティ] をクリックします。
4. 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。
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。

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

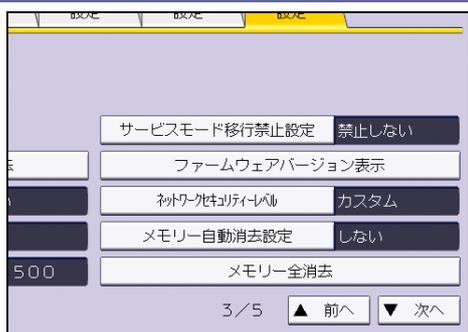
- ネットワークセキュリティレベルによっては一部のユーティリティにおいて通信ができない、またはログインに失敗する場合があります。

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。

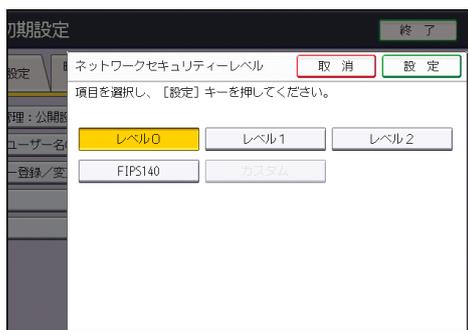
操作部から設定する

1. 操作部からネットワーク管理者がログインします。
2. [システム初期設定]を押します。
3. [管理者用設定]を押します。
4. [▼次へ]を2回押します。
5. [ネットワークセキュリティレベル]を押します。

ネットワークセキュリティーを強化する



6. ネットワークのセキュリティーレベルを選択します。



レベル 0、レベル 1、レベル 2、FIPS140 のどれかを選択します。

7. [設定] を押します。
8. ログアウトします。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [ネットワークセキュリティー] をクリックします。
4. 「セキュリティーレベル」で設定するレベルを選択します。
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。

各機能とネットワークセキュリティーレベルの関係

- =使用可能です。
- =使用不可です。
- ▲=ポートが開いています。
- =ポートが閉じています。

ネットワークセキュリティを強化する

☆=暗号化/平文

★=必ず暗号

×=暗号文優先

TCP/IP*1

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	×	×	★	★
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	○	○	○	○

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
RSH/RCP	○	○	-	-
TELNET	○	-	-	-
Bonjour	○	○	-	-
SSDP	○	○	-	-
SMB	○	○	-	-
NetBIOS over TCP/IPv4	○	○	-	-
WSD (Device)	○	○	○	○
WSD (Printer)	○	○	○	○
WSD (機器の暗号化通信)	-	-	○	○

AppleTalk*3

機能	レベル 0	レベル 1	FIPS 140	レベル 2
AppleTalk	○	○	-	-

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	☆	☆	★	★

*1 IPv4、IPv6 共通です。

ネットワークセキュリティを強化する

*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。

*3 AppleTalk、および PS3 カードのどちらかが搭載されていない場合、○であっても利用できません。

TCP/IP 暗号強度設定

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
S/MIME > 暗号化アルゴリズム	3DES-168 ビット	3DES-168 ビット	3DES-168 ビット	AES-256 ビット

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
S/MIME > ダイジェスト アルゴリズム	SHA1	SHA1	SHA1	SHA-256 ビット
SNMP v3 > 認証 アルゴリズム	MD5	SHA1	SHA1	SHA1

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
SNMP v3 > 暗号化アルゴリズム	DES	DES	AES128	AES128
Keyserver os 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

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
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、S/MIME、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、導入する必要があります。

機器証明書には、以下の 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

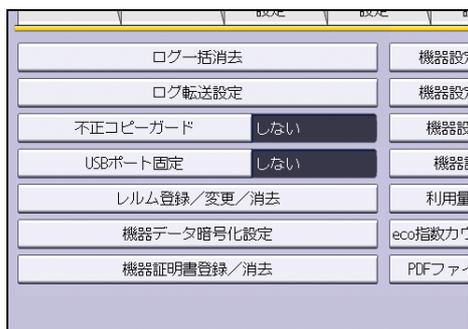
- 管理者の方は、証明書の期限を管理し、期限が切れる前に証明書の更新を行ってください。
- 管理者の方は、証明書の発行元が適切であることを確認してください。
- 機器証明書の署名アルゴリズムに SHA256、SHA512 を設定した場合、Internet Explorer 6.0 で接続するには、Windows XP SP3 以降が必要です。

操作部から機器証明書を作成、導入する（自己証明書）

本機の操作部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. 操作部からネットワーク管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 3 回押します。
5. [機器証明書登録／消去] を押します。



6. [登録] が選択されていることを確認します。
7. [証明書 1] を押します。

操作部では [証明書 1] だけを作成できます。

8. 必要な設定項目を入力します。

S/MIME、デジタル署名 PDF、デジタル署名 PDF/A に使用するときは、メールアドレスの

ネットワークセキュリティーを強化する

項目に本機の管理者メールアドレスを設定します。

9. [設定] を押します。

「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。

10. ログアウトします。



- 機器証明書を削除するときは、[消去] を選択します。
- 操作部で作成した機器証明書を、S/MIME やデジタル署名 PDF/A などを使用するときは、Web Image Monitor の“利用する証明書”で [証明書 1] を選択します。

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. [機器の管理] をポイントし、[設定] をクリックします。

3. 「セキュリティー」の [機器証明書] をクリックします。

4. 作成する証明書番号を選択します。

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。

5. [作成] をクリックします。

6. 必要な設定項目を入力します。

表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。

S/MIME、デジタル署名 PDF、デジタル署名 PDF/A に使用するときには、メールアドレスの項目に本機の管理者メールアドレスを設定します。

7. [OK] をクリックします。

設定が書き換えられます。

8. [OK] をクリックします。

セキュリティーの警告に関するダイアログが表示されます。

9. 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。

10. ログアウトします。



- 本機から機器証明書を削除する場合は、[削除] をクリックします。

機器証明書を作成、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。

ネットワークセキュリティーを強化する

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [機器証明書] をクリックします。
4. 作成する証明書番号を選択します。
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。
5. [要求] をクリックします。
6. 必要な設定項目を入力します。
表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。
S/MIME、デジタル署名 PDF、デジタル署名 PDF/A に使用するときには、メールアドレスの項目に本機の管理者メールアドレスを設定します。
7. [OK] をクリックします。
8. [OK] をクリックします。
「機器証明書」エリアの「証明書状態」に「要求中」が表示されます。
9. ログアウトします。
10. 機器証明書を認証局に申請します。
申請方法は、認証局により異なります。申請先の認証局に確認してください。
また、申請に必要な情報は、Web Image Monitor の詳細アイコンをクリックして表示される「証明書詳細情報」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。導入する際に証明書の目的と導入順について確認してください。
- Web Image Monitor 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場合は、[取りやめ要求] をクリックします。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [機器証明書] をクリックします。
4. 導入する証明書番号を選択します。
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。
5. [導入] 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. 機器証明書の内容を入力します。

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場合、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。

7. [OK] をクリックします。

8. 本機が再起動するのをしばらく待ってから、[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。

9. 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. [機器の管理] をポイントし、[設定] をクリックします。

3. 「セキュリティー」の[機器証明書] をクリックします。

4. 導入する証明書番号を選択します。

5. [中間証明書導入] をクリックします。

6. 中間証明書の内容を入力します。

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。

7. [OK] をクリックします。

8. 本機が再起動するのをしばらく待ってから、[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。

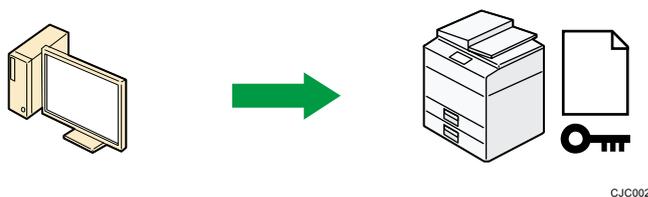
9. ログアウトします。

SSL/TLS を設定する

SSL/TLS を設定することで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 PC 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 PC へ機器証明書と公開鍵が送られます。



3. PC 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。

ネットワークセキュリティーを強化する

2. SSL/TLS を有効にする

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、認証局の要求する申請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場合、または認証局証明書を利用する場合のどちらにも共通の設定方法です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [SSL/TLS] をクリックします。
4. 「SSL/TLS」で使用するインターネットプロトコルのバージョンを [有効] に設定します。
5. 「SSL/TLS 通信許可設定」から暗号化通信モードを選択します。
6. 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。TLS1.2、TLS1.1、TLS1.0、SSL3.0 のうち少なくとも1つを有効にする必要があります。
7. 「暗号強度設定」から AES、3DES、RC4 それぞれで使用する暗号強度をチェックします。少なくともひとつチェックしている必要があります。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変わります。

ネットワークセキュリティを強化する

8. [OK] をクリックします。
9. 「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。
10. ログアウトします。

↓ 補足

- 「SSL/TLS 通信許可設定」を [暗号文のみ] に設定した場合、本機にアクセスするときは、「https:// (本機の IP アドレス、またはホスト名) /」と入力します。
- SSL のバージョンは、3.0 になります。
- 「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、本体操作部から [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なおしてください。
- 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] 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 サーバに接続できないことがあります。

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 PC 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、Windows Server 2008/2008 R2 で IPP-SSL を利用して本機で印刷する場合は、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。

↓ 補足

- 証明書の有効期限が切れているなどの問題でユーザーから問い合わせがあるときは、適切な対応をしてください。
- IPP で本機にアクセスするときの証明書ストアの場所は、「信頼されたルート証明機関」を選択してください。
- 本機に導入している機器証明書が認証局証明書のときは、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、Windows Server 2008/2008 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 アドレスを変更する場合は、先に PC のプリンターを削除し、[共通名称] の変更後にプリンターを再インストールしてください。

ネットワークセキュリティを強化する

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）を変更する場合も、プリンターを削除してユーザー認証の設定を変更後、プリンター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。 暗号化できない場合は、通信できません。
暗号文優先	暗号化できる場合は、暗号化通信します。 暗号化できない場合は、平文で通信します。
暗号文／平文	暗号化、または平文の指定された方法で通信します。

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. [システム初期設定] を押します。
3. [インターフェース設定] を押します。
4. [▼次へ] を押します。
5. [SSL/TLS 通信許可設定] を押します。



6. 暗号化通信モードを選択します。
暗号化通信モードは、[暗号文のみ]、[暗号文優先]、[暗号文／平文] のどれかを選択します。
7. [設定] を押します。
8. 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。Web Image

ネットワークセキュリティを強化する

Monitor のヘルプを参照してください。

SMTP 通信の SSL を設定する

1. 操作部からネットワーク管理者がログインします。
2. [システム初期設定] を押します。
3. [ファイル転送設定] を押します。
4. [SMTP サーバー] を押します。

配信オプション	0. 0. 0. 0	
文書管理サーバーIPv4アドレス	0. 0. 0. 0	管理者
SMTPサーバー	192.168.0.1	メール
SMTP認証	使用しない	受信
POP before SMTP	しない	サー
受信プロトコル	POP3	送

5. 「SSL」の [利用する] を押します。

機能を選択してください。

▶サーバー名 192.168.0.1

▶ポート番号 25 変更
<初期値25>

▶SSL 利用する 利用

SMTP 通信で SSL を設定しないときは、[利用しない] を押します。

「SSL」を [利用する] に設定すると、ポート番号は 465 に変更されます。

6. [設定] を押します。
7. ログアウトします。

↓ 補足

- 「SSL」を [利用する] に設定したときは、SMTP サーバーを経由しないで、相手先に直接インターネットファクスを送信できません。

S/MIME を設定する

本機のアドレス帳にユーザーの証明書を登録すると、公開鍵による暗号方式を用いたメッセージ送信ができ、情報漏洩を防止します。また本機に機器証明書を導入し、秘密鍵を使用した電子署名を添付することで、送信者の成りすましやメール内容の改ざんを防止できます。メッセージの暗号化とメールへの署名添付は、どちらか一方の機能だけを使用することもできます。メッセージの暗号化をするには、送信者側（本機）とメールの受信者側がともに S/MIME に対応している必要があります。

動作保証メーラー

本機の S/MIME 機能は以下のアプリケーションで使用できます。

- Microsoft Outlook 98 以降
- Microsoft Outlook Express 5.5 以降
- Thunderbird 3.1.7 以降
- Lotus Notes R5 以降
- Windows Live メール 2009 以降

★重要

- S/MIME の機能を使用するときは、[システム初期設定] の [ファイル転送設定] で [管理者メールアドレス] を必ず設定してください。

↓補足

- メールに電子署名を添付した場合、メールの「From」に管理者のメールアドレス、また「Reply-To」に「送信者」として選択したユーザーのメールアドレスが設定されます。
- S/MIME に対応したユーザーと対応していないユーザーに同時に送信をするとき、メールは暗号化されたものとされないものに分かれて送信されます。
- S/MIME 使用時は通常のメールよりもメールサイズが増加します。
- ファクスおよびスキャナーの S/MIME 機能については、『ファクス』『インターネットファクス/メールの暗号化・署名』、『スキャナー』『メールにセキュリティの設定をする』を参照してください。

メッセージを暗号化する

暗号化メール送信を行うには、事前に各ユーザーの証明書を用意し、ユーザー管理者が Web Image Monitor を使用して各ユーザーの証明書を本機のアドレス帳に登録しておく必要があります。証明書を登録すると各ユーザーの公開鍵が本機に設定されます。証明書の導入後に Web Image Monitor で暗号化に使用するアルゴリズムを設定します。アルゴリズムの設定はネットワーク管理者がします。

ネットワークセキュリティを強化する

メッセージの暗号化と復号

1. ユーザー証明書を準備します。
2. Web Image Monitor で本機のアドレス帳にユーザー証明書を導入します。(ユーザー証明書の公開鍵がアドレス帳に設定されます。)
3. Web Image Monitor で暗号アルゴリズムを設定します。
4. 共通鍵を使用してメッセージを暗号化します。
5. ユーザーの公開鍵を使用して共通鍵を暗号化します。
6. 暗号化されたメールがユーザーに送信されます。
7. メールを受信したユーザーは、公開鍵に対応した秘密鍵で共通鍵を復号します。
8. 共通鍵を使用してメッセージを復号します。

↓ 補足

- 本機に導入できるユーザー証明書は、「DER Encoded Binary X.509」、「Base 64 Encoded X.509」、「PKCS #7 証明書」の3種類です。
- アドレス帳にユーザー証明書を導入するとき、証明書ファイルが複数の証明書を含んでいると、Web Image Monitor 上にエラーメッセージが表示されます。複数の証明書を含む証明書ファイルを導入するときは、個別に導入してください。

ユーザー証明書を設定する

事前に各ユーザーの証明書の準備が必要です。

1. Web Image Monitor からユーザー管理者がログインします。
2. [機器の管理] をポイントし、[アドレス帳] をクリックします。
3. 証明書を導入するユーザーを選択します。
4. [通常入力] をクリックし、[変更] をクリックします。
5. 「メール」の「メールアドレス」欄にユーザーのメールアドレスを入力します。
6. 「ユーザー証明書」の [変更] をクリックします。
7. [参照] をクリックし、ユーザー証明書に使用するファイルを選択して、[開く] をクリックします。
8. [OK] をクリックします。
9. 「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。
10. ログアウトします。

↓ 補足

- 選択したユーザー証明書の有効期限が過ぎていると、暗号化したメッセージを送信

ネットワークセキュリティーを強化する

できません。有効期限内の証明書を選択してください。

暗号化アルゴリズムを設定する

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [S/MIME] をクリックします。
4. 「暗号化」の「暗号化アルゴリズム」でドロップダウンメニューから使用する暗号アルゴリズムを選択します。
5. [OK] をクリックします。
6. ログアウトします。

↓ 補足

- ユーザーのメールソフトでサポートしている暗号アルゴリズム、ダイジェストアルゴリズムを考慮して設定してください。

署名を添付する

署名を添付したメールを送信するには、事前に機器証明書の導入が必要です。機器証明書は、本機で証明書を作成する自己証明書と、認証局から発行される証明書のどちらも使用できません。機器証明書の作成、導入についてはP. 106「機器証明書による通信経路の保護」を参照してください。

★ 重要

- S/MIME に使用する機器証明書には、メールアドレスの設定が必要です。システム初期設定で設定する管理者のメールアドレスを設定してください。メールアドレスが設定されていない証明書は S/MIME の証明書に指定できません。また、S/MIME 認証の機能を使用しない場合でも、S/MIME 用に証明書を設定したときは、管理者メールアドレスをメールアドレスに設定する必要があります。

署名の添付と識別

1. 本機に機器証明書を導入します。(機器証明書の秘密鍵が本機に設定されます。)
2. 機器証明書の秘密鍵を使用してメールに署名を添付します。
3. 署名付きのメールがユーザーに送信されます。
4. メールを受信したユーザーは、本機に機器証明書と公開鍵を要求します。
5. 公開鍵を使用して添付された署名が正しいものであるかどうかを識別し、メッセージに改ざんがないかどうかを知ることができます。

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

ネットワークセキュリティーを強化する

操作部または、Web Image Monitor で機器証明書を作成、導入します。

2. 証明書を設定する

Web Image Monitor で、S/MIME に使用する証明書を設定します。

3. 署名の条件を設定する

Web Image Monitor で、署名に関する設定をします。

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、認証局の要求する申請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、認証局より発行された機器証明書を導入します。

3. 証明書を設定する

Web Image Monitor で、S/MIME に使用する証明書を設定します。

4. 署名の条件を設定する

Web Image Monitor で、署名に関する設定をします。

証明書を選択する

署名に使用する証明書を設定します。

1. Web Image Monitor からネットワーク管理者がログインします。

2. [機器の管理] をポイントし、[設定] をクリックします。

3. 「セキュリティー」の [機器証明書] をクリックします。

4. 「利用する証明書」の「S/MIME」で、使用する証明書を選択します。

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。



- 選択した機器証明書の有効期限が過ぎていると、メールに署名を添付できません。有効期限内の証明書を選択してください。

署名の条件を設定する

本機に機器証明書を導入後、S/MIME の署名の条件を設定します。

この設定は、機器証明書として自己証明書を利用するときと、認証局証明書を利用するとき

ネットワークセキュリティーを強化する

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [S/MIME] をクリックします。
4. 「署名」の「ダイジェストアルゴリズム」で署名に使用するダイジェストアルゴリズムを選択します。
5. 「署名」の「スキャナーでのメール送信」でメール送信時の署名添付方法を選択します。
6. 「署名」の「ファクス転送時」で受信ファクス転送時の署名添付方法を選択します。
7. 「署名」の「ファクスでのメール送信」でファクスをメール送信するときの署名添付方法を選択します。
8. 「署名」の「ファクスでの送信結果メール通知」で、ファクス機能の通知メール送信時の署名添付方法を選択します。
9. 「署名」の「ドキュメントボックス（ユーティリティー）蓄積文書転送時」で、蓄積文書転送時の署名添付方法を選択します。
10. [OK] をクリックします。
11. ログアウトします。

補足

- ユーザーのメールソフトでサポートしている暗号アルゴリズム、ダイジェストアルゴリズムを考慮して設定してください。

証明書の有効期限チェックを設定する

S/MIME で使用する証明書は、メール送信時に有効期限がチェックされます。

有効期限をチェックするタイミングを変更できます。

動作モード	説明
セキュリティー優先	以下のタイミングで有効期限をチェックします。 ユーザー証明書 (a). あて先選択時 (b). [スタート] キーを押したとき 機器証明書 (c). 1 件目のあて先を選択したとき (d). [スタート] キーを押したとき

ネットワークセキュリティを強化する

動作モード	説明
パフォーマンス優先	(b)と(c)のチェックを省略します。 あて先を選択したときや、[スタート] キーを押したときなど、有効期限のチェックに時間がかかる場合は、“パフォーマンス優先”にすると、素早く操作できます。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [S/MIME] をクリックします。
4. 動作モードを選択します。
5. [OK] をクリックします。
6. ログアウトします。

↓ 補足

- 送信時に有効期限内であっても、メールサーバーからクライアント PC に引き取る間に証明書の期限が切れたときは、サーバーからメールが引き取れなくなることがあります。
- メモリー転送や、時刻指定送信など、自動的にS/MIMEメール送信したときに証明書の有効期限外エラーが起きたときは、送信者か管理者用メールアドレスに平文のメールで通知されます。エラー内容はジョブログで確認できます。S/MIMEを使用するときは、常にジョブログ収集機能を有効にしてください。ログの確認方法は、P. 178「ログを管理する」を参照してください。

電子署名付き PDF の設定をする

本機では電子署名付き PDF を作成できます。電子署名付き PDF は、PDF 文書の作成者と作成日時を証明できます。また、電子署名によって文書の改ざんを検知できるので、改ざんの防止になります。

電子署名付き PDF を作成するには、事前に作成、導入された機器証明書から、署名に使用する証明書を選択します。

機器証明書は、本機で証明書を作成する自己証明書と、認証局から発行される証明書のどちらも使用できます。機器証明書の作成、導入についてはP. 106「機器証明書による通信経路の保護」を参照してください。

★重要

- 電子署名付き PDF を作成するときは、[システム初期設定] の [ファイル転送設定] で [管理者メールアドレス] を必ず設定してください。
- 電子署名付き PDF に使用する機器証明書には、メールアドレスの設定が必要です。[システム初期設定] で設定した管理者のメールアドレスを設定してください。

証明書を選択する

署名に使用する証明書を選択します。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [機器証明書] をクリックします。
4. 「利用する証明書」の「デジタル署名 PDF」または「デジタル署名 PDF/A」で、使用する証明書を選択します。
 - 「デジタル署名 PDF」: PDF/A 以外の PDF に使用します。
 - 「デジタル署名 PDF/A」: PDF/A の PDF に使用します。
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

- 選択した機器証明書の有効期限が過ぎていると、PDF に署名を添付できません。有効期限内の証明書を選択してください。
- PDF/A に署名を添付するときは、機器証明書の署名アルゴリズムが

ネットワークセキュリティを強化する

SHA1withRSA1024 になります。

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、手動鍵設定方式と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、PC 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、本体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。本体操作部による IPsec 有効/無効設定の切り替え方法については、『ネットワークの接続/システム初期設定』『システム初期設定』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。
- IPv4 の IPsec に対応している OS は Windows XP SP2、Windows Server 2003/2003 R2 です。IPv4 と IPv6 両方の IPsec に対応している OS は、Windows Vista/7、Windows Server 2008/2008 R2、Mac OS X 10.4.8 以降、Red Hat Enterprise Linux WS 4.0、Solaris 10 です。ただし、OS によって対応していない設定項目があります。IPsec の設定をするときは、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通信をします。

ネットワークセキュリティーを強化する

- 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。自動鍵交換設定のときは、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。自動鍵交換設定のときは、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。自動鍵交換設定のときは、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。自動鍵交換設定のときは、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。自動鍵交換設定のときは、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。

自動鍵交換設定と手動鍵設定

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

自動鍵交換設定方式では、SA の設定が自動的に行われますが、最初に ISAKMP SA が自動設定 (フェーズ 1) され、続いて IPsec 通信のための IPsec SA が自動設定 (フェーズ 2) されます。また、より高いセキュリティーを確保した通信をするために、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。

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

自動鍵交換設定、手動鍵設定ともに、SA の設定を複数設定できます。

個別設定とデフォルト設定

ネットワークセキュリティーを強化する

自動鍵交換設定、手動鍵設定ともに、IPsec で使用するアルゴリズムや鍵などの SA 設定を個別に 4 種類設定できます。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。

自動鍵交換設定／手動鍵設定共通設定項目

設定項目	設定内容	設定値
IPsec*1	IPsec 機能を有効にするか無効にするか設定します。	・有効 ・無効
HTTPS 通信の除外	HTTPS 通信を IPsec から除外するかしないかを設定します。	・有効 ・無効 HTTPS 通信を IPsec の対象から除外する場合は有効を選択します。
手動鍵設定	手動鍵設定を有効にするか無効にするか設定します。	・有効 ・無効 手動鍵設定を使用する場合は有効を選択します。

*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以下のとおりです。

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の強度は低い設定です。
認証と暗号化（高）	通信相手の認証と改ざん防止に加え、パケットデータ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以下のとおりです。

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

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
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"> ・ 無効 ・ IPv4 ・ IPv6 ・ IPv4/IPv6（デフォルト設定のみ）

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
ローカルアドレス	機器のアドレスを設定します。IPv6 で複数のアドレスを使用しているときは、範囲の指定もできます。	<ul style="list-style-type: none"> ・ 機器の 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 はアドレスの後に 32 を入力し、IPv6 はアドレスの後に 128 を入力します。
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"> ・ 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 はアドレスの後に 32 を入力し、IPv6 はアドレスの後に 128 を入力します。
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"> ・ IPsec を適用して送受信する (Apply) ・ IPsec を適用せずに送受信する (Bypass) ・ パケットを破棄する (Discard)

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
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"> ・ トランスポート ・ トンネル (トンネル始点 IP アドレス—トンネル終点 IP アドレス) セキュリティレベルに関係なくトランスポートモードが選択されます。 トンネルモードを選択したときは、トンネルエンドポイントで始点 IP アドレスと終点 IP アドレスを指定します。 トンネルエンドポイントの始点 IP アドレスにはローカルアドレスと同じ値を設定します。
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"> ・ 可能な場合使用する ・ 必須

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
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"> ・ PSK ・ 証明書 セキュリティレベルに関係なく「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く必要があります。
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"> ・ MD5 ・ SHA1 ・ SHA256 ・ SHA384 ・ SHA512
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"> ・ DES ・ 3DES ・ AES-128-CBC ・ AES-192-CBC ・ AES-256-CBC
フェーズ 1 Diffie-Hellman グループ	IKE の暗号鍵生成に使う 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"> ・ 1 ・ 2 ・ 14

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 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には 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"> ・ ESP ・ AH ・ ESP+AH
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"> ・ HMAC-MD5-96 ・ HMAC-SHA1-96 ・ HMAC-SHA256-128 ・ HMAC-SHA384-192 ・ HMAC-SHA512-256
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"> ・ 平文 (NULL 暗号) ・ DES ・ 3DES ・ AES-128 ・ AES-192 ・ AES-256
フェーズ 2 PFS	PFS の有効/無効と有効時の Diffie-Hellman グループ番号を選択します。 (自動設定対象項目)	<ul style="list-style-type: none"> ・ 無効 ・ 1 ・ 2 ・ 14
フェーズ 2 有効期間	フェーズ 2 で使用する SA の有効期間を設定します。	300 秒 (5 分) ~172800 秒 (48 時間) の間で秒単位で設定します。

手動鍵設定の設定項目

設定項目	設定内容	設定値
アドレスタイプ	IPsec の対象とする IP アドレスのタイプを選択します。	<ul style="list-style-type: none"> ・ 無効 ・ IPv4 ・ IPv6 ・ IPv4/IPv6 (デフォルト設定のみ)
ローカルアドレス	機器のアドレスを設定します。IPv6 で複数のアドレスを使用しているときは、範囲の指定もできます。	<ul style="list-style-type: none"> ・ 機器の 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 はアドレスの後に 32 を入力し、IPv6 はアドレスの後に 128 を入力します。
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"> ・ 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 はアドレスの後に 32 を入力し、IPv6 はアドレスの後に 128 を入力します。
カプセル化モード	カプセル化モードを選択します。	<ul style="list-style-type: none"> ・ トランスポート ・ トンネル (トンネル始点 IP アドレス—トンネル終点 IP アドレス) トンネルモードを選択したときは、トンネルエンドポイントで始点 IP アドレスと終点 IP アドレスを指定します。 トンネルエンドポイントの始点 IP アドレスにはローカルアドレスと同じ値を設定します。
SPI 値 (出力)	通信相手先の入力の SPI 値と同一の値を設定します。	256~4095 の間の任意の整数値

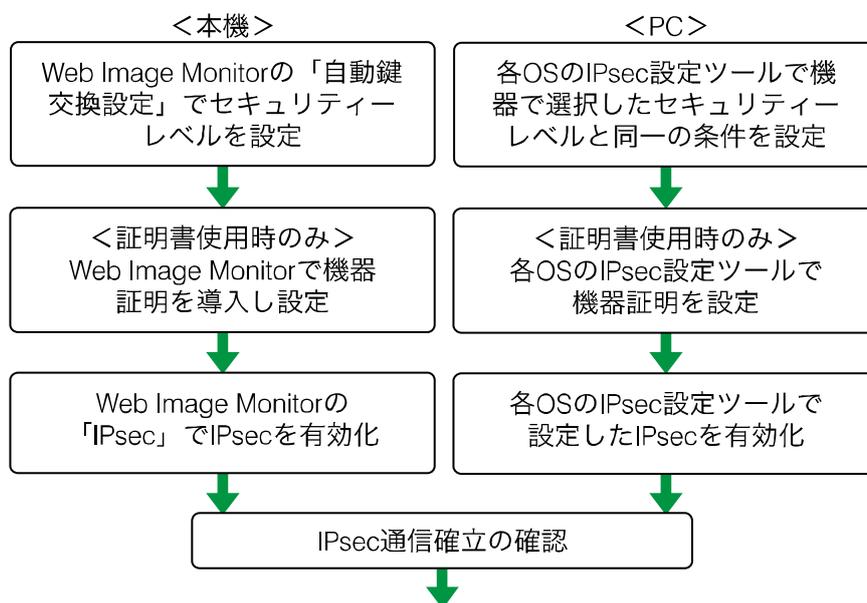
ネットワークセキュリティを強化する

設定項目	設定内容	設定値
SPI 値（入力）	通信相手先の出力の SPI 値と同一の値を設定します。	256～4095 の間の任意の整数値
セキュリティプロトコル	暗号化と認証を同時にするときには ESP もしくは AH+ESP を、認証だけをする場合は AH を選択します。	<ul style="list-style-type: none"> ・ ESP ・ AH ・ ESP+AH
認証アルゴリズム	認証に使用するアルゴリズムを選択します。	<ul style="list-style-type: none"> ・ HMAC-MD5-96 ・ HMAC-SHA1-96 ・ HMAC-SHA256-128 ・ HMAC-SHA384-192 ・ HMAC-SHA512-256
認証鍵	認証アルゴリズムの鍵を設定します。	<p>認証アルゴリズムによって以下の長さの任意の値を設定します。</p> <p><16 進数の場合></p> <p>半角の 0～9、a～f、A～F</p> <ul style="list-style-type: none"> ・ HMAC-MD5-96 選択時 32 桁 ・ HMAC-SHA1-96 選択時 40 桁 ・ HMAC-SHA256-128 選択時 64 桁 ・ HMAC-SHA384-192 選択時 96 桁 ・ HMAC-SHA512-256 選択時 128 桁 <p><アスキー文字列の場合></p> <ul style="list-style-type: none"> ・ HMAC-MD5-96 選択時 16 文字 ・ HMAC-SHA1-96 選択時 20 文字 ・ HMAC-SHA256-128 選択時 32 文字 ・ HMAC-SHA384-192 選択時 48 文字 ・ HMAC-SHA512-256 選択時 64 文字

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
暗号化アルゴリズム	暗号化に使用するアルゴリズムを選択します。	<ul style="list-style-type: none"> ・ 平文 (NULL 暗号) ・ DES ・ 3DES ・ AES-128 ・ AES-192 ・ AES-256
暗号鍵	暗号化アルゴリズムの鍵を指定します。	<p>暗号化アルゴリズムによって以下の長さの任意の値を設定します。</p> <p><16 進数の場合> 半角の 0~9、a~f、A~F</p> <ul style="list-style-type: none"> ・ DES 選択時 16 桁 ・ 3DES 選択時 48 桁 ・ AES-128 選択時 32 桁 ・ AES-192 選択時 48 桁 ・ AES-256 選択時 64 桁 <p><アスキー文字列の場合></p> <ul style="list-style-type: none"> ・ DES 選択時 8 文字 ・ 3DES 選択時 24 文字 ・ AES-128 選択時 16 文字 ・ AES-192 選択時 24 文字 ・ AES-256 選択時 32 文字

自動鍵交換設定の流れ



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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [IPsec] をクリックします。
4. 「自動鍵交換設定」の [編集] をクリックします。
5. 「個別設定 1」で自動鍵交換設定の条件を設定します。
複数の個別設定条件を設定する場合は、個別設定番号を切り替えて追加設定します。
6. [OK] をクリックします。
7. 「IPsec」の「IPsec:」で [有効] を選択します。
8. 「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。
9. [OK] をクリックします。
10. 「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

ネットワークセキュリティーを強化する

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。

11. 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. 106 「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 に割り当てる方法については、「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. 106 「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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [機器証明書] をクリックします。
4. 「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。
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。

PC で IPsec の条件を設定する

機器で選択したセキュリティーレベルの IPsec SA 設定と同一の条件を PC 側で設定します。設定方法は OS によって異なります。ここではセキュリティーレベルで「認証と暗号化(低)」を選択したときの Windows 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 XP の場合は、[スタート] メニューから [コントロールパネル] - [パフォーマンスとメンテナンス] - [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)] 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

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」に機器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. 機器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。
存在しない場合は [追加] をクリックし作成します。
12. [OK] を 2 回クリックします。
13. [規則] タブを選択し、[追加] をクリックします。
「セキュリティの規則ウィザード」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。
17. Windows XP の場合は、認証方法を選択して [次へ] をクリックします。
機器の自動鍵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機器で設定した PSK と同じ文字列を入力します。
Windows 7 の場合は、手順 18 に進みます。
18. 「IP フィルター一覧」で [追加] をクリックします。
19. 「名前」に任意の IP フィルター名を入力し、[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。
20. [次へ] をクリックします。
Windows XP の場合は、手順 22 に進みます。
21. 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。
22. 「発信元アドレス」で「このコンピュータの IP アドレス」を選択し、[次へ] をクリックします。
23. 「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、機器の IP アドレスを入力して [次へ] をクリックします。
24. 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。

25. [完了] をクリックします。
26. [OK] をクリックします。
27. 設定した IP フィルターを選択し、[次へ] をクリックします。
28. [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。
29. [次へ] をクリックします。
30. 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。
31. [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。
32. [セキュリティで保護された接続が確立できない場合、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。
33. 「カスタム」を選択し、[設定] をクリックします。
34. 「整合性アルゴリズム」で機器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。
35. 「暗号化アルゴリズム」で機器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。
36. 「セッションのキーの設定」で「新しいキーの生成間隔 (R)」にチェックを入れ、機器の自動鍵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。
37. [OK] をクリックします。
38. [次へ] をクリックします。
39. [完了] をクリックします。
40. 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。
41. 認証方法を選択して [次へ] をクリックします。
Windows XP の場合は、手順 42 に進みます。
機器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機器で設定した PSK と同じ文字列を入力します。
42. [完了] をクリックします。
43. [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。
44. 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。
PC の IPsec 設定が有効になります。

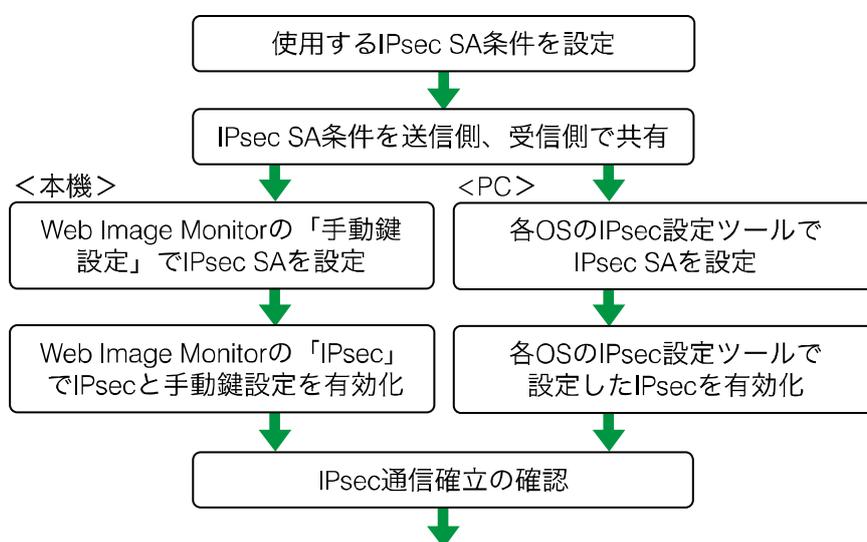
 補足

- PC の IPsec を無効にするときは、設定したセキュリティ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。

ネットワークセキュリティを強化する

- 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 を使うときは、自動鍵交換設定のフェーズ 2 で使われる 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、機器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、機器の「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。

手動鍵設定の流れ



CJC016

★重要

- まず、送信者、受信者で IPsec 通信のための IPsec SA 情報を共有しそれぞれに設定します。このとき、IPsec SA の漏洩を防止するために、情報の交換はネットワークを使用しないで行うことをお勧めします。
- 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。

手動鍵設定をする

Web Image Monitor を使用して設定します。

- Web Image Monitor からネットワーク管理者がログインします。
- [機器の管理] をポイントし、[設定] をクリックします。
- 「セキュリティ」の [IPsec] 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

4. 「手動鍵設定:」で [有効] を選択します。
5. 「手動鍵設定」の [編集] をクリックします。
6. 「個別設定 1」で手動鍵設定の条件を設定します。
複数の個別設定条件を設定するときは、個別設定番号を切り替えて追加設定します。
7. [OK] をクリックします。
8. 「IPsec」の「IPsec:」で [有効] を選択します。
9. 「HTTPS 通信の除外:」で HTTPS 通信を IPsec の除外対象とするときは [有効] を選択します。
10. [OK] をクリックします。
11. 「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。

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。工場出荷時は、telnet にログインするユーザー名の初期値は「admin」です。パスワードは設定されていません。telnet のログイン方法、操作方法については、『ネットワークの接続/システム初期設定』「telnet を使う」を参照してください。

★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
```

- 以下の IPsec 関連の設定情報がすべて表示されます。
 - IPsec 共通設定の設定値
 - 手動鍵設定の個別 SA 設定値
 - 手動鍵設定のデフォルト SA 設定値
 - 自動鍵交換設定の個別 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
```

ネットワークセキュリティを強化する

- IPsec 関連の設定情報を分割して表示します。

ipsec manual_mode

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

現在の設定の表示

```
msh> ipsec manual_mode
```

- 手動鍵設定の設定情報が表示されます。

手動鍵設定の設定

```
msh> ipsec manual_mode {on|off}
```

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

ipsec 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 manual

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

現在の設定の表示

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

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

設定の無効化

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

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

個別設定のローカル／リモートアドレスの設定

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

ネットワークセキュリティを強化する

レス

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

デフォルト設定のアドレスタイプの設定

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

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

セキュリティープロトコルの設定

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

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

SPI 値の設定

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

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

カプセル化モードの設定

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

- 個別設定番号、またはデフォルト設定を指定し、カプセル化モードを設定します。
- トランスポートモードを使用するときは「transport」、トンネルモードを使用するときは「tunnel」を指定します。
- デフォルト設定のアドレスタイプで「any」を指定しているときは、カプセル化モードに「tunnel」を指定することはできません。
- 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 manual {1|2|3|4|default} tunneladdr 始点 IP アドレス 終点
```

ネットワークセキュリティを強化する

IP アドレス

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

認証アルゴリズムと認証鍵の設定

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

```
{hmac-md5|hmac-sha1|hmac-sha256|hmac-sha384|hmac-sha512} 認証鍵
```

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

暗号アルゴリズムと暗号鍵の設定

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

```
{null|des|3des|aes128|aes192|aes256} 暗号鍵
```

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

手動鍵 (manual) 設定値の初期化

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

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

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}
```

ネットワークセキュリティを強化する

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

デフォルト設定のアドレスタイプの設定

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

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

処理方法の設定

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

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

セキュリティプロトコルの指定

```
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。

ネットワークセキュリティを強化する

要求レベルの設定

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

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

カプセル化モードの設定

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

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

トンネルモードの始点/終点 IP アドレスの設定

```
msh> ipsec ike {1|2|3|4|default} 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。
- 始点/終点 IP アドレスの指定値を省略したときは、現在の設定が表示されます。

IKE の相手認証方式の設定

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

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

PSK 文字列の設定

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

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

ISAKMP SA (フェーズ 1) のハッシュアルゴリズムの設定

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

ネットワークセキュリティを強化する

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 タイプに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。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [サイト証明書] をクリックします。
4. 「インポートするサイト証明書」の [参照] をクリックし、入手した「CA 証明書」を選択します。
5. [開く] をクリックします。
6. [インポート] をクリックします。
7. 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。

ネットワークセキュリティーを強化する

8. [OK] をクリックします。
9. 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.106「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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の[機器証明書] をクリックします。
4. 「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。
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。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティー」の [IEEE 802.1X] をクリックします。
4. 「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。
5. 「ドメイン名」に、ご利用環境のドメイン名を入力します。
6. 「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

ネットワークセキュリティを強化する

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 (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 (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。
 - 「サブドメイン許可」を選択します。

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. 「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。

10. 「イーサネット」の「セキュリティ (802.1X)」で [有効] を選択します。

11. [OK] をクリックします。

12. 「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

ネットワークセキュリティを強化する

一の [更新] ボタンをクリックします。

13. 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、本機からネットワークサマリーを印刷して状況を確認できます。
- 原因が特定できないときは、本機の設定を変更前に戻したあと、はじめから手順をやり直してください。

無線 LAN 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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「セキュリティ」の [IEEE 802.1X] をクリックします。
4. 「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。
5. 「ドメイン名」に、ご利用環境のドメイン名を入力します。
6. 「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 (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。

ネットワークセキュリティを強化する

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 (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。
 - 「サブドメイン許可」を選択します。
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. 「インターフェース」の [無線 LAN 設定] をクリックします。
 10. 「ネットワークインターフェース選択」に [無線 LAN] を選択します。
 11. 「通信モード」に [インフラストラクチャーモード] を選択します。
 12. 「SSID」をご利用のアクセスポイントに合わせて入力します。
 13. 「セキュリティ方式」に [WPA] を選択します。
 14. 「WPA 認証方式」に、[WPA] を選択します。
 15. [OK] をクリックします。
 16. 「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。
 17. 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、本機からネットワークサマリーを印刷して状況を確認できます。
- 原因が特定できないときは、本機の設定を変更前に戻したあと、はじめから手順を

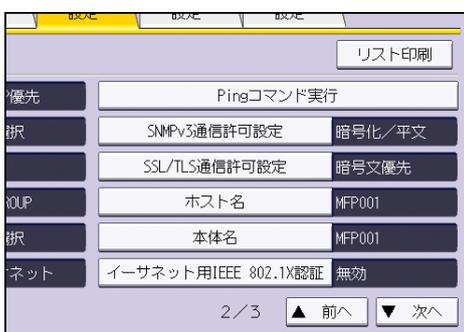
ネットワークセキュリティを強化する

やり直してください。

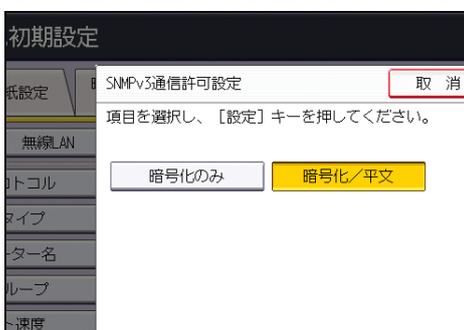
SNMPv3 暗号化通信を設定する

Network Monitor for Admin など、各種の設定をするときの通信データを暗号化できます。この設定により、通信データの改ざんを防止できます。

1. 操作部からネットワーク管理者がログインします。
2. [システム初期設定] を押します。
3. [インターフェース設定] を押します。
4. [▼次へ] を押します。
5. [SNMPv3 通信許可設定] を押します。



6. [暗号化のみ] を押します。



7. [設定] を押します。
8. ログアウトします。

補足

- Network Monitor for Admin をご利用の場合は、販売店にご確認ください。
- Network Monitor for Admin で各種の設定をするときに暗号化通信するには、本機の「SNMPv3 通信許可設定」の設定以外にネットワーク管理者の暗号パスワードの設定と Network Monitor for Admin の「SNMPv3 認証情報の入力」の暗号鍵の設定が必要です。Network Monitor for Admin の暗号鍵の設定は、Network Monitor for Admin のヘルプを参照してください。
- ネットワーク管理者の暗号パスワードが設定されていない場合、通信データが暗号化されないことや、通信できないことがあります。ネットワーク管理者の暗号パス

ネットワークセキュリティを強化する

ワードの設定は、P. 12「管理者を登録、変更する」を参照してください。

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ことで、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 PC で使用するドライバーに、同じドライバー暗号鍵を設定する必要があります。

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。

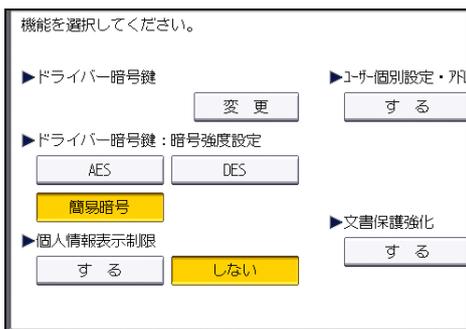
補足

- 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。
- 管理者認証のログインパスワードの暗号化については、P. 12 「管理者を登録、変更する」を参照してください。

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。

1. 操作部からネットワーク管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [セキュリティ強化] を押します。
6. 「ドライバー暗号鍵」の [変更] を押します。



ネットワークセキュリティを強化する

7. ドライバー暗号鍵を入力し、[OK] を押します。

ドライバー暗号鍵は、半角英数字 32 文字以内で入力します。

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

8. [設定] を押します。

9. ログアウトします。



補足

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

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. [機器の管理] をポイントし、[設定] をクリックします。

3. 「セキュリティ」の [IPP 認証] をクリックします。

4. 「認証:」のドロップダウンメニューから [DIGEST] を選択します。

5. ユーザー名を「ユーザー名:」ボックスに入力します。

6. パスワードを「パスワード:」ボックスに入力します。

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

- Windows XP/Vista/7、Windows Server 2003/2003 R2/2008/2008 R2 で IPP ポートを使用するときは、OS の標準 IPP ポートを使用できます。

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">▪ RC4-HMAC (ARCFOUR-HMAC-MD5)
Windows Server 2008	<ul style="list-style-type: none">▪ AES256-CTS-HMAC-SHA1-96▪ AES128-CTS-HMAC-SHA1-96▪ RC4-HMAC (ARCFOUR-HMAC-MD5)
Windows Server 2008 R2	<ul style="list-style-type: none">▪ AES256-CTS-HMAC-SHA1-96▪ AES128-CTS-HMAC-SHA1-96▪ RC4-HMAC (ARCFOUR-HMAC-MD5)*
Heimdal	<ul style="list-style-type: none">▪ AES256-CTS-HMAC-SHA1-96▪ AES128-CTS-HMAC-SHA1-96▪ DES3-CBC-SHA1▪ RC4-HMAC (ARCFOUR-HMAC-MD5)▪ DES-CBC-MD5

* OS の設定で有効にすると使用できます。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [機器の管理] をポイントし、[設定] をクリックします。
3. 「機器」の [Kerberos 認証] をクリックします。
4. 有効にする暗号化アルゴリズムを選択します。
少なくとも1つを有効にする必要があります。
5. [OK] をクリックします。
6. ログアウトします。

文書の漏洩を防止する

本機で保存したり、出力する文書データを保護する方法を説明します。

蓄積文書にアクセス権を設定する

ドキュメントボックスに蓄積された文書やスキャナーで読みこんだ蓄積文書に対して、その文書を使用できるユーザーとアクセス権を設定できます。アクセス権のあるユーザー以外の第三者による蓄積文書の印刷や、送信などの不正利用を防止できます。また、アクセス権のあるユーザーの中で特定のユーザーに蓄積文書の変更や削除を許可できます。

アクセス権の種類

4種類のアクセス権を設定し、蓄積文書の使用方法を制限できます。

アクセス権	説明
閲覧	蓄積文書の内容や情報を確認でき、印刷や送信もできます。
編集	蓄積文書の印刷条件を変更できます。 閲覧のアクセス権を含みます。
編集／削除	蓄積文書を消去できます。 閲覧、編集のアクセス権を含みます。
フルコントロール	蓄積文書にユーザーとアクセス権を設定できます。 閲覧、編集、編集/削除のアクセス権を含みます。

文書パスワード

- 文書管理者、または文書作成者（オーナー）は、蓄積文書にパスワードを設定できます。それにより、文書の不正利用に対する安全性をより強化できます。
文書パスワードの設定方法は、P. 165「蓄積文書にパスワードを設定する」を参照してください。
- ユーザー認証が設定されていなくても、蓄積文書にはパスワードを設定できます。
詳しくは、各機能の使用説明書を参照してください。

↓ 補足

- 文書の蓄積は、コピー機能、ドキュメントボックス、スキャナー機能、ファクス機

文書の漏洩を防止する

能、プリンター機能を使用できるユーザーであれば、どのユーザーでも可能です。

- 蓄積文書の内容は、Web Image Monitor でも確認できます。詳しくは、Web Image Monitor のヘルプを参照してください。
- 文書作成者（オーナー）のアクセス権の初期値は、[閲覧] です。また、アクセス権を設定できます。
- 文書管理者はアクセス権の設定のほかに、蓄積文書を消去できます。消去方法については、『コピー/ドキュメントボックス』「蓄積した文書を消去する」を参照してください。

蓄積文書ごとにアクセス権を設定する

文書管理者と、文書作成者（オーナー）が設定します。

蓄積文書ごとに、文書を使用するユーザーとそのアクセス権を設定します。

★重要

- 文書へアクセスできなくなったときは、文書作成者（オーナー）が該当する文書のアクセス権を再設定します。文書管理者も再設定できます。アクセス権限のない文書にアクセスする必要があるときは、文書作成者（オーナー）に確認してください。
- 文書管理者は文書の [アクセス権変更] でオーナーの変更、オーナーのアクセス権の変更、オーナー、および他のユーザーのアクセス権の変更ができます。
- 文書のオーナー、およびフルコントロール権限を持つ他のユーザーは、その文書の [アクセス権変更] でオーナー、および他のユーザーのアクセス権の変更ができます。

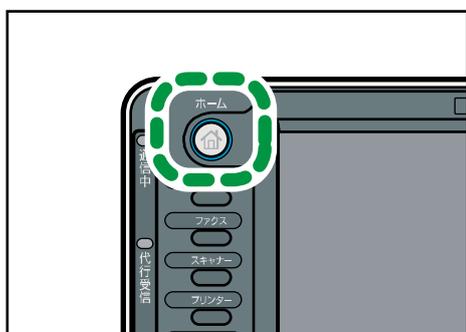
1. 操作部から文書管理者、または文書作成者（オーナー）がログインします。

2. [初期設定/カウンター] キーを押して、通常画面を表示します。

「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。

3. 操作部左上の [ホーム] キーを押して、ホーム画面上の [ドキュメントボックス] アイコンを押します。

「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。



4. 対象文書を選択します。

文書の漏洩を防止する

種別	ユーザー名	文書名	月日	ページ	印刷順
<input type="checkbox"/>	user1	COPY0014	09/30	5	
<input type="checkbox"/>	user1	COPY0013	09/30	5	
<input type="checkbox"/>	user1	COPY0012	09/30	5	
<input type="checkbox"/>	user1	COPY0011	09/30	5	
<input type="checkbox"/>	user1	COPY0010	09/30	5	

5. **【文書情報変更】**を押します。

名	文書名	月日	ページ	印刷順	残り: 99%
	COPY0005	09/30	5	1	詳細
	COPY0004	09/30	5		プレビュー
	COPY0003	09/30	5		文書情報変更...
	COPY0002	09/30	5		文書消去
	COPY0001	09/30	5		指定ページ印刷...

1/1
印刷画面へ

6. **【アクセス権変更】**を押します。

名	文書名	月日	ページ	印刷順	文書情報変更
	COPY0005	09/30	5	1	<input type="button" value="OK"/>
	COPY0004	09/30	5		アクセス権変更...
	COPY0003	09/30	5		文書ロック解除
	COPY0002	09/30	5		パスワード変更
	COPY0001	09/30	5		

7. **「アクセス許可ユーザー／グループ」**の**【登録／変更／消去】**を押します。

文書アクセス権登録／変更／消去	
▶オーナー	user1
▶アクセス許可ユーザー／グループ	登録／変更／消去

8. **【新規登録】**を押します。

文書の漏洩を防止する

9. 登録するユーザーまたはグループを選択します。

常用	AB	CD	EF	GH	IJK	LMN	OPQ	RST
【00001】赤坂支店	【00002】横浜事業所	【00003】企画課	【00004】ロサンゼルス支局	【00005】営業課				
【00007】沼津ショールーム	【00008】鹿児島事業所	【00010】上海工場	【00011】香港オフィス	【00012】支局グループ				

複数のユーザーを選択できます。

【すべてのユーザー】を押すと、全ユーザーを選択できます。

10. [閉じる] を押します。

11. アクセス権を設定するユーザーを選択し、アクセス権を選択します。

アクセス権は、[閲覧]、[編集]、[編集/削除]、[フルコントロール] のどれかを選択します。

12. [閉じる] を押します。

13. [OK] を押します。

14. 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。
- Web Image Monitor からも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

文書の漏洩を防止する

蓄積文書のオーナーを変更する

文書作成者（オーナー）を変更します。文書管理者が設定します。

1. 操作部から文書管理者がログインします。
2. [初期設定/カウンター] キーを押して、通常画面を表示します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
3. 操作部左上の [ホーム] キーを押して、ホーム画面上の [ドキュメントボックス] アイコンを押します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
4. 対象文書を選択します。
5. [文書情報変更] を押します。
6. [アクセス権変更] を押します。
7. 「オーナー」の [変更] を押します。
8. 登録するユーザーを選択します。
9. [閉じる] を押します。
10. [OK] を押します。
11. ログアウトします。

ユーザーごとに蓄積文書に対するアクセス権を設定する

ユーザー管理者と、文書作成者（オーナー）が設定します。

特定のユーザーが蓄積する文書に対して、文書を使用できるユーザーとそのアクセス権を設定します。

蓄積文書ごとにアクセス権を設定する場合と比較して、アクセス権の管理が容易になります。

★重要

- 文書へアクセスできなくなったときは、必ずユーザー管理者の設定を有効にしてから、ユーザー管理者が該当する文書のアクセス権を再設定してください。

1. 操作部から文書作成者（オーナー）、またはユーザー管理者がログインします。
2. [アドレス帳管理] を押します。
3. ユーザーを選択します。
4. [認証保護] を押します。
5. 「文書保護」、「アクセス許可ユーザー／グループ」の [登録／変更／消去] を押しします。

文書の漏洩を防止する

6. [新規登録] を押します。

7. 登録するユーザーまたはグループを選択します。

複数のユーザーを選択できます。

すべてのユーザーを押すと、全ユーザーを選択できます。

8. [閉じる] を押します。

9. アクセス権を設定するユーザーを選択し、アクセス権を選択します。

アクセス権は、[閲覧]、[編集]、[編集/削除]、[フルコントロール] のどれかを選択します。

10. [閉じる] を押します。

11. [設定] を押します。

12. [閉じる] を押します。

13. ログアウトします。

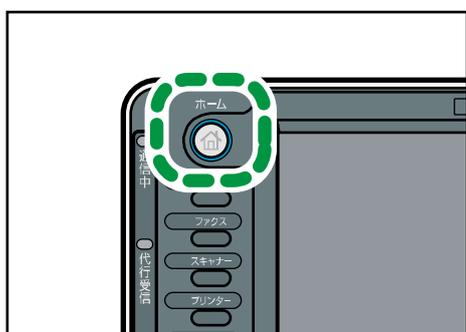
補足

- 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。

蓄積文書にパスワードを設定する

文書管理者と、文書作成者（オーナー）が設定します。

1. 操作部から文書管理者、または文書作成者（オーナー）がログインします。
2. [初期設定/カウンター] キーを押して、通常画面を表示します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
3. 操作部左上の [ホーム] キーを押して、ホーム画面上の [ドキュメントボックス] アイコンを押します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。



CJR001

4. 対象文書を選択します。

種別	ユーザー名	文書名	月日	ページ	印刷履歴
<input type="checkbox"/>	user1	ICOPY0014	09/30	5	
<input type="checkbox"/>	user1	ICOPY0013	09/30	5	
<input type="checkbox"/>	user1	ICOPY0012	09/30	5	
<input type="checkbox"/>	user1	ICOPY0011	09/30	5	
<input type="checkbox"/>	user1	ICOPY0010	09/30	5	

5. [文書情報変更] を押します。

名	文書名	月日	ページ	印刷履歴	残り： 99%
	ICOPY0005	09/30	5	1	詳細
	ICOPY0004	09/30	5		プレビュー
	ICOPY0003	09/30	5		文書情報変更 ...
	ICOPY0002	09/30	5		文書消去
	ICOPY0001	09/30	5		指定ページ印刷 ...

1/1

印刷画面へ

6. [パスワード変更] を押します。

文書の漏洩を防止する



7. 設定するパスワードをテンキーで入力します。
文書パスワードで使用できるのは、4桁～8桁の数字です。
8. [OK] を押します。
9. 確認用のパスワードをテンキーで入力します。
10. [OK] を押します。
パスワードで保護された文書に🔒が表示されます。
11. [OK] を押します。
12. ログアウトします。

蓄積文書のロックを解除する

文書管理者だけが操作できます。

セキュリティ強化機能の「文書保護強化」を[する]に設定したときは、誤ったパスワードを10回入力すると文書はロックされます。「文書保護強化」については、P. 230「セキュリティ強化機能を設定する」を参照してください。

1. 操作部から文書管理者がログインします。
2. [初期設定/カウンター] キーを押して、通常画面を表示します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
3. 操作部左上の[ホーム] キーを押して、ホーム画面上の[ドキュメントボックス] アイコンを押します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
4. 対象文書を選択します。
文書保護強化機能で保護された文書に🔒が表示されます。
5. [文書情報変更] を押します。

文書の漏洩を防止する



6. **【文書ロック解除】を押します。**



7. **【解除する】を押します。**

がに変わります。

8. **【OK】を押します。**
9. **ログアウトします。**

不正コピー抑止機能

本機のプリンター機能では、プリンタードライバーの設定で、不正コピーを抑止するための地紋をつけた印刷ができます。

不正コピー抑止は、プリンタードライバーで設定した文字列地紋（「コピー禁止」などの任意の文字列）が浮き上がるため、不正な文書複製を抑止します。

不正コピー抑止機能

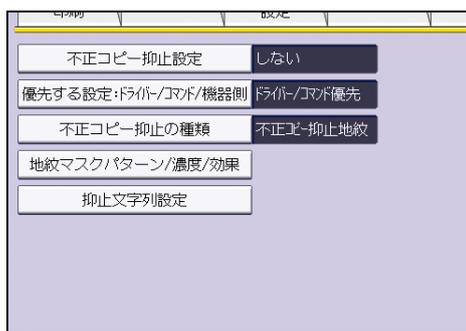
1. 本機で地紋印刷の設定をします。機器管理者が設定します。
2. プリンタードライバーで不正コピー抑止印刷を設定して印刷します。
印刷をするユーザーが設定します。詳細は、『プリンター』「複製できない文書を印刷する」を参照してください。

地紋印刷を有効にする

不正コピー抑止用の地紋印刷を有効にします。

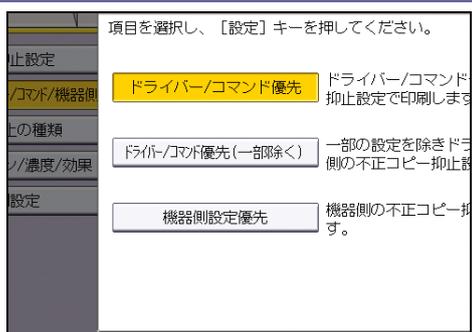
本機に PS3 カードが装着され、かつエミュレーションで、[PS3] を選択しているときに設定できます。

1. 操作部から機器管理者がログインします。
2. [プリンター初期設定] を押します。
3. [不正コピー抑止] を押します。
4. [不正コピー抑止設定] を押します。



5. [する] を押してから、[設定] を押します。
6. [優先する設定: ドライバー/コマンド/機器側] を押します。
7. 地紋の設定をプリンタードライバーと本機のどちらで行うかを選択します。

文書の漏洩を防止する



- [ドライバー/コマンド優先]
印刷する地紋の内容を、すべてプリンタードライバーで設定します。
- [ドライバー/コマンド優先(一部除く)]
地紋の種類、濃度以外をプリンタードライバーで設定します。
- [機器側設定優先]
プリンタードライバーで地紋の設定はできません。本機で設定した地紋が印刷されます。

8. [設定] を押します。

9. ログアウトします。

補足

- 本機で地紋を設定するときの、設定項目は『プリンター』『プリンター初期設定』を参照してください。

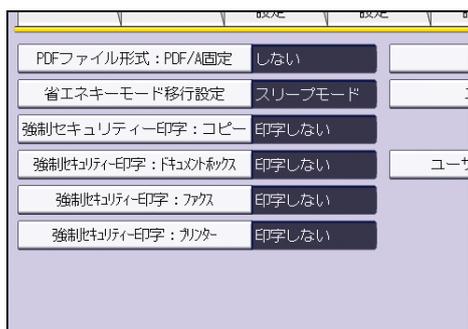
印刷紙にユーザー情報を印字する

印刷紙にジョブの開始時刻、出力者情報（名前もしくはログインユーザー名）、マシン番号、本機の IP アドレスを強制的に印字できます。この機能を強制セキュリティ印字といいます。

出力者の情報が必ず印字されることで、情報漏洩の抑止効果があります。また情報漏洩元を特定するときに活用できます。

コピー、ドキュメントボックス、ファクス、プリンターそれぞれの機能で、強制セキュリティ印字ができます。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 4 回押します。
5. 強制セキュリティ印字をする機能を選択します。



コピー機能の印字設定は、[強制セキュリティ印字: コピー] を押します。

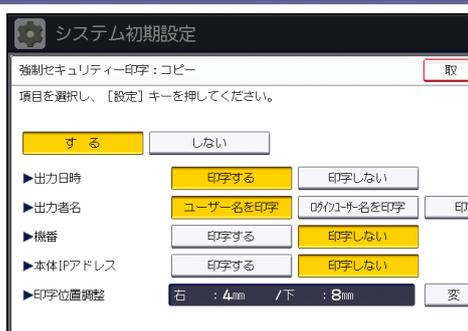
ドキュメントボックス機能の印字設定は、[強制セキュリティ印字: ドキュメントボックス] を押します。

ファクス機能の印字設定は、[強制セキュリティ印字: ファクス] を押します。

プリンター機能の印字設定は、[強制セキュリティ印字: プリンター] を押します。

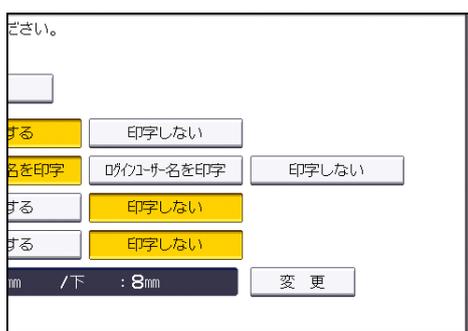
6. [する] を押します。
強制セキュリティ印字をしないときは、[しない] を押します。
7. 印字する項目を [印字する] にします。

文書の漏洩を防止する

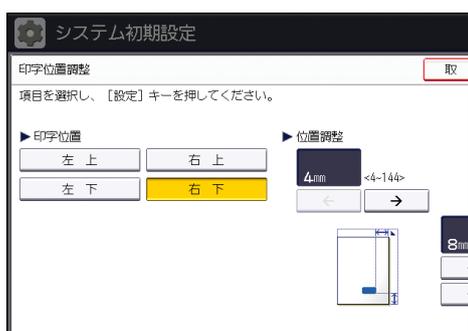


- 出力日時
ジョブの開始時刻が印字されます。
- 出力者名
「ユーザー名を印字」を選択すると、アドレス帳の「登録情報」の「名前」が印字されます。「ログインユーザー名を印字」を選択すると、アドレス帳の「認証情報」の「ログインユーザー名」が印字されます。ユーザー認証を設定していないとき、または、ユーザーコード認証を設定しているときは、出力者情報は印字されません。
- 機番
[問い合わせ情報] の機械番号と同じ番号が印字されます。
- 本体 IP アドレス
本機の IP アドレスが印字されます。IPv4 アドレスと IPv6 アドレスが共存している場合は、IPv4 アドレスが印字されます。IP アドレスが設定されていないと印字されません。

8. 「印刷位置調整」の[変更]を押します。



9. 印字位置を設定します。



文書の漏洩を防止する

10. [設定] を 2 回押します。

11. ログアウトします。

機密印刷文書を管理する

本機の設置場所がユーザーの席から離れているときなど、移動する間に印刷した文書を他人に見られてしまうことがあります。このようなときに、他人に見せたくない文書を印刷するときは、機密印刷機能を利用します。

機密印刷機能

プリンターの機密印刷機能を使用し、出力文書を機密印刷文書として本機に蓄積してから印刷します。本機の操作部を使用して印刷し、印刷した文書をすぐに回収できるため、他人に見られることを防止できます。

補足

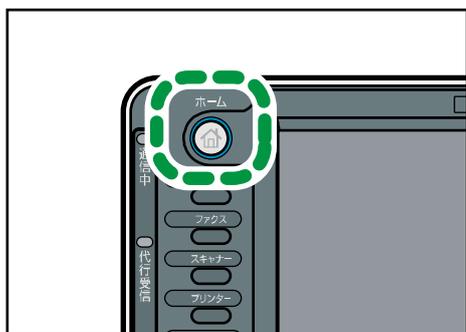
- ユーザー認証が設定されていなくても機密印刷ができます。設定方法は、『プリンター』「機密印刷をする」を参照してください。
- 一時的な文書の保存をするときには、プリンタードライバーの「印刷方法」で「プリンターに保存する」を選択します。また、「プリンターに保存するジョブを共有する」を選択すると、ジョブの共有ができます。
- 機密印刷の方法は、『プリンター』「機密印刷をする」を参照してください。

機密印刷文書を消去する

文書管理者と、文書作成者（オーナー）が設定します。

機密印刷文書を消去するには、機密印刷文書のパスワードが必要です。文書作成者（オーナー）がパスワードを忘れたときは、文書管理者がパスワードを変更できます。

1. 操作部から文書管理者、または文書作成者（オーナー）がログインします。
2. 「初期設定/カウンター」キーを押して、通常画面を表示します。
「この機能を利用する権限はありません。」が表示されたときは、「確認」を押します。
3. 操作部左上の「ホーム」キーを押して、ホーム画面上の「プリンター」アイコンを押します。
「この機能を利用する権限はありません。」が表示されたときは、「確認」を押します。



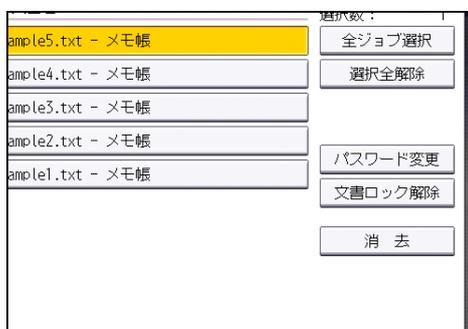
CJR001

文書の漏洩を防止する

4. **【文書印刷】** を押します。
5. **【機密印刷文書】** を押します。



6. **消去する機密文書** を選択します。
7. **【消去】** を押します。



8. **パスワード入力画面が表示されたら機密印刷文書のパスワードを入力し、【実行】** を押します。
文書管理者が操作する場合、パスワード入力画面は表示されません。
9. **【消去する】** を押します。
10. **ログアウト** します。

補足

- 「一時置き文書自動消去設定」を有効にすると、蓄積文書を自動で消去できます。「一時置き文書自動消去設定」の設定方法は、『プリンター』『調整 / 管理』を参照してください。
- Web Image Monitor からも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

機密印刷文書のパスワードを変更する

文書管理者と、文書作成者（オーナー）が設定します。

文書作成者（オーナー）がパスワードを忘れたときは、文書管理者がパスワードを変更します。

1. **操作部から文書管理者、または文書作成者（オーナー）** がログインします。
2. **【初期設定/カウンター】** キーを押して、**通常画面** を表示します。

文書の漏洩を防止する

「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。

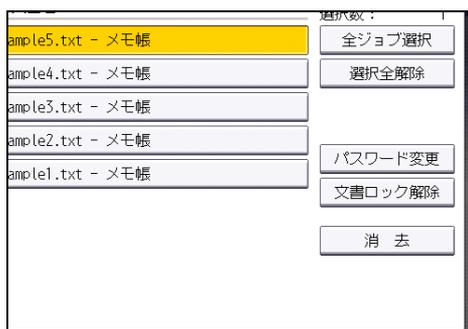
3. 操作部左上の [ホーム] キーを押して、ホーム画面上の [プリンター] アイコンを押します。

「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。

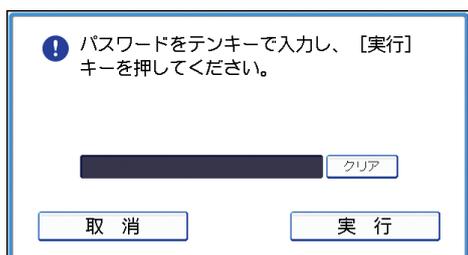
4. [文書印刷] を押します。
5. [機密印刷文書] を押します。



6. 対象文書を選択します。
7. [パスワード変更] を押します。



8. パスワード入力画面が表示されたら機密印刷文書のパスワードを入力し、[実行] を押します。



文書管理者が操作する場合、パスワード入力画面は表示されません。

9. 新しいパスワードを入力し、[OK] を押します。
10. 確認用パスワードを入力し、[OK] を押します。
11. ログアウトします。

補足

- Web Image Monitor から設定できます。詳しくは、Web Image Monitor のヘルプ

文書の漏洩を防止する

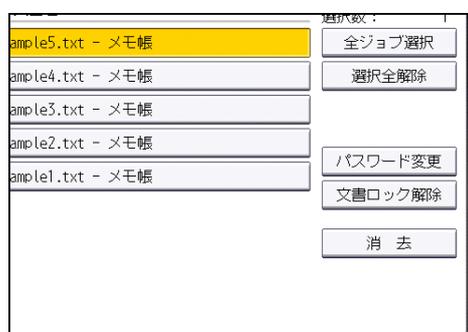
を参照してください。

機密印刷文書のロックを解除する

文書管理者だけが操作できます。

セキュリティ強化機能の「文書保護強化」を [する] に設定したときは、誤ったパスワードを 10 回入力すると文書はロックされます。「文書保護強化」については、P. 230 「セキュリティ強化機能を設定する」を参照してください。

1. 操作部から文書管理者がログインします。
2. [初期設定/カウンター] キーを押して、通常画面を表示します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
3. 操作部左上の [ホーム] キーを押して、ホーム画面上の [プリンター] アイコンを押します。
「この機能を利用する権限はありません。」が表示されたときは、[確認] を押します。
4. [文書印刷] を押します。
5. [機密印刷文書] を押します。
6. 対象文書を選択します。
文書保護強化でロックされた機密印刷文書は  が表示されます。
7. [文書ロック解除] を押します。



8. [解除する] を押します。
 の表示が消えます。
9. ログアウトします。

↓ 補足

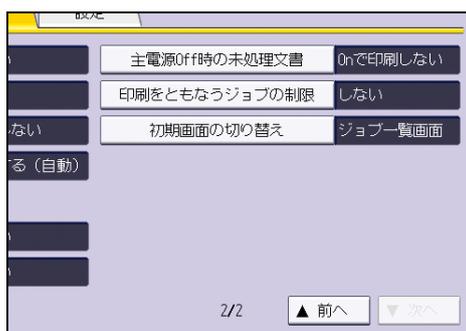
- Web Image Monitor から設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

プリンターの印刷文書を強制的に蓄積する

プリンターで印刷する文書を強制的に蓄積することで、出力紙の取り忘れや、放置による情報漏洩を防止します。

出力をとまなう、以下の印刷ジョブが強制蓄積の対象です。

- 通常印刷
 - 試し印刷
 - プリンターに保存して印刷
1. 操作部から機器管理者がログインします。
 2. [プリンター初期設定] を押します。
 3. [システム設定] を押します。
 4. [▼次へ] を押します。
 5. [印刷をとまなうジョブの制限] を押します。



6. [自動蓄積] を選択します。
7. [設定] を押します。
8. ログアウトします。

補足

- [印刷取消] を選択すると、出力をとまなう印刷ジョブはすべて取り消され、蓄積もされません。
- 蓄積文書の印刷方法については、『プリンター』「蓄積文書を印刷する」を参照してください。

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ことで、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な情報が確認できます。

また、ログを消去してハードディスクの容量を空けたり、暗号化してログの漏洩を防止できます。

ログは Web Image Monitor を使用して確認します。収集したログは CSV 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
コピー・ドキュメントボックスへの文書蓄積・プリンター印刷・ファクス送信などのユーザーの文書に関わるワークフローすべてのログ情報/操作部から出力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/蓄積文書の作成・編集・削除などの文書操作/ハードディスク初期化などの販売店操作、不正コピー読み取り時のシステム動作/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動作
- eco ログ
主電源のオン、オフ/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/機器の消費電力量

本機からログを管理する

ログの一括消去ができます。

ログを一括消去する

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。

本機を管理する

4. [▼次へ] を 3 回押します。
5. [ログ一括消去] を押します。
6. [消去する] を押します。
7. [確認] を押します。
8. ログアウトします。

↓ 補足

- 本機からログ一括消去を実行するには、Web Image Monitor で、ジョブログ、アクセスログ、eco ログのいずれかの収集設定を有効に設定されていることが必要です。

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。

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. [機器の管理] をポイントし、[設定] をクリックします。
 3. 「機器」の [ログ] をクリックします。
 4. 「ジョブログ収集」、「アクセスログ収集」、「eco ログ収集」で、それぞれ [有効] を選択します。
 5. 「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。

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

本機を管理する

[ユーザー設定] に変更されます。

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

- 「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する設定になります。

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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「機器」の [ログ] をクリックします。
4. 「ログ暗号化」の [有効] を選択します。
暗号化しないときは [無効] を選択します。
5. [OK] をクリックします。
ログ消去の確認が表示されます。
6. [OK] をクリックします。
7. 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。
- 機器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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「機器」の [ログ] をクリックします。
4. 「ログ一括消去」の [削除] をクリックします。
5. [OK] をクリックします。
6. ログアウトします。

↓ 補足

本機を管理する

- 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. [機器の管理] をポイントし、[設定] をクリックします。
3. 「機器」の [ログダウンロード] をクリックします。
4. [ダウンロードするログ] をクリックし、ダウンロードするログの種類を選択します。
セキュリティログには、ジョブログ、アクセスログの 2 種類が含まれます。
5. [ダウンロード] をクリックします。
6. 保存場所を指定して保存します。
7. [戻る] をクリックします。
8. 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。設定は Web Image Monitor の [設定] の [ログ] で行なえます。
- ログで取得できる情報は、P. 192 「ダウンロードできるログ情報の属性一覧」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 ログにおいて、本機に保持できる最大件数を超過して新しいログが発生すると、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

本機を管理する

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実施してください。

本機に保持できる件数

ジョブログ	アクセスログ	eco ログ
2000 件	6000 件	2000 件

ログ発生量の目安

ジョブログ	アクセスログ	eco ログ
100 件（1 日あたり）	300 件 左記のジョブにともなうログイン／ログアウト（200 件）、およびその他のアクセスログ（初期設定の操作や Web からのアクセスなど）が 100 件で合計 300 件	100 件（1 日あたり）

本条件で 20 日間のログ件数を保持できますが、ログのダウンロードは、余裕をもって半分の 10 日ごとを目安に実施することをお勧めします。

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後は、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他の動作をさせないでください。
- ログの一括消去は操作部と 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ます。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。

本機を管理する

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場合」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。

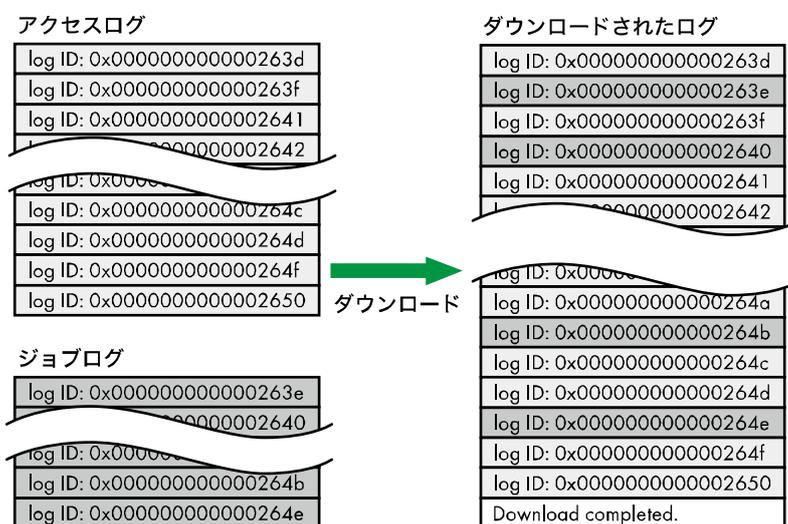
図の「上書きが発生している場合」は、アクセスログで上書きが発生したときの例を示します。

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。

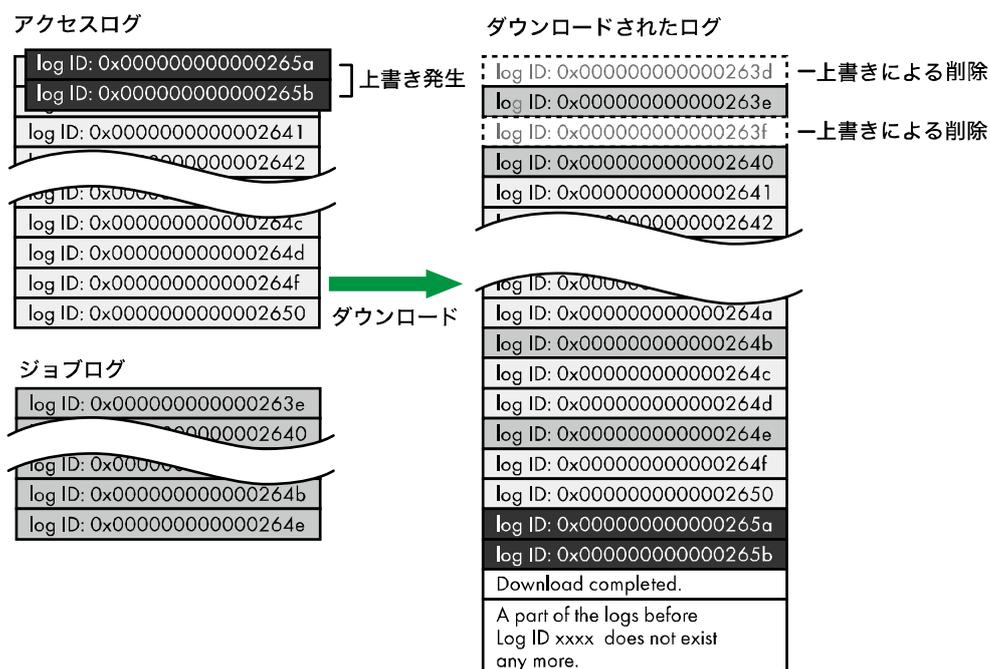
上書きが発生していない場合



CJC006

上書きが発生している場合

本機を管理する



CJC007

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、以下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場合
Download completed.
- 上書きが発生している場合
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）。

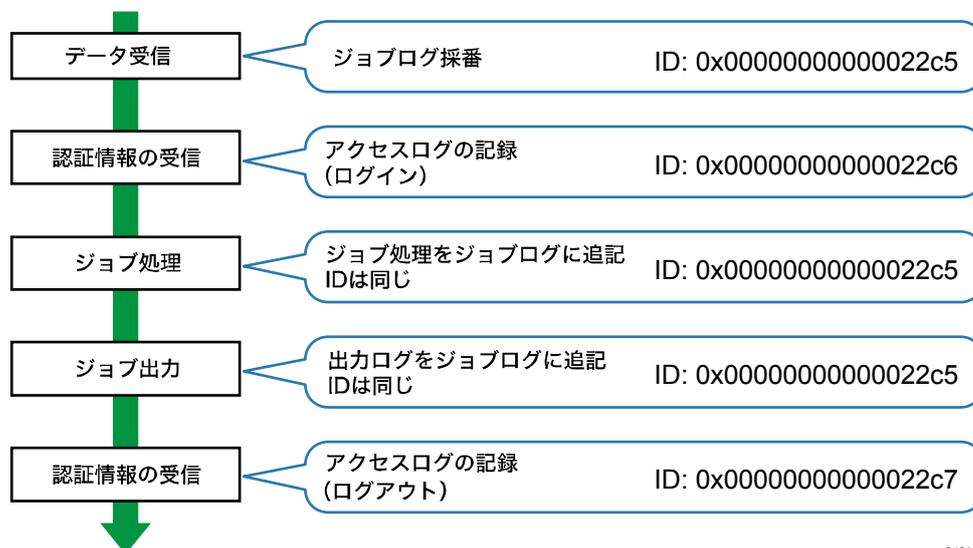
その後ログアウトのアクセスログが記録されます。

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



CJC008

Web Image Monitor で管理できるログ項目

収集できるログ項目

Web Image Monitor でログを収集する機能を有効にすると、機器にログが蓄積されます。収集できるログは以下のとおりです。設定についてはWeb Image Monitor の [設定] の [ログ] で行なえます。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。

ジョブログ

設定項目	Log Type の属性値	収集するログ
コピー : コピー	Copier: Copying	通常のコピーおよび試しコピーのログ
コピー : コピーと文書蓄積	Copier: Copying and Storing	コピーをしながらドキュメントボックスに文書を蓄積したときのログ
ドキュメントボックス : 文書蓄積	Document Server: Storing	ドキュメントボックス機能の画面から文書を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
蓄積文書（ドキュメントボックス）ダウンロード	Document Server: Stored File Downloading	Web Image Monitor からドキュメントボックスに蓄積された文書をダウンロードしたときのログ
蓄積文書印刷	Stored File Printing	ドキュメントボックス機能の画面から文書を印刷したときのログ
スキャナー：送信	Scanner: Sending	スキャナー機能で読み取った文書を送信したときのログ
スキャナー：URL リンク送信と文書蓄積	Scanner: URL Link Sending and Storing	スキャナー機能で読み取った文書をドキュメントボックスに蓄積して、その URL をメール送信したときのログ
スキャナー：送信と文書蓄積	Scanner: Sending and Storing	スキャナー機能で読み取った文書を送信しながらドキュメントボックスに蓄積したときのログ
スキャナー：文書蓄積	Scanner: Storing	スキャナーで読み取った文書をドキュメントボックスに蓄積したときのログ
蓄積文書（スキャナー）ダウンロード	Scanner: Stored File Downloading	Web Image Monitor からドキュメントボックスに蓄積された文書をダウンロードしたときのログ
スキャナー：蓄積文書送信	Scanner: Stored File Sending	スキャナー機能で蓄積された文書を送信したときのログ
スキャナー：蓄積文書 URL リンク送信	Scanner: Stored File URL Link Sending	蓄積文書の URL アドレスをメール送信したときのログ
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

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：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
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：ドキュメントボックスに蓄積	Printer: Document Server Sending	プリンタードライバーの設定で印刷方法を [ドキュメントボックス] を選択し、ドキュメントボックスに文書を蓄積したときのログ
レポート印刷	Report Printing	操作部からレポートを出力したときのログ

本機を管理する

設定項目	Log Type の属性値	収集するログ
結果レポート印刷/ メール通知	Result Report Printing/E-mailing	レポートの印刷またはメールの送信によ って、ジョブの実行結果を通知したとき のログ
スキャナー：TWAIN ドライバー読み取 り	Scanner: TWAIN Driver Scanning	TWAIN ドライバーで文書を読み取りした 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
ファクス：送信	Fax: Sending	本機からファクスを送信したときのログ
ファクス：PC ファ クス送信	Fax: LAN-Fax Sending	パソコンからファクスを送信したとき のログ
ファクス：文書蓄積	Fax: Storing	ファクス機能を使用して本機に文書を蓄 積したときのログ
ファクス：蓄積文書 印刷	Fax: Stored File Printing	ファクス機能を使用して本機に蓄積した 文書を印刷したときのログ
蓄積文書（ファク ス）ダウンロード	Fax: Stored File Downloading	Web Image Monitor からドキュメントボ ックスに蓄積された文書をダウンロード したときのログ
ファクス：受信	Fax: Receiving	本機がファクスを受信したときのログ
ファクス：受信と配 信	Fax: Receiving and Delivering	本機で受信したファクスを配信したとき のログ
ファクス：受信と文 書蓄積	Fax: Receiving and Storing	本機で受信したファクスを蓄積したとき のログ

アクセスログ

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	ドキュメントボックスに文書が生成されたときのログ
蓄積文書削除	Stored File Deletion	ドキュメントボックスから文書が削除されたときのログ
蓄積文書一括削除	All Stored Files Deletion	ドキュメントボックスに蓄積された文書が一括で削除されたときのログ
HDD フォーマット*2	HDD Format	ハードディスクを初期化したときのログ
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	ログに関する設定を変更したときのログ
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、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*3	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	本体電源投入時など、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

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	本体電源投入時など、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
文書アクセス権変 更	File Access Privilege Change	蓄積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
キャプチャー失敗	Capture Error	文書のキャプチャーに失敗したときのログ
機器設定	Machine Configuration	機器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	トラッキングに失敗したときのログ

本機を管理する

設定項目	Log Type の属性値	収集するログ
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	機器の設定情報ファイルをインポートしたときのログ
機器設定情報のエ クスポート	Export Device Setting Information	機器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	主電源を入れたときのログ
主電源 OFF	Main Power Off	主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

本機を管理する

- 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、以下の項目のログが収集されます。
 - HDD フォーマット
 - 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。
- 「ファームウェア:構成」のログは本体電源投入後、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、それぞれのログに対して、以下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。

ログに対して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”

ログの並び方

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。

ログのデータ形式の違い

- ジョブログの場合
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。
- アクセスログの場合
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 ログの場合

本機を管理する

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。

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			

CJC001

- 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。

共通項目

項目名	説明
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. 185「収集できるログ項目」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。

本機を管理する

項目名	説明
Result*1	操作、または事象の結果が記録されます。 ジョブログでは、操作が正常に終了すると「Succeeded」、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。

項目名	説明
Status	<p>操作、または事象の状態が記録されます。</p> <ul style="list-style-type: none"> ▪ ジョブログは、正常終了すると「Completed」と記録されます。 異常終了すると「Failed」と記録されます。 進行中は、「Processing」と記録されます。 ▪ ジョブログのソース、およびターゲットでは、正常終了すると「Completed」と記録されます。 異常終了すると「Failed」と記録されます。 進行中は、「Processing」と記録されます。 エラーが発生したときは「Error」と記録されます。 中断したときは「Suspended」と記録されます。 ▪ アクセスログでは、正常終了すると「Succeeded」と記録されます。 異常終了すると「Password Mismatch」（パスワード不一致）、「User Not Programmed」（ユーザー未登録）、「Other Failures」（その他失敗）、「User Locked Out」（ユーザーロックアウト中）、「File Password Mismatch」（文書パスワード不一致）、「No Privileges」（権限無し）、「Failed to Access File」（使用中ファイルへのアクセス・セキュリティー強化モードのロック中）、「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）、「Power Failure」（電源断によるキャプチャー失敗）、「Lost File」（文書消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）のいずれかが記録されます。

本機を管理する

項目名	説明
Status (ユーザー別カウンターク リア結果用、全ユーザーカ ウンタークリア結果用)	ユーザー別カウンター、または全ユーザーカウンターのクリアに失敗したときは、「Failure in some or all parts」(失敗もしくは一部失敗)と記録されます。

項目名	説明
<p>Status (機器情報のインポート、 エクスポート用)</p>	<p>操作、または事象の状態が記録されます。 他ユーザーによるインポート、もしくはエクスポート 処理が実行されているときは、「Importing/Exporting by Other User」と記録されます。 出力先と接続が失敗したときは、「Connection Failed with Remote Machine」と記録されます。 出力先への書き込みエラーが発生したときは、「Write Error to Remote Machine」と記録されます。 指定ファイルが不適合だったときは、「Specified File: Incompatible」と記録されます。 指定ファイルとのフォーマットエラーが発生したとき は、「Specified File: Format Error」と記録されます。 指定ファイルが見つからなかったときは、「Specified File: Not Exist」と記録されます。 指定ファイルへの操作権限がなかったときは、 「Specified File: No Privileges」と記録されます。 指定ファイルへのアクセスエラーが発生したときは、 「Specified File: Access Error」と記録されます。 外部メディアの容量が満杯だったときは、「Memory Storage Device Full」と記録されます。 外部メディアが異常だったときは、「Memory Storage Device Error」と記録されます。 暗号化に失敗したときは、「Encryption Failed」と記 録されます。 複合化に失敗したときは、「Decoding Failed」と記録 されます。 共通鍵がなかったときは、「Common Key Not Exist」と 記録されます。 通信異常が発生したときは、「Connection Error」と記 録されます。</p>

項目名	説明
Status Supplement	<p>ログの状態が異常終了 (Failed) したときに記録されます。</p> <p>異常終了しなかったときは、何も記録されません。</p> <p>ユーザーがキャンセルしたときは、「Cancelled by User」と記録されます。</p> <p>入力中の異常終了のときは、「Input Failure」と記録されます。失敗した理由は下段に記載している各入力情報 (Source) を参照してください。</p> <p>出力中の異常終了のときは、「Output Failure」と記録されます。失敗した理由は下段に記載している各出力情報 (Target) を参照してください。</p> <p>ジョブの実行前に検知したエラーは、「Other Error」と記録されます。</p> <p>電源が切れたときは、「Power Failure」と記録されます。</p>

項目名	説明
<p>Status Supplement (Source が Scan File の場合)</p>	<p>動作中に課金装置が抜けたときは、「External Charge Unit Disconnected」と記録されます。</p> <p>合成コピーの実行時に原稿が不足していたときは、「Insufficient No. of Original for Overlay」と記録されます。</p> <p>ドキュメントボックスで蓄積可能なページ数を越えたときは、「Exceed Max. Stored Page (File Storage)」と記録されます。</p> <p>ドキュメントボックスで蓄積可能な文書数を越えたときは、「Exceed Max. Stored File (File Storage)」と記録されます。</p> <p>ドキュメントボックスで蓄積可能なハードディスクの容量を超えたときは、「Hard Disk Full (File Storage Memory)」と記録されます。</p> <p>メールサイズの制限を超えたときは、「Exceeded Max. Email Size」と記録されます。</p> <p>1文書のサイズ上限値を超えたときは、「Exceeded Max. File Size」と記録されます。</p> <p>自動原稿送り装置による読取りエラーが発生したときは、「Scanner Error」と記録されます。</p> <p>タイムアウトが発生したときは、「Timeout」と記録されます。</p> <p>その他のエラーが発生したときは、「Other Error」と記録されます。</p>

本機を管理する

項目名	説明
Status Supplement (Source が Stored File の場合)	<p>キャプチャー可能なページ数を越えたときは、「Exceed Max. Stored Page (Image Area)」と記録されます。</p> <p>キャプチャー可能なハードディスクの容量を超えたときは、「Hard Disk Full (Image Area)」と記録されます。</p> <p>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ときは、「Memory Full」と記録されます。</p> <p>本機に搭載されていないPDL、もしくはポートを利用したときは、「Print Data Error」と記録されます。</p> <p>異なる機種ドライバーを利用したとき、ネットワーク障害が発生したとき、PC FAX ドライバーからキャンセルしたとき、もしくはファクスの通信障害が発生したときは、「Data Transfer Interrupted」と記録されます。</p> <p>その他のエラーが発生したときは、「Other Error」と記録されます。</p>
Status Supplement (Source が Received File の場合)	<p>ファクスの受信ができなかったときは、「Reception Error」と記録されます。</p>

項目名	説明
Status Supplement (Source が Printer の場合)	<p>受付可能なジョブ数を超えたときは、「Over Job Limit」と記録されます。</p> <p>不正なあて先を指定したとき、もしくはあて先の指定桁数が 41 桁以上を超えたときは、「Specifying Destination Error」と記録されます。</p> <p>回線の指定に誤りがあったときは、「Specifying Line Error」と記録されます。</p> <p>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ときは、「Memory Full」と記録されます。</p> <p>本機の認証に失敗したときは、「Authentication Failed (Access Restricted)」と記録されます。</p> <p>異なる機種ドライバーを利用したとき、ネットワーク障害が発生したとき、PC FAX ドライバーからキャンセルしたとき、もしくはファクスの通信障害が発生したときは、「Data Transfer Interrupted」と記録されます。</p> <p>本機に搭載されていない PDL、もしくはポートを利用したときは、「Print Data Error」と記録されます。</p> <p>ドキュメントボックスで蓄積可能なページ数を超えたときは、「Exceed Max. Stored Page (File Storage)」と記録されます。</p> <p>ドキュメントボックスで蓄積可能な文書数を超えたときは、「Exceed Max. Stored File (File Storage)」と記録されます。</p> <p>その他のエラーが発生したときは、「Other Error」と記録されます。</p>
Status Supplement (Source が Report の場合)	<p>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。</p>

項目名	説明
<p>Status Supplement (Target が Store の場合)</p>	<p>動作中に課金装置が抜けたときは、「External Charge Unit Disconnected」と記録されます。</p> <p>ログインしたユーザーの利用量制限枚数を超えたときは、「Exceeded Print Volume Use Limitation」と記録されます。</p> <p>タイムアウトが発生したときは、「Timeout」と記録されます。</p> <p>文書や機能の利用権限がなかったときは、「No Privilege」と記録されます。</p> <p>ドキュメントボックスで蓄積可能なページ数を超えたときは、「Exceed Max. Stored Page (File Storage)」と記録されます。</p> <p>ドキュメントボックスで蓄積可能な文書数を超えたときは、「Exceed Max. Stored File (File Storage)」と記録されます。</p> <p>ドキュメントボックスで蓄積可能なハードディスクの容量を超えたときは、「Hard Disk Full (File Storage Memory)」と記録されます。</p> <p>指定の用紙サイズ（不定形も含む）が蓄積不可能なサイズだったときは、「Unavailable Size to Store」と記録されます。</p> <p>キャプチャー可能なページ数を超えたときは、「Exceed Max. Stored Page (Image Area)」と記録されます。</p> <p>キャプチャー可能なハードディスクの容量を超えたときは、「Hard Disk Full (Image Area)」と記録されます。</p> <p>その他のエラーが発生したときは、「Other Error」と記録されます。</p>

項目名	説明
<p>Status Supplement (Target が Send の場合)</p>	<p>タイムアウトが発生したときは、「Timeout」と記録されます。</p> <p>送信した文書が削除された、不達ファイルの保持期間を経過した文書が消去されたときは、「Transmission Failed (Data Deleted)」と記録されます。</p> <p>文書や機能の利用権限がなかったときは、「No Privilege」と記録されます。</p> <p>文書のパスワードが未入力の場合は、「Not Entered Document Password」と記録されます。</p> <p>指定したサーバーやフォルダーが見つからなかったときは、「Connection Failed with Destination」と記録されます。</p> <p>送信先の認証で失敗したときは、「Authentication Failed with Destination」と記録されます。</p> <p>送信先の記憶領域の容量がいっぱいのときは、「Transmission Failed with Memory Full」と記録されます。</p> <p>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ときは、「Memory Full」と記録されます。</p> <p>異なる機種ドライバーを利用したとき、ネットワーク障害が発生したとき、PC FAX ドライバーからキャンセルしたとき、もしくはファクスの通信障害が発生したときは、「Data Transfer Interrupted」と記録されます。</p> <p>相手先が話し中のときは、「Line Busy」と記録されます。</p> <p>相手先からの応答がなかったときは、「No Response」と記録されます。</p> <p>相手先がファクスではなかったときは、「Not Facsimile Destination」と記録されます。</p> <p>メールサイズの制限を超えたときは、「Exceeded Max. Email Size」と記録されます。</p> <p>その他のエラーが発生したときは、「Other Error」と記録されます。</p> <p>機器証明書がなかったとき、有効期限が切れていたとき、もしくは管理者のメールアドレスと証明書のメールアドレスが一致しなかったときは、「Invalid Device Certificate」と記録されます。</p> <p>宛先の証明書の有効期限が切れていたときは、</p>

項目名	説明
User Entry ID	<p>エントリーID が記録されます。</p> <p>ジョブログ、アクセスログに関する操作要求を行ったユーザーを一意に指す ID です。16 進数で出力されます。</p> <p>スーパーバイザーには 0xffffffff86 が、管理者には 0xffffffff87、0xffffffff88、0xffffffff89、0xffffffff8a が対応します。</p> <p>ユーザーやユーザーコードには 0x00000001～0xffffffffeff の範囲の値が対応します。</p> <p>ユーザー認証では、0x00000000、0xffffffff80、0xffffffff81 はシステム起動の操作を表します。</p> <p>蓄積文書とアドレス帳に対するシステム操作のときに 0xffffffff80 と 0xffffffff81 が使われ、それ以外のときは 0x00000000 が使われます。</p> <p>0xffffffff80 は、保留印刷・機密印刷・保存文書印刷の「一時置き文書自動消去設定」などによる削除とアクセス権の変更、Windows 認証時/LDAP 認証時のユーザー自動登録などのシステムによるアドレス帳更新のログに現れます。</p> <p>0xffffffff81 は、システム操作で削除することを前提とした蓄積文書の生成のときだけ使われます。</p> <p>ユーザー認証のとき、未認証利用者の操作（コピー、スキャナーなど）は、User Entry ID は 0x00000000 と 0xffffffff81 が使われます。</p> <p>蓄積文書とアドレス帳に対する操作とジョブログのときに 0xffffffff81 が使われ、それ以外のときには 0x00000000 が使われます。</p>
User Code/User Name	<p>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。</p> <p>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。</p>
Log ID	<p>ログに ID が記録されます。</p> <p>ログを一意に指す ID で、16 進数で出力されます。</p>

*1 ジョブログの「蓄積文書（ドキュメントボックス）ダウンロード」「蓄積文書印刷」「蓄積文書（スキャナー）ダウンロード」「スキャナー：蓄積文書送信」「プリンター：保存文書印刷」「蓄積文書（ファクス）ダウンロード」とアクセスログの「文書蓄積」「蓄積文書削除」のログ項目は、その事象が成功したときだけログを記録します。

アクセスログに記録される情報

項目名	説明
Access Log Type	アクセスログの種類が記録されます。 ユーザー認証のときは「Authentication」、文書のときは「Stored File」、システムのときは「System」、攻撃検知／通信のときは「Network Attack Detection/Encrypted Communication」、ファームウェアの正当性確認のときは「Firmware」、アドレス帳のときは「Address Book」と記録されます。
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。 ユーザーのログアウト操作のときは「by User's Operation」、時間経過によって自動的にログアウトされたときは「by Auto Logout Timer」と記録されます。
Login Method	認証要求を受けた経路が記録されます。 操作部からの操作は「Control Panel」、ネットワークを介した操作は「via Network」、その他からの要求は「Others」と記録されます。

項目名	説明
Login User Type	<p>ログインユーザーの種別が記録されます。</p> <p>認証ユーザーのとき、「User」と記録されます。</p> <p>ゲストの場合、「Guest」と記録されます。</p> <p>ユーザー管理者のとき、「User Administrator」と記録されます。</p> <p>文書管理者のとき、「File Administrator」と記録されます。</p> <p>機器管理者のとき、「Machine Administrator」と記録されます。</p> <p>ネットワーク管理者のとき、「Network Administrator」と記録されます。</p> <p>スーパーバイザーのとき、「Supervisor」と記録されます。</p> <p>カスタマーエンジニアのとき、「Customer Engineer (Service Mode)」と記録されます。</p> <p>その他のときは「Others」と記録されます。</p>
Target User Entry ID	<p>対象者にエントリーIDが記録されます。</p> <p>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。</p> <ul style="list-style-type: none"> ▪ ロックアウト操作 ▪ パスワード変更
Target User Code/User Name	<p>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。</p> <p>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。</p>
Registration No.	<p>操作したユーザーの登録番号が記録されます。</p>
Address Book Operation Mode	<p>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。</p>
Address Book Change Item	<p>アドレス帳のどの内容を変更したか記録されます。</p>
Client Address	<p>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。</p>

本機を管理する

項目名	説明
Lockout/Release	ロックアウト機能が働いてパスワードがロックされると「Lockout」、ロックが解除されると「Release」と記録されます。
Lockout/Release Method	手動によるロックアウト解除のときは「Manual」、解除タイマーによるロックアウト解除のときは「Auto」と記録されます。
Lockout Administrator	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。
Clear Counters	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 Range	<p>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。</p> <p>記録される情報は次のとおりです。</p> <ul style="list-style-type: none"> ▪ システム初期設定、コピー初期設定、ファクス初期設定、プリンター初期設定、スキャナー初期設定、プログラム（コピー）、プログラム（スキャナー）、プログラム（ドキュメントボックス）、Web Image Monitor 設定、Web サービス設定、システム/コピーSP、スキャナーSP、プリンターSP、ファクス SP
File to Import	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。
File Location	文書を一括削除したときの対象領域が記録されます。ハードディスクから文書が削除されると「Document Server」と記録されます。

項目名	説明
Collect Job Logs	<p>ジョブログ収集の設定を変更したかどうか記録されます。</p> <p>有効に変えたときは「Active」、無効に変えたときは「Inactive」、設定を特に変更していないときは「Not Changed」と記録されます。</p>
Collect Access Logs	<p>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。</p> <p>有効に変えたときは「Active」、無効に変えたときは「Inactive」、設定を特に変更していないときは「Not Changed」と記録されます。</p>
Collect Eco-friendly Logs	<p>eco ログ収集の設定を変更したかどうか記録されます。</p> <p>有効に変えたときは「Active」、無効に変えたときは「Inactive」、設定を特に変更していないときは「Not Changed」と記録されます。</p>
Encrypt Logs	<p>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。</p> <p>有効に変えたときは「Active」、無効に変えたときは「Inactive」、設定を特に変更していないときは「Not Changed」と記録されます。</p>
Log Type	<p>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。</p> <p>ジョブログのときは「Job Log」、アクセスログのときは「Access Log」、eco ログのときは「Eco-friendly Log」と記録されます。</p> <p>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。</p>

項目名	説明
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。 暗号化通信のときは「Encryption Communication」、非暗号化通信のときは「Cleartext Communication」と記録されます。
Machine Port No.	本機のポート番号が記録されます。
Protocol	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。 通信開始要求を受ける側 (IN) のときは、「Communication Start Request Receiver (In)」と記録されます。 通信開始要求を出す側 (OUT) のときは、「Communication Start Request Sender (Out)」と記録されます。

本機を管理する

項目名	説明
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。 ネットワーク攻撃を検知したときは、「Violation Detected」と記録されます。 ネットワーク攻撃を収束したときは、「Recovered from Violation」と記録されます。 ホスト数上限に到達して管理不能になったときは、「Max. Host Capacity Reached」と記録されます。 ホスト管理不能から復帰したときは、「Recovered from Max. Host Capacity」と記録されます。
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。

本機を管理する

項目名	説明
Add/Update/Delete Firmware	<p>ファームウェア変更の方式が記録されます。</p> <p>SD カードによる更新のときは、「Updated with SD Card」と記録されます。</p> <p>SD カードによる追加のときは、「Added with SD Card」と記録されます。</p> <p>SD カードによる削除のときは、「Deleted with SD Card」と記録されます。</p> <p>別の SD カードへの移動のときは、「Moved to Another SD Card」と記録されます。</p> <p>リモートによる更新のときは、「Updated via Remote」と記録されます。</p> <p>その他の理由による更新のときは、「Updated for Other Reasons」と記録されます。</p>
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	<p>暗号鍵の操作の種別が記録されます。</p> <p>暗号鍵をバックアップしたときは、「Back Up Machine Data Encryption Key」と記録されます。</p> <p>暗号鍵をリストアしたときは、「Restore Machine Data Encryption Key」と記録されます。</p> <p>NVRAM をクリアしたときは、「Clear NVRAM」と記録されます。</p> <p>暗号鍵更新を開始したときは、「Start Updating Machine Data Encryption Key」と記録されます。</p> <p>暗号鍵更新を終了したときは、「Finish Updating Machine Data Encryption Key」と記録されます。</p>

項目名	説明
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	設定変更を行ったカテゴリーが記録されます。 詳しくは、「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、「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、「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「SDK Tracking」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 Init Partition No.	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

項目名	説明
Source	ジョブログの入力情報が記録されます。 入力情報が原稿読み取りでは「Scan File」、文書蓄積は「Stored File」、プリンタードライバーからの印刷指示は「Printer」、ファクス受信は「Received File」、レポート印刷は「Report」と記録されます。
Start Date/Time	入力情報が「Scan File」、「Printer」、または「Received File」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「Scan File」、「Printer」、または「Received File」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。 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。

出力情報

項目名	説明
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」、送信されると「Send」と記録されます。
Start Date/Time	文書の印刷、蓄積、送信の開始日時が送信されます。
End Date/Time	文書の印刷、蓄積、送信の終了日時が送信されます。
Destination Name	出力情報が「Send」のとき、相手先のあて名名称が記録されます。

本機を管理する

項目名	説明
Destination Address	出力情報が「Send」のとき、相手先の IP アドレス、パス、またはメールアドレスが記録されます。
Stored File ID ^{*1}	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 ^{*2}	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。

ファクス送信蓄積文書をファクスメニューから印刷したとき、ジョブログは取得できません。

*1 ファクス機能では「Stored File ID」はログに記録されません。

*2 ファクス機能では「Stored File Name」はログに記録されません。

eco ログに記載される情報

項目名	説明
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。
Log ID	ログを特定する ID が記録されます。16 進の ID です。

本機を管理する

項目名	説明
Power Mode	<p>本機の電源状態（移行後）がログとして記録されます。待機状態のときは、「Standby」と記録されます。低電力状態のときは、「Low Power」と記録されます。静音状態のときは、「Silent」と記録されます。ハードディスクが起動しているときは、「HDD On」と記録されます。エンジンが停止しているときは、「Engine Off」と記録されます。コントローラーが停止しているときは、「Controller Off」と記録されます。STR (Suspend To RAM) 状態のときは、「STR」と記録されます。静音印刷状態のときは、「Silent Print」と記録されます。低音印刷状態のときは、「Low Power Print」と記録されます。</p>
Log Type	<p>ジョブログのログの種類が記録されます。</p>
Job Interval Times (seconds)	<p>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。</p>
Job Times (seconds)	<p>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。</p>
Consumption of paper (Big Size)	<p>1時間ごとの片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。</p>
Consumption of paper (Small Size)	<p>1時間ごとの片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。</p>

本機を管理する

項目名	説明
Consumption of paper (Both Side/Big Size)	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。
Consumption of paper (Both Side/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。
Measuring the power state	消費電力量計測時の電源状態が記録されます。 コントローラ待機状態は、「Controller Standby」が記録されます。 STR (Suspend to RAM) 状態は、「STR」が記録されます。 主電源 OFF 状態は、「Main Power Off」が記録されます。 読取/印刷状態は、「Scanning/Printing」が記録されます。 印刷状態は、「Printing」が記録されます。 読取状態は、「Scanning」が記録されます。 エンジン待機状態は、「Engine Standby」が記録されます。 エンジン低電力状態は、「Engine Low」が記録されます。 エンジン静音状態は、「Engine Night」が記録されます。 機器全体の消費電力は、「Engine Total」が記録されます。
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

本機を管理する

カテゴリー	属性	説明
User Lockout Policy	<ol style="list-style-type: none"> 1. Lockout 2. Number of Attempts before Lockout 3. Lockout Release Timer 4. Lock Out User for 	<ol style="list-style-type: none"> 1. ロックアウトの有効 (Active)、無効 (Inactive) が記録されます。 2. ログインパスワード入力許容回数 (回) が記録されます。 3. 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. ロックアウト解除までの時間が記録されます。
Auto Logout Timer	<ol style="list-style-type: none"> 1. Auto Logout Timer 2. Auto Logout Timer (seconds) 	<ol style="list-style-type: none"> 1. 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. オートログアウトが働くまでの時間が記録されます。

カテゴリー	属性	説明
Device Certificate	<ol style="list-style-type: none"> 1. Operation Mode 2. Certificate No. 3. Certificate No. (XXX) 「XXX」には、次のいずれかが入ります。 <ul style="list-style-type: none"> ▪ SSL/TLS ▪ IEEE 802.1X ▪ S/MIME ▪ IPsec ▪ デジタル署名 PDF ▪ デジタル署名 PDF/A 	<ol style="list-style-type: none"> 1. 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「InstallIntermediateCertificate」と記録されます。 中間証明書を削除したときは「DeleteIntermediateCertificate」と記録されます。 2. 操作対象の証明書の番号が記録されます。 3. 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ったときは「Do not Use」と記録されます。

本機を管理する

カテゴリー	属性	説明
IPsec	<ol style="list-style-type: none"> 1. IPsec 2. Encryption Key Auto Exchange / Encryption Key Manual Exchange: Setting1-4: Remote Address 3. Encryption Key Auto Exchange: Setting1-4, Default): Security Level 4. Encryption Key Auto Exchange: Setting1-4, Default): Authenticat ion Method 	<ol style="list-style-type: none"> 1. IPsecの有効 (Active)、無効 (Inactive) が記録されます。 2. リモートアドレスが記録されます。 3. 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. 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。

本機を管理する

カテゴリー	属性	説明
S/MIME	<ol style="list-style-type: none"> 1. Operation Mode 2. When Sending E-mail by Scanner 3. When Transferring by Fax 4. When Sending E-mail by Fax 5. When E-mailing TX Results by Fax 6. When Transferring Files Stored in Document Server (Utility) 	<ol style="list-style-type: none"> 1. 動作モードが記録されます。 2. スキャナーを利用したメール送信時の署名が記録されます。 3. ファクス転送時の署名が記録されます。 4. ファクスを利用したメール送信時の署名が記録されます。 5. ファクスを利用した通知メール送信時の署名が記録されます。 6. ドキュメントボックス（ユーティリティー）を利用した蓄積文書転送時の署名が記録されます。

操作部をカスタマイズする

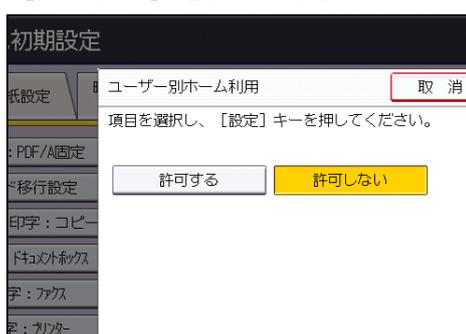
ユーザーごとのホーム画面の設定を有効にすると、ホーム画面のアイコンの配置などをユーザーごとに設定できます。

ユーザー別ホームを設定する

ユーザー別ホームの利用を許可します。

ユーザーがログインしたときに、そのユーザー専用のホーム画面が表示されます。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を4回押します。
5. [ユーザー別ホーム利用] を押します。
6. [許可する] を押します。



7. [設定] を押します。
8. ログアウトします。

↓ 補足

- Web Image Monitor からも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。
- [許可しない] に設定しても、各ユーザーのホーム情報は保持されます。再度、[許可する] に設定したときに、再び利用できます。

ユーザー別ホーム利用時の注意事項

以下の注意事項を確認して運用してください。

- アドレス帳にユーザーが登録された時点で、そのユーザー専用のホームが作成されます。そのときのユーザー別ホームは、デフォルトホームの設定値（アイコン配置）です。
- メニュープロテクトが [レベル 1]、または [レベル 2] に設定されているとき、ユーザーは、その機能のプログラム登録、編集、削除ができません。ただし、ユーザー別ホー

本機を管理する

ムへのアイコン追加は制限されません。

- メニュープロテクトを [レベル 1]、または [レベル 2] に設定したときは、管理者が必要なプログラムを作成してください。
- 管理者によって、使用できる機能が制限されたユーザーのホーム画面には、制限された機能のアイコンは表示されません。
- アドレス帳からユーザーを削除すると、そのユーザーのホーム情報も削除されます。
- ユーザーがプログラムを編集したとき、そのプログラムのアイコンをユーザー別ホームに配置しているすべてのユーザーに反映されます。
- ユーザーがプログラムを削除したとき、そのプログラムのアイコンを配置しているすべてのユーザーのホーム画面からアイコンが削除されます。
- ユーザー別ホームは、ユーザーによって管理、運用されるため、管理者が各ユーザーのホーム情報（ユーザー別ホームのカスタマイズ状況）を確認することはできません。

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。

インポート・エクスポートできるデータ

- コピー/ドキュメントボックス初期設定
- プリンター初期設定
- スキャナー初期設定
- ファクス初期設定
- プログラム（ドキュメントボックス）
- プログラム（コピー機能）
- プログラム（スキャナー機能）
- Web Image Monitor 設定
- Web サービス設定
- システム初期設定*1 *2

*1 年月日の設定、機器証明書を使用する設定、画像の補正值など機体ごとに調整する項目はインポート・エクスポートの対象外です。

*2 実行するだけの項目と閲覧するだけの項目は、インポート・エクスポートの対象外です。

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（ファクス機能）
- プログラム（プリンター機能）
- パスワードの設定を含むスキャナー機能のプログラム
- コピー初期設定のユーザースタンプ
- telnet から設定する設定

本機を管理する

- 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）

↓ 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ことで同じ設定にできます。
- ホーム画面に画像を挿入しているときは、JPG 形式の画像ファイルもエクスポートされます。
- 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。
- Web Image Monitor または、外部ツールでアドレス帳のバックアップ/リストアをしているときに、機器情報のインポートをすると、[セキュリティー強化] の [パスワードポリシー] が設定されないことがあります。この場合は、インポート後に手動でパスワードポリシーを設定してください。
- 使用できる外部メディアは SD カードです。ただし、すべての SD カードで動作を保証するものではありません。推奨する外部メディアについては販売店にご確認ください。
- 使用できる SD カードの容量は 32GB までです。

機器情報をエクスポートする

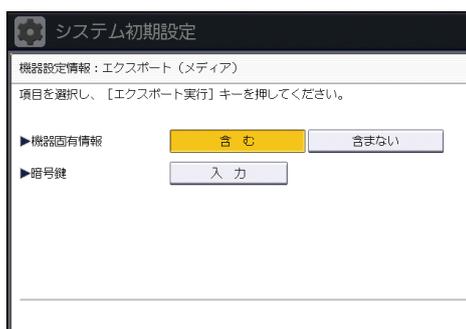
操作部から機器情報をエクスポートするときは、SD カードに保存されます。

1. SD カードを操作部側面のメディアスロットに挿入します。
2. 操作部からすべての権限を持つ管理者がログインします。
3. [システム初期設定] を押します。
4. [管理者用設定] を押します。
5. [▼次へ] を 3 回押します。
6. [機器設定情報：エクスポート（メディア）] を押します。

本機を管理する



7. エクスポート条件を設定します。



- 機器固有情報の [含む]、[含まない] を選択します。機器固有情報とは、IP アドレス、ホスト名、ファクス番号などです。
- 暗号鍵を設定します。

8. [エクスポート実行] を押します。

9. [実行] を押します。

10. [確認] を押します。

11. ログアウトします。

補足

- 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。

機器情報をインポートする

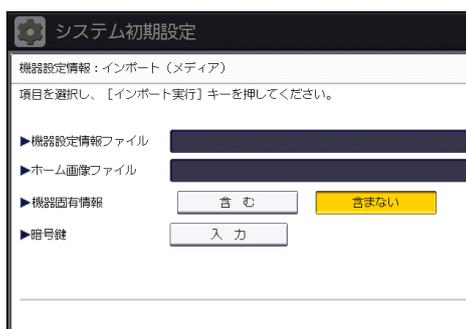
SD カードに保存された機器情報をインポートします。

1. SD カードを操作部側面のメディアスロットに挿入します。
2. 操作部からすべての権限を持つ管理者がログインします。
3. [システム初期設定] を押します。
4. [管理者用設定] を押します。
5. [▼次へ] を 3 回押します。
6. [機器設定情報: インポート (メディア)] を押します。

本機を管理する



7. インポート条件を設定します。



- 機器設定情報ファイルの [選択] を押して、インポートするファイルを選択します。
- ホーム画面に挿入するときは、ホーム画像ファイルの [選択] を押して、ファイルを選択します。
- 機器固有情報の [含む]、[含まない] を選択します。機器固有情報とは、IP アドレス、ホスト名、ファクス番号などです。
- エクスポート時に設定した暗号鍵を設定します。

8. [インポート実行] を押します。

9. [実行] を押します。

10. [確認] を押します。

本機が再起動されます。

補足

- イン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。

eco 指数カウンターを管理する

ユーザー認証を使用しているとき、ログイン時に eco 指数カウンターのインフォメーションを表示します。

eco 指数カウンターは、トータルの出力枚数に対して両面印刷、集約印刷の利用率です。トナーや用紙の節約がどの程度であるかを eco 指数として表示します。

↓ 補足

- ユーザー認証にベーシック認証、Windows 認証、またはLDAP 認証を使用しているときは、ユーザーごとの eco 指数カウンターを集計し、表示します。
- ユーザー認証にユーザーコード認証を使用しているとき、またはユーザー認証が無効なときは、機器全体の eco 指数カウンターを集計し、表示します。

eco 指数カウンターの表示を設定する

eco 指数カウンターの集計期間や管理者のメッセージを設定します。

1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を 3 回押します。
5. [eco 指数カウンター集計期間／管理者メッセージ設定] を押します。
6. 設定を変更します。
7. [設定] を押します。
8. [確認] を押します。
9. ログアウトします。

eco 指数カウンターの設定項目

集計期間

eco 指数カウンターの集計期間を設定します。

[指定日数ごと] を選択したときは、指定した日数で eco 指数カウンターが集計されま

す。

- 週ごと
- 月ごと
- 指定日数ごと
- 集計しない

工場出荷時の設定：集計しない

管理者メッセージ

本機を管理する

メッセージを選択します。

〔固定メッセージ〕は、あらかじめ設定されているメッセージが表示されます。

〔任意メッセージ〕は、機器管理者がメッセージを自由に設定できます。

- 固定メッセージ
- 任意メッセージ

工場出荷時の設定：固定メッセージ

インフォメーション画面表示

ログイン時のインフォメーションに eco 指数を表示するかどうか設定します。

- する
- しない

工場出荷時の設定：しない

表示のタイミング

インフォメーションを表示するタイミングを設定します。

- 毎ログイン時
- 初回ログイン時のみ

工場出荷時の設定：毎ログイン時

機器の eco 指数カウンターをクリアする

機器の eco 指数カウンターをクリアできます。

1. 操作部から機器管理者がログインします。
2. 〔システム初期設定〕を押します。
3. 〔管理者用設定〕を押します。
4. 〔eco 指数カウンター表示／クリア〕を押します。
5. 〔現在値をクリア〕または〔現在値と前回値をクリア〕を押します。
6. 〔実行〕を押します。
7. ログアウトします。

ユーザー別の eco 指数カウンターをクリアする

ユーザー別の eco 指数カウンターをクリアできます。

1. 操作部から機器管理者がログインします。
2. 〔システム初期設定〕を押します。
3. 〔管理者用設定〕を押します。
4. 〔ユーザー別 eco 指数カウンター表示／クリア〕を押します。
5. 〔現在値をクリア〕または〔現在値と前回値をクリア〕を押します。
6. 〔実行〕を押します。
7. ログアウトします。

本機を管理する

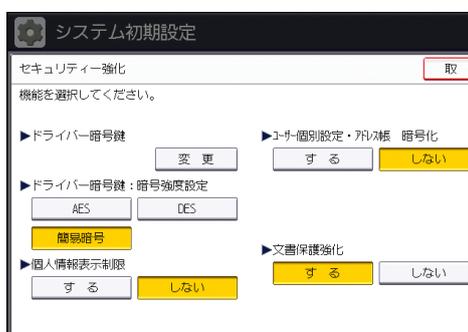
↓ 補足

- すべてのユーザーの eco 指数カウンターがクリアされます。任意のユーザーについて、個別に eco 指数カウンターをクリアすることはできません。

セキュリティー強化機能を設定する

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

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. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [セキュリティー強化] を押します。
6. 設定を変更する項目を押して、設定を変更します。



7. [設定] を押します。
8. ログアウトします。

↓ 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。

セキュリティー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. 156「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。

本機を管理する

[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
- 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。たとえば、管理者として認証されていないとき、Network Monitor for Admin から SNMP を使ってジョブ履歴を確認するとき、個人情報がわからないように「*****」表示にできます。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

ユーザー個別設定・アドレス帳 暗号化

ユーザー管理者が設定します。

本機のユーザー個別設定情報、および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、暗号化によりユーザー個別設定と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. 73 「アドレス帳を暗号化する」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。

本機を管理する

文書保護強化が設定されているときは、画面にが表示されます。

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となります。

- する
- しない

工場出荷時の設定：しない

宛先利用制限（ファクス）、宛先利用制限（スキャナー）

ユーザー管理者が設定します。

ファクスやスキャナーの送信先を機器のアドレス帳に登録されている相手先に限定します。ユーザーが送信時に相手先を直接入力することはできません。

「宛先利用制限（スキャナー）」が [する] に設定されているときは、ユーザーはファクス番号だけ、登録できます。

LDAP 検索で検索した宛先を利用できます。

SMTP 受信したメールを配信するとき、宛先利用制限は使用できません。

設定方法は、P. 55「宛先表の利用を制限する」を参照してください。

- する
- しない

工場出荷時の設定：しない

個人宛先登録制限（ファクス）、個人宛先登録制限（スキャナー）

ユーザー管理者が設定します。

「宛先利用制限（ファクス）」か「宛先利用制限（スキャナー）」またはその両方を [しない] に設定しているときに設定できます。通常、ユーザーがファクスやスキャナーの相手先を直接入力したときに、[宛先登録] を押すことで、アドレス帳に入力した相手先を登録できます。「個人宛先登録制限（ファクス）」か「個人宛先登録制限（スキャナー）」またはその両方を [する] に設定すると、ユーザーは直接入力して送信先を指定できますが、[宛先登録] を使って、アドレスに登録できません。

また、個人宛先登録制限が設定されているときでも、宛先に登録されているユーザーは、パスワードを変更できます。パスワード以外の項目は、ユーザー管理者のみ変更できます。

- する
- しない

工場出荷時の設定：しない

受信指定先への転送（ファクス）

機器管理者が設定します。

ファクスのメモリー転送や中継送信機能を使用すると、機器に蓄積された文書が転送、

本機を管理する

配信されることがあります。[禁止する]に設定するとメモリー転送や、中継送信機能で蓄積した文書を転送することを禁止します。受信した文書が不用意に転送されることを防止できます。

- 禁止する
- 禁止しない

工場出荷時の設定：**禁止しない**

[禁止する]に設定すると、次の機能が無効になります。

- メモリー転送
- Fコード中継ボックス
- Fコード親展ボックスからの配信
- Fコード掲示板
- SMTP 受信したメールの配信
- ファクス受信配信

詳しくは、『ファクス』「受信するときの機能」を参照してください。

遠隔診断（ファクス）

「管理者認証管理」と「ユーザー認証管理」を設定していないときだけ、設定できます。サービス実施店から電話回線を使用して、アドレス帳を登録できます。[禁止する]に設定すると適切なサービスが受けられないことがあります。[禁止する]に設定するときは、サービス実施店に相談してください。

「管理者認証管理」と「ユーザー認証管理」を設定しているときは、遠隔診断機能は使用できません。

- 禁止する
- 禁止しない

工場出荷時の設定：**禁止しない**

実行中ジョブへの認証の実施

機器管理者が設定します。

コピーの中断、プリンター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可能です。[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]に設定するとコピー、印刷を行ったユーザー、および機器管理者が操作可能です。

[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、コピー機能やプリンター機能などの操作権限がユーザーになければ、コピーの中断、およびプリンターのジョブキャンセルはできません。

本機を管理する

「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なくなります。

[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、アップデートを実施できます。

- 禁止する
- 禁止しない

工場出荷時の設定：禁止しない

ファームウェア構成変更

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]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、アクセス攻撃を検出しません。

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に対する応答時間を遅らせ、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」の範囲でテンキーで入力し、[#] を押します。
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。

本機を管理する

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」の範囲でテンキーで入力し、[#] を押します。

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、ログイン要求に対する応答を遅らせる時間を設定します。

「0-9」の範囲でテンキーで入力し、[#] を押します。

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」の範囲でテンキーで入力し、[#] を押します。

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。

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、メールにて機器管理者に通知します。

許容回数を「0」に設定した場合、パスワード攻撃の検知は行いません。

- 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」の範囲でテンキーで入力し、[#] を押します。

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」の範囲でテンキーで入力し、[#] を押します。

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。

アクセスセキュリティ設定

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機器にログインしようとしたとき、ユーザーの認証操作と機器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くなる場合があります。

「アクセスセキュリティ設定」を [する] に設定すると、そのような誤ったロックアウトを回避できます。

- 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」の範囲でテンキーで入力し、[#] を押します。
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」の範囲でテンキーで入力し、[#] を押します。
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」の範囲でテンキーで入力し、[#] を押します。
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」の範囲でテンキーで入力し、[#] を押します。
工場出荷時の設定：3 秒
- しない
工場出荷時の設定：しない

その他のセキュリティー機能

情報漏洩を防止するための設定について説明します。

また、ユーザー認証を設定したときに制限がかかる機能について説明します。

ファクス機能

本機はファクスのセキュリティーに関するガイドラインである FASEC 1 に適合したファクスセキュリティー機能を搭載しています。

詳しくは、『ファクス』「FASEC 1」を参照してください。

レポートやリストで相手先/送信者名を表示しない

機器管理者が設定します。

[ファクス初期設定]にある[導入設定]の[パラメーター設定]の「スイッチ 04」の「ビット番号 4」、および「スイッチ 04」の「ビット番号 5」を設定すると、相手先、および送信者名の表示・非表示を設定できます。受信側や送信側の情報がわからないため、不特定のユーザーに受信側（本機）と送信側の情報の漏洩を防止できます。

詳しくは、『ファクス』「ファクス初期設定」を参照してください。

蓄積受信文書ユーザー設定

文書管理者が設定します。

[ファクス初期設定]にある[受信設定]の[蓄積受信文書ユーザー設定]を[する]に設定することで、ハードディスクに蓄積されているファクス受信文書を管理するユーザーを設定できます。

設定されたユーザーがネットワークから本機にアクセスするときは、ユーザーコードまたは、ログインユーザー名とログインパスワードの入力が必要です。認証で認められたユーザーだけ、管理できます。

詳しくは、『ファクス』「ファクス初期設定」を参照してください。

通信管理レポートの出力

ユーザー認証を設定しているときは、通信履歴内の個人情報が自動で出力されることを防ぐため、通信管理レポートは自動で出力されません。通信管理レポートに記載される情報は、200 通信を超えると、通信ごとに上書きされます。

以下のどちらかの方法で、通信履歴の上書きを防止します。

- [ファクス初期設定]にある[導入設定]の[パラメーター設定]の「スイッチ 03」、「ビット番号 7」を設定し、通信管理レポートを自動出力する設定に変更します。
- [ファクス初期設定]にある[導入設定]の[パラメーター設定]の「スイッチ 21」、「ビット番号 4」を設定し、通信管理情報をメールで送信します。

本機を管理する

詳しくは、『ファクス』「ファクス初期設定」を参照してください。

誤った相手先への送信を防止する

ファクスを送信するとき、相手先のファクス番号の入力を2度繰り返して確認します。1度目と2度目で入力したファクス番号が異なるときは送信されないため、誤った相手先への送信を防止できます。

この機能を使用するときは、サービス実施店に連絡してください。

ファクス番号入力の操作設定方法は、『ファクス』「相手先を指定する」「宛先を繰り返し入力する」を参照してください。

スキャナー機能

履歴満杯時印刷

ユーザー認証を設定しているときは、送信/配信履歴内の個人情報自動で出力されることを防止するため、送信履歴満杯時印刷は[しない(送信不可)]に設定されます。送信履歴満杯時印刷に記載される情報が250件を超えると、スキャナー送信できません。そのときは「送信履歴印刷」または「送信履歴消去」を行ってください。

送信履歴印刷を自動で実行させるときは、「送信履歴満杯時印刷設定」を[する]に設定します。

詳しくは『スキャナー』「スキャナー初期設定」を参照してください。

システム状態

操作部の[状態確認]キーで本機の状態や設定内容を確認できます。管理者認証が設定されているときは、管理者としてログインしたときだけ、[保守/問い合わせ/機器情報]に[機器アドレス/ファクス番号]が表示されます。

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。

機器の操作をお客様に限定する

使用している機器を管理者の認証がなければ操作ができないようにしたり、サービス実施店からの遠隔操作によるアドレス帳の登録を禁止できます。

弊社ではお客様の情報につきまして厳重な管理を行っております。さらに管理者の認証を行ってから操作させていただくことで、お客様の管理の元でサービスエンジニアが作業します。

設定項目

サービスモード移行禁止設定

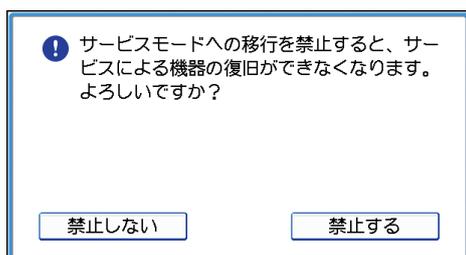
サービスモードは、カスタマーエンジニアが点検や修理をするときに使用する設定です。サービスモード移行禁止設定を「禁止する」に設定すると、点検や修理にお伺いしたカスタマーエンジニアが機器を操作するときに一度機器管理者がログインして、サービスモード移行禁止設定を解除しないとサービスモードを使うことはできません。必ず機器管理者が確認した状態で点検や修理をすることになります。

サービスモード移行禁止設定を有効にする

1. 操作部から機器管理者がログインします。
2. 「システム初期設定」を押します。
3. 「管理者用設定」を押します。
4. 「▼次へ」を2回押します。
5. 「サービスモード移行禁止設定」を押します。



6. 「禁止する」を押して、「設定」を押します。
7. 「禁止する」を押します。



8. ログアウトします。

より安全にお使いいただくために

セキュリティーが保たれた状態で本機をお使いいただくための設定項目と設定値について説明します。

操作部から設定する項目

セキュリティーの保たれた状態にするために、本機の操作部から設定する初期設定項目を、次のように設定してください。

システム初期設定

タブ項目	設定項目	設定値
時刻タイマー設定	オートログアウト時間設定	[する] :180 秒以下 本設定では、Web Image Monitor からログアウトするまでの時間は変更できません。 詳しくは、P. 54 「オートログアウト時間設定」を参照してください。
管理者用設定	ユーザー認証管理	[ベーシック認証] を選択し、「プリンタージョブ認証」を [すべて] に設定します。 詳しくは、P. 28 「ベーシック認証」を参照してください。
管理者用設定	管理者認証管理 →ユーザー管理	[する] を選択し、「適用初期設定項目」で [管理者用設定] を選択します。 詳しくは、P. 10 「管理者認証を設定する」を参照してください。
管理者用設定	管理者認証管理 →機器管理	[する] を選択し、「適用初期設定項目」ですべての項目を選択します。 詳しくは、P. 10 「管理者認証を設定する」を参照してください。

本機を管理する

タブ項目	設定項目	設定値
管理者用設定	管理者認証管理 →ネットワーク 管理	[する] を選択し、「適用初期設定項目」で [インターフェース設定]、[ファイル転送設定]、[管理者用設定] を選択します。 詳しくは、P. 10「管理者認証を設定する」を参照してください。
管理者用設定	管理者認証管理 →文書管理	[する] を選択し、「適用初期設定項目」で [管理者用設定] を選択します。 詳しくは、P. 10「管理者認証を設定する」を参照してください。
管理者用設定	セキュリティー 強化 →SNMPv1, v2 に よる設定	[禁止する] 詳しくは、P. 230「セキュリティー強化機能を設定する」を参照してください。
管理者用設定	セキュリティー 強化→ドライバ ー暗号鍵：暗号 強度設定	[AES] 詳しくは、P. 230「セキュリティー強化機能を設定する」を参照してください。
管理者用設定	セキュリティー 強化→実行中ジ ョブへの認証の 実施	[アクセス権限] 詳しくは、P. 230「セキュリティー強化機能を設定する」を参照してください。
管理者用設定	セキュリティー 強化→パスワー ドポリシー	「複雑さ制限」：[複雑度 1] 以上 「最小文字数」：8 文字以上 詳しくは、P. 230「セキュリティー強化機能を設定する」を参照してください。
管理者用設定	ネットワークセ キュリティーレ ベル	[レベル 2] プリンタードライバーや Web Image Monitor で 本体の状態を取得するときは、Web Image Monitor から「SNMP」を有効にします。 詳しくは、P. 98「ネットワークセキュリティー レベルを設定する」を参照してください。

本機を管理する

タブ項目	設定項目	設定値
管理者用設定	サービスモード移行禁止設定	[禁止する] 詳しくは、P. 240「機器の操作をお客様に限定する」を参照してください。
管理者用設定	機器データ暗号化設定	[暗号化] をクリックし、ハードディスクに残すための初期化しないデータを選択する画面で [全データ] を選択します。 すでに [暗号化] が設定されているときは、再度設定する必要はありません。 詳しくは、P. 76「機器のデータを暗号化する」を参照してください。

スキャナー初期設定

タブ項目	設定項目	設定値
導入設定	メニュープロテクト設定	[レベル 2] 詳しくは、P. 58「メニュープロテクト」を参照してください。

ファクス初期設定

タブ項目	設定項目	設定値
受信設定	蓄積受信文書ユーザー設定	[する] を設定したあと、受信文書を扱うユーザーまたはグループを指定します。 詳しくは、P. 238「その他のセキュリティー機能」を参照してください。
導入設定	メニュープロテクト設定	[レベル 2] 詳しくは、P. 58「メニュープロテクト」を参照してください。

補足

- SNMP の設定は、Web Image Monitor の [設定] の [SNMP] で行います。

本機を管理する

- 蓄積受信文書ユーザー設定は、『ファクス』「ファクス初期設定」を参照してください。

Web Image Monitor から設定する項目

セキュリティの保たれた状態にするために、Web Image Monitor から初期設定項目を以下のように設定してください。

カテゴリー	設定項目	設定値
機器→ログ	ジョブログ収集	[有効]
機器→ログ	アクセスログ収集	[有効]
セキュリティ→ユーザー ロックアウト	ロックアウト	[有効] 詳しくは、P. 51「ロックアウト機能」を参照してください。
セキュリティ→ユーザー ロックアウト	ログインパスワード入力許 容回数	5回以下 詳しくは、P. 51「ロックアウト機能」を参照してください。
セキュリティ→ユーザー ロックアウト	ロックアウト解除タイマー	[有効] または [無効] に設定します。 [有効] に設定したときは [ロックアウト解除までの 時間] を 60 分以上に設定 します。 詳しくは、P. 51「ロックアウト機能」を参照してください。

本機を管理する

カテゴリー	設定項目	設定値
セキュリティ→ユーザー ロックアウト	ロックアウト解除までの時間	「ロックアウト解除タイマー」で [有効] に設定したときは、[ロックアウト解除までの時間] を 60 分以上に設定します。 詳しくは、P. 51「ロックアウト機能」を参照してください。
ネットワーク→SNMPv3	SNMPv3 機能	[無効] SNMPv3 を使った機能を使用するときは、「SNMPv3 機能」を [有効] にし、「SNMPv3 通信許可設定」を [暗号化のみ] にします。この設定にしたときは、ユーザー認証は行われますが、ユーザー認証がパケット毎に非常に頻繁に行われるため、「ログイン」ログは記録されませんのでご注意ください。
セキュリティ→ネットワークセキュリティ	FTP	[無効] 操作部でネットワークセキュリティレベルを [レベル 2] にしてから設定します。
セキュリティ	S/MIME	「暗号化アルゴリズム」: [AES-128 ビット]、 [AES-256 ビット]、または [3DES-168 ビット] S/MIME を利用するときは、ユーザー証明書の登録が必要になります。

本機を管理する

カテゴリー	設定項目	設定値
アドレス帳→メール	ユーザー証明書	S/MIME を利用するには、ユーザー証明書の登録が必要です。

↓ 補足

- 暗号化アルゴリズムをどの強度に設定するかは、管理者が指示してください。
- 暗号アルゴリズムの設定とユーザー証明書の登録方法は、P. 115 「S/MIMEを設定する」を参照してください。

IPsec 有効/無効時の設定

IPsec を利用すると、IPsec が設定されている機器とのすべての通信が暗号化されます。使用しているネットワーク環境で IPsec が利用できるときは、より安全にネットワーク通信を使用するために、IPsec を有効にすることをお勧めします。

IPsec 有効時の設定

使用しているネットワーク環境で IPsec が利用できるときは、下記の表のように設定すると、暗号化されたネットワーク通信を使用できます。

操作部から設定する項目

システム初期設定

タブ項目	設定項目	設定値
インターフェース設定	IPsec	[有効]
インターフェース設定	SSL/TLS 通信許可設定	[暗号文のみ]

Web Image Monitor から設定する項目

カテゴリー	設定項目	設定値
セキュリティ→IPsec	手動鍵設定	無効
セキュリティ→IPsec	自動鍵交換設定→セキュリティレベル	認証と暗号化（高）

IPsec 無効時の設定

使用しているネットワーク環境で IPsec が利用できないときは、下記の表のように設定することをお勧めします。さらに「IPsec 無効時の運用方法」のとおり運用を徹底することで、暗号化されたネットワーク通信を使用できます。

操作部から設定する項目

システム初期設定

タブ項目	設定項目	設定値
インターフェース設定	IPsec	[無効]
インターフェース設定	SSL/TLS 通信許可設定	[暗号文のみ]

↓ 補足

- IPsec および SSL/TLS 通信許可設定は、Web Image Monitor から設定できます。

IPsec 無効時の運用方法

IPsec 無効時は、データを保護するため、管理者はユーザーに下記の機能を使用するように指導してください。

ファクス

- **IP-ファクスを使用しない送受信**
相手先を指定するときに、ファクス番号、インターネットファクス宛先、メール宛先、フォルダー宛先を相手先として指定し、IP-ファクスを使用しないようにします。相手先の指定方法は、『ファクス』「相手先を指定する」を参照してください。

プリンター

- **暗号化に対応したプロトコルによる印刷**
sftp を使用するか、SSL/TLS が有効に設定された状態で IPP を使ってプリンター機能を運用します。sftp の詳細は、『ネットワークの接続/システム初期設定』「Windows からファイルを直接印刷する」、IPP については、『ドライバーインストールガイド』「ポートを指定してインストールする」を参照してください。
SSL/TLS の設定は、P. 110 「SSL/TLS を設定する」を参照してください。

スキャナー

- **蓄積文書 URL アドレス送信**
読み取った文書をメールに添付しないで、文書の URL アドレスをメールで送信して

ください。蓄積文書の URL アドレス送信は、『スキャナー』「URL をメール送信する」を参照してください。

- **Web Image Monitor を使用したスキャナー文書管理**

Web Image Monitor から、ネットワーク経由でスキャナー文書の閲覧、削除、送信、およびダウンロードをします。

- **S/MIME 認証機能**

読み取った文書をメールに添付して送信するときは、「セキュリティー」を設定してから送信します。S/MIME 認証機能が設定されて送信されます。スキャナーからのメール送信は、『スキャナー』「メールにセキュリティーの設定をする」を参照してください。

↓ 補足

- 操作部による IPsec の設定は、『ネットワークの接続/システム初期設定』「システム初期設定」を参照してください。
- Web Image MonitorによるIPsecの設定は、P.123「IPsecを設定する」を参照してください。

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。

認証がうまくいかなかったとき

ユーザーがユーザー認証を行って操作しているときに、操作ができない状況になったときの対処方法を説明します。ユーザーから問い合わせがあったときにご覧ください。

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場合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。

こんなときには

メッセージ	原因	対処方法
この機能を利用する権限がありません。	機能を使う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 <ul style="list-style-type: none">▪ 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。▪ ユーザー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 <ul style="list-style-type: none">▪ 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。▪ 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。
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. 252「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. 10「管理者認証を設定する」を参照してください。

こんなときには

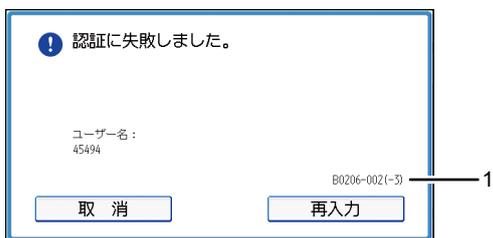
メッセージ	原因	対処方法
選択された文書にアクセス権のない文書が含まれていました。アクセス権のある文書のみ消去されます。	削除する権限のない文書を削除しようとした。	文書作成者（オーナー）、または文書管理者が削除できません。削除する権限のない文書を削除したいときは、文書作成者（オーナー）に確認してください。

↓ 補足

- サービスコールのメッセージが表示されたとき、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、画面にエラーコードも合わせて表示されます。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表示されたときは、エラーコードをお控えの上、サービス実施店に連絡してください。



CJC014

1. エラーコード表示部

ベーシック認証時のエラーコード

エラーコード	原因	対処方法
B0103-000	機器にユーザーがログイン中または、ログイン操作中に TWAIN 操作を行いました。	機器に他のユーザーがログインしていないことを確認してから、TWAIN 操作を行ってください。

エラーコード	原因	対処方法
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可能になります。
		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	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。
	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。
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。

こんなときには

エラーコード	原因	対処方法
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。

Windows 認証時のエラーコード

エラーコード	原因	対処方法
W0103-000	機器にユーザーがログイン中または、ログイン操作中に TWAIN 操作を行いました。	機器に他のユーザーがログインしていないことを確認してから、TWAIN 操作を行ってください。
W0107-000	パスワード復号処理に失敗しました。	<p>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。</p> <p>「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可能になります。</p> <p>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。</p>
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。

こんなときには

エラーコード	原因	対処方法
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か、セキュリティモジュール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。 セキュリティモジュールが搭載されているか確認してください。
W0400-107	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) となっていますので、sAMAccountName でログインしてください。

エラーコード	原因	対処方法
	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。	<ul style="list-style-type: none"> ・DC（ドメインコントローラ）上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。 ・機器へ登録したユーザーグループ名とDC上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。 ・機器へ登録したアドレス帳においてユーザーの認証情報タブ内、「使用できる機能」が非選択になっている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	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	認証サーバーと機器のSSL設定が合いません。	認証サーバーと機器のSSL設定が合っているか確認してください。

エラーコード	原因	対処方法
	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す。
W0406-107	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」で接続確認が可能です。 他の PC から認証できるか確認してください。
	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。 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。

エラーコード	原因	対処方法
	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	ドメイン名の名前解決ができません。	<p>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。</p> <p><成功する場合></p> <p>①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。</p> <p>②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。</p> <p><失敗する場合></p> <p>①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。</p> <p>②機器からドメインコントローラの接続経路上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。</p>

エラーコード	原因	対処方法
W0406-107	ドメイン名の名前解決ができません。	<ul style="list-style-type: none"> ・ Windows 7 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」にチェックすることで137番がOPEN します。
W0406-107	Kerberos 認証に失敗しています。	<p>Kerberos 設定が正しく設定されていません。</p> <p>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。</p> <hr/> <p>KDC (キー配布センター) と機器の時刻が合っていません。</p> <p>KDC (キー配布センター) と機器との間に5分以上の時刻差があるときは、認証に失敗します。</p> <p>時刻が合っているか確認してください。</p>

エラーコード	原因	対処方法
		<p>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。</p> <p>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。</p>
W0409-00	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。
W0511-00	機器内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）	<p>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。</p> <p>認証サーバーを切り替えた後であるときは、古いサーバー側のユーザーを削除してください。</p>
W0606-04	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。
W0607-01	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。

こんなときには

エラーコード	原因	対処方法
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

エラーコード	原因	対処方法
L0103-000	機器にユーザーがログイン中または、ログイン操作中に TWAIN 操作を行いました。	機器に他のユーザーがログインしていないことを確認してから、TWAIN 操作を行ってください。
L0104-000	パスワード復号処理に失敗しました。	<p>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。</p> <p>「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可能になります。</p> <p>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。</p>

エラーコード	原因	対処方法
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。

エラーコード	原因	対処方法
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。	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す。
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。

エラーコード	原因	対処方法
L0406-202 L0406-203	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、接続テストで成功でき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。
	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。

エラーコード	原因	対処方法
		<p>機器内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。</p> <p>以下に当てはまるときは、認証に失敗します。</p> <ul style="list-style-type: none"> ・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。
<p>L0406-202 L0406-203</p>	<p>簡易認証モードの使用方に誤りがあります。</p>	<p>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。</p> <p>空パスワードを許可したいときは、サービス実施店に連絡してください。</p> <hr/> <p>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。</p> <p>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いか確認してください。</p>

エラーコード	原因	対処方法
L0406-204	Kerberos 認証で失敗しました。	<p>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。</p>
		<p>KDC（キー配布センター）と機器の時刻が合っていない。 KDC（キー配布センター）と機器との間に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。</p>
		<p>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。</p>
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	機器内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後であるときは、古いサーバー側のユーザーを削除してください。

こんなときには

エラーコード	原因	対処方法
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。

こんなときには

状態	原因	対処方法
<p>プリンタードライバーから印刷できない。 TWAIN ドライバーで接続できない。 PC FAX ドライバーで送信または印刷ができない。</p>	<p>ユーザー認証が拒否された可能性があります。</p>	<p>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、ご利用の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。</p>
	<p>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なかった可能性があります。</p>	<p>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. 156「ドライバー暗号鍵を設定する」を参照してください。</p>
<p>TWAIN ドライバーで接続できない。</p>	<p>SNMPv3 のアカウント、パスワード、暗号化アルゴリズムが本機と一致しなかった可能性があります。</p>	<p>Network 接続限定ツールでの SNMPv3 アカウント、パスワード、暗号化アルゴリズムを本機で設定している値にしてください。 Web Image Monitor のヘルプを参照してください。</p>
<p>TWAIN ドライバーで認証ができない。</p>	<p>本機でほかにログインしているユーザーがいます。</p>	<p>そのユーザーがログアウトするのをしばらくお待ちください。</p>
	<p>装置側の都合により、認証に時間がかかっています。</p>	<p>LDAP サーバーの設定が正しいか確認してください。ネットワーク環境の設定が正しいか確認してください。</p>

こんなときには

状態	原因	対処方法
	<p>本機でアドレス帳の編集をしているため認証処理できません。</p>	<p>アドレス帳の編集が終わるまでしばらくお待ちください。</p>
<p>Network Monitor for Admin から「ユーザー情報管理ツール」や「アドレス情報管理」を起動後、正しいログインユーザー名、ログインパスワードを入力しても、パスワード違いのメッセージが表示され、使用できない。</p>	<p>「ドライバー暗号鍵:暗号強度設定」の設定が正しくありません。またはSSL/TLSの設定を有効にしているが、PCに証明書がインストールされていない可能性があります。</p>	<p>「ドライバー暗号鍵:暗号強度設定」を[簡易暗号]に設定するか、または、SSL/TLSの設定を有効にして、本機に機器証明書を導入後、PCに証明書をインストールしてください。</p> <p>「ドライバー暗号鍵:暗号強度設定」の設定はP. 230「セキュリティ強化機能を設定する」、SSL/TLSの設定はP. 110「SSL/TLSを設定する」を参照してください。</p>
<p>コピーやスキャナーを使用しているときにログアウトできない。</p>	<p>原稿の読み取りが終了していません。</p>	<p>原稿の読み取りがすでに終わっているときは、[#]を押して原稿を取り除いてから、ログアウトしてください。</p>
<p>ファクス/スキャナーの宛先指定画面に[宛先登録]が表示されない。</p>	<p>「セキュリティ強化」の「宛先利用制限(ファクス)」か「宛先利用制限(スキャナー)」、またはその両方で、「個人宛先登録制限(ファクス)」か「個人宛先登録制限(スキャナー)」、またはその両方が[する]に設定されているため、ユーザー管理者以外アドレス帳に登録することはできません。</p>	<p>ユーザー管理者が登録を行ってください。</p>

こんなときには

状態	原因	対処方法
<p>スキャナーのメール送信ができない。 (類似状態)</p> <ul style="list-style-type: none"> ▪ あて先が選択できない。 ▪ 署名が設定できない。 ▪ メディアに蓄積できない。 	<p>以下の原因が考えられます。</p> <ul style="list-style-type: none"> ▪ ユーザー証明書(あて先証明書)の有効期限が切れている。 ▪ 機器証明書(S/MIME)の有効期限が切れている。 ▪ 機器証明書(S/MIME)が存在しない、あるいは不正な証明書である。 ▪ 機器証明書(デジタル署名 PDF またはデジタル署名 PDF/A)の有効期限が切れている。 ▪ 機器証明書(デジタル署名 PDF またはデジタル署名 PDF/A)が存在しない、あるいは不正な証明書である。 ▪ 管理者のメールアドレスが間違っている。 	<ul style="list-style-type: none"> ▪ ユーザー証明書(あて先証明書)を導入してください。 ユーザー証明書(あて先証明書)は Web Image Monitor のアドレス帳から導入できます。ユーザー証明書(あて先証明書)自体は、事前に準備する必要があります。 ▪ S/MIME 用の機器証明書を導入してください。 ▪ デジタル署名 PDF 用またはデジタル署名 PDF/A 用の機器証明書を導入してください。 詳しくは、P. 106「機器証明書による通信経路の保護」を参照してください。 ▪ 管理者のメールアドレスを設定してください。 詳しくは、『ネットワークの接続/システム初期設定』「ファイル転送設定」を参照してください。

状態	原因	対処方法
<p>ファクス文書の転送ができない。 (類似状態)</p> <ul style="list-style-type: none"> ▪ あて先が選択できない。 ▪ 署名が設定できない。 	<p>以下の原因が考えられます。</p> <ul style="list-style-type: none"> ▪ ユーザー証明書(あて先証明書)の有効期限が切れている。 ▪ 機器証明書(S/MIME)の有効期限が切れている。 ▪ 機器証明書(S/MIME)が存在しない、あるいは不正な証明書である。 ▪ 機器証明書(デジタル署名 PDF またはデジタル署名 PDF/A)の有効期限が切れている。 ▪ 機器証明書(デジタル署名 PDF またはデジタル署名 PDF/A)が存在しない、あるいは不正な証明書である。 ▪ 管理者のメールアドレスが間違っている。 	<ul style="list-style-type: none"> ▪ ユーザー証明書(あて先証明書)を導入してください。 ユーザー証明書(あて先証明書)は Web Image Monitor のアドレス帳から導入できます。ユーザー証明書(あて先証明書)自体は、事前に準備する必要があります。 ▪ S/MIME 用の機器証明書を導入してください。 ▪ デジタル署名 PDF 用またはデジタル署名 PDF/A 用の機器証明書を導入してください。 詳しくは、P. 106「機器証明書による通信経路の保護」を参照してください。 ▪ 管理者のメールアドレスを設定してください。 詳しくは、『ネットワークの接続/システム初期設定』『ファイル転送設定』を参照してください。

状態	原因	対処方法
ユーザー認証を無効にしているのに蓄積文書が表示されない。	[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た可能性があります。	ユーザー認証の設定を再び有効にし、表示されていない文書に [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. 159「蓄積文書にアクセス権を設定する」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た可能性があります。	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. 72「アドレス帳の登録情報を保護する」を参照してください。
ユーザー認証を設定しているときに、プリンターから印刷できない。	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ない可能性があります。	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については、管理者にお問い合わせください。

こんなときには

状態	原因	対処方法
コピー中、または文書の読み取り中に、ジョブを中断しようとしたが、認証画面が表示された。	本機はコピー中、または文書の読み取り中にログアウトが可能です。 ログアウト後はコピーの中断や、文書の読み取りを中断したりすると、認証画面が表示されます。	コピーや読み取りを実行したユーザーでないと中断できません。 ジョブが終了するまでお待ちください。または、ジョブを実行したユーザー、および管理者にお問い合わせください。
アドレス帳の暗号化を実行し、しばらくしても、終了が表示されない。	ハードディスクまたはファイルが不良の可能性があります。	サービス実施店に連絡してください。

操作権限を確認する

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。

設定項目の操作権限一覧

ヘッダーの見方

- 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。
- なし
ログインユーザーの操作権限です。
「管理者認証管理」の [適用初期設定項目] で設定項目が選択されていない状態です。
- あり
ログインユーザーの操作権限です。
「管理者認証管理」の [適用初期設定項目] で設定項目が選択されているときの状態です。
- Lv. 1
[メニュープロテクト設定] 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設定] が [レベル 2] に設定されている状態です。

マークの見方

- 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

- ユーザー認証有効時は、未認証のユーザー、およびログイン情報を持たないユーザーは、本機を操作できません。

操作権限を確認する

- [メニュープロテクト設定] 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。

システム初期設定

管理者認証を設定しているとき、「適用初期設定項目」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	なし	あり
定型文字列登録／変更／消去	R	R/W	R	R	R/W	R
ブザー音	R	R/W	R	R	R/W	R
ウォームアップ通知音	R	R/W	R	R	R/W	R
用紙枚数カウンター表示	R	R/W	R	R	R/W	R
優先機能設定	R	R/W	R	R	R/W	R
機能キー割り当て設定	R	R/W	R	R	R/W	R
画面表示色切り替え	R	R/W	R	R	R/W	R
印刷優先機能設定	R	R/W	R	R	R/W	R
印刷機能移行時間	R	R/W	R	R	R/W	R
割り込み動作時の出力	R	R/W	R	R	R/W	R
排紙先: コピー	R	R/W	R	R	R/W	R
排紙先: ドキュメントボックス	R	R/W	R	R	R/W	R
排紙先: ファクス	R	R/W	R	R	R/W	R
排紙先: プリンター	R	R/W	R	R	R/W	R
状態確認/ジョブ一覧表示時間設定	R	R/W	R	R	R/W	R
キーリピート設定	R	R/W	R	R	R/W	R
外付けキーボード	R	R/W	R	R	R/W	R
倍率補正: コピー	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
倍率補正：プリンター	R	R/W	R	R	R/W	R

用紙設定

設定項目	User	機器	N/W	文書	なし	あり
給紙トレイ優先設定:コピー	R	R/W	R	R	R/W	R
給紙トレイ優先設定:ファクス	R	R/W	R	R	R/W	R
給紙トレイ優先設定:プリンター	R	R/W	R	R	R/W	R
用紙サイズ設定:トレイ 1~5	R	R/W	R	R	R/W	R
プリンター手差し用紙サイズ	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 1~5	R	R/W	R	R	R/W	R
不定形サイズ指定	R	R/W	R	R	R/W	R
表紙トレイ設定	R	R/W	R	R	R/W	R
合紙トレイ設定	R	R/W	R	R	R/W	R
章区切り紙トレイ設定	R	R/W	R	R	R/W	R
紙厚設定：給紙トレイ	R	R/W	R	R	R/W	R
紙厚設定：用紙手差し	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	なし	あり
スリープモード移行時間設定	R	R/W	R	R	R/W	R
低電力モード移行時間設定	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
システムオートリセット時間設定	R	R/W	R	R	R/W	R
コピー/ドキュメントボックスオートリセット時間設定	R	R/W	R	R	R/W	R
ファクスオートリセット時間設定	R	R/W	R	R	R/W	R
プリンターオートリセット時間設定	R	R/W	R	R	R/W	R
スキャナーオートリセット時間設定	R	R/W	R	R	R/W	R
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
オートログアウト時間設定	R	R/W	R	R	R/W	R
電源オフ解除コード設定	R	R/W	R	R	R/W	R
ウィークリータイマー：月～日	R	R/W	R	R	R/W	R

インターフェース設定

ネットワーク

設定項目	User	機器	N/W	文書	なし	あり
本体 IPv4 アドレス*1	R	R	R/W	R	R/W	R
IPv4 ゲートウェイアドレス	R	R	R/W	R	R/W	R
本体 IPv6 アドレス	R	R	R	R	R	R
IPv6 ゲートウェイアドレス	R	R	R	R	R	R
IPv6 ステートレスアドレス自動設定	R	R	R/W	R	R/W	R
DHCPv6 設定	R	R	R/W	R	R/W	R
DNS 設定*2	R	R	R/W	R	R/W	R
DDNS 設定	R	R	R/W	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
IPsec	R	R	R/W	R	R/W	R
ドメイン名*1	R	R	R/W	R	R/W	R
WINS 設定	R	R	R/W	R	R/W	R
有効プロトコル	R	R	R/W	R	R/W	R
NCP 配信時プロトコル	R	R	R/W	R	R/W	R
NW フレームタイプ	R	R	R/W	R	R/W	R
SMB コンピュータ名	R	R	R/W	R	R/W	R
SMB ワークグループ	R	R	R/W	R	R/W	R
イーサネット速度	R	R	R/W	R	R/W	R
ネットワークインターフェース選択	R	R	R/W	R	R/W	R
Ping コマンド実行	—	—	R/W	—	R/W	—
SNMPv3 通信許可設定	R	R	R/W	R	R/W	R
SSL/TLS 通信許可設定	R	R	R/W	R	R/W	R
ホスト名	R	R	R/W	R	R/W	R
本体名	R	R	R/W	R	R/W	R
イーサネット用 IEEE802.1X 認証	R	R	R/W	R	R/W	R
IEEE802.1X 認証初期化	—	—	R/W	—	R/W	—

*1 自動取得するに設定したときは、閲覧のみできます。

*2 接続テストはすべての管理者、ユーザーが実行できます。

パラレルインターフェース

設定項目	User	機器	N/W	文書	なし	あり
パラレルタイミング	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
パラレル通信速度	R	R/W	R	R	R/W	R
セレクト状態	R	R/W	R	R	R/W	R
インプットプライム	R	R/W	R	R	R/W	R
双方向通信	R	R/W	R	R	R/W	R
信号線制御	R	R/W	R	R	R/W	R

無線 LAN

設定項目	User	機器	N/W	文書	なし	あり
通信モード	R	R	R/W	R	R/W	R
SSID 設定	R	R	R/W	R	R/W	R
アドホックチャンネル	R	R	R/W	R	R/W	R
セキュリティ方式選択	R	R	R/W	R	R/W	R
電波状態	R	R	R/W	R	R/W	R
設定値初期化	—	—	R/W	—	R/W	—

ファイル転送設定

設定項目	User	機器	N/W	文書	なし	あり
SMTP サーバー	R	R	R/W	R	R/W	R
SMTP 認証*3	R	R/W	R	R	R/W	R
POP before SMTP	R	R/W	R	R	R/W	R
受信プロトコル	R	R/W	R	R	R/W	R
POP3/IMAP4 設定	R	R/W	R	R	R/W	R

操作権限を確認する

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	R/W	R	R	R/W	R
メール通信ポート設定	R	R	R/W	R	R/W	R
メール受信間隔時間設定	R	R	R/W	R	R/W	R
受信メールサイズ制限	R	R	R/W	R	R/W	R
サーバー側メール保持	R	R	R/W	R	R/W	R
送信初期ユーザー名・パスワード*3	R	R/W	R	R	R/W	R
送信メール本文登録／変更／消去	R	R/W	R	R	R/W	R/W
送信者名自動指定	R	R	R/W	R	R/W	R
ファクスメールアカウント	R	R/W	R	R	R/W	R
スキャナー再送信間隔時間	R	R	R/W	R	R/W	R
スキャナー再送信回数	R	R	R/W	R	R/W	R

*3 パスワードは閲覧できません。

管理者用設定

設定項目	User	機器	N/W	文書	なし	あり
アドレス帳登録／変更／消去	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R *6
グループ登録／変更／消去	R/W	R/W *5	R/W *5	R/W *5	R/W *6	R *6
並び順入れ替え	R/W	—	—	—	R/W	—
アドレス帳:宛先リスト印刷	R/W	—	—	—	R/W	R/W
見出し編集	R/W	—	—	—	R/W	—
アドレス帳見出し切り替え	R/W	—	—	—	R/W	R
ユーザー個別設定・アドレス帳 バックアップ／リストア	R/W	—	—	—	R/W	—

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
アドレス帳自動登録時データ利用設定	R/W	R	R	R	R/W	R
印刷利用量制限度数設定	R	R/W	R	R	R	R
カウンター表示／印刷	R	R/W	R	R	R/W	R/W
ユーザー別カウンター表示／クリア／印刷	R/W *7	R/W *8	R	R	R/W	—
eco 指数カウンター表示／クリア	—	R/W	—	—	—	—
ユーザー別 eco 指数カウンター表示／クリア	—	R/W	—	—	—	—
上限到達時動作設定	R	R/W	R	R	R	R
メディアスロット使用	R	R/W	R	R	R	R
ストップキー印刷ジョブ停止設定	R	R/W	R	R	R	R
ユーザー認証管理	R	R/W	R	R	R/W	R
管理者認証管理	R/W *9*10	R/W *10	R/W *10	R/W *10	R/W	—
管理者登録／変更	R/W *11	R/W *11	R/W *11	R/W *11	—	—
セキュリティ強化						
▪ ドライバー暗号鍵	—	—	R/W	—	R/W	—
▪ ドライバー暗号鍵：暗号強度設定	R	R	R/W	R	R/W	R
▪ 個人情報表示制限	R	R/W	R	R	R/W	R
▪ ユーザー個別設定・アドレス帳 暗号化	R/W	R	R	R	R	R
▪ 文書保護強化	R	R	R	R/W	R	R
▪ 宛先利用制限（ファクス）	R/W	R	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
▪ 個人宛先登録制限（ファクス）	R/W	R	R	R	R	R
▪ 宛先利用制限（スキャナー）	R/W	R	R	R	R	R
▪ 個人宛先登録制限（スキャナー）	R/W	R	R	R	R	R
▪ 受信指定先への転送（ファクス）	R	R/W	R	R	R	R
▪ 実行中ジョブへの認証の実施	R	R/W	R	R	R/W	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	—	—
▪ パスワードポリシー	R/W	—	—	—	—	—
▪ SNMPv1, v2 による設定	R	R	R/W	R	R/W	R
▪ アクセス攻撃検知	—	R/W	—	—	—	—
▪ パスワード攻撃検知	—	R/W	—	—	—	—
▪ アクセスセキュリティー設定	R	R/W	R	R	—	—
ドキュメントボックス蓄積文書自動消去	R	R	R	R/W	R/W	R
ドキュメントボックス蓄積文書一括消去	—	—	—	R/W	R/W	—
LDAP サーバー登録／変更／消去*4	—	R/W	—	—	R/W	R
LDAP 検索	R	R/W	R	R	R/W	R
低電力モードレベル設定	R	R/W	R	R	R/W	R
印刷利用量上限初期値	R/W	R	R	R	R	R
サービスモード移行禁止設定	R	R/W	R	R	R/W	R
ファームウェアバージョン表示	R	R	R	R	R	R
ネットワークセキュリティーレベル	R	R	R/W	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
メモリー自動消去設定	R	R/W	R	R	R	R
メモリー全消去	—	R/W	—	—	—	—
ログ一括消去	—	R/W	—	—	R/W	—
USB ポート固定	R	R/W	R	R	R/W	R
レーム登録/変更/消去	—	R/W	—	—	—	R
機器データ暗号化設定	—	R/W	—	—	—	—
機器証明書登録/消去	—	—	R/W	—	—	—
機器設定情報：インポート（サーバー） 設定*12	—	—	—	—	—	—
機器設定情報：インポート（サーバー） 実行*12	—	—	—	—	—	—
機器設定情報：エクスポート（メディア） *12	—	—	—	—	—	—
機器設定情報：インポート（メディア） *12	—	—	—	—	—	—
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
eco 指数カウンター集計期間/管理者メ ッセージ設定	R	R/W	R	R	R	R
PDF ファイル形式：PDF/A 固定	R	R/W	R	R	R	R
省エネキーモード移行設定	R	R/W	R	R	R/W	R
強制セキュリティ印字：コピー	R	R/W	R	R	R/W	R
強制セキュリティ印字：ドキュメント ボックス	R	R/W	R	R	R/W	R
強制セキュリティ印字：ファクス	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
強制セキュリティ印字：プリンター	R	R/W	R	R	R/W	R
ユーザー別ホーム利用	R	R/W	R	R	R/W	R

*4 パスワードは閲覧できません。

*5 見出し切り替えとユーザーの検索のみできます。

*6 アクセス権によって、実行、変更、閲覧できる項目が異なります。

*7 クリアのみできます。

*8 印刷のみできます。

*9 個人認証機能を利用しているときは変更できません。

*10 権限を持つ管理者項目のみ変更できます。

*11 管理者が管理者自身のアカウントのみを変更できます。

*12 すべての権限を持つ管理者が実行、変更、閲覧できます。

リスト印刷

設定項目	User	機器	N/W	文書	なし	あり
リスト印刷	—	—	R/W	—	R/W	—

ホーム編集

管理者認証を設定しているとき、「適用初期設定項目」の設定で、ユーザーの操作権限が異なります。

ホーム編集

設定項目	User	機器	N/W	文書	なし	あり
アイコンの編集：アイコンの移動	—	R/W	—	—	R/W	—
アイコンの編集：アイコンの消去	—	R/W	—	—	R/W	—
アイコンの編集：アイコンの追加	—	R/W	—	—	R/W	—
アイコンの編集：アイコンを初期値に戻す	—	R/W	—	—	R/W	—
画像の設定：ホーム画像の設定	—	R/W	—	—	R/W	—

コピー／ドキュメントボックス初期設定

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。

基本コピー設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
自動濃度優先	R	R/W	R	R	R	R
優先写真原稿種類	R	R/W	R	R	R	R
原稿種類省略表示	R	R/W	R	R	R	R
用紙種類省略表示	R	R/W	R	R	R	R
両面原稿ひらき方向設定	R	R/W	R	R	R	R
両面コピーひらき方向設定	R	R/W	R	R	R	R
コピーセット枚数制限設定	R	R/W	R	R	R	R
リミットレス給紙	R	R/W	R	R	R	R
原稿忘れブザー音	R	R/W	R	R	R	R
ジョブ終了お知らせ	R	R/W	R	R	R	R
カラー選択<黒赤>優先設定	R	R/W	R	R	R	R
登録機能: コピー	R	R/W	R	R	R/W	R
登録機能: ドキュメントボックス読み取り	R	R/W	R	R	R/W	R

変倍率設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
基本画面倍率キー設定	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
変倍率設定	R	R/W	R	R	R	R
優先変倍率設定	R	R/W	R	R	R	R
すこし小さめ変倍率設定	R	R/W	R	R	R	R

基本編集設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
左右とじしろ幅設定（おもて面）	R	R/W	R	R	R	R
左右とじしろ幅設定（うら面）	R	R/W	R	R	R	R
上下とじしろ幅設定（おもて面）	R	R/W	R	R	R	R
上下とじしろ幅設定（うら面）	R	R/W	R	R	R	R
片面→両面時裏面左右とじしろ	R	R/W	R	R	R	R
片面→両面時裏面上下とじしろ	R	R/W	R	R	R	R
枠消去幅設定	R	R/W	R	R	R	R
集約コピー一時枠消去	R	R/W	R	R	R/W	R
センター消去幅	R	R/W	R	R	R	R
おもて表紙ページ集約設定	R	R/W	R	R	R/W	R
集約時並び順	R	R/W	R	R	R/W	R
ひらき方向:ミニ本・週刊誌	R	R/W	R	R	R/W	R
章区切りページ集約設定	R	R/W	R	R	R/W	R
リピート仕切り線	R	R/W	R	R	R/W	R
ダブルコピー仕切り線	R	R/W	R	R	R/W	R
集約コピー仕切り線	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
フォーマット登録/削除	R	R/W	R	R	R/W	R

印字編集設定

機密管理印字

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
管理番号印字サイズ設定	R	R/W	R	R	R/W	R
管理番号印字濃度設定	R	R/W	R	R	R/W	R

スタンプ印字

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
スタンプ言語切り替え	R	R/W	R	R	R/W	R
スタンプ種類優先設定	R	R/W	R	R	R	R
スタンプ条件設定: マル秘	R	R/W	R	R	R/W *1	R
スタンプ条件設定: 回収	R	R/W	R	R	R/W *1	R
スタンプ条件設定: 複製厳禁	R	R/W	R	R	R/W *1	R
スタンプ条件設定: 至急	R	R/W	R	R	R/W *1	R
スタンプ条件設定: マル仮	R	R/W	R	R	R/W *1	R
スタンプ条件設定: 回覧	R	R/W	R	R	R/W *1	R
スタンプ条件設定: CONFIDENTIAL	R	R/W	R	R	R/W *1	R
スタンプ条件設定: DRAFT	R	R/W	R	R	R/W *1	R
印字色優先設定: マル秘	R	R/W	R	R	R	R
印字色優先設定: 回収	R	R/W	R	R	R	R
印字色優先設定: 複製厳禁	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
印字色優先設定：至急	R	R/W	R	R	R	R
印字色優先設定：マル仮	R	R/W	R	R	R	R
印字色優先設定：回覧	R	R/W	R	R	R	R
印字色優先設定：CONFIDENTIAL	R	R/W	R	R	R	R
印字色優先設定：DRAFT	R	R/W	R	R	R	R

*1 印刷位置の調整のみ設定できます。印刷位置自体は設定できません。

ユーザースタンプ

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
スタンプ登録/削除	R	R/W	R	R	R/W	R
スタンプ条件設定：1~4	R	R/W	R	R	R/W	R
印字色優先設定：1~4	R	R/W	R	R	R/W	R

日付印字

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
印字種類設定	R	R/W	R	R	R	R
印字フォント設定	R	R/W	R	R	R/W	R
印字サイズ設定	R	R/W	R	R	R/W	R
自動白黒反転印字	R	R/W	R	R	R/W	R
印字色優先設定	R	R/W	R	R	R	R
印字条件設定	R	R/W	R	R	R/W *2	R

*2 印刷位置の調整のみ設定できます。印刷位置自体は設定できません。

ページ印字

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
印字種類優先設定	R	R/W	R	R	R	R
印字フォント設定	R	R/W	R	R	R/W	R
印字サイズ設定	R	R/W	R	R	R/W	R
うら面印字位置	R	R/W	R	R	R/W	R
集約時ページ印字設定	R	R/W	R	R	R/W	R
章区切りページ（合紙）への印字	R	R/W	R	R	R/W	R
印字位置設定:P1, P2 . . .	R	R/W	R	R	R/W *3	R
印字位置設定:1/5, 2/5 . . .	R	R/W	R	R	R/W *3	R
印字位置設定:-1-, -2- . . .	R	R/W	R	R	R/W *3	R
印字位置設定:P. 1, P. 2 . . .	R	R/W	R	R	R/W *3	R
印字位置設定:1, 2 . . .	R	R/W	R	R	R/W *3	R
印字位置設定:1-1, 1-2 . . .	R	R/W	R	R	R/W *3	R
印字位置設定:1 ページ, 2 ページ . . .	R	R/W	R	R	R/W *3	R
自動白黒反転印字	R	R/W	R	R	R/W	R
印字色優先設定	R	R/W	R	R	R/W	R

*3 印刷位置の調整のみ設定できます。印刷位置自体は設定できません。

周辺設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
大量原稿モード切り替え	R	R/W	R	R	R/W	R
SADF オートリセット時間設定	R	R/W	R	R	R	R
回転ソート:回転給紙継続設定	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
ソート全数読み取り設定	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
ステープル種類選択	R	R/W	R	R	R/W	R
パンチ種類選択	R	R/W	R	R	R/W	R
簡単画面：後処理種類選択	R	R/W	R	R	R/W	R

管理者用設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
メニュープロテクト設定	R	R/W	R	R	R	R

ファクス初期設定

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。

基本設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
クイック操作キー1~3	R	R/W	R	R	R/W	R
宛先表見出し切り替え	R	R/W	R	R	R/W	R
宛先検索対象	R	R/W	R	R	R/W	R
通信枚数カウンター	R	R	R	R	R	R
音量調節	R	R/W	R	R	R/W	R
Fコードボックス設定	—	R/W	—	—	R	—
Fコードボックス設定: リスト印刷	—	R/W	—	—	R/W	—
オンフック解除時間	R	R/W	R	R	R/W	R
宛先履歴消去	—	R/W	—	—	—	—
通信管理レポート自動印刷	R	R/W	R	R	R	R
リングング音	R	R/W	R	R	R/W	R

読み取り設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
読み取りサイズ登録/変更/消去	R	R/W	R	R	R/W	R

送信設定

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
送信メールサイズ制限	R	R	R/W	R	R	R
定型文登録／変更／消去	R	R/W	R	R	R	R
全文書転送	—	R/W	—	—	—	—
バックアップ送信設定	R	R/W	R	R	R	R
IP ファクス送信ルート自動切替 (IP/G3)	R	R/W	R	R	R	R
IP ファクス最大送信速度設定	R	R/W	R	R	R	R

受信設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
受信文書設定	R	R/W	R	R	R	R
受信モード切り替え	R	R/W	R	R	R	R
受信モード自動切り替え時設定	R	R/W	R	R	R	R
受信モードタイマー切り替え	R	R/W	R	R	R	R
特定相手先設定	—	R/W	—	—	—	—
特定相手先設定: リスト印刷	—	R/W	—	—	—	—
蓄積受信文書ユーザー設定	R	R	R	R/W	R	R
SMTP 受信ファイル配信設定	R	R/W	R	R	R	R
両面印刷	R	R/W	R	R	R/W	R
しおり印字	R	R/W	R	R	R/W	R
センターマーク印字	R	R/W	R	R	R/W	R
受信時刻印字	R	R/W	R	R	R/W	R
受信文書印刷部数	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
給紙トレイ選択	R	R/W	R	R	R/W	R
回線別排紙先設定	R	R/W	R	R	R/W	R
フォルダー転送結果メール通知	R	R/W	R	R	R	R
回線別受信連携先設定	R	R/W	R	R	R	R

導入設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
パラメーター設定	R	R/W	R	R	R	R
パラメーター設定: リスト印刷	—	R/W	—	—	R/W	—
ID 送受信用 ID 登録	—	R/W	—	—	R	—
封筒 ID 登録	—	R/W	—	—	R	—
インターネットファクス設定	R	R/W	R	R	R	R
ダイヤルイン設定	R	R/W	R	R	R	R
ダイヤル/プッシュ選択	R	R/W	R	R	R	R
発信元情報登録	R	R/W	R	R	R	R
H. 323 使用	R	R	R/W	R	R	R
SIP 使用	R	R	R/W	R	R	R
H. 323 設定	R	R	R/W	R	R	R
SIP 設定	R	R	R/W	R	R	R
ゲートウェイ登録/変更/消去	R	R	R/W	R	R	R
ISDN-G3 回線登録	R	R/W	R	R	R	R
ISDN-G4 回線登録	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
メニュープロテクト設定	R	R/W	R	R	R	R
メール設定	R	R/W	R	R	R	R
フォルダー設定	R	R/W	R	R	R	R
転送ファイル形式	R	R/W	R	R	R	R
NGN 設定方法	R	R/W	R	R	R	R
送信結果メール通知セキュリティー設定	R	R/W	R	R	R	R

プリンター通常画面

ホーム画面の「プリンター」を押して表示される、プリンター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。

プリンター通常画面

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
ジョブ一覧	—*1	R	—*1	—*1	R	R
文書印刷	—	—	—	R/W	R/W	R/W
メディアプリント	—	—	—	—	R/W	R/W
印刷取消	R/W	R/W	R/W	R/W	R/W	R/W
ジョブ操作	R/W	R/W	R/W	R/W	R/W	R/W
強制排紙	R/W	R/W	R/W	R/W	R/W	R/W
エミュレーション/プログラム	R/W	R/W	R/W	R/W	R/W	R/W
ジョブスプルー一覧	R	R/W	R	R	R	R
エラー履歴	R	R/W	R	R	R	R

*1 「セキュリティ強化」の「実行中ジョブへの認証の実施」が「しない」のときに閲覧できます。

プリンター初期設定

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。

テスト印刷

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
一括リスト印刷	—	R/W	—	—	R/W	R/W
システム設定リスト	—	R/W	—	—	R/W	R/W
エラー履歴	—	R/W	—	—	R/W	R/W
印刷条件リスト	—	R/W	—	—	R/W	R/W
登録フォームリスト	—	R/W	—	—	R/W	R/W
PS 情報リスト	—	R/W	—	—	R/W	R/W
PDF 情報リスト	—	R/W	—	—	R/W	R/W
ヘキサダンプ	—	R/W	—	—	R/W	R/W

調整/管理

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
メニュープロテクト	R	R/W	R	R	R	R
テスト印刷禁止	R	R/W	R	R	R	R
一時置き文書全消去	—	—	—	R/W	—	—
保存文書全消去	—	—	—	R/W	—	—
一時置き文書自動消去設定	R	R	R	R/W	R	R
保存文書自動消去設定	R	R	R	R/W	R	R

操作権限を確認する

システム設定

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
エラージョブ蓄積・追い越し	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
ジョブ仕分け	R	R/W	R	R	R	R
180度回転	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
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
印刷枚数	R	R/W	R	R	R	R
スムージング	R	R/W	R	R	R	R
トナーセーブ	R	R/W	R	R	R	R
予約印刷明け渡し時間設定	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
トレイ指定時動作切り替え	R	R/W	R	R	R	R
拡張リミットレス給紙	R	R/W	R	R	R	R
主電源 Off 時の未処理文書	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
印刷をとまなうジョブの制限	R	R/W	R	R	R	R
初期画面の切り替え	R	R/W	R	R	R	R

システム設定 (EM)

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
白紙排紙	R	R/W	R	R	R	R
自動排紙時間	R	R/W	R	R	R	R
水平補正初期値	R	R/W	R	R	R	R
垂直補正初期値	R	R/W	R	R	R	R

PS 設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
ジョブタイムアウト	R	R/W	R	R	R	R
ウェイトタイムアウト	R	R/W	R	R	R	R
両面印刷	R	R/W	R	R	R	R
両面印刷ページ切り替えコマンド	R	R/W	R	R	R	R
白紙排紙	R	R/W	R	R	R	R
データ形式	R	R/W	R	R	R	R
解像度	R	R/W	R	R	R	R
最大領域印刷	R	R/W	R	R	R	R
印刷方向自動検知	R	R/W	R	R	R	R

PDF 設定

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
PDF パスワード変更	R	R/W	R	R	R	R
PDF グループパスワード	R	R/W	R	R	R	R
両面印刷	R	R/W	R	R	R	R
白紙排紙	R	R/W	R	R	R	R
最終ページから印刷	R	R/W	R	R	R	R
解像度	R	R/W	R	R	R	R
最大領域印刷	R	R/W	R	R	R	R
印刷方向自動検知	R	R/W	R	R	R	R

インターフェース設定

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替時間	R	R/W	R	R	R	R

印字設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
On/Off 設定	R	R/W	R	R	R	R
機密管理ナンバリング	R	R/W	R	R	R	R
スタンプ印字	R	R/W	R	R	R	R
ユーザースタンプ印字	R	R/W	R	R	R	R
日付印字	R	R/W	R	R	R	R

操作権限を確認する

不正コピー抑止

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
不正コピー抑止設定	R	R/W	R	R	R	R
優先する設定/ドライバー/コマンド/機器側	R	R/W	R	R	R	R
不正コピー抑止の種類	R	R/W	R	R	R	R
地紋マスクパターン/濃度/効果	R	R/W	R	R	R	R
抑止文字列設定	R	R/W	R	R	R	R

スキャナー初期設定

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。

基本設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
宛先表見出し切り替え	R	R/W	R	R	R	R
宛先検索対象	R	R/W	R	R	R	R
外部認証：フォルダーパス上書き設定	R	R/W	R	R	R	R
TWAIN 割り込み禁止時間設定	R	R/W	R	R	R	R
宛先表初期表示選択	R	R/W	R	R	R	R
優先本体宛先表	R	R/W	R	R	R	R
送信履歴満杯時印刷設定	R	R/W	R	R	R	R
送信履歴印刷	—	R/W	—	—	—	—
送信履歴消去	—	R/W	—	—	—	—
宛先履歴消去	—	R/W	—	—	—	—

読み取り設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
次原稿待機設定：原稿ガラス	R	R/W	R	R	R	R
次原稿待機設定：SADF	R	R/W	R	R	R	R
自動濃度の濃度設定（フルカラー）	R	R/W	R	R	R	R
変倍率設定	R	R/W	R	R	R	R

操作権限を確認する

送信設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
圧縮設定（白黒 2 値）	R	R/W	R	R	R/W	R
圧縮方式（白黒 2 値）	R	R/W	R	R	R/W	R
圧縮設定（グレースケール/フルカラー）	R	R/W	R	R	R/W	R
高圧縮 PDF 圧縮率設定	R	R/W	R	R	R/W	R
送信メールサイズ制限	R	R	R/W	R	R*1	R*1
メールサイズ制限オーバー時分割	R	R	R/W	R	R*1	R*1
メール付加情報	R	R/W	R	R	R/W	R
シングルページ番号桁設定	R	R/W	R	R	R/W	R
蓄積文書メール内容	R	R/W	R	R	R/W	R
デフォルトメール件名	R	R/W	R	R	R	R

*1 [管理者認証管理] の [ネットワーク管理] が [しない] に設定されているときは、ユーザーの権限は R/W になります。

導入設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
メニュープロテクト設定	R	R/W	R	R	R	R

操作権限を確認する

Web Image Monitor: eco 指数カウンター表示

[機器の情報] の中の項目です。

ユーザーは自身のカウンターだけを閲覧できます。

設定項目	User	機器	N/W	文書	なし	あり
機器トータルカウンター	—	R	—	—	—	—
ユーザー別カウンター	—	R	—	—	R	R
ダウンロード	—	R/W	—	—	R	R

Web Image Monitor : ジョブ

[機器の情報] 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のみを操作できます。

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：順序入れ替え	—	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：予約削除	—	R/W	—	—	—	R/W
ジョブ履歴	—	R	—	—	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	User	機器	N/W	文書	なし	あり
スプール：削除	—	R/W	—	—	—	R/W
ジョブ履歴	R	R/W	R	R	R	R
エラー履歴	—	R	—	—	—	R

ファクス

設定項目	User	機器	N/W	文書	なし	あり
送信履歴	—	R	—	—	R	R*1
受信履歴	—	R	—	—	R	R*1
PC ファクス	—	R	—	—	R	R*1

操作権限を確認する

*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。

ドキュメントボックス

設定項目	User	機器	N/W	文書	なし	あり
印刷ジョブ履歴	—	R	—	—	R	R*1
ファクス リモート送信履歴	—	R	—	—	R	R*1
スキャナー リモート送信履歴	—	R	—	—	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。

Web Image Monitor : 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、「適用初期設定項目」の設定によって、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
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
スプール印刷	R	R/W	R	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	—	—
印刷優先機能	R	R/W	R	R	—	—
印刷機能移行時間	R	R/W	R	R	—	—
省エネキーモード移行設定	R	R/W	R	R	R/W	R
ストップキー印刷ジョブ停止設定	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	—	—
ファームウェア構成変更許可	R	R/W	R	R	—	—
IP アドレス機器画面表示	R	R/W	R	R	—	—
メディアスロット使用	R	R/W	R	R	R	R
PDF ファイル形式 : PDF/A 固定	R	R/W	R	R	R	R
排紙トレイ	R	R/W	R	R	R/W	R
優先給紙トレイ	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
表紙トレイ	R	R/W	R	R	R/W	R
合紙トレイ設定	R	R/W	R	R	R/W	R
章区切り紙 1-2 トレイ設定	R	R/W	R	R	R/W	R

機能キー割り当て/優先機能設定

設定項目	User	機器	N/W	文書	なし	あり
機能キー割り当て設定	R	R/W	R	R	R/W	R
優先機能設定	R	R/W	R	R	R/W	R

用紙

設定項目	User	機器	N/W	文書	なし	あり
トレイ 1~5	R	R/W	R	R	R/W	R
手差しトレイ	R	R/W	R	R	R/W	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

タイマー

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
スリープモード移行時間設定	R	R/W	R	R	R/W	R
低電力モード移行時間設定	R	R/W	R	R	R/W	R
システムオートリセット時間設定	R	R/W	R	R	R/W	R
コピー/ドキュメントボックスオートリセット時間設定	R	R/W	R	R	R/W	R
ファクスオートリセット時間設定	R	R/W	R	R	R/W	R
スキャナーオートリセット時間設定	R	R/W	R	R	R/W	R
プリンター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
電源オフ解除コード設定	R	R/W	R	R	R/W	R
ウィークリータイマー：月曜日～日曜日	R	R/W	R	R	R/W	R

ログ

設定項目	User	機器	N/W	文書	なし	あり
ジョブログ	R	R/W	R	R	R/W	R
アクセスログ	R	R/W	R	R	R/W	R
eco ログ	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
ログ一括消去	—	R/W	—	—	R/W	—

ログダウンロード

操作権限を確認する

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
署名	—	R/W	—	—	R/W	R
受信プロトコル	—	R/W	—	—	R/W	R
受信間隔設定	—	—	R/W	—	R/W	R
受信メールサイズ制限	—	—	R/W	—	R/W	R
サーバー側メール保持	—	—	R/W	—	R/W	R
SMTP サーバー名	—	—	R/W	—	R/W	R
SMTP ポート番号	—	—	R/W	—	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*2	—	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*2	—	R/W	—	—	R/W	—

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
POP 認証後待機時間	—	R/W	—	—	R/W	R
POP3/IMAP4 サーバー名	—	R/W	—	—	R/W	R
POP3/IMAP4 暗号化	—	R/W	—	—	R/W	R
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
ファクスメールアドレス	—	R/W	—	—	R/W	R
ファクスマールの受信	—	R/W	—	—	R/W	—
ファクスマールユーザー名	—	R/W	—	—	R/W	—
ファクスマールパスワード	—	R/W	—	—	R/W	—
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*2	—	R/W	—	—	R/W	—

*2 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	R	R/W	R	R	R	R
項目ごとの通知先	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

操作権限を確認する

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	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

ファイル転送

設定項目	User	機器	N/W	文書	なし	あり
SMB 送信ユーザー名	—	R/W	—	—	R/W	—
SMB 送信パスワード* ²	—	R/W	—	—	R/W	—
FTP 送信ユーザー名	—	R/W	—	—	R/W	—
FTP 送信パスワード* ²	—	R/W	—	—	R/W	—
NCP 送信ユーザー名	—	R/W	—	—	R/W	—
NCP 送信パスワード* ²	—	R/W	—	—	R/W	—

*² パスワードは閲覧できません。

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
プリンタージョブ認証設定	R	R/W	R	R	R/W	R
ユーザーコード設定	R	R/W	R	R	R/W	R
ベーシック認証設定	R	R/W	R	R	R/W	R
Windows 認証設定	R	R/W	R	R	R/W	R
グループ設定 (Windows 認証)	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
LDAP 認証設定	R	R/W	R	R	R/W	R

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
ユーザー管理者適用初期設定項目	R/W	R	R	R	R	R
機器管理者認証	R	R/W	R	R	R	R
機器管理者適用初期設定項目	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
ネットワーク管理者適用初期設定項目	R	R	R/W	R	R	R
文書管理者認証	R	R	R	R/W	R	R
文書管理者適用初期設定項目	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	—	—
ログインユーザー名*1	R/W	R/W	R/W	R/W	—	—
ログインパスワード*1	R/W	R/W	R/W	R/W	—	—
暗号パスワード*1	R/W	R/W	R/W	R/W	—	—

操作権限を確認する

*1 管理者が管理者自身のアカウントのみを変更できます。

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
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
LDAP 検索	—	R/W	—	—	R/W	—
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
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	—	R/W	—	—	—	—

操作権限を確認する

eco 指数カウンター集計期間/管理者メッセージ設定

設定項目	User	機器	N/W	文書	なし	あり
インフォメーション画面表示	R	R/W	R	R	R/W	R
表示のタイミング	R	R/W	R	R	R/W	R
集計期間	R	R/W	R	R	R/W	R
管理者メッセージ	R	R/W	R	R	R/W	R

強制セキュリティー印字

設定項目	User	機器	N/W	文書	なし	あり
強制セキュリティー印字	R	R/W	R	R	R	R
印字位置調整	R	R/W	R	R	R	R

Web Image Monitor : 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
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
ジョブ仕分け	R	R/W	R	R	R	R
一時置き文書自動消去	R	R	R	R/W	R	R
保存文書自動消去	R	R	R	R/W	R	R
主電源 Off 時の未処理文書	R	R/W	R	R	R	R
180 度回転	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
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
印刷枚数	R	R/W	R	R	R	R
スムージング	R	R/W	R	R	R	R
トナーセーブ	R	R/W	R	R	R	R
予約印刷明け渡し時間設定	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
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
エラージョブ蓄積・追い越し	R	R/W	R	R	R	R
トレイ指定時動作切り替え	R	R/W	R	R	R	R
テスト印刷禁止	R	R/W	R	R	R	R
拡張リミットレス給紙	R	R/W	R	R	R	R
印刷をともなうジョブの制限	R	R/W	R	R	R	R
初期画面の切り替え	R	R/W	R	R	R	R
インターフェース設定	R	R/W	R	R	R	R
PS 設定	R	R/W	R	R	R	R
PDF 設定	R	R/W	R	R	R	R
スタンプ : ON/OFF 設定	R	R/W	R	R	R	R
スタンプ : 機密管理ナンバリング設定	R	R/W	R	R	R	R
スタンプ : スタンプ印字設定	R	R/W	R	R	R	R
スタンプ : ユーザースタンプ設定	R	R/W	R	R	R	R
スタンプ : 日付印字設定	R	R/W	R	R	R	R

不正コピー抑止

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
不正コピー抑止設定	R	R/W	R	R	R	R
優先する設定 (ドライバー/コマンド/ 機器側)	R	R/W	R	R	R	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
不正コピー抑止の種類	R	R/W	R	R	R	R
地紋マスクパターン/濃度/効果	R	R/W	R	R	R	R
抑止文字列設定	R	R/W	R	R	R	R

トレイ読み替え (PS)

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
トレイ読み替え (PS)	—	R/W	—	—	—	—

PDF 一時パスワード

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
PDF 一時パスワード	—	—	—	—	R/W	R/W

PDF グループパスワード

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
PDF グループパスワード	—	R/W	—	—	—	—

PDF 固定パスワード

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
PDF 固定パスワード	—	R/W	—	—	—	—

仮想プリンター設定

操作権限を確認する

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
プロトコル	R	R/W	R	R	R	R
エラーレポート印刷	R	R/W	R	R	R	R
ジョブ仕分け	R	R/W	R	R	R	R
180度回転	R	R/W	R	R	R	R
エミュレーション検知	R	R/W	R	R	R	R
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
印刷枚数	R	R/W	R	R	R	R
スムージング	R	R/W	R	R	R	R
トナーセーブ	R	R/W	R	R	R	R
補助用紙サイズ	R	R/W	R	R	R	R
給紙トレイ	R	R/W	R	R	R/W	R/W
用紙種類	R	R/W	R	R	R/W	R/W
排紙トレイ	R	R/W	R	R	R/W	R/W
レターヘッド紙使用設定	R	R/W	R	R	R	R
PS 設定	R	R/W	R	R	R	R
PDF 設定	R	R/W	R	R	R	R

Web Image Monitor : ファクス

[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、「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。

導入設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
ID 送受信用 ID	—	R/W	—	—	—	—
インターネットファクス	—	R/W	—	—	—	—
ダイヤルイン	—	R/W	—	—	—	—
メニュープロテクト	—	R/W	—	—	—	—
封筒 ID 登録	—	R/W	—	—	—	—
送信結果メール通知セキュリティー設定	—	R/W	—	—	—	—
発信元情報	—	R/W	—	—	—	—
ダイヤル/プッシュ選択	—	R/W	—	—	—	—
ISDN-G3 回線	—	R/W	—	—	—	—
ISDN-G4 回線	—	R/W	—	—	—	—
NGN 設定方法	—	R/W	—	—	—	—

送受信設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
送信メールサイズ制限	—	—	R/W	—	—	—
IP ファクス送信ルート自動切替 (IP/G3)	—	R/W	—	—	—	—

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
IP ファクス最大送信速度設定	—	R/W	—	—	—	—
受信モード切り替え	—	R/W	—	—	—	—
受信モード自動切り替え時設定	—	R/W	—	—	—	—
SMTP 受信ファイル配信設定	—	R/W	—	—	—	—
両面印刷	—	R/W	—	—	R/W	—
しおり印字	—	R/W	—	—	R/W	—
センターマーク印字	—	R/W	—	—	R/W	—
受信時刻印字	—	R/W	—	—	R/W	—
受信文書印刷部数	—	R/W	—	—	R/W	—
給紙トレイ選択	—	R/W	—	—	R/W	—
封筒受信	—	R/W	—	—	—	—

受信文書設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
出力切り替えタイマー設定	—	R/W	—	—	—	—
自動印刷禁止設定	—	R/W	—	—	—	—
待機文書印刷	—	R/W	—	—	—	—

IP-ファクス設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
H. 323	—	—	R/W	—	—	—
SIP	—	—	R/W	—	—	—

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
NGN 接続設定	—	—	R/W	—	—	—

IP-ファクスゲートウェイ設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
識別番号	—	—	R/W	—	—	—
プロトコル	—	—	R/W	—	—	—
ゲートウェイアドレス	—	—	R/W	—	—	—

パラメーター設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
ジャストサイズ印刷	—	R/W	—	—	—	—
集約印刷	—	R/W	—	—	—	—
フォルダー転送時 PDF 変換	—	R/W	—	—	—	—
自動印刷レポート	—	R/W	—	—	—	—
メール	—	R/W	—	—	—	—

Web Image Monitor : スキャナー

[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
あて先表見出し切り替え	R	R/W	R	R	R	R
あて先検索対象	R	R/W	R	R	R	R
TWAIN 割り込み禁止時間設定	R	R/W	R	R	R	R
あて先表初期表示選択	R	R/W	R	R	R	R
優先本体あて先表	R	R/W	R	R	R	R
送信履歴満杯時印刷設定	R	R/W	R	R	R	R
外部認証：フォルダーパス上書き設定	R	R/W	R	R	R	R

読み取り設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
次原稿待機設定	R	R/W	R	R	R	R
自動濃度の濃度設定（フルカラー）	R	R/W	R	R	R	R

送信設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
圧縮設定（白黒2値）	R	R/W	R	R	R/W	R
圧縮設定（グレースケール/フルカラー）	R	R/W	R	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
高圧縮 PDF 圧縮率設定	R	R/W	R	R	R/W	R
送信メールサイズ制限	R	R	R/W	R	R *1	R *1
メールサイズ制限オーバー時分割	R	R	R/W	R	R *1	R *1
メール付加情報	R	R/W	R	R	R/W	R
シングルページ開始番号桁設定	R	R/W	R	R	R/W	R
蓄積文書メール内容	R	R/W	R	R	R/W	R
デフォルトメール件名	R	R/W	R	R	R	R

*1 [管理者認証管理] の [ネットワーク管理] が [しない] に設定されているときは、ユーザーの権限は R/W になります。

導入設定

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
メニュープロテクト設定	R	R/W	R	R	R	—

初期値登録（機器通常画面用）

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
文書蓄積	—	R/W	—	—	R	R
プレビュー	—	R/W	—	—	R	R
読み取り条件	—	R/W	—	—	R	R
ファイル形式	—	R/W	—	—	R	R

初期値登録（機器簡単画面用）

操作権限を確認する

設定項目	User	機器	N/W	文書	Lv. 1	Lv. 2
読み取り条件	—	R/W	—	—	R	R
ファイル形式	—	R/W	—	—	R	R

Web Image Monitor : 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、「適用初期設定項目」の設定によって、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
ネットワークインターフェース選択	—	—	R/W	—	R	—
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/W	R
イーサネット速度	R	R	R/W	R	R/W	R
Bluetooth	R	R	R/W	R	R/W	R
動作モード	R	R	R/W	R	R/W	R
USB	R	R/W	R	R	R/W	R
USB ホスト	R	R	R	R	R	R

無線 LAN 設定

設定項目	User	機器	N/W	文書	なし	あり
ネットワークインターフェース選択	—	—	R/W	—	R	—
ネットワーク	R	R	R	R	R	R
物理アドレス	R	R	R	R	R	R
使用可能な無線 LAN	R	R	R	R	R	R
通信モード	R	R	R/W	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
SSID	R	R	R/W	R	R/W	R
チャンネル	R	R	R/W	R	R/W	—
セキュリティー方式	R	R	R/W	R	R/W	R
WEP 認証方式	—	—	R/W	—	R/W	—
WEP キー番号	R	R	R/W	R	R/W	R
WEP キー	R	R	R/W	R	R/W	R
WPA 認証方式	R	R	R/W	R	R/W	R
WPA-PSK/WPA2-PSK 設定	R	R	R/W	R	R/W	R

パラレルインターフェース

設定項目	User	機器	N/W	文書	なし	あり
パラレルインターフェース	—	R/W	—	—	R/W	R
パラレルタイミング	—	R/W	—	—	R/W	R
パラレル通信速度	—	R/W	—	—	R/W	R
セレクト状態	—	R/W	—	—	R/W	R
インプットプライム	—	R/W	—	—	R/W	R
双方向通信	—	R/W	—	—	R/W	R

Web Image Monitor : 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、「適用初期設定項目」の設定によって、ユーザーの操作権限は異なります。

IPv4

設定項目	User	機器	N/W	文書	なし	あり
IPv4	R	R	R	R	R	R
ホスト名	R	R	R/W	R	R/W	R
DHCP	R	R	R/W	R	R/W	R
ドメイン名	R	R	R/W	R	R/W	R
IPv4 アドレス	R	R	R/W	R	R/W	R
サブネットマスク	R	R	R/W	R	R/W	R
DDNS	R	R	R/W	R	R/W	R
WINS	R	R	R/W	R	R/W	R
プライマリ-WINS サーバー	R	R	R/W	R	R/W	R
セカンダリ-WINS サーバー	R	R	R/W	R	R/W	R
LLMNR	R	R	R/W	R	R/W	R
スコープ ID	R	R	R/W	R	R/W	R
詳細情報	R	R	R/W	R	R/W	R

IPv6

設定項目	User	機器	N/W	文書	なし	あり
IPv6	R	R	R/W	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
ホスト名	R	R	R/W	R	R/W	R
ドメイン名	R	R	R/W	R	R/W	R
リンクローカルアドレス	R	R	R	R	R	R
ステータスアドレス	R	R	R/W	R	R/W	R
手動設定アドレス	R	R	R/W	R	R/W	R
DHCPv6	R	R	R/W	R	R/W	R
DHCPv6 アドレス	R	R	R	R	R	R
DDNS	R	R	R/W	R	R/W	R
LLMNR	R	R	R/W	R	R/W	R
詳細情報	R	R	R/W	R	R/W	R

AppleTalk

設定項目	User	機器	N/W	文書	なし	あり
AppleTalk	R	R	R/W	R	R/W	R
ネットワーク番号	R	R	R	R	R	R
プリンター名	R	R	R/W	R	R/W	R
タイプ名	R	R	R	R	R	R
ゾーン名	R	R	R/W	R	R/W	R

SMB

設定項目	User	機器	N/W	文書	なし	あり
SMB	R	R	R/W	R	R/W	R

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
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/W	R
コンピュータ名	R	R	R/W	R	R/W	R
コメント	R	R	R/W	R	R/W	R
共有名	R	R	R	R	R	R
印刷完了通知	R	R	R/W	R	R/W	R

SNMP

設定項目	User	機器	N/W	文書	なし	あり
SNMP	—	—	R/W	—	—	—
プロトコル	—	—	R/W	—	—	—
SNMPv1, v2 共通設定	—	—	R/W	—	—	—
コミュニティー	—	—	R/W	—	—	—

SNMPv3

設定項目	User	機器	N/W	文書	なし	あり
SNMP	—	—	R/W	—	—	—
プロトコル	—	—	R/W	—	—	—
SNMPv3 設定	—	—	R/W	—	—	—
SNMPv3 Trap 送信設定	—	—	R/W	—	—	—
アカウント(一般)	—	—	R/W	—	—	—
アカウント(ネットワーク管理者)	—	—	R/W	—	—	—

操作権限を確認する

設定項目	User	機器	N/W	文書	なし	あり
アカウント(機器管理者)	—	R/W	—	—	—	—

SSDP

設定項目	User	機器	N/W	文書	なし	あり
SSDP	—	—	R/W	—	—	—
UUID	—	—	R	—	—	—
プロフィール有効期限	—	—	R/W	—	—	—
TTL	—	—	R/W	—	—	—

Bonjour

設定項目	User	機器	N/W	文書	なし	あり
Bonjour	R	R	R/W	R	R/W	R
ローカルホスト名	R	R	R	R	R	R
詳細情報	R	R	R/W	R	R/W	R
印刷優先順位	R	R	R/W	R	R/W	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	—

Web Image Monitor : セキュリティー

[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
ネットワークセキュリティー	—	—	R/W	—	—	—
アクセスコントロール	—	—	R/W	—	—	—
IPP 認証	—	—	R/W	—	—	—
SSL/TLS	—	—	R/W	—	—	—
Ssh	—	—	R/W	—	R	R
サイト証明書	—	—	R/W	—	—	—
機器証明書	—	—	R/W	—	—	—
S/MIME	—	—	R/W	—	—	—
IPsec	—	—	R/W	—	—	—
ユーザーロックアウト	—	R/W	—	—	—	—
IEEE 802.1X	—	—	R/W	—	—	—

Web Image Monitor : Webpage

[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、「適用初期設定項目」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	なし	あり
Web 表示言語	R	R	R/W	R	R/W	R
リンクページのリンク先設定	R	R	R/W	R	R/W	R
ホームでの関連サイトのリンク表示	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
ヘルプファイルをダウンロードする	R/W	R/W	R/W	R/W	R/W	R/W

Web Image Monitor : 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 *1	R/W *1
変更	R/W	—	—	—	R/W *1	R/W *1
削除	R/W	—	—	—	R/W *1	R/W *1
グループ追加	R/W	—	—	—	R/W *1	R/W *1
アドレス帳自動登録時データ利用設定	R/W	—	—	—	R/W *1	R/W *1
メンテナンス	R/W	—	—	—	R/W *1	R/W *1

*1 [セキュリティ強化] の [個人宛先登録制限 (ファクス)]、[個人宛先登録制限 (スキヤナー)]、またはその両方を [する] に設定したときは、ベーシック認証設定時に、自身のアカウントのパスワードのみ変更できます。

操作権限を確認する

Web Image Monitor : 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	—	—	—	—

操作権限を確認する

Web Image Monitor : 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、「適用初期設定項目」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	なし	あり
リセット	—	R/W	—	—	R/W	—

Web Image Monitor : 機器のホーム画面の管理

[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、「適用初期設定項目」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	なし	あり
アイコンの編集	R	R/W	R	R	R/W	R
アイコンを初期値に戻す	—	R/W	—	—	R/W	—
ホーム画面設定	R	R/W	R	R	R/W	R

操作権限を確認する

Web Image Monitor : ユーザーカスタマイズ

ユーザーは自身の設定だけを変更できます。

設定項目	User	機器	N/W	文書	なし	あり
アイコンの編集	—	—	—	—	—	R/W
アイコンを初期値に戻す	—	—	—	—	—	R/W
ユーザー別優先機能設定	—	—	—	—	—	R/W

Web Image Monitor : ドキュメントボックス

[文書操作] の中の項目です。

蓄積文書のユーザー操作は、文書のアクセス権によって異なります。詳しくは、P. 343 「蓄積文書の操作権限一覧」を参照してください。

設定項目	User	機器	N/W	文書	なし	あり
印刷	—	—	—	—	R/W	R/W
送信	—	—	—	—	R/W	R/W
削除	—	—	—	R/W	R/W	R/W
詳細情報の編集 (詳細情報アイコン)	—	—	—	R/W	R/W	R/W
ダウンロード	—	—	—	—	R/W	R/W
文書ロック解除	—	—	—	R/W	—	—

Web Image Monitor : ファクス蓄積受信文書

[文書操作] の中の項目です。

設定項目	User	機器	N/W	文書	なし	あり
印刷	—	—	—	—	R/W *1	R/W *1
削除	—	—	—	—	R/W *1	R/W *1
ダウンロード	—	—	—	—	R/W *1	R/W *1
詳細情報の編集	—	—	—	—	R/W *1	R/W *1

*1 [ファクス初期設定] → [受信設定] → [蓄積受信文書ユーザー設定] を [する] に設定している場合は、指定されたユーザーのみ文書の操作ができます。

Web Image Monitor : プリンター文書印刷

[文書操作]の中の項目です。

ユーザーは、自身で蓄積したプリンター文書、またはユーザー認証を設定していないときに蓄積されたプリンター文書进行操作できます。

他のユーザーが蓄積したプリンター文書は表示されません。

設定項目	User	機器	N/W	文書	なし	あり
印刷	—	—	—	—	R/W *1	R/W *1
削除	—	—	—	R/W	R/W *1	R/W *1
詳細情報の編集 (詳細情報アイコン)	—	—	—	R/W	R/W *1	R/W *1
文書ロック解除	—	—	—	R/W	—	—

*1 保存文書は、設定されたアクセス権によって操作権限が異なります。

蓄積文書の操作権限一覧

ヘッダーの見方

- 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。
- オーナー
文書を登録したユーザー、またはオーナーとして設定されたユーザーです。
- 文書
文書管理者です。

マークの見方

R/W : 実行できます。

— : 実行できません。

設定項目	閲覧	編集	編/削	フル	オーナー	文書
印刷	R/W	R/W	R/W	R/W	R/W	—
詳細	R/W	R/W	R/W	R/W	R/W	R/W
プレビュー	R/W	R/W	R/W	R/W	R/W	—
アクセス権変更 : オーナー	—	—	—	—	—	R/W
アクセス権変更 : アクセス許可 ユーザー/グループ	—	—	—	R/W	R/W*1	R/W
ユーザー名変更	—	—	—	—	—	R/W
文書名変更	—	R/W	R/W	R/W	R/W*1	—
パスワード変更	—	—	—	—	R/W	R/W

操作権限を確認する

設定項目	閲覧	編集	編/削	フル	オーナ ー	文書
文書ロック解除	—	—	—	—	—	R/W
文書の結合	—	—	R/W	R/W	R/W*1	—
文書挿入	—	—	R/W	R/W	R/W*1	—
ページの削除	—	—	R/W	R/W	R/W*1	—
指定ページ印刷	R/W	R/W	R/W	R/W	R/W	—
文書複製	R/W	R/W	R/W	R/W	R/W	—
文書消去	—	—	R/W	R/W	R/W*1	R/W

*1 オーナーの任意によって、操作権限を変更できます。

アドレス帳の操作権限一覧

ヘッダーの見方

- 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になります。
- User
ユーザー管理者です。

マークの見方

- 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。

登録情報

設定項目	閲覧	編集	編/削	フル	登録者	User
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
キー表示名	R	R/W	R/W	R/W	R/W	R/W
登録番号	R	R/W	R/W	R/W	R/W	R/W
見出し選択	R	R/W	R/W	R/W	R/W	R/W

認証情報

操作権限を確認する

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
SMTP 認証	—	—	—	—	R/W*1	R/W*1
フォルダー認証	—	R/W*1	R/W*1	R/W*1	R/W*1	R/W*1
LDAP 認証	—	—	—	—	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
使用対象	R	R/W	R/W	R/W	R/W	R/W
宛先保護: 保護コード	—	—	—	R/W*2	R/W*2	R/W*2
宛先保護: 保護対象	—	R/W	R/W	R/W	R/W	R/W
宛先保護: アクセス許可ユーザー/グループ	—	—	—	R/W	R/W	R/W
文書保護: アクセス許可ユーザー/グループ	—	—	—	R/W	R/W	R/W

*2 保護コードは閲覧できません。

ファクス

設定項目	閲覧	編集	編/削	フル	登録者	User
ファクス宛先	R	R/W	R/W	R/W	R/W	R/W

操作権限を確認する

設定項目	閲覧	編集	編/削	フル	登録者	User
回線選択	R	R/W	R/W	R/W	R/W	R/W
拡張宛先	R	R/W	R/W	R/W	R/W	R/W
海外送信モード	R	R/W	R/W	R/W	R/W	R/W
発信元名称選択	R	R/W	R/W	R/W	R/W	R/W
宛名差し込み	R	R/W	R/W	R/W	R/W	R/W

メールアドレス

設定項目	閲覧	編集	編/削	フル	登録者	User
メールアドレス	R	R/W	R/W	R/W	R/W	R/W
メールアドレス使用対象	R	R/W	R/W	R/W	R/W	R/W
SMTP サーバーを經由	R	R/W	R/W	R/W	R/W	R/W

フォルダー

設定項目	閲覧	編集	編/削	フル	登録者	User
SMB/FTP/NCP 選択	R	R/W	R/W	R/W	R/W	R/W
SMB パス名	R	R/W	R/W	R/W	R/W	R/W
FTP サーバー名	R	R/W	R/W	R/W	R/W	R/W
FTP パス名	R	R/W	R/W	R/W	R/W	R/W
FTP 日本語文字コード	R	R/W	R/W	R/W	R/W	R/W
FTP ポート番号	R	R/W	R/W	R/W	R/W	R/W
NCP パス名	R	R/W	R/W	R/W	R/W	R/W
NCP 接続種別	R	R/W	R/W	R/W	R/W	R/W

操作権限を確認する

設定項目	閲覧	編集	編/削	フル	登録者	User
接続テスト	—	R/W	R/W	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
見出し切り替え	R/W	R/W	R/W	R/W	R/W	R/W

↓ 補足

- [セキュリティ強化] の [個人宛先登録制限 (ファクス)]、[個人宛先登録制限 (スキャナー)]、またはその両方を [する] に設定すると、ユーザーの操作権限に関係なく、ユーザー管理者以外のユーザーは、アドレス帳へのアクセスができなくなります。

商標

- ドキュメントボックス、RPCS、RP-GL/2、RTIFF は株式会社リコーの商標または登録商標です。
- Adobe、Acrobat、PostScript、Reader は、Adobe Systems Incorporated（アドビ システムズ社）の米国ならびにその他の国における登録商標または商標です。
- AppleTalk、Mac OS、Bonjour は、米国および他の国々で登録された Apple Inc. の商標です。
- Linux は Linus Torvalds の米国およびその他の国における登録商標または商標です。
- Lotus Notes は世界の多くの国で登録された IBM Corp. の商標です。
- Microsoft、Windows、Windows Server、Windows Vista、Internet Explorer、Outlook は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- RED HAT は、米国およびその他の国において登録された Red Hat, Inc. の商標です。
- Solaris は、米国 Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
- Thunderbird は、Mozilla Foundation の商標です。
- UPnP is a trademark of UPnP Implementers Corporation.
- Internet Explorer 6 の正式名称は Microsoft® Internet Explorer® 6 です。
- Windows XP の製品名は以下のとおりです。
 - Microsoft® Windows® XP Professional
 - Microsoft® Windows® XP Home Edition
 - Microsoft® Windows® XP Media Center Edition
 - Microsoft® Windows® XP Tablet PC Edition
- Windows Vista の製品名は以下のとおりです。
 - Microsoft® Windows Vista® Ultimate
 - Microsoft® Windows Vista® Business
 - Microsoft® Windows Vista® Home Premium
 - Microsoft® Windows Vista® Home Basic
 - Microsoft® Windows Vista® Enterprise
- Windows 7 の製品名は以下のとおりです。
 - Microsoft® Windows® 7 Home Premium
 - Microsoft® Windows® 7 Professional
 - Microsoft® Windows® 7 Ultimate
 - Microsoft® Windows® 7 Enterprise

操作権限を確認する

- Windows Server 2003 の製品名は以下のとおりです。
Microsoft® Windows Server® 2003 Standard Edition
Microsoft® Windows Server® 2003 Enterprise Edition
 - Windows Server 2003 R2 の製品名は以下のとおりです。
Microsoft® Windows Server® 2003 R2 Standard Edition
Microsoft® Windows Server® 2003 R2 Enterprise Edition
 - Windows Server 2008 の製品名は以下のとおりです。
Microsoft® Windows Server® 2008 Standard
Microsoft® Windows Server® 2008 Enterprise
 - Windows Server 2008 R2 の製品名は以下のとおりです。
Microsoft® Windows Server® 2008 R2 Standard
Microsoft® Windows Server® 2008 R2 Enterprise
- その他の製品名、名称は各社の商標または登録商標です。

索引

- A-**
AH プロトコル 123
- E-**
eco 指数カウンター 227
ESP プロトコル 123
- I-**
IEEE 802.1X 方式の認証を設定する . 148
IPP 認証のパスワード 156
IPsec 通信 123
- K-**
Kerberos 認証 32, 158
- L-**
LDAP 認証 40
- N-**
NTLM 認証 32
- S-**
S/MIME 115
SMTP 通信の SSL を設定する 114
SNMPv1, v2 による設定 230
SNMPv3 暗号化通信を設定する 154
SSL 110
SSL/TLS 通信許可設定 113
- あ-**
アクセスコントロール 91
宛先利用制限 55
宛先利用制限 (スキャナー) 230
宛先利用制限 (ファクス) 230
アドレス帳の暗号化 230
アドレス帳の操作権限 345
暗号化通信モード 113
暗号強度設定 230
- い-**
イーサネットで IEEE802.1X を使用する
..... 149
- 印刷利用量制限 62
- え-**
エラーコード 252
エラーメッセージ 250
遠隔診断 (ファクス) 230, 240
- お-**
オートログアウト 54
- か-**
管理者 9
管理者認証 10
管理者の種類 57
管理者の登録 12
管理者の変更 12
- き-**
機器証明書 108, 110, 117, 149
機器設定の変更防止 57
機能の利用制限 60
機密印刷文書の管理 173
強制蓄積 177
- こ-**
個人宛先登録制限 55
個人宛先登録制限 (スキャナー) ... 230
個人宛先登録制限 (ファクス) 230
個人情報表示制限 230
誤送信防止 238
- さ-**
サーバー証明書 38
サービスモード移行禁止設定 240
サイト証明書の導入 148
- し-**
実行中ジョブへの認証の実施 230
自動鍵 124

索引

受信指定宛先への転送（ファクス）	230	ファームウェア構成変更	230
手動鍵	124	プリンタジョブ認証	45
商標	349	プロトコル	92
署名	117	文書パスワード	165
-す-		文書保護強化	230
スーパーバイザー	19	文書ロック解除	166
-せ-		-へ-	
セキュリティー機能	238	ベーシック認証	28
セキュリティー機能を使う前に	7	-む-	
セキュリティー強化機能	230	無線 LAN で IEEE 802.1X を使用する	151
セキュリティー設定	8	-め-	
-そ-		メニュープロテクト	57, 58
操作権限	274	メモリー自動消去設定	83
-ち-		メモリー全消去	88
蓄積受信文書ユーザー設定	238	-ゆ-	
蓄積文書の操作権限	343	ユーザーコード認証	26
中間証明書	109	ユーザー証明書	116
-つ-		ユーザー認証	22
通信管理レポートの出力	238	ユーザー認証設定	24
通信経路の保護	106	ユーザー認証に失敗したとき	250
-て-		-り-	
電子署名付き PDF	121	利用量制限	62
-と-		履歴満杯時印刷	239
ドライバ暗号鍵	156, 230	-ろ-	
-に-		ログアウト（管理者）	18
認証情報	29	ログイン（管理者）	16
-ね-		ログインパスワードの設定	30
ネットワークセキュリティーレベル	98	ログインユーザー名の設定	30
-は-		ログイン用認証情報	30
パスワードポリシー	230	ログ情報の管理	178
パスワードロックアウト解除	52	ログ情報の管理（Web Image Monitor）	179, 185
パスワードロックアウト設定	52	ログ情報の管理（本機）	178
パスワードを暗号化通信する	156	ログの暗号化	179
-ふ-		ログの一括消去	178, 179
ファームウェアアップデート	230	ログの種類	178
ファームウェアアップデート時の注意	8		

索引

ログのダウンロード	179	ロックアウト機能.....	51
ログの転送	178, 179		