RICOH



RICOH MP C6004/C5504/C4504/C3504/
C3004/C2504シリーズ

使用説明書
〈セキュリティーガイド〉

安全に正しくお使いいただくために、操作の前には必ず『はじめにお読みください』「安全上のご注意」をお読みください。

目次

1. はじめに

セキュリティー機能を設定する前に....9
本機の運用を開始する前に....10
管理者とユーザー....11
管理者とは....12
管理者認証を設定する....13
管理者の権限を設定する....14
管理者を登録、変更する....15
Web Image Monitor を使用して管理者認証を設定する....18
管理者のログイン方法....19
操作部からログインする....19
Web Image Monitor からログインする....20
管理者のログアウト方法....21
操作部からログアウトする....21
Web Image Monitor からログアウトする....21
スーパーバイザーとは....22
管理者のパスワードを再設定する....22
スーパーバイザーを変更する....23

2. ユーザー認証を設定する

ユーザーとは....25
ユーザー認証の概念....26
ユーザー認証を設定する....27
ユーザーコード認証....29
ベーシック認証....32
ベーシック認証を設定する....32
アドレス帳の認証情報....34
ログインユーザー名とログインパスワードを設定する....34
ログイン用認証情報を設定する....35
Windows 認証....37
Windows 認証を設定する....39
「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....43
サーバー証明書を作成する....45
ファクス情報を取得できなかったとき....45

LDAP 認証....47
プリンタージョブ認証....52
プリンタージョブ認証のレベル....52
プリンタージョブの種類....52
authfree コマンド....54
アドレス帳の自動登録....56
自動登録されるアドレス帳の項目....56
アドレス帳自動登録時データ利用設定....56
ロックアウト機能....58
パスワードロックアウト設定....59
パスワードロックアウト解除....59
オートログアウト時間設定....60
かんたんカード認証....62
かんたんカード認証を設定する....62
IC カードリーダー設定を変更する....62
アドレス帳登録ユーザーに IC カードまたはスマートデバイスを登録する....63
優先ユーザーを設定する....64
外部機器を使用した認証....65
IC カード認証システムを使用する....65
FeliCa を使用して管理者を登録する....66

3. 機器の使用を制限する

宛先表の使用を制限する....67
管理者設定項目の変更を防止する....69
管理者による設定の変更を制限する....69
ユーザーによる設定の変更を禁止する....69
メニュープロテクトを設定する....70
コピー機能....70
ファクス機能....70
プリンター機能....70
スキャナー機能....71
プログラムの登録／変更を禁止する....71
機能の使用を制限する....72
メディアスロットへのアクセスを制限する....74

ユーザーの印刷利用量を制限する....75
利用量制限を設定する....76
利用量上限の初期値を設定する....78
ユーザーごとに利用量上限を設定する....79
ユーザーの利用量を確認する....80
ユーザーの利用量カウンターを印刷する....81
利用量カウンターをクリアする....82
自動リセット機能を設定する....83

4. 機器情報の漏えいを防止する

アドレス帳の登録情報を保護する....85
アドレス帳にアクセス権を設定する....85
アドレス帳を暗号化する....87
機器のデータを暗号化する....89
暗号化設定を有効にする....91
暗号鍵をバックアップする....92
暗号鍵を更新する....93
暗号化を解除する....94
機器のデータを上書き消去する....96
メモリー自動消去....96
メモリー全消去....100

5. ネットワークセキュリティーを強化する

アクセスコントロールを設定する....105
プロトコルの有効／無効を設定する....106
操作部から設定する....109
Web Image Monitor から設定する....109
ネットワークセキュリティーレベルを設定する....111
操作部から設定する....111
Web Image Monitor から設定する....112
各機能とネットワークセキュリティーレベルの関係....112
機器証明書による通信経路の保護....116
操作部から機器証明書を作成、導入する（自己証明書）....116
Web Image Monitor から機器証明書を作成、導入する（自己証明書）....117
機器証明書を作成、申請する（認証局証明書）....118

機器証明書を導入する（認証局証明書）.....119
中間証明書を導入する（認証局証明書）.....119
SSL/TLS を設定する.....121
SSL/TLS を有効にする.....122
SSL/TLS のユーザー設定.....123
SSL/TLS 暗号化通信モードを設定する.....124
SMTP 通信の SSL を設定する.....125
S/MIME を設定する.....126
メッセージを暗号化する.....126
署名を添付する.....128
証明書の有効期限チェックを設定する.....130
電子署名付き PDF の設定をする.....132
IPsec を設定する.....133
通信データの暗号化と認証.....133
自動鍵交換設定.....134
IPsec 設定項目.....135
自動鍵交換設定の流れ.....139
telnet で IPsec を設定する.....144
IEEE 802.1X 認証を設定する.....149
サイト証明書を導入する.....149
機器証明書を選択する.....150
イーサネットで IEEE 802.1X を使用する.....150
無線 LAN で IEEE 802.1X を使用する.....152
SNMPv3 暗号化通信を設定する.....155
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.....159

6. 文書の漏えいを防止する

フォルダーを管理する.....161
フォルダーを削除する.....161
フォルダーのパスワードを変更する.....162
フォルダーのロックを解除する.....163

蓄積文書を管理する..... 164
蓄積文書ごとにアクセス権を設定する.....164
蓄積文書のオーナーを変更する.....167
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..... 168
蓄積文書にパスワードを設定する..... 169
蓄積文書のロックを解除する.....171
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.....175
機密印刷文書のロックを解除する..... 176
不正コピー抑止／不正コピーガード機能..... 178
地紋印刷を有効にする.....178
不正コピーガード検知を有効にする..... 180
印刷紙にユーザー情報を印字する.....182
プリンターの印刷文書を強制的に蓄積する.....184

7. 本機を管理する

ログを管理する.....185
Web Image Monitor からログを管理する.....186
Web Image Monitor で管理できるログ項目..... 186
ダウンロードできるログ情報の属性一覧.....190
収集するログを設定する..... 212
ログをダウンロードする..... 213
本機に保持できるログ件数..... 214
ログフル時の注意事項.....215
プリンター印刷時のログ..... 216
ログを一括消去する.....217
ログ収集サーバーへのログ転送を無効にする..... 218
本機からログを管理する.....219
収集するログを設定する..... 219
ログ収集サーバーへのログ転送を無効にする..... 219
ログを一括消去する.....220
ログ収集サーバーからログを管理する.....220
ユーザー別ホームを設定する..... 221

ユーザー別ホーム使用時の注意事項 221
ブラウザー機能を設定する 223
Web ブラウザーを使用する前に 223
こんなときには 223
機器情報を管理する 225
機器情報をエクスポートする 226
機器情報をインポートする 228
機器情報を定期的にインポートする 229
サーバーの設定情報ファイルを手動でインポートする 232
こんなときには 233
eco 指数カウンターを管理する 235
eco 指数カウンターの表示を設定する 235
機器の eco 指数カウンターをクリアする 236
ユーザーの eco 指数カウンターをクリアする 237
アドレス帳を管理する 238
アドレス帳の自動消去を設定する 238
アドレス帳の一括消去 238
セキュリティー強化機能を設定する 239
その他のセキュリティー機能 248
ファクス機能 248
スキャナー機能 249
システム状態 249
ファームウェアの正当性確認 249
カスタマーエンジニアの操作を制限する 251
より安全にお使いいただくために 252
操作部から設定する項目 252
Web Image Monitor から設定する項目 254
IPsec 有効/無効時の設定 255

8. こんなときには

メッセージが表示されたとき 259
エラーコードが表示されたとき 260
ベーシック認証時のエラーコード 260
Windows 認証時のエラーコード 261

LDAP 認証時のエラーコード....266
IC カード認証時のエラーコード....270
操作ができないとき....271

9. 設定項目の操作権限一覧

表の見方....277
システム初期設定....278
コピー／ドキュメントボックス初期設定....286
ファクス初期設定....291
プリンター通常画面....294
プリンター初期設定....295
スキャナー初期設定....300
ブラウザー設定....302
拡張機能初期設定....303
調整／管理....304
操作部初期設定....305
ホーム編集....306
かんたんカード認証設定....307
Web Image Monitor: eco 指数カウンター表示....308
Web Image Monitor：ジョブ....309
Web Image Monitor：操作部初期設定....310
Web Image Monitor：機器....311
Web Image Monitor：プリンター....319
Web Image Monitor：ファクス....323
Web Image Monitor：スキャナー....325
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....332
Web Image Monitor：@Remote....334
Web Image Monitor：Webpage....335
Web Image Monitor：拡張機能初期設定....336
Web Image Monitor：アドレス帳....337
Web Image Monitor：集中管理設定....338
Web Image Monitor：主電源オフ....339

Web Image Monitor：印刷取消.....340
Web Image Monitor：機器のリセット.....341
Web Image Monitor：操作部画面の監視.....342
Web Image Monitor：ドキュメントボックス.....343
Web Image Monitor：ファクス蓄積受信文書.....344
Web Image Monitor：プリンター文書印刷.....345
蓄積文書の操作権限一覧.....346
アドレス帳の操作権限一覧.....347
索引.....351

1. はじめに

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

セキュリティー機能を設定する前に

重要

- **機器のセキュリティー設定をしないときは、悪意を持った攻撃者により被害を受けることがあります。**
- 本機が持ち出されたり壊されたり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。
- 本機購入者は、本機を適切に運用して頂ける方を、管理者とスーパーバイザーとして選定し、その方の管理下で運用してください。管理者とスーパーバイザーが適切な運用をしないときは、ユーザーにセキュリティーの被害が発生する恐れがあります。
- 管理者の方はセキュリティー機能を使用する前に、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。
- 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、使用方法をご指導ください。
- 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。
- 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使用するときは、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。
- 例外や異常な動作を確認するためには、定期的なログ情報の監査をお勧めします。

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してください。情報の暗号化通信を有効にし、管理者アカウントを設定します。

1. **本機の主電源を入れます。**

   主電源の入れかたは、『本機をお使いになる方へ』「電源の入れかた、切りかた」を参照してください。

2. **画面中央下の［ホーム］（）を押します。**
3. **左にフリックし、［初期設定］アイコン（）を押します。**
4. **［本体初期設定］を押します。**
5. **［システム初期設定］を押します。**
6. **［インターフェース設定］を押します。**
7. **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。

8. **［システム初期設定］の［ファイル転送設定］を押します。**
9. **［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。**
10. **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.116「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 9 で入力した管理者メールアドレスを設定してください。

11. **管理者のログインユーザー名、パスワードを変更します。**

    管理者のログインユーザー名、パスワードの設定については、P.15「管理者を登録、変更する」を参照してください。

12. **本機を運用環境で使用するネットワークに接続します。**

補足

- より高度なセキュリティーを希望するときは、P.252「より安全にお使いいただくために」を参照してください。

管理者とユーザー

本書で扱っている「管理者」、「スーパーバイザー」、「ユーザー」、「オーナー」の用語について説明します。

管理者

本機の管理者は４人（４種類）います。ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者です。

主な役割は、本機を運用するための各種設定です。管理者によって操作権限が異なります。コピーやプリンター印刷などの通常の操作はできません。

スーパーバイザー

スーパーバイザーは１人です。各管理者のパスワードを設定できます。

通常の運用では、管理者のパスワードは管理者自身が設定するためスーパーバイザーを使用しません。

ユーザー

コピーやプリンターなど通常の操作で本機を使用する人たちです。

オーナー

コピーやプリンターなどで本機に文書を登録したユーザーです。

管理者とは

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

管理者がアクセス制限や設定項目を管理するときは、まず本機の管理者を決定し、認証機能を有効にします。認証機能を有効にすると、本機を使用するときに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 人で兼務することも、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.15「管理者を登録、変更する」、スーパーバイザーについては P.22「スーパーバイザーとは」、ユーザーについては P.25「ユーザーとは」を参照してください。

管理者認証を設定する

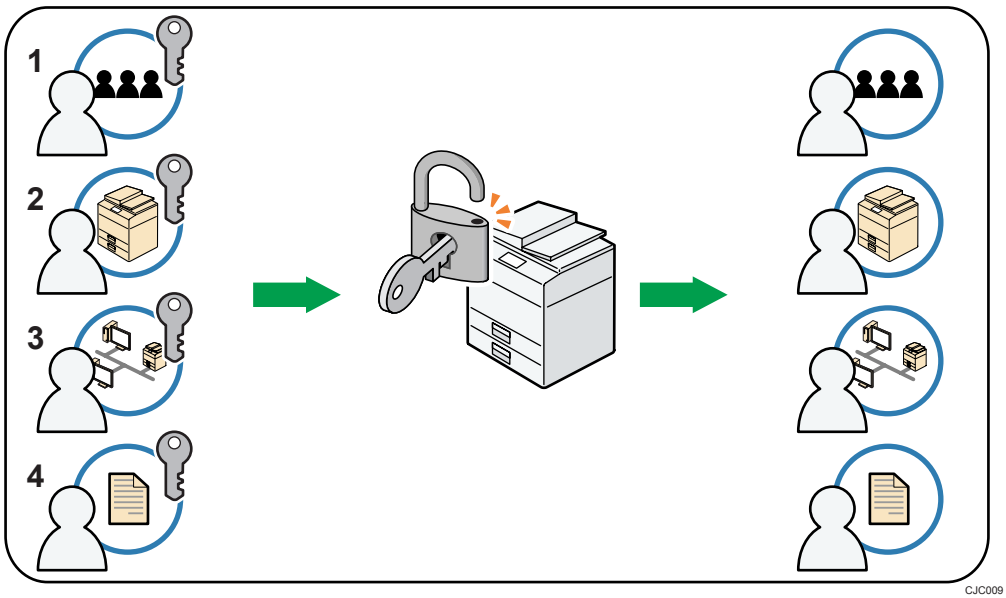
管理者認証とは、管理者が本機の各種設定を開始するとき、またはネットワークから本機にアクセスするとき、ログインユーザー名とログインパスワードによって確認する仕組みです。

管理者はアドレス帳に登録されるユーザーとは区別されます。管理者を登録するときに、すでにアドレス帳に登録されているログインユーザー名は使用できません。また、Windows 認証や LDAP 認証の対象にならないので、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.15「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。Ridoc IO Device Manager 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.27「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を管理します。ユーザー管理者は、アドレス帳へユーザーを登録・削除したり、ユーザーの個人情報を変更できます。アドレス帳に登録されたユーザー自身も自分の

情報を変更、削除できます。ユーザー管理者はユーザーが自分のパスワードを忘れたときに削除したり、新規に設定でき、ユーザーが操作できなくなることを防止できます。

2. **機器管理者**

主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。本機に蓄積した文書を、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えい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。

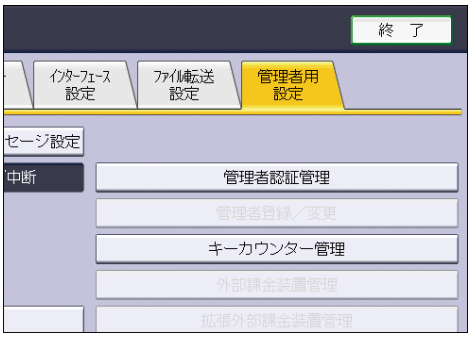
管理者認証のログイン、ログアウトの方法は、P.19「管理者のログイン方法」、P.21「管理者のログアウト方法」を参照してください。

重要

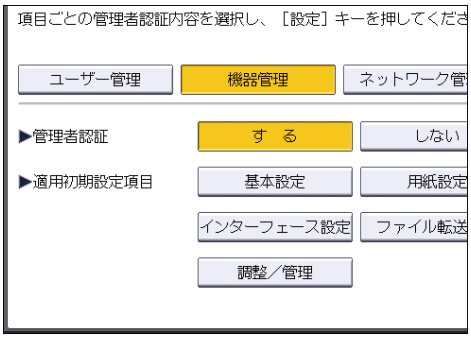
- **管理者認証を有効にしたときは、管理者のログインユーザー名とログインパスワードを絶対に忘れないようにしてください。万一忘れたときは、スーパーバイザーの権限でパスワードを新しく設定します。スーパーバイザーの権限については、P.22「スーパーバイザーとは」を参照してください。**

1. 画面中央下の［ホーム］（）を押します。
2. 左にフリックし、［初期設定］アイコン（）を押します。
3. ［本体初期設定］を押します。
4. ［システム初期設定］を押します。

5. [管理者用設定] を押します。
6. [▼次へ] を押します。
7. [管理者認証管理] を押します。



8. [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。
9. 「管理者認証」で [する] を選択します。
10. 「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。

管理者の種別によって設定項目は異なります。

複数のカテゴリーに管理者認証を設定するときは、手順 8 から 10 を繰り返します。

11. [設定] を押します。
12. 画面右上の [初期設定] () を押します。
13. 画面中央下の [ホーム] () 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す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

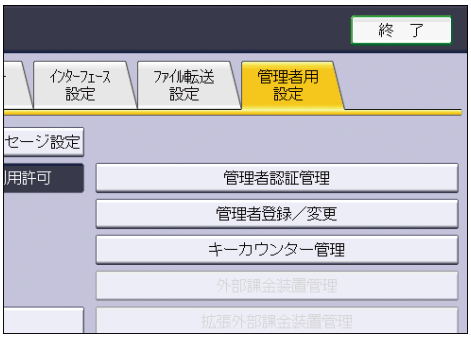
者による不正操作も制限できます。管理者の権限を与えられるログインユーザー名は管理者 1～4 の 4 件です。

各管理者の権限は、その管理者権限を持つ管理者だけが変更できます。

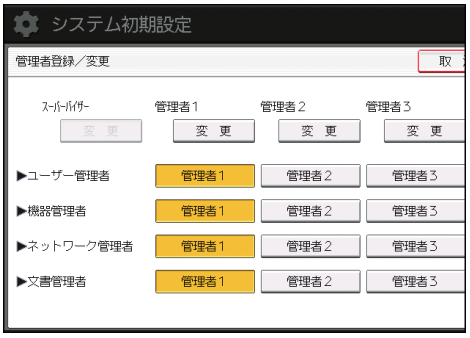
各管理者権限には、必ず 1 人以上の管理者を割り当ててください。

管理者認証のログイン、ログアウトの方法は、P.19「管理者のログイン方法」、P.21「管理者のログアウト方法」を参照してください。

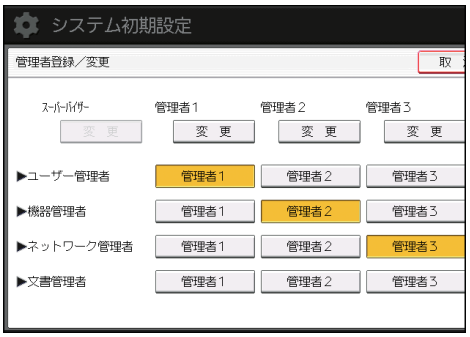
1. **操作部から管理者がログインします。**
2. **[システム初期設定] を押します。**
3. **[管理者用設定] を押します。**
4. **[▼次へ] を押します。**
5. **[管理者登録／変更] を押します。**



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。**



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。



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。
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。
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.239「セキュリティー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.17「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。
- リコー IC カード、または FeliCa を使用して管理者登録できます。登録方法は IC カード認証の使用説明書を参照してください。

ユーザー名、パスワードに使用できる文字

ログインユーザー名とログインパスワードには、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。
- 空白にはできません。
- 管理者は半角で 8 桁以下の数字だけでは登録できません。
- 最大文字数は半角で 32 文字です。

ログインパスワード

- 最大文字数は管理者とスーパーバイザーは 32 文字、ユーザーは 128 文字です。
- パスワードに禁則文字はありません。ただしセキュリティー上、アルファベットの大文字、小文字、数字、記号を組み合わせて作成することをお勧めします。文字数が多いほど第三者に推測されにくくなります。
- ［セキュリティー強化］の［パスワードポリシー］の設定で、英大文字、英小文字、数字、記号の組み合わせと最小文字数を設定できます。パスワードポリシーの設定方法は、P.239「セキュリティー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.19「管理者のログイン方法」、P.21「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。

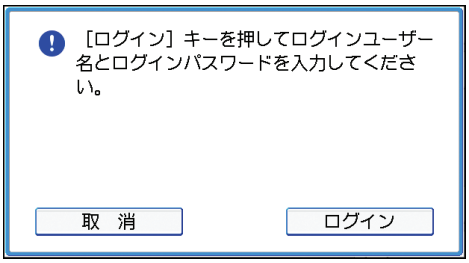
管理者のログイン方法

管理者認証が設定されているときは、管理者のログインユーザー名とパスワードでログインします。スーパーバイザーも同じ方法でログインします。

管理者とスーパーバイザーのログインユーザー名、ログインパスワードについては管理者へ問い合わせてください。

操作部からログインする

1. 画面中央下の［ホーム］（）を押します。
2. 左にフリックし、［初期設定］アイコン（）を押します。
3. ［本体初期設定］を押します。
4. ［ログイン］を押します。
5. ［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。

6. 管理者のログインユーザー名を入力し、［実行］を押します。
7. 管理者のログインパスワードを入力し、［実行］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持つログインユーザー名でログインしたときは、管理者権限を持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。

Web Image Monitor からログインする

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

   IPv4 アドレスを入力するときは、各セグメントの先頭につく「0」は入力しないでください。たとえば「192.168.001.010」のときは、「192.168.1.10」と入力します。

   「192.168.001.010」と入力すると、本機に接続できません。

   IPv6 アドレスは［2001:db8::9abc］のように、前後に［ ］をつけて入力してください。

   「SSL/TLS 通信許可設定」を［暗号文のみ］に設定した場合に、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。
3. **画面右上の［ログイン］をクリックします。**
4. **管理者のログインユーザー名とログインパスワードを入力し、［ログイン］をクリックします。**

補足

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

管理者のログアウト方法

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

操作部からログアウトする

1. [ログアウト]を押し、[実行]を押します

補足

- ジョブが終了したあとに［省エネ］を押してもログアウトできます。

Web Image Monitor からログアウトする

1. 画面右上の［ログアウト］をクリックします。

補足

- ログアウト後は、Web ブラウザーのキャッシュを削除してください。

スーパーバイザーとは

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

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

ログイン、ログアウトの方法は管理者と同様です。P.19「管理者のログイン方法」、P.21「管理者のログアウト方法」を参照してください。

重要

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

補足

- ログインユーザー名、ログインパスワードに使用できる文字は、P.17「ユーザー名、パスワードに使用できる文字」を参照してください。
- スーパーバイザーと各管理者は同じログインユーザー名にできません。
- 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.19「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。



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ユーザー名やログイン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.14「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.19「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. 「スーパーバイザー」の［変更］を押します。
7. 「ログインユーザー名」の［変更］を押します。
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。

10. ログインパスワードを入力し、[OK] を押します。
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. [設定] を 2 回押します。

    自動的にログアウトされます。

2. ユーザー認証を設定する

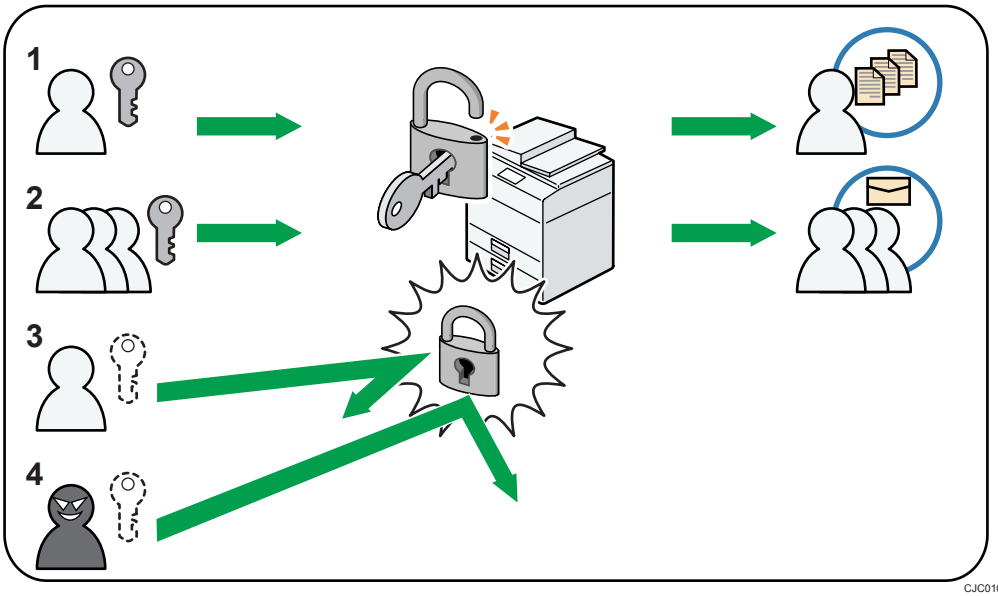
ユーザー認証の設定方法と、ユーザー認証によって有効になる機能について説明します。

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使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.12「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』「ユーザー情報を登録する」、または Web Image Monitor のヘルプを参照してください。

ユーザー認証の概念

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



1. ユーザー

   文書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。緊急のときに使用してください。**
- **同時に 2 つ以上の認証方法は設定できません。**

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.14「管理者の権限を設定する」 P.15「管理者を登録、変更する」
ユーザー認証を設定する	ユーザー認証には以下の方法があります。 • P.29「ユーザーコード認証」 • P.32「ベーシック認証」 • P.37「Windows 認証」 • P.47「LDAP 認証」

ユーザー認証の方法

認証方法	詳細
ユーザーコード認証	8 桁のユーザーコードを使って認証します。個人単位ではなくユーザーコードごとに認証します。 事前にユーザーコードを本機のアドレス帳に登録してください。
ベーシック認証	本機のアドレス帳を使って認証します。 事前にユーザーを本機のアドレス帳に登録してください。 個人単位の認証ができます。
Windows 認証	本機と同一ネットワークに接続される Windows サーバーのドメインコントローラを使って認証します。 個人単位の認証ができます。
LDAP 認証	本機と同一ネットワークに接続される LDAP サーバーを使って認証します。 個人単位の認証ができます。

Windows 認証や 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。

ユーザー認証の方法を途中で切り替えたとき

- 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 認証に切り替えたあとでも、ログインユーザー名として引き継がれ使用できます。このとき、ユーザーコード認証にパスワードはないため、ログインパスワードが空のアカウントとして設定されます。
- 外部の認証（Windows 認証、LDAP 認証）に切り替えたときは、引き継がれたユーザーコードアカウントが外部の認証機器に登録されていないと認証はされず、本機を使用できません。ただし、認証できなくても本機のアドレス帳にはユーザーコードアカウントが残ります。
- ユーザーコード認証からほかの認証方式に切り替えたときは、セキュリティーの観点から、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.34「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。

補足

- 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。
- 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。

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。

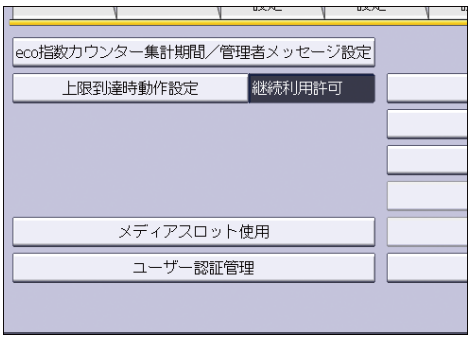
ユーザーコードの設定については、『ネットワークの接続/システム初期設定』「ユーザーコードを登録する」を参照してください。

プリンタードライバー、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。

重要

- **本機に蓄積した文書で、Ridoc Desk Navigator からの配信を制御するときは、ベーシック認証、Windows 認証、LDAP 認証のどれかを使用してください。**

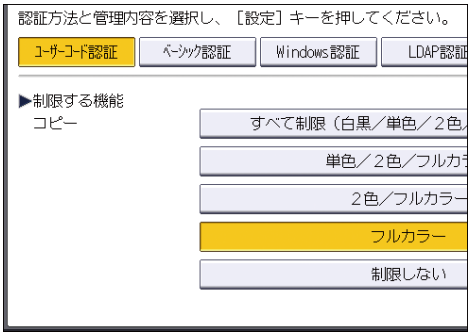
1. 操作部から機器管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [ユーザー認証管理] を押します。



6. [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」で使用を制限する本機の機能を選択します。



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。

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コード認証をしません。

機能の使用制限については、P.72「機能の使用を制限する」を参照してください。

8. プリンタージョブ認証を設定するときは、「制限する機能」の「プリンター」で［自動登録］以外を選択します。

項目が表示されていないときは［▼次へ］を押します。

プリンタージョブ認証を設定しないときは、手順 14 に進みます。

9. [▼次へ] を押します。

10.「プリンタージョブ認証」のレベルを選択します。

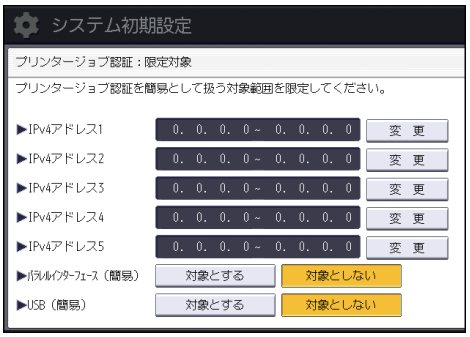
プリンタージョブ認証については、P.52「プリンタージョブ認証」を参照してください。

[簡易]、[すべて] を選択したときは、手順 14 へ進みます。

[簡易（限定）] を選択したときは、手順 11 へ進みます。

11.「限定対象」の［変更］を押します。

12. プリンタージョブ認証を簡易として扱う対象範囲を限定します。



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

13. [閉じる] を押します。
14. [設定] を押します。
15. [ログアウト] を押します。

確認画面が表示されます。

［実行］を押すと自動的にログアウトされます。

ベーシック認証

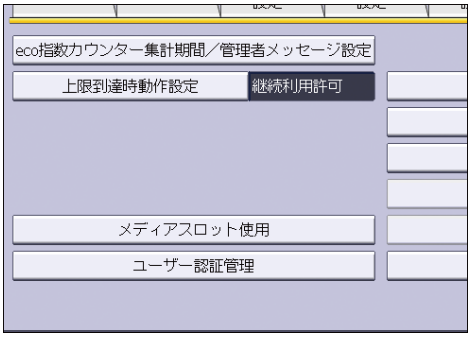
本機のアドレス帳を使用して個人単位の認証をするときに設定します。個人単位で使用できる機能を設定したり、アドレス帳や蓄積文書などのアクセスに制限をかけられます。

ベーシック認証では認証を設定したあとに、管理者がアドレス帳に登録されたユーザーごとに本機の使用制限を設定します。使用制限の設定については、P.34「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。

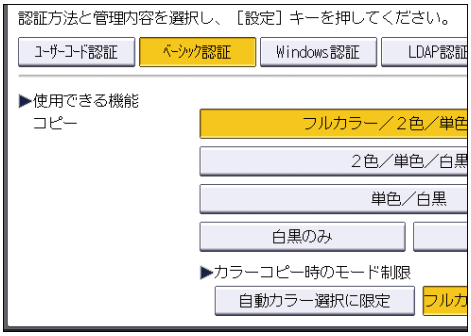
1. **操作部から機器管理者がログインします。**
2. **[システム初期設定]を押します。**
3. **[管理者用設定]を押します。**
4. **[▼次へ]を押します。**
5. **[ユーザー認証管理]を押します。**



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. 「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。



選択したい機能が表示されていないときは、［▼次へ］を押します。

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。

機能の使用制限については、P.72「機能の使用を制限する」を参照してください。

8. ［▼次へ］を押します。

9. 「プリンタージョブ認証」のレベルを選択します。

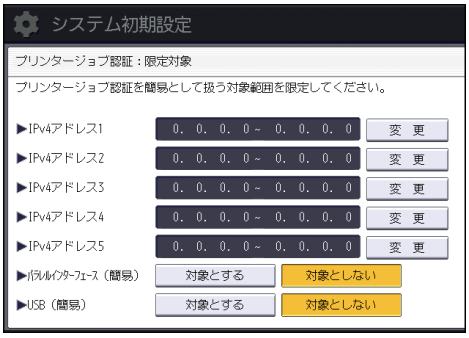
プリンタージョブ認証については、P.52「プリンタージョブ認証」を参照してください。

［簡易］、［すべて］を選択したときは、手順 13 へ進みます。

［簡易（限定）］を選択したときは、手順 10 へ進みます。

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。



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

12. ［閉じる］を押します。

13. ［設定］を押します。

14. ［ログアウト］を押します。

確認画面が表示されます。

［実行］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、本機の使用制限を設定できます。機器の使用制限は、P.32「ベーシック認証」を参照してください。

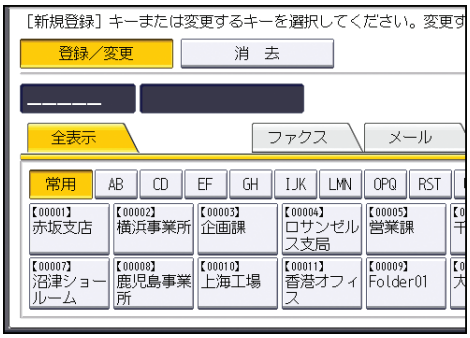
ユーザーが正しく本機を使用できるように、アドレス帳でユーザーごとの設定をします。事前にユーザーをアドレス帳に登録してください。アドレス帳へのユーザーの登録方法は、『ネットワークの接続/システム初期設定』「ユーザー情報を登録する」を参照してください。Web Image Monitor でも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

ログインユーザー名とログインパスワードを設定する

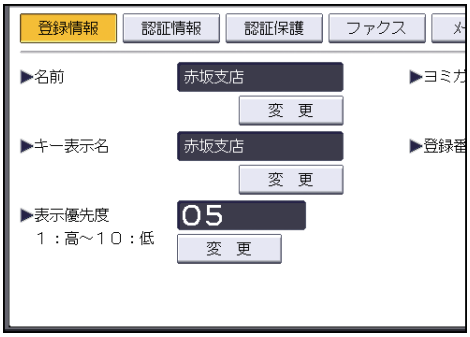
ユーザー認証で使用するログインユーザー名とログインパスワードを設定します。

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.17「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. ［終了］を押します。
3. ［アドレス帳管理］を押します。
4. ユーザーを選択します。



5. [認証情報] 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。
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] を押します。
12. [閉じる] を押します。
13. 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。

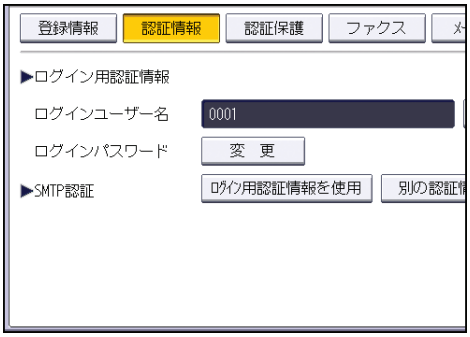
「SMTP 認証」、「フォルダー認証」、「LDAP 認証」で、別のログインユーザー名とログインパスワードを使用するときは、『ネットワークの接続/システム初期設定』「共有フォルダーを登録する」「アドレス帳の認証情報」を参照してください。

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」、「HIDE***」以外の名前を設定します。「***」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. [終了] を押します。
3. [アドレス帳管理] を押します。
4. ユーザーを選択します。
5. [認証情報] を押します。

6. 「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。

7. ［設定］を押します。
8. ［閉じる］を押します。
9. 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られません。Windows 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定できます。ディレクトリサーバーに登録されているアドレス帳を本機に自動で登録できるため、本機でアドレス帳の個人設定を登録しなくてもユーザー認証ができます。

はじめて使用するときは、所属するグループに割り当てられている機能を使用できます。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使用できます。ユーザーごとに機能の制限をするときは事前にアドレス帳で設定してください。

Windows 認証で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。そのときは事前にドメインコントローラのサーバー証明書を作成します。証明書の作成方法は、P.45「サーバー証明書を作成する」を参照してください。

重要

- **Windows 認証を設定しているときは、認証のときに、ディレクトリサーバーに登録されているユーザー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」を選択したときは、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。**
- **Windows サーバーで「Guest」アカウントが有効に設定されているときは、ドメインコントローラに存在しないユーザーでも認証できます。そのとき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使用できます。**

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

NTLM 認証の使用条件

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

- 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 を使用します。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 を使用するときは、TLSv1 または SSLv3 がサーバーで動作することが必要です。
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 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必要です。
- Kerberos 認証を使用するには、KDC（キー配布センター）に対応した OS が必要です。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 を使用します。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 を使用するときは、TLSv1 または SSLv3 がサーバーで動作することが必要です。
  - Windows Server 2003/2003 R2
  - Windows Server 2008/2008 R2
  - Windows Server 2012/2012 R2

  Windows Server 2008 で Kerberos 認証を使用するには、Service Pack 2 以降の導入が必要です。
- 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.159「Kerberos 認証の暗号化設定」を参照してください。

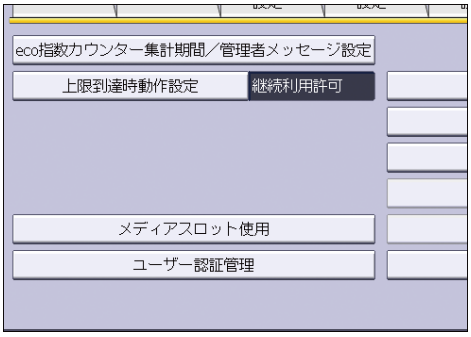
補足

- ログインユーザー名、ログインパスワードに使用できる文字は、P.34「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。
- 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使用できます。
- 2 度目以降に使用するときは、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使用できます。
- Windows 認証でユーザー名などのユーザー情報を SSL/TLS による通信を使用しないで自動登録するとき、または自動登録を使用しないときは、証明書の作成は不要です。
- 認証時にファクス情報取得に失敗するときは、P.45「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。

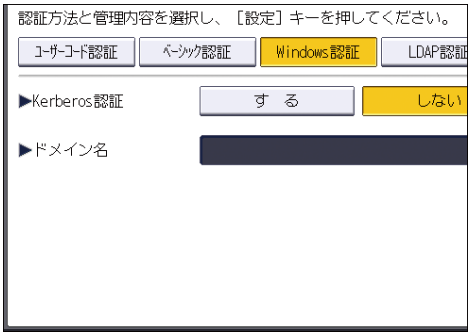
Windows 認証を設定する

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。

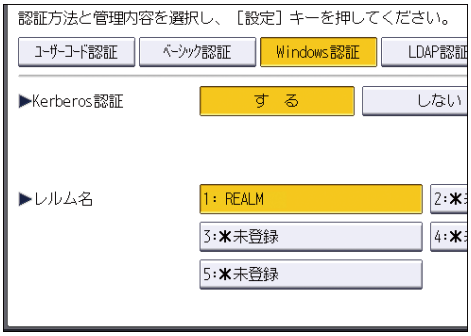


6. [Windows 認証] を選択します。
   ユーザー認証管理を使用しないときは、[認証しない] を選択します。
7. Kerberos 認証を使用するときは「Kerberos 認証」の [する] を押します。



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。



Kerberos 認証を有効にするには、レルムの登録が必要です。

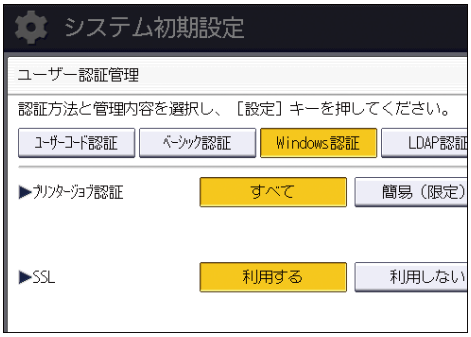
レルム名は半角大文字で登録します。レルムの登録は、『ネットワークの接続/システム初期設定』「レルムを設定する」を参照してください。

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、認証をするドメイン名を入力して［OK］を押します。

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。

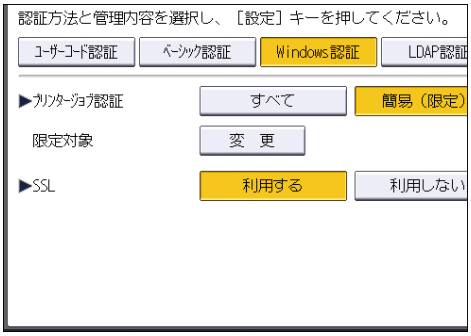


プリンタージョブ認証については、P.52「プリンタージョブ認証」を参照してください。

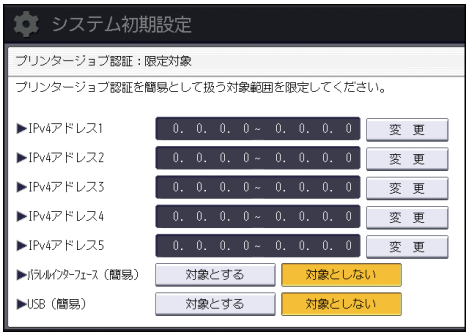
［簡易］、［すべて］を選択したときは、手順 15 へ進みます。

［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。



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

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 を使用しないときは、［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。

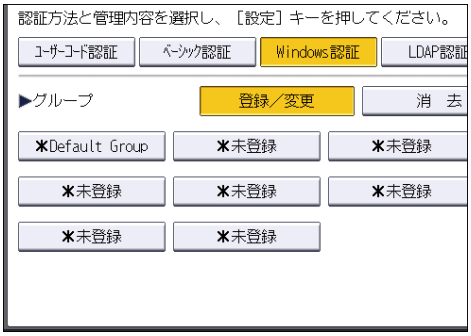
グローバルグループを登録しているときは、手順 16 へ進みます。

Windows サーバーでグローバルグループを登録していれば、グローバルグループごとに機能の使用制限ができます。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きます。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、本機の機能の使用制限を設定します。初めて使用したとき、ユーザーは［＊Default Group］の機能が使用できます。［＊Default Group］は、工場出荷時にすべての機能が使用できるように設定されています。運用に合わせて機能の使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。

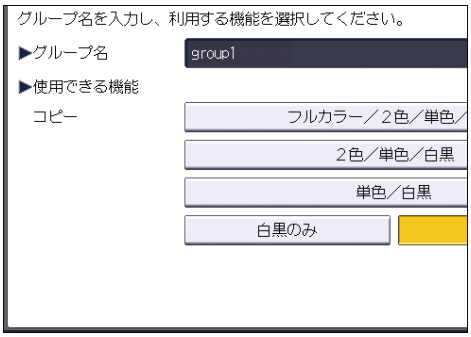


18.「グループ名」の［変更］を押します。

19. サーバー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。



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。

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。

機能の使用制限については、P.72「機能の使用を制限する」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.［ログアウト］を押します。

確認画面が表示されます。

［実行］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 に登録されているユーザー情報を、本機に自動で取得するときに設定します。

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

すでにインストールされているときは、サーバー証明書の作成をしてください。

Windows Server 2008 R2 での設定

1. [スタート] メニューから、[管理ツール] をポイントし、[サーバーマネージャー] をクリックします。
2. 左枠の [役割] をクリックし、[操作] メニューから [役割の追加] をクリックします。
3. [次へ] をクリックします。
4. [Web サーバー(IIS)] と [Active Directory 証明書サービス] のチェックボックスにチェックを付け、[次へ>] をクリックします。

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

17. インストールが完了したというメッセージが表示されたら、[閉じる] をクリックします。
18. サーバーマネージャーを終了します。

Windows Server 2012 での設定

1. [スタート] メニューから、[サーバーマネージャー] をクリックします。
2. [管理] メニューから [役割と機能の追加] をクリックします。
3. [次へ] をクリックします。
4. [役割ベースまたは機能ベースのインストール] を選択し、[次へ] をクリックします。
5. サーバーを選択します。
6. [Active Directory 証明書サービス] と [Web サーバー(IIS)] のチェックボックスにチェックを付け、[次へ] をクリックします。

   確認メッセージが表示されたときは、[機能の追加] をクリックします。
7. インストールする機能にチェックを付け、[次へ] をクリックします。
8. 表示された内容を確認したあと、[次へ] をクリックします。
9. Active Directory 証明書サービスのインストールする役割サービスで、[証明機関] にチェックが付いていることを確認し、[次へ] をクリックします。
10. 表示された内容を確認したあと、[次へ] をクリックします。
11. Web サーバー (IIS) のインストールする役割サービスにチェックを付け、[次へ] をクリックします。
12. [インストール] をクリックします。
13. インストールの終了後、サーバーマネージャーの通知アイコンをクリックし、[対象サーバーに Active Directory 証明書サービスを構成する] をクリックします。
14. [次へ] をクリックします。
15. 役割サービスで [証明機関] にチェックを付けて、[次へ] をクリックします。
16. [エンタープライズ CA] を選択し、[次へ] をクリックします。
17. [ルート CA] を選択し、[次へ] をクリックします。
18. [新しい秘密キーを作成する] を選択し、[次へ] をクリックします。
19. 秘密キーを作成するため、暗号化プロバイダー、キー長、ハッシュアルゴリズムを選択し、[次へ] をクリックします。

20. 「この CA の共通名:」に CA の名前を入力し、［次へ］をクリックします。
21. 証明書の有効期間を選択し、［次へ］をクリックします。
22. 「証明書データベースの場所:」と「証明書データベース ログの場所:」は変更しないで［次へ］をクリックします。
23. ［構成］をクリックします。
24. 構成に成功しましたというメッセージが表示されたら、［閉じる］をクリックします。

サーバー証明書を作成する

「Web サーバー(IIS)」と「Active Directory 証明書サービス」のインストール後に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。

   Windows Server 2012 のときは、［スタート］画面で［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。

   確認メッセージが表示されたら［はい］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入力します。
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. [スタート] メニューから、[すべてのプログラム] をポイントし、[アクセサリ] - [コマンド プロンプト] をクリックします。

   Windows Server 2012 のときは、スタート画面で右クリックし、[すべてのアプリ] - [コマンド プロンプト] をクリックします。

2. 「regsvr32 schmmgmt.dll」を入力し [Enter] キーを押します。
3. [OK] をクリックし、コマンドプロンプトを閉じます。
4. [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。

   Windows Server 2012 のときは、スタート画面で右クリックし、[すべてのアプリ] - [ファイル名を指定して実行] をクリックします。

5. 「mmc」を入力し、[OK] をクリックします。
6. [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。
7. [Active Directory スキーマ] を選択し、[追加>] をクリックします。
8. [OK] をクリックします。
9. 左枠の [Active Directory スキーマ] をクリックし、[属性] フォルダーを開きます。
10. [facsimileTelephoneNumber] を右クリックし、[プロパティ] をクリックします。
11. [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。
12. [OK] をクリックします。
13. [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。
14. 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。
15. 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られません。LDAP サーバーに登録されているアドレス帳を本機に自動で登録できるため、本機でアドレス帳の個人設定登録をしなくてもユーザー認証ができます。

LDAP 認証時にユーザー名、パスワードがネットワークに平文で流れるのを防止するために、本機と LDAP サーバー間で SSL による暗号化された通信をすることをお勧めします。そのときは事前に LDAP サーバーのサーバー証明書の作成が必要です。証明書の作成方法は、P.45「サーバー証明書を作成する」を参照してください。SSL の使用設定方法は、『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。

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

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

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

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ることがあるので注意してください。**
- **LDAP 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定できません。**
- **Active Directory を使用して LDAP 認証をするときは、LDAP の認証種別で Kerberos 認証を選択し、同時に SSL を設定するとメールアドレスは取得できません。**
- **LDAP 認証を使用する場合に、LDAP サーバーの設定で匿名認証を禁止にしていないときは、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 で構成されている場合は、匿名認証が許可されることがあります。このような環境で使用するときは Windows 認証の使用をお勧めします。**

LDAP 認証の使用条件

LDAP 認証を設定するときは、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
- 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。

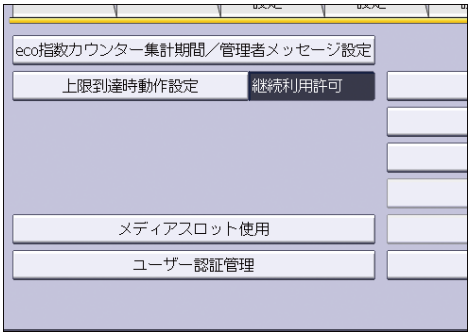
補足

- 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.17「ユーザー名、パスワードに使用できる文字」を参照してください。
- LDAP 簡易認証時に空パスワードでログインすると、認証に失敗します。空パスワードを許可するときは、サービス実施店にお問い合わせください。
- 設定後に未登録のユーザーが初めて本機を使用したときは、本機にユーザーが新規登録され、LDAP 認証設定時に「使用できる機能」で設定した機能が使用できます。ユーザーごとに使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 度目以降の使用時には、ユーザーごとの「使用できる機能」の設定は維持されます。
- Kerberos 認証では、本機と KDC サーバーの間で暗号化通信をします。暗号化通信の設定は、P.159「Kerberos 認証の暗号化設定」を参照してください。

管理者認証が設定されていることを確認してから設定してください。

1. **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。**

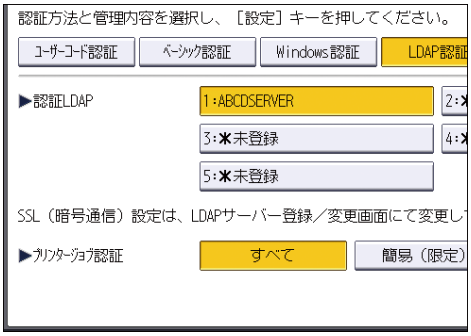
5. [ユーザー認証管理] を押します。



6. [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。



8. 「プリンタージョブ認証」のレベルを選択します。

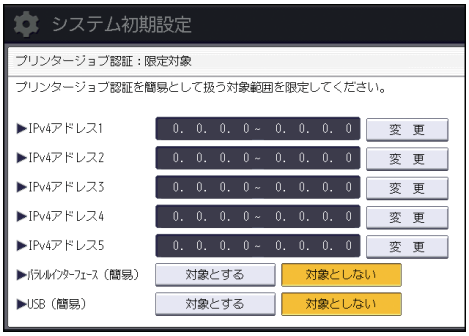
プリンタージョブ認証については、P.52「プリンタージョブ認証」を参照してください。

[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。

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。

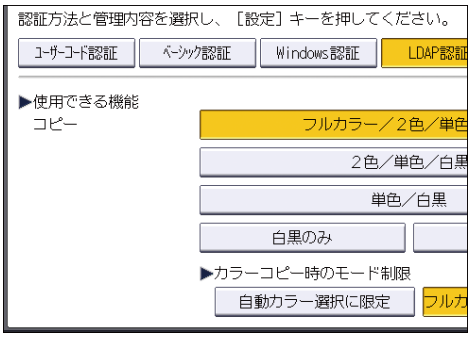


IPv4 アドレスの範囲と、パラレル接続、USB 接続を対象とするかを設定できます。

11. **[閉じる] を押します。**

12. **[▼次へ] を押します。**

13. **「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。**



選択したい機能が表示されていないときは、[▼次へ] を押します。

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

機能の使用制限については、P.72「機能の使用を制限する」を参照してください。

14. **[▼次へ] を押します。**

15. **「ログイン名属性」の［変更］を押します。**

16. **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使用します。ログイン名属性で検索フィルターを作成して、ユーザーを特定してそのユーザーの情報を LDAP サーバーから本機のアドレス帳へ取得します。

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

DN 形式で認証するときは、ログイン名属性を登録する必要はありません。

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

17. **「一意属性」の［変更］を押します。**

18. **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 でも指定できます。

19. [設定] を押します。

20. [ログアウト] を押します。

確認画面が表示されます。

[実行] 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、PCL、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

セキュリティー強度は「すべて」が最も高く、続いて「簡易（限定）」、「簡易」の順です。

［すべて］

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

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

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

［簡易（限定）］

範囲を限定して［簡易］のプリンタージョブ認証をするときに選択します。

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

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

［簡易］

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

ユーザー認証に対応していないプリンタードライバーからのジョブや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と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用されることがあるので注意してください。

プリンタージョブの種類

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

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

プリンタージョブの種類

1. 本機用の RPCS、RP-GL/2、PCL 6 プリンタードライバーの設定で、「ユーザー認証」をチェックしたとき
2. 機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックし、さらに「暗号化する」をチェックしたとき
3. 機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックしたとき
4. 本機用の RPCS、RP-GL/2、PCL 6 プリンタードライバーまたは、機種共通のプリンタードライバーの設定で、「ユーザー認証」をチェックしないとき
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ときも同様です。
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ときも同様です。
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、PictBridge 印刷のとき、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。
9. Ridoc Desk Navigator から RTIFF ダイレクトプリントで印刷する場合に、認証をしないとき
10. Ridoc Desk Navigator から RTIFF ダイレクトプリントで印刷する場合に、認証をするときです。認証にはユーザー名・パスワード・暗号鍵の 3 つが必須です。

組み合わせ一覧

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

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

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

×：ユーザー認証に関係なく印刷できません。ジョブがリセットされます。

補足

- 「ドライバー暗号鍵：暗号強度設定」については、P.239「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

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

telnet にログインするときのログインユーザー名とログインパスワードは管理者へ問い合わせてください。telnet のログイン方法、操作方法は、『ネットワークの接続/システム初期設定』「telnet を使用する」を参照してください。

現在の設定の表示

msh> authfree

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

IPv4 アドレスの設定

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

IPv6 アドレスのレンジでの設定

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

IPv6 アドレスのマスクでの設定

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

パラレル/USB の設定

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

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

補足

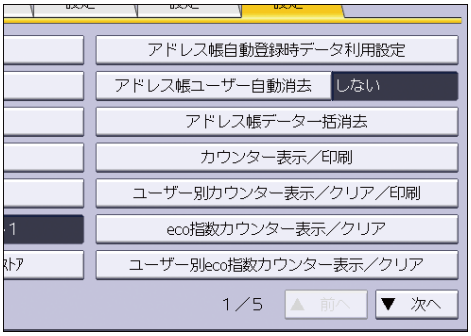
- 自動登録の場合に、アドレス帳の登録件数が上限に達しているときは、古いユーザーを自動で消去できます。詳細は P.238「アドレス帳を管理する」を参照してください。

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. [ログアウト] を押します。

   確認画面が表示されます。

   [実行] 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ると、ロックアウト機能が働き、そのログインユーザー名でのログインが禁止されます。ロックアウトされたユーザーは、正しいパスワードを入力したときも認証失敗となり、一定時間が経過してロックアウトが解除されるか、管理者またはスーパーバイザーがロックアウト機能を解除するまで、機器を使用できません。

ユーザー認証でロックアウト機能を使用するには、認証方法をベーシック認証にします。ほかの認証選択時では、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

ロックアウト機能は Web Image Monitor で設定します。

設定項目	設定内容	設定値	工場出荷時の設定値
ロックアウト	ロックアウト機能を有効にするかしないかを設定します。	• 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。	• 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

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. 「セキュリティー」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、一定時間で解除するときは「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. [詳細入力] 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」で [無効] を選択します。
6. [OK] をクリックします。
7. ログアウトします。

補足

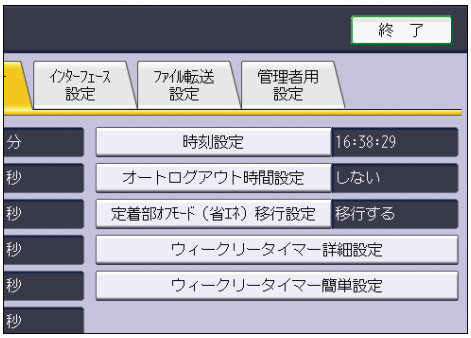
- 管理者とスーパーバイザーのパスワードロックアウトは、主電源を一度切ってから再び入れるか、Web Image Monitor の [設定] の [管理者登録/変更] で解除できます。

オートログアウト時間設定

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

オートログアウト機能が働くまでの時間を設定します。

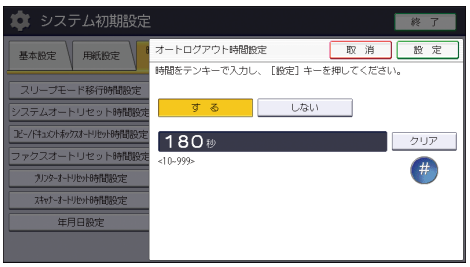
1. 操作部から機器管理者がログインします。
2. [システム初期設定]を押します。
3. [時刻タイマー設定]を押します。
4. [オートログアウト時間設定]を押します。



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. 「10～999」(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. [設定]を押します。
8. [ログアウト]を押します。

   確認画面が表示されます。

   ［実行］を押すと自動的にログアウトされます。

補足

- Web Image Monitor 画面のオートログアウト時間設定は、［Webpage 設定］からできます。詳しくは Web Image Monitor のヘルプを参照してください。

かんたんカード認証

かんたんカード認証機能を使用してユーザー認証をするときに設定します。

本機のアドレス帳に登録されたユーザーに IC カードを登録することで、認証画面で IC カードをかざすだけでログインできます。

IC カードの代わりに、RICOH カンタン入出力をインストールしたスマートデバイスを使用することもできます。

重要

- **かんたんカード認証では、管理者はカード操作でログインできません。管理者としてログインするときは、［キーボード入力でログイン］を押して、ログインユーザー名とパスワードを入力してログインしてください。**

かんたんカード認証を設定する

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. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。
   「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. 画面中央下の［ホーム］（🏠）を押します。
4. ［⌨］を押します。
5. ［かんたんカード認証設定］アイコンを押します。
6. ［認証機能を使用する］を押します。
7. 画面の指示に従い本機の主電源を切り、再度、主電源を入れます。

IC カードリーダー設定を変更する

IC カードリーダーの設定を変更することができます。

1. 操作部から機器管理者がログインします。
2. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。
   「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. ［操作部初期設定］を押します。
4. ［操作部機器設定］を押します。
5. ［IC カード/Bluetooth 用ソフトウェア設定］を押します。

6. 必要な設定をします。
7. ログアウトします。
8. 設定を変更した場合は本機の主電源を切り、再度、主電源を入れます。

設定項目

項目名	説明
[IC カードリーダー選択]	使用する IC カードリーダーの種類を選択します。
[USB カードリーダー設定]	「IC カードリーダー選択」で「USB カードリーダー」が選択されているときに選択できます。 USB カードリーダーの設定を変更できます。 USB カードリーダーごとに、認証機能に使用するかどうか設定できます。
[NFC カードリーダー設定]	「IC カードリーダー選択」で「NFC カードリーダー」が選択されているときに選択できます。 NFC カードリーダーの設定を変更できます。 IC カード種別ごとに、認証機能に使用するかどうか設定できます。 設定画面で IC カードをかざすと対応する IC カード種別にマークがつきます。
[Bluetooth 設定]	認証で Bluetooth を使用するかどうかを設定できます。 [Bluetooth 設定] を有効にすると、IC カードの代わりに RICOH カンタン入出力をインストールしたスマートデバイスを使用できます。

補足

- 「USB カードリーダー設定」、「NFC カードリーダー設定」、「Bluetooth 設定」は「かんたんカード認証設定」画面からも開けます。

アドレス帳登録ユーザーに IC カードまたはスマートデバイスを登録する

本機のアドレス帳に登録されたユーザーに、IC カードまたはスマートデバイスを登録します。

重要

- **IC カードをかざすときは、ラベルの表示と同じ向きにかざしてください。**
- **IC カードまたはスマートデバイスは 1 回の操作で 1 つだけかざしてください。**

1. **かんたんカード認証の認証画面で、未登録の IC カードまたはスマートデバイスをかざします。**

   IC カードのときは、カードリーダーの位置を示すラベルにかざします。ラベルは操作部の右奥に貼られています。

スマートデバイスのときは操作部にかざします。

2. **IC カードまたはスマートデバイスを登録したいユーザーのログインユーザー名とパスワードを入力し、［登録］を押します。**

   ユーザーに IC カードまたはスマートデバイスが登録されます。

3. **［確認］を押します。**

補足

- すでに IC カードまたはスマートデバイスが登録されているユーザーに別の IC カードまたはスマートデバイスを登録すると、先に登録されていた IC カードまたはスマートデバイスは未登録の状態になります。

優先ユーザーを設定する

IC カードまたはスマートデバイスを登録したユーザーの中で、特定のユーザーを優先ユーザーとして設定することができます。優先ユーザーとして設定したユーザーは、かんたんカード認証のログイン処理がほかのユーザーよりも早くなります。

優先ユーザーは 100 件まで設定できます。

1. **操作部からユーザー管理者と機器管理者の権限を持つ管理者がログインします。**
2. **画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。**

   「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. **画面中央下の［ホーム］（🏠）を押します。**
4. **［⌨］を押します。**
5. **［かんたんカード認証設定］アイコンを押します。**
6. **［優先ユーザー設定］を押します。**
7. **優先ユーザーとして設定したいユーザーを選択し、［OK］を押します。**

   選択したユーザーが優先ユーザーとして設定されます。
8. **ログアウトします。**

補足

- IC カードまたはスマートデバイスが登録されていないユーザーでも、優先ユーザーを設定できます。

外部機器を使用した認証

ベーシック認証、Windows 認証、LDAP 認証のどれかが設定され、拡張認証管理が［する］に設定されているときに、リコー IC カードや FeliCa を使用して認証できます。FeliCa を使用するときはパスワードを設定できないため、ベーシック認証を選択します。

この機能を使用するために必要なオプションについては、『本機をお使いになる方へ』「オプションが必要な機能一覧」を参照してください。

IC カード R/W によるログイン、ログアウトの方法は、IC カード R/W の使用説明書を参照してください。

重要

- **リコー IC カードや FeliCa を使用してユーザー認証をするときは、事前にアドレス帳にログインユーザー名の登録が必要です。アドレス帳へのユーザー登録方法は、『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。**
- **外部認証機器で認証するには、機器管理者カードの登録が必要です。詳しい登録の方法は IC カード R/W の使用説明書を参照してください。**
- **機器管理者用の認証カードはなくさないようにしてください。万一のときは、工場出荷時の値に戻すことになり、本機のデータが失われることがあります。**

IC カード認証システムを使用する

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. ［拡張認証管理］を押します。
6. ［する］を選択します。
7. ［詳細設定］を押します。
8. 「IC カード認証種別」で［リコー IC カード］または［FeliCa(IDm)］を選択します。
9. 「認証方法の併用」を設定します。

   認証カードと直接入力を併用して認証するときは、［する］を選択し、手順 11 へ進みます。

   認証カードだけで認証するときは、［しない］を選択し、手順 10 へ進みます。

10. IC カード R/W に、機器管理者用の認証カードをセットします。

    IC カード R/W への認証カードセット方法は、IC カード R/W の使用説明書を参照してください。

    認証失敗のメッセージが表示されたときは、機器管理者用の IC カードが認証されていません。USB ケーブルが接続されていることを確認し、正しい機器管理者用の IC カードをセットしてください。

    IC カードに暗証番号を設定していると、暗証番号の入力画面が表示されます。IC カードに設定されている暗証番号を入力してください。

    IC カード認証種別を変更したときは、「認証方法の併用」の設定が自動的に［する］に変更されます。

11. ［閉じる］を押します。
12. ［設定］を押します。
13. ログアウトします。

FeliCa を使用して管理者を登録する

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. ［管理者登録／変更］を押します。
6. 権限を設定する管理者を選択し、［変更］を押します。
7. ［FeliCa ID 取得］を押します。
8. IC カード R/W に FeliCa をセットします。

   カードのセット方法は IC カード R/W の使用説明書を参照してください。
9. ［設定］を 2 回押します。
10. ログアウトします。

3. 機器の使用を制限する

ユーザーによる本機の使用を制限する方法を説明します。

宛先表の使用を制限する

ファクス機能と、スキャナー機能それぞれで宛先表の使用を制限できます。

宛先利用制限（ファクス）、宛先利用制限（スキャナー）

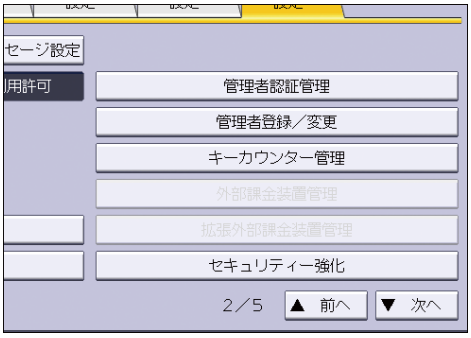
ファクスまたはスキャナーの送信先を、アドレス帳に登録された宛先だけに限定します。

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）

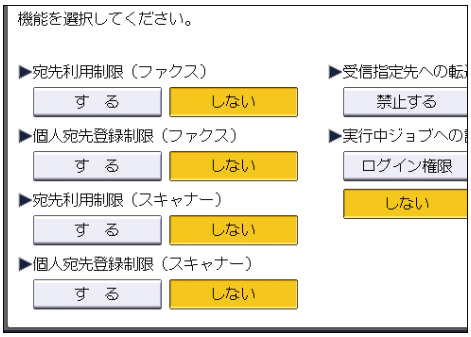
ファクスまたはスキャナーの送信時に直接入力した宛先を［宛先登録］でアドレス帳に登録することを禁止します。また、ユーザー管理者以外は、アドレス帳へのユーザーの新規登録や、登録済みユーザーのパスワードなどのユーザー情報の変更ができなくなります。個人宛先登録制限が設定されているときでも、宛先に登録されているユーザーは、パスワードを変更できます。パスワード以外の項目は、ユーザー管理者だけが変更できます。

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. ［セキュリティー強化］を押します。



6. ［▼次へ］を押します。
7. 宛先利用制限、または個人宛先登録制限で［する］を選択します。

ファクスとスキャナーそれぞれで選択します。



「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. ［ログアウト］を押します。

確認画面が表示されます。

［実行］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

管理者による設定の変更を制限する

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。

本機では以下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.277「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.15「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.13「管理者認証を設定する」を参照してください。

メニュープロテクトを設定する

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

メニュープロテクトを設定するには、事前に機器管理者の管理者認証を有効にします。管理者認証の設定方法は、P.13「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.277「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。無効にするときは、[しない]を選択します。

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. [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。

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. [データ操作/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。

プログラムの登録／変更を禁止する

メニュープロテクトを有効にすると、ユーザーによるプログラムの登録／変更を禁止できます。プログラムの登録や変更は機器管理者が行います。

プログラムの登録/変更については、『本機をお使いになる方へ』「よく使用する設定を登録する」、『エミュレーション』「プログラムを登録する」を参照してください。

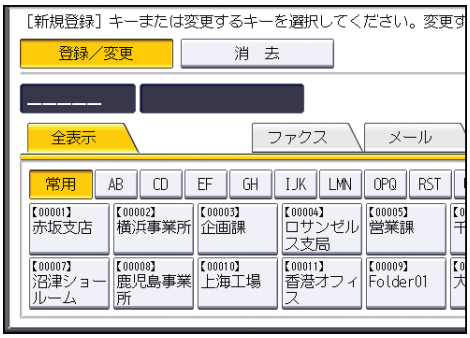
機能の使用を制限する

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

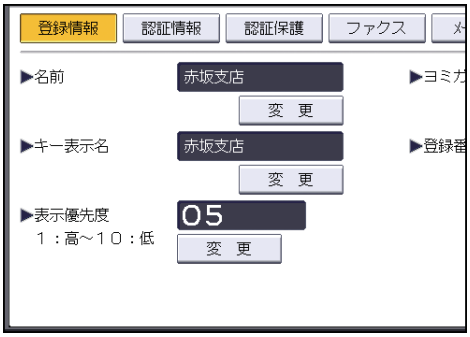
アドレス帳に登録されたユーザーに、そのユーザーがログインしたときに使用できる機能を設定します。この設定により、ユーザーが使用できる機能を制限できます。

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、拡張機能の各機能で使用を制限できます。

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

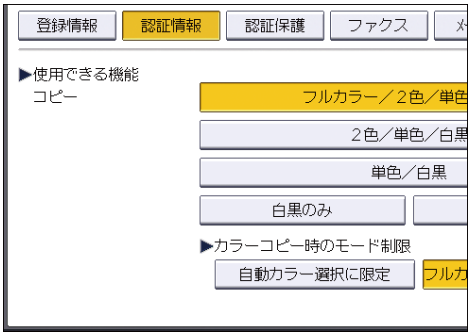


5. [認証情報] を押します。



6. [▼次へ] を 2 回押します。

7. 「使用できる機能」で設定する機能を選択します。



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。

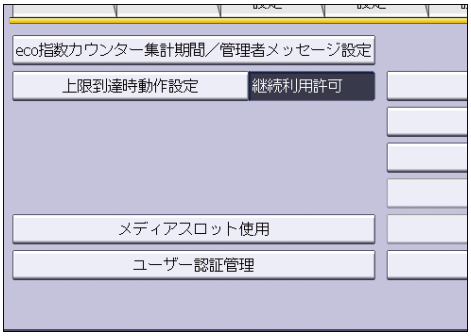
8. ［設定］を押します。

9. 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）への保存と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。

集中管理をしているときは、印刷利用量を集中管理するかどうか設定できます。集中管理設定については、『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。

印刷利用量

印刷利用量は「印刷ページ数 × 度数」という計算方法でカウントされます。

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

印刷利用量は、ユーザーごとにカウントされます。

設定項目

項目名	説明	設定値
上限到達時動作設定	利用量制限をするかしないかと、制限の方法を選択します。 • ジョブ中断 上限に達すると、実行中のジョブと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。 集中管理をしていて、集中管理サーバー機で「印刷利用量制限」が「集中管理する」に設定されているときは、集中管理サーバー機での設定が集中管理クライアント機に適用されます。	• 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**）

項目名	説明	設定値
印刷利用量制限度数設定	以下の 8 つの条件それぞれに限度値を設定できます。 • ｺﾋﾟｰ：ﾌﾙｶﾗｰ：A 3/D L T • ｺﾋﾟｰ：ﾌﾙｶﾗｰ：その他 • ｺﾋﾟｰ：ﾓﾉｶﾗｰ：A 3/D L T • ｺﾋﾟｰ：ﾓﾉｶﾗｰ：その他 • ﾌﾟﾘﾝﾀｰ：ﾌﾙｶﾗｰ：A 3/D L T • ﾌﾟﾘﾝﾀｰ：ﾌﾙｶﾗｰ：その他 • ﾌﾟﾘﾝﾀｰ：ﾓﾉｶﾗｰ：A 3/D L T • ﾌﾟﾘﾝﾀｰ：ﾓﾉｶﾗｰ：その他 集中管理をしているときでも、印刷する機器の設定が適用されます。	0～200 （工場出荷時の度数は 1）

利用量制限を設定したときの注意事項

以下の操作をしたときは、印刷ができません。

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

以下の条件のときは、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ユーザー名でログインし、別々のユーザーとしてアドレス帳に登録されたとき

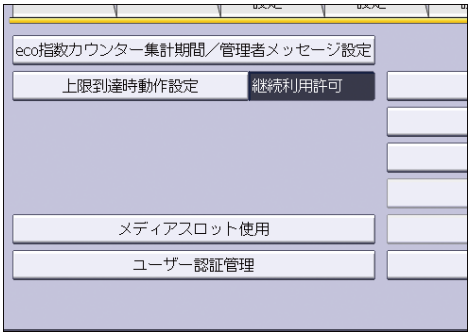
以下の条件のときは、利用量制限の対象外です。

- 使用中の認証方式に対応していない OS からの印刷
- 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、PC FAX データの印刷

利用量制限を設定する

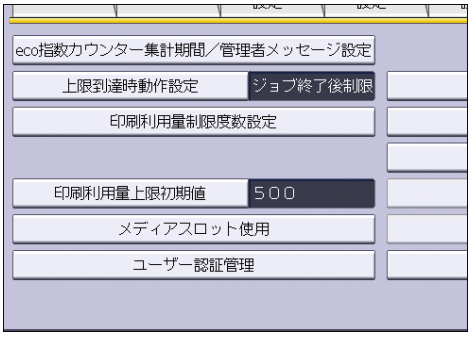
1. **操作部から機器管理者がログインします。**
2. **[システム初期設定] を押します。**
3. **[管理者用設定] を押します。**
4. **[▼次へ] を押します。**

5. [上限到達時動作設定] を押します。

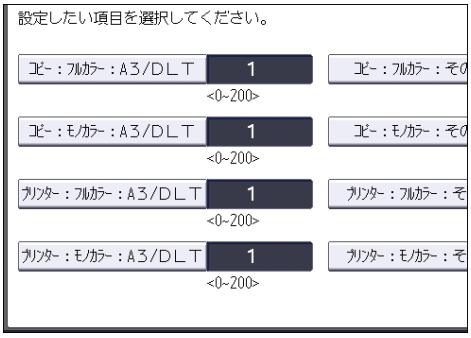


6. [ジョブ中断] または [ジョブ終了後制限] を選択し、[設定] を押します。
利用量の制限をしないときは、[継続利用許可] を選択してください。

7. [印刷利用量制限度数設定] を押します。



8. 印刷条件を選択し、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、利用量は制限されません。



9. [設定] を押します。

10. 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

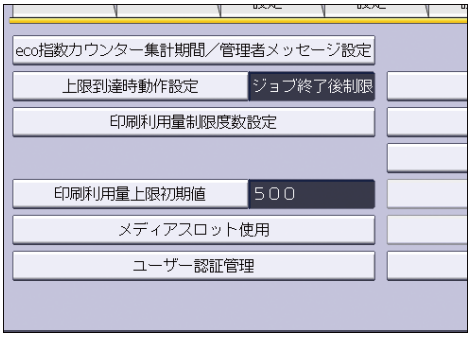
ユーザーコード認証有効時に、利用量制限を設定したときは、以下の制限事項があります。

- 「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ときは、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、画面右上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できます。［ユーザー認証管理］の［ユーザーコード認証］の「制限する機能」ですべての機能を制限してください。

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。

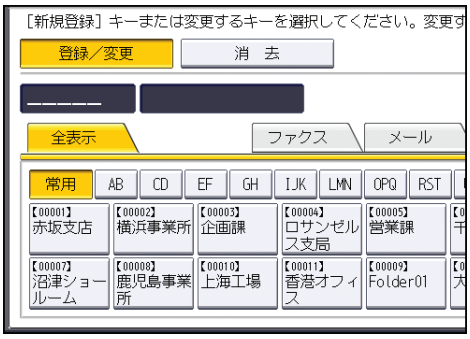


「上限到達時動作設定」で［継続利用許可］が選択されているときは、［印刷利用量上限初期値］は選択できません。

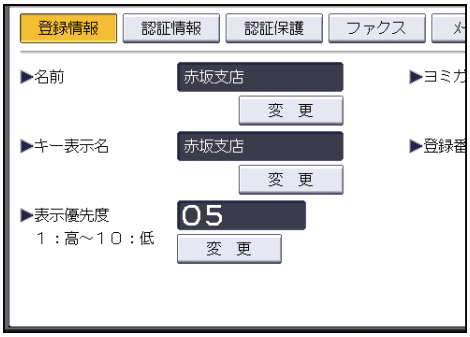
6. テンキーを使って「0～999,999」の範囲で度数を入力し、［#］を押します。
7. ［設定］を押します。
8. ログアウトします。

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. ［終了］を押します。
3. ［アドレス帳管理］を押します。
4. 利用量を設定するユーザーを選択します。



5. ［認証情報］を押します。



6. ［▼次へ］を 4 回押します。
7. 「印刷利用量制限」の［制限する］を選択し、［変更］を押します。

「印刷利用量制限」は、「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。

8. 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。
   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。
9. [設定]を押します。
10. ログアウトします。

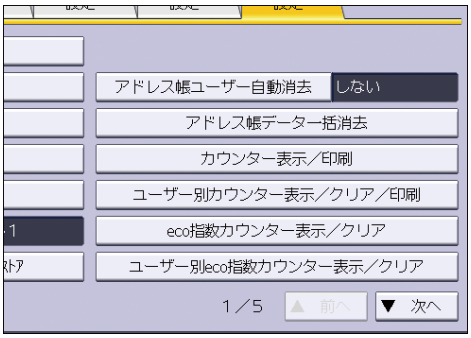
補足

- 利用量の制限は、Web Image Monitor の［アドレス帳］でも設定できます。

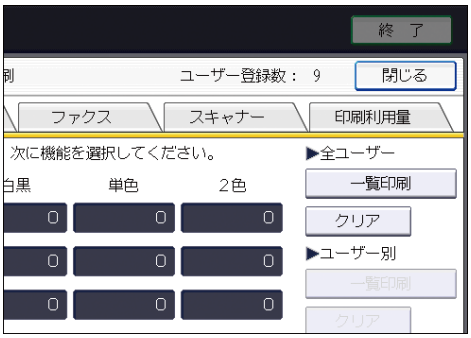
ユーザーの利用量を確認する

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。



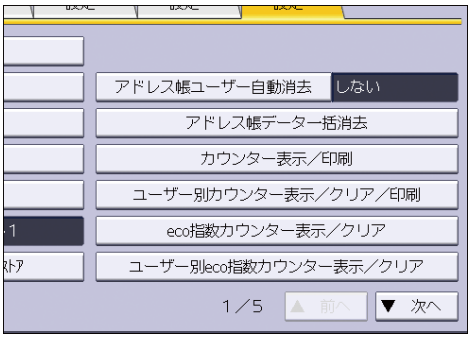
   ユーザーごとの利用上限度数と、利用済みの度数が表示されます。
6. 確認が終了したらログアウトします。

補足

- ユーザー管理者と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。

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。

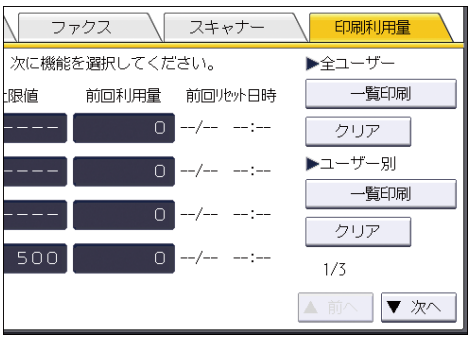


5. ［印刷利用量］を押します。

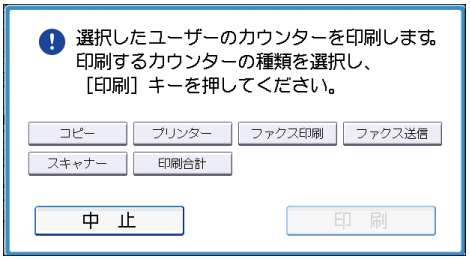
   ユーザーごとのカウンターが表示されます。

   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。



8. ログアウトします。

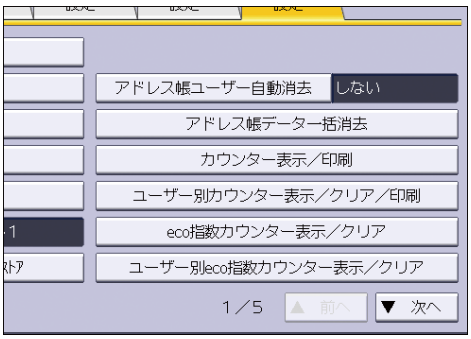
補足

- 利用量カウンターを印刷するときは、A4□□、$8^1/_2$×11□□、B4□、$8^1/_2$×14□、A3□、11×17□、$8^1/_2$×$13^2/_5$□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ときは、該当するユーザーのカウンターをクリアするか、上限度数の設定値を上げると、印刷を再開できます。

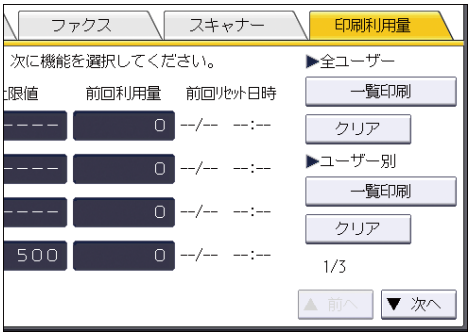
1. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [ユーザー別カウンター表示／クリア／印刷] を押します。



5. [印刷利用量] を押します。

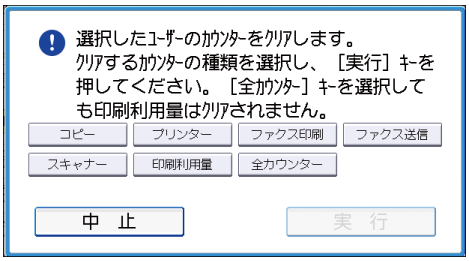
   ユーザーごとのカウンターが表示されます。

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ときは、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。

集中管理をしていて、集中管理サーバー機で「印刷利用量制限」が「集中管理する」に設定されているときは、集中管理サーバー機での設定が集中管理サーバー機と集中管理クライアント機に適用されます。

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

選択項目	詳細
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。
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. [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

- 指定した日時に本機の主電源が入っていないときは、主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。

4. 機器情報の漏えいを防止する

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。

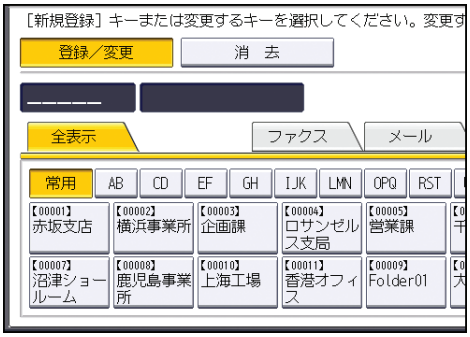
アドレス帳の登録情報を保護する

アドレス帳のデータに、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たりして、個人情報の漏えいを防止できます。

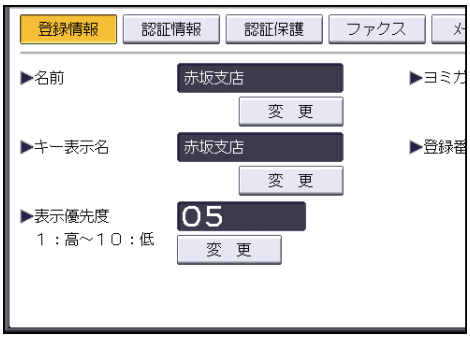
アドレス帳にアクセス権を設定する

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、ユーザー管理者が設定します。

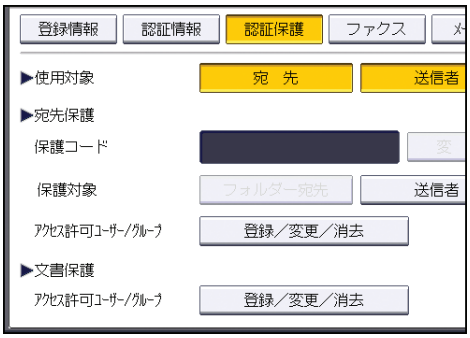
1. 操作部からユーザー管理者がログインします。
2. [終了] を押します。
3. [アドレス帳管理] を押します。
4. アクセス権を変更するユーザーを選択します。



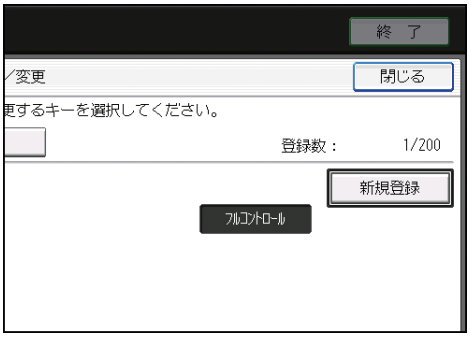
5. [認証保護] を押します。



6. 「宛先保護」にある「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。



7. ［新規登録］を押します。



8. アクセス権を与え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。

9. ［閉じる］を押します。

10. 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。

11. ［閉じる］を押します。

12. ［設定］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。

アドレス帳を暗号化する

重要

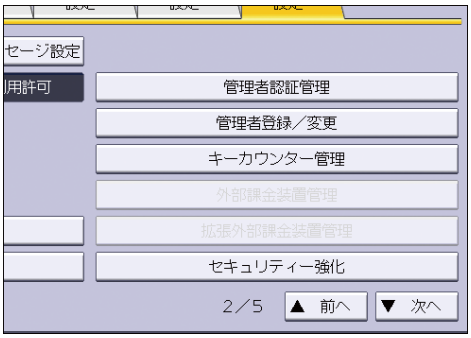
- **アドレス帳暗号化の処理中は、本機を使用できません。**
- **次の機能を利用するときは、アドレス帳が暗号化されていると処理に時間がかかったり、失敗したりすることがあります。アドレス帳データの読み取り防止には、機器データ暗号化機能を利用してください。**
  - **ユーティリティーを使用したアドレス帳インポート／エクスポート**
  - **個人認証システム AE-2 を使用した認証**

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。

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異なります。

アドレス帳の暗号化処理の実行は、時間がかかることがあります。

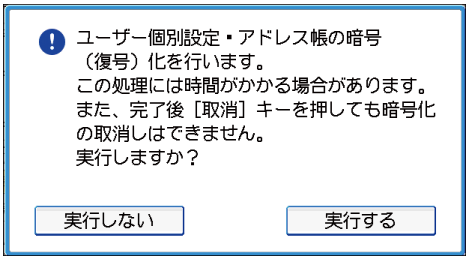
1. 操作部からユーザー管理者がログインします。
2. [システム初期設定] を押します。
3. [管理者用設定] を押します。
4. [▼次へ] を押します。
5. [セキュリティー強化] を押します。



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。

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、USB メモリーは、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、USB メモリー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。

本機に保存されるアドレス帳、認証情報、蓄積文書などのデータを暗号化して、本体搭載メモリーやハードディスクが物理的に取り出されたときの情報の漏えいを防止します。

暗号化を有効にすると、それ以降に本機に保存されるデータはすべて暗号化されます。

また既存のデータは暗号化して残すか、消去するかを選択できます。

暗号化のアルゴリズムは AES-256 です。

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（NVRAM）と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。

本体搭載メモリー（NVRAM）

- 機器設定情報
- ネットワーク I/F 情報
- ユーザーコード
- カウンター情報

ハードディスク

- アドレス帳
- Embedded Software Architecture アプリケーションプログラム/ログ
- ジョブログ/アクセスログ/eco ログ
- 送受信メール
- 登録したフォント
- スプールされたジョブ
- 蓄積した文書のサムネール画像
- 蓄積文書
- 登録したスタンプ
- 登録したフォーム

暗号化設定の種類

ハードディスク内の既存のデータを暗号化して残すか、消去（初期化）するかを選択します。残すデータが多いと暗号化設定の完了に時間がかかります。

NVRAM のデータは消去（初期化）されません。

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]	• Embedded Software Architecture アプリケーションプログラム/ログ • 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ール画像 • 送受信メール • 文書管理サーバーに転送された文書 • Mail to Print で受信したファイル • スプールされたジョブ	• 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）	2 時間 15 分
[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	5 時間 30 分
[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ときの注意事項

- Embedded Software Architecture アプリケーション、あるいは App2Me を使用するときは、必ず［ファイルシステムデータのみ］または［全データ］を選択してください。
- [全データ初期化]、[ファイルシステムデータのみ]、[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。

データの復元

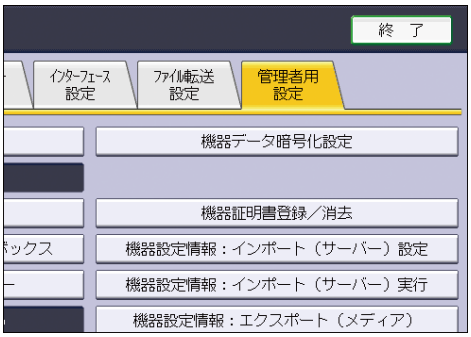
- 機器の入れ替え時などに既存のデータを引き継ぐときは、暗号化されたデータの復元が必要です。データの引き継ぎはサービス実施店に依頼してください。
- データの復元には、暗号化設定時に生成される暗号鍵を使用します。
- 暗号鍵は紙に印刷するか、SD カードに保存するかを選択できます。
- 暗号鍵はあとから変更できます。

暗号化設定を有効にする

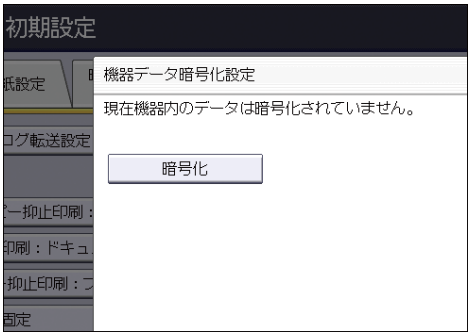
重要

- 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。実行中に主電源が切られるとハードディスクが破損しすべてのデータが使用できなくなります。
- 暗号鍵は、障害時のデータリカバリーなどに必要です。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号化の設定は、操作部での設定手順を完了し、主電源を一度切ってから再び入れて本機が再起動されたあとに有効になります。メモリー全消去機能と暗号化機能を同時に設定していると、メモリー全消去機能が実行されたあと、主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。
- メモリー全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のと合わせて、メモリー全消去で乱数方式の 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 9 時間 30 分かかります。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主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。

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。

   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は [全データ初期化] を選択します。

8. 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] を押して機器データ暗号鍵のバックアップをします。

   SD カードの取り扱いと装着方法は、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。

   [紙に印刷] を選択したときは、[スタート] 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。

    主電源の入れかた、切りかたは、『本機をお使いになる方へ』「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だけをします。暗号化の設定は変更しません。

重要

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

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. [機器データ暗号鍵バックアップ] を押します。
7. 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] を押して機器データ暗号鍵のバックアップ後に、[確認] を押します。

   SD カードの取り扱いと装着方法は、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。

   [紙に印刷] を選択したときは、[スタート] 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

暗号鍵を新しくします。新しい暗号鍵で暗号化をやり直すので、暗号化を開始するときと同じ時間がかかります。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実施できます。

重要

- **暗号鍵の更新中は本機の操作はできません。**
- **暗号鍵は、障害時のデータリカバリーなどに必要です。出力されるバックアップ用データ暗号鍵は大切に保管してください。**
- **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、主電源を一度切ってから再び入れて本機が再起動したあとに有効になります。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。**
- **暗号鍵の更新を一度実行すると、途中で中止できません。また、暗号鍵の更新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。実行中に主電源が切られるとハードディスクが破損しすべてのデータが使用できなくなります。**

- **暗号鍵の更新が正常に終了しなかったときは、生成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。**
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. **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。

   SDカードの取り扱いと装着方法は、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。

   [紙に印刷]を選択したときは、[スタート]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。

    主電源の入れかた、切りかたは、『本機をお使いになる方へ』「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。暗号化を開始するときと同じ時間がかかります。

重要

- 暗号化の解除中は本機の操作はできません。
- 暗号化の解除は、操作部での設定手順を完了し、主電源を一度切ってから再び入れて本機が再起動したあとに有効になります。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。
- 暗号化の解除を一度実行すると、途中で中止できません。また、暗号化の解除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。実行中に主電源が切られるとハードディスクが破損しすべてのデータが使用できなくなります。
- 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.96「機器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。

    主電源の入れかた、切りかたは、『本機をお使いになる方へ』「電源の入れかた、切りかた」を参照してください。

機器のデータを上書き消去する

本機に保存されたデータを上書き消去することで、データの漏えいを防止します。

上書き消去には以下の 2 つがあります。

メモリー自動消去

コピーやプリントをするときに本機のハードディスクに一時的に保存されるデータを自動で消去します。詳細は P.96「メモリー自動消去」を参照してください。

メモリー全消去

本機のハードディスクに保存されているすべてのデータを一括で上書き消去します。本体搭載メモリーに保存されている機器の設定は初期化します。本機を移設や廃棄するときなど、すべてのデータと設定を消去するときに実施します。詳細は P.100「メモリー全消去」を参照してください。

メモリー自動消去

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。メモリー自動消去を使用すると、これらの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てから開始します。

メモリー自動消去で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

- 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
  - フォームデータ

フォームデータは、削除されてはじめて上書き消去の対象となります。

- ファクス
  - PC FAX の印刷のデータ
  - 連携先機器を使って送受信したファクス
    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
  - メール送信データ
  - フォルダー送信データ
  - Ridoc Desk Navigator や Web Image Monitor を使った文書配信データ
  - ネットワーク TWAIN スキャナーのデータ

    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。先読みモードにチェックをつけていないデータは、上書き消去の対象となりません。
- ドキュメントボックス
  - 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。
- その他
  - アドレス帳に登録されているデータ

    アドレス帳の変更や削除をすると上書き消去の対象になります。
  - Embedded Software Architecture アプリケーション

    Embedded Software Architecture アプリケーションのデータは 削除されてはじめて上書き消去の対象となります。

上書き消去できないデータ

- ユーザーコード別カウンター

消去方式（メモリー自動消去）

メモリー自動消去の消去方式は以下の中から選択できます。

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 1 回目の乱数、1 回目の乱数の補数、2 回目の乱数で上書きし、検証処理をします。

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。

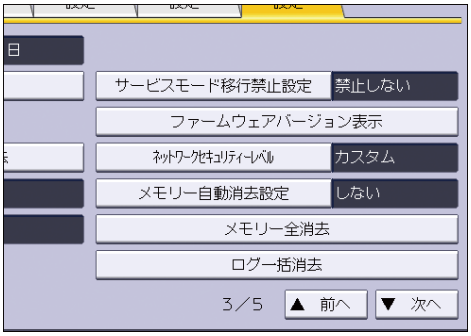
メモリー自動消去を設定する

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」に設定したあと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です。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ときは、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。**
- **上書き消去中はスリープモードに移行しません。上書き処理が完了した時点で移行します。**

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 2 回押します。

5. [メモリー自動消去設定] を押します。



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] を選択したときは、手順 10 へ進みます。[乱数方式] を選択したときは手順 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. [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. 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。
6. [しない] を押します。
7. [設定] を押します。
8. ログアウトします。

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、操作部の画面左下に消去の状態を示すアイコンが表示されます。



DMM001

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。
- 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り、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」表示に変わるかを確認してください。表示が変わらないときはサービス実施店に連絡してください。

メモリー全消去

本機を移設または廃棄するときに、ハードディスクに保存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。本体搭載メモリーに保存されている機器の設定はすべて初期化されます。

メモリー全消去後に本機を使用するときは、サービス実施店に相談してください。

重要

- **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です。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、Ridoc IO Device Manager を使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、Ridoc IO Device Manager 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 回に設定したときは、最大約 3 時間 45 分かかります。**
- **メモリー全消去が完了すると、本機のセキュリティー設定も消去され、機器の管理やユーザーの管理ができなくなります。メモリー全消去後に再度データが不特定ユーザーに書き込まれないように取り扱いに注意してください。**
- **本機のハードディスクのデータを消去するとともに、操作部のデータも初期化してください。［操作部初期設定］の［操作部機器設定］の［操作部設定の初期化］で、操作部のデータを初期化できます。初期化されるのは、［操作部初期設定］で設定した内容や各アプリケーションの設定、キャッシュなどの情報です。**

メモリー全消去で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
  - 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
  - フォームデータ
- ファクス
  - PC FAX の印刷のデータ
  - 連携先機器を使って送受信したファクス
    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
  - メール送信データ

- フォルダー送信データ
- Web Image Monitor を使った文書配信データ
- ネットワーク TWAIN スキャナーのデータ

  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。先読みモードにチェックをつけていないデータは、上書き消去の対象となりません。

- ドキュメントボックス
  - 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
- その他
  - アドレス帳に登録されているデータ
  - ユーザーコード別カウンター
  - Embedded Software Architecture アプリケーション

システム初期設定などの機器の設定は初期化されます。

消去方式（メモリー全消去）

メモリー全消去の消去方式は以下の中から選択できます。

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 1 回目の乱数、1 回目の乱数の補数、2 回目の乱数で上書きし、検証処理をします。

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。

BSI/VSITR

データを 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA で上書きします。計 7 回上書きされます。

Secure Erase

ハードディスク内部に組み込まれたアルゴリズムで上書き消去します。

フォーマット

ハードディスクのフォーマットだけします。データの上書きはしません。

*1 National Security Agency（米）国家安全保障局

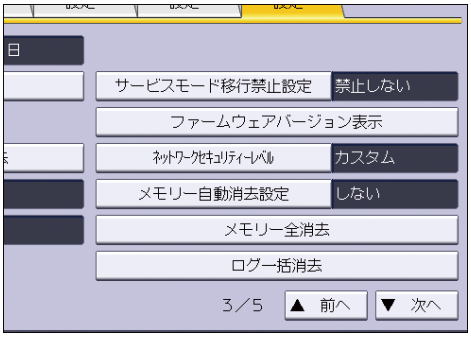
*2 Department of Defense（米）国防総省

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。

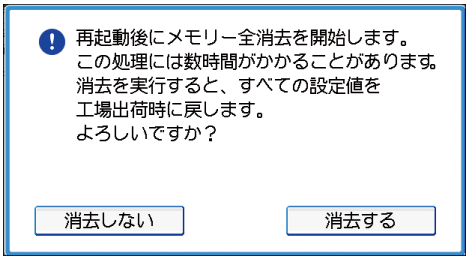


7. 消去方式を選択します。

   [NSA 方式]、[DoD 方式]、[BSI/VSITR 方式]、[Secure Erase]、[フォーマット] を選択したときは、手順 10 へ進みます。

   [乱数方式] を選択したときは手順 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、メモリー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。

主電源の切りかたは、『本機をお使いになる方へ』「電源の入れかた、切りかた」を参照してください。

補足

- 万一、メモリー全消去が完了する前に主電源スイッチを切ったときは、主電源スイッチを再び入れたときに、メモリー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

メモリー全消去の途中で本機の電源を切りたいときは、一時停止して電源を切ることができます。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。

重要

- **消去方式で［Secure Erase］または［フォーマット］を選択したときは一時停止できません。**
- **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. 本機の主電源を切ります。

主電源の切りかたは、『本機をお使いになる方へ』「電源の入れかた、切りかた」を参照してください。

5. ネットワークセキュリティーを強化する

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

アクセスコントロールを設定する

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

アクセスを許可する IP アドレスを範囲指定により制限します。

たとえば、アクセスコントロール範囲を［192.168.15.16］-［192.168.15.20］に設定すると、アクセスできる PC の IP アドレスは、192.168.15.16～192.168.15.20 です。

重要

- **アクセスコントロールは LPR、RCP/RSH、FTP、SSH/SFTP、Bonjour、SMB、WSD (Device)、WSD (Printer)、WSD (Scanner)/DSM、IPP、DIPRINT、RHPP、Web Image Monitor、Ridoc Desk Navigator からの使用を制限できます。Ridoc IO Navi の監視機能は制限できません。**
- Ridoc IO Device Manager などの SNMP と telnet の使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. **「セキュリティー」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、Ridoc IO Device Manager、または Ridoc IO OperationServer で設定できます。ただし設定対象プロトコルが異なります。

プロトコル	ポート	設定手段	無効時の状態
IPv4	-	• 操作部 • Web Image Monitor • telnet	IPv4 で動作するすべてのアプリケーションが使用できません。 IPv4 通信しているときは Web Image Monitor で IPv4 を無効にできません。
IPv6	-	• 操作部 • Web Image Monitor • telnet	IPv6 で動作するすべてのアプリケーションが使用できません。
IPsec	-	• 操作部 • Web Image Monitor • telnet	IPsec による暗号化通信ができません。
FTP	TCP:21	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	FTP の機能が使用できません。 操作部からの設定で個人情報の表示だけを制限できます。
ssh/sftp	TCP:22	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	sftp の機能が使用できません。 操作部からの設定で個人情報の表示だけを制限できます。
telnet	TCP:23	• Web Image Monitor • Ridoc IO Device Manager	telnet の機能が使用できません。
SMTP	TCP:25 （可変）	• 操作部 • Web Image Monitor • Ridoc IO Device Manager • Ridoc IO OperationServer	メール通知機能の SMTP 受信が使用できません。
HTTP	TCP:80	• Web Image Monitor • telnet	HTTP の機能が使用できません。 IPP による 80 ポートでの印刷ができません。

プロトコル	ポート	設定手段	無効時の状態
HTTPS	TCP:443	• Web Image Monitor • telnet	HTTPS の機能が使用できません。 また、操作部と Web Image Monitor からの設定で SSL 通信だけを許可し、非 SSL 通信を禁止できます。
SMB	TCP:139	• 操作部 • Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	SMB の機能が使用できません。
NBT	UDP:137 UDP:138	• telnet	TCP/IP 経由での SMB 印刷の機能と、WINS サーバーによる NetBIOS 名解決機能が使用できません。
SNMPv1/v2	UDP:161	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	SNMPv1/v2 の機能が使用できません。 操作部、Web Image Monitor、telnet で SNMPv1/v2 による設定だけを禁止し、参照は許可できます。
SNMPv3	UDP:161	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	SNMPv3 の機能が使用できません。 操作部、Web Image Monitor、telnet からの設定で SNMPv3 暗号通信だけ許可し、非 SNMPv3 暗号通信は禁止できます。
RSH/RCP	TCP:514	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	RSH の機能とネットワーク TWAIN 機能が使用できません。 操作部からの設定で個人情報の表示だけを禁止にできます。
LPR	TCP:515	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	LPR の機能が使用できません。 操作部からの設定で個人情報の表示だけを制限できます。
IPP	TCP:631	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	IPP の機能が使用できません。

プロトコル	ポート	設定手段	無効時の状態
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)	• 操作部 • Web Image Monitor • Ridoc IO Device Manager • Ridoc IO OperationServer	IP-ファクス接続の H.323/SIP/T.38 接続機能が使用できません。
SSDP	UDP:1900	• Web Image Monitor • telnet	Windows からの UPnP による機器検索ができません。
Bonjour	UDP:5353	• Web Image Monitor • telnet	Bonjour の機能が使用できません。
@Remote	TCP:7443 TCP:7444	• 操作部 • telnet	RICOH @Remote が使用できません。
DIPRINT	TCP:9100	• Web Image Monitor • telnet • Ridoc IO Device Manager • Ridoc IO OperationServer	DIPRINT の機能が使用できません。
RFU	TCP:10021	• 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。
WSD (Device)	TCP:53000（可変）	• Web Image Monitor • telnet	WSD (Device)の機能が使用できません。
WSD (Printer)	TCP:53001（可変）	• Web Image Monitor • telnet	WSD (Printer)の機能が使用できません。
WSD (Scanner)/DSM	TCP:53002（可変）	• Web Image Monitor • telnet	WSD (Scanner)と DSM の機能が使用できません。
WS-Discovery	TCP:3702 UDP:3702	• telnet	WSD (Device/Printer/Scanner)の機器検索ができません
RHPP	TCP:59100	• Web Image Monitor • telnet	RHPP で印刷ができません。
LLMNR	UDP:5355	• Web Image Monitor • telnet	LLMNR による名前解決要求に応答できません。

補足

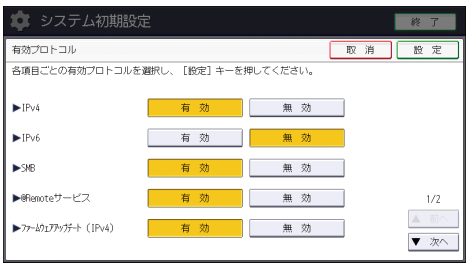
- 「無効時の状態」欄に記載されている個人情報の表示禁止は、操作部の「個人情報表示制限」で設定できます。詳しくは、P.239「セキュリティー強化機能を設定する」を参照してください。

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。



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. 「セキュリティー」の[ネットワークセキュリティー]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ーレベルを設定する

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、セキュリティーの強度を変更できます。この設定により不正なアクセスを制限できます。

ネットワークセキュリティーレベル設定は、操作部、または Web Image Monitor で設定できます。ただし設定対象プロトコルが異なります。

重要

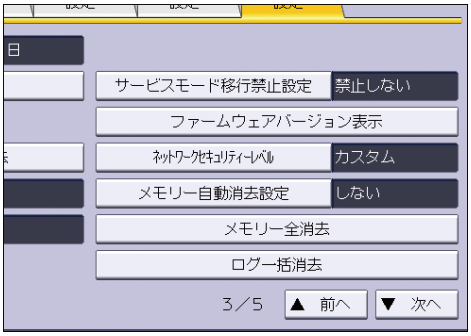
- **ネットワークセキュリティーレベルによっては一部のユーティリティーで通信ができないことや、ログインに失敗することがあります。**

セキュリティーレベル	説明
[レベル 0]	全機能を最も容易に使用できます。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ー強度を持ちます。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ー強度を持ちます。 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ー強度を持ちます。脅威から守るべき情報が極めて重要なときに設定します。
[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ーレベル] を押します。



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

○=使用できます。

- =使用できません。

▲=使用できます。ポートが開いています。

■=使用できません。ポートが閉じています。

TCP/IP*1

機能	レベル 0	レベル 1	FIPS 140	レベル 2
TCP/IP*2	○	○	○	○
HTTP > ポート 80	▲	▲	▲	▲
IPP > ポート 80	▲	▲	▲	▲
IPP > ポート 631	▲	▲	■	■
SSL/TLS > ポート 443	▲	▲	▲	▲
SSL/TLS > SSL/TLS 通信許可設定	暗号文優先	暗号文優先	暗号文のみ	暗号文のみ
SSL/TLS バージョン > TLS1.2	○	○	○	○
SSL/TLS バージョン > TLS1.1	○	○	○	○
SSL/TLS バージョン > TLS1.0	○	○	○	○
SSL/TLS バージョン > SSL3.0	○	–	–	–
暗号強度設定 > AES	128 ビット/256 ビット	128 ビット/256 ビット	128 ビット/256 ビット	128 ビット/256 ビット
暗号強度設定 > 3DES	168 ビット	168 ビット	168 ビット	–
暗号強度設定 > RC4	–	–	–	–
DIPRINT	○	○	–	–
LPR	○	○	–	–
FTP	○	○	○	○
sftp	○	○	○	○
ssh	○	○	○	○
RSH/RCP	○	○	–	–
TELNET	○	–	–	–
Bonjour	○	○	–	–
SSDP	○	○	–	–
SMB	○	○	–	–
NetBIOS over TCP/IPv4	○	○	–	–
WSD (Device)	○	○	○	○
WSD (Printer)	○	○	○	○
WSD (Scanner)/DSM	○	○	○	○

機能	レベル 0	レベル 1	FIPS 140	レベル 2
WSD (機器の暗号化通信)	–	–	○	○
RHPP	○	○	–	–

*1 IPv4、IPv6 共通です。

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

SNMP

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

TCP/IP 暗号強度設定

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
S/MIME > ダイジェストアルゴリズム	SHA1	SHA1	SHA1	SHA-256 ビット
SNMPv3 > 認証アルゴリズム	MD5	SHA1	SHA1	SHA1
SNMPv3 > 暗号化アルゴリズム	DES	DES	AES128	AES128

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

機器証明書による通信経路の保護

本機では SSL/TLS、IPsec、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。また、デジタル署名 PDF、デジタル署名 PDF/A を使用することで、PDF を保護します。

これらを使用するには、事前に本機に機器証明書を作成、導入します。

機器証明書には、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

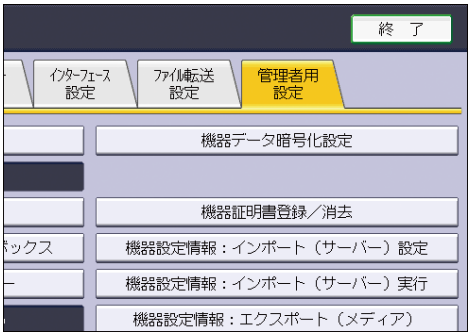
- **管理者の方は、証明書の期限を管理し、期限が切れる前に証明書の更新をしてください。**
- **管理者の方は、証明書の発行元が適切であることを確認してください。**

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、自己証明書を使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。

補足

- 機器証明書を削除するときは、手順 6 で［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 などで使用するときは、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、自己証明書を使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。

   本機から機器証明書を削除するときは、［削除］をクリックします。

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。
9. セキュリティーの警告に関するダイアログが表示されたら内容を確認して、[このサイトの閲覧を続行する] 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。

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、認証局証明書を使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」の内容を使用してください。

補足

- 2 つの証明書の申請を同時にすると、証明書の発行先が表示されないことがあります。導入するときに証明書の目的と導入順について確認してください。
- Web Image Monitor で機器証明書を作成できますが、Web Image Monitor から直接、認証局への申請はできません。
- 機器証明書の要求を取りやめるときは、[取りやめ要求] をクリックします。

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、認証局証明書を使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。**
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ときは、中間証明書の内容も入力してください。

   表示項目や設定項目の詳細は、Web Image Monitor のヘルプを参照してください。
7. **［OK］をクリックします。**
8. **1〜2 分待ってから、［OK］をクリックします。**

   「証明書状態」に「導入済み」が表示され、本機に機器証明書が導入されます。
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表示されます。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. 1〜2 分待ってから、[OK] をクリックします。

本機に中間証明書が導入されます。中間証明書が導入されたかについては、「証明書詳細情報」から確認できます。「証明書詳細情報」は、Web Image Monitor のヘルプを参照してください。

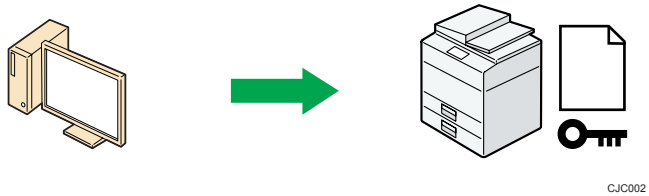
9. ログアウトします。

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。

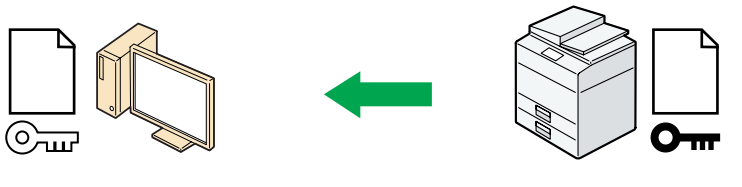
SSL/TLS による暗号化通信の流れ

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。



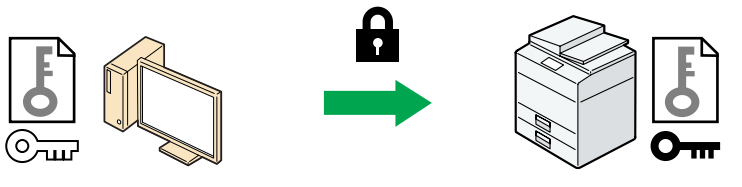
CJC002

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。



CJC003

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。



CJC004

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。



CJC005

自己証明書使用時の設定の流れ

1. 機器証明書の作成と導入

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

2. SSL/TLS を有効にする

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

認証局証明書使用時の設定の流れ

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ことを確認するには、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使用するとき、または認証局証明書を使用するときのどちらにも共通の設定方法です。

1. **Web Image Monitor からネットワーク管理者がログインします。**
2. **［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. **IPv4, IPv6 のうち SSL/TLS を有効にするものを「有効」にします。**
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。**

   暗号化通信モードは、［暗号文優先］、［暗号文/平文］、［暗号文のみ］のどれかを選択します。
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 つを有効にします。

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 1 つはチェックしておきます。

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。

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」が［暗号文のみ］になっているときに、Web ブラウザーが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直してください。
- SSL/TLS バージョンと暗号強度設定は、［ネットワークセキュリティー］でも変更できます。
- TLS1.2、TLS1.1、TLS1.0、SSL3.0 の有効または無効の設定により、LDAP サーバーに接続できないことがあります。

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/7/8/8.1、Windows Server 2008/2008 R2/2012/2012 R2 で IPP-SSL を使用して本機で印刷するときは、証明書のインストールが必要です。証明書のインストールについては、ネットワーク管理者から、各ユーザーにお伝えください。

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

補足

- 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。
- 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/7/8/8.1、Windows Server 2008/2008 R2/2012/2012 R2 で OS 標準の IPP ポートを使っているときに、機器証明書の［共通名称］のホスト名や IP アドレスを変更するときは、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。またユーザー認証の設定（ログインユーザー名とログインパスワード）を変更するときも、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。

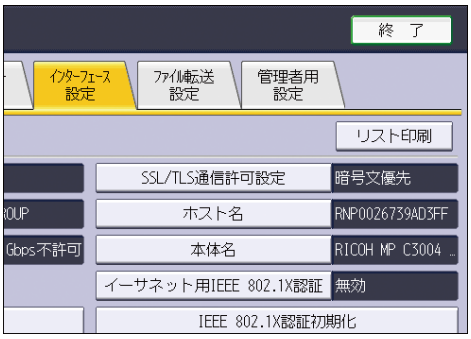
SSL/TLS 暗号化通信モードを設定する

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

暗号化通信モード	説明
暗号文のみ	暗号化通信だけを許可します。 暗号化できないときは、通信できません。
暗号文優先	暗号化できるときは、暗号化通信します。 暗号化できないときは、平文で通信します。
暗号文／平文	暗号化、または平文の指定された方法で通信します。

機器証明書を導入後、SSL/TLS の暗号化通信モードを設定します。

1. **操作部からネットワーク管理者がログインします。**
2. **［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。

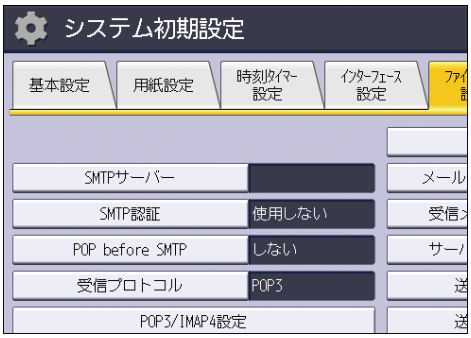
7. **［設定］を押します。**
8. **ログアウトします。**

補足

- Web Image Monitor からも SSL/TLS の暗号化通信モードを設定できます。Web Image 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。



5. 「SSL」の［利用する］を押します。

   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使用したメッセージ送信ができ、情報漏えいを防止します。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。メッセージを暗号化するには、送信者側（本機）とメールの受信者側がともに S/MIME に対応していることが必要です。

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。**

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 2003 以降
- Thunderbird 3.1.7 以降
- Windows Live メール

補足

- メールに電子署名を添付したときは、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は、S/MIME に対応したユーザーのメールは暗号化されますが、S/MIME に対応していないユーザーのメールは暗号化されません。
- 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。
- ファクスとスキャナーの 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ーの設定をする」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するには、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ことが必要です。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。

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 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. **［詳細入力］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す。機器証明書の作成、導入については P.116「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します。**

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を識別し、メッセージに改ざんがないことを確認できます。

自己証明書使用時の設定の流れ

1. 機器証明書の作成と導入

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

2. 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。

認証局証明書使用時の設定の流れ

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。**

補足

- 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使用するときと、認証局証明書を使用するときのどちらにも共通の設定方法です。

1. Web Image Monitor からネットワーク管理者がログインします。
2. [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］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］を押したとき
パフォーマンス優先	(b)と(c)のチェックを省略します。 あて先を選択した場合や、［スタート］を押した場合など、有効期限のチェックに時間がかかるときは、「パフォーマンス優先」にすると、操作にかかる時間が短縮されます。

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［S/MIME］をクリックします。
4. 「動作モード」で、［セキュリティー優先］か［パフォーマンス優先］のどちらかを選択します。
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.185「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.116「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。**

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 に添付できる機器証明書は、署名アルゴリズムが sha1WithRSA-1024 のものです。

IPsec を設定する

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

重要

- **「HTTPS 通信の除外」で［無効］を選択しているとき、誤った鍵設定をすると、Web Image Monitor にアクセスできなくなります。アクセス不能となることを防止するために HTTPS 通信を IPsec の除外対象に設定できます。HTTPS 通信も IPsec の対象とするときは、IPsec 機能が正しく設定されたことを確認したあとに、「HTTPS 通信の除外」で［無効］を選択します。「HTTPS 通信の除外」で［有効］を選択し、HTTPS 通信を IPsec の対象から外していても、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。**
- **DHCP、DNS、WINS で取得する情報とパケットは IPsec の対象にならないものがあります。**

対応 OS

OS	備考
• Windows Server 2003/2003 R2	IPv4 の IPsec が使用できます。
• Windows Vista/7/8/8.1 • Windows Server 2008/2008 R2/2012/2012 R2 • Mac OS X 10.4.8 or later • Red Hat Enterprise Linux WS 4.0 • Solaris 10	IPv4/IPv6 両方の IPsec が使用できます。

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 つのセキュリティープロトコルに対応しています。

ESP プロトコル

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

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

AH プロトコル

ヘッダを含むパケットの認証だけに対応したセキュリティー通信をします。

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

AH プロトコル + ESP プロトコル

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

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

補足

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

自動鍵交換設定

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

自動鍵交換設定方式では、SA の設定が自動的にされますが、最初に ISAKMP SA が自動設定（フェーズ 1）され、続いて IPsec 通信のための IPsec SA が自動設定（フェーズ 2）されます。また、より高いセキュリティーを確保した通信をするために、設定の有効期間を定めることで SA の定期的な自動更新ができます。本機の自動鍵交換設定方式は IKEv1 だけ対応しています。SA の設定は、複数設定できます。

個別設定とデフォルト設定

自動鍵交換設定は、IPsec で使用するアルゴリズムや鍵などの SA 設定を個別に 4 種類設定できます。また個別設定に含まれない通信相手を対象としたデフォルト設定を別途設定できます。個別設定の優先度は 1 が最も高く 4 が最も低くなります。優先度の低い個別設定で IP アドレス範囲を指定し、優先度の高い個別設定でその範囲内の特定の通信者を指定した設定ができます。

IPsec 設定項目

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

IPsec の設定項目

設定項目	設定内容	設定値
IPsec*1	IPsec 機能を有効にするか無効にするか設定します。	・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 の対象から外すときは有効を選択します。

*1「IPsec」の設定は操作部からもできます。

自動鍵交換設定のセキュリティーレベル

自動鍵交換設定では、セキュリティーレベルの項目を選択すると、セキュリティー詳細項目はレベルに応じて自動設定されます。

各セキュリティーレベルの特徴は以下のとおりです。

セキュリティーレベル	セキュリティーレベルの特徴
認証のみ	パケットデータの暗号化はしないで、通信相手の認証とデータの改ざん防止だけをするときに選択します。パケット単位のデータは平文のままネットワークを流れるので、盗聴される危険性があります。
認証と暗号化（低）	通信相手の認証と改ざん防止に加え、パケットデータを暗号化するときに選択します。「認証と暗号化（高）」よりもセキュリティーの強度は低い設定です。
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ー強度の高い設定です。

各セキュリティーレベル選択時の自動設定値は以下のとおりです。

設定項目	各セキュリティーレベル選択時の設定値		
	認証のみ	認証と暗号化（低）	認証と暗号化（高）
セキュリティーポリシー	Apply	Apply	Apply
カプセル化モード	トランスポート	トランスポート	トランスポート
IPsec 要求レベル	可能な場合使用する	可能な場合使用する	必須
認証方式	PSK	PSK	PSK
フェーズ 1 ハッシュアルゴリズム	MD5	SHA1	SHA256
フェーズ 1 暗号化アルゴリズム	DES	3DES	AES-128-CBC
フェーズ 1 Diffie-Hellman グループ	2	2	2
フェーズ 2 セキュリティープロトコル	AH	ESP	ESP
フェーズ 2 認証アルゴリズム	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	HMAC-SHA1-96/ HMAC-SHA256-128/ HMAC-SHA384-192/ HMAC-SHA512-256	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	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

セキュリティーレベルを選択すると、セキュリティー詳細項目は自動設定されますが、アドレスタイプや、ローカルアドレス、リモートアドレスは手動での入力が必須です。また自動設定された内容を手動で変更すると、セキュリティー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。

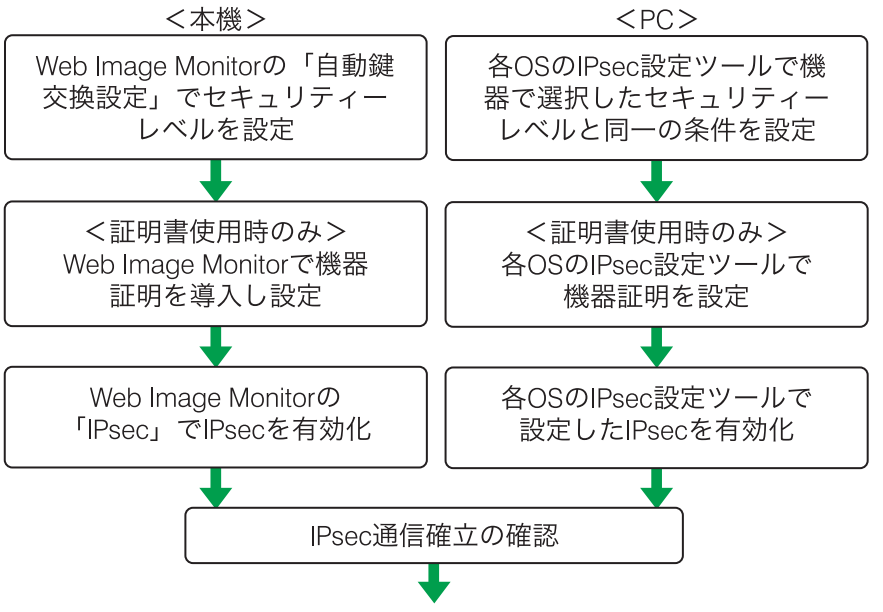
設定項目	設定内容	設定値
アドレスタイプ	IPsec の対象とする IP アドレスのタイプを選択します。	・無効 ・IPv4 ・IPv6 ・IPv4/IPv6（デフォルト設定のみ）

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。	・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。	・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。
セキュリティーポリシー	IPsec の処理方法を設定します。	・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)
カプセル化モード	カプセル化モードを選択します。 (自動設定対象項目)	・トランスポート ・トンネル セキュリティーレベルに関係なくトランスポートモードが選択されます。 トンネルを選択したときは、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)	・可能な場合使用する ・必須

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）	・PSK ・証明書 セキュリティーレベルに関係なく「PSK」方式が選択されます。 「PSK」を使用するときは、PSK の文字列を設定します。 「証明書」を選択するときは、事前に機器証明書を導入して、IPsec 用の証明書を割り当てておきます。
PSK 文字列	自動鍵交換で使用する PSK 文字列を設定します。	認証方式が PSK のときに、アスキー文字列で 32 文字以内の文字列を入力します。
フェーズ 1 ハッシュアルゴリズム	フェーズ 1 で使用するハッシュアルゴリズムを選択します。 （自動設定対象項目）	・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）	・DES ・3DES ・AES-128-CBC ・AES-192-CBC ・AES-256-CBC
フェーズ 1 Diffie-Hellman グループ	IKE の暗号鍵生成に使用する Diffie-Hellman グループ番号を選択します。 （自動設定対象項目）	・1 ・2 ・14
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 セキュリティープロトコル	フェーズ 2 で使用するセキュリティープロトコルを選択します。 暗号化と認証を同時にするときは ESP または ESP ＋ AH 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）	・ESP ・AH ・ESP ＋ AH

設定項目	設定内容	設定値
フェーズ 2 認証アルゴリズム	フェーズ 2 で使用する認証アルゴリズムを選択します。 （自動設定対象項目）	・HMAC-MD5-96 ・HMAC-SHA1-96 ・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）	・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 DiffieHellman グループ番号を選択します。 （自動設定対象項目）	・無効 ・1 ・2 ・14
フェーズ 2 有効期間	フェーズ 2 で使用する SA の有効期間を設定します。	300 秒（5 分）～172800 秒（48 時間）の間で秒単位で設定します。

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

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.116「機器証明書による通信経路の保護」の機器証明書の作成方法、導入方法を参照してください。導入した証明書を IPsec に割り当てる方法は、P.141「証明書を選択する」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［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ときは、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。**

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.116「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］ー［システムとセキュリティ］ー［管理ツール］をクリックします。**

   Windows 8 のときは、画面の右上端または、右下端をポイントし［設定］ー［コントロールパネル］ー［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 10 のときは、［スタート］ボタンを右クリックし、［設定］ー［コントロールパネル］ー［システムとセキュリティ］ー［管理ツール］をクリックします。
2. **［ローカルセキュリティポリシー］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）］をダブルクリックします。**
4. **［操作］メニューから［IP セキュリティポリシーの作成］をクリックします。**

   ［IP セキュリティポリシーウィザード］が表示されます。
5. **［次へ］をクリックします。**
6. **任意の IP セキュリティポリシー名を入力し、［次へ］をクリックします。**
7. **「既定の応答規則をアクティブにする」のチェックを外し、［次へ］をクリックします。**

8. 「プロパティを編集する」にチェックを付け、[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。

    存在しないときは [追加] をクリックし作成します。
12. [OK] を 2 回クリックします。
13. [規則] タブを選択し、[追加] をクリックします。

    「セキュリティの規則ウィザード」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. 「IP フィルター一覧」で [追加] をクリックします。
18. 「名前」に任意の IP フィルター名を入力し、[追加] をクリックします。

    「IP フィルターウィザード」が表示されます。
19. [次へ] をクリックします。
20. 必要に応じて IP フィルターの説明を入力し、[次へ] をクリックします。
21. 「発信元アドレス」で「このコンピューターの IP アドレス」を選択し、[次へ] をクリックします。
22. 「宛先アドレス」で「特定の IP アドレスまたはサブネット」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。
23. IPsec の対象とするプロトコルを選択し、[次へ] をクリックします。

    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。

    「TCP」または「UDP」を選択したときは、「IP プロトコルポートの設定」で発信ポートと宛先ポートを指定し、[次へ] をクリックします。
24. [完了] をクリックします。
25. [OK] をクリックします。
26. 設定した IP フィルターを選択し、[次へ] をクリックします。

27. [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。

28. [次へ] をクリックします。

29. 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。

30. [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。

31. [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。

32.「カスタム」を選択し、[設定] をクリックします。

33.「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。

34.「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。

35.「セッションのキーの設定」で「新しいキーの生成間隔（R)」にチェックを付け、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。

36. [OK] をクリックします。

37. [次へ] をクリックします。

38. [完了] をクリックします。

39. 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。

自動鍵交換設定でセキュリティーレベルを「認証と暗号化（高)」に指定するときは、作成したフィルター操作を選択し [編集] をクリックします。フィルター操作のプロパティ画面で [セッションキーの PFS (Perfect Forward Secrecy)を使う] をチェックします。Windows で PFS を使用するときは、自動鍵交換設定のフェーズ 2 で使用される PFS グループ番号は、ステップ 11 にある Diffie-Hellman グループ番号から自動的に変換されます。このため、機器の自動鍵交換設定で指定されたセキュリティーレベルを変更し、「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。

40. 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。

41. [完了] をクリックします。

42. [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。

43. 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。

telnet で IPsec を設定する

本機では、telnet からも IPsec 設定の確認、変更ができます。telnet にログインするときのログインユーザー名とパスワードは管理者へ問い合わせてください。telnet のログイン方法、操作方法は、『ネットワークの接続/システム初期設定』「telnet を使用する」を参照してください。

5

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 設定の設定値

  自動鍵交換設定の個別 IKE 設定値

  自動鍵交換設定のデフォルト IKE 設定値

現在の設定の分割表示

msh> ipsec -p

- IPsec 関連の設定情報を分割して表示します。

ipsec exclude

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

現在の設定の表示

msh> ipsec exclude

- 現在の除外対象プロトコルが表示されます。

除外対象プロトコルの設定

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

- 設定するプロトコルを指定し、除外対象とするときは「on」を、除外対象にしないときは「off」を指定します。プロトコルで「all」を指定するとすべてのプロトコルを一括して設定できます。

ipsec ike

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

現在の設定の表示

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

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

設定の無効化

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

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

個別設定のローカルアドレス／リモートアドレスの設定

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

- 個別設定番号を指定し、使用するアドレスタイプを指定してから、ローカルアドレスとリモートアドレスを指定します。
- ローカルアドレス、リモートアドレスの値は、アドレスタイプが IPv4 のときは、アドレスのあとに「/」を入れて 0-32 の整数値でマスク長を指定します。アドレスタイプが IPv6 のときは、アドレスのあとに「/」を入れて 0-128 の整数値でマスク長を指定します。
- 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ときは「any」を指定します。

処理方法の設定

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

- 個別設定番号、またはデフォルト設定を指定し、指定したアドレスに該当するパケットの処理方法を指定します。

- 該当するパケットに IPsec を適用するときは、「apply」を指定し、IPsec を適用しないときは、「bypass」を指定します。
- 該当するパケットを破棄するときは、「discard」を指定します。
- 処理方法の指定値を省略したときは、現在の設定が表示されます。

セキュリティープロトコルの指定

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

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

要求レベルの設定

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

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

カプセル化モードの設定

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

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

トンネルモードの始点/終点 IP アドレスの設定

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

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

IKE の相手認証方式の設定

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

- 個別設定番号、またはデフォルト設定を指定し、相手認証方式を指定します。
- 事前共有鍵による認証方式を使用するときは「psk」を指定し、証明書による認証方式を使用するときは「rsasig」を指定します。

  証明書による認証方式を使用するときは、事前に機器証明書を導入し、IPsec 用の証明書を割り当てておきます。機器証明書の導入は Web Image Monitor を使用して設定します。
- 「psk」を指定したときは、PSK 文字列の設定が必要です。

PSK 文字列の設定

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

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

ISAKMP SA（フェーズ 1）のハッシュアルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}

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

ISAKMP SA（フェーズ 1）の暗号アルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}

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

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

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

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

ISAKMP SA（フェーズ 1）の有効期間の設定

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

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

IPsec SA（フェーズ 2）の認証アルゴリズムの設定

msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-sha384|hmac-sha512}

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

IPsec SA（フェーズ 2）の暗号アルゴリズムの設定

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

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

IPsec SA（フェーズ 2）の PFS の設定

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

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

IPsec SA（フェーズ 2）の有効期間の設定

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

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

自動鍵（ike）設定値の初期化

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

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

IEEE 802.1X 認証を設定する

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

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

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

サイト証明書を導入する

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

証明書の入手方法は、使用している環境により異なります。

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

1. **Web Image Monitor からネットワーク管理者がログインします。**
2. **［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［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。
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.116「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、使用している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」の［変更］をクリックして、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」の［変更］をクリックして、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 ブラウザーの［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、操作部の［インターフェース設定］の［リスト印刷］でネットワークサマリーを印刷して状況を確認できます。
- 原因が特定できないときは、操作部の［インターフェース設定］の［ネットワーク］の［IEEE 802.1X 認証初期化］で設定を初期化してから、手順をやり直してください。

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、使用している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」の［変更］をクリックして、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」の［変更］をクリックして、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」を使用しているアクセスポイントに合わせて入力します。

13. 「セキュリティー方式」に［WPA2］を選択します。

14. 「WPA2 認証方式」に、［WPA2］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

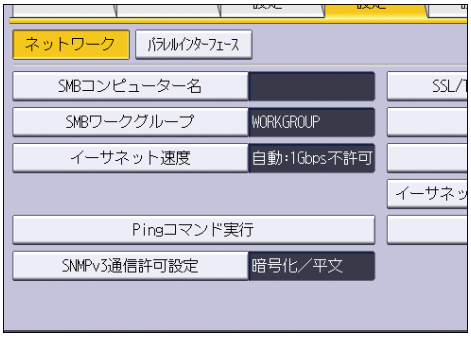
- 設定の不具合により、本機と通信できなくなることがあります。このようなときは、操作部の［インターフェース設定］の［リスト印刷］でネットワークサマリーを印刷して状況を確認できます。
- 原因が特定できないときは、操作部の［インターフェース設定］の［ネットワーク］の［IEEE 802.1X 認証初期化］で設定を初期化してから、手順をやり直してください。

SNMPv3 暗号化通信を設定する

Ridoc IO Device Manager などの SNMPv3 プロトコルを使用するソフトウェア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

- Ridoc IO Device Manager は、リコーのホームページからダウンロードできます。詳しくは、『本機をお使いになる方へ』「ダウンロードできるソフトウェア」を参照してください。
- Ridoc IO Device Manager 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 Ridoc IO Device Manager の「SNMP アカウント設定」の暗号化パスワードの設定が必要です。暗号化パスワードの設定方法は、Ridoc IO Device Manager 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ときは、通信データが暗号化されないことや、通信できないことがあります。ネットワーク管理者の暗号パスワードの設定は、P.15「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

ドライバー暗号鍵と 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します。

IPP 認証のパスワード

IPP 認証のパスワードを暗号化するには、Web Image Monitor を使用し、認証方法で［DIGEST］を選択し、本機に IPP 認証のパスワードを設定します。

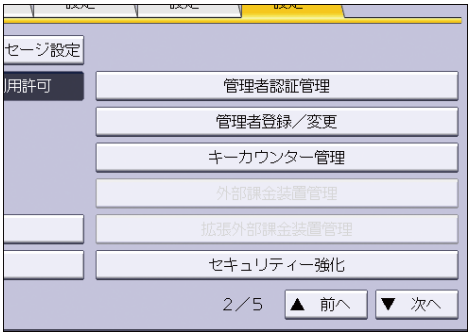
補足

- 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.15「管理者を登録、変更する」を参照してください。

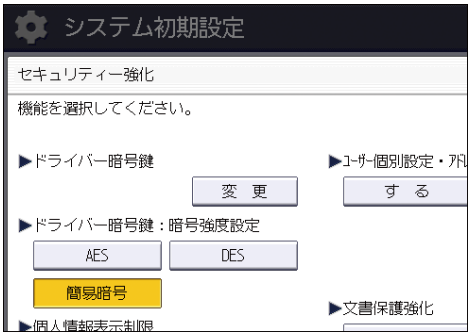
ドライバー暗号鍵を設定する

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. ［セキュリティー強化］を押します。



6. 「ドライバー暗号鍵」の［変更］を押します。



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

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. 「セキュリティー」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。

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	• RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5
Windows Server 2008 R2/2012/2012 R2	• AES256-CTS-HMAC-SHA1-96 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC (ARCFOUR-HMAC-MD5) • DES-CBC-MD5*
Heimdal	• 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 [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 つを有効にします。
5. [OK] をクリックします。
6. ログアウトします。

6. 文書の漏えいを防止する

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。

フォルダーを管理する

ドキュメントボックスのフォルダーの削除、パスワード変更、ロックされたときの解除方法を説明します。

フォルダーを削除する

文書管理者、またはユーザーが操作します。

が表示されたフォルダーを削除するときは、パスワードが必要です。

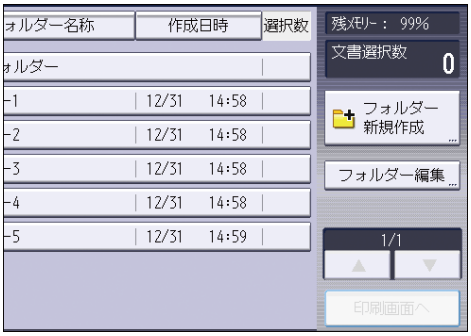
ユーザーがフォルダーのパスワードを忘れたときは、文書管理者がパスワードを変更できます。

文書管理者はパスワードなしでフォルダーを削除できます。

削除権限のない文書が含まれているときは、フォルダーを削除できません。

共有フォルダーは削除できません。

1. **操作部から文書管理者、またはユーザーがログインします。**
2. **画面右上の［初期設定］（ ）を押して初期設定画面を閉じます。**
   「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. **ホーム画面の［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. **［フォルダー編集］を押します。**



5. **対象のフォルダーを選択します。**

6. パスワード入力画面が表示されたらフォルダー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ときは、パスワード入力画面が表示されません。

7. [削除] を押します。

8. [削除する] を押します。

9. 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。

フォルダーのパスワードを変更する

文書管理者、またはユーザーが設定します。

ユーザ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。

共有フォルダーはパスワードを設定できません。

1. 操作部から文書管理者、またはユーザーがログインします。

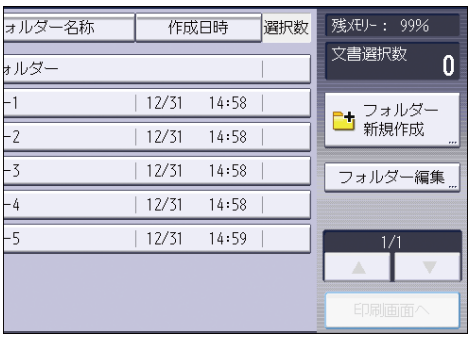
2. 画面右上の [初期設定] (⚙) を押して初期設定画面を閉じます。

   「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. ホーム画面の [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. [フォルダー編集] を押します。



5. 対象のフォルダーを選択します。

6. パスワード入力画面が表示されたらフォルダー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ときは、パスワード入力画面が表示されません。

7. [パスワード変更] を押します。
8. 新しいパスワードを入力し、[OK] を押します。
   フォルダーのパスワードに使用できるのは、4 桁～8 桁の数字です。
9. 確認のためにもう一度パスワードを入力し、[OK] を押します。
   パスワードで保護されたフォルダーはが表示されます。
10. 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。

フォルダーのロックを解除する

文書管理者だけが操作できます。

セキュリティー強化機能の「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 回入力するとフォルダーはロックされます。「文書保護強化」については、P.239「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。

1. 操作部から文書管理者がログインします。
2. 画面右上の［初期設定］（）を押して初期設定画面を閉じます。
   「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. ホーム画面の［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. [フォルダー編集] を押します。
5. 対象のフォルダーを選択します。
   ロックされたフォルダーはが表示されます。
6. [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. 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。

蓄積文書を管理する

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、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、送信などの不正使用を防止できます。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、文書の不正使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.169「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、どのユーザーもできます。
- 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。
- オーナーのアクセス権の初期値は、［閲覧］です。オーナーは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、または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。

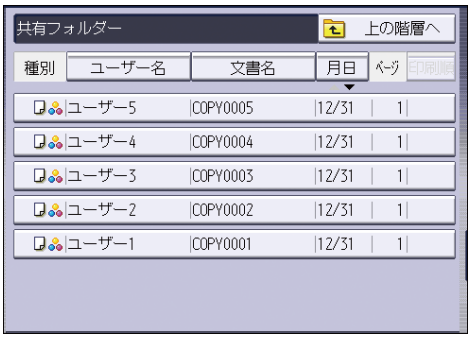
重要

- **文書へアクセスできなくなったときは、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へのアクセスが必要なときは、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、ほかのユーザーのアクセス権の変更ができます。**
- **文書のオーナーとフルコントロール権限を持つほかのユーザーは、その文書の［アクセス権変更］でオーナーとほかのユーザーのアクセス権を変更できます。**

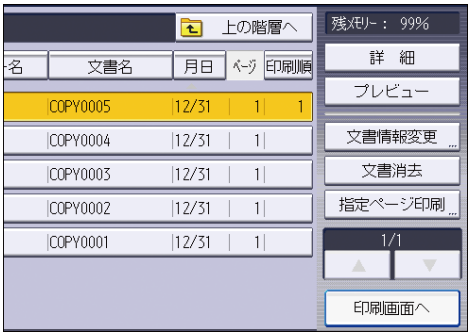
1. 操作部から文書管理者、またはオーナーがログインします。
2. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。
   「この機能を利用する権限はありません。」が表示されたときは、［確認］を押します。
3. ホーム画面の［ドキュメントボックス］アイコンを押します。
   「この機能を利用する権限はありません。」が表示されたときは、［確認］を押します。
4. 対象のフォルダーを選択します。



5. 対象文書を選択します。

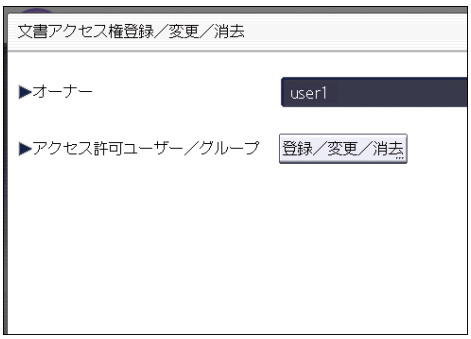


6. [文書情報変更] を押します。



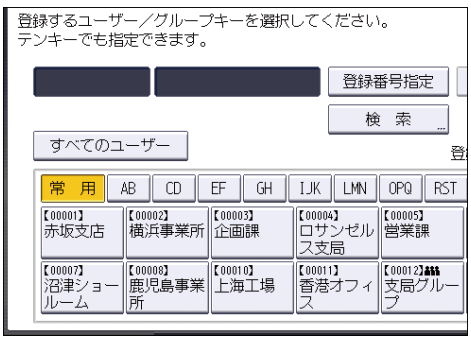
7. [アクセス権変更] を押します。

8. 「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。



9. [新規登録] を押します。

10. 登録するユーザーまたはグループを選択します。

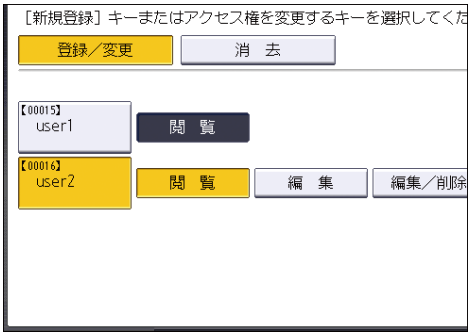


複数のユーザーを選択できます。

[すべてのユーザー] を押すと、全ユーザーを選択できます。

11. [閉じる] を押します。

12. 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。

13. ［閉じる］を押します。
14. ［OK］を押します。
15. 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。

蓄積文書のオーナーを変更する

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. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。

「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. ホーム画面の［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. 対象のフォルダーを選択します。
5. 対象文書を選択します。
6. ［文書情報変更］を押します。
7. ［アクセス権変更］を押します。
8. 「オーナー」の［変更］を押します。

9. 登録するユーザーを選択します。
10. [閉じる] を押します。
11. [OK] を 2 回押します。
12. 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、またはオーナーが設定します。

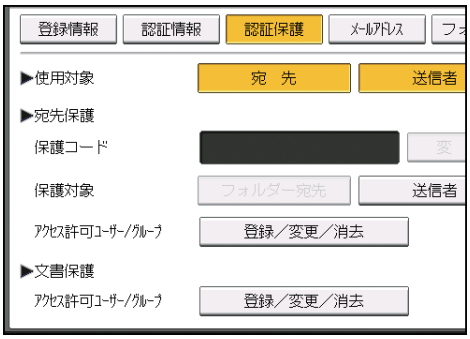
特定のユーザーが蓄積する文書に、文書を使用できるユーザーとそのアクセス権を設定します。

蓄積文書ごとにアクセス権を設定するときと比較して、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。**

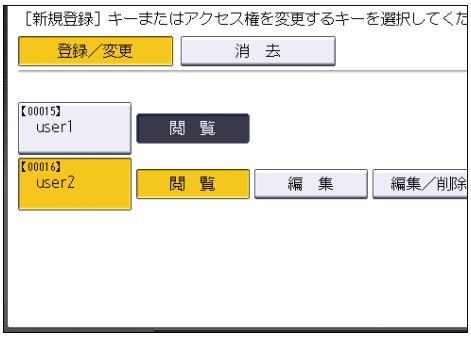
1. 操作部からユーザー管理者、またはオーナーがログインします。
2. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。
   「この機能を利用する権限はありません。」が表示されたときは、［確認］を押します。
3. [アドレス帳管理] を押します。
4. ユーザーを選択します。
5. [認証保護] を押します。
6. 「文書保護」にある「アクセス許可ユーザー／グループ」の［登録／変更／消去］を押します。



7. [新規登録] を押します。
8. 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。

9. **［閉じる］を押します。**
10. **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。

11. **［閉じる］を押します。**
12. **［設定］を押します。**
13. **［閉じる］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。

蓄積文書にパスワードを設定する

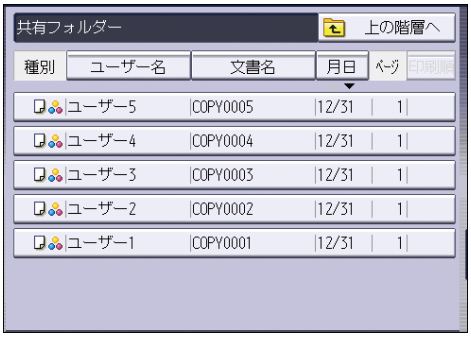
文書管理者、またはオーナーが設定します。

1. **操作部から文書管理者、またはオーナーがログインします。**
2. **画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。**
   「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. **ホーム画面の［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。

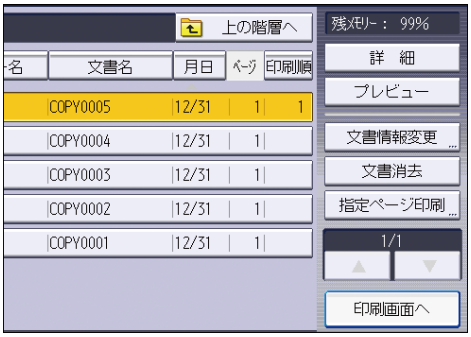
4. 対象のフォルダーを選択します。



5. 対象文書を選択します。



6. [文書情報変更] を押します。



7. [パスワード変更] を押します。
8. 設定するパスワードを入力し、[OK] を押します。

   文書パスワードで使用できるのは、4 桁～8 桁の数字です。
9. 確認のためにもう一度パスワードを入力し、[OK] を押します。

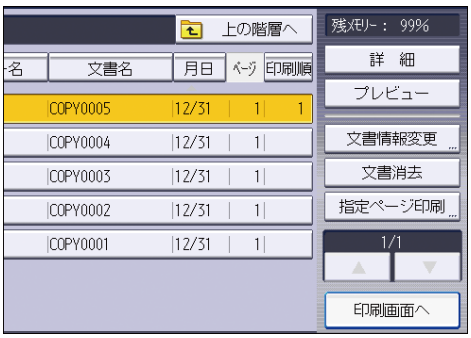
   パスワードで保護された文書は が表示されます。
10. [OK] を押します。
11. ログアウトします。

蓄積文書のロックを解除する

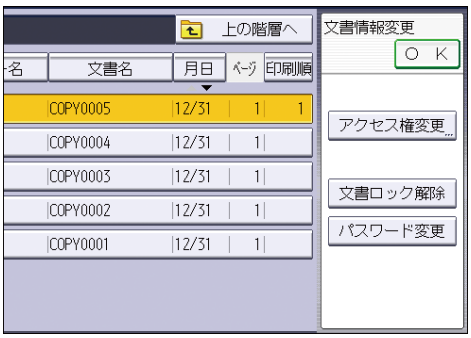
文書管理者だけが操作できます。

セキュリティー強化機能の「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.239「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。

1. **操作部から文書管理者がログインします。**
2. **画面右上の［初期設定］（ ）を押して初期設定画面を閉じます。**
   「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. **ホーム画面の［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. **対象のフォルダーを選択します。**
5. **対象文書を選択します。**
   ロックされた文書は が表示されます。
6. **［文書情報変更］を押します。**



7. **［文書ロック解除］を押します。**



8. **［解除する］を押します。**
   が に変わります。

9. [OK] を押します。
10. 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ることがあります。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、機密印刷機能を使用します。

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。
- 一時的な文書の保存をするときは、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、またはオーナーが操作します。

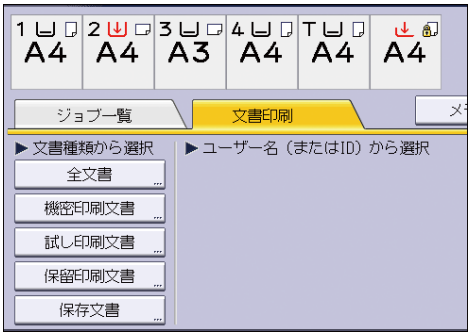
オーナーが機密印刷文書を消去するには、機密印刷文書のパスワードが必要です。オーナーがパスワードを忘れたときは、文書管理者がパスワードを変更できます。

文書管理者はパスワードなしで機密印刷文書を消去できます。

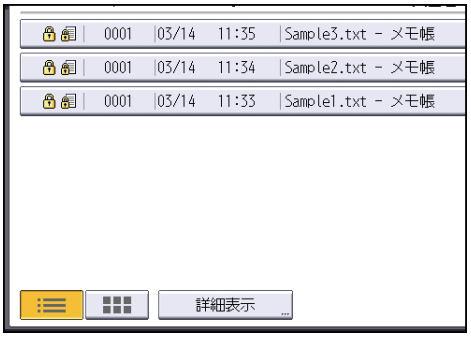
1. **操作部から文書管理者、またはオーナーがログインします。**
2. **画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。**

   「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. **ホーム画面の［プリンター］アイコンを押します。**
4. **［文書印刷］を押します。**

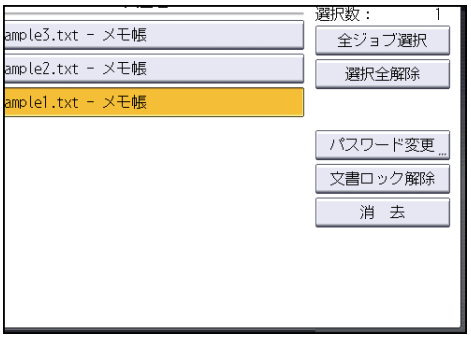
5. [機密印刷文書] を押します。



6. 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ときは、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

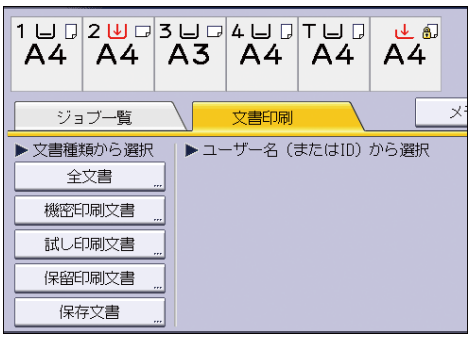
- 「一時置き文書自動消去設定」を有効にすると、蓄積文書を自動で消去できます。「一時置き文書自動消去設定」の設定方法は、『プリンター』「データ操作/管理」を参照してください。
- Web Image Monitor からも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。

機密印刷文書のパスワードを変更する

文書管理者、またはオーナーが設定します。

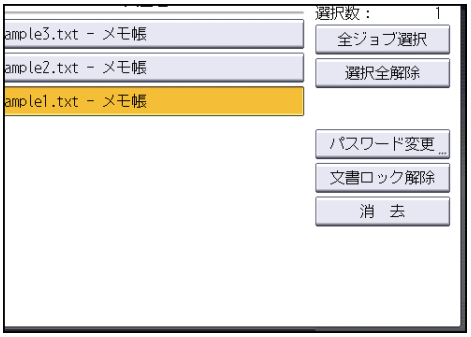
オーナーがパスワードを忘れたときは、文書管理者がパスワードを変更します。

1. **操作部から文書管理者、またはオーナーがログインします。**
2. **画面右上の［初期設定］（ ）を押して初期設定画面を閉じます。**
   「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. **ホーム画面の［プリンター］アイコンを押します。**
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ときは、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。

   文書パスワードに使用できるのは、4 桁～8 桁の数字です。

10. 確認のためにもう一度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。

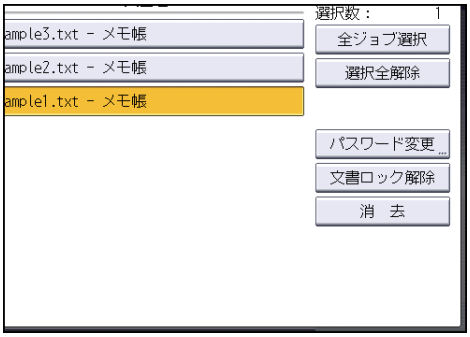
セキュリティー強化機能の「文書保護強化」を［する］に設定したときは、誤ったパスワードを 10 回入力すると文書はロックされます。「文書保護強化」については、P.239「セキュリティー強化機能を設定する」を参照してください。

1. 操作部から文書管理者がログインします。
2. 画面右上の［初期設定］（⚙）を押して初期設定画面を閉じます。

   「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. ホーム画面の［プリンター］アイコンを押します。
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。

不正コピー抑止／不正コピーガード機能

本機ではコピー、ドキュメントボックス、プリンターで出力するときに、不正コピーを抑止・ガード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、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。

不正コピーガードは、専用の地紋を設定して印刷すると、その文書の読み取りをしたときに文書全体がグレー地に変換されるため、文書情報の漏えいを防止します。ただし、グレー地に変換するためには、文書の読み取りをする複写機／複合機で不正コピーガード機能を有効にする必要があります。

不正コピーガード機能を有効にした機器で不正コピーガード文書を検知すると、ブザー音が鳴ります。また、不正コピーのログが残ります。

不正コピー抑止機能を使用するには

1. 本機で地紋印刷を有効にします。機器管理者が設定します。設定方法は P.178「地紋印刷を有効にする」を参照してください。
2. コピー、ドキュメントボックス、プリンターでの印刷時に不正コピー抑止を設定して印刷します。設定の権限は［不正コピー抑止強制設定］の設定により異なります。詳しくは、P.178「地紋印刷を有効にする」を参照してください。

不正コピーガード機能を使用するには

1. 本機で地紋印刷を有効にします。機器管理者が設定します。設定方法は P.178「地紋印刷を有効にする」を参照してください。
2. コピー、ドキュメントボックス、プリンターでの印刷時に不正コピーガード印刷を設定して印刷します。設定の権限は［不正コピー抑止強制設定］の設定により異なります。詳しくは、P.178「地紋印刷を有効にする」を参照してください。
3. 本機で不正コピーガード検知を有効にします。

   不正コピーガード文書をコピーやファクス、またはスキャナーで読み取ったり、ドキュメントボックスに蓄積したときに、検知してグレー地に変換します。

   機器管理者が設定します。設定方法は、P.180「不正コピーガード検知を有効にする」を参照してください。

補足

- コピー時の画質の設定によって、地紋効果の画像の一部に濃淡が発生することがあります。そのときは、画質の設定を［文字］または［写真］に切り替えて使用してください。

地紋印刷を有効にする

不正コピー抑止、不正コピーガード用の地紋印刷を有効にします。

コピー/ドキュメントボックスの地紋印刷を有効にする

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 3 回押します。
5. [不正コピー抑止印刷：コピー]、[不正コピー抑止印刷：ドキュメントボックス] のうち、設定するものを選択します。
6. 「不正コピー抑止強制設定」の [変更] を押します。
7. 地紋印刷を強制するかしないかを選択します。
   - [しない]

     地紋印刷を強制しません。

     ユーザーはコピー/ドキュメントボックスの操作画面から、地紋の印刷有無と地紋の設定を変更できます。
   - [する：一部ユーザー変更可]

     強制的に地紋印刷をします。

     ユーザーはコピー/ドキュメントボックスの操作画面から、地紋の設定を変更できますが、地紋の種類と濃度は変更できません。
   - [する：ユーザー変更不可]

     強制的に地紋印刷をします。

     ユーザーはコピー/ドキュメントボックスの操作画面から、地紋の設定を変更できません。
8. [設定] を 2 回押します。
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、『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。

プリンターの地紋印刷を有効にする

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 3 回押します。

5. [不正コピー抑止印刷：プリンター] を押します。
6. 「不正コピー抑止設定」の [変更] を押します。
7. [する] を押してから、[設定] を押します。
8. 「不正コピー抑止強制設定」の [変更] を押します。
9. 地紋印刷を強制するかしないかを選択します。
   - [ドライバー/コマンド優先]

     地紋印刷を強制しません。

     ユーザーはプリンタードライバーで地紋印刷の有無と、地紋の設定を変更できます。
   - [ドライバー/コマンド優先(一部除)]

     強制的に地紋印刷をします。

     ユーザーはプリンタードライバーで地紋の設定を変更できますが、地紋の種類、色、濃度は変更できません。
   - [機器側設定優先]

     強制的に地紋印刷をします。

     ユーザーはプリンタードライバーで地紋の設定を変更できません。
10. [設定] を 2 回押します。
11. 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、『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。

不正コピーガード検知を有効にする

不正コピーガード文書を、コピー、ファクス・スキャナーで読み取ったり、ドキュメントボックスに蓄積すると、全体をグレー地に変換し、不正なコピーからガードします。

重要

- **不正コピーガード文書以外をコピー、ファクス・スキャナーで読み取ったり、ドキュメントボックスに蓄積したときは、グレー地に変換されません。**

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. [不正コピーガード検知] を押します。
6. [する] を押します。
   [不正コピーガード検知] を設定しないときは、[しない] を押します。
7. [設定] を押します。
8. ログアウトします。

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（名前また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ー印字といいます。

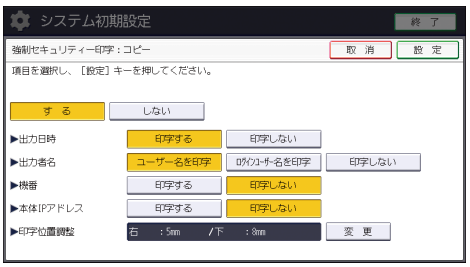
出力者の情報が必ず印字されることで、情報漏えいの抑止効果があります。また情報漏えい元を特定するときに活用できます。

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、強制セキュリティー印字ができます。

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. **強制セキュリティー印字をする機能を選択します。**
   - [強制セキュリティー印字：コピー]
   - [強制セキュリティー印字：ドキュメントボックス]
   - [強制セキュリティー印字：ファクス]
   - [強制セキュリティー印字：プリンター]
6. **[する] を押します。**

   強制セキュリティー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。**

   出力者名を印字するときは [ユーザー名を印字] または [ログインユーザー名を印字] を選択します。



- 出力日時

  ジョブの開始時刻が印字されます。
- 出力者名

  ユーザー認証が有効なときに印字されます。
  - ユーザー名を印字

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

  アドレス帳の「認証情報」の「ユーザーコード」または「ログインユーザー名」が印字されます。

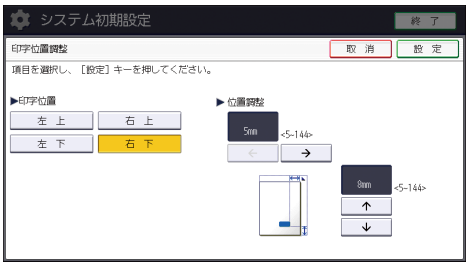
- 機番

  [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ときは、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. 「印字位置調整」の[変更]を押します。
9. 印字位置を設定します。



10. [設定]を 2 回押します。
11. ログアウトします。

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、放置による情報漏えいを防止します。

出力をともなう、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
- 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. **[印刷をともなうジョブの制限]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、出力をとも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は、『プリンター』「蓄積文書を印刷する」を参照してください。

7. 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られます。

ログは Web Image Monitor、またはログ収集サーバーを使用して確認します。収集したログは 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・スキャナー配信などのユーザーの文書にかかわるワークフローすべてのログ情報/操作部から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カスタマーエンジニア操作/ログ転送結果などのシステム動作/暗号化通信、アクセス攻撃、ロックアウト、ファームウェアの正当性確認などのセキュリティー動作

- eco ログ

  主電源のオン、オフ/電力ステータスの遷移/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

補足

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

Web Image Monitor からログを管理する

本機で記録するログの種類、収集レベルを設定できます。また、ログの一括消去やダウンロードができます。

Web Image Monitor で管理できるログ項目

Web Image Monitor でログを収集する機能を有効にすると、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。Web Image Monitor の［設定］の［ログ］で設定します。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	通常のコピーと試しコピーのログ
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
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 または Ridoc Desk Navigator 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: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、Ridoc Desk Navigator、または Ridoc Edit Manager Pro 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

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

設定項目	Log Type の属性値	収集するログ
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 または Ridoc Desk Navigator 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

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
不正コピー	Unauthorized Copying	不正コピーガード文書を読み取ったときのログ
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
ログ転送結果	Transfer Log Result	Ridoc IO OperationServer へのログ転送結果のログ
ログ収集項目変更	Log Collection Item Change	ジョブログ収集レベル、アクセスログ収集レベル、収集する項目を変更したときのログ
暗号化通信ログ収集	Collect Encrypted Communication Logs	ユーティリティー、Web Image Monitor、または外部機器との間で暗号化通信をするときのログ

設定項目	Log Type の属性値	収集するログ
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 カードの抜き差しや異なった 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*4	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
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
Web Image Monitor オートログアウト	Web Image Monitor Auto Logout	Web Image Monitor からのオートログアウトのログ
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
ユーザ別カウンタークリア結果	Counter Clear Result: Selected User(s)	ユーザー別のカウンターをクリアしたときのログ

設定項目	Log Type の属性値	収集するログ
全ユーザーカウンタークリア結果	Counter Clear Result: All Users	全ユーザーのカウンターをクリアしたときのログ
機器設定情報のインポート	Import Device Setting Information	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
フォルダー新規作成/削除	Creating/Deleting Folders	フォルダーが作成または削除されたときのログ

*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 頻繁なリモートログインによるユーザー認証 DoS 攻撃をアクセス攻撃と呼びます。

*4「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

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

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、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

  共通項目（ジョブログとアクセスログ）、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。

	Start Date/Time	…	Result	…	Access Result	Source	…	Print File Name	Target	…	Stored File Name
1	20XX-12-03T15:43:03.0	…	Completed	…			…			…	
2		…	Completed	…		Report	…			…	
3		…	Completed	…			…		Print	…	

CJD022

1. 共通項目

   共通項目が 1 行で出力されます。

2. ソース

   共通項目の「Result」、「Status」、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。

3. ターゲット

   共通項目の「Result」、「Status」、ジョブログの出力情報が出力されます。複数のターゲットがあるときは、複数行が出力されます。

- アクセスログ

  共通項目とアクセスログ情報が 1 行で出力されます。

- eco ログ

  eco ログ情報が 1 行で出力されます。

共通項目（ジョブログとアクセスログ）

Start Date/Time

操作/事象の開始日時が記録されます。

End Date/Time

操作/事象の終了日時が記録されます。

Log Type

ログの種類が記録されます。

ログの種類は、P.345「Web Image Monitor：プリンター文書印刷」を参照してください。

Result

操作、または事象の結果が記録されます。

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。

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

Operation Method

操作の手段が記録されます。

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

Status

操作、または事象の状態が記録されます。

値	説明
Completed	正常終了
Failed	異常終了
Succeeded	成功
Password Mismatch	パスワード不一致
User Not Programmed	ユーザー未登録
Other Failures	その他の失敗
User Locked Out	ユーザーロックアウト中
User Cancel	ユーザーによるキャンセル

値	説明
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	文書喪失によるキャプチャー失敗
Functional Problem	デバイス不良によるキャプチャー失敗
Communication Failure	通信失敗
Communication Result Unknown	通信結果判定不能
Failure in some or all parts	失敗または一部失敗
Importing/Exporting by Other User	ほかのユーザによるインポート／エクスポート処理・実行中
Connection Failed with Remote Machine	出力先との接続失敗
Write Error to Remote Machine	出力先への書込みエラー
Specified File: Incompatible	指定ファイル不適合
Specified File: Format Error	指定ファイルフォーマットエラー
Specified File: Not Exist	指定ファイルなし
Specified File: No Privileges	指定ファイル権限なし
Specified File: Access Error	指定ファイルアクセスエラー
Memory Storage Device Full	外部メディア容量フル
Memory Storage Device Error	外部メディア異常
Encryption Failed	暗号化失敗
Decoding Failed	復号化失敗
Common Key Not Exist	共通鍵なし
Connection Error	通信異常
Specified Server Error	サーバー未設定エラー
Specified Client Error	クライアント未設定エラー
Authentication Settings Mismatch	アドレス帳スペック不一致
Authentication Method Mismatch	認証モード不一致
Maximum Limit of Registered Number	集中管理登録台数上限

値	説明
Invalid Password	パスコードエラー
Processing	仕掛かり中
Error	エラー
Suspended	中断

Cancelled: Details

操作または事象が異常終了のときにその状況が記録されます。

値	説明
Cancelled by User	ユーザーによるキャンセル
Input Failure	入力中の異常終了
Output Failure	出力中の異常終了
Other Error	ジョブの実行前に検知したエラー、またはその他のエラー
Power Failure	電源断
External Charge Unit Disconnected	動作中に課金装置が抜けた
Insufficient No. of Original for Overlay	合成コピーの実行時の原稿不足
Exceed Max. Stored Page (File Storage)	ドキュメントボックスで蓄積できるページ数を超えた
Exceed Max. Stored File (File Storage)	ドキュメントボックスで蓄積できる文書数を超えた
Hard Disk Full (File Storage Memory)	ドキュメントボックスで蓄積できるハードディスクの容量を超えた
Exceeded Max. Email Size	メールサイズの制限を超えた
Exceeded Max. File Size	1 文書のサイズ上限値を超えた
Scanner Error	自動原稿送り装置による読取りエラー
Timeout	タイムアウト
Exceed Max. Stored Page (Image Area)	キャプチャーできるページ数を超えた
Hard Disk Full (Image Area)	キャプチャーできるハードディスクの容量を超えた
Specified Folder to Store does not Exist	蓄積先のフォルダーが存在しない
Password for Folder Specified to Store is Incorrect	蓄積先のフォルダーパスワード不一致

値	説明
Folder is Locked	フォルダーがロック中
Memory Full	データを処理するためのメモリー領域がいっぱいになった
Print Data Error	本機に搭載されていない PDL、またはポートを使用した
Data Transfer Interrupted	以下のときに記録されます。 • 異なる機種のドライバーを使用した • ネットワーク障害が発生した • PC FAX ドライバーからキャンセルした • ファクスの通信障害が発生した
Reception Error	ファクスの受信ができなかった
Over Job Limit	受け付けできるジョブ数を超えた
Specifying Destination Error	不正なあて先を指定した、またはあて先の指定桁数が 41 桁以上を超えた
Specifying Line Error	回線の指定に誤りがあった
Authentication Failed (Access Restricted)	本機の認証に失敗した
Exceeded Print Volume Use Limitation	ログインしたユーザーの利用量制限枚数を超えた
No Privilege	文書や機能の使用権限がなかった
Unavailable Size to Store	指定の用紙サイズ（不定形も含む）が蓄積できないサイズだった
Transmission Failed (Data Deleted)	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
Not Entered Document Password	文書のパスワードが未入力
Connection Failed with Destination	指定したサーバーやフォルダーが見つからなかった
Authentication Failed with Destination	送信先の認証で失敗した
Transmission Failed with Memory Full	送信先の記憶領域の容量がいっぱい
Line Busy	相手先が話し中
No Response	相手先からの応答がなかった
Not Facsimile Destination	相手先がファクスではなかった
Invalid Device Certificate	機器証明書がなかった、有効期限が切れていた、また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

値	説明
Invalid Expiration Date: Destination's Certificate	宛先の証明書の有効期限が切れていた
Invalid Device/Destination's Certificate	宛先の証明書と機器証明書の両方が不正
Exceeded Print Volume Use Limitation: Communication Error	印刷利用量を集中管理しているときに、集中管理サーバー機との通信エラーが発生した。
Exceeded Print Volume Use Limitation: No Remaining Print Volume	印刷利用量を集中管理しているときに、 残度数が他のクライアント機に割り当てられているため、度数取得に失敗した。
Print Cancelled (Error)	システムによるジョブキャンセル

User Entry ID

エントリー ID が記録されます。

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

値	説明
0x00000000	システム操作、未認証利用者の操作
0x00000001～0xfffffeff	ユーザーやユーザーコード
0xffffff80	システム操作
0xffffff81	システム操作、未認証利用者の操作
0xffffff86	スーパーバイザー
0xffffff87	管理者
0xffffff88	管理者 1
0xffffff89	管理者 2
0xffffff8a	管理者 3
0xffffff8b	管理者 4

User Code/User Name

ユーザーの操作では、ユーザーコードまたはログインユーザー名が記録されます。

管理者では、管理者のログインユーザー名が記録されます。

Log ID

ログに ID が記録されます。ログを一意に指す ID で、16 進数で出力されます。

アクセスログ

Access Log Type

アクセスログの種類が記録されます。

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

Authentication Server Name

最後に認証を試みたサーバー名が記録されます。

No. of Authentication Server Switches

認証サーバーがダウンしたときにサーバーを切り替えた回数が記録されます。

サーバーダウンを検出したかを判断できます。

サーバー切り替え回数は、0〜4 回です。

0 のときは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。

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

Login Method

認証要求を受けた経路が記録されます。

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

Login User Type

ログインユーザーの種別が記録されます。

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

Target User Entry ID

対象者にエントリー ID が記録されます。

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

- ロックアウト操作
- パスワード変更

Target User Code/User Name

対象者のユーザーコードまたはユーザー名が記録されます。

管理者のときは、管理者のログインユーザー名が記録されます。

Address Book Registration No.

操作したユーザーの登録番号が記録されます。

Address Book Operation Mode

アドレス帳の変更をどのように実施したか記録されます。

Address Book Change Item

アドレス帳のどの内容を変更したか記録されます。

Address Book Change Request IP Address

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

Lockout/Release

ロックアウト状態が記録されます。

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

Lockout/Release Method

ロックアウトを解除した方法が記録されます。

値	説明
Manual	手動によるロックアウト解除
Auto	解除タイマーによるロックアウト解除

Lockout Release Target 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。

Counter to Clear

ユーザーごとにどのカウンターをクリアしたかが記録されます。

Export Target

機器情報のエクスポートの対象となる設定情報が記録されます。

値	説明
System Settings	システム初期設定
Copier Features	コピー初期設定
Fax Features	ファクス初期設定
Printer Features	プリンター初期設定
Scanner Features	スキャナー初期設定
Program (Copier)	プログラム（コピー）
Program (Scanner)	プログラム（スキャナー）
Program (Document Server)	プログラム（ドキュメントボックス）
Browser Features	ブラウザー初期設定
Web Image Monitor Setting	Web Image Monitor 設定
Web Service Settings	Web サービス設定
System/Copier SP	システム/コピー SP
Scanner SP	スキャナー SP
Printer SP	プリンター SP
Fax SP	ファクス SP

Target File Name

機器情報のインポート・エクスポート対象となるファイル名が記録されます。

Stored File ID

作成または削除された文書に ID が記録されます。

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

Stored File Name

作成または削除された文書のファイル名が記録されます。

Delete File Type

文書削除の種類が記録されます。

値	説明
Delete Normal File	通常文書削除
Auto Delete	自動削除
Others	その他の理由による削除

Folder Number

フォルダー番号が記録されます。

Folder Name

フォルダー名が記録されます。

Creating/Deleting Folders

フォルダーにどのような操作をしたか記録されます。

値	説明
Delete Folder	フォルダー削除
New Folder	フォルダー新規作成

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。

Collect Job Logs

ジョブログ収集の設定を変更したかどうかが記録されます。

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

Collect Access Logs

アクセスログ収集の設定を変更したかどうかが記録されます。

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

Collect Eco-friendly Logs

eco ログ収集の設定を変更したかどうかが記録されます。

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

Transfer Logs

ログ転送機能の設定を変更したかどうかが記録されます。

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

Log Type

ログ収集状態の変更で対象となるログタイプの種別が記録されます。

値	説明
Job Log	ジョブログ
Access Log	アクセスログ
Eco-friendly Log	eco ログ

Log Collect Level

ログレベル設定値が記録されます。

値	説明
Level 1	レベル 1
Level 2	レベル 2

値	説明
User Settings	ユーザー設定

Encryption/Cleartext

暗号化通信か、平文通信かの状態が記録されます。

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

Machine Port No.

本機のポート番号が記録されます。

Protocol

通信先のプロトコルが記録されます。

特定できないときは「Unknown」と記録されます。

IP Address

通信先の IP アドレスが記録されます。

Port No.

通信先のポート番号が記録されます。

10 進数で出力されます。

MAC Address

通信先の物理アドレスが記録されます。

Primary Communication Protocol

第一階層の通信プロトコル名が記録されます。

Secondary Communication Protocol

第二階層の通信プロトコル名が記録されます。

Encryption Protocol

暗号化プロトコル名が記録されます。

Communication Direction

通信方向が記録されます。

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

Communication Start Log ID

通信開始時のログ ID が記録されます。

通信開始時のログを一意に指す ID で、16 進数で出力されます。

Communication Start/End

通信開始／終了を判断するための識別子が記録されます。

Network Attack Status

攻撃検出の状態が記録されます。

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

Network Attack Type

攻撃の種別が記録されます。

値	説明
Password Entry Violation	パスワード攻撃
Device Access Violation	認証 DoS 攻撃
Request Falsification Violation	リクエストの改ざん

Network Attack Type Details

攻撃種別の詳細が記録されます。

値	説明
Authentication Error	認証エラー
Encryption Error	暗号エラー

Network Attack Route

攻撃経路が記録されます。

値	説明
Attack from Control Panel	操作部からの攻撃を受けた
Attack from Other than Control Panel	操作部以外からの攻撃を受けた

Login User Name used for Network Attack

ネットワーク攻撃に使用されたログインユーザー名が記録されます。

Add/Update/Delete Firmware

ファームウェア変更の方式が記録されます。

値	説明
Updated with SD Card	SD カードによる更新
Added with SD Card	SD カードによる追加
Deleted with SD Card	SD カードによる削除
Moved to Another SD Card	別の SD カードへの移動
Updated via Remote	リモートによる更新
Updated for Other Reasons	その他の理由による更新

Module Name

ファームウェアのモジュール名が記録されます。

Parts Number

ファームウェアの部品番号が記録されます。

Version

ファームウェアのバージョンが記録されます。

Machine Data Encryption Key Operation

暗号鍵の操作の種別が記録されます。

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

Machine Data Encryption Key Type

暗号鍵の種別が記録されます。

値	説明
Encryption Key for Hard Disk	HDD 暗号鍵
Encryption Key for NVRAM	NVRAM 暗号鍵
Device Certificate	機器証明書

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

設定変更をしたカテゴリーが記録されます。

値	説明
User Lockout Policy	ユーザーロックアウト
Auto Logout Timer	オートログアウト時間設定
Device Certificate	機器証明書
IPsec	IPsec
Compulsory Security Stamp	強制印字設定
S/MIME	S/MIME
WIM Auto Logout Timer	Web Image Monitor のオートログアウト時間設定
Extended Security	セキュリティー強化
Firmware Update Start	ファームウェアアップデート
Prohibit printing stored files from Web Image Monitor	Web Image Monitor での蓄積文書出力禁止

Configuration Name / Configuration Value

カテゴリーの属性が記録されます。

属性の値が記録されます。

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

値	説明
Auto Logout Timer	オートログアウト時間設定のする（On）、しない（Off）が記録されます。
Auto Logout Timer (seconds)	オートログアウトが働くまでの時間が記録されます。
Operation Mode	操作の種類が記録されます。
Certificate No.	操作対象の証明書の番号が記録されます。
Certificate No.: IEEE 802.1X (WPA/WPA2)	アプリケーションの使用する証明書の番号が記録されます。証明書を使用しなかったときは「Do not Use」と記録されます。
Certificate No.: S/MIME	アプリケーションの使用する証明書の番号が記録されます。証明書を使用しなかったときは「Do not Use」と記録されます。
Certificate No.: IPsec	アプリケーションの使用する証明書の番号が記録されます。証明書を使用しなかったときは「Do not Use」と記録されます。
Certificate No.: Digital Signature PDF	アプリケーションの使用する証明書の番号が記録されます。証明書を使用しなかったときは「Do not Use」と記録されます。
Certificate No.: Digital Signature PDF/A	アプリケーションの使用する証明書の番号が記録されます。証明書を使用しなかったときは「Do not Use」と記録されます。
IPsec	IPsec の有効（Active）、無効（Inactive）が記録されます。
Encryption Key Auto Exchange: Setting1-4: Remote Address	リモートアドレスが記録されます。
Encryption Key Auto Exchange: Setting1-4, Default Setting: Security Level	セキュリティーレベルが記録されます。 「認証のみ」を選択したときは「Authentication Only」と記録されます。「認証と暗号化（低）」を選択したときは「Authentication and Low Level Encryption」と記録されます。「認証と暗号化（高）」を選択したときは「Authentication and High Level Encryption」と記録されます。「ユーザー設定」を選択したときは「User Settings」と記録されます。
Encryption Key Auto Exchange: Setting1-4, Default Setting: Authentication Method	自動鍵交換方式の認証方法が記録されます。「PSK」、または「Certificate」が記録されます。
Compulsory Security Stamp	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。
Operation Mode	動作モードが記録されます。
Scanner: Email Sending	スキャナーを使用したメール送信時の署名が記録されます。
Fax: Transferring	ファクス転送時の署名が記録されます。

値	説明
Fax: Email Sending	ファクスを使用したメール送信時の署名が記録されます。
Fax: Notification Email Sending	ファクスを使用した通知メール送信時の署名が記録されます。
Document Server (Utility): Stored File Transferring	ドキュメントボックス（ユーティリティー）を使用した蓄積文書転送時の署名が記録されます。
WIM Auto Logout Timer (minutes)	Web Image Monitor のオートログアウト時間（分）が記録されます。
Update Firmware	[ファームウェアアップデート] の変更が記録されます。 「禁止」、または「禁止しない」が記録されます。
Change Firmware Structure	[ファームウェア構成変更] の変更が記録されます。 「禁止」、または「禁止しない」が記録されます。
Firmware Update Start	ファームウェア更新の開始が記録されます。
Prohibit printing stored files from Web Image Monitor	[Web Image Monitor での蓄積文書出力禁止] の変更が記録されます。 「禁止」、または「禁止しない」が記録されます。

Destination Server Name

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

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

HDD Format Partition

ハードディスク初期化の理由が記録されます。

値	説明
HDD Exchange	HDD 交換を検出
Problem with HDD Encryption Key	HDD 暗号鍵異常
Problem with Disk Label	ディスクラベルが読めない
Problem with File System	ファイルシステム異常発生

Access Result

ログが発生した操作の結果が記録されます。

値	説明
Completed	正常終了
Failed	異常終了

ジョブログ入力情報

Source

ジョブログの入力情報が記録されます。

値	説明
Scan File	原稿読み取り
Stored File	文書蓄積
Printer	プリンタードライバーからの印刷指示
Received File	ファクス受信
Report	レポート印刷

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。

Folder Number

蓄積されていたフォルダー番号が記録されます。

Folder Name

蓄積されていたフォルダー名が記録されます。

Print File Name

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

ジョブログ出力情報

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。

Target

ジョブログの出力情報が記録されます。

値	説明
Print	印刷
Store	蓄積
Send	送信

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。

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

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。

ファクス機能では「Stored File ID」はログに記録されません。

Stored File Name

出力情報が「Store」のとき、蓄積される文書のファイル名が記録されます。

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

Folder Number

蓄積したフォルダー番号が記録されます。

Folder Name

蓄積したフォルダー名が記録されます。

eco ログ

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。

値	説明
Main Power On	主電源を入れたときのログ
Main Power Off	主電源を切ったときのログ
Power Status Transition Result	電源ステータス移行結果のログ
Job Related Information	ジョブ関連情報のログ
Paper Usage	用紙使用量のログ
Power Consumption	消費電力量のログ

Log Result

イベントが終了しているかどうかを表します。

値	説明
Completed	正常終了
Failed	異常終了

Result

イベントの結果が記録されます。

値	説明
Succeeded	成功
Failed	失敗

Log ID

ログを特定する ID が記録されます。16 進の ID です。

Power Mode

本機の電源状態（移行後）がログとして記録されます。

値	説明
Standby	待機状態
Low Power	低電力状態
Silent	静音状態
HDD On	ハードディスク起動の状態
Engine Off	エンジン停止の状態
Controller Off	コントローラー停止の状態
STR	STR (Suspend To RAM)状態
Silent Print	静音印刷状態

値	説明
Low Power Print	低電力印刷状態
Fuser Unit Off	定着ユニット停止状態

Log Type

ジョブログのログの種類が記録されます。

Job Interval (seconds)

前回のジョブ開始から該当ジョブ開始までの経過時間が記録されます。

Job Duration (seconds)

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。

Paper Usage (Large Size)

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。

Paper Usage (Small Size)

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。

Paper Usage (2 Sided: Large 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。

Paper Usage (2 Sided: Small Size)

1 時間ごとの両面小サイズの紙の使用量が記録されます。

小サイズは、A3 または、11 × 17 インチ未満の用紙です。

Detected Power

消費電力を測定する本機の電源状態をログとして記録されます。

値	説明
Controller Standby	コントローラー待機状態
STR	STR (Suspend To RAM)状態
Main Power Off	主電源が切れている状態
Scanning/Printing	プリンター/スキャナー動作中
Printing	プリンター動作中
Scanning	スキャナー動作中
Engine Standby	エンジン待機状態
Engine Low	エンジン低電力状態

値	説明
Engine Night	エンジン静音状態
Engine Total	機器全体の状態
Fuser Unit Off	定着ユニット待機状態

Power Consumption(Wh)

電源状態別の消費電力量が記録されます。

収集するログを設定する

ログの種類ごとに収集設定を有効にし、収集レベルを設定します。

- ジョブログ収集レベル

  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

  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。

- eco ログ収集レベル

  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。

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［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します。

ログをダウンロードする

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

ログを収集するにはジョブログ、アクセスログ、eco ログの収集設定を有効にしてください。Web Image Monitor の［設定］の［ログ］で設定できます。

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」で、ダウンロードするログの種類を選択します。**

   セキュリティーログには、ジョブログ、アクセスログの 2 種類が含まれます。
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。
- ログで取得できる情報は、P.186「Web Image Monitor からログを管理する」を参照してください。

本機に保持できるログ件数

ジョブログ、アクセスログ、eco ログで、本機に保持できる最大件数を超え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ロードを実施しないと、ファイルに古いログが記録されないことがあります。

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

ログをダウンロードしたあとは、ログを一括消去してください。

ログを［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。

本機に保持できるログの最大件数

ログの種類	ログ最大件数
ジョブログ	4000
アクセスログ	12000
eco ログ	4000

ログ発生量の目安

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

本条件で 40 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 20 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

- ログのダウンロード中に動作したログは記録されないことがあるので、ログのダウンロード中はほかの動作をさせないでください。
- ログの一括消去は操作部と 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。

ジョブログとアクセスログは、1 つのファイルとしてダウンロードされます。

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

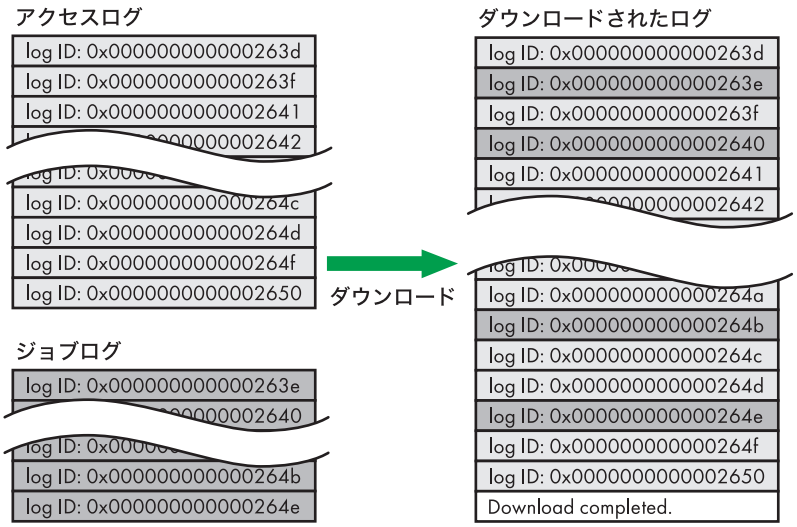
図の「上書きが発生しているとき」は、アクセスログで上書きが発生したときの例を示します。

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

eco ログは、単独のファイルとしてダウンロードされます。

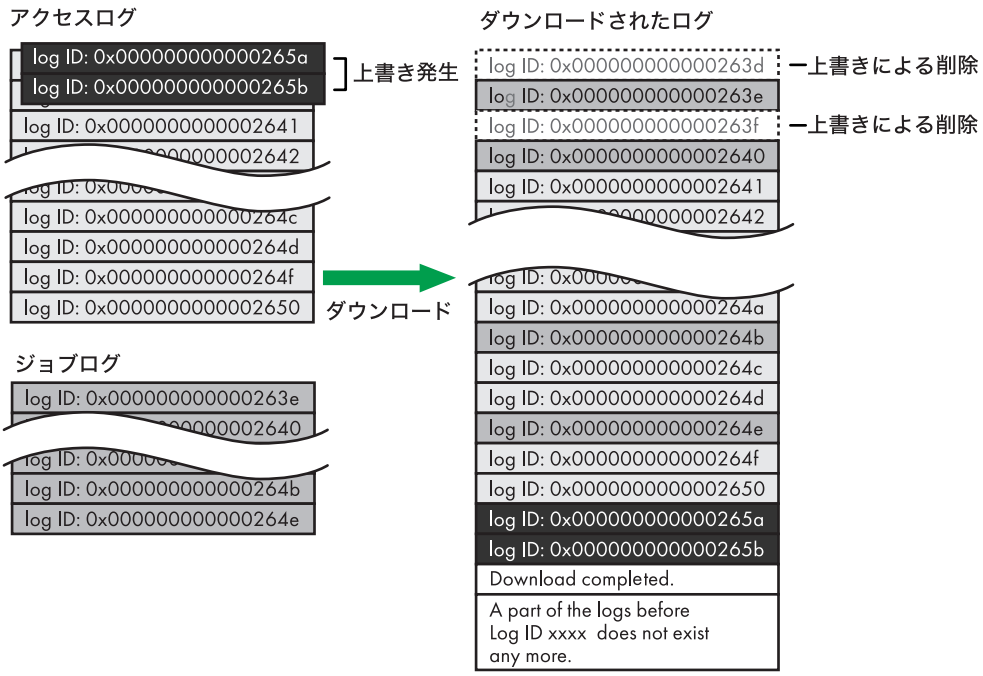
ログが上書きされるときは、優先順位にしたがって上書きされるため、優先順位の高いログは上書きされずに残ります。

上書きが発生していないとき



CJC006

上書きが発生しているとき



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とき

  Download completed.

- 上書きが発生しているとき

  Download completed.

  A part of the logs before Log ID xxxx does not exist any more.

補足

- 上書き発生しているときは、上書きによって一部のログが抜けるため、「Log ID xxxx」以降のログを確認してください。

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。

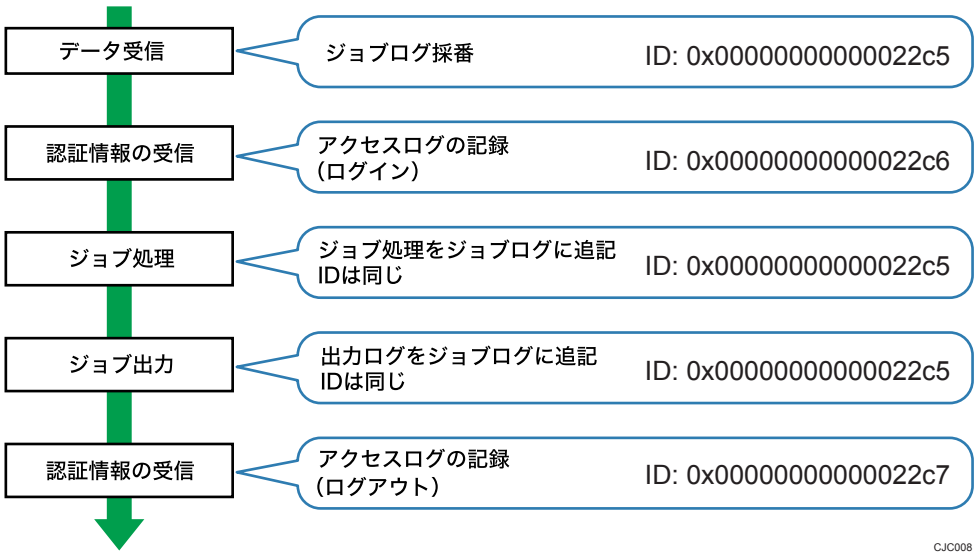
その後、認証情報を受けてログインのアクセスログが記録されます。

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

プリントジョブの流れ



ログを一括消去する

本機に記録されたログをまとめて消去できます。

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］のときに、「ログ一括消去」が表示されます。

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。

ログ収集サーバーへのログ転送を無効にする

ログ収集サーバーへのログ転送を無効にできます。

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

1. Web Image Monitor から機器管理者がログインします。
2. ［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. 「共通設定」で「ログ転送」の［無効］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。

本機からログを管理する

ログの収集設定、ログ収集サーバーへのログ転送設定、ログの一括消去ができます。

収集するログを設定する

ログの種類ごとに収集設定を有効にします。

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. [ログ収集設定]を押します。
6. 「ジョブログ」、「アクセスログ」、「eco ログ」で、それぞれ[有効]を選択します。
7. [設定]を押します。
8. ログアウトします。
9. 本機の主電源を切り、再度、主電源を入れます。

ログ収集サーバーへのログ転送を無効にする

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

ログ収集サーバーについては、販売店にお問い合わせください。

ログ転送の設定についてはログ収集サーバーの使用説明書を参照してください。

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. [ログ転送設定]を押します。
6. [しない]を押します。
7. [設定]を押します。
8. ログアウトします。

ログを一括消去する

本機からログ一括消去を実行するには、ログ収集サーバーを使用しているか、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していることが必要です。

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 2 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。

ログ収集サーバーからログを管理する

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

ユーザー別ホームを設定する

ユーザー別ホームの使用を許可します。

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. [終了] を押します。
3. [操作部初期設定] を押します。
4. [操作部機器設定] を押します。
5. [ユーザー別カスタマイズ利用] を押します。
6. [許可する] を押します。
7. 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、再び使用できます。

ユーザー別ホーム使用時の注意事項

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、機器管理者が必要なプログラムを作成してください。
- 管理者が使用を許可したアイコンだけが表示されます。
- 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すると、そのプログラムのアイコンは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すると、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、管理者は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）を確認できません。

ブラウザー機能を設定する

Web ブラウザーを使用する前に

Web ブラウザーとサーバー間の通信は盗聴や、改ざんされたりすることがあるため、事前にサイト証明書を導入し、本機のサイト証明書のチェック機能を有効にすることをお勧めします。事前に証明書が登録されているサイトだけがアクセスできるため、不正なサイトへのアクセスを抑制できます。

特に拡張 JavaScript を使用したデータ送信機能を使用するときは、サイト証明書のチェック機能を有効にすることをお勧めします。

サイト証明書のチェック機能を有効にするには、本機の SSL を有効にしてサイト証明書を導入します。

SSL の設定について詳しくは、P.121「SSL/TLS を設定する」を参照してください。サイト証明書を導入する方法は、P.149「IEEE 802.1X 認証を設定する」を参照してください。サイト証明書のチェック機能の設定は、Web Image Monitor から設定します。Web Image Monitor のヘルプもあわせて参照してください。

サイト証明書のチェック機能無効時は、信頼されていないサイトに接続すると警告メッセージが表示されることがあります。このときは、接続先のサイトにセキュリティーの問題があるので、本機の管理者は、P.223「こんなときには」を参照のうえユーザーに適切な処置をするよう指導してください。

また、メッセージが表示されないときも、情報漏えいや改ざんが心配なときは、不正なサイトに接続しないよう証明書や接続先の URL を確認するなどの注意をしてください。

信頼されていないサイトとは

信頼されていないサイトとは、以下の条件を一つでも満たすサイトです。

- 証明書が発行されていない
- 証明書の発行元が不明である
- 証明書の有効期限が切れている

こんなときには

接続先のサイトにセキュリティーの問題があるときはメッセージが表示されることがあります。本機の管理者は確認してユーザーに適切な処置をするよう指導してください。

メッセージ

- このサイトのセキュリティーには問題があります。証明書の期限が切れています。
- このサイトのセキュリティーには問題があります。検証するルート証明書が存在しません。

- このサイトのセキュリティーには問題があります。接続先のサーバー証明書との検証がとれません。
- このサイトのセキュリティーには問題があります。https サイトに http サイトのサブコンテンツが含まれています。*1

*1 接続先のサイトに暗号化されていないコンテンツが含まれています。

機器情報を管理する

⚠注意



- SD カード、USB メモリーは、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、USB メモリー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。

本機の機器情報は、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、変更した設定を戻せるのでバックアップとして使用できます。

また、サーバーで機器の設定情報ファイルを管理すると、定期的に機器への設定情報の反映（インポート）ができます。

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
- ブラウザー初期設定
- 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
- 操作部初期設定
- ホーム画面のカスタマイズ内容*1

*1 壁紙にライブ壁紙が選択されているときは壁紙はエクスポートされません。

インポート・エクスポートできないデータ

- システム初期設定の一部の項目*2 *3

*2 年月日の設定、機器証明書を使用する設定、画像の補正値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。

*3 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。

- 拡張機能初期設定
- 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）
- telnet から設定する設定
- RICOH @Remote 関連の情報
- 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）

サーバーで機器の設定情報を管理するとき

機器管理サーバーまたは Web サーバーを使用します。

機器管理サーバーを使用するときは、機器管理サーバーの使用説明書を参照してください。Web サーバーを使用するときは、専用アプリケーションで作成した設定情報の csv ファイルを開いて「ModuleID」の下の行を「-」に修正してから Web サーバーに格納します。

補足

- エクスポートされるファイル形式は、CSV 形式です。
- 機種が同一なときだけ、インポート/エクスポートができます。
- 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。
- 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インポート・エクスポートできません。
- インポート・エクスポート中は、本機の操作はできません。
- SD カードの取り扱いについて詳しくは、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。
- インポート、エクスポート、サーバーの設定は Web Image Monitor からもできます。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. **操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。**
2. **[システム初期設定] を押します。**

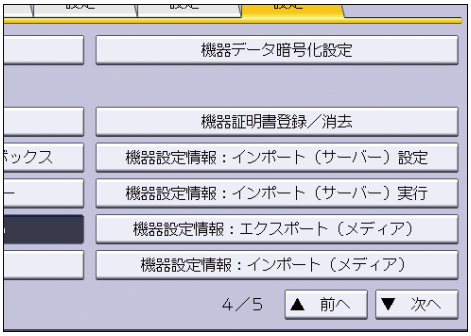
3. SD カードを操作部側面のメディアスロットに挿入します。

   SD カードの装着方法は、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。

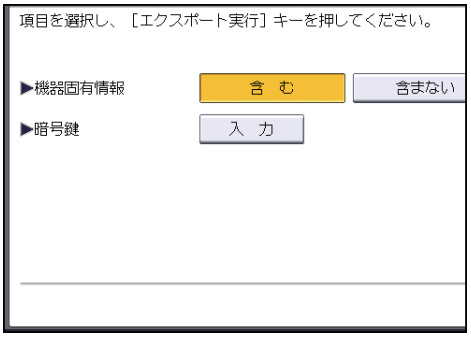
4. [管理者用設定] を押します。

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。



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

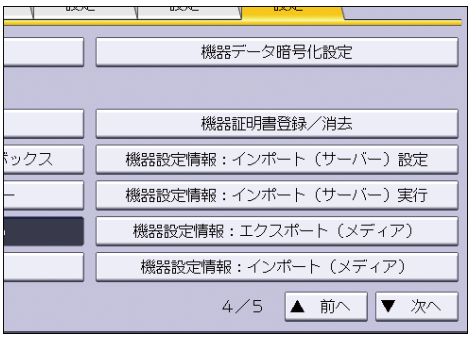
- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。

機器情報をインポートする

SD カードに保存された機器情報をインポートします。

1. **操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。**
2. **[システム初期設定] を押します。**
3. **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。**

   SD カードの装着方法は、『本機をお使いになる方へ』「外部メディアを取り付ける/取り外す」を参照してください。
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。**



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

機器情報を定期的にインポートする

集中管理指示ファイルを作成して、サーバーに格納された機器情報を自動で本機にインポートできるように設定します。本機に複数の設定情報ファイルをインポートすることができます。

集中管理指示ファイルのフォーマットファイルを本機からダウンロードできます。Web ブラウザーで「http://（本機の IP アドレス、またはホスト名）/DH/directionsFormat.ini」をダウンロードしてください。

以下のように集中管理指示ファイルを作成し、Web サーバーに格納してください。

集中管理指示ファイルの例

```
########################################
# <<< Format >>>
#
#   [section]
#   name=value
#
#
# <<< Directions >>>
#
#   name : must NOT change.
#   value :
#             url=enter URL
#             kind=choose from options       : [exportFile] or [logoImgFile]
#             type=choose from options       : [forSameModel] or [forAllModels]
#             doSetup=choose from options              : [yes] or [no]
#
########################################

# AAAの設定情報ファイル
[file1]
url=http://XXXX
kind=exportFile
type=forSameModel
doSetup=yes

# BBBの設定情報ファイル
[file2]
url=http://XXXX
kind=exportFile
type=forSameModel
doSetup=no

[file8]
url=http://XXXX
kind=exportFile
type=forSameModel
doSetup=yes

##### end of file
```

DLA003

集中管理指示ファイルの記載項目

設定情報ファイルに関する情報を記載します。

- セクション

  設定情報ファイルごとに[file1]、[file2]、[file3]…の形式で記載します。記載できるセクションの最大数は 8 です。8 を超えて記載されたセクションは無視されます。

- 設定項目

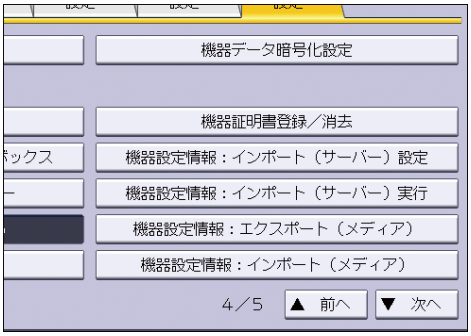
  設定情報ファイルごとに設定します。“=”の前が項目名、“=”の後が設定値となります。項目名は変更しないでください。

項目名	設定
url	設定情報ファイルの URL を記載します。最大文字数は 255 文字です。
kind	本機では「exportFile」と記載します。「logoImgFile」は本機で使用できないデータです。
type	「forSameModel」と記載します。「forAllModels」は機器管理サーバー用の設定です。
doSetup	対象の設定情報ファイルをインポートするときは「yes」、インポートしないときは「no」と記載します。

- コメント

  行の先頭に「#」（半角）を記載すると、その行はコメントとして扱われ、インポート処理の内容に影響しません。

1. **操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。**
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. **[機器設定情報：インポート（サーバー）設定]を押します。**



6. [機器管理サーバー] または [Web サーバー] を選択します。

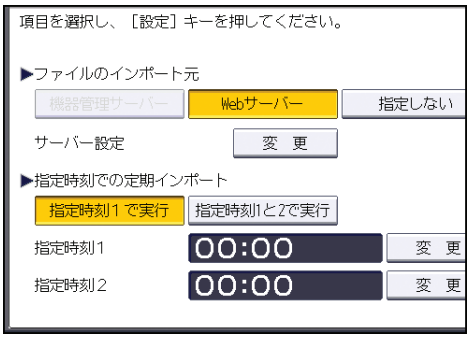
[機器管理サーバー] は本機からは選択できないので、機器管理サーバー側で有効にします。

7. 「サーバー設定」の [変更] または [サーバー設定] を押します。

サーバーの URL、ログインユーザー名、パスワードを設定します。またインポート失敗時の再試行回数、再試行間隔を設定します。

8. [設定] を押します。

9. インポート条件を設定します。



- 指定時刻での定期インポート

  設定情報ファイルをインポートする頻度を選択し、時刻を設定します。

- 前回のインポートファイルとの比較

  前回のインポートしたファイルと比較し、設定情報ファイルが同じとき、インポートするか、しないかを選択します。

- 暗号鍵

  暗号鍵を設定します。

- メール通知

  インポートに失敗したとき、機器管理者にメールを通知するか、しないかを選択します。メール通知をするには Web Image Monitor で「自動メール通知」の設定が必要です。詳細は Web Image Monitor のヘルプを参照してください。

10. [設定] を押します。

11. ログアウトします。

補足

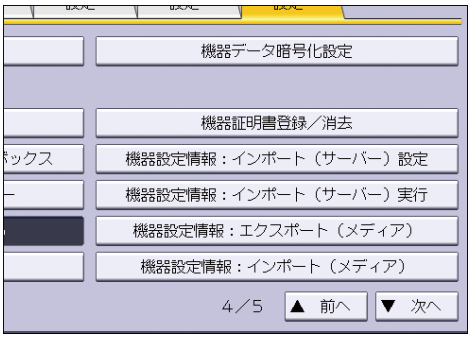
- Web Image Monitor からも設定できます。詳しくは、Web Image Monitor のヘルプを参照してください。
- 機器管理サーバーを使用すると、より詳細なインポート設定ができます。詳しくは、機器管理サーバーの使用説明書を参照してください。

- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。
- 複数の設定情報ファイルをインポートするときは、集中管理指示ファイルに記載された順にインポートされます。一つの設定情報ファイルのインポートに失敗したときは、次の設定情報ファイルのインポート処理に進みます。
- 集中管理指示ファイルおよび設定情報ファイルを格納したサーバーへのアクセスには、「サーバー設定」で指定したユーザー名・パスワードが使用されます。別のユーザー名やパスワードが必要なサーバーにはアクセスできません。
- 暗号化された設定情報ファイルをインポートするときは、[機器設定情報：インポート（サーバー）設定]で指定した暗号鍵が使用されます。別の暗号鍵で暗号化された設定情報ファイルはインポートできません。

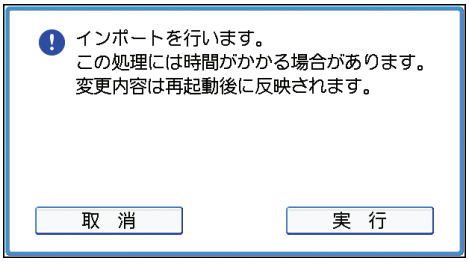
サーバーの設定情報ファイルを手動でインポートする

[機器設定情報：インポート（サーバー）設定]で指定された設定情報ファイルを手動で本機にインポートします。

1. **操作部からユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者がログインします。**
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. **[機器設定情報：インポート（サーバー）実行]を押します。**



6. [実行] を押します。



7. [確認] を押します。

本機が再起動されます。

補足

- 前回のインポートファイルとの比較はしないで常にインポートされます。
- インポート失敗時のメール通知はありません。
- インポート・エクスポートに失敗したときは、ログでエラーの内容を確認できます。ログはエクスポートされた設定情報ファイルと同じ場所に格納されます。

こんなときには

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

ログファイルの例

```
"1.0.0"
"ExecType", "Date", "SerialNo",PnP", "Model", "Destination","IP","Host","Storage","FileNam
e","FileID","TotalItem","NumOfOkItem","ResultCode","ResultName","Identifier"
"IMPORT"
"20XX-07-05T15:29:16+09:00"
"3C35-7M0014"
"Brand Name"
"Product Name"
"0"
"10"
"10.250.155.125"
"RNP00267332582D"
"SD"
"20XX07051519563C35-710220.csv"
"20XX07051519563C35-710220"
"    0"
"  2"
"      REQUEST"
"TargetID","ModuleID","PrefID","Item","NgCode","NgName"
```

CJD023

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

ResultCode	原因	対処方法
2 (INVALID REQUEST)	異なる機種のファイルでインポートを実行しました。	同一の機種でエクスポートしたファイルをインポートしてください。
4 (INVALID OUTPUT DIR)	出力先に機器情報を書き込めません。	出力先が正常に動作しているか確認してください。
7 (MODULE ERROR)	インポート・エクスポート処理時に予期せぬエラーが発生しました。	主電源を入れ直して再度、実行してください。それでも同じエラーが発生するときは、サービス実施店に問い合わせてください。
8 (DISK FULL)	外部メディアの保存領域が不足しています。	十分な空き容量を確保してから実行してください。
9 (DEVICE ERROR)	ログファイルの書き込み、読み込みに失敗しました。	保存先・格納先のパスが存在することを確認してください。
10 (LOG ERROR)	ログファイルの書き込みに失敗しました。HDD が故障しています。	サービス実施店に問い合わせてください。
20 (PART FAILED)	一部の設定項目の設定値をインポートできませんでした。	失敗した理由が NgName に記録されます。内容を確認してください。 **失敗理由(NgName)** 2 INVALID VALUE 設定値が項目の許容範囲外 3 PERMISSION ERROR 項目の編集権限がない 4 NOT EXIST 項目がシステムに存在しない 5 INTERLOCK ERROR システムの状態またはほかの設定値との連動により項目の変更ができない 6 OTHER ERROR その他の理由により、項目の変更ができない
21 (INVALID FILE)	メディアに保存されているデータが正しくないため、データがインポートできません。	適切なデータが使用されているか確認してください。データのフォーマットは CSV 形式です。
22 (INVALID KEY)	暗号鍵が不正です。	正しい暗号鍵を使用してください。

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、カラー印刷や両面印刷、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。eco 指数が高いほど省資源化につながります。

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。**

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

ユーザーがログインしたときに通知するメッセージを選択します。

[固定メッセージ 1] または [固定メッセージ 2] 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 1
- 固定メッセージ 2
- 任意メッセージ

工場出荷時の設定：**固定メッセージ 1**

インフォメーション画面表示

ユーザーがログインしたときにインフォメーション画面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画面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。

ユーザーの eco 指数カウンターをクリアする

ユーザー別 eco 指数カウンターをクリアすると、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。

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。

アドレス帳を管理する

アドレス帳の自動消去を設定する

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

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

［しない］のときは、古いユーザーが消去されないため、新しいユーザーも追加されません。

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. ［アドレス帳ユーザー自動消去］を押します。
5. ［する］を選択し、［設定］を押します。
6. ログアウトします。

補足

- 自動で消去されるのは、自動登録の要求があったときだけです。手動でユーザーを追加するときは、先に古いユーザーを消去してください。
- 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が入力されているユーザーが自動消去の対象です。

アドレス帳の一括消去

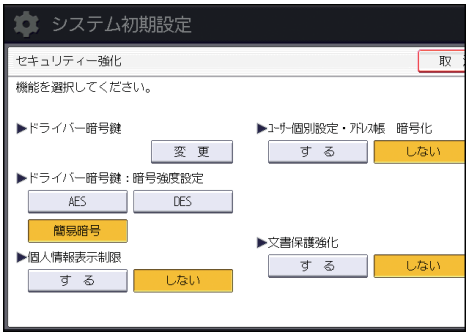
アドレス帳の登録情報をすべて消去できます。

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. ［アドレス帳データー括消去］を押します。
5. ［消去する］を押し、［確認］を押します。
6. ログアウトします。

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使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し、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。

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。

［DES］に設定したときは、DES、または 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場合に、Web Image Monitor から SNMP を使ってジョブ履歴を確認するときは、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と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の読み取りを防止します。

設定方法は、P.87「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。

文書保護強化が設定されていると、画面左下にが表示されます。

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します。

- 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。ユーザーは送信時に相手先を直接入力できません。

「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.67「宛先表の使用を制限する」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）」またはその両方が［しない］の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、［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］でアドレス帳に登録できません。

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、ユーザー管理者だけが変更できます。

- 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、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、以下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。

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と機器管理者が操作できます。[ログイン権限]の設定が有効で、すでにユーザーが本機にログイン中のときは認証を要求されません。

[アクセス権限]に設定するとコピーや印刷をしたユーザーと機器管理者が操作できます。

[ログイン権限]に設定し、ユーザーが本機にログインできるときでも、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、コピーの中断とプリンターのジョブキャンセルはできません。

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

- ログイン権限
- アクセス権限
- しない

工場出荷時の設定：**しない**

@Remote サービス

機器管理者が設定します。

[禁止する]に設定すると、RICOH @Remote サービスのための HTTPS 通信を停止できます。[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。

[一部禁止する]に設定すると、リモート接続での設定変更などができなくなり、セキュアな運用に最適です。

- 禁止する
- 禁止しない
- 一部禁止する

工場出荷時の設定：**禁止しない**

ファームウェアアップデート

機器管理者が設定します。

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

[禁止する]を選択すると、ファームウェアアップデートを実行できません。

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

- 禁止する
- 禁止しない

工場出荷時の設定：**禁止しない**

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ことが必要です。

［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設定が変更されることがあります。［禁止する］に設定すると、SNMPv1、v2 を使った設定はできません。確認だけできます。

- 禁止する
- 禁止しない

工場出荷時の設定：**禁止しない**

アクセスセキュリティー設定

機器管理者が設定します。

ネットワーク接続を使用したアプリケーションで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いことがあります。

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

    「50-200」件の範囲でテンキーで入力し、[#]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ー設定」で管理できるパスワード情報の管理件数を設定します。

    「50-200」件の範囲でテンキーで入力し、[#]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」秒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**

パスワード攻撃検知

機器管理者が設定します。

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

許容回数を「0」に設定したときは、パスワード攻撃を検知しません。

- 許容回数

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

  「0-100」回の範囲でテンキーで入力し、[#]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」秒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。操作部と Web Image Monitor にメッセージが表示されます。

許容回数を「0」に設定したときは、アクセス攻撃を検知しません。

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

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

- 許容回数

  過剰なアクセス回数をアクセス攻撃として検知しない最大許容回数を設定します。

  「0-500」回の範囲でテンキーで入力し、[#]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。

  測定時間を超えると累積されたアクセス回数はクリアされます。

  「10-30」秒の範囲でテンキーで入力し、[#]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、ログイン要求への応答を遅らせる時間を設定します。

  「0-9」秒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」件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。
- メールの受信が頻繁に発生するときは、内容を確認し、設定値を見直してください。

その他のセキュリティー機能

情報漏えい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」と「ビット番号 5」を設定すると、相手先と送信者名の表示・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えいを防止できます。

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止するため、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で出力します。
- ［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、通信管理情報をメールで送信する設定に変更します。

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。

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が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」をしてください。

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。

WSD スキャナー機能

ユーザー認証を設定したとき、WSD スキャナー機能は自動的に無効になります。自動的に無効になったあとでも、Web Image Monitor から「導入設定」で有効に設定できます。

設定方法は、『スキャナー』「WSD スキャナー（Push 型）を使用するための準備」「WSD スキャナー（Pull 型）を使用するための準備」を参照してください。

システム状態

操作部の［状態確認］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］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 は使用できないので、操作部の表示を確認してください。

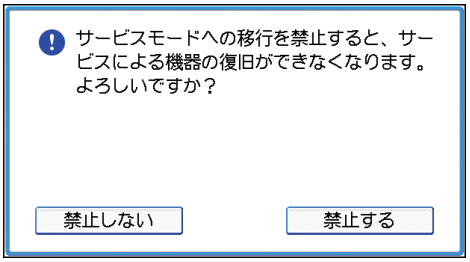
検証エラーが表示されたときは、サービス実施店に連絡してください。

カスタマーエンジニアの操作を制限する

カスタマーエンジニアによるサービスモードの操作を制限できます。

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

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使用するための、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、以下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 詳しくは、P.60「オートログアウト時間設定」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.32「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.13「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.13「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→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.13「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.13「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.239「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。

タブ項目	設定項目	設定値
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.239「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.239「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.239「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.111「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。
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.251「カスタマーエンジニアの操作を制限する」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] を選択し、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.89「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.70「メニュープロテクトを設定する」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.248「その他のセキュリティー機能」を参照してください。

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.70「メニュープロテクトを設定する」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。

Web Image Monitor 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、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。

機器の管理→設定

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］
セキュリティー→ユーザーロックアウト	ロックアウト	［有効］ 詳しくは、P.58「ロックアウト機能」を参照してください。
セキュリティー→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.58「ロックアウト機能」を参照してください。
セキュリティー→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.58「ロックアウト機能」を参照してください。
セキュリティー→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.58「ロックアウト機能」を参照してください。

カテゴリー	設定項目	設定値
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ごとに非常に頻繁に行われるため、「ログイン」ログは記録されないのでご注意ください。
セキュリティー→ネットワークセキュリティー	FTP	[無効] 操作部でネットワークセキュリティーレベルを［レベル 2］にしてから設定します。
セキュリティー	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 を使用するときは、ユーザー証明書の登録が必要です。

機器の管理

カテゴリー	設定項目	設定値
アドレス帳→詳細入力→ユーザー追加・変更→メール	ユーザー証明書	S/MIME を使用するには、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。
- 暗号化アルゴリズムの設定とユーザー証明書の登録方法は、P.126「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 を使用すると、IPsec を設定し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 が使用できるときは、より安全なネットワーク通信のために、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 が使用できるときは、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

機器の管理→設定

カテゴリー	設定項目	設定値
セキュリティー→IPsec→自動鍵交換設定	編集→セキュリティーレベル	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 が使用できないときは、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 と SSL/TLS 通信許可設定は、Web Image Monitor からも設定できます。

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。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.121「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、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』「インターフェース設定」を参照してください。
- Web Image Monitor による IPsec の設定は、P.133「IPsec を設定する」を参照してください。

8. こんなときには

本機がうまく操作ができないときの対処方法を説明します。

メッセージが表示されたとき

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

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

この機能を利用する権限はありません。

機能を使用する権限が設定されていません。

- 各機能を使用しようとして表示されたとき
  - アドレス帳の認証情報で、機能を使用できるように設定されていません。
  - 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
  - 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。
  - 設定項目一覧表を基に、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.260「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.13「管理者認証を設定する」を参照してください。

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

削除する権限のない文書を削除しようとしました。

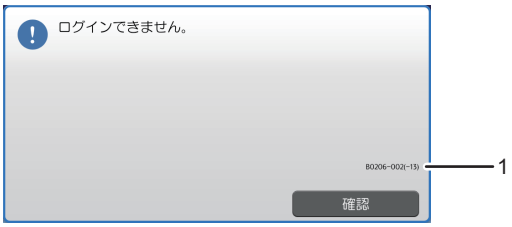
- オーナー、または文書管理者が削除できます。削除する権限のない文書を削除するときは、オーナーに確認してください。

補足

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

エラーコードが表示されたとき

認証機能設定時にエラーメッセージが表示されたとき、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、エラーコードを控えて、サービス実施店に連絡してください。



DLA002

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

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 操作をしました。

- 機器にほか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 操作をしてください。

B0104-000

パスワード復号処理に失敗しました。

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

B0105-000

Ridoc Desk Navigator のログインユーザー名を未設定のまま、Ridoc Desk Navigator からの操作が実行されました。

- Ridoc Desk Navigator のログインユーザー名を正しく設定してください。

B0206-002：ケース 1

ログインユーザー名かパスワードに誤りがあります。

- ログインユーザー名とパスワードを正しく入力してログインしてください。

B0206-002：ケース 2

アプリケーション別個人認証機能を使用している環境で、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ました。

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

B0206-003

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

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

B0207-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

B0208-000 / B0208-002

認証に失敗した回数が、設定値を超えたため、アカウントがロックされました。

- アカウントを確認し、ロックを解除してください。

B09XX-019

集中管理設定を使用してクライアント機で認証したときに、サーバー機へのユーザー自動登録に失敗しました。

- クライアント機とサーバー機とのネットワーク通信を確認してください。
- サーバー機のアドレス帳が編集中のときは登録できません。

Windows 認証時のエラーコード

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 操作をしました。

- 機器にほか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 操作をしてください。

W0104-000

パスワード復号処理に失敗しました。

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

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

W0105-000

Ridoc Desk Navigator のログインユーザー名を未設定のまま、Ridoc Desk Navigator からの操作が実行されました。

- Ridoc Desk Navigator のログインユーザー名を正しく設定してください。

W0206-002

アプリケーション別個人認証機能を使用している環境で、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。

W0206-003

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

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

W0207-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

W0208-000 / W0208-002

認証に失敗した回数が、設定値を超えたため、アカウントがロックされました。

- アカウントを確認し、ロックを解除してください。

W0400-102

サーバーが動作していないため、Kerberos 認証に失敗しました。

- サーバーが動作しているか確認してください。

W0400-200

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：ケース 1

認証サーバーと機器の SSL 設定が合っていません。

- 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。

W0400-202：ケース 2

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：ケース 1

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

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

W0406-107：ケース 2

ユーザーグループが取得できるように設定されていません。

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

W0406-107：ケース 3

ドメイン名の名前解決ができていません。

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

W0406-107：ケース 4

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」で接続確認ができます。
- ほかの PC からも認証できるか確認してください。

W0406-107：ケース 5

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。

W0406-107：ケース 6

ドメイン名に誤りがあります。

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

W0406-107：ケース 7

ドメイン名の名前解決ができません。

- ドメイン名に IP アドレスを設定して、認証に成功するか確認してください。

  ＜成功するとき＞

  - 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。
  - ドメイン名に NetBIOS ドメイン名（DOMAINNAME）を指定するとき、「インターフェース設定」の WINS を設定しているか確認してください。

  ＜失敗するとき＞

  - 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。
  - 機器からドメインコントローラの接続経路のファイアウォール、またはドメインコントローラのファイアウォール設定などでポートをクローズしていないか確認してください。

- Windows ファイアウォールを有効にしているときは、Windows ファイアウォールの「詳細設定」で、137 番と 139 番のポートを許可する新しい規則を作成します。
- 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：ケース 8

Kerberos 認証に失敗しています。

- Kerberos 設定が正しく設定されていません。

レルム名、KDC（キー配布センター）名、対応ドメイン名を正しく設定しているか確認してください。

- KDC（キー配布センター）と機器の時刻が合っていません。

  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。

- レルム名を小文字で設定しているとき、Kerberos 認証に失敗します。

  レルム名が小文字になっていないか確認してください。

- KDC（キー配布センター）の自動取得に失敗するとき、Kerberos 認証に失敗します。

  KDC（キー配布センター）取得設定が自動取得になっているかサービス実施店に確認を依頼してください。

  自動取得が上手く動作しないときは、手動設定に切り替えて使用してください。

W0409-000

認証サーバーからの応答が返らないため、認証タイムアウトが発生しました。

- ネットワーク環境と認証に使用するサーバーを確認してください。

W0511-000 / W0517-000

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あとであるときは、古いサーバー側のユーザーを削除してください。

W0606-004

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

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

W0607-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

W0612-005

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

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

W0707-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

W09XX-019

集中管理設定を使用してクライアント機で認証したときに、サーバー機へのユーザー自動登録に失敗しました。

- クライアント機とサーバー機とのネットワーク通信を確認してください。
- サーバー機のアドレス帳が編集中のときは登録できません。

LDAP 認証時のエラーコード

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 操作をしました。

- 機器にほか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 操作をしてください。

L0104-000

パスワード復号処理に失敗しました。

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

L0105-000

Ridoc Desk Navigator のログインユーザー名を未設定のまま、Ridoc Desk Navigator からの操作が実行されました。

- Ridoc Desk Navigator のログインユーザー名を正しく設定してください。

L0206-002

アプリケーション別個人認証機能を使用している環境で、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。

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。

L0307-001

アドレス帳が使用中の状態のため、認証に失敗しました。

- しばらく経ってから操作してください。

L0400-210

LDAP 検索結果を表示・記録するコードです。

- 検索条件となるログイン名属性が設定されていないか、情報が取得できない属性が指定されていることがあります。

  LDAP 認証の設定でログイン名属性が正しく設定されているか確認してください。

L0406-003

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

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

L0406-200

同時に大量の認証が発生しているためログインできません。

- 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。

L0406-202 / L0406-203：ケース 1

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

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

  これに成功しないときは、ネットワーク設定に誤りがあることがあります。

  インターフェース設定のドメイン名や DNS 設定を確認してください。
- LDAP 認証設定で LDAP サーバーが正しく選択されていることを確認してください。
- LDAP 認証設定でログイン名属性が正しく入力されていることを確認してください。
- SSL 設定が LDAP サーバーでサポートされているか確認してください。

L0406-202 / L0406-203：ケース 2

ログインユーザー名かパスワードに誤りがあります。

- ログインユーザー名とパスワードが正しく入力されているか確認してください。
- 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。

  以下に当てはまるときは、認証に失敗します。
  - スペース、「:」、「"」の禁則文字を使用しています。
  - ログインユーザー名が 128 バイトを超えています。

L0406-202 / L0406-203：ケース 3

簡易認証モードの使用方法に誤りがあります。

- 簡易認証モードでは空パスワードでは認証に失敗します。

  空パスワードを許可するときは、サービス実施店に連絡してください。
- 簡易認証モードでは代表者アカウントでログインユーザー名の DN を取得します。この取得に失敗したときも認証に失敗します。

  サーバー名、ログインユーザー名／パスワードや検索フィルターの入力情報に誤りがないか確認してください。

L0406-204

Kerberos 認証で失敗しました。

- Kerberos 設定が正しく設定されていません。

  レルム名、KDC（キー配布センター）名、対応ドメイン名を正しく設定しているか確認してください。
- KDC（キー配布センター）と機器の時刻が合っていません。

  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。
- レルム名を小文字で設定しているとき、Kerberos 認証に失敗します。

  レルム名が小文字になっていないか確認してください。

L0409-000

認証サーバーからの応答が返らないため、認証タイムアウトが発生しました。

- ネットワーク環境と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。

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。

L09XX-019

集中管理設定を使用してクライアント機で認証したときに、サーバー機へのユーザー自動登録に失敗しました。

- クライアント機とサーバー機とのネットワーク通信を確認してください。
- サーバー機のアドレス帳が編集中のときは登録できません。

IC カード認証時のエラーコード

*0150-401

PIN ロックされたカードが IC カード R/W 上に置かれました。

- カードの PIN ロックを解除してください。

*0151-401

PIN に誤りがあります。

- PIN を正しく入力してログインをしてください。

*0153-402

IC カード R/W が外れているか、正しく接続されていません。または IC カードに問題があります。

- IC カード R/W の接続を確認してください。解決しないときはほかのカードを使用して認証をしてください。
- それでも解決しないときは、サービス実施店にお問い合わせください。

*0154-402

カードの読み取りに失敗しました。

- IC カード R/W 上にカードを正しくセットし、カードを置く時間を長くしてください。解決しないときは、ほかのカードを使用して認証を実行してください。
- それでも解決しないときはサービス実施店にお問い合わせください。

*0156-401

ユーザー名/パスワードの入力が正しくありません。

- 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を実行してください。

操作ができないとき

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

状態	原因	対処方法
プリンタードライバーから印刷できない。 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。	ユーザー認証が拒否されました。	プリンタードライバーにログインユーザー名とログインパスワードを入力してください。 Windows 認証と LDAP 認証を使用しているときは、使用しているネットワークの管理者にログインユーザー名とログインパスワードを確認してください。ベーシック認証のときは、ユーザー管理者に確認してください。
	ドライバーで暗号化を設定しているときに、ドライバー暗号鍵が本機と一致しませんでした。	本機に登録されているドライバー暗号鍵をドライバーに正しく設定してください。 詳しくは、P.156「ドライバー暗号鍵を設定する」を参照してください。
TWAIN ドライバーで接続できない。	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ませんでした。	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。
TWAIN ドライバーで認証ができない。	本機でほかにログインしているユーザーがいます。	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。
TWAIN ドライバーで認証ができない。	装置側の都合により、認証に時間がかかっています。	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。
TWAIN ドライバーで認証ができない。	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。	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。

状態	原因	対処方法
Ridoc IO Device Manager の「アドレス帳」を操作するとき、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。 Ridoc Desk Navigator から［ドキュメントボックス（認証／暗号）］でログインできない。	「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ません。	「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。 「ドライバー暗号鍵：暗号強度設定」の設定は P.239「セキュリティー強化機能を設定する」、SSL/TLS の設定は P.121「SSL/TLS を設定する」を参照してください。
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。	原稿の読み取りが終了していません。	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。
スキャナーの宛先指定画面に［宛先登録］が表示されない。	「セキュリティー強化」の「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できません。	ユーザー管理者が登録をしてください。

状態	原因	対処方法
スキャナーのメール送信ができない。 (類似状態) • 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。	以下の原因が考えられます。 • 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。	• 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、事前に準備が必要です。 • 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.116「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
ファクス文書の転送ができない。 (類似状態) • あて先が選択できない。 • 署名が設定できない。	以下の原因が考えられます。 • 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。	• 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、事前に準備が必要です。 • 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.116「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。
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ました。	ユーザー認証の設定を再び有効にし、表示されていない文書に [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.164「蓄積文書を管理する」を参照してください。
ユーザー認証を無効にしているのに本機で設定したアドレス帳の宛先が表示されない。	[すべてのユーザー] が設定されていない状態で、ユーザー認証の設定を無効にしました。	ユーザー認証の設定を再び有効にし、表示されていない宛先に [すべてのユーザー] の設定を有効にしてください。 詳しくは、P.85「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ません。	プリンタードライバーにユーザー認証の設定をしてください。 プリンタードライバーのヘルプを参照してください。

状態	原因	対処方法
「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することがあります。	ジョブがキャンセルされたユーザーの利用量カウンターをクリアするなどし、印刷利用量制限の設定を変更してください。利用量カウンターをクリアする方法は、P.75「ユーザーの印刷利用量を制限する」を参照してください。
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できます。 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待つか、ジョブを実行したユーザーに確認してください。 機器管理者は、ジョブを取り消せます。
ユーザー個別設定・アドレス帳の暗号化を実行し、しばらく待ったが終了が表示されない。	アドレス帳の件数が多く暗号化に時間がかかっています。 または、ファイルまたは、ハードディスクが破損しています。	P.89「機器のデータを暗号化する」の［ファイルシステムデータのみ］の所要時間を過ぎても画面が更新されないときは、サービス実施店に連絡してください。

9. 設定項目の操作権限一覧

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

表の見方

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。

ー：実行、変更、閲覧ができません。

システム初期設定

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。

[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
[用紙枚数カウンター表示]	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
[割り込み印刷優先機能設定]	R	R/W	R	R	R/W	R
[印刷機能移行時間]	R	R/W	R	R	R/W	R
[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
[キーリピート設定]	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
[ADF 底板上昇設定]	R	R/W	R	R	R/W	R
[外付けキーボード]	R	R/W	R	R	R/W	R
[Compatible ID]	R	R/W	R	R	R/W	R
[USB デバイスリスト登録/変更]	R	R/W	R	R	R/W	R
[針なしステープル位置画像消去]	R	R/W	R	R	R/W	R
[針なしステープルとじ方式]	R	R/W	R	R	R/W	R
[人体検知センサー]	R	R/W	R	R	R/W	R
[針なし／針ありステープル自動切り替え]	R	R/W	R	R	R/W	R
[フィニッシャー排紙時出力優先設定]	R	R/W	R	R	R/W	R
[ビジネスアプリケーション向け省エネ復帰設定]	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

設定項目	User	機器	N/W	文書	なし	あり
[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 1～4]	R	R/W	R	R	R/W	R
[用紙サイズ設定：大量給紙トレイ]	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 1～4]	R	R/W	R	R	R/W	R
[用紙種類設定：大量給紙トレイ]	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
[自動検知:Legal/Oficio サイズ切替]	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
[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
[定着部オフモード（省エネ）移行設定]	R	R/W	R	R	R/W	R
[ウィークリータイマー詳細設定]	R	R/W	R	R	R/W	R
[ウィークリータイマー簡単設定]	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

設定項目	User	機器	N/W	文書	なし	あり
[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
[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
[SMB コンピューター名]	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 IEEE 802.1X 認証]	R	R	R/W	R	R/W	R
[IEEE 802.1X 認証初期化]	–	–	R/W	–	R/W	–

*1 自動取得するに設定したときは、閲覧だけできます。

*2 接続テストはすべての管理者と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
[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

設定項目	User	機器	N/W	文書	なし	あり
[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
[セキュリティー方式選択]	R	R	R/W	R	R/W	R
[無線 LAN：簡単／ダイレクト接続]	ー	ー	R/W	ー	R/W	ー
[ダイレクト接続設定]	ー	ー	R/W	ー	R/W	ー
[電波状態]	R	R	R	R	R	R
[設定値初期化]	ー	ー	R/W	ー	R/W	ー

[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]	ー	ー	R/W	ー	R/W	ー

[ファイル転送設定]

設定項目	User	機器	N/W	文書	なし	あり
[文書管理サーバー IPv4 アドレス]	R	R/W	R	R	R/W	R
[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
[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

設定項目	User	機器	N/W	文書	なし	あり
[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 *4	R/W *4	R/W *4	R/W *5	R *5
[グループ登録／変更／消去]	R/W	R/W *4	R/W *4	R/W *4	R/W *5	R *5
[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	–
[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
[アドレス帳ユーザー自動消去]	R/W	–	–	–	R/W	–
[アドレス帳データー括消去]	R/W	–	–	–	R/W	–
[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 *6	R/W *7	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	–	–	–	–
[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
[上限到達時動作設定]	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
[拡張印刷利用量制限]	R	R/W	R	R	R	R
[印刷利用量上限初期値]	R/W	R	R	R	R	R

設定項目	User	機器	N/W	文書	なし	あり
[メディアスロット使用]	R	R/W	R	R	R	R
[ユーザー認証管理]	R	R/W	R	R	R/W	R
[拡張認証管理]	R	R/W	R	R	R/W	R
[管理者認証管理]	R/W *8*9	R/W *9	R/W *9	R/W *9	R/W	–
[管理者登録／変更]	R/W *10	R/W *10	R/W *10	R/W *10	–	–
[キーカウンター管理]	R	R/W	R	R	R/W	R
[外部課金装置管理]	R	R/W	R	R	R/W	R
[拡張外部課金装置管理]	R	R/W	R	R	R/W	R
[セキュリティー強化]						
• [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
• [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
• [@Remote サービス]	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
• [アクセスセキュリティー設定]	R	R/W	R	R	–	–
• [パスワード攻撃検知]	–	R/W	–	–	–	–
• [アクセス攻撃検知]	–	R/W	–	–	–	–
[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

設定項目	User	機器	N/W	文書	なし	あり
[ドキュメントボックス蓄積文書一括消去]	ー	ー	ー	R/W	R/W	ー
[文書管理：送信待ち文書一括消去]	ー	R/W	ー	ー	R/W	ー
[LDAP サーバー登録／変更／消去] *3	ー	R/W	ー	ー	R/W	R
[LDAP 検索]	R	R/W	R	R	R/W	R
[通信テストコール実行]	ー	R/W	ー	ー	R/W	ー
[機器情報通知実行]	ー	R/W	ー	ー	R/W	ー
[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
[メモリー自動消去設定]	R	R/W	R	R	R	R
[メモリー全消去]	ー	R/W	ー	ー	ー	ー
[ログ一括消去]	ー	R/W	ー	ー	R/W	ー
[ログ転送設定] *11	R	R/W	R	R	R/W	R
[不正コピーガード検知]	R	R/W	R	R	R/W	R
[不正コピー抑止印刷：コピー]	R	R/W	R	R	R/W	R
[不正コピー抑止印刷：ドキュメントボックス]	R	R/W	R	R	R/W	R
[不正コピー抑止印刷：プリンター]	R	R/W	R	R	R/W	R
[USB ポート固定]	R	R/W	R	R	R/W	R
[レルム登録／変更／消去]	ー	R/W	ー	ー	R/W	R
[機器データ暗号化設定]	ー	R/W	ー	ー	ー	ー
[連携先機器登録／変更／消去]	ー	R/W	ー	ー	R/W	ー
[機器証明書登録／消去]	ー	ー	R/W	ー	ー	ー
[機器設定情報：インポート（サーバー）設定] *12	ー	ー	ー	ー	ー	ー
[機器設定情報：インポート（サーバー）実行] *12	ー	ー	ー	ー	ー	ー
[機器設定情報：エクスポート（メディア)] *12	ー	ー	ー	ー	ー	ー
[機器設定情報：インポート（メディア)] *12	ー	ー	ー	ー	ー	ー
[PDF ファイル形式：PDF/A 固定]	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

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：コピー]	R	R/W	R	R	R/W	R
[強制セキュリティー印字：ドキュメントボックス]	R	R/W	R	R	R/W	R
[強制セキュリティー印字：ファクス]	R	R/W	R	R	R/W	R
[強制セキュリティー印字：プリンター]	R	R/W	R	R	R/W	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
[ログ収集設定]	R	R/W	R	R	R/W	R
[集中管理設定]						
• [集中管理設定]	R	R/W	R	R	R	R
• [クライアント同期設定] *13	R/W	R/W	R	R	R	R
• [サーバーと同期実行] *14	R/W	R/W	R	R	R	R
• [印刷利用量制限] *15	R	R/W	R	R	R	R
• [eco 指数カウンター] *15	R	R/W	R	R	R	R
• [非接続時の利用量制限] *15	R	R/W	R	R	R	R
[ADF 動作設定：コピー/ドキュメントボックス]	R	R/W	R	R	R	R

*3 パスワードは閲覧できません。

*4 見出し切り替えとユーザーの検索ができます。

*5 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。

*6 クリアができます。

*7 印刷ができます。

*8 個人認証機能を使用しているときは変更できません。

*9 権限を持つ管理者項目が変更できます。

*10 管理者が管理者自身のアカウントを変更できます。

*11 [しない] への変更ができます。

*12 ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が R/W になります。

*13 本機をサーバー機にすると表示されます。

*14 本機をクライアント機にすると表示されます。

*15 本機をサーバー機またはクライアント機にすると表示されます。

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
[優先原稿種類]	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
[カラー選択＜2色＞優先選択]	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
[手差し選択時の用紙設定画面表示]	R	R/W	R	R	R	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
[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

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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

[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
[印字色優先設定]	R	R/W	R	R	R	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

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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
[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 印刷位置の調整だけ設定できます。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 *1	R

*1 印刷位置の調整だけ設定できます。印刷位置自体は設定できません。

[ページ印字]

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 *1	R
[印字位置設定:1/5, 2/5・・・]	R	R/W	R	R	R/W *1	R
[印字位置設定:-1-, -2-・・・]	R	R/W	R	R	R/W *1	R
[印字位置設定:P.1, P.2・・・]	R	R/W	R	R	R/W *1	R
[印字位置設定:1, 2・・・]	R	R/W	R	R	R/W *1	R
[印字位置設定:1-1, 1-2・・・]	R	R/W	R	R	R/W *1	R
[印字位置設定:1 ページ, 2 ページ・・・]	R	R/W	R	R	R/W *1	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

*1 印刷位置の調整だけ設定できます。印刷位置自体は設定できません。

[文字印字]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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	R
[ジョブ通番印字の開始番号変更]	R	R/W	R	R	R	R

[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
[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
[針なしステープル種類選択]	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

[カラー画質設定]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[自動濃度の濃度設定（フルカラー・2 色)]	R	R/W	R	R	R/W	R
[カラー幅調整]	R	R/W	R	R	R/W	R
[カラー判定]	R	R/W	R	R	R/W	R
[自動カラー選択時優先画質設定]	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
[リンギング音]	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
[次原稿待機設定：原稿ガラス]	R	R/W	R	R	R/W	R

[送信設定]

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	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（印刷不可時）]	–	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	R/W	R	R	R
[IP ファクス最大送信速度設定]	R	R	R/W	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
[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
[IP ファクス H.323 使用]	R	R	R/W	R	R	R
[IP ファクス SIP 使用]	R	R	R/W	R	R	R

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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
[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	R/W	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］	R	R	R	R	R	R
［文書印刷］	R	R	R	R/W	R/W	R/W
［メディアプリント］	ー	ー	ー	ー	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
［ジョブスプール一覧］	R	R/W	R	R	R	R
［エラー履歴］	ー	R	ー	ー	R	R

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
[メニューリスト]	–	R/W	–	–	R/W	R/W
[登録フォームリスト]	–	R/W	–	–	R/W	R/W
[カラーサンプル]	–	R/W	–	–	R/W	R/W
[全文字印刷]	–	R/W	–	–	R/W	R/W
[フォントリスト]	–	R/W	–	–	R/W	R/W
[PCL 情報リスト]	–	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

[データ操作/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
[4C 描画モード]	R	R/W	R	R	R	R
[トレイ読み替え(PCL)]	R	R/W	R	R	R	R
[トレイ読み替え(PS)]	R	R/W	R	R	R	R
[針なし/針ありステープル表示]	R	R/W	R	R	R	R

[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
[PDL エラージョブ自動取消の確認画面]	R	R/W	R	R	R	R
[エラー発生時のジョブ自動取消]	R	R/W	R	R	R	R
[ジョブ仕分け]	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
[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
[印刷枚数]	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
[グレー印刷方式（グレー認識広め）]	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
[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
[ステープル枚数オーバー動作設定]	R	R/W	R	R	R	R
[中綴じ枚数オーバー動作設定]	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

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[自動排紙時間]	R	R/W	R	R	R	R
[マクロキャッシュ]	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
[線幅補正量]	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

PCL 設定

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[用紙サイズ]	R	R/W	R	R	R/W	R
[最大領域印刷]	R	R/W	R	R	R	R
[両面印刷]	R	R/W	R	R	R	R
[印刷方向]	R	R/W	R	R	R	R
[行数]	R	R/W	R	R	R	R
[フォントソース]	R	R/W	R	R	R	R
[フォント番号]	R	R/W	R	R	R	R
[ポイントサイズ]	R	R/W	R	R	R	R
[フォントピッチ]	R	R/W	R	R	R	R
[シンボルセット]	R	R/W	R	R	R	R
[クーリエフォント]	R	R/W	R	R	R	R
[A4 サイズ最大幅印刷]	R	R/W	R	R	R	R
[LF 設定]	R	R/W	R	R	R	R
[解像度]	R	R/W	R	R	R	R
[トナーセーブ]	R	R/W	R	R	R	R
[白紙排紙]	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
[用紙選択方式]	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
[トナーセーブ]	R	R/W	R	R	R	R
[RGB 補正]	R	R/W	R	R	R	R
[カラープロファイル]	R	R/W	R	R	R	R
[プロセスカラーモデル]	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
[グレー印刷方式]	R	R/W	R	R	R	R

[PDF 設定]

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
[トナーセーブ]	R	R/W	R	R	R	R
[RGB 補正]	R	R/W	R	R	R	R
[カラープロファイル]	R	R/W	R	R	R	R
[プロセスカラーモデル]	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

[XPS 設定]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[両面印刷]	R	R/W	R	R	R	R
[白紙排紙]	R	R/W	R	R	R	R
[解像度]	R	R/W	R	R	R	R
[トナーセーブ]	R	R/W	R	R	R	R
[カラープロファイル]	R	R/W	R	R	R	R
[プロセスカラーモデル]	R	R/W	R	R	R	R
[最大領域印刷]	R	R/W	R	R	R	R
[グレー印刷方式]	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
[PC からの読み取り要求禁止時間]	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	R/W	R	R	R	R
[送信履歴消去]	R	R/W	R	R	R	R
[宛先履歴消去]	R	R/W	R	R	R	R
[WSD／DSM 機能の利用]	R	R/W	R	R	R/W	R
[DSM 以外の宛先表の利用]	R	R/W	R	R	R/W	R
[プログラムへの宛先設定登録]	R	R/W	R	R	R	R
[URL リンクから文書を直接ダウンロード]	R	R/W	R	R	R/W	R
[ログインユーザー宛先優先]	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
[カラー判定]	R	R/W	R	R	R	R
[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
[白紙検知]	R	R/W	R	R	R	R
[変倍率設定]	R	R/W	R	R	R	R
[読み取りサイズ登録／変更／消去]	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
[クリアライト PDF 作成時の圧縮方式]	R	R/W	R	R	R/W	R
[クリアライト PDF 圧縮率設定]	R	R/W	R	R	R/W	R
[OCR テキスト付き PDF 白紙検知レベル]	R	R/W	R	R	R/W	R
[送信メールサイズ制限]	R	R	R/W	R	R	R
[メールサイズ制限オーバー時分割]	R	R	R/W	R	R	R
[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
[デフォルトメール件名]	R	R/W	R	R	R	R
[文書送信方法]	R	R/W	R	R	R/W	R
[URL 送信文書保持時間]	R	R/W	R	R	R/W	R

[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

ブラウザー設定

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
[全般]	ー	R/W	ー	ー	R/W	ー
[プライバシーとセキュリティ]	ー	R/W	ー	ー	R/W	ー
[ユーザー補助]	ー	R/W	ー	ー	R/W	ー
[高度な設定]	ー	R/W	ー	ー	R/W	ー
[帯域幅の管理]	ー	R/W	ー	ー	R/W	ー
[Labs]	ー	R/W	ー	ー	R/W	ー
[PDF プレビュー設定]	ー	R/W	ー	ー	R/W	ー

拡張機能初期設定

拡張機能初期設定

設定項目	User	機器	N/W	文書	なし	あり
[起動設定]	R	R/W	R	R	R	R
[インストール]	R	R/W	R	R	R	R
[アンインストール]	R	R/W	R	R	R	R
[拡張機能情報]	R	R/W	R	R	R	R
[管理者用設定]	ー	R/W	ー	ー	ー	ー
[追加プログラム起動設定]	R	R/W	R	R	R	R
[追加プログラムインストール]	R	R/W	R	R	R	R
[追加プログラムアンインストール]	R	R/W	R	R	R	R
[追加プログラム情報]	R	R/W	R	R	R	R

調整／管理

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。

[調整／管理]

設定項目	User	機器	N/W	文書	なし	あり
[自動階調補正]	−	R/W	−	−	R/W	−
[色ずれ補正]	−	R/W	−	−	R/W	−

操作部初期設定

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

[無線とネットワーク]

設定項目	User	機器	N/W	文書	なし	あり
[インターフェース設定]	–	–	R/W	–	R/W	–
[Wi-Fi]	–	–	R/W	–	R/W	–
[ワイヤレスダイレクト設定]	–	R	R/W	–	R/W	R
[Bluetooth]	–	R	R/W	–	R/W	R
[プロキシ設定]	–	R/W	–	–	R/W	–
[本体へのポート転送]	–	–	R/W	–	R/W	–

[端末]

設定項目	User	機器	N/W	文書	なし	あり
[音]	–	R/W	–	–	R/W	–
[ディスプレイ]	–	R/W	–	–	R/W	–
[ストレージ]	–	R	R	–	R	R

[ユーザー設定]

設定項目	User	機器	N/W	文書	なし	あり
[セキュリティー]	–	R/W	–	–	R/W	–
[言語と入力]	–	R/W	R/W *1	–	R/W	–

*1 [言語切り換え] のみ

[システム]

設定項目	User	機器	N/W	文書	なし	あり
[操作部情報]	–	R	R	–	R	R
[操作部機器設定]	–	R/W	–	–	R/W	–

ホーム編集

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

設定項目	User	機器	N/W	文書	なし	あり
アイコン／ウィジェット／フォルダーの追加	−	R/W	−	−	R/W	−
アイコン／ウィジェット／フォルダーの並べ替え	−	R/W	−	−	R/W	−
アイコン／ウィジェット／フォルダーの削除	−	R/W	−	−	R/W	−
壁紙の変更	−	R/W	−	−	R/W	−

かんたんカード認証設定

設定項目	User	機器	N/W	文書
[認証機能を使用する] ／ [認証機能を使用しない]	–	R/W	–	–
[アドレス帳管理]	R/W	–	–	–
[優先ユーザー設定]	R/W	–	–	–
[USB カードリーダー設定]	–	R/W	–	–
[NFC カードリーダー設定]	–	R/W	–	–
[Bluetooth 設定]	–	R/W	–	–

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
［ダウンロード］	−	R/W	−	−	−	−
［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

Web Image Monitor：ジョブ

［機器の情報］の中の項目です。

ユーザーは、ユーザー自身が実行したジョブだけを操作できます。

［ジョブリスト］

設定項目	User	機器	N/W	文書	なし	あり
［実行中/待機中ジョブ一覧］：［予約削除］	ー	R/W	ー	ー	ー	R/W
［実行中/待機中ジョブ一覧］：［印刷保留/印刷再開］	ー	R/W	ー	ー	ー	ー
［実行中/待機中ジョブ一覧］：［順序入れ替え］	ー	R/W	ー	ー	ー	ー
［ジョブ履歴］	ー	R	ー	ー	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	R/W	R	R	R	R
［ジョブ履歴］	R	R/W	R	R	R	R
［エラー履歴］	ー	R	ー	ー	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］	ー	R	ー	ー	R	R*1
［受信履歴］	ー	R	ー	ー	R	R*1
［PC ファクス］	ー	R	ー	ー	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。

［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］	ー	R	ー	ー	R	R*1
［ファクス　リモート送信履歴］	ー	R	ー	ー	R	R*1
［スキャナー　リモート送信履歴］	ー	R	ー	ー	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：操作部初期設定

［機器の管理］の［設定］の項目です。

設定項目	User	機器	N/W	文書	なし	あり
すべての項目	R/W	R/W	R/W	R/W	ー	ー

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	ー	ー
［印刷優先機能］	R	R/W	R	R	R/W	R
［印刷機能移行時間］	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
［IP アドレス機器画面表示］	R	R/W	R	R	ー	ー
［メディアスロット使用］	R	R/W	R	R	R	R
［Compatible ID］	R	R/W	R	R	R/W	R
［PDF ファイル形式：PDF/A 固定］	R	R/W	R	R	R/W	R
［針なしステープル設定］	R	R/W	R	R	R/W	R
［Web Image Monitor からの蓄積文書の印刷］	R	R/W	R	R	R	R
［人体検知センサー］	R	R/W	R	R	R	R
［ビジネスアプリケーション向け省エネ復帰設定］	R	R/W	R	R	R/W	R
［ADF 動作設定：コピー/ドキュメントボックス］	R	R/W	R	R	R/W	R
［フィニッシャー排紙時出力優先設定］	R	R/W	R	R	R/W	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
［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

[用紙]

設定項目	User	機器	N/W	文書	なし	あり
[トレイ 1～4]	R	R/W	R	R	R/W	R
[大量給紙トレイ]	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]

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
[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
[定着部オフモード移行設定]	R	R/W	R	R	R/W	R
[ウィークリータイマー]	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
[ログ転送] *2	R	R/W	R	R	R/W	R

設定項目	User	機器	N/W	文書	なし	あり
[分類コード]	R	R/W	R	R	R/W	R
[ログ一括消去]	−	R/W	−	−	R/W	−

*2 [無効] への変更だけできます。

[ログダウンロード]

設定項目	User	機器	N/W	文書	なし	あり
[ダウンロードするログ]	−	R/W	−	−	−	−
[ダウンロード]	−	R/W	−	−	−	−

[メール]

設定項目	User	機器	N/W	文書	なし	あり
[管理者メールアドレス]	−	R/W	−	−	R/W	R
[送信者名自動指定]	−	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
[SSL]	−	−	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] *3	−	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] *3	−	R/W	−	−	R/W	−
[POP 認証後待機時間]	−	R/W	−	−	R/W	R

設定項目	User	機器	N/W	文書	なし	あり
[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
[ファクスメールの受信]	–	R/W	–	–	R/W	–
[ファクスメールユーザー名]	–	R/W	–	–	R/W	–
[ファクスメールパスワード]	–	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] *3	–	R/W	–	–	R/W	–

*3 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/W	R
[通知先グループ]	R	R/W	R	R	R/W	R
[項目ごとの通知先]	R	R/W	R	R	R/W	R
[各項目の詳細設定]	R	R/W	R	R	R/W	R

[要求時メール通知]

設定項目	User	機器	N/W	文書	なし	あり
[共通件名]	R	R/W	R	R	R/W	R
[共通本文]	R	R/W	R	R	R/W	R
[要求時メール通知のアクセス制限]	R	R/W	R	R	R/W	R
[受信可能メールアドレス/ドメイン設定]	R	R/W	R	R	R/W	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] *3	–	R/W	–	–	R/W	–

設定項目	User	機器	N/W	文書	なし	あり
[FTP 送信ユーザー名]	−	R/W	−	−	R/W	−
[FTP 送信パスワード] *3	−	R/W	−	−	R/W	−

*3 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
[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
[機器管理者認証]	R	R/W	R	R	R	R
[ネットワーク管理者認証]	R	R	R/W	R	R	R
[文書管理者認証]	R	R	R	R/W	R	R

[管理者登録/変更]

設定項目	User	機器	N/W	文書	なし	あり
[ユーザー管理者]	R/W	R	R	R	−	−
[機器管理者]	R	R/W	R	R	−	−
[ネットワーク管理者]	R	R	R/W	R	−	−
[文書管理者]	R	R	R	R/W	−	−
[ログインユーザー名] *4	R/W	R/W	R/W	R/W	−	−
[ログインパスワード] *4	R/W	R/W	R/W	R/W	−	−
[暗号パスワード] *4	R/W	R/W	R/W	R/W	−	−

*4 管理者が管理者自身のアカウントだけを変更できます。

[印刷利用量制限]

設定項目	User	機器	N/W	文書	なし	あり
[上限到達時動作設定]	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	–
[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	–	–	–	–

[連携先機器登録/変更/消去]

設定項目	User	機器	N/W	文書	なし	あり
[登録]	–	R/W	–	–	–	–
[変更]	–	R/W	–	–	–	–
[消去]	–	R/W	–	–	–	–

[機器設定情報のインポート設定（サーバー）]

設定項目	User	機器	N/W	文書	なし	あり
[ファイルのインポート元] *5	–	–	–	–	–	–
[指定時刻での定期インポート] *5	–	–	–	–	–	–
[前回のインポートファイルとの比較] *5	–	–	–	–	–	–

設定項目	User	機器	N/W	文書	なし	あり
[失敗時のメール通知] *5	–	–	–	–	–	–
[再試行回数] *5	–	–	–	–	–	–
[再試行間隔] *5	–	–	–	–	–	–
[暗号鍵] *5	–	–	–	–	–	–

*5 ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が、R/W になります。

[インポートテスト]

設定項目	User	機器	N/W	文書	なし	あり
[実行] *5	–	–	–	–	–	–

*5 ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が、R/W になります。

[機器設定情報のインポート/エクスポート]

設定項目	User	機器	N/W	文書	なし	あり
[機器設定情報のエクスポート] *5	–	–	–	–	–	–
[機器設定情報のインポート] *5	–	–	–	–	–	–
[ホーム画像ファイルのエクスポート] *5	–	–	–	–	–	–

*5 ユーザー管理者、機器管理者、ネットワーク管理者、文書管理者のすべての権限を持つ管理者が、R/W になります。

[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
[集計期間（日数)]	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
[コピー]	R	R/W	R	R	R	R
[ドキュメントボックス]	R	R/W	R	R	R	R

設定項目	User	機器	N/W	文書	なし	あり
[ファクス]	R	R/W	R	R	R	R
[プリンター]	R	R/W	R	R	R	R

[不正コピー抑止：コピー]

設定項目	User	機器	N/W	文書	なし	あり
[不正コピー抑止強制設定]	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

[不正コピー抑止：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
[不正コピー抑止強制設定]	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

[不正コピー抑止：プリンター]

設定項目	User	機器	N/W	文書	なし	あり
[不正コピー抑止設定]	R	R/W	R	R	R	R
[不正コピー抑止強制設定]	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

[USB デバイスリスト登録/変更]

設定項目	User	機器	N/W	文書	なし	あり
[デバイス 1-10]	R	R/W	R	R	R/W	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
［PDL エラージョブ自動取消の確認画面］	R	R/W	R	R	R	R
［エラー発生時のジョブ自動取消］	R	R/W	R	R	R	R
［ジョブ仕分け］	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
［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
［針なし/針ありステープル表示設定］	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
［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
［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
［手差しトレイ用紙確認画面］	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

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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
[仮想プリンター]	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
[グレー印刷方式（グレー認識広め）]	R	R/W	R	R	R	R
[初期画面の切り替え]	R	R/W	R	R	R	R
[ステープル枚数オーバー動作設定]	R	R/W	R	R	R	R
[中綴じ枚数オーバー動作設定]	R	R/W	R	R	R	R
[インターフェース設定]	R	R/W	R	R	R	R
[PCL 設定]	R	R/W	R	R	R/W *1	R
[PS 設定]	R	R/W	R	R	R	R
[PDF 設定]	R	R/W	R	R	R	R
[XPS 設定]	R	R/W	R	R	R	R

*1 [用紙サイズ] だけ設定できます。

[トレイ読み替え（PCL）]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[トレイ読み替え（PCL）]	–	R/W	–	–	–	–

[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	–	–	–	–

[トレイ読み替え（RPDL）]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[トレイ読み替え（RPDL）]	–	R/W	–	–	–	–

[イメージオーバーレイ用フォーム割り当て]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[イメージオーバーレイ用フォーム割り当て]	R	R/W	R	R	R	R

[プリンターフォーム一覧]

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[削除]	R	R/W	R	R	R	R

[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]

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
[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
[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
[PCL 設定]	R	R/W	R	R	R/W *1	R

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[PS 設定]	R	R/W	R	R	R	R
[PDF 設定]	R	R/W	R	R	R	R
[XPS 設定]	R	R/W	R	R	R	R
[RHPP 設定]	R	R/W	R	R	R/W	R/W

*1 [用紙サイズ] だけ設定できます。

[プリンター言語のファイルシステム操作許可設定]

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

［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］	ー	ー	R/W	ー	ー	ー
［IP ファクス送信ルート自動切替（IP/G3）］	ー	ー	R/W	ー	ー	ー
［IP ファクス最大送信速度設定］	ー	ー	R/W	ー	ー	ー
［受信モード切り替え］	ー	R/W	ー	ー	ー	ー
［受信モード自動切り替え時設定］	ー	R/W	ー	ー	ー	ー
［SMTP 受信ファイル配信設定］	ー	R/W	ー	ー	ー	ー
［両面印刷］	ー	R/W	ー	ー	R/W	ー
［しおり印字］	ー	R/W	ー	ー	R/W	ー
［センターマーク印字］	ー	R/W	ー	ー	R/W	ー
［受信時刻印字］	ー	R/W	ー	ー	R/W	ー
［受信文書印刷部数］	ー	R/W	ー	ー	R/W	ー

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[給紙トレイ選択]	–	R/W	–	–	R/W	–
[ファクス印刷色]	–	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	–	–	–
[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
［外部認証：フォルダーパス上書き設定］	R	R/W	R	R	R	R
［PC からの読み取り要求禁止時間］	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
［URL リンクから文書を直接ダウンロード］	R	R/W	R	R	R	R
［ログインユーザー宛先優先］	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
［カラー判定］	R	R/W	R	R	R	R
［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
［白紙検知］	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
［OCR テキスト付き PDF 白紙検知レベル］	R	R/W	R	R	R/W	R
［クリアライト PDF 圧縮率設定］	R	R/W	R	R	R/W	R
［クリアライト PDF 作成時の圧縮方式］	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

設定項目	User	機器	N/W	文書	Lv.1	Lv.2
[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
[デフォルトメール件名]	R	R/W	R	R	R	R
[文書送信方法]	R	R/W	R	R	R/W	R
[URL 送信文書保持時間]	R	R/W	R	R	R/W	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
[WSD/DSM 機能の利用]	R	R/W	R	R	R	R
[WSD あて先表表示]	R	R/W	R	R	R	R
[WSD からの読み取り要求禁止設定]	R	R/W	R	R	R	R
[DSM 以外の宛先表の利用]	R	R/W	R	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）]

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］	ー	ー	R/W	ー	R	ー
［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
［PictBridge］	R	R/W	R	R	R/W	R
［パラレルインターフェース］	R	R/W	R	R	R/W	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］	ー	ー	R/W	ー	R	ー
［ネットワーク］	R	R	R	R	R	R
［ファームウェアバージョン］	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
［電波状態］	R	R	R	R	R	R
［通信モード］	R	R	R/W	R	R/W	R
［SSID］	R	R	R/W	R	R/W	R
［チャンネル］	R	R	R/W	R	R/W	ー
［セキュリティー方式］	R	R	R/W	R	R/W	R
［WEP 設定］	R	R	R/W	R	R/W	R

設定項目	User	機器	N/W	文書	なし	あり
[WPA2 設定]	R	R	R/W	R	R/W	R
[ダイレクト接続設定]	R	R	R/W	R	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/W *1	R	R/W *1	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
［プライマリー WINS サーバー］	R	R	R/W	R	R/W	R
［セカンダリー 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

*1 IPv4 で通信しているときは Web Image Monitor で IPv4 を無効にできません。

［IPv6］

設定項目	User	機器	N/W	文書	なし	あり
［IPv6］	R	R	R/W *2	R	R/W *2	R
［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
［ステートレスアドレス］	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

設定項目	User	機器	N/W	文書	なし	あり
[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

*2 IPv6 で通信しているときは Web Image Monitor で IPv6 を無効にできません。

[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
[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	—	—	—
[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]	ー	ー	R/W	ー	ー	ー
[UUID]	ー	ー	R	ー	ー	ー
[プロファイル有効期限]	ー	ー	R/W	ー	ー	ー
[TTL]	ー	ー	R/W	ー	ー	ー

[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	ー

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］	ー	ー	R/W	ー	ー	ー
［アクセスコントロール］	ー	ー	R/W	ー	ー	ー
［IPP 認証］	ー	ー	R/W	ー	ー	ー
［SSL/TLS］	ー	ー	R/W	ー	ー	ー
［ssh］	ー	ー	R/W	ー	R	R
［サイト証明書］	ー	ー	R/W	ー	ー	ー
［機器証明書］	ー	ー	R/W	ー	ー	ー
［S/MIME］	ー	ー	R/W	ー	ー	ー
［IPsec］	ー	ー	R/W	ー	ー	ー
［ユーザーロックアウト］	ー	R/W	ー	ー	ー	ー
［IEEE 802.1X］	ー	ー	R/W	ー	ー	ー
［セキュリティー強化］						
• ［ドライバー暗号鍵］	ー	ー	R/W	ー	R/W	ー
• ［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
• ［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
• ［@Remote サービス］	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	ー	ー
• ［ファームウェア構成変更］	R	R/W	R	R	ー	ー
• ［パスワードポリシー］	R/W	ー	ー	ー	ー	ー

設定項目	User	機器	N/W	文書	なし	あり
• [SNMPv1,v2 による設定]	R	R	R/W	R	R/W	R
• [アクセスセキュリティー設定]	R	R/W	R	R	ー	ー
• [パスワード攻撃検知]	ー	R/W	ー	ー	ー	ー
• [アクセス攻撃検知]	ー	R/W	ー	ー	ー	ー

Web Image Monitor：@Remote

［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
［RC Gate セットアップ］	－	R/W	－	－	－	－
［RC Gate ファームウェア更新］	－	R/W	－	－	－	－
［RC Gate プロキシサーバー］	－	R/W	－	－	－	－
［機器の故障を通報する］	－	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。

［Webpage 設定］

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
［Web Image Monitor オートログアウト］	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：拡張機能初期設定

［機器の管理］の［設定］の項目です。

設定項目	User	機器	N/W	文書	なし	あり
［起動設定］	ー	R/W	ー	ー	ー	ー
［拡張機能情報］	R	R	R	R	R	R
［インストール］	ー	R/W	ー	ー	ー	ー
［アンインストール］	ー	R/W	ー	ー	ー	ー
［管理者用設定］	ー	R/W	ー	ー	ー	ー
［追加プログラム起動設定］	ー	R/W	ー	ー	ー	ー
［追加プログラムインストール］	ー	R/W	ー	ー	ー	ー
［追加プログラムアンインストール］	ー	R/W	ー	ー	ー	ー
［拡張機能複製］	ー	R/W	ー	ー	ー	ー
［カードセーブデータ複製］	ー	R/W	ー	ー	ー	ー

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	ー	ー	ー	R/W *1	R/W *1
［変更］	R/W	ー	ー	ー	R/W *1	R/W *1
［削除］	R/W	ー	ー	ー	R/W *1	R/W *1
［グループ追加］	R/W	ー	ー	ー	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	ー	ー	ー	R/W	R
［メンテナンス］	R/W	ー	ー	ー	ー	ー
［集中管理設定］	R/W	ー	ー	ー	ー	ー

*1 ［セキュリティー強化］の［個人宛先登録制限］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だけ変更できます。

Web Image Monitor：集中管理設定

［機器の管理］の中の項目です。

ユーザー管理者の権限があると表示されません。ユーザー管理者の権限があるときは［機器の管理］ ＞ ［アドレス帳］で設定します。

設定項目	User	機器	N/W	文書	なし	あり
［集中管理設定］	－	R/W	－	－	－	－

Web Image Monitor：主電源オフ

［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
［主電源オフモード］	－	R/W	－	－	－	－
［実行する］	－	R/W	－	－	－	－

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	－	－	－	－

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
［機器のリセット］	－	R/W	－	－	R/W	－

Web Image Monitor：操作部画面の監視

［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
［表示中の画面を取得］	－	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.346「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
［フォルダー新規作成］	－	－	－	R/W	R/W	R/W
［フォルダー編集］	－	－	－	R/W	R/W	R/W
［フォルダー削除］	－	－	－	R/W	R/W	R/W
［フォルダーロック解除］	－	－	－	R/W	－	－
［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］	－	－	－	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］に設定しているときは、指定されたユーザーだけ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を操作できます。

ほか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］	－	－	－	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
[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
[文書ロック解除]	－	－	－	－	－	R/W
[文書消去]	－	－	R/W	R/W	R/W*1	R/W
[指定ページ印刷]	R/W	R/W	R/W	R/W	R/W*1	－

*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です。

- 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。

ー：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
[表示優先度]	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]

設定項目	閲覧	編集	編/削	フル	登録者	User
[ユーザーコード]	ー	ー	ー	ー	ー	R/W
[ログインユーザー名]	ー	ー	ー	ー	R	R/W

設定項目	閲覧	編集	編/削	フル	登録者	User
[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	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
[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

設定項目	閲覧	編集	編/削	フル	登録者	User
[SMTP サーバーを経由]	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 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
[接続テスト]	R	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	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

- [セキュリティー強化] 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。

索引

記号・数字

@Remote サービス....243

アルファベット

AH プロトコル....133
eco 指数カウンター....235
ESP プロトコル....133
IC カード認証....65
IEEE 802.1X 方式の認証を設定する....149
IPP 認証のパスワード....156
IPsec 通信....133
Kerberos 認証....37, 159
LDAP 認証....47
NTLM 認証....37
S/MIME....126
SMTP 通信の SSL を設定する....125
SNMPv1,v2 による設定....244
SNMPv3 暗号化通信を設定する....155
SSL....121
SSL/TLS 通信許可設定....124
WSD スキャナー機能....249

あ

アクセス攻撃検知....246
アクセスコントロール....105
アクセスセキュリティー設定....244
宛先利用制限....241
アドレス帳の暗号化....240
アドレス帳の操作権限....347
暗号化通信モード....124
暗号強度設定....239
イーサネットで IEEE 802.1X を使用する....150
印刷利用量制限....75
エラーコード....260
エラーメッセージ....259
オートログアウト....60

か

管理者....12
管理者認証....13
管理者の種類....69
管理者の登録....15
管理者の変更....15
機器証明書....119, 121, 128, 150
機器設定の変更防止....69
機能の使用制限....72
機密印刷文書の管理....173
強制蓄積....184
個人宛先登録制限....241
個人情報表示制限....240
誤送信防止....248

さ

サーバー証明書....45
サービスモード移行禁止設定....251
サイト証明書の導入....149
実行中ジョブへの認証の実施....242
自動鍵....134
受信指定先への転送....242
署名....128
スーパーバイザー....22
セキュリティー機能....248
セキュリティー機能を設定する前に....9
セキュリティー強化機能....239
セキュリティー設定....10
操作権限....277

た

蓄積受信文書ユーザー設定....248
蓄積文書の操作権限....346
中間証明書....119
通信管理レポートの出力....248
通信経路の保護....116
電子署名付き PDF....132
ドライバー暗号鍵....156, 239

な

認証情報....34
ネットワークセキュリティーレベル....111

は

パスワード攻撃検知....245
パスワードポリシー....244
パスワードロックアウト解除....59
パスワードロックアウト設定....59
パスワードを暗号化通信する....156
ファームウェアアップデート....243
ファームウェアアップデート時の注意....10

ファームウェア構成変更.....243
不正コピーガード設定.....180
ブラウザー機能.....223
プリンタージョブ認証..... 52
プロトコル..... 106
文書パスワード.....169
文書保護強化.....240
文書ロック解除.....171
ベーシック認証.....32

ま

無線 LAN で IEEE 802.1X を使用する.....152
メディアスロット.....74
メニュープロテクト.....69, 70
メモリー自動消去.....96
メモリー全消去.....100

や

ユーザー.....25
ユーザーコード認証..... 29
ユーザー個別設定の暗号化..... 240
ユーザー証明書.....127
ユーザー認証..... 26
ユーザー認証設定.....27

ら

利用量制限..... 75
履歴満杯時印刷.....249
ログアウト（管理者）..... 21
ログイン（管理者）..... 19
ログインパスワードの設定.....34
ログインユーザー名の設定.....34
ログイン用認証情報..... 35
ログ情報の管理.....185
ログ情報の管理（Web Image Monitor）.186
ログ情報の管理（本機）.....219
ログの暗号化.....186
ログの一括消去.....186, 219
ログの種類..... 185
ログのダウンロード..... 186
ログの転送..... 186, 219
ロックアウト機能.....58

JA JP 2016年2月 D241-7048A © 2015,2016 Ricoh Co., Ltd