

6. セキュリティー強化機能を設定する

セキュリティ強化機能を設定する

項目によって、設定する管理者が異なります。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

ユーザー認証や、管理者による機器の利用制限だけではなく、機器が通信する情報に暗号をかけたり、アドレス帳などのデータを暗号化したりすることにより、保護を強化することができます。セキュリティの強化を必要とする場合は、本機のセキュリティ強化機能を設定して使用してください。

ここでは、セキュリティ強化の各機能の概要と設定方法を説明します。

参照

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

セキュリティ強化機能の変更

セキュリティ強化機能の変更をするときは、以下の手順でセキュリティ強化機能の設定画面を表示させます。

セキュリティ強化機能の変更のしかた

- 1 [メニュー] キーを押します。
- 2 [セキュリティ管理] を選択し、[OK] キーを押します。
- 3 [▲] [▼] キーを押して [セキュリティ強化] を選択し、[OK] キーを押します。
- 4 [▲] [▼] キーを押して設定を変更する項目を選択し、[OK] キーを押します。
- 5 設定を変更し、[OK] キーを押します。
- 6 [メニュー] キーを押します。

設定項目について

各設定項目の工場出荷時の値は太字で示しています。

◆ 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送信するパスワードの暗号化を行います。ドライバー暗号鍵を設定する場合は本機で設定した暗号鍵を印刷するドライバーに入力してください。パスワードの暗号化を行います。

設定方法については、「ドライバー暗号鍵の設定」を参照してください。

◆ アドレス帳暗号化

ユーザー管理者が設定します。

機器のアドレス帳情報を暗号化します。内部の部品が流出した場合でも、暗号化によりアドレス帳の情報を読み取ることはできません。

設定方法については、「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**

◆ 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することができます。個人認証ができない接続方法でジョブ履歴を確認する際に個人情報を全て「*****」表示にすることができます。たとえば、管理者として認証されていないときに、Ridoc IO Admin から SNMP を使ってジョブ履歴を確認するときに、個人情報がわからないように「*****」表示にすることができます。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ぐことができます。

- ・ **する**
- ・ **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可能性もあります。文書保護強化を設定した場合、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することができます。

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

- ・ **する**
- ・ **しない**

◆ SNMPv1,v2 による設定

ネットワーク管理者が設定します。

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

- ・ **禁止する**
- ・ **禁止しない**

◆簡易暗号化使用制限

ネットワーク管理者が設定します。

高度な暗号化が設定できないときに、簡易暗号化処理を行います。たとえば、Ridoc IO Admin の「ユーザー情報管理ツール」と「アドレス帳情報管理」でアドレス帳を編集したり、Ridoc Desk Navigator と Ridoc Document Router を使用したりする場合に、SSL/TLS の設定を有効（暗号化）にできないときに、[しない] に設定します。SSL/TLS の設定を有効（暗号化）にしているときは、[する] に設定します。SSL/TLS の設定については、「SSL/TLS 通信許可設定」を参照してください。また、[する] に設定した場合は、プリンタードライバーで暗号化の設定を行ってください。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。

- ・する
- ・しない

◆実行中ジョブへの認証の実施

機器管理者が設定します。

コピーの中断、プリンターのジョブキャンセル等の操作に認証を必要とするか、不要とするか設定できます。

[ログイン権限] に設定すると認証の許可があるユーザー、および機器管理者が操作可能です。[ログイン権限] の設定が有効で、すでにユーザーが本機にログイン中の場合は認証の要求はされません。

[アクセス権限] に設定するとコピー、印刷を行ったユーザー、および機器管理者が操作可能です。

[ログイン権限] に設定し、ユーザーが本機にログインできる場合でも、コピー機能やプリンター機能などの操作権限がユーザーになければ、コピーの中断、およびプリンターのジョブキャンセルはできません。

「ユーザー認証管理」を設定しているときのみ、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

◆パスワードポリシー

ユーザー管理者が設定します。

「ベーシック認証」が設定されているときのみ、パスワードポリシーの設定が有効となります。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くパスワードのみ設定できます。

[複雑度 1] に設定した場合、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るパスワードを設定します。

[複雑度 2] に設定した場合、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るパスワードを設定します。

- ・複雑度 1
- ・複雑度 2
- ・制限しない（0 文字）

◆ @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 @Remote サービスのための HTTPS 通信を停止することができます。[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。

- ・ 禁止する
- ・ 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することができなくなります。

[禁止しない] を選択した場合、ファームウェアアップデートの制限は無効になり、誰でもアップデートを実施することができます。

- ・ 禁止する
- ・ 禁止しない

◆ 構成変更

機器管理者が設定します。

ファームウェア構成変更を監視するかどうかを設定します。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 of 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場合、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ることで、管理者は構成変更が正当なものか不正なものかを確認することができます。不正な構成変更であった場合は、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] に設定する場合は、「管理者認証管理」を有効に設定しておく必要があります。

[禁止する] に設定したあとに、「管理者認証管理」を一度無効にし、再度「管理者認証管理」を有効に設定した場合、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] に設定した場合、構成変更の検知は無効になります。

- ・ 禁止する
- ・ 禁止しない

☞ 参照

- ・ P.98 「ドライバー暗号鍵の設定」
- ・ P.66 「アドレス帳を暗号化する」
- ・ P.106 「SSL/TLS 通信許可設定」

機器の操作をお客様に限定する

お使いの機器を管理者の認証がなければ操作ができないようにしたり、サービス実施店より遠隔操作でアドレス帳の登録を行うことを禁止することができます。

弊社ではお客様の情報につきまして厳重な管理を行っております。さらに管理者の認証を行ってから操作させていただくことで、お客様の管理の元での作業を行います。

利用する設定は次の設定です。

設定項目について

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

◆ サービスモード移行禁止設定

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

目 参照

- ・P27 「操作部での管理者認証でのログインのしかた」
- ・P28 「操作部での管理者認証でのログアウトのしかた」
- ・P129 「セキュリティー強化機能を設定する」

サービスモード移行禁止設定を有効にする

- 1 [メニュー] キーを押します。
- 2 [▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] キーを押します。
- 3 [▲] [▼] キーを押して [サービスモード移行禁止設定] を選択し、[OK] キーを押します。
- 4 [▲] [▼] キーを押して [する] を選択し、[OK] キーを押します。
- 5 メッセージを確認し、[禁止する] を押します。
- 6 [メニュー] キーを押します。

サービスモード移行禁止設定を解除する

カスタマーエンジニアがサービスモードで点検または修理を行うときには、機器管理者でログインし、サービスモード移行禁止設定を解除します。

- 1** [メニュー] キーを押します。
- 2** [▲] [▼] キーを押して「セキュリティー管理」を選択し、[OK] キーを押します。
- 3** [▲] [▼] キーを押して「サービスモード移行禁止設定」を選択し、[OK] キーを押します。
- 4** [▲] [▼] キーを押して「しない」を選択し、[OK] キーを押します。
- 5** [初期設定] キーを押します。
カスタマーエンジニアがサービスモードに移行できます。