

4. 本機へのアクセスを管理する

機器設定の変更を防止する

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

管理者を登録して本機を運用します。

◆ 管理者の種類

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

- ・ユーザー管理者
- ・機器管理者
- ・ネットワーク管理者
- ・文書管理者

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

◆ メニュープロテクト機能

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

目 参照

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

メニュープロテクトについて

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

☒ 参照

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

4

メニュープロテクトを設定する

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

メニュープロテクトは [しない]、[レベル 1]、[レベル 2] から設定することができます。[しない] を設定した場合はメニュープロテクトによる制限はありません。アクセス権の制限をより強くする場合は、[レベル 2] に設定してください。

- 1 [メニュー] キーを押します。
- 2 [▲] [▼] キーを押して [調整 / 管理] を選択し、[OK] キーを押します。
- 3 [▲] [▼] キーを押して [一般管理] を選択し、[OK] キーを押します。
- 4 [▲] [▼] キーを押して [メニュープロテクト] を選択し、[OK] キーを押します。
- 5 [▲] [▼] キーを押して設定するメニュープロテクトのレベルを選択し、[OK] キーを押します。
- 6 [メニュー] キーを押します。

↓ 補足

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

☒ 参照

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

機能の使用を制限する

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

使用できる機能を設定する

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

登録されたユーザーに対して、使用できる機能を設定します。この設定により、ユーザーの使用できる機能を制限することができます。

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

参照

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

ログ情報の管理

1) ログについて

本機は以下のログ情報の蓄積をメモリーやハードディスクに行います。

ログ情報を確認するためには、Ridoc IO OperationServer が必要です。

- ・ジョブログ

ユーザーの文書に関わるワークフロー全てのログ情報

- ・アクセスログ

ログイン / ログアウト / 文書生成 / 文書削除 / 文書自動削除 / 文書一括削除 / 不正コピーガード文書読み取り / 管理者操作 ^{*1} / カスタマーエンジニア操作 ^{*2}

^{*1} 管理者操作 : ジョブログ機能設定変更 / アクセスログ機能設定変更 / ログ情報一括削除 / ログ暗号化設定変更

^{*2} カスタマーエンジニア操作 : ハードディスク初期化

2) ログ消去について

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

3) ログ転送について

転送されるログはジョブログ、アクセスログ、不正読み取りの事実、読み取り者、読み取り時刻です。

ログを転送することで、不正読み取り履歴や読み取り者の確認ができます。

4

ログ消去の設定

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

本機に記憶されたログをまとめて消去することができます。本機に記録されたログを消去することで、ハードディスクの容量を空けることができます。

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

2 [設定] をクリックします。

3 [機器] メニューの [ログ] をクリックします。

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

5 [OK] をクリックします。
[ログ] メニューに戻ります。

6 [OK] をクリックします。

7 [ログアウト] をクリックします。

8 Web Image Monitor を終了します。

参照

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

ログ転送の設定

機器管理者は、Ridoc IO OperationServer からのみ [する] に設定できます。本機からは [する] に設定されている場合のみ [しない] に設定の変更ができます。本機への管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

ログ転送設定の設定値の確認や変更ができます。この設定により Ridoc IO OperationServer へログを転送し、不正読み取り履歴や読み取り者の確認ができます。

Ridoc IO OperationServer については、販売店にお問い合わせください。

ログ転送の設定については Ridoc IO OperationServer の使用説明書を参照してください。

- 1** [メニュー] キーを押します。
- 2** [▲] [▼] キーを押して [セキュリティ管理] を選択し、[OK] キーを押します。
- 3** [▲] [▼] キーを押して [ログ転送設定] を選択し、[OK] キーを押します。
- 4** [▲] [▼] キーを押して [しない] を選択し、[OK] キーを押します。
- 5** [メニュー] キーを押します。

参照

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

