

2. 認証の概念と運用

2

管理者とユーザー

管理者によって設定された認証を使用してアクセス制限する場合、まず本機の管理者を決定し、認証機能を有効にして運用します。管理者は割り当てられた機能についてのアクセス権を管理し、ユーザーは管理者によって、アクセス権を与えられた機能だけを使用できるようになります。認証機能を有効にした場合、本機を使用するためにはログインユーザー名とログインパスワードが必要になります。管理者認証を設定してから、ユーザー認証を設定してください。

★重要

- ハードディスクの故障やネットワークのトラブルなどで、ユーザー認証できないときは、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することができます。緊急で本機を使用する必要がある場合に使用してください。

管理者

管理を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することができます。1人の管理者が複数の管理者の役割を兼務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、管理者名でコピーやプリンターなどのユーザー機能を使用することはできません。アドレス帳に新規にユーザーを作成しユーザーとしての認証が必要になります。

管理者の登録方法については「管理者を登録する」、スーパーバイザーについては「スーパーバイザーの操作」を参照してください。

◆ユーザー管理者とは

アドレス帳の個人情報を管理する管理者です。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することができます。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、削除することができます。ユーザー管理者は使用しているユーザーが自分のパスワードを忘れた場合に削除したり、新規に作成することができ、ユーザーが操作できなくなることを防ぐことができます。

◆機器管理者とは

主に機器の初期設定を管理する管理者です。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することができます。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ぎます。

◆ **ネットワーク管理者とは**

ネットワークに接続するための設定を管理する管理者です。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することができます。それにより、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いだり、適切なネットワーク設定を行うことができますようにします。

◆ **文書管理者とは**

蓄積した文書のアクセス権を管理する管理者です。本機に蓄積した文書に対して、登録したユーザーや許可したユーザーのみ閲覧、編集できるようパスワードを設定したりすることができます。それにより、登録した文書を不特定のユーザーが閲覧したり、操作することによって起こる情報漏洩や改ざんを防ぐことができます。

◆ **スーパーバイザーとは**

各管理者のパスワードを削除したり、新規に設定することができます。初期設定、通常の操作をすることはできません。管理者がパスワードを忘れてしまい、操作ができなくなってしまったときに対応することができます。

E 参照

- P.26 「管理者を登録する」
- P.139 「スーパーバイザーの操作」

ユーザー

ユーザーは本機のアドレス帳に登録された個人情報によって管理されます。ユーザー認証を有効に設定することで、アドレス帳に登録されたユーザーのみを機器の利用者として設定することができます。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。アドレス帳へのユーザーの登録方法については、Ridoc IO Admin、Web Image Monitor のヘルプ、または Ridoc IO OperationServer の使用説明書を参照してください。

管理機能の概念

ログインユーザー名、ログインパスワードによる認証機能が本機には搭載されています。認証機能を使用することで、個人やグループ単位でのアクセス制限を設定することができます。アクセス制限は本機で使用できる機能を制限するだけでなく、本機に蓄積された文書やデータ、また本機での設定項目を保護できます。

★重要

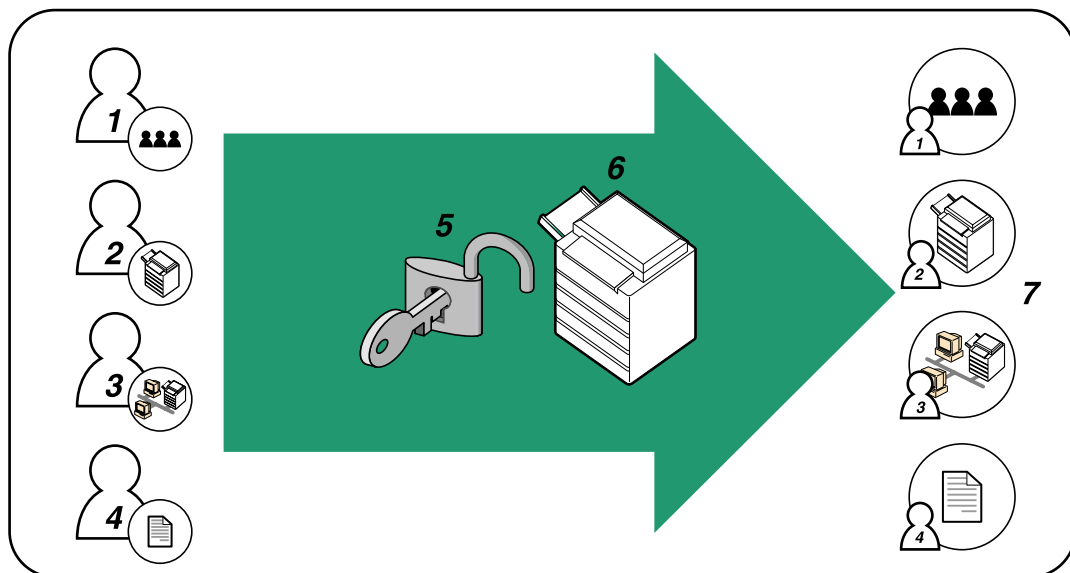
- 管理者認証を有効にした場合は、管理者のログインユーザー名とログインパスワードを絶対に忘れないようにしてください。万一忘れてしまった場合は、スーパーバイザーの権限でパスワードを新しく設定します。スーパーバイザーについては、「スーパーバイザーの操作」を参照してください。
- スーパーバイザーのログインユーザー名とログインパスワードは、絶対に忘れないようにしてください。万一忘れてしまった場合は、サービス実施店に連絡し、工場出荷時の値に戻すこととなります。本機のデータや設定が失われますのでご了承ください。

E 参照

- P.139 「スーパーバイザーの操作」

管理者認証の概念

管理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。



BBC005S

1 ユーザー管理者

アドレス帳の個人情報管理する管理者です。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することができます。

2 機器管理者

主に機器の初期設定を管理する管理者です。不正コピーガード機能やログ消去の設定などの初期設定を機器管理者だけが設定できるようにすることができます。

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する管理者です。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することができます。

4 文書管理者

蓄積した文書のアクセス権を管理する管理者です。本機に蓄積した文書に対して、登録したユーザーや許可したユーザーのみ閲覧、編集できるようパスワードを設定したりすることができます。

5 認証

本機の正しい管理者であることを確認するために、ログインユーザー名とログインパスワードを使用した管理者認証を行います。

6 本機

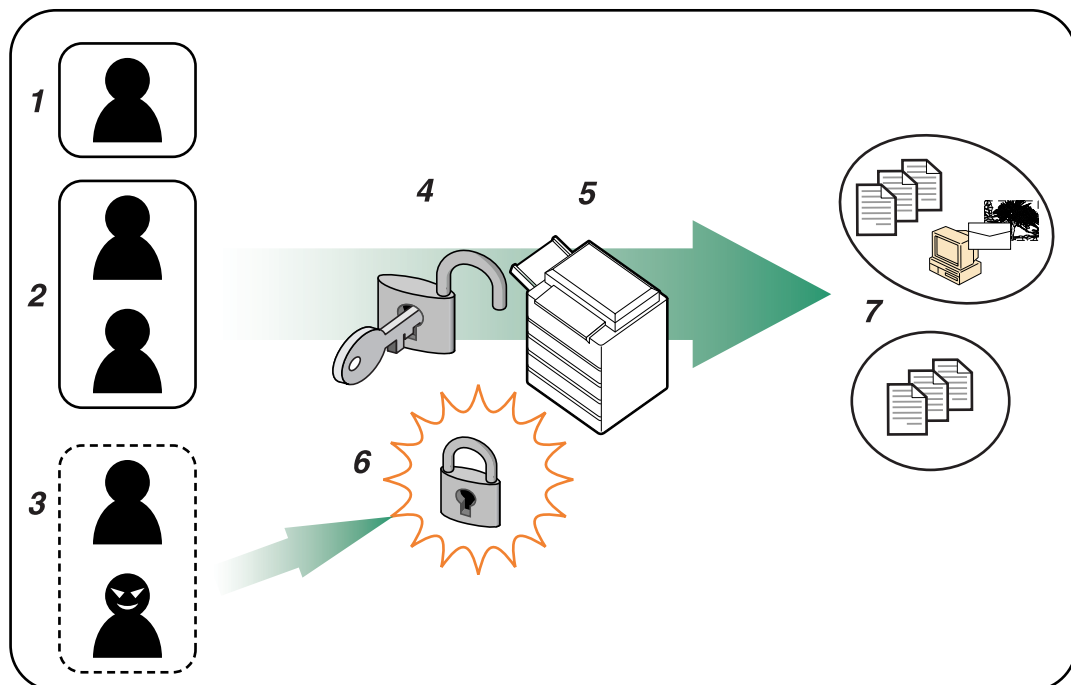
7 各管理者は機器のアクセス制限や設定項目を管理します。各管理者の担当機能については、「管理者」を参照してください。

参照

・P.17 「管理者」

ユーザー認証の概念

本機には不正なアクセス、不正な操作を防止するために認証機能が搭載されています。ユーザー認証では、ログインユーザー名、ログインパスワードにより個人やグループ単位でのアクセス制限が設定できます。



BBC004S

- 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や不正アクセス者**
- 4 認証**
本機の正しいユーザーであることを確認するために、ログインユーザー名とログインパスワードを使用したユーザー認証を行います。
- 5 本機**
- 6 アクセス制限**
アクセスを許可されていないユーザーや不正アクセス者は認証により本機へのアクセスを制限されます。
- 7 認証により本機へのアクセスを許可され、それぞれのユーザー、グループは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。**

認証機能の設定

本機の正しい管理者、また正しいユーザーであることを確認するために、ログインユーザー名とログインパスワードを使用した管理者認証、ユーザー認証を行います。認証を行うためには本体の初期設定で、認証機能を有効に設定する必要があります。また、認証機能を設定する場合は、管理者の登録が必要です。管理者の登録方法については、「管理者を登録する」を参照してください。

目 参照

- ・ P.26 「管理者を登録する」

認証機能設定の流れ

次の流れで管理者認証、ユーザー認証の設定を行います。

認証機能設定の流れ

管理者認証を行う ▼	管理者の権限を設定する 管理者を登録する
ユーザー認証を行う	ユーザー認証を設定する ユーザー認証には次の方法があります。 1) 本機のみで行える認証方法 <ul style="list-style-type: none"> ・ ユーザーコード認証 ・ ベーシック認証 2) 外部機器を必要とする認証方法 <ul style="list-style-type: none"> ・ Windows 認証 ・ LDAP 認証 ・ 統合サーバー認証（弊社別売り製品が必要です）

↓ 補足

- ・ ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証を設定する場合は、管理者認証を設定してください。
- ・ ユーザーコード認証を設定する場合は、管理者認証を設定せずに、ユーザー認証の設定ができます。

目 参照

- ・ P.23 「管理者認証を設定する」
- ・ P.25 「管理者の権限を設定する」
- ・ P.26 「管理者を登録する」
- ・ P.30 「ユーザー認証を設定する」
- ・ P.30 「ユーザーコード認証」
- ・ P.32 「ベーシック認証」
- ・ P.35 「Windows 認証」
- ・ P.41 「LDAP 認証」
- ・ P.45 「統合サーバー認証」

管理者認証を設定する

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を使用することはできません。また、Windows 認証、LDAP 認証および統合サーバー認証の対象とはならないため、ネットワーク環境で障害が起き、サーバーに接続できないときでもログインすることができます。各管理者は、ログインユーザー名で区別されます。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ことによって、複数の管理者を兼務することが可能です。

各管理者に対して設定できる項目は、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、Ridoc IO Admin で設定するときに、SNMPv3 で暗号化するときのパスワードです。本機に登録したパスワードを Ridoc IO Admin などに入力する必要があります。

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を使用することはできません。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になります。

↓ 補足

- ・管理者認証は、Web Image Monitor 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。

Web Image Monitor の管理者モードへのログインのしかた

各種認証の設定や機器の設定は Web Image Monitor から行います。設定をするためには管理者モードにログインする必要があります。

◆ 本機の実環境設定

Web Image Monitor を使用する場合は、本機で TCP/IP プロトコルの設定を行ってください。

◆ 推奨ブラウザ

- ・ Windows 環境：
Internet Explorer 5.5 SP2 以降
Firefox 1.0 以降
- ・ Macintosh 環境：
Firefox 1.0 以降
Safari 1.0、1.2、2.0(412.2) 以降

↓ 補足

- ・ Mac OS 10.4.1 上の Safari はご使用になれません。
- ・ 使用するブラウザのバージョンが推奨ブラウザより低い場合や、使用するブラウザの設定で、「JavaScript」、「Cookie の使用許可」が有効になっていない場合は、表示や操作に不具合が生じる場合があります。
- ・ プロキシサーバーをご使用の場合、本機との接続にプロキシサーバーを経由しない設定にしてください。詳しくはネットワーク管理者に確認してください。

- ブラウザの [戻る] で前のページに戻れないことがあります。そのときはブラウザの [更新] または [再読み込み] をクリックしてください。
- Web Image Monitor で取得できる情報は、自動的に更新されません。情報を更新する場合は、Web Image Monitor のワークエリアに表示された [最新の情報に更新] をクリックしてください。
- Firefox をご使用の場合、テーブルがくずれ、フォントや色が違うなどの現象が起こることがあります。

2

1 Web ブラウザを起動する。

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

IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。

Web Image Monitor のトップページが表示されます。

DNS サーバー、WINS サーバーを使用し、本機のホスト名が設定されている場合、ホスト名を入力することができます。

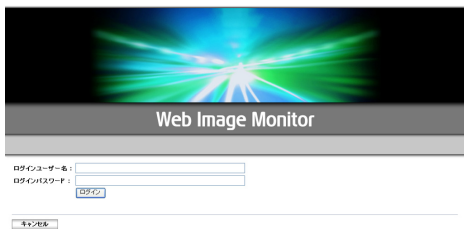
サーバー証明を発行し、SSL (暗号化通信) の設定をしている場合は、「https:// (本機の IP アドレス、またはホスト名) /」と入力します。

3 [ログイン] をクリックします。



ログインユーザー名とログインパスワードを入力する画面が表示されます。

4 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。



工場出荷時の値は、ログインユーザー名は admin、ログインパスワードは空欄に設定されています。

Web Image Monitor の管理者モードからのログアウトのしかた

1 [ログアウト] をクリックします。



2

↓ 補足

- ・ログインをした場合、操作が完了したら、必ず [ログアウト] をクリックしてログアウトしてください。

管理者の権限を設定する

管理者認証を有効にするときは、管理者認証管理の設定で [する] を選択します。

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

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。

★重要

- ・管理者認証を有効にした場合は、管理者のログインユーザー名とログインパスワードを絶対に忘れないようにしてください。万一忘れてしまった場合は、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、「スーパーバイザーの操作」を参照してください。

1 Web Image Monitor を起動し、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 [管理者認証管理] をクリックします。

4 [ユーザー管理者認証] [機器管理者認証] [ネットワーク管理者認証] [文書管理者認証] の中で設定したい管理者認証を「する」にし、[OK] をクリックします。

「設定」メニューに戻ります。

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。

E 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」
- P.139 「スーパーバイザーの操作」

管理者を登録する

2

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

登録されている管理者名とパスワードでログインしてください。工場出荷時の値は、管理者のログインユーザー名は admin、パスワードは空に設定されています。

ログインユーザー名、ログインパスワードに登録できる文字は、アルファベット、数字、記号です。登録できる文字数は、半角で最大32文字です。アルファベットは、大文字、小文字を区別して正しく登録してください。ログインユーザー名にスペース、「:」、「"」を登録することはできません。また、数字のみや空白にすることもできません。

管理者認証のログイン方法については、「操作部での管理者認証でのログインのしかた」を参照してください。

- 1 Web Image Monitor を起動し、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 [管理者登録 / 変更] をクリックします。
- 4 権限を設定したい管理者を [管理者 1] [管理者 2] [管理者 3] [管理者 4] のいずれかにチェックします。
- 5 「ログインユーザー名」を入力し、「ログインパスワード」の [変更] をクリックします。
- 6 新規パスワードと確認用パスワードに同じものを入力し、[OK] をクリックします。
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推奨します。パスワードポリシーについては P.131 「パスワードポリシー」を参照してください。
- 7 「暗号パスワード」の [変更] をクリックします。
- 8 暗号パスワードと確認用パスワードに同じものを入力し、[OK] をクリックします。

- 9 [OK] をクリックします。
「設定」メニューに戻ります。

- 10 管理者モードからログアウトします。

- 11 Web Image Monitor を終了します。

↓ 補足

- ・リコー認証 IC カード、または FeliCa を使用して管理者登録することもできます。登録方法については IC カード認証の使用説明書を参照してください。

📖 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.131 「パスワードポリシー」

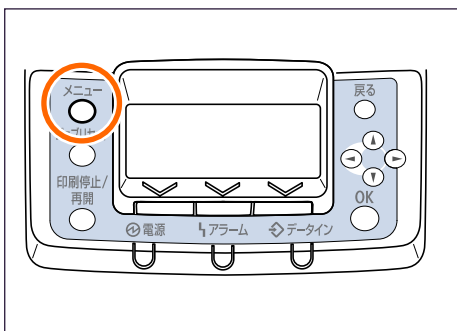
操作部での管理者認証でのログインのしかた

管理者認証が設定されているときは、管理者のユーザー名とパスワードでログインします。ここでは、ログインするまでの方法について説明します。

すでにユーザー認証が設定されているときは、認証画面が表示されます。管理者としてログインするときは、管理者のログインユーザー名とログインパスワードを入力します。管理者権限でログインしたときは、ログインしている管理者名が表示されます。複数の管理者権限をもつログインユーザー名でログインしたときは、管理者権限をもついずれかの管理者名が表示されます。

操作画面でログインしたときは、「機能は使用できません。」と表示されます。そのまま、[確認] キーを押します。

- 1 [メニュー] キーを押します。



BEJ008S

- 2 [ログイン] を押します。



3 [入力] キーを押します。

2

4 ログインユーザー名を入力し、[入力終了] キーを押します。

[▲] [▼] [◀] [▶] キーで文字を選び、[OK] キーで決定します。
管理者ではじめてログインするときは、「admin」と入力します。

5 [入力] キーを押します。

6 [ログインパスワード] を入力して、[入力終了] キーを押します。

管理者をはじめて設定するときは、ログインパスワードを入力せずに [OK] キーを押します。

操作部での管理者認証でのログアウトのしかた

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。ここでは、各種設定が終了して、ログアウトする方法について説明します。

1 [ログアウト] を押します。

2 [する] を押します。**2**

管理者を変更する

管理者のログインユーザー名、ログインパスワードを変更します。また、各管理者の権限を管理者 1～管理者 4 までのログインユーザー名に割り当てることができます。

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。

例えば、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。

管理者認証のログイン方法については、「操作部での管理者認証でのログインのしかた」を参照してください。

1 Web Image Monitor を起動し、変更したい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 [管理者登録 / 変更] をクリックします。

4 ログインした管理者の管理者番号を変更したい番号にチェックし直し、[OK] をクリックします。

「設定」メニューに戻ります。

ログインした管理者番号に権限がなくなる場合は、エラーが表示されたあと、自動的にログアウトします。

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。

E 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」

ユーザー認証を設定する

ユーザー認証にはユーザーコード認証、ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証の 5 つの認証方法があります。ユーザー認証を使用する場合、操作パネルでいずれか 1 つの認証を選択し、各認証方法に必要な項目を設定します。設定項目は認証方法によってことなります。

ユーザー認証は、Web Image Monitor で設定します。

★重要

- ・ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証を設定するには、ハードディスクが必要です。

↓補足

- ・最大登録件数は 400 件です。
- ・ユーザーコード認証は個人単位ではなくユーザーコードごとの認証を行う場合に使用し、ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証は個人単位の認証を行う場合に使用します。
- ・ユーザーコード認証で使用する 8 桁以内のユーザーコードアカウントは、認証方式をユーザーコード認証からベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証に切り替えた後でも、ログインユーザー名として継続され使用することができます。この場合、ユーザーコード認証にパスワードは無いため、ログインパスワードは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、統合サーバー認証）に切り替えた場合、継続さ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、機器を利用することはできません。ただし、認証できなくても本機のアドレス帳にはユーザーコードアカウントが残ります。
- ・ユーザーコード認証から他の認証方式に切り替える場合、セキュリティの観点から、使用しないアカウントの削除、または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については、Web Image Monitor のヘルプを参照してください。パスワード設定方法については、「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。

📖参照

- ・P.35 「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行う場合に使用する認証方法です。複数のユーザーが同一のユーザーコードを使用することが可能です。

本機に蓄積した文書において、Ridoc Desk Navigator からの配信を制御する場合は、ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証のいずれかを使用してください。ユーザーコードの設定については Web Image Monitor のヘルプを参照してください。

プリンタードライバーのユーザーコード設定については、ソフトウェアガイドまたはプリンタードライバーのヘルプを参照してください。

ユーザーコード認証を設定する

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。

- 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 [ユーザー認証管理] をクリックします。
- 4 「ユーザー認証管理:」のドロップダウンメニューから「ユーザーコード」を選択します。
設定項目が表示されます。
ユーザー認証管理を使用しない場合は「しない」を選択してください。
- 5 「プリンタージョブ認証設定」メニューの「プリンタージョブ認証」でドロップダウンメニューから認証レベルを選択します。

↓ 補足

- ・ [すべて] を選択した場合は、PostScript3 やミニドライバーなど認証機能に対応していないプリンタードライバー、または装置からの印刷はできません。認証機能に対応していない環境からの印刷も行う場合は、[簡易 (限定)] または [簡易] を選択してください。
- ・ [簡易 (限定)] を選択した場合は、プリンタージョブ認証を行わなくても印刷できる機器を設定で限定できます。限定の対象は、パラレル接続、USB 接続、およびクライアントの IP アドレスで設定できます。IP アドレスの場合、その範囲を指定することにより、プリンタージョブ認証を除外することができます。認証に対応していないプリンタードライバーを使いたいときや、プリンタードライバーを利用せずに印刷を行いたいとき等にご利用下さい。限定されている機器以外からの印刷は認証機能に対応している必要があります。
- ・ [簡易] を選択した場合は、認証機能に対応していないプリンタードライバー、または装置からの印刷も許可します。この設定は印刷を指示するプリンタードライバー、または装置が特定できない場合か、プリンターの印刷に対して認証を必要としない場合にご利用下さい。ただし、認証を行わなくても印刷ができるため、機器が想定外のユーザーから不正に使われてしまう可能性があるのご注意下さい。

[簡易]、[すべて] を選択した場合は、手順 11 へ進んでください。

[簡易 (限定)] を設定する場合は手順 6 へ進んでください。

6 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。

IP アドレスの範囲、パラレル接続、USB 接続を設定できます。

IP アドレスの範囲を設定する場合は手順 7 へ進んでください。

パラレル接続の設定をする場合は手順 8 へ進んでください。

USB 接続の設定をする場合は手順 9 へ進んでください。

7 「限定対象 (IPv4)」メニューの「IPv4 アドレス 1」から「IPv4 アドレス 5」のいずれかを選択し IPv4 アドレスを入力します。

終了 IPv4 アドレスには開始 IPv4 アドレスより大きな値を入力してください。
IPv6 環境でご使用の場合は、「限定対象 (IPv6)」メニューで設定してください。

8 「パラレルインターフェース (簡易)」メニューで [対象とする] を選択します。

9 「USB (簡易)」メニューで [対象とする] を選択します。

10 「ユーザーコード設定」メニューの [利用機能] で、ユーザーが使用できる機能を選択し、[OK] キーをクリックします。

「設定」メニューに戻ります。

11 管理者モードからログアウトします。

12 Web Image Monitor を終了します。

補足

- ・ユーザーコード認証は telnet でも設定できます。
- ・拡張 1284 ボードが本体に装着されていない場合、「パラレルインターフェース (簡易)」メニューは表示されません。

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」
- ・P.85 「機能の使用を制限する」

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行う場合に設定します。ベーシック認証による個人認証で本機の機能の使用権を管理できるだけでなく、アドレス帳や蓄積文書などの個人データへのアクセス制限をかけることができます。

ベーシック認証では認証を設定した後に、管理者がアドレス帳に登録されたユーザーごとに本機の利用制限の設定をする必要があります。利用制限の設定については、「アドレス帳の認証情報について」を参照してください。

ベーシック認証は、Web Image Monitor から設定します。

重要

- ・ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証を設定するには、ハードディスクが必要です。

参照

- ・P.34 「アドレス帳の認証情報について」

ベーシック認証を設定する

設定を行う前に、管理者認証管理で管理者認証が設定されていることを確認してください。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。

- 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 [ユーザー認証管理] をクリックします。
- 4 「ユーザー認証管理」のドロップダウンメニューから「ベーシック認証」を選択します。
設定項目が表示されます。
ユーザー認証管理を使用しない場合は [しない] を選択してください。
- 5 「プリンタージョブ認証設定」メニューの「プリンタージョブ認証」でドロップダウンメニューから認証レベルを選択します。

補足

- ・ [すべて] を選択した場合は、PostScript3 やミニドライバーなど認証機能に対応していないプリンタードライバー、または装置からの印刷はできません。認証機能に対応していない環境からの印刷も行う場合は、[簡易 (限定)] または [簡易] を選択してください。
- ・ [簡易 (限定)] を選択した場合は、プリンタージョブ認証を行わなくても印刷できる機器を設定で限定できます。限定の対象は、パラレル接続、USB 接続、およびクライアントの IP アドレスで設定できます。IP アドレスの場合、その範囲を指定することにより、プリンタージョブ認証を除外することができます。認証に対応していないプリンタードライバーを使いたいときや、プリンタードライバーを利用せずに印刷を行いたいとき等にご利用下さい。限定されている機器以外からの印刷は認証機能に対応している必要があります。
- ・ [簡易] を選択した場合は、認証機能に対応していないプリンタードライバー、または装置からの印刷も許可します。この設定は印刷を指示するプリンタードライバー、または装置が特定できない場合か、プリンターの印刷に対して認証を必要としない場合にご利用下さい。ただし、認証を行わなくても印刷ができるため、機器が想定外のユーザーから不正に使われてしまう可能性があるのでご注意下さい。

[簡易]、[すべて] を選択した場合は、手順 10 へ進んでください。

[簡易 (限定)] を設定する場合は手順 6 へ進んでください。

6 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。

IP アドレスの範囲、パラレル接続、USB 接続を設定できます。

IP アドレスの範囲を設定する場合は手順 7 へ進んでください。

パラレル接続の設定をする場合は手順 8 へ進んでください。

USB 接続の設定する場合は手順 9 へ進んでください。

7 「限定対象 (IPv4)」メニューの「IPv4 アドレス 1」から「IPv4 アドレス 5」のいずれかを選択し、IPv4 アドレスを入力します。

終了 IPv4 アドレスには開始 IPv4 アドレスより大きな値を入力してください。
IPv6 環境でご使用の場合は、「限定対象 (IPv6)」メニューで設定してください。

8 「パラレルインターフェース (簡易)」メニューで [対象とする] を選択します。

9 「USB (簡易)」メニューで [対象とする] を選択します。

10 「ベーシック認証設定」メニューの [利用機能] で、ユーザーが使用できる機能を選択し、[OK] キーをクリックします。

ここで最初に設定された指定値が、これ以降にアドレス帳などでユーザーを作成する場合のデフォルト値として設定されます。

「設定」メニューに戻ります。

11 管理者モードからログアウトします。

12 Web Image Monitor を終了します。

↓ 補足

- ・ベーシック認証は telnet でも設定できます。
- ・拡張 1284 ボードが本体に装着されていない場合、「パラレルインターフェース (簡易)」メニューは表示されません。

E 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」
- ・P.85 「機能の使用を制限する」

アドレス帳の認証情報について

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。

「ユーザー認証管理」を設定した場合、個人やグループ単位でのアクセス制限、本機の利用制限を設定することができます。機器の利用制限については、「機能の使用を制限する」を参照してください。

ユーザーが正しく本機を利用できるように、アドレス帳でユーザーごとの設定を行います。事前にユーザーをアドレス帳に登録してください。アドレス帳については、Web Image Monitor のヘルプを参照してください。Ridoc IO Admin を使用して設定することもできます。詳しくは、Ridoc IO Admin のヘルプを参照してください。

E 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」
- ・P.85 「機能の使用を制限する」

ログインユーザー名とログインパスワードを設定する

ユーザー認証管理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。

- 1 Web Image Monitor を起動し、ユーザー管理者にログインします。
- 2 [アドレス帳] をクリックします。
リストが表示されます。
- 3 設定したいユーザーを選択し、[変更] をクリックします。
登録番号、名前 / ヨミガナ、ユーザーコードから検索することができます。
- 4 [ログインユーザー名] を入力します。
- 5 「ログインパスワード」エリアの [変更] をクリックします。
- 6 ログインパスワードを入力し、[OK] をクリックします。
- 7 使用可能にする機能を設定し、[変更] をクリックします。
- 8 レベルを選択し、[OK] をクリックします。
設定を変更したユーザーをグループに加えたい場合は、「グループに追加」の [変更] をクリックし、[OK] をクリックします。
- 9 [戻る] をクリックします。
- 10 管理者モードからログアウトします。
- 11 Web Image Monitor を終了します。

2

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行う場合に設定します。ディレクトリサーバーにアカウントがないユーザーは認証を受けることができません。Windows 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定することが可能です。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することができるため、本機でアドレス帳の個人設定登録をすることなくユーザー認証を可能にします。

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

- ・ハードディスクが必要です。
- ・NTLMv1 認証のみに対応しています。
- ・NTLM 認証を設定する場合は、指定したドメイン内にドメインコントローラが設置されている必要があります。

- ・対応 OS は以下になります。ActiveDirectory 動作時のユーザー情報の取得には LDAP を利用します。その際に SSL を利用する場合は、Windows 上で TLSv1、SSLv2、SSLv3 のいずれかがサーバー上で動作することが必要です。

- ・ Windows NT 4.0 Server
- ・ Windows 2000 Server
- ・ Windows Server 2003

◆ Kerberos 認証の使用条件

- ・ハードディスクが必要です。
- ・Kerberos 認証を設定する場合は、指定したドメイン内にドメインコントローラが設置されている必要があります。
- ・Kerberos 認証を使用するには、KDC（キー配布センター）に対応した OS が必要です。対応 OS は以下になります。ActiveDirectory 動作時のユーザー情報の取得には LDAP を利用します。その際に SSL を利用する場合は、Windows 上で TLSv1、SSLv2、SSLv3 のいずれかがサーバー上で動作することが必要です。
- ・ Windows 2000 Server
- ・ Windows Server 2003

★重要

- ・Windows 認証を設定しているときは、認証の際に、ディレクトリサーバーに登録されているユーザーのメールアドレスなどの情報が自動登録されます。ディレクトリサーバーのメールアドレスなどの情報を編集した後に、認証を行うと編集した情報が上書きされる場合があります。
- ・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することはできませんが、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 を設定していると、メールアドレスは取得できません。
- ・ドメインコントローラに新規ユーザーを作成し、パスワード設定で「次回ログオン時にパスワード変更が必要」を選択した場合は、先にコンピューターよりログオンしてパスワードの変更を行ってください。
- ・Kerberos 認証が選択されていても、認証先のサーバーが NTLM 認証のみに対応している場合は自動的に NTLM 認証に切り替わり認証動作が実行されます。

↓補足

- ・ログインパスワードの大文字、小文字は正しく入力してください。
- ・はじめて利用する場合は、所属するグループに割り当てられている機能を利用できます。グループに登録されていない場合は [* Default Group] に設定されている機能を利用できます。ユーザーごとの機能の制限をしたい場合は事前にアドレス帳で設定を行ってください。
- ・複数のグループに登録されているユーザーは、複数のグループに割り当てられている機能のすべてを利用できます。
- ・2 度目以降に利用する場合は、ユーザーごとに割り当てられた機能と、所属するグループに割り当てられた機能を利用できます。
- ・Windows サーバーで「Guest」アカウントが有効に設定されているときは、ドメインコントローラ上に存在しないユーザーでも認証できます。その際にユーザーはアドレス帳に登録され、[* Default Group] に設定されている機能を利用できます。
- ・Windows 認証では、認証時に SSL の利用をするか、しないかの選択ができます。

- Windows 認証で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 による暗号化された通信を行うことをお勧めします。その場合は事前にドメインコントローラのサーバー証明書を作成する必要があります。証明書の作成方法については、「サーバー証明書を作成する」を参照してください。
- Windows 認証でメールアドレスなどのユーザー情報を SSL による通信を利用せずに自動登録するとき、または自動登録を利用しないときは、証明書の作成は必要ありません。
- Kerberos 認証を使用するには、事前にレلمムの登録が必要です。レلمム名は必ず大文字で登録する必要があります。レلمムの登録方法については、Web Image Monitor のヘルプを参照してください。

E 参照

- P40 「サーバー証明書を作成する」

Windows 認証を設定する

設定を行う前に、管理者認証管理で管理者認証が設定されていることを確認してください。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。

- 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 [ユーザー認証管理] をクリックします。
- 4 「ユーザー認証管理」のドロップダウンメニューから「Windows 認証」を選択します。
設定項目が表示されます。
ユーザー認証管理を使用しない場合は [しない] を選択してください。
- 5 「プリンタージョブ認証設定」メニューの「プリンタージョブ認証」でドロップダウンメニューから認証レベルを選択します。

補足

- [すべて] を選択した場合は、PostScript3 やミニドライバなど認証機能に対応していないプリンタードライバー、または装置からの印刷はできません。認証機能に対応していない環境からの印刷も行う場合は、[簡易 (限定)] または [簡易] を選択してください。
- [簡易 (限定)] を選択した場合は、プリンタージョブ認証を行わなくても印刷できる機器を設定で限定できます。限定の対象は、パラレル接続、USB 接続、およびクライアントの IP アドレスで設定できます。IP アドレスの場合、その範囲を指定することにより、プリンタージョブ認証を除外することができます。認証に対応していないプリンタードライバーを使いたいときや、プリンタードライバーを利用せずに印刷を行いたいとき等にご利用下さい。限定されている機器以外からの印刷は認証機能に対応している必要があります。

- ・ [簡易] を選択した場合は、認証機能に対応していないプリンタードライバー、または装置からの印刷も許可します。この設定は印刷を指示するプリンタードライバー、または装置が特定できない場合か、プリンターの印刷に対して認証を必要としない場合にご利用下さい。ただし、認証を行わなくても印刷ができるため、機器が想定外のユーザーから不正に使われてしまう可能性があるのご注意下さい。

[簡易]、[すべて] を選択した場合は、手順 **10** へ進んでください。

[簡易 (限定)] を設定する場合は手順 **6** へ進んでください。

2

6 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。

IP アドレスの範囲、パラレル接続、USB 接続を設定できます。

IP アドレスの範囲を設定する場合は手順 **7** へ進んでください。

パラレル接続の設定をする場合は手順 **8** へ進んでください。

USB 接続の設定をする場合は手順 **9** へ進んでください。

7 「限定対象 (IPv4)」メニューの「IPv4 アドレス 1」から「IPv4 アドレス 5」のいずれかを選択し、IPv4 アドレスを入力します。

終了 IPv4 アドレスには開始 IPv4 アドレスより大きな値を入力してください。

IPv6 環境でご使用の場合は、「限定対象 (IPv6)」メニューで設定してください。

8 「パラレルインターフェース (簡易)」メニューで [対象とする] を選択します。

9 「USB (簡易)」メニューで [対象とする] を選択します。

10 「Windows 認証設定」メニューで「SSL の利用」を選択し、ドメイン名を入力します。

SSL を利用しない場合は、「利用しない」を選択してください。

Windows サーバー上でグローバルグループを登録していれば、グローバルグループごとの機能利用制限が可能です。あらかじめ Windows サーバー側でグローバルグループを作成し、そのグループに認証するユーザーを登録しておく必要があります。本機ではそのグローバルグループメンバーに許可する機能を登録しておく必要があります。

Windows サーバーに登録したグループと同じ名前でも、本機に大文字小文字を正しく入力してグループを作成してください。作成したグループごとに、本機の機能の利用制限を設定してください。初めて利用した場合、ユーザーは、[Default Group] に設定されている機能が利用できます。[Default Group] は、工場出荷時に全ての機能が利用可能に設定されています。運用にあわせて機能の利用制限を設定してください。

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

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

11 [OK] をクリックします。

「設定」メニューに戻ります。

12 管理者モードからログアウトします。

13 Web Image Monitor を終了します。

補足

- Windows 認証は telnet でも設定できます。
- 拡張 1284 ボードが本体に装着されていない場合、「パラレルインターフェース（簡易）」メニューは表示されません。

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」
- P.85 「機能の使用を制限する」

2

「インターネット インフォメーション サービス (IIS)」と「認証サービス」をインストールする

Active Directory に登録されているメールアドレスを、本機に自動で取得する場合に設定してください。

Windows のコンポーネントとして「インターネット インフォメーション サービス (IIS)」と「認証サービス」をインストールすることをお勧めします。

インストールされていない場合は下記の手順でコンポーネントを追加してください。
インストールされている場合は、サーバー証明書を作成してください。

- 1 「コントロールパネル」から [アプリケーションの追加と削除] を選択します。
- 2 [Windows コンポーネントの追加と削除] を選択します。
- 3 インストールする Windows コンポーネントとして、「インターネット インフォメーション サービス (IIS)」をチェックします。
- 4 「認証サービス」をチェックし、[次へ] をクリックします。
インストールが開始されます。
- 5 インストール開始直後に警告が表示されますので、[はい] をクリックします。
- 6 証明機関の種類を選択し、[次へ] をクリックします。
ここでは [エンタープライズルート CA] を選択します。
- 7 CA 識別情報は CA の名前 (任意) のみ入力し、[次へ] をクリックします。
- 8 データ記憶域の保管場所はデフォルトのまま、[次へ] をクリックします。
以上で「インターネット インフォメーション サービス (IIS)」と「認証サービス」のインストールは完了となります。

サーバー証明書を作成する

「インターネット インフォメーション サービス (IIS)」と「認証サービス」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。

- 1 「インターネット サービス マネージャ」を起動します。
- 2 [既定の Web サイト] を右クリックし、[プロパティ] を選択します。
- 3 [ディレクトリ セキュリティ] タブの [サーバー証明書] を選択します。
- 4 「サーバー証明書ウィザード」が起動しますので、[次へ] をクリックします。
- 5 [証明書の新規作成] を選択し、[次へ] をクリックします。
- 6 [証明書の要求を作成して後で送信する] を選択し、[次へ] をクリックします。
- 7 [次へ] をクリックします。
- 8 「組織」、「部門名」を入力します。
- 9 「一般名」としてコンピューター名が表示されますのでデフォルトのまま次へ進みます。
- 10 「国 / 地域」、「都道府県」、「市町村」情報を入力します。
- 11 「要求ファイルの概要を請求」として設定した情報が表示されますので、内容を確認して次へ進みます。
以上でサーバー証明書の作成は完了となります。

機器証明書の導入（認証局証明書）

Web Image Monitor を使用し、機器証明書を導入します。

機器証明書に、認証局証明書を利用する場合の説明です。認証局から送られてきた機器証明書の内容を導入します。

- 1 Web ブラウザーを起動します。
- 2 Web ブラウザーのアドレスバーに「http:// (本機の IP アドレス、またはホスト名) /」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。
「192.168.001.010」と入力すると、本機に接続できません。
- 3 [ログイン] をクリックします。
ネットワーク管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティ」の [機器証明書] をクリックします。

「機器証明書」エリアが表示されます。

5 導入する証明書番号を選択します。

6 [導入] をクリックします。

7 機器証明書の内容を入力します。

「証明書要求」の入力ボックスに認証局から送られてきた機器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。

8 [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] をクリックします。

LDAP 認証

LDAP サーバーを使用して、LDAP サーバーにアカウントを持つユーザーの認証を行う場合に設定します。LDAP サーバーにアカウントがないユーザーは認証を受けることができません。LDAP サーバーに登録されているアドレス帳を本機に自動で登録することができるため、本機でアドレス帳の個人設定登録をすることなくユーザー認証を可能にします。

LDAP 認証ではユーザー名、パスワードの情報がネットワーク上に平文で流れるのを防止するために、認証を行うには本機と LDAP サーバーが SSL による暗号化された通信を行うことをお勧めします。その場合は事前に LDAP サーバーのサーバー証明書を作成する必要があります。証明書の作成方法については、「サーバー証明書を作成する」を参照してください。SSL の利用設定は LDAP サーバーの設定で行います。

SSL サーバーにアクセスする際に接続先サーバーが信頼できるかのチェックを行うサーバーチェック機能の設定を Web Image Monitor から行えます。詳しくは Web Image Monitor のヘルプを参照してください。

◆ LDAP 認証の使用条件

LDAP 認証を設定する場合は、以下の条件が必要です。

- ・ハードディスクが搭載されている
- ・本機が LDAP サーバーを認識できる環境に接続されている
- ・SSL 使用時には、TLSv1、SSLv2、SSLv3 のいずれかが LDAP サーバー上で動作する
- ・本機に LDAP サーバーが登録されており、以下の項目がすべて設定されている
 - ・サーバー名
 - ・検索開始位置
 - ・ポート番号
 - ・SSL
 - ・認証^{*1}
 - ・文字コード

^{*1} 認証は [Kerberos 認証]、[ダイジェスト認証]、[平文認証] のいずれかに設定してください。

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

★重要

- LDAP 認証を運用する場合、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等を本機で編集した場合は、続く認証時の再取得により、メールアドレス等が書き込まれてしまう場合がありますので注意してください。
- LDAP 認証はディレクトリサーバー側に登録されたグループごとにアクセス制限を設定することはできません。
- LDAP 認証を使用する場合は、LDAP 検索時に SSL 設定されたサーバーに対しては、参照機能の利用ができません。
- ユーザーのログインユーザー名は 128 文字以内、ログインパスワードは 128 文字以内で入力してください。ログインユーザー名の先頭から 32 文字はユーザーごとに異なる文字列を使用してください。

↓補足

- 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を行うことができます。
- LDAP 簡易認証時に空パスワードでのログインを禁止することができます。詳しくはサービス実施店にお問い合わせください。
- LDAP 認証を使用する場合、LDAP サーバーの設定で匿名認証を禁止にしていないときは、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可能性があります。
- 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場合があります。このような環境で使用される場合は Windows 認証の利用をお勧めします。
- 設定後に未登録のユーザーが初めて本機を利用した場合、本機にユーザーが新規登録され、LDAP 認証設定時に「使用できる機能」で設定した機能が使用可能になります。ユーザーごとに利用できる機能を制限する場合は、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、新規登録後にユーザーごとに「使用できる機能」を変更してください。2 度目以降の利用時には、ユーザーごとの「使用できる機能」の設定は維持されます。
- Active Directory を使用して LDAP 認証を行う場合、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 の認証方式で Kerberos 認証を選択するには、事前にレルムの登録が必要です。レルム名は必ず大文字で登録する必要があります。レルムの登録方法については、Web Image Monitor のヘルプを参照してください。

📖参照

- P.40 「サーバー証明書を作成する」

LDAP 認証を設定する

設定を行う前に、管理者認証管理で管理者認証が設定されていることを確認してください。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。

- 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 [ユーザー認証管理] をクリックします。
設定項目が表示されます。
ユーザー認証管理を使用しない場合は [しない] を選択してください。
- 4 「ユーザー認証管理」のドロップダウンメニューから「LDAP」を選択します。
- 5 「プリンタージョブ認証設定」メニューの「プリンタージョブ認証」でドロップダウンメニューから認証レベルを選択します。

補足

- ・ [すべて] を選択した場合は、PostScript3 やミニドライバーなど認証機能に対応していないプリンタードライバー、または装置からの印刷はできません。認証機能に対応していない環境からの印刷も行う場合は、[簡易 (限定)] または [簡易] を選択してください。
- ・ [簡易 (限定)] を選択した場合は、プリンタージョブ認証を行わなくても印刷できる機器を設定で限定できます。限定の対象は、パラレル接続、USB 接続、およびクライアントの IP アドレスで設定できます。IP アドレスの場合、その範囲を指定することにより、プリンタージョブ認証を除外することができます。認証に対応していないプリンタードライバーを使いたいときや、プリンタードライバーを利用せずに印刷を行いたいとき等にご利用下さい。限定されている機器以外からの印刷は認証機能に対応している必要があります。
- ・ [簡易] を選択した場合は、認証機能に対応していないプリンタードライバー、または装置からの印刷も許可します。この設定は印刷を指示するプリンタードライバー、または装置が特定できない場合か、プリンターの印刷に対して認証を必要としない場合にご利用下さい。ただし、認証を行わなくても印刷ができるため、機器が想定外のユーザーから不正に使われてしまう可能性があるのでご注意下さい。

[簡易]、[すべて] を選択した場合は、手順 10 へ進んでください。

[簡易 (限定)] を設定する場合は手順 6 へ進んでください。

6 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。

IP アドレスの範囲、パラレル接続、USB 接続を設定できます。

IP アドレスの範囲を設定する場合は手順 7 へ進んでください。

パラレル接続の設定をする場合は手順 8 へ進んでください。

USB 接続の設定する場合は手順 9 へ進んでください。

7 「限定対象 (IPv4)」メニューの「IPv4 アドレス 1」から「IPv4 アドレス 5」のいずれかを選択し、IPv4 アドレスを入力します。

終了 IPv4 アドレスには開始 IPv4 アドレスより大きな値を入力してください。
IPv6 環境でご使用の場合は、「限定対象 (IPv6)」メニューで設定してください。

8 「パラレルインターフェース (簡易)」メニューで [対象とする] を選択します。

9 「USB (簡易)」メニューで [対象とする] を選択します。

10 「LDAP 認証設定」メニューで認証 LDAP で認証に使用する LDAP サーバーを選択し、[ログイン名属性] [一意属性] を入力します。

ログイン名属性は、認証ユーザーの情報取得のための検索条件として利用します。ログイン名属性で検索フィルターを作成して、ユーザーを特定してそのユーザーの情報を LDAP サーバーから本機のアドレス帳へ取得します。DN 形式で認証する場合は、ログイン名属性を登録する必要はありません。お使いの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。お使いのサーバー環境をご確認の上、入力してください。

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為に設定します。一意属性を本機で設定する事により、LDAP サーバーで一意属性が同一のユーザー情報は、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的な情報の管理に使用している属性を指定します。serialNumber、uid 等で、一意であれば cn や employeeNumber でも可能です。一意属性を指定しない場合は、ユーザーが特定されず、異なるログイン名で同じユーザー情報をもつアカウントが本機に作成されることがあります。

11 「利用機能」を選択し、[OK] をクリックします。

「設定」メニューに戻ります。

12 管理者モードからログアウトします。

13 Web Image Monitor を終了します。

↓ 補足

- LDAP 認証は telnet でも設定できます。
- 初めて LDAP 認証を行ったユーザーは、本機にユーザーのアドレス帳が新規登録され、初期状態で LDAP 認証設定時に「認証時の利用可能機能」で設定した機能が利用可能になります。
- LDAP 認証時、ユーザーごとに利用可能な機能を制限したい場合は、本機に登録されている各ユーザーのアドレス帳において「認証時の利用可能機能」をそれぞれ設定してください。
- 初回以降の LDAP 認証では、各ユーザーのアドレス帳において「認証時の利用可能機能」の設定は維持されます。
- 拡張 1284 ボードが本体に装着されていない場合、「パラレルインターフェース (簡易)」メニューは表示されません。

E 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」
- P.85 「機能の使用を制限する」

統合サーバー認証

統合サーバーは外部認証装置の窓口となり、ネットワーク上のサーバーにおける利用者の認証を一括して行い、サーバーに依存しない一元的なユーザー認証環境を構築することで、使い勝手のよい安全で快適な運用を可能にします。サーバーに登録されているアドレス帳を本機にダウンロードすることができるため、本機でアドレス帳の個人設定登録をすることなくユーザー認証を可能にします。

[統合サーバー認証]を使用する場合は、本機以外に Ridoc IO OperationServer などがインストールされているサーバーが必要です。

ソフトウェアについては、販売店にお問い合わせください。

SSL サーバーにアクセスする際に接続先サーバーが信頼できるかのチェックを行うサイト証明書チェック機能の設定を Web Image Monitor から行えます。詳しくは Web Image Monitor のヘルプを参照してください。

★ 重要

- ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証を設定するには、ハードディスクが必要です。
- 統合サーバー認証を運用する場合に、認証成功後に自動保存した認証済みユーザーのメールアドレス等を本機で編集した場合は、続く認証時の再取得により、メールアドレス等が上書きされてしまう場合がありますので注意してください。
- Ridoc Document Systemの管理者名は、ソフトウェアがインストールされているサーバー側では「Admin」、本機では「admin」とデフォルトが異なります。

統合サーバー認証を設定する

設定を行う前に、管理者認証管理で管理者認証が設定されていることを確認してください。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。

ここでは本機の設定を説明しています。

詳細は、認証管理ツールの使用説明書を参照してください。

- 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 [ユーザー認証管理] をクリックします。
設定項目が表示されます。
ユーザー認証管理を使用しない場合は [しない] を選択してください。

4 「ユーザー認証管理」のドロップダウンメニューから「統合サーバー認証」を選択します。

5 「プリンタジョブ認証設定」メニューの「プリンタジョブ認証」でドロップダウンメニューから認証レベルを選択します。

↓ 補足

- ・ [すべて] を選択した場合は、PostScript3 やミニドライバなど認証機能に対応していないプリンタードライバ、または装置からの印刷はできません。認証機能に対応していない環境からの印刷も行う場合は、[簡易 (限定)] または [簡易] を選択してください。
- ・ [簡易 (限定)] を選択した場合は、プリンタジョブ認証を行わなくても印刷できる機器を設定で限定できます。限定の対象は、パラレル接続、USB 接続、およびクライアントの IP アドレスで設定できます。IP アドレスの場合、その範囲を指定することにより、プリンタジョブ認証を除外することができます。認証に対応していないプリンタードライバを使いたいときや、プリンタードライバを利用せずに印刷を行いたいとき等にご利用下さい。限定されている機器以外からの印刷は認証機能に対応している必要があります。
- ・ [簡易] を選択した場合は、認証機能に対応していないプリンタードライバ、または装置からの印刷も許可します。この設定は印刷を指示するプリンタードライバ、または装置が特定できない場合か、プリンタの印刷に対して認証を必要としない場合にご利用下さい。ただし、認証を行わなくても印刷ができるため、機器が想定外のユーザーから不正に使われてしまう可能性があるのご注意下さい。

[簡易]、[すべて] を選択した場合は、手順 **17** へ進んでください。

[簡易 (限定)] を設定する場合は手順 **6** へ進んでください。

6 プリンタジョブ認証を簡易として扱う対象範囲を限定します。

IP アドレスの範囲、パラレル接続、USB 接続を設定できます。

IP アドレスの範囲を設定する場合は手順 **7** へ進んでください。

パラレル接続の設定をする場合は手順 **8** へ進んでください。

USB 接続の設定をする場合は手順 **9** へ進んでください。

7 「限定対象 (IPv4)」メニューの「IPv4 アドレス 1」から「IPv4 アドレス 5」のいずれかを選択し、IPv4 アドレスを入力します。

終了 IPv4 アドレスには開始 IPv4 アドレスより大きな値を入力してください。

IPv6 環境でご使用の場合は、「限定対象 (IPv6)」メニューで設定してください。

8 「パラレルインターフェース (簡易)」メニューで [対象とする] を選択します。

9 「USB (簡易)」メニューで [対象とする] を選択します。

10 「統合サーバー認証設定」メニューで「SSL の利用」を [する] または [しない] にします。

「SSL の利用」は認証管理ツールの設定に合わせてください。

11 [統合サーバー名] を入力します。

外部認証に用いるサーバー名を設定します。
IPv4 アドレス、またはホスト名を入力します。

12 「認証種別」 をドロップダウンメニューから選択します。

利用可能な実際の認証方法から選択します。

13 「URL 取得」メニューで、「サーバー名」で設定されているサーバーの URL 取得状態を表示します。

URL 取得後に「サーバー名」や SSL の利用設定が変更された場合は、URL の取得状態は未取得となります。

14 [ドメイン名] を入力します。

ドメイン非対応の認証方式にドメインを指定しても無効になります。
ドメイン非対応の認証方式の場合は手順 **15**に進んでください。

15 「グループ設定 (統合サーバー認証)」メニューで [グループ名] を入力し、利用できる機能を選択します。

グループごとの利用制限が可能です。グループごとに許可する機能を登録しておく必要があります。

認証種別で、Windows を選択した場合は、グローバルグループ、Notes を選択した場合は、Notes グループ、ベーシック (統合サーバー) を選択した場合は、認証管理ツールで作成したグループが利用できます。

16 [OK] をクリックします。

「設定」メニューに戻ります。

17 管理者モードからログアウトします。**18** Web Image Monitor を終了します。**↓** 補足

- 拡張 1284 ボードが本体に装着されていない場合、「パラレルインターフェース (簡易)」メニューは表示されません。

目 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」
- P.85 「機能の使用を制限する」

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について

ここでは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について説明しています。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組み合わせによっては、正しく印刷されない場合があります。ご使用の環境に合わせて設定してください。

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、RPDL、RP-GL/2、PCL です。

◆ 組み合わせ一覧

本機の各設定項目			プリンタージョブの種類									
[ユーザー認証管理]	[プリンタージョブ認証]	[簡易暗号化使用制限]	1	2	3	4	5	6	7	8	9	
[認証しない]	-	-	☆	☆	☆	☆	☆	☆	☆	☆	☆	
[ユーザーコード認証]、[ベーシック認証]、[Windows 認証]、[LDAP 認証]、[統合サーバー認証]	[簡易]	[しない]	●	○	×	☆	☆	☆	○	☆	●	
		[する]		×								
	[すべて]	[しない]	●	○								
		[する]		×	×	○	×	×	○	×	●	

☆: ユーザー認証に関係なく印刷できます。

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

●: ユーザー認証が通り、プリンタードライバーと本機の [ドライバー暗号鍵] が一致していれば印刷できます。一致していなければ、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。

「簡易暗号化使用制限」については、「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。

◆ [プリンタージョブ認証]

・ [すべて]

全てのプリンタージョブ、およびリモートからの設定に対し認証のチェックを行い、認証が得られないジョブおよび設定に対しては、処理を行いません。

プリンタージョブの場合: ジョブリセット

設定の場合: 無効

・ [簡易]

認証情報の付加されたプリンタージョブ、および認証情報が付加されたりリモートからの設定に対しては認証チェックを行い、認証が得られないプリンタージョブ、および設定に対しては処理を行いません。認証の付加されないプリンタージョブ、および認証の付加されない設定に対しては、認証チェックを行わず、ジョブの実行および設定を行います。

・ [簡易 (限定)]

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

◆ プリンタージョブの種類

- 1) RPCS プリンタードライバーの設定で、[印刷時に認証情報を確認する] をチェックし、さらに[暗号化する] をチェックした場合です。PCL 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] をチェックした場合です。プリンタージョブに個人認証情報が付加されている状態です。ログインパスワードはプリンタードライバーで高度な暗号化が行われます。プリンタードライバー暗号鍵を使用することで、ログインパスワードが明かになるのを防止することができます
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。「簡易暗号化使用制限」については、「セキュリティ強化機能を設定する」を参照してください。
- 2) RPCS プリンタードライバーの設定で、[印刷時に認証情報を確認する] をチェックした場合です。PCL 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] をチェックした場合です。プリンタージョブに個人認証情報が付加されている状態です。ログインパスワードはプリンタードライバーで簡単な暗号化が行われます。
「簡易暗号化使用制限」については、「セキュリティ強化機能を設定する」を参照してください。
- 3) RPCS プリンタードライバーの設定で、[印刷時に認証情報を確認する] をチェックしない場合です。PCL プリンタードライバーの設定で、[ユーザー認証] をチェックをチェックした場合です。プリンタージョブに個人認証情報が付加されて無効になっている状態です。
- 4) PostScript 3 プリンタードライバーのプリンタージョブで、ユーザコードの情報を含んでいる場合です。プリンタージョブに個人認証情報が付加されていませんがユーザコードの情報が付加されている状態です。他機種の認証機能に対応していないRPCS / PCL プリンタードライバーから、本機に対して代行印刷を行った場合も同様です。
- 5) PostScript 3 プリンタードライバーのプリンタージョブで、ユーザコードの情報を含まない場合です。プリンタージョブに個人認証情報、およびユーザコードの情報が付加されていない状態です。他機種の認証機能に対応していないRPCS / PCL プリンタードライバーから、本機に対して代行印刷を行った場合も同様です。
- 6) BMLinkS プリンタードライバーのプリンタージョブ、プリンタードライバーを使用しないホストやPCからのプリンタージョブ、およびPDFをLPR印刷した場合です。プリンタージョブに個人認証情報が付加されていない状態です。
- 7) PDFをFTPまたはSFTP印刷した場合です。FTPまたはSFTP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。SFTPではユーザーIDとパスワードは暗号化されますが、FTPでは暗号化されません。

E 参照

- P.129 「セキュリティ強化機能を設定する」

ユーザー認証が設定されているとき

ユーザー認証（ユーザーコード認証、ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証）が設定されているときは、画面に認証画面が表示されます。個人ごとに設定されたログインユーザー名とログインパスワードを入力しないと、本機を操作できません。本機を操作できる状態になることをログインといいます。また、操作できる状態を解除することをログアウトといいます。ログインして操作が終了したときは、不正に使用できないよう必ずログアウトしてください。オートログアウト時間設定が設定されていると、一定時間画面を操作しないときは、自動的にログアウトされます。また、外部機器を使用して認証を行うこともできます。

オートログアウト時間設定については、「オートログアウト時間設定について」を参照してください。

外部機器を使用した認証については、「外部機器を使用した認証について」を参照してください。

補足

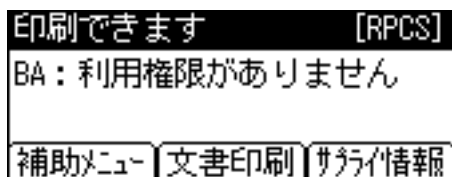
- ・ログインユーザー名、ログインパスワード、ユーザーコードは、ユーザー管理者に確認してください。
- ・ユーザーコード認証のときに、ユーザーコードとして入力するのは、アドレス帳に [ユーザーコード] として登録されている数字です。

参照

- ・P55 「オートログアウト時間設定について」
- ・P56 「外部機器を使用した認証について」

操作部からのユーザーコード認証のしかた

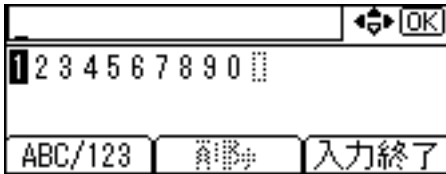
ユーザーコード認証を設定しているときは、次の画面が表示されます。



■ ログインのしかた

- 1 [メニュー] キーを押します。
- 2 [ログイン] を押します。

- 3 ユーザーコード (1桁から8桁の任意の数字) を入力して、[入力終了] を押します。



■ ログアウトのしかた

- 1 [メニュー] キーを押します。
- 2 [ログアウト] を押します。
- 3 [する] を押します。

ドライバーからのユーザーコード認証のしかた

ユーザーコード認証が設定されているときは、各ドライバーのプロパティ画面でユーザーコードを設定します。各ドライバーの操作については、各ドライバーのヘルプを参照してください。

操作部からのログインのしかた

ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証のいずれかが設定されているときにログインします。

- 1 [メニュー] キーを押します。
- 2 [ログイン] を押します。
「ログインユーザー名を入力してください。」と表示されます。
- 3 [入力] を押します。
- 4 ログインユーザー名を入力して、[入力終了] を押します。
「ログインパスワードを入力してください。」と表示されます。
- 5 [入力] を押します。
- 6 ログインパスワードを入力して、[入力終了] を押します。
認証に成功したときは、各機能の画面が表示されます。

操作部からのログアウトのしかた

ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証のいずれかが設定されているときにログアウトします。

- 1 [メニュー] キーを押します。
- 2 [ログアウト] を押します。
- 3 [する] を押します。

ドライバーからのログインのしかた

ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証のいずれかが設定されているときは、各ドライバーのプロパティで暗号化の設定をしてから、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。各ドライバーの設定については、各ドライバーのヘルプを参照してください。

↓ 補足

- ・ドライバーからログインしたときは、ログアウトする必要はありません。

Web Image Monitor からのログインのしかた

Web Image Monitor からログインする方法について説明します。

- 1 Web Image Monitor のトップページで [ログイン] をクリックします。
- 2 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

- ・ユーザーコード認証のときは、ログインユーザー名にユーザーコードを入力し、[OK] をクリックします。

Web Image Monitor からのログアウトのしかた

Web Image Monitor からログアウトするときは、[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。

ログイン時のロックアウト機能について

ログイン時にパスワードを連続して間違えて入力すると、ロックアウト機能が働き、そのユーザー名でのログインが禁止されます。ロックアウトされたユーザーは、正しいパスワードを入力した場合も認証失敗となり、機器が利用できなくなります。

ユーザー認証でロックアウト機能を使用するには、認証方法がベーシック認証に設定されている必要があります。他の認証選択時では、スーパーバイザーと各管理者のみがロックアウトの対象となり、一般ユーザーには機能しません。

2

◆ パスワードロックアウト機能の設定項目

ロックアウト機能の設定は Web Image Monitor で行います。

設定項目	設定内容	設定値	工場出荷時の設定値
ロックアウト	ロックアウト機能を有効にするかしないかを設定します。	・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、スーパーバイザー	機器管理者
機器管理者	スーパーバイザー

パスワードロックアウト設定

機器管理者が設定します。

パスワードロックアウトの設定は Web Image Monitor で行います。

1 Web ブラウザーを起動します。

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

IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。

「192.168.001.010」と入力すると、本機に接続できません。

3 [ログイン] をクリックします。

機器管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。

4 [設定] をクリックし、「セキュリティ」の [ユーザーロックアウト] をクリックします。

「ユーザーロックアウト」エリアが表示されます。

5 「ロックアウト」で [有効] を選択します。

6 「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。

7 ロックアウト後、一定時間で解除したいときは「ロックアウト解除タイマー」で [有効] を選択します。

8 「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。

9 [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。

10 [ログアウト] をクリックします。

パスワードロックアウト解除設定

パスワードロックアウト対象者の解除権利を保有する管理者が設定します。

- 1 Web ブラウザーを起動します。
- 2 Web ブラウザーのアドレスバーに「http:// (本機の IP アドレス、またはホスト名) /」と入力し、本機にアクセスします。
IPv4 アドレスを入力する場合、各セグメントの先頭につく「0」は入力しないでください。例えば「192.168.001.010」の場合は、「192.168.1.10」と入力します。「192.168.001.010」と入力すると、本機に接続できません。
- 3 [ログイン] をクリックします。
ロックアウト対象者の解除権利を保有する管理者がログインします。ログインユーザー名とログインパスワードを入力し、ログインしてください。
- 4 [アドレス帳] をクリックします。
「アドレス帳」エリアが表示されます。
- 5 ロックアウトを解除するユーザーを選択します。
- 6 [変更] をクリックします。
- 7 「認証情報」の「ロックアウト」の「無効」にチェックを入れます。
- 8 [OK] をクリックします。
パスワードロックアウトが解除されます。
- 9 [ログアウト] をクリックします。

オートログアウト時間設定について

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。

「ユーザー認証管理」を使用している場合に一定時間、画面の操作を行わなかったときに、自動的にログアウトします。これを「オートログアウト」といいます。

オートログアウト機能が働くまでの時間を設定します。

- 1 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 [タイマー] をクリックします。
- 4 「オートログアウト時間設定」で [する] を選択します。
オートログアウト時間設定を設定しない場合は「しない」を選択してください。

5 オートログアウトするまでの時間を「60～999」（1 秒単位）の範囲で入力し、[OK] をクリックします。

「設定」メニューに戻ります。

6 管理者モードからログアウトします。

7 Web Image Monitor を終了します。

↓ 補足

- ・紙づまりやトナー切れなどの時には、オートログアウトが働かない場合があります。

E 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」

外部機器を使用した認証について

この機能を利用するにはオプションの IC カード認証が必要です。

ベーシック認証、Windows 認証、LDAP 認証、統合サーバー認証のいずれかが設定され、拡張認証管理が [する] に設定されているときに、IC カードを使用して認証をすることができます。ただし、FeliCa ID を使用して認証する場合はベーシック認証に設定されている必要があります。

IC カードを使用した管理者、およびユーザーのログイン、ログアウトの方法については、IC カード認証の使用説明書を参照してください。

★重要

- ・IC カードを使用してユーザー認証を行うときは、事前にアドレス帳にユーザー名を登録しておく必要があります。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。アドレス帳へのユーザーの登録方法については、Ridoc IO Admin、Web Image Monitor のヘルプ、または Ridoc IO OperationServer の使用説明書を参照してください。

IC カード認証システムを使用する

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。

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] を押します。

3 [▲][▼] キーを押して [拡張認証管理] を選択し、[OK] を押します。

4 [▲][▼] キーを押して [する] を選択します。

E 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」