1. はじめに

セキュリティー機能をご使用になる前に

重要

・機器のセキュリティー設定を行わない場合には、悪意を持った攻撃者により被害を受ける可能性があります。

1) 本機が持ち出されたり壊されたりすることなどがないように、セキュリティー管理の行き届いた環境に本機を設置してください。
2) 本機購入者は、本機を適切に運用してくれる方を、管理者として選定し運用してください。管理者の方が適切な運用を行わない場合、ユーザーの方にセキュリティー上の被害が発生する恐れがあります。
3) 管理者の方はセキュリティー機能をご使用になる前に、この使用説明書「セキュリティー編」を最後までよくお読みの上、正しくお使いください。特に、「セキュリティー機能をご使用になる前に」はよく読んでご理解ください。
4) 管理者の方は、ユーザーの方がセキュリティー機能を正しくお使いいただけるように、利用方法をご指導ください。
5) 例外や異常な動作の確認のためには、定期的なログ情報の監査をお勧めします。
6) 本機をネットワークに接続する場合は、ファイアウォール等によって保護された環境でお使いください。
7) 通信中のデータを守るために、本機でセキュリティー通信機能を利用する場合は、暗号化機能等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。

まずはじめに

より高度なセキュリティーを希望される場合は本機を使用される前に以下の設定を速やかに行ってください。情報の暗号化通信を有効にし、管理者アカウントを設定します。

1

1 本機の電源を入れます。

2 [メニュー] キーを押します。

3 [▲] [▼] キーを押して [インターフェース設定] を選択し、[OK] キーを押します。

4 [▲] [▼] キーを押して [ネットワーク設定] を選択し、[OK] キーを押します。

5 本体 IP アドレスを設定します。

6 本機をネットワークに接続します。

7 Web Image Monitor を起動し、管理者としてログインします。
Web Image Monitor のログイン方法は、「Web Image Monitor のログインのしかた」を参照してください。

8 機器証明書を導入します。
機器証明書の導入方法は、「通信経路の保護と暗号化通信」を参照してください。

9 SSL を有効にします。
SSL を有効にする設定については、「SSL を有効にする」を参照してください。

10 管理者のユーザー名、パスワードを変更します。
※ 6 ～ 9 の手順の操作中は工場出荷時に設定された管理者アカウントがネットワーク上を平文で流れるため、場合によってはこのアカウントを用いてネットワークから攻撃されてしまう恐れがあります。
この状態を危険と判断される場合は、手順 6 でネットワーク接続を行う前に、一度限り使用するパスワードを事前に設定しておき、Web Image Monitor への初回アクセス時にパスワードも使用してログインすることをお勧めします。管理者のユーザー名、パスワードの設定については、「管理者を登録する」を参照してください。

補足

・IP アドレスの設定方法は、『ハードウェアガイド』を参照してください。

参照

・P.52 「Web Image Monitor からのログインのしかた」
・P.101 「通信経路の保護と暗号化通信」
・P.105 「SSL を有効にする」
・P.26 「管理者を登録する」

セキュリティーに関する強化機能

本機では、認証機能の拡張により機器の管理、ユーザーの管理を実現することでセキュリティー機能を強化しています。本機の機能や本機で扱う文書、各種データに対してのアクセス制限を設定し、情報漏洩や第三者の不正操作の介入を防止することができます。また、暗号化技術を利用し、ネットワーク上での不正アクセスや利用者の成りすまし、データの解析、改ざんの脅威から保護することができます。その他に、本機の電源スイッチを入れたときにファームウェア構成と提供元を自動的に確認しています。ファームウェアをインストールする時も同様です。

♦ 認証機能とアクセス制限

認証機能を有効にし本機を運用すると、管理者による本機の管理と本機を使用するユーザーの管理ができます。認証機能を有効にするためには、管理者の登録やユーザーの個人情報の登録が必要になり、本機を使用するとき、ログインユーザー名とログインパスワードによって個人を確認するようになります。

管理者は、4 種類に分けて役割が定義されており、本機の各種の機能設定やユーザーの登録など、本機を管理します。

ユーザーは、管理者によりアクセス制限が設定され、本機の機能や本機に蓄積された文書や各種データの使用に制限がかけられます。

管理者とユーザーの関係については、「管理者とユーザー」を参照してください。

♦ 暗号化技術

ネットワークの各種の通信形態に対して、通信経路の保護、通信データの暗号化、パスワードの暗号化に対応することができます。

参照

・P.17 「管理者とユーザー」

用語集

♦ 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。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。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。
管理者は、本機の各種設定と管理が役割となり、文書のコピーや印刷など通常の機能は使用できません。

♦ 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。

♦ 文書作成者（オーナー）
本機に文書を蓄積したユーザーです。蓄積した文書の閲覧、編集、削除の権限を、他のユーザーに対して設定・変更することができます。

♦ アドレス帳登録者
アドレス帳に個人情報を登録されたユーザーです。ユーザーのログインユーザー名とログインパスワードを認知している本人になります。

♦ 管理者認証
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管理者を確認する仕組みです。

♦ ユーザー認証
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によってユーザーを確認する仕組みです。ログインユーザー名とログインパスワードは本機のアドレス帳により管理されます。また個人情報は、本機とネットワークで接続された Windows のドメインコントローラ（Windows 認証）、LDAP サーバー（LDAP 認証）、統合サーバー（統合サーバー認証）から取得することができます。統合サーバーとは、認証管理ツールがインストールされている PC のことです。

♦ ログイン
管理者認証、およびユーザー認証のための操作です。本機の操作パネルで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。また、ネットワークから本機にアクセスするときや、Web Image Monitor や Ridoc IO Admin などのユーティリティーを使用するときにも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。

♦ ログアウト
管理者認証、およびユーザー認証のための操作です。本機との接続を切り、各種操作設定の使用を終了するときに行います。

本機でできるセキュリティー対策

認証機能の利用とユーザー管理

♦ 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。認証機能の設定については、「認証機能の設定」を参照してください。

♦ ログイン認証情報を設定する

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。ログイン認証情報の設定については、「ベーシック認証」を参照してください。

♦ 使用できる機能を設定する

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。使用できる機能の設定については、「使用できる機能を設定する」を参照してください。

参照

・P.22 「認証機能の設定」
・P.32 「ベーシック認証」
・P.85 「使用できる機能を設定する」

情報の漏洩を防ぐ

♦ 文書の複製を抑止する

プリンター機能の不正コピー抑止機能を使用し、不正コピーを抑止するために文字列の地紋をつけて印刷できます。不正コピー抑止機能については、「文書の複製を抑止・ガードする」を参照してください。

♦ 文書の複製をガードする

プリンター機能のコピーガード機能を使用し、不正コピーをガードするために地紋を背景全体につけて印刷できます。

不正コピーガード文書を本機でコピーや蓄積をしたときに、文書をグレー地にする効果を得るためには、オプションの不正コピーガードモジュールが必要です。不正コピーガード機能については、「文書の複製を抑止・ガードする」を参照してください。

♦ **文書を他人に見せないように印刷する**

プリンター機能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。本機の操作パネルで印刷を指示し、印刷した文書をすぐに本人が回収するため、他人に見られることを防止することができます。機密印刷機能については、「文書を他人に見せないように印刷する」を参照してください。

♦ **アドレス帳の登録情報を保護する**

アドレス帳のデータに対して、ユーザーのアクセス権を設定することができます。登録されたユーザー以外の第三者によるアドレス帳のデータの不正利用を防止することができます。

また、アドレス帳のデータを暗号化し、データの読み取りを防止することができます。

アドレス帳のアクセス権設定と暗号化については、「アドレス帳の登録情報を保護する」を参照してください。

♦ **ログ情報の管理**

本機に記憶されたログを消去することでデータの漏洩を防止したり、ログデータを転送することで、不正読み取り履歴や読み取り者の確認ができます。

ログデータを転送するためには Ridoc IO OperationServer が必要です。

ログデータの転送については、「ログ情報の管理」を参照してください。

♦ **蓄積データを暗号化する**

本機に蓄積されるデータを暗号化して、情報の漏洩を防止します。

蓄積データを暗号化するためには、オプションの蓄積文書暗号化カードが必要です。

蓄積データの暗号化については、「蓄積データを暗号化する」を参照してください。

♦ **ハードディスクのデータを上書き消去する**

本機を廃棄するときに、ハードディスクに蓄積されていたすべてのデータを上書き消去することや、一時的に保存していたデータを自動で上書き消去することで、データ漏洩を防止することができます。

ハードディスクのデータを上書き消去するためには、オプションのセキュリティーカードが必要です。

ハードディスクデータの上書き消去については、「ハードディスクのデータを上書き消去する」を参照してください。

参照

・P.57 「文書の複製を抑止・ガードする」
・P.62 「文書を他人に見せないように印刷する」
・P.66 「アドレス帳の登録情報を保護する」
・P.86 「ログ情報の管理」
・P.68 「蓄積データを暗号化する」
・P.76 「ハードディスクのデータを上書き消去する」

アクセスの制限と管理

♦ 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。また、管理者が設定すべき項目は、ユーザーでは変更できません。管理者を登録して本機を運用します。機器設定の変更防止については、「機器設定の変更を防止する」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。機器の使用制限については、「機能の使用を制限する」を参照してください。

参照

・P.83 「機器設定の変更を防止する」
・P.85 「機能の使用を制限する」

ネットワークのセキュリティー強化

♦ 不正なアクセスを防止する

IP アドレスに制限をかけたり、ポートを無効に設定することによって、ネットワーク上での不正アクセスを防止し、アドレス帳や蓄積文書、初期設定のデータなどを保護することができます。不正アクセスの防止については、「不正なアクセスを防止する」を参照してください。

♦ パスワードを暗号化通信する

ログインパスワード、PDF 文書のグループパスワード、および IPP 認証のパスワードを暗号化通信し、パスワードを解析される脅威から保護することができます。パスワードの暗号化通信については、「パスワードを暗号化通信する」を参照してください。

♦ 通信経路の保護と暗号化通信

本機では SSL、SNMPv3、IPsec を使用して暗号化通信を確立することができます。通信経路の保護や通信データの暗号化を行うことで、通信途中でのデータの盗聴、内容の解析、改ざんを防止することができます。

SSL、SNMPv3、IPsec を使用した暗号化通信については、「通信経路の保護と暗号化通信」を参照してください。

参照

・P.89 「不正なアクセスを防止する」
・P.98 「パスワードを暗号化通信する」
・P.101 「通信経路の保護と暗号化通信」

1