ApeosPort®-VII C7773 DocuCentre-VII C7773
ApeosPort®-VII C6673 DocuCentre-VII C6673
ApeosPort®-VII C5573 DocuCentre-VII C5573
ApeosPort®-VII C4473 DocuCentre-VII C4473
ApeosPort®-VII C3373 DocuCentre-VII C3373
ApeosPort®-VII C2273 DocuCentre-VII C2273

セキュリティ機能補足ガイド

ご注意

① 本書の内容の一部または全部を無断で複製・転載・改変することはおやめください。
ただし、本機をご利用いただくために本書を参照する場合に限り、本書を複製することができます。
② 本書の内容に関しては将来予告なしに変更することがあります。
③ 本書に、ご不明な点、誤り、記載もれ、乱丁、落丁などがありましたら弊社までご連絡ください。
④ 本書に記載されていない方法で機械を操作しないでください。思わぬ故障や事故の原因となることがあります。
万一故障などが発生した場合は、責任を負いかねることがありますので、ご了承ください。
⑤ 本製品は、日本国内において使用することを目的に製造されています。諸外国では電源仕様などが異なるため使用できません。
また、安全法規制（電波規制や材料規制など）は国によってそれぞれ異なります。本製品および、関連消耗品をこれらの規制に違反して諸外国へ持ち込むと、罰則が科せられることがあります。

セキュリティ機能をお使いいただく前に

ここでは、セキュリティ機能に関する概要と確認事項を説明しています。

はじめに

本書は、本機を管理するシステム管理者を対象に、セキュリティ機能に関する設定手順と環境条件を説明しています。

また一般利用者を対象にセキュリティ機能に関する操作も補足しています。

他の機能の操作方法などについては下記のマニュアルをご覧ください。

対象機種	メディア（ソフトウェア / 製品マニュアル）帳票番号
ApeosPort-VII C7773/C6673/C5573/C4473/ C3373/C2273、DocuCentre-VII C7773/ C6673/C5573/C4473/C3373/C2273	電子マニュアル (HTML 形式) ME8355J1-2

ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C2273, DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C2273 のセキュリティ機能は以下の ROM バージョンで動作します。

ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C2273 PFS

DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C2273 PFS

Controller ROM Ver. 1.1.14

FAX ROM Ver. 2.2.1

ご注意

- 本製品は IT セキュリティ評価及び認証制度に基づき HCD PP v1.0 適合認証を取得しています。
- 本製品が取得した情報セキュリティに係る認証は、評価に用いた評価対象（Target of Evaluation）が所定の評価基準及び評価方法に基づく評価の結果、セキュリティ保証要件に適合していることを示すものです。ご使用の機械が、評価対象の機種であることを確認するには、電源投入後、起動時に操作パネルに表示される “Fuji Xerox” の表示と機種名をご確認ください。また、ご使用の機械の各 ROM バージョンと評価対象の商品コードを確認するには、「ROM バージョン、システム時計、商品コードの確認」(P.8) 記載の方法でご確認ください。
- 尚、機械の改善や改良のため、Controller ROM バージョンが更新される場合があるため、お客様がお使いの機械の ROM およびマニュアルのバージョンが IT セキュリティ認証の対象バージョンとは異なることがあります。
- 納入された機械に関して、配送用の段ボール箱の梱包状態に異常が無いことを確認してください。
- 確認できなかった場合、または機械の機能に関する質問、その他の質問がある場合は弊社の営業担当者かカストマーエンジニアにご連絡ください。
- 本マニュアルではセキュリティ機能、ファクス機能、スキャナー機能、ネットワークスキャン機能を利用することを前提としているため、データ上書き消去キットを購入し装着することが必要です。装着はカストマーエンジニアが実施します。また、初期設置時、カストマーエンジニアの設定により、印字速度と商品名が決定します。カストマーエンジニアの作業時は、その場に立ち会い、作業状況をご確認ください。
- 本製品にセキュリティ機能、ファクス機能、スキャナー機能、ネットワークスキャン機能が提供されていることは操作パネル上の機能ボタンで確認することができます。セキュリティ機能は、操作パネル上で「カストマーエンジニアの操作制限」設定メニューが表示されることで確認できます。ファクス機能、スキャナー機能、ネットワークスキャナー機能は、それぞれメニュー画面上に「ファクス / インターネットファクス」ボタン、「スキャナー（ボックス保存）」ボタン、「スキャナー（PC 保存）」ボタンが表示されることで確認できます。
- 各ボタンを表示する詳細な手順は、文末の付録「設定手順一覧」をご確認ください。また、機械管理者 ID, パスワードの初期値はユーザーズガイド「認証 / セキュリティ設定」「機械管理者情報の設定」をご確認ください。

IT セキュリティ認証評価で使用したハードウェアとソフトウェア

IT セキュリティ認証を取得するにあたり、以下に示すような機材を用いて評価しました。

Windows PC

以下のような用途で利用しました。

- 一般利用者がプリント機能を利用するために使用しました。プリンタードライバーは“ART EX ドライバー（Microsoft WHQL 認証取得ドライバー）”を使用しました。
- 一般利用者、または、システム管理者が本機の Web サーバー機能を利用する際、Web ブラウザーを使用しました。Web ブラウザーには Microsoft Edge を使用しました。
- システム管理者が本機の監査ログを取り出す際に使用しました。PowerShell も使用しました。

SMTP メールサーバー

本製品のメール送信機能を利用するために使用しました。通信プロトコルとして SMTP over TLS をサポートするメールサービスを使用しました。

本製品をセキュアにご利用いただくための注意事項

本製品のご利用時、原稿として使用された紙データ、出力された紙データの置き忘れ、取り忘れにご注意ください。

セキュリティ機能

ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C2273、DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C2273 は、以下に示すセキュリティ機能を持ちます。

- 識別認証
- セキュリティ監査
- アクセス制御
- セキュリティ管理
- 高信頼な運用
- 暗号化
- 高信頼な通信
- PSTN ファクス - ネットワーク間の分離
- データ消去

セキュリティ機能を有効にするための設定

セキュリティ機能を効果的に使用するために、システム管理者は以下の設定指示を遵守してください。

参照

- 各設定の手順について詳しくは、以下の項で説明しています。
  「セキュリティを有効にするための設定 1 （本機操作パネルからの初期設定）」（P.10）
  「セキュリティを有効にするための設定 2 （CentreWare Internet Services からの初期設定）」（P.17）
  「セキュリティを有効にするための設定 3 （PJL によるデータ読み書きの禁止）」（P.26）
  「セキュリティを有効にするための設定 4 （監査ログによる定期検査）」（P.27）

- スキャナー（URL 送信）
  無効に設定。
- リモートアシスタンス
  無効に設定。
- BMLinkS
  無効に設定。
- カスタムサービス
  無効に設定。
- パスワード使用 - パネル入力時
  ［する］に設定。
- ハードディスクデータの上書き消去
  ［1 回］あるいは［3 回］に設定。
- ハードディスクデータの暗号化
  有効に設定。
- 認証方式
  ［本体認証］に設定。
- 認証 / プライベートプリント
  ［プリンターの認証に従う］に設定。
- SMB
  無効に設定。
- ファクス
  ダイレクトファクスを無効に設定。
  相手機からのポーリング / 蓄積を禁止に設定。
- 受信ファクス文書蓄積用親展ボックスの作成
  ファクス受信文書を蓄積する親展ボックスを作成。
- 受信回線別ボックスセレクターの設定
  ファクス受信文書を蓄積する親展ボックスを指定。
- ソフトウェアダウンロード
  ［禁止］に設定。
- 自動リセット
  有効に設定。
- レポート出力
  無効に設定。
- 機械起動時のプログラム診断
  ［する］に設定。
- 機械管理者パスワード
  工場出荷時の初期値から 9 文字以上の別のパスワードに変更。
- 認証失敗アクセス拒否回数
  ［5］回に設定。

- アクセス制御
  ［デバイスへのアクセス］を［制限する］に設定。
  ［使用できるサービス］を［すべてを制限する］に設定。
- パスワードの最小文字数
  ［9］文字に設定。
- TLS 通信
  有効に設定。
- TCP/IP
  IPv4 に設定。
- WebDAV
  無効に設定。
- メール受信
  無効に設定。
- IPP
  有効に設定。
- IPSec 通信
  無効に設定。
- SNMP
  無効に設定。
- WSD（Scan）
  無効に設定。
- WSD（Print）
  無効に設定。
- LPD
  無効に設定。
- Port 9100
  無効に設定。
- FTP クライアント
  無効に設定。
- SOAP
  無効に設定。
- Bonjour
  無効に設定。
- USB
  無効に設定。
- CSRF
  有効に設定。
- カストマーエンジニアの操作制限
  ［する］に設定し、9 文字以上のパスワードを入力。

- 監査ログ

  有効に設定。
- ブラウザー表示更新

  無効に設定。
- ブラウザセッションタイムアウトの設定

  6 分に設定
- カスタムサービス

  無効に設定。
- PJL によるデータ読み書きの禁止

  PJL によるデータ読み書きを禁止します。

補足
- 「WSD」とは、「Web Services on Devices」の略です。

注記
- 各項目で上記以外の設定を行った場合は、セキュリティ機能を保つことができなくなりますので、ご注意ください。
- 運用中にセキュリティ設定を変更する場合は、本書の手順に従い、最初から設定を確認し直してください。
- 本書での設定は、カストマーエンジニアの操作制限機能を有効にして運用することが前提です。カストマーエンジニアに保守操作を許可した場合は、保守作業後、最初から設定を確認しやり直してください。
- ファクス - ネットワーク間の分離機能については、システム管理者による特別な設定は不要です。
- カストマーエンジニアの操作制限が有効な場合、受信回線別ボックスセレクターを設定すると、親展通信のファクスを受信できなくなりますので、ご注意ください。

セキュリティ機能を最適に使用するために

本製品を利用・運用する組織の責任者は、次の事項を遵守してください。

- システム管理者、機械管理者の適切な人選を行うと共に、管理や教育を実施してください。
- システム管理者は利用者に組織の方針およびガイダンス文書に従い、本機の使用方法及び注意事項に関する教育をしてください。
- 本機は許可されない物理的アクセスから保護するために、安全もしくは監視された環境に設置してください。
- 外部ネットワークから、本機を設置する内部ネットワークへのアクセスを遮断するために、ファイアウォールなどの機器を設置してください。
- パスワードは、次のルールに従って設定してください。
  - 容易に推測可能な文字列を使用しない
  - 英数特殊文字を混在させて使用する
- 利用者は User ID とパスワードを他の人に知られないように、機械を操作・管理してください。
- 利用者はプリンタードライバーの［認証情報の設定］で、必ず User ID とパスワードを設定してください。
- 共有親展ボックスは評価対象外の機能のため、機械管理者は共有親展ボックスを作成しないでください。
- 「電話番号 /G3ID 別ボックスセレクター設定」機能は評価対象外の機能のため、使用しないでください。

- 受信ファクス文書を蓄積する親展ボックスは一般利用者が作成したものを使用しないでください。一般利用者が作成した親展ボックスへ蓄積する構成は評価対象外です。また、受信ファクス文書蓄積用に作成した親展ボックスにプリント機能を有効化した指示書を関連付ける場合は、自動実行しないように設定してください。
- 本機を管理するシステム管理者は、本機が対応する暗号化通信プロトコル（TLS）を、それぞれクライアント PC およびサーバー側のセキュリティ方針に沿って適用した上で、本機を運用してください。

■TLS

本機が接続する TLS クライアント（Web ブラウザー、監査サーバー）および TLS サーバー（メールサーバー）には、以下の暗号化方式に対応したものを利用します。

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

ご注意

・安全のために、CentreWare Internet Services を使用中は、他の Web サイトへアクセスや他のアプリケーションの使用をしないでください。
・安全のために、機械を廃棄する場合は、暗号化をリセットし、データの一括削除を実施してください。
・TLS の脆弱性を避けるために、ブラウザーのプロキシ例外リストに機械のアドレスを設定してください。機械とリモート PC 上のブラウザーが、プロキシサーバーを介さずに直接通信することで、中間者攻撃（MITM）を避けることができます。
・CentreWare Internet Services を利用時、6 分間操作を行わないと自動的にログアウトします。CentreWare Internet Services での操作終了後、6 分以内に席を離れる場合は、必ずログアウトしてください。また、システム管理者はすべてのユーザーがこの運用ができるように指導してください。

補足

- NTP サーバーとの接続機能は評価対象外です。

ROM バージョン、システム時計、商品コードの確認

初期設定を行う前に、システム管理者は機械の ROM バージョンとシステム時計と商品コードが正しいことを確認してください。

操作パネルからの確認方法

1 タッチパネルディスプレイで［機械確認］を押します。

2 ［ソフトウェアバージョン］を押します。

画面上で、機械のソフトウェアバージョンを確認できます。

レポート出力による ROM バージョン、商品コードの確認方法

1 タッチパネルディスプレイで［機械確認］を押します。

2 ［レポート / リストの出力］を押します。

3 ［プリンター設定］を押します。

4 ［機能設定リスト（共通項目)］を押します。

5 ［スタート］を押します。

プリントされたレポート上で、機械のソフトウェアバージョン、商品コード（機種コード）を確認できます。

システム時計の確認方法

1 タッチパネルディスプレイ左上の［一般ユーザー］を押します。

2 表示されるキーボードを使って、機械管理者 ID を入力します。

3 ［確定］を押します。

4 警告メッセージに対して［閉じる］を押します。

5 ［仕様設定 / 登録］を押します。

6 ［仕様設定］を押します。

7 ［共通設定］を押します。

8 ［システム時計 / タイマー設定］を押します。

画面上で時刻と日付を確認できます。設定変更が必要な場合は、以下の手順で変更してください。

9 変更する項目を選択します。

10 ［確認 / 変更］を押します。

11 変更する項目を選択して、変更します。

12 ［決定］を押します。

13 ［閉じる］を押します。

セキュリティを有効にするための設定 1 （本機操作パネルからの初期設定）

ここでは、セキュリティ機能に関連した初期設定について、本機の操作パネルで設定する手順について説明しています。

スキャナー（URL 送信）の設定

1 タッチパネルディスプレイ左上の［一般ユーザー］を押します。

2 表示されるキーボードを使って、機械管理者 ID を入力します。

3 ［確定］を押します。

4 警告メッセージに対して［閉じる］を押します。

5 ［カスタマイズ］を押します。

6 ［スキャナー（URL 送信)］を選択し［削除］を押します

7 ［OK］を押します。

リモートアシスタンスの設定

1 ［カスタマイズ］を押します。

2 ［リモートアシスタンス］を選択し［削除］を押します

3 ［OK］を押します。

BMLinkS の設定

1 ［カスタマイズ］を押します。

2 ［BMLinks］を選択し［削除］を押します

3 ［OK］を押します。

カスタムサービスの設定

1 ［カスタマイズ］を押します。

2 ［カスタムサービス］で始まる項目を選択し［削除］を押します

3 ［OK］を押します。

本機操作パネルからのパスワード使用の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［パスワードの運用］を押します。

4 ［パスワードの運用］画面で、［パスワード使用 - パネル入力時］を押します。

5 ［確認 / 変更］を押します。

6 ［パスワード使用 - パネル入力時］画面で、［する］を選択します。

7 ［決定］を押します。

8 ［閉じる］を押します。

ハードディスクの上書き消去の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［ハードディスクの上書き消去設定］を押します。

3 ［上書き回数の設定］を押します。

4 ［上書き回数の設定］画面で、［1 回］または［3 回］を押します。

5 ［決定］を押します。

ハードディスクデータの暗号化設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［その他の設定］を押します。

4 ［データの暗号化］を押します。

5 ［確認 / 変更］を押します。

6 ［する］を押します。

7 ［OK］を押します。

8 確認画面が表示されたら、［はい（変更する）］を押します。

9 再度確認画面が表示されたら、［はい（再起動する）］を押します。

認証方式の設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［認証方式の設定］を押します。

4 ［認証方式の設定］画面で、［本体認証］を押します。

5 ［決定］を押します。

6 ［閉じる］画面右上の［X］を押します。

7 確認画面が表示されたら、［はい（再起動する）］を押します。

認証方式の設定後、ユーザーズガイド「認証と集計管理機能について」の記述にしたがってユーザーを登録してください。

＊上記で設定した認証方式は以下のインターフェースからの操作において適用されます。

- 操作パネル
- CentreWare Internet Services
- プリンタードライバー

プライベートプリントの設定

1 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

2 ［認証の設定］を押します。

3 ［認証 / プライベートプリントの設定］を押します。

4 ［認証 / プライベートプリントの設定］画面で、［受信制御］を選択します。

5 ［確認 / 変更］を押します。

6 ［受信制御］画面で、［プリンターの認証に従う］を選択します。

7 ［認証成功のジョブ］で［プライベートプリントに保存］を選択します。

8 ［認証が不正のジョブ］で［ジョブを中止］を選択します。

9 ［User ID なしのジョブ］で［ジョブを中止］を選択します。

10 ［閉じる］を押します。

11 ［決定］を押します。

SMB の設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［ ネットワーク設定 ］を押します。

3 ［ ポート設定 ］を押します。

4 ［SMB クライアント ］を押します。

5 ［確認 / 変更］を押します。

6 ［SMB クライアント - ポート］を押します。

7 ［確認 / 変更］を押します。

8 ［停止］を選択します。

9 ［決定］を押します。

10 ［閉じる］を 2 回押します。

ファクスの設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［ファクス設定］を押します。

3 ［ファクス動作制御］を押します。

4 ［ダイレクトファクスの使用］を押します。

5 ［確認 / 変更］を押します。

6 ［禁止］を選択します。

7 ［決定］を押します。

8 ［相手機からのポーリング / 蓄積］を押します。

9 ［確認 / 変更］を押します。

10 ［禁止］を選択します。

11 ［決定］を押します。

12 ［閉じる］を押します。

13 確認画面が表示されたら、［はい（再起動する）］を押します。

受信ファクス文書蓄積用親展ボックスの作成

1 機械管理者ではないシステム管理者権限をもつ利用者 ID でログインします。

2 ［仕様設定 / 登録］画面で、［登録 / 変更］を押します。

3 ［ボックス登録］を押します。

4 登録する親展ボックスを選択します。

5 ［アクセス制御/パスワード］画面で、［アクセス制御］に［［設定］しない］を選択します。

6 ［決定］を押します。

7 ［登録 / 変更］画面で［ボックス名称］に適当な名称を入力し、［X］を押します。

8 ［ボックス登録］画面で［X］を押して画面を閉じます。

受信回線別ボックスセレクターの設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［ファクス設定］を押します。

3 ［ファクス動作制御］を押します。

4 ［受信回線別ボックスセレクター］を押します。

5 ［受信回線別ボックスセレクター］を押します。

6 ［有効］を押します。

7 ［決定］を押します。

8 ［閉じる］を押します。

9 ［受信文書の保存先 / 排出先］を押します。

10 ［受信回線別ボックスセレクター］を押します。

11 登録したい回線を選択し、［確認 / 変更］を押します。

12 ［指定する］を押します。

13 事前に作成した受信ファクス文書蓄積用親展ボックスの番号 (3 桁) を<数字>ボタンで入力します

14 ［決定］を押します。

11 に戻って未登録の回線を選択します。これをすべての回線が登録されるまで繰り返します。

15 ［閉じる］を押します。

16 ［閉じる］を押します。

ソフトウェアダウンロードの設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［その他の設定］を押します。

4 ［ソフトウェアダウンロード］を選択します。

5 ［確認 / 変更］を押します。

6 ［禁止］を押します。

7 ［決定］を押します。

8 ［閉じる］を押します。

自動リセットの設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［システム時計 / タイマー設定］を押します。

4 ［自動リセット］を押します。

5 ［確認 / 変更］を押します。

6 ［する］を押します。

7 ［決定］を押します。

8 ［閉じる］を押します。

レポート出力の設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［レポート設定］を押します。

4 ［レポート出力の許可］を押します。

5 ［確認 / 変更］を押します。

6 ［しない］を押します。

7 ［決定］を押します。

8 ［閉じる］を押します。

機械起動時のプログラム診断の設定

1 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

2 ［共通設定］を押します。

3 ［保守］を押します。

4 ［機械起動時のプログラム診断］を選択します。

5 ［する］を押します。

6 ［決定］を押します。

7 ［閉じる］を押します。

8 確認画面が表示されたら、［はい（再起動する）］を押します。

セキュリティを有効にするための設定 2 （CentreWare Internet Services からの初期設定）

ここでは、セキュリティ機能に関連した初期設定について、CentreWare Internet Services から設定する手順について説明しています。

CentreWare Internet Services を利用する前に、ユーザーズガイド「仕様設定」「ネットワーク設定」「プロトコル設定」の記述に従って、IP アドレスの設定を行ってください。

CentreWare Internet Services からの設定準備

CentreWare Internet Services を利用するためには、ネットワークプロトコルとして TCP/IP が利用でき、「TLS」(P.7) の条件を満たす Web ブラウザーを有するコンピューターが必要です。

1. ご使用のコンピューター上で Web ブラウザーを起動して、アドレス入力欄に本機の TCP/IP アドレスを入力して、〈Enter〉キーを押します。
2. 機械管理者 ID とパスワードを入力します。
3. ［OK］をクリックします。
4. 警告メッセージに対して［OK］をクリックします。
5. ［プロパティ］タブをクリックして、［プロパティ］画面を表示します。

機械管理者パスワードの変更

1. ［プロパティ］画面で、［セキュリティー］をクリックします。
2. ［機械管理者情報の設定］をクリックします。
3. ［機械管理者 ID］へ機械管理者 ID を入力します。
4. ［機械管理者パスワード］へ 9 文字以上の新しいパスワードを入力します。
5. ［機械管理者パスワードの確認入力］へ同じパスワードを入力します。
6. ［新しい設定を適用］をクリックします。

補足

- パスワードに指定可能な文字 :
  アルファベットの大文字と小文字、数字、及び次の特殊文字
  (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “ (space)”, “””, “”, “+”, “,”, “-“, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “¥”, “]”, “_”, “`”, “{“, “|”, “}”, “~”)

認証失敗アクセス拒否回数の設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［認証情報の設定］をクリックします。

3 ［機械管理制限ユーザー］と［一般ユーザー］の［認証回数制限］へ［5］を入力します。

4 ［新しい設定を適用］をクリックします。

アクセス制御の設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［認証管理］をクリックします。

3 ［次へ］をクリックします。

4 ［デバイス / 仕様設定へのアクセス］の［設定］をクリックします。

5 ［デバイスへのアクセス］で［制限する］を選択します。

6 ［新しい設定を適用］をクリックします。

7 ［認証管理］をクリックします。

8 ［次へ］をクリックします。

9 ［サービスへのアクセス］の［設定］をクリックします。

10 ［使用できるサービス］で［すべてを制限する］をクリックします。

11 ［新しい設定を適用］をクリックします。

12 ［ジョブ操作の設定］をクリックします。

13 ［実行中 / 待ちジョブの表示設定］をクリックします。

14 ［表示情報の制限］で［する］を選択します。

15 ［新しい設定を適用］をクリックします。

16 ［ジョブ操作の制限］をクリックします。

17 すべての操作に対して［本人と管理者］を選択します。

18 ［新しい設定を適用］をクリックします。

19 ［再起動］をクリックします。

パスワードの最小桁数の設定

補足
- 本機能は、本体認証時のみ有効です。

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［認証情報の設定］をクリックします。

3 ［パスワードの最小桁数］へ［9］を入力します。

4 ［新しい設定を適用］をクリックします。

5 ［再起動］をクリックします。

TLS の設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［証明書の設定］をクリックします。

3 ［証明書の作成］をクリックします。

4 ［自己証明書］を選択します。

5 ［次へ］をクリックします。

6 必要に応じて、詳細情報を設定します。

7 ［新しい設定を適用］をクリックします。

8 ［SSL/TLS 設定］をクリックします。

9 ［HTTP-SSL/TLS 通信］の［有効］チェックボックスをチェックします。

10 ［SMTP-SSL/TLS 通信］の欄で［SSL/TLS 接続 ］を選択します。

11 ［IPP］の欄で［SSL/TLS 通信のみ有効 ］チェックボックスをチェックします。

12 ［相手サーバーの証明書の検証］の［ 有効 ］チェックボックスをチェックします。

13 ［プロトコルバージョン］の欄で［TLS1.2］を選択します。

14 ［新しい設定を適用］をクリックします。

15 ［再起動］をクリックします。

注記
- ［相手サーバーの証明書の検証］の［有効］チェックボックスをチェックする前に、「デバイス証明書のインポート」（P.21）と同じ手順で、相手サーバーの CA 証明書をインポートする必要があります。
- 自己証明書の作成方法については、「デジタル証明書の設定」（P.43）をご確認ください。

TCP/IP の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2 ［プロトコル］をクリックします。
3 ［TCP/IP］をクリックします。
4 IP Mode の欄で IPv4 を選択します
5 ［新しい設定を適用］をクリックします。

WebDAV の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2 ［ポート起動］をクリックします。
3 ［WebDAV］の［起動］チェックボックスのチェックを外します。
4 ［新しい設定を適用］をクリックします。

メール受信の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2 ［ポート起動］をクリックします。
3 ［メール受信］の［起動］チェックボックスのチェックを外します。
4 ［新しい設定を適用］をクリックします。

IPP の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。
2 ［ポート起動］をクリックします。
3 ［IPP］の［起動］チェックボックスをチェックします。
4 ［新しい設定を適用］をクリックします。

デバイス証明書のインポート

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［証明書の設定］をクリックします。

3 ［証明書のインポート］をクリックします。

4 ［証明書］の欄にインポートするファイルの名前を入力します。または［参照］をクリックしてインポートするファイルを選択します。

5 必要であれば［パスワード］の欄にパスワードを入力して、［パスワードの確認］の欄に同じパスワードを入力します。

6 ［インポート］をクリックします。

IPSec の通信設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［IP Sec］をクリックします。

3 ［プロトコル］の［有効］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

5 ［再起動］をクリックします。

WSD（Scan）の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［WSD（Scan）］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

補足
- 「WSD」とは、「Web Services on Devices」の略です。

WSD（Print）の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［WSD（Print）］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

LPD の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［LPD］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

Port9100 の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［Port9100］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

FTP の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［FTP クライアント］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

SOAP の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［SOAP］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

SNMP の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［SNMP］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

Bonjour の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［Bonjour］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

USB の設定

1 ［プロパティ］画面で、［サービス設定］をクリックします。

2 ［USB］をクリックします。

3 ［一般］をクリックします。

4 ［スキャナー（USB メモリー保存 ）の使用］と［メディアプリントの使用］の［有効］チェックボックスのチェックを外します。

5 ［新しい設定を適用］をクリックします。

6 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

7 ［ポート起動］をクリックします。

8 ［USB］の［起動］チェックボックスのチェックを外します。

9 ［新しい設定を適用］をクリックします。

補足
- 機器の構成により設定メニューが表示されない場合があります。

CSRF の設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［プロトコル設定］をクリックします。

3 ［HTTP］をクリックします。

4 ［CSRF 対策］の［有効］チェックボックスをチェックします。

5 ［新しい設定を適用］をクリックします。

カストマーエンジニアの操作制限の設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［カストマーエンジニアの操作制限］をクリックします。

3 ［操作制限］の［する］チェックボックスをチェックします。

4 ［保守パスワード］に 9 文字以上の新しいパスワードを入力します。

5 ［保守パスワードの確認入力］に同じパスワードを入力します。

6 ［新しい設定を適用］をクリックします。

補足
- パスワードに指定可能な文字 :
  アルファベットの大文字と小文字、数字、及び次の特殊文字
  (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ” (space)”, “””, “”, “+”, “,”, “-“, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “¥”, “]”, “_”, “`”, “{“, “|”, “}”, “~”)

監査ログの起動

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［監査ログ］をクリックします。

3 ［監査ログの起動］の［有効］チェックボックスをチェックします。

4 ［新しい設定を適用］をクリックします。

ブラウザ表示更新時間の設定

1 ［プロパティ］画面で、［一般設定］をクリックします。

2 ［Internet Services 設定］をクリックします。

3 ［表示更新時間］ボックスに［0］を入力します。

4 ［新しい設定を適用］をクリックします。

ブラウザセッションタイムアウトの設定

1 ［プロパティ］画面で、［一般設定］をクリックします。

2 ［Internet Services 設定］をクリックします。

3 ［セッションタイムアウト時間］ボックスに［6］を入力します。
（セッションタイムアウト時間は 6 分から 240 分の範囲で指定できます。）

4 ［新しい設定を適用］をクリックします。

カスタムサービスの設定

1 ［プロパティ］画面で、［セキュリティー］をクリックします。

2 ［ プラグイン / カスタムサービス設定］をクリックします。

3 ［ 組み込みプラグイン機能 ］をクリックします。

4 ［ 組み込みプラグイン機能 ］の［ 有効 ］チェックボックスのチェックを外します。

5 ［ カスタムサービス ］をクリックします。

6 ［ カスタムサービス ］の［ 有効 ］チェックボックスのチェックを外します。

7 ［新しい設定を適用］をクリックします。

8 確認画面が表示されたら、［はい（再起動する）］を押します。

セキュリティを有効にするための設定 3 （PJL によるデータ読み書きの禁止）

PJL によるデータ読み書きを禁止するため、以下に示す記述の PJL コマンドファイルを作成し、LPR コマンド等で複合機にプリントジョブを発行してください。

@PJL JOB PASSWORD=<current password>

@PJL DEFAULT DISKHIDE=ON

@PJL DEAFULT PASSWORD=<new password>

@PJL EOJ

<current password> は工場出荷時は何も設定されていません。任意の文字列を指定してください。<new password> には、A ～ Z, a ～ z, 0-9 の 8 文字以上、255 文字以内の英数字で構成される任意の文字列を指定してください。

注記

- LPR コマンドで上記設定を実行する場合、一時的に複合機の LPD ポートを有効化してください。上記設定後、「LPD の設定」（P.22）の手順に従い、LPD ポートは無効化してください。
  Windows PC で LPR コマンドを利用するには、Windows の設定で、LPR ポートモニターの機能を有効化してください。
  上記で作成したファイルを複合機に送るには、コマンドプロンプト上で以下のような書式で LPR コマンドを実行してください。
  lpr -S “ 複合機の IP アドレス ” -P lp “ ファイル名 ”

セキュリティを有効にするための設定 4 （監査ログによる定期検査）

ここでは、監査サーバーから監査ログを自動で取り出す手順について説明しています。

監査ログファイルは、セキュリティ管理者や外部の解析者の援助を得て定期的に検査することにより、試みられた機密漏洩に関し違反を識別して、また将来の違反を防止します。

監査ログ対象のイベント（例えば障害や構成変更、ユーザー操作など）は、タイムスタンプと共に一つのファイル（以降、「監査ログファイル」と呼びます）に、最大 15,049 件まで本機内部に保存されます。15,049 件を超えた場合は、一番古い監査ログイベントから順次消去され、繰り返してイベントが記録されます。

監査サーバーから取り出す都度、本機に保存された監査ログファイルがダウンロードされますが、ダウンロードされたログデータは本機から消去されません。取り出す間隔によって、以前取り出した監査ログファイルに記録されたイベントと同じものが記録されている可能性があります。一方で、取り出す間隔が長すぎると、監査ログファイルから削除され、確認できないイベントが発生する可能性があります。約 15,000 件のイベントがすべて更新されるまでの時間は、本機の利用頻度によって異なりますが、システム管理者は、適切な間隔で、取り出しを実行するように設定してください。15,000 件のイベントが記録された監査ログファイルのサイズは約 1.5M バイトになります。取り出しの頻度と保存領域の空き容量に応じて、保存するファイル数を決め、適切な間隔で古いログファイルを削除してください。以下に記した PowerShell スクリプトをご利用の場合、ダウンロードした監査ログファイルのファイル名には秒単位でダウンロードした日時のタイムスタンプが含まれます。古い監査ログファイルを調べる場合は、ファイル名から所望の時間帯をご確認ください。

監査ログファイルは、PowerShell スクリプトがあるフォルダに以下の形式の名称で保存されます。運用を開始する前に、正しく保存されることをご確認のうえ、必要に応じて、PowerShell スクリプトを修正してください。

なお、本機に保存された監査ログの削除機能はありません。

監査ログファイルの取り出し

監査ログファイルの取り出し方法について説明します。

監査ログファイルをダウンロードする場合は、［HTTP-SSL/TLS 通信］が［有効］に設定されている必要があります。

以下の条件を満たすサーバーを使用する事を前提として、手順を記載します。

- Windows OS を搭載
- PowerShell version3.0 以降インストール済み
- PowerShellでのスクリプト実行が可能なように、PowerShell実行ポリシーが設定済み

1 以下の内容で PowerShell スクリプトを作成します。

```
# Replace "11111" with actual Login ID of system administrator
$USER = "11111"
# Replace "x-admin" with actual Passcode of system administrator
$PASS = "x-admin"

# Replace "127.0.0.1" with actual URL of target device
$Uri = "https://127.0.0.1/auditfile.txt"

# Define download file name rule
$date_time = Get-Date -Format "yyyy-MMdd-HHmmss"
$DownloadPath = "./auditfile_${date_time}.txt"

# Download audit log
$secpasswd = ConvertTo-SecureString $PASS -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential($USER, $secpasswd)
$ProgressPreference = 'SilentlyContinue'
[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri $Uri -OutFile $DownloadPath -Credential $cred -DisableKeepAlive
```

注記

- Windows から PowerShell で本機に TLS 通信を行うためには、本機にインストールされている SSL サーバー証明書が、Windows で正しく検証出来るように信頼できるルート証明書として登録されている必要があります。
- 本 PowerShell スクリプトに記述されたシステム管理者の ID、パスワードが漏えいしないよう、スクリプトファイルの保管には十分注意してください。

2 1 で作成したスクリプトを PowerShell で実行するタスクをタスクスケジューラに登録します。主な設定項目を以下に記載しますが、お客様の環境・ポリシーに応じて適切に変更・設定をしてください。

操作：プログラムの開始

操作 > 設定 > プログラム / スクリプト：“ < PowerShell のパス > ”

操作 > 設定 > 引数の追加：“-Command < 上記スクリプトのパス >”

操作 > 設定 > 開始：“< スクリプトを実行し、監査ログを保存するフォルダのパス >”

PowerShell やタスクスケジューラの詳細に関しては、Windows のヘルプを参照してください。

監査ログファイルには、次の情報が記録されています。アクセス、または試行の違反がないか、定期的にチェックしてください。

- Log ID： 監査ログ識別子としての通し番号
- Date、Time： イベントが記録された日時

- Logged Events： 記録される事象の名称
- User Name： 事象を起こした利用者名
- Description： イベントに関する内容の説明
- Status： イベントの処理結果、または状態
- Optionally Logged Items：共通保存項目以外に監査ログへ保存される追加情報

例：誰かが、User1 という ID でログインを試みて、パスワードの不一致のためにログインが失敗した場合、次の監査ログが記録されます。

Item	Description
Log ID	1
Date	01/01/2018
Time	10:00:00
Logged Events	Login/Logout
User Name	User1
Description	Login
Status	Failed（Invalid Password）
Optionally Logged Items	-

ユーザー認証

ここでは、本機を利用するためのユーザー認証の操作を説明しています。

本機を利用する前に、利用者は User ID とパスワードによる認証が必要です。

1 表示されるキーボードを使って、User ID を入力します。

2 ［次へ］を押します。

3 パスワードを入力します。

4 ［確定］を押します。

この状態で本機からの利用が可能になります。

補足

- 機械管理者 ID だけは本機にあらかじめ登録されていますが、他の User ID は登録されていません。User ID の登録について詳しくは、『ユーザーズガイド』の「仕様設定」>「認証 / セキュリティ設定」>「認証の設定」>「ユーザー登録 / 集計管理」を参照してください。
- WebUI からユーザー登録する場合、ユーザー名に設定されている文字列“<<新規登録>>”を削除してください。

利用者は、大きく 3 種類のユーザーに分けられます。

- システム管理者

  本機または外部のサーバーに登録され、使用環境に合わせてシステムの設定値を登録 / 変更できるユーザーです。

  工場出荷時の初期状態で設定されている機械管理者と、使用環境で追加され、機械管理者権限を付与されたシステム管理者が存在します。

- 一般利用者

  本機または外部のサーバーに登録され、本機の基本機能は利用できるが、システムの設定値の登録 / 変更はできないユーザーです。登録されたユーザーの初期状態の役割は一般利用者となります。

- 未認証ユーザー

  ユーザー認証せずに本機にアクセスするユーザーです。未認証状態では、本機は操作できません。

ログインした利用者には、割り当てられた権限に応じて、各基本機能の利用によって発生する文書やジョブに対して可能な操作が異なります。

注記

- システム管理者は強い権限を持ちますので、登録する利用者は必要最低限にしてください。また、セキュリティ認証評価の対象外の機能のため、「集計管理」権限をもつ利用者は登録しないでください。

プライベートプリント機能において、一般利用者は、自身が発行し本機に保存されたプリントデータのプレビューや印刷指示、部数変更、削除、印刷指示後の印刷中ジョブのキャンセルが可能ですが、他者が発行し、本機に保存されたデータとジョブにはアクセスできません。

システム管理者（機械管理者を含む）は、自身だけでなく他者が発行し、本機に登録されたプリントデータならびにジョブの操作が可能です。

ネットワークスキャン機能において、一般利用者は、スキャン操作時にプレビューを有効にした場合、自身が操作したスキャンイメージの参照、実行中スキャンジョブのキャンセルが可能ですが、他者が操作したデータとジョブにはアクセスできません。

システム管理者（機械管理者を含む）は、自身だけでなく他者が操作したスキャンデータならびにジョブの操作が可能です。

コピー機能において、一般利用者は、自身が一時停止したコピージョブの部数変更、再開、中止が可能ですが、他者が操作したデータとジョブにはアクセスできません。

システム管理者（機械管理者を含む）は、自身だけでなく他者が操作したコピージョブの操作が可能です。

ファクス送信機能において、一般利用者は、送信操作時にプレビューを有効にした場合、自身が操作したファクス送信イメージの参照、実行中ファクス送信ジョブのキャンセルが可能ですが、他者が操作したデータとジョブにはアクセスできません。

システム管理者（機械管理者を含む）は、自身だけでなく他者が操作したファクス送信データならびにジョブの操作が可能です。

ファクス受信機能おいて、受信されたファクスデータは受信回線別ボックスセレクターに設定された受信データ蓄積用親展ボックスに保存されます。保存された受信データの読みだし、印刷指示、削除は、保存された親展ボックスの所有者のみに許されます。ただし、機械管理者のみ、他者の親展ボックス内のデータにアクセスできます。

親展ボックスへのスキャン機能において、親展ボックスに保存されたスキャンイメージの表示、印刷指示、削除、印刷指示時の部数、用紙選択の変更は、親展ボックスの所有者のみが可能です。ただし、機械管理者のみが、他者の親展ボックス内のデータにアクセスできます。

自己テスト

ここでは、自己テスト（機械起動時のプログラム診断）について説明しています。

本機は、プログラムの実行コードおよび設定データの完全性を検証するための自己テスト機能を実行することが可能です。

本機は起動時に NVRAM と SEEPROM の設定データを含む領域を照合し、異常時は操作パネルにエラーを表示します。

ただしセキュリティ監査ログデータ、時計の日時データはこれらには含まれないため異常の検出はしません。

また本機は起動時に自己テスト機能が設定されていると、以下のテストを実施します。

Controller ROMのチェックサムを計算し所定の値と一致するかを確認し異常時は操作パネルにエラー（117-311）を表示します。

Fax ROM のチェックサムを計算し所定の値と一致するかを確認し異常時は操作パネルにエラー（033-321）を表示します。

乱数生成器の既知解テストを実施し、結果が失敗の場合は操作パネルにエラー（116-321）を表示します。

エラーが表示された場合は、本機の電源を切り、操作パネルのディスプレイが消灯してから、もう一度電源を入れてください。それでも状態が改善されないときは、弊社のカストマーコンタクトセンターまたは販売店にご連絡ください。状況により、お客様に確認を依頼する場合や、カストマーエンジニアによる保守が必要となる場合があります。

ファームウェアアップデート

ここでは、ファームウェアアップデートについて説明しています。本機は、ファームウエア・バージョンアップツールを使って本機のファームウェアをアップデートすることが可能です。

ファームウェアアップデートを実行する前に、ファームウェアアップデートを許可するように本機の設定を行ってください。本機操作パネルからの設定とCentreWare Internet Services からの設定が必要となります。

また、Port 9100 と SNMP を一時的に有効にしてください。

さらに、ファーム・バージョンアップツールを実行するクライアント PC と本機は、他の PC からアクセスできない独立したネットワークに接続し直してください。

弊社から提供するファームウエア・バージョンアップツールを、本機とネットワークで繋がったクライアント PC 上で実行することで、本機のファームウェアがアップデートされます。

ファームウェアのアップデート終了後は、管理者以外の人がファームウェアのアップデートを行えないようにするために、ファームウェアアップデートを禁止するように再度本機の設定を行ってください。また、本機を運用環境のネットワークに接続し直してください。

本機操作パネルからのソフトウェアダウンロード許可設定

1. タッチパネルディスプレイ左上の［一般ユーザー］を押します。
2. 表示されるキーボードを使って、機械管理者 ID を入力します。
3. ［確定］を押します。
4. 警告メッセージに対して［閉じる］を押します。
5. ［ 仕様設定 / 登録 ］画面で、［仕様設定］を押します。
6. ［ 共通設定 ］を押します。
7. ［ その他の設定 ］を押します。
8. ［ ソフトウェアダウンロード ］を選択します。
9. ［ 確認 / 変更 ］を押します。
10. ［ 許可 ］を押します。
11. ［ 決定 ］を押します。
12. ［ 閉じる ］を押します。

CentreWare Internet Services からのソフトウェアダウンロード許可設定

CentreWare Internet Services からの設定に必要な準備は、前述の「CentreWare Internet Services からの設定準備」を参照してください。

1 [プロパティ] 画面で、[サービス設定] をクリックします。

2 [ソフトウェアの更新] をクリックします。

3 ［ネットワーク経由のソフトウェアダウンロード］をクリックします。

4 [有効] チェックボックスをチェックします。

5 ［新しい設定を適用］をクリックします。

CentreWare Internet Services からの Port9100 許可設定

1 [プロパティ] 画面で、[ネットワーク設定] をクリックします。

2 [ポート起動] をクリックします。

3 ［Port9100］の［起動］チェックボックスをチェックします。

4 ［新しい設定を適用］をクリックします。

CentreWare Internet Services からの SNMP 有効化設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［SNMP］の［起動］チェックボックスをチェックします。

4 ［新しい設定を適用］をクリックします。

クライアント PC からファームウェアアップデートの実施

弊社から提供するファームウエア・バージョンアップツールを、本機とネットワークで繋がったクライアント PC 上に保存した上で、下記の手順を実行することで、本機のファームウェアがアップデートされます。

1. ご使用のクライアント PC 上で、ファームウエア・バージョンアップツールを起動します。
2. 使用許諾をご確認の上、[同意] をクリックします。
3. ご使用の機種名を選択し、[次へ] をクリックします。
4. 通信インターフェースで [ネットワーク (port9100)] を選択し、[次へ] をクリックします。
5. [IP アドレスを直接指定する] を選択し、本機の IP アドレスを入力して、[次へ] をクリックします。

上記の手順後、ファームウエアの転送が開始され、転送状況が表示されます。

転送が終了すると実行結果が表示されますので、結果を確認の上、[完了] をクリックしてください。

ファームウエアの転送が完了すると、本機でファームウェアのアップデートが開始されます。操作パネルに実行状況、結果が表示されますので、アップデートが正常に終了したことを確認してください。

本機操作パネルからのソフトウェアダウンロード禁止設定

1. タッチパネルディスプレイ左上の［一般ユーザー］を押します。
2. 表示されるキーボードを使って、機械管理者 ID を入力します。
3. ［確定］を押します。
4. 警告メッセージに対して［閉じる］を押します。
5. [仕様設定 / 登録] 画面で、［仕様設定］を押します。
6. [共通設定] を押します。
7. [その他の設定] を押します。
8. [ソフトウェアダウンロード] を選択します。
9. [確認 / 変更] を押します。
10. [禁止] を押します。
11. [決定] を押します。
12. [閉じる] を押します。

CentreWare Internet Services からのソフトウェアダウンロード禁止設定

CentreWare Internet Services からの設定に必要な準備は、前述の「CentreWare Internet Services からの設定準備」を参照してください。

1 [プロパティ] 画面で、[サービス設定] をクリックします。

2 [ソフトウェアの更新] をクリックします。

3 ［ネットワーク経由のソフトウェアダウンロード］をクリックします。

4 [有効] チェックボックスのチェックを外します。

5 ［新しい設定を適用］をクリックします。

CentreWare Internet Services からの SNMP 無効化設定

1 ［プロパティ］画面で、［ネットワーク設定］をクリックします。

2 ［ポート起動］をクリックします。

3 ［SNMP］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

CentreWare Internet Services からの Port9100 禁止設定

1 [プロパティ] 画面で、[ネットワーク設定] をクリックします。

2 [ポート起動] をクリックします。

3 ［Port9100］の［起動］チェックボックスのチェックを外します。

4 ［新しい設定を適用］をクリックします。

IPP プリントを利用する

IPP プリント機能を利用するには、お使いのクライアント PC に以下の手順でプリンタードライバーをインストールする必要があります。

(以下では、Windows 10 を例に説明します。)

1 管理者権限のあるアカウントでログインする。

2 設定メニュー内のデバイスアイコンを選択する。

3 「プリンターとスキャナー」画面で「プリンターまたはスキャナーを追加します」ボタンをクリックし、「プリンターが一覧にない場合」リンクを選択する。

4 「共有プリンターを名前で選択する」を選択し、以下のように接続先を入力して、「次へ」をクリックする。

接続先指定方法 : “https://< 本機の IP アドレスまたはホスト名 >/ipp“

5 プリンターの追加ウィザード内で「ディスク使用」をクリックする。

6 プリンタードライバーが保存されているフォルダを指定し、INF ファイルを選択し、「開く」をクリックする。

注記

- クライアントPCから本機にIPPS通信を行うためには、本機にインストールされているSSLサーバー証明書が、Windows で正しく検証できるように、信頼できるルート証明書として登録されている必要があります。

クライアント PC からプライベートプリント機能を利用する

クライアント PC からプライベートプリント機能を利用する際、以下の方法で本機に設定された認証ユーザーを指定してください。

(以下では、Windows 10 を例に説明します。)

1 プリンターのプロパティで、“プリンター構成”タブの“認証設定”ボタンをクリックする。

2 “ 認証管理 ” ダイアログ上で、以下の設定を行う。

“ ジョブごとに認証の入力画面を表示する ” ラジオボタンを選択する。

注記

- より安全にご利用いただくため、“ 認証管理 ” ダイアログでは、“ 常に同じ認証情報を使用する ” ラジオボタンを使用しないでください。

プリントジョブ発行時のプリンタプロパティで、“ プリント種類 ” として、“ 通常プリント ”, “ セキュリティー ”, “ サンプル ”, “ 時刻指定 ”, “ ボックス保存 ”, “ フォーム登録 ” などが指定できますが、“ フォーム登録 ” 以外は、どの指定をしても、プライベートプリントジョブとして、本機に登録されます。“ フォーム登録 ” が指定されたジョブは印刷されず、フォームデータとして本機に保存されます。

CentreWare Internet Services での操作

クライアント PC では、Web ブラウザーを使って、CentreWare Internet Serivces に接続し、本機をリモートから操作することができます。

ここでは、CentreWare Internet Services の [ジョブ]、[スキャン]、[プリント] の各タブで可能な操作について説明します。

ジョブ

[ジョブ] タブでは、各プロトコルまたは操作パネルで指示したジョブに関する情報が表示されます。また、実行待ちのジョブを削除することができます。

- ジョブ一覧

  処理中のジョブの一覧が表示されます。

- 履歴一覧
  - ジョブ履歴

    今までに完了したジョブの履歴が表示されます。

  - ジョブ履歴 - 関連ジョブのまとめ

    今までに完了したジョブの履歴が表示されます。ファクスの同報送信やジョブフローのジョブなど、関連ジョブがある場合は、一つにまとめたジョブが表示されます。

- エラー履歴

  今までに発生したエラー情報が表示されます。

ジョブ一覧では、「ジョブ名」「所有者」「状態」「種別」「部数」が表示されます。[実行待ち][実行中] 状態のプリントジョブは削除することができます。表示されているジョブの左にあるチェックボックスをクリックし、チェックマークを付け、画面右上の [削除] ボタンをクリックすることにより、削除できます。ジョブ削除には、ユーザー ID とパスワードが必要です。機械管理者、システム管理者、またはジョブ所有者の [User ID] と [パスワード] を入力してください。

履歴一覧 - ジョブ履歴、履歴一覧 – ジョブ履歴 – 関連ジョブのまとめ、では、「ジョブ名」「所有者」「結果」「種別」「ページ数」「排出先」「ホスト I/F」「完了時刻」が表示されます。情報が不明または未設定の項目には、[-] が表示されます。

エラー履歴では、エラーが発生した [日付 / 時刻] と [エラーコード] が表示されます。

スキャン

[スキャン] タブでは、親展ボックスの操作ができます。

親展ボックスの一覧を表示し、[登録]、[編集]、[削除]、[文書の一覧表示] が可能です。

[文書の一覧表示] ボタンをクリックすると、[ボックスの文書一覧] 画面が表示されます。

[ボックスの文書一覧] 画面には、親展ボックス内の文書が一覧表示されます。親展ボックス内の文書が一覧表示できるのは、CentreWare Internet Services にログインしている利用者と、親展ボックスの所有者が一致している場合のみです。ログインユーザーと親展ボックスの所有者が一致していない場合、指定された親展ボックス所有者の UserID とパスワードが求められます。ただし、機械管理者としてログインしている場合は、全親展ボックス内の文書を一覧表示できます。

- ボックス番号

  親展ボックスの番号が表示されます。
- ボックス名称

  親展ボックスの名称が表示されます。
- 文書番号

  文書番号が表示されます。
- 文書名

  文書名が表示されます。
- 登録日時

  文書が親展ボックスに登録された日時が表示されます。
- 圧縮形式

  [MH]、[MR]、[MMR]、[JBIG]、[JPEG]、[非圧縮] のどれかの圧縮方式が表示されます。
- ページ数

  蓄積された文書のページ数が表示されます。
- 種別

  文書が何のジョブかが表示されます。種別には、[ファクス]、[プリンター]、[スキャナー]、[メール]、[未完了文書] があります。

  [未完了文書] とは、ファクス受信が途中で中断された文書のことです。

  本マニュアルの設定では、[プリンター][メール] のジョブは親展ボックスには蓄積されません。
- 高圧縮 (MRC)

  スキャン文書を取り出すときに、高圧縮指定ができるかどうかが表示されます。

  親展ボックスに保存するスキャン文書の全ページが次の設定になっているときに高圧縮指定ができます。

  - 読み取り解像度：200dpi または 300dpi
  - カラーモード：フルカラー
  - 読み取り倍率：100%

- 読み取りサイズ：50 x 50mm 以上
- 色空間：標準色空間

• 少数色

文書を取り出すときに、少数色指定ができる文書かどうかが表示されます。

[ボックスの文書一覧] 画面では、文書を選択して、[文書の取り出し][プリント][削除] が可能です。

< 文書取り出し >

取り出したい文書のチェックボックスにチェックマークを付けて、[文書取り出し] ボタンをクリックすると、[親展ボックスの文書取り出し] 画面が表示され、ここで指定した取り出し方法に従って、文書を取り出すことができます。

• 1 ページ取り出し

カラー文書を JPEG で取り出す場合は、チェックボックスをチェックします。

• ページ番号

カラー文書を JPEG で取り出す場合は、ページ番号を指定します。[1 ページ取り出し] をチェックしないと、複数ページの文書は、マルチページ TIFF になります。

• 取り出しフォーマット

取り出すときのフォーマットを設定します。

TIFF/JPEG、PDF、DocuWorks、または XML Paper Specification（XPS）フォーマットのいずれかを指定できます。

• サムネール

サムネールを付加するかどうかを設定します。

• 高圧縮（MRC）

文書の高圧縮を行うかどうかを設定します。

• 画質

高圧縮をするときの圧縮率を設定します。

< 文書のプリント >

親展ボックスにあるファクス文書、スキャン文書のプリント方法を指定します。

用紙トレイ、プリント部数などの設定項目が表示されます。

プリントしたい文書のチェックボックスにチェックマークを付けて、[文書のプリント] ボタンをクリックすると、ここで指定したプリント方法に従って、文書をプリントできます。

プリント

[プリント] タブでは、ファイルを指定して、本機に直接プリントを指示できます。

以下に示す設定項目を、必要に応じて変更して、[スタート] ボタンをクリックすることにより、プリント指示できます。

- ファイル

  [参照 ...] ボタンをクリックして表示されるダイアログボックスから、プリントするファイルを指定します。プリントできるファイルフォーマットは、PDF、JPEG、TIFF、XML Paper Specification（XPS）、DocuWorks です。

- プリント部数

  プリント部数を、1 ～ 999 の間で設定します。

- ソート（1 部ごと ）

  ソート処理をするかどうかを設定します。

- 両面

  両面印刷を行うかどうかを設定します。

- カラーモード

  カラープリントするかどうかを設定します。カラーモードでは［自動］、［カラー］、または［白黒］が選択できます。

  カラーモードを［自動］に設定すると、原稿の色を自動的に判断し、原稿がカラーの場合はカラーで、白黒の場合は白黒でプリントされます。

- ホチキス

  ホチキスとめをするかどうかを設定します。オプションのフィニッシャーを装着している場合だけ設定できます。

- パンチ

  パンチ穴をあけるかどうかを設定します。オプションのフィニッシャーを装着している場合だけ設定できます。

- 排出先

  排出先を設定します。排出先が 2 つ以上ある場合に表示されます。本体に装着されているものだけ表示されます。

- 用紙トレイ

  使用する用紙トレイを設定します。［自動］を選択すると、本機が自動的にトレイを選択します。

- 用紙サイズ

  使用する用紙サイズを設定します。

- 用紙種類

  使用する用紙の種類を設定します。

- プリント種類

  プリントする方式を設定します。[通常プリント][サンプルプリント][時刻指定プリント][セキュリティープリント] などが指定できますが、本マニュアルに沿って設定された本機では、指定されたプリント方式は無視され、CentreWare Internet Services にログインしたユーザーのプライベートプリントジョブとして本機に蓄積保存されます。

デジタル証明書の設定

CentreWare Internet Services を使って、本機のデジタル証明書を設定できます。自己証明書を作成するか、外部で作成した証明書をインポートできます。また、証明書署名要求（CSR）を生成することもできます。

新規証明書の作成

作成する証明書の種類を選択し、［次へ］ボタンをクリックします。

［自己証明書］を選択すると、［自己証明書の作成］画面が表示されます。

［証明書署名要求（CSR)］を選択すると、［証明書署名要求（CSR）の生成］画面が表示されます。

自己証明書の作成

以下の項目を設定し、［新しい設定を適用］ボタンをクリックすると、自己証明書が本機に設定されます。すでに自己証明書がある場合は、上書きされます。

- デジタル署名の方式

  ［RSA/SHA-256］、［RSA/SHA-384］、［RSA/SHA-512］、［ECDSA/SHA-256］、［ECDSA/SHA-384］、［ECDSA/SHA-512］から選択します。
- 公開鍵のサイズ

  ［2048bit］、［3072bit］から選択します。
- 楕円曲線

  ［P-256］、［P-384］、［P-521］から選択します。
- 発行者

  署名者の識別名を半角 64 文字以内で入力します。
- 有効期間 (日数)

  証明書の有効日数を 1 から 9999 日の範囲で入力します。

証明書署名要求（CSR）の生成

以下の項目を設定し、［新しい設定を適用］ボタンをクリックすると、［証明書署名要求（CSR）の詳細］画面が表示されます。

- デジタル署名の方式

  ［RSA/SHA-1］、［RSA/SHA-256］、［RSA/SHA-384］、［RSA/SHA-512］、［ECDSA/SHA-1］、［ECDSA/SHA-256］、［ECDSA/SHA-384］、［ECDSA/SHA-512］から選択します。
- 公開鍵のサイズ

  ［2048bit］、［3072bit］から選択します。
- 楕円曲線

  ［P-256］、［P-384］、［P-521］から選択します。

- 2 文字の国名（C）

  本機の所在地の国名コードを、アルファベット 2 文字で入力します。

- 都道府県名（ST）

  本機の所在地の都道府県名を、英数字 16 文字以内で入力します。この項目は、省略できます。

- 市区町村名（L）

  本機の所在地の市、区、町、または村名を、英数字 32 文字以内で入力します。この項目は、省略できます。

- 組織名（O）

  証明書を申請する組織名を、英数字 32 文字以内で入力します。

- 組織単位名（OU）

  証明書を申請する部署の名前を、英数字 32 文字以内で入力します。

- 一般名（CN）

  本機のホスト名が表示されます。ホスト名は、［プロパティ］タブ > ［本体説明］で設定できます。

- アドレス

  本機のメールアドレスが表示されます。メールアドレスは、［プロパティ］タブ > ［本体説明］で設定できます。

証明書のインポート

以下の項目を設定し、［インポート］ボタンをクリックすると、指定した証明書が本機に設定されます。

- パスワード

  PKCS#12 形式データの復号用のパスワードを英数字 36 文字以内で入力します。

  入力したパスワードは［*］（アスタリスク）、または［●］（黒丸）で表示されます。

- パスワードの確認

  確認のために、PKCS#12 形式データの復号用のパスワードをもう一度入力します。

  入力したパスワードは［*］（アスタリスク）、または［●］（黒丸）で表示されます。

- 証明書

  インポートするファイルを指定します。

  X.509（DER/PEM）形式、PKCS#7（DER）形式、および PKCS#12（DER）形式のデータがインポートできます。

補足

PSTN ファクス - ネットワーク間の分離

本機は、ファクスモデム機能を持ち、公衆電話回線を介して、ファクスデータの送受信機能を提供します。サポートするプロトコルは ITU-T G3 モードのみです。

データモデム機能は持たず、ファクスインタフェースで送受信が許されているのは、利用者のファクス画像データのみです。

ファクス回線とネットワークの処理は完全に分離されおり、ファクス回線からのデータがネットワーク側に影響することはありません。

監査ログの詳細

監査ログには以下の表に記載される事象が記録されます。

対象事象	記録される監査事象名	監査事象詳細	結果
監査機能の起動と終了	System Status	Started normally (cold boot)	–
		Started normally (warm boot)	
		Shutdown requested	
ジョブの終了	Job Status	Print	Completed, Canceled by User
		Copy	
		Scan	
		Fax	
		Mailbox	
		Print Reports	
利用者認証失敗 利用者識別失敗 (操作パネルから)	Login/Logout	Login	Failed (Invalid UserID), Failed (Invalid Password)
利用者認証失敗 利用者識別失敗 (CentreWare Internet Services から)	Login/Logout	Login	Failed Web User Interface
利用者認証失敗 利用者識別失敗 (プリンタードライバーから)	Job Status	Print	Aborted
管理機能の利用	Device Settings	View Security Setting	Successful
		Change Security Setting	
		Switch Authentication Mode	
		Edit User	Successful
		Add User	
		Delete User	
	Audit Policy	Audit Log	Enable/Disable
役割の一部である利用者グループの改変	Device Settings	Edit User	Successful
時刻の変更	Device Settings	Adjust Time	Successful
セション確立の失敗 (ＴＬＳ，ＩＰＳｅｃ)	Communication	Trusted Communication	Failed (プロトコル、通信先、失敗の理由も保存)

付録

設定手順一覧

本機は機械管理者および機械管理の権限が設定された認証ユーザーのみに、下記表に示すセキュリティ管理機能の参照と設定変更、および各機能の詳細情報を設定するユーザーインタフェースを提供します。

また、機械管理の権限もしくは集計管理の権限が設定されていない認証ユーザーは、自分のパスワード変更のみ可能です。

項目	操作パネルから	CentreWare Internet Services から	初期値
日付、時刻の設定	［仕様設定］>［共通設定］>［システム時計 / タイマー設定］	−	−
スキャナー（URL 送信）の設定	［カスタマイズ］>［スキャナー(URL 送信)］	−	有効
リモートアシスタンスの設定	［カスタマイズ］>［リモートアシスタンス］	−	有効
BMLinkS の設定	［カスタマイズ］>［BMLinkS］	−	有効
外部アクセス	［カスタマイズ］>［外部アクセス］	−	有効
本体パネルからのパスワード使用の設定	［認証 / セキュリティ設定］>［認証の設定］>［パスワードの運用］>［パスワード使用 - パネル入力時］	−	無効
ハードディスクの上書き消去の設定	［認証 / セキュリティ設定］>［ハードディスクの上書き消去設定］	［プロパティ］>［セキュリティー］>［ハードディスクの上書き消去設定］	1 回
ハードディスクデータの暗号化設定	［仕様設定］>［共通設定］>［その他の設定］>［データの暗号化］	−	無効
認証方式の設定	［認証 / セキュリティ設定］>［認証の設定］>［認証方式の設定］	［プロパティ］>［セキュリティー］>［認証管理］	無効
プライベートプリントの設定	［認証 / セキュリティ設定］>［認証の設定］>［認証 / プライベートプリントの設定］>［認証成功のジョブ］	−	プリント
SMB の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［SMB クライアント ］	−	有効
ファクスの設定	［仕様設定］>［ファクス設定］>［ファクス動作制御］>［ダイレクトファクスの使用］	−	有効
	［仕様設定］>［ファクス設定］>［ファクス動作制御］>［相手機からのポーリング / 蓄積］	−	有効
受信ファクス文書蓄積用親展ボックスの作成	［登録 / 変更］>［ボックス登録］	［スキャン］>［ボックス］>［登録］	−

項目	操作パネルから	CentreWare Internet Services から	初期値
受信回線別ボックスセレクターの設定	［仕様設定］>［ファクス設定］>［ファクス動作制御］>［受信回線別ボックスセレクター］ ［仕様設定］>［ファクス設定］>［受信文書の保存先 / 排出先］>［受信回線別ボックスセレクター］	−	無効
ソフトウェアダウンロードの設定	［仕様設定］>［共通設定］>［その他の設定］>［ソフトウェアダウンロード］	−	有効
自動リセットの設定	［仕様設定］>［共通設定］>［システム時計 / タイマー設定］>［自動リセット］	−	有効
レポート出力の設定	［仕様設定］>［共通設定］>［レポート設定］>［レポート出力の許可］	−	有効
機械起動時のプログラム診断の設定	［仕様設定］>［共通設定］>［保守］>［機械起動時のプログラム診断］	−	無効
機械管理者パスワードの変更	［認証 / セキュリティ設定］>［機械管理者情報の設定］>［機械管理者パスワード］	［プロパティ］>［ セキュリティー ］>［ 機械管理者情報の設定 ］	−
認証失敗アクセス拒否回数の設定	［認証 / セキュリティ設定］>［認証の設定］>［不正使用防止の設定］	［プロパティ］>［セキュリティー］>［認証情報の設定］>［認証回数制限］	5
アクセス制御の設定	［認証 / セキュリティ設定］>［認証の設定］>［アクセス制御］	［プロパティ］>［セキュリティー］>［認証管理］	無効
パスワードの最小文字数の設定	［認証 / セキュリティ設定］>［認証の設定］>［パスワードの運用］>［パスワードの最小桁数］	［プロパティ］>［セキュリティー］>［認証情報の設定］>［パスワードの最小桁数］	0
TLS の設定	［仕様設定］>［ネットワーク設定］>［セキュリティ設定］>［SSL/TLS 設定］	［プロパティ］>［セキュリティー］>［証明書の設定］>［証明書の作成］>［自己証明書］>［SSL/TLS 設定］	無効
TCP/IP の設定	［仕様設定］>［ネットワーク設定］>［プロトコル設定］>［TCP/IP - 共通設定］	［プロパティ］>［ネットワーク設定］>［プロトコル］>［TCP/IP］	ー
WebDAV の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［WebDAV］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［WebDAV］	有効
メール受信	［仕様設定］>［ネットワーク設定］>［ポート設定］>［メール受信］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［メール受信］	無効
IPP の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［IPP］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［IPP］	無効
デバイス証明書のインポート	−	［プロパティ］>［セキュリティー］>［証明書の設定］>［証明書のインポート］	ー
IPSec の通信設定	［仕様設定］>［ネットワーク設定］>［セキュリティ設定］>［IPSec］	［プロパティ］>［セキュリティー］>［IPSec］	無効

項目	操作パネルから	CentreWare Internet Services から	初期値
WSD スキャンの設定	−	［プロパティ］>［ネットワーク設定］>［ポート起動］>［WSD（Scan）］	有効
SOAP の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［SOAP］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［SOAP］	有効
SNMP の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［SNMP］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［SNMP］	有効
Bonjour の設定	［仕様設定］>［ネットワーク設定］>［ポート設定］>［Bonjour］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［Bonjour］	有効
USB の設定	−	［プロパティ］>［サービス設定］>［USB］	有効
	［仕様設定］>［ネットワーク設定］>［ポート設定］>［USB］	［プロパティ］>［ネットワーク設定］>［ポート起動］>［USB］	有効
CSRF の設定	−	［プロパティ］>［ネットワーク設定］>［プロトコル設定］>［HTTP］>［CSRF 対策］	無効
カストマーエンジニアの操作制限の設定	［仕様設定］>［共通設定］>［その他の設定］>［カストマーエンジニアの操作制限］	［プロパティ］>［セキュリティー］>［カストマーエンジニアの操作制限］	無効
監査ログの起動、取り出し	−	［プロパティ］>［セキュリティー］>［監査ログ］>［監査ログの起動］	無効
ブラウザ表示更新の設定	−	［プロパティ］>［一般設定］>［Internet Services 設定］>［表示更新時間］	有効
ブラウザセッションタイムアウトの設定	−	［プロパティ］>［一般設定］>［Internet Services 設定］>［セッションタイムアウト時間］	20
カスタムサービスの設定	−	［プロパティ］>［セキュリティー］>［ プラグイン / カスタムサービス設定 ］>［ 組み込みプラグイン機能 ］ ［プロパティ］>［セキュリティー］>［ プラグイン / カスタムサービス設定 ］>［ カスタムサービス］	有効

補足

- 「WSD」とは、「Web Services on Devices」の略です。

商品構成表

商品名	商品コード	備考
DocuCentre-VII C2273 PFS	NC100559	別途、データ上書き消去キットが必要
DocuCentre-VII C3373 PFS	NC100559	別途、データ上書き消去キットが必要
ApeosPort-VII C2273 PFS	NC100559	別途、データ上書き消去キットが必要
ApeosPort-VII C3373 PFS	NC100559	別途、データ上書き消去キットが必要
DocuCentre-VII C4473 PFS	NC100560	別途、データ上書き消去キットが必要
DocuCentre-VII C5573 PFS	NC100560	別途、データ上書き消去キットが必要
ApeosPort-VII C4473 PFS	NC100560	別途、データ上書き消去キットが必要
ApeosPort-VII C5573 PFS	NC100560	別途、データ上書き消去キットが必要
DocuCentre-VII C6673 PFS	NC100561	別途、データ上書き消去キットが必要
DocuCentre-VII C7773 PFS	NC100561	別途、データ上書き消去キットが必要
ApeosPort-VII C6673 PFS	NC100561	別途、データ上書き消去キットが必要
ApeosPort-VII C7773 PFS	NC100561	別途、データ上書き消去キットが必要
ApeosPort-VII C3373 PFS-2TS	NC100562	別途、データ上書き消去キットが必要
ApeosPort-VII C5573 PFS-2TS	NC100563	別途、データ上書き消去キットが必要
データ上書き消去キット	EC103666	

ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C2273、
DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C2273
セキュリティ機能補足ガイド

著作者 – 富士ゼロックス株式会社
発行者 – 富士ゼロックス株式会社

発行年月 – 2019 年 11 月　第 1 版

（帳票番号 :ME8390J1-1_20191007）