

DocuCentre-VI C2264

セキュリティ機能補足ガイド

- セキュリティ機能をお使いいただく前に 2
- 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) 9
- 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) 15
- 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) 22
- 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) 23
- ユーザー認証 25
- 自己テスト 26
- 付録 27

Bonjour は、米国および他の国々で登録された Apple Inc. の商標です。
その他の社名、または商品名等は各社の登録商標または商標です。

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・改編することはおやめください。
- 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。

Xerox、Xerox ロゴ、および Fuji Xerox ロゴは、米国ゼロックス社の登録商標または商標です。
CentreWare は、米国ゼロックス社の登録商標または商標です。

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。

メディア（ソフトウェア / 製品マニュアル） 帳票番号	PDF 帳票番号
電子マニュアル (HTML 形式) MB3639J1-1	DocuCentre-VI C2264 ユーザーズガイド： ME8371J1-1
	DocuCentre-VI C2264 管理者ガイド： ME8372J1-1

DocuCentre-VI C2264 のセキュリティ機能は以下の ROM バージョンで動作しません。

DocuCentre-VI C2264 CP

Controller ROM Ver. 1.1.3

FAX ROM Ver. 2.2.0

DocuCentre-VI C2264 CPFS

Controller ROM Ver. 1.1.3

FAX ROM Ver. 2.2.0

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 EAL2+ALC_FLR.2 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 バージョンは、「ROM バージョン、システム時計、商品コードの確認」(P.7) に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ります。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タマーエンジニアにご連絡ください。また、購入されたオプション商品が、IT セキュリティ認証の対象商品を構成するものであることを確

認するには、各オプション商品の梱包ラベルに記載の商品コードが、付録 商品構成表にある商品コードと一致することをご確認ください。

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、これらの機能がオプションのモデルでは、データセキュリティキット、ファクスキット 3、スキャナーキットを購入し装着する必要があります。

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「カスタ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。また、ハードディスクが装備されていることは、操作パネル上で「ハードディスクデータの上書き消去」設定メニュー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『管理者ガイド』の「5. 仕様設定」>「仕様設定の流れ」をご確認ください。

セキュリティ機能

本機は、以下に示すセキュリティ機能を持ちます。

- ハードディスク蓄積データ上書き消去機能
- ハードディスク蓄積データ暗号化機能
- ユーザー認証機能
- システム管理者セキュリティ管理機能
- カスタマーエンジニア操作制限機能
- セキュリティ監査ログ機能
- 内部ネットワークデータ保護機能
- インフォメーションフローセキュリティ機能
- 自己テスト機能

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.9)
 - 「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.15)
 - 「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.22)
 - 「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.23)
- 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
[する] に設定し、12文字の暗号化キーを入力。
- 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。
- ダイレクトファクス
無効に設定。
- 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。
- SMB
無効に設定。
- スキャナー (URL 送信)
無効に設定。
- ソフトウェアダウンロード
[禁止] に設定。
- オートクリア
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。
- システム管理者の認証失敗アクセス拒否
[5] 回に設定。
- アクセス制御
[デバイスへのアクセス] と [機能の使用制限] を [制限する] に設定。
[サービスへのアクセス] を [制限する (表示)]、または [制限する (非表示)] 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。
- WebDAV
無効に設定。
- メール送信

- 無効に設定。
- メール受信
無効に設定。
- IPP
有効に設定。
- IPSec 通信
有効に設定。
- SNMP
無効に設定。
- WSD (スキャン)
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。
- カスタ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。
- ジョブの削除
機械管理者のみに設定。
- 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、本書の順に従い最初からやり直してください。
- 本書での設定は、カスタ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。カスタマーエンジニアに保守操作を許可した場合は、セキュリティ機能が維持できなくなることがありますので、ご注意ください。
- インフォメーションフローセキュリティ機能については、システム管理者による特別な設定は不要です。
- 暗号化を無効にしてから、再度有効にする場合は、12文字の暗号化キーを入力してください。
- カスタ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、共有鍵（クライアント PC と本機のセットアップの両方に対して）と、暗号化キーは、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。
- システム管理者は、組織変更等により利用者がなくなった場合、適切に登録ユーザーを削除してください。
- 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、IPSec）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）および TLS 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

■IPSec

本機が接続する IPSec ホストでは、以下の暗号化方式およびメッセージダイジェスト方式が利用されるように設定します。

- AES(128 ビット)/SHA1
- 3Key Triple DES(168 ビット)/SHA1

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暗号化キーを変更することで、ハードディスクを初期化してください。
- TLS の脆弱性を避けるために、ブラウザ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。
- 本機は S/MIME 機能を有していないため、E メールとインターネットファクス機能は使用しないでください。
- CentreWare Internet Services を利用時、20 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、20 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、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 操作パネルの〈機械確認 (メーター確認)〉ボタンを押します。
- 2 タッチパネルディスプレイの [機械状態 レポート出力] 画面で、[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 操作パネルの〈機械確認 (メーター確認)〉ボタンを押します。
- 2 タッチパネルディスプレイの [機械状態 レポート出力] 画面で、[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 操作パネルの〈スタート〉ボタンを押します。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 操作パネルの〈認証〉ボタンを押します。
- 2 〈数字〉ボタン、またはタッチパネルディスプレイに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 タッチパネルディスプレイの [確定] を押します。

- 4 [仕様設定 / 登録] を押します。
- 5 [仕様設定] を押します。
- 6 [共通設定] を押します。
- 7 [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。
- 8 変更する項目を選択します。
- 9 [確認 / 変更] を押します。
- 10 変更する項目を選択して、変更します。
- 11 [決定] を押します。
- 12 [閉じる] を 2 回押して、[仕様設定 / 登録] 画面を終了します。

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。

機械管理者モードに入るための認証

- 1 操作パネルの〈認証〉ボタンを押します。
- 2 〈数字〉ボタン、またはタッチパネルディスプレイに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 タッチパネルディスプレイの [次へ] を押します。
- 4 パスワード入力が必要された場合は、キーボードからパスワードを入力します。
- 5 [確定] を押します。
- 6 [仕様設定 / 登録] 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。

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 [その他の設定] 画面で、[データの暗号化] を選択します。
- 5 [確認 / 変更] を押します。
- 6 [する] を押します。
- 7 [新しい暗号化キー] を押して、12 文字の暗号化キーを入力します。
- 8 [決定] を押します。
- 9 [暗号化キーの再入力] を押して、暗号化キーを再入力します。
- 10 [決定] を 2 回押します。
- 11 確認画面が表示されたら、[はい (変更する)] を押します。
- 12 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。

認証方式の設定後、『管理者ガイド』の「14 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。

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 [決定] を押します。
- 11 [閉じる] を押して、[認証 / プライベートプリントの設定] 画面を終了します。

ダイレクトファクスの設定

- 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 [禁止] を選択します。
- 6 [閉じる] を押します。
- 7 画面右上の [閉じる] を押して、[ファクスの設定] 画面を終了します。

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ます。
- 8 [閉じる] を押します。

受信回線別ボックスセレクトターの設定

- 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トター] を選択し「確認 / 変更」を押します。
- 5 [有効] を押します。
- 6 [決定] を押します。
- 7 [閉じる] を押します。
- 8 [受信文書の保存先 / 排出先] を押します。
- 9 [受信回線別ボックスセレクトター] を押します。
- 10 登録したい回線を選択し、[確認 / 変更] を押します。
- 11 [指定する] を押します。
- 12 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。
- 13 [決定] を押します。
10 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。
- 14 [閉じる] を押します。
- 15 画面右上の [閉じる] を押して、[ファクスの設定] 画面を終了します。

SMB の設定

- 1 [仕様設定 / 登録] 画面で、[ネットワーク設定] を押します。
- 2 [ポート設定] を押します。
- 3 [SMB クライアント] を押します。
- 4 [確認 / 変更] を押します。
- 5 [停止] を選択します。
- 6 [閉じる] を押します。
- 7 画面右上の [閉じる] を押して、[ネットワーク設定] 画面を終了します。

スキャナー (URL 送信) 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 [画面 / ボタンの設定] を押します。
- 4 [メニュー画面の機能配列] を選択します。
- 5 [確認 / 変更] を押します。
- 6 [スキャナー (URL 送信)] を押し [未設定] を選択します。
- 7 [閉じる] を押します。
- 8 [決定] を押します。
- 9 [閉じる] を押して、[画面 / ボタンの設定] 画面を終了します。

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 [その他の設定] 画面で、[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] を押して、[その他の設定] 画面を終了します。

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] を押して、[システム時計 / タイマー設定] 画面を終了します。

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 [レポート出力ボタンの表示] を押します。
- 5 [しない] を押します。
- 6 [決定] を押します。
- 7 [閉じる] を押して、[レポート設定] 画面を終了します。

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 [保守] 画面で、[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 2 回押して、[仕様設定 / 登録] 画面を終了します。
- 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、『管理者ガイド』の「5 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.6) 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 認証を要求された場合は、機械管理者 ID とパスワードを入力します。
- 3 [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。

システム管理者の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 [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 ID の認証失敗によるアクセス拒否:] へ [5] 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。

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 [再起動] をクリックします。

パスワードの最小桁数の設定

- 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 [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 必要に応じて、公開キーのサイズを設定します。
- 5 必要に応じて、発行者を設定します。

- 6 [新しい設定を適用] をクリックします。
- 7 [SSL/TLS 設定] をクリックします。
- 8 [HTTP-SSL/TLS 通信] の [有効] チェックボックスをチェックします。
- 9 [新しい設定を適用] をクリックします。
- 10 [再起動] をクリックします。

メール送信の設定

- 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 [メール送信] 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。

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] 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 [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 以下の手順で [事前共有鍵] での設定を行います。
 - 1) [IPSec] をクリックします。
 - 2) [プロトコル] の [有効] チェックボックスをチェックします。
 - 3) [IKE 認証方式] の欄で、[事前共有鍵] を選択します。
 - 4) [共有鍵] と [共有鍵の照合] の欄に 9 文字以上の共有鍵を入力します。続けて、IPSec アドレスの設定を行います。

IPSec アドレスの設定

- 1 [IP Sec] 画面で、[相手アドレスの指定 [IPv4]] の欄に、IP アドレスを入力します。
- 2 [相手アドレスの指定 [IPv6]] の欄に、IP アドレスを入力します。
- 3 [IPSec 未対応機器との通信] で、[通常の通信] または [通信しない] を選択します。
- 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 スキャンの設定

- 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。

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。

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。

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。

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 [起動] 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。

補足

- 機器の構成により設定でき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。

カスタ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 [カスタ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。

監査ログの起動

- 1 [プロパティ] タブをクリックします。
- 2 [セキュリティー] をクリックします。
- 3 [監査ログ] をクリックします。
- 4 [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。
- 5 [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。

ジョブ削除の設定

- 1 [プロパティ] 画面で、[一般設定] をクリックします。
- 2 [ジョブ管理] をクリックします。
- 3 [ジョブの削除] で [機械管理者のみジョブを削除] を選択します。
- 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。

注記

- 利用者は機械で実行中のコピー、プリント、スキャンジョブを一時停止することができます。ただし、本機能によりシステム管理者だけが停止中のジョブを終了させることができますので、安全のためにジョブの削除を必ず実施してください。

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

- Windows PC で LPR コマンドを利用するには、Windows の設定で、LPR ポート 모니터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、システム管理者のクライアント PC から CentreWare Internet Services を使用して、監査ログを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 NV メモリーに保存され、50 件単位で一つのファイル（以降、「監査ログファイル」と呼びます）として、最大 15,000 件まで本機のハードディスクへ保存されます。15,000 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。

監査ログファイルへは、CentreWare Internet Services にシステム管理者として認証した場合だけアクセス可能で、操作パネルからアクセスすることはできません。

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。

- 1 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 認証を要求された場合は、システム管理者の ID とパスワードを入力します。
- 3 [プロパティ] タブをクリックします。
- 4 [セキュリティー] をクリックします。
- 5 [監査ログ] をクリックします。
- 6 [監査ログの取り出し] の [txt ファイルで取り出す] をクリックします。

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、一般利用者は User ID とパスワードによる認証が必要です。

- 1 操作パネルの〈認証〉ボタンを押します。
- 2 〈数字〉ボタン、またはタッチパネルディスプレイに表示されるキーボードを使って、User ID を入力します。
- 3 [次へ] を押します。
- 4 パスワードを入力します。
- 5 [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。

注記

- 他の人が使用している途中で割り込み操作を行う場合は、作業が終了したら必ず認証を解除してから割り込みを解除してください。

例：A さんの認証で使用中 > 割り込み > B さんで認証（ログイン） > 割り込み作業
> B さんで認証解除（ログアウト） > 割り込み解除

補足

- 本体認証を利用する場合、機械管理者 ID だけが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 の登録については、『管理者ガイド』の「5 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。

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、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を表示します。

付録

設定手順一覧

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]	-	-
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]	[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]	[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]	-	無効
ダイレクトファクスの設定	[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]	-	有効
受信回線別ボックスセクターの設定	[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クター]	-	無効
SMB の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	-	有効
スキャナ (URL 送信) の設定	[仕様設定] > [共通設定] > [画面 / ボタンの設定] > [メニュー画面の機能配列]	-	有効
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] > [レポート出力ボタンの表示]	-	有効
機械起動時のプログラム診断の設定	[仕様設定] > [保守] > [機械起動時のプログラム診断]	-	無効

項目	操作パネルから	CentreWare Internet Services から	初期値
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]	[セキュリティー] > [機械管理者情報の設定]	-
システム管理者の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] > [機械管理ユーザーの認証失敗アクセス拒否]	[セキュリティー] > [機械管理者情報の設定]	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]	[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]	[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]	[セキュリティー] > [証明書の設定] > [自己証明書の作成] > [SSL/TLS 設定]	無効
WebDAV の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	有効
メール送受信の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	無効
IPP の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	無効
デバイス証明書のインポート	-	[セキュリティー] > [証明書の設定] > [証明書のインポート]	-
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 設定]	[セキュリティー] > [IPSec]	無効
SNMP の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	有効
WSD(スキャン) の設定	-	[ネットワーク設定] > [ポート起動]	有効
SOAP の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	有効
Bonjour の設定	[仕様設定] > [ネットワーク設定] > [ポート設定]	[ネットワーク設定] > [ポート起動]	有効
USB の設定	-	[サービス設定] > [USB]	有効
CSRF の設定	-	[ネットワーク設定] > [プロトコル設定] > [HTTP]	無効
カスタ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] > [カスタマーエンジニアの操作制限]	[セキュリティー] > [カスタ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	-	[セキュリティー] > [監査ログ]	無効
ブラウザ表示更新の設定	-	[一般設定] > [Internet Services 設定] > [表示更新時間]	有効

項目	操作パネルから	CentreWare Internet Services から	初期値
ジョブ削除の設定	-	[一般設定] > [ジョブ管理] > [ジョブの削除]	全ユーザー

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-VI C2264 CP	NC100556	別途、データセキュリティキット、ファクス キット 3、スキャナーキットが必要
DocuCentre-VI C2264 CPFS	NC100557	別途、データセキュリティキットが必要
データセキュリティキット	EC103551	
ファクスキット 3	QC100164	
スキャナーキット	EC103545	

DocuCentre-VI C2264
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 4 月 第 1 版

(帳票番号 :ME8373J1-2_20190306)