ApeosPort® 3060
ApeosPort® 2560
ApeosPort® 1860

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

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。

対象機種
ApeosPort 3060/2560/1860

セキュリティ機能

ApeosPort 3060/2560/1860 は、次の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

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、システム管理者は次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は、次を参照してください。
  - 「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.8）
  - 「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.14）
  - 「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.23）
  - 「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.24）

各設定手順において変更が失敗した場合、変更操作を実施した直後に失敗のメッセージが表示されます。その場合は、再度手順に沿って設定を確認してください。それでも失敗する場合には、弊社の営業担当者またはカストマーエンジニアにお問い合わせください。

- スキャン送信

  無効に設定。

- リモートアシスタンス

  無効に設定。

- パスワード使用 - パネル入力時
  ［する］に設定。
- データの暗号化
  有効に設定。
- 認証方式
  ［本体認証］に設定。
- プライベートプリント
  ［プリンターの認証に従う］に設定。
- ダイレクトプリント機能の禁止
  ［する］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。
- 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
  ［操作パネルへのアクセス］、［仕様設定操作］を［制限する］に設定。
  ［アプリの制限］を［すべて制限する］に設定。
- ジョブ操作
  ［実行中 / 待ちジョブの表示設定］の［表示情報の制限］を［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。
- 証明書のインポート
  必要な証明書をインポートする。

- FIPS140-2
  有効に設定。
- HTTP
  ［HTTPS のみ起動］に設定。
- TCP/IP
  IPv4 に設定。
- BMLinkS
  無効に設定。
- WebDAV
  無効に設定。
- POP3
  無効に設定。
- IPP
  有効に設定。
- IPSec 通信
  無効に設定。
- WSD
  無効に設定。
- LPD
  無効に設定。
- Port9100
  無効に設定。
- FTP クライアント
  無効に設定。
- SOAP
  無効に設定。
- SNMP
  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。
- プラグイン
  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。
- 監査ログによる定期検査
  監査ログを自動で取り出す設定をします。

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。
- 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ともに、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、本機の使用方法およ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。
- パスワードを容易に推測されないようにするため、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
- 利用者はユーザー 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、必ずユーザー 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。
- 親展ボックスには指示書を関連付けないでください。親展ボックスに指示書を関連付けた運用は評価対象外です。

- 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。受信ファクス文書が出力され、放置される可能性があり、情報漏洩となる恐れがあります。
- 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、次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 サイトへの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。攻撃者により、他の Web サイトや他のアプリケーションを経由した攻撃を受けるおそれがあります。
TLS の脆弱性を避けるために、Web ブラウザーのプロキシ例外リストに本機のアドレスを設定してください。本機とリモート PC 上の Web 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。使用を許可されていない人が、ログアウトされていない CentreWare Internet Services を使用して本機を操作する恐れがあります。

補足

- NTP サーバーとの接続機能は評価対象外です。

ソフトウェアバージョン、システム時計、商品コードの確認

初期設定を行う前に、システム管理者は本機のソフトウェア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［設定］をタップします。

2 ［機械確認 / レポート］をタップします。

3 ［ソフトウェアバージョン］をタップします。

画面上で、本機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ソフトウェアバージョン、商品コードの確認方法

1 タッチパネルディスプレイで［設定］をタップします。

2 ［機械確認 / レポート］をタップします。

3 ［レポート / リストの出力］をタップします。

4 ［プリンター設定］をタップします。

5 ［機能設定リスト（共通項目）］をタップします。

プリントされたレポート上で、本機のソフトウェアバージョン、商品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］をタップします。

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 ［OK］をタップします。

4 警告メッセージに対して［閉じる］をタップします。

5 タッチパネルディスプレイで［設定］をタップします。

6 ［システム設定］をタップします。

7 ［システム時計 / タイマー設定］をタップします。

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 適切な日時に変更します。

10 ［OK］をタップします。

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。
また、設定変更後に再起動の確認画面が表示された場合は、再起動を行ってください。

スキャン送信の設定

1 タッチパネルディスプレイ左上の［一般ユーザー］をタップします。

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 ［OK］をタップします。

4 警告メッセージに対して［閉じる］をタップします。

5 画面下までスクロールして、［カスタマイズ］をタップします。

6 ［ホームの編集］をタップします。

7 ［スキャン送信］の［×］をタップして削除します。

8 ［完了］をタップします。

リモートアシスタンスの設定

1 画面下までスクロールして、［カスタマイズ］をタップします。

2 ［ホームの編集］をタップします。

3 ［リモートアシスタンス］の［×］をタップして削除します。

4 ［完了］をタップします。

パスワード使用 - パネル入力時の設定

1 ［設定］画面で、［認証 / 集計管理］をタップします。

2 ［認証・セキュリティ設定］をタップします。

3 ［認証の設定］をタップします。

4 ［パスワードの運用］をタップします。

5 ［パスワードの運用］画面で、［パスワード使用 - パネル入力時］をタップします。

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 ［OK］をタップします。

データの暗号化設定

1 ［設定］画面で、［システム設定］をタップします。

2 ［共通設定］をタップします。

3 ［その他の設定］をタップします。

4 ［データの暗号化］をタップします。

5 ［する］をタップします。

6 ［OK］をタップします。

7 確認画面が表示されたら、［はい（変更する)］をタップします。

認証方式の設定

1 ［設定］画面で、［認証 / 集計管理］をタップします。

2 ［認証・セキュリティ設定］をタップします。

3 ［認証の設定］をタップします。

4 ［認証方式の設定］をタップします。

5 ［認証方式の設定］画面で、［本体認証］をタップします。

6 ［OK］をタップします。

7 ホームボタンをタップします。

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

補足

- 本体認証の場合、ユーザーを削除すると、ユーザーに関連する親展ボックスや、プライベートプリントデータなどが削除されます。

* 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 ［設定］をタップします。

2 ［設定］画面で、［認証 / 集計管理］をタップします。

3 ［認証・セキュリティ設定］をタップします。

4 ［認証の設定］をタップします。

5 ［認証 / プライベートプリントの設定］をタップします。

6 ［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。

7 ［受信制御］画面で、［プリンターの認証に従う］を選択します。

8 ［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。

9 ［認証が不正のジョブ］で［ジョブを中止］を選択します。

10 ［ユーザー ID なしのジョブ］で［ジョブを中止］を選択します。

11 ［OK］をタップします。

ダイレクトプリント機能の禁止の設定

1 ［設定］をタップします。

2 ［設定］画面で、［認証 / 集計管理］をタップします。

3 ［認証・セキュリティ設定］をタップします。

4 ［ダイレクトプリント機能の禁止］をタップします。

5 ［する］をタップします。

6 ［OK］をタップします。

SMB の設定

1 ［設定］をタップします。

2 ［ネットワーク設定］をタップします。

3 ［ポート設定］をタップします。

4 ［SMB クライアント］をタップします。

5 ［SMB クライアント - ポート］をタップします。

6 ［停止］を選択します。

ファクスの設定

1 ［設定］画面で、［アプリ設定］をタップします。

2 ［ファクス設定］をタップします。

3 ［ファクス動作制御］をタップします。

4 ［ダイレクトファクスの使用］をタップします。

5 ［禁止］を選択します。

6 ［相手機からのポーリング / 蓄積］をタップします。

7 ［禁止］を選択します。

8 ［OK］をタップします。

9 ホームボタンをタップします。

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 ［ボックス操作］をタップします。

3 ［+］ボタンをタップします。

4 登録する親展ボックスを選択します。

5 ［ボックス名称］に適当な名称を入力します。

6 ［アクセス制御 / パスワード］のチェックマークを外します。

7 ［OK］をタップします。

8 ［OK］をタップします。

受信回線別ボックスセレクターの設定

1 ［設定］をタップします。

2 ［設定］画面で、［アプリ設定］をタップします。

3 ［ファクス設定］をタップします。

4 ［ファクス動作制御］をタップします。

5 ［受信回線別ボックスセレクター］をタップします。

6 ［有効］をタップします。

7 ［<］をタップします。

8 ［ファクス設定］の［受信文書の保存先 / 排出先］をタップします。

9 ［受信回線別ボックスセレクター］をタップします。

10 ［回線 1 の保存先］をタップします。

11 ［設定する］をタップします。

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) を入力します。

13 ［OK］をタップします。

14 ［OK］をタップします。

手順 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。

15 ホームボタンをタップします。

自動リセットの設定

1 ［設定］をタップします。

2 ［システム設定］をタップします。

3 ［システム時計 / タイマー設定］をタップします。

4 ［自動リセット］をタップします。

5 30 秒に設定し、［する］をタップします。

6 ［OK］をタップします。

レポート出力の設定

1 ［設定］をタップします。

2 ［システム設定］をタップします。

3 ［レポート設定］をタップします。

4 ［レポート出力の許可］のチェックマークを外します。

機械起動時のプログラム診断の設定

1 ［設定］をタップします。

2 ［保守］をタップします。

3 ［機械起動時のプログラム診断］を選択します。

4 ［する］をタップします。

5 ホームボタンをタップします。

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』の「詳細設定」＞「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。
また、設定変更後に再起動の確認画面が表示された場合は、再起動を行ってください。

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 ブラウザーをインストールした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〉キーをタップします。

2 ［ログイン］をクリックします。

3 機械管理者 ID とパスワードを入力し、［ログイン］をクリックします。

4 警告メッセージに対して［確認］をクリックします。

機械管理者パスワードの変更

1 ホーム画面で、機械管理者 ID をクリックします。

2 ［プロファイル］をクリックします。

3 ［パスワード変更］をクリックします。

4 ［現在のパスワード］を入力します。

5 ［新しいパスワード］に 9 文字以上の新しいパスワードを入力します。

6 ［パスワードの再入力］に同じパスワードを入力します。

7 ［保存］をクリックします。

補足

- パスワードに指定可能な文字 :
  英数字、および次の特殊文字
  (“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、“)”、” (space)”、“””、“’”、“+”、“、”、“-“、“/”、“:”、“;”、“<”、“=”、“>”、“?”、“［“、“¥”、“］”、“_”、“`”、“{“、“|”、“}”、“~”)

認証失敗アクセス拒否回数の設定

1 ホーム画面で、［認証 / 集計 / 権限］をクリックします。

2 ［認証設定］をクリックします。

3 ［詳細設定］をクリックします。

4 ［管理者権限ユーザーの認証失敗アクセス拒否］を選択します。

5 ［有効］にチェックマークを付けます。

6 ［認証回数］に［5］を入力します。

7 ［保存］をクリックします。

8 確認画面が表示されたら［後で再起動］をクリックします。

9 ［一般ユーザーの認証失敗アクセス拒否］を選択します。

10 ［有効］にチェックマークを付けます。

11 ［認証回数］に［5］を入力します。

12 ［保存］をクリックします。

アクセス制御の設定

1 ホーム画面で、［認証 / 集計 / 権限］をクリックします。

2 ［権限設定］をクリックします。

3 ［アクセス制限設定］をクリックします。

4 ［操作パネル / 仕様設定操作の制限］の［操作パネルへのアクセス］をクリックします。

5 ［制限する］を選択します。

6 ［操作パネル / 仕様設定操作の制限］の［仕様設定操作］をクリックします。

7 ［制限する］を選択します。

8 ［アプリの制限］で［すべて制限する］を選択します。

9 ［ジョブ操作の制限］ですべての操作に対して［本人と機械管理者］を選択します。

10 ［保存］をクリックします。

ジョブ操作の設定

1 ホーム画面で、[ジョブ] をクリックします。

2 [ジョブ動作設定] をクリックします。

3 [実行中 / 待ちジョブの表示設定] の [表示情報の制限] で [する] を選択します。

4 [保存] をクリックします。

パスワードの最小文字数の設定

補足
- 本機能は、本体認証時のみ有効です。

1 ホーム画面で、[認証 / 集計 / 権限] をクリックします。

2 [認証設定] をクリックします。

3 [パスワードの運用] をクリックします。

4 [最小文字数] で [制限する] を選択します。

5 [制限する最小文字数] に [9] を入力します。

6 [保存] をクリックします。

TLS の設定

1 ホーム画面で、[システム] をクリックします。

2 [セキュリティー設定] をクリックします。

3 [電子証明書] の [証明書設定] をクリックします。

4 プルダウンメニューから [デバイス証明書] をクリックします。

5 [新規作成] プルダウンメニューから [自己署名証明書の作成] を選択します。

6 必要に応じて、詳細情報を設定します。

7 [実行] をクリックします。

8 [閉じる] をクリックします。

9 [閉じる] をクリックします。

10 [ネットワークセキュリティー] の [SSL/TLS 設定] をクリックします。

11 [プロトコルバージョン] の [TLS1.2 以上] を選択します。

12 ［TLS1.3 の使用］のチェックマークを外します。

13 ［SMTP-SSL/TLS 通信］の［SSL/TLS 接続］を選択します。

14 ［相手サーバーの証明書の検証］のチェックボックスにチェックマークを付けます。

15 ［保存］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、「証明書のインポート」(P.17) 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.33) を参照してください。

証明書のインポート

本機がネットワーク接続するメールサーバーなどの証明書をインポートします。

1 ホーム画面で、［システム］をクリックします。

2 ［セキュリティー設定］をクリックします。

3 ［証明書設定］をクリックします。

4 ［インポート］をクリックします。

5 ［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。

6 必要に応じて［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。

7 ［実行］をクリックします。

FIPS140-2 の設定

1 ホーム画面で、［システム］をクリックします。

2 ［セキュリティー設定］をクリックします。

3 ［FIPS140-2 認定モード］をクリックします。

4 ［有効］をクリックします。

5 ［保存］をクリックします。

HTTP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［HTTP］をクリックします。

3 ［HTTP］の［ポート (HTTP/HTTPS)］をクリックします。

4 ［HTTPS のみ起動］を選択します。

5 ［保存］を選択します。

CSRF の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［HTTP］をクリックします。

3 ［CSRF 対策］にチェックマークを付けます。

4 ［保存］をクリックします。

TCP/IP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［インターフェイス設定］の［Ethernet］をクリックします。

3 ［共通］の［確認 / 変更］をクリックします。

4 ［IP 動作モード］をクリックします。

5 ［IPv4 モード］を選択します。

6 ［保存］をクリックします。

BMLinkS の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［BMLinkS］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

WebDAV の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［WebDAV］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

POP3 の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［POP3］をクリックします。

3 ［ポート (メール受信)］のチェックマークを外します。

4 ［保存］をクリックします。

IPP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［IPP］をクリックします。

3 ［IPP］の［ポート］にチェックマークを付けます。

4 ［保存］をクリックします。

IPSec の通信設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［IPSec］をクリックします。

3 ［IPSec］の［有効］のチェックマークを外します。

4 ［保存］をクリックします。

WSD の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［WSD］をクリックします。

3 ［WSD］の［ポート (WSD スキャン)］のチェックマークを外します。

4 ［ポート (WSD プリント)］のチェックマークを外します。

5 ［保存］をクリックします。

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

LPD の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［LPD］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

Port9100 の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［Port9100］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

FTP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［FTP クライアント］をクリックします。

3 ［FTP クライアントポート］のチェックマークを外します。

4 ［保存］をクリックします。

SOAP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［SOAP］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

SNMP の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［SNMP］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

Bonjour の設定

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［プロトコル設定］の［Bonjour］をクリックします。

3 ［ポート］のチェックマークを外します。

4 ［保存］をクリックします。

USB の設定

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。

1 ホーム画面で、［ネットワーク］をクリックします。

2 ［インターフェイス設定］の［USB］をクリックします。

3 ［USB］の［有効］のチェックマークを外します。

4 ［保存］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 ホーム画面で、［システム］をクリックします。

2 ［セキュリティー設定］をクリックします。

3 ［カストマーエンジニアの操作設定］をクリックします。

4 ［操作制限］の［有効］にチェックマークを付けます。

5 ［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。

6 ［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。

7 ［保存］をクリックします。

8 ［はい（変更する）］をクリックします。（2 回実施）

補足
- パスワードに指定可能な文字 :
  英数字、および次の特殊文字
  (“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、“)”、” (space)”、“””、“’”、“+”、“、”、“-“、“/”、“:”、“;”、“<”、“=”、“>”、“?”、“［“、“¥”、“］”、“_”、“`”、“{“、“|”、“}”、“~”)

監査ログの起動

1 ホーム画面で、［システム］をクリックします。

2 ［ログ設定］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［有効］にチェックマークを付けます。

5 ［保存］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 ホーム画面で、[システム] をクリックします。

2 [タイムアウト設定] をクリックします。

3 [自動リセット (インターネットサービス)] の [タイムアウト] 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 1 分から 240 分の範囲で指定できます。）

4 [保存] をクリックします。

カスタムサービスの設定

1 ホーム画面で、[アプリ] をクリックします。

2 [カスタムサービス設定] をクリックします。

3 [カスタムサービス設定] の [有効] のチェックマークを外します。

4 [保存] をクリックします。

プラグイン設定

1 ホーム画面で、[システム] をクリックします。

2 [プラグイン設定] をクリックします。

3 [プラグイン設定] の [組み込みプラグイン機能] のチェックマークを外します。

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、次に示す記述の PJL コマンドファイルを作成し、LPR コマンドなどで本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、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、一時的に本機の LPD ポートを有効化してください。上記の設定後、「LPD の設定」（P.19）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本機に送るには、コマンドプロンプトで次の書式で LPR コマンドを実行してください。
  lpr -S “ 本機の 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 1.5MB 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。

次の条件を満たすサーバーを使用することを前提として、手順を記載します。

- Windows OS を搭載
- PowerShell version3.0 以降をインストール済み
- 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 次の内容で PowerShell スクリプトを作成します。

```
# Replace "12345" with actual Login ID of system administrator
$USER = "12345"
# Replace "passcode" with actual Passcode of system administrator
$PASS = "passcode"

# 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 手順 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。

取り出した監査ログのフォーマット

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。

■ヘッダ情報

項目	形式	説明
フォーマットバージョン	整数	設定値は「3」
デバイス IP アドレス	半角英数字（a ～ z、0 ～ 9）、ドット（.）、コロン（：）、文字列	IP アドレス（IPv4 または IPv6）
符号化方式	文字列	UTF8 に固定
タイムゾーン	-720 ～ 720	GMT を基準とした時差単位は分、子午線より西まわりはマイナス値とします。
年月日フォーマット	YYYY/MM/DD、MM/DD/YYYY、または DD/MM/YYYY	

■監査ログ情報

項目	形式	説明
ログ識別子（Log ID）	整数（1 ～ 60000）	監査事象発生時に割り振られる識別子
年月日（Date）	文字列	監査事象発生の年月日
時間（Time）	hh:mm:ss	監査事象発生の時間（時分秒）
監査事象識別子（Audit Event ID）	16 進整数（0x0000 ～ 0xffff）	監査事象に対応する識別子
監査事象名（Logged Events）	文字列	監査事象の種別を表す文字列
ユーザー名（User Name）	文字列	監査事象を発生させたユーザーを表す文字列 *
監査事象詳細（Description）	文字列	監査事象の詳細
結果 / 状態（Status）	文字列	発生した監査事象の処理結果または状態
個別保存項目（Optionally Logged Items）	文字列	監査事象の個別保存情報

* : 通常の場合：ユーザー ID
ユーザー ID が不明な場合：ユーザー名
ユーザー ID、ユーザー名が両方とも不明な場合：-
機械管理者：KO
カストマーエンジニア：CE
承認未登録ユーザー：Guest
システム内部動作に起因する場合：System
NMP 経由の場合：SNMP:admin

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	-

監査ログファイルに記録される操作

監査ログファイルに記録される操作は以下の通りです。

- 操作パネルの識別認証
- CentreWare Internet Services の識別認証
- プリンタードライバー
- 操作パネルの管理機能
- CentreWare Internet Services の管理機能
- 電源ボタン（本体起動時、本体停止時）
- 操作パネルのコピー機能、プリント機能、スキャン機能、ファクス機能、文書取り出し機能
- 操作パネルのジョブ管理・履歴の表示機能
- CentreWare Internet Services のジョブ状態・履歴の表示機能
- CentreWare Internet Services の親展ボックスからの文書データ取り出し機能
- CentreWare Internet Services のファイル指定によるプリント機能
- 外部監査サーバー
- ファームウェアのバージョンアップ
- 公衆電話回線

参照

- 監査ログの詳細については、弊社公式サイトで提供している『監査ログリファレンスガイド』を参照してください。

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、利用者はユーザー 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、ユーザー ID を入力します。

2 [次へ] をタップします。

3 パスワードを入力します。

4 [OK] をタップします。

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、他のユーザー ID は登録されていません。ユーザー ID の登録について詳しくは、『ユーザーズガイド』の「詳細設定」>「認証 / 集計管理」>「集計管理」>「ユーザー登録 / 集計確認」を参照してください。

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、適切な運用を徹底するために、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できます。

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、次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。

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］ボタンをクリックします。

2 ［認証管理］ダイアログ上で、以下の設定を行います。

“ 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します。

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。

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

ホーム画面の［システム］>［セキュリティー設定］の［電子証明書］で、［証明書設定］をクリックします。証明書の種類のプルダウンメニューから作成する証明書の種類を選択し、［新規作成］のプルダウンメニューから［自己署名証明書の作成］か［証明書署名要求 (CSR) の作成］を選択します。

［自己署名証明書］を選択すると、［自己署名証明書の新規作成］画面が表示されます。

［証明書署名要求 (CSR) の作成］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。

自己署名証明書の作成

次の項目を設定し、［実行］をクリックすると、自己署名証明書が本機に設定されます。すでに自己署名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（［RSA/SHA-256］、［RSA/SHA-384］、［RSA/SHA-512］を選択した場合）

  ［2048bit］、［3072bit］から選択します。

- 楕円曲線（［ECDSA/SHA-256］、［ECDSA/SHA-384］、［ECDSA/SHA-512］を選択した場合）

  ［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

次の項目を設定し、［実行］をクリックすると、［証明書署名要求（CSR）のダウンロード］画面が表示され、ダウンロードできるようになります。

- 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（［RSA/SHA-256］、［RSA/SHA-384］、［RSA/SHA-512］を選択した場合）

  ［2048bit］、［3072bit］から選択します。

- 楕円曲線（[ECDSA/SHA-256]、[ECDSA/SHA-384]、[ECDSA/SHA-512] を選択した場合）

  [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

次の項目を設定し、[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。

- 証明書のインポート

  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。

- 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。

- パスワードの再入力

  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。

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 モードだけです。

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

監査ログには次の事象が記録されます。

参照

- 監査ログの詳細については、弊社公式サイトで提供している『監査ログリファレンスガイド』を参照してください。

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、監査サーバーから)	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

対象事象	記録される監査事象名	監査事象詳細	結果
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	
	Device Config	Software	Updated
	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）	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できます。

項目	操作パネルから	CentreWare Internet Services から	初期値
日付、時刻の設定	［設定］＞［システム設定］＞［システム時計 / タイマー設定］	−	−
スキャン送信の設定	［カスタマイズ］＞［ホームの編集］	−	有効
リモートアシスタンスの設定	［カスタマイズ］＞［ホームの編集］	−	有効
パスワード使用 - パネル入力時の設定	［設定］＞［認証 / 集計管理］＞［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
データの暗号化設定	［設定］＞［システム設定］＞［その他の設定］＞［データの暗号化］	−	無効
認証方式の設定	［設定］＞［認証 / 集計管理］＞［認証 ・セキュリティ設定］＞［認証の設定］＞［認証方式の設定］	［認証 / 集計 / 権限］＞［認証設定］	無効
プライベートプリントの設定	［設定］＞［認証 / 集計管理］＞［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］＞［受信制御］	−	プリント
ダイレクトプリント機能の禁止の設定	［設定］＞［認証 / 集計管理］＞［認証 ・セキュリティ設定］＞［ダイレクトプリント機能の禁止］	−	−
SMB の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［SMB クライアント］＞［SMB クライアント - ポート］	−	有効
ファクスの設定	［設定］＞［アプリ設定］＞［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
	［設定］＞［アプリ設定］＞［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	［ボックス操作］＞［登録 +］	［アプリ］＞［ボックス操作］＞［一覧表示］	−

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	［設定］＞［アプリ設定］＞［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］ ［設定］＞［アプリ設定］＞［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
自動リセットの設定	［設定］＞［システム設定］＞［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	［設定］＞［システム設定］＞［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	［設定］＞［システム設定］＞［保守］＞［機械起動時のプログラム 診断］	－	無効
パスワードの最小文字数の設定	［設定］＞［認証 / 集計管理］＞［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］	［認証 / 集計 / 権限］＞［認証設定］＞［パスワードの運用］＞［最小文字数］	無効
機械管理者パスワードの変更	［設定］＞［認証 / 集計管理］＞［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］	［機械管理者］＞［プロファイル］＞［パスワード変更］	－
認証失敗アクセス拒否回数の設定	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［認証の設定］＞［不正使用防止の設定］> ［認証回数制限 - 機械管理者］	［認証 / 集計 / 権限］＞［認証設定］＞［詳細設定］> ［管理者権限ユーザーの認証失敗アクセス拒否］	5
	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［認証の設定］＞［不正使用防止の設定］> ［認証回数制限 - 一般ユーザー］	［認証 / 集計 / 権限］＞［認証設定］＞［詳細設定］> ［一般ユーザーの認証失敗アクセス拒否］	5
アクセス制御の設定	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［認証の設定］＞［アクセス制御］> ［仕様設定へのアクセス］	［認証 / 集計 / 権限］＞［権限設定］＞［アクセス制限設定］＞［操作パネル / 仕様設定操作の制限］＞［仕様設定操作］	有効
	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［認証の設定］＞［アクセス制御］> ［デバイスへのアクセス］	［認証 / 集計 / 権限］＞［権限設定］＞［アクセス制限設定］＞［操作パネル / 仕様設定操作の制限］＞［操作パネルへのアクセス］	有効
	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［認証の設定］＞［アクセス制御］> ［サービスへのアクセス］	［認証 / 集計 / 権限］＞［権限設定］＞［アクセス制限設定］＞［アプリの制限］	有効

項目	操作パネルから	CentreWare Internet Services から	初期値
ジョブ操作の設定	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［ジョブ操作の設定］＞［実行中 / 待ちジョブの表示設定］	［ジョブ］＞［ジョブ動作設定］＞［実行中 / 待ちジョブの表示設定］＞［表示情報の制限］	有効
	［設定］＞［認証 / 集計管理］＞［認証・セキュリティ設定］＞［ジョブ操作の設定］＞［ジョブ操作の制限］	［認証 / 集計 / 権限］＞［権限設定］＞［アクセス制限設定］＞［ジョブ操作の制限］	ー
TLS の設定	ー	［システム］＞［セキュリティー設定］＞［証明書設定］＞［デバイス証明書］＞［自己署名証明書の作成］	ー
	［設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［SSL/TLS 設定］	［システム］＞［セキュリティー設定］＞［SSL/TLS 設定］	ー
デバイス証明書のインポート	ー	［システム］＞［セキュリティー設定］＞［証明書設定］＞［インポート］	ー
FIPS140-2 の設定	［設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［その他の設定］＞［FIPS140 認定モード］	［システム］＞［セキュリティー設定］＞［FIPS140-2 設定モード］	無効
HTTP の設定	［設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［SSL/TLS 設定］＞［HTTP-SSL/TLS 通信］	［ネットワーク］＞［プロトコル設定］＞［HTTP］＞［ポート (HTTP/HTTPS)］	すべて起動
TCP/IP の設定	［設定］＞［ネットワーク設定］＞［プロトコル設定］>［TCP/IP - 共通設定］	［ネットワーク］＞［Ethernet］＞［共通］	ー
BMLinkS の設定	［設定］＞［ネットワーク設定］＞［ポート設定］>［BMLinkS］	［ネットワーク］＞［BMLinkS］	無効
WebDAV の設定	［設定］＞［ネットワーク設定］＞［ポート設定］>［WebDAV］	［ネットワーク］＞［WebDAV］	有効
メール受信 (POP3)	［設定］＞［ネットワーク設定］＞［ポート設定］＞［メール 受信］	［ネットワーク］＞［POP3］	無効
IPP の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［IPP］	［ネットワーク］＞［IPP］	無効
IPSec の通信設定	［設定］＞［ネットワーク設定］＞［セキュリティ設定］＞［IPSec 設定］	［ネットワーク］＞［IPSec］	無効
WSD の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［WSD］	［ネットワーク］＞［WSD］	有効
LPD の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［LPD］	［ネットワーク］＞［LPD］	有効
Port9100 の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［Port9100］	［ネットワーク］＞［Port9100］	有効
FTP クライアントの設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［FTP クライアント］	［ネットワーク］＞［FTP クライアント］	有効
SOAP の設定	［設定］＞［ネットワーク設定］＞［ポート設定］＞［SOAP］	［ネットワーク］＞［SOAP］	有効

項目	操作パネルから	CentreWare Internet Services から	初期値
SNMP の設定	［設定］＞［ネットワーク設 定］＞［ポート設定］＞［SNMP］	［ネットワーク］＞［SNMP］	有効
Bonjour の設定	［設定］＞［ネットワーク設 定］＞［ポート設定］＞［Bonjour］	［ネットワーク］＞［Bonjour］	有効
USB の設定	［設定］＞［ネットワーク設 定］＞［ポート設定］＞［USB］	［ネットワーク］＞［USB］	有効
CSRF の設定	－	［ネットワーク］＞［HTTP］＞［CSRF 対策］	無効
カストマーエンジニアの操作制限の設定	［設定］＞［システム設定］＞［その他の設定］＞［カストマーエンジニアの操作制限］	［システム］＞［セキュリティー設定］＞［カストマーエンジニアの操作設定］	無効
監査ログの起動	［設定］＞［監査ログ設定］	［システム］＞［ログ設定］＞［監査ログ］	無効
監査ログの取り出し	－	［システム］＞［ログ設定］＞［監査ログ］＞［ログ取得］	無効
ブラウザセッションタイムアウトの設定	－	［システム］＞［タイムアウト設定］	20
カスタムサービスの設定	－	［アプリ］＞［カスタ ムサービス設定 ］	有効
プラグインの設定	［設定］＞［システム設定］＞［プラグイン設定］	［システム］＞［プラグイン設定］＞［組み込みプラグイン機能］	有効

補足

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

ApeosPort 3060/2560/1860
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 ― 2020 年 4 月　　第 1 版

（帳票番号 :ME8816J1-1）