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	PDF 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）MB3638J1-1	ユーザーズガイド：ME8356J1-1

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.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.13）
  「セキュリティを有効にするための設定 3 （監査ログによる定期検査）」（P.21）

- 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］または［外部認証］に設定。
- 認証 / プライベートプリント
  ［プリントの認証に従う］に設定。
- スキャナー（URL 送信）
  無効に設定。
- SMB
  無効に設定。
- ダイレクトファクス
  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。
- 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］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
  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。
- LDAP サーバー
  LDAP サーバーの情報を設定。
- Kerberos サーバー
  Kerberos サーバーの情報を設定。
- 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。
- カスタムサービス
  無効に設定。

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やり直してください。
- 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、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。
- 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。

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
- システム管理者は外部認証サーバーのアカウントポリシーを次のルールに従って設定してください。
  - パスワードポリシーを 9 文字以上に設定する
  - アカウントロックポリシーを 5 回に設定する
- 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。
- 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
- 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

■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、256 ビット）/SHA（256、384、512）

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、認証方式を変更する場合、または機械を廃棄する場合は、暗号化をリセットし、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。

補足
- NTP サーバーとの接続機能は評価対象外です。

ROM バージョンとシステム時計の確認

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。

本機操作パネルからのパスワード使用の設定

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 ［仕様設定 / 登録］画面で、［認証 / セキュリティ設定］を押します。

6 ［認証の設定］を押します。

7 ［パスワードの運用］を押します。

8 ［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。

9 ［確認 / 変更］を押します。

10 ［パスワード使用 - パネル入力時］画面で、［する］を選択します。

11 ［決定］を押します。

12 ［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］、または［外部認証］を押します。

5 ［決定］を押します。

手順 4 で［外部認証］を選択した場合は、手順 6 から手順 13 を実行してください。

6 ［仕様設定 / 登録］画面で、［仕様設定］を押します。

7 ［ネットワーク設定］を押します。

8 ［外部認証サーバー / ディレクトリサービス設定］を押します。

9 ［認証システムの設定］を押します。

10 ［認証システム］を選択します。

11 ［確認 / 変更］を押します。

12 ［認証システム］画面で、［LDAP］または［Kerberos］を選択します。

13 ［決定］を押します。

14 ［閉じる］を 2 回押します。

15 確認画面が表示されたら、［はい（再起動する）］を押します。

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、［プリントの認証に従う］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。

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 ［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 ［閉じる］を押します。

スキャナー（URL 送信）の設定

1 ［カスタマイズ］を押します。
2 ［スキャナー（URL 送信)］を選択し［削除］を押します
3 ［OK］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 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.5) 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。

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

10 ［新しい設定を適用］をクリックします。

11 ［再起動］をクリックします。

注記
- より安全な通信のために、［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、「デバイス証明書のインポート」（P.16）と同じ手順で、サーバーの CA 証明書をインポートし てください。

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

注記
- ［IKE 認証方式］を［デジタル署名］に設定する場合は、設定する前に、「デバイス証明書のインポート」（P.16）と同じ手順で IPSec の証明書をインポートしておきます。

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 以下の手順で［事前共有鍵］または［デジタル署名］での設定を行います。

［事前共有鍵］を選択する場合は、

1）［IP Sec］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)［事前共有鍵］と［事前共有鍵の照合］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。

［デジタル署名］を選択する場合は、

1)［セキュリティー］の［証明書管理］をクリックします。

2)［証明書の目的］の欄で、［IP Sec］を選択します。

3)［一覧の表示］をクリックして、必要な証明書をチェックします。

4)［証明書の表示］をクリックします。

5)［証明書の選択］をクリックします。

6)［IP Sec］をクリックします。

7)［プロトコル］の［有効］チェックボックスをチェックします。

8)［IP Sec］画面の［IKE 認証方式］の欄で、［デジタル署名］を選択します。
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。

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。

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。

LDAP サーバーの設定

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 ［LDAP］をクリックします。

4 ［LDAP サーバー / ディレクトリサービス］を選択します。

5 各メニューから LDAP サーバーの情報を設定します。

6 ［新しい設定を適用］をクリックします。

Kerberos サーバーの設定

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 ［外部認証サーバー設定］をクリックします。

3 ［Kerberos サーバー設定］を選択します。

4 各メニューから Kerberos サーバーの情報を設定します。

5 ［新しい設定を適用］をクリックします。

補足

- Kerberos サーバーが外部認証サーバーとして設定されている場合、LDAP サーバーの［機械管理の権限］に、システム管理者権限を与えられたユーザーグループを設定することができます。

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］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。

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。

セキュリティを有効にするための設定 3 （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. ［OK］をクリックします。
4. ［プロパティ］タブをクリックします。
5. ［セキュリティー］をクリックします。
6. ［監査ログ］をクリックします。
7. ［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 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

- 外部認証を設定している場合、User ID とパスワードを入力する前に、［登録ユーザー］または［機械管理者］を選択してください。
- 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。
- 外部認証を利用する場合、外部認証サーバーで管理されているユーザー情報を使用して認証するため、本機の機械管理者 ID は外部認証サーバーに登録されません。

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］	［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］	−	無効
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
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の使用］	−	有効
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
ソウ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

項目	操作パネルから	CentreWare Internet Services から	初期値
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
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
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
LDAP Server の設定	［仕様設定］>［ネットワーク設定］>［外部認証サーバー / ディレクトリサービス設定］>［LDAP サーバー / ディレクトリサービス設定］	［プロパティ］>［ネットワーク設定］>［プロトコル設定］>［LDAP］>［LDAP サーバー / ディレクトリサービス］	ー
Kerberos Server の設定	［仕様設定］>［ネットワーク設定］>［外部認証サーバー / ディレクトリサービス設定］>［Kerberos サーバー設定］	［プロパティ］>［セキュリティー］>［外部認証サーバー設定］>［Kerberos サーバー設定］	ー

項目	操作パネルから	CentreWare Internet Services から	初期値
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
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。

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 – 2018 年 11 月　第 1 版

（帳票番号 :ME8390J1-1）