TOSHIBA
Leading Innovation

東芝デジタル複合機 / デジタル複写機

ハイセキュリティモード 管理ガイド

●このたびは東芝デジタル複合機 / デジタル複写機をお買い上げいただきましてまことにありがとうございます。
●お使いになる前に取扱説明書をよくお読みください。お読みになった後は必ず保管してください。

はじめに

このたびは東芝デジタル複合機 / デジタル複写機をお買い上げいただきまして、まことにありがとうございます。
この取扱説明書は、本機をIEEE Std 2600.1™-2009 に準拠した状態で使用するための、条件や設定について説明しています。
本機をハイセキュリティモードで使用する前に、この取扱説明書をよくお読みください。また、本機をIEEE Std 2600.1™-2009に準拠した状態で運用するために、日常的に気を付けていただきたいセキュリティ上の注意点については、「安全にお使いいただくために」の「セキュリティに関するご利用上の注意事項」をご参照ください。
本機をIEEE Std 2600.1™-2009に準拠した状態に保つために、この取扱説明書をいつもお手元に置いて有効にご活用ください。

注 意

配送された段ボールに不審な開梱の痕跡があった場合は販売店にお問い合わせください。また配送された梱包の状態を覚えていない場合は販売店にご連絡ください。

■ 本書の読みかた

□ 本文中の記号について

本書では、重要事項には以下の記号を付けて説明しています。これらの内容については必ずお読みください。

⚠警告　「誤った取り扱いをすると人が死亡する、または重傷*1を負う可能性があること」を示しています。

⚠注意　「誤った取り扱いをすると人が傷害*2を負う可能性、または物的損害*3のみが発生する可能性があること」を示しています。

注 意　操作するうえでご注意いただきたい事柄を示しています。

補 足　操作の参考となる事柄や、知っておいていただきたいことを示しています。

📖　関連事項を説明しているページを示しています。必要に応じて参照してください。

*1　重傷とは、失明やけが・やけど（高温・低温）・感電・骨折・中毒などで、後遺症が残るものおよび治療に入院・長期の通院を要するものを指します。
*2　傷害とは、治療に入院や長期の通院を要さない、けが・やけど・感電を指します。
*3　物的損害とは、財産・資材の破損にかかわる拡大損害を指します。

□ 本書の対象機種について

本書の対象機種は、本文中で以下のように表記しています。

対象機種	本文中の表記
e-STUDIO2050C	e-STUDIO2550C Series
e-STUDIO2555C/3555C/4555C/5055C	e-STUDIO5055C Series
e-STUIDO287CS/347CS/407CS	e-STUIDO407CS Series
e-STUDIO477S/527S	e-STUDIO527S Series
e-STUDIO5560C/6560C/6570C	e-STUDIO6570C Series
e-STUDIO257/357/457/507	e-STUDIO507 Series
e-STUDIO657/857	e-STUDIO857 Series

□ 本文中の操作パネルとタッチパネル画面について

- 本書に掲載している操作パネルとタッチパネル画面は、e-STUDIO4540C Seriesを例にしています。
  その他の機種の操作パネルとタッチパネル画面は、操作パネルの形状とボタンの配置、タッチパネル画面のサイズが機種によって異なりますが、各部の名称や機能は共通です。
- タッチパネル画面はオプション機器の装着状況など、ご使用の環境によって異なる場合があります。

□ オプション機器について

使用可能なオプション機器は、お使いの機種の**かんたん操作ガイド**―「本機のオプション」をご覧ください。

□ 本書の表記について

本書では、東芝デジタル複合機 / デジタル複写機を総称して「複合機」と表記します。

□ 商標について

- Windows Vistaの正式名称は、Microsoft Windows Vista Operating Systemです。
- Windows 7の正式名称は、Microsoft Windows 7 Operating Systemです。
- Windows 8の正式名称は、Microsoft Windows 8 Operating Systemです。
- Windows Server 2003の正式名称は、Microsoft Windows Server 2003 Operating Systemです。
- Windows Server 2008の正式名称は、Microsoft Windows Server 2008 Operating Systemです。
- Windows Server 2012の正式名称は、Microsoft Windows Server 2012 Operating Systemです。
- Microsoft、Windows、Windows NT、またはその他のマイクロソフト製品の名称及び製品名は、米国 Microsoft Corporationの米国およびその他の国における商標または登録商標です。
- Apple、AppleTalk、Macintosh、Mac、Mac OS、Safari、iPhone、iPod touch、およびTrueTypeは、米国Apple Inc.の米国およびその他の国における商標または登録商標です。
- AirPrint、AirPrintロゴ、iPadはApple Inc.の商標です。
- IOS は、米国およびその他の国におけるCisco 社の商標または登録商標であり、ライセンスに基づき使用されています。
- Adobe、Acrobat、ReaderおよびPostScriptは、Adobe Systems Incorporated（アドビシステムズ社）の商標です。
- Mozilla、Firefox、Firefoxロゴは、米国Mozilla Foundationの米国およびその他の国における商標または登録商標です。
- IBM、ATおよびAIXは、International Business Machines Corporationの商標です。
- NOVELL、NetWare、NDSは米国NOVELL, Inc.の商標または登録商標です。
- TopAccessは、東芝テック株式会社の登録商標です。
- その他、本書および本ソフトウェアに掲載または表示されている会社名、製品名は、それぞれの会社の商標または登録商標である場合があります。

目次

1

ハイセキュリティモード

ハイセキュリティモードについての注意事項

ハイセキュリティモードとは、MFPからの情報漏えいやMFPへの不正アクセスから、お客様の大切な情報を守る運用モードです。

IEEE Std 2600.1™-2009に準拠した運用時のセキュリティ機能は、以下のとおりです。

- ユーザ認証機能
- ロール管理機能
- HDDに書き込むデータを暗号化する機能 *1
- ログを収集、閲覧する機能
- ジョブ終了時や電源投入時にHDD上の対象データを消去する機能
- SSL*2やTLSによる通信機能
- インテグリティチェックする機能
- ログの管理、各パスワードの管理、ユーザ管理、パスワードポリシーの管理、日付と時間の管理、オートクリアの管理、セッション確保時間の管理、SSL*2/TLSの有効・無効の管理、の各管理機能

＊1　e-STUDIO5560C/6560C/6570C、e-STUDIO257/357/457/507、e-STUDIO657/857のHDDに書き込むデータを暗号化する機能は、ISO/IEC15408の評価認証対象外です。

＊2　e-STUDIO5560C/6560C/6570C、e-STUDIO257/357/457/507、e-STUDIO657/857では、TLSのみがサポートされています。

ISO/IEC15408の認証は、以下のOSとブラウザの組み合わせ、および日本語または英語で運用しているMFPに対して取得または取得予定です。

OS：Windows XP
ブラウザ：Internet Explorer 8
MFP：
e-STUDIO2050C
e-STUDIO2555C/3555C/4555C/5055C

OS：Windows 7
ブラウザ：Internet Explorer 9
MFP：
e-STUDIO5560C/6560C/6570C*
e-STUDIO257/357/457/507*
e-STUDIO657/857*
＊　評価認証作業中（2015年3月現在）

ハイセキュリティモードであっても、MFPをIEEE Std 2600.1™-2009に準拠した状態で運用するためには、データやプロトコルを暗号化する、認証されたサーバーやクライアントのみと接続するといった、環境およびその環境に合わせたMFPの設定が必須となります。

本章に書かれている条件を満たさない場合、本機をIEEE Std 2600.1™-2009に準拠した状態で運用できない可能性がありますので、充分にご注意ください。

補 足

- 各セキュリティ機能の詳細や、関係する項目の設定方法については、TopAccess ガイドをご参照ください。
- ハードディスクが装着されていない e-STUDIO2050C をハイセキュリティモードでご利用になるためには、オプションのハードディスクキット（GE-1220）が必要です。

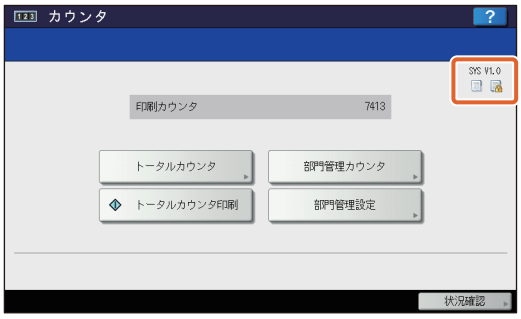
■ モードの確認

本機がハイセキュリティモードで運用されている場合、本機のタッチパネルに  が表示されています。

補 足

- ハイセキュリティモードで運用されている機体は、内部のHDDが暗号化されています。また、ハイセキュリティモードで運用されている機体には、データ消去オプション（GP-1070）がインストールされています。
  各機能が動作していることは、本機タッチパネルの［カウンタ］画面右上の表示で、ご確認ください。

HDDが暗号化されている	 が表示される 本機がハイセキュリティモードで運用されていれば、ハードディスクは暗号化されています。
データ消去オプションが正常に動作している	 が表示される 動作しているシステムバージョンが表示されます。 **補 足** お使いの機種によって表示されるシステムバージョンは異なります。 e-STUDIO2550C Series： SYS V4.0 e-STUDIO5055C Series： SYS V4.0 e-STUDIO6570C Series： SYS V3.0 * e-STUDIO507 Series： SYS V3.0 * e-STUDIO857 Series： SYS V3.0 * e-STUIDO407CS Series： SYS V2.0 e-STUDIO527S Series： SYS V2.0 Loops LP301： SYS V2.0 ＊ ISO/IEC15408の認証取得バージョン



- データ消去オプションがインストールされている場合、ユーザがログアウトした際に、ジョブを処理する過程で一時的に使用したハードディスクの領域は、上書き消去した後に、他のジョブで使用します。

■ 運用条件

運用条件に従って運用しなかった場合、MFPから情報漏えいやMFPへの不正アクセスにより、お客様の情報を守ることができません。

ユーザ管理の認証種別は、内部認証を選択してください。ユーザ認証にWindowsドメイン認証やLDAP認証を使用すると、IEEE Std 2600.1™-2009の対象から外れます。

ファイリングボックス BackUp/Restore Utility、ファイルダウンローダ、TWAINドライバ、AddressBook Viewerの各アプリケーションからMFPに接続する際には、IDとパスワードを入力してMFPにログインする必要があります。パスワードは伏せ字で表示されます。また、一定回数パスワードを間違えて入力するとロックアウトされます。

インテグリティチェックは手動で、［全て］を選択して設置時および定期的に実施してください。

＊ インテグリティチェックの実施方法は、設定管理ガイドを参照してください。

本機の通信に関する設定を初期値から変えずに運用することで、ネットワークを介した通信はSSLによって保護されます。本機の通信に関する設定は、初期値から変更しないでください。

［設定／登録］-［管理者設定］-［リスト印刷レポート設定］-［レポート出力設定］-［通信結果表］-［メモリ送信］はOFFにしてください。

「HDDが暗号化されているアイコン  」、「データ消去オプションが正常に動作しているアイコン  」が表示されない場合やシステムバージョンが異なる場合は、サービスエンジニアにお問い合わせください。

SNMPV3使用する場合、［管理者］タブ -［セットアップ］- メニュー -［ネットワーク］サブメニューのSNMP設定のSNMPV3ユーザ情報作成時には、必ず許可レベルを一般ユーザで作成してください。

ハイセキュリティモードでは、以下の機能は使用できません。

- 割り込みコピー
- ネットワークファクス
- Addressbook Viewer
- ファイルダウンローダ
- TWAIN ドライバ
- Backup/Restore Utility
- 予約印刷
- プリンタドライバからのファイリングボックスへの保存*

  ＊ 機能を選択することはできますが、エラーとなってジョブは削除され、印刷もされません。ジョブが削除された場合はエラーログが残ります。TopAccessの［ログ］タブおよび、本体タッチパネルの［状況確認］-［ログ］-［印刷］でご確認ください。
- ログ認証を無効にする

本機に同梱されているクライアントソフトウェアの、自動ログイン機能は使用できません。クライアントソフトウェアを使用する際には、必ずユーザ名およびパスワードを入力してください。

プリンタドライバからの印刷*や受信したファクスやインターネットファクスなど、本機に送信されたデータは、出力する権限のあるユーザがログインした場合にのみ出力することができます。

＊ 本機との通信には、IPP SSLを使用してください。

IPP印刷を行う際は、［ホスト名またはIPアドレス］ボックスに「https://［IPアドレス］:［SSLポート番号］/Print」と入力して作成したポートを使用してください。

（例：https://192.168.1.2:443/Print）

＊ 詳細はインストールガイドの「プリンタドライバのインストール」-「その他のインストール」-「IPP印刷」を参照してください。

アドレス帳などのデータをインポートする場合は、必ず本機からエクスポートしたデータを使用してください。

TopAccess -［管理者］タブ -［セットアップ］メニュー -［ODCA］サブメニューの設定変更が必要なアプリケーションは、使用しないでください。

Universal Printer 2 / Universal PS3 / Universal XPSプリンタドライバから本機で印刷を行う場合は、［印刷ごとに、ユーザ認証のためのIDとパスワードを入力する］を有効にしないでください。

本機をセキュアな状態で運用するために、以下の通り必ず設定してください。

注 意

設定は初期値一覧（📖 P.16）の内容を参照して確実に行ってください。

- プリントサービスでは、［Raw TCP印刷使用］および［LPD印刷使用］を［無効］にすること。
- ファイルを保存／送信するときには、暗号化PDF形式を使用し、暗号化レベルは128-bit AESとすること。
- スキャンデータなどの保存先には、信頼されたリモートPCを指定すること。
- パスワードを設定できないため、ファイリングボックスの共有ボックスは使わないこと。
- パスワードを設定できないため、本機のローカルフォルダは使わないこと。
- インターネットファクスで通信結果表を出力する場合、通信結果表に原稿を付加しないこと。
- 管理者は、定期的にログをエクスポートして保管すること。
- Twainスキャンは、［無効］にすること。
- SLP使用は、［無効］にすること。
- Web Serviceプリントは、［無効］にすること。
- SMBサーバプロトコルは、［無効］にすること。
- Bonjour使用は、［無効］にすること。
- FTPサーバー使用は「無効」に設定すること。

管理者の方は、ユーザに対して本機がハイセキュリティモードで運用されていることを伝えてください。また、ハイセキュリティモードでは、以下の内容を遵守するようにユーザに伝えてください。

- IPP印刷時のプリンタドライバの設定を使用して印刷すること。
- スキャンデータの保存先には、信頼されたリモートPCを指定すること。
- ファイリングボックスの共有ボックスを使用しないこと。
- 本機のローカルフォルダは使用しないこと。

2

固有の機能

仮パスワード

ハイセキュリティモードでは、ユーザが本機にアクセスするために、管理者により暫定的に付与されるパスワードを、仮パスワードとして扱います。仮パスワードでは本機を操作できません。本機を操作するためには、仮パスワードで本機にアクセス後に、本パスワードを登録する必要があります。

注 意

仮パスワードである間はセキュアな状態ではありません。できるだけすみやかに本パスワードを登録してください。

■ 仮パスワードとなる条件

以下のような場合に、ユーザのパスワードは仮パスワードとなります。

- 管理者によりMFPに登録された後、はじめてログインするとき
- 管理者がユーザのパスワードをリセットしたとき
- 管理者によりインポートされたユーザ情報のパスワードが平文になっていたとき

注 意

管理者がユーザのパスワードをリセットした際は、リセットしたことをユーザに通知し、本パスワードへの変更を促してください。

補 足

MFPからエクスポートされたユーザ情報は、改ざん防止のためハッシュ化されています。エクスポートしたユーザ情報のパスワードを修正すると、パスワードは平文となります。

■ 仮パスワード時のユーザの対応方法

アクセス時に本パスワードを登録できる場合

- パネルで本パスワードを登録する
  ユーザ認証画面で、［ユーザ名］と仮パスワードを入力します。仮パスワードであることの確認画面で［OK］を押すと、本パスワードの入力画面が表示されます。現在のパスワード］に仮パスワードを入力します。［新しいパスワード］および［新しいパスワードの確認］に本パスワードを入力し、［OK］を押します。本パスワードが登録され、MFPにログインできるようになります。
- TopAccessで本パスワードを登録する
  TopAccessで本機に接続すると、ログイン画面が表示されます。ログイン画面で［ユーザ名］と仮パスワードを入力し、［ログイン］を押します。本パスワードの登録画面が表示されるので、［新しいパスワード］および［パスワードの確認］に本パスワードを入力し、［保存］を押します。本パスワードが登録され、TopAccessにログインできるようになります。

アクセス時に本パスワードを登録できない場合

以下のユーティリティでは、仮パスワードを入力するとエラーとなってログインできず、本パスワードを登録することもできません。これらのユーティリティをご利用になる場合は、パネルやTopAccessで本パスワードを登録してからご利用ください。

- Remote Scanドライバ
- ファイリングボックス Webユーティリティ

ホールド印刷（ファクス）

ハイセキュリティモードでは、ファクス、インターネットファクスおよび画像が添付されたEメールを受信した際、自動的に出力することはありません。これらのジョブはホールド印刷（ファクス）キューに保管され、「ファクス受信印刷」権限を持つユーザのみが出力できます。

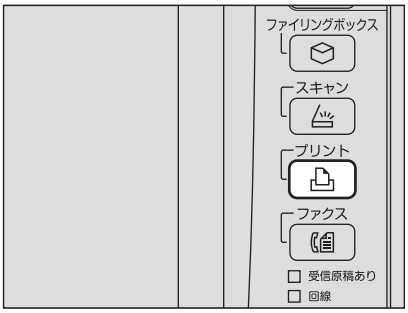
補 足

ホールド印刷（ファクス）キューにジョブが入っているときには、「受信原稿あり」のLEDが点滅します。

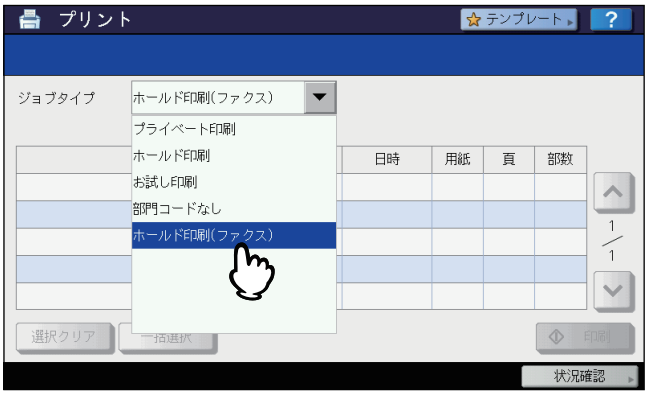
ホールド印刷（ファクス）からの印刷方法

1 **「ファクス受信印刷」権限を持つユーザでログインします。**

2 **操作パネルの［プリント］を押します。**

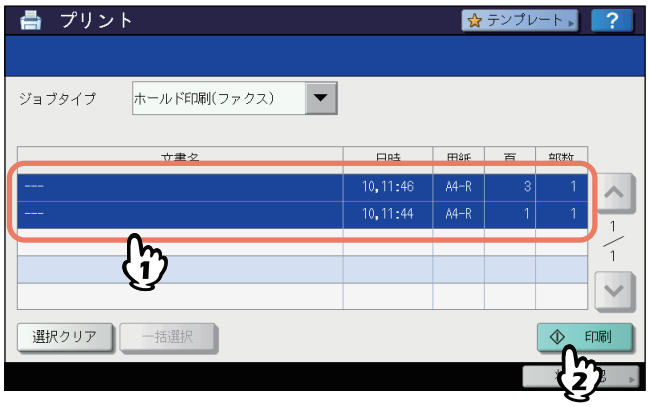


3 **［ホールド印刷(ファクス)］を選択します。**



- ホールド印刷（ファクス）キューに入っている全ジョブが表示されます。

4 出力したいジョブを押すか、または［一括選択］を押し、［印刷］を押します。



- 出力したジョブは、ホールド印刷（ファクス）キューから削除されます。

3

初期値

初期値についての注意事項

MFPをよりセキュアに運用するため、ハイセキュリティモードの機体では、初期値や選択できる値が、ノーマルセキュリティモードの機体と異なる場合があります。本章では、初期値や設定項目が、ノーマルセキュリティモードと異なる項目についてのみ記載しています。
IEEE Std 2600.1™-2009に準拠した状態で運用するため、本機の利用開始時に本章に記載されているハイセキュリティモードの初期値を備考欄の指示の通り確実に変更し、その状態から設定を変更せずにご利用ください。

注 意

- ノーマルセキュリティモードの初期値や設定値については、TopAccess ガイドおよび設定管理ガイドをご参照ください。
- 本機の「初期化」を実行して全設定を初期値に戻す場合は、実行前に、本機の設定やお客様のデータをバックアップしてください。詳しくはTopAccess ガイドおよび設定管理ガイドをご参照ください。

■ ログイン方法

- TopAccessの［ユーザ管理］タブおよび［管理者］タブは、Administrator権限を持ったユーザがログインすることで表示されます。TopAccessを開き、右上の“ログイン”をクリックし、ユーザ名とパスワードを入力してログインしてください。

- 本機の「設定／登録」モードの［管理者］タブへは、Administrator権限を持ったユーザでログインしてください。

■ 初期値一覧

［管理者］タブ
　［セットアップ］メニュー
　　［一般］サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
機能設定		
FTP保存	無効	
ネットワークインターネットファクス	無効	
ネットワークファクス	無効	
Web Serviceスキャン	無効	
Twain スキャン	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
管理者によるアドレス帳操作制限		
管理者のみ操作可能		
節電モード設定		
オートクリア*	45秒	初期値はノーマルセキュリティモードと同じですが、OFFを選択することはできません。

＊　本機タッチパネルの［設定／登録］モードの［管理者］タブでも変更可能です。

［ネットワーク］サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
HTTP		
SSL使用*	有効	
SMTPクライアント		
SSL使用	登録されたCA証明書を使用する	「登録されたCA証明書を使用する」または、「全ての証明書を受け入れる」がセキュアな設定です。
認証	自動	お使いの環境で、「CRAM-MD5」、「Digest-MD5」、「Kerberos」または「NTLM（IWA）」のどれかが適用されていることを、必ずご確認ください。
SMTPサーバー		
SMTPサーバー使用	無効	
POP3		
SSL使用	登録されたCA証明書を使用する	
FTPクライアント		
SSL使用	登録されたCA証明書を使用する	
FTPサーバー		
FTPサーバ使用	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
SSL使用	有効	
SNMP		
SNMP V1/V2使用	無効	
SNMP V3使用	有効	
Web Service設定		
SSL使用	有効	
Web Serviceプリント	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
Web Serviceスキャン	無効	
SLP		
SLP使用	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
SMB		
SMBサーバープロトコル	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
Bonjour		
Bonjour使用	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。

＊ 本機タッチパネルの［設定／登録］モードの［管理者］タブでも変更可能です。

［プリンタ］サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
一般設定		
プリント制限	ホールド印刷限定	

［プリントサービス］サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
IPP印刷		
SSL使用	有効	
FTP印刷		
FTP印刷使用	無効	
Raw TCP印刷		
Raw TCP印刷使用	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。
LPD印刷		
LPD印刷使用	有効	初期値はノーマルセキュリティモードと同じですが、必ず無効にしてください。

［ODCA］サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
ネットワーク		
ポートの使用	無効	

［セキュリティ］メニュー

[認証]サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
ユーザー認証設定		
ユーザ認証	有効	「無効」への変更はできません。
認証種別	内部認証	
ゲストユーザを有効にする	無効	初期値はノーマルセキュリティモードと同じですが、有効にすることはできません。
PINコード認証	無効	有効にしないでください。
印刷ごとに、ユーザ認証のためのIDとパスワードを入力する	無効	有効にしないでください。

[パスワードポリシー]サブメニュー

メニュー	ハイセキュリティモードの初期値	備考
ユーザパスワードポリシー		
パスワード最小桁数	8桁	
文字列の制限	有効	
ロックアウト設定	有効	ノーマルセキュリティモードと同じです。
リトライ回数	3回	
ロックアウト時間	2分	
有効期間設定	無効	ノーマルセキュリティモードと同じです。
有効期間	90日	
管理者、監査者パスワードポリシー		
パスワード最小桁数	8桁	
文字列の制限	有効	
ロックアウト設定	有効	ノーマルセキュリティモードと同じです。
リトライ回数	3回	
ロックアウト時間	2分	
有効期間設定	無効	ノーマルセキュリティモードと同じです。
有効期間	90日	
パスワードポリシー（ファイリングボックス、テンプレートグループ、テンプレート、暗号化PDF、SNMPv3、クローニング、機密受信）		
パスワード最小桁数	8桁	

メニュー	ハイセキュリティモードの初期値	備考
文字列の制限	有効	
ロックアウト設定	有効	ノーマルセキュリティモードと同じです。
リトライ回数	3回	
ロックアウト時間	2分	

FC-2050C
FC-2555C/3555C/4555C/5055C
FC-287CS/347CS/407CS
DP-4710S/5210S
FC-5560C/6560C/6570C
DP-2572/3572/4572/5072
DP-6570/8570
OMJ100077N0

東芝デジタル複合機
ハイセキュリティモード管理ガイド

東芝テック株式会社

QUALITY SERVICE

R100520J1314-TTEC
Ver14 F 2015-01