TOSHIBA

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

e-STUDIO2010AC
e-STUDIO2515AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO6518A/8518A

●このたびは弊社製品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

このたびは弊社製品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CC認証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CC認証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CC認証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。

□ 本書の対象読者について

本書は機器管理者向けの取扱説明書です。一般使用者は読む必要はありません。

□ 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-STUDIO2010AC	e-STUDIO5015AC Series
e-STUDIO2515AC/3515AC/4515AC/5015AC	
e-STUDIO2518A/3518A/4518A/5018A	e-STUDIO5018A Series
e-STUDIO5516AC/6516AC/7516AC	e-STUDIO7516AC Series
e-STUDIO6518A/8518A	e-STUDIO8518A Series

□ 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**をご覧ください。

□ 商標について

商標については**安全にお使いいただくために**をご覧ください。

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。
CC認証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
- ログを収集、閲覧する機能
- TLS1.2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、TLSの有効・無効の管理、の各管理機能

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（FAXユニットを装着、IPv4を使用）に対して取得または取得予定です。

適合PP名：HCD-PP

OS：	Windows 10
ブラウザ：	Internet Explorer 11
MFP：	e-STUDIO2010AC e-STUDIO2515AC/3515AC/4515AC/5015AC e-STUDIO2518A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO6518A/8518A

ハイセキュリティモードであっても、MFPをCC認証に準拠した状態で運用するためには、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CC認証に準拠した状態で運用できない可能性がありますので、十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。

■ 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。

注 意

サービスエンジニアが本機の設定などの操作を実施した場合、作業後に本機のタッチパネルに が表示されていることを確認してください。
また、初期値一覧を参照して正しい設定になっていることを確認してください。
P.19 「初期値一覧」

補 足

- ハイセキュリティモードで運用されている機体は、内蔵ストレージが暗号化されています。
  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。

内蔵ストレージ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、内蔵ストレージは暗号化されています。

- FIPS Hard Diskが装着されている場合は、装着されていることを示すアイコンが表示されます。

■ 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、CC認証の対象から外れます。

CC認証に適合したセキュリティ状態を維持するには、自己証明書を作成する際、公開キーは「RSA2048」を、署名アルゴリズムは「SHA256、SHA384、SHA512」のいずれかをお使いください。

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TLS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。

「内蔵ストレージが暗号化されているアイコン  」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。

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。
- ファイリングボックス
- 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
- ログ認証を無効にする
- Fコード通信
- Eメール受信印刷
- POP3設定を無効にする
- データバックアップ/リストア

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/TLS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/TLS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://192.168.1.2:631/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（Windows）」-「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。

本機の起動時には、自動的にインテグリティチェックが実行されます。サービスマンコールが表示された場合は、サービスエンジニアにお問い合わせください。

本機をハイセキュリティモードで運用するためには、TLS1.2に対応したSyslogサーバーが必要です。

ユーザ認証機能により、印刷/コピー /スキャン/ファクス送受信はアクセス制御の対象となります。実行中または実行待ちのジョブのリストは、すべてのユーザが確認することができます。ただし、ファクス受信ジョブは、AdministratorまたはFaxOperatorのロールを持ったユーザのみが確認することができます。ユーザはロールの権限に応じ、ジョブの出力・削除、中断・実行する順番の変更などの操作を行うことができます。ユーザのロールがAdministratorまたはUserの場合、ジョブを作成することができます。ユーザのロールがFaxOperatorの場合、ファクス送受信ジョブの作成・出力・削除ができます。ただし、ファクス送信ジョブは、自アカウントのジョブのみ出力・削除ができます。ユーザのロールがUserの場合、自アカウントのジョブのみ出力・削除することができます。ユーザのロールがAdministratorの場合、すべての実行待ちのジョブに対して削除・中断・実行する順番の変更などの操作を行うことができます。ただし、ユーザのロールがAccountManagerまたはAddressBookRemoteOperatorの場合、印刷/コピー /スキャン/ファクスの出力・削除、中断・実行する順番の変更などの操作はできません。

本機をセキュアな状態で運用するために、以下のとおり必ず設定してください。

注 意

設定は初期値一覧（P.19）の内容を参照して確実に行ってください。

- 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、本機のローカルフォルダは使わないこと。
- 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。
- Eメールダイレクト印刷の［自動］を有効にしないこと。
- CA証明書をアップロード／削除した場合、必ず本体の電源を再起動すること。

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。
- 本機のローカルフォルダは使用しないこと。

管理者の方は、Syslogサーバーとの通信が切断されていないよう、常に確認してください。

MFPを廃棄する場合は、必ずサービスエンジニアに内蔵ストレージの完全消去を依頼してください。

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。

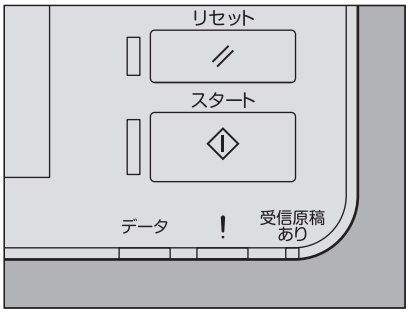
- Remote Scanドライバ
- ファイリングボックス Webユーティリティ

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

- ファクスを印刷する前にタッチパネルで受信したファクス画像のプレビューを表示することができます。詳しくは**GD-1370Jファクスガイド**を参照してください。
- 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。

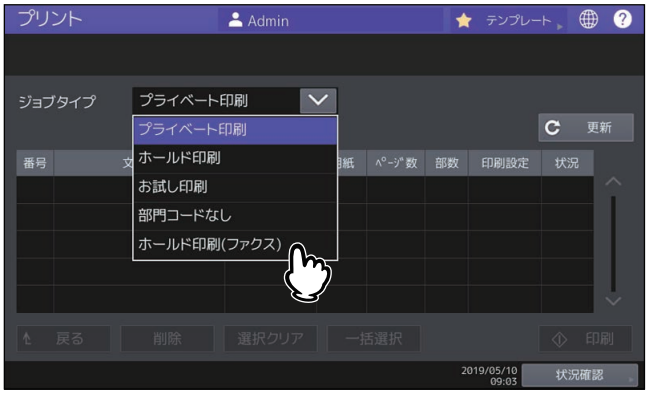


■ ホールド印刷（ファクス）からの印刷方法

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。

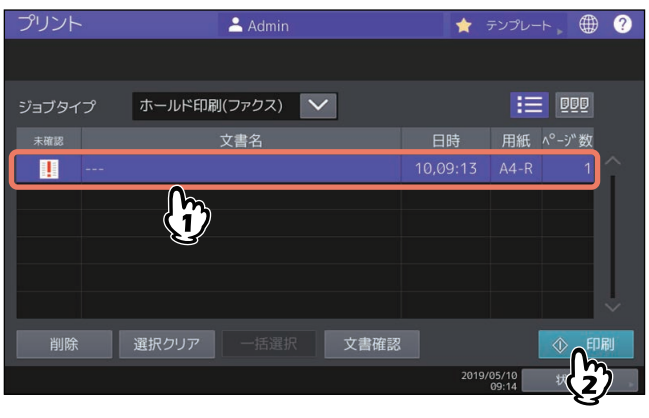
2 ホーム画面の［プリント］を押します。

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

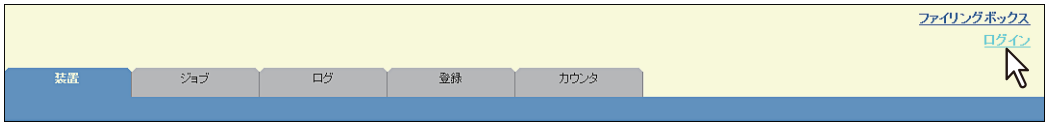
MFPをよりセキュアに運用するため、ハイセキュリティモードの機体では、初期値や選択できる値が、ノーマルセキュリティモードの機体と異なる場合があります。本章では、初期値や設定項目が、ノーマルセキュリティモードと異なる項目についてのみ記載しています。
CC認証に準拠した状態で運用するため、本機の利用開始時に本章に記載されているハイセキュリティモードの初期値を備考欄の指示のとおり確実に変更し、その状態から設定を変更せずにご利用ください。

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

ホーム画面：
［設定登録 -ユーザ-］メニュー
［管理者設定］タブ
［リスト印刷/レポート設定］メニュー
［レポート出力設定］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
通信結果表		
［メモリ送信］	OFF	「ON」にしないでください。

＊TopAccessからは操作できません。

TopAccess：
［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
装置情報		
USBダイレクト印刷	無効	
機能設定		
ファイリングボックス	有効	必ず「無効」に変更してください。
FTP保存	無効	
USBメディアを使用	無効	
SMB保存	無効	
Netware保存	無効	
インターネットファクス送信	有効	
ファクス送信	有効	
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	無効	
管理者／AddressBookRemoteOperatorによるアドレス帳操作制限		
管理者／AddressBookRemoteOperator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。
ホーム設定		
ポート番号	990	
SSL/TLS使用	有効	

＊本機タッチパネルの［設定登録-ユーザ-］モードの［管理者設定］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
IPv6		
IPv6使用	有効	必ず「無効」に変更してください。
SMB		
SMBサーバプロトコル	無効	
HTTP		
SSL/TLS使用*	有効	
WSD		
SSL/TLS使用	有効	
Web Servicesプリント	無効	
Web Servicesスキャン	無効	
SMTPサーバー		
SMTPサーバー使用	無効	
FTPサーバー		
FTPサーバー使用	無効	
SSL/TLS使用	有効	
SMTPクライアント		
SSL/TLS使用	登録されたCA証明書を使用する	
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。
POP3クライアント		
POP3クライアント使用	有効	必ず「無効」に変更してください。
SSL/TLS使用	登録されたCA証明書を使用する	
FTPクライアント		
SSL/TLS設定	登録されたCA証明書を使用する	
Bonjour		
Bonjour使用	無効	
SNMP		
SNMP V1/V2使用	無効	
SNMP V3使用	有効	
SLP		
SLP使用	無効	
Syslog設定		
Syslog使用	有効	
SSL/TLS使用	登録されたCA証明書を使用する	
ログの重要度 エラー	有効	

メニュー	ハイセキュリティモードの初期値	備考
ログの重要度 警告	有効	
ログの重要度 情報	有効	
ログの種類 セキュリティ /認証	有効	
ログの種類 ローカルユース0	有効	
ログの種類 ローカルユース1（ジョブログ）	有効	

＊本機タッチパネルの［設定登録-ユーザ-］モードの［管理者設定］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
Raw TCP印刷		
Raw TCP印刷使用	無効	
LPD印刷		
LPD印刷使用	無効	
IPP印刷		
SSL/TLS使用	有効	
FTP印刷		
FTP印刷使用	無効	

［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
サーバ認証設定		
ユーザ認証	有効	「無効」への変更はできません。
機能別ユーザ認証設定	無効	「有効」への変更はできません。
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。
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。
認証種別	内部認証	
PINコード認証	無効	有効にしないでください。
ユーザ管理情報の共有	無効	「有効」への変更はできません。

［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	半角英数字（ドイツ語のウムラウトとフランス語のセディラを持つ文字を含む）と記号（! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \ スペース）で15文字以上のパスワードを設定してください。
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	半角英数字（ドイツ語のウムラウトとフランス語のセディラを持つ文字を含む）と記号（! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \ スペース）で15文字以上のパスワードを設定してください。
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）		

メニュー	ハイセキュリティモードの初期値	備考
パスワード最小桁数	8桁	半角英数字（ドイツ語のウムラウトとフランス語のセディラを持つ文字を含む）と記号（! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \ スペース）で15文字以上のパスワードを設定してください。
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	

4

付録

監査対象イベントとSyslogサーバーに送信されるログの一覧

Syslogサーバーには、以下の情報が送信されます。イベントが成功したかどうかは「結果」列で確認することができます。

- 登録日時
- 内部ログ記録日時
- コード
- メッセージ
- ユーザ名
- ドメイン名

監査対象イベント			Syslogサーバーに送信されるログ		
			コード	結果	メッセージ
監査機能の起動	MFPの電源オン		D801	—	電源が入りました
監査機能の終了	MFPの電源オフ		D800	—	シャットダウンしました
ジョブの終了	プリントジョブの終了		4000	OK	job:Print jobId:6
	スキャンジョブの終了		2D01	OK	job:FTPStore jobId:8 to:
			2C00	OK	job:EmailSend jobId:33 to:
	コピージョブの終了		4000	OK	job:Copy jobId:11
	ファクス送信ジョブの終了		0000	OK	job:FaxSend jobId:9 to:1
	ファクス受信ジョブの終了		0000	OK	job:FaxReceive jobId:10 from:1
ユーザ認証失敗	ログインの失敗		6001	NG	ユーザログインに失敗しました
ユーザ識別失敗					
ユーザ識別失敗	ログインの失敗（プリントジョブ）		4041	NG	job:Print jobId:29
管理機能の利用	ユーザの追加		7174	OK	新規ユーザが追加されました
			7129	NG	ユーザ情報のインポートに失敗しました
	ユーザID・設定の変更		7175	OK	ユーザ情報の変更が実行されました
			717D	OK	ユーザのロール/グループ割り当てが更新されました
			7129	NG	ユーザ情報のインポートに失敗しました
	ユーザの削除		7176	OK	ユーザが削除されました
	設定の変更	ログインパスワードの入力リトライ回数	7184	OK	セキュリティ設定を変更しました
		ロックアウト時間	7184	OK	セキュリティ設定を変更しました
		ロックアウトされたアカウントステータス	7175	OK	ユーザ情報の変更が実行されました
		ユーザパスワードポリシー情報	7184	OK	セキュリティ設定を変更しました
		オートログアウト時間	7182	OK	デバイス設定を変更しました
		アドレス帳登録	7160	OK	新規宛先を追加しました
		アドレス帳変更	7166	OK	アドレス帳の編集を実行しました
		アドレス帳削除	7170	OK	宛先を削除しました
		ネットワーク設定	7183	OK	ネットワーク設定を変更しました
役割の一部であるユーザグループの改変	役割情報の変更		717B	OK	グループ情報の変更が実行されました

監査対象イベント		Syslogサーバーに送信されるログ		
		コード	結果	メッセージ
時刻の変更	時刻の変更	718A	OK	MFPの時刻を変更しました
セッション確立の失敗	TLSセッション確立の失敗	80C1	NG	TLSセッションの確立に失敗しました（不正なMACデータ）
		80C5	NG	TLSセッションの確立に失敗しました（ハンドシェイク失敗）

注 意

「ジョブの終了」に関して、表に記載されたコード以外が表示された場合、「結果」は「NG」となります。

CC認証を取得したバージョンの一覧

各製品でCC認証を取得したバージョン、取扱説明書、オプションの組み合わせは以下のとおりです。取扱説明書の識別番号と、製品、梱包箱などに記載されている情報をご確認ください。

シリーズ名	取扱説明書		SYS バージョン	必要なオプション	
	名称	識別番号		FAXユニット	FIPSハードディスクキット
e-STUDIO5015AC Series、e-STUDIO5018A Series	かんたん操作ガイド	OMJ17004300	V1.0 *1	GD-1370J *2	GE-1230 *3
	安全にお使いいただくために	OMJ17005500			
	コピーガイド	OMJ17005900			
	スキャンガイド	OMJ17006500			
	設定管理ガイド	OMJ17007300			
	インストールガイド	OMJ17007100			
	印刷ガイド	OMJ17006900			
	TopAccessガイド	OMJ17007500			
	トラブルシューティングガイド［ソフトウェア編］	OMJ17006100			
	トラブルシューティングガイド［ハードウェア編］	OMJ17004700			
	ハイセキュリティモード管理ガイド	OMJ170077B0			
	用紙準備ガイド	OMJ17004500			
	仕様ガイド	OMJ17005700			
	ファクスガイド GD-1370J	OMJ17007900			
e-STUDIO7516AC Series、e-STUDIO8518A Series	かんたん操作ガイド	OMJ17004900			
	安全にお使いいただくために	OMJ170055A0			
	コピーガイド	OMJ170059A0			
	スキャンガイド	OMJ170065A0			
	設定管理ガイド	OMJ170073A0			
	インストールガイド	OMJ170071A0			
	印刷ガイド	OMJ170069A0			
	TopAccessガイド	OMJ170075A0			
	トラブルシューティングガイド［ソフトウェア編］	OMJ170061A0			
	トラブルシューティングガイド［ハードウェア編］	OMJ17005300			
	ハイセキュリティモード管理ガイド	OMJ170077B0			
	用紙準備ガイド	OMJ17005100			
	仕様ガイド	OMJ170057A0			
	ファクスガイド GD-1370J	OMJ170079A0			

＊1　SYSバージョンの確認方法は「モードの確認」（P.9）を参照してください。

＊2　FAXユニットのファームウェアバージョンは「H625TA10」であることを確認してください。確認方法は**TopAccessガイド**を参照してください。
＊3　内蔵ストレージのモデル名を操作パネルに表示するようサービスエンジニアに依頼し、GE-1230が装着されていることを示す識別子「MQ01ABU032BW」が表示されていることを確認してください。

FC-2010AC
FC-2515AC/3515AC/4515AC/5015AC
DP-2518A/3518A/4518A/5018A
FC-5516AC/6516AC/7516AC
DP-6518A/8518A
OMJ170077C0

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

e-STUDIO2010AC
e-STUDIO2515AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO6518A/8518A

東芝テック株式会社

QUALITY SERVICE

R171020T8202-TTEC
Ver03 F 発行 2020年2月