TOSHIBA

# セキュリティガイド Vol.6.8

2023 年 11 月

＊ 製品名”e-BRIDGE SKY Suite”は欧州地域では利用できません

R13121304112-TTEC
OMJ150115M0

TOGETHER INFORMATION

# 目次

## 商標について

本書で記載されている登録商標を下記に記します。

- Windows またはその他のマイクロソフト製品の名称および製品名は、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。
- FeliCa は、ソニー株式会社の登録商標です。
- MIFARE は、NXP セミコンダクターズの登録商標です。

その他、本書に記載されている会社名、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。

# 1. はじめに

東芝テック株式会社（以降「東芝テック」と言う）は、お客様のデータやドキュメントの安全性を確保し、今日世界的に高まるビジネス上のセキュリティ課題に対応するさまざまな可能性を提供します。すべての e-BRIDGE Next モデルは、最高水準の安全性基準を満たし、業務効率やシステム性能を犠牲にすることなく、不正アクセスからお客様のデータやドキュメントを保護します。

**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-STUDIO550/650/810 | e-STUDIO810 Series |
| e-STUDIO3511/4511 | e-STUDIO4511 Series |
| e-STUDIO600/720/850 | e-STUDIO850 Series |
| e-STUDIO281c/351c/451c | e-STUDIO451c Series |
| e-STUDIO232/282 | e-STUDIO282 Series |
| e-STUDIO352/452 | e-STUDIO452 Series |
| e-STUDIO2500C/3500C/3510C | e-STUDIO3510C Series |
| e-STUDIO163/165/205 | e-STUDIO205 Series |
| e-STUDIO166/167/207 | e-STUDIO207 Series |
| e-STUDIO2330C/2830C/3520C/4520C | e-STUDIO4520C Series |
| e-STUDIO5520C/6520C/6530C | e-STUDIO6530C Series |
| e-STUDIO255/355/455 | e-STUDIO455 Series |
| e-STUDIO655/755/855 | e-STUDIO855 Series |
| e-STUDIO2040C/2540C/3540C/4540C | e-STUDIO4540C Series |
| e-STUDIO5540C/6540C/6550C | e-STUDIO6550C Series |
| e-STUDIO206L/256/306/356/456/506 | e-STUDIO506 Series |
| e-STUDIO556/656/756/856 | e-STUDIO856 Series |
| e-STUDIO2050C/2550C | e-STUDIO5055C Series |
| e-STUDIO2555C/3055C/3555C/4555C/5055C | |
| LOOPS LP30 | LOOPS LP30 Series |
| e-STUDIO5560C/6560C/6570C | e-STUDIO6570C Series |
| e-STUDIO257/357/457/507 | e-STUDIO507 Series |
| e-STUDIO657/857 | e-STUDIO857 Series |
| e-STUDIO2000AC | e-STUDIO5005AC Series |
| e-STUDIO2505AC/3505AC/4505AC/5005AC | |
| e-STUDIO2508A/3508A/4508A/5008A | e-STUDIO5008A Series |
| e-STUDIO5506AC/6506AC/7506AC | e-STUDIO7506AC Series |
| e-STUDIO6508A/8508A | e-STUDIO8508A Series |
| Loops LP35/LP45/LP50 | LOOPS LP50 Series |
| e-STUDIO2010AC | e-STUDIO5015AC Series |
| e-STUDIO2515AC/3515AC/4515AC/5015AC | |

| 対象機種 | 本文中の表記 |
| --- | --- |
| e-STUDIO2518A/3518A/4518A/5018A | e-STUDIO5018A Series |
| e-STUDIO5516AC/6516AC/7516AC | e-STUDIO7516AC Series |
| e-STUDIO6518A/8518A | e-STUDIO8518A Series |
| e-STUDIO2020AC/2021AC | e-STUDIO5525AC Series |
| e-STUDIO2525AC/3525AC/4525AC/5525AC | |
| e-STUDIO2528A/3528A/4528A/5528A | e-STUDIO5528A Series |
| e-STUDIO6527AC/7527AC | e-STUDIO7527AC Series |
| e-STUDIO6529A/9029A | e-STUDIO9029A Series |

## 2. セキュリティ機能一覧

| 想定される脅威 | 対応機能 | e-STUDIO5055C Series<br>e-STUDIO6570C Series<br>e-STUDIO507 Series<br>e-STUDIO857 Series | e-STUDIO5005AC Series<br>e-STUDIO5008A Series<br>e-STUDIO7506AC Series<br>e-STUDIO8508A Series | LOOPS LP50 Series | e-STUDIO5015AC Series<br>e-STUDIO5018A Series<br>e-STUDIO7516AC Series<br>e-STUDIO8518A Series | e-STUDIO5525AC Series<br>e-STUDIO5528A Series<br>e-STUDIO7527AC Series<br>e-STUDIO9029A Series |
|---|---|---|---|---|---|---|
| セキュリティ標準 | IEEE2600.1 適合 | ✓ | ✓ | | | |
| | IEEE2600.2 適合 | | | ✓ | | |
| | HCD PP 適合 | | | | ✓ | ✓ |
| | FIPS 140-2 認証 HDD<br>（認証有効期限 2023 年 12 月）<br>JCMVP 認証 HDD | オプション<br>※北米は標準 | オプション<br>※北米は標準 | オプション<br>※北米は標準 | オプション<br>※北米は標準 | オプション |
| | FIPS 140-2 認証 SSD<br>（認証有効期限 2025 年 12 月） | | | | | オプション<br>※北米は標準 |
| | 暗号アルゴリズム | | | | JCMVP 取得<br>CAVP 取得 | JCMVP 取得 |
| HDD 盗難による情報漏えい | 廃棄時の HDD 全消去 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ジョブ終了後自動消去<br>（データ消去キット） | オプション | オプション | オプション | オプション | 標準搭載<br>（オプション HDD 搭載時） |
| | Wipe 機能付暗号 HDD | ✓ | ✓ | ✓ | ✓ | ✓ |
| ネットワークからの不正アクセス | 不要ポートの閉鎖 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IP アドレス/MAC アドレスのフィルタリング | ✓ | ✓ | ✓ | ✓ | ✓ |
| 不正 E メール | 電子メール認証機能<br>（POP before SMTP） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | 電子メール認証機能（SMTP 認証） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | 電子メール認証機能（LDAP 認証） | ✓ | ✓ | ✓ | ✓ | ✓ |

| 想定される脅威 | 対応機能 | e-STUDIO5055C Series<br>e-STUDIO6570C Series<br>e-STUDIO507 Series<br>e-STUDIO857 Series | e-STUDIO5005AC Series<br>e-STUDIO5008A Series<br>e-STUDIO7506AC Series<br>e-STUDIO8508A Series | LOOPS LP50 Series | e-STUDIO5015AC Series<br>e-STUDIO5018A Series<br>e-STUDIO7516AC Series<br>e-STUDIO8518A Series | e-STUDIO5525AC Series<br>e-STUDIO5528A Series<br>e-STUDIO7527AC Series<br>e-STUDIO9029A Series |
|---|---|---|---|---|---|---|
| ネットワーク上のデータを盗聴 | SSL/TLS<br>（SMTP, POP3, LDAP, IPP, DPWS,<br>FTP, HTTP, SOAP, Syslog） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IPsec | オプション | オプション | オプション | オプション | オプション |
| | デジタル証明書（PKI/SCEP） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SNMPv3 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SNTP Authentication | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Secure DDNS | ✓ | ✓ | ✓ | ✓ | ✓ |
| | 有線 LAN での IEEE802.1X | ✓ | ✓ | ✓ | ✓ | ✓ |
| 無線 LAN 上のデータ盗聴 | WPA/WPA2 準拠 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | IEEE802.1X | ✓ | ✓ | ✓ | ✓ | ✓ |
| 電子ファイルの漏えい | 暗号化 PDF | ✓ | ✓ | ✓ | ✓ | ✓ |
| 電話回線から不正なアクセス | ファクスプロトコル以外の通信切断 | ✓ | ✓ | ✓ | ✓ | ✓ |
| ファクス/IP ファクス送信時の宛先間違い | ファクス誤送信防止機能 | ✓ | ✓ | ✓ | ✓ | ✓ |
| 印刷物の持去り | プライベートプリント | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ホールド印刷<br>（プリント、ファクス/IP ファクス、電子メール） | ✓ | ✓ | ✓ | ✓ | ✓ |
| 不正コピー | 地紋印刷（複製抑止） | ✓ | ✓ | ✓ | ✓ | ✓ |

| 想定される脅威 | 対応機能 | e-STUDIO5055C Series<br>e-STUDIO6570C Series<br>e-STUDIO507 Series<br>e-STUDIO857 Series | e-STUDIO5005AC Series<br>e-STUDIO5008A Series<br>e-STUDIO7506AC Series<br>e-STUDIO8508A Series | LOOPS LP50 Series | e-STUDIO5015AC Series<br>e-STUDIO5018A Series<br>e-STUDIO7516AC Series<br>e-STUDIO8518A Series | e-STUDIO5525AC Series<br>e-STUDIO5528A Series<br>e-STUDIO7527AC Series<br>e-STUDIO9029A Series |
|---|---|---|---|---|---|---|
| | 地紋印刷（複製禁止、情報トラッキング） | オプション | オプション | オプション | オプション | オプション |
| 不正アクセス | ユーザー認証機能（Windows 認証） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザー認証機能（LDAP 認証） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Role-Based Access Control | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザー認証機能（IC カード認証：FeliCa/MIFARE/HID 等） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザー認証機能（PIN 認証） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザー認証機能（二要素認証） | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザー認証機能（NFC 認証） | | | ✓ | ✓ | ✓ |
| | 管理者権限パスワード認証 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | サービスエンジニアアクセス制限 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ボックスパスワード認証 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | セキュリティログの記録 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ユーザーごとのジョブ操作のログの記録 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | アドレス帳編集権限 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ログに対するアクセス制御 | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Syslog | ✓ | ✓ | ✓ | ✓ | ✓ |

# 3. デバイスセキュリティ

東芝テックは、セキュリティに必要な技術を開発・提供することで、運用中の複合機を不正アクセス等の不正行為から守るだけでなく、導入からサービス運用、廃棄に至るまでの全ライフサイクルに渡って安全性を確保します。

## 3.1 HDD データの保護


東芝テックの e-BRIDGE コントローラー搭載複合機には HDD（ハードディスク装置）、または SSD（Solid State Drive）が搭載されており、コピー時などに読み込まれた原稿のデータが一時的に保存されます。このような一時的な保存データは、コピーが終わるとその管理データ（FAT : File Allocation Table）は消去されますが、データ自体は HDD/SSD 内に残存しております。また、機密文書を HDD/SSD 内のファイリングボックスにパスワード付きで保存・管理することができますが、データ自体は HDD/SSD 内に残存しております。もしも悪意を持った人物がこの HDD/SSD を入手すると、残存しているデータやファイリングボックス内のデータからお客様の文書を再現し、機密情報や個人情報を盗み出してしまうかもしれないと心配される方がおられるかもしれません。しかし、以下の暗号化機能およびデータ消去機能を利用することで、HDD/SSD データを保護することができます。

## 3.2 データ暗号化機能

### 3.2.1 Wipe 機能付セキュリティ HDD

Wipe 機能付セキュリティ HDD は、e-STUDIO5005AC Series、e-STUDIO5008A Series、e-STUDIO7506AC Series、e-STUDIO8508A Series、LOOPS LP50 Series には標準搭載され、e-STUDIO5525AC Series、e-STUDIO5528A Series、e-STUDIO7527AC Series、e-STUDIO9029A Series にはオプションで提供されます。HDD 上のすべてのデータは、256 ビットの AES（Advanced Encryption Standard）というアルゴリズムによって暗号化されるうえ、Wipe 機能によって HDD が盗難にあっても他の機器に HDD を装着したその瞬間にデータの無効化が働くため、情報漏えいを防止することができます。また、複合機の使用終了時に、お客様の指示に従ってサービスエンジニアが操作することで、HDD データはすべて一瞬で無効化され、読み出すことは完全に不可能となります。

### 3.2.2 ソフトウェアによる HDD 内データの暗号化

Wipe 機能付き HDD や SED SSD が搭載されていない機種は、ソフトウェアによる HDD 暗号化機能が標準装備されているので、適用することができます。暗号方式には、e-STUDIO5015AC Series、e-STUDIO5018A Series、e-STUDIO7516AC Series、e-STUDIO8518A Series までは 128 ビットの AES（Advanced Encryption Standard）を、e-STUDIO5525AC Series、e-STUDIO5528A Series、e-STUDIO7527AC Series、e-STUDIO9029A Series から 256 ビットの AES というアルゴリズムが採用されています。Wipe 機能付き HDD や SED SSD が搭載されている機種は、ソフトウェアによる HDD 内データ暗号化機能を有効にする必要はありません。

### 3.2.3 自己暗号 SSD

e-STUDIO5015AC Series、e-STUDIO5018A Series、e-STUDIO7516AC Series、e-STUDIO8518A Series、e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種から、標準搭載されるストレージが自己暗号 SSD（SED SSD）になりました。256 ビットの AES（Advanced Encryption Standard）というアルゴリズムによって SSD 上のすべてのデータが暗号化されます。

### 3.2.4 FIPS/JCMVP 認証 HDD、FIPS 認証 SSD

オプションとして、FIPS 140-2/JCMVP 認証を取得した Wipe 機能付セキュリティ HDD や、FIPS 140-2 認証を取得した SSD を提供しています。

e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、オプションの FIPS 認証 HDD/SSD を装着した場合、標準の自己暗号 SSD にはデータを保存せず、すべてのデータはオプションの FIPS 認証 HDD/SSD に保存されます。これにより、すべてのユーザーデータは FIPS 認証された暗号で守られていることを保証します。

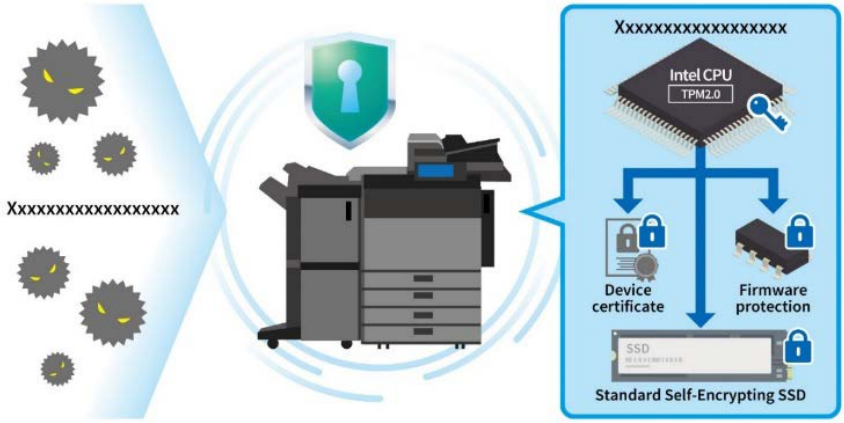
### 3.2.5 上書き消去機能

オプションのデータ消去キット（GP-1060/1070）を取り付けると、コピー、プリント、スキャン、ファクス/IP ファクスなどを行ったとき HDD に一時的に保存されたデータをジョブ終了後、DOD 規格に準拠した方法で自動的に上書き消去します。また、HDD のすべての領域を上書き消去し、HDD 内のデータを完全に消去する機能も備えており、複合機の使用終了時に、お客様の指示に従ってサービスエンジニアがこの機能を実行します。したがって、HDD に残存しているデータを読み出すことは完全に不可能となります。

e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、標準装備の SED SSD に対する上書き消去機能はありません。これは、ウェアレベリング機能により SSD にデータが書き込まれる際にブロックごとに分散されて書き込まれるため、上書き消去を行っているのと同様の効果があり、さらに暗号機能と組み合わさることで、消去された残存データを復元することがとても困難になるからです。また、オプションの Wipe 機能付きセキュリティ HDD や、SED HDD 装着時には、HDD に対して暗号機能や Wipe 機能が働くため、上書き消去機能を有効にする必要はありませんが、もし、お客様が希望する場合はサービスエンジニアが上書き消去機能の設定を有効にすることで、HDD に対して上書き消去機能を動作させることができます。複合機の使用終了時に、お客様の指示に従ってサービスエンジニアがすべてのデータを完全消去することができます。

### 3.2.6 TPM2.0 によるデータ保護

e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種から、Intel CPU が提供する TPM2.0 機能（Intel Platform Trust Technology）に対応しました。これまでの機種では、Wipe 機能付セキュリティ HDD で保存するデータを保護していましたが、e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、SED SSD（標準搭載）/ Wipe 機能付セキュリティ HDD（オプション搭載）、FIPS 認証 SSD オプション、SED SSD オプションにアクセスするための認証キーを TPM によって保護しますので、さらに安全になりました。SED を搭載していない機種では、ソフトウェアによる HDD 暗号化機能がありますので、この機能を有効にした際の暗号鍵を TPM によって保護しますので、不正アクセスなどの攻撃からユーザー情報は安全に保護されます。TPM によるセキュアブートにも対応しました。TPM によるセキュアブートに関しては、6.6 章をご参照ください。



### 3.3　ネットワークセキュリティ

複合機はネットワークサービスを提供するために TCP/UDP ポートをオープンにしており、クライアントコンピュータはネットワークを介してサービスに対応した複合機のポートに接続します。たとえば、LPD 印刷サービスを提供するために、複合機は 515 ポートをオープンにしております。不必要なポートをオープンにしていると、セキュリティホールになるのではと心配される方がおられるかもしれません。

#### 3.3.1 ネットワークアクセス制御

サービスを提供していないポートはオープンにしておりません。また、運用上必要ないポートは管理者設定で閉じることができます。使用しないプロトコルはなるべく無効にし、不要なポートを閉じるようにしてください。

#### 3.3.2 IP/MAC アドレスフィルタリング

IP アドレスフィルタおよび MAC アドレスフィルタに対応しています。複合機に登録したアドレスを持ったネットワークノード（クライアントコンピュータ等）からのアクセス要求のみ受け付けたり、登録したアドレスからのアクセスを拒否したりすることができます。これによって、悪意のあるネットワークノードからのアクセスを制限することが可能となります。
複合機に登録した IP アドレス、もしくは MAC アドレスからのアクセスのみを受け付ける設定と、複合機に登録した IP アドレス、もしくは MAC アドレスからのアクセスを受け付けない設定の両機能をサポートしています。
e-STUDIO5005AC Series 以降の機種では、ポートごとにフィルタを設定することができます。また、ICMP に対する応答を拒否する設定も可能です。

#### 3.3.3 通信経路保護（有線 LAN）

ネットワーク上を流れる通信データを暗号化することにより、通信を保護することができます。ネットワークトレースツールを使用すると通信データを簡単に盗聴することができますが、通信データを暗号化することにより、万が一通信データを盗聴されてもデータを盗まれることがなくなります。

#### 3.3.4 SSL（Secure Socket Layer）/ TLS（Transport Layer Security）

当社の複合機は TLS1.2 までサポートしており、脆弱性が発見された SSL3.0 は使用されません。
HTTP Server/Client、IPP、LDAP、SMTP Client、POP3、FTP Server、Web Service プリント、FTP Client と WS スキャン（Web Services Scan）、Syslog、SOAP で SSL/TLS 通信に対応しています。
HTTP Client 機能では、TopAccess への接続で SSL/TLS による暗号化を行うことができます。
AddressBook Viewer のアクセスにも、HTTPS による暗号化通信が使用されます。
IPPS では、印刷データを SSL/TLS で暗号化するため、印刷データを盗聴される心配がありません。
POP3/SMTP では、SSL/TLS 通信を行うことでメールデータを盗聴される心配がありません。
FTP サーバー機能は、FTP 印刷データとファイリングボックスデータのバックアップリストアで使用しています。SSL/TLS で暗号化するため、これらのデータの盗聴を防ぐことができます。
Web Service プリントでは、印刷データを SSL/TLS で暗号化するため、印刷データの盗聴を防ぐことができます。
WS スキャン、TWAIN スキャンでは、SSL/TLS で暗号化するため、リモートスキャンからのデータの盗聴を防ぐことができます。
FTPS では、Scan to Remote における通信を、暗号化することができます。
また、POODLE や FREAK 対応も行っており、SSL2.0/3.0 や SHA-1 といったセキュリティ強度の低い暗号方式/通信方式は使用されません。
e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、TLS1.2 と TLS1.3 をサポートします。

### 3.3.5 IPsec（IP Security Architecture）

IPsec は、IP 層を流れるデータのセキュリティを確保するプロトコルです。セキュリティ確保とは、機密性（Confidentiality）と完全性（Entirety）の確保、データを送受信する相手を認証し、データの送信否認を防止することであると言われています。

セキュリティプロトコルとしては、AH（Authentication Header）および ESP（Encapsulating Security Payload）の両方をサポートしています。AH は、IP パケットの完全性を確保し、ESP は IP パケットの機密性と完全性を確保するセキュリティプロトコルです。また、IPsec とともに使用される鍵管理のプロトコルとして IKEv1、および IKEv2 の両方をサポートしています。証明書のインストールには、Import あるいは SCEP が利用可能です。また、IPv6 Ready logo for IPsec にも対応しており、IPv6 Ready logo Phase2 を取得しています。

### 3.3.6 有線 IEEE802.1X

IEEE802.1X とは、LAN 接続時に使用する認証方式の規格です。IEEE802.11b などの無線 LAN でのユーザー認証仕様として一般に知られていますが、仕様自体は有線 LAN にも対応しています。サプリカント、802.1X 対応スイッチ、認証サーバーで構成され、認証されていないクライアントからの通信を止めて、認証されたユーザーにのみ通信を許可します。認証方式には、EAP（Extensible Authentication Protocol）を使い認証メッセージを伝送します。EAP 認証方式には、EAP-MD5 や EAP-TLS 方式などがあります。

802.1X に使用できる EAP はいくつかありますが、サプリカントと認証サーバーの両方が対応している必要があります。今回対応している EAP は、EAP-MD5、MSCHAPv2、EAP-TLS、EAP-TTLS、PEAP の 5 つの方式です。EAP-TLS、EAP-TTLS、PEAP で用いる証明書のインストールには、Import あるいは SCEP が利用可能となります。

### 3.3.7 ネットワーク認証

LDAP の認証には、CRAM-MD5、Digest-MD5 や Kerberos 認証に対応しており、LDAP サーバーへアクセスするためのユーザー名およびパスワードを保護します。

SMTP の認証には、CRAM-MD5、Digest-MD5、Kerberos、NTLM（IWA：Integrated Windows Authentication）に対応しており、SMTP サーバーへアクセスするためのユーザー名およびパスワードを保護します。

POP3 の認証には、Kerberos や NTLM（SPA: Secure Password Authentication）、APOP に対応しており、POP3 サーバーへアクセスするためのユーザー名およびパスワードを保護します。

SMB の認証には、NTLMv2、Kerberos に対応しています。

Dynamic DNS において、セキュア Dynamic DNS（Domain Name System）をサポートしています。セキュア Dynamic DNS を使用すると，そのリソースレコードを登録した当の複合機か，あるいは DNS サーバーに対して管理権限を有するもの以外は，ゾーン情報を更新できなくなります。

SNTP において、SNTP 認証に対応しています。複合機と SNTP サーバーの間の SNTP セッションの認証を行うことができます。

### 3.3.8 SNMPv3

ネットワークプロトコル SNMP v3 の採用により、データ暗号化機能、ユーザー認証機能が組み込まれ、セキュリティも強化されています。

### 3.3.9 通信経路保護（無線 LAN）

無線通信を暗号化し、第三者による解読・アクセスを防止する機能です。また、接続相手を認証することにより、あらかじめ許可された相手とのみ通信を行うことができる機能です。無線は電波を使用して通信するため電波の届く範囲では通信内容を傍受できその通信データを盗まれる可能性があります。

第三者による不正使用（データの改ざん、なりすまし等）を防止するため、無線 LAN オプションは通信データの暗号化と通信相手のユーザー認証を行う WPA/WPA2 Mixed Mode および WPA2 に対応しています。

WPA および WPA2 は、Wi-Fi アライアンスが制定したセキュリティ規格です。WPA は IEEE802.11i のサブセットとして認証および暗号化などを先立って規格策定されたもので、後に完全準拠した WPA2 が公開されました。WPA2 は WPA と比較し暗号化や接続性の改良が行われています。接続方法としては、あらかじめアクセスポイントとクライアントに共通の「パスフレーズ」と呼ばれる 8 文字から 63 文字の任意の文字列を設定して認証および通信データの暗号化を行う WPAPSK に加え、RADIUS サーバー（認証サーバー）を使用したさらに強力なセキュリティ方式（802.1X 認証）をサポートしています。これは、接続するアクセスポイントとクライアントがお互いに正しい相手であるかどうかを確認する仕組みです。

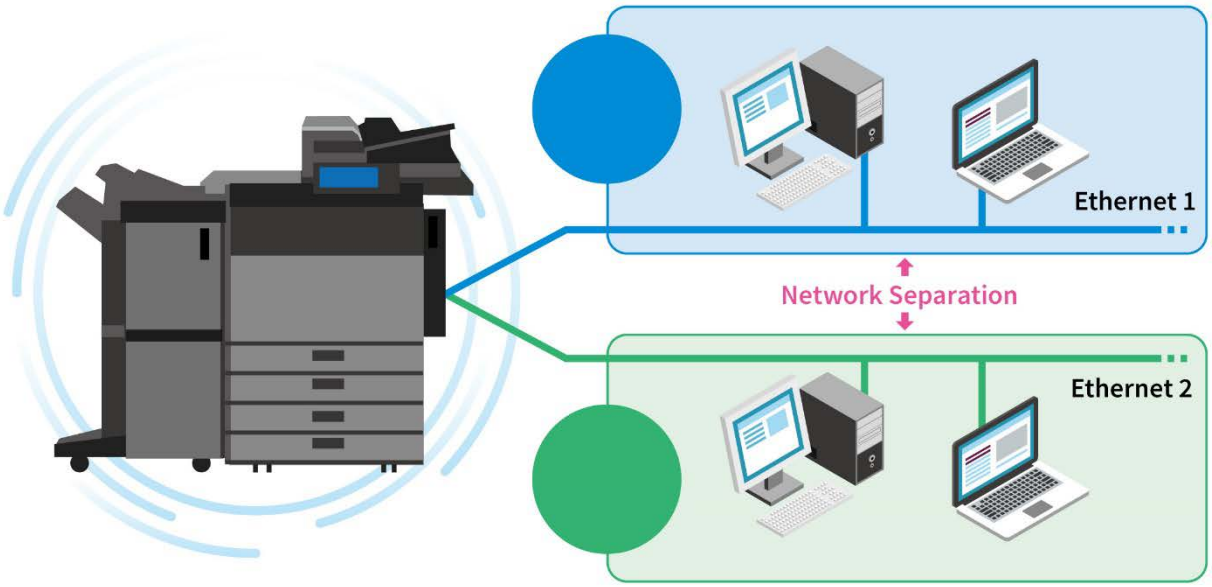
802.1X 証方式として、デジタル証明書を使用する方式である EAP-TLS およびパスワードを使用する方式である PEAPv0/EAP-MSCHAP v2 に対応しています。

WPA2 では、これらに加えて移動時に無線 LAN アクセスポイントが切り替わったときにもスムーズに接続するために暗号鍵を含めた認証結果を保存して 802.1X 認証を高速化する手段である Pairwise Master Key（PMK）キャッシングをサポートしています。また、無線 LAN の脆弱性である、KRACKs も対策されています。

### 3.3.10 セカンダリイーサネット（2nd NIC）

e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、セカンダリイーサネットキットを接続すると、1 台の複合機を 2 つの異なるネットワークで利用できます。

プライマリ（既存）イーサネットとセカンダリイーサネットはそれぞれ独立しており、複合機は各々のネットワーク通信を他方のネットワークにルーティングをすることはございません。これにより、一方のネットワークから複合機を経由して他方のネットワークに侵入することは不可能となります。



### 3.3.11 SMBv3

ネットワークプロトコル SMB として、v1/v2 に加えて、データ暗号化機能が組み込まれセキュリティも強化されている v3 に対応しています。 また、脆弱となった SMBv1 を無効化することも可能です。

## 3.4 電話回線および IP ファクスのアクセス制御

複合機はファクス機能をオプションで提供している機種があります。

### 3.4.1 電話回線のアクセス制御

電話線からのアクセスについては、ファクスのプロトコル以外は受け付けないようになっています。現在のファクスボードは、厳格に規定された ITU-T 準拠規格の標準 G3 ファクスと東芝テック独自手順プロトコルのみがサポートされております。規格外のファクスと東芝テックのファクス以外の相手と接続された場合は、プロトコルが成立せず通信異常として回線を切断します。したがって、電話回線からファクスボードを介してネットワークへアクセスすることはできません。また、不正規データが混入する可能性もありません。また、ファクス回線からのリモートメンテナンスは対応しておりません。

### 3.4.2 IP ファクスのアクセス制御

IP ファクスでは、SIP（Session Initiation Protocol）サーバー経由による送受信と、SIP サーバーを介さないダイレクト送受信および、Gateway 経由での送受信がありますが、セキュリティを考慮し登録された SIP サーバー以外からの SIP メッセージのみを受け付ける設定にすることが可能です。

### 3.4.3 ファクス/IP ファクスの誤送信防止

ファクス/IP ファクスの送信時にダイヤル入力や操作を誤って、予期せぬ宛先に機密情報が漏えいする可能性があります。これを防ぐためにさまざまな機能を利用することができます。

誤送信防止が必要な場合、サービスエンジニアに依頼して設定を変更することで、以下の誤操作防止ができます。

- ダイヤル入力後のスタートボタンを押す前に、確認のための画面が表示されます。
- 短縮番号入力またはワンタッチボタンを押した後、確認のための画面が表示されます。確認後、スタートボタンを押すことで送信可能となります。
- グループ同報送信の場合でも、確認のために選択したグループが画面に表示され、もう一度スタートボタンを押すことで送信可能となります。
- オンフックおよび外付け電話機の受話器を持ち上げた状態でスタートボタンの操作を禁止し、またスタートボタンを押した場合　拒否音が鳴り操作を防止します。（IP ファクスは対象外）

# 4. アクセスセキュリティ

アクセスセキュリティは、所定のデータあるいはデバイスにアクセス権限を持つ特定のユーザーのみにアクセスを認めています。デバイスへのアクセスとして3つのカテゴリに分類しています。

- 複合機へのアクセスは利用権限のあるユーザーのみに限定され、物理的またはデジタル環境的に利用可能な場所でのみアクセスが可能です。
- セキュリティポリシーは一元管理されているためハイレベルなアクセスセキュリティが確保できます。
- アクセス状況を監視することで不正アクセスに対し主体的に警告を発します。

## 4.1 利用の制限

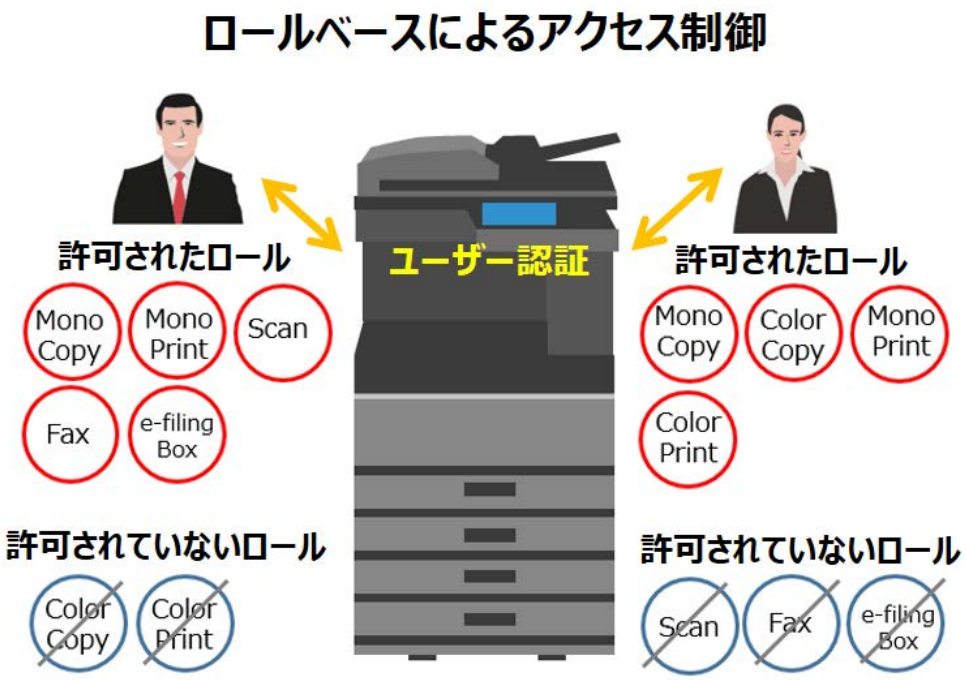
### 4.1.1 ロールベースによるアクセス制御（Role-Based Access Control）

複合機を不正に使用され、コピー・プリント・スキャン・ファイリングボックスなどの操作により情報が漏えいする可能性があります。これを防ぐためにユーザーごとに利用できる機能を制限することができます。

操作パネルや TopAccess で、ユーザー認証が完了した後に利用が許可されている操作（オブジェクト）のみが可能となります。たとえば、B さんに対してコピー、プリント、ファクス/IP ファクス、モノクロ出力は利用可能、スキャン、カラーアウトプットは禁止といった設定が可能です。

ユーザーごとのロール設定（ユーザーの役割を意味し、管理者、一般ユーザーなどや所属部門などが設定できます）は集中管理されたディレクトリデータベース LDAP（Active Directory の LDAP 機能）で行います。また LDAP サーバーがあらかじめ持っている属性をロールとして使用することもできます。

ユーザー認証機能を利用して複合機にログインすると、複合機は LDAP サーバーでユーザーにあらかじめ割り当てられているロール情報を取得し、そのロールに割り当てられている複合機へのアクセス権（Access Control List: ACL）をチェックし、ユーザーに複合機の各種機能への使用許可を与えます。ロールに割り当てることができるアクセス権は、複合機の各種設定/コピー/E メール送信/共有ファイルに保存/インターネットファクス/印刷/ファイリングボックス/ファクス/カラー出力（コピー/プリント）/リモートスキャン、USB 印刷/保存、アドレス帳編集、ログ管理等、20 項目が設定できます。ロール情報の設定には、既存の LDAP サーバーのあらゆるユーザー属性にアクセス権を割り当てることができますので、新規に LDAP サーバーを構築する必要がなく、安全に設定することが可能です。また、ローカル認証でのロールの設定や、管理者がロールの作成ができるようになります。



### 4.2　ログ情報へのアクセス

複合機の不正利用の抑止およびトレーサビリティを確保するため、操作パネルや TopAccess などからの操作をすべてログとして記録することができます。

ユーザー認証を有効にすることにより、各種操作（コピー、プリント、スキャン、ファクス/IP ファクスの送受信等）についてユーザーごとに操作の履歴に加えて失敗のログについても記録することができますので、不正アクセスや不正行為が行われていることを検出することができます。取得したログについては、操作パネルや TopAccess から見ることができますが、ユーザー認証を有効にすることにより、ジョブログは、ユーザー自身のジョブログのみ見ることができます。また、ユーザー認証無効にすることにより、ジョブログは表示/非表示の切り替えができ、管理者（Administrator）と監査者（Auditor）はすべてのログを閲覧することができます。

また、多くのセキュリティログが追加されております。

e-STUDIO5005AC Series 以降の機種では、Syslog にも対応しました。

### 4.3　識別認証

#### 4.3.1 ユーザー認証機能

複合機への不正アクセスを防止するためユーザー認証機能を搭載しています。ユーザー認証機能を用いると以下のようなユーザー管理を行うことができます。

- タッチパネルの操作を制限することができます。
- 機器の設定情報やログ情報へのアクセスを制限することができます。
- ユーザー単位に利用できる操作（コピー/プリント/スキャン/ファクスなど）を制限することができます。（Role-Based Access Control）
- ユーザー単位に操作ログを残すことができます。
- ユーザー単位でのカウンタ管理を行うことができます。
- 機能単位に認証要不要の設定が可能です。
- パスワードを入力する代わりに Android モバイル端末による NFC 機能を用いた本人認証も可能です。

#### 4.3.2 各種認証方式

以下の認証方式をサポートしています。

- 部門コードによる認証
- ユーザーID/パスワードによる認証
  - ローカル認証（複合機自身が認証を行う）
  - Windows ドメイン認証（認証サーバーとして Windows サーバーを使用）
  - LDAP Server を使った認証（認証サーバーとして LDAP サーバーを使用）
- PIN による認証
- IC カードによる認証
- IC カードと PIN を使った二要素認証
- Android モバイル端末による NFC 機能を用いた認証
- 指紋による認証
- 指紋と IC カード/PIN を使った二要素認証

### 4.3.3 ユーザー認証による操作の制限

タッチパネルを操作する際に認証画面を表示することで、操作を制限することができます。機能ごとにユーザー認証を設定することで、複合機の各機能ボタン（コピー、スキャン、プリント、ファクス）を押したときに認証画面を表示するかどうかを設定することができます。

### 4.3.4 ユーザー情報の登録管理

ユーザー認証に利用できるユーザー情報の登録管理方法は 2 種類あります。

1) 部門管理について最大 1,000 部門まで登録し利用できることが可能です。また複合機本体に最大 10,000 ユーザーまで登録できます。

2) 企業においてすでに構築されているユーザー認証システムと連携することができます。利用できるユーザー認証システムは、一般的に広く利用されているディレクトリサービスである Windows 認証システム（Active Directory）および LDAP です。

ユーザー認証の方法としては、キーボードから ID とパスワードを入力する方法に加え、マルチカードリーダーをサポートしており各種 IC カードおよび磁気カードにも対応しております。また、オプションの認証装置として、利便性とセキュリティを兼ね備えた非接触 IC カードである FeliCa/MIFARE/HID などを利用することができます。

これにより認証パスワードの代わりに複合機に接続されている FeliCa/MIFARE/HID などカードリーダーにカードをかざすだけで、本人を認証し複合機機能が利用可能になりますので、複合機操作パネルからのユーザー名入力などの煩雑な作業を解消することができます。また入退室管理などで利用している既存の FeliCa/MIFARE/HID/社員証などをそのまま複合機で利用することが可能であり、低コストで導入することができます。

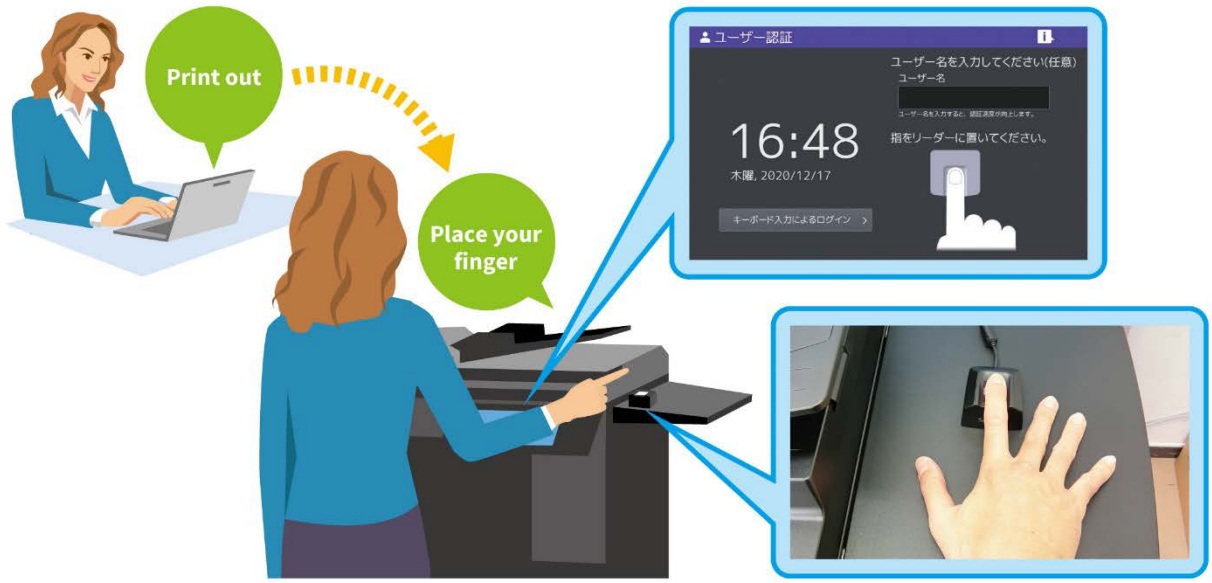

### 4.3.5 パスワードポリシー設定

ローカル認証を行う際、下記のようなパスワードポリシーを設定可能です。これによって、より複雑なパスワードを設定することができるようになります。

- 最低パスワード長
- パスワード有効期間
- パスワードでの使用を禁止する文字列の設定
- ログイン失敗によるロックアウトの回数や時間設定

### 4.3.6 指紋認証

指紋リーダーで読み取った指紋データを、あらかじめ複合機に登録されている指紋情報と照合することで、ユーザーを認証することができます。また、指紋認証に IC カードまたは PIN を併用して 2 段階認証でログインすることができます。指紋リーダーで読み取った指紋画像は、個人を特定できないファイル（テンプレートデータ）に変換して複合機の内部ストレージに保存されます。同時に、複合機で読み取った指紋画像は保存せずに破棄するため、指紋に関する個人情報が漏洩することはありません。




## 4.4 トラッキング

### 4.4.1 画像ログによるトラッキング

複合機でコピー、スキャン、ファクス/IP ファクスしたデータのトレーサビリティを確保するために、コピー、スキャン、ファクス/IP ファクスしたデータを画像のサムネイルデータとしてジョブ情報とともに保存することができます。

複合機でコピー、スキャン、ファクス/IP ファクス送信、ファクス/IP ファクス受信を行った際に、データを画像のサムネイルデータとして、ジョブ情報（日時、ユーザー名、ファイル名、複合機のシリアル番号等）とともに外部の指定したサーバーに送信することができます。これにより、複合機からのコピー、スキャン、ファクス/IP ファクスにより情報が漏えいした際に、追跡することが可能となります。

本機能を不正に利用することで複合機から情報が漏えいすることを防止するために、本機能はデフォルトでは無効となっています。本機能を利用する場合は、サービスエンジニアに依頼して設定を変更する必要があります。

### 4.4.2 強制印刷によるトラッキング

複合機でコピー/印刷出力した文書をトレースできるようにするために、ユーザー名や日時等の情報を、出力文書の中に強制的に付加することができます。

コピー出力、印刷出力、ファクス/IP ファクス送信に対して、日付、時間、ユーザー名、カード ID を強制的に印刷することにより、コピー出力、印刷出力、ファクス/IP ファクス送信のジョブを誰がいつ出力したかをトラッキングすることができるようになります。

### 4.4.3 電子メール送信時のセキュリティ機能

電子メール送信 では、機能を不正に利用されることで電子メールによる情報漏えいが発生したり、送信データが盗聴されたりする可能性があります。これを防ぐために電子メール送信時のセキュリティ機能を利用することができます。

複合機では電子メール送信時のセキュリティ機能として以下をサポートしています。

### 4.4.4 電子メール認証

認証方式としては標準プロトコル（POP before SMTP、SMTP Authentication （LOGIN/PLAIN/CRAM-MD5/Digest-MD5）、LDAP Authentication （LOGIN/PLAIN/CRAM-MD5/Kerberos））を搭載していますので、企業のポリシーに合わせて選択することができます。

### 4.4.5 BCC 送信機能

インターネットファクス送信時も電子メール送信と同様に BCC での宛先選択が可能です。

# 5. ドキュメントセキュリティ

複合機自体のセキュリティに加えてドキュメントのセキュリティについても、ライフサイクル全般に渡って保護します。いかなる場面においても（例：複合機への取り込み、保存、複合機によるコピー/印刷出力、ファクス送受信などの物理的およびデジタル的情報配信）、お客様の機密文書を徹底して保護します。


## 5.1 印刷セキュリティ

### 5.1.1 セキュアプリント

ユーザー認証機能無効時には、プライベートプリントを使用することで、クライアントから最大 64 桁（数字、アルファベットを含む）のパスワードを付けて印刷データを複合機本体に送信すると、送られた印刷データは複合機本体の HDD に一時的に蓄積され、操作パネルからパスワードを入力しない限り印刷がスタートしません。

また、ユーザー認証機能利用時は、ホールドプリント/プライベートプリントおよび、オプションであるマルチステーションプリントを使用することで、ユーザーは複合機にログイン後、自身の送信した印刷ジョブのみをプライベートプリントのパスワードを入力せずに出力指示を行うことが可能になります。プリンタドライバから印刷ジョブを複合機に送信する際に、ユーザー名およびパスワードを要求するように設定することで、複数のユーザーがクライアントコンピュータを共有している場合でもユーザーを制限することができます。

さらに、オプションである非接触型 IC カード FeliCa/MIFARE/HID などによる認証装置を利用することで、複合機操作パネルからユーザー認証の操作を入力せずに、カードをかざすのみでログイン操作を行うことができ、自身のプリントデータの出力指示を行うことが可能になります。ログインした時点で、出力操作なしに、自身の印刷データを自動的に出力させることも可能です。プライベートプリント強制、ホールドプリント強制に設定することも可能です。

このように他人に見られたくない機密文書を保管したり印刷するときには、パスワード付きのファイリングボックスを使用したり、プライベートプリント/ホールドプリント/マルチステーションプリントを使用することができます。

管理者が設定することで、すべてのジョブがすぐにリリースされずにプライベートキュー、ホールドキュー、あるいはマルチステーションキューにいったん保存されてから、リリースしたいときにリリースできます。

また、ステータス画面で文書名/ユーザー名を非表示にすることで、セキュリティが確保できます。

### 5.1.2 地紋印刷

地紋印刷は、プリント時に特殊な地紋パターン（微細なドットパターン）を埋め込むことにより、その文書をコピーした場合に隠し文字が浮き出ることにより、印刷された紙文書のセキュリティ機能として不正コピーを抑止する効果があり、紙文書による情報漏えいを防止する機能です。

また、オプション（GP-1190A）では、不正コピー抑止に加え、不正コピー禁止と、情報トラッキングが可能となります。プリンタドライバにより地紋印刷の設定をしてプリントを行うことで、印刷文書に地紋（微細なドットパターン）が付加され印刷されます。この印刷文書をコピーすると、「COPY」というあらかじめ設定してある文字が浮かび上がり、不正コピーによる情報漏えいを抑止できるようになります。さらにコピー禁止機能を持つ当社複合機でその印刷物をコピー、ファクス/IP ファクス、スキャンしようとした場合、この地紋を検出すると、コピー、ファクス/IP ファクス、スキャンの動作が停止しますので、機密文書のセキュリティを厳格に守ることができます。またこの印刷物が放置されていた場合などに、その印刷物をオプションのソフトウェアを使ってスキャンした画像データを解析することにより、印刷物が作成/出力された際の情報「いつ」「誰が」「何を」「どのクライアントコンピュータで作成し」「どの複合機で出力したか」という情報を読み出せるようにして、コンピュータ画面上に表示します。

## 5.2 スキャンデータセキュリティ

### 5.2.1 パスワード付きファイリングボックス


複合機本体の HDD に 64 桁のパスワードを設定してファイリングボックスを作成することができます。このファイリングボックスに保管したファイルを操作パネルから印刷したり、クライアントコンピュータの Web ブラウザからのサムネイル表示や編集もパスワードによるアクセス制限をかけたりすることができます。ボックスのパスワードは、パスワードポリシーを適用できます。

### 5.2.2 PDF ファイルのセキュリティ

#### 5.2.2.1 暗号化 PDF


この機能はスキャン時に暗号化 PDF を選択することで、PDF ドキュメントをパスワードで保護し、ドキュメントの暗号化や操作の制限を行うことができます。PDF ドキュメントは暗号化 PDF を開くためのパスワード（ユーザーパスワード）を入力することで表示できます。暗号レベルは、128bit RC4、40bit RC4、128bit/256bit AES から選択できます。操作の制限は、印刷・文書の変更・内容の抽出・アクセシビリティそれぞれについて設定することができます。制限の設定情報はパスワード（マスタパスワード）により保護されています。この機能を利用することで PDF ドキュメントを誤送信したり万が一盗聴されたりした場合でも、パスワードを知らない人はデータを見ることができません。また、配布した PDF ドキュメントの不正な印刷や改ざんなどからも保護することもできます。

#### 5.2.2.2 電子署名付き PDF

PDF ドキュメントの改ざん防止や原本保証することを目的とした、電子署名付き PDF ファイルを作成することができます。電子署名に使用する証明書は、複合機内で作成することもできますし、任意の証明書をインポートすることも可能です。暗号法方式は、複合機内で作成した証明書を使用する場合 RSA2048 で作成されます。

### 5.2.3 文書名、ユーザー名の機密化

ジョブの状態やログを操作パネルや TopAccess に表示する際、文書名やユーザー名、宛先等を”＊”で表示することが可能です。

## 5.3 ファクス/IP ファクス受信データ保護

休日、夜間等、ファクス/IP ファクスが受信され、印刷されることで機密情報の漏えいを心配される方がおられるかもしれません。以下の機能設定を行うことにより、機密情報の漏えいを防止します。

### 5.3.1 ファクス/IP ファクス機密受信機能

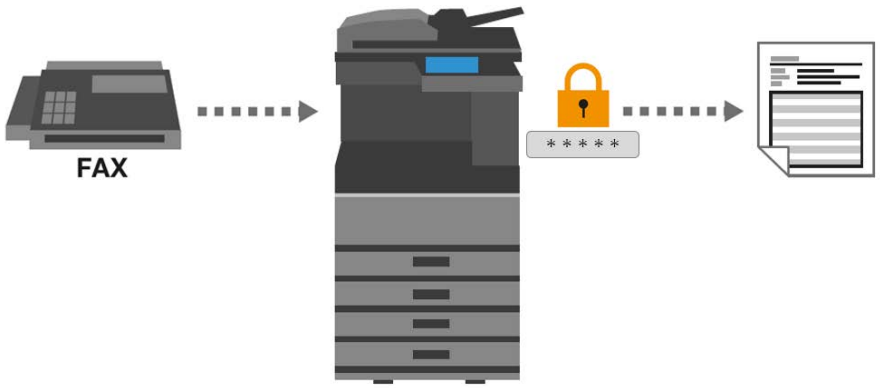
管理者により、曜日ごとの開始時刻（機密受信を有効にする）と終了時刻（機密受信無効モード）の設定をすることで、曜日ごとの設定操作ができます。

- 有効モード：機密受信機能が有効で、受信したデータを複合機内に蓄積される状態を指します。
- 無効モード：機密受信機能が有効であるが、受信したデータは印刷される状態を指します。

機密受信有効モード中に受信したデータは、以下のタイミングで印刷されます。

- 有効モード中にパスワード入力にて印刷。
- 無効モードへ切り替わり時に自動印刷。

ファクスホールド機能が有効となっている場合は、ファクス機密受信は機能しません。たとえ機密受信のスケジュールが設定されていても、ファクスホールド機能が有効になれば、ファクスホールドキューに格納されます。
機密受信有効モード時に、受信した受信データがある場合、本体パネルの下段に受信データがある旨のメッセージが表示されます。
受信データがすべて印刷されるまで、受信データありのメッセージは消えません。機密受信有効モード時に受信した受信データがある場合は、データランプを点灯させます。受信データがすべて印刷されるまで点灯します。受信データがある状態で、スリープ状態になってもデータ LED は点灯しており、受信データがある状態で、スーパースリープ状態になった場合は、データ LED は消灯します。



### 5.3.2 ファクスホールド機能

ファクスホールド機能設定を行うことにより、ファクス/IP ファクス受信データの機密情報の漏えいを防御します。ファクスホールド機能を行いたい場合は、サービスエンジニアが有効にできますので、サービスエンジニアにお問い合わせください。

ファクスホールド機能を有効にすると、ファクス/IP ファクスで受信したデータは常に複合機のファクスホールドキューに保存されます。

初期登録ユーザーである”Faxope”ユーザー、もしくは”FaxOperator”ロールを付与した一般ユーザーがファクス/IP ファクスで受信したデータをファクスホールドキューから出力することができます。印刷操作には、[プリント]ボタンを押して、「ホールド印刷（ファクス）」を選択します。“FaxOperator”ロールは、管理者の設定によりどのユーザーにも割り当てることができます。

ファクスホールド機能有効時に、ファクス/IP ファクス受信データがある場合は、本体パネルの下段に受信データがある旨のメッセージが表示され、受信データありの LED が点灯します。

# 6. 脆弱性への対応

## 6.1 セキュリティパッチの提供

万が一ファームウェアに脆弱性が発見された場合は、適宜セキュリティパッチをご提供いたします。

## 6.2 Windows を対象としたマルウェア

Windows を対象とした WannaCry をはじめとするネットワーク型ウイルス（ワーム）への感染や Web サイト（TopAccess）からの感染を心配される方がおられるかもしれません。また、USB を通して複合機に侵入するウイルスの対策を心配される方がおられるかもしれません。

複合機には Windows を対象としたネットワーク型マルウェア（ウイルス等）の影響を受けません。たとえば、WannaCry に対する影響はありません。

## 6.3 OSS の脆弱性

複合機は、いくつかのオープンソース（OSS）を使用しておりますが、これらの公開された脆弱性には、逐次対応しております。公知の脆弱性として、クロスサイト・リクエスト・フォージェリ、クロスサイトスクリプティング、SQL インジェクション、OS コマンドインジェクション等がありますが、複合機はこれらの脆弱性の対策が施されております。これまでに報道されました、以下のような各種脆弱性にも対応しています。POODLE、FREAK、GHOST、Heartbleed、Shellshock、KRACK、Faxploit、KNOB 等にも対応済みです。

## 6.4 USB ポートから侵入に関して

USB を通して侵入するウイルスの対策も施されております。USB Direct 印刷では、ファイルを印刷データとしてのみ扱うため、たとえファイルにマルウェアやスクリプトが含まれていたとしても、画像描画エラーになるだけであり、マルウェアやスクリプトが実行されることはありません。

Scan で USB メモリに保存する場合は、複合機側から USB メモリにファイルを書き込むだけであり、USB メモリ内のマルウェアが動作することはありません。

したがって、USB メモリ内のマルウェアやスクリプトが実行されることはありません。


## 6.5 電子メール

複合機には電子メールを受信して、添付ファイルを印刷したり、ファイリングボックスに保存したりする機能があり、メール受信で感染するウイルスを心配される方がおられるかもしれません。

メール受信機能では、添付ファイルは、印刷データとしてのみ扱うため、たとえ添付ファイルにマルウェアやスクリプトが含まれていたとしても、画像描画エラーになるだけであり、マルウェアやスクリプトが実行されることはありません。

### 6.6　サイバー攻撃評価

東芝研究開発センターのセキュリティ部門の技術者によって、当社複合機に対してサイバー攻撃評価を実施しております。セキュリティ専門家が考えうるサイバー攻撃に対して、問題ないことを確認しております。

### 6.7　ツールによる脆弱性確認

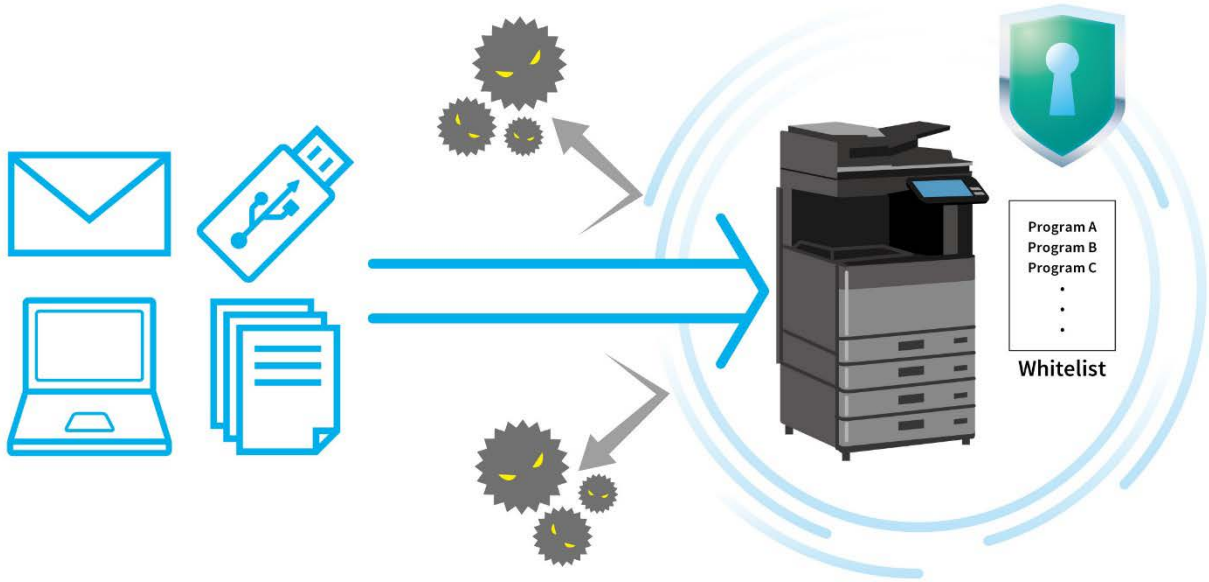
脆弱性スキャナーによる検査や、ファジングツールを使った検査も実施しており、検出された問題点はすべて対策しております。

### 6.8　ファームウェアの改ざん防止

当社複合機には、起動時、もしくは稼働時に管理者による操作で、複合機を制御するファームウェアが改ざんされていないかどうか検証するインテグリティチェック機能を持っています。この機能は、複合機がファームウェアデータのハッシュ値の検証を行い、ハッシュ値が一致しない場合はサービスコールを出して複合機の動作を停止します。また、ファームウェアをアップデートする場合は、ファームウェアに電子署名が付加されており、電子署名の検証を行ってからインストールを実施しますので、不正なファームウェアがインストールされることはございません。e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種では、TPM を使ったセキュアブート機能に対応しました。起動時に行うインテグリティチェックのハッシュ値を TPM で保護しますので、さらに安全になりました。

### 6.9　アンチマルウェア

e-STUDIO5525AC Series、e-STUDIO5528A Series 以降の機種から、アンチマルウェア機能に対応しました。
東芝製ホワイトリスト型マルウェア対策ツールを搭載することにより、ホワイトリストに登録された正規の実行モジュール以外起動することができませんので、たとえ未知のマルウェアであっても実行を拒否することができ、また誤検知も発生せず、定義ファイルの更新も不要です。



# 7. ソリューションプラットフォームセキュリティ

## 7.1 e-BRIDGE Open Platform セキュリティ

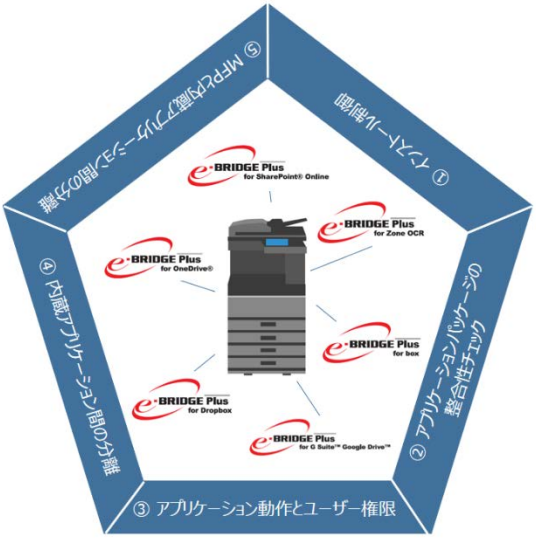
e-BRIDGE Open Platform でメタスキャン機能（オプション：GS-1010）および外部連携機能（オプション：GS-1020）（Embedded Web Browser＋Web サービスインターフェイス）をサポートしております。複合機のパネル操作を制限することができるユーザー認証機能を利用することで、これらの機能のセキュリティを保つことができます。またスキャン操作後、保存された機密データは、第三者に漏えいしたり改ざんされたりしないように保護します。
部門管理やユーザー認証時、認証しないと Embedded Web Browser およびメタスキャン機能を使用することはできません。

## 7.2 内蔵アプリケーションプラットフォーム

内蔵アプリケーション機能は、複合機に追加のアプリケーションをインストールし、複合機において追加の機能を実行できるというものです。複合機の内蔵アプリケーション機能は下記の特長を備えており、お客様の複合機を保護します。

### 7.2.1 インストール制御

内蔵アプリケーションのインストールとアンインストールは、管理者・サービスエンジニアなど複合機の管理権限のあるユーザーのみが行うことができます。管理権限のないユーザーによるインストールができないように制御されるため、管理者の意図しないアプリケーションが複合機上で動作することを防ぐことができます。




### 7.2.2 アプリケーションパッケージの整合性チェック

内蔵アプリケーションのアプリケーションインストーラは東芝テックにより署名されたパッケージのみが複合機にインストール可能となっています。そのため、改ざんされたパッケージや、不明な作成者により作成されたパッケージなどの、不正なアプリケーションが複合機にインストールされることを防ぎます。

### 7.2.3 アプリケーション動作とユーザー権限

複合機のパネルで動作する内蔵アプリケーションを一般ユーザーが操作した場合、複合機のロールベースユーザー認証によりユーザーに与えられた権限を越えた操作はできないように制御されます。そのため、管理者が一般ユーザーに許可していない操作が内蔵アプリケーション経由で実行されることを防ぎます。

### 7.2.4 内蔵アプリケーション間の分離

内蔵アプリケーションの操作できるファイルストレージは相互に分離されています。複数の内蔵アプリケーションがインストールされた場合でも、相互のデータに対するアクセスはできませんので、内蔵アプリケーションストレージ内に機密データが保管された場合でも安全に保管されます。

### 7.2.5 複合機と内蔵アプリケーション間の分離

内蔵アプリケーションと複合機のファイルストレージは相互に分離され、複合機に保存された機密データは内蔵アプリケーションからは直接参照できません。

そのため、ユーザーパスワードなどの機密データが内蔵アプリケーションにより漏えいすることはありません。また、アプリケーションからの複合機データの操作は、上記ロールベースユーザー認証により制御されるので、権限以上のデータが参照・操作されることを防ぎます。

# 8. リモートメンテナンス

## 8.1 e-BRIDGE CloudConnect のセキュリティ

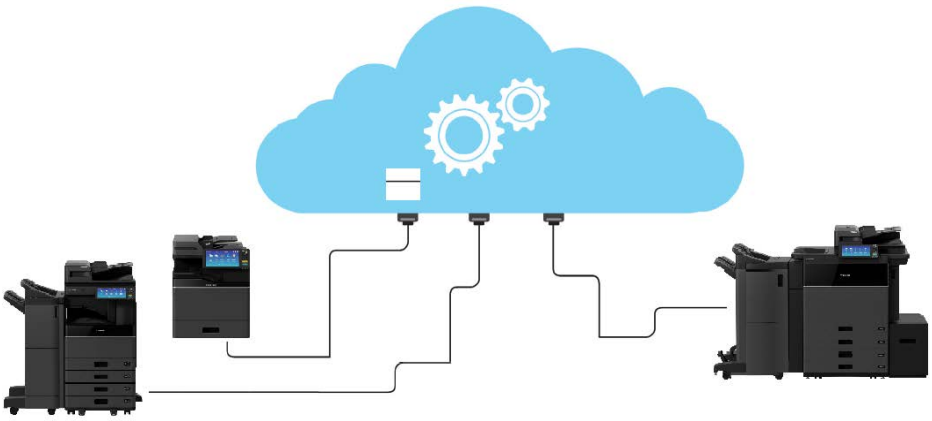
e-BRIDGE CloudConnect は、お客様の複合機から送信された稼動情報を、安全・確実に収集します。

e-BRIDGE CloudConnect は、クライアントコンピュータからブラウザを用い HTTPS（サーバー認証・暗号化）でアクセスするのと同じ原理を採用。しかも、複合機側からしか発信できず、かつ、アクセス先をサーバー証明書のある e-BRIDGE CloudConnect サーバーに限定することで、非常に高いセキュリティを実現しています。

e-BRIDE CloudConnect では、複合機がサーバー認証機能を行うことで、アクセスする e-BRIDE CloudConnect サーバーが本物であることを確認し、データを受信するサーバーの詐称や、誤ったサーバーにデータを送信することがないことを確保します。さらに送受信するデータを暗号化して、盗聴・漏えい・改ざんから守り、機密性・完全性を確保しています。また、東芝インフォメーションシステムズ株式会社によるセキュリティ診断を定期的に実施し、安全性を確認しています。

e-BRIDGE CloudConnect で扱う情報は、装置の稼動状況（利用枚数などのカウンタ値、装置の障害発生情報、消耗品の交換時期に関する情報、装置の設定・調整データなど課金、保守にかかわるデータ）だけです。お客様のドキュメント情報は一切扱いませんので、このシステムを導入することで複写データ、ファクスデータ、スキャンデータが外部に漏えいすることはありません。お客様の要請に基づき、サービス技術者が送信許可、禁止を設定することができます。運用管理についても、情報セキュリティマネジメントの国際標準 ISO27001 に準拠した本システムの情報セキュリティポリシーに基づき運用管理しています。

万が一セキュリティ問題が発生しても、e-BRIDGE CloudConnect を使用して、セキュリティパッチの配信が可能です。



# 9. クラウド接続

## 9.1 e-BRIDGE Cloud Login のセキュリティ

e-BRIDGE Cloud Login は、お客様のモバイルデバイスやコンピュータを利用して、東芝製複合機にインストールされた内蔵アプリケーションから、お客様が利用しているクラウドサービスへのログイン認証を、安全に行うクラウドサービスです。

e-BRIDGE Cloud Login における通信は、当社複合機からクライアント証明書を持った内蔵アプリケーションからしか開始できず、複合機とは 256 ビット ECDSA 方式での暗号化、さらに、お客様のモバイルデバイスやコンピュータとは 2048 ビットの証明書を使った HTTPS 通信により、高いセキュリティを実現しています。

e-BRIDGE Cloud Login では、お客様の個人情報およびドキュメント情報を、一切扱いません。

このサービスで扱う情報は、次のとおりです。

- アクセス時間
- 複合機のモデル名
- 複合機のシリアル番号
- アプリケーション ID
- 認可コード

これらは個人を特定する情報を含んでいません。また、これら情報を再利用することはありません

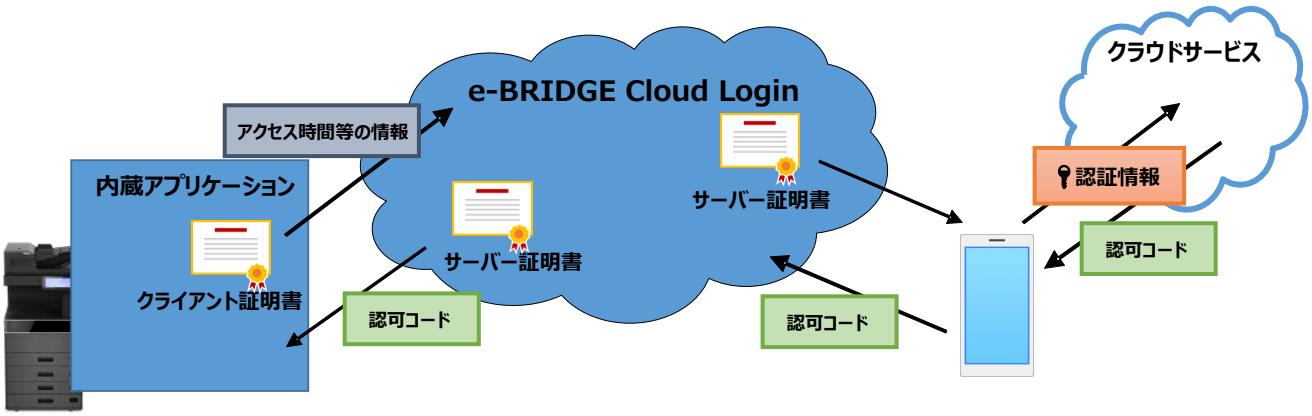
また、お客様のモバイル機器やコンピュータから入力した認証情報は、e-BRIDGE Cloud Login を経由しません。

e-BRIDGE Cloud Login は、AWS（アマゾンウェブサービス）を利用しており、ISO/IEC 27001（情報セキュリティ）、ISO/IEC 27017/27018（クラウドサービスセキュリティ）等に準拠しています。

詳しくは AWS のサイトを参照してください。

https://aws.amazon.com/security/

また、東芝インフォメーションシステムズ株式会社によるセキュリティ診断を定期的に実施し、安全性を確認しています。



### 9.2　e-BRIDGE Remote Assist のセキュリティ

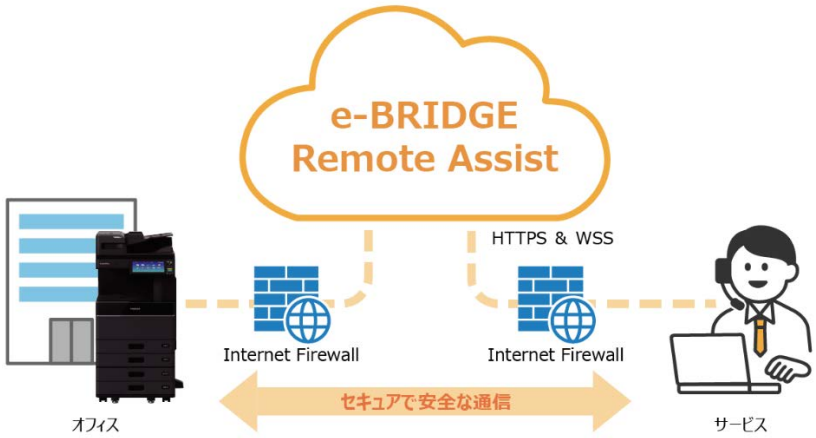
e-BRIDGE Remote Assist は、安全にお客様の複合機の操作画面を遠隔地のサービスからリアルタイムに操作する機能です。

e-BRIDGE Remote Assist は、クライアントコンピュータからブラウザを用い HTTPS（サーバー認証・暗号化）でアクセスするのと同じ原理を採用しています。

お客様の複合機からアクセス先のサーバーへ接続する場合は、サービスが準備した認証コードをお客様が操作パネルから入力することによって開始され、勝手に外部から接続が開始されることがないため、非常に高いセキュリティを実現しています。

e-BRIDGE Remote Assist では、複合機がサーバー認証機能を行うことで、アクセスする e-BRIDGE Remote Assist サーバーが本物であることを確認し、データを受信するサーバーの詐称や、誤ったサーバーにデータを送信することがないことを確保します。さらに送受信するデータを暗号化して、盗聴・漏えい・改ざんから守り、機密性・完全性を確保しています。

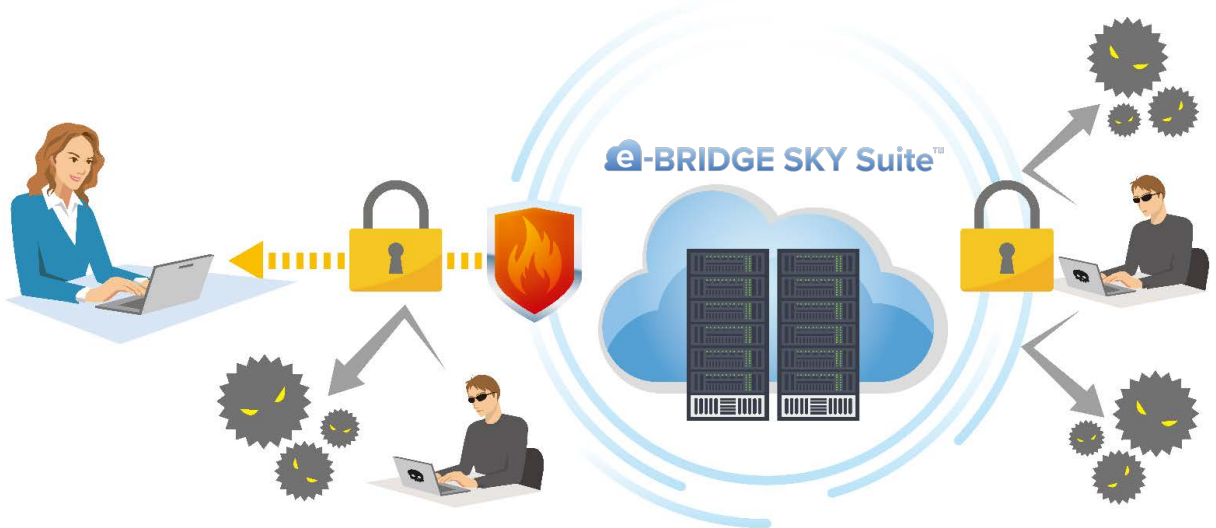
e-BRIDGE Remote Assist で扱う情報は、複合機の操作画面にかかわる画像データだけです。そのため、複合機内のお客様のドキュメント情報やアドレス帳などのデータは一切扱いませんので、このシステムを導入しても複写データ、ファクスデータ、スキャンデータが外部に漏えいすることはありません。お客様の要請に基づき、サービス技術者が e-BRIDGE Remote Assist 機能を有効に設定します。運用管理についても、情報セキュリティマネジメントの国際標準 ISO27001 に準拠した本システムの情報セキュリティポリシーに基づき運用管理しています。



### 9.3　e-BRIDGE SKY Suite のセキュリティ

e-BRIDGE SKY Suite は、リモートで、いつでもどこでもデータやデバイスのアクセスや管理が可能、コストや時間を削減することで業務効率も大幅に改善できます。

e-BRIDGE SKY Suite は、情報セキュリティマネジメントシステム ISMS（ISO/IEC 27001）認証を取得したサイトで運用されています。e-BRIDGE SKY Suite のサービス群は、Microsoft Azure 上に構成されており、データセンターのセキュリティは Microsoft Azure によって常に最新に保たれています。データベースのバックアップは、Azure が提供するバックアップ機能を利用しており、バックアップデータはすべて Azure 内のストレージに暗号化（AES256）され保管されています。また、当社が直接に処分または再利用を行う資源（装置、データストレージ、メモリ、ファイル）を保有しておりません。当社が契約するクラウドサービスプロバイダが、契約に基づき資源の処分または再利用を適切に実施していることを確認しています。
e-BRIDGE SKY Suite のユーザー認証は、Microsoft Azure AD B2C を利用しています。
Microsoft Azure AD B2C は、Microsoft が提供する ID 管理基盤で OpenID Connect（OIDC）を使用して、ユーザーを安全にアプリケーションにサインインさせることができます。
ユーザーが e-BRIDGE SKY Suite を介してデータにアクセスする場合、すべての通信データは HTTPS プロトコルを使用し暗号化されています。なお、HTTPS で用いるプロトコルは TLS1.2 以降のみサポートしています。
e-BRIDGE SKY Suite では、マルウェア（悪意のあるソフトウェア）、ウイルス、その他の脅威からシステムを保護するために Microsoft Defender ウイルス対策を導入しています。万が一脅威が検出された場合でも、適切な対策により迅速な対応が可能となりアカウントの侵害やデータの盗難などの情報漏えいを防止します。また、サイバー攻撃によるセキュリティリスクへの対策として、e-BRIDGE SKY Suite のバックエンドサービスを構成するリソース（サーバーやデータベース等）は、仮想ネットワーク（VNet）でインターネットから分離され、重要データ等に直接アクセスできないように保護されています。
e-BRIDGE SKY Suite は、東芝インフォメーションシステムズ株式会社による脆弱性監査をリリース前および定期的に実施し、システムの安全性を最大限確保しています。脆弱性診断ツールは、「Micro Focus 社 WebInspect」および「Rapid7 社 InsightVM」を使用し、Web アプリケーション特有の脆弱性診断を実施しています。また、SQL インジェクションやクロスサイトスクリプティングをはじめとする Web アプリケーションの脆弱性を突いた攻撃を検知・防御して Web サイトを守るなど、Web アプリケーション固有のリスクを軽減するために、WAF（Web Application Firewall）を設置しています。



### 9.4　e-BRIDGE Global Print のセキュリティ

e-BRIDGE Global Print は、お客様のモバイルデバイスやコンピュータから、印刷したいドキュメントをクラウドサーバーにアップロードすることで、お客様のグループ内に設置された東芝製複合機であれば、どこからでも印刷できるクラウドサービスです。

e-BRIDGE Global Print における通信は、サーバーとお客様のモバイルデバイスやコンピュータとの通信、サーバーと複合機との通信のどちらも、HTTPS 通信（TLS v1.2）により高いセキュリティを実現しています。

e-BRIDGE Global Print では、Google アカウント、または Microsoft アカウントを用いた OAuth2 による認証を行うことにより、高いセキュリティと使いやすい操作性を両立させています。

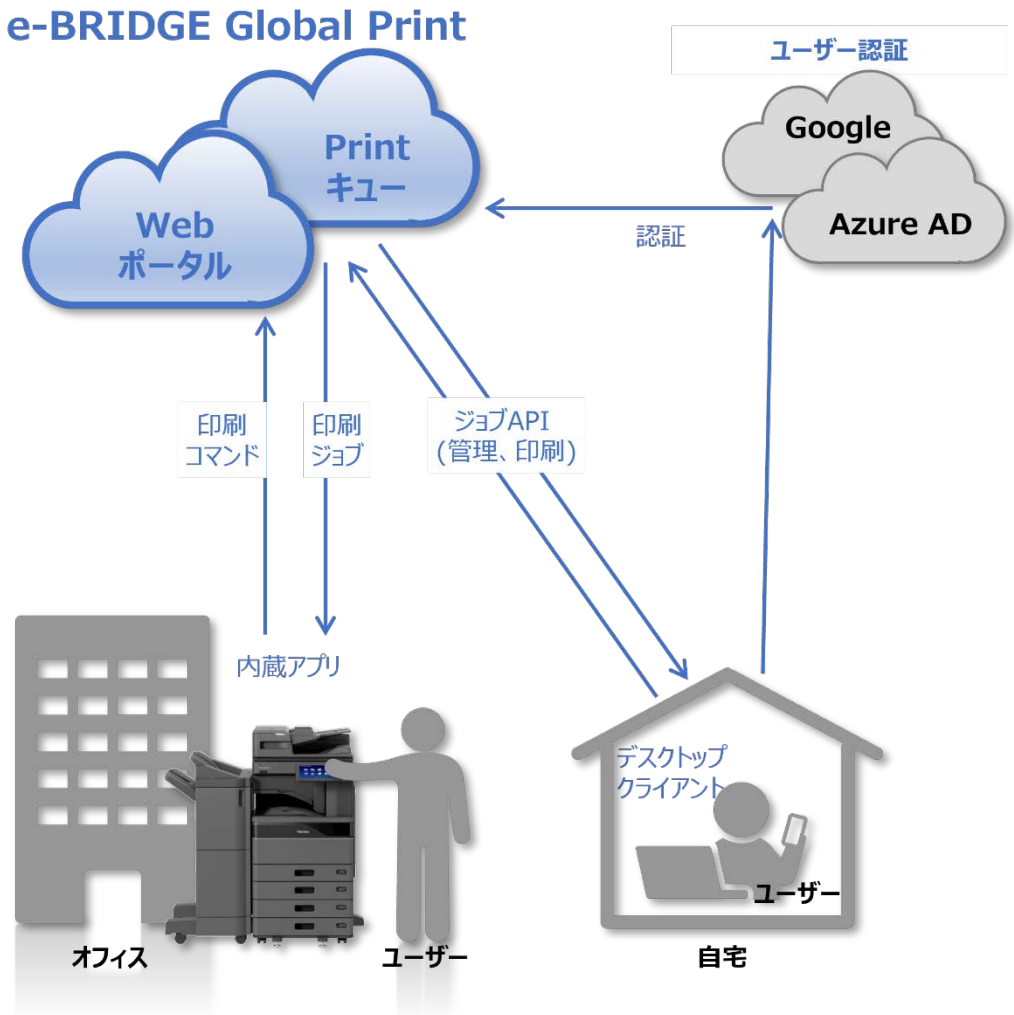
e-BRIDGE Global Print では、管理者があらかじめ発行した登録コードに基づいて、サーバーに認証された複合機のみが接続することができます。これにより、認証されていない複合機がサーバーに接続することはありません。

e-BRIDGE Global Print は、Microsoft Azure 上に構成されており、データセンターのセキュリティは Microsoft Azure によって常に最新に保たれています。Microsoft Azure は、ISO 27001、ISO 27018、SOC 1、SOC 2、SOC3、FedRAMP、HITRUST、MTCS、IRAP、ENS を含む多数の認定に準拠しています。詳細については、Microsoft Azure Web サイトの下記 URL を参照してください

https://www.microsoft.com/ja-jp/TrustCenter/Compliance/

e-BRIDGE Global Print で印刷されるドキュメントデータは、暗号化されたうえで AWS（Amazon Web Service） S3 に保管され、外部からアクセスすることはできません。AWS は、ISO/IEC 27001（情報セキュリティ）、ISO/IEC 27017/27018（クラウドサービスセキュリティ）等に準拠しています。詳しくは AWS のサイトを参照してください。

https://aws.amazon.com/security/



# 10. 法令

## 10.1 複合機本体

### 10.1.1 ISO/IEC15408

ISO/IEC 15408（情報セキュリティ評価基準）は、CC 認証とも呼ばれ、IT 製品のセキュリティ機能および品質を評価・認証する国際基準規格であり、この認証を取得した IT 製品は CCRA（Common Criteria Recognition Arrangement）に加盟している多くの国々において、そのセキュリティ機能、品質が認められております。

EAL は Evaluation Assurance Level の略で、評価の内容を保証するレベルです。評価の対象となる IT 製品は、EAL に定義された内容に従って評価されます。EAL の上位レベルは下位レベルの評価内容を含んでおります。ただし、EAL はセキュリティの強度を示すものではなく、あくまで評価内容の深さを示すものです。EAL のレベルと評価対象のセキュリティレベルの高さとは必ずしも一致致しません。

e-STUDIO4540C Series、および e-STUDIO6550C Series 以降では、IEEE2600.1 に適合した EAL3+ALC_FLR2 で認証を取得しています。

LoopsLP50 Series は、IEEE2600.2 に適合した EAL2+ALC_FLR2 で認証を取得しています。

e-STUDIO5015AC Series および e-STUDIO5018A Series、e-STUDIO7516AC Series、e-STUDIO8518A Series、e-STUDIO5525AC Series、e-STUDIO5528A Series では、HCD PP v1.0（Protection Profile for Hardcopy Devices 1.0）に適合した CC 認証を取得しています。

HCD PP v1.0 とは、日米の IT セキュリティ認証機関である IPA（独立行政法人情報処理推進機構）と NIAP（National Information Assurance Partnership）および日米のデジタル複合機ベンダー各社が共同で作成したデジタル複合機の政府調達のためのセキュリティ要件を記述した文書であり、デジタル複合機に必要とされる数多くのセキュリティ機能や暗号の要件が規定されています。

**CC 認証取得状況**

| 機種名 | 取得時期 | URL |
|---|---|---|
| e-STUDIO550/650/810 | 2004 年 3 月取得 | — |
| e-STUDIO3511/4511 | 2005 年 3 月取得 | — |
| e-STUDIO600/720/850 | 2006 年 3 月取得 | — |
| e-STUDIO281c/351c/451c | 2006 年 3 月取得 | — |
| e-STUDIO232/282 | 2006 年 3 月取得 | — |
| e-STUDIO352/452 | 2006 年 3 月取得 | — |
| e-STUDIO2500C/3500C/3510C | 2006 年 6 月取得 | — |
| e-STUDIO163/165/205 | 取得なし | — |
| e-STUDIO166/167/207 | 取得なし | — |
| e-STUDIO232/282 | 2008 年 8 月取得 | — |
| e-STUDIO352/452 | 2008 年 8 月取得 | — |
| e-STUDIO600/720/850 | 2008 年 8 月取得 | — |
| e-STUDIO2330C/2830C/3520C/4520C | 2008 年 12 月取得 | — |
| e-STUDIO5520C/6520C/6530C | 2008 年 12 月取得 | — |
| e-STUDIO255/355/455 | 2009 年 6 月取得 | — |
| e-STUDIO655/755/855 | 2009 年 6 月取得 | — |

| 機種名 | 取得時期 | URL |
|---|---|---|
| e-STUDIO2040C/2540C/3540C/4540C | 2011 年 10 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0328_it0296.html |
| e-STUDIO5540C/6540C/6550C | 2011 年 10 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0327_it0297.html |
| e-STUDIO206L/256/306/356/456/506 | 2012 年 5 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0348_it1388.html |
| e-STUDIO556/656/756/856 | 2012 年 5 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0349_it1389.html |
| e-STUDIO2050C/2550C | 2012 年 10 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0376_it2409.html |
| e-STUDIO2555C/3055C/3555C/4555C/5055C | 2013 年 4 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0388_it2432.html |
| LOOPS LP30 | 2013 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0412_it3465.html |
| e-STUDIO5560C/6560C/6570C | 2015 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0491_it4484.html |
| e-STUDIO257/357/457/507 | 2015 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0489_it4482.html |
| e-STUDIO657/857 | 2015 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0490_it4483.html |
| e-STUDIO2000AC | 2016 年 9 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0522_it5581.html |
| e-STUDIO2505AC/3505AC/4505AC/5005AC | 2016 年 9 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0523_it5582.html |
| e-STUDIO2508A/3508A/4508A/5008A | 2016 年 9 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0524_it5583.html |
| e-STUDIO5506AC/6506AC/7506AC | 2016 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0528_it5584.html |
| e-STUDIO6508A/8508A | 2016 年 11 月取得 | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0529_it5585.html |
| Loops LP35/LP45/LP50 | 2017 年 7 月取得 (IEEE2600.2) | https://www.ipa.go.jp/archive/security/jisec/software/certified-cert/c0566_it6624.html |
| e-STUDIO2010AC （SYS V1.0） | 2019 年 3 月取得 (Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0629_it8689.html |
| e-STUDIO2515AC/3515AC/4515AC/5015AC （SYS V1.0） | 2019 年 3 月取得 (Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0633_it8690.html |

| 機種名 | 取得時期 | URL |
| --- | --- | --- |
| e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V1.0） | 2019 年 3 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0631_it8692.html |
| e-STUDIO5516AC/6516AC/7516AC | 2019 年 3 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0632_it8693.html |
| e-STUDIO6518A/8518A | 2019 年 3 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0630_it8691.html |
| e-STUDIO2020AC<br>（SYS V1.0） | 2022 年 9 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0756_it1791.html |
| e-STUDIO2525AC/3525AC<br>（SYS V1.0） | 2022 年 9 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0757_it1792.html |
| e-STUDIO4525AC/5525AC<br>（SYS V1.0） | 2022 年 9 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0759_it2808.html |
| e-STUDIO2528A/3528A/4528A<br>（SYS V1.0） | 2022 年 9 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0758_it1793.html |
| e-STUDIO5528A<br>（SYS V1.0） | 2022 年 9 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0760_it2809.html |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>（SYS V2.0） | 2022 年 6 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0746_it1798.html |
| e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 2022 年 6 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0747_it1799.html |

| 機種名 | 取得時期 | URL |
| --- | --- | --- |
| e-STUDIO2020AC<br>（SYS V2.1） | 2023 年 2 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0774_it2810.html |
| e-STUDIO2525AC/3525AC<br>（SYS V2.1） | 2023 年 2 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0775_it2811.html |
| e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 2023 年 2 月取得<br>(Protection Profile for Hardcopy Devices 1.0) | https://www.ipa.go.jp/security/jisec/software/certified-cert/c0776_it2812.html |
| e-STUDIO6527AC/7527AC<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO6529A/9029A<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO2020AC<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO2525AC/3525AC<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO4525AC/5525AC<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO2528A/3528A/4528A<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO5528A<br>（SYS V5.0） | 取得予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 取得予定 | |

#### 10.1.1.1 JCMVP 認証

独立行政法人情報処理推進機構（IPA）によって行われている、暗号モジュールが JIS X 19790（ISO/IEC 19790）に適合することを認証する制度です。

複合機に実装されている各暗号アルゴリズムが正しく実装されたと確認され、以下 IPA の確認リストに登録されています。

**AES 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>（SYS V1.0） | 47 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#47 |
| | 48 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#48 |
| | 49 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#49 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 71 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#71 |
| | 72 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#72 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 74 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#74 |
| | 75 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#75 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 81 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#81 |
| | 82 | https://www.ipa.go.jp/security/jcmvp/verified/aesval.html#82 |
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

**RSA 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>(SYS V1.0) | 20 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#20 |
| | 21 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#21 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 43 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#43 |
| | 44 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#44 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 45 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#45 |
| | 46 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#46 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 52 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#52 |
| | 53 | https://www.ipa.go.jp/security/jcmvp/verified/rsaval.html#53 |
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

**SHS 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>(SYS V1.0) | 31 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#31 |
| | 32 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#32 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 56 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#56 |
| | 57 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#57 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 59 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#59 |
| | 62 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#62 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 65 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#65 |
| | 66 | https://www.ipa.go.jp/security/jcmvp/verified/shaval.html#66 |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

**HMAC 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>(SYS V1.0) | 22 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#22 |
| | 23 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#23 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 35 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#35 |
| | 36 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#36 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 37 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#37 |
| | 40 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#40 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 42 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#42 |
| | 43 | https://www.ipa.go.jp/security/jcmvp/verified/hmacval.html#43 |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

**DRBG 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>(SYS V1.0) | 8 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#8 |
| | 9 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#9 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 20 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#20 |
| | 21 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#21 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 22 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#22 |
| | 24 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#24 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 26 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#26 |
| | 27 | https://www.ipa.go.jp/security/jcmvp/verified/drbgval.html#27 |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

**KDF 確認リスト**

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A<br>(SYS V1.0) | 1 | https://www.ipa.go.jp/security/jcmvp/verified/kdfval.html#1 |
| e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>（SYS V2.0） | 3 | https://www.ipa.go.jp/security/jcmvp/verified/kdfval.html#3 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V1.0） | 4 | https://www.ipa.go.jp/security/jcmvp/verified/kdfval.html#4 |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V2.1） | 5 | https://www.ipa.go.jp/security/jcmvp/verified/kdfval.html#5 |
| e-STUDIO6527AC/7527AC<br>e-STUDIO6529A/9029A<br>（SYS V5.0） | 登録予定 | |

| 機種名 | 確認番号 | URL |
|---|---|---|
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>e-STUDIO2528A/3528A/4528A<br>e-STUDIO5528A<br>（SYS V5.0） | 登録予定 | |
| e-STUDIO2020AC<br>e-STUDIO2525AC/3525AC<br>e-STUDIO4525AC/5525AC<br>（SYS V6.0） | 登録予定 | |
| e-STUDIO2021AC<br>（SYS V5.0） | 登録予定 | |

KDF：Key Derivation Function 鍵導出関数

#### 10.1.1.2 CAVP 認証（FIPS140-2）

CAVP は米国政府機関 NIST とカナダ政府機関 CSEC とで共同で行っている暗号アルゴリズム認証制度（Cryptographic Algorithm Validation Program）であり、認証された暗号アルゴリズムとして NIST にて以下の URL で公開されています。

| 機種名 | Validations | URL |
|---|---|---|
| e-STUDIO2010AC<br>e-STUDIO2515AC/3515AC/4515AC/5015AC<br>e-STUDIO2518A/3518A/4518A/5018A<br>e-STUDIO5516AC/6516AC/7516AC<br>e-STUDIO6518A/8518A | C374 | https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10734 |
| | C375 | https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10735 |
| | C376 | https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?product=10736 |

### 10.2 Wipe 機能付セキュリティ HDD

ハードディスクオプション（GE-1230）に使用している Wipe 機能付セキュリティ HDD は、暗号製品に対する認証制度として、日本の独立行政法人情報処理推進機構（IPA）が行う JCMVP 認証と、アメリカの NIST が行う CMVP（FIPS140-2）認証を取得しております。

#### 10.2.1 JCMVP 認証

JCMVP は、独立行政法人情報処理推進機構（IPA）が行う、JIS X 19790（ISO/IEC 19790）に基づく暗号モジュール認証制度で、AES、SHS、HMAC、DRBG が暗号モジュールとして正しく実装されたと認証され、以下 IPA の暗号モジュール認証製品リストに登録されています。

| 機種名 | 確認番号 | URL |
|---|---|---|
| GE-1230<br>（東芝製 Wipe 機能付セキュリティ HDD：<br>MQ01ABU050BW, MQ01ABU032BW,<br>MQ01ABU025BW） | F0022 | https://www.ipa.go.jp/security/jcmvp/val.html#F0022 |

#### 10.2.2 CMVP 認証（FIPS140-2）

CMVP は米国政府機関 NIST とカナダ政府機関 CSEC とで共同で行っている暗号モジュールの認証制度であり、Cryptographic Module Validation Program を意味しており、認証された暗号モジュールとして NIST にて以下の URL で公開されています。

| 機種名 | 確認番号 | URL |
|---|---|---|
| GE-1230<br>（東芝製 Wipe 機能付セキュリティ HDD：<br>MQ01ABU050BW, MQ01ABU032BW,<br>MQ01ABU025BW） | 2082 | https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2082 |
| GE-1350<br>（Phison 製 SSD：<br>PHSSS512GECTI-IA-TE1010） | 3758 | https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3758 |

### 10.3 HIPAA

医療保険の相互運用性と説明責任に関する法律は、患者情報が医療組織内と組織外の両方で最高レベルの機密性で扱われることを保証するように設計されています。 東芝のセキュリティソリューションは、保護された患者情報のプライバシーとセキュリティに対処するさまざまな機能を提供します。 安全なデバイスアクセス、プライベート印刷機能、および監査証跡は、デバイスの不適切な使用を防ぎ、許可されたユーザーのみが機密データまたはドキュメントを受信できるようにします。

### 10.4 GLB Act

Gramm-Leach-Bliley Act は金融機関に直接関係しており、消費者が自分の個人的な財務情報がどのように使用および共有されているかを認識できるようにします。 財務プライバシー規則およびセーフガード規則は、個人の財務情報の開示を管理し、すべての金融機関が顧客情報の保護をサポートするシステムを設計および保守することを要求します。

### 10.5 FERPA

家庭教育の権利とプライバシー法は、学生の教育記録のプライバシーを保護する連邦法です。 これには、米国教育省に準拠する教育機関のセキュリティレベルを高める必要があります。 パスワードの印刷、制御されたデバイスアクセス、データの暗号化および/または削除により、多機能デバイスで機密情報にアクセスできないようにします。

### 10.6 サーベンス・オクスリー法 （SOX）

先頃、金融慣行とコーポレートガバナンス規制を変更することを目的とした厳格な規則が導入されました。 注目を集める企業スキャンダルを受けて、これは証券法に関連して行われた企業財務開示の正確さを改善することによって投資家を保護するために可決されました。 データセキュリティセーフガードは、情報へのアクセスの制限、データの追跡、およびデータの整合性の保護に重点を置いています。

### 10.7 DoD

アメリカ合衆国大統領直属の国防総省は、国家安全保障および防衛政策を策定しています。 国防総省のマニュアルは、米国の安全を保護するための厳格なポリシーと基準の概要を示しています。 東芝のディスク上書きソリューションは、機密情報を含むハードディスクドライブをクリアおよびサニタイズするという DoD 標準に準拠しています。

### 10.8 カリフォルニア州 IoT 機器セキュリティ法（SB-327）

2020 年 1 月 1 日に施行されたこのカリフォルニア州法では、ネットワーク接続デバイスの製造業者に対して、デバイスが収集、格納、または送信する可能性のある情報に応じて、デバイスおよびデバイスに含まれる情報を不正アクセス、破壊、使用、変更、または開示から保護するように設計された、合理的なセキュリティ機能をデバイスに装備することを要求しています。

### 10.9 組織におけるセキュリティ

情報化社会の進展の中、個人情報は益々重要な資産となっております。一方で、本人の知らないところで個人情報が不正に収集され、予想外の目的で使用される事態が増大し、個人情報の取り扱いに対する社会的関心が急激に高まっています。

このような環境下、いったん大量の個人情報が漏えいすれば企業の信用失墜のみに留まらず、企業の存続にかかわるほど甚大な被害を及ぼす危険性が潜んでおります。お客様との信頼関係を築き、個人情報を有効に活用するとともに個人情報の保護を図ることは企業の社会的責務です。

東芝テックでは、製品ユーザーである企業様が情報漏えいを防ぐために前述したような多様なセキュリティ機能を搭載した製品を提供しております。今後、お客様とのパートナーシップを強め、より安全なセキュリティ対策を進めていきます。

また東芝テックは、早い時期より個人情報保護の重要性を認識し、2001 年 2 月に社内規程として「個人情報保護方針」および「個人情報保護ガイドライン」を制定しておりました。

2004 年 8 月に「個人情報保護方針」を改定し Web 上で公開。2004 年 11 月に「個人情報保護ガイドライン」を法令等に沿った形で大幅に改定し、新たに「個人情報保護プログラム」（PDPP：Personal Data Protection Program）として制定する等、体制整備を行いました。

東芝テックの個人情報保護方針の詳細については以下の URL を参照してください。

https://www.toshibatec.co.jp/privacy/