SHARP

シャープ デジタル複合機のセキュリティガイド

- デジタル複合機を安心してお使いいただくために -

シャープ株式会社

はじめに

平素は、シャープのデジタル複合機をご愛用いただき、誠にありがとうございます。
シャープのドキュメントセキュリティシステムは、デジタル複合機を利用するお客様の大切なデータを守るため、想定されるさまざまな脅威への対策を用意しております。
本書をご一読いただき、適切な環境を構築し、適切な対応を選択頂くよう、お願いいたします。

ご注意:
本書に記載する一部のセキュリティ機能については、機種によって非搭載、またはオプションが必要となる場合があります。詳しくは、各機種のユーザーマニュアル、巻末の「機種別搭載セキュリティ機能」、または当社 Web サイト
https://jp.sharp/business/print/solution/security/state3-9.html をご覧ください。

目　次

はじめに 2
複合機のセキュリティに対するシャープの取り組み 3
複合機のセキュリティ 4
デジタル複合機のセキュリティとは …… 4
セキュリティの脅威と脅かされる情報資産 …… 4
セキュリティの脅威と求められるセキュリティソリューション 5
外部からの不正アクセスによる情報漏洩 …… 6
デジタル複合機内データからの情報漏洩 …… 8
本体メモリ装置の持ち出しによる情報漏洩 …… 8
ネットワークからの不正アクセスによる情報漏洩 …… 9
悪意のあるプログラムからの不正アクセスによる情報漏洩 …… 10
撤去・廃棄されたデジタル複合機のメモリ装置からの情報漏洩 …… 10
ネットワーク入出力データへの不正アクセスによる情報漏洩や改竄 …… 11
誤送信による情報漏洩 …… 12
出力した紙文書の持ち去りによる文書データの漏洩 …… 13
不正コピーによる文書データの漏洩 …… 13
権限の無いユーザーの使用による可用性の低下やデータの漏洩 …… 14
BIOS・ファームウェアの改竄・破損によるセキュリティ機能の喪失 …… 15
ウイルス感染による情報漏洩・システムの破壊やウイルスの拡散 …… 15
使用状況の把握、および情報漏洩の心理的な抑止対策 …… 16
機種別搭載セキュリティ機能 17

複合機のセキュリティに対するシャープの取り組み

シャープは、デジタル複合機のデータセキュリティにいち早く取り組み、2000 年 4 月、米国をはじめ海外向けにデータセキュリティキットを発売。2001 年 4 月には、米国認証機関から複写機・プリンター業界では世界で初めて「Common Criteria」の認証（セキュリティ認証）を取得しました。
さらに、2017 年 10 月には、日本の認証機関から業界では世界で初めて「ハードコピーデバイスプロテクションプロファイル v1.0」に適合した Common Criteria の認証を取得しました。

Common Criteria とは
Common Criteria（コモンクライテリア）とは、情報システムやそれを構成するハードウェア／ソフトウェアの IT 製品について、目標となるセキュリティ保証レベルを基準に基づいて評価するための国際規格の名称です。
1999 年 12 月に「ISO/IEC 15408 情報技術セキュリティ評価基準」として国際規格化されました。
1998 年 10 月、米英独仏加の 5 ヵ国により CCRA（Common Criteria Recognition Arrangement）が設立され、Common Criteria に基づき評価・認証された IT 製品は、認証を取得した国だけではなく、CCRA に加盟している他国でも認証の適用が認められます。日本では、2000 年 7 月に ISO/IEC 15408 が「JIS X 5070」として JIS 化、2001 年 4 月に、「IT セキュリティ評価及び認証制度（JISEC）」が創設され、2003 年 10 月に CCRA に加盟しました。

ハードコピーデバイスプロテクションプロファイルとは
ハードコピーデバイスプロテクションプロファイル(Hardcopy Device Protection Profile、HCD PP)とは、日本と米国のデジタル複合機の政府調達のためのセキュリティ要件の名称です。日本の IT セキュリティ認証機関 IPA(独立行政法人情報処理推進機構)と米国政府の IT セキュリティ認証機関 NIAP (National Information Assurance Partnership)が共同で、デジタル複合機ベンダー各社や評価機関と協力し開発、バージョン 1.0 が 2015 年 9 月 10 日付で完成、公開されました。

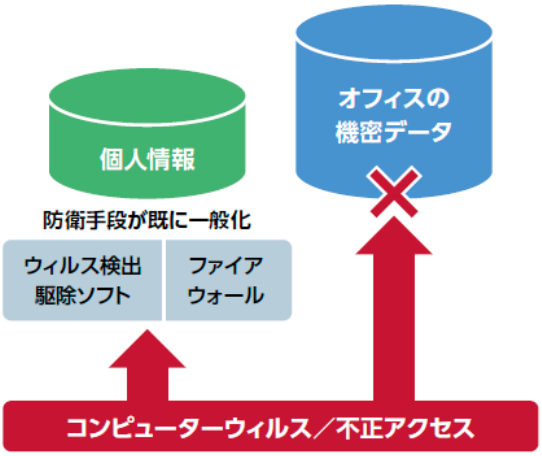
(注) 各製品が取得した情報セキュリティに係る認証は、評価に用いた評価対象(Target of Evaluation)が所定の評価基準及び評価方法に基づく評価の結果、セキュリティ保証要件に適合していることを示すものです。
また、本書に記載されているすべてのセキュリティ機能に対して認証を取得したものではありません。認証を取得した各製品のセキュリティ機能について、詳しくは、各製品のセキュリティターゲットをご覧ください。
認証を取得した製品のセキュリティターゲットは以下の Web サイトからご覧いただけます。
https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html

シャープはデジタル複合機の企画開発段階から、お客様のオフィス環境におけるセキュリティの脅威を想定し、あらゆる知識と技術を結集してその対策を提供しております。
また、進化し続けるネットワーク技術により変化するお客様のオフィス環境では、デジタル複合機に対するセキュリティの脅威も日々進化しています。この過程で、デジタル複合機のシステムに対する脆弱性が発見された場合には、速やかに対応を行っております。

複合機のセキュリティ

デジタル複合機のセキュリティとは

ネットワーク環境の急速な発展とコンピューターの普及に伴い、コンピューターウイルスや外部からの不正アクセス、機密データ漏洩等の情報犯罪が急増し、深刻化しています。
このような状況下で自らを守るためには、リスクに対して効果的な防衛手段が必要なのは言うまでもありません。コンピューターウイルスに対してはウイルス検出/駆除ソフト、不正アクセスに対してはファイアウォールというように、従来から危険視されていた情報犯罪については有効な防衛手段が既に一般化しています。しかしながら、オフィスの情報漏洩という問題に対しては、いまだ利用者のモラルに依存しているというケースが多いのではないでしょうか。



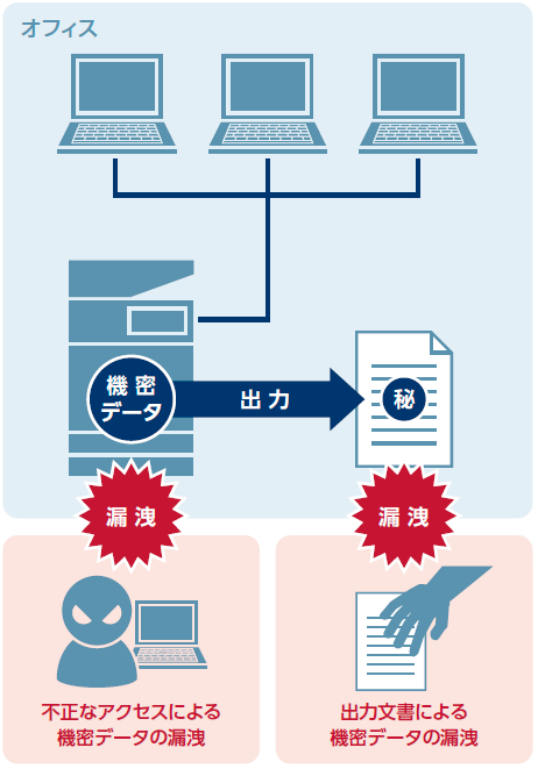
2016 年 1 月から本格的に運用が開始されたマイナンバーは、法令で定められている目的で収集する場合を除きコピーが禁止されています。従業員から預かったマイナンバーを含めた個人情報を安全に管理することは、事業者として重要となっています。また、2020 年 6 月に改正・公布され、2022 年 4 月に施行される「個人情報保護法」をはじめとした法令の整備などに伴って、さらに内部統制・コンプライアンスの重要性が増しています。

セキュリティの脅威と脅かされる情報資産

オフィスでは毎日、重要な情報が扱われています。顧客データや未発表の新商品情報、経営/人事情報……

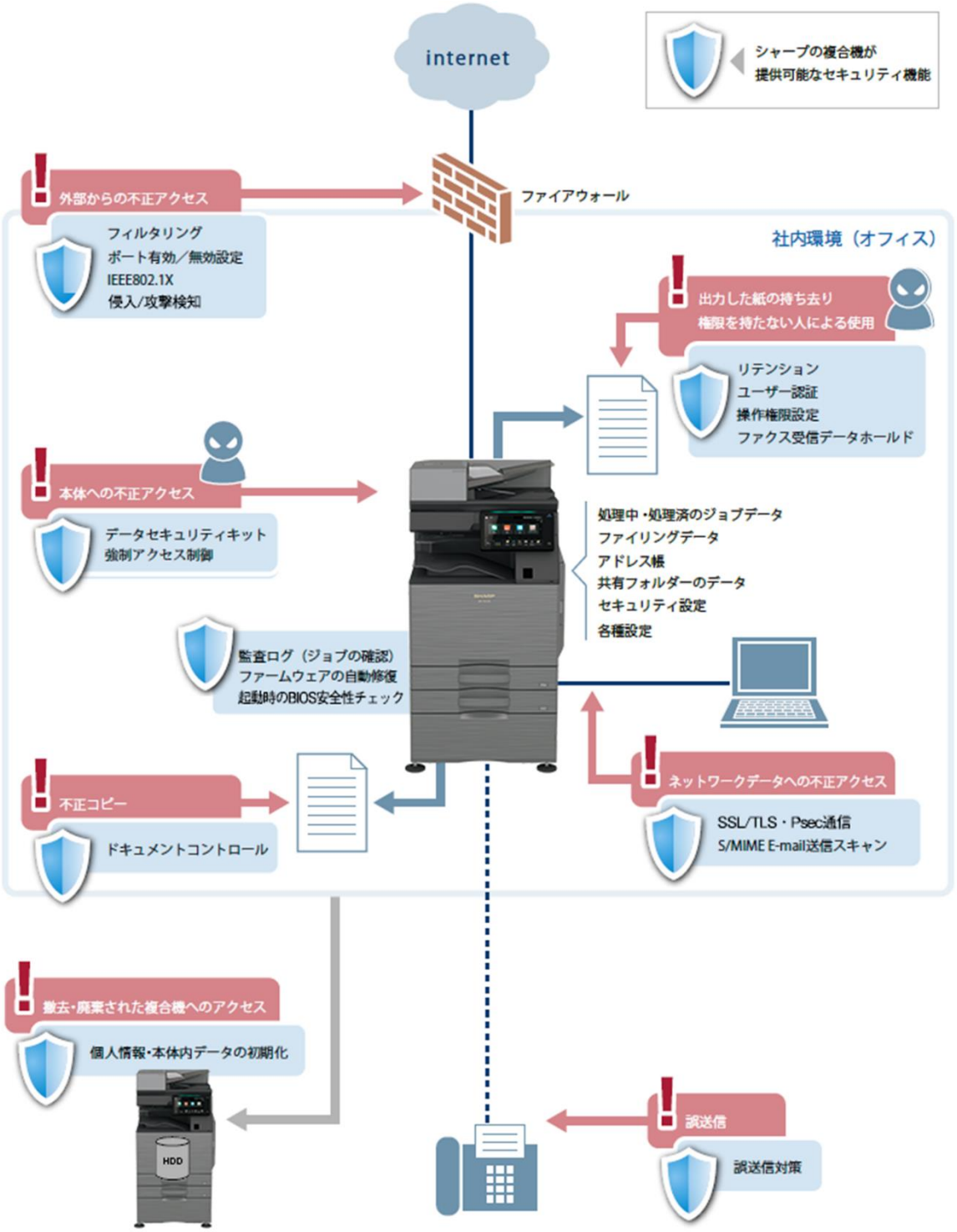
もし万が一、これらの重要な情報が、悪意を持つ者に閲覧・利用された場合、どうなるでしょうか？お客様や取引先からの信用は失われ、経営に深刻なダメージを受けることはもちろん、情報の種類によっては、企業としての社会的責任を問われることもあるでしょう。企業や組織にとって、機密情報の漏洩は致命的です。

このように機密情報が漏洩することによりもたらされる被害の深刻さは容易に想像できると思いますが、その反面、日常の業務においてその危険性を認識している方は少ないのではないでしょうか。しかし、オフィスで扱われるデータは、漏洩の危険と常に隣り合わせなのです。



セキュリティの脅威と求められるセキュリティソリューション

お客様のオフィス環境や取り扱う情報に対して、どのような脅威が考えられるでしょうか。それらの脅威に対して、シャープがご提供するソリューションについてご説明いたします。



※製品によっては、一部の機能に対応しない場合があります。

外部からの不正アクセスによる情報漏洩

➤脅威

ファイアウォール等、外部からのアクセスを防御する機器を設置せずインターネットへ接続している場合は、インターネットからの攻撃に直接さらされる危険性があります。具体的には、複合機 Web ページにブラウザーから直接アクセスされ、セキュリティ設定や受信データの転送先情報を変更されたり、以下のようなデータを不正に閲覧、取得されたりする可能性があります。

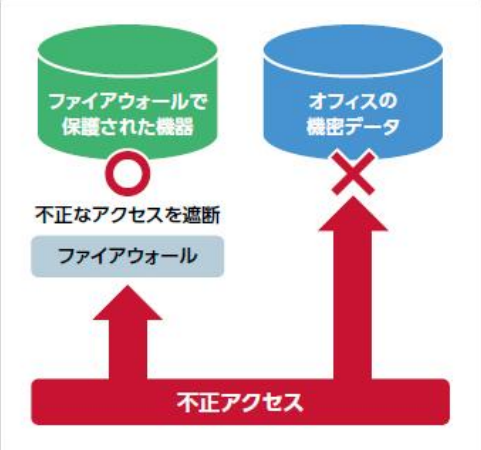
- デジタル複合機に保存したドキュメントファイリングデータ
  - 一時保存フォルダー内のデータ
  - 標準フォルダー内のパスワードの設定されていないデータ
  - パスワードの設定されていないユーザーフォルダー内のパスワードの設定されていないデータ
- アドレス帳のエントリー(名前、メールアドレス、ファクス番号等)
- 共有フォルダーのデータ

➤対策

基本的には、IPv4 環境ではプライベート IP アドレスでの運用をお願いします。

デジタル複合機は法令上、電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダなど）の通信回線（公衆無線 LAN を含む）に直接接続することはできません。デジタル複合機をインターネットに接続する場合は、必ずルーターなどを使用し、割り振られた範囲のサブネットワーク内でファイアウォールなどの保護を行い管理してください。

一般的なオフィス環境においては、利用可能な IPv4 アドレスが逼迫していることからルーターなどの機器をお使い頂いている場合がほとんどであり、プライベート IP アドレス(インターネットから分離され、オフィス内のみに利用を制限した IP アドレス)での運用となりますので、外部からのアクセスを遮断することができます。しかしながら、一部環境においては、グローバル IP アドレス(直接インターネットに接続する際に使用される IP アドレス)にて接続されている場合があり、速やかにご対応いただく必要があります。



お客様のネットワーク環境がファイアウォール等により外部からのアクセスから保護されているかどうかをご判別いただくには、デジタル複合機にプライベート IP アドレスが割り当てられていることをご確認ください。
プライベート IP アドレスは、右表の範囲と定義されています。

プライベート IP アドレスの範囲		
10.0.0.0	～	10.255.255.255
172.16.0.0	～	172.31.255.255
192.168.0.0	～	192.168.255.255

※デジタル複合機に割り当てられている IP アドレスの確認方法については、お買い上げの販売店にお尋ねください。

管理者パスワードを工場出荷時の初期値から変更してください。

複合機 Web ページを操作するためには、所定のパスワードを入力(管理者としてログイン)する必要があります。
デジタル複合機の工場出荷時には、管理者パスワードが設定されていますが、パスワードの初期設定値は取扱説明書にも記載されており、誰でも容易に知ることができます。はじめてデジタル複合機をご使用になるときに管理者が変更するとともに、厳重に管理してください。
※管理者パスワードの変更方法については、スタートガイドを参照、もしくはお買い上げの販売店にお尋ねください。

お使いの PC やサーバーには、できる限り最新のセキュリティ更新を適用してください。

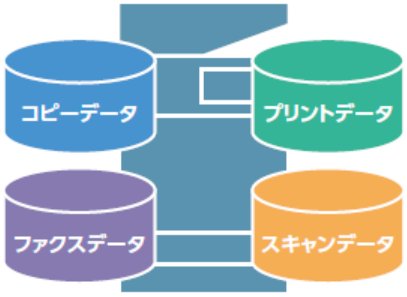
デジタル複合機だけでなく、お客様の重要なデータを扱う PC やサーバーへの攻撃が行われることがあります。これらの攻撃から保護するために、できる限り最新のセキュリティ更新を行ってください。

ごくまれに、最新のセキュリティ更新により、使用可能な通信プロトコルが制限されることがあるため、デジタル複合機と PC やサーバーとの接続が行えなくなることがあります。まずはお使いのネットワーク環境をファイアウォール等によりインターネットからの接続を制御した上で、イントラネット内で特定のセキュリティ更新を行うことによる機器の可用性の低下と更新を行わないことにより起こり得るリスクの大きさとを勘案し、適切なレベルのセキュリティ更新を行うようにしてください。

デジタル複合機内データからの情報漏洩

デジタル複合機は、電子ソートなど、その多彩な機能を実現するために、一旦ハードディスクなどのメモリ装置にコピー/プリント/ファクス/ネットワークスキャンなどのジョブデータを一時的に保存する仕組みになっています。また、デジタル複合機によっては、これらのジョブデータを後で再利用するためにファイリング機能を有しているものもあります。

■ デジタル複合機に蓄積されている様々なデータ



本体メモリ装置の持ち出しによる情報漏洩

➤脅威

ジョブデータやファイリングデータを保存したデジタル複合機内のハードディスクやフラッシュメモリー等のメモリ装置を不正に持ち出すことにより、情報漏洩する可能性があります。

➤対策

データセキュリティキット

シャープのデータセキュリティキットは、暗号化、実データ消去、パスワード保護機能等により高い安全性を確保しています。

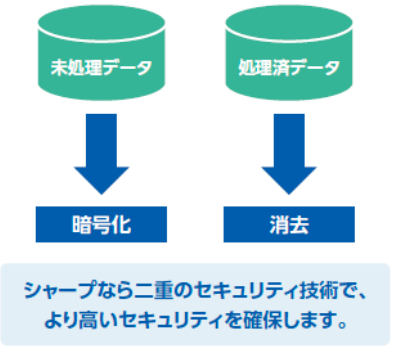
— 機能 —

■暗号化

ジョブデータとドキュメントファイリングデータは、デジタル複合機内の記憶装置に保存されています。これらのデータを暗号化することにより、たとえ何らかの方法でデータを入手できたとしても、復元できない状態となります。

シャープのデータセキュリティキットでは、データの暗号化に用いる暗号鍵を保護する手段の一つとして、TPM(Trusted Platform Module)を利用します(一部製品を除く)。TPM はセキュリティに関するさまざまな機能を搭載した専用チップであり、パーソナルコンピューターなど今日の IT 機器に広く搭載されています。

■ シャープの二重セキュリティ技術



■ハードディスク内の実データ消去

通常、ハードディスクに書き込まれたジョブデータやドキュメントファイリングデータは、消去操作を行っても実データ部は消去されません。これは、ジョブデータやドキュメントファイリングデータの所在を示す情報だけを消去しているためです。したがって、一見、消去されたように見えていても、実際には他のデータで上書きされるまで実データ部は残存しています。専門的な知識・技術をもってすれば、消去後であっても実データを復元させることも可能です。

ハードディスクを装着したシャープのデジタル複合機において、データセキュリティキットでは、ハードディスクに書き込まれたジョブデータやドキュメントファイリングデータの消去には、実データ部を乱数値等により上書きした後に、データの所在を示す情報を消去する方法を採っており、実データ部を復元できないようにします。

― 特長 ―

■操作性の良さ

シャープのデータセキュリティキットによるデータの暗号化/ハードディスク内の実データ部の消去は、利用者が意識することなく自動的に機能します。そのため、機密データを扱う際に特別な操作を行うことなく、高いセキュリティレベルを維持できます。

ネットワークからの不正アクセスによる情報漏洩

➤脅威

例えば、多くのオフィスでは、インターネットへの接続に際してファイアウォールを設置するなど不正アクセス対策を施していると思います。しかし、イントラネット内部からのデジタル複合機への不正アクセスについては特に対策していないという場合が多いのではないでしょうか？重要なデータを入力したり出力したりするデジタル複合機は情報漏洩の格好のターゲットとなり得ます。

➤対策

ネットワークアドレス（IP/MAC アドレス）のフィルタリング

ネットワークインタフェースでは、特定の IP アドレスや MAC(マック)アドレス※をアクセス許可/拒否に指定することにより、複合機にアクセス可能なアドレス範囲を特定することで、不正なアクセスを防止します。

例えば、IP アドレスフィルタリングでは、社内ネットワークで特定の部署・グループの PC や端末のみでデジタル複合機を使えるように設定することができます。また、MAC アドレスフィルタリングでは登録していない端末(外部から持ち込み社内ネットワークに接続した PC や端末等)をデジタル複合機に接続できなくすることができます。

※MAC アドレスによるフィルタリングは、アクセスを許可するアドレスの指定のみ可能です。

ネットワークポートの有効/無効設定/ポート番号の変更

ネットワークプロトコルを用いて通信を行う際に必要なネットワークポートの有効/無効の設定や、ポート番号の変更を行なうことにより、ポートスキャン等、悪意を持ったアクセスを受け付けないようにしたり、外部への意図せぬデータ送信を制御したりすることが可能です。

侵入/攻撃検知

一定の時間内に規定値以上のネットワークアクセスを複合機が検知した場合、この複合機に対する攻撃が行われたと判断し、これらのアクセスをきっかけに行われる侵入を防止するため、当該アクセス元からのアクセスを拒否します。

拒否するアクセス元が 100 件を超えた場合は、その複合機に対する全てのネットワークアクセスを拒否します。

特定発信元からの受信可否設定

ファクス、インターネットファクスの受信時に、不正な発信者からの送信により、通常の受信が阻害される、あるいは有害/不要な情報を受信することを防ぐために、特定番号/特定アドレスからの受信を拒否することができます。また、特定番号/特定アドレスからのみ受信することもできます。

番号/アドレスの指定は、ファクス、インターネットファクスのそれぞれについて 50 件ずつ設定可能です。

IEEE802.1X

IEEE802.1X は、無線 LAN や有線 LAN にネットワーク機器を接続する際に、許可された利用者のみ接続を許可するための認証技術です。悪意を持つ者がネットワークに機器を接続し、デジタル複合機を不正使用するのを防ぐことが可能になります。

認証プロトコルは EAP-TLS と PEAP に対応しています。

ドキュメントファイリングのパスワード保護

ドキュメントファイリングとは、再利用を前提としてデジタル複合機にジョブデータを保存する機能ですから、利用者の消去指示があるまでデータはドキュメントファイリングデータとしてデジタル複合機内に存在します。このドキュメントファイリングデータは、データ毎にパスワードを付加できるようになっています。このパスワードが一致しなければ、ドキュメントファイリングデータを再利用できないようにします。

ファクス回線からネットワークへの侵入について

デジタル複合機に搭載のファクスモデムソフトウェアは、スーパーG3/G3 通信をサポートするもので、PPP、TCP/IP フレームの送受信等の電話回線を通じてコンピューターをネットワークに接続するためのプロトコルは実装しておらず、公衆回線経由の LAN への侵入は不可能です。

悪意のあるプログラムからの不正アクセスによる情報漏洩

➤脅威

デジタル複合機の外部や内部からの不正なアクセスにより、本体機能が不正に使用されたり、その結果本体に格納されたデータが漏洩したりすることが考えられます。

➤対策

強制アクセス制御

本体内のプログラムやデータに対するアクセスを監視し、許可されていないプログラムからそれらへのアクセスが発生したことを検知した場合、そのアクセスを拒否するとともに、設定により、監査ログに記録したり、E-mail アラートによる管理者への通知をしたりすることができます。

撤去・廃棄されたデジタル複合機のメモリ装置からの情報漏洩

➤脅威

リース期間が終了、あるいはご購入後に撤去されたり、廃棄されたりしたデジタル複合機についても、お客様の管理から離れた後に情報が漏洩する危険性があります。

➤対策

個人情報及び本体内データの初期化機能

デジタル複合機の撤去・廃棄に際し、本体内の以下の情報を上書き消去(初期化)することができます。

- 本機内のジョブデータ、および、ドキュメントファイリングデータ
- アドレス帳及び関連する個人情報
- 利用者情報
- 登録プログラム、ファクス/イメージ送信定型文、ジョブログ
- システム設定

ネットワーク入出力データへの不正アクセスによる情報漏洩や改竄

➤脅威

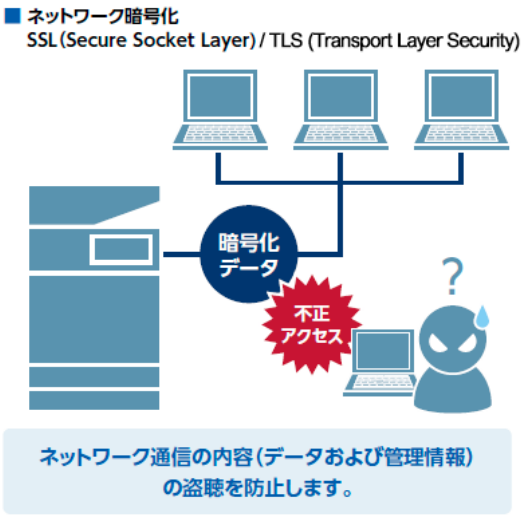
オフィスのネットワークでは、重要な情報がやり取りされています。これは、デジタル複合機のプリントデータやデジタル複合機のリモート管理等のネットワーク入出力データにおいても同様です。これらデジタル複合機のネットワーク入出力データが盗聴されることにより、情報が漏洩したり、改竄されたりする可能性があります。

➤対策

SSL（Secure Socket Layer）/TLS (Transport Layer Security) 暗号化通信

ネットワーク通信データの盗聴を防止するには、ネットワークプリントや Web ブラウザーを介したデジタル複合機との通信は、ネットワーク通信データそのものを暗号化することが効果的です。これにより、たとえ盗聴されたとしても、その内容を解読することが非常に困難になります。

ネットワークを利用してパソコンからデジタル複合機へデータを送信するときや、パソコンの Web ブラウザーを利用してデジタル複合機の管理用 Web ページにアクセスするとき、E-mail、FTP サーバー等でのデータ通信には、SSL/TLS プロトコルを使うことにより、これらの機器間の通信を暗号化します。



暗号化 PDF ファイル対応（送信/ダイレクトプリント）

スキャンした文書を PDF ファイル化する際に暗号化します。また、デジタル複合機のオペレーションパネルでパスワードを入力することにより、暗号化された PDF ファイルの印刷も可能です。暗号化された PDF ファイルが通信途中で盗聴されたとしても、その内容を解読することは困難です。

IPsec

IP のパケット単位で暗号化を行なうことにより、通信途中でのデータ内容の盗聴や改竄を防止します。

SNMPv3

デジタル複合機の管理に使用される通信も、暗号化をサポートする SNMPv3 により、盗聴を防止します。

S/MIME (Secure/Multipurpose Internet Mail Extensions)

スキャンデータを E-mail で送信する際、宛先となる受信者の公開鍵を用いて暗号化します。暗号化されたデータは、その受信者のみが持つ秘密鍵でのみ復号することができますので、通信途中で盗聴されたとしても、その中身を解読することは困難です。公開鍵はアドレス帳にあらかじめ登録しておき、S/MIME 暗号化送信はアドレス帳からの宛先選択の場合のみ使用可能です。また、スキャンデータに対し、送信元となるデジタル複合機の秘密鍵を用いて電子署名すると、そのデジタル複合機の公開鍵を用いてのみ署名を検証することができますので、送信元の証明、および、通信途中での改竄が行われていないことの証明となります。

※スキャンによるメール送信時のみ対応しています。

誤送信による情報漏洩

➤脅威

イメージ送信とは、スキャンしたデータをファクス、E-mail、FTP などでオフィスや外部のファクス/サーバー/パソコンに送信する機能です。意図せず送信先を間違った場合、情報が漏洩する可能性があります。

➤対策

宛先直接入力禁止

宛先指定にはアドレス帳を利用することにより、宛先の入力ミスによる誤送信を防止することができます。

再送信キーの利用禁止

前の人が送信したアドレスに、誤送信してしまうのを防止します。

宛先確認機能

宛先を一度入力した後、再度宛先を確認、もしくは、再度入力するダブルチェック機能で送信先の入力間違いを防止します。

暗号化 PDF ファイル対応（送信）

送信ファイルに暗号化 PDF を指定することで、万一誤送信されたとしても、パスワードを知らなければ解読することができません。

FASEC 1 に準拠

FASEC とは、情報通信ネットワーク産業協会（CIAJ）がファクシミリ通信のセキュリティ向上を目指して制定したガイドラインの呼称です。

誤送信の防止や受信紙の放置防止など、ファクスデータにおいてもセキュリティ対策に努めております。

出力した紙文書の持ち去りによる文書データの漏洩

➤脅威

プリントやファクス出力を放置したままにしているのを見かけた方も多いのではないでしょうか。特にプリントの場合、忘れてしまっていることも多く、盗み見されたり、持ち去られたりして、情報漏洩して初めて気づくことになります。

➤対策

リテンション（親展プリント）機能

プリントデータをデジタル複合機に保存しておき、必要なときに本機の操作パネルからプリントする機能です。パソコンからプリントするときにパスワードを設定し、デジタル複合機に保存されているデータをプリントするときにパスワードを入力することにより、プリント結果を他人に見られたり持ち去られたりすることを防止します。

プリントリリース機能によるプリントジョブの保護

複数のデジタル複合機を有している場合、「プリントリリース」機能を使用することにより、対応した任意のデジタル複合機からプリントデータを出力することができます。印刷したいデジタル複合機が稼働中でプリントできない場合でも、他のデジタル複合機を利用することにより、本人がログインし印刷指示をすることでプリントが可能で、出力用紙の取り忘れや放置による情報漏洩を抑止します。

※プリントリリース機能の詳細については、販売店にお尋ねください。

ファクス受信データホールド

ファクス受信データを出力せずに一旦メモリに保存します。あらかじめ登録したパスワードを入力することで出力します。ファクス受信データを出力する場合に比べ、盗み見や、用紙の持ち去りによる情報漏洩の危険を減らします。

不正コピーによる文書データの漏洩

➤脅威

オフィスで使用される機密文書には、「社外秘」「極秘」等と指定されていることが多いですが、悪意を持ってコピーされれば簡単に情報漏洩してしまいます。

➤対策

ドキュメントコントロール

例えばマイナンバーなどが記載された機密文書の出力時に不正コピー防止データを埋め込むことができます。不正コピー防止データが埋め込まれた文書を、ドキュメントコントロール機能を搭載したシャープデジタル複合機で不正にコピーしようとした場合は、白紙出力やコピーキャンセルなどによって不正コピーを防止します。

※オプションのデータセキュリティキットが必要です。

権限の無いユーザーの使用による可用性の低下やデータの漏洩

➤脅威

情報漏洩事件は、その多くが内部犯行であるという報告があります。内部の人間は必然的に機密情報に触れる機会が多く、故意ではなくとも、情報漏洩を起こす可能性がないとは言い切れません。また、使用権限の無いユーザーがデジタル複合機を使用する、また使用権限があってもその範囲を超えて使用することにより、本当に使用したいユーザーが使用できなくなったり、そのため作業効率が低下したりする恐れがあります。

➤対策

ユーザー認証/操作権限設定

ユーザーID/パスワード、または、IC カードによる個人認証により、デジタル複合機への不正アクセスを防止します。

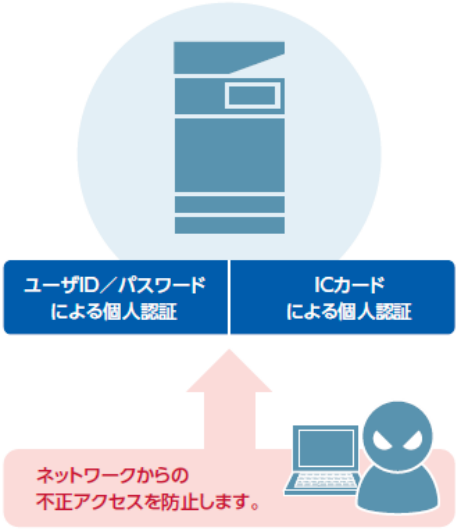
■操作パネル/IC カードによる認証

ユーザーID とパスワードの操作パネルからの入力、または IC カードによる個人認証※を行うことで、許可された利用者のみ、デジタル複合機を使用可能になります。また、本体での認証とともに外部サーバーでの認証も可能です。

※オプションの IC カードリーダーライターと IC カードが必要です。IC カードリーダーライターの詳しい内容につきましては、ご販売店にお尋ねください。

■操作権限の設定

ユーザーグループごとに、デジタル複合機の各機能の使用許可/禁止、また、デジタル複合機の設定を行う権限を付与することができます。



Active Directory によるユーザー管理

企業に導入された PC の多くは Active Directory によりユーザーやセキュリティレベルが集中管理されています。デジタル複合機もこの Active Directory を利用した管理を行うことで、複数のデジタル複合機のユーザー認証や機能の利用権限を一元管理することができます。Active Directory サーバーにセキュリティおよび省エネルギー関連の設定をグループポリシーとしてあらかじめ用意しておくことにより、Active Directory 環境に参加したデジタル複合機の起動時に、自動的にグループポリシーを適用することができます。

また、「SharpAccountant Lite」を活用すると各ユーザーの使用状況を把握でき、デジタル複合機の効率的な運用をサポートします。

※Active Directory 連携、SharpAccountant Lite の詳細については、販売店にお尋ねください。

BIOS･ファームウェアの改竄･破損によるセキュリティ機能の喪失

➤脅威

デジタル複合機の BIOS(Basic Input/Output System)やファームウェアが、悪意のある第三者やプログラムにより改竄されたり、何らかの理由によって破損したりすると、機能の喪失によりデジタル複合機が正常に使えなくなったり、セキュリティ機能の改竄や喪失を招き、本体に格納されているお客様のデータの漏洩や喪失が起こる可能性があります。

➤対策

起動時の BIOS 完全性チェック

BIOS は、デジタル複合機の起動時に最初に読み込まれ、かつ重要な役割を果たすプログラムであり、デジタル複合機の機能を司るファームウェアを読み込むために必要なプログラムです。この BIOS の改竄や破損が行われていないこと(完全性)を、デジタル複合機のシステムとは独立した仕組みでチェックします。異常が検出されると、デジタル複合機の起動処理を停止します。

ファームウェアの自動修復

本機能を搭載したデジタル複合機には、実際に動作するファームウェアの他に、破損修復用のファームウェアが格納されています。ファームウェアの異常検出は、デジタル複合機の起動時、および稼働中一定のタイミングで行い、異常が検出されると、自動的に修復を開始してすばやく復元を試みます。

ウイルス感染による情報漏洩･システムの破壊やウイルスの拡散

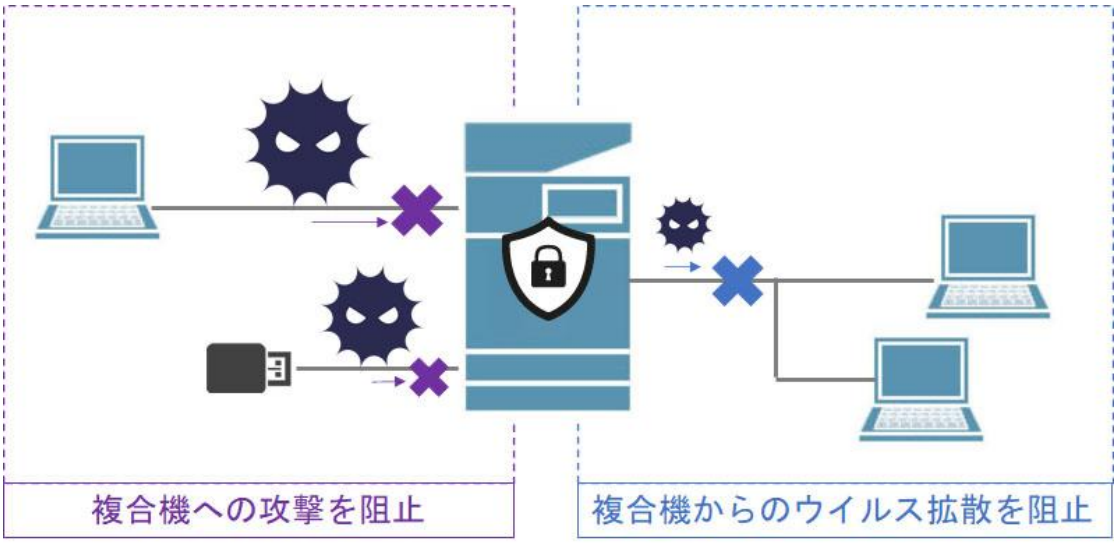
➤脅威

近年では、デジタル複合機を踏み台にした、オフィスのネットワークに接続する他のデバイスへの攻撃も脅威となっています。デジタル複合機でウイルスを動作させるには高度な専門知識が必要となるため、ウイルスの開発は困難であると考えられますが、万一ファームウェアがウイルスに感染することにより、本来の動作に支障をきたしたり、情報漏洩や他のデバイスへの攻撃につながる動作を引き起こすことも想定されます。

➤対策

ウイルス検知キット

パソコンや USB メモリーからのデジタル複合機への入力データ、デジタル複合機から送信されるデータに対してウイルス検知を行います。 また、デジタル複合機の NAS 機能に使用されるストレージに対してもウイルス検知を行うことで、デジタル複合機には直接感染しないがパソコンへ感染するウイルスについて検知・削除を行い、ウイルスの拡散を防止します。



使用状況の把握、および情報漏洩の心理的な抑止対策

デジタル複合機から情報漏洩を防ぐには、常にデジタル複合機の使用状況を把握しておくことが必要です。また、使用状況を把握していることを周知させることにより、情報漏洩に対する心理的な抑止対策効果が期待できます。

➤対策

ジョブログ管理機能により、誰がいつ何の作業を行なったか、どこへ送信したのか把握できます。

デジタル複合機本体には、完了したジョブの履歴を最大 6 万件まで保存することができます。また、保存されたログは、外部のパソコンに取り出して一覧することができます。

また、監査ログ生成機能により、システムやセキュリティに関する設定の変更等、さらに詳細な作業の記録が確認できます。監査ログは SIEM(Security Information and Event Management)システムなどの外部サーバーへも送信することができ、他の IT 機器との統合管理も可能です。

(注)監査ログを外部に送信する場合、送信先となる監査ログサーバーはお客様でご用意いただく必要があります。また、監査ログサーバーは syslog プロトコルをサポートする必要があります。外部監査ログサーバーへ送信時、監査ログをデジタル複合機内部に保存することはできません。

機種別搭載セキュリティ機能

機種別の搭載セキュリティ機能一覧については、以下の弊社 Web サイトをご覧ください。

https://jp.sharp/business/print/solution/security/state3-9.html

※本表は 2023 年 12 月現在の状況です。

表の見方:

○…標準で対応しているセキュリティ機能です。
△…オプションで対応しているセキュリティ機能です。
×…対応しておりません。
－…該当機種では脅威として想定されません。
ネットワーク接続、暗号化 PDF ファイルのダイレクトプリント、およびイメージ送信にはオプションの装着が必要となる機種があります。

デジタルフルカラー複合機

対策機能	BP-20C25 DX-20C20	BP-40C26 BP-60C26 BP-40C36 BP-60C31 BP-50C45 BP-60C36 BP-50C55 BP-70C26 BP-50C65 BP-70C45 BP-70C55 BP-70C65	MX-8081
コモンクライテリア(CC)認証	×	△ (HCD PP v1.0 適合)	△ (HCD PP v1.0 適合)
■本体メモリ装置の持ち出しによる情報漏洩への対策			
保存されたデータの暗号化	×	○	○
ジョブ完了後の実データ消去	×	○*2	○*2
全データ消去	×	△*2	△*2
■ネットワークからの不正アクセスによる情報漏洩への対策			
ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○
ネットワークポートの有効/無効設定/ポート番号の変更	○	○	○
特定発信元からの受信拒否設定	○	○	○
IEEE 802.1X	×	○	○
ドキュメントファイリングのパスワード保護	—	○	○
侵入/攻撃検知	×	○	○
■悪意のあるプログラムからの不正アクセスによる情報漏洩への対策			
強制アクセス制御	×	○	○
■撤去・廃棄された複合機のメモリ装置からの情報漏洩への対策			
個人情報及び本体内データの初期化機能	○	○	○*2
■ネットワーク入出力データへの不正アクセスによる情報漏洩や改竄への対策			
SSL/TLS 暗号化通信	○	○	○
暗号化 PDF ファイル対応（送信/ダイレクトプリント）	×	○	○
IPsec	○	○	○
SNMPv3	○	○	○
スキャンデータの S/MIME 暗号化送信と電子署名	×	○	○
■誤送信による情報漏洩への対策			
送信者名の選択禁止	×	○	○
宛先直接入力禁止	×	○	○
再送信キーの利用禁止	×	○	○
宛先確認	○	○	○
FASEC 1 準拠	○	○	○
■出力した紙文書の持ち去りによる文書データの漏洩への対策			
リテンション（親展プリント）	○	○	○
プリントリリース	×	○	○
ファクス受信データホールド	○	○	○

■不正コピーによる文書データの漏洩への対策			
ドキュメントコントロール	×	△	△
■権限の無いユーザーの使用による可用性の低下やデータの漏洩への対策			
ユーザー認証/操作権限設定	○	○	○
Active Directory 連携	×	○[*1]	○[*1]
■ウイルス感染による情報漏洩・システムの破壊やウイルスの拡散			
ウイルス検知	×	△	×
■BIOS・ファームウェアの改竄・破損によるセキュリティ機能の喪失への対策			
起動時の BIOS 完全性チェック	×	○	×
ファームウェアの自動修復	×	○	○
■使用状況の把握、および情報漏洩の心理的な抑止対策			
ジョブログ管理	×	○	○
監査ログ生成・管理	×	○	○

*1 セキュリティおよび省エネルギー設定のグループポリシーの適用にも対応しています。
*2 消去方式の設定はできません。

デジタル複合機(モノクロ複合機)

対策機能	BP-30M28 BP-30M31 BP-30M35 BP-30M31L	BP-70M45 BP-70M55 BP-70M65	BP-70M75 BP-70M90	MX-M1056 MX-M1206
コモンクライテリア(CC)認証	×	△ (HCD PP v1.0 適合)	△ (HCD PP v1.0 適合)	×
■本体メモリ装置の持ち出しによる情報漏洩への対策				
保存されたデータの暗号化	○	○	○	○
ジョブ完了後の実データ消去	○*2	○*2	○*2	○
全データ消去	△*2	△*2	△*2	△
■ネットワークからの不正アクセスによる情報漏洩への対策				
ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○	○
ネットワークポートの有効/無効設定/ポート番号の変更	○	○	○	○
特定発信元からの受信拒否設定	○	○	○	○
IEEE802.1X	○	○	○	○
ドキュメントファイリングのパスワード保護	○	○	○	○
侵入/攻撃検知	○	○	○	○
■悪意のあるプログラムからの不正アクセスによる情報漏洩への対策				
強制アクセス制御	○	○	○	○
■撤去・廃棄された複合機のメモリ装置からの情報漏洩への対策				
個人情報及び本体内データの初期化機能	○	○	○	○
■ネットワーク入出力データへの不正アクセスによる情報漏洩や改竄への対策				
SSL/TLS 暗号化通信	○	○	○	○
暗号化 PDF ファイル対応（送信/ダイレクトプリント）	○	○	○	○
IPsec	○	○	○	○
SNMPv3	○	○	○	○
スキャンデータの S/MIME 暗号化送信と電子署名	○	○	○	○
■誤送信による情報漏洩への対策				
送信者名の選択禁止	○	○	○	○
宛先直接入力禁止	○	○	○	○
再送信キーの利用禁止	○	○	○	○
宛先確認	○	○	○	○
FASEC 1 準拠	○*3	○	○	—
■出力した紙文書の持ち去りによる文書データの漏洩への対策				
リテンション（親展プリント）	○	○	○	○
プリントリリース	○	○	○	○
ファクス受信データホールド	○	○	○	○
■不正コピーによる文書データの漏洩への対策				
ドキュメントコントロール	△*1	△	△	△
■権限の無いユーザーの使用による可用性の低下やデータの漏洩への対策				
ユーザー認証/操作権限設定	○	○	○	○
Active Directory 連携	○	○	○	○
■ウイルス感染による情報漏洩・システムの破壊やウイルスの拡散				
ウイルス検知	×	△	△	×
■BIOS・ファームウェアの改竄・破損によるセキュリティ機能の喪失への対策				
起動時の BIOS 完全性チェック	×	○	○	×
ファームウェアの自動修復	○	○	○	○
■使用状況の把握、および情報漏洩の心理的な抑止対策				
ジョブログ管理	○	○	○	○
監査ログ生成・管理	○	○	○	○

*1 ドキュメントコントロール検知によるジョブ停止のみ対応しています。
*2 消去方式の設定はできません。
*3 BP-30M31L はファクス非搭載のため”－”です。

A4 複合機・プリンター

対策機能	AR-B350W	MX-B455W	MX-C305W MX-C306W
コモンクライテリア(CC)認証	×	△ (HCD PP v1.0 適合)	△ (HCD PP v1.0 適合)
■本体メモリ装置の持ち出しによる情報漏洩への対策			
保存されたデータの暗号化	×	○	○
ジョブ完了後の実データ消去	×	○	○
全データ消去	×	△	△
■ネットワークからの不正アクセスによる情報漏洩への対策			
ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○
ネットワークポートの有効/無効設定/ポート番号の変更	○	○	○
特定発信元からの受信拒否設定	○*1	○	○
IEEE802.1X	×	○	○
ドキュメントファイリングのパスワード保護	—	○	○
■悪意のあるプログラムからの不正アクセスによる情報漏洩への対策			
強制アクセス制御	×	×	○
■撤去・廃棄された複合機のメモリ装置からの情報漏洩への対策			
個人情報及び本体内データの初期化機能	○	○	○
■ネットワーク入出力データへの不正アクセスによる情報漏洩や改竄への対策			
SSL/TLS 暗号化通信	○	○	○
暗号化 PDF ファイル対応（送信/ダイレクトプリント）	○*2	○	○
IPsec	○	○	○
SNMPv3	○	○	○
スキャンデータの S/MIME 暗号化送信と電子署名	×	○	○
■誤送信による情報漏洩への対策			
送信者名の選択禁止	×	○	○
宛先直接入力禁止	×	○	○
再送信キーの利用禁止	×	○	○
宛先確認	○	○	○
FASEC 1 準拠	○	○	○
■出力した紙文書の持ち去りによる文書データの漏洩への対策			
リテンション（親展プリント）	○	○	○
プリントリリース	×	○	○
ファクス受信データホールド	○	○	○
■不正コピーによる文書データの漏洩への対策			
ドキュメントコントロール	×	△	△
■権限の無いユーザーの使用による可用性の低下やデータの漏洩への対策			
ユーザー認証/操作権限設定	○	○	○
Active Directory 連携	×	○	○*3
■BIOS・ファームウェアの改竄・破損によるセキュリティ機能の喪失への対策			
起動時の BIOS 完全性チェック	×	×	×
ファームウェア自動修復	×	×	○
■使用状況の把握、および情報漏洩の心理的な抑止対策			
ジョブログ管理	×	○	○
監査ログ生成・管理	×	○	○

*1 受信拒否のみ対応しています。
*2 パスワードなし暗号化 PDF のダイレクトプリントのみ対応しています。
*3 セキュリティおよび省エネルギー設定のグループポリシーの適用にも対応しています。

お客様ご相談窓口のご案内

修理・使い方・お手入れ・お買い物などのご相談・ご依頼、及び万一、製品による事故が発生した場合は、
お買い上げの販売店または下記窓口にご相談ください。

「よくあるご質問」「メールでのお問い合わせ」などはホームページをご活用ください。 ▶▶▶▶

シャープサポートページ
https://jp.sharp/business/print/support/

修理のご相談など

【カスタマーセンター】シャープマーケティングジャパン株式会社

ナビダイヤル
0570 - 05 - 1001
（一部地区を除く）

受付時間 ●月曜～土曜：9:00～17:40
（日曜、祝日など弊社休日は休ませていただきます）

■IP電話からは…

東日本地区	043-332-9910
西日本地区	06-6794-2909

シャープ株式会社

本　　社 〒590-8522 大阪府堺市堺区匠町1番地
ｽﾏｰﾄﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝ事業本部 〒639-1186 奈良県大和郡山市美濃庄町492番地

シャープホームページ　https://jp.sharp/