富士フイルムビジネスイノベーション デジタル複合機の セキュリティー白書

2023 年 11 月 13 日
Version 2.3

はじめに

デジタル複合機のセキュリティー対策

富士フイルムビジネスイノベーションでは、お客様の情報セキュリティーに関する課題にお応えすべく、商品を開発するにあたり、各種のセキュリティー機能の拡充、暗号アルゴリズムの危殆化対応などを通じて、情報セキュリティー機能の充実と品質の確保に取り組んでいます。

また、 近年、製品のサプライチェーンの弱点を利用して、不正な部品やプログラムを製品に混入するなどの高度なサイバー攻撃が増加しており、製品のライフライクル全体における完全性確保のためのサプライチェーン・セキュリティーにもいち早く取り組んでいます。

さらに、商品のリリース後においても、情報セキュリティーリスクに対する課題が判明した時点で、直ちに対策会議を招集して対応を検討、お客様に不測の事態が起こらないよう努めています。

富士フイルムビジネスイノベーションは、付加価値機能の追求とそのセキュリティー強化のバランスの重要性を強く認識しています。セキュリティーの信頼性を保証すべく、富士フイルムビジネスイノベーションの複合機は、情報技術セキュリティーの設計や運用などの国際標準規格「ISO/IEC15408」や米国の第三者評価機関である Keypoint Intelligence 社の Security Validation Program に合格し、セキュリティー認定（ BLI Security Seal - Device Penetration ）を取得しています。

米国政府機関が定めたセキュリティー基準を示すガイドラインである NIST SP800-171（NIST Special Publication 800-171 rev.1）にも対応しており、2020 年 9 月には、日本初の AAAis（トリプル A）格を取得しました。さらに、2022 年 12 月にはこれまでの「NIST SP800-171」のみならず、「NIST SP800-172」への準拠で求められる対策（特定、防御、検知、対応、復旧の管理策）についても極めて高い水準で織り込んでいることが評価され、国内で初めて「NIST SP800-171/172」の両セキュリティー基準において、最高評価の「AAAis」を取得しました。

また、近年増加する製品のサプライチェーンの弱点を利用したサイバー攻撃に対抗するため、製品のライフサイクル全体を通じた完全性確保のためのプロセスを構築し、サプライチェーン・セキュリティーの国際標準規格「ISO/IEC 20243」の自己評価認証を取得しました。

富士フイルムビジネスイノベーションは、今後も、先端情報技術の商品への活用、適切な品質管理・迅速な対応、ならびに高度な情報セキュリティーサービスの提供を通じて、お客様の情報セキュリティー確保にお役に立てるよう一層努力してまいります。

認証製品の詳細については以下の URL を参照してください。
https://www.fujifilm.com/fb/product/multifunction/promotion/security_measure/isoiec.html

本書に記載されている全ての内容は作成された時点の情報です。富士フイルムビジネスイノベーションでは、今後さらなるサービスの向上を計画しているため、記載内容は変更される場合があります。
また、本書に記載されている機能の対象機種や詳細については、弊社へご確認ください。

組織におけるセキュリティー

法令を遵守し、公正で誠実な事業活動を行うことは、オフィス複合機の生産者として当社が大切にする基本的な価値観の一つです。富士フイルムビジネスイノベーションおよび関連会社では、企業倫理・コンプライアンス体制の構築に取り組んでおり、基本方針を役員および従業員一人ひとりの行動に定着させるよう、体制・仕組みの充実を図っています。

富士フイルムビジネスイノベーションの倫理・コンプライアンスの詳細については以下の URL を参照してください。

https://holdings.fujifilm.com/ja/sustainability/vision/compliance/

富士フイルムビジネスイノベーションは、お客様との信頼関係を構築すると同時に、お客様の立場で考え、理解し、課題を解決するプロフェッショナル集団として、お客様に安心してソリューションサービスをご利用いただけるよう、また情報資産を当社にお預けいただけるよう、情報セキュリティー対策の強化に尽力してきました。富士フイルムビジネスイノベーションおよび関連会社は、第三者評価・認証の取得に取り組んでいます。

弊社の取り組みについて、より詳しくご理解いただくために情報セキュリティー報告書を発行していますので、そちらもご覧ください。

https://www.fujifilm.com/fb/company/public/i_security/

富士フイルムビジネスイノベーションは、引き続き情報セキュリティーガバナンスの強化に取り組んでまいります。

複合機のセキュリティー上の脅威と対策

情報漏えい、データ改ざんおよび情報への不正アクセスの攻撃の観点から、以下の項目がオフィス複合機に対するセキュリティー上の脅威と捉えています。

1. **他の利用者による不正な操作**
2. **通信データの盗聴、改ざん**
3. **管理機能への不正なアクセス**
4. **複合機のソフトウェアの改ざん・破損**
5. **監査ログの改ざん**
6. **複合機内に蓄積された文書データの漏えい**
7. **管理者またはエンドユーザーのうっかりミスによる情報漏えい**

富士フイルムビジネスイノベーションのオフィス複合機は、下記の表 1～7 のように、想定される全てのリスクに対し、最適な対策を提供します。

オフィス複合機のセキュリティー上の脅威と対策

表 1

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
1. 他の利用者による不正な操作 各利用者が複合機を操作するにあたり、取り扱う文書データに適切な保護（データアクセス権、各種操作の制御等）を行うことができなければ、蓄積される文書および文書関連データの漏えい、情報の改ざん等が発生する。	**A) ユーザー認証と権限** ● **ユーザー認証** 利用者個人の識別/管理が可能です。 ● **機能の利用制限** 各ユーザーの使用状況を管理します。 ● **自動ログアウト** ログインした本人以外のユーザーによる複合機の不正な利用を防止します。 ● **セキュリティープリント、プライベートプリント** 機密文書を他者に見られることなく出力できます。 ● **ユーザー認証と利用権限を統合** ApeosWare Management Suite 2 により、ユーザー認証と利用権限の統合を実現します。 ● **一元管理による安全な出力** ApeosWare Management Suite 2 によりユーザー認証後のプリントジョブを安全に出力する環境を提供します。一元管理で安全な出力を実現します。

A)ユーザー認証と権限

認証機能

認証機能を使用することにより、複合機の使用を許されていないユーザーの操作や不正なアクセスを抑止。ジョブ履歴からユーザーごとの利用実績の集計も可能です。

IC カードリーダー

複合機に IC カードリーダーをプラスすることで、IC カードによる認証機能を実現します。出力機器の利用制限をはじめ、さまざまな機能と連動。ドキュメントのセキュリティー管理強化と利便性の向上を両立します。

読み取りフォーマットに応じた IC カードリーダーB、IC カードリーダーD の 2 種類があり、それぞれ本体内蔵型、ウイングテーブル内蔵型、外付け型の 3 タイプをご用意しております。

外部サーバー認証

IC カードの情報を Active Directory や LDAP [注1] サーバーに属性情報として登録することで、サーバーが管理するユーザー情報を、複合機やプリンターの利用時のユーザー認証に活用することができます。万が一 IC カードを忘れた場合は、ユーザーID とパスワードの入力で利用可能。ネットワーク上の多様なリソースを Active Directory で管理するお客様においては、出力機器も同様に一元管理が行え、管理の手間を軽減します。また、Azure Active Directory 認証にも対応しています。

注 1：Lightweight Directory Access Protocol

機能の利用制限

ユーザー認証による利用制限機能により、利用可能な複合機の機能を制限できます。コピー、ファクスを含む全ての機能ボタンが制御されます。管理者による操作パネルや複合機のソフトウェアからの設定が可能です。

以下の 3 種類の利用制限があります。

1. 機器の利用制限

   操作パネルの操作が制限されます。複合機が起動すると、最初にログイン画面が表示されます。

2. サービスの利用制限

   以下のサービスが制限されます。これらのアイコンを非表示にすることも可能です。

   - コピー
   - ファクス/インターネットファクス
   - スキャナー(ボックス保存)
   - スキャナー(PC 保存)
   - スキャナー(メール送信)
   - ボックス操作
   - ジョブフロー
   - 文書プリント
   - デジカメプリント
   - 外部アクセス
   - プリンター

3. ユーザーごとの利用制限

   機能の利用およびプリント・コピーの上限枚数をユーザーごとに制限できます。

   プリント・コピーの上限枚数は、管理者が操作パネルや複合機のソフトウェアから設定します。

   プリントやコピー枚数が登録されている上限枚数を超えた場合、以降そのユーザーは該当機能を利用できません。利用可能にするためには、管理者がカウント数をクリアする必要があります。

利用制限・管理設定の例		ユーザーの利用制限条件			
		コピー	プリント	スキャン	FAX／インターネットFAX
システム担当	フルカラー	×	×	○	○
	モノクロ	○	○	○	
一般社員	フルカラー	×	×	×	×
	モノクロ	○	○		
カラー資料作成社員	フルカラー	○	○	○	○
	モノクロ	○	○		
グループ A	フルカラー	○	○	○	○
	モノクロ	○	○	○	

ボックス内文書へのアクセス制御

スキャン文書やファクス文書を保存するボックスには、パスワードを設定することができます。パスワードを設定することで、文書データを保護することができます。また、ユーザーを識別する認証モードにすれば、他のユーザーによる文書データへのアクセスを抑制できます。

自動ログアウト

ログインした本人以外のユーザーによる複合機の不正な利用を防止します。複合機が一定の時間利用されない場合、自動的にログアウトし初期状態に戻ります。

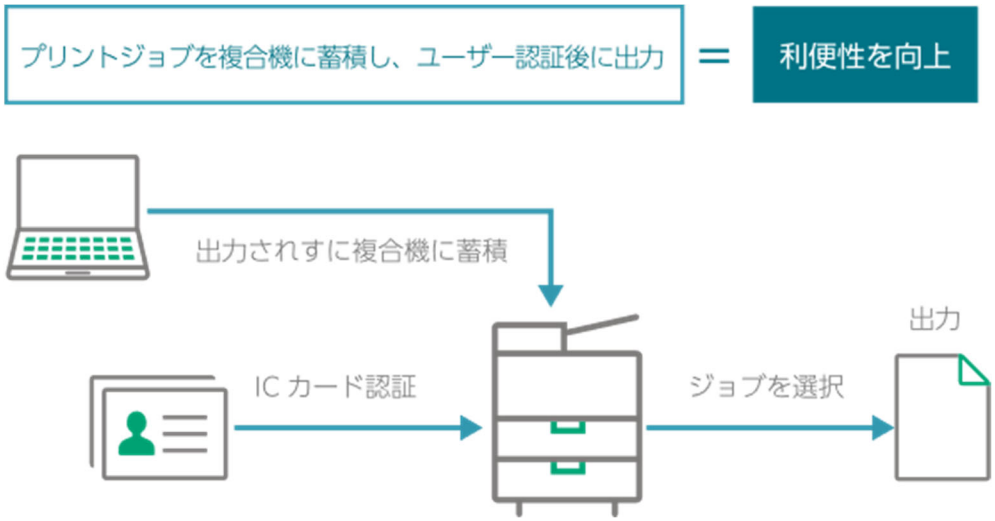
セキュリティープリント

第三者に見られたくない文書、機密書類などを出力する場合に出力データを本体内に一時蓄積し、パスワード入力で出力を開始させることができます。

無償のツールである Print Driver Customization Tool を使うことで、プリンタードライバーの設定をセキュリティープリントに固定することも可能です。

プライベートプリント

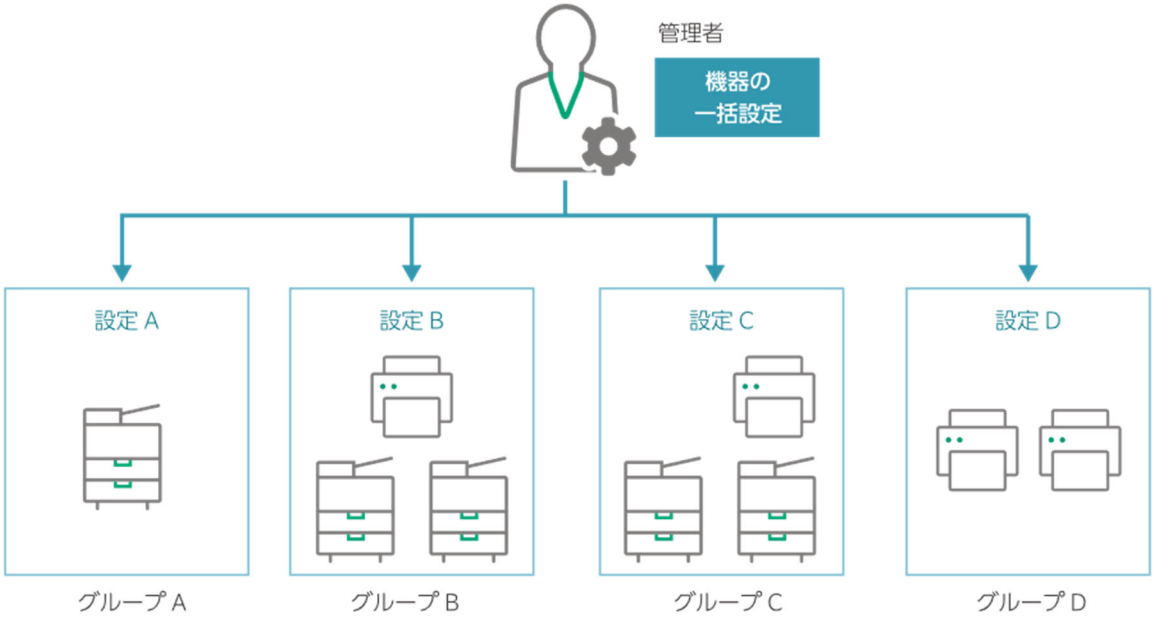
プリントジョブを強制的に複合機の記憶装置に蓄積、認証後に出力します。これにより放置プリントやミスプリントを抑止できます。さらに出力の際、部数や両面/片面、カラーモードを白黒にするなど、印刷設定の変更も可能なため、ミスやムダを抑え、TCO 削減に貢献します。



注記：認証モードでの運用が必要。

ユーザー認証/利用権限の統合

サーバーベースの機器管理ソフトウェア ApeosWare Management Suite 2 により、認証に必要なユーザー情報を複数の機器に対して一元管理することができます。管理者による煩雑な作業を省いたユーザー認証と利用権限の統合を実現します。



一元管理による安全な出力

ApeosWare Management Suite 2、ユーザー認証後のプリントジョブを安全に出力する環境を提供します。本機能により放置プリントやミスプリントを防止。サーバーで情報が一元管理されているため、管理者は複数の機器の設定を一括管理できます。

オフィス複合機のセキュリティー上の脅威と対策

表 2

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
2. 通信データの盗聴、改ざん 複合機を利用（プリント、スキャン等）するために使用する PC やファイルサーバーと複合機の間でやりとりされるネットワーク上の通信データが盗聴、改ざんされる可能性がある。	**B）通信データの保護** ● **SSL/TLS および IPSec** PC やファイルサーバーと複合機の間の通信を暗号化し情報を保護します。 ● **SMBv3、SFTP** PC やファイルサーバーと複合機の間の通信を暗号化し情報を保護します。 ● **FIPS 140** FIPS 140-2 認定モードを有効にすることで米国連邦基準規格に準拠したモジュールで動作します。 ● **電子証明書の検証** 証明書チェーン、証明書の失効および有効期間を検証します。 管理者が手作業で行っていた証明書更新(新規発行含む)と、それに付随する設定更新処理を自動化可能です。 ● **プロトコル毎、ポート毎の使用禁止の設定** 不正なアクセスや情報漏洩を防止します。 ● **スキャン文書の暗号化** パスワードや公開鍵により情報漏えいを防止します。 ● **暗号化文書のダイレクトプリント** 暗号化された DocuWorks ファイルや PDF ファイルを復号して直接出力できます。 ● **メール暗号とメール署名** メール配信中の盗聴や改ざんのリスクを低減します。 ● **異なるインターフェイス間での情報漏えいの防止** ファクス回線、セカンダリーイーサネット、無線 LAN、USB ポートなどからの複合機や内部ネットワークへの攻撃、および、USB メモリー内不正プログラムによる攻撃を抑止します。

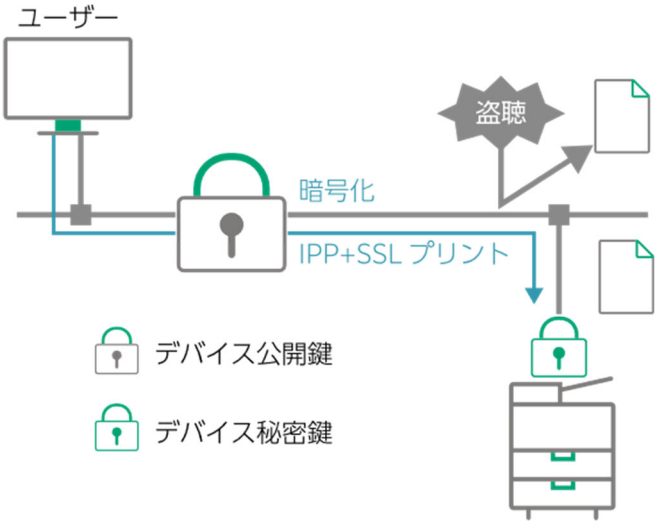
B) 通信データの保護

サーバーやクライアント PC と複合機との通信を暗号化（SSL/TLS、IPSec）

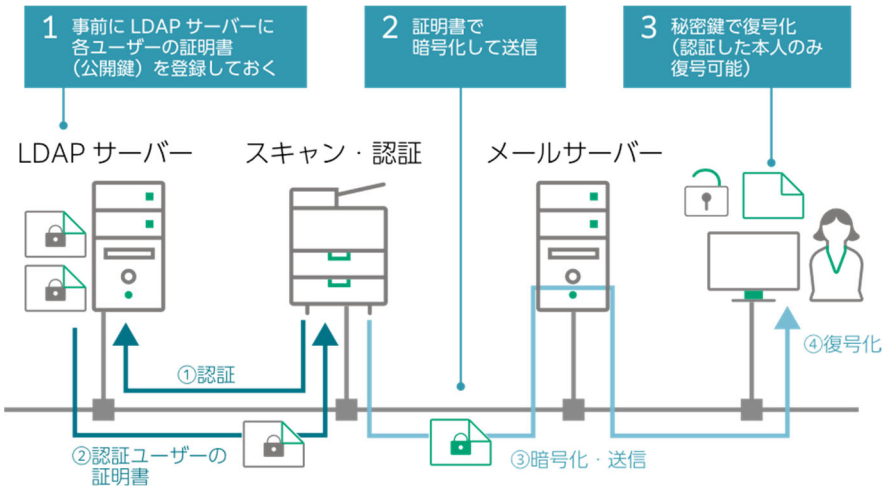
複合機とネットワーク上にあるサーバーやクライアントのコンピューターとの通信を暗号化すると、仮にネットワーク上で不正アクセスしようとしても、経路が暗号化されているため、情報漏えい・改ざんを抑止できます。以下の通信の暗号化が可能です。標準では TLS1.2 のみが有効*ですが設定変更により TLS1.3 への対応も可能です。

* TLS1.0/TLS1.1/TLS1.3 は標準では無効化されています。

- IPP ポートを利用したプリントジョブ（プリント）
  プリントデータのやりとりに利用される IPP(Internet Printing Protocol)の通信経路を暗号化して認証情報や印刷データが盗聴されるのを防止します。



- HTTP による安全な通信
  PC から複合機のインターネットサービスにアクセスするとき、または複合機から外部サーバーへアクセスするときに HTTP による通信を安全に行います。
- LDAP サーバーとの通信（アドレス帳検索・認証）
  LDAP サーバーとの通信経路を暗号化して、認証情報やアドレス帳データが盗聴されるのを防止します。



- SMTP サーバーとの通信（メール）
  SMTP(メール送信)サーバーとの通信経路を暗号化して、認証情報やメールのデータが盗聴されるのを防止します。
- POP サーバーとの通信（メール）
  POP(メール受信)サーバーとの通信経路を暗号化して、認証情報やメールのデータが盗聴されるのを防止します。
- SFTP による通信(スキャン/ファイル転送)
  ジョブフローの FTP 転送でデータをサーバーに転送する際、セキュアシェル方式で通信経路の暗号化・認証を行い、認証情報やデータが盗聴されるのを防止します。
- SMB による通信（スキャン/ファイル転送）
  SMBv3 では通信の暗号化機能が新規に追加されており、ファイル送信先に安全にファイル送信することが可能です。
- IPsec による IP 通信の暗号化
  IPsec での接続設定をした機器の間で IP パケット単位で改ざんや盗聴を防止することが可能です。

証明書を利用したクライアント通信では、SSL サーバー認証や IPSec の PKI 認証により、なりすましを防止します。

- IEEE802.1X 認証によるネットワーク機器の認証
  ネットワークで機器同士が接続する際、機器のネットワークへの接続規制を行う認証規格である IEEE802.1X 認証に対応していますので、接続機器の制限をかけたネットワークにも安全に複合機を接続することが可能です。

FIPS 140 準拠

FIPS 140 (Federal Information Processing Standard 140) とは、暗号モジュールに関するセキュリティー要件の仕様を規定する米国連邦標準規格です。FIPS140-2 認定モードを［有効］に設定することによって FIPS 140 に準拠したモジュールで動作します。

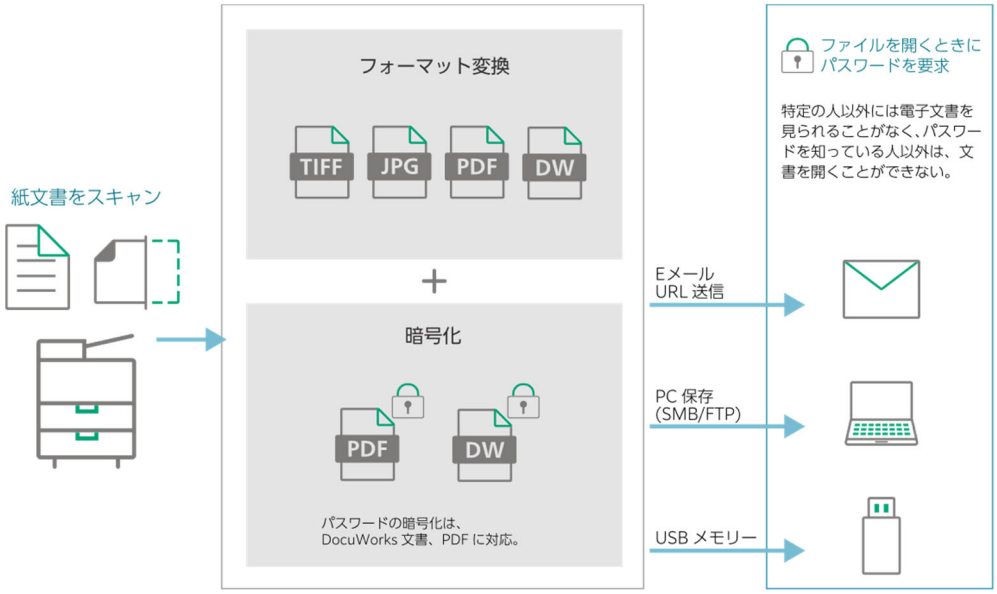
電子証明書の検証

証明書チェーン、証明書の失効および有効期間などの確認により、通信に使用する証明書を検証する機能です。トラストアンカー制御により、証明書の確実な検証/管理を行います。

Windows Server の Network Device Enrollment Service(NDES)による証明書自動配布機能に対応しており、SCEP(Simple Certificate Enrollment Protocol)を用いてこれまで管理者が手作業で行っていた証明書更新(新規発行含む)と、それに付随する設定更新処理を自動化可能です。

スキャン文書のパスワード暗号化

スキャン文書を PC に保存したり、メールで送信したりする際、 DocuWorks 文書と PDF へのフォーマット変換では、パスワードによる「ファイル暗号化」を複合機本体で設定できます。ファイルを開くためのパスワード設定はもちろん、印刷や編集の制限などアプリケーションソフトのセキュリティー機能にも対応。スキャン文書からの情報漏えいや改ざんのリスクを軽減します。



注記：暗号化された DocuWorks 文書および PDF を開くには、DocuWorks Viewer Light または Acrobat® Reader® / Adobe® Reader®が必要です。ただし、古いバージョンでは文書が開かない場合がありますので、最新の DocuWorks Viewer Light、Acrobat® Reader®をご利用ください。

スキャン文書の署名・PKI 暗号化

証明書と秘密鍵を複合機にインポートすることで、スキャン文書（DocuWorks/PDF/XPS）に電子署名をつけることが可能になり、第三者による改ざんを検知できます。DocuWorks 文書であれば PKI 暗号化もできるので、パスワード暗号化よりもセキュリティーを高め、特定の人のみが開ける文書を生成することが可能です。

注記：ApeosPort、Apeos のみ対応しています。

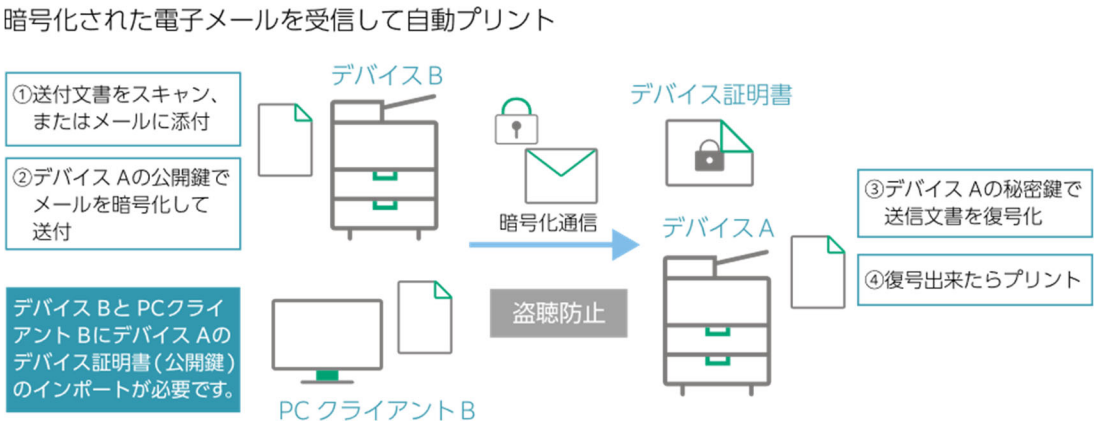
暗号化文書のダイレクトプリント

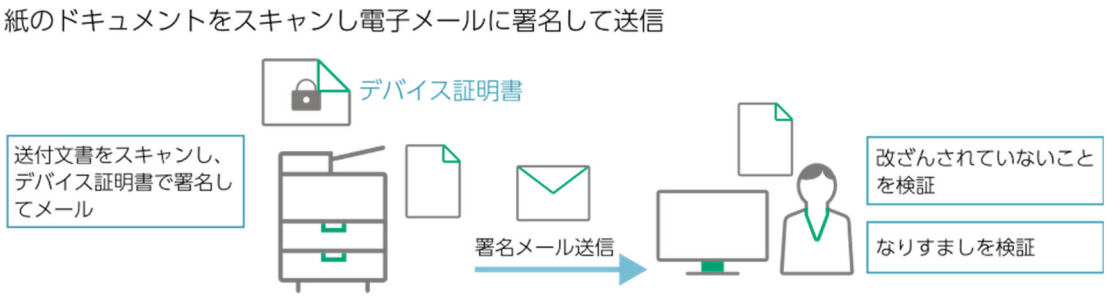
予め複合機に登録してあるパスワードを使って、USB メモリー、Working Folder などに格納されている暗号化された DocuWorks ファイルや PDF ファイルを復号化して直接出力ができます。また、Contents Bridge ユーティリティを使って DocuWorks ファイルや PDF ファイルをパスワードと同時に送信する方法にも対応しています

メール暗号とメール署名

メール暗号(S/MIME)：メール(添付文書含む)をユーザーの電子証明書で暗号化し、該当ユーザーにしか開けないようにします。メール配信中の盗聴による情報漏えいのリスクを低減できます。

メール署名(S/MIME)：メール(添付文書含む)を複合機の電子証明書で署名をつけて送信します。メール配信中の改ざんのリスクを低減し、差出人を客観的に証明できるため、受信者は安心して利用することができます。



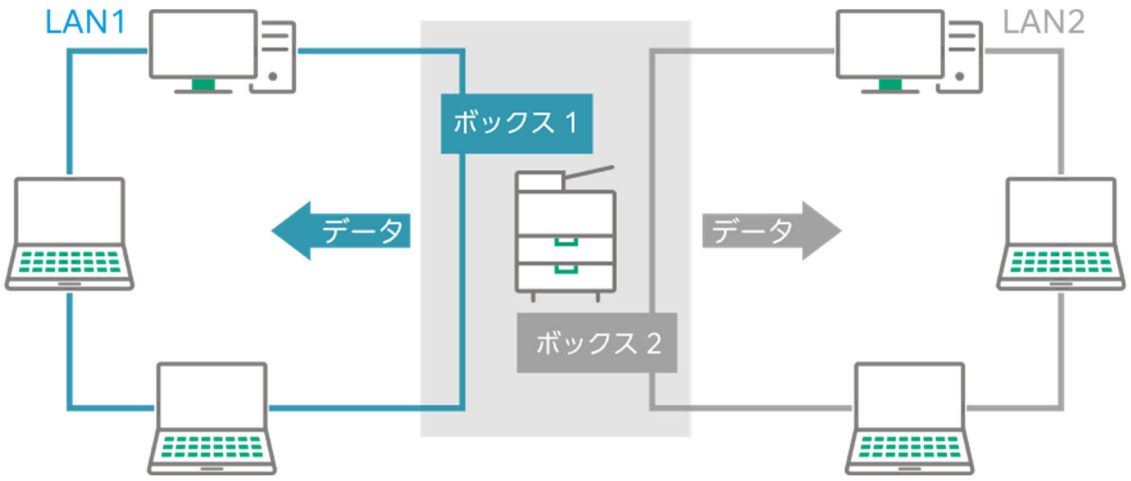


ファクス回線からの攻撃、傍受、情報漏えい防止

ファクス回線（電話網）からのアクセスは、ファクスのプロトコル制御による通信しか受け付けませんので、ウィルスの混入により複合機の動作が影響を受ける、または不正コマンドが実行されるということはありません。受信したデータは、全てファクスの画像/原稿（画情報）として扱いますので、規格に合わない疑わしいデータの場合、デコードエラー等の画像情報エラーとして処理します。

セカンダリーイーサネットからの攻撃、傍受、情報漏えい防止

セカンダリーイーサネット（オプション）と、プライマリーイーサネット（標準）は、各々独立して通信（TCP/IP）を行います。つまり、複合機は各ネットワークインターフェースに対して、通信(TCP/IP）のルーティングを行うことはありません。このように、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へアクセスできない仕様になっています。
ボックスは、ネットワークアクセス制限が可能です。ネットワークからのボックスに対する表示/文書蓄積/文書転送は、ボックス毎にプライマリーイーサネットまたはセカンダリーイーサネットのいずれかに制限することが可能です。これにより、他方のネットワークからの不正アクセスによる、ボックス内文書の漏洩はありません。なお、ボックスのパスワード管理が必要になります。



セカンダリーイーサネットで利用できるスキャナー機能は、「ボックス保存」でインターネットサービスによる文書取り出し、ボックスから始まるジョブフロー(SMB転送)、AirPrintスキャンです。ボックスを利用する機能については、ネットワークアクセス制限により保護されます。AirPrintスキャンについては、セカンダリーイーサネットからスキャン指示を受けた場合のみ、セカンダリーイーサネット側へ送信します。
従って、セカンダリーイーサネットを不正に利用して情報を漏えいさせることはできません。

無線 LAN(Wi-Fi)ポートからの攻撃、傍受、情報漏えい防止

オプションの無線 LAN コンバーターは、有線 LAN ケーブルにて接続、無線 LAN キット、無線キット、無線キット 2 は、複合機に取り付けて、無線 LAN 通信を行なう無線端末です。

これらの無線端末は、WPA/WPA2 に存在する「KRACKs 脆弱性」に対応しています。
無線キット 2 は、2018 年 6 月に Wi-Fi アライアンスにて策定された WPA3-SAE にも対応しており、より安心してお使い頂けます。

また、これらの無線端末は、ルーティング機能を持っていませんので、各ネットワークインターフェース間通信(TCP/IP)のルーティングを行うことはありません。

ボックスのアクセスと不正アクセスの対応は、セカンダリーイーサネットと同じです。従って、これらの無線端末を不正に利用して情報を漏えいさせることはできません。

USB ポートからの攻撃、傍受、情報漏えい防止

USB ポート経由でのプリントジョブにおいて、データはプリントジョブ言語および画像データとして扱います。仮にプリントジョブ言語および画像データ以外のデータを受信した場合、ジョブエラーとなりジョブを中止します。
また、USB ポートからネットワーク、ファクス回線等の通信回線への中継機能は実装していません。

USB メモリー上のウィルス感染ファイルによる攻撃、傍受、情報漏えい防止

下記の理由から、USB メモリーを利用したスキャンジョブ、プリントジョブでは複合機、および複合機に接続されたネットワーク上の PC 等はウィルス感染しません。

- ✓ スキャンジョブでは USB メモリー内のファイルにはアクセスしません。
  そのため USB メモリー内のファイルがウィルス感染していても複合機はウィルスに感染しません。
- ✓ プリントジョブでは USB メモリー内のファイルを画像データとして扱います。
  仮にファイルがウィルス感染していた場合でも、画像データの形式と異なる場合には、画像処理エラーとしてジョブを中止します。不正プログラムを自動実行することはありません。
- ✓ 上記のように複合機がウィルス感染しないために、複合機が踏み台となってネットワーク上の PC 等にウィルス感染することはありません。
- ✓ USB メモリーから直接ネットワーク上の PC 等に通信する手段は実装していません

オフィス複合機のセキュリティー上の脅威と対策

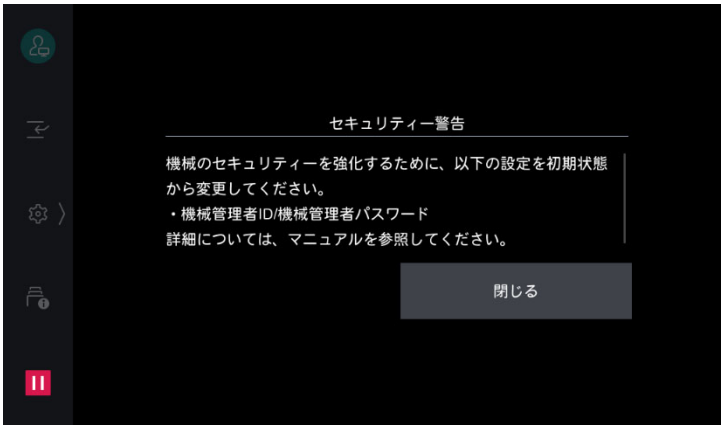
表 3

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
3. **管理機能への不正なアクセス** 取り扱う文書データに対する設定された規則（セキュリティーポリシー）や複合機の利用者情報を管理する機能等に対して、操作できる者を適切に識別認証できない場合には、不正に操作される可能性がある。	**C) 管理機能の保護** ● **管理者パスワード** 初期値のまま運用されている場合、警告表示により、パスワード変更を促します。 ● **アカウントロック** 管理者にてログインを連続して失敗した場合に実施します。 ● **カストマーエンジニア操作制限機能** カストマーエンジニアのなりすましによる複合機の設定変更などの攻撃を防止します。 ● **ユーザープロファイルの一元管理** ApeosWare Management Suite 2 により、。部門組織や機器の設置場所に基づく利用制限の設定を実現します。

C) 管理機能の保護

管理者 ID/パスワードが初期値の場合に表示される警告メッセージ

複合機をより安全にご利用いただくために、管理者 ID やパスワードが初期値のままの状態で管理者モードに入ると、メニュー画面にセキュリティー警告が表示されパスワードの変更を促します。



管理者ログイン連続失敗時の認証ロック

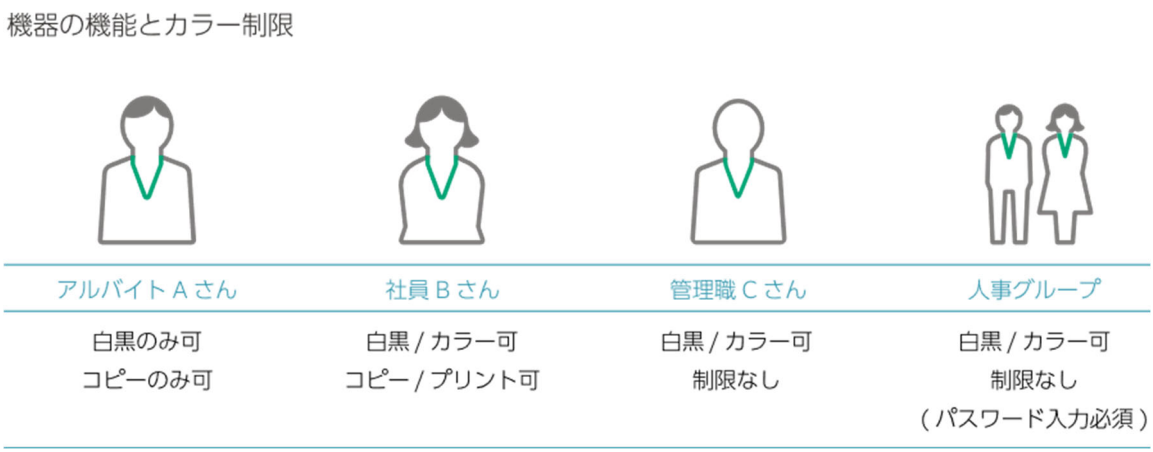
管理者としてログインする際に、所定回数認証に失敗した場合、複合機を再起動するまで管理者としてログインができなくなります。

カストマーエンジニア操作制限

管理者による設定で、特別な権限をもつカストマーエンジニアの操作を制限できます。カストマーエンジニアになりすまして複合機にアクセスされることを防ぐために、カストマーエンジニアモードに入る際にパスワードを設定することができます。

部門組織・設置場所でユーザー権限を一元管理

ApeosWare Management Suite 2 により、ユーザープロファイルを統合した権限の一元管理が可能となり、その権限を部門組織のユーザーグループ単位または設置先の機器グループ単位に適用することができます。さらに、ユーザープロファイルを使用し、セキュリティーレベルや ApeosWare Management Suite 2 の利用可能なサービスに応じた利用制限を設定することも可能です。



オフィス複合機のセキュリティー上の脅威と対策

表４

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
4. **複合機のソフトウェアの改ざん・破損** 複合機のソフトウェアが改ざん・破損された場合、設定されたセキュリティーポリシーが適切に実施されない可能性がある。 製品のアップデートプログラムが正規のものであるかを検証する仕組みがない場合には、不正なソフトウェアやシステムファイルがアップロードされ、暗号化機能が無効にされる、または不正なアプリケーションがインストールされる可能性がある。	**D) 複合機ソフトウェアの完全性を確保** ● **脆弱性検知とソフトウェアアップデート** 定期的に実施しています。 ● **ソフトウェア更新時の完全性確保** 不正なコントローラーソフトウェアや追加型アプリケーションが複合機にインストールされるのを防止します。 ● **起動時の完全性の確保** 起動時に不正なコントローラーソフトウェアの実行を防止します。 ● **稼働時の完全性確保** ホワイトリストに基づいてコントローラーの動作を監視し、不正な動作を防止します。

D) 複合機ソフトウェアの完全性を確保

脆弱性検知とソフトウェア更新の定期実施

複合機の開発時に脆弱性検査ツールにより、複合機に対する攻撃可能性への対応を定期的に行っており、必要な対策はコントローラーソフトウェアのアップデートとして提供しています。富士フイルムビジネスイノベーションでは、新商品の開発中に複数の脆弱性ツールを使用して検査を実施しています。万が一脆弱性が検出された場合には、プログラムの修正やセキュリティーパッチの適用等の対策を実施しています。脆弱性検査ツールに関しては、脆弱性情報・データベースが毎日更新されるため、常に最新の状態で検査しています。既存商品についても定期的に同様の検査/対応を実施し、必要に応じてソフトウェアを更新しています。 また、SSH 等リモートから操作可能な機能は提供しておらず、外部からの不正な操作を防止しています。

ソフトウェア更新時の完全性の確保

コントローラーソフトウェアや複合機追加型アプリケーションを更新する際には、電子署名検証機能により、悪意のある第三者が作成した不正なソフトウェアに書き換えされることを防止します。改ざんを検知した場合は、複合機を起動せずに監査ログにそのイベントを記録します。

セキュリティーレベルの強化として、ネットワーク越しの不正なソフトウェア更新を防止するため、ネットワークからの更新機能を停止することが可能です。

なお、ファクス回線からソフトウェアを更新することはできません。

起動時の完全性確保(セキュアブート機能による起動時改ざん検知機能)

複合機の起動時にコントローラーソフトウェアの電子署名の検証を行い、改ざんを検知した場合、ゴールデンマスターから自動復旧します（レジリエンス）。

信頼の起点に書換え不可能なハードウェアを使用することでより強固なセキュリティーを実現（HW Root Of Trust）します。

稼働時の完全性確保(ホワイトリストによる稼働時改ざん防止機能)

正当なアプリケーションを保護し、不審なアプリケーションが実行されないよう、ホワイトリストに基づいてコントローラーの動作を監視し、不正な動作を防止します。

また、IP アドレス制限機能を使用したネットワーク通信先制御により、予期せぬアクセスを遮断することもできます。

オフィス複合機のセキュリティー上の脅威と対策

表 5

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
5. **監査ログの改ざん・不正な削除** 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。	**E) 監査ログとそれの保護、その他のログ関連機能** ● **監査ログ** 複合機の停止/起動、設定変更やジョブの実行状況を記録する機能により、履歴の追跡が可能です。 ● **監査ログの保護** 権限を持たない人による監査ログの閲覧・編集・削除を禁止することが可能です。 ● **監査ログの SIEM 連携** 複合機の監査ログを Syslog プロトコルを利用して SIEM 製品と連携させることで監査ログの一元管理や分析が可能になります。 ● **ジョブ情報の表示制限** ジョブ実行結果を示すジョブログの記録を他のユーザーに見せない設定も可能です。 ● **文書固有の識別子「UUID」印字** 情報漏えいが発生した際に特定のユーザーを追跡することが可能です。 ● **実行ジョブのトレーサビリティー** ApeosWare Management Suite 2 や ApeosWiz Image Log により、実行ジョブのトレーサビリティーを一元化。

E) 監査ログとそれの保護、その他のログ関連機能

監査ログ

インターネットサービスから、Web ブラウザー経由で「監査ログ」をダウンロードできます。システムデータの変更や、認証の有無、電源の ON/OFF といった詳細な履歴が収集でき、管理強化に役立つともに、ユーザーのセキュリティー意識向上に向けたデータとして活用できます。

監査ログには以下の項目に関連する操作が記録されます。

- 状態変化：デバイスの電源 ON/OFF、ユーザーの操作開始、終了等
- ログイン状態：ユーザーログイン、ログアウト、管理者の認証ロック等
- ジョブの状態：ジョブ終了等
- 設定変更：時刻設定、セキュリティー設定変更、ユーザー情報設定、ボックス開設等
- データ変更：証明書変更、アドレス帳変更等
- 構成変更：ストレージ交換、ROM バージョン変更等
- 通信結果：信頼性通信エラー等

監査ログの保護

その使用目的から、第三者による監査ログの閲覧・編集・削除を不可能にする必要があります。監査ログ保護のために以下の対策を実施しています。

- 監査ログを編集・削除するためのインターフェイスはありません。
- 管理者だけが監査ログにアクセスできます。ダウンロードには SSL/TLS で暗号化した通信が必要です。
- ストレージの交換や複合機からの取り出しがあった場合でも、監査ログ情報はストレージ蓄積データ暗号化機能により保護されます。

監査ログの SIEM 連携

複合機の監査ログを Syslog [*1] プロトコルを利用して外部に転送する機能を利用し、SIEM [*2] 製品と連携させることで、複合機の監査ログを一元管理・分析することが可能になり、セキュリティー上の脅威となる事象の早期検知・分析をサポートします。

*1：Syslog とは、IP ネットワークを通じて時系列の記録（ログ）を伝送する標準プロトコル。

*2：SIEM（=Security Information and Event Management）とは、機器やソフトウェアの動作状況の記録（ログ）を一元的に蓄積・管理し、セキュリティー上の脅威となる事象をいち早く検知・分析するセキュリティーソフト/サービス。

ジョブ情報の表示制限

認証していないユーザーが、実行中ジョブ、実行待ちジョブ、終了ジョブなどの情報を見られなくするなど、ジョブに関する表示の制限が可能です。

また認証しているユーザーも自分のジョブのみ表示し、他人のジョブを見られなくするなど、表示する情報を制限できます。これによりプライバシーを保護し、情報漏えいを抑止します。

ジョブログ識別子 UUID 印字

コピーやプリント、ファクスの出力文書に、文書固有の識別子「UUID」を印字します。これにより文書の検索・特定に対応。「いつ」「誰が」「どのような処理をしたか」を確認でき、万一の情報漏えい時のユーザー特定に役立ちます。

実行ジョブのトレーサビリティーを確保

ApeosWare Management Suite 2 により実行したジョブのログ情報の収集が可能です。管理者は作成されたレポートから、ジョブの履歴を追跡できます。

サーバーソフトウェアである ApeosWiz Image Log では、イメージログという実行ジョブの文書を画像データとユーザー情報と共に保存する機能や実行ジョブの UUID 機能を使用すれば、ジョブの画像データでも追跡ができます。ApeosWiz Image Log による画像データの監視ができますので、設定されたセキュリティー基準に反した場合、自動的に管理者に警告することで情報漏えいを防止します。

オフィス複合機のセキュリティー上の脅威と対策

表 6

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
6. **複合機内に蓄積された文書データの漏えい** プリントやコピー、ファクス機能で扱われる文書データは、複合機のストレージに一時的又は継続的に保存される場合があり、リース終了返却、又は廃棄処理となった複合機から、それらの文書データが漏えいする可能性がある。これらの文書データは暗号化または物理的に消去されていない場合、表面的にはアクセスできないようになっていても復元される可能性がある。	**F) 複合機内に蓄積された文書データの保護** ● **ストレージ内に蓄積したデータの暗号化** 複合機から取り出されたストレージの第三者による解析を防止します。 ● **HDD 内に蓄積したデータの上書き消去** HDD 内に一時的に蓄積されるデータの上書き消去によりジョブ内容の漏えいを抑止します。 ● **複合機内データの一括削除** 複合機を他の組織で再利用する場合、また廃棄する場合に、複合機内の情報が漏えいしないように設定情報および文書情報を一括して消去することができます。

F) 複合機内に蓄積された文書データの保護

ストレージ*1 蓄積データの暗号化

ストレージへのデータ書き込み時に非常に強固な方式*2 で暗号化することにより、保存データへの不正なアクセスなどを防ぎます。また、複合機の搬出時にもデータが第三者によって解析されるのを防ぎます。

暗号鍵自体は不揮発性メモリーに保存されることはなく、複合機が起動するたびに生成され、利用されます。そのため、万が一不揮発性メモリーが取り出されたとしても暗号鍵は流出しません。
また、一部機種ではストレージ内に蓄積されるデータの暗号化に使われる暗号鍵は、ストレージとは独立したセキュリティーチップ(TPM: Trusted Platform Module)内部のルート暗号鍵によって更に暗号化されます。ルート暗号鍵は TPM の耐タンパー性により外部から読み取られることなく安全に保護されます。

*1 HDD および SSD

*2 AES-256

各機種に対する暗号化強化の詳細については以下のサイトからセキュリティーターゲットを参照してください。

https://www.fujifilm.com/fb/product/multifunction/promotion/security_measure/isoiec.html

HDD 内に蓄積したデータの上書き消去

HDDに一時的に蓄積されるデータの上書き消去*により、コピー、ファクス、スキャン、プリントといったジョブ内容の漏えいを抑止します。オプションの「データ上書き消去キット」が必要です。

*ハードディスクの上書き消去機能は上書き回数 1 回(”0(ゼロ)”による上書き)と、3 回(0・1・乱数による上書きと検証) の選択が出来ます。

複合機内のデータを一括削除

複合機を廃棄または他の部門に移動する場合などに複合機に登録・設定されている情報を管理者が全て削除できます。廃棄時、複合機内のデータ漏えいを抑止します。

HDD 搭載機の場合、オプションのデータ上書き消去キットの導入機では、HDD のストレージ蓄積データを上書き消去（一括削除）します。オプション未導入機は、初期化(フォーマット処理)のみ実施できます。
SSD 搭載機の場合、初期化(Secure Erase)によりデータを消去します。ストレージ蓄積データの暗号化を実施している場合は、データ一括消去により暗号化鍵も削除されます。暗号化鍵を削除する事によって暗号化されたストレージ蓄積データの復号（読み出し）が出来なくなりますので、データそのものを削除する事と同様の効果があります（Cryptographic Erase）。

表 7

オフィス複合機のセキュリティー上の脅威	富士フイルムビジネスイノベーションのセキュリティー対策
7. **管理者またはエンドユーザーのうっかりミスによる情報漏えい** 問題なく設定したつもり、問題なく操作したつもりであっても、誤った操作により予期せぬ情報漏えいを招く。	**G) 設定ミスや操作ミスの抑止、文書取り扱い意識の向上** ● **グローバル IP アドレスの利用警告** 管理者による IP アドレスの変更やユーザー認証モードの使用を促します。 ● **スキャン文書の配信先/格納先固定** 通信先(ファクスを含む)を特定の宛先に限定することにより、誤送信/情報漏えいを防止できます。 ● **ファクス誤送信抑止** 宛先再入力、手動リダイヤルなどによりミスを抑止します。 ● **ファクス受信制限** 迷惑なダイレクトメールなどを防止します。 ● **プリント禁止時間帯** 放置プリントを防止できます。 ● **出力後の文書からの情報漏えいを抑止** アノテーション、複製管理出力(隠し文字印刷)、ペーパーセキュリティー機能を提供しています。

G) 設定ミスや操作ミスの抑止、文書取り扱い意識の向上

グローバル IP アドレスに対するセキュリティー警告メッセージ

管理者のログイン時にグローバル IP アドレスが設定され、かつ［認証方式の設定］が［認証しない］に設定されている場合、セキュリティー警告が表示されます。管理者による IP アドレスの変更やユーザー認証モードの使用を促します。

スキャン文書の配信先/格納先を固定

本体からスキャン文書をメール送信する際は、認証ユーザー自身のメールアドレスを宛先や送信者として設定できます。誤送信防止や、外部への送信の抑止などに効果的に利用できます。

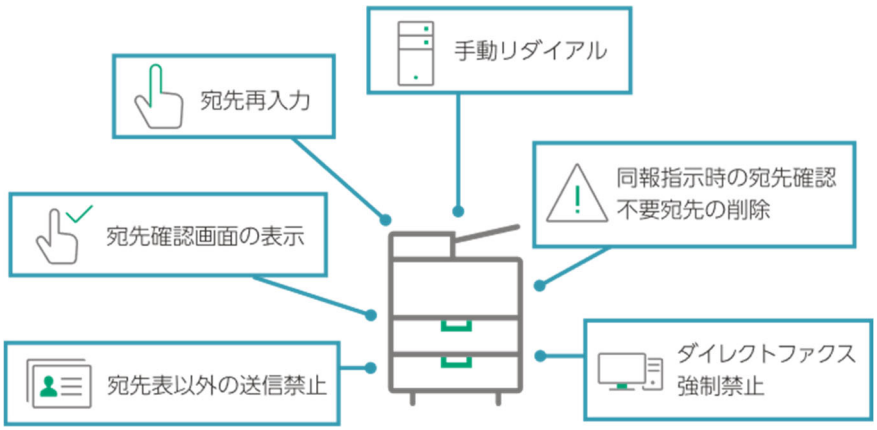
また、文書保存先を PC 上の任意のフォルダーに固定することができます。さらに、本体にスキャン文書をいったん格納して、格納先の URL を添付したメールを認証ユーザーに送信することも可能です。格納されているスキャン文書は、メールに記載の URL をクリックするだけで簡単にダウンロードできます。認証ユーザー自身への確実な配信だけでなく、ネットワークやメールサーバーの負荷軽減に役立ちます。

注：認証モードでの運用が必要です。

ファクスの誤送信抑止

ファクスの宛先間違いは、誰もが起こしうるミスである一方、取り返しのつかない重大な事態に発展しかねません。そこで、確認のために宛先を 2 度入力させる「宛先再入力」や、以前送信した相手先をリストから選択し送信する「手動リダイヤル」など、誤送信抑止に貢献する機能を充実させました。ビジネス用途向けファクスのセキュリティー機能のガイドライン「FASEC 1 [注 1]」に適合しています。

- 宛先再入力
  宛先の 2 度入力で、入力ミスを回避
- 宛先表以外の送信禁止
  あらかじめ登録された宛先以外の送信を禁止
- ダイレクトファクス強制禁止
  PC からのファクス送信を禁止
- 宛先確認画面の表示
  送信前に確認画面を表示し、間違った宛先の削除が可能
- 同報指示時の宛先確認・不要宛先の削除
  任意に宛先を削除・修正し、同報送信可能
- 手動リダイヤル
  送信すると宛先を記憶し、その後は記憶した宛先を選んで、テスト送信後に確実に送信



注 1: 電話回線におけるファクシミリ通信のセキュリティー機能強化を推進するために、情報通信ネットワーク産業協会により制定されました。

また、以下の機能もファクス誤送信抑止に適用可能です。

- ファクス同報送信の禁止
- ファクス送信時の中継同報送信および転送機能の禁止

ファクス受信制限

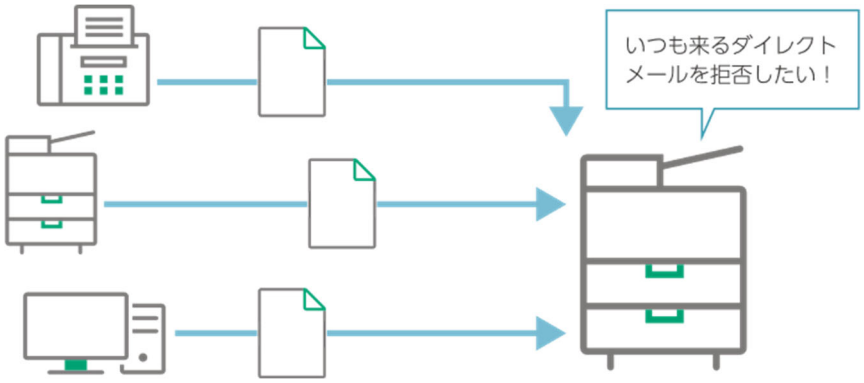
迷惑ファクス防止機能

着信拒否機能で迷惑なダイレクトメールなどを防止します。
受けたくない相手や非通知設定のファクスを拒否することができます。不特定に送信されるダイレクトメールファクスによる無駄なプリントをなくします。

- 受信制限番号: ファクス受信を拒否する G3 ID(電話番号)を登録します。最大 50 件まで登録できます。
- 非通知番号の受信制限: G3 ID(電話番号)が非通知のファクス受信を制限できます。

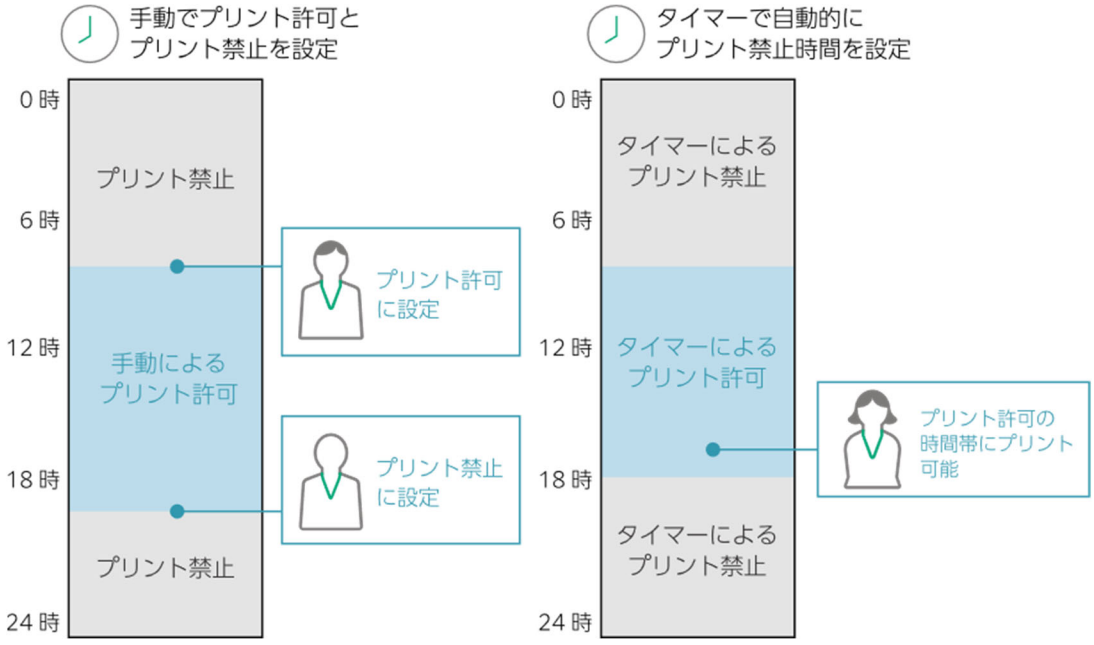
登録済み宛先以外からの受信制限

カストマーエンジニアによる設定で複合機に登録されている宛先以外からのファクス受信を制限することが可能です。



プリント禁止時間帯

設定した時間帯でのプリントを禁止する設定ができますので、オフィスに誰もいないときの放置プリント/ファクスを防止することができます。

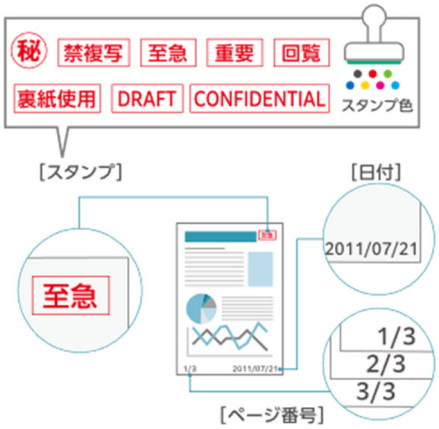


タイマー設定でプリント禁止中でも、ユーザーの操作によりプリント許可に変更することができます。

出力後文書からの情報漏洩の抑止

アノテーション

コピー時に、「禁複写」などのスタンプをつけて書類の重要性を知らせることができます。

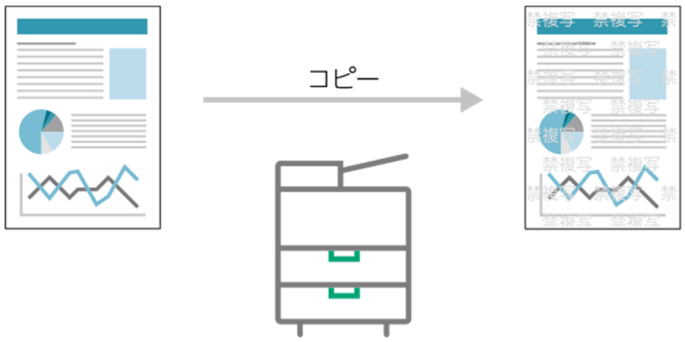


強制アノテーション

コピーやプリント、ファクス受信文書に、強制的にユーザーID や出力年月日時などを印字します。「いつ」「誰が」出力したかを容易に確認できるほか、４パターンあるレイアウトテンプレートをジョブごとに関連付けて設定可能。本体機能のみで利用できるため、簡単・手軽に、紙文書の適切な取り扱いを促します。

複製管理出力（隠し文字印刷）

管理番号や隠し文字を背景に印刷して、コピーすると文字が浮かび上がるように出力できます。不正コピーによる情報漏えいの抑止に役立ちます。また、ユーザーの文書取り扱い意識の向上を促進します。

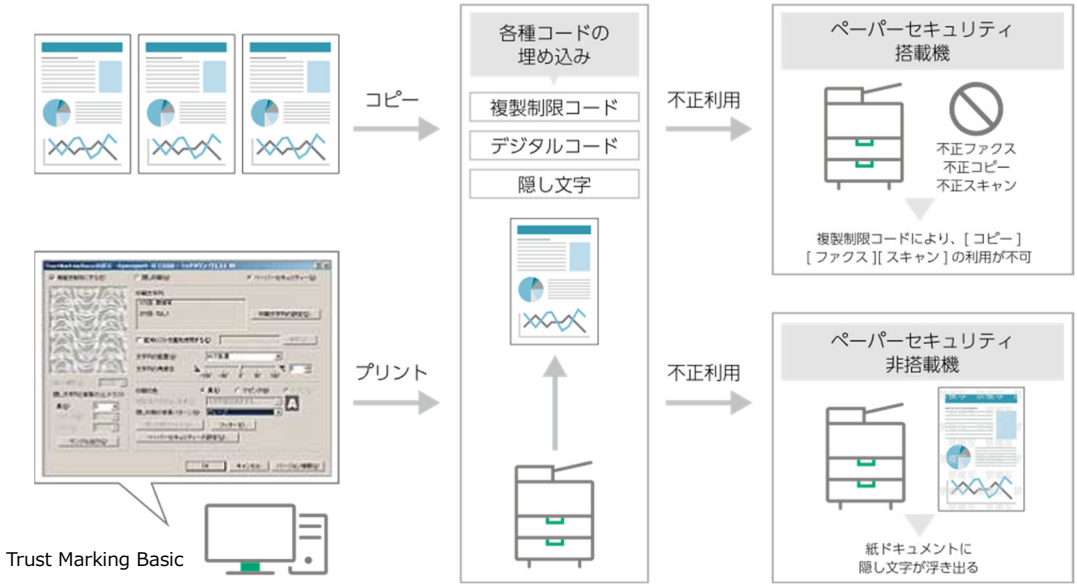


注記：オプション。複製管理拡張キットが必要です。

ペーパーセキュリティー

コピーやプリント時、複製制限コードやジョブ情報などのデジタルコードの埋め込みを都度指定できます。これにより複製そのものの抑止や、出力履歴の分析が可能に。また、管理者によりデジタルコードを強制的に埋め込むように設定することもできます。情報漏えいが発生した際、管理者による情報追跡を可能にします。

紙文書そのものにセキュリティー機能を付与し、不正コピーを防止



注記 1：オプション。ペーパーセキュリティーキットが必要です。

注記 2：文書の複製制限、デジタルコードの分析機能、隠し文字の牽制効果は、常に機能を保証するものではありません。原稿や設定条件によっては、機能が有効に働かない場合があります。

注記 3：プリント時のデジタルコードの任意の埋め込み指示には、別売ソフトウェア TrustMarkingBasic が必要です。

FUJIFILM

富士フイルム ビジネス イノベーション株式会社

〒107-0052　東京都港区赤坂 9-7-3　Tel 03-6271-5111　fujifilm.com/fb