RICOH
imagine. change.

複合機・プリンターのセキュリティ白書

Version 1.01 2023/9/29

目次

1. はじめに

リコー製品の安全性・リコーグループ全体にとっての製品セキュリティの重要性

情報化社会の発展とともに、サイバー攻撃の頻発、外部からの不正アクセスなど様々な脅威が我々の周りを取り囲んでいます。また、各国規制の強化・多様化、地政学的リスクの顕在化など企業における対応範囲の拡大に伴い、サプライチェーン全体でのセキュリティ対策の推進が求められています。

リコーは、「お客様情報を脅威から安心・安全に守る」ために必要な活動範囲を「情報セキュリティ」と捉え、さまざまな施策を実施しております。本書では、その中でも製品・サービスで取り扱うお客様情報を攻撃者から守る活動として、機能・体制をご紹介しております。

セキュリティを確保するためにはお客様の環境に合わせ、セキュリティ設定・運用をお願いいたします。
リコーはセキュリティの重要性をお客様にお伝えし、正しいセキュリティ設定ができるようにサポートしていきます。

リコーにおける製品セキュリティ基本ポリシーや考え方

リコーグループの情報セキュリティへの取り組みの全体像について、情報セキュリティ報告書にてご紹介しております。ぜひご一読くださいますようお願い申し上げます。

詳細については、当社の Web **サイト** で確認できます。
URL：https://jp.ricoh.com/security

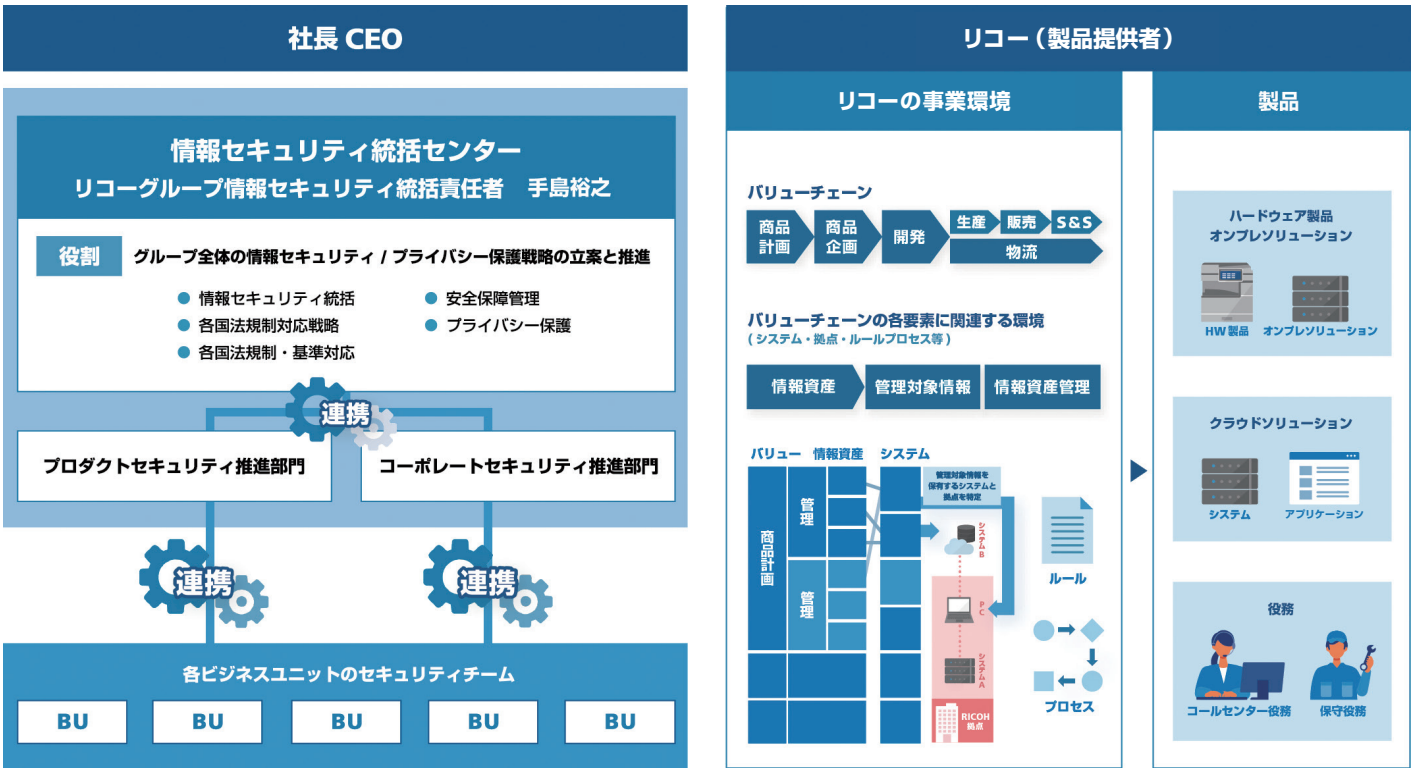
2. 情報セキュリティにおけるマネジメント体制

プロダクトセキュリティを実現・維持するための体制

国際的な情報セキュリティ標準（ISO/IEC[*1]、NIST[*2] など）に基づき、当社グループのサプライチェーン全体の情報セキュリティを意識した体制を構築 / 強化するとともに、企画・設計・購買・生産・販売・サポートの各過程の業務システムに関わるセキュリティリスクを適宜想定し、継続的に対策検討および実施を行っております。

CEO の直轄に、グループ全体の情報セキリティの戦略の立案・推進およびプライバシー保護に戦略の立案・推進を担う「情報セキュリティ統括センター」を設置しています。情報セキュリティ統括センターでは、製品のセキュリティを担うプロダクトセキュリティ推進部門と事業全体の情報セキュリティを担うコーポレートセキュリティ推進部門や、各ビジネスユニットに設置されたセキュリティチームと連携しながら、グループ全体の活動の強化に取り組んでいます。

*1)
ISO/IEC：International Organization of Standardization/International Electrotechnical Commission
*2)
NIST：National Institute of Standards and Technology



3. 複合機・プリンターにおけるセキュリティ対応方針

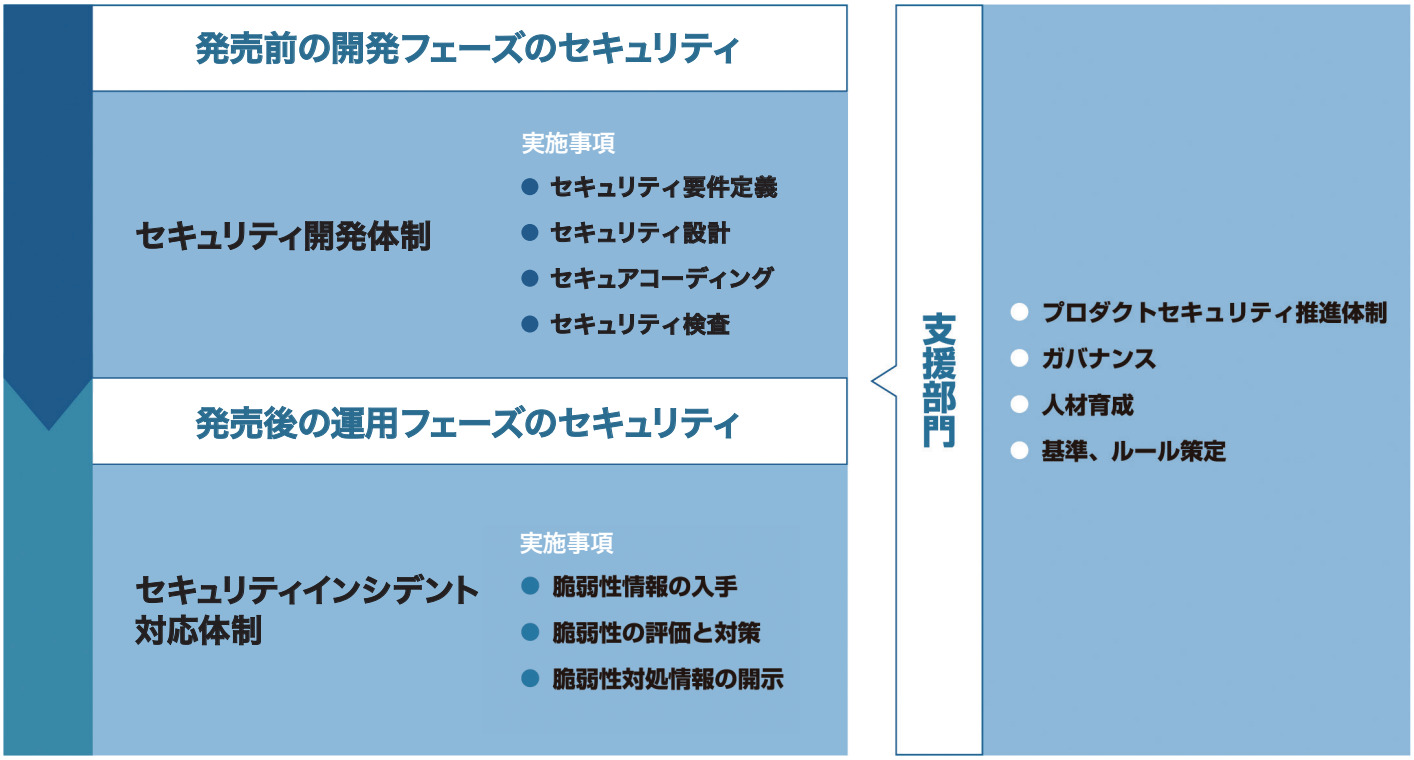
3 - 1 2つのフェーズに分かれた体制

生活の場所や働く場所のデジタル化が進み、多くのモノ・コトがつながる環境へと変化し、サイバー攻撃は高度化・巧妙化しています。

このような背景を踏まえ、リコーグループは、お客様に安心して製品・サービスをご利用いただけるよう、右記のセキュリティ対応方針に基づき、発売前と後でそれぞれフェーズを設定しています。発売前の開発フェーズでは、脆弱性混入/流出を防止するセキュリティ開発体制を構築しています。また、発売後の運用フェーズでは脆弱性の早期発見・早期対応を実現するセキュリティインシデント体制を構築しています。

＜セキュリティ対応方針＞

- デジタル技術の進歩・革新に追随するセキュリティ技術を習得します
- プロダクトセキュリティを実践する体制を構築します
- 国際的な標準に準拠したグループ内基準を整え、セキュリティに関する品質を維持し続けることに努めます
- セキュリティに考慮した製品、サービスの開発とセキュリティ検査で脆弱性混入と流出の防止に努めます
- 脆弱性に関する情報を収集し、製品・サービスに影響がある場合は適切に対処します
- お客様にとって有益な製品・サービスのセキュリティに関する情報を提供します



複合機・プリンターにおけるセキュリティ対応方針

3 - 2 開発フェーズのセキュリティ方針と取り組みについて

リコーグループは、製品・サービスをお客様やご利用者様に安心してご利用いただくために、製品・サービスのライフサイクル全体のセキュリティを企画・設計の段階から考慮するセキュリティ・バイ・デザインを「ISO/IEC27034-1:2011(Application security — Part 1: Overview and concepts)」に基づき実践してまいります。

3 - 2 - 1 セキュリティ開発ポリシー

リコーグループは、セキュリティ開発体制を構築し、製品・サービスの開発時に脆弱性の混入と流出を防止するための対策を実践してまいります。

脆弱性の混入防止

製品・サービスの脅威へのセキュリティ対策の設計し、セキュリティ対策を正確かつ安全に実装します。

脆弱性の流出防止

脆弱性診断を実施し、脆弱性が見つかった場合は必要な対策を講じます。

3 - 2 - 2 セキュリティ開発の行動指針

リコーグループは、脆弱性の混入と流出を防止するために、次に示す各事項をグループ規定とし実践するとともに、研鑽してまいります。

セキュリティ要件定義

セキュリティで保護すべき情報と機能（以下、保護対象）、セキュリティ対策を取る運用環境、製品・サービスの特性に適合したセキュリティリスク低減の目標値を決定します。

セキュリティ設計

セキュリティ要件に応じた、保護対象への脅威を抽出し、脅威の発現を軽減するためのセキュリティ機能や安全な運用環境・運用方法（セキュリティ対策）を設計します。
また、脅威に対抗するセキュリティ機能は、それ自体の無効化や性能低下を引き起さないプログラムの構造・仕組み（セキュリティアーキテクチャ）を取り入れて設計します。

セキュアコーディング

実装時に脆弱性を作り込まないよう、静的解析で確認します。

セキュリティ検査

製品・サービスの特性に応じたセキュリティ検査を実施し、脆弱性が見つかった場合は必要な対処をします。

複合機・プリンターにおけるセキュリティ対応方針

3 - 3 運用フェーズのセキュリティの方針と取り組みについて

リコーグループは、市場提供後の製品・サービスに影響する脆弱性を早期に発見して早期に対応するために「ISO/IEC 29147（脆弱性の公開）」、及び「ISO/IEC30111（脆弱性取扱いプロセス）」に基づき、脆弱性に対応してまいります。また、「情報セキュリティ早期警戒パートナーシップ [*3]」に参画し脆弱性による被害発生を抑制しております。

*3)
情報セキュリティ早期警戒パートナーシップガイドライン（IPA 発行）

3 - 3 - 1 脆弱性の処理および開示のポリシー

リコーグループは、製品・サービスのご利用者様に安心してご利用いただくために、セキュリティインシデント対応体制を構築し、脆弱性情報の入手、脆弱性の評価と対策、および脆弱性対処情報の開示を実施してまいります。

*4)
脆弱性を情報入手から対策完了まで管理するリコーグループ内システム
*5)
Japan Computer Emergency Response Team Coordination Center の略。一般社団法人 JPCERT コーディネーションセンターの略称。コンピューターセキュリティの情報を収集し、インシデント対応の支援、コンピューターセキュリティ関連情報の発信などを行う

脆弱性情報の入手

リコーグループは、グループ内外から広く早く脆弱性情報を入手し、脆弱性管理システム [*4] を利用して、脆弱性情報の評価と脆弱性の対策を担当する製品・サービスの開発部門と共有します。

リコーグループ内の脆弱性情報入手

製品・サービスの特性に応じたセキュリティ検査を製品・サービスのライフサイクルを通して継続的に実施します。

リコーグループ外からの脆弱性情報入手

製品・サービスのご利用者様、セキュリティ研究者、セキュリティ関連情報の収集・配信機関（JPCERT/CC [*5] など）からプロダクトの脆弱性に関する情報を収集します。

複合機・プリンターにおけるセキュリティ対応方針

脆弱性の評価と対策

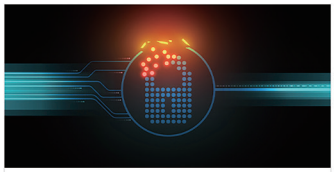
製品・サービスの開発部門は、脆弱性管理システムで受けた脆弱性の製品・サービスへの影響を評価し、製品・サービスに影響する脆弱性であることを確認した場合は、必要なセキュリティ対策を実施した上で、脆弱性情報と対策方法を脆弱性対処情報として準備します。
客観的視点で脆弱性の評価を行うために、セキュリティ技術委員会を設置し、公正な判断を行えるよう体制を整備しています。

脆弱性の対応時間について、リコーはセキュリティ先進企業レベルの迅速な対応を目指し、対策実施の期日を設定しています。
さらに、設定した目標に対する対策実施状況の監視と評価を定期的に行い、改善することで、より迅速な対応に努めてまいります。

脆弱性対応情報の開示

リコーグループは、脆弱性情報とその対策方法（回避方法の場合を含みます）を脆弱性対処情報とし、その情報を必要とする方へ、「対策情報同時開示の原則[*6]」と「情報開示日一致の原則[*7]」に従い、適切な時期に開示します。
情報開示は脆弱性ごと、製品・サービスごとのビューでリコーWebサイトのプロダクトセキュリティのページから提供を行っており、お客様がご利用中の機種の対応状況を素早く検索・閲覧いただけます。

詳しくはプロダクトセキュリティページの製品・サービスの脆弱性対処情報の提供をご参照ください。
URL：https://jp.ricoh.com/security/products/



脆弱性ごとの情報リスト
2022年10月1日以降、脆弱性情報を本ページに掲載する予定です。 ›

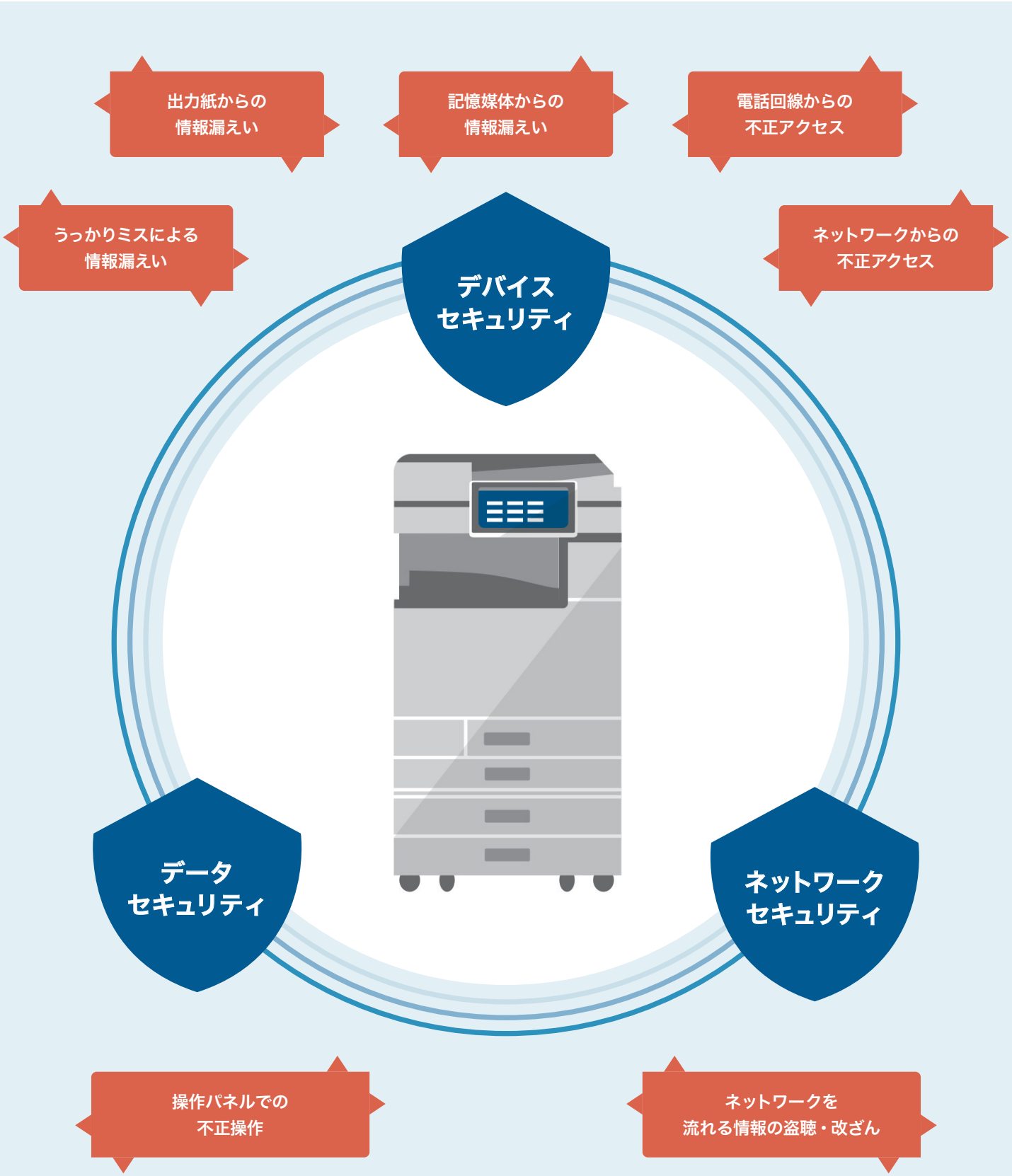
製品・サービスごとの脆弱性情報リスト
2022年10月1日以降に発見・改善されたリコー製品・サービスの脆弱性を、製品・サービス別に検索することができます。 ›

*6）
脆弱性情報の開示の時点で、対策方法も同時に提供することです。対策方法が整う前に脆弱性を情報開示してしまうと、脆弱性を悪用する攻撃コードが悪意ある第三者によって開発されて流通し、お客様へのサイバー攻撃に使われる可能性があるからです。
*7）
他社の製品・サービスにも影響がある脆弱性の場合に、関係者間で一定の足並みをそろえて情報開示することです。関係者間で調整された情報開示日を待たずに、単独で情報開示してしまうと、他社の製品・サービスをご利用のお客様をサイバー攻撃の危険にさらしてしまうことになるからです。

4. 複合機・プリンターにおけるセキュリティ上の脅威と対策

4 - 1 様々な脅威に対するセキュリティ機能概要

情報化社会の発展と共に、コンピューターウイルスや個人情報の漏えい、外部からの不正アクセスなど様々な脅威が我々の周りを取り囲んでいます。多様化する脅威に対し、リコーでは複合機のセキュリティ対策にいち早く着目し、あらゆるセキュリティ脅威を可能な限り想定して下記のように３つのカテゴリに分け、様々な取り組みを行っています。



複合機・プリンターにおけるセキュリティ上の脅威と対策

4-2 デバイスセキュリティ

4-2-1 ファームウェアの改ざん防止

複合機・プリンターにはその機器の動作をつかさどるファームウェアと呼ばれるソフトウェアが内蔵されています。
このファームウェアが悪意を持った者により不当に改ざんされると正常な動作ができず、それらの機器を踏み台としたネットワーク内部への侵入や、不正なプログラムによる機器の破壊などが行われる危険性が発生します。
リコーが設計したデバイスは、トラステッド プラットフォーム モジュール (TPM) を使用して構築されており、ファームウェアが改ざんされた場合に起動しないように設計されています。

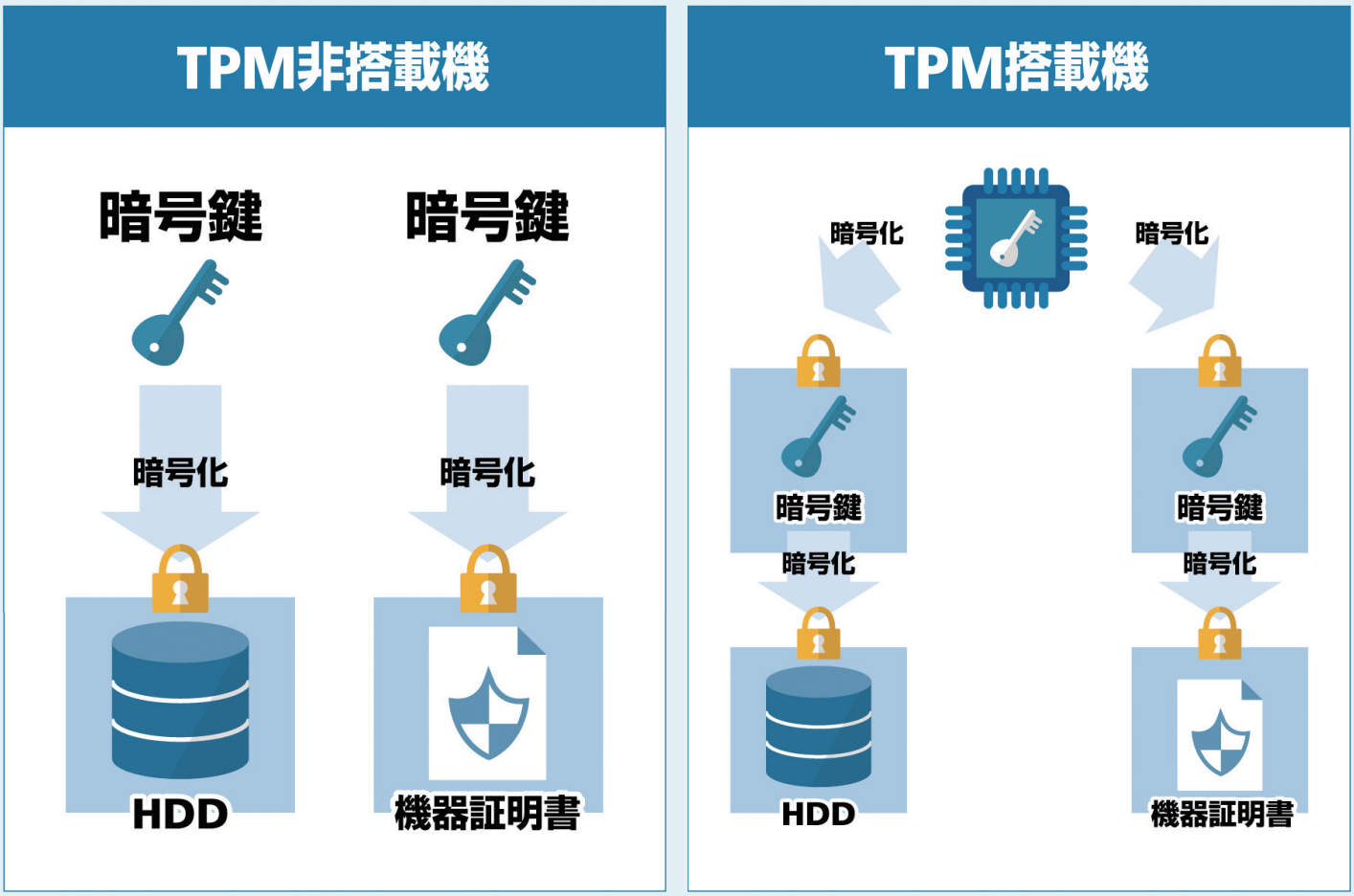
また、ハードディスク暗号化や機器証明書の暗号化に使われる暗号鍵は、この TPM 内部のルート暗号鍵によってさらに暗号化され保護されています。
ルート暗号鍵は TPM 外部から読み取ることはできないため、複合機内の情報を安全に保護することができます。

RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010 では最新規格である TPM2.0 をサポートしています。

TPM の対応製品のリストは、当社の Web サイト で確認できます。
URL：https://www.ricoh.co.jp/mfp/security/function/tpmlist.html

暗号鍵の記録場所を突き止められると、
暗号化したデータを解読されてしまう。

ルート暗号鍵はTPM内部で保持しているため、
不正に読みとることはできない。



複合機・プリンターにおけるセキュリティ上の脅威と対策

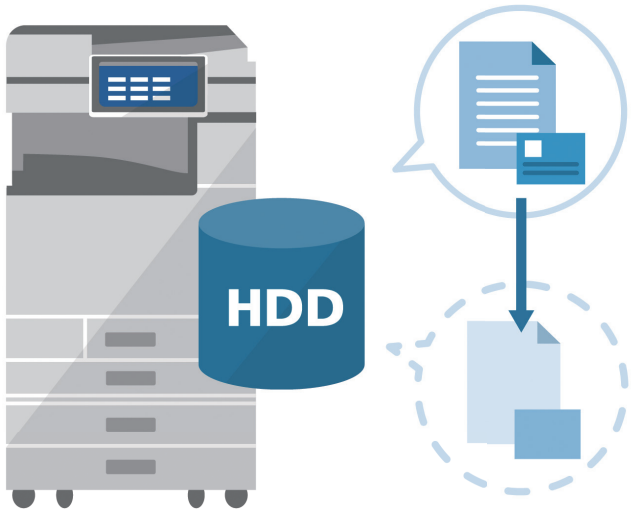
4 - 2 - 2 一時的に保存されるデータの逐次消去 *8

コピー・スキャナーによる原稿読み取り、パソコンからの出力などの際、データの一部がハードディスクドライブやメモリーに一時的に保存される場合があります。
これらのデータには、画像情報、ユーザーが入力した情報、デバイス構成情報などが含まれています。
こういった情報が何らかの方法で窃取されることにより、情報漏えいが発生する可能性があります。
リコーの複合機はハードディスクドライブに保存されている一時データを「0」と「1」でランダムに上書きして消去します。
コピーやプリント時に複合機に蓄積されたイメージデータをジョブの実行ごとに逐次に消去していきます。

- **機密情報の取り扱いに関するアメリカ国家安全保障局（NSA）および アメリカ国防総省（DoD）の推奨事項に準拠した方式を採用しています。**
- **上書き消去を繰り返すにより、一時データにアクセスすることは事実上不可能になります（上書き回数は 1 回から 9 回まで選択できます）。**

逐次消去の方式

NSA	データを乱数 2 回、ゼロ 1 回で上書きします。
DoD	データを 1 回目の乱数、1 回目の乱数の補数、2 回目の乱数で上書きします。
Random Numbers	データを指定された回数の乱数で上書きします。乱数の書き込み回数は 1 ～ 9 回まで選択できます。



*8)
データストレージとしてハードディスクドライブを搭載している機種でご利用可能な機能です。

4 - 2 - 3 データの一括消去

複合機本体を他部門に移設するときや廃棄するときに本体内のハードディスク /SSD に登録したユーザー情報などを一括して消去します。

一括消去の方式

NSA	データを乱数 2 回、ゼロ 1 回で上書きします。
DoD	データを 1 回目の乱数、1 回目の乱数の補数、2 回目の乱数で上書きします。
Random Numbers	データを指定された回数の乱数で上書きします。乱数の書き込み回数は 1 ～ 9 回まで選択できます。
BSI / VSITR	データを 0x00,0xFF,0x00,0xFF,0x00,0xFF,00xAA で上書きします。計 7 回上書きされます。
Secure Erase	ハードディスク内部に組み込まれたアルゴリズムで上書き消去します。
Format	ハードディスクのフォーマットだけします。データの上書きはしませんが高速です。

お客様の社内ポリシーに合った消去方式を実施できるように、上記の消去方式をサポートしております。Format 以外の上書き消去の効果は同等となっています。

複合機・プリンターにおけるセキュリティ上の脅威と対策

4-2-4 ストレージ暗号化によるデータ盗難の防止

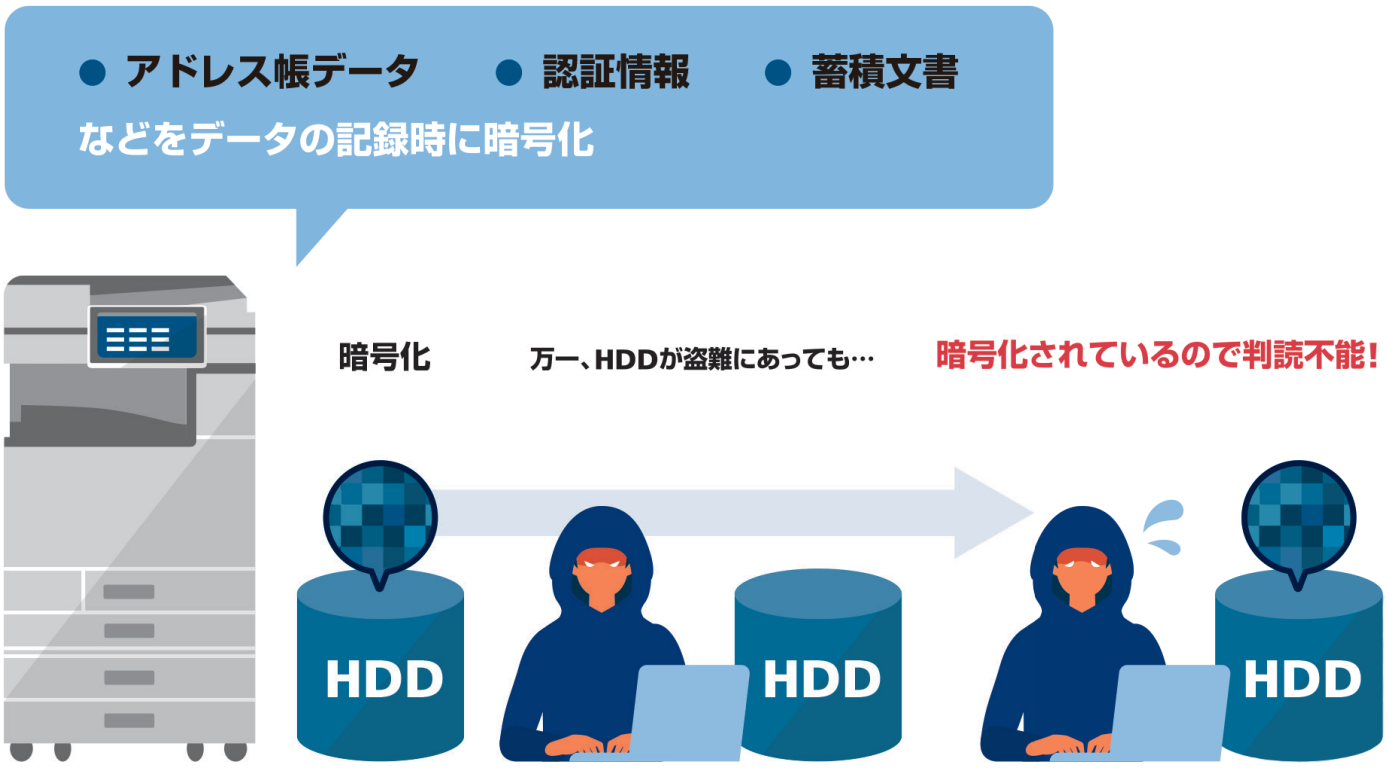
複合機本体に蓄積されるアドレス帳データ、認証情報、蓄積文書などはデータの記録時に暗号化します。これにより、万一、ストレージが物理的に盗難された場合でも情報漏えいを防ぎます。
ストレージの暗号化機能を有効にすることは、複合機・プリンターのデータを盗難から保護するだけでなく、組織のセキュリティポリシー準拠に貢献します。

暗号化対象となるデータ

電源を切ってもデータを保持する本体搭載メモリー、またはストレージに蓄積される以下のデータが暗号化されます。

- アドレス帳
- ユーザー認証データ
- 蓄積文書データ
- 一時保存されている文書データ
- ログ
- ネットワーク I/F 設定情報
- 機器設定情報

リコーは、Advanced Encryption Standard (AES) 256 ビットのストレージ暗号化を提供しています。



複合機・プリンターにおけるセキュリティ上の脅威と対策

4-2-5 ファクス回線のセキュリティ

ファクス機能を有する複合機は、電話回線で外部とつながっているため、そこからの不正アクセスを防止する必要があります。
リコーの複合機内部のソフトウェア（プロセス）は目的の機能を実現するための他の所定のプロセス以外と連携を行うことはできません。
また、扱うデータの種類も制限されています。
つまり、ファクス回線から入力されたデータは、ファクス動作を実行するためのプロセス以外に通信されることはないため、ファクス回線を介してネットワークへの不正なアクセスや、機器内部のプログラムへの不正なアクセスはできない機構となっています。

4-2-6 ジョブログ／アクセスログ管理機能

複合機などの機器内に蓄積されたログを収集することで、各機能の使用履歴、エラー履歴、本機へのアクセス状況やアクセス者の詳細な情報が確認できます。この機能により、情報漏えいに対する心理的な抑制と万一の発生時に追跡が可能になります。収集するログ情報は下記のとおりです。

ジョブログ

- コピー、ドキュメントボックスへの文書蓄積、プリンター印刷、ファクス送信、スキャナー配信などのユーザーの文書に関わるワークフローすべてのログ情報
- 操作部から出力するシステム設定リストなどのレポート印刷

アクセスログ

- ログイン、ログアウトなどの認証
- 蓄積文書の作成・編集・削除などの文書操作
- ハードディスク初期化などのサービスエンジニア操作
- ログ転送結果、不正コピー読み取り時のシステム動作
- 暗号化通信、アクセス攻撃、ロックアウト、ファームウェアの正当性確認などのセキュリティ動作

複合機・プリンターにおけるセキュリティ上の脅威と対策

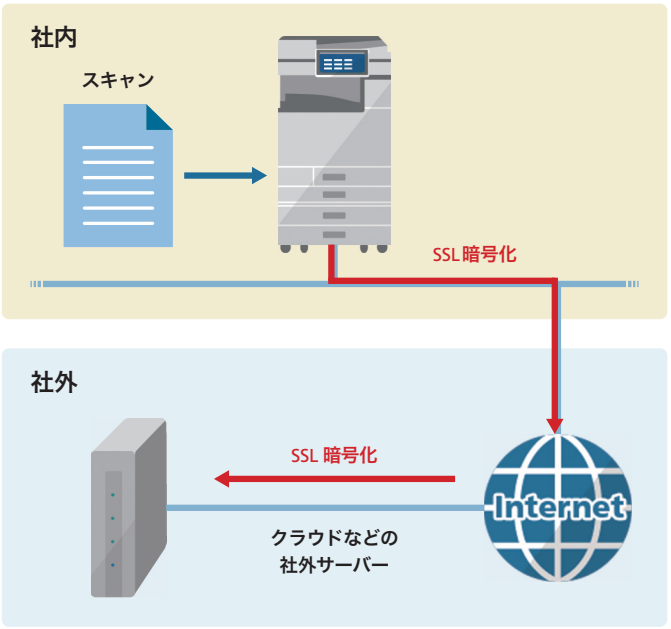
4 - 3　データセキュリティ

複合機・プリンターが扱うデジタルデータと紙媒体で出力したドキュメントは、どちらも情報漏えいなどの深刻なセキュリティリスクに繋がる可能性を抱えています。
リコー製品は、企業のセキュリティポリシー遵守活動をサポートするだけでなく、誤用や不注意から発生するセキュリティ事故を防止するための機能を備えています。

4 - 3 - 1　スキャン機能

紙媒体の情報をスキャンしてファイルサーバーに保存したり、電子メール経由で送信したりするプロセスを適切に保護するためには、ユーザー権限の設定が有効です。
ユーザー ID とパスワードによるログイン、オプションの Kerberos 認証など、複数の認証オプションを使用して、スキャン操作を利用できるユーザーを制限することができます。

また、スキャンデータを送信する通信を SSL/TLS で暗号化すると、社外にある SMTP サーバーを利用する場合に懸念される情報漏えいや改ざんのリスクを大幅に軽減できます。
RICOH IM 6000/5000/4000/3500/2500 発売以降の機種より、TLS1.3 に対応しています。



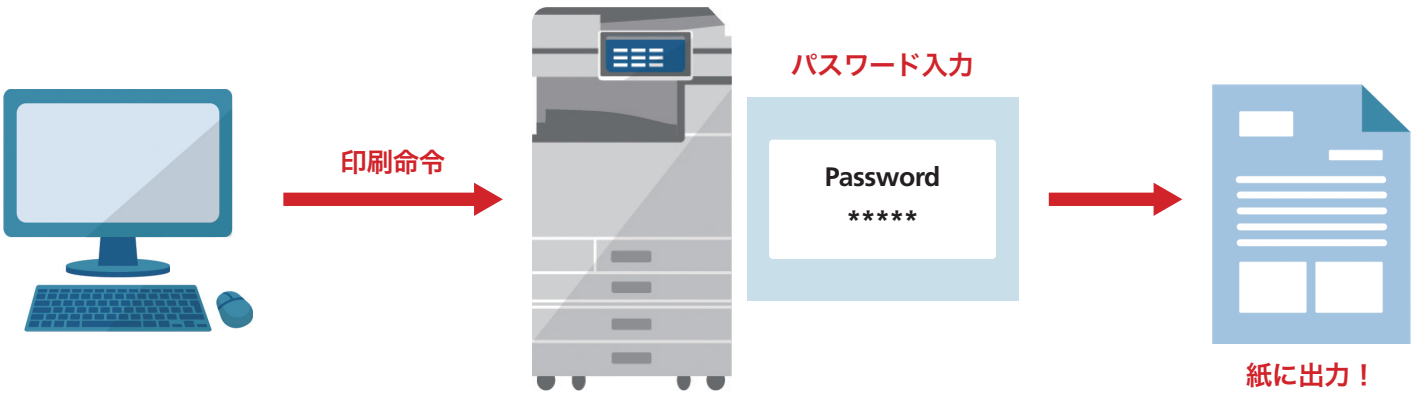
4 - 3 - 2　機密印刷

印刷した文書が出力されたまま放置されることは、情報漏えいの大きなリスクです。機密情報が人目に触れたり、回収されて悪用されたりする可能性があります。

印刷する文書を複合機本体のストレージに蓄積することが可能です。機密印刷機能では、パソコンからパスワードを指定して印刷後、複合機の操作パネルでパスワードを入力して出力します。機密文書を他人に見られることなく出力できます。

印刷物の出しっぱなし、持ち帰りを防止

「機密印刷」を指定すれば、本体側でパスワードを入力するまで紙に出しません。



複合機・プリンターにおけるセキュリティ上の脅威と対策

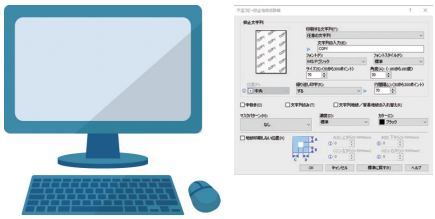
4 - 3 - 3 不正コピーガード / 地紋印刷

リコーはドキュメントのセキュリティ対策にも配慮した不正コピーガード機能を提供しています。出力時またはコピー時に、全体に特殊な地紋を埋め込んで印刷。地紋を埋め込んだ文書をコピーすると埋め込まれた牽制文字が浮かび上がります。また、地紋を検知して画像を破壊し、紙一面をグレーに印刷して情報漏えいを抑止します。例えば、機密情報などを出力しなければならない場合に本機能をご使用いただくことで、コピーによる情報の拡散を牽制することができ、情報漏えいを抑えることが可能です。

「不正コピー抑止」のワークフロー（イメージ図）

「機密印刷」を指定すれば、本体側でパスワードを入力するまで紙に出しません。

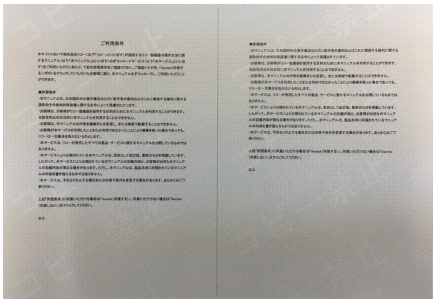
プリンターで地紋を埋め込んだ文書を出力



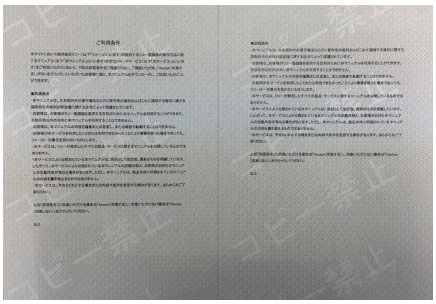
不正コピー抑止文書、または不正コピーガード文書が印刷できます。

コピー時に複合機の操作パネルで地紋を設定

地紋を埋め込んだ文書



不正コピー地紋文書



牽制文字が浮き上がります。

不正コピーガード文書

文書全体をグレー地に変換します。

4 - 3 - 4 強制セキュリティ印字

文書を印刷したユーザー名、いつ、どのデバイスから印刷されたかなどの識別情報を強制的に付与することができます。この機能はコピー、プリント、ファクス、およびドキュメントサーバー機能に対して有効化できます。
右記の中から付与する情報の種類を選択することができます。

- **文書が印刷された日時**
- **文書を印刷した人の名前またはログインユーザー ID**
- **印刷したデバイスの IP アドレスとシリアル番号**

4 - 3 - 5 機能の使用制限

複合機・プリンターの無断使用は企業のセキュリティポリシー違反に繋がる可能性があります。
リコー製品では、個人の使用状況を追跡することができます。
ユーザーまたは部署ごとに利用可能な機能や印刷ボリュームを制限することも可能です。

複合機・プリンターにおけるセキュリティ上の脅威と対策

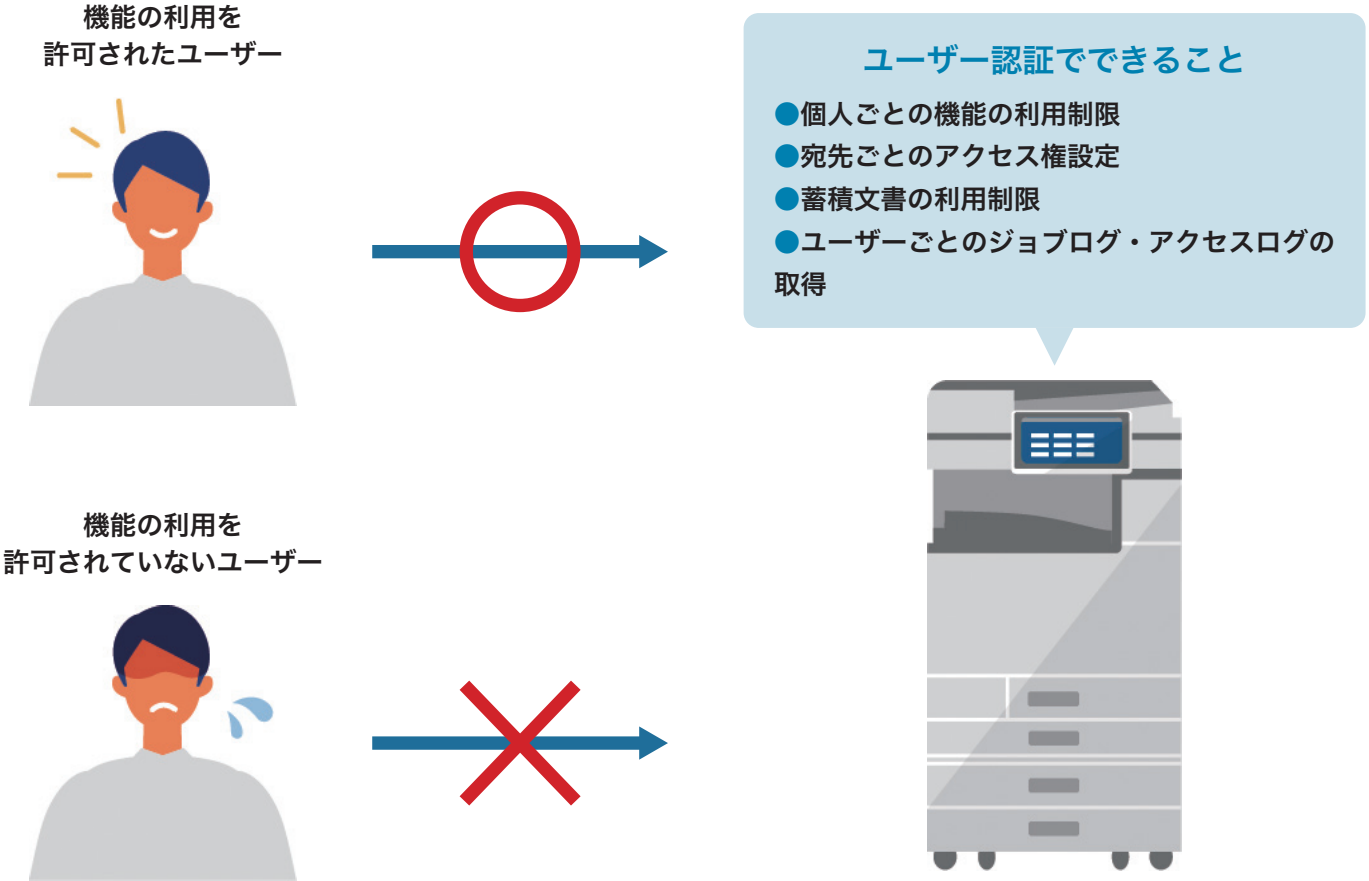
4-4 ネットワークセキュリティ

複合機・プリンターはネットワークを介してコンピューターやサーバーと重要な情報を含む通信を行います。通信が保護されていない場合、重要な情報が悪意を持って改ざん・窃取される可能性があります。
リコーの製品と技術は、ネットワークを介した不正アクセスから重要な情報を保護する機能を提供しています。

4-4-1 ユーザー認証

ログインユーザー名とパスワードを使ったユーザー認証システムを搭載しているので、個人識別が可能です。また、ネットワークで接続されている Windows のドメインコントローラーや LDAP サーバーとの連携により、既存の認証システムによる個人認証も可能です。

最新のモデルではオプションのカードリーダーとの組み合わせによる多要素認証を利用可能です。



選択可能な認識方式

●ベーシック認証 ●Windows 認証 ●LDAP 認証 ●ユーザーコード認証 ●結合サーバー認証

4-4-2 使用していないポートの制限

複合機・プリンターのネットワークポートを開放したままにすると、保存されたデータの破壊や改ざん、サービス拒否（DOS 攻撃）、ウイルスやマルウェアの侵入など、様々な脅威に繋がる可能性があります。
リコー製品では、使用していないポートを閉じることだけでなく、SNMP や FTP などの特定のプロトコルについても無効化ができ、悪用のリスクを遮断することができます。

複合機・プリンターにおけるセキュリティ上の脅威と対策

4-4-3 ネットワーク通信の暗号化

SSL/TLS

複合機管理者は SSL/TLS を設定することで暗号化通信ができます。これにより、通信途中でのデータの盗聴、内容の解析、改ざんの危険を抑えることができます。

リコーは、アメリカ国立標準技術研究所（NIST）が要求する暗号化アルゴリズム（AES256bit ならびに SHA-2）を暗号通信機能を持つ最新機種で標準搭載、および暗号論的擬似乱数生成アルゴリズム（HMAC_DRBG）を暗号鍵の生成に採用することで、機器との通信や機器内の処理の安全性を高めています。

例えば、インターネットを活用したメールサービスやクラウドサービスを導入されているお客様は、スキャン to E-Mail 機能での通信を SSL/TLS で暗号化すると、社外にある SMTP サーバーを利用する場合に懸念される情報漏えいや改ざんのリスクを大幅に軽減できます。スマートフォンアプリケーション「RICOH カンタン入出力」と複合機との通信も、SSL/TLS で保護することができます。

SNMP

SNMP（Simple Network Management Protocol）はネットワーク機器の監視や制御を行うために、ネットワーク機器の印刷総枚数やエラーなどの情報を収集するためのプロトコルです。ネットワーク機器の構成内容が記述された MIB（Management Information Base）から情報を取得し、サービスの稼働状況を監視することなど機器の運用に役立てられます。
SNMP v3 には、ユーザー認証機能やデータ暗号化機能などが組み込まれおり、お客様のデータやネットワーク機器の情報を守ることができます。

4-4-4 印刷ジョブデータの暗号化

IPP over SSL/TLS

印刷ジョブデータの傍受には、IPP over SSL/TLS による暗号化で対処できます。
リコー製品はインターネット印刷プロトコル（IPP）の印刷データを Secure Sockets Layer/Transport Layer Security（SSL/TLS）によって暗号化することにより、通信経路上での印刷ジョブデータの情報傍受を防ぎます。

S/MIME

複合機本体のアドレス帳にユーザーの証明書を登録することで、公開鍵による暗号方式を用いたメッセージ送信が可能になり、情報漏えいを抑止することができます。また本体に機器証明書を導入し、秘密鍵を使用した電子署名を添付することで、送信者のなりすましやメール内容の改ざんの危険を抑えることができます。
※ W-NET FAX、ダイレクト SMTP では使用できません。

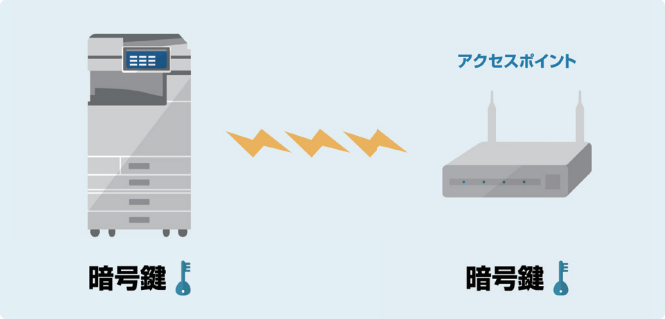
POP3/IMAP4 over SSL

サーバーからメールを受信する通信を暗号化できます。

Wi-Fi™

Wi-Fi™ セキュリティについては、AES 暗号化（Wi-Fi Protected Access™）を使用する WPA3™[*9]、WPA2™、WPA2™-PSK をサポートしています。

*9)
RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010
のみサポート



ドライバーを用いたエンドツーエンド暗号化

ユーザーのシステムとリコー製品との間で、印刷データをエンドツーエンドで暗号化することも可能です。ドライバーからこの設定を有効にして機密印刷を行うと、印刷ジョブデータが印刷指示の実行から印刷の直前まで暗号化されます。復号は機密印刷のパスワードが入力されるまで行われません。

5. 認証と評価

リコーでは、お客様の情報資産であるドキュメントのセキュリティを高めるために、電子文書や紙文書の改ざん、漏えいを防ぐセキュリティ対策にいち早く取り組み、ドキュメントのライフサイクル全般（文書の発生から、処理、保管、保存、破棄まで）にわたり想定されるリスクに対処すべく製品のセキュリティ機能の開発に注力してまいりました。
そして、2010 年 2 月、複合機・プリンターが備えるべきセキュリティ機能の国際的な規格「IEEE 2600.1」に適合した CC 認証を「imagio MP 5000 SP/4000 SP」（2008 年 2 月発売）、また、2020 年 1 月には「ハードコピーデバイス（ディジタル複合機）プロテクションプロファイル（HCD PPv1.0）」に適合した CC 認証を「RICOH IM C6000/C5500/C4500/C3500/C3000/C2500/C2000」（2019 年 1 月発売）で取得しました。
リコーでは、お客様により安心して機器をお使いいただけるように、「IEEE 2600.2」「HCD PPv1.0」に適合した CC 認証取得製品を幅広いラインアップで揃えております。

5 - 1 セキュリティ認証（CC認証）

Common Criteria（CC）は情報セキュリティのための国際評価規格で、IT 製品が備えるべきセキュリティ機能が適正に開発されているかを評価する規格です。
お客様は IT 製品の調達時に、CC 認証（ISO/IEC 15408）というセキュリティ規格を用いて要求仕様を明確に製品提供者に伝えることができ、各社のセキュリティ機能を比較検討することができます。
現在、世界の 25 カ国以上で政府の調達基準となっており、近年では国内外の複合機ベンダーが複合機においても積極的に認証取得を行っています。
また、他業種においても国際市場競争力の確保に本制度が利用されています。

認定製品のリストは、当社の Web サイトで確認できます。
URL：https://www.ricoh.co.jp/mfp/security/cc/

5 - 1 - 1 Hardcopy Device Protection Profile（HCD PPv1.0）

ハードコピーデバイス（ディジタル複合機）プロテクションプロファイル v1.0 は、2012 年に国際的なセキュリティ評価認証制度の利用者団体 CCUF（Common Criteria Users Forum）において、複合機 TC（Multifunction Printers Technical Community：ディジタル複合機 技術部会）を創設し、日米の認証機関や、リコーをはじめとした各複合機メーカー主導のもと、政府調達のセキュリティ要件としてのデジタル複合機用のプロテクションプロファイルです。

右記の領域について、リコーがラインアップする複合機の多くが HCD PP v1.0 に基づいて評価されています。

- **ユーザー識別および認証システム**
- **データ暗号化技術**
- **システムのファームウェアの正当性検証**
- **アナログファクス回線と コピー / プリント / スキャン コントローラーの分離**
- **データ暗号化アルゴリズムの検証**
- **データ上書き処理**

5 - 1 - 2 IEEE 2600.2

IEEE 2600 は、2003 年に複合機の主要ベンダーを中心に、複合機において、それまで各社でバラバラに決められていた CC 認証取得機能を、顧客視点でどうあるべきかを業界各社が集まって規定した国際標準です。
リコーは、IEEE のワーキンググループにおいて積極的な活動を行い、「プロテクション・プロファイル（PP：Protection Profile）」の策定に貢献しました。
IEEE 2600 には、軍・政府向け用、大手企業向け用、公共スペース用、SOHO 用などの用途別に作成された PP と呼ばれる文書が含まれています。
PP は、CC 認証評価の対象となるセキュリティ機能 / 条件などを特定する文書として利用されます。
この PP 適合を「セキュリティターゲット（ST：Security Target）」に組み込んで CC 認証評価を受けることで、CC 認証において PP 適合していることが認められます。
IEEE 2600 の同じ PP に適合している製品であれば、同一レベルのセキュリティ機能が搭載されていることになります。
IEEE 2600 の PP 文書には以下のものがあります。想定される使用環境ごとに PP が定義されています。

認証と評価

5 - 2 Cisco社によるペネトレーションテストの実施

RICOH IM C6010/C5510/C4510/C3510/C3010/C2510/C2010 は、Cisco 社によるペネトレーションテストを実施しています。
幅広い専門知識を持つセキュリティベンダーのホワイトハッカーが侵入を試行するテストを通過することにより、悪意ある攻撃に対する耐性を確認しています。

グローバルフットプリント

- 米国と英国に技術人材を集中させたワールドワイドなチーム
- 米国および EMEA における優れた対応業務

専門知識

- ハードウェア、チップ、クラウド、アプリケーション、プログラムに関するセキュリティの専門知識
- 専用のプラクティス管理と技術面でのリーダーシップ

成熟した手法

- 様々な業界での実績

オペレーショナルエクセレンス

- グローバルなコラボレーションメカニズム

サポートテクノロジー

- ラボ開発への多額の投資
- 専用のラボ管理
- 米国のヴァージニア州ハーンドン、イリノイ州シカゴ、英国のワトフォードに IoT ラボを構える

知識共有の取り組み

- アドバイザリアクセラレータの提供とコラボレーションツール
- カスタム Jira の開発
- 社内および社外のエキスパートが持つ知識を活用

※ IoT:Internet of Things

6. おわりに

世界的なサイバー攻撃の増加による情報保護のニーズの高まりはいまや普遍なものであり常識となりつつあります。攻撃者とのいたちごっこは これからも続き、今後もそれが緩むことはないでしょう。リコーグループは、各業界、国を挙げてのセキュリティ水準強化などの外部環境の変化を常に注視しながら、デジタルサービス会社として柔軟に対応できるよう、継続的にセキュリティの取り組みを強化・改善し、それを実現するための 情報セキュリティ体制の強化を継続的に実施していきます。

RICOH
imagine. change.

株式会社リコー
東京都大田区中馬込1-3-6 〒143-8555

https://www.ricoh.co.jp

リコー製品に関するお問い合わせは下記のダイヤルで承っております。

リコーテクニカルコールセンター 0120-892-111（イチ イチ イチ）

●受付時間：平日（月～金）9時～17時（祝祭日、弊社休業日を除く）
※お問い合わせの内容は対応状況の確認と対応品質の向上のため、録音・記録をさせていただいております。
※受付時間を含め、記載のサービス内容は予告無く変更になる場合があります。あらかじめご了承ください。
https://www.ricoh.co.jp/contact/
■リコーにご提供いただいたお客様の個人情報の取り扱い方針については、当社ホームページでご確認いただけます。

●お問い合わせ・ご用命は・・・

本書の記載内容は、2023年9 月現在のものです。