Konica Minolta
Security Technical Support Paper

セキュリティー基本方針と対応技術に関する報告書

Ver. 10.4

February 2024

改訂履歴

版	発行日	改訂内容
第 1 版	2004 年 8 月	初版
第 1.1 版	2004 年 9 月	対応機種追加
第 2.0 版	2005 年 2 月	対応機種追加
第 2.1 版	2005 年 2 月	第 2.0 版修正
第 2.2 版	2005 年 3 月	第 2.1 版修正
第 3.0 版	2005 年 9 月	対応機能見直し 及び 対応機種追加
第 4.0 版	2007 年 1 月	対応機能見直し 及び 対応機種追加
第 4.1 版	2008 年 8 月	対応機種のみ追加
第 4.2 版	2009 年 3 月	記載追加、対応機種追加
第 4.3 版	2009 年 11 月	記載追加、対応機種追加
第 4.4 版	2010 年 4 月 27 日	記載追加、対応機種追加
第 4.5 版	2011 年 2 月 16 日	記載追加、対応機種追加
第 5.5 版	2012 年 1 月 16 日	記載追加、対応機種追加
第 5.6 版	2012 年 3 月 15 日	記載追加、対応機種追加
第 5.6.1 版	2012 年 4 月 12 日	記載追加、対応機種追加
第 5.7 版	2012 年 9 月 12 日	記載追加、対応機種追加
第 6.0 版	2012 年 11 月 30 日	記載追加、対応機種追加
第 7.0 版	2013 年 2 月 26 日	記載追加、対応機種追加
第 7.0.1 版	2013 年 7 月 30 日	対応機種追加
第 7.1 版	2013 年 10 月 18 日	記載追加
第 8.0.1 版	2014 年 6 月 10 日	記載追加、対応機種追加
第 8.0.3 版	2014 年 7 月 14 日	TPM 記載追加
第 8.0.4 版	2014 年 8 月 26 日	対応機種追加（C3110, C3100P, 4700P, 4000P, 3300P）
第 8.0.6 版	2015 年 4 月 13 日	CSRA 記載追記 対応機種追加（bizhub PRESS C71hc）
第 8.0.7 版	2015 年 8 月 19 日	対応機種追加（C368, C308, 367, 287, 227）
第 8.0.8 版	2016 年 7 月 27 日	記載追加（MFP 内蔵 GW に関するセキュリティー）
第 9.0 版	2016 年 11 月	本書名称変更
第 9. 1 版	2017 年 6 月 28 日	記載追加（モバイル機器との連携におけるセキュリティー、Remote Deployment Tools）
第 9.2 版	2017 年 9 月 5 日	記載追加（World Wide Remote Service Platform に関するセキュリティー）、第 9.1 版修正
第 9.3 版	2017 年 12 月 14 日	対応機種追加（C759, C659, 658e, 558e, 458e, 368e, 308e, C3080, C308P, C3070, C3070P, C3070L）
第 9.4 版	2018 年 12 月	記載追記（MFP 本体内データのセキュリティー：SSD を用いた場合、CS Remote Care に関するセキュリティー： LTE を用いた場合） 対応機種追加（C360i, C300i, C250i, C4050i, C3350i, C3320i, C4000i, 3300i, 4752, 4052）
第 9.5 版	2019 年 7 月	記載削除（PageACSES との連携による機能拡張）、記載追加（CWH に関するセキュリティー、ユーザー情報の保護）、RDT に関する詳細を別紙として追加。
第 9.6 版	2019 年 10 月	対応機種追加（C650i, C550i, C450i, 306i, 266i, 246i, 226i, Accurio Press 6136, 6120, 6136P）
第 9.7 版	2020 年 9 月	記載追加と改定（HDD 及び SSD 廃棄時のデータ完全消去、HDD データ上書き削除機能、全データ削除後のレポート印刷）
第 9.8 版	2021 年 6 月 4 日	記載追加（Fleet RMM）
第 9.9 版	2022 年 4 月 20 日	対応機種追加（4700i, AccurioPress 6272P, C7100, C7090, C4080, 4070, AccurioPrint 2100, C4065）
第 10.0 版	2022 年 9 月 2 日	文言追記（自己暗号化による SSD の保護:”常時”） World Wide Remote Service Platform の章に RSA(Remote Service Agent)を追記
第 10.1 版	2022 年 12 月 2 日	対応機種追加（bizhub C450iS, C360iS, C300iS, C250iS）、FleetRMM 改定
第 10.2 版	2023 年 6 月 12 日	記載追加（MarketPlace に関するセキュリティー） 誤記訂正（①本文・添付資料から古い機種の残存情報を削除、②代替テキスト情報を削除）

版	発行日	改訂内容
第 10.3 版	2023 年 10 月 31 日	Fleet RMM v1.3 リリースに伴う更新 – 個人情報を含むデータから Configuration data (SMB)を削除 – Fleet RMM が使用する通信プロトコル種類とポート番号を更新 – その他、従来の誤記を訂正
第 10.4 版	2024 年 2 月 29 日	下記の記載を追加 – 一時データは MFP の暗号化機能による保護の対象（ただし、SSD の自己暗号化は対象外） – ウイルス検知後動作の選択 – Secure Erase 機能 – 不正アクセス等検出時の通知 – 不正な事象の兆候検知 対応機種追加（bizhub C751i, C651i, C551i, C451i, C361i, C301i, C251i, C4051i, C3351i, C3321i, C4001i, C3301i, 950i, 850i, 751i, 651i, 551i, 451i, 361i, 301i, 4751i, 4051i, 4701i） 対応機種追加（AccurioPress 7136, 7120, 7136P） 古い機種の情報を削除 ◇2024/3/5 下記を修正（10.4.1 版） ・非連続になっていたページ番号を修正 ・「V. 認証装置」項の下記ファイルの URL を修正 U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0

コニカミノルタの製品は、セキュリティーの面においてさまざまな技術を搭載しておりますが、コニカミノルタのセキュリティーポリシーに従ったお客様による正しい運用が前提条件となります。本記載内容を参考に、コニカミノルタの製品を運用いただきたく何卒ご理解の程お願いいたします。各種設定については、ユーザーマニュアルをご覧ください。また、ここに記された内容は万全なセキュリティーを保証するものではないことをあらかじめご了承ください。

用語の定義：

用語	説明
MFP	複合機のことです。
GW	ゲートウェイのことです。
DB	データベースのことです。

商標：

Active Directory はマイクロソフト社の商標です。
Adobe Acrobat はアドビシステムズ社の登録商標です。
FeliCa はソニー株式会社の登録商標です。
Linux は Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

目次

別紙

Remote Deployment Tools 編

Fleet RMM 編

第 1 章 はじめに

ネットワークの基盤が整備され IT が普及した現在社会に於いては、膨大な情報が流通し、ビジネスの中心には様々な形で情報が集まり、より高度な情報資産として姿を変え活用されています。企業活動に於いては、この情報資産を守ること、即ちリスクをマネージすることが重要な課題となります。

本書では、コニカミノルタの各シリーズが提供するセキュリティー基本機能を紹介します。

I. セキュリティー基本方針

1. セキュリティー最新技術の搭載

コニカミノルタは、次項に分類されるさまざまな脅威からお客様の情報資産を守るため、あらゆる角度から、最新のセキュリティー機能を開発・提供します。

① ネットワーク経由の不正アクセスと情報漏洩
② 機器の直接操作による不正使用と情報漏洩
③ 電子情報・紙情報の改竄、複製、消去
④ 人災、機器障害からの情報破壊
⑤ ログ等によるトレース機能

2. 第３者機関による認証取得

コニカミノルタは、セキュリティー機能の実装を客観的に証明する為、平成 16 年 3 月以降の MFP（A4/20 枚機以上のほとんどの機種）において ISO15408 の認証を取得しています。

ISO15408 の認証取得は、初期の Firmware をベースに認証取得を実施します。メンテナンスリリースなどの Firmware をリリースした場合、今後保証継続制度は利用しないこととしますが、セキュリティー機能は、そのまま維持する様に対応します。

また、搭載された暗号モジュールが FIPS140-2 の認証を取得しています。これにより、ソフトウェアが堅牢で安全であることが証明され、FIPS140-2 の認証を必須とする機関への販売が可能になります。

ISO15408 認定取得状況の確認は下記アドレスの IPA の認証製品リストを活用ください。常に最新の情報が掲載され、認証製品リスト一覧のダウンロードが可能です。

認証製品リスト：
https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html (和文)
https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/certfy_list_e31.html (英文)

評価中の製品リスト：
https://www.ipa.go.jp/security/jisec/certified_products/in_eval_list.html (和文)
https://www.ipa.go.jp/security/jisec/jisec_e/prdct_in_eval.html (英文)

第 2 章 機器に関係するセキュリティー項目と対応技術

I. 公衆電話回線に対するセキュリティー

1. FAX 回線に対するセキュリティー

FAX 回線は G3 FAX プロトコルのみを使用した通信であり、これ以外の通信プロトコルはサポートしていません。

公衆回線を通して異なるプロトコルで外部より侵入された場合や、FAX データとしては処理できないデータを送付された場合には、内部のソフトウェア処理でエラーとなり通信は遮断されます。

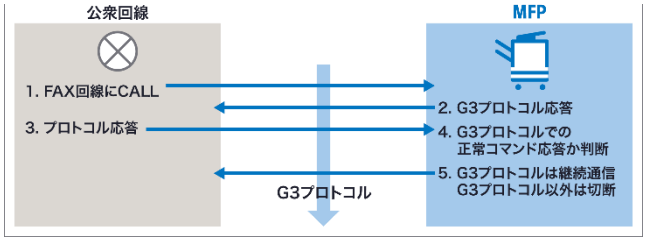


図 1-1

2. 宛先 2 度入力

FAX 送信の宛先を電話番号で入力する場合、再度電話番号を入力し、一致することを確認することで、電話番号の入力間違いによる誤送信を防ぎます。

また、短縮番号へ電話番号を登録する場合にも、再度電話番号を入力し、一致することを確認することで、電話番号の入力間違いによる誤送信を防ぎます。

3. チェーンダイアル

FAX 送信時の宛先入力として、短縮番号やテンキーでの直接入力を組み合わせて行うことができるため、市外番号などを短縮番号に登録して利用することで、誤入力を防ぐことができます。

4. 宛先確認画面表示

送信の宛先（短縮番号、電話番号、等）の入力時に、入力した宛先を再度操作パネルに表示/確認後に送信することで、誤送信を防ぎます。

5. 複数宛先禁止

送信時の宛先入力を 1 宛先のみ許可する設定にすることで、意図しない宛先に送信することを防ぎます。

6. 相手機確認送信

FAX 送信開始時に、相手機から受信する FAX プロトコル信号（CSI）により相手機の電話番号を確認し、一致する場合のみ送信することで、より安全に送信することができます。

II. LAN 接続に対するセキュリティー

1. ネットワークプロトコルに対する対応

ポートごとにプロトコルの ON/OFF の設定が可能です。

必要でないポートは OFF することで外部からの侵入を防止できます。

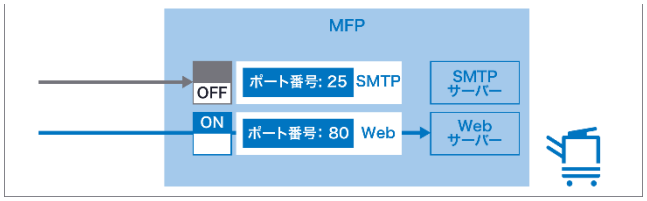


図 2-1

また、IP アドレスのフィルタリング機能を用いて、アクセスを許可するアドレスと許可しないアドレスを指定する事で、アクセスを許可する機器をネットワーク上で選別できます。

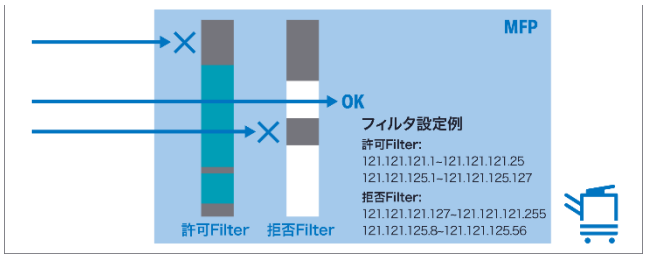


図 2-2

2. ユーザー認証

Active Directory サービスを利用したネットワーク認証機能により、ネットワークを使用した機能に対してユーザー認証が可能です。また、本体を使用する場合であっても、ユーザー認証設定で、Active Directory の認証設定がされている場合には、Active Directory での認証を行います。

予め登録されたユーザーとパスワードの組み合わせで使用権限が与えられます。登録ユーザー以外は装置の使用ができない為、内部データを保護することができます。

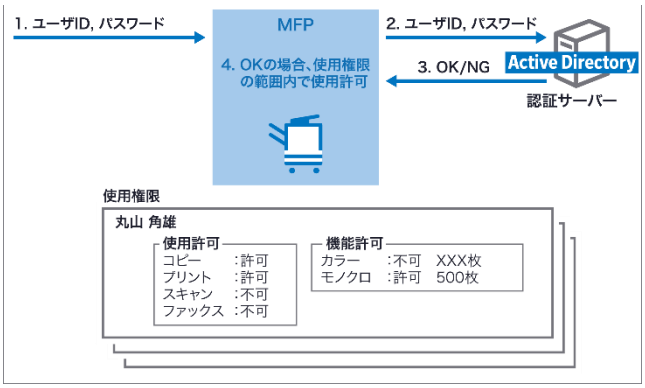


図 2-3

3. ネットワーク経由の装置管理セキュリティー

(1) アドレス帳一括登録時のセキュリティー

ネットワークからのアドレス帳一括登録には、装置の管理者パスワードの入力を必要とします。装置の管理者パスワードが不正であれば登録できません。

この機能により本体に登録されているアドレス帳が一括で改竄されることを防ぐことができます。

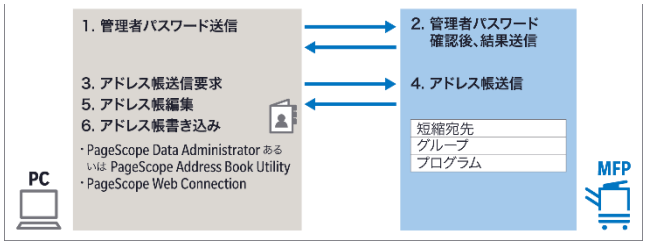


図 2-4

(2) bizhub OpenAPI

bizhub OpenAPI では、SSL/TLS 暗号化プロトコルを使い、ネットワーク越しに装置の情報を取得／設定する事が可能となります。また、bizhub OpenAPI 独自のパスワードを設定する事で、より安全に通信を行う事ができます。

bizhub OpenAPI を使うことにより、PageScope Data Administrator によるユーザー認証情報の設定で装置の安全を守ります。

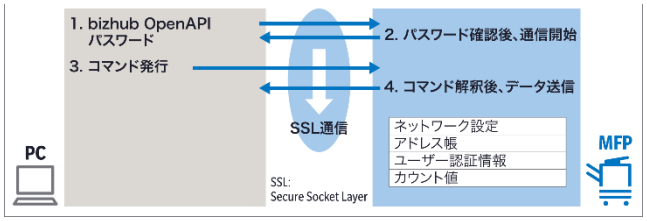


図 2-5

4. データ通信の暗号化

LDAP サーバー、PageScope Data Administrator (或いは Address Book Utility)、PageScope Web Connection と本体間のデータ通信には、SSL/TLS 暗号化プロトコルが用いられます。ネットワーク間でやりとりするデータは暗号化されて保護されます。更に、IPsec を採用する事で、通信プロトコルに依存しない暗号化と IPv6 の対応を合わせた通信の暗号化を行っています。

5. 検疫ネットワーク対応

IEEE802.1X 機能により、LAN への接続段階でネットワーク機器の認証を行い、物理的なポートを対象として、MFP の LAN への接続を管理します。認証は RADIUS (Remote Access Dial In User System) サーバーで行われ、LAN への接続制御はそれに対応したスイッチングハブで行なわれます。本機能により、認証が許可された MFP だけが、LAN 環境への接続が許可されます。

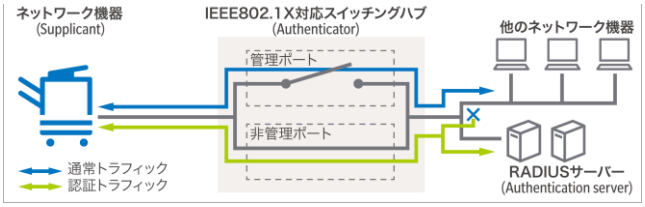


図 2-6

6. 双方向証明書検証

MFP の装置内にある証明書を通信相手に通知し、自身の正当性を証明するだけでなく、通信相手の正当性を MFP 装置自身が検証する事で、双方向で正当性を確認した上で通信制御を行うため、MFP 及び通信相手の「なりすまし」防止ができます。

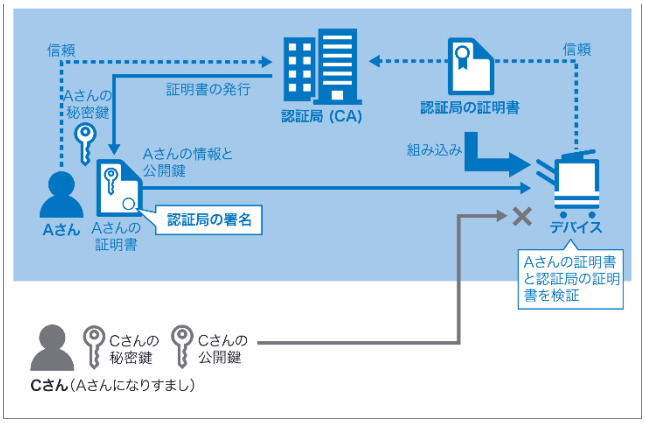


図 2-7

7. ウイルスに対する対応

本体に内蔵しているコントローラの OS には Linux kernel を採用しています。

EFI 社 Fiery のサーバータイプコントローラは、Windows 系の OS を採用していますが、必要な Windows セキュリティーパッチを適時に供給することにより、Windows の脆弱性への対策を行っています。

8. ウイルススキャン機能

ウイルススキャン機能を導入することで、検知したウイルスはすべて除去されます。

送信ジョブでウイルスを検知した場合、そのジョブは削除されます。

一方、受信ジョブでウイルスを検知した場合、従来は、KM 独自の形式に変換する過程でウイルスが消失する為、印刷や BOX への保存などそのジョブを常に実行していましたが、より安心してセキュアな運用も行えるよう、現在はジョブを実行するか否かを選択可能としています。

選択肢	検知したウイルス	ウイルスを検知したジョブの処理	
		送信ジョブ	受信ジョブ
“継続”	削除	削除	実行
“自動判定”	削除	削除	削除 (除.FAX･E-mail)
“削除”	削除	削除	削除

9. 外部からの USB メモリを介したウイルスへの対応状況

USB メモリを介してのウイルスは USB メモリを指しただけで実行されてしまいウイルス感染するケースが主ですが、MFP には USB メモリを指しただけで実行ファイルを起動するといった仕組みがありませんので、これらのウイルスによる影響はありません。

MFP には USB メモリを接続し、USB メモリの画像データをプリントする、またスキャンした画像データやボックスに保存された画像データを USB メモリに保存する機能がありますが、これらの機能はユーザーの操作によって実行されるもので、自動で実行されるものではありません。

10. Linux kernel の定常的監視

Linux kernel については、脆弱性公開情報、及びセキュリティーパッチの有無を定常的に監視し、公開された脆弱性が MFP 機能に影響しないか確認しています。

11. USB インターフェースパスとの分離

USB インターフェースのパスとネットワークのパスは、システム構造的に分離されています。インターネットに接続している PC に MFP を USB で接続しても、MFP は PC 越しにインターネット環境からアクセスされることはありません。

12. 無線 LAN と有線 LAN との通信分離

MFP には無線 LAN と有線 LAN の間のルーティング機能は搭載されていません。そのため、モバイル端末等から無線 LAN を経由して MFP の有線 LAN に接続された機器にアクセスされることはありません。

III. MFP 本体内データのセキュリティー

1. 画像処理及び出力処理におけるセキュリティー

スキャナから読み込んだ／Fax 基板から受信したデータは画像処理後に圧縮され、本体内のメモリ（揮発性のメモリ）に書き込まれます。さらにプリントデータは伸張処理後にプリンターへ送られ用紙上にプリントされます。

データは、1 ページごとの出力と、HDD または SSD 内に一時的に蓄えた後の一括出力が選択できます。1 ページごとの出力は、データがメモリ上に重ね書きされるため、再出力は不可能です。

「2. HDD 一時保存データ上書き削除機能」が有効になっている時には、出力完了や転送完了と同時にメモリからジョブデータ（圧縮データ）が削除され、第三者による再出力、再転送を防止します。

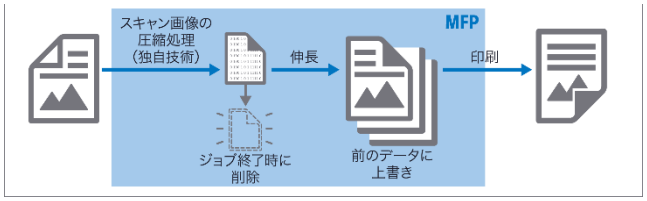


図 3-1

HDD 内に蓄えられる場合、「5. HDD、SSD 及び microSD 内データの暗号化による保護」が有効になっている時、ジョブデータは、独自の圧縮処理に加え、全て暗号化して保存されますので、万一 HDD を取り出されてもデータの機密性は保持されます。

セキュアプリント機能を使用した場合、プリントジョブは本体内のメモリに一旦保存され、本体のパネルでパスワードが入力されてからプリント動作を開始します。この機能により、本人以外がプリント用紙を持ち去ることを防止します。

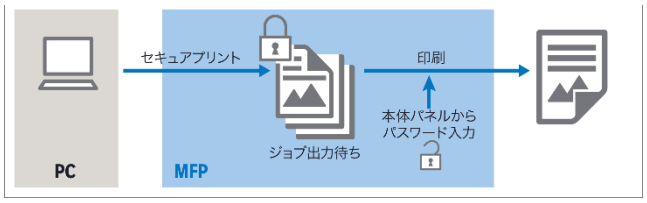


図 3-2

2. HDD 一時保存データ上書き削除機能

■HDD (Hard Disk Drive)

HDD 上書き削除機能の設定により、ハードディスクに一時的に保存されたデータは、プリントやスキャンなどのジョブの完了、ボックス保存文書の削除操作など、画像データの利用終了時に上書き消去されます。ハードディスク上の不要になった画像データが再利用されるリスクを軽減できます。

[モード 1]

1. 0x00 で上書き

[モード 2]

1. 0x00 で上書き
2. 0xff で上書き
3. 文字「a」(0x61)で上書き
4. 検証

参考：

SSD (Solid State Drive) では HDD データ上書き削除機能はサポートされていません。SSD で使われるフラッシュメモリは直接データを書き換えることができません。データを書き換えるには、消去してから書込む必要があります。また、書込みはページという単位で行いますが、消去は複数ページで構成されるブロックという単位で行います。

新しくデータを書き込む時は、ウェアレベリング機能(※) により、前回データが記録されたセルを避けて書き込まれます。データの消去はガベージコレクション機能（※）によりブロック単位の空きが作られて消去されます。しかし、書き込まれるデータは KM 独自フォーマットで圧縮されているので、意味ある情報を復元することはできません。MFP の暗号化機能が有効の場合、データは圧縮された後、暗号化されます。

※ ウェアレベリング機能：

SSD、microSD では、フラッシュメモリのセルにデータを記録します。同一セルを偏って使用し続けるとセルが劣化します。セルの利用を平滑化して SSD、microSD の寿命を延ばすために、SSD、microSD に内蔵されたコントローラが自動的に利用セルを変更します。そのため、通常は SSD、microSD 利用者は特定のセルを指定してデータを書き込むことはできません。

※ ガベージコレクション機能：
　ガベージコレクション機能では、データを書込むことができるページを増やすために、自動的に不要なデータのみのブロックをつくり効率よくデータを消去しておきます。このときに、有効なデータは別のブロックに移動されます。

3.　HDD、SSD 及び microSD 廃棄時のデータ完全消去

■HDD (Hard Disk Drive)

ハードディスクの内部データは、設定により乱数などの上書きで消去できます。ハードディスク及び MFP 本体を廃棄した後に機密が漏洩することを防止できます。

ハードディスクにはディスク上の残留磁気（※）により前のデータの痕跡が残っている可能性があります。より確実にデータを消去するために、複数回上書きをおこなう方法も実装されています。

※残留磁気：
　HDD はディスク上に塗布された磁性体を、磁気ヘッドで磁化する事でデータを記録する方式です。
　新しくデータを書込んでも各ビットに相当する箇所の磁性体の塊が境界を境にすべて同じ方向に向かないため、前の情報の痕跡が残留磁気として残ります。
　そのため、通常の HDD 利用では閾値を用いて 1/0 の判断をおこないます。

[モード 1]：JEITA 推奨 / ロシア標準方式
1. 0x00 で上書き

[モード 2]：米国国家安全保障局方式（NSA 標準）
1. 1 バイトの乱数で上書き
2. 1 バイトの乱数で上書き-0x00 で上書き

[モード 3]：米国コンピュータセキュリティセンタ方式（NCSC-TG-025）/ 米国海軍方式（NAVSO P-5239-26）/ 米国国防総省方式（DoD5220.22-M）
1. 0x00 で上書き
2. 0xff で上書き
3. 1 バイトの乱数で上書き
4. 検証

[モード 4]：米国陸軍方式（AR380-19）
1. 1 バイトの乱数で上書き
2. 0x00 で上書き
3. 0xff で上書き

[モード 5]：旧米国国家安全保障局（NSA 標準）
1. 0x00 で上書き
2. 0xff で上書き
3. 0x00 で上書き
4. 0xff で上書き

[モード 6]：北大西洋条約機構標準方式（NATO 規格）
1. 0x00 で上書き
2. 0xff で上書き
3. 0x00 で上書き
4. 0xff で上書き
5. 0x00 で上書き
6. 0xff で上書き
7. 1 バイトの乱数で上書き

[モード 7]：ドイツ標準方式（VSITR）
1. 0x00 で上書き
2. 0xff で上書き
3. 0x00 で上書き
4. 0xff で上書き
5. 0x00 で上書き
6. 0xff で上書き
7. 0xaa で上書き

[モード 8]：米国空軍方式（AFSSI5020）
1. 0x00 で上書き
2. 0xff で上書き
3. 0x00 で上書き
4. 0xff で上書き
5. 0x00 で上書き
6. 0xff で上書き
7. 0xaa で上書き
8. 検証

■SSD (Solid State Drive)、microSD

"全領域上書き削除"により 0x00 を書き込みます。

HDD などの磁気データとは異なり、SSD、microSD で使われるフラッシュメモリのデータは 1 回の上書きで完全に消去が可能です。

SSD、microSD ではウェアレベリング機能により、0x00 書込み時にアクセスできない箇所がありますが、それは論理アドレスで指定できない箇所のため、そのデータを読み出すことは困難です。

また、「5. HDD、SSD 及び microSD 内データの暗号化による保護」の機能を使えば、"全領域上書き削除"で上書きできなかったデータも含めて、全てのデータの漏洩を防ぐことが出来ます。

より厳密に「完全消去」が求められる場合、Format NVM command（Secure Erase）による消去を行うことができます。この消去方法は NIST SP800-88 Rev1 の Purge レベルに準拠しており、データの復元は完全に不可能になります。消去後にはその証明となるログが出力されます。

※なお、本機能の実施につきましては、実施後に装置の起動が出来なくなる為、サービス管理店へご用命ください。

4. 全データ削除後のレポート印刷

データ消去後に結果報告のレポートを印刷できます。

5. HDD、SSD 及び microSD 内データの暗号化による保護

コニカミノルタの MFP はデータの暗号化を 2 つの方法のどちらか、または両方で行います。

・SSD の自己暗号化機能を利用する

・MFP の暗号化機能を利用する

どちらの暗号化も AES256 で行います。暗号鍵は MFP の電源投入時にコニカミノルタ独自の鍵生成アルゴリズムで生成されます。そのため、MFP から取り外した HDD、SSD、microSD のデータを復元することはできません。

6. 自己暗号化による SSD の保護

SSD を搭載するコニカミノルタの MFP は、自己暗号化 SSD を採用しています。

自己暗号化 SSD では SSD 内で生成される暗号化鍵（DEK: Data Encryption Key）を用いて、常時、SSD 内データを暗号化します（一時保存データは除く）。この DEK 自体も MFP の生成する認証鍵（AK: Authentication Key）で暗号化することで、SSD 内データを保護しています。

AK はロックパスワードを用いて MFP 電源投入時に生成されます。さらに AK は SSD 自体を利用するための認証にも使われます。

7. PDF ファイルの暗号化

本体でスキャンしたデータを PDF 形式のファイルで保存する際、共通鍵による暗号化ができます。

暗号化した PDF ファイルを Adobe Acrobat で開く時には、共通鍵の入力が必要となります。

図 3-3

8. ユーザー認証

本体に搭載した認証機能、Active Directory などの外部サーバーや PageScope Authentication Manager を利用する認証をサポートしています。パスワードによる認証のほか、PageScope Authentication Manager を利用して非接触 IC カードや生体情報による認証が可能です。

MFP のコピー、プリント、スキャン、FAX の機能やカラー機能の利用に関し、本体の使用権限をユーザー認証と組み合わせて制限することができます。また、権限レベルによってアクセス可能な FAX や E-mail などの登録宛先を制限することができます。

(1) 外部サーバーを使用して認証を行う事が可能ですが、ネットワーク上に外部サーバーを用意できない場合でも、装置内部に認証機能を持つためユーザー認証機能が可能です。

(2) ユーザー単位や部門単位で出力枚数データの上限値を設定して使用制限を管理できます。

(3) カラーとモノクロ別に出力権限や上限値を設定する事も可能です。

設定された時間内に設定された回数の認証失敗が発生した場合、パスワード攻撃の可能性があると判断し、それをジョブログに記録すると共に管理者に SNMP Trap もしくは E-mail で通知します。これにより不正アクセスの兆候を早期に察知できます。

同様に、設定された時間内に設定された回数の認証要求があった場合※、認証アクセス攻撃の可能性があると判断し、ジョブログに記録すると共に管理者に SNMP Trap もしくは E-mail で通知します。また、認証応答を遅延させます。これにより攻撃の兆候を早期に察知するとともに、装置の負荷増大／動作停止を回避します。※認証の成否は問いません。

9. ボックスのセキュリティーとその活用

ボックス内のデータを安全に守るために、ユーザー認証に加えてボックスへのアクセスもパスワードで保護しています。

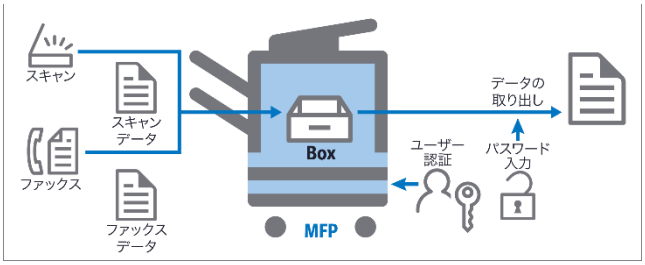


図 3-4

10. メールデータの暗号化

MFP にてメールを発信するにあたり、受信者の証明書（公開鍵：アドレス帳への登録が可能）を使ってメールを暗号化し、受信者は PC 上で自分の秘密鍵を使ってメールを復号する事ができます。

これにより、メールの内容を他人に傍受される事なく、安全な送受信が可能になります。ネットワーク上から公開鍵を取得するには、LDAP サーバーに登録された証明書を使用します。

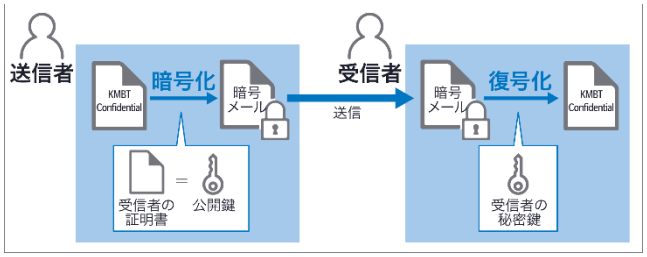


図 3-5

11. メールの署名機能

送信者は MFP の秘密鍵でメールに署名をつけ、受信者は MFP の証明書で署名の検証を行います。これにより、受信者は、改竄が無いことを検証する事ができます。

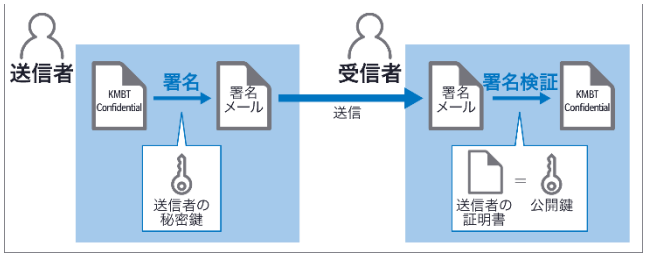


図 3-6

12. Scan to Me, Scan to Home & Scan to Authorized Folder

スキャンデータの自分宛への送信が簡単に利用できます。

ユーザー認証を設定している場合、登録宛先の欄に「Me」のボタンと、管理者設定で機能を有効にすることにより「Home」のボタンが表示されます。

宛先の「Me」を選択した場合は、認証されている利用者の E-mail アドレスへ送信し、「Home」を選択した場合は、あらかじめ登録された PC フォルダーへ送信するので、ワンタッチで簡単かつ確実なファイル送信が行えます。

SMB 宛先の［ユーザーID］と［パスワード］の欄に何も登録しないでおくことで、ログインしたユーザーが、自分の SMB 宛先をアドレス帳から選択して送信する場合に、ユーザー認証のユーザー名とパスワードをそのまま使用しますので、SMB の認証を自分以外の SMB 宛先の利用を制限することができます。

また、管理者設定により宛先の登録範囲や直接入力を制限・禁止することで、送信先を管理者が管理している宛先のみに送信できるように規制をかけることができます。

図 3-7

13. 監査ログによるアクセス管理

セキュリティー機能の動作に関する履歴を監査ログとして保存します。不正なアクセスに対して、トレースすることができます。

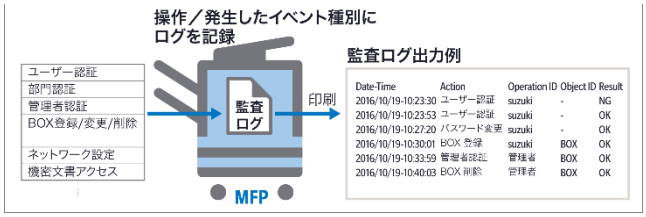


図 3-8

また、ログイン操作や設定変更などの情報を記録したログを Syslog プロトコルで送信することができます。これにより複合機を他の IoT 機器と共に SIEM (Security Information and Event Management）製品で統合的に管理することができます。ログの形式は CEF/LEEF に対応しています。

また、意図しないインシデントにつながる操作などを検知した時に、SNMP trap もしくは e-mail でそれを管理者に通知することが可能です。SIEM 製品が導入されていない環境でも早期に不正な事象に対処できます。

14. 認定を受けた暗号モジュールの採用

MFP 内部には OpenSSL 等の暗号モジュールを搭載し、暗号化や認証機能を提供してきました。FIPS140-2 の認定を受けた暗号モジュールを利用している主な機能は、下記になります。

(1) スキャンデータ配信時の暗号化通信
- Scan to WebDAV, TWAIN 等の SSL/TLS 通信時
- Scan to E-mail の S/MIME 送信時

(2) PSWC の SSL/TLS 通信時

(3) PDF 暗号化ファイル生成機能

15. TPM によるデータ保護

(1) 目的

MFP 内の物理的解析やネットワークパケットの盗聴によってパスワードなどの情報が悪意のあるユーザーに漏えいすると、MFP が不正アクセスされ、内部の重要データが流出する恐れがあります。

TPM 内で生成した鍵（=ルート鍵）は、TPM 外に取り出すことが出来ないため、ルート鍵を用いて暗号化したデータは、復号時に必ず TPM チップが必要となります。TPM を用いることで、パスワードなどの情報が漏えいすることを防ぐことができます。

保護対象データ：
1. 管理者が登録する証明書
2. 管理者パスワード、および管理者が設定するパスワード
3. MFP がサーバーとしてサービスを提供する時に設定されるパスワード

(2) TPM による保護のしくみ

通常、MFP 内にあるパスワードなどの情報は、漏えいを防ぐために、AES 鍵（256bit）と RSA 鍵（2048bit）を用いて保護しています。TPM によるデータ保護を有効にすると、下図のように、TPM のルート鍵を用いて、RSA 鍵を暗号化します。

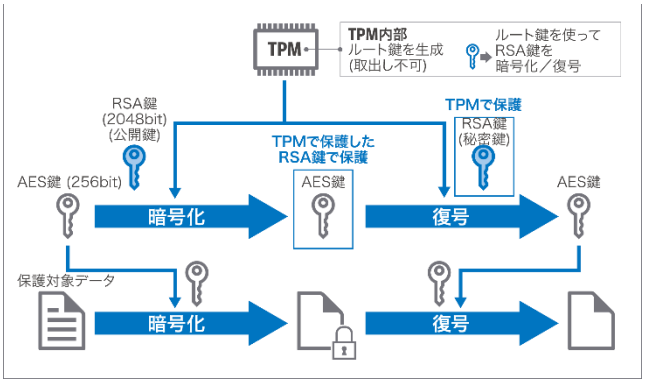


図 3-9

ルート鍵は TPM 内から取り出すことが出来ないため、RSA 鍵を復号するには TPM チップが必要となります。RSA 鍵が復号できない場合は、AES 鍵も復号できず、その結果、パスワードなどの保護対象データも復号できません。

したがって、TPM を用いることで、悪意のあるユーザーが、パスワード情報などを解析、盗聴しようとしても、TPM チップが無ければ暗号化したデータを復号できないため、パスワード情報などの漏えいを防ぐことができます。

(3) TPM 鍵のバックアップ

TPM チップの故障に備えて、事前に USB メモリなどに RSA 鍵をバックアップしておくことで、暗号化しているデータを救済することができます。セキュリティー上、RSA 鍵は暗号化するなど安全に保管してください。

IV. 出力データのセキュリティー

1. コピーセキュリティー機能

(1) コピープロテクト印字機能

コピーやプリントによる出力文書（原本）に地紋を埋め込み、複製文書には“コピー”などの模様を浮かび上がらせる事で、明確に原本と複製との区分ができます。

また、出力に使用された MFP のシリアル No や出力日時を地紋に設定する事もできます。シリアル No と出力日時が入った複製文書と上記の監査ログとの組み合わせで不正コピーを行ったユーザーの特定が可能です。

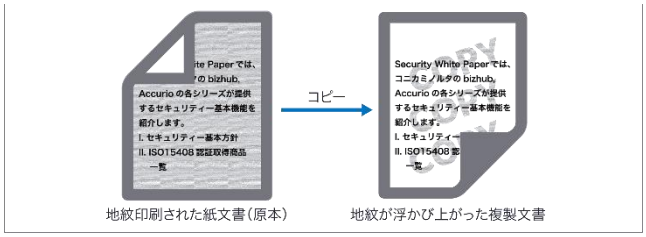


図 4-1

(2) コピーガード機能／パスワードコピー機能

コピーガード機能では、コピーやプリント時に特殊な地紋セキュリティーパターンを付加して出力した原稿を 2 次コピーしようとしても、コピーが禁止されているというメッセージが出てコピーされません。

また、パスワードコピー機能では、予め設定しておいたパスワードを入力した場合に限り、地紋セキュリティーパターンを付加した 2 次コピーが許可されます。

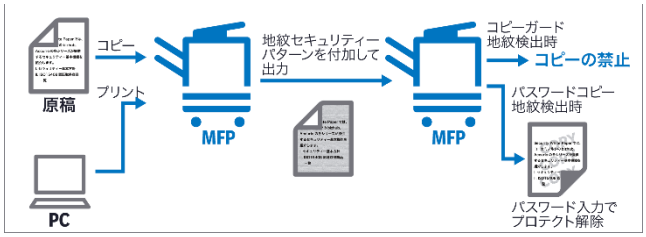


図 4-2

V. 認証装置

1. 生体認証装置のデータに関するセキュリティー

生体認証装置（AU-101/102）のデータは非常に高いセキュリティーで管理されている為、不法に利用することは不可能です。

● 生体データとしての指静脈

静脈は体内にあり、指紋の様に不用意に読み取られる事はありません。従って、偽造する事は非常に困難です。

● 本システムで採用しているデータ処理方法

このシステムは、「U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0」に基づくセキュリティーガイドラインに対応しています。種々の重要なセキュリティー/プライバシーに関する仕様をこのシステムで対応しています。

● 生体データの再現

HDD には（登録時の）読み取りデータの特徴に基づき算出された乱数データが登録されます。HDD 内のデータから元の静脈データを再現する事は理論上不可能です。

● HDD 内のデータ構造

HDD 内のデータ構造は公にされていません。従って、偽造やなり済ましは不可能です。

● 認証装置内にデータ消去

装置内のデータは、RAM に一時的に保管される際に暗号化され、MFP に転送された後、消去されます。

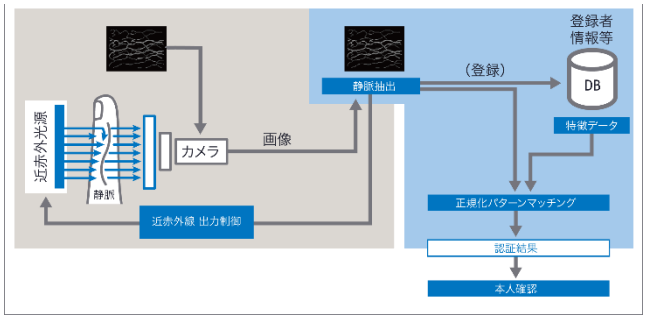


図 5-1

※ U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0：
https://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_mr_v1.0.pdf 参照

2. 認証&プリント（ワンタッチセキュリティープリント）

ユーザー認証機能との連携により、シンプルで機密性の高いプリント作業が実現します。プリント出力物が、他人に持ち去られたり、覗き見されたりすることはなくなります。また、生体認証装置やカード認証装置を利用することで、認証が簡単に行えます。

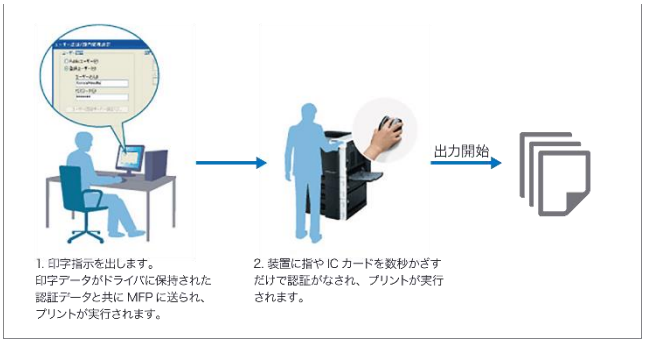


図 5-2

VI. モバイル機器との連携におけるセキュリティー

コニカミノルタでは、モバイル端末と MFP/プリンターを連携する様々なセキュリティーを提供しています。それぞれのセキュリティーの概要と情報セキュリティーの脅威と回避策を説明します。

1. AirPrint に対するセキュリティー

AirPrint は iOS の標準印刷機能です。アプリケーションやドライバのインストールが不要で、簡単な操作でアプリケーションからプリントできます。セキュリティー脅威と回避策を以下に説明します。

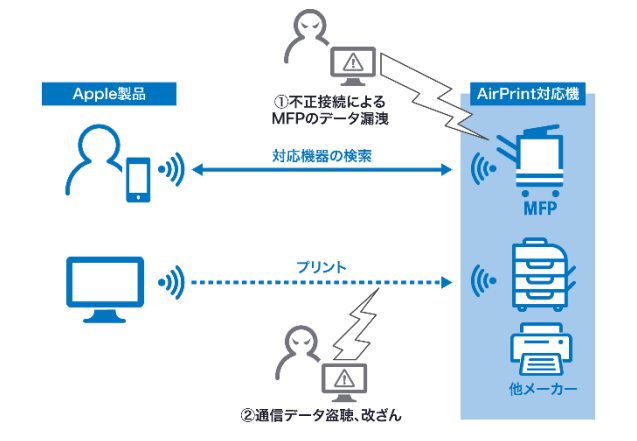


図 6-1

脅威	回避策
① 不正接続による MFP のデータ漏洩	IPP 認証による不正接続防止
② 通信データ盗聴、改ざん	SSL/TLS 通信によるデータ暗号化

2. Mopria に対するセキュリティー

Android 端末に Mopria のプラグインをインストールすることで、簡単な操作でアプリケーションからプリントできます。セキュリティー脅威と回避策を以下に説明します。

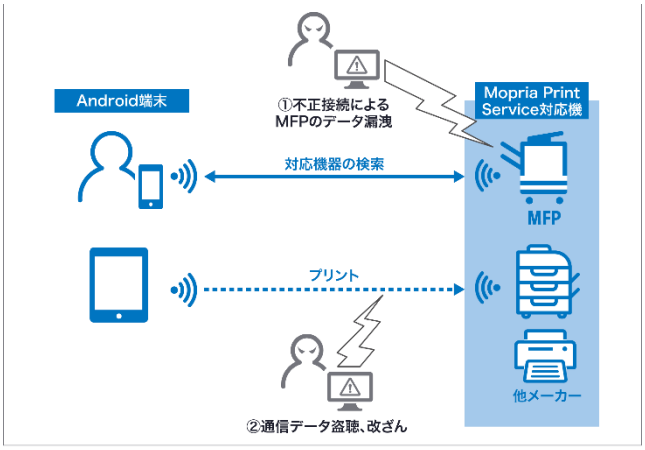


図 6-2

脅威	回避策
① 不正接続による MFP のデータ漏洩	IPP 認証による不正接続防止
② 通信データ盗聴、改ざん	SSL/TLS 通信によるデータ暗号化

3. Google Cloud Print に対するセキュリティー

Google Cloud Print はインターネット経由で MFP からプリントするサービスです。セキュリティー脅威と回避策を以下に説明します。

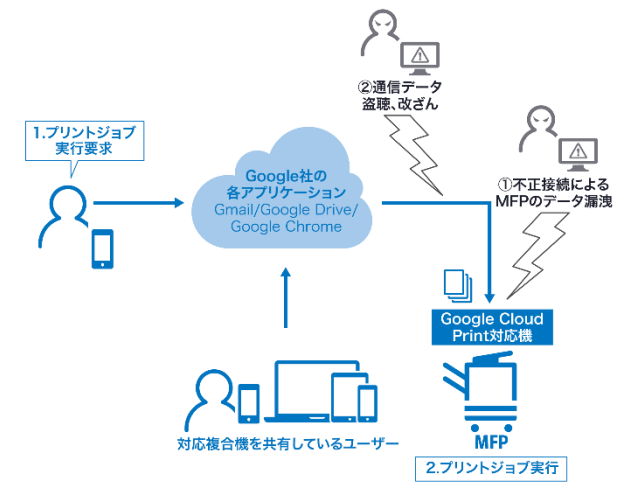


図 6-3

脅威	回避策
① 不正接続による MFP のデータ漏洩	IP フィルタリング設定によるアクセス制限
② 通信データ盗聴、改ざん	・本体無線の「WEP」や「WPA」などの認証によるデータ保護 ・SSL/TLS による通信データ暗号化

4. Konica Minolta Print Service に対するセキュリティー

Konica Minolta Print Service は Android 端末にコニカミノルタのプラグインをインストールすることで、MFP からプリントするサービスです。セキュリティー脅威と回避策を以下に説明します。

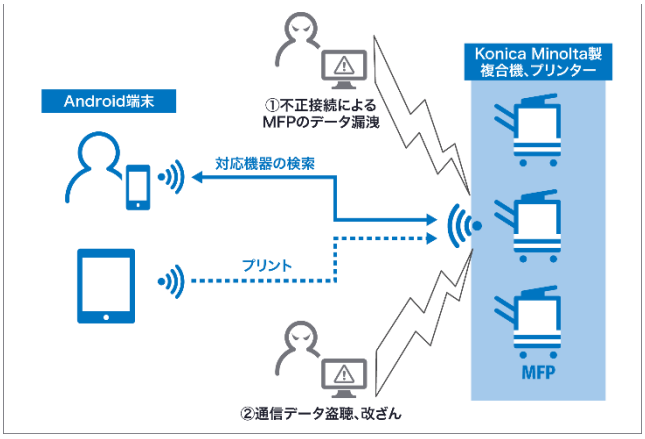


図 6-4

脅威	回避策
① 不正接続による MFP のデータ漏洩	IP フィルタリング設定によるアクセス制限
② 通信データ盗聴、改ざん	本体無線の「WEP」や「WPA」などの認証によるデータ保護

5. Konica Minolta Mobile Print, PageScope Mobile に対するセキュリティー

Konica Minolta Mobile Print, PageScope Mobile は Wi-Fi を利用して、モバイル端末内またはオンラインストレージ上のドキュメントや Konica Minolta Mobile Print, PageScope Mobile で閲覧している Web ページやメールの内容を MFP からプリントします。セキュリティー脅威と回避策を以下に説明します。

- Konica Minolta Mobile Print, PageScope Mobile によるスキャン、プリント

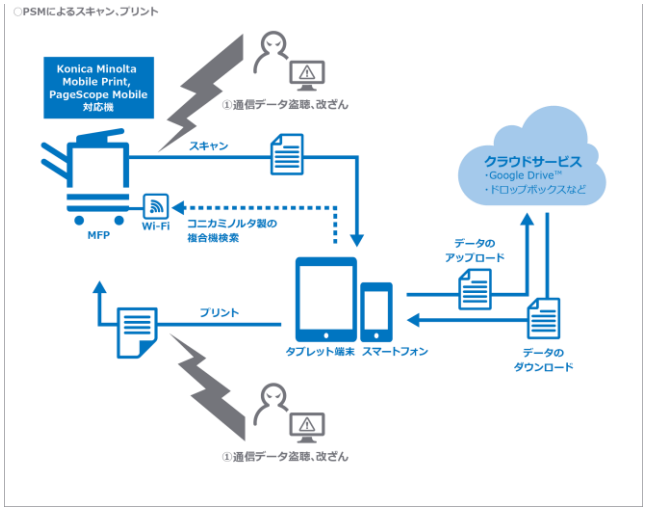


図 6-5

- NFC、Bluetooth LE や QR コード読み取りによるペアリング

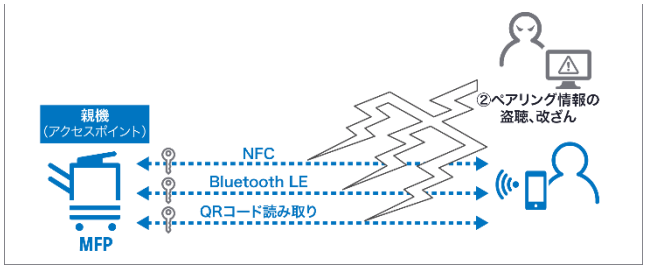


図 6-6

- NFC 認証

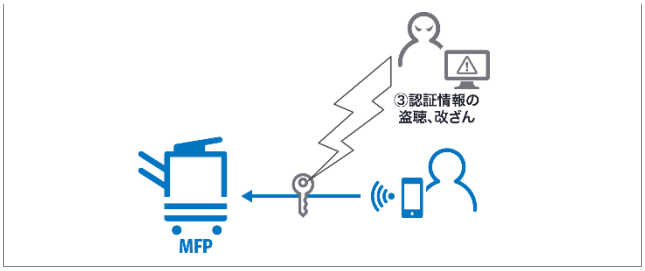


図 6-7

脅威	回避策
① 通信データ盗聴、改ざん	本体無線の「WEP」や「WPA」などの認証によるデータ保護
② ペアリング情報の盗聴、改ざん（NFC、Bluetooth LE、QR コード）	秘密鍵によるデータ暗号化
③ 認証情報の盗聴、改ざん（NFC）	秘密鍵によるデータ暗号化

VII. PKI カード認証システム

<概要>

PKI カードは暗号化/復号化、電子署名の機能を持ったカードです。このカードと MFP の機能を連携させることにより、セキュリティーレベルの高い MFP の使用環境を構築することができます。

1. PKI カードを使用したログイン

カードリーダーに PKI カードを挿入し、PIN を入力すると、Active Directory への認証を実施します。その際、Active Directory から MFP に送られてくるデジタル証明書を MFP で検証することができます。

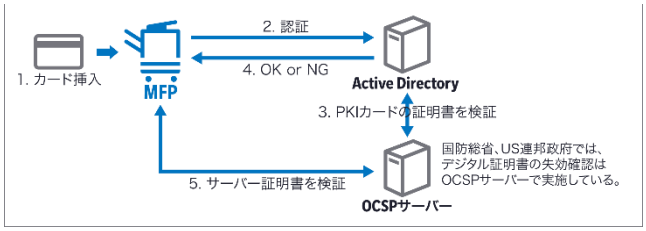


図 7-1

2. PKI カードを使用した LDAP 検索

LDAP サーバーで宛先検索を行うときに、Active Directory 認証で取得した Kerberos 認証チケットを使用して LDAP サーバーにログインします。一度の認証でアクセスできるため、利便性の高いシングルサインオン環境を構築することができます。

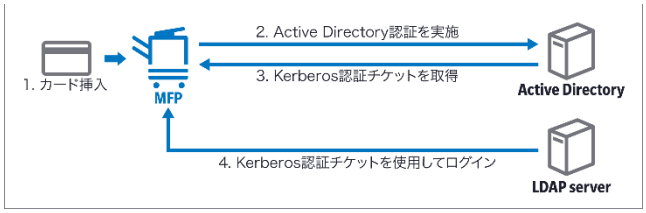


図 7-2

3. PKI カードを使用した SMB 送信

スキャンしたデータを SMB 送信するときに、Active Directory 認証で取得した Kerberos 認証チケットを使用して宛先のコンピューターにログインします。1 度の認証でアクセスできるため、利便性の高いシングルサインオン環境を構築することができます。また、認証チケットを使用することで、ネットワーク上にパスワードを流さない運用が可能になるため、安全に SMB 送信を行うことができます。

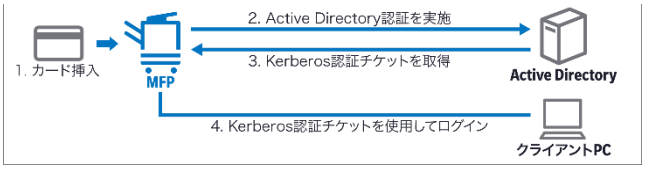


図 7-3

4. PKI カードを使用した E-mail 送信（S/MIME）

E-mail 送信時に PKI カードを使用してデジタル署名を実施することができます。デジタル署名を実施することにより、E-mail の送信元を証明することができます。

また、宛先の証明書が登録されていれば、E-mail の暗号化を組み合わせて送信することもできます。E-mail を暗号化して送信することで、伝送経路上での第 3 者への情報漏洩を防止できます。

図 7-4

5. PKI カードプリント

プリンタドライバから印刷データを PKI カードで暗号化して MFP に送信します。印刷データは MFP の PKI 暗号化ボックスに蓄積され、同じユーザーが MFP で PKI カード認証を実施することで、復号化してプリントすることができます。印刷データは、MFP で PKI カードによる認証が成功してはじめてプリントが可能になるため、データの機密性を保持することができます。

図 7-5

6. Scan to Me / Scan to Home

スキャンしたデータを自分の E-mail アドレスやコンピューターに送信する機能です。自分の E-mail アドレスや Home フォルダーのパスは Active Directory 認証時に取得するので、簡単に送信することができます。

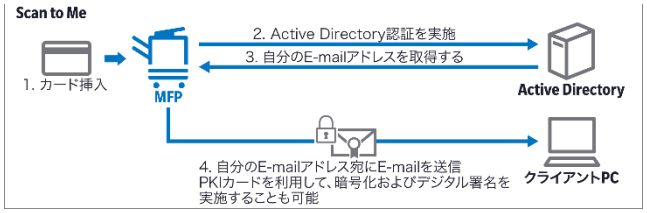


図 7-6

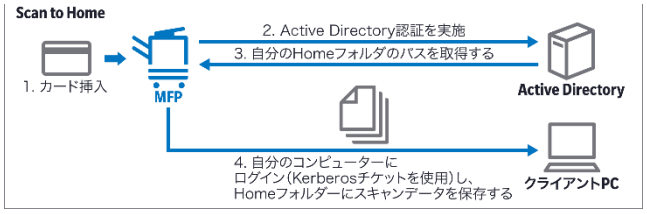


図 7-7

VIII. MFP 自己保護に関するセキュリティー

1. Firmware 検証機能

MFP 本体 Firmware の書き換え時に、Firmware データが改ざんされていないかハッシュ値チェックを行います。ハッシュ値が一致しない場合は警告を出し、Firmware 書き換えを行いません。
また、セキュリティー強化モードを利用している場合、主電源 ON 時にもハッシュ値チェックを行います。ハッシュ値が一致しない場合は警告を出し、MFP 本体の起動を禁止します。
Firmware データのハッシュ値は電子署名されたハッシュ値と比較されます。
FW データは非公開です。また、顧客の管理者が Firmware の書換えを禁止設定にしている場合、コニカミノルタのサービスマンもアップデートできなくなるため、第三者による書換えもできません。

IX. CS Remote Care に関するセキュリティー

1. 基本的なセキュリティーと収集データ

CS Remote Care (以下 CSRC) は、本体と CSRC ホストとの間で通信を行って本体データを送信したり、本体の設定を変更したりします。
遠隔診断システムで通信を行うには、CSRC ホストとデバイスの双方にあらかじめ登録した ID を使って、接続通信を行います。この通信では CSRC ホストの登録内容とデバイスの送信内容とが一致するかを確認し、通信が正常終了すると、以降、遠隔診断通信を行うことが可能な状態になります。遠隔診断通信は、通信毎に ID を確認の上、通信を行います。通信時に ID が合致しないと通信を行いません。
また、CSRC が収集するデータは、カウンタ値などのサービス情報のみであり、FAX 宛先や個人情報に関係する内容は含まれません。
公衆回線を使用した通信手順を示します。

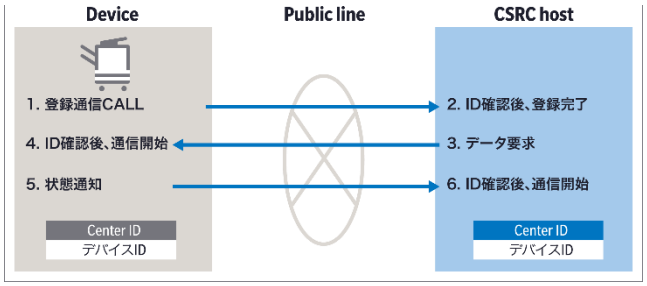


図 9-1

2. LTE を用いた場合のセキュリティーについて

MFP に接続される LTE 端末は内臓 SIM が閉域網としか通信できません。また、「LTE ゲートウェイサーバ」が MFP に接続されている LTE 端末かどうかを ID 認証しているため、予め許可した LTE 端末しか通信できません。
LTE 端末から基地局との空中通信のセキュリティーは AES と SNOW3G を用いた暗号化によって安全性を確保しています。

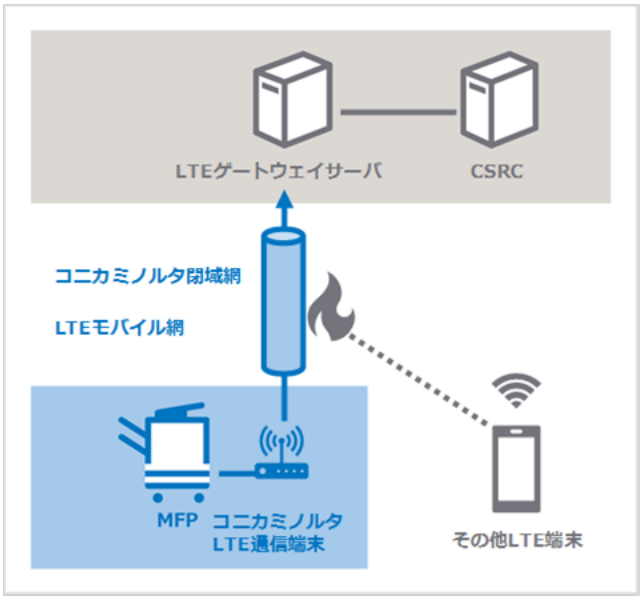


図 9-2

3. メールでのセキュリティー

● 送信データ暗号化

本体および CSRC ホストで暗号鍵(共通鍵)を使用し、データを暗号化します。
※本体およびセンターで暗号化可否設定可能
共通鍵暗号方式では、本体とセンターの暗号化と復号で同じ鍵を使用しています。
これにより、メールの内容を他人に傍受される事なく、安全な送受信が可能になります。

● ID などの確認

送受信メールには、送信元や送信先が確認可能な情報（センターID やシリアル No）が含まれています。この情報が合致するか確認を行い、正しい送受信先かどうか確認しています。また、センターから送信されたメールには、メール ID が割り振られています。
MFP からの応答メールには、応答元メールのメール ID が利用されています。センターが送信したメール ID と一致するかチェックし、ID の確認を行います。

● 不正メールの排除

上記の ID などの確認で、送信元や送信先が確認可能な情報(センターID やシリアル No）やメール ID が一致しなかった場合、その送受信メールは不正データと見なし、データ登録は行わずに排除します。

4. HTTP 通信でのセキュリティー

● 送信データ暗号化

前項のメールと同じく、本体および CSRC ホストで暗号（共通鍵）を使用し、データを暗号化します。
共通鍵暗号方式により、デバイスと CSRC ホストの暗号化と復号で同じ鍵を使用しています。

● CSRC と MFP 間の通信

HTTP 通信における CSRC と MFP 間の全ての通信は、それぞれコニカミノルタのライセンス管理サーバー（LMS）が発行した証明書を使い、クライアント、サーバー認証（プロダクト認証）による HTTPS（TLS）通信を行います。LMS が発行した証明書を持った MFP のみ通信が可能ですので、なりすましがない、セキュアな通信を行っています。
TLS では、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティー技術を組み合わせ、データの盗聴や改ざんを防いでいます。

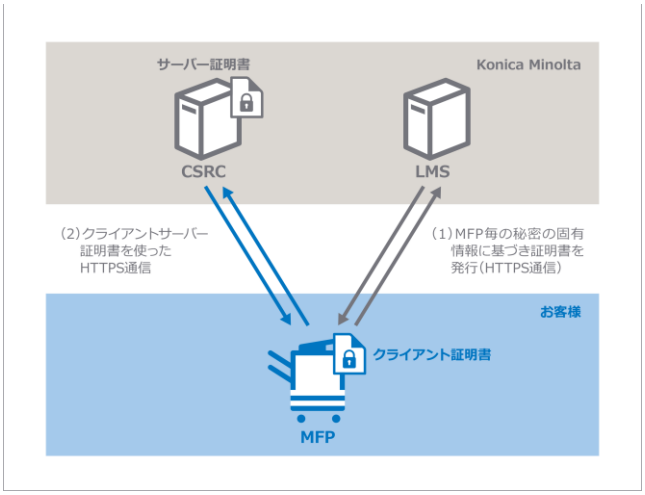


図 9-3

5. DCA でのセキュリティー

● DCA-デバイス間の SNMPv3 通信

DCA（Device Collection Agent）では、装置との通信方法として SNMPv1 と SNMPv3 通信をサポートします。
SNMPv1 通信では、平文のデータがネットワーク経路上を流れるため、外部からパケットをキャプチャされてしまう可能性がある環境の場合、通信中のデータが盗聴されてしまう危険性があります。
また、SNMPv1 通信における唯一の認証である「コミュニティ名」も同時に漏れてしまうため、流出した「コミュニティ名」で管理されている装置の MIB に格納されたすべてのデータにアクセスすることが可能となってしまいます。
SNMPv3 通信では、SNMPv1 通信のコミュニティ名に相当する「ユーザー名」に加え、認証のための仕組みが追加されており、装置へのアクセスに対して堅牢性を高めます。また、通信経路を流れるデータはすべて暗号化されており、同じ暗号化方式・暗号鍵を知らない限り、データを盗聴することは困難になります。

● DCA-CSRC ホスト間の通信

DCA と CSRC ホストとの間の通信は、HTTP プロトコル上で SSL/TLS を使用して、暗号化通信をしています。
また、DCA には固有の ID が割り当てられ、通信毎にこの ID を確認の上、データ転送を行います。
通信時にこの ID が一致しない場合、データ転送は実施されないようになっています。

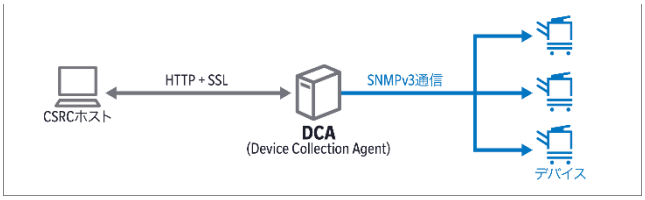


図 9-4

X. bizhub Remote Panel に関するセキュリティー

1. 通信、接続トリガー

bizhub Remote Panel は必ず SSL/TLS による暗号化を行う HTTPS で通信します。
また、bizhub Remote Panel Server 側からデバイスに接続することはできず、デバイス側からのみ接続できるため、顧客のセキュリティーを確保します。

2. 認証

第三者機関である CA (認証局) が発行した証明書をデバイスと bizhub Remote Panel Server に設定して通信を行うことで、さらにセキュリティーの高い通信を行うことができます。

3. Access Code

bizhub Remote Panel Server は、複数のデバイス、複数の Client (ユーザー) が同時に接続して使用することができます。ユーザーは、複数のデバイスリストの中から接続したいデバイスを選択して、4 桁の Access Code を入力して接続します。Access Code は、顧客が許可した Client (サービスマン、オペレーター) に、デバイスのパネル上に表示される 4 桁の Access Code を事前に連絡しておきます。

4. 監査ログ

デバイスと bizhub Remote Panel Server の接続時、Client (ユーザー) がデバイスを遠隔操作開始時、終了時などのログを記録します。管理者は、ログを追跡することで、bizhub Remote Panel ユーザーのアクセスを監視することができます。

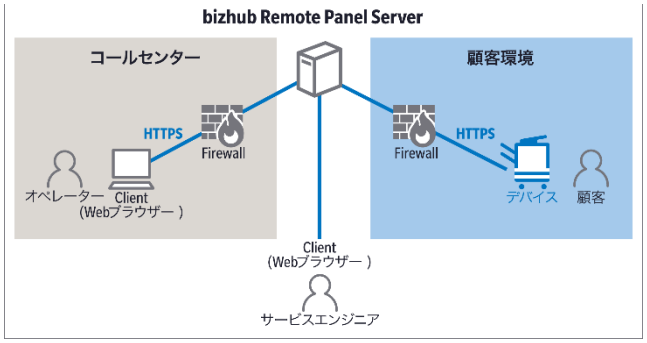


図 10-1

XI. World Wide Remote Service Platform に関するセキュリティー

<概要>

WWRSPF (World Wide Remote Service Platform) は、通信する全ての装置およびシステムとの通信において SSL/TLS 通信を行い、データを保護しています。また、クライアント-サーバー認証、送信元の Global IP アドレス制限、XMPP の固有な ID などにより、なりすましを防止することでセキュアな通信を実現しています。

1. WWRSPF と MFP 間の通信

WWRSPF と MFP 間の全ての通信は、それぞれコニカミノルタのライセンス管理サーバー (LMS) が発行した証明書を使い、クライアント、サーバー認証 (プロダクト認証) による HTTPS 通信を行うことで、なりすましがない、セキュアな通信を行っています。

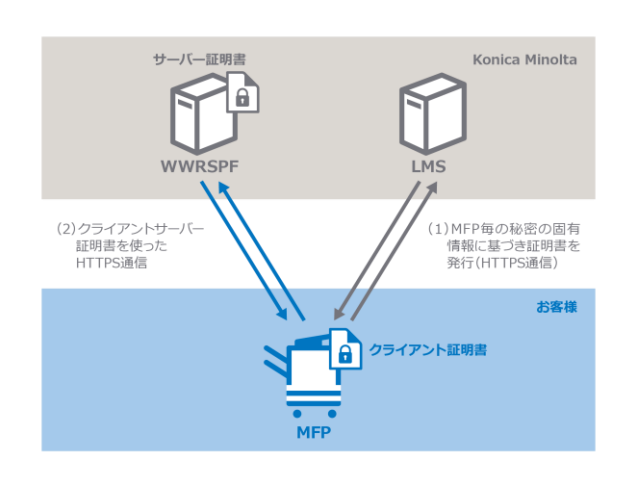


図 11-1

2. WWRSPF と XMPP PF 間の通信

WWRSPF と XMPP PF 間は、双方向の HTTPS 通信を行っており、データの暗号化を行っています。WWRSPF と XMPP PF それぞれの送信元の Global IP アドレスしか、受け付けない IP アドレス制限を行っています。

3. XMPP PF と MFP 間の通信

WWRSPF は、MFP からの (a) 初期接続時に、XMPP PF に (b) 登録をおこない、XMPP PF の接続先 URL、ログイン ID、パスワードなどを MFP に返します。MFP は、それらの情報を用い XMPP PF と XMPP over BOSH または XMPP で双方向の暗号化通信を行います。

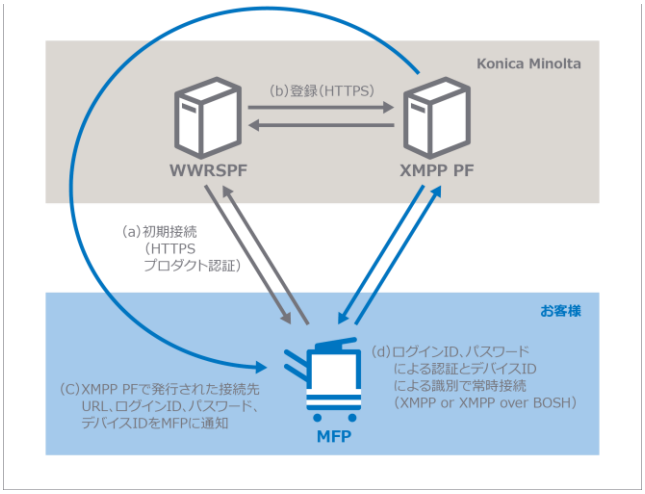


図 11-2

4. WWRSPF から MFP への通信

WWRSPF は、(a) XMPP PF 経由でチケット ID を暗号化して、XMPP PF 経由で MFP に送ります。(b1, b2) MFP は、WWRSPF に接続し、チケット ID を渡し詳細な指示内容を取得します。この際、WWRSPF はチケット ID を照合し、指示内容と指示した MFP からの応答かどうかを確認します。

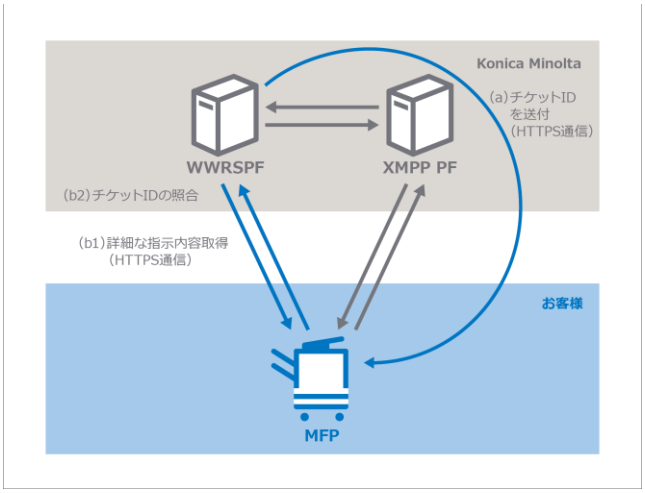


図 11-3

5. WWRSPF と CSRC 連携

CSRC と WWRSPF は、以下 (1) (2) を満たし、HTTPS 通信を行うことで、データ漏洩なくセキュアなデータ通信を行っています。

(1) WWRSPF の管理者が、CSRC の Global IP アドレスを事前登録しておく必要があります。

(2) CSRC は、WWRSPF のログインに必要な User ID、Password を使って WWRSPF にアクセスします。

また、ユーザーが WWRSPF の UI または CSRC の UI から指示した情報は、監査ログとして保存しています。

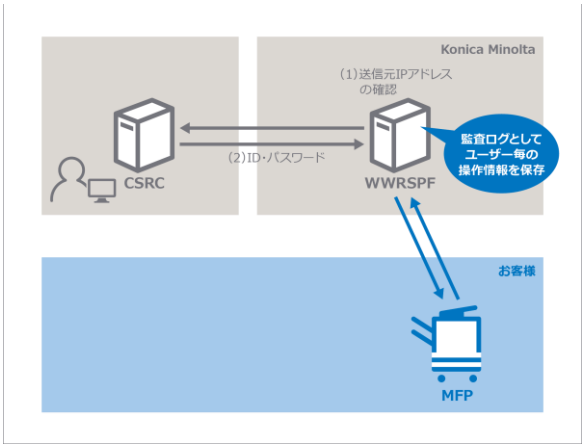


図 11-4

6. RSA (Remote Service Agent) を使った通信

RSA (Remote Service Agent) Cloud / Edge 経由することで、お客様のネットワーク上に設置されている複数の MFP と WWRSPF 間の通信を集約することができます(図 11-5)。通信が集約されることで、IT 管理者が、通信を管理しやすくなることで、外部との不正な通信を把握しやすくなります。

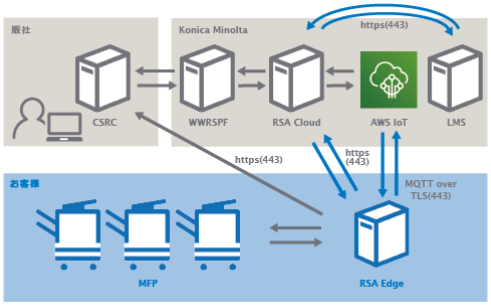


図 11-5

7. RSA Edge の登録と RSA Cloud および AWS IoT との接続に必要な情報の取得

CSRC 上で RSA Edge 登録の指示を行う (a～c) と、RSA Cloud は、LMS から RSA Edge のプロダクト認証用証明書を取得します (d) 。

RSA Cloud は、取得した RSA Edge 証明書と、その証明書から作成される RSA Edge 署名用秘密鍵、RSA Cloud 証明書、RSA Edge 毎に発行したアクティベーションキーを、Edge 毎に異なる AES 秘密鍵で暗号化し 1 つのデータファイルにします。このデータファイルは、CSRC 上でダウンロードすることができます。

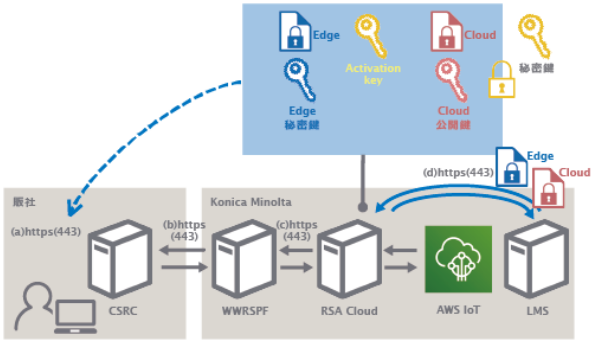


図 11-6

8. RSA Edge と RSA Cloud の通信

RSA Edge のインストール時に、CSRC 上でダウンロードしたデータファイルを、(a) AES 秘密鍵で復号化し読み込みます。

(b) RSA Edge が RSA Cloud と HTTPS 通信を行う際、RSA Edge の証明書を RSA Cloud に送り、クライアント認証により RSA Edge の正当性を確認します。

また、RSA Edge は、(c) アクティベーションキーを RSA Edge の秘密鍵で署名し、RSA Cloud に送ります。RSA Cloud は、RSA Edge の公開鍵で復号化し、復号化とアクティベーションキーにより RSA Edge の正当性を確認します（アクティベーション）。問題が無ければ、RSA Cloud は、アクセスキー（アクセストークン）を発行し、RSA Edge に返します。以後、RSA Edge は、RSA Cloud と通信する場合は、生成したアクセスキーを使って通信を行います。

RSA Cloud から RSA Edge に送られる指示スクリプトは、スクリプトのハッシュ値を RSA Cloud の証明書から作成した秘密鍵で署名し送信します。RSA Edge は、RSA Cloud の公開鍵で署名を確認し、スクリプトに改ざんが無いか確認します。以上により、RSA Edge と RSA Cloud は、完全性、機密性を担保したセキュアな通信を行います。

ところで、同じ RSA Edge ID で、RSA Edge を再構築したい場合、RSA Edge 毎に発行したアクティベーションキーは再利用できない為、CSRC 上からアクティベーションキーを再発行する必要があります。再発行すると、以前アクティベーションで生成したアクセスキー（アクセストークン）は利用できなくなり、RSA Cloud と通信ができなくなります。

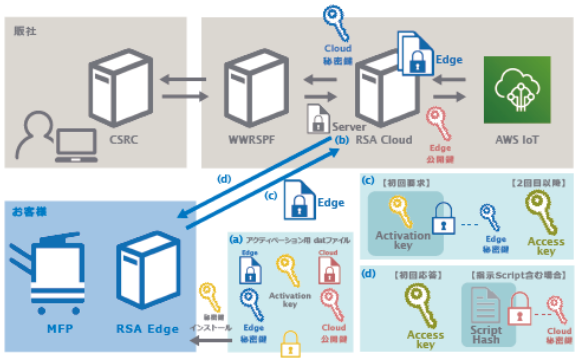


図 11-7

9. RSA Edge と AWS IoT の通信

(a) RSA Edge が AWS IoT と MQTT over TLS 通信を確立する際、RSA Edge の証明書を AWS IoT に送り、クライアント認証により RSA Edge の正当性を確認します。

以上により、RSA Edge と AWS IoT は、セキュアな通信を行います。

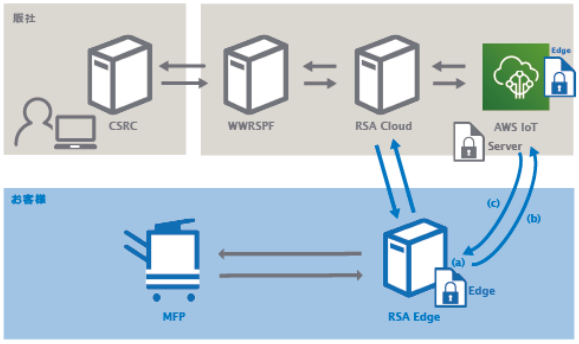


図 11-8

XII. bizhub Remote Access に関するセキュリティー

<概要>

Google Play や AppStore から bizhub Remote Access をスマートフォンやタブレット端末にインストールすることで、ネットワークで接続している MFP の本体パネル画面をスマートフォンやタブレット端末の画面に遠隔表示できます。端末上に表示された本体パネル画面をタッチ操作することで、MFP をリモート操作することができます。

1. ペアリング

NFC、Bluetooth LE、QR コードで実現されるペアリング情報の盗聴や改竄は秘密鍵によるデータの暗号化で防止されます。

2. 通信、接続トリガー

MFP は、bizhub Remote Access の機能を有効にしない限り、bizhub Remote Access からのリモート接続を拒否します。これにより、許可しない MFP がリモート操作されることを防ぎます。

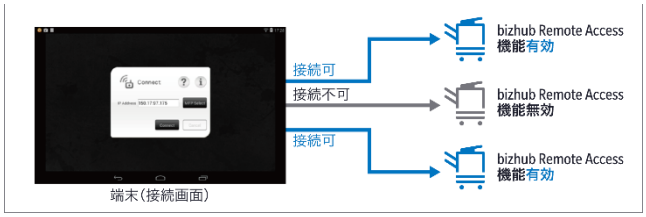


図 12-1

3. タイムアウトによる自動切断

bizhub Remote Access でリモート接続中に長時間放置された場合、MFP は自動的に bizhub Remote Access との接続を切断することで、リモート操作中に端末から離れたユーザーに対してもセキュリティーを保証します。

4. 管理者モード中のセキュリティー

MFP が管理者モードの時、MFP は bizhub Remote Access からのリモート接続を拒否することで、管理者モード中のセキュリティーを保証します。

5. リモート操作中に切断された時のセキュリティー

bizhub Remote Access は、リモート操作中に切断された場合、MFP は画面をリセットすることで、パスワードのかかった BOX の閲覧中や、パスワード入力中でもセキュリティーを確保します。

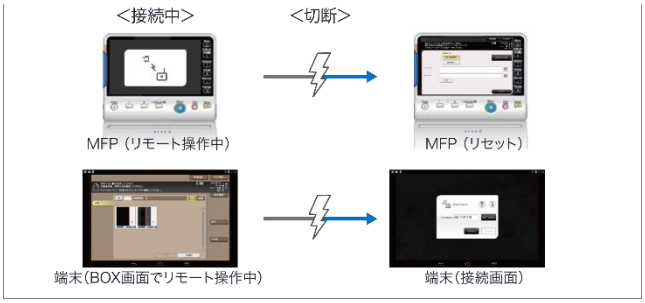


図 12-2

6. ユーザー認証・部門認証併用時のセキュリティー

bizhub Remote Access で接続しようとしている MFP がユーザー認証中もしくは部門認証中だった時、MFP は bizhub Remote Access からの接続を拒否します。
また、認証中に MFP と bizhub Remote Access が切断された時、MFP は自動的にログアウトします。
これらの機能により、認証ユーザー・認証部門のセキュリティーを保証します。

図 12-3

XIII. CSRA (CS Remote Analysis) に関するセキュリティー

<概要>

CSRA は複写機のセンサーデータなどを定期的に収集し、そのデータを解析する事により、不具合解析/不具合予測/部品寿命予測を行うシステムです。保守が発生した時に、訪問前に不具合原因解析と対応策を準備できるのでスムーズな保守作業が可能です。

また、CSRA が収集するデータは、センサーデータ値などの機械制御情報であり、個人情報に関係する内容は含まれません。

CSRA の機能を有効にするには、サービスマンによる設定が必要です。

1. HTTP 通信でのセキュリティー

CSRA で通信を行う為には、CSRC 通信が事前に確立している必要があります。 接続されるデバイスの正当性は、CSRC 接続により確認されます。

- 片方向通信

MFP 本体から指定されたサーバーにデータを定期的に送信する片方向通信のみサポートしています。 外部サーバーからの通信要求を受け付ける機能はありません。

- 送信データ暗号化

HTTP 通信では SSL/TLS を設定できます（HTTPS）。

SSL/TLS により、「デバイス⇔WebDAV サーバー」および「WebDAV サーバー⇔CSRC ホスト」の通信データの暗号化を行います。

- HTTP プロトコルが持つ数多くのセキュア機能を流用可能

HTTP プロトコルは環境に依存せず、認証、Proxy、SSL/TLS などのセキュア機能を多く利用する事が出来ます。

SSL/TLS では、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティー技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができます。

センターにおいても、これらのセキュア機能を利用することで、顧客環境にマッチしたセキュリティー対策を施行することが可能です。

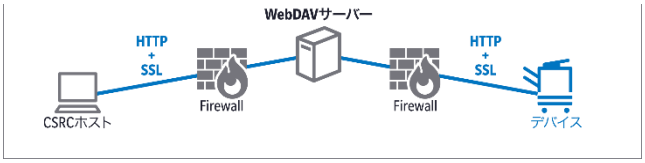


図 13-1

XIV. MFP 内蔵 SaaS GW に関するセキュリティー

<概要>

MFP 内蔵 SaaS ゲートウェイ（以降、GW）は、コニカミノルタのクラウドとオフィス機器間を連携させるゲートウェイ機能を MFP に内蔵化したもので、HTTPS と XMPP 通信機能と連携して実現しています。

MFP 内蔵 SaaS GW は、以下の機能を実現します。

- クラウド上のサービスと双方向のリアルタイム通信を行う
- クラウド上のサービスからローカルデバイスを特定できるように管理する

MFP 内蔵 SaaS GW の機能を有効にするには、サービスマンまたは管理者による設定が必要です。

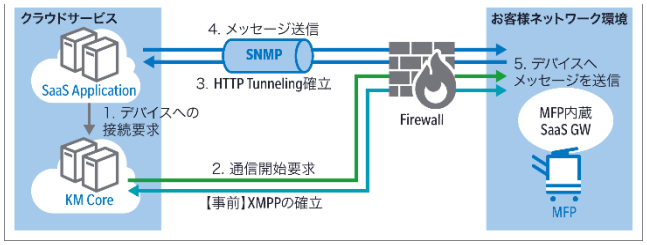


図 14-1

1. SaaS GW とクラウドとの通信

あらかじめ MFP にクラウドサービスの接続情報を登録します。また、対応する情報を、クラウド側でも保存・管理します。このような、双方向で相手を確認して通信先を特定する事でなりすましや、通信経路での改竄による間違った接続のリスクを排除します。

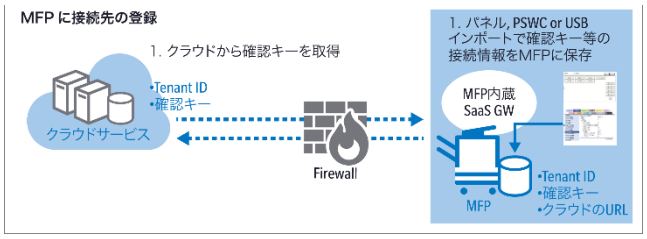


図 14-2

2. 通信上の保護と暗号化

SaaS GW とクラウドサービス間は HTTPS 通信であり、認証用データの暗号化は、RSA の秘密鍵を使って暗号化しています。

3. なりすましの防止

SaaS GW をクラウドに登録する際、Tenant ID と確認キーを SaaS GW からクラウドに通知し、クラウド側でデータを照合した後、SaaS GW へ GW ID と秘密鍵を送ります。GW ID と秘密鍵の対応リストは、クラウド側で管理します。

その後、SaaS GW はクラウドとの通信開始時に秘密鍵を使って暗号化した認証用データと GW ID を送り、クラウドは、GW ID に対応した秘密鍵で復号することで相手が正しいかを判定しています。

(1) SaaS GW をクラウド登録

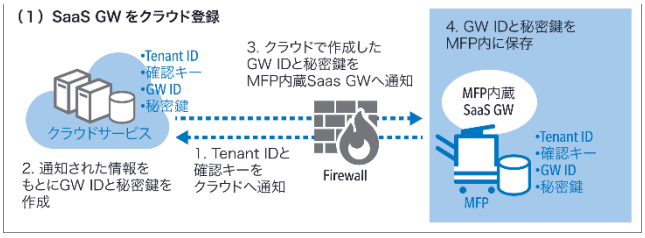


図 14-3

(2) クラウドとの通信開始時

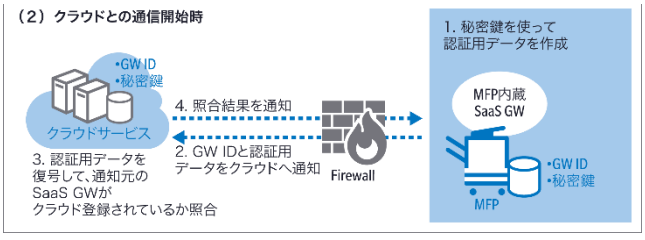


図 14-4

XV. Remote Deployment Tools に関するセキュリティー

<概要>

Remote Deployment Tools は、複数の MFP に対して各種設定を一括して行うためのツール群です。このツールの利用により、市場にて設置・運用中の MFP に対する変更作業の効率化が可能となります。

Remote Deployment Tools は、PageScope Net Care Device Manager の拡張機能として動作します。

1. 通信の安全性

(1) 装置との通信

Remote Deployment Tools における装置(MFP)との通信は、SNMP v 3 や SSL/TLS を使い安全にデータを送受信することができます。

送受信データ	プロトコル	暗号化方式
Configuration data	HTTPS	SSL/TLS
Configuration data (MIB)	SNMP v1/v3	SNMP v3 使用時に、DES または AES で暗号化通信が可能。

(2) ポート番号の変更

Remote Deployment Tools で使用するポート番号は変更が可能です。Remote Deployment Tools 以外のアプリケーションとポート番号の競合が発生した場合や、不正なアプリケーションからの攻撃を受けた場合には、ポート番号の変更で回避が可能になります。

現状で使用しているポート番号を下記に記載します。

種類	ポート番号（デフォルト）	使用目的
HTTP/HTTPS	非 SSL/TLS: 80 SSL/TLS: 443	サーバーへの Web アクセス MFP から能力通知ファイルを取得
WebDAV	非 SSL/TLS: 80 SSL/TLS: 443	MFP からの設定値取得及び設定
SNMP v1/v3	161	MFP からの設定値取得及び設定
OpenAPI	MFP 側ポート(デフォルト値) 非 SSL/TLS: 50001, 50907 SSL/TLS: 50003, 50908	MFP からの設定値取得及び設定

2. アクセス制限

Remote Deployment Tools は、PageScope Net Care Device Manager の権限管理を利用しております。Remote Deployment Tools の各機能を使用するためには、PageScope Net Care Device Manager のシステム管理者の権限でログインする必要があります。

3. データの管理

Remote Deployment Tools はデータを暗号化して保持をします。万一データが漏えいしても、データの機密性は保持されます。

4. 電子署名

Remote Deployment Tools のインストーラーおよび実行ファイルには電子署名を付加しています。これにより、下記のことができるようになります。
(1) Windows Server 2008 以降で、「ユーザーアカウント制御：署名され検証された実行ファイルのみを昇格する」の設定が有効になっているパソコンでも動作が可能です。
(2) Konica Minolta が提供するソフトウェアであることが確認でき、安心してお使いになれます。

5. ウイルス対策

Remote Deployment Tools をご使用の際には、必ず市販のウイルス対策ソフトをインストールしてお使いください。
また、ウイルス定義ファイルを定時に自動更新する設定でご使用いただくことを推奨いたします。

XVI. CWH に関するセキュリティー

<概要>

Center Ware House（以下 CWH）は MFP のセンサーデータなどを定期的に収集し、そのデータを解析する事により、不具合解析/不具合予測/部品寿命予測を行うシステムです。保守が発生した時に、訪問前に不具合原因解析と対応策を準備できるのでスムーズな保守作業が可能です。
また、CWH が収集するデータは、センサーデータ値などの機械制御情報が含まれる CSRA データと CSRC データであり、個人情報に関係する内容は含まれません。
CWH の機能を有効にするには、サービスマンによる設定が必要です。

1. 2-way HTTPS 通信でのセキュリティー

MFP と Precheck サーバー間の全ての通信は、それぞれコニカミノルタのライセンス管理サーバー（LMS）が発行した証明書を使い、クライアント、サーバー認証（プロダクト認証）による HTTPS 通信を行うことで、なりすましがない、セキュアな通信を行っています。
MFP と Bridge サーバー間は、プロダクト認証無しの HTTPS 接続をします。しかし、セキュアな Precheck サーバーから提供された Bridge サーバー情報を使用して通信する為、この通信のセキュリティーレベルはプロダクト認証を利用した通信と同等レベルとなります。

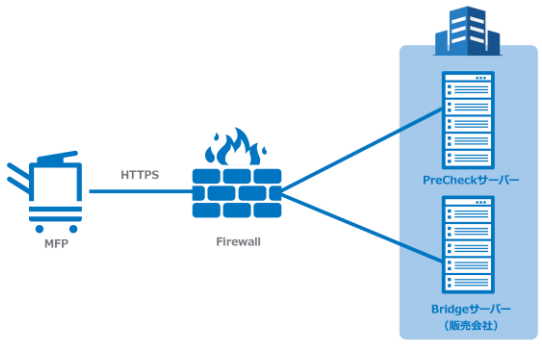


図 16-1

2. 1-way HTTPS 通信でのセキュリティー

MFPとBridgeサーバー間の全ての通信は、それぞれコニカミノルタのライセンス管理サーバー（LMS）が発行した証明書を使い、クライアント、サーバー認証（プロダクト認証）によるHTTPS通信を行うことで、なりすましがない、セキュアな通信を行っています。

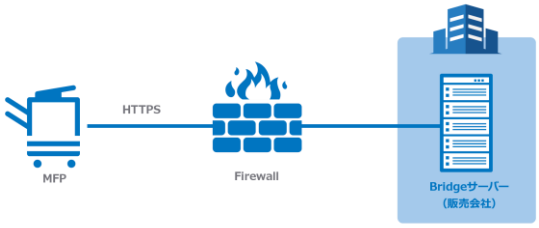


図 16-2

XVII. ユーザー情報の保護

工場出荷時、コニカミノルタの MFP では利用者に関する個人情報は必要な情報のみ扱えるように設定されています。

1. 個人情報の表示制限

実行中の[ジョブ表示]画面、および[ジョブ履歴]には、ログインユーザー／ログイン部門以外の項目は表示されません。

2. 管理者パスワード設定

管理者パスワードが初期値から変更されていない場合やパスワード規約の条件を満たしていない場合に、電源投入時に、初期パスワードの変更を促すメッセージが表示されます。

3. 簡易 IP フィルタリング

IPv4 アドレスの場合、本機に設定されている IPv4 アドレスと上位 3 バイトが同一の IPv4 アドレスのみアクセスを許可します。

例）

本機の IPv4 アドレスが「192.168.0.134」の場合、アクセスを許可する IPv4 アドレスの範囲は以下のとおりです。

192.168.0.0 ～ 192.168.0.255

IPv6 アドレスの場合、グローバルユニキャストアドレス（2000::/3）のみアクセスを許可します。また、本機に設定されている IPv6 アドレスと上位 64 ビットが同一の IPv6 アドレスのみアクセスを許可します。

例）

本機の IPv6 アドレスが「2345:1:2:3:4:5:6:7」の場合、アクセスを許可する IPv6 アドレスの範囲は以下のとおりです。

2345:1:2:3::0 ～ 2345:1:2:3:FFFF:FFFF:FFFF:FFFF

4. 簡単セキュリティー設定へのショートカット表示

上記設定の変更及び、次の設定をおこなうためのショートカットが表示されています。

[パスワード規約]

MFP で利用するパスワードの規約を有効にできます。

- [パスワード最小文字数]で設定した最小文字数（初期値：12 文字）
- 英字の大文字と小文字は区別する
- 記号は、半角記号のみ使用可能
- 同一文字だけのパスワードは禁止する
- 変更前と同じパスワードは禁止する

[Web Connection 設定]

Web Connection 経由での MFP 利用可否が設定できます。

[USB 使用設定]

USB ポートの利用許可が設定できます。

XVIII. Fleet RMM に関するセキュリティー

＜概要＞

Fleet RMM は、複数の装置に対して、各種機能の一括設定、装置情報の閲覧・監視を行うためのシステムです。ユーザーは WEB ブラウザからログインして操作することができます。Fleet RMM は、以下のアプリケーションで構成されています。

表 18-1 Fleet RMM の構成

アプリケーション	説明
エッジ	装置と通信を行う 1 つ以上の通信レイヤー。 Fleet RMM アプリケーションの指示に従い、装置と情報取得や設定を行います。
Fleet RMM アプリケーション	装置データ管理及び各機能を実現するビジネスインテリジェンスレイヤおよびユーザーとのインターフェースとなるプレゼンテーションレイヤー。 ユーザーの指示、または、タイマーによる自動起動により、各種タスクを実行します。Fleet RMM アプリケーションは、データベースを内包し、装置情報やタスク実行結果などのデータを保持します。 装置との通信は、エッジを介して実施されます。

1. 通信の安全性

Fleet RMM を使った認証の通信は、SSL/TLS を使い安全に認証データを送受信します。

Fleet RMM は「Super Admin」がユーザーを作成し、ユーザー認証はパスワードで行います。

(1) 装置との通信

Fleet RMM における装置(MFP)との通信は、SNMP v 3 や SSL/TLS を使い安全にデータを送受信することができます。

表 18-2 送信データの詳細

送信データ	プロトコル	暗号化方式	備考
Configuration data	HTTP	SSL/TLS	OpenAPI Ext/Int
Configuration data (MIB)	SNMP v1/v3	SNMP v3 使用時に、DES または AES で暗号化通信が可能	
Configuration data (XML)	HTTP	SSL/TLS XMLファイルを暗号化し転送	WebDAV 経由でのデータ送信

(2) ポート番号

表 18-3 Fleet RMM 使用する通信のプロトコル種類とポート番号の詳細

送信元	送信先	プロトコルの種類	送信先ポート番号（デフォルト）	トランスポートプロトコル	使用目的
ユーザー (Web ブラウザ)	Fleet RMM アプリケーション	HTTPS	443 *3	TCP	Fleet RMM Web アプリへのアクセス, Fleet RMM WebAPI へのアクセス
Fleet RMM アプリケーション	Fleet RMM エッジ	HTTPS	5000 *2	TCP	エッジへの WebAPI アクセス
Fleet RMM アプリケーション	SQL サーバー	ms-sql-s	1433	TCP	SQL サーバーへのアクセス
Fleet RMM アプリケーション	メールサーバー	SMTP	25 *3	TCP	メールサーバーへのメール送信
Fleet RMM アプリケーション	AD サーバー	Active Directory Web サービス (ADWS) Active Directory Management Gateway サービス	9389	TCP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	msft-gc	3268 *3	TCP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	msft-gc-ssl	3269 *3	TCP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	LDAP	389 *3	TCP/UDP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	LDAPS	636 *3	TCP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	IPsec ISAKMP	500	TCP/UDP	AD サーバーへのアクセス
Fleet RMM アプリケーション	AD サーバー	NAT-T	4500	UDP	AD サーバーへのアクセス
Fleet RMM アプリケーション	CA 証明書サーバー	PRC	135	TCP/UDP	CA 証明書サーバー(AD CS)へのアクセス
Fleet RMM アプリケーション	CA 証明書サーバー	SMB	445、139	TCP/UDP	CA 証明書サーバー(AD CS)へのアクセス
Fleet RMM アプリケーション	CA 証明書サーバー	ランダムに割り当てられた TCP ポート	1024~65535	TCP	CA 証明書サーバー(AD CS)へのアクセス
Fleet RMM エッジ	MFP	HTTP	80	TCP	MFP のデバイス能力取得, 設定値取得/設定, FW 更新 ※セキュアな通信を行うために https での通信を推奨します。設定については各デバイスのマニュアルを参照してください。
Fleet RMM エッジ	MFP	HTTPS	443	TCP	MFP のデバイス能力取得, 設定変更, FW 更新

送信元	送信先	プロトコルの種類	送信先ポート番号(デフォルト)	トランスポートプロトコル	使用目的
Fleet RMM エッジ	MFP	SNMP v1/v3	161 *3	TCP	MFP の各種設定情報取得
Fleet RMM エッジ	MFP	OpenAPI (非 SSL/TLS)	50001	TCP	MFP の各種設定情報取得 ※セキュアな通信を行うために SSL/TLS での通信を推奨します。設定については各デバイスのマニュアルを参照してください。
Fleet RMM エッジ	MFP	OpenAPI (SSL/TLS)	50003	TCP	MFP の各種設定情報取得
Fleet RMM エッジ	MFP	RAW	9100 *3	TCP	MFP (C3100i/C3120i) の FW 更新
Fleet RMM エッジ	MFP	SNMP	161		MFP (4000i/4020i/5000i/5020i) の各種ステータス取得
Fleet RMM エッジ	MFP	HTTPS	443		MFP (4000i/4020i/5000i/5020i) の各種設定情報取得
Fleet RMM エッジ	MFP	RAW	9100		MFP (4000i/4020i/5000i/5020i) の FW 更新及び一部の設定変更
MFP	Fleet RMM エッジ	OpenAPI (非 SSL/TLS)	5001 *2	TCP	MFP からの各種通知受付 ※セキュアな通信を行うために SSL/TLS での通信を推奨します。設定については各デバイスのマニュアルを参照してください。
MFP	Fleet RMM エッジ	OpenAPI (SSL/TLS)	5002 *2	TCP	MFP からの各種通知受付
Fleet RMM エッジ	MFP	SMB	139, 445	TCP/UDP	FW 更新 (*1)
Fleet RMM エッジ	MFP	FTP	21	TCP	FW 更新 (4702PSeries/4422_3622, 4700PSeries/4020_3320)
Fleet RMM アプリ	NDES サーバー	NDES	443 *3	TCP	NDES (Network Device Enrollment Service) サーバーへのアクセス
Fleet RMM エッジ	Fleet RMM アプリケーション	HTTPS	443 *3	TCP	Fleet RMM アプリケーションに対するエッジのアクティベーション、装置情報の通知

*1 bizhub CXX4e シリーズ以降

*2 カスタムインストールを選択した場合に限り、変更可能

*3 インストール後、ポート変更可能

2. アクセス制限

Fleet RMM は Super Admin がユーザーを作成して機能権限を割り当てます。 機能権限を割り当てられたユーザーはその範囲内で操作が可能となります。

3. データの管理

Fleet RMM で取り扱う機密データ（メールアドレス、パスワードなど）は暗号化され、アプリケーション内の SQL データベースや設定ファイル内で管理しています。

4. 電子署名

Fleet RMM のインストーラーおよび実行ファイルには電子署名を付加しています。これにより、下記のことができるようになります。

(1) 「ユーザーアカウント制御：署名され検証された実行ファイルのみを昇格する」の設定が有効になっている PC でも動作は可能です。

(2) Konica Minolta が提供するソフトウェアであることが確認でき、安心してお使いになれます。

5. ウイルス対策

Fleet RMM にはウイルス駆除機能を備えていませんので、ご使用の際には、必ず市販のウイルス対策ソフトをインストールしてお使い下さい。
また、ウイルス定義 DB を定時に自動更新する設定でご使用いただくことを推奨いたします。

XIX. MarketPlace に関するセキュリティ

Konica Minolta MarketPlace は、MFP アプリケーション、コネクター、ライセンス、カスタム MFP ユーザーインターフェース（UI）などのソフトウェアを販売するための革新的なプラットフォームです。これらの製品は、お客様が MFP でのワークフローを効率化し、MFP をお客様のニーズに合わせてカスタマイズするために必要なツールを提供します。MarketPlace のお客様は、無料アカウントの作成、さまざまなアプリケーション/コネクターの閲覧、クレジットカードによるライセンス購入（米国およびカナダのみ）、アプリケーションの運用管理、アプリケーションやカスタム UI のインストールなどが可能です。
注）MFP のユーザーインターフェース（UI）カスタマイズ機能は、すべての国で利用できるわけではありません。

お客様情報、ビジネスデータ、決済取引などには、不正なアクセスから保護されるべき機密性の高いものが含まれています。コニカミノルタは、以下の方法でお客様を保護することをお約束します：

- ユーザーデータ（例：クレジットカード情報）の保護
- お客様の閲覧履歴の機密保持
- サイトインテグリティの確保
- サイト偽装を防止する

Konica Minolta MarketPlace は、お客様からの信頼と信用を得るために、厳格なセキュリティプロトコルを導入しています。当社のポリシーは、ホスティングサービスである Amazon Web Services（AWS）が提供する制御を補完するように設計されています。AWS は、クラウドコンピューティングの業界リーダーであり、継続的にリスクを管理し、業界標準への準拠を保証するために定期的な評価を受けています。

1. クッキー

Konica Minolta MarketPlace は、情報を保存し、ユーザーがサイト内を移動する際にシームレスなユーザーインターフェースを提供するために、ウェブクッキーを使用しています。クッキーを使用することにより、ユーザーはサイト内の機能やページにアクセスすることができます。

(1) 目的

Konica Minolta MarketPlace のクッキーは、主に認証目的（ユーザーアカウントを確認し、ユーザーがいつログインしているかを判断すること）で使用されます。例えば、クッキーは、ユーザーが MarketPlace のページ間を移動する際にログイン状態を維持するために使用され、ユーザーが Konica Minolta MarketPlace サイトに繰り返しログインする必要がないようにします。

重要なお知らせ：Konica Minolta MarketPlace のクッキーは、機密情報や重要な情報（ユーザーパスワードなど）を保存するために使用することはありません。

(2) ユーザーの同意

欧州連合（EU）の電子プライバシー指令の一環として、ウェブサイトがトラッキング技術の使用についてユーザーの同意を得ることを要求しており、Konica Minolta MarketPlace サイトの各ページにフッターリンクとしてクッキーに関する通知が表示

されます。これにより、ユーザーが Cookie の使用について同意することができるようになっています。下図をご参照ください。

(3) クッキーのトラッキング

Konica Minolta MarketPlace は、コンテンツを第三者に提供していないため、Konica Minolta MarketPlace のサイト内で「Do Not Track」機能を特別に使用することはありません。しかし、「Do Not Track」の設定は、ブラウザによって、アナリティクスツール（Google Analytics、Matomo など）のようなすべての 3rd パーティーウェブサイトに渡すことができます。ブラウザの「Do Not Track」設定を有効にすることで、ユーザーはウェブ上で追跡されないという希望を表明することができます。ウェブブラウザで「Do Not Track」をオンにすると、訪問したすべてのウェブサイトに、ユーザーがサイトからサイトへ追跡されることを望まないという信号が送られます。

2. 暗号化

Konica Minolta MarketPlace でのやり取りは、すべて Transport Layer Security (TLS)によって安全に行われます。これは、Web 取引の機密性を保護するために用いられる最も一般的で安全なプロトコルです。TLS 暗号化を使用することで、第三者が密かに忍び込んで、行われているトランザクションを監視、ハイジャック、シャットダウンすることができないようにします。さらに、安全でない通信は、TLS を使用するように強制的にリダイレクトされます。

(1) 公開鍵暗号

Konica Minolta MarketPlace に接続する際、ブラウザはサーバーに認証処理を依頼します。認証プロセスでは、公開鍵暗号方式を使用して、信頼できる独立した第三者がサーバーを登録し、識別していることを確認します。Konica Minolta MarketPlace の公開鍵暗号方式では、メッセージは受信者の秘密鍵でしか復号化できないため、計算上非現実的なものとなります。

(2) セキュア通信

TLS は送信するデータを暗号化し、送信中の改ざんを検知するため、Web トラフィックの盗聴や改ざんは不可能です。

(3) HTTPS 接続

Konica Minolta MarketPlace は、Web サーバーとクライアントブラウザ間の通信をすべて暗号化する HTTPS（Hyper Text Transfer Protocol Secure）接続を確立しています。また、業界をリードする認証局（Amazon）を介して、Web サーバーの識別も確保されます。

(4) プロキシ対応

多くの企業や組織では、インターネットへのアクセスを制限することで、プリンターを不正なアクセスから保護しています。MFP のインターネットへのアクセスを制限したいお客様には、MFP のインターネット接続にプロキシを必要とするように設定することができます。プロキシを使用することで、Konica Minolta MarketPlace との通信のみ許可するように MFP をロックダウンすることができます。また、ファイアウォールのルールを設定することで、MFP が Konica Minolta MarketPlace としか通信しないようにすることも可能です。

3. アカウント作成

Konica Minolta MarketPlace では、Web 上でのライセンス購入、サポート資料の閲覧、MFP UI Design Tool によるカスタム UI の作成、アプリケーション/カスタム UI の MFP へのインストールなどを行うために、アカウントを作成する必要があります。これらのサービスを提供するために、Konica Minolta MarketPlace は、お客様がアカウントを作成する際に、メールアドレス、パスワードのハッシュ値、姓名を含む限られたユーザー情報を収集します。個人情報の取り扱いについては、コニカミノルタの個人情報保護方針（MarketPlace の全ページのフッターに記載）に従っています。

4. アナリティクスツール

Konica Minolta MarketPlace は、ウェブサイトのトラフィックを監視、追跡、および報告するために、サードパーティの分析サービスを使用しています。これらのサービスは、ウェブサイトのトラフィックがどこから来ているのか、何人の訪問者がサイトに来たのか、訪問者はどこへ行ったのか、どの検索エンジンとキーワードでサイトを見つけたのかを追跡します。Google Analytics は、米国とカナダで使用されています。Matomo は欧州連合(EU)で使用されています。

5. DDoS プロテクション

Konica Minolta MarketPlace は、ホスティングサービスである Amazon Web Services（AWS）を通じて DDoS（分散型サービス拒否）攻撃から保護されています。AWS は、SYN/ACK フラッド、Reflection 攻撃、HTTP スローリードなどの一般的な攻撃から保護するために、AWS Shield という DDoS 攻撃軽減技術をすべてのお客様に提供しています。

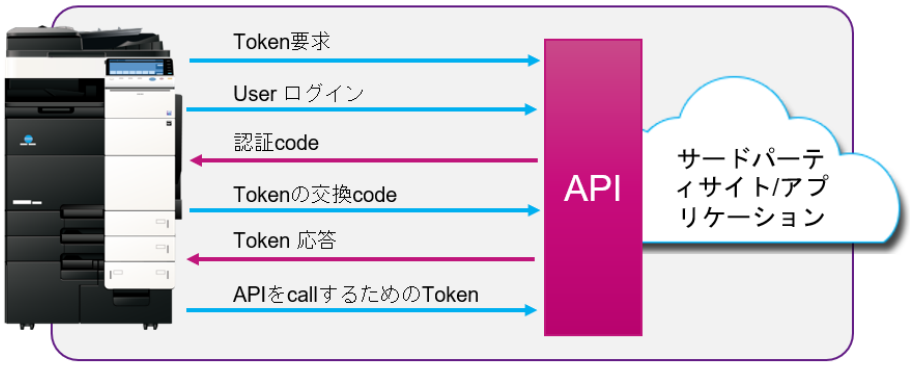
6. Konica Minolta MarketPlace アプリケーション

(1) 個人情報の保管・データ暗号化について

コニカミノルタが開発したアプリケーションは、サイトの下に設定されたコニカミノルタのプライバシーポリシーに従います。MarketPlace は、お客様の MarketPlace アカウントを使用してこれらのサービスに認証した後、Personalize、Shield Guard、ScanTrip Cloud とユーザーデータ（姓、名、電子メール、国）を共有する場合があります。

(2) OAuth 認証

サードパーティのアプリケーションに接続するアプリケーション（bizhub Connector to Box、SharePoint Connector など）は、パスワードにアクセスすることなく情報にアクセスする方法として、OAuth を使用してログインすることができます。OAuth（Open Authorization）は、パスワードや ID プロバイダーとして機能するサードパーティのサーバーを必要とせずに、アプリケーションがユーザーとしてサーバーに対して認証できるようにするプロトコルです。その代わり、サーバーが生成するトークンを使用します。



(3) bizhub SECURE Notifier App

MFP のセキュリティー設定をリアルタイムで確認できる Konica Minolta MarketPlace アプリケーション（bizhub SECURE Notifier）を用意しています。このアプリケーションを使用することにより、どの機能が有効になっているかをすぐに確認することができます：

- 管理者パスワード
- HDD の暗号化
- 一時的なデータの上書き
- HDD ロックパスワード
- 自動ドキュメント削除
- 暗号化された PDF の削除
- ID＋プリント削除
- 安全な文書削除
- バックアップスケジュール

KONICA MINOLTA