別紙

Konica Minolta
Security Technical Support Paper

セキュリティ基本方針と対応技術に関する報告書

Fleet RMM 編

Ver. 1.5

Oct 2024

改定履歴

版	日付	内容
第 1 版	2021 年 6 月	初版
第 1.2 版	2022 年 12 月	RAW ポート追加、データ管理情報追加
第 1.3 版	2023 年 10 月	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 1.4 版	2024 年 5 月	Fleet RMM v1.4 リリースに伴う更新 – 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
第 1.5 版	2024 年 10 月	Fleet RMM v1.5 リリースに伴う更新 – Fleet RMM が使用する通信プロトコルのポート番号の記載を更新 – データの送受信に SMB を追加

コニカミノルタの製品は、セキュリティ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下さい。また、ここに記された内容は万全なセキュリティ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。

MFP は複合機のことです。

Active Directory, Outlook はマイクロソフト社の商標です。

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 Fleet RMM が提供するセキュリティ基本機能を紹介します。

第 2 章 Fleet RMM 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 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。

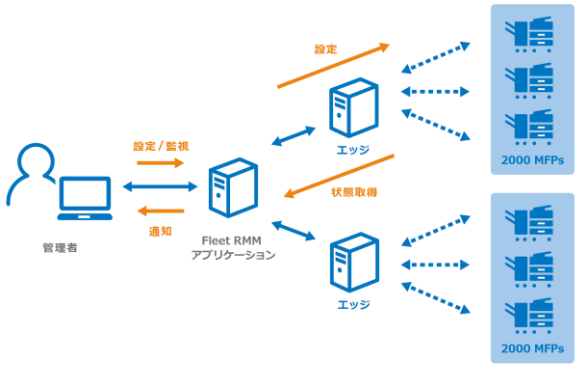

図 1 Fleet RMM の構成図

<代表的なユースケース>

Fleet RMM は、多数の装置からステータスやカウンター等の情報を取得したり、同じ設定を行ったりするために、顧客の IT 管理者が使用することを想定しています。

顧客の IT 管理者のワークフロー

装置設定

装置の導入後、装置の管理者パスワードの変更やサマータイムの設定変更等、定期的なメンテナンス作業が発生する場合には、IT 管理者がその設定を行うことができます。

1. 顧客環境で、IT 管理者が Fleet RMM アプリケーションに「Super Admin」としてログインします。
2. Web ブラウザ上で設定の編集を行い、テンプレートファイルに保存して、個別に、または、複数の装置へ一斉に配信します。

モニタリング（状態監視）

1. Fleet RMM アプリケーションは、装置のステータスやカウンターを定期的に取得します。装置の異常を検出した時は、指定のメールアドレスへ通知します。
2. IT 管理者はメール通知を受け取る事ができ、最小限のダウンタイムで装置へ適切な処置を実施する事が出来ます。

第３章 通信の安全性

---

1. ユーザー認証

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。

2. 個人情報を含むデータの送受信

個人情報を含む情報（ユーザーアカウント）に関するデータとその通信方法は下記の通りです。

表 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
Configuration data (JSON)	SMB	JSONファイルをAES暗号化して転送	SMB 経由でのデータ送信

3. ポート番号の変更

各アプリケーションのポート番号は変更が可能です。Fleet RMM 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。

参考までに、現状で使用しているポート番号を下記に記載します。ポート番号をデフォルトから変更しても Fleet RMM の動作には影響がありません。

表 3 Fleet RMM が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	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 *2*3	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

送信元	送信先	プロトコル	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 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	139, 445	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
Fleet RMM エッジ	MFP	SNMP v1/v3	161 *3	UDP	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 ※4
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	UDP	MFP (4000i / 4020i / 5000i / 5020i) の各種ステータス取得
Fleet RMM エッジ	MFP	HTTPS	443	TCP	MFP (4000i / 4020i / 5000i / 5020i) の各種設定情報取得
Fleet RMM エッジ	MFP	RAW	9100	TCP	MFP (4000i / 4020i / 5000i / 5020i) の FW 更新及び一部の設定変更
Fleet RMM エッジ	MFP	SMB	139, 445	TCP	FW 更新 ※ bizhub 287 (機能バージョン 4.0 以降のストレージ搭載機種) で使用 MFP の各種設定値変更 ※5
MFP	Fleet RMM エッジ	OpenAPI (非 SSL/TLS)	5001 *2	TCP	MFP からの各種通知受付 ※4
MFP	Fleet RMM エッジ	OpenAPI (SSL/TLS)	5002 *2	TCP	MFP からの各種通知受付
MFP	Fleet RMM エッジ	WebDAV	443	TCP	FW 更新

送信元	送信先	プロトコル	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	SMB	139, 445	TCP/UDP	FW 更新 (bizhub CXX4e シリーズ以降)
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

*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

*4 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。

*5 C360i/C361i/C4050i/C4051i/306i Series (機能バージョン 2.3) 以降のストレージ搭載の機種で使用。

第 4 章 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。

表 4 Fleet RMM の機能

カテゴリ	機能権限名	可能な操作
基本	基本 (Public)	・Fleet RMM へのログイン ・システム情報画面など特にロールを必要としない画面の閲覧
Fleet RMM 管理	システム管理 (System Management)	・証明書自動更新の初期設定（CA 局、証明書情報等） ・テンプレート配信用設定（WebDAV 設定） ・メールサーバー設定 ・表示フォーマット（日付等）設定 ・エッジの新規登録
	ロール管理 (Role Management)	・ロール一覧閲覧 ・ロール（個別）情報閲覧 ・ロールのコピー 自身が所属しているロールのみコピー可能であり、コピーされたロールはコピー元の（ロール機能、対象装置グループ、対象 Edge）の範囲を超えた権限設定は不可能とする。 ・ロールの編集 そのロールの「管理者」である場合にのみ可能。 そのロールの権限（ロール機能、対象装置グループ、対象 Edge）の範囲を超えた権限設定は不可能とする。 「管理者」のみ「管理者」の変更が可能。「管理者」の初期値はロールをコピーしたユーザー。 ・ロール削除 そのロールの「管理者」である場合にのみ可能。
	ユーザー管理 (User Management)	・ユーザーの登録、編集、削除 ・AD プロパティの登録、編集、削除
装置管理	装置グループ管理 (Device Group Management)	・装置グループ管理画面における装置グループ一覧の閲覧 ・装置グループの作成、編集、削除
	装置管理 (RW)/(RO)	・テンプレート配信、テンプレートスケジュール登録 ・証明書更新、証明書更新スケジュール登録 ・Scan&Reset の Reset 実行
	テンプレート管理 (Admin Template Management)	・テンプレート一覧の閲覧 ・管理者テンプレートのインポート/エクスポート ・テンプレート（サービス設定を除く）の作成、編集、削除 但し、本ロールを所有していても、パスワード付きのテンプレートの編集と削除は PW 入力が必要。

第 5 章 データの管理

Fleet RMM で取り扱うデータは全て暗号化され、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。各データの保管場所は以下の通りです。

表 5 データの種類と保管場所

データの種類	保管場所
ユーザー情報 (ユーザー名、メールアドレス、パスワード)	SQL データベース (メールアドレス、パスワードは暗号化して保存している。)
装置の情報 (CE パスワード、管理者パスワード)	SQL データベース (パスワードは暗号化して保存している。)
サーバアカウント情報 (メールサーバー設定、AD サーバー設定)	SQL データベース (パスワードは暗号化して保存している。)
DB アクセス用アカウント	Fleet RMM アプリケーション内のストレージ
装置の情報 (ユーザー、部門、宛先)	SQL データベース
ドメインユーザーアカウント情報 (ユーザーID、パスワード)	Fleet RMM アプリケーション内のストレージ (パスワードは暗号化して保存している。)

第 6 章 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、以下の電子署名を付加しています。

表 6 電子署名

署名者名	KONICA MINOLTA, INC.
ハッシュアルゴリズム	SHA256

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。

第 7 章 ウイルス対策

ポートアタック対応の為に、ポート番号を変更可能であることは既述した通りですが、Fleet RMM にはウイルス駆除機能を備えていませんので、Fleet RMM 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。

第 8 章 バージョン比較

Fleet RMM の主なセキュリティに関する機能のバージョン間での違いについて下記に記載します。

表 7 Fleet RMM の機能とバージョン

機能		Version					
		v1.0	v1.1	v1.2	v1.3	v1.4	v1.5
通信の安全性	ユーザー認証	○	○	○	○	○	○
	個人情報を含むデータの送受信	○	○	○	○	○	○
	ポート番号の変更	○	○	○	○	○	○
アクセス制限		○	○	○	○	○	○
データの管理		○	○	○	○	○	○
電子署名		○	○	○	○	○	○
ウイルス対策		ー	ー	ー	ー	ー	ー

KONICA MINOLTA