デジタル複合機のセキュリティに関する調査報告書

V2.1

2014 年 6 月

独立行政法人情報処理推進機構
技術本部 セキュリティセンター

改訂履歴

V1.0	2010/8/30	「MFP の脆弱性に関する調査報告書」として公開
V2.0	2013/3/12	「デジタル複合機のセキュリティに関する調査報告書」として改訂版を公開
V2.1	2014/6/9	「図 4-5 ファクス受信のデータフロー」を修正

目次

図目次

表目次

1. はじめに

1.1 MFP とは

MFP とは、Multi Function Peripheral(多機能周辺機器)、Multi Function Printer(多機能プリンタ)または Multi Function Product(多機能製品）の略称である。

本書において MFP とは、機能的にコピー、プリンタ、スキャナ、及びファクスが一体になった機器のことを指す。

また、本書での調査対象は、MFP の中でも企業や政府機関などのオフィス環境で、高度な情報セキュリティ機能を要求される MFP 製品を対象にしている。このような MFP 製品は、日本語の製品カタログでは機能別に「デジタル複合機」、「カラー複合機」または「モノクロ複合機」と呼ばれているが、単に「複合機」と呼ばれる場合もある。本書では英語の略称である MFP と表記する。

1.2 本書の背景

MFP はセキュリティ機能を備えた日本を代表する IT 製品であり、日本は MFP に関して、世界への供給元である複数のベンダを有している。

単なる一般事務機器としての MFP から、昨今は LAN への接続、情報の蓄積等、オフィスの情報流通のハブ的な役割を持つようになってきた。それに伴い MFP ベンダは MFP に対する情報セキュリティに対する要求の高まりから、情報セキュリティ機能の品質向上を重視しており、IPA が運営する「IT セキュリティ評価及び認証制度」[1]において、数多くの認証取得の実績を持っている。

その一方で、攻撃対象として MFP が話題になる機会も増えている。2011 年 11 月には MFP の遠隔操作機能を悪用した MFP を不正に動作させる脆弱性が公開された[2]。近年では、クラウド環境での利用を初めとするインターネット環境の利用や、スマートデバイスへの対応等、利便性向上に伴う多機能化・高度化が進み、MFP が攻撃される機会は更に増えている。このような環境において、MFP ベンダは情報セキュリティ面でも、既知の脆弱性の影響のあるプラットフォームを使うことによるリスクや、ネットワーク接続に起因する脅威など、設計段階から多岐にわたる脅威への対抗を網羅的に考慮しなければならない。

また、一般的に MFP はセキュリティを意識しなければならない IT 機器としての認識が弱く、開発者が予想しなかった利用形態や設計段階での見落としなど、潜在的な問題点が脆弱性として後から認知されるケースや、設置条件に応じた適切な設定や、機密情報の管理が行われていないといったケースが発生していることも事実である。（例えば、本来利用者が知り得ない、保守インタフェースへのアクセス手法や、アクセス制御されるはずの管理者用インタフェースがインターネット上に公開されている。）

[1] http://www.ipa.go.jp/security/jisec/index.html

[2] http://redtape.nbcnews.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-devastating-hack-attack-researchers-say

1.3 本書の目的

前回の調査報告書（V1.0）では、MFP のセキュリティ要件に対する脆弱性について網羅的に洗い出し、特筆すべきいくつかの項目に関して、どのような脅威があり、どの程度の攻撃能力により、どのような損害となる恐れがあるのか、そして、その対策としてはどのようなことが有効なのか、詳細解説を行った。

今回の報告書では、MFP を開発、もしくは運用する上で留意しなければならない脆弱性の観点に関して網羅的に詳細解説を行う。具体的には、近年話題となり、攻撃される機会の多い脆弱性や、古くから存在していたが、関係者が認識できていなかったために放置されている脆弱性などに重点を置き、MFP で本来考慮しなければならない脆弱性の観点に関して、多角的に調査し解説する。

7 章以降で解説するこれらの脆弱性に対する攻撃手法は、今回調査を進める中で実際に実機検証を行い、一部の MFP 製品に対して攻撃が成功したものを含んでいる。そこで本書では、関係者が実際にその脆弱性が特定の MFP に存在するか否かを確認する際に必要となる検査手法についても解説する。

本書に記載する脆弱性を認識することにより、各ベンダの開発プロセスにおけるセキュリティ確保への取組みや、動作環境における課題や利用者の誤使用といった問題への対処法、MFP の一般的な機能において疑われる脆弱性に講じる対策の指針となること、強いてはそれらに対するセキュリティ検査において本書を活用することにより、検査の水準が向上することを目的とする。

1.4 対象とする読者

本書が対象とする読者は、主に MFP 製品の企画・設計・開発を行う開発者、MFP を利用する利用者、及び MFP のセキュリティ機能を検査する評価者とする。

1.5 本書の前提

本書では、漏洩した場合に利用者（団体）の不利益に繋がるような情報資産が格納され、企業内のネットワークに接続されている MFP を想定し、悪意を持った利用者（攻撃者）が、ネットワークや MFP の操作パネル、怪しまれない範囲での MFP への接触を通じて、その情報資産へアクセスを試みることができる環境を前提とする。このような環境において、ファイルサーバやウェブサーバといった機能を併せ持つ MFP は、必然的にファイルサーバやウェブサーバと同等のセキュリティを確保する必要があると言える。

本書では MFP の中でも上位機種であり SDK や多彩な認証機能までを備えた製品を前提としている。MFP には本書に記載するような脆弱性に繋がる機能をそもそも搭載していない製品も存在する。また例えば「IT セキュリティ評価及び認証制度」の認証製品では、セキュアに利用したい場合は、運用状態に入る前に脆弱性に繋がる機能のみ停止して利用する MFP も存在する。

本書では、網羅的に脆弱性を洗い出しているため、導入する MFP、利用する環境、またはオフィスのセキュリティポリシによって当てはまらない項目があることを、読者には留意頂きたい。

1.6　主な用語の定義

本書で用いる主な用語の意味を、以下の通り定義する。ここで説明する以外の用語に関しては登場した際に脚注などで用語の意味を補足する。

用語	説明
MFP	Multi Function Peripheral(多機能周辺機器)、Multi Function Printer(多機能プリンタ)または Multi Function Product(多機能製品）の略称。SPC (Scan Print Copy)、AIO (All In One)、または MFD (Multi Function Device) と呼ぶこともある。本書において MFP とは、機能的にコピー、プリンタ、スキャナ、及びファクスが一体になった機器のことを指す。
IT セキュリティ評価及び認証制度	IT 製品の政府等での調達において、IT 製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて第三者（評価機関）が評価し、その評価結果を認証機関が認証するわが国の制度。 略称：JISEC（Japan Information Technology Security Evaluation and Certification Scheme）
暗号モジュール試験及び認証制度	電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることについて、第三者が試験及び認証するわが国の制度。 略称：JCMVP（Japan Cryptographic Module Validation Program）
CVSS	共通脆弱性評価システム（Common Vulnerability Scoring System）の略称。情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法であり、MFP ベンダに依存しない共通の評価方法を提供する。
CEM	ISO/IEC 15408 に基づく評価に使用される手法を明確にした規格。Common Evaluation Methodology の略称。正式な規格名称は Common Methodology for Information Technology Security Evaluation であり、ISO 標準（ISO/IEC 18045）として発行されている。
SSD	記憶媒体としてフラッシュメモリを用いたストレージデバイス。ハードディスクドライブ（HDD）と同じ接続インタフェースを備え、ハードディスクの代替として利用できる。 Solid State Drive の略称。
SLC チップ	NAND 型フラッシュメモリにおけるデータ記録方式の一つ。記憶素子（メモリセル）に 2 値からなる 1 ビットのデータを格納する。 Single Level Cell の略称。
MLC チップ	NAND 型フラッシュメモリにおけるデータ記録方式の一つ。記憶素子（メモリセル）に 3 値以上からなる多ビットのデータを格納する。 Multiple Level Cell の略称。
保守インタフェース	MFP の設定や初期化、管理者パスワードの設定等の保守用に用いられるインタフェース。保守員が MFP を直接操作するローカルな保守インタフェースと遠隔から操作する遠隔保守インタフェースに大別される。
LPR	TCP/IP ネットワークを経由して印刷を行うプロトコル。LPR プロトコルはネットワーク上のプリントサーバに接続した MFP やプリンタに印刷を行わせるためのプロトコルであり、RFC 1179 で規定され

	ている。
ページ記述言語	パソコン等の利用者端末から文書や画像等を印刷する際に、出力イメージを記述して MFP やプリンタに指示する言語。
リバースエンジニアリング	ソフトウェアやハードウェア等を分解、あるいは解析し、その仕組みや仕様、目的、構成部品、要素技術等を明らかにすること。
クロスコンパイラ	開発プラットフォームとは異なるプラットフォームで実行可能なプログラムを生成するコンパイラ。
バックドア	パソコンやサーバ等に設けられた裏の侵入経路。開発時に盛り込まれるものや、攻撃者による不正アクセスやマルウェア等により設けられる場合がある。
バッファオーバーフロー	動的、あるいは静的に確保されたメモリ領域に対して書き込みを行う際に、確保されたサイズ以上のデータがそのバッファに書き込まれてしまう脆弱性。本脆弱性により、不正アクセスや権限昇格等が行われる可能性がある。
ディレクトリ・トラバーサル	相対パス等を指定することにより管理者が想定（許可）していないディレクトリのファイルへアクセスする攻撃手法。
リモートシェル	ネットワーク経由で別のコンピュータ上でシェルコマンドを実行したりする CUI（キャラクターユーザーインターフェース）プログラム。
ポートスキャン	ネットワーク経由で外部からサービスが利用可能な状態であるか等を調査すること。
ブラックボックス検査	内部構造とは無関係に、外部から見た機能等を検査すること。対義語はホワイトボックス検査。

2. 調査分析手法

本資料では MFP に関する脆弱性を網羅的に抽出するため、下の図 2-1 のような調査分析手法で進める。左から、「1.機能・用途」の特定、「2.機能分担」、「3.保護の対象」の特定、「4.脅威と脆弱性の分析」から、最終的な成果として図の右側にある「5.想定される脆弱性リスト」と「6.MFP 独特の脆弱性詳細解説」を作成した。MFP に独特な脆弱性の詳細解説は、想定される脆弱性リストの一部から抽出した、一部の脆弱性を、構成図や背景、原因について詳細に解説したものである。

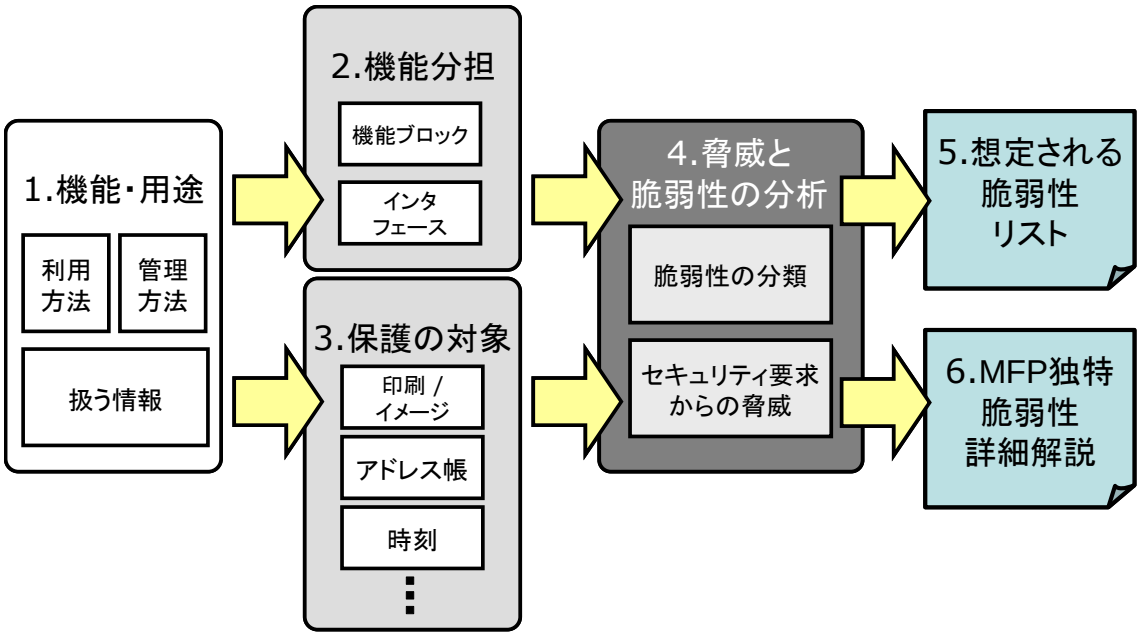


図 2-1 調査分析手法の概要

本調査の手順では、MFP の利用環境における情報システム上の脅威の一覧を特定する。脅威の一覧は、IPA「セキュア・プログラミング講座」で「脅威の洗い出し手順」として紹介されている「脅威モデリング」の手順[3]に従って進める。脅威モデリングでは、システム構成図からデータフローを特定し、インタフェースなどの境界をたどりながら脅威の洗い出しを行う。

本調査では、システム構成図を特定するために、図中左の「1.機能・用途」で MFP の用途と機能を整理した。次に「2.機能分担」で MFP 内部と外部のシステム上の機能分担を特定している。また、「3.保護の対象」で情報資産を一次資産から二次資産へと順に特定する作業を行うため MFP の用途に従ってデータフローを整理している。「4.脅威と脆弱性の分析」では、一般的な情報セキュリティへの要求事項として、情報セキュリティマネジメントの標準である ISO/IEC 27001[4]の機密性、完全性、可用性の 3 つと、オプションとして定義されている 4 つの要求事項(真正性、責任追跡性、否認防止、信頼性)をあてはめて、この要件を破ることが脅威で

[3] 脅威モデリング - IPA「セキュア・プログラミング講座」脅威モデリング
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c101.html
「脅威モデル～セキュアなアプリケーション構築」Frank Swiderski ほか著、渡部 洋子訳、日経 BP 出版センター、2005 年

[4] ISO/IEC 27001 - 対応する日本工業規格は JIS Q 27001:2006
http://www.isms.jipdec.or.jp/doc/JIP-ISMS111-21_2.pdf

あると想定して脅威の洗い出しを行った。

本調査では「4.脅威と脆弱性の分析」で、脅威の一覧から攻撃手法の例を想定しながら、特に網羅的に脆弱性を抽出することを目的としている。その際、CWE 共通脆弱性タイプ一覧[5]を網羅性の確認に利用した[6]。

そして、脆弱性の中から近年 MFP において話題となった脆弱性や MFP の利用者や開発者が再認識すべき脆弱性など 21 項目に関して、攻撃手法などの詳細な解説を行う。詳細解説する項目に関しては、具体性を確保するため MFP ベンダ関係者へのヒアリングや実機検証を行った部分もある。

2.1 MFP の用途と機能を整理

日本国内の MFP ベンダ主要 5 社から一般公開されている MFP のうち、IT セキュリティ評価及び認証制度の認証を取得している機種に関する公開資料[7]やニュースサイトから用途と機能を特定し、確認のため一部の MFP ベンダに対してヒアリングや実機操作を行った結果を踏まえ、結果を 3 章に整理する。

2.2 機能ブロックの整理

IT セキュリティ評価及び認証制度で一般公開されている情報から MFP で利用されていると考えられる機能ブロックを特定した。機能ブロックの整理は「3.5 MFP のシステム構成例」から「3.7 MFP 内部のソフトウェア」までで行っている。

2.3 守るべき資産として機能ブロック間で交換されるデータを特定

MFP の利用環境で守るべき資産を特定するため、ハードウェアの機能ブロックの間、ソフトウェアの主要ブロックの間で交換されるデータを特定する。このうち、MFP の利用者が直接扱う資産としての一次資産と、一次資産が具体的な媒体に記録された状態や、MFP という情報システムを利用するために副次的に関連する処理データやセキュリティ制御情報などの二次資産を分離しておく。

一次資産と二次資産の整理は「5 MFP の守るべき資産」で行っている。

2.4 各資産に対して脅威と脆弱性を列挙

一次資産が具体的な情報や媒体となっている状態の二次資産のすべてについて、一般的なセキュリティの要求事項 7 項目をあてはめることにより網羅性を確保して、脅威を列挙する。また、それぞれ列挙された脅威について、その脅威がどのような攻撃や事故などで具体化するか例を挙げながら、原因となると考えられる脆弱性を想定例として列挙する。

これら脅威の一覧と、対応する攻撃例、想定される脆弱性は「6 脅威から想定される脆弱性」に表形式で掲載している。

---

[5] CWE 共通脆弱性タイプ一覧（http://www.ipa.go.jp/security/vuln/CWE.html）

[6] 6 章に列挙する脆弱性と、7.15 節で解説する WEB インタフェースに関する脆弱性の観点で CWE 共通脆弱性タイプ一覧を網羅していることを確認した。

[7] セキュリティターゲット、カタログといった製品の公開資料、及び MFP ベンダが公開しているホワイトペーパー

2.5　特筆すべき脆弱性の詳細解説

列挙した脆弱性の観点から、脆弱性データベース[8]、ニュースサイト[9]、及び BlackHat などの国際会議の場で公表されている MFP に関する脆弱性に関して考察し、一部実機検証を行った結果も含め、攻撃手法やそれに対する利用者や開発者が考慮すべき対策について解説する。また例示した攻撃手法がどの程度現実的に行われる可能性がある攻撃なのかを判断する基準として、攻撃能力のスコアリングも項目毎に記載する。詳細解説する項目については、2012 年 7 月時点の脆弱性データベース、CVE を確認し、実際に報告されている公知の脆弱性の観点を本書で全て網羅していることを確認している。

[8] CVE（http://cve.mitre.org/cve/index.html）
[9] 特定のニュースサイトでは無く、Google で MFP と脆弱性をキーワードに検索した結果出力される各ニュースサイト

3. MFP の用途、機能

3.1　MFP の発展の経緯

MFP は日々進化しており、さまざまな利用方法が開拓されている。下の図 3-1 は、これまでの MFP の発展の経緯と、今後予想される MFP の利用想定例を左から順に列挙したものである。

MFP は本来、コピーを中心とした「イメージング」処理を行う装置であったが、これにファクスが統合され、電子化されたイメージデータを転送する機能とネットワーク機能が加わり、飛躍的に機能が増大した。その後、ネットワークを経由して MFP を複数利用者が共有する「遠隔共有」や、MFP を既存の業務システムなどと連携させる「アプリ拡張」などの機能が加わり、MFP への信頼性やセキュリティへの要求も増大するようになった。

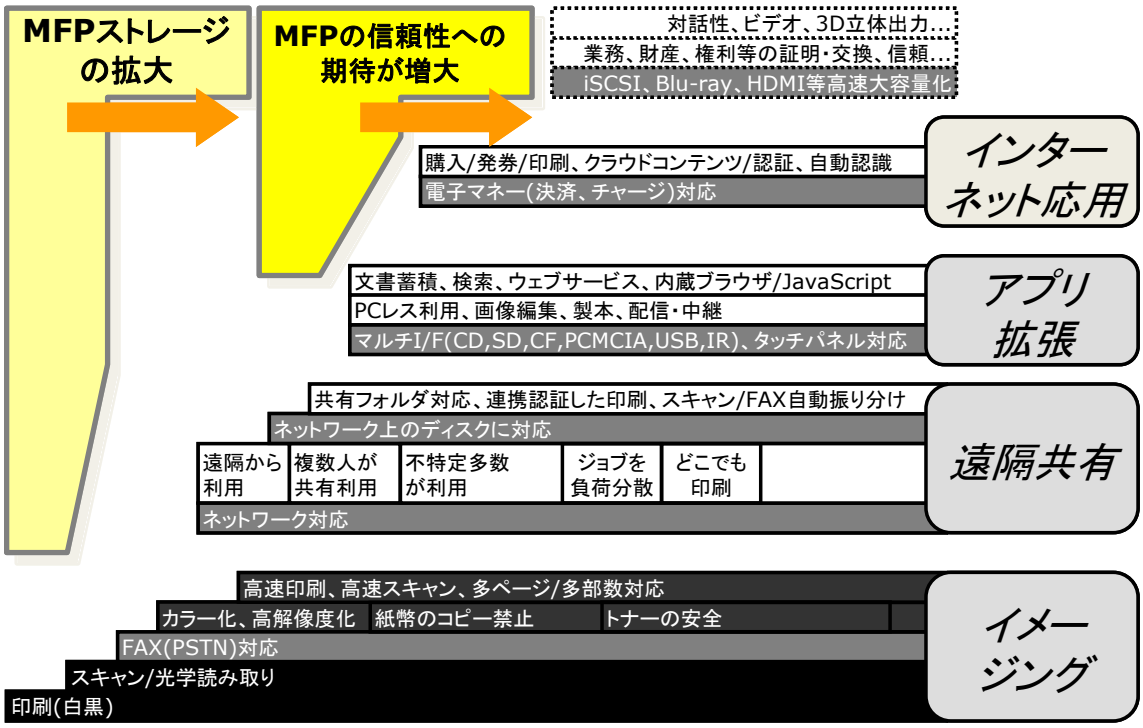


図 3-1 MFP の発展の経緯

図 3-1 の右上にある黒い点線の枠内は、将来 MFP が機能拡張する可能性を、社会インフラの一部としての役割や、生活小道具(Life Kit)的な面も含めて想定した例である。また、「インターネット応用」は、MFP をインターネット上のサービスやクラウドサービスと連携させ、さらに多数の用途で活用するという方向がある。本書で前提としている企業のオフィス環境においては、企業の各拠点にあるオフィスを跨いだシームレスな環境での印刷など、今後の発展が期待される分野である。

なお本書では、企業のオフィス環境で利用される MFP に一般的に普及している機能を調査対象としているため、一部のベンダの MFP にのみ実装されている機能や将来の機能については言及しない。

3.2　MFP に求められるセキュリティ

下の図 3-2 では MFP の進化の方向にあると考えられる、MFP に求められるセキュリティの一例である。ただし、MFP には非常に多数の機能が実装されているため、網羅的な脆弱性の特定が必要だと考えられる。そのため、本資料では MFP の本来必要とする用途や機能から順に、MFP の利用環境での脅威と脆弱性を抽出するものとする。

図 3-2 MFP に求められる機能、セキュリティ

図 3-2 の「インターネット応用」は、MFP の内蔵機能だけではなくインターネットやネットワーク上にあるさまざまな機能を応用する方向性を指す。例えば MFP 内部に共有できるように蓄積された文書を高速に検索するためにインデックスを付与するサービスとの連携がある。また、スキャンした画像から文字を抽出して検索しやすくする機能や、写真画像から顔を検出し、自動的に分類する機能などがある。それ以外にも、現金や電子マネーによる決済機能と連携したコンテンツ販売機能や、住民基本台帳カードと連携した住民票印刷などの証明書の印刷機能を持つ MFP もあるし、販売サービスだけではなく、例えば保険の申込み受付サービスなどもある。

インターネット応用についてはクラウドサービスと連携した外部ストレージへの一時保存している文書の漏洩や、文書検索に必要なインデックス情報の漏洩も、間接的に MFP の利用環境における脅威と考えられる。インターネット応用については MFP 自体の機能や運用で保護するものではなく、一般化も困難なため、6 章の脆弱性列挙の対象とはしていないが、9 章において考察している。

「アプリ拡張」については、MFP ベンダ以外のサードパーティが開発したソフ

トウェアによる拡張アプリによって、さまざまな機能が利用できる特徴がある。特定の専用型式のファイルの処理や、外部の認証機能との連携機能などがある。認証については既存の単機能を対象にした認証手順だけではなく、複数の機能で利用できるオープンな認証手順がある。こうしたオープンな認証手順ではセッション情報の維持や、なりすましのセッション情報の再利用などの脅威への対策が必要だが、オープンであるため管理が複雑になる。そのためセッション情報の管理機能を統合的に提供する開発フレームワークの採用などの対策が必要になる。

「遠隔共有」ではネットワークの高速化により、遠隔地との高速なファイル共有や機能の共有がさらに使いやすくなっている。ファイル共有だけではなく、プリント機能を USB デバイスとして遠隔地で共有する機能もある。また、遠隔共有を支えるネットワークは TCP/IP を使って国単位や地域単位での広がりを持って利用されている。TCP/IP については現在、IPv4 というプロトコルが主に利用されているが、ほとんどの MFP が IPv4 よりアドレス帯域が広く、今後利用されていく可能性が高い IPv6 というプロトコルも実装している。

「イメージング」では、MFP の基本機能であるコピー、プリント、スキャン、ファクスのための画像処理と印刷、読み取りの高解像度化、高速化がある。画素数の増大、色の深さの増大、紙送りと印字速度の高速化が一体となって進んでいる。こうした高速化に対応して、暗号処理などのセキュリティ対策も相当の高速化が行われている。

3.3　MFP を利用する環境でのライフサイクル

下の図 3-3 は、MFP の利用者から見た、MFP の利用計画から廃棄までのライフサイクルを示している。本調査では製品に関する一般的なライフサイクルのうち、「導入」「利用」「利用後」のフェーズのみを対象としている。主に図の左側に利用者自身が行うもの、図の右側に MFP ベンダや専門業者など、外部に委託することが多いと考えられる作業を整理した。

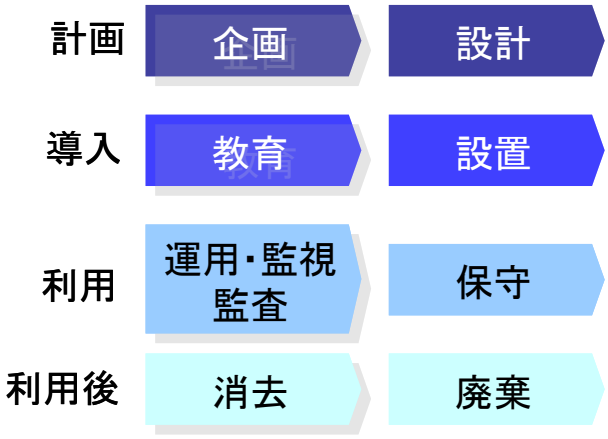


図 3-3 MFP を利用する環境でのライフサイクル

3.3.1 計画

「計画」は、利用者が MFP を利用する目的や得たい効果を検討する段階を指す。MFP 利用目的には、例えば「MFP を利用して文書取り出しを容易にわかりやすくする」、「業務手順を短縮しながら文書交換の安全性を高める」「必要な業務や作業の記録を自動化して効率化・確実化する」などがあるだろう。目標に従って、得たい効果を実現するためのしくみや利用方法の特定を行うことが、「設計」にあたる。

また、企画・設計の過程で、守るべき資産と、確保が必要な安全性の基準、その具体的な対策方針も検討する。安全性の基準と対策方法はセキュリティポリシとして、一般的には MFP を含む利用者の情報システム全体として規定されるが、MFP の利用環境については、一部のセキュリティポリシを追加・変更する場合がある。

3.3.2 導入

「導入」には、MFP 利用者への教育と、MFP 機材の設置がある。MFP 利用者への教育では、MFP 上での文書の取り扱い方や、認証方法、操作がわからないときの問い合わせ先などが一般利用者に周知される。運用者や保守員に対しても、特定の MFP 機種に関する構成・設定方法や、MFP 動作の監視・確認方法、故障時の対応方法などのトレーニングが行われる。

MFP 機材の設置では、機材を所定の場所に適切に配置し、所定のソフトウェアの投入や初期設定を行う。また、関連システムとの配線を行って、連携した動作の確認を行う。

3.3.3 利用

「利用」フェーズでは、MFP を利用する現場で主に行う作業として「運用・監視」と「監査」、保守専門業者などが行う作業として「保守」に分けている。

「運用」には、管理者が MFP の設定を変更する作業のほか、一般利用者による MFP の利用も含めている。MFP の監視については、MFP の利用形態が一般的には利用者のサイト内で閉じたネットワーク内で運用されることが前提となっているため、利用者寄りの作業として位置づけている。

「監査」では、稼働量の情報や運用中のインシデントなどの記録から、適正な運用が行われていたかどうか、その結果対策として何をするべきか検討する。
「保守」では、MFP 本体の故障修理や、部品またはソフトウェアの追加変更などの作業がある。

3.3.4　利用後

「利用後」には「消去」と「廃棄」の作業がある。利用後には、利用者は廃棄に備えてデータや設定情報の「消去」を行う。「廃棄」では、利用しなくなった MFP を廃棄業者や中古業者に回収してもらうときに何をすべきかなどを含む。

3.4　情報システムから見た MFP

下の図 3-4 は MFP を利用する環境を、情報システムとしてみた図である。図の右上の MFP は、図中央の通信システムを介して、図の左上にある利用者端末や図の中央上にある蓄積・外部処理などの他のサービスと連携して動作する。また、図 3-4 の下にある遠隔管理システムは、MFP のコンソールパネルではなく、ほかの端末やサーバから MFP の設定ができる。遠隔管理システムには、MFP の利用者や MFP 本体、蓄積・外部処理サービスのそれぞれの認証や許可の機能も持つ。

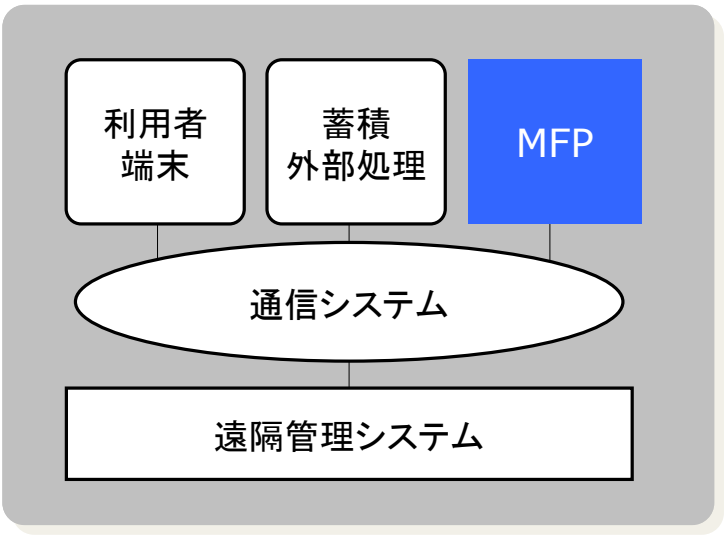


図 3-4 情報システムから見た MFP

3.4.1　利用者端末

利用者端末はネットワークや通信システムを経由して MFP を利用する入出力インタフェースを提供する端末を指す。MFP の利用者には印刷やファクス送信などを行う一般的な利用者、MFP 本体のユーザ管理や設定を行う管理者を含む。「端末」の意味は、人が操作と表示を行う点を重視している。

3.4.2　蓄積・外部処理

蓄積・外部処理は、主に MFP 外部のシステムのうち、人が直接操作せず、自動

的に機械が処理するシステムをまとめている。MFP の利用環境においては特に文書の長期格納やジョブデータの一時的な保存やスプール処理を行う「蓄積」と、画像処理や文字抽出と業務システムとの連携、文書の検索処理などさまざまな処理を含めて「外部処理」として呼んでいる。

3.4.3 通信システム

「通信システム」は MFP が外部のシステムと通信を行うために MFP の外部にある通信システムを指す。通信システムの中には、Ethernet スイッチや IP ルータとその配線、無線 LAN アクセスポイントなどがある。MFP に USB ハブを経由して接続する場合は、USB ハブと USB ケーブルも含まれる。

「通信システム」は一般的なオフィス向けの MFP の利用形態では、MFP を利用する企業内の LAN や VPN などの、企業内で閉じられたネットワーク内に限定されている。MFP と利用者端末、蓄積・外部処理はすべて企業内に閉じられたネットワークの中で接続されている。なお、企業内に閉じられたネットワークを通称して「内部ネットワーク」と呼ぶこともある。

例外的に、企業外の保守員が利用する遠隔保守インタフェースのようにインターネットや企業外のネットワークを経由する場合がある。

3.4.4 遠隔管理システム

「遠隔管理システム」は MFP の機能を利用する際の利用者などの認証、権限管理、操作や機能の監視、構成管理等を行う MFP 外部のシステムである。構成変更や設定作業、保守作業などを行うために MFP ベンダから配布されている専用ソフトウェアや、MFP 内の設定変更を行うときに利用されるブラウザも遠隔管理システムの一部と考える。遠隔管理システムには、通信システムを経由した遠隔からの管理、監視、及び保守の機能も含む。

3.5 MFP のシステム構成例

下の図 3-5 は MFP のシステム構成例を示している。中心の青い「MFP」とあるのが MFP である。MFP には USB メモリなどのポータブルメディア(以下、着脱式メディア)や、認証用の IC カードリーダが接続されることがある。機種によってはあらかじめ MFP の本体内に内蔵されている場合がある。

MFP の右下にある「保守用端末」は、保守員が MFP の故障診断を行ったり、バックアップを取り出したりするための端末である。図の左上には、「利用者端末」と「管理者端末」がある。利用者端末は内部に MFP 用のドライバ(プリンタスキャナドライバ)をインストールし、MFP と通信をして MFP のサービスを利用する。管理者端末は MFP を遠隔で設定するのに利用される。

図の右下にあるのはファクス機能である。PSTN ファクス[10]は、既存の電話網を利用したアナログファクスモデムによるイメージ伝送を行う。IP ファクスには、メールサーバを使ったメールファクスと、IP アドレスで直接相手の MFP に SMTP 接続する IP ファクス、さらに SIP[11]を利用してファクスのイメージ伝送を行う SIP ファクスがある。

なお、既存の PSTN ファクスの場合でも、SIP または H.323 手順に変換可能な

[10] Public Switched Telephone Networks（公衆電話交換回線網）の略
[11] Session Initiation Protocol の略（http://www.ietf.org/rfc/rfc3261.txt）

TA(Terminal Adapter)という装置を利用して IP 化する場合もある。TA を利用すると、遠隔地の PSTN ファクス間での通信を IP ネットワークまたはインターネット経由で中継し、既存の PSTN 経由でのファクス通信料金を削減できるメリットがある。図 3-5 では、図の右下にある TA で、MFP の PSTN ポートを IP 化する例を示している。

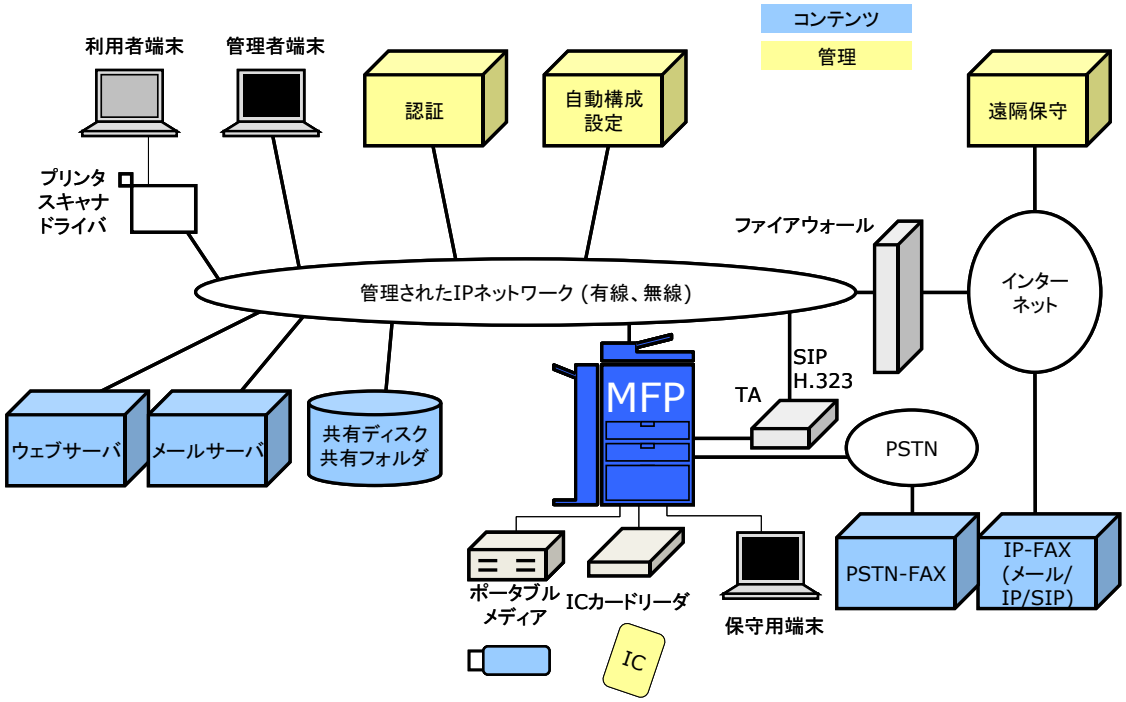


図 3-5 MFP のシステム構成例

MFP のすぐ左にある「共有ディスク 共有フォルダ」は MFP がスキャンしたイメージやファクスで受信したイメージを保存するのによく利用される。その左の「メールサーバ」は、やはりスキャンイメージや受信したファクスのイメージをメールで受信したいときに MFP からイメージが送られる先である。また、MFP 内部での異常や失敗した処理の通知が、このメールサーバを経由して管理者や利用者に送信される場合もある。メールサーバの左の「ウェブサーバ」は、MFP が内蔵しているウェブブラウザを利用して MFP の外部の画像を利用したり、MFP の外部にある業務システムと連携したりするために利用されることがある。

黄色の四角でいちばん左にある「認証」は、ネットワーク上に接続されている MFP 外部の認証サーバで、例えばオフィスに設置済みの社内システムにおける社員認証用サーバである。シングルサインオン機能を提供することもある。認証の右にある「自動構成 設定」は、MFP を含むネットワーク内で、自動的に IP アドレスを割り当てたり、正しい時刻に同期させたり、MFP の稼動を監視したりする機能がある。図の右上の「遠隔保守」は、MFP ベンダや保守業者による、遠隔地からの MFP の保守サービスである。遠隔保守では、トナーやドラムの寿命の監視、印刷などの利用枚数の監視などを行う。

この例では、特に MFP 用のスプールを行うサーバと、利用者サイト内の監視サーバ、MFP が利用するプロキシサーバについては記述しなかったが、利用者の環境によっては利用されることがある。

3.6　MFP 内部のハードウェア

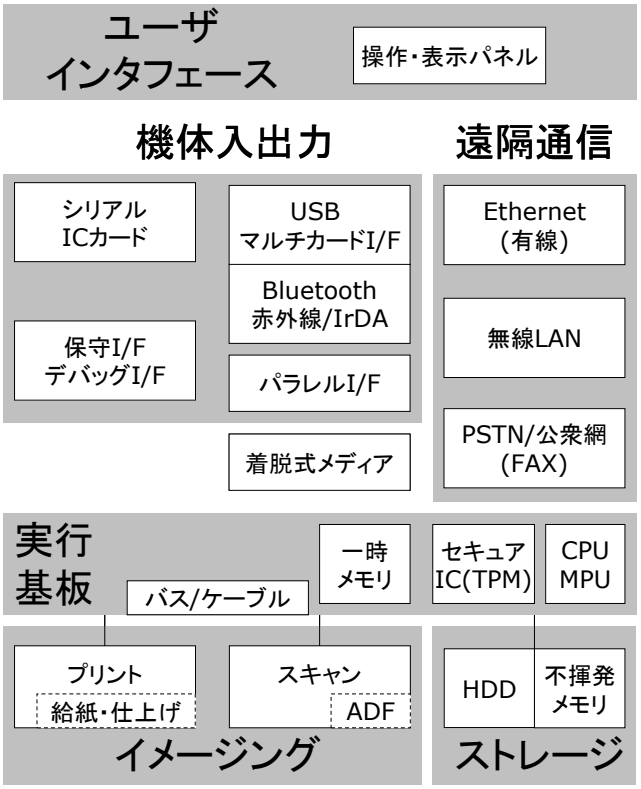


図 3-6 MFP 内部のハードウェア

MFP はプリントとスキャン、ネットワークなどの複数の機能を搭載し、連携して動作させるため、プリント、スキャン、実行基板などの複数のハードウェアを組み合わせて構成する。

3.6.1　MFP 内部のハードウェア - イメージング

プリントには、用紙トレイから用紙を取り出す給紙機構や、内部から外部へと紙を送る機構、イメージを転写して定着させる機構などからなる。また、プリント機能の追加機能として、仕上げ機構がある。仕上げ機構は「フィニッシャ」などと呼ばれる。仕上げ機構には、プリントされた印刷物を部単位でソートしたり、ホチキスで留めたり、印刷物を折ったりする機能がある。

スキャンは原稿に光をあてて、反射光をデジタルデータとして読み取る装置である。原稿を 1 面ずつ読み取るためのガラスなどの読み取り台がある。また、積み重ねられた複数枚の原稿を連続的に読み取るために、ADF(Auto Document Feeder)が装着されている。読み取り台には、読み取り台に置かれた原稿を読み取るための、移動式のスキャナモジュールがある。ADF には、原稿をスキャナに給紙するときに両面で一度に読み込むために、読み取り台とは別のスキャナモジュールを内蔵する機種もある。MFP の場合、高速なスキャン処理を実現するため、ADF 内にスキャナモジュールを内蔵する機種は多いと見られる。

3.6.2 MFP 内部のハードウェア – ストレージ

「ストレージ」は、MFP 内部で文書や一時的なジョブデータ、設定値などを保管するために利用される。ストレージ上のデータは利用者のなんらかの操作によって書き換え可能である。

3.6.3 MFP 内部のハードウェア - 機体入出力

「機体入出力」は、本資料中で独自に、MFP 本体と対向で通信するインタフェースを抽出してまとめた呼び名である。主なものは、USB マルチカードインタフェースで、USB メモリや SD カードメモリ、CF カードなどの複数の着脱式メディアを装着できるユニットのインタフェースである。また、Bluetooth や赤外線(IrDA)インタフェースも、ほぼ MFP と対向で接続するものと考えられる。パラレルインタフェースとは、古くからあるプリンタ中心に用いられたインタフェースで、プリンタと接続する端末にも昔は装備されていた。

「機体入出力」にはその他、認証用のインタフェースと、保守/デバッグ用のインタフェースがある。

認証用として MFP のコンソールを操作する利用者を認証するための IC カード認証装置や生体認証用のインタフェースがある。

保守インタフェースとしては、MFP 本体の保守時に MFP の故障診断を行う機能がある。また、デバッグインタフェースは製品には残っていないと考えられるが、MFP 製品を開発するときに、実行基板上のソフトウェアの状態を確認・変更したり、書き換えたりすることができるインタフェースである。デバッグインタフェースは CPU の特権レベルで制御を行うため、MFP 内部に設定された権限や制限などの制約からは一切影響を受けずに動作する。

3.6.4 MFP 内部のハードウェア - 遠隔通信

遠隔通信は、MFP から多段の通信機器などを経由して通信するインタフェースを、本資料中で独自にまとめた呼び名である。Ethernet や無線 LAN、PSTN 公衆網(PHS を含む)がこれにあたる。これらの通信インタフェースは、ルータやスイッチ、交換機などを通じて全世界とグローバルに通信することができる。遠隔通信はグローバルなインタフェースとすれば、機体入出力は MFP 周辺のローカルなインタフェースともいえる。

3.6.5 MFP 内部のハードウェア - ユーザインタフェース

MFP の「ユーザインタフェース」は、MFP の表示用の液晶画面と、キーボードを含むコンソールパネル(略してコンソール)がある。コンソールが MFP 本体に組み込まれている MFP のほか、一部機種ではコンソールが外部に分離され、大型化されているものもある。

3.6.6　MFP 内部のハードウェア - 実行基板

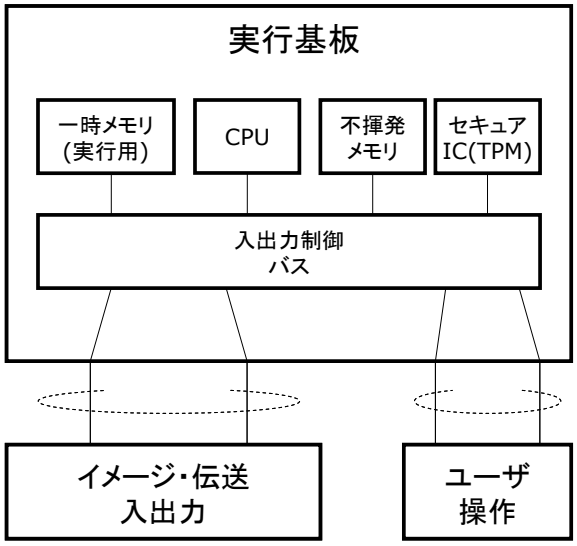


図 3-7 MFP 内部のハードウェア - 実行基板と主なインタフェース

図 3-7 は MFP 内部のハードウェアの実行基板と主なインタフェースを示す。「一時メモリ(実行用)」は DRAM(Dynamic Random Access Memory)などで提供される、ソフトウェアの実行時に利用される、揮発性のメモリを指す。「CPU」はソフトウェアを実行するための演算処理を行う。「不揮発メモリ」は実行用のソフトウェアや、実行用の設定値を保管するために利用される。「セキュア IC(TPM)」は、内部に暗号処理用の秘密鍵を持ち、暗号処理が可能な IC である。セキュア IC(TPM: Trusted Platform Module)は暗号処理を行う際に、秘密鍵をセキュア IC 外部に取り出す必要がなく、安全に秘密鍵を保管できる特徴を持つ。

3.6.7　MFP 内部のハードウェア – モジュール間の接続

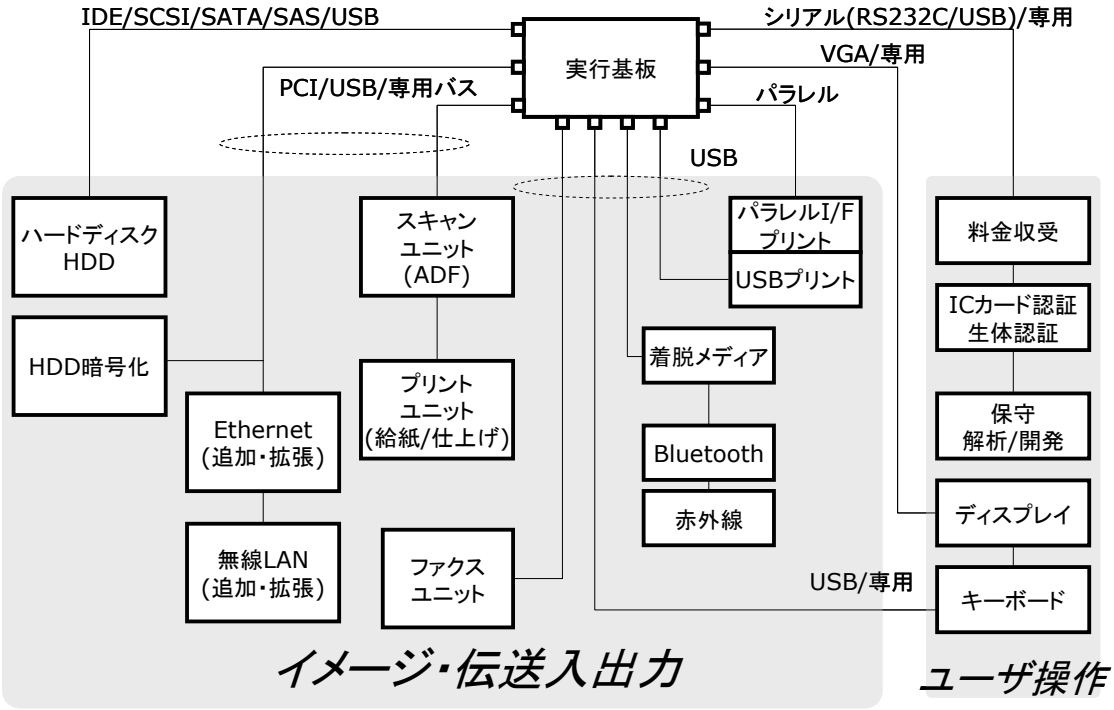


図 3-8 MFP 内部のハードウェア - ユニットまたはモジュール間の接続

上の図 3-8 は MFP 内部のハードウェアのうち、実行基板とそれ以外のハードウェアが接続される構成を示したものである。図は実行基板からどのインタフェースを利用して各ハードウェアが接続されているかを表しており、ハードウェア間の接続は表現していない。例えば Ethernet モジュールは HDD 暗号化を経由して実行基板に接続している訳ではない。

図の左、ハードディスク用の標準インタフェースとしては、IDE/SCSI/SATA/SAS/USB などがある。IDE(Integrated Drive Electronics)は古くからあるパソコン用の安価なインタフェースだが、ケーブルの配線本数が多く、コネクタが大きくなるデメリットがある。SCSI(Small Computer System Interface)はハードディスクに限らずスキャナなども複数台接続できるメリットがあるが、IDE と同じくケーブルの配線本数が多い。SATA(Serial Advanced Technology Attachment)はケーブルの配線本数を大幅に減らしながら、IDE よりも高速な転送が可能で、安価に提供されている。ハードディスク用インタフェースには SAS(Serial Attached SCSI)というインタフェースも標準化されているが、一般的に高価である。USB はハードディスクへのインタフェースとして利用されることもあるが、転送速度を確保しにくい場合がある。

図 3-8 の左から二列目の HDD 暗号化はハードディスクに書き込み/読み出しするデータを暗号化/復号する機能である。「Ethernet」と「無線 LAN」は、実行基板上で提供される場合もあるが、実行基板とは別のモジュールを追加する形で提供される場合もある。これら HDD 暗号化モジュールや Ethernet モジュールは高速なデータ転送が必要であるのと、モジュール自体は小型にできるため、PCI(Peripheral Components Interconnect)バスや USB バス、または MFP ベンダ独自の専用インタフ

ェースで提供される。

スキャンユニットとプリントユニットは、MFP のイメージ処理の中核にあたるため、実行基板との間では PCI バスなどの高速インタフェースのほか、MFP ベンダ独自の専用インタフェースが利用される。また、印刷イメージの展開や、読み取り画像の加工などのイメージ処理機能がスキャンユニットやプリントユニットの側に装備されている場合もある。

ファクスユニットよりも右の列にあるモジュールは、より低速なインタフェースである。ファクスユニットの主な用途はモノクロで、カラー画像のイメージ転送も行う場合でも、ファクスイメージの伝送のリアルタイム性はあまり重要視されていない。また、ファクス機能自体がオプション機能として扱われることがよくあるため、USB などの汎用インタフェースで接続されることもある。

ファクスユニットの右にある、「着脱式メディア」は USB メモリや SD カードなどの着脱できるメディア用のモジュールである。MFP に対してデジタルカメラの画像をメディアの抜き差しによって投入できる。「Bluetooth」と「赤外線」は携帯電話やデジタルカメラなどと近距離で通信し、MFP にプリント画像を投入できる無線のインタフェースである。同じ無線 LAN との間の違いは、Bluetooth や赤外線は別のネットワークを広域に接続せず、MFP の周辺に限って接続できる点である。Bluetooth の場合は最大で半径約 10m、赤外線は間に光をさえぎるものがない状態で最大数 10cm 程度である。

図のいちばん右側下の、「ディスプレイ」と「キーボード」は、MFP 本体に装備されている表示用のコンソールパネルと、操作用のキーボードを指す。一部機種では MFP の本体外に独立した表示装置やキーボードを持つ。

図の右上にある「料金収受」は、公衆向けの MFP などで料金として貨幣を投入して利用するための装置である。「IC カード認証・生体認証」は、MFP の利用者を認証するために、非接触 IC カードや指紋などの生体情報を使って認証を行うモジュールである。IC カード認証・生体認証と MFP 実行基板の間は RS232C や USB などで接続されている。「保守/解析/開発」は MFP の故障時に故障原因を詳細に調べたり、一部の設定やソフトウェアを更新したりするために利用される。ただし、開発インタフェースは通常は利用者にとっては用途がないため、製品内では削除しておくか、無効にしておく。

なお、本書ではオフィス環境での利用を前提としているため、「料金収受」の装置についての検討は行っていない。

3.7　MFP 内部のソフトウェア

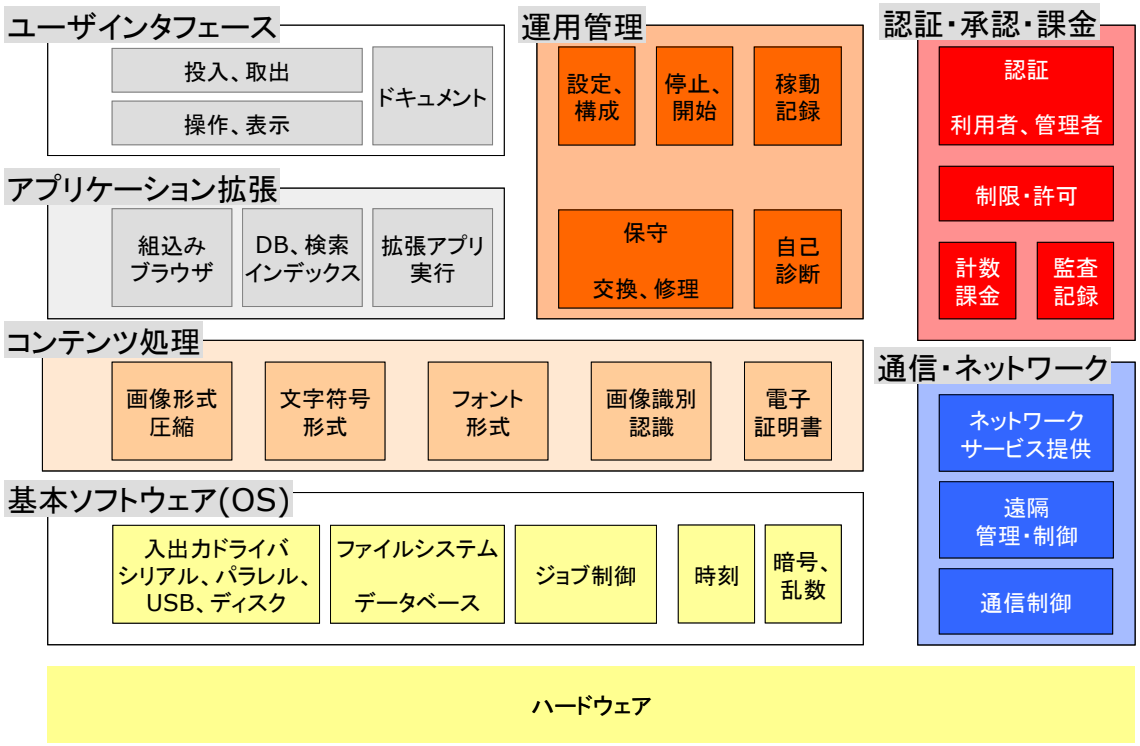


図 3-9 MFP 内部のソフトウェア

MFP のハードウェア上で実行される、MFP 内部のソフトウェアについて機能ブロックを整理した。以下に、各機能ブロックの内容について説明する。

3.7.1　ユーザインタフェース – 投入、取出

ユーザインタフェースの「投入、取出」は、紙としての原稿や印刷物の投入と取り出しを指している。

ネットワーク経由でのジョブデータの投入と取り出しについては通信・ネットワークの「ネットワークサービス提供」としている。

3.7.2　ユーザインタフェース – 操作、表示

ユーザインタフェースの「操作・表示」は、MFP 本体のコンソールやキーボードを使った操作・表示を指している。必要があれば本体上に貼られたシールなどで示された操作ガイドやマークなども含む。

3.7.3　ユーザインタフェース – ドキュメント

ユーザインタフェースの「ドキュメント」は取扱説明書やマニュアルなど、MFP の使い方を説明した資料のことを指す。MFP で動作する機能の使い方がすべて記載されたものである。

3.7.4 アプリケーション拡張 – 組込みブラウザ

アプリケーション拡張の「組込みブラウザ」は、MFP 内部に組み込まれたウェブブラウザを指す。組込みブラウザは所定の処理に従って、MFP の外部のウェブサーバやウェブサービスに対して要求を行い、ウェブサーバから応答として受信した HTML ファイルの解釈や JavaScript の実行を行い、必要な情報を得る。一般的なウェブブラウザと近い機能を持ち、PDF リーダーなどがアドオンされている場合がある。

組込みブラウザの利用例としては、他の MFP の操作や、外部の業務システムで動作するウェブサーバへの印刷用のデータの要求、などがある。

3.7.5 アプリケーション拡張 – DB、検索インデックス

「DB」は MFP 内で利用されるデータベースである。多数のアドレスや、MFP 内のボックスや共有文書として格納さるファイル、長時間にわたるジョブデータなどを管理するために利用される場合がある。DB については汎用的な SQL 言語インタフェースを持つデータベースが利用される場合もある。ただし SQL 言語インタフェースについては、インターネットのウェブと DB を利用したシステムで SQL インジェクションなどの攻撃事例が多数発生しているため、MFP においても配慮が求められるところである。

「検索インデックス」は MFP 内に保管された文書ファイルを全文検索するために利用されるインデックス情報のことである。

全文検索では、1 つ以上の単語をもとに、高速で多数のファイルを検索するため、事前に単語単位で文書ファイルを指し示すよう整理されたデータとして検索インデックスを用意する。そのため、検索インデックスには、多数の文書から抽出された単語と、その出現頻度や含まれる文書ファイル名などが含まれている。

また、検索インデックスのデータ量はほぼ元の文書の大きさと同等かそれ以上と、大きくなりがちなため、複数の利用者間で共有するのが一般的である。しかし、文書によっては特定の利用者にのみ閲覧や書き込みを許可するなどのアクセス制御が必要なため、検索インデックスの扱いには注意が必要である。

3.7.6 アプリケーション拡張 - 拡張アプリ実行

「拡張アプリ実行」は、MFP 上で、その MFP ベンダではないサードパーティの開発者や利用者が開発したソフトウェアを実行できるようにする機能のことを指す。拡張アプリ実行では、Java で開発したアプリケーションを実行[12]させたり、その MFP 用に開発した特定の命令を MFP 内部のブラウザに実行させ[13]たりすることがある。

また、各 MFP 用に拡張アプリを開発するための環境として、MFP ベンダでは「SDK (Software Development Kit)」と呼ばれる開発環境を配布している。一般的に SDK では、特定 MFP ベンダや特定機種が提供している MFP 上のサービスや MFP

[12] RICOH Developers Challenge - 「Java で複合機を駆使する」
http://www.ricoh.co.jp/javachallenge/outline/
Canon MEAP - 「Java 技術によって OS 非依存」
http://www.canon.us/technology/canon_tech/explanation/meap.html

[13] FujiXerox Apeos IntegrationPlus
http://www.fujixerox.co.jp/solution/dsp/product/integrationplus/index.html
KonicaMinolta OpenAPI
http://en.wikipedia.org/wiki/Konica_Minolta_OpenAPI

用のドライバの機能を他のソフトウェアから呼び出せるよう、ライブラリや呼び出し仕様(API: Application Programming Interface)が提供されている。

SDK を利用すれば、MFP ベンダではない第三者が新しいソフトウェアを開発し、MFP の機能をさらに拡張したり、別のシステムと連携動作させたりすることができる。また、SDK には、MFP の外部で動作するソフトウェアを前提にしたものと、MFP の内部に追加して実行させる前提のものがある。

3.7.7 コンテンツ処理 - 画像形式・圧縮

MFP では紙にプリントをするために、MFP ごとにあらかじめ決められた形式の画像を受信して処理し、紙に転写する処理を行っている。そのため、MFP 内部では特定の画像形式のデータを高速に扱う機能がある。また、MFP は一般的に JPEG や TIFF、PDF などの特定の画像形式や画像圧縮形式を利用したファイルを直接取り込んで展開するなどの処理ができる。

3.7.8 コンテンツ処理 - 文字符号形式

一般に MFP はビットマップ化された画像データをもとに印刷処理しているが、PDF または PostScript のように、文字コードを受信して、MFP 上に搭載されているフォントを独自に展開してプリントイメージを生成する場合がある。その際、文字の符号形式(文字コード)への対応が必要となる。日本語では JIS、SJIS、EUC、Unicode など複数の文字コードが存在し、それぞれはマルチバイト文字コードと呼ばれ、1 文字につき 2 バイト以上の長さを持つ。

3.7.9 コンテンツ処理 – フォント形式

PDF または PostScript のように MFP 内で文字コードから文字のイメージを展開するためには、文字ごとに字の形を定義した「フォント」というデータが必要になる。MFP がフォントを展開するには、特定のフォント形式に対応した処理が必要である。PDF または PostScript 用には、PostScript フォントが MFP ベンダから提供されている。

3.7.10 コンテンツ処理 - 画像識別・認識

MFP の一部の機種では、MFP 内部でスキャンした画像やファクス受信した画像から、画像内の文字を識別・認識する機能を持つものもある。ただしこの機能は MFP 一般に内蔵されている機能ではないため対象外とする。

3.7.11 コンテンツ処理 – 電子証明書

MFP の一部の機種では、MFP 内部でスキャンした画像や、MFP に登録した電子ファイルに対して電子証明書を使った電子署名を行い、業務上の証拠として残す機能を提供しているものがある。

また、メールファクスについては S/MIME という電子メールのコンテンツを暗号化・電子署名する方式があり、ここで電子証明書が利用される。

文書の処理ではないが、SSL/TLS の暗号化通信機能では、電子証明書を利用したサーバ/クライアントの認証、鍵の交換の機能がある。

3.7.12 基本ソフトウェア(OS) - 入出力ドライバ、シリアル、パラレル、USB、ディスク

一般的に基本ソフトウェア(OS)については、すべてのハードウェアの制御、リソース管理機能などが含まれるが、ここでは特に市販の MFP 製品に共通な機能について特定しておく。

MFP の OS には、複数の組込み製品に汎用的に利用できる、汎用の OS と、その MFP ベンダや機種ごとに限定された専用の OS がある。専用の OS では、OS のソースコードが開示されていなかったり、OS の API も非公開であったりするため、攻撃者への認知度が低い。一方、汎用 OS では Windows、Linux、VxWorks のように広く普及しているため攻撃者への認知度も高いが、標準的な API を利用でき、必要があればソースコードを入手して確認できるというメリットがある。そして共通することだが、どちらの OS でも、高機能化と高性能化に伴って、さまざまな脆弱性をはらむ可能性がある。

MFP の基本ソフトウェア(OS)として、入出力ドライバがある。MFP の外部のインタフェースとして、シリアル、パラレル、USB、ハードディスクの入出力を制御する。

3.7.13 基本ソフトウェア(OS) - ファイルシステム、データベース

MFP 内部で、一時的なジョブデータや長期的に保存する共有の文書ファイルを格納する。MFP が格納する設定情報や、利用履歴、監査記録については MFP 内部のファイルシステム上か、データベース上で格納されることがある。

3.7.14 基本ソフトウェア(OS) - ジョブ制御

MFP にはプリント、スキャン、ファクス、コピーなどの複数の要求が指示され、それらが順序良く処理されていかなければならない。それぞれの処理は数分以上かかるものもあり、多くのあとから指示された要求は「ジョブ」という形で MFP 内部のハードディスクやメモリ上に保留される。

ジョブ制御は、受け付け中のジョブ、実行中ジョブ、保留ジョブ、完了ジョブを制御して、なんらかの結果を出すようにジョブを実行する。

3.7.15 基本ソフトウェア(OS) – 時刻

オフィス向きの MFP の場合、運用履歴を記録したログ、認証サーバや暗号化機能、電子証明書などのために、時刻は常にシステム内で同期していなければならない。MFP 上では、リアルタイムクロックと呼ばれる部品が、電源を停止している間も時刻を刻み、電源が投入されたあとも、ほぼ正しい時刻で動作する。ネットワーク上の時刻サーバを利用して時刻を同期させることもある。

3.7.16 基本ソフトウェア(OS) - 暗号、乱数

「暗号」にはハッシュ値を計算する処理や、暗号化を行う処理などが含まれている。「乱数」は一般的に暗号を利用するときに、暗号鍵として予想しにくい値を生成するために重要な役割を果たす。

3.7.17 運用管理 - 設定、構成

MFP の運用管理における「設定、構成」は多くの項目があり、数百項目以上になることもある。個別の設定項目については MFP の機種ごとに依存するため、個別の詳細な設定項目については検討せず、機能ブロック単位での設定に関して検討している。

3.7.18 運用管理 - 停止、開始

MFP には省電力機能があり、自動的に節電モードに入る。また、ファクス搭載機は常時電源を投入するが、ファクスを搭載しない機種では、業務時間外は電源をオフにすることもある。

3.7.19 運用管理 - 稼動記録

MFP のプリントまたはコピーの枚数を利用者ごとに記録し、設定変更やソフトウェアの追加削除など運用管理の履歴を記録する。

3.7.20 運用管理 - 保守、交換、修理

MFP の故障に対応し、ハードウェア部品やソフトウェアの交換をするための機能。ライセンスの管理機能も含まれる。

3.7.21 運用管理 – 自己診断

MFP の故障時に MFP 内部のソフトウェアが MFP 内部のハードウェアやソフトウェアの状態を確認して、故障や不具合箇所を報告する機能。

3.7.22 認証・承認・課金 - 認証、利用者、管理者

MFP が利用者や管理者を認証する機能。保守員も認証する。

3.7.23 認証・承認・課金 - 制限、許可

MFP が特定の利用者グループや全利用者に課す利用制限と許可。

3.7.24 認証・承認・課金 – 計数・課金

特定の MFP でプリントまたはコピー、スキャンなどのサービスが利用された回数や枚数の集計値。MFP 単位で集計され、保守業者が課金する根拠として利用する。

3.7.25 認証・承認・課金 - 監査記録

特に MFP のセキュリティ機能を利用するときに、セキュリティ機能を利用した処理が行われたか、そのセキュリティ処理の結果は成功か失敗か、などの履歴を記録する。定期的な MFP のセキュリティ機能の稼動に関する監査のときに参照、集計される。

3.7.26 通信・ネットワーク - ネットワークサービス提供

MFP が利用者端末や他システムに対してサービスを提供するために、MFP はネットワークからの要求、リクエストが届くのを待機している。MFP は外部の利用者端末や他システムから要求が届くと、この要求に対して何らかの処理を行って応答する。このような、他のシステムに対する要求・処理・応答をネットワークサービスと呼ぶ。

ネットワークサービスは、MFP 内部で動作するサーバによって提供されるため、サーバ機能とも呼ぶ。MFP のサーバ機能には、MFP の機能の共有サービスを提供する SMB サーバや HTTP サーバ、ファイル共有サービスを提供する FTP サーバ、ファクスやスキャンのイメージデータを転送・配信する SMTP サーバなどがある。

また、MFP の管理や保守用にも複数のネットワークサービス機能ある。管理用途では、MFP 内部の稼動状態などを応答したり、状態を変更させたりする SNMP サーバがある。

3.7.27 通信・ネットワーク – 遠隔管理・制御

管理者が遠隔から MFP の設定を行ったり、構成管理を行ったりするための機能。MFP 上のウェブサーバ上で提供されている管理ページまたは保守ページを、管理者端末から開いて利用する。

3.7.28 通信・ネットワーク - 通信制御

ファクスの送受信手順制御や IP ネットワーク上の通信制御を行う機能。IP ネットワークでは、「ネットワークサービス」に比較して、Ethernet と IPv4/IPv6 の制御を行う。

4. MFP 利用時のデータフロー

MFP を利用するときのデータフローを以下の構成図に従って特定する。データはイメージや文書などのコンテンツデータと、指示や制御などの制御データの二つに分けて整理する。コンテンツデータについては実線で、制御データについては点線で示している。

なお、稼動記録についてはすべての処理で記録が行われる共通の処理であるため、稼動記録の書き込み処理については読み出しのみデータフローを特定した。

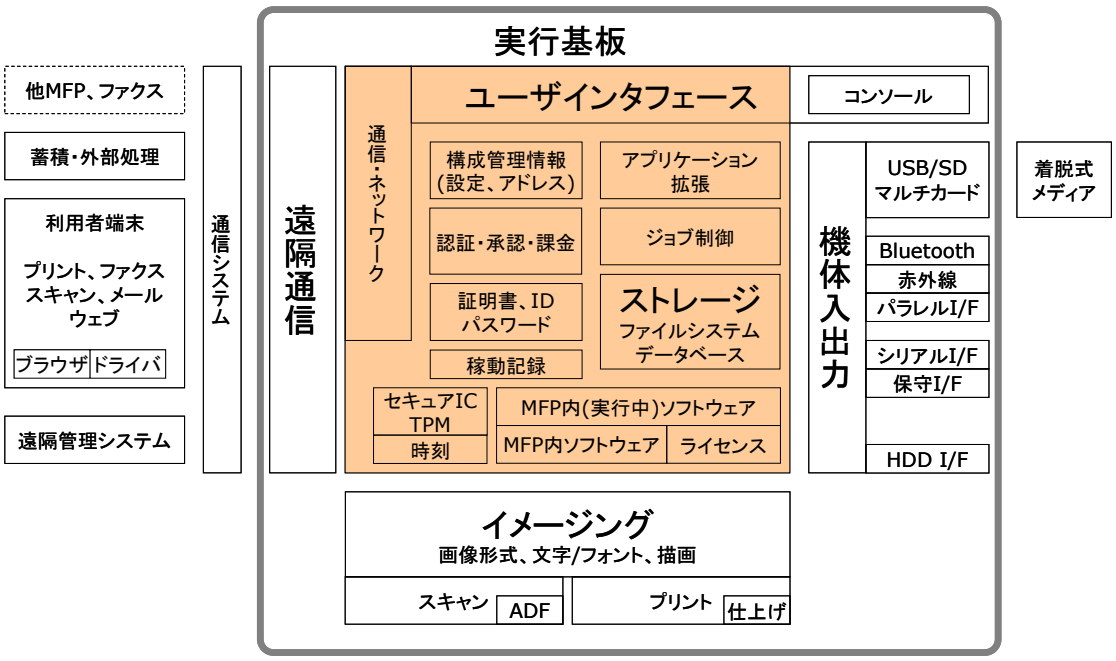


図 4-1 MFP 利用時のデータフローの構成図

4.1　プリント

下の図 4-2 はプリントのデータフローである。利用者端末から印刷用のイメージと印刷方法などの指示が MFP に送信される。MFP では、通信・ネットワークモジュール内のプリント受付機能が接続を受け付ける。接続を受け付けると、保護された通信路の確立を行い、利用者の認証後、ジョブを受け付けてファイルシステム内に保存する。認証は、MFP 内部の認証データを利用するか、遠隔管理システム上の外部認証サーバを利用する。

保存されたジョブデータをジョブ制御に通知したあとは、ジョブ制御が他のジョブとの調整を行いながらイメージングユニットにプリントを指示して、印刷物が出力される。

利用者端末を認証して、MFP がその利用者端末用のセッション情報を作成した場合は、ジョブの受け入れが完了した時点で、その利用者端末用のセッション情報を削除する。

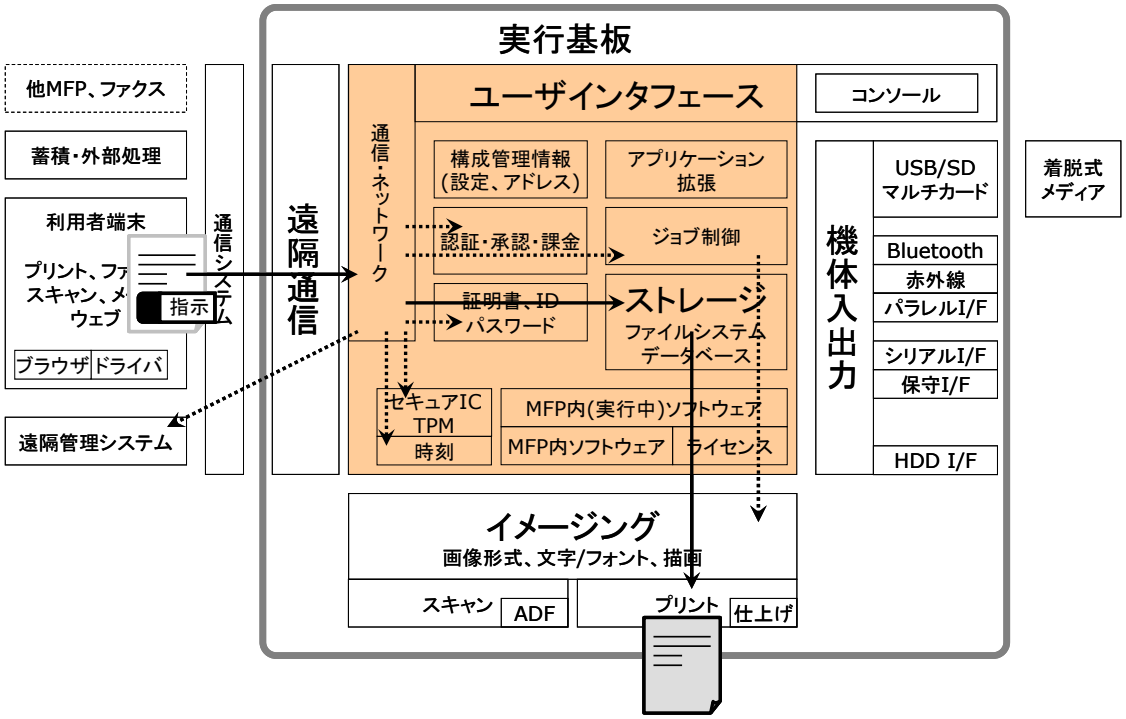


図 4-2 プリントのデータフロー

4.2　負荷分散印刷

下の図 4-3 は負荷分散印刷のデータフローである。この図はすでにジョブデータを受信した直後からのデータフローを示している。

ジョブ制御は、ジョブデータに含まれる指示から、構成管理情報を確認して、外部にある MFP のうち、どの MFP に印刷を指示するか、特定する。ジョブ制御は特定された依頼先のアドレスと印刷枚数などの新しい指示データを添えて、アプリケーション拡張にあるブラウザのプリントクライアント機能に印刷指示を行う。

プリントクライアント機能は通信・ネットワーク機能を利用して、他の MFP との間で保護された通信路を確立する。このとき、MFP 内部の証明書やパスワード、セキュア IC、時刻を利用する。保護された通信路を確立すると、プリントクライアントはストレージから指定の枚数でジョブデータを他の MFP に転送する。

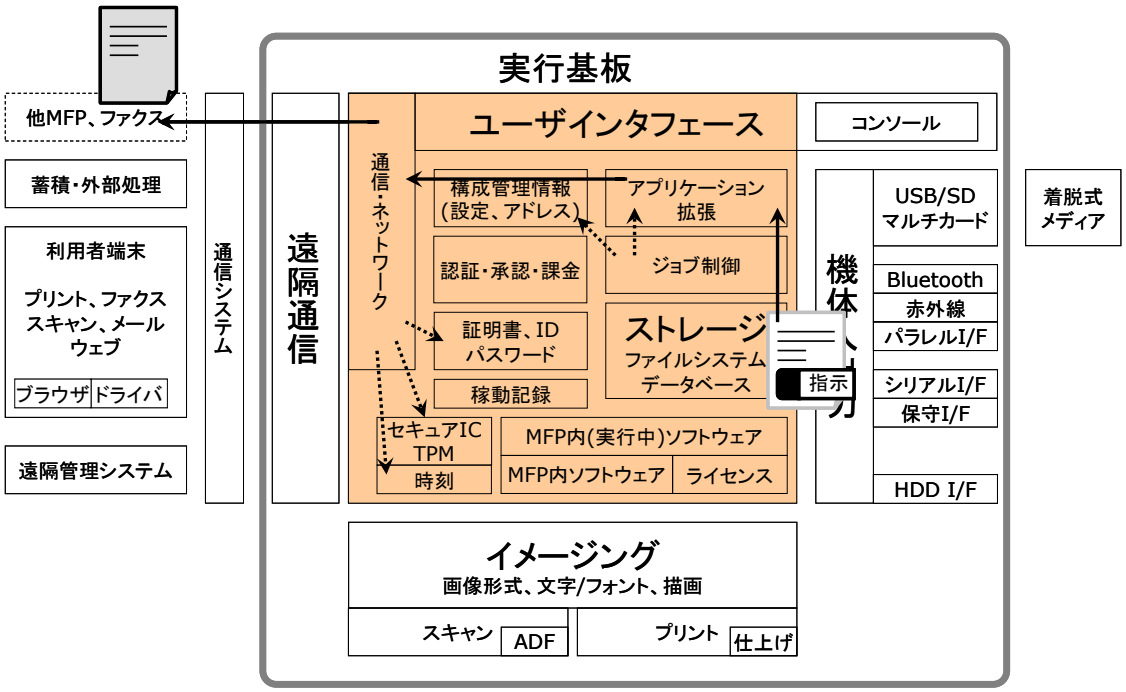


図 4-3 負荷分散印刷のデータフロー

4.3　スキャン to X、ファクス送信

下の図 4-4 はスキャンの結果を何かに配信する「スキャン to X」のデータフローを示した図である。ここで言う「X」とは、スキャン結果の配信先や配信する手段であり、ファイル（MFP 内のストレージ）、FTP、E メールなどが入る。ファクス送信も含む。

利用者は、MFP の前で、MFP に対してコンソールから作業の指示を行う。コンソールからは、スキャンを行って、スキャン結果を何に配信するかを指示する。スキャンの利用に認証が必要な場合は、ユーザインタフェースがコンソールか、MFP のシリアルインタフェースの先に接続した IC カード認証装置や生体認証装置で利用者として認証する。

利用者はスキャンの方法と宛先を指定する。宛先は MFP 内のアドレス帳から選択する。場合によって、アドレス帳は遠隔通信を経由して、遠隔管理サーバ上の共有のアドレス帳から検索することがある。利用者はこのときまでに原稿をスキャン台に置く。

上記で指定された、利用者の識別情報、宛先、スキャン方法はまとめて指示としてジョブ制御に渡される。ジョブ制御はイメージングに制御指示を行い、スキャンユニットでスキャン処理が行われる。スキャン処理の結果、作成されたファイルがイメージングからストレージに渡される。

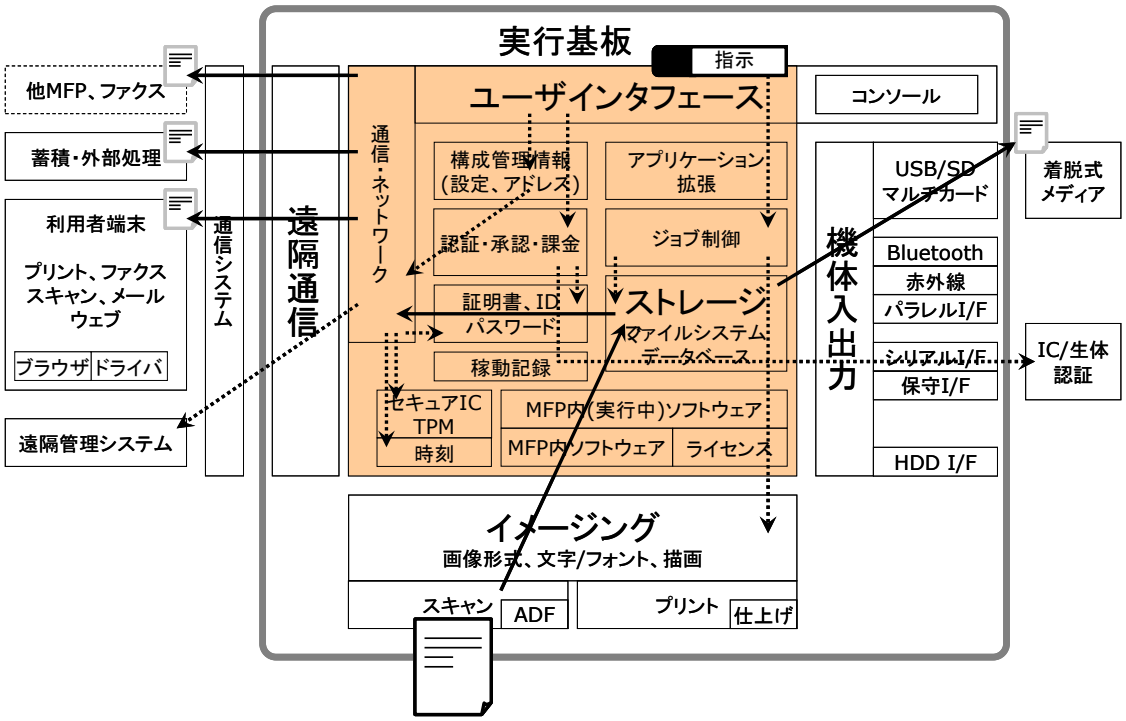


図 4-4 スキャン to X、ファクス送信のデータフロー

ストレージからは、ジョブ制御からの指示に従い、所定の宛先に配信を行う。以下に、この図での配信先を列挙する。

1)　他の MFP、ファクスへの配信: 図の左上
2)　蓄積・外部処理へのサーバ配信: 図の左上から 2 番目
3)　利用者端末へのサーバ配信: 図の左上から 3 番目
4)　着脱式メディアへの配信: 図の右上

上記配信先のうち、着脱式メディア以外については、保護された通信路の確立のために、証明書、ID、パスワードを使った相互認証を行い、セキュア IC と時刻を利用して保護された通信路を確立する。

上記配信先のうち、蓄積・外部処理については、ほとんどの場合、何らかの認証処理が必要になるだろう。その際は MFP 内部の認証データを利用するか、遠隔管理システム上の外部認証サーバを利用する。

すべての指定された宛先について配信が完了すると、この処理が完了する。

利用者は指示の作業が終了しログアウト手順を実行するか、MFP への操作がなく一定時間が経過すると、MFP は自動的に「証明書、ID、パスワード」に生成されたセッション情報を削除する。

4.4　ファクス受信

下の図 4-5 はファクス受信のデータフローを示している。ここではファクスを受信し、ストレージに格納されるまでの手順としている。利用者を認証した上での認証印刷については、プリントの手順で特定している。

図の左上にある「他の MFP、ファクス」で、原稿が読み取られるか、パソコンからファクスイメージが他の MFP、ファクスに送信され、「他の MFP、ファクス」から、「通信・ネットワーク」のファクス受信機能を使ってファクスイメージを受信する。ファクス受信機能には、PSTN ファクス、メールファクス、SIP ファクスがある。メールファクスの場合は、保護された通信路を確立するため、証明書、セキュア IC/TPM、時刻を利用する。SIP ファクスの場合、一般的には保護された通信路を動的に確立はせず、「通信システム」を閉域網や隔離することでセキュリティを確保している。

受信されたファクスイメージはストレージに格納され、受信結果がジョブ制御に渡される。ジョブ制御は構成管理情報にある、ファクスの発番号や着番号によるボックス振り分け条件を確認し、親展ボックスやサーバなどに配信するか、紙に印刷するかなどの、新たな宛先を特定する。

このあとの印刷の処理はプリント、印刷以外の処理はスキャン to X でイメージをストレージに格納したあとのデータフローと同じである。

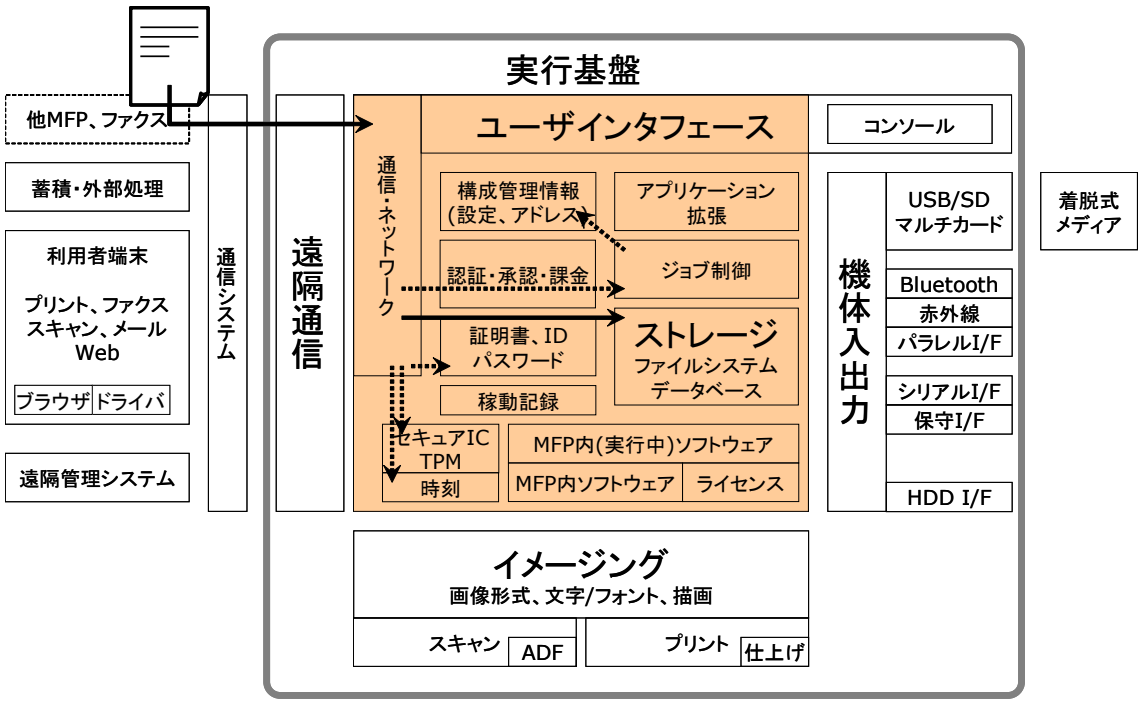


図 4-5 ファクス受信のデータフロー

4.5　コピー

下の図 4-6 はコピーのデータフローである。利用者はコンソールからコピーの指示を開始する。必要に応じて、利用者の認証が行われる。認証は MFP 内部の認証データを利用するか、遠隔管理システム上の外部認証サーバを利用して、パスワード、IC カード、または生体認証を使って行われる。また、利用者の認証を MFP の外部にある認証サーバと行う場合は、「通信・ネットワーク」を経由して「遠隔管理システム」上の認証サーバに、コピーをしようとする利用者の認証を要求する。

利用者はコピーの処理条件をコンソールで指定する。事前に設定された設定値のセットや、印刷の負荷分散を指定する場合は、設定構成情報の中に利用者や管理者が設定した情報を参照して利用する。

このときまでに利用者はコピーの原稿をスキャン台や ADF に設置する。

利用者によるコピー処理の指示が終わると、指示がジョブ制御に渡され、コピー処理が開始される。ジョブ制御は、イメージングにコピーの指示を行う。原稿がスキャンされ、ストレージに格納される。ストレージに格納されたイメージはプリントに渡されて印刷される。ストレージへの格納は、ハードディスクにファイルを作成する場合と、メモリ(一時メモリ、DRAM)上に格納される場合がある。

利用者は指示する作業が終了すると、コンソールでログオフするか、操作がない状態が一定時間経過すると MFP が自動ログオフし、「認証・承認・課金」にあるセッション情報が削除される。

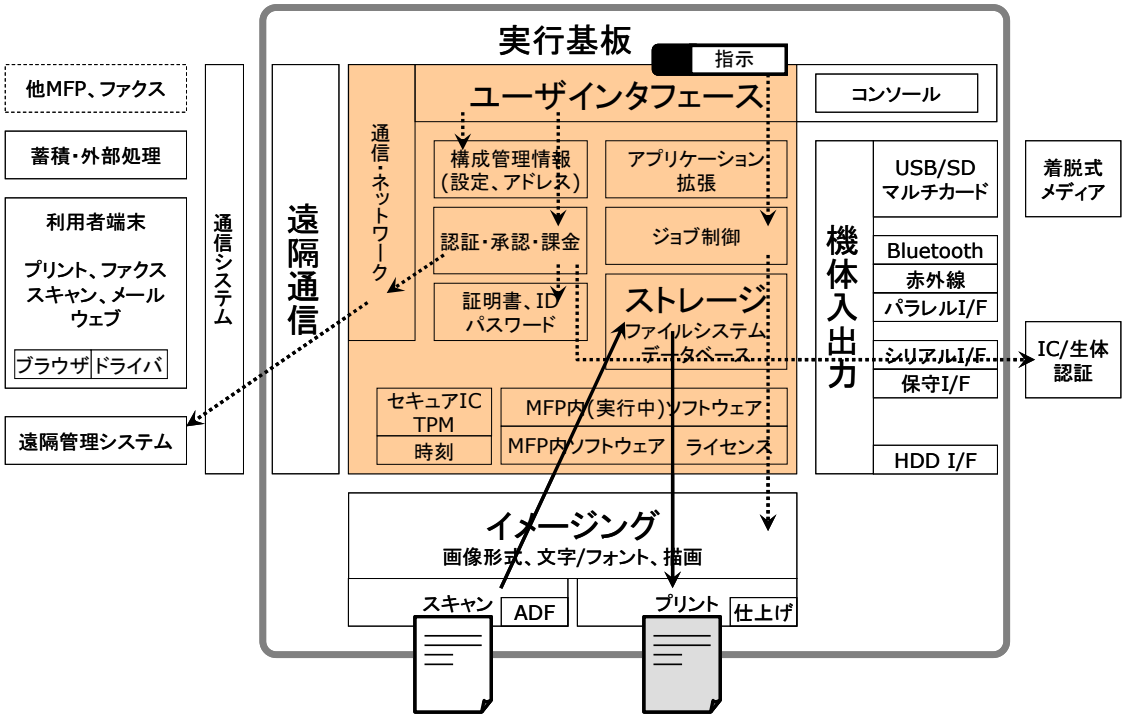


図 4-6 コピーのデータフロー

4.6　構成管理情報の設定、取得(コンソール)

下の図 4-7 は、MFP 本体の構成管理情報の設定、取得を行うときのデータフローである。MFP 本体の構成管理情報には、「証明書、ID、パスワード」や、「セキュア IC/TPM」への操作、「時刻」への変更を含んでいる。また、ここでは MFP のコンソールから指示を行う手順を示している。

MFP の管理者はコンソールから構成管理情報の変更指示を行う。そのために管理者の認証手順を行う。ユーザインタフェースは「認証・承認・課金」に指示して、管理者認証処理を行う。必要に応じて IC カードや生体認証を行う。IC カードや生体認証は場合によって「遠隔管理システム」にある認証サーバによる認証が必要である。

管理者認証が済むと、ユーザインタフェースで構成管理情報の設定メニューが表示されるようになり、「構成管理情報」「証明書、ID、パスワード」「セキュア IC/TPM」「時刻」の内容変更または上書き、追加、削除、または内容の取り出しと表示が行われる。セキュア IC/TPM については、秘密鍵などの重要な機密の情報は取り出しができないが、秘密鍵の名前や識別名などについては表示される。

管理者は作業が終了すると、ログアウト手順を実行し、MFP の「証明書、ID、パスワード」に生成されたセッション情報が削除される。

なお、ソフトウェアやライセンスについては保守員が変更するため、管理者は操作しない。

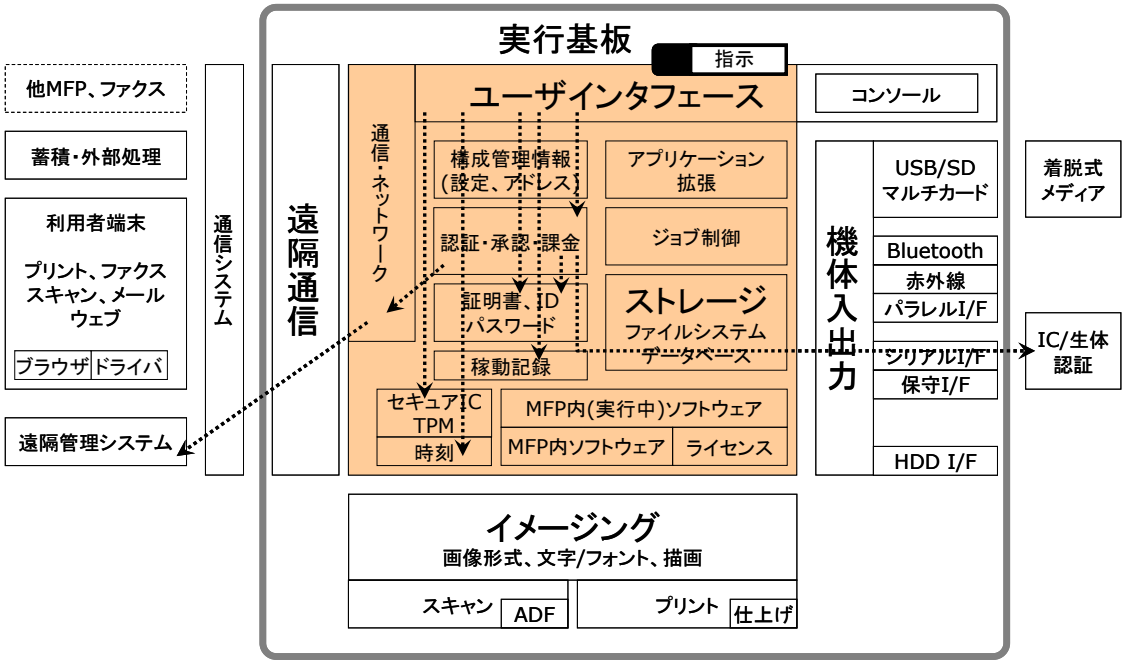


図 4-7 構成管理情報の設定、取得データフロー

4.7　遠隔通信経由での構成管理情報の設定、取得

下の図 4-8 は、遠隔通信経由で、MFP の構成管理情報の設定または取得を行うときのデータフローである。

管理者は遠隔管理システムにある、管理者端末から MFP の「通信・ネットワーク」内の管理用サーバに SSL や SSH などにより保護された通信路を確立し、ログインする。保護された通信路を確立する場合は「証明書、ID、パスワード」、場合によってはこれらに加えて「セキュア IC/TPM」、「時刻」を利用する。また、このあと遠隔から接続要求をしてきた管理者の認証を、MFP から遠隔管理システム上の認証サーバに対して行う。

管理者端末と MFP との間で保護された通信路が確立し、管理者の認証が完了すると、管理者はユーザインタフェースから提示された、設定ページやコマンドラインを操作して、MFP 内部の複数のデータを変化させる。「構成管理情報」については設定値の追加、変更、削除を行う。「証明書、ID、パスワード」についても追加、変更、削除の操作を行う。「セキュア IC/TPM」については秘密鍵とその属性情報の追加または削除を行う。「時刻」については変更のみ行う。共通の操作として、値かデータの読み取りがあるが、「セキュア IC/TPM」については秘密鍵の読み取りはできない。

管理者は作業が終了すると、ログアウト手順を実行し、MFP の「証明書、ID、パスワード」に生成されたセッション情報が削除される。

なお、ソフトウェアやライセンスについては保守員が変更するため、管理者は操作しない。

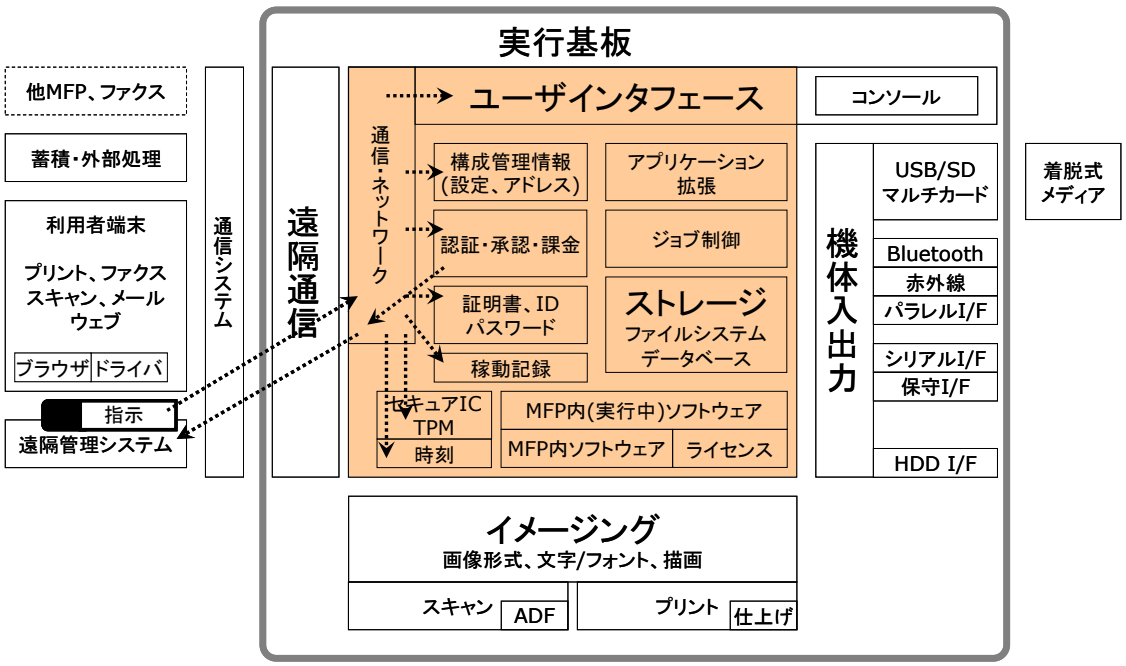


図 4-8 遠隔通信経由での構成管理情報の設定、取得データフロー

4.8　保守作業 部品交換、課金取得、診断

下の図 4-9 は保守作業 部品交換、課金取得、診断のデータフローである。

MFP の保守員はコンソールで保守員認証を行う。MFP 外部の認証手順についてはほかのデータフローと共通であるため割愛し、保守員の認証を MFP 本体内で行うデータフローのみを示している。保守員は MFP のコンソールからキーボード入力などで保守員の ID とパスワード文字列を入力し、保守員認証を行う。場合によっては、保守用インタフェースから保守用端末を接続し、保守用端末上での簡易メニューかコマンドラインを操作する。保守用インタフェースについては、その存在自体が不明な場合と、存在する場合、認証が不要な場合もある。

保守員認証が完了すると、保守員用のメニューが表示されるので、保守員はコンソールから必要な処理を選択する。

点検などの保守作業と部品交換では、通常は診断処理を行う。診断処理では、図中のハードウェアの個別の診断機能の実行と結果取り出し、ファイルやデータの一貫性の検査などがあるが、MFP 内部の診断機能は保守用の取扱説明書に記述され、一般には公開されていないため確認ができていないが、診断可能な対象や項目は MFP ベンダや機種によって異なると考えられる。

保守員は作業が終了すると、コンソールでログオフし、「証明書、ID、パスワード」に生成されたセッション情報が削除される。

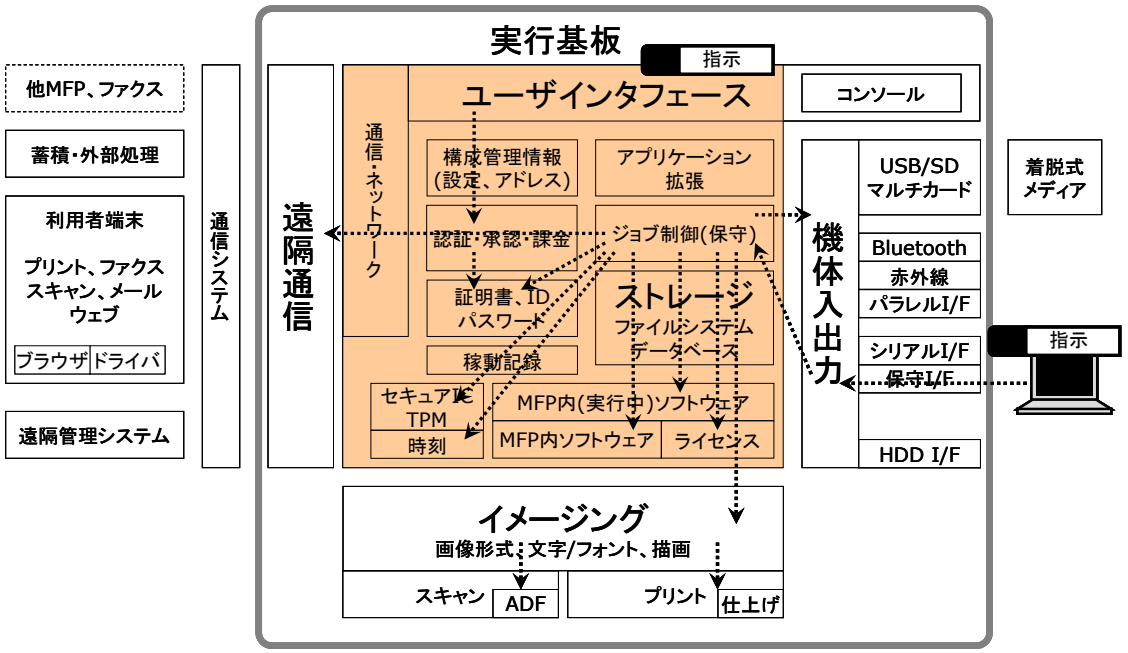


図 4-9 保守作業 部品交換、課金取得、診断のデータフロー

5. MFP の守るべき資産

5.1　MFP を利用する環境での一次資産

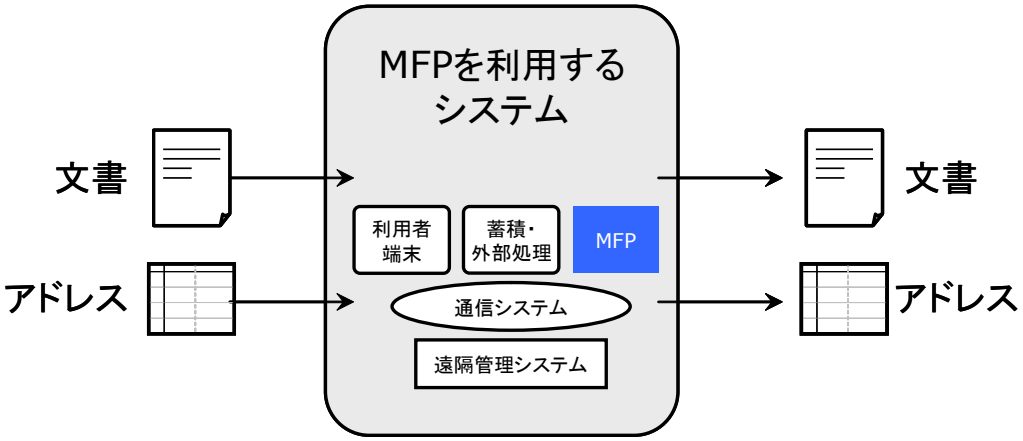


図 5-1 MFP 利用時のデータフロー

利用者から見て、MFP を利用する直接的な目的は、文書の保存と配布である。利用者が文書の保存と配布を行うときに、直接的に守るべき情報資産を「一次資産」として位置づける。上の図 5-1 は一次資産である文書とアドレスが MFP を通じて処理が行われる概念を示している。文書は保存や配布したい内容の情報である。アドレスは配布したい宛先をあらわす情報である。

ただし、一次資産は情報の資産であるため、実体を持たない。実体としての情報資産は具体的にはそれぞれの場面で異なる。このように、MFP を情報システムのひとつとして利用するときに、一次資産を守るために必要になる具体的な情報資産を、「二次資産」と位置づける。例えば、文書については紙媒体の場合は原稿や印刷物として具体化する。MFP 上では電子化されたイメージやページの描画内容を記述したデータがジョブデータと呼ばれるファイルやメモリ上のビット列して扱われている。また送付先や配信先のアドレスはジョブデータの中に、制御命令の一部として格納されている。また、認証やセキュリティのための情報も、一次資産を守るために必要となる、二次資産と考えられる。

なお、7 章以降、一次資産と二次資産を併せて「保護資産」と定義する。

5.2　MFP を利用するために守るべき対象としての二次資産

下の表 5-1 は、MFP の利用環境で関連する二次資産を一覧表にしたものである。大きく 4 つのカテゴリに分類した。

「MFP 本体」は MFP の機器とソフトウェアなどである。USB メモリや SD メモリカードなどの着脱式メディアは、本体ではないが、本体と密接する着脱式メディアであるため MFP 本体に分類した。MFP はこれら機器とソフトウェアがそろうことで、稼動させることができる。

「実行時データ」はコピーやプリントなどの処理が行われる間に交換される情報資産を指す。

「他システム」は、MFP が稼動するために、MFP の外部から認証や管理などのサービス提供する、外部のホストや機器のことを指す。本調査では、MFP 本体の

脆弱性が中心となっているため、これら他システムについては、各他システムの内部の詳細については検討せず、他システムの外部インタフェースにのみ注目して分析を行う。

「稼動結果情報」は、処理後に得られる原稿や印刷物、ファイルや記録を指す。

表 5-1 MFP を利用するために守るべき対象としての二次資産

カテゴリ	二次資産
MFP本体	本体機器 （ハードウェア）
	MFP内ソフトウェア
	使用ライセンス、保守ライセンス
	着脱式メディア
実行時データ	ジョブデータ （スプール,イメージ,宛先,制御）
	管理構成情報
	電子証明書、ID、パスワード、 セッション情報
	正しい時刻

カテゴリ	二次資産
他システム	通信システム (スイッチ、DHCP, DNS, NTP)
	遠隔管理システム (認証、構成管理、監視、保守)
	一般利用者端末
	蓄積・外部処理 (スプーラ、共有フォルダ、メール、 業務システム)
稼動結果情報	原稿、印刷物
	MFP内共有ファイル
	利用履歴、監査記録
	MFP利用課金情報

次の章では、これら二次資産について、さらに詳細に脅威の分析を行うが、以下に、二次資産のそれぞれについて、その概要とセキュリティ上要求される主な点などを参考にまとめておく。

5.3 MFP 本体

5.3.1 本体機器(ハードウェア)

MFP の本体機器を指す。「3.6 MFP 内部のハードウェア」で説明したように、いくつかのユニットに分割されている。正しい本体機器が装着され、配線されている必要がある。

5.3.2 MFP 内ソフトウェア

MFP を動作させるためのソフトウェア。「3.7 MFP 内部のソフトウェア」で説明したように、複数のモジュールやアプリケーションに分かれて搭載されている。

ソフトウェアは追加や更新が比較的容易に行えるが、MFP 内には正しいソフトウェアが必要である。不正ソフトウェアは排除される必要がある。

5.3.3 使用ライセンス、保守ライセンス

利用者が MFP を利用する間、搭載しているソフトウェアの利用権や、保守サービスの利用権が使用ライセンスや保守ライセンスとして MFP ベンダか販売業者、

保守業者から発行され、それぞれの MFP 内部に登録される。
ライセンスにはさまざまな契約条件があるが、一般的にライセンスは期間が限定されており、契約期間が過ぎるとライセンスが無効になり、そのライセンスに該当する機能も停止する、という前提で分析を行う。逆に、契約していないライセンスが登録されると、予定していなかった機能やサービスが動作してしまうこともある。

5.3.4 着脱式メディア

USB フラッシュメモリや SD メモリカードなどのように、簡単に挿抜して移動できるメディアのことを指す。MFP 本体ではないが、直接本体に装着してよいハードウェアであるため、本体に分類した。
着脱式メディアには、利用者が文書を交換するために利用するものと、保守員が MFP の管理情報やソフトウェアの構成などを行うためのものがある。利用者向けの着脱式メディアのスロットと、保守員向けの着脱式メディアのスロットは別になっており、用途も異なるが、脅威と脆弱性の一覧では、異なる扱いが必要な場合はそのつど記述する。

5.4 実行時データ

5.4.1 ジョブデータ(スプール、イメージ、宛先、制御)

ジョブデータとは、プリント、ファクス、コピー、配信などのイメージデータと制御情報を記録したものである。
イメージデータには、原稿や印刷物の表示領域の画像を再現するための、デジタル化されたイメージや描画命令などが含まれる。
制御情報には、転送先のアドレスまたは宛先とその転送手順、印刷物の排出先や仕上がりの条件などがある。仕上がり条件には、印刷物での画像の配置方法などの画像処理方法、印刷部数や出力トレイなどが含まれる。仕上がり条件に従った処理は、フィニッシャと呼ばれる装置で処理される。
また、制御情報には認証情報を含むことがある。例えば、利用者を認証してプリントする場合で、認証サーバを利用せず MFP 内に設定されたユーザ ID だけを利用した簡易な認証プリントの場合は、ジョブデータ内に一般利用者端末で入力されたユーザ ID が書き込まれ、MFP 内の利用者ごとのスプールにジョブデータが保存されるものもある。

5.4.2 管理構成情報

MFP を所定の条件で動作させるために MFP に設定、登録する情報、または MFP 内に保存された設定情報。
MFP が所定のサービスを提供し、必要なセキュリティを確保するために認証などセキュリティ機能を動作させ、他システムと連携するために必要なアドレスやパス名、番号、呼び名の文字列など。
管理構成情報には、MFP が所定の機能を停止させるための情報や、特定の利用者には特定の機能を利用させない、などの制限のための情報も含む。

5.4.3　電子証明書、ID、パスワード、セッション情報

認証を求められたときに応答する電子情報。電子証明書は秘密鍵を検証できる公開鍵を持ち、秘密鍵はセキュア IC や TPM などの格納装置に保存し、認証時にはセキュア IC に計算処理を行わせて照合する。公開鍵は秘匿する必要は無い。ID とパスワードは認証処理時に照合処理が必要なため MFP 内部のストレージか、MFP 起動時に参照できる不揮発メモリ内に格納しておく。

セッション情報は、サービスを利用する利用者や他システムの利用セッションごとに許可を与えるためのトークンのようなもので、ウェブブラウザのクッキー情報や、URL に含まれるセッション ID、HTTP POST リクエストの要求データ内に含まれるセッション ID なども該当する。

5.4.4　正しい時刻

ファクスで送受信の履歴を記録するときに必要になる。稼動の履歴情報を記録する際にも、記録としてそのときの時刻もいっしょに記録する。稼動の履歴情報にある時刻は、他システムや他の MFP の記録と照らし合わせて確認するときのために、同じ正しい時刻に合わせておく必要がある。

また、暗号通信や署名・検証を行うための基本となる情報である。自己署名証明書の時刻としても重要である。

認証・認可・課金の機能では、認証された時刻や認可を継続できる時間幅などを管理するため、認証サーバやシングルサインオン機能を提供するサーバと MFP の間で、同期した正しい時刻が必要である。

ソフトウェアのライセンスについては、ライセンスの期間が特定されている場合は、正しい時刻との比較が必要である。

5.5　他システム

5.5.1　通信システム(スイッチ、DHCP、DNS、NTP)

MFP 本体と遠隔通信をする他システムを接続するための通信機器と、ネットワークの基盤的な情報を提供するサーバ。

通信機器には、Ethernet スイッチやルータ、あるいは無線 LAN のアクセスポイントなどと、これら機器の配線が含まれる。

ネットワークの基盤的な情報を提供するサーバには、DHCP サーバ、DNS サーバ、NTP サーバがある。DHCP サーバは、IP アドレスの自動割当とルータの IP アドレス、DNS の IP アドレスの配布を行う。DNS サーバはホスト名から IP アドレスを検索する要求やその逆の検索などに応答する。NTP サーバは複数の MFP やシステム内のホストの間で時刻を同期させるため、現在の正確な時刻を応答する。

5.5.2　遠隔管理システム(認証、構成管理、監視、保守)

遠隔管理システムには、認証サーバと、構成管理サーバ、監視サーバ、保守用端末などが含まれる。管理者が MFP の設定変更などに利用する端末上の管理用アプリケーションや MFP 上のウェブサーバは遠隔管理システムの一部である。

認証サーバは利用者の ID とパスワード、または証明書情報などを集中して保持し、MFP を含む他のホストからの利用者を認証する要求に応答する。構成管理サ

ーバは管理者が複数の MFP を一括して設定できるなどの機能がある。監視サーバは 1 台以上の MFP の稼動状態を定期的に取り出して、異常があると管理者や別のシステムに通報をする機能がある。

保守用端末は MFP の保守が必要なときに MFP の内部の診断や、ソフトウェアやライセンスの追加などの作業を行う。こうした保守作業については端末ではなく保守サーバが定期的に処理を行う場合もある。

5.5.3 一般利用者端末

プリント、ファクス送信、スキャン開始、MFP 内に一時的また長期に格納されたファイルの取得など、MFP の利用者向けのサービスを利用するための端末。利用者端末がファクス受信するときは MFP 内からのファイル取り出しを行う形になる。利用者端末からコピーを実行することはない。

これら MFP の利用者向けのサービスは、保守員が利用することはない。試験用に利用する場合は利用者として実行するものとする。また、利用者端末から MFP の設定やアドレス帳などの構成管理情報を変更することは遠隔管理システムに含めている。

利用者端末上では一般的に、特定の機種の MFP に対応したドライバソフトウェアを追加インストールする。ドライバソフトウェアには、MFP にプリントやスキャンイメージ取出しを指示するときに必要なパス名や、ID・パスワードなどを設定することがある。メールファクスを利用する場合は、その利用者のメールアドレスやクライアント証明書を指定する場合もある。

5.5.4 蓄積・外部処理(スプール、共有フォルダ、メール、業務システム)

MFP の外部にあって、文書の蓄積や配信を行う。一般的には直接人が操作しないサーバとして動作している。MFP を利用するための情報システムの一部であり、ジョブのスプールサーバ、共有フォルダやメールサーバ、業務システム用のウェブサーバなどがある。スプールサーバは、MFP へのプリントジョブを一時保留しておくサーバで、利用者に対する認証機能や、MFP に対するジョブデータの分配機能、負荷分散処理機能がある。共有フォルダは、電子ファイルを格納するディスクをネットワーク上で複数の利用者が共有するためのサービス。メールサーバは、メールファクスやメールでの配信に利用される、メールの送信受付サーバ(SMTP)、メールの転送サーバ(SMTP)、メールボックス内への電子メールメッセージを提供するメールボックスサーバ(POS3, IMAP4)からなる。

メールの転送サーバとメールボックスサーバは、MFP を利用する組織の外にある場合がある。また、ファクスの宛先に当たる MFP も他組織である場合もある。これらの他組織の間では、機密情報保護契約などが結ばれて、それぞれが交換した機密を保護することを前提とする。ただし、MFP の脆弱性については、異なる MFP ベンダや機種の MFP を利用したとしても、どちらの組織にも同じように脆弱性が発生するものとみなす。

5.6 稼動結果情報

5.6.1 原稿、印刷物

コピーまたはスキャンで MFP に読み取りさせる紙が原稿。コピー、プリント、ファクスで MFP から出力される紙が印刷物。文書の内容を含む。

5.6.2 MFP 内共有ファイル

MFP 内部で共有されている電子ファイルで、文書のイメージを含む。一部は宛先や、PDF やジョブデータのように追加の制御情報を含むものもある。共有ファイルは MFP の外部の利用者端末が閲覧、更新することができる。

5.6.3 利用履歴、監査記録

ある MFP 上で、どの利用者がいつ何をしたか、どこから何のリクエストがあり、どのような結果になったか、という情報。サーバやホストのアドレスや、処理を行ったときの認証 ID を含むことがある。

利用履歴と監査記録は MFP 内部に記録する場合と、MFP の外部に記録する機能がある。一般的に、監査記録は管理者のみがアクセスできるようにアクセス制御される。管理者が定期的に監査記録を確認することにより、不正アクセスやセキュリティ侵害がないことを確認し、インシデントの早期発見と対応を行うことができる。

5.6.4 MFP 利用課金情報

MFP でプリントやコピーをした枚数や回数の情報を含む。これらの情報は利用者から手動、もしくは自動的に MFP ベンダ等に通知され、課金に利用される。

6. 脅威から想定される脆弱性

本章では、MFP の利用環境における脅威の一覧から、それぞれの脅威において原因となると考えられる脆弱性を列挙する。

6.1 脅威の抽出

本章では、脅威を網羅的に特定するため、情報セキュリティの要求事項を、図 6-1 に示す 7 つのタイプごとにあてはめて検討する。

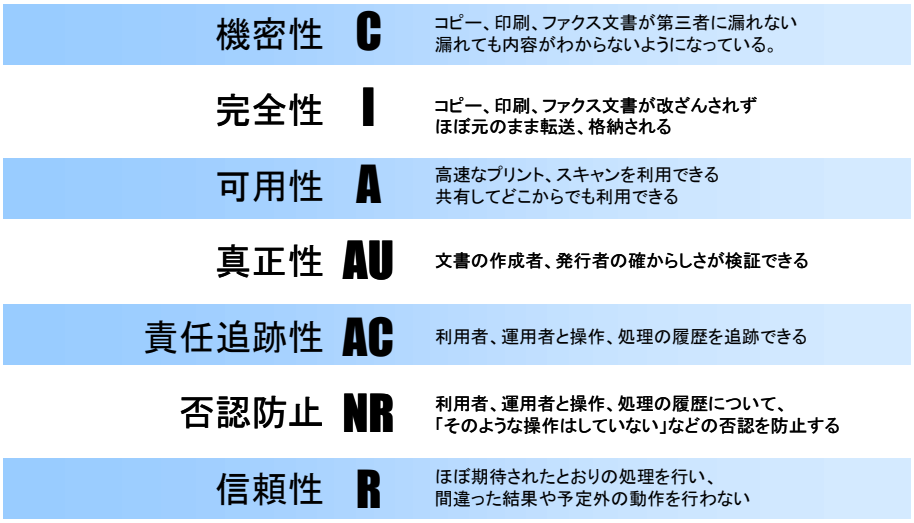


図 6-1 情報セキュリティの要求事項 – 7 つのタイプ

本章では、5 章で特定した 16 種類の二次資産のそれぞれについて、セキュリティの要求事項を破る想定を行い、脅威を列挙する。列挙した脅威は、次の「6.3 本体機器（ハードウェア)」から、表の「T. この二次資産に対する脅威」の列に記録する。さらにこれらの脅威それぞれについて、現段階である程度の攻撃手法や、誤操作などの実現性が想定できる「M. この脅威を実現する攻撃手法または事故の例」をそれぞれ例示し、事故の原因として考えられる脆弱性を「V. この攻撃例または事故例の原因となる脆弱性」に列挙する。

なお、本章で列挙する脆弱性は攻撃に必要な攻撃者能力や攻撃できる機会を区別していない。利用者は MFP で取り扱う保護資産や MFP を利用するオフィスのセキュリティポリシに従って考慮すべき項目を検討し、対策が必要か否かを判断すべきである。

6.2 脅威に対抗すべき関係者

本章で列挙する脆弱性には、対抗すべき関係者を付加している。関係者は、利用者と開発者の 2 種類を設定している。利用者は MFP を調達して実際に利用する企業であり、その企業の責任者、情報資産や個人情報の管理者、そして一般社員や派遣社員を含む。一方の開発者は機能的なセキュリティ対策を盛り込む立場であり、MFP ベンダにおいて管理面を含めて設計、開発、及びセキュリティに関す

る機能試験、納品までの責任を負う関係者と、納品後の保守する側に係る保守員等の関係者の総称である。

列挙した脆弱性に対して対策すべき関係者に「○」を付けて分類している。開発者が実装すべきセキュリティ機能が実装されていない場合、利用者が運用面でその脆弱性をカバーすることが考えられる。一方、利用者が MFP を劣悪な環境で運用することで発生する MFP の誤動作や停止を、開発者が電源断保護機能などの機能面でカバーすることも考えられる。しかし、本章では、一般的に考えて本来対策すべき関係者を選定している。対応すべき関係者の欄に斜線が引いてある項目は MFP や関連するアプリケーションの正常な機能による反応であり、一般的に利用者や開発者が対応できない項目である。

6.3 本体機器(ハードウェア)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体内部の端子や配線の途中に直接接続されて盗聴される。または、MFP 本体内部の機器に電気的な影響を与えられ、盗聴される	・MFP 本体内部の基板上のバス、デバッグ端子、モジュールのバス端子、機器の接続端子などに電気的に接続し、バス上または端子上の通信データを盗聴する	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
			・MFP 本体内部のユニット間インタフェースが標準インタフェースとなっており接続方式や通信方式を容易に予測できる脆弱性		○
			・MFP 本体のユニット間インタフェース上の通信データが保護されていない脆弱性		○
		・攻撃者は電源スイッチ ON または OFF 操作直後に、特定のキーボード操作を行うか、シリアルポートからブレーク信号を送るなどの操作により、認証操作なしで MFP を特権状態で動作させ、MFP の保護機能をオフにする	・機能モジュールが電気的な影響で停止または誤動作する脆弱性		○
			・MFP に電源投入後の起動中または停止指示後の停止処理中に特定のキー操作またはハードウェア割り込みを発生させると特権状態で動作してしまう脆弱性		○
		・攻撃者は保守員になりすまして MFP の実行基板上の DRAM を含むボードを急速冷却して取り出し、DRAM 内部のデータを読み取り、DRAM 上に残されていた暗号鍵が攻撃者に漏洩する	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
			・DRAM 上の暗号鍵が保護されていない脆弱性		○
		・攻撃者が実行基板上の不揮発メモリ(FlashROM など)か HDD を取り出して MFP 内ソフトウェアのコピーを容易に入手する	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
			・実行基板上のストレージに格納されたソフトウェアが保護されていない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP 本体機器の一部または全部の機器、配線が入れ替えられる	・MFP 本体内の HDD を入れ替えられ、HDD 内の保護されていない機密文書や、保護されていないアドレス帳、保護されていない証明書、ID、パスワードを、攻撃者が入手する[本体機器の入れ替え]	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性（本体内部の機器や端子に直接、第三者がアクセスでき、MFP 本体内部に機器や部品を追加、交換できる脆弱性） ・ストレージに格納されているデータが保護されていない脆弱性	○	○
		・攻撃者によって、印刷の排紙口、ADF の内部に追加のスキャナを装着させられ、機密の原稿と印刷結果のイメージを、追加スキャナまたはフラッシュメモリの交換で攻撃者が入手する[本体機器の入れ替え]			
		・攻撃者が実行基板上の不揮発メモリ(EEPROM, NVRAM など)を交換して MFP 用の設定、構成管理情報を書き換える[機器の入れ替え]	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性 ・不揮発性メモリが容易に識別でき、交換可能な脆弱性	○	○
3. 可用性	・本体機器の一部または全部が盗難または破壊され、MFP を利用できない ・電源、通信の配線が抜かれるか撤去されて MFP を利用できない ・電源の電圧が頻繁に大きく変動するためにMFPが起動せず、動作しても途中で停止する	・MFP 本体内部の暗号化用ハードウェアモジュールや実行用一時メモリの盗難、破壊により MFP が利用できなくなる	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性（本体内部の機器や端子に直接、第三者がアクセスでき、MFP 本体内部の一部機器や部品を持ち出せる脆弱性）	○	
		・MFP 本体用、スキャナ用の電源ケーブルが盗難にあい、MFP を利用できなくなる			
		・MFP 本体内部の一部機器に電源系統や信号切り替え系統などに、直接接続して電気的な負荷を与えるか、電磁波によって電気的な負荷を与えて、MFP の動作を停止させる	・MFP が攻撃者から物理的に操作可能、または付近に不正な機器を設置可能な状態にある脆弱性 ・機能モジュールが電気的な影響で停止または誤動作する脆弱性 ・ハードウェアモジュールが外界からの電磁波を受けて誤動作する脆弱性	○	○ ○
4. 真正性	・本体に装着されている機器が適切な正しい機器であるかどうか確認できないため、機器の追加、取り外しがあってもわからない	・MFP 本体内に偽の HDD ユニットを装着し、機密文書のジョブデータやファイルそのものを記録させ、HDD を交換することで攻撃者が機密文書とアドレスの一部を入手する	・本体内または本体に直接接続されている HDD などが、正当な機器であるかどうか確認できない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
5. 責任追跡性	・本体機器の一部または全部の追加、取り外しがあっても、その詳細や原因を確認できない	・攻撃者によって MFP 本体内の HDD を入れ替えられたが、いつ、だれが入れ替えたかわからないため、対策を検討できない	・本体内または本体に直接接続されている HDD などを追加・取り外ししても記録が残らない脆弱性		○
6. 否認防止	・本体機器の一部または全部の追加、取り外しが、保守員によって行われたことがあるのに、特定の保守員が行ったということを立証できない	・攻撃者によって MFP 本体内の HDD を入れ替えられたが、MFP が記録する保守の監査履歴には、なりすまされた偽の保守員 ID が注入されたため、対策を検討できない	・履歴に他の利用者の名前、ID・パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性) ・履歴の記録を行うとき、任意の時刻や、任意のユーザ ID を記録できてしまう脆弱性		○ ○
7. 信頼性	・本体機器内の一部機器や配線の間違い、部品の欠落、不足などにより、適切な処理が行われない	・MFP 本体内部の配線が間違っており、暗号化モジュールがバイパスされ、HDD への暗号化処理が行われずにデータが記録され、MFP 廃棄時に残存していた機密の文書が漏洩する ・一時メモリの不足があると、処理の一部だけが不完全な出力や配信が行われ、不具合があったこと自体がわからない ・MFP 内部で電子証明書の生成を行う際に、MFP 内部にセキュア IC/TPM が存在しない場合、電子証明書の秘密鍵が保護されていないハードディスク上のファイルに保存され、MFP 内部にアクセスした攻撃者に秘密鍵が漏洩する	・本体機器内の配線または装着箇所の間違い ・「基本動作」や「セキュリティモード」などの所定の用途を実現するときに、MFP 本体内部の機器と配線の構成(リソース容量や処理能力、機能の有無など)が正しいかどうか検証できないか、検証していない脆弱性		○ ○

6.4 MFP 内ソフトウェア

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 内部のソフトウェアが漏洩する ・MFP 内部の実行中のソフトウェアの情報が漏洩する	・MFP 内部に格納されたソフトウェアを遠隔の管理システムから追加、更新するときに、途中の通信システム上で盗聴され、ソフトウェアが漏洩する	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性		○
		・MFP 内部のデバッグインタフェースに接続し、認証なしでデバッグインタフェースを制御し、MFP 内部のファイルシステムに指示してソフトウェアをダウンロードする	・デバッグインタフェースは JTAG や GDB など標準的なコマンド体系が実装されており容易に推測される脆弱性 ・MFP 内部のソフトウェアを取り出すインタフェースが稼動し、認証なしで利用できるようになっている脆弱性		○ ○
		・MFP 内部で動作するソフトウェアのいずれかの脆弱性を利用して任意のコードを注入し、(特権モードを取得して、)MFP 内部のファイルシステムに指示してソフトウェアを取り出す	・MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モード(管理者モードまたは MFP 内部の権限不要状態)での制御を奪取される脆弱性		○ ○
		・攻撃者が、本来残存していないはずの MFP のデバッガインタフェースに接続することで、MFP 内部の実行中のソフトウェアのシンボル名、実行時アドレス、機械語命令を入手し、その MFP 用に攻撃コードを開発し、販売する	・MFP のデバッグインタフェースが動作したまま残っている脆弱性(MFP 内部の機械語レベルでのソフトウェアの実行状態が容易に奪取または制御される脆弱性)		○
		・攻撃者が実行基板上の不揮発メモリ(FlashROM など)にアクセスして MFP 内ソフトウェアのコピーを容易に入手し、このソフトウェアの内容と動作を容易に解析して、脆弱性を特定し、攻撃コードを開発し、販売する	・MFP 内ソフトウェアを取り出し、容易に解析またはリバースエンジニアリングできる脆弱性		○
		・あるサードパーティが MFP 用の SDK を利用して開発した拡張アプリケーションで、MFP 内部のアドレス帳の内容を認証なしですべて応答する機能が悪用され、アドレス帳の内容が漏洩する	・SDK を利用してサードパーティが開発した拡張アプリケーションが MFP 内部の特権モードで動作するとき、特定の機密のデータを認証なしで公開してしまう脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP 内ソフトウェアの一部または全部が不正なソフトウェアに入替、追加させられるか、一部ソフトウェアが停止または削除され、適切な処理ができない(実行前、実行中)	・MFP 内部で、利用されないはずの拡張アプリ実行サービスが動作しており、攻撃者が任意の命令を実行させて、機密の文書を入手する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(動作させていないサービスを誤って動作させている場合) ・MFP 内部で動作させていないはずのサービス、または待ち受けていないはずのポートが開いている脆弱性	○	○
		・MFP 内部の一部ソフトウェアが、第三者や利用者でも書き換え可能な場所に配置されるため、攻撃者が任意のコードを追加して、MFP の処理の途中で機密の文書を入手する	・MFP 内部のソフトウェアが、保守員以外でも書き換え可能な場所に配置されている脆弱性		○
		・MFP 内部のソフトウェアを遠隔の管理システムから追加、更新するときに、途中の通信システム上で通信データが改ざんされ、不正なソフトウェアが注入される	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性		○
		・MFP 内部または外部のデバッグインタフェース、ソフトウェア交換インタフェースに接続し、認証なしでインタフェースを制御し、MFP 内部のファイルシステムやソフトウェア更新機能に指示して不正なソフトウェアを追加、更新する	・MFP 内部のソフトウェアを追加、書き換えるインタフェースが稼動し、認証なしで利用できるようになっている脆弱性		○
		・攻撃者が LPR の入力脆弱性を利用して不正コードを注入することにより、MFP 内部の監査記録機能が停止させられ、操作履歴が記録されないまま稼動を続けたため攻撃者のその後の操作内容がわからないまま攻撃の被害にあった	・入力されたデータにより MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モードでの制御を奪取される脆弱性		○ ○
		・攻撃者が MFP の入力脆弱性を利用して、MFP が受け付ける特定のサービスポートでの認証機能だけがバイパスされるように実行中のソフトウェアにフックを挿入し、以後攻撃者が認証なしで MFP を攻撃し、他システムへのなりすましのアクセスが行われ、他システムの業務データが漏洩する	・MFP 内部で実行される特定のソフトウェア機能がバイパスまたは停止させられたまま実行が継続してしまう脆弱性		○
		・攻撃者が MFP の入力脆弱性を利用して、MFP 内部の乱数生成機能を改ざんし、常に同じ乱数を返すようにする。この乱数生成機能を使った暗号化処理で処理された SSL/TLS の暗号通信を、攻撃者が解読し、他システムのパスワードや機密の文書が漏洩する			

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・MFP 内ソフトウェアの一部または全部が削除または破壊されるか、ソフトウェアの脆弱性を悪用して動作を停止させられ、MFP を利用できない(実行前、実行中)	・MFP 内部のソフトウェアを遠隔の管理システムから更新するときに、途中の通信システム上で通信データが改ざんされ、破壊されたソフトウェアが注入される	・MFP と遠隔の管理システムとの間の通信が保護されていないか、保護が不完全である脆弱性		○
		・MFP 内部、外部のデバッグインタフェース、ソフトウェア更新インタフェースに接続し、認証なしでインタフェースを制御し、MFP 内部のファイルシステムかソフトウェア更新機能に指示して、ソフトウェアを削除するか、破壊されたソフトウェアで書き換えする	・MFP 内部のソフトウェアを削除、書き換えするインタフェースが稼動し、認証なしで利用できるようになっている脆弱性		○
		・MFP 内部で動作するソフトウェアのいずれかの脆弱性を利用して任意のコードを注入し、(特権モードを取得して、)MFP 内部のファイルシステムに指示してソフトウェアを削除、書き換えする	・MFP 内部で任意のコードが実行させられる脆弱性 ・MFP 内部の特権モードでの制御を奪取される脆弱性		○ ○
		・SDK を利用した一部の拡張アプリケーションがメモリを大量に消費し、MFP 本体のサーバ機能が停止してしまう	・SDK を利用した一部の拡張アプリケーションが CPU またはメモリなどのリソースを大量消費し、MFP 本体の機能か、拡張アプリケーションの機能を停止させる脆弱性		○
4. 真正性	・MFP 内ソフトウェアまたはダウンロードやメモリで導入しようとするソフトウェアが適切なソフトウェアかどうか確認できないため、ソフトウェアのすり替えがあってもわからない	・保守員が間違って古いバージョンのソフトウェアを導入してしまい、一部の機能が使えなくなってしまう	・MFP に追加、更新されるソフトウェアが正当なものであるか検証できない脆弱性		○
		・その MFP 用に拡張アプリケーションとしてソフトウェアを配布することが認められていないサードパーティの開発者が、MFP の内部にインストールできる拡張アプリケーションを作成し、特定の MFP にインストールする			
5. 責任追跡性	・MFP 内ソフトウェアが改ざんをされていたとしても、その原因を特定できない	・保守員が間違って古いバージョンのソフトウェアを導入して、一部の機能が使えなくなってしまったが、どの保守員がどのインタフェースを経由して行ったのか特定できない	・保守員権限を複数の人が共有しているため実行者を特定できない脆弱性 ・保守操作で利用者の認証が行われていない脆弱性 ・保守操作の履歴が記録されていない脆弱性 ・保守操作の履歴に時刻、ユーザ ID、操作名の必須情報がない脆弱性		○ ○ ○ ○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
6. 否認防止	・MFP 内ソフトウェアの一部または全部の入替えが、保守員によって行われたことがあるのに、特定の保守員が行ったということを立証できない	・特定の保守員が間違って古いバージョンのソフトウェアを導入したという記録があったが、その保守員は否認しており立証する証拠がない	・他の利用者の名前、ID・パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性) ・履歴、監査情報の記録を行うとき、任意の時刻や、任意のユーザ ID を記録できてしまう脆弱性		○ ○
7. 信頼性	・MFP 内部に追加または更新するソフトウェアが正しい場所に配置されなかったり、間違ったコードや不正なコードを混入させられたり、ソフトウェアの一部が欠落することで MFP を正しく動作させられない ・MFP 内部のソフトウェアの脆弱性が発見されて、実際に悪用される	・保守員が実施する、遠隔からのソフトウェアの更新手順の途中で、通信終了を示すパケットを注入するか、手順を飛び越えてソフトウェア更新完了メッセージを注入することでソフトウェアを不完全な形で書き込みさせる	・追加、更新対象のソフトウェアが正しく書き込まれたか検証できない脆弱性 ・ソフトウェアが正しく書き込まれたことを検証する処理をバイパスまたは中断できる脆弱性		○ ○
		・攻撃者が、特定の MFP に対して侵入試験、ファジング試験を行い、脆弱性を発見し、MFP 上の脆弱性を攻撃し、MFP 上で任意のコードが実行される	・MFP 内部のソフトウェア試験の計画、実施が充分に行われていない脆弱性(自社開発または外部から導入した OS やライブラリ、ミドルウェアを含む)		○
		・SDK を利用した複数の拡張アプリケーションを導入した MFP で、複数の長大なジョブデータが投入されると、メモリの取得で競合が発生し、ジョブデータが失われる	・SDK を利用した複数の拡張アプリケーションの競合による脆弱性		○
		・善意の第三者が脆弱性を発見して MFP ベンダに通報してきたが、回答をせず脆弱性への対応もしなかったため、通報者が脆弱性を公開し、悪意の攻撃者が攻撃用ソフトウェアを開発販売し、大規模に被害が発生し、損害賠償を請求される	・MFP の脆弱性が発見されたあとの体制と対応方法の計画がない人為的脆弱性		○
		・攻撃者は、MD5 ハッシュ関数がコリジョンを起こしやすい脆弱性を利用して、ファクスメールの S/MIME 署名されたメッセージを改ざんし、正しく電子署名したかのように見せて着信させる	・暗号とハッシュ関数が必要な暗号強度に満たない脆弱性		○
		・MFP が SSL/TLS 接続をしようとすると、RSA 暗号の 512bit 長の鍵処理にした対応していなかったため、SSL サーバ証明書の 1024bit RSA 鍵を持つサーバに SSL/TLS で保護された接続ができない			
		・MFP が SSL 3.0 と TLS 1.0 の両方に対応していない			

6.5 使用ライセンス、保守ライセンス

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・利用者環境でのMFPの使用ライセンス許可情報が漏洩、暴露し、第三者が利用した使用ライセンス費用、保守ライセンス費用を負担させられる	・MFPのコンソール上で、そのMFPに登録されているライセンス情報を表示させ、ライセンスコード文字列などのメモをとり、別のMFPにライセンス情報として入力して利用する	・管理者がMFPのライセンス情報を攻撃者に閲覧される脆弱性	○	
		・MFP上の公開フォルダに、ネットワークかUSB経由でアクセスし、ライセンスとなる電子ファイルを取り出し、別のMFPに入力、登録して利用する	・MFPのライセンスとなる電子ファイルがMFP上で誤って公開されている脆弱性		○
		・MFP内のハードディスクに登録されているライセンス情報を、直接HDDをスキャンして取り出す。暗号化されている場合は暗号鍵をスキャンして取り出す	・MFPのストレージ上のライセンス情報が暗号化やハッシュ化などで保護されていない脆弱性		○
			・ライセンス情報を暗号化するときの暗号鍵が充分に保護されていない脆弱性		○
2. 完全性	・使用ライセンスの一部または全部が入れ替えられ、契約利用者のMFP内のソフトウェアが動作しないか、未契約利用者のMFPが動作してしまう	・中古などのMFPに、別の利用者のライセンスが投入されて販売され、未契約の利用者がMFPを利用する	・利用者が廃棄時にライセンス情報を削除しなかった脆弱性	○	
			・ライセンス情報に有効期間がない脆弱性		○
			・ライセンス情報内の機種名やシリアル番号、ソフトウェア名など、特定の固有情報が検証されていない脆弱性		○
3. 可用性	・時刻を変えるなどして使用ライセンスを無効な状態にされ、MFPを利用できなくなる	・すでに正しいライセンス情報を入力した稼動中のMFPで、不適切なライセンス情報を入力しなおしたためMFPが動作しなくなる（操作間違いまたは攻撃）	・MFPに無効なライセンスデータを投入され、MFPが利用できなくなる脆弱性	○	
		・すでに正しいライセンス情報を入手した稼動中のMFPで、MFPの時刻を1年早く入力してしまったため、契約期間の1年前にMFPが動作しなくなる（操作間違いまたは攻撃）	・MFPに誤った時刻を設定され、MFPが利用できなくなる脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	・使用ライセンスが正しいライセンスかどうかわからないため、偽造された使用ライセンスにより、未契約利用者が MFP を利用できる	・他の MFP で利用されていたライセンス情報や、それに似せたライセンス情報を、再販売業者や中古業者などの攻撃者が MFP に投入して、MFP を利用する	・発行されたライセンス情報が、特定機種だけではなくほかの機種でも利用できてしまう脆弱性 ・発行されたライセンス情報が、MFP 内部で充分に検証されておらず、第三者が作成したライセンス情報でも MFP が動作してしまう脆弱性		○ ○
		・ライセンス情報が数桁の数字であるため、順番に加算して試すことで登録可能なライセンス情報を特定し、悪用される	・MFP のライセンスとして MFP に入力すべき文字列が、容易に予想できる数字や、順序のある文字である脆弱性		○
5. 責任追跡性	・使用ライセンスが無効にされるか偽造されていたとしても、その原因を特定できない	・ライセンス情報を入れ替えても記録が残らないため、他社のライセンス情報を投入した MFP を中古として販売される	・ライセンス入れ替え操作の履歴が記録されていない脆弱性 ・ライセンス入れ替え操作の履歴ログが充分な情報を含んでいない脆弱性［日付、ユーザ ID、アクセス経路、操作内容、結果］		○ ○
6. 否認防止	・使用ライセンス/保守ライセンスの削除または入替えが保守員によって行われたのに、特定の保守員が行ったということを立証できない	・組織内部の攻撃者は、ライセンス情報を入れ替えると記録が残るので、記録上のユーザ ID を書き換えるか、任意の別の利用者が操作したような記録を追加して、MFP が動作しなくなるライセンスを投入し、サービス停止攻撃を行う	・ライセンス入れ替え操作の記録にユーザ ID が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］		○
7. 信頼性	・特定のライセンスデータや特定の環境条件により、無効なライセンスデータが有効と判定されるか、有効なライセンスデータを有効と判定できない	・ライセンス情報の検証機能に不具合を起こさせるようなライセンス情報を作成して MFP に投入し、契約がない利用者が MFP を利用するか、攻撃者が任意のコードが実行する	・ライセンス情報に予想外の値が含まれていると、ライセンス検証機能が中断し、ライセンス検証機能がバイパスされてしまう脆弱性 ・ライセンスのパラメータがバッファオーバーフローを起こす脆弱性		○ ○

6.6 着脱式メディア(利用者用、管理者用)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・着脱式メディア上に保護されずに記録された情報が、着脱式メディアの盗難により漏洩する ・着脱式メディアのスロット内で、スロットとメディアの間の接点で転送される情報が盗聴される	・着脱式メディアのスロットに挿入されたままのメディアを、攻撃者が抜き出して入手する。または異なる利用者が間違って回収して、機密の文書が漏洩する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・MFP 内の、パスワードを含む管理構成情報をバックアップした SD カードが、抜き忘れのため管理者以外の者に抜き取られ、コピーされて機密の文書が漏洩する	・着脱式メディアの抜き忘れが、視覚的聴覚的にわかりにくい脆弱性 ・着脱式メディアに記録された機密の文書または管理構成情報などの二次資産が暗号化などで保護されてない脆弱性		○ ○
		・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵がそのメディアに共通の文字列だったため攻撃者に機密の文書が漏洩してしまう	・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵が予想しやすい、またはそのメディアに共通の文字列である脆弱性	○	
		・攻撃者は MFP に挿入したまま抜き忘れられた着脱式メディアを入手し、着脱式メディアの暗号化機能で使われているデフォルトの共通パスワードを使って、着脱式メディア内に残っていた機密の文書を入手する			
		・スロットとメディアの間の接点またはスロット側の装置内にプローブが装着され、付属の盗聴装置から送信され、攻撃者に機密の文書か、パスワードを含む管理構成情報が漏洩する	・MFP が攻撃者から物理的に操作可能な脆弱性 ・着脱式メディアと、メディアスロットの間の転送データが暗号化されていないか、保護が不完全である脆弱性	○	 ○
2. 完全性	・着脱式メディア内の保護されていない情報が改ざんされる	・着脱式メディアのスロットにメディアが挿入されたあと、抜き忘れられたメディアを抜き取って、メディア内にあった、ほかにコピーがないオリジナルの機密の文書を書き換えられる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性 ・着脱式メディア上で文書データを保護する機能がない脆弱性	○	 ○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・着脱式メディア内の保護されていない情報が改ざんされる	・着脱式メディアのスロットにメディアを挿入されたあと、抜き忘れられたメディアを抜き取って、メディア内にあった、他の MFP に投入するための構成情報を書き換えられ、他の MFP 20 台に投入してしまう	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性 ・構成情報の読み込みが権限無く行える脆弱性 ・着脱式メディア上で文書データを保護する機能がない脆弱性	○	○ ○
		・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵がそのメディアに共通の文字列だったため攻撃者に構成情報を書き換えられてしまった	・着脱式メディア上の電子ファイルは暗号化されていたが、暗号鍵が予想しやすい、またはそのメディアに共通の文字列である脆弱性	○	
		・スロットとメディアの間の接点またはスロット側の装置内に介入装置が挿入され、機密の文書または管理構成情報が書き換えられる	・MFP が攻撃者から物理的に操作可能な脆弱性 ・着脱式メディアと、メディアスロットの間の転送データが暗号化されていないか、保護が不完全である脆弱性	○	○
3. 可用性	・着脱式メディアが盗まれるか破壊されるか、読み書きの利用を遮断され、その着脱式メディアを利用できなくなる	・オリジナルのデータが保存してあった着脱式メディアを抜き忘れたあと、攻撃者か異なる人に回収されたため、オリジナルのデータを利用できなくなる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性 ・着脱式メディアの抜き忘れが、視覚的聴覚的にわかりにくい脆弱性	○	○
		・着脱式メディアのスロットを破壊して着脱式メディアを利用できなくする	・MFP が攻撃者から物理的に操作可能な脆弱性	○	
4. 真正性	・ある特定の着脱式メディアが、その組織の管理者によって承認されたメディアかどうか、確認できない	・攻撃者は MFP の不具合を発生させるために作成した SD カードを用意して、MFP 内部に侵入し、機密の文書が漏洩する	・着脱式メディアに識別機能、認証機能がない脆弱性		○
5. 責任追跡性	・ある特定の着脱式メディアへの読み書きの履歴をさかのぼって利用者を特定できない	・MFP 内部から着脱式メディアに機密の文書が大量に転送され、攻撃者に漏洩したと考えられるが、どの利用者が実行したのか特定できない	・着脱式メディアの操作について利用履歴が記録されない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
6. 否認防止	・ある特定の着脱式メディアに関する読み書きの履歴に残された利用者のユーザ ID および時刻の記録について、立証できる根拠がない	・SD カードから大量の写真の印刷処理が実行されていたが、記録にあるユーザ ID では、誰が実行したのか確認できなかった	・操作の記録にユーザ ID が記録されていたが、そのユーザ ID は利用者から任意の文字列を投入できる脆弱性［ログが任意のユーザ ID を受け付ける脆弱性］		○
		・ある SD カードから不正な構成情報が投入されたが、どのカードから投入されたのか特定できなかった	・操作の記録にユーザ ID が記録されていたが、その記録は第三者が改ざん可能な脆弱性［ログが改ざんされることがある脆弱性］		○
7. 信頼性	・MFP に装着した着脱式メディアについて、メディア内のディレクトリや電子ファイルの内容が一部読み込めないか、ファイル名をジョブの名前として表示できなくなる	・SD カードに巨大なファイルを保存し、MFP で読み込もうとしたところ、それ以外のファイルが読み込めない	・着脱式メディアで特定の大きさ以上のファイルがあると、処理が途中で異常終了する脆弱性		○
		・SD カードのファイル名に特定の言語の Unicode 文字を使うと、ファイル名として表示されず、操作メニューが初期状態に戻る	・着脱式メディア上のファイル名に予想外の文字を書き込んでおくと、任意のコードが実行される脆弱性		○

6.7 ジョブデータ(イメージ,宛先,制御)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体内、MFP と他システム間で交換されるジョブデータが漏洩し、文書とアドレスが漏洩する	・攻撃者が一般利用者用の USB メモリポートに、別の USB ハブを介入させ、MFP に入力するジョブデータを盗聴する	・MFP 内部のユニット間のインタフェース上で送受信されるジョブデータか通信路が保護されていないか、保護が不完全である脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体内、MFP と他システム間で交換されるジョブデータが漏洩し、文書とアドレスが漏洩する	・以下の経路のいずれかで MFP が交換するジョブデータを盗聴する: MFP 内部のバスや端子、MFP と外部 USB 機器の間、MFP と外部の Bluetooth または赤外線通信機器の間、MFP と IP/AppleTalk/IPX で通信する機器の間 または以下のジョブ伝送手順の経路: IP, TCP,raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース	・MFP と利用者端末、他システム、遠隔管理システムとの間で送受信されるジョブデータか通信路が保護されていないか、保護が不完全である脆弱性		○
		・メールファクスのメールヘッダは S/MIME で暗号化されないため、攻撃者は SMTP、POP3、IMAP4 の保護されていない通信路で盗聴して宛先と発信者アドレスを収集する			
		・以下の機器内のいずれかで、ジョブデータが権限のない者に入手される: MFP 内部の HDD、利用者端末内、ジョブデータをスプールする蓄積・外部処理サーバ、proxy サーバ、着脱式メディア	・他システム上で扱われるジョブデータが保護されていないか、保護が不完全である脆弱性 ・MFP 内部 HDD に記録された機密の文書または管理構成情報などの二次資産が暗号化などで保護されてない脆弱性	○	○
		・攻撃者は一般利用者端末内に侵入し、残存していた保護されていないジョブデータを入手し、機密の文書が漏洩する			
		・攻撃者は保守交換されて一部が故障した MFP 用に利用されていたハードディスクを盗み、ハードディスク上に残っている保護されていないジョブデータから、機密の文書を入手する	・MFP 上で扱われるジョブデータが保護されていないか、保護が不完全である脆弱性		○
		・攻撃者は MFP に多数のリクエストを送信して、MFP を過負荷にし、MFP がジョブデータの削除または上書き消去できないようにする。その後攻撃者は別の脆弱性を利用して MFP 内部のスプールファイルをとりだし、機密の文書が漏洩する	・ジョブデータの処理終了時にジョブデータが削除または上書き消去されない脆弱性		○
2. 完全性	・MFP 本体内、他システム間で交換されるジョブデータが改ざんされ、文書の内容または排出先、保存先ボックス名、宛先のアドレスなどが改ざんされる	・以下の保護されていない通信経路のいずれかで MFP が交換するジョブデータが改ざんされる: MFP 内部のバスや端子、MFP と外部 USB 機器の間、MFP と外部の Bluetooth または赤外線通信機器の間、MFP と IP/AppleTalk/IPX で通信する機器の間	・MFP 内部のユニット間のインタフェース上で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性 ・MFP と入出力機器との間で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性		○ ○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP 本体内、他システム間で交換されるジョブデータが改ざんされ、文書の内容または排出先、保存先ボックス名、宛先のアドレスなどが改ざんされる	・攻撃者はMFPと他システムの間の通信路に介入し、ジョブデータを改ざんしてボックス名や宛先のアドレスなどを 介入対象は以下のジョブ伝送手順のいずれかの経路上:：IP, TCP, raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース	・MFP と遠隔通信機器との間で送受信されるジョブデータが保護されていないか、保護が不完全である脆弱性 ・MFP を利用するために使われる通信システムが、攻撃者から物理的に操作可能な状態にある脆弱性	○	○
		・以下の機器内のいずれかで、ジョブデータが権限のない者にジョブデータが改ざんされる: MFP 内部の HDD、利用者端末内、ジョブデータをスプールする蓄積・外部処理サーバ、proxy サーバ	・他システム上で扱われるジョブデータが保護されていないか、保護が不完全である脆弱性		○
3. 可用性	・ジョブデータの伝送と処理ができなくなり、MFP のコピー/プリント/ファクス/配信機能が利用できなくなる	・MFP の処理で予想外の値を含むジョブデータを連続的に作成して MFP に与え、停止や誤動作を起こすジョブデータを調べ(ファジング)、繰り返し停止させる 以下のジョブ伝送手順の処理機能を誤動作させるか過負荷を与えて動作を停止させる: IP, TCP, raw9100, LPR, HTTP, FTP, SMB, IPP, SOAP, WebDAV, SMTP, POP3, IMAP4, SSL/TLS, IPsec, Ethernet, 無線 LAN, USB, Bluetooth, 赤外線/IrDA, AppleTalk, IPX, パラレルインタフェース, ITU-T T.30	・予想外のジョブデータを受信するか、処理すると誤動作してしまう脆弱性		○
		・攻撃者は、特定の MFP と他システム(利用者端末、蓄積・外部処理、遠隔管理)との間の特定のセッションに対し、各伝送手順で終了または中断を意味するメッセージ(TCP FIN など)、またはセッションを喪失させる鍵交換不良メッセージなどを注入し、そのセッションを異常終了させる	・MFP を利用するために使われる通信システムが、攻撃者から物理的に操作可能な状態にある脆弱性	○	
		・MFPのジョブ伝送以外の、VLAN認証機能、通信機能、遠隔管理用機能、外部認証機能を誤動作させるか過負荷にし、ジョブ伝送を停止させる: 802.1x, EAP, DHCP, DNS, NTP, SNMP, SSH, TELNET, LDAP, Kerberos, X.509, OCSP	・受付可能な処理要求量を制限できない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・ジョブデータの伝送と処理ができなくなり、MFP のコピー/プリント/ファクス/配信機能が利用できなくなる	・MFP と他システムとの間の通信路を破壊、切断するか、電磁的に干渉してジョブデータの転送を妨害する	・MFP を利用するために使われる通信システムが、攻撃者から物理的に干渉可能な状態にある脆弱性	○	
		・MFP と機体入出力機器の間の通信路で配線を切断するか、電磁的・光的に干渉してジョブデータの転送を妨害する	・MFP を利用するために使われる通信システムが、攻撃者から物理的、電磁的・光的に干渉可能な状態にある脆弱性	○	
		・MFP 内部バスかユニット間の配線を切断するか、電磁的に干渉してジョブデータの転送を妨害する	・MFP が攻撃者から物理的に操作可能、または付近に不正な機器を設置可能な状態にある脆弱性	○	
4. 真正性	・ある処理要求について、ジョブデータを投入しようとする利用者または他システム名が正しいかどうか確認または検証ができない	・認証のないジョブデータ伝送手順(LPR, raw9100 など)を使って MFP にジョブデータを投入し、利用者ではない者が MFP で印刷する	・ジョブデータの伝送手順自体に認証機能そのものがない脆弱性		○
		・MFP 上で動作する LPR,raw9100 サーバでは、ジョブデータを受け入れる接続を確立するときに認証手順がないため、攻撃者は何度でも認証なしで攻撃し、脆弱性を発見することができ、次の攻撃を成功させることができる			
		・他の MFP の IP アドレスを発アドレスに持つ偽装マシンを使って、他の MFP になりすました攻撃者が、特定の MFP にジョブデータを投入し、印刷を行わせる	・ジョブデータ伝送時に接続認証が行われていない脆弱性		○
		・MFP がジョブデータを受け入れる接続を確立するときに、他システムとの間で交わされる認証手順の通信内容が保護されていないため、攻撃者にユーザ ID とパスワードが漏洩し、なりすましをされる	・ジョブデータ伝送時の接続認証の通信が保護されていない脆弱性		○
		・ジョブデータに利用者を識別する情報が含まれている場合、ジョブデータ内の利用者識別情報を改ざんして別の利用者が出力したかのように見せかける	・ジョブデータ伝送時の接続認証の通信が保護されていない脆弱性		○
		・攻撃者は MFP に送信するジョブデータに任意のジョブ制御命令を入力しておくことで、特定の MFP に対して任意のメールアドレスに電子メールを配信させ、攻撃者が特定 MFP を迷惑メール送信サーバとして悪用する	・MFP が受信したジョブデータ内のそれぞれのジョブ制御命令について実行許可が検査されていない脆弱性(対向の MFP やホスト、システムごとなど)		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
5. 責任追跡性	・ジョブデータを伝送または転送、廃棄した処理の過程で、それぞれの処理がどのモジュールや他システム、どの利用者の指示によって発生したものか確認できず、特定処理の発生原因を確認できない	・メール転送型のファクス伝送処理で、伝送途中にある任意のSMTP サーバで、攻撃者がジョブデータの転送をすりかえて別のファクスイメージを注入しても、どのサーバで書き換えられたのかわからない	・ジョブデータ伝送の経路上で、異なる運用方針を持つ他組織が運用するサーバが介入している脆弱性	○	
		・複数の配信先を指定したジョブデータを MFP に投入したところ、一部の処理が中断して失敗していたが、どの処理が失敗、廃棄されているのかわからない	・ジョブデータに対する複数の処理の処理結果か、失敗や廃棄などの例外的な処理結果が記録されていない脆弱性 ・例外的処理結果の記録がされていても、時刻、利用者、処理内容など十分な内容が記録されていない脆弱性		○ ○
6. 否認防止	・ジョブデータの処理過程での特定処理がどのモジュールや他システム、どの利用者によって行われたか記録があっても立証できない	・LPR では誰でもジョブデータを投入できるので、攻撃者がジョブデータ内に任意の利用者の識別情報を書き込んだ大量のジョブデータを特定の MFP に投入して MFP のサービスを停止させても、ジョブデータ内に攻撃者を特定できるような情報がない	・他の利用者のユーザ ID、パスワード、セッション情報を再利用して、なりすましができる脆弱性(検証できない脆弱性) ・履歴、監査情報の記録を行うとき、攻撃者を特定できる情報が無いか改ざんできてしまう脆弱性		○ ○
7. 信頼性	・ジョブデータが、別のジョブと混同され、イメージデータと宛先が入れ替わってしまう ・イメージデータが破壊され、適当なイメージデータが出力されない ・ジョブの転送処理が悪用され、他システムへの攻撃に利用される	・MFP 内部へのジョブデータの受信、または MFP 外部へのジョブデータの転送中または前後で、攻撃者が並行して特定アドレスへのジョブを MFP に送信し続けると、別のジョブデータの宛先が入れ替り、攻撃者にジョブデータのコピーが送られ、機密の文書が漏洩する	・ジョブの多重制御やジョブデータの宛先の排他制御が不十分な実装上の脆弱性		○
		・ある利用者ジョブデータの受付処理を行っている MFP に対して、攻撃者または他システムが受付処理の途中でジョブ制御の範囲外データや、TCP RESET、HTTP の転送データ長を無視したデータなど、例外的なジョブデータや制御を行って、誤ったジョブデータを保存させる、または任意のコードを実行させる	・ジョブデータのパラメータチェックが不十分な実装上の脆弱性		○
		・MFP が他システムへの問い合わせを行いながら進められる処理で、大量の不正なジョブデータを与えて、特定の MFP から他システムへ大量の負荷を与えたり、特定の MFP から他システムに不正な問い合わせを行わせて他システムを停止させたり、誤動作させたりする	・ジョブデータのパラメータチェックが不十分な実装上の脆弱性 ・処理要求量を制限する機能がない脆弱性		○ ○

6.8 管理構成情報

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体の構成情報、他システムと通信するための構成情報が漏洩し、資産情報が集中するホストなどの重要な攻撃対象が特定される	・保守員が、権限を悪用して MFP 内部の管理構成情報をコピーして持ち出す	・保守員の契約や教育の不十分さに関する脆弱性		○
		・管理者が構成情報を SD メモリにコピーしたが、紛失し、第三者に管理構成情報が漏洩する	・MFP の構成情報が保護されないまま MFP の外部に保存される脆弱性 ・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	○
		・管理者が MFP に管理者モードで認証後、ログアウトされずそのままになっている MFP コンソールまたは管理者の端末を悪用し、攻撃者が管理者になりすまして管理構成情報を取り出し、漏洩する	・MFP コンソールまたは MFP 上の管理用ウェブページは、管理者の操作が数分以上なくても自動終了しない脆弱性 ・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	○
		・コンソールキーボードと実行基板の間の USB ケーブルに攻撃者がキーロガーをしかけ、管理構成情報を盗聴する	・MFP 内部のユニット間インタフェース上で通信するデータが保護されていないか、保護が不完全である脆弱性 ・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	○
		・攻撃者が MFP 上で稼動するサービスの脆弱性を攻撃し、MFP 内部で任意のコードを実行し、特権的操作を実行して管理構成情報をコピーし、管理構成情報が漏洩する	・外部インタフェースから MFP 内部に侵入され特権的操作が実行される脆弱性		○
2. 完全性	・管理構成情報のうち、セキュリティ機能の使用を無効にさせられ、所定のセキュリティポリシを実現するための構成にできない ・表示される項目が多く、間違いやすい。個々の管理構成情報の項目の間で、設定値の矛盾があっても判定されないため、目標とするサービス条件を達成できない	・管理者が MFP に管理者モードで認証後、ログアウトされずそのままになっている MFP コンソールまたは管理者の端末を悪用し、攻撃者が管理者になりすまして構成情報を変更する	・MFP コンソールまたは MFP 上の管理用ウェブページは、管理者の操作が数分以上なくても自動終了しない脆弱性 ・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・管理構成情報のうち、セキュリティ機能の使用を無効にさせられ、所定のセキュリティポリシを実現するための構成にできない ・表示される項目が多く、間違いやすい。個々の管理構成情報の項目の間で、設定値の矛盾があっても判定されないため、目標とするサービス条件を達成できない	・管理者が所定のセキュリティポリシを実現する設定を MFP に投入したが、数百項目のうち数項目が間違っていたため通信時データが保護されていなかった。警告メッセージはなかったため継続使用した。	・MFP の構成が所定のセキュリティポリシに適合しているか、違反しているかどうか判断しにくい脆弱性		○
		・管理者は取扱説明書のとおりに MFP の不要サービスを停止させ、利用するサービスだけを動作させた。しかし、攻撃者は MFP のサービスポートを調査して取扱説明書に記載がないサービスポートを発見し、そのサービスポートに対して脆弱性調査を行って攻撃し、MFP 内に侵入する	・MFP 内部に侵入され特権的操作が実行されるサービスの脆弱性 ・MFP 内部で動作させていないはずのサービス、または待ち受けていないはずのポートが開いている脆弱性		○ ○
3. 可用性	・MFP 本体の構成情報、他システムと通信するための構成情報が破壊または削除され、事前に登録しておいた設定構成情報が利用できなくなる ・構成情報を投入できない、更新できなくなる	・MFP の管理コンソールに対して、攻撃者が管理者になりすましてログインし、構成情報を削除する	・認証強度が十分ではない脆弱性（管理者パスワードが単純、または長期間同一である等） ・認証強度を十分な強度に保つ実装になっていない脆弱性	○	 ○
		・攻撃者からの大量リクエストによる過負荷で、管理コンソールを開けなくなり、数十台ある MFP が連続印刷しているのに、すべて遠隔から制御できなくなってしまった	・通信制御機能が適切に実装されていない脆弱性		○
4. 真正性	・MFP 本体の構成情報、他システムと通信するための構成情報が正しい値であるかどうかが確認できない	・ほかの MFP と同じ設定だから設定しておいて、と渡された MFP の設定が、会社のセキュリティポリシに反していた（例: HDD 暗号化機能が on になっていなかった、S/MIME 利用がオフだった）	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・MFP に設定して接続させていた他システムのアドレスかポート番号が間違っており、サービスが提供されていなかったか、間違った情報が配布される	・MFP が通信する他システムについて、MFP 内に設定されているアドレスやポート番号などの構成情報が正しいかどうか検証する方法がない脆弱性	○	
5. 責任追跡性	・MFP 本体の構成情報、他システムと通信するための構成情報がどの利用者によって変更・削除されたか、履歴を確認することができない	・運用後数ヶ月で、数十台ある MFP のそれぞれが、少しずつ違う設定になっていたが、複数存在する管理者のうち誰がいつ設定したのかわからず、構成管理の安全対策がとれない	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性（管理構成情報の操作の記録）	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
6. 否認防止	・MFP 本体の構成情報、他システムと通信するための構成情報を変更・削除した利用者が記録されているが、明確な根拠とともに立証できない	・攻撃者が管理者になりしまして管理構成情報を変更するとき、操作記録に自分以外のユーザ ID が残るよう、別の管理者の名前を追加して、記録内容をかく乱する	・管理者などによるログの書き換えを受け付ける脆弱性		○
		・複数の利用者で同じユーザ ID でログインできるため、どの利用者が実行したかわからない	・同一のユーザ ID が複数設定できる脆弱性		○
7. 信頼性	・管理構成情報として入力した情報が適切に表示、保存されない ・入力した管理構成情報のうち一部が保存されなかったり、表示されなかったりする	・管理者パスワードが空欄のまま設定されたが、何も警告表示がなかったためそのままにされ、複数の権限がない利用者が管理者になりすまして MFP の構成情報を勝手に変更し、機密の文書が漏洩する	・受け付けた管理構成情報に、矛盾した設定や範囲外などの間違いがないことを確認する方法がないか、確認していない脆弱性		○
		・MFP の複数の処理が集中していたときに構成情報を変更しようとしたら、MFP が停止した。起動しなくなるか、起動後も一部機能の動作がおかしい	・ソフトウェアの更新を含む管理構成情報の更新処理を受け付けたときに、処理用のリソースが不足していても処理を実行し、処理の中断または処理後の MFP 内構成情報が予期せぬデータで置き換えられてしまう脆弱性		○
		・MFP の複数の処理が集中していたときに MFP 内のソフトウェアの追加または更新をしようとしたら、MFP が再起動しようとしたあと、まったく起動しなくなる	・受け付けた管理構成情報を処理する際に、MFP 内部で実行されている処理への負荷を考慮せず、実行中の処理を中断または異常な状態に遷移させる脆弱性		○
		・管理者が MFP のウェブサーバ上にある管理ページを利用して設定変更しようとしたが、利用したウェブブラウザで一部の設定項目の値が一部隠れていたため、セキュリティ機能の一部を有効にできず、攻撃者に機密の文書を盗聴された	・ウェブブラウザの違いやバージョンの違いによって、MFP の管理ページの設定項目や説明表示、メニューや入力値のうち一部が表示されないか、間違って表示されるか、わかりにくい脆弱性		○

6.9 電子証明書、ID、パスワード、セッション情報(本体内、他システム内)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体の電子証明書用の秘密鍵や、利用者または他システムの ID とパスワードが漏洩し、文書やサーバのなりすましに悪用される	・管理者の ID、パスワードが以下の経路のいずれかで盗聴されて漏洩する: ユニット間のバス上、ネットワーク/遠隔通信、USB・SD メモリ・Bluetooth など機体入出力	・MFP 本体のユニット間インタフェース上の通信データが保護されていない脆弱性		○
		・攻撃者が管理者になりすまして MFP の管理者モードを利用し、MFP 内の共有文書が攻撃者に漏洩する	・MFP 設置時の設定を的確に行っていないため、デフォルトの管理者パスワードを利用される脆弱性 ・管理者パスワードがつけられていない脆弱性	○ ○	
		・攻撃者が MFP 内に管理者になりすましてログインし、文書の配信経路に攻撃者の宛先を加えられ、継続的に機密の文書が攻撃者に漏洩する	・ID、パスワード、セッション情報を容易に予測できる脆弱性(辞書にある文字列、同じ文字の羅列、IP アドレス、時刻などを使うか、生成された乱数値に偏りがあるなど)	○	
		・攻撃者は MFP と業務システムの間で保護されていない通信を盗聴し、攻撃者は盗聴して得た ID またはパスワード、セッション情報を悪用して、MFP が接続する業務システムに対して、攻撃者が MFP になりすまして接続し、業務システムで扱う情報が攻撃者によって取り出されるか、書き換えられる	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の外部に転送、保存できる脆弱性(他システムとの通信路での漏洩、パスか URL の履歴が渡される、パスワードを保護する認証手順がないか選択されない)		○
		・MFP 廃棄後に、MFP 内部に残っていた電子証明書、ID、パスワードが第三者に漏洩する	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の内部に保存される脆弱性(ストレージからの漏洩、不揮発メモリからの漏洩、履歴・記録からの漏洩) ・電子証明書、ID、パスワードを MFP 内部から完全に消去できない脆弱性		○ ○
		・管理者端末が、攻撃者が注入したマルウェアに乗っ取られ、MFP 内部の証明書、ID、パスワード、セッション情報すべてが攻撃者に漏洩する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP 本体の電子証明書用の秘密鍵や、利用者または他システムの ID とパスワードが漏洩し、文書やサーバのなりすましに悪用される	・MFP 内部から MFP の電子証明書の秘密鍵を取り出し、その MFP になりすまして他社にファクスを送信し、あたかもその組織が発注したかのような発注書を送付する	・電子証明書の秘密鍵を MFP 内部から許可無く取り出せる脆弱性 ・電子証明書の秘密鍵をセキュアに保存していない脆弱性		○ ○
2. 完全性	・利用者の ID・パスワードが改ざんされ、MFP が提供するサービスを利用者が利用できなくなる ・MFP 本体の電子証明書用の秘密鍵が入替え、改ざんされ、電子証明書を利用するセキュリティ機能が停止または無効にさせられる ・自社または他社の電子証明書が改ざんされ、成りすまされた発信者による文書を信用してしまう	[電子証明書] ・攻撃者が管理者になりすましてログインし、MFP 本体の電子証明書用の秘密鍵を、攻撃者が作った秘密鍵に入れ替え、MFP 上のサーバの SSL/TLS 通信を継続的に盗聴する	・電子証明書の秘密鍵をセキュアに保存していない脆弱性		○
		・攻撃者は SQL インジェクションを悪用して MFP 内部の管理構成情報を改ざんし、他社宛のメールファクスが、先方で解読できなくなるか、他社から届いたメールファクスの内容を検証できなくなる。場合によって攻撃者からのメールファクスを、特定他社からの文書であると誤認識してしまう	・管理構成情報へのアクセス時の認証がバイパスされる脆弱性 ・証明書の信頼性を検証する機能が無い脆弱性		○ ○
		[ID、パスワード] ・攻撃者は、よくある管理者の ID とパスワードを使って管理者になりすまして MFP にログインし、利用者の ID、パスワードを変更または削除して MFP を利用できなくする	・ID、パスワード、セッション情報を容易に予測できる脆弱性(辞書にある文字列、同じ文字の羅列、IP アドレス、時刻などを使うか、生成された乱数値に偏りがあるなど)	○	
		・攻撃者は MFP と管理者端末の間の保護されていない通信を盗聴して管理者の ID とパスワードを取り出し、管理者になりすまして別の管理者 ID を作成し、以後も継続的に MFP で交換される文書とアドレスが攻撃者に収集される	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の外部に転送、保存できる脆弱性(他システムとの通信路での改ざん、パスワードを保護する認証手順がないか選択されない) ・管理者の ID とパスワードがあれば、MFP 内部のすべての電子証明書、ID とパスワードを追加、変更でき、権限が集中している脆弱性		○ ○
		・攻撃者は MFP 内部から HDD を取り出して、HDD のコピーを作成し、管理者の ID とパスワードを抽出して取り出す	・ID、パスワード、セッション情報と、パスワードを含む構成情報が保護されないまま MFP の内部に保存される脆弱性(ストレージ上での改ざん、不揮発メモリ上での改ざん)		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・利用者の ID・パスワードが改ざんされ、MFP が提供するサービスを利用者が利用できなくなる ・MFP 本体の電子証明書用の秘密鍵が入替え、改ざんされ、電子証明書を利用するセキュリティ機能が停止または無効にさせられる ・自社または他社の電子証明書が改ざんされ、成りすまされた発信者による文書を信用してしまう	[セッション情報] ・MFP で”POP before SMTP 認証”が設定されていると、POP3 または IMAP4 で認証後数分以内の MFP の IP アドレスをソース IP アドレスとしてなりすませば認証なしで SMTP メール送信サービスを利用できてしまうため、攻撃者が MFP になりすましてメールファクスや迷惑メールを送信する	・IP アドレスをセッション情報に利用しているため、容易になりすましされる脆弱性		○
		・攻撃者が、他の利用者端末が利用中の親展ボックスへのリクエストになりすまして、セッション情報なしか任意のセッション情報を指定するだけで親展ボックスの内容を取り出す	・あるリクエストに対して、その時点で有効な認証、認可済みのセッション情報が照合されていないか照合が不完全である脆弱性		○
		・攻撃者が、ログアウトした利用者のセッション情報を使って MFP のスキャナボックスへのリクエストを行って、スキャナボックス内の機密の文書が漏洩する	・利用者がログアウトしたあとでもセッション情報が削除されずに利用できる脆弱性		○
3. 可用性	・MFP 内で生成、登録した電子証明書または秘密鍵が削除され、電子署名やファイル暗号化、サーバ証明書の検証が利用できなくなる ・CA 証明書が削除または改ざんされ、サーバ証明書、文書への署名、コード署名を階層的に検証できなくなる ・対応する CA 証明書が MFP 内にないため、利用者が取得した電子証明書を、MFP が検証できない ・利用者、他システムのための ID・パスワードが削除または改ざんされて MFP を利用できなくなる、または MFP から他システムを利用できなくなる	[電子証明書] ・管理者になりすました攻撃者が MFP の時刻設定を 1 年先に変更し、MFP に格納されている MFP 本体と、宛先メールアドレス、他システム用の電子証明書が無効になり使えなくなる。そのまま MFP は通信路とコンテンツを保護しないまま稼動しつづけ、攻撃者はネットワーク上で容易に盗聴し、文書が漏洩する	・MFP 内部の証明書の有効/無効状態がわかりにくい脆弱性		○
		・MFP 本体のホスト名を変更したが、MFP 内部の証明書を入れ替えなかったため MFP 内部のサーバ証明書が機能停止していた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性 ・MFP 内部の証明書の有効/無効状態がわかりにくい脆弱性 ・MFP がサイトのセキュリティポリシに従って動作しているかわかりにくい脆弱性	○	 ○ ○
		・攻撃者が電磁的な攻撃などにより MFP 内部のセキュア IC/TPM 部品か、この部品内のデータだけを破壊し、その MFP のサーバ証明書とクライアント証明書を利用したセキュリティ機能を停止させる	・MFP が攻撃者から物理的に操作可能、または付近に不正な機器を設置可能な状態にある脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・MFP 内で生成、登録した電子証明書または秘密鍵が削除され、電子署名やファイル暗号化、サーバ証明書の検証が利用できなくなる ・CA 証明書が削除または改ざんされ、サーバ証明書、文書への署名、コード署名を階層的に検証できなくなる ・対応するCA証明書がMFP内にないため、利用者が取得した電子証明書を、MFP が検証できない ・利用者、他システムのための ID・パスワードが削除または改ざんされて MFP を利用できなくなる、または MFP から他システムを利用できなくなる	・ある MFP 内部の MFP 本体用の電子証明書が、操作間違いか通信・ネットワークモジュールの脆弱性で侵入され、MFP 本体の電子証明書が作り直されるか改ざんされたため、その MFP 本体の SSL/TLS サーバ機能と S/MIME の保護機能を利用者が利用できなくなる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(操作間違い) ・MFP 内部に侵入され特権的操作が実行されるサービスの脆弱性	○	○
		[ID、パスワード] ・数回以上連続して認証に失敗すると、そのIDかパスワードが数分から数時間以上、使えなくなるため、攻撃者が被害者の ID で継続的に認証失敗を繰り返し、被害者の ID を使えなくさせる	・攻撃者が認証を何度でも試行できるアクセス許可の脆弱性		○
		・攻撃者が MFP の時刻を 1 年早め、MFP 内部の有効期限つきパスワードを無効化させ、自動的にパスワードを更新する機能がない他システムとの通信を停止させる	・パスワードの有効期限切れによりサービスが利用できなくなる脆弱性		○
		[セッション情報] ・攻撃者が、他の認証済みの利用者のログアウトのリクエストを MFP に送り、その利用者の同意なしでログアウトさせる。再度認証手順を行わせ、ID とパスワードを盗聴または介入する攻撃に利用する	・認証済みのセッション情報が、任意の第三者によって消去できる脆弱性		○
		・攻撃者が、他の認証済みの利用者のセッションに対して、直前の操作で MFP から提示された秘密の値を指定せず、利用者のなりすましを行うと、その利用者のセッションが無効化される			

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	・特定の利用者または他システム用の ID・パスワードについて、権限のある管理者から提供されたものかどうか確認できない	・管理者の間違いで、一部の MFP 数台にだけ、利用者とユーザ ID の対応が異なっていたため、ある利用者のプリントが別の利用者のスプールボックスに投入されて、権限のないものに機密の文書が漏洩した	・複数の MFP に ID、パスワード文字列を設定するとき、間違って異なる利用者に割り当てられる可能性がある人為的脆弱性	○	
	・特定の電子証明書が特定の信頼できる証明書発行局から発行された証明書であるか、確認できない	・ある MFP は外部の認証サーバを利用して、MFP 利用者から ID、パスワード文字列を受け付けて、認証サーバに問い合わせるようになっていた。攻撃者はこれを悪用して、その MFP に特定の ID についてのパスワードを総当りで問い合わせ、MFP に認証サーバに問い合わせて確認させることで、MFP をパスワード解析に悪用した	・MFP が認証応答をする必要がない利用者端末に応答してしまう脆弱性(MFP への接続許可範囲の設定不良、不要なサービスポートの開放) ・MFP 自体または認証サーバが、特定 ID の認証失敗が連続しても、ロックや知恵円をせずに認証要求に応答してしまう脆弱性		○ ○
		・攻撃者は A 社の名前をかたる偽の証明書を B 社に渡し、B 社は A 社宛のファクスを攻撃者に送ってしまう	・MFP 内部で電子証明書が正しく実装されていない脆弱性(証明書発行手順の間違い、有効期限切れ、所有者識別子[DN]文字列の相違、不適切な CA、秘密鍵の保護が不十分、名前[CN]の存在確認がない、脆弱な暗号方式または暗号鍵の使用) ・MFP 内部の証明書発行局(CA)証明書(ルート CA 証明書と中間 CA 証明書)に不適切な CA 証明書が混在する脆弱性	 ○	○
5. 責任追跡性	・MFP 内電子証明書の生成・登録手順において誰が行ったものか特定できない	・攻撃者は管理者になりすまして MFP にログインし、すでに作成されている MFP 内部の電子証明書を上書きして別の証明書を登録し、MFP 内部で証明書を利用するセキュリティ機能を停止させるが、記録がないためいつ誰が行ったかわからない	・MFP 内部で生成した電子証明書要求に関する記録が残らない脆弱性		○
	・利用者または他システムの ID・パスワードについて、新規で MFP に設定したか、変更した操作の履歴を確認できない	・攻撃者は管理者になりすまして MFP にログインし、攻撃者が利用するための ID を追加したが記録がないためいつ誰が行ったかわからない	・MFP 内部で削除、追加、または変更された ID、パスワードについて操作の履歴が記録されていない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
6. 否認防止	・MFP 内の電子証明書を登録したと記録された、特定の管理者名について、確かにその管理者が実行したものであるということが立証できない ・利用者または他システムの ID・パスワードについて、新規登録・変更・削除を行った利用者を特定する記録があっても、根拠がなく立証できない	・攻撃者が管理者になりすまして MFP の電子証明書を一時的に削除したが、作業記録に偽の情報を追加して別の管理者が操作したように見せかけた、または、操作記録を消去した上で別の管理者が操作したように見せかけた	・管理者などによるログの書き換えを受け付ける脆弱性		○
7. 信頼性	・利用者または他システムの ID・パスワードについて、長さや文字種が適切に入力・表示・保存されない。短くされるか、表示されていない文字列が挿入・追加されている ・ある電子証明書と対応する秘密鍵が正しく対応づけられていないため、電子証明書の検証ができない	・MFP 利用者または他システムから MFP に送られてきた ID、パスワードが予想外の値であったため、MFP 内部で任意のコードが実行されたり、MFP 内部の別のモジュールに命令が注入されたり、MFP 内部の情報を一覧する操作が行われた	・受け付けた電子証明書、ID、パスワード、セッション情報に、矛盾した設定や範囲外などの間違いがないことを確認する方法がないか、確認していない脆弱性 ・メモリ保護機能などが無く、MFP が受信または送信する電子証明書、ID、パスワード、セッション情報のデータが予想外の形式であった場合に MFP 内部のソフトウェアが誤動作を起こす脆弱性		○ ○
		・特定の処理中か、大量の負荷があるときに、受信したサーバ証明書または S/MIME メールに添付されている公開鍵証明書の検証が中断しバイパスされる	・電子証明書、ID、パスワード、セッション情報の更新処理を受け付けたときに、処理用のリソースが不足していても処理を実行し、処理の中断または処理後の MFP 内構成情報が予期せぬデータで置き換えられてしまう脆弱性		○
		・ある特定の処理または大量の処理があると、正しく SSL/TLS 通信ができない、メールファクスで正しい S/MIME 処理ができない	・電子証明書、ID、パスワード、セッション情報を処理する際に、MFP 内部または他システムとの間で実行されている処理への負荷を考慮せず、実行中の処理を中断または異常な状態に遷移させる脆弱性		○
		・偽の CA 証明書(ルート、中間)か、検証局(OCSP など)が登録され、他システムの偽のサーバのサーバ証明書が有効だとして、誤って検証され、偽のサーバで攻撃者に情報資産を漏洩してしまう	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・利用者または他システムのID・パスワードについて、長さや文字種が適切に入力・表示・保存されない。短くされるか、表示されていない文字列が挿入・追加されている ・ある電子証明書と対応する秘密鍵が正しく対応づけられていないため、電子証明書の検証ができない	・以前、別の利用者が使っていた電子証明書か、漏洩があり無効にしなければならないパスワードを更新する機能がないため、古い証明書またはID、パスワードを利用していた以前の利用者またはその情報を入手した攻撃者から、MFP に侵入される	・電子証明書、ID、パスワードを更新する機能がない脆弱性 ・パスワードを定期的に更新する運用が行われていない脆弱性	○	○
		・MFP のコンソールから、外部のファイル共有サーバ上の特権ユーザと同じユーザ ID を空のパスワードで登録すると、MFP のコンソールで空のパスワードでログインするだけで外部のファイル共有サーバに、事前に設定された特権ユーザのパスワードを使わないでアクセスできてしまうため、権限のない第三者や利用者に機密の文書が漏洩する	・異なる認証手順で利用される異なるユーザ名が、サービスの利用者識別や権限認可の際に間違って対応づけられる脆弱性	○	

6.10 正しい時刻

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	(世界標準時は世界同一なため機密性はない) (MFP 本体内の時刻が世界標準時に比べて何秒ずれているかを示すオフセット値は漏洩しても直接的な脅威はなく危険度は低い: タイムゾーン、サマータイム)	・攻撃者は、MFP の内蔵ウェブサーバに問い合わせると、認証なしで MFP 内部の時刻がわかる。MFP 内部の時刻が大幅に狂っていることがわかったときは、時刻に依存したセキュリティ機能が停止してしまっている通信路を特定して盗聴する	・時刻に依存したセキュリティ機能を利用している場合、MFP の内部時刻をメンテナンスしていない脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・履歴データの時刻が大幅にずれてしまい監査・監視がしにくくなる ・時刻を大幅にずらされて、正しい時刻を使えない ・MFP 内部の時刻を大幅にずらされ、MFP 内部の電子証明書のほとんどが利用できず、署名の検証、復号、署名による否認防止ができない	・電子証明書を利用中に、攻撃者が管理者になりすましてMFPの時刻設定を1ヶ月先に変更し、SSL/TLSを利用する通信路保護機能とS/MIME でのメール転送文書のコンテンツ保護機能が停止させられ、通信路上で攻撃者に文書を盗聴、改ざんされる	・認証強度が十分ではない脆弱性(管理者パスワードが単純、または長期間同一である等) ・認証強度を十分な強度に保つ実装になっていない脆弱性	○	○
		・有効期間が定められたライセンス情報を利用中に、攻撃者が NTP 通信に介入して改ざんしたメッセージを MFP に応答し、MFP 内部の時計を同期させないようにした。この結果、MFP のセキュリティ機能を含む、ライセンスが必要な一部または全部の機能が停止させられた	・NTPの通信先を特定していない脆弱性(マルチキャストなど)	○	
		・攻撃者により NTP サーバの ARP が偽装され、MFP は偽の NTP サーバと時刻同期を行い、大幅に遅れた時刻に同期させられた	・NTPの通信先との相互認証を行っていない脆弱性	○	
		・攻撃者は犯行時に、MFPの時刻を大幅に狂わせておいたため、該当時刻の攻撃が記録として残らないようにした。記録されたが、保存期間範囲外として翌日の定期処理で削除され、記録が残らなかった	・NTP の時刻同期が成功しているかどうか確認していないか、時刻同期失敗の警告表示がわかりにくい脆弱性		○
3. 可用性	・正しい時刻を取り出せなくなるか、表示できなくなる	・メールファクスで、不正なタイムゾーン値を受け取るとMFP内部の時刻応答機能が停止し、セキュリティ機能や操作履歴の記録や監査ログの記録機能が停止させられる。またはライセンス期間を検査されたソフトウェアモジュールの機能が停止させられる	・不正なタイムゾーン値を受け取ると、MFP 内部の時刻応答機能が応答しなくなる脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・正しい時刻を取り出せなくなるか、表示できなくなる	・MFP 内部の時刻が正しい時刻ではないため、セッション情報が常に無効と判定され、Cookie を利用する MFP 上のウェブページが動作しなくなっていた	・リアルタイムクロック用ハードウェアの故障または停止を検出できない脆弱性		○
		・MFP 内部の時刻が正しくないため、Kerberos の認証が常に失敗しており、集中化した認証サーバによるシングルサインオン機能が利用されておらず、保護されていない通信路上でパスワード入力による認証が実行されていたため、攻撃者にパスワードが漏洩した			
		・MFP 内部のリアルタイムクロック用の電池が切れた状態で MFP を起動後、MFP 内部の時刻が初期値(1970 年)のままだったためセキュリティ機能が動作しないまま利用しており、通信路で文書とパスワードが盗聴されていた			
4. 真正性	・MFP 内部の時刻が、どこの時刻ソースに同期しているか確認できない ・NTP の時刻ソースは確かに所定のソースかどうか識別できず、偽ソースを参照してしまう	・管理者は MFP に正しい NTP サーバのホスト名を指定したが、攻撃者が MFP に対して DNS 偽装データを応答し、偽の NTP に接続させた。しかし、MFP は接続した NTP サーバホスト名は表示するが、接続中の NTP サーバの IP アドレスがわからないため、設定したとおりに動作しているのかどうかわからず、MFP の時刻は攻撃者によって狂わされたままとなる	・NTP の時刻同期ソースを管理していないか表示できない脆弱性 ・NTP サーバとの間の時刻同期のための通信内容を保護していないか、保護が不完全である脆弱性		○ ○
5. 責任追跡性	・MFP 内部の時刻を同期したときの記録に記載されている時刻ソースのホスト名や時刻機器の名前が確認できない	・特定の MFP から利用中の NTP サーバのうち一部が故障し、異常な時刻と同期するようになったが、履歴がないためどの NTP サーバとの同期を停止すればよいかわからず、対策がとれない	・NTP の時刻同期処理の履歴が記録されていないか、履歴があってもどの同期ソースと同期したか記録されていないなど履歴の内容が不十分な脆弱性		○
6. 否認防止	・MFP 内部の時刻を同期させた他システムが間違った時刻を提供したことが立証できない	・攻撃者が、ある MFP が利用している NTP サーバのうちのひとつになりすまして、時刻同期応答を返すと、MFP が間違った時刻に同期する。この記録が MFP 内に残されたが、この MFP は NTP 通信を保護していなかったため、確かにその NTP サーバが間違った応答をした、ということを立証できない	・NTP サーバとの間の時刻同期のための通信内容を保護していないか、保護が不完全である脆弱性		○
		・時刻同期の履歴が記録されていたが、その記録は改ざんされる可能性があるため立証に使えない	・管理者などによるログの書き換えを受け付ける脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・起動時の時刻が大幅にずれている ・標準時刻に同期し、地域の時刻オフセットに合わせた時刻が出力されない ・時間が経過すると、時刻が標準時刻に同期せずに変動してしまう ・出力された文書を時刻順に並べることができない	・ある中古の MFP でクロック用の電池が切れていたために、他システムに送信されるジョブデータやメール、ファイルの日付が大幅にずれた時刻になってしまう。その結果、日付順の新しい順でジョブ実行記録をソートして表示しているため、攻撃者が不正にコピー転送したジョブ記録が、古いほうに分類されて表示されないため、気がつかない	・リアルタイムクロック用ハードウェアの故障または停止（電池喪失など）を検出できない脆弱性		○
		・ある新古品の MFP で、購入時に時刻合わせをしないまま利用していたところ、管理または監査用の操作履歴やエラーの記録内の時刻情報が大幅にずれることから、他システムの動作記録と参照したときに、履歴の記録として利用できなくなる	・MFP の初期設定時に時刻合わせを行わなくても運用状態に移行できる脆弱性 ・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	 ○	○
		・ある管理者が MFP のコンソールを操作して MFP 内の時刻を設定したが、年の数字の入力をひとつ間違えたため時刻が 1 年ずれたまま運用し、正しい有効期限を持つ電子証明書が期間外と判定され、MFP 内で利用されていなかった	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・指定した NTP サーバと時刻の同期ができず、MFP 内の時刻がずれている	・NTP 手順を適切に処理できない脆弱性		○
		・MFP を常時通電させ一度も電源オフすることなく 1 年ほど経過すると MFP 内部の時刻が異常な値になり、MFP 内部のライセンス期間との比較で、MFP の利用権が無効と判定され、その MFP の一部または全部の機能が利用できなくなる	・MFP 内部のクロックがいくつかの数値オーバフローを発生させる脆弱性（16bit signed/unsigned, 32bit signed/unsigned, 秒/ms/us）		○
		・2010 年の時点で、30 年間有効な電子証明書を作成し、MFP にインストールしたところ、MFP 内部で日時の比較が適切に処理されず、どうしても電子証明書の有効性を検証できない	・MFP 内部の時刻の処理が 2038 年問題を持つ脆弱性（32bit オーバフロー）		○
		・MFP に、世界標準時から 5 時間 30 分進んだタイムゾーンと、1 時間進んだサマータイムを設定しようとしても、ファクス文書の時刻には 5 時間 0 分のオフセットしか反映されない	・タイムゾーンとサマータイムに分単位で対応していない脆弱性 ・MFP 内部に世界標準時(GMT)を保持していない脆弱性 ・タイムゾーンとサマータイムの処理が不完全な脆弱性		○ ○ ○

6.11 原稿、印刷物

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・機密情報を含む原稿または印刷物が、第三者に漏洩する	・原稿台や排出トレイに放置された原稿や印刷物を、第三者が読むか、コピー/スキャンして複製を持ち去る	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
			・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
			・ファクス受信または遠隔からの印刷で無条件に紙出力してしまう脆弱性		○
2. 完全性	・原稿または印刷物が、置き換えられるか、すりかえられてしまう	・原稿台や排出トレイに放置された原稿や印刷物を、第三者が取り替えて、偽の文書を扱わされる	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
			・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
			・ファクス受信または遠隔からの印刷で無条件に紙出力してしまう脆弱性		○
		・大量コピー中の A さんの処理中に割り込みで十枚程度のコピーをさせてもらったが、同時並行で大量の処理をネットワークで受け付けていたため、MFP の処理が誤り、A さんのコピー出力の一部が割り込み処理の印刷物の中に紛れ込んだ	・多段の割り込み処理によるリソース不足、競合により、フィニッシャへの制御が誤って実行される脆弱性		○
3. 可用性	・原稿を自動読み込みできない ・印刷物が適切なトレイに排出できない	・攻撃者によって ADF に異物が挿入され、原稿を自動読み込みできない	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
		・攻撃者が MFP の ADF へのケーブル、フィニッシャへのケーブルを撤去して、ADF とフィニッシャを使用不能にする			
		・MFP 近くの強い電磁波の発生源により ADF とフィニッシャが適切に動作せず、利用できない	・付近に不正な機器を設置可能な状態にある脆弱性	○	
		・MFP 内に装填しておいた用紙とトナーカートリッジが盗難にあい、コピー/印刷/ファクス受信ができない	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・原稿を自動読み込みできない ・印刷物が適切なトレイに排出できない	・MFP に大量のファクス出力が行われ、用紙とトナーがなくなり、コピー/印刷/ファクス受信ができない	・ファクス受信または遠隔からの印刷で無条件に紙出力してしまう脆弱性		○
4. 真正性	・原稿を、許可された利用者が回収しているかどうかわからない	・ADF が排出した原稿を、第三者が回収し、機密の文書が漏洩する	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
	・ある印刷物が、許可された利用者が回収しているかどうかわからない	・コピーの排紙トレイに排出された印刷物を、第三者が回収し、機密の文書が漏洩する	・ファクス受信または遠隔からの印刷で無条件に紙出力してしまう脆弱性		○
5. 責任追跡性	・あるスキャンデータやあるファクスデータについて、その元原稿を投入した利用者を特定できない	・ある他社に自社名で偽の注文指示がファクスで届いたが、誰が送ったか特定できない	・MFP 利用時の利用者認証機能を提供していない。		○
			・MFP 利用者の認証結果を操作履歴とともに記録しない脆弱性		○
	・ある印刷物について、印刷を行った利用者を特定できない	・ある MFP から大量の印刷物が出力されたが、誰が出力したか特定できない	・MFP 利用時の利用者認証機能を提供していない。		○
			・MFP 利用者の認証結果を操作履歴とともに記録しない脆弱性		○
6. 否認防止	・あるスキャンデータやあるファクスデータについて、その元原稿を投入したユーザ ID が記録されていたが、立証する根拠がない	・攻撃者が架空の領収書/請求書をスキャンして保存回覧していたが、監査のあと指摘を受けると、それは別人がスキャンしたデータだと主張され、立証できない	・管理者などによるログの書き換えを受け付ける脆弱性		○
	・ある印刷物について、出力した利用者のユーザ ID が記録されていたが立証する根拠がない	・ある大量のカラー印刷物について、出力記録にユーザ ID がある利用者に確認したが、自分ではないと主張され、立証できない	・管理者などによるログの書き換えを受け付ける脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・大量の原稿や印刷物を正しい順序で出力できない ・割り込み処理を多段で行うと間違った出力や保存が行われる ・印刷物を指定どおりのイメージと仕上げにできない: 出力されたイメージや配置が異なる、適切なトレイに排出できない、印刷物が指定どおりの数で出力されない、部単位のソートができない、ホチキス止めができない、穴あけできない、ホチキス/穴あけの場所が違う、折りができないか間違っている	・数千部の印刷を開始したが、攻撃者からの多数のリクエストを受け付けることで、一部の印刷物のイメージ配置、ページ順、綴じが不良になり、廃棄処分となり、納期も遅れて損害が発生した	・MFP が大量の処理を受けつけると、MFP 内部のリソースが不足するか、一部または全部のジョブデータの一部が破壊、混同され指示どおりの処理ができなくなる脆弱性		○
		・数千部の印刷を開始したが、攻撃者からの電磁波妨害によりすべての印刷物の綴じが不良になり、廃棄処分となった。数十万枚の用紙と大量のトナーが無駄になる	・攻撃者が付近に不正な機器を設置可能な状態にある脆弱性	○	
		・穴あけのゴミの滞留、補充用のホチキスの針の間違いによる大量印刷の失敗	・穴あけのゴミの滞留、補充用のホチキスの針の誤挿入がわかりにくい(セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない)脆弱性	○	
		・用紙トレイの中に厚みが異なる用紙が数枚混入したため、大量印刷の途中で用紙が詰まったり、複数枚吸い込まれたりして印刷不良になった	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	

6.12 MFP 内共有ファイル

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・機密情報を含むファイルが、MFP 本体内の共有フォルダから第三者に漏洩する	・攻撃者がリクエスト引数を変化させ、MFP 内部のパスワードを含む構成管理ファイルのパス名を突き止める	・MFP 内部の共有フォルダへのリクエストの内容の検査が不十分で、非公開のフォルダやファイル名を読み取られる脆弱性		○
		・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、どのような制限にも影響なく、機密のファイルを取り出す			
		・機密のファイルが MFP 内部の共有フォルダの公開フォルダにあったため、第三者に機密のファイルが漏洩した	・機密の文書が、間違って公開されたフォルダに配置されてしまう(セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない)脆弱性	○	
		・機密のファイルが機密のフォルダにあったが、攻撃者がゲストの権限または一般利用者の権限でファイルを入手できる状態だったため機密の情報が不適切な権限者に漏洩した	・適切な利用権限が設定されていない脆弱性 ・適切な利用者を認証し、適切な利用権限を割当処理できない脆弱性	○	○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・機密情報を含むファイルが、MFP 本体内の共有フォルダから第三者に漏洩する	・MFP 内部の共有フォルダを検索する機能を使うと機密の文書名が誰にでも提示され、場合によってはそのままダウンロードができるため機密の文書が第三者に漏洩する	・検索すると非公開のファイル名が漏洩する脆弱性		○
			・検索経由でファイルを開くとセキュリティ機能がバイパスできる脆弱性		○
		・MFP 内部の共有フォルダ内のファイルをコンソールで表示したり、SD メモリに出力したり、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL へ送信する場合、認証不要になることを利用して、権限がない利用者に機密の情報が漏洩する	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性		○
		・攻撃者が管理者になりすまして、MFP 内部の共有フォルダを含めてバックアップを作成して入手し、共有フォルダ内の機密の文書が漏洩する	・認証強度が十分ではない脆弱性（管理者パスワードが単純、または長期間同一である等）	○	
			・認証強度を十分な強度に保つ実装になっていない脆弱性		○
		・保守業者が、ストレージ装置を交換するときに不良品の HDD を回収して持ち帰り、機密の文書を含む共有フォルダ内のファイルを取り出す	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性		○
2. 完全性	・MFP 本体内の共有フォルダにあるファイルが、置き換えられるか、すりかえられてしまう	・攻撃者から、MFP 内部の DB エンジンに対して SQL インジェクションやコマンド・インジェクションを注入され、ファイルが書き換えられてしまう	・MFP 内部共有ファイルへのフォルダ名やパス名、ID 番号、属性などのリクエストの内容の検査が不十分		○
		・MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させながら、特定文書が投入されたときに一部データのすり替えを行う	・MFP の大量処理中にリソース不足または競合によりデータのすりかえが発生してしまう脆弱性		○
		・負荷が多いと、検索用のインデックスや文書管理用のデータベースの一部または全部が破壊される			
		・攻撃者は MFP の共有ファイルサーバの認証手順に対し、手順の途中で「認証完了」のメッセージを送信するか、認証の途中でリクエストを送信し、認証手順のバイパスが成功してしまう	・MFP 内部共有ファイルへの認証をバイパスできる脆弱性		○
		・攻撃者は管理者端末と MFP の共有ファイルサーバの間の保護されていない通信を盗聴して、とりだしたセッション情報を悪用して共有ファイルサーバに対して管理者になりすまし、管理者特権によって MFP 内部の共有ファイルを別のファイルに入れ替える	・MFP 内部共有ファイルと他システムの間の通信が保護されていない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP 本体内の共有フォルダにあるファイルが、置き換えられるか、すりかえられてしまう	・攻撃者は管理者になりすまして、バックアップを取り出し、改ざんしてから書き戻し(レストア)して MFP 内共有ファイルを改ざんする	・認証強度が十分ではない脆弱性(管理者パスワードが単純、または長期間同一である等) ・認証強度を十分な強度に保つ実装になっていない脆弱性	○	○
		・攻撃者はストレージ部品を抜き取り、ストレージ部品内部のセクタを書き換えて、ストレージ部品を MFP 内部に戻し、MFP 内部の共有ファイルを改ざんする	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性		○
3. 可用性	・MFP 本体内の共有フォルダのサービスが利用できなくなるか、非常に長い応答時間がかかるようになる(ファイル取り出し、書き込み、更新、一覧)	・攻撃者が MFP 内部の DB エンジンに対して SQL インジェクションを投入して、MFP 内部のファイルか、DB 内の文書情報を削除される	・MFP 内部の共有ファイルへのリクエストの内容の検査が不十分でリソース不足または処理が停止、遅延する脆弱性		○
		・攻撃者が、MFP に対して認証が失敗するリクエストを大量に送信し、MFP がほとんどの利用者の認証をしばらくの間ロックアウトしてしまう	・攻撃者からの要求で認証失敗が連続すると正規利用者をロックアウトする機能が悪用される脆弱性		
		・MFP 内部の共有ファイルの処理内で処理の無限ループが発生するようなリクエストを注入され、MFP の反応が遅くなるか、停止する	・大量のリクエストや処理の滞留により共有フォルダ上のサービスが利用できなくなる脆弱性(処理メモリ、CPU 処理量、バス帯域の圧迫、一時ファイル、文書ファイル、ログファイルによるディスクの圧迫)		○
		・MFP が大量のリクエストを受けて、MFP 内の共有ファイルサービスが停止する			
		・MFP 内部のストレージ装置が抜き取られるか故障し、MFP 内部の共有ファイルがすべて利用できなくなる	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
4. 真正性	・MFP 本体内の共有フォルダにあるファイルの一部または全部が、どの利用者が作成したものかわからない	・MFP 内部の共有ファイルにファイルを作成しても利用者属性が記録されず、攻撃者はいつでも利用者不明のファイルを作成できる	・MFP 内部の共有フォルダへの作成者による電子署名が行われていない脆弱性 ・MFP 内部の共有ファイルの利用者属性が、文書内容の作成者を示していない脆弱性		○ ○
		・攻撃者は異常に長いユーザ ID を指定したジョブファイルを MFP に送り、MFP 内部の共有ファイル管理ソフトがユーザ属性情報を記録せずにファイルを保存してしまう	・MFP 内部の共有ファイル作成時に利用者識別機能や識別情報の記録処理がバイパスされる脆弱性 ・MFP 内部の共有ファイルへの格納時に入力値を充分に検査していない脆弱性		○ ○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
5. 責任追跡性	・MFP 本体内の共有フォルダにある特定のファイルが、誰が作成し、誰が閲覧したか、履歴をたどれない	・攻撃者はディレクトリ・トラバーサル攻撃を実行して、MFP 共有ファイルをすべて閲覧し、重要な文書を作成している人物の部署と名前を特定し、さらに次に攻撃を行う。しかし、MFP の運用者による監視と監査ではこの攻撃者の行動を検出することができず、攻撃を防止できない	・MFP 内部の共有ファイルの操作履歴が記録されていない脆弱性		○
6. 否認防止	・MFP 本体内の共有フォルダにある特定のファイルを、作成、更新、閲覧した記録にユーザ ID が残っていたが、否認されても立証できない	・運用者は、ある利用者が大量のファイルを閲覧している記録を確認したが、その利用者の閲覧記録は、簡単に注入または改ざんできる記録で、本人のものではなかった	・管理者などによるログの書き換えを受け付ける脆弱性		○
7. 信頼性	・投入したはずの文書ファイルか、取り出した文書ファイルの内容の一部が別のファイルかジョブの内容と置き換わっている ・投入したはずの文書ファイルが、取り出そうとしてもなくなっている ・任意のコードが実行させられる	・攻撃者が MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させながら、特定文書が投入されたときに一部データのすり替えを行う	・大量処理によるリソース不足、競合で誤って処理される脆弱性		○
		・攻撃者が MFP 内部のリソースあふれか競合状態を発生させるようなリクエストを発生させると、一部文書の保存処理が不完全になる。そのため一般利用者からは保存できたように見えるが、保存できていないため取り出せない	・多段の割り込み処理によるリソース不足か競合により、誤って処理される脆弱性		○
		・攻撃者が不正なファイル属性値を指定する命令を注入し、MFP 内部の共有ファイル管理ソフトにスタックオーバフローを起こさせ、任意の命令を実行させる	・MFP 内部共有ファイル属性の入力値の検査不足により、任意のコードが実行させられる脆弱性(パス名、ID、属性値、ファイルデータ)		○

6.13 利用履歴、監査記録

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・利用履歴または監査記録に含まれる、宛先、発番号、サーバアドレスなどのアドレスが 1 件以上漏洩する	・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、どのような制限にも影響なく、利用履歴を取り出した	・MFP へのリクエストの内容の検査が不十分で、非公開のフォルダやファイル名を読み取られる脆弱性、内部命令を注入されて認証と権限の検査をバイパスされる脆弱性(コマンド・インジェクション)		○
		・利用履歴が機密のフォルダにあったが、攻撃者がゲストの権限または一般利用者の権限でファイルを入手できる状態だったため利用履歴が不適切な権限者に漏洩した	・利用履歴、監査記録に関する利用者の認証と権限が適切に設定されていないか、適切に割当処理ができない脆弱性		○
		・利用履歴が MFP 内部の公開フォルダにあったため、第三者に利用履歴が漏洩した	・利用履歴が、利用権限不要なフォルダに公開されている脆弱性		○
		・検索する機能を経由して利用履歴にアクセスすると、権限なしでダウンロードができるため利用履歴が第三者に漏洩する	・検索経由でファイルを開くとセキュリティ機能がバイパスできる脆弱性		○
		・利用履歴をコンソールで表示するか、SD メモリに出力するか、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL へ送信する場合、認証不要になることを利用して、権限がない利用者に利用履歴が漏洩する	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性		○
		・攻撃者が管理者になりすまして、利用履歴を含めてバックアップを作成して入手し、利用履歴が漏洩する	・認証強度が十分ではない脆弱性(管理者パスワードが単純、または長期間同一である等) ・認証強度を十分な強度に保つ実装になっていない脆弱性	○	○
		・保守業者が、ストレージ装置を交換するときに不良品の HDD を回収して持ち帰り、利用履歴が取り出されて漏洩する	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・利用履歴または監査記録が記録されていても内容の一部が改ざんされている	・攻撃者は SQL インジェクションやコマンド・インジェクションにより、利用履歴と監査履歴の特定レコードの時刻かユーザ ID、処理内容の記録を改ざんする	・リクエストの内容の検査が不十分で、利用履歴、監査記録が改ざんされる脆弱性		○
		・攻撃者は利用履歴をかく乱するため、他の利用者が攻撃者と同じ操作をしたかのような記録を、MFP 内部の利用履歴記録モジュールに注入した	・利用履歴、監査記録の追加または削除操作に関する利用者の認証と権限が適切に設定されていないか、適切に割当処理ができない脆弱性		○
		・攻撃者は認証なしで利用履歴を更新した			
		・攻撃者は一般利用者の一人として認証を受け、利用履歴を更新した			
		・攻撃者は書き込み可能なフォルダに配置されていた利用履歴を改ざんした	・利用履歴が、利用権限不要なフォルダに公開されている脆弱性		○
		・攻撃者は MFP に不正な形式の利用履歴リクエストか、認証が完了する前に認証を完了させるかリクエストを送り、MFP は認証なしで利用履歴を更新した	・MFP へのリクエストの内容の検査が不十分で、権限なしで内部データを削除または追加、更新できてしまう脆弱性 ・リクエストの受付インタフェースでセキュリティ機能がバイパスされる脆弱性		○ ○
		・攻撃者は管理者になりすまして MFP 内部の利用履歴を更新した	・認証強度が十分ではない脆弱性（管理者パスワードが単純、または長期間同一である等） ・認証強度を十分な強度に保つ実装になっていない脆弱性	○	 ○
		・攻撃者がストレージのバックアップを取り出し、利用履歴を改ざんしてから書き戻した	・ストレージ内のデータが暗号化などで保護されていないか、保護が不完全である脆弱性		○
		・攻撃者はストレージを抜き出して利用履歴を改ざんしてストレージを元に戻した			
3. 可用性	・利用履歴または監査記録の表示または確認、検査ができなくなる	・攻撃者は SQL インジェクションにより利用履歴と監査履歴をすべて削除する	・MFP へのリクエストの内容の検査が不十分で、ファイルやプロセスにアクセスできる脆弱性		○
		・攻撃者はコマンド・インジェクションにより、MFP 内部にある履歴の記録用プロセスを強制終了させる			
		・攻撃者は MFP に大量のリクエストを送り、その MFP 内部で利用履歴が記録されないようにした上で、攻撃を行う	・大量のリクエストや処理の滞留により利用履歴が記録されなくなる脆弱性(処理メモリ、CPU 処理量、バス帯域の圧迫、一時ファイル、文書ファイル、ログファイルによるディスクの圧迫)		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
3. 可用性	・利用履歴または監査記録の表示または確認、検査ができなくなる	・攻撃者は管理者になりすまして利用履歴の記録を停止させる、または MFP の入力脆弱性を利用して利用履歴の動作を停止させるか、記録処理をしないまま正常終了するよう、実行コードを書き換える	・利用履歴を記録するソフトウェア機能が停止またはバイパスされる脆弱性		○
		・攻撃者は認証なしで利用履歴を削除した	・充分な権限がなくても利用履歴を削除できる脆弱性		○
		・攻撃者は一般利用者の一人として認証を受け、利用履歴を削除した			
		・攻撃者は書き込み可能なフォルダに配置されていた利用履歴を削除した	・削除または書き換え可能な場所に利用履歴を記録する脆弱性		○
		・攻撃者はストレージを抜き出して別のコンピュータからストレージにアクセスし、利用履歴を削除してストレージを元に戻した	・ストレージ上の利用履歴データが保護されていない脆弱性		○
4. 真正性	・利用履歴または監査記録の削除について、誰が行ったものか、正しい時刻かどうかわからない	・MFP 内部の利用履歴を削除しても利用者属性が記録されないため、攻撃者は攻撃を行ったあとでいつも利用履歴を削除する	・利用履歴の操作時に利用者を識別していない脆弱性		○
		・MFP 内部の利用履歴を操作した記録については、攻撃者が任意のユーザ ID を指定して追記させ、どの管理者が利用履歴を削除したかわからないようにする	・利用履歴の操作時に追加記録されるユーザ ID が、任意の値にできる脆弱性		○
5. 責任追跡性	・利用履歴または監査記録の削除について、誰が行った処理の記録か、特定できない	・昨日まではあった利用履歴が削除されていても、どの管理者が行ったのかわからない	・利用履歴の削除操作自体は記録していない脆弱性		○
6. 否認防止	・利用履歴または監査記録の削除について、特定の利用者が実行したものと記録があっても、記録の根拠がなく立証できない	・利用履歴の削除を行った利用者として、管理者のユーザ ID が記録されていたが、攻撃者が任意の文字列に改ざんできるようになっていたため、誰が行ったのかわからなかった	・MFP の既存の利用履歴記録を修正できる脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・利用履歴または監査記録が正しい時刻と真正なユーザ ID、正しい処理名とともに記録されていない ・実際に行った利用の履歴の一部または全部が記録されていない	・ある MFP は再起動すると管理者が手動で時刻合わせをするまで MFP 内部の時刻が 1970 年になるため、攻撃者は攻撃の前に MFP に不正なパケットを送って再起動させ、それから MFP に攻撃を行うことで、攻撃中の記録を古い記録として残させる。管理者が時刻を合わせると、古い時刻の攻撃の記録は自動的に削除され、管理者は攻撃の確認ができなくなる	・MFP が正しい時刻を保持していない脆弱性		○
		・攻撃者は、ある MFP が利用履歴と監査情報をあとから修正できる機能があるため、これを悪用して MFP に攻撃を加えたあと、すぐに記録を消去した	・MFP の既存の利用履歴記録を修正できる脆弱性		○
		・ある MFP は監査記録のユーザ ID が常に同じになるため、攻撃者が MFP を攻撃して機密の文書を取り出した記録を特定できない	・MFP が利用履歴の記録時に、識別済みか認証済みの利用者情報を記録していない脆弱性		○
		・MFP の一部の利用履歴だけは、数値データの範囲やメッセージ長の長さの異常により、間違った処理名や、メッセージの一部しか記録されないため、攻撃者の攻撃手法を分析できない	・MFP の一部の利用履歴は、間違った処理名や値が記録されている脆弱性		○
		・攻撃者は異常に長いユーザ ID を MFP に送り、MFP 内部の履歴記録機能がユーザ属性情報を記録しないようにする	・利用履歴または監査記録に記録されるユーザ ID は利用者認証の結果を反映していない脆弱性(常に固定か、不定の値)		○

6.14 MFP 利用課金情報

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・課金情報、利用量情報が、権限のない者に漏洩する	・攻撃者がリクエスト引数に SQL インジェクションを仕掛けて、適切な権限なしで、課金情報を取り出す	MFP へのリクエストの内容の検査が不十分で、認証をバイパスできる脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・課金情報、利用量情報が、権限のない者に漏洩する	・課金情報が公開フォルダにあったため、第三者に課金情報が漏洩する	・課金情報が、利用権限不要なフォルダに公開されている脆弱性		○
		・課金情報が、攻撃者がゲストの権限または一般利用者の権限でファイルを入手できる状態だったため課金情報が不適切な権限者に漏洩する			
		・検索する機能を経由して課金情報にアクセスすると、権限なしでダウンロードができるため第三者に漏洩する	・検索経由でファイルを開くとセキュリティ機能がバイパスできる脆弱性		○
		・課金情報をコンソールで表示したり、SD メモリに出力したり、紙に印刷、ファクスに送信、ボックスに配信、PC など他システムのフォルダに配信、メールで配信、他システムの URL へ送信する場合、認証不要になることを利用して、権限がない利用者に課金情報が漏洩する	・出力先の種類によってセキュリティ機能をバイパスできる脆弱性		○
		・攻撃者は、管理者がログインしたままになっている管理者端末を悪用して、課金情報を含めて MFP 内部データのバックアップを作成して入手し、スプールされていたジョブデータの機密の文書と、ID、パスワード、セッション情報が漏洩する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
2. 完全性	・MFP 利用課金情報の一部または全部が改ざんされ、利用者の適切な課金情報を収集できないか、利用者に適切な請求が行われない	・攻撃者は SQL インジェクションを悪用して、MFP の利用課金情報を 30%少ない値に書き換え、保守業者に支払う毎月の課金を 30%減少させた	・MFP へのリクエストの内容の検査が不十分で、利用課金情報をコマンド・インジェクションによって書き換えできる脆弱性		○
		・攻撃者は管理者になりすまして、MFP の利用課金情報をゼロに書き換えていた	・認証強度が十分ではない脆弱性(管理者パスワードが単純、または長期間同一である等)	○	
		・攻撃者は保守員になりすまして、MFP の利用課金情報を 2 倍に書き換えていた	・認証強度を十分な強度に保つ実装になっていない脆弱性		○
		・攻撃者は MFP の遠隔保守用の課金集計 API を特定し、利用課金情報をゼロに書き換えていた	・利用者に公開されていないインタフェース（遠隔保守インタフェース)の脆弱性		○
			・認証が行われていない外部インタフェースの脆弱性		○
		・攻撃者は MFP の遠隔保守用の http proxy 上に追加の処理を挿入し、課金報告メッセージ内の課金数値をゼロに書き換えるようにして、保守業者への従量課金を継続的に毎月ゼロにした	・遠隔保守インタフェースの通信データが保護されていないか、保護が不完全である脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP 利用課金情報の一部または全部が改ざんされ、利用者の適切な課金情報を収集できないか、利用者に適切な請求が行われない	・攻撃者は、MFP 内部にある EEPROM を部品交換して、利用済みの利用課金情報を書き込み、過大な料金が請求されるようにした	・MFP が攻撃者から物理的に操作可能な状態にある脆弱性	○	
		・攻撃者は、MFP 内部にある、利用課金情報を書き込むストレージ部品を撤去または破壊し、課金情報が記録されないまま利用を継続した			
3. 可用性	・MFP の利用があったのに利用課金情報が加算されなくなる ・保守機能または遠隔保守機能の機能が無効またはアクセス不能にさせられ、課金情報をとりだせなくなる	・攻撃者は、MFP 内部にコードを注入し、MFP をよく利用する時間帯だけ、利用課金を加算する処理をバイパスさせ、保守員に支払う課金を 6 割減少させた	・利用課金を加算する処理が停止またはバイパスされる脆弱性		○
		・攻撃者は間違った保守員認証を連続的に実行し、保守業者がログインできないようにした	・保守員認証で間違ったパスワードが数回連続すると保守員モードを一定時間ロックする機能が悪用される脆弱性(コンソール認証、遠隔認証ともに)		
		・攻撃者は管理者になりすまして課金情報を消去した	・管理者が課金情報を消去できる脆弱性		○
4. 真正性	・MFP 利用課金情報が正しい値かどうかわからないため、MFP 利用課金情報が改ざんされていてもわからない	・攻撃者は MFP の課金集計 API を特定し、マイナスの数値を注入して、利用課金情報を減らし、課金を減額した	・利用者に公開されていないインタフェースが動作してしまう脆弱性 ・利用課金情報を交換する外部インタフェースで認証が行われていない脆弱性		○ ○
		・攻撃者はMFPの課金集計APIを悪用し、過大な利用実績値数値を注入して、利用者課金情報を実際よりも 60%増大させ、課金を増額させた	・利用課金情報を加算するソース情報を識別、特定していない脆弱性		○
5. 責任追跡性	・MFP 利用課金情報が初期化されるか、予想外の数値に改ざんされていたとしても、その原因を確認できない	・その MFP 内部のソフトウェアには利用課金情報の操作履歴を記録する機能がオプションで、搭載されていなかった	・利用課金情報の操作履歴が記録される機能が無い脆弱性		○
		・その MFP 内部の利用課金情報の操作履歴の記録を行うソフトウェアにはユーザ ID を記録する機能がなかった	・利用課金情報の操作履歴の記録に、時刻、ユーザ ID、操作種別のいずれかが記録されていない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
6. 否認防止	・MFP 利用課金情報の一部または全部が消去・改ざんされたのに、特定の保守員が行った、ということを立証できない	・攻撃者は利用課金情報を削除したあと、遠隔保守業者が削除したかのような操作履歴を API 経由で注入し、原因利用者を特定しにくくした	・操作の記録にユーザ ID が記録されていたが、そのユーザ ID は利用者が改ざんできる脆弱性		○
7. 信頼性	・長大で多数のジョブデータが集中するなど、特定の条件下で MFP の利用課金情報が適切な値でなくなり、正しい課金ができなくなる	・攻撃者は MFP 内部に特定の競合状態が発生するように、長時間かかるジョブを投入し続け、利用課金情報が加算されないように、別の大量のジョブを実行させた	・競合状態、リソース管理に関する脆弱性		○
		・攻撃者は犯行時に、MFP の時刻を大幅に狂わせておいたため、該当時刻の攻撃が記録されたが、保存期間範囲外として翌日の定期処理で削除され、記録が残らなかった。(「正しい時刻」にも同じ記載	・MFP が正しい時刻を保持していない脆弱性		○
		・1,000 部の印刷を 4 台の MFP に分散して処理したところ、4,000 部の課金が加算され、過大な利用課金請求があった	・他の MFP に分割したジョブデータの印刷を二重に課金する脆弱性(不具合)		○

6.15 通信システム(スイッチ、DHCP, DNS, NTP を含む)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP が通信するための配線またはコネクタが露出しており、容易に別の装置を挿入して盗聴される。無線電波が容易に盗聴される ・スイッチングハブまたは VLAN に、物理的制限も認証もなしで容易に接続でき、盗聴、第三者中継を行われる (通信機器には DNS、DHCP,NTP を含む)	・攻撃者が、装置を通信システムのケーブルの間に挿入し、以下の保護されていない通信を盗聴してメールサーバ用の ID とパスワードを収集、記録する 保護されていない通信: IPv4, IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, raw9100, IPP など	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全な脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・MFP が通信するための配線またはコネクタが露出しており、容易に別の装置を挿入して盗聴される。無線電波が容易に盗聴される ・スイッチングハブまたは VLAN に、物理的制限も認証もなしで容易に接続でき、盗聴、第三者中継を行われる (通信機器には DNS、DHCP,NTP を含む)	・MFP の USB プリンタポート、USB メモリポート、USB 認証ユニットポートが、TCP/IP で伝送され、遠隔地に延長されていたが、通信内容が保護されていなかったため、機密の文書、認証用のカード番号などが盗聴され、攻撃者に漏洩する	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全な脆弱性		○
		・攻撃者が、MFP が利用する無線 LAN の WEP 鍵を解読し、MFP が通信する外部の共有ファイルサーバとの ID とパスワードを FTP プロトコルから取り出す。攻撃者は MFP になりすまして共有ファイルサーバ内の文書を取り出す	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(暗号強度に関するポリシ)	○	
		・攻撃者は遠隔のスイッチングハブ上で、VLAN 配布プロトコルを使って MFP 専用の VLAN に所属する Ethernet ポートを作成し、MFP と同一の VLAN に接続する。その後攻撃者は MFP のデフォルトゲートウェイになりすまし、第三者中継攻撃を実行する	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全な脆弱性		○
		・MFP を間違った VLAN に接続したか、IPsec の構成が間違っていたため、ネットワーク上で MFP が隔離されておらず、一般利用者と同じネットワークに接続し、保護されていない通信が盗聴されていた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(ネットワークケーブル接続、設定誤り)	○	
2. 完全性	・MFP の保護されていない通信が改ざんされる ・USB/SCSI などの汎用インタフェースで第三者中継され、印刷・スキャン・ファクスのイメージデータやアドレスが改ざんされる (通信機器には DNS、DHCP,NTP を含む)	・DNS サーバからのホスト名解決応答が保護されていなかったため攻撃者によって改ざんされ、以後の MFP からのリクエストが、攻撃者が用意したホストへと誘導される	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全な脆弱性		○
		・攻撃者が、装置を通信システムのケーブルの間に挿入し、保護されていない通信に介入してメールサーバ用の ID とパスワードを改ざんする その他の保護されていない通信: IPv4/IPv6, DHCP, ARP, ICMP, ICMPv6, LLMNR, Rendezvous, TCP, UDP, UPnP, DNS, TELNET, SNMP, SMTP, POP3, IMAP4, SIP, FTP, HTTP, SMB, LPR, raw9100, IPP など			

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・MFP の保護されていない通信が改ざんされる ・USB/SCSI などの汎用インタフェースで第三者中継され、印刷・スキャン・ファクスのイメージデータやアドレスが改ざんされる (通信機器には DNS、DHCP,NTP を含む)	・DHCP/DHCPv6 サーバからの応答メッセージが保護されていなかったため、改ざんされた DHCP 応答メッセージを受信した MFP はそれ以後、攻撃者が用意したデフォルトゲートウェイを常に使うようになった	・MFP と他システムとの間の通信で相互認証が行われていない脆弱性		○
		・MFP の USB プリンタポート、USB メモリポート、USB 認証ユニットポートが、TCP/IP で伝送され、遠隔地に延長されていたが、通信内容が保護されていなかったため、攻撃者が介入し、ジョブデータが改ざんされて、印刷部数が常に一部多く改ざんされていて、機密の文書が漏洩した	・MFP と他システムとの間の通信内容が保護されていないか、保護が不完全な脆弱性		○
		・攻撃者が、MFP が利用する無線 LAN の WEP 鍵を解読し、MFP が通信する、保護されていない外部の共有アドレスサーバとの通信に介入し、グループアドレスに攻撃者を追加する改ざんを行い、攻撃者は MFP が特定のグループに送信するファイルのコピーをメールで得ることになり、機密の文書が漏洩する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(暗号強度に関する認識不足)	○	
		・MFP を間違った VLAN に接続したか、IPsec の構成が間違っていたため、ネットワーク上で MFP が隔離されておらず、一般利用者と同じネットワークに接続し、保護されていない通信が改ざんされていた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(ネットワークケーブル接続、設定誤り)	○	
3. 可用性	・通信機器の盗難または配線の切断や盗難、端子の抜けにより、MFP を利用できなくなる ・通信機器の動作停止により MFP を利用できなくなる ・通信システムの構成間違いにより、MFP 自体に通信できないか、他システムと MFP が通信できないために MFP を利用できない (通信機器には DNS、DHCP,NTP を含む)	・攻撃者は MFP に接続された Ethernet ケーブルを抜いたところ、通信を必要としない MFP のサービスも停止した	・MFP は通信システムが介在しないと利用できない脆弱性		○
		・スイッチングハブまたは無線 LAN アクセスポイントの故障により、通信を必要としない MFP のサービスも停止した			
		・VLAN または IPsec、VPN の構成を間違うか、所定の VLAN ポートか所定の Ethernet ポートに接続しなかったため、MFP がサービス提供できない	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性(ネットワークケーブル接続、設定誤り)	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	・通信相手の機器が所定のセキュリティ要件で特定された機器かどうか、確認できない (通信機器には DNS、DHCP,NTP を含む)	・数十台の MFP が利用する NTP サーバとの通信で、認証が行われていなかったため、偽の NTP サーバを利用させられる	・MFP と他システムとの間の通信で相互認証が行われていない脆弱性		○
		・DNS サーバからの応答に偽のホスト名情報が紛れ込んでいて、MFP の外部共有フォルダにファイルを書き込むときに偽のホストに誘導される			
		・偽の DHCP から偽の DNS サーバの IP アドレスを注入される			
5. 責任追跡性	・偽のソースアドレスで通信が行われても、どの機器からの通信だったのか特定できない (通信機器には DNS、DHCP,NTP を含む)	・MFP の時刻が大幅に変化する現象があったが、記録がないため、どの NTP サーバの不具合かわからない	・MFP が通信システム上で設定した IP アドレス構成を履歴として記録していない脆弱性		○
		・MFP が偽の IP アドレスを注入されていたが、どの DHCP サーバから注入されていたか特定できず、対策を立てられない			
		・DNS の応答に脆弱性を攻撃するデータが含まれていたが、記録がないためどのホストが応答または注入したものか特定できない			
6. 否認防止	・通信相手を特定するためのアドレスについて記録があっても、対向システムの管理者が否認すると立証できない (通信機器には DNS、DHCP,NTP を含む)	・通信の記録にユーザ ID は含まれているが、任意のユーザ ID を投入できるため証拠にならない	・接続の記録にユーザ ID が記録されていたが、そのユーザ ID は改ざんできる脆弱性		○
		・通信の記録はどのホストからでも注入可能なため、攻撃者からの記録が混じり、不具合の原因を特定できない			
		・IPsec で接続していた通信相手との間で、グループ鍵を使っていたため他のホストでもなりすまし可能だったため、接続記録から攻撃があったと見られる利用者端末を特定できなくなる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
7. 信頼性	・通信において送信したデータが他のデータと混同されて受信されるか、送信したデータの一部が欠落して受信されることで正しい動作ができない (通信機器には DNS、DHCP,NTP を含む)	・通信システムの負荷が容量を超えると、IP パケットの欠落が発生する。その結果 MFP は、再送処理を行うが、MFP 内部でも処理負荷が高まることから、競合やリソース不足が発生し、処理を中断したり不完全なまま処理が実行されたりする	・競合またはリソース不足による脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・通信において送信したデータが他のデータと混同されて受信されるか、送信したデータの一部が欠落して受信されることで正しい動作ができない (通信機器には DNS、DHCP,NTP を含む)	・攻撃者が DNS、DHCP、NTP サーバに複雑な多種類のリクエストを送り、これらサーバ内の競合により一部のパケットや応答メッセージが欠落したり入れ替わったりし、MFP は適切な応答を受信できない	・他システム上の脆弱性	○	
		・攻撃者が DNS、DHCP、NTP サーバのいずれかに、既知の脆弱性を利用してサーバ内部に侵入し、任意のコードを実行し、MFP は適切な応答を受信できないか、上記サーバが MFP など関連する他システムを攻撃する			

6.16 遠隔管理システム

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	[遠隔管理機能の利用時] ・権限のない遠隔管理機能の利用 ・MFP 内部に保存されている、機密を含む共有ファイル、複数のアドレスが、遠隔管理機能を経由して漏洩する [遠隔管理システムそのもの] ・外部管理システムが攻撃され、外部にあったアドレス帳またはバックアップデータが攻撃者に漏洩する	・攻撃者は、MFP のアドレス帳を送受信する通信のうち保護されていない通信を盗聴し、攻撃者にアドレス帳の内容が漏洩する: アドレス帳の登録・更新、アドレス帳のバックアップ、単発のファクス配信またはメール配信またはサーバ配信を定義するためのアドレス帳同期、複数配信処理を定義するためのアドレス帳同期、他システムからの制御用アドレス帳参照	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・攻撃者は、構成管理サーバ上の脆弱性を突いて侵入またはリクエスト強要し、他システム上に保存されている、MFP で利用するアドレス帳と同じデータ、または MFP のバックアップデータを入手する	・他システム自体の脆弱性	○	
		・攻撃者が管理サーバ、認証サーバ、監視サーバのいずれかに、既知の脆弱性を利用してサーバ内部に侵入し、任意のコードを実行し、MFP は適切な応答を受信できないか、上記サーバが MFP など関連する他システムを攻撃する			

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	[遠隔管理機能の利用時] ・MFP に投入または取り出すアドレス、構成情報が改ざんされる [遠隔管理システムそのもの] ・外部の管理システム上の構成情報が改ざんされ、複数の MFP が予期せぬ動作をする ・認証サーバの一部が置き換えられるか、認証データの一部が改ざんされてなりすましされるか、サービスが停止させられる	・攻撃者は通信路上で ARP 偽装を使って管理者端末や保守用端末と MFP の間の通信に介入し、MFP に投入されるアドレスを改ざんし、攻撃者のアドレスを追加し、以後継続的に機密の文書の盗聴を行う	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・MFP の遠隔保守を行うインタフェースのポートはデフォルトで閉じているはずが開いており、このポートに攻撃者が接続して遠隔保守機能を悪用する	・MFP の一部の遠隔サービスインタフェースまたは API に、管理者権限で命令を実行できる API が残って稼動している脆弱性		○
		・MFP の遠隔バックアップ機能の CSRF 脆弱性を悪用して、攻撃者が管理者または保守員のウェブブラウザに特定の URL を開かせ、攻撃者が任意の管理機能を実行する	・管理者の端末ブラウザ、保守員の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性		○
3. 可用性	[遠隔管理機能の利用時] ・攻撃者によって MFP に破壊された設定が投入され、MFP を利用できなくなるか、動作不良になる [遠隔管理システムそのもの] ・認証サーバの応答が停止させられ、MFP を利用できなくなる ・監視サーバが停止させられ、稼動情報が得られなくなる ・構成管理サーバが停止させられ、新しいアドレスを追加できなくなる。アドレス帳を検索できなくなる	・攻撃者が、保護されていない構成システムから MFP への構成変更指示のメッセージを改ざんし、破壊された構成データが MFP 内部に登録され、MFP が停止するか、所定の動作をしなくなる	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・攻撃者は利用者端末になりすまして、MFP の遠隔管理インタフェースにアクセスし、何度も ID、パスワードによる認証を試す。すると MFP 用の認証サーバは連続したログイン失敗を検出して、しばらく(数分間)、管理者のログインを禁止する。この作業を連続して行うことで、その他 MFP の管理機能を停止させる	・管理者の認証失敗が連続すると、管理者をログインできなくする機能が悪用される脆弱性		
		・攻撃者は監視サーバの脆弱性を突いて、監視サーバを停止させることで、MFP の稼動情報が収集されないようにする	・遠隔管理システム自体の脆弱性(開発者が準備した遠隔管理システムの場合)		○
		・攻撃者は構成管理サーバの脆弱性を突いて、共有アドレス帳を削除し、MFP に空のアドレス帳を同期させ、MFP でアドレス選択ができなくする			

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	[遠隔管理機能の利用時] ・遠隔管理システムからの認証応答、アドレス帳応答、設定構成変更の要求、保守要求が、認められた遠隔管理システムからのものではなかった [遠隔管理システムそのもの] ・特定の MFP に対して、ある管理サーバや認証サーバが正しい応答を行っているか確認できない	・認証サーバが正しい認証サーバであるか、MFP 側から検証を行っていないシステムで、攻撃者は偽の認証サーバを用意して、MFP と通信させ、別の悪意の端末を利用者になりすましさせて MFP を悪用する	・MFP と遠隔管理システムとの間で、相互認証が行われていない脆弱性		○
		・攻撃者は MFP の監視サーバになりすまし、MFP に対して大量の監視要求メッセージを送信し、MFP を過負荷状態にする	・MFP と遠隔管理システムとの間の通信が保護されていない脆弱性 ・MFP と遠隔管理システムとの間で相互認証が行われていない脆弱性		○ ○
		・攻撃者は管理者に特定の URL を開かせ、管理者の利用端末に CSRF 攻撃を行い、MFP のバックアップデータを取得させ、攻撃者が用意した詐取可能なフォルダに転送させ、攻撃者が MFP のバックアップデータを入手する	・管理者の端末ブラウザ、保守員の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性 (他システムと MFP の間の認証後のステートレスな通信(HTTP など)で、重要な操作や機能に関する要求が、その直前の操作に特有な情報と関連づけがあることを検査していない)		○
		・攻撃者はアドレス帳サーバから MFP への応答メッセージを通信路上で改ざんし、宛先アドレスを攻撃者のアドレスに変更し、機密の文書を攻撃者が入手する	・MFP と遠隔管理システムと間の通信が保護されていないか、保護が不完全である脆弱性		○
		・攻撃者が既知の脆弱性を利用して、認証サーバに任意のコードを実行させて制御を乗っ取り、MFP が要求する遠隔管理システムの認証がすべて正しいと応答させられる。そのため、MFP は偽の管理サーバからの接続を受け入れてしまう	・認証サーバそのものの脆弱性(開発者が準備した遠隔管理システムの場合)		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
5. 責任追跡性	[遠隔管理機能の利用時] ・MFP が遠隔管理システムから要求された処理または遠隔管理システムからの応答について、MFP 内部に記録されているはずなのに記録されていない [遠隔管理システムそのもの] ・遠隔管理システムが、どの MFP にどのような要求を行い、応答結果の成否、失敗理由などの履歴が遠隔管理システムの側に記録されていないため、不具合時に原因調査ができない	・アドレス帳への通信履歴は MFP 内にも、アドレス帳サーバにも記録されていなかったため、攻撃者がアドレス帳データを外部から検索要求して引き出し、外部の業者に販売していたことがわからなかった	・遠隔管理システムとの通信履歴が記録されていない脆弱性		○
		・監視サーバの記録に一部欠けている部分があったが、遠隔管理システムとの通信履歴に時刻がなかったため、監視記録がなかった期間にMFPがどのような処理を行っていたかどうかが特定できず、対策を立てられない	・遠隔管理システムとの通信履歴の記録に、時刻、ユーザ ID、操作種別のいずれかが記録されていない脆弱性		○
		・管理権限で構成変更を行う構成サーバからMFPへの要求を行ったが、MFP には要求が見当たらない。構成サーバがいつなんという要求を送信したか確認しようとしたが、構成サーバ内での履歴がなく確認できず、対策を立てられない	・遠隔管理に通信履歴が記録されていない脆弱性		○
6. 否認防止	[遠隔管理機能の利用時] ・遠隔管理システムからの要求を処理したときに、MFP 内に記録される認証サーバ、監視サーバ、管理サーバの名前が、改ざんされたか、なりすましされたものではないことを立証できない [遠隔管理システムそのもの] ・遠隔管理システム上に、どの MFP に要求したか、どの MFP から要求が来たか記録するとき、MFP のホスト名やユーザ ID が改ざんされたか、なりすましされたものでないことを立証できない	・ある管理者が MFP 内部のバックアップデータを不正に取り出したという、遠隔管理システムから MFP の管理機能を利用した記録があったが、MFP 内部の操作履歴には任意の値を注入できるか、改ざん可能な脆弱性があったため、攻撃者を特定できない	・操作の記録に遠隔管理システムの IP アドレスが記録されていたが、そのユーザ ID は改ざんできる脆弱性		○
		・MFP を遠隔から監視するシステムに、特定の MFP が正常稼動していた、という記録があったが、この状態通知は攻撃者による偽の通知だったため、攻撃者から攻撃を受けていたときの異常通知から警報を出せない(SNMP)	・遠隔管理システムが監視対象の MFP の正当性を検証していない脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	[遠隔管理機能の利用時] ・MFP が遠隔管理システムとの処理を正しく行えない ・MFP は複数の遠隔管理システムからの要求を、受付順序どおり、または優先順序どおり処理できず、前後の入れ替えがある ・受け付けた処理を全部処理せず、一部だけ欠落した。要求の一部が別の要求に置き換わるか、一部の処理を重複して処理する ・受け付けた一部の要求は繰り返し処理され止まらなくなる [遠隔管理システムそのもの] ・遠隔管理システム自体の異常により MFP が正しい処理を行えない ・認証サーバがユーザ ID を取り違えるか、処理中のパスワードの一部が欠落するために MFP を利用できなくなる ・監視サーバが異なる MFP を監視してしまうため結果がおかしい ・アドレス帳共有サーバ内のアドレスデータの対応がずれて欠落しているため適切なアドレスが得られない	・管理者端末のブラウザ上で、攻撃者が送ったメールの本文内にあった URL を開いたところ、不正な JavaScript コードが実行され、その管理者がログイン済みだった共有アドレス帳サーバのアドレス内容がすべて攻撃者にコピーされる	・管理者の端末ブラウザ、保守員の端末ブラウザに対する CSRF リクエスト強要攻撃が成功する脆弱性		○
		・ある MFP へのリクエスト数が一定以上になると、認証サーバから MFP への認証応答を元のリクエストに正しく対応させられなくなり、第三者に意図しない権限を与えてしまう。攻撃者はこれを利用して管理者権限を奪取する	・複数の利用者が同時に同じ MFP を設定変更することにより構成情報が破壊される脆弱性		○
		・あるタイプの保留中ジョブデータが増えると、管理サーバから MFP 内部のアドレス帳への変更操作で、削除と追加の順で処理される指示が逆になり、削除されるべきアドレスが残ってしまう。残ったアドレスは管理外になるため、攻撃者はこれを利用して別の MFP 利用者への偽メッセージを送る	・競合状態、リソース管理に関する脆弱性		○
		・長大なジョブデータの処理中に、MFP 内のリソース不足から、アドレス帳の更新が途中で中断してしまう			
		・複数ある MFP 内部の時刻がばらばらだったため、複数 MFP に分散処理した出力がすべて終わったかどうか監視サーバから確認するのに、さらに数時間かかる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・遠隔管理システム自体の脆弱性を突いて攻撃者が遠隔管理システム上に侵入することにより、遠隔管理システム上で正しい順序で所定の内容の応答をすることができなくなり、MFP が正しく動作しなくなる	・遠隔管理システム自体の脆弱性	○	
		・ある一般利用者の ID とパスワードが漏洩したが、この一般利用者は管理者権限を持ち、管理者用にも同じ ID とパスワードを使っていたため、攻撃者が遠隔から管理者として MFP に接続し、すべての構成情報と ID とパスワードをだましとり、別のホストへの攻撃に利用しながら、機密の文書とアドレスを販売した	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・ある MFP に対して SNMP で監視を行っていたが、ジョブデータのバイトカウンタが 32bit であふれたあと不定値になり監視できない、またはジョブデータのデータ量のカウントのはずがほかのパケットのデータ量も加算されていて比較ができない	・MFP が SNMP で応答する MFP 内部の状態値が間違っている脆弱性(測定方法の間違い、測定対象か応答対象値が入れ替わっている、不適切な型変換や数値変換が行われている)		○

6.17 利用者端末

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・利用者端末内で実行されるドライバソフトウェアで保存される認証用のID・パスワードが漏洩する ・利用者端末内で保存されるスプールファイルが保護されていないため、スプールファイルに含まれる文書とアドレスが漏洩する ・利用者端末から定期的に行われるMFP への状態確認問合せにより、MFP のアドレスと機種が特定される	・攻撃者から利用者端末へのリクエスト強要攻撃により、利用者が過去に送信した履歴が残っていた文書を任意のアドレスに印刷またはファクス、配信させられ、攻撃者に漏洩する	・他システムと MFP の間の認証後のステートレスな通信(HTTP など)で、重要な操作や機能に関する要求が、その直前の操作に特有な情報と関連づけがあることを検査していない脆弱性(CSRF リクエスト強要など)		○
		・攻撃者は利用者端末上の MFP 用ドライバ API、または MFP 用 SDK API の脆弱性を突いて、任意のコードを実行させ、任意のアドレスへ機密の文書のコピーを送信させる	・MFP ベンダが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）(プリント、ファクス、スキャンドライバ)		○
		・攻撃者は利用者端末上にすでに動作しているマルウェアを操作し、MFP 用のドライバに設定してあるアドレスとパスワード、または機密の文書を含むスプールファイルを入手する	・利用者端末の MFP ドライバ用に設定された電子証明書、ID、パスワードが保護されずに保存される脆弱性		○
		・攻撃者は、利用者端末と MFP の間の保護されていない通信を盗聴して、MFP の IP アドレス、型番、利用者の ID、パスワードを収集し、攻撃の準備を行う	・他システム(他の MFP、利用者端末、蓄積・外部処理、遠隔管理システム)と MFP の間の通信が保護されていない脆弱性		○
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、プリントとスキャンの入出力を含めて、MFP と交換するファイルのコピーが攻撃者に転送されていた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
2. 完全性	・利用者端末で実行されるドライバソフトウェアそのもの、または実行中のソフトウェアの状態が改ざんされ、攻撃者により任意のコードが実行される ・利用者端末内に保存されたドライバソフトウェア用に設定された構成情報、認証情報が改ざんされる ・利用者端末と MFP の間のメッセージが改ざんされる	・攻撃者は利用者端末用の MFP 用ドライバ API または SDK 用 API の脆弱性を突いて、特定の脆弱性を攻撃するコードを利用者に実行させ、利用者端末の制御を奪い、ジョブデータを改ざんする	・MFP ベンダが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）(プリントドライバ、ファクスドライバ、スキャンドライバ)		○
		・攻撃者は利用者端末にマルウェアを感染させ、利用者端末上の MFP 用のドライバの構成情報と ID・パスワードを書き換え、利用者が MFP に送信する機密の文書を攻撃者にも送信させる	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
		・攻撃者は MFP と利用者端末の通信路上で ARP 偽装による介入や偽の無線 LAN AP による介入、偽のプロキシサーバによる介入により、MFP と利用者端末の間のジョブデータの改ざんを行い、攻撃者に機密の文書のコピーを送る	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、プリント時のスプールファイルが改ざんされて、攻撃者にもプリントイメージのコピーが配信されていた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
3. 可用性	・利用者端末内で実行されるドライバソフトウェアが削除されるか破壊されていて MFP を利用できない ・利用者端末内に保存されている、ドライバソフトウェアの構成情報または認証情報が削除または改ざんされて MFP を利用できない	・利用者端末にインストールした MFP 用ドライバがすでに破壊されており、MFP を利用できない	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・攻撃者は利用者端末用の MFP 用ドライバ API または SDK 用 API の脆弱性を突いて、利用者端末の制御を停止または暴走させ、MFP を利用できないようにする	・MFP ベンダが提供する MFP 用ドライバソフトウェア自体、または MFP 用 SDK ライブラリ自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ） ・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	○
		・利用者端末が侵入され、MFP 用ドライバが削除されて MFP を利用できない			
		・利用者端末が侵入され、MFP 用ドライバの設定情報が削除または破壊されて MFP を利用できない			
		・攻撃者は一般利用者端末と MFP の間の通信中のセッションに対して、セッション終了メッセージ（無線 LAN, TCP, SSL/TLS)を挿入してセッションを強制終了させる	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・攻撃者は利用者端末上のサービスポート、または MFP 上のサービスポートに多量のリクエストを送り、サービスを停止させる	・利用者端末用のサービスポート上での競合またはリソース不足の脆弱性		○
		・利用者端末内に、MFP 以外のアプリケーションの脆弱性を突いたマルウェアが動作しており、特定の MFP 以外へのプリントができないようになっており、特定の MFP にプリントすると、攻撃者にコピーが転送されるようになっていた	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	・利用者端末上にインストールするドライバソフトウェアが、これから利用しようとしている MFP 用の正しいソフトウェアであるかどうかわからない ・特定の MFP 用のドライバをインストールしようとしている利用者端末が、MFP を利用してよい端末かどうかわからない	・ある利用者端末上にインストールされた、あるMFP用のドライバソフトウェアは、マルウェアが同梱されたものだった。特に警告表示がなかったため、利用者はそのまま利用を継続し、機密の文書が漏洩することにつながった	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・ある利用者端末は、既知の脆弱性がある未修正の OS を利用しており、すでにマルウェアに感染していたが、MFP 用のドライバをインストールされ、MFP へのサービス停止攻撃が実行されてしまった			
5. 責任追跡性	・利用者端末の内部のソフトウェアを、正しい利用者が正しい手順で利用したか、さかのぼって確認できない	・ある他社に自社名で偽の注文指示がファクスで届いたが、誰が送ったか特定できない	・ファクス利用時に MFP を利用する利用者の認証を行わない脆弱性		○
		・ある MFP から大量の印刷物が出力されたが、誰が出力したか特定できない	・MFP を利用する利用者の認証結果を操作履歴とともに記録する機能が無い脆弱性 ・MFP を利用する利用者の認証結果を操作履歴とともに記録する機能を利用していない脆弱性	○	○
6. 否認防止	・ドライバソフトウェアが記録として残した操作記録、処理記録の内容に、改ざんがありえないなどの根拠を示して立証できない	・利用者端末の OS 上で、ドライバソフトウェアが利用されるたびにドライバが行う操作記録の処理において、操作記録には任意の文字列を投入できるなどの改ざんが可能なため、利用履歴にある情報の立証ができない	・操作の記録に利用者端末のホスト名が記録されていたが、そのユーザ ID は改ざんできる脆弱性		○
		・利用者端末上に記録されている使用履歴は、利用者端末上に感染したマルウェアによって改ざんされており利用できなかった			
7. 信頼性	・利用者端末内のドライバソフトウェアと関連するアプリケーションがデータを取り違えるか、欠落させてしまう ・ドライバソフトウェアの制御が乗っ取られ、異なるデータや異なる利用者からのジョブとしてすりかえられてしまう	・特定のデータが含まれるプリントを実行すると、プリンタドライバの脆弱性により、期待どおりに印刷できないか、別のジョブデータやプリンタ内ファイルの内容が混入した印刷物が出力されて、機密の文書が漏洩する	・MFP ベンダが提供するドライバソフトウェア自体の脆弱性（数値処理、情報漏えい、入力の確認、セキュリティ機能、競合状態、リソース管理）（プリントドライバ、ファクスドライバ、スキャンドライバ）		○
		・攻撃者がプリンタドライバの脆弱性を突いて、プリンタドライバ内の制御を乗っ取り、プリンタドライバの設定を書き換えて、プリントが実行されると必ず攻撃者にもプリントの複製が送られるようにされ、継続的に機密の文書が漏洩する			

6.18 蓄積・外部処理(スプーラ、共有フォルダ、メール、業務システム)

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
1. 機密性	・蓄積・外部処理サーバが行う通信が保護されていないために通信路上で盗聴され文書が漏洩する。 ・あるMFPが特定の処理のために他システムから取り出した機密の文書を、その MFP 上で漏洩させてしまう ・蓄積・外部処理サーバ(文書を蓄積するサーバやプロキシサーバ、コンテンツの変換処理などを行うサーバ)で、文書が漏洩する	・攻撃者は、蓄積・外部処理サーバと MFP の間の保護されていない通信を盗聴し、機密の文書を含むジョブデータを入手する。攻撃者は入手したデータを販売し、機密の情報が漏洩する	・他システムとMFPの間の通信が保護されていないか、保護が不完全である脆弱性		○
		・多数の拠点に一度に文書の配信を行う際、複数 MFP ベンダの MFP と複数機種の MFP を使っていたため、一部の MFP に配信するための通信が保護されていなかった。攻撃者は保護されていない通信だけを盗聴して、機密の文書が漏洩する			
		・一部の一般利用者は、MFP 外部の共有フォルダでは権限がないファイルでも、MFP 上に配信を要求すると閲覧できるようになり、部外者に機密の文書が漏洩する	・他システムと MFP の間で、ファイルの所有者や権限などの属性が異なる脆弱性	○	
		・あるサイトではMFPでスキャンされたイメージデータは常に外部の共有フォルダの特定の公開フォルダに格納されるため、似たような文書名の違う資料と取り違えて機密の文書が権限のない者に漏洩する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性 ・誤操作を招く複雑な設定条件と、操作結果がわかりにくい脆弱性	○	○
		・多数の拠点に一度に文書の配信を行う際、複数 MFP ベンダの MFP を使っていたために用語が異なり、配信、親展、ボックス、送信、プリント、メール、サーバ送信、URL 送信などの機能を誤って使用し、不要な印刷出力を行うか、不適切なサーバへの文書のコピーを行っていたため、機密の文書が部外者に漏洩する			
		・攻撃者は、MFP へのジョブデータを一時蓄積するスプールサーバ内部に侵入し、スプールサーバ内に蓄積されるジョブデータを攻撃者にコピーして、ジョブデータに含まれる機密の情報を入手する	・他システム自体の脆弱性	○	
2. 完全性	・蓄積・外部処理サーバ(文書を蓄積するサーバやプロキシサーバ、コンテンツの変換処理などを行うサーバ)で文書またはアドレスが改ざんされる	・攻撃者は、蓄積・外部処理サーバと MFP の間の保護されていない通信に介入し、機密の情報を含むジョブデータを改ざんし、サポートセンタから顧客に新しいパスワードを送信させ、攻撃者が入手する	・他システムとMFPの通信が保護されていないか、保護が不完全である脆弱性		○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
2. 完全性	・蓄積・外部処理サーバ(文書を蓄積するサーバやプロキシサーバ、コンテンツの変換処理などを行うサーバ)で文書またはアドレスが改ざんされる	・攻撃者は、MFP に対して蓄積・外部処理サーバになりすました偽の一時応答を返し、攻撃者が用意した偽の蓄積・外部処理サーバに MFP をリダイレクト接続させる	・他システムと MFP の通信が保護されていないか、保護が不完全である脆弱性		○
		・スプールサーバ、またはスキャン結果を格納するファイルサーバ上で、ジョブデータまたはスキャン結果ファイルを、認証不要で書き換え可能な公開フォルダ上に格納していたため、攻撃者がすべて削除する	・セキュリティポリシの漏れか、管理者にセキュリティポリシが徹底されていない脆弱性	○	
		・攻撃者は MFP に集中的にジョブデータを投入するスプールサーバの脆弱性を悪用してスプールサーバ内部に侵入し、機密の情報を含むジョブデータを改ざんする。	・他システム自体の脆弱性	○	
3. 可用性	・MFP の停止または誤動作、乗っ取りにより、蓄積・外部処理サーバが停止するか誤動作する ・蓄積・外部処理のサーバが停止し、MFP の利用者が MFP を利用できなくなる	・攻撃者は MFP が蓄積・外部処理サーバと通信するポートに対しファジング試験を行い、特定の脆弱性に対して侵入するメッセージを作成し、一般のパソコンに感染させたマルウェアから特定の MFP に送信する。メッセージを受信した MFP は停止するか、誤動作を起こし、利用できなくなる	・MFP が蓄積・外部処理サーバと通信するポートに接続できるホストかサーバを特定し、制限していない脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信を保護していない脆弱性		○ ○
		・攻撃者は、MFPと蓄積・外部処理サーバとの間の特定のセッションに対して、「通信終了」または「メッセージ終了」などのメッセージをなりすまして挿入し、セッションを異常終了させる	・MFP と蓄積・外部処理サーバとの間で相互認証していない脆弱性 ・MFP の他システム用通信ポートで、予想外のデータを受信すると停止または誤動作する脆弱性		○ ○
		・攻撃者が、負荷分散設定がある MFP に、負荷分散処理を許可した大量のジョブデータを投入し、負荷分散対象の MFP も含めて、複数台の MFP が同時に利用不能になる	・受付可能な処理要求量を制限できない脆弱性 ・受付可能な処理要求量の制限を設定していない脆弱性	 ○	○
		・攻撃者は共有ファイルサーバの脆弱性を突いて、共有ファイルサーバを停止させ、共有ファイルサーバ経由でのファイル転送での MFP のスキャナ機能とファクスの配信機能が利用できなくなる	・蓄積・外部処理サーバ自体の脆弱性	○	

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
4. 真正性	・偽の蓄積・外部処理サーバとの間で文書とアドレスを送受信してしまう	・攻撃者が動作させた偽の共有ファイルサーバに、電子ファイルを格納したため、機密の文書が攻撃者に漏洩する	・蓄積・外部処理サーバとMFPとの間で相互認証を行う機能が無い脆弱性 ・蓄積・外部処理サーバとMFPとの間で相互認証を行う設定となっていない脆弱性	○	○
		・攻撃者が動作させた偽のメールサーバを経由してファクスメールが MFP に送られ、送信者を偽装した偽の請求ファクスが着信し、間違った口座に送金した			
5. 責任追跡性	・特定の蓄積・外部処理サーバが扱うデータが、どのサーバを経由して伝送されたものであるか、確認できない。不具合があっても原因を特定できない ・正しい経路で通信が行われているかどうか確認できない	・攻撃者が、あるメールサーバの脆弱性を利用して MFP に偽の配信要求を送信したが、MFP には記録がなく、どのメールサーバが攻撃に使われたか特定できず対策を立てられない	・外部・蓄積システムとの間で通信を行った履歴が MFP に記録されていない脆弱性 ・蓄積・外部処理サーバ自体の脆弱性	○	○
		・MFP と蓄積・外部処理サーバとの間の通信について、多数の認証失敗の通信履歴が記録されていたが、通信相手のホスト名は DNS サーバ上で偽装されたもので、ホスト名から相手サーバを特定できなかった	・MFP 内部に記録する利用者端末との通信履歴の内容のうち、逆引きされたホスト名は DNS で偽装される脆弱性	○	
6. 否認防止	・特定の蓄積・外部処理サーバの処理記録について、サーバを特定する情報が確かである根拠を示せない	・蓄積・外部処理サーバとの間の転送記録のうち、IP アドレスについては認証時に記録されるが、セッション情報を利用してほかの IP アドレスからもサービスを利用できるため、攻撃者は記録にない IP アドレスから攻撃を行う	・操作の記録に蓄積・外部処理サーバの IP アドレスが記録されていたが、その IP アドレスは改ざんできる脆弱性		○
		・MFP と蓄積・外部処理サーバとの間の転送記録のデータは、SQL インジェクションで改ざんされていることがわかり、原因調査に使えない			
		・ファクスの中継機能を利用した多段の配信で、途中に不正なファクスが中継を行っていないことを確認しようとしたが、2 段目のメールファクスの一部で、どこからのファクス着信があったか通信記録の項目が欠けていたため、経路の確認ができなかった	・外部・蓄積システムとの間で通信を行った履歴が MFP に記録されていない脆弱性 ・外部・蓄積システムとの間で通信履歴に、充分な記録が含まれていない脆弱性		○ ○

	T. この二次資産に対する脅威	M. この脅威を実現する攻撃手法または事故の例	V. この攻撃例または事故例の原因となる脆弱性	対策すべき関係者	
				利用者	開発者
7. 信頼性	・蓄積・外部処理サーバから MFP が受信したジョブデータが壊れている ・MFP から蓄積・外部処理サーバに送信したジョブデータが正しく保存または処理されない	・攻撃者は、MFP に対して、特定の業務サーバになりすまして偽の応答メッセージを返す。偽の HTTP 応答メッセージには SQL インジェクションをしかけて、MFP 内部のデータベースを破壊する	・MFP へのリクエストの内容の検査が不十分で、SQL コマンドが入力できてしまう脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信が保護されていない脆弱性		○ ○
		・MFP から特定の業務システムに対して、特定のデータ取得要求を送ると、失敗応答を返したり、タイムアウトを起こしたりするが、MFP 内部のソフトウェアは成功応答が返るまで処理を繰り返し、以後複数のプロセスが起動するためリソース不足に陥る	・競合、リソース管理が不十分な脆弱性		○
		・攻撃者は MFP から負荷分散処理のために送信される、別の MFP への処理要求を、再びスプールサーバにリダイレクトさせて投入させ、ジョブデータを無限に循環処理させる	・ジョブデータの宛先などの識別情報を確認していない脆弱性 ・MFP と蓄積・外部処理サーバとの間の通信が保護されていない脆弱性		○ ○
		・外部のファイルサーバが脆弱性を突かれて侵入され、MFP から送信したファクスイメージやスキャンイメージのファイルが正しく保存されず、利用できない	・蓄積・外部処理サーバ自体の脆弱性	○	

7. 脆弱性の詳細解説

本章では、前章で列挙した MFP に関する脆弱性の中で、特に注目しなければならない項目について詳細解説を行う。具体的には、近年話題となり、攻撃方法が公知になっているもの、及び実際に脆弱性が報告されているものを網羅的[14]に解説する。各解説においては脆弱性の概要、解説、及びその対策を示す。解説では脆弱性に係る具体的な攻撃手法を例示する。対策は、読者対象を利用者（主に管理者）、開発者、及び評価者に分けて記載し、それぞれの立場で MFP の当該脆弱性に対する考察の参考として頂くことを目的としている。本章で新しく登場する関係者である「評価者」とは、MFP 製品に対して脆弱性検査サービスを実施する第三者、及びセキュリティ機能面の検査を独自に行う開発ベンダの担当者など MFP 製品の脆弱性を確認する立場にある者である。

7.1 攻撃の前提条件について

まず、1.5 節で記述したように、本章に記述する MFP に関する脆弱性は全ての MFP に当てはまるものではなく、該当する機能を有し、かつその機能が利用可能な状態で運用されていることが前提となる。

本書における攻撃とは、本来権限の無い第三者や利用者が閲覧や改ざんを目的として 5 章で定義した保護資産にアクセスすることを目的とした行為を意味している。例えば以下のような行為が攻撃にあたる。

1) **第三者や利用者が他の利用者の保護資産へアクセスする**
2) **第三者や利用者が管理者機能、または保守機能を利用し、権限のない保護資産へアクセスする**
3) **第三者や利用者が MFP を異常な状態にして権限のない保護資産へアクセスする**

一方、保守員や MFP を導入した企業の管理者による利用者の保護資産へのアクセスは、保守員や管理者に与えられた特権機能、例えば利用者パスワード初期化（変更）等の機能を用いれば可能であるが、それらの機能の制限等については MFP ベンダや MFP を導入した企業の規定やポリシーで扱うべき問題である。よって、本書では当該 MFP の運用状態においては、保守員や管理者といった特権を持った関係者は正しく振舞うことを前提とする。また MFP 製品の製造や配付段階のセキュリティが確保されていることも前提とする。製造や配付のプロセスに関する考察は 8 章で行う。

7.2 深刻度と攻撃能力評価について

各詳細解説項目に記述している深刻度と攻撃能力評価の値は、解説した脆弱性を利用することの容易さ、それに必要な攻撃能力をそれぞれ CVSS の計算ツール[15]によって計算した結果を参考としている。

CVSS2.0 ベースでは色が赤に近い程攻撃される機会が多いことを表している。

[14] 実際、2010 年 1 月～2012 年 7 月までに報告され、CVE に掲載されている MFP に関する脆弱性は全てここで解説する項目に分類される。

[15] http://jvndb.jvn.jp/cvss/ScoreCalc2.swf?lang=ja&g=1

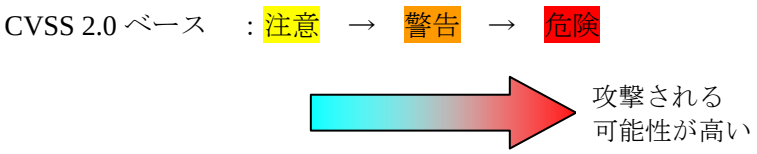


図 7-1 攻撃能力の説明図

なお、以下に解説する脆弱性に関して、例えば 6.3 節の 1.機密性の欄に記載したような攻撃、つまり企業内に置かれた運用状態の MFP を気づかれずに開け、RAM（揮発性メモリ）を瞬時に冷却し、冷却したことによりデータが保持される僅かな時間内に当該メモリを攻撃に使用する設備のある場所まで運び解析するような非常に高度で攻撃機会も限られた攻撃は、現実的に考えても MFP の機能的な対策のみで解決できる脆弱性ではない。その様な脆弱性は CVE 等にも登場しない。よって本章では、利用者、開発者、及び評価者が認識し対応すべき項目、現段階で現実問題として攻撃される可能性の高い項目を網羅的に解説する。

7.3 記録媒体のデータ保護に関する問題

近年の MFP に内蔵されている代表的な記憶媒体は HDD である。保護資産を扱うことを想定した MFP では、HDD に一時的に保存される機密文書のデータや、永続的に保存される管理者や利用者のパスワード及び設定情報といった資産を保護しなければならない。一方、MFP に内蔵された HDD は、簡単に視認でき、通常は取り外しや交換が可能である。したがって攻撃者の手に HDD が渡っても、その中にあるデータ（保護資産）が漏洩しない仕組みが必要となる。

基本的な話ではあるが、HDD に格納される保護資産の保護手段として安全だと言われているのは、HDD 上の全領域の暗号化である。HDD 上の一部のデータの暗号化や、HDD のパスワードによるロックは脆弱であることが知られている。但し、近年セキュリティを意識した MFP において HDD をロックパスワードのみにより保護しているような MFP 製品は国内ベンダ製品において殆ど存在しない。

7.3.1 【HDD 暗号化】

最初に考慮しなければならない攻撃は、HDD 上の全領域暗号化を実施してない MFP から、攻撃者が HDD を持ち出し、別の MFP や PC に接続して保存されている保護資産を読み出す攻撃である。この攻撃はローカル環境で直接 MFP にアクセスできる利用者であれば簡単である。攻撃の危険度は高く、攻撃に必要な能力は低い。本節では暗号化されていない HDD 等の記憶媒体の持出しに関してもスコアリングするが、現在殆どの MFP に HDD 暗号化が実装されていることを考慮し、HDD 暗号化が実装されていることを前提とした攻撃手順について考察する。

また、HDD 暗号化による対策はハイバネーション（休止状態にする）機能を実装している MFP に対しても有効である。ハイバネーションの状態においては揮発性メモリ上の保護資産が一時的に HDD 上に展開されているため、HDD の持ち出しによりそれら揮発性メモリ上の保護資産（これは本来攻撃が困難なものである）まで漏洩する可能性がある。

7.3.2 【廃棄時の全領域削除】

また、利用者が MFP 製品を廃棄、もしくはリース返却する場合は、MFP に内蔵されている HDD の内容を全領域上書き削除すること等により HDD 上のデータが復元できない状態とすることが望ましい。上書き削除の方式には、米国国防総省方式（DoD5220.22-M）方式[16]、Gutmann 方式[17]などが存在し、どちらの方式でもデータの復元をほぼ不可能な状態にできると言われている。これらの方式は実際に現在の MFP で採用されている。廃棄後の MFP 製品を攻撃者が入手した場合、非常に長い時間攻撃を試みることが可能である。計算量的に安全な暗号アルゴリズムにより暗号化されている場合であっても、鍵や鍵を生成するパスワードの漏洩[18]等を考慮し記憶媒体の全領域が削除されることが望ましい。

16 http://www.usaid.gov/policy/ads/500/d522022m.pdf
17 http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
18 鍵が利用者が入力するパスワードから生成されている場合、非常に長い時間をかけた辞書攻撃等により鍵が漏洩する場合が考えられる。

7.3.3 【攻撃手法とその対策】

MFP から、全領域暗号化された HDD を利用者（攻撃者）が取り出し、攻撃者の任意の鍵で暗号化した HDD と入れ替える攻撃を考察する。これにより、以後 MFP の HDD に記録される保護資産は攻撃者が任意に読める形式で保存されるため、保護資産の機密性が失われる。

この攻撃が成立するには、いくつかの条件がある。既存の HDD を復号する鍵は必要ないが、入れ替えた後の HDD を復号するための鍵を攻撃者が MFP に設定できる必要がある。HDD 自体が暗号化チップを搭載していて HDD と MFP 間は復号されたデータがやりとりされている場合[19]、攻撃者は HDD を入れ替えたことに気づかれないように、MFP の設定情報を真似れば良い。設定情報が HDD にある場合、持ち出した暗号化された HDD から設定情報を読み取るのは不可能なため、運用状態の MFP から想定して同様の設定を行うのが妥当である。しかしその場合、攻撃者は同型の MFP を保持している必要があるかもしれない。もし設定情報を HDD でなく不揮発性 RAM に格納する MFP の場合、この準備は必要ない場合もある。

このような、HDD の差し替えを利用した攻撃への対策としては機能的な対策、具体的には HDD を一意に識別し検証する機能が有効である。利用していた HDD を一意に識別できる情報（HDD 個体毎に一意な識別子のハッシュ値など）を本体側に保持し、HDD が差し替えられた場合にはエラーとなり、運用状態にならないことが望ましい。また、HDD を復号するための鍵を入力する機能が攻撃者となる利用者に開放されていなければ（保守機能や管理機能の中で入力する等であれば）入れ替えた後の HDD が利用できない。[20]

補足：正しい暗号アルゴリズムの実装

HDD の暗号化においては、考慮しなければならない項目が 2 つある。1 つは暗号強度、具体的には暗号化するアルゴリズムや鍵長、鍵の強度であり、もう 1 つは鍵管理の仕組みである。

暗号強度の確認材料としては、例えば暗号アルゴリズムが正しく実装されているかどうかを確認する制度がある。このような制度には、米国政府の国立標準技術研究所(National Institute of Standards and Technology／NIST)の FIPS140-2 に基づく CMVP 制度、及び IPA の「暗号モジュール試験及び認証制度」による暗号アルゴリズム確認がある。例えば、利用者は保護資産を暗号化している仕組みが、これらの制度による確認を受けているか否かを、その暗号アルゴリズムの実装が信頼できるかどうかの判断基準とすることができる。これらの制度では、鍵生成を行う場合の鍵の強度も確認することができる。

補足：鍵管理

鍵管理に関しては、例えばその鍵をさらに別の鍵で暗号化して管理する場合においても、最終的には MFP のどこかに平文で鍵が保存されることになる。その平文の鍵が、どこに保存され、どの様に保護されているかが重要となる。平分の鍵が RAM 等に保存されている場合、どうしても保護資産が漏洩してしまう可能性が残る。その最終的に秘匿しなければいけない鍵を保存する手段の一つとして、TPM[21]を搭載することが有効と考えられる。TPM は、TPM 内部のメモリへ不正にアクセスしようとするとメモリの内容が消去される等の耐タンパ性を持っている。

---

19 例えば、Seagate の DriveTrust 等は HDD に暗号化チップをもっている。
http://www.seagate.com/docs/pdf/whitepaper/TP564_DriveTrust_Oct06.pdf

20 但し、保守機能に関しては後述する脆弱性も考慮しなければならない。

21 http://www.trustedcomputinggroup.org/developers/trusted_platform_module/

補足：USB メモリなどの着脱式メディアへの保護資産の保管

USB メモリなどの着脱式メディアに保護資産を格納する場合、利用者は HDD と同様、暗号化機能により着脱式メディアのセキュリティを担保することが望ましい。例えば USB メモリの場合、運用状態において USB メモリに保存される保護資産は当該 USB メモリの所有者のものに限られ、他の利用者からアクセスされる機会は少ないが、USB メモリ自体を紛失する可能性も高い。USB メモリに保護資産を格納する運用を行っている利用者は前述した CMVP や「暗号モジュール試験及び認証制度」の認証を取得した USB メモリの選定と運用ポリシーが必要であると考える。

7.3.4 【原因と考察】

HDD などの記憶媒体を持ち出されてしまう原因は、汎用的なものを利用しており、攻撃者が視認し易いためである。しかし、持ち出しそのものは MFP に限らずサーバやアプライアンス製品でも同様であり、利用者が運用面で対応すべきである。開発者に要求されることは、持ち出されても既存の保護資産が計算量的に安全で読み出せないような暗号化による保護を実装すること、及び暗号化されたデータを復号するための情報を適切に管理するよう実装することである。その上で、上記のような HDD の差し替えや、RAM からの鍵情報の読み出しなどに対して、どこまで対応しているのかを確認し、製品の目指すセキュリティレベルに応じて必要な機能を実装することが重要である。

7.3.5　対策

【運用ガイド】

1) 暗号化機能を有効にする。もしくは機能を実装した MFP を選択する。
2) 廃棄／返却時に全領域削除する機能を実行する。（全領域削除する機能を実装した MFP を選択する。）
3) 暗号化に用いる暗号アルゴリズムや鍵の安全性がどのように担保されているかを確認する。
4) TPM 等により秘密鍵が保護されている場合、PIN コード[22]を適切に管理する。
5) USB メモリなどを保護資産の保管先として用いる場合、例えば CMVP や「暗号モジュール試験及び認証制度」の認証を取得した製品を選択[23]する。

【開発ガイド】

6) HDD の全領域暗号化機能を実装する。
7) MFP に保護資産が入った記憶領域の全領域上書き削除機能を実装する。
8) 安全性が担保できるような暗号化の仕組みを実装（選定）する。
9) HDD 等の交換可能部品について、不正な入れ替えを検出する検証機能を実装する。

【検査ガイド】

10) HDD の暗号化による保護を評価する場合は、暗号アルゴリズムや秘密鍵の強度、及び鍵の生成方法や保管場所の安全性を確認する。
11) HDD の検証が無い場合、HDD の復号鍵を復号するコード等の入力が保護されていること、もしくはその強度を確認する。

7.3.6　参考情報

公開年月	情報源
2009 年 3 月	HDD パスワードロック解除 http://homepage3.nifty.com/3gatudo/hddlock.htm#hdd HDD ロックパスワードが公開されている DOS ツールで再設定できるという記事
2008 年 7 月	Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications http://www.cs.washington.edu/research/security/truecrypt.pdf HDD 上の一部領域のみの暗号化は脆弱な場合があるという例示
2012 年 5 月	CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP) http://csrc.nist.gov/groups/STM/cmvp/index.html 北米 FIPS140-2 に基づく CMVP の説明
2012 年 8 月	暗号モジュール試験及び認証制度(JCMVP®) http://www.ipa.go.jp/security/jcmvp/index.html IPA の「暗号モジュール試験及び認証制度」の説明
2009 年 4 月	ハイバネーションの危険性 http://www.st.rim.or.jp/~shio/winsec/hibernation/ ハイバネーション時に HDD 上に展開されるデータの扱いに関する危険性の説明

[22] 数桁からなる暗証番号。PIN とは Personal Identification Number のこと。
[23] それぞれ、MODULE VALIDATION LISTS(http://csrc.nist.gov/groups/STM/cmvp/validation.html)、暗号モジュール認証製品リスト(http://www.ipa.go.jp/security/jcmvp/val.html)に製品が列挙されている。

7.3.7　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

まずワーストケースとして、設定情報等を含んだ保護資産が、暗号化されていない HDD に保存されている MFP 製品を考察する。持ち出された HDD が汎用 OS を搭載した PC で容易にマウントできる場合もあるが、スコアリングでは前提として以下を想定する。

・攻撃対象と同型の MFP を所有していること。
・HDD 上の保護資産が削除されていないこと。
・MFP に物理的にアクセス可能であること。

【スコアリング】

CVSS 2.0 ベース 基本値： 6.6（警告）

攻撃元区分	ローカルでのみ攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	影響なし
可用性	全面的な影響

【攻撃の前提条件】

次に、上記した攻撃手法通り暗号化された HDD を差し替えて一定期間後に回収することにより、その間の HDD 上に保存された保護資産が漏洩する攻撃を考察する。この場合も同型の MFP を保持し、以下の条件を前提とする。

・MFP に物理的にアクセス可能であること。
・HDD 上の保護資産が削除されていないこと。
・HDD の復号鍵の入力が利用者に開放されていること。
・HDD の識別検証機能が MFP に実装されていないこと。

【スコアリング】

CVSS 2.0 ベース 基本値： 4.4（警告）

攻撃元区分	ローカルでのみ攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	部分的な影響
可用性	部分的な影響

7.4　SSD 搭載による情報漏えいの問題

従来､MFP は保護資産を格納する大容量の記憶媒体として HDD を内蔵している。HDD は第三者や利用者により持ち出される危険性があり、また削除したデータが比較的簡単に復元できるといった特性があるため、殆どの MFP は 7.3 節で解説したデータの上書き削除や暗号化により保護資産の漏洩に対策している。

その HDD が、近年では、データアクセスの高速化、故障率低下を目的として、SSD に代替されつつある。HDD と SSD を両方内蔵し、高速なアクセスが要求されるデータに関してのみ SSD に格納する MFP も存在する。いずれにしても、SSD に保護資産が格納される以上、SSD の暗号化やデータ削除といった対策が必要となる。

7.4.1　【SSD の特徴】

説明のため、本書では SSD の用語を図 7-2 論理ブロックと物理ブロックの関係図の通り定義する。

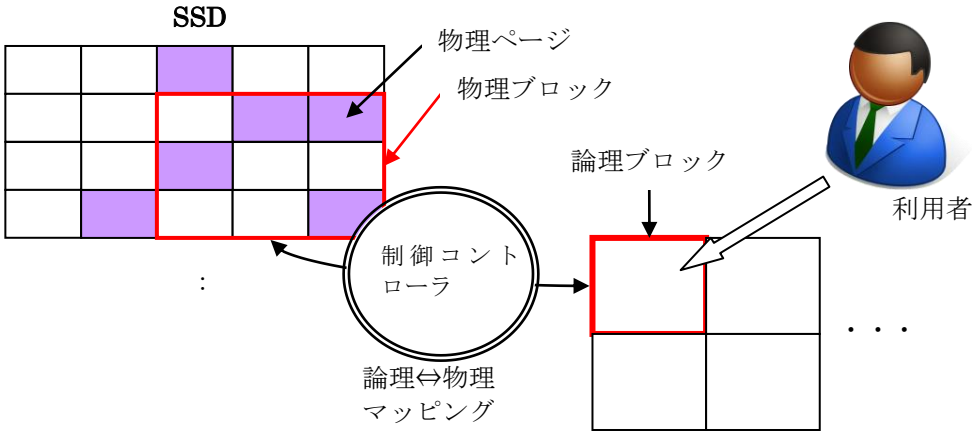


図 7-2 論理ブロックと物理ブロックの関係図

SSD は記憶領域がブロック／ページ単位で別れており、利用者がアクセスする論理ブロックと、物理ブロックは制御コントローラによって対応付けられている。そのため利用者は物理領域を意識することはできず、任意の物理領域へアクセスすることはできない。またその対応付けは物理領域の状況により変化する。これは、SSD の欠点である書き換え可能回数の上限に一部のブロック／ページのみが到達するのを防止するためで、ウェアレベリング機能と呼ばれている。実際、SSD は書き換え可能回数が SLC チップで 10 万回､MLC チップで 1 万回と制限がある。

もし、SSD の持ち去りを考慮して、HDD と同様の一時保存データを上書き削除する場合、米国国防総省方式（DoD5220.22-M）方式で 3 回、Gutmann 方式だと 35 回の書込みが行われる。更に、前述したウェアレベリング機能により、任意の物理領域をブロック／ページ単位で上書き削除することは極めて困難である。

7.4.2　【攻撃手法とその対策】

HDD と同等に、運用状態の MFP からの SSD の持ち出しと、使用済み MFP の廃

棄時、返却時の SSD の持ち出しが攻撃として考えられる。

まず上述した通り、SSD の特性上、任意の物理ブロック／ページを上書き削除する機能を実装することは困難であり、一時保存データの上書き削除機能は実装していない可能性が高い。一方、MFP に内蔵されている SSD は、目視で識別可能であり、標準的なコネクタで接続されていることが一部の MFP で確認された。この場合 MFP 本体へのアクセスが可能であれば、SSD を持ち出すことが可能と言える。そのため、SSD の持ち出しによる情報漏えいを防止する対策としては、SSD 上のデータを暗号化することが有効である。

次に、MFP の廃棄時、返却時以降の保護資産の漏洩に関しては、暗号化に加え、全領域上書き削除機能を実装することも有効である。SSD は任意の物理領域へのアクセスは出来ないが、SSD の制御コントローラには SSD の全ての物理領域の電荷を放出（リセット）し、工場出荷状態に戻す機能が実装されているため、ウェアレベリング機能の影響を受けることなく、全領域の削除を実装することが可能である。

但し、一部の SSD では、制御コントローラに電荷を放出（リセット）する機能が誤って実装されていることが報告されている[24]。MFP ベンダが全領域の削除機能を実装する場合は、適切な SSD の選定も考慮しなければならない。

以上より、MFP が機能的に実装可能な対策としては SSD の暗号化と MFP の廃棄時、返却時の物理領域のリセットが有効と考えられる。

補足：攻撃者の観点

SSD の任意の物理ブロック／ページにアクセスできないという特性は、攻撃者にとっても、SSD に格納されたデータへの攻撃を困難にしている。上書き削除等の技術を用いず論理的に削除された一部のデータ（物理的にはページにデータが残っているが、制御コントローラ経由では見えない余剰ブロック上のデータ）を、制御コントローラを迂回して物理的なページ／ブロックへアクセスして、余剰ブロックからデータを復元するには、高い技術力が必要だと言われている。

7.4.3 【考察】

MFP に SSD を搭載した目的の一つは、保護資産を含むデータへのアクセス速度の向上である。この目的を重視する場合、攻撃に対抗できる有効な手段である暗号化を実装しないケースが考えられる。論理的なデータの削除により残存している余剰ブロック上のデータに関しては、攻撃には高い技術が必要だと言われているため、問題は発生しないかもしれない。しかし論理的に対応付けられているブロック上のデータや、削除されていない SSD 上のデータに関しては HDD 上のデータと同様にアクセスできる。保護資産を SSD に保存する仕様の場合、MFP ベンダの開発者は、SSD へデータを格納する際には暗号化機能を利用する必要がある。

[24] 2011 年 2 月に行われた 9th USENIX Conference on File and Storage Technologies でカリフォルニア大サンディエゴ校のチームが発表した。

7.4.4　対策

【運用ガイド】

1)　SSD に保護資産を格納する場合、暗号化機能を有効にする。もしくは機能を実装した MFP を選択する。
2)　SSD に保護資産を格納する場合、廃棄／返却時に全領域削除する機能を有効にする。もしくは機能を実装した MFP を選択する。
3)　暗号化に用いる暗号アルゴリズムや鍵の安全性がどのように担保されているかを確認する。

【開発ガイド】

4)　SSD と HDD を併用している場合、SSD には秘密情報を格納しない仕様とする。
5)　SSD に暗号化機能を実装する。
6)　SSD に全領域削除機能を実装する。
7)　全領域削除機能が正しく実装された SSD を選定する。
8)　安全性が担保できるような暗号化の仕組みを実装（選定）する。

※4)の対策が取られていれば、他の対策は必要ではない。

【検査ガイド】

9)　SSD の特性を理解し、SSD の特性に応じた検査を行う。また余剰ブロックへの攻撃可能性に関しては常に最新情報を基にレーティングし、攻撃可能な場合 MFP が実装している機能で対抗できることを実証する。

7.4.5　参考情報

公開年月	情報源
2011 年 2 月	Reliably Erasing Data From Flash-Based Solid State Drives http://static.usenix.org/events/fast11/tech/full_papers/Wei.pdf リセット機能が誤って実装されている SSD に関する報告
2011 年某月	NPO デジタル・フォレンジック研究会コラム http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=399&continue=on フラッシュメモリのフォレンジックに関する記事
2011 年 7 月	ITmedia エンタープライズ記事 http://www.itmedia.co.jp/enterprise/articles/1107/16/news001.html SSD 上のデータ保護手段の記事
不明	インテル SSD オプティマイザーサイト http://www.intel.com/jp/consumer/Shop/diy/features/ssd/optimizer/p1.htm SSD の特徴についての記事

7.4.6　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは、運用状態の MFP に内蔵された SSD 上の保護資産へアクセスする攻撃を考察する。HDD への攻撃と同様に MFP から持ち出した場合を想定する。但し、SSD の特性から、余剰ブロックにあり論理的に対応付けられていない保護資産と、それ以外の保護資産では、スコアリングは大きく異なる。(一方 HDD の場合はどちらの保護資産に関してもスコアリングは同値である。) 本節では SSD の特性を考慮し機密性の影響範囲を部分的としている。

・攻撃対象と同型の MFP を所有していること。
・MFP に物理的にアクセス可能であること。
・SSD に暗号化機能が実装されていないこと。

【スコアリング】

CVSS 2.0 ベース 基本値：　5.4（警告）

攻撃元区分	ローカルでのみ攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	影響なし
可用性	全面的な影響

7.5 ローカルな保守インタフェースへのアクセスによる問題

MFP には利用者がアクセスできるインタフェース（一般利用者、管理者等）以外に、保守用のインタフェースが存在する。保守インタフェースは、MFP 本体の前に保守員が立って直接操作を行うローカルな保守インタフェースと、遠隔から http や別のプロトコルを利用して操作する遠隔保守インタフェースに大別される。本節では、ローカルな保守インタフェースに関する脆弱性について近年の公開されている情報を踏まえて考察する。[25]

7.5.1 【ローカルな保守インタフェースの機能】

ローカルな保守インタフェースから操作可能な主な機能は以下である。
・トナーやカウンターの確認／リセット
・MFP 機能の設定（制限）／初期化
・管理者パスワードの設定／初期化
・MFP の機能、動作に関する微調整

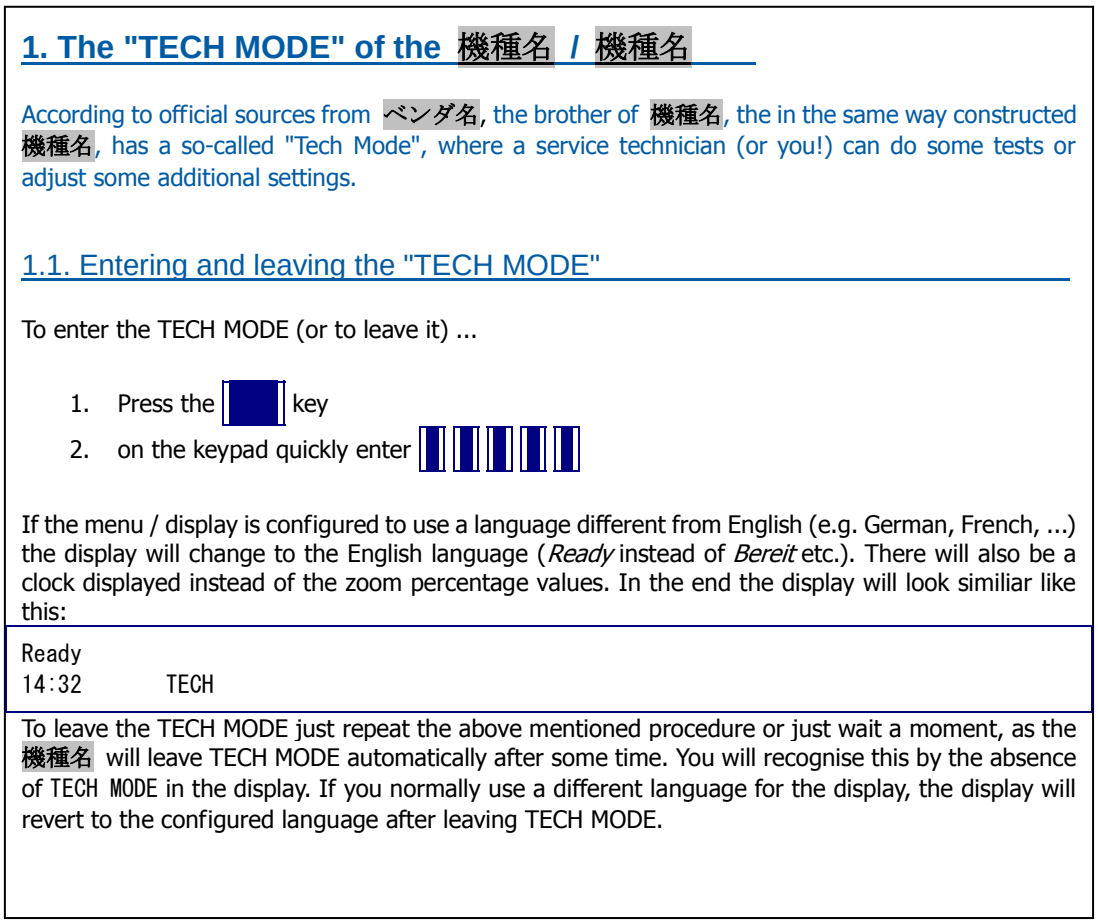
これら保守インタフェースから操作できる機能を悪用すれば、保守員でなくとも管理者の設定を初期化し、管理者として利用者の認証データを変更することで保護資産を閲覧・操作することが可能である。またオフィスで MFP をリース／レンタルし料金を課金している場合に、カウンターを改変して課金情報を偽ることも可能である。このため多くの MFP では、ローカルな保守インタフェースは、秘匿された特殊な操作と強固なパスワードによる認証、もしくはそのいずれかの手段により保護されている。

7.5.2 【攻撃手法とその影響】

一部の MFP は、ローカルな保守インタフェースの保護手段として、秘匿された特殊な操作を採用している。その操作手順は、対応する保守員のコストを考慮すると、MFP 個体毎に異なる手順になっているとは考えにくく、ベンダの製品種別や型番毎に同じ特定の手順が適用されている場合もありうる。この場合、その操作手順が漏洩しないことが大前提となる。

しかし、実際は、一部の MFP の保守インタフェースへアクセスするための特殊な操作手順（MFP の操作パネルによるキー操作等）が海外のＱ＆Ａサイト等で公開されており、その公開されている手順により実際の MFP の保守インタフェースにアクセスすることが可能である。つまり、この手順が公開された時点から、特定の操作手順による保護は何の対抗策にもなっていないことになる。また MFP に接触できる攻撃者がこれらの公開情報を利用した場合、攻撃は極めて容易である。

[25] 保守インタフェースのファームウェアアップデート機能を悪用した攻撃に関しては 7.7 節、http プロトコルを使ったウェブベースの保守インタフェースに関しては 7.16 節で解説する。



1. The "TECH MODE" of the 機種名 / 機種名

According to official sources from ベンダ名, the brother of 機種名, the in the same way constructed 機種名, has a so-called "Tech Mode", where a service technician (or you!) can do some tests or adjust some additional settings.

1.1. Entering and leaving the "TECH MODE"

To enter the TECH MODE (or to leave it) ...

1. Press the [redacted] key
2. on the keypad quickly enter [redacted]

If the menu / display is configured to use a language different from English (e.g. German, French, ...) the display will change to the English language (*Ready* instead of *Bereit* etc.). There will also be a clock displayed instead of the zoom percentage values. In the end the display will look similiar like this:

Ready
14:32　　TECH

To leave the TECH MODE just repeat the above mentioned procedure or just wait a moment, as the 機種名 will leave TECH MODE automatically after some time. You will recognise this by the absence of TECH MODE in the display. If you normally use a different language for the display, the display will revert to the configured language after leaving TECH MODE.

図 7-3 公開されている保守モードに入るための操作

7.5.3 【原因と考察】

本節で考察した攻撃の直接的な原因は保守インタフェースへアクセスする手順がサイトに公開されたことにある。しかし根本的には管理者権限をも操作できる保守インタフェースの保護手段が「固定のキー操作」に頼っている実装に問題があると考える。保守インタフェースに関しては、最低でも管理者や利用者と同等のパスワードによる保護が必要である。

しかし、その場合でも、一人の保守員が担当する無数の MFP が全て異なるパスワードで管理されているとは一般的に考えにくい。ある程度の台数の MFP が同一のパスワードにより管理され、かつパスワードを更新しない場合、上記の特殊な手順と同様、そのパスワードが公開されれば極めて脆弱な状態となる。実際に調査したところ、パスワードと考えられる入力情報が公開されているケースが確認された。

これらの脆弱性に対抗するためには、MFP 個体毎に保守インタフェースへアクセスするパスワードを異なるものとすることが理想的な運用方法である。また、MFP を利用する管理者や利用者以上に強固なパスワードで保護することが望ましい。ある程度の台数の MFP で同一もしくは規則的なパスワードを使用する場合は、特殊な操作手順やパスワードを知りえる人（保守員など）を特定し、永続的に有効となる守秘義務契約や教育による周知徹底等、万全な管理が必要となる。その

他、MFP に物理的にアクセスできる人を、コントロール可能な要員のみに制限することが、外部攻撃者による保護資産の漏洩や改ざんへの一般的な対策として想定される。しかし、アクセス制限を設けた場合においても、MFP に物理的にアクセス可能な正当な利用者による攻撃は防ぐことができない。

補足：初期パスワードの検討

7.6 節では、本節の脆弱性の攻撃手段と類似した工場出荷状態へ戻すことによる脆弱性を解説している。この脆弱性を利用することにより、保守インタフェースのパスワードが保護された状態であっても、公知の固定の初期パスワードに戻されるかもしれない。

補足：隠しインタフェース

本節で解説した保守インタフェース以外に、存在自体が秘匿されている「隠しインタフェース」があるかもしれない。例えば、デバッグや障害対応のために設けられた組込み OS への特定のアクセス方法や、メモリの内容を確認する機能を提供するものが考えられる。アクセス手法としては保守員も知らないような特殊な操作や、MFP 内部に設置された特殊なコネクタへの接続が必要となるかもしれない。これら開発者の一部しか知らない特殊なインタフェースは、本節で解説した保守インタフェースに比べれば、その存在やアクセス手順が公開されるリスクは低いかもしれない。それでも開発者はこれらのインタフェースに関して、漏洩を含めた脅威を想定して、保守インタフェースと同様に保護しなければならない。[26]

7.5.4　対策

【運用ガイド】

1)　保護資産を扱う MFP は、保守インタフェースがどのような仕組みで保護されているかを MFP 選定時に確認する。

【開発ガイド】

2)　保守インタフェースの認証強度を、管理者や利用者への認証強度以上とする。
3)　隠しインタフェースに関しても脅威を想定し、保護する。
4)　保守インタフェースや隠しインタフェースに対して、複数の製品で同じ操作やパスワードを用いない仕組みを実装する。

【検査ガイド】

5)　インタフェースの存在や、操作手順が秘匿されていることをセキュリティの根拠としない。
6)　保守インタフェースの認証強度が十分であることを確認する。その際、パスワードの一意性や、予測可能性も考慮する。

7.5.5　参考情報

※本節では情報の悪用を考慮し、割愛する。

[26] また、例外発生時にデバッグ画面が利用者インタフェースに表示されるような実装は、フェールセキュアの考えから行ってはならない。

7.5.6　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ローカルな保守インタフェースへのアクセス手順を利用して利用者が攻撃した場合（他の利用者や管理者の保護資産を入手する、あるいは課金に関するカウンターを改ざんする等）を想定する。

・上記開発ガイドの対策を講じていない機種であること。
・保守インタフェースへアクセスする手順が公開されていること。

【スコアリング】

CVSS 2.0 ベース 基本値：　7.2（危険）

攻撃元区分	ローカルでのみ攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.6　工場出荷時の設定に戻されることによる問題

本書で前提としているような保護資産を扱う MFP 製品であっても、工場出荷時の状態は利便性が優先される傾向があり、保護資産のセキュリティを考慮した設定にはなっていない場合がある。ここでの利便性とは、7.11 節で述べる通信プロトコルが必要最小限のものに制限されていない状態、あるいは管理者や利用者向けの強固なパスワードも設定されていない状態等のことである。また、工場出荷時は、保守インタフェースにアクセスするためのパスワード設定も初期化された状態かもしれない。

7.6.1　【攻撃手法とその影響】

工場出荷時の状態に戻すことにより、MFP の設定を改ざんする攻撃について考察する。保護資産の機密性や完全性に対する攻撃として、以下のシナリオが考えられる。

1) MFP の基本設定情報や登録されているユーザ ID 等を把握する
2) MFP を工場出荷時の設定に戻す
3) 管理者になりすまして、基本設定情報を設定し直し、ユーザ作成を行う
4) その後、MFP に格納される各利用者の保護資産を入手する

上記手順 1)の基本設定情報とは、MFP に割り当てた IP アドレスなど、通常、利用者が知りえる情報である。また、ユーザ ID 等は攻撃者となる利用者自身がどのようなユーザ ID で MFP に登録されているかを確認すれば他の利用者のユーザ ID 等は想定できる情報である。機密性や完全性以外にも、設定を工場出荷時の状態に戻された時点で、保護資産の可用性は失われる。

以上から、工場出荷時の状態がセキュアでは無い MFP に関しては、利用者が任意に工場出荷時の状態に戻すことができないことが求められる。つまり、工場出荷時の状態に戻す手順を保護する仕組みは、管理者や利用者の認証、及び保守インタフェースへアクセスする仕組みと同等かそれ以上に強固でなければならない。

しかし実際には、一部の MFP において、工場出荷時の状態に戻す仕組みが特殊な操作手順により利用者でも可能な場合がある。たとえば、図 7-4 のような情報が公開されている。

You can also reset the NVRAM. Resetting the NVRAM will clear the page count and reset the service mode settings to factory defaults. On printers with a display panel you need to enter service mode to manually change the information stored in NVRAM. On printers that don't have a display panel, such as a 機種名 there is a different procedure outlined below.

"Older" printers with a display panel. (e.g.機種名, etc.)

Cold resetting the printer is simply a matter of [redacted], holding down the [redacted] while turning the printer on.
Resetting NVRAM settings must be done manually through service mode. See entering service mode.

"Newer" printers with a display panel. (e.g. 機種名 etc.)

Turn the printer off and then on. When the printer begins its memory count, press and hold down the [redacted] and [redacted]. Then release the [redacted], and use the [redacted] to find the Cold Reset option, then press the [redacted] to choose that option.

図 7-4 公開されている工場出荷状態に戻す操作（海外 MFP 製品）

7.6.2 【原因と考察】

このようなケースでは、秘匿すべき手順が公開されているものの、工場出荷時の設定に戻す機能をメンテナンス機能の一つとして位置付けており、その影響は設定や保護資産がクリアされるのみであるため、情報漏洩につながる攻撃手段とは捉えられていないことが考えられる。しかし実際は上述したように、ひとたび攻撃されれば、それ以降 MFP に保存される保護資産は攻撃者に晒されることになるなど、そのリスクは看過できないものとなる。

この脆弱性への一般的な対策は、保守インタフェースと同様に強固な認証や使用制限により、利用者や第三者の手により工場出荷時の設定に戻すことができないようにすることである。たとえば、保守インタフェースから接続した後のメニューにのみ、工場出荷時の状態に戻す機能を配置することで、この対策は容易に実現できるであろう。但し、保守インタフェースが強固に保護されていることが前提である。

工場出荷状態に戻された際の影響を少なくする対策としては、工場出荷状態をセキュアな状態とすることが考えられる。これはデフォルトセキュアという考え方であり、初期状態では必要最小限のサービスしか動作させず、それらのサービスもセキュアに動作する範囲に使用を制限した状態とする。必要に応じて利用するサービスを動作させるなど、運用側のリスクマネジメントに委ねて設定を広げていく考え方である。この考え方は、MFP 設置時に万が一設定漏れがあっても、セキュアな側に倒れるという利点もある。

補足：状態の表示

セキュアな環境で利用されることを想定した MFP は、デフォルトセキュアであることが望ましい。しかし、一部の MFP 製品はセキュアな環境での使用だけではなく、利用者の利便性を考えて一般的なサービスを活性化させた設定で出荷されることを想定した製品があるかもしれない。そのような MFP 製品は、MFP がセキュアな状態に設定されているか否かを利用者が一目で識別できる機能が実装されていることが望ましい。また、デフォルトセキュアであるか否かに関わらず、工場出荷状態に戻った場合など MFP のその時点の設定のステータスを管理者が識別

できる機能が実装されていることが望ましい。

7.6.3　対策

【運用ガイド】

1) 保護資産を扱うMFPは、工場出荷時の設定に戻す機能がどのように実装されているかを MFP 選定時に確認する。
2) MFP がセキュアな設定状態になっていることを確認して利用する。

【開発ガイド】

3) 工場出荷時の設定に戻す機能を、保守機能のメニュー内に配置し、独自の強固な認証の仕組みを設ける。
4) 独自の認証の仕組みを設ける場合、複数の製品で同じ操作やパスワードを用いない仕組みを実装する。
5) 設定によりセキュアでない状態となり得る MFP の場合、MFP が現在セキュアな状態かどうかを利用者が識別できる仕組みを実装する。
6) セキュリティを意識した環境での利用を想定した MFP 製品に対してはデフォルトセキュアの考え方を適用する。

【検査ガイド】

7) 工場出荷時の設定に戻す機能を実行するまでの認証強度が十分であることを確認する。その際、パスワードの一意性や、予測可能性も考慮する。
8) MFP がセキュアな状態かどうかのインジケータと、実際の MFP の状態が食い違うことがないか、セキュアな状態に影響する全ての設定項目を操作し検査する。

7.6.4　参考情報

※本節では情報の悪用を考慮し、割愛する。

7.6.5　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは本節の攻撃手法で解説した通り、MFP の操作パネルから工場出荷時の状態に戻した後､利用者の環境に併せて攻撃者が MFP の再設定を行うことにより、再設定後の MFP に格納される保護資産へ不正なアクセスを行う攻撃について考慮する。

・上記開発ガイドの対策を講じていない機種であること。

【スコアリング】

CVSS 2.0 ベース 基本値：　5.9（警告）

攻撃元区分	ローカルでのみ攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	部分的な影響
可用性	全面的な影響

7.7　ファームウェアアップデート機能の悪用による問題

イントラネットや外部からのネットワーク経由で保守機能を提供する保守インタフェースを持つ MFP は、その保守機能の一環として、ファームウェアアップデート機能を有する場合が多い。このファームウェアアップデート機能を用いて、不正なファームウェアをアップデートし、そのファームウェアを動作させることで MFP の不正な動作を誘発させることや、保護資産へアクセスすることができる。

2011 年 11 月、コロンビア大学の教授らにより、このファームウェアアップデート機能を悪用して不正なプログラムを動作させることにより、MFP の定着ローラーを過熱させることが可能であることを実証した記事が公開された。そこで紹介されている記事を元に詳細な攻撃手段を以下に解説する。

7.7.1　【攻撃手法とその影響】

Step.1　ファームウェアアップデート方法の確認

ファームウェアアップデートの手順は、ベンダ及び MFP の機種などにより異なるが、一部の MFP のファームウェアアップデートの方法は公開されている。そのため、その手順に従えば簡単にファームウェアアップデートを行うことができる。例えば「remote firmware update LPR command」といったキーワードで検索すると、LPR を使ったファームウェアアップデートの手順が検索できる。

Remote firmware update by using the LPR command

NOTE:　This remote firmware update method is for use in Windows 2000 Service Pack 3, Windows XP, Windows Server 2003, and Windows Server 2008.

Complete the following steps to update the firmware by using the LPR command.

1. From a command window, type the following:
   lpr -P -S -o l
   OR
   lpr -S -Pbinps
   where IPADDRESS can be either the TCP/IP address or the hostname of the product, and where FILENAME is the filename of the .RFU file.
   NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not the numeral 1. This parameter sets the transport protocol to binary mode.
2. Press Enter on the keyboard. The messages described in the section Printer messages during the firmware update appear on the control panel.
3. The download process begins and the firmware is updated on the product. This can take several minutes.

図 7-5 LPR を使ったファームウェアアップデート手順の抜粋

Step.2　正規のファームウェアの確認

まず正規のファームウェアを準備する。上記で検索したページからのリンクや、「[ベンダ名] [機種名] firmware download」といったキーワードで、攻撃対象の機器に適した正規のファームウェアの入手を試みる。

ファームウェアが入手できたら、ファームウェアのバイナリデータを改変し、不正なファームウェアを生成する。

例えば、後述の「7.7.4　参考情報：PRINT ME IF YOU DARE ?Firmware update attack and the rise of printer malware-」ではファームウェアのバイナリ情報が紹介されており、それが PJL コマンドの列記であり、意味を読み取ることが出来る。「@PJL

UPGRADE SIZE=792990」という記述からファームウェアは 7M のデータであることがわかり、「@PJL ENTER LANGUAGE=ACL<CR><LF>」の後ろに実際のファームウェアのデータが記述されている。ACL とは Advanced control language の略で、MFP のファームウェア記述に用いられる言語である。ここで重要なのはファームウェア部分が暗号化されておらず、圧縮されているにすぎないことである。これは構文を理解していれば、ファームウェアが作成できるということを表している。

Step.3　MFP 側のファームウェア検証機能の確認

現在の MFP の大半は、電子署名という暗号技術を用いてファイルの正当性を検証する機能を有している。電子署名を用いた検証では、秘密鍵、及びファームウェアのハッシュ値から署名を生成し、MFP へアップロードされたファームウェアのハッシュ値と、その署名から生成したハッシュ値が同一であることを確認する。そのため、デジタル署名の持つハッシュ値が衝突しないという特性から、秘密鍵を知らない攻撃者が不正なファームウェアを生成した場合、検証を通るような電子署名を生成することができない。

しかし、一部の MFP では暗号技術を用いておらず、CRC チェック等による検証のみを行っている場合がある。実際に以下の情報が 2012 年 5 月時点で、ガイダンスとして公開されている。Firmware 不整合に関する他の記述が見当たらないため、この機種では、ファームウェアファイルは CRC チェックをクリアすれば、アップロードできることがわかる。

Control panel message	Description	Recommended action
CODE CRC ERROR	An error has occurred during a firmware upgrade.	1. Reinstall the firmware. 2. If the problem persists, contact **ベンダ名** Support.

図 7-6 ファームウェア検証方法の公開情報

Step.4 不正なファームウェアの確認

Step.3 までで、MFP に正規なファームウェアと詐称して任意のファームウェアをアップロードさせる手段を確認した。後は、任意のコードを組み込んだファームウェアを作成すれば、一部の MFP の保守インタフェースを利用して、結果的に MFP の不正な動作の誘発や保護資産へのアクセスが可能となる。記事では、構文の理解のために別ハードウェアを組み立ててバイナリのリバースエンジニアリングを行い、攻撃に成功している。つまり解析には標的となる MFP を解析するためのハードウェアやデバッグ環境を構築するためのコストに加え、電気回路やリバースエンジニアリングといった複数の技術が必要となると推測される。しかし、誰かが特定の MFP の不正なファームウェアを公開すれば、それを利用した攻撃が可能といえる。

なお記事には不正なファームにより、MFP の定着ローラーを加熱し続けることもできると記載されている。

補足：開発者の見解

上記の報告を受けてこの問題を指摘された MFP ベンダは、定着ローラーの過熱を防ぐよう設計されたサーマルブレーカーがあるので、問題とならないと自社のホームページ 上で発表している。しかし、不正なファームウェアの書き換えに関

しては否定しておらず、ファイアウォールの無い外部ネットワークに MFP が接続されていない限り問題ないとコメントしている。これは、攻撃者の存在する内部ネットワークからの攻撃には、当該脆弱性が影響することが認められる可能性を否定するものではない。

また、ファームウェアの書き換えに必要な全てのポートが開いているとは限らないが、2012 年 5 月現在、SHODAN や Google 検索を用いると、多数の MFP のウェブインタフェースが公開されており、外部からアクセス可能であることを確認している。

7.7.2 【原因と考察】

当該 MFP の問題点は、不正なファームウェアをアップロードできてしまう点である。その原因は、保守インタフェース機能を利用したファームウェアアップロード機能において、ファームウェアデータの CRC による完全性のチェックしか行わないこと、及びアップデートするファームウェアのバイナリが暗号化されていないことによる。補足に記述したベンダのコメント通り、保守インタフェースが外部からは接続できない内部ネットワークからのアクセスを想定しており、さらに内部ネットワークの利用者が全て信頼できるという前提があればここで解説した実装でも問題無いかもしれない。しかし、実際の利用場面を想定すると、保守インタフェースは外部からの接続（Ethernet 経由以外にも、電話回線、WebDAV サーバを介した接続など）を考慮し、外部からの攻撃に対して強固であることが望ましい。なお、アップデートするファームウェアの暗号化を適用する場合は 7.3.3 節で解説したような暗号アルゴリズムや鍵管理に関しても考慮する必要がある。

7.7.3　対策

【運用ガイド】

1)　必要が無ければネットワーク経由の保守インタフェースを停止する。
2)　アップデートするファームウェアバイナリデータに対して強固な正当性検証機能（電子署名など）がある MFP を利用する。
3)　アップデートするファームウェアバイナリデータに対して安全なアルゴリズムによる暗号化機能がある MFP を利用する。

※ネットワーク経由の保守インタフェースを停止することは解決策として効果的ではあるが、本来の目的である利便性を損なう。ファームウェアバイナリデータの暗号化や電子署名等による検証機能を実装した機器の選定が現実的な対応といえる。暗号化もしくは強固な正当性検証はどちらか一方が実装されていることを選定の条件とすることが望ましい。

【開発ガイド】

4)　アップデートするファームウェアバイナリデータに対して強固な正当性検証機能（電子署名など）を提供する。
5)　アップデートするファームウェアバイナリデータに対して安全なアルゴリズムによる暗号化機能を提供する。（暗号に利用する秘密鍵も安全に管理する。）

※MFP の可用性を考慮すると、強固な正当性検証を実装することが望ましい。

【検査ガイド】

6)　ファームウェアバイナリデータの正当性検証機能が、想定する攻撃者レベルで悪用できない仕組みであることを確認する。
7)　ファームウェアバイナリデータの暗号化機能が、安全な仕様でありかつ正しく実装されていること、及び当該暗号化機能の運用が安全な手順であることを、仕様・設計、開発環境、及び配付・設置（アップデート手続きを含む）における安全性の観点から確認する。（秘密鍵が漏洩しないことも確認する必要がある。）

7.7.4　参考情報

公開年月	情報源
2011 年 11 月	Exclusive: Millions of printers open to devastating hack attack, researchers say http://redtape.msnbc.msn.com/_news/2011/11/29/9076395-exclusive-millions-of-printers-open-to-__devastating-hack-attack-researchers-say コロンビア大学の教授らが発表した MFP の保守インタフェースを利用した脆弱性に関する記事
2011 年 12 月	CVE-2011-4161 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4161 HP 社一部 MFP のファームウェアアップデート機能に関する脆弱性情報
2011 年 12 月	PRINT ME IF YOU DARE –Firmware update attack and the rise of printer malware- http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf コロンビア大学の教授らが発表した攻撃手順が記載された資料

7.7.5　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは攻撃区分として隣接ネットワークからの攻撃に限定している。セキュリティを意識した設置環境の場合、機能的にファクス回線を用いたアップデート機能は停止されており、ファイアウォールなどにより外部からの通信が制御されていると仮定する。また、以下を前提とする。

・ファームウェアアップデート機能は認証無しでアクセスできること。
・上記開発ガイドの対策を講じていない機種であること。

【スコアリング】

CVSS 2.0 ベース 基本値：　7.9（危険）　※不正なファームウェアが公開された場合、8.3（危険）となる

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.8 組込み OS の脆弱性による問題

近年オープンソースの組込み Linux（MontaVista, Wind River, Timesys, Denx 等）を、OS そのものの価格面と、オープンソースによる開発や機能追加の利便性から選択する MFP ベンダも少なくない。しかしその一方で多機能な組込み OS の採用がセキュリティ的な欠陥を MFP に埋め込む原因となる場合がある。具体的には distcc を使った PC 上でクロスコンパイラによる開発の結果、開発言語の関数が持つバッファオーバーフローなどの脆弱性が引き継がれる危険性や、デフォルトで組み込まれている遠隔操作のサービス（NFS、Tftpboot、Gdbserver 等）の悪用、組込み Linux 自体や搭載されている各種アプリケーションの脆弱性を突いた攻撃により、保護資産の漏洩や改竄が行われる可能性や、サービス不能攻撃により MFP が適切に動作しなくなる可能性がある。

ここでは、組込み Linux 自体や搭載されている各種アプリケーションに存在する脆弱性によるリスクやデフォルト設定状態で利用することの問題点についてとりあげる。

7.8.1 【攻撃手法とその影響】

参考情報に記載のとおり、MontaVista 社は提供する製品に関する脆弱性情報をウェブサイトにて広く公開している。この脆弱性情報を参照すると、MontaVista Linux（Carrier Grade Edition は除く。）に関する脆弱性は 2012 年 10 月時点では以下の 4 件が報告されている。

表 7-1 組込み Linux に存在する脆弱性の例

CVE	説明[27]
CVE-2012-1165 (JVNDB-2012-001801)	OpenSSL の crypto/asn1/asn_mime.c にある mime_param_cmp 関数には、サービス運用妨害（NULL ポインタデリファレンス及びアプリケーションクラッシュ）状態となる脆弱性が存在する。
CVE-2012-0884 (JVNDB-2012-001735)	OpenSSL の Cryptographic Message Syntax（CMS）及び PKCS #7 の実装は、特定の動作を適切に制限しないため、容易にデータを復号化される脆弱性が存在する。
CVE-2012-0814 (JVNDB-2012-001739)	OpenSSH 内の sshd にある auth-options.c の auth_parse_options 関数は、authorized_keys コマンドオプションを含んだデバッグメッセージを出力するため、重要な情報を取得される脆弱性が存在する。
CVE-2012-0021 (JVNDB-2011-003659)	Apache HTTP Server の mod_log_config モジュールにある mod_log_config.c 内の log_cookie 関数は、スレッド化された MPM が使用されている際、%{}C 形式の文字列を適切に処理しないため、サービス運用妨害（デーモンクラッシュ）状態となる脆弱性が存在する。

上記の CVE-2012-1165 及び CVE-2012-0884 は、組込み Linux（MontaVista Linux）と一体となって提供されている（サポートされている）OpenSSL の実装に係る脆

[27] JVN iPedia（http://jvndb.jvn.jp）より当該脆弱性情報を抜粋。

弱性である。本組込み Linux を採用した MFP において上記脆弱性を放置したまま利用していた場合は、サービス不能攻撃や MFP とクライアント端末間における通信データの盗聴等が行われる可能性がある。

また、Wind River Linux においては、主に Linux カーネルの脆弱性に起因する脆弱性が、バージョン 3.1 においては 5 件、バージョン 3.0 においては 4 件存在することが SecurityFocus を参照することにより確認することが可能である。(詳細は参考情報に解説されている。) これらの脆弱性を悪用することで、保護資産への不正アクセスが行わる可能性や、サービス不能攻撃により MFP が適切に動作しなくなる可能性がある。

上記のような組込み Linux の脆弱性に起因するリスクの他に、セキュリティ設定等を意識せずにデフォルト設定状態で組込み Linux を利用していた場合は、MFP で本来不要なネットワークサービスが稼動している可能性がある。これら不要なネットワークサービスの実装に脆弱性が存在する場合や識別認証や暗号化等の適切なセキュリティ設定が行われていない場合は、保護資産への不正アクセスによる漏洩・改竄等、様々な情報セキュリティ上のリスクが発生する可能性がある。

さらに、MFP 起動時に、パネル上に OS 等の情報が表示される機種が存在することが確認されている。これらの情報（バナー情報）を悪用された場合、当該 OS の脆弱性を突いた攻撃等が行われることにより保護資産への不正アクセスや情報漏洩等が発生する可能性がある。

7.8.2 【原因と考察】

近年、組込み Linux は、コストやオープンソースのメリットである開発の利便性等の理由により、数多くの MFP において採用されている。これらのメリットがある一方で、組込み Linux 及びその上で稼動するアプリケーションの脆弱性や不要なサービスを攻撃者が悪用することにより、MFP 内に格納された保護資産への不正アクセスによる漏洩・改竄等、様々な情報セキュリティ上のリスクが発生する可能性がある。

上記リスクへ対応するには、開発者は採用した組込み OS（Linux）の脆弱性情報に注意して必要に応じて適宜セキュリティパッチを適用する（もしくは、利用者に通知・配布する）等の対応を行う必要がある。また、不要なサービスが稼動している可能性があるため、一般的な Linux サーバ等と同様に、製品リリース前にはポートスキャナや脆弱性スキャナ等でサービス稼動状態や実装上の脆弱性の有無を確認することが望まれる。

7.8.3　対策

【運用ガイド】

1) MFP に導入されている組込み OS 及びアプリケーションの脆弱性情報及びセキュリティパッチ等の適用方法について、MFP 提供ベンダに確認する。

【開発ガイド】

2) クロスコンパイル環境において言語自体の脆弱性（バッファオーバーフロー等）を持ち込まないコーディング規定を徹底する。
3) 組込み OS 及びその上で稼動するアプリケーションの脆弱性について確認し、必要に応じてセキュリティパッチの適用や脆弱性対策機能を実装する。
4) 不要なサービスや、脆弱性が公開されているサービスが稼動していないことをシステム設定情報、ポートスキャナや脆弱性スキャナ等で確認し、必要に応じてサービスの停止もしくは削除を行う。
5) OS や稼動するアプリケーション（モジュール）のバージョン等のバナー情報が不必要に提示されないように実装する。
6) 脆弱性情報やセキュリティパッチ等の適用方法について、利用者にガイドライン等で明示的に説明する。

【検査ガイド】

7) 組込み OS 及びその上で稼動するアプリケーションの脆弱性の有無とその実行可否について検証する。
8) 不要なサービスや、脆弱性が公開されているサービスが稼動していないことをシステム設定情報、ポートスキャナや脆弱性スキャナ等で検証する。
9) 利用者ガイドライン等に脆弱性情報の通知方法、セキュリティパッチの適用方法等が明記されていることを確認する。

7.8.4　参考情報

公開年月	情報源
随時更新	CVE Vulnerabilities List（MontaVista） http://www.mvista.com/cve_vulnerabilities.php MontaVista 社が提供する製品の脆弱性情報（CVE）が広く公開されている
随時更新	SecurityFocus http://www.securityfocus.com/ 様々なベンダが提供する製品の脆弱性情報が公開されているウェブサイト
2009 年 12 月	Linux e1000 Driver 'Jumbo Frame' Handling Remote Security Bypass Vulnerability http://www.securityfocus.com/bid/37519 Wind River Linux に関する脆弱性の例（セキュリティ機能の迂回）
2010 年 3 月	Linux Kernel Bluetooth Sysfs File Local Privilege Escalation Vulnerability http://www.securityfocus.com/bid/38898 Wind River Linux に関する脆弱性の例（権限昇格、サービス不能攻撃）
2010 年 1 月	Linux Kernel 'ipv6_hop_jumbo()' Remote Denial of Service Vulnerability http://www.securityfocus.com/bid/37810 Wind River Linux に関する脆弱性の例（サービス不能攻撃）

7.8.5　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

組込み Linux にリモート（内部 LAN）から任意のコードが実行可能な脆弱性が存在し、その脆弱性を利用して MFP の OS 管理者コマンドを利用できるシェルが起動できる攻撃ツールが公開されている場合を想定し考察する。

【スコアリング】

CVSS 2.0 ベース 基本値：　8.3（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.9　SDK（Software Development Kit）に関する脆弱性

本節で考察する SDK とは、MFP 本体の機能拡張を目的として MFP に搭載することができるアプリケーションの開発環境である。例えば MFP に付属している操作パネルのユーザインタフェースを、利用者が利用環境に適した使い易い形にカスタマイズすることを目的としている。SDK で準備されている機能はユーザインタフェース以外にも、以下の様なものがある。

・コピー、プリント、及びスキャン
・機器の設定管理、ジョブ管理
・ネットワーク設定
・ファイル／フォルダ（ボックス）操作　等

上記の通り、MFP にデフォルトで組み込まれている利用者向けの機能と同等の機能が SDK で開発されたアプリケーションからも利用できる。これは SDK で開発したアプリケーションから保護資産へアクセスできることを表している。そのため、SDK を使って利用者が開発したアプリケーションには、MFP ベンダの開発者が MFP 本体のセキュリティ機能を低下させないことを確認し、問題ないと判断したアプリケーションのみ、暗号化して電子署名を付加するという手順を取っている。利用者は MFP ベンダの開発者が署名、暗号化したファイルを、MFP にインストールする。その際 MFP 本体では、署名を検証して復号している。

7.9.1　【攻撃手法とその影響】

「標準のローダー」は利用者が開発したアプリケーションのファイルを MFP にアップロードする際に、上記したような MFP ベンダによるファイルへの署名を必要とする。そのため、悪意のあるアプリケーションファイルはアップロードされない。

しかし、2002 年にあるベンダが公開していたローダーは、署名の検証を行わずにアプリケーションをアップロードできる機能を持っていた。その「署名検証の無いローダー」を導入しない限り不正なアプリケーションがアップロードされることはないため、利用者が「署名検証の無いローダー」を導入しない運用にすれば良いと考えられた。しかし攻撃は成立する。

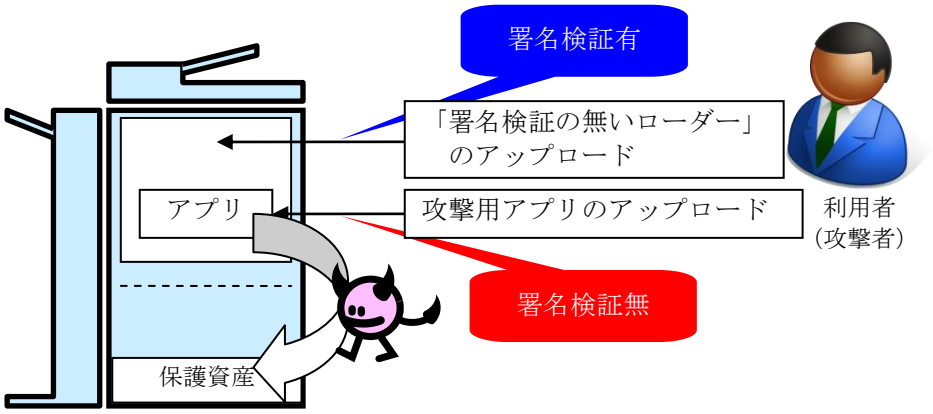


図 7-7 SDK を悪用した不正なアプリケーションインストール

1) まず、「標準のローダー（署名検証の有るローダー）」で、「署名検証の無いのローダー」をアップロードする。
2) 次に「署名検証の無いローダー」の機能を利用して攻撃用アプリをアップロードする。
3) 攻撃用アプリの機能を使い保護資産を攻撃する。

7.9.2 【原因と考察】

攻撃が成功した原因は、「署名検証の無いローダー」は、ベンダが正規に公開したアプリケーションであったこと、つまりベンダが署名したアプリケーションであったことにある。署名されたアプリケーションであるため、「署名検証の無いローダー」を導入しない運用をしていた MFP にも問題なく「署名検証の無いローダー」をアップロードすることができる。あとは「署名検証の無いローダー」の機能で、ファイル操作の命令等が準備されている SDK の仕様に従い、悪意をもって作成したアプリケーションをアップロードしたに過ぎない。

「署名検証の無いローダー」は保護資産を扱わないような MFP 向けに公開されたアプリケーションであったと考える。しかし、結果的にはそのアプリケーションを悪用することにより、「署名されていないアプリケーションはアップロードされない」という保護機能を無効にしてしまったことになる。MFP ベンダの開発者が SDK の保護機能を提供する際には、保護資産を扱わないような環境向けに提供するアプリケーションに関しても、バックドアにならないか否かを統合的に管理する必要がある。

補足：メモリ領域保護の突破

SDK は、他にも Java の Sandbox の様に SDK を利用してアップロードしたアプリケーションがアクセスできるメモリ領域を制限することにより、MFP や保護資産を保護している。しかし、SDK のライブラリや関数が 1 つでもバッファオーバーフローを起こすパラメータを抱えていれば、メモリ領域は突破され、MFP の動作や保護資産は攻撃されてしまう可能性がある。実際 JRE ではこのような SDK 側の関数の不備により発生する脆弱性が報告されている。

補足：利用者が開発したアプリケーションの保護

利用者が作成したアプリケーションを秘匿するための暗号化に関しても考察が

必要となる。MFP の導入環境を考慮すると MFP 単位で暗号化（復号）に用いる鍵が異なることは想定しがたい。作成したアプリケーションを資産として考える場合、利用者は開発者が提供する暗号化の仕組みに関しても確認すると良いかもしれない。

7.9.3　対策

【運用ガイド】

1) SDK の提供している署名や暗号化といった保護機能が、利用者のセキュリティポリシを満たしていることを開発者に確認する。
2) 署名検証機能を有効にして SDK を運用する。（デバッグモードは SDK を開発する環境でのみ利用する。）

【開発ガイド】

3) 署名するアプリケーションの審査基準は、他のセキュリティを意識していないような製品向けのアプリケーションを含めて統一する。
4) SDK 用に提供する全てのライブラリや関数に対してバッファオーバーフローなどを起こさないか検査を行う。

【検査ガイド】

5) SDK を使って不正なアプリケーションアップロードが行えないことを検査する。
6) SDK のメモリ保護機能等にバッファオーバーフローなどの脆弱性が存在しないことを検査する。
7) SDK の提供する機能によって MFP が本来持っている機能のセキュリティレベルが低下する部分が無いことを確認する。

7.9.4　参考情報

公開年月	情報源
2003 年	MEAP の技術解説 http://gijutsu.jbmia.or.jp/03kaisetu-canon.pdf MEAP の機能概要、及び保護機構の解説
2002 年 7 月	Vulnerability in ChaiVM EZloader http://en.securitylab.ru/notification/235126.php EZloader が署名の検証を行わないことに関する記事
2012 年 1 月	CVE-2012-0507 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507 JVM の BOF により Sandbox の制限を越えられる脆弱性の報告

7.9.5　深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

本節で解説した任意のアプリケーションをアップロードできるアプリケーションを、MFP にアップロードする場合でも、一般的に SDK を利用したアプリケーションのアップロード機能の使用が管理者に限定されていることが想定される。しかしここでは攻撃者が管理者認証を突破している場合を前提とする。また以下も前提とする。

・攻撃者は SDK の開発環境を利用できること。

【スコアリング】

CVSS 2.0 ベース 基本値：　7.9（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.10 利用者端末に導入するアプリケーションの脆弱性による問題

MFP ベンダから提供され利用者端末に導入するアプリケーション[28]は、MFP 内の保護資産へのアクセスが可能である。MFP がセキュアであっても、利用者端末用に提供されるソフトウェアの脆弱性から保護資産が漏洩することが考えられる。開発者は利用者端末に導入するアプリケーションの最新の脆弱性情報を利用者に提供しなければならないし、利用者は定期的に CVN 等の脆弱性情報を確認し、脆弱性が公開された段階で一時的に利用者端末に導入するアプリケーションの利用を停止するといった運用が必要となる。

7.10.1 【攻撃手法とその影響】

MFP の開発者から提供される利用者端末に導入するアプリケーションに関して、参考情報に示す通り、近年多くの脆弱性が報告されている。これら脆弱性の殆どは直接 MFP 本体を攻撃するものでは無く、当該アプリケーションがインストールされる利用者端末への攻撃を可能とする脆弱性として報告されている。しかし、単純に考えても MFP に送付する前、もしくは MFP から受信した利用者端末上の（スキャンデータやファクスなどの）保護資産は漏洩や改ざんの脅威にさらされるし、管理者端末が乗っ取られれば MFP 内の保護資産が間接的に影響を受けるかもしれない。バッファオーバーフローに起因するものが多いが、もっと単純な攻撃に対する脆弱性をもつアプリケーションも報告されている。

例えば、後述の参考情報の 2011 年 8 月に報告された利用者端末に導入するアプリケーションの脆弱性を利用して、攻撃者は次の手順でアプリケーションをインストールした利用者端末を攻撃することができる。

攻撃に利用する脆弱性は、アプリケーションの SaveXML 関数が持つディレクトリ・トラバーサルである。以下のように Windows のシステムディレクトリ配下に vbs ファイルと、それを実行するための mof ファイルを設置する。設置するためには、攻撃対象の利用者端末から、不正なウェブページや不正なファイルを開かせて以下のコマンドを実行させる必要がある。

```
・hoge.SaveXML("../../../../../WINDOWS/system32/hoge.vbs",”UTF-8”);
・hoge.SaveXML("../../../../../WINDOWS/system32/wbem/mof/hoge.mof",”UTF-8”);
```

図 7-8 利用者端末を攻撃するために設置するファイル例

mof ファイルによって Windows Management Instrumentation service を使って設置した任意の vbs ファイルを実行する。後は vbs によって、利用者端末上の保護資産をメールで送付することも、リモートシェルを提供させることも可能となる。攻撃コード作成の参考となる、検査用のコードが Metasploit の Exploit Database[29]でも公開されている。

次の段階として、攻撃者は乗っ取った利用者端末上のアプリケーションを解析、又はデータを収集[30]することにより、MFP 本体へアクセスするための情報を入手する。そして管理者、又は利用者として MFP にアクセスし、MFP 上の保護資産を不正に入手するなどの攻撃を行うことが考えられる。

---

28 プリンタドライバ等の MFP 製品に同梱、またはインターネット上からダウンロードできる MFP ベンダが提供するソフトウェア製品のこと。

29 http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/browser/hp_easy_printer_care_xmlsimpleaccessor.rb

30 パケットアナライザやキーロガーを仕掛けるなど

7.10.2 【原因と考察】

保護資産を扱う MFP で利用することを前提とした、MFP ベンダが提供する利用者端末に導入するアプリケーションについては、MFP で想定したセキュリティレベルが当該アプリケーションの脆弱性によって低下しないように、当該アプリケーションのセキュリティレベルを確保しなければならないと考える。対策としては一般的なアプリケーションと同様に、ソースコードを検査するツール[31]や手動によるソースコードレビューを行い、バッファオーバーフロー等の脆弱性が組み込まれないように注意することが重要である。評価者にとっては MFP に組み込まれたアプリケーションの検査とは異なり、Ollydbg や gdb といった実行環境に見合ったデバッガを利用できる分、比較的プリンタドライバの脆弱性検査は容易であると言える。

補足：OS やサードパーティ製の利用者端末用アプリケーションの脆弱性

上記攻撃手法は、OS やサードパーティ製のアプリケーションにも存在する。そして、それらのアプリケーションの脆弱性を利用することにより間接的に、利用者端末上の MFP ベンダが提供したアプリケーションや MFP が攻撃される可能性もある。例えば、攻撃者がある利用者端末上の OS の管理者権限を OS の脆弱性を利用して取得した場合、MFP ベンダが提供するアプリケーションに脆弱性が無くても、上述した様に MFP ベンダが提供したアプリケーションのデバッグや、キーロガー等の組込が行われることにより、MFP にアクセスするための利用者のパスワードが漏洩してしまうかもしれない。利用者が混同してはいけないのは、その様な利用者端末上の OS、他のアプリケーション、及びサードパーティ製の MFP 管理ソフトに起因する脆弱性は、利用者が運用によって対処しなければならないということである。実際に Novell の提供する iPrint Client[32]には、2011 年から 12 個以上の脆弱性[33]が CVE で公開されている。脆弱性の中には、任意のコードが実行される危険度の高いものも含まれている。

[31] IPA「セキュア・プログラミング講座 C/C++言語編」ソースコードレビュー
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c103.html
[32] http://www.novell.com/ja-jp/documentation/nw6p/pdfdoc/iprntenu/iprntenu.pdf
[33] CVE-2011-4186 CVE-2011-4185 CVE-2011-1708 CVE-2011-1707 CVE-2011-1706 CVE-2011-1705 CVE-2011-1704 CVE-2011-1703 CVE-2011-1702 CVE-2011-1701 CVE-2011-1700 CVE-2011-1699 など

7.10.3 対策

【運用ガイド】

1)　保護資産へのインタフェースとして端末に導入するアプリケーションを考慮する場合、MFP ベンダから提供されるアプリケーションに関して、利用者のポリシーに合致するものであることを確認する。

※MFP ベンダから提供されるアプリケーションに限らず、利用者端末上の他のソフトウェアも含め、管理する必要があることに留意する。

【開発ガイド】

2)　利用者端末用のアプリケーションを提供する場合、MFP で想定するセキュリティレベルを担保できるよう、同等のセキュリティレベルを持った使い方のできるアプリケーションを提供する。

【検査ガイド】

3)　MFP ベンダが提供する利用者端末に導入するアプリケーションに関して、保護資産に影響を与えないかを検討し、必要な場合は検査する。

7.10.4 参考情報

公開年月	情報源
2011 年 10 月	利用者端末に導入する MFP ベンダのアプリケーションに関する脆弱性 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3163 HP のソフトウェアが、ワークフローメタデータを取得される脆弱性
2011 年 3 月	利用者端末に導入する MFP ベンダのアプリケーション関する脆弱性 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0279 HP のソフトウェアのデバイステンプレートの認証設定が適切でない脆弱性
2010 年 5 月	利用者端末に導入する MFP ベンダのアプリケーション関する脆弱性 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1558 HP のソフトウェアの e-mail 機能を悪用して保護資産を得る脆弱性
2011 年 8 月	利用者端末に導入する MFP ベンダのアプリケーション関する脆弱性 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2404 HP のソフトウェアのディレクトリ・トラバーサルを悪用して保護資産を得る脆弱性
2010 年 12 月	利用者端末に導入する MFP ベンダのアプリケーション関する脆弱性 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3920 セイコーエプソンのプリンタドライバの一時的な権限不正による脆弱性

7.10.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは攻撃手法で解説した脆弱性を利用して利用者端末を乗っ取る場合について考察する。以下を前提とする。実際は乗っ取った利用者端末を悪用して MFP への攻撃を行うことが一般的であり、その場合は機密性、完全性、及び可用性の影響が全面的となる。しかしここでは利用者端末を乗っ取るまでを考察する。

・保護資産が利用者端末上にあること。

【スコアリング】

CVSS 2.0 ベース 基本値： 4.3（警告）

攻撃元区分	ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	影響なし
可用性	影響なし

7.11 多数のプロトコルに含まれる脆弱性による問題

本節では標準化されたプロトコルの網羅的な概説を行う。MFP は組込み機器の中でも最も多数のプロトコルを同時に実装し稼動させる機器のひとつである。これらの各プロトコルにはそれぞれ脆弱性が存在するため、多くのプロトコルを実装する MFP では、ベンダが実装したプロトコルの脆弱性を常に監視し、MFP の実装形態でも影響があると判断した脆弱性の場合、利用者への通知と、パッチを当てる等の保守体制が必要となる。

7.11.1 解説

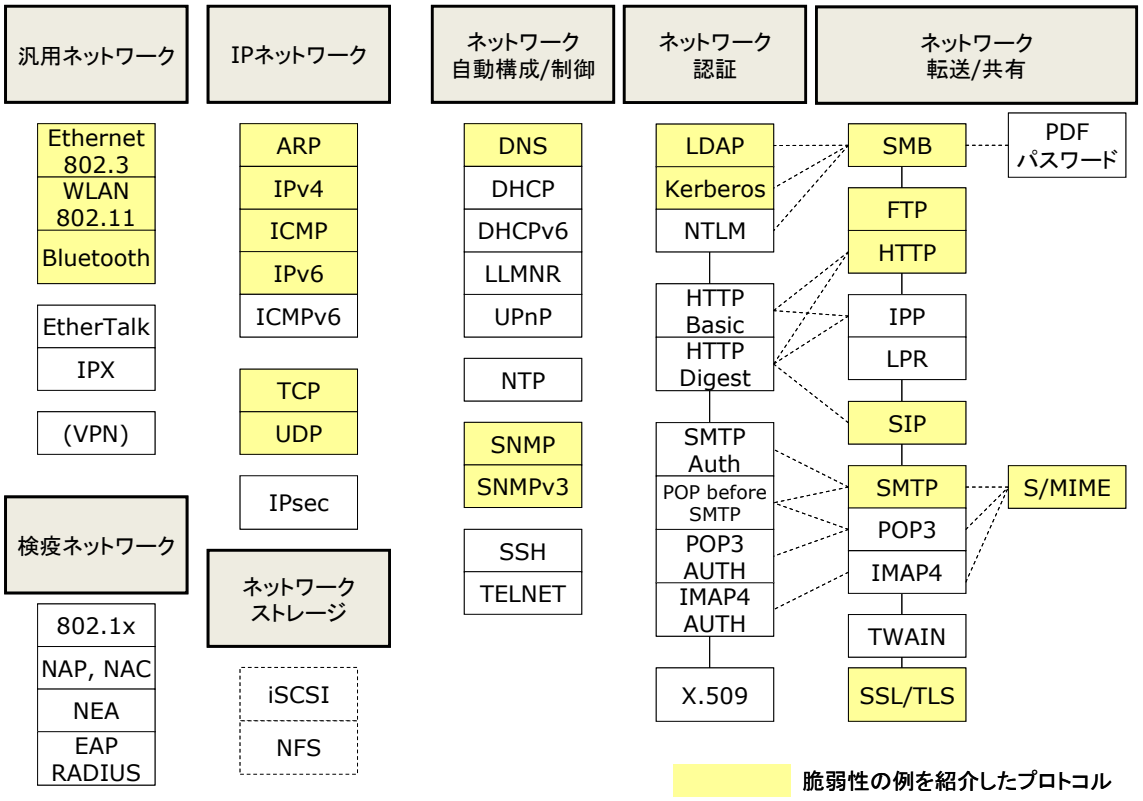


図 7-9 MFP で一般的に利用される通信プロトコルの一覧

上の図 7-9 は、MFP で一般的に利用される通信プロトコルの一覧である。左上の「汎用ネットワーク」は Ethernet や無線 LAN などの物理的な通信プロトコルである。「検疫ネットワーク」は、MFP のような重要なホストを独立したネットワークに隔離し、重要なソフトウェアの更新が済んでいない端末をネットワーク上で自動的に隔離しておくことなどに利用される。「IP ネットワーク」はインターネットを支えるための、複数のネットワークを相互接続し、HTTP などのアプリケーションプロトコルを伝送する手順である。「ネットワークストレージ」はネットワーク上のハードディスクなどの格納装置を扱う手順だが、現在の主要 MFP には該当がない。「ネットワーク自動構成/制御」は、IP アドレスを自動的に配布したり、ホスト名を IP アドレスに変換したり、サービス名をほかのマシンに広報する手順である。「ネットワーク認証」は、MFP にネットワーク経由で接続する利用者端末や管理者端末が MFP との間でユーザ ID などを利用して利用者を確認する手順であ

る。「ネットワーク転送/共有」は、MFP を介して文書データの交換や格納を行うための手順である。

図 7-9 の右半分にある点線で示している部分は、転送プロトコルと、それに対応または関連する認証プロトコルの関係を示している。例えば SMB というファイル共有プロトコルは LDAP、Kerberos、NTLM を認証プロトコルとして利用する。HTTP の場合は、HTTP Basic 認証、HTTP Digest 認証を利用する。IPP は HTTP ベースであるので、同様の認証プロトコルを利用する。SIP は HTTP と似たような形式のプロトコルで、HTTP Digest 認証と同じ手順を利用する。メールを転送する SMTP については SMTP AUTH と POP before SMTP という認証手順がある。メールボックスにアクセスする手順の POP3 には、POP3 専用の認証プロトコル(POP3 AUTH)があるが、POP before SMTP はこれを利用している。メールボックスにアクセスする手順で、より高機能な IMAP4 には IMAP4 専用の認証プロトコル(IMAP4 AUTHENTICATION)がある。

図 7-9 の右上の PDF パスワードは、PDF 型式のファイルにパスワードをつけて暗号化する機能である。これは通信プロトコルではないが、MFP の利用者が利用できるコンテンツの保護機能の一つである。また図 7-9 の右側中ほどの S/MIME も、メールのコンテンツを保護する機能で、メールの本文部分にあたるイメージデータを暗号化したり、電子署名を追加してイメージデータの改ざんを検出したりする機能がある。

上記のそれぞれのカテゴリごとに、複数のプロトコルが存在している。それにより、利用者は自分の環境に合ったプロトコルを選択して利用することができる。

例えば、「ネットワーク転送/共有」では、ファイル転送のプロトコルとして、SMB を使った SMB サーバへの書き込み、読み出しがある。FTP も FTP サーバへの書き込み、読み出しの手順となる。HTTP については HTTP プロトコル上でさらに拡張された、SOAP を使ったウェブサービスも提供され、書き込み、読み出しのほかに、どのようなサービスがあるか広報する機能も提供されている。

特定の利用者の環境に限ってみれば、これらプロトコルのうち、すべてを使うわけではない。しかし、グローバルに製品を出荷するベンダとしては複数を搭載しておかなければならない事情がある。

過去の歴史では、こうした機能を実装した製品はそれぞれに脆弱性を持っていた。そうした脆弱性が現在の MFP には含まれていないと考えられるが、MFP の機能はソフトウェアの規模としても大きいため、必ずしもそうでない場合もあるだろう。

7.11.2 【攻撃手法とその影響】

MFP が実装する複数のプロトコルへの攻撃手法は、それぞれのプロトコルに応じて、簡単な手法から複数の手順を必要とする高度な手法まで複数の方法がある。

ここでは個々の詳細な手法については割愛するが、MFP の TCP/IP をベースとした主だったプロトコルについて、最近においてもさまざま脆弱性が発見されているということを紹介したい。

1) Ethernet (IEEE 802.3)の脆弱性

Ethernet (IEEE 802.3)はワイヤ上で Ethernet フレームを交換するプロトコルで、Ethernet 自体は通信データを保護する機能はない。Ethernet はルーティング機能がなく IP よりも単純なプロトコルだが、世界レベルの広域な Ethernet 接続サービスも提供されており、予想外の範囲まで同じ Ethernet セグメントでつながっているこ

とがあるのでネットワーク構成に注意が必要である。

最近の Ethernet 関連の脆弱性の例としては、一部の Ethernet デバイスドライバが Ethernet フレームの大きさを検査していなかった例がある(CVE-2009-4537)。また、「Broadcom NetXtreme 管理用ファームウェアにバッファオーバーフローの脆弱性(JVNVU#512705)」のように、Ethernet カード(またはモジュール)上に遠隔管理用のソフトウェアが追加されていて、脆弱性が発見される場合もある。

Ethernet は安価な標準的な通信インタフェースとして普及しながら、10 ギガビット/毎秒を超える高速通信を実現し、信頼性向上のために運用管理機能も拡充されるなど変化を続けている。

2) 無線 LAN の脆弱性

無線 LAN には端末と端末が直接接続を行うアドホックモードや、アクセスポイントを経由して端末が通信するインフラストラクチャモードの別があり、アドホックモードでの認証は難しい。また、他の端末の通信を中継するアクセスポイントは、本来はよく管理された状態で動作させなければならないが、目に見えない無線で接続するため第三者が偽のアクセスポイントを動作させることが簡単であり、無線 LAN 端末を偽のアクセスポイントに接続させることも容易である。

セキュリティを意識した環境においては現在殆ど利用されていないが、WEP という方式では数分で暗号化を行う鍵が解読されるという問題がある。

無線 LAN のセキュリティについては、WPA/WPA2 という通信の保護方式を利用するなどの対策があり、「総務省 無線 LAN における危険性[34]」などのサイトで、安全な無線 LAN の使い方が紹介されている。

3) Bluetooth の脆弱性

Bluetooth は 2.4GHz の周波数帯域を使った比較的近距離で利用される無線通信の規格であり、事前共有した PIN によるチャレンジ&レスポンス方式の認証と 128bit 長までの鍵に対応したストリーム暗号「E0」による暗号化を採用している。一般的な利用用途はオーディオ機器のスピーカーや PC のキーボード等、常時接続する機器間の無線接続だが、スマートフォンやタブレット端末間でのデータ送受信にも利用されており、一部の MFP では、端末から Bluetooth 経由でデータを受信して印刷する等の機能を実装している。Boetooth は仕様上、SPP や DUN といったバックドアとなる可能性があるプロファイル[35]を持っている。また、数多くのプロファイルが存在するため、プロファイルの実装段階でバッファオーバーフロー等の脆弱性が組み込まれてしまう可能性が多いと言われている[36]。

4) TCP/IP の脆弱性

TCP/IP の脆弱性については、IPA「TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 5 版」としてまとめられている。ARP、IPv4、ICMP、TCP、UDP についての脆弱性が含まれており、これらの脆弱性を検証するためのソフトウェア「TCP/IP に係る既知の脆弱性検証ツール V5.0 」も配布されている。

---

[34] 無線 LAN における危険性 - http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan12.htm

[35] 機器の種類ごとに策定された固有の通信手順のこと

[36] http://www.net-security.org/secworld.php?id=11663

TCP/IP は一般的に OS のカーネル内で動作するため、脆弱性を攻撃されると OS が停止するなど、影響が大きい。

5) IPv6 の脆弱性

IPv4 の 32 ビットアドレスの枯渇に伴い、1982 年アメリカ国防総省において標準化された IPv6 は、現在殆どの MFP が対応済であり利用可能な状態となっている。プロトコルの仕様上起こり得るネットワークレベルの脆弱性に関しては第 13 回情報セキュリティ・シンポジウムで発表された「IPv6 の導入におけるセキュリティ上の影響と対策」[37]が参考となる。一方 OS やアプリケーションの実装漏れによる IPv6 が関係する脆弱性は CVE の公開情報として 2011 年 1 月から 2012 年 7 月までに 36 個確認できる。OS の実装漏れにより DOS 攻撃によるサービス妨害を受けるものやアクセス制御リストを回避されるものなどが確認されている。

6) DNS の脆弱性

DNS は www.example.jp などのホスト名を IP アドレスに変換するためのプロトコルである。ホスト名を使わず、IP アドレスだけを使う場合、DNS は不要だが、インターネットを経由したメールファクスを利用する場合は DNS が必要になることが多い。

DNS の代表的な脆弱性としては、DNS のメッセージが保護されていないことを悪用して、DNS で名前解決をしようとするホストに偽の IP アドレスを注入する「DNS キャッシュポイズニング」がある。2008 年に DKA(Dan Kaminsky Attack)という手法が発見され、影響が大きいと指摘された。その後、DNS の脆弱性に対処するため DNSSEC という保護方式が徐々に導入されつつある。

7) SNMP、SNMPv3 の脆弱性

SNMP は主にネットワーク機器や通信機器の動作状態を監視するためのプロトコルである。SNMP では、通信機器の内部の動作状態を示す情報にアクセスするために、MIB(Management Information Base)と呼ばれる、階層化された名前のラベルから、型つきの値を応答する処理を行う。SNMP プロトコル上では、要求と応答の両方のメッセージデータが ASN.1(Abstract Syntax Notation One)というバイナリ形式で符号化されるが、ASN.1 の解釈を行う実装を中心に SNMP では多数の脆弱性が発見されている[38]。

2002 年には HP のプリンタに対して「.iso.3.6.1.4.1.11.2.3.9.4.2.1.3.9.1.1.0」という OID を入れると、管理者パスワードが取得できるという脆弱性があった[39]。SNMP で閲覧できる情報に保護資産が存在する場合は、利用者を制限する必要がある。そのため SNMPv3 では、識別認証の機能が追加されたが、認証手順の実装にも脆弱性が発見されている[40]。

その後、SNMP は、SNMP のメッセージの型式を定義する仕様と、SNMP メッセージの伝送を定義する仕様(RFC5590)を分離し、通信内容を保護する伝送方式を選択しやすいようにしている。

SNMP は階層化された MIB 情報をツリー状にたどりながら問合わせ処理ができる特徴がある。そのため、設定を間違えるか処理量の制限がないと、再帰的に多

37 http://www.imes.boj.or.jp/citecs/13sympo/ref2.pdf
38 http://www.ipa.go.jp/security/ciadr/20020213snmp.html
39 http://securitytracker.com/id/1004860
40 http://jvn.jp/cert/JVNVU878044/

数の MIB 情報の問合わせが発生して機器の動作に問題が発生することがある。
また、SNMP による監視結果を元にした「アクション」などの特定の動作を定義できる実装がある。こうした実装では、偽の SNMP 応答の内容を検査しないでアクションを実行すると、任意のコマンドを実行させられることがある。

8) FTP の脆弱性

FTP(File Transfer Protocol)は HTTP 以前からインターネットでのファイル転送の標準プロトコルであったためよく普及している。
しかし、FTP には長期にわたって通信を保護する手順がなく、制御用の TCP ポートとデータ転送用の TCP ポートが分かれている複雑な構造から、IPsec で保護する場合も設定が困難であった。現在は FTP を SSL/TLS 上で利用する、制御用 TCP ポートとデータ転送用 TCP ポートを同一のポートにする、などの改良も行われているが、MFP 製品で採用しているかどうかはカタログベースでは特に記述がなく確認できなかった。
また、FTP の一部のコマンドはすでに悪用された事例がある。FTP の port コマンドは、他の FTP サーバに対して任意のホストの任意のポート番号の TCP ポートに接続させる命令である。port コマンドを悪用する例として「FTP バウンス攻撃」がある。FTP site コマンドは接続先の FTP サーバ上で任意のコマンドを実行させる機能で、この機能が残っている FTP サーバを動作させることは非常に危険である。FTP cwd コマンドは、接続先の FTP サーバ上でのカレントディレクトリを移動するコマンドである。cwd コマンドはファイルを書き込む FTP put か、ファイルを読み出す FTP get と組み合わせて利用するが、特権が必要なディレクトリやファイルへの操作がないよう、FTP サーバ上でのアクセス可能なディレクトリを一部のサブディレクトリ以下だけに限定するのが普通である。
FTP サーバの利用方法として、認証不要の anonymous FTP サーバというものがある。これは FTP プロトコルでのログイン時にユーザ ID として”ftp”または”anonymous”と送信し、任意にパスワード文字列を送信すれば、誰でもその FTP サーバを利用できる使い方である。一部の FTP サーバの実装には、標準的に anonymous FTP サーバが動作するようになっていることがあり、FTP サーバの動作には注意が必要である。
以上のような状況から、MFP を利用する環境では FTP の利用には相当に充分な注意が必要だと考えられる。

9) HTTP、HTTPS の脆弱性

HTTP をベースとしたサービスは、ウェブブラウザのグラフィカルなユーザインタフェースを活用して効率よく機能を提供できるため、殆どの MFP に搭載されており、非常に広範囲に利用されている。また、プリント機能を提供する「IPP(Internet Printing Protocol)」や、ウェブサーバ間で処理を自動化する「Web サービス」、共有ファイルへのアクセスを提供する「WebDAV」などの用途を特化したサービスも HTTP をベースにしている。HTTP 通信に関しては多くの脆弱性の観点が存在するため、7.15 節で別途解説する。

なお、HTTP の通信路を保護する HTTPS (HTTP over SSL/TLS)も非常に広く普及しているため、HTTPS の脆弱性が及ぼす影響も大きい。最近の例では SSL/TLS の renegotiation(SSL/TLS 通信中に再び接続を確立する)機能の脆弱性が報告されている。

10) LDAP、Kerberos の脆弱性

LDAP と Kerberos はネットワーク上で集中的に認証・認可を行う代表的なプロトコルである。LDAP と Kerberos を効率的に利用すれば、何台もの MFP のそれぞれに利用者登録をすることなく認証ができて、パスワードの更新も集中管理できる。しかし、認証情報や権限認可情報が集中している分、影響も大きい。

LDAP 自体には通信内容を保護する機能がないため、SSL/TLS と組み合わせて利用する。Kerberos はバージョン 4 以降で、暗号化する機能がプロトコルに組み込まれている。また、LDAP サーバに対しては、ID やメールアドレスなどの検索を要求するときに、LDAP インジェクションを実行させる引数が含められることがある。

最近の LDAP の脆弱性には「JVNDB-2009-001779 - Active Directory の LDAP サービスにおけるサービス運用妨害(DoS) の脆弱性[41]」などがある。Kerberos については「JVNDB-2010-001344 - MIT Kerberos の kadmind におけるサービス運用妨害 (DoS) の脆弱性[42]」などがある。

11) SMB の脆弱性

SMB(Server Message Block)はファイル共有サービスを提供するプロトコルである。CIFS という、SMB の上位バージョンのプロトコルも提供されているが、一般的には CIFS も含めて SMB と呼ばれている。

SMB のファイル共有サービスでは、MFP からスキャンしたファイルを転送したり、MFP 内部に格納されたスキャンイメージを利用者端末から取り出したりする形で利用する。また、ファクス受信で到着したファクスイメージを MFP から利用者端末に対して直接転送することもある。さらに MFP にプリントを要求するときに利用することも可能である。

SMB では、NTLM と呼ばれる認証手順が利用されてきたが、NTLM ではパスワードを交換するとき、生のパスワードを解読しやすい問題があり、NTLMv2 という改良された手順がある。SMB で利用される NetBIOS というプロトコルでは、ブロードキャストを利用して SMB サーバの名前を IP アドレスに解決するため任意の偽の応答にだまされやすい。また、Windows XP SP1 以前の Windows で動作する SMB ファイル共有サーバでは、ファイル共有機能がパスワードなしでも動作する脆弱性[43]があった。

最近でも深刻な脆弱性として「JVNDB-2011-005032- Samba の RPC コードジェネレータにおける任意のコードを実行される脆弱性」[44]などが公開されている。

12) SIP の脆弱性

SIP(Session Initiation Protocol)は 2 つの端末間でセッション制御を行うプロトコルである。MFP では、ファクスの伝送のために、SIP と RTP(Real-time Transport Protocol)を利用する。

SIP は通信内容を保護するためのいくつかの仕様があるが、通信事業者の間では、通信事業者内だけで SIP の通信をする前提となっているため、一般的に通信の保護

---

41 JVNDB-2009-001779 - Active Directory の LDAP サービスにおけるサービス運用妨害(DoS) の脆弱性 - http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-001779.html

42 JVNDB-2010-001344 - MIT Kerberos の kadmind におけるサービス運用妨害 (DoS) の脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001344.html

43 http://itpro.nikkeibp.co.jp/members/NBY/techsquare/20021129/3/

44 http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-005032.html

機能は利用されていない。一方で、SIP を利用した製品などの実装では、通信の保護機能がなくても、IP アドレスを指定すればインターネット上の SIP サーバや SIP 端末とも通信できてしまう脆弱性がある。また、SIP については電子メールの迷惑メールのような「SPIM」と呼ばれる「迷惑着信」の問題もある。

SIP の脆弱性については IPA「SIP に係る既知の脆弱性に関する調査報告書 改訂第 3 版」[45]に詳述されている。また、この脆弱性に対応する IPA「SIP に係る既知の脆弱性検証ツール V2.0」[46]も配布されている。

13) SMTP、POP3、IMAP4 の脆弱性

SMTP は電子メールの転送を、POP3 と IMAP4 はメールボックスへのアクセスを提供するプロトコルである。これらも HTTP 以前から存在し、普及している。

SMTP については、もともと認証手順も通信の保護手順も仕様になかったため、さまざまな問題が発生していた。現在も、商品の広告やコンピュータウイルスを添付した「迷惑メール」が大量に届いてしまう問題などがある。

また、これらの電子メールのプロトコルの実装にもさまざまな脆弱性が発見されてきた。SMTP のコマンドについては、認証なしでメールアドレスの存在確認ができる SMTP vrfy コマンドと、別名アドレスやメーリングリストのメンバー名を展開できる SMTP expn コマンドの脆弱性がある。SMTP auth コマンドは SMTP プロトコルでユーザ認証を行う手順だが、パスワード文字列をハッシュ化して交換するため SMTP auth 手順を盗聴されるとパスワードを解読される可能性が高い。さらに SMTP 自体にはメッセージや SMTP の通信路を保護する機能がないため、SMTP を安全に利用するには SSL/TLS か IPsec で SMTP 通信路を保護する必要がある。

最近の SMTP の脆弱性には「Microsoft Windows の SMTP コンポーネントにおける情報漏えいの脆弱性[47]」などがある。POP3 については認証用のパスワード交換手順の脆弱性として「APOP におけるパスワード漏えいの脆弱性[48]」などがある。最近の事例では POP3 と IMAP4 の両方で、応答処理の脆弱性として「複数の Microsoft 製品の inetcomm.dll における整数オーバーフローの脆弱性[49]」が報告されている。

S/MIME は電子メールのメッセージを安全に交換するための、メッセージやコンテンツの保護仕様である。S/MIME の保護を確実にするには電子証明書を正しく運用する必要がある。また、S/MIME ではメールの宛先や送信元などを示すメールヘッダは保護されない、などの注意事項をよく理解する必要もある。詳しい S/MIME の利用方法は IPA「電子メールのセキュリティ - S/MIME を利用した暗号化と電子署名[50]」を参照いただきたい。

---

[45] IPA「SIP に係る既知の脆弱性に関する調査報告書 改訂第 3 版」- http://www.ipa.go.jp/security/vuln/vuln_SIP.html

[46] IPA「SIP に係る既知の脆弱性検証ツール V2.0」- http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html

[47] JVNDB-2010-001391 - Microsoft Windows の SMTP コンポーネントにおける情報漏えいの脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001391.html

[48] JVNDB-2007-000295 - APOP におけるパスワード漏えいの脆弱性 http://jvndb.jvn.jp/ja/contents/2007/JVNDB-2007-000295.html

[49] JVNDB-2010-001471 - 複数の Microsoft 製品の inetcomm.dll における整数オーバーフローの脆弱性 - http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-001471.html

[50] IPA「電子メールのセキュリティ - S/MIME を利用した暗号化と電子署名」 http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html

7.11.3 【原因と考察】

1) プロトコルの多さ

MFP には、さまざまなレベルのプロトコルが混在している。MFP の業界団体である JBMIA が配布している BMLinkS[51]のように、複数ベンダの複数機種の MFP に対応する共通ドライバを開発する活動もあるが、既存のプロトコルは利用者端末の条件や他システムとの制約などの依存関係を相互に持っており、簡単にいずれかひとつのプロトコルには集約できない、という状況がある。

原則的な開発者による対策としては、不要なサービスは実装しないことと、動作させる必要があるサービスに関してはサービスからアクセスできる情報を必要最低限に絞ることが有効である。利用者としては、運用上利用しないサービスは起動しないことが有効と考えられる。

実際の攻撃では、これらのサービスが動いていることを確認するために、攻撃者は MFP に対してポートスキャンを行う。このポートスキャンを抑止し、サービスを隠蔽することによって MFP は攻撃の初期段階時に攻撃対象から除外されるかもしれない。ポートスキャンを抑止する方法は大きく 2 種類あり、ある程度のスキャンに対し応答しないようにカーネルを修正する方法と、65,535 個のポート全てがスキャンに対して応答するようにカーネルを修正する方法がある。どちらの方法も攻撃者が空いているポート（サービス）を特定できなくなるという観点では有効である。但し、ポートスキャンへの対応は、MFP で実装されているサービスや機能、外部機器との連携機能への影響が無いことを確認した上で行う必要がある。

2) 今なお発見される脆弱性には、事後対応も含めた対策

上述した様に、MFP は本体の豊富な機能に伴い、多くのサービスが動いている。そのため、MFP の脆弱性はどうしてもゼロにはできないという状況もある。ソフトウェアについての脆弱性は、「7.11.2【攻撃手法とその影響】」で列挙したように、どのプロトコルにもどこかの実装で脆弱性が報告されている。実際多くの MFP が実装している SMB の脆弱性に関する報告は 2012 年 4 月に公開されているものである。

MFP の脆弱性は完全にゼロにはできないとすれば、MFP の利用者も、MFP ベンダの開発者も、それぞれが脆弱性に事後対応することを想定しておく必要がある。脆弱性への利用者としての事後対応については、利用している製品に関する脆弱性情報と対応策についてベンダから情報収集することや、ソフトウェアの更新や利用手順の変更などの対応を想定した体制を整えておくこと、万一被害が起こったときのための担当者と対応手順を検討しておくこと、などがある。

製品を提供する側での脆弱性への事後対応の例としては、脆弱性の確認と報告の手順、被害と脅威の低減方法の検討、製品への反映方法の検討、対応の優先度づけ、などがあるだろう。

3) 複数のプロトコル実装に含む脆弱性への対策

こうした多数のプロトコルを同時に実装せざるを得ない状況で、MFP 製品の脆弱性を最小限に抑えるための設計、開発者向けの対策として、IPA で普及活動を行

[51] BMLinkS – JBMIA: 社団法人ビジネス機械・情報システム産業協会 BMLinkS プロジェクト委員会 http://bmlinks-committee.jbmia.or.jp/

っている「セキュリティエンジニアリング」[52]や「セキュア・プログラミング講座」[53]、「組込みシステムのセキュリティへの取組みガイド」[54]などがある。

これら脆弱性対策の取り組みでは、既存の方法では検討事項や試験項目が増え過ぎて対応が難しい。そのため、いくつかの自動化された試験ツールや検査方法の利用も検討が必要だろう。

試験ツールには、ソースコードを検査して脆弱性を発見するツール[55]、製品の HTTP 通信などを書き換えて網羅的に確認するファジングツールやブラックボックス的に外部から試験して脆弱性を発見するツールがある。ファジングに関してはファジングの解説から具体的なファジングツールの使用方法までを網羅した資料が IPA から公開[56]されている。ブラックボックス的に脆弱性の検査を行うことでよく知られている製品としては Codenomicon、AppScan、Nessus などがある。こうした脆弱性試験手順を含む評価手順については Microsoft の Windows Logo[57]で行われているような、脆弱性のテストを含む製品認証制度も参考になるだろう。

但し、これらのツールはあくまで HTTP 通信を初めとした標準化されたプロトコルにしか適用できない上、HTTP 通信においても、手動で確認すれば検出できるような作りこみによる脆弱性は検出できないことを留意しておかなければならない。

---

[52] IPA「セキュリティエンジニアリング」- http://www.ipa.go.jp/security/awareness/vendor/software.html
[53] IPA「セキュア・プログラミング講座」- http://www.ipa.go.jp/security/awareness/vendor/programming/
[54] IPA「組込みシステムのセキュリティへの取組みガイド」- http://www.ipa.go.jp/security/fy20/reports/emb_app/
[55] IPA「セキュア・プログラミング講座 C/C++言語編」ソースコードレビュー http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/c103.html
[56] http://www.ipa.go.jp/security/vuln/fuzzing.html
[57] Windows Logo - http://www.microsoft.com/japan/whdc/winlogo/hwrequirements.mspx Windows 用デバイスドライバ向けに提供されている製品認証試験制度

7.11.4 対策

【運用ガイド】

1) MFP 上で利用する機能を必要最小限に特定し、利用しない機能をすべて停止する
2) ベンダの脆弱性対策情報を購読するか、いつでも入手できるように準備する
3) 監査記録から、利用動向、セキュリティ違反の動向を定期的に把握し、対策する
4) MFP 製品の脆弱性が発見された場合の対応方法を計画しておく
5) 脆弱性の被害が発生したときの対応方法を計画しておく

【開発ガイド】

6) 実装しているサービスを管理し、利用しなくなったサービスは実装しない。
7) 保護資産へのアクセスを含む通信か否かを明確に定義し明記する。場合により、カーネルレベルで攻撃への対策を実装する。
8) 製品の企画、開発のプロセスを通じて、製品の脆弱性対策に取り組む
9) MFP を利用する環境で適用されるセキュリティポリシを MFP にも容易に反映しやすくなるようなツールを検討する
10) 脆弱性検査ツールとして、ソースコードの静的分析ツール、ファジングツール、侵入テストツールなどの利用を検討する
11) 脆弱性が発見された場合の対応を行う体制を整え、対応手順を計画しておく

【検査ガイド】

12) 保護資産へアクセスできる通信プロトコルを検査する際は、利用者が入力可能かどうかに関わらず、全てのパラメータを検査対象とする
13) 利用する脆弱性検査ツールで何をどこまで検査できるのかを把握し、検査できない部分は手動、もしくはソースコードレビューにより網羅的な検査を行う

7.11.5 参考情報

公開年月	情報源
2002 年 2 月	IPA: 広範囲に該当する SNMP の脆弱性について http://www.ipa.go.jp/security/ciadr/20020213snmp.html SNMPv1 の脆弱性に関する情報
2008 年	SE のための情報セキュリティ対策 - HTTP 脆弱性 http://www.chuu-information.com/security/fragile_6.html HTTP プロトコル自体の脆弱性の要点がまとめられている
2008 年 6 月	JVNVU#878044 SNMPv3 実装の不適切な HMAC 処理による認証回避の脆弱性 http://jvn.jp/cert/JVNVU878044/ SNMPv3 で特定のメッセージにより認証が回避されてしまう脆弱性
2008 年 7 月	An Illustrated Guide to the Kaminsky DNS Vulnerability http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html DKA による CACHE Poisoning の概要と対処
2010 年 11 月	IPA: TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 5 版 http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html TCP, ICMP, IPv4, ARP プロトコルの解説つき脆弱性資料。

2010 年 11 月	IPA: TCP/IP に係る既知の脆弱性検証ツール V5.0 http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html TCP, ICMP, IPv4, ARP と、一部 IPv6 に対応
2009 年 11 月	JVNVU#120541 SSL 及び TLS プロトコルに脆弱性 http://jvn.jp/cert/JVNVU120541/ SSL/TLS の通信中に再び接続を確立する機能の脆弱性
2009 年 12 月	CVE-2009-4537: r8169: straighten out overlength frame detection http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4537 Realtek 製 Ethernet チップのドライバに含まれていたフレーム長検査の不良
2011 年 7 月	CVE-2011-1265 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1265 Microsoft 製品が不正な Bluetooth パケットによりコードを実行される脆弱性
2012 年 4 月	CVE-2012-0475 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0475 Mozilla 製品における IPv6 リテラルのアクセス制御リストを回避される脆弱性
2012 年 5 月	CVE-2011-2699 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-2699 Linux OS の IPv6 実装における DOS 攻撃による影響の脆弱性

7.11.6 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

本節では複数のプロトコルについて紹介したが、ここでは MFP 内部の HTTP サーバが、攻撃用のツールを使った DOS 攻撃により、MFP のサービスが停止した場合を想定する。

・上記運用ガイドの対策を講じていない機種であること。

【スコアリング】

CVSS 2.0 ベース 基本値： 5.8（警告）

攻撃元区分	隣接ネットワークから
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	影響なし
完全性	影響なし
可用性	全面的な影響

7.12 MFP 独自プロトコルに懸念される脆弱性

本節では、7.11 節で解説したような標準化されたプロトコルには含まれない独自プロトコルについて解説する。独自プロトコルとは、MFP 外との通信サービスを提供するためにベンダが独自に開発もしくは改造した通信プロトコルを表す。標準化されたプロトコルと異なり、7.11 節で解説したような検査ツールによる検査では脆弱性が発見されない。一方で設計から開発の段階で、思いがけない部分にバッファオーバーフロー等の脆弱性に繋がる実装上のバグがあるかもしれない。そこで本節では通信制御部分のソースコードを例示して、漏れやバグが発生しやすい部分を解説する。但し本書で例示するソースコードは参考であり、MFP に実装されるサービスではない。

7.12.1 【攻撃手法とその影響】

一部のベンダの MFP では、一般的なポート以外に割り当てたサービスを実装していることが確認されている。これらは 7.11 節で列挙したような標準化された通信プロトコルによるサービスを独自のポート番号で提供しているだけの場合もある。しかし、ベンダが提供する付加サービスや機器連携を提供するために独自のサービスを実装している場合もある。独自のサービスである場合、ウェルノウンポートの標準化された通信プロトコルのように RFC 等で仕様が公開されることは無い。また、世間一般に知られているサービスと異なり、脆弱性が洗い出されていない。これらは良く言えば攻撃対象となりにくく、そのため脆弱性やその攻撃手段が公開されることは稀である。しかし一方で、良く知られているサービスでは塞がれているような脆弱性が、未だ存在している可能性がある。

ここでは MFP には実装が確認されていないプロトコルの脆弱性を例示して、独自プロトコルの仕様もしくは実装時に発生し得る脆弱性の例について説明する。

脆弱性自体は 2012 年 7 月 7 日に参考資料の CVE にも公開されている。図 7-10 は、有名なメッセージ交換用ツールの通信制御部分のソースコードである。この脆弱性は、メッセージに添付する規定のインラインイメージ、つまり規定サイズのアイコン（携帯の絵文字の様なもの）の領域を悪用し、スタック領域のバッファオーバーフローを引き起こし、任意のコードが実行可能となるものである。

```
void mxit_show_message( struct RXMsgData* mx )
  {
  char*             pos;
  int               start;
  unsigned int      end;
  int               emo_ofs;
  char              ii[128];
  char              tag[64];
  int*              img_id;

  if ( mx->got_img ) {
      while ( ( pos = strstr( mx->msg->str, MXIT_II_TAG ) ) != NULL ) {
          start = pos - mx->msg->str;
          emo_ofs = start + strlen( MXIT_II_TAG );
          end = emo_ofs + 1;

          while ( ( end < mx->msg->len ) && ( mx->msg->str[end] != '>' ) )
              end++;

          if ( end == mx->msg->len )     /* end of emoticon tag not found */
              break;

          memset( ii, 0x00, sizeof( ii ) );
          memcpy( ii, &mx->msg->str[emo_ofs], end - emo_ofs );

          /* remove inline image tag */
          g_string_erase( mx->msg, start, ( end - start ) + 1 );

          /* find the image entry */
          img_id = (int*) g_hash_table_lookup( mx->session->iimages, ii );
          if ( !img_id ) {
              /* inline image not found, so we will just skip it */
              purple_debug_error( MXIT_PLUGIN_ID, "inline image NOT found (%s)¥n", ii );
          }
          else {
              /* insert img tag */
              g_snprintf( tag, sizeof( tag ), "<img id=¥"%i¥">", *img_id );
              g_string_insert( mx->msg, start, tag );
          }
      }
  }
```

図 7-10 脆弱なプロトコル処理を行うソースコードの例

赤字の部分が問題のある箇所であり、128Byte 固定で確保されている変数 ii に対して、大きな文字列 str[mem_ofs]を入力される可能性がありスタック領域をオーバーフローさせ、戻りアドレスを書き換えることが可能である。これにより任意のコードや管理者権限のシェルを実行することが可能となる。MFP に搭載される OS によってはシェルの奪取は困難と言われている。しかし、7.8 節で解説したように、汎用 OS を搭載した MFP で実際に OS の脆弱性が適用できた例もある。

なおバッファオーバーフローの仕組みや、上記の様にスタック領域に任意の値を書き込める実装を利用してシェルを実行する攻撃コードは IPA のサイト[58]に掲載

[58] http://www.ipa.go.jp/security/awareness/vendor/programmingv1/b06_01.html

され公開されている。

7.12.2 【原因と考察】

この脆弱性の原因は、開発段階でバッファオーバーフローを引き起こす関数が見逃されてそのまま実装されてしまったことにある。一般的なポートのプロトコルであれば、実装後のファジングツールによる検査が効果的かもしれない[59]。しかし、独自プロトコルの場合はそのプロトコルの特性を考慮した設計及び検査手法を考慮する必要がある。

7.12.1 節で説明したような実装レベルの脆弱性は、主として開発環境においてコーディングルールが整備をしていない、もしくはルールがあってもルールに従った開発をしているかどうかチェックする仕組みが整備されていないといった理由から発生する。利用者が入力するテキストや、プルダウンで選択する項目であれば、そこに不正な値が入る可能性を想定し、設計時もしくは検査時に不備が見つけ出せたかもしれない。このケースでは、ベンダ側で用意した固定のイメージやアイコン等が入ると決まっている領域を扱うプログラム内部処理であるために、検査対象から漏れてしまったのかもしれない。

コーディングルールを定めてプログラミングする際にも、変数領域とその操作の設計及び検査には十分注意を払わなければならない。例に挙げたプログラムでは、現在ソースコードをダウンロードすると、以下の通り改善されていることが確認できる。

```
:
int             emo_ofs;
char*           ii;
char            tag[64];
int*            img_id;
:
        if ( end == mx->msg->len )     /* end of emoticon tag not found */
            break;

        ii = g_strndup(&mx->msg->str[emo_ofs], end - emo_ofs);

        /* remove inline image tag */
        g_string_erase( mx->msg, start, ( end - start ) + 1 );
:
            g_snprintf( tag, sizeof( tag ), "<img id=¥"%i¥">", *img_id );
            g_string_insert( mx->msg, start, tag );
        }
        g_free(ii);
:
```

図 7-11 改善されたプロトコル処理のソースコード

開発段階であれば、この様な目視では見落とし易い変数領域の操作に対して、ソースコードの静的分析ツールの適用は有効である。また、攻撃の糸口とする独自プロトコルの存在検出を妨害する対策として、7.11 節でも解説したカーネルレベルでのポートスキャンへの対応は有効かもしれない。

一方、実装された MFP 上の独自プロトコルによるサービスを評価者がブラック

[59] 但し、手動による検査を併用しなければ、セッション維持管理等の作り込みによる脆弱性は検出できない場合が多い。

ボックス検査を行う場合、前述したような脆弱性検査ツールでは検出できない場合も多い。Nessus の様な公知脆弱性データベースを元に検査するツールでは、独自プロトコルは検査されないし、独自プロトコルに対して自動検査を行うツールそのものが存在しない。独自プロトコルが何らかの標準化されたプロトコルを拡張したものであれば、ファジングツールにより一部は検査できるかもしれないが、その場合でも拡張部分は検査されない場合が多い。そのため独自プロトコルを実装レベルで検査する際は、検査を行う者が手動で侵入検査を行い、パラメータ部分を探しだし、パラメータに不正な値を入れてもオーバーフローを起こさないかを網羅的に確認する必要がある。

独自プロトコルを検査する場合は、評価者がソースコードを開発者から開示してもらい、ソースコードレビューや静的分析ツールによる解析を行うことにより確認する方が現実的である。ソースコードが入手できない場合、デバッグすることは非常に困難であるため、通信プロトコルの仕様をヒアリングした上で、パラメータ部分に不正な値を入力して、応答を確認しながら攻撃コードを作成しなければならない。パラメータ部分に不正なコードを挿入する攻撃コードの参考となる例は Metasploit の Exploit Database に多数公開されている。

7.12.3 対策

【運用ガイド】

1) MFP 上で利用する機能を必要最小限に特定し、利用しない機能をすべて停止する
2) ベンダの脆弱性対策情報を購読するか、いつでも入手できるように準備する

【開発ガイド】

3) 実装しているサービスを管理し、利用しなくなったサービスは実装しない。
4) 他の機能に影響が無い場合、ポートスキャンへの対策の実装を検討する。
5) 実装したプロトコルの全てのパラメータに対して、コーディングルールに準拠したソースコードになっていることを確認する。
6) 開発段階における脆弱性検査ツールとして、ソースコードの静的分析ツールなどの利用を検討する
7) 脆弱性が発見された場合の対応を行う体制を整え、対応手順を計画しておく

【検査ガイド】

8) 保護資産へアクセスできる通信プロトコルを検査する際は、利用者が入力可能かどうかに関わらず、全てのパラメータを検査対象とする
9) 実装レベルの脆弱性により、間接的に保護資産へのアクセスが行われないかを調査する
10) 独自プロトコルの仕様を確認した上で(ファジングツール等が利用できれば利用し、)手動による検査を行う。ソースコードの閲覧が可能であればソースコードレビューや、静的分析ツールによる検査を行う

7.12.4 参考情報

公開年月	情報源
2012 年 7 月	CVE-2012-3374 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3374 Pidgin というメッセージ交換ソフトの実装漏れによる脆弱性の情報
2012 年 9 月（随時更新）	Metasploit の Exploit Database http://www.metasploit.com/modules/ 独自プロトコル等のオーバーフローに伴うコード作成等の参考となるコード集
2012 年 3 月	ファジング活用の手引き http://www.ipa.go.jp/security/vuln/documents/fuzzing-guide.pdf ファジングに関する詳細な説明

7.12.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

本節で解説した脆弱性は、MFP が実装している独自プロトコルにバッファオーバーフローを引き起こすことが可能なパラメータが含まれているバグである。ここではそのパラメータを悪用し、任意のコードを実行することによりバックドアを設け、MFP 上の OS コマンドを実行できる権限を奪取することを目的とする。影響範囲は、OS コマンドレベルから保護資産が完全に操作できる場合を想定する。

・上記開発ガイド、及び検査ガイドの対策を講じていない機種であること。

【スコアリング】

CVSS 2.0 ベース 基本値： 7.9（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.13 ドライバ用プロトコルを経由した侵入の問題

近年の MFP では、表 7-2 に示すように多数のドライバプロトコルを標準でサポートしており、利用シーンに応じて自由に選択・利用することが可能である。

表 7-2 MFP で利用されている主なドライバプロトコル

ドライバプロトコル	用途	認証手順の有無	暗号化手順の有無
LPR	プリント	-	-
raw9100	プリント	-	-
IPP	プリント	○	○
SMB	プリント、スキャン	○	○
TWAIN	スキャン	○	○
FTP	スキャン	○	○
WebDAV	スキャン	○	○
SMTP	ファクス	○	○
POP3	ファクス	○	○
IMAP4	ファクス	○	○
WSD (Web Service Discovery)	プリント、スキャン、ファクス	○	○
BMLinkS	プリント、スキャン、ファクス	○	○

クライアントから MFP を操作するドライバプロトコルの実装には、数多くの脆弱性が報告されている。これらの脆弱性を悪用することで、MFP の不正な操作（表示画面の詐称、意図しない印刷処理のリクエスト等）や格納されている保護資産への不正アクセスによる情報漏洩やデータ毀損、システムファイルの破壊による MFP の動作不安定化等の様々な攻撃が行われる可能性がある。

また、MFP と接続する機器との互換性を確保することを目的に脆弱性の存在する実装（バージョン）がそのまま利用されている場合も考えられることから、ドライバプロトコルの脆弱性とその影響について開発者・利用者双方で十分認識し、必要な対策を施すことが重要である。

ここではドライバプロトコルにおける脆弱性の例として、LPR をとりあげる。

7.13.1 【攻撃手法とその影響】

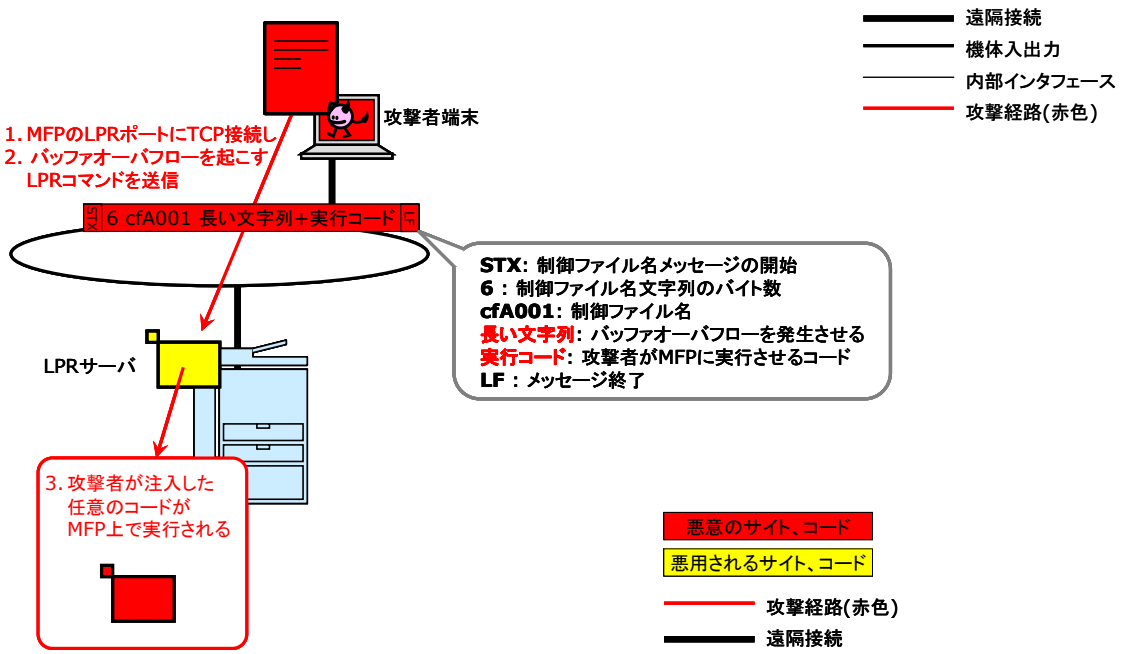


図 7-12 ドライバ用プロトコル LPR を経由した侵入の例

はじめに攻撃者は MFP 上で実行されている LPR サーバの TCP ポート 515 番に TCP 接続する。LPR プロトコルにはユーザ認証の手順はないため、攻撃者は MFP 上の LPR サーバに対して無条件で LPR コマンドを送信できる。

攻撃者は MFP 上の LPR サーバに対して、プリント用の制御ファイルのファイル名として、予想外の長い文字列を与えてバッファオーバーフローを起こさせる。この非常に長い文字列に続けて、攻撃者は任意の実行コードを LPR サーバに送り最後に LPR のコマンド終端文字として改行コード(LF: 0x0a)を送ると、LPR サーバ内でバッファオーバーフローが発生し、攻撃者が送り込んだ実行コードに制御が移る。

下の図 7-13 に、LPR コマンドによる侵入のシーケンス例を示す。

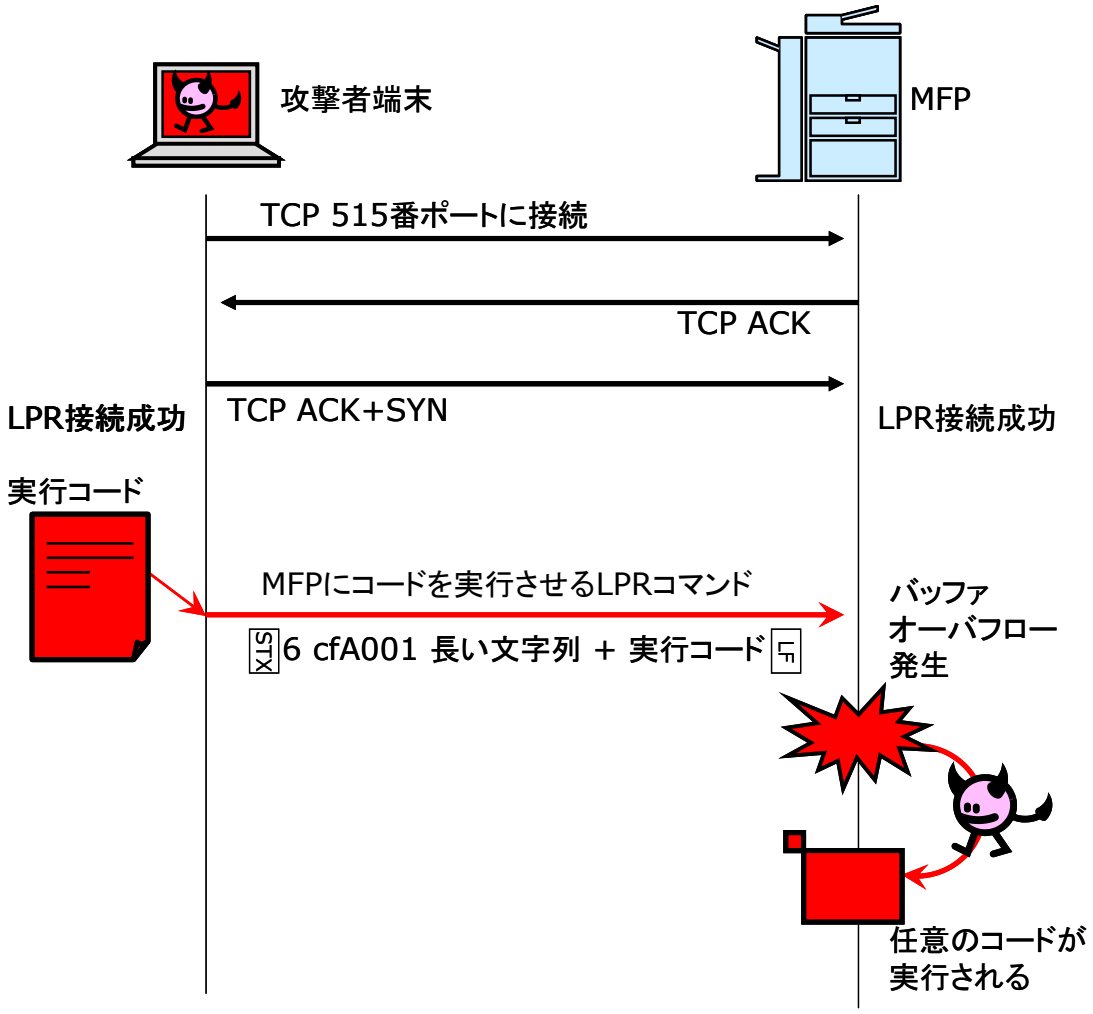


図 7-13 ドライバ用プロトコル LPR コマンドによる侵入のシーケンス例

その結果、MFP 上の LPR サーバを実行している実行環境で、攻撃者による任意のコードが実行させられる。攻撃者が MFP 上で任意のコードを実行できると、MFP 上でさらに別のプログラムを導入して実行させたり、MFP が扱う文書やジョブデータを攻撃者のホストにコピーしたり、MFP から別のホストへの攻撃が可能になる場合がある。また、攻撃者が MFP 上で任意のコードを実行できなかった場合でも、MFP 上の LPR サーバ内でバッファオーバーフローが発生すると、その LPR サーバなどの動作が停止するか、LPR サーバまたは MFP 全体が再起動することがあり、結果としてその MFP の LPR サーバか、MFP 全体が一時的に利用できなくなる。

7.13.2 【原因と考察】

LPR プロトコルでは、印刷を制御するためにいくつかのコマンドが標準化されている。しかし LPR プロトコルのコマンドでは引数となる文字列は LF(Line Feed)コードで区切られているだけでコマンド文字列の長さを示す引数がない。また、転送されるジョブ制御ファイルとジョブデータファイルのファイル名を指定するコマンドがあるが、ファイル名には任意の文字列を指定でき、ファイル名の文字列長を指定する引数がない。また、制御ファイル、ジョブデータファイルともに、転送するファイルの長さをバイト単位で示す引数があるが、テキスト形式による数字での指定となっており、ファイルの長さを示す数字の表現には桁数や最大長に制限がない。

LPR プロトコル仕様を標準化した RFC 1179 では、ジョブ制御ファイル名とジョブデータファイル名の文字列長は 6 文字程度になる仕様になっているが、LPR プロトコル上では文字列長の制限はないため、何文字でも送り込むことができる。

また、テキストで表現された数値の扱いで、予想外の範囲を指定されてヒープメモリのオーバランが発生することもありえる。

このようなテキスト表現による「リラックスした」プロトコル仕様は HTTP や SMTP、SIP のような手順に共通しているが、逆に言えば厳密な形式ではなく自由度が高い分、受信する側での詳細な検査が必要になる。このような、外界から受信したデータの検査処理は「入力値の確認」や「入力データの無害化」、「サニタイジング」などと呼ばれる。IPA ではこの脆弱性と開発上の対策について「セキュア･プログラミング講座」”C/C++言語編・著名な脆弱性対策”で、イメージ図入りの解説をウェブで公開しているので参考にしていただきたい。

この攻撃が成功しやすい前提条件として、注入した実行コードを攻撃者の意図通りに動作させるため、MFP 上の LPR サーバ実行環境が Linux や Windows、VxWorks などのよく知られた OS で、利用されている CPU またはマシン語もよく知られたものである必要がある。また、スタックメモリ上やヒープメモリ上に配置したマシン語を実行できる環境が必要である。

なお、MFP のドライバプロトコルは多数のプロトコルがサポートされており、LPR のような脆弱性はその他のドライバプロトコルにも残存している可能性がある。MFP 製品の開発者は、表 7-2 に示したような MFP で利用されるドライバプロトコルのそれぞれについて、脆弱性の確認が必要である。特に、MFP で利用されるドライバプロトコル（LPR、IPP、raw9100 等）の実装においては、参考情報に示すように数多くの脆弱性が報告されている。MFP と接続する機器との互換性確保等を目的に脆弱性の残る実装を意図せず利用している場合も考えられるため、開発している MFP 製品で利用するドライバプロトコルの実装における脆弱性については常に最新情報を確認し、製品情報サイトなどで利用者に通知しパッチを公開するか、保守契約に基づいて脆弱性に対するパッチを当てたファームウェアに置き換えるなど、適宜対応することが望ましい。一方、MFP の利用者がセキュリティの確保を図るときは、運用環境で利用する必要があるドライバ用プリンタポートを限定し、不要なポートは MFP の設定で停止することが有効である。

7.13.3 対策

【運用ガイド】

1) LPR、raw9100、IPP、SMB、SOAP、WebDAV など、MFP 上で利用するサーバを特定し、MFP 上で利用しないサービスの待ち受けポートを停止しておく。その上で、MFP ベンダの脆弱性情報を確認し、必要な対策があれば実施を検討する。
2) MFP に対してジョブデータを投入できるホストとして、特定のプリントスプールサーバや、スキャンとファクスのゲートウェイサーバなどに限定する。

【開発ガイド】

3) MFP に実装したドライバプロトコルに関して、常に最新の脆弱性を確認し、利用者に通知する。また脆弱性が自社の MFP に影響を及ぼすものであった場合は、通知すると共に脆弱性に対応したパッチやファームウェアを提供する。

【検査ガイド】

4) MFP 上で採用されている全てのドライバプロトコルに対して、各プロトコルの公知脆弱性が該当しないかを確認する。
5) MFP 上で採用されている全てのドライバプロトコルに対して、実装により脆弱性に対応している場合は、正しく仕様どおりに実装されていることを確認する。

7.13.4 参考情報

公開年月	情報源
1990 年 8 月	RFC 1179 Line Printer Daemon Protocol http://tools.ietf.org/html/rfc1179 IETF による LPR のプロトコル仕様。
1998 年 7 月	LPR とはなんですか? http://support.apple.com/kb/TA21876?viewlocale=ja_JP&locale=ja_JP アップルコンピュータのサポート情報より。PAP(Apple 社の AppleTalk 上で利用できるプリントジョブ伝送手順"Printer Access Protocol"と LPR との違いが説明されている。
2000 年 10 月	LPD Vulnerability Issues http://lpd.brooksnet.com/lpd-security.html 次のような指摘と、プリントサーバ側での対策例を示している。 (1)LPR 経由でプリントサーバ上に任意のファイルを作成できる (2)LPR 経由でプリントサーバ上の任意のファイルを削除できる (3)LPR 経由でプリントサーバ上の任意のコマンドを実行できる
2001 年11月	CERT® Advisory CA-2001-30 Multiple Vulnerabilities in lpd http://www.cert.org/advisories/CA-2001-30.html LPR のプリントサーバ側(lpd)の複数の脆弱性。 (1)バッファオーバーフローにより任意のコードが実行させられる (2)プリントサーバ上で sendmail に任意のオプションを指定できる
2006 年 10 月	LPR プロトコルと標準 TCP/IP ポート・モニタの違い http://www.atmarkit.co.jp/fwin2k/win2ktips/809stdprnprt/stdprnprt.html Microsoft 社の TCP/IP ポート・モニタで使われる raw9100 と LPR の違いが説明されている。
2007 年 10 月	US-Cert: Cisco IOS LPD buffer overflow vulnerability: VU#230505 https://www.kb.cert.org/vuls/id/230505 Cisco IOS の LPD で、99 文字を超えるホスト名を入力すると sprintf()の呼出し後にバッファオーバーフローが発生する。
2007 年 12 月	US-Cert: CUPS buffer overflow vulnerability: VU#446897 http://www.kb.cert.org/vuls/id/446897 UNIX 系 OS の印刷システム「Common UNIX Printing System」(CUPS)にバッファオーバーフローの脆弱性があり、任意のコードが実行される可能性があることが報告されている。
2010 年 4 月	Mocha W32 LPD Remote Buffer Overflow Vulnerability http://www.securityfocus.com/bid/39498/info Mocha 社の Windows 用 LPR プリントサーバソフト上で、LPR の制御ファイル受信コマンドで制御ファイル名文字列のバッファオーバーフローにより任意のコードが実行される脆弱性。Python スクリプトによる手順の実証コードがある。

7.13.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは例として、LPR プロトコルにおけるバッファオーバーフローの脆弱性（LPR サーバで任意のコードを実行する。）を悪用して任意のコードを実行することによりバックドアを設け、MFP 上の OS コマンドを実行できる権限を奪取することを目的とする。影響範囲は、OS コマンドレベルから保護資産が完全に操作できる場合を想定する。

・上記対策を実施していない環境であること。

・ファイアウォール等によりインターネットからの LPR 通信が遮断されていること。

【スコアリング】

CVSS 2.0 ベース 基本値： 7.9（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.14 ページ記述言語の脆弱性による問題

ページ記述言語とは、クライアント PC 上で作成された文書や画像等を MFP 等で印刷する際に出力イメージ等の指示や、環境設定等を行うために用いる言語のことであり、PJL（Print Job Language）、PCL（Printer Control Language）、PostScript などを含む。一般に MFP では、これらページ記述言語を用いることでプリントジョブの投入やキューの削除等を行うことが可能であるが、一方で攻撃者により印刷登録されたデータ（保護資産）への不正アクセスによる暴露やデータ毀損、ファイルシステムへの不正アクセスによるパスワードの取得等が行われる可能性がある。ここではページ記述言語の例として PJL をとりあげる。

7.14.1 【攻撃手法とその影響】

PJL の仕様では、PJL コマンドを利用することで MFP の環境設定やジョブ管理、ファイルシステム操作等を行うことが可能である。以下にファイルシステムの操作に関係する PJL コマンドを示す。

表 7-3 ファイルシステム操作に関係する PJL コマンド

PJL コマンド	説明
FSAPPEND	ファイルへのデータの追加や新規作成を行うコマンド
FSDIRLIST	ファイルやディレクトリを表示するコマンド
FSDELETE	ファイルや空ディレクトリを削除するコマンド
FSDOWNLOAD	ファイルのダウンロードを行うコマンド
FSINIT	ファイルシステムを初期化するコマンド
FSMKDIR	ディレクトリの作成を行うコマンド
FSQUERY	エントリの有無を問い合わせるコマンド
FSUPLOAD	ファイルのアップロードを行うコマンド

上記のような PJL コマンドを悪用することにより、他人が登録したデータ（保護資産）の取得による情報漏洩やデータ毀損、ファイルシステムへの不正アクセス等を行うことが可能な場合がある。

実際の MFP に対し、上記のファイルシステム操作に関するコマンド（FSDIRLIST コマンド）を用いてディレクトリ・トラバーサルの手法によりファイルシステムへの不正アクセスを行った例を以下に示す。

```
%-12345X@PJL INFO FILESYS
VOLUME    TOTAL SIZE          FREE SPACE          LOCATION LABEL     STATUS
0:        2929683456          2922577920          HDD                READ-WRITE

%-12345X@PJL FSDIRLIST NAME="0:..¥..¥..¥..¥¥" ENTRY=1 COUNT=128
ENTRY=1
pjl TYPE=DIR
plwform TYPE=DIR
artform TYPE=DIR
seal TYPE=DIR
smb TYPE=DIR
jtpool TYPE=DIR
del TYPE=DIR

%-12345X@PJL FSDIRLIST NAME="0:..¥..¥..¥..¥smb¥¥" ENTRY=1 COUNT=128
ENTRY=1
passwd.txt TYPE=FILE SIZE=243
share.txt TYPE=FILE SIZE=67
```

図 7-14 PJL コマンドを悪用した攻撃（ディレクトリ・トラバーサル）

上記の例は、攻撃者が MFP に対して raw9100（9100/tcp）にてアクセスしてファイルシステム情報を取得し、その情報を基にディレクトリ・トラバーサルの手法を用いてディレクトリ構成情報や保護資産（ここでは passwd.txt）にアクセスすることが可能なことを示している。アクセスできる範囲に保護資産があれば、PJL のコマンドを用いてファイルを取得することも、改ざんすることも可能である。実際にこの攻撃では passwd.txt を取得、改ざんできることを確認した。

ページ記述言語を悪用した場合、上記のような保護資産への不正アクセスのみならず、MFP の画面表示を改竄したり（RDYMSG コマンドの利用）、設定情報の改竄を行ったりすることが可能な場合がある。また、INQUIRE コマンドを用いてバッファオーバーフローを発生させることで任意のコードを実行させる攻撃例も報告されている。この攻撃手法により、MFP に格納された保護資産の暴露や毀損、MFP 自体の破壊等を行うことが可能な場合がある。

PJL の他、参考資料にも示すとおり PostScript においても脆弱性の存在が報告されていることから、開発者はページ記述言語の脆弱性に留意して開発することが望まれる。

7.14.2 【原因と考察】

MFP 上のファイルシステムへ不正アクセスが可能となる原因は、開発者のディレクトリ・トラバーサルへの対応不備と不必要な PJL コマンドの実装である。

ディレクトリ・トラバーサルへの対策としては、攻撃者が MFP へアクセス可能なネットワーク上に存在することを想定して PJL コマンドを利用してアクセスできるファイルやディレクトリの範囲を制限する実装とすることが重要である。また、保護資産や設定情報の漏洩、バッファオーバーフロー等の脆弱性への対策としては、MFP で利用可能な PJL コマンドを制限する（利用できなくしておく）ことが効果的である。

7.14.3 対策

【運用ガイド】

1) MFP に対してジョブデータを投入できるホストとして、特定のプリントスプールサーバや、スキャンとファクスのゲートウェイサーバなどに限定する
2) MFP で利用できる PJL コマンドの一覧を開発者に確認し、不要と考えられるコマンドがあれば、開発者に問い合わせる。

【開発ガイド】

3) PJL コマンドからアクセス可能なファイルやディレクトリを制限する。
4) MFP 製品で利用可能な PJL コマンドを制限する。(利用者にとって必要な機能に限定する)
5) 利用可能な PJL コマンドに関しては情報確認コマンドなどを含め全て実行し、MFP の挙動や、取得できる情報が問題ないことを確認する。

【検査ガイド】

6) ディレクトリ・トラバーサルやバッファオーバーフローなど、PJL コマンドを利用した公開されている攻撃コードを参考に、検査対象の MFP に対して有効な検査用攻撃コードを作成し、挙動や、取得できる情報に問題の無いことを確認する。

7.14.4 参考情報

公開年月	情報源
2003 年 6 月	HP PCL/PJL Reference (Printer Job Language Technical Reference Manual) http://h20000.www2.hp.com/bc/docs/support/SupportManual/bpl13208/bpl13208.pdf HP 社による PCL/PJL の仕様書。
2010 年 3 月	CVE-2010-0619 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0619 PJL INQUIRE コマンドを用いたバッファオーバーフローについて報告されている。
2010 年 11 月	HP LaserJet Directory Traversal in PJL Interface http://www.exploit-db.com/exploits/15631/ PJL コマンドを用いたディレクトリ・トラバーサルについて報告されている。
2012 年 1 月	Hacking MFPs PostScript(um–you've been hacked) http://andreicostin.com/papers/Conf%20-%2028C3%20-%20Hacking%20MFPs%20(part2)%20-%20PostScript_um%20you_ve%20been%20hacked%20-%20SRLabs%20-%20v2.pdf PostScript の脆弱性について報告されている。
2012 年 2 月	MULTIFUNCTION PRINTER VULNERABILITIES http://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf MFP の脆弱性について広く言及されている。

7.14.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは PJL でディレクトリ・トラバーサルにより保護資産へアクセスし、PJL コマンドにより保護資産を取得する攻撃について考察する。以下を前提とする。

・社外ネットワークから直接 MFP へはアクセスできない

【スコアリング】

CVSS 2.0 ベース 基本値： 5.8（警告）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	部分的な影響
可用性	部分的な影響

7.15 ウェブ管理コンソールの脆弱性による問題

昨今の MFP 製品は、MFP のネットワークやプリント設定、印刷機能やジョブやデバイスのステータス管理、バックアップ機能を始めとする各種セキュリティ設定等を行う際、ウェブ管理コンソールから行うことが一般的となっている。通常、ウェブ管理コンソールは、MFP 管理者、一般利用者、保守員等の利用者区分に応じた機能を提供しており、利用者の識別認証とアクセス制御を行うことで、それぞれの利用者区分に応じた機能を利用できるようにするものが多い。したがって、MFP で提供されるウェブ管理コンソールにおいても、ウェブサーバを内部に含む一般的なウェブアプリケーションとして共通の脆弱性への対応が求められる。

7.15.1 【攻撃手法とその影響】

インターネットに公開されているウェブサイトとは異なり、MFP は組織内 LAN に接続され、主として LAN 内に閉じて利用するための配置・設定がなされる。このため、インターネット上の攻撃者が MFP のウェブ管理コンソールにアクセスして脆弱性を突いた攻撃を行うことは通常困難であるが、組織内部に侵入した攻撃者や内部犯行者による保護資産への不正アクセスやウェブアプリケーションの誤使用等を考慮すると、MFP のウェブ管理コンソールにおける脆弱性対策は非常に重要である。

IPA の提供する「安全なウェブサイトの作り方（第 5 版）」では、ウェブアプリケーションを構築する上で留意すべき事項（脆弱性）を以下のように分類し、対応策を提示している。[60]これらウェブアプリケーションの脆弱性への対応は MFP 製品であっても必要不可欠であり、それぞれの脆弱性を考慮した開発と利用者への適切な利用方法の周知が求められる。

1) SQL インジェクション

MFP 内部にデータベースサーバを持ち、保護資産を管理している場合、そのデータベースと連携した MFP 上のウェブアプリケーションは、入力情報を基に SQL 文を組み立てている。この SQL 文の組み立て方法に問題がある場合、攻撃者によるデータベースの不正利用（データの不正閲覧や改竄・消去、認証回避による不正ログイン等）を招く可能性がある。

対応策としては、以下のようなものが挙げられる。

- SQL 文の組み立ては全てプレースホルダで実装する。
- SQL 文の組み立てを文字列連結により行う場合は、エスケープ処理等を行うデータベースエンジンの API[61]を用いて、SQL 文のリテラルを正しく構成する。
- エラーメッセージをそのまま返さない。
- データベースアカウントに適切な権限を与える。[62]

---

60 メールヘッダ・インジェクションの脆弱性については、MFP のウェブ管理コンソールでは用いられる可能性は少ないため、記載を省略する。

61 アプリケーション側で使用している言語やフレームワークで用意されている API についても同様。

62 全オブジェクトに対して更新や削除が行える万能型の権限を持った 1 つのデータベースアカウントを使いまわさない。

2) OS コマンド・インジェクション

MFP の場合、OS コマンドそのものが特殊な場合もあるが、ウェブアプリケーションの入力パラメータチェックが不十分であると、ウェブアプリケーションを開発した言語によっては外部からウェブサーバの OS コマンドを不正に実行されて、データの不正閲覧や改竄・消去、不正なシステム操作等が行われる可能性がある。

対応策としては、以下のようなものが挙げられる。

- シェルを起動できる言語機能の利用を避ける。
- シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。

3) パス名パラメータの未チェック／ディレクトリ・トラバーサル

OS コマンド・インジェクションの一部とも言えるが、外部からのパラメータにウェブサーバ内のファイル名を直接指定しているウェブアプリケーションが存在する場合、ファイル名指定の実装に問題がある場合は攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行う可能性がある。

対応策としては、以下のようなものが挙げられる。

- 外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。
- ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。
- ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。
- ファイル名のチェックを行う。

4) セッション管理の不備

MFP のウェブアプリケーションにおいて、利用者や管理者のログイン状態の維持に利用するセッション ID の発行や管理に不備がある場合、攻撃者にログイン中の利用者や管理者のセッション ID を不正に取得され、その利用者になりすましてアクセスされてしまう可能性がある。

対応策としては、以下のようなものが挙げられる。

- セッション ID を推測が困難なものにする。
- セッション ID を URL パラメータに格納しない。
- HTTPS 通信で利用する Cookie には secure 属性を加える。
- ログイン成功後に、新しくセッションを開始する。
- ログイン成功後に、既存のセッション ID とは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。
- セッション ID を固定値にしない。
- セッション ID を Cookie にセットする場合、有効期限の設定に注意する。

5) クロスサイト・スクリプティング

ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプト等を埋め込まれてウェブサイトの改竄や利用者ブラウザが保存している Cookie の取得等が行われる可能性がある。これにより例えばセッション情報が漏洩する。

対応策としては、以下のようなものが挙げられる。

- ウェブページに出力する全ての要素に対して、エスケープ処理を施す。
- URL を出力するときは、「http://」や「https://」で始まる URL のみを許可す

る。
- <script>...</script> 要素の内容を動的に生成しない。
- スタイルシートを任意のサイトから取り込めるようにしない。
- 入力値の内容チェックを行う。
- 入力された HTML テキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する
- 入力された HTML テキストから、スクリプトに該当する文字列を排除する。
- HTTP レスポンスヘッダの Content-Type フィールドに文字コード（charset）を指定する。
- Cookie 情報の漏えい対策として、発行する Cookie に HttpOnly 属性を加え、TRACE メソッドを無効化する。

6) CSRF（クロスサイト・リクエスト・フォージェリ）

MFP のウェブサーバ上のアプリケーションが、ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たない場合、外部サイトを経由した悪意のあるリクエストを受け入れてしまう場合がある。このようなウェブアプリケーションの作りだと、ログインした利用者は、攻撃者が用意した罠により、利用者が予期しない処理（ログイン後の利用者のみが利用可能な機能の実行や保護資産の改竄・消去等）を実行させられてしまう可能性がある。

対応策としては、以下のようなものが挙げられる。
- 処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。
- 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。
- Referer が正しいリンク元かを確認し、正しい場合のみ処理を実行する。
- 重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。

7) HTTP ヘッダ・インジェクション

リクエストに対して出力する HTTP レスポンスヘッダのフィールド値を、外部から渡されるパラメータの値等を利用して動的に生成するウェブアプリケーションでは、HTTP レスポンスヘッダの出力処理に問題がある場合、攻撃者がレスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃を仕掛ける可能性がある。

対応策としては、以下のようなものが挙げられる。
- ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する。
- 改行コードを適切に処理するヘッダ出力用 API を利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。
- 外部からの入力の全てについて、改行コードを削除する。

8) アクセス制御や認可制御の欠落

MFP のウェブサーバ上のアプリケーションにおいて、利用者や管理者がログイン状態でなければアクセスできないウェブページに、アクセス制御や認可制御の

不備が存在していた場合、攻撃者の利用者へのなりすましや許可されていない機能への不正アクセス等が発生する可能性がある。

対応策としては、以下のようなものが挙げられる。

- アクセス制御機能による防御措置が必要とされるウェブページには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。
- 認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。

上記した観点以外にも、基本的な対策、例えばラジオボタンやリストボックスに無い値を不正に入力されるなどのパラメータに対する想定外の値の入力に対して誤動作を起こさない対策や、エラー時に応答するメッセージに攻撃者が有利になるような情報を含まない、トレース情報などを出力しないといった対策を講じたウェブアプリケーションの開発が必要となる。

参考情報に記述した通り、2012 年には国内 MFP ベンダのウェブ管理画面において、認証回避により管理者権限を奪取できる脆弱性が公開された。ここでは、ウェブ管理コンソールに実在した脆弱性の例として認証 CSRF の脆弱性を示す。

＜ウェブ管理コンソールの概要＞

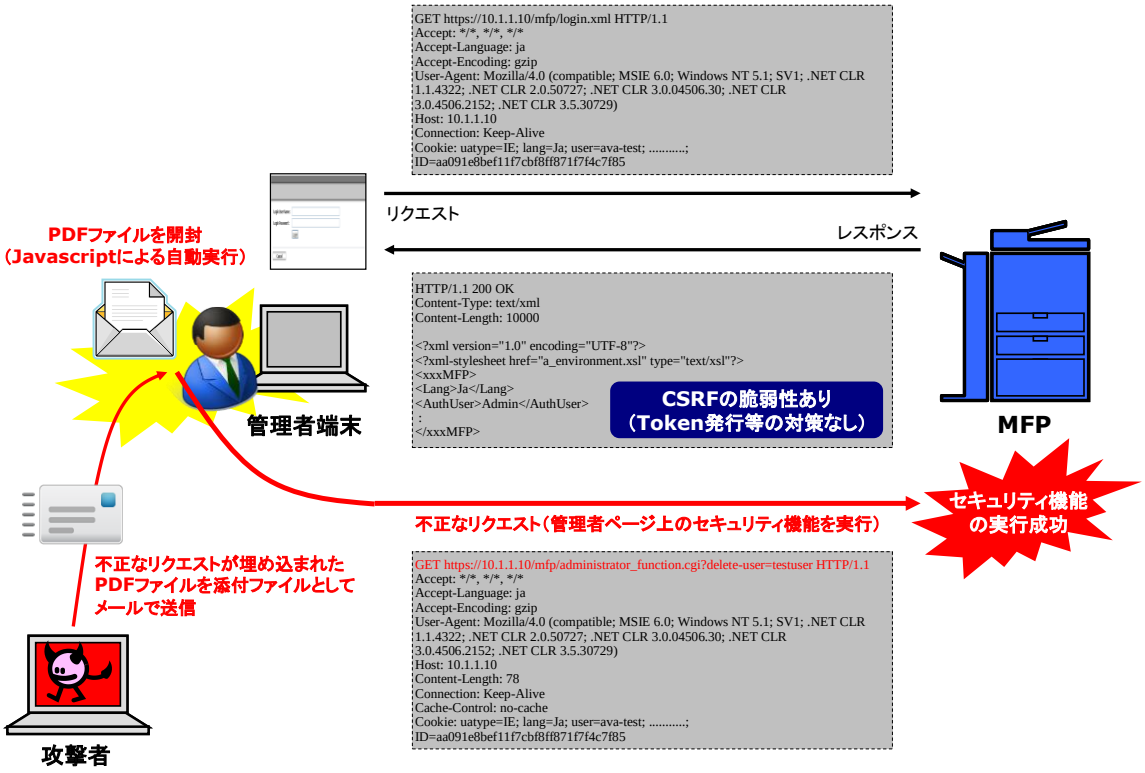
このウェブ管理コンソールでは、トップページにて利用者（管理者等含む）の識別認証とログイン後のセッション管理が適切に行われており、利用者の権限に応じた各種機能を提供している。また、ウェブ管理コンソールへのアクセスは SSL/TLS で暗号化することが可能であり、この場合通信内容を盗聴して取得することは一般的に難しいといえる。

＜ウェブ管理コンソールが提供していた主な機能＞

- 利用者
  利用者情報管理機能、ボックス管理機能　等
- 管理者
  ネットワーク設定機能、HDD 暗号化機能、HDD 一括削除機能、バックアップ・リストア機能、セキュリティモード設定機能　等
- 保守員
  ファームウェアアップデート機能、HDD フォーマット機能、パスワード初期化機能　等

上記のように、このウェブ管理コンソールは適切に識別認証、セッション管理、通信の暗号化等が行われていたが、図 7-15 のように CSRF の脆弱性への対策が行われていなかったため、本来識別認証及び認可された管理者のみが実行可能な各種機能が攻撃者により誘導され実行される可能性があった。この例の場合、攻撃者は管理者に不正な行為を行わせるための別のウェブサイトを作成する CSRF の手法では無く、PDF ファイルを管理者に送りつけ、その PDF ファイルを管理者が閲覧した際に Javascript が自働実行されるという PDF の閲覧ソフトの機能を悪用して、任意の操作を管理者に行わせている。

この攻撃により、利用者情報の漏洩や登録データの暴露や毀損、HDD 一括削除等の管理者機能の不正実行やセキュリティモードの設定解除、不正なファームウェアへの書き変え等、ウェブアプリケーションで提供されている MFP に対する機能が、一定の条件を満たせばすべて攻撃者により実行される可能性があった。



1

図 7-15 CSRF による攻撃の例

7.15.2 【原因と考察】

CSRF の脆弱性をついた攻撃が可能となる原因は、前述したクロスサイト・リクエスト・フォージェリに対する対策（例：Token 等のセッション ID 以外の識別 ID を用いて MFP 側で照合する等）が行われていないためである。本来識別認証及び認可された利用者のみが実行可能な各種機能を提供する場合は、CSRF の脆弱性への対策が必要である。

本節で解説したウェブアプリケーションにおける CSRF などの脆弱性は、7.11.3 節で取り上げた一般的なウェブの脆弱性検査ツールによりある程度確認することが可能である。セッション管理などに関してはツールではほとんど確認されないため、手動検査により本当にセッション値がチェックされ利用されているか、セッション値の再利用や予測が可能な実装になっていないかなどについて確認する必要がある。

7.15.3 対策

【運用ガイド】

1) ウェブ管理コンソールに関する脆弱性情報がベンダ等から提供された場合は、その影響範囲を考慮して提供されたパッチの MFP への適用やブラウザ設定変更等を実施する。
2) SSL/TLS 等の暗号化通信にてウェブ管理コンソールにアクセスする。
3) MFP のセキュリティガイドラインに従い、セキュリティの確保可能なネットワークに MFP を設置する。(ガイドラインが存在する場合)

【開発ガイド】

4) 参考情報に示す文献等を参考に、MFP のウェブアプリケーションを開発する。
5) MFP で実装しているウェブサーバやウェブアプリケーションで利用している言語など、関連するアプリケーションに関する最新の脆弱性を常に確認し、利用者に通知する。また脆弱性が自社の MFP に影響を及ぼすものであった場合は、通知すると共に脆弱性に対応したパッチやファームウェアを提供する。

【検査ガイド】

6) MFP で実装しているウェブサーバやウェブアプリケーションで利用しているスクリプト言語などに対して、公知脆弱性が該当しないかを確認する。
7) ウェブ脆弱性検査ツールと手動検査を併用し、ウェブアプリケーションに脆弱性が存在しないことを確認する。

7.15.4 参考情報

公開年月	情報源
2012 年 3 月	IPA:安全なウェブサイトの作り方(改訂第 5 版) http://www.ipa.go.jp/security/vuln/websecurity.html 安全なウェブサイト作成に係る留意点や対策チェックリスト等がまとめられている。
随時更新	OWASP(The Open Web Application Security Project) https://www.owasp.org/index.php/Category:OWASP_Guide_Project ウェブアプリケーション開発における留意事項等が記載されたガイドライン。上記の他、本サイトにはテストに関するガイド等有益な情報が多数掲載されている。
随時更新	The Common Attack Pattern Enumeration and Classification (CAPEC) http://capec.mitre.org/index.html 様々な攻撃パターンがわかりやすく分類されてまとめられている。
2011 年 4 月	CVE-2011-1531 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1531 EWS の脆弱性について報告されている。
2011 年 4 月	CVE-2011-1533 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1533 クロスサイト・スクリプティングの脆弱性について報告されている。
2012 年 4 月	CVE-2012-1239 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1239 認証回避が可能な脆弱性が報告されている。

7.15.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは､管理用ウェブアプリケーションのセッション管理に CSRF に対する脆弱性があることを想定し､攻撃者が CSRF を利用して管理者に不正な命令を実行させる攻撃について考察する。またここでは管理者に保護資産を含めた MFP 全体のバックアップ及びリストアの機能を実行させることにより機密性、完全性、及び可用性に全面的な影響がある場合を想定する。

【スコアリング】

CVSS 2.0 ベース 基本値： 7.9（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.16 ウェブベースの保守機能の悪用から起こる問題

一部のウェブベースの保守機能を提供している MFP において、攻撃者がこの保守インタフェースを悪用することにより、MFP 内部の情報と MFP に関連する他システムの情報が攻撃者に不正に入手される。

7.16.1 【攻撃手法とその影響】

MFP の保守機能は、一般的にはコピー枚数やトナーの残量、故障診断と故障部品の交換修理がある。このうち、故障したハードディスクを交換するために、以下のような機能がある。[63]

1) MFP 内部の文書ファイル、アドレス帳を一括してバックアップする機能
2) MFP 内部の文書ファイル、アドレス帳を一括して所定のファイルから上書きする機能
3) MFP 内部の文書とアドレス帳を一括して削除、上書き削除する機能

1)文書ファイルをバックアップする機能では、MFP 内部のハードディスクに格納されている文書を一括して MFP の外部に取り出すことができる。この機能は MFP 内部の HDD が故障したときに、新しい HDD と交換するために必要な機能である。

2)の MFP 内部の文書ファイルなどを所定のファイルから上書きする機能は、1)で保存しておいた HDD のバックアップデータを使って HDD の内容を復元する機能であり、「リストア(restore)」と呼ばれている。

3)の MFP 内部の文書とアドレス帳を一括して削除、上書き削除する機能は、交換対象の廃棄が必要なハードディスクの内容を消去するために利用される。また、MFP を廃棄するときに MFP 内部の情報が第三者に漏洩しないようにするためにも利用される。

しかし、上記のような MFP 内部のインタフェースでは、MFP の保守作業を行うために MFP が設置された場所に出向かなければならないため、ネットワークを経由して遠隔地から保守を行うための機能も提供されている。

下の図 7-16 の左上の保守用端末のように、保守機能は一般的には組織内のネットワーク上の端末から実行する。また、開発者や保守員が提供する外部からの保守サービスを利用している場合は、図 7-16 の右上にあるような組織外のネットワークを通じて遠隔保守のための通信を行っている。また、MFP 本体に直接接続する保守インタフェースを使う場合もある。

[63] これらの機能は一部 MFP においては管理者機能として利用者に提供されているが、本節では保守機能として実装されている MFP を想定している。

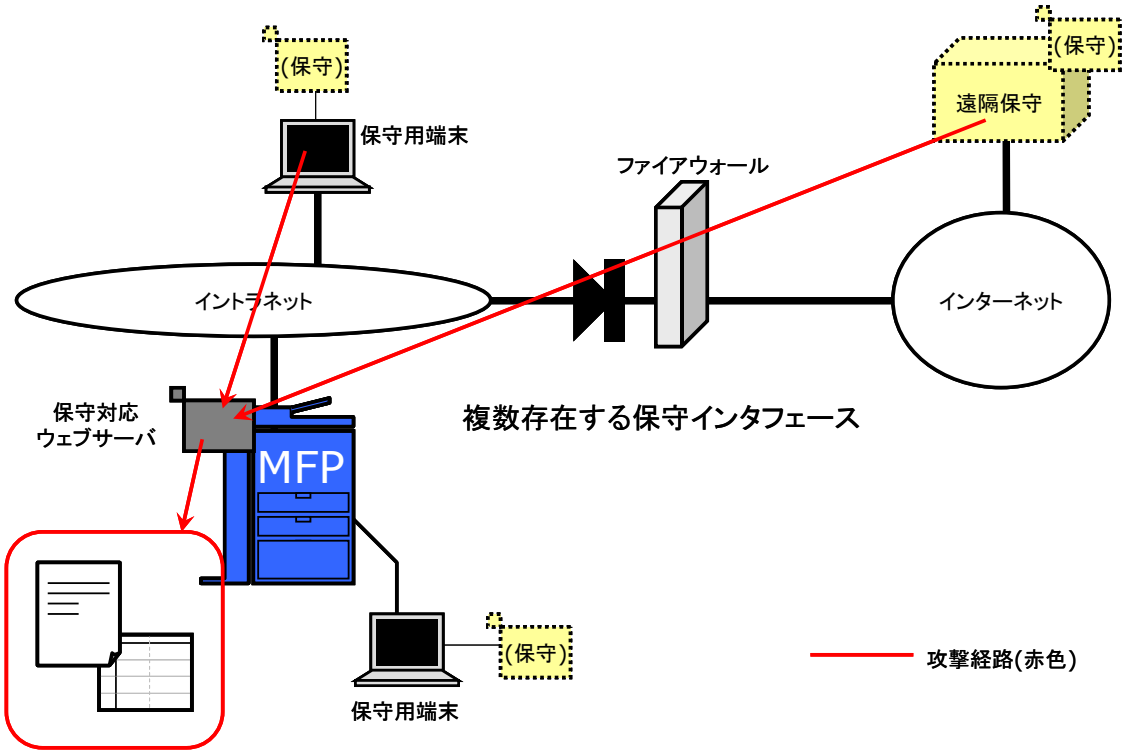


図 7-16 保守インタフェース(http)へのアクセス方法例

このように保守機能には複数の経路がある。このうち、ここでは保守員が利用者のイントラネット内で MFP のウェブベースの保守機能を保守用端末のウェブブラウザから利用する場面を想定する。

下の図 7-17 は、ウェブベースの保守機能を利用する管理者のウェブブラウザに CSRF を行い、攻撃者である利用者が認証なしで、保守員のセッションを悪用し MFP 内のデータを消去させる操作を保守員に行わせる例である。

保守員が保守用のウェブサイトで認証を済ませ保守機能のページを開く。ブラウザが保守機能のページを開いたままの状態で、赤線で示すような特定の URL を開かせる JavaScript コードを管理者のブラウザに注入することで、認証手順なしで、MFP の内部データのバックアップなどの保守機能を実行させられる。

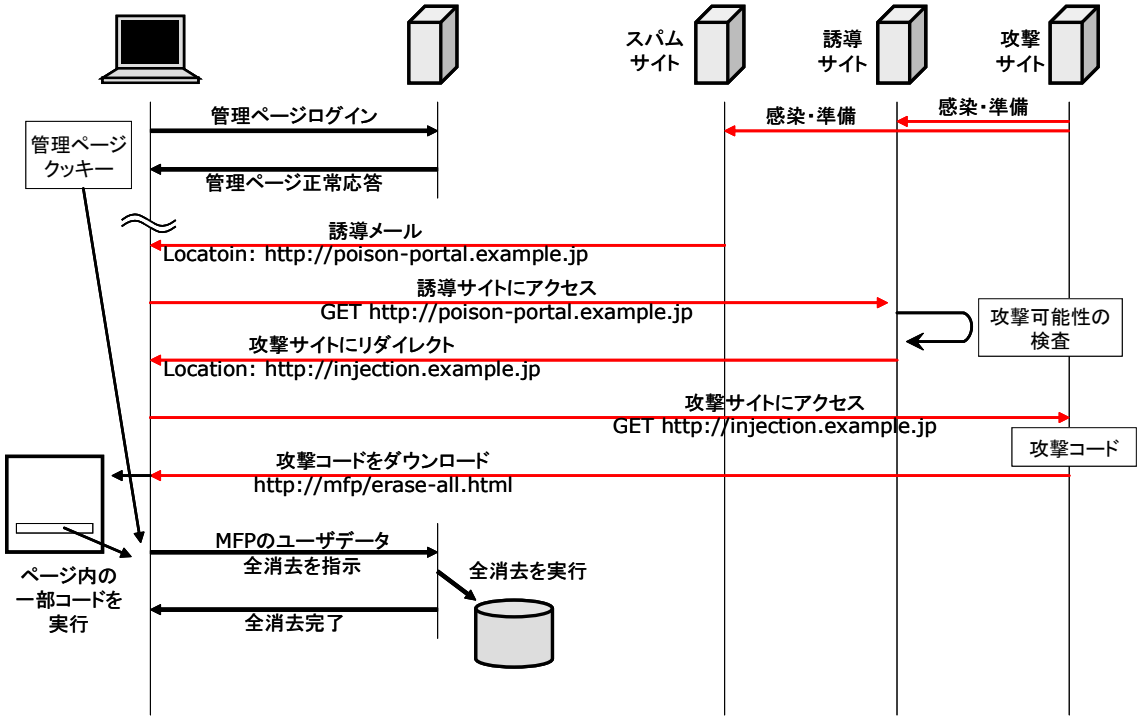


図 7-17 CSRF を利用した保守インタフェース悪用のシーケンス例

この攻撃手法にはいくつかの条件がある。まず大前提として保守用ウェブサイトに CSRF に対抗できるセッション管理機能が組み込まれていないこと。そして保守員が保守機能を利用するためのページであらかじめ開いたままにしている状態中か、保守用ウェブサイトにログオフを管理しない等の不備がある必要があり、保守端末上にセッション情報が残っていることである。その上で保守端末のブラウザを特定サイトに誘導し、攻撃コードをダウンロードさせる必要である。また攻撃者が保守用ウェブサイトのコマンド体系を推測できている必要もある。

攻撃機会の観点では、7.15 節で解説した様な管理者や他の利用者への CSRF よりもさらに少ないと言える。しかし保守員の動作や作業が見て取れるような状況では、可能性が無いとは言い切れない。

なお、遠隔地から保守作業を行う保守サービスでは、MFP 自体が保守サイトにアクセスし、簡易的に VPN のような専用接続を設定する方法などがあり、IP アドレス変換やファイアウォールを設定した利用者のネットワークにおいても容易に利用可能である。

7.16.2 【原因と考察】

MFP 機器本体の保守インタフェースは MFP 機器本体内部の一部の故障部品を交換するときなどのため、内部情報をバックアップするなどの重要機能を持っている。一般的には MFP ベンダの保守担当者や委託業者が保守作業を行うが、利用者の利便性のため、一部の保守機能が利用者側に開示されている場合がある。また、専用の保守用ソフトウェアが一部利用者に開示されている場合もある。

こうした保守機能は便利な反面、HDD の交換や MFP を廃棄するための機能については、MFP の取扱説明書で明確に記述されていない場合もある。部品の交換は MFP の保守員の役目だが、保護資産などを含む HDD の内容については利用者に管理責任があるため、HDD の交換を行う際は利用者か HDD の内容をバックアップ

する必要がある。ただし本調査では、HDD の内容の取り扱いについては保守員が交換時にバックアップとリストアをすることもありえると仮定した。利用者としてはHDDの交換作業やバックアップとリストアの方法や注意について一般的には知識がない場合も多く、保守員に依頼するメリットが大きい。

また、MFP に対して高可用性を求める利用者のニーズに対応するため、保守機能がネットワークを経由した外部に開放されている場合も想定される。しかし、保守機能が社内ネットワークや外部に公開されれば、当然攻撃者から狙われる対象となり、本節で例示したようなウェブアプリケーションの保守機能であれば、7.15 で解説した多くの脆弱性に対策した強固な作りで提供されなければならない。

このように MFP の利便性が高まると、同時に脅威も増大する。特に保守インタフェースが MFP 本体内部の専用インタフェースだけではなく、ネットワーク上に開放されることで、侵入される可能性が高まる。また、HDD の内容を保守員のような第三者が扱うことに対して、どのような保護や対策がとれるかも問題になる。

現在のところ、すべての MFP ベンダがバックアップ機能を提供しているわけではないが、MFP の利用者へのサービス停止時間を短くし、高度な MFP の機能をいつでも継続的に利用するために、バックアップ機能を活用するための対策がいくつか考えられる。主な対策としては、バックアップと消去などの重要な保守機能はローカルな保守機能からしか利用できないなど、機能毎にアクセスできる範囲を特定する、バックアップデータそのものが暗号化などで保護されること、などがあるだろう。

7.16.3 対策

【運用ガイド】

1) 運用環境に応じて、必要なければ外部からの保守機能への接続を停止する。
2) 保守機能が複数存在し、ウェブアプリケーションを利用した保守機能以外でも運用可能な場合、ウェブアプリケーションを利用した保守機能は停止する。

【開発ガイド】

3) 外部からの保守機能を有効化することによる危険性の利用者への周知
4) セキュアな保守機能の実装と、セキュリティ設定のデフォルト化

【検査ガイド】

5) 保守インタフェースがウェブサーバにより実装されている場合、通常のウェブコンソールと同様、7.15 節で解説したような脆弱性対策が実装されていることを検査する。

7.16.4 参考情報

公開年月	情報源
2009 年 6 月	CWE-352 クロスサイト・リクエスト・フォージェリ (リクエスト強要攻撃) http://jvndb.jvn.jp/ja/cwe/CWE-352.html

7.16.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

本節で仮定した通り、ウェブベースの保守機能を保守員がイントラネットから利用した際、攻撃者が保守員と平行して CSRF によりバックアップ、及びリストアなどの機能を実行し MFP 上の全ての保護資産へアクセスする攻撃を想定する。

・上記した運用ガイドの対策がとられていない環境であること。
・保守員の挙動を攻撃者が確認できる環境であること。

【スコアリング】

CVSS 2.0 ベース 基本値： 7.9（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

7.17 外部認証の利用による問題

MFP 内の保護資産への適切なアクセス制御を行うために、MFP は利用者の識別認証機能を有している。一部の MFP は、その認証機能を外部の認証サーバに委託し、その結果を元にアクセス制御を行う「外部認証」の機能を実装している。この外部認証の機能は、MFP を導入するオフィス内に利用者の識別認証のシステムが既に構築されている場合、ユーザ管理の一元化による利便性の観点から、利用される場合が多いと考えられる。その場合、外部認証サーバに存在するいくつかの脆弱性[64]に対しては利用者が運用環境に併せて適宜パッチを当てる等の対応を行うことが要求される。しかし脆弱性の観点はそれだけではない。外部認証を用いる MFP の仕組み自体に脆弱性が存在することも考えなければならない。

7.17.1 【攻撃手法とその影響】

本節では、MFP に外部認証の連携先として多く実装されている Microsoft Active Directory を用いた仕組みをもとに説明する。MFP の外部認証は、Active Directory 以外にも、Windows NT4.0 以前で利用されていた NTLM[65]と連携できるものもある。しかし NTLM は仕様が古く、中間者攻撃に対して脆弱性であることが知られている。この脆弱性は考察するまでもなく NTLM を MFP の利用者認証に利用した場合にも適用できる。よって本節では一般的な利用では問題が無い Active Directory の認証の仕組みを用いた場合に関する攻撃手法について考察する。

補足:Kerberos 認証の概要

Active Directory のユーザ認証には Kerberos という仕組みが使われている。Kerberos は図 7-18 Kerberos 認証のイメージに示したように、利用者の利用者端末、利用者がアクセスしたいサーバ、及び KDC（Key Distribution Center）から成る。KDC は利用者の利用者端末の（パスワードから計算する）秘密鍵、サーバの秘密鍵を全て保持している。KDC を利用した Kerberos 認証は、利用者が目的のサーバとセキュアな通信を行うためのセッション鍵を共有する手段として適用される。以下に Kerberos 認証の概要を説明する。

64 例えば Microsoft Active Directory にはバックドアの脆弱性があることが知られており、ディレクトリサーバの情報が信頼できるとは限らない。
65 Windows NT LAN Manager authentication

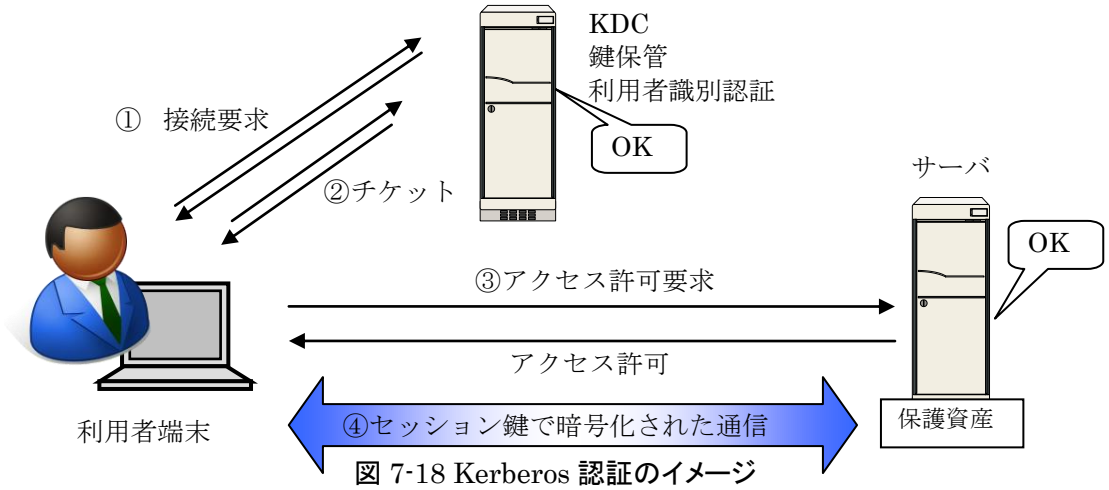


図 7-18 Kerberos 認証のイメージ

1) 利用者が、利用者端末からサーバにアクセスしたい場合、まず KDC との間でお互いに秘密鍵を知っていることを確認する手続きにより利用者を認証する。このとき秘密鍵は利用者のパスワードから計算により求める。
2) KDC は認証した利用者に対してサーバとやりとりするためのチケットを利用者端末に送付する。チケットにはサーバの鍵で暗号化した情報が付加されている。
3) 利用者端末はチケットを確認しサーバに送付。サーバはチケットを自身の秘密鍵で復号し確認することにより KDC に許可された利用者と判断し、「アクセス許可」を利用者に与える。
4) 以降は、チケットに暗号化して含まれていたセッション鍵で、利用者端末－サーバ間の暗号化通信が行われる。

MFP の保護資産への不正アクセス

この仕組みの中で MFP の利用者を認証する場合の攻撃について検討した。その結果、攻撃者が MFP の接続されたネットワークにアクセスできる環境であれば、攻撃者はパスワードを知らない任意の利用者になりすまし、その利用者の保護資産へアクセスすることが可能であることが、実機検証により確認できた。

この攻撃手法は、現時点では一般に公開されていないものである。また、非現実的な手法とは言い切れず、特段高い攻撃能力も必要としないものである。
そのため、対策を講じていないベンダ・機種が存在していた場合には、攻撃手法の詳細を公開することで攻撃の機会を増やしてしまうことが懸念されるため、本報告書では詳細な攻撃手法及びその原因については割愛する。

7.17.2 対策

攻撃手法の詳細は割愛したが、実機検証により MFP で「外部認証」の仕組みを用いた場合に、保護資産への不正アクセスが可能になる攻撃が成立することが確認できた。外部認証機能を利用する際に、そのような攻撃を防ぐために考慮すべ

き対策を示す。

【運用ガイド】

1) サーバで稼動しているサービスの生存監視、不正な ARP パケットの監視等がきるような環境で MFP を運用する。
2) 外部認証に係るサーバのサービスや OS の脆弱性情報を確認し、必要に応じてパッチを当てる等の対策を行う。

【開発ガイド】

3) 外部認証を利用した場合でも、本体認証と同等のセキュリティが確保できるように、外部認証経由で保護資産へアクセスする際のセキュリティ機能を追加する。

【検査ガイド】

4) MFP 外部の環境を利用した MFP 内部への攻撃についても網羅的に確認し、攻撃できる可能性があれば侵入検査を実施する。

7.17.3 参考情報

公開年月	情報源
2012 年 1 月	A Backdoor in the Next Generation Active Directory http://www.exploit-db.com/wp-content/themes/exploit/docs/18415.pdf Microsoft Active Directory に潜むバックドアの脆弱性に関する解説記事
2004 年 5 月	NTLM 認証とマン・イン・ザ・ミドル攻撃 http://www.st.rim.or.jp/~shio/csm/ntlm/ NTLM による認証サーバが簡単に成りすましできることの解説
2011 年 12 月	CVE-2011-3406 Active Directory Buffer Overflow Vulnerability http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3406 認証された利用者がバッファオーバーフローにより任意の命令を実行できる脆弱性
2011 年 6 月	CVE-2011-1264 Active Directory Certificate Services Vulnerability http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-1264 Active Directory Certificate Services ウェブの XSS に関する脆弱性
2011 年2月	CVE-2011-0040 Active Directory SPN Validation Vulnerability. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0040 不正なリクエストによる DOS の脆弱性

7.17.4 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

・詳細を割愛した攻撃手法が成功するような環境を想定する。
・上記した運用ガイドの対策がとられていない環境であること。

【スコアリング】

CVSS 2.0 ベース 基本値： 5.4（警告）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	中
攻撃前の認証要否	認証操作が不要
機密性	部分的な影響
完全性	部分的な影響
可用性	部分的な影響

7.18 マルウェア感染ファイルの MFP への混入による問題

マルウェアとは、対象機器で動作し、不正または有害な作用を及ぼす意図で作成されたプログラム等の総称である。本書で扱うマルウェアは、感染した MFP や利用者端末に対して保護資産を不正に漏洩、改ざんさせるプログラムを対象とする。MFP がマルウェアの攻撃を受ける代表的な例としては、7.7 節で解説したようなファームウェアアップデート機能を用いてマルウェアを組み込んだ不正なファームウェアをアップロードする場合などがある。また、動作中の感染した MFP に接続する利用者端末へのマルウェアの伝播も想定される。本節では MFP に保存されたマルウェアが利用者端末に伝播する可能性について考察する。

7.18.1 【攻撃手法とその影響】

MFP にマルウェアを混入させる方法としては、以下が考えられる。

- ファームウェアアップデート機能を不正に利用してマルウェアの仕組まれたファームウェアをアップロードする。（7.7 節）
- 7.14 節で解説した PJL を用いたファイルアップロード機能を用いてマルウェアの仕組まれたプログラムをアップロードする。
- 7.5 節で解説した手法で奪取した保守インタフェースの機能から任意の不正なプログラムをアップロードする。
- 7.9 節で解説したような脆弱な SDK を利用して、MFP 内部にマルウェアを保存する。

ここでは上記のいずれかの手段により MFP を不正に動作させることで、マルウェアが添付された文書ファイルが利用者に送付されるメールのキューに格納された状態を仮定する。

キューに格納されたマルウェアを利用端末に伝播させる手法は、一般的な MFP の機能を用いる。近年の MFP にはファクス受信した画像や MFP でスキャンした画像を自動でメールに添付し、利用者端末に配信する機能が付いている[66]。その機能は任意の利用者として実行しても良いし、直接不正な手段で命令を実行しても良い。命令の実行は 7.14 節の PJL を用いたバッファオーバーフローなどが利用できると考える。また、不正に改変した USB を刺すことによりオートランの機能により命令を実行できるかもしれない。

メールに添付されたマルウェアを実行するよう利用者を誘導するためには、利用者が信頼する「メールタイトル」や「送信元」を探りこれらを付加した偽メールを作成する。それでもセキュリティを意識した利用者であれば、偽のメールタイトルや送信元アドレスから察知し、不正な添付ファイルを実行することは考えにくい。しかし通常利用している正規の MFP を送信元として、正規のタイトルで、ファイルが添付されたメールが送られてきた場合、利用者は比較的その添付ファイルを開く（実行する）かもしれない。

[66] 各国内ベンダの MFP が Scan to Mail や Scan to E-Mail という名称でメールの添付ファイルとして文書データを配布する機能を展開している。

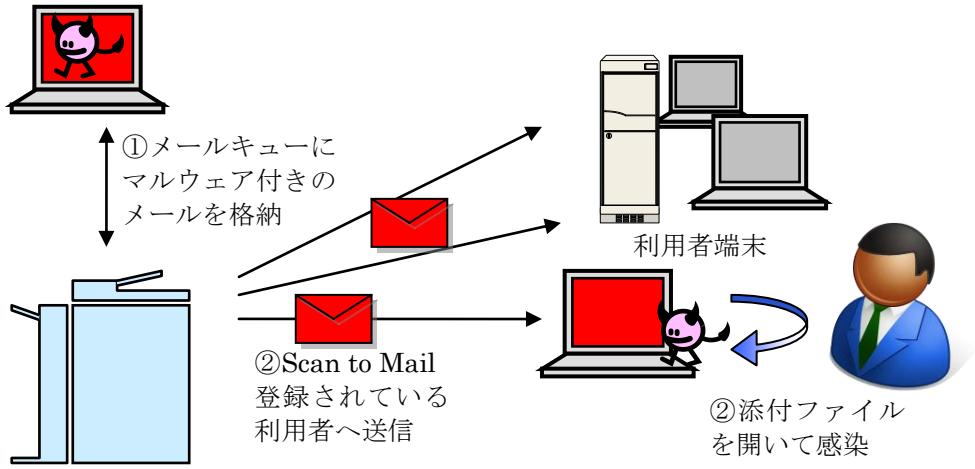


図 7-19 MFP から利用者端末へのマルウェア伝播のイメージ図

補足:MFP が攻撃の影響を受けるマルウェアの存在

本節で説明しているような MFP が感染媒体となり、マルウェアを利用者のオフィス内に伝播させる攻撃が考えられる一方、利用者端末がマルウェアに感染した影響で利用者端末の不正動作により MFP が影響を受けるマルウェアも報告されている。2011 年には米国商工会議所が標的型攻撃により狙われた。更に 2012 年には感染した利用者端末により MFP より大量の印刷が行われるというプリンタウィルスが有名となった。このような、感染した利用者端末からネットワーク接続されている MFP が多量の印刷命令を受けて正常動作の範囲で影響を受ける場合に関しては、MFP の機能で防ぐことは一般的に困難である。

補足:MFP 自体が感染するマルウェア

次に、MFP に混入したマルウェアにより MFP 自身が感染する（MFP 上の OS やファームウェアが影響を受ける）可能性もある。不正なファームウェアへの書き換え以外にも、文書に添付されたスクリプトにより MFP 自体が感染することもある。2003 年には、Windows ベースの組込み OS を利用していた MFP がマルウェアに感染した事例がある。つまり、オフィス内の 1 台の利用者端末にこのようなマルウェアが存在するだけで、MFP は外部ネットワークから見えない、管理者は不正を行わないといった前提は、成立しなくなってしまう。

2012 年現在確認できる MFP ベンダの公開文書には、図 7-20 MFP ベンダのセキュリティに対する考え方の例 の通り、MFP に搭載した OS がマイナーであるためマルウェアへの感染の可能性は低いとの記載が、いくつかの MFP ベンダ[67]で見受けられる。

しかし、例えばマルウェアの埋め込まれたスクリプトを添付した文書が MFP に保存され、MFP 付属パネルのブラウザから当該文書を開いた場合。そのブラウザ上のアプリケーションに脆弱性があれば、MFP のファームウェアや OS がマルウェアによる影響を受ける可能性はある。更に近年では MFP の OS を汎用の組込み Linux に移行した MFP も確認できる。開発者は、文書ファイル上からスクリプトを削除する、もしくは MFP 上で有効化しないなどの機能面での対策を実装するこ

[67] 参考情報に、MFP ベンダ各社のセキュリティに対する考え方の公開文書を例示した。

とが望ましいのかもしれない。

・・・since the majority of viruses and worms exploit vulnerabilities in Windows-based computers. ベンダ名 **MFPs use non-standard operating systems** other than Windows. **Consequently, they are immune** to these viruses and worms.・・・

図 7-20 MFP ベンダのセキュリティに対する考え方の例

7.18.2 【原因と考察】

一部の MFP は、スキャンやファクス受信したデータを PDF ファイル、Microsoft Word、及び Microsoft Excel 形式で保存し利用者に送付できる機能を持っている。その機能を悪用すれば、利用者端末にメールの添付ファイル等の形でマルウェアの仕組まれた文書を送付することが可能かもしれない。ただし通常の使用方法では、紙やファクスを入力として PDF 等の形式に変換され保存されるデータにスクリプトを埋め込むことは不可能である。この攻撃が成立するためには、前提として MFP が既に不正な状態であること、例えば攻撃者となる利用者が、仕込まれた不正な手順を使ってメールのキューに直接スクリプト付文書データを保存するといった手続きが必要になる。

利用者が行うべき対策は、覚えのないファイルが添付した MFP からのメールを開かないといったポリシーの整備と、そのポリシーの周知徹底が必要となる。また、万が一添付ファイルを開いてしまった場合の対策として、常に、利用者端末上の PDF リーダーなどのアプリケーションを脆弱性が無いバージョンに保つことも必要である。

7.18.3 対策

MFP 上の文書ファイルを自動で利用者端末等に送付する機能は、利用者の利便性を追及したものである。この脆弱性は MFP の機能的脆弱性に依存するものではなく、利用者のオフィスのセキュリティポリシやその運用に依存する。ここでは解説した攻撃に対して、利用者が考慮すべき対策を示す。

【運用ガイド】

1) 覚えの無い添付ファイルに関しては、例え信頼する送信元からのメールであっても開かないといったポリシーを運用する。
2) アプリケーションの脆弱性情報を参照して、利用者のオフィス内で利用しているアプリケーションを常に問題の無いバージョンに保つ。
3) ファクスやスキャンしイメージを保存する形式として利用しないものは、MFP の設定で OFF にする。

開発ガイドとしては、MFP のメールキューから利用者端末に文書データを送る際に、文書データに埋め込まれたスクリプトが自動的に削除されるなどの機能を実装することが考えられるが、不正なファームウェアへの書き換えによってその機能が無効となる場合も考えられる。ここでは、補足として記載した MFP 自身がマルウェアの影響を受けることへの対策は以下が考えられる。但し、保守機能を利用した不正な手順での MFP へのマルウェア混入などは、各節で解説した機能的対策を講じて対応する必要がある。

【開発ガイド】

4) MFP のファームウェアや通信制御を行うソフトウェアにマルウェアの影響を受けるような脆弱性が無いことを、ソースコード分析ツール等で確認する。
5) MFP の操作パネル上で、文章確認等を行った際に、文書に添付されたスクリプトが実行されない実装とする。
6) 公開されている攻撃コードを改造することにより、MFP が実装している OS が影響を受けることがないか確認する。

【検査ガイド】

7) MFP で動作するアプリケーションに関しても検査する。例えばパネルにブラウザが搭載されている MFP では、ブラウザ自体もしくはリンクして動作するアプリケーションに関して、悪用し MFP の保護資産に影響を与えることが無いかを検査する。
8) 同系統の OS 用に公開されている攻撃コードを利用して、MFP に影響が無いか検査する。

7.18.4 参考情報

公開年月	情報源
2012 年 2 月	MULTIFUNCTION PRINTER VULNERABILITIES http://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf MFP に関するマルウェア混入を含めた脆弱性報告
2012 年 6 月	Malware attack spread as email from your office's HP scanner http://nakedsecurity.sophos.com/2012/07/24/malware-hp-scanner/ スキャナから利用者にマルウェアを送信するという話題
2012 年 5 月	PostScript: Danger Ahead?! http://hackinparis.com/slides/hip2k12/Andrei-PostScript%20Danger%20Ahead.pdf マルウェアを MFP に格納し伝播する手法の概要
2011 年 2 月	2005 年の BlackHat で公開された USB 経由の攻撃に関する記事 http://news.mynavi.jp/articles/2005/08/03/blackhat4/index.html USB を自動実行されるデバイスとして誤認識させる手法
2011 年 12 月	China Hackers Hit U.S. Chamber http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html 米国商工会議所が中国から攻撃され不正な印字がされた事件に関する記事
2012 年 6 月	プリンタウィルス http://blog.trendmicro.co.jp/archives/5415 2012 年に流行したプリンタウィルスに関する記事
2007 年 10 月	やはり出てきた、例のアドビの脆弱性を突く「PDF ウイルス」 http://itpro.nikkeibp.co.jp/article/NEWS/20071024/285333/ PDF の脆弱性をついた添付ファイルによるファイル感染
2010 年7月	The SHARP Security Suite http://files.sharpusa.com/Downloads/ForBusiness/DocumentSystems/MFPsPrinters/Security/cop_dow_securitybro.pdf MFP の OS がマルウェアの影響を受けにくいとの主張
2006 年 7 月	HP のセキュリティに関するコメント http://h20424.www2.hp.com/program/wdyhts/enterpriseprint/sg/en/pdfs/whitepaper/HP_security_solutions.pdf

	MFP の OS がマルウェアの影響を受けにくいとの主張
2006 年 2 月	Lexmark technical white paper (Security) http://www.lexmark.com/vgn/images/portal/Security%20Features%20of%20Lexmark%20MFPs%20v1_1.pdf MFP の OS がマルウェアの影響を受けにくいとの主張
2009 年 4 月	Samsung 「MFP Security Overview」 http://www.samsung.com/us/it_solutions/healthcare/_pdf/5_MFP%20Security%20Overview%20Rev0A.pdf MFP の OS がマルウェアの影響を受けにくいとの主張
2003 年 10 月	Windows の脆弱性及びコンピュータウイルスへの対応について http://www.fujixerox.co.jp/company/news/release/2003/0919_msblast.html MFP に搭載された OS がマルウェアの影響を受けた例

7.18.5 深刻度と攻撃能力評価(参考値)

【攻撃の前提条件】

ここでは、補足で解説した MFP 自体がマルウェアに感染する攻撃について考察する。2003 年に発生した Windows 組込み OS を持つ MFP が影響を受けるマルウェアと同様に、MFP の組込み OS に対して任意のコードが実行可能である脆弱性を利用したマルウェアをオフィス内のネットワークに流すことにより、MFP が感染する場合を想定する。また、この脆弱性を利用してバックドアを設置できる機能を持つマルウェアが一般に公開されている場合を想定する。

・上記対策を実施していない利用環境であること

【スコアリング】

CVSS 2.0 ベース 基本値： 8.3（危険）

攻撃元区分	隣接ネットワークから攻撃可能
攻撃条件の複雑さ	低
攻撃前の認証要否	認証操作が不要
機密性	全面的な影響
完全性	全面的な影響
可用性	全面的な影響

8. その他のセキュリティ対策

8.1 開発者の製造、配付時の問題

7 章で解説した各脆弱性への攻撃手法では、MFP の設計資産そのものへの攻撃や、製造または配付プロセスへの攻撃については「開発拠点のセキュリティや製造及び配付プロセスにおけるセキュリティは開発者により保証されている」ことを前提としている。ここでは、開発者が保証すべきこれらのプロセスに対する攻撃の側面について説明する。もし開発者の製造や配付のプロセスにおいて適切なセキュリティが確保されていなければ、7 章で解説したような攻撃手順を追わなくてもより容易な手段で攻撃が成立してしまう。例えば、7.7 節の保守インタフェースから不正なファームウェアをアップロードする攻撃では、攻撃者の手元にファームウェアのソースコードが無いために、公開されているバイナリから特殊なハードウェアを用いたリバースエンジニアリングを行う必要があった。しかし、開発者へのソーシャルエンジニアリング手法の適用、管理不備を突いた設計資産の抜き取り、製造・配付プロセスにおける管理システムのホールの悪用などにより、攻撃者がソースコードを直接入手した場合、リバースエンジニアリングの必要は無くなり、攻撃ははるかに容易になる。それ以外にも 7.5 節で解説した秘密のインタフェースへのアクセス手順が記載された内部資料の漏洩などが開発者の製造や配付のプロセスにおいて発生し得る。開発者は、開発拠点のセキュリティや利用者に MFP 製品が提供されるまでの製造や配付プロセスのセキュリティを確保するために、これらのプロセスにおいて攻撃を受ける可能性についても十分に意識し、各プロセスにおける適切な運用手段を設計し、これを保証していかなければならない。

8.2 ガイダンスによる利用者への情報提供

本書で解説した様な脆弱性に対して、MFP の設定やセキュリティポリシ、またその組み合わせにより利用者が対応する場合も想定される。その場合、開発者は、MFP をセキュアな運用状態にするための設定や操作、例えばログを記録するためには利用者による設定が必要な場合や、MFP をセキュアな状態で運用するために利用者が従わなければならない事項について、ガイダンスに明記するなどの手段により確実に利用者へ注意喚起しなければならない。

8.3 MFP に関する出口対策

本節で考察する出口対策とは、オフィス内のネットワークに接続されたサーバやクライアント PC がマルウェアに感染した場合を想定した対策であり、感染した場合でもオフィスから外部へマルウェアの感染が拡大することを防ぐことが目的である。出口対策ではマルウェアの外部への拡大だけではなく、マルウェアを利用した最終的な攻撃目標である保護資産の外部への漏洩も考慮する必要がある。

IPA の提供する「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（改定第 2 版）」[68]では、バックドアの検知やマルウェア拡散を防止する観点から、上記出口対策を行う上でのポイントを以下のように分類し、対応策及び実装手法を

[68] http://www.ipa.go.jp/security/vuln/documents/newattack.pdf

提示している。

1)　サービス通信経路設計

- ファイアウォールの外向き通信の遮断ルールを設定する。
- ファイアウォールの遮断ログを監視する。

2)　ブラウザ通信パターンを模倣する http 通信検知機能の設計

- http メソッド利用バックドア通信を遮断する。

3)　RAT[69]の内部 proxy 通信(CONNECT 接続)の検知遮断設計

- RAT の CONNECT 確立通信の特徴を利用し、内部 proxy ログで監視する。

4)　最重要部のインターネット直接接続の分離設計

- 最重要部がインターネットへ直接接続しないように VLAN 等を設計する。

5)　重要攻撃目標サーバの防護

- AD を管理する管理セグメントを防護する。
- 利用者から見える AD のサービスに対するパッチ当てを行う。

6)　スイッチ等での VLAN ネットワーク分離設計

- 利用者セグメントと管理セグメントを分離設計する。

7)　容量負荷監視による感染活動の検出

- スイッチ等の負荷やログ容量等における異常検知を行い、セキュリティ部門と連携する。

8)　P2P 到達範囲の限定設計

- 対策 3)、4)の対策に加え、不要な RPC[70]通信の排除を目的としたネットワーク設計を行う。

7.18 節で解説した通り、MFP はマルウェアの感染源となる可能性があるため、オフィス内の他のサーバやクライアント PC と同様に出口対策の管理対象としなければならない。また MFP の設置環境にもよるが、ファクス回線などファイアウォールを介さず直接外部の回線に接続される経路も存在する。マルウェアに感染した MFP はそれらの回線を利用して保護資産を外部に送信するかもしれない。出口対策を行う場合は、ファイアウォールなどで管理できないこれらの回線に関しても、対策を行う必要がある。

---

[69] Remote Access Trojan / Remote Administration Tool。侵入したシステムを遠隔から操作するツールで、潜伏活動や窃取活動に用いられる。Poison ivy、Gh0st RAT など。

[70] Remote Procedure Call。ネットワーク接続されたリモートのコンピュータ上で動作しているサービスを呼び出し、処理を依頼する機能。接続時に動的に新たなポートを割り当てて利用する機能を持っている。

9. 新機能に関する脆弱性の考察

MFP ベンダは近年、従来クライアント端末 PC 向けに展開していたアプリケーションのスマートフォンやタブレットへの実装や、クラウド環境と連携したシームレスな文書管理など、新しいサービスを展開している。これらのサービスは利用者の利便性を向上するものであり、4 章で説明した MFP 利用時のデータワークフローが新たに追加されるものではない。スマートフォンやタブレットは利用者端末の一つであるし、クラウドは通信システムの延長である。しかし例えばクラウドでは外部認証に加えて、その認証情報を使ったクラウドサービスの利用という認証連携が行われる。そこで本章では認証連携における新たな脆弱性の観点に着目し、クラウド環境への展開時の影響を含めて考察する。具体的には、法人向けに展開されているサービス、及び 7.17 節で解説した外部認証で利用する Active Directory による認証と連携して、クラウド上のストレージにデータをセキュアに保管し、支社や別拠点の MFP から出力するようなサービスを対象とする。

なお、本章は、ベンダが提供する MFP や関連するクライアントソフトウェアに関する攻撃手順の解説では無いため､機能的に MFP が対応できる脆弱性ではない。利用者がクラウド環境と連携した MFP の利用を検討する際の参考として、公開されている SAML の実装不備により発生した Active Directory とクラウドサービスの認証連携に関する攻撃手順に関して解説する。

9.1 SAML の実装不備による問題

クラウド環境においてセキュリティを確保するための技術的な観点は大きく 2 つある。1 つはクラウド上のストレージに保管される保護資産の機密性、完全性の確保であり、もう 1 つは適切な利用者認証である。

ストレージに保管される保護資産に関しては、暗号化による機密性確保、パリティー用のディスクを用いた冗長化による完全性確保、及び秘密分散法を用いた計算量的なセキュリティの確保といった機密性と完全性をバランスさせて実現する方法が一般的であり、実際多くのクラウド業者がこれらの技術的手段を組み込んだサービスを収容している。

認証に関しては、企業内で運用している Active Directory による利用者認証との連携（シングルサインオン）を実現する技術として、SAML[71]が有名である。SAML は 2002 年に 1.0 版が承認された認証連携技術であり、現在では Google 等のクラウド事業者で採用されている。[72]SAML2.0 の認証連携の標準的な手順は図 9-1 のイメージとなる。

[71] Security Assertion Markup Language

[72] 他にも WS-Federation や、コンシューマー向けの OpenID といった技術があるが、本書では解説しない。

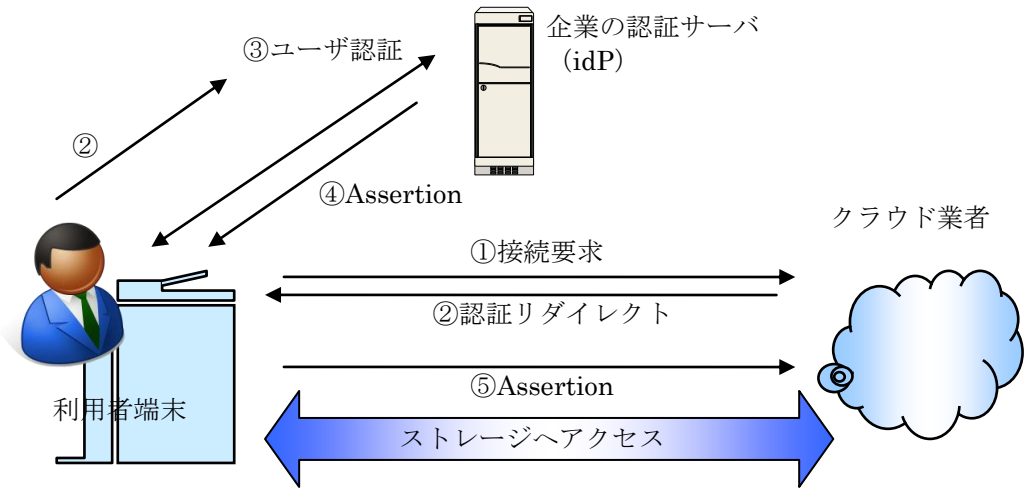


図 9-1 Active Directory とクラウドサービスの認証連携イメージ

利用者が利用者端末からクラウド上の保護資産にアクセスする際、アクセスのタイミングで認証要求を社内の認証サーバ（Active Directory と連携した idP と言われる認証サーバ）にリダイレクトする（図 9-1 の①～②）。認証サーバは利用者に向け Assertion を発行する（図 9-1 の③～④）。利用者は Assertion をもってクラウド上のサービスにアクセスし、Assertion の検証を経てクラウド上でも認証された利用者として保護資産にアクセスすることが可能となる（図 9-1 の⑤）。

9.1.1 【攻撃手法とその影響】

本節では、SAML の実装不備による脆弱性[73]を利用し、攻撃者が上述した認証連携を行う利用者としてクラウド上の当該利用者の保護資産にアクセスする攻撃に関して解説する。この攻撃にはネットワークレベルの中間者攻撃（MiM）を用いる。攻撃者はパケットを操作し、利用者端末に対してはクラウドと偽り、クラウドからの通信に対しては利用者と偽ることにより、最終的に当該利用者としてクラウド上は認証され、当該利用者の保護資産にアクセスすることができる。図 9-2 の④番や⑤番で idP から受け取ってクラウド側に送信する Assertion には利用者や接続先の識別情報が入っているため、本来 SAML は MiM を防止できるプロトコル仕様である。しかし当該クラウドサービスで実装されていた SAML は、簡略化したために MiM への対策が不完全であったため、この攻撃が成立する。この攻撃は任意の利用者がクラウド上の保護資産にアクセスするための認証作業を行っている際に MiM を行う必要があるため、攻撃できる機会は少ないかもしれないが、攻撃自体はスクリプト等を準備すれば難しくは無い。

[73] http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-3891

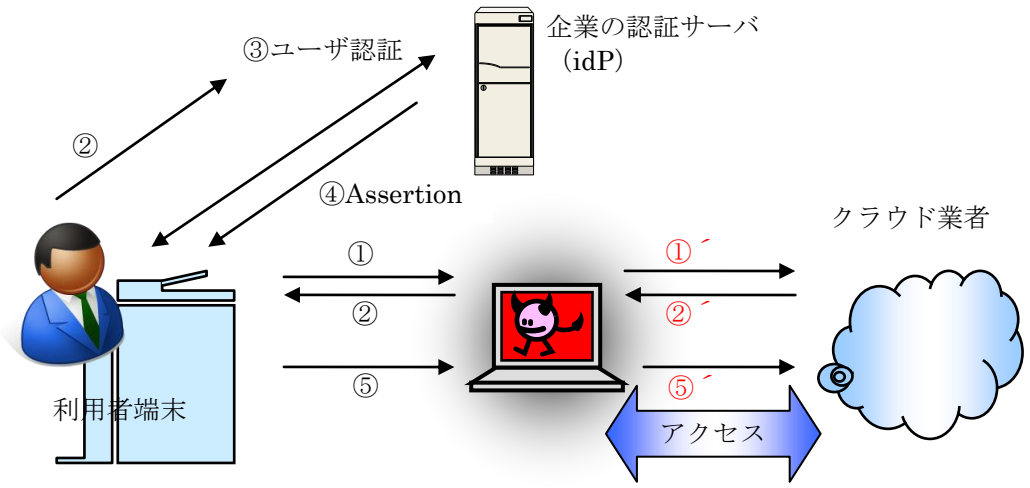


図 9-2 MiM による不正認証イメージ

9.1.2　対策

本章で解説した攻撃に対して、利用者が考慮すべき対策を示す。

【運用ガイド】

1) クラウドサービスのストレージに保存される保護資産が、暗号化や秘密分散などの安全な方法で保存されることを確認する。
2) クラウドサービスのストレージ上のデータが分散管理され、障害発生時においても完全性が確保されることを確認する。
3) クラウドサービスと利用者の認証連携において、MiM 等の攻撃に脆弱な実装をクラウドサービス側が提供していないことを確認する。

クラウドサービスを利用するうえで考慮すべき項目は、例えば Open Government Cloud consortium のサイトに記載されている。MFP との連携に関わらずクラウドサービスを利用する際は、クラウドサービスを利用することによる様々なリスクを把握するためにも事前に一読することが望ましい。

9.1.3　参考情報

公開年月	情報源
2012 年 1 月	SHARP CLOUD SOLUTION http://www.sharp.co.jp/print/solution/cloud/ 各種利用者端末からコンビニ等の MFP からプリントできるサービスの紹介
2012 年 4 月	コニカミノルタの PageScope Mobile の記事 http://www.konicaminolta.jp/about/release/2012/0403_02_01.html スマートフォンやタブレット向けの MFP ドライバ&クライアントソフトの記事
2011 年 1 月	クラウド時代に求められる認証連携とアカウント管理技術を学ぶ http://enterprisezine.jp/iti/detail/2754 シングルサインオンとアカウント管理に関する解説記事
2011 年 11 月	Google や Dropbox のセキュリティ事故とクラウドセキュリティガイドラインに学ぶクラウドの選び方 http://web-tan.forum.impressrd.jp/e/2011/11/09/11249

適宜更新	OASIS Security Services (SAML) TC https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security SAML の技術委員会のサイト
2008 年 10 月	Formal Analysis of SAML 2.0 Web Browser Single Sign-On:Breaking the SAML-based Single Sign-On for Google Apps http://www.ai-lab.it/armando/pub/fmse9-armando.pdf

10. まとめ

MFP は、保護資産を扱うオフィスでの利用において多くの脆弱性を考慮しなければならない製品の 1 つである。MFP の HDD や SSD に保管される保護資産は、オフィス内のファイルサーバと同等のセキュリティが保たれている必要があり、利用者や管理者に提供されているウェブサイトを初めとするインタフェースは、それぞれインジェクションやバッファオーバーフローといった攻撃の可能性を排除しなければならない。その意味ではオフィス内のファイルサーバやウェブサーバと同等にセキュリティを意識した運用が求められ、このような運用を可能とするセキュリティを確保できる機能を搭載していなければならない。

V2.0 の調査報告書では、MFP の利用者、開発者及びセキュリティ機能の確認を行う評価者が認識すべき脆弱性について具体的に解説した。本報告書は、MFP やプリンタに関して CVE に報告されている 2010 年度以降の全ての脆弱性の観点を網羅するよう考慮した。それらの多くは海外 MFP 製品に対して発覚した脆弱性であり、セキュリティを意識した環境での利用を前提とした日本の MFP 製品に関しては、殆ど脆弱性が報告されていないことを本調査過程で確認した。

しかし本報告書で解説した攻撃手順のうちのいくつかは、日本の MFP ベンダの MFP に対する実機検証で攻撃が成功し、実際に日本の MFP にもいくつかの脆弱性が存在することを確認した。それらの脆弱性は利用形態によっては顕著化しないかもしれない。利用者がセキュリティを意識した MFP を調達する際には、利用環境やオフィスのセキュリティポリシに鑑み、懸念される脆弱性に関して問題が無いことを開発者に確認することが望ましい。

今後、新たな機能追加や外部サービスとの連携に伴い、MFP に対する脆弱性も新たに発見され、現在では非現実的な攻撃手法に対する簡単な攻撃手法が公開されていくことが考えられる。MFP が日本を代表するセキュリティ製品として世界中で利用され続けるためには、利用者、開発者それぞれが継続的に脆弱性情報を確認し、対策していくことが必要となる。

デジタル複合機のセキュリティに関する調査報告書 V2.1
独立行政法人情報処理推進機構 技術本部 セキュリティセンター
2014 年 6 月