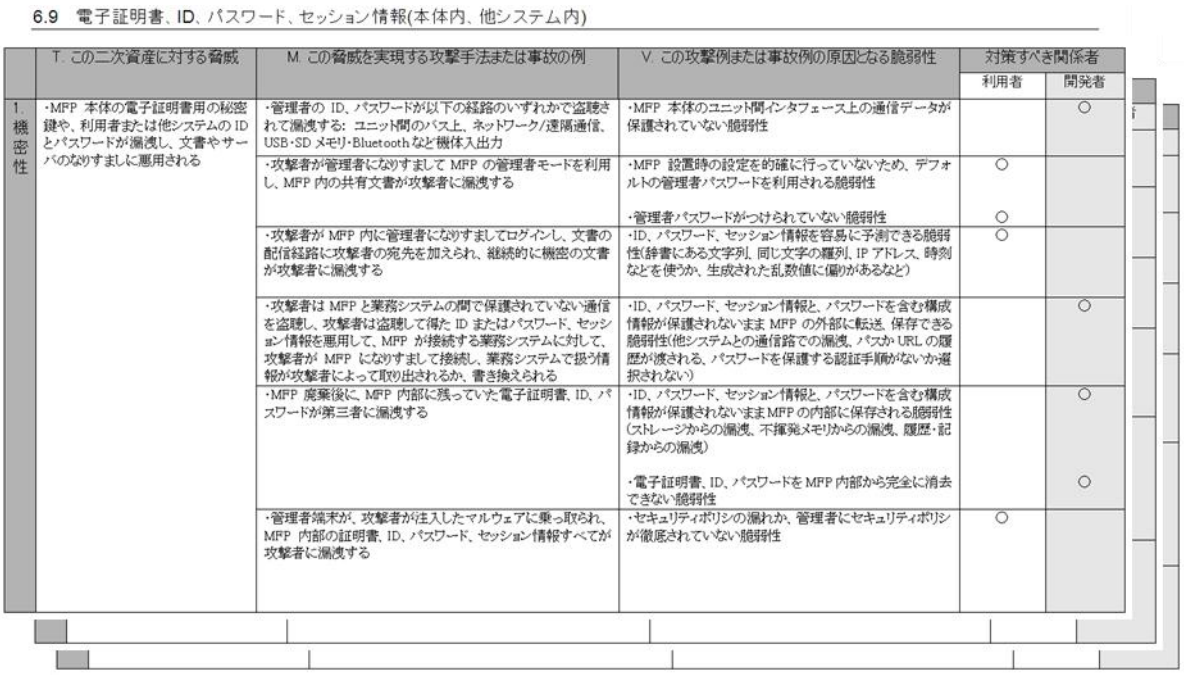
別紙

■調査報告書の概要

本調査報告書では、デジタル複合機の用途や機能、データの流れを整理し、守るべき資産を明確にしたうえで、それらに対する脅威や脆弱性を網羅的に識別しています。
また、それらの脅威についての詳細な解説や対策についても述べています。

- **デジタル複合機の脅威・脆弱性リスト**

デジタル複合機における守るべき資産を特定した上で、それらに対する脅威を網羅的に洗い出し、原因となりうる脆弱性をリスト（図 1 参照）として提供します。
各脆弱性については、利用者が運用環境で対策すべきものと、開発者がセキュリティ機能を実装することで対策すべきものを分類しており、調達者がデジタル複合機を購入する際や安全な運用のために考慮すべき事項が明確となります。



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避択されない)		○
		・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	○	

図 1：デジタル複合機の脅威・脆弱性リスト（一部抜粋）

- **脆弱性の詳細解説**

上記のリストに示した脆弱性の中で、特に近年話題となっている脆弱性（表 1 参照）について、単なる脆弱性データベースの探索にとどまらず、実機での検証や開発者へのヒアリングなどの手法を用いて調査を行い、具体的な攻撃手法を例示して解説しています。また、対策方法について、利用者向けの「運用ガイド」、開発者向けの「開発ガイド」、およびセキュリティ検査者向けの「検査ガイド」に分けて留意点を記載し、それぞれの立場において脆弱性対策を検討する際に参考としやすくなっています。

別紙

表 1：新たに調査したデジタル複合機に関する脆弱性とその問題の概要

脆弱性の項目	問題の概要
記録媒体のデータ保護に関する問題 SSD 搭載による情報漏えいの問題	HDD や SSD などの記録媒体を攻撃者が取り出し、保存される機密文書のデータ、管理者や利用者のパスワード、複合機の設定情報などが漏えいしてしまう。
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	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が海外の Q&A サイト等で公開されてしまっている。
工場出荷時の設定に戻されることによる問題	工場出荷状態に戻す操作が公開されている製品があり、工場出荷時の設定がセキュリティを考慮していない場合には問題となる。
ファームウェアアップデート機能の悪用による問題	不正なファームウェアにアップデートすることで、複合機の不正な動作の誘発や、保護資産への不正アクセスが可能となる。
組込み OS の脆弱性による問題	組込み OS 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・改竄や、サービス不能攻撃を受ける可能性がある。
SDK[1]（Software Development Kit）に関する脆弱性	SDK の不備を利用し、悪意のあるアプリケーションをアップロードすることで、保護資産への不正アクセスが可能となる。
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	利用者端末に導入するプリンタドライバなどに関して、近年多くの脆弱性が報告されている。
複合機の独自プロトコルに懸念される脆弱性	標準化されたプロトコルと異なり、ベンダが独自に開発もしくは改造した通信プロトコルは、検査ツールでは脆弱性が発見されない。また、思いがけない部分に脆弱性に繋がるバグがある可能性がある。
ページ記述言語[2]の脆弱性による問題	攻撃者により保護資産となる印刷登録されたデータへの不正アクセスやデータ毀損、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。
ウェブ管理コンソールの脆弱性による問題	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などの可能性がある。
ウェブベースの保守機能の悪用から起こる問題	複合機内部の情報や、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可能性がある。
外部認証の利用による問題	複合機が接続されたネットワークに攻撃者がアクセスできる環境であれば、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となる。
マルウェア感染ファイルの複合機への混入による問題	マルウェアに感染した複合機に接続すると、利用者端末に影響が伝播する可能性がある。

本報告書では、表 1 に示した脆弱性の他に、今後の普及が予想されるクラウド環境におけるデジタル複合機の脆弱性についても考察しています。

[1] デジタル複合機本体の機能拡張を目的とした利用者アプリケーションの開発環境。
[2] PC 上で作成された文書や画像等を複合機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