プレスリリース
2010 年 8 月 30 日
独立行政法人情報処理推進機構

デジタル複合機の脆弱性に関する調査報告書の公開

～多機能化するデジタル複合機に潜む脆弱性の多角的な調査～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、「ITセキュリティ評価及び認証制度[1]」において、多くのセキュリティ評価が実施されているデジタル複合機（Multi Function Peripheral、以下MFP）に関して脆弱性の調査を行い、報告書を 2010 年 8 月 30 日（月）から、IPAのウェブサイトで公開しました。

URL：http://www.ipa.go.jp/security/fy21/reports/mfp/index.html

近年、MFPにおいては、従来のコピーやプリントといった基本的な用途に加え、ネットワークからの利用、各種メディアへの対応など、利便性を向上させるための多機能化・高性能化が進んでおり、オフィスなどの情報システムにおいて文書データを扱う主要なIT製品として利用されています（図 1参照）。

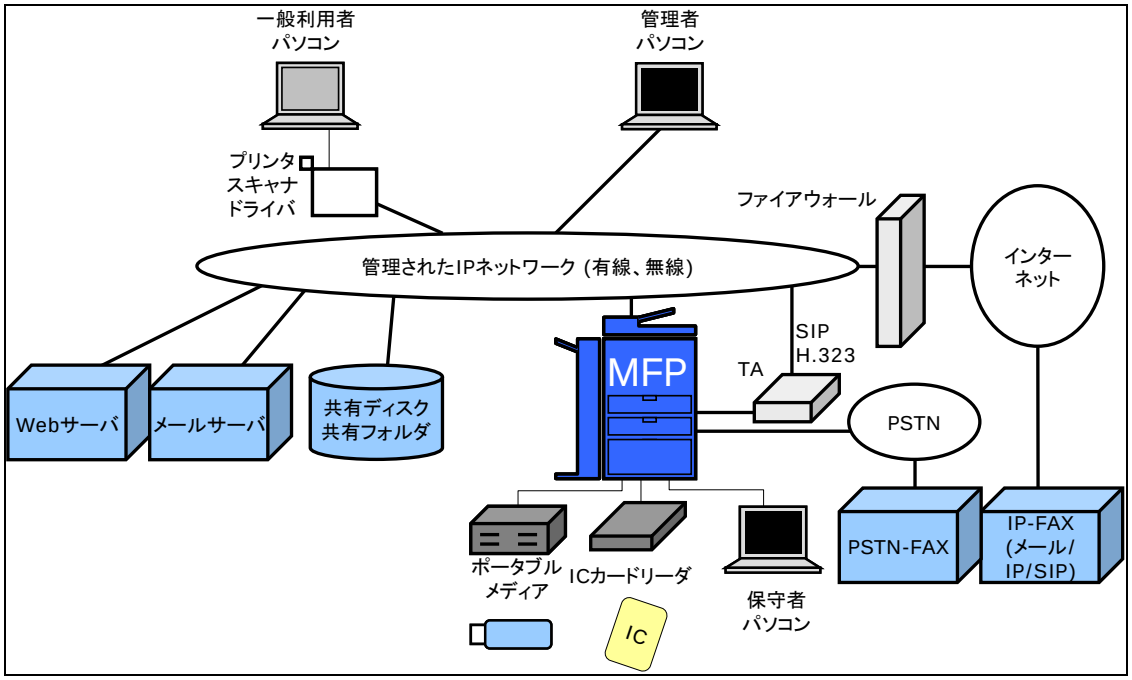

図 1　MFP のシステム構成例

MFP は多機能化に伴い、情報セキュリティに対する要求が高まっており、IPA が運営する「IT セキュリティ評価及び認証制度」では、現在までに多くの MFP のセキュリティ評価が実施されています。

MFPは、今後も様々な情報システムへ対応するため、更なる多機能化が進み、IPv6[2]ネットワークなど多岐にわたる利用環境で使用されることが予想されます。それに伴い、情報セキュリティの面でも、今まで想定されることがなかった利用環境での脅威などを考慮する必要が生じます。

そこで IPA では、MFP の多様な利用環境における脅威・脆弱性を網羅的に洗い出し、今後の MFP のセキュリティ評価に活用することにより、「IT セキュリティ評価及び認証制度」の更なる水準向上を目

[1] IT 関連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/IEC15408 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である IPA が認証する制度

[2] Internet Protocol Version 6：アドレス空間の増大、セキュリティ機能の追加などが施された次世代のインターネットプロトコル

的とした調査を実施しました。

本報告書では、ソフトウェア、ハードウェア、通信システムなどMFPに関する 16 種類の情報資産毎に、ISO/IEC 27001[3]の情報セキュリティの要求事項 7 タイプ（機密性、完全性、可用性、真正性、責任追跡性、否認防止、信頼性）[4]を破る想定から脅威を洗い出し、脅威の発生に至る攻撃手法または事故の例を挙げ、その原因となる脆弱性を網羅的に調査し、約 200 件を脅威・脆弱性リストとしてまとめました（図 2参照）。

	MFP内ソフトウェア に対する脅威	この脅威を実現する 攻撃手法または事故の例	この攻撃例または事故例の 原因となる脆弱性
1.機密性	・MFP内部の実行前の格納された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
		⋮	⋮
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
		⋮	⋮
≀	≀	≀	≀
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	・保守者が実施する、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
		⋮	⋮

図 2　MFP の脅威・脆弱性リスト（一部抜粋）

また、MFPに関する代表的な 6 件の脆弱性[5]について、原因、攻撃手法とその影響、対策となる運用・実装ガイドを詳細に解説しています。

IPA としては、本報告書を「IT セキュリティ評価及び認証制度」に活用するとともに、多機能化が進む MFP の脆弱性に関して各 MFP ベンダーが有効な対策を講じ、MFP 利用者に、より安全性の高い製品が提供されるようになることを期待します。

本書（全 154 ページ）は、次の URL よりダウンロードの上、ご参照ください。
URL：http://www.ipa.go.jp/security/fy21/reports/mfp/index.html

■本件に関するお問い合わせ先
IPA　セキュリティセンター　情報セキュリティ認証室　山里／中村
Tel: 03-5978-7538　Fax: 03-5978-7548　E-mail: jisec@ipa.go.jp
■報道関係からのお問い合わせ先
IPA　戦略企画部　広報グループ　横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

[3] 情報セキュリティマネジメントシステムの国際標準規格（対応する日本工業規格は JIS Q 27001:2006）
[4] 情報セキュリティの要求事項 7 タイプの定義：http://www.isms.jipdec.jp/doc/JIP-ISMS111-21.pdf
[5] 次の MFP の機能に関する脆弱性：①プリンタ、スキャナ、ファクスなどのユニット間でのデータの盗聴、②ドライバ用プロトコルを経由した侵入、③複数配信を一括して実行する機能、④多数のプロトコルに含まれる脆弱性、⑤遠隔保守インタフェースの悪用、⑥着脱式媒体を利用した MFP の構成変更