

静岡県警察からのお願い

デジタル複合機のセキュリティ対策していますか？

デジタル複合機のセキュリティの脆弱性

多機能のコピー機やプリンター等のいわゆるデジタル複合機は、取扱ったデータが機器の内部に保存されます。

適切なセキュリティ対策を講じないままインターネットに接続して利用すると、機器の内部に保存されたデータが外部からアクセスできる危険な状態となります。

情報漏洩対策

- 必要のない場合は、デジタル複合機をインターネットに接続しない。
- デジタル複合機をインターネットに接続する場合はファイアウォールを用いる。
- デジタル複合機の管理者パスワードを納入時のものから変更する。
- デジタル複合機のアクセス制御機能を有効にし、アクセス時にIDとパスワードにより認証を行うように設定する。

参考事項

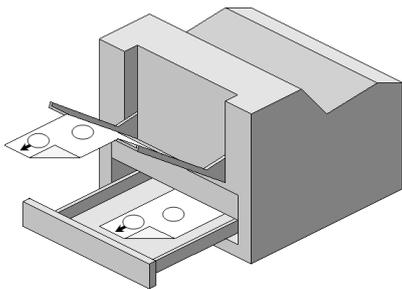
デジタル複合機のセキュリティ調査結果及び調査・対策要領については、独立行政法人情報処理推進機構（IPA）が作成した報告書等を参考にしてください。

- デジタル複合機のセキュリティ調査結果

<https://www.ipa.go.jp/security/fy24/reports/mfp>

- デジタル複合機のセキュリティ調査・対策要領

<https://www.ipa.go.jp/security/technicalwatch/20140227.html>



【お問い合わせ先】

〒420-8610

静岡市葵区追手町6番1号（静岡中央警察署内）

静岡県警察本部生活安全部サイバー犯罪対策課

企画指導係 松島、鈴木

TEL：054-271-0110（代表）

内線：711-3496