セキュリティ対策虎の巻（第5回）

複合機は情報セキュリティー対策で選べ

2017.02.01

コピー、ファクス、プリンター、スキャナーなど、ビジネスに必要な各種の機能が1台にまとめられた「複合機」。今やあらゆる職場で活躍する。ところが最近、この複合機が情報漏えいの温床になっていたとの報道が相次ぎ、不安が高まっている。複合機を安心して使うためにはどうすればいいのか考えてみたい。

情報セキュリティー強化をめざし機能を拡充

複合機の脆弱性に関する指摘を受けたメーカーは、ユーザーの管理体制に応じた各種の対策をアドバイスするとともに、情報機器としての情報セキュリティー強化に力を入れている。具体的には複合機の各機能を高度化して不正アクセスを防ぐという仕組みだ。

まず、部外者による不正アクセス対策として、認証機能を強化し、使用時にパスワードやICカードで個人認証する。これにより、あらかじめ登録されたユーザー以外の操作を制限する。同時に操作の履歴（ログ）を収集・蓄積して、問題発生時の追跡を可能にした。また、パソコンやサーバーとの通信の暗号化や、通信プロトコルを次世代型（IPv6）対応にするなどの取り組みも進められている。

しかし、これらの対策は以前から行われてきたものだ。思うように改善が進まない現在の状況を説明するのには不十分だ。複合機はパソコンやサーバーなど他の情報機器とは異なる管理体制があり、これが対応の遅れにつながっている可能性がある。

コピー機は多くの社員で共用することから、主に総務担当者が管理してきた。メンテナンス、故障発生時の対応窓口も総務になっている場合が多い。プリンター、ファクス、スキャナーなどの機能を併せ持つ複合機はLANを構成する情報機器で、パソコンと同様に管理する必要がある。だが、現在も相変わらず「総務任せ」になっているケースが見受けられる。

これは、トナーや用紙といった消耗品の手配など、他の文具類と同様に総務担当による購買業務が継続的にあり、そこにネットワーク設定や情報セキュリティー管理といった情報システム部門の業務が加わったことが要因といえる。この状況は各部署の責任というよりも、全社の体制の問題だ。管理体制を再検討する必要がある。

データを確実に消去できる複合機… 続きを読む