平成28年1月8日

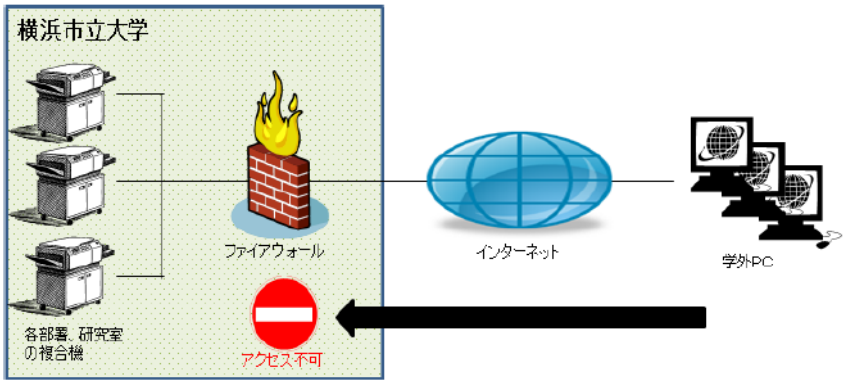
教職員各位

経営企画課IT推進担当

【重要】ネット接続の複合機による情報漏洩の危険性について

インターネットとつながる複合機やプリンターのセキュリティ対策がとられず、内部データが外部から見えていた大学などが多数あるという事件が、新聞等で報道されました。（ネット接続の複合機など、データ丸見え　大学など26校　2016年1月6日朝日新聞）

現在、国内で販売されている複合機の大半はネット接続されており、初期設定では複合機にアクセスするためのＩＤ・パスワードが設定されていないケースが多いため、そのままでは、複合機に蓄積されたデータが外部から見られる状態になっているとのことです。
ただし、本学では、学内LANに接続されている複合機はファイアウォールで遮断されているため、学外から複合機のデータを見ることはできません。



しかし、学内LANではないネットワーク（NTT フレッツ光など個人で契約している回線）に接続している複合機はファイアウォールで守られてないことや、学内LANに接続している複合機でも学内LANに接続された端末からはアクセス可能であることから、情報漏洩の危険性が全くないとは言えません。そのため、各部署、各研究室に設置している複合機につきましては、以下の確認、対策を実施していただきますようお願いします。

１.複合機にアクセスするためのＩＤ・パスワードを設定する。

２.今後、複合機を導入する際は、導入時にＩＤ・パスワードを設定することを、契約内容に盛り込む。

３.複合機の廃棄時は、必ず蓄積データを破棄する。データ破棄を廃棄業者に委託する場合は破棄証明書を提出さる。

※アクセスするためのＩＤ・パスワードの設定手順や蓄積データの破棄手順につきましては、機種ごとに異なるため、導入業者にお尋ねください。

【担当】経営企画課 IT推進担当
電話 ： 787-2340、2341
E-mail: center@yokohama-cu.ac.jp