電気通信大学における不正アクセスされた端末を踏み台にした学外への多量フィッシングメール送信について

2016 年 06 月 03 日

情報システムセキュリティ責任者
三橋　渉

この度、国立大学法人電気通信大学（学長：福田喬）レーザー新世代研究センターの研究室が管理する端末ＰＣが不正アクセスされ、学外への多量のフィッシングメールが送信されるという事案が発生しました。メールを受信し、不快な思いをされた皆様にお詫び申し上げます。

不正アクセスされた端末には、学生のデータ等の個人情報は格納されておらず個人情報の流出の痕跡はありません。

学内の端末が不正アクセスを受け、フィッシングメールが送信されてしまうという、大学としての情報機器のセキュリティが徹底していなかったことを深く反省しております。

今後、法人として、ネットワークに接続する機器への外部からの不正アクセス防止について、さらなる強化に努めてまいります。

なお、事案発見後、すみやかに警察へ被害状況について報告しており、対応について相談しております。

１．事案の概要

2016 年 5 月 3 日本学レーザー新世代研究センターの研究室が管理する端末 PC が不正アクセスを受け、2016 年 5 月 3 日から 5 月 4 日までの間、学外の約 280 万のアドレス向けに、銀行のアドレスを模倣した学内のメールアドレスから海外の銀行のインターネットバンキングのログイン ID とパスワードを窃取する目的のフィッシングメールが送信されました。

不正アクセスの原因としては、端末のパスワードを安易なものに設定していたこと及びアクセス制限が適切に設定されていなかったことでした。

メールの本文にあるリンクのフィッシングサイトは 5 月 9 日から本日まで閉鎖されていることを確認しております。

２．送信元アドレス（×は任意の文字）

・ko×@cs.uec.ac.jp
・【銀行名】@cs.uec.ac.jp
・【銀行名】s@cs.uec.ac.jp

３．フィッシングメールの主な内容

・5 月 4 日にインターネットバンキングの認証システムが変更されること。
・メール本文の URL からログインし、お客様の情報を確認すること。
・お客様の情報の確認がない場合インターネットバンキングが使用できなくなること。

４．緊急対応

不正アクセスを受けた端末からのフィッシングメール送信は 5 月 4 日に遮断しました。

５．今後の対応

関係者に対して、ホームページ、学内掲示等により説明を行うとともに、お問合せについては、以下の電話番号にて対応いたします。

６．再発防止策

今回のようなインシデントを再発させないため、全学生や全教職員に対して端末や利用するシステム等のパスワードを強固なものに変更させるとともに、不要なサービスの停止、不要アカウントの削除、学外からのアクセス制御の厳格化を実施し、情報セキュリティ対策の強化を実施してまいります。

【お問合せ先】

担当部署：電気通信大学総務課情報システム係
電話番号：０４２－４４３－５０３４（直通）
開設時間：午前９時～午後６時まで（土・日・祝日を除く。）
メールアドレス：abuse@uec.ac.jp

【取材に関するお問合せ先】

担当部署：電気通信大学総務課広報係
電話番号：０４２－４４３－５０１９（直通）
開設時間：午前９時～午後６時まで（土・日・祝日を除く。）
メールアドレス：kouhou-k@office.uec.ac.jp