# 公立大学法人横浜市立大学記者発表資料

平成30年6月6日
ＩＣＴ推進課

電子メールの不正転送被害による個人情報の漏えいについて

横浜市立大学の教職員及び学生に対し、本学で利用しているクラウドメールサービスのログイン画面に似せた偽の英文サイトに誘導して、ID およびパスワード入力を求める英文の「フィッシングメール」が届きました。これにより、教職員等が使用している 29 のアドレスで偽のサイトにアクセスしたことにより、29 のアドレスに届いた受信メール 3,512 通が、不正に外部に転送され、メールアドレスを含む個人情報が漏えいしたことが判明しました。現時点で、新たな不正ログイン及びメール不正転送が生じないように対応しています。漏えいした情報に関する二次被害等の報告はありませんが、漏えいしたメールの内容の詳細については、現在も確認を続けています。

関係者や市民の皆様の信頼を損ねる事態となり、誠に申し訳ございませんでした。

## １　漏えいが確認された個人情報

| 個人情報の件数 | 計　5,794 件 |
|---|---|
| ①　不正に転送されたメールにある個人情報<br>・差出人の氏名・メールアドレス | 3,512 件 |
| ②　メールの添付ファイルや本文に含まれていた個人情報（6 月 5 日 18 時時点） | |
| ・個人の氏名・住所・電話番号 | 2,266 件 |
| ・学生情報 | 16 件 |

※メールの不正転送が確認されたのは、教職員等が使用している 29 のアドレスに届いた受信メール 3,512 通。期間；5 月 15 日（火）～30 日（水）。

※フィッシングメールが届いたアドレス数は、1,037 アドレス。期間；4 月 24 日（火）～5 月 23 日（水）。

## ２　経過

| | | |
|---|---|---|
| 5/23(水) | 8:30 | システム管理者（ICT 推進課）がフィッシングメールの存在を検知する。 |
| | 13:30 | ICT 推進課から全ての教職員及び学生に対してフィッシングメールに関する注意喚起を行う。偽のサイトにアクセスし、ＩＤ及びパスワードを入力した場合は、即時のパスワード変更や ICT 推進課への報告を指示。 |
| 5/28(月) | 11:50 | 偽のサイトにアクセスし、ID 及びパスワードを入力した教員から、転送設定したアドレスにメールが届かないという問合せが ICT 推進課にあり、不審なメールアドレス（1 つ目）への転送が発覚。すぐに転送設定に関する調査を開始。 |
| | 20:30 | 全ての教職員及び学生に、転送設定を至急確認するようメールを一斉配信。<br>2 つ目の不審なメールアドレスへの転送が発覚し、これを受けてこれら 2 つのアドレスへの送信を停止。<br>不正に転送されたメールアドレス数が 29 であることを確認。 |
| 5/30(水) | | 全ての教職員及び学生のメールアドレスの転送設定の調査が完了し、この結果 3 つ目の不審なメールアドレスへの転送が発覚したため、追加で、このアドレスへの送信を停止。 |
| 5/31(木) | | フィッシングメールが届いたアドレス数 1,037 を確認。あわせて、この 29 アドレスに不正転送されたメール数が 3,512 通であることが判明。 |
| 6/1(金) | | 不正なログイン及び不正なメールアドレスへの転送を防止するため、全ての教職員及び学生に、ID のパスワード変更とメールの転送設定を停止することを通知。<br>また、不正にメールが転送された 29 アドレスに対し、メールに含まれる個人情報等の数について本人に調査を依頼。<br>全ての教職員及び学生のパスワード有効期限を 6/4(月)23:59 に設定。 |

裏面あり

| | | |
|---|---|---|
| 6/5(火) | 00:00 | パスワードを変更していない教職員及び学生については、ID のパスワードが無効になり、メールサービスへのログインができなくなる。 |
| | | 漏えいが確認された 3,512 通のメールの差出人の皆様に、情報漏えいの事実と謝罪文を送付。電話およびメールでの臨時対応窓口を設置。<br>同、臨時対応窓口では、教職員及び学生のパスワード変更、転送停止に関する問い合わせにも併せて対応する。 |

## 3　対応について

### (1)　個人情報が漏えいした方について

漏えいが確認された 3,512 通のメールの差出人の皆様には、6 月 5 日(火)に本学よりメールにて情報漏えいの事実をお知らせし、謝罪文を送付いたしました。また、あわせて本件に関する問合せについては、同日 6 月 5 日(火)より、電話およびメールでの臨時対応窓口を設置し、個別にご説明、対応を開始しています。

### (2)　被害拡大の防止について

不正なログイン及び不正なアドレスへのメール転送が新たに生じないよう、全教職員及び学生について現在の ID のパスワード変更を行ったこととあわせて、メールの転送設定を順次停止しています。

### (3)　今後の対応について

添付ファイルやメール本文に記載されていた個人情報の漏えいについては、メールの内容を調査したうえで事情説明や謝罪を改めて行っていきます。

## 4　再発防止策

今後は、全教職員及び学生に対して、不審なメールについてどう対応すべきか、徹底した注意喚起と周知を図るとともに、セキュリティに関する研修の実施など、情報リテラシーの向上に努めます。あわせて、不正ログインの検知や防止を強化する仕組みなど、システム面の改善について至急検討を進め、早期に対応していきます。

## 5　横浜市立大学事務局長　宇都木　朗（うつき　あきら）コメント

このような情報管理面での大きな問題が発生し、関係者の皆様に大変なご迷惑をおかけしましたことを心よりお詫び申し上げます。また、関係者や市民の皆様の信頼を損ねることとなり、誠に申し訳ありませんでした。

早急に調査を行い、全容の把握に努めるとともに迅速に対処してまいる所存です。今回の事態を重く受け止め、真摯に対応していくとともに、二度とこのようなことを起こさないよう、再発防止について大学をあげて取り組んでまいります。

## 参考；今回のフィッシングメールについて

攻撃者は本学のメール管理者を装い、利用者のアドレスに対して「送信サーバの障害によりメールの送信ができませんでした。再送信する場合は、以下のリンクをクリックしてください」という趣旨の英文メールを送付。

本文中のリンクにより実際のクラウドメールサービスのログイン画面に酷似している、偽の英文サイトへ誘導し、ID およびパスワードを入力させることで（偽のログインページには本人の ID を初期値として表示)、パスワードを詐取。

詐取した ID とパスワードを使って不正にログインし、攻撃者の所有するメールアドレス宛に受信メールが転送されるように設定することで、メールを盗み出した。


| お問い合わせ先 |
|---|
| 企画総務部 ICT 推進課長　鈴木 崇広　　Tel 045-787 -2486 、8900 |