



## News Release

令和8年7月3日

# 学生のクラウドサービスアカウント及び学生団体 HP に対する不正アクセスについて

本年5月及び6月に、本学内で利用しているクラウドサービス「Microsoft365」の学生アカウント(2名)から大量の迷惑メールが送信されていたことが判明しました。また、本学の学生団体が運営する公式ホームページ(HP)において、編集権限を持つ学生アカウント(2名)から不審な投稿がなされていたことが明らかになりました。

各事案ともに、海外からの不正アクセスの形跡が確認されたことから、判明後速やかに当該アカウント及びHPを緊急停止しており、危険な状況は現在解消されております。

現時点において、迷惑メールの送信及び学生団体HPへの不審な投稿による具体的な被害は確認されておりませんが、迷惑メールを受け取られた方々など関係者の皆様には多大なご迷惑をお掛けしましたことを深くお詫び申し上げます。

今後は、富山県警察本部の協力も得ながらさらに調査を進めるとともに、再発防止に努め、情報セキュリティ対策の徹底に万全を期してまいります。

### 事案1：学生のクラウドサービスアカウントへの不正アクセスについて

#### 1 事案概要

##### (1) 送信された迷惑メールの内容

	学生Aのアカウント	学生Bのアカウント
件数	計4,419件(5月13日(水)～20日(水)にかけて断続的に送信)	計162件(6月15日(月)～16日(火)にかけて断続的に送信)
宛先	不特定多数(GmailやYahoo!メールなど)	不特定多数(Gmailなど)
内容	英語で写真等の入手を促す短い文章とリンクが記載	ドイツ語で公的機関への情報入力を促す短い文章とリンクが記載

##### (2) 原因

- ・本人所有のPCが何らかの原因で悪意のあるソフトウェアに感染し、ID・パスワードが不正に窃取された可能性がある。(両学生とも、直前に私用SNSアカウントから本人の意図しない投稿があったことが確認されている。)

##### (3) 当面の対応

- ・Microsoft365以外の学内サービスも含め当該学生のアカウントを停止したうえでアクセス状況を確認。今のところ、メール送信以外の不正操作及び機密情報の漏洩は確認されていない。
- ・立て続けに学生が被害を受けていることに鑑み、本学の全学生のMicrosoft365アカウントについて、海外のIPアドレスからのアクセスを遮断。

- ・当該学生に事実関係の確認を行うとともに、県警と連携のうえ原因等を調査。
- ・安全なセキュリティ環境が確保された時点で、緊急停止したアカウントに代わる新たなアカウントを当該学生に対して発行。

## 2 今後の対応（再発防止策）

- ・全学生に対し、適切なウイルス対策の実施をはじめとした情報セキュリティ対策を徹底するよう注意を喚起する通知を发出する。
- ・教職員のセキュリティ対策研修において、インターネット上の脅威から身を守るために教職員及び学生がとるべき対策に関し、改めて周知徹底を図る。
- ・学生の Microsoft365 利用に係るセキュリティ対策を強化するため、認証方式の見直しを図る。

## 事案2：学生団体の公式HPへの不正アクセスについて

### 1 事案概要

#### (1) 不審な投稿の内容等

- ・対象：本学の学生団体が外部サーバーで運用する公式HP
- ・内容(件数)：不適切なサイトに誘導する内容のロシア語の文章とリンク(数十件)
- ・投稿された時期：5月29日(土)～6月1日(月)

#### (2) 原因

- ・HPの編集権限を持つ学生の2アカウントに対し、5月10日(日)～6月1日(月)の間に海外から何回もアクセスを試みた記録が確認されたことから、パスワードが総当たり攻撃によって破られ、不正に認証を突破された可能性がある。

#### (3) 当面の対応

- ・当該団体において、記事の削除及び編集権限を持つ学生アカウント(16名)のパスワード変更を行うとともに、HPの運用を緊急停止。
- ・学内の他のHP担当者に対し、外部からの侵入の有無を確認及びパスワード変更を依頼。今のところ、他の不正アクセス及び機密情報の漏洩は確認されていない。
- ・当該団体に事実関係の確認を行うとともに、県警と連携のうえ原因等を調査。
- ・安全なセキュリティ環境が確保された時点で、HPの運用を再開する。

## 2 今後の対応（再発防止策）

- ・HPを運営する学生及び教職員に対し、適切なパスワード設定を含め、情報セキュリティ対策を徹底するよう注意を喚起する通知を发出する。
- ・教職員のセキュリティ対策研修において、HPの運営上必要となる教職員及び学生のセキュリティ対策に関し、改めて周知徹底を図る。
- ・学内のHPの運用管理に係るセキュリティ対策を強化するため、認証方式の見直しを図る。

現時点において、上記の事象による具体的な被害は確認されておりませんが、ご不明な点やご心配なこと等がございましたら、どうぞ下記の窓口までお問い合わせください。

### 【お問い合わせ窓口】

E-mail : contact\_secincident※pu-toyama.ac.jp

※を@に換えてください