岐阜大学 CSIRT の活動について

万田真樹[1]・田中昌二[1]・渡邉美穂[1]・上田康信[1] ・田中宏和[1]

1.岐阜大学 情報連携統括本部

岐阜大学が定める規定に基づき，情報セキュリティに関する教育・研修および情報セキュリティインシデント発生時の対応を行う岐阜大学 CSIRT（Computer Security Incident Response Team）が設置されている．本稿では，岐阜大学における CSIRT 活動を実例をあげて報告する．

Key Words：*情報セキュリティ，CSIRT*

１．はじめに

CSIRT とは Computer Security Incident Response Team の頭文字をとった略称であり，一般的にシーサートと呼称されている．この組織は，コンピュータやネットワークにおいてセキュリティ上問題として捉えられる事案にチームで対応し，原因究明・解決を行っている．

本学の CSIRT 体制は，CIO（最高情報責任者）に情報担当理事，CISO（情報セキュリティ最高責任者）として情報連携統括本部教授，CISO 補佐として技術専門員を配し，情報連携統括本部職員が情報管理対策室員としてチームに属している．

2．CSIRT の活動

情報セキュリティに関する教育・研修と情報セキュリティインシデント発生時の対応が主な活動となっている．

（1）情報セキュリティに関する教育・研修

本学構成員における情報セキュリティに関する意識を高め，セキュリティインシデントを起こさない，万が一セキュリティインシデントが発生した時も正しい対処が行えるような教育・研修を行っている．

(a) e-ラーニング研修

LMS（Learning Management System）を利用した e-ラーニング研修を構成員（教職員・学生）に対して行っている．研修内容はそれぞれに研修内容を分け，教職員向けは情報セキュリティに関するものに加え，ICT の活用や個人情報保護などの情報倫理についても学ぶ内容となっている．教職員の受講率は部署によって 100%から 50%以下と幅があるが，年度により大きな差はなく，平均で 65%程度である．

学生向けの研修内容は，基本的なインターネットの利用方法や利用における注意点などとしている．学生の受講率も年度によってばらつきがあり，2017 年度の全学部平均受講率が約 60%に対し，2018 年度は約 20%，2019 年度は約 13%となった．

(b) 標的型メール訓練

情報セキュリティインシデントが発生した際に対応するための実践的かつ関係部門横断的な対応訓練の実施体制の一環として，標的型メール訓練を計画的に実施している．

外部情報セキュリティ会社の協力のもと，標的型訓練メールの文案検討および啓蒙サイトの構築を行い，教職員を対象に2016年度から役職別に実施し，2019年度の実施をもって，ほぼ全ての教職員が訓練を経験した．

標的型メールを模した訓練メールは，数週間の間隔をあけ，内容の異なるメールを2回送信した．1回目の内容は対象者の職位に応じて年度ごとに変更しており，2回目のメールは 2017 年度から 2019 年度まで同一の内容とした．なお，2 回目の訓練メールは，添付ファイル付きのメール（Fig.1）を対象者に送信し，添付ファイルに内包した html ファイルを開いてしまった場合に啓蒙サイトへアクセスさせ，そのアクセス状況を調査した．

送信者：給与支払係（kyuuyo.gihu-u@***）
件名：（要確認）年末調整の書類について
メール本文：
各位
お世話になります。給与支払係年末調整担当です。
過日提出いただきました年末調整の書類につきまして、税務署から不備を指摘されました。
修正いただく箇所を添付にてご案内いたしますので、添付ファイルを開き内容をご確認の上、再度の提出をお願いいたします。

■再提出期日：平成 〇 年 12 月 △ 日

■確認方法
セキュリティのためアクセスは必ず学内のパソコンから実施してください。
1）添付ファイル（年末調整確認用.zip）を解凍してください。
2）パスワードは以下に記載しています。
3）解凍したファイルをダブルクリックするとブラウザが立ち上がりますので、 ID を入力 し、了解ボタンを押してください。

■パスワード：gifudai#syusei

※添付ファイル 年末調整確認用.zip

Fig.1 標的型メールを模した訓練メール内容例

2016 年度対象者は役員および部課長クラスとし，2017 年度対象者は主任～課長補佐クラスの一般職員および医療職の一部の計290名．2018年度対象者は一般職員および補佐員の計500名，2019年度対象者は教育職員 800 名に実施した．

2017 年度から 2019 年度の 2 回目の訓練メールの内容が同じにも関わらず，実施年度によって啓蒙サイトへのアクセス率（訓練メールの開封率）に大きな差があり，2017 年度は約 40%，2018 年度は約 21%，2019 年度は約 58%の結果となった．

標的型メール訓練実施後は，訓練対象者に対し，最近の情報セキュリティに関する傾向や実施した訓練メールの見極め方などの内容で研修会を実施した．

標的型メール訓練においては，メール開封率を0%にすることはほぼ不可能であると思われる．標的型メールを見破ることも重要であるが，開封してしまった後に正しい対処が出来るかどうかが重要である．本訓練により，万が一標的型メールを開封してしまった場合でも，正しい対処ができるよう本学構成員のセキュリティ意識向上を期待する．

（2）情報セキュリティインシデントの対応

情報セキュリティインシデント発生時の初動対応に関わる手順書を CSIRT において作成し，各部局の担当者間で共有するとともに，「岐阜大学における情報セキュリティインシデント対応手順」を周知することで外部からのインシデント通報の窓口を明確にしている．

また，「岐阜大学の情報セキュリティインシデント対応体制と対応フロー」を作成し，学内に周知することによって，対応手順を明確にしている．

情報セキュリティインシデント発生時には，これらの手順書および対応フローを基に，緊急性と重要性の度合いに応じて，データの保全・システムの停止およびインシデント緊急対処チーム設置の判断を行い，CISO の主導のもと，CSIRT を中心に関係部門の担当者らで，以下の任務を遂行している．

- インシデント事実関係の確認
- 状況・原因の調査および分析
- 対応方針・復旧計画・再発防止策の検討・実施
- 報告書の作成

一例として 2020 年初頭にアカウントおよびパスワードが詐取され，不特定多数の相手に迷惑メールを送信した本学の情報セキュリティインシデントを例に，CSIRT としての対応を次の（a）～（e）に報告する．

(a)他機関からの情報提供

本学のメール送信サーバより，不審なメールが送信されているとの情報提供があり，送信されたメールの内容を調査したところ，間違いなく本学のメール送信サーバから送られていることが判明した．

(b)情報セキュリティインシデントと認識

サーバのログを調査したところ，不審なメールを送信したアカウントが海外の IP アドレスから本学の Web メールを利用していることが確認された．ユーザの所在を確認したところ，ユーザは海外渡航を行っていなかった．

直ちに情報管理対策室員から CISO へ報告し，CISO より CIO へ事案発生の報告がなされた．

アカウントのロックを実施後，メール送信サーバのログを調査したところ，大量のメールを送信していることが確認された．

(c)情報セキュリティインシデント発生原因

ユーザへ聞き取り調査を実施したところ，本学からのメールに模したフィッシングメール(Fig.2)を開封し，メール本文中のリンク先へアクセス後に表示されたログイン画面でアカウントおよびパスワードを入力したとのことであった．

学内の情報サービスを利用する際に，Web 上でアカウントおよびパスワードの入力が必要だが，学内で提供される情報サービスのドメインはすべて gifu-u.ac.jp となっている．また，利用者に対して通常は英文メールでの案内は行っておらず，当該メールには本学情報部門のシグネチャも記載されていなかった．

当該メールのリンク先を調査したところ，本学のロゴマークを使用したログイン画面に遷移し，アカウントおよびパスワードが入力できるようになっており(Fig.3)，フィッシングサイトが開設されていることが確認された．ロゴマークは本学の Web サイトから流用されたものと推察されるが，明らかに本学のログイン画面とは異なるものであった．

From: 国立大学法人 岐阜大学<***@gifu-u.ac.jp>
Sent: Wednesday, ***, 2020 9:48 PM
To: undisclosed-recipients:
Subject: (IMAP/POP/SMTP) Notification

Your e-mail box has exceeded the storage limit which is 1024MB as set by your administrator, you are currently running on 1150MB, due to some hiding files you may not be able to send or receive new e-mails until you re-validate your mailbox.
To re-validate your mailbox ***CLICK ON THIS LINK BELOW OR COPY AND PASTE IN YOUR BROWSER*** and enter your User Name and Password

https://***/plugins/form-builder/view/***?mode=page

Your account shall remain active after you have successfully confirmed your account details.
Thank you for your swift response to this notification we apologize for any inconvenience. We appreciate your continued help and support.

Fig.2 本学からのメールに模したフィッシングメール

Fig.3 本学を模したフィッシングサイトのログイン画面

(d) 迷惑メール大量送信の状況調査

サーバのログを調査したところ，約 5 時間の間に約 800 回 Web メールにログインされたことが判明した．ログイン成功後，複数回に分けて約 80000 件の宛先に対してメールを送信し，その内約 48000 通が配送先のメールサーバに受理されていた．宛先はアルファベット順にソートされた大量のドメインにまたがったメールアドレス群となっており，特定組織を標的としたものではなく，バラ撒き型の迷惑メールが送信されたと推定された．

(e) 情報セキュリティインシデント終息への対応

状況を鑑み，文部科学省へ情報セキュリティインシデント発生報告を行い，指示を仰いだ．学内においては，情報セキュリティインシデントの原因となったユーザが所属する部署が報告書を作成し，CISO から CIO に報告したのちに学長へと報告された．

文部科学省の指示により，迷惑メールの宛先に含まれていた他機関へ CISO が謝罪を行い，学内の構成員へは不審メールに対する注意喚起を行った．

情報セキュリティインシデントの原因となったユーザへは，フィッシングメールに関する注意点・他の情報サービスとのパスワードの使いまわしの禁止・類推されにくい強固なパスワードへの変更等を個別に指導し，パスワードの再設定を行ったのちにアカウントのロックを解除した．

フィッシングサイトが開設されたレンタルフォームサイトの管理者に対してサイトの閉鎖依頼を行い，数日の内に本学を模したフィッシングサイトは閉鎖された．

3. まとめ

本稿では，本学における CISRT 活動を紹介した．情報セキュリティインシデントは，ある日突然に誰にでも起こりうることである．教育・研修以外にも，平素から構成員に対して情報セキュリティに関する情報発信を行っているが，過多な情報発信や注意喚起は構成員のストレスになったり，情報を聞き流されてしまったりすることがあるため，匙加減が難しいところである．

しかしながら，本学における情報セキュリティインシデントは構成員の不注意によるところもあるため，更なる教育・研修の充実化および受講率の上昇を図るとともに，利便性を確保しながらも，情報サービス利用時における多要素認証や不正ログインの自動検知機能を採用するなど，よりセキュリティ性の高い環境を構築することが必要と思われる．

謝辞

本報告を作成するにあたり，岐阜大学情報セキュリティ最高責任者（CISO） 松原正也教授，情報連携統括本部 村上茂之教授，情報連携調整役 髙田真也氏をはじめ，多くの方々からご協力とご助言をいただきました．ここに感謝いたします．