岐阜大学情報管理対策室における活動について

○田中宏和、田中昌二、渡邉美穂、上田康信

情報技術支援室（東海国立大学機構 情報環境部 情報システム運用課）

東海国立大学機構（以下、機構という）および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機器の監視、また情報セキュリティインシデント発生時の対応を行うため、機構には機構セキュリティ室や機構 CSIRT が、岐阜大学には情報管理対策室がそれぞれ設置されている。

本稿では、岐阜大学における情報管理対策室の体制と活動状況、および基幹情報システム等の更新に合わせた運用変更、また最近の注意すべきヒヤリハット事案、標的型メール攻撃訓練の結果と今後の課題といった情報セキュリティについて紹介する。

1　用語と情報セキュリティ体制解説

1.1　用語解説（読みと主な任務）

- CSIRT（シーサート）： Computer Security Incident Response Team
  主に情報セキュリティインシデント発生時の対応を行う
- SOC（ソック）： Security Operation Center
  主に情報セキュリティ機器を監視インシデントやサイバー攻撃の前兆などを検知し、利用者への注意喚起等を行う

1.2　機構と岐阜大学の情報管理および情報セキュリティ体制

岐阜大学では、情報連携推進本部が情報システムの構築および管理とセキュリティを担っており、情報環境整備室がシステムやネットワークの構築と管理を、情報管理対策室が情報セキュリティを担当している。また情報管理対策室は上記 CSIRT と SOC を兼ねて活動している。

※なお医学部附属病院には独自 CSIRT があり、情報管理対策室会議の場などで情報交換を行っている。

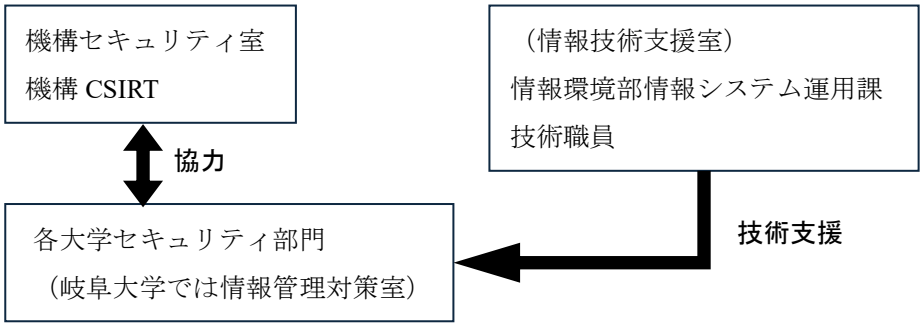

図 1　情報管理対策室の関係図

2　情報管理対策室活動概要

サイバーセキュリティ対策等基本計画に基づいて、以下のような活動を行っている。

- 情報セキュリティ e ラーニング研修（以下、研修）（毎年 1 回）
- 標的型メール攻撃訓練（毎年 1 回）
- 各階層別セキュリティセミナー
  「サーバー管理者向け」「教職員向け（各部局）」「学生向け（初年次セミナー等）」などを実施
- 休暇前や注意を要する事象発生の際などに通知を出して注意喚起
- 情報機器の監視および予防的対応（※通信遮断を伴う場合がある）
  基準を超えた不審な通信が検知された機器の管理者に安全確認を依頼
- 情報セキュリティインシデント（情報事故）発生時の各種対応
  ※インシデントにならないヒヤリハット事案への対応を含む
- 情報セキュリティ監査（外部機関と情報セキュリティに関する相互監査を実施）
- 情報セキュリティに関する情報収集**標的型メール攻撃訓練（毎年 1 回）**
- 情報セキュリティに関する情報収集

3　不審な通信の検知基準と解除手続きの一部変更について

3.1　不審な通信検知と遮断基準に関する変更

3.1.1　変更の経緯

令和 5 年度に、判定基準を超え通信遮断にあたる事例が頻発し、情報機器の確認作業が追いつかない状況になった。(1 日最大 10 件程度が限界　対象サイト数によってはさらに少なくなる場合もある。)

また通信遮断を受ける利用者からも、研究活動に通信が必要なのでいきなり通信遮断をしないでほしい、などといった苦情が寄せられたが基準の回答に苦慮していた。

3.1.2　判断基準や手順の変更および文書化

調査や遮断の判断基準と対応手順について情報管理対策室で検討し内部文書化した。その後、対応に苦慮するような事態にはなっていない。このことから、判断基準については概ね妥当で、利用者への回答も自信を持って行えていることから状況は改善されたと考えている。

なお、苦情対応については全学の情報安全が優先との判断から不許可となった。

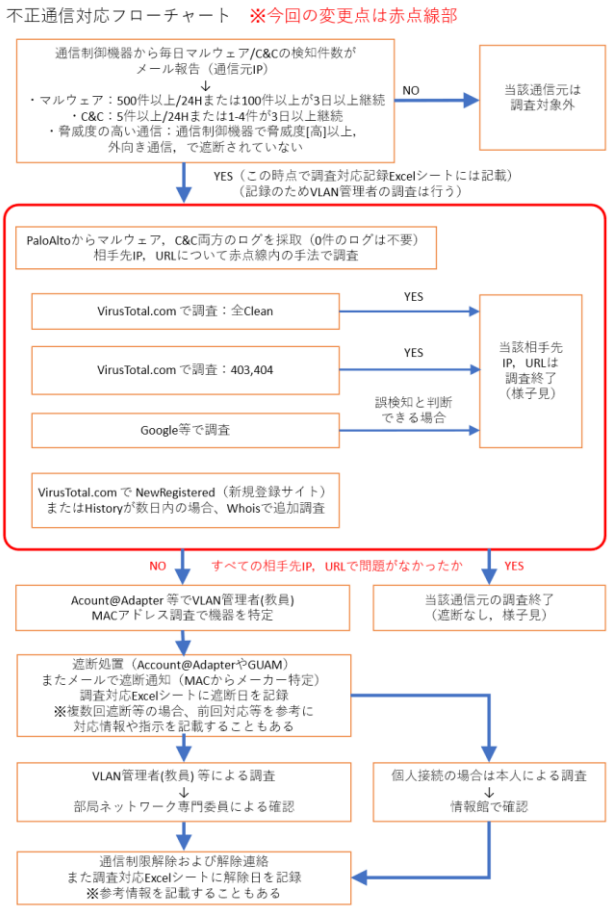

図 2　不正通信対応フローチャート（改善版）

3.2　不審な通信の解除手続きに関する変更

3.2.1　変更の経緯

令和 6 年度、遮断中の退職等により VLAN 管理者権限を喪失した場合に、単純に遮断解除を行うことで管理者不在の PC 等端末登録が残る状況が発生することが発覚した。このことについて、ネットワーク管理上問題があるとの指摘が情報環境整備室から寄せられた。

(例) ・３月に不審な通信を検出して通信遮断を実施（この時点の管理者は A 先生）
・A 先生は３月末で退職、その後の管理を B 先生に移管
※この時点で遮断中に機器以外の機器管理が A 先生から B 先生に引き継がれる。
・４月に当該機器（管理者 A 先生）の安全確認が終了。通信遮断解除。
※この時点で管理者 A 先生（実質管理者不在）の機器登録が残置されてしまう。

3.2.2　通信遮断解除手続きの一部変更

解除手続きを一部変更した。（以下、変更点）

- 遮断解除時に管理者の在籍状態を確認する。（※在籍の場合は従前と同じ）
- 在籍していない場合は、部局情報ネットワーク専門委員を通じ、新管理者を選定していただく。
- 新管理者にて安全確認の実施 → 部局 → 情報管理対策室と報告をあげる。
- 安全確認できたら､機器登録を削除し､新管理者で再登録し直してもらうことで遮断解除に代える。

4　情報インシデント未満（ヒヤリハット）事例紹介

情報管理対策室の活動として、情報事故になる前の未然防止は非常に重要である。最近のヒヤリハット事例から２件紹介する。

4.1　不審なメール（電子ギフトカードの詐欺未遂）

学内で実在の教員 A を騙った送信者（メールアドレスは実在しない）から学内の実在の教員 B に向けた詐欺メールを受信した（内容としては Apple ギフトカードの代理購入依頼）というものだった。

教員 A と教員 B はお互いに連絡が取れる学内関係者だったこともあり、すぐに詐欺メールと判明した。そのため、実際の送信相手と連絡を取ることもなく被害には至らなかった。

この時点で情報管理対策室に連絡があり、関係者に反応しないよう注意喚起のうえ、メールは削除対応した。

本件は比較的分かりやすい事例であった（文言も大学関係者としてはおかしい）が、最近は運送会社の再配達やネットショップ・カード会社等を騙ったもの、詐取した本当のやり取りから参照用として指示した URL 等だけを別のものに書き換えたものなど、本物の連絡と区別が困難な場合もある。また、メール

【メールの主な内容】
氏名(学内で実在する教員 A)
******@gmail.com（存在しない）
宛先: 氏名.x0@f.gifu-u.ac.jp（教員 B）
受信：x 月 x 日　x 曜日　xx:xx
はい、それはあなたのためです。
Apple ギフトカードをご存知ですか？近くの店から買ってほしい、送らなきゃいけない見込み客がいるんだけど、今は打ち合わせ中。
あなたが私に代わってそれらを取得し、私にコードを電子メールで送ることができるかどうか私に知らせてください。
返金します。

図３　不審なメール（参考用）

はその仕組み上偽装行為が可能で、検閲との兼ね合いで機械的に予防することも困難である。まずは利用者自身が注意深く対応するとともに、情報管理対策室でも判断できるよう事例収集に努める必要を感じる案件だった。

4.2　サポート詐欺画面の表示

mac パソコン利用の教員に突然表示された画面で、コンピュータがウィルス感染を起こしたこと、サポート窓口と称する電話に連絡を取ることが画面上に指示されている。実際には表示されたセキュリティセンターなるものは存在せず、海外のおそらく犯罪グループ（本件の場合は海外の電話番号が表示）に連絡させて、逆に機器を危険な状態にさせたり金品を要求したりするものと推察された。

この時点では致命的なマルウェア感染を起こしている可能性は低いと判断されたので、念のためネットワークからパソコンを切り離して通信できないようにすると共に、画面採取した後、強制再起動で対応した。再起動後、動作に異常がないこと、ウィルスチェックで異常がないことを確認後に、ネットワーク接続を再開し情報提供していただいた。

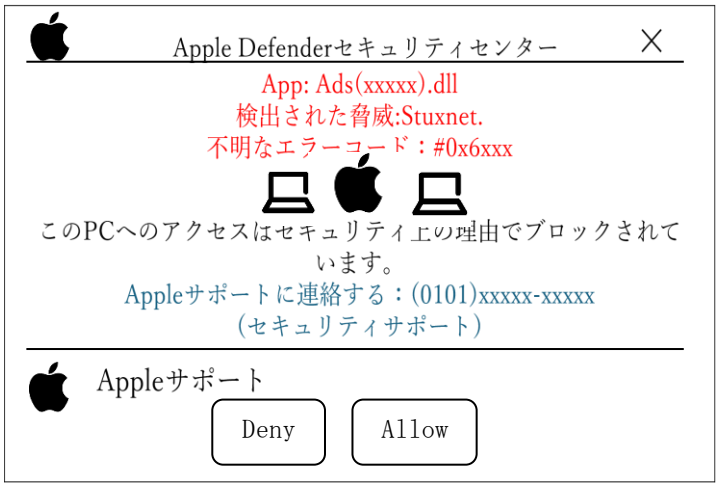

図４　サポート詐欺画面（参考用）

この感染警告とサポート詐欺画面の表示事例は、一般社会でも最近報告が増加していて問題となっている。

また画面はインターネット閲覧中に、広告や画面内に表示されている画像などから自動的に表示させられるケースもあり、現時点ではシステム的防御が困難な事例である。

本件ではないが別の報告事例では、学内の利用者が相手に連絡を取ってしまい、やり取りする中で詐欺を疑うようになって連絡を絶ち、被害を免れるという、本当に間一髪と言える事例も発生している。また一般では、やり取りの中でインストールを指示されるソフトウェアこそが、機器を勝手に操作されたりパソコン内の情報を盗まれたりする、あるいはデータを暗号化され解除のために金銭を要求される（ランサムウェア）などの原因になることが多く報告されている。

こういった画面が表示されると、利用者は強い心理的ストレスなどから正常な判断ができず、専門家に相談することすら思いつかなくなり、ただただ早く解決しようと焦ることになる。また相手方はそれこそが狙いであるとも言える。こういった不測の事態に対処するには、利用者には経験を積んだ専門家（本学においては情報管理対策室）に一刻も早く相談や報告をしてもらうようにする必要がある。また早く連絡いただければ被害を受ける前に対処が可能であると、改めて気づかされた事例だった。

今後、利用者に対して訓練や啓発活動をさらに強化し、情報管理対策室へ早く相談いただくことで被害発生の防止につなげる必要を強く感じている。

5　標的型メール攻撃訓練

上記 4.1 のような不審メールへの対応訓練として、前述 2 にある標的型メール攻撃訓練（毎年 1 回）を実施している。令和５年度と令和６年度で文面などは同じにしたが、一部条件を変えたことにより、大きな変化があった。以下、簡単に紹介する。

【前年度から変更した条件】

・URL をクリックした際に表示されるコンテンツ内で、周囲への注意喚起を行ってよいとした。

・URL をクリックした際に表示されるコンテンツ内で、情報管理対策室への報告を求めた。

【結果】

・開封率が 1/10 程度とかなり低下した。（前年度 29.5% → 今年度 2.8%）

・開封者のうち 1 名しか情報管理対策室に報告していなかったことが分かった。

【考察と今後の対応】

前年と同一文面だったこともあるが、周囲への注意喚起の効果が相当に大きいことが分かった。

不審なメールを開封すること自体は、何らかの理由で注意力が低下したりすることもあるのでやむを得ないこともあるが、被害拡大防止には速やかな報告や相談が不可欠である。前回と今回の比較から、今後の改善方針を検討するうえで大きな材料を明確に得ることができたと考えている。次回以降、教育や訓練の改善に生かしていく。

教員向け文面例（前年と同一文面）
件名：ユーザ登録の件
先生様　株式会社　教育連携システム企画東京支社です。メールにご返信いただき，ありがとうございました。
当社にて貴方のユーザ情報の登録いたしますので，下記 Web サイトに氏名・生年月日・メールアドレスを入力しなさい。
http://……
****
株式会社教育連絡システム企画　担当
xxx@xxxx.xxx
****

図５　標的型訓練メール（教員用）

6　まとめ

岐阜大学における情報管理対策室（情報セキュリティ担当部門）について、本稿ではその体制と活動概要の紹介、最近の動きから、不審な通信検知および解除に関する変更点、また情報インシデント未満（ヒヤリハット）の対応事例２例、および標的型メール攻撃訓練の結果と今後の改善点、を紹介した。

情報管理対策室の活動として、今後とも利用者に注意深く情報ネットワークを利用してもらうため、教育研修や情報発信および対応（予防対応を含む）は継続的に行っていくことが非常に重要であることを改めて確認することができた。またそのためには、情報管理対策室自身が、手続きや対応手順等のアップデートを行って、常に最新の攻撃の手口に対して備えられるようにしていくことが重要である。

最後に、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、岐阜大学情報連携推進本部 村上茂之教授、機構情報環境部情報企画課主幹 小倉美穂氏をはじめ、機構情報環境部情報企画課・情報システム運用課など多くの方々のご協力とご助言をいただきました。ここに感謝申し上げます。