令和４年度　厚生労働行政推進調査事業費補助金
地域医療基盤開発推進研究事業

分担研究報告書

医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究（２１ＩＡ２０１３）

研究分担者　美代 賢吾
（国立研究開発法人国立国際医療研究センター医療情報基盤センター長）
研究分担者　星本 弘之
（国立研究開発法人国立国際医療研究センター医療情報基盤センター専門職）
研究分担者　辻岡 和孝
（国立研究開発法人国立国際医療研究センター医療情報基盤センター上級研究員）

研究要旨
令和 2 年度の厚生労働科学研究での調査結果に基づき、医療機関、特に中小規模医療機関など IT に関する専門職員が不在の組織に求められるサイバーセキュリティ対策教育のあり方について検討し、令和 3 年度に標的型メール対応訓練の実施基盤の要素技術開発を行った。令和 4 年度については、令和 3 年度の成果を拡張し、実用的な迷惑メール対応訓練システムの構築を行った。本システムにより、一般的な迷惑メール対応訓練のためのメール配信および配信された訓練メールに対する反応結果の把握が可能となった。今後は、このシステムを用いることにより、民間病院において実施率が著しく低いサイバーセキュリティ対応訓練の普及につながることが期待される。一方、訓練サービスの提供と合わせて、訓練結果などに基づく支援のあり方について検討する必要がある。

A. 研究目的

重要インフラに該当する医療分野において、医療機関等のサイバーセキュリティに対する取り組みを強化することは喫緊の課題である。病院情報システムは、これまで外部と隔絶した情報ネットワークであった状況に対し、データヘルス改革、働き方改革、オンライン診療、モバイルヘルス(m-Health)等の導入で外部ネットワークへの接続が始まっており、情報化が進んでいなかった小規模病院、診療所における電子カルテの導入・普及も進みつつある。さらに、CT や MRI、検体検査機器などが高度化し、開発ベンダーによる常時リモートメンテナンスの体制も一般的となっているほか、進化するクラウド技術により、医療機関内にあったサーバをクラウド上に移行することも現実的になりつつある。

このように急速にネットワーク化され外部との接点が増す医療機関において、近年多発しているランサムウェア攻撃などの事例においては、不適切に構築・管理運用されたシステムにより医療機関内部に侵入されていることが明らかになっていることから、組織としてのサイバーセキュリティ対策への取り組みにくわえ、一般利用者等への適切な教育は喫緊の課題である。しかしながら、令和 2 年度に分担研究者らが実施した医療機関のサイバーセキュリティ実態調査の結果、サイバーセキュリティに関する教育は全体の約 39%（198/508）の病院で実施されているが、より実践的なサイバーセキュリティ対応訓練を実施している医療機関は約 7.7%(39/508)であり、特に、民間医療機関では 3.6%（11/304）のみが実施と大幅に実施率が下がっていることから、セキュリティ訓練を容易に実施できる基盤の整備が有効であると考えられた。

このような背景のもと、主任研究者がおこなう、医療分野におけるサイバーセキュリティ対策と課題についての整理、および医療機関同士が相互にサイバーセキュリティ対策に関する情報共有・相談を行う体制のあり方等の検討状況を参考に、分担研究者らは、医療機関に対する情報セキュリティ教育の方法や、その実施に必要なサービスについての検討し、実用性評価のためのリファレンスシステムについて開発を目的として本研究を行った。

B. 研究方法

令和 4 年度は、令和 3 年度に開発した要素技術検証用のプロトタイプシステムの評価に基づき、以下の内容についての検討と開発評価を行った。

1. 令和 3 年度に構築したプロトタイプシステムの評価にもとづき、実用可能な訓練システムの要件について検討整理した。

2. 1）の検討結果に基づき、評価用のリファレンスシステムについての開発を行った。

C．結果

1. 要件検討

分担研究者らの所属機関におけるサイバーセキュリティ事案分析の結果、令和 4 年度上半期においては、メールシステムによりブロックされた者を含め、受信したメールの 14～16%が迷惑メールであり、システムが検知しなかったものを考えると、一般職員に対する情報セキュリティの脅威としては電子メールによるものが大きな割合を占めると考えられた。これに対して、標的型メールへの対応方法などについて、電子メールなどによる情報提供都度行っているが、これはその他の業務上のメールなどに紛れて、きちんと読まれていない実態が明らかとなっているため、情報提供以外に実際のメールでの訓練については依然有効であると考えられた。そのため、令和 4 年度の開発では、令和 3 年度に評価を実施した要素技術を用いて実運用を行うために必要な以下の機能についての追加開発と検証を行った。

2. 標的型メール対応訓練のリファレンスシステムの仕様

標的型メール対応訓練システムとしては、実運用においては、以下の機能が必要と判断された。

■メールの扱いの検知機能

以下、送信した対象メールアドレスごとに

1）送信したメールの開封の有無の検知機能

2）フィッシングを想定した URL へのアクセスの有無の検知機能

3）マルウェアを模した添付ファイルの開封検知機能

■管理機能

4）訓練結果の集計・表示機能（開封率、URL アクセス率、添付ファイル開封率、など）

5）送信アドレスごとの反応状況（開封、URL アクセス、添付ファイル開封）一覧表示

特に、管理機能のうち送信先アドレスごとの振る舞い状況一覧確認機能は、訓練参加者に対する事後のフィードバックを行う上で必須となることから、今回実装を行った。

3. 開発結果

令和 4 年度の開発の結果を以下に示す。

1） 管理画面

図 1 に示す管理画面では、発信した訓練メール数およびそれらのメールに対する受信者（訓練参加者）による①メール開封、②メール内に記載の URL へのアクセス、③メールに添付されたファイルの開封（閲覧）の各イベントの発生数の集計値を確認可能である。表示期間は任意に設定可能としている。

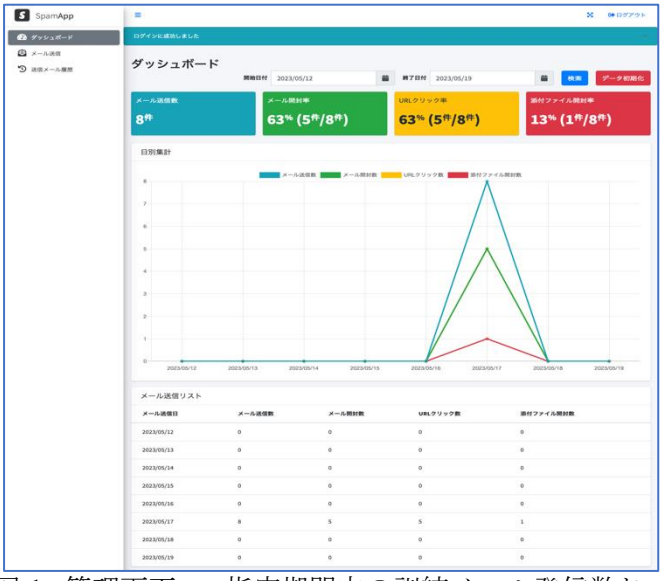

図 1：管理画面： 指定期間内の訓練メール発信数およびそれらのメールに対する受信者の反応状況を集約表示し、一覧で把握可能としている。

2） 訓練メール作成・発信画面

図 2 に訓練メールの作成画面を示す。この画面において、訓練メールの送信先アドレス、件名・本文と URL や添付ファイルの有無などを設定可能である。添付ファイル名については任意に設定可能であるが、現時点ではファイル形式は html 形式のみとなっている。

図 2：訓練メール作成及び発信画面。任意の宛先アドレスに対して、入力された件名・本文および添付ファイルなど設定して送信する。

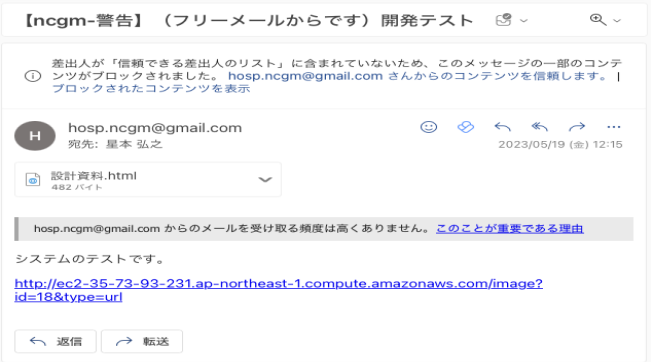

図 2-2：実際に受信された訓練メールの例。コンテンツブロックにより、この時点ではメール開封の検知はできていない。

3） 各受信者の反応状況確認画面
図３に訓練メールを送信したアドレスごとの訓練メールに対する反応状況の確認画面を示す。この画面では、送信先アドレスごとに①メール開封、②メール本文中の URL へのアクセス有無、③添付したファイルの開封・閲覧の有無、の各イベントの発生状況についてそれぞれ確認可能である。また、それぞれのイベントごとに表寿の有無を設定可能である。

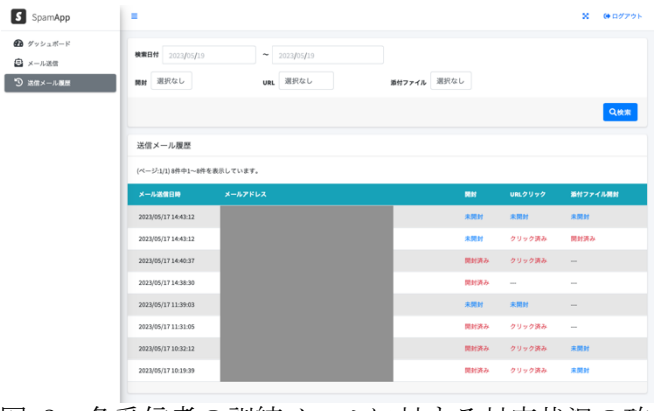

図 3：各受信者の訓練メールに対する対応状況の確認画面。開封、ＵＲＬクリック、添付ファイル開封について確認可能なほか、表示するイベントの絞り込みが可能。

D．評価と考察

今年度開発したシステムにより、迷惑メール対応訓練の実施に向けて必要となる機能の実装はほぼ完了したと考えられる。一方、本システムを用いて分担研究者らの所属組織のメールシステム（Microsoft 社の Office365）に対して訓練メールを試験送信したところ、一部受信者において訓練メールが本物の迷惑メールと判定され、検疫処理が行われるという事象が見られた。これはメールシステム自体のセキュリティ機能の高さを示すと考えられるが、一方では円滑に訓練を実施する上では若干の障害になると考えられるため、訓練の実施においては注意が必要である。しかし、当センターにおいても、度重なる注意喚起にもかかわらず、検疫処理されたメールに対してわざわざ検疫を解除して開封し、さらに添付ファイルや本文中の URL にアクセスを行い、マルウェア感染などに至った事例もあることから、一般利用者に対する訓練としてはこのようなケースもあるいは有効である可能性もある。さらに、セキュリティ訓練を円滑に実施する上では、メールシステム自体にそのような訓練機能を組み込むことも有効と考えられるため、その点についてはメールシステム運用事業者などの意見を今後確認したいと考えている。
本システムの実装とサービスの提供により、中小規模医療機関などにおける標的型メール対応訓練の実施率向上が期待できることから、医療機関のサイバーセキュリティレベルの向上が期待される。

なお、分担研究者らの所属組織においても、一般職員からの不審メールに関する通報・相談に加え、不審サイトなどに実際にアクセスしてしまったケースが日々発生しており、それらの対処には複数の専任職員やオペレータなどがあたっているが、業務上かなりの負荷となっている。これに対し、中小規模の医療機関においては情報システムの専任担当者が置かれていないケースが非常に多く見られることから、本システムなどによる訓練の実施と合わせ、その結果の分析や対応方法に関する情報提供、教育の実施などについて支援する組織が必要と考えられることから、教材作成と提供や支援のあり方について早急に整理し、体制を構築する必要があると考えられる。

E．結論

本システムの開発により、標的型メール対応訓練の実施基盤の実用に向けた開発と検証を行った。今回の開発により、必要な機能についての開発と評価が行えたと考えられる。一方、本システムなどの外部システムなどによる訓練メールは実際のメールシステムにおいて検疫対象と判定される場合もあることから、実際の訓練実施においては、その点も考慮した計画が必要と考えられる。

F．健康危険情報

特になし

G．研究発表

１．論文発表
特になし

２．学会発表
特になし

３．その他
(1) 美代 賢吾. 医療機関のための情報セキュリティ対策　サイバー攻撃から守る、情報漏えいを防ぐためのノウハウ】病院管理者・医療情報部門に求められる情報セキュリティ対策 医療情報システム・医療機器のリモート保守をめぐって. IT Vision 37:2-43, 2022.
(2) 美代 賢吾. ランサムウェアって知っていますか−医療機関を狙うサイバー攻撃への防御と対策. LiSA 29 巻 8 号:739-746, 2022,
(3) 菅沼景子, 星本弘之, 美代賢吾. 医療情報システムにおける二要素認証技術の現況と課題―効果的導入法を含め―. 新医療 50 号:62-66, 2023.

H．知的財産権の出願・登録状況（予定を含む。）

特になし