令和３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、標的型メール対応訓練の実施基盤の開発を行った。開発の結果、標的型メールを模した訓練メールの送信とその開封状況（開封、添付ファイル開封、URL クリック）などの検出機能の実装を行った。次年度以降、多施設対応機能やより有効な訓練メール作成機能の追加実装を行い、医療機関に対する訓練サービスの提供について検討を行う。

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いる。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。また、今後、拡大する m-Health 機器（携帯に連携した継続的なモニタリングと適時な介入をする治療アプリを含む。）は病院、診療所のシステムと連携され、研究基盤として活用されることも考慮する必要がある。同時に、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へのサイバーセキュリティ対策への取り組み、適切な教育は喫緊の課題である。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しつつ、分担研究者は、医療機関に対する情報セキュリティ教育の方法論や、医療機関が求めるサービスについての検討をおこなう。

B.研究方法

２０２１年度

1. 2020 年度に実施した厚生労働科学特別研究事業「オンライン診療・遠隔医療や『非接触』を念頭に置いたＩＣＴ化の中で医療機関が具備すべきサイバーセキュリティ対策や技術に関する研究（研究代表者：国立大学法人鳥取大学 近藤博史教授)」で分担研究者が実施した、医療機関のサイバーセキュリティ実態調査を参考に、医療機関の体制にあった教育方法、ニーズの検討をおこなう。
2. 検討した教育方法、ニーズに基づき、医療機関への教育・対策につながる、オンラインサービスのプロトタイプ的なシステムの構築をおこなう。
3. 必要に応じて、国内での実際の医療機関の状況についてヒアリングとともに情報セキュリ

ティ対策のニーズ等について情報収集をおこなう。
4. 得られた知見及び成果について、関連学会で報告する

２０２２年度
1. 2021 年度に構築したプロトタイプシステムの評価をおこない、医療機関が求めるサービスのニーズについて、考察をおこなう
2. 必要に応じて、国内での実際の医療機関の状況についてヒアリングとともに情報セキュリティ対策のニーズ等について、追加の情報収集をおこなう。
3. 医療機関の求める、教育ニーズ、対策ニーズについて、全体の手順書の一部としてまとめる。
4. 得られた知見及び成果について、関連学会で報告する

C．研究結果

1. 方法

2021 年度の研究では、2020 年度に分担研究者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に基づき、医療機関に必要と考えられるサイバーセキュリティ教育のあり方について検討を行った。

実態調査は 4000 病院に対して回答を依頼し、508 病院より回答を得た。結果の詳細については、文献 1 にまとまっているが、概要としては、サイバーセキュリティ教育は全体の約 39%（198/508）の病院で実施しているが、サイバーセキュリティ訓練は約 7.7%（39/508）の実施率と大幅に実施率が下がっていること、さらに開設主体別の分析では、国・大学が開設した施設では 42.9%(12/28)

がサイバーセキュリティ訓練を実施しているが、民間では 3.6%（11/304）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。また、分担研究者の所属機関におけるサイバーセキュリティ事案のヒアリングの結果、標的型メールなどの情報提供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おり、情報提供以外に実際のメールでの訓練が有効であると考えられたこと。また、昨今のサイバー攻撃の事案を考慮し、emotet などの標的型メール攻撃に分類されるものが事例としても多く見られたことから、標的型メール対応訓練の実施基盤を開発することとし、必要な機能についての整理を行った。

2. 標的型メール対応訓練の実施基盤の仕様

標的型メール対応訓練基盤としては、必要な機能について調査と検討を行った結果、以下の機能が必要と判断された。

■メール送信機能
1）登録した複数のメールアドレスに対して、訓練メールを送信する機能
2）メールの内容（本文、フィッシングを模したＵＲＬ情報、題名、発信元メールアドレス、発信元メールアドレス表示名）を任意に設定可能であること

■メールの扱いの検知機能
以下、送信したメールアドレスごとに
3）送信したメールの開封の有無の検知機能
4）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
5）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
6）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）
7）複数施設で並行して訓練実施可能であること
8）参加施設ごとに訓練結果の集計表が出力可能であること

3. 開発結果

2021 年度は、開発工数の関係から 1）,3）～6）までについて開発と検証を行うこととした。2）については、本文テキストは手動で設定することとし、メール本文に埋め込むＵＲＬについては検出機能との連携の関係からシステムが自動的に作成することとした。また、メールアドレス表示名の任意設定については、プロトタイプでは省略することとした。

メール開封、URL アクセス、添付ファイル開封の判定については、HTML メールおよび HTML 形式の添付ファイルを用い、Web サーバにアクセスが行われたかによって判定することとした。

以下、図 1 にメール作成画面のキャプチャ、図 2 に送信されたメールのイメージ、図 3 に管理画面のキャプチャを示す。

図 1 : メール作成画面 :　件名と本文は任意に設定可能。埋め込み URL と添付ファイル名は自動生成されるため、表示されていない。

図 2：送信されたスパムメール（仮）：本文や送信アドレス、URL などの偽装については機能検証のため省略している。また、HTML 形式メールのため、開封判定のために外部参照している画像の表示がメールクライアントの機能でブロックされている。

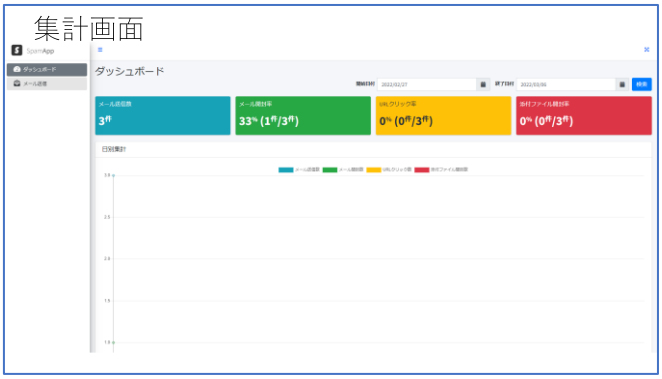

図 3：集計画面：メール送信数、開封率、ＵＲＬクリック率、添付ファイル開封率が集計可能。多施設対応は未実装。

D．考察

開発したシステムの試験運用の結果、メール開封、URL クリック、添付ファイル開封の検出は可能であった。但し、メール開封判定が HTML メールに埋め込んだ特定の画像が表示されたかで行っているため、プレビュー表示が無効に設定されている電子メールクライアントの場合、開封して本文の文字情報を表示しても Web サーバ上の画像へのアクセスがプレビュー抑止のため作動せず、開封の検出ができない場合があることが明らかとなった(結果図 2 参照)。

これについては、セキュリティ上の理由からプレビュー機能が初期段階では無効とされていることから、セキュリティ的にはより安全側になる設定であるため、この環境にも関わらず開封が検出されたケースはよりセキュリティ上の問題につながる可能性があることから、より対応に注意が必要であると考えられる。

なお、現時点の評価システムでは、以下の機能が未実装であることから、より訓練効果の高いダミーメール送信を実現するため、以下の点の追加開発が必要であると考えられる。

1）メール送信アドレスの表示名部分を任意に設定：標的型メールの多くの事例では、表示名が知人（上司、同僚、取引先関係者、など）となっているケースが多いため。

2）埋め込みＵＲＬ表示名を任意に設定：　同じく、認証画面や資料入手画面などへのリンクが設定されているケースが多いため。

3）添付ファイルを html 以外にＷｏｒｄ形式なども可能に：　同じく、Word のマクロによりマルウェア本体のダウンロードを行うものも存在するため。

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。

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プロトタイプ開発と検証を行った。その結果、開封判定には一部不可能なケースが存在することが明らかとなったが、これはセキュリティ的にはより安全な側の設定であり問題とはならないと考えられた。今後は、実際に多施設での訓練に適用し、その効果や訓練メールのあり方についての検討を進める。

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. 医療機関とサイバー攻撃標的型攻撃とランサムウェアを中心に. 週刊医学界新聞, 3411. 医学書院, 2021.

(2) 美代賢吾. 医療情報システムと新興感染症・災害・サイバー攻撃を考える；医療者・患者を支援し、診療を継続するために. IT Vision, 43：42-43, 2021.

H．知的財産権の出願・登録状況（予定を含む。）

特になし