# サイバー攻撃防御のための医療機関の情報セキュリティオーケストレーション基盤における情報収集に関する研究（30指1009）

報告書

課題番号：30指1009
研究課題名　：サイバー攻撃防御のための医療機関の情報セキュリティオーケストレーション基盤における情報収集に関する研究
主任研究者名 ：美代賢吾
分担研究者名 ：石井雅通、石割大範
キーワード　：医療情報システム、情報セキュリティ、プライバシー、病院管理

## 本研究の目的

- 近年のサイバー攻撃は情報または金銭の詐取を目的として組織的に実行
- 頻度と巧妙さが増し、患者情報など機微な情報をあつかう医療機関にとって大きな脅威
- 米国では、医療分野のISAC（Information Sharing and Analysis Center）が設立され、活動しており、国内においても、電力や鉄道、金融など医療以外の分野でISACが活動

- 組織的サイバー攻撃に対して、単独施設ではなく、攻撃情報の共有など、医療機関横断的に組織的に対処することが有効
- NCGMに対しても様々な形でのサイバー攻撃がおこなわれており、情報を集約し、複数の医療機関と連携し、サイバー攻撃情報の共有やマルウェア検体分析を行うための仕組みを構築
- 各医療機関での情報セキュリティ教育に生かすことで、技術的対応に加えて組織全体の情報セキュリティマネージメントの向上の可能性を検討
- 研究成果は、さまざまな形で公表し、日本の医療機関全体のセキュリティマネージメントの向上を図る

## 研究の方法と成果

### 情報セキュリティオーケストレーション基盤の開発・運用

1.1　情報セキュリティオーケストレーション基盤・ポータルの開発

- セキュリティに関する情報取集、集計分析を一元管理可能なポータルサイトの基盤構築をサイボウズのクラウド上で行った。ポータルサイトへのアクセスはクライアント証明書にて認証された端末から限られたユーザーのみアクセスが許可とした。
- 収集されたセキュリティ情報の分類は「悪意のあるサイト、フィッシング、標的型、注意喚起」の４項目に分類化した。
- 開発したシステムの概要は、次ページ参照

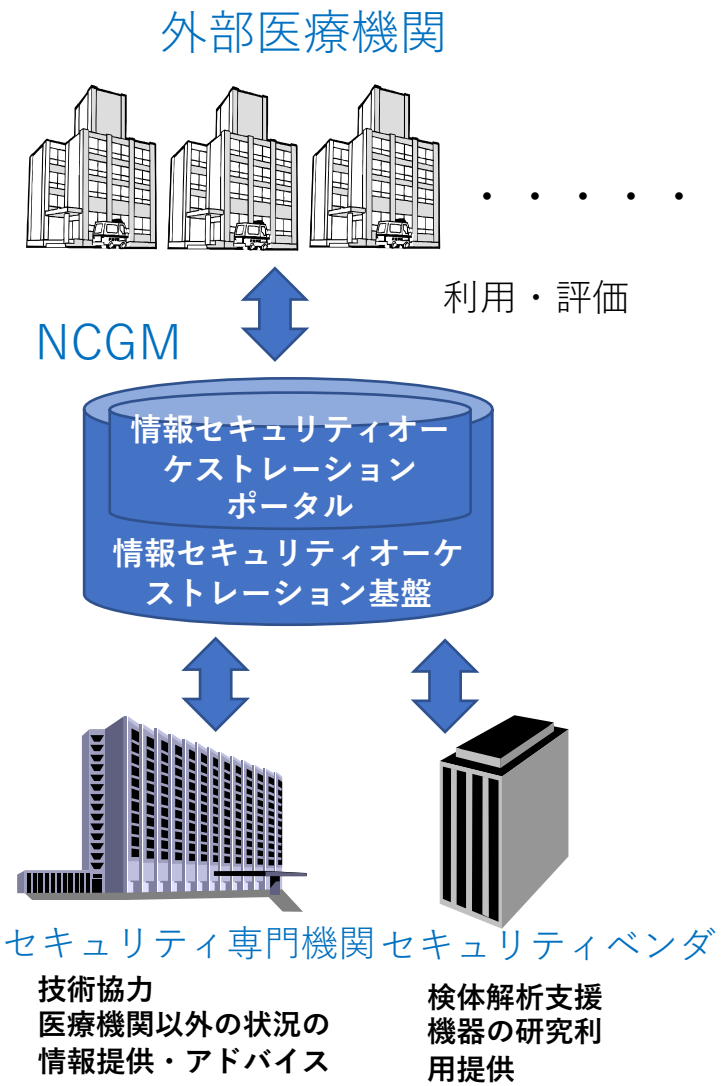
1.2情報セキュリティオーケストレーションポータルの評価

情報セキュリティオーケストレーションポータル及び登録されたセキュリティ情報に関して、外部医療機関の医療情報研究者にIDを発行し、実際に使用することで、意義や使用方法評価をおこなった。

**外部医療機関からの主な評価**

- 実例が収集されているため、被害にあったことが無い職員も疑似体験ができる
- 自分に来た怪しいメールを、このシステムで検索することにより、判断ができる
- 月ごとの攻撃種別のグラフにより傾向がつかめる
- 攻撃もとのURLがわかるため、自施設へのフィルタリングに活用できる
- 個別医療機関での情報収集は限界があるが、共有することにより全体でセキュリティを守ることができる

## 研究の全体像



# 情報セキュリティオーケストレーション基盤およびポータルの概要


①専用のログイン画面から限られた端末とユーザーのみがログインできる仕様で、セキュリティを考慮し構築


②ログインをすると外部機関や参加施設から提供されたセキュリティ情報を一覧で確認することが可能

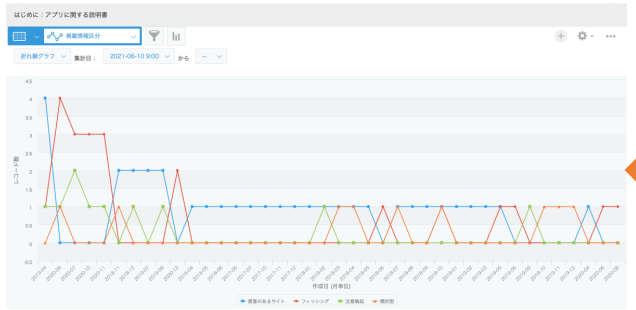
## セキュリティ情報の収集、ウイルス検体提供、集計


①外部医療機関からの専用の検体提供フォームを構築


②必要事項を入力し投稿することで、管理者が入力情報とマルウェア検体が確認できる。


③提供された情報、検体を解析後、結果を参加施　設がポータルサイトから確認可能

④セキュリティ情報を登録する際に攻撃手法や注意喚起の区分フラグを追加



⑤攻撃手法や注意喚起に登録された情報を自動的に集計しポータルサイトに日時で情報を更新しセキュリティ情報の可視化

## サイバー攻撃への対応方法の検討

### 2.1　職員に対する教育

- 情報セキュリティ教育のために実例に基づくコンテンツを作成し、研修を実施
- そのコンテンツをもとに学会等での発表を実施（右表参照）
- 標的型攻撃訓練用システムを開発し、訓練を実施

### 2.2　マルウェア解析等の分析対処能力に関する検討

セキュリティベンダー提供のマルウェア自動解析装置の運用と評価をおこなった。情報セキュリティ専門機関による手動解析をおこなった17件との一致率は17件中12件の70.6%、手動解析を正解とした場合の陽性的中率は、0.75（3/4）、陰性的中率0.818（9/11）であった。

## 結語

医療機関におけるセキュリティ情報を収集し共有するための仕組みを構築し評価した。個々の医療機関で得られる以上の情報が共有されることによる有用性が示唆された。

本研究の波及効果として、本研究の成果が、主任研究者を通じて、ヘルスケアISACに関わる厚生労働省委託事業および令和3年度の厚生労働科学研究に活用され、日本における医療機関の情報セキュリティ体制の構築へとつながることが期待される。

## 研究成果の公表

日本の医療機関全体のセキュリティ向上のため、研究成果は以下の通り、積極的に公開した

【論文】

1. 美代賢吾．医療機関に対するサイバー攻撃の現状とその対策．新医療，45(10):91-94，2018.
2. 美代賢吾、医療機関への攻撃の実例とその対応：今ここで何が起こっているのか（第39回医療情報学連合大会論文集、17-18）、2019.
3. 美代賢吾．医療施設におけるネットワークセキュリティの考察．新医療，47(11):22-25，2020.
4. 美代賢吾，急速に広がるオンライン診療・遠隔医療におけるサイバーセキュリティを考える；医療機関の情報セキュリティ管理者の役割：ある日の出来事から（第40回医療情報学連合大会論文集（CD-ROM））、2020.

【学会発表】

1. Miyo K. Organizing a Multi-Institutional Information Platform for Protection against Cyber-Attack onHealthcare. GMDS, 2018.9.3 (Osnabrueck, Germany)
2. 美代賢吾．医療機関を狙ったサイバー攻撃の現状と医療機器の情報セキュリティ；医療機関を狙ったサイバー攻撃：リスクと対策．第93回日本医療機器学会大会，2018.6.1（横浜）
3. 美代賢吾．医療期間における情報保護のための次の一歩．関東医療情報技師会．2019年9月9日（東京）
4. 美代賢吾．医療機関への攻撃の実例とその対応：今ここで何が起こっているのか．第39回医療情報学連合大会、2019年11月．（千葉）
5. 美代賢吾．大学病院が考えておくべきサイバーテロ対策．国立大学病院情報マネジメント部門連絡会議、2020年1月30日（秋田）
6. 美代賢吾．急速に広がるオンライン診療・遠隔医療におけるサイバーセキュリティを考える；医療機関の情報セキュリティ管理者の役割：ある日の出来事から．第40回医療情報学連合大会、2020年11月19日．（浜松）

【その他】

1. 美代賢吾．医療機関に対するサイバー攻撃の実態に迫る；今そこにある現実の危機にどう対処するか．モダンホスピタルショウ2018，2018.7.12（東京）
2. 美代賢吾．医療機関を取り巻く情報セキュリティの現状；攻撃されていないのか、気づいていないだけか．国際モダンホスピタルショウ特別企画医療情報システムWebセミナーEXPO，2020年11月（東京）
3. 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」．ITvision No.43. 2021.
4. 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．第3411号．2021.

謝辞：本研究の実施にあたり貴重なアドバイスをいただきました、大江和彦先生（東京大学医学部附属病院）、大原信先生（筑波大学病院）、川村浩二先生（東京都健康長寿医療センター）、紫藤秀文先生（東京医科大学病院）、山本俊成先生（琉球大学医学部附属病院）に深く感謝申し上げます。（50音順）