別紙3

厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）
分担研究報告書

テーマ：情報セキュリティ担当者が持つべき知識、備えるべきスキル、実行レベルに関する研究

研究分担者　鳥飼　幸太　群馬大学医学部附属病院システム統合センター　准教授
研究分担者　谷川 琢海　北海道科学大学　保健医療学部　診療放射線学科　准教授

研究要旨
近年、産業の種類を問わずサイバー攻撃が実社会に甚大な被害をもたらしている。医療においては電子カルテシステムを含む情報システムが攻撃された場合、入院・手術・外来にわたる診療停滞を引き起こすとともに、診療録が暗号化され、復号化を条件に身代金を要求するランサムウェア攻撃にも警戒しなくてはならない。攻撃に対応でき自施設の情報システムを守備できる能力ならびに日頃の備えを怠りなく進めるために、病院における情報セキュリティ担当者が持つべき知識、備えるべきスキル、実行レベルについて調査し情報処理推進機構(IPA)と共同で検討を行ったので報告する。

A．研究目的

日本の病院情報システムにおけるオーダリングシステム（医師の指示を電子化して取り扱う仕組み）は1990年頃に広がりを見せており、インターネットが一般に開放された1995年と前後する。1990年当時には病院間を情報システム接続する考え方は稀であること、病院における医療情報は守秘義務を履行する必要性から、病院情報システムは外部ネットワークとの接点を持たない「閉鎖系」を意識して構成されてきた。隔離の例外として、システム障害時の緊急メンテナンスラインや機器保守についてはISDNなどを用いたダイヤルアップ接続などが具備され利用されてきた。東日本大震災で津波の被害を被った病院において、遠隔地に電子化診療録のバックアップを作成していたことでカルテ喪失の被害を免れた事例が知られることになり、医療情報においてネットワークを介したバックアップが構成される活動が浸透したと考えられる。その後COVID-19の流行により、物理的隔離による感染防止対策と診療や業務の遂行を両立させる目的で、Webカメラやマイクを併用して対話コミュニケーションを行う仕組み(Web会議サービス)が急激に浸透した。併せて、信用を伴う情報操作（FinTech/オンライン通販など）が浸透し、費用を伴う社会活動について電子化が浸透した。特にWeb会議サービスは「ネットワークへの常時接続」が可能になることで、院内での隔離観察などにも広く活用されることとなった。一方、サイバー攻撃手段の拡充/カジュアル化が浸透し、攻撃ツール等がインターネットを介して容易に入手されるようになった。このように医療情報を取り巻く環境はこの10年程で大きく変遷しているが、医療機関における病院情報システムはその更新間隔が5年程度と長いため、医療機関によって対策の度合いに質的差異が生じている。2021年に被害が生じたつるぎ町半田病院ならびに2022年の大阪急性期総合医療センターではいずれもVirtual Private Network(VPN)の脆弱性を突いたランサムウェア攻撃が行われている。従来のサイバー攻撃では、マルウェア（悪意のあるソフトウェア）やコンピュータウィルスの被害が広く知られており、侵入経路の境界にソフトウェア等を設置するスタティック対策を行う境界型防御が主流であった。一方、広域ネットワ

ークからの人為的な侵入には、病院側でも人為的なアクティブディフェンス（早期検知・早期対応）が必要とされている。しかしながら、アクティブディフェンスを速やかに実施できる医療情報人材を備えた医療機関は必ずしも多くないことがこれまでの調査によって明らかになっている。そこで本研究では、均てん化を目標とした、現代的サイバー攻撃に対応できる、病院における情報セキュリティ担当者が持つべき知識、備えるべきスキル、実行レベルについて調査し情報処理推進機構(IPA)と共同で検討を行った。

B．研究方法

病院における情報セキュリティ担当者を速やかに育成するためには、ゼロベースからの教育ではなく、情報セキュリティに役立つ知識ならびに技能を備えた人材に対し、不足分の知識と技能を充当する方法が有効であると考えられる。情報セキュリティを担う基礎技能を有するロールモデルとして、病院情報システムの理解の観点からはカリキュラムが既に整備されている医療情報技師を、情報セキュリティの理解の観点からは情報安全管理確保支援士（IPA レベル 4）ならびに情報セキュリティマネジメント試験（IPA レベル 2）を基礎とした。

また、病院における情報セキュリティの能力として、次に示す３種類の職能人材を検討することとした。１：大病院ならびに高度急性期病院にみられる、高度に病院情報システムを運用しなければ診療が維持できない規模・高度化度合の病院に必要な能力を有し、更に他院がサイバー攻撃を受けた際に、その状況を迅速・的確にヒアリングして必要な示唆を提供する能力を有するグループ、

２：高度に病院情報システムを運用しなければ診療が維持できない規模・高度化度合の病院に必要な能力を有し、大規模なサイバー攻撃を受けた際には１：に所属する高度人材に連絡し、病院情報システムの状況の的確な説明ならびに必要な対策指示を正確に聞き取って自院の対策チームに指示展開できること、３：２に所属する人材の指示を正確に把握し、保守業者や病院スタッフからのヒアリングや指示展開を確実に行えること。

情報人材の名称については、これまで公共で停止されてきた名義と重複せず、かつその役目を適切に表象するものが必要であり、武田班の会議の中で議論を行った。コーポレートガバナンスの体制が、再考責任権限を信頼の元にチーフ制とする（CxO 制）機能分離を行う場合、情報セキュリティにおける最高責任者は Chief Information Security Officer(CISO)と呼ばれる。武田班では、厚労省において均てん化の施策として段階的に推進される診療録管理体制加算に対して、現時点で実施展開が可能な施策、ならびに将来的な人材の登用が可能になった場合に実施展開が可能な施策の両側面から検討を進めた。

先に示した３種類の職能人材については、１：について、医療情報技師育成部会が規定する上級医療情報技師、２：について医療情報技師以上の能力を備えていることを基礎とした。３：については、必ずしも資格に合格している必然性はないが、一定の講習を受けていることを条件とするような、到達要求ではなく履修要求の形での認定もあるのではないかとの議論が行われた。

以上の議論を元に、情報処理推進機構理事・奥村明俊氏、岩男英明氏との議論を重ね、３種類の職能人材が有するスキルについて表形式に表現することを試みた。

C．研究結果

CISO はサイバー攻撃を受けた際に、最高執行責任者(Chief Executive Officer)とともに経営に影響する最終判断を下す権限を有するが、日本の経営体制においては、最高責任者を複数のメンバーで分担しているとは限らないため、通俗的に用いられる CISO を先の職能人材１：の呼称として割り当てることが難しいのではないかと考えられ

る。このため、呼称については次年度以降の議論でより詳細に議論を行うことを提案した。３種類の職能人材が有するスキルについて表形式に纏めたものについて別添表１に示す。表では、奥村氏、岩男氏と協議し、必要技能分類として、
1・役職間の関係（任務分離）
2・Cybersecurity Framework(CSF)視点（攻撃者視点対策能力）
識別、防御、検知、対応、復旧の視点
3・Continuous Diagnostics and Mitigation (CDM)視点（防衛者視点対策能力）
データ、ネットワーク、認証とアクセス制御、資産管理、統合可視化
4・security-by-design（設計者視点）
（システム更新などの病院情報システム換装、新棟建設などにおける基礎設計の立案）
5・incident-response-recovery（緊急対応能力）
（APT などの攻撃を受けていることを覚知した後、速やかに防衛すること）
6・保守業務ならびに計画（運用維持能力）
の６題を要求項目として挙げた。

Ｄ．考察

これまでのサイバーセキュリティに関する議論から、稼働中に侵害・攻撃を受けるタイプのサイバー攻撃に対し、アクティブディフェンスを完遂するためには、攻撃を受けた機関のワークフローを事前に把握しておき、攻撃に対して機関が損なう機能や維持すべき機能を選択するとともに、迅速な検知・対応を進める必要があることが示されている。この意味では、あらゆる業態でのサイバーセキュリティにおけるアクティブディフェンス実践能力の付与とは、その業態におけるワークフローを適切に理解できる人材の育成が不可欠であることが導きだされる。一般に、ある機関における情報システムの構成は。支出可能な予算のタイミングや敷設された IT インフラの性状によって個性を有するため、ワークフローが理解できる人材の育成は当該機関の内部に長期間従事する人材に限定されることが示唆される。本研究はそのような長期に従事する人材が、特にサイバーセキュリティ対処能力を獲得する場合に参考となる技能要件を提案したことに意義を有するものと考えられる。また、班研究の議論当初で懸念されていた、高度な能力を有する人材は必ずしも潤沢に存在しないことを踏まえ、ファーストステップとしてあらゆる医療機関におけるサイバーセキュリティ向上能力の獲得を目指すとともに、頻度は少ないが被害の程度が大きい高度持続型脅威(Advanced Persistent Thread: APT)に対し、自組織外の支援を可能とする機関が緊急対応の支援を提供できる形でのカバー方法を提案したことに意義があると考える。

Ｅ．結論

本研究では、攻撃に対応でき自施設の情報システムを守備できる能力ならびに日頃の備えを怠りなく進めるために、病院における情報セキュリティ担当者が持つべき知識、備えるべきスキル、実行レベルについて調査し情報処理推進機構(IPA)と共同で検討を行い、表形式での要求項目を作成した。

Ｇ．研究発表

1.　論文発表
なし
2.　学会発表
[1] 鳥飼幸太　医療機関に特有の事業継続課題をシナリオとするサイバー攻撃対策：２・NISC シナリオベース訓練、第 27 回日本医療情報学会春季学術大会チュートリアル、2023 年 6 月

[2] 須藤泰史、鳥飼幸太　サイバー攻撃に備えた医療 IT-BCP の策定、第 27 回日本医療情報学会春季学術大会シンポジウム、2023 年 7 月

[3]鳥飼幸太、医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究、第 43 回医療情報学連合大会シンポジウム、2023 年 11 月

H．知的財産権の出願・登録状況

なし

1. 特許取得

なし

. 実用新案登録

なし

3.その他

なし

表１．情報セキュリティ人材が持つべき知識、備えるべきスキル

必要技能分類	Group A 人材	Group B 人材	Group C 人材
Cybersecurity Framework(CSF)視点 （攻撃者視点対策能力） 識別、防御、検知、対応、復旧の視点	他院の CSF 実施状況について、充実度を把握できること CSF の改善方法について Group B 人材ならびに他院の経営層にアドバイスできること	自院の CSF について調査できること 自院の CSF 向上ロードマップを起案できること CSF に基づく院内スタッフのセキュリティ教育を企画・実行できること	自院の CSF について理解できること CSF 向上ロードマップを理解し、適切なベンダーと具体化の情報収集ができること 作成された教育マニュアル等に基づき院内スタッフのセキュリティ教育を実施できること
Continuous Diagnostics and Mitigation (CDM)視点 （防衛者視点対策能力） データ、ネットワーク、認証とアクセス制御、 資産管理、統合可視化	他院の CDM 実施状況について、充実度を把握できること CDM の改善方法について Group B 人材ならびに他院の経営層にアドバイスできること	自院の CDM について調査できること 自院の CDM 向上ロードマップを起案できること CDM に基づく院内スタッフのセキュリティ教育を企画・実行できること	自院の CDM について理解できること CDM 向上ロードマップを理解し、適切なベンダーと具体化の情報収集ができること 作成された教育マニュアル等に基づき院内スタッフのセキュリティ教育を実施できること
Security-by-Design （設計者視点） システム更新などの病院情報システム換装、新棟建設などにおける基礎設計の立案	医療ワークフローならびに医療 IT システムに配慮したサイバーセキュリティデザインが提供できること 政府方針や各種ガイドラインなどに基づくセキュリティ強化方針を理解でき、自院ならびに他院の改善方針と統合できること	自院における長期システム改善計画をセキュリティ、運用改善の両面から検討し、起案できること Group C 人材からの運用上の課題を把握でき、起案を適切に編集できること 不足箇所を適切に認識し、Group A 人材や専門家へコンサルテーションを依頼できること	自院において策定された長期システム改善計画を理解し、適切なベンダーに対して調査依頼ができること 運用保守における実作業をマニュアル化し、Group C 人材間でスキル習得ならびに共有ができること
Incident-Response-Recovery （緊急対応能力） APT などの攻撃を受けていることを覚知した後、速やかに防衛すること	システム停止に伴う診療停止時に、状況把握に基づく医療ワークフローにおける医療事故発生リスクとフォレンジック不能リスクを推測し、Group B 人材に対して優先順位と共に作業指示が出せること 長期間の診療停止に際してシステム的、医療ワークフロー的に配慮すべき点を復旧段階に応じて適切にアドバイスできること	診療停止を伴わないインシデント（部門システムの停止など）時に、院内状況を適切に把握し、バックアップ保全などの 1 次的緊急対策を指示できること 関係省庁、警察サイバー課、情報システムを通じた診療連携を行なっている関連病院への速やかな連絡が指示できること 経営層に対し、記者会見などに必要な院内状況を端的に纏め、迅速に提出できること	提供されている適切な手段に基づき、日常的な脅威を監視できること 攻撃の予兆に気づくことができ、Group B 人材以上に速やかに連絡・報告ができること Group B 人材の指示を理解でき、システム操作などの実務が確実に行えること
保守業務ならびに計画 （運用維持能力）	サイバーセキュリティ対策の先端ソリューションを把握し、自院および他院の全体における対策実施の最適解を提案できること 実務負荷、コスト、長期的視点のバランスが取れた保守計画を提案できること	自院の全体に対してセキュリティ保守業務で調査すべき点を適切に割り出せること Group C 人材ならびにベンダーと協力し、全体的な保守業務についての改善計画を立案できること Group C 人材ならびにベンダーと協力し、部分的な保守業務についての改善計画を実施できること	Group B 人材の立案に基づき、業務負荷の変化について正確な情報を提供できること 定められた保守要件に従い、確実な保守業務を遂行できること 保守計画の見直しに際し、業務範囲内での効率改善などを提案できること

表2. 情報セキュリティ人材が持つべき資格・試験

必要技能分類	医療情報技師	上級医療情報技師	IPA レベル 2 （情報セキュリティマネジメント ）	IPA レベル 3 （応用情報技術者）	IPA レベル 4 （情報処理安全確保支援士）
役職間の関係 （任務分担）	GIO7.4（医療情報システムの安全管理に関するガイドライン）	6（情報セキュリティについて理解し、対策を講じることができる能力を習得する） 6-2-8（医療情報の外部委託に関する瀬キュリティについての知識を有しており、対応できる）	Group A 人材または Group C 人材について習得すべき知識・技能に相当する	「修得し、適用する」：知識を規則や原理などにあてはめ、自ら解決していく能力が必要な項目 「修得し、応用する」：知識を状況に応じて組み合わせ、また応用し、自ら解決していく能力が必要な項目	「修得し、高度に応用する」： プロフェッショナルとして、高度な知識を状況に応じて組み合わせ、また応用し、自ら解決していく能力が必要な項目
Cybersecurity Framework(CSF) 視点	NIST CSF GIO7.5（医療・介護関係事業者における個人情報の適切な取り扱いのガイダンス）	6-2-2（情報セキュリティ対策における PDCA サイクルを実践できる） 6-2-5（セキュリティ千咲の分類について説明ができ、活用できる） 6-2-7（リスク対策の分類を知り、適切に適用できる）	I 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること II 情報セキュリティマネジメントの運用・継続的改善に関すること 9 情報セキュリティの意識向上	大分類 8:経営戦略 中分類 20:技術戦略マネジメント 大分類 3:技術要素 中分類 11:2. 情報セキュリティ管理 大分類 3:技術要素 中分類 11:セキュリティ 1. 情報セキュリティ 4. 情報セキュリティ対策	1 情報セキュリティマネジメントの推進又は支援に関すること
Continuous Diagnostics and Mitigation （CDM） 視点	CISA CDM GIO4.4（病院情報システムの評価・改善を理解できる）	2-5-5（情報システムに関する問題点やリスクを評価し、改善に向けた方向性を示すことができる） 6-2-3（セキュリティポリシーについての知識を有しており、相応の実践を実行ないし指示できる）	II 情報セキュリティマネジメントの運用・継続的改善に関すること 9 情報セキュリティの意識向上	大分類 3:技術要素 中分類 11:2. 情報セキュリティ管理 大分類 3:技術要素 中分類 11:セキュリティ 1. 情報セキュリティ 4. 情報セキュリティ対策 大分類 5:プロジェクトマネジメント 中分類 14:プロジェクトマネジメント 1. プロジェクトマネジメント	3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること
Security-by-Design （設計者視点）	GIO7.6（医療情報に関する各種ガイドライン）	6-2-6（セキュリティ対策に関する先端的技術・方策につき情報収集できる） 7-8（保健医療福祉分野における各種標準規格について例示できる）	I 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること 4 情報セキュリティを継続的に確保するための情報セキュリティ要求事項の 提示 3-2 部門の情報システムの 調達・利用に関する技術的及び運用のセキュ リティ	大分類 3:技術要素 中分類 11:セキュリティ 1. 情報セキュリティ 大分類 3:技術要素 中分類 11:セキュリティ 3. セキュリティ技術評価 大分類 3:技術要素 中分類 11:セキュリティ 5. セキュリティ実装技術 大分類 7:システム戦略 中分類 18:システム企画 大分類 4:開発技術 中分類 12:システム開発技術 1. システム要件定義・ソフトウェア要件定義 2. 設計 3. 実装・構築	2 情報システムの企画・設計・開発・運用でのセキ ュリティ確保の推進又は支援に関すること
Incident-Response-Recovery （緊急対応能力）	GIO2.4（診療全般・診療録の電子化に関するシステム） GIO2.5（外来診療に関する機能） GIO2.6（入院診療に関する機能）	6-2-4（リスクによる損害とのバランスを考慮した対策を行うことができる） 7-3（地域連携における連携施設間の業務フローを説明できる） 6-3（情報セキュリティに関するインシデントおよびアクシデントへの対応ができる）	II 情報セキュリティマネジメントの運用・継続的改善に関すること 8 情報セキュリティインシデントの管理 8-1 発見 8-2 初動処理 8-3 分析及び復旧 10 コンプライアンスの運用	大分類 3:技術要素 中分類 11:2. 情報セキュリティ管理 大分類 9:企業と法務 中分類 23:法務 2. セキュリティ関連法規	4 情報セキュリティインシデント管理の推進又 は支援に関すること
保守業務ならびに計画 （運用維持能力）	GIO4（病院情報システムの運用） GIO4.2（病院情報システムの運用管理規程）	2-5-2（情報資産のライフサイクルを考慮した保守計画を策定できる） 2-5-6（保守計画の遂行に必要となる要因、資源およびコストを管理できる）	II 情報セキュリティマネジメントの運用・継続的改善に関すること 6 部門の情報システム利用時の情報セキュリティの確保 11 情報セキュリティマネジメントの継続的改善 12 情報セキュリティに関する動向・事例情報の収集と評価	大分類 4:開発技術 中分類 12:システム開発技術 2. 情報セキュリティ管理 大分類 4:開発技術 中分類 12:システム開発技術 6. 保守・廃棄 大分類 6:サービスマネジメント 中分類 15:サービスマネジメント 1. サービスマネジメント	2-7 運用・保守（セキュリティの観点）