

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

安全な地域医療の継続性確保に資する医療機関における  
情報セキュリティ人材の育成と配置に関する研究

(令和)5年度 総括・分担研究報告書

研究代表者 武田 理宏

(令和)6(2024)年 5月

## 目 次

I. 総括研究報告	
安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究	1
武田 理宏 (資料) なし	
II. 分担研究報告	
1. 情報セキュリティ人材配置に関するアンケート調査に関する研究	19
武田理宏、鳥飼幸太、谷川琢海、川真田実、肥田泰幸 (資料) 調査依頼と質問項目一覧	
2. 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	42
鳥飼幸太、谷川琢海 (資料) 情報セキュリティ人材別表	
3. 情報セキュリティに関する医療系専門職等の教育状況および医療情報に関する専門職の育成状況の把握に関する研究	48
谷川琢海 (資料) なし	
4. 情報セキュリティに対する医療系専門職（診療放射線技師）の教育状況の調査に関する研究	58
川真田実 (資料) なし	
5. 情報セキュリティに対する医療系専門職（臨床工学技士）の教育状況の調査に関する研究	61
肥田泰幸 (資料) なし	
6. 情報セキュリティに関する業務を担う可能性のある医療系専門職の調査に関する研究	64
武田理宏、鳥飼幸太、谷川琢磨、川真田実、肥田泰幸、吉川肇 (資料) なし	
III. 研究成果の刊行に関する一覧表	68

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)  
総括研究報告書

テーマ:安全な地域医療の継続性確保に資する医療機関における  
情報セキュリティ人材の育成と配置に関する研究

研究代表者 武田理宏 国立大学法人大阪大学大学院医学系研究科 医療情報学 教授

研究要旨

本研究では、保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とする。令和5年度は、情報セキュリティ人材の適正状況、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、実行レベル等の検討、情報セキュリティに対する医療系専門職の教育状況を調査し、情報セキュリティ人材の人材育成、医療機関への適正配置について議論を行った。

情報セキュリティ人材の適正状況の調査では、医療機関でのサイバーインシデントの発生や厚生労働省の施策により医療情報システム安全管理責任者の配置が進む一方、情報セキュリティに関する資格、試験の保有率は低く、情報セキュリティに関する知識の担保を如何に行うかが課題と考えられた。

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、実行レベル等の検討では、医療機関を3つのグループに分類し、それぞれの組織の情報セキュリティ人材が持つべき知識、備えるべきスキルを「役職間の関係」、「Cybersecurity Framework(CSF)視点」、「Continuous Diagnostics and Mitigation (CDM)視点」、「security-by-design, incident-response-recovery」、「保守業務ならびに計画」の6題に対して要求項目を整理した。6題に対して、(上級)医療情報技師や情報処理推進機構(IPA)が定める情報セキュリティに関する資格、試験の到着目標のマッピングを行った。

情報セキュリティに対する医療系専門職の教育状況の調査では、(上級)医療情報技師、診療放射線技師、臨床工学技士、診療情報管理士を調査の対象とした。診療放射線技師、臨床工学技士、診療情報管理士は教育カリキュラムに情報セキュリティに関する項目が含まれていたが、総論的な内容で、追加の教育が必要と考えられた。現時点では、上級医療情報技師、医療情報技師が、医療情報システムや情報セキュリティの教育カリキュラムが充実していた。

以上の調査結果を踏まえ、研究班で「人材」、「組織体制」、「教育体制」の観点で、情報セキュリティ人材の配置についての議論を行った。

研究代表者

武田理宏(国立大学法人大阪大学大学院  
医学系研究科 医療情報学 教授)

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)

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)

川真田 実(大阪府立病院機構国際がんセ  
ンター 放射線診断・IVR科 副技師長)

肥田 泰幸(東都大学 幕張ヒューマンケア  
学部臨床工学科 助教)

研究協力者

吉川 肇(一般社団法人日本病院会 事業  
部 部長)

A. 研究目的

医療分野は、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国

民生活または社会経済活動に多大なる影響を及ぼす恐れが生じる重要インフラ分野の1つに定められている。また、政府においては、医療DX推進本部を設置し、医療分野におけるDXをスピード感を持って進めているところ、近年、医療機関におけるサイバー攻撃被害が増加しており、地域医療を支える医療機関が、実際に、サイバー攻撃により、長期にわたり診療が停止し、地域医療の安全性を脅かす事案が発生している。

政府の有識者会議において、2022年9月に「医療機関のサイバーセキュリティ対策の更なる強化策」をとりまとめ、医療機関向けサイバーセキュリティ対策研修の充実、医療分野におけるサイバーセキュリティに関する情報共有体制(ISAC)の構築、インシデント発生時の駆けつけ機能の確保ならびに対応手順の作成と訓練の実施等の短期的な策を講じている。また、並行してサイバーセキュリティ対策の強化も踏まえ、「医療情報システムの安全管理に関するガイドライン」の改定も進められている。

本研究では、これらの医療を取り巻く社会状況や技術動向を踏まえ、安全・安心な地域医療を継続的に維持確保するために必要な保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とし、関係する省庁・学会・業界団体等と連携しながら調査・試作・検証・評価等を行う。

## B. 研究方法

### 1. 概要

本研究班の概要を図1に示す。

最初に医療機関の情報セキュリティ担当者

の実態調査(雇用条件、業務内容、保有資格など)を実施する。本調査により、現在の医療機関の情報セキュリティ対策の課題を把握するとともに、本研究成果物となる提言が各医療機関の実態を踏まえたものするための資料とする。

これと並行し、各医療機関の情報セキュリティ担当者が目指すべき目標を明確にするため、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、実行レベル等の検討を行う。

医療機関の経営状況や情報セキュリティ人材の状況、多くの医療機関に広く情報セキュリティ担当者を配置する必要があることを考えると、各医療機関が新規に情報セキュリティ人材を雇用するだけでなく、医療機関の既存人材の活用を考える必要がある。そこで、情報セキュリティを担当できる可能性のある医療系専門職に対し、情報セキュリティに対する教育状況の調査を実施する。研究計画を立てた段階で、上級医療情報技師、医療情報技師、診療放射線技師、臨床工学技士が、医療機関の情報セキュリティを担う人材の候補として挙げたが、他に情報セキュリティを担う可能性のある医療系専門職についても調査を行う。

令和6年度は、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、実行レベルと情報セキュリティに対する医療系専門職の教育状況を比較し、医療系専門職がそれぞれの知識やスキル等に加えて持つべき、または、備えるべき情報セキュリティに関する知識、スキル、資格や認定等の検討を行う。

以上の研究成果を取りまとめ、情報セキュリティ人材を継続して雇・配置等するための課題を調子した上で、「医療分野における持続可能な情報セキュリティ人材育成と継続的雇用・配置・キャリア形成等に関する提言」、「医療安全の確保や医療の質保証と情報セキュリティ対策

の確保に関して、継続的にPDCAサイクルを実行するための提言」に作成を行う。

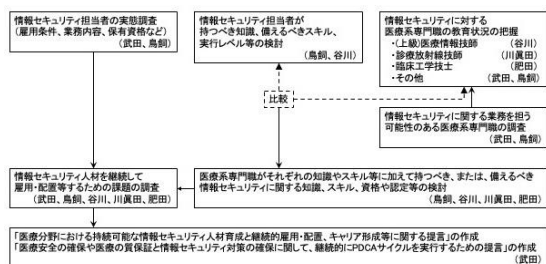


図1. 医療機関における情報セキュリティ人材の育成と配置に向けた検討課題

## 2. 情報セキュリティ担当者の実態調査(担当: 武田・鳥飼、分担研究成果報告書1)

Microsoft office 365 の Form を用いて、医療情報システム安全管理責任者と情報セキュリティ担当者の配置状況と保有する資格について、Web アンケート調査を行った。具体的な質問内容は R5 年度分担者報告書 1\_添付資料\_調査依頼と質問項目一覧のとおり。

## 3. 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、実行レベル等の検討(担当: 鳥飼・谷川、分担研究成果報告書 2)

医療機関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、分担研究者と情報処理推進機構(IPA)と共同で検討を行った。

医療機関における情報セキュリティ担当者は医療情報システムと情報セキュリティの双方の理解が求められる。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、医療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。

## 4. 情報セキュリティに対する医療系専門職の教育状況の調査(担当: 谷川(上級医療情報技師、医療情報技師)、分担研究成果報告書3、川眞田(診療放射線技師)、分担研究成果報告書4、肥田(臨床工学技士)、分担研究成果報告書5)

## 情報セキュリティに関する業務を担う可能性のある医療系専門職の調査(担当: 武田・鳥飼、分担研究報告書6)

本研究班では研究計画当初、情報セキュリティを担当する医療系専門職の候補として、上級医療情報技師、医療情報技師、診療放射線技師、臨床工学技士を上げた。教育状況については、それぞれの専門職の資格を持つ分担研究者が調査を行った。上記の専門職以外で、情報セキュリティを担当する候補となる医療系専門職を研究班で議論を行った。その結果、診療情報管理士が候補に上がった。診療情報管理士の教育状況を調査するため、診療情報管理士を企画、運営している一般社団法人日本病院会に研究協力依頼を行った。情報セキュリティ担当者の実態調査から、他に候補となる医療系専門職の有無を確認した。

## 5. 総合討論(担当: 武田、鳥飼、谷川、川眞田、肥田、吉川)

情報セキュリティ人材の実態調査、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、実行レベル等の検討、情報セキュリティに対する医療系専門職の教育状況の調査を踏まえ、研究班で総合討論を行った。

## C. 研究結果

### 1. 情報セキュリティ担当者の実態調査(担当:

## 武田・鳥飼、分担研究成果報告書1)

643 施設から回答があった。

医療情報システム安全管理責任者を配置する医療機関は 521 施設(81%)であった。医療情報システム安全管理責任者の職位は院長が 127 施設(24%)、院長を補佐する立場が 83 施設(16%)、事務部門の長が 73 施設(14%)で、医療情報システム部門の長が 144 施設(28%)であった。

医療情報システム安全管理責任者のうち、上級医療情報技師の資格を保有するのは 12 名(2%)、医療情報技師が 72 名(14%)、情報処理安全確保支援士が 4 名(0.8%)、応用情報技術者試験が 10 名(2%)、基礎情報技術者試験が 23 名(4%)、情報セキュリティマネジメント試験が 12 名(2%)であった。上記いずれの資格を有さない医療情報システム安全管理責任者は 440 名(84%)であった。

院長、院長を補佐する立場、事務部門の長(合わせて 283 施設)に限定すると、上級医療情報技師の資格を保有するのは 1 名(0.3%)、医療情報技師が 7 名(2%)、情報処理安全確保支援士が 2 名(0.7%)、応用情報技術者試験が 1 名(0.3%)、基礎情報技術者試験が 1 名(0.3%)、情報セキュリティマネジメント試験が 2 名(0.7%)で、上記いずれの資格を有さない医療情報システム安全管理責任者は 273 名(96%)であった。

医療機関で情報セキュリティ対策を講じるためには、情報セキュリティ対策の方針を策定し、全職員に周知するとともに、情報セキュリティ対策への投資が必要となる。このため、医療情報システム安全管理責任者が、経営・運営上の意思決定に関与する立場にあるか否かは重要である。本調査では、医療情報システム安全管理責任者のうち 350 名(67%)が意思決定に関与

する立場であった。意思決定に関与する立場であるのは、上級医療情報技師が 12 名のうち 3 名(25%)、医療情報技師が 72 名のうち 24 名(33%)、情報処理安全確保支援士が 4 名のうち 3 名(75%)、応用情報技術者試験が 10 名のうち 4 名(40%)、基礎情報技術者試験が 23 名のうち 4 名(17%)、情報セキュリティマネジメント試験が 12 名のうち 5 名(42%)であった。上記いずれかの資格を有する 81 名のうち、意思決定に関与する立場であるのは 30 名(37%)であった。

各医療機関における情報セキュリティ対策の必要性の高まりや診療情報管理加算での医療情報システム安全管理責任者の配置などにより医療情報システム安全管理責任者を配置する医療機関は多く見られた。一方、情報セキュリティに対する資格、試験を保有する医療情報システム安全管理責任者は少なかった。資格、試験だけで情報セキュリティの知識を測ることはできないが、医療機関における立場から医療情報システム安全管理責任者となっているが、情報セキュリティに知識が十分でない方が相当数いることが推測された。

すくなくとも 1 名は医療情報システムの情報セキュリティ事案の担当者を配置している医療機関は 499 施設(78%)と、医療情報システム安全管理責任者を配置する医療機関より施設数は少なかった。3 人目までに登録された医療情報システムの情報セキュリティ事案の担当者 922 人のうち、上級医療情報技師の資格を保有するのは 28 名(3%)、医療情報技師が 257 名(28%)、情報処理安全確保支援士が 12 名(1%)、応用情報技術者試験が 52 名(6%)、基礎情報技術者試験が 56 名(6%)、情報セキュリティマネジメント試験が 22 名(2%)であった。上記いずれの資格を有さない医療情報システム

の情報セキュリティ事案の担当者は 530 名 (57%) であった。情報セキュリティに関する資格、試験を保有する割合は、医療情報システム安全管理責任者よりも高い割合であったが、半数以上はこれらの資格、試験を保有していなかった。

回答があった 643 施設のうち、51 施設 (8%) は医療情報システム安全管理責任者、医療情報システムの情報セキュリティ事案の担当者のいずれも配置していなかった。400 床以上の医療機関 (235 施設) では、医療情報システム安全管理責任者、医療情報システムの情報セキュリティ事案の担当者のいずれも配置していなかった施設は 1 施設のみであった。一方、情報セキュリティに関する資格、試験 (上級医療情報技師、医療情報技師、情報処理安全確保支援士、応用情報技術者試験、基礎情報技術者試験、情報セキュリティマネジメント試験) を保有する人材を 1 名も配置していない医療機関は 461 施設 (72%)、400 床以上の医療機関では 150 施設 (33%) であった。

今回のアンケート調査では、400 床以上の医療機関を中心に情報セキュリティに関わる人材配置が進んでいたが、情報セキュリティの資格、試験の保有率は低かった。各医療機関が情報セキュリティに対する知識を高めるためには、情報セキュリティに対する資格、試験の保有率を上げる必要があり、資格、試験の取得を誘導する仕組みを考える必要があると考えられた。一方、資格、試験の保有率の低さから、性急な制度変更を行うと各医療機関が対応できない可能性があるため、十分な周知期間と教育コンテンツの整備などが必要と考えられた。

## 2. 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、実行レベル等の検討 (担当:

### 鳥飼・谷川、分担研究成果報告書 2)

医療機関における情報セキュリティの能力として、1 : 大病院ならびに高度急性期病院にみられる、高度に医療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 : 高度に医療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、医療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ができるグループ、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こなせることができるグループに分類した。

3 種類の職能人材が持つべき知識、備えるべきスキルについては、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)、3. Continuous Diagnostics and Mitigation (CDM) 視点 (防衛者視点対策能力)、4. security-by-design (設計者視点)、5. incident-response-recovery (緊急対応能力)、6. 保守業務ならびに計画 (運用維持能力) の 6 題に対して要求項目を整理した。また、6 題に対して、医療情報技師、上級医療情報技師、情報セキュリティマネジメント (IPA レベル 2)、応用情報技術者 (IPA レベル 3)、情報処理安全確保支援士 (IPA レベル 4) のそれぞれの団体が定める到着目標のマッピングを行った。

3. 情報セキュリティに対する医療系専門職の教育状況の調査(担当:谷川(上級医療情報技師、医療情報技師)、分担研究成果報告書3、川真田(診療放射線技師)、分担研究成果報告書4、肥田(臨床工学技士)、分担研究成果報告書5)

情報セキュリティに関する業務を担う可能性のある医療系専門職の調査(担当:武田・鳥飼、分担研究報告書6)

情報セキュリティ担当者の実態調査では、診療情報管理士は、医療情報システム安全管理責任者 521 名のうち 30 名、医療情報システムの情報セキュリティ事案の担当者 922 名のうち 119 名、合計 149 名が保有しており、情報セキュリティに関する業務を担う可能性がある医療系専門職として検証する必要があることが確認された。その他の職種では、臨床検査技師が合計 19 名と多かったが、上級医療情報技師の保有割合が 27%、医療情報技師の保有割合が 43%と、他の専門職に比べて高く、臨床検査技師の資格より、上級医療情報技師、医療情報技師として情報セキュリティ対策に関わっている可能性が高いと判断して、検証の候補から除外した。

医療情報技師の到達目標には、「診療録およびその他の医療記録」(医学・医療系 GIO-8)、「医療管理」(医学・医療系 GIO-3)、「病院情報システムの機能」(医療情報システム系 GIO-2)、「病院情報システムの運用」(GIO-4)、「医療情報分野の関連法規とガイドライン」(医療情報システム系 GIO-7)、「情報セキュリティ」(情報処理技術系 GIO-6)などの情報セキュリティへの対応に必要な内容が網羅的に含まれていた。上級医療情報技師の一般目標及び行動目標群 (GIO・SBOs) ver.1.5 では、「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修得する」(GIO-6) など、医療情報システムに対する情報セキュリティの実践に必要な内容が示されていた。また、生涯研修セミナーや e-Learning コンテンツが用意されており、情報セキュリティに関する内容のものも含まれていた。

診療放射線技師では、情報セキュリティ教育としては専門分野に医療画像情報学 6 単位、医療安全管理学 2 単位が定められていた。医療画像情報学では、情報処理学、医療画像、医療情報の 3 つの細項目が設けられていた。医療安全管理学では医療安全の基礎、放射線診療の安全管理、医療機器および機器の安全管理、医薬品の安全管理、救急医療、診療の補助行為に関する安全管理の 6 つの細項目から構成されていた。しかしながら、教育期間中に情報セキュリティ対策の全てを学習することは厳しいと考えられた。卒後の診療放射線技師に対して、専門技師制度の一つとして、日本医用画像情報専門技師共同認定育成機構(社員は日本医療情報学会と日本放射線技術学会の 2 団体)が参画しており、医用画像情報専門技師の認定を行っている。医用画像情報専門技師は、医療情報技師の能力を礎に、医用画像の高度な知識と豊かな経験を備えており、最低限習得すべき技術・知識として情報セキュリティが含まれていることから、情報セキュリティを担う人材候補であると考えられた。

臨床工学技士の情報セキュリティ教育としては専門基礎分野に臨床工学に必要な医療情報システムとシステム工学の基礎として 7 単位が定められている。臨床工学に必要な医療情報システムとシステム工学の基礎では、必修科目として 1.情報科学概論、2.情報リテラシー、3.システム工学基礎、4.情報処理技



術基礎、5.医療情報処理技術、6.医療情報システム、7.情報通信ネットワーク、8.医療用 IoT 概論が、選択科目として、1.パソコン基礎演習、2.医療情報処理技術演習、3.医療情報システム演習、4.医用画像処理情報技術、5.人工知能が設けられ、医療情報システムの特性や医療機器との情報連携、情報リテラシーや情報通信ネットワークに加えて、実技による医療情報処理技術演習、医療情報システム演習によって情報セキュリティに関する知識を学習することができるカリキュラムが構成されている。一方、情報セキュリティ対策については、総論的、基礎的な内容となっており、臨床工学技士の教育コンテンツで、情報セキュリティ対策のすべてを学習することは難しいと考えられた。公益社団法人日本臨床工学技士会では、サイバーセキュリティに関して世論に広く注意を促す啓発動画の公開や IPA 独立行政法人情報処理推進機構が実施する各種国家試験や一般社団法人日本医療情報学会が実施する医療情報技師能力検定試験の受験を支援する「ICT 分野の国家資格等取得における奨励金制度」を実施している。本制度を利用して医療情報技師や IPA の資格の取得が進む事で、臨床工学技士は情報セキュリティを担う良い人材となりうる。

診療情報管理士は、日本病院会診療情報管理士教育委員会が策定した通信教育カリキュラムに保健医療情報学が自習時間 17 時間、授業 3 時間の 2 単位が定められている。診療情報管理士の養成テキストでは、保健医療情報学の項目として、医療情報システムと情報セキュリティが設けられている。医療情報システムでは、1.医療情報システムとは、2.病院情報システム概論、3.部門の業務を支える情報システム、4.オーダエントリーシステム、5.電子カルテシステム 6.地域医療情報システムの細項目が設け

られ、医療情報システムの特性や多施設での医療情報連携を学習することができるコンテンツとなっている。情報セキュリティでは、1.診療情報の安全管理、2.医療情報システムにおけるセキュリティ対策、3.医療情報システムの安全管理に関するガイドライン、4.医療情報システムの安全管理、5.診療情報管理士として実践すべき事項が細項目として設けられ、情報セキュリティ担保に向けたガイドラインの把握や情報セキュリティ対策が学習できるコンテンツとなっている。一方、情報セキュリティ対策については、総論的、基礎的な内容となっており、診療情報管理士の教育コンテンツで、情報セキュリティ対策のすべてを学習することは難しいと考えられた。紙カルテから電子カルテへの移行に伴い、医療情報技師の資格を取得する診療情報管理士が増加している。情報セキュリティ担当者の実態調査では、情報セキュリティを担当する診療情報管理士 149 名のうち、上級医療情報技師が 8 名(5%)、医療情報技師が 42 名(28%)、情報処理安全確保支援士が 3 名(2%)、応用情報技術者試験が 8 名(5%)、基礎情報技術者試験が 12 名(8%)、情報セキュリティマネジメント試験が 13 名(9%)、資格、試験を有していた。

医療系専門職の過去 5 年の国家試験で情報セキュリティに関する出題が行われていたのは、診療放射線技師が 2 問、臨床検査技師が 1 問、臨床工学技士が 10 問であり、臨床工学技士国家試験では毎年、出題されていた。問題の内容は、いずれも情報セキュリティに関する基礎的な技術に関する内容の出題であった。医療情報技師能力検定試験は、過去 5 年間の出題実績では、医療情報システム系(全 60 問)と情報処理技術系(全 50 問)においてそれぞれ 10 問程度の出題があった。

診療情報管理士は試験問題が非公開で出題数は調査できなかった。

情報セキュリティを担当する候補となる医療系専門職では、上級医療情報技師、医療情報技師が医療情報システム、情報セキュリティについて、もっとも教育カリキュラムが整備されていた。診療放射線技師、臨床工学技士、診療情報管理士についても医療情報システム、情報セキュリティに関する教育コンテンツは整備されていたが、いずれも総論的な内容で、教育カリキュラム全体のボリュームからも、教育期間に情報セキュリティの知識を十分に習得することは容易でないと考えられた。一方、診療放射線技師は医用画像情報専門技師、臨床工学技士は ICT 分野の国家資格等取得における奨励金制度、診療情報管理士はその職域から医療情報技師や IPA の資格の保有率が高いことから、資格取得後の専門教育として、医療情報技師や IPA の資格の取得を誘導することが良いと考えられた。

医療情報技師や上級医療情報技師は情報セキュリティの教育コンテンツが充実しているものの、特に医療情報技師は当該領域の学習が必須とはなっていない(他の領域の成績が良ければ資格を取得できる)。このため、医療情報技師や上級医療情報技師間で、情報セキュリティに関する知識のばらつきは大きいことが予想される。IPA が提供する資格・試験は情報セキュリティに対する知識が担保されるものとなるため、医療情報技師や上級医療情報技師に IPA の資格・試験の取得を勧める、あるいは情報セキュリティの e-learning 等の教育コンテンツを受講した医療情報技師や上級医療情報技師に対して受講証明を出すなど、情報セキュリティの知識を担保する仕組みを検討する必要があると考えられた。

#### 4. 総合討論(担当:武田、鳥飼、谷川、川眞田、肥田、吉川)

これまで、6 回の班会議を開き、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、実行レベル等について、検討を重ねてきた。

情報セキュリティは紙に記載される情報から、インターネットに上がる情報まで、セキュリティの対象は広い。本研究班で議論するセキュリティの対象を明確にするため、サイバーセキュリティという表現を使用することが適切であるとの意見が上がった。

医療機関に必要な情報セキュリティ人材は①情報セキュリティ対策の知識、スキルを有し、実行できる力があること、②保健医療福祉分野の特性を理解していることが求められる。

本研究班では、これらの情報セキュリティ人材について、「人材」、「組織体制」、「教育体制」に分けて整理を行った。

#### 【情報セキュリティ人材】

##### Group A 人材:

- ・自立して自院の情報セキュリティを向上できる能力があること。
- ・自院の経営層に情報セキュリティ改善の提案ができること。
- ・重大事象発生時に、適切な防御、反応を起案し指示できること。
- ・他院の Group B 人材の指導育成を行う能力を有すること。
- ・他院の経営層から情報セキュリティの相談を受けられること。
- ・長期の診療停止に至る重大インシデントに対して監督できること。
- ・Group C 人材からの問い合わせに適切なコンサルテーションを提供できること。

### Group B 人材:

- ・自立して自院の情報セキュリティを向上できる能力があること。
- ・自院の経営層に情報セキュリティ改善の提案ができること。
- ・重大事象発生時に、適切な防御、反応を起案し指示できること。

### Group C 人材:

- ・必要に応じて事業者と連携して、自院の情報セキュリティを向上できる能力があること。
- ・自院の情報セキュリティに関する状況を Group A 人材や Group B 人材に正確に伝えることができること。
- ・Group A 人材や Group B 人材の指示を受けて、必要な実務作業ができること。
- ・Group A 人材や Group B 人材からの指示内容を正確に経営層に伝達できること。
- ・仕様書やチェックリストを参照し、正確に実行できること。

※Group A 人材、Group B 人材、Group C 人材については、より分かりやすい表現に変える必要があり、今後、研究班で議論を重ねていく。

それぞれの人材が持つべき知識、備えるべきスキルについては、鳥飼、谷川によ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、実行レベル等の検討に従い、Cybersecurity Framework (CSF) 視点(攻撃者視点对策能力)、Continuous Diagnostics and Mitigation (CDM)視点(防衛者視点对策能力)、Security-by-Design (設計者視点)、Incident-Response-Recovery (緊急対応能力)、保守業務ならびに計画(運用維持能力)の観点による整理に従う形になる。

Group C 人材が学習や経験、資格試験を受けることで Group B 人材に、Group B 人材が学習や経験、資格試験を受けることで Group A 人材を目指すことが可能とすることで、人材育成が進んでいくことを期待する。

情報セキュリティに関する能力獲得には学習時間を要する。情報セキュリティに関する知識は日々更新されるため、能力獲得後も継続的な学習が必要となる。情報セキュリティに関する資格、試験取得を目指す場合、学習時間と受験費用等が必要となる。資格、試験の維持には、継続的な学習や維持費用が必要になる。臨床工学技士は「ICT 分野の国家資格等取得における奨励金制度」を設けているが、自費での資格取得、資格維持は少なくない。

情報セキュリティに関する学習や資格、試験の取得や維持、さらに上の学習や資格、試験の取得が進む事は、日本の情報セキュリティ対策の向上につながる。各医療機関に配置する情報セキュリティ人材がさらに上を目指そうとする仕掛けが必要と考える。

### 【医療機関の組織体制】

医療情報システムは、電子カルテシステム等いわゆる基幹システムだけではなく、連携する様々な部門システム、医療機器等で構成されており、ネットワークで接続されている。医療機器や部門システムは、基幹システム管理者とは別部門で管理されている医療機関も存在しており、それぞれの部門においても情報セキュリティの重要性について認識し、基幹システム管理者と連携をとる必要がある。医療機関の経営者等においては、各部門が円滑な連携をとれる体制を整備することが重要である。

情報セキュリティ人材は診療情報を電子的に取り扱う全ての医療機関に置くべきであるが、ス

キルの高い情報セキュリティ人材の確保は容易でない。そこで、医療機関を「指導的な立場の医療機関」、「自院の情報システムを守ることができる医療機関」、「他施設や企業の助けを借りて情報システムを守る医療機関」に分け、各医療機関が協働して、情報セキュリティ対策に臨む態勢を構築するべきであると考えた。

### 指導的な立場の医療機関

- ・統括情報セキュリティ責任者あるいは統括情報セキュリティ補助者が Group A 人材の資格を有すること。
- ・Group A 人材を中心に、他施設の情報セキュリティの問い合わせに体制して、適切なアドバイスや指導を行うことができること。
- ・情報システムを管理する中央診療部門には、可能な限り Group C 人材を配置すること。

### 自院の情報システムを守ることができる医療機関

- ・統括情報セキュリティ責任者あるいは統括情報セキュリティ補助者が Group B 人材の資格を有すること。
- ・情報システムを管理する中央診療部門には、可能な限り Group C 人材を配置すること。

### 他施設や事業者の助けを借りて情報システムを守る医療機関

- ・Group C 人材を配置すること

組織体制については、自施設の情報システムを守る体制を強化することは医療機関のメリットにつながるが、指導的な立場の医療機関になることは、医療機関自体へのメリットは少ない。情報セキュリティに関してより高いスキルを持つ人材を確保することは医療機関にとって容易で

なく、確保後は人件費が必要となる。

令和5年度賃金構造基本統計調査(表1)では、システムコンサルタント・設計者、ソフトウェア作成者、その他の情報処理・通信技術者の給与は医師、歯科医師を除いた医療系専門職よりも高い給与であり、医療機関側の人材確保の困難につながっていると、第44回医療情報学連合大会のシンポジウムで指摘があった。

医療機関がより高いスキルを持つ人材を雇用すること、指導的な立場の医療機関となることには、何らかの仕組みが必要であると考えられた。

表1. 令和5年賃金構造基本統計調査、職種(小分類)、性別きまって支給する現金給与額、所定内給与額及び年間賞与その他特別給与額(産業計)

	年齢	勤続年数	現金給与×12+特別給与(千円)
企業規模計(10人以上)			
システムコンサルタント・設計者	41.8	12.5	6,849.1
ソフトウェア作成者	38.6	10.7	5,575.8
その他の情報処理・通信技術者	40	11.3	5,582.5
医師	46.1	8.4	14,364.7
歯科医師	42.5	8.3	9,243
薬剤師	40.3	7.9	5,778.7
看護師	41.9	9.8	5,081.7
診療放射線技師	41.1	13.4	5,369.7
その他の保健医療従事者	40.1	9.7	4,592.6
企業規模計(1,000人以上)			

システムコンサルタント・設計者	39.7	14.4	7,480.3
ソフトウェア作成者	38.1	11.9	5,984.2
その他の情報処理・通信技術者	38.6	10.8	5,950.6
医師	42.5	7.2	13,259.7
歯科医師	39.2	5.7	9,401.1
薬剤師	36.9	7.6	5,699.6
看護師	37.7	10.2	5,571.2
診療放射線技師	39.5	14	5,718.4
臨床検査技師	39.6	12	5,557
その他の保健医療従事者	40.6	10.2	5,070.5

### 【教育体制】

#### 情報セキュリティ人材教育を行う医療機関

- ・Group A 人材を配置していること。
- ・OJT (On the Job Training) をできる教育環境を有していること。

情報セキュリティ人材の教育には、講習会や e-learning 等での座学に加えて、医療機関での OJT が必要であるとの議論があった。情報セキュリティ人材教育を行う医療機関は、前項の指導的な立場の医療機関と一致する可能性が高いが、全ての指導的な医療機関が OJT を提供できるわけではないため、教育体制は切り分けて整理を行った。人材教育を行う医療機関については、自施設にとっては負担になることはあっても、メリットとなることは少ない。このため、人材教育を行うことのメリットを明示する必要があると考えられた。

人材教育については本研究班で十分な議論ができておらず、令和 6 年度の課題とした。

#### D. 考察

### 1. 医療機関が配置すべき情報セキュリティ人材が保有すべき試験、資格等

医療機関における情報セキュリティを担当するには、一般的な情報セキュリティの知識に加え、医療情報システムの特性を理解する必要がある。医療情報システムは、電子カルテシステム等いわゆる基幹システム、基幹システムと連携する様々な部門システム、基幹システムと連携あるいは独立して設置される医療機器等で構成される。これらのシステム、機器は、事業者によるリモートメンテナンス、医療 DX 等による外部サービスとの接続が求められる。一方、医療情報システム、医療機器は薬事承認やその他の理由により OS のアップデートができないことが少なくない。また、医療機関の経済的な理由により、保守期限の過ぎた OS で稼働するシステム、機器の利用の継続が必要となるケースが少なくない。このように特殊な環境におかれる医療情報システムを情報セキュリティから守るには、情報セキュリティのより深い知識が必要となる。

最初に、一般的な情報セキュリティの知識や能力を評価することを考え、情報処理推進機構 (IPA) が定める資格、試験について着目をした。IPA では、各種 IT 関連サービスの提供に必要とされる能力を明確化・体系化した指標として IT スキル標準を定めている。IT スキル標準はレベル 1 からレベル 7 が定められている。レベル 1 は、「情報技術に携わる者に最低限必要な基礎知識を有する。スキル開発においては、自らのキャリアパス実現に向けて積極的なスキルの研鑽が求められる。」、レベル 2 は、「上位者の指導の下に、要求された作業を担当する。プロフェッショナルとなるために必要な基本的知識・技能を有する。スキル開発においては、自らのキャリアパス実現に向けて積極的なスキルの研

鑽が求められる。」、レベル3は「要求された作業を全て独力で遂行する。スキルの専門分野確立を目指し、プロフェッショナルとなるために必要な応用的知識・技能を有する。スキル開発においても自らのスキルの研鑽を継続することが求められる。」、レベル4は「プロフェッショナルとしてスキルの専門分野が確立し、自らのスキルを活用することによって、独力で業務上の課題の発見と解決をリードするレベル。社内において、プロフェッショナルとして求められる経験の知識化とその応用(後進育成)に貢献しており、ハイレベルのプレーヤとして認められる。スキル開発においても自らのスキルの研鑽を継続することが求められる。」、レベル5は「プロフェッショナルとしてスキルの専門分野が確立し、社内においてテクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。社内において、プロフェッショナルとして自他共に経験と実績を有しており、企業内のハイエンドプレーヤとして認められる。」、レベル6は「プロフェッショナルとしてスキルの専門分野が確立し、社内外において、テクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。社内だけでなく市場においても、プロフェッショナルとして経験と実績を有しており、国内のハイエンドプレーヤとして認められる。」、レベル7は、「プロフェッショナルとしてスキルの専門分野が確立し、社内外において、テクノロジーやメソドロジ、ビジネスを創造し、リードするレベル。市場全体から見ても、先進的なサービスの開拓や市場化をリードした経験と実績を有しており、世界で通用するプレーヤとして認められる。」となっている。医療機関においては、Group A 人材は IT スキル標準レベル 4、Group B 人材はレベル 3、Group C 人材はレベル 2 に相当すると考えられた。情報セキュリティに関する資格、試験に当てはめると、Group A

人材は情報処理安全確保支援士、Group C 人材は情報セキュリティマネジメント試験が対応する。IT スキル標準レベル 3 は情報セキュリティに限定する試験ではないが応用情報技術者試験が対応すると考えた。

医療機関における情報セキュリティを担当する候補となる医療系専門職については、本研究班での教育カリキュラムの調査の結果、医療情報技師が最も教育カリキュラムが整備されていた。診療放射線技師は医用画像情報専門技師、臨床工学技士は ICT 分野の国家資格等取得における奨励金制度、診療情報管理士はその職域から医療情報技師や IPA の資格の保有率が高いことから、資格取得後の専門教育として、医療情報技師の取得を求めることは適切であると考えられた。

医療情報技師は試験で一定の基準をクリアすることで取得できる資格である。上級医療情報技師は、一定期間の実務経験と試験への合格が必要となる。医療情報技師や上級医療情報技師は情報セキュリティの教育コンテンツが充実しているものの、特に医療情報技師は情報セキュリティ領域の学習が必須とならない(他の領域の成績が良ければ資格を取得できる)。このため、医療情報技師や上級医療情報技師間で、情報セキュリティに関する知識のばらつきは大きいことが予想される。診療情報管理士には、DPC コース、腫瘍学分類コース、医師事務作業補助者コースといった専門分野に特化したコースが作られている。医療情報技師に対して(あるいは他の医療系専門職に対しても)、情報セキュリティコースを設置することが考えられる。あるいは、IPA が提供する情報処理安全確保支援士や情報セキュリティマネジメント試験の資格、試験を取得することで、情報セキュリティに対する知識を担保することが想定された。

## 2. 厚生労働省医療情報システムの安全管理に関するガイドラインとの整合性

厚生労働省医療情報システムの安全管理に関するガイドライン第6.0版では、経営管理編、企画管理編、システム運用編に分けられ、経営管理編は医療機関等において組織の経営方針を策定し、意思決定を担う経営層、企画管理編は医療機関等において医療情報システムの安全管理(企画管理、システム運営)の実務を担う担当者(企画管理者)、は医療機関等において医療情報システムの実装・運用の実務を担う担当者を主な対象者としている。経営管理編、「3. 1. 2 医療情報システムにおける統制上の留意点」では、遵守事項に「②医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること」、「医療情報システム安全管理責任者としての職務は、経営層が担うことを想定しているが、医療機関等の規模・組織等を考慮して、企画管理者が医療情報システム安全管理責任者を兼務することは妨げられない」とされている。

本研究班で行った情報セキュリティ人材の実態調査では、医療情報システム安全管理責任者は経営層と考えられる院長、院長を補佐する立場、事務部門の長が54%(283施設)、企画管理者と考えられる医療情報システム部門の長が28%(144施設)であった。医療情報システム安全管理責任者のうち84%(440名)は、上級医療情報技師、医療情報技師、情報処理安全確保支援士、応用情報技術者試験、基礎情報技術者試験、情報セキュリティマネジメント試験いずれの資格を有さず、院長、院長を補佐する立場、事務部門の長に限定するとその割合は96%(273名)に増加した。資格、試験だ

けで情報セキュリティの知識を語ることはできないが、多くの医療情報システム安全管理責任者は情報セキュリティの知識が十分でないことが予想された。

医療情報システム安全管理責任者は自施設の情報セキュリティ対策を講じ、その対策を病院職員に周知することや、情報セキュリティ対策に必要な人材確保や設備投資を行うことが求められ、このために、経営・運営上の意思決定に関与する立場であることが理想的である。情報セキュリティ人材の実態調査では、医療情報システム安全管理責任者のうち67%(350名)が経営・運営上の意思決定に関与する立場にあったが、上級医療情報技師、医療情報技師、情報処理安全確保支援士、応用情報技術者試験、基礎情報技術者試験、情報セキュリティマネジメント試験いずれの資格を有する人材に限定すると、その割合は37%(30名)に減少した。

医療情報システム安全管理責任者が情報セキュリティに対する正しい知識を持ち、CIO: Chief Information Officer あるいは、CISO: Chief Information Security Officer として、自施設の情報セキュリティ対策を勧めることが理想的である。このために、本研究班で議論を行った情報セキュリティ人材では、Group A 人材あるいは Group B 人材の配置を目指すべきである。一方、本研究班の情報セキュリティ人材の実態調査では、情報セキュリティに関する資格、試験の保有率は低く、資格、試験を保有するものは経営、運営上の意思決定に関わる割合が低かった。このことから、現時点では、全ての医療情報システム安全管理責任者に Group A 人材あるいは Group B 人材を求めることは現実的でない。Group A 人材あるいは Group B 人材の医療情

報システム安全管理責任者を配置すること、あるいは医療情報システム安全管理責任者を補佐する Group A 人材あるいは Group B 人材を配置することを医療機関ごとに選択することが現実的と考える。将来的には、医療情報システム安全管理責任者を補佐する立場の人材が経営、運営上の意思決定を行う立場に成長し、医療情報システム安全管理責任者を務めることが期待される。

医療情報システム安全管理責任者を補佐する立場の人材を配置したからと言って、医療情報システム安全管理責任者が情報セキュリティに関する知識が不要であるわけではない。医療情報システムの安全管理に関するガイドラインの経営管理編(あるいは企画管理編)を正しく理解すること、医療情報システム安全管理責任者を補佐する人材のアドバイスを正しく理解すること、情報セキュリティに対する正しい経営、運営判断を行うためには一定の情報セキュリティの知識が必要になる。このため、どのような教育、資格、試験を求めていくかについては、令和6年度の課題としたい。

### 3. 医療機関の特性に合わせた情報セキュリティ人材の配置

医療情報システムの情報セキュリティを担保するためには病院情報システムの基幹システム、部門システム、医療機器の情報セキュリティ対策を進める必要がある。一般的に病院情報システムの調達には医療機関と導入事業者が協力しながら、情報セキュリティを考慮したシステム導入が行われることが多い。しかし、医療機関を支える部門システムの全てが病院情報システムの調達に含まれるわけではない。医療機器の調達については、病院情報システムの調達に

含まれることは稀である。病院情報システムとは別調達の部門システムや医療機器は、それぞれの部門、診療科で行われることが多く、情報セキュリティ対策が甘くなることは少なくない。情報セキュリティ対策は、システム、機器導入時だけでなく、日常診療における運用や保守作業など、導入後の運用管理が必須となり、各部門、診療科の細かい運用までを医療情報システム安全管理責任者が把握することは容易でない。このため、医療情報システム、医療機器を運用する全ての部門、診療科に情報セキュリティを理解する人材を配置することが望まれる。医療機関が配置する Group A 人材、Group B 人材の指示を受けて、適切な情報セキュリティ対策を講じることを考えると Group C 人材あるいはそれに準じる人材が想定される。

部門システムについては、診療放射線技師や臨床検査技師、診療情報管理士が、医療機器については、臨床工学技士管理に関わることが多い。情報セキュリティ対策の配置状況の調査では、医療情報システムの情報セキュリティ事案の担当者の多くは医療系専門職ではなかったが、今後は医療系専門職で部門システムの運用管理に携わる人材については、情報セキュリティに関する資格、試験の取得を促す必要がある。

部門システム、医療機器を管理する全ての部門、診療科に医療情報システムの情報セキュリティ事案の担当者を配置することは困難であると予想される。医療情報システムの安全管理責任者はこのような部門、診療科を把握し、調達から運用管理における情報セキュリティ対策を把握する必要がある。

医療情報システムは巨大なシステムで、医療情報安全管理責任者がその全てを把握すること容易でない(ウイルス対策の施されていない



ワークステーションに USB メモリを使っていたといった事例は良く聞かれる)。医療情報システム安全管理責任者の知識や技量、業務キャパシティに合わせて、医療情報システムの情報セキュリティ事案担当者を適切に配置して、医療情報システムの情報セキュリティを点ではなく、面で支えることが大切で、実現に向けた人材育成と配置が必要である。

#### 4. 情報セキュリティ人材の教育について

IPA (<https://www.ipa.go.jp/index.html>) の情報セキュリティ教材では、スライド形式で、情報セキュリティ対策(コンピュータウイルス、ネット詐欺、パスワード、外出先での利用、物理的なセキュリティ対策)、手口を知る(コンピュータウイルス、ネット詐欺)、SNS との付き合い方(交友関係、投稿内容、トラブル発生時の対処法)、情報社会の問題解決(インターネット上の情報、情報端末との向き合い方)、情報に関する法や制度(著作権、肖像権)が、動画としてインターネット安全教室が用意されていた。また、映像で知る情報セキュリティが用意されていた。初学者向けや啓発コンテンツが主で、IPA が実施する資格、試験の学習については民間で販売される教育コンテンツでの学習が求められた。

厚生労働省が設置する医療機関向けセキュリティ教育支援ポータルサイト(<https://mhlw-training.saj.or.jp/>)では、初学者・医療従事者向け研修、経営者向け研修、システム・セキュリティ管理者向け研修が実施されている。令和 5 年度は導入研修－立ち入り検査対策コース、導入研修－大阪急性期・総合医療センター事例コース、経営者向け研修、システム・セキュリティ管理者向け研修、初学者等向け研修、E-

learning が実施されているが、報告書を記載している令和 6 年 5 月現在閲覧できるコンテンツは限定されている。情報セキュリティ対策は日々アップデートされるため、教育コンテンツの最新性の確保は課題となるはずである。情報セキュリティ対策を補佐する人材を配置する経営者や医療情報システム安全管理責任者や一般職員が情報セキュリティ対策の重要性を理解する教育コンテンツとして利用できると考えられた。

内閣府サイバーセキュリティセンター(<https://www.nisc.go.jp/pr/index.html>)では、普及啓発活動として、みんなで使おうサイバーセキュリティポータルサイト、インターネットの安全・安心ハンドブックが用意されていた。みんなで使おうサイバーセキュリティポータルサイトでは、目的や所属・役割から選ぶ施策一覧として、自宅でインターネットを利用する方向け(子ども層、中間層、シニア層)、オフィス等でシステムを利用する人向け(一般社員、管理職、経営層)、セキュリティに関する教育・普及啓発をする人向け(子ども層、中間層、シニア層)、セキュリティのプロフェッショナル向け、相談窓口を利用する人向けに施策がまとめられていた。安全・安心ハンドブックでは、「プロローグ：インターネットにある基本的なリスクやトラブルを知ろう」、「第 1 章：まずはサイバーセキュリティの基礎を固めよう」、「第 2 章：よくあるサイバー攻撃の手口やリスクを知ろう」、「第 3 章：SNS・ネットとの付き合い方や情報モラルの重要性を知ろう」、「第 4 章：災害・テロ、海外でのトラブル、普段とは違う環境のリスクに備えよう」、「第 5 章：スマホやパソコン、IoT 機器を安全に利用するための設定を知ろう」、「第 6 章：パスワードの大切さを知り、通信の安全性を支える暗

号化について学ぼう」、「第7章：【中小組織向け】セキュリティ向上が利潤追求につながることを理解しよう」、「付録：知っておくと役立つサイバーセキュリティに関する手引き・ガイドンス」、「おわりに：インターネットとよい付き合いを続けるために」、「用語集」、「索引」が用意されていた。

民間では多くは一般向けの教育コンテンツを作成していた。医療機関向けの情報セキュリティ教育コンテンツを作る民間企業も認められたが、初学者や一般職員向けのコンテンツが主であった。

医療機関の情報セキュリティ人材の育成や育成した情報セキュリティ人材の知識更新に向けては、適切な教育コンテンツの整備や医療機関での実地学習、サイバーインシデント訓練が必要と思われる。これらについては、令和6年度に検討を進めていくこととする。

## 5. 情報セキュリティ人材の配置状況の改善に向けて

医療機関が情報セキュリティ対策を進めるには、医療機関の特性に合わせて情報セキュリティ人材の配置が必要である。情報セキュリティ人材の配置状況の調査では、8%の医療機関は医療情報システム安全管理責任者、医療情報システムの情報セキュリティ事案の担当者のいずれも配置していなかった(400床以上の医療機関では1施設のみ)、一方、72%の医療機関(400床以上の医療機関では33%)は、情報セキュリティに関する資格、試験(上級医療情報技師、医療情報技師、情報処理安全確保支援士、応用情報技術者試験、基礎情報技術者試験、情報セキュリティマネジメント試験)を保有する人材を1名も配置していなかった。資格、

試験だけで情報セキュリティの知識をはかることはできないが、この割合を上げていくことが、日本の医療機関の情報セキュリティ対策能力を担保することにつながることは間違いない。

本研究班を設置し、様々な学会のシンポジウム等で日本の医療機関の情報セキュリティ対策の議論を行う中で、情報セキュリティ人材を確保するための費用、情報セキュリティに関する資格試験を取得するための費用、維持するための費用に関する意見が多く寄せられた。厚生労働省が実施する賃金構造基本統計調査によれば、システムコンサルタント・設計者、ソフトウェア作成者、その他の情報処理・通信技術者は、医師、歯科医師を除く医療系専門職やその他の保健医療従事者と比べ給与が高い。医療機関の情報セキュリティ担当者が、他領域の情報セキュリティ担当者と同等の給与が支払われることになれば、これらの資格、試験の取得は大きく進むことが期待される。一方、医療機関の経営者の立場では情報セキュリティ人材の人件費増加に対する収入が必要となる。令和6年度の診療報酬改定では、医療DX推進体制整備加算が設置されるなど、国としての対策も進むが、医療DXの推進には設備への投資と人材への投資が必要となる。現時点では情報セキュリティ人材への投資の根拠となる診療報酬は十分でなく、今後の議論が期待される。

## E. 結論

「人材」、「組織体制」、「教育体制」の観点から、保健医療福祉分野の特性を理解した情報セキュリティ人材の検討を実施した。実態調査情報セキュリティを担当する人材配置が進むものの、情報セキュリティに関する知識が十分でない人材が一定数いることが予想された。

情報セキュリティ人材の育成とキャリア形成、

適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等に向けて、令和6年度さらに議論を深めていく。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

(1) 武田 理宏、サイバーインシデント対策と医療安全、医療安全推進ジャーナル 73, 10-15, 2023

(2) 川真田 実、医療機器サイバーセキュリティに備える ～海外における現状と課題～、日本診療放射線技師会誌 2023 年 70 巻 846 号 p.399-405

### 2. 学会発表

(1) 肥田泰幸、サイバーセキュリティの現状と対策、第 68 回日本透析医学会学術総会、2023 年 6 月、横浜

(2) 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

(3) 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、沖縄（座長：武田 理宏、下村 剛）

① 須藤 泰史（つるぎ町立半田病院）

② 鳥飼 幸太

(4) 川真田 実、ランサムウェア被害に遭うということ、日本放射線技術学会 九州支部講演会、2023 年 9 月、福岡

(5) 武田 理宏、医療機関に求められる医療情報人材とは、日本医療情報学会関西支部会、2023 年度第 1 回講演会、2023 年 10 月、大阪

(4) 医療分野のセキュリティ人材の育成をどうするか、第 43 回医療情報学連合大会シンポジウム、2023 年 11 月、神戸、（座長：武田 理宏、谷川 琢海）

① 武田 理宏、医療機関における情報セキュリティ人材の育成と配置に向けて

② 岡本 潤（厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室）、厚生労働省における医療機関の情報セキュリティの強化に向けた取り組み

③ 大道 道大（大道会 森之宮病院）、病院の ICT の変遷と医療情報システムの人材確保について

④ 奥村 明俊（情報処理推進機構（IPA））サイバーセキュリティ人材育成に関する IPA の取り組み

⑤ 谷川 琢海、診療業務を理解したセキュリティ人材の育成に向けて

(6) みんなでつくるセキュリティの医療現場改革に向けて 情報共有体制の重要性、第 43 回医療情報学連合大会産学官連携企画、2023 年 11 月、神戸、（座長：武田 理宏、並川 寛和

（保健医療福祉情報システム工業会（JAHIS））

① 新畑 覚也（厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室）、医療分野におけるサイバーセキュリティ対策の厚生労働省の取組について

② 谷川 琢海、医療情報技師の観点からの医療分野の ISAC の必要性

③ 大谷 俊介（誠馨会 千葉中央メディカルセンター）、医療分野における医療機関関係者・医療従事者を中心とした ISAC 設立に向けた検討

④ 洞田 慎一（JPCERT コーディネーションセンター）、ISAC 等で使用するサイバーセキュリティに関連する情報共有ツール SIGNAL に関して

(7) IT-BCP をどう実現するか、第 43 回医療情報学連合大会共同企画（医療情報マネジメント部門連絡会議）、2023 年 11 月、

神戸、(座長:鳥飼 幸太、平田 哲生 (琉球大学病院)

①栗倉 康之 (大阪府立病院機構大阪急性期・総合医療センター)、まさかの大規模システム障害に備えるべきことーサイバー攻撃を受けた医療機関からの IT-BCP 策定に向けた提言ー

②脇元 直彦 (徳島大学病院)、サイバー攻撃を受けた際の利益損失と IT-BCP の策定について

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

(8) 医用画像部門におけるセキュリティ対策. 坂本博, 木村通男, 原瀬正敏, 谷祐児, 坂野隆明, 川真田実 第 43 回医療情報学連合大会共同企画 5, 2023 年 11 月. 神戸

#### H. 知的財産権の出願・登録状況

(予定を含む。)

##### 1. 特許取得

なし

##### 2. 実用新案登録

なし

##### 3. その他

なし

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

テーマ:情報セキュリティ人材配置に関するアンケート調査

研究代表者 武田理宏 国立大学法人大阪大学大学院医学系研究科 医療情報学 教授  
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  
研究分担者 川真田 実 大阪府立病院機構国際がんセンター 放射線診断・IVR科 副技師長  
研究分担者 肥田 泰幸 東都大学 幕張ヒューマンケア学部臨床工学科 助教

研究要旨

本研究では、各医療機関の情報セキュリティ人材の配置状況や、情報セキュリティ人材が保有する資格、試験、情報セキュリティ人材の雇用環境などの現状を把握することを目的としたアンケート調査を実施した。アンケート調査は Microsoft Form を用いた Web 調査とし、医療機関の各団体に調査協力依頼を行った。回答は任意で、医療機関を特定する情報は収集していない。643 の医療機関から回答を得た。医療情報システム安全管理責任者は 81%の医療機関で配置されていた。医療情報システム安全管理責任者は院長や院長を補佐する立場、事務部門の長などが多く、情報セキュリティに関する資格・試験を保有する割合は低かった。医療情報システムの情報セキュリティ事案の担当者を少なくとも 1 名は配置する医療機関は 78%であった。医療情報システムの情報セキュリティ事案の担当者が情報セキュリティに関する資格・試験を保有する割合は、医療情報システム安全管理責任者よりは高いものの、半数以上は資格を有していなかった。自施設の情報セキュリティ人材の配置状況について、不十分であると回答した施設が 8 割を超え、引き続き情報セキュリティ体制の整備が必要と考えられた。

A. 研究目的

安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究では、安全・安心な地域医療を継続的に維持確保するために必要な保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とし、関係する省庁・学会・業界団体等と連携しながら調査・試作・検証・評価等を行うことをも目的としている。

本研究では、各医療機関の情報セキュリティ人材の配置状況や、情報セキュリティ人材が保有する資格、試験、情報セキュリティ人材の雇

用環境などの現状を把握することを目的としたアンケート調査を実施することを目的とする。

B. 研究方法

Microsoft office 365 の Form を用いて Web アンケート調査を行った。

全国自治体病院協議会、日本医療法人協会、日本医療法人協会、日本精神科病院協会、日本病院会、日本慢性期医療協会、国立病院機構、労働者健康安全機構、日本社会医療法人協会、地域医療機能推進機構、日本リハビリテーション病院・施設協会、地域包括ケア病棟協会、地域包括ケア病棟協会、日本リハビリテーション病院・施設協会、国立大学病院医療情報部長会、公立大学病院医療情報協議会、日

本私立医科大学協会の事務局に調査の趣旨を伝え、各施設にメールリスト等を用いて調査協力をして下さるよう依頼を行った。回答は任意とした。情報セキュリティ対策が不十分な施設にも回答いただけるように、施設を特定できる情報は収集しなかった。

質問は 10 個のセクションで構成され、セクション 1 では貴施設について(6 問)、セクション 2 では医療情報システム安全管理責任者の配置状況と保有する資格(最大 9 問)の質問を行った。次に、情報セキュリティ事案対応について、医療情報システム安全管理責任者を配置しない医療機関(セクション 3、最大 4 問)と医療情報システム安全管理責任者を配置する医療機関(セクション 4、最大 4 問)へ質問を行った。次に、情報セキュリティ担当者の配置状況と保有する資格について、1 人目(セクション 5、7 問)、2 人目(セクション 6、7 問)、3 人目(セクション 7、7 問)、4 人目以降(セクション 8、1 問)の質問を行った。最後に、貴施設の情報セキュリティ人材の配置状況について(セクション 9、最大 4 問)、アンケート調査回答者について(セクション 10、1 問)について質問を行った。具体的な質問内容を添付資料\_調査依頼と質問項目一覧に示す。

## C. 研究結果

### 1. 回答医療機関

回答があった医療機関数は 643 施設で、国公立大学病院が 40 施設、公的な医療機関が 344 施設、私立大学病院が 32 施設、私立の医療機関が 227 施設であった。公的な医療機関とは、医療法第 31 条に規定される、都道府県、市町村、地方公共団体の組合、国民健康保険団体連合会及び国民健康保険組合、日本赤十字社、社会福祉法人恩賜財団済生会、厚生

農業協同組合連合会、社会福祉法人北海道社会事業協会掲げる者が開設する医療機関とし、国立病院機構や労働者健康安全機構は公的な医療機関として回答を依頼した。

回答医療機関の内、特定機能病院は 68 施設、地域医療支援病院は 218 施設、災害拠点病院(基幹)は 211 施設、災害拠点病院(地域)は 126 施設、第三次救急医療機関は 126 施設、第二次救急医療機関は 382 施設、総合周産期母子医療センターは 61 施設、地域周産期母子医療センターは 95 施設、小児中核病院は 21 施設、小児地域医療センターは 15 施設、小児地域支援病院は 2 施設、これらの認定、指定は受けていない施設は 128 施設であった。病床数は 1000 床以上が 14 施設、800 床以上 1000 床未満が 31 施設、600 床以上 800 床未満が 61 施設、400 床以上 600 床未満が 129 施設、300 床以上 400 床未満が 94 施設、200 床以上 300 床未満が 85 施設、100 床以上 200 床未満が 144 施設、100 床未満が 85 施設であった。

アンケート回答者は、医療情報システム安全管理責任者が 131 名、情報セキュリティ担当者が 269 名、医療機関の経営・運営上の意思決定に関与する立場の医療職が 8 名、医療機関の経営・運営上の意思決定に関与する立場の事務職が 56 名、その他の医療職が 5 名、その他の事務職が 167 名、その他が 7 名であった。

### 2. 医療情報システム安全管理責任者の配置

医療情報システム安全管理責任者を配置する医療機関は 521 施設(81%)であった(表1)。病床数で見ると 400 床以上の医療機関は 224 施設(95%)に配置が行われていた。国公立大学病院では 38 施設(95%)、公的な医療機関では 276 施設(80%)、私立大学病院では 30 施設(94%)、私立の医療機関では 177 施設(78%)

であった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関は 515 施設で、425 施設(83%)が医療情報システム安全管理責任者を配置していた(表2)。

表1. 医療情報システム安全管理責任者を配置する医療機関(病床数)の数と割合

病床数	配置あり		配置なし
～99床	49	58%	36
100床～199床	106	74%	38
200床～299床	71	84%	14
300床～399床	71	76%	23
400床～599床	120	93%	9
600床～799床	60	98%	1
800床～999床	30	97%	1
1000床～	14	100%	0
合計	521	81%	122

表2. 医療情報システム安全管理責任者を配置する医療機関(機能別)の数と割合

	配置あり		配置なし
特定機能病院	64	94%	4
地域医療支援病院	196	90%	22
災害拠点病院(基幹)	49	96%	2
災害拠点病院(地域)	181	86%	30
第三次救急医療機関	123	98%	3
第二次救急医療機関	298	78%	84

総合周産期母子医療センター	60	98%	1
地域周産期母子医療センター	90	95%	5
小児中核病院	21	100%	0
小児地域医療センター	15	100%	0
小児地域支援病院	2	100%	0
合計	425	83%	90

### (1) 医療情報システム安全管理責任者を配置しない医療機関(122 施設)

医療情報システム安全管理責任者を配置しない 122 施設について今後の配置予定を聞いたところ、予定あり(既存人材の活用)が 61 施設(400 床以上は 7 施設)、予定あり(新規雇用)が 5 施設(400 床以上は 0 施設)、予定なしが 56 施設(400 床以上は 4 施設)であった。また、医療情報システムの情報セキュリティ事案の担当者の配置の有無を確認したところ、配置ありと回答したのが 71 施設(400 床以上は 10 施設)で配置人数は 5 人以上が 4 施設、4 人が 3 施設、3 人が 11 施設、2 人が 21 施設、1 人が 32 施設であった。配置なしと回答した 51 施設のうち、今後の配置予定ありが 28 施設、配置予定なしが 23 施設(400 床以上は配置予定なし:1 施設)であった。情報セキュリティ事案の担当者の配置がない施設での情報セキュリティ事案への対応については、同一組織別施設の情報セキュリティ担当者として協力して対応が 10 施設、外部委託契約あるいは保守契約が 20 施設、十分な対応はとれていないが 18 施設であった。

### (2) 医療情報システム安全管理責任者を配置する医療機関(521 施設)

医療情報システム安全管理責任者の職位は、院長が 127 施設(24.4%)、院長を補佐する立

場(副院長、院長補佐など)が 83 施設(15.9%)、医療情報システム管理部門の長が 144 施設(27.6%)、事務部門の長が 73 施設(14.0%)、上記以外の部門の長が 31 施設(6.0%)、その他が 63 施設(12.1%)であった。

医療情報システム安全管理責任者が経営・運営上の意思決定に関与する立場にあるかについては、ありが 350 名(67.2%)、なしが 171 名であった。

医療情報システム安全管理責任者が保有する医療系国家資格は、医師・歯科医師が 267 名、看護師・助産師・保健師が 2 名、薬剤師が 5 名、診療放射線技師が 8 名、臨床検査技師が 5 名、臨床工学技士が 5 名、その他が 8 名であり、医療系国家資格を保持していないのは 231 名であった。

医療情報システム安全管理責任者が上級医療情報技師、医療情報技師、診療情報管理士など学会・団体等が認定する資格・試験を保有するかについては、資格を保持していないが 432 名(83%)であった。資格を保有するのは、上級医療情報技師が 12 名、医療情報技師が 61 名、診療情報管理士が 30 名、その他が 8 名であった。

医療情報システム安全管理責任者が、情報処理推進機構(IPA)が認定する資格・試験を保有するかについては、資格・試験を保持していないが 451 名(87%)であった。資格を保持しているのは、情報処理安全確保支援士が 4 名、応用情報技術者試験が 10 名、基礎情報技術者試験が 23 名、情報セキュリティマネジメント試験が 12 名、IT パスポート試験が 17 名、その他が 33 名であった。

医療情報システム安全管理責任者の勤務形態は、常勤(雇用期限なし)が 482 名、常勤(雇用期限あり)が 64 名、非常勤が 5 名であった。

また、専従(就業時間の少なくとも 5 割以上、当該業務に従事しているもの)が 73 名、専任(就業時間の少なくとも 8 割以上、当該業務に従事しているもの)が 64 名、兼任が 384 名であった。

医療情報システムの情報セキュリティ事案を担当する部署については、ありが 454 施設、なしが 67 施設(設置予定あり:21 施設、設置予定なし:46 施設)であった。医療情報システムの情報セキュリティ事案の担当者の配置については、配置ありが 428 施設(400 床以上:190 施設)で配置人数は 1 人が 124 施設、2 人が 117 施設、3 人が 106 施設、4 人が 26 施設、5 人が 17 施設、6 人が 10 施設、7 人が 12 施設、8 人以上が 14 施設であった。配置なしは 93 施設(400 床以上:34 施設)で今後、配置予定ありが 27 施設(400 床以上:10 施設)、配置予定なしが 66 施設(400 床以上:24 施設)であった。

情報セキュリティ事案の担当者の配置がない施設での情報セキュリティ事案への対応については、医療情報システム安全管理責任者が全て対応が 33 施設、同一組織別施設の情報セキュリティ担当者と協力して対応が 13 施設、外部委託契約あるいは保守契約が 24 施設、十分な対応はとれていないが 17 施設、その他が 6 施設であった。

### 3. 医療情報システムの情報セキュリティ事案の担当者について

医療情報システムの情報セキュリティ事案の担当者を少なくとも 1 名は配置する医療機関は 499 施設(78%)であった(表 3)。病床数で見ると 400 床以上の医療機関は 200 施設(85%)に配置が行われていた。国公立大学病院では 32 施設(80%)、公的な医療機関では 294 施設(86%)、私立大学病院では 28 施設(88%)、私立の医療機関では 145 施設(64%)であった。



特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関 515 施設で、415 施設(81%)が医療情報システムの情報セキュリティ事案の担当者を配置していた(表 4)。

表3. 医療情報システムの情報セキュリティ事案の担当者を配置する医療機関(病床数)の数と割合

病床数	配置あり		配置なし
～99 床	41	48%	44
100 床～199 床	102	71%	42
200 床～299 床	73	86%	12
300 床～399 床	83	88%	11
400 床～599 床	109	84%	20
600 床～799 床	53	87%	8
800 床～999 床	26	84%	5
1000 床～	12	86%	2
合計	499	78%	144

表4. 医療情報システムの情報セキュリティ事案の担当者を配置する医療機関(機能別)の数と割合

	配置あり		配置なし
特定機能病院	53	78%	15
地域医療支援病院	192	88%	26
災害拠点病院 (基幹)	45	88%	6
災害拠点病院 (地域)	191	91%	20
第三次救急医療機関	111	88%	15

第二次救急医療機関	300	79%	82
総合周産期母子医療 センター	52	85%	9
地域周産期母子医療 センター	83	87%	12
小児中核病院	16	76%	5
小児地域医療 センター	15	100%	0
小児地域支援病院	2	100%	0
合計	415	81%	90

医療情報システムの情報セキュリティ事案の担当者について、各施設最大 3 名まで詳細情報を聞き取った。

#### (1) 1 人目として登録された医療情報システムの情報セキュリティ事案の担当者(499 人)

所属する部門は、医療情報システム管理部門が 257 名、診療情報管理部門が 22 名、事務部門が 205 名、その他が 15 名であった。保有する医療系国家資格は、医師・歯科医師が 21 名、看護師・助産師・保健師が 6 名、薬剤師が 4 名、診療放射線技師が 9 名、臨床検査技師が 7 名、臨床工学技士が 2 名、その他が 11 名で、医療系国家資格を保持していない方が 441 名であった。

上級医療情報技師、医療情報技師、診療情報管理士など学会・団体等が認定する資格・試験については、上級医療情報技師が 18 名、医療情報技師が 118 名、診療情報管理士が 76 名、その他が 9 名で、310 名(62%)はこれらの資格を保持していなかった。

情報処理推進機構(IPA)が認定する資格・試験については、情報処理安全確保支援士が 12 名、応用情報技術者試験が 26 名、基礎情報技術者試験が 56 名、情報セキュリティマネジ

メント試験が 22 名、IT パスポート試験が 30 名、  
 その他が 32 名で、369 名(74%)は IPA が認定  
 する資格・試験を保持していなかった。

医療情報システムの情報セキュリティ事案の  
 担当者の勤務形態は、常勤(雇用期限なし)が  
 455 名、常勤(雇用期限あり)が 32 名、非常勤  
 が 12 名であった。また、専従(就業時間の少な  
 くとも 5 割以上、当該業務に従事しているもの)  
 が 141 名、専任(就業時間の少なくとも 8 割以  
 上、当該業務に従事しているもの)が 83 名、兼  
 任が 275 名であった。

### (2) 3 人目までに登録された医療情報システム の情報セキュリティ事案の担当者(922 人)

医療情報システムの情報セキュリティ事案の  
 担当者を 1 人登録したのが 220 施設、2 人登録  
 したのが 135 施設、3 人登録したのが 144 施設  
 であった。

所属する部門は、医療情報システム管理部  
 門が 491 名、診療情報管理部門が 37 名、事務  
 部門が 363 名、その他が 31 名であった。保有  
 する医療系国家資格は、医師・歯科医師が 23  
 名、看護師・助産師・保健師が 15 名、薬剤師が  
 5 名、診療放射線技師が 13 名、臨床検査技師  
 が 9 名、臨床工学技士が 3 名、その他が 18 名  
 で、医療系国家資格を保持していない方が 838  
 名であった。

上級医療情報技師、医療情報技師、診療情  
 報管理士など学会・団体等が認定する資格・試  
 験については、上級医療情報技師が 28 名、医  
 療情報技師が 232 名、診療情報管理士が 119  
 名、その他が 16 名で、585 名(63%)はこれらの  
 資格を保持していなかった。

情報処理推進機構(IPA)が認定する資格・  
 試験については、情報処理安全確保支援士が  
 15 名、応用情報技術者試験が 47 名、基礎情

報技術者試験が 124 名、情報セキュリティマネ  
 ジメント試験が 48 名、IT パスポート試験が 62  
 名、その他が 64 名で、651 名(71%)は IPA が  
 認定する資格・試験を保持していなかった。

医療情報システムの情報セキュリティ事案の  
 担当者の勤務形態は、常勤(雇用期限なし)が  
 810 名、常勤(雇用期限あり)が 71 名、非常勤  
 が 41 名であった。また、専従(就業時間の少な  
 くとも 5 割以上、当該業務に従事しているもの)  
 が 270 名、専任(就業時間の少なくとも 8 割以  
 上、当該業務に従事しているもの)が 149 名、  
 兼任が 498 名であった。

## 4. 情報セキュリティの人材の配置

情報セキュリティに関する資格・試験を保有  
 している医療情報システム安全管理責任者ま  
 たは医療情報システムの情報セキュリティ事案  
 の担当者の人数、配置される施設数とその割  
 合を表 5 に示す。

表5. 情報セキュリティ人材の配置状況

	延べ 人数	配置 施設	割合
上級医療情報技師	40	36	6%
医療情報技師	329	219	34%
診療情報管理士	149	129	20%
情報処理安全確保支 援士	16	16	2%
応用情報技術者試験	36	33	6%
基礎情報技術者試験	102	98	15%
情報セキュリティマネ ジメント試験	34	31	5%
IT パスポート試験	48	46	7%

### (1) 上級医療情報技師

上級医療情報技師は、延べ 40 名、36 施設

(6%)に配置されていた(表6)。国公立大学病院が8施設(20%)、公的な医療機関が16施設(5%)、私立大学病院が6施設(19%)、私立の医療機関が6施設(3%)で大学病院に配置が多い傾向があった。病床数別では、600床以上の医療機関に多い傾向があった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関515施設で、34施設(7%)が上級医療情報技師を配置していた(表7)。特定機能病院、災害拠点病院(基幹)、第三次救急医療機関、総合周産期母子医療センター、小児中核病院などが高い配置割合を示した。

上級医療情報技師は、医師・歯科医師、薬剤師、臨床検査技師の国家資格保有者が資格取得していた(表8)。

表6. 上級医療情報技師を配置する医療機関(病床別)の施設数と割合

病床数	施設数	割合
～99床	0	0%
100床～199床	2	1%
200床～299床	2	2%
300床～399床	7	7%
400床～599床	2	2%
600床～799床	12	20%
800床～999床	7	23%
1000床～	4	29%

表7. 上級医療情報技師を配置する医療機関(機能別)の施設数と割合

	施設数	割合

特定機能病院	13	19%
地域医療支援病院	20	9%
災害拠点病院(基幹)	9	18%
災害拠点病院(地域)	15	7%
第三次救急医療機関	19	15%
第二次救急医療機関	16	4%
総合周産期母子医療センター	11	18%
地域周産期母子医療センター	12	13%
小児中核病院	6	29%
小児地域医療センター	1	7%
小児地域支援病院	1	50%
合計	34	7%

表8. 国家資格ごとの上級医療情報技師保有数と割合

	人数	割合
医師・歯科医師;	7	2%
看護師・助産師・保健師;	0	0%
薬剤師;	1	10%
診療放射線技師;	0	0%
臨床検査技師;	4	27%
臨床工学技士;	0	0%
その他	0	0%
国家系医療資格なし	28	3%

## (2) 医療情報技師(上級医療情報技師を含む)

医療情報技師(上級医療情報技師を含む)は、延べ329名、219施設(34%)に配置されていた(表9)。国公立大学病院が20施設(50%)、公的な医療機関が119施設(35%)、私立大学病院が17施設(53%)、私立の医療機関が63施設(28%)で大学病院に配置が多い傾向があった。病床数別では、病床数が多い医療機関が、配置割合が多い傾向があった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関 515 施設で、195 施設(38%)が医療情報技師を配置していた(表10)。第二次救急医療機関の配置割合が低い傾向を示した。

医療情報技師の資格を有する国家資格は表11に示す通りであった。

表9. 医療情報技師を配置する医療機関(病床別)の施設数と割合

病床数	施設数	割合
～99 床	8	9%
100 床～199 床	37	26%
200 床～299 床	23	27%
300 床～399 床	39	41%
400 床～599 床	54	42%
600 床～799 床	30	49%
800 床～999 床	19	61%
1000 床～	9	64%

表10. 医療情報技師を配置する医療機関(機能別)の施設数と割合

	施設数	割合
特定機能病院	35	51%
地域医療支援病院	103	47%
災害拠点病院(基幹)	27	53%
災害拠点病院(地域)	96	45%
第三次救急医療機関	74	59%
第二次救急医療機関	127	33%
総合周産期母子医療センター	29	48%

地域周産期母子医療センター	47	49%
小児中核病院	13	62%
小児地域医療センター	7	47%
小児地域支援病院	2	100%
合計	195	7%

表11. 国家資格ごとの医療情報技師保有数と割合

	人数	割合
医師・歯科医師;	18	3%
看護師・助産師・保健師;	2	18%
薬剤師;	2	0%
診療放射線技師;	4	8%
臨床検査技師;	6	43%
臨床工学技士;	1	25%
その他	2	22%
国家系医療資格なし	294	12%

### (3) 情報処理安全確保支援士

情報処理安全確保支援士は16施設(2%)に配置されていた。国公立大学病院が5施設(13%)、公的な医療機関が8施設(2%)、私立大学病院が0施設(0%)、私立の医療機関が3施設(1%)で国公立大学病院に配置が多い傾向があった(表12)。病床数別では、600床以上の医療機関に多い傾向があった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関 515 施設で、16 施設(4%)が情報処理安全確保支援士を配置していた(表13)。総合周産期母子医療センター、小児中核

病院などが高い配置割合を示した。

情報処理安全確保支援士の資格を保有するのは医療系国家資格を保有していない人材がほとんどであった(表14)。

表12. 情報処理安全確保支援士を配置する医療機関(病床別)の施設数と割合

病床数	施設数	割合
～99床	0	0%
100床～199床	1	1%
200床～299床	0	0%
300床～399床	1	1%
400床～599床	3	2%
600床～799床	6	10%
800床～999床	2	6%
1000床～	3	21%

表13. 情報処理安全確保支援士を配置する医療機関(機能別)の施設数と割合

	施設数	割合
特定機能病院	5	7%
地域医療支援病院	9	4%
災害拠点病院(基幹)	0	0%
災害拠点病院(地域)	11	5%
第三次救急医療機関	6	5%
第二次救急医療機関	9	2%
総合周産期母子医療センター	8	13%
地域周産期母子医療センター	3	3%
小児中核病院	3	14%
小児地域医療センター	0	0%
小児地域支援病院	0	0%
合計	16	4%

表14. 国家資格ごとの情報処理安全確保支援士保有数と割合

	人数	割合
医師・歯科医師;	3	1%
看護師・助産師・保健師;	0	0%
薬剤師;	0	0%
診療放射線技師;	0	0%
臨床検査技師;	0	0%
臨床工学技士;	0	0%
その他	1	11%
国家系医療資格なし	294	12%

#### (4) 情報セキュリティマネジメント試験

情報セキュリティマネジメント試験合格者は34名、31施設(2%)に配置されていた。国公立大学病院が5施設(13%)、公的な医療機関が16施設(5%)、私立大学病院が1施設(3%)、私立の医療機関が9施設(4%)で国公立大学病院に配置が多い傾向があった(表15)。病床数別では、600床以上1000床未満の医療機関に多い傾向があった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関515施設で、27施設(5%)が情報セキュリティマネジメント試験合格者を配置していた(表16)。総合周産期母子医療センター、小児中核病院などが高い配置割合を示した。

情報セキュリティマネジメント試験合格者は、医師・歯科医師と国家資格を保有しない人材であった(表17)。

表15. 情報セキュリティマネジメント試験合格者を配置する医療機関(病床別)の施設数と割合

病床数	施設数	割合
～99床	3	4%
100床～199床	8	6%
200床～299床	1	1%
300床～399床	5	5%
400床～599床	4	3%
600床～799床	7	11%
800床～999床	3	10%
1000床～	0	0%

表16. 情報セキュリティマネジメント試験合格者を配置する医療機関(機能別)の施設数と割合

	施設数	割合
特定機能病院	6	9%
地域医療支援病院	14	6%
災害拠点病院(基幹)	2	4%
災害拠点病院(地域)	13	6%
第三次救急医療機関	10	8%
第二次救急医療機関	18	5%
総合周産期母子医療センター	6	10%
地域周産期母子医療センター	7	7%
小児中核病院	1	5%
小児地域医療センター	0	0%
小児地域支援病院	1	50%
合計	6	9%

表17. 国家資格ごとの情報セキュリティマネジメント試験合格者数と割合

	人数	割合

医師・歯科医師;	5	2%
看護師・助産師・保健師;	0	0%
薬剤師;	0	0%
診療放射線技師;	0	0%
臨床検査技師;	0	0%
臨床工学技士;	0	0%
その他	0	0%
国家系医療資格なし	29	3%

### (5) IT パスポート試験

IT パスポート試験合格者は 48 名、46 施設(7%)に配置されていた。国公立大学病院が 7 施設(18%)、公的な医療機関が 26 施設(8%)、私立大学病院が 1 施設(3%)、私立の医療機関が 12 施設(5%)で国公立大学病院に配置が多い傾向があった(表18)。病床数別では、600床以上の医療機関に多い傾向があった。

特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関 515 施設で、42 施設(8%)が IT パスポート試験合格者を配置していた(表19)。

IT パスポート試験合格者は、医師・歯科医師、臨床検査技師、臨床工学技士や国家資格を保有しない人材であった(表20)。

表18. IT パスポート試験合格者を配置する医療機関(病床別)の施設数と割合

病床数	施設数	割合
～99床	0	0%
100床～199床	1	1%
200床～299床	0	0%
300床～399床	1	1%

400床～599床	3	2%
600床～799床	6	10%
800床～999床	2	6%
1000床～	3	21%

表19. ITパスポート試験合格者を配置する医療機関(機能別)の施設数と割合

	施設数	割合
特定機能病院	11	16%
地域医療支援病院	20	9%
災害拠点病院(基幹)	5	10%
災害拠点病院(地域)	18	9%
第三次救急医療機関	11	9%
第二次救急医療機関	30	8%
総合周産期母子医療センター	6	10%
地域周産期母子医療センター	11	12%
小児中核病院	1	5%
小児地域医療センター	1	7%
小児地域支援病院	0	0%
合計	11	16%

表20. 国家資格ごとのITパスポート試験合格者数と割合

	人数	割合
医師・歯科医師;	4	1%
看護師・助産師・保健師;	0	0%
薬剤師;	0	0%
診療放射線技師;	0	0%
臨床検査技師;	2	13%
臨床工学技士;	1	13%
その他	0	0%
国家系医療資格なし	40	4%

## 5. 自施設の情報セキュリティ人材の配置状況について

自施設の情報セキュリティ人材の配置状況について、十分であると回答したのが113施設、不十分であると回答したのが530施設であった。不十分である理由として、自施設で既存人材の育成を現在行っている(今後、充足する見込み)が55施設、既存の情報セキュリティ人材の長期雇用が困難であるが72施設、少ない人数の情報セキュリティ人材に頼っており、退職時に引継ぎや新規雇用が困難と予想されるが317施設、新規雇用したくても、適切な人材が見つからないが265施設、新規雇用の費用捻出が困難が100施設、その他が68施設であった。その他の理由として、知識不足、人材育成の困難さなど知識の問題や、異動(公的医療機関)や専従専任ではないなど人事の問題が記載されていた。

## D. 考察

### 1. 医療情報システム安全管理責任者

医療情報システム安全管理責任者はアンケート回答施設の81%、病床数が400床以上の医療機関では90%を超える割合で配置されていた。特定機能病院、地域医療支援病院、災害拠点病院(基幹)、災害拠点病院(地域)、第三次救急医療機関、第二次救急医療機関、総合周産期母子医療センター、地域周産期母子医療センター、小児中核病院、小児地域医療センター、小児地域支援病院の認定や指定を受けている医療機関は、各地域の医療の中核的役割が強いと考えられる。これらの医療機関では、83%の割合で医療情報システム安全管理責任者が配置されていたが、災害拠点病院(地域)、第二次救急医療機関は配置割合がやや低めと結果となった。

医療情報システム安全管理責任者のうち、401名(77%)は上級医療情報技師、医療情報技師、診療情報管理士など学会・団体等が認定する資格・試験、IPAが認定する資格・試験のいずれも保有していなかった。医療情報システム安全管理責任者のうち、医療情報システム安全管理責任者は院長、院長を補佐する立場が210名(40%)、事務部門の長が73名(14%)を占めていた。これらのうち、調査対象となった資格・試験のいずれも保有しない人材は259名(92%)とその割合は全体に比較して高くなった。資格や試験だけで情報セキュリティの知識を判断することはできないが、役職として医療情報システム安全管理責任者となっているが、情報セキュリティの知識が十分でない方が一定数いることが予想された。

医療機関において、情報セキュリティ対策を講じるためには、医療機関として情報セキュリティ対策の方針を策定し、全職員に周知するとともに、情報セキュリティ対策への投資が必要となる。このため、医療情報システム安全管理責任者が、経営・運営上の意思決定に関与する立場にあるか否かは重要である。本調査では、医療情報システム安全管理責任者のうち350名(67%)が意思決定に関与する立場であった。調査対象となった資格・試験を有する医療情報システム安全管理責任者は119名で、意思決定に関与する立場は45名(38%)にとどまった。今後、人材育成の中で、調査対象となった資格・試験を有する人材を増やし、これらの資格を有する人材が自施設の経営・運営上の意思決定に関与する立場に育てていくことが大切と考えられた。

## 2. 医療情報システムの情報セキュリティ事案の担当者

すくなくとも1名は医療情報システムの情報セキュリティ事案の担当者を配置している医療機関は499施設(78%)で、医療情報システム安全管理責任者または情報セキュリティ事案の担当者を少なくとも1名配置する施設は592施設(92%)であった。200床を超える医療機関では、情報セキュリティ事案の担当者の配置割合は80%を超えていたが、病床数増加によりその割合が増えることはなかった。医療情報システム安全管理責任者の設置割合が低かった災害拠点病院(地域)や第二次救急医療機関では、医療情報システムの情報セキュリティ事案の担当者の設置率については、災害拠点病院(地域)は90%を超えており、第二次救急医療機関でも79%と他と変わらない設置率であった。一方、特定機能病院や小児中核病院は医療情報システムの情報セキュリティ事案の担当者の設置率が80%未満となる結果であった。

3人目までに登録された医療情報システムの情報セキュリティ事案の担当者922人のうち、468名(51%)は上級医療情報技師、医療情報技師、診療情報管理士など学会・団体等が認定する資格・試験、IPAが認定する資格・試験のいずれも保有していなかった。少なくとも1名は医療情報システムの情報セキュリティ事案の担当者を配置する499施設のうち、208施設(42%)は調査対象となった資格・試験を保有する医療情報システムの情報セキュリティ事案の担当者が1名も配置されていなかった。

医療情報システム安全管理責任者が調査対象となった資格・試験を有さない401施設のうち、348施設(87%)は医療情報システムの情報セキュリティ事案の担当者を配置していた。これらの医療情報システムの情報セキュリティ事案の担当者のうち、調査対象となった資格・試験を有する人材は156名(45%)にとどまった。院



長、院長を補佐する立場、事務部門の長に限定すると、医療情報システム安全管理責任者が資格・試験を有さない259施設のうち、230施設(89%)は医療情報システムの情報セキュリティ事案の担当者を配置していた。これらの医療情報システムの情報セキュリティ事案の担当者のうち、調査対象となった資格・試験を有する人材は127名(55%)であった。

現時点においては、院長、院長を補佐する立場(副院長、院長補佐など)、事務部門の長などが医療情報システム安全管理責任者となり意思決定を行い、医療情報システム安全管理責任者の知識が不足するところを医療情報システムの情報セキュリティ事案の担当者を配置することで補っている施設が多いと考えられた。

### 3. 情報セキュリティの人材の配置

IPAのITスキル標準レベル4に相当する情報処理安全確保支援士は、回答があった施設ではわずか16施設(2%)が配置されている状況であった。情報処理安全確保支援士の検索サイトで勤務先名称を病院で検索すると26名の情報処理安全確保支援士が見つかった。情報処理安全確保支援士の全てが検索サイトに登録されているわけではないが、医療機関に所属する情報処理安全確保支援士は多くはないと考えられる。情報セキュリティマネジメント試験(レベル2)、ITパスポート試験(レベル1)の取得割合はやや増えるが、いずれも1桁の割合であり、ITスキル標準が下がると保有割合が増えるわけではなかった。IPAの資格、試験を有する人材は多くないことが明らかになった。

上級医療情報技師の配置は36施設(6%)にとどまったが、医療情報技師は219施設(34%)に配置されていた。上級医療情報技師は600

床を超える医療機関に多く配置されていたが、医療情報技師は病床数の比較的少ない医療機関でもある程度の割合で配置されていた。上級医療情報技師が医療情報技師を指導する体制を取ることができれば、病床数が少ない医療機関の情報セキュリティ体制を強化できる可能性もある。

上級医療情報技師40人のうち、情報処理安全確保支援士は2名(5%)、応用情報技術者試験は9名(23%)、基礎情報技術者試験は9名(23%)、情報セキュリティマネジメント試験は8名(20%)、ITパスポート試験は5名(13%)保有しており、上級医療情報技師の資格を有さない人材に比較し、IPAの資格の保有率は高かった。今後、上級医療情報技師がIPAの資格、試験を目指すことで、さらに情報セキュリティ対策の知識が深まることが期待される。

自施設の情報セキュリティ人材の配置状況について、不十分であると回答したのが530施設(82%)であり、今後もさらに情報セキュリティ人材の育成を進める必要があると考えられた。

### 3. 制限事項

今回の調査はWebアンケート調査であり、各医療機関の団体にアンケート調査依頼をメールリスト等で送っていただいた。回答は任意であり、医療機関名などは収集していない。このため、どのような医療機関が回答をいただいたのかは不明である。

情報セキュリティ対策に前向きな医療機関が積極的に回答いただいた可能性がある一方、情報セキュリティ対策に課題を感じている医療機関が積極的に回答いただいた可能性も考えられる。

## E. 結論

Web を用いたアンケート調査で、全国の医療機関の情報セキュリティ人材の配置状況を調査した。一定の割合で、医療情報システム安全管理責任者や医療情報システムの情報セキュリティ事案担当者が配置されていたが、上級医療情報技師や情報処理安全確保支援士といった資格、試験を有する人材は限定され、情報セキュリティに対して、どの程度の知識を有するかは課題があると考えられた。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

(1) 武田 理宏、サイバーインシデント対策と医療安全、医療安全推進ジャーナル 73, 10-15, 2023

### 2. 学会発表

(1) 武田 理宏、医療機関に求められる医療情報人材とは、日本医療情報学会関西支部会、2023 年度第 1 回講演会、2023 年 10 月、大阪

(2) 医療分野のセキュリティ人材の育成をどうするか、第 43 回医療情報学連合大会シンポジウム、2023 年 11 月、神戸、(座長：武田 理宏、谷川 琢海)

① 武田 理宏、医療機関における情報セキュリティ人材の育成と配置に向けて

② 岡本 潤(厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室)、厚生労働省における医療機関の情報セキュリティの強化に向けた取り組み

③ 大道 道大(大道会 森之宮病院)、病院の ICT

の変遷と医療情報システムの人材確保について

④ 奥村 明俊(情報処理推進機構(IPA))サイバーセキュリティ人材育成に関する IPA の取組み

⑤ 谷川 琢海、診療業務を理解したセキュリティ人材の育成に向けて

(3) みんなでつくるセキュリティの医療現場改革に向けて 情報共有体制の重要性、第 43 回医療情報学連合大会産学官連携企画、2023 年 11 月、神戸、(座長：武田 理宏、並川 寛和 (保健医療福祉情報システム工業会(JAHIS)))

① 新畑 覚也(厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室)、医療分野におけるサイバーセキュリティ対策の厚生労働省の取組について

② 谷川 琢海、医療情報技師の観点からの医療分野の ISAC の必要性

③ 大谷 俊介(誠馨会 千葉中央メディカルセンター)、医療分野における医療機関関係者・医療従事者を中心とした ISAC 設立に向けた検討

④ 洞田 慎一(JPCERT コーディネーションセンター)、ISAC 等で使用するサイバーセキュリティに関連する情報共有ツール SIGNAL に関して

## H. 知的財産権の出願・登録状況

(予定を含む。)

### 1. 特許取得

なし

### 2. 実用新案登録

なし

### 3. その他

なし

## 情報セキュリティ人材配置状況の調査へのご協力をお願い

今年度より、厚生労働行政推進調査事業「安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究(23IA2007)」(研究代表者:大阪大学 武田 理宏)が実施しています。

本事業は、保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等を調査、検証をすることを目的としています。実現可能な提言を作成するために、最初に各医療機関の情報セキュリティ人材の配置状況を調査させていただくことになりました。

質問では、医療情報システム安全管理責任者、情報セキュリティ担当者の保有する資格・試験を問う項目があります。

医療系国家資格(医師・歯科医師、看護師・助産師・保健師、薬剤師、診療放射線技師、臨床検査技師、臨床工学技士)、医療情報に関して学会・団体等が認定する資格・試験(上級医療情報技師、医療情報技師、診療情報管理士)、情報処理推進機構(IPA)が認定する資格・試験(情報処理安全確保支援士、応用情報技術者試験、基礎情報技術者試験、情報セキュリティマネジメント試験、ITパスポート試験、その他 IPA が認定する資格・試験)をあらかじめご確認いただき、ご回答をお願いします。別紙、「医療情報システム安全管理責任者、情報セキュリティ担当者の保有する資格・試験」をご活用ください。

様々な特性を持つ医療機関の状況を把握するために、できるだけ多くの医療機関からご回答をお願いしたいと思っております。大変お忙しいと思いますが、ご協力をよろしくお願いいたします。

回答は下記 URL からお願いします。スマートフォンからも回答が可能です。

<https://forms.office.com/r/m6gJgrPJPd>



回答期限:2023年12月26日(月)

問い合わせ先:

大阪大学大学院 医学系研究科 医療情報学

武田 理宏

ttakeda@hp-info.med.osaka-u.ac.jp

## 情報セキュリティ人材配置状況の調査 質問項目

質問は下に示す構成となっています。

【セクション 1】 貴施設について（6 問）

↓

【セクション 2】 医療情報システム安全管理責任者の配置状況と保有する資格（最大 9 問）

↓

【セクション 3】 医療情報システム安全管理責任者を配置しない医療機関の情報セキュリティ事案対応（最大 4 問）

【セクション 4】 医療情報システム安全管理責任者を配置する医療機関の情報セキュリティ事案対応（最大 4 問）

↓

情報セキュリティ担当者を配置している場合（配置していない場合は回答不要）

【セクション 5】 情報セキュリティ担当者（1 人目）について（7 問）

【セクション 6】 情報セキュリティ担当者（2 人目）について（7 問）

【セクション 7】 情報セキュリティ担当者（3 人目）について（7 問）

【セクション 8】 情報セキュリティ担当者（4 人目）について（1 問）

↓

【セクション 9】 貴施設の情報セキュリティ人材の配置状況について（最大 4 問）

↓

【セクション 10】 アンケート調査回答者について（1 問）

## 情報セキュリティ人材配置状況の調査 質問項目一覧

### 【セクション 1】 貴施設についておしえてください。

1.【必須】所在地(都道府県)についてお教えてください。(自由記載)

2.【必須】所属する二次医療圏をお教えてください。(自由記載)

3.【必須】貴施設に該当するものをお選びください。(単一選択)

※公的な医療機関とは、医療法第 31 条に規定される、次に掲げる者が開設する医療機関を指します。

都道府県、市町村、地方公共団体の組合、国民健康保険団体連合会及び国民健康保険組合、日本赤十字社、社会福祉法人恩賜財団済生会、厚生農業協同組合連合会、社会福祉法人北海道社会事業協会

国公立大学病院  公的な医療機関(大学病院を除く)  私立大学病院  私立の医療機関

4.【必須】貴施設の認定、指定についてお教えてください。(複数選択)

特定機能病院  地域医療支援病院  災害拠点病院(基幹)  災害拠点病院(地域)

第三次救急医療機関  第二次救急医療機関  総合周産期母子医療センター

地域周産期母子医療センター  小児中核病院  小児地域医療センター  小児地域支援病院

上記の認定、指定は受けていない

5.【必須】許可病床数についてお教えてください。(単一選択)

1000 床以上  800 床以上 1000 床未満  600 床以上 800 床未満  400 床以上 600 床未満

300 床以上 400 床未満  200 床以上 300 床未満  100 床以上 200 床未満  100 床未満

6.【必須】診療録管理体制加算の算定状況をお聞かせください。(単一選択)

加算1  加算2  算定していない

**【セクション 2】医療情報システム安全管理責任者について**

**7.【必須】医療情報システム安全管理責任者を配置していますか。(単一選択)**

- はい →問9に  
 いいえ →問8に

**8.【必須】今後、医療情報システム安全管理責任者を配置する予定はありますか。(単一選択)**

- はい(既存人材の活用)  はい(新規人材の雇用)  いいえ →【セクション 3】に

**9.【必須】医療情報システム安全管理責任者の職位をお答えください。(単一選択)**

※兼任等されている場合、上位の職位をお答えください。

- 院長  院長を補佐する立場(副院長、院長補佐など)  医療情報システム管理部門の長  
 事務部門の長  上記以外の部門の長  その他(自由記載)

**10.【必須】医療情報システム安全管理責任者の所属する診療科や部署の名称をお答えください。(自由記載)**

**11.【必須】医療情報システム安全管理責任者は医療機関の経営・運営上の意思決定に関与する立場にありますか。(単一選択)**

- あり  なし

**12.【必須】医療情報システム安全管理責任者が保有する医療系国家資格についてお答えください。(複数選択)**

※リストにない場合は、その他の欄に記載してください。

- 医師・歯科医師  看護師・助産師・保健師  薬剤師  診療放射線技師  
 臨床検査技師  臨床工学技士  医療系国家資格を保持していない  その他(自由記載)

**13.【必須】医療情報システム安全管理責任者が保有する学会・団体等が認定する資格・試験についてお答えください。(複数選択)**

※医療情報に関する資格・試験についてお答えください。※リストにない場合は、その他の欄にご記載ください。

- 上級医療情報技師  医療情報技師  診療情報管理士  
 上記、資格を保持していない  その他(自由記載)

**14.【必須】医療情報システム安全管理責任者が保有する情報処理推進機構(IPA)が認定する資格・試験についてお答えください。(複数選択)**

※IPA が認定する資格・試験で、リストにない場合は、その他の欄にご記載ください。

- 情報処理安全確保支援士  応用情報技術者試験  基礎情報技術者試験  
 情報セキュリティマネジメント試験  IT パスポート試験  IPA が認定する資格・試験は保持していない  
 その他(自由記載)

**15.【必須】医療情報システム安全管理責任者の雇用形態についてお答えください。(単一選択)**

- 常勤(雇用期限なし)  常勤(雇用期限あり)  非常勤

**16.【必須】医療情報システム安全管理責任者の勤務形態についてお答えください。(単一選択)**

※専任・専従とはそれぞれ、その就業時間の少なくとも5割以上・8割以上、当該業務に従事しているものとします。

- 専従  専任  兼任

→【セクション 4】に

**【セクション 3】医療情報システム安全管理責任者を配置しない医療機関の情報セキュリティ事案対応**

17.【必須】医療情報システムの情報セキュリティ事案を担当する部署はありますか。(単一選択)

- はい →問18 に
- いいえ(今後、設置する予定がある) →問 19 に
- いいえ(今後、設置する予定はない) →問 19 に

18.【必須】医療情報システムの情報セキュリティ事案を担当する部署名をお答えください。(自由記載)

19.【必須】医療情報システムの情報セキュリティ事案の担当者はいますか。(単一選択)

- はい →問 20 に
- いいえ(今後、担当者を配置する予定がある) →問 21 に
- いいえ(今後、担当者を配置する予定はない) →問 21 に

20.【必須】医療情報システムの情報セキュリティ事案の担当者の人数を教えてください。(数値記載)

→【セクション 5】に

21.【必須】医療情報システムの情報セキュリティ事案への対応をお教えてください。(単一選択)

- 同一医療法人など同一組織の別施設の情報セキュリティ担当者と協力して対応している。
- 業者等に外部委託契約あるいは保守契約に含めて対応している。
- 十分な対応はとれていない。 ○その他(自由記載)

→【セクション 9】に

**【セクション 4】医療情報システム安全管理責任者を配置する医療機関の情報セキュリティ事案対応**

22.【必須】医療情報システムの情報セキュリティ事案を担当する部署はありますか。(単一選択)

- はい →問 23 に
- いいえ(今後、設置する予定がある) →問 24 に
- いいえ(今後、設置する予定はない) →問 24 に

23.【必須】医療情報システムの情報セキュリティ事案を担当する部署名をお答えください。(自由記載)

24.【必須】医療情報システム安全管理責任者以外に医療情報システムの情報セキュリティ事案の担当者はいますか。(単一選択)

- はい →問 25 に
- いいえ(今後、担当者を配置する予定がある) →問 26 に
- いいえ(今後、担当者を配置する予定はない) →問 26 に

25.【必須】医療情報システムの情報セキュリティ事案の担当者の人数を教えてください。(数値記載)

→【セクション 5】に

26.【必須】医療情報システムの情報セキュリティ事案への対応をお教えてください。(単一選択)

- 医療情報システム安全管理責任者が全て対応をしている。
- 同一医療法人など同一組織、別施設の情報セキュリティ担当者と協力して対応している。
- 業者等に外部委託契約あるいは保守契約に含めて対応している。
- 十分な対応はとれていない。 ○その他(自由記載)

→【セクション 9】に

**【セクション 5】情報セキュリティ担当者(1人目)について**

**27.【必須】情報セキュリティ担当者(1人目)の所属する部門をお答えください。(単一選択)**

- 医療情報システム管理部門 診療情報管理部門 事務部門 その他(自由記載)

**28.【必須】情報セキュリティ担当者(1人目)が保有する医療系国家資格についてお答えください。(複数選択)**

※リストにない場合は、その他の欄にご記載ください。

- 医師・歯科医師 看護師・助産師・保健師 薬剤師 診療放射線技師、  
臨床検査技師 臨床工学技士 国家系医療資格を保持していない その他(自由記載)

**29.【必須】情報セキュリティ担当者(1人目)が保有する学会・団体等が認定する資格についてお答えください。(複数選択)**

※医療情報に関する資格・試験についてお答えください。※リストにない場合は、その他の欄にご記載ください。

- 上級医療情報技師 医療情報技師 診療情報管理士  
上記、資格を保持していない その他(自由記載)

**30.【必須】情報セキュリティ担当者(1人目)が保有する情報処理推進機構(IPA)が認定する資格・試験についてお答えください。(複数選択)**

※IPAが認定する資格・試験でリストにない場合は、その他の欄にご記載ください。

- 情報処理安全確保支援士 応用情報技術者試験 基礎情報技術者試験  
情報セキュリティマネジメント試験 ITパスポート試験 IPAが認定する資格は保持していない  
その他(自由記載)

**31.【必須】情報セキュリティ担当者(1人目)の雇用形態についてお答えください。(単一選択)**

- 常勤(雇用期限なし) 常勤(雇用期限あり) 非常勤

**32.【必須】情報セキュリティ担当者(1人目)の勤務形態についてお答えください。(単一選択)**

※専任・専従とはそれぞれ、その就業時間の少なくとも5割以上・8割以上、当該業務に従事しているものとします。

- 専従 専任 兼任

**33.【必須】情報セキュリティ担当者(2人目)の入力を行いますか。(単一選択)**

- はい →【セクション6】に  
いいえ →【セクション9】に



**【セッション 6】情報セキュリティ担当者(2人目)について**

34.【必須】情報セキュリティ担当者(2人目)の所属する部門をお答えください。(単一選択)

- 医療情報システム管理部門 診療情報管理部門 事務部門 その他(自由記載)

35.【必須】情報セキュリティ担当者(2人目)が保有する医療系国家資格についてお答えください。(複数選択)

※リストにない場合は、その他の欄にご記載ください。

- 医師・歯科医師 看護師・助産師・保健師 薬剤師 診療放射線技師  
臨床検査技師 臨床工学技士 国家系医療資格を保持していない その他(自由記載)

36.【必須】情報セキュリティ担当者(2人目)が保有する学会・団体等が認定する資格についてお答えください。(複数選択)

※医療情報に関する資格・試験についてお答えください。※リストにない場合は、その他の欄にご記載ください。

- 上級医療情報技師 医療情報技師 診療情報管理士  
上記、資格を保持していない その他(自由記載)

37.【必須】情報セキュリティ担当者(2人目)が保有する情報処理推進機構(IPA)が認定する資格・試験についてお答えください。(複数選択)

※IPAが認定する資格・試験で、リストにない場合は、その他の欄にご記載ください。

- 情報処理安全確保支援士 応用情報技術者試験 基礎情報技術者試験  
情報セキュリティマネジメント試験 ITパスポート試験 IPAが認定する資格は保持していない  
その他(自由記載)

38.【必須】情報セキュリティ担当者(2人目)の雇用形態についてお答えください。(単一選択)

- 常勤(雇用期限なし) 常勤(雇用期限あり) 非常勤

39.【必須】情報セキュリティ担当者(2人目)の勤務形態についてお答えください。(単一選択)

- 専従 専任 兼任

40.【必須】情報セキュリティ担当者(3人目)の入力を行いますか。(単一選択)

- はい →【セッション7】に  
いいえ →【セッション9】に

**【セクション 7】情報セキュリティ担当者(3 人目)について**

41.【必須】情報セキュリティ担当者(3 人目)の所属する部門をお答えください。(単一選択)

- 医療情報システム管理部門 診療情報管理部門 事務部門 その他(自由記載)

42.【必須】情報セキュリティ担当者(3 人目)が保有する医療系国家資格についてお答えください。(複数選択)

※リストにない場合は、その他の欄にご記載ください。

- 医師・歯科医師 看護師・助産師・保健師 薬剤師 診療放射線技師  
臨床検査技師 臨床工学技士 国家系医療資格を保持していない その他(自由記載)

43.【必須】情報セキュリティ担当者(3 人目)が保有する学会・団体等が認定する資格についてお答えください。(複数選択)

※医療情報に関する資格・試験についてお答えください。※リストにない場合は、その他の欄にご記載ください。

- 上級医療情報技師 医療情報技師 診療情報管理士  
上記、資格を保持していない その他(自由記載)

44.【必須】情報セキュリティ担当者(3 人目)が保有する情報処理推進機構(IPA)が認定する資格・試験についてお答えください。(複数選択)

※IPA が認定する資格・試験でリストにない場合は、その他の欄にご記載ください。

- 情報処理安全確保支援士 応用情報技術者試験 基礎情報技術者試験  
情報セキュリティマネジメント試験 IT パスポート試験 IPA が認定する資格は保持していない  
その他(自由記載)

45.【必須】情報セキュリティ担当者(3 人目)の雇用形態についてお答えください。(単一選択)

- 常勤(雇用期限なし) 常勤(雇用期限あり) 非常勤

46.【必須】情報セキュリティ担当者(3 人目)の勤務形態についてお答えください。(単一選択)

※専任・専従とはそれぞれ、その就業時間の少なくとも5割以上・8割以上、当該業務に従事しているものとします。

- 専従 専任 兼任

47.【必須】情報セキュリティ担当者(4 人目以降)の入力を行いますか。(単一選択)

- はい →【セクション 8】に  
いいえ →【セクション 9】に

**【セクション 8】情報セキュリティ担当者(4人目以降)について**

48.【必須】4人目以降の情報セキュリティ担当者について、簡単に状況をご記載ください。(自由記載)

**【セクション 9】貴施設の情報セキュリティ人材の配置状況について**

49.【必須】貴施設の情報セキュリティ人材の配置状況についてお考えをお聞かせください。(単一選択)

- 十分である →問 51 に
- 不十分である →問 50 に

50.【必須】貴施設の情報セキュリティ人材の配置が不十分である理由をお聞かせください。(複数選択)

- 自施設で既存人材の育成を現在行っている(今後、充足する見込み)。
- 既存の情報セキュリティ人材の長期雇用が困難である。
- 少ない人数の情報セキュリティ人材に頼っており、退職時に引継ぎや新規雇用が困難と予想される。
- 新規雇用したくても、適切な人材が見つからない。  新規雇用の費用捻出が困難。  その他(自由記載)

51.情報セキュリティ人材の育成、配置について、ご意見があればご記載ください。(自由記載)

52.厚生労働行政推進調査事業費「安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究(23IA2007)」に対するご意見があればご記載ください。(自由記載)

**【セクション 10】アンケート調査回答者について**

53.【必須】ご協力ありがとうございました。

最後に、あなた(アンケートにご回答いただいている方)のお立場をお聞かせください。(単一選択)

- 医療情報システム安全管理責任者  情報セキュリティ担当者(医療情報システム安全管理責任者を除く)
- 医療機関の経営・運営上の意思決定に関与する立場の医療職(医療情報システム安全管理責任者を除く)
- 医療機関の経営・運営上の意思決定に関与する立場の事務職(医療情報システム安全管理責任者を除く)
- その他の医療職  その他の事務職  その他(自由記載)

## 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年程度と長いと、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実行できること。

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

(Cx0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の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（攻撃者視点对策能力）

識別、防御、検知、対応、復旧の視点

3・Continuous Diagnostics and Mitigation (CDM)視点（防衛者視点对策能力）

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 Threat: 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

なし  
1. 特許取得  
なし  
・ 実用新案登録  
なし  
3. その他  
なし

#### H. 知的財産権の出願・登録状況

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の、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実行できること
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セ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な要件の運用管理規程) 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)

## 分担研究報告書

テーマ：情報セキュリティに関する医療系専門職等の教育状況  
および医療情報に関する専門職の育成状況の把握

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**

本研究では、医療機関における情報セキュリティ人材の育成と配置を進めていくため、保健医療系国家資格を有する医療系専門職と、日本医療情報学会で育成している医療情報技師の教育カリキュラムを含む育成状況について調査を行った。国家試験の出題基準と出題実績の調査結果から、情報セキュリティに関する基礎的な教育を行っていると考えられたのは、臨床工学技士、診療放射線技師、臨床検査技師であった。また、上級医療情報技師と医療情報技師の到達目標や教科書、過去の試験問題、セミナー内容のなかに、医療機関が情報セキュリティに取り組むために必要な内容が豊富に含まれていた。医療情報技師の育成は長期にわたり継続して行われており、医療情報技師や上級医療情報技師の認定者の医療機関への配置が進みつつある状況であった。安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材として、これらの人材を活用できる可能性があることが示唆された。

**A. 研究目的**

サイバーセキュリティ戦略本部が作成している「重要インフラのサイバーセキュリティに係る行動計画及び重要インフラの情報セキュリティ対策に係る第4次行動計画」によると、情報セキュリティ対策にあたっては、自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施することが示されている。安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置においては、限られた医療資源と財源のなかで効率的に情報セキュリティ人材の育成と配置に取り組んでいくことや、保健医療福祉分野の特性や診療業務の実際を理解しながら情報セ

キュリティへの対応を効果的に行っていく体制づくりを行っていくことが求められる。

本研究では、保健医療系国家資格を有する医療系専門職と、学会が認定する医療情報に関する専門職の教育、試験、研修の状況の現状を把握することを目的として調査を行った。

**B. 研究方法****1. 保健医療系国家資格を有する医療系専門職の教育状況**

厚生労働省が所管する保健医療・福祉関係の国家資格（表1）ごとの情報セキュリティに関する教育状況と内容について、インターネットに公開されている国家試験出題基準（薬学教育モデル・コア・カリキュラム等を含む）と過去5年間の国家試験において出題された問題を

調べることによって調査を行い、教育状況について検討を行った。

表1 厚生労働省が所管する保健医療関係の国家資格

医師、歯科医師、薬剤師、保健師、助産師、看護師、診療放射線技師、臨床検査技師、理学療法士、作業療法士、言語聴覚士、視能訓練士、臨床工学技士、義肢装具士、歯科衛生士、歯科技工士、救急救命士、あん摩マッサージ指圧師、はり師、きゅう師、柔道整復師、管理栄養士
--

## 2. 医療情報技師（日本医療情報学会）の情報セキュリティに関する教育カリキュラム

一般社団法人日本医療情報学会が医療情報に関する専門職として育成、能力検定試験を実施している医療情報技師および上級医療情報技師について、日本医療情報学会医療情報技師育成部会のホームページ（図1）に公開されている情報などをもとに、教育コンテンツ、能力検定試験の概要、及びこれまでの合格者数（認定者数）等について情報収集して調査を行った。



図1 日本医療情報学会のホームページ  
(<https://www.jami.jp>)

## C. 研究結果

### 1. 保健医療系国家資格を有する医療系専門職の教育状況

国家試験の2024年4月現在のインターネットに公開されている最新の出題基準と過去問

題における情報セキュリティに記載の有無および過去5年間（2019年～2023年）の国家試験における出題実績を表2に示す。

表2 国家資格ごとの情報セキュリティに関する出題動向

資格	出題基準	出題実績
医師	○	×
歯科医師	×	×
薬剤師	×	×
保健師	○	×
助産師	×	×
看護師	×	×
診療放射線技師	○	○
臨床検査技師	○	○
理学療法士	○	×
作業療法士	○	×
言語聴覚士	-	×
視能訓練士	×	×
臨床工学技士	○	○
義肢装具士	-	×
歯科衛生士	-	×
歯科技工士	-	×
救急救命士	×	×
あん摩マッサージ指圧師	×	×
はり師	×	×
きゅう師	×	×
柔道整復師	-	×
管理栄養士	×	×

注:「-」はインターネット上に公開されている出題基準を確認できなかった。

出題基準に情報セキュリティに関係する用語の記載があったのは、医師、保健師、診療放射線技師、臨床検査技師、理学療法士、作業療法士、臨床工学技士であった。言語聴覚士、義肢装具士、歯科衛生士、歯科技工士についてはインターネットでの出題基準の掲載を確認することができず、それ以外の職種については出題基準のなかに情報セキュリティに関係する用語は記載されていなかった。

また、過去5年間の国家試験において、情報

セキュリティに関する出題が行われていたのは、5年間のなかで診療放射線技師で2問、臨床検査技師で1問、臨床工学技士で10問であり、臨床工学技士国家試験が最も出題頻度が高く、毎年、出題されていた。問題の内容は、いずれも情報セキュリティに関する基礎的な技術に関する内容の出題であった。それ以外の職種については、個人情報保護に関する出題はあるものの、情報セキュリティに関する技術的な主題は確認することができなかった。

## 2. 医療情報技師（日本医療情報学会）の情報セキュリティに関する教育カリキュラム

日本医療情報学会は、医療情報に関心を持つ研究者および実務担当者の学術交流の場として設立された学会である。会員は、医師のほか、看護師、薬剤師、臨床検査技師、診療放射線技師、事務担当者、病歴担当者、コンピュータ技術者等の多様な職種から構成される。当学会では、医療情報に関する専門職の育成が目的のひとつに掲げられており、2003年から専門職として位置付ける「医療情報技師」および2007年から「上級医療情報技師」（以下、医療情報技師等という）の能力検定試験を通じた認定、2009年から医療情報システムの利用者を主な対象とする医療情報基礎知識検定試験の実施している。

日本医療情報学会では、医療情報技師と上級医療情報技師を表3に示すように定義しており、医療情報技師等を目指す人のための教育コンテンツとして、到達目標（一般目標と行動目標群：GIO・SBOs）の設定、教科書の刊行、セミナー・e-Learningの実施等を行っている。教科書「医療情報」は、医学医療編、医療情報システム編、情報処理技術編の3編から構成されており、医療情報技師の到達目標に基づいた

内容に編集されている。

**表3 医療情報技師と上級医療情報技師の定義**  
医療情報技師の定義

保健医療福祉の質と安全の向上のために、医療の特質をふまえ、最適な情報処理技術を用い、医療情報を安全かつ適切に管理・活用・提供することができる保健医療福祉分野の専門職

上級医療情報技師の定義

保健医療福祉の質と安全の向上のために、幅広い知識と豊かな経験を背景として、全体最適の観点から保健医療福祉分野の情報化と医療情報の利活用を総括的に推進できる医療情報技師

医療情報技師の到達目標(2022年3月24日更新)には、「診療録およびその他の医療記録」(医学・医療系 GIO-8)、「医療管理」(医学・医療系 GIO-3)、「病院情報システムの機能」(医療情報システム系 GIO-2)、「病院情報システムの運用」(GIO-4)、「医療情報分野の関連法規とガイドライン」(医療情報システム系 GIO-7)、「情報セキュリティ」(情報処理技術系 GIO-6)などの情報セキュリティへの対応に必要な内容が網羅的に含まれていた(表4、5)。また、上級医療情報技師の一般目標及び行動目標群(GIO・SBOs) ver.1.5(2024年4月21日更新)では、「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修得する」(GIO-6)など、医療情報システムに対する情報セキュリティの実践に必要な内容が示されていた。また、生涯研修セミナーやe-Learningコンテンツが用意されており、情報セキュリティに関する内容のものも含まれていた。

表4 医療情報技師の到達目標の情報セキュリティに関する主な記述(抜粋)

医療情報システム系	
項番	GIO・SBOs
4	病院情報システムのシステム構成と機能
4-1	病院情報システムの運用管理のための組織体制を理解する。
4-2	病院情報システムの運用管理規程を作成する目的と作成方法を理解する。
4-3	病院情報システムの運用管理を理解する。
4-4	病院情報システムの評価・改善を理解できる。
7	医療情報分野の関連法規とガイドラインを理解する。
7-1	医療情報分野の関連法規とガイドラインの全体構成を理解する。
7-2	個人情報保護法の概要を理解する。
7-3	次世代医療基盤法の概要を理解する。
7-4	医療情報システムの安全管理に関するガイドラインの概要を理解する。
7-5	医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスの概要を理解する。
7-6	医療情報に関するその他のガイドラインの概要を理解する。
情報処理技術系	
6	情報セキュリティ
6-1	情報セキュリティの概念やその対策を理解する。
6-2	情報を安全に管理・活用するための基本的な情報セキュリティ技術を理解する。

表5 上級医療情報技師の到達目標の情報セキュリティに関する主な記述(抜粋)

項番	GIO・SBOs
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修得する。
6-1	情報セキュリティのリスク分析を行うことができる。
6-2	情報セキュリティ対策についての知識を有しており、協議、立案することができる。
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。
6-4	情報システムの監査についての知識を有しており、立案できる。
6-5	個人情報の保護についての知識を有しており、適切に医療情報システム内に取り込むことができる。
6-6	医療情報セキュリティに関連する諸ガイドラインの内容を具体的に説明できる。

### 3. 医療情報技師能力検定試験・上級医療情報技師能力検定試験の内容および合格者

能力検定試験は、医療情報基礎知識検定試験（年2回）、医療情報技師能力検定試験（年1回）、上級医療情報技師検定試験（年1回）をそれぞれ実施しており、医療情報基礎知識検定試験と医療情報技師能力検定試験については受検資格が特に設けられておらず、上級医療情

報技師については医療情報システムに関する実務経験を受験資格として設けていた。医療情報技師能力検定試験は、医療情報システム、医学・医療、情報処理技術の3科目の試験となっており、過去5年間の出題実績では、医療情報システム系（全60問）と情報処理技術系（全50問）においてそれぞれ10問程度の出題があった。医療情報技師能力検定試験の情報セキュリティに関する出題の抜粋を表6に示す。また、上級医療情報技師能力検定試験は、午前試験（マークシート方式、50問程度）、午後Ⅰ試験（マークシート方式・記述方式、15問程度）、午後Ⅱ試験（小論文方式）の構成となっており、情報セキュリティに関する出題は2023年度の試験で幅広い知識を問う午前試験で7問、診療現場での実践的な知識・技術を問う午後Ⅰ試験で2問の出題があった（表7）。

2023年度末までに医療情報技師 26,963人（累計）、上級医療情報技師 532人（累計）が試験に合格して認定を受けていた。また、2022年度末時点において、資格の更新を継続的に行い、資格を保有していたのは医療情報技師が合格者累計の約56%にあたる14,566名、上級医療情報技師が約94%にあたる502名であった。合格者（累計）が受検時に申告した勤務先が保健医療福祉施設だったのは、医療情報技師が勤務先の回答のある25,836名のうち7,571名（29.3%）、上級医療情報技師が532名のうち183名（34.4%）であった。

表6 医療情報技師能力検定試験の情報セキュリティに関する出題の抜粋

医療情報システム系 (2023 年度 医療情報技師能力検定試験)
<p>問32 病院情報システムの「運用管理規程」の説明として正しいのはどれか。</p> <ol style="list-style-type: none"> <li>1) 国が定めた医療情報の取り扱いについてのガイドラインである。</li> <li>2) 病院情報システムの運用に関する基本方針を定めたものである。</li> <li>3) 医療情報技師が医療現場での業務遂行に必要な情報をまとめたものである。</li> <li>4) 医療機関における患者のプライバシー保護を目的とした規則を定めたものである。</li> <li>5) 医療従事者が患者の安全を確保するために遵守すべき基準や運用手順をまとめたものである。</li> </ol>
<p>問33 医療情報システムの運用について正しいのはどれか。</p> <ol style="list-style-type: none"> <li>1) ユーザーに管理者権限を付与する。</li> <li>2) すべての端末で共通のパスワードを設定する。</li> <li>3) サーバにウイルス対策ソフトをインストールする。</li> <li>4) リモート保守用の VPN 装置の設定を外部業者に一任する。</li> <li>5) 遠隔地から telnet で病院端末にアクセスできるようにする。</li> </ol>
<p>問35 特定の個人に権限が集中して不正の温床となることを回避するための手法はどれか。</p> <ol style="list-style-type: none"> <li>1) 多要素認証</li> <li>2) レジリエンス</li> <li>3) セグリゲーション</li> <li>4) シングルサインオン</li> <li>5) スイスチーズモデル</li> </ol>
<p>問36 障害発生時の連絡を受けたとき、病院の医療情報システム担当者が最初に行うべき対応はどれか。</p> <ol style="list-style-type: none"> <li>1) 障害の範囲を確認する。</li> <li>2) 端末やサーバを再起動する。</li> <li>3) 障害の発生を病院内にアナウンスする。</li> <li>4) 自動動作しているバックアッププロセスを中断する。</li> <li>5) 今後の障害発生防止のためにマニュアルを整備する。</li> </ol>
<p>問37 電子カルテシステムが導入された医療機関における障害時の紙運用について正しいのはどれか。</p> <ol style="list-style-type: none"> <li>1) 白紙にオーダ内容を手書きして実施部門へ搬送する。</li> <li>2) 防災訓練等の機会に紙伝票による運用を実行し検証する。</li> <li>3) 停電などにより病院情報システムが完全停止した際に実施される。</li> <li>4) システム復旧後、紙運用された情報は紙のまま保存しなければならない。</li> <li>5) ディザスターリカバリーとして予備系システムを準備していれば不要である。</li> </ol>
<p>問38 医療情報のバックアップの 3-2-1 ルールについて正しいのはどれか。</p> <ol style="list-style-type: none"> <li>1) 「1」はクラウドバックアップを指す。</li> <li>2) 「1」はオフラインバックアップを指す。</li> <li>3) 「2」は正・副のバックアップを指す。</li> <li>4) 「3」は 3 世代のバックアップを指す。</li> <li>5) 「3」は 3 種類の媒体によるバックアップを指す。</li> </ol>
<p>問39 サービスデスクが行うオペレーションでないのはどれか。</p> <ol style="list-style-type: none"> <li>1) 障害や課題の一次切り分けを行う。</li> <li>2) 障害や課題の原因を把握してシステム管理者への報告書を作成する。</li> <li>3) 障害や対応記録をデータベース化して迅速に対応する体制を構築する。</li> </ol>

<ol style="list-style-type: none"> <li>4) システム改修に向けて、コスト(費用や工数)の見積と明細内訳を作成する。</li> <li>5) システム管理者、保守ベンダーと相互に連絡を取り復旧にかかる時間を確認する。</li> </ol> <p>問 53 「医療情報システムの安全管理に関するガイドライン」(第 5.2 版)における「ブレイクグラス」の説明として適切なのはどれか。</p> <ol style="list-style-type: none"> <li>1) 通信内容を検査して、動的にポートの閉鎖・開放を制御すること。</li> <li>2) 無線 LAN のアクセスポイントで、SSID を外部から見えなくする機能のこと。</li> <li>3) ユーザーが一度認証を受けるだけで、許可されているすべての機能を利用できること。</li> <li>4) 情報システムにおいて非常時専用の ID、パスワードを準備し、使った痕跡を残すこと。</li> <li>5) 大量のサービス要求パケットを送りつけ、過大な負荷をかけて相手のサーバやネットワークを使用不能にすること。</li> </ol> <p>問54 端末がランサムウェアに感染した兆候を確認したシステム利用者が最初にとるべき行動はどれか。</p> <ol style="list-style-type: none"> <li>1) システム管理者に電話して指示を仰ぐ。</li> <li>2) 業務を続けるため別の部署の端末を借りに行く。</li> <li>3) ウイルス対策ソフトのスキャンを手動実行する。</li> <li>4) 近傍の端末で同じ現象が発生しているか確認する。</li> <li>5) 端末に接続されているネットワークケーブルを抜く。</li> </ol>
情報処理技術系 (2023 年度 医療情報技師能力検定試験)
<p>問31 情報セキュリティの 3 要素の組み合わせについて正しいのはどれか。</p> <ol style="list-style-type: none"> <li>1) 機密性 - 安全性 - 可用性</li> <li>2) 機密性 - 完全性 - 可用性</li> <li>3) 真正性 - 安全性 - 可用性</li> <li>4) 真正性 - 完全性 - 可用性</li> <li>5) 真正性 - 機密性 - 可用性</li> </ol> <p>問32 リスクマネジメントにおいてリスクを発見、確認および記録するプロセスはどれか。</p> <ol style="list-style-type: none"> <li>1) リスク対応</li> <li>2) リスク特定</li> <li>3) リスク評価</li> <li>4) リスク分析</li> <li>5) リスク保有</li> </ol> <p>問33 情報セキュリティ対策のうち、物理的対策にあたるのはどれか。</p> <ol style="list-style-type: none"> <li>1) 入退室管理</li> <li>2) アクセス権の設定</li> <li>3) セキュリティ教育</li> <li>4) ファイアウォールの設定</li> <li>5) セキュリティポリシーの策定</li> </ol> <p>問35 DoS 攻撃についての説明はどれか。</p> <ol style="list-style-type: none"> <li>1) データを改ざんする攻撃</li> <li>2) サービスを不正利用する攻撃</li> <li>3) データを不正に取得する攻撃</li> <li>4) サーバを過負荷状態にする攻撃</li> <li>5) サーバの管理者権限を奪取する攻撃</li> </ol> <p>問38 図のように攻撃者が納入業者側のシステムを介して病院の医療情報システムに侵入・攻撃することを表すのはどれか。</p>



- 1) スパイウェア
- 2) ランサムウェア
- 3) サプライチェーン攻撃
- 4) ブルートフォース攻撃
- 5) SQL インジェクション

問45 コールドスタンバイの説明はどれか。

- 1) 障害発生時に自動的にシステムを停止すること
- 2) 地理的に離れた場所にバックアップデータを保管すること
- 3) 本番系と同一構成の予備システムを停止状態で待機させること
- 4) 障害発生時には一部機能を停止し、最小限の機能を維持すること
- 5) 本番系と同一構成の予備システムを常に同期をとった状態で待機させること

問46. 情報システムの運用管理における PDCA サイクルのうち、「D」にあたるのはどれか。

- 1) 教育の実施
- 2) パフォーマンス評価
- 3) マネジメントの計画
- 4) 問題個所の是正、改善
- 5) セキュリティポリシーの見直し

問47 信頼性評価指標 RASIS において平均故障間隔(MTBF)で評価する指標はどれか。

- 1) 安全性
- 2) 可用性
- 3) 完全性
- 4) 信頼性
- 5) 保守性

問49 非意図的なシステム障害発生要因はどれか。

- 1) 機器故障
- 2) 内部不正
- 3) 不正侵入
- 4) 情報の詐取
- 5) ウイルス攻撃

表7 上級医療情報技師能力検定試験の午後 I 試験の出題例

午後 I (2021 年度 上級医療情報技師能力検定試験)

問 14 次の文章を読み、下の設問に答えよ。解答は、それぞれ 24 文字以内とすること。

- 1) 下線部①について、事象が発覚した際、「個人データの漏えい等の事象が発生した場合等の対応について」(平成 29 年個人情報保護委員会告示第1号)に基づきどのような対応を行うべきか。2 つ挙げよ。
- 2) 下線部②について、どのような技術的対策を行うべきか。
- 3) 下線部③について、どのような組織的・人的対策を行うべきか。

A 病院では、医療情報システム部門が原則として DWH を用いて、電子カルテに蓄積されたデータを抽出する作業を担っている。この病院では 5 年前に運用管理規程が定められており、実際に依頼者からの作業依頼書をもって、医療情報システム部門が作業を行い、抽出した結果をデジタルデータもしくは紙媒体で提供する運用としている。なお、提供時には、患者が特定できる情報を削除することを原則とし、依頼者からは、情報の取り扱いに関する誓約書を署名するに受領することになっている。今回、下記の事象が発生し、医療情報システム部門内でも、その対応について問題があったのではないかと検討することになった。

- 2020.09.01 医師 B より、医療情報システム部門の担当 C に口頭でデータ抽出の依頼があった。その依頼をもとに、DWH からデータ抽出を試みたが、必要とされる情報の抽出ができないことが判明した。最終的に、電子カルテのデータベースに ODBC 接続した上でデータを抽出し、CSV 形式のデータを提供した。
- 2020.11.02 医師 B が提供された①USB メモリを紛失したことが判明した。医師 B は医療情報システム部門にその旨を申告した。その後、病院としての対応が協議された。
- 2020.11.25 次のとおり、病院ホームページを通して経緯等が報告された。なお、USB メモリには当該データのみが格納されていた。

<ホームページ掲載内容>

「個人情報が含まれた USB メモリの紛失について」

本院において、患者情報を含む USB メモリ 1 本を紛失したことが判明いたしました。当該 USB メモリには、患者さんり名分の氏名、ID、医療機器に関する情報及び 3 名分の疾患名が記録されておりました。

現在のところ、情報の流出や悪用は確認されておりませんが、患者さん、御家族、関係者の皆様方には多大なる御迷惑と御心配をお掛けすることになり、心よりお詫び申し上げます。

本件につきましては、該当の患者さん御本人や御家族に対しまして、経緯を説明し、お詫びいたしました。

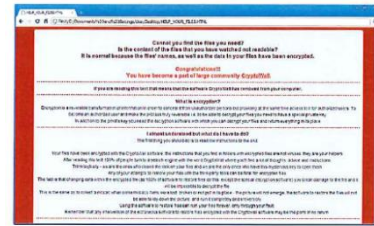
今後、②このような事態を繰り返さないよう再発防止を徹底し、皆様の信頼回復に努めてまいります。

病院長

午後 I (2022 年度 上級医療情報技師能力検定試験)

問 10 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」(経済産業省 令和2年8月)において、一律の要求事項を定めるのではなく、顕在化するリスクの内容に応じた対応方法の選択を実施する手法のことを何というか。解答は、15 文字以内で記入せよ。

問 14 電子カルテ端末を操作していたところ、突然下の画面が表示された。何が起きたと考えられるかを具体的に解答せよ。解答は、24 文字以内で記入せよ。



画面に表示されている英文 (一部)

Cannot you find the files you need?  
Is the content of the files that you have watched not readable?  
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!  
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?  
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized uses. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.  
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?  
The first thing you should do is to read the instructions to the end.

午後 I (2023 年度 上級医療情報技師能力検定試験)

問 15 Emotet のような「標的型攻撃メール」によるウイルス感染を防止するための取り組みについて、下の設問に答えよ。解答は、それぞれ 24 文字以内とする。

- 1) 医療情報部門が病院職員に対してとる人的安全対策にはどのようなものがあるか。
- 2) 各職員がメールを受信した際にとるべき具体的な行動にはどのようなものがあるか。

#### 4. 医療情報技師育成部会が実施する生涯研修・e-Learning の内容

医療情報技師・上級医療情報技師については、質の維持と向上を図るために、5年ごとの資格更新制度が設けられており、日本医療情報学会医療情報技師育成部会が実施する生涯研修セミナーを1回以上受講するほか、勉強会やe-Learningごとにポイントを設定して必要なポイントを取得することを資格更新の条件としている。このなかには情報セキュリティに関する内容を講義とグループワークの構成で取り扱うものがあり、2023年6月に大阪で開催されたセミナーには28名、2024年2月に東京で開催されたセミナーには39名の参加があった。2024年2月に開催されたセミナーのプログラム概要を表8に示す。

表8 2023年度に開催された生涯研修セミナーのプログラム概要

タイトル	みんなで議論して考える ～医療機関のサイバーセキュリティ～
日時	2024年2月25日(日)10:30～17:00
開催方法	集合形式・事前e-Learningあり・グループワークあり
会場	国立がん研究センター 築地キャンパス
受講料	10,000円(税込)
セミナー概要	本研修セミナーは、「医療情報システムの安全管理に関するガイドライン第6.0版」に基づいて、医療機関に求められる情報セキュリティについて理解し、実践的な知識や管理技術を向上させ、日常業務に役立てることを目的とするものです。
前日まで	事前e-Learning 【特別講義】医療情報システムの安全管理に関するガイドライン第6.0版を中心に 【講義1】ネットワークの計画～運用フェーズにおける基本と必須要件～ 【講義2】医療情報管理と個人情報保護のための法令・ガイドライン 【講義3】医療情報システムの情報セキュリティ対策
当日	集合形式 【講義】 医療情報システム担当者の運用フェーズにおけるセキュリティ業務 【グループワーク】 ・仮想医療機関とグループワークの進め方の説明 ・グループワーク ・グループごとの発表 ・総合討論・課題の模範的解答などの説明・質疑応答

#### 5. 医療機関の情報セキュリティ事案の担当者のなかでの医療情報技師

医療情報技師と上級医療情報技師のIPAが実施する情報処理技術者試験・情報処理安全確保支援士試験に基づく認定の取得状況について、本研究班が医療機関を対象にアンケート調査を行った結果を表9に示す。

アンケート調査に回答のあった643施設の情報セキュリティ事案の担当者の延べ人数(総数)は1,443名であった。このうち、医療情報技師(上級を含む)の資格を有するのは329名(22.8%)、上級医療情報技師の資格を有するのは40名(2.8%)であった。医療情報技師(上級を含む)のなかでは、基本情報技術者試験の認定を受けている者が47名(14.3%)で最も多く、その割合は情報セキュリティ事案の担当者の延べ人数に対する基本情報技術者試験の認定を受けている者79名(5.5%)に比べて高かった。

表9 医療機関における情報セキュリティ事案の担当者である医療情報技師(上級を含む)が認定を受けている情報処理関連の他の資格・試験

情報処理推進機構(IPA)が実施する試験・資格	情報セキュリティ事案の担当者の延べ人数	医療情報技師(上級を含む)
情報処理安全確保支援士(レベル4)	16名	9名
応用情報技術者試験(レベル3)	36名	27名
基本情報技術者試験(レベル2)	79名	47名
情報セキュリティマネジメント試験(レベル2)	34名	28名
ITパスポート(レベル1)	48名	32名
合計	1,443名	329名

#### 6. 医療情報技師の地域での活動のなかでの情報セキュリティに関する取り組み

医療情報技師・上級医療情報技師の有志が地域のなかで自発的に立ち上げて活動している



団体として地域の医療情報技師会がある。2023年度末において、北海道、関東、中部、関西、広島、岡山、四国、九州沖縄などが活動を行っていた。日本医療情報学会医療情報技師育成部会が資格更新ポイントを付与している最近の勉強会での情報セキュリティに関する取り組みの例を表10に示す。近年、多くの医療情報技師会において、情報セキュリティに関する内容を含む勉強会等を実施していた。

表10 地域の医療情報技師会の勉強会での情報セキュリティに関する最近の主なトピック・講演

北海道医療情報技師会 第17回勉強会(2023年9月23日) 「サイバーセキュリティの脅威に対してどのような対応があるか。」
関東医療情報技師会 第33回勉強会(2023年5月20日) 「ランサムウェア対策を意識したバックアップのあり方について」
中部医療情報技師会 第20回研究会(2024年2月17日) 「今、病院に必要なサイバーセキュリティ対策」
静岡県医療情報技師会 第13回勉強会(2023年12月9日) 「医療機関に求められるセキュリティ対策について」
関西医療情報技師会 第40回勉強会(2022年1月22日) 「狙われる病院医療情報システム～ランサムウェアへの対応～」
岡山県医療情報技師会 第15回研修会(2023年9月9日) 「医療情報システムの安全管理ガイドラインの改定と医療法の改正－医療情報技師に求められる役割とは－ほか」
広島県医療情報技師会 第32回研修会(2022年5月21日) 「サイバー犯罪に狙われる医療機関～コロナ禍における標的型攻撃への備え～」
四国医療情報技師会 第11回勉強会(2023年2月25日) 「サイバー攻撃に対するセキュリティ対策と初動」
九州沖縄医療情報技師会 第22回勉強会(2023年12月16日) 「医療法改正・ガイドライン改定と医療DX」、「医療機関におけるサイバーセキュリティの取り組み～病院立ち入り検査を受けてわかったこと～」、「医療業界を取り巻くサイバー犯罪の現状とその防御」

#### D. 考察

保健医療系国家資格については、それぞれの資格について定めた法令のなかで、試験にすることが示されている。各養成校は指定規則等に従って開講する授業科目を設定しており、各科目の教育内容の詳細については国家試験の出題範囲や過去の国家試験での出題実績などを参考にしながら作成しているものと考えられる。今回、国家試験の出題基準と出題実績から情報セキュリティに関する医療系専門職の教育状況を調査した結果、臨床工学技師、診療

放射線技師、臨床検査技師について、情報セキュリティに関する内容が出題基準に含まれており、養成校のなかである程度の基礎的な教育が行われていることもと考えられる。一方、その他の職種については個人情報保護などについては教育を行っているものの、情報セキュリティに関する技術的な教育はほとんど行われていないことが示唆された。

日本医療情報学会では2003年から20年以上にわたり、医療情報に関する専門職として医療情報技師等の育成が行われてきた。医療情報技師および上級医療情報技師の人材像が示す範囲は、情報セキュリティに留まらないものの、その教育カリキュラムには、医療機関における情報セキュリティの実践、つまり保健医療福祉分野の特性や診療業務の実際を理解しながら情報セキュリティへの対応を効果的に行っていくために必要となる知識・技術が体系的にまとめられていた。過去の医療情報技師能力検定試験と上級医療情報技師能力検定試験においては、情報セキュリティに関する問題が保健医療系国家資格の国家試験と比べて、遥かに多く出題されていた。そのなかには、医療情報システムの運用担当者として知っておくべき、個人情報の取り扱い、厚生労働省の医療情報システムの安全管理に関するガイドラインなどについての出題が含まれ、具体的なインシデントの事例等も示してどのような問題や解決策があるかを問うような実践的な設問も含まれていた。また、上級医療情報技師能力検定試験の問題には一般的な医療機関の組織構造、システム構成や業務フローを理解したうえで解くような、実践的な問題が含まれていた。これらの内容は、情報セキュリティの専門家には至らないまでも医療機関でサイバーセキュリティインシデントが発生した場合の初動対応に必要な

内容であると考えられる。

情報セキュリティへの対応を充実させるにあたっては、独立行政法人情報処理推進機構（IPA）が提唱する「本来の業務を担いながらITを利活用する中でセキュリティスキルも必要となる『プラス・セキュリティ人材』」の考え方に基づく育成と配置が現実的であると考えられる。医療機関においては、平常時の対応として医療情報システムの運用管理のなかで、日々巧妙化・複雑化するサイバー攻撃の脅威への対応、医療従事者への「プラス・セキュリティ」の教育・研修を行っていくことが考えられる。また、有事の際には診療業務の継続に向けた経営層や診療科・部門との情報共有や適切な判断などを行いながら、サイバーセキュリティ専門業者と自施設の橋渡しを行っていくことが求められる。これらのことを行うことができる人材として、保健医療系国家資格を有する医療系専門職や医療機関の事務職などの既存の人的資源や教育の仕組みを活用し、必要なセキュリティスキルを身につけた情報セキュリティ人材の育成を進めていく必要があるだろう。

医療機関を対象にしたアンケート調査結果から、医療機関に勤務する情報セキュリティ事案の担当者には、医療情報技師（上級を含む）を有する者が多く、医療機関における配置が進みつつあることが示唆された。また、そのなかにはIPAの情報処理技術者試験の認定を受ける者も比較的多いことがわかった。医療機関において情報セキュリティのリスクに対応できるようになるためには、1) 現場の業務フローを理解している、2) 現場でリーダーシップを発揮できる、3) 現場のマネジメントができる、4) 情報セキュリティに関するリスク分析を行うことができる、5) 情報セキュリティに関するインシデントに即応できることが求められ

る。情報処理技術の知識・技術を有する人材として、診療現場に精通する既存人材として医療情報技師を有効に活用していくとともに、サイバーセキュリティに関する知識や演習・訓練などに関してはIPAなどの専門機関と協力すること、安全な地域医療の継続性確保に資する医療機関の情報セキュリティ人材として活用できる可能性が高いことが示唆され、そのことを踏まえて人材の育成と配置を進めていくことが最も迅速かつ効率的であると考えられる。

## E. 結論

情報セキュリティに関する医療系専門職の教育状況について、保健医療関係の国家資格の出題基準および出題実績を調査した結果、幾つかの職種については、情報セキュリティに関する基礎的な内容が教育カリキュラムに含まれるが、職種と内容のいずれも限定的であった。

医療情報技師については、日本医療情報学会が20年以上にわたって継続して育成に取り組んでおり、医療機関における情報セキュリティの実践に必要な知識・技術が教育カリキュラムのなかに体系的にまとめられていた。医療情報技師については、既に2万5千名以上の認定者を輩出されており、また質の担保のための資格更新の取り組みや、資格取得者による地域のなかでの自発的な取り組みなどが行われていた。

安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置を限られた医療資源のなかで行っていくための方策として、既に医療機関における配置が進みつつある人的資源や基礎的な教育を受けた人材に対して、既に確立している教育の仕組みをうまく活用して育成していくことが効果的かつ効率的であることが示唆された。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

なし

### 2. 学会発表

谷川琢海. 診療業務を理解したセキュリティ人材の育成に向けて, 第 43 回医療情報学連合大会 (神戸), 2023 年 11 月.

## H. 知的財産権の出願・登録状況

(予定を含む。)

### 1. 特許取得

なし

### 2. 実用新案登録

なし

### 3. その他

テーマ:情報セキュリティに対する医療系専門職(診療放射線技師)の教育状況の調査

研究分担者 川真田 実 大阪府立病院機構国際がんセンター 放射線診断・IVR科 副技師長

#### 研究要旨

情報セキュリティに関する業務を担う可能性がある医療系専門職として、診療放射線技師の情報セキュリティに関する教育について調査を行った。診療放射線技師国家試験出題基準には、医療画像情報学と医療安全管理学が含まれており、診療放射線技師学校養成所指定規則にて定められている単位数は医療画像情報学が6単位で全体の5.9%、医療安全管理学が2単位で0.2%となっている。これにより、診療放射線技師には情報セキュリティ対策に関する一定の教育が行われ、ある程度の素養を持っていると言える。しかしながら、診療放射線技師という職業の性質上、基礎医学分野をはじめとする検査や治療等の教育が中心であるため、情報セキュリティに関する教育は基礎的な内容に留まる。そのため、卒後ある程度の実務経験を経た後に、追加の教育や資格を取得することで院内における情報セキュリティ担当者になり得ると考える。

#### A. 研究目的

安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究では、安全・安心な地域医療を継続的に維持確保するために必要な保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とし、関係する省庁・学会・業界団体等と連携しながら調査・試作・検証・評価等を行うことをも目的としている。

本研究班では、研究開始当初、情報セキュリティに関する業務を担う可能性のある医療系専門職として、医療情報技師、診療放射線技師、臨床工学技士を想定した。本報告では、診療放射線技師の情報セキュリティに関する教育状況について、調査することを目的とした。

#### B. 研究方法

##### 1. 診療放射線技師の情報セキュリティに関する

#### る教育状況の調査

診療放射線技師について、診療放射線技師養成所指定規則(昭和二十六年文部省・厚生省令第四号)をはじめ、診療放射線技師国家試験出題基準や実際に教育現場で利用されている教科書を用いて教育状況の調査を行った。

#### C. 研究結果

##### 1. 診療放射線技師の情報セキュリティに関する教育状況の調査

診療放射線技師になるには、厚生労働省が管轄する国家試験に合格し、診療放射線技師免許を得る必要がある。大学(4年制)、短期大学(3年制)、専門学校(昼間3年制・夜間4年制)など、国が指定した診療放射線技師教育機関にて規定の時間数を習得することで試験の受験資格を得ることができる。現在、3年制教育機関は4年制への移行が進んでおり、4年制大学が年々増加傾向にある。

診療放射線技師養成所指定規則第二条三に定められている教育内容は、基礎分野・専門

基礎分野・専門分野の3つから構成されている。基礎分野14単位、専門基礎分野31単位、専門分野57単位、合計102単位が義務づけられている。情報セキュリティ教育としては専門分野に医療画像情報学6単位、医療安全管理学2単位が定められている。

医療情報学では、情報処理学、医療画像、医療情報の3つの細項目が設けられている。情報処理学の領域では、情報の表現、論理回路、およびコンピュータと情報処理の基礎について学ぶ。論理回路では論理素子、論理演算、論理回路の構造を学び、さらに、コンピュータと情報処理の基礎として、ハードウェア、ソフトウェア、ネットワーク、情報処理システムの構成、そして情報セキュリティに関する知識を学ぶカリキュラムが構成されている。また、医療情報の領域では、DICOMやHL7といった標準規格、病院情報システム(HIS)や放射線情報システム(RIS)や医療画像情報管理システム(PACS)などの医療情報システム、さらには、個人認証および資格管理、個人情報保護とプライバシー、画像表示モニタの品質管理など、情報セキュリティに関する知識を含む医療情報システムの安全管理のための基礎的な知識を習得できるカリキュラムとなっている。

また、医療安全管理学では医療安全の基礎、放射線診療の安全管理、医療機器および機器の安全管理、医薬品の安全管理、救急医療、診療の補助行為に関する安全管理の6つの細項目から構成されている。放射線診療の安全管理では、個人情報保護として個人情報の管理やセキュリティ対策について学び、医療機器および器具の安全管理では医療機器の安全な使用についてのカリキュラムが設けられている。

これらのカリキュラムについては国家試験の出題範囲としても設定されており、診療放射線

技師が情報に関する一定の知識を備え、最低限の情報セキュリティに関する知識を持っているという事が分かる。しかしながら、教育期間中に情報セキュリティ対策の全てを学習することは厳しいと考えられた。

診療放射線技師の試験については、過去5年間に情報セキュリティ対策に関する問題は2問出題されていた。

## 2. 診療放射線技師の情報セキュリティに関する卒業教育状況の調査

卒業後の診療放射線技師に対して、日本放射線技術学会や日本診療放射線技師会等の団体によって構成される専門技師制度が存在する。本専門技師制度には日本医用画像情報専門技師共同認定育成機構(社員は日本医療情報学会と日本放射線技術学会の2団体)が参画しており、医用画像情報専門技師の認定を行っている。

医用画像情報専門技師は、医療情報技師の能力を礎に、医用画像の高度な知識と豊かな経験を備えています。医用画像領域において企画立案、構築、運営、利活用などの様々な場面で医療の質を担保し向上させるためのマネジメントを行う専門技師と定義されている。最低限習得すべき技術・知識として情報セキュリティが含まれている。認定制度が開始された2010年から298名の方が認定されている。

また、専門技師のスキルアップを目的として、対面型セミナーやディスカッション型のセミナーが開催されている。ここ数年ではサイバーセキュリティ対策や医療情報システムの安全管理のガイドラインの解説、医療機関におけるサイバーセキュリティ対策をチェックリストを用いて考察する内容が取り上げられている。

## D. 考察

診療放射線技師の教育カリキュラムは診療放射線技師養成所指定規則第二条三に定められており、国家試験においても本教育カリキュラムが出題範囲として定義されている。本カリキュラムの中で情報セキュリティに対する教育は、総論的で基本的な内容にとどまった。診療放射線技師の国家試験を取得した時点で、医療機関の情報セキュリティ対策の即戦力になるとは言いが、医療情報学に関する一定のカリキュラムが備わっていることから、医療情報システムの特性を理解し、情報セキュリティ対策を担う素養を持った人材であると言える。

診療放射線技師という職業の性質上、CT 検査や MRI 検査、放射線治療などの実務経験を一定期間積むことが求められます。しかし、高額な医療機器の導入やデータフローの確立、そしてその利活用までを体系的に取り組むために、医用画像情報専門技師の資格取得に取り組む技師が一定数存在し、情報セキュリティに関する知識の習得に非常に前向きである事が分かった。今後、このような方々が追加の実地教育やより専門的な資格を取得することで、病院内において情報セキュリティを担う人材となる可能性があると考えられる。

## E. 結論

診療放射線技師の教育カリキュラムとして、医療画像情報学と医療安全管理学が整備されており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。一方情報セ

キュリティに対する教育は、総論的、基本的な内容にとどまり、情報セキュリティ対策の実務を担うには、追加の教育や資格、試験の保有が必要であると考えられた。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

川真田 実. 医療機器サイバーセキュリティに備える ～海外における現状と課題～, 日本診療放射線技師会誌 2023 年 70 巻 846 号 p.399-405

### 2. 学会発表

(1) 川真田 実. ランサムウェア被害に遭うということ, 日本放射線技術学会 九州支部講演会, 2023 年 9 月. 福岡

(2) 医用画像部門におけるセキュリティ対策. 坂本博, 木村通男, 原瀬正敏, 谷祐児, 坂野隆明, 川真田実 第 43 回医療情報学連合大会共同企画 5, 2023 年 11 月. 神戸

## H. 知的財産権の出願・登録状況

(予定を含む。)

### 1. 特許取得

なし

### 2. 実用新案登録

なし

### 3. その他

なし

テーマ:情報セキュリティに対する医療系専門職(臨床工学技士)の教育状況の調査

研究分担者 肥田 泰幸 東都大学 幕張ヒューマンケア学部臨床工学科 助教

#### 研究要旨

情報セキュリティに関する業務を担う可能性がある医療系専門職として臨床工学技士の情報セキュリティに関する教育について調査を行った。臨床工学技士の教育カリキュラムとして、臨床工学に必要な医療情報システムとシステム工学の基礎が整備されており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。一方情報セキュリティに対する教育は、総論的、基本的な内容にとどまるが、公益財団法人日本臨床工学技士による人材育成計画や国際医療機器規制当局のガイダンス導入による情報セキュリティ対策強化の必然性から、今後充実が図られるものと考えられる。

#### A. 研究目的

安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究では、安全・安心な地域医療を継続的に維持確保するために必要な保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とし、関係する省庁・学会・業界団体等と連携しながら調査・試作・検証・評価等を行うことをも目的としている。

本研究班では、研究開始当初、情報セキュリティに関する業務を担う可能性のある医療系専門職として、医療情報技師、診療放射線技師、臨床工学技士を想定した。本報告では、臨床工学技士の情報セキュリティに関する教育状況について、調査することを目的とした。

#### B. 研究方法

##### 1. 臨床工学技士の情報セキュリティに関する教育状況の調査

臨床工学技士について、厚生労働省、公益社団法人日本臨床工学技士会、一般社団法人

人日本医療機器産業連合会、一般社団法人日本臨床工学技士施設協議会の Web 情報を用いて教育状況の調査を行った。

#### C. 研究結果

##### 1. 臨床工学技士の情報セキュリティに関する教育状況の調査

臨床工学技士になるには、厚生労働省が管轄する国家試験に合格し、臨床工学技士免許を得る必要がある。大学(4年制)、短期大学(3年制)、専門学校(3年制)、医療系国家資格者(看護師、臨床検査技師など)養成校や大学、短期大学で2年以上修業し、厚生労働大臣の指定する科目を収めた者など、国が指定した臨床工学技士教育機関にて規定の時間数を習得することで試験の受験資格を得ることができる。現在、北海道6校、東北3校、関東26校、中部11校、近畿18校、中国9校、四国4校、九州15校の計92校の臨床工学技士養成校があり、文部科学省先導的の大学改革推進委託事業(医工連携教育)の影響により、さらに新設校が増加傾向にある。

臨床工学技士学校養成所指定規則(昭和63年文部省・厚生省令第2号。以下「指定規

則」という。)第4条においては、文部科学大臣及び都道府県知事が行う臨床工学技士法(昭和62年法律第60号)第14条第1号から第3号までに規定する学校又は臨床工学技士養成所の指定に係る基準について定めており、基礎分野・専門基礎分野・専門分野の3つから構成されている。基礎分野14単位、専門基礎分野38単位、専門分野49単位、合計101単位が義務づけられている。情報セキュリティ教育としては専門基礎分野に臨床工学に必要な医療情報システムとシステム工学の基礎として7単位が定められている。

臨床工学に必要な医療情報システムとシステム工学の基礎では、必修科目として1.情報科学概論、2.情報リテラシー、3.システム工学基礎、4.情報処理技術基礎、5.医療情報処理技術、6.医療情報システム、7.情報通信ネットワーク、8.医療用IoT概論が、選択科目として、1.パソコン基礎演習、2.医療情報処理技術演習、3.医療情報システム演習、4.医用画像処理情報技術、5.人工知能が設けられ、医療情報システムの特性や医療機器との情報連携、情報リテラシーや情報通信ネットワークに加えて、実技による医療情報処理技術演習、医療情報システム演習によって情報セキュリティに関する知識を学習することができるカリキュラムが構成されている。一方、情報セキュリティ対策については、総論的、基礎的な内容となっており、臨床工学技士の教育コンテンツで、情報セキュリティ対策のすべてを学習することは難しいと考えられた。

診療情報管理士の試験については、過去5年間に情報セキュリティ対策に関する問題は7問出題されていた。

公益社団法人日本臨床工学技士会では、サイバーセキュリティに関して世論に広く注意を

促す啓発動画の公開やIPA独立行政法人情報処理推進機構が実施する各種国家試験や一般社団法人日本医療情報学会が実施する医療情報技師能力検定試験の受験を支援する「ICT分野の国家資格等取得における奨励金制度」を実施している。

近年は、ソフトウェアや通信機能を搭載している医療機器も増加しており、厚生労働省が国際医療機器規制当局(IMDRF)によって進められるガイダンスの導入に向け検討を進め、そのガイダンスの技術基準などを明確化した『製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」』を2021年12月に発表している。

#### D. 考察

臨床工学技士の教育カリキュラムとして、臨床工学に必要な医療情報システムとシステム工学の基礎が整備されているが、情報セキュリティに対する教育は、総論的、基本的な内容にとどまった。現時点では臨床工学技士国家資格取得によって、医療機関の情報セキュリティ対策の即戦力になるとは言い難いが、国際医療機器規制当局(IMDRF)のガイダンス導入によって医療機関における医療機器のサイバーセキュリティ対策が強化され、公益財団法人日本臨床工学技士によるICT分野の国家資格等取得における奨励金制度によって人材育成が進んでいくものと思われる。臨床工学技士は養成機関によって、情報セキュリティに対する基本的な教育が実施されていることに加え、公益財団法人日本臨床工学技士による人材育成計画によって、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。

また、情報セキュリティ対策がと医療機器の保守管理が脆弱とされる中小の医療機関に、



臨床工学技士が介入することによって、医療情報システム安全管理責任者と医療機器安全管理責任者の一人二役を担うことが出来れば、医療経営の面においても貢献できると考える。

## E. 結論

臨床工学技士の教育カリキュラムとして、臨床工学に必要な医療情報システムとシステム工学の基礎が整備されており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。一方情報セキュリティに対する教育は、総論的、基本的な内容にとどまり、情報セキュリティ対策の実務を担うには、追加の教育や資格、試験の保有が必要であるが、公益財団法人日本臨床工学技士による人材育成計画や国際医療機器規制当局のガイダンス導入による情報セキュリティ対策強化の必然性から、今後充実が図られるものと考ええる。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

なし

### 2. 学会発表

(1) 肥田泰幸、サイバーセキュリティと医療安全、第29回日本臨床工学会、2019年5月、岩手

(2) 肥田泰幸、臨床工学技士の医療情報とセキュリティの関わり、第31回広島県医療情報技師研修会、2022年1月、広島

(3) 肥田泰幸、サイバーセキュリティの現状と対策、第68回日本透析医学会学術総会、2023年6月、横浜

## H. 知的財産権の出願・登録状況

(予定を含む。)

### 1. 特許取得

なし

### 2. 実用新案登録

なし

### 3. その他

なし

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

テーマ:情報セキュリティに関する業務を担う可能性のある医療系専門職の調査

研究代表者 武田理宏 国立大学法人大阪大学大学院医学系研究科 医療情報学 教授  
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  
研究分担者 川真田 実 大阪府立病院機構国際がんセンター 放射線診断・IVR科 副技師長  
研究分担者 肥田 泰幸 東都大学 幕張ヒューマンケア学部臨床工学科 助教  
研究協力者 吉川 肇 一般社団法人日本病院会 事業部 部長

研究要旨

本研究班では、研究開始当初、情報セキュリティに関する業務を担う可能性のある医療系専門職として、医療情報技師、診療放射線技師、臨床工学技士を想定した。本研究では、他に情報セキュリティに関する業務を担う可能性がある医療系専門職を研究班内で議論を行い、対象となった専門職の教育カリキュラムについて、調査を行った。

情報セキュリティに関する業務を担う可能性がある医療系専門職として診療情報管理士が候補として挙げられた。診療情報管理士の教育カリキュラムとして、医療情報システムと情報セキュリティが整備されており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。一方情報セキュリティに対する教育は、総論的、基本的な内容にとどまり、情報セキュリティ対策の実務を担うには、追加の教育や資格、試験の保有が必要であると考えられた。

A. 研究目的

安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究では、安全・安心な地域医療を継続的に維持確保するために必要な保健医療福祉分野の特性を理解した情報セキュリティ人材の育成とキャリア形成、適材配置、協働体制整備に必要な教育カリキュラム、キャリアデザイン、適材配置計画、協働体制制度等の策定を目的とし、関係する省庁・学会・業界団体等と連携しながら調査・試作・検証・評価等を行うことをも目的としている。

本研究班では、研究開始当初、情報セキュリティに関する業務を担う可能性のある医療系専門職として、医療情報技師、診療放射線技師、臨床工学技士を想定した。本研究では、他に情報セキュリティに関する業務を担う可能性が

ある医療系専門職を研究班内で議論を行い、対象となった専門職について、情報セキュリティに関する教育状況について、確認することを目的とした。

B. 研究方法

1. 情報セキュリティに関する業務を担う可能性がある医療系専門職

情報セキュリティに関する業務を担う可能性がある医療系専門職について、研究班内で議論と情報セキュリティ人材に関するアンケート調査から、候補となる医療系専門職を決定した。

2. 候補となった医療系専門職の情報セキュリティに関する教育状況の調査

候補となった医療系専門職について、Webや教科書を用いて教育状況の調査を行った。

## C. 研究結果

### 1. 情報セキュリティに関する業務を担う可能性がある医療系専門職

研究班で情報セキュリティに関する業務を担う可能性がある医療系専門職について議論を行った。診療情報管理士は医療機関の診療記録を管理しており、電子カルテの普及により、電子カルテの特性を理解している人材が多ことから、情報セキュリティを担う人材と候補と考えた。そこで、診療情報管理士を企画、運営している一般社団法人日本病院会に研究協力依頼を行い、承諾をいただいた。研究班では、診療情報管理士の他に、候補となる医療系専門職は挙がらなかった。

情報セキュリティ人材配置に関するアンケート調査を行い(分担研究報告、情報セキュリティ人材配置に関するアンケート調査参照)、他に候補となる医療系専門職がないか検討した。

アンケート調査は Web 形式で行われ、643 施設から回答が得られた。回答施設で、医療情報システム安全管理責任者(521 名)が保有する医療系国家資格は、医師・歯科医師が 267 名、看護師・助産師・保健師が 2 名、薬剤師が 5 名、診療放射線技師が 8 名、臨床検査技師が 5 名、臨床工学技士が 5 名、その他が 8 名であった。医療情報システムの情報セキュリティ事案の担当者が保有する国家資格は、医師・歯科医師が 23 名、看護師・助産師・保健師が 15 名、薬剤師が 5 名、診療放射線技師が 13 名、臨床検査技師が 9 名、臨床工学技士が 3 名、その他が 18 名であった。

診療情報管理士は、医療情報システム安全管理責任者 521 名のうち 30 名、医療情報システムの情報セキュリティ事案の担当者 922 名のうち 119 名、合計 149 名が保有しており、情報

セキュリティに関する業務を担う可能性がある医療系専門職として検証する必要があることが確認された。

### 2. 診療情報管理士の情報セキュリティに関する教育状況の調査

診療情報管理士は、日本病院会通信教育および日本病院会認定専門学校、大学にて統一されたカリキュラムで養成されており、四病院団体協議会(日本病院会、全日本病院協会、日本医療法人協会、日本精神科病院協会)および医療研修推進財団の共同で認定された資格である。

日本病院会診療情報管理士教育委員会が策定した通信教育カリキュラムは、基礎 12 科目、専門 12 科目、合計 24 科目で構成されている。専門科目の 1 科目として、保健医療情報学が自習時間 17 時間、授業 3 時間の 2 単位が定められている。

日本病院会診療情報管理士教育委員会策定の養成テキストでは、保健医療情報学の項目として、医療情報システムと情報セキュリティが設けられている。医療情報システムでは、1. 医療情報システムとは、2. 病院情報システム概論、3. 部門の業務を支える情報システム、4. オーダエントリーシステム、5. 電子カルテシステム 6. 地域医療情報システムの細項目が設けられ、医療情報システムの特長や多施設での医療情報連携を学習することができるコンテンツとなっている。情報セキュリティでは、1. 診療情報の安全管理、2. 医療情報システムにおけるセキュリティ対策、3. 医療情報システムの安全管理に関するガイドライン、4. 医療情報システムの安全管理、5. 診療情報管理士として実践すべき事項が細項目として設けられ、情報セキュリティ担保に向けたガイドラインの把握や情報セキュリティ対

策が学習できるコンテンツとなっている。一方、情報セキュリティ対策については、総論的、基礎的な内容となっており、診療情報管理士の教育コンテンツで、情報セキュリティ対策のすべてを学習することは難しいと考えられた。

#### D. 考察

情報セキュリティに関する業務を担う可能性がある医療系専門職として、上級医療情報技師、医療情報技師、診療放射線技師、臨床工学技士に加え、診療情報管理士が候補として挙げられた。

診療情報管理士の教育カリキュラムとして、医療情報システムと情報セキュリティが整備されているが、情報セキュリティに対する教育は、総論的、基本的な内容にとどまった。診療情報管理士取得時点で、医療機関の情報セキュリティ対策の即戦力になるとは言い難いが、医療情報システムの特徴を理解し、情報セキュリティの基本的な知識を有しており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。

診療情報管理士が情報セキュリティに対する資格・試験を受けることや、e-learning や実地教育などの教育を追加で受けることで、医療機関の情報セキュリティを担う良い人材となる。

実際に、医療情報セキュリティ人材の配置に関するアンケート調査では、医療情報システム安全管理責任者につく診療情報管理士は 30 名おり、上級医療情報技師が 4 名 (13%)、医療情報技師 13 名 (43%)、情報処理安全確保支援士が 1 名 (3%)、応用情報技術者試験が 1 名 (3%)、基礎情報技術者試験が 3 名 (10%)、情報セキュリティマネジメント試験が 7 名 (23%)、IT パスポートが 4 名 (13%)、資格、試験を有していた。また、医療情報システムの情報セキュリ

ティ事案担当者につく診療情報管理士は 119 名おり、上級医療情報技師が 4 名 (3%)、医療情報技師 29 名 (24%)、情報処理安全確保支援士が 2 名 (2%)、応用情報技術者試験が 7 名 (6%)、基礎情報技術者試験が 9 名 (8%)、情報セキュリティマネジメント試験が 6 名 (5%)、IT パスポートが 8 名 (7%)、資格、試験を有していた。各資格、試験の保有率は全体に対して著しく高く、診療情報管理士がこれらの資格、試験を用いて情報セキュリティ対策の知識を獲得し、業務に活かしている状況を確認することができた。

医療機関で情報セキュリティ対策に関わる診療情報管理士の 28%が医療情報技師の資格を保有していた。医療情報技師と診療情報管理士は相性の良い資格で、医療情報技師の資格の取得を推奨している診療情報管理士の教育指定校も少なくない。医療情報技師の教育カリキュラムを活用しながら、診療情報管理士の情報セキュリティ教育を行っていく方法が想定される。

日本病院協会の診療情報管理士の通信教育には、DPC コース、腫瘍学分類コース、医師事務作業補助者コースといった専門分野に特化したコースが作られている。情報セキュリティ対策に従事する診療情報管理士を育成するために、情報セキュリティコースを独自に作ることも想定される。

情報セキュリティ対策に関わる教育コンテンツの作成には一定の労力が必要であるため、各医療系専門職が協力をしながら、教育環境を整備していく必要があると考えられる。

#### E. 結論

情報セキュリティに関する業務を担う可能性がある医療系専門職として、上級医療情報技

師、医療情報技師、診療放射線技師、臨床工学技士に加え、診療情報管理士が候補として挙げられた。

診療情報管理士の教育カリキュラムとして、医療情報システムと情報セキュリティが整備されており、医療機関の情報セキュリティ対策を担う素養を持った人材であると言える。一方情報セキュリティに対する教育は、総論的、基本的な内容にとどまり、情報セキュリティ対策の実務を担うには、追加の教育や資格、試験の保有が必要であると考えられた。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

(1) 武田 理宏、サイバーインシデント対策と医療安全、医療安全推進ジャーナル 73, 10-15, 2023

### 2. 学会発表

(1) 武田 理宏、医療機関に求められる医療情報人材とは、日本医療情報学会関西支部会、2023 年度第 1 回講演会、2023 年 10 月、大阪

(2) 医療分野のセキュリティ人材の育成をどうするか、第 43 回医療情報学連合大会シンポジウム、2023 年 11 月、神戸、(座長：武田 理宏、谷川 琢海)

① 武田 理宏、医療機関における情報セキュリティ人材の育成と配置に向けて

② 岡本 潤(厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室)、厚生労働省における医療機関の情報セキュリティの強化に向けた取り組み

③ 大道 道大(大道会 森之宮病院)、病院の ICT の変遷と医療情報システムの人材確保について

④ 奥村 明俊(情報処理推進機構(IPA))サイバーセキュリティ人材育成に関する IPA の取り組み

⑤ 谷川 琢海、診療業務を理解したセキュリティ人材の育成に向けて

(3) みんなでつくるセキュリティの医療現場改革に向けて 情報共有体制の重要性、第 43 回医療情報学連合大会産学官連携企画、2023 年 11 月、神戸、(座長：武田 理宏、並川 寛和

(保健医療福祉情報システム工業会(JAHIS))

① 新畑 覚也(厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室)、医療分野におけるサイバーセキュリティ対策の厚生労働省の取組について

② 谷川 琢海、医療情報技師の観点からの医療分野の ISAC の必要性

③ 大谷 俊介(誠馨会 千葉中央メディカルセンター)、医療分野における医療機関関係者・医療従事者を中心とした ISAC 設立に向けた検討

④ 洞田 慎一(JPCERT コーディネーションセンター)、ISAC 等で使用するサイバーセキュリティに関連する情報共有ツール SIGNAL に関して

## H. 知的財産権の出願・登録状況

(予定を含む。)

### 1. 特許取得

なし

### 2. 実用新案登録

なし

### 3. その他

なし

研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
武田 理宏	サイバーインシデント対策と医療安全	医療安全推進ジャーナル	73	10-15	2023
川真田 実	医療機器サイバーセキュリティに備える ～海外における現状と課題～	日本診療放射線技師会誌	70 (846)	399-405	2023

厚生労働大臣 殿

機関名 国立大学法人大阪大学

所属研究機関長 職 名 大学院医学系研究科長

氏 名 熊ノ郷 淳

次の職員の令和5年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1. 研究事業名 地域医療基盤開発推進研究事業
2. 研究課題名 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究
3. 研究者名 (所属部署・職名) 大学院医学系研究科・教授  
(氏名・フリガナ) 武田 理宏 ・ (タケダ トシヒロ)

## 4. 倫理審査の状況

	該当性の有無		左記で該当がある場合のみ記入 (※1)		
	有	無	審査済み	審査した機関	未審査 (※2)
人を対象とする生命科学・医学系研究に関する倫理指針 (※3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
遺伝子治療等臨床研究に関する指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
その他、該当する倫理指針があれば記入すること (指針の名称: )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

(※1) 当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

## その他 (特記事項)

(※2) 未審査に場合は、その理由を記載すること。

(※3) 廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

## 5. 厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 <input checked="" type="checkbox"/> 未受講 <input type="checkbox"/>
-------------	---

## 6. 利益相反の管理

当研究機関におけるCOIの管理に関する規定の策定	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究機関におけるCOI委員会設置の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合は委託先機関: )
当研究に係るCOIについての報告・審査の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究に係るCOIについての指導・管理の有無	有 <input type="checkbox"/> 無 <input checked="" type="checkbox"/> (有の場合はその内容: )

(留意事項) ・該当する□にチェックを入れること。  
・分担研究者の所属する機関の長も作成すること。

厚生労働大臣  
—(国立医薬品食品衛生研究所長)— 殿  
—(国立保健医療科学院長)—

機関名 国立大学法人群馬大学

所属研究機関長 職 名 学長

氏 名 石崎 泰樹

次の職員の令和5年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1. 研究事業名 地域医療基盤開発推進研究事業
2. 研究課題名 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究
3. 研究者名 (所属部署・職名) 医学部附属病院・准教授  
(氏名・フリガナ) 鳥飼 幸太 (トリカイ コウタ)

## 4. 倫理審査の状況

	該当性の有無		左記で該当がある場合のみ記入 (※1)		
	有	無	審査済み	審査した機関	未審査 (※2)
人を対象とする生命科学・医学系研究に関する倫理指針 (※3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
遺伝子治療等臨床研究に関する指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
その他、該当する倫理指針があれば記入すること (指針の名称: )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

(※1) 当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

## その他 (特記事項)

(※2) 未審査の場合は、その理由を記載すること。

(※3) 廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

## 5. 厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 <input checked="" type="checkbox"/> 未受講 <input type="checkbox"/>
-------------	---

## 6. 利益相反の管理

当研究機関におけるCOIの管理に関する規定の策定	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究機関におけるCOI委員会設置の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合は委託先機関: )
当研究に係るCOIについての報告・審査の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究に係るCOIについての指導・管理の有無	有 <input type="checkbox"/> 無 <input checked="" type="checkbox"/> (有の場合はその内容: )

(留意事項) ・該当する□にチェックを入れること。  
・分担研究者の所属する機関の長も作成すること。



厚生労働大臣 殿

機関名 北海道科学大学

所属研究機関長 職名 学長

氏名 川上 敬

次の職員の令和5年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1. 研究事業名 地域医療基盤開発推進研究
2. 研究課題名 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究
3. 研究者名 (所属部署・職名) 北海道科学大学・准教授  
(氏名・フリガナ) 谷川 琢海 (タニカワ タクミ)

## 4. 倫理審査の状況

	該当性の有無		左記で該当がある場合のみ記入 (※1)		
	有	無	審査済み	審査した機関	未審査 (※2)
人を対象とする生命科学・医学系研究に関する倫理指針 (※3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
遺伝子治療等臨床研究に関する指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
その他、該当する倫理指針があれば記入すること (指針の名称: )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

(※1) 当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

## その他 (特記事項)

(※2) 未審査に場合は、その理由を記載すること。

(※3) 廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

## 5. 厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 <input checked="" type="checkbox"/> 未受講 <input type="checkbox"/>
-------------	---

## 6. 利益相反の管理

当研究機関におけるCOIの管理に関する規定の策定	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究機関におけるCOI委員会設置の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合は委託先機関: )
当研究に係るCOIについての報告・審査の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究に係るCOIについての指導・管理の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (有の場合はその内容: )

(留意事項) ・該当する□にチェックを入れること。  
・分担研究者の所属する機関の長も作成すること。

令和6年4月1日

厚生労働大臣  
—(国立医薬品食品衛生研究所長) 殿  
—(国立保健医療科学院長) 殿

機関名 地方独立行政法人大阪府立病院機構  
大阪国際がんセンター

所属研究機関長 職 名 総長

氏 名 松浦 成昭

次の職員の令和5年度厚生労働行政推進調査事業費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1. 研究事業名 地域医療基盤開発推進研究事業
2. 研究課題名 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究
3. 研究者名 (所属部署・職名) 放射線診断・IVR科・副技師長  
(氏名・フリガナ) 川真田 実・カワマタ ミノル

#### 4. 倫理審査の状況

	該当性の有無		左記で該当がある場合のみ記入 (※1)		
	有	無	審査済み	審査した機関	未審査 (※2)
人を対象とする生命科学・医学系研究に関する倫理指針 (※3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
遺伝子治療等臨床研究に関する指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
その他、該当する倫理指針があれば記入すること (指針の名称: )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

(※1) 当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

#### その他 (特記事項)

(※2) 未審査の場合は、その理由を記載すること。

(※3) 廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

#### 5. 厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 <input checked="" type="checkbox"/> 未受講 <input type="checkbox"/>
-------------	---

#### 6. 利益相反の管理

当研究機関におけるCOIの管理に関する規定の策定	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究機関におけるCOI委員会設置の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合は委託先機関: )
当研究に係るCOIについての報告・審査の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究に係るCOIについての指導・管理の有無	有 <input type="checkbox"/> 無 <input checked="" type="checkbox"/> (有の場合はその内容: )

(留意事項) ・該当する□にチェックを入れること。  
・分担研究者の所属する機関の長も作成すること。

厚生労働大臣 殿

機関名 東都大学

所属研究機関長 職 名 学長

氏 名 吉岡 俊正

次の職員の令和5年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

1. 研究事業名 地域医療基盤開発推進研究事業
2. 研究課題名 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究
3. 研究者名 (所属部署・職名) 東都大学・助教  
(氏名・フリガナ) 肥田 泰幸 (ヒダ ヤスユキ)
4. 倫理審査の状況

	該当性の有無		左記で該当がある場合のみ記入 (※1)		
	有	無	審査済み	審査した機関	未審査 (※2)
人を対象とする生命科学・医学系研究に関する倫理指針 (※3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	東都大学幕張ヒューマンケア学部	<input type="checkbox"/>
遺伝子治療等臨床研究に関する指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
その他、該当する倫理指針があれば記入すること (指針の名称: )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

(※1) 当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他 (特記事項)

(※2) 未審査に場合は、その理由を記載すること。

(※3) 廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

#### 5. 厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 <input checked="" type="checkbox"/> 未受講 <input type="checkbox"/>
-------------	---

#### 6. 利益相反の管理

当研究機関におけるCOIの管理に関する規定の策定	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究機関におけるCOI委員会設置の有無	有 <input type="checkbox"/> 無 <input checked="" type="checkbox"/> (無の場合は委託先機関: 倫理審査委員会 )
当研究に係るCOIについての報告・審査の有無	有 <input checked="" type="checkbox"/> 無 <input type="checkbox"/> (無の場合はその理由: )
当研究に係るCOIについての指導・管理の有無	有 <input type="checkbox"/> 無 <input checked="" type="checkbox"/> (有の場合はその内容: )

(留意事項) ・該当する□にチェックを入れること。  
・分担研究者の所属する機関の長も作成すること。