別紙3

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)
川眞田 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勢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。

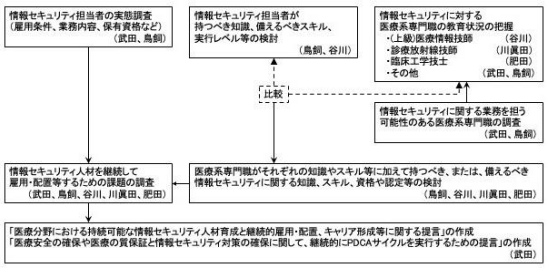

図1. 医療機関における情報セキュリティ人材の育成と配置に向けた検討課題

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行え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)

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となる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、最低限習得するべき技術・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(攻撃者視点対策能力)、Continuous Diagnostics and Mitigation (CDM)視点(防衛者視点対策能力)、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るべき試験、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・ガイダンス」、「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)川眞田 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)川眞田 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, 川眞田実 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