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～（令和）６年度　総合研究報告書

研究代表者　武田　理宏

（令和）７（２０２５）年　５月

目　　次

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)
総合研究報告書

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。

「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、試験の保有率は低かった。「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」で整理し、(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、診療情報管理士は情報セキュリティに関する教育が含まれていたが、総論的な内容で、追加教育が必要と考えられた。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、「人材」、「組織体制」、「教育体制」の観点で、医療情報セキュリティ人材の育成や配置について議論を行った。「人材」、「組織体制」については、人材育成や組織体制確立やに成功している医療安全領域や感染症対策領域の取り組みを参考にした。「教育」については、医療情報セキュリティ人材の育成カリキュラムの開発を行った。

次に、「情報セキュリティ担当者の実態調査」と「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」から、「情報セキュリティ人材を継続して雇用・配置するための課題の調査」を行った。この際、外部情報セキュリティ人材の活用に関する検討を行った。

以上の研究成果を取りまとめ、「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」の作成を行った。

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)」を実施した。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した。

これと並行し、医療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」を行った。

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」を実施した。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った。

次に、「情報セキュリティ担当者の実態調査」と「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」から、「情報セキュリティ人材を継続して雇用・配置するための課題の調査」を行った。この際、「情報

セキュリティ担当者の実態調査」では医療機関に情報セキュリティの知識とスキルセットを持つ人材が少ないことが確認されたため、外部情報セキュリティ人材の活用に関する検討を行った。

以上の検討から、医療情報セキュリティ人材の育成、配置について、「組織体制」、「人材」、「教育」を基軸に検討を行うこととした。「人材」、「組織体制」については、先行して組織体制の確立や人材育成に成功している医療安全領域や感染症対策領域の取り組みを参考にした。「教育」については、医療情報セキュリティ人材の育成カリキュラムの開発を行った。

以上の研究成果を取りまとめ、「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」の作成を行った。

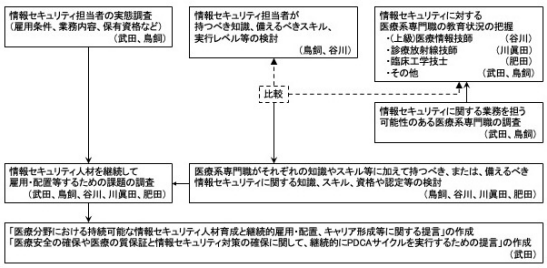

図1. 医療機関における情報セキュリティ人材の育成と配置に向けた検討課題

2. 情報セキュリティ担当者の実態調査（担当：武田・鳥飼）

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。

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）

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: Information –technology Promotion Agency)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）、川眞田（診療放射線技師）、肥田（臨床工学技士））
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）

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、臨床工学技士を挙げた。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. 医療機関が配置すべき医療情報セキュリティ人材と持つべき知識、スキルセット、実行レベル（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。

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。「人材」、「組織体制」については、人材育成や組織体制確立に成功している医療安全領域や感染症対策領域の取り組みを参考にした。「教育」については、医療情報セキュリティ人材の育成カリキュラムの開発を行った。

6. 医療情報セキュリティ人材の育成カリキュラムの開発（担当：谷川）

医療情報セキュリティ人材の Group A 人材、Group B 人材、Group C 人材のそれぞれに対して、情報セキュリティ人材が持つべき知識を 5 つの視点（攻撃者視点、防衛者視点、設計者視点、緊急時対応、日常運用保守）から整理し、医療機関で求められるスキルレベルをもとに必要技能分類別の学習目標の検討を行った。

次に、医療情報セキュリティ人材の育成カリキュラム開発のため、人材ごとのベースとなるスキルレベルの目安をもとに、IPA が実施する情報処理技術者試験のシラバスおよび関連書籍、日本医療情報学会が作成している医療情報技師能力検定試験の到達目標および教科書等を調査し、情報セキュリティ担当者に求められるスキルを検討した。

これらの調査結果をもとに、学習目標を達成するための教育コンテンツを検討・体系化し、既存の情報処理関連資格や医療情報関連資格との整合性を考慮しながら、新規講習と定期（継続）講習に分けたカリキュラム案を検討した。

7. 外部情報セキュリティ人材の活用に関する検討（担当：武田・鳥飼・谷川・川眞田・肥田）

IPA、一般社団法人医療サイバーセキュリティ協議会（MedCSC: Medical Cyber Security Council, General Inc. Association）と外部人材の活用についての議論を行った。

8. 情報セキュリティ人材を継続して雇用・配置するための課題の調査（担当：武田・鳥飼・谷川・川眞田・肥田）

「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」、「情報セキュリティ人材配置に関するアンケート調査」、「医療系専門職における情報セキュリティに対する教育状況」、「外部情報セキュリティ人材の活用に関する検討」の結果から、研究班で情報セキュリティ人材を継続して雇用・配置するための課題の議論を行った。

9. 情報セキュリティ人材の育成と配置に向けた提言（担当：武田・鳥飼・谷川・川眞田・肥田）

「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

報セキュリティ人材配置に関するアンケート調査」、「医療系専門職における情報セキュリティに対する教育状況」、「情報セキュリティ人材の育成カリキュラムの開発」、「外部情報セキュリティ人材の活用に関する検討」、「情報セキュリティ人材を継続して雇用・配置するための課題」の調査から、「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」と「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」の作成を行った。

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）

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）

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）、川眞田（診療放射線技師）、肥田（臨床工学技士））

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）

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 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. 医療機関が配置すべき医療情報セキュリティ人材と持つべき知識、スキルセット、実行レベル（担当：武田、鳥飼、谷川、川眞田、肥田、吉川）

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、これらの医療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。

各医療機関や各医療機関が配置する医療情報セキュリティ人材が果たすべき役割として、日ごろの情報セキュリティ対策を講じるところまでを考慮した。実際に情報セキュリティインシデントが発生した際は、外部からさらに専門性の高い情報セキュリティ人材が医療機関に派遣され、医療機関が配置する医療情報セキュリティ人材と協働して、医療提供機能の回復を図ることを想定している。

「人材」、「組織体制」については、組織体制の構築や人材育成に成功している医療安全対

策や感染症対策を参考にした。これらは診療報酬でそれぞれ、医療安全対策加算や感染症対策加算が認められている。

医療安全対策加算に関する施設基準では、医療安全管理部門を設置すること、医療安全管理者として、医療安全対策に係る適切な研修を修了した医療系専門職を置くことが求められている。この研修は、40 時間以上の研修で、「医療安全の基本的知識、安全管理体制の構築、医療安全についての職員研修の企画・運営、医療安全に資する情報収集と分析、対策立案、フィードバック、評価、医療事故発生時の対応、安全文化の醸成等について研修するものであること。」が求められている。医療安全対策地域連携加算では、加算1では「少なくとも年1回程度、当該加算に関して連携している医療安全対策加算1に係る届出を行っている保険医療機関より評価を受けていること。」、加算2では「医療安全対策加算1に係る届出を行っている保険医療機関と連携し、少なくとも年1回程度、医療安全対策地域連携加算2に関して連携しているいずれかの保険医療機関より医療安全対策に関する評価を受けていること。」と相互チェックの仕組みが導入されている。医療安全に倣い、医療情報システム管理部門を設置することや、医療情報セキュリティに関する教育カリキュラムを規定すること、他施設と相互チェックを行うことは、情報セキュリティ対策向上につながると考えられた。

感染症対策加算では、感染対策向上加算1の医療機関が指導的な医療機関として、感染対策向上加算2、加算3の保険医療機関等と連携することが求められている。「保健所、地域の医師会と連携し、加算2又は3の医療機関と合同で、年 4 回以上カンファレンスを実施（このうち 1 回は新興感染症等の発生を想定した訓練を実施）」や「加算2、3及び外来感染対策向上加算の医療機関に対し、必要時に院内感染対策に関する助言を行う体制を有する」が求められる。情報セキュリティに関しても、指導的な立場の医療機関がカンファレンスを開催し、最新の情報セキュリティに関する知識を共有することや、サイバー攻撃合同訓練を実施することが想定された。

4-1.医療情報セキュリティ人材

医療情報セキュリティ人材が持つべき知識やスキルセットについては、Group A 人材、Group B 人材、Group C 人材の 3 つに分けて整理を行った。

Group A 人材、Group B 人材、Group C 人材が持つべき知識、備えるべきスキル、実行レベルについては、「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、実行レベル等の検討」のとおり、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）に対して要求項目を整理した（添付資料 1_表 1）。

「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、医療系国家資格の教育カリキュラムや国家試験ごとの出題基準と出題実績、医療情報技師、診療情報管理士の教育カリキュラムや資格試験の出題基準を調査した結果、医療情報技師がもっとも情報セキュリティに関する教育カリキュラムが充実していた。そこで、上記 6 視点に対して、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（表 1、添付資料 1_表 2）。

表 1．医療情報セキュリティ人材が持つべき資格・知識

	医療情報システムに対する知識の担保	情報セキュリティに対する知識の担保
Group A 人材	「上級医療情報技師」相当の資格・知識	「情報処理安全確保支援士」（IPA レベル 4）相当の資格・知識
Group B 人材	「医療情報技師」相当の資格・知識	「情報セキュリティマネジメント試験」（IPA レベル 2）相当の知識
Group C 人材	「医療情報基礎知識検定試験」相当の知識	「IT パスポート試験」（IPA レベル 1）相当の知識

Group A 人材、Group B 人材、Group C 人材に対し、「医療情報システムに対する知識の担保」、「情報セキュリティに対する知識の担保」、「求められる業務」について取りまとめを行った。一人の人材が医療情報システムに対する知識と情報セキュリティに対する知識を合わせ持つことが望まれるが、同一組織内で良好なコミュニケーションが取れることを条件に、医療情報システムに対する知識を持つ人材と情報セキュリティに対する知識を持つ人材が協力して情報セキュリティ対策に取り組むことを許容することとした。

① Group A 人材

Group A 人材は医療情報システムの特性を理解した上で、自施設に対しては、自立的に情報システムのセキュリティ対策を施すこと、情報セキュリティインシデント発生を想定した診療継続計画（IT-BCP）を策定すること、情報セキュリティインシデントが発生した際には外部から派遣される情報セキュリティ専門家と協力してシステム復旧に向けた活動を行うこと、ができる人材、さらに、他施設に対しては、情報システムのセキュリティ対策や IT-BCP の策定の指導を行うこと、他施設の情報システムのセキュリティ監査を実施すること、他施設に情報セキュリティインシデントが発生した際には、当該施設に赴き、復旧に向けた活動を行うこと、ができる人材を想定する。

Group A 人材は、医療機関の情報セキュリティ人材の育成や、自施設、他施設の病院職員に対する情報セキュリティ教育を実施することが求められる。

このために、医療情報システムと情報セキュリティに対する高度の知識が求められる。また、情報セキュリティに関する最新の知識を継続して獲得する能力が求められる。一人の人材が医療情報システムと情報セキュリティに対する高度の知識を持つことが望ましいが、医療情報システム管理部門に医療情報システム対する知識を持つ人材と情報セキュリティに対する知識を持つ人材を配置し、両者が良好なコミュニケーションのもと業務にあたることを許容する。

Group A 人材は「統括情報セキュリティ責任者」やそれを補助するものとして、病院経営に関わることが求められる。このためには

中長期的な事業計画に対して破綻をきたさないよう、計画的なセキュリティ維持強化計画を提案する能力が必要となる。セキュリティリスクはサイバー攻撃トレンドと自施設で残存するセキュリティ課題の両側面について、重要な医療ワークフローならびに患者保全のリスクの高い箇所を指摘できる必要がある。改善箇所のセキュリティ強化については、現場で許容されうる IT 変更負担を適切に推測しながら、IT インフラ、計算機類、ソフトウェア、サービス層におけるセキュリティ実装の形態を勘案するとともに、特に医療においては容体急変対応で不可欠な IT の可用性を重視した実装形態を選択する能力が求められる。

Group A 人材

【医療情報システムに対する知識の担保】

- 「上級医療情報技師」相当の資格を有し、更新が行われていること。
- 「上級医療情報技師」相当の資格を有さない場合は、①から⑤の 2 つ以上を満たすことが望まれる。

  ※将来的には、「上級医療情報技師」相当の資格を取得することが推奨される。

  ①医療系国家資格や「医療情報技師」、「診療情報管理士」の資格を有すること

  ②医療機関において専従で 5 年以上医療情報システム管理に従事した経験があること

  ③医療機関や事業者で、医療情報システム導入（更新）で主導的な役割を果たした経験があること

  ④所定の医療情報システムに関する教育（「３.医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。

  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと
- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】

- IPA「情報処理安全確保支援士」相当の資格を有し、更新が行われていること
- IPA「情報処理安全確保支援士」相当の資格を有さない場合、所定の情報セキュリティに関する教育（「３．医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。

  ※将来的には、「情報処理安全確保支援士」相当の資格取得を推奨する。
- 内閣府サイバーセキュリティセンターから最新の情報セキュリティ情報を収集するなど、情報セキュリティに対する最新の知識を取得すること。

【求められる業務】

≪自施設≫

- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 医療情報システムに対する情報セキュリティ対策
- 情報セキュリティインシデントに向けた IT-BCP の策定
- 情報セキュリティインシデント発生時のシステム復旧に向けた取り組み

  （外部から派遣される情報セキュリティ専門家や電子カルテベンダーとの協働、病院職員に向けた司令塔の役割）
- 自施設の職員に対する情報セキュリティ

教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」間で実施する情報システムのセキュリティ相互チェックへの対応
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練への参加

≪他施設≫
- Group A 人材間や他の情報セキュリティ人材との情報セキュリティ対策に関する情報共有や連携
- 他施設の病院経営層に向けた情報セキュリティ対策体制の指導やアドバイス
- 他施設の医療情報システムに対する情報セキュリティ対策や情報セキュリティインシデントに向けた IT-BCP の策定の指導やアドバイス
- 他施設の情報セキュリティインシデント発生時のシステム復旧に向けた取り組みの支援
- 他施設の職員に対する情報セキュリティ教育の支援
- 他施設の情報システムのセキュリティチェックの実施
- 他施設との情報セキュリティカンファレンスの主催
- 他施設とのサイバー攻撃合同訓練の主催

② Group B 人材

Group B 人材は医療情報システムの特性を理解した上で、自施設に対して、自立的に情報システムのセキュリティ対策を施すこと、情報セキュリティインシデント発生を想定した診療継続計画（IT-BCP）を策定することができる人材を想定する。また、自施設に情報セキュリティインシデントが発生した際には、他施設の Group A 人材の指導のもと、システム復旧に向けた活動を行うことができる人材を想定する。Group B 人材は自施設の病院職員に対して、情報セキュリティ教育を実施できる必要がある。

このために、医療情報システムと情報セキュリティに対する高い知識が求められる。また、情報セキュリティに関する最新の知識を継続して獲得する能力が求められる。

一人の人材が医療情報システムと情報セキュリティに対する高度の知識を持つことが望ましいが、医療情報システム管理部門に医療情報システム対する知識を持つ人材と情報セキュリティに対する知識を持つ人材を配置し、両者が良好なコミュニケーションのもと業務にあたることを許容する。

Group B 人材は「統括情報セキュリティ責任者」やそれを補助するものとして、病院経営に関わることが求められる。このためには中長期的な事業計画に対して破綻をきたさないよう、計画的なセキュリティ維持強化計画を提案する能力が必要となる。セキュリティリスクはサイバー攻撃トレンドと自施設で残存するセキュリティ課題の両側面について、重要な医療ワークフローならびに患者保全のリスクの高い箇所を指摘できる必要がある。改善箇所のセキュリティ強化については、現場で許容されうる IT 変更負担を適切に推測しながら、IT インフラ、計算機類、ソフトウェア、サービス層におけるセキュリティ実装の形態を勘案するとともに、特に医療においては容体急変対応で不可欠な IT の可用性を重視した実装形態を選択する能力

が求められる。

Group B 人材

【医療情報システムに対する知識の担保】

- 「医療情報技師」相当の資格を有し、更新が行われていること。
- 「医療情報技師」相当の資格を有さない場合は、①から⑤の 2 つ以上を満たすことが望まれる。

  ※将来的には、「医療情報技師」相当の資格取得を強く推進する。

  ①医療系国家資格や「診療情報管理士」の資格を有すること

  ②医療機関において専任で 3 年以上医療情報システム管理に従事した経験があること

  ③医療機関や事業者で、医療情報システム導入（更新）で主導的な役割を果たした経験があること

  ④所定の医療情報システムに関する教育（「３.医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。

  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと
- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】

- IPA の「情報セキュリティマネジメント試験」相当の資格を有すること。
- IPA の「情報セキュリティマネジメント試験」相当の資格を有さない場合、
  所定の情報セキュリティに関する教育（「３.医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。

  ※将来的には、「情報セキュリティマネジメント試験」相当の資格取得を強く推進する。
- 内閣府サイバーセキュリティセンターから最新の情報セキュリティ情報を収集するなど、情報セキュリティに対する最新の知識を取得すること。

【求められる業務】

- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 自施設の情報システムに対する情報セキュリティ対策
- 自施設の情報セキュリティインシデントに向けた IT-BCP の策定
- 情報セキュリティインシデント発生時のシステム復旧に向けた取り組み
  （外部から派遣される情報セキュリティ専門家や電子カルテベンダーとの協働、病院職員に向けた司令塔の役割）
- 自施設の職員に対する情報セキュリティ教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」が開催する情報セキュリティカンファレンスへの参加
- 「指導的な立場の医療機関」や事業者が実施する情報システムのセキュリティチェックへの対応
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練への参加
- Group A 人材間や他の情報セキュリティ

人材との情報セキュリティ対策に関する情報共有や連携

③ Group C 人材

Group C 人材は医療情報システムと情報セキュリティに対する最低限の知識を有し、Group A 人材の力を借りながら、自施設の情報システムの情報セキュリティ対策を講じることができる人材である。医療情報システムの新規導入や更新時に導入事業者から情報セキュリティ対策の説明を受け、情報セキュリティ対策の懸念があれば、Group A 人材に問い合わせをすることができることが求められる。

自施設に情報セキュリティインシデントが発生した際、導入業者と連携した初動対応と、「指導的な立場の医療機関」や公的機関、事業者から派遣される Group A 人材と連携して復旧対応をすることが求められる。

このために、医療情報システムや情報セキュリティ対策で使用される言葉が理解できることが最も大切となる。Group C 人材は病院内の医療情報システム安全管理責任者ならびに管理者の方針指示を受け、現在の医療情報システムに対するセキュリティ強化対策を電子カルテ事業者と共に運用する能力が求められる。システムトラブル発生時には、障害箇所の推定情報からサイバー攻撃の可能性についての予兆、続いて生じる IT としてのサービス停止、IT システムに関する被害推定ならびに BCP に必要な一時対応について、医療情報システム安全管理責任者ならびに管理者の指示を仰ぎながら、可能な範囲で実施ならびに確認を行う必要がある。

Group C 人材は一次対応と並行して、Group A 人材に把握できる範囲の自施設のサイバー被害状況ならびに診療機能不全状況について、迅速かつ的確に伝達する能力が求められる。また Group A 人材が考察し指示した対応方法についてこれを理解し、対応作業を行う院内スタッフまたは電子カルテ事業者の対応者の助力を得ることについて、日常的なコミュニケーションを通じて備える必要がある。

Group C 人材

【医療情報システムに対する知識の担保】

- 「医療情報基礎知識検定試験」に合格していること
  または、「医療情報技師」相当の資格を有すること。
- 「医療情報基礎知識検定試験」、「医療情報技師」相当の資格を有さない場合は、①から⑤のいずれか 1 つを満たすことが望まれる。
  ※将来的には、「医療情報基礎知識検定試験」の合格を目指すことを強く推奨する。
  ①医療系国家資格や「診療情報管理士」の資格を有し、医療機関で医療情報システムを使った実務経験があること
  ②医療機関において、1 年以上医療情報システム管理に従事した経験があること
  ③医療機関や事業者で、医療情報システム導入（更新）に関わった経験があること
  ④所定の医療情報システムに関する教育（「３. 医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと

- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】
- IPA「IT パスポート試験」に合格していることが望ましい
- 所定の情報セキュリティに関する教育（「３.医療情報セキュリティ人材が受けるべき教育について」を参照）を受講していること。

【求められる業務】（必要に応じて Group A 人材から指導、アドバイスを求める）
- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 自施設の情報システムに対する情報セキュリティ対策
- 自施設の情報セキュリティインシデントに向けた IT-BCP の策定
- 自施設の情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家や電子カルテベンダーに協力し、システム復旧に向けた取り組むこと
- 自施設の職員に対する情報セキュリティ教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」が開催する情報セキュリティカンファレンスへの参加
- 内閣府サイバーセキュリティセンターなどから、最新の情報セキュリティ情報の収集

4-2. 医療機関の組織体制

医療機関を「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」、「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」に分け、その役割や配置すべき医療情報セキュリティ人材の整理を行った。

「指導的な立場の医療機関」は Group A 人材を配置し、Group A 人材が中心となって、自施設、「自施設の情報システムを守ることのできる医療機関」、「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」に所属する Group B 人材、Group C 人材と協働しながら、地域の医療機関が広くサイバーセキュリティ対策を強化することを想定した。また、「指導的な立場の医療機関」は地域の医療情報セキュリティ人材の育成に努めることとした。

① 指導的な立場の医療機関

「指導的な立場の医療機関」は、自施設の情報システムを自立的に守るだけでなく、「自施設の情報システムを守ることができる医療機関」や「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」に対して支援や教育を行うことができる医療機関である。このため、医療情報システムと情報セキュリティに関する高い知識を有した Group A 人材の配置が必要となる。

「指導的な立場の医療機関」を目指すべき医療機関として、大学病院や特定機能病院などを想定するが、その他の医療機関が「指導的な立場の医療機関」となることを否定するものではない。

将来的に、少なくとも各都道府県に 1 施設は「指導的な立場の医療機関」の配置を目指す。あるいは、自治体に医療機関を指導するセキュリティ人材を配置することも考え

られる。

指導的な立場の医療機関

【自施設での組織体制】

- 医療情報システム管理部門を設置すること。
- 医療情報システム管理部門に「統括情報セキュリティ責任者」を配置すること。
  ※「統括情報セキュリティ責任者」が「医療情報システム安全管理責任者」となることも想定される。
- 必要に応じて、「統括情報セキュリティ責任者」の補助者を配置すること。
- 「統括情報セキュリティ責任者」またはその補助者は専任で医療情報システム管理に従事すること。
  ※将来的には、「統括情報セキュリティ責任者」または、その補助者は専任で医療情報システム管理に従事すること。
- 「統括情報セキュリティ責任者」または、その補助者は Group A 人材の資格を有すること。
  ※将来的には、「統括情報セキュリティ責任者」が Group A 人材の資格を有すること。
- 医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門に、Group C 人材を配置すること。
- 医療情報システムに関するセキュリティ委員会を設置し、「統括情報セキュリティ責任者」は病院経営層や部門に配置する Group C 人材と協力して、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【「指導的な立場の医療機関」間の取り組み】

- 「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築すること。
- 「指導的な立場の医療機関」間で、互いの施設の医療情報システムの相互チェックを実施すること。

【地域の医療機関との連携】

- 「自施設の情報システムを守ることができる医療機関」や「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」と合同で、定期的に情報セキュリティに関するカンファレンスを開催すること。
- 「自施設の情報システムを守ることができる医療機関」と合同で、サイバー攻撃合同訓練を実施すること。
- 他医療機関から情報セキュリティ対策に関する実地研修を受け入れる体制を有すること。
- 「自施設の情報システムを守ることができる医療機関」の情報システムのセキュリティチェックを実施できること。
- 「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」の Group C 人材に対し、必要時に情報セキュリティに関する助言(セキュリティチェックを含む)

を行う体制を有すること。
- 「自施設の情報システムを守ることができる医療機関」や「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」に情報セキュリティインシデントが発生した際、システム復旧に向けた支援を行う体制を有すること。

② 自施設の情報システムを守ることができる医療機関

「自施設の情報システムを守ることができる医療機関」は、自施設の情報システムを自立的に守ることができる医療機関である。病床数に関わらず、情報セキュリティインシデントにより診療が停止した場合、地域医療に大きな影響が生じる医療機関は、「自施設の情報システムを守ることができる医療機関」を目指す必要がある。

400 床以上の医療機関については、情報システム構成が複雑となることが多く、情報セキュリティ対策が難しくなる。また、情報セキュリティインシデント発生時のシステム復旧に時間を要することが想定されるため、「自施設の情報システムを守ることができる医療機関」を目指す必要がある。

自施設の情報システムを守ることができる医療機関

【自施設での組織体制】
- 医療情報システム管理部門を設置すること。
- 医療情報システム管理部門に統括情報セキュリティ責任者」を配置すること。
- 必要に応じて、「統括情報セキュリティ責任者」の補助者を配置すること。
- 「統括情報セキュリティ責任者」またはその補助者は専任で医療情報システム管理に従事すること。

  ※将来的には、「統括情報セキュリティ責任者」は専任で医療情報システム管理に従事すること。
- 「統括情報セキュリティ責任者」または、その補助者は Group B 人材の資格を有すること。

  ※将来的には、「統括情報セキュリティ責任者」が Group B 人材以上の資格を有すること。

  ※「指導的な立場の医療機関」や公的機関、医療機関の中央組織、民間事業者に所属する Group A 人材と継続的な契約する場合は、Group C 人材の資格を有する人材の配置で可とする。
- 医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門には、Group C 人材を配置すること。
- 医療情報システムに関するセキュリティ委員会を設置し、「統括情報セキュリティ責任者」は病院経営層や部門に配置する Group C 人材と協力し、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【「指導的な立場の医療機関」や Group A 人

材を配置する公的機関、事業者との取り組み】

- 「指導的な立場の医療機関」が定期的に開催するカンファレンスに参加すること。
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練に参加すること。
- 「指導的な立場の医療機関」や公的機関、事業者による医療情報システムのセキュリティチェックを実施すること。

③ 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

「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」は、「指導的な立場の医療機関」や Group A 人材を配置する事業者の力を借りて、自施設の情報システムを守ることができる医療機関である。オンプレミスで医療情報システムサーバーを立てる医療機関が対象となる。情報システム新規導入時や更新時、情報セキュリティインシデント発生時に、「指導的な立場の医療機関」や Group A 人材を配置する事業者から指導を受けることを想定する。このため、Group A 人材との情報共有に必要な知識を有する Group C 人材の配置が必要となる。

※適切な契約のもと、クラウド型電子カルテを導入する医療機関は、本対象の医療機関からは外れる。ただし、導入電子カルテベンダー等から情報セキュリティ教育を受けることは必要となる。

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

【自施設での組織体制】

- 「医療情報システム安全管理責任者」を配置すること。
- 「医療情報システム安全管理責任者」または、その補助者は Group C 人材以上の資格を有することが望ましい。
- 「指導的な立場の医療機関」または事業者の Group A 人材の助けを借りて、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会または e-learning を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【地域の医療機関との連携】

- 「指導的な立場の医療機関」が定期的に開催するカンファレンスに参加すること。
- 情報システム新規導入時や更新時は必要に応じて、「指導的な立場の医療機関」や Group A 人材を配置する事業者から情報セキュリティに関する指導を受けること。

5. 医療情報セキュリティ人材の育成カリキュラムの開発（担当：谷川）

医療情報セキュリティ人材の育成カリキュラムとして、Group A、Group B、Group C 人材それぞれについて、必要技能分類別の学習目標と教育カリキュラム案を策定した。

5-1. Group A 人材

情報処理安全確保支援士試験や上級医療情報技師能力検定試験に関する内容を参考に、新規講習では組織的な情報セキュリティへの取り組みや他部署・施設への助言に必要となる内容を洗い出し、情報セキュリティマネジメントの実践から情報戦略の立案、チームマネジメント、セキュリティ教育などの事項を中心に、到達目標と計15項目の学習項目を設定した。また、定期(継続)講習では、最新の脅威動向やインシデント対応、ガイドラインの更新内容などを学ぶ内容とした。

Group A 人材の新規講習について、情報処理安全確保支援士の資格を有していれば項番1～7、上級医療情報技師の資格を有していれば8～15を免除することができる。

Group A 人材の教育カリキュラム案

○ 到達目標

診療業務フローについての十分な理解と医療情報セキュリティの実践経験が豊富にあり、情報セキュリティの技術的観点から、組織全体を導く指針を示し、実効性のある助言を行うことができる。

○ 教育コンテンツ

【新規講習】

組織的に情報セキュリティへの取り組み、他の部署・施設へ助言を行うために必要となる事項について学ぶ。

1. 情報セキュリティマネジメントの実践
2. 情報システムのリスク分析と評価
3. 侵入検知・防御に関する技術
4. アクセス制御と認証に関する技術
5. 暗号に関する技術
6. システム開発におけるセキュリティ対策
7. 情報セキュリティに関する法制度・ガイドライン
8. 医療情報関連法令・ガイドライン
9. 情報戦略の立案
10. プロジェクトマネジメント
11. チームマネジメント
12. セキュリティインシデントへの対応
13. 医療情報システムのシステム監査
14. 災害やシステム障害に備えた対策
15. セキュリティ教育及び人材育成の方法

【定期(継続)講習】

医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威
B. インシデント発生時の初動対応とその際の留意点
C. 医療情報システムの安全管理に関するガイドラインについて

5-2. Group B 人材

情報セキュリティマネジメント試験や医療情報技師能力検定試験に関する内容を参考に、新規講習では情報システム等のセキュリティに関する管理と技術的対策、診療業務フローのなかでの医療情報システムの役割と機能、医療情報システムの安全管理に関するガイドライン等の法令などを中心に、到達目標と計 15 項目の学習項目を設定した。定期(継続)講習は、Group A 人材と同一の内容として、最新の脅威動向やインシデント対応、ガイドラインの更新内容などを学ぶ内容とした。

Group B 人材の新規講習について、情報セ

キュリティマネジメント試験に合格していれば項番1～7、医療情報技師の資格を有していれば8～15を免除することができる。

Group B 人材の教育カリキュラム案

○ 到達目標

医療情報システムの機能及び役割と情報セキュリティの基本的な知識及び技術を備えており、医療現場の診療業務フローを理解して、日常的なセキュリティ対策を実践するとともに、インシデント発生時の適切な初動対応を行うことができる。

○ 教育コンテンツ

【新規講習】

医療情報システムの機能及び役割と情報セキュリティの基本的な知識及び技術、診療業務フローについて学ぶ。

1. 情報セキュリティマネジメントの概要
2. 情報システムの脅威と脆弱性
3. 情報セキュリティ技術の概要
4. コンピュータシステムのセキュリティ対策
5. ネットワークのセキュリティ対策
6. データベースのセキュリティ対策
7. 情報セキュリティに関する法制度
8. プロジェクトマネジメントとサービスマネジメント
9. 医療現場の診療業務フロー
10. 医療情報システムの機能及び役割
11. 医療情報システムの調達と運用保守
12. 医療情報の安全管理に関する関係法令／医療情報システムの安全管理対策（経営管理編）
13. 医療情報システムの安全管理対策（企画管理編）
14. 医療情報システムの安全管理対策（システム運用編）
15. 医療情報システム／セキュリティを支える施設基盤

【定期（継続）講習】

医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威
B. インシデント発生時の初動対応とその際の留意点
C. 医療情報システムの安全管理に関するガイドラインについて

5-3. Group C 人材

IT パスポート試験や医療情報基礎知識検定試験に関する内容を参考に、新規講習では基本的な内容を効率的に学べるよう、「医療情報セキュリティの基本」（必須プログラム）と「医療および医療情報システム」「情報処理技術」（任意プログラム）に分け、到達目標と学習項目を設定した。定期（継続）講習は他のグループと同様の内容とした。

Group C 人材は、他に比べて基本的なことのみを求めており、多様な方が候補となりうる。そのなかでも医療資格等の養成課程において情報処理技術について一定の学習を行っている、診療放射線技師、臨床工学技士、臨床検査技師、診療情報管理士などは主要な候補となると思われる。本カリキュラムでは、多様な方が Group C の人材になるための必要な教育が受けられるよう、必須プログラムと必要に応じて受講する選択プログラムの構成という柔軟な設計とした。

Group C 人材の教育カリキュラム案

○ 到達目標

医療情報システムの利用と情報セキュリティに必要となる基本ルールを理解し、医療現場での日常業務における基礎的なセキュリティ対策を行うとともに、インシデント発生時には速やかに関係部署・機関に通報することができる。

○ 教育コンテンツ

【新規講習】

医療情報システムの利用と情報セキュリティに必要となる基本事項について学ぶ。

A. 医療情報セキュリティの基本（必須プログラム：30 分程度の e-Learning）
1. 情報セキュリティの基礎
2. 病院情報システムの最低限の運用管理とセキュリティ
3. トラブル発生時の初期対応と関係機関への連絡

B. 医療および医療情報システム（任意プログラム①　：50 分程度の e-Learning）
1. 日本の医療制度と医療関連法規
2. 医療機関の業務と診療情報管理
3. 病院情報システムの主な構成と機能
4. 病院情報システムのアカウント管理とアクセス制御
5. 病院情報システムの運用と保守管理

C. 情報処理技術（任意プログラム②　：50 分程度の e-Learning）
1. コンピュータの基礎
2. ネットワーク技術とネットワークサービス
3. データベースとデータ管理
4. 情報システムの導入・運用・保守
5. 情報セキュリティ技術

【定期（継続）講習】

医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威
B. インシデント発生時の初動対応とその際の留意点
C. 医療情報システムの安全管理に関するガイドラインについて

6. 外部情報セキュリティ人材の活用に関する検討（担当：武田・鳥飼・谷川・川眞田・肥田）

外部セキュリティ人材は、他施設、団体に所属する医療情報セキュリティ人材と、医療領域以外で活躍する情報セキュリティ人材が想定される。

6-1. 医療領域で活躍する医療情報セキュリティ人材の活用

本研究で定義する Group A 人材、Group B 人材は医療情報セキュリティに対する高い知識とスキルセットと実行レベルが求められる。保健医療福祉分野では、これらの人材を育成していく必要があるが、「情報セキュリティ人材配置に関するアンケート調査」からこれらの人材から、全ての医療機関にこれらの人材を配置することは困難であることが予想される。このため、他施設、団体で活躍する医療情報セキュリティ人材の活用が必要となる。

「指導的な立場の医療機関」は地域の医療機関の情報セキュリティ対策に対する指導や人材育成が求められることから、人材不足があったとしても Group A 人材の配置が必須と考えら

れた。「自施設の情報システムを守ることができる医療機関」が Group B 人材を確保することが困難な場合、自施設に Group C 人材に置き、他施設、団体の Group A 人材と顧問契約等を結び、Group C 人材が Group A 人材の指示を受けながら、情報セキュリティ対策を進めることが想定される。ここで、Group A 人材の所属は「指導的な立場の医療機関」、「同一法人などの中央組織」、「医療機関に情報セキュリティサービスを提供する民間事業者」、「医療機関に情報セキュリティサービスを提供する個人事業者」が想定される。「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」は上記施設、団体に所属する Group A 人材に必要時、指導を受けながら情報セキュリティ対策を進めることが想定された。

6-2. 医療領域外で活躍する情報セキュリティ人材の活用

保健医療福祉分野の情報セキュリティ対策を進める場合、医療情報システムの特性を理解することが必須となる。このため、外部情報セキュリティ人材に如何にこれらの知識の学習機会を提供するかが課題となる。

MedCSC からは、MedCSC や医療情報技師育成部会が医療領域の情報セキュリティに関する講習会、ワークショップを運営し、IPA の情報処理安全確保支援士の特定講習に組み込む案が提示された。今年度、本研究班で示された Group A 人材向けの教育コンテンツ 8 から 15（8. 医療情報関連法令・ガイドライン、9. 情報戦略の立案、10. プロジェクトマネジメント、11. チームマネジメント、12. セキュリティインシデントへの対応、13. 医療情報システムのシステム監査、14. 災害やシステム障害に備えた対策、15. セキュリティ教育及び人材育成の方法）がその候補となる。また、本研究班で検討した「指導的な立場の医療機関」が提供する実地研修の活用が想定された。もちろん、本研究班で提案する医療情報技師、上級医療情報技師の資格取得を推奨することも必要である。

教育コンテンツの情報処理安全確保支援士の特定講習への組み込みや、情報処理安全確保支援士に対する医療情報技師、上級医療情報技師の資格取得に向けた推奨を行うことができないか、IPA と議論を継続する必要がある。

6-3. 医療領域内外で活躍する医療情報セキュリティ人材の検索

情報セキュリティ人材を必要とする医療機関が、医療情報システムの特性を理解した医療情報セキュリティ人材を如何に検索するかが課題となる。

IPA では、中小企業等のセキュリティコンサルが対応可能な登録セキスペのリスト（アクティブリスト）を作成が検討されていた。アクティブリストでは、地域、支援可能期間、得意とする支援領域、支援実績、経験業種、経験業務、保有資格、専門分野（技術）、一言アピールが登録されることが検討されていた。得意とする支援領域、支援実績、経験業種は医療機関が医療情報セキュリティ人材を検索するために有用であると考えられる。一歩踏み込むと、自己申告ではなく、客観的に医療情報システムの特性を理解していることを判別できることが望まれる。本研究班で示した教育コンテンツの受講（特定講習としての受講）や「指導的な立場の医療機関」での実地研修の経験などが検索できるとより良いと考えられた。保有資格として、上級医療情報技師や医療情報技師が登録され、検索できると、アクティブリストは有効に活用できると考えられた。

MedCSC からは、MedCSC や情報処理安全確保支援士会（JP-RISSA）が医療情報セキュリティ人材の登録や医療機関向け相談窓口の設置を行い、医療機関等と情報セキュリティ人材との情報交換プラットフォームを構築する案が示された。医療情報セキュリティ人材の登録に際し、本研究班で定める教育コンテンツの受講や「指導的な立場の医療機関」での実地研修、上級医療情報技師や医療情報技師の資格取得を推奨し、受講情報等を管理することができれば、きめ細かい人材斡旋が可能になると考えられた。

これらの人材検索システムは、医療情報セキュリティ人材が不足する保健医療福祉領域にとって大変有用な仕組みと考えられるため、本研究班終了後も、IPA、MedCSC と継続的に議論を続ける必要があると考えられた。

7. 情報セキュリティ人材を継続して雇用・配置するための課題の調査（担当：武田・鳥飼・谷川・川眞田・肥田）

MedCSC からは、医療情報セキュリティ人材について、適任者の圧倒的不足と低い人材流通性が課題として挙げられた。人材難の背景としては、医療職と事務職で構成する組織では、IT 職のポストが限定的で待遇も良くないこと、IT 人材は組織内でのキャリアが頭打ちで、人材が流動せず、若手が入りにくいこと、より高い評価、報酬を得たい人材は医療機関に留まらず民間大手等に流出すること、社会的にセキュリティ人材不足が継続する中で、施設それぞれで専門性の高い人材を正規職員で雇用、厚遇することは困難であること、が指摘された。

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（表2）。しかし、医療機関においては医療系専門職を持つ医療情報セキュリティ人材は医療系専門職の給与体系の維持が想定されること、医療系専門職を持たない医療情報セキュリティ人材は事務職の給与体系が適応されることが想定される。このため、単施設で、医療情報セキュリティの知識、スキルセット、実行レベルを有することで待遇改善は容易でないと考えられた。

もう一つの課題は医療情報セキュリティ人材のキャリアパスの提示である。医療系専門職を持つ医療情報セキュリティ人材はそれぞれの部門の所属となることが多く、医療情報セキュリティの知識を持つことよりも、それぞれの専門職の技能を持つことが、キャリアパスでは優先される。医療系専門職を持たない医療情報セキュリティ人材は事務部に配属されることが想定されるが、特に公的医療機関等では事務職は様々な部署を経験することがキャリアパスに求められることが多い。せっかく、医療情報セキュリティの学習を行った事務職員が数年後に全く違う部署に異動となることも十分に考えられる。

表2. 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	41.8	12.5	6,849.1

ント・設計者			
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

7-1. 安定した情報セキュリティ対策の維持に向けた情報セキュリティ人材の確保

医療情報セキュリティ人材の不足や雇用経費の確保が困難であることから、医療情報セキュリティ人材が 1 名で組織の情報セキュリティ対策を担うことが少なくない。しかし、これには大きなリスクがあることを認識する必要がある。

医療機関における情報セキュリティ対策は各医療機関の医療情報システムの特性や運用に合わせて講じる必要があるため、情報セキュリティ人材が適切な情報セキュリティ戦略を講じるためには、ある程度当該医療機関への勤務経験が必要となることが多い。情報セキュリティ人材が退職する場合、医療情報セキュリティ人材が不足する現状から、すぐに後任が見つからないケースが想定される。また、すぐに後任が見つかったとしても、自施設の情報セキュリティ対策を十分に引き継ぐことができない可能性も想定される。

「指導的な立場の医療機関」は言うまでもなく、「自施設の情報システムを守ることができる医療機関」については、情報セキュリティ人材を育成し、地域の医療機関に提供する役割が望まれる。「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」で最低限の人数の情報セキュリティ人材で情報セキュリティ管理を行った場合、自施設の情報セキュリティ対策を賄うことに精一杯となり、他施設への人材提供は困難となる。

以上の理由から、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」は、複数の情報セキュリティ人材を雇用することが推奨される。複数の医療情報セキュリティ人材を雇用することで、医療情報セキュリティ人材間での知識の共有や人材育成を行うことが可能となる。医療情報セキュリティ人材の急な休職や退職があった場合も、安定した情報セキュリティ対策を維持できる。

7-2. 情報セキュリティ人材の雇用経費の確保

医療機関においては、情報セキュリティ人材の配置や情報セキュリティ対策への設備投資について、費用の確保が課題となる。医療機関で医療安全人材や感染症対策人材が定着していることは、医療機関における人材確保の

必要性はもちろんのこと、医療安全対策加算や感染対策向上加算での施設基準や診療報酬によることが大きいことは間違いない。情報セキュリティ人材の確保においても、加算がつくことで医療機関は施設基準を満たすように努力することが想定され、医療機関での情報セキュリティ対策の向上に大きく貢献することが期待される。また、加算が付くことは、医療領域外の情報セキュリティ人材が医療領域に参入するきっかけとなり、人材不足が解消する可能性も期待される。

本研究班で求める医療情報セキュリティに関する資格や試験の取得には、教育の受講、資格、試験の取得に向けた学習に対する多大な労力と、受験費用、資格取得後の資格の維持費用が発生する。このため、資格、試験取得後も待遇が変わらなければ、資格、試験の取得は進まないと考えられる。

私立の医療機関や医療機関から独立した法人等の中央組織では医療情報セキュリティ人材が保有する知識、スキルセット、実行レベルに応じた給与を設定することができる可能性はあると思われる。一方、公的医療機関では給与水準が医療系資格により決められているため、待遇改善は容易でないことが想定される。どの分野でも情報セキュリティ人材は不足している。このため、待遇改善がない場合、せっかく育成した医療情報セキュリティ人材が他施設や医療領域外に流出する懸念がある。特に、医療領域外への流出は避ける必要がある。

MedCSC からは、圧倒的な人材不足がある中、医療情報セキュリティを専門とする高度人材の兼業促進、ポスト創出のためには、医療機関では本務先では正職員として勤務する傍ら、週 1 から数日、他施設へ非常勤に出ることで、副収入を得つつ、支援先の調達や運用、人材育成に寄与する案が提案された。また、本務先の施設では、後進へのタスクシフト、育成を進めることで組織の代謝を促すことが可能である。このようなIT専門職の働き方改革には、柔軟な雇用形態についての支援、制度化の検討が必要と考えられた。

7-3 医療機関の情報セキュリティ対策を支援する行政、団体の設置

MedCSC から、行政、団体が情報セキュリティ対策を支援する組織を設置し、セキュリティアドバイザーを配置または連携することで、地域内施設の支援を行う方法が提案された。このことで、中小規模医療機関で対応力が十分でないところへ、地域医療の枠組みに準じた支援体制を構築することができる。また、厚生労働省から一方向の情報伝達のみではなく、地域医療行政の責任として分担される実効的な支援体制を構築することが可能である。このような仕組みの構築には、各自治体、団体にて医療情報セキュリティ人材雇用のための予算化、組織内担当ポストの整備や、情報セキュリティ人材間で連携するネットワークづくりが必要になると考えられた。

7-4. 医療機関における情報セキュリティ人材のキャリアパス

「医療機関におけるサイバーセキュリティ対策チェックリスト」では医療機関に医療情報システム安全管理責任者を置くことが求められている。本研究班で行った調査で、多くの医療機関で医療情報システム安全管理責任者を配置が進んでいるが、病院長や副病院長、事務長など病院執行部がその役割を担うことが多く、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い。

医療機関が情報セキュリティ対策を進めるためには、病院執行部の意思決定が重要であり、意思決定者が医療情報システム安全管理責任者となることの意義は大きい。一方、意思決定者が情報セキュリティに対する知識が乏しい場合、正しい意思決定を行うことができるかについては課題が残る。

大企業などでは組織のデータを保護するために使用するサイバーセキュリティ戦略を設計し、組織全体のリスクを評価して、サイバー防御を改善する責任をもつ CISO（Chief Information Security Officer）を配置することが求められる。医療機関においても、医療情報システム安全管理責任者が CISO として活動することで、確実な情報セキュリティ対策が進むと考えられるが、今すぐ、CISO の候補となる人材を確保している医療機関は多くないと考えられる。そこで、将来、CISO の候補となる人材を育成することが求められる。

本研究班では、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」に医療情報システム管理部門を設置することを求めている。医療情報システム管理部門の設置により、組織としては、確実な情報セキュリティ戦略の設計を求めることが可能となる。雇用される Group A 人材、Group B 人材に対しては、医療情報システム管理部門の長として登用されることを想定するキャリアパスを提示することができ、部門長あるいはさらに上の立場で病院運営に関わることは、情報セキュリティ人材が CISO の役割を担う組織づくりにつながると考えられる。

本研究班では、医療情報システム管理部門に「統括情報セキュリティ責任者」、必要に応じて「統括情報セキュリティ責任者」の補助者を配置することを求めている。医療機関における情報セキュリティ対策は迅速な対応が求められ、人材育成を待つ時間はない。このため、現時点においては情報セキュリティ戦略に向けた意思決定部分を統括情報セキュリティ責任者が、戦略立案に向けた知識、技能部分を Group A 人材、Group B 人材が担うことを想定される。Group A 人材、Group B 人材が統括情報セキュリティ責任者を補助する立場で仕事をすることで情報セキュリティ戦略に向けた意思決定を学び、将来的には医療機関における CISO の役割を担うことができる人材として育成されることが期待される。

全ての Group A 人材、Group B 人材が部門長、CISO となるわけではない。「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で育成された Group A 人材、Group B 人材が、より良い待遇で地域の医療機関や医療情報セキュリティを支援する行政、民間事業者に就職する、あるいは個人開業するキャリアパスが想定される。このような事例を積み重ねることは、医療情報セキュリティ人材を目指す若手が、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で教育を受け、医療情報システム、情報セキュリティに関する資格、試験を取得する大きなモチベーションになる。

「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」は、複数の情報セキュリティ人材を雇用しており、人材育成、知識の共有ができていれば、このような医療情報セキュリティ人材の退職にあたっても、情報セキュリティ対策を安定して継続することができる。これらの医療機関は欠員となった枠を使って若手の情報セキュリティ人材を雇用し、教育をすることで、当該施設の組織の若返りをはかることが可能となる。

一方、Group C 人材には異なるキャリアパスを示す必要がある。「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」では CISO を置くことは現実的でなく、外部 CISO の力を借りて、情報セキュリティ戦略を立案することが想定される。このため、「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」では診療放射線技師や臨床工学技士といった医療系専門職を Group C 人材として育てることが現実的である。また、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」においても、医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門に Group C 人材を配置が求められるが、それぞれの部門で働く医療系専門職から Group C 人材を育成することが想定される。多くの医療機関ではぎりぎりの人数で業務が遂行されているが、Group C 人材を配置することでプラス1の雇用枠が確保できれば、本来業務の負担軽減、業務拡大につながることが期待される。近年、部門業務の遂行には部門システムの有効活用が必須となっており、部門システム戦略に関わることになる Group C 人材は部門の管理者として育成されることが期待される。

8. 情報セキュリティ人材の育成と配置に向けた提言（担当：武田・鳥飼・谷川・川眞田・肥田）

8-1. 「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」（添付資料 2）

本研究班では、「組織体制」、「人材」、「教育」に着目して、整理を行った。

「組織体制」は「1. 医療機関ごとの役割分担や配置すべき医療情報セキュリティ人材」として、① 指導的な立場の医療機関、② 自施設の情報システムを守ることができる医療機関、③ 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を定義し、それぞれ、【自施設での組織体制】、【「指導的な立場の医療機関」間の取り組み】、【地域の医療機関との連携】について取りまとめた。

「人材」については、「2. 医療情報セキュリティ人材が持つべき知識や備えるべきスキル、実行レベル」として、① Group A 人材、② Group B 人材、③ Group C 人材を定義し、それぞれに対し、【医療情報システムに対する知識の担保】、【情報セキュリティに対する知識の担保】、【求められる業務】について取りまとめた。

「教育」については、「3. 医療情報セキュリティ人材が受けるべき教育について」として、① Group A 人材、② Group B 人材、③ Group C 人材が受けるべき教育の【到達目標】と【教育カリキュラム】を取りまとめた。

最後に補足事項として、「4-1. 医療情報セキュリティ人材が持つべき知識やスキルセットについて」、「4-2. Group A 人材の安定した雇用に向けて」、「4-3. 個人、事業者等の情報セキュリティ人材の活用について」の記述を行った。

8-2. 「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」（添付資料 3）

本研究班が実施した「情報セキュリティ人材配置に関するアンケート調査」では、保健医療福祉分野の情報システムの特性を理解しながら、情報セキュリティの知識を持つ人材の医療機関への配置は十分ではないことが明らかとなっている。このため、「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」は、将来の資格保有を推奨しながら、まずは各医療機関

が情報セキュリティ人材の配置を進めることができるように、実務経験や教育の受講を重視する提言となっている。医療機関や医療機関に雇用された情報セキュリティ人材は、最新の医療情報システムや情報セキュリティに関する知識の獲得や、他医療機関の取り組みや経験の共有により、組織、個人として成長し、将来、医療機関でより確実な情報セキュリティ対策を確保するための PDCA サイクルを実行するための提言となっている。

「1. 医療情報セキュリティ人材の育成と情報セキュリティに関する最新の知識の確保」では「保健医療福祉分野の情報システムの特性の理解」、「情報セキュリティに対する知識の担保」に加え、「最新の情報セキュリティの知識の担保」について記述を行った。

「2. 情報セキュリティ人材の育成と医療機関等におけるサイバーセキュリティ対策の質的向上」では。「指導的な立場の医療機関」に配置される「Group A 人材」を中心に、各組織に配置される「Group B 人材」、「Group C 人材」が情報共有や他施設での情報セキュリティ対策を学びながら、地域として情報セキュリティ対策の質の向上を行うことを記述している。

「3. サイバー攻撃を想定した事業継続計画（BCP）の策定とサイバー攻撃合同訓練」では、IT-BCP の策定と、相互チェック、セキュリティチェック、「指導的な立場の医療機関」がサイバー攻撃合同訓練による IT-BCP の見直しを行うことが記載されている。

「4. 情報セキュリティ人材の適正配置、キャリアパス、医療領域からの人材流出の防止」では、「情報セキュリティ人材のキャリアパス」、「情報セキュリティ人材の待遇」、「人材セキュリティ人材の医療領域からの流出防止」、「情報セキュリティ人材の適正配置と継続的な確保」について取りまとめている。

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、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 2、Group C 人材はレベル 1 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 B は情報セキュリティマネジメント試験、Group C は IT パスポート試験が対応する。

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。

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

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、実行レベルの検討を行った結果、医療情報セキュリティ人材は、医療情報技師、上級医療情報技師、情報処理安全確保支援士、情報セキュリティマネジメント試験など、医療情報セキュリティの知識、スキルセット、実行レベルを担保する資格、試験を保有することが望まれる。一方、情報セキュリティ人材配置に関するアンケート調査ではこれらの資格を保有する医療情報セキュリティ人材は医療機関にほとんど配置されていないことが明らかになった。

資格、試験の保有には時間が必要となる。一方、医療機関における情報セキュリティ対策は少しでも早く進める必要があり、医療情報セキュリティに関する教育を実施することが現実的と考えられた。

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。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 などが実施されている。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。そこで、Group A 人材、Group B 人材、Group C 人材に対応する医療情報セキュリティ人材の育成カリキュラムを開発した。医療情報システムに対する資格と情報セキュリティに対する資格の保有状況に合わせて、受講するべきコンテンツを明確にした。「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」では、医療情報システムに対する知識の担保、情報セキュリティに対する知識の担保、それぞれに対し、保有すべき資格や試験、または教育受講、または実地経験または実地研修の修了を記述した。

医療情報技師育成部会では生涯研修セミナー・e-Learning で情報セキュリティに関する教育コンテンツを公開している（https://www.hcit.or.jp/seminars/）。生涯研修セミナーでは、「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～」、「みんなで議論して考える～IT-BCP 策定と訓練～」、e-learning では「いまさら聞けない～ネットワーク編～」といったコンテンツが用意されている。本研究班で開発した育成カリキュラムが整備されているわけではないが、今後、医療樹法技師育成部会が育成カリキュラムを整備することが期待される。

MedCSC から医療領域への参入を考える情報処理安全確保支援士に対し、特定講習として医療に特化した情報セキュリティコンテンツを提供する案が出されたが、本研究班で開発した育成カリキュラムは特定研修に活用することが可能と考える。F 医療情報技師育成部会が医療情報システムの知識を担保するコンテンツを整備し、IPA や MedCSC が情報セキュリティに関する知識を担保するコンテンツを整備するといった協力体制を作ることができれば、効率的に教育コンテンツの作成、維持管理ができることが期待される。

作成した育成コンテンツは、診療情報管理士の 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同様に、医療情報技師、

あるいは診療情報管理士で医療情報セキュリティコースを作り、受講を管理する方法が考えられる。医療安全領域や感染症対策領域では、医療安全対策加算や感染対策向上加算で講習の受講が義務付けられている。すでに「医療安全管理者養成講習会」や「感染対策担当者のためのセミナー」を提供、受講管理するシステムが構築されているため、このシステムを使って医療情報セキュリティコースの提供や受講管理をする方法も考えられるかもしれない。

5. 最新の情報セキュリティの知識の担保

情報セキュリティ対策に向けて、情報セキュリティ人材だけでなく、全ての病院職員がそれぞれのレベルに応じて、情報セキュリティに対する最新の知識を確保する必要がある。情報セキュリティの知識の獲得に向けては、内閣府サイバーセキュリティセンター、厚生労働省医療機関向けセキュリティ教育支援ポータルサイト、IPA などが最新の情報セキュリティに関する情報を発信している。また、CISSMED (Cyber Intelligence Sharing SIG for Medical)などを利用し、情報セキュリティ人材間での知識共有を行うことが想定される。全ての医療機関の情報セキュリティ人材が等しく、自律的に最新の情報を担保することは容易ではないと考えられる。

「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」では、「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築することを求めている。さらに、「指導的な立場の医療機関」および Group A 人材は定期的に情報セキュリティに関するカンファレンスを開催すること、「自施設の情報システムを守ることができる医療機関」や「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」がこのカンファレンスに参加することを求めた。「指導的な立場の医療機関」および Group A 人材はカンファレンス開催に向けて、最新の情報セキュリティに関する知識の獲得に取り組むことが想定され、カンファレンスに参加する情報セキュリティ人材はカンファレンスで最新の知識を獲得することが期待される。

「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」では、「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」、「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」、全ての医療機関に対して自施設の病院職員教育を求めている。なお、Group A 人材については、自施設だけでなく他施設の職員教育を求めている。Group C 人材が自ら職員教育を行うことが難しいケースを想定して、Group A 人材への講演依頼や e-Learning の活用も想定をしている。

6. 情報セキュリティ人材の育成と医療機関等におけるサイバーセキュリティ対策の質的向上

医療機関等におけるサイバーセキュリティ対策については、医療情報システムの安全管理に関するガイドラインのうち優先的に取り組むべき事項が「医療機関におけるサイバーセキュリティ対策チェックリスト」として取りまとめられた。各医療機関ではチェックリストに従いサイバーセキュリティ対策が進められているが、具体的な対策は各医療機関の情報セキュリティ担当者の判断に委ねられており、有効な対策がどこまでとられているかは医療機関ごとに異なることが想定される。全国の医療機関が広くサイバーセキュリティ対策について向上するためには、各医療機関のサイバーセキュリティ対策の質的評価や、グッドプラクティスの共有などの仕組み

が求められる。

「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」では「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築すること、互いの施設の医療情報システムの相互チェックを実施することやGroup A 人材がその実務を担当することを求めている。Group A 人材が「指導的な立場の医療機関」の情報セキュリティ対策の相互チェックを行うことは、対象施設の情報セキュリティ対策の向上に向けた具体的なアドバイスだけでなく、自施設の情報セキュリティ対策の向上に活かすことができると考えられる。また、Group A 人材は「指導的な立場の医療機関」間の相互チェックで得られた知見を用いて、「自施設の情報システムを守ることができる医療機関」に対するセキュリティチェックを実施することが可能となる。「自施設の情報システムを守ることができる医療機関」の Group B 人材はセキュリティチェックを通じ、Group A 人材との交流や情報共有を行うことが可能となる。このように、数年間は医療機関同士がお互いの情報セキュリティ対策を学ぶ形で、各医療機関の情報セキュリティ対策の質を高めるとともに、Group A 人材、Group B 人材の育成につながると考える。さらに、「指導的な立場の医療機関」同士の相互チェックや「自施設の情報システムを守ることができる医療機関」に対するセキュリティチェックを重ねることにより、保健医療福祉分野における情報セキュリティ対策の水準を定めることができる。「指導的な立場の医療機関」は、将来、医療機関等における情報セキュリティ監査基準として取りまとめることが期待される。情報セキュリティ人材を配置する医療機関は、「医療機関におけるサイバーセキュリティ対策チェックリスト」に加え、相互チェックやセキュリティチェックでの経験（将来的には情報セキュリティ監査基準）を活かし、自施設の医療情報システムの内部監査（自己点検・評価）を行い、外部評価（自施設に対する相互チェック、セキュリティチェック）の結果と合わせて、日々の情報セキュリティ対策向上につなげることが求められる。

医療情報システムの保守運用について外部委託を行っている医療機関は少なくない。既に導入されている医療情報システムに対して適切なセキュリティ対策を講じることは、契約や運用面、費用面、導入システムでの制限事項などの理由により、容易でないケースが想定される。日々の情報セキュリティ対策が大切であることは当然のことであるが、大きく情報セキュリティ対策を向上させるために、医療情報システム全体の運用や契約・費用に関する現状の棚卸しが必要となる。医療機関では5、6年に一度、医療情報システムの更新が行われるが、医療情報システムの更新は情報セキュリティ対策を見直す絶好の機会となる。情報セキュリティ人材は、医療情報システム更新に向けて、自施設の医療情報システムの仕様、運用、契約を整理し、セキュリティチェックリスト、内部監査、外部監査（相互チェックやセキュリティチェック）を通じて学んだ自施設の問題点、改善点を取りまとめた上で、公的医療機関は医療情報システム仕様書、民間医療機関は医療情報システム機能要求に反映をする必要がある。仕様書の作成や機能要求を外部コンサルタント業者に委託する場合は、外部コンサルタントが情報セキュリティに対する正しい知識を保有することを確認し（できれば Group A 人材を配置するコンサルタントが好ましい）、自施設の問題点、改善点が反映される仕様書となるように、連携を密に取る必要がある。医療情報システムの保守運用を

外部事業者に委託する場合は、自施設の情報セキュリティ人材と外部事業者の役割を明確にし、契約に反映をさせる必要がある。

7. サイバー攻撃を想定した事業継続計画（IT-BCP）の策定とサイバー攻撃合同訓練

「医療機関におけるサイバーセキュリティ対策チェックリスト」ではサイバー攻撃を想定した事業継続計画（IT-BCP）の策定が求められる。厚生労働省は「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き」、「医療情報システム部門等における事業継続計画（BCP）のひな形」を公開している。サイバー攻撃の被害にあった大阪急性期・総合医療センターではホームページ上で IT-BCP が公開されている。各医療機関で策定したサイバー攻撃を想定した BCP についても「指導的な立場の医療機関」間の相互チェックや「自施設の情報システムを守ることができる医療機関」へのセキュリティチェックの対象となり、IT-BCP の質向上につながると考える。また、「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」に対しては、Group A 人材が上記取り組みを通じた獲得した知見を含め、IT-BCP の策定や改訂を支援することが想定される。

策定した IT-BCP が正しく機能するためには、サイバー攻撃合同訓練への参加が必要となる。サイバー攻撃訓練については、内閣府サイバーセキュリティセンターが重要インフラ対策として実施する全分野一斉演習への参加などを行っている状況である。災害対策については災害派遣医療チーム（DMAT）による合同防災訓練が実施されている。保健医療福祉分野により特化したサイバー攻撃訓練となるためには、医療機関がサイバー攻撃合同訓練を主催することが必要と考え、「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」では「指導的な立場の医療機関」に「自施設の情報システムを守ることができる医療機関」と合同で、サイバー攻撃合同訓練を実施することを求めた。サイバー攻撃合同訓練を繰り返すことで、有効な訓練の主催が可能となると共に、IT-BCP へのフィードバックが可能になることが想定される。

8. 医療機関で働く情報セキュリティ人材のキャリアパス

病院職員が医療情報セキュリティ人材を目指すため、新規雇用あるいは育成した医療情報セキュリティ人材が医療機関に定着するために、医療情報セキュリティ人材のキャリアパスを示す必要がある。

医療機関に医療情報システム管理部門を設置することは、医療情報セキュリティ人材の専門性を持って仕事ができる場として重要である。一部の医療機関では医療情報技師を医療技術部の所属としたり、医療情報技師長というポストを作ったりする試みが行われている。このように医療情報セキュリティ人材が事務職ではなく、新しい医療技術職として位置付けることができると、医療情報セキュリティ人材を目指す人が増えるかもしれない。医療機関が複数の医療情報セキュリティ人材を雇用し、先輩が後輩を指導する体制があれば、安心して入職ができる。

医療情報システム部門に配属された医療情報セキュリティ人材は、部門長を目指し、さらにその先として CISO として病院経営に関わることが期待される。一方、勤務する医療機関外に活躍する場があることも、様々なキャリアパスが提示できる点で大切である。医療機関の情報セキ

ュリティ対策を支援する行政組織や団体は、医療情報セキュリティ人材の受け皿となる。医療機関が複数の医療情報セキュリティ人材を雇用していれば、転職に対するストレスが少なく、医療機関も当該人材の退職を機に、医療情報セキュリティ人材の世代交代を進めることができる。

9. 医療領域の他施設で活躍する医療情報セキュリティ人材の活用

本研究で定義するGroupA人材、GroupB人材は医療情報セキュリティに対する高い知識とスキルセットと実行レベルが要求される。保健医療福祉領域の情報セキュリティ人材は不足しているため、これらの人材を確保できない医療機関が相当数でることが予想される。そこで、医療領域内外で活躍する外部情報セキュリティ人材の活用が課題となる。

「指導的な立場の医療機関」は地域の医療機関の情報セキュリティ対策の指導や人材育成が求められることから、Group A 人材の配置が必須である。一方、「自施設の情報システムを守ることができる医療機関」は、他施設、団体の Group A 人材と顧問契約等を結び、自施設のGroupC人材と連携しながら、情報セキュリティ対策を進めることが許容される。この Group A 人材の所属は「指導的な立場の医療機関」、「同一法人、同一グループなどの中央組織」、「医療機関に情報セキュリティサービスを提供する民間事業者」、「医療機関に情報セキュリティサービスを提供する個人事業者」が想定される。こういった外部組織があることは、医療情報セキュリティ人材に医療機関以外でのキャリアパスを提示する観点からも大切である。

10. 医療領域外で活躍する情報セキュリティ人材の活用

医療領域以外で活躍する情報セキュリティ人材については、情報セキュリティ人材への医療情報システムに関する知識の担保とこれらの人材の検索が課題となる。前者に対しては、医療情報技師や上級医療情報技師の資格取得の推奨や、本研究班で定める Group A 人材に対する教育コンテンツの受講、「指導的な立場の医療機関」が提供する実地研修の修了が想定される。MedCSC や医療情報技師育成部会が教育コンテンツを整備し、IPA の協力のもと、情報処理安全確保支援士の特定研修に活用することができれば、医療情報セキュリティ人材を増やすことができると考えられた。後者に対しては、IPA が作成を検討している登録セキスペアクティブリストの活用や MedCSC が検討している医療情報セキュリティ人材の登録や医療機関向け相談窓口の活用が有効と想定された。

医療機関に対するサイバーインシデントは社会的なインパクトが大きい。本研究班の提言は医療機関側から情報セキュリティ人材を必要としている明確なメッセージとなる。また、本研究班で提案する兼業を許すことで、本務先以外から副収入を得ることや、医療機関の情報セキュリティ対策を支援する行政組織や民間事業者、個人事業者が広がることで、現在活躍している領域と同程度の報酬を得ることができる可能性は十分にある。

情報処理安全確保支援士、登録セキスペへのメッセージ発信や情報処理安全確保支援士の特定講習に医療情報セキュリティに特化したコンテンツの組み込み、登録セキスペアクティブリストを使った医療情報セキュリティ人材の検索など、IPA や MedCSC とは継続的に議論を重ねる必要がある。

11. 医療情報セキュリティ人材の医療領域外への流出の防止

医療情報セキュリティ人材が不足する状況で、医療領域外で活躍する情報セキュリティ人材の医療領域への参入を促すことは必要であるが、せっかく育成した医療情報セキュリティ人材が医療領域外に流出することを防ぐことは、より大切となる。

MedCSC からは、医療系専門職と事務職で構成する医療組織では、IT 職のポストが限定的で待遇も良くないこと、IT 人材は組織内でのキャリアが頭打ちで、人材が流動せず、若手が入りにくいこと、より高い評価、報酬を得たい人材は医療機関に留まらず民間大手等に流出すること、社会的にセキュリティ人材不足が継続する中で、施設それぞれで専門性の高い人材を正規職員で雇用、厚遇することは困難であること、が指摘されている。

本研究班で示したとおり、医療機関内外で医療情報セキュリティ人材が活躍できるキャリアパスの実現、他領域に劣らない報酬を得る仕組みの構築を実現できる必要がある。

12. 情報セキュリティ対策経費、医療情報セキュリティ人材の雇用経費の確保

「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」は医療情報セキュリティ対策を安定して継続するためには、複数の医療情報セキュリティ人材を確保することが好ましい。また、医療情報セキュリティ人材が情報セキュリティ対策を施すには設備投資が必要となる。医療機関はこれらの経費を確保する必要がある。本研究班で情報セキュリティ対策の向上で参考にした医療安全領域や感染対策領域では、それぞれ医療安全管理体制加算や感染対策向上加算が診療報酬として設けられている。

診療報酬では、診療録管理体制加算で医療情報システム安全管理責任者の配置を求めているが、サイバーセキュリティ対策の知識や技術の保有を担保できていない。また、サイバーセキュリティに関する評価対象は診療録としての管理に留まらず、施設内での情報の保全、診療連携など施設外にも及ぶプロセスや質管理に及ぶ幅広いものである。それを診療録の内容に関する情報管理を主たる業務とする診療情報管理人材でカバーすることは不可能である。このため、サイバーセキュリティ対策向上加算といった新たな診療報酬の枠組みが必要と考える。情報セキュリティ対策加算が認められれば、医療情報セキュリティ人材の雇用が進み、医療機関の情報セキュリティ対策は進むことが期待される。また、医療領域を目指す情報セキュリティ人材が増えることが期待される。

情報セキュリティ対策は組織として実施するもので、その費用を患者から診療報酬として請求するものではないかもしれない。しかし、医療機関が適切な情報セキュリティ人材を配置しないことで、患者への直接のデメリットが生じうる。

医療領域では官民でクラウドサービスを用いた医療 DX が推進されているが、サイバーセキュリティの知識が十分でない医療機関では、適切なクラウドサービスへの接続の判断ができない。その結果、クラウドサービスを利用しない医療機関では、患者がよりよい医療サービスを受ける機会が奪われることになる。不適切なクラウドサービス利用が行われた場合、サイバーインシデントや診療情報紛失・漏えいのリスクに晒されることになる。更に、医療機関がサイバーインシデントの被害にあうと、表3に示すような患者へのデメリットや公費支出のリスクが発生

する。医療情報セキュリティ人材の適切な配置により、医療機関のサイバーセキュリティ体制は強化され、医療 DX サービスに対する患者の信頼が醸成され、患者が安心して医療サービスを受けることができるようになる。

表 3. サイバーインシデント被害時の患者や公費支出へのリスク

時期	患者や公費支出のリスク
超短期	救急医療等が提供できず、命を救う機会が奪われかねない
	緊急性の高い患者の搬送で公費支出がかさむ
短期	患者情報のダークウェブ等への漏洩による患者への直接被害
	透析等の診療継続ができず、遠隔地への患者搬送が必要になる
中長期	過去の診療記録が失われ、継続診療に不具合が生じる
	デジタルフォレンジック・システム復旧・BCP 復旧中の大幅減収等で財政的に医療継続が困難になり、医療機関が失われかねない

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。

医療情報セキュリティ人材を、Group A 人材、Group B 人材、Group C 人材に分け、それぞれの人材が医療機関で果たすべき役割、保有すべき資格や試験、受けるべき教育や実務経験を整理した。

医療機関を「指導的な立場の医療機関」、「自施設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」に分類し、それぞれの医療機関に医療情報システム管理部門の設置と適切な医療情報システムの特性を理解した情報セキュリティ人材を配置し、情報セキュリティ対策を講じる。外部評価として「指導的な立場の医療機関」間の相互チェックや「指導的な立場の医療機関」によるセキュリティチェックを実施し、「指導的な立場の医療機関」が主催するセキュリティカンファレンスやサイバー合同訓練を定期的（年に 1 回）に開催することで、各施設は自施設のサイバーセキュリティ対策の向上に努める。また、「指導的な立場の医療機関」に配置する Group A 人材が他施設のセキュリティ人材に対し、情報共有、指導、教育を行う体制を構築することでセキュリティ人材の育成を行うこととした。このような、医療情報セキュリティ人材は圧倒的に不足しているため、正しい知識を持つ人材育成のための教育プログラムを開発した。

本研究班では医療機関の職員の人材育成を想定しているが、外部情報セキュリティ人材の活用も必要となる。このため、IPA や MedCSC との協力が有効であると考えられた。

医療機関で安定した情報セキュリティ対策を講じるためには、複数の情報セキュリティ人材の確保が必要と考えられ、雇用費用の確保が課題となった。これらの人材が医療機関で継続的に雇用するために、情報セキュリティ人材の待遇改善とキャリアパスの提示が必要と考えられた。

これまでの研究成果を取りまとめ、「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」と「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」の作

成を行った。

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)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

(3)武田 理宏、情報セキュリティ人材の育成と適正な配置に向けて、日本病院会雑誌「メディカルジャパン大阪」、in press

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
(9)デジタル化社会における臨床工学技士の未来像～医療 DX とセキュリティ対策～、第 34 回日本臨床工学会、パネルディスカッション、2024 年 5 月、福井、(座長:**肥田 泰幸**、川崎路浩)
①**武田 理宏**、**鳥飼 幸太**、**谷川 琢海**、**川眞田 実**、**肥田 泰幸**、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岡田 未奈、臨床の視点から考える臨床工学技士の医療DXとサイバーセキュリティー資格取得の意義を再考するー
③田中 健、IT パスポート取得までの道
④相原 瞳、安藤 勝信、職場の IT 知識向上に貢献するために～IT パスポート受験～
(10)医療 DX 推進体制整備加算・診療録管理体制加算がもたらすインパクト、第28回日本医療情報学会春季学術大会、2024 年 6 月、千葉、(オーガナイザー:**鳥飼 幸太**、座長:**武田 理宏**、演者:中島 直樹、横井 英人、小笠原 克彦、**谷川 琢海**、**鳥飼 幸太**)
(11)情報セキュリティ人材の育成と適正な配置に向けて、第 44 回医療情報学連合大会、2024 年 11 月、福岡、(オーガナイザー、座長:**武田 理宏**、座長:**鳥飼 幸太**)
①鳥飼 幸太、医療機関規模ならびに機能に応じたセキュリティ担保の分類に関する検討
②**谷川 琢海**、医療情報技師が情報セキュリティ人材として医療機関および地域で活躍することへの期待と課題
③**川眞田 実**、診療放射線技師が取り組む情報セキュリティ人材育成
④**曽根 玲司那**、情報セキュリティ人材の育成と適正な配置に向けて ―臨床工学技士の立場から―
⑤**武田 理宏**、情報セキュリティ人材の育成と適正な配置に向けて
(4)第 3 回医療機関のセキュリティセミナー 脅威への新たな取り組みに向けて(主催:株式会社シードプランニング、座長:**武田 理宏**)、2024 年 11 月、東京
①高柳 大輔(情報処理推進機構(IPA))、最近のサイバー攻撃の動向と対応策
②須藤 泰史(つるぎ町病院事業管理者 つるぎ町立半田病院)、大規模インシデントからの復旧と再発防止に向けて
③橋本 智広(大津赤十字病院)、現場目線で考える医療機関の情報セキュリティ対策 ～今、すべきことを再認識する～
④パネルディスカッション 医療現場のセキュリティ体制を確保するための”壁” を乗り越えるには？(モデレーター:**武田 理宏**)
(12)**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、全国自治体病院協議会 医療 DX 委員会、2025 年 1 月、Web
(13)**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、第 47 回兵庫医療情報研究会、2025 年 2 月、姫路

(14)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、第 204 回医療情報システム研究会、2025 年 2 月、大阪
(15)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、第 11 回 メディカルジャパン 大阪(医療・介護・薬局 Week 大阪)、2025 年 3 月、大阪
(16)谷川 琢海、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に関する報告、医療 DX 教育研究センター シンポジウム 2025、第1部【医療サイバーセキュリティに関する最近の話題】、2025 年 3 月、Web
(17)セキュリティ人材の育成と適正な配置、関西健康・医療創生会議オンラインセミナー、2025 年 6 月(予定)
①大道 道、演題未定
②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
③パネルディスカッション
(18)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、全国自治体病院協議会富山県支部講演会、2025 年 6 月(予定)、富山
(19)谷川 琢海、医療機関で活躍するセキュリティ人材の重要性と育成、第 100 回日本医療機器学会大会、2025 年 6 月、横浜
(20)サイバーセキュリティ人材育成の最前線～厚生労働科学研究武田班報告より～、第 29 回日本医療情報学会春季学術大会、2025 年 7 月(予定)、仙台、(オーガナイザー、座長:武田 理宏)
①鳥飼 幸太、(仮)医療分野のサイバーセキュリティ対策の現状や最新の取り組み
②高柳 大輔(情報処理推進機構(IPA))、(仮)IPA が育成するセキュリティ領域の高度専門人材の取り組み
③武田 理宏、(仮)情報セキュリティ人材の育成と適正配置
④谷川 琢海、(仮)医療情報セキュリティに関わる人材が受けるべき教育
⑤指定発言:横井 英人(香川大学)、(仮)日本医療情報学会保険委員会としての取り組み

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

「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」

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班
（令和 7 年 5 月 30 日）

初めに

医療機関の医療情報システムがサイバー攻撃の被害にあった場合、医療情報システム停止により診療業務の継続が困難になる可能性と、医療情報システムで管理される患者情報の紛失、外部への漏えいの可能性がある。

患者情報の紛失、外部への漏えいの可能性を考えると、医療情報システムを用いて診療を行う全ての医療機関は、情報システムに対して適切なセキュリティ対策を施す必要がある。

一方、診療業務の継続が困難になる可能性については、規模が大きい医療機関ほど、医療情報システムへの依存度が高くなるため、診療継続が困難になる可能性が高い。また、医療機関の規模に関わらず、診療継続が困難となった際、その地域の医療提供への影響が大きい医療機関（他医療機関で代替の診療を提供することができない）と小さい医療機関（他医療機関が代替の診療を提供することができる）が存在する。このように、地域ごとの医療機関の役割や規模に応じて、重点的に情報セキュリティ対策を施す必要のある医療機関が存在する。

保健医療福祉分野における情報セキュリティ人材は、保健医療福祉分野の情報システムの特性を理解していることと情報セキュリティに対する知識の双方が必要となる。このような人材は、保健医療福祉領域において、ほとんど存在しないのが実情である。このため、数の少ない医療情報セキュリティ人材を、医療継続が必要不可欠な医療機関に重点的に配置することが必要となる。

一方、全ての医療機関において最低限求められる情報セキュリティ対策を行う必要がある。このため、医療情報セキュリティ人材が配置された医療機関やその人材は、自施設だけでなく、地域の他医療機関に対して情報セキュリティ対策の指導やアドバイスを行うことが求められる。さらに、これらの医療機関や医療情報セキュリティ人材は、新たな医療情報セキュリティ人材の育成に向けた取り組みを平行して行うことが求められる。

このように、医療機関ごとの点ではなく、地域として面で、情報セキュリティ対策を施しながら、人材育成を平行して進めることで、将来的には多くの医療機関に医療情報セキュリティ人材が充填され、患者に対して安全、安心な医療が提供できることを期待する。

１．医療機関ごとの役割分担や配置すべき医療情報セキュリティ人材

医療機関を「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」、「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」に分け、その役割や配置すべき医療情報セキュリティ人材の整理を行った。

各医療機関や各医療機関が配置する医療情報セキュリティ人材が果たすべき役割として、日ごろの情報セキュリティ対策を講じるところまでを考慮した。実際に情報セキュリティインシデントが発生した際は、外部からさらに専門性の高い情報セキュリティ人材が医療機関に派遣され、医療機関が配置する医療情報セキュリティ人材と協働して、医療提供機能の回復を図ることを想定している。

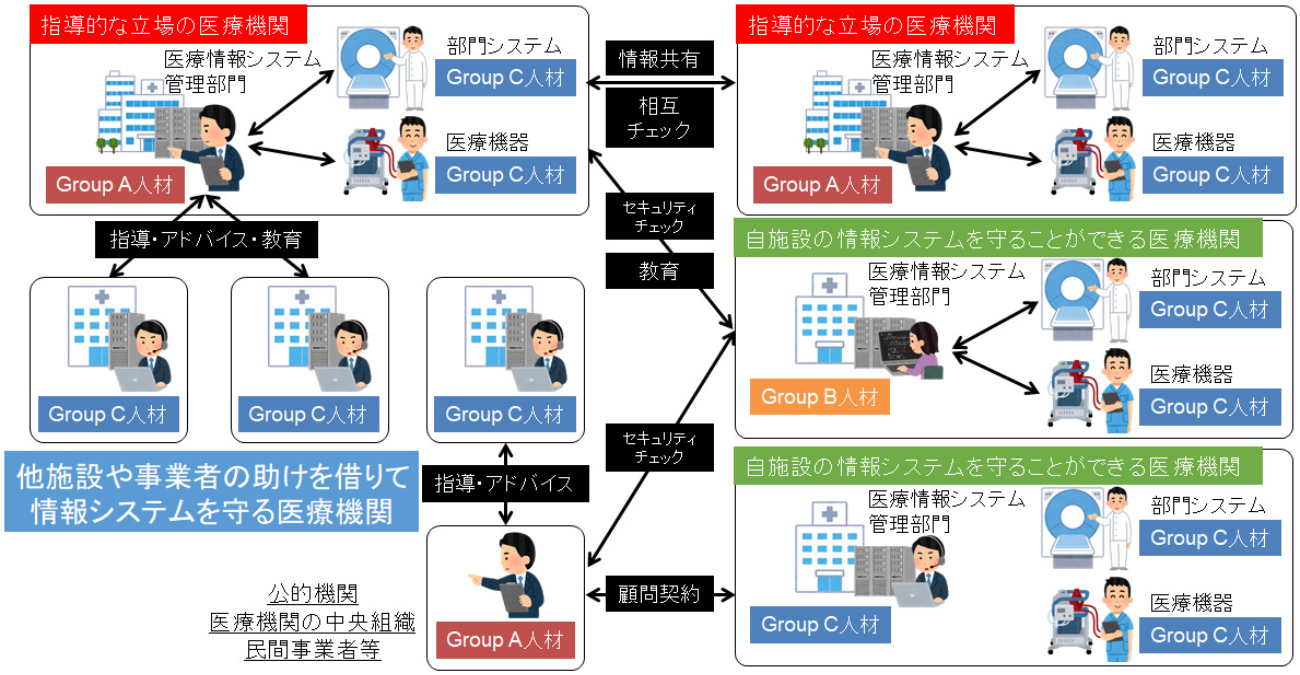

図１．医療機関ごとの役割分担や配置すべき医療情報セキュリティ人材の概念図

「指導的な立場の医療機関」の Group A 人材が中心となって、自施設、「自施設の情報システムを守ることのできる医療機関」、「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」に所属する Group B 人材、Group C 人材と協働しながら、地域の医療機関が広くサイバーセキュリティ対策を強化する。また、「指導的な立場の医療機関」は地域の医療情報セキュリティ人材の育成に努める。

① 指導的な立場の医療機関

「指導的な立場の医療機関」は、自施設の情報システムを自立的に守るだけでなく、「自施設の情報システムを守ることができる医療機関」や「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」に対して支援や教育を行うことができる医療機関である。

このため、医療情報システムと情報セキュリティに関する高い知識を有した人材（本研究班での「Group A 人材」）の配置が必要となる。

「指導的な立場の医療機関」を目指すべき医療機関として、大学病院や特定機能病院などを想定するが、その他の医療機関が「指導的な立場の医療機関」となることを否定するものではない。

将来的に、少なくとも各都道府県に 1 施設は「指導的な立場の医療機関」の配置を目指す。あるいは、自治体に医療機関を指導するセキュリティ人材を配置することも考えられる。

【自施設での組織体制】

- 医療情報システム管理部門を設置すること。
- 医療情報システム管理部門に「統括情報セキュリティ責任者」を配置すること。
  ※「統括情報セキュリティ責任者」が「医療情報システム安全管理責任者」となることも想定される。
- 必要に応じて、「統括情報セキュリティ責任者」の補助者を配置すること。
- 「統括情報セキュリティ責任者」またはその補助者は専任で医療情報システム管理に従事すること。
  ※将来的には、「統括情報セキュリティ責任者」または、その補助者は専任で医療情報システム管理に従事すること。
- 「統括情報セキュリティ責任者」または、その補助者は「Group A 人材」の資格を有すること。
  ※将来的には、「統括情報セキュリティ責任者」が「Group A 人材」の資格を有すること。
- 医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門に、「Group C 人材」を配置すること。
- 医療情報システムに関するセキュリティ委員会を設置し、「統括情報セキュリティ責任者」は病院経営層や部門に配置する「Group C 人材」と協力して、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【「指導的な立場の医療機関」間の取り組み】

- 「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築すること。
- 「指導的な立場の医療機関」間で、互いの施設の医療情報システムの相互チェックを実施すること。

【地域の医療機関との連携】

- 「自施設の情報システムを守ることができる医療機関」や「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」と合同で、定期的に情報セキュリティに関するカンファレンスを開催すること。
- 「自施設の情報システムを守ることができる医療機関」と合同で、サイバー攻撃合同訓練を実施すること。
- 他医療機関から情報セキュリティ対策に関する実地研修を受け入れる体制を有すること。
- 「自施設の情報システムを守ることができる医療機関」の情報システムのセキュリティチェックを実施できること。
- 「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」の「Group C 人材」に対し、必要時に情報セキュリティに関する助言（セキュリティチェックを含む）を行う体制を有すること。
- 「自施設の情報システムを守ることができる医療機関」や「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」に情報セキュリティインシデントが発生した際、システム復旧に向けた支援を

行う体制を有すること。

② 自施設の情報システムを守ることができる医療機関

「自施設の情報システムを守ることができる医療機関」は、自施設の情報システムを自立的に守ることができる医療機関である。

病床数に関わらず、情報セキュリティインシデントにより診療が停止した場合、地域医療に大きな影響が生じる医療機関は、「自施設の情報システムを守ることができる医療機関」を目指す必要がある。

400 床以上の医療機関については、情報システム構成が複雑となることが多く、情報セキュリティ対策が難しくなる。また、情報セキュリティインシデント発生時のシステム復旧に時間を要することが想定されるため、「自施設の情報システムを守ることができる医療機関」を目指す必要がある。

【自施設での組織体制】

- 医療情報システム管理部門を設置すること。
- 医療情報システム管理部門に統括情報セキュリティ責任者」を配置すること。
- 必要に応じて、「統括情報セキュリティ責任者」の補助者を配置すること。
- 「統括情報セキュリティ責任者」またはその補助者は専任で医療情報システム管理に従事すること。
  ※将来的には、「統括情報セキュリティ責任者」は専任で医療情報システム管理に従事すること。
- 「統括情報セキュリティ責任者」または、その補助者は「Group B 人材」の資格を有すること。
  ※将来的には、「統括情報セキュリティ責任者」が「Group B 人材」以上の資格を有すること。
  ※「指導的な立場の医療機関」や公的機関、医療機関の中央組織、民間事業者に所属する「Group A 人材」と継続的な契約する場合は、「Group C 人材」の資格を有する人材の配置で可とする。
- 医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門には、「Group C 人材」を配置すること。
- 医療情報システムに関するセキュリティ委員会を設置し、「統括情報セキュリティ責任者」は病院経営層や部門に配置する「Group C 人材」と協力し、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【「指導的な立場の医療機関」や「Group A 人材」を配置する公的機関、事業者との取り組み】

- 「指導的な立場の医療機関」が定期的に開催するカンファレンスに参加すること。
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練に参加すること。
- 「指導的な立場の医療機関」や公的機関、事業者による医療情報システムのセキュリティチェックを実施すること。

③ 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

「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」は、「指導的な立場の医療機関」や「Group

A 人材」を配置する事業者の力を借りて、自施設の情報システムを守ることができる医療機関である。
オンプレミスで医療情報システムサーバーを立てる医療機関が対象となる。
情報システム新規導入時や更新時、情報セキュリティインシデント発生時に、「指導的な立場の医療機関」や「Group A 人材」を配置する事業者から指導を受けることを想定する。
このため、「Group A 人材」との情報共有に必要な知識を有する「Group C 人材」の配置が必要となる。
※適切な契約のもと、クラウド型電子カルテを導入する医療機関は、本対象の医療機関からは外れる。
ただし、導入電子カルテベンダー等から情報セキュリティ教育を受けることは必要となる。

【自施設での組織体制】

- 「医療情報システム安全管理責任者」を配置すること。
- 「医療情報システム安全管理責任者」または、その補助者は「Group C 人材」以上の資格を有することが望ましい。
- 「指導的な立場の医療機関」または事業者の 「Group A 人材」の助けを借りて、自施設の情報セキュリティ対策を実施すること。
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策を実施していること。
- 全病院職員に対して年に 1 回以上、情報セキュリティ講習会または e-learning を実施していること。
- 自施設への情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家と協力して、医療機能の復旧に努めることができること。

【地域の医療機関との連携】

- 「指導的な立場の医療機関」が定期的に開催するカンファレンスに参加すること。
- 情報システム新規導入時や更新時は必要に応じて、「指導的な立場の医療機関」や「Group A 人材」を配置する事業者から情報セキュリティに関する指導を受けること。

２．医療情報セキュリティ人材が持つべき知識や備えるべきスキル、実行レベル

医療情報セキュリティ人材が持つべき知識やスキルセットについては、「Group A 人材」、「Group B 人材」、「Group C 人材」の 3 つに分けて整理を行った。
「Group A 人材」、「Group B 人材」、「Group C 人材」が持つべき知識、備えるべきスキル、実行レベルについては、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）に対して要求項目を整理した（別表 1)。医療系国家資格の教育カリキュラムや国家試験ごとの出題基準と出題実績、医療情報技師、診療情報管理士の教育カリキュラムや資格試験の出題基準を調査した結果、医療情報技師がもっとも情報セキュリティに関する教育カリキュラムが充実していた。そこで、上記 6 視点に対して、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（表 1、別表 2)。
「Group A 人材」、「Group B 人材」、「Group C 人材」に対し、「医療情報システムに対する知識の担保」、

「情報セキュリティに対する知識の担保」、「求められる業務」について取りまとめを行った。一人の人材が医療情報システムに対する知識と情報セキュリティに対する知識を合わせ持つことが望まれるが、同一組織内で良好なコミュニケーションが取れることを条件に、医療情報システムに対する知識を持つ人材と情報セキュリティに対する知識を持つ人材が協力して情報セキュリティ対策に取り組むことを許容することとした。

表１．医療情報セキュリティ人材が持つべき資格・知識

	医療情報システムに対する知識の担保	情報セキュリティに対する知識の担保
Group A 人材	「上級医療情報技師」相当の資格・知識	「情報処理安全確保支援士」（IPA レベル 4）相当の資格・知識
Group B 人材	「医療情報技師」相当の資格・知識	「情報セキュリティマネジメント試験」（IPA レベル 2）相当の知識
Group C 人材	「医療情報基礎知識検定試験」相当の知識	「IT パスポート試験」（IPA レベル 1）相当の知識

① Group A 人材

「Group A 人材」は医療情報システムの特性を理解した上で、自施設に対しては、自立的に情報システムのセキュリティ対策を施すこと、情報セキュリティインシデント発生を想定した診療継続計画（IT-BCP）を策定すること、情報セキュリティインシデントが発生した際には外部から派遣される情報セキュリティ専門家と協力してシステム復旧に向けた活動を行うこと、ができる人材、さらに、他施設に対しては、情報システムのセキュリティ対策や IT-BCP の策定の指導を行うこと、他施設の情報システムのセキュリティ監査を実施すること、他施設に情報セキュリティインシデントが発生した際には、当該施設に赴き、復旧に向けた活動を行うこと、ができる人材を想定する。

「Group A 人材」は、医療機関の情報セキュリティ人材の育成や、自施設、他施設の病院職員に対する情報セキュリティ教育を実施することが求められる。

このために、医療情報システムと情報セキュリティに対する高度の知識が求められる。また、情報セキュリティに関する最新の知識を継続して獲得する能力が求められる。

一人の人材が医療情報システムと情報セキュリティに対する高度の知識を持つことが望ましいが、医療情報システム管理部門に医療情報システム対する知識を持つ人材と情報セキュリティに対する知識を持つ人材を配置し、両者が良好なコミュニケーションのもと業務にあたることを許容する。

「Group A 人材」は「統括情報セキュリティ責任者」やそれを補助するものとして、病院経営に関わることが求められる。このためには中長期的な事業計画に対して破綻をきたさないよう、計画的なセキュリティ維持強化計画を提案する能力が必要となる。セキュリティリスクはサイバー攻撃トレンドと自施設で残存するセキュリティ課題の両側面について、重要な医療ワークフローならびに患者保全のリスクの高い箇所を指摘できる必要がある。改善箇所のセキュリティ強化については、現場で許容されうる IT 変更負担を適切に推測しながら、IT インフラ、計算機類、ソフトウェア、サービス層におけるセキュリティ実装の形態を勘案するとともに、特に医療においては容体急変対応で不可欠な IT の可用性を重視した実装形態を選択する能力が求められる。

【医療情報システムに対する知識の担保】

- 「上級医療情報技師」相当の資格を有し、更新が行われていること。
- 「上級医療情報技師」相当の資格を有さない場合は、①から⑤の 2 つ以上を満たすことが望まれる。
  ※将来的には、「上級医療情報技師」相当の資格を取得することが推奨される。
  ①医療系国家資格や「医療情報技師」、「診療情報管理士」の資格を有すること
  ②医療機関において専従で 5 年以上医療情報システム管理に従事した経験があること
  ③医療機関や事業者で、医療情報システム導入（更新）で主導的な役割を果たした経験があること
  ④所定の医療情報システムに関する教育（「３．医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと
- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】

- IPA「情報処理安全確保支援士」相当の資格を有し、更新が行われていること
- IPA「情報処理安全確保支援士」相当の資格を有さない場合、所定の情報セキュリティに関する教育（「３．医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ※将来的には、「情報処理安全確保支援士」相当の資格取得を推奨する。
- 内閣府サイバーセキュリティセンターから最新の情報セキュリティ情報を収集するなど、情報セキュリティに対する最新の知識を取得すること。

【求められる業務】

≪自施設≫

- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 医療情報システムに対する情報セキュリティ対策
- 情報セキュリティインシデントに向けた IT-BCP の策定
- 情報セキュリティインシデント発生時のシステム復旧に向けた取り組み
  （外部から派遣される情報セキュリティ専門家や電子カルテベンダーとの協働、病院職員に向けた司令塔の役割）
- 自施設の職員に対する情報セキュリティ教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」間で実施する情報システムのセキュリティ相互チェックへの対応
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練への参加

≪他施設≫

- 「Group A 人材」間や他の情報セキュリティ人材との情報セキュリティ対策に関する情報共有や連携
- 他施設の病院経営層に向けた情報セキュリティ対策体制の指導やアドバイス
- 他施設の医療情報システムに対する情報セキュリティ対策や情報セキュリティインシデントに向けた IT-BCP の策定の指導やアドバイス
- 他施設の情報セキュリティインシデント発生時のシステム復旧に向けた取り組みの支援

- 他施設の職員に対する情報セキュリティ教育の支援
- 他施設の情報システムのセキュリティチェックの実施
- 他施設との情報セキュリティカンファレンスの主催
- 他施設とのサイバー攻撃合同訓練の主催

② Group B 人材

「Group B 人材」は医療情報システムの特性を理解した上で、自施設に対して、自立的に情報システムのセキュリティ対策を施すこと、情報セキュリティインシデント発生を想定した診療継続計画（IT-BCP）を策定することができる人材を想定する。また、自施設に情報セキュリティインシデントが発生した際には、他施設の「Group A 人材」の指導のもと、システム復旧に向けた活動を行うことができる人材を想定する。「Group B 人材」は自施設の病院職員に対して、情報セキュリティ教育を実施できる必要がある。このために、医療情報システムと情報セキュリティに対する高い知識が求められる。また、情報セキュリティに関する最新の知識を継続して獲得する能力が求められる。

一人の人材が医療情報システムと情報セキュリティに対する高度の知識を持つことが望ましいが、医療情報システム管理部門に医療情報システム対する知識を持つ人材と情報セキュリティに対する知識を持つ人材を配置し、両者が良好なコミュニケーションのもと業務にあたることを許容する。

「Group B 人材」は「統括情報セキュリティ責任者」やそれを補助するものとして、病院経営に関わることが求められる。このためには中長期的な事業計画に対して破綻をきたさないよう、計画的なセキュリティ維持強化計画を提案する能力が必要となる。セキュリティリスクはサイバー攻撃トレンドと自施設で残存するセキュリティ課題の両側面について、重要な医療ワークフローならびに患者保全のリスクの高い箇所を指摘できる必要がある。改善箇所のセキュリティ強化については、現場で許容されうる IT 変更負担を適切に推測しながら、IT インフラ、計算機類、ソフトウェア、サービス層におけるセキュリティ実装の形態を勘案するとともに、特に医療においては容体急変対応で不可欠な IT の可用性を重視した実装形態を選択する能力が求められる。

【医療情報システムに対する知識の担保】

- 「医療情報技師」相当の資格を有し、更新が行われていること。
- 「医療情報技師」相当の資格を有さない場合は、①から⑤の 2 つ以上を満たすことが望まれる。
  ※将来的には、「医療情報技師」相当の資格取得を強く推進する。
  ①医療系国家資格や「診療情報管理士」の資格を有すること
  ②医療機関において専任で 3 年以上医療情報システム管理に従事した経験があること
  ③医療機関や事業者で、医療情報システム導入（更新）で主導的な役割を果たした経験があること
  ④所定の医療情報システムに関する教育（「３. 医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと
- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】

- IPA の「情報セキュリティマネジメント試験」相当の資格を有すること。
- IPA の「情報セキュリティマネジメント試験」相当の資格を有さない場合、
  所定の情報セキュリティに関する教育（「３．医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ※将来的には、「情報セキュリティマネジメント試験」相当の資格取得を強く推進する。
- 内閣府サイバーセキュリティセンターから最新の情報セキュリティ情報を収集するなど、情報セキュリティに対する最新の知識を取得すること。

【求められる業務】
- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 自施設の情報システムに対する情報セキュリティ対策
- 自施設の情報セキュリティインシデントに向けた IT-BCP の策定
- 情報セキュリティインシデント発生時のシステム復旧に向けた取り組み
  （外部から派遣される情報セキュリティ専門家や電子カルテベンダーとの協働、病院職員に向けた司令塔の役割）
- 自施設の職員に対する情報セキュリティ教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」が開催する情報セキュリティカンファレンスへの参加
- 「指導的な立場の医療機関」や事業者が実施する情報システムのセキュリティチェックへの対応
- 「指導的な立場の医療機関」や公的機関、事業者が開催するサイバー攻撃合同訓練への参加
- 「Group A 人材」間や他の情報セキュリティ人材との情報セキュリティ対策に関する情報共有や連携

③ Group C 人材

「Group C 人材」は医療情報システムと情報セキュリティに対する最低限の知識を有し、「Group A 人材」の力を借りながら、自施設の情報システムの情報セキュリティ対策を講じることができる人材である。医療情報システムの新規導入や更新時に導入事業者から情報セキュリティ対策の説明を受け、情報セキュリティ対策の懸念があれば、「Group A 人材」に問い合わせをすることができることが求められる。
自施設に情報セキュリティインシデントが発生した際、導入業者と連携した初動対応と、「指導的な立場の医療機関」や公的機関、事業者から派遣される「Group A 人材」と連携した復旧対応をすることが求められる。
このために、医療情報システムや情報セキュリティ対策で使用される言葉が理解できることが最も大切となる。「Group C 人材」は病院内の医療情報システム安全管理責任者ならびに管理者の方針指示を受け、現在の医療情報システムに対するセキュリティ強化対策を電子カルテ事業者と共に運用する能力が求められる。システムトラブル発生時には、障害箇所の推定情報からサイバー攻撃の可能性についての予兆、続いて生じる IT としてのサービス停止、IT システムに関する被害推定ならびに BCP に必要な一時対応について、医療情報システム安全管理責任者ならびに管理者の指示を仰ぎながら、可能な範囲で実施ならびに確認を行う必要がある。「Group C 人材」は一次対応と並行して、「Group A 人材」に把握できる範囲の自施設のサイバー被害状況ならびに診療機能不全状況について、迅速かつ的確に伝達する能力が求

められる。また「Group A 人材」が考察し指示した対応方法についてこれを理解し、対応作業を行う院内スタッフまたは電子カルテ事業者の対応者の助力を得ることについて、日常的なコミュニケーションを通じて備える必要がある。

【医療情報システムに対する知識の担保】

- 「医療情報基礎知識検定試験」に合格していること
  または、「医療情報技師」相当の資格を有すること。
- 「医療情報基礎知識検定試験」、「医療情報技師」相当の資格を有さない場合は、
  ①から⑤のいずれか 1 つを満たすことが望まれる。
  ※将来的には、「医療情報基礎知識検定試験」の合格を目指すことを強く推奨する。
  ①医療系国家資格や「診療情報管理士」の資格を有し、医療機関で医療情報システムを使った実務経験があること
  ②医療機関において、1 年以上医療情報システム管理に従事した経験があること
  ③医療機関や事業者で、医療情報システム導入（更新）に関わった経験があること
  ④所定の医療情報システムに関する教育（「３.医療情報セキュリティ人材が受けるべき教育について」を参照）を受講したこと。
  ⑤「指導的な医療機関」における所定期間の医療情報システムに関する実地研修を修了したこと
- 「医療情報システムの安全管理に関するガイドライン」を理解していること。

【情報セキュリティに対する知識の担保】

- IPA「IT パスポート試験」に合格していることが望ましい
- 所定の情報セキュリティに関する教育（「３．医療情報セキュリティ人材が受けるべき教育について」を参照）を受講していること。

【求められる業務】（必要に応じて「Group A 人材」から指導、アドバイスを求める）

- 病院経営層と連携した自施設の情報セキュリティ対策体制の構築
- 自施設の情報システムに対する情報セキュリティ対策
- 自施設の情報セキュリティインシデントに向けた IT-BCP の策定
- 自施設の情報セキュリティインシデント発生時、外部から派遣される情報セキュリティ専門家や電子カルテベンダーと協力した、システム復旧に向けた取り組み
- 自施設の職員に対する情報セキュリティ教育
- 厚生労働省が求める医療機関等におけるサイバーセキュリティ対策の実施
- 「指導的な立場の医療機関」が開催する情報セキュリティカンファレンスへの参加
- 内閣府サイバーセキュリティセンターなどから、最新の情報セキュリティ情報の収集

３．医療情報セキュリティ人材が受けるべき教育について

Group A 人材、Group B 人材、Group C 人材が受けるべき教育の到達目標と教育カリキュラムを下記にまとめた。感染症対策や医療安全などと同じ様に、セミナーの開催や受講管理、受講修了証の発行などを管

理する仕組み（組織）が必要となる。
教育コンテンツについては、厚生労働省や経済産業省・IPA、内閣サイバーセキュリティセンター（NISC）などの行政のプラットフォームをはじめ、学会・団体でも多くのコンテンツが用意されている。これらのコンテンツと提示する教育カリキュラムとのマッピングを行うことができれば、教育コンテンツ作成や更新に係る労力を抑えることが期待される。
不足する教育コンテンツについては、新規作成が必要となる。IPA や医療情報技師育成部会の協力を得ながら、コンテンツを作成することが期待される。

① Group A 人材

〇到達目標
診療業務フローについての十分な理解と医療情報セキュリティの実践経験が豊富にあり、情報セキュリティの技術的観点から組織全体を導く指針を示し、実効性のある提案や助言を行うとともに、セキュリティ人材の育成を行うことができる。
〇教育コンテンツ
【新規講習】
組織的に情報セキュリティへの取り組み、他の部署・施設へ助言を行うために必要となる事項について学ぶ。

1. 情報セキュリティマネジメントの実践
2. 情報システムのリスク分析と評価
3. 侵入検知・防御に関する技術
4. アクセス制御と認証に関する技術
5. 暗号に関する技術
6. システム開発におけるセキュリティ対策
7. 情報セキュリティに関する法制度・ガイドライン
8. 医療情報関連法令・ガイドライン
9. 情報戦略の立案
10. プロジェクトマネジメント
11. チームマネジメント
12. セキュリティインシデントへの対応
13. 医療情報システムのシステム監査
14. 災害やシステム障害に備えた対策
15. セキュリティ教育及び人材育成の方法

※「上級医療情報技師」の資格保有者は、新規講習 8〜15 の受講を免除する。
※IPA「情報処理安全確保支援士」資格保有者は新規講習 1-7 の受講を免除する。
【定期（継続）講習】
医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威

B. インシデント発生時の初動対応とその際の留意点
C. 医療情報システムの安全管理に関するガイドラインについて

② Group B 人材

○到達目標

医療情報システムの機能及び役割と情報セキュリティの基本的な知識及び技術を備えており、医療現場の業務フローを理解して、日常的なセキュリティ対策を実践するとともに、インシデント発生時の適切な初期対応を行うことができる。

○教育コンテンツ

【新規講習】

医療情報システムの機能及び役割と情報セキュリティの基本的な知識及び技術、診療業務フローについて学ぶ。

1. 情報セキュリティマネジメントの概要
2. 情報システムの脅威と脆弱性への対応
3. コンピュータシステムのセキュリティ対策
4. ネットワークのセキュリティ対策
5. データベースおよびデータのセキュリティ対策
6. 情報セキュリティに関する法制度
7. プロジェクトマネジメントとサービスマネジメント
8. 医療現場の診療業務フロー
9. 医療情報システムの機能及び役割
10. 医療情報システムの調達と運用保守
11. 医療情報の安全管理に関する関係法令／医療情報システムの安全管理対策（経営管理編）
12. 医療情報システムの安全管理対策（企画管理編）
13. 医療情報システムの安全管理対策（システム運用編）
14. 医療情報システム／セキュリティを支える施設基盤
15. インシデント発生時の適切な初動対応

※「医療情報技師」 「上級医療情報技師」の資格保有者は、新規講習 8～15 の受講を免除する。

※IPA「情報セキュリティマネジメント試験」合格者、「情報処理安全確保支援士」試験合格者は新規講習 1-7 の受講を免除する。

【定期（継続）講習】

医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威
B. インシデント発生時の初動対応とその際の留意点
C. 医療情報システムの安全管理に関するガイドラインについて

③ Group C 人材

〇到達目標

医療情報システムの利用と情報セキュリティに必要となる基本ルールを理解し、医療現場での日常業務における基礎的なセキュリティ対策を行うとともに、インシデント発生時には速やかに関係部署・機関に通報することができる。

〇教育コンテンツ

【新規講習】

医療情報システムの利用と情報セキュリティに必要となる基本事項について学ぶ。

新規講習は必須プログラムと医療および医療情報システムに関する任意プログラム①、情報処理技術に関する任意プログラム②で構成される。

A. 医療情報セキュリティの基本（必須プログラム：30 分程度の e-Learning）
   1. 情報セキュリティの基礎
   2. 病院情報システムの最低限の運用管理とセキュリティ
   3. トラブル発生時の初期対応と関係機関への連絡

B. 医療および医療情報システム（任意プログラム①：50 分程度の e-Learning）
   1. 日本の医療制度と医療関連法規
   2. 医療機関の業務と診療情報管理
   3. 病院情報システムの主な構成と機能
   4. 病院情報システムのアカウント管理とアクセス制御
   5. 病院情報システムの運用と保守管理

C. 情報処理技術（任意プログラム②：50 分程度の e-Learning）
   1. コンピュータの基礎
   2. ネットワーク技術とネットワークサービス
   3. データベースとデータ管理
   4. 情報システムの導入・運用・保守
   5. 情報セキュリティ技術

※出題基準等に情報セキュリティに関する項目が含まれている国家資格（診療放射線技師、臨床工学技士、臨床検査技師）および診療情報管理士、医療情報基礎知識検定試験の合格者は必須プログラムのみ受講を義務付ける。

※IPA の IT パスポート（レベル 1）以上の合格者は、必須プログラムの受講を義務付けるほか、任意プログラム①の受講を推奨する。

※出題基準等に情報セキュリティに関する項目が含まれていない国家資格については、必須プログラムの受講を義務付けるほか、任意プログラム②の受講を推奨する。

【定期（継続）講習】

医療現場での最新動向を踏まえたセキュリティ対策およびインシデント発生時の関係機関への通報を適切かつ円滑に行うための事項について学ぶ。

A. サイバーセキュリティに関する最近の脅威
B. インシデント発生時の初動対応とその際の留意点

C. 医療情報システムの安全管理に関するガイドラインについて

４．補足事項

４－１．医療情報セキュリティ人材が持つべき知識やスキルセットについて

本研究班で令和 5 年度に実施した情報セキュリティ人材配置に関するアンケート調査では、回答施設 643 施設のうち、92.1%（400 床以上 : 99.6%）の医療機関が医療情報システム安全管理責任者や情報セキュリティ事案の担当者を配置しており、情報セキュリティ対策の必要性は広く浸透していると考えられる。一方、「上級医療情報技師」は 5.6%（400 床以上 : 10.6%）、「医療情報技師」は 28.5%（400 床以上 : 37.4%）、「情報処理安全確保支援士」は 2.5%（400 床以上 : 6.0%）、「情報セキュリティマネジメント試験」は 4.8%（400 床以上 : 6.0%）の医療機関での雇用にとどまり、医療情報セキュリティの資格を有する人材は豊富でないことが明らかとなっている。そこで、医療情報セキュリティ人材が持つべき知識やスキルセットについては、医療機関で広く人材雇用が進むことを念頭に、将来の資格保有を推奨しながら、実務経験や教育の受講で対応できる内容とした。

４－２．Group A 人材の安定した雇用に向けて

「Group A 人材」は高い知識や技術を持つ人材となるため、医療福祉領域で、十分な人数の確保が困難となることが想定される。このため、「Group A 人材」を雇用する医療機関は、「Group A 人材」が他施設の情報セキュリティ対策を援助できる体制を構築する必要がある。

「Group A 人材」の雇用経費を単一の医療機関で確保できないケースが想定される。また、安価な報酬を理由に、せっかく育った「Group A 人材」が医療福祉領域以外に流出することを防ぐ必要がある。

このために、「Group A 人材」を雇用する医療機関は、兼業を認めることで他施設から報酬を得る仕組みを考慮するなど、地域として「Group A 人材」を確保する取り組みが求められる。

４－３．個人、事業者等の情報セキュリティ人材の活用について

「自施設の情報システムを守ることができる医療機関」は、病床数に関わらず、情報セキュリティインシデントにより診療が停止した場合、地域医療に大きな影響が生じる医療機関や 400 床以上の医療機関を想定しており、候補となる医療機関は少なくない。すべての医療機関が Group B 人材の確保をすることは困難であることが想定され、一部の医療機関では Group C 人材を確保し、個人、事業者等の Group A 人材と契約の上、情報セキュリティ対策を講じることを想定した。

医療機関外の Group A 人材との契約については、大きく 3 つが想定される。１つ目として、自治体等が配置する医療機関を指導する Group A 人材と契約を結ぶ方法が考えられる。Group A 人材を配置する自治体等に限定されることは言うまでもない。2 つ目として、グループ医療機関や同一法人の医療機関が中央組織に Group A 人材を配置する方法が考えられる。３つ目として、個人や事業者が雇用する Group A 人材と契約を結ぶ方法が考えられる。医療機関外の情報セキュリティ人材については、医療情報システムの特性を理解している人材を見つけることが課題となる。独立行政法人情報処理推進機構（IPA）では令和 6 年度セキュリティ人材活用促進実証として、登録情報セキュリティスペシャリスト（登録セキスペ）アクティブリストの活用が検討されている。アクティブリストでは支援業種を選択して人材検索を行うことが検討されている。医療領域の人材として、Group A 人材の知識やスキルセットを要求することで人

材検索が可能となることが期待される。また、一般社団法人医療サイバーセキュリティ協議会（MedCSC）では、医療機関と情報処理安全確保支援士会（JP-RISSA）との情報交換プラットフォームの構築が検討されている。医療情報セキュリティ人材登録のプロセスで Group A 人材の知識やスキルセットを要求することが考えられる。今後、IPA や MedCSC と継続して連携をすることで、個人、事業者等の情報セキュリティ人材活用に向けた課題解決が期待される。

医療現場での経験がない人材が今後活躍できるよう支援することも人材増加に対して重要なアプローチであると考えられる。高いレベルでの医療情報システムを体系的に習得できるプログラムの例として、2024 年度に開設された名古屋医療情報学プログラム(NCIP)企業(一般社会人向け)リスキリングコースが挙げられる。現在、全国の大学病院ならびに医学部では、院内電算化に始まり電子カルテ導入まで継続する一連の医療情報システム化時代に比べて運用が定型化され外注化が進んだことから、体系的に病院情報システムについて習得する機会や OJT に相当する経験を積むことができる施設が減少していると考えられる。Group A 人材ならびに Group B 人材は高い実践能力が求められることから、特に Group A 人材を擁する医療機関においては、Group A 人材の支援環境整備に加えて OJT を可能にする環境整備の充実が強く求められると考察される。

「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、組織的に PDCA サイクルを実行するための提言」

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班
（令和 7 年 5 月 30 日）

初めに

医療情報システムがサイバー攻撃の被害にあった場合、医療情報システム停止により診療業務の継続が困難となることが想定される。短期的には、救急医療等の緊急性の高い医療が提供できず、患者の命を救う機会が奪われかねない。また、緊急性の高い患者の救急車・ヘリコプターによる搬送で公費支出がかさむことが想定される。先例により、医療情報システムの復旧には月単位の時間が必要となることが想定され、この間、医療機関は限られた診療情報を使った紙カルテ運用を行う必要がある。大規模医療機関では 2010 年前後より電子カルテ導入が進められており、40 歳未満の医療スタッフの多くは紙カルテ運用が未経験であることが想定される。限られた診療情報、慣れない紙カルテ運用、電子カルテの医療安全機能が使えない状況での、診療、看護の実施は医療安全上、大きなリスクとなる。

さらに、サイバーインシデントの際、患者の個人情報（診療情報）が漏えいすることが少なくない。漏えいした個人情報の回収は難しく、ダークウェブサイトで公開されるリスクが永続的に発生する。また、システム障害が発生した医療情報システムに対してはデジタルフォレンジック作業、システム復旧作業が行われるが、全ての診療情報の復旧が困難となるケースが想定される。その結果、過去の診療記録が失われ、患者の継続診療に不具合が生じることになる。

医療安全の確保や医療の質保証を行うため、患者の個人情報を適切に守るために、医療機関は日ごろから情報セキュリティ対策を徹底すること、情報セキュリティインシデントへの備え（医療情報システムの早期復旧に向けた対策、サイバーインシデント想定した事業継続計画の策定、サイバーインシデントを想定した災害訓練など）を行う必要がある。このためには、「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」で示した組織体制の構築と人材配置が求められる。

本研究班が令和 5 年度に実施した情報セキュリティ人材配置に関するアンケート調査では、保健医療福祉分野の情報システムの特性を理解しながら、情報セキュリティの知識を持つ人材の医療機関への配置は十分ではないことが明らかとなっている。このため、「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」は、将来の資格保有を推奨しながら、まずは各医療機関が情報セキュリティ人材の配置を進めることができるように、実務経験や教育の受講を重視する提言となっている。医療機関や医療機関に雇用された情報セキュリティ人材は、最新の医療情報システムや情報セキュリティに関する知識の獲得や、他医療機関の取り組みや経験の共有により、組織、個人として成長し、将来、医療機関でより確実な情報セキュリティ対策を確保するための PDCA サイクルを実行する必要がある。

1. 医療情報セキュリティ人材の育成と情報セキュリティに関する最新の知識の確保

医療情報セキュリティ人材は保健医療福祉分野の情報システムの特性を理解していることと情報セキュリティの知識の双方が要求される。さらに、情報セキュリティの知識は常に最新の情報に更新を行う必要がある。

保健医療福祉分野の情報システムの特性の理解

保健医療福祉分野の情報システムの特性の理解については、医療機関等での実務経験が重要となる。実務経験については、医療機関等の職員や医療情報システム事業者の担当者として医療情報システムの導入、更新、維持管理に関わるケースが想定される。これらの実務経験により、ある程度、保健医療福祉分野の情報システムの特性を理解することは可能であるが、より系統だった知識の担保に、本研究班での調査で教育カリキュラムが最も整理されていた医療情報技師、上級医療情報技師の資格取得が望まれる。

情報セキュリティ人材については、医療領域に所属する人材では不足することが想定される。このため、医療領域外の情報セキュリティ人材が、保健医療福祉分野の情報システムの特性を理解して、情報セキュリティ対策を講じることができる枠組みが必要となる。「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」では「指導的な立場の医療機関」に他医療機関から情報セキュリティ対策に関する実地研修を受け入れる体制を有することを求めている。医療領域外の情報セキュリティ人材についても実地研修受け入れることで、保健医療福祉分野の情報システムの特性の理解が進むと考えられる。情報処理安全確保支援士は登録情報セキュリティスペシャリスト（登録セキスペ）に登録することが可能であるが、独立行政法人情報処理推進機構（IPA）では、登録セキスペアクティブリストの整備が検討されている。アクティブリストによる人材検索で、支援業種として医療を選択した場合、保健医療福祉分野の情報システムの特性の理解した情報セキュリティ人材が検索される仕組みが望まれる。このためには、情報処理安全確保支援士の更新に必要な講習で、保健医療福祉領域に特化した講習を用意し受講した人材を検索対象にすることや、医療情報技師、上級医療情報技師の資格を有する人材を検索対象にする方法が考えられる。アクティブリスト整備が進む事で、保健医療福祉領域に参入する登録セキスペが増えることが期待される。

情報セキュリティに対する知識の担保

本研究班の調査では、医療系専門職において医療情報技師、上級医療情報技師が最も情報セキュリティに対する教育が整備されていることを確認した。一方、医療情報技師は医学・医療、医療情報システム、情報処理技術、それぞれの領域で合格点の取得が必要となる試験で、各領域で全ての知識を網羅する必要はなく、結果、情報セキュリティに知識を担保する資格とはなっていない。

情報セキュリティに対する知識の担保については、IPA の情報処理安全確保支援士、情報セキュリティマネジメント試験、IT パスポート試験などが挙げられる。本研究班のアンケート調査では、これらの IPA 資格、試験を有する病院職員は多くない。情報セキュリティに対する知識を持つ人材を広く医療機関に配置するために、短期的には情報セキュリティに対する教育の受講が有効であると考えた。長期的には、情報セキュリティ人材の知識の担保や安定した雇用を考えると、「Group A 人材」では情報処理安全確保支援士の資格取得、「Group B 人材」では情報セキュリティマネジメント試験への合格、「Group C 人材」では IT パスポート試験への合格が強く推奨される。

最新の情報セキュリティの知識の担保

情報セキュリティ対策に向けて、情報セキュリティ人材だけでなく、全ての病院職員がそれぞれのレベルに応じて、

情報セキュリティに対する最新の知識を確保する必要がある。情報セキュリティの知識の獲得に向けては、内閣府サイバーセキュリティセンター、厚生労働省医療機関向けセキュリティ教育支援ポータルサイト、独立行政法人情報処理推進機構などが最新の情報セキュリティに関する情報を発信している。また、CISSMED (Cyber Intelligence Sharing SIG for Medical)などを利用し、情報セキュリティ人材間での知識共有を行うことが想定される。全ての医療機関の情報セキュリティ人材が等しく、自律的に最新の情報を担保することは容易ではないと考えられる。

「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」では「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築することを求めている。さらに、「指導的な立場の医療機関」および「Group A 人材」は定期的に情報セキュリティに関するカンファレンスを開催すること、「自施設の情報システムを守ることができる医療機関」や「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」がこのカンファレンスに参加することを求めた。「指導的な立場の医療機関」および「Group A 人材」はカンファレンス開催に向けて、最新の情報セキュリティに関する知識の獲得に取り組むことが想定され、カンファレンスに参加する情報セキュリティ人材はカンファレンスで最新の知識を獲得することが期待される。

提言では「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」、「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」、全ての医療機関に対して自施設の病院職員教育を求めている。なお、「Group A 人材」については、自施設だけでなく他施設の職員教育を求めている。「Group C 人材」が自ら職員教育を行うことが難しいケースを想定して、「Group A 人材」への講演依頼や e-Learning の活用も想定をしている。

2. 情報セキュリティ人材の育成と医療機関等におけるサイバーセキュリティ対策の質的向上

医療機関等におけるサイバーセキュリティ対策については、医療情報システムの安全管理に関するガイドラインのうち優先的に取り組むべき事項が「医療機関におけるサイバーセキュリティ対策チェックリスト」として取りまとめられた。各医療機関ではチェックリストに従いサイバーセキュリティ対策が進められているが、具体的な対策は各医療機関の情報セキュリティ担当者の判断に委ねられており、有効な対策がどこまでとられているかは医療機関ごとに異なることが想定される。全国の医療機関が広くサイバーセキュリティ対策について向上するためには、各医療機関のサイバーセキュリティ対策の質的評価や、グッドプラクティスの共有などの仕組みが求められる。

「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」では「指導的な立場の医療機関」間で情報セキュリティに関する情報共有を行う体制を構築すること、互いの施設の医療情報システムの相互チェックを実施することや「Group A 人材」がその実務を担当することを求めている。「Group A 人材」が「指導的な立場の医療機関」の情報セキュリティ対策の相互チェックを行うことは、対象施設の情報セキュリティ対策の向上に向けた具体的なアドバイスだけでなく、自施設の情報セキュリティ対策の向上に活かすことができると考えられる。また、「Group A 人材」は「指導的な立場の医療機関」間の相互チェックで得られた知見を用いて、「自施設の情報システムを守ることができる医療機関」に対するセキュリティチェックを実施することが可能となる。「自施設の情報システムを守ることができる医療機関」の「Group B 人材」はセキュリティチェックを通じ、「Group A 人材」との交流や情報共有を行うことが可能となる。このように、数年間は医療機関同士がお互いの情報セキュリティ対策を学ぶ形で、各医療機関の情報セキュリティ対策の質を高めるとともに、「Group A 人材」、「Group B 人材」の育成につながると考える。さらに、「指導的な立場の医療機関」同士の相互チェックや「自施設

の情報システムを守ることができる医療機関」に対するセキュリティチェックを重ねることにより、保健医療福祉分野における情報セキュリティ対策の水準を定めることができる。「指導的な立場の医療機関」は、将来、医療機関等における情報セキュリティ監査基準として取りまとめることが期待される。情報セキュリティ人材を配置する医療機関は、「医療機関におけるサイバーセキュリティ対策チェックリスト」に加え、相互チェックやセキュリティチェックでの経験（将来的には情報セキュリティ監査基準）を活かし、自施設の医療情報システムの内部監査（自己点検・評価）を行い、外部評価（自施設に対する相互チェック、セキュリティチェック）の結果と合わせて、日々の情報セキュリティ対策向上につなげることが求められる。

医療情報システムの保守運用について外部委託を行っている医療機関は少なくない。既に導入されている医療情報システムに対して適切なセキュリティ対策を講じることは、契約や運用面、費用面、導入システムでの制限事項などの理由により、容易でないケースが想定される。日々の情報セキュリティ対策が大切であることは当然のことであるが、大きく情報セキュリティ対策を向上させるために、医療情報システム全体の運用や契約・費用に関する現状の棚卸しが必要となる。医療機関では 5、6 年に一度、医療情報システムの更新が行われるが、医療情報システムの更新は情報セキュリティ対策を見直す絶好の機会となる。情報セキュリティ人材は、医療情報システム更新に向けて、自施設の医療情報システムの仕様、運用、契約を整理し、セキュリティチェックリスト、内部監査、外部監査（相互チェックやセキュリティチェック）を通じて学んだ自施設の問題点、改善点を取りまとめた上で、公的医療機関は医療情報システム仕様書、民間医療機関は医療情報システム機能要求に反映をする必要がある。仕様書の作成や機能要求を外部コンサルタント業者に委託する場合は、外部コンサルタントが情報セキュリティに対する正しい知識を保有することを確認し（できればGroup A 人材を配置するコンサルタントが好ましい）、自施設の問題点、改善点が反映される仕様書となるように、連携を密に取る必要がある。医療情報システムの保守運用を外部事業者に委託する場合は、自施設の情報セキュリティ人材と外部事業者の役割を明確にし、契約に反映をさせる必要がある。

3. サイバー攻撃を想定した事業継続計画（BCP）の策定とサイバー攻撃合同訓練

「医療機関におけるサイバーセキュリティ対策チェックリスト」ではサイバー攻撃を想定した事業継続計画（BCP）の策定が求められる。厚生労働省は「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き」、「医療情報システム部門等における事業継続計画（BCP）のひな形」を公開している。サイバー攻撃の被害にあった大阪急性期・総合医療センターではホームページ上でIT-BCPが公開されている。各医療機関で策定したサイバー攻撃を想定したBCPについても「指導的な立場の医療機関」間の相互チェックや「自施設の情報システムを守ることができる医療機関」へのセキュリティチェックの対象となり、IT-BCPの質向上につながると考える。また、「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」に対しては、「Group A 人材」が上記取り組みを通じた獲得した知見を含め、IT-BCPの策定や改訂を支援することが想定される。

策定したIT-BCPが正しく機能するためには、サイバー攻撃合同訓練への参加が必要となる。サイバー攻撃訓練については、内閣府サイバーセキュリティセンターが重要インフラ対策として実施する全分野一斉演習への参加などを行っている状況である。災害対策については災害派遣医療チーム（DMAT）による合同防災訓練が実施されている。保健医療福祉分野により特化したサイバー攻撃訓練となるためには、医療機関がサイバー攻撃合同訓練を主催することが必要と考え、「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」では「指導的な立場の医療機関」に「自施設の情報システムを守ることができる

医療機関」と合同で、サイバー攻撃合同訓練を実施することを求めた。サイバー攻撃合同訓練を繰り返すことで、有効な訓練の主催が可能となると共に、IT-BCP へのフィードバックが可能になることが想定される。

4. 情報セキュリティ人材の適正配置、キャリアパス、医療領域からの人材流出の防止

サイバーインシデントにより医療機関が診療停止に追い込まれる事案の経験や、厚生労働省によるサイバーセキュリティ対策の施策等により、各医療機関はサイバーセキュリティ対策の必要性を認識し、その対策を進めている。一方、本研究班の調査では、医療機関が配置する情報セキュリティ担当者の資格、試験の保有率は低く、「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」での「Group A 人材」、「Group B 人材」、「Group C 人材」の適正配置が強く望まれる。

医療機関においては、情報セキュリティ人材の配置や情報セキュリティ対策への設備投資について、費用の確保が課題となる。医療機関で医療安全人材や感染症対策人材が定着していることは、医療機関における人材確保の必要性はもちろんのこと、医療安全対策加算や感染対策向上加算での施設基準や診療報酬によることが大きいことは間違いない。情報セキュリティ人材の確保においても、加算がつくことで医療機関は施設基準を満たすように努力することが想定され、医療機関での情報セキュリティ対策の向上に大きく貢献することが期待される。また、加算が付くことは、医療領域外の情報セキュリティ人材が医療領域に参入するきっかけとなり、人材不足が解消する可能性も期待される。

医療機関においては、現在の情報セキュリティ担当者に対して、保健医療福祉分野の情報システムの特性の理解と情報セキュリティに対する知識の担保を求めることが最も効率的であると考える。確実な知識や技術の担保には、「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」で取り上げた資格や試験の取得が望まれる。個々の人材においては、情報セキュリティに関する教育の受講、資格、試験の取得に向けた学習や受験、資格取得後の資格の維持に多大な労力と費用が発生するため、その対価を示すことが大切となる。

情報セキュリティ人材のキャリアパス

「医療機関におけるサイバーセキュリティ対策チェックリスト」では医療機関に医療情報システム安全管理責任者を置くことが求められている。本研究班で行った調査で、多くの医療機関で医療情報システム安全管理責任者を配置が進んでいるが、病院長や副病院長、事務長など病院執行部がその役割を担うことが多く、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い。医療機関が情報セキュリティ対策を進めるためには、病院執行部の意思決定が重要であり、病院執行部が医療情報システム安全管理責任者となることの意義は大きい。一方、情報セキュリティに対する知識が乏しい場合、正しい意思決定を行うことができるかについては課題が残る。大企業などでは組織のデータを保護するために使用するサイバーセキュリティ戦略を設計し、組織全体のリスクを評価して、サイバー防御を改善する責任をもつ CISO（Chief Information Security Officer）を配置することが求められる。医療機関においても、医療情報システム安全管理責任者が CISO として活動することで、確実な情報セキュリティ対策が進むと考えられるが、今すぐ、CISO の候補となる人材を確保している医療機関は多くないと考えられる。そこで、将来、CISO の候補となる人材を育成することが求められる。

「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」では、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」に医療情報システム管理部門を設置することを求めている。医療情報システム管理部門の設置により、組織としては、確実な情報セキュ

リティ戦略の設計を求めることが可能となる。雇用される「Group A 人材」、「Group B 人材」に対しては、医療情報システム管理部門の長として登用されることを想定するキャリアパスを提示することができ、部門長あるいはさらに上の立場で病院運営に関わることは、情報セキュリティ人材が CISO の役割を担う組織づくりにつながると考えられる。

「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」では、医療情報システム管理部門に「統括情報セキュリティ責任者」、必要に応じて「統括情報セキュリティ責任者」の補助者を配置することを求めている。医療機関における情報セキュリティ対策は迅速な対応が求められ、人材育成を待つ時間はない。このため、現時点においては情報セキュリティ戦略に向けた意思決定部分と戦略立案に向けた知識、技能部分を「Group A 人材」、「Group B 人材」が担うことを想定している。「Group A 人材」、「Group B 人材」が「統括情報セキュリティ責任者」を補助する立場で仕事をすることで、情報セキュリティ戦略に向けた意思決定を学び、医療機関における CISO の役割を担うことができる人材として育成されることが期待される。

一方、「Group C 人材」には異なるキャリアパスを示す必要がある。「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」では CISO を置くことは現実的でなく、外部 CISO の力を借りて、情報セキュリティ戦略を立案することが想定される。このため、「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」では診療放射線技師や臨床工学技士といった医療系専門職を「Group C 人材」として育てることが現実的である。また、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」においても、医療情報部門システムを管理する部門や外部と接続する医療機器を管理する部門に「Group C 人材」を配置が求められるが、それぞれの部門で働く医療系専門職から「Group C 人材」を育成することが想定される。多くの医療機関ではぎりぎりの人数で業務が遂行されているが、「Group C 人材」を配置することでプラス1の雇用枠が確保できれば、本来業務の負担軽減、業務拡大につながることが期待される。近年、部門業務の遂行には部門システムの有効活用が必須となっており、部門システム戦略に関わることになる「Group C 人材」は部門の管理者として育成されることが期待される。

情報セキュリティ人材の待遇

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。医療機関においては、情報セキュリティに関する資格、試験の取得に向けた経済的支援はもちろんのこと、資格、試験の取得者に対する待遇改善は、資格、試験の取得、維持に向けた最も分かりやすいモチベーションとなる。私立の医療機関ではこういった待遇改善が可能と思われるが、公的医療機関では給与水準が医療系資格により決められているため、待遇改善は容易でないことが想定される。一方、待遇改善がない場合、育成した情報セキュリティ人材が他施設や医療領域外に流出する懸念がある。特に、医療領域外への流出は避ける必要がある。

「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」では、「自施設の情報システムを守ることができる医療機関」に「Group B 人材」の配置と、外部「Group A 人材」との契約下に「Group C 人材」の配置の 2 つの選択肢を提案している。これは、グループ医療機関の中央組織に「Group A 人材」を配置、各医療機関には「Group C 人材」を配置し、グループ全体で情報セキュリティ戦略を構築することを想定している。このような中央組織に配置される「Group A 人材」に対する適切な待遇は比較的容易であることが期待される。

保健医療福祉領域で情報セキュリティ人材が不足する中、「Group A 人材」は自施設だけでなく、他施設の情報セキュリティ対策の支援が求められる。公的な医療機関等で「Group A 人材」への待遇改善が困難である場合、他施設に対する支援を兼業として認め、他施設から報酬を得る仕組みを考慮することで、「Group A 人材」の継続確保が可能になると考える。

人材セキュリティ人材の医療領域からの流出防止

「Group A 人材」は必ずしも医療機関に所属する必要はなく、民間事業者に所属しながら、あるいは個人として医療機関の情報セキュリティ対策を支援するビジネスモデルが想定される。民間事業者が医療機関で経験を積んだ「Group A 人材」の受け皿となること、「Group A 人材」が個人として活躍するキャリアパスを示すことは、せっかく育った情報セキュリティ人材が医療領域外に流出することを防ぐ意味でも大切である。

前述の通り、IPA では登録セキスペアクティブリストの整備が検討され、医療領域で活躍する登録セキスペの検索が可能となることが期待される。一般社団法人医療サイバーセキュリティ協議会（MedCSC）では、医療機関と情報処理安全確保支援士会（JP-RISSA）との情報交換プラットフォームの構築が検討されており、医療情報セキュリティ人材登録のプロセスで「Group A 人材」の知識やスキルセットを要求することが想定される。これらの取り組みを通じて、医療機関と民間事業者あるいは個人で活躍する「Group A 人材」のマッチングが成立することが期待される。

情報セキュリティ人材の適正配置と継続的な確保

医療機関の立場に応じて、情報セキュリティ人材を適切に配置することの重要性は、「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」で示した通りである。

医療機関における情報セキュリティ対策は各医療機関の医療情報システムの特性や運用に合わせて講じる必要があるため、情報セキュリティ人材が適切な情報セキュリティ戦略を講じるためには、ある程度当該医療機関への勤務経験が必要となることが多い。また、医療領域における情報セキュリティ人材は不足しており、欠員ができた際に、すぐに情報セキュリティ人材を確保することは難しいことが予想される。以上の状況から、最低限の人数の情報セキュリティ人材で情報セキュリティ対策を講じることは医療機関にとってリスクとなることをまず理解する必要がある。

「指導的な立場の医療機関」は言うまでもなく、「自施設の情報システムを守ることができる医療機関」については、情報セキュリティ人材を育成し、地域の医療機関に提供する役割が望まれる。「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」で最低限の人数の情報セキュリティ人材で情報セキュリティ管理を行った場合、自施設の情報セキュリティ対策を賄うことに精一杯となり、他施設への人材提供は困難となる。

以上の理由から、「指導的な立場の医療機関」、「自施設の情報システムを守ることができる医療機関」が安定して継続的に情報セキュリティ対策を講じ、自施設で育成した情報セキュリティ人材を地域に提供するために、これらの医療機関は、余裕を持った人数の情報セキュリティ人材を確保することが強く望まれる。

「Group A 人材」、「Group B 人材」はそれぞれの組織の医療情報システム部門長や CISO を目指すことが想定されるが、全ての人材が部門長、CISO となれるわけではない。「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で育成された「Group A 人材」、「Group B 人材」が、より良い待遇で地域の医療機関に就職することができれば、これらの人材が「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で教育を受け、医療情報システム、情報セキュリティに関する資格、試験を取得する大きな

モチベーションになる。退職後、民間事業者や個人として医療機関の情報セキュリティ対策に従事する情報セキュリティ人材にとっても同様である。「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」は欠員となった枠を使って若手の情報セキュリティ人材を雇用し、教育をすることで、新たな情報セキュリティ人材が育ってくる上、当該施設の組織の若返りをはかることが可能となる。

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	70（846）	399-405	2023
武田　理宏	情報セキュリティ人材の育成と適正な配置に向けて	日本病院会雑誌	In press		