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 6 年度は「教育」の観点から、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「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」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。

令和 5 年度、6 年度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。提言の作成には、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。

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。

本研究班では、「組織体制」、「人材」、「教育」を基軸に検討を行うこととした。令和 5 年度は、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）を行った。また、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い、「組織体制」、「人材」の観点で整理を行った。

令和 6 年度は「教育」の観点から、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（雇用条件、業務内容、保有資格など）」と「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」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。

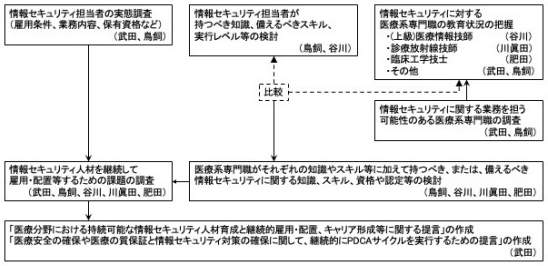

図1. 医療機関における情報セキュリティ人材の育成と配置に向けた検討課題

2. 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、分担研究成果報告書1）

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、情報処理推進機構（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。

3. 医療機関が地域で情報セキュリティ対策を向上させるための取り組み（担当：武田・鳥飼・谷川・川眞田・肥田、分担研究成果報告書 2）

医療機関が地域で情報セキュリティ対策を向上させるために必要な、医療情報セキュリティ人材の要件と、医療機関の組織体制について、検討を行った。この際、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対策を参考にした。

4. 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、分担研究成果報告書 3）

独立行政法人情報処理推進機構（IPA: Information –technology Promotion Agency）、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）を班会議にお招きし、外部人材の活用についての議論を行った。

5. 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、分担研究成果報告書 4）

令和 5 年度に実施し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、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と、令和 6 年度に実施した外部情報セキュリティ人材の活用に関する検討結果から、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。

6. 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、

分担研究成果報告書 5、添付資料1、添付資料 1_1、資料 2）

令和 5 年度に実施し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、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と、令和 6 年度に実施した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. 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、分担研究成果報告書1）

1－1. 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

1－2. 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。

<u>Group B 人材の教育カリキュラム案</u>

○ 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

1－3. 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

2. 医療機関が地域で情報セキュリティ対策を向上させるための取り組み（担当：武田・鳥飼・谷川・川眞田・肥田、分担研究成果報告書 2）

「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。

2-1. 医療情報セキュリティ人材

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

2-2. 医療機関の組織体制

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。

3. 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、分担研究成果報告書 3）

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。

3-1. 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、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。

3-2. 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。

3-3. 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。

4. 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、分担研究成果報告書 4）

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。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。

4-1. 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。

4-2. 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。

4-3 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。

4-4. 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。

5. 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、

分担研究成果報告書 5, 添付資料1、添付資料 1_1、資料 2）

5-1. 「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」

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。

「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」作成に当たっては、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るため、提言に反映させた。

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る。そこで、提言に「指導的な立場の医療機関」の役割として反映させた。

5-2．「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」

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

本研究班では、「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。

令和5年度の研究成果で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。

保健医療福祉領域で医療情報セキュリティ人材が圧倒的に不足している状況を考えると、外部情報セキュリティ人材の活用が大切になる。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。

他施設、団体に所属する医療情報セキュリティ人材の活用を可能とするため、「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」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」が「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、と整理を行った。「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」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、と整理されている。

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。提言作成の参考とした医療安全や感染

症対策の領域では、診療報酬制度で加算が認められている。医療情報セキュリティ対策に対する加算が認められれば、医療機関は情報セキュリティ対策費用や人件費の確保が可能となる。また、加算取得を目指して医療機関は情報セキュリティ対策を進め、また、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ことや、医療機関に対する情報セキュリティを支援する民間事業者の設立が期待される。

医療情報セキュリティ人材に対しては、学習や資格、試験を取得するための労力や費用に見合う報酬と将来のキャリアパスを提示する必要がある。報酬については、特に公的医療機関では、医療系専門職や事務職の給与体系が適用されると考えられるため、単施設では十分な給与を得られない可能性が高い。

大学病院では医師は教育職としての給与体系が適応されるため、市中病院に比し、給与が十分でないことが多い。しかし、医師の兼業で副収入を得ることで、人材確保に成功している。医師の兼業は、医師不足に悩む医療機関への人材提供の意味もあり、大学病院の社会的役割の一つとなっている。Group A 人材や Group B 人材に対して兼業を認めることで、医療情報セキュリティ人材は副収入を得ることができる。また、Group B 人材を配置できない「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」は、これらの人材の力を借りて、自施設の情報セキュリティ対策を進めることが可能となる。

キャリアパスについては、医療機関に医療情報システム部門を設置することで専門職としての役割が明確になると共に、部門の長やさらに CISO として病院執行部で活躍するキャリアパスを提示することができる。また、部門の長を目指さない場合は、他の医療機関や、医療機関の情報セキュリティ対策を支援する行政や民間事業者により良い待遇で転職することや、個人事業者として独立するキャリアパスを描くことができる。

情報セキュリティ人材が退職した場合でも、複数の医療情報セキュリティ人材を雇用していれば、後任として若い人材を雇用し、情報共有、教育を施すことで、医療情報セキュリティ人材に世代交代が実現できる。

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。

医療情報セキュリティ人材は、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が、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。

令和 5 年度、6 年度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

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)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～

(2)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)

(3)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)

(5)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

(6)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

(7)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

(8)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

（9）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

（10）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

（11）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

（12）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

（13）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