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)
分担研究報告書

テーマ: 医療情報セキュリティ人材の育成カリキュラムの開発

研究分担者 谷川 琢海 北海道科学大学 保健医療学部 診療放射線学科 准教授

研究要旨
本研究では、医療機関における情報セキュリティを強化するために必要となる教育カリキュラムの開発を目的として検討を行った。本研究班で昨年度に整理した Group A、Group B、Group C で構成される医療情報セキュリティ人材に応じて、各グループに求められる到達目標を攻撃者視点、防衛者視点、設計者視点、緊急時対応、日常運用保守の観点から整理した。その上で、新規講習と定期(継続)講習に分けた教育内容を策定し、さらに情報処理関連の国家試験および医療情報関連の資格認定との整合性を図り、効率的な人材育成のフレームワークを構築した。この教育カリキュラムの実践により、医療現場の特性を理解した情報セキュリティ人材の効率的かつ体系的な育成が可能となり、医療機関のセキュリティ体制強化に貢献することが期待される。

## A. 研究目的

近年、医療機関を標的としたサイバー攻撃や情報漏えい事案が継続して発生している。医療機関は、医療法施行規則の定めに従ってサイバーセキュリティ確保のための措置を講じる必要があるなか、特に医療機関において必要十分な組織体制を構築するうえでは診療業務を理解した医療情報セキュリティ人材を育成することが喫緊の課題である。

昨年度、本研究班では医療情報セキュリティ人材について検討を行い、Group A、Group B、Group C の3つの分類で人材を整理した。このなかで、Group A 人材は自施設の情報セキュリティの向上や情報セキュリティ事案の対応のほか、他施設の情報セキュリティ人材の教育・指導を行える人材、Group B 人材は独立して自施設の情報セキュリティの向上や情報セキュリティ事案に対応できる人材、Group C 人材は事業者や Group A、Group B 人材の助けを借りながら自施設の情報セキュリティの向上や情報セキュリティ事案に対応できる人材としている。

本研究では、医療情報セキュリティ人材の効果的かつ体系的な人材育成の教育体制を構築することを目的として、それぞれのグループに必要なスキルレベルに到達するための教育カリキュラム、および継続的にスキルを維持するために必要な教育カリキュラムについて検討を行った。

## B. 研究方法

医療情報セキュリティ人材の Group A、Group B、Group C 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、表1に示す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。作成したカリキュラム案について、本研究班のなかでの議論を通じて妥当性について評価を行った。

（倫理面への配慮）

本研究は情報セキュリティ人材の教育カリキュラムに関して、文献検索や会議体で議論をした内容をまとめたものであり、特段の倫理的配慮を必要としない。

## C. 研究結果

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（表２）と教育カリキュラム案（表３～表５）を策定した。

### 1. Group A 人材の教育カリキュラム案

Group A 人材は、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すとともに、地域の医療機関に対して実効性のある指導・助言を行うことができる人材である。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、表3に示す到達目標と計 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。

医療機関が登録セキスペを活用することは、IPA にとってもメリットがあることと考えられるため、令和 7 年度以降も継続的に IPA と議論を重ねる必要があると考えられた。

### 2. Group B 人材の教育カリキュラム案

Group B 人材は、医療情報システムの運用管理と情報セキュリティの基本的な知識及び技術を備え、医療現場の診療業務フローを理解して自施設の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人材である。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、表4に示す到達目標と計 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。

### 3. Group C 人材の教育カリキュラム案

Group C 人材は、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人材である。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、表5に示す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。

**D. 考察**

本研究では、人材育成カリキュラムの検討に先立ち、Group A、Group B、Group C という 3 つの段階的な人材像を定義し、それぞれの到達目標を明確にした上で教育カリキュラムを策定した。このアプローチにより、各グループに必要とされる知識・技能を体系的に整理することができた。今回作成した教育カリキュラムでは、Group C、Group B、Group A の順序でスキルアップしていくキャリアパスを想定している。これにより、医療機関のセキュリティ人材が基礎的なセキュリティ知識（Group C）から始め、経験を積みながら組織内のセキュリティ実務者（Group B）へと成長し、最終的には組織や地域を指導できる専門家（Group A）へと研鑽を積むことが可能になり、地域における医療情報セキュリティ人材のスキルの長期的な底上げが期待できる。

本研究で提案する各グループのスキルレベル、到達目標および学習項目は、既存の資格制度との整合性を考慮したものである。教育カリキュラムの社会実装に当たっては、第三者による評価によってスキルレベルを担保された人材の配置が望ましく、将来的には資格取得等によって評価する仕組みが期待される。具体的には、Group A 人材については情報処理安全確保支援士試験と上級医療情報技師能力検定試験、Group B 人材については情報セキュリティマネジメント試験と医療情報技師能力検定試験、Group C 人材については IT パスポート試験と医療情報基礎知識検定試験といった資格を取得していることが想定される。

ただし、迅速に医療情報セキュリティ人材の配置を全国で進めていくためには、短中期的には e-Learning 等を含む講習を受講することによる仕組みをベースとすることが有効であろう。そのうえで、資格取得によって新規講習の一部または全部の受講を免除する制度を設けることによって、既存人材の負担を軽減し、効率的な人材配置が可能になるものと考える。

例えば、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。また、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 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。

定期（継続）講習は、全てのグループに共通

の内容とした。医療情報セキュリティを取り巻く環境は日々変化しているため、教育内容も定期的に見直し、最新の脅威や対策技術に対応したものにアップデートしていく必要がある。また、共通の内容とすることで、最新の脅威動向や適切なインシデント対応などの情報が広く共有されるとともに、地域や組織内での情報セキュリティに対する共通理解を醸成し、インシデント発生時の連携体制を強化することが期待できる。

医療情報セキュリティ人材の育成は、安全・安心な医療サービスの提供を支える重要な基盤である。この教育カリキュラムを実践することにより、医療現場の特性を理解した情報セキュリティ人材の効率的かつ体系的な育成が可能になるだろう。将来においては、技術の進化や脅威の変化に応じて、カリキュラム内容を定期的に見直すことが必要である。

## E. 結論

本研究では、医療情報セキュリティ人材を 3 つのグループに分類し、それぞれに適した教育カリキュラムを開発した。各グループの人材に求められる学習目標を「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」の 5 つの観点から整理し、それを達成するための教育コンテンツを体系化した。また、既存の情報処理関連資格および医療情報関連資格との整合性を図ることで、効率的な人材育成の仕組みを提案した。今後は本カリキュラムを活用した e-Learning コンテンツの開発、実証研究を行い、その効果を検証する必要がある。本研究で開発した教育カリキュラムが、医療機関の情報セキュリティ体制強化の一助になることを期待する。

## F. 健康危険情報

なし

## G. 研究発表

### 1. 論文発表

なし

### 2. 学会発表

(1)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)

(2)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

(3)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

(4)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

(5)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

表 1　人材ごとのベースとなるスキルレベルの目安

| | Group　C 人材 | Group　B 人材 | Group　A 人材 |
|---|---|---|---|
| ベースとなるスキルレベルの目安 | IT パスポート試験<br><br>医療情報基礎知識検定試験 | 情報セキュリティマネジメント試験<br><br>医療情報技師能力検定試験 | 情報処理安全確保支援士試験<br><br>上級医療情報技師能力検定試験 |

表２　必要技能分類別の学習目標

| | Group　C 人材 | GroupB 人材 | GroupA 人材 |
|---|---|---|---|
| 攻撃者視点 | NIST CSF(Cyber Security Framework)で定義された識別・防御・検知・対応・復旧のそれぞれに関する医療情報システムのセキュリティ対策について理解している。 | NIST CSF(Cyber Security Framework)で定義された識別・防御・検知・対応・復旧のそれぞれの視点から、現在の医療情報システムのセキュリティ対策の問題点と改善案を挙げることができる。 | NIST CSF(Cyber Security Framework)で定義された識別・防御・検知・対応・復旧のそれぞれの視点から、現在の医療情報システムのセキュリティ対策が適切であるかを確認し、他院事例などのベストプラクティスに基づく適切な対応を提案・助言・指導できる。 |
| 防衛者視点 | NIST CDM(Continuo-us Diagnostics and Mitigation)で定義されたデータ・ネットワーク・認証とアクセス制御・資産管理・統合可視化のそれぞれに関する医療情報システムのセキュリティ対策について理解している。 | NIST CDM(Continuo-us Diagnostics and Mitigation)で定義されたデータ・ネットワーク・認証とアクセス制御・資産管理・統合可視化のそれぞれの視点から、現在の医療情報システムのセキュリティ対策の問題点と改善案を挙げることができる。 | NIST CDM(Continuo-us Diagnostics and Mitigation)で定義されたデータ・ネットワーク・認証とアクセス制御・資産管理・統合可視化のそれぞれの視点から、現在の医療情報システムのセキュリティ対策が適切であるかを確認し、他院事例などのベストプラクティスに基づく適切な対応を提案・助言・指導できる。 |
| 設計者視点 | Security-by-Design の考え方を理解し、医療情報システムの設計、構成等における代表例を挙げることができる。 | Security-by-Design の考え方に基づき、サイバーセキュリティの観点から医療情報システムの設計、構成等についての問題点と改善案を挙げることができる。 | Security-by-Design の考え方に基づき、サイバーセキュリティの観点から医療情報システムの設計、構成等が適切であるかを確認し、他院事例などのベストプラクティスに基づく適切な対応を提案・助言・指導できる。 |
| 緊急時対応 | 診療業務フローを考慮した IT-BCP について理解し、作成することができる。また、インシデント発生時の初動対応を IT-BCP をもとに行うことができる。 | 診療業務フローを考慮した適切な IT-BCP の作成を主導することができる。また、インシデント発生時の初動対応を IT-BCP をもとに主導することができる。 | IT-BCP が初動対応から復旧までの各フェーズについて診療業務フローを考慮したなかで適切であるかを確認し、他院事例などのベストプラクティスに基づく適切な対応を提案・助言・指導できる。 |
| 日常運用保守 | 医療情報システムと情報セキュリティの安定的な運用のために日常的に行う保守業務の代表的な内容について理解している。 | 医療情報システムと情報セキュリティの安定的な運用のために日常的に行う保守業務について、問題点と改善案を挙げることができる。 | 医療情報システムと情報セキュリティの安定的な運用のために日常的に行う保守業務について、適切であるかを確認し、他院事例などのベストプラクティスに基づく適切な対応を提案・助言・指導できる。 |

表３　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

表４　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

表５　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