

分担研究報告書

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

研究分担者 谷川 琢海

（北海道科学大学 保健医療学部 診療放射線学科 准教授）

研究要旨

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

A. 研究目的

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

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

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

B. 研究方法

1. 保健医療系国家資格を有する医療系専門職の教育状況

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

調べることによって調査を行い、教育状況について検討を行った。

表1 厚生労働省が所管する保健医療関係の国家資格

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

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

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



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

C. 研究結果

1. 保健医療系国家資格を有する医療系専門職の教育状況

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

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

表2 国家資格ごとの情報セキュリティに関する出題動向

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

注:「-」はインターネット上に公開されている出題基準を確認できなかった。

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

また、過去5年間の国家試験において、情報

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

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

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

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

内容に編集されている。

表3 医療情報技師と上級医療情報技師の定義
医療情報技師の定義

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

上級医療情報技師の定義

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

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

表4 医療情報技師の到達目標の情報セキュリティに関する主な記述(抜粋)

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

表5 上級医療情報技師の到達目標の情報セキュリティに関する主な記述(抜粋)

項番	GIO・SBOs
6	情報セキュリティについて理解し、対策を講じることができる能力を修得する。
6-1	情報セキュリティのリスク分析を行うことができる。
6-2	情報セキュリティ対策についての知識を有しており、協議、立案することができる。
6-3	情報セキュリティに関するインシデントおよびアクシデントへの対応ができる。
6-4	情報システムの監査についての知識を有しており、立案できる。
6-5	個人情報の保護についての知識を有しており、適切に医療情報システム内に取り込むことができる。
6-6	医療情報セキュリティに関連する諸ガイドラインの内容を具体的に説明できる。

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

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

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

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

表6 医療情報技師能力検定試験の情報セキュリティに関する出題の抜粋

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

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

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

問45 コールドスタンバイの説明はどれか。

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

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

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

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

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

問49 非意図的なシステム障害発生要因はどれか。

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

表7 上級医療情報技師能力検定試験の午後 I 試験の出題例

午後 I (2021 年度 上級医療情報技師能力検定試験)

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

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

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

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

<ホームページ掲載内容>

「個人情報が含まれた USB メモリの紛失について」

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

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

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

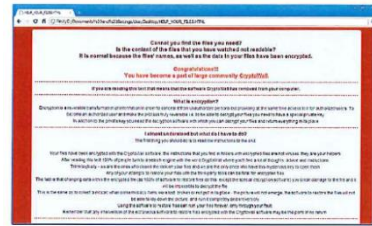
今後、②このような事態を繰り返さないよう再発防止を徹底し、皆様の信頼回復に努めてまいります。

病院長

午後 I (2022 年度 上級医療情報技師能力検定試験)

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

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



画面に表示されている英文 (一部)

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

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

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

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

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

午後 I (2023 年度 上級医療情報技師能力検定試験)

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

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

4. 医療情報技師育成部会が実施する生涯研修・e-Learning の内容

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

表8 2023年度に開催された生涯研修セミナーのプログラム概要

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

5. 医療機関の情報セキュリティ事案の担当者のなかでの医療情報技師

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

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

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

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

6. 医療情報技師の地域での活動のなかでの情報セキュリティに関する取り組み

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

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

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

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

D. 考察

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

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

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

内容であると考えられる。

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

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

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

E. 結論

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

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

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

F. 健康危険情報

なし

G. 研究発表

1. 論文発表

なし

2. 学会発表

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

H. 知的財産権の出願・登録状況

(予定を含む。)

1. 特許取得

なし

2. 実用新案登録

なし

3. その他