

大会企画 | 2023年11月24日

📅 2023年11月24日(金) 13:30 ~ 15:30 📍 D会場 (EX2-A)

大会企画3

医療分野のセキュリティ人材の育成をどうするか

オーガナイザー：谷川 琢海（北海道科学大学）

座長：谷川 琢海（北海道科学大学）、武田 理宏（大阪大学）

[3-D-3] 医療分野のセキュリティ人材の育成をどうするか

*谷川 琢海^{1,2}、武田 理宏³、岡本 潤⁴、田中 彰子⁴、大道 道大⁵、奥村 明俊⁶ (1. 日本医療情報学会医療情報技師育成部会、2. 北海道科学大学保健医療学部、3. 大阪大学大学院医学系研究科医療情報学、4. 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、5. 社会医療法人大道会 森之宮病院、6. 独立行政法人情報処理推進機構)

キーワード：Cyber security、Medical Information security、Human resource development

近年、日本国内外において医療機関へのサイバー攻撃による被害が多く報告されており、国内においても複数の医療機関が被害を受けている。医療分野は政府が定める重要インフラ分野のひとつであり、地域医療を支える医療機関が長期にわたり診療が停止することがないように万全の対策が望まれる。本年4月に医療法施行規則が改正され、医療機関の管理者が遵守すべき具体的事項として、サイバーセキュリティの確保について必要な措置を講じることが定められたほか、厚生労働省から同年5月に公表された「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、医療機関の経営管理層の関与をはじめ、情報セキュリティに関する組織的な対応を強く促す内容に改訂されたところである。これから医療DXを推進していくためには、国民や患者が安心できるように、サイバーセキュリティが確保された環境を構築し、その環境を継続して維持していかなければならない。しかし、医療分野では情報セキュリティに対応できる人材の不足が指摘されており、知識、技術、経験を有する人材の育成が急務となっている。医療分野においては、診療業務をよく理解し、医療をとりまく技術動向等を踏まえたなかで対策を講じていくことが肝要であり、現在、厚生労働行政推進調査事業費により「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（23IA2007）」（研究代表者：大阪大学 武田 理宏 教授）のなかで人材育成と配置について研究が進められている。本セッションでは、厚生労働省医政局 岡本 潤 室長補佐、日本病院会 大道 道大 副会長、情報処理推進機構 奥村 明俊 理事のほか、学会内の有識者に登壇いただき、医療機関等において、情報セキュリティを継続的に担える人材の必要性や、その人材に求められるスキルセット、スキルレベルについて議論する。

医療分野のセキュリティ人材の育成をどうするか

谷川 琢海^{*1,*2}、武田 理宏^{*3}、岡本 潤^{*4}、田中 彰子^{*4}、大道 道大^{*5}、奥村 明俊^{*6}

*1 日本医療情報学会医療情報技師育成部会、*2 北海道科学大学保健医療学部

*3 大阪大学大学院医学系研究科医療情報学、

*4 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

*5 社会医療法人大道会 森之宮病院、*6 独立行政法人情報処理推進機構

Strategies for Fostering Cyber Security Human Resources in Healthcare

Takumi Tanikawa^{*1,2}, Toshihiro Takeda^{*3}, Jun Okamoto^{*4}, Akiko Tanaka^{*4}, Michihiro Omichi^{*5}, Akitoshi Okumura^{*6}

*1 Japan Association for Medical Informatics (JAMI), *2 Hokkaido University of Science,

*3 Graduate School of Medicine, Osaka University, *4 Ministry of Health, Labour and Welfare,

*5 Morinomiya Hospital, *6 Information-technology Promotion Agency (IPA)

In recent years, there have been a lot of reports of cyberattacks on hospitals both in Japan and abroad, with several domestic hospitals falling victim to these attacks. The healthcare sector is considered one of the critical infrastructures designated by the government, and comprehensive measures are essential to ensure that healthcare institutions supporting regional medical services do not experience prolonged interruptions. In April 2023, the Medical Care Act Enforcement Regulations were revised, mandating specific cybersecurity measures for healthcare administrators. Additionally, in May, the Ministry of Health, Labour, and Welfare introduced "Guidelines for the Secure Management of Medical Information Systems version 6.0," encouraging active participation of healthcare management in information security and revising organizational responses. To promote healthcare digital transformation (DX) successfully, it is crucial to establish and maintain cybersecurity measures that assure the confidence of citizens and patients. However, there is a noted shortage of personnel with the capability to address information security in the healthcare field, emphasizing the urgent need for the development of specialists with knowledge, skills, and experience. Particularly in the medical field, human resources are required who understand medical practice workflow and can adapt to the evolving information and communication technology.

Keywords: Cyber security, Medical Information security, Human resource development

1. はじめに

近年、日本国内外において医療機関へのサイバー攻撃による被害が多く報告されており、国内においても複数の医療機関が被害を受けている。医療分野は政府が定める重要インフラ分野のひとつであり、地域医療を支える医療機関が長期にわたり診療が停止することがないように万全の対策が望まれる。本年4月に医療法施行規則が改正され、医療機関の管理者が遵守すべき具体的事項として、サイバーセキュリティの確保について必要な措置を講じることが定められたほか、厚生労働省から同年5月に公表された「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、医療機関の経営管理層の関与をはじめ、情報セキュリティに関する組織的な対応を強く促す内容に改訂されたところである。

これから医療DXを推進していくためには、国民や患者が安心できるように、サイバーセキュリティが確保された環境を構築し、その環境を継続して維持していかなければならない。しかし、医療分野では情報セキュリティに対応できる人材の不足が指摘されており、知識、技術、経験を有する人材の育成が急務となっている。医療分野においては、診療業務をよく理解し、医療をとりまく技術動向等を踏まえたなかで対策を講じていくことが肝要であり、現在、厚生労働行政推進調査事業費により「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(23IA2007)」(研究代表者:大阪大学 武田 理宏 教授)のなかで人材育成と配置について研究が進められている。

本セッションでは、厚生労働省医政局 岡本 潤 室長補佐、日本病院会 大道 道大 副会長、情報処理推進機構 奥村 明俊 理事のほか、学会内の有識者に登壇いただき、医療機

関等において、情報セキュリティを継続的に担える人材の必要性や、その人材に求められるスキルセット、スキルレベルについて議論する。

2.1 「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て」

大阪大学大学院医学系研究科医療情報学

武田 理宏

医療分野はその機能が障害された場合、国民生活・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つに定められる。また、政府は医療 DX 推進本部を設置し、医療機関は医療 DX を進める必要がある。一方、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、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、「医療情報システムの安全管理に関するガイドライン」の改定も行われた。我々は、「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」を受託し、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に調査研究を行っており、その研究進捗の報告を行う。

2.2 「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」

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
岡本 潤、田中 彰子

医療機関では、医療情報システムを取り巻く環境の変化や医療情報システム・機器の高度化等に伴い、サイバーセキュリティの脆弱性への対応やインシデント発生時に対処するためのポリシーの策定、安全管理体制の整備やトレーニング／教育等に関する早急に対策を講じることが喫緊の課題となっている。また、近年は医療機関を標的としたサイバー攻撃により、一時的に診療機能が停止すること等の事案が発生している。

医療分野の情報セキュリティ対策に関しては、平成 27 年 9 月 4 日閣議決定の「サイバーセキュリティ戦略」で「機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。その際、重要インフラに該当する医療分野においても厚生労働省と医療機関等が連携し、実効性のある情報セキュリティ対策を講じていくことが求められている。平成 30 年 3 月には医療セプターが設置され、内閣サイバーセキュリティセンターや厚生労働省との連携の下、IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報を適切に重要インフラ事業者等に提供して関係者間で共有するとともに、演習参加等の活動に取り組んでいる。

このような状況の中、厚生労働省では、令和4年 9 月に第 12 回 健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループにおいて、予防対応・初動対応・復旧対応からなる「医療機関のサイバーセキュリティ対策の更なる強化策」を取りまとめた。その中で医療従事者等の情報セキュリティに関するリテラシーのより一層の向上を図るべく、医療従事者の階層（医療従事者・経営層・システムセキュリティ管理者）に応じた研修、情報共有体制の強化等に取り組んでおり、これら取組に関して述べる。

2.3 「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」

社会医療法人大道会 森之宮病院
大道 道大

病院における電子化は、1970 年代のレセコン、1980 年代のオーダリング、そして 2000 年代からの電子カルテへとすすんできた。しかし、院内のシステムを維持・管理する部門はベンダーなどの外部業者に依存することが多く、内製化している病院は少ない。医療という機微情報を扱うにもかかわらず、病院においてはシステムが外から攻撃されるという危機感はなく、セキュリティポリシーはもっぱら個人情報漏洩の防止に重点が置かれ、それこそが IT リテラシーと考えられてきた。そこには「電子カルテは閉鎖された院内ネットワークなので安全である」という誤った神話があったように思う。

日本病院会が行った会員へのアンケート結果によると、病院管理者の9割はサイバー攻撃への脅威を感じているものの、情報セキュリティへの年間予算は病院の半数は 500 万円以

下であり、これで十分だという回答は1割しかなかった。1970 年代から 2000 年までの経営状況と異なり、現在の病院には情報システムにかける資金が乏しいことも問題と思われる。

2.4 「サイバーセキュリティ人材育成に関する IPA の取り組み」

独立行政法人情報処理推進機構 (IPA) 奥村 明俊

IPA は、社会の仕組みをデジタル対応させていくためのアーキテクチャ設計・データ標準化を推進しながら、デジタルトランスフォーメーション (DX) の促進、サイバー・フィジカル一体化時代におけるサイバーセキュリティの確保やデジタル人材育成などに取組んでいる。コロナ禍により世の中のデジタル化が加速するとともに、DX を推進する中で、デジタル人材不足が大きな課題として認識されてきている。日本における 2022 年のサイバーセキュリティ関連従事者は約 38.8 万人と推定され、40.4%増加しているが、サイバーセキュリティ人材の不足は 5.6 万人で、前年よりも 37.9%不足数が増加している。これには、IT・セキュリティベンダー等の専門的なセキュリティ人材、企業情報システム部門等のセキュリティ人材以外に、DX を推進する中でセキュリティ人材が求められる領域が広がっていることが大きな要因と推測される。この状況に対して政府は、2026 年度末までにデジタル推進人材 230 万人を育成する方針を打ち出している。デジタル推進人材の五つの人材類型の一つとしてサイバーセキュリティ人材が挙げられている。サイバーセキュリティ人材は、業務プロセスを支えるデジタル環境におけるサイバーセキュリティリスクの影響を抑制する対策を担う人材である。本稿では、デジタル人材の育成・確保、DX 推進スキル標準におけるサイバーセキュリティ人材、産業サイバーセキュリティ人材育成に関する IPA の取り組みを紹介する。

2.5 「診療業務を理解したセキュリティ人材の育成に向けて」

日本医療情報学会医療情報技師育成部会 谷川 琢海

昨今、医療機関が被害を受けているサイバー攻撃を受け、本年4月に医療法施行規則が改正され、サイバーセキュリティ確保するために必要な措置を講じることが新たに医療機関の責務として明文化された。また、同年5月には厚生労働省から「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」が示され、経営管理層の責任のもと医療機関の組織的な対応が求められるようになった。医療 DX を実現するためには、サイバーセキュリティの確保が前提あり、ガイドラインの要求に対して適切に対応していくためには、医療機関のなかでセキュリティに関する役割を担う人材の育成や配置を進めていくことが必要である。

医療機関に求められるセキュリティ人材は、サイバー攻撃による被害を未然に防止するための予防的な取り組みをはじめ、業務継続計画 (BCP) の策定と発動するための用意、万一被害を受けた場合にはセキュリティの専門家と医療機関の経営層との橋渡しなどの様々な役割を担うことが予想される。そのためには、医療機関の診療業務、病院情報システムの構成、ネットワーク構成を常に把握していなければならない。

医療情報技師は、医学医療、医療情報システム、情報処理技術について一定レベル以上の知識・技術を有する者、上級医療情報技師はそれに加えて医療情報システムに関する実務経験を求め、幅広い知識と豊かな経験に基づく、より

高度な実践的な知識・技術を有する者として、日本医療情報学会では能力検定試験を通して認定を行っている。医療情報技師と上級医療情報技師は、わが国の医療の情報化を担い、医学医療の専門家と情報処理技術の専門家の橋渡しができる人材であり、今後、上級医療情報技師や一定の業務経験を有する医療情報技師が、セキュリティに関する知識・技術をさらに身に着けることにより、診療現場を理解したセキュリティ人材として幅広く活躍することが期待される。