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

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
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
研究分担者 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
研究分担者 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

研究要旨
本研究は、安全・安心な地域医療を継続的に確保するため、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配置を目指すものである。医療機関におけるサイバー攻撃のリスクが高まる中、各機関は対策を進めているが、現状では資格やスキルを有する情報セキュリティ人材の配置が不十分である。そこで、本研究で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、「施設」や「人材」」が満たすべき要件を検討した。「医療情報セキュリティ人材」として Group A 人材、Group B 人材、Group C 人材が満たすべき要件を、「組織体制」については、「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」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」が満たすべき施設基準を定義した。

A. 研究目的

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では、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ている。

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、適切なスキルセットを持った情報セキュリティ人材の配置は十分に進んでいないと考えられる。このような人材不足の中、医療機関がより適切にサイバーセキュリティ対策を講じるためには、施設ごとに情報セキュリティ対策を進めることは難しく、医療機関が地域で情報セキュリティ対策を向上させる必要があると考えられた。そこで、本研究班では、地域に「指導的な立場の医療機関」を置き、「指導的な立場の医療機関」が「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」と連携して、情報セキュリティ対策を向上させる枠組みを提案している。本研究では、「施設」や「人材」」が満たすべき要件を、先行する医療安全対策や感染対策を参考に議論を行った。

B. 研究方法

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。

（倫理面への配慮）

本研究は情報セキュリティ人材の育成と配置に関して会議体で議論をした内容をまとめたものであり、特段の倫理的配慮と必要としない。

C. 研究結果および考察

「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。診療報酬の施設基準等には医療安全対策領域、感染症対策領域の目指すべき姿が記載されていると考え、加算の施設条件等を確認した。

1. 医療安全対策加算

医療安全対策加算に関する施設基準では、医療安全対策加算１の(1) 医療安全管理体制に関する基準として「ア 当該保険医療機関内に、医療安全対策に係る適切な研修を修了した専従の看護師、薬剤師その他の医療有資格者が医療安全管理者として配置されていること。」と適切な研修の修了が求められ、適切な研修とは、「(イ) 国又は医療関係団体等が主催するものであること。」、「(ロ) 医療安全管理者としての業務を実施する上で必要な内容を含む通算して 40 時間以上のものであること。」、「(ハ) 講義及び具体例に基づく演習等により、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。」が挙げられていた。情報セキュリティ人材についても、適切な研修を受けることは必要で、そのカリキュラムを開発することは意義があると判断した。そこで、医療情報セキュリティ人材の育成カリキュラムを開発することにした。

次いで、「イ 医療に係る安全管理を行う部門（以下「医療安全管理部門」という。）を設置していること。」と医療安全管理部門の設置が求められていた。医療情報セキュリティ人材の適正配置やキャリアパスを考えると、医療機関に医療情報システム管理部門があることは大切と思われる。そこで、「指導的な立場の医療機関」、「自院の情報システムを守ることができる医療機関」に対して、医療情報システム管理部門の設置を求めることとした。

(2) 医療安全管理者の行う業務に関する事項では、「オ 医療安全対策に係る体制を確保するための職員研修を企画・実施すること。」が求められている。医療情報セキュリティ対策についても、病院職員に広く周知を行う必要があり、これは情報セキュリティ対策を実施する全ての医療機関に必要なものと判断した。

医療安全対策地域連携加算１の施設基準では、「(3) 他の医療安全対策加算１に係る届出を行っている保険医療機関及び医療安全対策加算２に係る届出を行っている保険医療機関と連携し、それぞれ少なくとも年１回程度、医療安全対策地域連携加算１に関して連携しているいずれかの保険医療機関に

赴いて医療安全対策に関する評価を行い、当該保険医療機関にその内容を報告すること。また、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。」が求められていた。また、医療安全対策加算２では、「(2) 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。」が求められていた。「指導的な立場の医療機関」同士、あるいは「指導的な立場の医療機関」と「自院の情報システムを守ることができる医療機関」が互いの施設の情報セキュリティ対策を評価することが、評価を受ける施設の情報セキュリティ対策を高めるだけでなく、評価を行う情報セキュリティ人材が知見を深めることにつながる。そこで、「指導的な立場の医療機関」同士が相互チェックを行うこと、「指導的な立場の医療機関」が「自院の情報システムを守ることができる医療機関」のセキュリティチェックを行うこと、を求めることにした。

2. 感染対策向上加算

感染対策向上加算では、「感染対策向上加算1の届け出を行っている保険医療機関」が「感染対策向上加算2、感染対策向上加算3又は外来感染対策向上加算に係る届出を行った保険医療機関」に院内感染対策に関する助言を行う仕組みを有していた。「(1) 感染対策向上加算1の届出を行っている保険医療機関」が「感染制御チームの専従医師又は看護師が、過去1年間に4回以上、感染対策向上加算2、感染対策向上加算3又は外来感染対策向上加算に係る届出を行った保険医療機関に赴き院内感染対策に関する助言を行っていること。」で指導強化加算を得ることができる。また、「感染対策向上加算2又は感染対策向上加算3に係る届出を行っている保険医療機関」が「当該保険医療機関が連携する感染対策向上加算1に係る届出を行った他の保険医療機関に対し、過去1年間に4回以上、感染症の発生状況、抗菌薬の使用状況等について報告を行っていること。」で連携強化加算を得ることができる。本研究班では、「指導的な立場の医療機関」が「自院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」と連携し、地域で情報セキュリティ対策を向上させることを考えており、感染対策の仕組みはこれに合致すると考えられた。

感染対策向上加算 1 の施設基準として「(7) (2)の感染制御チームにより、保健所及び地域の医師会と連携し、感染対策向上加算2又は3に係る届出を行った保険医療機関と合同で、少なくとも年4回程度、定期的に院内感染対策に関するカンファレンスを行い、その内容を記録していること。また、このうち少なくとも1回は、新興感染症の発生等を想定した訓練を実施すること。」や、「(7) (2)の感染制御チームにより、感染対策向上加算2、感染対策向上加算3又は外来感染対策向上加算に係る届出を行った他の保険医療機関に対し、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こと。」が求められている。定期的なカンファレンスは、情報セキュリティの最新の知識を共有するために活用できると考えた。「新興感染症の発生等を想定した訓練」は情報セキュリティ領域では、「サイバー攻撃合同訓練」と読み替えること

ができると考えた。

感染対策においても、「(1) 感染防止対策部門を設置していること。」が求められ、やはり、医療情報システム管理部門を設置することは重要と考えられた。また、「(2) 感染制御チーム」では、「ア 感染症対策に３年以上の経験を有する専任の常勤医師（歯科医療を担当する保険医療機関にあっては、当該経験を有する専任の常勤歯科医師）」、「イ ５年以上感染管理に従事した経験を有し、感染管理に係る適切な研修を修了した専任の看護師」、「ウ ３年以上の病院勤務経験を持つ感染防止対策にかかわる専任の薬剤師」、「エ ３年以上の病院勤務経験を持つ専任の臨床検査技師」と感染管理や病院勤務の経験を求めていた。また、「(3) 感染症管理に係る適切な研修」では、医療安全と同様に、「(イ) 感染予防・管理システム」、「(ロ) 医療関連感染サーベイランス」、「(ハ) 感染防止技術」、「(ニ) 職業感染管理」、「(ホ) 感染管理指導」、「(ヘ) 感染管理相談」、「(ト) 洗浄・消毒・滅菌とファシリティマネジメント等について」と講義及び演習内容が定められていた。

これらの内容を参考にし、Group A 人材、Group B 人材、Group C 人材の要件と、「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」の施設要件を検討、更新した。

3. 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

4. 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。

D. 結論

医療安全管理や感染対策を参考に、「医療情報セキュリティ人材」として Group A 人材、Group B 人材、Group C 人材が満たすべき要件を、「組織体制」については、「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」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」が満たすべき施設基準を定義した。

E. 健康危険情報

なし

F. 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－

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

G. 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