「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」

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班
（令和 7 年 5 月 30 日）

初めに

医療機関の医療情報システムがサイバー攻撃の被害にあった場合、医療情報システム停止により診療業務の継続が困難になる可能性と、医療情報システムで管理される患者情報の紛失、外部への漏えいの可能性がある。

患者情報の紛失、外部への漏えいの可能性を考えると、医療情報システムを用いて診療を行う全ての医療機関は、情報システムに対して適切なセキュリティ対策を施す必要がある。

一方、診療業務の継続が困難になる可能性については、規模が大きい医療機関ほど、医療情報システムへの依存度が高くなるため、診療継続が困難になる可能性が高い。また、医療機関の規模に関わらず、診療継続が困難となった際、その地域の医療提供への影響が大きい医療機関（他医療機関で代替の診療を提供することができない）と小さい医療機関（他医療機関が代替の診療を提供することができる）が存在する。このように、地域ごとの医療機関の役割や規模に応じて、重点的に情報セキュリティ対策を施す必要のある医療機関が存在する。

保健医療福祉分野における情報セキュリティ人材は、保健医療福祉分野の情報システムの特性を理解していることと情報セキュリティに対する知識の双方が必要となる。このような人材は、保健医療福祉領域において、ほとんど存在しないのが実情である。このため、数の少ない医療情報セキュリティ人材を、医療継続が必要不可欠な医療機関に重点的に配置することが必要となる。

一方、全ての医療機関において最低限求められる情報セキュリティ対策を行う必要がある。このため、医療情報セキュリティ人材が配置された医療機関やその人材は、自施設だけでなく、地域の他医療機関に対して情報セキュリティ対策の指導やアドバイスを行うことが求められる。さらに、これらの医療機関や医療情報セキュリティ人材は、新たな医療情報セキュリティ人材の育成に向けた取り組みを平行して行うことが求められる。

このように、医療機関ごとの点ではなく、地域として面で、情報セキュリティ対策を施しながら、人材育成を平行して進めることで、将来的には多くの医療機関に医療情報セキュリティ人材が充填され、患者に対して安全、安心な医療が提供できることを期待する。

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

医療機関を「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」に分け、その役割や配置すべき医療情報セキュリティ人材の整理を行った。

各医療機関や各医療機関が配置する医療情報セキュリティ人材が果たすべき役割として、日ごろの情報セキュリティ対策を講じるところまでを考慮した。実際に情報セキュリティインシデントが発生した際は、外部からさらに専門性の高い情報セキュリティ人材が医療機関に派遣され、医療機関が配置する医療情報セキュリティ人材と協働して、医療提供機能の回復を図ることを想定している。

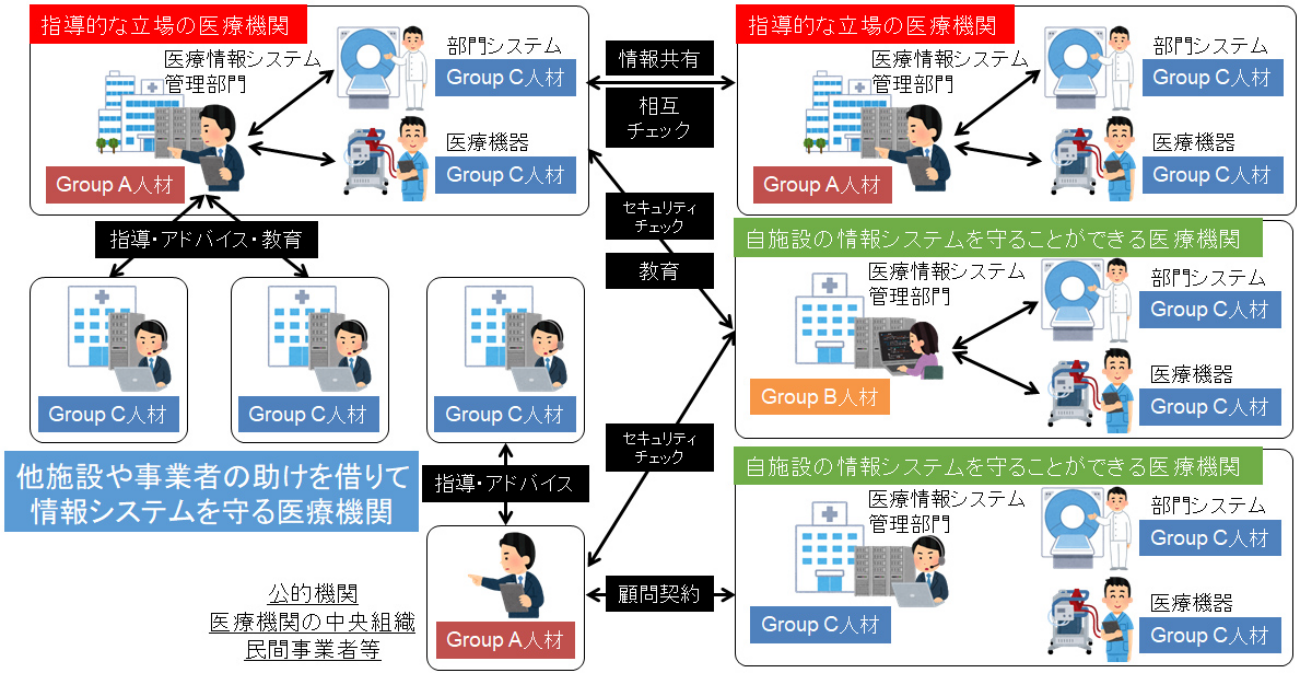

図１．医療機関ごとの役割分担や配置すべき医療情報セキュリティ人材の概念図

「指導的な立場の医療機関」の Group A 人材が中心となって、自施設、「自施設の情報システムを守ることのできる医療機関」、「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」に所属する Group B 人材、Group C 人材と協働しながら、地域の医療機関が広くサイバーセキュリティ対策を強化する。また、「指導的な立場の医療機関」は地域の医療情報セキュリティ人材の育成に努める。

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人材（本研究班での「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。

【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。

【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。

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

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は、「Group A 人材」、「Group B 人材」、「Group C 人材」の 3 つに分けて整理を行った。
「Group A 人材」、「Group B 人材」、「Group C 人材」が持つべき知識、備えるべきスキル、実行レベルについては、１．役職間の関係（任務分離）、２．Cybersecurity Framework(CSF)視点（攻撃者視点対策能力）、３．Continuous Diagnostics and Mitigation (CDM)視点（防衛者視点対策能力）、４．security-by-design（設計者視点）、５．incident-response-recovery（緊急対応能力）、６．保守業務ならびに計画（運用維持能力）に対して要求項目を整理した（別表 1)。医療系国家資格の教育カリキュラムや国家試験ごとの出題基準と出題実績、医療情報技師、診療情報管理士の教育カリキュラムや資格試験の出題基準を調査した結果、医療情報技師がもっとも情報セキュリティに関する教育カリキュラムが充実していた。そこで、上記 6 視点に対して、医療情報技師、上級医療情報技師、情報セキュリティマネジメント（IPA レベル 2)、応用情報技術者（IPA レベル 3)、情報処理安全確保支援士（IPA レベル 4）のそれぞれの団体が定める到着目標のマッピングを行った（表 1、別表 2)。
「Group A 人材」、「Group B 人材」、「Group C 人材」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を行った。一人の人材が医療情報システムに対する知識と情報セキュリティに対する知識を合わせ持つことが望まれるが、同一組織内で良好なコミュニケーションが取れることを条件に、医療情報システムに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が協力して情報セキュリティ対策に取り組むことを許容することとした。

表１．医療情報セキュリティ人材が持つべき資格・知識

	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
Group A 人材	「上級医療情報技師」相当の資格・知識	「情報処理安全確保支援士」（IPA レベル 4）相当の資格・知識
Group B 人材	「医療情報技師」相当の資格・知識	「情報セキュリティマネジメント試験」（IPA レベル 2）相当の知識
Group C 人材	「医療情報基礎知識検定試験」相当の知識	「IT パスポート試験」（IPA レベル 1）相当の知識

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。

【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。

【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」と連携した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。

【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と協力した、システム復旧に向けた取り組み
- 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

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

Group A 人材、Group B 人材、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下記にまとめた。感染症対策や医療安全などと同じ様に、セミナーの開催や受講管理、受講修了証の発行などを管

理する仕組み（組織）が必要となる。
教育コンテンツについては、厚生労働省や経済産業省・IPA、内閣サイバーセキュリティセンター（NISC）などの行政のプラットフォームをはじめ、学会・団体でも多くのコンテンツが用意されている。これらのコンテンツと提示する教育カリキュラムとのマッピングを行うことができれば、教育コンテンツ作成や更新に係る労力を抑えることが期待される。
不足する教育コンテンツについては、新規作成が必要となる。IPA や医療情報技師育成部会の協力を得ながら、コンテンツを作成することが期待される。

① Group A 人材

〇到達目標
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、実効性のある提案や助言を行うとともに、セキュリティ人材の育成を行うことができる。
〇教育コンテンツ
【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

※「上級医療情報技師」の資格保有者は、新規講習 8〜15 の受講を免除する。
※IPA「情報処理安全確保支援士」資格保有者は新規講習 1-7 の受講を免除する。
【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 Group B 人材

○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期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への対応
3. コンピュータシステムのセキュリティ対策
4. ネットワークのセキュリティ対策
5. データベースおよびデータのセキュリティ対策
6. 情報セキュリティに関する法制度
7. プロジェクトマネジメントとサービスマネジメント
8. 医療現場の診療業務フロー
9. 医療情報システムの機能及び役割
10. 医療情報システムの調達と運用保守
11. 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）
12. 医療情報システムの安全管理対策（企画管理編）
13. 医療情報システムの安全管理対策（システム運用編）
14. 医療情報システム／セキュリティを支える施設基盤
15. インシデント発生時の適切な初動対応

※「医療情報技師」 「上級医療情報技師」の資格保有者は、新規講習 8～15 の受講を免除する。

※IPA「情報セキュリティマネジメント試験」合格者、「情報処理安全確保支援士」試験合格者は新規講習 1-7 の受講を免除する。

【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

③ Group C 人材

〇到達目標

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。

〇教育コンテンツ

【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。

新規講習は必須プログラムと医療および医療情報システムに関する任意プログラム①、情報処理技術に関する任意プログラム②で構成される。

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

※出題基準等に情報セキュリティに関する項目が含まれている国家資格（診療放射線技師、臨床工学技士、臨床検査技師）および診療情報管理士、医療情報基礎知識検定試験の合格者は必須プログラムのみ受講を義務付ける。

※IPA の IT パスポート（レベル 1）以上の合格者は、必須プログラムの受講を義務付けるほか、任意プログラム①の受講を推奨する。

※出題基準等に情報セキュリティに関する項目が含まれていない国家資格については、必須プログラムの受講を義務付けるほか、任意プログラム②の受講を推奨する。

【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

４．補足事項

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

本研究班で令和 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、回答施設 643 施設のうち、92.1%（400 床以上 : 99.6%）の医療機関が医療情報システム安全管理責任者や情報セキュリティ事案の担当者を配置しており、情報セキュリティ対策の必要性は広く浸透していると考えられる。一方、「上級医療情報技師」は 5.6%（400 床以上 : 10.6%）、「医療情報技師」は 28.5%（400 床以上 : 37.4%）、「情報処理安全確保支援士」は 2.5%（400 床以上 : 6.0%）、「情報セキュリティマネジメント試験」は 4.8%（400 床以上 : 6.0%）の医療機関での雇用にとどまり、医療情報セキュリティの資格を有する人材は豊富でないことが明らかとなっている。そこで、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は、医療機関で広く人材雇用が進むことを念頭に、将来の資格保有を推奨しながら、実務経験や教育の受講で対応できる内容とした。

４－２．Group A 人材の安定した雇用に向けて

「Group A 人材」は高い知識や技術を持つ人材となるため、医療福祉領域で、十分な人数の確保が困難となることが想定される。このため、「Group A 人材」を雇用する医療機関は、「Group A 人材」が他施設の情報セキュリティ対策を援助できる体制を構築する必要がある。

「Group A 人材」の雇用経費を単一の医療機関で確保できないケースが想定される。また、安価な報酬を理由に、せっかく育った「Group A 人材」が医療福祉領域以外に流出することを防ぐ必要がある。

このために、「Group A 人材」を雇用する医療機関は、兼業を認めることで他施設から報酬を得る仕組みを考慮するなど、地域として「Group A 人材」を確保する取り組みが求められる。

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

「自施設の情報システムを守ることができる医療機関」は、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や 400 床以上の医療機関を想定しており、候補となる医療機関は少なくない。すべての医療機関が Group B 人材の確保をすることは困難であることが想定され、一部の医療機関では Group C 人材を確保し、個人、事業者等の Group A 人材と契約の上、情報セキュリティ対策を講じることを想定した。

医療機関外の Group A 人材との契約については、大きく 3 つが想定される。１つ目として、自治体等が配置する医療機関を指導する Group A 人材と契約を結ぶ方法が考えられる。Group A 人材を配置する自治体等に限定されることは言うまでもない。2 つ目として、グループ医療機関や同一法人の医療機関が中央組織に Group A 人材を配置する方法が考えられる。３つ目として、個人や事業者が雇用する Group A 人材と契約を結ぶ方法が考えられる。医療機関外の情報セキュリティ人材については、医療情報システムの特性を理解している人材を見つけることが課題となる。独立行政法人情報処理推進機構（IPA）では令和 6 年度セキュリティ人材活用促進実証として、登録情報セキュリティスペシャリスト（登録セキスペ）アクティブリストの活用が検討されている。アクティブリストでは支援業種を選択して人材検索を行うことが検討されている。医療領域の人材として、Group A 人材の知識やスキルセットを要求することで人

材検索が可能となることが期待される。また、一般社団法人医療サイバーセキュリティ協議会（MedCSC）では、医療機関と情報処理安全確保支援士会（JP-RISSA）との情報交換プラットフォームの構築が検討されている。医療情報セキュリティ人材登録のプロセスで Group A 人材の知識やスキルセットを要求することが考えられる。今後、IPA や MedCSC と継続して連携をすることで、個人、事業者等の情報セキュリティ人材活用に向けた課題解決が期待される。

医療現場での経験がない人材が今後活躍できるよう支援することも人材増加に対して重要なアプローチであると考えられる。高いレベルでの医療情報システムを体系的に習得できるプログラムの例として、2024 年度に開設された名古屋医療情報学プログラム(NCIP)企業(一般社会人向け)リスキリングコースが挙げられる。現在、全国の大学病院ならびに医学部では、院内電算化に始まり電子カルテ導入まで継続する一連の医療情報システム化時代に比べて運用が定型化され外注化が進んだことから、体系的に病院情報システムについて習得する機会や OJT に相当する経験を積むことができる施設が減少していると考えられる。Group A 人材ならびに Group B 人材は高い実践能力が求められることから、特に Group A 人材を擁する医療機関においては、Group A 人材の支援環境整備に加えて OJT を可能にする環境整備の充実が強く求められると考察される。