「医療安全の確保や医療の質保証と情報セキュリティ対策の確保に関して、組織的に PDCA サイクルを実行するための提言」

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となることが想定される。短期的には、救急医療等の緊急性の高い医療が提供できず、患者の命を救う機会が奪われかねない。また、緊急性の高い患者の救急車・ヘリコプターによる搬送で公費支出がかさむことが想定される。先例により、医療情報システムの復旧には月単位の時間が必要となることが想定され、この間、医療機関は限られた診療情報を使った紙カルテ運用を行う必要がある。大規模医療機関では 2010 年前後より電子カルテ導入が進められており、40 歳未満の医療スタッフの多くは紙カルテ運用が未経験であることが想定される。限られた診療情報、慣れない紙カルテ運用、電子カルテの医療安全機能が使えない状況での、診療、看護の実施は医療安全上、大きなリスクとなる。

さらに、サイバーインシデントの際、患者の個人情報（診療情報）が漏えいすることが少なくない。漏えいした個人情報の回収は難しく、ダークウェブサイトで公開されるリスクが永続的に発生する。また、システム障害が発生した医療情報システムに対してはデジタルフォレンジック作業、システム復旧作業が行われるが、全ての診療情報の復旧が困難となるケースが想定される。その結果、過去の診療記録が失われ、患者の継続診療に不具合が生じることになる。

医療安全の確保や医療の質保証を行うため、患者の個人情報を適切に守るために、医療機関は日ごろから情報セキュリティ対策を徹底すること、情報セキュリティインシデントへの備え（医療情報システムの早期復旧に向けた対策、サイバーインシデント想定した事業継続計画の策定、サイバーインシデントを想定した災害訓練など）を行う必要がある。このためには、「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」で示した組織体制の構築と人材配置が求められる。

本研究班が令和 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、保健医療福祉分野の情報システムの特性を理解しながら、情報セキュリティの知識を持つ人材の医療機関への配置は十分ではないことが明らかとなっている。このため、「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」は、将来の資格保有を推奨しながら、まずは各医療機関が情報セキュリティ人材の配置を進めることができるように、実務経験や教育の受講を重視する提言となっている。医療機関や医療機関に雇用された情報セキュリティ人材は、最新の医療情報システムや情報セキュリティに関する知識の獲得や、他医療機関の取り組みや経験の共有により、組織、個人として成長し、将来、医療機関でより確実な情報セキュリティ対策を確保するための PDCA サイクルを実行する必要がある。

1. 医療情報セキュリティ人材の育成と情報セキュリティに関する最新の知識の確保

医療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の知識の双方が要求される。さらに、情報セキュリティの知識は常に最新の情報に更新を行う必要がある。

保健医療福祉分野の情報システムの特性の理解

保健医療福祉分野の情報システムの特性の理解については、医療機関等での実務経験が重要となる。実務経験については、医療機関等の職員や医療情報システム事業者の担当者として医療情報システムの導入、更新、維持管理に関わるケースが想定される。これらの実務経験により、ある程度、保健医療福祉分野の情報システムの特性を理解することは可能であるが、より系統だった知識の担保に、本研究班での調査で教育カリキュラムが最も整理されていた医療情報技師、上級医療情報技師の資格取得が望まれる。

情報セキュリティ人材については、医療領域に所属する人材では不足することが想定される。このため、医療領域外の情報セキュリティ人材が、保健医療福祉分野の情報システムの特性を理解して、情報セキュリティ対策を講じることができる枠組みが必要となる。「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」では「指導的な立場の医療機関」に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を求めている。医療領域外の情報セキュリティ人材についても実地研修受け入れることで、保健医療福祉分野の情報システムの特性の理解が進むと考えられる。情報処理安全確保支援士は登録情報セキュリティスペシャリスト（登録セキスペ）に登録することが可能であるが、独立行政法人情報処理推進機構（IPA）では、登録セキスペアクティブリストの整備が検討されている。アクティブリストによる人材検索で、支援業種として医療を選択した場合、保健医療福祉分野の情報システムの特性の理解した情報セキュリティ人材が検索される仕組みが望まれる。このためには、情報処理安全確保支援士の更新に必要な講習で、保健医療福祉領域に特化した講習を用意し受講した人材を検索対象にすることや、医療情報技師、上級医療情報技師の資格を有する人材を検索対象にする方法が考えられる。アクティブリスト整備が進む事で、保健医療福祉領域に参入する登録セキスペが増えることが期待される。

情報セキュリティに対する知識の担保

本研究班の調査では、医療系専門職において医療情報技師、上級医療情報技師が最も情報セキュリティに対する教育が整備されていることを確認した。一方、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、それぞれの領域で合格点の取得が必要となる試験で、各領域で全ての知識を網羅する必要はなく、結果、情報セキュリティに知識を担保する資格とはなっていない。

情報セキュリティに対する知識の担保については、IPA の情報処理安全確保支援士、情報セキュリティマネジメント試験、IT パスポート試験などが挙げられる。本研究班のアンケート調査では、これらの IPA 資格、試験を有する病院職員は多くない。情報セキュリティに対する知識を持つ人材を広く医療機関に配置するために、短期的には情報セキュリティに対する教育の受講が有効であると考えた。長期的には、情報セキュリティ人材の知識の担保や安定した雇用を考えると、「Group A 人材」では情報処理安全確保支援士の資格取得、「Group B 人材」では情報セキュリティマネジメント試験への合格、「Group C 人材」では IT パスポート試験への合格が強く推奨される。

最新の情報セキュリティの知識の担保

情報セキュリティ対策に向けて、情報セキュリティ人材だけでなく、全ての病院職員がそれぞれのレベルに応じて、

情報セキュリティに対する最新の知識を確保する必要がある。情報セキュリティの知識の獲得に向けては、内閣府サイバーセキュリティセンター、厚生労働省医療機関向けセキュリティ教育支援ポータルサイト、独立行政法人情報処理推進機構などが最新の情報セキュリティに関する情報を発信している。また、CISSMED (Cyber Intelligence Sharing SIG for Medical)などを利用し、情報セキュリティ人材間での知識共有を行うことが想定される。全ての医療機関の情報セキュリティ人材が等しく、自律的に最新の情報を担保することは容易ではないと考えられる。

「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」では「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を求めている。さらに、「指導的な立場の医療機関」および「Group A 人材」は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」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」がこのカンファレンスに参加することを求めた。「指導的な立場の医療機関」および「Group A 人材」はカンファレンス開催に向けて、最新の情報セキュリティに関する知識の獲得に取り組むことが想定され、カンファレンスに参加する情報セキュリティ人材はカンファレンスで最新の知識を獲得することが期待される。

提言では「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」、「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」、全ての医療機関に対して自施設の病院職員教育を求めている。なお、「Group A 人材」については、自施設だけでなく他施設の職員教育を求めている。「Group C 人材」が自ら職員教育を行うことが難しいケースを想定して、「Group A 人材」への講演依頼や e-Learning の活用も想定をしている。

2. 情報セキュリティ人材の育成と医療機関等におけるサイバーセキュリティ対策の質的向上

医療機関等におけるサイバーセキュリティ対策については、医療情報システムの安全管理に関するガイドラインのうち優先的に取り組むべき事項が「医療機関におけるサイバーセキュリティ対策チェックリスト」として取りまとめられた。各医療機関ではチェックリストに従いサイバーセキュリティ対策が進められているが、具体的な対策は各医療機関の情報セキュリティ担当者の判断に委ねられており、有効な対策がどこまでとられているかは医療機関ごとに異なることが想定される。全国の医療機関が広くサイバーセキュリティ対策について向上するためには、各医療機関のサイバーセキュリティ対策の質的評価や、グッドプラクティスの共有などの仕組みが求められる。

「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」では「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、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や「Group A 人材」がその実務を担当することを求めている。「Group A 人材」が「指導的な立場の医療機関」の情報セキュリティ対策の相互チェックを行うことは、対象施設の情報セキュリティ対策の向上に向けた具体的なアドバイスだけでなく、自施設の情報セキュリティ対策の向上に活かすことができると考えられる。また、「Group A 人材」は「指導的な立場の医療機関」間の相互チェックで得られた知見を用いて、「自施設の情報システムを守ることができる医療機関」に対するセキュリティチェックを実施することが可能となる。「自施設の情報システムを守ることができる医療機関」の「Group B 人材」はセキュリティチェックを通じ、「Group A 人材」との交流や情報共有を行うことが可能となる。このように、数年間は医療機関同士がお互いの情報セキュリティ対策を学ぶ形で、各医療機関の情報セキュリティ対策の質を高めるとともに、「Group A 人材」、「Group B 人材」の育成につながると考える。さらに、「指導的な立場の医療機関」同士の相互チェックや「自施設

の情報システムを守ることができる医療機関」に対するセキュリティチェックを重ねることにより、保健医療福祉分野における情報セキュリティ対策の水準を定めることができる。「指導的な立場の医療機関」は、将来、医療機関等における情報セキュリティ監査基準として取りまとめることが期待される。情報セキュリティ人材を配置する医療機関は、「医療機関におけるサイバーセキュリティ対策チェックリスト」に加え、相互チェックやセキュリティチェックでの経験（将来的には情報セキュリティ監査基準）を活かし、自施設の医療情報システムの内部監査（自己点検・評価）を行い、外部評価（自施設に対する相互チェック、セキュリティチェック）の結果と合わせて、日々の情報セキュリティ対策向上につなげることが求められる。

医療情報システムの保守運用について外部委託を行っている医療機関は少なくない。既に導入されている医療情報システムに対して適切なセキュリティ対策を講じることは、契約や運用面、費用面、導入システムでの制限事項などの理由により、容易でないケースが想定される。日々の情報セキュリティ対策が大切であることは当然のことであるが、大きく情報セキュリティ対策を向上させるために、医療情報システム全体の運用や契約・費用に関する現状の棚卸しが必要となる。医療機関では 5、6 年に一度、医療情報システムの更新が行われるが、医療情報システムの更新は情報セキュリティ対策を見直す絶好の機会となる。情報セキュリティ人材は、医療情報システム更新に向けて、自施設の医療情報システムの仕様、運用、契約を整理し、セキュリティチェックリスト、内部監査、外部監査（相互チェックやセキュリティチェック）を通じて学んだ自施設の問題点、改善点を取りまとめた上で、公的医療機関は医療情報システム仕様書、民間医療機関は医療情報システム機能要求に反映をする必要がある。仕様書の作成や機能要求を外部コンサルタント業者に委託する場合は、外部コンサルタントが情報セキュリティに対する正しい知識を保有することを確認し（できればGroup A 人材を配置するコンサルタントが好ましい）、自施設の問題点、改善点が反映される仕様書となるように、連携を密に取る必要がある。医療情報システムの保守運用を外部事業者に委託する場合は、自施設の情報セキュリティ人材と外部事業者の役割を明確にし、契約に反映をさせる必要がある。

3. サイバー攻撃を想定した事業継続計画（BCP）の策定とサイバー攻撃合同訓練

「医療機関におけるサイバーセキュリティ対策チェックリスト」ではサイバー攻撃を想定した事業継続計画（BCP）の策定が求められる。厚生労働省は「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き」、「医療情報システム部門等における事業継続計画（BCP）のひな形」を公開している。サイバー攻撃の被害にあった大阪急性期・総合医療センターではホームページ上でIT-BCPが公開されている。各医療機関で策定したサイバー攻撃を想定したBCPについても「指導的な立場の医療機関」間の相互チェックや「自施設の情報システムを守ることができる医療機関」へのセキュリティチェックの対象となり、IT-BCPの質向上につながると考える。また、「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」に対しては、「Group A 人材」が上記取り組みを通じた獲得した知見を含め、IT-BCPの策定や改訂を支援することが想定される。

策定したIT-BCPが正しく機能するためには、サイバー攻撃合同訓練への参加が必要となる。サイバー攻撃訓練については、内閣府サイバーセキュリティセンターが重要インフラ対策として実施する全分野一斉演習への参加などを行っている状況である。災害対策については災害派遣医療チーム（DMAT）による合同防災訓練が実施されている。保健医療福祉分野により特化したサイバー攻撃訓練となるためには、医療機関がサイバー攻撃合同訓練を主催することが必要と考え、「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」では「指導的な立場の医療機関」に「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を求めた。サイバー攻撃合同訓練を繰り返すことで、有効な訓練の主催が可能となると共に、IT-BCP へのフィードバックが可能になることが想定される。

4. 情報セキュリティ人材の適正配置、キャリアパス、医療領域からの人材流出の防止

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、「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」での「Group A 人材」、「Group B 人材」、「Group C 人材」の適正配置が強く望まれる。

医療機関においては、情報セキュリティ人材の配置や情報セキュリティ対策への設備投資について、費用の確保が課題となる。医療機関で医療安全人材や感染症対策人材が定着していることは、医療機関における人材確保の必要性はもちろんのこと、医療安全対策加算や感染対策向上加算での施設基準や診療報酬によることが大きいことは間違いない。情報セキュリティ人材の確保においても、加算がつくことで医療機関は施設基準を満たすように努力することが想定され、医療機関での情報セキュリティ対策の向上に大きく貢献することが期待される。また、加算が付くことは、医療領域外の情報セキュリティ人材が医療領域に参入するきっかけとなり、人材不足が解消する可能性も期待される。

医療機関においては、現在の情報セキュリティ担当者に対して、保健医療福祉分野の情報システムの特性の理解と情報セキュリティに対する知識の担保を求めることが最も効率的であると考える。確実な知識や技術の担保には、「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」で取り上げた資格や試験の取得が望まれる。個々の人材においては、情報セキュリティに関する教育の受講、資格、試験の取得に向けた学習や受験、資格取得後の資格の維持に多大な労力と費用が発生するため、その対価を示すことが大切となる。

情報セキュリティ人材のキャリアパス

「医療機関におけるサイバーセキュリティ対策チェックリスト」では医療機関に医療情報システム安全管理責任者を置くことが求められている。本研究班で行った調査で、多くの医療機関で医療情報システム安全管理責任者を配置が進んでいるが、病院長や副病院長、事務長など病院執行部がその役割を担うことが多く、情報セキュリティに関する資格、試験を保有する割合は低い。医療機関が情報セキュリティ対策を進めるためには、病院執行部の意思決定が重要であり、病院執行部が医療情報システム安全管理責任者となることの意義は大きい。一方、情報セキュリティに対する知識が乏しい場合、正しい意思決定を行うことができるかについては課題が残る。大企業などでは組織のデータを保護するために使用するサイバーセキュリティ戦略を設計し、組織全体のリスクを評価して、サイバー防御を改善する責任をもつ CISO（Chief Information Security Officer）を配置することが求められる。医療機関においても、医療情報システム安全管理責任者が CISO として活動することで、確実な情報セキュリティ対策が進むと考えられるが、今すぐ、CISO の候補となる人材を確保している医療機関は多くないと考えられる。そこで、将来、CISO の候補となる人材を育成することが求められる。

「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」では、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」に医療情報システム管理部門を設置することを求めている。医療情報システム管理部門の設置により、組織としては、確実な情報セキュ

リティ戦略の設計を求めることが可能となる。雇用される「Group A 人材」、「Group B 人材」に対しては、医療情報システム管理部門の長として登用されることを想定するキャリアパスを提示することができ、部門長あるいはさらに上の立場で病院運営に関わることは、情報セキュリティ人材が CISO の役割を担う組織づくりにつながると考えられる。

「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」では、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」、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を求めている。医療機関における情報セキュリティ対策は迅速な対応が求められ、人材育成を待つ時間はない。このため、現時点においては情報セキュリティ戦略に向けた意思決定部分と戦略立案に向けた知識、技能部分を「Group A 人材」、「Group B 人材」が担うことを想定している。「Group A 人材」、「Group B 人材」が「統括情報セキュリティ責任者」を補助する立場で仕事をすることで、情報セキュリティ戦略に向けた意思決定を学び、医療機関における CISO の役割を担うことができる人材として育成されることが期待される。

一方、「Group C 人材」には異なるキャリアパスを示す必要がある。「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」では CISO を置くことは現実的でなく、外部 CISO の力を借りて、情報セキュリティ戦略を立案することが想定される。このため、「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」では診療放射線技師や臨床工学技士といった医療系専門職を「Group C 人材」として育てることが現実的である。また、「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」においても、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」を配置が求められるが、それぞれの部門で働く医療系専門職から「Group C 人材」を育成することが想定される。多くの医療機関ではぎりぎりの人数で業務が遂行されているが、「Group C 人材」を配置することでプラス1の雇用枠が確保できれば、本来業務の負担軽減、業務拡大につながることが期待される。近年、部門業務の遂行には部門システムの有効活用が必須となっており、部門システム戦略に関わることになる「Group C 人材」は部門の管理者として育成されることが期待される。

情報セキュリティ人材の待遇

厚生労働省が実施する賃金構造基本統計調査によれば、システムコンサルタント・設計者、ソフトウェア作成者、その他の情報処理・通信技術者は、医師、歯科医師を除く医療系専門職やその他の保健医療従事者と比べ給与が高い。医療機関においては、情報セキュリティに関する資格、試験の取得に向けた経済的支援はもちろんのこと、資格、試験の取得者に対する待遇改善は、資格、試験の取得、維持に向けた最も分かりやすいモチベーションとなる。私立の医療機関ではこういった待遇改善が可能と思われるが、公的医療機関では給与水準が医療系資格により決められているため、待遇改善は容易でないことが想定される。一方、待遇改善がない場合、育成した情報セキュリティ人材が他施設や医療領域外に流出する懸念がある。特に、医療領域外への流出は避ける必要がある。

「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」では、「自施設の情報システムを守ることができる医療機関」に「Group B 人材」の配置と、外部「Group A 人材」との契約下に「Group C 人材」の配置の 2 つの選択肢を提案している。これは、グループ医療機関の中央組織に「Group A 人材」を配置、各医療機関には「Group C 人材」を配置し、グループ全体で情報セキュリティ戦略を構築することを想定している。このような中央組織に配置される「Group A 人材」に対する適切な待遇は比較的容易であることが期待される。

保健医療福祉領域で情報セキュリティ人材が不足する中、「Group A 人材」は自施設だけでなく、他施設の情報セキュリティ対策の支援が求められる。公的な医療機関等で「Group A 人材」への待遇改善が困難である場合、他施設に対する支援を兼業として認め、他施設から報酬を得る仕組みを考慮することで、「Group A 人材」の継続確保が可能になると考える。

人材セキュリティ人材の医療領域からの流出防止

「Group A 人材」は必ずしも医療機関に所属する必要はなく、民間事業者に所属しながら、あるいは個人として医療機関の情報セキュリティ対策を支援するビジネスモデルが想定される。民間事業者が医療機関で経験を積んだ「Group A 人材」の受け皿となること、「Group A 人材」が個人として活躍するキャリアパスを示すことは、せっかく育った情報セキュリティ人材が医療領域外に流出することを防ぐ意味でも大切である。

前述の通り、IPA では登録セキスペアクティブリストの整備が検討され、医療領域で活躍する登録セキスペの検索が可能となることが期待される。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おり、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想定される。これらの取り組みを通じて、医療機関と民間事業者あるいは個人で活躍する「Group A 人材」のマッチングが成立することが期待される。

情報セキュリティ人材の適正配置と継続的な確保

医療機関の立場に応じて、情報セキュリティ人材を適切に配置することの重要性は、「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」で示した通りである。

医療機関における情報セキュリティ対策は各医療機関の医療情報システムの特性や運用に合わせて講じる必要があるため、情報セキュリティ人材が適切な情報セキュリティ戦略を講じるためには、ある程度当該医療機関への勤務経験が必要となることが多い。また、医療領域における情報セキュリティ人材は不足しており、欠員ができた際に、すぐに情報セキュリティ人材を確保することは難しいことが予想される。以上の状況から、最低限の人数の情報セキュリティ人材で情報セキュリティ対策を講じることは医療機関にとってリスクとなることをまず理解する必要がある。

「指導的な立場の医療機関」は言うまでもなく、「自施設の情報システムを守ることができる医療機関」については、情報セキュリティ人材を育成し、地域の医療機関に提供する役割が望まれる。「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」で最低限の人数の情報セキュリティ人材で情報セキュリティ管理を行った場合、自施設の情報セキュリティ対策を賄うことに精一杯となり、他施設への人材提供は困難となる。

以上の理由から、「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」が安定して継続的に情報セキュリティ対策を講じ、自施設で育成した情報セキュリティ人材を地域に提供するために、これらの医療機関は、余裕を持った人数の情報セキュリティ人材を確保することが強く望まれる。

「Group A 人材」、「Group B 人材」はそれぞれの組織の医療情報システム部門長や CISO を目指すことが想定されるが、全ての人材が部門長、CISO となれるわけではない。「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で育成された「Group A 人材」、「Group B 人材」が、より良い待遇で地域の医療機関に就職することができれば、これらの人材が「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」で教育を受け、医療情報システム、情報セキュリティに関する資格、試験を取得する大きな

モチベーションになる。退職後、民間事業者や個人として医療機関の情報セキュリティ対策に従事する情報セキュリティ人材にとっても同様である。「指導的な立場の医療機関」や「自施設の情報システムを守ることができる医療機関」は欠員となった枠を使って若手の情報セキュリティ人材を雇用し、教育をすることで、新たな情報セキュリティ人材が育ってくる上、当該施設の組織の若返りをはかることが可能となる。