公募シンポジウム
公募シンポジウム1
医療 CISOの人材育成ロードマップは如何にあるべきか
2022年11月18日(金) 09:30 ～ 11:30 C会場 (中ホールA)

[2-C-1] 医療 CISOの人材育成ロードマップは如何にあるべきか How is the roadmap of human resource development of medical CISO?

*黒田 知宏[1]、齋藤 勇一郎[2] （1. 京都大学、2. 群馬大学）
*Tomohiro Kuroda[1], Yuichiro Saito[2] （1. Kyoto University, 2. Gunma University）

キーワード：medical CISO, information security, business of medical institutions, human resource development

近年、全世界的にサイバー攻撃が増加しており、医療機関を狙った攻撃も後を絶たない。本邦においても、残念ながらサイバー攻撃を受けて医療機関が機能停止に陥る事例が相次いで報告されており、医療機関の BCP（事業継続）、ひいては地域の医療体制の維持への重大な脅威になっている。 厚生労働省からは令和4年度の診療報酬改定に伴い、診療録管理体制加算の施設基準に400床以上の保険医療機関については専任の医療情報システム安全管理責任者を配置することなどが加えられた。「医療情報システム安全管理責任者」の明確な定義は与えられていないが、厚生労働省「医療情報システムの安全管理に関するガイドライン」の付属文書「医療情報システム等の障害発生時の対応フローチャート」の「サイバーセキュリティ体制図（例）」を見ると、情報セキュリティ責任者（ CISO: Chief Information Security Officer）の直下にあって全部門を束ね、委託事業者や所轄官庁等へ連絡をする扇の要として描かれていることから、一般的に CISO補佐と呼ばれる、技術・戦略立案面で CISOを補佐する役割を負い、将来 CISOとなるキャリアパスも想定される人物を指すものと考えられる。 CISOは自社の経営状況や経営戦略を理解したうえで、セキュリティー施策の立案と施行を担う役割であることから、医療機関の CISO・CISO補佐は、医療と情報技術の両方に深い知識を有することが求められる人物であり、正に本会に集う方々に他ならない。 本シンポジウムでは、サイバーレジリエンス構成学がご専門の奈良先端科学技術大学院大学 門林雄基教授、内閣情報セキュリティーセンター 紺野博行 審議官、情報処理推進機構 奥村明俊 理事 の他、学会内の有識者に講演を賜り、 CISO・ CISO補佐に求められる人材像を考え、その育成を本会が担うにあたっての方略を議論する。

©一般社団法人 日本医療情報学会

医療 CISO の人材育成ロードマップは如何にあるべきか

黒田知宏[*1]、齋藤勇一郎[*2]、
*1 京都大学、*2 群馬大学、

How is the roadmap of human resource development of medical CISO?

Tomohiro KURODA[*1], Yuichiro SAITO[*2]
*1 Kyoto University, *2 Gunma University

Abstract

Nowadays, cyberattacks targeting social infrastructures including medical organizations are increasing. Unfortunately, several cases in which hospitals stop their function due to cyberattacks are reported in Japan. Thus, cybersecurity is indispensable factor of business continuity plan of medical institutions. The Chief Information Security Officer (CISO), a person responsible for cybersecurity of an organization, is should understand business management of the organization and cybersecurity technologies. Thus, the CISO of medical institutions, should be a person who understand clinical medicine and cybersecurity. The Japanese Association of Medical Informatics has been developing human resources who understand business of clinical medicine and information technology to support development, implementation and management of hospital information systems. Adding education, training, and examination opportunities to be information security specialist to this human resource development system, we should quickly establish the roadmap of human resource development system of medical CISO.

Keywords: medical CISO, information security specialist, business of medical institutions, human resource development.

1. 緒言

近年、世界的にサイバー攻撃が増加しており、医療機関を狙った攻撃も後を絶たない。本邦においても、残念ながらサイバー攻撃を受けて医療機関が機能停止に陥る事例が相次いで報告されており [1~3]、医療機関の事業継続、ひいては地域の医療体制の維持への重大な脅威になっている。したがって、医療機関が自らの事業継続計画 (Business Continuity Plan：BCP) 策定を行う上では、情報セキュリティ対策もその中に組み入れる必要がある。

近年、組織の情報セキュリティ戦略を定める存在として、CISO（Chief Information Security Officer）という新たなC-Suite の必要性が論じられている。

したがって、医療分野全体のセキュリティを高めるためには、その役割を負える人材を育成する必要があるのでは無いかと考える。

本稿では、その人材のあり方について考える。

2. CISO の定義と求められる人材像

本邦で CISO という役割が注目を集めることになったきっかけは、経済産業省と情報処理推進機構（IPA）が「サイバーセキュリティ経営ガイドライン」[4]を発行したことにあるといわれている。同ガイドラインは、「経営戦略上 IT の利活用が不可欠である企業等の経営者を対象に、経営者のリーダーシップの元で、サイバーセキュリティ対策を推進するため」のガイドラインとして定められており、病院情報システムを用いて患者情報を取り扱う医療機関も対象に含まれると考えられる。

同ガイドラインでは、CISO を「経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のこと」と定め、経営者がサイバーセキュリティ対策を実施する上で「重要 10 項目」を指示する相手とされている。

CISO が担うべき役割については、日本ネットワークセキュリティ協会が作成した「CISO ハンドブック」[5]にまとめられている。同ハンドブックの冒頭では、「CISO が経営陣の一員として、セキュリティに取り組むためには、想定される危険性や損失に取り組むだけではなく、ビジネスの視点を持って業務を執行することが求められます」と記載されており、単なる技術者では務まらないと考えられていることが窺われる。

同ハンドブックでは続いて「本書の使い方」として、

- 技術担当から CISO になった人がビジネスを理解するための参考として
- セキュリティ経験の少ない CISO がセキュリティ業務を理解するための参考として

と書かれており、CISO の人物像として、「ビジネスとセキュリティを同時に理解できる人」が想定されていることが判る。CISO が業務執行の責任者である C-Suite の一員であることを考慮すると、「経営も理解しながら情報セキュリティの業務を試行する責任者」であることを考慮すれば、違和感のない人物像であると言える。

3. 医療情報セキュリティを巡る動き

セキュリティインシデント事案の散発的な発生などを受けて、厚生労働省は、令和 4 年度の診療報酬改訂において、400 床以上の保険医療機関については専任の「医療情報システム安全管理責任者」を配置することを、診療録管理体制加算の要件に追加した（図 1）。

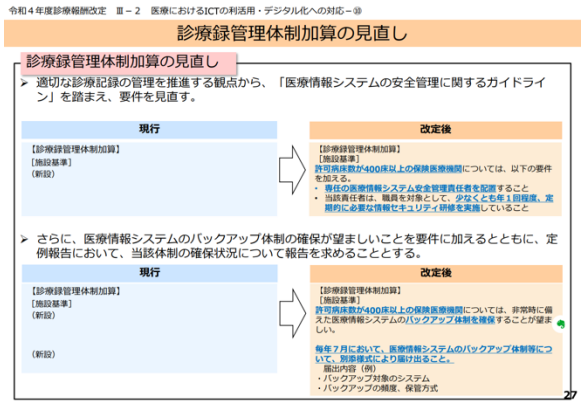

図 1 令和 4 年診療録管理体制加算の見直し [6]

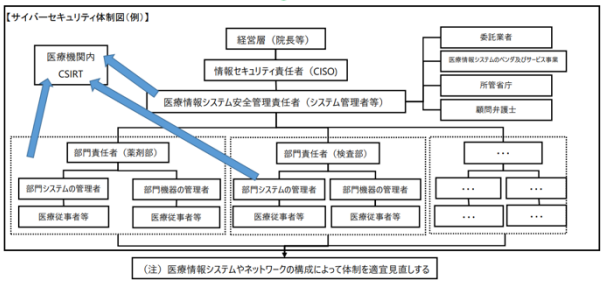

図 2 サイバーセキュリティ体制図 [7)]

「医療情報システム安全管理責任者」の明確な定義は与えられていないが、厚生労働省「医療情報システムの安全管理に関するガイドライン」の付属文書「医療情報システム等の障害発生時の対応フローチャート」[7)]の「サイバーセキュリティ体制図（例）」（図 2）を見ると、情報セキュリティ責任者（CISO）の直下にあって全部門を束ね、委託事業者や所轄官庁等へ連絡をする扇の要として描かれていることから、一般的に CISO 補佐と呼ばれる、技術・戦略立案面で CISO を補佐する役割を負う人物を指すものと考えられる。

但し、同フローチャート等の記載を見ると、「サイバーセキュリティ体制」は「サイバー攻撃等の事案発生時の体制」として描かれており、本来 CISO に求められる「サイバーセキュティ計画の立案」の機能が考慮されていない点で、やや検討が十分なされていない印象を受ける。

同図において、「医療情報システム安全管理責任者」は「システム管理者等」とされ、本邦の医療機関においては、旧来医療情報システム管理に当たってきた人物が想定されていることが判る。

一般的に、CISO 補佐は、自ら所属する業界・組織の経営戦略等に関する知識や経験を得て将来 CISO となるキャリアパスも想定される人物とされている。したがって、「医療情報システム安全管理責任者」のための人材育成は、則ち「医療 CISO」の人材育成そのものでよく、それは、医療情報システム管理に当たる人材育成の延長線上に置かれるべきものであると考えるのが妥当であろうと考えられる。

4. 情報セキュリティ教育の体系

2016 年、「情報処理の促進に関する法律」が改正され、「情報処理安全確保支援士」制度が定められた。情報処理安全確保支援士は「登録セキュリティスペシャリスト（登録セキスペ）」とも呼ばれ、サイバーセキュリティに関する相談に応じ、必要な情報の提供・助言・調査・分析・評価・指導を行うものとされている。

医療 CISO・CISO 補佐が必ずしも登録セキスペたる必要は無いが、少なくとも登録セキスペの助言を理解し、実践できる能力は必要であろう。従って、医療 CISO・CISO 補佐の人材育成においては、登録セキスペ等の認証制度やシラバスを参考にすることが好ましいと考えられる。

情報処理安全確保支援士試験・情報処理のシラバス等については、IPA が公開している [8)]ことから、これらを参考にして検討することが適当であろう。

5. 結語

医療 CISO の人材育成のロードマップは、医療情報システム管理に当たる人材の育成ロードマップの先に、登録セキスペ等の制度を参照しながら、描かれるのが適当であろうと考えられる。

6. 参考文献

1) 黒田知宏．電子カルテの安全な導入と運用―宇陀市立病院事件を事例に．情報処理 2020；61(6)：552-556.
2) 島津忠承．ランサム被害の徳島・半田病院、報告書とベンダーの言い分から見える根深い問題．日経クロステック 2020. [https://xtech.nikkei.com/atcl/nxt/column/18/00001/06927/ (cited 2022-Aug-12)].
3) 徳島県．危機管理連絡会議の開催結果について（令和 4 年 6 月 20 日）．徳島県防災・機器管理情報 安心とくしま 2022. [https://anshin.pref.tokushima.jp/docs/2022062000017/ (cited 2022-Aug-12)].
4) 経済産業省，独立行政法人譲歩処理推進機構．サイバーセキュリティ経営ガイドライン．2022. [https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf (cited 2022-Aug-12)].
5) 高橋正和，荒木粧子，池上美千代，他．CISO ハンドブック-業務執行のための情報セキュリティ実践ガイド．技術評論社，2021.
6) 厚生労働省．令和 4 年診療報酬改訂資料.
7) 厚生労働省．医療情報システムの安全管理に関するガイドライン 医療情報システム等の障害発生時の対応フローチャート．2022. [https://www.mhlw.go.jp/content/10808000/000936168.pdf (cited 2022-08-12)].
8) 情報処理通信機構．情報処理技術者試験・情報処理安全確保支援士試験 試験要項・シラバスなど. [https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.html (cited 2022-08-12)].