公募シンポジウム
# シンポジウム10
# IoTにおけるサイバーセキュリティの現状と対策、および対策としてのISAC
2021年11月21日(日) 09:10 ～ 11:10 F会場 (2号館2階224)

[4-F-1-04] 医療分野におけるサイバーセキュリティ対策と情報共有・相談体制の試行
Cyber security of healthcare and Trial of information sharing system

*田中 彰子[1] （1. 厚生労働省 医政局 研究開発振興課 医療情報技術推進室）
*Akiko Tanaka[1] （1. Ministry of Health, Labor and Welfare）
キーワード：Medical Information Systems, Guideline, Cyber Security

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・機器の高度化等により、サイバーセキュリティ対策を講じることが喫緊の課題となっている。
厚生労働省では、医療機関等における電子的な医療情報の取扱いに関して「医療情報システムの安全管理に関するガイドライン」を定めており、令和3年1月には第5.1版への改定を行った。サイバー攻撃を受けた（疑い含む）場合等には厚生労働省への報告を求め、内閣サイバーセキュリティセンター等と連携し、必要に応じて当該医療機関に対するサイバーセキュリティに係る技術的事項等の助言や、マルウェアや不正アクセスに関する技術的な相談窓口の紹介等を行っている。データヘルス改革では、令和3年6月に2025年度に向けた工程表を策定しており、こうした動きも踏まえ、医療機関等を中心とした医療分野のサイバーセキュリティ対策の強化はより一層重要となっている。
厚生労働省では、令和2年度に医療機関等が自院のサイバーセキュリティ対策の現状を把握することを目的としたサイバーセキュリティ対策チェックリストや、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等を整備し、さらに医療機関等向けの研修・ E-learningも実施した。加えて、実際に医療現場の利用者を募り、情報共有・掲示板ツールを用いた情報共有・相談体制等を試行することで、その意義や効果、課題等についても検討を行った。
今後の医療分野におけるサイバーセキュリティ対策に当たって、医療機関同士の共助の精神の下、医療機関同士が安心して相談や意見交換をし合える場を整備することには一定の有用性がある。厚生労働省としても引き続き医療機関等のサイバーセキュリティ対策の支援、研修・ E-learningの実施、情報共有・相談体制の試行を予定しており、医療分野のサイバーセキュリティに関する共助の取組が進んでいくことに期待したい。

医療分野におけるサイバーセキュリティ対策と情報共有・相談体制の試行

田中 彰子[*1]
*1 厚生労働省

Cyber security of healthcare and Trial of information sharing system

Akiko Tanaka[*1]
*1 Ministry of Health, Labor and Welfare

Abstract

According to the changes in the environment surrounding medical information systems and the development of medical information systems and medical devices, hospitals (and clinics) are required to act immediately when they received cyber attack. Ministry of Health, Labor and Welfare (MHLW) has been providing guidelines for handling electronic medical information for hospitals. When a medical information system fails due to a cyber attack, it is necessary to report to MHLW. MHLW created checklists for security measures for them, and flowcharts when the medical information system fails, and also provided training and e-learning. We also tried the tool for sharing information between them. In order to promote cyber security measures of healthcare in the future, it is useful to provide opportunities for them to discuss and exchange opinions about cyber security. MHLW plans to support these activities and hopes hospitals to be going to promote their mutual support efforts related to cyber security by themselves.

Keywords: Medical Information Systems, Guideline, Cyber Security.

1. 背景

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やインシデントを処理するためのポリシーの策定、セキュリティ体制の整備やトレーニング／教育等、早急に対策を講じることが喫緊の課題となっている。

医療分野のサイバーセキュリティに関しては、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」[1]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、民間は全てを政府に依存するのではなく、政府も民間だけに任せるのではない、緊密な官民連携が求められる」とされ、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た。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。また、平成 30 年 7 月 27 日に閣議決定された「サイバーセキュリティ戦略」[2]では、従来の枠を超えた情報共有・連携体制の構築として、国は ISAC（Information Sharing and Analysis Center/情報共有分析組織）を含む情報共有の取組の推進を支援することとされ、その後の年次計画「サイバーセキュリティ 2020」[3]（令和 2 年 7 月 21 日にサイバーセキュリティ戦略本部決定）においても、厚生労働省は医療分野における ISAC 等のサイバーセキュリティ対策に関する情報共有のあり方について引き続き検討することとされている。

他方、新型コロナウイルス感染症により、オンライン診療・遠隔医療等の活用、医療機器の IoT 化への期待も高まり、こうした中にあって、我が国の医療分野におけるサイバーセキュリティ対策の充実・強化に資する取り組みを図っていくことは急務となっている。

2. 2025 年度に向けたデータヘルス改革の方向性

データヘルス改革では、令和 2 年 7 月に示したデータヘルス集中改革プランに基づき、レセプトに基づく全国で医療情報を確認できる仕組みの拡大（薬剤情報に加えて、医療機関名、手術・透析情報、医学管理等の対象情報の拡大）、電子処方箋の仕組みの構築、自身の保健医療情報を活用できる仕組みの拡大を令和 4 年度までに進めることとしている。令和 3 年 6 月には、上記を含むデータヘルス改革に関する工程表を策定し、2025 年度に向けて、さらなる自身の保健医療情報を閲覧できる仕組みの整備、医療・介護分野での情報利活用の推進、ゲノム医療の推進、審査支払機関改革等の基盤の整備に関する工程を示した。現在、医療分野におけるデータ利活用やオンライン化の加速を目指し、レセプト・処方箋情報をはじめとする保健医療情報をマイナポータル等において閲覧可能とするとともに、本人同意の上で、医療機関等でも閲覧可能とする仕組みの整備を順次進めている。さらに、電子カルテ情報及び交換方式の標準化について、医療現場の有用性を考慮し、技術の発展に対応できるような国際的なデータ連携仕様等に基づいた HL7FHIR の規格を用いることの検討・決定を行い、異なる電子カルテスシステムや PHR とデータ交換可能な仕組みと、医療機関ネットワークへの取り込みを進めつつ、全国的な医療情報ネットワークの基盤のあり方について調査検討を行うこととしている。こうした動きも踏まえ、医療機関等を中心とした医療分野のサイバーセキュリティ対策の強化は、より一層重要な取組となっている。

3. 医療情報システムの安全管理に関するガイドライン（第 5.1 版）改定

厚生労働省では、医療機関等における電子的な医療情報の取扱いに関して、個人情報保護に資する情報システムの運用管理とe-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示した「医療情報システムの安全管理に関するガイドライン」を定めており、令和 3

年 1 月には第 5.1 版への改定を行っている[4]。

本ガイドラインは、医療情報を扱うシステムと、それらシステムに関わる人又は組織を対象とし、電子的な医療情報を扱う際の責任のあり方、情報セキュリティマネジメントシステム(ISMS)の実践、組織的・物理的・技術的・人的安全対策、診療録等を電子化・外部保存する際の安全管理基準等を示しているが、第 5.1 版では、クラウドサービスへの対応や認証・パスワードの対応、外部保存受託事業者の選定基準等対応に加え、サイバー攻撃等の非常時の対応の観点からも、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等について、情報セキュリティ責任者（CISO）等の設置や、緊急対応体制（CSIRT 等）の整備等が強く求められること等の追記・見直しを行っている。

また、本ガイドラインでは、最低限のガイドラインとして、コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発 1029 第 1 号 医政地発 1029 第 3 号 医政研発 1029 第 1 号 平成 30 年 10 月 29 日）に基づき、厚生労働省医政局研究開発振興課医療情報技術推進室への連絡等の必要な対応を行うほか、そのための体制を整備することとしている。厚生労働省は、障害等の判明（発生）日時、障害等が発生したシステムや障害等の内容、対処状況、影響範囲、個人データの漏えいの有無等を把握し、内閣サイバーセキュリティセンター等と連携して事案に対応するほか、必要に応じて当該医療機関に対してサイバーセキュリティに係る技術的事項等についての助言や、マルウェアや不正アクセスに関する技術的な相談窓口の紹介等を行っている。個人データの漏えい等が発生した場合にあっては、当該医療機関等は上記の対応とともに、適用される個人情報保護制度に基づいて速やかに漏えい等報告を行うなど、適切に対応を行うことも求められる。

4. 医療機関等を中心とした医療分野のサイバーセキュリティ対策の強化と情報共有・相談体制の試行

厚生労働省では、「令和2年度 医療分野におけるサイバーセキュリティ対策調査事業」において、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、医療機関等が自院のサイバーセキュリティ対策の現状を把握することを目的とした医療機関の経営層向け、システム管理者・セキュリティ管理者向け、医療従事者・システム利用者向けのサイバーセキュリティ対策チェックリストを整理した。また、医療機関等で医療情報システム等の障害が発生した場合に迅速に対応するための体制整備に資するよう、システム障害発生時の対応フローチャート等も整備した。さらに、サイバーセキュリティ対策に関する理解を深めるため、医療機関等の経営者、システム管理者・セキュリティ管理者、医療従事者・システム利用者向けの研修・E-learning を実施し、本研修教材を各医療機関内での研修にもご活用頂けるよう、厚生労働省ホームページ「医療分野のサイバーセキュリティ対策について」（https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html）上にも掲載している。

加えて、実際に医療現場の利用者を募り、情報共有・掲示板ツールを用いた情報共有・相談体制等を試行することで、医療機関等の当事者間でサイバーセキュリティ対策に関する情報共有を行う意義や効果、課題等についても検討を行った。その結果、医療分野におけるサイバーセキュリティに関する情報のニーズとしては、「各種ガイドラインの解釈や運用実態」、「医療分野におけるサイバーセキュリティに関するニュースの背景、分析等」、「医療従事者に対するセキュリティ教育の工夫や課題」等が高く、一方、情報収集における課題については「収集およびその整理にかける要員・時間を確保できない」、「情報源や情報量が多く、自組織に必要な情報の選別の基準がない」等が高く、さらに「同じ地域や同規模の医療機関のシステム担当者」や「公的機関（厚生労働省、NISC 等）」、「セキュリティの専門家」等から情報・助言を得たいとの声が多くなっており、コミュニティや情報収集・分析等を支援する仕組みの必要性が示唆された。自らが他の参加者に情報を提供するとした場合、「提供する情報の正確性などが担保できず、情報提供を躊躇してしまうのではないか」、「自組織に関する機密情報のため提供できないと考えて一般的な情報しか提供できないのではないか」といった課題や懸念も伺えた。

今後の医療分野におけるサイバーセキュリティ対策に当たって、医療機関同士の共助の精神の下、医療機関同士が安心して相談や意見交換をし合える場を整備することには一定の有用性があると考える。厚生労働省としても上記の点も考慮しつつ、引き続き、医療機関等のサイバーセキュリティ対策の支援、研修・E-learning の実施、情報共有・相談体制の試行を進めることを予定しており、医療分野のサイバーセキュリティに関する共助の取り組みが進んでいくことに期待したい。

参考文献

1) サイバーセキュリティ戦略（平成 27 年 9 月 4 日閣議決定）, 2015. [https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf (cited 2020-Aug-25)].
2) サイバーセキュリティ戦略（平成 30 年 7 月 27 日閣議決定）, 2018. [https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf (cited 2020-Aug-25)].
3) サイバーセキュリティ戦略本部. サイバーセキュリティ 2020. 内閣サイバーセキュリティセンター, 2020. [https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf (cited 2020-Aug-25)].
4) 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 第 5.1 版. 厚生労働省医政局, 2021. [https://www.mhlw.go.jp/content/10808000/000730541.pdf (cited 2021-Aug-20)].