共同企画 | 第40回医療情報学連合大会（第21回日本医療情報学会学術大会） | 共同企画
共同企画3
急速に広がるオンライン診療・遠隔医療におけるサイバーセキュリティを考える
2020年11月19日(木) 14:00 ～ 16:20 B会場 (コングレスセンター3階・31会議室)

[2-B-2-06] 医療分野の情報化とサイバーセキュリティ対策の実施・強化に向けた方向性

*前田 彰久[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）
*Akihisa Maeda[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）

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 第５版」（平成29年５月）を定め、情報セキュリティマネジメントシステム(ISMS)の実践や、組織的・物理的・技術的・人的安全対策等を示している。また、サイバー攻撃等で医療情報システムに障害が発生した場合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、新型コロナウイルス感染症を踏まえた新たな日常にも対応したデータヘルス集中改革プランを進めることとしている。こうした動きを踏まえつつ、厚生労働省として、医療機関等におけるセキュリティ対策のベストプラクティスやチェックリストの作成、医療機関や医療従事者向けの研修・ E-learningの実施、医療現場の利用者による情報共有・掲示板ツールを用いた情報共有や相談体制の試行等を行うことも予定している。
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は、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が必要不可欠である。サイバー攻撃時に専門家から助言や支援が得られること、医療セプターと連携した情報共有や継続的な研修・教育・演習が行われること、インシデントが公開された際には医療機関が行う具体的な対策等にも言及した医療機関目線のペーパー・手順書等が作成・共有されること等を厚生労働省としても支援し、医療分野の共助の取組に期待したい。

医療分野の情報化とサイバーセキュリティ対策の実施・強化に向けた方向性

前田 彰久[*1]、井髙 貴之[*1]
*1 厚生労働省

Informatization of Healthcare in Japan, and Cyber Security

Akihisa Maeda[*1] , Takayuki Idaka[*1]
*1 Ministry of Health, Labor and Welfare

Abstract

With the changes in the environment surrounding medical information systems and the sophistication of medical information systems and medical devices, medical institutions are required to take immediate cyber security measures. Ministry of Health, Labor and Welfare (MHLW) has provided guidelines for handling electronic medical information at medical institutions. When a medical information system fails due to a cyber attack, it is necessary to report to MHLW. As information technology advances of healthcare, MHLW plans to prepare best practices and checklists for security measures at medical institutions, as well as conduct training and e-learning at medical institutions. It also plans to experiment with tools for sharing information between medical institutions. In order to advance cyber security measures of healthcare in the future, it is essential to provide opportunities for medical institutions to discuss and exchange opinions. MHLW will support these activities, and I hope that medical institutions will promote mutual assistance efforts related to cyber security.

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。また、平成 30 年 7 月 27 日に閣議決定された現行の「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、医療現場の TV 会議システム等の活用、医療機器の IoT 化等が急速に拡がっており、また、国外では新型コロナウイルス感染症に乗じたサイバー攻撃により医療機関で IT インフラが停止した事例などが確認されている。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. 医療情報システムの安全管理に関するガイドラインと医療情報システムにおける障害等発生時の対応

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 第5版」[4]（平成 29 年 5 月）を定めている。

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。

また、サイバー攻撃等で医療情報システムに障害等が発生した場合には、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報告を求めている。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（情報処理推進機構情報セキュリティ安心相談窓口）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。

重要インフラの情報セキュリティ対策については、これに加え、内閣サイバーセキュリティセンターの総括の下、各分野の所管省庁と重要インフラ事業者等とセプターが連携しながら対応を行っている。セプターとは、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、関係者間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資することを目指すものである。平成 30 年3月より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、医療関係者へのサイバーセキュリティに関する情報提供や演習参加等の活動を実施している。

3. 加速する医療分野の情報化

データヘルス改革では、新型コロナウイルス感染症を踏まえ、新たな日常にも対応するデジタル化を通じた強靭な社会保障を構築するため、オンライン資格確認等システムやマイナンバー制度等の既存インフラを最大限活用しつつ、データヘルス集中改革プランを進めることとしている。

具体的には、患者や全国の医療機関等で医療情報を確認できる仕組みについて対象となる情報（薬剤情報に加えて、手術・移植や透析等の情報）を拡大すること、重複投薬の回避にも資する電子処方箋の仕組みを構築すること、PCやスマートフォン等を通じて国民・患者が自身の保健医療情報を閲覧・活用できる仕組みについて対象となる健診等を拡大することについて、この2年間の工程の中で実現することを目指している。

こうした加速する医療分野の情報化の動きも踏まえ、厚生労働省では、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、医療機関等におけるセキュリティ対策のベストプラクティスの作成や、IT の専門知識がなくとも自組織のセキュリティの現状確認ができるチェックリストの整備を進めるとともに、これらの活用方法も含めたセキュリティ対策の基礎を学ぶための医療機関等の経営者、システム/セキュリティ管理者、医療従事者向けの研修・E-learningを実施することを予定している。また、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・相談体制等も試行することで、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仕組みの意義や効果、課題等について検討することを予定している。

4. 医療分野のサイバーセキュリティ対策に向けた今後の方向性

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は、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が必要不可欠である。例えば、インシデント対応、情報システム管理といった現場の課題を取り上げたワークショップや活動報告会を立ち上げ、インシデント対応でいえば、事例や対応策・手順書等を参加者間で共有して好事例を取り上げ参考にすること、あるいは最低限必要な項目を抜き出してホワイトペーパーを作成・発信すること等は、現場の意識や知識・技術の向上を図るうえでも非常に有意義であろう。サイバー攻撃時に専門家から助言や支援が得られること、医療セプターと連携した情報共有や継続的な研修・教育・演習が行われること、インシデントが公開された際には医療機関が行う具体的な対策等にも言及した医療機関目線のペーパー・手順書等が作成・共有されること等を厚生労働省としても支援し、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 版. 厚生労働省政策統括官付情報化担当参事官室, 2017. [https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf (cited 2020-Aug-25)].