令和４年度全国薬務関係主管課長会議資料

説明資料

厚生労働省医政局

特定医薬品開発支援・医療情報担当参事官室

医療機関におけるサイバーセキュリティ対策について

現状等・今後の取組等

○　令和４年９月に予防対応・初動対応・復旧対応からなる「医療機関のサイバーセキュリティ対策の更なる強化策」をとりまとめた。予防対応の主な項目としては、

１，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、医療従事者の階層（医療従事者・経営層・システムセキュリティ管理者）に応じた研修

２，脆弱性が指摘されている機器・ソフトウェアの確実なアップデートを医療機関への立入検査の実施等による確認

３，不正侵入検知・防止システム（IDS・IPS）等の検知機能の医療機関への設置・活用の推進

医療従事者へのサイバーセキュリティ対策に関する研修の開始に伴い、医療機関向けセキュリティ教育支援ポータルサイト(MIST：Medical Information Security Training)を開設した。本ポータルサイトを通じ、各種研修の申し込みや、自組織内のサイバーセキュリティ教育に活用できるコンテンツ集の掲載など医療機関への継続的な教育支援を行っている。

次に初動対応の項目として、

１，サイバーセキュリティインシデントが発生した医療機関への初動対応支援
２，サイバーインシデント発生時に厚生労働省等行政機関等への報告の徹底を挙げた。

最後に復旧対応の項目として、

１，バックアップの具体的な作成が明記された「医療情報システムの安全管理に関するガイドライン」に基づいたバックアップの作成・管理の徹底
２，「令和４年医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、サイバーセキュリティインシデントが発生した際の対応手順の調査を行い、適切な対応フローの整理、また整理した対応フローをもとにサイバーセキュリティインシデントに備えたBCPの提案を行うことを挙げている。

○　10 月 31 日に発生した大阪急性期・総合医療センター（以下 OGMC）のサイバー攻撃事案に対しては、強化策の一つである初動対応支援として速やかに専門家を派遣し、感染原因の特定や対応の指示等を行った。

○　さらに、11 月 10 日には、特に今回の OGMC の事案を踏まえ、全国の医療機関に対して、

１、サプライチェーンリスク全体の確認

２、リスク低減のための措置

３、インシデントの早期検知

４、インシデント発生時の適切な対処・回復

５、金銭の支払いに対する対応

に関して、サイバーセキュリティ対策が適切に講じられているかについて注意喚起を行った。

○　また、昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であったため、平時の予防対応として、脆弱性が指摘されている機器の確実なアップデートの実施が必要との意見がワーキンググループであった。そのため、医療法第 25 条第１項の規定に基づく立入検査にかかる省令改正の施行を行い、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○　最後に、G-MIS（G-MIS、医療機関等情報システムは新型コロナウイルス感染症対策として、全国の医療機関の医療提供体制関連情報を迅速に収集するために、令和２年５月に構築・運用されている）による医療機関に対するサイバーセキュリティ対策の実態調査を令和５年１月 27 日より開始している。

都道府県へのお願い

○　各都道府県におかれても、医療機関等でサイバー攻撃等のサイバーセキュリティインシデントが発生した際の厚生労働省への迅速な報告をお願いする。

担当者：医政局　特定医薬品開発支援・医療情報担当参事官室
岡本補佐(内線：4568)