資料２－２

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第12回健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

２０２２（令和４）年９月５日

医療機関におけるサイバーセキュリティ対策の更なる強化策

－　今後の医療機関におけるサイバーセキュリティ対策の基本方針　－

医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

医療機関におけるサイバーセキュリティ対策の更なる強化策
－　今後の医療機関におけるサイバーセキュリティ対策の基本方針　－

（1）短期的な医療機関におけるサイバーセキュリティ対策

1．平時の予防対応

①医療機関向けサイバーセキュリティ対策研修の充実　　②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

③医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築　　④検知機能の強化

⑤G-MIS用いた医療機関への調査実施

2．インシデント発生後の初動対応

①インシデント発生時の駆けつけ機能の確保　　②行政機関等への報告の徹底

3．日常診療を取り戻すための復旧対応

①バックアップの作成・管理の徹底　　②緊急対応手順の作成と訓練の実施

（2）中・長期的な医療機関におけるサイバーセキュリティ対策

1．バックアップデータの暗号化・秘匿化

2．保健医療分野におけるSOCの構築

（１）短期的な医療機関におけるサイバーセキュリティ対策

【取組事項】

予防対応

① 医療機関向けサイバーセキュリティ対策研修の充実

– 「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」を８月19日より公示開始。本事業により、**医療従事者や経営層等へ階層別のサイバーセキュリティ対策に関する研修の実施**や、本事業において作成される**ポータルサイトを通じた研修資材の提供**により、医療従事者や経営層等のサイバーセキュリティ対策の意識の涵養を図る。

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の実施

– 医療法第25条第１項の規定に基づく**立入検査の実施により確認**を行う。また、例年発出している「医療法第25条第１項の規定に基づく立入検査の実施について」（医政局長通知）において、令和４年度は**サイバーセキュリティ対策の強化に関する事項について記載**した。**令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正**を行う。

– NISCより情報提供のあった脆弱性情報について、医療セプターを通じた情報提供を引き続き行う。

③ 医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築

– 他分野のISAC関係者の協力を得つつ、医療関係者数名のコアメンバーによる**検討グループを年内に立ち上げる。**

④ 検知機能の強化

– **不正侵入検知・防止システム（IPS／IDS）の設置・活用を進める**よう、医療情報システムの安全管理に関するガイドライン**改定の検討**を行う。

⑤ G-MISを用いた医療機関への定期調査の実施

– 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４年度中に実施する。

【質問項目（例示）】

・医療法に基づく立入検査の留意事項を認識し、必要な措置を講じているか。

・（許可病床数が400床以上の保険医療機関に対して）診療録管理体制加算の見直しを受けて、専任の医療情報システム安全管理責任者を配置しているか。

初動対応

① インシデント発生時の駆けつけ機能の確保

– 200床**以下**の医療機関に対し、**サイバーセキュリティお助け隊の活用を促進するための周知・広報**を行う

– 200床**以上**の医療機関に対し、「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医療機関の初動対応支援**を行う。

② 行政機関等への報告の徹底

– **医療情報セキュリティ研修およびG-MIS調査を通じ**、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**厚生労働省への報告の徹底**や、個人情報保護法改正に伴う**個人情報保護委員会への報告義務化の周知**を図る。

– 厚生労働省より、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て医療機関より報告のあったサイバーインシデント事案について、攻撃先が同定されない程度に報告内容を適時情報提供し、攻撃手法や脅威について分析を行い、全国の医療機関へ情報発信・注意喚起を行う。

復旧対応

① バックアップの作成・管理の徹底

– 医療情報セキュリティ研修およびG-MIS調査を通じ、**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（５．２版）の周知を行う。

– 令和３年６月28日発出「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」の記載事項に留意し、データ・システムのバックアップを行う。

– 令和4年度診療報酬改定における診療録管理体制加算に係る報告書（７月報告）により、**バックアップ保管に係る体制等の確認**を行う。

② 緊急対応手順の作成と訓練の実施

– 「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**を行う。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。

（２）中・長期的な医療機関におけるサイバーセキュリティ対策

【今後の検討事項】

バックアップデータの暗号化・秘匿化

・**最新技術を利用したバックアップの検討**
－医療情報のよりセキュアなバックアップを行うため、**バックアップデータの暗号化・秘匿化**に向けた検討を進める。

保健医療分野におけるSOC（Security Operation Center）の構築の検討

※ SOCとは、セキュリティ・サービス及びセキュリティ監視を提供するセンターのこと。（引用元：サイバーセキュリティ2022）

・ **24時間365日体制**で、プロキシサーバーを経由した医療機関に対する不審な通信やウェブサイトの稼働状況を監視することで、**サイバー攻撃の早期発見が可能**となる。

・保健医療分野を横断的に監視することで、医療機関に対して**多く使われる攻撃手法**・**昨今のサイバー攻撃の傾向**を**観測**することができ、その観測データを医療機関内のCSIRTや情報共有体制（ISAC）へ提供することにより、**分析および対策に資することが可能**となる。ただし、セキュリティ対策にかける費用と損害のバランスには留意が必要。

・厚生労働省において、令和４年度事業として「保険医療機関等へのセキュリティ監視環境検証事業」を実施予定。医療機関へ情報資産の実地調査等を行い、**セキュリティ監視システムの全体構成の検討**や**保健医療分野において望ましいSOC構築に向けた検討**を行っていく。

その他

・「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の対象事業者と医療機関等の合意形成の項目及び、HELICS協議会において医療情報化指針として採択した（令和4年8月）「製造業者/サービス事業者による医療情報セキュリティ開示書」（MDS/SDS）の遵守を業界団体及び医療機関に徹底する。