資料１

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

第11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
令和４年５月27日

医療機関におけるサイバーセキュリティ対策の徹底について

Ministry of Health, Labour and Welfare of Japan

医療機関のサイバーセキュリティ対策の徹底

（現状・課題）

医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきたところ。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。

（対応策）

また、「重要インフラの情報セキュリティ対策に係る第４次行動計画」において、①安全基準等の整備・浸透、②情報共有体制の強化、③障害対応体制の強化、④リスクマネジメント及び対処態勢の整備、⑤防護基盤の強化が挙げられており、短期的な対策として、長期に診療が停止することのないよう以下について対策の徹底を図る。

１．平時の予防対応

①医療従事者への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医療業界独自の情報共有機能を構築するためのISACの立ち上げ

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

１．平時の予防対応

平時の医療機関における対応として、人材育成、情報共有体制の強化、脆弱性機器への対応の徹底をはかる必要がある。

対応	具体的な対応方針や主体等
①医療従事者へのセキュリティ対策研修の充実	・令和4年度診療報酬改定における診療録管理体制加算の見直し ・医療機関の管理者および医療従事者向け研修等を実施するための院内研修用資材を提供し、病院内の研修で活用できるようにする
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（セプターを通じた情報提供）	・医療法に基づく立入検査で確認
③医療分野におけるISAC設立に向けた検討	・令和2・3年度の事業結果を踏まえ、コアメンバーによる設立準備を開始

①医療従事者へのセキュリティ対策研修の充実

適切な診療記録の管理を推進する観点から、「医療情報システムの安全管理に関するガイドライン」を踏まえ、要件を見直し、400床以上の保険医療機関におけるセキュリティ対策を徹底する。

【診療録管理体制加算の見直し】

現行	改定後
【診療録管理体制加算】 [施設基準] (新設)	【診療録管理体制加算】 [施設基準] **許可病床数が400床以上の保険医療機関**については、以下の要件を加える。 • **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 • 当該責任者は、職員を対象として、**少なくとも年１回程度、定期的に必要な情報セキュリティ研修を実施**していること

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

最近のランサム攻撃等では、セキュリティアップデート未適用VPNの脆弱性をついた認証情報の窃取が原因で有ることが多く、ネット接続に係る資産管理の重要性を認識し、VPNの重要性の再認識と脆弱性を含めた管理の厳格化が必要である。

課　題	今後の対応方針
脆弱性が指摘されているVPN装置のアップデートを行っている病院は約６割	• 令和４年度は医療法に基づく立入検査の留意事項に、安全管理ガイドライン5.2版に関する記載を新たに追加。 • 令和４年度中に医療機関の管理者が遵守するべき事項に位置づけることを検討

③医療分野におけるISAC設立に向けた検討

情報共有体制の強化については、令和２・３年度事業によって、医療分野におけるISACの設立に向けた方策が得られたことから、今年度はコアメンバーによる組織の立ち上げを検討する。

（2019年度医療機関におけるサイバーセキュリティ対策調査事業より抜粋）

ISACの概要

ISAC(Information Sharing and Analysis Center)について

- ISACとは、**主にサイバーセキュリティに関連する脅威の情報について、各業界(金融、通信、電力、医療等)内で共有・分析するための組織**である。

- ISACの組織形態について確立した定義はないが、主に以下のような機能を担うものとされている。
  - 各業界において重要な警戒情報を収集・分析し、インシデントに関するレポートを会員に対して提供する
  - インシデント、脅威、及び脆弱性が業界に与える影響について、関係政府機関への説明を行う
  - 重要インフラ防護の目的において、あらゆる脅威情報を会員間で共有するための信頼出来るシステムを提供する
  - 意図的/非意図的に関らず政府や他ISACに被害をもたらす、又はその可能性がある事象が発生した場合、専門的な支援や情報共有を行う

- 現状、以下のようなISACが運営されている。
  - 医療：H-ISAC(米国)
  - 金融：金融ISAC(日本)、FS-ISAC(米国)
  - 通信：ICT-ISAC(日本)、IT-ISAC(米国)
  - 電力：電力ISAC(日本)、E-ISAC(米国)

２．インシデント発生後の初動対応

診療体制の復旧には、インシデント発生時の駆けつけ対応の強化が必要であり、病床規模毎に利用できるサービスなどについて明らかにすると共に、適切に各医療機関に周知する必要がある。

具体例	対応方針や主体等
④インシデント発生時の駆けつけ対応の強化	【医療機関の規模別の対応】 ・200床以下の病院及び診療所等に対し、サイバーセキュリティお助け隊の活用を促進（議題３） ・200床以上の病院に対しては、 駆けつけ対応の強化及び医療機関における対応強化を目的に、以下の内容を含む調査事業を実施 ・実際にインシデントが発生したときの現地駆けつけ事例を調査し、医療機関におけるサイバー対策の強化が必要な点などを明らかにする
⑤行政機関等への報告の徹底	・安全管理ガイドラインに基づいた厚労省への報告を徹底し、その報告内容を攻撃先が同定されない範囲で医療機関の対策に活用できる方策を検討する。 ・個人情報保護法改正に伴う報告の義務化の周知（議題２）

３．日常診療を取り戻すための復旧対応

長期に診療が停止しない方策として、まずは短期的にバックアップの実施について徹底を図る必要がある。今後長期的には、ランサムウエア攻撃への対策としては、バックアップの暗号化、秘匿化も必要。

具体例	対応方針や主体等
①バックアップの実施の徹底	・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版にバックアップの具体的な作成についてすでに明記されており（6.10 Ｂ項）、ガイドラインの周知を行う。 ・医療法に基づく立入検査の留意事項に、安全管理ガイドライン5.2版に関する記載を新たに追加。

【診療録管理体制加算の見直し】

現行	改定後
【診療録管理体制加算】 ［施設基準］ （新設）	【診療録管理体制加算】 ［施設基準］ **許可病床数が400床以上の保険医療機関**については、非常時に備えた医療情報システムの**バックアップ体制を確保**することが望ましい。 **毎年7月において、医療情報システムのバックアップ体制等について、別添様式により届け出ること。** 届出内容（例） ・バックアップ対象のシステム ・バックアップの頻度、保管方式

３．日常診療を取り戻すための復旧対応

医療サービスを提供し続けるためのBCPの一環として、災害及びサイバー攻撃等を“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めておくことが、医療情報システムの安全管理に関するガイドラインに明記されており、この徹底を図る。

具体例	対応方針や主体等
②緊急対応手順の作成と訓練の実施	・医療情報システムの安全管理に関するガイドラインにすでに明記されており（6.10 C項）、ガイドラインの周知を行う。 ・医療法に基づく立入検査の留意事項に、安全管理ガイドライン5.2版に関する記載を新たに追加。

令和４年度の医療法第25条第１項の規定に基づく立入検査の実施について（抜粋）

カ．医療機関におけるサイバー攻撃への対策について、医療機関の情報システムがランサムウェアに感染すると、保有する情報資産（データ等）が暗号化され、電子カルテシステムが利用できずに診療に支障が生じたり、患者の個人情報が窃取されたりする等の甚大な被害をもたらす可能性があることから、医療機関においてサイバーセキュリティ対策の強化を図るため、以下に掲げる事項について確認を行う。

① PC やVPN 機器等の脆弱性情報を収集し、速やかに対策を行える体制が確保されていること

② 診療継続のために直ちに必要な情報をあらかじめ十分に検討し、データやシステムのバックアップを確実に行っていること

③ 不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、BCPとして定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認すること

④ 医療情報システムの保守会社等への連絡体制（サイバー攻撃を受けた疑いがある場合）や厚生労働省への連絡体制（当該サイバー攻撃により医療情報システムに障害が発生し、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）が確保されていること

また、医療機関において情報セキュリティインシデントが発生した場合の立入検査等については、厚生労働省に報告を行う。

なお、医療機関における情報セキュリティインシデントに係る立入検査の実施にあたっては、サイバーセキュリティに係る技術的事項等について厚生労働省より助言を行うことが可能である。

【参考】
- 「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」（平成30年10月29日付け医政総発第1029第1号・医政地発第1029第3号・医政研発第1029第1号厚生労働省医政局総務課長・地域医療計画課長・研究開発振興課長通知）
- 「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）」（令和３年６月28日付け厚生労働省政策統括官付サイバーセキュリティ担当参事官室、厚生労働省医政局研究開発振興課医療情報技術推進室、厚生労働省医薬・生活衛生局医療機器審査管理課 、厚生労働省医薬・生活衛生局医薬安全対策課事務連絡）
- 「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（再注意喚起）」（令和３年11月26日付け厚生労働省医政局研究開発振興課医療情報技術推進室事務連絡）
- 「医療情報システムの安全管理に関するガイドライン　第5.2版」（令和４年３月31日付け医政発第0331第50号厚生労働省医政局長通知別添）

※立入検査の実施に当たっての留意事項を示したもの