令和４年度全国薬務関係主管課長会議資料

（参 考 資 料 編）

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

ポイント（医療機関におけるサイバーセキュリティ対策について）

- 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。
- 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、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、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を令和５年４月１日施行予定である。

（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

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ＷＧ（令和４年９月５日）
資料２－２

【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（IDS・IPS）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**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。

大阪府立病院機構 大阪急性期・総合医療センターのランサムウェア感染事案に関して

第13回健康・医療・介護情報利活用検討会医療等情報利活用WG（令和４年12月15日）
資料3

事案概要

2022年10月31日(月) 早朝、地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター（以下、大阪急性期・総合医療センター）において、ランサムウェアを用いたサイバー攻撃によりファイルが暗号化され、電子カルテが使用不能となる事案が発生した。厚生労働省から派遣した初動対応支援チーム（一般社団法人ソフトウェア協会）の調査によると、感染経路は、院外の調理を委託していた給食事業者のシステムを経由したものである可能性が高いことが判った。

新規外来患者の受入は引き続き停止しているが、緊急度の高い処置、手術は大阪急性期・総合医療センターにおいて継続して対応している。緊急度の低い患者については、一度自宅退院、周辺病院への転院を進めたので、患者の生命等への影響はなかった。また、個人情報の漏洩も確認されていない。　（12月12日時点）

(参考)地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
病床数：865床（一般病床831床、精神病床34床）
病院機能：基幹災害拠点病院、高度救命救急センター、地域周産期母子医療センター、小児地域医療センター、地域医療支援病院、
地域がん診療連携拠点病院　他
延べ入院患者数：22.3万人（646人/日）
延べ外来患者数：29.5万人（1,268人/日）

経過

10月31日(月)：インシデント発生。大阪急性期・総合医療センターからの初動対応支援の要請を受け、厚生労働省より初動対応支援チームを派遣
同日夜、記者会見により当該事案を公表。
11月４日(金)：予定手術を一部再開。
11月７日(月)：発生後一週間経過。当該事案の現状と今後の復旧計画について記者会見を実施。感染経路は、給食事業者に設置されたVPN装置を経由した可能性が高いことを公表。
11月10日(木)：電子カルテの一部が仮設環境により参照可能となり、三次救急患者の受け入れと小児救急診療の一部を再開。
11月17日(木)：仮設環境による参照が救急外来において可能となり、一般救急患者の受け入れが再開。
12月12日(月)：電子カルテ再構築を完了させ本環境で順次稼働開始。各種オーダも順次再開予定。
来年１月：システム全面復旧予定

厚生労働省の対応

１．医療機関から要請を受けて、厚生労働省から専門家を派遣し、感染原因の特定や対応の指示等といった初動対応の支援を行った。

２．11月10日に全国の医療機関に対して、サイバーセキュリティ対策の強化にかかる注意喚起を行った。

令和４年11月10日事務連絡
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(注意喚起）(抜粋)

1 サプライチェーンリスク全体の確認

関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

2 リスク低減のための措置

・パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。
・IoT 機器を含む情報資産の保有状況を把握する。
・VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
・悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。
・VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。
・メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

3 インシデントの早期検知

・サーバ等における各種ログを確認する。（例：大量のログイン失敗の形跡の有無）
・通信の監視・分析やアクセスコントロールを再点検する。（例：不審なサイトへのアクセスの有無）

4 インシデント発生時の適切な対処・回復

・サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。
・データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。
・インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。
・インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

5 金銭の支払いに対する対応

サイバー攻撃をしてきた者の要求に応じて金銭を支払うことは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。
・金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。
・一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

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施行に関して

経緯・概要

○　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。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。（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（令和４年５月27日））

○　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。（令和５年４月１日施行予定）

◎医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条　（略）

２　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じなければならない。

※　下線部を新設する。

（参照条文）

◎医療法（昭和二十三年法律第二百五号）

第十七条　第六条の十から第六条の十二まで及び第十三条から前条までに定めるもののほか、病院、診療所又は助産所の管理者が、その構造設備、医薬品その他の物品の管理並びに患者、妊婦、産婦及びじよく婦の入院又は入所につき遵守すべき事項については、厚生労働省令で定める。