参考資料１

情報セキュリティに関する現況及び今後の対応方針について

１　急性期・総合医療センターにおける対応

⑴ 概要

①　令和４年 10 月 31 日に大阪急性期・総合医療センター（以下「急性期センター」という。）においてサイバー攻撃による大規模システム障害が発生し、長期間、診療制限をせざるを得ない状況となったが、同年 12 月 12 日に電子カルテサーバーを再稼動し、令和５年１月 11 日に診療機能が完全復旧した。

※ サイバー攻撃の侵入経路は、以下のとおりと推定される。

ア　急性期センターが委託契約していた給食事業者内にある外部接続機器の脆弱性を悪用して給食事業者内のシステムに侵入

イ　給食事業者内のシステムから急性期センターにある給食サーバー認証情報を窃取し、急性期センター内の給食サーバーへ侵入。

ウ　給食サーバーから急性期センター内の別のサーバー認証情報を窃取し、電子カルテ等のサーバーに侵入。

②　急性期センターにおいて、令和５年１月２５日に外部有識者による事故調査委員会を設置し、同年３月に原因究明・再発防止策の報告あり。

⑵ 現在までの主な取り組み等

事故調査委員会報告書において指摘された情報セキュリティインシデントの発生要因と再発防止策に対して、サイバーセキュリティの専門家に指導を受けながら、以下のとおり取り組んでいる。

①技術的発生要因

ア　外部接続（リモートメンテナンス）の管理

・一旦すべて遮断

・専門家監修のもと外部接続基準を策定し、新たな外部接続管理体制を構築

イ　内部セキュリティ

・指摘された脆弱事項については、基幹システム復旧時にすべて改善

②組織的発生要因

ア　ＩＴガバナンスの確立

・医療機器購入の際のセキュリティチェックリストを策定

・ＩＴ資産管理システムの運用を開始

イ　契約に関する諸問題

・入札時に示すセキュリティ特記仕様書の内容を専門家監修のもとで策定中

⑶ 今後の対応について

厚生労働省の令和５年度医療情報セキュリティ調査等事業を受託した一般社団法人ソフトウェア協会と共同で、ＩＴガバナンス確立に向けたフレームワークやテンプレート等の検討を行い、経営的な視点から投資や運営、リスク管理などについての方針を策定し、組織的なＩＴ管理体制の構築に取り組む。

２　４センター及び本部事務局における対応

⑴ 現在までの主な取り組み等

急性期センター事案では、外部からの侵入によりランサムウェアに感染したため、４センター及び本部事務局において、外部セキュリティの観点からの対策を優先的に実施。

主な取り組みは下記のとおり。

①　外部接続する業者への個別ヒアリングの実施
②　外部接続時に使用する機器（ファイアウォール）の脆弱性点検やバージョンアップの実施
③　電子カルテ等の端末でＵＳＢ機器が使用できないよう制限

⑵ サイバーセキュリティ安全性確認調査業務の結果について

４センター及び本部事務局における情報セキュリティインシデント発生防止に取り組むため、サイバーセキュリティの安全性に関する委託調査を実施（～令和５年５月）。

その結果、現時点でランサムウェアの感染は認められないものの、引き続き対策が必要との調査結果が示された。

示された主な対策は次のとおり。

①センター内のシステムやネットワークの把握
②情報資産（医療機器や端末等）の棚卸、管理の徹底
③外部セキュリティのさらなる強化

⑶ 今後の対応方針

⑵で示された事項をはじめ、令和５年５月に改正された「医療情報システムの安全管理に関するガイドライン」、医療法に基づく令和５年度の立入検査で使用される「医療機関におけるサイバーセキュリティ対策チェックリスト」への対応等、セキュリティ強化を機構全体の優先課題として取り組むこととし、対応項目ごとに工程表を作成の上で、今年度内の完了を目指す。

また、セキュリティポリシー及びＢＣＰなど、機構全体での統一化が必要なものについては、現在、先行して急性期センターにおいて作成中の内容をベースに、今後、機構内での横展開を図っていく。