医療 ISAC Security Lecture 2022

#010
医療機関へのサプライチェーン攻撃で留意すべきポイント

講師：江原悠介
日時：2022 年 12 月 21 日（水）17:00～18:00　Google Meet によるライブ配信

講師略歴
医療 ISAC 理事

ヘルスケアや金融を中心とした社会インフラ型のリスクアシュアランスに係る様々な業務に従事。医療機関や情報処理事業者に対する 3 省ガイドラインに基づく態勢整備/セキュリティ監査、患者個人情報等の二次利用に際したプライバシーガバナンスの整備支援等、官公庁ガイドラインや医療 DX に伴うガバナンス設計に対する業務知識・経験を有する。

- 特定非営利活動法人 デジタル・フォレンジック研究会 理事（医療分科会 主査）
- 経済産業省・総務省「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」検討委員会　委員
- 経済産業省　情報セキュリティサービス審査基準 技術検討会 委員
- 経済産業省　DX システムガバナンスに係る検討会 委員
- 徳洲会インフォメーションシステム（株）　セキュリティアドバイザー
- 情報処理推進機構　社会実装推進委員会　民法改正 WG/セキュリティ検討 PT　委員
- 内閣府　SIP 第 2 期「AI（人工知能）ホスピタルによる高度診断・治療システム」 採択課題 /「AI ホスピタルの研究開発に係る知財管理等、システムの一般普及のための技術標準化・Open/Close 戦略、官民学連携のためのマッチング等に関する対応」プロジェクト 研究責任者経験者

講演要旨

10 月末に大阪急性期・総合医療センターが、外部事業者が提供する外部サービスの提供網を介してランサムウェアに感染し、外来患者の受入や手術の停止等、診療業務の継続性が深刻に損なわれる事態が発生し、完全復旧に向けた取り組みが現在も行われていることは様々なメディアに取り上げられているとおりである。

病院側は厚生労働省の通知・連絡に従い、院内システムへのリモートメンテナンスに用いる VPN 機器の脆弱性の対応を行っていた。
それにもかかわらず、外部事業者のシステム環境に設置されていた VPN 機器の脆弱性が十分でなく、そこが起点となり、安心なはずの拠点間の接続を介して、感染が病院にまで拡大したと報道されている。

院内で利用している外部サービス（サプライチェーン）との接点を介した今回の感染事案は、国内病院に多く見られる、境界防御を前提としたセキュリティの考え方の死角 --- システム・サービスは基本的に何らかのかたちで繋がっている ---を示したものといえる。

ただ、こうした事例は国内の医療分野では少ないが（医療 ISAC が把握する限り、初ではない）、他業界（金融や通信、製造等）ではすでに数年前から見受けられているものであり、特に珍しいものではなく、どのような対策が合理的なのかについての検討もすでに行われているものである。

本レクチャーでは、今回の大阪急性期・総合医療センターの感染事案を取り上げながら、他業界での同種のサプライチェーン型のマルウェア感染事案を参考に、どのような対策を優先的に検討すべきかについて解説したいと思う。