医療情報システムの「サプライチェーン攻撃」対応のための提言

2022 年 12 月 19 日

大学病院 医療情報・企画部長会

本年 10 月 31 日に発覚した大阪急性期・総合医療センターにおけるランサムウェア攻撃は、同院に給食を提供する事業者である社会医療法人 生長会 ベルキッチンとの間に張られた VPN を経由して攻撃を受けた、典型的な「サプライチェーン攻撃」であった。

旧来、医療情報システムは「外部と隔離されている」という「神話」によって、その安全性が担保されているとされてきたが、実際には様々な支援や保守を遠隔で受けるため、様々な接続が為されている。医療機器や、医療サービスは、実際にそのサービスを受ける部門が個別に選定・調達することが多いことから、各病院の情報部門や医療情報システム安全管理者に相談されることなく、外部との接続が行われている医療機関も少なくない。

病院情報システムの安全管理については、厚生労働省「医療情報システムの安全管理に関するガイドライン」と経済産業省・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」の二つのガイドライン、通称「3 省 2 ガイドライン」が示されている。この内、厚生労働省のガイドラインと診療録管理体制加算の要件は、400 床以上の全ての医療機関に専任の医療情報システム安全管理者を置くことを求め、経済産業省・総務省のガイドラインは、システム・サービス提供事業者に自社のシステム・サービスの全情報流に渡る安全性をアセスメントした上で「サービス仕様適合開示書」の形で医療機関に示すことを、医療機関にこれを適切に理解して「サービス・レベル・アグリーメント」を結ぶことを、さらに両者が定期的に見直してこれらを更新することを求めている。

サプライチェーン攻撃を未然に防ぐためには、医療機関の情報システムに接続する全ての医療機器や情報システムの提供事業者、および、医療機関の情報システムを操作してサービスを提供する全ての事業者が、経済産業省・総務省のガイドラインに定められた書面を、医療機関の医療情報システム安全管理責任者に示すようにすべきである。また、全ての医療機関は医療情報システム安全管理者を任じ、安全性を適切に判断し実地に対応する能力を有する人物を含んだ体制を構築させるべきである。また、政府機関はこのような体制を整備するために必要な財政的措置等を講じるべきである。

医療機関の情報セキュリティの向上を果たし、優れた医療を途切れることなく提供し続けられるようにするために、大学病院医療情報・企画部長会は、全ての医療機関・関係事業者・関係政府機関に、上記に示す体制を整備するよう提言する。