令和 3 年 7 月 16 日

各位

一般社団法人 日本病院会
副会長　大　道　道　大
（情報発信担当）

遠隔業務委託システムにおけるサイバーセキュリティの再点検（注意喚起）

昨年来米国を始めとする各国において、重要インフラ事業者がサイバー攻撃の被害を受け、業務停止や制限、情報窃取、身代金請求等の被害に遭遇しています。特にランサムウェアによる被害件数、被害金額は著明な増加傾向を示しており、わが国においても例外ではありません。

国内の医療分野においては、2018 年に関西の病院において電子カルテシステムのランサムウェア感染が報告されていますが、多くの医療機関においては、業務系システムは原則インターネットと分離されたネットワーク構成となっているため、ネットワークを介した直接的なサイバー攻撃の被害は受けにくいと認識される経緯があり、外部からのサイバー攻撃を防ぐ対策の優先順位が未だに低いと言わざるを得ません。

しかしながら、電子カルテを含む医療情報システムは、地域医療連携システム、遠隔医療システム、遠隔読影システム、遠隔病理システムなどの外部への業務委託を前提とした業務システムや、医療機器やシステムの遠隔保守などの、外部とのネットワーク接続を前提としたいわゆる「バックドア」が複数存在しており、これらのシステムに存在しうる脆弱性を介して攻撃被害を受ける可能性があります。

近年では Citrix や Remote Desktop などの仮想化システムにおいても、仮想化システムサーバー自体の感染による大規模な被害も報告されており、絶対に安全なシステムは存在せず、特に遠隔業務委託システムとの接続に国内の医療機関が多く利用している FortiGate のファイヤーウォールアプライアンスには、高度なサイバー攻撃を仕掛ける APT グループが標的とする脆弱性が存在する旨の注意喚起を米国 FBI が行っております。

さらに、これらの脆弱性については、セキュリティ修正パッチが発行されているにも関わらず、システムにパッチを適用せずに運用している医療機関も多く、サイバー攻撃グループはそのような未パッチの機器をネット上で検索し攻撃を仕掛けてきます。

また外部委託先が提供する PC 端末やサーバー等において、ウイルス対策ソフトウェアの定義ファイルの更新が滞っている場合が少なからず存在すると思われることから、一日も早く状況を再点検して対策を講じることが必要な状況であると考えられます。

上記を踏まえ、医療機関等に対し以下の対策を推奨いたします。

1．遠隔業務システム等を含む外部へのネットワーク接続を前提とするシステムについて、委託先管理も含めて現状を再点検し、脆弱性対策やウイルス対策ソフトの更新等を行うこと。
2．現在猛威を奮うランサムウェア対策として、オフライン環境でのデータのバックアップを確実に保存しておくこと。（オンラインバックアップでは、ネットワークを介して暗号化が進行してしまうリスクが高い）
3．万が一事故が発生した場合の初動対応等についてマニュアル等の文書を整備し、インシデントレスポンスの依頼先についても、事前に検討しておくこと。

以上