医療機関・医療従事者各位

2021 年 12 月 2 日
一般社団法人 医療 ISAC

ランサムウェア対策に関する注意喚起

前略
平素は弊法人の運営に関して多大なご支援をいただき感謝申し上げます。

さて既に報道等でご存知とは思いますが、徳島県の公立病院の電子カルテシステムがランサムウェアに感染し、診療が大幅に制限される事態となっております。
また本年 5 月には大阪府の公立病院にて、遠隔読影システムがランサムウェアに感染し、放射線画像やレポートの閲覧が不可能となる自体が生じています。

上記の 2 事例に共通する点として、米国 Fortinet 製 Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)からマルウエアの侵入を許した可能性が高いと報道されており、また、データのバックアップがオンラインのみであったため、バックアップデータまで暗号化されてしまった結果、復旧が非常に困難になったという状況が推定されています。

上記の事情を鑑み、医療 ISAC としては一般的なサイバーセキュリティ対策に加え、以下の提言を行いますのでご参考にしていただけると幸いです。

1. 2021 年 4 月 30 日に内閣サイバーセキュリティセンター(NISC)が注意喚起を行っているように、以下の脆弱性の対策を早急に講じること。
   https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf
   特に Fortinet 製 Virtual Private Network(VPN)装置は、遠隔画像診断等で広く採用されており、委託事業者が病院側に持ち込んでいる場合もあるため、外部からの何らかの接続を行っている事業者に対して、以下のシステムを用いていないかどうか、また用いている場合は脆弱性対策を行っているかどうかの確認を行うこと。

   - Fortinet 製 Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)
   - Ivanti 製 VPN 装置「Pulse Connect Secure」の脆弱性(CVE-2021-22893、 CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)
   - Citrix 製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)

・ Microsoft Exchange Server の脆弱性(CVE-2021-26855 等)
・ SonicWall Secure Mobile Access (SMA) 100 シリーズの脆弱性(CVE-2021-20016)
・ QNAP Systems 製 NAS(Network Attached Storage)製品「QNAP」に関する脆弱性(CVE-2021-28799、CVE-2020-36195、CVE-2020-2509 等)
・ Windows のドメインコントローラーの脆弱性(CVE-2020-1472 等)

2. データのバックアップは、オンラインのみではなく、コールドスタンバイ、オフライン、オフサイト（外部のクラウドでの保管）を組合せて、仮にランサムウェアにメインシステムが感染しても、バックアップからデータ復旧ができる環境を構築しておくこと。
   またそのバックアップから実際に復旧が可能であることを確認しておくこと

以上、何卒ご確認のほどよろしくお願い申し上げます。

草々