JAHIS
健康で豊かな国民生活を保健医療福祉情報システムが支えます

2021年度　業務報告会

セキュリティ委員会　活動報告

2022年2月25日
セキュリティ委員
委員長　茗原　秀幸

JAHIS　サイバーセキュリティに対するJAHISの対応

- 今年度は医療機関に対するランサムウェアによる重篤な被害が発生し、マスコミでも大きく報道されている。
- JAHISセキュリティ委員会としても厚生労働省等と協力し各種啓発活動を実施している。
  - リモートサービスセキュリティガイドライン対応「ISMS準拠リスクアセスメントテンプレート」の公開（RSS-WG）
  - SDS書き方セミナーの開催による会員への啓発（MDS-WG）
  - 日本薬剤師会による啓発用コンテンツ開発への協力（セキュリティ委員会）
  - 審査支払基金に対するセキュリティリスクアセスメント支援（RSS-WG）

なぜこのような問題が生じたのか（推測）

- 当該病院の見解として「サーバーの遠隔保守用の通信回線などが、侵入経路の可能性がある」旨が公表されたが特定はされていない。（痕跡が消去されていた模様）
- バックアップシステムが同一ネットワーク上にあり、バックアップも暗号化された。（水害対策を考慮し同一施設内の高所に設置されていた模様）

境界型防御の境界を突破され、ネットワークアクセス可能な機器が全て攻撃を受けることとなったと考えられる。

各サーバやクライアントはウイルスチェックプログラムが稼働していたはずであるが、突破されているということはゼロデイ攻撃（防疫システムのパターンファイルに登録されていない攻撃）が行われた可能性が高い。

どうすれば被害を極小化できたのか　その1

その1：リモート保守用のノードの脆弱性を塞ぐことができていなかった可能性

令和3年6月28日付「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」（厚生労働省政策統括官付サイバーセキュリティ担当参事官室、厚生労働省医政局研究開発振興課医療情報技術推進室、厚生労働省医薬・生活衛生局医療機器審査管理課、厚生労働省医薬・生活衛生局医薬安全対策課事務連絡）

以下の注意喚起が出ていることが事務連絡によって通知されていた。

2021年4月30日付NISCによる「ランサムウエアによるサイバー攻撃に関する注意喚起」

ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。

- 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」「CitrixSD-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)

どうすれば被害を極小化できたのか　その2

その2：データの論理破壊に対する防護措置の不備

物理破壊対策としてのバックアップは用意されていたが、論理破壊に対する防護手段が用意されていなかった。

論理破壊に対する防護：ネットワークを切り離した環境や物理媒体などにバックアップを作成することで防護可能

論理破壊はランサムウェアのみならず、プログラムのバグによる異常動作、人為的ミスによる消去、悪意による消去などでも発生するため、サイバー攻撃であるか否かにかかわらず本来は対策が必要となる。

厚生労働省の医療情報システムの安全管理に関するガイドライン第5．1版にも7．3保存性の確保についてのB項考え方に「コンピュータウイルスや不適切なソフトウェア等による情報の破壊及び混同等」が脅威として記載されている。ただ、C項では「いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。」となっており、具体的な防護策には言及していない。

適切に管理する→論理破壊に対する対策の実施が必要

サイバー攻撃と医療安全

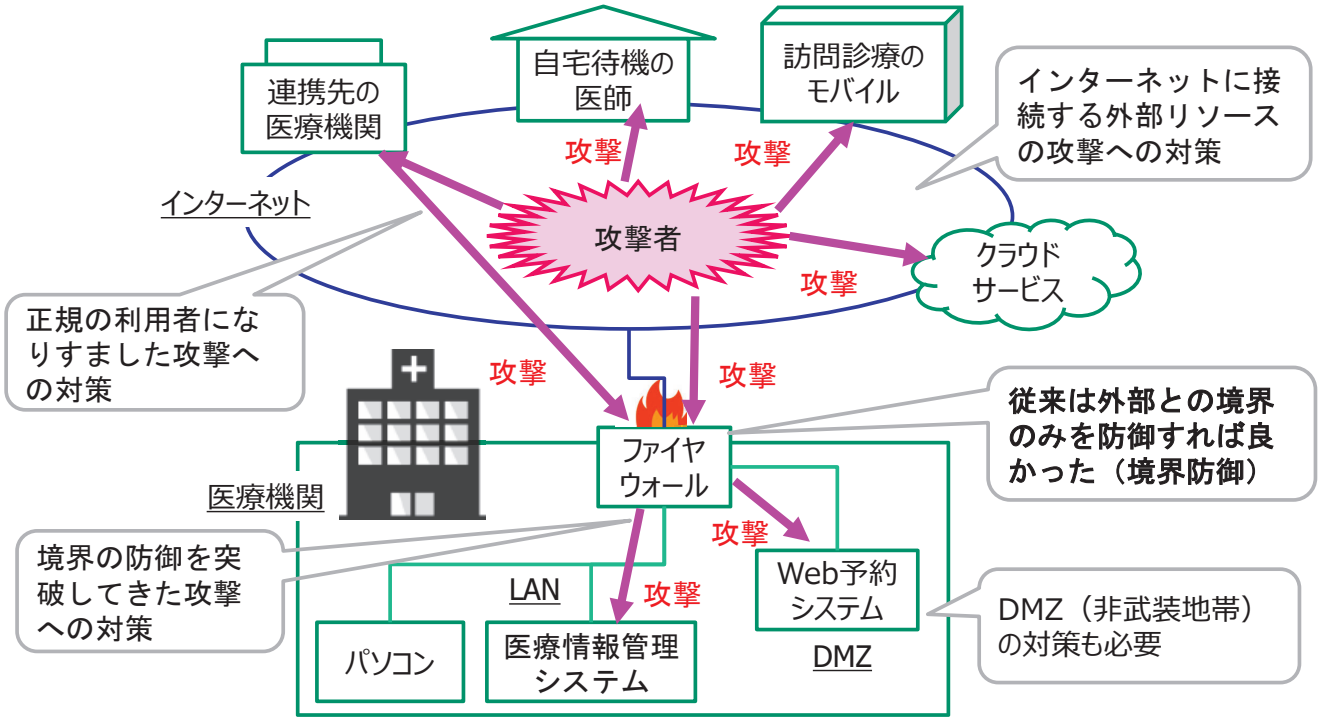
- サイバー攻撃は引き金事象でそれによって起こるのは医療情報システムの異常である
- 医療情報システムの異常＝医療事故ではない
- 通常の情報セキュリティ対策で対処可能であればインシデントとして事態は収束する
- 異常が生じたシステムを起因とする医療安全問題が発生した場合に医療安全管理上のアクシデントとなる。

医療情報システムの異常に対する対策と引き金事象の予防の両方の対策が必要

セキュリティマネジメントの観点から考えると、片方に過剰な対策を実施することは費用対効果などの観点から経営上のバランスを欠く可能性があるため、意思決定権者は適切な視点で意思決定を行う必要がある。

サイバーセキュリティ対策の考え方

多様な攻撃パターンを想定した対策が必要です。



究極の結論：サイバー攻撃で医療は止まるのか→効率は落ちることがあるが止まらない

サイバー攻撃によるシステム停止と経年劣化による故障は何が違うのか→発生する現象は同じ

サイバー攻撃は引き金事象、その結果として引き起こされるのはシステムの異常
システム異常に対する対策や対処は従来から行われてきた

システムの異常が患者安全に影響を与える可能性がある場合は医療安全管理の問題に移行
システム異常に伴う医療安全問題に対する対策や対処は従来から行われてきた

結局、事象が起きた後は、やることは従来と一緒でサイバー攻撃に特化したものはない

じゃあ何もしなくてよいのか、というとそうでもない→事象の発生の防止の視点も重要
引き金事象が起きる前に出来ることはある→サイバー攻撃を意識したセキュリティ対策の実施
引き金事象を起こさないようにすればサイバー攻撃は防ぐことができる
ただし、セキュリティに100%はない→発生確率を下げることが目的
発生確率を下げるための対策費とリスク受容のバランスがセキュリティ対策のポイント
要するに純粋に経営判断
（1年あたりの引き金事象発生確率を1%にするのに10万円、0.1%にするのに100万円、0.01%にするのに1000万円かかるとして、医療機関等が支払うべき費用はいくらが適正なのか）
発生した後の対応を上記のように準備している状態で、発生確率を下げるための適正コストは？
（引き金事象が発生してもシステム異常の対策が適正なら大きな事故には至らない）

JAHIS会員各社が行うべきこと

- 自社が提供するシステム・サービスに対する脆弱性の把握と可及的速やかな対応
- 医療機関等からの問い合わせや相談に対する適切な対応と情報開示
- 昨今の情報セキュリティ事故を踏まえた適切なシステム・サービス設計

行わなければならないことは、サイバーセキュリティに特化したものではなく、常日頃から様々なセキュリティのリスクを踏まえた対応が必要

健康で豊かな国民生活を保健医療福祉情報システムが支えます

ご清聴ありがとうございました