インシデントからの学び

－より安全な医療に向けて－

2023年2月15日

一般社団法人ソフトウェア協会（SAJ）理事
Software ISAC 共同代表
萩原健太

構成

- はじめに
- 大阪急性期・総合医療センターのインシデント
- 皆様へのお願い
  - 医療機関の皆様へ
  - 医療関連ベンダーの皆様へ
  - 販売・セキュリティベンダーの皆様へ
- 終わりに

はじめに

医療機関、関係機関の皆様へ

見ているもの・思いは同じ

医療従事者、システム・医療機器ベンダー、セキュリティ専門家も…

- 命・健康のために
- 医療行為を中断させたくない
- 日本・世界の医療提供・研究のために
- 安心・安全の医療のために

デジタルトランスフォーメーション

デジタル技術を用いて、これまでの枠組みに取られず
事業を変革すること

セキュリティ対策の考え方もリセット

何が起きているのか？

主に世の中で起きているインシデント

シンプルに…

- セキュリティ機器を始めとしたソフトウェアの脆弱性を突いた攻撃が発生
- メールなどの添付ファイルやリンクからマルウェアをダウンロード、実行
- USBのデータ持ち込み時のマルウェア持ち込み
- 設定不備等によるインシデント

大阪急性期・総合医療センターの
インシデント

医療業界のシステムに対する常識は非常識？

- 閉域網だから安心
- ベンダーにお任せ
- 他部門や医療機器のシステムはわからない
- 古いソフトウェアの利用や更新を行わない
- セキュリティ対策ソフトを適切に機能させない

インシデントの概要

大阪急性期C（OGMC）での対応

日付	項目
22年 10月31日 (オンライン)	• **厚生労働省より初動対応支援に関する依頼** • 電子カルテベンダー、関連事業者（給食事業者）の関係者と打ち合わせ • 警察庁を経由し、大阪府警察本部（以下、大阪府警）との調整
11月1日 (現地)	OGMC、大阪府警、電子カルテベンダー等が出席する会議に参加（以降、定例化） 以下の確認や対応のお願いを実施 • 給食事業者側の証拠保全対応（To 大阪府警） • バックアップの確認（To 電子カルテベンダー） • ステークホルダーへの報告、院内システムの現状把握、調査方法・方針、復旧に向けた情報整理、復旧対応の優先順位付けと行動の整理など（To OGMC） ＜確認・調査＞ • 環境（ネットワーク構成、システム、外部接続ポイントなど）、感染状況、対応状況の確認・ヒヤリング • セキュリティネットワーク機器等のログ確認 • 感染していなかったActive Directoryのポリシー及び同サーバのログ取得・分析 • ツールを用いた侵害確認
11月2日	• 定例会議に参加 • 経営者（総長、病院長等）向けに状況や対応の方向性等に関する説明の実施 • 継続調査、フォレンジック端末の選定 • 関係組織との連携（厚生労働省、警察庁、NISC、大阪府警、電カルベンダー（サイバーセキュリティ関連部門、ネットワーク事業者、セキュリティ事業者）など
11月3日	• 定例会議に参加 • 継続調査（給食サーバの調査（検体を含む攻撃ツール等の発見）） • 現状整理（現時点での報告書作成）
11月4日	• 定例会議に参加 • 電子カルテベンダー、給食事業者、大阪府知事との打ち合わせ

初動対応の想定範囲

遮断
- ネットワーク、他の端末への感染拡大を防ぐためにすべてを遮断する

状況確認
- 状況を把握し、調査や対応方針作成などの初動支援　（→セキュリティベンダーの紹介で本来は終了想定）

侵入経路の特定
- 想定される侵入経路はどこか？（ネットワーク機器やプロキシ、ADなどのログを確認する）

簡易調査
- ツールを用いた侵害調査や他の不正プログラムなどを探す調査を実施する

詳細調査
- 疑わしい端末を選定して、セキュリティ企業に解析やフォレンジック依頼をする

復旧
- 基本的には初期化をして再セットアップ／ファイル調査／USBタイプのフルスキャン／複数ベンダーによるフルスキャン）
- 委託先のセキュリティ状況などの確認

No	項目
1	関連サーバや端末の保全
2	電子カルテ参照環境の検討・構築
3	電子カルテシステムの再構築
4	部門システムのサーバ再構築

皆様へのお願い

ソフトウェアとは？

- コンピュータを動作させる命令の集合体
- 最近のソフトウェアはインターネット接続が基本となっている

ソフトウェアは「更新」を行い、機能や脆弱性などの改善を行い、利便性や機能性、安全性などを高めていく必要がある

医療機関の皆様へ

責任はベンダーではなく利用者（医療機関）にある

- どの業界でも、どの規模でも、システムやサービスを使っていれば、利用者にも責任はある。

システムも「かもしれない」運転

- × インシデント対応してくれるだろう…　○ インシデント対応してくれないかもしれない…

システムをセキュリティ（＋契約）を考える

- 自分たちの情報資産（パソコン、サーバ、ネットワーク、データなど）を把握する。
- 脆弱性を残したまま使用している製品やシステムは健全か？
- ベンダーの言いなり？

今あるセキュリティ製品を「使い切る」

- 新しいセキュリティ製品やサービスを使うことが、セキュリティ強化ではない。（DXでもない…）

バックアップを適切にとる

- データ、システム、設定ファイル、オフラインなど

医療関連ベンダーの皆様へ

「情報の非対称性 ＋ 説明責任」の理解

- **私たちの身体を診てくれる専門家は病院。それでは、システムや機器を見てくれる専門家は？**

脆弱性が存在する（または、生み出す可能性がある）モノの提供が適切か？

- **サポートが切れたソフトウェアや脆弱性を放置しない。**
- **サポートが切れる想定のソフトウェア使用製品は出荷しない。**
- **人が脆弱性を生み出さない。（管理者権限、簡単なパスワード、フラットなネットワーク構成など）**

「仕様です」だけでは、医療に安全をもたらさない

- **検証が必要なのであれば、使用している医療機関や競合、業界全体で解決を図る。**
- **使う立場でものを考える（セキュリティ対策ソフトを入れない？ネットワーク接続するのにセキュリティは無し？）**

医療関連ベンダーの皆様へ
(医療機関の皆様も…)

- もし自分たちの組織で使っているシステムや機器などが…
  - 内部に侵入されたら簡単に、横展開されてしまう仕組みだったら？ → マイクロセグメンテーション
  - 誰でも、どの情報にアクセスできる状況だったら？ → アクセスコントロール
  - 外部のどこからでもアクセスできる状況だったら？ → ジオブロック、IPアドレス制限
  - 好きなソフトウェアは導入・利用し放題だったら？ → ユーザ権限運用、アプリ制御
  - 簡単なパスワードを利用していたら？ → 類推しにくい、個別、長く
  - セキュリティ対策ソフトが入っていなかったら？ → 適切に導入、設定
  - バージョンが古かったら？パッチを当てていなかったら？ → バージョンアップ、パッチマネジメント
  - ログが取れていなかったら？ → ログリスト、ログ保存の最長化
  - バックアップが無かったら？ → クラウドやオフラインバックアップの活用
  - 脅威・脆弱性情報が無かったら？ → 情報収集
  - インシデント対応ができなかったら？ → 訓練・演習

販売・セキュリティベンダーの皆様へ

特にセキュリティ製品に売り切りはありえない

- 脅威や脆弱性対応のために継続的に更新が行われている

今あるものをどう使ってもらうのか？

- 導入している製品のバージョンアップや使えるオプション情報の提供や設定支援

お客様の身の丈に合った提案ができているのか？

- 一人情シスでEDRが使いこなせるか？

脅威ベースではなく、お客様の資産や資源の視点から

- 脅威は変わる。でも大切な資産の根幹は変わらない。

終わりに

医療機関、関係機関の皆様へ

安心・安全の医療のために

【インシデントからの学び】

【医療の安心・安全のために】

医療継続の体制の凄み	**倫理・使命・事業継続の考え方の継続**
閉域網神話、ベンダー依存	**意識改革と行動が必要**
責任分界点の不明瞭さ	**対話・協議を継続し、役割・責任・リスクの捉え方を明確に**
ガイドラインも大切ですが通知(注意喚起)の対応	**今できることをやる**

もし困ったら…

あまり大事になっては困る

自分たちで解決できる

「インシデントかも？」にご相談ください

（厚生労働省にもご報告を…）

https://mhlw-training.saj.or.jp/

明日、サイバー攻撃を受けるのは
皆様かもしれません…

Fin.