つるぎ町立半田病院から学ぶ インシデント対応と対策

2022年6月20日

萩原　健太

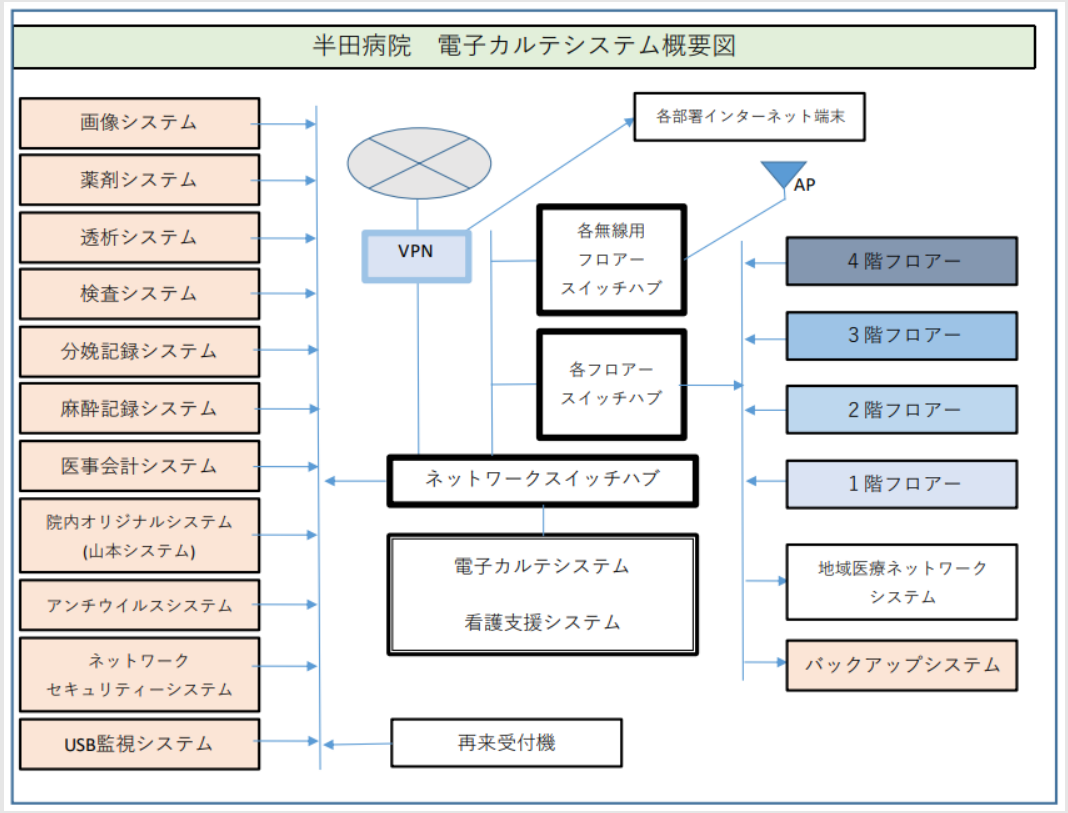
本日のお話にあたって

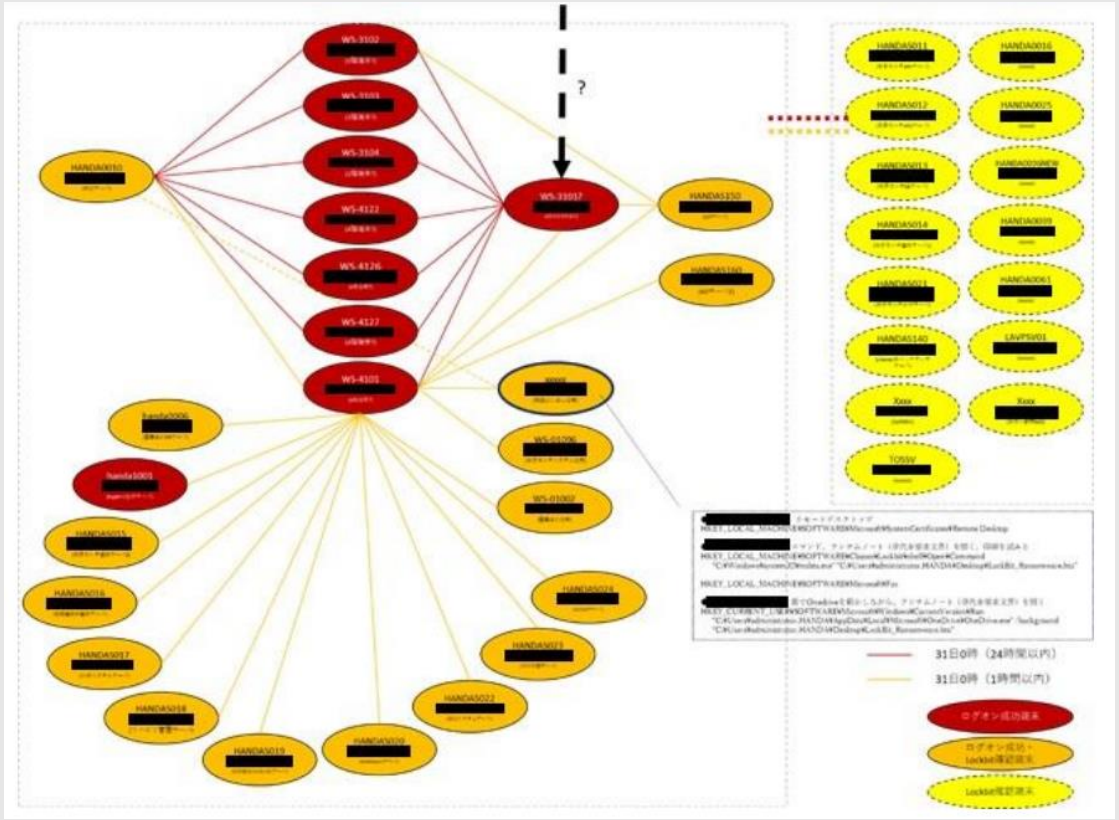
- スクリーンショット、録音、SNSの投稿などを一切禁止とさせていただきます。
- 本講演はつるぎ町立半田病院が公開している報告書の範囲でお話をいたしますが、チャタムハウスルールを適用いたします。
- 一部、報告書以外の内容で、講演者の私見が入る場合がありますが、当方が所属するすべての組織を代表したコメントではございませんので、ご了承ください。

何が起きたのか？

- Lockbitによってランサムウェアに感染し、医療システムに関連するサーバやPCで大規模に感染
- 電子カルテシステム、麻酔記録／分娩台帳、透析管理、健診システム、医事会計DBなど、医療に関連するサーバや端末の大規模感染
- VPNの脆弱性を悪用した侵入した可能性が極めて高い
- 電カルベンダー（C社）、保守ベンダー（A社）、フォレンジックベンダー（B社）の不誠実な対応

システム構成・インシデントの流れ





そもそも半田病院の体制は？

- 電カルシステムを2011年導入、2018年に更新（IE7との互換）
- 電子カルテ端末のウイルス対策は無効か。Windows updateなども実施せず
- HTTP通信が前提の電カル
- 一人情シス状態
- 資源（ヒト、カネなど）は議会承認ありき
- ステークホルダーの多さと難しさ（公営企業法など）
- BCPはあり、サイバー攻撃に関するマネジメントシステムの欠如

どうやって対応したの？

- 南海トラフ地震を想定したBCPの発動と対応
- 徳島県警へ相談　→　被害届へ
- IPAに連絡（役に立っていない…）
- A社紹介のB社対応（データ保全の観点の欠如）
- 現地の担当者中心に対応
- B社によるデータ復元

どうしたら防げたのか？

- VPN装置のファームを更新していたら…（インシデントの3－4日後…）
- ウイルス対策ソフトを有効化していたら…
- 閉域網という「ウソ」？
- Windows Updateやパターンファイルの更新をしていたら？
- 電カルを使っていなかったら？（ActiveX、Silverlight..）
- 電カルベンダーや保守のベンダーとコミュニケーションができていたら？
- AD設定していたら？（パスワード数、ロックアウト設定など）
- 電カルやVPN装置など、適切に情報を入手していたら？
- パスワードの設定を強くしていたら？

医療関連のシステムについての疑問

- 既にオープン系ではないのか？（リモートメンテナンスしないと壊れるものも？）
- 電カルシステムが古くはないか？
  - 導入したらおしまいになっていないか？
  - クラウドに移行しても注意が必要（アプリケーションそのものの構造や仕様変更など）
- 責任分界点は？ステークホルダーとの断続的な連携は？
- ISMS並みの厚労のガイドラインには準拠できないのでは？

サイバーボランティア制度

- セキュリティの専門家が不在の中小公益団体に向けて
  - サイバー攻撃に対する初動体制への助言
  - 確実に実績のあるセキュリティ調査会社の紹介
  - 調査結果に基づく防御対策
  - 制度改革を支援など、広くノウハウを共有

  → 社会全体のセキュリティ防御態勢の向上と事業継続を狙うもの

2022/6/24

TO BE CONTINUED…?