令和6年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【システム・セキュリティ管理者向け研修】
新規Aコース
～ インシデント対応　平時編 ～

大阪大学　D3センター　教授　CISO
猪俣　敦夫
Ph.D, RISS, CISSP

自己紹介（いのまたあつお）

大阪大学　教授

D3センター、大学院情報科学研究科

情報セキュリティ対策室室長, OU-CSIRT隊長

- (一社)　公衆無線LAN認証管理機構　代表理事
- (一社)　ライフデータイニシアティブ(LDI)　理事
- (一社)　大学ICT協議会（AXIES）理事
- (一社)　JPCERTコーディネーションセンター　理事
- 京都女子大学、東京薬科大学、慶應義塾大学、NAIST、東京電機大学　他
- 経済産業省　ソフトウェアセキュリティTF委員
- 総務省　公衆無線LANセキュリティ委員会座長
- 2025大阪・関西万博サイバーセキュリティ有識者会議委員
- (株)カプコン　セキュリティ監督委員
- 阪急阪神HD (株)　サイバーセキュリティ顧問
- (株)ベネッセHD　情報セキュリティ監視委員
- NEXCO東日本・中日本・西日本　ETC開発委員、　他多数
- IPA 情報処理安全確保支援士　特定講習講師
- 大阪府警、奈良県警察サイバーセキュリティアドバイザ
- NTT西日本情報漏洩事案内部調査委員会 委員
- 大阪急性期・総合医療センターインシデント調査委員会委員長、他

セキュリティ3大要素

今や何も考えずに使っている「情報セキュリティ」という言葉

機密性 Confidentiality	完全性 Integrity	可用性 Availability

CIA

でも最近

AIC　これはどうしてでしょうか

IT-BCPに大切な準備、それが「平時」

今回は、大きく以下の４つの視点で見ていきます

1. 資産管理
2. ステークホルダー管理
3. リカバリー・復旧への準備
4. 教育・訓練

情報から情報資産に視点を移していこう

- 情報資産の流出（例えば、個人情報漏洩など）
  - 物理的脅威
    - パソコンやHDDの物理的盗難
  - 技術的脅威
    - アンケート・懸賞、掲示板やSNSの書き込み、ホームページからの情報流出
    - マルウェアの侵入やキーロガーによる監視
  - 人(為)的脅威
    - 設定方法ミス、安易なパスワード設定、内部での情報収集

1. 情報資産

ネットワーク機器の棚卸し

- 院内設置のすべてのVPN装置、Firewall、ルーターの所在と、IPアドレス、使用用途を明記した一覧を作成
  - 何が存在しているのか、実はベンダー任せになっていることが多い
- ルーターについては、詳細なルーティング情報を取得
  - インターネットはどこ（のISP）に接続されているのかを確認
- 部門・診療科システムにおいて、サーバーのNIC（ネットワークインタフェースカード）2 枚挿しについては、当該サーバーでスタティック・ルートを確認し、HIS系ネットワークとの疎通状況を把握の上、適切なルーティングを適用
  - NIC 2枚挿しのサーバーが存在しているか、あればその確認が重要

ネットワーク構成図の整備

- HIS 系、インターネット系等の院内LAN、外部接続点（Firewall, VPN, 地域連携, オンライン資格確認等）のネットワーク構成が判別できるようIPアドレスおよびルーティングがわかる構成図を整備
  - 院内ネットワークのトポロジ図はすぐ参照できるようにしておくこと
- 各診療科をはじめ、病院内にシステムや機器を別途有する場合、情報システム主幹に情報を提供し、病院として１つのネットワーク構成図が整備できるように協力
  - 部局任せにするのではなく、本部（中央）でネットワークのトポロジを管理できることが望ましい

ネットワーク機器の脆弱性管理

- 病院が管理する機器と、ベンダーが管理する機器を明確化し「脆弱性情報の収集」「脆弱性対応プログラムの適用基準」「ロールバックの手順」を定義
  - 誰が「調達」「設置」「導入」「運用」「管理」しているのかを今一度見直すこと。ベンダー任せがリスクを招くことも多く、(部門の管理者など)自身の目で見ておくことも大切
  - 責任分界点の曖昧さがインシデント発生時に混乱を招くことになる

サーバー、クライアント一覧の整備

- 院内のサーバーおよびクライアントの「コンピュータ名」「OS」「IP アドレス」「 役割（ドメインコントローラー、電子カルテサーバー等）」「脆弱性対応状況」「コンピューターウイルス対策ソフトの稼働状況」の一覧の整備
  - 現場担当者の負担を増加させることになってはならない、Excelシートなどでの簡単な台帳管理が望ましい
  - 管理者権限（特権ユーザ）でログオンする必要のあるコンピュータを明示しておくこと

外部接続ネットワーク装置一覧の整備

- 病院設置、ベンダー設置を問わず外部ネットワークと接続する 「Firewall」 「ルーター」「 VPN装置の型番」「OS/ファームウェアのバージョン」「 接続先 IP グローバルアドレス」「 接続先会社名」「接続方式(IP-Sec、SSL-VPN 等）」「 許可されているポート」の明確化
  - インターネットと接続するポイントをすべて洗い出すこと
  - サイバー攻撃との結節点であることを認識すること
- ファームウェアのアップデートについて、ベンダー等からの対応の是非の提案に対し、対応方針の明確化
  - ファームウェアのアップデートについてベンダーと取り決めがなされているのかを確認すること

外部接続サービスに対する監査の実施

- 外部接続サービスを行っている契約先事業者の管理体制状況や契約遵守状況を、必要に応じて監査の受入れを求めた上で現地で確認を行い、その状況を情報セキュリティ管理者に報告
  - ベンダーがさらに再委託を行っている場合なども多々あり、その管理体制について話をしておくことが重要。その体制の曖昧さによって、インシデント発生時に想定外のミスが重なることも現実的にありうる
  - シャドーITと呼ばれる把握できていないネットワーク機器が設置されていた事例もある。
    例えば、監視・リモート保守用にベンダーによって持ち込まれた、4G LTE対応モバイルルータなど

脆弱な情報システム・医療機器・検査装置等の保護

- 医療機器のサイバーセキュリティ 導入に関する手引書（第2版）に基づく情報提供を受け、通信の厳格化、不要な通信ポートの停止、脆弱な通信プロトコルの停止等の実施
  - とりあえず「今後使うかもしれない」がリスクを招くことにもなる
- IoT 機器用通信制御機器等を設置し、異常の検出や通信の遮断を実施
  - 安価なデバイスだから監視は不要という考えが大きな誤り
- 脆弱なシステム等の更新・刷新の計画
  - 短期的(1年以内)、中期的(3年程度)、にどのようなシステム更新計画があるかを経営層が認識できるようにすること

運用環境の取りまとめ

- システムごとの管理者権限の使用状況、コンピューターウイルス対策ソフトの稼働状況（更新等を含む）、脆弱性対策プログラムの適用状況、IDなどのロックアウト(使用不可)設定、 Microsoft Defenderなどのパーソナルファイアウォールの稼働・設定状況、管理者ID及びパスワードの一覧、RDP（リモートデスクトップ）ポートの状況、その他の通信許可ポートの一覧を取得し、フォレンジック調査等へ貢献
  - 一度実施したら終わりでなく、現場担当者の負担を考慮した上で定期的に見直しを実施し、現況を共有し合うことが大切

ログの整備

- 重要なサーバーログを上書き設定（既定値）からアーカイブ設定に変更することが望ましい

例えば　Windowsサーバ

- Security ログ、アプリケーションログ、システムログ、
- TerminalServices-RDPClient%4Operational.evtx
- TerminalServices-RemoteConnectionManager%4Operational.evtx、
- TerminalServices-LocalSessionManager%4Operational.evtx
- PowerShell%4Operational.evtx

- Microsoft Sysmonのインストール Sysmon.exe -i オプションを実施
- Syslog サーバーを設置し、Firewall、ルーター、VPN 装置のSyslog動作が望ましい

インシデント後、ログが全てを助けてくれる唯一の情報になる

2. ステークホルダー管理

ステークホルダー連絡先整備

- 非常時用の病院内外のステークホルダーへの連絡先（電話、メール、携帯・スマートフォン）の整備
  - インシデント発生時を想定した連絡網の用意、定期的確認
- インシデント発生時に協力を得られるセキュリティベンダーの選定
  - きっと何かしてくれるに違いない、という思い込みからの脱却
- ステークホルダーからの連絡や問い合わせの増加が見込まれる場合に備え、電話窓口を増やす準備
  - インシデント発生時にはHPを閉鎖せざるを得ないこともあるため、問い合わせ窓口をどうするか事前に検討しておくこと

セキュリティベンダーとの事前打ち合わせ・訓練

- ユーザー判断で保全を行わずに措置を講じると原因究明が困難になることから、あらかじめセキュリティベンダーと最低限実施すべき措置と行ってはいけない措置を定め、病院職員向けにトレーニングの実施が望ましい
  - マニュアルの整備だけでは実際に動けないことも多い、現場の負荷を考慮しつつ最低限のトレーニング計画を策定、実施について検討すること

責任分界の確認

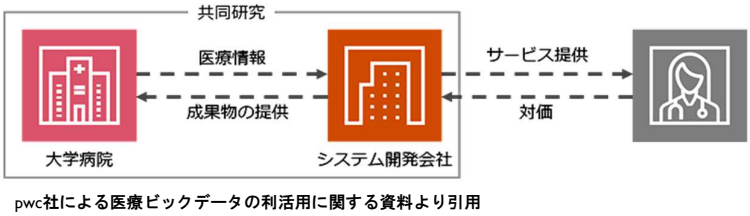
- 医療情報システムに関する情報システム・サービスの委託において、JAHISおよびJIRAに基づくMDS/SDSやサービス仕様適合書等の機能仕様に関する情報等の収集
  - MDS/SDSは、自組織のリスクアセスメントに活用でき、技術的かつ運用的対策の立案に有効

- 委託時の仕様書等により事業者と通常運用時や非常時における技術的な対応に関する責任分界の調査
  - 脆弱性情報の収集と共有、リモート保守接続元機器・端末、通信機器、接続先機器・端末の脆弱性管理の実施主体の明確化

責任分界の確認

- サイバー攻撃等が生じた場合、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整しその結果を情報セキュリティ管理者に報告
  - 侵入された可能性のあるポイントはどこか
  - 横展開されている可能性がある構成か
- 医療情報の第三者提供を行う際の責任分界について、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、情報セキュリティ管理者に報告
  - 第三者提供を行う情報の詳細は整理されているか
  - 適切な手段で提供が行われているか

図表2：システム開発会社と大学病院のAIの共同研究の内容□



pwc社による医療ビックデータの利活用に関する資料より引用
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/privacy-articles09.html

3. リカバリー・復旧への準備

待機系電子カルテサーバー

- 感染したサーバーからの復旧が困難な場合があることから、待機系サーバーをオフラインで用意、なおクラウド利用でも良い
  - インシデント発生後には、利用できるPCが大きく制限されることを意識しておくことが大事

オフラインバックアップ

- ライトワンス（一度だけ書き込み可）、イミュータブル（変更不可）、オフラインのバックアップを確保
  - ライトワンス、イミュータブルであっても、システムのOS、ファームウェアが攻撃されることを想定した検討をしておくこと

安全なシステムイメージの取得

- 正常な状態でのサーバー、クライアントのシステムイメージを取得しておき、インシデント対応時にシステムイメージから復旧、なおシステム構築・刷新時での取得が望ましい
  - 可能な限り、定期的に正常状態のスナップショットをとっておくことが望ましい

ワープロ端末システムイメージの取得

- 電子カルテ、HIS 系ネットワークが停止した場合、紙カルテ運用となるが、手書きによるインシデントが発生しやすくなるため早期にワープロ端末の提供が必要となることも多い
  - OS、アプリ、プリンタードライバーのシステムイメージを取得しておき、早期にワープロ端末を提供できるようにしておくことが望ましい
  - スタンドアロン動作でWord、Excel等の事務処理ができる環境を用意しておくこと

USB型ポータブルコンピューターウイルススキャナーの導入

- Windows、（Linux）でのコンピューターウイルス検索ツールの導入
  - AntiVirusソフトウェアのほとんどがこの機能を提供しているが、念の為確認しておくこと

4. 教育・訓練

インシデント発生に備えた一般職員向け教育の実施

以下の点を教育しておくことが大切

- 日頃からサイバー攻撃のニュースなどに目を通し、最新の事例（標的型攻撃など）を把握しておくこと
- インシデント発生の兆候を認識できるように、ウイルス感染時のPCの挙動について知ること
- 感染の兆候もしくは、感染が確認された端末の LAN 抜線以外は調査の観点から電源を落とさずにすぐ連絡すること
- インシデント発生時の連絡先について、所属部局の上長ら（不在であれば担当部署）に可及的速やかに報告すること

IT-BCPの維持管理

- IT-BCPの策定および定期的な見直しの実施、ならびにBCPに基づく定期的な訓練・演習の実施を行うことによる必要な改善に向けた対応の実施
  - なぜIT-BCPが必要なのか、その意義をもう一度、職員全体で考えることが大切。会議の場などにおいて定期的にIT-BCPについて取り上げることが望ましい

おわりに

サイバー攻撃は決して他人事ではない

自分たちの組織でも起こることを前提とした
備えがとても大事

今あなたの周りに何人相談出来る人はいますか？

ありがとうございました。