日本のサイバーセキュリティを「連携」「学び」「創造」

日本ネットワークセキュリティ協会 (JNSA) 社会活動部会 医療ITワーキンググループの紹介

2026年 7月 22日

医療ITワーキンググループ リーダー
新　善文

Agenda

- 医療IT WGの紹介
- 医療情報・IT関連の課題
- 医療関連団体との連携

背景知識：医療情報セキュリティを取り巻く状況

サイバーインシデントの増加

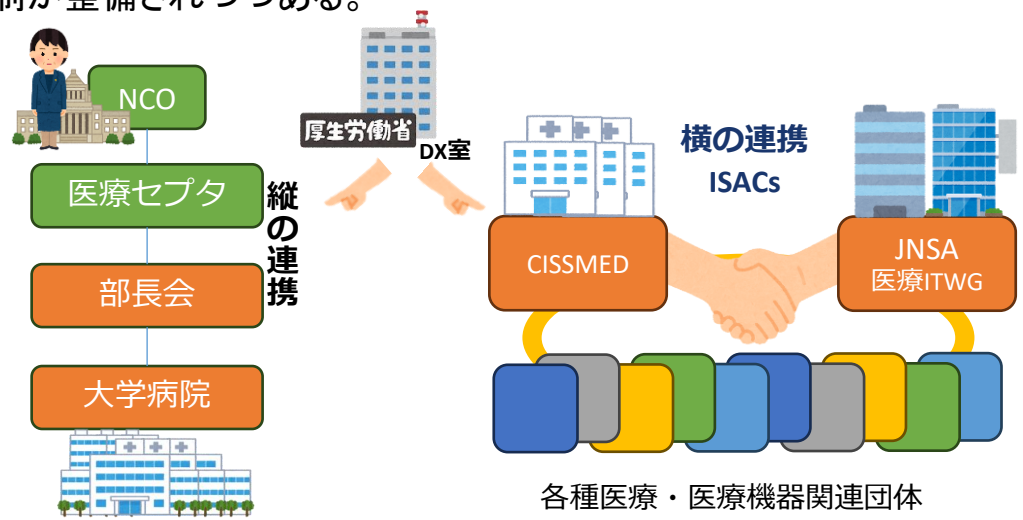
医療機関のサイバーインシデントは繰り返し発生し、増加傾向。
2018 宇陀市立・2021 半田病院・2022 大阪急性期・2026 日医大武蔵小杉

政府による制度整備の進展

政府は、臨床現場のセキュリティ向上に資する制度と実践を推進中。
2022年 医療情報GL改定 2023年 医療法改正 2026年 診療報酬改定
2026年 経済安保法改正で特定機能病院を基盤インフラに指定する方向

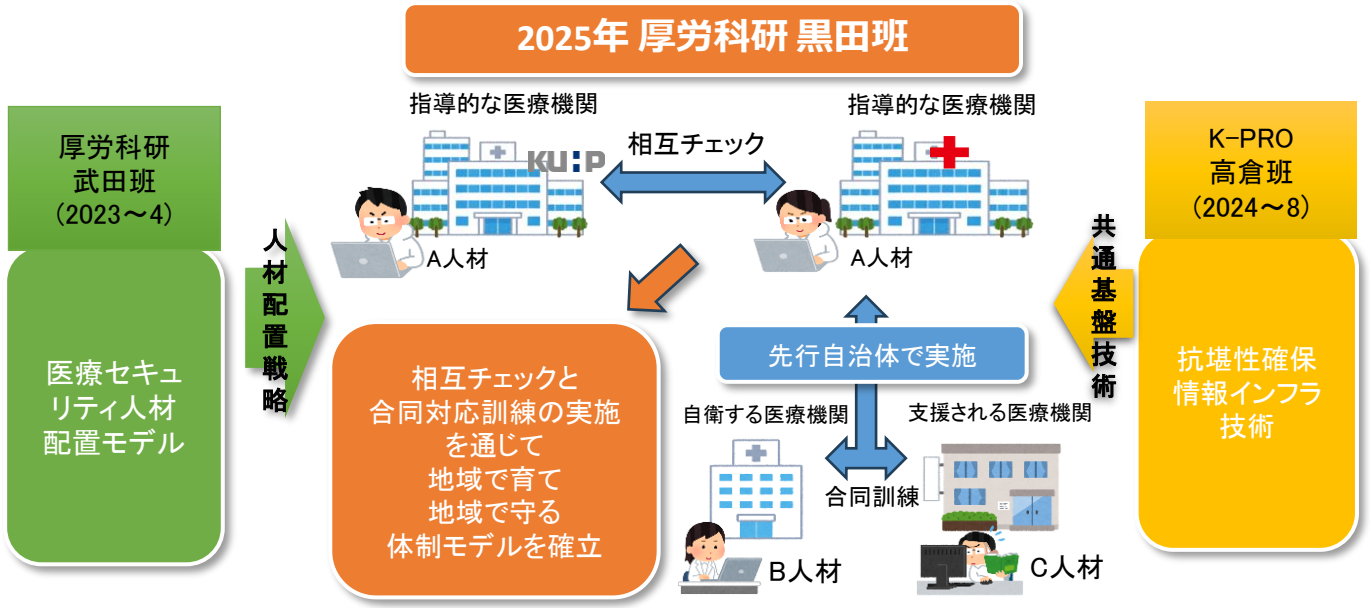
人材ネットワークと連絡体制の整備

厚生労働省DX室は、NICTから病院情報部門への連絡体制の再整備を図り、医療セプター構成員に大学病院医療情報・企画関連部長会（部長会）を追加。併せて、同室の支援の下で、臨床現場のIT担当者の情報共有組織（ISAC）としてCISSMEDが設置。 ベンダーのISACとして日本ネットワークセキュリティ協会（JNSA）の下に医療ITWGも設置され、各種医療・医療機器関連団体との協力・連絡体制が整備されつつある。



実装パッケージの設計とモデル化を推進

厚労科研　武田班（2023）で、人材配置の在り方を検討し、医療情報学会（JAMI）と情報処理推進機構（IPA）が協定を結び、教育コンテンツの整備を実施中。
また、厚労科研　黒田班（2025）で、合同訓練パッケージの開発・整備を進めるとともに、臨床現場で容易に実質的な対策を打つ方法等をK-PRO高倉班等で検討・開発中。



医療IT WGの紹介

背景

- 電子カルテの普及、ネットワーク接続する医療機器の増加、医療DXが推進される中で医療情報システムの重要性が高まってる。
- 一方でサイバー攻撃などセキュリティや情報システムの運用や委託といった課題がある。
- 各省庁や団体から各種ガイドラインが発行されているが実装や運用とのへだたりがある。
- 省庁間や団体がが必ずしも連携が取れていない中で機器ベンダーやサービスベンダーの意見とりまとめをおこない、現実的な対応の調整を行う必要がある。
- 技術が進歩し、ネットワーク環境(サービス、技術)が変化、Sierなど取り巻く状況も大きくかわってきている
- セキュリティについても攻撃の高度化や技術の進歩で常識が変化している

目的

- 医療システム(電子カルテ、ネットワーク、医療機器などを含む)と医療機器のセキュリティや安全性の確保のために、機器、システム、運用といった観点からどのような技術や体制、運用をするとよいかを整理し、その実証実験などをおこないながら、実システム・実運用への適用を目指していくことを目的に活動する。

JNSAはITベンダー、セキュリティベンダー、SIerなどが集まっている

- 医療業界の常識、問題意識、課題を共有して対応できるようにしたい
- 解決にむけての協力体制を作りたい

医療IT WGの紹介

活動内容

- 定期的な会議の開催（勉強会を含む）
  - ハイブリッドまたはオンライン
- 医療情報関係の各種のセキュリティや運用ガイドラインへの意見、政策提言等のとりまとめ
- セキュリティや運用方法の啓発・普及活動
  - 他の組織との連携
    - 共同開催
    - 講師派遣など
- 医療IT関連組織との意見交換

勉強会

毎月　第3金曜 10:30-12:00 ハイブリッドまたはオンラインで開催

2025-2026の内容

- 医療サイバーセキュリティ協議会（MedCSC)紹介
- 経済産業省　サイバーセキュリティ課の取り組み
- 保険医療福祉情報システム工業会(JAHIS)紹介
- CISSMED紹介
- JNSA全般紹介
- 医療機器業界団体（JEITA、医機連など）の活動について
- JNSA CISO支援WG
- 医療機関における情報セキュリティ人材の育成と配置に向けて(医療情報学会)
- 実際の病院ネットワークについて(京都大学医学部附属病院)
- サイバーインフラ事業者に求められる役割等に関するガイドラインの活用(経産省)

等

医療情報・IT関連団体との連携(セキュリティ)

政策提言など
- 健康医療情報が拓く未来会議

セキュリティ情報共有
- CISSMED

人材教育(CISO他)
- 医療情報学会
- ソフトウェア協会
- JNSA CISO支援WG

機器・サービス
- JNSA 医療IT WG

セキュリティプロセス
- 医療サイバーセキュリティ協議会

医療機器
- JEITA 医療機器委員会
- 日本医療機器産業連合会
- 日本画像医療システム工業会(JIRA)
- 保険医療福祉情報システム工業会(Jahis)

セキュリティ情報等を共有するために連携・協力体制を検討中
- 医療サイバーセキュリティ協議会
- CISSMED
- 保険医療福祉情報システム工業会(Jahis)
- 医療情報学会
- 医機連

等

医療情報・IT関連団体

- 健康医療情報が拓く未来会議
  - https://medical-mirai.com/
  - 「情報未来社会」の視点から、医療情報で実現すべきイノベーションについて政策提言を議論し、検証実験等を推進。
- CISSMED (Cyber Intelligence Sharing SIG for Medical)
  - https://www.cissmed.org/
  - 医療におけるサイバーセキュリティについて考える有志の集まり。医療機関においてセキュリティ業務に携わる者により構成される。
- 医機連（日本医療機器産業連合会）
  - https://www. jfmda.gr.jp/
  - 医療機器を製造・販売する事業者が作る団体の連合会。2021年6月現在の会員団体は20、傘下企業約4,300社。
- JAHIS（保健医療福祉情報システム工業会）
  - https://www.jahis.jp/
  - 保健・医療・福祉分野の情報システムや医療機器を扱う企業で構成される団体。電子カルテ情報などの標準化や品質向上を通じて、医療Tの発展と相互運用性の確保を目指して活動している。
- MedCSC（医療サイバーセキュリティ協議会）
  - https://medcsc.org/
  - 医療業界におけるサイバーリスクを憂慮する有志の集まり。医療分野のサイバーセキュリティ成熟度向上を使命とし、実践的なトレーニングや情報共有の場を提供している。
- JP-RISSA（情報処理安全確保支援士会）
  - https://www.jp-rissa.or.jp/
  - 情報処理安全確保支援士の集まり。会員のスキル向上を目指した勉強会等を運営。
- 日本医療情報学会
  - https://www.jami.jp/
  - 保険医療福祉情報に関する研究者及び実務担当者の交流の場となることを目指した団体。日本学術会議強力学術団体、日本医学会分科会。
- JIRA（日本画像医療システム工業会）
  - https://www.jira-net.or.jp/
  - 放射線機器を中心とする医療画像機器・関連システムを製造する事業者が作る工業会。
- JEITA（電子情報技術産業協会）
  - https://www.jeita.or.jp/japanese/about/overview/index.html
  - 電子機器産業、電子部品産業、ITソリューションサービス産業等に関わる事業者が作る団体。医療機器についてはヘルスケアインダストリ部会が担当。
- 大学病院医療情報・企画関連部長会
  - https://square.umin.ac.jp/johobuchokai/
  - 大学の医療情報・企画関連部門の長が集い、医療情報などに関わる諸問題を話し合う団体。

医療情報・IT関連の課題

- **地域格差**
  - ベンダー、Sierの対応状況に差がある
    - 理解不足
    - 人材不足(注力されていない、、、)
- **予算不足**
  - 情報通信は社会インフラ
    - 医療情報はITだけどOT的な側面を持っている
    - 社会インフラはコストをかけて対応　(鉄道、道路、電力など)
    - 医療分野や他のインフラとどうようなアプローチがきかない(基幹インフラとして、体制整備中)
- **新しい技術やシステムの情報が更新されない**
  - 20年近く前のネットワーク導入時のまま
    - 現在は使用が推奨されないセキュリティ対策機器が使われている
      - 攻撃ツールと同等(悪影響がある)であり、使用禁止すべき
    - VPNからZTNA、最近ではSASEを使うといった新しいセキュリティ対策が普及していかない
      - SASE(オンプレ併用型)にするとVPNの設定ミスやユーザ教育といった問題から解放される

医療情報・IT関連団体で連携して取り組んでいく

医療機関におけるサイバー脅威の現状

サイバー攻撃の増加と影響

医療機関へのサイバー攻撃は診療停止を引き起こし、患者の生命に深刻なリスクをもたらす

攻撃対象となる背景

高価値の患者情報と24時間稼働の医療体制により、医療機関は攻撃者に狙われやすい

システム脆弱性の課題

古いOSや医療機器の長期使用で脆弱性が生じ、更新やパッチ適用が困難である

サプライチェーン攻撃のリスク

外部委託先経由の侵入が増加し、医療機関全体での包括的なセキュリティ対策が必要

医療機関で求められる対策

強化されたセキュリティ対策
多要素認証や脆弱性管理により、医療機関の情報システムの安全性を高める

AIによる攻撃の高度化
AI技術の進展で攻撃が自動化・高速化し、迅速な対応が必要となる

経営層のリーダーシップ
経営層が主体的に関与し、組織体制と教育訓練を統合して推進していくことが大切

事業継続計画(BCP)
インシデント時の初動対応とオフラインバックアップで事業の継続を確保する

新しい技術やシステムの情報が更新されない

約20年前に整備されたIT・ネットワーク環境の経緯

電子カルテシステム導入
2000年代に紙カルテから電子カルテへの移行で業務効率化と情報共有を促進した

限定的なネットワーク設計
ネットワークやサイバーセキュリティは必要最低限の設計で、境界防御が中心だった

更新困難な医療IT環境
医療機器接続やサポート制約でOSやミドルウェアの更新が困難な状態が継続

サイバー脅威への構造的課題
20年前の設計思想が現代の高度なサイバー攻撃に対応困難な問題を生んでいる

老朽化した環境がもたらすリスク

フラットなネットワークのリスク
医療機関の分離されていないネットワークは、マルウェア感染が広がりやすく診療停止の危険性が高い

サポート切れOSの脆弱性
Windows 7やServer 2008などサポート切れOSの使用は医療機器のセキュリティリスクを増加させる

複雑化したネットワーク管理
長年の小規模改修によりネットワークが複雑化し、担当者不在の人的リスクも顕在化

攻撃手法類似技術は採用してはいけない！

- L2Blockというような名称でよばれている技術は未許可端末遮断のためARP Cache Poisoning/偽装ARPを利用する方式である
- ARP Poisoningは中間者攻撃や通信妨害で使われる代表的な攻撃技術
- 現在のセキュリティデザインの考え方では攻撃的手法による制御を避ける
- 多くの組織では認証・認可ベースの制御を優先すべき
- 監視やアクセス制御技術は最近のネットワーク機器は対応済みである

「攻撃ツールと同様の手法で端末を妨害する」のではなく、
認証・可視化・継続監視によるゼロトラストを採用する

医療IT WG リーダー

フォーティネットジャパン合同会社

新　善文　(あたらし　よしふみ)

yatarashi@fortinet.com