令和6年度 栃木県地域医療構想推進セミナー

サイバーセキュリティー対策の取組

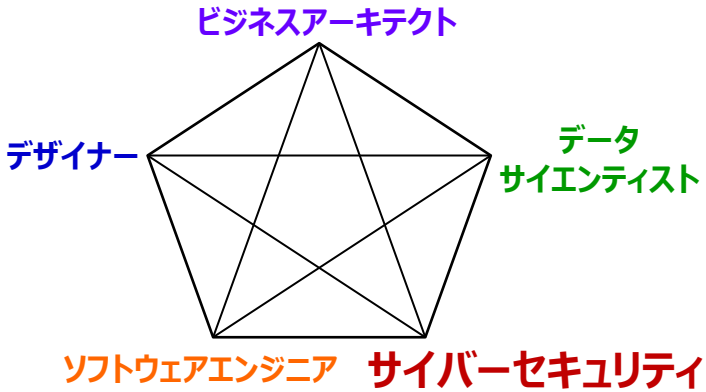
2025/3/21

足利銀行
法人コンサルティング部
寺井　義起

医療機関を取り巻くサイバー脅威

足利銀行

- **地域医療構想とDX**　Digital Transformation:データやデジタル技術を用いて、製品・サービス、ビジネスモデル、業務、組織を変革し競争力を高めること
  - **DXや地域の医療・介護の連携強化を通じ、限られたマンパワーで、より効率的な医療を実現**
- **DXにおいてサイバーセキュリティは必須分野**



サイバーセキュリティ ・・・ 業務を支えるデジタル環境における
サイバーセキュリティリスクの影響を抑制する対策を
担う人材(管理者およびエンジニア)

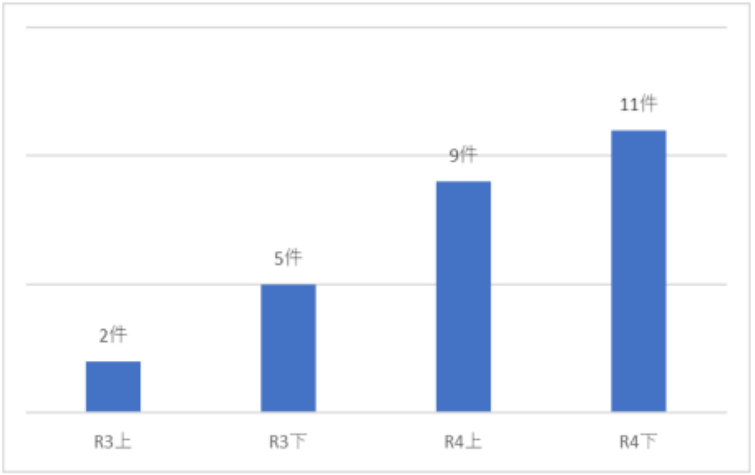
- **サイバーセキュリティと医療機関**
  - **患者等の機微な情報を大量に扱う ⇒ 攻撃者には高い価値があり、保護すべき情報**
  - **外部とデータのやり取りが増加 ⇒ 多様な侵入経路、拡散経路**
    - Web予約受付、オンライン資格確認
    - 医療メーカ,薬品会社,検査機関等多くの外部組織とのデータのやり取り
    - 電子カルテと医療用画像,問診,決済といったシステム連携、将来はAI支援診断、IoT連携の増加
  - **社会全体でIT人材不足 ⇒ セキュリティ体制構築が追いつかない**

ランサムウェア

足利銀行

- **ランサムウェアとは**
  - **情報セキュリティ 10大脅威2025[組織の脅威]のトップ** 出展:情報処理推進機構
  - Ransom(身代金)、Software(ソフトウェア)を組み合わせた造語
  - 8割以上は、データ暗号化だけでなく、窃取データを公開する二重恐喝 出展:警察庁
  - 復旧に1カ月以上、1千万円以上の費用を要した組織がそれぞれ約5割 出展:警察庁
- **医療機関とランサムウェア**
  - **医療関係を標的としたランサムウェアの被害が増加**
  - 電子カルテシステム等のデータが暗号化され、患者の受け入れが停止
  - 医療機関がサービス中断を避けるために身代金を支払う可能性が高いと考え、この分野を標的としている

感染した端末の画面　出展:情報処理推進機構



医療・福祉分野におけるランサムウェア被害件数
出展：警察庁

医療機関のランサムウェアの被害事例

足利銀行

① **どの医療機関でも起こりうるリスク。都市・地方、規模を問わず発生**
② **復旧まで2ヵ月余り要した例もあり、患者や業務に多大な影響**
③ **対策していた場合は短期に復旧できる**

事案	問題事象 ①	病院業務への影響
徳島県 120床	•VPN機器の脆弱性により侵入 •電子カルテシステムが暗号化	•診療や請求の停止・制限 2021/10/31～2022/1/4 ②
大阪府 865床	•給食業者のVPN機器経由で連携システムから侵入 •電子カルテを含めた総合情報システムが暗号化	•救急診療、外来診療、手術の停止・制限 2022/10/31～2023/1/11
徳島県 90床	•VPN機器の脆弱性により過去に暴露されたパスワードにより侵入 •電子カルテシステムが暗号化	•新規外来診察の停止 2022/6/19～2022/6/22 ③ **•同県の先行例から対策を強化していたバックアップも取っていたため短期復旧**

被害事例でみる脆弱性と被害拡大

足利銀行

- 「必要性を感じていない」「対策にコストをかけられない」という事業者が多いが、**基本的なセキュリティの不備を突かれている**

大阪 情報セキュリティインシデント調査報告書 概要　2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪[redacted]にてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順　（調査報告書11～12頁）

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入（漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある）。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

◆被害状況　（調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテを含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。PC端末（院内に約2,200台）も不正アクセスの痕跡あり。 ⇒全てのサーバ、端末をクリーンインストール 基幹システムサーバ再稼働に43日間、部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数：558人（前年同月比33.3%）、延入院患者数：10,191人（前年同月比52.9%） 初診患者数　：465人（前年同月比17.9%）、延外来患者数：15,744人（前年同月比61.6%）
3	被害額	現在精査中　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

出展：大阪府の病院の事例の調査報告書

業者の**VPN装置の脆弱性**を経由し感染

- **ユーザ全てに管理者権限**
- **推定が容易なパスワード**
- **サーバーと端末に共通のパスワード**

電子カルテにウイルス対策ソフト未導入

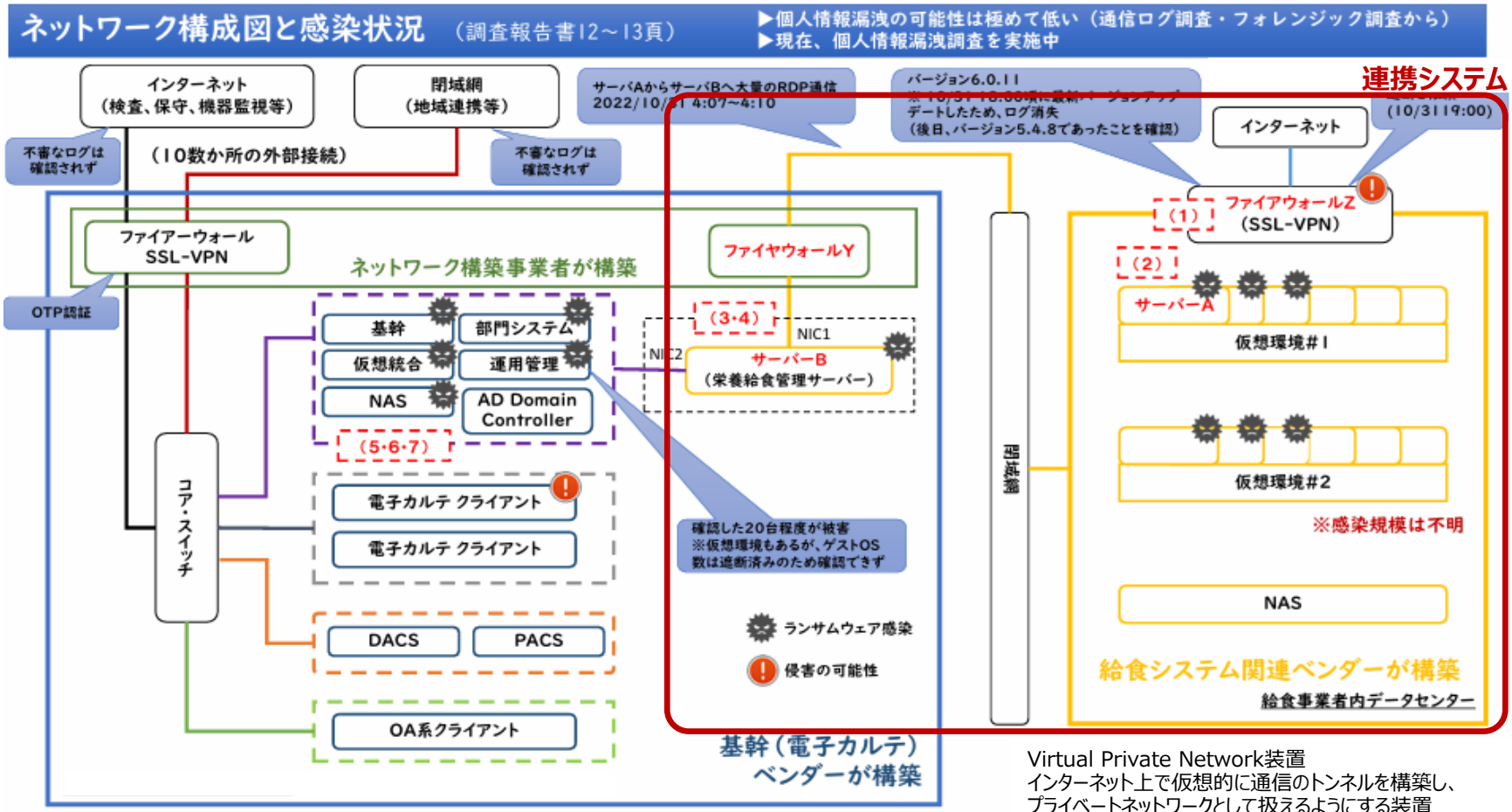
甚大な被害

バックアップが正しく取得できているか確認できていなかった

ご参考：被害事例のシステム構成

足利銀行

- **インターネット接続する業者の連携システムから感染拡大**
  ⇒ 閉域網と考えてはいけない。サプライチェーンに影響ある問題



出展：大阪府の病院の事例の調査報告書

Virtual Private Network装置
インターネット上で仮想的に通信のトンネルを構築し、プライベートネットワークとして扱えるようにする装置

被害を受けない・最低限に抑えるために

足利銀行

- **2023/4 医療法施行規則改正により医療機関のサイバーセキュリティ対策が義務化**
  - 医療情報システムの安全管理に関するガイドライン
  - 優先的に取り組むべき事項がチェックリスト化され、立入検査時に確認される

- **「医療機関におけるサイバーセキュリティ対策チェックリスト」に基本的対策がわかり易く表現**

  ⇒ **厚生労働省から、令和6年度中に、全項目で「はい」にマルが付くべく取り組むよう指導**
  医療機関におかれましては、担当者やベンダ任せにせず、チェックリストを是非ご確認下さい

厚生労働省のチェックリストのURL(PDFファイル)

体制構築

- **責任者の設定**

脅威の低減

- **パスワードを強固にし、共通化しない**
- **業務に応じアカウントに最低限の権限を与え、共用しない、棚卸しして不要なものは削除**
- **ファイアウォールやルータの通信、サーバやPCで起動するプログラムを最低限にする**
- **セキュリティパッチを適用**
- **アクセスログの監視**

発生への備え

- **バックアップ取得**　バックアップ時以外のオフライン化、接続の限定や上書き制限も検討下さい
- **インシデント発生時の対応や連絡体制、復旧手順の策定と確認**

弊行のご支援

足利銀行

弊行では、経営相談業務の一環で、
お客さまのセキュリティ対策の強化を支えるために、ご支援を用意しております
ご相談は、最寄りの営業店にお問い合わせ下さい

- **当行によるデジタル化コンサルティング：リスク評価・対策策定・対策実行の伴走支援**
  - **システムセキュリティ対策支援サービス**
    - プランニング(リスク評価・対策策定)から対策実行(導入・フォローアップ)まで一貫支援
    - プランニング(リスク評価・対策策定)のスポット支援

- **パートナー企業のご紹介**
  - セキュリティ対策製品の導入(ファイアウォール、統合脅威管理、ウィルス対策、IT資産管理、バックアップ、攻撃検知・遮断、誤送信対策、文書の暗号化等)