令和7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】

岡山県精神科医療センターの報告書を読み解く

2025年10月30日
一般社団法人ソフトウェア協会

目的

- **「ランサムウェア事案調査報告書」の解説**
  - 1. はじめに　　ランサムウェア事案に対応して (p1)
    - 2. 用語解説（この項は省略）
    - 3. 地方独立行政法人岡山県精神科医療センターについて（この項は省略）
  - 4. 病院情報システム（HIS）概要 (p8)
  - 5. 概要編 (p12～p13)
    事案の時系列 当日 (p17)

- **攻撃ベクトルの理解**
  - 初期侵入、水平展開、暗号化の手法の Fault Tree 分析

報告書 はじめに p1

正常性バイアス

・山田理事長のあいさつ

実は前年の暮れ頃から5月にかけての間に**数回、AD*サーバーの不調が発生**したことがありました。

～略～

当時、執拗に調査を依頼しておけば良かったのではないかという反省に加えて、**何度かの軽微な不調と復旧が繰り返され**たことから、「オオカミ少年」に慣れた村人のような**正常性バイアスを持ってしまった**ことも悔やまれます。

*Active Directory の略。Windows環境におけるセキュリティと資産を統合的に管理するための仕組み。ユーザーやコンピュータの権限を一元的に管理できるため、「誰が」「どのPCで」「何をできるか」を集中して制御できる。たとえば、ファイルサーバーのアクセス権設定、パスワードの変更・再設定、退職者アカウントの無効化など、さまざまなセキュリティ管理を ADサーバー（ドメインコントローラとも呼ばれる）で統一的に実施できる。

何がおきていたのか？

- **5.6 事案の時系列 (p17)**
  - **2023/11/30**
    Active Directoryサーバーが原因不明の障害、バックアップより復旧
  - **2023/12/8**
    同様の事象が発生、バックアップより復旧

- **疑問点**
  - 僅か1週間程度で、連続して Active Directory サーバーに障害が発生するだろうか？
  - 可動部分の少ないコンピュータにおいて、動作不良を引き起こす原因は何か？

正常性バイアスについて

■ 障害発生時の切り分けの考え方

段階	目的	主な担当	主な手法
一次切り分け	障害の「発生範囲」を特定する（どこが悪いか）	運用担当・ヘルプデスクによる一次保守	Ping・サービス確認・ログイン確認など基本チェック
二次切り分け	障害の「原因」を特定する（なぜ悪いか）	専門技術者・ベンダによる二次保守	詳細ログ解析・設定・通信・ハード診断など技術的分析

■ 対策

- 何らかの障害が発生した場合は**「1次切り分け」**でサイバー攻撃を排除せずに調査を実施し、**「正常性バイアスを排除」**する。
  - ランサムウェアの特徴である「大量の暗号化されたファイルの拡張子」がないかを確認する。
  - Windows アプリケーションログ、システムログ、セキュリティログの解析を必ず行う。

障害発生時の分類と報告に関する考え方

■ 障害分類

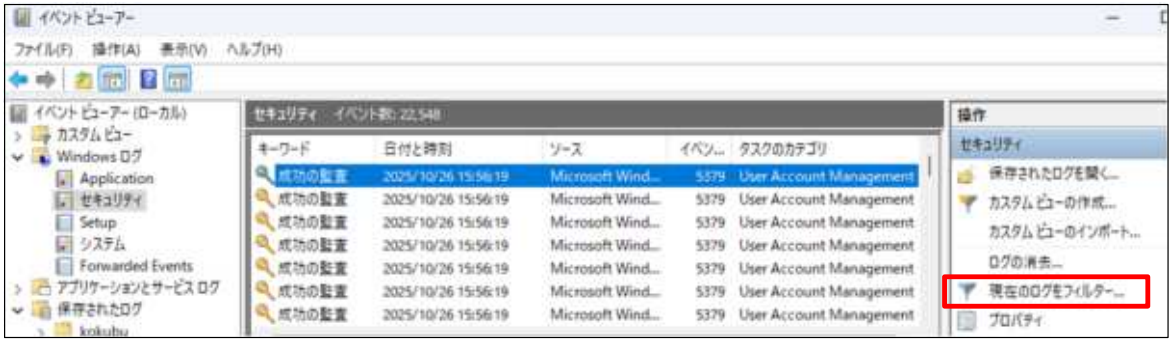
分類	内容
ハードウェア障害	電源の故障、ディスクの故障、ホットスワップ作業のミス
ソフトウェア障害	OSクラッシュ、アプリケーションエラー、時刻同期の不良、サイト間のレプリケーション（同期）の失敗、Group Policy 設定ミス
ネットワーク障害	スイッチ・ルーターの故障、DNS の設定ミス、ネットワークの設定ミス
リソース不足	メモリ不足、ディスク容量不足、CPU 高負荷
サイバー攻撃	ランサムウェアによる暗号化、ウイルス感染、いたずらによるシステム破壊

■ 報告

- 1次切り分け、2次切り分けは口頭説明だけで終わらず、必ず、メールで説明内容を送信するように要求する。
- 最終報告書は PDF 等での提出を求め、証跡管理を行う。

Windows ログの分析（参考資料）

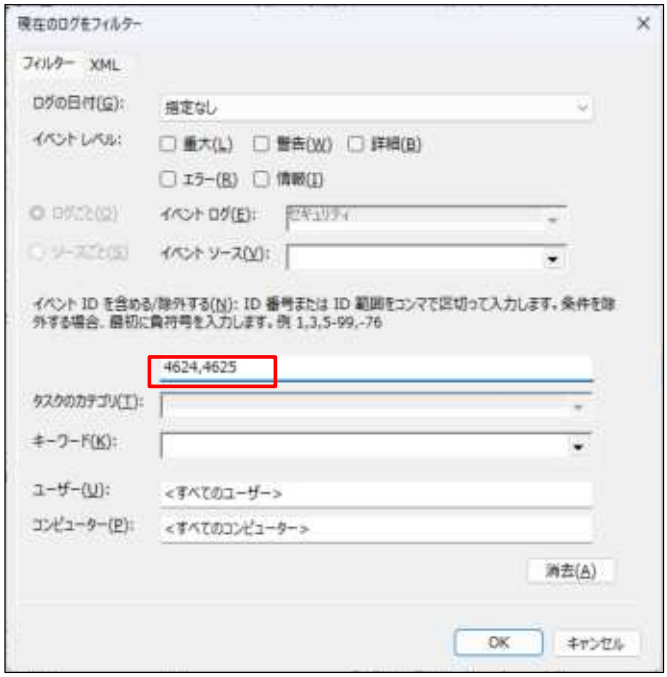
- **対象**
  - 障害を発生したサーバー、端末、ドメインコントローラー
- **Security Log**
  - C:¥Windows¥System32¥winevt¥Logs¥Security.evtx
  - ダブルクリックし、イベントビューワーを立ち上げる



  - 資料：調査すべきイベント、ログオンタイプの確認

調査すべきイベント（参考資料）

- **対象イベント**
  - 4624：ログオン成功
  - 4625：ログオン失敗
- **着目点**
  - 4624：深夜に Administrator や、Administrators に所属するアカウントがログオンに成功している
    - タスクスケジューラー、バッチ処理、ファイルコピーなど、正常な場合もある
  - 4625：短時間に大量のログオン失敗が発生している
    - ファイル共有のPW設定ミスなどで大量に発生する場合もある



ログオンタイプの確認（参考資料）

ログオンタイプ		内容	備考
1	システム アカウント	システムアカウントによって生成されるセッション。バックグラウンドサービスやシステムタスクが使用する。	
2	対話型	インタラクティブにコンピュータに直接ログオンする。	あり得ない時間帯で人が操作しているか。
3	ネットワーク	ファイル共有やプリンタ共有、リモートサービス。	外部IPや不自然なホスト→ホストの組合せ、サービスアカウントでの頻繁なNetworkログオンは要警戒
4	バッチ	バッチ処理のためのログオン、スクリプトやバッチファイルが実行。	
5	サービス	Windows サービスやバックグラウンドサービスが開始する際のログオン。	
6	プロキシ	サービスやアプリケーションがユーザーの代理としてログオンする場合。	
7	ロックの解除	ワークステーションのロックを解除した場合。	深夜に大量発生している等は、不正利用の可能性。
8	ネットワーク クリアテキスト	ユーザーがネットワークを通じて認証情報を平文で送信する場合。	通常はありえない。未知のFTP、HTTP、NTLM等は攻撃の可能性。
9	新しい資格情報	既存のログオンセッションの認証情報を更新するために使用される。	通常はありえない。サービス、バッチログオンで新規設定がなければ、攻撃の可能性。
10	リモートデスクトップ	リモートデスクトップやterminalサービスを介してリモートログオンする場合。	未知のソースIP・通常業務時間外・同一ユーザの短時間連続ログオン失敗→成功などを検証。
11	キャッシュ ログオン	ドメインコントローラーにアクセスできない場合、ローカルのキャッシュされた資格情報を使用する場合。	

監視するイベント（参考資料）

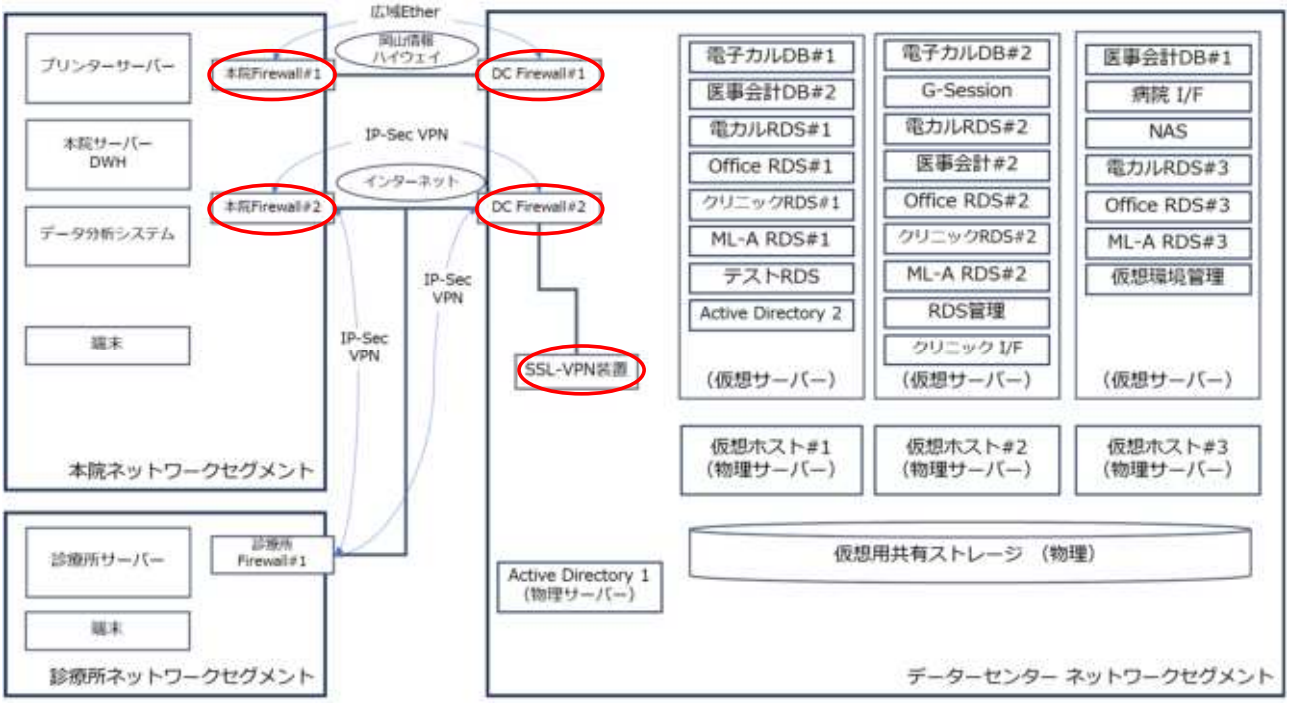
- **JPCERT/CC 侵入型ランサムウェア攻撃発生時に残るWindowsイベントログの調査**
  - https://blogs.jpcert.or.jp/ja/2024/09/windows.html

ランサムウェア	主なイベント ID	ログ種別	記録の特徴
Conti / Akira / Lockbit3.0 / HelloKitty / Abysslocker 等	10000, 10001	アプリケーションログ	Restart Managerの短時間大量発生。ファイル暗号化時に記録。
Phobos / 8base / Elbie	612, 524, 753	Setupログ	シャドーコピー削除やバックアップ関連イベント。感染時に発生。
Midas / Axxes	7040	システムログ	サービス設定変更。感染拡大のためのネットワーク機能や、重要なサービスの停止等。
BadRabbit	7045	システムログ	永続化、特権昇格、ウイルス対策ソフトの監視を逃れるため等の、新しいサービスがシステムにインストールされたことを示すもの。
Bisamware	1040, 1042	アプリケーションログ	Windows Installer を使い、ウイルスのインストールや、ウイルス対策ソフトのアンインストールを示すもの。
Shade / GandCrab / AKO / avoslocker / BLACKBASTA / VICE SOCIETY	13, 10016	システムログ	13は、Windows のバックアップであるボリュームシャドーコピー削除時に発生。10016はCOMアクセス許可エラー（権限不足）。連続で13と10016が発生した場合は、攻撃の可能性が高い。

4. 病院情報システム（HIS）概要

ネットワーク全体構成

病院情報システムネットワーク全体構成



5 概要 (p12～p19)

5.1 インシデント概要 (p12)

- 2024年5月19日16:00頃、病院の電子カルテが使用できなくなり、同日より電子カルテベンダーであるA社が調査を開始、翌20日6:15頃、バックアップファイルから不審な拡張子のファイルを発見、ランサムウェアに感染しプログラム及びデーターが暗号化されていることが確認された。

- 初期侵入が確認できたのは2024年5月13日02:41（サーバーのフォレンジック調査により後日判明）で、その後、病院内のネットワークのスキャン、バックアップデーターの探索と破壊、Active Directoryに登録されたサーバー・端末ユーザー、コンピューター等の情報の窃取、ウイルス対策ソフトの停止と削除等を周到に実施した上で、5月19日13:10頃から電子カルテシステム等の暗号化が行われた。

5月13日～5月20日の攻撃者の行動

初期侵入
5/13 02:41

暗号化開始
5/19 13:10～

電子カルテ停止
5/19 16:00

脅迫状発見
5/20 6:15

院内ネットワークのスキャン
バックアップデーターの探索と破壊
情報の窃取
ウイルス対策ソフトの停止と削除

初期侵入における留意点

■ **初期侵入後は、調査に時間を費やし身代金の獲得チャンスを増やす行動をとる**
- バックアップの破壊　→ 復旧時間がかかる
- データーの窃取を行う　→ 2重脅迫を行う
- ネットワークの探索　→ 大量のコンピューターを暗号化する

■ **暗号化開始から電子カルテ停止までは3時間**
- 仮想ホストサーバーを暗号化すれば、すべての仮想サーバーが暗号化されるが、仮想ホストサーバーの暗号化にかかる時間は1分程度
- 3時間かかったのは、仮想用共有ストレージ（大容量データー）の暗号化を優先したと考えられる
- 暗号化された場合、大量の同じ拡張子が表示される

■ **脅迫状の表示を抑制するグループの存在**
- 発見を遅らせ、暗号化を継続する
  - C:¥Windows¥Users 以下のすべてのユーザーの Desktop を調査する

暗号化ファイルの特徴

■ **拡張子が変更される**
- 同じ拡張子に変更される
- アプリケーションやデーターを暗号化するため
  C:¥Program Files
  C:¥Users¥
  等を検索する

■ 国内一般企業での暗号化されたファイル

GUID-F9AEB18B-11B6-4243-B835-A0A5CB8750FC.html.destroy26	24,669 (25 KB)
GUID-F4406B9A-9A36-4864-8796-3DD5709CDF73.html.destroy26	22,845 (23 KB)
GUID-F3DB2634-7024-4C89-995F-2F33A8FAC28F.html.destroy26	33,518 (33 KB)
GUID-F35FE0AD-6E06-41EC-ACA4-843274BEFBCD.html.destroy26	28,069 (28 KB)
GUID-EF3CCB67-A87F-46EF-B4F2-02712C1F87B3.html.destroy26	25,633 (26 KB)
GUID-EE35A2B9-31AE-44F9-8C5A-8A7C2FB08866.html.destroy26	27,083 (27 KB)
GUID-ED00591F-F502-4C6C-9A44-7AA3BF00AB19.html.destroy26	23,334 (23 KB)
GUID-EA0C12B4-794B-4765-AD85-879A18C663D9.html.destroy26	21,850 (22 KB)
GUID-E983C04E-0503-4C7F-9B02-3CF0DE8B39B2.html.destroy26	25,040 (25 KB)
GUID-E2612963-C020-4680-B3D2-D500C6136145.html.destroy26	23,599 (24 KB)
GUID-E1E7B08F-80B4-4CE0-986B-044FDA2F0F4B.html.destroy26	23,155 (23 KB)
GUID-E1E73018-2794-4213-A2A5-35A660A2B178.html.destroy26	29,177 (29 KB)
GUID-E03C6631-3103-47B5-BFF3-83D550DFE278.html.destroy26	27,888 (28 KB)
GUID-DD22168B2-4AF7-41BC-84B4-0D0E3733B592.html.destroy26	23,043 (23 KB)
GUID-D9F83041-DBD6-4AF6-8D8C-1D73E6DEFCA8.html.destroy26	20,803 (21 KB)
GUID-D691AA98-D72D-472C-B389-AD2997DC7945.html.destroy26	29,872 (30 KB)
GUID-D5DE8444-0A79-43A0-A4BA-A73438A0505E.html.destroy26	29,439 (29 KB)

インシデントかも（資料例）

こんな表示をみつけたら
24時間365日 問わず、事務局総務当直
内線 xxx に連絡してください！
PC をネットワークから切り離して下さい。

インシデントかも（資料例）

こんな表示をみつけたら
24時間365日問わず、事務局総務当直
内線 xxx に連絡してください！
PC をネットワークから切り離して下さい。

インシデントかも（資料例）

前のページのような表示を
みかけたら、躊躇せず、LAN
ケーブルを抜線して下さい。

ツメを押しながら引き抜くとLANケーブルを抜線できます。

インシデントかも（資料例）

前のページのような表示をみかけたら、躊躇せず、Wi-Fi を停止して下さい。

初期侵入対策

■ **定期的に、不審な行動がないかログを調査する**

- 夜間や通常、あり得ない時間帯に管理者アカウントでログオンをしていないか？
- 新たにアカウントやセキュリティグループが作成されていないか？

■ **オフラインバックアップの取得**

- バックアップの破壊に備え、オフラインバックアップを必ず取得する

■ **Office 文書等には長い PW を設定する**

- 情報が窃取されても、情報公開が困難になる

5.1 インシデント概要 (p12 続き)

■ 被害は、電子カルテシステム等の仮想サーバー23台と仮想用共有ストレージ1台、仮想基盤用物理サーバー3台、その他の物理サーバー6台、HIS系端末244台の暗号化によるシステム稼働障害と仮想用共有ストレージのデーター全喪失である。

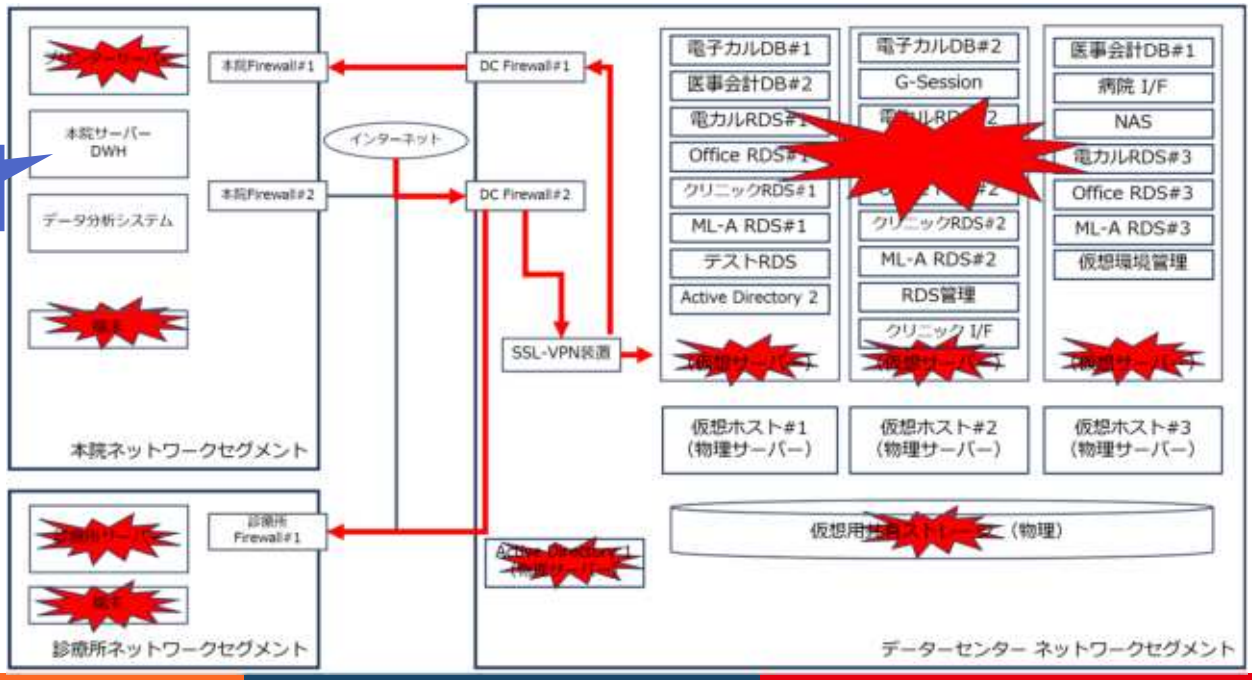
仮想用共有ストレージのデーター全喪失とは

■ **データー全喪失＝すべての診療録を失った状態**

- 医師法第24条および歯科医師法第23条 違反 50万円以下の罰金
- 保険医療機関及び保険医療養担当規則第9条 違反
- 法律に基づき、罰金以上の刑に処せられた医師は、厚生労働大臣による行政処分（戒告、医業の停止、免許の取消し）の対象となる可能性がある

被害範囲

DWH* は
被害を免れた



*DWH（Data Warehouse）とは、組織の中にある さまざまなシステムのデータを集約して、分析しやすくするためのサーバー。

5.1 インシデント概要 (p13)

- 病院内のサーバーで発見されたランサムウェアは、Microsoft Defender ウイルス対策や、多くのウイルス対策ソフトで検出、検疫が可能なものであった。
- 攻撃犯 X は手動で、管理者権限によりウイルス対策ソフトの設定を変更、もしくはプログラムの削除等を行った痕跡が発見された。

ウイルス対策ソフトの効果

■ ランサムウェアはウイルス対策ソフトで駆除可能

- ウイルス対策ソフトのサービスを停止させない環境づくりが最重要
  - ① ユーザーに管理者権限を与えず、標準ユーザーで運用する
  - ② ウイルス対策ソフトで「改ざん防止」「セルフ・プロテクション」「不正改造防止」「センサー保護」などのサービス停止を防止する機能を有効化する

※「セーフモード」で起動されると改ざん防止機能が無効化されるので、
ウイルス対策ソフトが万能ではないことに留意する
標準ユーザー運用との組み合わせが重要

■ 復旧の際は、複数のウイルス対策ソフトでチェックを実施する

- 最新のエンジンと、最新のパターンに更新することが重要

5.1 インシデント概要 (p13 続き)

■ 侵入の原因は複数が考えられるが、保守用VPN装置の脆弱性の放置、推測可能なID/パスワードの使用が考えられ、水平展開及び暗号化の原因は、推測可能なID/パスワードが使いまわされ、病院内のコンピューターにすべて共通に設定されていたことに加え、一般ユーザーにも管理者権限を付与していたことによるウイルス対策ソフトの設定変更、停止と考えられる。

■ また、保守用VPN装置への接続元IPアドレス制限がなく、インターネット上から誰でも攻撃が可能であった。多くは、厚労省ガイドラインの遵守で容易に防げたものである。本件事案の原因は、病院及び電子カルテシステムを構築したA社の同ガイドラインの理解不足、過去のインシデント事例の軽視、「閉域網過信」によるセキュリティ意識の欠如に起因するものである。

インシデント概要のポイント

■ **VPN を侵入口とさせない**
- 脆弱性の修正、2要素認証の使用、接続元 IP アドレス制限の実施

■ **推測困難な管理者 PW の使用、もしくは多要素認証の使用**
- 推測可能な PW の使用せず、長いパスフレーズを使用する
- PW を使わない2要素認証：スマートカードログオンを使用する

■ **管理者権限の限定的使用**
- ユーザーに管理者権限を付与すると、ウイルス対策ソフトの停止、設定の変更が可能になる

■ **Windows の脆弱性管理**
- 標準ユーザーであっても、特権昇格の脆弱性があれば悪用される

ここまでのまとめ

■ **電子カルテベンダーとともに「厚生労働省安全管理ガイドライン」の遵守状況を確認する**
- **最優先事項**
  - VPN 装置の脆弱性対策を実施する
  - 1週間に一度は、不審な行動がないかログを調査する
  - ウイルス対策ソフトの「改ざん防止」を設定する
  - オフラインバックアップを取得する
  - Windows の脆弱性管理を実施する
- **システム更新時の優先事項**
  - ユーザーに管理者権限を与えず標準ユーザーで運用する
  - VPN の脆弱性の修正、2要素認証の使用、接続元 IP アドレス制限の実施
- **情報漏洩対策**
  - 可能な限り Office 文書等には長い PW を設定する

復旧経緯 (p13)

5.2 復旧経緯（p13)

- インシデントが発覚した5月20日以降、病院は対策本部を設置し、病院主要メンバー数十人で医療継続のための定例会議を、当初は1日3回実施、6月8日から7月19日までは1日2回実施した。
- また、システム復旧の進捗管理のため、理事長、院長、病院幹部、情報システム担当者とA社との進捗連絡会議を1日2回開催し、7月20日から11月末までは1日1回、12月以降は週に1回、現在に至るまで継続している。

医療継続とシステム復旧

■ インシデント発生時の課題

- グループウェアが HIS 系で構築されていたため、情報伝達が困難となった
  - 個人のスマートフォンなどを臨時で活用することを平時に検討しておく
  - この際、個人情報、患者情報は取り扱わない等、取り決めと教育が必須

■ 会議での留意事項

- 極端な人手不足、リソース不足が発生するため、幹部が優先順位の決定し、要員、リソースの調整を素早く意思決定できるようにする
  - 朝　　前日の残課題と当日の予定、計画、目標を報告する
  - 昼　　午前中の進捗の報告、課題・阻害要因を報告し、調整する
  - 夕　　当日の進捗の確認、課題・阻害要因を報告し、調整する
- 長時間労働が発生するため、メンタル・体調維持に十分留意する

5.2 復旧経緯（p13 続き）

■ 病院とA社はオフライン・バックアップの取得に関する契約を締結済みであったが、インシデント発生直後にオフライン・バックアップを確認したところ、オフライン・バックアップが正しく取得されておらず、オフライン・バックアップからの復旧は不可能であることが判明した。

バックアップについて

■ **不完全なオフライン・バックアップ**
- オフライン・バックアップの差分は存在したが、フルバックアップが存在しておらず、復旧ができなかった

■ **警察庁の調査では、バックアップから復旧できたのは21%***
- 取得していたバックアップから復元を試みた57件の回答のうち、バックアップから被害直前の水準まで復旧できなかったものは45件で79%、復旧できたのは21%だけ

■ **バックアップは、システム構築時に必ず復旧テストを実施する**
- 復旧ができないと、法律違反となるため、確実なバックアップ→復旧の確認が必須
- 誰でも実施可能な詳細な手順書の作成を行う（属人化しないように留意する）
- 手順に沿った復旧の確認を病院関係者とベンダー合同で実施する

■ **バックアップの月次監査**
- フルバックアップ、差分、増分の状況を月次でチェックする

* 出典：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

5.2 復旧経緯（p13 続き）

■ そのため、暗号化を免れた医療情報DWHサーバーから、電子カルテのデーターを取り出し復旧することとし、5月21日に仮復旧用の中古サーバーを手配、5月24日からDWHからデーターを取り出し、6月1日に中古サーバーで電子カルテシステムの仮復旧を行った。その後、6月20日に電子カルテ用新サーバーを入手し、７月4日に電子カルテを復旧した。8月17日にサーバーストレージの入れ替えを行い、インシデント発生から90日を経て病院情報システムの完全復旧を果たした。

電子カルテサーバーの調達

■ 電子カルテサーバーと仮想ストレージの RAID* 情報が破壊

- 再起動の影響、もしくは実際の攻撃のいずれかによって、ハードディスクの RAID 情報が破壊され、システムの起動が不可能になり、OS の再インストールすら不可能な状態になった
- このため、ディスク復旧業者にサーバーと仮想ストレージの復旧を依頼
- 参照用サーバーの緊急調達を行わざるを得なくなった

■ サーバーの調達に時間がかかる状況

- 現在、AI ブームの影響により、サーバーの調達期間が長くなる傾向にある
  - 小型、中型サーバー：　3週間～1か月程度
  - 大型サーバー：　1.5か月～3ヵ月以上

*RAID（Redundant Array of Independent Disks）：複数の物理ディスクをまとめて1つの論理ドライブとして扱うことで、信頼性と性能を向上させる技術。

サーバー調達と DWH からの復旧

■ サーバー調達対策

- クラウド上の仮想マシンの活用を検討する
  - 既設の回線を使用し、IPsec 等の VPN で接続した場合の帯域が確保できるか、平時に、電子カルテベンダーと検討をしておく

■ 暗号化されなかった医療情報 DWH サーバー

- 原因は不明だが、奇跡的に難を免れた
- DWH には、電子カルテの情報がすべて入っており、そこから復旧が可能となった
- 大阪急性期・総合医療センターでも、インシデント直後は、DACS（診療記録文書統合管理システム（Document Archiving and Communication System）による参照ができたため、医療継続が可能であった
- システム更新時には、インシデントに備えた参照系システムを検討する

ベンダーとの協調のポイント

■ **復旧定例会議での原因究明**

- 複数の課題が積み重なりインシデントに至っているため、電子カルテベンダー、ネットワークベンダー、部門・診療科システムベンダー、医療機器ベンダーへの原因調査の指揮命令は病院が主体となって実施する
- ベンダー任せの場合、責任回避や擦り合いが発生する恐れ

■ **原因究明に基づく復旧方針、再発防止策の策定**

- あらゆる機器の ID/PW は漏洩している可能性があるため、長いパスフレーズに変更する
- 原因が不明確なまま復旧すると、再感染、再侵入を招く恐れが高くなるため、侵入経路、水平展開の手法については、必ず特定した上で、復旧にあたる
- 必ず、複数のオプションや方法を求め、最善の方法・方式を選択できるように、ベンダーに働きかける
- 多角的に「再侵入の防止策」、「情報漏洩の防止策」を病院自らが評価し、復旧後の運用に支障がでないよう再発防止策を確定する

よくあるベンダーの対応

■ **営業所が固定 IP アドレスでないので接続元 IP アドレス制限ができない**

- 固定 IP アドレスサービスを利用するよう要請する

■ **VPN 装置の脆弱性アップデートがサポート終了でできない**

- 厚労省ガイドライン違反になるので、至急、機器更新を要請する
- 更新までは利用停止、もしくは、都度接続とする

■ **VPN 装置の2要素認証ができない（機能がない）**

- 可能な限り長い PW の設定を要請する
- 厚生労働省安全管理ガイドラインでもR9年度までに2要素認証が必須となる
- 次回、調達時には2要素認証が対応可能なベンダーを選定する

■ **医療情報システムで個別に管理者 PW を設定すると緊急時に対応できない**

- PW の設定ルールを定め、ルールを知っている人なら対応でき、推測困難なパスフレーズを採用する
  - 病院名略称+コンピュータ名+キーワード
  - OGMC#SV0011#SecureString

復旧対応の実態（p17）

電子カルテベンダーとの連携・協調

5.6 事案の時系列（p17）

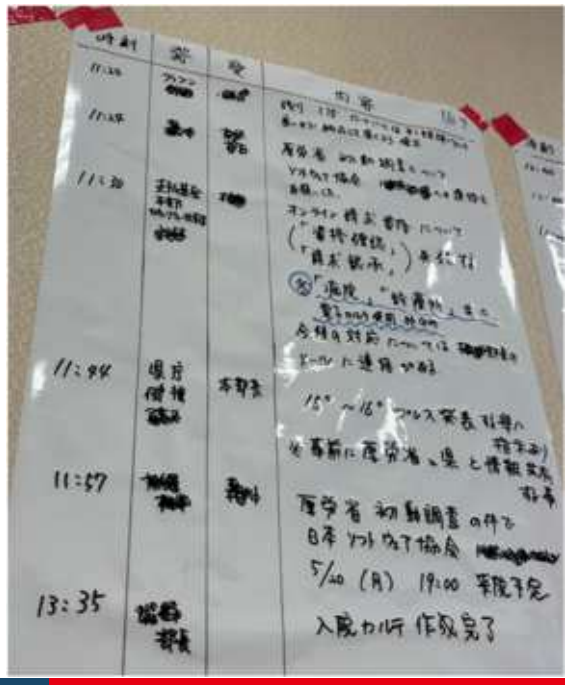
日付	時刻	内容
5/20	06:15頃	バックアップファイルから不審な拡張子を発見、ランサムウェアであることを確認。
	07:00頃	病院幹部が病院に集結。対策本部会議（第1回）で、本日からの診療は、入院、外来とも紙カルテを使用して継続することを決定。
	07:40頃	岡山県、岡山市、岡山県警察本部、厚生労働省に連絡。
	08:15頃	病院内に対策本部を設置、クロノロジー*の取得を開始。
	09:58頃	厚生労働省に追加報告した際に、初動対応支援を打診され支援を依頼。
	10:30頃	初動対応チームと現状を共有、遮断指示やベンダーからの報告を要請される。
	11:10頃	厚生労働省より、内閣サイバーセキュリティセンターへの連絡及び支払基金のオンライン接続の停止について代理で対応する旨連絡。
	11:20頃	紙カルテ運用リングファイル300個を発注。
	11:30頃	電子カルテシステムベンダーから初動対応チームに入電。完全なネットワーク遮断、データーやログ等の現環境の保全、システム一覧、ネットワーク構成図の準備、VPN装置のアドレス等の取得を依頼。

*クロノロジー：災害発生時に情報を時系列に記録・整理する手法。
出来事や情報を、時刻、発信元、発信先と共に記録する。

事案認識時点でのアクション

■ **幹部会議による診療継続の意思決定**
- 紙カルテ運用に切り替え、入院、外来の継続

■ **クロノロジーの取得開始**
- 専任記録員を設置し、すべての事象・情報を一か所に時系列でとりまとめる
- 「時刻」「発信者」「受信者」「内容」 をホワイトボード、ホワイトボードシートに記入
- 情報の整理整頓と情報共有・意思決定を支援する



初動のアクション

■ **厚生労働省初動対応チームと現状を共有、遮断指示やベンダーからの報告**
- 有事の際は、すべての LAN 抜線、無線 LAN 停波を速やかに実施する

① インターネット接続回線
② コアスイッチ
③ フロアスイッチ、Wi-Fi アクセスポイント
④ サーバー、PC

■ **禁止事項**
- サーバー、PC 等は電源遮断、再起動は絶対にしない
  - ランサムウェアが再起動し、多重暗号化で復旧が困難になる可能性
- ウイルス対策ソフトのスキャンを実施しない
  - スキャン開始とともにウイルスが自身を削除し、ウイルス確保が難しくなる可能性
- 保全を優先し、解析結果をもって復旧方針を定める
  - ウイルス感染しない環境で解析を行い、原因を究明する

保全とは

■ 保全

- 事件・事故・不正などの調査対象となるデジタル証拠を、元の状態を損なわずに、確実に取得・保存すること

目的	内容
改ざん防止	調査者やシステムによる意図しない変更を防ぐ
証拠能力の確保	裁判などで「信頼できる証拠」と認められるようにする
再現性の確保	他の専門家が同じデータから同じ結論を得られるようにする
連鎖証拠性	誰がいつ、どのように証拠を扱ったかを記録し、正当性を保証する

■ 取得方法

- ログなどが上書きされるため、最優先で保全を実施する
- 専門業者、警察に依頼し、業界標準の E01形式（EnCase Evidence File、拡張子 .E01）で取得する
  - FTK Imager 等で HDD、SSD全体のイメージをビット単位で取得、メモリの情報を取得
  - 取得には対象となるディスクサイズ以上の HDD が必要
- 日本ネットワークセキュリティ協会 サイバーインシデント緊急対応企業一覧
  - https://www.jnsa.org/emergency_response/
  - 与信等の関係で、緊急対応してくれない場合があるため、事前に相談を行っておく

ステークホルダーへの報告

■ 厚生労働省より、国家サイバー統括室*への連絡、及び支払基金のオンライン接続の停止について代理で対応する旨連絡

- 支払基金のオンライン接続は、完全復旧まで行えない、この間、支払いが止まることに留意する
- 再接続の際は、復旧対策の内容報告と第三者の確認を求められる

■ 個人情報保護委員会へのランサムウェア事案の報告

- https://www.ppc.go.jp/personalinfo/legal/leakAction/#ransome
- 発覚日から3～5日以内：　第1報
- 発覚日から60日以内：　確報

■ ステークホルダーの連絡先の整備

- 所轄警察、救急本部、医師会、地域連携、自治体、ステークホルダー等の連絡先の整備（電話番号、担当者名、メールアドレス等）と半期に一度の更新を実施する

*インシデント発生時点の呼称は「内閣サイバーセキュリティセンター」

紙カルテ運用への切り替え

■ **紙カルテ運用リングファイル300個を発注。**
- 紙カルテ運用に切り替えると、大量の用紙と複写が必要となる
- 投薬の場合：紙カルテ用、薬局用、医事会計用、病棟送達用の4枚複写が必要
  - 各部門・診療科での平時のシミュレーションが重要

■ **手書きでのインシデントが発生する**
- カタカナの形態的類似性を避け、「ひらがな」を使用する
  - シーツ、ウーラ、ヌータ、ソーン
  - ワープロ端末を早急に用意する
- 外来用標準検査チェックシート、外来用標準投薬チェックシート等を事前に準備しておき、手書きを最小限にする

■ **コピー用紙、カーボン紙を備蓄しておく**

初動チームから電子カルテベンダーへの依頼事項

■ **完全なネットワーク遮断、データーやログ等の現環境の保全、システム一覧、ネットワーク構成図の準備、VPN装置のアドレス等の取得を依頼。**
- ネットワーク回線の請求書から、院外接続ポイントを洗い出しておく
- システム構成図、ネットワーク構成図を整備し、更新しておく
- 全ベンダーに VPN の利用、設置状況を聞き取りしておく
- VPN装置のグローバル IP、OS バージョン、院内接続先を台帳管理しておく

- ネットワーク構成図がないと、ネットワーク調査から始まるため、復旧が大幅に遅延することに留意する

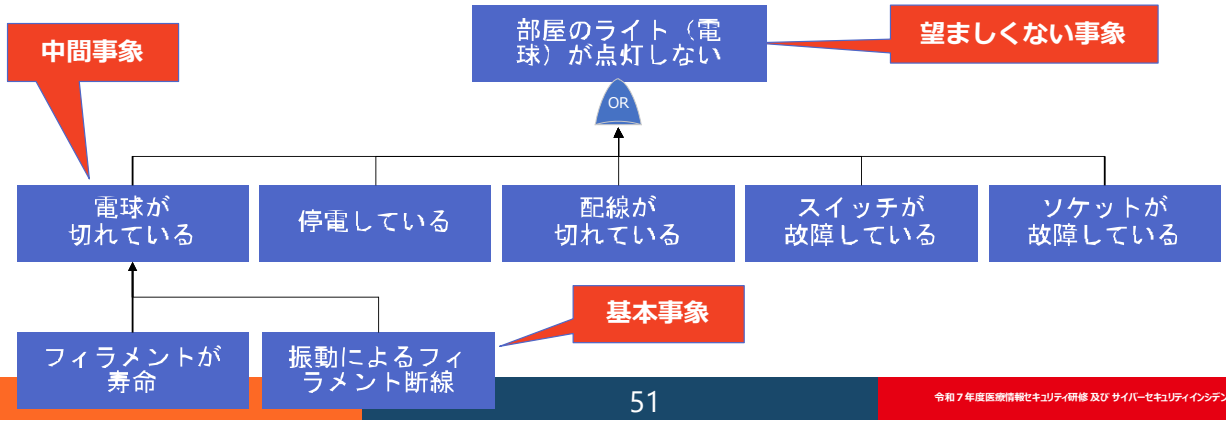
復旧対策まとめ

- 素早い意思決定ための平時の備えが重要
- 紙カルテの準備、クロノロジーの取得
- 最新のネットワーク構成図、VPN 管理台帳の整備
- 非常時のコミュニケーションツールと規定の整備
- メンタル・体調維持に十分留意する
- バックアップからの復旧手順書の整備とテスト
- クラウドサーバーの活用の検討
- 参照系システムの検討
- Syslog、NetFlow の取得
- 管理者権限を付与しない、管理者 PW を使いまわさない、脆弱性対策はセットで実施しないと意味がない

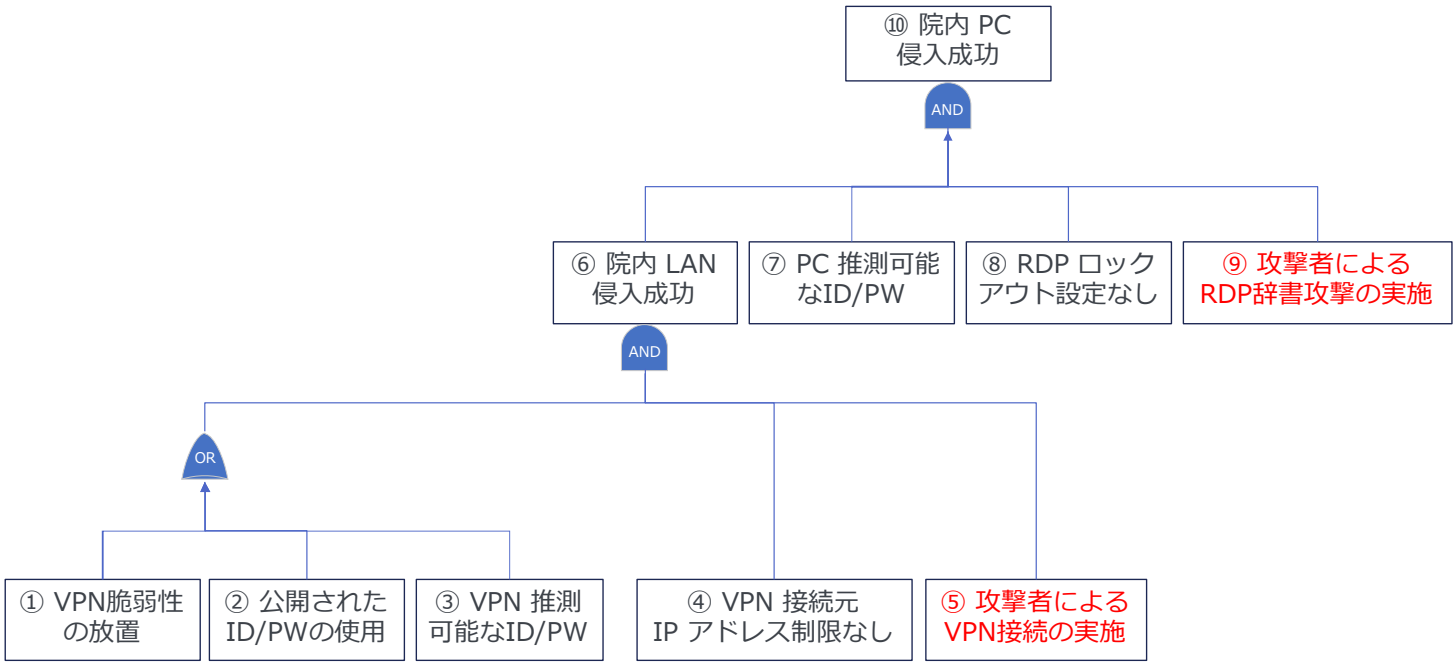
実際の攻撃ベクトル

Fault Tree 分析

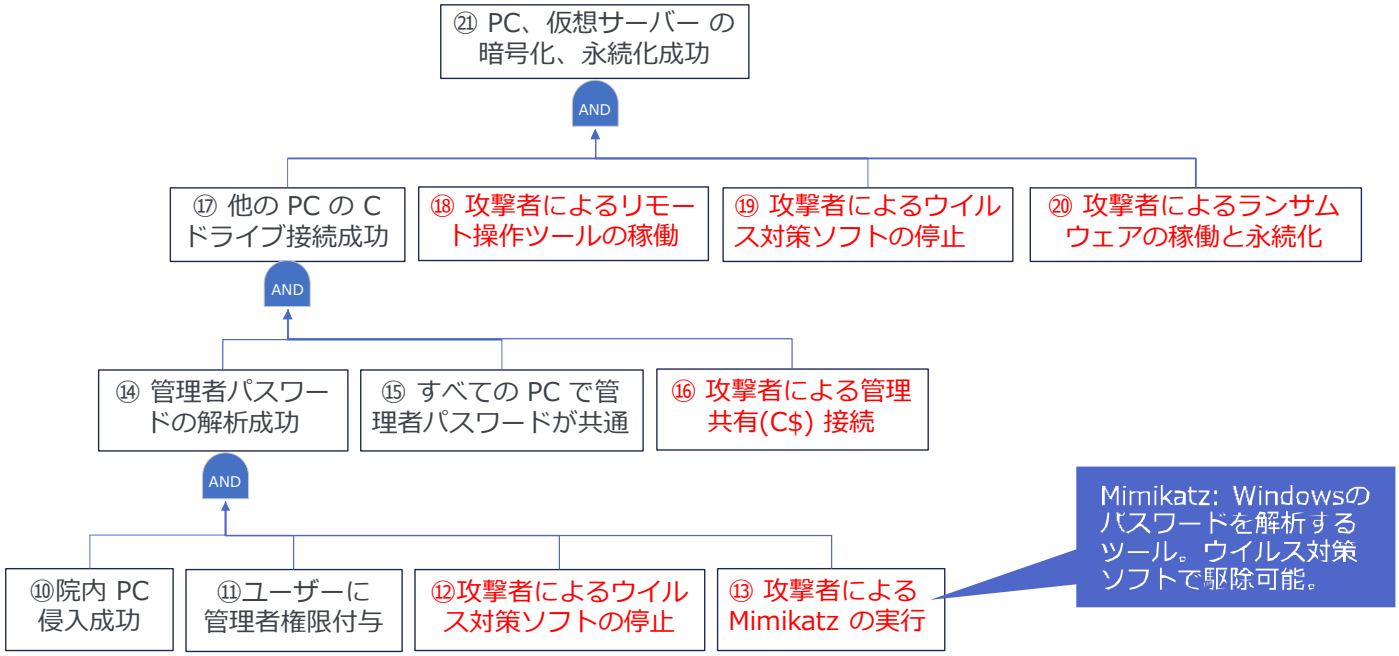
- **故障の木解析手法**
  - 1960年代にミサイル制御システムの開発に活用、その後、航空・宇宙産業、原子力、化学工業などの信頼性、安全性、稼働率向上に活用
  - 自動車、鉄道、通信システム、原子力、航空・宇宙、医療機器のリスクマネジメントで幅広く普及
- **特徴**
  - 「望ましくない事象」を定義し、「望ましくない事象」を発生させる要因を摘出



岡山県精神科医療センターの Fault Tree ①



岡山県精神科医療センターの Fault Tree ②



過去、インシデントでの共通点

組織名	ネットワーク侵入の原因	PCログインの原因	水平展開の原因	暗号化の原因
徳島県つるぎ町立半田病院	**接続元 IP アドレス制限なし** VPN 装置の脆弱性放置、公開された資格情報の悪用 (Fortigate)	管理者のPWを「P@ssw0rd」等の推測しやすいものに設定	すべてのコンピューターで管理者PWを使いまわし（共通）	管理者権限によるウイルス対策ソフトの停止
大阪急性期・総合医療センター				
北陸某病院				
関西某病院				
鹿児島県国分生協病院	**接続元 IP アドレス制限なし** 認証なしで院内 LAN に接続できる設定			
岡山県精神医療センター	**接続元 IP アドレス制限なし** VPN 接続にP@ssw0rd等の推測しやすいPW設定			

侵入は防げた

局所化は可能だった

長いパスフレーズの有効性

長さを確保できれば
辞書攻撃は不可能になる

kusamakurasanshiroUu　19桁
草枕三四郎

sangatsutanjoubihaha　20桁
三月誕生日母

furisakemirebakasuganaru　24桁
ふりさけ見れば春日なる

1秒間に1億回試行しても
11,782,543,468,864,200年かかる

n = 94

桁数	組み合わせ数
1	94
2	8,836
3	830,584
4	78,074,896
5	7,339,040,224
6	689,869,781,056
7	64,847,759,419,264
8	6,095,689,385,410,820
9	572,994,802,228,617,000
10	53,861,511,409,490,000,000
12	475,920,314,814,253,000,000,000
14	4,205,231,901,698,740,000,000,000,000
16	37,157,429,083,410,100,000,000,000,000,000
18	328,323,043,381,012,000,000,000,000,000,000,000
20	2,901,062,411,314,620,000,000,000,000,000,000,000,000

岡山県精神科医療センターのベクトルに学ぶ対策

- **■ VPN関連**
  - **接続元 IP アドレス制限の実施**
  - **VPN 装置の棚卸の実施と脆弱性管理の実施**
    - ベンダーへの脆弱性対策実施状況の聞き取り
    - サポート切れの排除と最新修正プログラムの適用
  - **VPN 認証の強化**
    - 2要素認証の実施
    - 可能な限り長いパスワードの設定、もしくは2要素認証+8桁パスワードの採用
- **■ 医療情報システム**
  - **ベンダーへの「管理者ID/PWの設定状況」の聞き取りと変更依頼**
    - 推測しにくい13桁以上の長いパスワードへの変更の依頼
    - 院内での管理者 PW の使いまわしの状況を確認
    - 使いまわしの場合、個別ユニークに設定する

まとめ

- 障害発生時は、サイバー攻撃も念頭に入れて究明する
- 週次で不審な行動がないかログを調査する
- オフラインバックアップを取得する
- ウイルス対策ソフトの改ざん防止を設定する
- VPN 機器の脆弱性修正、2要素認証、接続元制限の実施
- 管理者権限の限定、Windows の脆弱背管理の実施
- 有事の際は、すべての LAN 抜線、Wi-Fi 停波し、そのまま保全
- ステークホルダー連絡先の整備
- 手書きインシデントの発生防止
- 早期復旧のためのネットワーク・システム構成図の整備
- 長時間労働に備えたメンタル・体調管理
- バックアップの月次監査
- 復旧会議では、病院が主体となって原因究明を実施、複数の選択肢を求める
- 長いパスフレーズが有効