ランサムウェア事案調査報告書
（地方独立行政法人　岡山県精神科医療センター）

2025 年 2 月 13 日

一般社団法人ソフトウェア協会・Software ISAC
岡山県精神科医療センター ランサムウェア事案調査委員会

ランサムウェア事案調査報告書によせて

ランサムウェア（英：Ransomware）とは、組織のネットワークで結ばれたコンピューターに感染・拡散し、コンピューター内のプログラムやデーターを暗号化、情報システムを徹底的に機能不全に追い込むコンピューターウイルスです。暗号化に成功すると身代金（英：Ransom）の支払いを要求する文書を表示することから、ランサムウェアと呼ばれています。

この恐ろしいランサムウェアが活躍するのは、プログラムやデーターの暗号化という最終局面であって、その直前までは「手動」で実行犯が遠隔操作を行い、様々な下準備を行います。つまり、組織のネットワークやコンピューターへの侵入から始まり、暗号化対象となるコンピューターの調査や、ランサムウェアの妨げとなるウイルス対策ソフトの停止などは、すべて生身の実行犯の直接の操作によるものです。この際、実行犯は、コンピューターやネットワーク装置のソフトウェアの脆弱性と呼ばれる欠陥や、安直で推測しやすいパスワードを狙い、ランサムウェア稼働の条件を整えます。

逆にいえば、ウイルス対策ソフトを稼働させ、ソフトウェアの脆弱性を確実に修正し、いくつかの単語を組み合わせたパスフレーズを使用することで、ランサムウェアの攻撃リスクを大幅に低下させることが可能であることが判明しています。こまめにソフトウェアのアップデートを実行し、短いパスワードを使用せず、以下のような長いパスフレーズを使うだけで、攻撃側の負荷は天文学的に高まり、サイバー攻撃を失敗させる可能性が高くなります。

sakurameishotuyamajou	桜名所津山城：21 桁
bizenokayamakourakuen	備前岡山後楽園：21 桁
rainenchichikannreki	来年父還暦：20 桁

さて、本報告書は、地方独立行政法人岡山県精神科医療センター（以下、「病院」といいます。）の依頼により、一般社団法人ソフトウェア協会のサイバー攻撃情報の共有や分析を行う Software ISAC に「岡山県精神科医療センターランサムウェア事案調査委員会」を設け作成したものです。Software ISAC は、2021 年にランサムウェア攻撃にあった徳島県つるぎ町立半田病院や、2022 年に被害にあった大阪急性期・総合医療センターの調査報告書の策定に関わっており、また、調査委員は多くの民間組織のランサムウェア事案の調査に関わってきました。

今回の報告書の取りまとめに当たっては、病院が作成した時系列や調査報告と、第三者機関が実施したランサムウェア攻撃の分析報告書を基に時系列を整理し、病院理事長、院長を始めとする病院関係者、医療情報システムベンダー、医療機器ベンダーへの聞き取り調査を行い、また、被害にあったシステムへの追加調査を実施し、ランサムウェア攻撃が成功した原因を推測もしくは特定し、原因に基づく復旧方針、復旧時の再発防止策を、病院関係者と医療情報システムベンダーと協議の上策定し、再発防止策の実施状況を確認しています。

また、報告書策定にあたって病院理事長、院長からは、病院への忖度なく、ランサムウェア対策となる再発防止策については、広く岡山県民と全国の病院関係者に分かりやすく参考となるように求められました。ただ、再発防止策は技術的な設定が中心となる事から、分かりやすさという意味では、期待に応えられていません。また、事案発生時にネットワーク機器やコンピューターが初期設定のまま稼働していたため、攻撃

の端緒となる部分のログ（記録）が失われているなどにより、残念ながら本報告書は、すべての事実を網羅できておらず、一部推測に基づく記述も含まれています。

しかしながら、今回のランサムウェア攻撃のきっかけとなった、ネットワーク機器やコンピューターのソフトウェアの脆弱性、弱いパスワードや、弱い初期設定などは、過去のランサムウェア事案とほぼ共通であることが判明しており、本報告書に記述した再発防止策は一定の効果が期待できるものと考えています。

岡山県民各位にあたっては、ウイルス対策ソフトの稼働、Windows Update の実施、長いパスフレーズの採用を頂き、サイバー攻撃に強靭な体制を維持して頂くようお願い申し上げる次第です。また、県内情報システム関係者各位と、全国の医療情報システムの関係者各位には、徳島県つるぎ町立半田病院、大阪急性期・総合医療センターの報告書と併せて、本調査報告書の再発防止策をランサムウェア攻撃の低減の一助としてご活用いただくことをお願いし、巻頭の挨拶と致します。

2025 年 2 月

岡山県精神科医療センター ランサムウェア事案調査委員会

委員長 板東直樹

目　次

1　はじめに　　ランサムウェア事案に対応して

2024 年 5 月 19 日の日曜日に、当病院の電子カルテを含めた病院情報システムがサイバー攻撃を受け、本院と東古松サンクト診療所の電子カルテが完全に機能停止しました。さらに 6 月に入って一部の個人情報の流出が発覚するという、起こってはならない事態を招いてしまいました。あらためて、患者の皆様、ご家族、関係の方々に多大なご心配、ご迷惑をおかけしたこと、深くお詫び申し上げます。

5 月 19 日は夕方 16 時頃にカルテの不調が感知され、病院のシステム担当者がすみやかに対応し、ベンダーもリモートおよび来院で復旧にあたりました。しかし仮想基盤の重篤な障害が発生しているため復旧ができないことが明らかとなり、翌午前 6 時頃にはランサムウェアの攻撃による障害であることが確認されました。

翌朝、関係機関に連絡するとともに災害対策本部を立ち上げ、月曜の診療は急遽紙カルテを運用して継続することにしました。以来 1 日も診療を止めずに来られたことは、何より患者の皆様をはじめ多くの方々のご理解とご協力のおかげであり、また全職員の奮闘の結果であったと本当に感謝しています。

現在当院の電子カルテは、信頼できる専門家の指導を頂いて、現時点で最も安全な形で復旧・運用しています。それだけでなく、今後にわたって再び被害を受けることのないように、一層強く柔軟なシステムを構築するべく、電子カルテベンダーを含めた一同で心血を注いでいます。

ランサムウェアによる攻撃を受けた病院は、国内で報告されているものでは当院が 15 病院目でした。精神科病院としては初の報告例になります。公表されていない事例もあるかもしれませんが、この数は今後さらに増えていっても不思議ではないでしょう。病院以外の企業や団体を含めると、事例数は 2024 年になって更に増え続けており、AI を使った攻撃も日常的なものとなっていると聞きます。ある調査では、世界中で 2024 年第一四半期に発生したサイバー攻撃は 2 億件にも上り、年間被害額は 1000 兆円を優に超えるという試算もあります。いまやサイバー攻撃は一種パンデミックのような様相を呈しており、私たちにきわめて身近なものであることを実感した次第です。

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。いずれもサーバーの再起動により速やかに復旧できたこともあり、当時は外部からの攻撃を感知するような兆候も見てとれませんでした。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。

病院の情報は重大な個人情報が多く、また広範囲に被害を及ぼす可能性があります。今回のような苦渋を経験される病院が今後現れないようにするためにも、私たちの経験を広く知っていただいて、できるだけ多くの病院の皆様に早く対策をして頂くことが何よりも重要です。あろうことか、私たちは過去の事例に十分学んでいませんでした。過去の、大阪急性期・総合医療センターや徳島県つるぎ町立半田病院からは、有識者会議等による報告書が公開されており、誰でも見ることができます。当院の担当者もその資料を読んでいましたが、経験のない者にはシステム担当者や電子カルテベンダーといえど理解が容易ではなく、対策がつい遅れがちになっていたことは事実です。

この度、医療情報セキュリティの第一人者であり、当院の事案について一から十までを把握している一般社団法人ソフトウェア協会の専門家による調査委員会に事案調査を依頼し、この報告書を頂きました。本報告書の目的は、ひとえに今後の対策にとって重要な情報をできるだけ正確に提供することであり、そのための最も正確かつ有意義な報告が期待できると考えたからです。本報告書は何かを争うといったことを目的にはしていませんが、一切の忖度なしで事実と責任の所在を明確にし、今後の警鐘とすることをお願いしています。そのことは本報告書にかかれた厳しい指摘の数々をお読み下さればご理解いただけると思います。厳正に調査をして頂いた、調査委員会にあらためて感謝申し上げます。

サイバーセキュリティ対策は、それ自体直接に診療実績等を生むわけでもなく、またシステム情報系の人材も不足しているため、後手後手になりがちかと思います。昨今の急激な経済変動も加わり、医療機関はどこも厳しい経営状況にあります。サイバーセキュリティに十分な人や資金を投入できる体力を持つ病院は非常に少数派であると思われます。

しかし私どものように、過去の事例の報告が世に出ていながら対策が遅れていたということが繰り返されてはなりません。セキュリティを高めるためにあたっては、シンプルな設定や OS 標準機能の活用で安価にできる事柄も多く、本報告書にはそうした具体的な対策の数々も記載されています。皆様が本報告書を参考にされて、有効な対策を打たれることを願っております。

2025 年 2 月

地方独立行政法人岡山県精神科医療センター
理事長　山田了士

1.1 謝辞

岡山県精神科医療センターでの復旧時における医療情報システム及び医療機器等の取り扱いにあたっては、大阪急性期・総合医療センターより「インシデント発生時の初期化判断基準」等の各種復旧対策資料の提供を受け、これらを参考に復旧にあたりました。この場を借りて、大阪急性期・総合医療センター及び資料策定にあたったシステムベンダー各位に深く感謝の意を表します。

1.2 参考資料

- フォレンジック調査報告書
  株式会社 LAC 社 2024 年 9 月 25 日
  株式会社くまなんピーシーネット 2024 年 9 月 27 日

- クロノロジー及び調査報告
  岡山県精神科医療センター 2024 年 10 月 11 日

1.3 一般社団法人ソフトウェア協会・Software ISAC 岡山県精神科医療センター ランサムウェア事案調査委員会

委員長	板東直樹	一般社団法人ソフトウェア協会フェロー/Software ISAC 共同代表 アップデートテクノロジー株式会社代表取締役社長
委員	加藤智巳	一般社団法人ソフトウェア協会理事/Software ISAC 共同代表 BC Signpost 株式会社 代表取締役副社長
委員	松山征嗣	一般社団法人ソフトウェア協会 上席研究員

※ 一般社団法人ソフトウェア協会について
パッケージソフト、クラウドサービスなど自社ソフトウェア、サービスの開発、販売を中心としたソフトウェア関連企業の業界団体。
会　長：田中邦裕 （さくらインターネット株式会社代表取締役社長）
所在地：東京都港区赤坂 1-3-6
設　立：1986 年
会員数：805 社・団体、個人会員 18 名（2025 年 1 月）

※ Software ISAC について
Software ISAC (Information Sharing and Analysis Center) は、サイバーセキュリティの脅威やインシデントに関する情報を共有・分析するためのソフトウェア協会の下部組織。サイバー攻撃の手法、脆弱性、新たな脅威などに関する情報の共有や、提供された情報を基に、脅威の詳細やその影響の分析、サイバーインシデント発生時の対応や復旧を支援している。また、Software ISAC は公共団体、医療機関に対して、「サイバーセキュリティボランティア制度」による無償の復旧支援やトレーニング、システムの脆弱性分析などをおこなっている。

2 用語解説

用語	定義
フォレンジック調査	コンピューターやネットワーク機器のログや証跡を収集・分析し、不正行為やサイバー犯罪の証拠を特定するための調査手法
病院	地方独立行政法人岡山県精神科医療センター。
HIS	Hospital Information System、病院情報システムのこと。一般的に、インターネット接続がない閉域網を指してHIS系などと呼ぶ。
基幹システム	病院情報システムの内、電子カルテ、医事会計、オーダーリングなどの中核をなすシステムのこと。
部門システム	薬剤、放射線、臨床検査、栄養など、基幹システムとオーダーやデーター連携が必要な医療部門のサブシステムの総称。
支払基金	社会保険診療報酬支払基金のこと。
A 社	基幹システムのソフトウェア構築・保守統括事業者。
B 社	基幹システムのデーターセンター側ハードウェア・ネットワーク構築・保守事業者。
C 社	基幹システムの病院内ネットワーク構築・保守事業者
ベンダー	医療情報システム、医療機器、ネットワーク等の導入・構築を行う事業者の総称。
X	本件のランサムウェアによるサイバー攻撃者。
ランサムウェア	被害者のファイルを暗号化したり、システムへのアクセスを制限したりして、データーやシステムの復旧に対する身代金（ランサム）を要求する悪意のあるソフトウェア。
仮想基盤	物理的なコンピューター上で動作する、ソフトウェアで作られた「仮想的なコンピューター」を稼働させるための基盤ソフトウェア。1台の物理コンピューターで、複数の仮想コンピューターを稼働でき、それぞれは、独立したコンピューターとして動作する。
仮想用共有ストレージ	複数の仮想マシンが同時にアクセスできる共有ストレージ。障害発生時に仮想マシンを再構築したり、ストレージ容量を追加、削除でき、拡張性や効率的利用を実現する。
閉域網	構内ネットワーク（LAN）において、特に、外部との接続を一切行わない閉じたネットワークを指す。外部との接続がないことから、ウイルス感染やサイバー攻撃を受けない。
Active Directory	組織内のユーザー、コンピューター、プリンターやファイル共有などを一元的に管理するためのシステム。ユーザーの認証やアクセス許可を司る。ADと省略する。
ADサーバー	Active Directoryサーバーのこと。
DWH（Data Ware House）	大量のデータを整理・統合し、分析しやすい形で保存するデーターベース。医療では、基幹システムから診療録、サマリや看護情報、オーダー情報等を取得し、データーベースに蓄積し、情報の集計、分析に使用される。
Firewall	一般的には、ルーター機能に加え、ネットワーク攻撃や不正なWebサイトへの通信を遮断するなどのセキュリティ機能や、SSL-VPN機能を提供する通信装置を指す。パーソナルFirewallという場合は、Windowsに組み込まれている通信の許可・拒否を行うパケットフィルタリング機能を指す。
IP-Sec VPN	インターネット等を経て、企業内ネットワークや各拠点間の通信を安全に行うための仕組み。IP-Secが暗号化、改ざんの検証、相互認証を司り、仮想専用ネットワーク (VPN)を構成する。IP-Secで接続されたVPNは、通信の傍受や改ざんが困難であり、これを利用することで、インターネットを使った企業ネットワークを安価に構築できる。
LAN (Local Area Network)	特定の構内ネットワークのこと。
PSEXEC	Windows の遠隔操作ツール。接続先のコンピューターでコマンドやプログラムの実行ができ

用語	定義
	る。ランサムウェア事案で悪用される。
ルーター（router）	ネットワーク間で特定の許可された通信だけを転送したり、ネットワークのアドレス変換を行う通信装置。LANとインターネットの接点に設置し、LAN側からの電子メールやWebへのアクセスと、その応答に限って通信を許可するなどの橋渡しを行う。
SMB (Server Message Block)	Windows 等のコンピューターで、LANを通じてファイルの共有やプリンターの共有を行うための通信手順。Windowsでファイルサーバーや NASにアクセスする場合は、大半がSMBによるファイル共有機能を使用している。ネットワークに接続されたコンピューターのファイルの閲覧や編集が可能で、認証機能を使い特定の利用者だけにアクセス許可を行うなどが可能。
SSL-VPN装置	暗号化技術であるSSLと、仮想専用ネットワーク (VPN) を組み合わせた通信装置。インターネットを経由してLANへ安全に接続するために利用される。多くはFirewallに組み込まれたSSL-VPN機能を利用することが多い。
WMI（Windows Management Instrumentation）	システムの情報取得や設定変更を可能にする管理インターフェースで、遠隔保守などに使用される。システム情報や、プログラムの実行状況、パーソナルFirewall の設定変更等が可能。ウイルスやランサムウェア攻撃で悪用される。
管理共有（C$）	Windows に標準で用意されている共有フォルダー。管理者権限があればネットワーク経由でアクセス可能。
リモートデスクトップ接続（RDP）	Windows標準の遠隔操作機能。リモートデスクトップ接続を行うと、操作端末のキーボードやマウスの手元の操作が遠隔端末側に伝達され、自由に遠隔端末を操作、設定できる。
初動対応チーム	厚生労働省から派遣されたセキュリティ専門家の派遣チーム。
厚労省ガイドライン	厚生労働省 医療情報システムの安全管理に関するガイドラインの略称。
２省ガイドライン	総務省・経済産業省 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドラインの略称。
3省2ガイドライン	厚労省ガイドラインと2省ガイドラインの総称。
要配慮個人情報	不当な差別や偏見その他不利益が生じないようにその取扱いに特に配慮を要するものとして個人情報保護法第２条第３項、個人情報保護法施行令第２条及び個人情報保護法施行規則第５条で定める記述等が含まれる個人情報。医療、介護関係においては、診療録等の診療記録や介護関係記録に記載された病歴、診療や調剤の過程で、患者の身体状況、病状、治療等について、医療従事者が知り得た診療情報や調剤情報、健康診断の結果及び保健指導の内容、障害（身体障害、知的障害、精神障害等）の事実、犯罪により害を被った事実などがあたる。

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

3.1 病院概要

本院所在地	岡山県岡山市北区鹿田本町 3-16
理事長	山田 了士
院　長	来住　由樹
病床数	255 床
診療科目	精神科・児童精神科・心療内科
職員数	349 名（医師 37 名、看護師 207 名）
認定・指定	応急入院指定病院、精神科救急医療施設、精神科専門医研修指定病院、 臨床研修指定病院、医療観察法に基づく指定入院医療機関、 岡山県依存症治療拠点機関、子どもの心の診療拠点病院

診療所所在地	岡山県岡山市北区東古松 4 丁目 9-24
診療科目	精神科

3.2 外来患者数の推移

年度	2020 年	2021 年	2022 年	2023 年
初診患者数	2,478	2,759	2,821	2,685
再来患者数	44,158	45,672	46,191	44,548
一般延患者数	46,636	48,431	49,012	47,233
デイケア延患者数	7,295	9,217	10,649	10,724
延患者数（デイケア・訪問看護を含む）	63,539	64,932	59,661	57,957
１日平均患者数（デイケアを含む）	221.9	238.2	245.5	238.5

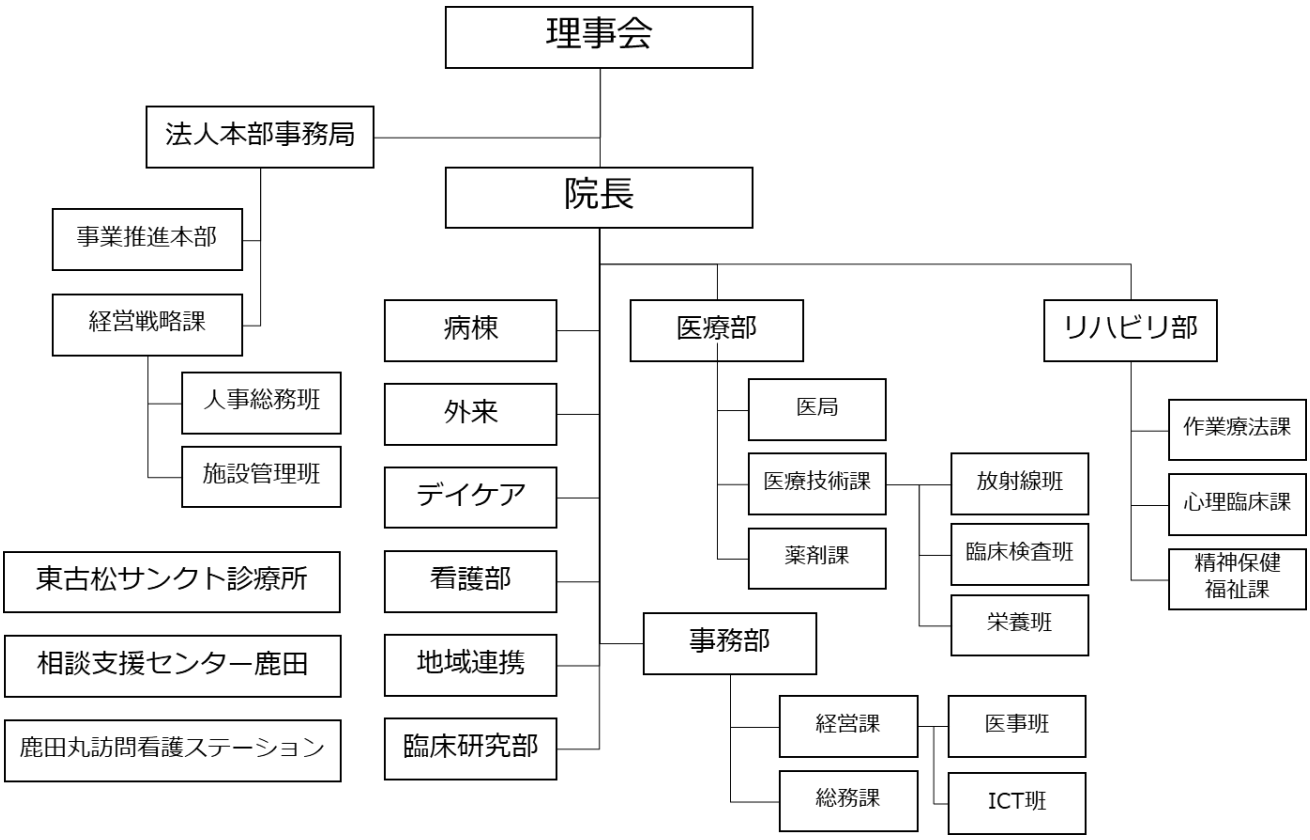
3.3 入院患者数の推移

年度	2020 年	2021 年	2022 年	2023 年
期首在院患者数	210	234	236	220
入院患者数	1,424	1,636	1,658	1,626
休日・夜間（再掲）	474	546	523	-
退院患者数	1,400	1,634	1,674	1,611
期末在院患者数	234	236	220	235
年度延在院患者数	84,412	82,515	84,442	87,731

3.4 病床利用数、平均在院日数、病床回転率の推移

年度	2020 年	2021 年	2022 年	2023 年
１日平均患者数(人)	200.1	192	195.4	206.2
病床利用率(%)	91.4	87.7	89.2	94.1
病床回転率(%)	700.3	844.1	850.6	782.1
平均在院日数(日)	52.1	43.2	42.9	46.8

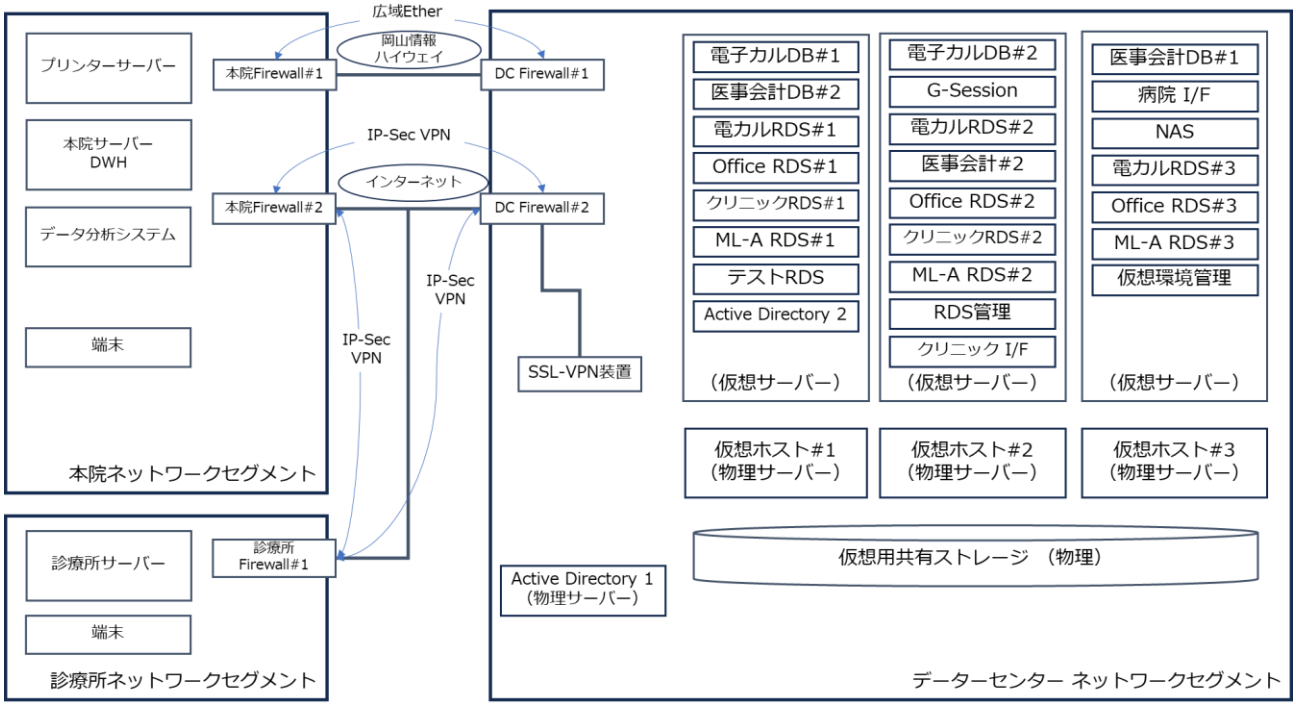
3.5 病院組織



4　病院情報システム（HIS）概要

4.1　病院情報システムネットワーク全体構成

ネットワークは、HIS 系で大きく 3 つ、データーセンターと本院、診療所に分けられる。それぞれは、岡山情報ハイウェイを介した主回線と、IP-Sec VPN によるバックアップ回線から構成されている。バックアップ回線はインターネットを介しているが、VPN 接続のため、データーセンター、本院、診療所のネットワークからインターネットを閲覧することはできない。また、データーセンターの Firewall に保守用の SSL-VPN 装置が接続されており、インターネットから病院情報システムネットワークへの接続は、この SSL-VPN 装置を通じ認証を経て接続が可能となっている。



4.1.1　データーセンター

データーセンターには、仮想基盤を構成する仮想ホスト 3 台（物理）、仮想サーバーが共有する物理共有ストレージ 1 台（物理）、認証やファイルのアクセス制御を司る Active Directory サーバー1 号機（物理）が設置されている。仮想ホスト上には、それぞれ電子カルテ、医事会計、NAS、Active Directory2 号機などが仮想サーバーとして構築されており、一元管理されている。また、データーセンターの Firewall2 号機の配下に病院情報システムの保守用の SSL-VPN 装置が設置されている。なお、本院、診療所、データーセンター設置の Firewall 装置は SSL-VPN 機能を稼働させておらず、外部からの VPN 接続はデーターセンター設置の SSL-VPN 装置だけである。

4.1.2　本院

本院には、プリンターサーバー、ファイル共有と医療情報の分析を行うための DWH 機能を有する本院サーバーと、データー分析システム及び端末が設置されている。端末からデーターセンターの仮想サーバーに接続し、電子カルテ等の基幹システムを操作している。

4.1.3　診療所

診療所には、診療所サーバーと端末があり本院同様に、端末からデーターセンターの仮想サーバーに接続し、電子カルテ等の基幹システムを操作している。

4.1.4　病院情報システムのソフトウェア、ハードウェア、ネットワーク担当ベンダー

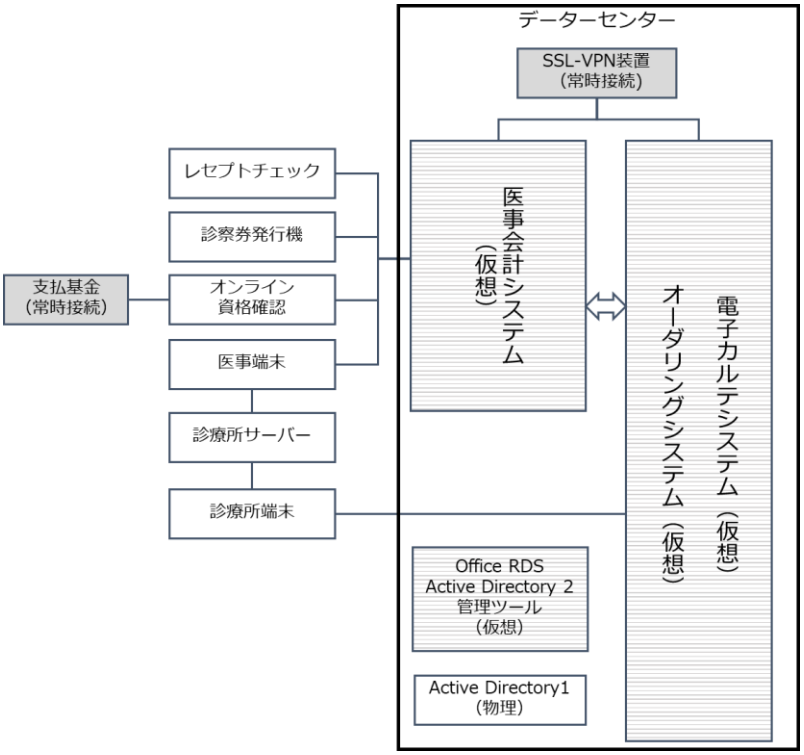
基幹システムおよび部門システムを含む病院情報システムは、A 社がソフトウェアの構築、設定、統括的な 1 次保守を請負、A 社の配下で、部門システムベンダーが部門システムの構築を行い、B 社がデーターセンター側の仮想基盤の物理サーバー、仮想用共有ストレージ構築、VPN 装置の構築と保守を、C 社が病院内ネットワークの構築と保守を行っている。

4.2 本院システム構成

本院には、データーセンター設置の電子カルテと連携する検査システム、医用画像システム、薬局システム等の部門システムと診療科システム等が設置されており、また、データーセンター設置の医事会計に連携する自動精算機、POS 精算機、診察券発行機などと、オンライン資格確認システムが接続されている。オンライン資格確認システム及びクレジットカード会社との接続を除く、外部接続点は本院側で 4 ヵ所あり、各システム専用の VPN 装置経由で独自のリモート保守が実施されている。また、独自のリモート保守を持たないシステムは、すべてデーターセンターの SSL-VPN 装置経由で保守を実施している。

4.3 診療所システム構成

診療所には、データーセンター設置の電子カルテ、医事会計システムにアクセスする端末および診療所サーバーが設置されている。診療所には、部門システムはなく、外部接続点としては、オンライン資格確認システムが存在している。



4.4 病院情報システムに接続された Firewall、SSL-VPN 装置について

HIS 系ネットワークに設置された Firewall、SSL-VPN 装置は以下のとおりである。

記号	設置場所	機器名	プロトコル	OS バージョン
DC Firewall#1	データーセンター	Fortinet FortiGate-60E	OSPF	6.0.4 2022/9/28 サポート終了[1] ※SSL-VPN は未使用
DC Firewall#2	データーセンター	Fortinet FortiGate-60E	IP-Sec	
本院 Firewall#1	本院	Fortinet FortiGate-60E	IP-Sec	
本院 Firewall#2	本院	Fortinet FortiGate-60E	IP-Sec	
診療所 Firewall#1	診療所	Fortinet FortiGate-60E	IP-Sec	
SSL-VPN 装置	データーセンター	Cisco ASA-5506-X	SSL-VPN	ASA 9.9(2)40 2023/5/31 サポート終了[2]

4.4.1 FortiGate の FotiOS の脆弱性について

CISA Known Exploited Vulnerabilities Catalog[3] によると、実際のランサムウェア攻撃に使用されたと確認されている FotiOS 6.0.4 の脆弱性は 5 個存在するが、すべて SSL-VPN に関連するものであった。

4.4.2 Cisco ASA-5506X の脆弱性について

[1] https://community.fortinet.com/t5/Support-Forum/FortiOS-End-of-Life-Overview/m-p/301142
[2] Cisco ASA 5500 Series End-of-Life and End-of-Sale Notices
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CISA Known Exploited Vulnerabilities Catalog によると、実際のランサムウェア攻撃に使用されたと確認できている脆弱性は 3 個存在した。

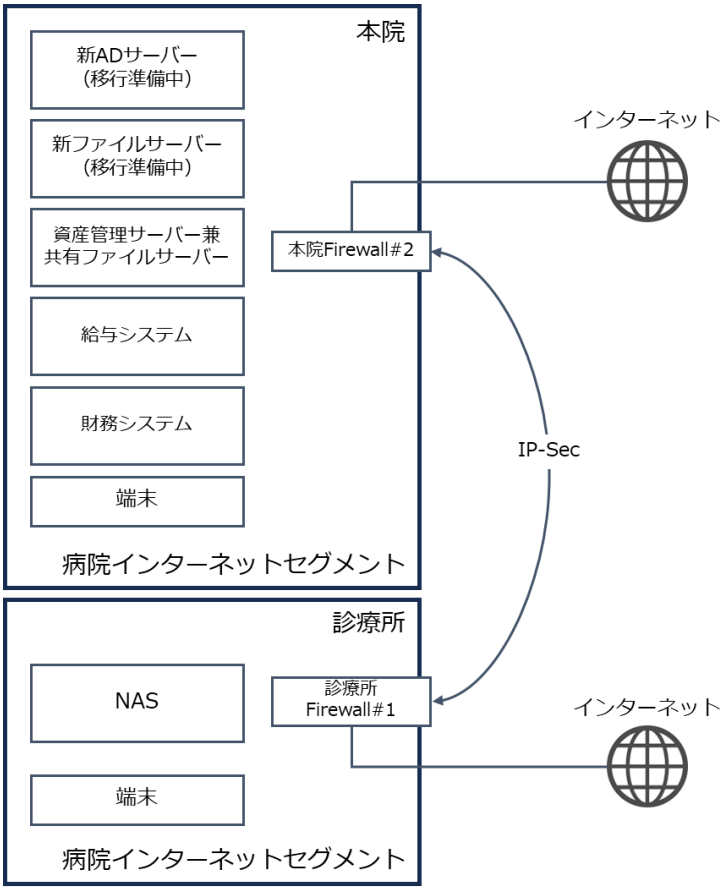
CVE-2020-3259

CVE-2023-20269

CVE-2020-3153

4.5 インターネット系ネットワーク全体構成

病院のインターネット系ネットワークは本院、診療所共に同一の VLAN 上の病院インターネットセグメントとして構成されており、給与、財務、ファイルサーバー、NAS が設置されている。インターネットへの接続は、本院、診療所に設置された Firewall からそれぞれ直接インターネットに抜けている。攻撃時点で、インターネット系 Active Directory サーバーとファイルサーバーの移行準備中であった。

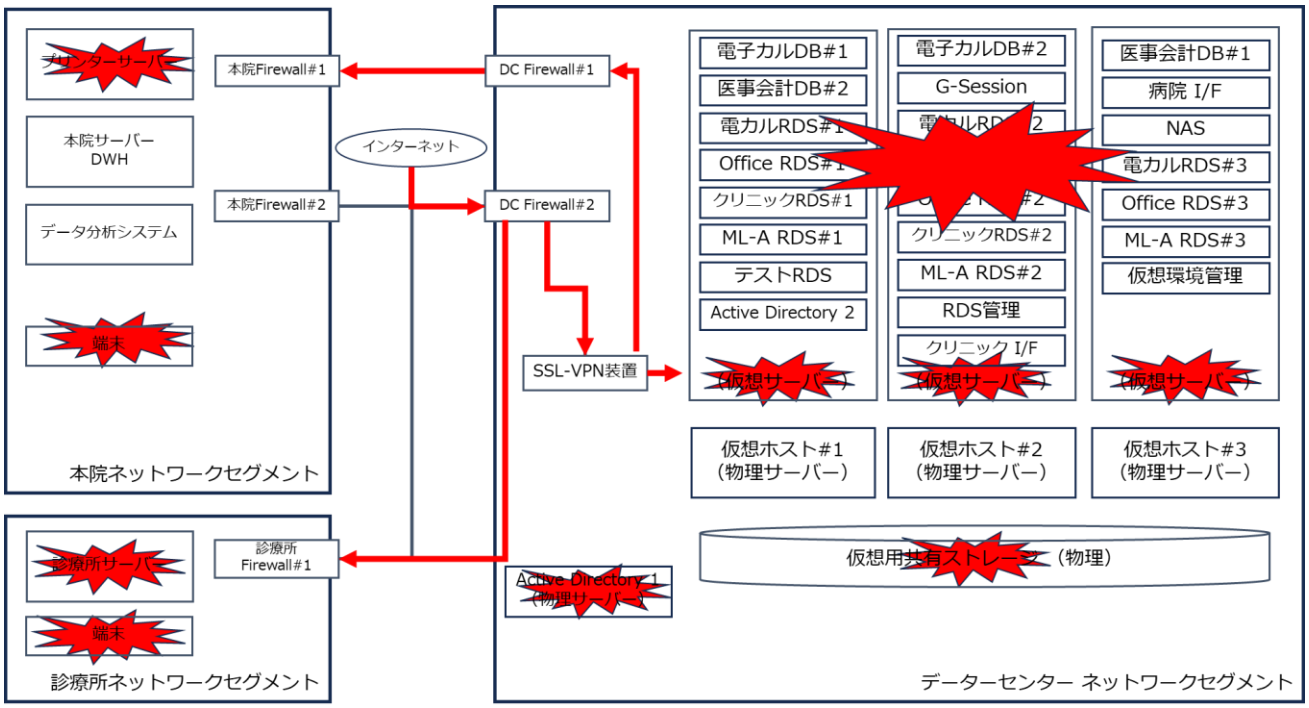


5　概要編

5.1　インシデント概要

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。直ちに病院ネットワークの停止を行い、厚生労働省、岡山県、岡山市、岡山県警察本部に報告、紙カルテ運用への切り替えを開始した。同日 16:00 には、病院ホームページへの掲載、プレスリリースを通じて、サイバー攻撃をうけ電子カルテが停止していることを県民にむけて公表し、入通院患者には紙面や口頭で説明を開始した。翌 21 日 15:30 にはランサムウェアとみられるサーバー攻撃であることを続報として公表した。また、病院としては、身代金の支払い、攻撃犯 X との連絡、交渉は一切行わず、自力で復旧する方針を固め、専門家の助言を仰ぎつつ A 社を中心とした復旧を目指すこととした。

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。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。



また、攻撃犯 X による情報窃取と情報漏洩が岡山県警により確認された。推定で氏名、住所、生年月日、病名等を含む最大 40,000 人分の個人情報の漏洩を招いた。このため、6 月 11 日に記者発表を行い、要配慮

個人情報の漏洩の事実を公表し、併せて、郵送によるお詫びと本人通知を実施した。一方で、サイバー空間上での情報漏洩のありかについては捜査上の秘密となっており、病院としてはサイバー空間上での漏洩の実態を把握できていない。なお、攻撃犯 X のリークサイトは 2025 年 2 月時点でアクセスができず、病院関連の組織名や情報は確認されていない。

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。

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[4]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。

攻撃発生から約 3 ヵ月で電子カルテシステム等は完全復旧し、2024 年 12 月時点で、ランサムウェアを含むサイバー攻撃抑止のための高水準の技術的な強化対策の適用をほぼ完了した。2025 年 1 月以降、組織的対策、人的対策を実施し、医療 DX 化に向けたサイバーセキュリティと病院経営の戦略的統合による要配慮個人情報のさらなる保護を図る予定である。

5.2 復旧経緯

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。

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。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

[4] 医療情報システムの安全管理に関するガイドライン　第 6.0 版（システム運用編）（令和 5 年 5 月）、8．利用機器・サービスに対する安全管理措置 遵守事項③「セキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用」⑤「推定しやすいパスワード等の利用を避ける」、⑥「IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用する」https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

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。

病院内のすべてのサーバー、端末は閉域網であることから、Windows Update 等の脆弱性対策が一切行われていなかった。また、すべての一般ユーザーに管理者権限が付与されていた。このため、脆弱性の悪用や、管理者権限によるウイルス対策ソフトの停止によるウイルスの残留やバックドアの設置が疑われたため、基本的にすべてのコンピューターは完全な初期化、もしくは新品との入れ替えを行った。
病院側の試算では、A 社を含めた復旧工数としてシステム再構築、データー入力、スキャナー取り込み等で約 65 人月の工数がかかったとされている。

5.3 情報漏洩

6 月 7 日、岡山県警察本部より個人情報の流出を確認した旨の連絡があり、病院長が県警本部に出向いて確認したところ、電子カルテ内の情報ではないが、本院サーバーの共有フォルダーであることが判明した。同フォルダーには医事情報、行政調査情報、ケア会議議事録等の Office 文書（氏名、住所、生年月日、病名等を含む最大 40,000 人分）であることが推定された。病院は 6 月 11 日に岡山県庁で記者会見を実施し、要配慮個人情報の漏洩の事実を公表し、併せて、郵送によるお詫びと本人通知を実施した。また、病院内に患者、家族に対する相談窓口を設置、当日約 100 件以上の問い合わせに対応、6 月 14 日以降は専用コールセンターを設置し、引き続き、お詫びと相談対応を実施した。

一般論としてランサムウェア事案の情報公開は、TOR ブラウザー[5]と呼ばれる匿名性を保つブラウザーを使い、複数の匿名化サーバーを経由して接続する「ダークウェブ」と呼ばれるサイバー空間の攻撃犯が所有するリークサイトで行われる。病院は捜査中であることから岡山県警から詳細なリークサイト等の情報提供は受けられなかったため、暗号化されたファイルの拡張子から攻撃犯 X を特定、攻撃犯 X のダークウェブ上のリークサイトを調査した。リークサイトは攻撃した組織ごとに、窃取した Office 文書や PDF 文書等の一部が閲覧できるように構成されていた。このため、リークサイトに掲示されている組織名をくまなく調査したが、「Okayama」、「Okayama Psychiatric Medical Center」、「Psychiatric」、「岡山」、「岡山県」、「岡山県精神科医療センター」、「医療センター」等のキーワードを見つけることができず、病院から漏洩したとされるフォルダーを発見することもできなかった。このため、病院は専門家に依頼し定期的にダークウェブの監視を実施したが、患者情報等の漏洩は 2025 年 2 月時点でも確認できていない。加えて、2024 年 10 月時点の攻撃犯 X のリークサイトでは 2024 年 5 月時点で攻撃を受けた他の組織名は確認可能だが、漏洩文書へのアクセスは不可能となっていた。なお、2024 年 11 月以降、攻撃犯 X のリークサイトにはアクセスができない状態にある。

[5] The Onion Router ブラウザー。匿名でインターネットを閲覧するための Web ブラウザーで、「タマネギの皮（Onion Routing）」のように、複数のレイヤーで通信を暗号化するため、接続元の IP アドレスや位置情報を隠すことができる。通常のブラウザー（Chrome, Edge など）ではアクセスできない ダークウェブと呼ばれる「.onion」ドメイン に接続が可能。

また、電子カルテシステムの診療情報データーベースについては、ファイル形式で 18,000 ファイル（テーブル）300 ギガバイト以上あり、全ファイルを取得しないと使用、閲覧ができない仕様となっていた。データーベースへの接続、閲覧には接続文字列（プロバイダー名[6]、ソース、ID、パスワード）が必要となるが、接続文字列は電子カルテシステムのプログラムを通じで引き渡されており、万一、データーベースが窃取されたとしても、推測によるデーターベースへの接続・閲覧は困難であると考えられる。

なお、5 月 19 日時点での電子カルテシステムのログより、電子カルテシステムへの端末からのログオン失敗は 35 件であり、そのうち 1 件を除いてすべて当日勤務をしていた職員による人為的な操作ミスであり、残りの 1 件についてはユーザーID の入力がなくログオンを試行したもので、操作ミスの可能性が高いと判断された。電子カルテのユーザーID は 4 桁もしくは 5 桁であり、ユーザーのパスワード設定初期値が 4 桁であることから、総当たり攻撃でのログオン成功は、少なくとも数千回から数万回程度の試行が必要となるが、連続した大量のログオン失敗は認められていない。以上のことから電子カルテへの端末からの接続および情報の閲覧、情報の漏洩の可能性は極めて低いと考えられる。

5.4 仮想基盤の破壊及び共有ストレージ喪失

病院の病院情報システムは、電子カルテ、医事会計、オーダーリング等の基幹システムが VMWare 社の仮想基盤上の仮想サーバーで動作していた。各仮想サーバーは、共有ストレージにデーターを保存し、データーを共有していた。仮想基盤は 3 台の物理サーバーで構成されていたが、この内、 1 台の仮想基盤（ESXi：ベアメタルハイパーバイザー ）がランサムウェアに感染した。仮想基盤の脆弱性を悪用したものと推測される。その後、すべての仮想マシンファイルを保存していた共有ストレージへ感染が拡大し、仮想基盤を統合的に管理する仮想プラットフォーム（vSphere）まで感染が及んだ。これに伴い、共有ストレージのハードディスクの割り当て情報を保存していたキャッシュ SSD の META 情報も破壊されたため、仮想基盤の起動が不可能となった。そこで、データー復旧解析事業者に解析と復旧を依頼し、約 3 ヵ月に渡り解析・復旧作業を行ったが、META 情報は回復できず基幹系システムのデーターは全喪失となった。

5.5 原因

5.5.1 初期侵入の原因

外部接続点となる Firewall、SSL-VPN 装置は、システムイベントやエラー、警告、状態情報を記録する Syslog の保存設定がなされておらず、各装置のメモリ上で上書き設定となっていた。侵入口と想定される SSL-VPN 装置は Syslog の保存が 4Mbyte であったため、暗号化発覚時点ではすべて上書きされてしまっており、侵入元 IP アドレスなどの調査は不可能であった。そこで、残存した物理サーバーのフォレンジック調査をセキュリティ調査会社に依頼した。物理サーバーのフォレンジック調査でも、実際の初期侵入の端緒および水平展開の経路は確定に至っていないが、病院関係者及び A 社への聞き取り調査により以下が確認された。

[6] プロバイダー名：データーベースとの接続管理、問い合わせ、セキュリティ等を司るソフトウェアのこと。

① 保守用 SSL-VPN 装置の ID/PW が、administrator/P@ssw0rd という推測可能なものが使用されていた。
② 病院内のすべての Windows コンピューターの管理者の ID/PW も、上記と同じ administrator/P@ssw0rd が使いまわされていた。
③ SSL-VPN 装置の脆弱性が 2018 年の設置以降、修正されておらず、過去、ランサムウェア攻撃に使用された脆弱性が複数存在した。
④ すべてのサーバー・端末ユーザーに管理者権限を付与していた。

以上のことから、初期侵入は、①保守用 SSL-VPN 装置への辞書攻撃 、②窃取した資格情報を売買する Initial Access Broker からの資格情報の購入、③SSL-VPN 装置の脆弱性の悪用、以上いずれかが原因と推測される。

5.5.2 水平展開の原因

病院内の水平展開は、物理サーバーの Windows ログに多数のリモートデスクトップ接続の形跡があるものの、端末側にはリモートデスクトップ接続のログがなく、主に攻撃者 X が作成したと思われるアカウントによる SMB 接続が多数見受けられたこと、他方で PSEXEC、WMI、PowerShell などの使用痕跡が認められないことから、管理者権限で攻撃先の端末の管理共有（C$）にリモート接続し、攻撃元コンピューターのリモートドライブとして暗号化した可能性が高い。サーバーの保全データーからは、多数のファイルの暗号化が確認されたことから、サーバーの暗号化については、手動でウイルス対策ソフトを停止し暗号化を実施したと考えられる。また、ウイルス対策ソフトの削除の痕跡が確認された。サーバーの再起動時にウイルス対策ソフトが再起動することに備えた措置と考えられる。いずれも、管理者の資格情報の使いまわしが水平展開と、ウイルス対策ソフトの停止による暗号化を容易にしたものである。また、仮に資格情報が使いまわされていなかったとしても、すべてのユーザーに管理者権限を付与していたことから、ウイルス対策ソフトの停止後、Mimikatz[7]等のパスワード解析ツールによるパスワードの窃取や様々な攻撃手法よる水平展開は容易であった。

A 社への聞き取り調査によれば、多くの医療情報システムは、管理者権限を付与することが半ば常態化している、とのことであった。病院情報システムにおける一般ユーザーへの管理者権限の付与については、業界全体での見直しが必須であるといえる。

5.5.3 過去事例との共通点

本件事案の原因は、管理者パスワードの使いまわし、サーバー・端末ユーザーへの管理者権限の付与、これによるウイルス対策ソフトの停止という点で、徳島県つるぎ町立半田病院、大阪急性期・総合医療センターで発生したランサムウェア事案とまったく同じである。

---

[7] Windows に保存されている ID、パスワードの解析、攻撃を行うツール。Pass-the-Hash (PtH)、Pass-the-Ticket (PtT)、ゴールデンチケットなど、窃取した認証情報でシステムへの様々な攻撃を可能する。解析には管理者権限が必須で、一般的なウイルス対策ソフトで検知、駆除が可能。「ミミカッツ」、「ミミキャッツ」と読む。

少なくとも、過去の国内の病院へのランサムウェア攻撃においては、決して高度な攻撃がなされた訳ではなく、脆弱性の放置と管理者権限の付与がされた「ランサムウェア攻撃に弱いシステム」が攻撃されたに過ぎない。病院に限らず、上記の脆弱性を有する組織であれば、同様のランサムウェア被害にあうことに留意すべきであり、VPN 装置の脆弱性管理、VPN 装置の ID、パスワードの見直し、サーバー・端末ユーザーに対する管理者権限の付与の取りやめ、サーバー、端末の管理者の ID、パスワードの使いまわしの停止を、至急、実施すべきである。

5.6 事案の時系列

病院関係者及び A 社への聞き取りとフォレンジック調査から判明した、事案の時系列は以下のとおりである。

日付	時刻	内容
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。
2024/5/13	02:41	AD サーバーへの初期侵入。これ以降 18 日まで連日、断続的にネットワークスキャン、AD 構成情報の窃取、共有フォルダーのデーター窃取、バックアップデーターの探索を実施。
5/14	08:35	AD サーバーが起動せず、バックアップから復旧。
5/15	08:06	AD サーバーの動作が不安定となる。再度、バックアップから復旧。
5/19	13:10～17:34	基幹システムを始めとする各サーバー、端末の暗号化の実施。
	16:00 頃	病院スタッフが電子カルテの動作停止を確認、A 社に連絡。
	18:00 頃	A 社がリモートで接続し、仮想基盤の障害と判断。
	23:00 頃	病院担当者と A 社がデーターセンターに設置された仮想基盤の調査を開始。AD2 号機、VMWare2 号機の再起動や復旧を試みる。
5/20	04:00 頃	病院担当者と A 社にて原因不明のため BCP 運用の切り替えの準備を開始し、バックアップからの復旧を計画。
	04:30 頃	前日のデーターベースのバックアップからのレストアを試みる。
	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。
	06:20 頃	A 社が病院担当者にランサムウェアであることを報告、病院担当者が幹部に連絡。
	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。
	09:15 頃	厚生労働省から初動対応チームに対し派遣待機の指示。
	09:45 頃	岡山県、岡山県警察本部が来院。
	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。

日付	時刻	内容
	11:50 頃	A 社が AD サーバー等の Event Log、Firewall 装置、VPN 装置のログを採取。
	12:40 頃	A 社がプリンターサーバーからランサムノートを発見。
	同	入院患者用紙カルテの作成を開始。
	13:00 頃	対策本部会議（第 2 回）ランサムウェアが発覚したが、犯人からの要求をのむことはしないことを決定。
	14:25 頃	オンライン資格確認認証停止を確認。
	14:30 頃	プレスリリースの作成、各機関との調整を開始。
	14:45 頃	各病棟に入院紙カルテを配付。
	16:00 頃	サイバー攻撃を受けたことを病院ホームページで公表するとともに、プレスリリースを配布。
	17:00 頃	対策本部会議（第 3 回）BCP カルテの PC が 5 台（のち 9 台）を調達、配布先を決定。
	18:00 頃	厚生労働省初動対応チームが病院に到着、病院関係者、岡山県、岡山県警察本部、A 社、B 社が参加して全体会議を開催、調査を開始。
5/21	08:00 頃	初動対応チームがプリンターサーバーからランサムウェアを発見、Autorun 設定がされており、システム再起動時に、ランサムウェアも起動し再暗号化すること及び Windows Defender での検出、検疫を確認。
	08:30 頃	Virus Total で、発見されたランサムウェアが主要ウイルス対策ソフト 60 製品以上で検出、検疫できることを確認。
	10:00	ランサムウェアがウイルス対策ソフトで検出可能であることを受け、全体会議で以下の暫定復旧方針を確認した。 ① 外部接続点の特定と脆弱性管理の実施、当面、外部接続は遮断 ② 複数のウイルス対策ソフトでのスキャンの実施 ③ ウイルス対策ソフトのアンインストールパスワードの設定 ④ サーバー・端末の標準ユーザーでの運用 ⑤ 16 桁以上の長いパスワード設定 ⑥ リモートデスクトップ接続（RDP）ポートの変更とロックアウト ⑦ 管理者のロックアウト設定
	13:30 頃	個人情報保護委員会向け速報を提出。
	15:30 頃	ランサムウェア攻撃あることを病院ホームページで公表するとともに、プレスリリースの続報をリリース。
5/22		電子カルテ参照系中古サーバーを手配。端末は総入れ替えの方針を決定、手配を開始。
6/1		中古サーバーで電子カルテ仮稼働開。端末は新たに 50 台のノート PC を調達。
6/7	09:00 頃	病院長が岡山県警察本部で流出した要配慮個人情報を確認。
6/11	13:00 頃	岡山県庁で要配慮個人情報漏洩の記者会見を実施。病院内に相談窓口を設置。
6/20		電子カルテ用新サーバーを入手。
6/24~		電子カルテ用新サーバー及び追加の新端末 150 台（計 200 台）が稼働開始。 医療情報システムベンダー、医療機器ベンダーへの聞き取り調査を開始。
7/4		DWH からのデーター移行、検証が完了し、電子カルテの復旧。
8/17		サーバーストレージの入れ替えを実施し、電子カルテの完全復旧。

2023 年 11 月と 12 月及び攻撃の直前の 2024 年 5 月 14 日、5 月 15 日に Active Directory サーバーが原因不明で起動できないという障害を連続して起こしているが、この障害と本件事案との関連は不明である。ただし、外部からの何らかの攻撃があった可能性は否定できない。一般的に、Active Directory サーバーが連続して起動不可能になることは考えにくい。2023 年 12 月時点でインシデントを疑い、Windows ログの詳細な調査を行うべきであったといえる。

5.7 ランサムウェア及びランサムノート

5.7.1 ランサムウェア

ランサムウェアは 5 月 21 日朝に厚生労働省初動対応チームが Windows 物理サーバーで発見した。Virus Total[8] の評価では 60 を超すウイルス対策ソフトで検出、暗号化への防御が可能なものであった。Avast、AVG、BitDefender、ESET、McAfee、Sophos、Symantec、TrendMicro など、国内で販売されている主要なウイルス対策ソフトで検出が可能である。

VirusTotal によれば、主な機能として、システム起動時の自動実行、Windows パーソナルファイアウォールの設定変更、ブラウザーの資格情報の窃取、ファイルとディレクトリの検出、システム情報の窃取、ネットワーク共有の検出、追加プログラムのインストール、暗号化、Windows VSS[9]の削除などであり、暗号化と復旧を困難とするための一般的なランサムウェアの機能が実装されている。

5.7.2 ランサムノート（脅迫状）

ランサムノートの要旨は以下のとおりである。

> 様々な情報を窃取し、暗号化した。最善は我々にコンタクトすることである。
> ファイルを編集したり、シャットダウンすると復活が困難になる。
> 連絡がない場合、数日以内にデーターは公開される。
> （注：連絡先については onion[10]サイトの URL が記述されていた）

徳島県つるぎ町立半田病院のランサムウェア攻撃を行った攻撃者集団である LockBit は、コンピューターの暗号化を終えたのち、病院内の多数のディスプレイとプリンターに脅迫状を出力し、自身の攻撃を大々的に誇示したが、本件事案では、残存した一部の物理サーバーの特定フォルダーにのみテキストファイルと HTA ファイル[11] でランサムノートを保存したにとどまっている。これが、初動でのランサムウェア攻撃の発見遅れにつながったともいえる。

以下、まったくの憶測となるが、本件事案の暗号化において、ターゲットとなるコンピューターの管理共有（C$）に接続し、暗号化プログラムを実行する攻撃サーバーのリモートドライブとして暗号化をおこなっていたと考えた場合、ターゲットとなるコンピューターのウイルス対策ソフトを停止する必要がなく、また、リモートデスクトップ接続をしなくてすむことから、ランサムウェアや攻撃ツールの開発工数が減る反面、暗号を実施するランサムウェアは攻撃サーバーで実施されることから、複数のターゲットコンピューターを同時並行的に暗号化するには、攻撃サーバーの負荷が高くなり、全体の暗号化に時間がかかるという欠

---

[8] https://www.virustotal.com/gui/home/search、Google が運営するファイルや Web サイトのマルウェア検査を行う Web サイト。70 種類以上のウイルス対策ソフトを使用し検査を行い、どのウイルス対策製品が検出したかの一覧が表示される。

[9] Windows VSS: Volume Shadow Copy Service）。Windows に組み込まれている機能で、スナップショットと呼ばれる特定時点での Windows の静的なバックアップを行うものである。この機能を使うことにより、常時変化するデーターベースなどのバックアップに一貫性を持たせることが可能となる。

[10] TOR ブラウザーを使用して接続するサイト。この onion サイトにダークウェブが存在する。

[11] HTA: HTML Application の略。HTA ファイルは、Web ページのように HTML や JavaScript 等で構築されている。mshita.exe を使い表示・実行され、ブラウザーでは表示されない。一般用途では、ほとんど使用されていない。

点がある。こうした欠点を補うために、あえてランサムノートの表示を抑制的に行ったと考えることが可能である。

すべての攻撃対象でランサムノートを表示しない、という点で、ランサムウェア攻撃の発見が遅くなり、逆に被害が拡大する可能性が高まることが考えられる。拡張子の変更を伴う異常を認めた際は躊躇せず、LAN 抜線、全体的なネットワークの遮断を行うことを教訓とすべきではないか。

物理サーバーに関しては、再起動に備えてランサムウェアが自動起動するよう永続化が図られていたことが、フォレンジック調査で確認されている。共有ストレージの破壊と、ランサムノートの記述である「シャットダウンすると復活が困難になる」との因果関係はまったく不明であるが、ランサムウェア事案における初動対応でのシステムの再起動については、ランサムウェアによる再暗号化や、META データーの破壊に関連する可能性があることに留意すべきである。

5.8 復旧方針と再発防止策

フォレンジック調査によると初期侵入は 2024 年 5 月 13 日となっているが、大阪急性期・総合医療センターでは攻撃の半年前からの侵入が確認されていること、病院内のネットワーク情報と、Active Directory に登録されたサーバー・端末ユーザー情報、グループ情報は完全に窃取されていること、加えて、コンピューターの起動時の最初に動作する UEFI[12] の汚染の可能性が否定できず、再侵入用のバックドアの設置が十分にあり得た。

また、被害にあった基幹システムと電子カルテ端末のネットワークセグメントと、医療機器が接続されたネットワークセグメントの IP アドレスが異なるクラスであったためか、医療機器制御端末等の暗号化の被害は確認されなかった。しかし、徳島県つるぎ町立半田病院では、CT スキャナー、MRI の制御用 Windows 端末も暗号化されたことから、医療機器、医療機器制御端末については慎重な調査と復旧策が必要となった。このため、前述の通り阪急性期・総合医療センターより「インシデント発生時の初期化判断基準」等の各種復旧対策資料の提供を受け、これらを参考に、ログの確認、システムの改ざんの形跡、不審なプログラムの存在の確認、複数のウイルス対策ソフトでのチェック等を実施し、改ざん等が疑われた際は、初期化することとした。なお、医療機器のネットワーク接続は、医療情報システムの完全復旧までオフラインで稼働とした。

基幹システムは、オフライン・バックアップからの復旧が不可能であったため、前述のとおり、侵害された共有ストレージの META 情報の復旧を試みるとともに、並行して、新規にサーバーを調達し、暗号化されていなかった DWH からの復元を行うこととした。繰り返しになるが、ランサムウェア自体は、ウイルス対策ソフトで検出が可能であったことから、最終的に、以下の方針を定め復旧作業にあたった。

[12] UEFI : Unified Extensible Firmware Interface。コンピューターの電源を入れた直後に起動し、ハードウェアを初期化し、ハードディスクや SSD から OS を読み込んで起動するためのソフトウェア。コンピューターと OS の橋渡しをする機能を提供する。

① **再侵入、再侵害の防止：**完全復旧までは、外部通信をすべて遮断し、再侵入、再侵害を防ぐ。すべてのサーバー、端末の（UEFI を含む）システムの完全な初期化、もしくは、新規導入による入れ替えを実施し、クリーンなシステムでの再構築を実施する。後述の技術的対策を確実に実施する。

② **早期電子カルテの稼働：**新品のサーバーの手配は数か月かかる可能性があり、当面、中古サーバーを調達し電子カルテを稼働、その後、新たなサーバーを入手し電子カルテの完全復旧を目指す。復旧にあたっては、管理者権限の付与は行わず標準ユーザーでの稼働を要件とする。

③ **医療機器・関連端末の復旧：**なんらかの攻撃があったことを前提に、可能な場合はシステムの初期化、初期化が不可能な場合は、医療機器ベンダーによる設定ファイルやログの詳細調査を行い、完全性、真正性を確認できた場合は、異なるウイルス対策ソフトでのスキャンを実施し、異常がなければ再稼働を許可する。電子カルテの復旧まではネットワークから切り離し運用し、医用画像等は機器本体で確認する。

④ **再発防止策の策定：**技術的対策、組織的対策、人的対策を策定し、速やかに実施する。

5.8.1 技術的対策

本件事案は、VPN 装置等の脆弱性、推測可能な資格情報の使用、資格情報の使いまわしなど、技術的な脆弱性、脆弱な設定と運用が引き起こしたものであり、これらの是正が最も重要となった。実際の対策では、侵入防止策、水平展開防止策、情報漏洩防止策、部門システム・医療機器脆弱性対策に分けて策定した。基本的に、セキュリティ製品の新規導入よりも、ネットワーク機器や Windows の強化設定で防御できるものを活用し、多層防御を構成した。詳細については、「7. 詳細編 復旧について」を参照されたい。

項目	課題・脅威	状況	実施策
侵入防止策	VPN 装置の脆弱性の放置、弱い資格情報の使用	実施済	NTT 東日本-IPA シン・テレワークシステム[13]による多要素認証、接続元制限の実施。
	Built-In Administrator の利用停止	実施済	Built-In Administrator は使用を停止、すべての管理者は個別ユニークな ID とし、16 桁以上のパスワードを設定。
	リモートデスクトップ接続の悪用	実施済	通信ポートの変更、接続元制限及びロックアウト設定。
	サーバー・端末ユーザーへの管理者権限の付与	実施済	電子カルテシステムを改修し、標準ユーザーでの運用を可能とした。
	ベンダー独自の VPN 装置の存在	実施済	Firewall の刷新と接続元 IP アドレス制限の実施。
	アカウントロックアウトが未設定	実施済	5 回連続して認証失敗でロックアウトする。
	多要素認証が未導入	実施済	電子認証局の導入及び管理者用スマートカードログオンの実施、Windows Hello for Business の導入。
	攻撃者 X によるバックドアの設置	実施済	サーバー、端末の総入れ替え、医療機器への複数のウイルス対策ソフトでの検査の実施及び一部初期化。
	ウイルス対策ソフトのリアルタイム保護が未活用	実施済	Firewall で Microsoft Defender ウイルス対策の通信を許可し、リアルタイム保護を実施。ASR 規則[14]による「ランサムウェアに対する高度な保護を使用する」を設定。
	VBA マクロウイルス対策がなされていない	実施済	VBA マクロへの電子署名の実施、未署名 VBA マクロの実行禁止。
	セキュアな DNS リゾルバが未使用	実施済	Quad9 による悪意のあるドメイン名へのアクセスをブロック。

[13] https://telework.cyber.ipa.go.jp/news/

[14] https://learn.microsoft.com/ja-jp/defender-endpoint/attack-surface-reduction-rules-reference

項目	課題・脅威	状況	実施策
水平展開防止策	Windows Update を実施していない	実施済	一時的に WSUS 導入による脆弱性管理の実施し。現在は、Firewall で Windows Update 関連の通信を許可。
	局所化が困難なネットワーク構成	実施済	システム毎に VLAN を構築し、マイクロセグメント化を実施。
	攻撃証跡取得のための Syslog サーバーが設置されていない	導入中	Syslog サーバーを設置、Firewall、VPN 等の Syslog を受信、1 年間保存。
	脆弱な Windows の既定値	実施済	CIS Benchmark[15]による Group Policy 強化設定の実施。アカウントポリシー、サーバー・端末ユーザー権利の割り当て、セキュリティオプション、管理用テンプレートの設定、ASR、ログ設定等、300 項を変更。
情報漏洩防止策	有線・無線 LAN が 802.1X 未対応	計画中	ADCS による電子証明書ベースの 802.1X EAP-TLS の導入予定。
	非暗号化ソケット通信の存在	一部、実施済	一部システムで、ソケット通信の暗号化を実施、順次、暗号化通信への切り替えを予定
	HTTP（平文）通信の存在	実施済	一部の医療機器、薬局システム、栄養システムでは、VLAN 化、パーソナル Firewall による通信制限を実施。HTTPS 通信への改修を申し入れ中。
	ライツマネジメントが未導入	導入計画中	Office 文書の暗号化及び読み込み制限
部門システム・医療機器脆弱性対策	サポート切れブラウザーの使用	実施済	IE の利用を停止し、Edge への切り替えを実施。
	サポート切れ OS の使用	一部、実施済	OS のアップグレードを実施。 アップグレードが困難な機器については入れ替えを計画中。接続元・接続先 IP アドレス制限と必要最小限の通信ポートの許可。
	保守用 VPN 装置の OS が古い	実施済	OS のアップグレードを実施。
	一部、医療機器で脆弱なプロトコル SMBv1 が明示的に禁止できていない	実施済	Firewall で院内の SMBv1 通信を禁止。
	部門システムがドメインに参加していない	一部、実施済	薬剤系 1 社、検査系 2 社、栄養系 1 社、放射線科 2 社をドメイン参加し、WSUS 対応を実施。
	医療機器の Windows Update が未実施	一部、実施済	アクティブスキャンによる脆弱性の検出とベンダーによる是正、不要なポートを閉じる。USB 型ウイルススキャナーによるスキャンの定期的実施。

基幹システム脆弱性対策

電子カルテ、医事会計、オーダーリングシステムについては、システムの設定状況の調査と、ベンダーの聞き取り調査を実施した。Windows Update の定期的な実施、管理者権限での稼働を禁止するため、電子カルテのプログラムの修正を依頼し、標準ユーザーでの稼働を実施した。また、基幹システムと部門システム、医療機器へのネットワーク構成については、全面的に見直しを行い、すべてのシステム間で VLAN を設定、盗聴やなりすまし、脆弱なプロトロルの悪用が困難となる構成とした。なお、ウイルス対策ソフトは Windows Defender ウイルス対策とし、Defender 関連のインターネット通信を Firewall で許可し、リアルタイム保護と攻撃面の縮小ルールである「ランサムウェアに対する高度な保護を使用する」機能を有効とした。

[15] CIS（Center for Internet Security）は、2000 年に米国政府と民間で設立された NPO で、米国政府機関、自治体、企業、教育機関などが利用できるセキュリティのベストプラクティスやガイドラインの開発、提供を行っている。

部門システム脆弱性対策

病院設置の部門システムとしては、オーダーリング給食システム、調剤支援システム、薬剤管理指導業務支援システム、精算機システム、資産管理サーバー、BI ツールサーバー、診断書作成管理システム、WEB データーベースサーバー、AI 診療支援システム等があった。2024 年 6 月以降、電子カルテベンダーと共にベンダー各社との協議を行い、OS のアップデートもしくはアップグレード、リモート保守の有無と方式、管理者権限の付与、パスワードの桁数、使用している通信ポート等のヒヤリングを実施した。

サポート切れ OS のアップグレードが困難な機器については入れ替えを計画し、入れ替え完了までは、VLAN の設定とパーソナル Firewall の設定による、接続先・接続元 IP アドレス制限等の通信の厳格管理と、USB 型ウイルススキャナーによる定期的なウイルススキャン、ログ監視を実施することとした。

多くの部門システムのシステムへのログオンパスワードの桁数が 4 桁、5 桁といった攻撃が容易なものが存在したため、16 桁以上のパスフレーズへの是正を求めた。また、ファイル共有等で使用する Windows 資格情報（ID、パスワード）をプログラムに直接記述するものもあり、設定ファイルに暗号化して保存するなどの改善を求めた。

また、診断書作成管理システムは、推奨のブラウザー設定を実施することで、当該端末のセキュリティレベルが著しく低下することから、継続使用を見送った。

医療機器脆弱性対策

病院設置の医療機器としては、X 線検査装置、CT、MRI、超音波診断装置、脳波計、心電図システムなどがあり、これらは、HIS 系ネットワークとは異なるクラスの IP アドレスであったためか、暗号化については免れていた。とはいえ、何らかの攻撃やバックドアの設置は可能性が十分あることから、慎重な調査を実施した。その際、大半の機器、制御端末で Windows Update が実施されていないことが判明した。攻撃側の手順として、アクティブスキャンによる脆弱性を確認し、それを悪用することが考えられたため、実際にアクティブスキャンを実施し、外部からの脆弱性情報の取得を試みた。結果は以下のとおりである。

機器	脆弱性識別子	脆弱性の概要	対策
CT 本体	CVE-2017-0143	脆弱な SMBv1 が有効、接続しただけでプログラムのリモート実行が可能	■ Firewall による医療機器セグメントでの SMBv1 の停止 ■ パーソナル Firewall による通信先の限定と不要なポートの停止、RDP ポートの変更とロックアウト設定 ■ SSL 3 .0 の停止 ■ 可能な場合、脆弱性アップデートの実施 ■ 機器の入れ替え ■ 各機器でのウイルス対策ソフトの稼働と USB ポータブルウイルス対策スキャナーでの定期的なスキャンの実施 ■ アプリケーションのバージョンアップ ■ 機器と端末間を専用ネットワークとし、他のシステムとの通信を停止
画像サーバー	CVE-2014-3566 "POODLE"	脆弱な SSL3.0 により平文データーを取得される脆弱性	
画像管理 PC	CVE-2017-0143	脆弱な SMBv1 が有効、接続しただけでプログラムのリモート実行が可能	
X 線制御 PC	CVE-2014-3566 "POODLE"	脆弱な SSL3.0 により平文データーを取得される脆弱性	
	CVE-2017-0143	脆弱な SMBv1 が有効、接続しただけでプログラムのリモート実行が可能	
画像診断 PC	CVE-2017-0143	脆弱な SMBv1 が有効、接続しただけでプログラムのリモート実行が可能	

脆弱性が発見された機器については、各ベンダーと打ち合わせを実施し、アップデートの実施を依頼したが、一部、脆弱性アップデートは困難との回答があったため、これらについては機器の更新まで、部門システムと同様の措置を講じ、VLAN の設定、パーソナル Firewall による通信の厳格化を行い、外的な影響が及びにくい構成とした。なお、これらについても、USB 型ウイルススキャナーでの定期的スキャンを継続的に実施している。

保守用に独自の VPN 装置を設置しているベンダーに関しては、脆弱性の是正に併せて、接続元 IP アドレス制限や、長いパスワードの使用、管理用インターフェースの制限、不要なポートの停止を求めた。

ベンダーのセキュリティポリシーについて

今回のヒヤリングを通じて、電子カルテベンダー、部門システムベンダー、医療機器ベンダーが、医療情報システムは「閉域網」であるからウイルスに感染しない、「閉域網」であるから脆弱性を放置しても大丈夫という意識を未だに持ち続けていることを確認した。インターネットから攻撃可能な VPN 装置が病院内に存在しても病院情報システムは「閉域網」であるという前提を固持し、脆弱性対策やセキュリティ設定は実施しないという考え方である。あくまで、自社製品の正常稼働を妨げないような独自のポリシーを適用し、納品、運用がなされている。

これは、発注者たる病院側に第一義的な責任があり、本来、厚生労働省ガイドラインや、病院が求めるセキュリティポリシーを提示し、それに見合う製品、システムを導入すべきである。その意味で、ベンダーにセキュリティポリシーや脆弱性管理を丸投げしている病院の責任は非常に重いといわざるを得ない。

一方で、ベンダー側もコロナ禍以降、リモート保守による省力化のために VPN 装置を病院に設置してきたという経緯がある。そもそも、VPN 装置が存在しなければ、「閉域網」に穴は開いておらず、病院におけるランサムウェア事象は発生しなかったはずである。その意味で、「閉域網に穴を開ける」VPN 装置に関しては、主たる利用者であるベンダーが、率先して病院とセキュリティ対策について協議を行うべきであった。その上で、いずれかの責任において VPN 装置の脆弱性管理を明確化し、その責任を果たすべきであったといえる。

徳島県つるぎ町立半田病院、大阪急性期・総合医療センターにおいて、まったく同様の指摘があったにも関わらず、同様の事案が発生した。未だに、全国の多くの病院やベンダーにおいて「閉域網に穴をあける」VPN 装置の脆弱性管理の重要性が認識されておらず、また、その対策がなされていない可能性が高いことを指摘したい。

5.8.2 組織的対策

組織的対策としては、基本的な考え方として ISO/IEC 27002:2022（情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策）を援用し、管理策を策定することとし、組織的対策の実施計画を策定中である。

課題・脅威	状況	実施策
HIS 系での USB メモリの厳格運用	実施済	ウイルス対策ソフト内蔵型 USB メモリのみ利用を許可。HIS 系へのファイルの持ち込み、持ち出しは、すべて IT 担当者が複数のウイルス対策ソフトでスキャンを確認する。
組織的な IT ガバナンスの欠如 情報セキュリティ規程の見直し	整備中	医療情報システム安全管理委員会を設置し、規程の見直しを計画。 ISO27002：2022 5.1~5.8、5.14~5.18 を援用。

課題・脅威	状況	実施策
システム管理台帳の不在	実施中	システム管理台帳（機器名、IP アドレス、接続先制限、VLAN、脆弱性情報入手先、脆弱性対策適用状況、サポート状況及びサポート切れ等）の整備。ISO27002：2022 5.9~5.11 を援用。
データー分類、ラベル付け基準の策定とアクセス制御等	策定中	データー分類、ラベル付けによるデーターの暗号化、保存、廃棄手順の策定。ISO27002：2022 5.12~5.13、5.14~5.18 を援用。
部門システムベンダー、医療機器ベンダーへのセキュリティ対策ヒヤリングの実施と是正	一部、実施済	すべての部門システムベンダー、医療機器ベンダーへのセキュリティ体制、脆弱性管理に関するヒヤリングを実施、脆弱性管理に対する管理強化を要請済み（一部、ベンダー未対応）。3 省 2 ガイドライン及び ISO27002：2022 5.19~5.23 を援用。
ベンダーとの契約の見直し	一部、実施済	仕様書のセキュリティ仕様の厳格化と、厚労省医療情報システムの契約における当事者間の役割分担等に関する確認表、3 省 2 ガイドライン遵守の要求。検収時の、設計書・手順書・設定報告書の厳格チェック、受入試験での実施確認。ISO27002:2022 5.31~5.32、5.37 を援用。
IT-BCP の策定	策定中	大阪急性期・総合医療センターの IT-BCP をベースに病院 BCP との整合性を図り策定を実施する。ISO27002:2022 5.24~5.30 を援用。

組織的な IT ガバナンスの欠如

以下の ISO/IEC 27002:2022 を援用し、IT ガバナンスの確立と強化を目指し、規程の見直し、運用の見直しを整備中である。

5.1 情報セキュリティに関する方針群、5.2 情報セキュリティの役割及び責任、5.3 職務の分離、5.4 経営陣の責任、5.5 関係当局との連絡、5.6 専門組織との連絡、5.7 脅威インテリジェンス、5.8 プロジェクトマネジメントにおける情報セキュリティ。

システム管理台帳

以下の ISO/IEC 27002:2022 を援用し、システム管理台帳の作成と、定期的な更新を実施中である。

5.9 情報及びその他の関連資産の目録、5.10 情報及びその他の関連資産の利用の許容範囲、5.11 資産の返却。

データー分類、ラベル付け基準の策定とアクセス制御等

以下の ISO/IEC 27002:2022 を援用し、情報セキュリティの要求に従った分類、情報分類体系の策定とアクセス制御に関する規程を整備中である。

5.12 情報の分類、5.13 情報のラベル付け、5.14 情報転送、5.15 アクセス制御、5.16 識別情報の管理、5.17 認証情報、5.18 アクセス権。

部門システムベンダー、医療機器ベンダーへのセキュリティ対策ヒヤリングの実施と是正

厚労省ガイドライン　第 6.0 版（令和 5 年 5 月）、2 省ガイドライン 第 1.1 版（令和 5 年 7 月改定）及び以下の ISO/IEC 27002:2022 を援用し、ICT サプライチェーンのセキュリティ体制の整備を実施中である。

5.19 供給者関係における情報セキュリティ、5.20 供給者との合意における情報セキュリティへの取扱、5.21 ICT サプライチェーンにおける情報セキュリティの管理、5.22 供給者のサービス提供の監視，レビュー及び変更管理、5.23 クラウドサービス利用における情報セキュリティ

ベンダーとの契約の見直し

厚生労働省医療情報システムの契約における当事者間の役割分担等に関する確認表、厚労省ガイドライン第 6.0 版（令和 5 年 5 月）、２省ガイドライン 第 1.1 版（令和 5 年 7 月改定）に基づき契約を見直す。また、以下の ISO/IEC 27002:2022 を援用、ベンダーとの契約の見直しを実施中である。
5.31 法令，規制及び契約上の要求事項、5.32 知的財産権、5.37 操作手順書。

IT-BCP の策定

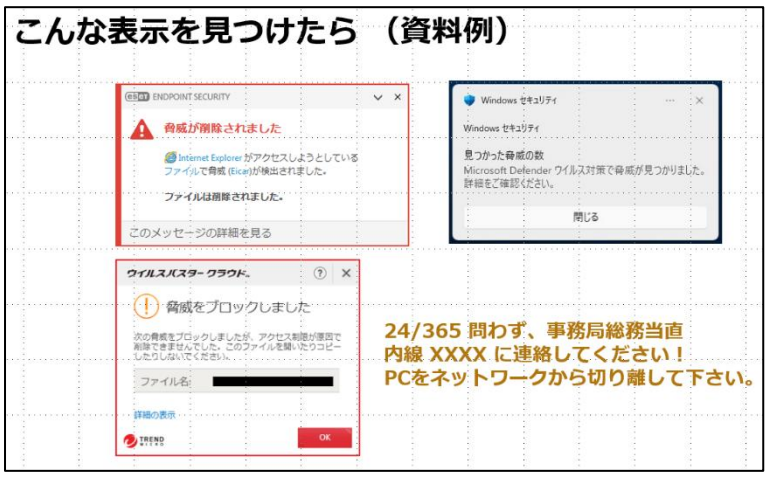
大阪急性期・総合医療センターの IT-BCP を参照し、病院の BCP との整合性を図る。また、以下の ISO/IEC 27002:2022 を援用し、IT-BCP を策定中である。
5.24 情報セキュリティインシデント管理の計画及び準備、5.25 情報セキュリティ事象の評価及び決定、5.26 情報セキュリティインシデントへの対応、5.27 情報セキュリティインシデントからの学習、5.28 証拠の収集、5.29 事業の中断・阻害時の情報セキュリティ、5.30 事業継続のための ICT の備え。

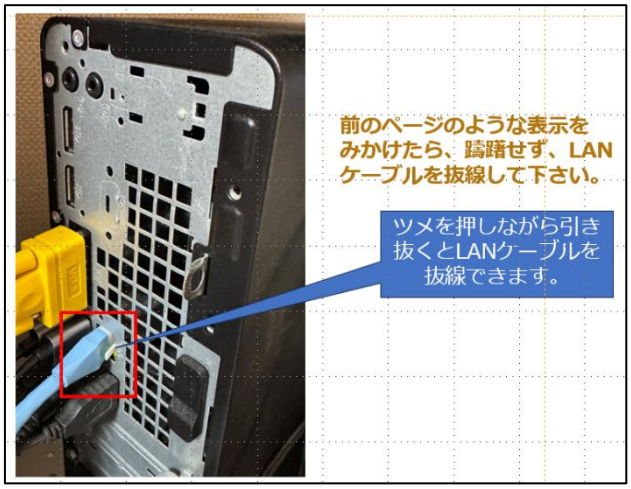
5.8.3 人的対策

人的対策としては、定期的なセキュリティ教育の実施と、脅威情報の共有を実施することとした。脅威情報の入手先としては、JPCERT/CC、CISA、CIS、MITRE とし、攻撃事例や初動対応の訓練を中心に教育コンテンツ策定を行うこととした。

課題・脅威	状況	実施策
定期的な脅威情報、攻撃手法の教育が実施されていない	実施予定	半期に一度をめどに、最新のフィッシング、ランサムウェア攻撃事例を共有し、異常時の LAN 抜線、無線 LAN 停止や保全、平時のウイルス対策ソフトの最新化やスキャンの実施手順を教育する。
ランサムウェア攻撃等初動対応教育が実施されていない	実施予定	年 1 回をめどに、IT スタッフ、病院幹部に対して、ランサムウェア攻撃、ウイルス感染における初動対応、IT-BCP 発動に関するシミュレーションやトレーニングする。
システム脆弱性情報及び対策案が共有されていない	整備中	IT スタッフ、関連ベンダーにシステム脆弱性情報の共有を実施する。

ランサムウェア事案やウイルス感染事案は、特にユーザーサイドの初動対応が重要である。そのため、どのような状況でユーザーが何をなすべきかを明確化した資料を作成中[16]である。





また、ランサムウェア事案では、外来の停止や入院患者の転院など、病院幹部に対して病院経営上の重大な判断を求められる。さらに、手書きカルテ運用を含めた医療継続と、医療情報システムの復旧という複数のプロジェクトの実施が求められる。そのため、幹部向けの IT-BCP 発動に関する考え方や、実際のインシデントを模擬したシミュレーションやトレーニングの実施を計画中である。

5.9 概要編まとめ

閉域網という境界型セキュリティは、閉域網が強固に守られていれば安全である。問題は、この閉域網に VPN という外部接続点を設けながら、そのリスクを評価してこなかった状況にある。VPN 接続によるリモート保守は、病院、ベンダーにとって様々なメリットをもたらすが、悪意ある第三者の侵入口となり得ることを現実として考えるべきであった。

インシデント発生後、復旧対策における医療情報システムベンダー及び医療機器ベンダー12 社への聞き取り調査でも、「病院は閉域網であるから安全である」という前提のもと、Windows Update の未実施、脆弱性のあるプロトコルの使用や、資格情報のハードコーディング、未使用ポートの放置が多数確認された。さらに、「3 省 2 ガイドライン」、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」を熟知している担当者はごくわずかであったことを報告する。残念ながら、医療関係者とベンダーが自ら作り上げた閉域網神話によって、社会一般においてごく当然に行われているセキュリティ対策や脆弱性対策が放置されている。そのため、医療関係者もベンダーもセキュリティ知識が向上しない、という悪循環に陥っている、といわざるを得ない。

---

[16] 大阪急性期・総合医療センター IT-BCP を参考した。https://www.gh.opho.jp/incident/2.html

病院はインシデント発生後の 2024 年 6 月に、医用画像管理システムの更改を企図し、ある医療情報システムベンダーに提案を求めたところ、その医用画像管理システムベンダーはサポートが終了した OS[17] を組み込んだ製品を公然と提案してきた。医療という社会生活に欠かせない重要インフラを担う、という意識がないベンダーが我が国の医療界には存在していることに留意すべきである。

本件事案は厚労省ガイドラインを遵守していれば十分に防げたものであった。しかし、ガイドラインに準拠していない組織であるならば、どこでも発生し得るものであり、決して対岸の火事ではないことを強調したい。病院のインシデントを、明日にでもご自身に降り注ぐ危機と捉え、以下の調査と是正措置を推奨する。

- ✓ **初期侵入の防止：**VPN 装置の脆弱性対策の実施
  月次で脆弱性情報を入手し、最新の脆弱性修正プログラムが適用されていることを確認する、もしくは、自動更新の設定の有無を確認し、自動更新を設定する
- ✓ **初期侵入の防止：**VPN 接続に使用している ID、パスワードを推測困難なものにする
  P@ssw0rd などのよく利用されるものを禁止する
  パスワードは 16 桁以上のパスフレーズを採用するなど、なるべく長いものにし、繰り返しやキーボード配列などが使用されていないことを確認する
  パスフレーズの例：
  Hahatanjoubisangatu → 母誕生日三月：19 桁
  asaborakeariakenotukito → 朝ぼらけ有明の月と：23 桁
  meishoubizenkourakuen → 名勝備前後楽園：21 桁
- ✓ **管理者権限の限定的付与：**一般ユーザーは標準ユーザーで運用する
  管理者権限が必要なアプリケーションは、是正、刷新を検討するとともに、使用するサーバー、端末を限定する
- ✓ **特権昇格の防止、水平展開の防止：**Windows Update の実施
  月次で Windows Update を必ず実施する
- ✓ **水平展開の防止：**Windows の管理者パスワードの使いまわしの禁止
  1 台ごとに管理者パスワードをユニークにする（コンピューター名＋フレーズを組み合わせる等）
- ✓ **個人情報漏洩防止：**個人情報が入ったファイルは暗号化、パワードを設定する
- ✓ **事業継続維持：**重要なシステムのオフライン・バックアップの取得、バックアップからの復旧のテストの実施

なお、EDR/XDR 等のセキュリティ製品の導入を行っても、電子カルテシステム等が「管理者権限」を必要とする場合は、悪意ある攻撃者によって EDR/XDR の無効化される可能性がある。これらの導入にあたっては、管理者権限が付与された状態での EDR/XDR の無効化ついて、ベンダーに確認する必要がある。ま

[17] Cent OS 7、2024 年 6 月サポート終了。https://www.redhat.com/ja/topics/linux/centos-linux-eol#:~:text=%E3%82%92%E9%81%B8%E3%81%B6%E7%90%86%E7%94%B1-,%E6%A6%82%E8%A6%81,EOL)%20%E3%82%92%E8%BF%8E%E3%81%88%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82

た、UTM/次世代 Firewall の導入を行っても、リモートデスクトップ接続された場合は、リモートデスクトップ接続の通信自体が暗号化されているため、UTM/次世代 Firewall によるランサムウェアやウイルスの検知は不可能である。UTM/次世代 Firewall は、あくまで Web サイトからのファイルのダウンロード等で有効であることに留意頂きたい。

EDR/XDR、UTM/次世代 Firewall の導入にあたっては、その効果を無効化もしくはバイパスする設定について、ベンダーに確認の上、確実な是正措置を講じるとともに、上記対策を実施の上で導入し、多層防御の一環として位置づけることを強く推奨する。

6　詳細編：推測攻撃経路および手順

本項では、再侵入・水平展開の防止や、確実な復旧対策を講じるために、物理サーバーのフォレンジック調査を基に、攻撃者 X が行ったと思われる手順や、推測される行動をまとめた。これは、あくまで復旧対策でのリスク想定のために作成したものであり、実際の攻撃とはかけ離れた推測も含まれることに留意願いたい。

6.1 初期侵入~探索

物理サーバーのフォレンジック調査で判明している最初の侵入は、2024 年 5 月 13 日 2:41 のリモートデスクトップ接続によるものである。フォレンジック調査では、暗号化までの 1 週間弱、データーセンターの SSL-VPN 装置を経由し、複数回の病院内のネットワークスキャン、情報窃取、攻撃用ツールの設置を行っていることが判明している。ネットワークスキャンツールは、都度、アンインストールし、取得した情報も消去するなどしており、慎重に病院内の情報の取得を行っていたことが判明している。

これらの攻撃とは別に、2023 年 11 月と 12 月、2024 年 5 月 14 日と 5 月 15 日に AD サーバーが起動しないという事象が発生し、それぞれ、バックアップから復旧している。本件事案とは異なる別な攻撃が存在した可能性があるが、ログ等はなく、詳細は不明である。

6.2 認証情報窃取

5 月 16 日から 18 日にかけて AD サーバーの認証情報の窃取、バックアップデーターの削除等が確認されている。

6.3 水平展開~暗号化

水平展開~暗号化では、5 月 19 日 13:10 から 17:34 にかけて、ランサムウェアによる暗号化が実施されている。同時刻にかけて、暗号化された端末のセキュリティログに「Event ID:4624 アカウントが正常にログオンしました。ログオンタイプ：3（ネットワーク）」が多数発見されたこと、暗号化された端末はリモートデスクトップ接続が無効に設定されていた[18]こと、PSEXEC、WMI、PowerShell 等の使用痕跡が認められないことから、管理共有（C$）へのリモート接続が使用された可能性が高い。

AD サーバーでは、ウイルス対策ソフトである TrendMicro Office Scan Client のファイルがすべて削除されており、再起動時のウイルス対策ソフトの起動を阻む攻撃が確認された。また、診療所サーバーでは、「Microsoft Defender ウイルス対策を無効にする」が有効にされており、このほか、以下の Defender ウイルス対策ソフトの機能が無効にされていた。

- ✓　「リアルタイム保護を無効にする」
- ✓　動作の監視を有効にする
- ✓　すべてのダウンロードファイルと添付ファイルをスキャンする

[18] Windows レジストリで禁止されていた。HKLM¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server¥DenyTSConnections:1(DWORD)

- ✓ コンピューターのファイルおよびプログラムの動作を監視する
- ✓ リアルタイム保護を無効にする
- ✓ リアルタイム保護が有効な場合は常にプロセスのスキャンを有効にする
- ✓ ’事前ブロック’ 機能を構成する
- ✓ Microsoft MAPS に参加する
- ✓ 詳細な分析が必要な場合はファイルのサンプルを送信する

以下の表は、フォレンジック調査報告書に記載された事象と、過去のランサムウェア攻撃事例を参考に、復旧方針立案のために攻撃者 X の手順や行為を推測したものである。特に断りがない場合は、フォレンジック調査報告書に基づく。

日時	項目	攻撃者Xの推測される手順や行為
不明	X が SSL-VPN 装置から侵入	（推測）データーセンターにB社が設置した SSL-VPN 装置の推測可能だった弱い ID・パスワード情報を用いて病院ネットワークに侵入、もしくは SSL-VPN 装置の脆弱性の悪用。端末、サーバー等への辞書攻撃やネットワークスキャンの実施。
2024/5/13 02:41	AD サーバー1を経由した本院サーバーフォルダーへのアクセス	その後、04:15までADサーバー1号機のバックアップフォルダーを探索。
5/14 08:35	AD サーバー1、AD サーバー2が起動しない事象、バックアップから復旧	（推測）本件事案との関連は不明、他の攻撃も考えられる。
5/14 22:56	AD サーバー1にリモートログオン	ネットワークスキャナーを設置。
5/14 23:04	AD サーバーから病院内ネットワークの探索	AD サーバーからネットワークスキャナーを使用し、病院内ネットワークを探索。攻撃用のツールの設置。
5/15 03:36	PSEXEC をインストール	ログローテートにより PSEXEC 使用等の詳細は不明。
5/15 08:06	AD サーバー1、AD サーバー2が起動しない事象が再発、再度、バックアップから復旧	（推測）本件事案との関連は不明、他の攻撃も考えられる。
5/15 16:32~20:58	AD サーバー1のバックアップフォルダーの探索	（推測）AD サーバーの本院サーバー、診療所サーバーのバックアップデーターのリストを作成。
5/16~5/18	共有フォルダー内の Office 文書等の窃取	（推測）病院共有フォルダーにアクセスし、医事情報、行政調査情報、病棟ケア会議の議事録等の Office 文書、PDF等を窃取。
5/17 22:27	PSEXEC をインストール	ログローテートにより PSEXEC 使用等の詳細は不明。
5/18 22:08~ 5/19 03:14	AD　サーバー1の認証情報の窃取	サービスをインストールし、comsvcs.dll を使い、LSASSメモリ[19]の認証情報を窃取した。（ADサーバー1の System.evtx に基づく）
5/19	AD サーバーから各サーバーのバ	バックアップデーターを削除。

[19] LSASS (Local Security Authority Subsystem Service)は Windows の認証を司るプロセスで、ユーザーのパスワードハッシュや認証トークンが一時的に保存される。

日時	項目	攻撃者Xの推測される手順や行為
03:05~06:28 12:39~12:49	ックアップデーターへのアクセス	
5/19 12:54	AD サーバーの TrendMicro Office Scan Client のフォルダーアクセス	ファイルの削除。 （推測）前後で TrendMicro Office Scan Client のサービスを停止。
5/19 14:31~14:33	Active Directory 情報の窃取	サーバー・端末ユーザー、コンピューター、ADサブネット、グループ等の情報を窃取。
5/19 14:42~14:43 14:46~14:47 16:20~16:21	仮想環境サーバー（物理）3台及び仮想環境管理ツールに対するWebアクセス	（推測）VMWare ESXi サーバーの捜索？
5/19 13:10～23:08	サーバー、端末の管理共有のマウントと暗号化 一部サーバーにランサムノート（脅迫状）を表示	Active Directory サーバー、プリンターサーバー、本院サーバー、診療所サーバー、端末の管理共有（C$）をマウント。 （推測）ウイルス対策ソフトを停止し、ランサムウェアによる暗号化を実施。 ランサムノート（脅迫状）は一部のサーバーにのみ表示されていた。DWH サーバーが攻撃を免れた理由は不明。
	ランサムウェアの Autorun 設定	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run に発見された検体を自動起動設定
	Chrome ブラウザーのインストールとサイトの閲覧	C:¥Users¥xxxx¥Downloads¥ChromeSetup(1).exe ESXi、vSphere、IIS、Fortigate への閲覧を実施。
	仮想基盤の暗号化	SSH 接続による VMWare ESXi サーバーのデーターストアのマウントと暗号化を実施。

今回の攻撃では、ネットワークスキャンやバックアップの探索、情報の窃取等は攻撃者 X 自身がリモートデスクトップ接続を経由して行われており、暗号化はランサムウェアが自動的に行ったと考えられる。

6.4 推測される攻撃の一覧と緩和策

以上のことから、実際の攻撃と推測される攻撃を、国際的な攻撃手法のナレッジベースである米国 MITRE ATT&CK の類型に割り当て、MITRE による推奨緩和策を、以下のように抽出し、復旧方針立案の参考とした。

攻撃分類	MITRE ATT&CKテクニック	MITRE による推奨緩和策
初期侵入	**VPN 接続** T1133: External Remote Services	**M1035：ネットワーク経由のリソースへのアクセスを制限する** VPN やその他の管理されたリモート アクセス システムなどの集中管理されたコンセントレータを通じてリモート サービスへのアクセスを制限する。 **M1032：多要素認証** リモート サービス アカウントには強力な 2 要素認証または多要素認証を使用して、盗まれた資格情報を悪用する攻撃者の能力を軽減するが、一部の 2 要素認証実装では多要素認証傍受手法に注意する。 **M1030：ネットワークセグメンテーション** ネットワーク プロキシ、ゲートウェイ、ファイアウォールを使用して、内部システムへの直接のリモート アクセスを拒否する。
	リモートデスクトップ（RDP）接続 T1563.002: Remote Service Session Hijacking: RDP Hijacking	

攻撃分類	MITRE ATT&CKテクニック	MITRE による推奨緩和策
永続化	**ランサムウェアの自動起動** T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	このタイプの攻撃手法は、システム機能の悪用に基づいているため、予防的制御では簡単に軽減できない。
水平展開	**SSH 接続** T1563.001: Remote Service Session Hijacking: SSH Hijacking	**M1042：機能またはプログラムを無効化または削除する** 誤用を防ぐために、この機能を明示的に必要としないシステムではエージェント転送が無効になっていることを確認する。 **M1027：パスワードポリシー** SSH キー ペアに強力なパスワードが設定されていることを確認し、適切に保護されていない限り、ssh-agent などのキーストア テクノロジの使用を控える。 **M1026：特権アカウント管理** root またはその他の特権アカウントとして SSH 経由のリモート アクセスを許可しない。 **M1022：ファイルとディレクトリの権限を制限する** 適切なファイル権限が設定されていることを確認し、システムを強化してルート権限の昇格の機会を防止する。
水平展開	**RDP 接続** T1563.002: Remote Service Session Hijacking: RDP Hijacking	**M1047：監査** リモート デスクトップ ユーザー グループのメンバーシップを定期的に監査する。リモート デスクトップ ユーザー グループから不要なアカウントとグループを削除する。 **M1042：機能またはプログラムを無効化または削除する** 不要な場合は RDP サービスを無効にする。 **M1035：ネットワーク経由のリソースへのアクセスを制限する** リモート デスクトップ ゲートウェイを使用する。 **M1030：ネットワークセグメンテーション** ファイアウォール ルールを有効にして、ネットワーク内のネットワーク セキュリティ ゾーン間の RDP トラフィックをブロックする。 **M1028：オペレーティング システムの構成** GPO を変更して、セッションのタイムアウトを短くし、単一のセッションがアクティブになる最大時間を定義する。GPO を変更して、切断されたセッションが RD セッション ホスト サーバー上でアクティブのままになる最大時間を指定する。 **M1026：特権アカウント管理** RDP 経由でログインできるグループのリストからローカルの Administrators グループを削除することを検討する。 **M1018：ユーザーアカウント管理** リモート アクセスが必要な場合は、リモート ユーザーの権限を制限する。
	PSEXEC のインストール T1570: Lateral Tool Transfer	**M1037：ネットワークトラフィックをフィルタリングする** SMB などのファイル共有通信を制限するためにホストファイアウォールの使用を検討する。 **M1031：ネットワーク侵入防止** ネットワーク侵入検知および防止システムは、ネットワーク署名を使用して特定の敵対的マルウェアのトラフィックや、FTP などの既知のツールやプロトコルを介した異常なデーター転送を識別することで、ネットワークレベルでの活動を軽減することができる。署名はプロトコル内の固有の指標であることが多く、特定の敵対者またはツールが使用する特定の難読化手法に基づいている可能性があり、さまざまなマルウェアファミリーやバージョン間で異なる可能性がある。
防御回避	**特権によるウイルス対策ソフト停止** T1562.001: Impair Defenses: Disable or Modify Tools	**M1038：実行防止** 適切な場合には、特に、システムの防御を弱めるために悪用されている組織のセキュリティ ポリシー外のツール (ルートキット削除ツールなど) の実行に関して、アプリケーション制御を使用する。承認されたセキュリティ アプリケーションのみがエンタープライズ システムで使用され、実行されるようにする。 **M1022：ファイルとディレクトリの権限を制限する** 攻撃者がセキュリティ サービスを無効化したり妨害したりしないように、適切なプロ

攻撃分類	MITRE ATT&CKテクニック	MITRE による推奨緩和策
		セスとファイルのアクセス許可が設定されていることを確認する。 **M1024：レジストリ権限を制限する** 攻撃者がセキュリティ サービスを無効化したり妨害したりすることを防ぐために、適切なレジストリ権限が設定されていることを確認する。 **M1018：ユーザーアカウント管理** 攻撃者がセキュリティ サービスを無効化したり妨害したりすることを防ぐために、適切なユーザー権限が設定されていることを確認する。
実行	**コマンド実行による資格情報のダンプ** T1059.003: Command and Scripting Interpreter: Windows Command Shell	**M1038：実行防止** 適切な場合はアプリケーション制御を使用する。
探索	**ネットワークスキャン** T1018: Remote System Discovery	このタイプの攻撃手法は、システム機能の悪用に基づいているため、予防的制御では簡単に軽減できない。
	ネットワークスキャン T1046: Network Service Discovery	**M1042：機能またはプログラムを無効化または削除する** 発見や潜在的な悪用のリスクを防ぐために、不要なポートとサービスが閉じられていることを確認する。 **M1031：ネットワーク侵入防止** ネットワーク侵入検知/防止システムを使用して、リモート サービス スキャンを検出し、防止する。 **M1030：ネットワークセグメンテーション** 重要なサーバーとデバイスを保護するために、適切なネットワーク セグメンテーションが確実に実行されるようにする。
	ドメイン情報の収集 T1069.002: Permission Groups Discovery: Domain Groups	このタイプの攻撃手法は、システム機能の悪用に基づいているため、予防的制御では簡単に軽減できない。
	管理共有接続 T1135: Network Share Discovery	**M1028：オペレーティング システムの構成** Windows グループポリシーの「SAM アカウントと共有の匿名列挙を許可しない」セキュリティ設定を有効にして、ネットワーク共有を列挙できるユーザーを制限する。
収集	**ローカルデーター収集** T1005: Data from Local System	**M1057：データー損失防止** データー損失防止により、機密データーへのアクセスを制限し、暗号化されていない機密データーを検出できる。
	共有データー収集 T1039: Data from Network Shared Drive	このタイプの攻撃手法は、システム機能の悪用に基づいているため、予防的制御では簡単に軽減できない。
影響	**ファームウェア破壊** T1495: Firmware Corruption	**M1046：ブートの整合性** 既存の BIOS とデバイス ファームウェアの整合性をチェックして、変更に対して脆弱かどうかを確認する。 **M1026：特権アカウント管理** 特権アカウントへの悪意のあるアクセスや、システム ファームウェアの置き換えに必要なアクセスを防止する。 **M1051：ソフトウェアの更新** 既知の脆弱性が悪用されるのを防ぐために、必要に応じて BIOS やその他のファームウェアにパッチを適用する。
	データー暗号化 T1486: Data Encrypted for Impact	**M1040：エンドポイントでの行動防止** Windows 10 では、クラウド配信の保護と Attack Surface Reduction（ASR）ルールを有効にして、ランサムウェアに似たファイルの実行をブロックする。 **M1053：データーのバックアップ** 組織のデーターを復元するために使用できるデーターバックアップを定期的に取得してテストする手順を含む IT 災害復旧計画の実装を検討する。バックアップがシステム外に保存され、敵対者がアクセスしてバックアップを破壊し、復旧を防ぐために使用する可能性のある一般的な方法から保護されていることを確認する。クラウド環境でバージョン管理を有効にすることを検討する。

攻撃分類	MITRE ATT&CKテクニック	MITRE による推奨緩和策
	データー破壊 T1485.001: Data Destruction	**M1053：データーのバックアップ** 組織のデーターを復元するために使用できる定期的なデーターバックアップの手順を含む IT 災害復旧計画の実装を検討する。バックアップがシステム外に保存され、敵対者がアクセスしてバックアップを破壊し、復旧を防ぐために使用する可能性のある一般的な方法から保護されていることを確認する。

7　詳細編 復旧について

復旧にあたっては、6.4 推測される攻撃の一覧と緩和策を参考に、その外縁となる「セキュリティの原則」を示し、病院および電子カルテベンダーに具体的な要求事項を示した。

7.1 セキュリティの原則

復旧対策では、基本原則を次のように定め、考え方のよりどころを示した。

- **多層防御：**各システム、ネットワークでのリスクの認識、対策のガイダンスと共有、異常や脅威の警告、Fail Safe、安全なバリア、バリアのすり抜けの防止、避難と復旧方針を示すこと。
- **最小特権：**管理者アカウントの使い回しの禁止、永続的でない一時的・制限された管理者権限の付与を計画すること。
- **攻撃表面の最小化：**承認されたアプリケーションの使用と脆弱性管理、電子署名されたプログラムとスクリプトのみ許可、必要最小限のポート許可、接続先制限を実施すること。
- **知る必要性に基づくアクセス権の付与：**役割（ロール）ベースの アクセス制御、属人化（集中）の排除、申請と承認の分離を行うこと。
- **管理接続の保護：**サーバー管理専用端末の設置と多要素認証、業務ネットワークとは異なる専用ネットワーク、VLAN での接続を行うこと。
- **資格情報の保護：**複雑性や定期変更を求めず、長いパスフレーズを使用する、パスワードの漏えいの定期的なチェックを行い、Windows 資格情報の保護設定を実施する。
- **レガシー保護と更新計画：**古い OS、脆弱なプロトコルを抱えているシステムの刷新、刷新までの防御と検出、対応のための計画と立案を実施する。
- **責任分界点の明確化：**サイバーセキュリティ条項、サプライチェーンを含めた監査権を求める契約を締結する。

7.2 復旧における要求事項

復旧設計における具体的な要求事項は、以下のとおりである。

① Security By Design、Security By Default に基づき初期侵入を確実に阻止すること。
② 仮に侵入を許しても水平展開を阻止し局所化すること。
③ 情報の窃取を極力防止すること。
④ 脅威検出が容易であること。
⑤ 迅速に復旧が可能で医療行為が継続できること。

7.3 初期侵入の阻止

初期侵入の経路は、HIS 系では 1. VPN 装置、Firewall などの通信機器の経由、2. HIS 系に持ち込んだ USB メモリ、3. 外部 PC からのウイルスの侵入、インターネット系では、4. 電子メールの添付ファイル、5. Web 閲覧によるウイルス感染、6. Built－In Administrator へのリモートデスクトップ接続等による辞書攻撃が考えられる。それぞれ、脆弱な初期設定や資格情報、脆弱性を悪用することが知られている。

7.3.1 HIS 系 Firewall、VPN 装置対策

① 脆弱性管理

Firewall 装置、VPN システムの脆弱性情報の入手、脆弱性の評価、脆弱性の修正を管理する台帳を作成し、定期的に脆弱性情報を取得し、都度、評価、修正を行う体制を整えた。Default のアカウント等の使用は禁止した。

② VPN 専用踏み台サーバーの設置と多要素認証

リモートデスクトップ接続専用の踏み台サーバーを設置し、NTT 東日本-IPA シン・テレワークシステムを導入した。シン・テレワークシステムによる接続元 IP アドレス制限、接続元端末 MAC アドレス制限、電子証明書による多要素認証を実施し、接続先サーバーは踏み台サーバー以外の接続を拒否とした。今後、電子カルテベンダー以外の保守用接続にあたっては、スマートカードに認証用証明書を設定し、スマートカードによる多要素認証を導入予定である。

③ リモートデスクトップ接続先サーバーの設定変更

リモートデスクトップ接続先サーバーでは、RDP ポートのスキャンを困難にするため既定値の 3389/TCP/UDP から変更し、かつ、辞書攻撃を防ぐ目的でロックアウト設定を実施した。

④ ログ監査

Firewall 装置、新テレワークシステムは Syslog を外部保存し、定期的に Syslog の監査を実施し、異常な通信の検出を行う事とした。

7.3.2 USB メモリ対策

医局からの外部持ち出しに際しては、病院指定のウイルス対策ソフト内蔵の USB メモリのみ使用を許可とした。外部からの持ち込みに際しては、同 USB メモリとは異なるウイルス対策ソフトでスキャンを実施し、最低 2 つ以上のウイルス対策ソフトでの検査の実施を強制している。

今後、病院指定のウイルス対策ソフト内蔵 USB メモリだけを接続許可する Group Policy の設定を予定している。

7.3.3 外部 PC 対策

外部 PC の HIS 系ネットワークの接続は禁止しており、Windows Server 標準搭載の Active Directory 証明書サービス（ADCS）の導入を行った。今後、Wi-Fi、イーサネットともに電子証明書ベースの 802.1X 認証（EAP-TLS）による外部 PC の接続拒否を計画している。

7.3.4 電子メールの添付ファイル対策

電子メールの添付ファイルに潜むウイルス対策としては、その手口が主に Office の VBA マクロを使用するものが多いため、VBA コード署名用証明書を導入し、電子署名された VBA マクロのみ実行を許可するポリシーを設定した。Office のアドインの使用を禁止する Group Policy の導入、メールサーバー側でのスパム検出、ウイルス検出、悪意あるリンクの検出の実施を予定している。

また、電子メールに埋め込まれた悪意ある Web リンクは、一般的にはマウスカーソルを Web リンクに重ね（マウスオーバー）実際のリンクを確認する方法があるが、うっかりリンクをクリックする危険性は残る。そのため、リンクの名前解決を行う DNS サーバーにセキュアな DNS リゾルバを採用した。IBM が運用

し無償で利用できる Quad9（IP アドレス：9.9.9.9）を Active Directory サーバーの DNS の Forwarder、Firewall の Forwarder に設定し、マルウェア、フィッシングサイト、ボットネットに接続する悪意あるリンクの名前解決をブロックした。無償のセキュア DNS リゾルバーは、Quad9 以外にも、Google Public DNS（IP アドレス：8.8.8.8）や OpenDNS（IP アドレス：208.67.222.222）などが利用可能である。

7.3.5 Web 閲覧によるウイルス感染

Firewall の UTM 機能によるウイルス検出機能、ウイルス対策ソフトでの検出、攻撃面の縮小ルールの Group Policy と、前述のセキュアな DNS リゾルバによるブロックを実施している。

7.3.6 Built-In Administrator の無効化と認証強化

① すべての Built-In Administrator を無効化し、ローカルの Administrators に所属する管理者を設定する。これによって初期の辞書攻撃を阻止する。

② 総当たり攻撃、辞書攻撃を防ぐため、Remote Desktop Users の多要素認証を採用し、Remote Desktop が許可されるセキュリティグループのユーザーには Group Policy でスマートカードログオンを強制した。

7.3.7 脆弱な初期設定対策

概要編でも述べたが、Windows では、ユーザーアクセス制御が適用されず、かつ、ロックアウトされない Buit-In Administrator という既定の管理者アカウントが存在する。また、後方互換性維持のため、ドメインコントローラーへのネットワーク接続に Everyone が許可されている。ファイル共有に使用される SMB プロトコルは、通信でのデジタル署名を強制していないことから、成りすまし、中間者攻撃に脆弱な初期設定となっている。

こうした Windows の既定値を悪用する攻撃があることから、CIS Benchmark Windows Server 2022 Ver.3.0.0 及び Windows 11 Enterprise Ver.3.0.0 を Default Domain Policy 及び Domain Controllers Policy に適用した。それぞれ、およそ 300 項目程度の強化設定を施した。具体的には、Built-In Administrator の利用の停止、すべてのサーバー・端末ユーザーへのロックアウトの適用・ユーザーアクセス制御の適用と 16 桁以上の長いパスフレーズの採用、Microsoft ネットワーククライアント、サーバーのデジタル署名、NTLMv1 の禁止、ローカルアカウントのネットワーク経由のアクセスを拒否、自動再生、自動実行の停止、Microsoft Defender でのローカルの設定変更を無効にする、などである。また、リモートデスクトップ接続については、既定値の 3389/TCP/UDP のポートを変更し、併せてロックアウト設定を実施した。今後、Office、Chrome に関しても同様の CIS Benchmark の適用を実施予定である。

7.4 水平展開の阻止

水平展開では、1. Administrators に所属する管理者アカウントパスワードの使い回しの悪用、2. Pass-The-Hash 攻撃、3. ファイル共有への暗号化攻撃、4. ネットワークスキャン、5. 脆弱性の悪用が考えられる。

7.4.1 Microsoft Local Administrator Password Solution（LAPS） の適用

本事案では、すべての Built-In Administrator のパスワードが共通であったことから、水平展開を許してしまった。このため、管理者パスワードをコンピューター毎にユニークに自動設定する LAPS[20]を適用し、パスワードの使いまわしができないように強制する。これにより、他のコンピューターへの水平展開を不可能とする。

7.4.2 Pass-The-Hash 攻撃の阻止

Windows Server 標準搭載の Active Directory 証明書サービス（ADCS）の導入により、Windows Hello for Business を導入し、多要素認証を実現する。Windows Hello for Business は、パスワードを使用せず電子証明書を使った多要素認証のシステムで、秘密鍵はコンピューターの TPM チップに保存されるため、鍵の窃取が非常に困難となる。また、PIN の辞書攻撃はロックアウト設定を行うことで防止する。

また、同時に NTLM ハッシュを削除することで Pass-The－Hash 攻撃[21]を不可能とする。なお、NTLM 認証の監査モードを導入し、NTLM 認証を行うシステム、端末等を把握し、早期に NTLM 認証の利用を根絶する予定である。

7.4.3 クライアントでの SMB ファイル共有の禁止

攻撃表面の最小化としてクライアントでの SMB ファイル共有は禁止し、ファイルサーバー以外のファイル共有を禁止する。また、SMB ファイル共有でクライアント側に Administrators 等の高位の資格情報を保存することを禁止する。

7.4.4 ネットワークスキャンの阻害

本件事案では、攻撃者 X によりネットワークスキャナーが設置され、病院内ネットワーク構成を取得された。攻撃者 X が使用した SoftPerfect 社のネットワークスキャナーでは、ワークグループ、ドメイン名の取得、Windows バージョン、ユーザーアカウント、ディスクドライブ、サーバーの役割等と通信可能なポート番号、共有フォルダーや管理共有が取得できる。病院では、ネットワークセグメントがフラットな構成であったため、探査は容易な構成であった。

このため、ネットワークの復旧に当たっては、マイクロセグメントの採用、ドメインコントローラー、アプリケーションサーバー、バックアップのセグメントの分離を行った。実際には Class を分けて設置しており、ドメインコントローラーが発見されても、他のサーバー、バックアップが芋づる式に発見されないように構成した。また、基幹システムとサブシステム間の通信を VLAN で独立させている。これにより、乗っ取られたコンピューターから意図しない通信を防止でき、病院ネットワークの全容が分かりにくい構成にしている。各医療機器、サーバーはパーソナル Firewall の設定により、特定の機器とサーバー間の通信のみを許可としており、Nmap[22]等を使ったアクティブスキャンでの通信ポート検出は難しい状況にある。また、Firewall によるアクティブスキャンの検出を設定し、加えてルーターを医療機器接続セグメントに設置し、Syslog の取得をする予定である。

---

[20] https://learn.microsoft.com/ja-jp/windows-server/identity/laps/laps-overview
[21] https://learn.microsoft.com/ja-jp/windows-server/security/windows-authentication/how-to-configure-protected-accounts
[22] Nmap: Network Mapper。ネットワークのスキャンやセキュリティ監査に使用されるオープンソースツールで、ネットワーク上のコンピュータや使用可能なサービス、OS、脆弱性等の検出が可能。

7.4.5　脆弱性の悪用

本件事案では、共有ストレージの全喪失の原因として仮想基盤の脆弱性の悪用による暗号化が疑われている。一方で、仮想基盤の脆弱性アップデートには、仮想サーバーの停止や移動、再起動などで時間がかかり、医療情報システムにおいては停止時間の長さから、脆弱性の修正プログラム適用を見送られることが多い。また、テストを理由に脆弱性アップデート後の動作保証を行わないベンダーも数多い。

他方、Windows の脆弱性修正は累積的となっており、過去の脆弱性も含め常に最新のアップデートが適用され、同じファイル構成となるようになっている。これによって、一部の更新が適用されていないコンピューターに新しいパッチを適用することで発生する不具合の発生が解消され、パッチによるファイルの競合やインストールの順序依存がなくなっている。他方、大半のベンダーは、毎月、最新のパッチ適用を行って出荷を行っているという。この際、異常がなければ、他の Windows にパッチ適用をしても同様に異常は発生しないこととなる。

このため、システムの再構築にあたっては、脆弱性アップデートの分割適用、基幹システムへの一斉適用を避ける、医療継続への影響性が低いシステムからの優先適用などを行い、脆弱性修正による不具合発生を抑え込む適用を実施している。なお、仮想基盤の脆弱性修正についても見直しを行い、月次で実施している。

7.5 情報窃取の阻止

本件事案では、AnyDesk という市販のリモート接続ツールの使用が判明している。これらのリモート接続ツールやリモートデスクトップ接続でのファイルコピーを実施されると、通信が暗号化されているため、Windows や Firewall には証跡が残らない。そのため、どのような情報が窃取されたかが不明となる。そこで、窃取されても情報の悪用や 2 次利用を困難にする必要がある。

7.5.1　ディスク暗号化と廃棄ポリシー

PC の内蔵ディスクはすべて BitLocker で暗号化を実施しする。接続が許可されるウイルス対策ソフト内蔵 USB メモリは、すべてハードウェアでの暗号化が可能、かつ、認証を必須とする。この場合、パスフレーズは 16 桁以上とする。ディスク、USB メモリ等の媒体の廃棄にあたっては、物理的破壊とする。

7.5.2　個人情報の暗号化

個人情報が含まれる Office 文書、PDF 文書は、ライツマネジメントシステム、もしくは、16 桁以上のパスフレーズによる個別暗号化によって第三者が解読できないように保存する。暗号化は AES-256 以上の強度とする。

7.5.3　個人情報の送受信

個人情報が含まれる Office 文書、PDF 文書は、電子メールに添付せず、認証付のコラボレーションツールを経由して送受信する。

7.5.4　　ファイルサーバーの移行

ファイルサーバーの運用を見直し、病院データーはすべてコラボレーションツールに移行する。組織外とのファイル共有は、リンクの有効期限を設定する。

7.5.5　コラボレーションツールの保護

コラボレーションツールは、すべて多要素認証を求める。

7.6 脅威検出が容易なこと

一般的に脅威検出は、EDR や SIEM の導入と、これらを 24/365 で監視する熟練の専門家によるセキュリティオペレーションセンターの設置が必要である。逆に言えば、EDR を単体で導入しても、一般的なシステム管理者では、実際の攻撃なのか単なるノイズなのかの判別はつかないことが多く、加えて最新の脅威動向に関する知識が必須である。また、夜間に攻撃された場合の対応などは、病院単独では困難である。一方で、本件事案では、管理者権限を有するアカウントの追加が確認されており、こうした事象を容易に検出できるようログの詳細な構成を実施するとともにツールを整備した。また、Windows Hello for Business の導入や、NTLM 認証の監査を実施し、将来的に NTLM 認証を廃絶することで、辞書攻撃の発見を容易にする環境づくりを行うこととした。

7.6.1 監査ポリシーの詳細な構成

Active Directory では、セキュリティログの監査設定を強化することで、多数の異常を検出することが可能であるが、既定値ではログ出力がなされない設定となっている。このため、監査ポリシーの詳細な構成を実施することで、150 項目を超す監査を可能とした。

カテゴリー	サブカテゴリー	設定値
アカウントログオン	Kerberos サービスチケット操作の監査	成功および失敗
	Kerberos 認証サービスの監査	成功および失敗
	資格情報の確認の監査	成功および失敗
アカウント管理	アプリケーショングループの管理の監査	成功および失敗
	コンピューターアカウント管理の監査	成功
	セキュリティグループ管理の監査	成功
	その他のアカウント管理イベントの監査	成功
	ユーザーアカウント管理の監査	成功および失敗
	配布グループの管理の監査	成功
詳細追跡	PNP アクティビティの監査	成功
	プロセス作成の監査	成功
DS アクセス	ディレクトリサービスアクセスの監査	失敗
	ディレクトリサービスの変更の監査	成功
ログオン/ログオフ	アカウントロックアウトの監査	失敗
	グループメンバーシップの監査	成功
	その他のログオン/ログオフイベントの監査	成功および失敗
	ログオフの監査	成功
	ログオンの監査	成功および失敗
	特殊なログオンの監査	成功
オブジェクトアクセス	その他のオブジェクトアクセスイベントの監査	成功および失敗
	ファイル共有の監査	成功および失敗
	リムーバブル記憶域の監査	成功および失敗
	詳細なファイル共有の監査	失敗

カテゴリー	サブカテゴリー	設定値
ポリシーの変更	MPSSVC ルールレベルポリシーの変更の監査	成功および失敗
	その他のポリシー変更イベントの監査	失敗
	監査ポリシーの変更の監査	成功
	承認ポリシーの変更の監査	成功
	認証ポリシーの変更の監査	成功
特権の使用	重要な特権の使用の監査	成功および失敗
システム	IPsec ドライバーの監査	成功および失敗
	システムの整合性の監査	成功および失敗
	セキュリティシステムの拡張の監査	成功
	セキュリティ状態の変更の監査	成功
	その他のシステムイベントの監査	成功および失敗

7.6.2 Log Parser の導入による Windows ログの監査

Windows のイベントビューワーは、ログの抽出、検索のためのフィルター設定に XPath1.0 のサブセットを使用するため、直感的な検索は困難である。そこで、マイクロソフト純正の無償のログ分析ツールである Log Parser[23]を導入し、辞書攻撃やセキュリティグループの変更など、ランサムウェア攻撃で特徴的な事象を容易に検出できるシステムを構築した。日次バッチ処理で簡単に異常を発見でき、NTLM 認証での連続的なログオン失敗や管理者アカウントの追加など、通常では起こり得ない事象を容易に分析できるようにした。なお、ログの出力量を勘案しつつ、Windows Sysinternals System Monitor[24] を導入に、さらに詳細なログの取得を計画中である。

7.6.3 Syslog 監査

Firewall とバックアップの Syslog は週に 1 回以上の割合で監査を実施することとした。

7.6.4 ランサムウェア、ウイルス対策について

ウイルス対策及びランサムウェア対策として、Windows の標準ウイルス対策機能である Microsoft Defender ウイルス対策の「攻撃面の縮小ルール」を適用し、「ランサムウェアに対する高度な保護を使用する」を適用した。また、グループポリシーで「リアルタイム保護を有効にする場合のローカル設定の優先を構成する」、「コンピューターでファイルとプログラムの動作を監視する場合のローカル設定の優先を構成する」、「受信ファイルと送信ファイルの動作を監視する場合のローカル設定の優先を構成する」、「すべてのダウンロードファイルと添付ファイルをスキャンする場合のローカル設定の優先を構成する」、「動作監視を有効にする場合のローカル設定の優先を構成する」を無効とし、ローカルでの設定変更を無効とした。

[23] https://www.microsoft.com/ja-jp/download/details.aspx?id=24659
[24] https://learn.microsoft.com/ja-jp/sysinternals/downloads/sysmon

なお、病院内での慎重な検討を重ねた上で、最新の情報に基づく検疫を優先するため、以下の FQDN に対する通信を Firewall で許可している。これにより、最新情報に基づく、ウイルス駆除、ランサムウェア駆除が可能となっている。

目的	FQDN	ポート
クラウド保護サービス	*.microsoft.com *.msft.net wdcp.microsoft.com wdcpalt.microsoft.com mp.microsoft.com amcorecdn.microsoft.com	80/TCP 443/TCP
リアルタイム保護とログ送信	dc.services.visualstudio.com us-v20.events.data.microsoft.com	
ポリシー同期と管理	securitycenter.windows.com endpoint.microsoft.com	
脅威インテリジェンス	winatp-gw-aus.microsoft.com winatp-gw-cus.microsoft.com winatp-gw-eus.microsoft.com winatp-gw-weu.microsoft.com	
Windows Update	update.microsoft.com download.windowsupdate.com *.delivery.mp.microsoft.com	
クラウドプロテクションサービス	cloud.microsoft.com *.blob.core.windows.net	

7.7 迅速な復旧

病院は令和 5 年度計画において、個人情報保護の取り組みの一環として、以下の方針を立てていた。

- ✓ サイバー保険に加入することで、個人情報保護の強化を目的とした事前対策方法について、検討を行う。
- ✓ データーのバックアップを定期的に行い、病院機能が止まらないようセキュリティ強化に努める。また、仮にサイバー攻撃を受け被害が発生したときであっても、被害を最小限に抑え迅速に現状復旧が行えるよう対応フローチャートを作成し、手順の確認を行う。

これに基づき、2024 年 5 月 15 日に、A 社とバックアップに関する契約を締結し、以下のサーバーのバックアップを取得していた。

- ✓ AD サーバー、電子カルテ DB サーバー、医事 DB サーバー
- ✓ I/F サーバー、NAS、ポータルサイトサーバー、DWH サーバー

一方で、本件事案では攻撃者 X の周到な調査によってバックアップデーターがすべて探知され、5 月 19 日の攻撃では、すべて破壊されてしまった。バックアップ全喪失という事態を招いたのは、オフライン・バックアップを取得しておらず、もしくは、書き換え不可能な媒体を使用しておらず、AD サーバーのドライブに保存したことが原因である。これにより DWH からの復旧を余儀なくされたため、復旧に時間がかかってしまった。迅速な復旧には、バックアップの完全性、真正性が証跡によって担保されていること、バックア

ップシステムで脅威を検出できることが要件となる。そのため、オンラインバックアップ、オフラインへのバックアップ、大規模災害にも耐えうるクラウドへのバックアップ保存を実施することとした。

7.7.1　バックアップシステム

医療におけるバックアップは、その真正性の確保が最も重要であり、また、確実な復元が保証されなければならない。そのため、バックアップシステム自身が脅威検出を行える機能を備えた製品を選定した。また、バックアップシステムからクラウドへの保存が行えることから、クラウド側に保存するバックアップを複数世代取得し、これらの書き換え、削除を不可能とすることで、確実なオフライン・バックアップを確保し復旧を可能するようにした。また、バックアップシステムの Syslog は、別途、異なるセグメントのサーバーかつオフライン・バックアップに保存し、バックアップへの攻撃や改ざん等が確認できる体制を構築している。

7.7.2　クラウド保存と電子カルテ参照系構築

免震、自家発電が備わったデーターセンターのクラウドに保存することで、大規模災害対応も可能とした。将来的には、同じクラウド上に待機系の電子カルテ参照システムを構築し、発災、サイバー攻撃等でも、医療継続を確実なものとしたい。

8 詳細編 組織的対策

8.1 医療情報システム安全管理委員会の適正な運営

病院情報システムのセキュリティ維持には、病院のベンダーへの丸投げ体質や、ベンダーの「閉域網神話」に基づくセキュリティ意識の欠如といった慣行を排除するとともに、病院とベンダーが緊張感をもって相互に牽制が可能となる体制の確立が重要となる。今後、医療情報システム安全管理委員会の機能を充実させ、IT ガバナンスの確立に向けた体制強化を実施する予定である。

8.1.1 組織的な IT ガバナンスの確立と強化

医療情報システム安全管理委員会の構成を病院幹部と IT 担当者とし、情報セキュリティ規程等の全面的見直しを実施する。主に、ISO/IEC 27002:2022 5.1 情報セキュリティに関する方針群、5.2 情報セキュリティの役割及び責任、5.3 職務の分離、5.4 経営陣の責任、5.5 関係当局との連絡、5.6 専門組織との連絡、5.7 脅威インテリジェンス、5.8 プロジェクトマネジメントにおける情報セキュリティ、5.14 情報転送、5.15 アクセス制御、5.16 識別情報の管理、5.17 認証情報、5.18 アクセス権、5.20 供給者との合意における情報セキュリティへの取扱の管理策、手引きを基に、医療情報システムの安全管理を実施する。

8.1.2 システム管理台帳による管理

IT 担当者による、システム管理台帳（機器名、IP アドレス、接続先制限、VLAN、脆弱性情報入手先、脆弱性対策適用状況、サポート状況及びサポート切れ等）の整備を実施する。主に、ISO/IEC 27002:2022 5.9 情報及びその他の関連資産の目録、5.10 情報及びその他の関連資産の利用の許容範囲、5.11 資産の返却の管理策、手引きを基にセキュリティ管理を実施する。システム管理台帳は医療情報システム安全管理委員会が実施状況を監査する。

8.1.3 データー分類、ラベル付け基準の策定

IT 担当者による、データー分類、ラベル付けによるデーターの暗号化、保存、廃棄手順を策定する。ISO27002：5.12 情報の分類、5.13 情報のラベル付け、5.14 情報転送、5.15 アクセス制御、5.16 識別情報の管理、5.17 認証情報、5.18 アクセス権の管理策、手引きを基にデーター分類、ラベル付けを実施し、その上で、データーの暗号化、認証強化、アクセス権の設定等の基準を策定する。なお、既に管理者権限に関してはスマートカードログオン、Windows Hello for Business による認証強化を図っている。

8.1.4 医療機器ベンダーへのセキュリティ対策ヒヤリングの実施と是正

すべての医療機器ベンダーへのセキュリティ体制、脆弱性管理に関するヒヤリングを実施、脆弱性管理に対する管理強化を要請済み（一部、ベンダー未対応）。3 省 2 ガイドライン及び ISO27002：2022 5.19 供給者関係における情報セキュリティ、5.20 供給者との合意における情報セキュリティへの取扱、5.21 ICT サプライチェーンにおける情報セキュリティの管理、5.22 供給者のサービス提供の監視，レビュー及び変更管理、5.23 クラウドサービス利用における情報セキュリティの管理策、手引きを基に、継続的にベンダーへのセキュリティ対策のヒヤリング、文書の提出を求めていく。

8.1.5 ベンダーとの契約の見直し

厚生労働省医療情報システムの契約における当事者間の役割分担等に関する確認表、厚労省ガイドライン第 6.0 版（令和 5 年 5 月）、２省ガイドライン 第 1.1 版（令和 5 年 7 月改定）を基に、ベンダー提案におけるガイドラインの適応状況を確認するとともに、発注仕様書、検収時の設計書、手順書、設定報告書等に基づく厳格な受け入れ試験を実施する。また、VPN 接続ベンダーチェックリストに基づく、ベンダーのセキュリティ体制のチェックを実施する。チェック内容は、①組織管理体制、②資産管理の状況、③脅威情報の入手、④セキュリティ教育、⑤開発環境とセキュア開発、⑥提供している製品・サービスの 3 省 2 ガイドライン適用状況、⑦脆弱性管理、⑧サポート終了時の対応、⑨保守作業等での個人情報取り扱い、⑩廃棄である。

8.2 IT-BCP の策定

病院は岡山県地域防災計画により、岡山県災害拠点精神科病院として、大規模災害発生時における精神科医療の提供・調整、災害派遣精神医療チーム (DPAT)[25]に関する調整を行う体制を構築している。2024 年 1 月の能登半島地震では、DPAT 事務局の派遣要請に基づき、1 チーム 4 名を石川県庁に派遣しており、また、平時には、県内の精神科医療機関等を対象に災害時の専門的技術研修を開催するなど中心的な役割を果たしている。一方で、本件事案により病院機能は大幅な縮小を余儀なくされ、医療の質の維持も困難を極めたといってよい。

セキュリティインシデントに対応しつつ、病院機能を維持するため、大阪急性期・総合医療センターの IT-BCP をベースに病院 BCP との整合性を図り策定を実施する。ISO27002:2022 5.24 情報セキュリティインシデント管理の計画及び準備、5.25 情報セキュリティ事象の評価及び決定、5.26 情報セキュリティインシデントへの対応、5.27 情報セキュリティインシデントからの学習、5.28 証拠の収集、5.29 事業の中断・阻害時の情報セキュリティ、5.30 事業継続のための ICT の備えの管理策、手引きを基にする。また、ISO27002:2022 の技術的対策は可能な限り踏襲し、平時の備えを強固にし、高度な防御体制と局所化を図れる体制を維持する。

8.3 病院、電子カルテベンダー、機器ベンダーの課題整理

本項は、昨今のサイバー攻撃に伴う、病院とベンダーの関係や契約上の問題を再整理した。

8.3.1 病院の丸投げ体質について

多くの医療機関では電子カルテ、医事会計、オーダーリングシステムなどの基幹システムと、部門システム、そして画像診断装置や検査機器などを導入し、医療情報システムに接続している。それぞれのシステム、医療機器はネットワークに接続され、相互に密結合されていることが多く、全容を理解するのは容易ではない。また、近年の病院経営の厳しさから、IT 要員を多数雇用することも難しい状況にある。

一方で、基幹システムと多数の部門システム、医療機器との連携には、電子カルテベンダーなどがプライマリベンダーとして調整にあたり、調達から稼働に至るまでを請負契約で受託し、病院側の負担を軽減しスムーズな医療情報システムの導入を実現している。基幹情ステムとの連携や医療機器との接続稼働などの機

[25] DPAT: Disaster Psychiatric Assistance Team

能的な検証は、病院の少数の担当者でも可能であり、請負契約における仕事の完成の確認は容易であり、病院が電子カルテベンダーに丸投げすること自体は、ある種の合理性があったとも言えなくはない。

他方、医療情報システムは多数の異なるベンダーがそれぞれ異なるセキュリティポリシーでシステムを結合することから、最も脆弱なシステムに、医療情報システム全体が合わせざるを得ない状況が生じ、例えば、管理者権限の全体への付与や、脆弱性管理の欠如などの原因となっている。

本来、プライム事業者である電子カルテベンダーが、こうした問題を病院に報告し、発注者たる病院と共に課題解決を行うべきであるが、病院側のセキュリティ意識の低さや厚労省ガイドライン、2 省ガイドラインの理解不足から、プライム事業者たる電子カルテベンダーにセキュリティも含めた丸投げ状態となっていたのは事実である。プライム事業者としては、契約の目的であるシステムの稼働を最優先することから、「閉域網神話」を盾にセキュリティは劣後する。

今後、病院としては、セキュリティに関する丸投げを止め、システム稼働とセキュリティの両立を契約の目的とし、プライム事業者とともに、さまざまなベンダーに対して、調達時点からセキュリティ設定や体制を評価し、システムに実装することが望まれる。

8.3.2　VPN 装置のリスク想定の欠如について

徳島県つるぎ町立半田病院、大阪急性期・総合医療センターの事案と同様に、本件事案も侵入元となった VPN 装置の接続元 IP アドレス制限が実施されておらず、全世界からの攻撃が可能であった。逆にいえば、保守をおこなうベンダーの IP アドレスに限って接続許可としておけば、本件事案は発生しなかったといえる。脆弱性の保守も行っておらず、VPN 装置への攻撃をまったく想定していない状況にあった。VPN 装置は閉域網に穴を開け、境界型セキュリティの強度を下げる仕組みであり、慎重なリスク評価を行うべきであった。

8.3.3　オフライン・バックアップが不完全であったことについて

本件事案では、共有ストレージの RAID 情報が失われ、かつ、オフライン・バックアップが不完全であり、オフライン・バックアップからの復旧ができなかった。実際の復旧は、DWH からの手動でのデーター復元となり、多大な時間とコストを費やすこととなった。一方で、オフライン・バックアップが存在したとしても、その真正性、完全性が担保されている必要がある。単にオフライン・バックアップを取得するだけでなく、確実な復旧、再稼働を病院として検証する必要があった。

8.3.4　保守契約について

本件事案発生時に、データーセンター側の Firewall、VPN 装置のログ及び設定等が直ちに取得できないという課題が発生した。

A 社への聞き取りによれば、データーセンターの構築、保守を行っていた B 社の担当者が交代したことに伴い、新たに B 社が主張する保守基準が適用され、従来実施されていた設定変更やトラブル調査が行われなくなったという。実際には、A 社と B 社の保守契約において、保守の定義が曖昧であり、ハードウェアだけの保守なのか、トラブル発生時の設定変更等を含む運用保守を含むか、といった実施内容が明記されておらず、従前の協力が得られなくなったとのことであった。インシデント発生においてログの取得は、原因究明、再発防止立案にとって極めて重要であり、致命的な事態となる。

また、多くの医療情報システムの保守契約は、あくまでハードウェア保守が中心であり、OS、ソフトウェア、ネットワーク装置の脆弱性や設定ミスといったインシデントにつながる状態を是正するためのセキュリティ保守という概念が存在していない。しかし、今となってはインシデント発生時の対応も含めた保守体制の確立が必須である。今後、法曹専門家を交えて、サイバー攻撃を前提とした保守契約の在り方について、病院としては議論を深める必要がある。

8.3.5　電子カルテベンダー一括調達について

病院情報システムは、電子カルテ、医事会計、オーダーリング、看護支援といった基幹システムと、部門システム、画像診断装置、検査機器等の医療機器との連携で成立している。そのため、一部の電子カルテベンダーでは、こうした部門システムの調達や医療機器との接続を含んだ調整を請け負っているケースが多い。

ところで、部門システムや医療機器のセキュリティポリシーは、各社で異なっており、場合によっては危殆化した暗号の使用や、資格情報をプログラムにハードコーディングするなどの脆弱なシステムも散見される。こうした中、電子カルテベンダーが部門システムを調達する際に、電子カルテベンダー主導でセキュリティ仕様の要求を出しても受け入れられない状況がある。結果として、管理者特権を付与せざるを得なくなったり、ウイルス対策ソフトを停止したり、ほとんどのサーバー・端末の Firewall を無効化[26]するなどの危険なシステム構成が、病院情報システム全体を脆弱にしている。

また、各社の 3 省 2 ガイドラインへの遵守状況も異なることから、電子カルテベンダーが全体を通して、3 省 2 ガイドラインの遵守状況をチェックするというプロセスも組み込みにくい。今後、一括調達仕様にセキュリティ仕様を組み込み、仕様を満たさない場合は調達から外す等の対応を求める必要がある。

8.3.6　Security By Design、Security By Default 対応

サイバーセキュリティ・インフラ安全庁（CISA）と内閣府内閣サイバーセキュリティセンターや各国のサイバーセキュリティ関連機関によって署名された Principles and Approaches for Security-by-Design and -Default では、ソフトウェア作成業者に対して、以下の要求を挙げている。

> 技術は、我々の日常生活のほぼすべての面に溶け込んでいる。身分証明書管理から医療に至るまで、我々の経済や生活、健康にも直接的に影響を与えうる重要システムが、益々インターネットに直結するシステムに接続するようになっている。このような利便性の欠点の一例として、病院が手術を中止し、治療をたらい回しなってしまうようなグローバルなサイバー攻撃の被害が挙げられる。安全でない技術や重要システムの脆弱性は、悪意あるサイバーの被害を招き、潜在的な安全上 1 のリスクに繋がる。 結果として、ソフトウェア作成業者がセキュアバイデザインとセキュアバイデフォルトを製品の設計と開発段階から重視することがかつてないほど重要になっている。ソフトウェアの品質保証に関して業界が前進するよう尽力するベンダーもあるが、引き続き遅々として進まないままのベンダーもいる。本文書を執筆・作成した組織（これ以降は「署名組織」）は、全ての技術製造業者に対し、顧客が自身のシステムに対するサイバー攻撃を緩和すべ

[26] 叶谷信治雄 (2024)「HIS 系システムにおける Firewall 設定状況調査」、「医療情報学」、第 44 巻 4 号、pp.199-204.

く、常に監視、日常的なアップデートおよびダメージコントロールを行わないで済むことを含め、顧客に係るサイバーセキュリティの負担を軽減することをベースに製品を作るよう強く推奨する。また、ソフトウェア作成業者には、設定、監視、定期的なアップデートの自動化を容易にするような方法で製品を作成するよう促したい。作成業者は、自身の顧客のセキュリティの結果を改善することに責任を持つことが望まれる。歴史を見ると、ソフトウェア作成業者は、顧客が製品を使用した後に脆弱性を発見し、修正することに頼り、顧客に対しては自己負担でこれらのパッチを適用させることを強いてきた。セキュアバイデザインの実践を取り入れることによってのみ、このような頻繁に修正パッチを作成して適用するという悪循環を断つことができる。

Security By Design、Security By Default の観点から、管理者権限を必要とする電子カルテシステムや、部門・診療科システムを見ると、管理者権限の付与によってサイバー攻撃の緩和は困難であり、常に監視、日常的なアップデートおよびダメージコントロールが必須であり、顧客に負担を強いる製品ということができる。多くの医療情報システム製品、医療機器が標準ユーザーでの稼働に向けた努力を行っているところ、一つのシステム製品、機器が管理者権限を要求することで、病院全体のサイバー攻撃へのリスクが高まってしまう。管理者権限の付与を要求するベンダーの可及的かつ速やかな改善を求めるものである。

8.3.7 Windows Update について

現在、医療で使用されているシステム、機器の大半は、Windows もしくは Linux で動作しており、インターネット接続を行い、脆弱性のアップデートを前提に、様々な悪用されやすい欠陥を除去した上で安全を確保するとした OS を基軸に作成されている。ところが、概要編でも述べた通り、医療を取り巻く医療情報システム、医療機器は、閉域網を前提にしてきた影響から、脆弱性のアップデートに対して極めて後ろ向きであり、かつ、傍観的である。また、脆弱性アップデートを実施することで動作保証ができないし対応もできない、といったベンダーの反応は、病院の聞き取り調査でも数を多く確認したところである。もちろん、外部接続が一切ない完全な閉域網で、かつ、ウイルスや悪意あるプログラムの侵入が絶対にないというデーター運用と監視がなされているというのであれば、脆弱性が存在しても、それを悪用する主体が入り込まない限り安全であると仮定できる。

だが、実際の医療現場でいわれている閉域網は、実際には閉域網ではない。医療関連ベンダーが自らの保守目的で導入した VPN 装置が存在する以上、それを指して閉域網というのは欺瞞であり、加えて、脆弱性の是正が困難であり、もしくは、サポート切れの製品の採用を平然と提案するベンダーが存在する中で、病院はガイドライン求められるセキュリティや個人情報の保護を担保できないといえる。ベンダーは医療を重要インフラとして正面から捉え、医療情報システムに組み込まれるコンポーネントとして、セキュリティに関する意識改善が必要である。

加えて、多くのベンダーから毎月のアップデートの実施に対して社内テストが困難で、不具合発生に対応できないという指摘も寄せられている。医療情報システムや医療機器においては、十分慎重な試験の積み重ねが必要という。しかし、現在の Windows Update は累積的パッチ適用がなされることから、ソフトウェ

アコンポーネントの相互依存性に基づく不整合の発生は極めて少なく、DLL Hell[27]の発生は Side-by-Side 機能[28]により解決されている。デバイスドライバーもテストツールや Framework の提供、ドライバー署名の強制等により強靭となっており、ドライバー起因のブルースクリーンも発生しない。一般的なソフトウェア開発 Framework を使用する限り、Windows Update の弊害はないといえる状況にある。また、特殊な環境での不具合発生に対して、Windows Update が、自身の適用をブロックする機能も提供されており、アップデートに起因する弊害は、ほぼなくなっているのが現状である。

他方、多くのベンダーは、当月の最新アップデートを適用した上で、製品出荷を行っているという。Windows の初期インストールの実施後、最新の累積的パッチを適用し正常動作するのならば、他の Windows コンピューターでも同様の累積的パッチが適用されるため、Windows コンポーネントの差異はなく、製品は正常動作するといえる。過去の Windows のように、ソフトウェアコンポーネントのバージョン不整合（依存関係の衝突）が起きないメカニズムが提供されている限り、Windows Update を実施し、Windows Update を実施しない場合の病院全体のリスクを医療情報システムの専門家として低減するべきではないか。

もっとも、Windows Update 適用にかかるシステム停止時間の長さを懸念する向きもある。多数の仮想サーバーを保有している場合は、仮想基盤のアップデート、再起動、仮想サーバーのアップデート、再起動が伴う事から、数時間システムが使用できない可能性も考えられる。他方、医療情報システム全体の冗長化、高信頼性確保の観点から、本番系電子カルテと、参照系電子カルテに分け、本番系電子カルテのメンテナンスの際には参照系を稼働させ、業務における完全なダウンタイムを短縮させる方法もあり、実際に運用されている施設も存在する。今後、ランサムウェア対策、ノーウェア対策として特権昇格につながる脆弱性管理は必須である。サイバーセキュリティ対策としての Windows Update を含めた医療情報システムアーキテクトの育成を望むところである。

8.3.8　医療機器におけるサイバーセキュリティについて

復旧にあたっては、医療機器への影響を慎重に調査せざるを得ず、一定期間、ネットワークの遮断等を余儀なくされた。この間、脆弱性スキャン調査結果に基づき医療機器ベンダーへの聞き取り調査を実施したが、サイバーセキュリティに関する改善提案などはなく、主に病院側の指摘した課題の修正に終始した。

一方で、医療機器の基本要件基準は令和 5 年に改正されており、基本要件基準第 12 条第 3 項では、以下の要件が定められている。

> プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し、当該医療機器の機能に支障が生じる又は安全

[27] Windows のコンポーネントである DLL （ダイナミックリンクライブラリ, Dynamic Link Library）は、複数のプログラムが共通して利用できる関数や機能を提供している。過去の古い Windows においては、特定のバージョンの DLL に依存しているアプリケーションソフトが DLL のバージョンアップに伴い、期待しない動作を起こすことがあった。アップデートすればするほど、不具合が増えるため、DLL Hell（DLL 地獄）と呼ばれた。

[28] Windows XP から導入された DLL Hell を防ぐ機能。異なるバージョンの DLL を同居させ、アプリケーション毎に必要な DLL が上書きされずに保存される。アプリケーションは必要な DLL を設定ファイルで指定し、必要なバージョンの DLL が使用できる。

性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理が行われていなければならない。
また、当該医療機器は、当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造されていなければならない。

基本要件基準の適合については、病院が独自にリスク評価することは当然のこと、医療機器ベンダーにおいても、開放しているネットワークポートの利用用途の開示や、通信プロトコルの脆弱性や、使用上のリスク等を評価し、積極的に改善提案を行うべきである。

9 詳細編 人的対策

9.1 教育及び情報共有

9.1.1 ランサムウェア攻撃等初動対応教育

年 1 回をめどに、病院幹部と事務局、IT スタッフに対して、ランサムウェア攻撃、ウイルス感染における初動対応のトレーニングを実施する。これには、病院制定の IT-BCP の発動に際しての基本的な考え方や基準と、初動指揮に対応するための、病院幹部による平時の対策の監査の考え方を含むものとする。手書きカルテ運用を含めた医療継続と、医療情報システムの復旧について、他病院事例を基にトレーニングを実施するとともに、実際のインシデントを模擬したシミュレーションソフトによる意思決定トレーニングを計画中である。

加えて、病院幹部による平時の対策に対する監査は、病院の IT ガバナンス向上に極めて有効であり、事務局、IT スタッフを含めた経営資源の最適化を確認する意味で重要であることから、監査に関するトレーニングも併せて計画中である。

9.1.2 定期的な脅威情報、攻撃手法の教育の実施

半期に一度をめどに、全職員に対する、最新のフィッシング、ランサムウェア攻撃事例を共有する。特に、インターネット環境におけるランサムウェア攻撃の端緒ともなるフィッシングに関しては、高度化、巧妙化が進み、専門家でも判断に迷うような状況となっている。SNS の公開情報を基に AI や機械学習を用いたイベントや業務内容に関連するフィッシングメールや、クラウドサービスの偽造ログイン画面による ID、パスワード、2 段階認証コードの窃取などが多発している。こうした現状を鑑み、タイムリーなコンテンツを Video ライブラリーとして提供する。

将来的には、簡易な試験を実施し、コンテンツの内容に反映させることを実施する。

9.1.3 システム脆弱性情報及び対策案の共有

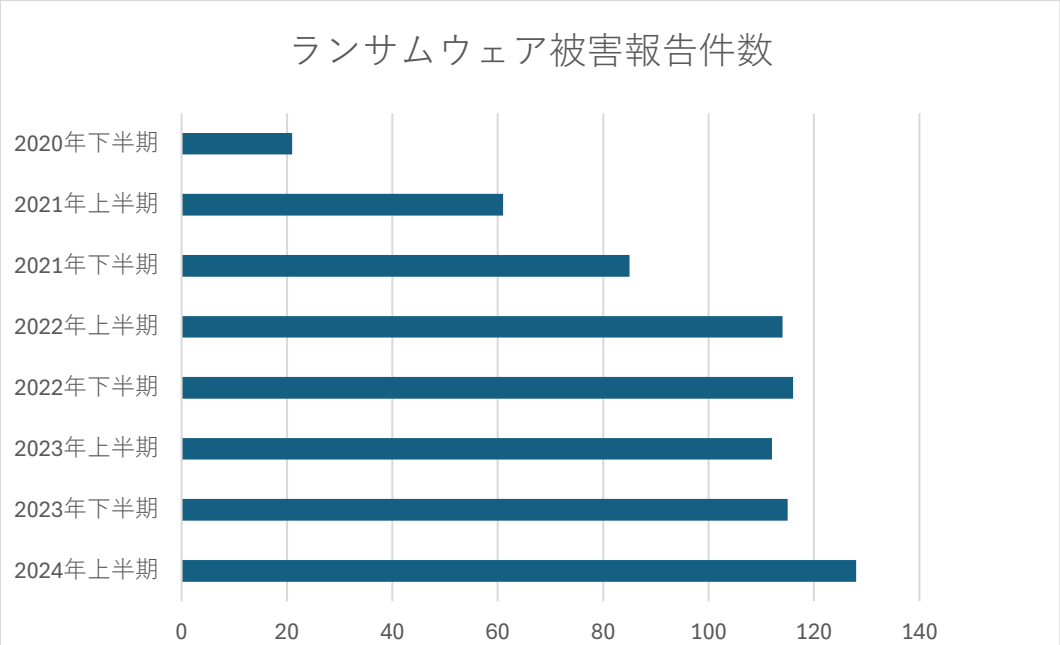
IT スタッフ、関連ベンダーにシステム脆弱性情報の共有を実施する。病院情報システムは、医療情報システムベンダーや医療機器ベンダーに依存しており、ベンダーが最新のセキュリティ情報を取得し、適切なアクションが出来るか否かが病院の死命を制することもある。メーリングリスト、Web ページ等を通じ、以下から提供される脆弱性情報等を共有する。

JPCERT/CC
CIS Advisory
CISA Known Exploited Vulnerabilities Catalog
Microsoft
Adobe
Google

10 総括

本件事案は、国内における精神科病院として初めての事案であり、精神疾患という極めて機微な情報を有する病院を揺るがし、また、ダークウェブと推定されるサイバー空間に要配慮個人情報が漏洩するという重大な事態を招いたものである。

警察庁の「令和６年上半期における サイバー空間をめぐる脅威の情勢等について」によれば、国内でのランサムウェア被害報告件数は、2024 年上半期で 128 件にも上り、すでに 2023 年の実績を超す勢いである。



出典：警察庁の「令和６年上半期における サイバー空間をめぐる脅威の情勢等について

このグラフで注目すべきは 2021 年以降、被害が増加している点にある。暗号通貨の普及により、攻撃者が匿名性を保ちながら身代金を要求できるようになったことと、2020 年のコロナ禍による、VPN 装置を介したリモートワークの定着、リモート保守の増加が一因と考えられる。また、従前から指摘されているランサムウェアの作り手（RaaS オペレーター）と、実際の攻撃犯（アフェリエイト）、脆弱な VPN システムの情報などを数百ドルで販売するといわれているイニシャル・アクセス・ブローカーらの分業化により、情報や技術力のない犯罪者が攻撃に参加でき、RaaS オペレーターは自らの手を汚すことなく収益の拡大が図れるようになっていることも、ランサムウェアというビジネスを考える際に重要なポイントといえる。

さて、何故、病院でランサムウェア事案が起きたのか。本件事案の攻撃ベクトルから読み取れるのは、徳島県つるぎ町立半田病院、大阪急性期・総合医療センターと同様に、脆弱な VPN 装置からの侵入、弱いパスワードの設定、一般ユーザーへの管理者権限の付与、管理者権限によるウイルス対策ソフトの停止という共通事項が浮かび上がる。つまり、攻撃犯はこうした脆弱なシステムを捜索し、もしくは脆弱なシステムの情報を購入し、攻撃を行っていると考えることができる。また、サーバー・端末ユーザーへの管理者権限の付与を停止し、ウイルス対策ソフトのサービス停止を招かない設定を施すことができれば、防御もしくは攻撃

の遅延の可能性は高い。同様に、侵入の端緒となるリモートデスクトップの設定変更やロックアウト設定を実施すれば、被害は軽減されたと考えられる。少なくとも、政府機関や先進的知財を有する研究機関・組織等への高度標的型攻撃に比べれば、ランサムウェアの攻撃犯の攻撃手法は、決して高度なものではなく、稚拙といっても過言ではない。言い換えれば、稚拙な攻撃を許す組織こそがランサムギャングの標的なのである。

一方、2021 年以前のシステム設計において、ランサムウェアによる攻撃や VPN 装置の脆弱性に対するリスク想定がなされることは少なく、システム設計上、特段、防御を施すという意識は低かったことも事実である。特に、VPN 装置等の脆弱性アップデートは、通信の停止や思わぬ不具合を招く可能性があり、多くのシステム事業者、ネットワーク事業者が脆弱性アップデートに躊躇することは容易に想像できる。また、電子カルテという 24 時間 365 日稼働が求められるミッションクリティカルシステムや、法律によって安全性の確保が求められる医療機器においても、厳重なテストなしに軽々と脆弱性アップデートができないという事情も想像に難くない。医療の IT 部門にセキュリティの専門家を雇い入れることも難しく、病院内での人材育成も容易ではない。

このように、医療における情報セキュリティの強化に対して課題は山積するが、冒頭に述べた通りランサムウェアの攻撃は減少どころか増加の一途をたどっている。また、近い将来、暗号化をせずに「窃取した情報を公開する」という脅迫で身代金を要求するノーウェアランサムも急増すると考えられる。単に、システムに侵入し、情報を窃取するだけなので、ランサムウェアの開発費も不要であり、イニシャル・アクセス・ブローカーから侵入情報を購入するだけでよい。病院内で取り扱う個人情報は要配慮個人情報となるため、一般企業に比べ、ノーウェアランサムが病院経営に与えるダメージは計り知れないものとなることが予想できる。

また、国内の医療情報システムは、制度的な転換期を迎えつつある。一部、報道によれば、経済安全保障推進法に基づき、国が企業の設備導入を事前審査する基幹インフラ制度を巡り「医療」の追加が検討されるという。医療が基幹インフラ制度に追加された場合、脆弱性テストや最新のセキュリティ・パッチの適用など、信頼できる品質保証体制の確立が求められる。従来の閉域網を理由とした、脆弱性管理の実施を取りやめることは困難になる。課題は多数あるが、地域医療の停止を招くサイバー攻撃に対する安全性、信頼性の確保は国民的要請ともいえる。業界を挙げての対応が望まれるところである。

本件事案は、徳島県つるぎ町立半田病院、大阪急性期・総合医療センターの報告書の指摘事項とまったく同じ脆弱性が招いたランサムウェア被害であり、厚労省ガイドラインの遵守で十分に防げた事案であった。脆弱性の放置や推測可能なパスワードの使いまわしなどは、サイバー攻撃が進化する中で「閉域網神話」による思考停止が招いた「人災」ともいうべきものである。改めて、医療情報システムベンダー、医療機器ベンダーと病院関係者による、外部接続点のリスクの再評価、基本的なセキュリティ設定の見直しを切に要望するものである。

11 資料

11.1　ニュースリリース

11.1.1 ニュースリリース初報 （2024/5/20）

電子カルテのシステムの不具合について

令和 6 年 5 月 19 日午後 4 時頃から、当センター及び東古松サンクト診療所の電子カルテを含めた総合情報システムに支障が生じています。地域における精神科医療の中核的な役割を担う病院として、県民の皆様、特に患者さんをはじめとする関係者の皆様に多大なるご迷惑、ご心配をおかけすることに深くお詫び申し上げます。

サイバー攻撃の可能性があることから、直ちに、岡山県、岡山県警、厚生労働省などの各方面に連絡をするとともに、原因の究明や早期の復旧に努めております。

当面、紙カルテの運用などにより診療体制の維持に取り組んでまいります。

なお、現在のところ、個人情報等の漏洩の事実は確認されておりません。

ご理解、ご協力のほど、どうぞよろしくお願い申し上げます。

令和 6 年 5 月 20 日

院長 来住 由樹

11.1.2 ニュースリリース第 2 報（2024/5/21）

令和 6 年 5 月 19 日午後 4 時頃発生した、当センター及び東古松サンクト診療所の電子カルテを含めた総合情報システムの障害は、ランサムウェアとみられるサイバー攻撃が原因であることが特定されました。今後も外部専門家の協力も得ながらシステムの復旧を進めつつ、職員一丸となって診療機能の維持に努めていきます。

なお、個人情報等の漏洩については引き続き調査中です。

令和 6 年 5 月 21 日

院長 来住 由樹

11.1.3 ニュースリリース第 3 報（2024/6/11）　＊7/14 一部修正

令和 6 年 5 月 19 日（日）ランサムウェアによるサイバー攻撃で、当センター及び東古松サンクト診療所の電子カルテを含めた総合情報システムに障害が発生いたしました。この件について、6 月 7 日（金）県警本部から連絡を受け、県警本部にて当センターの保有する患者情報の流出を確認いたしました。

当センターは、患者の皆様の人権を尊重し、利用者の方々の視点に立った良質な医療の提供を基本方針に掲げ、岡山県内の精神科医療の中核的な役割を担い、これまで多くの患者の皆様を受け入れてまいりました。しかし、この度、私どもの電子カルテのセキュリティー対策への管理監督が十分でなかったためにこのような事態を招き、これまで信頼いただいた皆様を裏切ることになってしまいました。患者の皆様、ご家族、関係者各位に多大なるご心配とご不安、ご迷惑を与えてしまったことに深くお詫び申し上げます。

今回の事態を重く受け止め、被害拡大の防止に全力で努めてまいります。

１．流出した可能性のある情報

総合情報システムで職員が業務で作成した資料を保存していた共有フォルダー内の次の情報

患者情報　氏名、住所、生年月日、病名　等（最大　約 40,000 人分）

病棟会議の議事録　等

２．経緯

2024 年 5 月 19 日（日）　総合情報システムダウン

2024 年 5 月 20 日（月）　県警本部、厚生労働省、県に連絡、システム障害のプレス発表

2024 年 5 月 21 日（火）　サイバー攻撃が原因と特定し、公表

2024 年 5 月 22 日（水）　個人情報保護委員会に報告

2024 年 6 月 7 日（金）　県警本部にて個人情報の流出を確認

令和 6 年 6 月 11 日

院長　来住　由樹

以上