調　査　報　告　書

2023 年 3 月 28 日

地方独立行政法人大阪府立病院機構
大阪急性期・総合医療センター
情報セキュリティインシデント調査委員会

1. はじめに（委員長挨拶）

2020 年、世界中の誰もが経験したことのない禍に否応なしに巻き込まれ、未知なる脅威への恐れと混乱の中、それに立ち向かう人々、特に医療に関わる全関係者の絶え間ない活動を、メディアなどを通して私たちは見てきました。これまでに世界中で医療が逼迫するといった事態がこの現代に起きるなど誰が想像していたでしょうか。緊迫した現場において医療機器が目まぐるしく動く映像をニュースなどで毎日のように流れていたことが思い出されるかもしれません。医療の現場と言えば「人間」が中心となり、私たちの健康や生命を支える場であることは誰もが知る事実ですが、その「人間」を支えるのが実に多くの計算機、すなわちコンピューター群です。もちろんコンピューターと言っても医療活動を支援する専門的なシステムであったり、私たちが普段から利用するものと似たパソコンやプリンターであったりと、様々なコンピューターが病院という組織内で接続されることはこの数年で特別なことではなくなりました。このように、私たちが普段目にすることのない病院の裏側に張り巡らされた通信路上で「情報」が 24 時間 365 日止まることなく流れ続けているのです。

さて、私たちの生活においてサイバー攻撃という言葉が割と一般的に使われるようになったのはさほど昔のことではありません。特にサイバー攻撃の中でもランサムウェアと呼ばれるコンピューターウイルスについて見聞きされたことがあるかもしれません。ランサムウェアは、アルファベットでは “Ransomware”と表記される造語です。その由来は Ransom（身代金）と Software（ソフトウェア）でありそれを繋げたワードであり、その意味は、一般的に悪い攻撃者たちが大切な「情報」すべてを勝手に暗号化して読み出せなくし、その大切な「情報」との引き換えに身代金を要求するというものです。令和に入ってからもこのランサムウェアに対する様々な手段が検討されていますが、未だその攻撃は増える一方です。そして、ランサムウェアに加えサプライチェーン攻撃と呼ばれる言葉もよく耳にするようになりました。これは、一つの組織だけの被害のみならず、ターゲットとなった組織と「情報」でつながるすべての組織にまで連鎖的に被害が及ぶという点が特徴的であり、例えば、部品を生産する工場など複数の企業と連携した組織への攻撃の一つとして考えられていました。しかし、病院などの医療機関や介護施設においてもこのような企業と同様に、一つの組織だけでなく複数の組織がその運営を支える関係者として携わっていることが今や当たり前となっており、これはすなわちサプライチェーン構造そのものです。結果、サプライチェーン攻撃によって、そのどこか一つでも何らかの被害を受けることにより、サプライチェーンの広範囲に影響が広がることにもなります。そしてもう一つ、サプライチェーンを構成する組織が複雑に絡み合うことにより、ネットワーク構成やルーター、VPN 等の装置、ファイアウォールやそのフィルタリング設定、あるいはそれぞれ組織ごとに異なるセキュリティポリシーが見えにくくなるということです。最終的に、サプライチェーンを成すそれぞれの組織を隔てる分界点が不明瞭になりやすくなる、という点です。これらすべての情報を一元的に把握し、最新の情報として管理することはセキュリティを担保するうえでは基本的なことかもしれませんが、医療機関をはじめ一般的な組織においても人員や機材等のリソースからすると未だ難しい課題であることは明白です。

大阪急性期・総合医療センターは、800 床以上を持つ大規模な総合病院であり、また様々な診療科を有する医療機関であることから、その病院機能を約 2 か月もの間、患者の治療に多大なる影響を及ぼすよ

うな診療制限をせざるを得なくなるという想像を超えた事態をサイバー攻撃によって引き起こされました。これはもはや情報システムの障害といったコンピューター世界だけの話ではありません。医療を必要としているすべての人の健康や生命に対する事案にもなりうる脅威そのものです。2021 年に徳島県つるぎ町立半田病院で起きたサイバー攻撃事案では、我が国における医療機関への脅威として業界を震撼させるに至りました。半田病院で構成されたコンピューターウイルス感染事案有識者委員会は、次なる被害の軽減を目的としてコンピューターウイルス感染事案有識者会議調査報告書を公開しました。しかしながら、いずれの医療機関において自身も同様の脅威が襲いかかるリスクを持ちうることを認識することはまだまだ難しいのも現実です。医療機関においても地域に密着したクリニックをはじめ総合病院などのように施設規模も多種多様であり、病院システムを構成するネットワークや電子カルテなどの電子システムも一概に同様とは言えないでしょう。このように、組織ごとに全く異なる現場において何かしら同様のセキュリティ対策を施しておけば問題は起きない、そんな単純な話ではないことも事実です。更には、セキュリティ対策と言えば技術的な面のみ注目されやすいですが、組織やマネジメント面など幅広い面においても認識しておくことも重要な時代になっています。

大阪急性期・総合医療センターが正常機能を取り戻したのが 2023 年 1 月、それに合わせて当サイバー攻撃事案に対する調査委員会が発足いたしました。当委員会では、既に病院側が取得した膨大な資料をもとに分析を行い、原因究明と今後の対策について検討を進めました。その過程において、様々な業態の組織が複雑に絡み合ったサプライチェーンを成していることから、調査委員会は公正・中立な立場で、すべての関係者に対してそれぞれ個別にヒアリングを実施しました。本報告書をまとめるにあたり、得られたすべての情報を整理し、再度報告書の整理の仕方について議論を重ねました。この結果、セキュリティ対策でよく言及されるような防御や事前の対策について示すだけでなく、セキュリティインシデントが起きたことを想定した準備体制や BCP として検討すべき点についても言及し、今後への提言をまとめました。これらは、医療機関のみに限定される話ではなく一般的な企業や組織を適切に運営していくための考え方として、最近ではプラス・セキュリティが重要になりつつあります。プラス・セキュリティとは、自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のことを指します。本報告書が、幅広い組織においてプラス・セキュリティについて気づきを与えるとともに、今後も発生しうる様々なサイバー攻撃による被害を軽減させるサイバーセキュリティ対策の一助となることを期待します。

大阪急性期・総合医療センター　情報セキュリティインシデント調査委員会　委員長
大阪大学 サイバーメディアセンター　教授　猪俣　敦夫

2. 調査委員会の設立

2.1. 設立の趣旨

大阪急性期・総合医療センターでは、本情報セキュリティインシデント事案を、重大な事故として位置付け、病院の事故調査委員会設置要綱に基づき、病院管理者である総長が事故調査委員会を外部委員のみの構成で設置することを決定し、今回のインシデント事案の原因を究明し、再発防止に資する事項を諮問した。

大阪急性期・総合医療センター事故調査委員会設置要綱

（設置）

第１条　総長は大阪急性期・総合医療センターにおける重大な事故の原因を究明し、再発防止に資するため事故調査委員会（以下「委員会」という。）を設置する。

（職務）

第２条　委員会は総長の諮問に応じて重大な事故の原因を調査し、審議し、再発防止に資するよう総長に答申する。

（組織）

第３条　総長は事故の内容により、内部委員と外部委員から構成される混合型調査委員会または外部委員のみで構成される外部調査委員会を決定し、委員を任命する。

２　委員会に委員長及び副委員長を置き、委員の中から総長が任命する。

３　委員長は会務を総括し、会議の議長となる。

４　副委員長は委員長を補佐し、委員長に事故があるときは代行する。

５　委員の任期は答申を持って終了する。

６　委員長は、必要に応じて関係者の出席を求め、報告または意見を聴取することができる。

（会議）

第４条　委員会は委員長が召集する。

２　委員会は随時開催する。

３　委員会は委員の３分の２以上の出席をもって開催するものとする。

４　委員会の決議は出席委員の過半数で決し、可否同数のときは議長の決するところによる。

（庶務）

第５条　委員会の記録その他の庶務は事務担当者が行う。

（雑則）

第６条　この要綱に定めるものの他、会議運営に関し必要な事項は委員長が定める。

2.2. 委員会の構成

総長は、事故調査委員会設置要綱第３条第 1 項に基づき、外部委員のみで構成される外部調査委員会の開催を決定し、6 名の外部委員を任命した。また、同設置要綱第３条第２項に基づき、総長は外部委員より委員長及び副委員長を任命した。委員の構成は以下の通り。

【大阪急性期・総合医療センター　情報セキュリティインシデント調査委員会】

職名	氏名	所属
委員長	【情報セキュリティ学識経験者】 猪俣　敦夫	大阪大学 サイバーメディアセンター 情報セキュリティ本部 教授
副委員長	【病院情報システム学識経験者】 黒田　知宏	京都大学 医学研究科 医療情報学 教授
委員	【情報セキュリティ有識者】 西本　逸郎	NPO 日本ネットワークセキュリティ協会 理事／株式会社ラック 代表取締役社長
委員	【地域医療有識者】※大阪府医師会推薦 阪本　栄	大阪府医師会 副会長
委員	【病院経営有識者】※大阪府病院協会推薦 三上　聡司	社会医療法人三上会 東香里病院 院長
委員	【情報関係契約法務有識者】 平野　高志	ブレークモア法律事務所 弁護士

2.3. 委員会開催概要

2023 年 1 月から 3 月に至るまで、3 回の調査委員会を開催した。また、調査委員会として本事案のステークホルダー（利害関係者）にヒアリング調査も実施した。

【情報セキュリティインシデント調査委員会　開催概要】

開催回	開催日時	主な議事
第 1 回	2023 年 1 月 25 日（水） 12 時 45 分～15 時	・インシデントの概要 ・これまでの調査結果報告 ・第 2 回委員会の検討事項
第 2 回	2023 年 2 月 20 日（月） 10 時～11 時 30 分	・追加調査報告 ・調査報告書の作成 ・ヒアリング調査の実施内容
第 3 回	2023 年 3 月 20 日（月） 10 時～12 時	・ヒアリング調査結果報告 ・調査報告書の内容確認 ・調査報告書の公表

【ステークホルダーヒアリング調査　実施概要】

調査対象	開催日時	ヒアリング調査目的
A 社	2023 年 2 月 20 日（月） 13 時 00 分～14 時 00 分	基幹システムベンダー、統括事業者としてのセキュリティの考え方など
B 社	2023 年 3 月 2 日（火） 15 時 00 分～16 時 00 分	ネットワーク構築事業者としてのセキュリティの考え方など
C 社	2023 年 2 月 20 日（月） 14 時 30 分～15 時 00 分	病院の給食システム情報基盤と E 社の情報基盤の構築事業者としての考え方など
D 社	2023 年 2 月 20 日（月） 15 時 00 分～15 時 30 分	給食システム提供者としてのセキュリティの考え方など
E 社	2023 年 2 月 20 日（月） 14 時 00 分～14 時 30 分	サプライチェーンとしてのセキュリティの考え方など
病院	2023 年 2 月 20 日（月） 15 時 30 分～16 時 10 分	総合情報システムを管理・運営する立場としてのセキュリティの考え方など

3. 用語説明

本報告書で独自に用いる用語について以下に解説する。なお、一般的な用語については別添の用語集を参照願いたい。

用語	定義
病院	地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
調査委員会(本委員会)	情報セキュリティインシデント調査委員会
総合情報システム	病院が運用する電子カルテを含む患者診療情報を扱う診療系システムの総称
機構本部	地方独立行政法人大阪府立病院機構本部
A 社	総合情報システム 基幹システム構築・保守統括事業者
B 社	総合情報システム ネットワーク構築・保守事業者
C 社	総合情報システム 栄養給食管理システム構築・保守事業者 （※E 社の給食調理センター情報基盤の構築・運用事業者でもある）
D 社	総合情報システム 栄養給食管理システムベンダー （※E 社の給食調理システムを提供している事業者でもある）
E 社	患者給食業務受託事業者
L 病院、M 病院	同様の給食システムを利用している他の医療機関
給食センター	E 社が運営する給食調理センター
ベンダー	システムやネットワーク、各種機器などの導入・構築、納品等を行う病院の外部委託事業者の総称
X	本事案のランサムウェアによるサイバー攻撃者
基幹システム	電子カルテシステムや医事会計システムなど中核となるシステムの総称
部門システム	調剤、検査、画像などオーダー連携やデータ連携が必要なシステムの総称
給食システム	栄養給食管理システム
サーバーA	給食センターの病院と連携するサーバー
サーバーB	病院の栄養給食管理システムのサーバー
ファイアウォールY	病院のファイアウォール（VPN 機器）
ファイアウォールZ	給食調理センターのファイアウォール（VPN 機器）
専門家チーム	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
半田病院	徳島県つるぎ町立半田病院
厚労省ガイドライン	「医療情報システムの安全管理に関するガイドライン（厚生労働省）」の略称
２省ガイドライン	「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（総務省・経済産業省）」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
リモートガイドライン	一般社団法人 保健医療福祉情報システム工業会（JAHIS）が発出する「リモートサービス セキュリティガイドライン」の略称

4. 調査委員会総括（報告書要約版）

今回の事案発生により、地域医療における病院の役割のかなりの部分を果たせない状況に陥り、患者や地域の方々に大きな影響を及ぼした。

情報セキュリティインシデント調査委員会は 2023 年 1 月から計 3 回の会合を開催し、本事案の状況や各種調査結果の内容を確認した。さらには、本事案の重要なステークホルダー 5 社および病院に対するヒアリング調査も実施した。本委員会としての報告の詳細は 5 章以降で記述するが、先に概要を以下にまとめる。

4.1　インシデントの概要

病院は、2022 年 10 月 31 日月曜日午前 7 時 45 分に電子カルテの障害発生により問題を認知し、8 時 30 分頃の調査でランサムウェアに感染していたことが A 社により確認された。感染経路や範囲が不明であったため、電子カルテに関連するすべてのネットワークの遮断および利用停止を行い、紙ベースのカルテ運用を開始した。

電子カルテを含む基幹システムの再開は、障害発生後 43 日目の同年 12 月 12 日、部門システムを含めた全体の診療システム復旧は障害発生後 73 日目の 2023 年 1 月 11 日であった。この間も限定されながらも診療継続を行い、システムの復旧状況に応じて病院は各診療機能を再開していった。

本事案は、病院が患者給食提供委託契約を締結していた E 社の給食センターのシステム構築事業者である C 社、および給食システムアプリケーションを提供している D 社がリモート保守に用いていたファイアウォール Z の脆弱性、または漏洩され公開されていた ID・パスワードを悪用して X が給食センターの情報基盤に侵入した。さらに C 社の情報基盤から病院に RDP[1]通信を用いて侵入。基幹システムや部門システムがランサムウェア「Elbie(エルビー)」に感染し、病院の電子カルテを含めたサーバーの大部分が暗号化され、ランサムノート（身代金要求文書）を提示し、内部侵入後には端末に不正なログオンを行った可能性もある事案であった。

今回のサイバー攻撃の侵入経路や攻撃の流れは、以下の通りと考える。

表 1　侵入経路と攻撃者の手順

No	項目	攻撃者（X）の手順
1	X が E 社給食センターに侵入	E 社給食センターに、C 社が設置したファイアウォール Z の脆弱性（または、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。

[1] リモートデスクトッププロトコル：Remote Desktop Protocol。Windows の標準機能で、接続先のコンピューターの画面を、ネットワークを通じて転送し、遠隔のコンピューターの操作を実現するもの。

No	項目	攻撃者（X）の手順
2	E 社探索・情報窃取	E 社給食センターのサーバーA の ID・パスワードが脆弱だったことから、X 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、給食センター内での攻撃拡大。
3	病院給食サーバー侵入	ファイアウォール Y を通じて、病院と E 社が常時接続の RDP 通信で結ばれていたことから、E 社給食センターで窃取した病院のサーバー認証情報を用いて、サーバーB に侵入。ウイルス対策ソフトをアンインストールした。
4	病院のシステム情報の窃取	サーバーB を踏み台に、病院の他サーバーの認証情報等を、X がツールを用いて窃取。なお、サーバーB と他サーバーの ID・パスワードが共通だったため、認証情報の窃取は容易であった。
5	他サーバー侵入	窃取した認証情報等を用いて、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）を表示した。

今回のサイバー攻撃は、自己増殖型のコンピューターウイルスが広域に拡散したわけではなく、X が手動で各機器に侵入し、ランサムウェアを実行したと考えられる。

なお、今回の事案における通信ログ、フォレンジック調査などにおいて、今回の攻撃において病院の情報システムから E 社給食センターへの顕著なデータ転送は観測されなかった。また、E 社が行ったフォレンジック調査結果や、病院が現在も実施している個人情報漏洩調査でも、外部への情報漏洩は確認されておらず、情報漏洩の可能性は極めて低い。

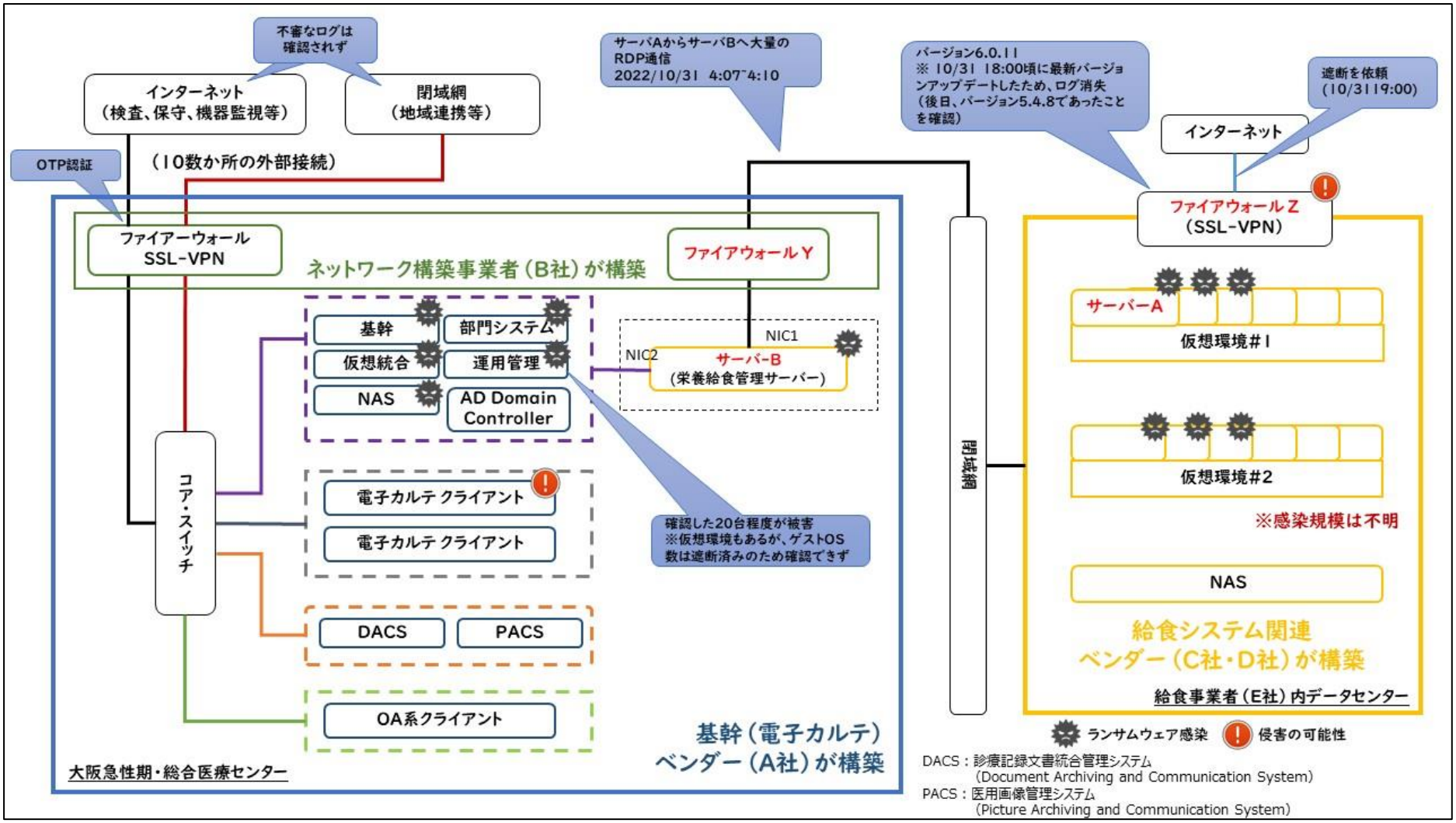


図 1　ネットワーク構成図と感染状況

4.2　発生要因と再発防止策

次に、本事案の直接的な発生要因と再発防止に係る提案について概略をまとめる。事案に関する詳細は、5 章を参照されたい。

まずは本事案の中核的な発生要因と、それに関連する周辺的な要因についてまとめる。

表 2　インシデント発生の中核的要因と周辺的要因の整理

項目	中核的要因	周辺的要因
組織的	● 電子カルテベンダーを始めとしたベンダーと医療機関の責任分界点が、契約を含む事前の取り決めがなく不明瞭であった。 ● 外部接続の方針やルール、運用が明確ではないなど、病院としてのセキュリティポリシーや仕様が明確ではなかった。 ● 情報資産の棚卸と把握が出来ていなかった。	● 給食事業におけるセキュリティ状況の把握が出来ていなかった。 ● インシデント対応可能な体制ではなかった。 ● 他の接続箇所や部門システムや機器を含む包括的な管理が不十分だった。 →総じて「IT ガバナンス」の欠如
人的	● 病院おけるセキュリティに関する知識と人材の不足。 ● ベンダーにおけるセキュリティの意識、知識、インシデント対応の経験や準備の不足。	● 各病院でセキュリティ専門家を配置することは難しかった。 ● 社会的なセキュリティ人材の不足。 ● 閉域網神話の中で医療 IT 人材のセキュリティに対する意識も知識も低下していた(技術的な周辺的要因とも言える)。
技術的	● RDP 通信の常時接続を、標準ポートを使用し、許可していた。 ● 管理者権限で運用し、管理者や利用者のパスワード運用が脆弱（初期パスワード最小桁数設定無し、パスワード共通化など）であった。	● ネットワークの境界を管理する機器の管理主体が曖昧であった。 ● 機器やシステムの脆弱性の未更新。 ● ウイルス対策ソフトが導入されていない。 ● セキュリティログの監視が実施できていない。

中核的要因は、医療機関とベンダーなどのいわゆるステークホルダーとの責任分界点の不明瞭さである。サイバーセキュリティインシデントが起きた際に、どちらがどの責任に基づき行動を行うのか、特に本事案に関連している A 社、B 社、C 社、D 社、E 社を始めとしたステークホルダーとの契約や役割分担が明確でなかったことに問題がある。なお、この責任分界点の不明瞭さは、インシデントが発生する前の段階においても同様であり、保守や脆弱性管理などのセキュリティ対策に係る役割分担など、インシデントを防ぐための行動についても誰が何をするかの責任が不明確であった。

さらに、病院におけるセキュリティに対する知識不足もさることながら、ベンダーの知識や意識、準備不足なども重なっていた。結果として、既定値のままのポートで RDP 常時接続が許可され、ユーザーにシステムの管理者権限が付与され、サーバーの管理者 ID とパスワードがほぼ同一であった。このように、一般的な対策が施されていなかったことによってインシデントが拡大した。

4.2.1. 組織的発生要因のサマリー

今回の攻撃者に侵入を許した要因として、組織的な発生要因についてまとめる。

① IT ガバナンスの欠如

システムや機器を使用する病院において、情報資産が把握されていないことに始まり、契約におけるセキュリティポリシーの不一致や責任分界点の不明瞭さ、脆弱性管理の役割分担など、組織的な IT ガバナンスが欠如していた。IT ガバナンスとは「経営陣がステークホルダーのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力」[2]のことである。以下に IT ガバナンス視点での問題点と予防に向けた提案を行う。

表 3　IT ガバナンスの問題と予防提案の整理

No	IT ガバナンスにおける問題点	予防に向けた提案
1	各契約単位で、保守や脆弱性管理といったセキュリティに関する責任分界点と役割が明確になっていない領域が存在した。	契約毎に、受注者と 2 省ガイドラインに基づいたサービス仕様適合開示書及びサービス・レベル合意書（SLA）により双方の責任分界点や役割を明確にし、文書化すること。
2	複数のベンダーが関与する契約において、そのプロジェクトマネジメント体制が明確になっていない状況があり、重要なセキュリティに関する事項について、関係者による十分なリスク評価が行われていないケースがあった。	合同企業体（JV）によるプロジェクトの場合（構築だけでなく保守も含む）は、受注側のプロジェクト体制を明確にさせるなど、責任の所在を明確にすること。
3	医療機器やその保守に係るセキュリティ仕様が、総合情報システムにおけるセキュリティ仕様に適合していないケースがあり、運用が共通化されていなかった。	調達が行われる場合には、病院共通のセキュリティポリシーに基づく共通仕様を作成し、共通運用となるような調達を行うこと。
4	医療情報部で調達している情報資産以外の医療機器（リモート保守用機器を含む）や建築関係の情報システムについて、一元管理されていなかった。	診療情報系のネットワークに接続されている機器やシステムはすべて情報資産としてリストアップしたうえで、安全管理上の重要度に応じて分類し、リスク分析を実施すること。
5	総合情報システムの仕様における厚労省ガイドラインは第 4.3 版であるが、現時点では第 5.2 版まで更新されている。第 5.2 版についてベンダーを交えて組織的に検証されている状況が確認されなかった。	ガイドライン改定時には組織的に適合状況を確認し、不足している項目があれば改善に向けた PDCA サイクルを回す活動を行うこと。

[2] 経済産業省「システム管理基準（骨子）」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanrikosshi_h30.pdf#page=4

No	IT ガバナンスにおける問題点	予防に向けた提案
6	2022 年 4 月より診療報酬で位置づけられた医療情報システム安全管理責任者について、その役割等の組織内での認知が不十分のようであった。	医療情報システム安全管理責任者を軸とした IT ガバナンスを効率的効果的に運用する組織体制を構築すること。

2020 年 8 月 21 日に策定されている 2 省ガイドラインにおいては、契約や共通理解について、「契約書や SLA などの契約上の文書による明示的な合意とは別に、共通の理解を形成することであり、その取組みの記録として議事メモや作業記録などの文書等に残すことは重要である。対象事業者は、医療機関等との共通理解のうえで、契約書や SLA などの契約上の文書を作成し、医療機関などと明示的な合意を形成すること」としている。本調査の中では、今回のステークホルダーにおける契約前、契約中の共通理解の形成が不足していたことが確認された。

また、病院の情報資産が一元的に管理されていない実態も明らかになった。医療における急速かつ高度なシステム化の流れにより、これまで電子カルテを含めた診療情報のネットワークに接続されていなかった医療機器が、データ連携のために接続されるようになった。リモート保守用の外部接続や、医療 DX（デジタルトランスフォーメーション）の急速な流れの中で、外部ネットワーク化による診療情報共有といった外部接続が急速に拡大していく流れの中では、より組織的な情報セキュリティ方針の下での資産管理が行われるべきであったが、それが病院ではできていなかった。この状況を誘発した原因の一つとして、情報システムを調達・管理する医療情報部門と、医療機器や建築設備を調達する施設管理部門が異なることが考えられる。

さらに、管理者が曖昧な機器や情報部門が監視できていないシステムやネットワークなどの存在が確認でき、ログの管理や監視などの「運用」についても組織内で曖昧な状況にあるなど、組織的な IT ガバナンスが欠如していた。

② 契約に関する諸問題

上記の IT ガバナンスが欠如していた影響により、契約に関する諸問題も生じていたことが明らかになった。さらに言うと、IT ガバナンスの欠如を誘発した根本的原因が契約問題であったともいえる。

契約に関する諸問題について、以下に整理する。

1）契約の規定があいまいで、セキュリティ対策について、誰が何を行うべきかが曖昧になり、お互いに相手がやってくれると期待し、結局誰も適切な対応を行わず、インシデントの発生および損害の拡大につながった可能性がある。今後の契約においては、単に 3 省 2 ガイドラインに従うということだけでなく、実施しなければならないセキュリティ対策を具体的に規定することが必要である。これにより誰が何をするかが明らかになり、インシデントの防止につながる。

2）今日のように技術の発達の速度が速い時代においては、契約書に具体的なセキュリティ対策を記載しても、時間とともにそれでは対策が十分ではなくなってしまう。今回の事件においても、契約締結時点でははっきりと認識されていなかった新たなリスクへの対応不足が事故につながった可能性が高い。そのため、今後は契約書の中に契約締結時点で考えられる具体的なセキュリティ対策を規定する

とともに、将来発生するリスクに対応するための規定を入れることが必要である。例えば、インシデント予防のためのアドバイス、情報提供を行う義務についての規定やインシデント発生時における協力体制についての規定などを入れることが望ましい。

3）いくら良い契約を締結しても、それを遵守していなければ絵に描いた餅である。本件においても当事者が契約の不遵守を知っていながら放置していて被害が拡大した可能性がある。今後の契約書においては、契約の当事者が契約をきちんと遵守していることを確保するための規定を入れることが望ましい。例えば、セキュリティで言えばセキュリティポリシーが契約書通りに運用されているかなど、一定期間ごとに契約が遵守されていることについての第三者による監査の規定を入れることが考えられる。

このような契約段階でのリスクを回避するためには、

1）共通したセキュリティポリシーによる調達
2）契約時のガイドラインに基づく文書確認（責任分界点や役割分担の確認）
3）医療情報部門との情報共有による情報資産管理の徹底
4）複数のベンダーによる保守を含んだ契約の場合のプロジェクトマネジメント体制の確認
5）保守を含んだ契約の場合の保守方法の確認

といった視点による予防措置の実施が必要と考えられる。そして、これらは IT ガバナンスの中で議論され改善されていくことが望ましい。病院には機構本部と連携したうえで、問題点などの解決を行っていただきたい。

病院としての統一したセキュリティポリシーの確立と、情報システムにつながる、情報システムを操作する、もしくは患者情報を取り扱うあらゆる契約に対する SLA 締結を通じた情報部門の関与が極めて重要である。

4.2.2. 人的発生要因のサマリー

病院は情報企画室を設置し、人員も豊富なようにも見えるが、基幹システムや部門システムで約 70 システムある環境において、決して潤沢な要員とは言えない。またセキュリティに対する高い知識を有しているわけではなく、ましてやインシデント対応を経験した人材もいない。

一方、ベンダーの現場担当の人材もセキュリティに対する知識や経験は同じような状況であったため、日常的な病院とベンダーのセキュリティ面からの相互間連携が不足していた。このような状況の中では、病院全体のシステムの脆弱性が進むとともに、サイバー攻撃にあった際の非常時対応も混乱していた。

こうした状況を生み出した背景には、「医療機関は閉域網だからセキュリティは問題ない」といった誤った閉域網神話の中で、両者のセキュリティに関する意識が薄れ緩慢になっていったことが挙げられる。セキュリティ向上について双方が先進の知識を習得し、常にリスク評価を行いながら協議を継続していれば、組織的、技術的な課題は事前に解決できていた可能性がある。特にベンダーはシステムや機器を提供する専門家として、サイバーセキュリティの知識と経験向上に努めるべきであった。病院も、セキュリティ意識を高く持ち、組織的にシステムや機器の導入および運用を心掛けた取り組みが必要であった。

4.2.3. 技術的発生要因のサマリー

今回の侵入経路は、E 社の給食センターを経由したサプライチェーン攻撃であった。侵入経路となったファイアウォール Z のファームウェア更新は行われておらず、当該機器の ID とパスワードの漏洩も確認された。また、病院は C 社の依頼にしたがって、ファイアウォール Y において、E 社の情報システムからの RDP 通信（ポート番号：3389）を常時接続可能にし、その後、運用状況の確認や改善を怠ったため、E 社への攻撃が病院に波及した。

外部接続（リモート保守）に係る発生要因と再発防止策については、以下の通り整理する。

表 4　外部接続（リモート保守）に係る発生要因と再発防止策の整理

No	発生要因	再発防止策
1	VPN 機器やファイアウォールなどの外部通信機器の保守における脆弱性管理の役割分担が曖昧だった。	機器毎に管理者と設置者が互いに保守の範囲や脆弱性管理の役割分担等について文書により確認を行う。
2	リモート保守を許可するための基準が曖昧で、またリモート保守を行う側のセキュリティ環境の確認が不十分だった。	外部接続やリモート保守を許可する場合の基準を定めるとともに、許可申請を受ける場合には、通信元のセキュリティ環境を確認する体制を構築する。
3	外部接続（リモート保守）を許可した後に、その利用状況を確認していなかった。	外部接続やリモート保守を行う場合は、相手にその目的や時間を確認したり、通信ログの確認を行ったり、他の不正なアクセスなどの記録が残されていないかを確認する運用を構築する。

さらに、閉域網の安全性を過信していたことにより病院の情報システムのセキュリティが脆弱となっていた。そのため、侵入後にその機器を足掛かりにネットワーク伝いに次第に重要なサーバーや機器に近づく、いわゆる「横展開（水平展開）」を許してしまった。

これまで医療機関においては「医療機関内部のシステムは外部とはつながっていない閉域網だから安心」という認識に基づいて、セキュリティを考えない傾向にあり、脆弱性が放置され、セキュリティを高める設定が行われない状況がある。その悪しき慣行も本事案を発生させる要因となってしまった。本事案においても、Windows の初期設定が適切に変更されていれば、大規模に横展開されることなく、インシデントの広がりを防げた可能性が高い。

横展開を許し大規模システム障害の要因となった主な初期設定の内容を、以下の通り整理する。

表 5　横展開を許した初期設定とその再発防止策の整理

No	横展開を許した初期設定	再発防止策
1	ユーザーすべてに管理者権限を与えていたため、X に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。	● ユーザーは原則管理者権限のない標準ユーザーアカウントに設定。 ● 管理者権限を持つユーザーは、「administrator」のような安直なユーザー名を利用しない。 ● ユーザーアクセス制御[3]を適用させ、管理者権限を要する重要な操作が意図せずに自動実行されることを防ぐ。
2	Windows のパスワードが、サーバー、端末毎にすべて共通であり、一つのパスワードが窃取されると、他のすべてのサーバー（端末）が乗っ取り可能な状態。	Windows のパスワードを、サーバー、端末毎にすべて個別化（ユニーク化）。
3	アカウントロックアウトの設定が無く、パスワード総当たり攻撃や辞書攻撃によりパスワードを数多く試行されログオンが成功した。	アカウントロックアウトの設定を有効化。
4	電子カルテシステムサーバーにウイルス対策ソフト未設定のため、容易に侵入され、ランサムウェアを実行された（他のサーバーや端末にはウイルス対策インストール済み）。	電子カルテシステムサーバーにもウイルス対策ソフトをインストールする。

1 から 3 については、本来であればシステム構築時に病院とベンダーが十分にリスク評価しながら初期設定を検討すべきところ、病院はベンダー任せになっていたようであった。重要な設定に係る確認事項についても、病院、ベンダー双方で文書に残していなかったのも問題である。

4 については、電子カルテサーバーにウイルス対策ソフトを導入しない慣習からは早期に脱却すべきである。病院においても、総合情報システム全体ではウイルス対策ソフトの導入が行われていたが、電子カルテシステムのサーバーに対しては、レスポンス低下を危惧したためか、ウイルス対策ソフトが導入されていなかった。サーバーB を踏み台に次に横展開した先は、電子カルテに係る各サーバーであり、わざわざウイルス対策をアンインストールしなくても簡単に攻撃ツールを設置し、暗号化ツールを実行できたことが、フォレンジック調査の結果、明らかになっている。

なお、医療情報に係るネットワーク上には、ネットワークの境界を不明瞭にしてしまうなどの課題のある NIC[4]二枚挿し[5]のサーバーや端末を経由した、医療情報部門が管轄していないシステムや機器なども数多く接続されており、それらにはウイルス対策ソフトが設定されていない場合も散見された。

---

[3] User Account Control：UAC。ユーザーの意図しない操作が勝手に実行されたり、許可していないプログラムが起動するのを防ぐ Windows のセキュリティ機能。

[4] Network Interface Card、ネットワークインターフェースカード。

[5] 一台のコンピューターに 2 枚の NIC を挿入し、それぞれ異なるネットワークセグメント間での通信を実現すること。

4.3　調査委員会としての気付き事項と国に期待する事項

本委員会活動を通じて気になった状況および国に対する期待について、以下の 4 項目に整理する。

①　地域医療への脅威からの保護

本調査の結果、今回の事案はどの医療機関でも起こりうることが判明した。本報告書の内容を、各医療機関および各行政機関が真摯に受けとめ、対応に当たらなければ、地域医療は常に脅威に晒され続けることになる。医療 DX が進み、全国的な医療分野のネットワーク化が推進される中で、我が国の重要インフラの一つである医療分野の情報セキュリティが向上しなければ、国民に対して安心安全な医療を提供できなくなる。

ガイドラインや法整備、財源の確保など、国の役割はさらに重要になるというのが、本委員会の一致した意見である。

②　役割と責任分界点の明確化

本委員会では、厚労省ガイドライン、2 省ガイドライン、リモートガイドラインの 3 つのガイドラインをテーマに、ヒアリング調査を行った。

ヒアリング調査は、事案当事者である病院と、そのシステム構築全般を行った基幹ベンダーおよびネットワークシステムベンダー、今回の侵入経路となったサプライチェーンである給食提供事業者、そしてそれぞれの事業所で給食システムの構築および運用を行っていた部門システムベンダーについて行った。

その中で本委員会として気になったことは、それぞれの責任分界点や役割分担が非常に曖昧で、システムや機器の管理や運用などについて「契約相手がやるものと思っていた」という発言が多かったことや、重要な設定について「言った」「聞いていない」といった双方の発言が食い違い、また記録が残されていない事例が非常に多かったことである。このような状況では、いわゆる「ポテンヒット」が生まれてしまう土壌が大いにあったことが、今回の事案を誘発した状況にあったことが推察される。

一般的に、医療情報システムの受注者側が情報システムやセキュリティに関して発注者側よりも見識を有しており、発注者側と受注者側間では、情報の非対称性が存在する。2 省ガイドラインが提起している、「サービス仕様適合開示書」の提示や、「サービス・レベル・アグリーメント（SLA)」の締結、さらに両者が定期的にこれらを更新するような運用が行われ、契約文書として双方の役割が明確になっていれば、このような状況には至らなかった可能性が高いというのが本委員会としての見解である。

医療現場では、患者に対する「説明と同意（インフォームドコンセント)」というのは、日常的に行われているが、事業者との調達契約においては、こうしたインフォームドコンセントが十分に行われていないのが実状のようである。

ガイドラインの運用推進および周知徹底は国の役割でもあるため、その責務をしっかり果たし、発注者と受注者の役割や責任分界点の明確化を推進していくことが必要である。

③　閉域網意識の見直し

今回の調査を通じて、「医療機関は閉域網の中にあるので安全だと思っていた」「OS のサポートが切れていても閉域網の中なので問題ないと思った」「医療機関は閉域網なので、ウイルス対策は不要と考えていた」といった発言が、システムベンダーや医療機器メーカーから相次いだ。特に印象的だったの

は、外部接続を構築した事業者から「リモートサービスセキュリティガイドラインの存在は知らなかった」といった発言があったことだ。

これまで医療情報システムは「インターネットなど外部と隔離されていることで安全性が担保されている」という「神話」が信じられてきた。実際には様々な支援や保守をリモートで受けていたり、医療DXの中でネットワーク化が急速に進んでいたりするなど、すでに閉域網神話は崩壊している。医療分野の情報セキュリティの低下は、神話にすがって怠惰になっていた医療界全体の問題でもあるというのが、本委員会としての見解である。

医療分野においても高度かつ複雑な様相を呈するシステム化やネットワーク化が推進される中で、医療系事業者におけるセキュリティ意識および見識の向上は早急に求められる。リモートサービスを行う場合や、医療機器におけるOSアップデートのルール策定など、セキュリティ対策向上に資するレギュレーションの策定や整備を行うとともに、それらを業界に対し浸透させていく取り組みが求められている。

④　医療継続支援への更なる取り組み

今回の事案における被害額についてはまだ精査中とのことだが、調査・復旧費用で数億円、診療制限に伴う逸失利益としては十数億円以上を見込んでいるという。ランサムウェアにより大規模システム障害に至った場合の財務上の影響は甚大である。

今回の事案以外にも、全国各地の医療機関でランサムウェアと思われるシステム障害が大小問わず次々に発生している。現代の医療は情報システムに大きく依存しているという現実を鑑みれば、大規模システム障害が起こりうる状況にあるという前提で、起きた時を想定した対策が必要となる。各医療機関は、大規模システム障害が発生した時にどのように医療継続を行うか、システム復旧に必要なバックアップがランサムウェア攻撃等によって失われないようにするためにどのように確保するか、バックアップからどのように速やかにシステム復旧を行うか、といった大規模システム障害を想定したBCPやコンティンジェンシープラン[6]の準備を進めるべきである。

そして国は、医療機関へのサイバー攻撃を災害の一つとして捉え、初動対応支援チームの更なる整備、サーバーや端末の備蓄および緊急時の拠出、診療報酬の優遇措置など、サイバー攻撃にあった医療機関に対する支援対策を充実させることで、医療が機能不全に陥ることを回避し、速やかに医療復旧できるような態勢を整え、患者が安全安心の医療を受けられるよう、更なる取り組みを推進するべきである。

[6] 事故や災害など非常事態が発生した場合に備えて、対応策をまとめた計画。緊急時対応計画。

5. 調査委員会報告（報告書詳細版：概要～インシデント対応～再発防止策）

ここから 4 章で述べた要約に至った背景、事故内容の詳細や調査結果、発生要因、解決策提言について整理する。

5.1. 大阪急性期・総合医療センターについて

5.1.1. 病院の組織概要

まず、大阪市南部の拠点病院である病院の組織概要について紹介する。

病院は一般病床 831 床、精神 34 床、計 865 床を有する医療機関で、そのうち ICU、CCU、SCU、HCU、MFICU、NICU、GCU を計 91 床を有する基幹災害拠点病院、地域医療支援病院などの特徴を有する大阪市南部の拠点病院である。また診療科は 36 を有し、医師は研修医を合わせると 300 人超、そして看護職員数は 1,024 人を有する。さらには病院の実績として、延べ入院患者数は 22.3 万人、延べ外来患者数 29.5 万人（2021 年度）と地域医療を支えている。インシデントが発生する前の実績を表 6 にまとめる。なお、データは 2022 年 4 月 1 日時点。

表 6　大阪急性期・総合医療センター概要

項目	内容	詳細
病床数	865 床	一般：831 床、精神：34 床 うち、ICU,CCU,SCU,HCU,MFICU,NICU,GCU　計 91 床
職員数	2,014 人	医師数；259 人、研修医 50 人 看護師数；1,024 人
診療科	36 診療科	臨床研修指定病院 基幹災害拠点病院 日本臓器移植ネットワーク 特定移植検査センター 障がい者医療・リハビリテーションセンター 地域医療支援病院 高度救命救急センター 地域周産期母子医療センター 地域がん診療連携拠点病院 がんゲノム医療連携病院 大阪府難病診療連携拠点病院 大阪府がん患者妊よう性温存治療実施医療機関 大阪府小児地域医療センター 卒後臨床研修評価機構認定病院 日本医療機能評価機構認定病院 ISO 9001 認証取得 ISO 15189 認定取得

新型コロナウイルス感染症対応前の 2019 年度から直近 2021 年度までの事業実績を表 7 に示す（大阪コロナ重症センター分を除く）。

表 7　大阪急性期・総合医療センター事業実績

項目	2019 年度	2020 年度	2021 年度
医業収益	309.4 億円	286.7 億円	296.2 億円
新入院患者数	23,649 人/年	18,440 人/年	18,256 人/年
延入院患者数	273,683 人/年 748 人/日	224,353/年 615 人/日	218,529 人/年 599 人/日
初診患者数	35,828 人/年	25,842 人/年	27,262 人/年
外来患者数	335,114 人/年 1,396 人/日	289,309 人/年 1,191 人/日	294,942 人/年 1,219 人/日
紹介率	94.7%	98.6%	101.5%
平均在院日数（一般病棟）	9.2 日	9.7 日	9.6 日
救急車搬入患者数	9,872 人/年	5,628 人/年	6,390 人/年
手術件数（眼科除く）	6,940 件/年	5,959 件/年	6,164 件/年
医業収支比率	99.5%	93.2%	93.9%
給与費比率	45.8%	50.9%	49.8%
材料費比率	32.1%	31.3%	32.1%

5.1.2.　病院の災害対策体制の概要

病院では、都道府県に 1 か所指定された基幹災害拠点病院として、大阪府内で災害が起きた場合には、災害拠点病院間の患者転送と、緊急医療班派遣を調整する任務があり、大阪北部地震や北新地の火災の際にもその活動を行っていた。また、府内の災害拠点病院に対し災害医療研修と災害医療訓練を行っていた。

2020 年 4 月からは災害対策室を設置し、DMAT 資格を持った専従者を配置し BCP の見直しなどを図りながらより一層の災害対策対応に取り組んでいたところで、新型コロナウイルス感染症対応においても、病院の新型コロナ対策本部の運営を行うなど、災害対策室を中心に非常事態対応に取り組んでいた。

今回の大規模システム障害においても、障害初日から BCP 対策本部会議を開催し、大規模システム障害における医療継続の方向性を検討した。災害対策室が中心となって、議事内容を取りまとめ、その日のうちに職員に周知・情報共有することで、BCM（事業継続マネジメント）を行った。それを連日繰り返すことで、病院全体の PDCA サイクルを回していた。

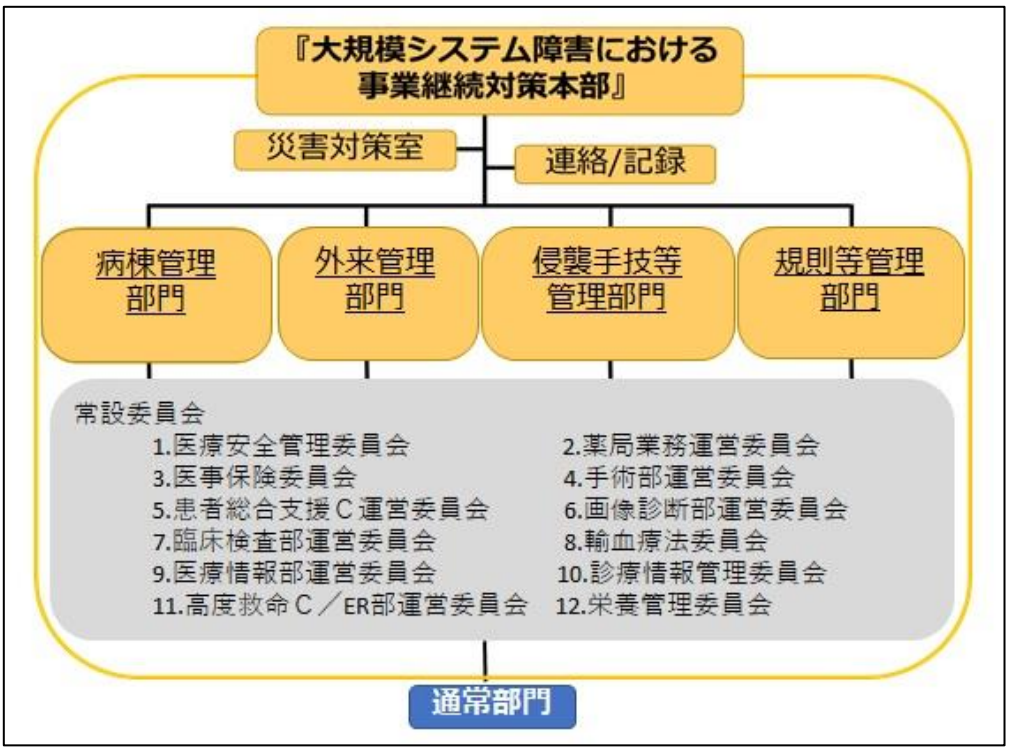


図 2　大規模システム障害における事業継続対策本部組織図

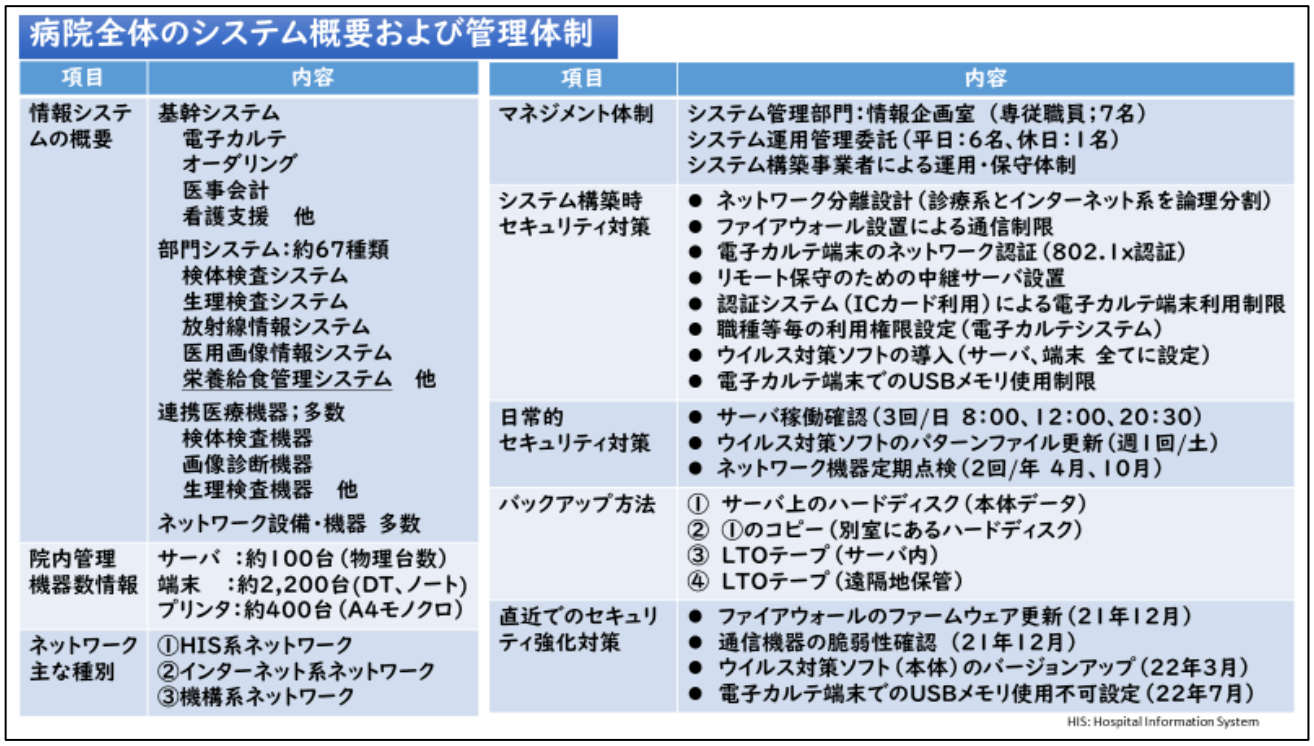
5.1.3.　病院の情報システム概要と管理体制

病院では 2018 年 3 月から、第 6 期総合情報システムの運用を開始している。契約は A 社系列のリース会社と 6 年間の保守も含めたリース契約を締結していた。総合情報システムを管理する体制として、専従職員 7 人に加え、システム運用管理（ヘルプデスク業務）委託の職員（平日 6 人、休日 1 人体制）により総合的な運用を行っていた。

基幹システムは、電子カルテシステム、オーダーリングシステム、看護支援システム、医事会計システム、データウェアハウス（DWH）の 5 つのサブシステムで総合情報システムの中核を構成している。部門システムには、総合情報システムの中で調達を行っている 39 のシステムに加え、別調達の部門システム 28 の計 67 のシステムが､基幹システムとデータ連携を行いながら総合情報システムを構成している。これらに加え、データ連携が必要な画像診断機器（CT、MRI など）や検査機器（エコー、心電図、血液分析機器など)、調剤機器といった医療機器が少なくとも 270 台以上あることから、かなり複雑なシステム構成となっていた。

セキュリティ対策としては、電子カルテ端末の USB メモリの使用制限や、ウイルス定義ファイルも定期的に更新するなどの仕組みを構築していた。

病院の体制や対策等をまとめると以下の図の通りである。



病院全体のシステム概要および管理体制

項目	内容
情報システムの概要	基幹システム 電子カルテ オーダリング 医事会計 看護支援　他 部門システム：約67種類 検体検査システム 生理検査システム 放射線情報システム 医用画像情報システム 栄養給食管理システム　他 連携医療機器；多数 検体検査機器 画像診断機器 生理検査機器　他 ネットワーク設備・機器　多数
院内管理機器数情報	サーバ　：約100台（物理台数） 端末　：約2,200台（DT、ノート） プリンタ：約400台（A4モノクロ）
ネットワーク主な種別	①HIS系ネットワーク ②インターネット系ネットワーク ③機構系ネットワーク

項目	内容
マネジメント体制	システム管理部門：情報企画室（専従職員；7名） システム運用管理委託（平日：6名、休日：1名） システム構築事業者による運用・保守体制
システム構築時セキュリティ対策	● ネットワーク分離設計（診療系とインターネット系を論理分割） ● ファイアウォール設置による通信制限 ● 電子カルテ端末のネットワーク認証（802.1x認証） ● リモート保守のための中継サーバ設置 ● 認証システム（ICカード利用）による電子カルテ端末利用制限 ● 職種等毎の利用権限設定（電子カルテシステム） ● ウイルス対策ソフトの導入（サーバ、端末　全てに設定） ● 電子カルテ端末でのUSBメモリ使用制限
日常的セキュリティ対策	● サーバ稼働確認（3回/日　8:00、12:00、20:30） ● ウイルス対策ソフトのパターンファイル更新（週1回/土） ● ネットワーク機器定期点検（2回/年　4月、10月）
バックアップ方法	① サーバ上のハードディスク（本体データ） ② ①のコピー（別室にあるハードディスク） ③ LTOテープ（サーバ内） ④ LTOテープ（遠隔地保管）
直近でのセキュリティ強化対策	● ファイアウォールのファームウェア更新（21年12月） ● 通信機器の脆弱性確認（21年12月） ● ウイルス対策ソフト（本体）のバージョンアップ（22年3月） ● 電子カルテ端末でのUSBメモリ使用不可設定（22年7月）

HIS: Hospital Information System

図 3　病院全体のシステム概要および管理体制概要図

病院のシステム管理体制としては、明らかに不足している状況ではないと考えるが、調査の結果、以下の課題が明らかになった。

① 外部接続管理

- 外部接続の状況をすべて（特に施設設備調達関係について）は把握していなかった。
- 外部接続を行う際に、その必要性やリスク評価を十分に行えていなかった。
- 定期的に外部接続の運用状況を確認していなかった。
- 外部接続機器（VPN 機器など）の脆弱性管理やファームウェアアップデートの役割分担が明確ではなかった。

② 情報資産管理

- ネットワークに接続されている情報資産の設置状況をすべて(特に施設設備調達関係について)は把握していなかった。
- その機器でどのような OS が使用され、どのようなセキュリティ対策が設定され、その脆弱性管理がどのようにされているかを、すべては把握していなかった。

③ バックアップ

- バックアップが、復旧に必要なシステムソフトウェアや設定ファイルなどを含めて、正しく仕様通りに取得できているか、確認できていなかった。

なお、現在、病院で稼働している第 6 期総合情報システムの概要を、次の図で示す。

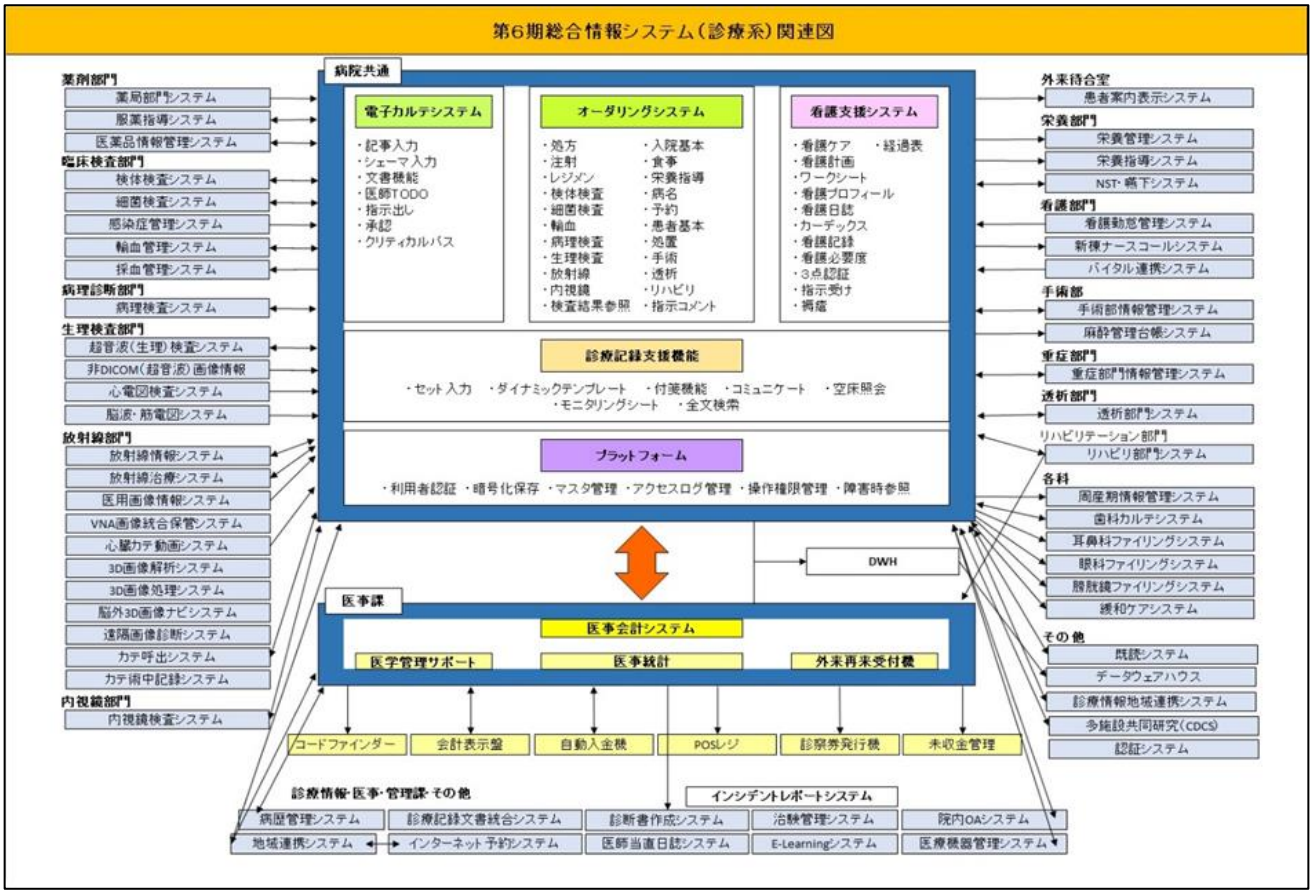


図 4　第 6 期総合情報システム（診療系）関連図

5.1.4.　給食システムについて

E 社との給食委託業務の契約を締結したのが 2017 年 7 月で、2018 年 4 月から 5 年間の契約を行った。

一方、病院給食部門システムは、A 社系列のリース会社と 2017 年 3 月に契約を締結した第 6 期総合情報システムの一つの部門システムとして、A 社がサーバーの準備及び設定、C 社が E 社の情報システムとの連携基盤構築、D 社が給食システムアプリケーションの提供と設定といった役割で構築された。

E 社の給食センターの情報システムにおいても C 社が情報基盤を、D 社がアプリケーションを構築・保守していた。なお、E 社は同じ情報システムを用いて、他の医療機関にも給食サービスを提供していた。

5.1.5.　ステークホルダーとの契約について

病院は、A 社系列のリース会社と 2017 年 3 月に総合情報システム賃貸借契約を締結し、2018 年 3 月から 6 年間の保守も含めたリース契約を締結している。A 社は統括事業者として位置付けられており、その配下に、給食システムを構築している C 社と給食システムアプリケーションを提供している D 社が位置付けられている。病院全体のネットワークやファイアウォールの設定はリース契約の中で B 社が行っている。

一方、患者給食提供業務については、E 社と 2017 年 7 月に締結し、2018 年 4 月から 5 年間の業務委託契約が開始されている。E 社の給食システム構築とアプリケーション提供を行っているのも、病院と同じ C 社と D 社である。以下、その状況を相関図にて示す。

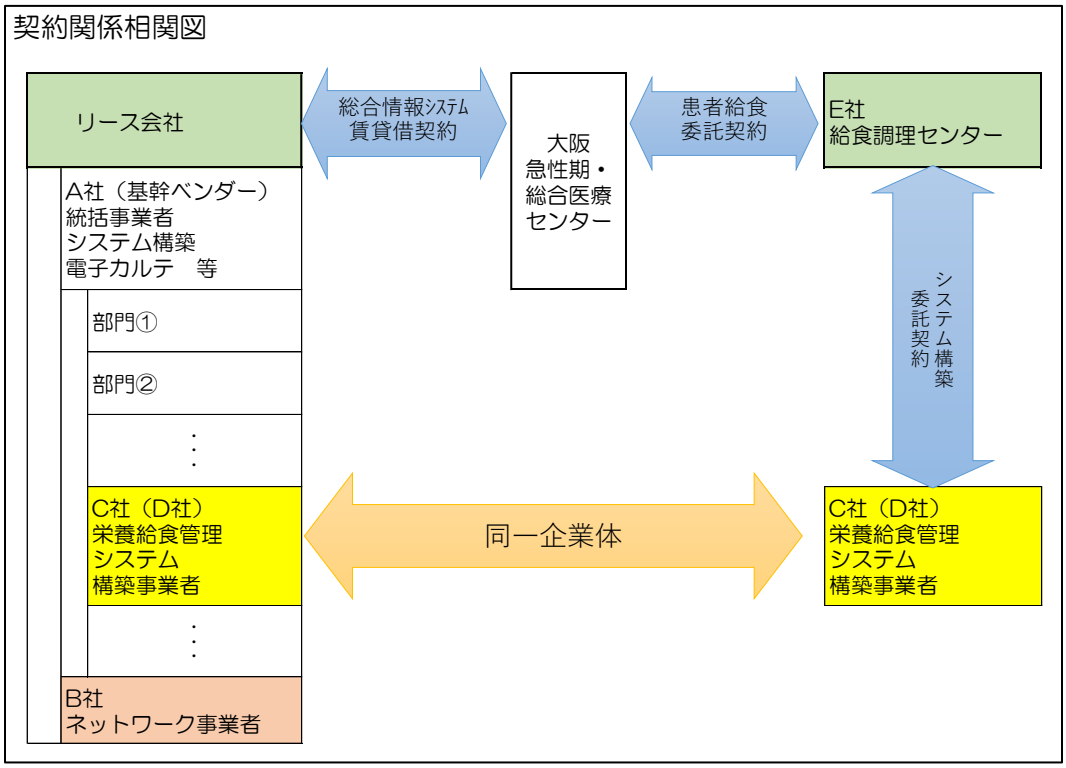


図 5　契約関係相関図

5.2.　発生した重大インシデントの内容について

5.2.1.　重大インシデント概説

2022 年 10 月 31 日月曜日早朝、E 社の給食センターのサーバーＡから、病院が管理するサーバーＢへリモートアクセスが行われ、サーバーＢを踏み台にして、電子カルテシステムを始め様々な部門システムにランサムウェアを感染させる攻撃が行われ、システムを使用停止せざるを得ない事態に陥った。病院は医療継続のために、紙カルテ運用の開始、外来診療の制限、救急受入の停止、予定手術の停止などを判断し、関係者への連絡や連携を行った。

病院や電子カルテシステムベンダー、部門システムベンダーなども、サイバー攻撃に対するインシデント対応の経験がなく混乱が生じていた。そこで、厚生労働省に初動対応支援を依頼し、3 名の専門家チームが派遣され、初動対応にあたった。発生当日には病院に設置していたファイアウォールＹの検出状況から、専門家チームは E 社経由のサイバー攻撃であると判断した。

しかし、病院のそれ以外の外部接続箇所が不明瞭で、多数存在することも確認できたことから断定には至らなかった。また同日 E 社の給食センターのシステム管理を受託している C 社がファイアウォールＺの更新作業を実施し始めるなど、証拠保全の動きがなかったため、専門家チームは警察庁および大阪府警察本部との調整を開始した。

感染した端末のランサムノートから Elbie ランサムウェアを用いた攻撃者グループ「Phobos（フォボス）」の可能性が高いことが推察されたが、複数の部門システムが感染していたこと、外部接続箇所や経路が多数存在すること、感染した環境と同一セグメントにサーバーやクライアント端末が存在することに加えて、ファイアウォールＹを始めとしたネットワークセキュリティ機器のログや Active Directory サ

ーバーのログなどの確認可能なログからは、いつから感染していたか確証を持てず、個々のサーバーや端末の正常時との比較ができない状況であった。そのため、オフラインで保存されていた患者のデータを用いて、端末・サーバーをすべて初期化する方針を立て、2 か月強で復旧を行った。

病院は、状況を説明するための記者会見を速やかに開くなど、一貫して情報公開を行った。また予定手術を 11 月 4 日に再開したほか、オフラインバックアップデータを参照可能にするシステムを 11 月 9 日までに、基幹システム（電子カルテシステム、オーダーリング、医事会計等）を 12 月 12 日までに、部門システムを翌年 1 月 10 日までに段階的に構築・接続し、2023 年 1 月 11 日から通常診療を再開した。

システム障害により全期間にわたり電子カルテシステムが停止していた 2022 年 11 月の患者数の実績は下表のとおりであり、地域医療に大きな影響を及ぼしたことがわかる。

表 8　大阪急性期・総合医療センター2022 年 11 月診療実績

	2021 年 11 月	2022 年 11 月	対前年同月対比
新入院患者数（人）	1,674	558	33.3%
延入院患者数（人）	19,267	10,191	52.9%
初診患者数（人）	2,605	465	17.9%
延外来患者数（人）	25,575	15,744	61.6%
手術件数（件）	597	168	28.1%
救急車搬入件数（人）	679	88	13.0%

なお、電子カルテシステムが完全に復旧するまでの 2 か月強の間、本事案に起因する死者は一人も出ていない。

5.2.2. 重大インシデント発生全体図

以下に今回発生した重大インシデントの全体像をまとめる。脆弱性は CWE、攻撃手法は MITRE ATT&CK より選択した。

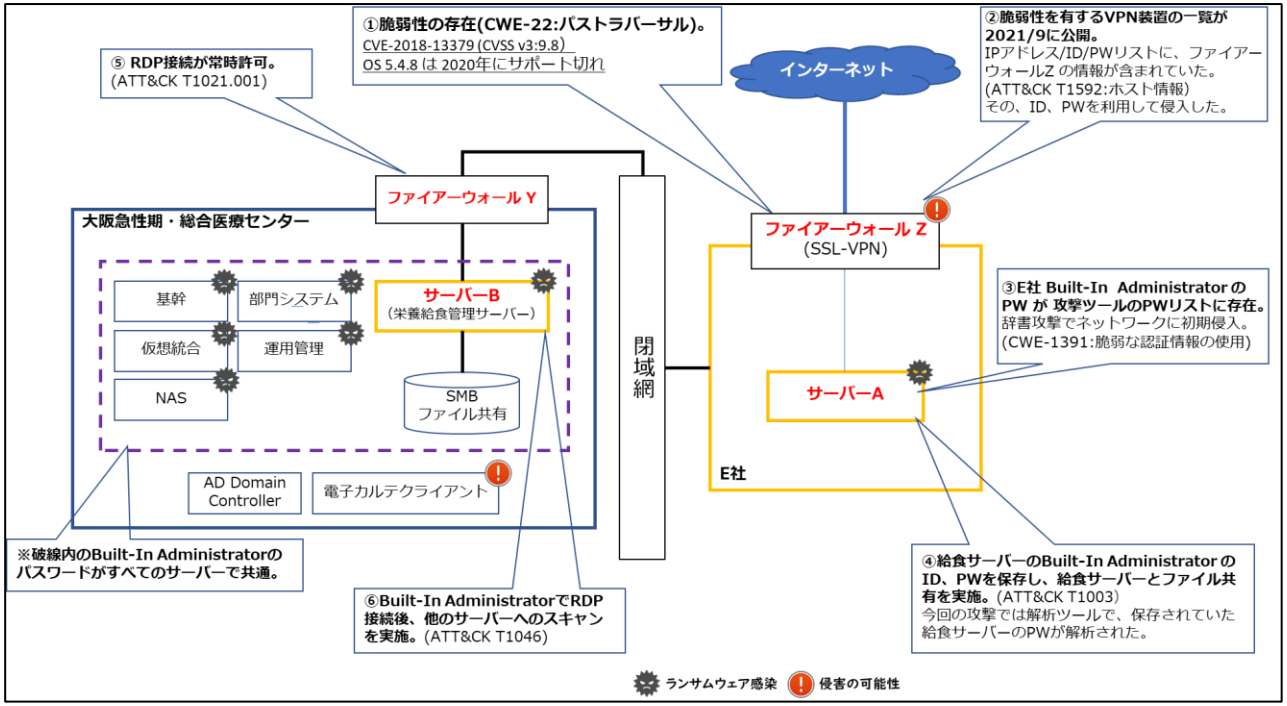


図 6　重大インシデント全体像

項番	内容
① CWE-22:パストラバーサル	ファイル名指定の実装に問題があり、攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行ってしまう脆弱性。
② MITRE ATT&CK T1592:被害者ホスト情報の収集	攻撃者は被害者のホストに関する情報を収集する場合がある。ホストに関する情報は、オンライン等を介して攻撃者に公開される可能性がある。
③ CWE-1391:脆弱な認証情報の使用	攻撃者が計算、導出、再利用、または推測できる脆弱な資格情報の使用。
④ MITRE ATT&CK T1003:OS 資格情報のダンプ	ツールを使用した OS に保存されている資格情報の解析。
⑤ MITRE ATT&CK T1021.001:RDP	有効なアカウントを使用し、RDP で遠隔地のコンピューターにログオン。
⑥ MITRE ATT&CK T1046:ネットワークサービスの探索	ネットワーク上で公開されているサービスをツールでスキャンし、攻撃に利用する。

5.2.3. 重大インシデント発生による病院の混乱

ランサムウェアによるインシデントと認知し、病院のシステムとネットワークを遮断し、電子カルテシステムおよび関連システムが使用できなくなったことにより病院は大混乱に陥った。2022 年 10 月 31 日月曜日午前 8 時 30 分頃、事務局からシステム障害の報告を受けた総長・病院長は、ただちに状況確認のための緊急会議の招集を指示し、午前 8 時 50 分に幹部職員等による会議を開催。会議では総長・病院長は、外来診療の停止、救急受入の停止、予定手術の中止などを判断し、病院の定める（本来は自然災害を想定した）事業継続計画（BCP）に基づき、紙カルテ運用への移行を決定。同日 12 時に BCP 対策本部会議を招集した。その間、情報収集や各方面への連絡などの対応が指示された。

BCP 対策本部会議を災害対策室主導で運営を開始。復旧の見通しが立たず障害が長期化することが見込まれる中、各現場における診療状況や紙運用への移行状況を確認したうえで、紙運用の見通しが立つまでの当面の間は、「予定手術中止」「救急受入停止」「外来化学療法と緊急手術は継続」「外来、新規患者は受けない」「入院患者の転院調整および外来診療の対応については各科判断」「11 月 1 日と 11 月 2 日の診療規模を可能な限り縮小する」と判断し、各部門に対応を指示。なお、病院の情報共有や公表に向けた準備を開始するとともに、インシデント認知後早々にホームページでシステム障害の影響により通常診療ができないことを公表。また 17 時に職員向け説明会を開催し、ランサムウェアによるシステム障害は長期化する見込みであることが説明された。18 時 30 分ごろには報道資料提供を行ったうえで、20 時から記者会見を開催した。

5.3. 医療継続のための対応

病院は患者の命を最優先にし、医療を止めることなく継続することに努めていた。以下に、地域医療連携、救急、外来等の対応についてまとめる。なお、すべての時系列は、巻末に添付の対応時系列を参照されたい。

5.3.1. 患者対応

5.3.1.1. 地域医療連携・救急対応

病院は、10 月 31 日の記者会見後、11 月 2 日の時点で復旧までには長期間要するとの見解を専門家チームから得たことから、当日に地域医師会宛に新規患者受入不可の案内を FAX 送信した。また祝日を挟んだ 11 月 4 日には、近隣の病院 94 か所宛に「通常診療不可・転院受入等協力要請」を FAX 送信し、病院としての支援要請を発信した。システム障害に起因して転医手続きを行った患者数は 669 人いた。限られた情報の中でも患者の受け入れに対応した医療機関の協力もあり、医療継続は上手く機能していたと評価できる。また救急対応については、障害発生後ただちに応需不可のシステム入力を行い、電話連絡で応需要請はあったものの、当面の間は断らざるを得ない状況が続いた。

5.3.1.2. 外来患者対応

病院は、障害初日の来院者に対しては、「サイバー攻撃」や「ランサムウェア」という文言を使わず、「システム障害のため、各科外来受付に直接行ってください」と玄関付近でアナウンスしながら各科外来へ誘導した。各科外来受付では、カルテ参照ができない中で来院者の状況を確認しながら、予約変更の手

続きを取り帰宅させるか、必要な処方や処置などを行うかなど、診療の必要性をトリアージしながら各科の判断で対応が行われた。なお、2 日目以降もシステム障害が継続している状況を説明し、患者の状況を確認しながらトリアージを実施。手書きの予約票を発行しながら必要な医療の継続を行いつつ、患者の要望に応じた他医療機関への紹介が行われた。

5.3.1.3. 入院患者対応

病院は、障害発生直前の 10 月 30 日 24 時時点で入院していた患者数は 532 人であった。またシステム障害発生当日に入院の予約があった患者数は 50 人で、すでに来院していた患者も含めて、入院延期とした患者は 42 人、診療科や病棟と調整のうえで入院となった患者は 8 人であった。

診療科によって患者の状況も異なるため、基本的に患者毎の医療継続方針は、診療科責任者の裁量に委ねられていた。患者を受け持つ 29 の診療科のうち、他の医療機関に支援要請を行った診療科が 19 診療科、支援要請をしなかった診療科が 10 診療科あり、システム障害の影響により転院させた患者数は 36 人であった。

5.3.1.4. 電話による患者対応

障害発生後、電子カルテの参照ができないため、予約状況の確認も患者の連絡先さえも確認ができない状況であった。そのような中で、予定入院の場合は事前に入院準備室で患者から提出されていた「入院申込書」の連絡先を頼りに、また、初診予約の場合は紹介元医療機関から事前に送付されていた「診療依頼書」に記載の連絡先を頼りに、患者への予約の延期等の電話連絡が行われた。

記者会見後の 2 日目以降は、問い合わせの電話が殺到する中、電話回線がパンク状態になり、病院から発信する電話回線も通じない状況が続いたことから、11 月 7 日には発信用の 10 回線が追加された（従来は受発信で 20 回線）。これによりかなり業務が改善された。

5.3.2. 患者・地域住民に向けた情報公開や連携

病院は、インシデント認知後、ただちに機構本部、大阪府、大阪府住吉警察署、大阪市保健所、厚生労働省、内閣サイバーセキュリティセンターなど、関係各方面に連絡を行った。また厚生労働省からは専門家チームが派遣可能である旨の連絡を受け、同日 12 時の対策本部会議において、紙カルテ運用をはじめとした医療方針を継続すること、専門家チームの受け入れを了承することなどを決定した。

病院は、病院幹部会議の方針を受けて、速報でホームページに図 7 の掲載を行い、当日来院された患者への説明に努めた。また、情報は隠すことなく、積極的に情報公開していく方針を掲げ、インシデント発生当日の 20 時に記者会見を開き、現状と今後の診療体制等について説明を行った。

システム障害のため、本日は 診察を停止しております。

ご迷惑をおかけしますが、ご理解いただきますようお願いいたします。

明日以降の診察は、当センターホームページをご確認ください。

図 7　ホームページ速報掲載内容

病院は、電子カルテの情報を参照することができず、患者への連絡手段も限られる中、診療を制限せざるを得ない状況を積極的に医療機関、ステークホルダーに情報が伝わるよう努めた。また、障害発生 1 週間後の翌週 11 月 7 日に二度目の記者会見を開き、調査状況や復旧計画などの説明を行い、継続的にホームページなどで外部発信を行った。

表 9　ホームページ掲載経過

日付	報数	内容
10 月 31 日	速報	システム障害のため、診察停止を案内。
	第 1 報	緊急以外の手術や外来診療の一時停止など通常診療ができない状況。
11 月 1 日	第 2 報	復旧目途が立っていない状況。
11 月 2 日	第 3 報	予定手術は一部再開も、引き続き、外来診療については一時停止の状況。
11 月 4 日	第 4 報	予定手術を 5 件実施も、引き続き、外来診療については一時停止の状況。
11 月 9 日	第 5 報	11/10 から電子カルテの参照可能になる状況。
11 月 6 日	第 6 報	11/10 から三次救急受入再開、11/17 から一般救急患者の受け入れ再開へ。
12 月 12 日	第 7 報	12/12 から電子カルテを含めた基幹システムが再稼働。外来から順次電子カルテ端末を設置し、電子カルテの参照や記事入力、一部のオーダーが可能になる。
12 月 22 日	第 8 報	通常診療の再開へ。 電子カルテ端末の再配置と部門システムの復旧が進み、ほぼすべての診療科において外来の初診患者受付を再開。病棟においても電子カルテ運用を再開し、紙運用を終了。
1 月 10 日	第 9 報	1/11 からの診療体制復旧を宣言（図 8）。

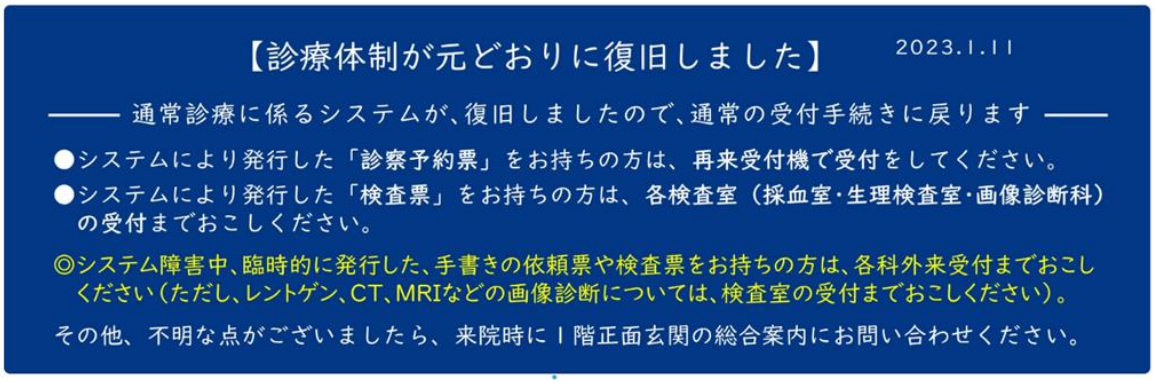


図 8　ホームページでの診療体制復旧案内

5.3.3. 事業継続計画に基づく対応

病院は、BCP に基づく対応を行っていた。BCP 対策本部会議は、主だったシステムが復旧するまで、計 19 回開催された。

表 10　BCP 対策本部会議開催状況

BCP 対策本部会議の開催状況		
回数	開催日	主な決定事項等
1 回目	10 月 31 日	・災害時の紙カルテ運用の実施とともに、直近 1 週間の方針を決定。 ⇒手術は緊急のみ　⇒外来は緊急のみ ⇒救急や時間外はやむを得ない理由がある場合以外は停止 ⇒新規入院は延期　⇒入院中の患者の診療は継続
2 回目	11 月 1 日	・外来開始方針、外来化学療法再開。 ・診療記録文書統合管理システム（DACS）の活用を開始。 （優先順位：①手術、②転院） ・各検査、処方、カルテなどの個人情報の取扱いを確認。
3 回目	11 月 2 日	・11/4 からの予定手術の一部再開を決定。 ・紙カルテ運用における安全な診療継続を確認。 ・図書室を閲覧スペースとして DACS 参照センター（10 台）の設置を決定。
4 回目	11 月 4 日	・病院での情報共有方法を確認。 ・検査、手術など可能件数を確認。
5 回目	11 月 7 日	・対策本部の組織や指示命令系統などを再構成。 ・11/8 から DACS 参照センターの運用を開始。
6 回目	11 月 8 日	・11/10 から三次救急の一部受け入れ再開。
7 回目	11 月 9 日	・11/10 からバックアップデータを利用した参照系端末の運用開始（20 台）。 ・DACS 参照センターの端末の拡充を決定（最大 20 台）。
8 回目	11 月 10 日	・11/14 から内視鏡再開。
9 回目	11 月 11 日	・11/11 から術前麻酔外来を再開。
10 回目	11 月 14 日	・12 月第三週での基幹システム稼働を想定し、端末の順次配置方法を確認。 ・11/17 から救急外来（ER）を再開。
11 回目	11 月 16 日	・11/16 から麻酔科外来カルテ運用開始。 ・11/16 から画像診断検査依頼書運用開始。
12 回目	11 月 18 日	・11/28 から手術枠拡充、2,000 cc以上の要輸血手術の実施不可。 ・11/18 から外注検査再開、11/22 から端末回収、ER へ参照端末追加予定。
13 回目	11 月 22 日	・手術オーダー手順の更新。 ・画像診断機器のウイルスチェックは、MRI と RI を除き完了。
14 回目	11 月 25 日	・11/28 から画像参照センター運用開始、12/9 までの CT,MRI 検査予約受付。 ・手術室に参照系端末 1 台追加、11/28 から食事対応一部変更。

BCP 対策本部会議の開催状況		
回数	開催日	主な決定事項等
15 回目	11 月 30 日	・12/12 から基幹システム再開。 ・端末再配置日程決定。まずは外来周辺から配置し病棟は後に。
16 回目	12 月 7 日	・12/12 からの再開は外来患者から。当面の入院患者利用は不可。 ・参照系は、電子カルテは 12/11 まで、DACS は 12/23 まで。
17 回目	12 月 14 日	・12/15 から従来通りの地域予約を再開、化学療法は 12/22 から制限解除。 ・入院患者の電子カルテ運用開始は 12/22 から。
18 回目	12 月 22 日	・12/28 をもって BCP 対策本部会議は終了。画像参照センターは 12/22 で終了。 ・12/22 から各ホットラインでの救急受入完全復旧。 ・手術オーダーは 1/4 予定手術分より再開。2,000 cc以上輸血手術再開。
19 回目	12 月 28 日	・復旧状況再確認。 ・診療機能復旧を確認し、本会議の終了を宣言。

病院の事業計画マネジメント（BCM）および当該体制や整備状況、今回の事案における活動状況から、病院が以下の状況にあったことが、医療を継続できた大きな要因であると言える。

- ◆ 事業継続対策本部が設置できる体制であったこと。
- ◆ インシデントを認知して短時間で幹部を含めて招集できたこと。
- ◆ 紙カルテ運用に移行できる体制であったこと。
- ◆ 対策本部会議で決定した事項を速やかに職員に周知できる体制であったこと。

システム障害において、医療継続を行ううえでの切り札は、参照系システムの構築であった。構築後は、患者診療情報の参照ができるようになり、その規模が拡大されるに従い、医療提供の範囲が拡充し、予定手術の再開、化学療法の継続、救急受入の再開、患者転院の際の診療情報提供書作成といった医療継続に必要な情報確認や、患者や家族連絡先の確認、予約情報の確認といったことまで、幅広い対応が行えるようになった。大規模システム障害時においても、電子カルテを参照できるようにすることが医療継続の鍵であると言える。

今回、幸いにも別セグメントにあった診療記録文書統合管理システム（DACS）や医用画像管理システム（PACS）がランサムウェア感染を免れていた。そのため、障害発生翌日の 11 月 1 日から DACS を活用し、予定手術の再開や診療情報提供書の作成などの対応ができた。DACS を参照できる端末も当初の 2 台から最大 20 台まで拡張した。また、11 月 10 日には、バックアップデータを活用した電子カルテの参照端末 20 台の運用も開始。電子カルテの参照端末はその後、高度救命救急センターに 1 台、手術室に 1 台増設できたことから、救急受入の拡充や予定手術の増枠などが実施できた。

以上のことから、医療機関には大規模システム障害時の迅速な参照系の構築を念頭に入れた BCP を策

定すべきである。本事案では DACS が運よくランサムウェア感染を免れていただけであり、ネットワークが細分化されていたり、BCP に基づいて参照系が構築されたりしていたわけではない。大規模システム障害時の医療継続を確実にするためには、バックアップデータを用いた参照系システムの早期または事前の構築を行うべきであり、そのためにはバックアップを確実に取得しておくことが重要である。特に、サイバー攻撃による大規模システム障害を考慮すれば、攻撃を直接受けることのないオフラインのバックアップを取得しておくことこそが、医療継続の最大の切り札と言える。

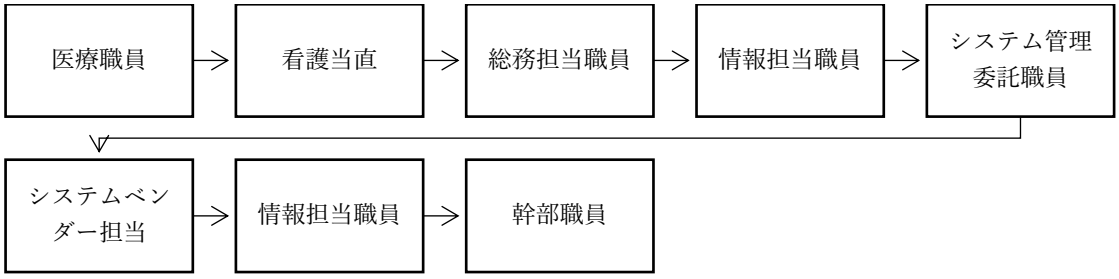
5.4. インシデントの認知から初動対応

ここからはシステムおよびシステムが被害を受けたサイバー攻撃に焦点を当て、まずは初動対応までを整理する。

5.4.1. インシデントの認知

病院がインシデントと判断し、ネットワーク遮断をしたのは、A 社などのシステムベンダーの到着と調査後の午前 8 時 30 分から 40 分までのことである。しかし、遮断する約 3 時間前には、病院に配置している給食関連の委託職員が、電子カルテシステムが動かないことを確認していた。その後、看護当直も電子カルテシステムで障害が発生していることを確認したが、重症部門システムなど動作しているシステムもあったため、この時点ではランサムウェアの感染を疑うことは難しかった。

ポイントになるのは、システム管理委託職員がランサムノートと暗号化の事実を確認した午前 7 時 45 分である。ランサムウェアに対する知識があれば、このタイミングでネットワーク遮断を判断できた可能性はある。



E 社は、病院配置の E 社職員に対し、午前 8 時にパソコンの電源を落とすように指示を行い、午前 8 時 15 分にマルウェア感染の可能性を伝えた。病院配置の E 社職員が、病院にその状況を報告したのは午前 8 時 20 分である。一方、ファイアウォール Y では、午前 3 時 45 分に E 社からの大量の RDP 通信のセッションを、午前 4 時 8 分以降には RDP 通信を用いた操作を検知している。このタイミングでファイアウォール Y のログやアラートが確認されていれば、ランサムウェアの可能性は疑えずとも不正アクセスを疑うことはできた。

病院としては、エスカレーションフローが不明瞭であったこと、ベンダーの調査や判断を待ったこと、ログ運用を適切にできていなかったことなどから、検知とトリアージ（判断）が連動していなかった。

5.4.2. 初動対応 I （1 日目：報告と関連事業者打ち合わせ）

ネットワーク遮断を行った後、先に述べた通り、電子カルテから紙カルテに運用するための準備を進め

るとともに、関係各所に通報や連絡を行った。連絡を行ったのは以下の機関である。

大阪府立病院機構本部／大阪府健康医療部／大阪府住吉警察署／内閣サイバーセキュリティセンター（NISC）／厚生労働省医政局／大阪市保健所

厚生労働省医政局に報告を行った際に、初動対応支援の専門家チーム派遣の提案があり、12 時（正午）からの第 1 回目 BCP 対策本部会議で受け入れが決定された。電子カルテシステムベンダーはインターネット接続を含むすべてのネットワーク遮断後、感染確認や原因、復旧のための手順確認など、作業を行っていたものと思われる。なお、ベンダーやシステム関係者を集めた会議は 16 時から開催され、専門家チームも会議に（オンラインで）加わった。専門家チーム主導で整理した内容は以下のとおりであった。

＜発生状況＞

- 2022/10/31 午前 4 時 7 分から 4 時 10 分頃に、E 社のサーバーA から病院ネットワークのサーバーB へ、大量の RDP 通信（ポート番号：3389）接続が発生。
- サーバーB に接続されている電子カルテシステムを管理する診療系サーバーに保存されているファイルが暗号化され、英文のランサムノート（身代金要求文書）が置かれていた。
- 本事案が二次被害で、発端は E 社のシステムの可能性がある。
- 物理サーバー単位で 20 台。仮想サーバー単位では 100 台以上が存在。
- 対象サーバーは診療系サーバーやウイルス対策サーバーなど。
- ファイアウォールとルーター間のネットワークを遮断し、さらにサーバーB 以下のサーバーはすべて隔離済み。
- ランサムウェアで暗号化されたファイルの拡張子は「.elbie」。

＜システム・ネットワーク関連情報＞

- サーバーB には NIC が 2 つあり、1 つはファイアウォール側、もう 1 つは病院情報システムセグメントに接続。
- 診療系ネットワーク配下から病院ネットワークはファイアウォールを経由しないため、通信有無の確認は不可能。一部医療機器も外部への接続があるが、被害は確認されていない。
- 閉域網とサーバーB の間にはファイアウォール Y を設置しており、TCP:1433、TCP/UDP:445、TCP:139、TCP/UDP:3389 の通信を許可していた。
- 被害サーバーはすべて Active Directory に参加。ドメインサーバーのイベントログに「4625（ログオン失敗）」のイベントが大量に発生しており、その後に成功が記録されていることも確認した。

〈パスワード関連情報〉

- パスワードポリシーは推測困難なもので、大文字小文字英数字の 12 桁で設定する運用ルール。
- 被災した各サーバーのパスワードは共通。
- 端末のローカル管理者アカウントのログオンパスワードは、すべて共通で運用。

上記から、E 社とそのシステムベンダーとの打ち合わせが必要不可欠と判断し、並行して打ち合わせを設定し、19 時から会議を行うことが決定した。

19 時から E 社およびシステム関連の C 社や D 社が参加し、病院と打ち合わせを行った。そこで、確認されたことは次の通りであった。

＜確認内容＞

- E 社の給食センター（仮想サーバーと NAS 内データ）もランサムウェアに感染し、暗号化が行われている。
- E 社 LAN は病院のサーバーと接続しており、この LAN は他の病院システムも繋がっている。しかし、他のシステム接続のある病院の被害の報告は入っていない。
- リモートアクセスについて
  - ファイアウォールＺ（SSL-VPN）を使用。
  - バージョンは 7.2.2 で、18 時以前は 6.0.11（後日確認したところ実際は 5.4.2 であった）。[7]
  - ログは syslog も含めて残っていない。
- 暗号化されたファイルの拡張子は「.elbie」。

上記の通り、①同様のランサムウェアに感染している可能性が高いこと、②ファイアウォールＺの脆弱性が存在していたこと、③ファイアウォールＺの攻撃者が活用するリストに ID とパスワードが漏洩していたことから、発生当日に経路と原因の推定はできていた。しかし、半田病院の事案同様に、ログが取得されておらず、ファームウェアが更新されてしまったため、侵入経路の断定を行うことができないことも判明していた。

大阪府警察本部から、復旧の進捗状況を踏まえた証拠保全をするために、会議に参加したい旨の依頼があったことから、本打ち合わせ結果とともに、専門家チームとも対応を検討し、翌日の会議から大阪府警察本部が参加することも決定した。

5.4.3. 初動対応 II（2 日目：調査および復旧に向けた準備）

インシデント発生当日に A 社などが現地に駆け付け、ネットワーク遮断などを行いインシデント対応が開始されたが、システムを利用する病院とシステムを運用するベンダーの双方がインシデント対応の司令塔になることができていなかった。午前 10 時から開催したシステム関係者の会議では、病院職員、大阪府警察本部、電子カルテシステムベンダー、ネットワークシステムベンダー、専門家チームを含め、40 名程度が参集し、専門家チームを中心に状況の整理を行っていった。当該会議で確認・整理していた内容を一部記述する。

---

[7] ファームウェアの更新は C 社によって 18 時頃に行われ、E 社はファイアウォールを利用している認識がなかった。本委員会のヒアリングによって、ファイアウォールＺはリモートからアクセスされた場合にはアップデートを促すメッセージを表示しないため、長期間にわたってファームウェアアップデートがされずに運用されていたところ、同日トラブル対応のために現地に駆け付けた C 社スタッフが、管理コンソールからアクセスした際に表示されたアップデートを促すメッセージにしたがって通常業務時の基本手順通り、作業開始前にアップデートを実施した。

＜各々の対応確認＞

- 電子カルテシステムベンダー
  - ✧ バックアップの確認、システムやネットワーク、感染状況情報などの情報提供
- 大阪府警察本部
  - ✧ 行為者特定のための解析及び解析結果の情報共有
- 病院
  - ✧ 状況の情報収集、対応方針や復旧システム優先順位付け、復旧に向けた情報整理
- 専門家チーム
  - ✧ 各種ログやシステムやネットワーク構成等の確認

＜対応の優先順位＞

また、医療情報部長を中心に対応の優先順位の検討と決定を行った。

1. オフラインバックアップが活用できる前提で患者の基本情報を見られる新たな電子カルテ環境を構築。
2. 画像系システムの安全性確認と機器自体での工夫を行い、画像を確認できる環境にする。
3. 重症系システムのバックアップや旧サーバーの利用可否などを確認。DACS をサーバー室の直下の図書室にネットワークを引き延ばし、構築し、参照できるようにする。

まず、バックアップデータがどの程度活用できるのか、急ぎ確認を行った。

確認の結果、重症系システムのバックアップはオンラインのみであったため活用できなかったが、電子カルテやオーダーリング、医事会計などは、バックアップの途中でランサムウェア攻撃に遭い、バックアップが完了せず一部保存できていないデータがあったものの、バックアップデータについてはほぼ問題なく利用できることを確認し、参照環境の構築を加速した。なお、バックアップデータの日時がすべて揃えられるのは 2022 年 10 月 27 日までということが判明し、10 月 27 日の状況に戻すことにしていた。10 月 28 日から 10 月 30 日までの完全なデータは損なわれるが、幸いにして期間のうち 2 日は土日であったため、失われたデータは通常の 3 日分よりも少ないものであった。

上記の通り、情報の把握と集約に努め、報告・共有方法の整理などを行った。システム復旧の方法については、予定されていたシステムの更新を前倒しして実施し、構築する案と、既存システムを復旧する案の二案を検討した。

5.4.4. 初動対応Ⅲ（3 日目以降：復旧方針の決定と関連組織との連携）

インシデント発生後 3 日目には、総長や病院長が参加する幹部打ち合わせ会議に専門家チームが参加し、安全に一日も早く復旧させることを確認した。前述したシステムの前倒し更新案は、要件が定まっていないことや、サーバーや端末の調達に時間を要することなどから断念し、部分的な端末調達は行うものの、基本的には既存システムを迅速に復旧させるという結論に至った。

しかし、既存システムがどこまで攻撃者による侵害を受けているのか、範囲や深度は計り知れなかった。いくつかの被疑クライアント（端末）の侵害確認を行ったところ、侵害された可能性は低そうではあ

ったが、その一方で、Active Directory サーバーのログからログオンの失敗や成功を繰り返している端末が 1,000 台程度あり、この数台の確認で「潜在的な脅威がない」と証明することはできなかった。厳密にフォレンジック結果を待てば 3 ～ 4 週間は現場が止まることになる。

さらに、今回の侵入経路において、ファイアウォール Y のログから RDP 通信は遡れば 2022 年 4 月まで確認ができ、またログオンの失敗などのログも 10 月 31 日以前から確認することができ、以前から E 社経由でサイバー攻撃を受けていた可能性も否定できなかった。なお、後の C 社 D 社 E 社とのリモート会議（2022 年 11 月 24 日開催）で判明したことだが、C 社の要請により開放した RDP 通信は、実際には不要で利用されていなかった。また、ファイアウォール Y には他に疑わしいログはないものの、他にも把握し切れていない外部接続箇所が複数ある可能性が明らかになった。

侵害されたサーバーB と同一セグメント上に、電子カルテを含めた総合情報システムのサーバーや端末があるため、横展開は簡単に行える環境にあった。サーバーおよび端末のパスワードもそれぞれ基本的に共通であり、かつアカウントロックの設定も施されていなかった。さらに、電子カルテシステム、部門システム、医療機器など、確認したほとんどのシステムや機器で、最新のバージョンの OS は利用されておらず、パッチも適用されていなかった。また、既にサポートが切れた OS の利用なども確認された。以上から、すべてのサーバーや端末の初期化を行う方針を固めた。

前述の通り、サポートが切れている OS を利用している機器やウイルス対策ソフトが導入できない端末や機器が確認された。ウイルス対策ソフトを端末や機器に導入できないのであれば、ネットワークで守る方策を考える必要があり、内在する脅威の検出やサポート切れの OS 対応のために、通信経路はできる限り集約し、ネットワークの振る舞い検知を行う機器の設置を急いだ。当該機器の手配を各セキュリティベンダーに打診したところ、検証機を 2 社から即座に提供してもらった。11 月 4 日から当該機器を設置し、コアスイッチを通る通信は監視できる環境を構築し、さらに USB タイプのウイルススキャンツールについてもセキュリティベンダーから賃借と早期調達を行い、インシデントの早期解決に向けた対応を行った。

大阪府警察本部からは、侵入方法等に関する積極的な情報共有を受け、継続して専門家チームとの連携を行っていた。11 月 3 日には踏み台となっていたサーバーB を専門家チームとともに調査し、検体や各種攻撃ツールを確認している。当該調査の結果、侵入に関する記録等から、E 社経由での感染とほぼ断定することができた。

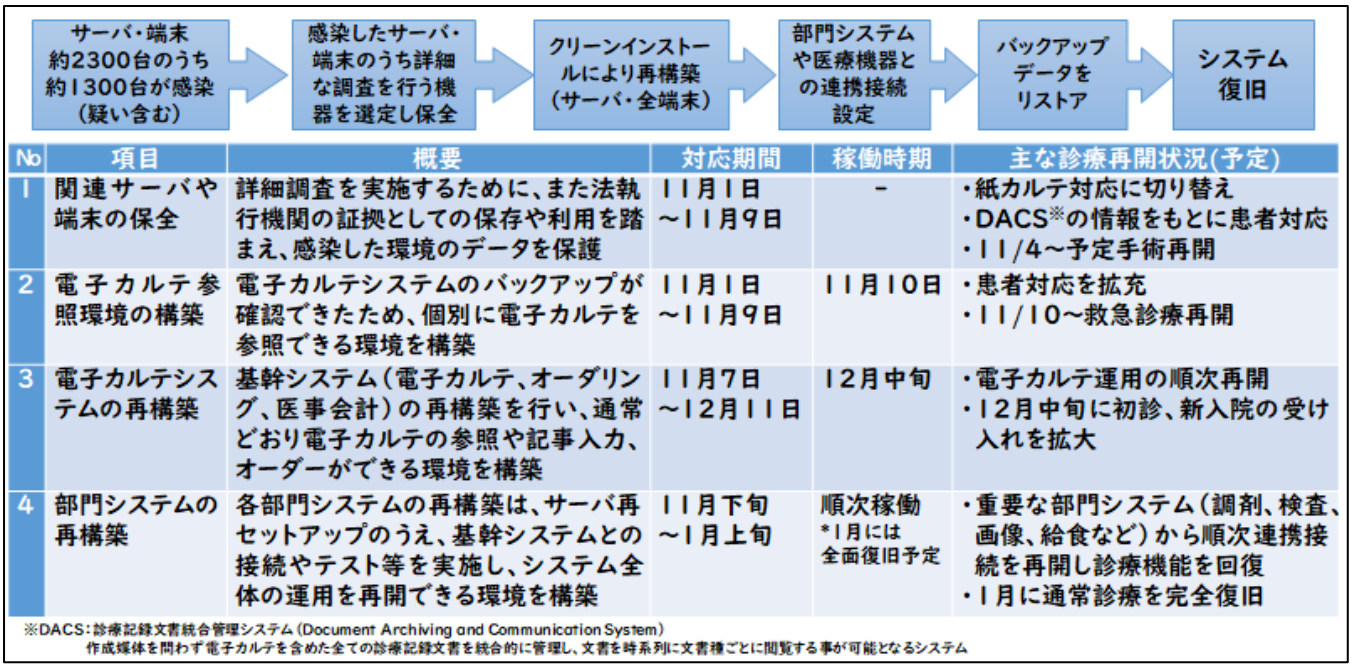
11 月 4 日には A 社の責任者が東京から来院し、復旧目途と今後のスケジュールについて説明を受け合意した。この時点で 12 月中旬に基幹システムを、1 月上旬には全システムを戻すことを確認した。

また、同日 E 社役員などが来院し、E 社のプレスリリースの内容相談や給食提供にリソースが割かれ、システムやサイバー攻撃への対応が進んでいない旨の説明があった。説明の中で、E 社が契約している L 病院でも E 社が持ち込んでいる機器の感染が確認されていることを認知したことから、当該会議の中で、大阪府警察本部へ電話連絡を行い、情報提供をするとともに対応を依頼した。

さらに、同日、大阪府知事や健康医療部部長などと打ち合わせも行った。病院と専門家チームから現状を報告し、知事からは府として必要な支援を行う旨の話があった。

5.5.　システム復旧

前述の通りシステムや機器の「正常性」を証明できないことから、原則初期化を行う方針を決定し、基幹システムのオフラインバックアップ（遠隔地テープ保存）から、電子カルテを参照できる環境を先に構築していくなど、以下のような方針で復旧を進めた。復旧に向けた流れは次の図の通りである。



No	項目	概要	対応期間	稼働時期	主な診療再開状況(予定)
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日 ～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日 ～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム（電子カルテ、オーダリング、医事会計）の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日 ～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬 ～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム（調剤、検査、画像、給食など）から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

※DACS：診療記録文書統合管理システム（Document Archiving and Communication System）
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

図 9　システム復旧方針

なお、復旧方針は、病院医療情報部情報企画室、A 社病院情報システム担当部門、A 社セキュリティ担当部門、B 社で合議のうえ決定し、保全を確実にするため、大阪府警察本部との調整を行いながら、復旧体制を整えた。

復旧にあたっては、医療の質の維持のため、電子カルテの参照システムの構築、画像診断系システムの復旧を優先し、その後、電子カルテシステムの復旧、各部門・診療科システムの復旧を実施した。また、画像診断システム、各部門・診療科システムには、一部、ウイルス対策ソフトが未稼働であったり、サポート切れの古い OS が使われていたりしたことから、画像診断システムベンダー、各部門・診療科システムベンダーへの聞き取りを行い、ネットワーク構成や HIS 系ネットワークとのルーティングを厳格化し、新たなポリシーの遵守を求めた。

5.5.1.　バックアップの確認と参照システムの構築

本事案では、病院に設置された LTO[8]バックアップ装置が暗号化の被害を受けたため、遠隔地保管の LTO バックアップからの復旧が可能かの判断が即座には困難であった。このため、A 社にて暗号化されたバックアップサーバーを初期化・再設定のうえ、スタンドアロンで LTO バックアップ装置が利用でき

[8] リニアテープオープン(Linear Tape-Open)。コンピューターのデータバックアップ、アーカイブに使用する磁気テープ技術の標準規格。カセットテープカートリッジを使用し、10TB を超える大容量のデータ保管に向いている。

る環境を準備し、遠隔地保管されたLTOテープを確認した。バックアップデータは正常に読み出し可能なことが確認され、このデータを新規で調達した参照サーバーにリストア（データを戻）し、アプリケーションを入れた端末から閲覧することで、電子カルテのバックアップデータを参照できる環境を構築した。参照専用の電子カルテシステムの構築によって、11月10日から20台の参照端末で10月27日以前の患者データの確認が行えるようになった。

5.5.2. 端末復旧

端末は全体で約2,200台あり、1台1台の安全性を確認することは復旧スケジュールからみて不可能であった。一方、これまで述べた通り、端末からのAdministratorでのログオン失敗などのログが確認されたこと、事象発生当時、ウイルス対策ソフトが未稼働の端末が一定数あったこと、市販の正規のVPNソフトを設置する攻撃者も存在することなど、ウイルス対策ソフトでの完全スキャンだけでは端末の真正性を証明することは困難と判断し、確実な再発防止を担保するため、端末全台を初期化し復旧することとした。初期化前の端末内のデータは、再感染の恐れがあると判断し原則使用不可とした。

端末の全数初期化は復旧に大きな影響を及ぼすため、1日200台の初期化と再設置の計画を、A社中心に立案・実施した。再配置を確実に実施するため、ロジスティック（回収から設定、配置などの対応を行う）事業者が端末を回収する際に設置の場所、向きやケーブル類などの情報を記入した用紙を端末設置場所に置いた。回収された端末はA社によってOS初期化、必要なアプリケーションのクリーンインストールが実施され、ロジスティック業者によって再設置された。全端末初期化は11月22日から開始され計画通り12月22日までに完了している。

5.5.3. 各部門・診療科システム復旧

各部門・診療科には診療科システムサーバーが設置され、HIS系ネットワークを経由して電子カルテなどから診療科システムサーバー上のデータが参照される。一方で、診療科システムサーバーには、NICが2枚挿されており、HIS系ネットワークと診療科内LANを特定の制限なしにルーティングしているケースが大半であった。各部門・診療科システムの復旧に当たっては、ルーターを設置したうえで、厳格なルーティングの適用とウイルス対策ソフトの稼働を求めた。

一方で、診療科内LANには、古いOSの端末が接続されて稼働[9]しており、かつ、予算的に早期のリプレース（更改や変更）が困難なものがあったため、診療科内LANとHIS系ネットワークの接続を禁止するか、コアスイッチのミラーポートで通信を継続的に監視することで、暫定的に稼働を認めることとした。また、これらの古いOSを有するシステムでスタンドアロンでの稼働を許したものは、原則USBポートを物理的にロックして、USBメモリなどの利用を不可能とする措置を講じた。

今回、サーバーBに設置されたツール類は、一部のウイルス対策ソフトを除き、検出・検疫が可能であったことから、復旧にあたっては病院とA社にて、以下の「サーバー・端末再構築方針」を策定し遵守を求め、対応した。

---

[9] 2013年頃にセンターに、新規で導入された複数の医療機器の制御端末のOSがWindows 2000であった。

表 11　サーバー・端末再構築方針

対象	対応内容
仮想サーバー （Windows）	• OS、アプリケーションは新規構築。 • ファイルが暗号化されていなければ、複数のウイルス対策ソフトで、フルスキャン後に、検出が無ければ再利用可(実行可能形式ファイルを除く)。
物理サーバー (Windows)	• OS、アプリケーションは新規構築。 • ファイルを格納した USB を接続して暗号化されれば感染と判断。 • 感染していなければ、局所的な NW を作成してファイルを取り出し、複数のウイルス対策ソフトで、フルスキャン後に、検出が無ければ再利用可(実行可能形式ファイルを除く)。
サーバー (Linux)	• OS、アプリケーションは新規構築もしくは再利用。 • 再利用の場合は、想定外/仕様外のプロセスが起動していないか確認。 • 複数のウイルス対策ソフトで、フルスキャン後に検出がなければ、再利用可。
端末	全端末クリーンインストール。

【復旧時に再利用を禁止するファイル一覧】

.ade .adp .app .application .appref-ms .asp .aspx .asx .bgi .cab .cer .chm .cmd .cnt .com .cpl .der .diagcab.exe .fxp .gadget .grp .hlp .hpj .hta .htc .iso .jar .jnlp .mad .maf .mag .mam .maq .mar .mas .mat .mau .mav .maw .mcf .mda .mdb .mde .mdt .mdw .mdz .msc .msi .msp .msu .pcd .prf .prg .printerexport .pst .reg .scf .scr .sct .shb .shs .theme .tmp .vbe .vbp .vhd .vhdx .vsmacros .vsw .webpnp .website .xbap .xll .xnk、各種ライブラリファイル（.dll/.lib)、サービスや web コンテンツ

【ID、パスワード関連復旧方針】

- 原則、Administrator、root などの組み込みの ID の使用禁止
- ID の共用を禁止し、個別ユニークな ID を付与する
- 禁止パスワード：P@ssw0rd、1qaz2wsx、admin、1q2w3e4r 等の安直なパスワードの禁止
- 共通パスワードの使用禁止
- サーバー、端末の Built-In Administrator のパスワードをすべて個別に設定
- 強力なパスワードの設定
  - ➢ 16 桁以上のパスフレーズを推奨
  - ➢ 複雑性は求めないが、連続したキーボード配列、単純な繰り返しは禁止する
  - ➢ 定期的にパスワードが漏洩しているかチェックを実施する
    （例）https://haveibeenpwned.com/Passwords/

【その他（Windows の基本設定等）復旧方針】

- 感染防止のため標準ユーザーで作業を実施
  管理者権限が必要な場合は、UAC の設定で、特権昇格の際は資格情報を要求する設定をする
- Windows パーソナルファイアウォールの設定（すべてのプロファイル）
  RDP 3389/TCP/UDP 受信拒否。Win-RM 80/TCP、5985/TCP 受信拒否
- Remote Registry （Windows サービス）の停止

- PowerShell の停止と PowerShell v2 の削除、および PowerShell のログ設定
- IP Block List の設定

＜初期復旧システム＞

すべてのシステムを同時期に再稼働させることは物理的、論理的に困難であり、A 社が中心となって各部門・診療科システムベンダーの調整を行い、11 月 14 日に復旧計画を策定し、外来受付を可能とする電子カルテ再稼働日を 12 月 12 日とした。同日、再稼働させた主要なシステムは以下の通り。

電子カルテシステム、オーダーリングシステム、医事会計システム、看護支援システム、
調剤システム、検体検査システム、採血システム、再来受付システム、患者案内システム、
服薬指導システムなど。

＜初期以降の復旧システム＞

- 12 月 14 日　PACS、放射線部門システム、放射線治療システムなど。
- 12 月 20 日　生理検査システム、輸血システム、非 DICOM 画像情報システム、DACS、歯科システムなど。
- 12 月 22 日　給食システム、栄養指導システム、手術部門システム、重症患者情報システムなど。
- 12 月 27 日　微生物システム、病理システム、内視鏡システム、心電図システム、脳波システム、診断書作成システム、DPC 情報など。
- 1 月 11 日　周産期システム、リハビリシステム、透析システム、DWH、麻酔管理システムなど。

上記の通り、段階的にシステムを再構築し、端末も配備し、2023 年 1 月 11 日に通常診療可能なシステムを復旧した。

5.6. 初動対応における調査

5.6.1. 初動調査概要

多くのランサムウェア事案では、放置された脆弱性や脆弱な設定・設計が悪用されることから、復旧時には、同様の脆弱性を再現することなく、強靭化を図る必要がある。そのため、初動調査は、フォレンジック調査の対象の決定、復旧方針や復旧時の詳細な設定などの決定を行うことを目的に実施した。また、過去の事例で、継続的な攻撃のための VPN 機器以外の攻撃経路の設置（VPN ソフトウェア等のインストール）などがあったことから、初動セキュリティ調査では、以下の点に留意し実施した。

1. 侵入経路の特定
   侵入端緒の特定と、病院ネットワークのルーティング、アクセス権の把握。
2. 被害範囲の特定
   暗号化、破壊の範囲及び VPN、バックドアの設置の状況の把握。
3. 今回の攻撃の特徴及び攻撃を可能とした要因の特定
   病院のセキュリティポリシーや OS の設定値、アプリケーションシステムの動作のための特有の設定値の把握。

一方で、事案発生当初は、侵入経路となった E 社も攻撃され、機器が暗号化された状況にあったことから情報が少なく、加えて病院システムの規模が大きく、多数の部門・診療科システムで保守目的の VPN 接続が存在し、それぞれの調査に時間を要したことから、侵入経路の確定や、それに応じた対策の策定に至ったのは、事案発生から 1 週間後の 2022 年 11 月 7 日であった。また、他の多くの事案と同様に、Windows の設定が既定値のままであったため、ログが上書きされており、少ない情報で被害範囲を推定せざるを得なかった[10]。他方、大阪府警察本部生活安全部サイバー犯罪捜査課からは、復旧に向けた示唆をいただいた。

事案発生直後、稼働していたのは、Active Directory Domain Controller とサーバーB など、物理サーバーで運用されていたものだけであり、仮想基盤上で稼働していたサーバーは仮想基盤への暗号化によって全滅状態にあった。そのため、調査は Active Directory のログ及び部門システムである給食システムを中心に行った。

また、端末は約 2,200 台あり、全数調査は困難であった。さらに、端末の多要素認証システム（IC カード＋PIN コード）も仮想基盤上で稼働していたため認証システムが停止し、ログオンが不可能な状態にあった。そのため、初動での一定台数の端末の調査を諦めざるを得なかった。これは、端末からみた事案の分析という視点が欠けることから、復旧に向けた方針策定に大きな影響を及ぼすこととなった。

5.6.2. 初動調査項目について

5.6.2.1. 外部接続ルートの調査

病院に接続する VPN 機器と、それらの脆弱性の存在や、通信経路の特定と病院 LAN へのルーティング情報、Syslog 等の通信ログを調査した。

5.6.2.2. Active Directory Domain Controller の調査

病院には、Active Directory の認証を司る Domain Controller が物理サーバーとして 2 台、仮想基盤上の仮想サーバーとして 1 台設置されていた。この内、仮想サーバーは仮想基盤が暗号化されたことによって稼働していなかったため、物理サーバーの FSMO[11]を調査した。なお、Domain Controller の構築を行ったのは A 社である。

調査範囲は、Windows ログ（Security、System、Application、リモートデスクトップ関連、SMB 関連、PowerShell 関連、Task Scheduler 他）、グループポリシー、パーソナルファイアウォール、Systeminfo、Autorun 他である。

---

[10] 本来、別項で言及すべきことではあるが、サプライチェーンを経由したインシデント発生においては、初動で相手方の状況を取得できるか、もしくは立ち入り調査ができるかによって、復旧対策は大きく影響を受ける。オンラインでのサプライチェーンが存在する場合は、相互に監査権を付与する、情報提供に協力するなどの、相互扶助を目的とした前向きな契約関係が必要であると考える。

[11] Flexible Single Master Operation（FSMO）。Active Directory では、Domain Controller が複数台ある場合、各 Domain Controller がユーザー情報の変更などを受信した場合、一旦、FSMO に情報を集約し、その後、FSMO から各 Domain Controller に情報を再配付する仕組みを有している。このため、FSMO は最新の情報を所有していることになる。

5.6.2.3. 給食サーバーの調査

サーバーB は侵入の端緒となったサーバーである。物理サーバーであり、基本設定は A 社が行い、給食システムの構築は C 社が実施した。

調査範囲は、Windows ログ（Security、System、Application、リモートデスクトップ関連、SMB 関連、PowerShell 関連、Task Scheduler 他）、グループポリシー、パーソナルファイアウォール、Systeminfo、Autorun 他である。専門家チームと大阪府警察本部が連携し、サーバーB のデスクトップには、X によってフォルダーX[12]が作成されており、そこに攻撃ツールが格納されていたことを確認した。なお、サーバーB は、NIC が 2 枚挿されており、1 枚目は病院 LAN のサーバーセグメントに、2 枚目はファイアウォール接続のためのセグメントに所属していた。

5.6.2.4. 病院設置のファイアウォール（ファイアウォール Y）

E 社の閉域網を通じてサーバーB への接続を許可していたファイアウォールの構築したのは B 社である。E 社からのサーバーB への通信はこのファイアウォールの Syslog によって確認された。

5.6.2.5. 病院の部門・診療科システムベンダーが設置したファイアウォール（VPN 機器）の調査

医療機器や医療情報システムの保守を行うための、複数のファイアウォール（VPN 機器）が設置されていた。システムベンダーにこれらの Syslog の調査を依頼し、保守目的以外の外部接続の有無を確認した。特に異常な通信の発生はなかったことが確認された。

5.6.3. 初動調査の判明事項サマリー

ここでは初動対応時において調査した内容をまとめる。なお、記述することによって病院に安全上の問題が生じる可能性のある情報は削除している。

1. E 社の VPN 機器には、CVE-2018-13379（CVSS v3:9.8、緊急）という脆弱性が存在し、管理者の ID、パスワードを保存したファイルを窃取できた。
2. 同脆弱性を悪用して収集された、世界中の脆弱な VPN 機器のグローバル IP アドレス、ID、パスワードが公開されていた。E 社の VPN 機器のグローバル IP アドレス、ID、パスワードが、同リストに掲載されていた。このことから、公開されたリストにある ID、パスワードを使用して侵入されたと考えるのが合理的である。
3. X は、E 社のネットワークに侵入後、社内 LAN 上の端末に対して、辞書攻撃ツールを使い RDP でログオンした。E 社の端末の Built-In Administrator のパスワードが共通であり、推測可能な弱いパスワードが使用されており、かつ、そのパスワードが攻撃ツールのパスワードリストに存在していた。
4. サーバーA は病院に設置されたサーバーB の Built-In Administrator の ID、パスワードを使用して、サーバーB の共有フォルダーに対して、業務で使用するファイルを日々、送受信していた。このサーバーB の Built-In Administrator のパスワードが、パスワード解析ツール（Mimikatz）で解析された。

[12] C:¥Users¥Administrator¥Desktop¥X

5. 病院のサーバーB と E 社のネットワークは閉域網で接続されており、この間で、C 社の要望によって、RDP が常時接続許可されていた。
6. X は E 社の端末からサーバーB に RDP でログオンし、ツールをデスクトップに設置後、病院の LAN に接続されたサーバー群をスキャンし、攻撃した。
7. 攻撃の際、病院のサーバーの Built-In Administrator のパスワードが共通であったため、横展開（水平展開）が容易となり、被害が拡大したと考える。
8. E 社とのデータ送受信については、RDP 接続は多数のセッションが確認されたもの、データサイズが大きいものは、約 1.8MBytes の通信の 1 度のみで、RDP を経由した E 社からサーバーB へのファイルのコピーではないかと推測される。また、SMB 接続では、サーバーB から E 社に向けて 7.9 MBytes の通信があったが、どのようなデータが送信されたかはログの詳細設定がなされていなかったため不明である。なお、それ以外は 10Kbytes 以下の通信であった。なお、サーバーB のデータベースは 50Mbyte を超すことからデータベースの窃取はなかったと考えられる。

なお、C 社が 10 月 31 日の夕方にファイアウォール Z のファームウェアを、バックアップを取らずにバージョンアップしたため VPN 機器の Syslog が消失した。そのため、10 月 31 日の攻撃が単独で行われたか否かを断定することはできなかった。また、端末の多要素認証システムが攻撃を受け、端末の調査が行えなかったため、端末へのバックドアの設置の有無やウイルス感染等の影響を特定することはできなかった。

5.7. 継続調査

5.7.1. フォレンジック調査の範囲

サーバー・端末のうち、感染の疑いのある約 1,300 台すべてを調査することはできないため、AD サーバーのログ、X が残していったスキャンに成功した端末などを中心に、病院及び A 社との協議により、以下のサーバーを A 社にてフォレンジック調査することとした。

- ✓ 給食サーバー(サーバーB)
- ✓ 基幹サーバー1-3 号機
- ✓ 運用管理サーバー
- ✓ テスト系仮想ホストサーバー
- ✓ 仮想統合ホスト 1-2 号機（Oracle）
- ✓ 仮想統合ホスト 1-2 号機（その他）
- ✓ 別館 NAS サーバー1-2 号機
- ✓ ドメインコントローラー（1 号機（FSMO)、2 号機）
- ✓ クライアント端末 2 台

5.7.2. フォレンジック調査

サーバーB に関しては、迅速な解析とセカンドオピニオンを求めるべく、他のフォレンジック調査会社に調査を依頼した。いずれも、保全を行う際の業界標準ツールである FTK イメージを使用して作成し、各社は FTK イメージをもとに解析を行っている。

フォレンジック調査によると、サーバー関連はドメインコントローラーを除いて（RDP 接続試行は確

認)、Elbie ランサムウェアの感染が確認された。端末については当該ランサムウェアや他のマルウェアは確認されなかったとしている。しかしながら、他ホストへの SMB 接続試行や攻撃者が攻撃によく用いられる PsExec[13]が確認された端末もあり、この結果をもって「正常」であったと判断し難いものであった。

表 12　フォレンジック調査結果一覧

対象サーバー・端末	攻撃ツールの有無	X によるスキャン成功	RDP 接続成功	不審な操作	他ホストへの不審な接続	ランサムウェア感染
給食サーバー（サーバーB）	※1	○	○	○	○	※2
基幹サーバー1-3 号機	-	○	○	-	-	○
運用管理サーバー	-	○	○	-	○	○
テスト系仮想ホストサーバー	-	○	○	○	-	○
仮想統合ホスト 1-2 号機（Oracle）	-	○	○	○（1 号機）	-	○
仮想統合ホスト 1-2 号機（その他）	-	○	○	-	○（2 号機）	○
別館 NAS サーバー1-2 号機	-	○	○	-	-	○
ドメインコントローラー（1 号機（FSMO)、2 号機）	-	○	○	-	-	-
クライアント端末①	※3	○	-	-	○	-
クライアント端末②	-	-	-	-	○	-

（※1：Mimikatz などの攻撃ツール、※2：検体はサーバー上にあり、※3：PsExec）

初動調査や当該フォレンジック調査の結果をみると、X は攻撃ツールの実行により到達可能な 240 程度の IP アドレスなどの情報を窃取し、また、サーバーB からも約 70 程度の IP アドレスに RDP 接続を試行している。フォレンジック調査対象のサーバーでは 11 個ランサムウェアを確認しており、仮想統合サーバー上のサーバーの感染状況と、NAS サーバーなどの感染状況を見ると、同一のネットワークセグメントにあったサーバーはランサムウェアに感染させるための、または攻撃の踏み台にするための X による調査などが行われたと考えられる。

クライアントについては、確認されたツールや他ホストへの接続などを鑑みると、ランサムウェアの感染はしていなかったものの、X の何かしらの攻撃アプローチが行われていた可能性は否定できない。平時のログが取得されていなかったことから、比較調査は行えなかった。

5.7.3.　他医療機関の調査

なぜシステム障害が発生したのが病院だけで、他の医療機関は無事であったかが疑問に残る点であった。E 社と接続していた医療機関でヒアリングを行った結果、以下の相違点が確認された。

[13] 遠隔から Windows 環境の操作を行うことができるマイクロソフトが公開しているツール

表 13　他医療機関との差異状況

	給食システム契約先	給食サーバーパスワード	給食サーバーセグメント
病院	A 社	電子カルテ群と共通	電子カルテ群と共通
L 病院	C 社	電子カルテ群と別	電子カルテ群と別
M 病院	E 社	電子カルテ群と別	電子カルテ群と別

L 病院の給食サーバーは、不正アクセスが試行された形跡はあったものの、侵入はされてはいなかった。L 病院では、給食サーバーのパスワードを C 社指定のパスワードから一文字変更していたので、侵入自体を免れていた可能性がある。仮に給食サーバーへの侵入を許していたとしても、そこから先の電子カルテサーバー群のパスワードもセグメントも別であったので、電子カルテサーバー群へ侵入するハードルは高かったものと思われる。

M 病院では、給食サーバーへの侵入は許したものの、その先の電子カルテサーバー群とはパスワードやセグメントが異なり、またゲートウェイ端末を設置したりするなど、二次侵入を防ぐ対策が施されていた。

一方、病院は、サーバーB への侵入を許した時点で、電子カルテサーバー群とのパスワードが共通であり、セグメントも同一であったため、X によりサーバーB を踏み台にして電子カルテサーバー群に容易に侵入されている。

これらの相違点により X は L 病院、M 病院への侵入を諦め、病院の侵入に集中したものと思われる。

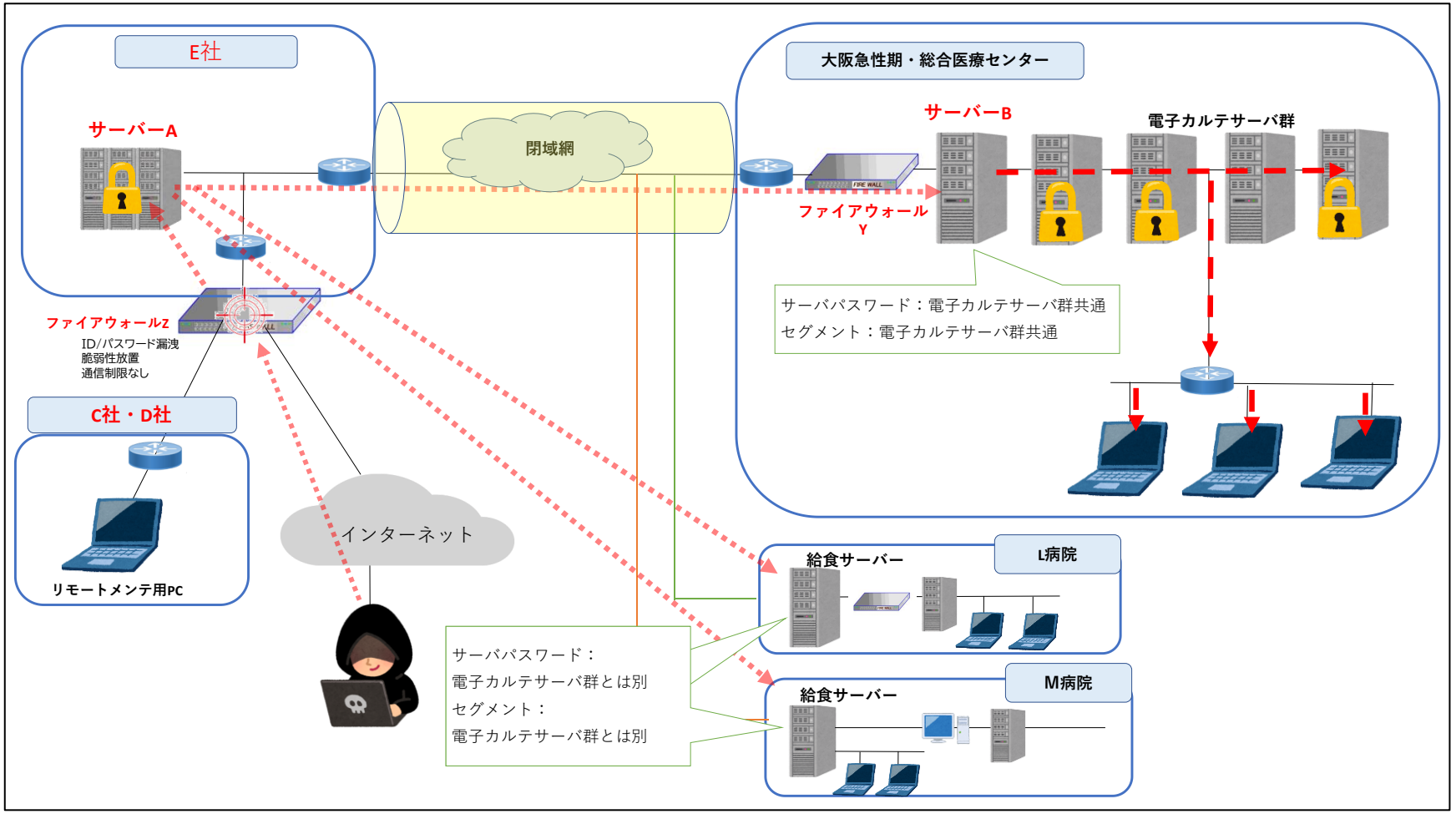


図 10　侵入経路イメージ図

5.7.4. 他の部門ベンダーや医療機器ベンダーの調査

現在も継続して調査を行っているが、今回の E 社給食センターからの攻撃を鑑みて、病院との取引がある他の部門ベンダーや医療機器ベンダーにも調査を行っている。病院に限らず医療機関全体の課題であるが、古い OS の使用を継続している部門システムおよび医療機器が確認されている。このような医療機器は、病院全体のセキュリティレベルを下げている。また、インシデント発生以降も、病院情報システム部門が認識していないリモート保守のための VPN 接続が発見されており、各ベンダーと保護方法について継続的に協議を行っている。

病院で稼働している古い OS（Windows 2000、Windows XP、Windows 7 等）は、主に医療機器や診断システムに搭載されている。一部の医療機器は数百万円～数千万円と高価なことから、すべてを一時期に更新することは不可能である。このため、更新までは、ネットワーク接続の禁止や、厳格なデータ送受信の管理、異常な通信の監視、USB メモリの接続禁止などの保護措置を講じている。

以下に、部門システムベンダーや医療機器ベンダーとの調整において、課題となるトピックを記述する。

① ベンダーのセキュリティ体制について

ベンダーのセキュリティに対する意識はベンダーによって全く異なる状況にある。厚労省ガイドラインが勧める ISO/IEC 27001 の実践についても、ISO/IEC 27001 を取得したうえで、さらにベンダーから病院に向けての侵入や攻撃があり得ないことを論理的に詳しく説明するベンダーが存在する一方で、自社のセキュリティレベルは十分であり、ISO/IEC 27001 などのコンプライアンス規格取得の意向はなく、かつ詳細なセキュリティに関する事項は未公開との報告を行うベンダーも存在した。

② 古い OS の取扱について

2013 年に導入した医療機器で、Windows 2000 を搭載していたケースがあった。Windows 2000 は 2005 年にサポートが終了しており、有償の延長サポートも 2010 年に終了していたが、その 3 年後に病院に Windows 2000 搭載の機器を販売していたことになる。

③ 保守目的での VPN 機器を設置したベンダーについて

リモート保守のための VPN 接続は、部門・診療科とベンダーが 4G（LTE）ルーターを設置するケースが多く、ネットワーク回線の敷設が不要なため、病院情報システム部門に報告が行われず、結果として把握が遅れた状態にあった。4G（LTE）ルーターの多くは、民生品もしくは産業用であるが、脆弱性保守が長期間にわたって行われていないものも散見されており、かつ、責任分界点という意識は総じて低調であり、是正を求めているところである。

また、保守目的で VPN 接続を行うベンダーに設置されている端末が閉域網であることを理由に、脆弱性対策を行っていない旨の回答を得たケースがあった。加えて、ベンダーのセキュリティ体制やネットワーク構成によっては、インターネットに接続できる端末から 4G（LTE）ルーターを経由して、部門システムのネットワークに接続可能なケースもあった。これらについては、引き続き精査を行うとともに、ベンダーのセキュリティ体制の厳格化を求めているところである。

④　部門システムサーバーでの NIC 二枚挿しについて

NIC が 2 枚挿された部門システムサーバーが、脆弱な Windows 端末が稼働している部門システム LAN と、電子カルテ系 LAN を結び付けている事例があった。一見二つの LAN は分離しているように見えるが、実際には明確なルーティングの定義を行っておらず、結果として、部門システム LAN と電子カルテ系 LAN が完全疎通していたケースもあった。ベンダーに問い合わせたところ、ネットワークに関して高度な知識がないことがわかった。今後、ネットワークベンダーを交えて注意したい旨の回答が複数件あった。

⑤　ウイルス対策ソフトの適用について

あるシステムで、ウイルス対策ソフトが設定されていないことが判明し、ウイルス対策ソフトの導入を求めた際に、何故ウイルス対策ソフトを導入しなかったのか、という質問に対して、建物設備として入札がなされ、その入札仕様にウイルス対策ソフトが入っていなかったことから導入をしていない、との回答があった。

⑥　資格情報のハードコーディング等の脆弱性について

復旧中、一部のシステム、医療機器においてパスワードの変更が不可能との報告があったことから確認したところ、プログラムの内部に ID やパスワードを埋め込んでいた（ハードコーディングされていた）ものが存在した。これらは機器の更新が必要であったが、予算、時期等によって再調達が困難であったため、ネットワークの監視などによる保護を行った。他の施設で資格情報を窃取したうえで、病院に侵入し、システム・医療機器に一定の操作を行わなければ攻撃できないことから、俄に大きな脅威とはならないが、利用者が覚知・修正出来ない脆弱性[14]を内在している点で許容されるものではない。

以上のことから、総じて部門システムベンダーや医療機器ベンダーには、自社システムを閉域網に置くことを前提にして、脆弱性を放置したりウイルス対策ソフトを稼働させなかったりしても問題ないという意識が根底にあると考えられる。さらに、脆弱な部門システムや医療機器の存在が、医療情報システム全体のセキュリティレベルを引き下げている現実もある。情報システムの安全性は最も弱い部分によって定まる。たった一台の脆弱性が、今回同様のインシデントを招く原因となることを想定するべきであろう。すべての部門システムベンダーや医療機器ベンダーは、病院情報システム部門とともに、自らの提供するシステムや機器が、病院全体のセキュリティにどのような影響を及ぼすのかを検討する必要がある。

一部のシステムにおいては X に悪用されるシステム設定や、行ってはならないプログラミング上の作法に起因する脆弱性が存在する可能性が大いに考えられる。今後はそうした脆弱性の存在を前提に、脆弱性診断ツールによる調査を進め、脆弱性が発見された際は必要に応じて独立行政法人情報処理推進機構（IPA）への届出を行い、修正を求めていきたい。

5.8.　再発防止策の検討と実行

ここでは再発防止策に焦点を当ててまとめる。

---

[14] 共通脆弱性タイプ一覧 CWE-798 「ハードコードされた資格情報の使用」に該当する。

5.8.1. セキュリティ強化方針

EDR（Endpoint Detection and Response）[15]をはじめとしたセキュリティ製品や SOC（Security Operation Center）などのサービス追加などが、サイバーセキュリティ事故が発生した際には検討される。当然ながら導入できる状況であれば、導入することが望ましい。しかし、病院が、他の一般的な医療機関同様、まだその段階にはないこと、また製品やサービスを利用すれば、人的資源が限られている中で運用負荷が高まることなどから、既存の製品を最大限活用した形でセキュリティを強化することを決定した。

今回のインシデントの主な原因は、E 社からの侵入を許してしまったこと、そして病院での感染が拡大してしまった（検知しにくい状況であった）ことであり、このポイントを重点的に強化する必要がある。

5.8.2. 復旧時のセキュリティポリシー

多くのシステムが 2017 年導入時のセキュリティ・アップデートしか適用されておらず、脆弱な状況にあった。また、グループポリシーも脆弱な状況にあったため、病院と A 社セキュリティ担当部門で新たなグループポリシーを検討し、A 社の本部でポリシー適用における可否を検証することとした。

サーバー向けグループポリシーは米国 CIS Benchmark とし、クライアント向けグループポリシーは、半田病院報告書掲載のものとした。

一部、各部門・診療科システムでの不具合が確認されたが、概ね、順調に稼働を果たしている。以下に代表的なグループポリシー設定値を記す。

表 14　復旧時のセキュリティポリシー

ポリシー	設定値
パスワード	16 桁以上
ロックアウト	連続 5 回以上の認証失敗で 15 分間ロックアウト
Built-In Administrator パスワード	端末ごとにすべてユニークに設定
ユーザー権限	標準ユーザー
PowerShell	実行禁止
RDP ポート	3389（既定値）以外
ウイルス対策ソフト	全数支給のうえ稼働
ユーザーアカウント制御	有効

5.8.3. 給食事業者を含むサプライチェーン経由での攻撃防御

外部からの侵入経路（すなわち、外部接続を伴うネットワーク化が行われている箇所）がどれだけあるのかきちんと棚卸を行い、各事業者と協議を行った。そこでは、リモート接続などの接続方法確認や、原則、ネットワークセキュリティ機器の監視下に置けるような経路の変更のお願い、そして古いファームウェアが確認されれば更新を促し、最新のパッチ対応を行うなどのセキュリティの強化を行った。そのうえで外部接続方法の強化を行い、不要なプロトコルの排除、ポート番号の変更、常時接続を原則許可せず、接続する場合には「申請制」にし、接続を管理できるよう管理体制の見直しを行った。

---

[15] ユーザーが使用する端末、サーバーなどの操作や動作を監視することで、インシデントや攻撃の兆候をいち早く検知することを目的とするシステム。

5.8.4. 侵入後のサイバー攻撃拡大防止策

今回、攻撃を受けた他の医療機関では感染が拡大せず、病院だけ感染が拡大してしまった。要因は、①共通のパスワードを使用していたこと、②アカウントロック設定がなかったこと、③管理者権限で運用していたこと、④一部サーバーにウイルス対策ソフトが導入されていなかったことの、主に 4 点である。

① 共通のパスワードを使用していたこと

管理者や利用者のパスワードとして、12 文字以上で複雑性に考慮していた。しかし、管理者では 2 種類の異なるパスワードを確認したが､利用者に至っては 1 種類の共通のパスワードを使いまわしていた。そのため、パスワードを個別に設定し、16 文字以上を原則に設定を行った。

② アカウントロック設定がなかったこと

グループポリシーを確認したが、何度でもパスワードが間違えられる（アカウントロック未設定）状態になっていた。そのため、X からの総当たり攻撃や辞書攻撃（事前に窃取または準備したパスワードリストを参照してパスワードを試す攻撃）が行いやすい環境にあったため、当該設定を見直し、アカウントロックを有効化した。

③ 管理者権限で運用していたこと

ソフトウェアのインストールやアンインストールなどを攻撃者も行うことができるのは、健全な運用とは言えない。そのため、基本的に標準ユーザーで運用し、ユーザーアカウント制御を有効化した。当初、電子カルテシステムの動作不備などが懸念されたが、特段の電子カルテ運用上の問題は発生しなかった。

④ ウイルス対策ソフトが導入されていなかったこと

電子カルテシステムの基幹サーバーであるデータベースサーバーに、サーバーの負荷を懸念し、ウイルス対策ソフトがインストールされていなかった。電子カルテシステムをウイルス対策によって停止や障害が発生しないようにしていたものである。医療界では電子カルテシステムサーバーなどにウイルス対策ソフトが未導入のところも少なくないようであるが、すべてのサーバーや端末にウイルス対策ソフトを導入し、ウイルスを検出できる状況にした。本対応を行っても電子カルテシステムに支障をきたすような問題は発生していない。

①から③については、GPO[16]での設定や制御によって実現できることから、GPO のランサムウェア感染前の設定の不備を改善し、詳細に設定を行った。

また給食システムに限らず、診療科のシステムサーバーが、NIC を 2 枚挿しして HIS 系ネットワークと診療科内 LAN を特定の制限なしにルーティングしているケースが多くあった。これでは、HIS 系ネットワークと診療科内 LAN の疎通が可能になってしまい、攻撃の範囲を拡大させてしまう原因となる。そのため、ルーターを設置し、必要最小限の通信のみ許可するよう、順次、更新中である。

---

[16] Group Policy Object（GPO）。Active Directory において、ユーザーやコンピューターのセキュリティ設定を一括管理するための機能。

このように、基本的な対策を行うことで、新たなセキュリティ対策システムを導入することなく、適切にセキュリティの強化が行える対策を一つ一つ優先的に実施した。それでもなお、内部のネットワークの監視は欠かすことができないため、こちらについてはネットワークセキュリティ機器を用いた監視できる体制を継続していく。

5.9. 主なステークホルダーの認識と対応

電子カルテシステムベンダー、ネットワークベンダー、給食システムベンダー、給食事業者の認識と対応について整理する。

5.9.1. 電子カルテシステムベンダー

電子カルテシステムを含む基幹システムベンダーであり、かつ病院の第 6 期総合情報システムにおける統括事業者でもある A 社は、システム障害当初から復旧に取り組み、障害発生後約 6 週間での基幹システム再稼動、障害発生後 8 週間での端末全台クリーンインストールのうえでの再配置といった作業を行い、医療機能の早期復旧に取り組んだ。また、システム復旧の際には、上述のセキュリティの脆弱性を改善した状態で復旧に対応したので、現状での病院のセキュリティはかなり向上した。

一方、ヒアリング調査の中では、「パスワードが同じであることは（病院にも）認識してもらっていた」といった発言があったが、そのような重要な取り決めについて合意の確認をしたという記録はなかった。

5.9.2. ネットワークベンダー

第 6 期総合情報システムの構築を担当した B 社は、システム障害発生初日より通信ログを確認し、給食事業者からの通信に不正アクセスが疑われると指摘した。

ヒアリング調査の際には、給食事業者 E 社と病院との VPN 接続による RDP の開放を C 社から依頼された際には、そのリスクを感じたので、C 社に対し病院の許可を取ったのか確認しながらメール等で記録を残しており、A 社に対してはメールで共有していたとの回答があった。

5.9.3. 給食システムベンダー

病院および E 社の給食システム構築やリモート接続設定の構築を行っていた C 社およびその給食システムアプリケーションを提供していた D 社にヒアリングを行ったところ、病院や A 社を含む関係他者と自社の責任分界点を十分に認識できていなかった。特にリモート接続の設定を行った C 社は、「JAHIS のリモートガイドラインについての認識はなかった」というような発言もあるなど、セキュリティ意識が不十分であった。

5.9.4. 給食事業者

2018 年 4 月から、病院と外部接続を行いながら給食提供業務を受託していた E 社は、同社側でもランサムウェアによるシステム障害が発生している中で、手作業による提供時間の遅延は発生したものの、病院や他の委託元医療機関に対する給食提供に与える影響を可能な限り抑え、混乱を生じさせなかった。

一方、E 社は同社側の給食システム構築を C 社に委託していたので、システムやリモート保守に関する詳細は聞いていなかった。問題となる VPN 機器についてもその存在を知らなかった。

6. 調査委員会報告（病院および社会の課題と解決に向けて）

今回のインシデントを通じて、病院としての課題を、組織的な視点、人的な視点、法的な視点から整理する。なお、技術的な課題については、これまでの調査結果などの記述のとおりであり、ここでは割愛する。

6.1. 病院としての課題と解決に向けて

6.1.1. 組織的な視点

まず、今回の最大の課題は、医療機関としてセキュリティの重要性を再認識し、医療機関とベンダーの責任分界点を明確にすることである。これまで述べた通り、セキュリティにおける双方の共通理解を求め、契約書や仕様書のレベルまで落とし込むなど、認識の相違が生じず、インシデント時も即応可能な体制にしておくべきである。

そして、上記の課題から生じている契約内容の不備の解消を行っていく必要がある。一般的に保守・運用をはじめ物品調達においても各種契約書にセキュリティに関する事項が明記されているケースはさほど多くはない。病院においても同じような状況であった。なお、厚生労働省が公開している「医療情報システムの安全管理に関するガイドライン（第 4.3 版）」に準拠したシステムを構築するよう明記はされていたが、インシデント発生時の対応、普段からの脆弱性管理の役割など、セキュリティ対応に関する記載はなかった。また、委託事業者とのインシデント対応の中で、システムを監査、監督する権利が明記されておらず、委託事業者との情報連携や情報共有が行われない（行われにくい）状況にあり、対応に苦慮していた。なお、具体的には「法的な視点」の部分で述べる。

また、次に大きい課題は、病院としての情報資産が把握できていないことである。セキュリティ対策を行うにしても、守るべき資産が明確でない限り適切なセキュリティ対策は実現できない。無論、すべてのシステムが重要で、すべてのシステムに対していくらでもお金をかけることができるのであれば考える必要はないが、そのような組織はおそらく存在しないであろう。つまり、守るべき情報資産を明確化したうえで、どのように最適にセキュリティ対策を実施していくのかを検討していかなければならない。

今回、初動対応の段階において、外部接続箇所の確認や、部門システムや医療機器などの現状確認から開始している。災害対策同様に情報技術を活用するうえでは準備が必要である。すなわち、病院においては「IT ガバナンス」が不足していたといえ、その確立に向けた取り組みが必要である。一方、どこまで病院に対応を求めるのかは、資源の観点から見ても課題である。

さらに、インシデント対応体制の不備も解決すべき課題である。今回、厚生労働省の専門家チームの協力があってこそインシデントの早期解決に向けた判断や対応ができたと考えられるが、病院や電子カルテシステムベンダーなどが、早期に対応できる体制が必要であった。病院としては電子カルテシステムを中心としたシステムをベンダーに依存し、一方でベンダーも情報の非対称性を理解したうえでの協議の継続などが不足していた。そのため、いざインシデントが起きた際に、決定するのは病院であり、病院の動きを待つベンダーとで認識や対応の隔たりが生じていた。しかし、これは病院に限らず、医療機関や他の業界においても共通した課題とも言え、課題解決には病院とベンダーの継続的な協議のうえ、認識を共

有することも必要不可欠である。これらのことは、 医療界全体の共通課題と捉え、解決に向けて社会全体で動く必要性もある。

本事案は、医療機関における IT ガバナンスの欠如、サプライチェーン全体のセキュリティ意識の低さが露呈したものであった。病院の IT ガバナンスの確立を目指した動きは勿論のこと、すべての医療機関、医療界のすべての組織において、セキュリティの重要性を再認識する必要がある。病院の情報部門も各システムやネットワークの把握に努めていたが、病院の情報資産の把握は適切に行われていなかった。まずは情報資産の棚卸を実施し、保護すべき対象を明確にし、保護対象の資産をどのように保護していくのか検討を深める必要がある。

そのうえで、IT ガバナンスの確立に向けて、セキュリティ運用を意識した組織としてのセキュリティ目標を定め、統制環境、リスクの評価と対応、統制活動、情報と伝達、監視、情報技術の活用などを確立していくべきである。

これまで医療界は「閉域網であるから安全である」といった考えで、セキュリティに対する考えや取り組みを停止し、ソフトウェアの更新すら行わず、ウイルス対策ソフトの導入や、セキュリティログの取得や運用も進んでいない。製品やサービスの開発思想が古いものも散見される。医療界としてこのような課題解決を行う必要があり、病院がそのけん引役となることを願いたい。

なお、病院は、地方独立行政法人大阪府立病院機構の一機関であり、機構本部との連携も欠かすことができない。機構内の各センターでは、それぞれ担当者を置くことができる環境ではあるが、どの組織もセキュリティ人材の不足は明らかである。

機構内の各センターでセキュリティの方針やルール、機能を個別に持つのは非効率であり、病院機構本部が骨格を作り、各センターはそれを実践していく体制に変更していくことが考えられる。つまり、セキュリティ指針やセキュリティポリシーの作成など、各センターに共通した取り組みについては、機構本部で整備することが望ましい。

またサイバー攻撃の検知や対応として Security Operation Center（SOC）[17]の活用などが、企業では検討されているが、医療機関においても検討は必要である。しかし、各センターに SOC 機能を有するのではなく、機構本部で機能を有し、各センターを効率的に保護する仕組みの検討と導入が必要である。

さらに当該枠組みが確立できれば府内の医療機関のセキュリティ監視などに発展できる可能性もあり、大阪府全体の医療機関のセキュリティ向上につながる可能性もある。

6.1.2. 人的な視点

医療機関においては、サイバーセキュリティは医療提供を行うシステムを保護する一機能に過ぎない。セキュリティの専門家をすべての組織で設置することが望ましいが、セキュリティ人材もそこまで潤沢にいるわけではない。しかし、医療情報システム安全管理責任者を中心にしたセキュリティ向上は必要であり、これまでのセキュリティに対する考え方を改め、脅威の変化に伴う対応、訓練のようなセキュリテ

[17] 外部からネットワーク機器やサーバー類を常時監視し、サイバー攻撃の検出と分析、対応策のアドバイスを提供する組織、企業のこと。SOC を提供する企業を SOC ベンダーという。

ィに対する意識付けも欠かせない。医療機関においてもセキュリティ教育を継続的に実施し、意識やスキルを高めていく必要がある。

さらにベンダーの意識向上も欠かすことはできない。そもそも製品やサービスを提供するにあたって、古い OS の利用や、ソフトウェアの更新思想がないもの、ID やパスワードの変更が難しいものなど、専門家としてのセキュリティの意識や知識の欠如が散見された。ベンダーは、医療機関にとっては機器やシステムの専門家であり、セキュリティを意識した相談や対応、製品やサービスの提供が行えるよう体制を確保すべきである。

大切なことは双方の意識や知識を高め合っていくことである。サービス仕様適合開示書などを用いた合意形成を行うことによって、契約前・契約中の双方の共通理解と合意を図り、医療機関もベンダーもシステムやセキュリティに対する理解と知識を高め合えるよう継続的に研鑽する必要がある。

6.1.3. 法的な視点

6.1.3.1. 契約書におけるあいまいな表現を具体的な表現に変えるべき

事故が起きたときに、誰が何をすべきだったのかが問われる。法令からみると、保守契約においては、いわゆる善管注意義務に違反したか、債務不履行があったか、不法行為の要件である「過失」があったかなどが責任の所在を決める基準だが、これらはいずれも抽象的な基準で具体的には適用するのは難しい場合が多い。そこで具体的な事件の裁判ではもっと具体的なことが書いてあるはずの、契約書の文言に基準を求めることが多い。

契約書に誰が何をやるべきかが網羅的に書いてあれば、事故が起こる前に、責任を負うべき当事者が何をやらなければならないかに気付くため、事故が起こるリスクを低減できる。事故が起こる理由は、事故を防ぐために何をすべきかを契約書に明確に書いていないからであることが多い。

本事案においても、単に「ガイドラインに従う」と記載するだけで、個々の当事者がどこまでのことを行うべきであったかが判然としていない点があった。さらに問題なのは、あいまいな点について、一方の当事者は、「重要な点は IT の専門家である相手方がきっとやってくれる」と考え、他方の当事者は「契約にはっきりと書いていないことはやらない」と考えていた可能性が高いことである。 以下のような点について誰が責任を負うかについて具体的に記載をしていれば事故が防げた可能性があるので、今後の契約における改善が望まれる。

1. セキュリティ設定
2. 強固なパスワードの設定
3. ロックアウトの設定
4. 管理者権限をもつものを最小限にする
5. サプライチェーンも含めた（外部接続）監視、監督
6. 安全なリモート接続の設定、監査
7. OS、アプリケーションのバージョン管理

6.1.3.2. 契約後の変化に対応できるための規定を入れるべき

契約書には契約を締結した時点でわかっていることしか書けない。上記のように具体的に誰が何をや

るべきかを書いたとしても、契約後の変化に対応できない。

本事案においても契約書締結時点にはなかったセキュリティのリスクが契約締結後に発生し、その点における手当のなさから事故につながった可能性がある。そこで、契約後の変化に対応することについての取り決めを行う必要がある。ここでの文言は契約締結時点ではわからないことに対応するので抽象的にならざるを得ないが、それでも工夫をして何をやるべきかをなるべく具体的に記載する必要がある。例えば以下のようなことを記載すべきである。

1. インシデント予防のためのアドバイス、情報提供、情報には以下のようなことを入れることが考えられる
   (1) 政府機関（省庁、NISC)、JPCERT コーディネーションセンター、IPA が注意喚起したセキュリティリスク
   (2) 国内 ISAC、セキュリティ関連団体が注意喚起したセキュリティリスク
   (3) OS、アプリケーションソフトのバージョンアップ情報
2. インシデント発生時のベンダーの協力体制

6.1.3.3. 契約を遵守するための体制

いくら良い契約を作ってもそれをきちんと遵守しなければ文字どおり絵に描いた餅である。本事案においても、契約書に書いていることを遵守しているかのチェックが徹底していなかった。その結果リスクにつながる契約の不遵守を見落とし、あるいは、不遵守に気が付いても一方の当事者は相手に遵守を求めることを行っていなかった可能性があり、結果として事故につながった。 したがって、今後の契約書には、契約書の遵守を確保するための規定が必要であることが望ましい。例えば、定期的に第三者による監査を行うことについての規定が考えられる。その結果、リスクの早期発見、対処につながると思われる。

6.1.4. 事業継続マネジメント全般的な視点

本節では、事業継続の視点で浮き彫りとなった現場対応、対応や課題について整理する。

6.1.4.1. 参照環境の構築

先述のとおり、システム障害が長期化すると決まった段階で最優先に行うべきは、電子カルテのバックアップデータを参照する環境の構築であった。これがシステム障害期間中の医療継続に大きな助力となる。バックアップデータを用いて参照環境を構築するには、①オフラインバックアップの確実な取得、②バックアップを戻して電子カルテのデータを参照できるようにするためのサーバー確保、が重要となる。また、今回の病院のようなオフラインバックアップが LTO テープのような外部媒体の場合は、それを読みだす機器も必要となる。今回の事案では、参照サーバー確保に 1 週間を費やしたため、参照環境構築に 10 日間必要であった。

医療機関がサイバー用の BCP 策定を検討する場合には、バックアップの確認（感染有無確認を含む）から、実際に参照サーバーにリストアし、端末から参照できるようにするまでの手順について訓練を行うべきである。なお、バックアップが正常に実行できているかを定期的に確認することも重要である。これは、いざという時にリストアできない可能性もバックアップシステムには起こり得るからである。

6.1.4.2. 災害用紙様式・マニュアル類の確保

今回のサイバー攻撃による医療継続にあたって、病院が困ったことの一つに、災害用に準備していた紙様式のデータや BCP などのマニュアル類が、電子カルテ上にあるグループウェアや、各所属の端末に保存されており、いざというときに利用できない、閲覧できない、様式の改定ができない、といったことが起きたことが挙げられる。自然災害用の紙様式は準備していたが、短期間を見据えた様式であって、長期間の運用には適しておらず、また定期的な見直しもできていなかった。そのうえ、様式を更新しようにもデータが電子カルテ端末に保存されていたので、紙様式を最初から作成し直さなければならなかったこともあったという。災害用のマニュアルや様式等のデータは、各部署において外部媒体に保存しておくことが得策であった。また、BCP は昨今の自然災害に主眼を置いた内容になっていたことは否めない。サイバーセキュリティインシデントに備えた BCP（IT-BCP）も必要である。 BCP 策定の際には考慮されたい。

6.1.4.3. 一般 OA 用端末の確保

電子カルテ端末が利用不能となった時点で、医療現場で困ったことが患者情報を入力するためのパソコンが不足したことであった。通常のパソコンはインターネットに接続されている場合が多く、診療情報管理の観点から、外部接続がされているパソコンでの患者情報入力を禁止していたためである。

手書き運用に慣れていない医療現場からは、患者情報が入力できる端末を要望する声がかなりあった。電子カルテが復旧した際には、データを貼り付けたいという気持ちもあったとのこと。しかしながら、病院にはそのようなパソコンの備蓄が無かったことから、医療現場には我慢してもらった経緯があった。

今後の BCP 策定に際には、このような事態も想定し対策を講じておく必要がある。

6.1.4.4. USB タイプのウイルスチェック

病院では数多くの医療機器が、OS をベースに稼働しているが、通常は医療機器にはウイルス対策ソフトが設定されていない場合が多い。これも閉域網神話に基づくものや、医療機器の動作保証がメーカーで担保されていないという理由もあった。しかしながら今回の事案ではウイルスチェックを行わないと、医療機器であっても再稼動ができない方針としたため、ウイルスチェック作業が必要となったが、そのようなツールが手元になく、USB タイプのウイルスチェックツールを緊急で 11 本購入し、1 週間後に受領した。このようなウイルスチェックができるような事前準備を、実施しておくことが望ましい。

6.1.4.5. 情報伝達手段の確立

病院での日常のコミュニケーションツールは、電子カルテ端末上で運用しているグループウェアを活用しており、掲示板や緊急連絡メールなどは電子カルテ上で行っていた。それが今回の事案で利用不能となったことから、別の手段で職員約 2,000 人に対して病院の方針などの決定事項を周知徹底させることになった。

具体的には、病院では電子カルテとは別の、府立病院機構全体のネットワーク上にグループウェアが稼働していたので、その掲示板機能を活用しつつ、各個別には、日常から災害医療用に活用していた全職員対応の BCP 対応ツールを活用し情報伝達を行ったり、役職者以上のメーリングリストを作成しメールでデータ送信を行ったりし、情報伝達手段を早期に確立したことにより、初動時の混乱を緩和することがで

きた。

自然災害時にも共通することだが、非常時には情報伝達手段を直ちに確立し、正しい情報を現場に周知できるような体制を構築することが重要である。

6.1.4.6. 情報統制と職員メンタルケア

専門家チームとの初会合（障害発生 2 日目）の際に、セキュリティ関係以外で助言を受けたことは、「情報統制を徹底すること」「職員のメンタルケアに注意すること」「こんなときだからこそ、ちゃんと休息をとること」の 3 点だった。その指摘を受けた病院職員は、その後の BCP 対策本部会議で専門家チームの 3 つの助言を報告し、会議に参加していた管理職員に周知した。

メンタルヘルスについては、サイバー攻撃により一部の部署において飛躍的な業務量の増大や、患者対応に疲弊した職員もいたようであった。病院は、12 月 5 日に専門講師を招き「災害等の危機的状況における職員のメンタルヘルス」と題した講演会を開催した。また普段、有給休暇が取得しにくい部署において積極的に取得させるなどの対応を行った。

結果的には、サイバー攻撃が発生してからこれまでの間で、メンタルに伴う病気休暇を取得する職員はいなかった。情報統制についても問題になった事例は発生しなかった。

6.1.4.7. その他 BCP 策定における要留意事項

その他、大規模システム障害における医療継続に当たって、各医療機関で BCP 策定の際に留意しておくべき事項を、以下に一覧に示す。

表 15　サイバー用 BCP 策定の際の主な留意事項

	項目	検討課題
1	外来受付混乱	障害発生時に、予約外来患者の予定がわからず、バックアップによる参照環境が構築され、予約患者リストが確認できるようになるまで混乱が続いた。 また、今回は各科外来での受付を継続させたが、総合受付方式が良かったのかどうかは、病院の規模や建物構造にもよると考えられる。 各医療機関においては、サイバー攻撃により電子カルテが長期間参照できない場合に、外来運用をどのように行うのか、予め検討しておき、BCP に反映させておく必要がある。
2	病棟での患者情報	今回の事案で、入院患者の医療継続にあたっては、DACS を稼働させていたこと、かつ運よく DACS サーバーが感染を免れていたため、その参照環境を早期に構築し運用を開始できたことが功を奏したが、それも偶然の産物であった。 電子カルテが参照できなくなった場合に、どこにどのような患者データ（紙媒体、データ保管）が存在し利用できるのか、どのような診療情報があれば医療継続や転院のための紹介状の作成などの作業ができるかなど、入院患者の医療継続に必要な手順を、各医療機関の状況において検討

	項目	検討課題
		し BCP に反映しておく必要がある。 バックアップデータを活用した参照環境が構築されるまでの間、目の前の入院患者の医療をどのように継続するかは、各医療機関の規模や状況に応じて検討し、活用可能な医療情報を整理しておくべきである。
3	電話回線増設	サイバー攻撃に関する報道発表を行うと、患者からの問い合わせが殺到し電話回線がパンクする。病院から患者への電話連絡さえ妨げられる。 発信専用の電話回線を予め準備するか、障害時には直ちに増回線を依頼するなど、電話環境を拡充することが重要である。
4	会議室の確保	BCP 会議や、大規模な復旧作業や打ち合わせの円滑運用など、大規模システム障害の際には部屋の確保が有用であった。主要な会議室などは当面の期間、確保しておく必要がある。

6.2. 社会的な課題

本事案により、医療機関におけるサイバー攻撃やサイバーセキュリティ対策は、日本社会全体の注目を集めることになった。今回は病院で発生したが、どの医療機関でも起きる可能性がある。医療界共通の課題として、医療機関そのもののセキュリティと、ステークホルダーの多い医療機関におけるサプライチェーンセキュリティの課題を露呈した。以下に全体的な課題を整理したうえで、各ステークホルダーの視点から社会的課題について整理する。

6.2.1. 社会全体の視点

医療機関は、安心・安全な医療を提供するのが主たる事業であり、どの業態においてもサイバーセキュリティはその一要素にしか過ぎない。しかし、医療においても DX(デジタルトランスフォーメーション)が叫ばれている昨今において、サイバーセキュリティは欠かせない要素になってきている。とはいえ、すぐにセキュリティ人材を確保することは難しい。また医療機関ごとにセキュリティの専門家を設置することも難しいと思われる。

昨今、プラス・セキュリティ人材という言われ方もされるように、職員それぞれが業務遂行にあたり少しでもセキュリティを意識することにより、組織全体のセキュリティレベルの底上げにつながり、セキュリティを考えられ、対策につなげることのできる人材を増やしていくことができる。情報システム関連職員に限らず、設備や広報、法務など関連しそうな職員は特に意識することが大切である。また「リスキリング」が注目されている中で、すべての人がセキュリティを少しでも学ぶように心がけることも大切である。

6.2.2. 医療機関としての視点

まず最大の課題は資源である。すなわち、資源とは特に「人材」と「財源」である。

そもそもサイバーセキュリティについての人材は継続して不足が叫ばれており、さらに医療機関にもセキュリティ人材を確保するとなると、そもそもの母数が少ない状況で、不足している問題を解消することは難しい。また、医療機関は情報技術の活用やシステムに関しては、ベンダーへの依存度が極めて高く

ベンダーに頼り切りになっている現実もある。この状況から脱却し、自らのセキュリティを向上するためには、医療機関におけるセキュリティのスキルの向上が必要である。ヒトの視点においてはセキュリティ人材の数といった量的視点と、セキュリティのスキルや経験といった質的視点が双方不足しており、人材育成が急務である。

もう一つは「財源」である。民間企業の視点で言えば「経営力」が問われるのでないかと思われるかもしれないが、例えば、ダイナミックプライシングのように需要と供給によって価格設定ができるような事業のやり方は医療機関ではできない。これは医療安全および安定した医療を継続的に提供するために、法律によって定められた公定価格である 「診療報酬」でしか、基本的に医療機関は収益を上げられないからである。

この診療報酬改定を行ってでも医療機関のセキュリティ強化に資源を割くことはできるかもしれないが、診療報酬を改定するということは、国民の負担が増えることであり、国民的な議論に発展することを忘れてはならない。

6.2.3. 電子カルテシステムベンダーの視点

電子カルテシステムベンダーの課題は、「古い仕組み」と「セキュリティの知識不足」である。

そもそも電子カルテシステムに限らず、医療機関のシステムや機器は「閉域網だから安全である」という神話に頼って、脆弱性を放置し、セキュリティ対策を適切に実施していないものが散見される。また電子カルテシステムによっては未だにサポートが終了している IE（Internet Explorer）に依存しているシステムもある。管理者権限での運用が前提と考えられていたり、ウイルス対策ソフトを動作させないサーバー設計になっていたり、セキュリティ思想そのものが古い。

加えて、電子カルテシステムベンダーのセキュリティ知識も不足している。たとえ、古いセキュリティ思想に基づいて、電子カルテシステムを安定動作させ続けることに障害になると考えて、セキュリティ対策アプリケーションの利用などを避けたとしても、改訂予定の厚労省ガイドラインで叫ばれる「ゼロトラスト」の基本となるマイクロセグメンテーションや内部通信の監視、Syslog の取得など、既存の環境でも実現可能な適切な運用を行っていれば、本事案を未然に攻撃を防げた可能性も高い。残念ながら国内最大手のシステムインテグレーターであってもセキュリティ人材は東京に集中してしまっているのが現状で、ベンダーにおけるセキュリティ知識や経験を地域に拡散していく努力も欠かせない。

ベンダーは、情報システムに関する知識の非対称性を理解したうえで、医療の専門家である医療者を支えるシステムの専門家であるシステムインテグレーターとして、その役割を果たすべきである。

6.2.4. 部門システムベンダー・医療機器ベンダーの視点

部門システムベンダーも前述した電子カルテシステムベンダーと同様のことが求められる。しかし、1つ付け加えたい点は、ベンダーとしての協力姿勢である。電子カルテシステムベンダーもこれだけ多岐にわたるシステムを管理するのに苦労することは想像に難くない。また、電子カルテベンダーがセキュリティの視点でより厳格に調整や協議を行えば、今のシステムや機器は導入できないものも生じる。

つまり、ベンダーが提供する製品やサービスに課題がある場合、電子カルテベンダーにも適切に情報共

有を行い、運用方法を協議していく必要がある。「仕様である」という台詞で事を済ませられるほど簡単な状況ではないことを理解し、ベンダー間での歩み寄りと連携も必要不可欠である。

6.2.5. ネットワークベンダーの視点

ネットワークベンダーについては、セキュリティを確保するためにはこの分野の適切な管理が極めて重要となる。外部接続を行う場合や、内部ネットワークでも医療機器側や建築側で構築されたネットワークを HIS 系ネットワークと接続を行う場合などには、リスク評価および管理方法など、病院や基幹ベンダーと十分に検討を行い、接続の可否を判断していく必要がある。

また日常的にも外部接続機器の脆弱性管理やその情報提供、またリスクのある接続を行った後の適切な運用状況の確認など、その管理については関係者と情報共有を行い、方針等を記録に残しておかないと、今回の事案のような状況が発生する可能性が高まる。

これから医療界全体でのネットワーク化がますます加速する中では、その役割の重要性は高まるばかりであり、ネットワークセキュリティに係る人材の育成も重要な課題となる。

6.2.6. 厚生労働省の視点

現行の「医療情報システムの安全管理に関するガイドライン」は網羅性という観点からも、ISMS ベースのガイドラインが作成されている。しかし、中病院（約 120 床）の半田病院でも、大病院（約 850 床）の病院でも実践が難しいという現実を受け止めるべきである。より実践的なガイドラインと、診療所やクリニックでも実施できる最低限のセキュリティ対策などを定め、基本的な対策から医療機関におけるセキュリティレベルを向上させていく必要がある。また ISMS は表層的であるため、他省との連携を行い、設定に踏み込んだ文書になることが望ましい。

また、既存の診療報酬制度は医療が停止せず、すべてのデータが存在し続けることが前提となっている。しかし、これだけランサムウェアによる被害が発生している状況では、発生させない対応は勿論だが、発生した場合でも柔軟に経済的にも安心して医療継続ができる制度検討が必要である。例えば、データ提出加算を 1 つとっても提出が行えない状況を鑑みる必要がある。「サイバー攻撃」が災害と同等という考え方を持つことによって、制度の設計思想も変化させ、診療報酬の在り方そのものを検討する必要がある。さらに、サイバー攻撃による大規模システム障害は「災害」と同様に捉え、DMAT 同様の初動チームの編成、緊急財政出動、各種要件の緩和、また、そもそもこのような災害が起きないために、基盤となるセキュリティ対策費用の診療報酬以外の手段での供給も必要である。

なお、医療機関におけるサイバーセキュリティ対策は、IT の専門家から見ると常識的なことすらなされていない。今回の事案のような大規模システム障害は今後も発生する可能性が高く、今回の初動対応支援事業は可能な限り継続をお願いしたい。

6.2.7. 国の視点

デジタル庁では自治体などを中心とした電子化や標準化が進められている。また、総務省においてはこれまで「セキュリティクラウド」のように都道府県単位でインターネットに接続される出入口を集約している。医療機関においても各自でセキュリティを検討し、例えば、ファイアウォールを個別に設定した

り、管理させたりするのではなく、包括的な枠組みと体制が必要である。国や自治体レベルでセキュリティ機能を集約したり、医療サービスにおける共通プラットフォームを確立したりするなどの検討を、厚生労働省に限らず、国全体で国民の命を守るための医療機関のセキュリティ体制の検討が必要である。

またサプライチェーンセキュリティの課題は、それぞれのステークホルダーの監督官庁が複数またがることもあるため、サイバーインシデント発生時には各監督省庁を横断的かつ機能的に司令塔的役割を担える国の部局を明確にするなど、課題解決に向けた取り組みが必要である。つまり、機能するサイバーセキュリティの司令塔を明確にし、サプライチェーン課題解決に向けた動きが必要である。

7. 課題解決のための提言

今回のインシデントは病院で発生したものの、医療機関、医療界が「閉域網神話」にすがり、これまでセキュリティを直視してこなかった結果であると言える。一方で、長年にわたり解決が難しいということは、各医療機関で解決を図ることは難しいということであり、社会全体で解決策を考えていく必要があるので、ここでは課題解決のための提言をまとめる。

7.1. 医療継続のための取り組み支援

自助（病院の）努力の必要性は理解したうえで、国や地方公共団体には医療機関のサイバーセキュリティの継続的な向上と維持のために、また地域医療を安定的に持続するために、以下のような支援や対応を願いたい。

- 「財政的」「人的」「物的」、そしてスキルなどの「情報的」視点の支援
  セキュリティの強化と言っても単純にセキュリティ製品やサービスを導入すれば強化できるわけではなく、そのような無駄な投資は避けなければならない。まずは、既存の製品を最大限活用して、設定やポリシーを強化することによってセキュリティを高めていくことが必要であり、その設定に必要なガイドラインやベースラインの整備を国にお願いしたい。また、新たなモノを買うのではなく、医療機関における設定や脆弱性の診断など、まずは脆弱な状態を認識し、打開することが最優先であると考える。
- インシデント発生当日から厚生労働省の「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・調査事業」によって、専門家チームが派遣され対応の支援を行った。現状、医療機関はこのようなサイバーセキュリティ上の事故が起きたときに、どのようなベンダーを頼りにすればよいのか、その相談相手や支援の依頼先が明確になっていない。半田病院と病院のインシデントを見れば明らかであり、各地域にそのようなセキュリティ人材も不足している。そのため、厚生労働省における当該事業は可能な限り長く継続いただきたい。
- 医療機関における医療情報システムやセキュリティに知見のある IT 人材の配置とともに、医療機関のすべての人がセキュリティ意識を高く持ち続けられるよう、共通的なセキュリティ教育の継続も欠かすことができない。現在は、診療録管理体制加算の一つの要件として 400 床以上の病院の場合には専任の医療情報システム安全管理責任者の配置や年 1 回の情報セキュリティに関する研修の実施などが施設基準の中で義務付けられているが、当該加算はそもそも診療情報管理士による診療情報管理の取り組みを評価したものであり、医療情報システムの管理およびセキュリティ強化やＩＴ人材の確保に係る診療報酬制度にはなっていない。診療録管理体制加算とは別建ての診療報酬の評価が必要であるとともに、すべての病院に適用できるような制度設計が望ましい。

7.2. セキュリティ機能の集中・集約化

医療機関と言っても小規模な診療所から、病院のような大規模病院まで様々であり、すべての医療機関で同等のセキュリティ対策を実現することは不可能である。そのため、セキュリティ対策も効率的に実施する必要がある。そこで、国および地方公共団体は、すべての医療機関でのセキュリティ責任者の設置を目指し、サイバーセキュリティに詳しい人材を仮想的にも集約し、すべての医療機関にセキュリティ支援が行えるような人材共有の枠組みも必要であると考える。

また国には、地方公共団体のセキュリティクラウドのように、医療機関における SOC を含めたセキュリティの集約を都道府県や国レベルで整備し、セキュリティの共通プラットフォーム化を検討することで、個別医療機関のセキュリティ負荷の軽減をお願いしたい。

7.3. 脆弱なシステムや機器を生み出さないための根本的な仕組み

現在あるガイドラインは医療機関の規模や体力を踏まえたものではなく、網羅性の観点で大規模病院でも実現が難しいものになっている。医療機関においてより現実的かつ実践的なガイドラインの整備など、現実に沿った法やガイドラインの整備をお願いしたい。

また医療機関に提供されてきたシステムや機器は「閉域網だからセキュリティは問題ない」といった前提で設計がされており、ベンダーの開発における根本的な設計思想の転換が必要である。これは現行の薬事法や薬機法の解釈や改正を含めた議論も必要である。また喫緊の課題として現状のシステムや機器が安全であるかどうか、脆弱性診断を始めとしたセキュリティチェックが必要であると考える。

なお、欧米では医療機器などにおける Software Bill Of Materials[18]が検討され、ハードウェアに限らずソフトウェアの領域にもより一層の安全性議論が進んでいる。このような状況下において古い機器を提供し続けている我が国においては国際競争力も損なわれ、医療システムや機器を提供している企業の衰退も招きかねない。また SBOM の議論が始まっている一面もあるが、もし今の状況で SBOM を作成し、構成管理を強化しても、脆弱性があってもそのリスクを医療機関が受け止めなければならない。このような近い将来想定できる医療機関におけるリスクや工数の高まりは、医療機関が望むところではない。ベンダーがソフトウェアの構成管理を適切に行い、脆弱性管理と対応を行う体制や機構を確立しなければ、今後も医療機関におけるサイバー攻撃リスクは継続することになる。このようにセキュリティにおける共通の考え方や枠組み、またセキュリティ運用を踏まえた現実的かつ具体的な規格が必要である。

7.4. インシデント情報等の医療機関同士の情報共有の場

インシデントは学会やセミナーなどでも共有は行われているが、今回のようなインシデントの詳細や具体的な対策、特殊な事情など、公の場では共有し難い情報もある。しかし、病院に限らず医療機関で起きたインシデントは共有と活用を行わなければ、同じ過ちを繰り返すことになる。

昨今、業界ごとにセキュリティインシデントの共有や必要な機能を集約した ISAC[19]の発足と運用が、金融、ICT、交通、自動車、ソフトウェアなど様々な業界で進んでおり、医療分野においての構築も急務である。現在、厚生労働省でも検討が進んでいるようであるが、特に医療機関同士がその大小に関係なく、連携できる枠組みを早期に立ち上げ、運用を行うべきである。そして、特にインシデントが起きてしまった医療機関は積極的にそのような枠組みに協力すべきである。

---

[18] SBOM:エスボム。脆弱性管理のためのソフトウェアの部品表のこと。どのようなソフトウェアコンポーネントを使用したかの一覧を作成するとともに、脆弱性情報の入手先やサポート終了などを管理する。

[19] Information Sharing and Analysis Center、アイザック。業界内でのセキュリティ情報の共有や、連携の取り組みを推進する組織。国内では金融 ISAC、電力 ISAC、交通 ISAC、ICT-ISAC（情報通信）、J-AUTO ISAC、software ISAC、貿易会 ISAC などの ISAC が活動している。

8. まとめ

今回、病院が、復旧の際に取り組んだ再発防止策の内容も含め、発生した内容をできる限り公開したいと考え、本報告書をまとめた。医療を守るために、命を守るために、医療機関だけではなく国民を含むステークホルダー全員が、サイバーセキュリティを考えるときが来ている。国内のすべての医療機関は、今回の事故を必ず生かし、同じような事態を起こさないよう努力する必要がある。またベンダーはその対応に最大限支援を行い、医療界全体としてセキュリティのレベルアップが必要である。医療業界はまさしく、サイバーセキュリティにおける転換点にある。

今回の事故は病院のシステムが停止する重大なインシデントであったが、本事故に起因した死者を出すことは無く、比較的短期間で病院機能を復旧することができた。これは、病院の医師・看護師をはじめとする全職員とその家族、地域医療機関の関係者、給食事業者をはじめとする様々なサプライヤー、電子カルテシステム・部門システム・医療機器・セキュリティベンダー、大阪府警察本部、大阪府、厚生労働省、ソフトウェア協会の専門家チームなど、すべての関係者の連携や支えがあったからに他ならない。

患者の皆様には電子カルテシステムが機能しなくなるという事態で困惑した方も多いと思うが、病院を始めとするすべての関係者が、医療継続のために最大限努力し、医療継続やインシデント対応に取り組み続けたことには是非ともご評価をいただきたい。残念ながら、昨今はサイバー攻撃も巧妙化しており、いつ、だれに起きてもおかしくない状況である。

最後に、病院には重ねてこのような事態を起こさぬよう、サイバーセキュリティに対しても不断の努力をお願いするとともに、今回、関係したすべての皆様に、心からの感謝の意を伝え、本報告書の括りとする。

参考資料等

調査報告書　用語の定義

用語の解説は、医療情報システムの安全管理に関するガイドライン別冊用語集や国立研究開発法人情報通信研究機構（NICT）のホームページ用語集を一部引用。

用語	定義
ATT&CK （アタック）	Adversarial Tactics, Techniques, and Common Knowledge の略。 MITRE が収集した脆弱性情報を整理し、脆弱性を悪用した攻撃を戦術とテクニックの観点で分類したナレッジベース。
BCP	事業継続計画（Business Continuity Plan） 災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関等の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用。
CWE	共通脆弱性タイプ一覧（Common Weakness Enumeration）。 コミュニティが作成した、セキュリティに影響を及ぼす一般的なソフトウェアおよびハードウェアの脆弱性の分類リスト。
LTO	リニアテープオープン(Linear Tape-Open)。 コンピューターのデータバックアップ、アーカイブに使用する磁気テープ技術の標準規格。カセットテープカートリッジを使用し、10TB を超える大容量のデータ保管に向いている。
MITRE （マイター）	国政府の資金援助を受けている NPO。 全世界の脆弱性情報（Common Vulnerabilities and Exposure：共通脆弱性識別子）の採番や、サイバーセキュリティの研究を行っている。
NIC	ネットワークインターフェースカード（Network Interface Card）。 コンピューターなどの機器を通信ネットワーク（LAN）に接続するためのカード型の拡張装置。
RDP	リモートデスクトッププロトコル（Remote Desktop Protocol）。 手元の端末からネットワークを通じて他の端末のデスクトップ環境などを遠隔操作する技術の総称。
SLA	サービス・レベル合意書（Service Level Agreement）。 書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書
SMB	サーバーメッセージブロック（Server Message Block） Windows のネットワークでのファイル共有やプリンター共有のための通信手順。

用語	定義
SSL-VPN	SSL-Virtual Private Network の略。リモートアクセスでの通信経路上を TLS（SSL の後継技術）で保護する技術。IPsec を用いた VPN のような特定端末間だけで VPN を構成する、いわゆる拠点間 VPN とは異なる。
TCP	Transmission Control Protocol の略。 インターネットで標準的に利用されているデータ転送の信頼が保証されるプロトコルで、Web のデータ転送を行う HTTP や HTTPS、電子メールの配送に使われる SMTP などは当該プロトコルを使って通信を行っている。
UDP	User Datagram Protocol の略。 インターネットで標準的に利用されているプロトコルで、TCP と比較して簡易化されていることから信頼性が保証されていないプロトコルで、リアルタイム性や速度が求められる通信で用いられる。
VPN	仮想プライベート・ネットワーク（Virtual Private Network）。 インターネット上を利用しながら、仮想的にプライベート・ネットワーク（イントラネットのように外部に対して非公開であるネットワーク）を構築する技術。
責任分界点	情報システムに係る関係者間の責任の移行点。
ファームウェア	ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。パソコンや周辺機器、家電製品等に搭載されており、機器に内蔵された ROM やフラッシュメモリに記憶されている。
ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器。ファイアウォールには防火壁の意味があり、火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。
フォレンジック	インシデントが生じた場合に、原因究明に必要な機器やデータなどを収集・分析し、当該インシデントの事象の調査および証拠の取得を行う技術のこと。
振る舞い検知	アンチウイルスの一種で、検査対象のプログラムを仮想環境で実行したり、実際の環境で監視し、その振る舞いによってウイルスかどうか判断する方法。

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
2022 年 4/29,5/24, 5/27,6/8			給食事業者からの RDP ログオンによる操作発生（※１）	
9/29,10/4			給食事業者から TCP:139,445 宛の通信を確認したがファイアウォール Y により遮断（※１）	
10/12			給食事業者から TCP:3389 宛の通信を確認したがファイアウォール Y により遮断（※１）	
10/18			給食事業者から TCP:445 宛の通信を確認（※）	
10/31 3:45～			給食事業者からサーバーB に対するスキャン通信が発生	
4:08～			給食事業者からの病院のサーバーB に対して RDP 通信発生	
5:31				運用管理サーバーでランサムウェアを実行、永続化
5:45			病院配置の委託職員（以下、給食員）が電子カルテの使用できないこと確認	
5:49～				基幹サーバー2→１→３号機でランサムウェアを実行、永続化
5:50～		看護当直が電子カルテ障害や端末が動作しないことを確認 （重症システムは稼働中）		
6:05		システム担当職員等への連絡を指示		

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
6:20			給食員は電子カルテ入力ができたため、変更入力を実施	
6:30			給食員は他施設での送信不可情報を確認	
6:50		重症システム障害発生		
7:10		基幹システム障害発生		
7:45		ヘルプデスク職員出勤し障害確認。ランサムメッセージ確認		
7:51～				仮想マシンの停止
8:05～				NAS サーバーでランサムウェア実行、永続化
8:10～				仮想統合サーバでランサムウェアを実行、永続化
8:30		重症システムベンダーが調査し、ランサムウェア感染確認。遮断		
8:40		電子カルテベンダーが調査し、ランサムウェア感染確認。遮断		
8:50	幹部職員を招集。紙カルテ運用への診療体制変更を指示 ×救急、予定手術、通常外来等 △病棟、必要な外来 〇緊急手術			
9:23	大阪府救急・災害医療情報システムに「救急の受入すべて不可」の旨、入力。			
12:00	BCP 対策本部会議（第 1 回） 直近 1 週間の対応方針と紙カルテ運用への移行を確認			
17:00	ホームページに初報を掲載（通常診療の停止）			
17:00	職員向け説明会の開催			
20:00	記者会見（１回目）			
23:22	大阪府内の救急担当医向けに救			

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
	急受入、コロナ受入の停止の旨、案内			
11/1	BCP 対策本部会議（第 2 回） 外来開始方針、外来化学療法再開。また DACS の活用を開始			
	診療情報地域連携システム利用医療機関へ「データ閲覧利用不可」の案内			
	ホームページに第 2 報を掲載（復旧未定）			
11/2	BCP 対策本部会議（第 3 回） 11/4 から予定手術再開を決定、紙カルテ運用状況確認､DACS 参照センター（10 台）の設置決定	基幹システムのバックアップデータの確認完了		
	地域医師会（9 ヶ所）宛に「新患受入不可」の案内			
	ホームページに第 3 報を掲載（予定手術の一部再開）			
11/3	専門家チームから調査報告			
11/4	BCP 対策本部会議（第 4 回） 病院での情報共有方法、検査・手術などの対応可能件数を確認	参照環境用の構築開始		
	近隣病院（94 ヶ所）宛に「通常診療不可・転院受入等の協力要請」の案内	内部通信可視化のためのセキュリティ機器の設置		
	ホームページに第 4 報を掲載（予定手術の実施）			
	電子カルテシステムベンダーの役員来院し、復旧計画の合意			
	大阪府知事が来院し、現状および対応方針説明。支援の約束。			
	給食事業者が来院し、情報共有と外部広報の相談を受ける			
11/7	BCP 対策本部会議（第 5 回） 11/8 から DACS 参照センター運用開始確認	サーバーのクリーンインストール（～11/30）		
	電話回線を 10 回線追加			
	記者会見（2 回目）			
11/8	BCP 対策本部会議（第 6 回）			

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
	11/8 から DACS 参照センター運用開始確認			
11/9	ホームページに第 5 報を掲載（11/10 から電子カルテを参照可能に）			
	BCP 対策本部会議（第 7 回） 11/10 から電子カルテシステムの参照系システム（20 台）の運用開始および DACS 参照センターの拡充決定（追加 10 台）	端末シール貼り		
11/10	BCP 対策本部会議（第 8 回） 11/4 から内視鏡再開方針	参照環境用の運用開始		
	三次救急一部受入再開	基幹システム再構築開始		
	取扱事業者向け説明会を実施（75 社参加）			
11/11	BCP 対策本部会議（第 9 回） 11/11 から術前麻酔外来を再開			
11/14	BCP 対策本部会議（第 10 回） 12 月参集から基幹システム稼働を目指し、配置方針などを確認。 11/17 から救急外来（ER）を再開			
11/16	ホームページに第 6 報を掲載（11/10 から三次救急受入再開、17 から一般救急患者の受け入れ再開）			
	BCP 対策本部会議（第 11 回） 術前麻酔外来を再開			
11/17	二次救急、救急外来再開			
	病院及び府立機構内の他センター向けの情報共有・研修会開催			
11/18	BCP 対策本部会議（第 12 回） 外注検査の再開、11/22 から端末回収決定			
11/21	大阪府警察本部の供述調書に署名・押印			
11/22	登録医等近隣医療機関(約 1,180 箇所)へ、過去データの参照可能、12 月中旬の検査再開、1 月の通常診療再開の案内	端末回収開始 （～11/30）		
	BCP 対策本部会議（第 13 回）			

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
	画像系のセキュリティ確認完了			
11/25	BCP 対策本部会議（第 14 回） 11/28 画像参照センター運用開始、CT,MRI 検査予約受付開始			
11/30	BCP 対策本部会議（第 15 回） 端末の再配備日程の確定			
12/1	取材対応（高度救命救急センター長対応）			
	フォレンジック調査結果報告［給食サーバー］（A 社）			
12/5	自由民主党サイバーセキュリティ対策本部会議出席・説明			
12/7	BCP 対策本部会議（第 16 回） 12/12 から電子カルテ再開			
12/9		セキュリティポリシー変更案確定		
12/11		基幹システムの再構築完了		
12/12	地域医師会、近隣病院にシステムの一部復旧と初診患者、新入院患者の受入順次再開を案内	基幹システム（電子カルテ、オーダーリング、医事会計、看護支援など）、外来電子カルテ、部門システムの一部（調剤、検体検査、採血管、再来受付など）を運用再開		
	ホームページに第 7 報を掲載（12/12 から基幹システム再稼働）			
	取材対応（医療情報部部長対応）			
12/14		部門システムの一部再開（放射線部門、PACS など）		
	BCP 対策本部会議（第 17 回） 地域予約を再開、入院患者の電子カルテ運用を 12/22 再開			
12/19	給食事業者への接続医療機関訪問調査			
12/20		部門システムの一部再開（生理検査、輸血など）		
12/22	ホームページに第 8 報を掲載（通常外来診療の再開）			

対応時系列				
日時	医療	病院関連（システム）	給食関連	ログ
		病棟電子カルテシステム運用開始、部門システムの一部再開（手術部門、重症患者情報など）		
		給食システムの再開		
12/23	フォレンジック調査結果報告［全体（18 機のみ)］(B 社)			
12/27	BCP 対策本部会議（第 18 回） 救急受入完全復旧、手術オーダーの 1/4 の再開確認。	部門システムの一部再開（微生物、病理など）		
12/28	BCP 対策本部会議（第 19 回） 診療機能の復旧を確認、本会議の竜を宣言			
2023 年 1/4	外来当日会計再開			
1/10	ホームページに第 9 報を掲載（診療体制復旧宣言）			
1/11	地域医師会、登録医等近隣医療機関へ診療復旧を案内	部門システムの一部再開（周産期、リハビリなど）		
1/12	近隣病院に診療復旧を案内			
1/16	手術枠 100%再開			

【代表的なイベントのみ記載】

（※１）EventLog や設置しているファイアウォールＹなどのログなどから検知や対処を行っているが、給食事業者としては当該経路を用いて、リモートアクセス等は行っていない旨の報告を受けており、対象の通信が正常または異常の判断ができない。