徳島県つるぎ町立半田病院
コンピュータウイルス感染事案
有識者会議調査報告書

2022 年 6 月 7 日

有識者会議調査報告書によせて

令和 3 年 10 月末、徳島県の西部山間部に位置するつるぎ町の町立半田病院がサイバー攻撃を受け、具体的にはランサムウェアに感染し、電子カルテ等、病院内のデータが暗号化され、利用不能になり、その後 2 か月間に及んで、治療行為を含む正常な病院業務が滞ったことは大きく国内はもとより、海外の新聞やテレビに取り上げられ、社会的な問題になったことは周知の事実です。その後、病院側では、災害時に発動する重大インシデントへの対応である「事業継続計画」に基づいて病院業務の継続に努めました。この緊急対応については称賛の声が聞かれたものの、完全復旧に時間がかかったことも事実です。なぜ、このような事態に陥ったのでしょうか。つるぎ町立半田病院だけが特別なのでしょうか。サイバー攻撃を防ぐことはできなかったのでしょうか。

情報システムは進化の一途をたどり、それは病院内の情報システムも同様です。その利用の恩恵に与かる以上に情報システムは高度化、複雑化し、それに合わせて「脆弱性」と呼ばれるシステム上の弱点も顕わになっています。サイバー攻撃はそれに呼応するがごとく高度化し、小さな「脆弱性」も見逃すことなく執拗な攻撃が昼夜を分かたず世界中から行われている現状なのです。もはや小さな組織や個人だから狙われない、ましてや地方の病院だから狙われないということではないのです。さらにサイバー攻撃の高度化は、「ウイルス（マルウェア）対策ソフトを入れているから安全」というような十年以上前の状況でもありません。

つるぎ町立半田病院では病院業務が復旧した令和 4 年 1 月から今回のインシデントの原因追求とこれからの対策を講ずるために有識者委員会の立ち上げを計画し、翌月から正式な活動を開始しました。本委員会の目的は、今後このようなサイバー攻撃を防ぎ、かつサイバー攻撃に遭ったとしても堅固な情報システムの構築を目指すだけでなく、全国各地の病院、さらには組織、企業が有する問題点を明らかにし、サイバー攻撃に耐性のある情報システムの構築、そして組織作りについて一つの指針を与えるものです。今後の、特に地方における組織のサイバーセキュリティ対策への一助となれば幸いです。

最期に病院内のシステムに対する調査だけでなく、広くサイバー攻撃への対策、一般的に導入されている情報システムに対する問題点の洗い出し等、強力に支援いただいた一般社団法人ソフトウェア協会の関係者の方々に謝意を表します。

つるぎ町立半田病院コンピュータウイルス感染事案有識者会議会長
神戸大学大学院工学研究科教授　森井　昌克

目次

1　**はじめに** ～サイバー攻撃事案に対応して～

令和３年 10 月 31 日の未明、つるぎ町立半田病院がサイバー攻撃を受け、電子カルテをはじめとする院内システムがランサムウェアと呼ばれる身代金要求型コンピュータウイルスに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。令和４年１月４日の通常診療再開までの間、患者さんをはじめ関係者の皆さまには多大なご迷惑とご心配をおかけいたしましたこと、改めて深くお詫び申し上げます。

当院においては、事件発生後、全国の病院や事業所が当院のようなサイバー攻撃を受けないためにもきちんと情報を公表することが責任であると考え、できうる限りの情報を公開してきました。その結果、あらゆるマスコミや業界誌当からの取材依頼があり、逆に様々な情報提供がありました。この状況は今も続いていますし、今後も積極的な情報提供に努めてまいります。

なぜ、当院がコンピュータウイルスに感染したかについては、今も警察当局においての捜査が続けられています。病院としては、有識者会議を設置いたしました。大学教授などの専門家に委員にご就任いただき、会議の開催と現地調査を経て、当院に対するサイバー攻撃に関し、その原因分析や被害状況の実態把握、再発防止策など病院運営に関する重要事項について審議いただき、調査報告書としてその提言をまとめていただきました。今後におきましては、本提言を踏まえ国の新たな指針も参考にしながらの再発防止と、セキュリティ対策強化を図る所存でございます。

事件発生後、当院の職員は一丸となって早期復旧を目指しました。患者さんには大変なご迷惑をおかけしていた中、現場では非常に厳しいお叱りのご意見を受けたこともあります。しかし、大半の方からは、必死になって対応する職員に対し、温かな励ましのお言葉をいただきました。このことは、今後も病院の運営にあたる職員の大きな心のよりどころになるものだと確信しています。12 月上旬に届いた県外の方からのお手紙を一例として紹介します。「このたびの災難に対し、心からお見舞い申し上げます。地域にお住まいの方々にとって、半田病院は本当に大切な病院です。多くの方が癒され、新しい生命が誕生してきた半田病院が理不尽な目にあい、憤りと悲しみでいっぱいです。何の力にもなりませんが応援しています。どうか皆さま、お体に気を付けて乗り越えてくださいますように、また、日常が早く戻りますようにお祈り申し上げます。」ほかにも、個人の方や病院関係者の皆さまから様々なお言葉をいただきました。本当にありがとうございました。

今後も、地域の中核病院の責務を果たすべく、財政の健全化と地域と共に歩む病院経営を目指して職員一丸となって対応してまいります。引き続きのご支援をどうぞよろしくお願い申し上げます。

令和４年６月
つるぎ町病院事業管理者
須藤　泰史

2　有識者会議について

2.1 設立の趣旨

　つるぎ町立半田病院（以下、「半田病院」という。）では今回のインシデントを受けて、外部の有識者による会議を設置し、本インシデントの課題の洗い出しや再発防止策の検討などを実施した。当該会議の規則は以下の通りとする。

つるぎ町立半田病院コンピュータウイルス感染事案有識者会議規則
令和４年１月１４日施行
（設　置）
第１条　つるぎ町立半田病院に、コンピュータウイルス感染事案有識者会議（以下「会議」という。）を置く。
（目　的）
第２条　会議は、令和３年１０月３１日に発生した事案に対し、その原因分析、被害状況の実態把握、再発防止策等など病院運営に関する重要事項について審議し、病院事業管理者（以下「管理者」という。）に提言する。
（構　成）
第３条　会議の構成は、次のとおりとする。
会長　１名　・　副会長　１名　・　委員　若干名
２　委員には次の職種から管理者が選出する。
外部学識経験者、国・県・町の職員
３　会長は、委員の互選により定める。
（任　期）
第４条　委員の任期は１年とする。但し、再任を妨げない。
２　補欠による委員の任期は、前任者の残任期間とする。
（会長）
第５条　会長は会議を統轄し、審議事項を決済する。会長に事故があるとき、副会長がその職務を代理する。
（会議の招集）
第６条　会議は病院長が招集し、会長がその議長となる。
２　会議は、必要に応じて開催するものとする。
（関係者の出席）
第７条　病院長、会長は、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事ができる。
（庶務）
第８条　会議の庶務は、総務課において処理するものとする。
　　付　則
この規則は、令和４年１月１４日から施行する。

2.2 委員会の構成

2.1 の会議規則に則り、以下の通り有識者を招聘した。

【つるぎ町立半田病院コンピュータウイルス感染事案有識者会議】

職名	氏名	所属
会　長	森井　昌克	神戸大学大学院工学研究科教授
副会長	上田　哲史	徳島大学情報センター教授
委　員	板東　直樹	一般社団法人ソフトウェア協会理事 同　Software ISAC 共同代表
委　員	廣瀬　和久・金丸　武史	徳島県保健福祉部医療政策課長 （※人事異動に伴う変更）
委　員	古城　忠美	つるぎ町副町長

なお、本会議を円滑に進行し、組織的、技術的なセキュリティの観点からも、さらに専門家を以下の通り招聘しました。当該調査については Software ISAC のサイバーボランティア制度による現地調査委員を招聘し、インシデントの課題や再発防止策の深化に努めた。

【つるぎ町立半田病院コンピュータウイルス感染事案現地調査委員会】

氏名	所属
板東　直樹	一般社団法人ソフトウェア協会 理事／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
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／ 株式会社ラック サイバー・グリッド・ジャパン主席研究員
萩原　健太	一般社団法人ソフトウェア協会 理事／Software ISAC 共同代表／ グローバルセキュリティエキスパート株式会社　最高セキュリティ責任者

【有識者会議開催者】

つるぎ町病院事業管理者　須藤　泰史

【有識者会議事務局】

つるぎ町立半田病院

病院長	中園　雅彦
事務長	丸笹　寿也
総務課長	猪岡　恭治
システム管理課長	山本　高也

総務課長補佐　　加藤　育典
医事課長補佐　　折目　慎一
医事課係長　　小林　圭一
職員労働組合代表

2.3 開催概要

令和４年２月から５月に至るまで、４回の有識者会議を開催し、また現地調査も複数回実施し、本調査報告書のとりまとめを行った。

【有識者会議および現地調査】

開催回	開催日時	概要
第１回	令和４年２月４日（金） 16 時 30 分～18 時 10 分	・病院側から経緯報告 ・会議規則について ・会長、副会長の選任について
第２回	令和４年２月 28 日（月） 16 時 30 分～18 時 20 分	・病院側から新セキュリティ対策と報告書についての説明 ・委員および調査事務局からの提言
現地調査 （第１回）	令和４年３月 12 日（土） 12 時 00 分～18 時 30 分	有識者会議・調査事務局による現地調査 （半田病院の体制全般とシステム内容等の確認）
現地調査 （第２回）	令和４年３月 13 日（日） 10 時 00 分～17 時 00 分	有識者会議・調査事務局による現地調査 （各種ヒヤリングを主に実施）
第３回	令和４年３月 28 日（月） 16 時 30 分～18 時 30 分	・現地調査結果の報告 ・委員および調査事務局からの提言
現地調査 （第３回）	令和４年３月 29 日（火） 9 時 00 分～14 時 00 分	調査事務局による現地調査 （半田病院の体制全般とシステム内容等の確認継続）
第 3.5 回 Web 開催	令和４年４月 27 日（火） 17 時 00 分～19 時 30 分	現地調査の結果と調査報告書についての協議
第４回事前 打ち合わせ	令和４年５月 12 日（木） 17 時 00 分～19 時 30 分	調査報告書についての協議
第４回	令和４年５月 20 日（金） 16 時 30 分～19 時 00 分	・調査報告書についての協議 ・今後の対応に関する協議

なお、有識者会議開催にあたり事務局会議や院内医療情報システムの安全管理委員会などを以下の通り開催した。

【事務局会議】

- 令和４年２月９日（水）15 時 00 分～17 時 00 分
- 令和４年２月 17 日（木）15 時 00 分～16 時 00 分
- 令和４年４月 13 日（水）17 時 00 分～17 時 40 分

【院内医療情報システムの安全管理委員会】

医療情報システムの安全管理に関するガイドライン 5.2 版についても内容確認と対応に関する協議を行った。

<院内医療情報システムの安全管理委員会>

- 令和４年４月 13 日（水）16 時 00 分～17 時 00 分
- 令和４年４月 27 日（水）16 時 00 分～17 時 00 分
- 令和４年５月 25 日（水）16 時 00 分～18 時 00 分

<院内電子カルテシステム委員会>

- 令和４年４月 21 日（木）16 時 00 分～17 時 30 分
- 令和４年５月 17 日（火）16 時 00 分～17 時 30 分

3　今回の災害級の重大インシデントについて

本章から半田病院および関係者から提出のあった資料やヒヤリング内容などに基づき、有識者会議および調査委員会での本インシデントの振り返りや課題、今後の対応の提言等についてまとめる。

3.1 事案概要

令和 3 年 10 月 31 日未明、病院内に設置されていた複数台のプリンタが、一斉に犯行声明を印字し始めたことでインシデントが発覚した。Lockbit2.0 によるランサムウェア（身代金要求型ウイルス）に感染し、患者の診察記録を預かる電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用できない甚大な被害が生じた。侵入経路としては導入している仮想プライベートネットワーク（Virtual Private Network、以下、「VPN」という。）装置の脆弱性を悪用して侵入したものと思われる。ランサムウェア感染の確認後は、ネットワークの遮断や端末の停止などを行い、一時、救急や新規患者の受け入れを中止し、手術も可能な限り延期にするなど、病院としての機能は事実上、停止する状態に陥った。

なお、半田病院は、事前に主に地震災害用に定めていた事業継続計画（Business Continuity Plan、以下「BCP」という。）を発動し、発生当初から災害級の取り扱いでインシデント対応にあたった。また迅速に徳島県警察本部に相談し、被害届が受理され、関係するベンターや公的機関にも連絡や連携を行った。しかしながら、電子カルテを導入・保守している事業者や、関連のシステムやセキュリティ製品を導入・保守している事業者、フォレンジックを請け負った事業者も、インシデント対応に秀でているわけではないため、事業者側の対応に対する不誠実さが生じていたのも事実である。

全容解明や情報漏えい有無の特定よりも、病院としての機能を一日も早く取り戻すために、患者のデータをいかに復元させるか、端末を利用できる状況に戻すかに焦点を当てインシデント対応を行っていた。幸いにして、フォレンジックを請け負った事業者が、（データを確認できる範囲で）元の通り復元をすることができたと考えられる。その後、端末の初期化対応を行い、端末を再利用したり、システムやネットワークを最低限見直したりした上で、令和 4 年 1 月 4 日の通常診療の再開にこぎつけることができた。

3.2 事案対応の姿勢

インシデントが発生した令和 3 年 10 月 31 日は、半田病院は地域の救急当番医であったが、電子カルテをはじめ各システムが稼働しないため、当直看護師がシステム担当者に連絡。ランサムウェアによるサイバー攻撃で電子カルテシステムの復旧が難しいとの報告をうけた当直医が、救急受け入れの不可も判断し、関係各位に連絡をした。同日午前 8 時過ぎには病院幹部職員も参集し災害相当と判断。10 時に災害対策本部を設置、BCP に基づく対応を行った。「災害」と判断したことが功を奏し、会議においても診療継続に向けた解決策や回避策の検討など、各部署の担当者が現場の状況を確認し合い、情報共有と連携を図ることができていた。

また、各種システムの停止により医療提供が制限されたため、最初に病院事業継続のための基本方針を以下の通り定めた。

① 今いる入院患者を守る

② 外来患者は基本的に予約患者のみ
③ 電子カルテ復旧に努める
④ 皆で助け合って乗り切ろう！

上記 4 つの基本方針に加え、攻撃者からの身代金要求に対する方針も固め、データが完全に復旧する保証はないことや、警察からの指導、さらに病院開設者のつるぎ町長から、犯人側への資金提供を行うことが、自治体の姿勢として理解を得られないことなどから、身代金を支払わない方針を定めていた。なお、犯人側との交渉や身代金の請求についても確認できる限りでは、プリンタから出力された暗号化を示す脅迫のみで、昨今の脅威とも言われる「二重脅迫」といったランサムウェア特有の攻撃者の行動は見受けられなかった。

さらに、半田病院はインシデント発生当日に記者会見を行い、病院としての説明や現状を迅速に公表している。また、病院の方針を決定した令和 3 年 11 月 29 日にも記者会見を開催し、継続的に情報公開や説明を行っている。一般的にインシデント情報は隠す傾向があるが、国内外を含み新聞やテレビ、専門誌などからの取材にはできる限り対応を行い、他病院や事業所が同様の被害にあわないよう、積極的に情報公開と提供を行っている。

3.3 事案対応の経緯

本項ではインシデントが発生した令和 3 年 10 月 31 日から診療再開の令和 4 年 1 月 4 日までの経緯をまとめる。なお、全ての活動は記載しきれないため、代表的な対応を記録から抜粋するものである。

No	月日	時間	概要
1	令和 3 年 10 月 31 日	未明	院内にある複数のプリンタから、データを窃取および暗号化した内容の文書の大量印刷を確認。
2		0 時 30 分	電子カルテの不具合確認。システム担当者に通報。
3		3 時 00 分	システム担当者到着後、即座に電子カルテのネットワークを遮断。
4		8 時 00 分	ランサムウェアの感染確認。
5		8 時 55 分	徳島県警察本部へ相談。被害届として受理される。
6		9 時 00 分 ～9 時 42 分	救急受入不可対応の連絡・連携。
7		10 時 00 分	災害対策本部を正式発足。医療提供状況の確認と各種連携の確認を行う。（BCP に基づき、紙ベースでの医療提供の実施など）
8		10 時 46 分	開設者であるつるぎ町長へ現状報告。
9		11 時 27 分	徳島県警察本部専門部門担当来院。状況説明。
10		12 時 02 分	災害対策本部会議の実施。2 時間での確認内容や連係状況等の確認、継続対応の指示。（CT、MRI などの機器もコンピュータウイルス混入の恐れがあるため使用停止を行うなど）

11		14 時 00 分	災害対策本部会議の実施。約 2 時間での確認内容や連係状況等の確認、継続対応の指示。（新患を受け入れない方針や他院からの受け入れ中止を決定。医療事務を行う端末などでもウイルス感染も確認。外来会計もできない状態になる。） 記者会見開催の決定。
12		15 時 45 分	災害対策本部会議の実施。約 2 時間での確認内容や連係状況等の確認、記者会見に向けた準備や確認。
13		15 時 55 分	徳島県医療政策課へ現状報告。
14		16 時 00 分	記者会見の実施。
15		17 時 30 分	徳島県危機管理課へ現状報告。
16		18 時 00 分	災害対策本部会議の実施。基本方針の決定と共有。メディア掲載による問い合わせ増加に関する連携体制の確認と整備。 病院 HP の掲載を進める。また、つるぎ町総務課へ町内放送での告知を依頼。
17		20 時 15 分	バックアップサーバーや医事サーバーがダウンしていることを確認。
18	11 月 1 日	10 時 00 分	災害対策本部会議の実施（医師会への連絡と医師会から各病院への展開などの連携確認など）※以降、記載は割愛するが一日 2～3 回の頻度で開催されている。
19		10 時 50 分	独立行政法人情報処理推進機構（以下、「IPA」という。）へ連絡。 →ウイルス感染に関する受付窓口のお知らせや、ウイルス対策ソフト利用に関する助言を受ける。
20		11 時 20 分 ～11 時 45 分	徳島県医療政策課よりリエゾン 2 名来院。 （人的・物的不足に関する調査）
21			ウイルス対策ソフトのワクチンを用いた対応を試みる。 ネットワークを介しない印刷対応実施確認。 入院患者一覧表の作成やコピー機の設置などを行う。 患者受け入れ方針の変更点確認　など
22	11 月 2 日	9 時 00 分	別回線の有線のインターネット回線を大元から遮断。
23		11 時 00 分	フリーWi-Fi の対応検討。 （Web 面会や院外とのやり取りができなくなってしまうため、パスワードの設定変更など、対応や調査を開始）
24			システムベンダー（以下、「A 社」という。）と電子カルテ復旧に向けた協議の実施。 古い行政端末（OS：Windows7）を各部署に配布し対応。 つるぎ町保健センターより、新型コロナワクチンの接種業務に関する支援申し出あり。

25	11 月 3 日	1 時 30 分	一部の環境でローカルネットワークを構築。
26		15 時 00 分	FortiGate（Fortinet 社）の VPN のファームウェアのアップデートを実施。 → VPN のログ確認や保全、保存などは未確認。
27		16 時 00 分	A 社紹介の修復会社（以下、B社という。）との調査と復旧に関する打ち合わせをオンライン会議にて実施。以下の方針を確認。 サーバー系統（約 15 台）、部門システムサーバー（台数不明）をB社（東京）に郵送し、調査復旧を試みる。 クライアント端末（200 台）は、ネットワークに接続し、ウイルススキャンを行い、駆除対応を行う。
28	11 月 4 日		徳島県政策創造部地方創生局デジタルとくしま推進課を通して、総務省自治行政局デジタル基盤推進課および内閣サイバーセキュリティセンターにインシデントの報告。
29		10 時 40 分	B社と検討した対応を徳島県警察本部に報告。対応を了承。
30		10 時 55 分	つるぎ町長へ報告。B社と検討した対応を了承。
31		12 時 00 分	救急当番の変更をホウエツ病院に依頼。了承が得られたため、医師会・消防等の関係機関に連絡。 県医療政策課より、災害として DMAT 派遣可能な旨の回答。
32		16 時 00 分	検査機器のウイルスチェックの実施。
33		17 時 00 分	端末での診療記録対応可能にする。（ワープロとしての利用にとどめる。）また、新規 USB の利用も許可する。
34		17 時 30 分	B社およびA社と打ち合わせを実施。全部で 41 台の端末やサーバーの発送を決定。エンジニアの派遣要請を行う。（→B社で検討も応じず。）
35		20 時 15 分	端末・サーバーリストの作成を行い、B社に送付。
36	11 月 5 日	11 時 00 分	県立三好病院へ災害ロジスティックス専門家の派遣依頼（本部活動支援）。6 日までの 2 日間活動。
37		13 時 38 分	端末・サーバーの梱包作業を開始。
38		13 時 40 分	徳島県医療政策課との打ち合わせを実施。 （金銭的、人的、物的資源などの支援要求。）
39		15 時 40 分	端末・サーバーの発送完了。
40		19 時 00 分	PC（ワープロ用）・プリンタの一部追加設置。
41			電子カルテ事業者である電子カルテベンダー（以下、「C 社」という。）が来社。
42	11 月 6 日	11 時 00 分	端末のウイルススキャンによる感染洗い出し作業の実施。
43		14 時 15 分	端末・サーバーがB社に到着。
44		23 時 00 分	システム復旧の優先順位の確認。 （医事会計関連→電カル関連→ファイルサーバー）

45	11 月 7 日	15 時 15 分	PC（ワープロ用）の一部追加設置を行う。
46	11 月 8 日	11 時 00 分	フリーWi-Fi のパスワード化を進める。
47		14 時 30 分	Ｂ社と直接協議を行う。 VPN を突破された可能性の指摘を受ける。 次の対応内容を確認。 →11 月 13 日までに約 3 分の 1 の端末やサーバーを初期化し返却。11 月中に使用可能な端末と不可の端末に分けて初期化の実施予定であることを確認。 全端末へのウイルス対策ソフトの導入決定
48		17 時 30 分	PC（ワープロ用）の一部追加設置。
49		19 時 20 分	Ｂ社と協議を行う。サーバー調査に関する打ち合わせ。
50	11 月 9 日		四国厚生支局徳島事務所員との報告と事務協議。
51		17 時 20 分	感染の確認された端末の回収。
52	11 月 10 日	16 時 10 分	感染の確認されなかった端末を含め端末の全回収。
53	11 月 11 日	8 時 30 分	回収した端末の感染状況の確認作業の開始。
54		13 時 00 分	フリーWi-Fi のパスワード対応のための使用停止。
55		18 時 00 分	フリーWi-Fi の再開。
56			医事過去分のデータ入力に関する対応や動作の確認を C 社と実施。
57	11 月 12 日		半田病院側でファストフォレンジック作業を実施も動作せず。 Ｂ社に追加の端末（6 台）を発送。 半田病院側でファストフォレンジック作業の開始（Lockbit によるデータ暗号化状況等の確認）
58	11 月 13 日		ファストフォレンジック作業の継続。 ウイルス対策ソフトによる端末のウイルス確認。
59	11 月 14 日		ファストフォレンジック作業の継続。 ウイルス対策ソフトによる端末のウイルス確認継続。 フォレンジック事業者の調査にて感染なしと確認された端末から、ウイルスが内在していることを確認。 Ｂ社と協議を行い、対応難航により 11 月 16 日の一部サーバーの返却を確認。
60	11 月 15 日		ファストフォレンジック作業の継続。 ウイルス対策ソフトによる端末のウイルス確認継続。 医療機器の一部でウイルスチェックができないため、医療機器提供事業者からハードウェアの交換要求。 Ｂ社と協議。 小児科の通常診療再開。
61	11 月 16 日		ファストフォレンジック作業の継続。

			ウイルス対策ソフトによる端末のウイルス確認継続。 追加の感染端末の梱包作業の実施。 Ｂ社と協議し、11 月 16 日返却不可の連絡あり。
62	11 月 17 日		ファストフォレンジック作業の継続。 ウイルス対策ソフトによる端末のウイルス確認継続。 Ｂ社と修復進捗に関する Web 協議。Windows7 などの古い OS などは感染なしとの報告を受ける。
63	11 月 18 日		全部署のモダリティチェックが完了。一部で過去のデータ確認。 A 社と打ち合わせを実施。一部、ファストフォレンジック作業に対する説明不備があったことを確認。
64	11 月 19 日		一部の端末でファストフォレンジックを再実施。 Ｂ社より暗号化されていたデータの一部が復元されたサンプルデータが送付される。（復元できる状況になったことの確認。） 電子カルテの再開目標をサーバーの返却目処や電カルのサーバー調整や導入などを鑑みて、22 年 1 月 4 日に設定。 産婦人科において新規の妊産婦の受け入れを再開。
65	11 月 22 日		一部の端末でファストフォレンジックを再実施。 身代金要求が行われていないが、支払わない方針を正式決定。 C 社、A 社と Web 協議（クラウドシステムは利用せずに仮復旧を行う旨の打ち合わせを実施。C 社に提案や対応の遅れに対するクレームを入れる。）
66	11 月 23 日		一部の端末でファストフォレンジックを再実施。
67	11 月 24 日		NTT にリモート回線の追加発注。
68	11 月 25 日		医療機器のハードウェア交換の 12 月中実施を指示。 健診開始に向けた環境整備開始。
69	11 月 26 日	17 時 30 分	現状と診療再開に向けての記者会見の実施。 診療方針の変更を行い、拡大する方針へ。
70			追加で感染確認された 42 台の端末をＢ社へ発送。 ホームページのお知らせを変更する。
71	11 月 27 日		追加で感染が確認された 12 台の端末とサーバーをＢ社へ発送。
72	11 月 30 日		感染端末のフォーマットの継続実施。 サーバー3 台がＢ社から返却される。
73	12 月 1 日		感染端末のフォーマットの継続実施。 C 社から 12 月 20 日にレンタルサーバー納品できるよう対応を確認する。また、追加でサーバー2 台（医事サーバーなど）がＢ社から返却される。
74	12 月 2 日		感染端末のフォーマットの継続実施。 返却されたサーバーの確認。

75	12 月 3 日		感染端末のフォーマットの継続実施。 返却されたサーバーの確認。 サーバーと端末の 1 台ずつがＢ社から返却される。 電子カルテの復旧対応について、C 社と「レンタルサーバー」か「従来サーバー」への移行か検討を行う。
76	12 月 4 日		感染端末のフォーマットの終了。 AD サーバーと端末が不具合にて、再度Ｂ社へ発送。さらに、Ｂ社にて修復された端末で修復漏れを確認。
77	12 月 6 日		サーバーが複数台Ｂ社から返却される。しかし、Ｂ社にて修復された端末で修復漏れを確認。 さらに、サーバー 9 台がＢ社から返却される。 C 社と電子カルテ再開に向けた院内向け説明会開催の実施を決定。 外来にて季節性インフルエンザの予防接種。大勢の方が来院し大混乱。
78	12 月 8 日		サーバー動作確認の継続。 サーバー 1 台が、復元不完全の状態でＢ社から返却される。
79	12 月 10 日		AD サーバーが返却され、クライアント PC との連携確認。
80	12 月 11 日		医事サーバーと AD サーバーの連携確認。 ウイルス対策ソフトがインストールされていない端末へのインストール作業を行う。 サーバー3 台がＢ社から返却される。
81	12 月 13 日		ウイルス対策ソフトがインストールされていない端末へのインストール作業を行う。 サーバー3 台、端末 8 台がＢ社から返却される。
82	12 月 14 日		ウイルス対策ソフトがインストールされていない端末へのインストール作業を行う。 C 社による電子カルテ再開に向けた院内向け説明会の開催。 Ｂ社の「ファストフォレンジック解析結果レポート（以下、「FF レポート」という。）」より、7 台の端末で不正アクセスの痕跡を確認。 一部端末を A 社に発送し、OS の入れ替え依頼の実施。
83	12 月 15 日		サーバー3 台がＢ社から返却される。 一部のサーバーで破損を確認し、配送業者と協議を行う。
84	12 月 16 日		サーバー 7 台（画像（2 台）、透析、健診、内視鏡、検査、薬剤）と端末 2 台がＢ社から返却される。 サーバー（AD、医事、ファイル）のウイルス対策ソフト更新作業の完了。

85	12 月 17 日		サーバー（透析、薬剤）のウイルス対策ソフト更新作業の完了。 画像、薬剤サーバーの確認。
86	12 月 18 日		各種サーバーの動作確認の継続。 電子カルテデータベースの起動確認ができず、連携サーバーと光ケーブルをＢ社へ発送。
87	12 月 20 日		C 社、A 社と打ち合わせ。バックアップサーバーのデータが 2018 年以降物理的に削除されていることを確認。 サーバーと端末 11 台がＢ社から返却される。
88	12 月 21 日		感染した端末全体の初期化、OS や各種ソフトウェアのセッティングが完了。
89	12 月 24 日		各種端末の設定作業の継続実施。 サーバー 1 台がＢ社から返却される。
90	12 月 25 日		各種端末の設定作業の継続実施。 電子カルテ DB サーバーがＢ社から返却される。 DB サーバーの基盤損傷の可能性があり、部品発注。
91	12 月 26 日		各種端末の設定作業の継続実施。 レンタルサーバー設定の完了。
92	12 月 27 日		各種端末の設定作業の継続実施。 全サーバーがＢ社から返却され、返却分の継続確認。
93	12 月 28 日		病院仕事納め式。 C 社より、電子カルテ再開に向けた院内向け説明会の開催。 電子カルテシステムの最終確認を行い、レンタルサーバー案か、従来のサーバー案かを決定。
94	12 月 29 日		電子カルテシステムのデータ復元を確認。 従来のサーバー利用案と破損したものはレンタルサーバーを利用するハイブリッドでの電子カルテシステムの再稼働を決定。 対応していた端末の半分を配布。
95	12 月 30 日 ～2022 年 1 月 3 日		各種端末やサーバーの設定対応継続。 残りの端末の配布。 データの移行作業。
96	1 月 4 日		電子カルテシステム再稼働し通常診療を再開。 （以降も各種不備、不具合は継続対応。）

病院として迅速に災害認定を行い、BCP に基づく行動ができたことは、インシデント病院機能の維持に向けた活動が行えている。しかし、サイバーセキュリティに対する知識や経験不足から、初動対応に戸惑いや遅れが生じていることは否定できない。また関係するいずれの事業者もサイバーセキュリティに関する知識や経験も浅く、封じ込めや復旧対応など、ちぐはぐな対応が行われていた。

しかし、半田病院はインシデント対応に不慣れな中も、記者会見や取材依頼にも誠実に対応し、地域医療の維持、そしてなにより患者を守るための活動に終始務めていた。その危機感が各事業者もより認識し、対

応や連携が行われていれば、約 2 か月強の時間をかけずとも対応できたと考える。またインシデント対応を行う専門家が不在であったため、終始インシデント対応に苦慮している。半田病院のエンジニア派遣要請に各事業者が応じ、現地で対応を協力していればインシデント対応はより迅速に行われたものと考える。

3.4 事案調査内容

3.4.1 前提情報

電子カルテとは紙ベースのカルテを電子化したものだが、実際には単純なシステムではない。厚生労働省は、「標準的電子カルテ推進委員会」の中で電子カルテについて、医事会計システムやオンラインで繋がる検査や処方箋のシステムの中心となり、患者さんの症状や治療経過の診療情報を保存し更新させ、この記録の検討と分析をするものであると説明している。

具体的には、会計システム、オーダリングシステム、診療情報システムなどをオンラインで連携させ、これらを患者情報として電子カルテに記録しているものである。

半田病院は、1998 年にオーダリングシステム、2011 年に電子カルテシステムを導入しており、2018 年にシステムの更新を行っている。図 1 に示す通りのシステム構成である。なお、山本システムと呼ばれる電子カルテシステムの不足部分を補うサブシステムを構築し運用しているところが特徴となっている。

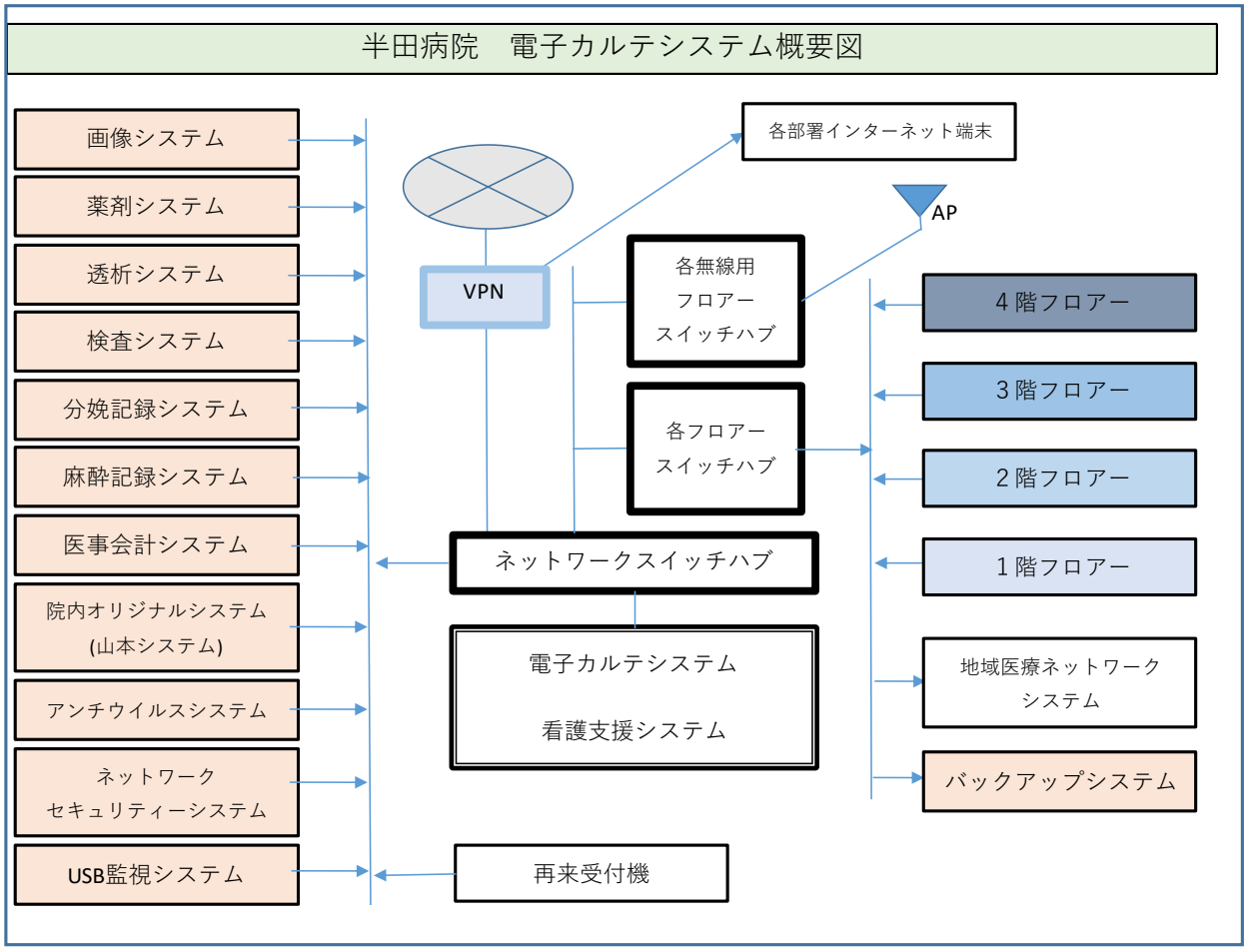

図 1　電子カルテシステム概要図

3.4.2　調査方法

まず調査を行ったタイミングでは、端末やサーバーの初期化や各種アップデートが行われ、これまでの端末を活用したシステム復旧が行われていたため、有識者会議は基本的にはヒヤリングや各事業者の対応、半田病院の記録確認を中心とした実地調査となった。そのため、インシデントに関係する各種ログを直接的に確認することはできず、あくまでも病院側から提出が可能な資料と、ヒヤリングを行ったのが基本的な調査方法である。

以下に、直接または間接的に確認できた情報またはヒヤリングや各種資料から確認できた情報を、調査の視点も含めながら整理する。

まず 1 つ目は今回のサイバー攻撃の侵入経路や水平展開など、攻撃プロセスを把握するための調査である。調査の視点としては以下の通りである。

① Windows、Active Directory[1]、システム関連の設定値及び各種ログの調査
② その他、導入している機器のログ調査
③ VPN 装置のログの調査
④ その他、導入しているセキュリティ製品の調査　など

上記は、システムを導入している A 社や、インシデント調査や復旧を行ったＢ社が実施すべきではあるが、調査は基本的にファストフォレンジックツールなどのツールを使用するのみであって、関連する詳細調査が行われていない。また、システムや端末を初期化していること、VPN 装置などはファームのアップデートなどを、ログ保存を行わずに実施していることから、ログの調査を実施することはできなかった。

２点目はインシデント対応の流れや対応が的確であったかを確認するための調査である。調査の視点としては以下の通りである。

① 保管しているインシデント対応の議事録やタイムラインなどの確認
② Ｂ社によるファストフォレンジック結果および復旧方法の確認
③ 有識者による関係者へのヒヤリング調査

災害対策本部が設置され、経時活動記録（クロノロジー）が作成されており、インシデント対応を時系列に追うことは比較的容易であった。しかしながら、一部の端末やサーバーはＢ社に送付し、フォレンジックの作業が行われているようだが、Ｂ社提出の調査報告書の内容が希薄なため、その全容を解明することはできなかった。また情報漏洩の有無の視点での調査対応が不足していることから、本事象は情報漏洩の可能性までしか示唆することができない。

3 点目は再発防止策の検討に向けた調査を行った時点での設定状況や体制の確認を現地の調査やヒヤリングにて実施した。主な確認は以下のとおりである。

---

[1] Microsoft が提供している Windows Server の統合管理機能、ユーザー認証やセキュリティ設定を制御する機能が搭載されている。

① 既存のシステム環境における Windows、Active Directory のポリシーや設定などの確認
② 導入しているセキュリティ製品のポリシーや設定などの確認
③ 導入している製品やサービスの評価
④ システム及びセキュリティの対応や運用体制の確認
⑤ 現在の各種契約に関する確認　など

これらの項目は現地調査にて確認できる範囲でシステムや端末などを確認し、対応を行った。詳細については報告書の「技術編」にて記述する。

3.4.3 調査結果

3.4.3.1 初期侵入

MITRE[2] の ATT&CK[3] に示されるようにサイバー攻撃の初期侵入は様々あるが、電子カルテシステムや医事会計システムでは電子メールそのものを使用しておらず、フィッシングメールによる初期侵入は考え難い。また Web 閲覧は異なるネットワークセグメントの PC で実施し、セグメント間の通信も許可されていなかった。さらには、外部に公開されたリモートデスクトップ接続（以下、「RDP」という。）等は存在していないため、公開 RDP 経由の侵入も不可能であった。その他にも内部協力者がいた事実や、侵害されたソフトウェアのインストールや新規に展開したソフトウェアもなく、ソフトウェアサプライチェーンの侵害も考えにくい。このように様々な侵入方法を検討していくと、電子カルテを始めとした医療機器のメンテンナンス等を行う際に接続する VPN のみが侵入経路と考えられ、当該ネットワークにおいて VPN 装置の脆弱性が放置されていた事実、また脆弱性を使い取得された VPN 装置の管理者の資格情報がダークウェブで公開されていた事実[4]を鑑みると、VPN 装置の脆弱性を悪用した侵入が考えられ、当該ネットワークを悪用して侵入した可能性が極めて高い。

なお、Fortinet 社製のネットワーク（VPN）装置は、導入当初からソフトウェアの更新が行われておらず、2021 年の夏に日本国内でも話題になった「CVE-2018-13379」が放置された状態であり、当該脆弱性を悪用して侵入した可能性が高い。本侵入経路を証明するために VPN 装置等のログの分析を試みたが、インシデント発生後に A 社によってファームウェアの更新などの作業を、ログ保存などを鑑みずに実施されていたため調査を実施することができなかった。

さらに、本脆弱性は Fortinet 社が 2019 年から 2021 年 6 月までに「4 度にわたり注意喚起を行ってきた」としているが、利用者自身が本情報を収集できずに認知できていなかった体制にも課題があるにせよ、本脆弱性の説明が利用者に行き届いていないことや、本情報を導入や保守を行っている A 社から利用者へ説明が行われていないことは、専門家としての対応や責任を果たしていないと言わざるを得ない。

---

[2] 米国の連邦政府が資金を提供する非営利組織。セキュリティや医療、宇宙安全保障などの研究や各種ガイドラインを提供している、

[3] Adversarial Tactics, Techniques, and Common Knowledge の略。実際に発生したシステムの脆弱性を悪用した攻撃の方法のナレッジベース。

[4] Security　NEXT VPN 機器 8.7 万台分の認証情報が公開 - Fortinet が注意喚起 https://www.security-next.com/129771

3.4.3.2　内部侵入（概要）

その後の侵入等については、Ｂ社が実施したファストフォレンジックの報告書である「FF レポート」に基づいて記載をするが、フォレンジックの質や実施方法にも課題があり、全てにおいて可能性の域を脱することができない。まず、半田病院としてはエンジニア派遣を要望したにもかかわらず、要望に応じなかったこと。侵入経路や被害範囲を想定しながら保全に努めていないこと。輸送によるハードウェアの損傷などが生じる可能性に丁寧な指示がないこと、また当該環境でなければシステムの動作などが正常に行われないなどの可能性があるにもかかわらず、対象端末を院外に持ち出して調査を行っている。さらにはネットワークに接続しての端末のウイルススキャンを指示するなど、インシデントの初動や調査の点からは考え難い対応を行っており、フォレンジックを行う企業としての対応に不備があると言わざるを得ない。

なお、同社は市販のフォレンジックツールを用いての調査を指示し、対象となる端末 166 台に対して 2021 年 12 月 7 日から 12 月 17 日において、半田病院で当該ツールの実行を行い、以下の Windows システムにある以下の領域に対してメタデータを取得し、解析を行っている。以下、項目は FF レポートの抜粋である。

- C drive
- System files
- Executable files
- Process
- Boot programs
- Schedule tasks
- Autorun programs
- Network connection analysis during the scanning period
- Windows Event Log

今回のＢ社の報告などをまとめると攻撃の流れや相関関係は図２の通りであり、FF レポートからは多くの PC やサーバーの攻撃の相関関係をつかむことができず、攻撃の全体像を解明することはできなかった。

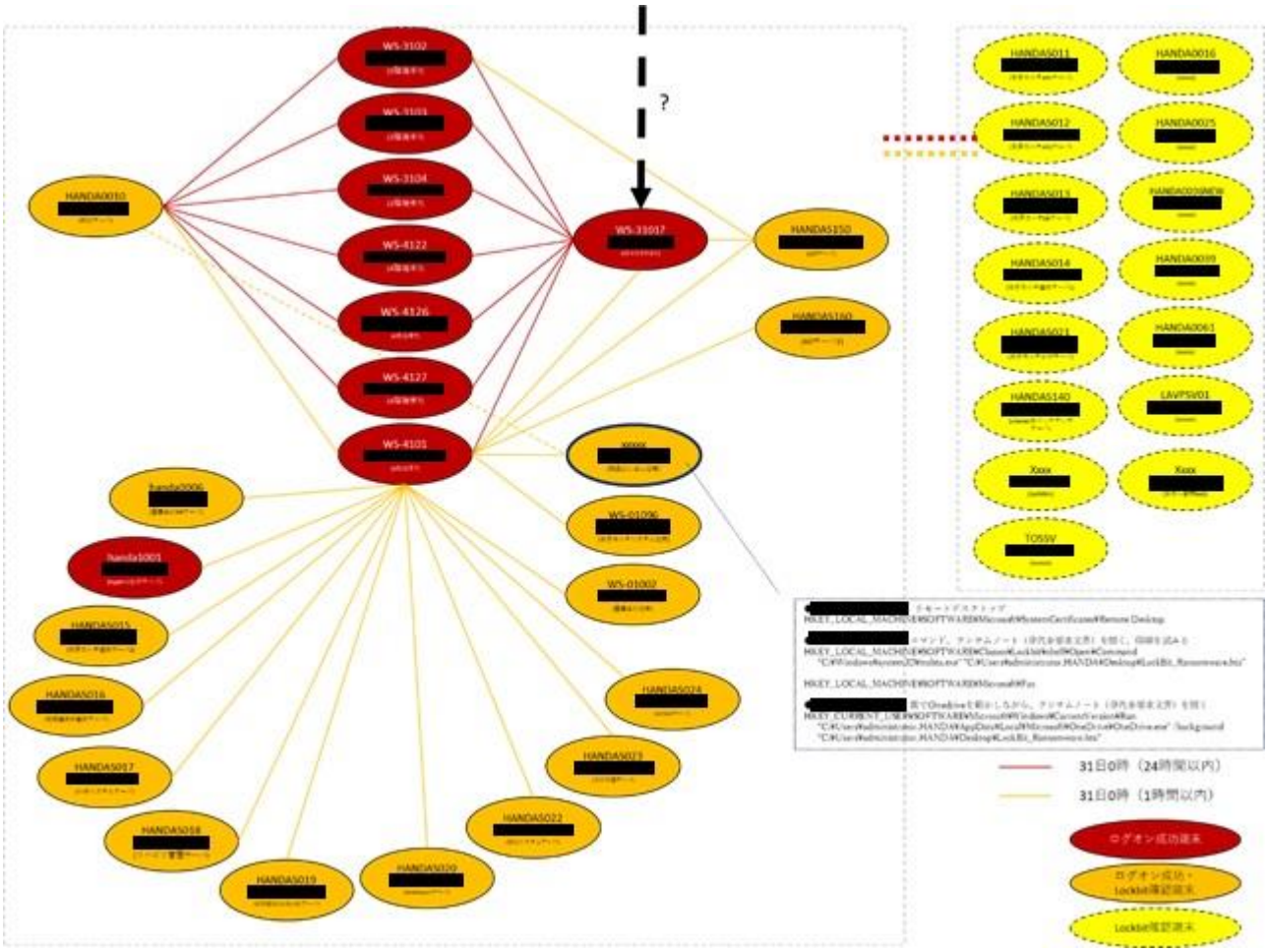

図 2　本サイバー攻撃の相関図

3.4.3.3　内部侵入（詳細）

内部侵入後、インシデント発覚時刻である 2021 年 10 月 31 日 0 時頃を起点として、前後 1 時間以内に、業務用端末の 1 台の端末（3 階端末）から業務用の 7 台の端末（3 階・4 階端末）へログオンされていたことが確認されている。その内 6 台の端末で不審なファイルやマルウェアの痕跡が確認され、Windows のリモート操作ツールである「PSEXESVC.exe」が実行された痕跡が確認されている。また、FF レポートにおいては Windows の資格情報を窃取するためのツールである「Mimikatz」が混入している可能性があることをフォレンジックツールの結果として示唆しているが、それ以上の調査や解析は行われておらず、それ以上の情報については知りうることができなかった。

最初の 7 台のログオン元となった端末（3 階端末）と 7 台の端末のうち、3 台の端末で AD サーバーへの接続を確認し、うち 1 台はもう 1 台の AD サーバーへのログオンを確認している。またログオンが行われていた 7 台の端末から印刷サーバーへのログオンを確認しており、大量の印刷へつながったものと思われる。

さらに、インシデント発生時刻の 24 時間以内に時間を広げると調査をしており、初期のログオンと思われる 7 台のうちの 1 台の端末から、AD サーバー、印刷サーバー等を含む 18 台の端末に対してログオンされていたことも確認されている。ログオンが成功した PC やサーバーは以下のとおりである。

（PC 関連）

- 業務端末（× 2 ）
- 電子カルテシステム端末
- 物品払い出し端末
- 医事会計端末

（サーバー関連：基本システム系）

- AD（Active Directory）サーバー（× 2 ）
- USB 監視システムサーバー
- Hyper-V 仮想サーバー
- 印刷サーバー

（サーバー関連：医療システム系）

- 院内オリジナルシステム（山本システム）サーバー
- WebReport 分析サーバー
- 麻酔記録／分娩台帳サーバー
- 透析管理サーバー
- 地域連携 IF 連携サーバー
- 健診システムサーバー
- 医事会計 DB サーバー
- 電子カルテ連携サーバー

さらに、Lockbit2.0 による暗号化、ランサムウェア感染が確認できたのは以下のとおりである。

（PC 関連）

- 電子カルテシステム端末
- 物品払い出し端末
- 医事会計端末

（サーバー関連：基本システム系）

- AD（Active Directory）サーバー（×２）
- USB 監視システムサーバー
- 印刷サーバー

（サーバー関連：医療システム系）

- 院内オリジナルシステム（山本システム）サーバー
- WebReport 分析サーバー
- 麻酔記録／分娩台帳サーバー
- 透析管理サーバー
- 地域連携 IF 連携サーバー
- 健診システムサーバー
- 医事会計 DB サーバー
- 電子カルテ連携サーバー
- 電子カルテ AP サーバー（×２）
- 電子カルテ DB サーバー
- 電子カルテ参照サーバー
- バックアップサーバー
- 電カル部門 NAS
- その他、詳細不明の端末やサーバー（×８）

そのうち、物品払い出し端末は、調査の時点で初期化されていなかったため、レジストリ情報などの確認を行い、以下のような攻撃の流れを確認することができた。

●21 年 10 月 30 日　23：57　リモートデスクトップ操作
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥SystemCertificates¥Remote Desktop

●21 年 10 月 31 日　3：04　コマンド、ランサムノート（身代金要求文書）を開く、印刷を試みる
HKEY_LOCAL_MACHINE¥SOFTWARE¥Classes¥Lockbit¥shell¥Open¥Command
"C:¥Windows¥system32¥mshta.exe"
"C:¥Users¥administrator.HANDA¥Desktop¥LockBit_Ransomware.hta"
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Fax

●21 年 11 月 6 日　13：04　裏で Onedrive を動かしながら、ランサムノート（身代金要求文書）を開く
HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
"C:¥Users¥administrator.HANDA¥AppData¥Local¥Microsoft¥OneDrive¥OneDrive.exe"
/background
"C:¥Users¥administrator.HANDA¥Desktop¥LockBit_Ransomware.hta"

表 1　物品端末の象徴的なレジストリ情報

上記から、インシデントが発覚した 10 月 31 日の未明以前の 10 月 30 日 23 時 57 分時点でリモートデスクトップの動作が確認できたことから、システムやネットワーク環境の探索などの攻撃の流れを鑑みると、同時刻以前に攻撃者は侵入に成功し、攻撃を開始していたものと考えられる。また、調査を行った OS は Windows 7 であったため、古い OS の端末を継続して利用していたことになる。時系列でみると Windows7 端末の感染はないと B 社は報告しているが、対象端末は Windows7 であり古い OS においてもランサムウェアの感染が確認された。サポート切れの OS を使用していたことは望ましくない一方で、電子カルテを始めとしたシステムを支障なく動かすためには、継続し続けるしかなかった現実もあった。

またこれまで述べた通り、多数の PC やサーバーでログオンの成功や Lockbit2.0 の暗号化されたファイルが確認されている。また 7 台の端末のログオン元となった端末を始め、3 台の端末は AD サーバーへのログオンが成功していることから、病院内の環境情報などが盗み見られ、全てのネットワークやシステム、端末にアクセスできた可能性は高く、情報が盗み見または漏洩した可能性は否定できない。

さらに各端末のログオンについては、そもそもの設定状況として、パスワードは最小桁数が 5 桁であったこと、一定回数以上、ログオンに失敗した際に一定時間ログオンを制限するロックアウトの設定は無かったこと、Administrator の ID は変更されていなかったなど、あらゆるパスワードを入力し結果的にログオンする「総当たり攻撃」を容易に行えてしまう状況であった。攻撃の流れにある端末は、共通または類似性の高いアカウントやパスワードであったことから、パスワードの長さの欠如や、導入当初からセキュリティポリシーが変更されていないことも大きな課題であったと言える。また、半田病院としてはウイルス対策ソフトを導入していたが、電子カルテシステムの導入時に不具合が生じたため、同セキュリティ対策ソフトは動

作させていなかった。リモートメンテンナンスを許可している環境であれば、導入時にウイルス対策ソフトを動作させる詳細なセキュリティ検証が必要であり、さらには定常的にパターンファイルの更新が行える環境の検討が必要であったと考える。しかし、これは半田病院に限らず、未だに続く閉域網の安全神話、閉域網によるセキュリティ対策の思考停止と言えるであろう。

3.4.3.4 水平展開

相関図でまとめた通り、ログオンに成功している端末 9 台、データの暗号化が確認されている端末 15 台、いずれも確認されている端末 16 台、合計 40 台の端末が今回の攻撃による被害や影響を受けていることになる。水平展開にあたっては、すべてのコンピュータの管理者アカウントである ビルトイン Administrator は共通であり、ユーザーでログインされていてもユーザーは 管理者グループであるビルトイン Administrators に所属していたため、Mimikatz などを利用することで資格情報の取得が可能な状況であった。これらから資格情報を取得し、悪用した可能性は高いと考える。なお、特権昇格時のビルトイン Administrator へのユーザーカウント制御（User Access Control、以下「UAC」という。）の 適用は設定されていなかった。

またＢ社の FF レポート内では、「PsExec」の利用が指摘されており水平展開にあたって、よく用いられる手法も実施しようとしていた。しかしながら、上記の通り脆弱なセキュリティポリシーとなっていたため、高度な手法を用いずとも水平展開は容易にできたものと考える。

3.4.3.5 データの復旧

上記の通り、多数の PC やサーバーが Lockbit2.0 によって暗号化されてしまったため、院内のシステムにあるデータが利用できない状況になってしまった。想定される復旧としては大きく二点である。2018 年までにオフラインで保管していたバックアップデータについては Lockbit2.0 の影響を受けなかったため、復旧することができた。もう一点は、Ｂ社による復旧で今回のデータ復元に必要な手段を入手し、対応した可能性である。特に後者の復旧においては、最終的な復旧方法はＢ社独自の調査のため詳細は把握できなかったが、半田病院側との会議の中で「適合が困難で復旧に時間がかかっている」「修復プログラムを組んでいる」といったようなやり取りがあったこと、さらには、データを復元できていることから、何かしらの方法で修復に必要な手段を入手し、データの復元を行った可能性がある。なお、楕円曲線暗号などの暗号技術そのものを解決しなければデータ復旧を行うことができないため、Ｂ社の回答はセキュリティの初心者であるユーザーへの説明不備であり、修復プログラムではなくデータ復元に必要な手段を入手したと考えるのが復旧の流れとしては考えるのが妥当である。しかしながら、攻撃者によるデータ暗号に関する脅迫文は最初のプリンタによる出力のみであり、データが攻撃者によって公開された事実などが確認できなかったこと、それ以降の身代金要求の事実も確認できなかったことなどから、Ｂ社の折衝は定かではない。なお、当然ながら半田病院は身代金を支払わない方針を決めており、身代金を支払った事実もない。

3.4.4　本事案の情報漏洩について

本調査は実際にフォレンジックなどの具体的な技術的調査を行ったわけではなく、有識者会議にて共有された資料やヒヤリング情報をまとめて記載をしているため、情報漏洩については可能性の域を脱することができなかった。しかしながら、アカウントやパスワードの設定状況、ログオンに成功している事実、また内部のネットワークへの感染拡大などを鑑みても、病院内に存在したデータが情報漏洩した可能性は高いとも考える。情報漏洩の可能性があるのはログオンが確認されている PC やサーバーに保管されていた以下の情報である。

端末項目	情報概要・例示
（PC 関連）	
業務端末	共有フォルダー（部門別のファイル（お知らせ文書、Wi-Fi カメラ経由の写真（自動的に飛ぶデータ（診察中に取った写真））、内部資料向けの画像データ
電子カルテシステム端末	患者情報
物品払い出し端末	半田病院が調達、使用している物品の情報
医事会計端末	患者の会計に関する情報
（サーバー関連：基本システム系）	
Active Directory（AD）サーバー	ポリシーや設定情報
USB 監視システムサーバー	医師や関係者の USB の接続情報やデータ情報
Hyper-V 仮想サーバー	環境情報
（サーバー関連：医療システム系）	
半田病院独自システムサーバー	各種医療情報（※半田病院にある各種システムの連携や、効果的な利用のために構築された独自サーバー）
WebReport 分析サーバー	
印刷サーバー	印刷を行ったデータ
麻酔記録／分娩台帳サーバー	麻酔や分娩を行っている患者情報
透析管理サーバー	透析管理を行っている患者情報
地域連携 IF 連携サーバー	連携地域や連携内容に関する情報
健診システムサーバー	健診に係る患者情報
医事会計 DB サーバー	半田病院で行った患者の会計に関わる情報
電子カルテ連携サーバー	患者情報

表 2　情報漏洩の有無と関連する端末情報

なお、先の記載の通り当該情報が攻撃者によってデータが公開された事実は確認できていないため、情報漏洩の事実を確認することはできていない。

3.4.5　C 社及び A 社への質問と回答

本事案発生の直接的な原因となった事業者及びベンダーの実態についてまとめる。課題を明確にするため論点の対象は電子カルテシステムと関連するネットワークに限定している。

3.4.5.1　電子カルテシステムに関する双方の意識

C 社は、アプリケーションの担当が自社、ハードウェア・OS 等のインフラの提供および設定は A 社が担当であるとしている。一方、A 社は(医療情報システムの)全体統括は C 社であり電子カルテシステム(システム全体の意味)の構築は C 社が担当であるとしていることから、この時点で双方に齟齬が見られる。

この齟齬があるにも関わらず、実際には構築時のハードウェア・OS 等のインフラの提供および設定は C 社の指示に従って A 社が作業を実施したとみられ、これらの責任は C 社にあると認識しながら A 社による構築が進められたと見られる。

A 社は、ハードウェア・OS 等のインフラの提供および設定について病院と直接契約したにもかかわらず、これらの責任は C 社にあると認識していた時点で、「ハードウェア・OS 等のデザインや設定の責任」とその後に関連するサポート業務は完全に宙に浮いていたといえる。事業者及びベンダーとして稼働後の運用保守支援サポートは必須であることは認識するも、契約がないため稼働後の責任は一切ないと認識していると思われる。また、「アプリケーション」は病院と C 社との契約、「ハードウェア・OS 等のインフラの提供および設定」は病院と A 社との契約、という契約形態はこのような齟齬を正す機会を逸しさせており、また意識的であったことは否めない。

3.4.5.2　電子カルテシステムの動作環境

C 社は、クライアントのアンチウイルスソフトの稼働に関する不具合の報告はないとし、A 社はアンチウイルスソフトの担当外であるとしていることから、双方ともにアンチウイルスソフトの稼働に関するサポートは範疇外である。

また、C 社は Windows アップデートは最新バージョンの動作検証をし、必要に応じてユーザーに案内も実施しているとされるが、C 社は A 社に対し、Windows アップデートの無効を指示している。
加えて C 社はパーソナルファイアウォールの稼働により、電子カルテに不具合が発生したケースは報告されていないとするも、A 社に対し稼働させないと指示をだしている。

C 社の A 社に対する Windows アップデート無効、およびパーソナルファイアウォールの不稼働の指示は、いずれも、稼働後の運用保守支援サポート契約がないなかでのシステムの安定稼働を優先したものと言えるが、ActiveX の利用や HTTPS への仕様変更予定がないことなど、セキュリティ意識が欠落していると言わざるを得ない。また、A 社は動作環境に関して「責任」はないと認識しているため、セキュリティに関する進言の意識もなかったと思われる。

3.4.5.3　電子カルテシステムのリモートメンテナンス

C 社は、電子カルテシステムのリモートメンテナンス業務の主体であるにもかかわらず、インフラ担当が A 社であることを理由にリモートメンテナンスに利用する VPN 装置の設定仕様書及び通信キャリア、サービスプロバイダー名、経路上の暗号化等の仕様について把握していない。

また、2010 年に　C 社が設置した旧 VPN 装置の故障にともない、2019 年に A 社が VPN 装置のリプレースを実施したが、10 年近く月日が経ちセキュリティ脅威が変化しているにも関わらず、VPN 装置の設定は旧 VPN の内容を踏襲している。踏襲して構わないと指示があったとしても、セキュリティ意識が欠落しているか、適切な設定を施す技術力が全く無かったと言わざるを得ない。

3.4.5.4　VPN 装置の脆弱性

C 社と A 社双方ともに、脆弱性情報(CVE-2018-13379)の存在は認識があったとしている。C 社は電子カルテシステムのアプリケーションが担当であり範疇外の意識、A 社は VPN 装置の担当であるが、ISO27001 に準ずる社内運用ルールに基づき管理運営していたとあり、脆弱性情報に関するセキュリティ知識が全く無かったと言わざるを得ない。

4　委員会での指摘及び改善事項

4.1 組織的な課題

4.1.1　サイバー攻撃リスクを回避・緩和するための課題

半田病院の運営において、今回のインシデントを未然に防御、または緩和できる状態とするには、サイバー攻撃による事業継続リスクが存在するという認識と、このリスクから回避するためのリソースの確保(情報セキュリティの重要性を有す管理者や専門知識を有したエンジニア、セキュリティ対策を施した基幹システムの調達など)が必須である。

サイバー攻撃による事業継続リスクが存在するという事実が認識されるには、マネジメントシステムの導入やリスク管理部門の活動、あるいは管轄省庁や自治体による具体的な啓発・注意喚起が考えられる。

このリスクの存在を十分認識した上で、その軽減策としてリソースの確保となるが、課題は多い。現状の自治体病院における予算策定は、伝統的に事務局主導の従前予算に対する利益改善のための調整であり、病院規模と医療スタッフにより診療能力は自ずと決まるため、予算案は主に材料費と経費の削減が主な計画となる。また、繰入金や県の補助金ありきの経営、または累積欠損金があればこの傾向は顕著となり、これまで想定していなかったリスクから回避するためのリソースの確保はほぼ不可能と考えるべきである。故に、「リスクの存在」と「加えて必要なリソース確保」はセットとして行政や自治体が連携し計画を共有しなければ、町議会への説明もままならないと考える。

4.1.2　マネジメントシステム

インシデント発生当時、半田病院にはマネジメントシステムは存在していなかった。マネジメントシステムへの期待は、トップが責任者として関与することを前提に、事業運営に関して継続的な改善のため、必要に応じて適切な資源（人、資金など）の提供が求められることであるが、情報システムを取り巻く環境の変化やそれにともなう新たな事業継続リスクに関する情報を組織として入手する仕組みがなかったと言える。

病院運営に寄与する各種委員会は 32 委員会あり、本インシデントに関連する「災害対策委員会」、「個人情報保護管理委員会」が年 6 回実施されているが、あくまでも具体的な既知(半田病院にとって)のリスクや、管轄省庁・自治体主導の啓発や指導に対する課題解決に関する会議体であり、新たな事業リスクに関する情報を入手する機会は皆無であったと思われる。故に、本インシデントのようなサイバー攻撃を想定し、これを事業継続上のリスクとして認識するには、少なくとも以下の項目のどれか一つが必要であったと考える。

- BCMS(事業継続マネジメントシステム)の策定と運用
- ISMS(情報セキュリティマネジメントシステム)の策定と運用
- リスク管理委員会の設立と運用

4.1.3　厚生労働省のガイドライン

厚生労働省が 2022 年 3 月に公開した「医療情報システムの安全管理に関するガイドライン 第 5.2 版」[7]によれば、医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、「通常運用における責任」いわゆる医療情報保護の体制を構築し管理する責任と、「事後責任」いわゆる医療業務に影響を及ぼす事象(インシデント)が生じた場合に対処すべき責任、を果たさなければならない。

通常運用における責任のうち、説明責任については、このガイドラインが推奨するような ISMS の導入がないため、具体的な仕様、運用方法の文書化や、監査、監査のフィードバックが実施されておらず、客観的に確認できない。管理責任は、院内の 1 人の情報システム責任者に委ねられ、その個人の知見とその業務範囲内で認識するに留まり、運用に関する委託契約もないことから事業者の監督もない。定期的に見直し必要に応じて改善を行う責任については、サイバー攻撃リスクに関する新しい情報は入手していないため、改善業務はほぼ医療情報システムの利便性に注がれている状況にある。基本的な安全管理の最低限のガイドラインの実施(Web による、個人情報保護に関する方針の策定・公開、文書による、医療情報システムの安全管理に関する方針の策定)は確認できるが、ISMS の実践を促されているものの、実施はされていない。

一方、事後責任については、災害拠点病院としての事業継続計画が策定され訓練も実施されていることもあり、DMAT の支援も功を奏したことで最低限の事業継続ともに監督機関である行政機関や社会への説明・公表も実施されている。また、この報告書により、原因の追求、善後策を講ずる責任も果たされると認識している。

また、「医療情報システムの安全管理に関するガイドライン 第 5.2 版」には、電子保存のための運用管理事項として、真正性の確保を義務付けられている。これは e-文書法の視点から医療情報が病院の管理下にあることを前提に、入力者及び確定者の識別・認証、記録の確定手順と識別情報の記録、更新履歴の保存、代行入力の承認記録、機器・ソフトウェアの品質管理や動作状況の内部監査規程等が定められている。今回のインシデントのようなケース(ランサムウェア等被害後のデータの真正性に関する記述)は記述が無いため、一旦管理から外れたデータの真正性の担保は想定外ということとなる。

つまり、「医療情報が一旦ランサムウェア被害に見舞われた場合、身代金を払って復元できたとしてもそのデータの真正性の担保はできないため、結果的に身代金を支払うことは合理的でない」という判断が妥当とも考える。このことにより、現状の運用(復元した DB での医療業務)は、真正性欠如の可能性に留意しながら医療業務を進めることが肝要である。

4.1.4　自治体の災害拠点病院に対する事業継続計画(BCP 策定の経緯)

半田病院は、厚生労働省医政局地域医療計画課　救急・周産期医療等対策室が主催した、平成 29 年度(2017 年)事業継続計画(BCP)策定研修(災害拠点病院等向け)に参加している。これは、厚生労働省医政局指導課から各都道府県衛生主管部長宛に対し、管内の病院に周知された災害対策マニュアルの整備に活用するよう促したもので、主旨は、「災害時における医療体制の充実強化について」(平成 24 年 3 月 21 日医政発

7 厚生労働省の「医療情報システムの安全管理に関するガイドライン 第 5.2 版」(2022 年 3 月)
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

第 0321 第 2 号厚生労働省医政局長通知)に基づき、医療機関は自ら被災することを想定して災害対策マニュアルを作成するとともに業務継続計画の作成を促すことである。

医療の世界で BCP が初めて意識された契機となったのが平成 23 年(2011 年)の東日本大震災であったが、当時、災害拠点病院であっても BCP の策定ができているのは当時半数以下であったため、まずは BCP の策定に取り組み、訓練等を通じてブラッシュアップしていくことを目的としていた。

研修では、平成 29 年 3 月版(2017 年)「病院 BCP を策定するための手引」に示された内容を具体化するため、「病院 BCP(災害拠点病院用)」及び「平成 25 年度版：BCP の考え方に基づいた病院災害対応計画作成の手引」等がテキストとして使われ、半田病院はこれをカスタマイズして同年に策定した。

これらのテキストは上記主旨に基づき、大災害時の基本となる最小公倍数としての直下型の地震災害に対する病院 BCP を例として取り上げている。本来 BCP が目指すところの、「事業継続に支障を及ぼす可能性のある災害は考慮する。場合によっては、想定される災害毎の BCP の整備が必要となる。」ともあるが、これは地域毎の環境に合わせた災害を想定し BCP 策定をする、という意図であり、サイバー攻撃等のインシデント発生に対する事業継続計画は想定されておらず、半田病院が BCP 策定の時点でサイバー攻撃等を災害と想定することは難しかったと考える。

4.1.5　安全管理のためのリソースの欠如

一方、総務省が 2022 年 4 月に公開した「公立病院の現状について」[8]にあるように、公立病院の経営状況は悪化の一途をたどっており、半田病院のような 200 床未満(全体の 54.1%)[9]は、一般的に IT 部門を持っておらず、少しパソコンに詳しい庶務係が IT 担当を一人で兼任しているような状況にある。仮に半田病院が前述したようなリスク管理対象にサイバー攻撃を含め BCP を策定することになっても、救急救命センターのような高度な医療行為を担っていないため、医者と看護師の配分を調整しても人件費が膨らむ(医療機能の低下していく病院はベッド当たりの入院単価が下がることとなるので人件費が上がる)。このような状況下では半田病院においても医療情報システムの安全管理を実現するリソースを割く余裕は無く、サイバー攻撃リスクを盛り込んだ BCP 策定を理由に、IT 担当者の増員を予算に含めても受け入れられないのは明白である。その結果、セキュリティ対策について医療システム事業者やサポートベンダーに頼らざるを得ない状況(且つ、サポートサービス契約によるキャッシュアウトも不可)となるのは自然の成り行きと考える。

半田病院の情報セキュリティに関連のある委員会では、主任会配下のコンピュータ委員会、電子カルテ委員会が「つるぎ町立半田病院医療情報システム運用管理規定」を策定するに留まっていた。

---

[8] 2021/04/01 総務省「公立病院の現状について」
https://www.soumu.go.jp/main_content/000742388.pdf

[9] 全国の 857 の公立病院のうち 200 床未満の病院が 464 拠点

行政が提示するガイドラインには具体的な対策が明示されないため、方針に基づく対策の考え方から具体策に落とし込むための知識やリソースがない、または、リソースを増やす理由(リスク認識)が無い。故に専門知識がない、適切なアドバイスもない、医療業界も含めた閉域網神話の浸透により、「閉域網であれば(セキュリティ対策を考えなくても)許される」となったと推測する。

4.1.6 事業者及びベンダーの善管注意義務

「医療情報システムの安全管理に関するガイドライン 第 5.2 版」によれば、医療情報の管理業務を受託していなければ定義上事業者は対象外であり、このケースでの事業者の果たすべき善管注意義務については明確にされていない。故に、このガイドラインに基づけば「通常運用における責任」および「事後責任」を果たす当事者は半田病院だけである。しかし、前述の情報システム管理リソース欠如の状況において、事業者及びベンダーはこの「丸投げ状態の理由」を十分認識していると思われ、事業者及びベンダーは医療情報を扱う当事者でなくとも、システム全体の構成要素の内容を含めたリスクマネジメント実施の提案、または知見が不足するのであれば、第三者への委託を含めそれらを促すなどの善管注意義務は十分にあったと考えるのが妥当である。ましてや事業者及びベンダーは VPN 装置の脆弱性および ID 情報の公開の事実があったにも関わらず、適切な対処を講じなかったために今回の事件発生を防止または緩和ができなかったこと。さらに、納入システムが閉域網であることを理由に、極めて初歩的なセキュリティ対策を継続的に怠ったため、最悪の事態に至らしめた責任は重いと考える。

4.1.7 閉域網に関する課題

本事案は、VPN 装置の脆弱性を狙われ閉域網が破られた事案であると判断するのが妥当といえる。

閉域網内に置かれた電子カルテシステムは、 Active Directory のセキュリティ設定から IE7 互換を要求しており、かつ、2000 年に開発された古いデザインのシステムであった。開発当時の代表的なウイルスは、OVELETTER、MTX、Nimda などで、主に電子メールの添付ファイル、悪意のある Web サイトなどが初期侵入の経路であった。多くは、アンチウイルスの完全スキャンでの検出、防御が可能であり、VPN がない閉域網であるならば、USB メモリ等のリムーバブルメディアの適切な管理によって感染リスクは十分下げることができたといえる。

一方、現在の医療情報システムがおかれた脅威環境を考えると、果たして 2000 年当時のシステム構成や動作環境を見直すことなく、開発当初と同等のセキュリティ設定を維持し続けることが正しかったのか、という疑問が残る。実際に、半田病院に対してはシステムの動作を阻害するセキュリティ設定を解除させ、その上で、VPN 装置の脅威を分析せず、結果として地域の医療を崩壊させ、かつ多額の税金を投じることとなったのである。いわば本事案は、ベンダーが昨今のセキュリティ事情を考慮せず、現在となっては極めて脆弱なシステムの販売と稼働を優先させたことにあった、といえるのではないか。

VPN に接続されても、最新の脆弱性修正プログラムが適用され、アンチウイルスソフトが稼働し、適切なロックアウト設定と標準ユーザーでの運用がなされていれば、少なくとも攻撃の遅延もしくは阻止ができた可能性がある。最早、悪意あるプログラムはインターネットに限って侵入してくるものではない。ベンダーやベンダーの協力会社の開発環境を侵害し、正規のソフトウェアのバージョンアップに紛れて、組織のネッ

トワークに侵入する手法が存在し、実際に多くの被害を招いている。我が国の IT 業界の多重下請け構造に照らせば、非常に危険な状態にあるといってよい。従って、ソフトウェアの開発サプライチェーン全体が侵害されていないという、清浄性を担保する必要がある。医療情報システムで閉域網と呼ばれているネットワークは、実際にはソフトウェアサプライチェーンに対しては開かれたネットワークであり、間接的にインターネットと接続されたネットワークであることを十分認識しなければならない。

4.2 技術的な課題

4.2.1 Active Directory の課題

以下に半田病院の Active Directory の課題について述べる。本来であれば、IPA「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」での詳細設定の全項目を実施、記述すべきであったが、項目数が多いことから、本項では特に初期ログイン、水平展開の阻止の観点で課題とされる点のみを指摘する。

- 短いパスワード設定
  パスワードの最小桁数が 5 桁に設定されていた。
- ロックアウト設定が無効
  Active Directory のグループポリシーでは、ロックアウトの設定が無効となっていた。短いパスワードであっても、ロックアウト設定を行っていれば、総当たり攻撃は防げたと考えられる。
- ドメインユーザーが Built-in¥Administrators に所属
  ドメインユーザーが Built-in¥Administrators に所属していたため、マルウェア侵入時のセキュリティ権限は管理者権限であり、OS の設定変更、資格情報のダンプ等が自由に行えた。
- UAC
  管理者承認モードでの管理者に対する昇格時のプロンプトの動作が既定値であった。既定では Microsoft 以外のアプリケーションの操作で特権の昇格が必要な場合、ユーザーはセキュリティで保護されたデスクトップで [許可] または [拒否] を、ID/パスワードの入力もしくはマウス操作で選択するように求められるが、常時、Microsoft のアプリケーションも含めて、すべての特権昇格時に「セキュリティで保護されたデスクトップで同意を要求する」とすべきであった。これによって、マルウェア侵入時の OS の設定変更等の特権昇格時に UAC が表示され、攻撃の阻止、遅延が期待できた。

4.2.2 脆弱性管理の課題

以下に電子カルテシステム、医事会計システムのシステム設定の課題について述べる。

- **VPN 装置の脆弱性管理を実施していなかった**
  病院情報システム、検査機器等のリモート保守のために設置された Fortinet 社の VPN 装置 FortiGate 60E の脆弱性（CVE-2018-13379）[10]が放置されていた。
- 同脆弱性を利用した認証情報が漏洩したが、ID、パスワードを変更していなかった

10 細工を施したデータを VPN 装置に送信することで、VPN 装置のシステムファイルがダウンロードでき、結果として、システム管理者の ID、パスワードを入手でき、インターネットから閉域網内に侵入が可能となる脆弱性。

- 87,000 台の VPN 装置の ID、パスワードがインターネットに公開
  2021 年 9 月に同脆弱性を悪用し全世界で 87,000 台の ID、パスワードが公開 されたが、本件調査では、その漏洩データに、半田病院のグローバル IP アドレス、ID、パスワードが含まれていた事を確認している。
- 開発元の Fortinet 社からは 2019 年 5 月、2019 年 8 月、2020 年 7 月、2021 年 4 月、2021 年 6 月、2021 年 9 月に渡って再三、是正措置の告知があった。加えて、事案の重大性によって、多数の報道がなされていたにもかかわらず、ステークホルダーのアクションはなかった。

媒体	日付	見出し
Security NEXT	2021/9/9	VPN 機器 8.7 万台分の認証情報が公開 - Fortinet が注意喚起
朝日新聞	2021/9/11	企業狙うハッカー「攻撃マニュアル」入手　身代金ビジネスの実態は
朝日新聞	2021/9/11	Fortinet 社製の VPN 認証情報が流出　日本含め世界で 8.7 万台分
時事通信	2021/9/11	国内１０００台以上で流出　在宅勤務時の接続認証情報
共同通信	2021/9/11	VPN 認証情報また流出 日本は 1000 社、中小企業中心
日経 XTECH	2021/9/11	VPN 装置からのパスワード大量流出、1 年前の脆弱性が突かれたわけ
日本経済新聞	2021/9/13	VPN 認証情報また流出　日本は 1000 社、中小企業中心
ITmedia	2021/9/13	8 万 7000 台に影響　「FortiGate」の SSL-VPN デバイスの認証情報が漏えい

表 3　対象の VPN 機器に関する報道例

■ **電子カルテシステム、医事会計システムの稼働を優先し、脆弱性管理とウイルス対策を実施していなかった**

電子カルテシステム、医事会計システムの動作が不安定になるという理由から脆弱性管理を実施せず、かつ、アンチウイルスソフトウェアの動作を停止していた。

- **Windows アップデートの未実施**
  グループポリシーによって、Windows アップデートを実施しない設定となっており、Windows 10 のすべての脆弱性がコンピュータに存在した。
- **Silverlight のアップデートの未実施**
  レジストリ設定によって ActiveX コントロールである Silverlight のアップデートが無効となっており、Silverlight のすべての脆弱性がコンピュータに存在した。
- **Acrobat DC のアップデートの未実施**
  レジストリの設定によって Acrobat DC のアップデートメニューの非表示、アップデートを実施しない設定となっており、Acrobat DC のすべての脆弱性がコンピュータに存在した。
- **アンチウイルスソフトが未稼働**
  既知のマルウェアに対して防御力がなかった。
- **Windows Endpoint Protection が無効**
  グループポリシーによって、Windows Defender 以外のアンチウイルスソフトが稼働していない場合の、Windows 標準のアンチウイルスソフト Windows Defender の動作が無効となっており、既知のマルウェアに対して防御力がなかった。

- サポートが終了した ActiveX コンポーネントである Silverlight が使用されていた
  - **Silverlight の利用**
    電子カルテシステムで図形描画を行うための Microsoft Silverlight が組み込まれていたが、Silverlight は 2021 年 10 月 12 日にサポートが終了しているにも関わらず、ベンダーからは説明もなく、漫然とその利用を継続していた。
  - **Silverlight の脆弱性**
    Silverlight には特権昇格を許す（MS15-049）や、リモートでコード実行が可能な脆弱性（MS16-006）などが存在していたが、前項の理由でこれらの脆弱性の修正は行われていなかった。
  - **Silverlight の代替措置について**
    2022 年 3 月の有識者会議の指摘で販売元である C 社に問い合わせを行ったが、バージョンアップにおいて対応を行う旨の回答が初めてあった。

4.2.3 システム設定の課題

以下にシステムやセキュリティ設定に関する課題について述べる。

- VPN 装置 FortiGate 60E への接続元 IP アドレス制限を怠っていた
  侵入元と考えられる FortiGate 60E への接続元の VPN 接続及び管理アクセスが可能な接続元 IP アドレス制限を行っていなかった。これによって、資格情報さえあればインターネット上のすべてのシステムからの接続が可能であった。
- **サーバーのパーソナルファイアウォールが無効となっていた**
  サーバーのパーソナルファイアウォールがすべて無効となっており、あらゆる通信に応答する設定となっていた。これによって、外部の攻撃者の問い合わせに応答してしまい、水平展開が極めて容易であった。
- **「信頼済みサイトゾーン」と設定されていた**
  電子カルテシステム、部門システムの IP アドレスに存在するすべてのサーバーを「(2) 信頼済みサイトゾーン」としていた。このアドレスに存在するサーバーとの通信はセキュリティ設定が「低」の状態となる。
  - 最小限度の保証および警告指示が提供される
  - ほとんどのコンテンツが警告なしにダウンロードされ実行される
  - すべてのアクティブコンテンツが実行できる
  - サイトを無条件に信頼する

  これにより、院内ネットワークに侵入され、なりすましサーバーが設置されると、ほぼ無条件で攻撃を受ける可能性があった。

- **電子カルテシステム系 IP アドレスに対してポップアップが許可されていた**
  ポップアップとは、Web サイト閲覧の際に、ボタンやリンクをクリックすると別ウインドウで開く新たなウインドウを指す。この際、スクリプトを使用して広告を多数表示したり、フィッシングサイ

トや悪意あるサイトに誘導したりするなどの行為が続出したため、殆どのブラウザでは、既定値でポップアップがブロックされる仕様となっている。

- 電子カルテシステムクライアント端末はポップアップが許可されてしまうため、ポップアップを悪用するサイトからの攻撃に脆弱であった。

■ 自己署名証明書での署名された ActiveX コントロールのサイレントインストールが許可されていた

本件システムでは、電子署名がある ActiveX コントロールはサイレントインストールを許可しているが、この中に自己署名証明書での署名も含まれていた。自己署名証明書を許可すると、攻撃者の自己署名証明書でもサイレントインストールが可能となり、危険である。Windows の既定値ではすべての Active X のインストールの確認をする仕様であり、あえて、自己署名証明書のサイレントインストールを許可していたといえる。

設定項目	アプリケーションサーバー①	アプリケーションサーバー②
信頼された発行元の証明書ストア(TPS)の証明書で署名された ActiveX コントロール	ActiveX コントロールがサイレント インストールされます。	ActiveX コントロールがサイレント インストールされます。
署名された ActiveX コントロール(自己署名証明書)	ActiveX コントロールがサイレント インストールされます。	ActiveX コントロールがサイレント インストールされます。
未署名の ActiveX コントロール	ActiveX コントロールのインストールを求めるメッセージがユーザーに対して表示されます。	ActiveX コントロールのインストールを求めるメッセージがユーザーに対して表示されます。
証明書の検証	不明、無効な認証局、有効期限、誤った証明書の使用方法を検証	不明、無効な認証局、有効期限、誤った証明書の使用方法を検証

表 4　証明書などの設定状況

通常、商用コードサイン証明書を使用すれば、信頼された発行元の証明書ストア（Trusted Publisher Store）には Windows の既定で発行元の認証局が含まれるため、自己署名証明書の使用をしなくても済むはずであった。

■ クライアントーサーバー間の通信は HTTP(TCP/80) であり平文であった

本件システムでは、機微情報を含む個人情報を取り扱うため、本来であれば HTTPS (TCP/443) として、盗聴を防ぐべきであったが HTTP (TCP/80) であった。

- **HTTPS 化について**

  2022 年 3 月の有識者会議の指摘で販売元である C 社に問い合わせを行ったが、「可能だがいくつか課題がある、また、全体的な検証が必要」との回答があった。

  その後、有識者会議の質問書に対して「実績はない」旨、回答があった。

4.2.4　課題となった脆弱性管理の放置と脆弱なシステム設定に至った理由について

これまでに述べたように半田病院のシステム環境は技術的に大きな課題を抱えていた。ここではこれまでの技術課題と根本的な問題について述べる。

■ アプリケーションソフトの動作を優先しセキュリティ設定を劣後せざるを得ないシステムであった。セキュリティ設定がことごとく劣後されたのは、古い設計の電子カルテシステムと、医事会計システムの動作を確保するためと考えられる。以下にその理由を述べる。

- **電子カルテシステムは 古い Internet Explorer 7 (IE7) を前提に設計されている**
  体温表描画のために Silverlight を使用しているが、Silverlight は Microsoft の IE の後継ブラウザである Edge では、サポートされていない。このため、IE だけを前提にしたシステムであるといえる。また、グループポリシー設定で IE7 互換の構成が設定されていたことから、設計当初より IE 7 をターゲットブラウザとしていたことが推定できる。
- **Web コンポーネントとして ActiveX コントロールを前提に設計されている**
  ActiveX コントロールのサイレントインストールを悪用したマルウェアが多数出回ったため、Microsoft は既定で ActiveX コントロールのサイレントインストールを禁止し、インストールの際には管理者の資格情報を求めるように変更した。このままだとシステム運用上、常時、資格情報の入力が求められるため、アプリケーションサーバーからの ActiveX コンポーネントのサイレントインストールを許可していた。
- **IE、Silverlight、ActiveX コントロールの動作を優先したセキュリティ設定になっている**
  IE のコンポーネントへの変更や Silverlight への変更、これらに対する Windows のバージョンアップの影響を避けるために各種アップデートを禁止する設定となっていた。
  また、ActiveX コントロールはアンチウイルスソフトから見た場合、マルウェアと判断されることがあるため、アンチウイルスソフトの運用を停止していたと考えるのが合理的である。
- **閉域網ではないにもかかわらずインターネット上の脅威を評価していなかった**
  VPN 装置 によってインターネットからの外部接続が可能なネットワークであったにもかかわらず、VPN 装置の脅威を評価しなかった。
  - ✧ VPN 装置の脆弱性の是正を行っていない
    VPN 装置の脅威をまったく評価せず、結果として、VPN 装置の脆弱性の是正、パスワードの変更を行っていなかった。
  - ✧ VPN 装置への接続元 IP アドレスの限定を行っていない
    保守のための接続であれば、接続元 IP アドレスを限定すべきであった。接続元 IP が限定されていれば、認証情報だけでは突破されなかった。
  - ✧ VPN 接続の際の多要素認証を行っていない
    第三者の成りすましを防ぐための多要素認証を設定すべきであった。
- **病院内ネットワークでの脅威を評価していなかった**
  病院内のサーバー、端末、ネットワークは、物理的立ち入りが制限されているエリアに設置されていることから、病院内ネットワークの脅威を評価していなかった。
  - ✧ **電子カルテシステム、医事会計システムは HTTPS 通信による暗号化をおこなっていない**
    何らかの悪意のある関係者による盗聴を前提に、病院内の通信は暗号化すべきであった。

- ✧ **医師の論文作成等のためにデータ持出のための USB メモリの利用が許可されていた**
  USB メモリからのマルウェア感染等に備え、アンチウイルス内蔵 USB メモリの使用、USB メモリ使用ごとの初期化などのルールを定め運用するべきであった。

4.3 社会的な課題

本インシデントは、兼ねてから叫ばれている「サプライチェーン」や「縦割り行政」「古いセキュリティ対策」などの課題が複合的に生じている。今回は偶発的に半田病院で発生したが、半田病院に限った話ではない。

病院システムを考えるとユーザーとベンダーの強い結びつきの一方で、情報の非対称性が大きく、さらには管理できないほどのステークホルダーがいるという根本的な課題が存在すること、加えてその責任分界点をベンダー間、ユーザーとベンダー間でも確認しきれていないこともインシデントを大きくしてしまった原因である。今回関係するステークホルダーを洗い出すだけでも、総務省、厚生労働省、徳島県、徳島県警察本部、つるぎ町、電子カルテの開発ベンダー、提供ベンダーである C 社、インフラやセキュリティ面などを支援した A 社、それ以外にも関連するベンダーが数十社存在する。またフォレンジックを行った B 社、その他の連携する医療機器の導入や保守を行っているベンダー、近隣自治体や連携している医療機関、医師会、その他にも調達に関連するベンダーなど、ステークホルダーの数は数えきれないほどである。

半田病院は利用者として自身でセキュリティのスキルや、組織としてのセキュリティレベルを向上していなかったという大きな課題があるが、事実上 1 人で院内のシステム導入・運用を行っていた状況ではセキュリティの情報収集から自身そして職員のセキュリティ向上に努めるのは極めて難しい。公立病院である組織の複雑性がもたらした弊害とも言える。利用者である半田病院は本事象の解消に努めなければならなかった責任もある一方で、法令や行政の仕組みによって解決しようもない現実があったのも事実である。

また地場のシステムインテグレーターである A 社の知識不足やリソース不足も課題である。先に述べた通り、ネットワーク機器の導入を行っていた事業者であればハードウェアの保守がある以上、機器に影響を及ぼす事案であればそれを伝える必要がある。この保守の在り方も利用者と SI の双方で事前に調整を行えていなかったことも大きい。このようなソフトウェアの継続的な保守の課題は、今回の半田病院に限った課題ではない。

さらに電子カルテの動作が優先でセキュリティ対策をないがしろにした責任も大きく、C 社側の対応も適切ではなかった。先の通り、システムの脆弱性を作り出すようなファイアウォールの無効化の設定、HTTP 前提の通信、ActiveX を必要とするアプリケーションの構造など、電子カルテベンダーとしての責任は重い。ここまで脆弱であると可用性に重きを置いていたとしても明らかに機密性や完全性が欠如しており、製品としても課題がある。また、これらをきちんと利用者に説明していなかった責任も極めて重く、利用者に対して説明責任を果たしていない。たとえ、時代や技術の進歩による変化が開発コストなどから対応できない場合であったとするのであれば、これは事前に本課題をユーザーに対して適切に通知を行い、注意を喚起するべきである。

これ以外にも、病院行政やガイドラインの複雑さなど、課題が多い。特に病院行政は、病院そのものは厚生労働省であるが、大学病院であれば文部科学省、公立病院であれば総務省など、関係省庁が複数存在する。また今回の場合は徳島県、つるぎ町など、公立病院としてのステークホルダーも増えている。各組織各様にインシデント報告を求められ、現場では各組織への配慮や対応が必要となった。誰が火災の最中に報告を求めるのであろうか。サイバー攻撃は目に見えないからと言って報告を求めがちだが、インシデント発生中は災害が発生しているものと考え、各行政が対応する必要があるとともに、一日も早いステークホルダーの整理が求められる。

またガイドラインも昨今 3 省ガイドラインが集約されてきていることに象徴されるように、早急にガイドラインの統一が求められる。またこれらのガイドラインも ISMS 的な表面上のガイドラインではなく、より製品メーカーとの具体的な設定に踏み込んだガイドラインが必要不可欠である。現行のガイドラインは抽象的すぎるため、結局のところ資源のない病院側に考え方や対策を求めている。これでは全国にある病院が単純に疲弊するだけであり、いくら資源があっても足りない。

さらに既にシステム担当者が一人で運用しているような、場合によっては兼務で一人もアサインできていないような組織においては、そのリソースをコミュニティの活用によって解決を図る方法も検討しなければならない。病院は患者の受け入れをはじめ横のネットワークが存在するため、このネットワークをサイバー空間まで想像を広げて活用していくべきである。

5 再発防止策の実施と検討状況について

5.1 組織的な課題の対応・対策

前述の４.1 項において、組織的な課題に関して以下のように述べた。

- **リスク認識の不在とリスク回避リソースの不備**

  本事案による損失を回避・緩和するためには、サイバー攻撃による事業継続リスクが存在するという認識と、このリスクから回避するためのリソースの確保が必須であるのに、それらはなかった。

- **サイバー攻撃を想定した BCP の不在**

  一方、自治体の指導による、災害拠点病院に対する事業継続計画(BCP)の策定と訓練は実施されたため、病院基幹システムが機能しない状態での事業継続は適切に実践されたが、サイバー攻撃によるリスクは想定されていないため、医療情報システムの安全管理に必要なリソース確保や管理手法、インシデントの対処、これらに必要なパートナーに関する備えは一切なかった。

- **情報システムの安全管理に関するマネジメントシステムの不備**

  既存のルールや規定および計画の見直し、または、新たなリソースを投入するような経営計画を盛り込み実施するには、マネジメントシステムを機能させることが一般的であるが、これに値する機能はなかった。

- **公立病院の経営的課題**

  半田病院が情報システムの安全管理を実施するため、例えば厚生労働省の「医療情報システムの安全管理に関するガイドライン」が推奨する ISO27001 等の実装を試みたとしても、半田病院のように 200 床未満の小規模病院の経営状況では、金銭的、人的、技術的に当てはめ実装できるような内容になっておらず、Web による個人情報保護に関する方針の策定・公開、および文書による医療情報システムの安全管理に関する方針の策定をするに留まっていた。

- **事業者及びベンダーの専門知識と善管注意義務の不在**

  120 床の半田病院が情報システムの安全管理を実施することを前提に、医療情報システムの調達、運用、安全管理について成熟するには、情報セキュリティに関する専門知識が不足するため、それを補うパートナーシップが必須となる。本事案では半田病院が選択した事業者及びベンダーには情報セキュリティに対する専門知識がなく、情報システムへのセキュリティ意識も低いため、閉域網問題の不理解や善管注意義務も果たされることがなかった。事業者及びベンダーに対して行政が推奨するガイドラインは、クラウドサービス事業者を前提とする医療情報の処理・管理を受託する事業者が対象であり、オンプレミスの医療情報システムの構築に関与する事業者及びベンダーは対象外となっていることが穴となった。

  また、これらを単に病院の事業者及びベンダーの選択の問題として片付けるのではなく、地方が抱える事業者及びベンダーの不足(選択肢の無さ)の問題を踏まえ、情報システムを扱う事業者及びベンダーに対する行政からの指導や啓発が必要であった。

  これらの課題を解決するには、以下の施策の実現が求められる。

- **行政・自治体連携による、公立病院の実態を想定した事業継続マネジメントシステム導入の指導**

  病院は事業継続計画において、サイバー攻撃によるリスクも含め、医療事業環境での新たなリスクを認

識・評価し事業継続計画の見直しを継続的に実施する仕組み(マネジメントシステム)を持つことを必須とする。同時に行政や自治体は、公立病院に対する事業継続計画の策定指導にとどめず、このマネジメントシステムの構築を促すとともに、公立病院経営強化策にもレジリエンス投資等の枠組みを盛り込むことで、病院の事業計画に対して、安全管理に必要なリソースを盛り込むことが受け入れられやすい環境となるようにする。

- **情報システムにおけるセキュリティ・コントロールの向上**

  サイバー攻撃に対する対策を含む医療情報システムの安全管理に関しては、適切な有識者とパートナーシップを結び、情報システムにおけるセキュリティ・コントロールを成熟させる。特に、情報資産、構成情報、設定情報、ログ管理、脆弱性対応状況等を管理するなど、サイバーハイジーンを主眼とした実装しやすいガイドラインを参考に、セキュリティ・コントロール力を継続的に向上させる。

  ※一般社団法人ソフトウェア協会 Software ISAC 「情報システムにおけるセキュリティ・コントロール・ガイドライン Ver1.0」を参考とする。

- **適切な事業者及びベンダーの選定**

  情報システムの調達及び刷新に関しては有識者の意見を取り入れ、「情報システムにおけるセキュリティ・コントロール・ガイドライン」や最新の ISMS の運用に必要な情報を理解し見識を提供できるとともに、ユーザーの安全管理に対して協力を怠らない事業者及びベンダーを選定・管理する。

- **医療情報システム従事者のコミュニティの創設**

  脅威情報や強化情報の交換のための「医療情報システム従事者のコミュニティ」を創設する。

5.2 技術的な課題の対応・対策

技術的な課題の対応・対策は、別途とりまとめた「徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議報告書―技術編―」を参照されたい。

5.3 社会的な課題の対応・対策

4.3 の社会的な課題で解決策も一部述べたように、様々な社会的な課題が存在し、解決策として書き切ることは難しい。その中でも、特筆すべき課題は政府機関、自治体、公営企業法などから生じる責任者の不透明さなど、公的機関や制度の根本的な課題である。病院行政の複雑さがインシデント対応に混乱を生じさせないように、公的機関による主体的な司令塔や統制の整備が必要である。その中で、様々存在するガイドラインについても統一化と具体化を図っていかなければならない。さらにはインシデントが起きたときに誰を、どのように頼ればいいのか。利用者が対応しやすい環境の整備が産官で求められる。

また、今回明らかになったのは情報の非対称性の解消に努める必要のあるベンダーの対応の不足である。そこには事業者が業務の多忙さからできなかった時間的な課題や、保守契約や責任分界点の不明瞭さから生じているかもしれないが、これは契約や双方で協議することによってまだ解消することが可能である。しかし、根本的に専門家としての知識および経験不足は、協議すれば解決できる課題ではなく、さらなるベンダーの努力が必要であると言わざるを得ない。都市部だからと言って決してセキュリティの知識や経験が豊富とは限らないが、地域のセキュリティ人材や知識、経験の不足は大きな課題として露呈したインシデントである。どの地域においても地場の事業者を頼っている現状があると思われるが、その専門家のセキュリティ

の知識や経験が乏しければ、対象のシステムやネットワークなどはセキュリティ上の問題を抱えながら運用していることになる。さらに、今回電子カルテシステムを全体統括する立場の C 社と、電子カルテを補助するインフラ、セキュリティ関連を担った地場のシステム会社である A 社とで、見解や回答の相違がみられることは、ベンダー間でも連携や責任分界点が明確になっていない証拠であり、ベンダーの知識や連携の不足も課題であることを示している。早急に本課題を解決するために、各地域の情報技術を生業とする事業者のセキュリティ教育と強化が必要である。将来的には事業者としての信頼性を証明するための評価制度などを設けて、セキュリティレベルの持続的な向上に努めていく必要もある。一方で、国はそのようなセキュリティの知識や経験に長け、言わば日本の安全に貢献している事業者は、減税や補助、表彰といったような制度などを検討し、具体的で持続的なセキュリティエコシステムを形成していくべきである。

本インシデントによって電子カルテシステムやセキュリティ製品の設定などの確認は関係するすべての事業者で実施するべきであり、特に重要インフラ事業者のシステム（特にサプライチェーン）の総点検が必要である。加えて、開発・提供する事業者およびシステムやネットワークを構築する事業者のセキュリティレベルの総点検も忘れてはならない。デジタルトランスフォーメーションが昨今であるが、脆弱なシステムを生み出せば生み出すほど、日本は近い将来サイバー攻撃によって日本の情報が世界に筒抜けになってしまうような窮地に陥る可能性があることを忘れてはならない。アクセル（デジタルトランスフォーメーション）とブレーキ（セキュリティ）は双方が健全に開発され、発展すべきである。

6 まとめ

今回のインシデントは起きるべくして起きしてしまったインシデントであった。病院側のセキュリティに対する意識が低かったというのは事実であるが、地域医療の拠点である半田病院であっても、事実上、情報システム担当者は 1 名の状態で運用していた。このような状態でサイバーセキュリティの知識を深めることや設定の見直しなどを行える状況になく、日々の機器やシステム、ネットワーク運用で手一杯の状況であった。

また今回のインシデントは、このようなインシデントを予測し、準備できていなかった半田病院側の責任がある一方で、電子カルテシステムを始めとした周辺機器やシステムなどを提供している事業者、そして本インシデント対応に関わった事業者の不誠実さの連鎖が生じていたのも事実である。その結果として、通常診療を取り戻すために 2 か月強の時間を要してしまった。しかしながら、不幸中の幸いにして、インシデント対応は地震災害を主として作成、運用していた事業継続計画が功を奏し、インシデント対応に円滑に入ることができた。本教訓からの学びとして、既存の事業継続計画を見直し、サイバーセキュリティインシデントも含めた上で、事業継続計画が機能するように半田病院だけでなく、全ての医療機関でも行われるべきである。

また、そもそも電子カルテシステムを導入している時点で、システムの正常動作を優先するあまり、提供事業者からセキュリティレベルを下げる指示や対応が行われていた。さらに、運用においても今回の侵入経路となった VPN の脆弱性に関する情報提供が行われていないことや、Silverlight や ActiveX 前提の電子カルテシステムを提供し、当該情報のサポート切れやセキュリティ上の懸念が示されていないことは、提供事業者または運用事業者として責任を果たしていない。半田病院側の指示や対応に不足があったとしても、事業者は情報の非対称性を理解し、その解消に努めるべきである。

民法改正に伴い改訂された「～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守・運用）〈第二版　追補版〉」（独立行政法人情報処理推進機構）においては、「信頼性の高い情報システムの確保は、ユーザーとベンダーのたゆまない緊密な協働によってのみ得られるとの立場から、取引全般においては、ユーザー自身が役割を理解しベンダーとの緊密な協働を行うことを前提」としており、このような緊密な協働がインシデント発生の事前、事中、事後からも確認することができなかった。

さらに、モデル契約は「ベンダーにおいては、情報システムの知識を有しない企業に対して、業として情報サービスを提供する専門家としての十分な配慮と注意を払う必要と一定の責任があり」と述べており、このような十分な配慮と注意についても不足していたと言わざるを得ない。なお、今回は幸いにしてデータが復元できたものの、フォレンジックを担当した事業者の実施方法や対応内容にも不手際があると共に、上記のような連携や配慮も不足している。

厚生労働省を始めとした政府機関が公開しているガイドラインも、そもそも複数のガイドラインが存在することや、抽象度が高いこと、また ISMS などを前提としているためにハードルが高い内容が示されているなど、ガイドラインそのものにも課題があると言える。また、今回はつるぎ町立の病院で発生したことを鑑

みると、総務省の公立病院経営強化プランなどにも、BCP に必要なリソースを捻出する配慮をすることや、中小企業や公営企業などの IT 弱者に対するモデル契約や実行しやすく、一人でシステム運用を行うような組織においてもより対応しやすい、具体的なガイドラインへの変更や作成が求められる。

今回のインシデントを教訓に、既存のシステムやソフトウェアのポリシーや設定変更で対応できるような技術的な対応も細部にわたってまとめた。サイバーセキュリティは新しい技術や製品などに注目されがちだが、まずは今の環境で最大限行えるセキュリティ対策の強化に努めてほしく、他の組織においても設定変更などの検討が促進されることを願いたい。（なお、当然ながら今回示されている技術的な対策は、半田病院で実施してもらう予定である。）

今回は偶発的に半田病院で発生し、日本全体に本インシデント情報が広まり、注目を集めたが、日本全体を見渡した時に、他の医療機関や公的機関、広くはサプライチェーンにおいても同じような状況と言えるであろう。利用者側の病院もセキュリティ意識を高め、強化することが欠かせないが、事業者は重ねて情報の非対称性が存在し続けていることを理解し、継続的な連携が必要であることを忘れてはならない。

病院は当然ながら医療の専門家であり、医療の知識に長け、医療サービスを提供している。地域住民はそのサービスの安全性を理解し、信じるからこそ医療サービスを享受していることになる。
その視点で言えば、電子カルテシステムを提供する企業やインフラなどの環境を構築する企業、またそれらの運用を行っている企業も、それぞれの担当分野においては専門家であり、知識に長け、利用者に安心して信頼されるサービスを提供する必要がある。

ここ数年間にわたり、サプライチェーンの課題が叫ばれ、国内でも工場や中小企業など、様々な組織でセキュリティインシデントが発生している。その一方でデジタルトランスフォーメーションが叫ばれ、日本はようやく情報技術の活用が活性化している。セキュリティ軽視のデジタルトランスフォーメーションが進めば、日本は近い将来、サイバー攻撃によって日本の産業が大規模に停止する事態が起きる可能性があることを強く認識すべきである。
決して今回のインシデントは対岸の火事ではなく、同様の医療機関、自治体などの公的機関、企業規模関係なく全ての事業者、そして政府機関も、今回のインシデントから学び、改善していかなければならない。今後のガイドラインの策定や、連携の強化も、産官学のより一層の連携強化と旗振り役の統一が必要であり、デジタル庁のようにサイバーセキュリティの旗振りを行う機能が強化されるべきである。

最後になるが、災害級のインシデント発生にもかかわらず、半田病院は患者を最後まで守り切ることができた。これは、半田病院の医師、看護師、職員、関係者の献身的な努力と、地域や自治体、他の医療機関、各事業者の支援によって実現できたことであり、これは最大の賛辞が贈られるべきである。

半田病院の患者情報や命を守る事業が終わることはない。これからも一人でも多くの人や組織の支援によって、地域医療が支えられ、住民の安全や健康につながることを切に願い、括りとする。