2023 年 7 月 25 日

日本医師会総合政策研究機構 委託研究

サイバー事故に関し
システムベンダーが負う責任
: 医療 DX を推進するために

堤　信之（客員研究員）

目次

１．現状認識と問題意識について

昨今、産業界におけるサイバー攻撃の脅威は世界中でいよいよ増大し、悪質化の傾向にある[1]。日本も同様の状況にあり[2]、遂には 2022 年 9 月～11 月末のサイバー攻撃の標的数は世界 2 位であったとのレポートすらある[3]。なお警察庁調査[4]によれば、国内ではサイバー攻撃の中でもランサムウェアによる感染被害が多発し、事業活動の停止・遅延等、社会経済活動に多大な影響を及ぼしているほか、サイバー攻撃や不正アクセスによる情報流出の相次ぐ発生など、サイバー空間における脅威は極めて深刻な情勢が続いている。

医療界も例外ではなく、警察庁調査によれば 2022 年度上期において、医療・福祉分野でのランサムウェア被害件数は 9 件（全産業 114 件のうち 8%を占める）であった。

一方で、医療機関と医療情報システムの構築・運用などの業務を一括して請け負う事業者（以下「システムベンダー」）とは、サイバーセキュリティ対応に関して、それぞれ相互に連携し、自らの責任を果たすこととされているが、一旦有事が発生してしまった場合の相互の責任関係については、必ずしも明確にされていない。また参考となる判例等も見当たらない。

このような環境下、内閣サイバーセキュリティセンター（NISC）より発出された 2021 年 4 月 30 日付通知「ランサムウェアによるサイバー攻撃に関する注意喚起」[5]の中で、Fortinet 製 VPN 装置（CVE-2018-13379）等の脆弱性

---

[1] WIRED「ランサムウェア集団による“オンライン恐喝”が、さらに凶悪化する新局面に突入した」（2023 年 3 月 16 日）https://wired.jp/article/ransomware-tactics-cancer-photos-student-records/

[2] 日本経済新聞（2022）「身代金ウイルス、悪質に　機密暴露の「二重恐喝」6 割」（2023 年 3 月 20 日朝刊）https://www.nikkei.com/article/DGKKZO69413860Z10C23A3CM0000/

[3] BlackBerry（2022）「グローバル脅威インテリジェンスレポート」
https://www.blackberry.com/ja/jp/solutions/threat-intelligence/2023/threat-intelligence-report-jan-jp

[4] 警察庁（2022）「令和 4 年上半期におけるサイバー空間をめぐる驚異の情勢等について」（2022 年 9 月 15 日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

[5] 4 頁に抜粋を掲載。https://ajhc.or.jp/siryo/20210430-4.pdf

が、具体名を明示して指摘された。厚生労働省ではこれを受け、各都道府県衛生主管部を通じて医療機関に周知すべく、同年 6 月 28 日及び 11 月 26 日の 2 回に亘り、通知を発出した[6]。しかし医療機関への周知は徹底されておらず、医療機関と医療情報システムの保守契約を結び当該 VPN 装置を設置したシステムベンダーからも脆弱性に関する情報提供がなされないまま、同装置の脆弱性を突いたサイバー事故*5 [頁注 1] が同年 10 月以降、頻発した（本稿では「特定類型のサイバー事故」と称する）。

特に、徳島県つるぎ町半田病院でのサイバー事故（2021 年 10 月末発生）では、Fortinet 製 VPN 装置の脆弱性を突かれたことが広くマスコミ報道され世間の注目を集めたにもかかわらず、その後も同じ Fortinet 製 VPN 装置の脆弱性を突かれた事故が立て続けに発生している。

当該 Fortinet 製 VPN 装置は、医療機関にかなり広く採用されているとの情報もあり、未だに脆弱性への対策が取られないままの医療機関が存在することが懸念される*5 [頁注 2]。

そこで、本稿ではまずは医療機関、システムベンダーそれぞれのサイバーセキュリティ対応に関する責任を整理し、加えて、並行して実施した医療機関に対するサイバー攻撃（ランサムウェア）事案における医療機関、システムベンダーの関係の実態を概観し、両者相互の責任関係に関する問題意識を提示したい。

---

[6] 厚生労働省医政局研究開発振興課 医療情報技術推進室 事務連絡「医療機関を標的としたランサムウェアによるサイバー攻撃について（再注意喚起）」（2021 年 11 月 26 日）
https://www.city.kawagoe.saitama.jp/jigyoshamuke/hokeneisei/jigyosha/iryoukikan/iryoukikannhenotuti3.files/R3.11.24rannsamu.pdf

内閣サイバーセキュリティセンター（NISC）による注意喚起【抜粋】

チェックポイント

- インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を十分検討したうえで、セキュリティパッチを迅速に適用する、外部からの管理機能、不要なポート(137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、3389(TCP/UDP)など)やプロトコルを外部に開放しない等の対応策等、IT資産管理を改めて確認する。特に、通信プロトコル「SMB」や「RDP」については、これまでも必要最小限のポートの開放やSMBv1の無効化等を呼びかけているところ、ファイアウォールを含む各機器の設定を改めて確認する。
- ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - Fortinet製Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)[2]
  - Ivanti製VPN装置「Pulse Connect Secure」の脆弱性(CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)[3]
  - Citrix製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)[4]
  - Microsoft Exchange Serverの脆弱性(CVE-2021-26855等)[5]
  - SonicWall Secure Mobile Access (SMA) 100シリーズの脆弱性(CVE-2021-20016)[6]
  - QNAP Systems製NAS(Network Attached Storage)製品「QNAP」に関する脆弱性(CVE-2021-28799、CVE-2020-36195、CVE-2020-2509等)[7]
  - Windowsのドメインコントローラーの脆弱性(CVE-2020-1472等)[8]
- テレワーク等に関連し、職場から持ち出したPCについて、休暇中に長期間、十分な管理下になかったPCを職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。
- 最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」に感染させる不正なメール等も確認されていることから、ウイルス対策ソフトの導入及び最新化、定期スキャンの実施、メール環境に対するセキュリティ対策等、通常のマルウエア対策も実施する。

資料：内閣官房　内閣サイバーセキュリティセンター（2021）「ランサムウエアによるサイバー攻撃に関する注意喚起について」p.2

＊注１：アクセスポイントの脆弱性を攻撃しデータセンターや IT 環境に侵入したら、次に認証情報の窃盗やフィッシング攻撃を通じて盗んだログイン認証情報を使用して正規ユーザーになりすまし、より深くシステムに侵入することで、機微な情報や知的財産などの価値の高い資産にアクセスしこれを窃取、悪用するという流れが一般的である。

＊注２：2022 年 1 月、厚生労働省により病院団体に対する調査「病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査について」[7]が実施され、VPN 装置の有無、存在する場合の同装置の詳細情報が把握されたが、診療所については把握できていない。

なお医療機関において VPN 装置が使われるケースは主に以下の２つであり、診療所にも該当する。

① 医療情報システムの保守点検等を目的とし、事業者とシステム接続する場合

② 訪問診療等、医療情報システム外で医療データを活用するため専用端末を使用する場合

[7] 調査依頼（1 月）：http://www.hospital.or.jp/pdf/15_20230127_01.pdf
調査結果（3 月）：https://www.mhlw.go.jp/content/10808000/000918813.pdf

２．本稿の目的

ソフトウェアや機器等の脆弱性が悪用され、医療機関がサイバー攻撃を受けた場合、医療機関には以下の損害の発生が想定される。

① 被害が生じたシステム、端末、データベース等の復旧や事業継続に要する費用等の損害。

② 患者（健診受診者含む）に影響(個人情報漏洩等)が及び、損害賠償責任を負った場合の損害。

本稿では、特定類型のサイバー事故において、上記①②に関する医療機関と保守契約の当事者であるシステムベンダーそれぞれの責任分担の適正な在り方を、明らかにする。

３．考察の手順

サイバー攻撃を受けた3つの医療機関のランサムウェア感染事例について、日医総研によるインタビュー調査[8]が2022年度に実施された。何れのケースも、2021年4月30日付内閣サイバーセキュリティセンター・重要インフラグループ発信「ランサムウェアによるサイバー攻撃に関する注意喚起」において公表され、「ソフトウェアや機器等の脆弱性」が機器を特定して指摘されていたFortinet製VPN装置（CVE-2018-13379）に起因したサイバー攻撃であった。

その調査結果と、事故報告書が公表されている徳島県つるぎ町半田病院の事例を加えた4医療機関について明らかになった実態は、以下(1)～(3)の通りであった。

なお、何れの事例でも、患者等の個人情報漏洩の事実は確認されていない。

また、時系列で整理すると、4事例とも上記情報公表後（2021年4月30日～）に発生し、さらに言えば、うち2事例は、徳島県つるぎ町半田病院へのサイバー攻撃が事件として報道された後（2021年10月末～）に発生した。

（1） 医療機関とシステムベンダーとの間の保守契約上、医療情報システムに係るソフトウェアや機器等のサイバーセキュリティ上の脆弱性（以下「当リスク」）に関する情報の通知義務が明記されている医療機関はなかった。

（2） 上記情報公表から事故発生までの期間において、システムベンダーが事前に医療機関に上記情報を知らせていたのは1事例だけであった。

（3） サイバー攻撃により医療機関に発生した直接の損害について、システムベンダーがその一定割合を負担したのは1事例だけであった。

---

[8] 日医総研（2022）リサーチレポート No.136「医療機関へのサイバー攻撃の事例研究：民間病院・診療所の被害事例に学ぶ」（2023 年 4 月 11 日）

上記実態を踏まえ、これらをモデルケースとして、医療機関とシステムベンダーの責任分担の適正な在り方に関し、以下の論点について考察する。

① Fortinet 製 VPN 装置の脆弱性が周知された環境下、保守契約当事者であるシステムベンダーの不作為（医療機関への情報提供なし）のうちに当リスクを突かれ、サイバー事故が発生した場合には、保守契約上、係るリスクの通知義務や対策提案義務が明記されていないとしても、システムベンダーの医療機関に対する一定の責任を問うべきではないか。

② 上記①同様に、個人情報漏洩事案が発生した場合も同様に、保守契約上、当リスクの通知義務や対策提案義務が明記されていないとしても、システムベンダーの医療機関に対する一定の責任を問うべきではないか。

４．考察

ソフトウェアや機器等の脆弱性が悪用され、医療機関がサイバー攻撃を受けて医療機関に損害が発生した場合の、医療機関とシステムベンダーの責任関係については、基本的には両者間で締結されたシステム保守契約の規定による。

保守契約上の規定がない場合には、法令上の解釈による判断となる。

４－１．保守契約上のシステムベンダーの責任

システム保守契約上、システムベンダーに当リスクにかかる情報提供義務が明記されている場合、または、保守契約上の明記がない場合であっても、契約時の経緯や保守契約料金の妥当性等から、当事者双方に当リスクにかかる情報提供義務をシステムベンダーが負う意思があったと認定できる場合であれば、システムベンダーが医療機関に対して負う善管注意義務（民法第 644 条、同 656 条）違反を問うことができる*以下注３。

しかしながら、本稿で参考とした 4 事例もそうであったように、保守契約に、当リスクにかかるシステムベンダーの情報提供義務が明記されていることは少ないと考えられる。また、保守契約上の明記がない場合に、黙示で情報提供義務をシステムベンダーが負っていると認定されるためのハードルは高いと思われる。

従って、保守契約上の善管注意義務違反を理由にシステムベンダーの責任を問えるケースは、実態としては極めて少ない現状にあると推察される。

＊注３：システム保守契約（システムを本番運用した後、問題が発生した場合の迅速な復旧や、システム改良の要望に応えてもらうために締結）は、仕事の完成

や成果物がないため、「請負契約」※ではなく、業務自体を委託する「準委任契約」※となることが一般的である。委任契約・準委任契約の受任者は、委任者に対して善管注意義務（善良な管理者の注意をもって、委任事務を処理する義務）を負う（民法 644 条、656 条）。

契約種類	仕事の完成や成果物	受託者の責任
委任契約（法律行為の委託）	なし	善管注意義務
準委任契約（事実行為の委託）	なし	善管注意義務
請負契約	あり	契約不適合責任

※委任契約、準委任契約、請負契約について

・委任契約（民法 643 条、旧民法 643 条）

当事者の一方が法律行為をすることを相手方に委託し、相手方がこれを承諾することによって、その効力を生じる。

・準委任契約（民法 656 条）

委任契約と民法上同じルールが適用される契約類型であるが、委任契約が法律行為を委託するのに対し、準委任契約は、事実行為（事務処理）の委託をする契約という違いがある。

・請負契約（新 632 条※旧民法でも同じ）

当事者の一方がある仕事を完成させることを約し、相手方がその仕事の結果に対して報酬を支払うことによってその効力を生じる。売買契約の規定が準用され、請負人は注文者に対して「契約不適合責任」を負う（民法 559 条、562 条以下）。

続いて法令上の責任について考察する。

４－２．システムベンダーの法令上の責任

特定類型のサイバー事故におけるシステムベンダーの法令上の責任について、筆者見解は次の通りである。

(1)医療機関とシステムベンダーで締結したシステム保守契約において、当リスクにかかるシステムベンダーの情報提供義務が明記されていないとしても、経済産業省ガイドライン等に照らし、医療機関とシステムベンダーのセキュリティに関する専門性の格差を鑑み、既に攻撃手法が知られて実際に被害も発生しているような顕在化率が極めて高い状況下では、システムベンダーは医療機関等に対し、委託契約又は信義誠実の原則（以下「信義則」）＊次頁注４に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために必要な情報を適時適切に提供する義務を負うと考える。

(2)従って、医療機関と医療情報システムの保守契約を結び Fortinet 製 VPN 装置（CVE-2018-13379）を設置したシステムベンダーから、医療機関に対し当該装置の脆弱性に関する情報提供がなされないまま、当該装置の脆弱性を突いたサイバー事故が発生した場合には、医療機関から保守契約の当事者であるシステムベンダーに対し、「信義則」違反を理由に一定の責任を問える可能性があると考える[9]。

(3)特定類型のサイバー事故で患者等の個人情報漏洩が発生し、医療機関が患者等に対し損害賠償責任を負ったことにより医療機関に発生した損害についても、考え方は上記同様である。

---

[9] 兼子･岩松法律事務所・木﨑孝弁護士から同様の見解を得ている。

＊注４：「信義誠実の原則」（信義則）とは、当該具体的事情のもとで、相互に相手方の信頼を裏切らないよう行動すべきであるという法原則のことで、民法第１条第２項では、「権利の行使及び義務の履行は、信義に従い誠実に行わなければならない。」と規定されている。信義則は、上記の倫理的な法原則を注意的に規定したものであるので、他の条項で解決できないときの最後の手段として利用される。

なお、医療機関とシステムベンダーで締結したシステム保守契約上、当リスクにかかるシステムベンダーの情報提供義務が明記されていない場合に関わるシステムベンダーの法令上の責任を考察するにあたり、厚生労働省（2021）「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　本編、別冊編」（2022 年 3 月）[10]（以下、「厚生労働省ガイドライン」）と、「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」（経済産業省；令和 4 年 8 月改定）[11]（以下、「経済産業省ガイドライン」）の規定が参考資料として重要であるので、以下で触れる。

・厚生労働省ガイドラインでは、医療に関わる全ての行為は医療法等で医療機関等の管理者の責任で行うことが求められていることを踏まえつつ、電子化された医療情報が、医療機関等の空間的境界を越えてネットワーク上に広がって存在するようになってきたことを鑑み、医療情報の管理責任は、医療機関等のみならず、ネットワークを介したサービスを提供する事業者やネットワークを提供する通信事業者、伝送先の医療機関等それぞれの「責任分界点」に応じ、

[10] 厚生労働省（2021）「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　本編、別冊編」（2022 年 3 月）
https://www.mhlw.go.jp/content/10808000/000936160.pdf
https://www.mhlw.go.jp/content/10808000/000923624.pdf
[11] 経済産業省（2022）「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」（令和 2 年 8 月；令和 4 年 8 月改定）
https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20220831.pdf

予め可能な限りの事態を想定し、各者の責任の分担について明記しておくこととされている。

（抜粋）

厚生労働省「医療情報システムの安全管理に関するガイドライン 第5.2版」

（令和4年3月）

責任分界について（4.2章）

【委託の場合】

（1）通常運用における責任の考え方

○管理責任の主体である医療機関等の管理者が患者に対し責任を果たす義務を負う。

○受託する事業者は医療機関等の管理者に対し、情報提供等の説明責任がある。

○医療機関等の管理者は、受託する事業者の管理実態を理解し、その監督を適切に行う。

○管理状況を定期的に見直し改善を行う責任の分担について契約事項に含めておく。

○予め可能な限りの事態を想定し各者の責任の分担について契約事項に含めておく。

（2）事後責任の考え方

○医療機関等の管理者は、受託する事業者の選任監督に十分な注意を払っている場合でも、患者に対しての善後策を講ずる責任を免れることはできない。

○しかしながらその責任の分担の程度等については別途考慮する必要があり、受託する事業者が原因で事故が生じた場合、最終的には受託する事業者が損害填補責任等を負うのが原則であり、医療機関等の管理者がすべての責任を負うことは原則としてあり得ない。

○事故発生時は原因追及や再発防止策を優先させることを委託契約に明記しておく。

○原因の程度等や、保険による損害分散の可能性などを考慮した上で、損害填補責任の分担について委託契約に明記しておく。

・経済産業省ガイドラインでは、システムベンダーすなわち医療機関等との契約等に基づいて医療情報システム等を提供する事業者は、本ガイドライン対象事業者とされており、「セキュリティに関する専門家としての義務」、「影響度、顕在化率の高い状況下でのリスク回避義務」といった責任が謳われている（以下、経済産業省ガイドラインより抜粋。採番①②括弧の標題は筆者が要約）。

① （セキュリティに関する専門家としての義務）

医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべきである。このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために 必要な情報を適時適切に提供する義務を負う。

② （影響度、顕在化率の高い状況下でのリスク回避義務）

サイバー攻撃においては、インターネット経由で直接的な攻撃が可能である場合や、認証を要求していない場合、既に攻撃手法が知られており被害が発生している場合等は、顕在化率（リスクが顕在化する可能性）は高いと考えられる。対象事業者は、影響度及び顕在化率ともに極めて高いリスクについては、リスク回避を検討すること。

ただし、上記のいずれのガイドラインにおいても、医療機関とシステムベンダーの相互の責任関係については直接触れられていない。

５．今後の課題と提言

（1） 特定類型のサイバー事故回避のための方策

装置のセキュリティ上の脆弱性が指摘されている Fortinet 製 VPN 装置（CVE-2018-13379）が設置されている全ての医療機関に対し、個別に注意喚起することで、事故の回避を図ることが急務である。

2022 年 1 月に厚生労働省により実施された病院団体に対する調査「病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査」[12]結果を活用し、該当する病院に対し行政として個別にフォローすべきである。

なお行政には、システムベンダー側に対しても、システムベンダー自身の責任として適正に対処するよう指導することを期待したい。

（2）システム保守契約の取扱い

① 行政による資金面の支援が必要

保守契約への責任分界点[13]の明文化（サイバーセキュリティ対策に関するサービス[14]提供を明記）に伴い、医療機関に発生する保守契約料金増額相当の資金面での支援（診療報酬上の加算等）を、行政が積極的に行うべきである。

---

[12] 本稿 5 頁注 2 脚注 7 参照。
調査依頼：http://www.hospital.or.jp/pdf/15_20230127_01.pdf
調査結果：https://www.mhlw.go.jp/content/10808000/000918813.pdf
[13] 13 頁厚生労働省ガイドライン参照。
[14] 当リスクにかかる情報提供サービス、リモート監視サービス、障害復旧支援サービス、受付窓口サービス、報告・分析サービス等が考えられる。

保守契約では、システムベンダーの役務として、概ねシステム開発・導入費用の 15%程度の料金[15]で、定期保守点検に加え、開発･導入したシステムのソフトウェアにバグ等のトラブルが発生した場合や各種端末等のハードウェアの調子が悪い時の対処、データのバックアップ処理等について規定されることが一般的であり、サイバーセキュリティ対策に関するサービスを明記することは少なかったと思われる。この実態に照らし、医療機関としては、システムベンダーからのサイバーセキュリティ対策関連サービスの提供を保守契約上に明記したいところであるが、他方で、システムベンダーとしては応分の保守契約料金の増額を医療機関に対して求めることが予想される。

医療 DX の推進を図る上でサイバーセキュリティ対策は避けて通れない重要なテーマであり、その対策に要する費用負担の問題が原因で、両者の円滑な関係構築を阻害するような事態は、絶対に避けなければならない。ついては、上記費用負担を行政による支援（診療報酬上の加算等）で行うべきと考える。

なお、保守契約にサイバーセキュリティ対策にかかるサービスをどこまで含めるかによって料金は大きく変わり、広く含める場合の料金は従来の数倍から数十倍になることも想定される*次頁注 5。まずはシステムベンダーの「経済産業省ガイドラインの遵守」を明記した保守契約を標準形とする取組から着手し、従来型契約に追加されるサービスを「当リスクにかかる情報提供」に限ることで料金の増額を抑える一方で、将来に亘り毎年発生し続ける費用であることを鑑み、当該増額相当を公的支援の対象とすることも一案と考える。

---

15 例えば診療所への電子カルテの概算の導入費用は 1 システム 300～450 万円、年間保守費用は 45～70 万円程度と言われている。
システム保守とは？費用っていくらかかるの？コスト削減方法も知りたい - システム開発のプロが発注成功を手助けする【発注ラウンジ】 (hnavi.co.jp)

＊注５：保守契約にサイバーセキュリティ対策関連サービスを幅広く含める場合の概算の追加料金（年間）の一例は次の通り。

・診療所の場合；120 万円

⇒外来患者数 30 人／日とすると 1 患者当たり約 162 円

∵120 万円÷(30 人×247 日･･･2023 年の土日祝日を除く日数)

・病院（病床数 200 床）の場合；1,500 万円

⇒入院、外来患者数それぞれ 180 人／日とすると 1 患者当たり約 136 円

∵1,500 万円÷（(180 人×365 日)＋(180 人×247 日)）

② 「サイバー攻撃免責条項」への注意が必要

各業界でのサイバー攻撃の多発を受け、取引先へのサイバー攻撃の影響がサプライチェーンを通じて自社に及ぶリスクに対する意識が高まっている。一部報道によれば、サイバー防衛策として「サイバー攻撃免責条項」（当事者にどうすることもできない事象の発生によりサービス提供等が出来なくなった場合に賠償責任を負わないことを定める「不可抗力条項」の発動条件に「サイバー攻撃」を明記）の導入といった動きがある[16]。システムベンダーにおいてもサイバーセキュリティ問題の意識が高まる中で、保守契約上に同条項を採用したいとの申し入れを医療機関が受ける可能性があるが、同条項があると、システムベンダーの信義則違反の判定結果に影響を及ぼす可能性があると考えられるので、医療機関としては慎重な対応が必要である。

（3）特定類型のサイバー事故における医療機関とシステムベンダーの責任分担

[16] 日本経済新聞朝刊（2022）「契約書もサイバー防衛／損害や調査費の負担、事前に取り決め」（2022 年 10 月 17 日）
https://www.nikkei.com/article/DGKKZO65134640U2A011C2TCJ000/

割合の明確化

特定類型のサイバー事故において、あくまで医療機関とシステムベンダーの責任分担割合の決定は個別事案毎の総合的な判断によると思われる。予め一定の判断基準を示すことも、医療機関とシステムベンダーの間で責任問題が争われた事例自体がほとんど知られておらず、両者の責任分担割合についても知見が積み上がっていない現段階では困難であり、今後の研究課題と思われる。ただし、医療情報の取扱いを含めた医療に関わる全ての行為は医療法等で医療機関等の管理者の責任で行うことが求められていることに照らせば、システムベンダーが 100%の責任を負う可能性は極めて低いことに留意する必要がある。

（4）その他のサイバー事故における医療機関とシステムベンダーの責任関係等について

特定類型のサイバー事故では、「既に攻撃手法が知られ被害が発生しており顕在化率が極めて高い」という特殊な事情が、適切な情報提供を怠ったシステムベンダーの不作為を信義則違反と判断する大きな要素になると考えた。このような特殊事情が認められない環境下でのサイバー事故について、医療機関とシステムベンダーとの責任関係の判断基準は今後の研究課題である。

また、システムベンダー以外の関係者（医療機器製造販売業者等）との責任関係の整理も同様である。

参考文献・資料[17]

・経済産業省（2022）「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」（令和 2 年 8 月；令和 4 年 8 月改定）
https://www.meti.go.jp/policy/mono_info_service/healthcare/01gl_20220831.pdf

・警察庁（2022）「令和 4 年上半期におけるサイバー空間をめぐる驚異の情勢等について」（2022 年 9 月 15 日）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf

・厚生労働省（2021）「病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査について」（2022 年 1 月）
調査依頼（1 月）：http://www.hospital.or.jp/pdf/15_20230127_01.pdf
調査結果（3 月）：https://www.mhlw.go.jp/content/10808000/000918813.pdf

・厚生労働省（2021）「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　本編、別冊編」（2022 年 3 月）
https://www.mhlw.go.jp/content/10808000/000936160.pdf
https://www.mhlw.go.jp/content/10808000/000923624.pdf

・日医総研（2022）リサーチレポート No.136「医療機関へのサイバー攻撃の事例研究：民間病院・診療所の被害事例に学ぶ」（2023 年 4 月 11 日）
https://www.jmari.med.or.jp/wp-content/uploads/2023/04/RR136-2.pdf

・内閣官房　内閣サイバーセキュリティセンター（2021）「ランサムウエアによるサイバー攻撃に関する注意喚起について」p.2
https://ajhc.or.jp/siryo/20210430-4.pdf

・日本経済新聞朝刊（2022）「契約書もサイバー防衛／損害や調査費の負担、事前に取り決め」（2022 年 10 月 17 日）
https://www.nikkei.com/article/DGKKZO65134640U2A011C2TCJ000/

[17] リンク先参照資料については、アドレス変更等によるリンク切れの場合もあること、お含み置き願う。

・日本経済新聞（2022）「身代金ウイルス、悪質に　機密暴露の「二重恐喝」6割」（2023 年 3 月 20 日朝刊）
https://www.nikkei.com/article/DGKKZO69413860Z10C23A3CM0000/

・BlackBerry（2022）「グローバル脅威インテリジェンスレポート」
https://www.blackberry.com/ja/jp/solutions/threat-intelligence/2023/threat-intelligence-report-jan-jp

・WIRED「ランサムウェア集団による“オンライン恐喝”が、さらに凶悪化する新局面に突入した」（2023 年 3 月 16 日）
https://wired.jp/article/ransomware-tactics-cancer-photos-student-records/