TOKIO MARINE

リスクマネジメント最前線

2023 | No. 2

医療機関におけるサイバーリスク

サイバーセキュリティ事業部　三宅　諒介研究員（専門分野：サイバーセキュリティ）

2021 年 10 月 31 日に徳島の病院で大規模なランサムウェア[1]インシデントが発生した。電子カルテなどのデータが暗号化され、利用不能の事態に陥った。また、まさにその 1 年後の 2022 年 10 月 31 日には、大阪の病院にて同様のランサムウェアインシデントが発生した。どちらの事例も通常診療に復帰するのに 2 カ月以上の時間を要し、治療行為を始めとした病院業務に甚大な影響を及ぼした。このような有名なインシデント以外にも、医療機関を標的とするサイバー攻撃は規模に関係なく多数発生している。全ての医療機関にとってサイバー攻撃に遭うリスクは他人事ではない。

そこで本稿では、医療機関におけるサイバーリスクをリスクの因子である脅威、脆弱性、事業への影響の順で概観した後に、医療機関が取るべきセキュリティ対策についてリスクマネジメントのフレームワークに依拠しつつ紹介する。

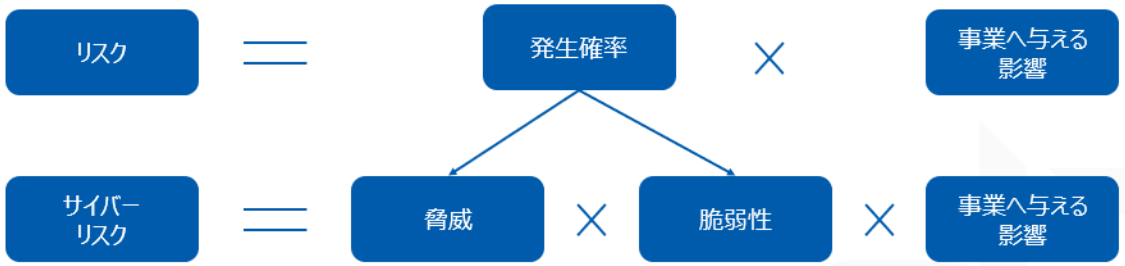
1. 医療機関におけるサイバーリスク

(1) サイバーリスクの考え方

リスクは一般的に図表 1 の上段の公式で算出される。しかし、サイバーリスクの場合、発生可能性を脅威と脆弱性という 2 つの因子に分解して考えることができるため、サイバーリスク算出の公式は図表 1 の下段のものに置き換えることができる。本章では、図表 1 の下段の公式を基に、各リスク因子に着目し、医療機関を取り巻くサイバーリスクを概観する。

[1] ランサムウェア(Ransomware)とは、悪意のあるソフトウェア(Softwaare)の呼称となるマルウェア(Malware)の一種である。ファイルを暗号化してデータ所有者からアクセス権を奪取し、データの復元と引き換えに金銭を要求(脅迫)することから、身代金を意味する Ransom と Software を合わせて Rasomware と名付けられた。また、近年では金銭を支払わなかった場合、窃取した情報を流出させると脅迫する、所謂「二重の脅迫」を行う事例も増えている。

■ 図表 1 リスク算定の公式



出典：弊社作成

(2) 医療機関における脅威について

脅威には自然災害なども含めて多くのものが存在しているが、医療機関におけるサイバー脅威の代表例として、攻撃者の存在が挙げられる。では、なぜサイバー攻撃者は医療機関を標的に攻撃を行うのであろうか。サイバー攻撃者の目的別の類型に依拠しつつ考察していきたい。

サイバー攻撃者を目的別に類型化すると、概ね以下の四つに大別される。①マフィアなどの「金銭窃取」を目的とする者、②産業スパイなどの「情報窃取」を目的とする者、③政治犯・愉快犯などの自らの「思想の主張」を目的とする者[2]、④国家主導による「国益」を目的とする者。上記の四つの類型の内、どの攻撃者が医療機関にとっての脅威となり得るだろうか。結論としては、全ての攻撃者が医療機関にとって脅威となり得る。だが、特に注意を払う必要があるのは①「金銭窃取」を目的とする者及び②「情報窃取」を目的とする者である。

①「金銭窃取」を目的とする攻撃者が標的を選定する際に重視するのは、被害者が金銭を支払う可能性の高さである。医療機関はその点において、非常に魅力的な標的である。なぜなら、ランサムウェアなどのサイバー攻撃によって医療システムが停止することは、人命に関わる事態であり、一般企業におけるシステム停止と比較して、その被害のインパクトが甚大だからである。攻撃者側から見て、医療機関は一般企業よりも自身の要求に屈し易く見えることは想像に難くない。続いて②「情報窃取」を目的とする者から見た場合だが、これは医療機関が扱う情報の性質に関係している。医療機関が取り扱っている診療情報、病歴、ゲノム情報は、改正個人情報保護法において特に取り扱いに注意が必要な要配慮情報に位置づけられる。特にゲノム情報は、個人の固有性を担保する究極の個人情報である。クレジットカード情報やマイナンバー情報は、窃取されたとしても再発行が可能だが、ゲノム情報は流出してしまったら最後、書き換えや再発行を行うことができない。まさに「取り返しのつかない情報」である。医療機関が取り扱っている情報は、情報それ自体の価値が高く、また被害を受けた際にリカバリーすることができない性質のものである。このように、サイバー攻撃者の目線に立って考えてみた場合、医療機関は非常に魅力的な攻撃対象となっている。

また、サイバー攻撃者の存在が医療機関にとって非常に厄介なものとなっていることの要因の一つに、彼らをコントロールすることができないことがある。セキュリティ対策を講じることによって、サイバー攻撃の被害に遭う確率を下げることは可能であったとしても[3]、サイバー攻撃者が攻撃の意思を持つことを医療機関が直接的に妨げることはできない。そのため、医療機関がどれだけセキュリティ対策を実施したとしても、そのセキュリティ対策のコントロール外の領域にサイバー攻撃者が存在していることになる。サイバー攻撃者の存在は医療機関にとってコントロール不能であり、その存在を根絶することは困難である。

[2] ハクティビスト(Hacktivist)と呼称される。Anonymous が代表的な例である。

[3] こちらは脅威への対応ではなく、脆弱性への対応となる。

(3) 医療機関における脆弱性について

前述の通り、サイバーリスクの因子の一つである脅威は医療機関においてコントロールすることができない。そのため、サイバーリスクの発生可能性を低減させるには、もう一つの因子である脆弱性を低減させる他ない。本項では、医療機関における脆弱性の問題について考えていきたい。

脆弱性とは、脅威によって悪用される可能性のある弱点のことを指す。脆弱性には様々なものが存在する。機密情報を取り扱うルールの欠如といった人間を介在する脆弱性があれば、OS やソフトウェアに存在するセキュリティ上の問題といった技術的な脆弱性も存在する。技術的な脆弱性は日々新規の脆弱性が公開されており、既に世間に対して公開されている脆弱性を既知の脆弱性と呼ぶ。既知の脆弱性は、その存在が公開されているため、攻撃者によって悪用されるリスクが非常に高い。そのため、修正用のプログラムを適用するなど、攻撃者によって脆弱性を悪用されないうちに対策を実施する必要がある。

しかし、昨今の医療機関におけるサイバーインシデントの多くは、この既知の脆弱性に対する対策を怠っていたが故に発生している。冒頭に紹介した徳島と大阪の病院の事例は、いずれも VPN 機器の既知の脆弱性を悪用されたことが要因であった[4]。徳島の事例における報告書では、脆弱性への対応が行われなかった理由として、医療システムの利便性を優先し、セキュリティ上のアップデートを怠っていたこと、IT 担当者が 1 名しかおらず、脆弱性情報の収集や脆弱性対策を講じる人的リソースが欠如していたことが挙げられる[5]。推測にはなるが、このような状況は全国の医療機関で多発しているのではないだろうか。利便性を重視したセキュリティ対策の軽視や、人的リソースの欠如などによる既知の脆弱性の放置は、機密情報の漏洩や事業停止が発生しても影響が全くない組織であればそのリスクを許容できるかもしれないが、医療機関の場合はそうはいかない。脅威がコントロール不可能である以上、サイバーインシデントの発生可能性を低減させるためには脆弱性への適切な対応が求められている。

(4) サイバーインシデントが企業に与える影響

リスク算出の 3 つ目の因子は、事業への影響である。本項では、医療機関がサイバー攻撃の被害に遭った際の影響について、考え得る 5 つの影響を紹介する。

第一に考えなければならない影響は、人命に関する問題である。医療機関がサイバー攻撃によって事業継続が困難となった場合、最悪のケースでは患者の生命に関わる事態となる。2020 年 9 月、ドイツの大学病院では、医療データがランサムウェアによって暗号化され、当該病院へ搬送中だった患者の受入れができなくなった。その患者は別の病院へ搬送中に不幸にも亡くなってしまった。この事例は、ランサムウェアによって人の命が奪われてしまった最初のケースと言われている[6]。

第二に、医療機関がサイバー攻撃によって事業停止した場合、地域医療の提供体制に大きな影響を及ぼすことが考えられる。徳島の事例も大阪の事例も、通常診療へ復帰するのに 2 カ月もの時間を要した。警察庁の調査[7]によると、ランサムウェア被害からの復旧に要した時間で最も多いのは 1 週間～1 カ月以内で 30%、2 カ月以上の時間を要したケースも存在している（図表 2）。被害に遭った医療機関の事業が復旧するまでの間、近隣の他の医療機関がその機能を補う必要が生じる。医療機関の数が限られてくる地方自治体においては、その影響の度合いは計り知れない。特に今後は地域医療構想に代表されるように、病院の機能分化及び統廃合が加速していくことが予想される。各病院の事業継続の重要性は今後ますます増大することになるだろう。

第三の影響として、病院への信頼の低下が考えられる。医療機関がサイバー攻撃を受け、機密情報が漏洩した場合、病院の信頼の低下は免れないだろう。脅威の事項でも前述したが、病院が扱う診療記録や病歴は、改正個人

[4] 半田病院の事案は脆弱性「CVE-2018-13379」が悪用されたものと考えられている。
[5] 『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、9 頁-16 頁を参照。
[6] ランサムウェアインシデントと当該患者が亡くなったことについての因果関係については、賛否両論存在している。
[7] 警察庁『令和 4 年上半期におけるサイバー空間をめぐる脅威の情勢などについて』を参照。

情報保護法が定める要配慮情報に該当する。要配慮情報は不当な差別などに繋がる恐れがある情報であり、取扱いには特に注意が必要である。当然このような情報が漏洩した場合、その病院に対する社会的評価が大きく低下することは想像に難くない。

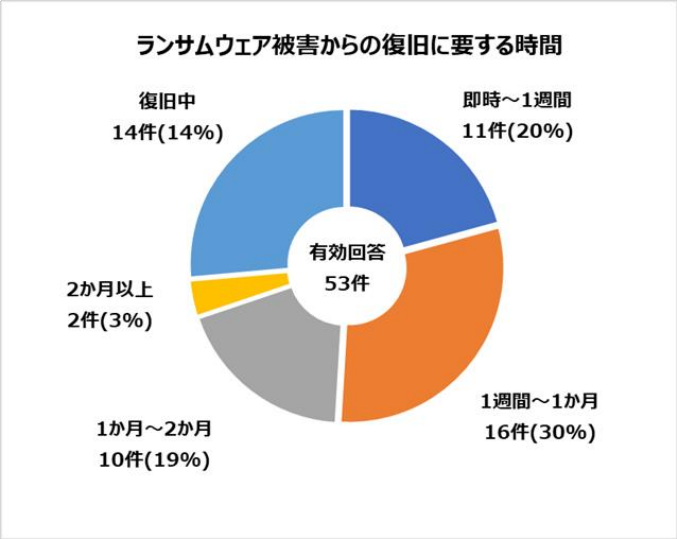
第四に、サイバーインシデントの発生による金銭的影響について取り上げる。第一に考えるべき金銭的影響は、事業停止に伴うキャッシュフローへの影響であろう。電子カルテや医事会計システムがランサムウェアによって暗号化された場合、診療報酬の計算ができなくなり、患者や国に対する診療報酬の請求が停止する。システム停止が長期化した場合、医師や職員への給料の遅配などの経営問題につながりかねない。また、その他の金銭的影響として、インシデントの対応に係る費用が挙げられる。原因分析や復旧・再発防止、対外対応などに外部の専門機関の協力を要請した場合は、当然その対応費用が発生する。例えば、被害の原因調査や再発防止策の策定に際して、デジタルフォレンジック調査[8]を行う場合が多い。パソコン 1 台をデジタルフォレンジックする際に掛かる費用は平均 200 万円程度で、調査する端末の台数に乗じて金額が増大する。また、警察庁の調査によると、ランサムウェアの感染からの復旧に要した金額として、最も大きい割合を占めたのは 1,000 万円～5,000 万円である（図表 3）。徳島の事例ではシステム復旧に約 2 億円もの費用を要したと報道されている。このように、サイバーインシデントへの対応には莫大な金額を必要とし、一時的に経営に大きな影響を及ぼす可能性がある。

サイバーインシデントが医療機関に与える影響として最後に着目したいのが、職員への影響である。インシデント対応は高いプレッシャーとストレスがかかる仕事である。状況が沈静化するまでは、通常業務に優先してインシデント対応に追われ、個人情報の漏洩などが発生した場合は漏洩被害者からの問合せ対応や謝罪対応の矢面に立つことになる。また、ランサムウェアインシデントは社会的関心も高く、その被害対象が医療機関ともなるとメディアからの取材依頼が寄せられ、記者会見などを開かざるを得ないケースもある。このようなことを通じて、職員のモチベーションの低下や、所属組織への不信感の醸成など、職員の休職・退職に発展する可能性もある。

このように、医療機関にサイバーインシデントが発生した場合、多くの影響が生じることが予想される。そのため、医療機関には適切なセキュリティ対策を講じることによって脆弱性を低減させ、サイバーリスクを低減することが求められている。

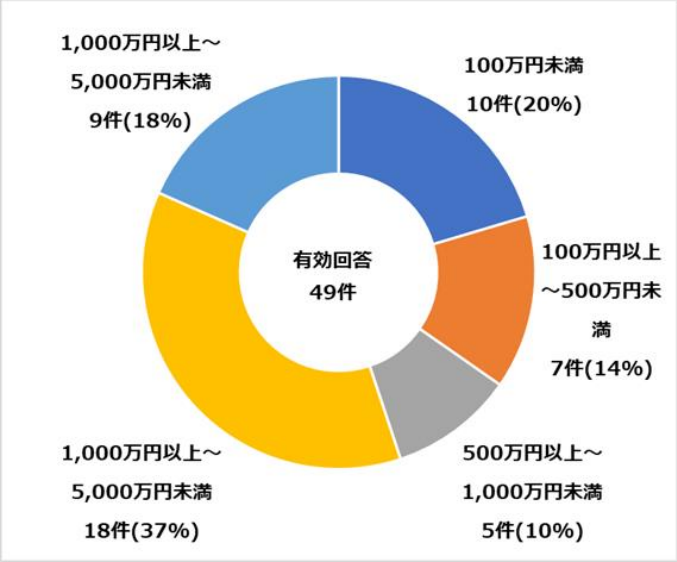
[8] デジタルフォレンジック(Digital Forensics)とは、サイバー攻撃等を受けた際に、デジタル機器に記録された情報の回収と分析などを行うことを指す。その主な目的は、原因究明、事件捜査、訴訟の証拠保全及び分析、不正行為防止等がある。

■ 図表２ ランサムウェア被害からの復旧に要した時間



出典：警察庁『令和４年上半期におけるサイバー空間をめぐる脅威の情勢などについて』

■ 図表３ ランサムウェア被害発生時の調査・復旧費用の総額



出典：警察庁『令和４年上半期におけるサイバー空間をめぐる脅威の情勢などについて』

2.医療機関に求められるセキュリティ対策

これまで見てきた通り、医療機関は脅威となるサイバー攻撃者から狙われやすく、かつ被害に遭った際の影響も大きい。すなわち、医療機関は高いサイバーリスクに曝されており、適切なセキュリティ対策を行う必要がある。しかし、医療機関の多くがセキュリティ対策を推進していくだけの十分なリソースに恵まれているわけではないだろう。予算・人員などリソースに限りがある以上、自組織にとって優先度の高いリスクを見極め、そのリスクに対してリソースを投入することが望ましい。そのためには、まず自組織にとってのリスクを洗い出し、洗い出したリスクに対する優先順位付けを行うことが求められる。それゆえに、まずはリスクの特定・評価に焦点を当てていきたい。

(1) リスクの特定・評価

リスクの特定では、想定されるリスクの洗い出しを行う。そのためには、自組織が保有する情報資産の棚卸を行い、自組織における「守るべきもの」を特定する。この際に重要なのがシャドーIT の潰しこみである。シャドーITとは、経営層や情報システムを管理している部門が認知していない、職員が独自に導入したシステムや通信機器のことを指す。シャドーIT は脆弱性管理が適切になされていない可能性もあるため、リスクの温床となり得る。そのため、情報資産の棚卸を行う際には、シャドーIT も含めた形で実施することが重要である。情報資産の棚卸が完了したら、各情報資産の事業へ与える影響を踏まえ重要度のラベル付けを行う。

情報資産の棚卸と重要度のラベル付けが完了したら、続いて脆弱性の把握を行う。自組織全体の脆弱性の把握の例として、業界ガイドラインに準拠したチェックシートを用いたリスクアセスメントの手法がある。業界で求められているセキュリティレベルとのギャップが把握できるため効率的な手法ではある。但し、チェックシートによっては設問が曖昧なものであったり、回答に窮するものも存在する。チェックシートの選定にあたっては、設問にやるべきことが具体的に記載されており、回答の揺れが生じにくく、その後の対策に繋がりやすいものを特に推奨する[9]。技術的な側面からの脆弱性の把握には、脆弱性診断やペネトレーションテストを定期的に行うのが有用である。攻撃者の目線から見た自組織のリスクを把握することができる。

情報資産への重要度のラベル付けと脆弱性の把握が完了したら、両者を突き合わせてリスクの重大度を計算する（図表 4）。この両者を突合することによって、リスクの重大度を明らかにし、リスク対応の優先順位付けを行う。

■ 図表 4 リスクの重大度の評価

脆弱性の重大度	事業への影響				
	非常に低い	低い	中間	高い	非常に高い
非常に高い	低い	中間	高い	非常に高い	非常に高い
高い	低い	中間	中間	高い	非常に高い
中間	低い	低い	中間	中間	高い
低い	非常に低い	低い	低い	中間	中間
非常に低い	非常に低い	非常に低い	低い	低い	低い

出典：NIST SP800-30、『リスクアセスメントの実施の手引き』、「表 G-5 アセスメントスケール – 総合的な可能性」を基に弊社作成

(2) リスクへの対応

リスクの優先順位付けが完了したら、優先順位に応じて対応を行っていく。リスクへの対応には、受容、回避、低減、移転の 4 つが存在するが、本項ではリスクの低減及び移転に焦点を当てて解説する。

□ リスクの低減

リスクの低減は、存在するリスクに対して対策を講じることによって、そのリスクレベルを受容可能なレベルにまで低減させることを指す。一般的にセキュリティ対策と呼ばれる措置は、このリスクの低減に該当する。セキュリティ対策は、大きく

[9] 参考例として、東京海上ディーアールのサイバーリスク総合評価サービスを紹介する。
https://www.tdr-cyber.jp/assess/

分けて組織的対策、物理的対策、技術的対策、人的対策が存在する[10]。 組織的対策は、組織のセキュリティ方針を定めたセキュリティポリシーの整備・運用などの各種規程類の整備、CISO[11]の任命をはじめとしたセキュリティを計画・推進していくための体制の整備などが挙げられる。また、平時の対策だけでなく、緊急時の対応フローや、CSIRT[12]の構築なども組織的対策として挙げることができる。物理的対策は、物理的な入退室の管理や、施錠やワイヤロックなどの盗難対策、のぞき見防止の措置などの対策が挙げられる。技術的対策は、セキュリティ機器の導入及び運用や、アクセス制御の導入、アクセスログの収集などの対策が挙げられる。人的対策は、従業員や外部委託先との守秘義務の締結や、セキュリティの教育・啓発などが挙げられる。

セキュリティ対策を推進していく上で重要なポイントは、経営層を体制に参加させることである。セキュリティ対策には多大なリソースが必要となる。現場に対応を丸投げしてしまうのではなく、経営者がセキュリティ対策を経営課題として捉え、当事者意識をもって進めていかないと、セキュリティ対策に実効性を持たせることはできない[13]。また、有事の際に事業停止の判断を迫られる事態に直面する可能性もある。このような時に経営層が体制に加わっていないと迅速な意思決定ができず、被害の拡大に繋がってしまう恐れもある。組織的対策において CISO の任命について触れたが、これまで述べてきた理由から、CISO は経営層から任命することが望ましいと言える。

これまで見てきた通り、セキュリティ対策は一般的にイメージされるようなセキュリティ装置を導入するなどの技術的対策に留まらず、上述した 4 つのカテゴリから構成される。限られたリソースを有効活用するためにも、自組織におけるリスクを分析し、4 つのカテゴリから最も有効と思われるセキュリティ対策を推進していくことが重要である。また、対策を進めていくにあたっては、経営層がその体制に加わることが望ましい。

□ リスクの移転

脅威の事項で説明した通り、サイバー攻撃者を医療機関がコントロールすることはできない。どれだけ医療機関がセキュリティ対策を推進したとしても、対策を上回る技量を持った攻撃者が存在した場合、サイバー攻撃を受ける可能性は残存してしまう。

そこで求められるのがリスクの移転、すなわち保険への加入である。公益財団法人損害保険事業総合研究所の報告によると、2020 年において、米国では 50%以上の企業がサイバーリスク保険に加入をしているが、日本の加入率は 10%にも満たない[14]。しかし、事業への影響での事項でも解説した通り、サイバー攻撃からの復旧には莫大な費用が必要となる。このような莫大な出費は経営に大きな影響を及ぼす可能性があるため、保険への加入はリスクコントロールの観点において非常に有用である。

また、保険への加入は金銭的補償以外のメリットも存在する。東京海上日動火災保険が提供するサイバーリスク保険では、保険付帯サービスとして緊急時ホットラインサービスを提供している。このサービスは、保険契約者にサイバーインシデントの恐れが生じた際に、第一報を受付け、初動対応のアドバイスと各インシデントに対する専門事業者の紹介を行うものである。インシデント対応の経験が少ない組織には、このようなサービスを保険付帯で利用できるのは魅力的であると思われる。保険への加入をこれから検討する際は、利用できるサービスも含めて検討を行うことを推奨する。

---

[10] 医療機関に求められる対策として、厚生労働省発行の『医療情報システムの安全管理に関するガイドライン』に詳細が記載されている。平成 17 年 3 月の初版の公開以後、サイバーセキュリティ情勢に合わせて改訂を重ね、2022 年 3 月に作成された第 5.2 版が最新版となっている。ボリュームは大きいが、必ず参照いただきたい。
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

[11] Chief Information Security Officer。最高情報セキュリティ責任者のこと。

[12] Computer Security Incident Response Team の略。「シーサート」と発音する。セキュリティインシデント対応を行うチームのこと。

[13] 経営者に求められるセキュリティ対策については、経済産業省が発行している『サイバーセキュリティ経営ガイドライン』を参照いただきたい。
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[14] 林圭一「米国を中心とするサイバーインシデント・サイバー保険市場の動向」『損保総研レポート 第 134 号』2021 年 1 月を参照。

3. 今まさに求められるセキュリティ対策

冒頭で紹介した大阪の病院の事例を受け、厚生労働省は 2022 年 11 月 10 日に自治体を通じて医療機関へ注意喚起を発表した[15]。その内容は図表 5 の計 13 項目となる。前章にて医療機関に求められるセキュリティ対策として、リスクの特定、評価、対応を紹介した。上述の流れに沿って対応を行うことが理想ではある一方、医療機関を標的としたサイバー攻撃が多数発生しており、その被害が甚大化している現状を踏まえると、取り組むべき喫緊の課題があることも事実である。本章では、医療機関が取り組むべき喫緊のセキュリティ対策について紹介する。

■ 図表 5 厚生労働省からの注意喚起

サプライチェーンリスク全体の確認	・関係事業者を全てリスクコントロールの範囲内に置く。
リスク低減のための措置	・アカウント窃取対策：PWの複雑化、IDの棚卸、不要アカウントの削除、多要素認証の導入 ・IoT機器を含めた情報資産の保有状況の整理 ・脆弱性管理：既知の脆弱性管理、セキュリティパッチの適用 ・アクセス制御 ・人的対策：不審メールの開封を防止する、不審メール受信時の報告フローの確立
インシデントの早期検知	・ログの収集 ・通信の監視、アクセス制御の実施
インシデント発生時の適切な対処、回復	・サイバー攻撃を想定したBCPの策定 ・インシデント対応体制、フローの構築 ・インシデント発生時には速やかに関係省庁(厚労省)へ報告する
金銭の支払いに対する対応	・金銭を支払ってもデータの漏洩を防止できたり、データを復号できる保証はない ・一度金銭を支払うと、「脅迫に屈する標的」として再度攻撃を受ける可能性がある

出典：厚生労働省「医療機関等におけるサイバーセキュリティ対策の強化について(注意喚起)」を基に弊社作成

(1) 情報資産管理及び脆弱性管理

脆弱性の事項でも解説した通り、徳島や大阪の病院の事例は既知の脆弱性を悪用される形でサイバーインシデントが発生した。既知の脆弱性を認識、適切な脆弱性対応を行うだけでも、サイバーインシデント発生の可能性を低減させることが可能である。

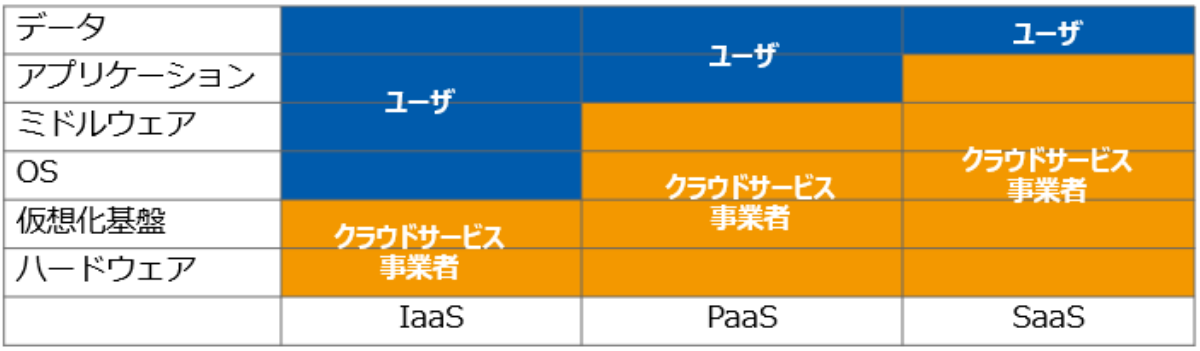
脆弱性管理を行うためには、自組織の情報資産管理が前提条件となる。すなわち、どの端末に何のシステムが入っているのかを把握し、それらのバージョン管理を行うことが必要となる。そのため、リスクの特定の事項でも解説した通り、シャドーIT の潰しこみを含めた自組織内の情報資産を棚卸することが、脆弱性管理を行う上での第一歩となる。

情報資産の棚卸が完了したら、続いて各情報資産を管理する主体を明確にする。具体的には、情報資産のバージョンアップなどのセキュリティ運用を行うのが自組織なのか、それともその製品を販売したベンダなどになるのかを、契約内容を確認することによって明確にすることである。脆弱性管理を行う責任がベンダにある場合は、脆弱性対策を依頼し、運用状況のモニタリングを行う。責任が自組織にある場合は、脆弱性情報を収集し、セキュリティパッチを適用するなどの脆弱性対応を行う。自組織内での対応が厳しい場合は、費用が掛かったとしてもアウトソースすることを推奨する。

[15] 厚生労働省　医療機関等におけるサイバーセキュリティ対策の強化について(注意喚起)
https://www.mhlw.go.jp/content/10808000/001011666.pdf を参照。

また、クラウドサービスを利用している場合は、自組織の契約しているクラウドサービスが図表 6 のどのモデルに該当するのかを確認し、責任分界点を明確にする。SaaS の場合は設定情報やデータまでが自組織の責任分界点となり、PaaS はアプリケーションまで、IaaS は OS までが責任分界点となる。クラウドサービスを利用しているからといって、全ての責任をクラウドサービス事業者が負う訳ではないことを認識しておくことが重要である。加えて、クラウドサービスには多数のステークホルダーが介在する場合が多い。クラウドサービスの責任分界点を理解するためには、ステークホルダーを整理し各ステークホルダーの果たすべき責任範囲を整理することが前提条件となる[16]。

■ 図表 6 クラウドサービスの責任分界点



出典：弊社作成

(2) 重要データのバックアップ

厚生労働省が発行している『医療情報システムの安全管理に関するガイドライン』は、徳島の病院の事例を受け、2022 年 3 月末に最新版の 5.2 版に改訂された。改訂された主なポイントの一つとして、緊急時の備え、特に重要データのバックアップに関する条項が追加されたことがある[17]。全ての情報をバックアップするのは現実的ではないため、事業継続における可用性を重視し、バックアップを取るデータや、システムを選定してバックアップを実施することが推奨されている。また、ランサムウェアの被害がバックアップデータに及ぶことがないよう、媒体の種類、バックアップ周期、世代管理の方法、バックアップデータをオフラインに保存するなどを考慮した対策の検討が求められる。

(3) 職員への教育

セキュリティ製品の性能がどれだけ向上したとしても、それを使用する人間側に脆弱性が存在していれば、その脆弱性を悪用される形で攻撃者による侵入を許してしまう可能性がある。実際、Emotet と呼ばれるマルウェアは、受信者が開封してしまうような巧妙な仕掛けを駆使して、感染を爆発的に増加させた [18]。まさに、人の脆弱性を悪用した攻撃手法の一つである。

職員に対するセキュリティ教育を実施するだけでも、このような人の脆弱性を悪用する攻撃に遭う可能性を低減することが可能である。一般社団法人ソフトウェア協会は、厚生労働省からの委託を受け、2022 年 12 月に医療機関

[16] 重要インフラがクラウドサービスを利用する際のガイダンスとして、以下の資料が詳しい。
内閣官房サイバーセキュリティセンター『クラウドを利用したシステム運用に関するガイダンス(詳細版)』
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html
[17] 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 5.2 版』
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html を参照。
[18] Emotet の詳細は、一般社団法人 JPCERT/CC の「マルウェア Emotet の感染再拡大に関する注意喚起」が詳しい。
https://www.jpcert.or.jp/at/2022/at220006.html

を対象としたセキュリティ研修を行うことをポータルサイトにて公表した[18]。当該研修は、経営者向け、情報システム管理者向け、初学者向けのレベル分けで講座が用意されている。12 月より順次公開をされていく予定のため、対象者を選定し、受講することを推奨する。

(4) 緊急対応フローの整備

繰返しになるがセキュリティ対策を実施したとしても、セキュリティリスクはゼロにはならない。どのような組織であったとしても、セキュリティインシデントが発生する可能性がある。インシデントが発生した際に、冷静に対処することは難しい。特に、インシデントの経験が希薄な組織であれば尚更だ。そこで重要なのがインシデント対応フローの作成である。

インシデント対応フローは、インシデントの関係者を洗い出し、各登場人物がインシデント発生時から収束までに行うことを定めたフローチャートである。厚生労働省が医療機関向けのチェックシートのひな型を提供しているため、ひな型を参照しつつ自組織に合った形にカスタマイズするのも有用である[19]。インシデント対応フローには、自組織内の関係者だけでなく、自組織外の関係者の欄を設けておくことも重要である。セキュリティ製品やサーバなどの管理をベンダに依頼をしている場合は、ベンダもインシデント対応の関係者となる。また、医療機関がサイバー攻撃を受けた際には、厚生労働省などの監督官庁に対する報告が求められる[20]。個人情報の漏洩が発生した場合には、個人情報保護委員会への報告義務も生じる。外部ベンダや監督官庁や個人情報保護委員会、それぞれの相談・報告窓口を明記しておくと、インシデント発生時の対応を円滑に行うことができる。また、インシデント発生時に相談できる窓口をフローに加えておくのも有用である。職員への教育の事項で紹介した厚生労働省のポータルサイトでは、インシデント対応の相談窓口を開設しており[21]、初動対応の支援を受けることができる[22]。リスク移転の事項で紹介した東京海上日動火災保険の緊急時ホットラインサービスも同様に緊急対応時の相談窓口となる。

また、インシデント対応フローを機能させるためには、インシデント分類表の作成が必要となる。インシデント分類表は、インシデントの定義を定めたものである。何をもってインシデントとするのか、重大なインシデントと軽微なインシデントの違いは何か、インシデントの定義によってその後の対応も変化する。そのため、事前にインシデント分類表を作成しておくと、インシデント対応フローにより実効性を持たせることが可能となる。

加えて、インシデント対応フローを補完するために、インシデント対応チェックシートを作成しておくことも有用である。インシデント対応チェックシートは、インシデント対応時に行うべきことや確認すべきことをリスト化し、対応の抜け漏れを防止するものである。上述の通り、インシデント対応時には冷静な対処を行うことは難しい。事前にチェックシートを作成しておくと、インシデント対応担当者の負担軽減にもつながる。

---

[18] 厚生労働省　医療機関向けセキュリティ教育支援ポータルサイト
https://mhlw-training.saj.or.jp/を参照。

[19] 厚生労働省　医療情報システム等の障害発生時の対応フローチャート
https://www.mhlw.go.jp/content/10808000/000936170.xlsx を参照。

[20] 厚生労働省　医療分野のサイバーセキュリティ対策について
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html を参照。

[21] 厚生労働省　医療機関向けセキュリティ教育支援ポータルサイト
https://mhlw-training.saj.or.jp/を参照。

[22] 厚生労働省は 200 床以上の病院を当該ポータルサイトの初動対応支援の主なターゲットとしており、200 床未満の病院に対してはサイバーセキュリティお助け隊の活用を推奨している。厚生労働省『厚生労働省におけるサイバーセキュリティに関する取り組み』を参照。
https://www.nisc.go.jp/pdf/council/cs/ciip/dai31/31shiryou0303.pdf

(5) 保険への加入

リスクの移転の事項で説明した通り、サイバーインシデント発生後の調査や復旧には莫大な費用が発生する可能性がある。医療機関が高いサイバーリスクに曝されている状況において、リスク移転策としての保険の加入を強く推奨する。また、保険に加入している場合、外部ベンダからの与信調査の行程を短縮できるなどのメリットもある。外部ベンダに有償で対応を依頼する場合、通常の取引と同様に与信調査や見積、契約手続きなどの事務作業が生じる[24]。インシデント対応では刻一刻を争う事態に直面することも多いため、与信調査を簡素化できることは、迅速な作業着手を可能にすることができる。

保険加入には金銭的補償以外にも付帯サービスなどのメリットがあることは、先述した通りである。

4. セキュリティの『かかりつけ医』を見つけることが重要

これまで医療機関を取り巻くサイバーリスクの状況と、求められるセキュリティ対策について解説をしてきた。医療機関は脅威であるサイバー攻撃者にとって魅力的な標的となっており、かつ被害に遭った際の事業への影響も大きい。その為、脆弱性対応を始めとするセキュリティ対策を行う必要がある。セキュリティ対策に効力を持たせるためには、事前にセキュリティリスクを洗い出し、セキュリティ対策の優先順位を決定しておくことが重要となる。

これらのことを医療機関が自組織内にて完結して推進することは困難であろう。多くの企業では、これらのセキュリティ対策を外部ベンダやコンサルティング企業に依頼をしている。サイバー攻撃が日々巧妙化している現代においては、セキュリティ対策はセキュリティの専門家に頼ることが最も費用対効果が高い。医療において、患者にとって信頼できる『かかりつけ医』を見つけることが重要であることと同様に、セキュリティ対策においても、信頼できるセキュリティ専門家を見つけて、困ったことがあった際には相談できる関係性を構築しておくことが重要である。

[2023 年 3 月 6 日発行]

[24] 現場の担当者は一刻でも早く調査に着手したいのに、契約等の事務作業が滞ることによって作業着手が遅れるケースが多々存在する。

東京海上ディーアール株式会社

サイバーセキュリティ事業部　三宅　諒介研究員（専門分野：サイバーセキュリティ）
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6674　Fax. 03-5288-6590 www.tokior-dr.co.jp