サイバーインシデント対策と医療安全

武田理宏
大阪大学大学院医学系研究科医療情報学 教授／大阪大学医学部附属病院 医療情報部

Summary

近年、医療機関がランサムウェアなどのサイバーインシデントに遭遇し、医療提供が困難となる事例が報告されている。医療機関は重要インフラの一分野として、サイバーセキュリティ対策を進めなければならない。対策には、ランサムウェアの感染防止や感染検知、データ暗号化による被害を軽減するためのバックアップ、迅速にインシデント対応を行うための事業継続計画（BCP）が挙げられる。サイバーインシデント時は、電子カルテ障害により少ない患者情報のもと、慣れない用紙運用を行う必要があり、医療機関全体で対策に取り組む必要がある。

独立行政法人情報処理推進機構（IPA: Information-technology Promotion Agency）が公表する「情報セキュリティ10大脅威2023」では、組織に対する脅威として、1位にランサムウェア（Ransomware）による被害、2位にサプライチェーンの弱点を悪用した攻撃、3位に標的型攻撃による機密情報の窃取を挙げている[1)]。医療機関においても、宇陀市立病院（2018年）、つるぎ町立半田病院（2021年）、鳴門山上病院（2022年）、大阪急性期・総合医療センター（2022年）が、ランサムウェア攻撃により診療継続が困難となったことは記憶に新しい[2-4)]。一方、医療機関などがサイバー攻撃を受けた場合、厚生労働省への報告が求められているが、報告を行っていない医療機関もあるとされ、その実数は明らかでないとされる。

内閣サイバーセキュリティセンター（NISC：National Center of Incident readiness and Strategy for Cybersecurity）では、医療機関を全14分野の重要インフラの1つと定めている[6)]。重要インフラに関してNISCは、機能保証の考え方を踏まえ、サイバー攻撃や自然災害などに起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する、としている。この目的を実現するために、医療機関は厚生労働省を所管省庁として、サイバーセキュリティ対策を進めていく必要がある。

これに対し、令和4（2022）年度の診療報酬改定では、診療録管理体制加算1に関する施設基準として、400床以上の保険医療機関については、専任の医療情報システム安全管理責任者を配置し、職員に対する情報セキュリティ研修や、非常時に備えた医療情報システムのバックアップ体制を確保することなどが求められた。

また、2023年5月31日に公表された「医療情報システムの安全管理に関するガイドライン第6版」では、ガイドラインが①概説編、②経営管理編、③企画管理編、④システム運用編に分冊化され、特集として小規模向けガイダンスが示されるなど、より多くの医療関係者がガイドラインに触れる工夫が行われた。加えて、「特集」としてサイバーセキュリティが取り上げられるなど、サイバーセキュリティ対策が多く盛り込まれている。

医療機関のサイバーセキュリティ対策としては、外

部からの不正アクセスの防御や、侵入された際の不審な動きに気づく挙動検知、ウイルス感染を起こした際にシステム復旧できることを目的としたバックアップなどが求められるが、システム復旧までの間に患者への医療提供を継続するためには、事業継続計画（BCP：Business Continuing Plan）の策定が大切である。

サイバーインシデント防御に向けて

ランサムウェア感染

「ランサムウェア」は、悪意のあるソフトウェア（マルウェア）の一種であり、感染したコンピュータやネットワーク上のファイルを暗号化して、利用者がデータにアクセスできないようにする。そのうえで、「データ復号化キー」を所持する攻撃者が、身代金（ランサム）を要求するものである。データを暗号化する際にデータを窃取し、「ダークウェブサイト」に公開することを脅す、二重の恐喝を行うことも少なくない。

ランサムウェア感染の際、最初に侵入するのは、ランサムウェアそのものではないことが多い。最初に侵入した不正ソフトウェアは、数日から数週間、医療情報システムを静かに観察し、どのファイルがよく使われて、システムがどのような構成になっているかを調査し、急所となる部分に、外部からランサムウェアを呼び込む不正ソフトウェアを配置する。

システム内に配置されたソフトウェアは、一気にランサムウェアを外部から呼び込み、呼び込んだランサムウェアは一斉に、重要なファイルを暗号化する。また、ランサムウェアは、バックアップシステムにも配置されることがある。その後、脅迫文書をプリンタから打ち出したり、画面に脅迫文などを表示したりする。

このように、
- ランサムウェア感染が発覚する前から感染は起こっていること、
- オンラインバックアップシステムも感染の対象となる可能性があること、

から、医療機関は、
- バックアップを保存する電磁的記録媒体などの種類、
- バックアップの周期・世代管理の方法、
- バックアップデータを保存した媒体を端末およびサーバ装置やネットワークから切り離して保管すること、

などを考慮して、対策を講じることが強く求められる。

著者紹介

武田理宏（たけだ・としひろ）
大阪大学大学院医学系研究科医療情報学教授／大阪大学医学部附属病院 医療情報部
1997年大阪大学医学部卒。循環器内科専門医。2008年より大阪大学医学部附属病院医療情報部に所属。「医療情報システムの安全管理に関するガイドライン第6版」の改訂や。医療現場のセキュリティ人材に育成に関する調査研究にかかわる。

大阪大学医学部附属病院（大阪府吹田市）：1086床

ランサムウェアの感染経路

ランサムウェアの感染経路は主に、
①メールの添付ファイルにランサムウェアが仕込まれているケース、
②USBメモリからの感染、
③インターネットとの接続機器、
が想定される。

◆添付ファイルやUSBメモリからの感染

①は、メールの添付ファイルにランサムウェアが仕込まれているケースや、メール本文に記載されているリンクをクリックすると、ランサムウェアをダウンロードして起動してしまうケースである。②は、ランサムウェアに汚染されているUSBメモリから、端末が感染するケースである。

①や②は、個人PCや事務PCでは非常に注意する必要があるが、電子カルテ端末でインターネット接続できる医療機関はほぼないこと、USBメモリの使用が制限されていることが多いことから、感染経路となるリスクは比較的少ないと考えられる。

◆インターネットとの接続機器からの感染

③は、リモートメンテナンス用にシステムベンダーが用意したVPN（Virtual Private Network：仮想プライベートネットワーク）ルータの脆弱性（セキュリティホール）を利用して、ネットワーク内に侵入するケースなどであり、電子カルテのランサムウェア感染は、③のケースがほとんどである。

実際に、医療機関のランサムウェア感染の多くは、事後の検証でVPNルータの脆弱性が存在したことが確認されている。このため、個々の医療機関は、VPN装置を適切に管理し、脆弱性が発見された場合はファームウェアのアップデートを速やかに行う必要がある。

◆最近のランサムウェア感染

OS(オペレーティングシステム)やソフトウェアなどの脆弱性が発見されてから、その情報公開や対策が講じられる前にその脆弱性を狙う「ゼロデイ攻撃」が知られる。これらの攻撃を防ぐためには、公開された更新プログラムをできるだけ速く適用することしかない。

業務目的で他施設とVPNで接続されている場合に、他施設のVPN装置の脆弱性を突き、水平移動で感染を引き起こすサプライチェーン型のランサムウェア感染も起こっている。大阪急性期・総合医療センターのランサムウェア感染事例は、医療機関にサービスを提供する事業者を介した水平感染であった。

◆境界型防御とゼロトラスト

ランサムウェア感染からの防御を考えた場合、従来は、外部(インターネット)と院内ネットワークを切り分け、院内ネットワークに侵入されることを防ぐため、外部との接続点にファイアーウォールや侵入検知システム(IDS:Intrusion Detection System)や侵入防御システム(IPS:Intrusion Prevention Systems)を置く「境界型防御」が主流であった。しかし、境界型防護では院内ネットワークに侵入された場合に無策となるため、院内ネットワークも含め、すべての通信を信頼しないことを前提にセキュリティ対策を講じる「ゼロトラスト」の考え方が普及してきている。

ゼロトラストでは、ネットワークの内外にかかわらない通信経路の暗号化、ユーザー認証の強化(多要素認証の利用)、ネットワークやそれに接続される各種デバイスの統合的なログ監視が試みられる。しかし、電子カルテシステムは、部門システムも含めた多くのシステムとともに稼働しており、境界型防御の考えで構築されたシステムであることが多いため、コスト面やその他の理由で、ゼロトラストの考え方を導入することは簡単ではない。

サイバーインシデント防御に向けた医療機関の取り組み

◆電子カルテシステムの構成管理、アカウント管理と挙動検知

最初に、医療機関はサイバーインシデント防御に向けて、電子カルテシステムの構成管理を行う必要がある。

電子カルテシステムの構成や利用するサービスの形態に応じて、システムやサービスを構成する機器や、利用するネットワーク構成を一覧化する。そして、システムが稼働するためのネットワークに接続する機器やネットワーク経路を掌握する。セキュアなネットワークを整備するため、ネットワークの論理的または物理的な構成の分割、接続機器の制御、通信するデータの制御などを実施する。

次に、アカウント管理が大切となる。医療情報システムを利用・管理する関係者をリストアップし、それぞれがどのような権限でどのようなシステムを操作するのかを掌握する。

運用系とバックアップ系などのセキュリティ系の認証を分離することで、時間稼ぎや、うまく行けばバックアップ系やセキュリティ系を守ることができる。そして、IDSやIPSやEDR(Endpoint Detection and Response)を導入して、ネットワークを監視する。

◆被害の範囲を少なくする対策の重要性

サイバーセキュリティインシデントからの防御を完全に行うことは容易でない。攻撃者(ハッカー)が、特定の医療機関を攻撃対象として定め、侵入を試みた場合、侵入を防御することは困難かもしれない。

しかし、金銭目的であれば、その攻撃者にとって侵入するのはどの施設でもよく、少しでも手間のかからない、つまり、サイバーセキュリティ対策が脆弱な施設を狙うことになる。また、万が一、院内ネットワークに侵入された場合も、院内ネットワークが適切な管理を行っていれば、パスワードの解読に時間がかかったり、不審な通信を検知して早期発見を行うことで、被害の範囲が少なくなることが想定される。

サイバーセキュリティ対策には費用が必要となるが、できることから対策を少しでも進めていくことが大切である。

サイバーインシデント発生への対応

自然災害とサイバーインシデント災害の違い

◆自然災害の場合

自然災害時に停電が発生したとしても、電子カルテシステムサーバーやネットワークインフラは非常用電源に接続されており、各部署に配置されるノートPCはバッテリーを積んでいるため、電子カルテシステムを使って患者情報にアクセスできる可能性が高い。また、電子カルテシステムが停止しても、システム自体の障害ではないため、早期に復旧できる可能性が高い。

自然災害時に医療機関を受診される患者は、外傷を中心とした救急搬送が想定され、日常診療の受診はむしろ減ることが予想される。さらに、患者も医療機関

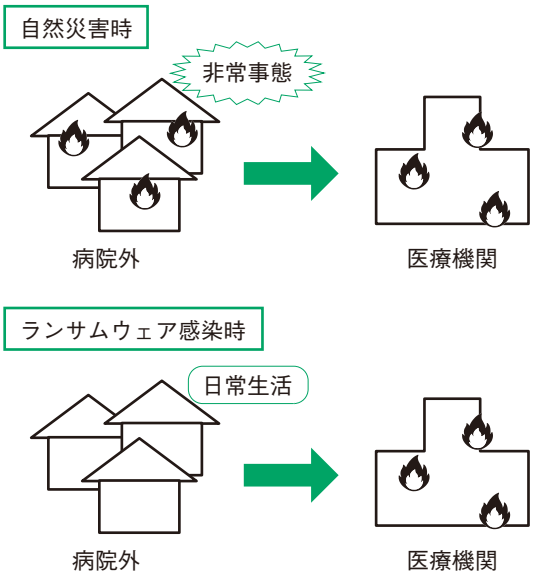

図1　自然災害とサイバーインシデント災害の違い
自然災害時は、病院外でも非常事態の状況は共有されるが、サイバーインシデント災害時は共有されない。

の状況をある程度予想できるため、広報の必要性は低いと考えられる（**図1**）。

◆サイバーインシデント災害の場合

ランサムウェア感染などサイバーインシデントによるシステム障害の場合、電子カルテシステムはバックアップサーバを含めて使用できず、医療スタッフが患者情報にまったくアクセスできないことが想定される。電子カルテシステム復旧に向けて、フォレンジック調査（サイバーインシデントが発生した際、デジタル端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする調査）や、電子カルテサーバーの再構築が必要となるため、完全復旧までは数カ月の期間がかかることが想定される。

一方、病院外では日常生活が営まれるため、適切な広報を行わないと、患者は被災医療機関の状況を知ることはできず、日常診療を求めて医療機関を受診することになる（**図1**）。これに対して、電子カルテにアクセスできないことは、外来や手術の予約情報や患者連絡先が把握できないことを意味しており、個々の患者への連絡は難しいことが想定される。

◆サイバーインシデント災害用BCP作成の必要性

医療機関では、災害時のBCPが策定されているが、多くは自然災害を想定したBCPとなっていることが多い。上述したとおり、自然災害時とサイバーインシデント時の課題は大きく異なるため、サイバーインシデント時のBCPを自然災害とは別に設定するべきである。

医療情報システム障害時の運用

◆用紙運用、そのための訓練

医療情報システム障害時は、多くの医療機関で用紙運用（紙カルテ、紙の伝票）が想定されている。ここで注意しなければならないことは、医療スタッフの用紙運用の経験である。ペーパーレスの電子カルテの導入時期は医療機関ごとに異なるが、電子カルテ運用が開始されて10年以上が経過している医療機関も少なくない。このことは、医療機関の最前線で勤務する中堅クラス以下の医療スタッフは、用紙運用の経験がほとんど、あるいはまったくないことを意味している。

大阪大学医学部附属病院（以下、当院）では2022年1月に電子カルテの更新を行った際に、数日間の用紙運用を行った。病棟では、旧システム停止前に、紙の指示箋に医師が指示を転記し、看護師が指示受けを行い、システム停止期間は用紙運用を行い、新システム稼働後に指示を電子カルテに入力した。

この際、多くの病棟から「紙の指示箋の書き方がわからない」との声があがり、紙の指示箋の記載方法のマニュアルを作成した。病棟での指示運用に関する医療安全にかかわるインシデントは、多くの医療機関で経験してきたことであるが、電子カルテ障害時の用紙運用で、指示伝達にかかわるインシデントが発生する可能性があることには、注意が必要である。

◆電子カルテ停止が医療安全を脅かすリスク

電子カルテでは、医療安全にかかわる多くの機能が実装されてきた。電子カルテの患者一覧では、同姓同名チェックがかかったり、患者カルテ起動時には漢字氏名、カナ氏名に加え、性別、年齢、居住地などの患者識別に必要な情報が表示されたりする。

また、注射薬投与時のバーコードチェックなど、患者間違いを防止する仕組みが多く組み込まれている。薬剤処方時には、禁忌・アレルギー、同一薬剤処方、絶対禁忌・相互作用薬剤、妊産婦禁忌薬剤、投与量上限などの多くのアラートが発出される。しかし、電子カルテ障害時に、これらの機能を使用することはできない。

そもそも、医師は紙の処方箋を記載することに慣れていない。電子カルテでは、3文字入力で候補薬剤名称が表示されるが、特にジェネリック医薬品の場合、その名称を紙の処方箋で正確に記載できるか、課題がある。また、薬剤用量や用法も、「選択肢から選ぶ」と「自ら記載する」のでは、大きな違いがある。

記載ミスや省略がある処方箋が、電子カルテによるチェックがかかることなく、薬剤部門に下りていくことで、薬剤監査の負担は大きくなる。多くの医療スタッフにとって、電子カルテの医療安全に係る機能は意識なく使用されているのであり、システム障害運用時には、医療安全への配慮が十分になされる必要がある。

サイバーインシデント発生時のBCPの策定

◆電子カルテシステム復旧までの時間の確認

サイバーインシデントにより電子カルテシステム障害が発生した場合、

- システム復旧までに電子カルテシステムの使用がまったくできない期間、
- 過去の診療情報のみ閲覧可能な期間、

が想定される。復旧に必要な期間は被害状況により異なるが、使用できない期間が数日間、完全復旧まで数カ月間が必要となることが想定される。

また、過去の診療情報のみ閲覧可能な期間については、院内ネットワークが使えずに限られた部屋（機器）でのみ診療情報が閲覧可能な状況、基幹システムや部門システムのうち一部の診療情報のみ閲覧可能な状況などが想定される。どの程度の期間が想定されるかは医療機関ごとに異なるため、各施設の医療情報担当者に確認したうえで、BCPを策定する必要がある。

◆チームで危機を乗り越える仕組みづくり

当院ではサイバーインシデント発生時には、病院執行部と関係チーム責任者で構成される対策本部を中心に、システム復旧対応チーム、広報・外部連絡チーム、院内（患者）対応チームが医療現場を支えるべきであると考えている（**図2**）。

対策本部は、情報の集約や方針の決定（例：診療制限、診療再開）、決定された方針の院内への情報共有を行う。

システム復旧対応チームは、院内の医療情報部門が病院情報システムベンダーや外部チームと連携し、システム復旧にあたる。初期には、インシデント発生時の状況の把握、感染拡大防止対応（ネットワーク遮断等）を行うとともに、復旧までの各フェーズにおけるシステム使用可能範囲の確認や、利用可能な参照系の確認および確立を行い、対策本部と共有する。

広報・外部連絡チームは、関係各所への報告（例：厚生労働省、警察）、マスメディア対応、病院ホームページへの公表、地域連携等の関連機関への連絡（患者対応依頼などを想定）を行う。

院内（患者）対応チームは、患者情報把握（例：外来予約患者、入院患者）、各部署への共有、患者問い合わせ対応などを行う。

臨床現場では、情報の不足と慣れない用紙運用で、混乱が生じると想定される。用紙の記載方法や記載内容の指導、用紙の不足への対応などは診療情報管理室が、混乱によるインシデントの把握と再発予防に向けた対策については医療安全管理室が、臨床現場をサポートすることができるように、BCPの策定を進める必要がある。

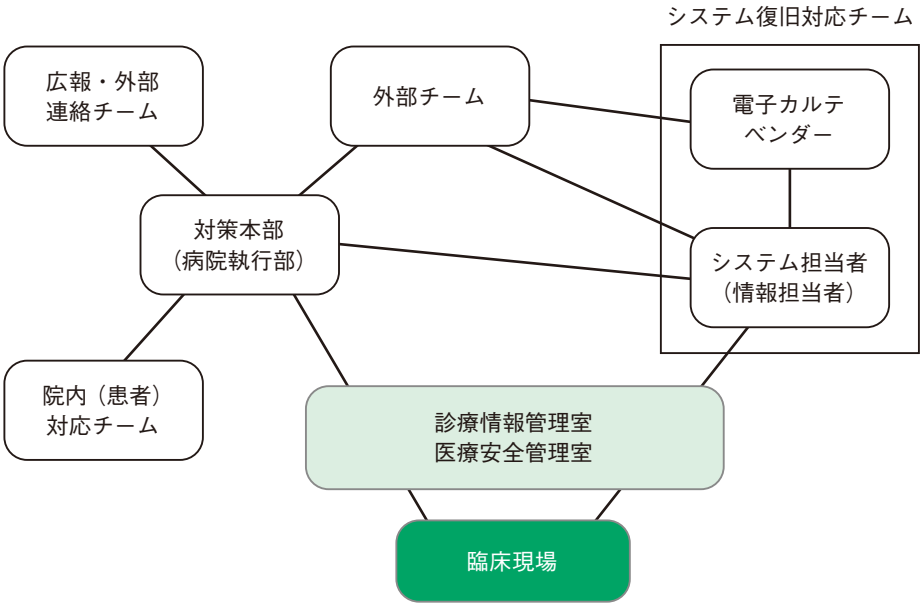

図2　サイバーインシデント発生時の対応体制案

サイバーインシデントに向けた災害訓練

◆システム更新のタイミングを利用した訓練

自然災害発生に向けた災害訓練を実施する医療機関は多いが、サイバーインシデントに向けた災害訓練を行っている医療機関は多くないと思われる。訓練は、電子カルテ障害下で日常診療を行うことが目的となるが、電子カルテシステムを止めて訓練を行うことは簡単ではない。

しかし、電子カルテシステムはシステム保守の問題から、5年から10年に一度はシステム更新を行う必要がある。システム更新のタイミングでは、医療機関ごとに期間は異なるものの、電子カルテシステム停止や利用制限が発生する。この機会を、訓練の機会として生かすことが考えられる。

◆訓練の実際

電子カルテシステム更新に向けて、医療情報部門、診療情報管理部門は、中央診療部門と連携をしながら、システム停止の準備を進めていく。用紙運用に必要な用紙が揃っているか、各部署に用紙が配置されている場合は必要時に取り出すことができるかを、この機会に確認をしておく。

中央診療部門では、電子カルテ導入以前から運用が変わっている可能性があるため、用紙運用を改めて見直し、必要があれば、用紙のフォーマットを変更する。上述したように、臨床現場は各種指示箋の記載方法がわからない職員が増えているため、記載マニュアルを整備することも必要である。

電子カルテ更新時のシステム更新の場合、最低限の診療情報閲覧環境は用意され、また、必要な文書は印刷するなどの対策がとられるため、サイバーインシデント時よりも医療提供環境は整っていると考えられる。しかし、実際に用紙運用を行い、発生した問題を検証することで、用紙運用の経験を引き継いでいくことができる。また、用紙運用後の遡及作業（電子カルテへの入力、用紙記録のスキャン、医事請求）についても確認することができる。

＊　＊　＊

医療機関は重要インフラの一分野として、患者情報を安全に管理し、安定した医療提供を継続するために、サイバーセキュリティ対策を進めなければならない。対策には、

- ランサムウェア感染を防止するための対策、
- データ暗号化による被害を軽減するための対策、
- 不正アクセスを迅速に検知するための対策、
- 迅速にインシデント対応を行うための対策、

が挙げられる。その多くは、医療情報部門が電子カルテベンダーと協調しながら対策を進めていく対策であるが、インシデント発生時の対策は、すべての医療職がかかわって考えるべき対策である。発生する事態の重大性がわかれば、病院職員個々が、セキュリティインシデントの発生につながる行動を慎むことにつながる。

また、BCPを策定し、訓練を行うことで、インシデント発生時の混乱を少しでも軽減することができる。インシデント発生時は、少ない患者情報と慣れない用紙運用で、医療安全にかかわるインシデントの発生が懸念されることを念頭において、災害対策本部、診療情報管理部門、医療安全部門が協調し、情報共有を図っていくことが大切である。

文献

1）独立行政法人情報処理推進機構：情報セキュリティ10大脅威.
https://www.ipa.go.jp/security/10threats/index.html（2023/8/1閲覧）
2）宇陀市：宇陀市立病院コンピューターウイルス感染事案に関する「報告書」.
https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/houkokusyo.pdf（2023/8/1閲覧）
3）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について.
https://www.handa-hospital.jp/topics/2022/0616/index.html（2023/8/1閲覧）
4）鳴門山上病院：令和4年6月20日 サイバー攻撃による被害について（第1報）.
https://kyujinkai-mc.or.jp/info/20220620/（2023/8/1閲覧）
5）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報告書について.
https://www.gh.opho.jp/important/785.html（2023/8/1閲覧）
6）内閣サイバーセキュリティセンター.
https://www.nisc.go.jp/（2023/8/1閲覧）