参考資料１－10

［特集］医療機関等におけるサイバーセキュリティ

（案）

目次

１．はじめに

診療情報等の機微な情報を扱う電子カルテをはじめとする医療情報システムは、情報の利用性を高めて連携を容易にし、質の高い医療の提供に極めて有用ですが、短時間で大量の情報を処理できることが可能であるために、何かセキュリティ上の問題が起こると被害や業務影響が大きくなる可能性があります。セキュリティ上の問題としては、例えば、システム利用終了時にログアウトし忘れるといった運用上の問題から、停電や機器の故障、さらにはマルウェア（コンピュータウイルス）と呼ばれる悪意のある不正ソフトウェアの混入など様々な事象があります。「医療情報システムの安全管理に関するガイドライン」は、これらすべてに対応するためのガイドラインで、どうしても扱う項目が多くなります。一方でサイバー攻撃と呼ばれる外部からの不正ソフトウェアの混入による被害が昨今増えてきており、最悪の場合は診療機能停止に至るなど、社会的にも問題になっています。そこで、「医療情報システムの安全管理に関するガイドライン」の中で、サイバーセキュリティに関係する部分を要約し、できるだけ具体的な例などにも触れてまとめたものがこの特集です。一読いただいて、ご自身の所属する医療機関の対策に役立てていただければ幸いです。

最初に述べなければならないことは、サイバーセキュリティは導入している医療情報システムによって異なるということです。例えば、フルクラウドの電子カルテサービスを導入している診療所など小規模医療機関等の場合は、サイバーセキュリティを踏まえたシステムやデータ、サービスが用意された適切なシステム関連事業者のサービスを採用していれば、医療機関等が主に取り組むことは医療情報システムの利用者認証を適切に行うことと想定されますので、当該事業者にサイバーセキュリティに関して医療機関等側が取り組むべきことを確認し、認識の齟齬や漏れがないようにして、適切に医療情報システムを利用してください。

これ以降の記載はオンプレミス型の医療情報システムや、オンプレミス型とクラウド型の混在した医療情報システムを導入・利用している医療機関等を想定しており、地域において地域医療の基幹を担う医療機関は必要最小限の対策に留まることなく、地域で担っている役割を維持できるよう各種対策に注力してください。

２．サイバーセキュリティとは

不正ソフトウェアによる感染被害や、外部から不法に医療情報システムに侵入し、データを盗み取ったり、または破壊したりするような被害を受けるか、または被害には至らなくとも対応が必要になる事象をサイバーインシデントと呼び、これに対応する対策がサイバーセキュリティです。

外部からネットワーク等を介して、侵入または不正ソフトウェアの送り込みをサイバー攻撃と呼びますが、例えばユーザや保守事業者の自宅のパソコンが不正ソフトウェアに感染し、USB メモリや CD/DVD、外付け HDD 等の可搬媒体を介して医療情報システムに不正ソフトウェアが入り込むこともあります。

3．サイバーインシデント

3．1　代表的な起因例

サイバーインシデントの代表的な起因例を以下に示します。

（1）USB メモリ、CD/DVD、業務に使っているスマートフォンなどを介して不正ソフトウェアに感染する。（媒体感染）

（2）送られてきた電子メールに添付されたファイルやソフトウェアを、不用意にダブルクリック等を行い、開封または起動する、あるいはメール本文中にあるリンク情報（URL）をクリックし、不正ソフトウェアを呼び込んでしまう。（メール攻撃）

（3）地域医療連携、オンライン保守作業（リモートメンテナンス）、インターネット利用などの外部に接続する部分を攻撃されて、侵入または不正ソフトウェアを送り込まれる。（サイバー攻撃）

上記以外にもありますが、本特集では代表的なものにとどめます。しかし、サイバーセキュリティの観点から、基本的に講ずるべき対策などに変わりはません。

3．2　サイバー攻撃の典型例

サイバー攻撃被害と対応の典型的な例として、ランサムウェア*と呼ばれる不正ソフトウェアが保守回線から医療情報システムに侵入した場合をあげます。

＊ランサムウェア：　身代金要求（Ransom）型の不正ソフトウェアで、典型的な場合はデータを暗号化し、復号するために暗号資産などで身代金を要求してきます。

[攻撃被害]

1．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です。最初に侵入した不正ソフトウェアは、医療情報システムを静かに観察します。どのファイルが良く使われて、システムがどのような構成になっているか調査し、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します。この時点で検出することは不可能ではありませんが、比較的難しいです。

2．ランサムウェアを外部から呼び込みます。呼び込まれたランサムウェアは一斉に重要なファイルを暗号化します。さらに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します。この時点で正常な業務はできなくなります。最初の不正ソフトウェアの侵入から被害が表面化するまでに数日～数週間かかることが多いようです。

[被害対応]

3．自機関の BCP（Business Continuity Plan：事業継続計画）に基づき、非常時における緊急的な情報アクセスを開始します。現状が BCP に記載されているどのフェイズにあるのかを確認することが重要です。

4．被害を把握した場合、被害届けを警察に提出します。警察では、被害防止対策に必要な情報の提供・助言や被害の復旧への貢献が行われています。また、こうした対応や捜査に当たって

は、被害医療機関の意向が最大限尊重され、業務への影響が最小限となるよう早期被害復旧等に配慮されます。

5．侵入経路に関係する通信ログの保全が完了すれば、医療情報システムの復旧に着手します。バックアップデータはすでに不正ソフトウェアが侵入している可能性があり、検出と適切な対応を行いながら復旧します。復旧が完了した医療情報システムの動作が確認できれば、必要に応じて緊急対応中のデータ復旧を行い、終了した時点で平常運用に戻り、BCP を終了します。

6．それまでの経過をレビューし、BCP の点検・検証・評価を行い、必要があれば改善し、すべての対応プロセスが完了します。

上記は比較的大規模な医療機関で最近見られた典型的な例を記載したもので、攻撃の種類や医療機関の規模によって被害や対応方法は変わってきます。

3．3　必要最小限の対策：バックアップ（システム・データ）

媒体感染、メール攻撃、サイバー攻撃等のサイバーインシデントの被害に遭ったとしても、被害や業務影響を少しでも小さくし、業務や情報システムの復旧が少しでも早くなるための必要最小限の基本的な対策として、システムやデータのバックアップがあります。

医療情報システムを利用して、診療等の患者に対する医療サービスを行っている医療機関等においては、自施設が提供している医療サービスの特性を踏まえ、利用する医療情報システムや取り扱う医療情報の重要性に鑑み、対象とするシステムの範囲やデータの期間を定め、地域医療に与える影響や業務の復旧に要するコストが許容できる最小限に留まるよう、システム関連事業者とも協議をし、バックアップを整える必要があります。

システムやデータのバックアップの目的は下記の２つがあります。

1．最低限の業務が継続できるように、最低限必要な情報へのアクセスをすばやく復旧させる。

2．医療情報システムになにかあった場合に、元の正常な状態に戻し、復旧させる。

1．は、診療等の最低限の業務を継続するために最低限必要なデータへのアクセスをできるだけ早く回復させるためのものです。何が最低限必要であるかは医療機関等によって異なります。またデータが利用可能でもシステムの機能が回復できず、アクセスできないこともありますので、非常時における緊急のデータへの代替アクセス方法も考えておく必要があります。

また、このバックアップは毎営業日に行うべきです。典型的なサイバー攻撃の例で述べたように、不正ソフトウェアは観察してから暗号化していきますので、バックアップも狙われます。したがってバックアップを一つ用意するだけでは、対応できないこともあります。これを防ぐためには複数世代のバックアップを用意し、少なくともその一つは暗号化などのデータの変更ができないように既に書き込まれたデータに対する追加の書き込みを禁止にする必要があります。

対策の例としては、テープカートリッジにバックアップし、次の日には前の日のバックアップをさらにコピーバックアップし、このバックアップカートリッジを外します。カートリッジを５セット用意してローテーションで使うと、常に３世代分は書き込みされる恐れのないバックアップが確保できます。

テープバックアップが利用できない場合は、複数世代のバックアップをディスク領域に保存した上で、OS の機能で書き込み禁止にしますが、不正ソフトウェアによって管理者権限が奪取されると、書き込み禁止の状態を解除される恐れがあります。完全に防止することは難しいですが、少なくとも医療情報システムの運用系とバックアップ系は管理者のパスワードを異なるものにするか、利用者の管理ドメインを変えるなどの措置を施すことで、リスクの軽減を講じることはできます。

２．におけるシステムの復旧には、データだけでなくシステムを動作させるためのプログラムや設定もバックアップしておく必要があります。フルバックアップと言ってもいいでしょう。一般的に医療機関等の判断と作業で実施できうるものではなく、医療情報システムを導入するシステム関連事業者がセットアップするものです。医療機関等はシステムを導入するときに、フルバックアップを適切に行うことを仕様に含め、検収の際に確認することになります。医療機関等の判断で、医療情報システムを複数のシステム関連事業者が構成することもあります。例えば放射線画像システムと電子カルテが異なる事業者が導入する場合で、LAN などのネットワークインフラは別事業者という場合もあります。複数のシステム関連事業者が関与する場合は、バックアップに抜け漏れや隙間があってはいけません。またシステムの稼働や利用に必要なサーバやクライアントＰＣ等の機器に障害が発生した場合で、同じ機器が手配・調達できない場合もあります。機器の設定等は、単純なバックアップと同時に、論理的な設定の記録も必要です。これがあるとないとでは復旧に要する時間や作業効率に差が出ます。

プログラムや設定のバックアップは変更した時に取ればいいですが、データはやはり毎日バックアップされると思います。こちらも１．の場合と同じで、バックアップも不正ソフトウェアに狙われますので、１．と同様の対策を取る必要があります。また、被害の範囲や性格等によっては、ソフトウェアやデータばかりでなく、医療情報システムで利用する機器（ハードウェア）のバックアップが求められることがあります。例えばサイバー攻撃による刑事事件とされるような場合には、警察による捜査のため、サーバや端末、機器等について証拠として提供を求められることがあります。また機器等のファームウェア等が書き換えられているリスクが認められる場合には、交換等の対応も必要となります。このように犯罪による被害やその範囲・内容によっては、既存のシステムと互換性を保つことが可能なハードウェアを準備しておくことが必要なこともあります。

診療の継続性をできる限り早く回復させるためのバックアップについては、医療機関によって何が必要か異なりますので、事前によく検討しておく必要があります。一般的に言って、情報が生成されてから時間が経てば経つほど、利用される頻度は低下します。もちろん過去の情報との比較は必要ですが、一般的な医療機関では、緊急事態である非常時では直近１年程度の期間の情報が比較できれば、緊急の診療としては可能なことが多いと思われます。したがって、バックアップ対象期間については、１年を少し超える期間をバックアップ対象とすることが推奨されます。なお、放射線画像診断検査結果データのようにデータサイズが大きい画像情報については、バックアップの環境にかけられるコストの都合から、このような目的でのバックアップが難しい場合は、読影レポートを保存するか、カルテ自体に所見を記載するようにしておくといいでしょう。検査結果や処方データなどは、厚生労働省標準規格である SS-MIX２標準化ストレージの形式で保存されていれば必要なバックアップデータを容易に作成することができます。また、HL7 FHIR 化が進んでいる場合は SS-MIX２標準のデータを HL7 FHIR 化した HL7 FHIR 規格準拠サーバでも同じことが言えます。

また、システム機能が回復できないためにバックアップデータがあってもアクセスできなくなる可能性もあります。一年程度のデータであれば CD-R や DVD-R にコピーすることも可能ですので、非常用のノート PC を用意して、SS-MIX2 ビューアや HL7 FHIR クライアントを用意することも考えられます。システム関連事業者と事前によく相談しておくことが必要です。

非常時における緊急用のデータアクセスで過去の記録まで用意することは一般的には難しく、対応も複雑になり経費もかかります。非常時はインシデント発生以前のデータは閲覧のみと割り切って、紙ベースで運用することも一つの方法です。その際、非常時の真っ只中や非常時からの復旧を急いで対応している中、データの事後入力や再入力が必要になりますが、非常時においては、診療の継続性の確保が優先すべき状況であるため、やむを得ないことだと考えられます。

４．対策

サイバーセキュリティを確保するために医療情報システムの稼働を支えるサーバや端末、ネットワーク等の機器、様々なシステム群の構成管理、そして、システムを利用・管理する利用者・管理者をシステム関連事業者の担当者も含めてリストアップし、かつ、複数のシステムが互いに連携したり、制御し合ったりして稼働しているためシステム自体も管理対象としてリストアップして、医療情報システムの稼働に接するすべてのアカウントの管理を行うことが重要である。そして、これらの多数の構成とアカウントが正常な動作をしていることをモニタリングし、正常ではない動き等をすることがないように制御、または、異常な動き等を検知した際には、予防的措置を発動する、というような監視を含め、ガバナンスを働かせる必要がある。

次に、ガバナンスを働かせていたとしてもサイバーインシデントの被害に遭う、という非常時を想定して、システムとの共存環境において、非常時における運用面の方針や判断基準や手順等を BCP（Business Continuity Plan：事業継続計画）として定め、業務継続に必要なシステムやデータの冗長化や複製などの保管を行い、運用面からシステム面までトータルでのバックアップを策定しておく必要がある。

４．１　ガバナンス

現在の医療情報システムは複雑で、外部サービスを利用することもありますし、機器やシステムの保守を外部からオンラインで行うこともあります。このような場合、外部接続するためのルータなどの機器や回線自体も外部事業者が管理している場合があります。この回線や通信機器あるいは外部事業者のシステムに脆弱性があると、ここが攻撃され、医療情報システム全体に被害が及びます。ガバナンスと言っても外部事業者を直接管理することはできませんので、医療機関としては接続の状況を把握し、契約等で、脆弱性が生じないように縛る必要があります。例えば、部門システムの保守は部門が業者と交渉し、契約も担当し、医療機関としては把握が不十分なことがありえます。このような状況では患者に対して責任あるセキュリティ対策を行うことは不可能です。医療機関として接続状況を把握し、コントロールすることが必須です。

４．１．１　構成管理

医療情報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し、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し、不正な機器が接続されたり、不正なソフトウェアやデータが混入されたり、異常なデータ通信が発生したりすることがないよう、管理する必要があります。

特に、セキュアなネットワークを整備する観点からは、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等を実施し、セキュリティを確保することが重要です。

４．１．２　アカウント管理

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しておく必要があります。

特に、システム関連事業者を含めて、システムの管理を行う関係者のアカウントの管理は厳重に行う必要があります。

３．３の項でも少し触れましたが、不正ソフトウェアはシステムを解析し、管理者権限を奪取し、防御を無力化します。管理者権限を奪取されると、アクティブディレクトリや LDAP のような利用者認証のコントロールは奪われますが、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しておくと、時間稼ぎにはなりますし、うまく行けばバックアアップ系やセキュリティ系を守ることができます。

また、昨今の情報システムは複雑で、様々なシステムが互いに自動的に連携したり、支援・制御していたりします。アカウント管理に、システムやアプリケーション等のソフトウェアも含めて管理することが重要です。

Windows のような PC の OS でもサーバ系の Linux 系の OS でも極めて多機能で、様々なプロセスがインストールされており、必要に応じて、あるいは自動的に起動されています。医療情報システムで利用しない機能は起動する必要はありません。起動していると、そのプロセスに脆弱性があればサイバー攻撃の侵入口になります。不要なプロセスやプログラムは削除あるいは起動しないようにシステム関連事業者に要求してください。また、実際に不要なプロセスが起動されていないかの監視も重要です。削除や起動静止していたプロセスが、セキュリティパッチによって再生することもあります。

４．１．３　監視

機器構成やアカウントを管理することで、システムやネットワークに対する不正な侵入が検知でき、不正アクセスを防止することが可能となり、さらには、不正な侵入等がなされた際においても、不正なソフトウェアやデータによる正常とは異なる振る舞いを検知する、監視の仕組みを整え、その効果を発揮することが可能となります。

不正侵入の検知や不正アクセスの防止を支援するシステムとしては、IDS（Intrusion Detection System：不正侵入検知システム）/IPS（Intrusion Prevention System：不正侵入防御システム）と称したセキュリティサービスが提供されています。

不正なソフトウェアやデータによる振る舞い検知によるセキュリティサービスとして、EDR（Endpoint Detective and Response）があります。最近の不正ソフトウェアの被害を見ると、従来のパターンマッチングによる不正ソフトウェア検出をすり抜ける不正ソフトウェアが多いと言えます（ゼロ・デイ攻撃)。100%検出できるわけではありませんが、不正ソフトウェアの異常な動きを検出して、被害が出る前に報告します。最近のコンピュータウイルス対策ソフトウェアには EDR 機能も持つものが増えていますが、ライセンス契約によっては活性化していないこともあります。EDR が導入されていればリスクを低下させることが可能です。

4．2　バックアップ

ガバナンスを補完し、少しでもサイバーインシデントが発生した際に、混乱を最小限にとどめ、業務影響や復旧に要する時間等を最小限にするために、システムも含んだ運用面での方針等を定めた BCP の策定、ならびに、システムやデータのバックアップの整備は重要です。

4．2．1　BCP（Business Continuity Plan：事業継続計画）

サイバーインシデントを 100%防止することは不可能ですし、大規模災害もないとは言えません。地域に一定の役割を担う医療機関としては BCP の策定と、BCP に基づく訓練、さらに BCP の持続的な見直しは必須です。昨今の状況を踏まえると、サイバーインシデントも BCP の重要なテーマです。大規模災害の BCP も重要ですが、サイバーインシデントも主要なテーマに入れて BCP を策定し運用してください。非常時には最悪の場合は紙運用や地域の他の医療機関等による支援も視野に含めることも必要です。

4．2．2　システム・データ

医療機関等の担う特性に応じて、「3．3　必要最小限の対策：バックアップ（システム・データ)」を参照し、継続できる業務の範囲を広げ、サイバー攻撃による影響が少しでも軽減されるように、システムやデータのバックアップを策定する必要がある。