御堂筋監査法人ニュースレター Oct 2022

医療機関におけるサイバーセキュリティ対策

公認会計士　川中 敏史
大手監査法人を経て 2022 年から御堂筋監査法人にて勤務。主に医療法人の内部統制指導、監査業務に従事。
保有資格：公認会計士

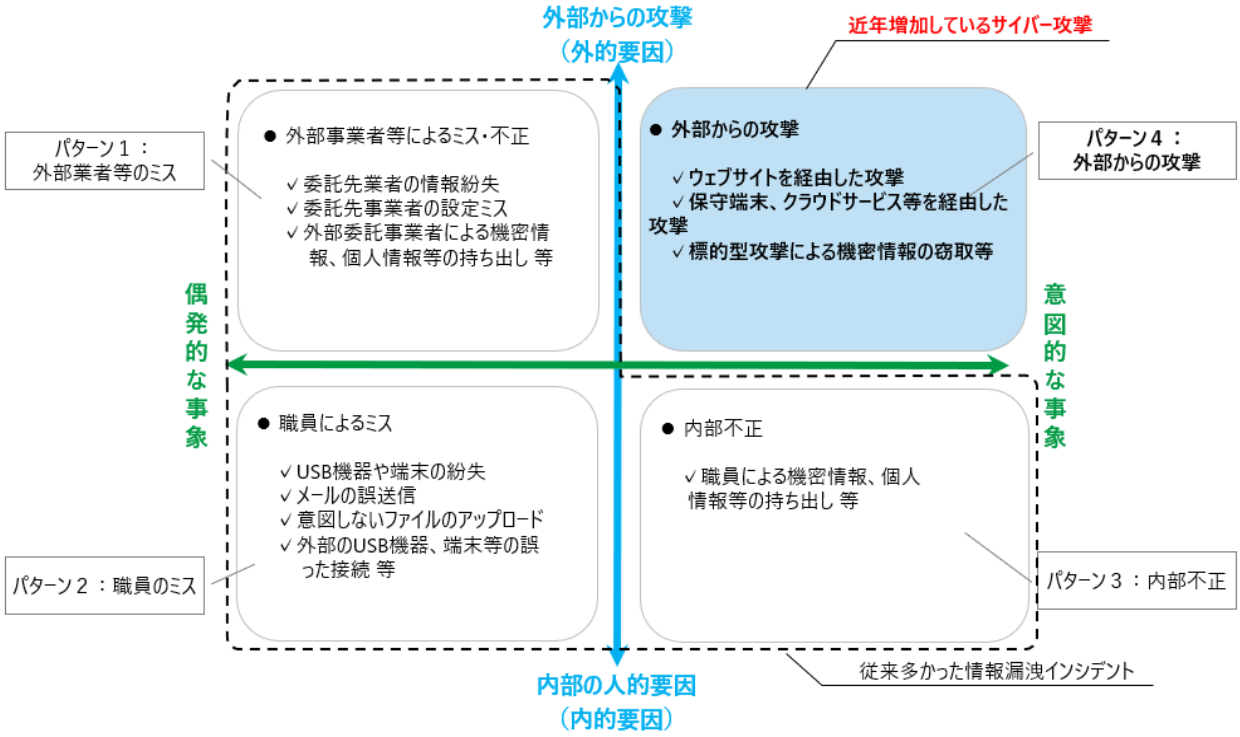
既に広く知られているとおり、近年は医療機関を対象としたサイバー攻撃が増加しています。中でも顕著なものが暗号化等によってファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに金銭（身代金）を要求する「ランサムウェア」を利用した事例です。

これに伴い、厚生労働省は「ランサムウェア」に代表される攻撃への対策を喫緊の課題と捉え、令和４年３月に「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」を公表しました。同ガイドラインの第 5.1 版は令和４年１月に公表されたばかりであり、さらに令和４年度中に具体的なセキュリティ対策の記載をより分かりやすく見直す予定です。これら経緯を考えると、その緊急度を伺い知ることができます。

医事会計システムや電子カルテ等の病院情報システムは、病院運営上不可欠な存在となっており、会計監査の観点からは、サイバーセキュリティ対策は IT アプリケーションシステムが有効に機能することを支える内部統制（IT 全般統制）において必須の評価項目となりますので、サイバー攻撃の事例やセキュリティに関係する厚生労働省や四病院団体協議会の動向等について解説したいと思います。

1. セキュリティ事故の増加

従来は、職員による不正目的の情報持ち出しが多い傾向にありましたが、近年はシステムの脆弱性を利用した外部からのサイバー攻撃被害が急速に増えています。



（引用：厚生労働省「情報セキュリティ研修教材」）

2. 近年のサイバー攻撃事例

下表は、各医療機関から公表されている内容や報道された内容をもとに作成しています。

病院名	鳴門山上病院（徳島県）	安江病院（岐阜県）
発生時期	令和4年6月	令和4年5月
被害状況	電子カルテ及び院内LANシステムが使用不能となり、2日間は新規患者の受け入れを制限。 3日後には通常診療再開。	院内の電子カルテが一時的に使用できなくなり、被害発生当日は一部の業務を制限した診療体制とした。 翌日には通常診療再開。
攻撃手法	ランサムウェア「Lockbit 2.0」によるシステムへの侵入被害。	第三者の不正アクセス（詳細不明）
その他	院内のプリンターから大量の印刷物が出るなどの異常現象が発生。プリンターからは身代金の支払いを求める内容の文書が大量に印刷された。	

病院名	青山病院（大阪府）	春日井リハビリテーション病院（愛知県）
発生時期	令和4年4月	令和4年1月
被害状況	院内の電子カルテが一時的に使用できなくなった。 3日後には通常診療再開。	電子カルテが使用できなくなり、またオンラインで管理していたバックアップデータが暗号化され、使用不能となった。 これにより、カルテはおよそ1ヶ月にわたって手書きでの対応を余儀なくされる等の影響。また、病院の会計システムもおよそ1ヶ月間使用できない状態が続いた。 完全な復旧には数ヶ月かかる見通しと発表。
攻撃手法	ランサムウェア（詳細不明）によるシステムへの侵入被害。	ランサムウェア（詳細不明）による「VPN」（外部接続サービス）の脆弱性が狙われた可能性が高い。
その他	院内のプリンターが一斉に作動して英文の書かれた紙が大量に印刷されたり、パソコンに英語で「金を支払え」といった文字が表示される等した。	サーバーを管理するパソコン画面上に英語で「おめでとう！」というタイトルの文面が表示されたうえ、「ファイルは暗号化した。復元させたければ金を払え」などと書かれており、連絡先として相手のメールアドレスも記載されていた。

病院名	つるぎ町立半田病院（徳島県）	市立東大阪医療センター（大阪府）
時期	令和3年10月	令和3年5月
被害状況	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、使用不能となった。 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。 令和4年1月に通常診療再開。	医療用の撮影画像参照システムがダウンし、使用不能となった。 代替サーバーを立ち上げて稼働を再開しているものの、再稼働前の画像データは閲覧できないままだとしており、通常通りの診察を行うことが困難として、患者が他の病院に行かざるを得ない状況も発生。 3日後には通常診療再開。
攻撃手法	ランサムウェア「Lockbit 2.0」によるシステムへの侵入被害。 米Fortinet社製のFortiGateにより設定されたVPN（外部接続サービス）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「REvil（レビル）」によるシステムへの侵入被害と言われている。 米Fortinet社製のFortiGateにより設定されたVPN（外部接続サービス）の脆弱性を悪用して侵入したものと思われる。
その他	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。	パソコンに英語の警告文が表示され、ＣＴやレントゲンの画像が見られなくなるトラブルが起きた。人の少ない当直時間帯で、現場は混乱。新たな画像も登録出来ないため、新規患者の受け入れをストップしたり、患者の予約を変更したりする等、２日にわたり診療が縮小された。

3. サイバー攻撃による影響

サイバー攻撃を受けた場合には、主に以下の影響が考えられます。

① 患者のプライバシー侵害
電子カルテ情報にアクセスされることで、患者の個人情報が流出する可能性が極めて高くなります。

② 診療業務の停止
電子カルテの情報を閲覧できなくなること等により、通常診療がストップします。
場合によっては、他の近隣医療機関への協力要請が必要となります。

③ 事後対応の負担
データ復旧や原因究明、場合によってはシステムネットワーク全体の見直し等により膨大な時間と費用が必要になる可能性があります。

④ 患者や社会からの信用失墜
最悪の場合には、経営環境悪化により病院存続に危険が及ぶことも想定されます。

4. 個人情報保護法との関係

令和４年４月に施行された改正個人情報保護法では、１件でも患者情報が漏えい、滅失、毀損等した場合もしくはこれらが発生したおそれがある場合には、国の個人情報保護委員会への報告（概ね３～５日以内）と本人通知が義務づけられます。これには、ランサムウェア被害のように患者情報が閲覧できなくなったケースも対象となります。
なお、本人通知が困難な場合は、代替措置として「公表」が求められます。

5. サイバーセキュリティ対策

代表的なセキュリティ対策は以下のとおりになります。

① 組織的対策
情報システム部門の設置、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策定、情報のキャッチアップ、予算確保　等

② 人的対策
情報システム部門への十分かつ適切なリソース配分、職員の教育訓練　等

③ 技術的対策
ウィルス対策、ソフトウェアの適時アップデート（VPN 装置の脆弱性対策等）、定期的なバックアップやログの確認と分析　等

④ 物理的対策
入退館（室）管理、パスワードの定期的な更新や複雑性の確保、専用 USB による制限　等

⑤ その他
セキュリティ知見を有するシステムベンダーの選定及び責任区分の明確化
※システム導入とその後のセキュリティ指導は必ずしもセットでは無いため、不明瞭な場合は契約内容を再確認する必要があります。

6. セキュリティ対策の課題

令和４年１月 31 日～２月 28 日にかけて実施された四病院団体協議会によるセキュリティアンケートに関する調査結果では、９割の医療機関がサイバー攻撃に脅威を感じると回答していますが、NISC や厚労省が指摘した VPN 機器の脆弱性への対応を行っていないと回答した病院が３割程度存在しており、その半数以上が理由を「情報をキャッチできていなかったため」「予算がなかったため」としています。

このように、危機意識を持ちながらも予算不足、人材不足、情報不足等により、厚生労働省が求める十分な体制を構築できていない医療機関が多数存在しているのが現状です。

7. 四病院団体協議会の動向

四病院団体協議会はセキュリティアンケートに関する調査結果を踏まえて、令和４年３月 31 日付けで厚生労働大臣に対し「病院のサイバーセキュリティ対策への公的補助金の支給について」として緊急提言を提出しています。

当該提言においては、サイバーセキュリティ対策の重要性を理解しながらも、厳しい経営環境のため予算に制約がある医療機関の現状を訴え、医療分野での ICT 利用は国が推進してきた施策であることから、サイバーセキュリティ対策に関しても国が費用面での措置を講ずる必要性を訴えています。当該緊急提言において試算された必要となる公的補助金額は下表のとおりです。

病床規模	対IT予算費15%試算 （公助の必要最低水準）	対IT予算費30%試算 （公助の十分水準）
20床~99床	**500万程度**	**800万程度**
100床～199床	**860万程度**	**1700万程度**
200床～299床	**1050万程度**	**2600万程度**
300床～499床	**2100万程度**	**5000万程度**
500床～	**5900万程度**	**1億3000万程度**

（引用：四病院団体協議会「病院のサイバーセキュリティ対策への公的補助金の支給について（緊急提言）」）

8. 公表資料等のご案内

＜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）
・「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」に関する Q&A（令和４年４月）
・「医療機関のサイバーセキュリティ対策チェックリスト」（令和４年５月）
・「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」（令和４年５月）

※上記以外にも、情報セキュリティの教育研修のための研修動画が（経営層向け）、（システム管理者・セキュリティ管理者向け）、（医療従事者向け）の各バージョンで公開されています。

＜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」（令和４年６月）
※全国の病院や事業所のセキュリティ強化に貢献するという目的から、インシデント発生に至った原因や構造的な問題点等を有識者によって詳細に分析した内容が公表されています。

9. まとめ

既に述べたように、医療機関独自で必要十分な対策を構築するには構造的な限界がある状況が浮き彫りになってきています。

医療が社会において重要なインフラである以上、今後は国も巻き込みながら改革を進めていく必要性は高いと考えられますが、まずは各医療機関における現状把握が必須と言えます。

セキュリティ対策を見直す際には、厚生労働省が公表する「医療機関のサイバーセキュリティ対策チェックリスト」やつるぎ町立半田病院の「有識者会議調査報告書」を利用すること及び外部機関による評価を受けることが有用と考えます。

以上