IT ベンダによる国内医療機関との
リスクコミュニケーションのありかた

2022 年 11 月

一般社団法人医療 ISAC

株式会社 Box Japan

０．はじめに

国内で医療情報を電子的に取り扱う場合、医療機関、及び医療情報システム・サービスを提供する事業者（以下、「IT ベンダ」）はいわゆる<3 省２ガイドライン>をそれぞれの立場で遵守することが求められている。具体的には、医療機関は厚生労働省「医療情報システムに関する安全管理ガイドライン」（以下、「医療機関向け GL」と記載）、IT ベンダは経済産業省・総務省「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」（以下、「事業者向け GL」）を遵守することがコンプライアンスとして求められている。

３省２ガイドラインは、リスクマネジメントとリスクコミュニケーションという二つのコンセプトにより構成されているといえるが、その中で**重要なものはリスクコミュニケーション**である。
医療情報システムを利用する医療機関と医療情報システムを提供する IT ベンダが、患者診療の継続性・信頼性を担保するために、互いにどのようなセキュリティ対策を講じるべきなのかについて、双方が同一の目線のもとで合意形成を行うコミュニケーションが十分でなければ、システム利用主体/提供主体のリスクマネジメントの地平はかみ合うことなく、本来行われるべき対策が見落とされる可能性がある。実際にこうした医療機関/IT ベンダ間のリスクコミュニケーションが十分でないことにより、昨今、様々な医療情報システムがランサムウェア等のサイバー攻撃の被害を受け、その結果として、本来最優先的に守られるべき患者への被害が発生している点は銘記すべきである。

医療 ISAC はこうしたリスクコミュニケーション --- 医療機関が自院のセキュリティ対策を検討する上で必要となる、IT ベンダによる能動的な情報提供 --- の重要性について、様々なセミナーや講演会で発信することに加え、IT ベンダとして果たすべきリスクコミュニケーションのあり方についてもレポートを公開する取組を行ってきた。日本マイクロソフト株式会社との共同レポートがそれである。

しかしながら、まだその取組が IT ベンダの多くには浸透していない状況が多く見受けられている。そのため、今回、医療 ISAC は、IT ベンダによるリスクコミュニケーションの事例を別の角度から照らすべく、株式会社 Box Japan（以下、「Box」と記載）の協力のもと、

Box が提供する SaaS サービス（以下、「Box サービス」と記載）を対象とした共同レポートを公開する。本レポートの目的は、医療機関における構造的な課題を分析するとともに、Box の SaaS サービスがどのようにその課題への対策になり得るものであるかについて、医療機関へ「翻訳」することにある。

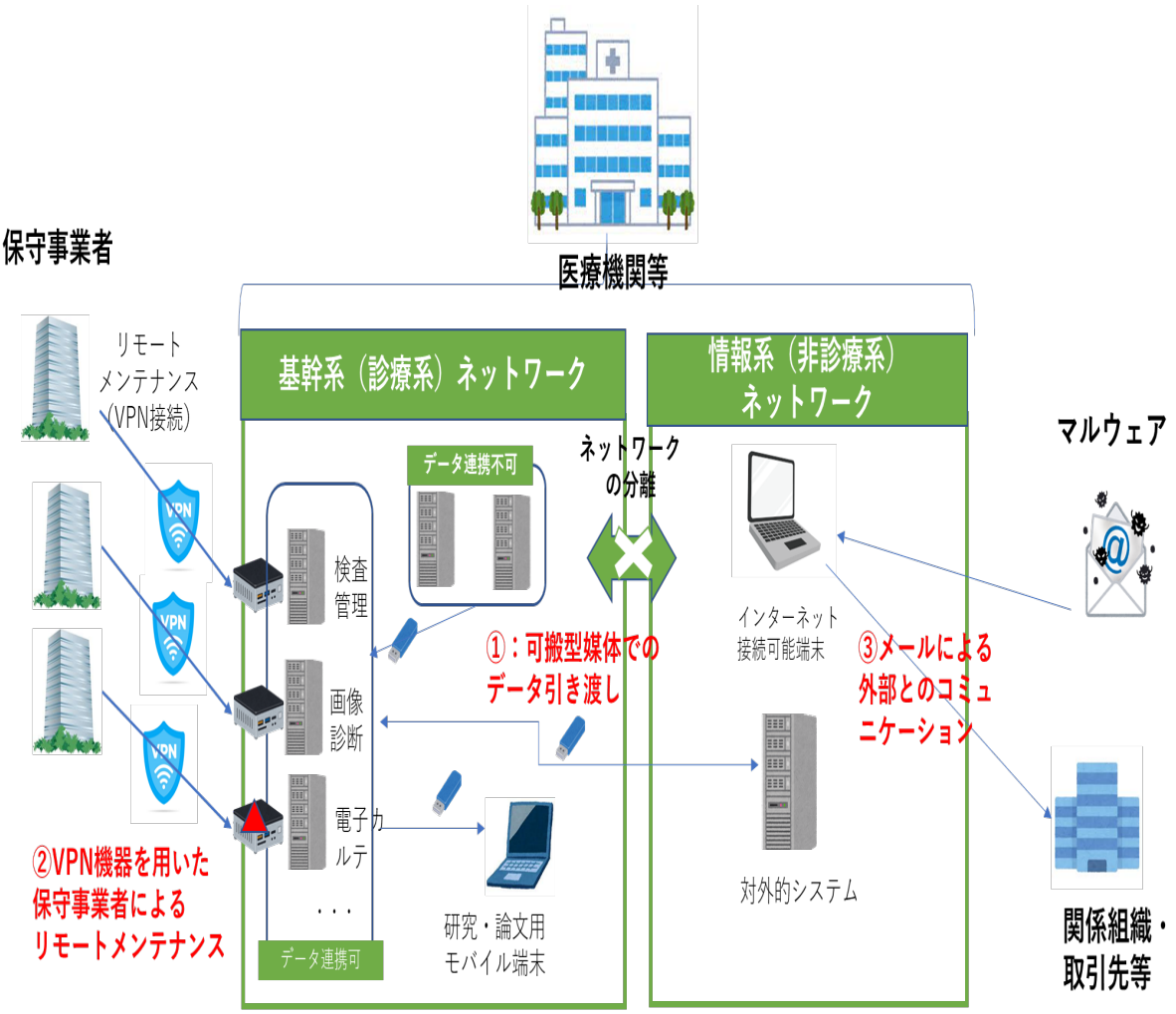
日本マイクロソフト株式会社との共同レポートでは、IaaS/PaaS レイヤーのクラウドサービスを論じたが、今回は SaaS サービスを取上げることで、SaaS レイヤーのクラウドサービスを提供する IT ベンダがどのような観点から医療機関とのリスクコミュニケーション ---- 能動的な情報提供を行うべきなのかの事例を示すことが出来ればと考えている。

本レポートでは、第 1 章で国内医療機関における医療情報の流れを規定する、一般的なシステム・ネットワーク環境を整理するとともに、そこにどのようなセキュリティ上の課題が想定されるかをリスクシナリオ別に紐解いていく。その内容に基づき、第 2 章では、その課題への対応を検討するうえで、Box サービスの機能を医療機関がどのように利活用できるかという観点で整理した。

今回、医療 ISAC の取組に賛同いただき、技術面の情報提供等にご協力頂いた Box には感謝の念を申し上げる。このレポートが、IT ベンダによる医療機関ファーストのリスクコミュニケーションというまだ数少ない取組の拡大に何らかの寄与ができることを期待する。

１．医療機関におけるセキュリティ管理の課題傾向

国内の医療機関 --- 本レポートでは病院とクリニックを指す ---- のシステム・ネットワークは、一般的に、患者診療に直結する医療情報システム（電子カルテシステム、画像診断システム、検査管理システム等）が設置される基幹系（診療系）ネットワークと、患者診療に間接的に関連するシステム、あるいは外部との対外的な情報のやり取りを目的としたシステム等が設置される非診療系（情報系）ネットワークが、分離されるかたちで管理されることが多い。この状況に基づき、一般的な医療機関におけるセキュリティリスクが顕在化するシナリオを図示すると以下の通りとなる。それぞれ検討すべきセキュリティ上のポイントを三つのリスクシナリオに応じて整理する。



＜①　：可搬型記憶媒体によるデータの引き渡し＞

前述の通り、基幹系ネットワークと情報系ネットワークは分離されているため、各ネットワークに設置されるシステム間のデータ移行は原則、USB メモリやポータブル HDD 等の可搬型の外部記憶媒体を利用せざるを得ない。さらに、基幹系ネットワークにおける、患者診療に不可欠な医療情報システムも必ずしも全てのシステム間で一元的なデータ連携が行える設定にはなっていない。医療情報システムはその用途・目的別に様々なメーカが開発・販売していることから、メーカ間の規格・仕様も異なることが多い。また、異なるメーカのシステム間のデータ連携機能を開発しようとすると、膨大なコストがかかることも少なくない。そのため、医療機関では、本来自動的に連携されるべきデータや共有するファイルを職員が可搬型の記憶媒体にコピーし、別の職員に引き渡すマニュアル作業がいまだに多く見受けられている。
また、医療機関には医師や看護師等、専門職が集うため、その専門性を研鑽するための研究・論文作成、または資格更新等の目的で、医療情報システムからデータを抜き出し、可搬型記憶媒体を用いて、持ち出し可能なモバイル端末にコピーすること等もおのずと発生する。

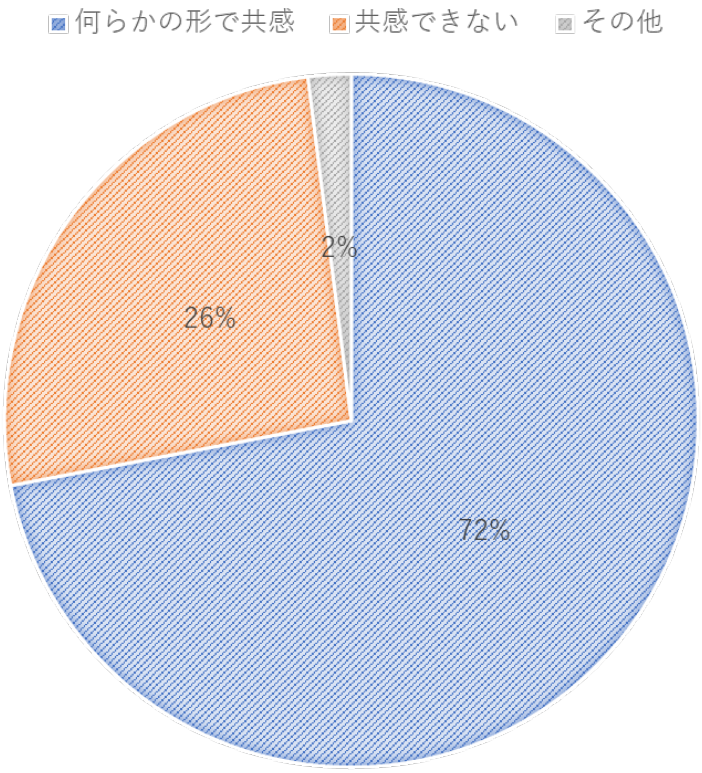
このような状況下では、患者情報を格納した可搬型記憶媒体の紛失、または患者情報をコピーしたモバイル端末の盗難に伴う、**情報漏洩というセキュリティリスクが非常に高い**と言える。実際に、昨今、医療機関におけるセキュリティインシデントはランサムウェアによる医療情報システムの利用停止という事態が急増している一方、こうした医療機関におけるシステム・ネットワーク構造固有の、昔ながらの可搬型記憶媒体による情報漏洩のインシデントは、今も多数発生している状況である点は留意すべきである。

＜②　：ＶＰＮ機器を用いた保守事業者によるリモートメンテナンス＞

院内ネットワークは基幹系と情報系に分離され、後者はインターネット接続が前提の環境となるため、この範囲にはウイルス対策ソフトやセキュリティパッチの適用等、セキュリティ対策が積極的に行われる一方、前者にはそうした対策が劣後しがちなことが医療機関の一般的な傾向である。これは、基幹系ネットワークはクローズド環境であるためセキュリティ面で無対策でも安心であるという考え方に基づいており、2022 年 3 月に四病院団体協議

会加盟病院向けに行ったセキュリティアンケート調査[1]においても、こうした考え方に何らかのかたちで共感する回答割合は７割以上と、根強いことがうかがえる。

■「診療系ネットワークは安全であるという考え」への共感度



しかしながら、**基幹系ネットワーク内の医療情報システムには保守業者によるリモートメンテナンス用の接続経路が高確率で設置されることも一般的**である。医療情報システムは患者診療に不可欠であるため、何らかの不具合が発生した場合は適時に保守事業者のメンテナンスが必要なためである。IT ベンダとしても毎回不具合が発生するたびに医療機関に直接訪問するより、リモートメンテナンスで対応可能な不具合は、効率的にリモートで対応したいものであり、医療機関と IT ベンダの利害が一致した結果といえる。

一方、リモートメンテナンス用の VPN 機器の脆弱性が標的とされ、基幹系ネットワークの医療情報システムがランサムウェアにより暗号化され、利用不可となる事態が相次いでい

[1] 一般社団法人医療 ISAC 「四病院団体協議会セキュリティアンケート調査結果（最終報告）
http://www.hospital.or.jp/pdf/06_20220323_01.pdf

る。2021 年 10 月に発生した徳島県の町立病院の調査報告書[2]でも同種の原因が指摘されているが、医療 ISAC が把握する限り、国内の医療機関でランサムウェア被害に遭遇している事例の大半はこれが主原因となっている。
また、院内の基幹系/情報系ネットワークを仮想的に分離しているネットワーク機器も医療 ISAC の調査によれば十分な設定が行われず、情報系から基幹系ネットワークへ接続できる抜け道が残っているケースも見受けられている。

こうした状況は、基幹系ネットワークは外部ネットワークと遮断しているため、セキュリティ対策を講じる必要がないという、安全神話に依拠することの危うさを示している。医療機関としては、基幹系/情報系ネットワークの区分なく、フラットに院内ネットワークにおけるセキュリティリスクを考えなければならない。こうした考えを欠くことは、**ランサムウェアによる感染被害により、患者診療の継続性を著しく損なう事態に直面するリスク**をもたらすことになる。

<③：メールによる外部とのコミュニケーション>

医療機関では通常業務の一環として、様々な外部組織とメールで電子的なコミュニケーションを行っている。連携/支援先の医療機関への患者照会・紹介、Doctor to Doctor による診療支援のやり取り等の診療業務に関連するものから、業者や取引先等とのやり取り等の事務業務に至るまで幅広く行われている。

外部との電子的なメールコミュニケーションというシナリオにおいて、メール受信主体の立場から見た場合、**受信したメールに悪意あるファイルが添付され、それにより院内ネットワーク・システムへウイルス感染が発生するリスク**が想定される。メールのやり取りを行うための院内 PC は情報系に設置されるかもしれないが、そもそも基幹系/情報系の仮想分離自体が十分でなければ、情報系で感染したマルウェアは基幹系へ増殖を図ることになる。
直近でも Emotet が爆発的に流行しているが、こうしたセキュリティリスクは本質的に**人的な脆弱性リスク**に強く関係している。

加えて、情報系ネットワークにおいて対外的な情報を発信する主体としては、もちろん**メー**

2 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)
https://www.handa-hospital.jp/topics/2022/0616/index.html

ルの送付先を誤り、本来知らせるべきでない第三者に患者情報等の機微情報を伝えてしまうという古典的な情報漏洩リスクが想定される。これは目新しいものではない。電子メールという技術が登場するまでは、FAX や郵便物を介してアナログに情報のやり取りが行われたが、そのような情報交換のシナリオのなかで、誤った相手先に郵便物が送られてしまうというリスクの変奏がこのシナリオに該当する。特に医療機関では常勤医師、非常勤医師、看護師、薬剤師、コメディカル、ひいては関係医療機関からの応援等も含め、人の出入りが著しく、IT・セキュリティリテラシーの水準も同一ではないことが一般的である。そのため、こうした環境下では、メールの誤送信というインシデントに対するリスク感度も異なることは避けられない。

なお、こうしたメールの誤送信による情報漏洩リスクも、メールを送付する者がしっかり事前にチェックをするという対策により低減可能なものである。しかし、その対策は結局**人的な脆弱性リスク**によってその水準が左右されてしまうという課題を抱えている。こうした人的な脆弱性リスクをいかに低減するかは情報漏洩リスクへの対策を検討する上で非常に重要である。

<まとめ>

論旨をまとめよう。国内の医療機関特有のシステム・ネットワーク環境における情報流を踏まえて、一般的に想定されうるリスクシナリオ別に、セキュリティポイントを整理した結果、以下 3 点の構造的な課題が浮かび上がった。

A) 医療情報システム間のシームレスなデータ連携の困難さは、可搬型の外部記憶媒体によりデータの授受という慣習をもたらし、その結果、そうした**記憶媒体の紛失・盗難等による情報漏洩リスクが極めて高いこと**。

B) 医療機関の院内ネットワークは内部関係者の多くにとっては患者診療に直結する医療情報システムは外部ネットワークと切り離して管理していると考えている。しかし、例えば保守事業者によるリモートメンテナンス接続経路の存在は、実質的にそうした考えが適用し得ない事態を示しており、**医療機関としては患者診療に不可欠なデータ・ファイルの優先的な保護・保全が重要である**こと。

C) 外部組織との電子的なコミュニケーションの代表例である電子メールは、受信主体として**悪意あるファイルによる攻撃リスクに常に晒されている**こと。また送信主体とし

ては添付ファイルを誤った第三者へ送信するといった、**人的な脆弱性リスクを抱えている**こと

このような医療機関を取り巻く課題に対して、Box サービスの機能を利活用することで対応が可能であろうか？

2．クラウドサービスの利用による課題対応方法

Box サービスは事業者向け GL が求めるリスクマネジメント、及び医療機関に対するリスクコミュニケーションに関する各種資料が公開[3]されている。そのため、事業者向けＧＬへの対応状況の詳細については、Box にコンタクトの上、情報提供を依頼することが合理的である。

そのため、本レポートでは主に第 1 章で整理した医療機関を取り巻く構造的なセキュリティ上の課題に対して、Box サービスの諸機能がどのように対応策を提示するのかについて、もう一歩踏み込んだ着眼点を医療機関へ情報提供することが目的である。

＜A. 情報漏洩リスクを低減する、効果的な医療情報共有に向けて＞

医療情報システム間のデータ引き渡し作業を可搬型記憶媒体を用いて行えば、その記憶媒体の紛失等に伴うセキュリティリスクが懸念される。

Box サービスでは、事業者向け GL への対応が図られたシステム環境のもとで、特定多数のサービスユーザがファイルを共有し、編集・管理等を行うことが可能な機能が提供されている。各サービスユーザは一意の ID を持ち、その権限に応じたファイルへのアクセス設定可能となっている。アクセス権限はフォルダ単位のみでなく、個々のファイル単位でも付与可能である。

また、ファイル編集中に該当ファイルへのアクセス権限を持たないメンバーの関与が必要となる場合には、当該ファイルのオーナーであれば、そのメンバー（組織の内外を問わない）へファイル単位でアクセス権限を付与（コラボレーション）することも可能[4]である。この場合、そのメンバーは他のフォルダやファイルにはアクセスできず、付与された権限の範囲の中でのみ操作が可能となる仕様である。

こうしたコラボレートに際した権限設定も様々な役割に応じた設定が可能となっているため、例えば、IT 管理リソースの少ない医療機関においてシステム管理者への申請を行わなくとも、**ファイルオーナー（例えば医師や看護師、あるいは現場職員等）の現実的な裁量の**

---

[3] Box 社：3 省 2 ガイドライン リファレンスドキュメント
https://www.boxsquare.jp/resource/3-ministry-2-guidelines-reference-document

[4] Box 社：コラボレータの権限レベルについて
https://support.box.com/hc/ja/articles/360044196413-コラボレータの権限レベルについて

もとで、詳細なデータアクセス権限の付与・管理が可能となるという利点がある。

Box サービスではファイルへのアクセスに際した本人認証として、多要素認証を標準的なサービスとして提供している[5]。医療機関向け GL では令和 9 年まで稼働している医療情報システム・サービスについては本人認証機能として多要素認証が義務付けられている。こうした機能が Box サービスに標準的に提供されていることは、本人認証の強度を高めるだけでなく、Box サービスにおいては、仮にパスワードという認証要素が第三者に悪用されたとしても、事前に登録してあるモバイル端末等、もう一つの認証要素に本人通知が行われることで、ユーザ自身がパスワード漏洩という事実に気づき、適切な対策を講じることを可能にすることも意味する。その意味で、**これはユーザ自身のセキュリティリテラシーの向上にも寄与するという点で教育的な効果も期待できる**ものである。

なお、こうした多要素認証は組織内部のみでなく、ファイルオーナーがコラボレーション権限を付与した外部組織においても要求することが可能である[6]。そのため、医療機関内部では認証強度が高い一方で、外部関係者にはパスワード認証しか要求できない等の理由で、内外のファイル共有における認証水準が低下するリスクにも対応が可能である。医師の多くは非常勤医師として兼業・副業を行うことが一般的であり、様々な医療機関における異なる患者情報へアクセスすることが求められる。そのため、こうした機能を用いることで、**様々な医療機関における担当患者の情報等へセキュアにアクセスする**ことが実現できると言える。
また、パスワードという認証要素を失念したとしても、自らがパスワードの再発行処理を行うことが出来るた[7]め、**医療機関のシステム管理者を悩ます「パスワードを忘れたので再発行してほしい」という声の量もおのずと減らす**ことができる。

加えて、Box サービス上のデータ・ファイルは、アップロード時点から、該当ファイルへの

---

[5] Box 社：アカウントの多要素認証の設定
https://support.box.com/hc/ja/articles/360043697154-アカウントの多要素認証の設定

[6] Box 社：外部コラボレーション向けの 2 要素認証の登録
https://support.box.com/hc/ja/articles/360044196473-外部コラボレーション向けの 2 要素認証の登録

[7] Box 社：　Box アカウントのパスワードをリセットする方法
https://support.box.com/hc/ja/articles/360044195593-Box アカウントのパスワードをリセットする方法

参照・更新・削除等のユーザーアクティビティ、つまりアクセス履歴が時系列で確認可能[8]となっており、ファイルへのアクセスログが一元的に管理・保全されている。これらのアクセスログはシステム管理者であっても変更できない仕様で厳密に保全されているため、ログの改ざん・削除等を内部不正、あるいはサイバー攻撃者による意図で行うことは困難な仕組みとなっている。医療情報の中には医師法等による法定保存義務が定められる文書が存在するが、こうした文書への電子的なアクセスの実績について、Box サービスでは標準で 7 年間の自動保存が行われる仕様となっている。患者診療に不可欠な診療録の法定保存期間は 5 年間であり、それに類する情報類も一定期間の保存が必要となるが、それを超える期間において**該当情報への電子的なアクセス記録を標準機能として保管できる点は、医療機関にとってはコンプライアンス対応の観点からもメリットがある**であろう。

このように Box サービスの本人認証・アクセス権限という予防的なセキュリティ対策に加え、当該サービスにおいて一定期間における該当ファイルへのアクセス履歴の保全性という発見的なセキュリティ対策は、必要最低限のメンバーに必要な権限に絞った範囲でファイルへのアクセスを効率的に実現するとともに、その履歴を十分な期間検証できる仕組みを提供している。そのため、可搬型記録媒体を用いずとも、**医療機関の内部関係者、あるいは地域医療連携等の横断的な医療機関間において、現場リードで患者情報の共有をセキュアに行う上で効果的な対策**と言えるだろう。

＜B. 患者診療に不可欠な医療データ・ファイルの優先的保護に向けて＞

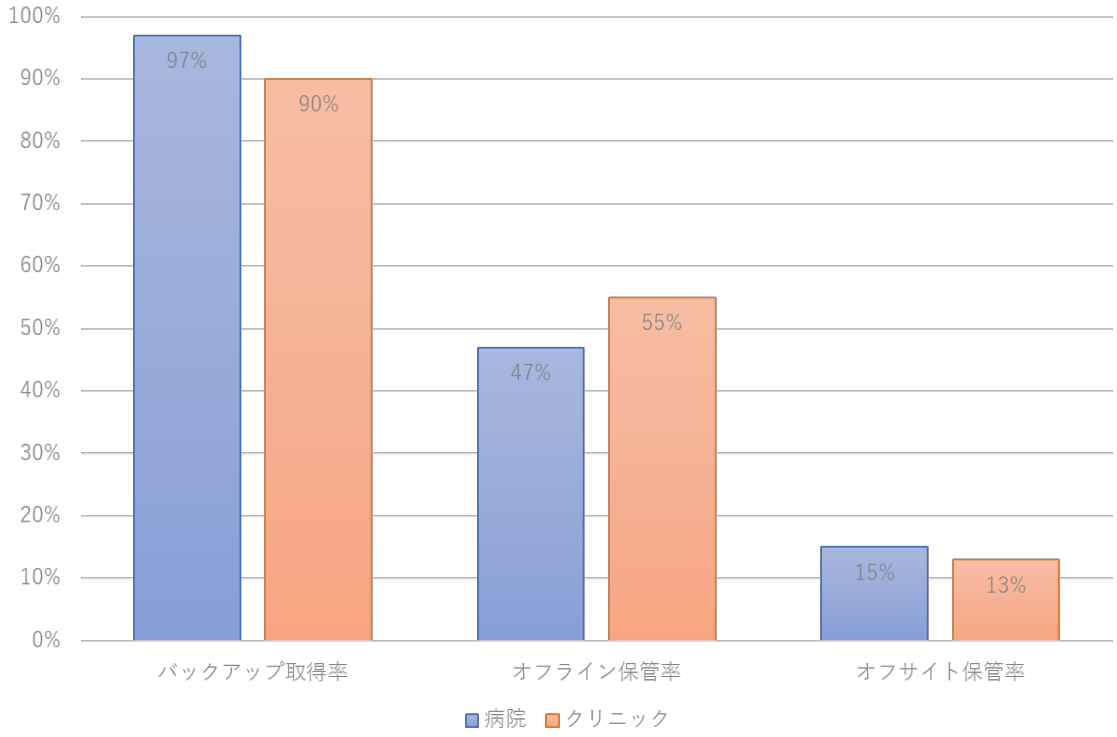
第 1 章で整理した通り、医療機関の院内ネットワークを構成する基幹系/情報系の区分に基づく境界防御的な考え方は、当今のサイバーセキュリティ動向等を勘案しても、すでに形骸化していると言える。院内ネットワークは外部と遮断した無菌室ではなく、常に外部との接点を持ち、見知らぬウイルスや脆弱性がネットワーク内には充満している状況と言える。例えるなら、新型コロナ対策で医療機関でもコロナ専用病床が厳重な感染症対策のもとで行われていたにもかかわらず、一部の機関では一般病床へのコロナ感染が見受けられていた通り、完全な無菌室の確保はサイバー空間においても不可能である。

[8] Box 社：[ユーザークティビティ] レポート
https://support.box.com/hc/ja/articles/4415012490387--ユーザークティビティ-レポート

こうした観点に立った場合、診療系ネットワークにおける医療情報システムが取り扱うデータ・ファイルのうち、特に患者診療の継続性に不可欠なもの特定し、**Box サービスをオフサイトのバックアップ環境として利活用すること**が一案として考えられる。

例えば、医療 ISAC による四病院団体協議会加盟病院、及び一部の都道府県保険医協会加盟クリニック群を対象としたセキュリティ調査ではバックアップの取得はほとんどの医療機関が行っているものの、ランサムウェアに備えて、バックアップをネットワークから切り離したオフライン環境で保管している割合は全体の半数前後に低下し、外部のクラウドサービスを利用したオフサイト環境に保管している割合は 2 割以下の水準である。

■医療機関におけるバックアップ取得、及び保管率



令和 4 年度の医療法 25 条第 1 項に基づく立入検査の中で、サイバーセキュリティは医療安全管理の一環として定義され[9]、ランサムウェア被害を想定したバックアップの十分性が検査されることになる。こうした医療行政の動向も考慮した場合、院内ネットワーク上にデータバックアップを保管するにとどまる医療機関にとって Box サービスはバックアップデ

[9] 厚生労働省「令和 4 年度の医療法第 25 条第 1 項の規定に基づく立入検査の実施について」(2022 年 5 月 27 日)
https://www.mhlw.go.jp/web/t_doc?dataId=00tc6767&dataType=1&pageNo=1

ータストレージとして利活用することができるだろう。

さらに Box サービスでは、アップロードされたデータについては変更・更新が発生する度に履歴管理が行われ、世代管理が自動的に行われるという特徴もある。そのため、オペレーションミスでデータの一部の誤った変更や削除等が発生したとしても、簡単な手続で適時に復元することが可能である。そのため、医療機関では必ずしも IT リテラシーの高くない職員がシステム管理者になることも多いが、**IT リテラシーの十分でない職員がバックアップの管理を担うことになり、そこで何らかのオペレーショミスが発生しても容易にデータの復元が可能**である。

<C. メールによるセキュアな電子的なコミュニケーションに向けて>

一般的に医療機関では、内外の関係者と情報共有を行う電子的なツールとしては未だメールが主流となる。電子メールにファイルを添付し、内外と情報共有を行う環境を持つということは、同時に外部から悪意のあるファイルを添付したメールを受信するリスクとともに、内部から本来共有すべきでない第三者に対して患者情報を含む内部の諸情報を送信するリスクを抱えることになる。

一般財団法人日本情報経済社会推進協会（JIPDEC）の調査によれば、2021 年度において、JIPDEC へ報告のあった国内セキュリティインシデントの中で、相手先を間違えた情報の送付 --- 書類等送付における宛名間違い・封入ミス、メールの誤送信、FAX 誤送信 ---はインシデント種別のなかで最も多く、その中でもメールの誤送信が最も多いことが示されている。[10]

こうしたインシデントは医療機関固有の課題ではないが、特に医療機関では、医師、看護師、薬剤師、コメディカル、介護福祉士等、該当機関のみでなく、関係機関も含めた多職種連携の下で患者ケアが行われるため、特定組織のポリシーを一元的に適用したセキュリティリテラシーの啓発も困難になりかねない。そのため、誤って無関係な別の医療機関の担当者へ

[10] 一般財団法人日本情報経済社会推進協会：「2021 年度個人情報の取扱いにおける事故報告集計結果」(2022 年 10 月 7 日)
https://privacymark.jp/system/reference/pdf/2021JikoHoukoku_221007.pdf

患者ファイルをメール送信してしまう、あるいは内部関係者を装ったメールに添付された悪意あるファイルを何気なく開封しウイルスに感染するというリスクを完全に低減することは難しい。

Box サービスでは、Box 共有リンクという機能を使用[11]することで、メールにファイルを添付せずとも、その共有リンク(URL)をメールに記すことで、情報を共有したい相手に対して容易にファイルへのアクセスしてもらうことが可能である。アクセス権限に加えて、共有するファイルへの操作も制限することができる。参照のみの他、編集権限、またはダウンロード可能等も設定できる。さらには、その共有リンクの有効期限（アクセス可能期間）の期間も設定可能である。
そのため、**この機能を利活用することで、何気なく添付ファイルを開封してしまう人的な脆弱性リスクを回避**できる。また、添付ファイルをダウンロードし、ローカル端末環境で開封することにより該当ファイルが相手先の PC に残存した結果、**その PC が盗難・紛失した場合の情報漏洩リスクも回避可能**と言える。

悪意ある攻撃者が仮に悪意あるファイルを添付したメールによる攻撃を行ってきても、そもそも Box サービスでの情報共有を医療機関の関係者が前提とする運用を採用していれば、ファイル添付によるメールコミュニケーション自体の不自然さ、つまり攻撃リスクにすぐに気付くことができるだろう。相手先の PC にファイルダウンロードを禁止すれば、PC 紛失・盗難によるメールにより共有していた情報の漏洩リスクの心配もない。有効期間の設定により、不要となった共有リンクがインターネット上でアクセスされるリスクも低減できる。

医療機関では IT・セキュリティリテラシー水準の異なる職員がメールによる情報共有等を行わざるをえず、おのずとうっかりミスといった人的な脆弱性リスクが高くなる傾向がある。しかし、こうした技術的な仕組みを採用することで、メールという電子的なコミュニケーションに不可避的に伴う人的な脆弱性リスクを効果的に低減し、セキュアなコミュニケーションが実現可能になると言える。

[11] Box 社：メール添付に代わる共有リンク
https://support.box.com/hc/ja/articles/360043693634-メール添付に代わる共有リンク

<おわりに>

以上の通り、医療機関のシステム・ネットワーク固有の環境、または業務構造等を踏まえた観点より、Box サービスが医療機関においてどのように利活用できるかについての着眼点を解説してきた。これらの着眼点はあくまで Box の懇意により提供された、限られた情報に基づくものとなる。そのため、医療機関としては、上記以外のセキュリティ・オペレーション上の課題を整理のうえ、より詳細な情報提供を Box に行うことで、医療機関としても能動的なリスクコミュニケーションに着手することが期待される。


Medical Information
Sharing and Analysis Center


box