クラウド時代の医療情報セキュリティの考え方
～国内病院の課題解決を志向する
リスクコミュニケーションの重要性～

2022 年 1 月

一般社団法人医療 ISAC

日本マイクロソフト株式会社

目次

はじめに 3

１. 国内病院固有のセキュリティ管理の実状 5

2. クラウド利用による課題対応方法 11

おわりに 16

はじめに

医療 ISAC では国内の病院がどのようなセキュリティ対策を講じているかの実態を把握するために、一般社団法人日本病院会の協力を得て、セキュリティに関するアンケート調査を行い、その結果を分析した報告書（以下、「セキュリティ分析レポート」）を公開した。[1]

本報告書では、国内病院では病床規模が小さくなればなるほどセキュリティ管理水準が低下する傾向があることが示されている。国内では報道に上がらないものも含め、ここ 1 年で、様々な病院がランサムウェアに感染し、医療提供の制限が発生している事例が相次いでいる状況である。ランサムウェアという、医療情報システムを利用不可にし、医療提供の継続性に深刻な影響をおよぼすサイバー攻撃に対して今や病院はまったなしの対応が必要となっている。

国内には医療情報システムのセキュリティを考える上で不可欠なガイドラインが存在する。いわゆる「3 省 2 ガイドライン」といわれるものである。厚生労働省が病院向けに公表する「医療情報システムの安全管理に関するガイドライン」と、経済産業省・総務省が IT 事業者向けに公表する「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」がそれに当たる。
特に 2020 年 8 月に改定された IT 事業者向けガイドラインでは、病院によるセキュリティ対策を IT 事業者がサポートする役割の重要性が強調されており、医療情報システム全体のセキュリティを確保する上で、IT 事業者としてどのようなセキュリティ対策を講じているのか、または病院に対してどのような対策を依頼するのか等を含め、「リスクコミュニケーション」を行うことが求められるようになっている。

病院におけるセキュリティリソースの不足という課題を踏まえた場合、IT 事業者によるセキュリティ対策に係る情報発信においても、病院というユーザ目線に立ち、その課題を意識したリスクコミュニケーションが必要になる。国内の病院で求められるセキュリティは、病院の業務構造・特性に

[1] Report：国内病院に対するセキュリティアンケート調査の結果と考察

https://www.m-isac.jp/2021/12/20/report01/f

大きく規定される。こうした病院の業務組織等を踏まえた上で、IT 事業者が提供する機能を用いることで、どのようなセキュリティ上の課題への対応が行えるのかについて、病院のユーザ目線に立って翻訳する取組は、しっかりしたセキュリティ組織を持たない多くの病院にとって有益な情報提供になるものである。こうした取組こそが「3 省 2 ガイドライン」で IT 事業者に本来求められているものである。

しかしながら、このような病院のセキュリティにおける現場の課題を踏まえた、ユーザファーストの「翻訳」の取組はいまだ十分に進んでいない状況である。

本レポートは、そうした取組の重要性を啓発し、その拡大に向けた一石になることを目的として、医療 ISAC が、日本マイクロソフト株式会社（以下、「日本マイクロソフト」）の協力の下で、取りまとめたものとなっている。

本レポートでは、第 1 章で医療 ISAC がセキュリティ分析レポートの結果に基づき、国内病院におけるセキュリティ対応上の課題傾向を分析している。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、Microsoft が提供するクラウドサービス上の製品・機能がどのように利活用できるのかについて解説を行った。

本取組の理念に共感頂き、情報提供等にご協力頂いた日本マイクロソフトに感謝の念を申し上げるとともに、病院向けのシステムやクラウドサービスを提供する他の IT 事業者においても、同様の取組が今後続いていくことを期待する。

1．国内病院固有のセキュリティ管理の実状

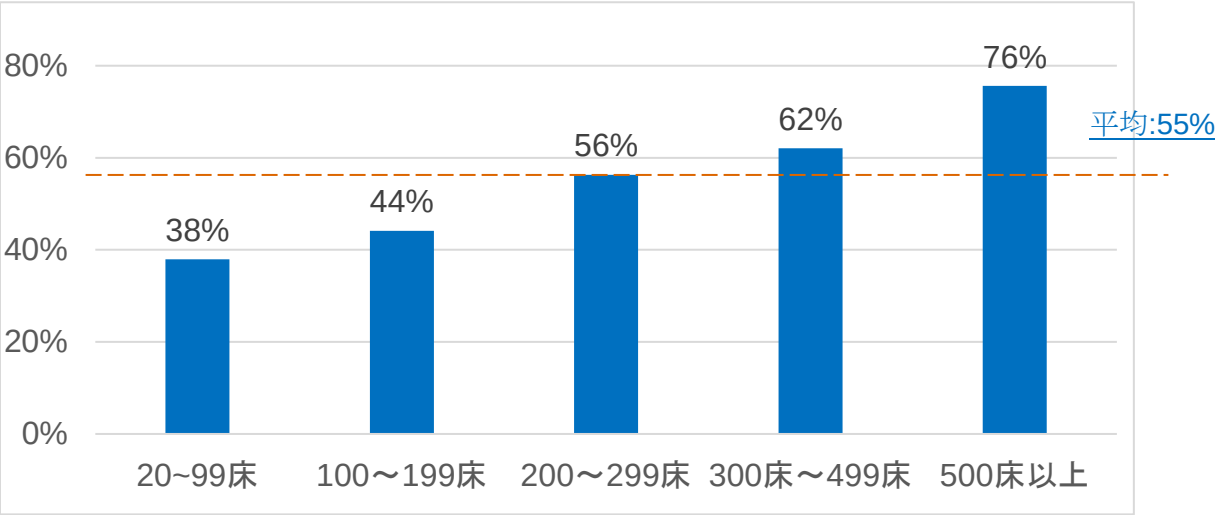
本レポートでは、セキュリティ分析レポートでも報告している一般的なセキュリティ対策、つまり医療情報への不適切なアクセスを防止するためのアクセスコントロール（予防的対策）、医療情報への不適切なアクセスを発見し是正対応を行うログモニタリング（発見的対策）、そしてセキュリティインシデントが発生してしまった場合における緊急時対応（復旧的対策）という 3 つの切り口から、国内病院のセキュリティ管理実状から、解決すべき課題の分析を行う。

1．1　アクセスコントロールについて

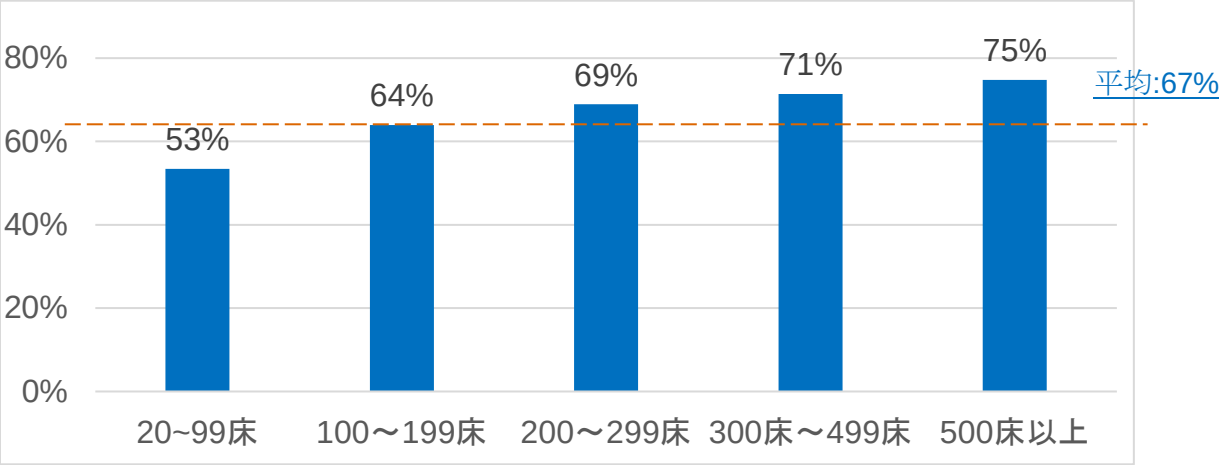
セキュリティ分析レポートからは、アクセスコントロールにおける医療現場に特徴的な傾向が見受けらる。

例えば、医療情報へのアクセスコントロールの方針（ルール）の整備状況、及び当該ルールに基づく管理状況についての調査結果からは、ルールの整備率は特に 200 床以下までの病院で相対的に低いものの**（図 1）**、実務的なアクセス制限の実施率は、病床数に関係なく 50%以上を超えている状況**（図 2）**である。

（図 1）『医療情報へのアクセス方針を定め、方針に基づき不適切なアクセスを制限しているか？』に「対応できている」と回答した病床規模別病院の割合



（図２）『医療情報システムへのアクセスは許可された利用者にのみ付与されており，未許可のアクセスを防止しているか？』に「対応できている」と回答した病床規模別病院の割合



ここからは、病院では、アクセスコントロールという管理策については、ルールの固定的な整備よりも、病院における人材の多様性・流動性の高さに即した実務的な制限が優先されていることが把握できる。

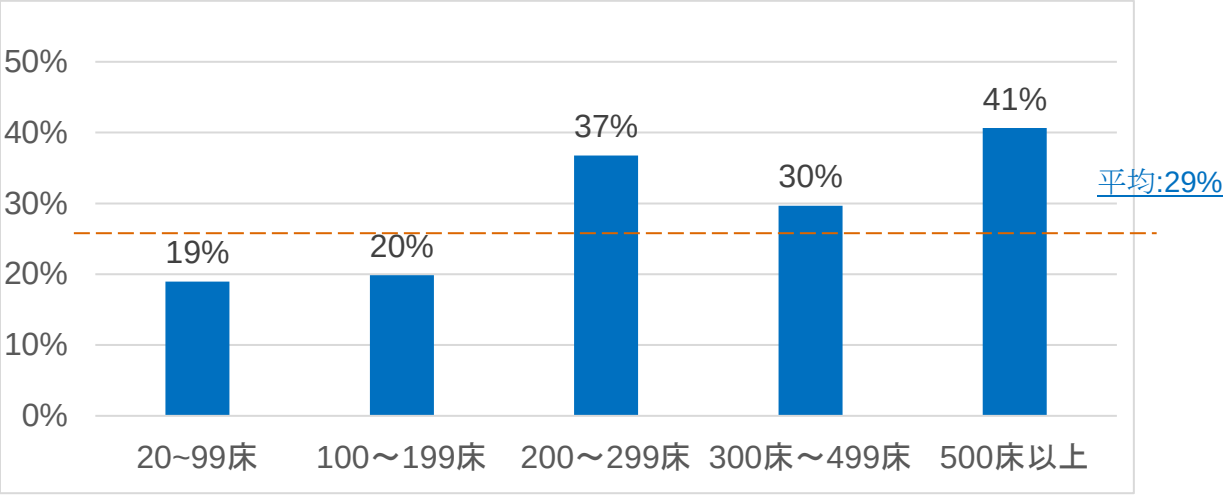
国内の病院は常勤の医療従事者のみでなく、人材不足の中で非常勤の医療従事者も多数存在しており、さらには遠隔読影や遠隔診療等、患者診療の実効性を確保すべく専門家同士のコミュニケーションが活発に行われている。これに加え、医療事務や経理・財務管理等の非医療業務の外部委託も行われる等、医療・非医療従事者も含めた、様々な労働形態を持つ多職種が医療情報にアクセスする業務特性を有している。そのため、事前に明確な職務に応じた情報へのアクセス管理方針を整備し、その方針に厳格に従い、例外を排除するアクセス管理アプローチは病院のセキュリティ管理にはそぐわない。**現場の状況・役割に応じて、情報へのアクセス権限・範囲を細やかに定義し、柔軟な見直しのもとで適用していくアプローチ**こそが病院実態に即した管理方式であると考えられる。

なお、セキュリティ分析レポートの精査のなかでは、システムの管理を行う専門部門が存在する病院であったとしても、電子カルテシステム等の院内横断的なシステムの管理を行っているものの、診療科が主管する医療情報システム（部門システム）については各診療科において独自管理されているというコメントが多数存在した。院内の医療情報システム群を統一的に管理することが困難であることは、セキュリティの統一的な水準を維持することが難しいことを示唆しているといえるだろう。

1.2　ログモニタリングについて

セキュリティ分析レポートからは、ログモニタリングについても、医療情報システムに関わる病院のセキュリティの考え方が浮かび上がる結果が出ている。アクセスログを取得し、定期的に確認を行うという対策を講じている病院は 500 床以上の病院においても 4 割程度であり、200 床以下では 2 割にも満たず、全体として実施率が低い**（図 3）**ことが示されている。

（図 3）病床規模別ログ保管・モニタリング実施率



ログモニタリングとは不適切なアクセスが発生したか否かを事後的に点検する発見的な管理策である。不適切なアクセスを未然防止する予防的な対策を優先的に行う病院の考え方に立脚した場合、ログモニタリングという発見的な管理策の優先度が相対的に低下していることがうかがえる。

この理由には、医療情報システムへのアクセスログを検証する専門的なリソースの不足という構造的な課題が大きいと思われるが、もう一つの観点として、医療情報システムへのアクセスが特定の時間帯、特定の人間のみに制限されることを前提とすることができない、病院固有の業務慣習上の理由もあると思われる。例えば、急患対応等での想定外の時間帯での医療情報へのアクセスの発生、また長期間アクセス実績のない非常勤の医師が患者対応目的で医療情報の確認の必要等、事前に想定できない医療情報へのアクセスが発生することが頻繁に発生する。ID や時間帯等、基本的な項目のみでログの絞り込みを行い、その文字情報のみを対象として検証を行おうとしても、院内のシステム担当者が不審なアクセスを検出することは難しい。そのため、**不審なアクセスの閾値を定義し、それに基づく文字情報ベースのログモニタリングを効果的に行うことが困難である**ことも理由の大きな一つと考えられる。

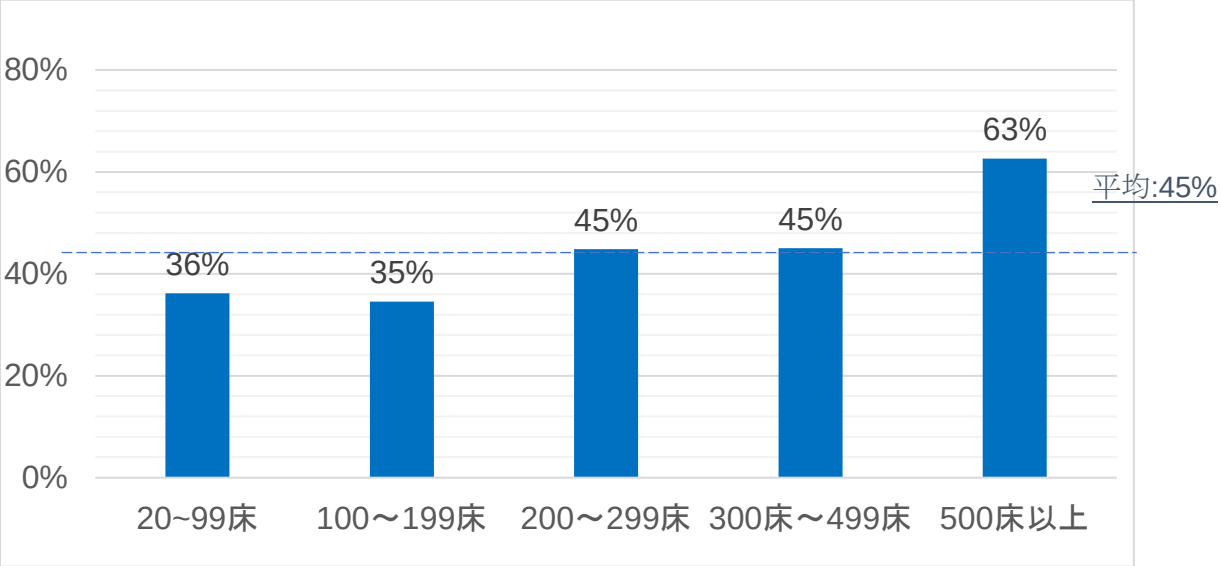
また、特に電子カルテシステム等の基幹系システムには様々な医療従事者が患者診療・治療の目的でアクセスするため、そのログの分量も非常に膨大になる。例えば、**ログの点検を行おうとした場合、その分量の多さゆえに医療情報システムのパフォーマンスへの影響が発生するような事態**も想定される。
こうした理由も含め、アクセスログの定期的なモニタリングによる不審アクセスの検知の取組が病院では困難になっていることが想定される。そのため、こうした病院の現場の課題を織り込んだ、ログモニタリングに関する情報提供が IT 事業者には求められるといえる。

1.3　非常時対応について

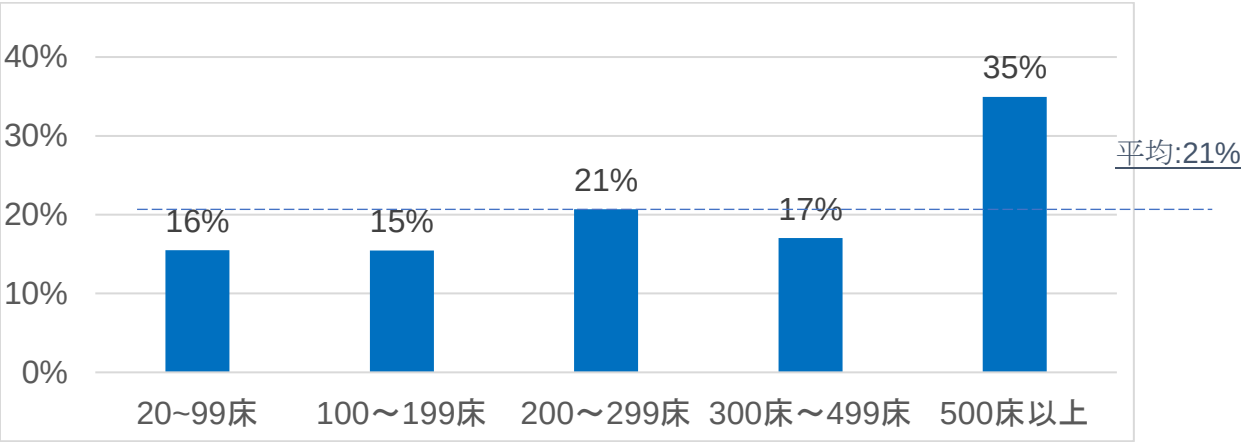
国内外の病院へのサイバー攻撃は激しさを増しており、ランサムウェアによる感染によって患者診療の継続性が損なわれる等、様々なサイバーインシデントに病院も見舞われている。

セキュリティ分析レポートでは、患者への被害発生を最小限化する観点から、インシデントの発生に対して組織として対応する取組の実施率は全体で 45%が実施している**（図４）**一方で、医療情報システムが利用不可となった場合における業務継続計画を整備し、訓練や外部施設へのバックアップ等を実施している病院は全体で 2 割程度**（図５）**とされている。

（図４）セキュリティインシデントの対応プロセスの整備率



（図５）BCP の整備率



これらの内容から把握できることは、特に激化の進むランサムウェアによるサイバー攻撃の被害を病院が受け、医療情報システムが利用不可となった場合、**患者診療の継続性を担保する態勢が多くの病院で十分に整備されていないリスクが高い**という点である。

さらに、ランサムウェア被害に備えたバックアップ取得の取組では、200 床以下の病院も含め、全体の半分程度がバックアップの取得を行っていることがセキュリティ分析レポートで判明しているが、一方で、オフライン環境へのバックアップ退避までには取り組めていない状況であった。医療情報システムが通常利用できなくなる事態に備えた態勢が十分でなく、ランサムウェア被害に備えたバックアップ管理も適切に行えていない病院が仮にその被害を受けた場合、より深刻な患者診療への影響が発生する可能性も考えなければならない。その意味では、まずは**有事に備えたバックアップの安全な保全が最も優先的に取り組むべき課題**であると言える。

2. クラウド利用による課題対応方法

常にサイバー脅威への新たな対策を継続的に講じ、様々なシステム管理機能を提供する外部のクラウドサービスを利活用することは、専門的なセキュリティ管理等を担う専門の担当者・担当部門の少ない国内の病院にとっては有益である。

国内の病院には、第 1 章で論じるように、セキュリティの推進に向けた課題がある。こうした課題も踏まえた上で、クラウドサービスを提供する IT 事業者は病院とのリスクコミュニケーションを行っていくことが必要である。つまり、クラウドサービスとして提供する機能は国内病院の課題にどのような解決・効果をもたらすものなのかという観点で情報発信を行うことこそが望ましいといえる。

ここでは、こうした情報発信の取組の拡大に寄与すべく、Microsoft が提供するクラウドサービスの製品・機能が、国内病院におけるアクセスコントロール・ログモニタリング・非常時対応上の課題の解決において、どのような具体的な役割を果たすかについて解説する。

なお、本解説は主に「「病院向けクラウドサービス対応セキュリティリファレンス (2021 年度)」[2] にて公開されている「利用可能なマイクロソフトの製品・サービスに関する情報」[3]の内容を参考にしているため、そちらの内容も参照することが望ましい。

[2] 日本マイクロソフト/ マイクロソフトクラウドの「病院向けクラウドサービス対応セキュリティリファレンス (2021 年度)」公開のお知らせ
https://cloudblogs.microsoft.com/industry-blog/ja-jp/health/2021/07/22/security-reference-of-cloud-services-for-medical-institutions-2021/

[3] 利用可能なマイクロソフトの製品・サービスに関する情報
https://aka.ms/control_mapping_results_v1

2. 1　アクセスコントロール上の課題への効果

国内の病院では常勤・非常勤の医療従事者や非医療業務を担う職員、または患者診療の目的で異なる病院に所属する医療従事者までを含め、多様な人間が様々な目的に応じて医療情報にアクセスする必要があり、アクセス権限の管理も細やかな設定が重要となる。
一方で、アクセス制御を適切に行うためには、システムやデータごとにアクセス権の設定が必要になり、異動などに伴う運用コストが膨大になる可能性がある。運用コストを削減し、アクセス権付与の抜け漏れを防ぐためには、**ID 管理基盤を一元化することが最も効果的**である。

また、ID 管理基盤には組織構造の把握やそれぞれのユーザが所有しているデバイスやファイルなどの資産管理を実施できるようにディレクトリサービスが付属しているものを利用することが望ましい。ディレクトリサービスを最大限に活用することによって、移動などに伴うアクセス権の付け替え作業をシステム単位に行うことなく、一括して実施することができる。

病院内のシステムは複数のベンダーで構築されていることもあり、それぞれの保守を各ベンダーが実施することによる管理の粒度の差が見られることがあるが、システム要件に統合 ID 基盤の利用を記載しておくことで、これらの問題を払拭することができる。

Microsoft では、ID 管理基盤として **Azure Active Directory** を提供している。この ID 管理基盤を利用することによって、**オンプレミスからクラウドまでの ID 管理を一元的に行う**ことができる。例えば、多要素認証を必要とするようなシステムにおいて、それを実装することが困難な場合であっても、ID の認証を Azure Active Directory に連携することによって、それを実現することができる。つまり、**ID 管理や認証に対する要件を全てのシステムにおいて満たせるのだ**。

Azure Active Directory には、多くの ID 管理基盤ではオプション扱いとなっているディレクトリサービスが標準で搭載されているため、**ユーザの属性に応じたアクセス制御を効率的に実施することも可能**だ。

Azure Active Directory は Microsoft のサービスだけではなく、Amazon Web Services が提供するサービスや、Google が提供するサービスの ID 管理を行うことが可能で、多くのサービスのアクセス記録（ログ）を一元的に残すことができるため、それぞれのサービス間のログを集約して比較するような手間もなく、セキュリティ運用において効率化といえる。

2. 2 ログモニタリング上の課題への効果

国内の病院ではアクセスログの定期的な点検率が低い。その大きな理由の一つとして、様々な医療・非医療従事者が不規則に医療情報へアクセスするため、**不審アクセスに係る規則的な閾値を設定することが難しい**ことが関係していると考えられる。

前述した **Azure Active Directory にはセキュリティオプションとして、世界中で発生した不正アクセスの記録から、自動的にアクセスを拒否する機能**を有している。自らが調査してアクセス制御のフィルタリングを作成しなくても、Microsoft が提供するさまざまなサービスや世界中の法執行機関と連動した不正アクセス情報により、自動的にブロックリストがユーザに提供される。

社内アクセスにおいても、普段からのアクセス状況を把握し学習していることによって、通常と異なるアクセスについて検出し、ブロックする。このような動的なアクセス制御を行うためには、ID 管理を統合し、アクセスログを一元化しておくことが重要になる。複数システムのログを個別に取得していると、それぞれに行われている不正アクセスに気がつくことが難しいが、複数のシステムへのアクセスログを統合しておけば、明らかにいつもと違う行動などを把握しやすい。

これは ID 管理だけの話ではなく、システム全体において同様である。個別システムのログだけを見ていても気がつくことができない事象が、複数のシステムを一元的に把握することによって、新たな気づきを得ることができる。

Microsoft Azure においては、**Azure Security Center** によってこのような一元管理を行うことができる。もちろん、ID 管理と同様に Amazon Web Services や Google の管理も Azure Security Center や、その関連サービスである **Azure Arc** で管理することができる。
全てのクラウドサービスの状態管理を一元化し、IT 担当者やセキュリティ担当者が同じデータをもとに判断することによって、システムやデータの状況を迅速に把握し、不適切な場合には修正することが可能になる。

Azure Security Center は、**医療情報システムの状態やアクセス履歴を文字列ベースのログでなく、グラフィカルなインタフェースによって把握し、直感的に状態を把握することが可能**となる。万が一のセキュリティ事故の調査を高度なセキュリティ技術を持って行う必要がないため、セキュリティ人材の少ない病院にとっても有用と考えられる。また、セキュリティ対応をアウトソースしている場合のコミュニケーション基盤としても役立つだろう。

Microsoft 365 においては、Windows だけではなく、MacOS、Linux、Apple iOS、Android などのさまざまな OS に対応したセキュリティ対策ソリューションとして、**Microsoft Defender for Endpoint** という機能を提供しており、ウイルスの検出や隔離、不正な URL へのアクセスブロック、そしてそれぞれの端末上で起きている不審な活動の抑制などを行うことができる。また、自組織内だけではなく、他組織で発生した事故についても、Microsoft が作成した脅威インテリジェンスを活用して自動的に防御する機能が備わっている。

これらのセキュリティソリューションは IT 製品の中に含まれて提供されているため、**OS やアプリケーションのアップデートとも親和性が高く、導入時の検証や既存システムへの影響把握などに大きな負担をかけることなく導入が可能**なことも、IT 人材が不足している病院などにとっては有用だといえる。

2. 3 非常時対応上の課題への効果

病院では、様々な医療/非医療従事者が不規則に活動し、医療情報システムの管理も一元的に行うことが困難な組織特性がある。このような状況下で、ランサムウェア等、医療情報システムを利用不可にするサイバー攻撃を想定した業務継続の態勢を確立し、関係者にしっかり教育を行っていく取組は、専門のシステム管理部門や担当者が不在の病院では困難を極めることが想定される。そのような態勢整備自体は重要であるものの、その整備が完了するまでにサイバー攻撃を受け、患者診療の継続性に影響が及ぶ事態を回避するための次善策を講じることのほうがまずは必要である。

例えば、ランサムウェア対応に有効だとされるバックアップひとつとってみても、大きな課題がある。医療情報システムのうち、例えば画像診断に用いるシステム等は非常にデータサイズが大きく、システムに備え付けられたデジタルテープ装置にバックアップしようとしても、多数の大容量のテープが必要になるケースも多い。これは院内にバックアップサーバを構築し、当該サーバへバックアップ取得を行う設計としている場合においても同様に直面する固有の課題であろう。

Microsoft 365 に含まれる **SharePoint Online** や **OneDrive for Business** では、ファイルの履歴を持っており、改ざんだけではなく、不意な改変についても元に戻すことができる機能もある。**バックアップ機能と連携することで、ランサムウェア攻撃だけではなく、業務上のミスのリカバリなどを行うことも可能**だ。

Azure 環境においても **Azure Backup** のようなサービスもあり、クラウド上で高速な回線を使ってのバックアップを実現できるため、**膨大な量のバックアップを短時間で実施**できる。

クラウド環境においては、バックアップをしやすい環境を構築するためにデータを独立して管理するなどの工夫をすることで、さらに効果的にバックアップを行うことができるといえる。

おわりに

以上の通り、セキュリティ分析レポートに基づき国内病院のセキュリティ上の課題ポイントを洗い出し、それらに対してクラウドサービスがどのような役割を果たしうるのかについて、Microsoftの具体的な製品・機能を元に、簡単にではあるが概説した。

重要な点は、**病院の組織特性を考慮した場合、既に外部のクラウドサービスは病院が直面する課題に対応しうる様々な製品・機能が用意されている**ということである。

現行の医療情報システムに個別にセキュリティ機能を追加開発するとなれば、費用面の問題もあれば、その運用の負荷も考慮しなければならず、経済的・人的なリソースが不足する国内病院にとっては、なかなか飛び越えられない壁になる。しかしながら、クラウドサービスが提供する機能のなかには、現行の医療情報システムにそれほど難しくなくアドオンできるものが多数存在する。

院内ネットワークのうち、電子カルテシステム等が設置された診療系ネットワークはインターネットとの接続を遮断した「無菌室」として管理すべきではある。しかしながら、セキュリティ分析レポートでも論じた通り、当今のサイバー攻撃は日々巧妙化・高度化を図っており、従前のセキュリティ管理策をすり抜けて、診療系ネットワークにも被害をもたらす事例も見受けられている。外部から遮断した「無菌室」であるがゆえに無条件に安全・安心であるという神話に依拠した結果、特に通常水準のセキュリティ対策すら不十分である場合、その被害の深刻さは想像に難くない。

病院としては、セキュリティ面の課題検討に際しては、インターネット経由のクラウドサービスであるがゆえに無条件に却下するのでなく、そのクラウドサービスが提供する機能が課題解決にどの程度の有効性・効率性をもっているのかをしっかり評価すべきである。

また、提供する機能を全面的に適用せずとも、部分的にでも導入することで、医療情報システムの現行機能と組み合わせて効率的な解決が図れないかといった観点も含め、幅広い検討を行うことが望ましいと考える。

そのような検討が進むためには、クラウドサービスを提供する IT 事業者によるコミュニケーション、つまり病院の目線に立ち、彼らを取り巻く環境・状況に適した機能の「翻訳」を行っていくリスクコミュニケーションこそが拡大していかなければならないといえる。

本レポートが病院の目線に立った、クラウドサービスを提供する IT 事業者によるリスクコミュニケーションが今後拡大していくことへの一石になるとともに、経済的・人的なリソース不足からセキュリティへの検討着手に悩む国内の医療機関の一助になることを強く願っている。

以上


Microsoft


Center Medical Information
Sharing and Analysis