AI・クラウドネイティブ時代に向けた医療機関の
セキュリティ対策に関する提言（第1版）

2026年7月8日

非営利法人　医療AIプラットフォーム技術研究組合

目次

はじめに

本ガイドラインの背景

高度で質の高い医療の提供や医療従事者の働き方改革をめざしさまざまな医療AIサービスが登場しています。さらに生成AIを用いた主に効率向上を目的とした様々なツールが開発され、クラウド環境の利用もすこしづつ進んでいますが、幅広い医療機関で利用されているとは言い難い状況です。経営環境に目を向けると、人件費・材料費・光熱費などの高騰により７０%以上の病院が赤字に苦しんでいます。赤字の解消には、生成AIに代表されるAIの活用及びデータ利活用による医療DX(Digital Transformation)の推進が不可欠ですが、昨今の経営状況を鑑みるとこれらを利用するための基盤整備に必須であるセキュリティへの投資優先順位があがらず、利用されているケースはまだ少ない状況です。医療AIは、医療従事者の働き方改革や医療の均てん化に重要な役割を果たしますが、病院は100床あたりに１名あるいはそれより少ない人数でシステム管理を行っている現状があります。この人数で、医療機関内のすべてのITシステムを把握し、CTやMRIなどの医療機器の保守網への接続やPACSや臨床検査システムなどの部門システムの保守網への接続、さらに患者モニタリングシステムや輸液ポンプなどネットワークに接続されたIoMT（Internet of Medical Things）など様々なネットワーク結節点を持つ装置やシステムを監視し、サイバーセキュリティ対策を施すのは極めて困難な状況です。政府から“様々なセキュリティの対策を打つべし”と言われても何から手をつけたらよいか判らず、具体的なアクションに結び付けられない厳しい現状があります。

本ガイドラインの目的及び対象読者

- 前述の背景を踏まえ、できるだけ少ないセキュリティ投資で、医療機関のセキュリティレベルを上げるための方策を提言します。

  なお、詳細資料については、研修教材としての利用を考慮した形で、別途26年夏から秋にかけて順次公開をしていきます。
- セキュリティ投資は、一時的なものではなく継続して行うことが肝要であるため、持続性のある制度的な支援策（インセンティブ）について提言します。
- 対象読者としては、医療機関・薬局・介護施設の経営者、システム管理者、実務者及び医療従事者を想定しています。

  また、制度的な支援策については、特に政府や自治体の政策立案者、民間事業者、シンクタンクも対象読者として想定しています。

補助事業名

本提言は、厚生労働省科学研究費補助金「クラウド上の医療AI利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言　（23AC1001）」にて研究を行った成果をベースとしています。但し、本研究外で実施した内容も一部含まれていることを言及しておきます。

第1章　提言の全体構成

＜現状認識＞
１）病院の7割が赤字経営かつIT・セキュリティ人財が大幅に不足している状況下で、サイバーセキュリティ対策が重要なので色々な施策を打て！！、とだけ言っていても、なかなか進まない難しい現状があります。
２）最近のサイバー攻撃は、AIを用いて行われるケースが多く、さらに使用しているAIを攻撃するケースも登場してきたため、対策の難易度が上がっています。

＜解決策＞
１）全体的にIT・セキュリティ人財が大きく不足している医療機関が多い状況下で、できるだけ投資を抑制しながら、医療機関のセキュリティレベルの底上げができないかについて提言します。
- アセスメント→対策→監査・訓練→人財育成・意識改革のサイクルの定着
- サイバー攻撃リスクを下げるために外部へのネットワーク結節点の集約
- 体制が脆弱な医療機関（点）を地域医療連携ネットワーク全体（面）で支えるためのプラットフォーム
- リスクベースアプローチによる境界防御型セキュリティからサイバーレジリエンス型セキュリティへのシフト
- 医療機関の認定制度の確立によるノウハウ（成功体験・苦労した点）の積極的な共有

２）医療機関に対するセキュリティ投資への多面的なインセンティブのあり方を提言します。
- 官からのインセンティブとして、診療報酬及び診療報酬以外のインセンティブの確立
- 民からインセンティブとして、出金を抑える方策や収入を増やすための方策の両面で検討
- 官民施策の組合せ及び認定制度の確立により、永続性のある制度支援（インセンティブモデル）の構築

医療機関のセキュリティ対策に関する提言の全体像(1)

	組織・運用面	技術面
①から④のPDCAサイクルを定期的・継続的に実行する		
①アセスメント	①-1:Webセキュリティアセスメント(1回/年) ①-2:院内ネットワーク構成類型化確認フローチャート	
②対策	②-1:アセスメント結果に沿った対策　②-2:ユースケースの共有 ②-3:外部へのネットワーク結節点の集約 ②-4:体制が脆弱な医療機関を支えるためのプラットフォーム	
③監査・訓練	③-1:システムセキュリティ監査(1回/2～3年、内部：1回/年) ③-2:IT-BCP訓練(1回/年)	
④人財育成・意識改革	④-1:定期的な研修の実施　④-2:経営層の意識改革 ④-3:組織横断的な啓発活動によるユースケースの共有	
⑤①～④の原資を生み出すインセンティブ	⑤-1:官-診療報酬＆診療報酬外の継続的なインセンティブ ⑤-2:民-出金を抑える＆収入を増やすインセンティブ	
⑥AI・クラウドネイティブ時代のひと中心の医療	⑥-1:サイバーレジリエンス型セキュリティへのシフト ⑥-2:セキュリティ・AI・DX Ready認定制度の確立 ⑥-3:ソフトウェア内製化等によるベンダーとの対等な関係構築	

医療機関のセキュリティ対策に関する提言の全体像(2)

（１）サイバーセキュリティ対策は、①アセスメント（己を知る）- ②対策（身の丈に合ったセキュリティ対策を行う）- ③監査（対策の定着を客観的にチェック）・訓練（有事の際の行動確認）- ④人財育成・意識改革のPDCAサイクルを定期的かつ継続的に廻し続けることが肝要です。
セキュリティ対策は、技術面よりもむしろ組織・運用面が重要となるケースが多く、両面の対策のバランスが重要となります。

（２）上記①から④のサイクルを定期的かつ継続的に廻し続けるためには、その原資が必要となります。
原資を確保するための策を⑤に示しています。

（３）AI・クラウドネイティブ時代のひと中心医療（市民・患者・医療従事者が中心の医療）の実現をめざして、⑥では、ZEROリスクを前提とした境界防御型セキュリティやゼロトラスト型セキュリティを進化させて、WITHリスクを前提としたサイバーレジリエンス型セキュリティの実現を提案します。また、医療機関の認定制度の提案を記載しています。認定制度の目的は２つあり、ひとつは、皆の規範となる医療機関を明示的に示すことにより、具体例の共有が進むことを期待しています。もう一つは、認定制度により、⑤に示す制度的なインセンティブが付きやすくすることを目的としています。
最後に、生成AIの活用が医療機関の進化のスピードとQoLの向上に大きく影響する時代を見据えて、また、ソフトウエア開発経験者ではなくてもプログラミングが容易な時代において、医療の本質を一番理解している医療従事者が組織としてソフトウエア内製化を行うことにより、ベンダーと医療機関の不平等性や非対称性の是正を進め、ひと中心の医療の実現やデータ利活用を進めていくための施策を提案します。

第2章．サイバーセキュリティのPDCAサイクル

サイバーセキュリティは、アセスメント（己を知る）- 対策（身の丈に合ったセキュリティ対策を行う）- 監査（対策が定着しているかを客観的にチェック）- 訓練（有事の際に実際に行動できるか？）をPDCAサイクルで廻し続けることが肝要です。
監査についても、まずは、ルールベースのシステムセキュリティ監査が必要です、
しかしながら、セキュリティ対策が境界防御型から境界防御型 x ゼロトラスト型へ強化される方向ではあるものの、医療機関においてはゼロトラスト型セキュリティの導入は、まだ少ない上に、両方のセキュリティ対策も基本的な考え方は、完全防御をめざす考え方であり、ZEROリスクををめざしています。しかしながら、昨今は、AIがサイバーアタックを行う時代であり、RaaS（Ransomware as a Service）というビジネスモデルも出現し、最新のテクノロジーを駆使しているため、ZEROリスクの実現は極めて困難となっています。従って、万一サイバー攻撃を受けても、いかに被害を最小化し、医療の提供を継続できるかを第一に考えることが最善となっています。従って、日頃より、実際のIT-BCP訓練を定期的に実施することが重要です。セキュリティ対策の最終ゴールは、サイバーレジリエンス型セキュリティの実現であり、サイバー攻撃が常態化し、完全防御は不可能であるとの前提に立って、万一に備えることです。つまり、リスクベースのセキュリティ対策とリスクベースのシステムセキュリティ監査が今後必要になってきます。また、セキュリティ対策の実行は、IT部門だけが行うのではなく、医療機関全体がトップダウンで推進する必要があります。特に組織・運用面の対策はトップダウンアプローチが必須です。技術面の対策においても投資判断が必要であり、経営層の理解と参画が不可欠です。万一、自医療機関がサイバー攻撃にさらされた場合の社外への説明責任は、IT部門ではなく、経営者の責任です。経営者は、その時になって慌てない様に、日頃からセキュリティ対策を一人称で考えておくことが重要です。

①アセスメント

①-1：Webセキュリティアセスメント

医療機関のセキュリティアセスメントの方法は、従来はコンサルテーションサービスによる実施が主であり、手厚い代わりに費用が高額でした。また、チェックリストによるアセスメント方法も存在しますが、自力で結果の分析や対策の優先順位付けが困難なケースが多くありました。これらの課題を解決するためにWebを用いて、セキュリティ対策の現状や意識を確認するアセスメントサービスを開発しました。

本サービスは、Webベースのサービスで、以下の3種類からなります。

1)病院の医療情報システム向け　：　病院の医療情報システムがガイドラインやチェックリストに準拠しているかを確認します

対象:病院のITシステム運用管理を行っている方　　質問:21分野80問

2)病院の経営層向け　：　病院の経営層がどれだけセキュリティの重要性を理解しているかを確認します　＊1

対象: 病院の理事長、院長、事務長　　質問: 9分野15問

＊1　15病院のシステムセキュリティ監査結果をみると、経営層のセキュリティに対する 理解度や認知度が高いほど監査の結果が良く、低いほど監査の結果が悪く、強い相関が見られました。

3)診療所の医療情報システム向け　：　診療所、介護施設、薬局などの小規模医療情報システムのセキュリティ対策が十分 かを確認します。　対象:診療所の院長または委託先のベンダー、介護施設、薬局など　　質問:11分野13問

https://secsrv.haip-cip.org/top

医療システムの安全管理に関するガイドライン(6．0 版)やR7年度版医療機関におけるサイバーセキュリティ対策チェックリストに準拠しています　＊2。ひとの定期健康診断と同様に、毎年Webセキュリティアセスメントを実施することを推奨します。

＊2　医療システムの安全管理に関するガイドライン(7．0 版)やR8年度版医療機関におけるサイバーセキュリティ対策チェックリストの反映は、年内を予定しています。

①-2：院内ネットワーク構成類型化確認フローチャート

ネットワーク構成の類型化の視点で、自組織のセキュリティレベルを簡易に判定できます。ネットワーク構成の類型化を行う上で、セキュリティ統制の観点からデータ通信（流通）経路という切り口で統制レベルを分類した結果、下記に示す4レベルに集約されました。2024年時点の調査では、レベル0、レベル1の医療機関が半数を超えていました。レベル２をめざすことを推奨しています。

レベル	統制の主な内容	外部NW接続統制	記憶媒体利用統制	院内NW統制
0	● システムのID/パスワードの管理レベルが不十分である ● USBメモリ利用に関するルールがあるが、運用が徹底されていない ● 外部(別の組織やサービス）接続されるネットワークの管理レベルが不十分である	×	△	×
1	● 医療情報系ネットワークと、外部(別の組織やサービス）や院内の別ネットワークとの通信制御がある程度実施されているが、管理レベルが不十分である	△	△	×
2	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている	○	○	×
3	● 医療情報系ネットワークと外部(別の組織やサービス）や院内の別ネットワークとの通信制御が実現され、構成やアクセス記録が維持管理されている ● マルウェア侵入や情報漏洩を防ぐため、USBメモリ等外部記憶媒体の利用制御・管理が行われている ● 医療情報系ネットワーク内部において、部門システム間の通信制御が実現され、維持管理されている	○	○	○

②対策

②-1:アセスメント結果に沿った対策

Webアセスメントの結果、点数が低い分野の対策案を提示します。具体的には、3点満点で1.5点以下の項目について表示します。
分野は、以下の21分野です。

・体制　・教育　・資産管理　・導入　・運用　・アクセス制御　・ネットワーク　・メディア　・モバイル
・ウイルス対策　・暗号化　・認証　・変更　・手順　・バックアップ　・保守　・廃棄　・監視　・ログ
・障害対応　・BCP

https://secsrv.haip-cip.org/top

②-2、④-1、④-3:ユースケースの共有、研修

医療機関に役立ちそうなユースケースを収集して、積極的に公開していくことが重要と考えています。
ユースケースだけではなく、アセスメント、対策、監査、訓練などを医療機関内の研修に役立つコンテンツとして、共有していきます。
安全・安心にクラウド上のAIサービスを利用する方法、自宅などのリモートから院内システムへのアクセスを行う方法、データを共有するのではなく映像データを共有する方法などがあります。
医療機関が具体的なアクションを起こしやすい様にヘルスISAC、医療トレーサビリティ推進協議会、ソフトウエアISAC、IPA AISIなど医療・ヘルスケア分野におけるセキュリティに関して知見を保有している組織との連携を強化して、ユースケースの共有を加速します。
また、厚労省の医療機関向けセキュリティ教育支援ポータルサイトに良質なコンテンツが公開されていますんどえ活用をお勧めします。

https://mist.mhlw.go.jp/

③-1:システムセキュリティ監査

システムセキュリティ監査は、徳洲会グループで実際に行っている監査ををもとに、徳洲会以外の複数病院で システムセキュリティ監査を行い、ブラッシュアップと標準化を進めた。

・現場のリアルな実態としては、病院幹部や現場の医療スタッフにはセキュリティは難しい。病院のシステム管理者も電子カルテには通じているがセキュリティについて十分な知識と経験を持つ者は多くない。
・医療現場で日常的にセキュリティを意識した運用が行われていると言えず、セキュリティ監査の準備も手探りになる。
・監査をして問題点を洗い出し解決策を提示しても、それを病院が理解しなければ改善はできない。しかしセキュリティのエキスパートによる監査や対策は多くの病院にとってハードルが高い。
・セキュリティ対策には少なくないコストが発生し、現場の職員の負担となる事項もある。
・病院幹部が監査結果を理解して費用を捻出し、システム担当者に、現場に強いメッセージを出す必要がある。
・病院幹部をはじめ中間管理職、現場の医療スタッフまでが理解できるシステムセキュリティ監査が求められている。

この様な状況から、年1回の内部監査（チェックシートとマニュアルを用いた内部監査）の実施及び２～３年に１回程度の外部監査で専門的視点からの助言や支援を行い、病院幹部とも面談し理解を得ることが重要だと考えています。
システムセキュリティに関する高い意識の醸成は、一朝一夕で出来上がるものではないが、医療機関の経営層がまず、率先してシステムセキュリティの意識を高めていくことが、重要である。
・セキュリティ対策が医療現場の日常になることをめざし、医療スタッフの意識に、医療現場の運用に根付いていく。幹部とシステム管理者、現場の医療スタッフの共通理解と協力のもと、病院のセキュリティレベルが向上していくと考えます。

③-2:IT-BCP

全ての医療機関が、独力でIT-BCPドキュメントの策定は困難であり、現在、厚労省で公開しているIT-BCPのリファレンス

ドキュメントでも策定はが困難だと思われる。

そのため、実際の医療機関で策定・運用されているIT-BCPドキュメントを公開して、これをリファレンスとしつつ、医療機関の規模、

体制など身の丈にあった第一歩を踏み出すことが重要だと考えいます。

研修と合わせて医療機関全体のレベルを継続的に上げていくことが重要だと考えます。

IT-BCPは、マニュアルという捉え方に留まらず、実践対策ガイドと考えてください。実際のIT-BCP訓練を通じて、ブラッシュアップを

継続することが重要です。

医療機関の本分は、万一サイバー攻撃を受けても、被害を最小限に抑えこんで、医療の提供を止めないで継続することです。

1回/年のIT-BCP訓練の実施及びIT-BCPドキュメントの見直しをお勧めします。

https://www.hosp.tohoku.ac.jp/wp-content/uploads/2020/08/it-bcp1.pdf

③-2:IT-BCP訓練

・東北大学病院で実際に実施したIT-BCP訓練の内容を下記に示します。

本訓練は、技術的な復旧手順の確認にとどまらず、「IT が止まった状態で病院は何を続け、何を止めるのか」を災害対策本部と現場が共通認識として持てるかを重視する。1 時間という限られた時間の中で、初動対応、ベンダー連携、患者即時対応、長期紙運用という複数の論点を俯瞰し、IT-BCP の実効性と今後の改善点を明確化することを最終目的とする。

2. IT-BCP 訓練 進行表（詳細版・所要時間：約 60 分）

訓練前提

想定事象：

- ランサムウェア感染
- 電子カルテ・検査・医事会計等が停止
- 復旧目安：1 か月
- IT-BCP に基づき災害対策本部を立ち上げ
- 訓練形式：机上訓練（役割別討議）

（ア）0〜5 分｜事象発生認知・初動判断（IT-BCP 発動判断）

① 状況付与（ファシリテータ）

- 「複数の診療端末にランサムノートが表示」
- 「情報部門が不正通信を検知」
- 「被害拡大防止のためネットワーク遮断を実施」

② 役割別行動

- 情報部門責任者
  （ア）ランサムウェア感染の可能性が高いことを報告
  （イ）影響が疑われる主なシステム（電子カルテ、部門システム等）を列挙
  （ウ）被害拡大防止のためのネットワーク遮断判断を説明
  （エ）主要システムベンダー（電子カルテ、検査、医事、NW 等）への一次連絡を開始した旨を共有
- サーバ対応エンジニア
  （ア）暗号化の兆候、ログ上の異常を簡潔に説明
  （イ）サーバ停止・ネットワーク遮断が診療に与える即時影響を補足
- 病院長
  （ア）IT-BCP に定められた発動基準を確認
  （イ）IT-BCP に基づき災害対策本部を立ち上げるか判断

IT-BCP 訓練 チェックシート（役割別）

1. 病院長（災害対策本部長）

初動・判断（0〜15 分）

- □IT インシデントを **IT-BCP に基づく危機事象**として認識できた
- □IT-BCP の発動基準を根拠に、災害対策本部立ち上げを判断できた
- □「短期障害」ではなく「長期停止（1 か月）」前提で状況を整理できた

意思決定・統括

- □患者安全を最優先とする基本方針を明確に示せた
- □継続する診療／停止・制限する診療の判断ができた
- □技術的制約を踏まえた現実的な判断ができた

情報共有・対外対応

- □本部の判断を各部門に伝える前提を確認できた
- □対外説明（患者・関係機関）の基本方針を整理できた

2. 情報部門責任者（IT 統括）

初動対応（0〜5 分）

- □ランサムウェア感染の可能性を明確に説明できた
- □ネットワーク遮断の判断理由を説明できた
- □各主要システムベンダー（電子カルテ、検査、医事等）への連絡を開始できた

本部対応（5〜15 分）

- □被害範囲・不確実点を整理して本部に共有できた
- □ベンダー・保守業者・セキュリティ事業者との役割分担を説明できた
- □技術情報を経営判断に必要な形に翻訳できた

技術対応（15〜30 分）

- □サーバ停止の判断根拠を説明できた
- □ネットワーク遮断範囲（院内／外部）を整理できた
- □バックアップの有無・世代・安全性確認状況を把握していた
- □想定される復旧方法（復元／再構築）を説明できた

3. サーバ対応エンジニア（技術担当）

技術状況把握

- □暗号化の兆候・影響範囲を説明できた
- □バックアップが被害を受けていないか確認できた
- □復旧に必要な作業・期間を現実的に提示できた

本部連携

IT-BCP 訓練 評価シート（総合）

評価方法

- 各項目を **5 段階評価**で記入
  - 5：非常に良好（実運用でも十分機能する）
  - 4：概ね良好（一部改善で実運用可能）
  - 3：可（訓練としては成立、実運用には課題）
  - 2：不十分（改善が必要）
  - 1：不適切（機能していない）
- 評価後、**コメント欄に具体的な理由・気づきを記載**

1. 初動判断・IT-BCP 発動の評価（0〜5 分）

評価項目	評点（1–5）	コメント
IT インシデントを IT-BCP 対象として認識できたか		
IT-BCP に定められた基準を根拠に判断できたか		
個人判断ではなく組織判断として処理できたか		
ベンダー連絡を初動対応に組み込めたか		

総合所見（初動）

- 良かった点：
- 課題点：

2. 災害対策本部の立ち上げ・運営評価（5〜15 分）

評価項目	評点	コメント
災害対策本部の立ち上げが迅速だったか		
本部の役割・意思決定範囲が明確だったか		
情報が整理されて共有されたか		
各部門に伝達・周知する前提が整っていたか		

総合所見（本部運営）

- 良かった点：
- 課題点：

3. システム部門対応の評価（技術・説明力）

評価項目	評点	コメント
サーバ停止・ネットワーク遮断判断は妥当だったか		
バックアップ状況を把握・説明できたか		

④-1、④-2、④-3:人材育成、意識改革

④-1、④-3:人材育成

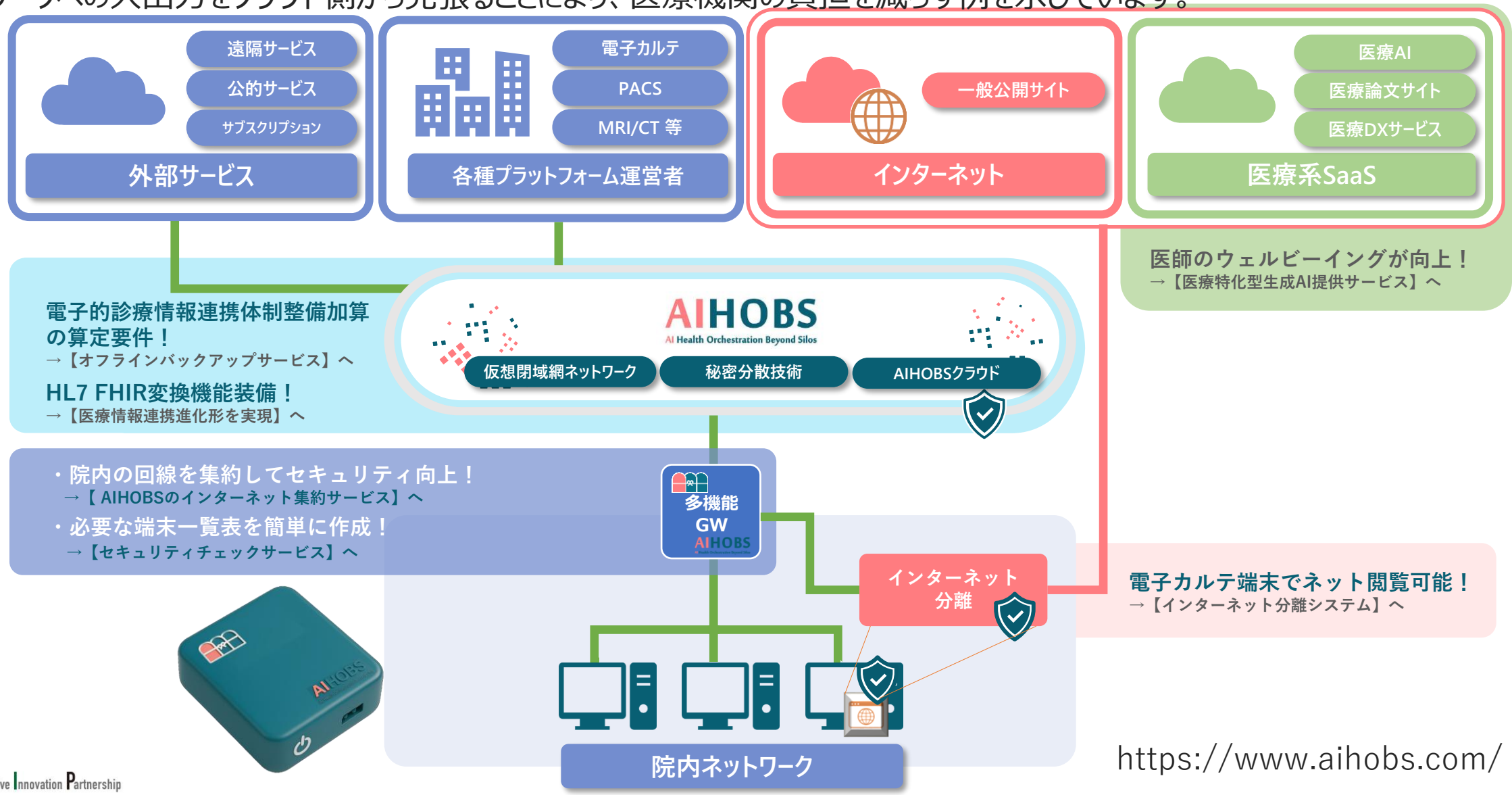
P.10にて言及のとおり。

④-2：意識改革

P.8、P.13にて言及のとおり。

3章. 医療機関に向けたユースケース　②-3:外部へのネットワーク結節点の集約

運用管理が不十分な外部ネットワーク結節点（モダリティ、サブシステム、電子カルテ等の保守回線や給食システムなどの外部サービス）を集約し、リスクを減らす方法の一例を示します。この例では、多機能GWにネットワーク結節点を集約することにより、ネットワークへの入出力をクラウド側から見張ることにより、医療機関の負担を減らす例を示しています。



https://www.aihobs.com/

3章. 医療機関に向けたユースケース　②-4:体制が脆弱な医療機関を支えるためのプラットフォーム

スキルの高い医療機関がセキュリティ弱者を守るプラットフォームの概念を検討しました。

全国の地域医療情報連携ネットワークは、３１１カ所（２０２５年１月現在）存在していますが、各々の地域で自助努力で運営を行っているところが多く、経営面のみならず、人材不足によるセキュリティ上の課題を多く抱えています。

本ユースケースは、力のある医療機関がセキュリティ弱者をできるだけ少ないコストで持続的に支えられるかを東北大学が中心となってMMWINと連携して実証を行いました。

decoyという罠掛けシステムを用いることにより、地域医療情報連携ネットワークに接続されている病院、診療所、薬局などが個々に行うべきセキュリティ対策を最小限にとどめ、本ネットワーク全体にサイバーアタックの予兆を監視する仕掛けを導入することにより、出来るだけ費用を抑えてセキュリティを担保する方法です。サイバー攻撃をかけられていることをいち早く察知し、対策を取る、あるいは、攻撃しても無駄と思わせることにより、予防的な対応を行うことが可能です。

スキルの高い医療機関を担う主体は、地域医療情報連携ネットワークの構成メンバーや運用主体のセキュリティに関する技術面や運用面のレベルによって、いくつかのパターンが考えられれます。いずれにしろ、更なる実証実験が必要であり、政府の積極的な予算措置が期待されます。

＜主体となり得る組織（例）＞

- 地連のメンバーである大学病院
- 地連のメンバーである地域中核病院
- 地域医療情報連携ネットワークの運用主体
- セキュリティ運用のアウトソーシング先ベンダー
- 安全・安心なネットワーク環境を提供サービスのオプションメニューとして提供（リモートから防御する）

4章. 医療機関への制度的な支援策

医療機関の経営は、依然として厳しい状況が続いているが、だからと言って、セキュリティ対策への投資を後回しにすることは、医療機関自身の存亡にかかわる。**医療機関の本分は、どんなことがあっても継続的に医療を提供すること**であり、サイバー攻撃により、医療が継続できなくことは、この本分を実行していないことになる。

適切なサイバーセキュリティ対策への投資インセンティブの機会を作ることにより、2030年医療機関の電子カルテ普及率100%の目標達成に合わせて、医療機関のサイバーセキュリティ対策が加速させるためにも継続的なインセンティブ設計が重要であると考えます。

考え方としては、官民でインセンティブを分担する事により、セキュリティを医療DXやデータ連携・利活用を加速するためのインフラと位置付け、持続的なインセンティブモデルを構築すること狙いとします。

（物流の発展には、高速道路の整備が不可欠だったのと同じで、セキュリティを医療発展のためのインフラと捉え、官民で投資をしていく姿勢が求められる）

⑤-1：官-診療報酬＆診療報酬外の継続的なインセンティブ

（１）一過性の支援（導入補助金）だけではなく、継続的な支援（セキュリティは継続的な対応が不可欠で機器導入とは大きく異なるため）そのための方法が必要と考えます。

・R8年度診療報酬改定の中で、セキュリティに関連が強いのは、電子的診療情報連携体制整備加算です。
しかしながら、本加算だけでは、セキュリティに関する投資額をカバーするには至りません。新たな診療報酬あるいは、診療報酬以外の継続的な支援策が必要と考えます。
・内閣府医療等情報の利活用の推進における検討会（中間まとめ）が発行され、2026年夏ごろに最終提言が発行される予定であり、これに沿ったセキュリティ対策を定義し、そこに診療報酬をつけることを検討していく必要があると考えます。
データ利活用が活性化する重要な方向性であり、引き続き注目していく。
・安全・安心なAIの利活用と合わせて、診療報酬における施設基準の設定をめざしたいです。2026年診療報酬改定では、医療事務作業補助体制加算が制定され、大きな前進であるが、カバー範囲の拡大やセキュリティ要件の厳格化による診療報酬の分類が理に適うのではないでしょうか。
・AIを安全・安心に利活用するためには、セキュリティ対策が必須であり、Security Ready病院の認定制度へつなげられないか。例えば、クラウドシフトを率先して行っている医療機関やガバメントクラウドと同等のセキュリティ的な備えをしている医療機関を認定するなどグローバル標準に照らして、セキュリティレベルの類型化を行い、それに沿ってインセンティブをつける。日本医療機能評価機構やIPAとの連携を検討する必要性も検討する。

⑤-2:民-出金を抑える＆収入を増やすインセンティブ

コストを抑える・収入を増やすための両面のインセンティブを検討する必要があります

①コストを抑えるためのインセンティブ：アセスメント、対策・訓練実施などの医療機関

（例）・損保会社がサイバー保険などのディスカウントや提供ソリューションのディスカウント、金融機関・WAMが金利を引き下げなど

・HIJ（ヘルスISAC　JAPAN）や医卜協等との連携により、セキュリティアセスメント結果と紐づいた複数の対策案を提供する（セキュリティ対策の紹介やディスカウントの検討）

②収入を増やすためのインセンティブ

（例）・医療データの提供、セキュリティやAI利用のユースケースを開示することに対して適正な対価を得るスキームを作る

・安全・安心なネットワーク環境やデータマネージメントにより、治験への参画を増やし、対価を得る(グローバル治験への参画を増やす)

AIやクラウドネイティブ時代に求められるサイバーレジリエンス型セキュリティは、図に示すサイクルを継続的に実行する事です

境界防御型セキュリティ

医療機関の内外の境界を守る

お城の城壁の考え方と近く

脅威は外部から来るが大前提

一度侵入されると脆い

✖

リモートアクセスやクラウド型サービスの利用が増加

ゼロトラスト型セキュリティ

ネットワーク内外を問わず常に信頼を維持する

Windowsやアプリケーションを常に最新に保つ

✖

内外を問わず、アクセスごとに認証を行う

医療DXの進展によりサイバー攻撃が激化

サイバーレジリエンス*)

計画
システム健全性
リスク評価・特定
セキュリティ設計

特定
ダメージ局所化
検知と防御
権限の最小化

組織改善
教育
訓練

復旧・対応

*)悪条件、攻撃、または侵害を予測し、耐え、回復し、適応する能力のこと

完全防御　～Zero リスク～

被害が日常化　～With リスク～

⑥-2:セキュリティ・AI・DX Ready認定制度の確立

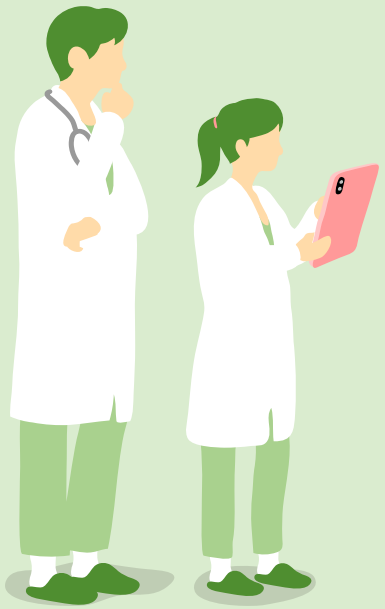
・AIを安全・安心に利活用するためには、セキュリティ対策が必須であり、Security Ready病院の認定制度へつなげられないかと考えています。例えば、クラウドシフトを率先して行っている医療機関やガバメントクラウドと同等のセキュリティ的な備えをしている医療機関を認定するなどグローバル標準に照らして、セキュリティレベルの類型化を行い、それに沿ってインセンティブをつけることが考えられる。また、AIがセキュリティを攻撃する時代において、AIとセキュリティは別々に考えられない時代に突入しているため、AI自身のガバナンスやセキュリティのガバナンスに関する備えを客観的に評価する方向を検討します。
・認定制度の目的は２つあり、ひとつは、皆の規範となる医療機関を明示的に示すことにより、具体例の共有が進むことを期待しています。もう一つは、認定制度により、⑤に示す制度的なインセンティブが付きやすくすることを目的としています。

⑥-3:ソフトウェア内製化等によるベンダーとの対等な関係構築

生成AIやAIエージェントの登場により、AIでAIを開発できる時代となりました。セキュリティ対策においても、必ずしも専門家を必要とせず、従来以上の適切な対応を取ることが可能な状況になりつつあります。これまでのランサムウェア被害の多くは、パスワード設定の不備など基本的な問題が引き金となっており、AIエージェントの積極的な活用によりこうした低レベルな脆弱性は大幅に改善される可能性があります。また、未経験者がAIエージェントを活用して物体検出AIモデルやウェブアプリケーションを開発できた事例が示すように、経験者や有識者に依存した従来の人材戦略からの脱却が可能な状況になりました。AIエージェントは人材育成のツールとしても有効であり、生成AIを活用した世代間の知識伝達の方法も大きく変わって行くものと思われます。今後の若者たちが独自に課題を解決していく可能性を踏まえた、新たな開発および運用体制の構築が必要です。
さらに、業務アプリケーションについても、医療従事者が開発できる時代が到来しています。
内製化の研修や伴走支援の整備などを進めることにより、今までのベンダーへの依存体制、ベンダーとの不平等な関係を改善することにより、コストの削減や開発速度の向上が期待されます。

謝辞

２０２３年度から厚生労働省科学研究費補助金「クラウド上の医療AI利用促進のためのネットワークセキュリティ構成類型化と実証及び施策の提言　（23AC1001）」に採択され、国立成育医療研究センター岡村浩司氏を研究代表者として、東北大学藤井進氏、東北大学病院中村直毅氏、徳洲会インフォメーションシステム株式会社尾崎勝彦氏、福田秀樹氏、国立成育医療研究センター松井俊大氏、医療AIプラットフォーム技術研究組合金子誠暁氏、宇賀神敦氏らで研究を進めてきました。



HAIP