別紙 3

厚生労働科学研究費補助金
政策科学総合研究事業（臨床研究等 ICT 基盤構築・人工知能実装研究事業）

分担研究報告書
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

研究分担者　金子 誠暁　BIPROGY 株式会社 第四室長

研究要旨

医療従事者と医療 AI との協調は、医療従事者の働き方改革の実現や医療の均てん化には重要である。質の高い医療データに基づいて開発された医療 AI サービスが次々に生まれ、幅広い医療機関で利用されるためには、利用しやすい価格とクラウドの利用が不可欠である。本研究では、医療機関の設立母体、病床数、地域などの特性を踏まえて 26 医療機関（24 病院、2 クリニック）に対して実態調査を行った。対面のヒアリング実施前に、事前アンケート調査票を送付し、その回答を入手した後に、25 医療機関については対面のヒアリング（1 医療機関はアンケート調査項目の回答）を実施することにより、効率向上とヒアリングで確認すべき内容を明確にすることができた。本ヒアリングを通して、医療機関の IT 導入状況、ネットワーク構成、人員体制、リスクアセスメント実施状況、システムセキュリティ監査状況、保健所によるセキュリティ立ち入り検査対応状況などの実態を把握及び医療現場が抱える課題を把握することができた。また、本ヒアリングから、医療機関のシステム構成を技術面から 3 種類に類型化することができた。類型化については JASO TP-15002 を活用し、脅威・リスクを整理した。脅威・リスクをもとに、最新クラウドセキュリティに関する整理を行い、現状の医療機関のセキュリティをもとにクラウド利用に発展した際の対策を机上で整理した。医療機関は、平均して 100 床あたり 1 名のシステム要員で院内システムのトラブル対応やセキュリティ対策を実施しており、リソース不足や知識不足、またベンダ依存体制が浮き彫りになった。技術面では、医療機関とクラウドシステムを安全・安心に接続するための必要とされる 4 種類のセキュリティ領域について、技術調査と整理を行った。今年度の成果を基に、医療機関がリーズナブルなコストで導入しやすい技術の実証を複数箇所で実施し、それに基づいたネットワークセキュリティ構成の提言を実施する予定である。

A. 研究目的

医療従事者と医療 AI との協調は、医療従事者の働き方改革の実現や医療の均てん化には重要である。質の高い医療データに基づいて開発された医療 AI サービスが次々に生まれ、幅広い医療機関で利用されるためには、利用しやすい価格とクラウドの利用が不可欠である。本研究では、医療機関の特性によって、費用対効果も意識した具体的なネットワーク構成やセキュリティ監査の方法を示すことにより、医療機関が安全・安心にクラウド環境上の医療 AI サービスを利用できるためのルール策定を目的としている。
2023 年度は、国内医療機関へのヒアリングを実行し、医療機関が外部ネットワークに出る際の類型化案を策定する。類型化に基づいて、医療機関が外部ネットワークに出る際の、国内外の最先端セキュリティ技術を探索し、機能評価を行う。

B. 研究方法

国内医療機関へ対面でネットワーク環境の実態調査のためのヒアリングにあたり事前アンケート調査票を提示し、医療機関にて記入後ヒアリングを実施した。
アンケート調査票とヒアリング内容をもとに、統計化および類型化を実施した。その際に JASO TP15002 を活用し、脅威・リスクを抽出した。
脅威・リスク及び現状のセキュリティ状況を理解した上で、最新クラウドセキュリティに関する整理を机上にて実施した。
（倫理面への配慮）
本研究においては特段なし。

C. 研究結果

26 医療機関にヒアリングを実施した。対面は 25 医療機関、1 医療機関はアンケート調査項目の回答のみであった。
ヒアリング前に以下の項目のアンケート調査項目を取得した。
調査項目は、病床数・平均外来来院数・機関組織・開設主体・病院機能・診療科区分・システム導入状況・サイバーセキュリティ対策チェックリストに記入状況・システム担当者の有無・セキュリティ人材の有無・院内でのセキュリティ監査の実施の有無・院内のリスクアセスメント実施状況の有無・BCP 対策の状況・ハイブリッドクラウドの採用の有無・診療系ネットワークにおける外部通信の有無・医療 AI サービスの利用状況・BYOD の利用状況・今後クラウドシフトへの想いなど、24 項目である。
添付（A1.　医療機関へのネットワークセキュリティ事前アンケート内容）
24 項目の回答状況をもとに、平均 1.5 時間程度医療機関へのヒアリングを実施し、図 1 のイメージでヒアリング結果をまとめた。
ヒアリングの中でアンケート調査項目のみでは回答しきれない現状の外部通信に関する医療機関内のネットワークに関する内容も確認し、ネットワークパターンを 3 つに類型化した。それが図 2～4 である。

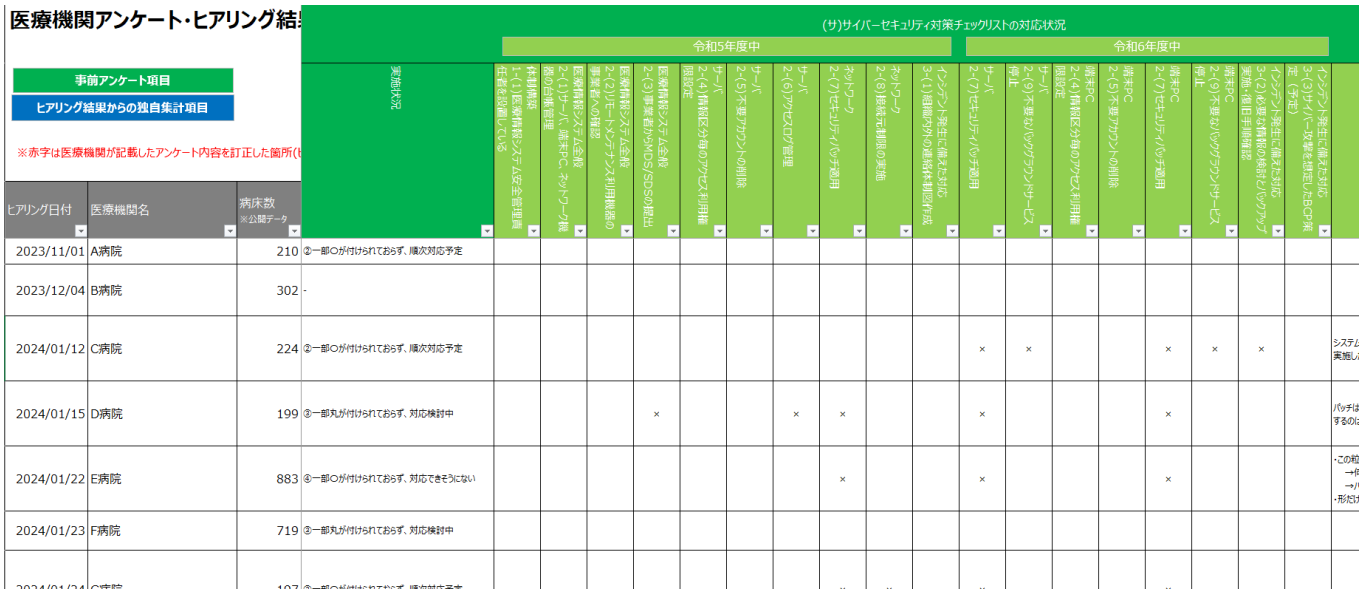

図１　ヒアリング結果イメージ

医療機関ネットワークモデル（レベル1）

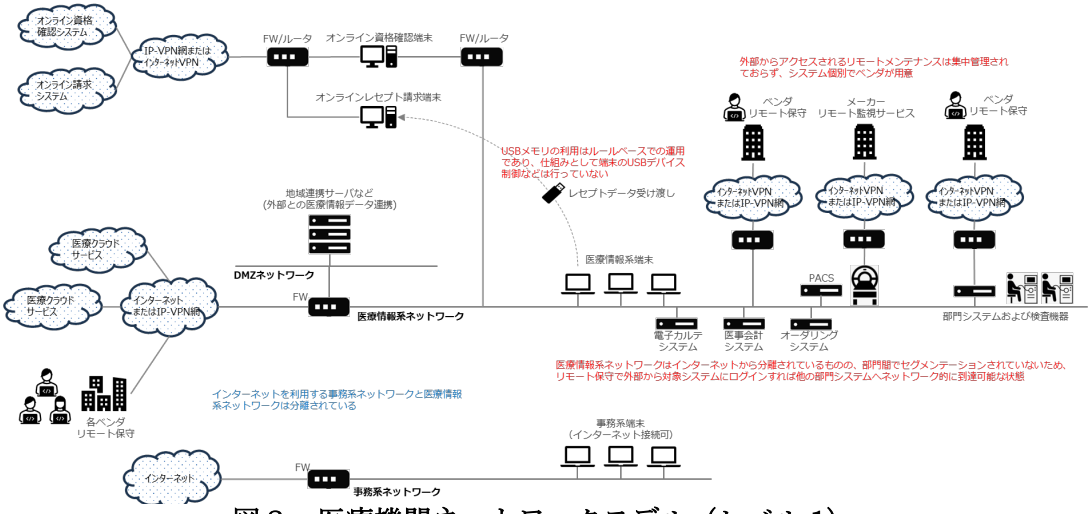

図２　医療機関ネットワークモデル（レベル 1）

医療機関ネットワークモデル（レベル2）

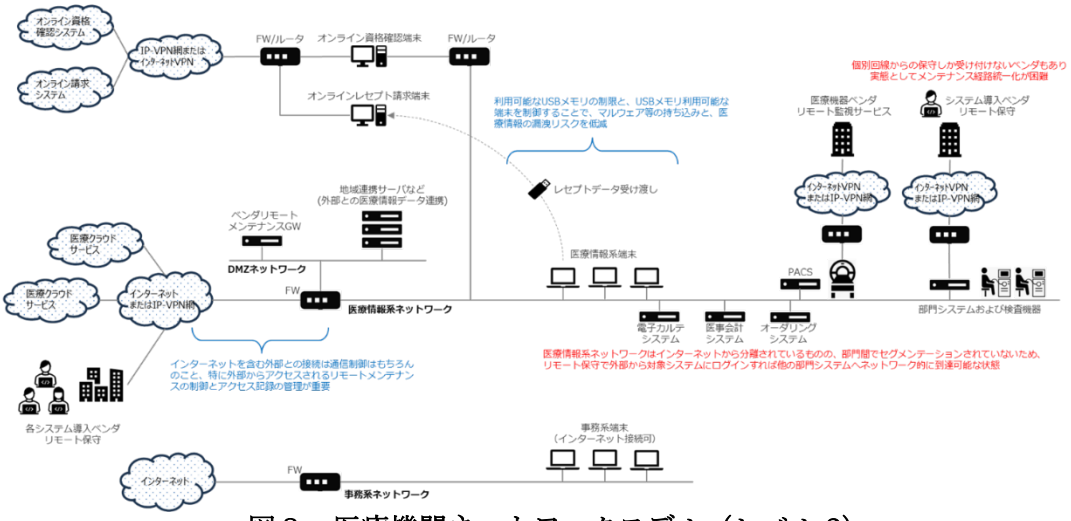

図３　医療機関ネットワークモデル（レベル 2）

医療機関ネットワークモデル（レベル3）

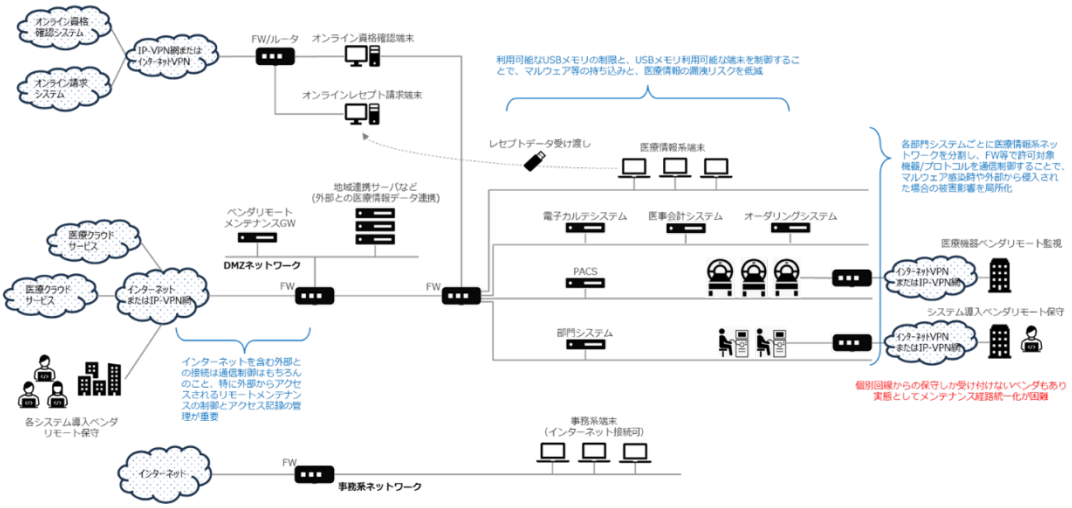

図４　医療機関ネットワークモデル（レベル 3）

今回の調査における医療機関ネットワークモデルの分類の状況としては、3 つのレベルに類型化した。
レベル 1 は、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。レベル 2 は、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。また、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。
レベル 3 は、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。また、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。さらに、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。
それらを図 5 の形で整理した。

医療機関のネットワークセキュリティを考察する上で、個別構成の議論にならないよう以下の観点で凡化モデルを作成した。汎化モデルを作成するうえで、以下を定義した。

- 電子カルテ、PACS などシステム個々ではなく、保護すべき医療情報として一つの塊とみなす（昨今の医療情報システムは、各システムが TCP/IP ネットワークを通じでつながっている）
- 医療情報（システム）へアクセスする主体を特定する
  - 院内の職員、院外からのリモートアクセス、外部連携システムなど
- ネットワークセキュリティ対策を施す領域を分類し凡化モデルにマッピングする（本書では以下の 4 つに分類した）
  - アカウント層：ID・認証情報の管理や権限管理を行う領域
  - エンドポイント層：医療情報システムへアクセスする端末
  - ネットワーク層：外部との接続を中心にセキュアなネットワーク接続を実現する領域
  - 監視・検知層：ネットワークや端末、サーバなどシステム全体にわたってセキュリティの監視や検知を実現する領域

上記を前提に、図 6 に汎化モデル図を作成した。

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	内部NW統制	分布割合	コメント
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	△	△	×	45% (10)	いずれの医療機関でも、医療情報とインターネットとの分離は実現済み。
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	○	○	×	45% (10)	USBメモリなど外部媒体の利用制限を、ルールと仕組みの両面で実現している医療機関は比較的多かった。 また、ベンダリモート保守のアクセス方法を院内統一化をめざし、ベンダ個別にID・パスワード発行のうえ、アクセス先システムを制御している機関も一定数あり。ただし、その接続方式を受け入れないベンダもあり、アクセス方式の完全統一は慣習上困難であるのが実情。 尚、各部門システムのネットワーク（VLAN）を分けている機関はいくつかあったが、通信制御までは実現できていないため、レベル2でもセキュリティリスクは存在。 • ランサムウェアに感染した場合に医療情報系ネットワークで被害が拡散 • ベンダリモートアクセスにおいて、対象システムにログイン後に、別の部門システムへ容易にネットワーク侵入が可能
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	○	○	○	9% (2)	部門システムごとにネットワークをセグメンテーションし、必要な通信のみ許可するよう制御している医療機関は2件のみだった（NWセキュリティに精通した人材が医療機関全体を把握し、各医療機器ベンダと会話しながら通信フローを把握する必要あり）

図 5　医療機関ネットワークモデル分類状況

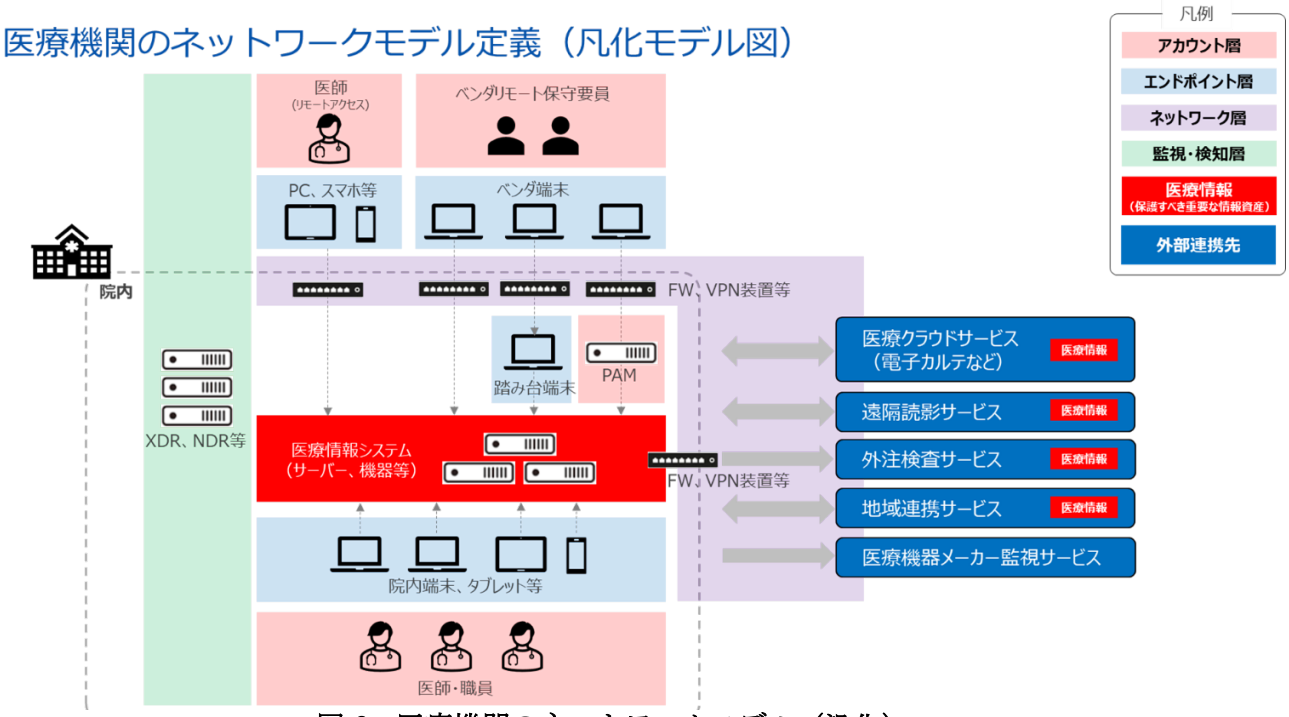

図 6　医療機関のネットワークモデル（汎化）

汎化したモデル図に対して脅威事象を抽出するにあたり、以下の基本的なセキュリティ対策は実施済と仮定した。

- 医療情報システム（サーバ、及び関連 NW 機器）はマシンルームや施錠されたラック等、物理的に関係者以外がアクセスできない場所に設置されているものとする
- 医療情報システム（サーバ、及び関連 NW 機器）が第三者（患者など）に物理アクセス可能な場所に設置されている場合は、不正操作の対策がされているものとする
  - 対策例 1:システムが設置されている部屋に入室する場合は職員が立ち会い、勝手に第三者に操作されない運用を行う
  - 対策例 2:ネットワークスイッチの未使用ポートはシャットダウンしておき、機器を接続してもネットワークにアクセスできない状態とする
  - 対策例 3：離席時はタイマー等で PC のスクリーンロックが自動的にかかる設定とし、第三者が不正に PC を操作しない対策を行う
- 医療情報システム（サーバ、及び関連 NW 機器）の、OS やアプリケーションは利用者ごとに ID が払い出され、パスワードが適切に管理されているものとする
  - NG 例 1：ユーザーに必要のない権限（特に管理者権限など）を付与している
  - NG 例 2：複数の利用者で ID を共用している
  - NG 例 3：複数のシステムや機器で共通の ID/パスワードを設定している
  - NG 例 4：初期設定のパスワードや機器のデフォルトパスワードを使い続けている
- 医療情報システムを設置設定およびメンテナンスするベンダ作業者の身元確認、作業内容確認を、医療機関職員が確認している
- 医療情報システムを設置設定およびメンテナンス（リモート含む）を行うベンダの作業用 PC は、アンチウィルスソフト導入などセキュリティ対策がされ、マルウェアに感染していないものとする
- 医療情報システム、及びそのシステムにアクセスするネットワークや端末は、直接的にインターネットに接続されていないものとする
- 特にインターネットに暴露されている NW 機器は、設定不備による意図しない外部からのアクセスはないものとする

本仮定を前提したアクセスパスごとに具体的な脅威を図 7 に洗い出した。

アクセスパス	具体的な脅威事象	備考
院内ネットワーク	悪意のある第三者が不正に院内ネットワーク（LAN）に対して接続し、医療情報の閲覧・搾取が行われる	特にWi-Fiは電波が届く範囲は盗聴可能となるため、適切な認証方式と暗号化強度で利用することが必須。
	悪意のある第三者が不正に院内ネットワーク（LAN）に対して接続し、マルウェア感染や医療情報システムが破壊される	特にWi-Fiは電波が届く範囲は盗聴可能となるため、適切な認証方式と暗号化強度で利用することが必須。
院内医療情報端末（タブレット等含む）	マルウェアが仕組まれたUSBデバイスを院内端末で利用することでウィルスに感染して、医療情報の搾取や、医療情報システムが破壊される	
	USBメモリなど外部記憶媒体を利用し、医療情報が外部に漏洩する（故意による持出し、不注意によるUSBメモリ紛失など）	
	他の医師や職員のIDを利用して、なりすましで医療情報システムを操作する	特にパスワードを変えずに運用し続けたり、退職済み職員や、一時作業用IDが放置されるとリスクが高くなる。
院外からの医療情報システムアクセス	職員がリモートでアクセスし、故意に医療情報の持ち出しを行う	
	職員がマルウェア等に感染した端末等で医療情報システムにアクセスし、ウィルスが院内に感染、医療情報システムが破壊されたり、医療情報が搾取される	端末が直接ネットワークでつながる形態だと感染被害が広がりやすいが、限定的なアプリケーションでのアクセスや、画面転送方式であれば、被害が局所化できると想定される。
	職員用のリモートアクセスルートから第三者が不正にアクセスし、医療情報の不正閲覧や医療情報搾取が行われる	特にインターネット経由で職員が医療情報システムに接続されるネットワーク形態の場合、不特定多数からアタックを受けやすい。 また、多要素認証の未活用、単純なパスワード設定、パスワード情報漏洩によりリスクが高くなる。
院外からの医療情報システムアクセス	職員用のリモートアクセスルートから第三者が不正にアクセスし、ウィルス感染を含む医療情報システムの破壊や、医療情報搾取が行われる	特にインターネット経由で職員が医療情報システムに接続されるネットワーク形態の場合、不特定多数からアタックを受けやすい。 また、単純なパスワード設定、パスワード情報漏洩、多要素認証の未活用などによりそのリスクは高くなる。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	医療情報システムが、間接的にでも物理的にインターネットに接続される場合は、インターネット境界のセキュリティ維持は非常に重要。
ベンダリモートメンテナンス	ベンダリモートアクセスのルートにて第三者が不正にアクセスし、ウィルス感染を含む医療情報システムの破壊や、医療情報搾取が行われる（単純なパスワード設定、パスワード情報漏洩、多要素認証の未活用などを原因として）	認証情報（パスワードや多要素認証の情報）がベンダで適切に管理されていない場合、リスクが高くなる。 また、インターネット経由でリモートメンテナンスされるネットワーク形態の場合、インターネット境界のセキュリティ維持は非常に重要。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	インターネット境界のセキュリティ維持は非常に重要。
	ベンダが医療情報システム（サーバやNW機器）にアクセスしたうえで、悪意をもって保守範囲外の別システムにアクセスし、医療情報を不正に閲覧したり情報搾取を行う	部門システム間で自由なNWの疎通ができる状態だと、サーバにログインさえ出来れば、他のサーバへラテラルムーブメントが可能。管理レベルの低い部門システム保守ベンダにより、院内システム全体がリスクにさらされる。
	ベンダが医療情報システム（サーバやNW機器）にアクセスしたうえで、悪意をもって保守範囲外の別システムにアクセスし、ウィルス感染を含む破壊活動を行う	部門システム間で自由なNWの疎通ができる状態だと、サーバにログインさえ出来れば、他のサーバへラテラルムーブメントが可能。管理レベルの低い部門システム保守ベンダにより、院内システム全体がリスクにさらされる。
外部サービス連携	医療情報システムと接続している外部のシステムや組織経由で、第三者が不正にリモートでアクセスし、医療情報の不正閲覧や医療情報搾取が行われる	閉域網で接続されていても発生する。セキュリティ強度の低い組織と接続することで自院のリスクも高まる。
	医療情報システムと接続している外部のシステムや組織がウィルスに感染したり、外部システム経由の不正アクセスで院内にウィルス感染が波及、医療情報システムの破壊や、医療情報搾取が行われる	閉域網で接続されていても発生、セキュリティ強度の低い組織と接続することで自院のリスクも高まる。 大阪急性期・総合医療センターのランサムウェア被害も、外部接続したシステムからの侵入が原因の一つであった。
	インターネットに露出されているNW機器の脆弱性を突かれて、インターネット経由で第三者が侵入、ウィルス感染を含む破壊活動や医療情報搾取が行われる	インターネット境界のセキュリティ維持は非常に重要。

図 7　脅威の事象

各脅威に対する対策有効性を評価するにあたり、汎化モデルで定義した各領域のネットワークセキュリティ対策の代表的なソリューションとして以下をピックアップした。

- アカウント層：ソリューション
  - IAM（権限のきめ細かな設定や、パスワードポリシー強制など含む認証基盤）
  - PAM（特権管理）
  - IGA（ID ライフサイクル管理）
- エンドポイント層：
  - EDR（PC やサーバにおけるウィルス等の不審な挙動を検知・対応）
  - UEM（デバイス設定、アプリケーション管理、セキュリティポリシー適用）
- ネットワーク層：
  - SASE（SSE、SD-WAN 含むネットワーク＆セキュリティ統合サービス）
- 監視・検知層：
  - EDR（PC やサーバにおけるウィルス等の不審な挙動を検知・対応）
  - XDR（エンドポイント、ネットワークなど広範囲に渡りウィルス等の不審な挙動を検

知・対応）
  - SIEM（ネットワーク機器や各種ソフトウェアが生成するイベント情報の統合管理）、NDR（ネットワークトラフィックを分析し攻撃や不正の兆候を可視化・検知）

以上を選定し、クラウドセキュリティ技術の机上調査を行った。
実態調査に関する考察としては、医療情報システムに求められるネットワークセキュリティを実現するためには、医療機関個々の取組みだけでなく、行政や地域連携、関係団体など多面的な支援が必要と考えられる。
ヒアリング通じて、具体的に以下の 4 点が感じられた。

- セキュリティ要件に対応するための具体的なノウハウ不足：具体的な対応手順や対策例、また対応すべき優先順位など、現場ですぐに活用可能なノウハウを行政や関連団体から積極的に展開し、現場担当者のスキルを補う対応は急務であると考えられる。例えば本調査と並行で実施されているシステム監査グループの成果物は、現場が必要としている具体的な監査ノウハウとして有効である考えられる。
- セキュリティ要件に対応する工数捻出：情報担当者が展開されたノウハウを活用し対応の見通し（期間・工数含む）を立てることと併せて、行政からも医療機関の経営者・管理者にセキュリティ対応の重要性と人員・コストの必要性を啓蒙することも重要である。
- セキュリティ対策コスト捻出：セキュリティレベルの底上げは医療業界全体の課題であるからには、各医療機関がセキュリティ対策に対してインセンティブが働くよう、行政が主導しアメ（補助金など）とムチ（診療報酬の減額や罰則など）を活用するマクロ的な取り組みは有効であると考えられる。
- 医療情報担当者の人員不足：多くの医療機関では医療情報担当者の待遇面は事務職扱いであるためエンジニアが集まりづらい。待遇改善による採用改善を試みることも必要だが、例えばネットワーク機器の継続的なパッチ適用は専門ベンダに外注することや、クラウドの活用など、人口減少時代に外部リソースの活用は避けて通れない打ち手となる。

また、電子カルテ及び周辺システム（オーダリング・医事会計）は比較的管理されているが、部門システム（例えば PACS、検査システム等）は部門担当者任せであるケースが多いため、院内ネットワーク全体の外部接続を把握している職員がかなり少ない状況であることがわかった。このような体制ではそれぞれの医療機関がセキュリティリスクに対応するのは困難であり、医療情報を扱う端末やシステムからセキュアに外部の医療クラウドサービスへ接続する仕組みを、今後新たに示す必要があると考えられる。
次年度には PoC の検証する候補として、今回調査にて各接続形態を医療機関と、クラウドサービス事業者の両者の視点から比較検討を行った。
図 8 は比較検討結果であるが、以下の 2 つの接続形態は今後の PoC 評価対象として有力な候補として SASE/SSE 及びセキュアブラウザとし、次年度 PoC 評価を行う予定である。

D. 考察

実態調査に関する考察としては、医療情報システムに求められるネットワークセキュリティを実現するや医療機関でのクラウド促進ためには、医療機関個々の取組みだけでなく、行政や地域連携、関係団体など多面的な支援が必要と考えられる。

E. 結論

医療機関の体制ではそれぞれの医療機関でセキュリティリスクに対応するのは困難であり、医療情報を扱う端末やシステムからセキュアに外部の医療クラウドサービスへ接続する仕組みを、今後新たに示す必要があると考えられると感じた。
次年度は医療機関から外部にでるユースケースを検討し、PoC を行う予定である。
PoC 評価対象として有力な候補として SASE/SSE 及びセキュアブラウザとし、次年度 PoC 評価を行う予定である。

接続形態	医療機関にとって様々な医療クラウドサービスを利用しやすい接続形態であるか	医療機関のセキュリティ確保がしやすい構成であるか	クラウド事業者が準備しやすい接続形態であるか	クラウド事業者側のセキュリティ確保がしやすい構成であるか	評価コメント
①専用線	サービスごとに回線を敷設するのはコスト的に困難であり、IPアドレス体系の重複は導入上の制約・課題となることが想定される。	外部と閉域網で接続されるため、セキュリティ確保が容易。	利用する医療機関ごとに回線を敷設する必要があり、またIPアドレス体系の重複は導入上の制約・課題となることが想定される。	外部と閉域網で接続されるため、セキュリティ確保が容易。	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
②IP-VPN	（同上）	（同上）	（同上）	（同上）	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
③拠点間VPN	（同上）	VPN機器がインターネットに晒されるが、論理的には閉域網で構成されるため、セキュリティ確保が比較的容易。	多くの医療機関とのVPN接続を収容できるNW機器が必要。またIPアドレス体系の重複は導入上の制約・課題となることが想定される。利用機関の増減に合わせてVPN接続のメンテナンス運用が必要。	VPN機器がインターネットに晒されるが、論理的には閉域網で構成されるため、セキュリティ確保が比較的容易。	クラウド事業者の接続形態として一般的ではないため、PoC対象から除外。
④リモートアクセスVPN	端末に専用ソフトウェア導入が必要。仕組み上、接続時は院内LANへのアクセスが制限されることが想定される。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。	専用のリモートアクセスVPN装置が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	インターネットの不特定多数にアクセスされる状態となるため、アクセス装置は特にタイムリーなパッチ適用などセキュリティ維持は必須。	④・⑤は技術的な差異はあるが、類似した接続形態となる。いずれも比較的枯れた技術であり候補となり得るが、敢えて検証を行う必要性は低いと考える。
⑤SSL-VPN	（同上）	（同上）	専用のSSL-VPN装置が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	（同上）	（同上）
⑥SASE/SSE	（同上）	アクセス先をSASEサービスに絞ることで、セキュリティの確保が比較的容易。	SASEの導入が必要。利用機関の増減に合わせてIDの発行・失効メンテナンス運用が必要。	常時SASEサービスへ接続され、各医療機関とも論理的な閉域網を構成するため、セキュリティ的に保護された状態となる。	単なる経路の暗号化だけでなく、様々なセキュリティ機能を有している。今後の評価対象の一つとして有力な候補であると考える。
⑦端末のブラウザを直接利用	利用しやすい。ただし、セキュリティ確保のためProxyサーバ等でのアクセス先制限は必須。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。	一般的なインターネットへのWeb公開と同等。	インターネットに直接公開するWebシステムとなるため、多層防御（FW、IPS、WAF、DDoS対策など）が必要	単に端末からインターネットへアクセスする構成となるため、敢えて検証を行う必要は無いと考える。
⑧セキュアブラウザ	利用しやすい。ただし、セキュアブラウザのシステム導入が必要。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。万が一不正なコードやファイルをダウンロードした場合でも、隔離された領域でブラウザが稼働するため端末の安全性が確保される。	（同上）	（同上）	今回のヒアリングにおいて、電カル端末からインターネット参照を実現するために採用している医療機関が一定数存在した。また、今後セキュアに電カル端末からインターネット上の医療クラウドサービスへのアクセス需要が増えると考えられる。 そのため、安全なファイル授受の機能も利用可能なセキュアブラウザは、今後の評価対象の一つとして有力な候補であると考える。
⑨仮想デスクトップアクセス（クラウド事業者側で用意）	比較的利用しやすい。 ただしVDIの種類によっては、端末に専用ソフトウェア導入が必要。	アクセス先をクラウドサービスに絞ることで、セキュリティの確保が比較的容易。 またVDIでの作業となるため、端末側の安全性が確保される。	VDIシステムを準備する必要があるため、この接続形態を採用するクラウド事業者は多くないことが想定される。	VDIシステムのパッチ適用などセキュリティ維持は必須。	広く展開するクラウドサービスとして、実際の採用は稀であることが想定されるため、PoC対象から除外。

図 8 次年度評価対象一覧（接続形態）

F. 健康危険情報

包括研究報告書に記載

G. 研究発表

なし

H. 知的財産権の出願

なし

資料　医療機関へのネットワークセキュリティ事前アンケート内容

回答者の情報	本アンケートの回答を頂く病院名と部署名を記入してください。	（記入欄）
	本アンケートの回答者の職種を教えてください。①②の場合は○、③の場合は記入お願いします。	①医師 ②情報システムの担当者 ③それ以外の場合は自由記載してください （③の記入欄）
病院基本情報	（ア）該当する病床数を○につけてください。 ①50床未満　②　50～100床未満　③100～200床未満　④200～400床未満　⑤400～600床未満　⑥600～800床未満　⑦800床以上	
	（イ）1日の平均外来来院数に○をつけてください。 ①50人未満　②　50～100人未満　③100～200人未満　④200～400人未満　⑤400～600人未満　⑥600～800人未満　⑦800人以上	
	（ウ）機関・組織に○をつけてください。 ①病院　②有床診療所　③無床診療所　④健診施設	
	（エ）開設主体に○をつけてください。 ①厚生労働省　②独立行政法人国立病院機構　③国立大学法人　④独立行政法人労働者健康安全機構　⑤国立高度専門医療研究センター ⑥独立行政法人地域医療機能推進機構　⑦都道府県、市町村、地方公共団体の組合　⑧国民健康保険団体連合会及び国民健康保険組合 ⑨日本赤十字社　⑩社会福祉法人恩賜財団済生会　⑪厚生農業協同組合連合会　⑫社会福祉法人北海道社会事業協会 ⑬全国社会保険協会連合会　⑭厚生年金事業振興団　⑮船員保険会　⑯健康保険組合及びその連合会 ⑰共済組合及びその連合会　⑱国民健康保険組合　⑲私立学校法人　⑳公益社団法人　㉑公益財団法人　㉒社会医療法人 ㉓社会福祉法人　㉔医療法人　㉕医療生協　㉖会社　㉗個人　㉘その他の法人	
	（オ）病院機能に○をつけてください。 ①特定機能病院　②地域医療支援病院　③臨床研究中核病院　④国立高度専門医療研究センター（National center） ⑤がん診療連携拠点病院　⑥救急医療　⑦へき地医療拠点病院　⑧災害拠点病院　⑨エイズ診療拠点病院　⑩総合周産期母子医療センター	
	（カ）該当する診療科区分に複数○をつけてください。 ①内科　②心療内科　③精神科　④神経科　⑤呼吸器科　⑥消化器科　⑦循環器科　⑧アレルギー科　⑨リウマチ科　⑩小児科 ⑪外科　⑫整形外科　⑬形成外科　⑭美容外科　⑮脳神経外科　⑯呼吸器外科　⑰心臓血管外科　⑱小児外科　⑲皮膚泌尿器科 ⑳性病科　㉑肛門科　㉒産婦人科　㉓眼科　㉔耳鼻咽喉科　㉕気管食道科　㉖リハビリテーション科　㉗放射線科　㉘神経内科 ㉙胃腸科　㉚皮膚科　㉛泌尿器科　㉜産科　㉝婦人科　㉞呼吸器内科　㉟循環器内科　㊱歯科　㊲歯科矯正科　㊳小児歯科 ㊴糖尿病科　㊵腎臓内科　㊶腎移植科　㊷血液透析科　㊸代謝内科　㊹内分泌内科　㊺救急医学科　㊻血液科　㊼血液内科 ㊽麻酔科　㊾消化器内科　51消化器外科　52肝胆膵外科　53糖尿内科　54大腸肛門科　55眼形成眼窩外科　56不妊内分泌科 57膠原病リウマチ内科　58脳卒中科　59腫瘍治療科　60総合診療科　61乳腺甲状腺外科　62新生児科　63小児循環器科	
	（キ）システム導入状況に○をつけてください。 ①医事会計システムを導入 ②オーダリングシステムを導入 ③電子カルテシステムを導入 ④電子レセプトオンライン請求を導入 ⑤マイナンバーカードの健康保険証利用のためマイナ受付の導入 ⑥電子処方箋の導入 ⑦外注検査依頼と結果のオンラインサービス ⑧遠隔読影のオンラインサービス ⑨その他院内のシステムと外部接続しているサービスがあれば自由記載	①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 ①導入済　②検討中　③未導入 （記入欄）
	（ク）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を知っていますか。（https://www.hospital.or.jp/site/news/file/1686540766.pdf） 該当箇所に○をつけてください。	①知っている　②知らない
	（ケ）サイバーセキュリティ対策チェックリストの記入しましたか。該当箇所に○をつけてください。	①記入した　②記入中　③記入していない
	（コ）サイバーセキュリティ対策チェックリストの対応状況はいかがですか。該当箇所に○をつけてください。	①全て○がつけられた ②一部○がつけられておらず、順次対応予定 ③一部○がつけられておらず、対応検討中 ④一部○がつけられておらず、対応できそうにない
	（シ）サイバーセキュリティ対策チェックリストを記載している医療機関において、チェックリストを本プロジェクトに公開していただくことは可能ですか。該当箇所に○をつけてください。	①可能 ②WEB会議で投影のみで説明だけであれば可能 ③不可能
	（ス）医療機関の中に、電子カルテシステム等の院内担当者はいますか。該当箇所に○をつけてください。	①医療情報部/情報システム課のような形で専属の部や室がある ある場合は、在籍人数を教えてください。（　　名） ②総務部や経理部といった部のメンバーが担当している システムを担当されている方は何名ですか。（　　名） ③院長が責任している ④その他（　　） ⑤全くいない。
	（セ）上記（ス）でカウントされた方の中に、セキュリティに詳しい人材はいますか。該当箇所に○をつけてください。	①自らセキュリティ対策を自発的に考え、委託しているシステムベンダーと会話することができる。 ②資格は有していないが、委託をしているシステムベンダーが言ったことを理解できる、 または学会等に参加する中で情報を得ている人数 ③委託しているシステムベンダーの言っていることをそのまま信用して対策を講ずるしか手段がない。 ④その他（　　）
	（ソ）セキュリティの外部資格を有している人材がいましたら何人いますか。該当箇所に○をつけてください。 セキュリティの外部資格候補例は以下です。 ・情報処理安全確保支援士試験 ・情報セキュリティマネジメント試験 ・SPREAD情報セキュリティサポーター能力検定 ・SPREAD情報セキュリティマイスター ・情報セキュリティ管理士認定試験 ・金融情報セキュリティマネージャー	①1名 ②1名程度 ③1名以上（この場合は＿＿名在籍） ④0名
	（タ）医療機関内で、セキュリティ監査を行っていますか。該当箇所に○をつけてください。 セキュリティ監査とは、病院が保有する情報資産を守るために正しく対策がとられているかを、第三者的な目線でチェックすることです セキュリティルール、組織のガイドラインを用意し、 セキュリティ対策を正しく実施し機能しているかを定期に検証や評価を行うことをいいます。	①はい、行っている ②いいえ、行っていない ①と回答した場合は、どのような形で監査しているか簡単でよいので記載してください （記入欄）
	（チ）医療機関内で、リスクアセスメントを行っているますか。該当箇所に○をつけてください。 リスクアセスメントとは、病院が抱える情報資産に対するリスクの洗い出しや分析、評価を行い、許容できるかどうかを決めるプロセスのことを表します。	①はい、行っている ②いいえ、行っていない ①と回答した場合はどのような形でリスクアセスメントしているか簡単でよいので記載してください （記入欄）
	（ツ）医療機関内で、BCPの対策は上っていますか。該当箇所に○をつけてください。 BCPとは、医療施設の災害対応のための事業継続計画を指します。	①はい、厚生労働省の医療施設の災害対応のための事業継続計画に基づいて、 または自院内の個別ルールに基づいてBCP対策を行っている、もしくは計画中である。 ※①は、院内に災害対策委員会等の常設、災害対策本部の立ち上げルール、 災害対策マニュアルの整備といったシステム外の対策がメインとなる質問です。 ②はい、①まではできていないが、システムバックアップ等の保管場所の工夫や、クラウドを利用した参照用のシステムを構築しており、システム面では診療を続けられる対策がとれている。 ③いいえ、①・②ともに行っていない ①②と回答した場合は、どのような形でBCP対策を行っているのか簡単に記載してください （記入欄）
	（テ）医療機関内で、ハイブリッドクラウドを採用していますか。該当箇所に○をつけてください。 ハイブリッドクラウドとは、パブリッククラウド、プライベートクラウド、院内の物理サーバを組合せて使うクラウドのことです。	①はい、採用している ②検討したが、採用はしていない（検討したものを簡単でよいので記載してください） ③聞いたことがあるが、具体的に検討をしたことがない ④初めて聞いた言葉である ①②と回答した場合は、どのようなソリューションを検討されたのか簡単に記載してください （記入欄）
	（ト）医療機関内で電子カルテの診療系ネットワークにおいて外部との通信している個所はどのようものがありますか。該当箇所に○をつけてください。 電子カルテが使えるネットワークを診療系ネットワークと表現しています。	①昼夜メンテナンス時に委託会社がアクセスするため接続方法について （接続方法はご存じの場合、閉域網、HW-VPN、SW-VPN、LTE、モバイル、その他） ①で答えた場合は、どのシステムが回線で接続されているのか記載してください。 （記入欄）サンプル　電子カルテシステムは閉域網、PACSはHW-VPN、リハビリシステムはSW-VPN ②マイナンバーカードによるオンライン資格確認のため ③レセプトオンライン提出のため ④クラウドサービス利用のため ①と回答した場合は、どのような外部クラウドサービスを使われているのか記載してください。 （記入欄） ⑤地域連携用に外部とのアクセスがある ⑥電子カルテの診療系ネットワークにて、他に外部との通信を行っているものがある ①と回答した場合は、どのような用途で使われているのか記載してください。 （記入欄）
	（ナ）医療機関内で、医療AIサービス利用状況を教えてください。該当箇所に○をつけてください。	①利用している（利用している場合は、商品名を記載してください。） ①-1　オンプレで利用しているか　商品名（　　） ①-2　クラウドで利用しているか　商品名（　　） ①-2-1　クラウド利用に踏み切った際に、注意した事項はなにかありますか。 （記入欄） ①-2-2　クラウド利用を行うにあたり、医療機関内で反対の声はありましたか。 （記入欄） ②検討中である ②と回答した場合は、どのような外部クラウドサービスを検討されているのか記載してください。 （記入欄） ③興味があるが、利用まで至っていない ④聞いたことがない
	（ニ）医療機関内で、職員や患者のスマートフォン等BYODを利用されているケースはありますか。該当箇所に○をつけてください。 BYODとは、業務に個人のスマートフォンやパソコンを持ち込んで利用する捉えてください。	①利用している ①で利用している場合は、サービス名もしくは用途を教えてください。（　　） ②検討中である ②で検討中場合は、サービス名もしくは用途を教えてください。（　　） ③利用していない
	（ヌ）医療機関内から外部に出ている点を中心にヒアリング時にネットワーク構成を教えて頂けますか。該当箇所に○をつけてください。	①ヒアリング時に説明してもよい ②ネットワーク構成のお話しはできない。 ②の場合は、なぜできないか可能な範囲で教えてください。 （記入欄）
	（ネ）電子カルテを含めた医療情報システムのクラウドシフトや今後の方針について、思われることを簡単でよいので記載してください。	（記入欄）