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）
分担研究年度終了報告書

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 藤井 進, 中村 直毅

研究要旨

本研究は医療機関の類型化に基づいた最適なネットワークセキュリティ構成やシステム監査のルールを示す事により、全国の医療機関が安全・安心かつリーズナブルな費用で医療 AI サービスが利用できることを目的とする。医療 AI は、深層学習による画像認識や生成系 AI の飛躍的な精度向上により医療への有用性が示されるが、個人情報保護への配慮やランサムウェアなどのサイバー攻撃の対応も喫緊の課題となっている。本分担班は東北大学が主導的に運用する地域医療ネットワークシステム MMWIN：Miyagi Medical and Welfare Information Netowork を通して、これら相反する課題を同時解決できないか検討した。

ガイドラインや医療機関へのヒアリングを参考に、ネットワークセキュリティに関するアンケート調査を超急性期病院(東北大学病院)の立場や地域医療ネットワーク(MMWIN)の立場で実施した。また AI 利用とセキュリティ対応が同時に成立するシステム構成の設計を、AWS を想定したクラウド基盤の前提で設計した。

ランサムウェア被害は近年高度化し、境界型防御を前提にしたセキュリティ対応が難しい現状が確認できた。またゼロトラスト型セキュリティ対応をガイドラインに合わせて導入したくとも、人材不足や資金の面で課題があることがわかった。これらセキュリティ対応において、地域医療連携システムを介して実現するならば有益であるとの見解もアンケート調査から確認ができた。また AWS 上に配置した特定のサーバと、医療施設内に設置したサーバがクラウド接続を通して、バックアップファイルの転送やリモート保守用途の接続、AI 利用に向けた API 連携ができることを確認した。

地域医療連携システムを活用することで、人材不足や投資抑制を補いながら、網羅的に多くの医療施設を課題解決できることが示唆された。来年度はこれらを具体的に検証し、実運用上の課題などを明らかにしながら、詳細なネットワークアーキテクチャーに落とし込む予定である。

藤井進：東北大学災害科学国際研究所　災害医療情報学分野 准教授/東北大学病院 医療データ利活用センター センター長/東北大学病院 メディカル IT センター 副センター長 中村直毅：東北大学病院 メディカル IT センター 副センター長・准教授

A. 研究目的

本研究は医療機関の類型化に基づいた最適なネットワークセキュリティ構成やシステム監査のルールを示す事により、全国の医療機関が安全・安心かつリーズナブルな

費用で医療 AI サービスが利用できることを目的とする。医療 AI は、深層学習による画像認識や生成系 AI の飛躍的な精度向上により医療への有用性が示されるが、個人情報保護への配慮やランサムウェアなどのサイバー攻撃の対応も喫緊の課題となっている。本分担班は東北大学が主導的に運用する地域医療ネットワークシステム MMWIN: Miyagi Medical and Welfare Information Netowork を通して、これら相反する課題を同時解決できないか検討した。

地域医療連携システムなどを介し、多くの医療施設が抱える人材不足や投資負担の軽減を目指し、実効性のある安心安全な AI 利用基盤のネットワークアーキテクチャーを明らかにする。

B. 研究方法

近年の本邦でのランサムウェア被害を調査し、その被害や原因を知ると同時に、医療機関の実態を明らかにする。また安心安全のための厚労省らのガイドラインや医療機関へのヒアリングを参考に、医療機関での課題を明らかにしながら、地域医療連携システムを介して解決が計れるか検討する。宮城県内の医療施設にネットワークセキュリティに関するアンケート調査を実施し、超急性期病院(東北大学病院)の立場や地域医療ネットワーク(MMWIN)の立場で解析を進める。また AI 利用とこうしたセキュリティ対応が同時に成立するシステム構成の設計を、AWS を想定したクラウド基盤の前提で設計する。

C. 研究結果

1. ネットワークアーキテクチャーの検討

■ランサムウェア被害の調査

2022 年 10 月 31 日に発生した大阪急性期・総合医療センターでのランサムウェア被害がある。2023 年 3 月 28 日の新聞報道では、被害総額は 10 億円超と報告されている。また外来診療の全面再開は翌年の 2023 年 1 月 11 日となっており、システム復旧に係る費用以外にも、病院経営や地域の医療提供にも大きな影響を与えていることが再認識された。

報道等からの情報では、2016 年以降の医療機関でのランサムウェア被害は 19 件、21 年には 5 件、22 年は 8 件と急増している。主なランサムウェア被害例は、福島医大病院(2017)、新潟大学医歯科学総合病院(2017)、宇陀市立病院 (2018)、多摩北部医療センター(2019)、市立東大阪医療センター (2021)、つるぎ町立半田病院(2021)、春日井リハビリテーション病院(2022)、日本歯科大学附属病院(2022)、青山病院(2022)、鳴門山上病院(2022)などがあった。

病床規模の大小、急性期や療養期など機能や役割に関係がない、被害を受けたシステムは検査システムや治験システム、遠隔読影システム、電子カルテシステム、医事会計システム、院内の研究用 PC などであり、ターゲットも広範囲になっている。さらにはバックアップデータも被害を受けた事例もあった。

■境界型防御の実態調査

今でも多くの医療機関では、医療情報システムは外部との接続をしないローカルエリアネットワーク(院内の閉域網)を構築す

ることを原則にしている。東北大学病院も例には漏れない。最低限の外部との接続はFW やウィルス対策、IDS/IPS などガイドラインに準拠してシステムは構築がされている。

一方で電子カルテシステムがあるネットワークは安全かつ信頼できるものとして、端末とサーバ間の認証や通信監視は極めて簡単なものになっている。信頼するエリア内の端末はウィルスチェックや USB 管理、ID やパスワード管理が中心であり、こうしたものは導入時からパッケージングで対応がなされている感がある。

電子カルテシステムが接続されるネットワークは信用できるネットワーク網(閉域網)であり、利用者のログイン認証など最低限の検証を行うセキュリティモデルを構築してきた。いわゆる境界型防御を前提にしたセキュリティ対応であることが、今回の研究調査で再認識がされた。

こうした境界型防御を前提にしたセキュリティ対応がどこの医療施設でも一般的であり、実際に被害を受けた医療施設では、パスワードや VPN のバージョン管理に不備があったなど報告があるものの、方針的にはどこも同じであることも確認ができた。

先の大阪急性期・総合医療センターの調査報告書[1]では、VPN ソフトのバージョン管理やパスワード・ID の不適切な運用などが指摘され、何かしらの運用上の課題が示されているものの、近年のサイバー攻撃の巧妙化は、こうした方針では対応できないことを示し、外部からの侵入し、無防備な内部からバックアップを含めて医療情報を暗号化、システム停止・診療機能の停止へとつながることへの対応が喫緊の課題であることが再確認された調査結果となった。

■外部接続の必要性からの実態調査

医療施設はシステム機器の保守だけでなく、自営式でない病院では給食などの委託サービスなど外部接続することが増えている。一般社団法人医療 ISAC が実施した実態調査アンケートがある[2]。回答した医療施設数は 1,279 件であるが、リモートメンテナンスを許可している医療施設は実に 76%もある。そのうちリモートメンテナンスに利用している機器・製品のバージョン情報等を把握している組織は 47%という低いレベルで、危険な状態にあることも示唆された。

過去の事例(徳島県のつるぎ町立半田病院)では、ＶＰＮソフトのバージョン管理などから生じる脆弱性が原因のひとつとして指摘された。同じＶＰＮソフトを利用している医療機関は 456 あり、そのうち脆弱性対応が未了の組織は 1 割程度あったことが報告されている。つまり既知の脆弱性だけでも 45 病院が危険にさらされていて、たまたま感染していないだけの状態ともいえる。

このようなこれまでのアンケート調査からも、多くの医療施設では外部との接続は行われており、そもそも安全な閉域網という考え方が成立していない現実があった。

■境界型防御(閉鎖網)を前提とした環境におけるサーバ OS における最新化検証

多くの医療機関では、厚労省からの指導もありシステムの最新化を要求されている。しかしながら医療システムは 24 時間稼働であり、また安定的に動作することが求められていることから、検証がされていない

OS バージョンとアプリケーションの組み合わせによる稼働は慎重にならざる得ない事情もある。また自施設で対応するにも、ＯＳのアップデートだけでなくサーバＯＳサポート切れに伴って、新ＯＳでのサーバ構築まで拡大する可能性があり、費用面も課題になることがある。

そこで実例として宮城県地域連携システムである MMWIN の環境にて検証し、どのような課題があるかを検討した。

令和５年度は Windows 2012 サーバの OS（済）と Linux サーバの最新化（済）が完了し、 現在～令和６年度初め（現在進行中）では、Windows2012 Server から Windows 2016 Server へのインプレースアップグレード（in-place upgrade）による更新を試みている。

※OS の入れ替えの方法の一つで、稼働中のシステムで、稼働したままアップグレードする方式で、システムの再セットアップが不要となる。

実際には、Linux サーバにおいて、ファイルシステムの mount 系のプログラムと java のソフトウェアの仕様変更に伴って、一部のプログラムが動作しなくなったという障害が出たが、設定変更で仕様変更に伴う不具合を回避して、大きな問題なくアップグレードできた。

しかしながら、技術的な検証はできたものの、こうしたアプローチを思いつく知識、作業が実施できるスキルを持つ人材がいる医療施設は少ないと考えている。もしくは外注に依頼する場合の費用は高額になることも予測される。OS やミドルウェア、サーバソフトの脆弱性が重要な対処事項となることは間違いなく、対処するべきことと理解できる。ただしシステムを持つことで生じるメンテナンス・システム維持に係るコスト・人材不足から脱却を図ることも課題と考えられる調査事例となった。

■環境面からの実態調査

地域医療の課題には「医療施設の最適配置」や「医師の偏在の是正」、「国民との適切な受診の推進」がある。医療の役割分担の推進であり、従来からの地域完結型医療が求められている。これを推進するために地域医療連携システムが期待され、施設間で医療情報を共有することが求められている。また医師不足の解消に、今後は臨床業務で医師が院外から情報システムを利用する機会も増える可能性がある。

つまり閉域網にある院内システムは外部との接続がこの環境面からも求められているのが現実である。またデータ Health 改革や「医療 DX 令和ビジョン 2030」[3]にあるように、国民との適切な受診の機会となれば、国民が自らの医療情報にアクセス可能な PHR などにより、患者との双方向性から外部接続が前提になる可能性が高い。

■ガイドラインなどの現状調査

「医療情報システムの安全管理に関するガイドライン 6.0」[4](2023 年 5 月に更新)がある。ガイドラインでは、ゼロトラスト型のセキュリティ対応へのシフト・併用による解決を求めている。従来の境界型防御：情報セキュリティに対する考え方を整理し(ネットワークの安全性の考え方や認証のあり方)、ゼロトラスト型防御を併用した対策の考え方を示している。また IT-BCP などサイバー攻撃を含む非常時に対する具体的

な対応についても言及している。

■新たな課題

しかしながら、ゼロトラスト型セキュリティ対応を、既存の境界型防御と併用するとしても、新たにクラウド型のセキュリティ対応や動的ポリシーなどが求められることになる。つまり一部は根本からの見直しであり、導入コストの負担が医療施設にとっては重大な懸念事項になる。

さらに保守対応する部門には、こうした新たなネットワークスキルを求めることとなり、人材育成や確保が現実の課題となる。そして新たなセキュリティ負荷からレスポンスを含め利便性の低下も懸念される。この対応に、システム自体も大幅な改修が必要となるかもしれなく費用負担がここでも懸念される。

こうした「導入コストや運用上の課題・人材育成と確保」と、「サイバー攻撃の巧妙化への対応や新たな外部接続(社会的)要求への対応」が相反することとなるが、社会にとって重要なインフラである医療では、ゼロトラスト型セキュリティ対応へ進むことは間違いないと考えるべきである。つまりネットワークアーキテクチャーの検討を行うのであれば、(1)病院側のコスト負担が軽減される方向であり、また(2)人材が少ない中で実現可能なこと、(3)地域連携や保守・外部委託先など外部接続があることが前提で、かつ(4)どこの医療施設でどんなシステムでも取りこぼさない仕組みが必要となる。つまり地域でのインクルーシブセキュリティ対応が求められることになる。

そこでネットワークアーキテクチャーのSWGでは、「地域連携システム上にゼロトラスト型防御を実現し、そこに接続する医療施設を取りこぼすことないようにセキュリティ対応が可能かを検討することとした。これが実現可能であれば、多くの医療施設を効率的にかつ短期間に対応できることが期待できることになる。

2. 【地域連携システム上に求めるセキュリティ対応の考察】

まず上図1に示す通り、病院情報システムの境界が曖昧になってきている。従来の病院情報システム内だけに閉域網を作り、

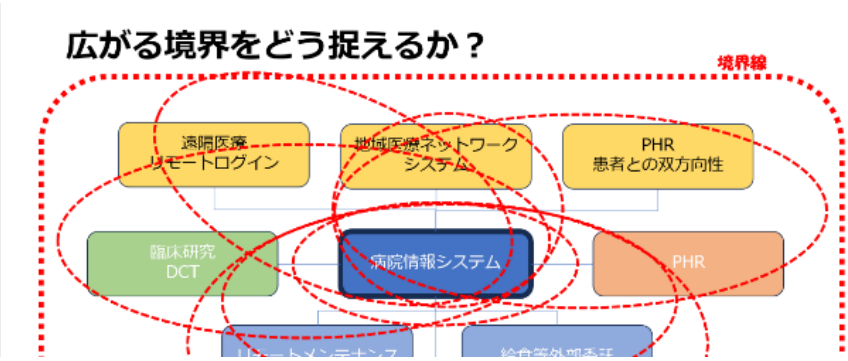

図1　境界型防御の境界はどこにあるのか

病院情報システムが中心にあるが、実際はリモートメンテナンスや外部委託、地域連携システムなど接続していることが多い。また将来的にPHRやクラウド型サービスなどのニーズから外部との接続が増えることが考えられる。そうなると境界型防御の境界をどこに設定するかの課題が生じるだろう

その内側を安全領域にするだけではセキュリティが成立ないことも理解できる。従来の院内における境界型防御：電子カルテシステムは外部接続しない、接続するにしてもファイヤーウォールやリバースプロキシを導入することで、内側は安心としてきている。つまり、端末とサーバ間の認証や通信監視は省略してきた(不正な要求を検知できない)経緯がある。

一方で USB など直接に端末に持ち込まれる悪意に対して、ウィルス対策ではウィルス対策ソフトのインストール、メール添付ファイルの取り扱い注意などの教育と啓発、USB 管理としてはポート制御、USB そのものの暗号化や認証機能を有するように多機能化することで対応を行ってきた。刑事的な罰則がある情報漏洩には不正アクセスの把握や教育と啓発によるもので、内部犯行には十分な対応がされているとは言えない状況ともいえる。

つまり水際戦略を実施しており、境界型防御と教育で、セキュリティは万全である(安全神話)という考え方である。サイバー攻撃の巧妙化はこうした安全神話を崩壊させ、外部からの侵入により無防備な内部からバックアップを含めて暗号化し、システム停止へと追い込むことから、この神話が成り立たないことは事実である。

海外事例でいえば、Tufts Medicine がある。Tufts Medicine は、クラウドのプラットフォーム上で、4 病院の 6 つの電子カルテや 40 以上のアプリケーションを統合・連携させることで、医療従事者が、PC からでもスマートフォンからでも、病院のデータに安心・安全にアクセスできる仕組みを構築している。これにより病院機能や働き方の改善を実現し、本業である医療への集中とデータ利活用の促進、20%のコスト削減が達成できたとしている。

※引用 AWS re:Invent 2022 “Realizing the full value of your EHR with a digital health ecosystem (HLC202)”, https://www.youtube.com/watch?v=7GhWW3JD5Sg
https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

この事例ではクラウド型アーキテクチャの実装を通じてゼロトラスト型の高いセキュリティレベルを実現している。*“AWS の Well-Architected Framework に従うことで、チームが目線を同じくして、セキュリティ対策に取り組むことが出来、最初のセキュリティレビューでは、驚くべきことに、5 点満点中 4.8 の非常に高い評価を得ることが出来た。(レビューアーは)これも、AWS のフレームワークに基づく推奨項目のすべてに、一つ一つに着実に従ったおかげだと明言している”(Jeremy Marut, Chief of Digital Modernization, Tufts Medicine)。※引用 AWS re:Invent 2022, “Realizing the full value of your EHR with a digital health ecosystem(HLC202)”, https://www.youtube.com/watch?v=7GhWW3JD5Sg*
https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

“これが業界の従来のやり方で、機能してきた。サーバを自分たちの机の下で管理しているから患者さんが生き残るのだ。”いう考えに

挑戦する必要があります。ナンセンスです。私たちのチーム全員が、日々、命を救っていると信じています。以前なら復旧に 6 週間か

現状を正しく把握し、クラウド利用など従来の技術に拘らず対応していくことが重要である。

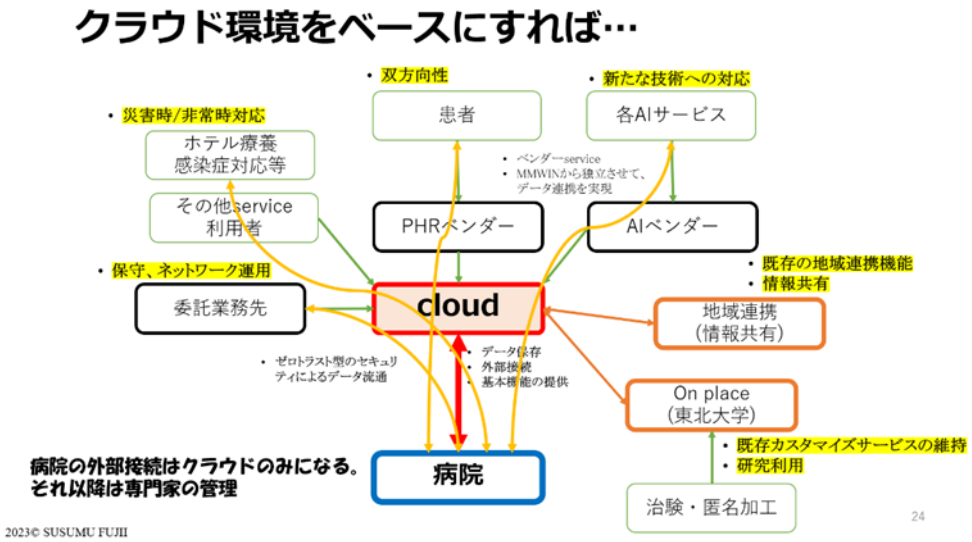

図 2 クラウドによる課題解決の関係

病院は外部接続がクラウド接続に集中できることで、境界型を強化しつつ、サービスがクラウド上での接続になることで全体解でのゼロトラスト型セキュリティ対応も行われる。

かる障害が起きても、救命救急を止めずに済みました(Jeremy Marut, Chief of Digital Modernization, Tufts Medicine)の言葉にあるように、セキュリティ対応の真の目的は、「Saving lives, not drives! 救うのは患者の命、ドライブではない!」

※引用 AWS re:Invent 2022, "Realizing the full value of your EHR with a digital health ecosystem (HLC202)", https://www.youtube.com/watch?v=7GhWW3JD5Sg

https://aws.amazon.com/jp/solutions/case-studies/tufts-case-study/

これらのように、セキュリティ対応の目的は患者の命であり、医療機能を停止しないことが重要である。こうした命題に対して、

そこで SWG では、まずクラウド導入により医療施設がもつ課題をどの程度改善できるかを検討した。図 2 に課題対応できる関係性を示した。

図 2 に示す通り、クラウドを経由してリモート保守や外部委託先との接続、地域連携システムとの接続、将来的なニーズを含む患者との双方向性、AI サービスなども接続可能となる。この場合、医療施設ではクラウド接続する 1 つの接続線を管理すれば良く、運用における管理対象が大幅に軽減される。クラウド上に展開されるサーバや接続サービスはクラウドベンダーやその先のベンダーによるものとなり、こうした管理からも解放される可能性が高い。

そこで SWG では図 3 に示す通り AWS 上で

図 2 に示した内容を実現することが可能かをアマゾン・ウェブ・サービス・ジャパン合同会社の協力を得て調査した。

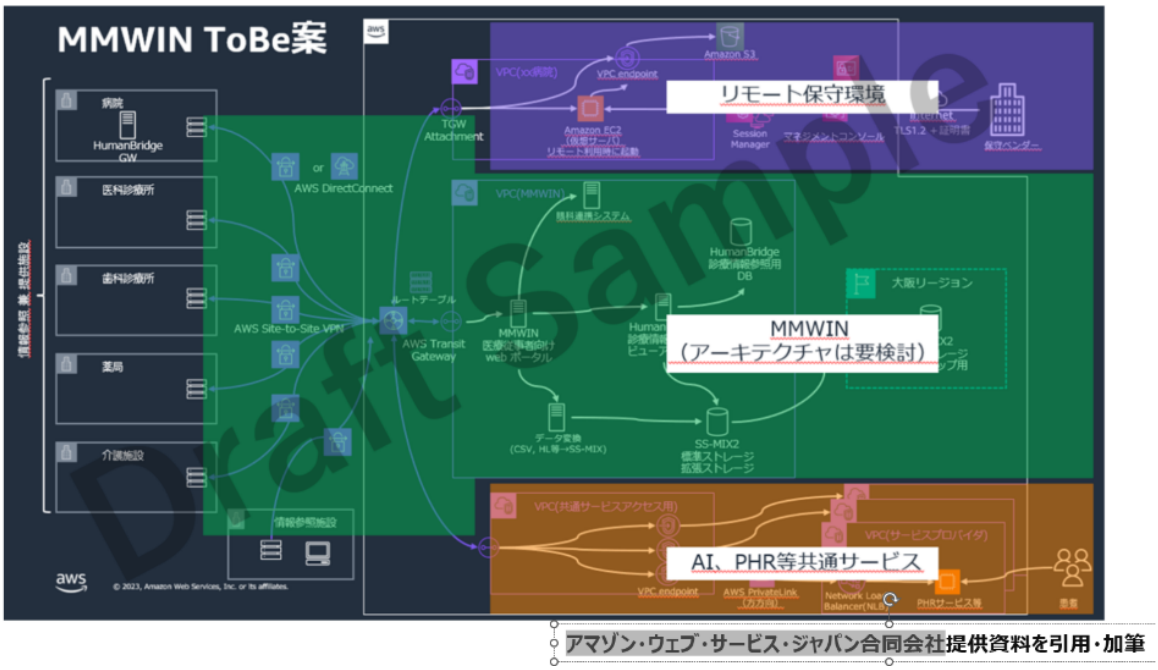

図 3　AWS を使ったセキュリティ対応モデルの設計

基本的に外部からの保守契約は、クラウド内にサーバ A、サーバ A のみが院内にあるサーバ X に到達できるような設定サービスで可能であり、外部委託サーバも同様に設定可能である。また外部委託サーバ自体をクラウド上のサービスに変更できれば、より安全性が高まることも考えられた。AI や PHR サービスは既に AWS などのクラウド上で展開されている事例が多く、AWS 内でのサーバ接続で対応可能であった。

一方で backup に関しては、遠隔地保存自体が災害や火事などの事象には有効な手段であるが、ランサムウェアなどにおいては全てが解決できる状況にないこともわかった。クラウド上に保存した backup は外部と遮断されていることから、backup データにあるウィルスが発症して悪意のある動作をしても問題が発生しにくい。また変更そのものができないから、暗号化されてしまうなどの被害を食い止めることは可能である。しかしながら、既に感染した情報であることは否定できないので、そこからリストアすることは再感染を起こす可能性があり、単純には利用できるデータにはならない。なにかしら感染を検知する事前の処理が必要となるだろう。

しかしながら、多くの課題が解決できることと、これがパッケージングされて導入すればゼロトラスト型セキュリティ対応の一部になるのであれば、その実効性も高いものになる。つまり地域連携システムのように今後は必要となるであろうシステム上に、もしくは宮城県のように 739 施設が参加するシステム上に、cloud 環境を有効に使

うことで、これまで院内だけの境界線を地域の医療システム全体を境界線とし、合わせてゼロトラスト型セキュリティ対応を併用できることになる。これはコストの面や人材育成・確保という課題解決にもつながるものであり、合理性が高いアプローチと考える。ただしbackupや外部接続なども鑑みながら、動的ポリシーなどにより要求を管理して安全性を高めることがなければ、成立しない安全性もあることを踏まえていく必要がある。

2023年度のSWGでは、これまでの実態調査からゼロトラスト型セキュリティ対応の必要性を再認識し、ゼロトラスト型セキュリティ対応の導入時の課題を整理し、人的リソースや導入コストを指摘した。また具体的にどのようなサービスが必要なのかをユースケースとして検討した。そこでクラウド環境を利用することで多くが解決できる可能性があることを示唆した。

2024年度はこれら知見をより詳細に定義し、クラウドベンダーの比較や疑似環境を通して課題を調査しながら、最終年度の実証に向けて研究を進める予定である。

3. 【地域連携システム上にゼロトラスト型セキュリティ対応ができることの意識調査】

宮城県内にある医療施設(介護施設内にある診療室を含む)1753施設にWEBによるアンケートを実施した(2024年3月)。内容には地域連携システムにおいてクラウドを活用し、そこでゼロトラスト型セキュリティ対応が実現するとしたら、ニーズがあるのかを調査である。

従来の境界型防御(電子カルテネットワーク内は安全)というセキュリティ対策から、ゼロトラスト型セキュリティ(安全な領域はない)の併用への転換を厚労省からも推奨している。しかしながら、これに対応したくとも、スキルを持った人材の育成や人材確保が難しいことを説明し、地域連携システムを通して外部接続やバックアップがされることで、ランサムウェア対策を兼ねることが可能であれば、医療機関にはメリットがあるかのニーズを調査となっている。

速報値でいえば60～70%が地域医療連携システムを介してセキュリティ対応がなされるのであれば、前向きな回答となった。詳細は次年度にまとめて設計に活かす。

なおアンケート項目は文末に「A1.地域連携システムにおけるセキュリティ対応のニーズ調査」に添える。

参考文献

1) 情報セキュリティインシデント調査委員会.調査報告書. 地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター,2023. https://www.gh.opho.jp/pdf/report_v01.pdf

2) 全国保険医団体連合会/日本病院会.セキュリティアンケート結果調査. 一般社団法人医療ISAC,2023.https://m-isac.jp/wp-content/uploads/2023/08/report_20230120.pdf

3) 「医療DX令和ビジョン2030」厚生労働省推進チーム.医療ＤＸ.厚生労働省,2022. https://www.mhlw.go.jp/content/10808000/000992373.pdf,

https://www.mhlw.go.jp/stf/shingi/other-isei_210261_00003.html
4) 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 6.0 版.厚生労働,
2023.[https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html]

D. 健康危惧情報

代表者報告書で適時記載

E. 研究発表

1. 報告書
   ① 地域連携システムをベースにしたゼロトラストセキュリティの実現性の検討：ネットワークアーキテクチャーの検討(本報告書)

2. 学会発表
   ① 第 43 回医療情報学連合大会 大会企画２　境界型防御からゼロトラストへ
      1. 医療情報システムにおけるプラス・セキュリティとは -起きることを待つ、から起きていることを当たり前に(猪俣敦夫：研究班有識者)
      2. 境界型防御からゼロトラストへ　医療機関からの視点(藤井進・中村直毅：東北大 SWG)
      3. 地域連携システムや PHR システムでのゼロトラストの考え方(名田茂)
      4. 安全・安心なネットワーク環境やクラウド基盤に支えられた AI サービスの利活用による医療・ヘルスケアのデジタルトランスフォーメーション(宇賀神敦：研究班主担当)
   ② 第 29 回日本災害医学会総会・学術集会
      1. 災害時の医療情報提供に関する意識調査

3. 大会論文集・査読付き詳細な抄録
   ① 藤井進, 境界型防御からゼロトラストへ - 様々な視点からゼロトラストへの転換を考える -, Vol43 Supplement, 43 回医療情報学連合大会論文集(24 回日本医療情報学会学術大会), p141, 2023/11.
   ② 藤井進　野中小百合　金秀明　浅見太一　江川　新一, 災害時の医療情報提供に関する意識調査, Vol28 Supplement,Japanese Journal of Disaster Medicine, p454, 2024/02.

F. 知的財産権の出願

・なし

以上

添付

A1.地域連携システムにおけるセキュリティ対応のニーズ調査　アンケート内容：

No	質問	回答
自院の状況についてご質問です		
1	病床規模を教えてください。	1：クリニック 2：病院（400 床以上） 3：病院（200～399 床） 4：病院（200 床未満） 5：薬局 6：介護施設 7：歯科
2	自院のセキュリティ人材が不足していると感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
3	自院ではセキュリティ対策がきちんとできていると思いますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
4	MMWIN には参加していますか？	1：はい 2：いいえ
地域医療連携システムの情報共有についてご質問です		
5	地域医療連携システムを使って、画像の共有ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない

6	地域医療連携システムを使って、検査結果、薬歴、病名の共有ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
7	地域医療連携システムを使って、紹介、逆紹介、診療予約ができることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
地域連携システムを使うことによって、医療情報の共有だけでなく、以下のセキュリティ対策がなされるとするとメリットがあるかに関するご質問です		
8	**医療機器や電子カルテシステムのリモート保守に対する向上することに魅力を感じるか。**	
8-1	リモート保守の向上１：複数ある“VPN回線（ベンダー毎の保守回線）”や“外部との接続方法”が、１つに集約されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
8-2	リモート保守の向上２：“VPN サーバ”や“リモートログインサーバ”の保守から解放されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
8-3	リモート保守の向上３：外部委託業者（例えば給食）の“外部持ち込みサーバとの接続管理”から解放されることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
9	**部門システムや電子カルテシステムの“バックアップを地域連携システムが稼働するクラウド上に保管”することに魅力を感じるか**	
9-1	地域連携の“クラウド上に院内の医療情報システムのバックアップができる”ことに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない

		4：あまり感じない 5：まったく感じない
9-2	地域連携の“クラウド上にバックアップを置くことで**ランサムウェアの対策**を兼ねる”のであれば、魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
9-3	**災害対策**として“クラウドにバックアップデータが保存される”ことに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
10	**地域医療連携システムのネットワークを活用したその他の用途について**	
10-1	地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)が使えることに魅力を感じますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない
10-2	地域連携システムを通して、AI(診断補助やカルテ作成などの医師の業務支援など)を使うときに、患者の診療情報が地域連携システムを通して安心安全(三省のガイドラインに準拠)に情報共有されるとしたら、利用したいと考えますか？	1：とても感じる 2：やや感じる 3：どちらでもない 4：あまり感じない 5：まったく感じない