

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 医療 AI プラットフォーム技術研究組合及びシステム WG リーダ

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た。

医療機関のセキュリティ対策の現状を理解するために、23医療機関に対面でヒアリングを実施した。ヒアリング内容をもとにネットワークの類型化を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。

2024～2025 年度は医療機関から外部接続するユースケースを整理し、あわせてベンダ目線・ディラー目線のヒアリングも実施した。

A. 研究目的

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の類型化案を策定し、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に、国内外の最先端セキュリティ技術を探査し、機能評価を行う。その結果、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を示した。

2024 年度は、2023 年度の成果をもとに、医療機関から外部接続するユースケースを整理し、クラウド利用における課題点等を抽出した。

2025 年度は、2024 年度に残として残っていたユースケース 2 の評価の実施、ならびに医療機関に対してメンテナンスを行っているベンダ及び医療機関に対して機器等を販売しているディラーを含めて幅広くヒアリングを実施した。

B. 研究方法

医療機関から外部接続するユースケースを選定し、該医療機関へ実態調査のためのヒアリングを実施した。

またベンダおよびディラーへヒアリングを実施した。

C. 研究結果

(1) ユースケースは以下の5パターンを選定した。No1,4,5 は実際国内医療機関にて稼働させているベンダ様へヒアリングを実施した。

No2,3 はネットワークアーキテクチャグループの東北大藤井先生・中村先生にご協力いただき、PoC 環境を準備し評価を実施した。

① ユースケース1：医療機関側で新たなネットワークやシステムの新設工事負担なしに、既設のネットワーク・システムを利用して、医療AIプラットフォーム技術研究組合（Healthcare AI Platform Collaborative Innovation Partnership、略称「HAIP」）に搭載されている医療AIを活用できるかを、株式会社ソフトウェア・サービス(略称SSI)と恵寿総合病院の協力を得て実証を行っている内容のヒアリングを行った。

医療機関にとってのメリットは以下である。

- ・ 既設のネットワークを利用することでシステム利用のための機器購入等のコスト負担がかからない。
- ・ 電子カルテベンダーは、既設のネットワークを利用することで、医療機関側と導入調整がしやすい。
- ・ 医師は、電子カルテ側の環境に機能を追加するため、医療従事者側の操作に影響がない。
- ・ 医師は、AI サービスを利用することで、異変の見落とし防止や、業務の効率化できた。

② ユースケース 2：各医療機関が AI を活用する場合に課題となるシステムの導入コスト負担を抑えるために、地域医療連携システムを経由し、HAIP の基盤に搭載されている AI に接続できるかを、東北大学病院の協力を得て実証を行った。

③ ユースケース3：AIの利用形態の1つとしてクラウド上にある音声AIの活用や電子カルテ端末によるWeb会議の利用を検討しており、端末側マイクデバイスで利用できる新しいインターネット分離ソリューションであるRevoWorks Browser(ジェイズ・コミュニケーション株式会社製品)を試験的に利用し、音声AIの活用やWeb会議が利用可能か東北大学病院様の協力を得て実証を行った。

医療機関にとってのメリットは以下である。

- ・ 既電子カルテ端末がインターネットに接続できる為、別途インターネットに接続可能な端末を用意する必要がなくコストの削減が可能。
- ・ 端末側のマイクデバイスを利用できるため、電子カルテ端末で音声 AI・Web 会議の利用もでき、医師の働き方改革に活用できる可能性がある。
- ・ インターネット分離製品のため、セキュアにインターネットに接続できる。(ローカルコンテナ技術を利用しているため、万が一感染しても、端末のローカルデータに影響を及ぼさない)

但し、システムを導入するためのネットワーク変更・機器の導入コストが多くかかるデメリットもある。

④ ユースケース 4：医師の働き方改革制度に伴い、これまで院内利用のみが主体であった電子カルテシステムに、医師が院外からセキュアにアクセスできる仕組みが必要になることが想定される。院外からセキュアに電子カルテシステムへアクセスできる仕組みについて、既にリモートデスクトップサービス(略 RDP)を活用しているケースをヒアリングした。医療機関のメリットとしては、併設のクリニックや外出先から電子カルテシステムにアクセスすることで、往診や緊急時のテレワーク等が可能になり、医師の働き方改革につながる可能性がある一方、サービス導入のコストとしてはネットワーク環境を用意するため割高になる。

- ・ 常時 3Mbps の回線を保有可能なネットワークを用意する必要がある。
- ・ クリニック⇄本院等医療機関を接続するための VPN または、閉域網を用意する必要がある。
- ・ 外出先から医療機関のネットワークに接続するための、端末および VPN 装置、閉域網が必要となる。

⑤ ユースケース5：離島やへき地における医療の地域差を縮め、医療の質の向上や患者の利便性の

向上のため、徳洲会グループ採用しているボーダレス・ビジョン株式会社、天馬諮問株式会社の2社へヒアリングを行った。

医療機関にとってのメリットは以下である。

- ・ 遠隔で医師と医師がつながることで、専門的な意識を持った医師の支援を受けながら、離島・へき地の医師が手術を行うことができる。
 - ・ ⇒患者も離島から本土に移動することなく、手術を受けられるため、移動等患者の負担も軽減できる。
 - ・ 教育ツールとして利用することで、離島・へき地の医師に対し、本土の医師が指導することができ、意思の技術力向上にもつながる。
 - ・ オンライン診療にも利用可能であり、遠方にいる患者の診察・診断ができる。
 - ・ 救急時に、専門外の患者に対して、専門医の支援をうけることができる。
 - ・ 既存でインターネットに接続可能な端末があれば、別途専用機器を用意することなくシステムの利用が可能(手術支援のための専用機器が必要な場合を除く)
 - ・ HIS系のネットワークに接続する必要がないため、重要ネットワークに影響なく導入が可能である。
- 但し、サービス導入のため、機材の購入が必要なことがある。

ユースケース導入難易度は以下と評価。

<<難易度：高>>

実証システムを利用するためにネットワークの大幅な変更や新設・または機器の調達が必要となる。セキュリティポリシーにより実証システムを導入することが難しい

<<難易度：中>>

既設ネットワークの軽微な変更、または機器の調達が必要となるが、実証システムの利用が可能

<<難易度：低>>

既設ネットワークの変更が少ない、または設定変更なく実証システムの利用が可能

それら難易度をユースケースに当てはめると、

ユースケース	難易度
No1	低
No2	高
No3	高
No4	低
No5	高または中

であった。

(2) 医療機関への保守業務に関するベンダヒアリングの結果として、以下総括。

本ヒアリングの結果、ベンダ各社においては、医療機関向けリモート保守に関するセキュリティ対策や運用体制について、一定のルールや管理のもとで実施されていることが確認された。

一方で、セキュリティチェックリストや3省2ガイドラインの運用に関しては、医療機器と一般的な医療情報システムとの特性の違いにより、現場での対応や判断が難しい場面があるとの意見も挙げられた。また、医療機関ごとに異なる運用ルールやチェックリスト対応、ガイドラインの解釈差などにより、ベンダ側・医療機関側双方に一定の対応負担が生じているとの指摘もあった。

そのため、医療機器の特性を踏まえたリスクベースでの運用や、チェックリスト・ガイドラインの解釈の明確化、関係者間での共通理解の促進が今後の課題として示唆された。

3省2ガイドラインについて、ベンダ側の視点から、業務運用上で感じている課題や支障の有無について以下に整理する。

① 医療機器の特性を踏まえたガイドライン適用の必要性

医療機器は装置の種類や用途により扱う情報や業務内容が大きく異なるが、現行のガイドラインではその違いが十分に考慮されていないとの意見があった。また、電子カルテ等の情報システムと同一の基準で要求されることで、実運用との乖離が生じる場合があるとの指摘があった。

② リスクベースの運用への見直し

現在はチェックリスト形式での対応が中心となっているが、本来のリスクマネジメントの考え方に基づいた運用ができるよう、よりリスクベースの内容に見直すことが望ましいとの意見があった。

③ 医療機器運用とセキュリティ対策のバランス

医療機器では装置の安定稼働や正確な検査結果の提供が重要であり、過度なセキュリティ対策が装置の動作や検査精度に影響を与える可能性があるため、機器特性を考慮した対策が必要との意見があった。

④ ガイドラインの適用範囲や解釈の分かりにくさ
ガイドラインの適用対象や参照すべき資料が多く、医療機関や事業者間で解釈に差が生じる場合があるため、省庁横断での整理や分かりやすい解説の提供を望む声があった。

⑤ 医療機関との理解差による対応負担

ガイドラインに基づくリスク説明やチェックリスト対応において、医療機関側の理解度に差があり、説明

や調整に時間を要するケースがあるとの意見があった。

⑥ 運用管理に伴う負担

ガイドラインの要求事項が網羅的であるため、自社の規程や運用手順と紐づけて継続的に管理・更新していく作業に一定の工数を要するとの意見があった。

(3) デイラーへのヒアリング結果としては以下に示された。

3省 2GL やサイバーセキュリティリストを知らない。セキュリティの商材を提案したことがない。サイバーセキュリティについて相談を受けることもほぼない。という結果が出た。つまり、デイラーはセキュリティへの意識は少なく、医療機関からも求められていない現状が見て取れた。

(4) 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調査を 2023 年度～2025 年度に実施した。

- ・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。今年度は一部調査を追加し、また 2023 年度からのピックアップソリューションが ISMAP の登録状況等確認を行った。

D. 考察

複数のユースケースをヒアリング・実証した結果、医療機関が医療 AI やシステムを利用する場合、以下の効果が考えられる。

- ・ 医療機関の既設のネットワーク・システム設備や地域医療連携システムを活用することで、病院側の費用・運用変更の負担を抑え医療 AI を推進できる
- ・ 遠隔医療のための IT ソリューションを活用することで離島やへき地における医療の地域差を縮めることを可能とし、医療の質の向上や患者の利便性の向上に有効。
- ・ クラウド上の医療 AI の利用による医療の質、業務の効率化が期待できる。
- ・ 外出先や自宅など医療機関外から電子カルテ等の情報を閲覧可能とする事例が増えてきている。今後の需要次第では働き方改革につながることも期待できる

また、ユースケースを実施する中で医療機関が安全・安心にデジタル技術を活用するための課題も見えてきた。

- 医療機関によってことなるセキュリティレベル
 - 医療機関によっては、セキュリティ方針により電子カルテ端末など HIS 系の情報をインターネット側に接続できない。
 - クラウド上の医療 AI を利用するには、医療機関のネットワークをインターネットに接続する場合もある。そのため外部からの攻撃に備えたセキュリティ対策も必要である。
 - 各医療機関が理想的なセキュリティ状態を維持するためには、セキュリティ有識者の協力やセキュリティ製品の導入コストも必要となる。
 - 医療機関ごとに異なるネットワーク・システム構成
 - 既設のネットワークを利用して医療 AI を利用可能な医療機関も、ネットワーク帯域量によっては利用できない、または帯域量の変更が必要となる場合がある。
 - 医療機関のネットワーク構成によっては、医療 AI や IT ソリューションを導入するために、大幅なネットワーク構成の変更や機器の導入が必要な場合がある。
 - IT ソリューションによっては、端末に標準搭載されているサービスで利用可のであるが、製品によっては専用ソフトウェアを導入する必要がある、端末の他ソフトウェアとの互換性も考える必要がある。

E. 結論

医療機関・ベンダ・ディーラそれぞれの立場からアンケートを取得した結果、医療機関においては以下の課題があると考ええる。

- ・保守メンテナンス用の回線がベンダ各々あるため、セキュリティが不十分になりがちである。
 - ・クラウドサービスの利用が停滞しており、情報の未活用の部分が多分にある。
 - ・医療情報を扱うシステム担当者が不足しており、従事者の業務負担が増大している。
 - ・医療にかかわるものがみなガイドラインを理解しているとは限らない。また、ガイドラインの適用対象や参照すべき資料が多く、医療機関や事業者間で解釈に差が生じている。
 - ・既存の境界防御型のみでは、ランサムウェアからは守れない。
- 課題への対策として、
- ・医療機関からの外接点のネットワーク集約

- ・既存の設備や技術を活用しながら、セキュアなネットワークインフラを構成し医療 DX を支えること
 - ・VPN+ α の新しい技術の活用をガイドラインとして導入可とする取り組み
 - ・ガイドラインの解釈に差が出ないように、省庁横断での整理や分かりやすい解説の提供
- これらの取り組みを行うことでより AI 等のクラウド利用が促進するものと考ええる。

F. 研究発表

該当なし

G. 知的財産権の出願・登録状況

1. 特許取得 特許取得予定なし
2. 実用新案登録 現時点で該当なし
3. その他 該当なし

資料 医療機関から外部接続するユースケースの整理

No	ユースケース名	ユースケースの目的や背景	本ステップにおける実証可否	実証協力病院	備考
1	医療機関の既設ネットワークを利用したAIサービスの活用	病院に新たな工事負担なしに、既設ネットワークを利用し、クラウド上の医療AIサービスを活用できるか実証が行われていたため、その内容をヒアリングしレポートに記載 実証期間: 2024/5-2024/8	未実証 既に実証が行われていたため、その内容をヒアリングしレポートに記載 実証期間: 2024/5-2024/8	恵寿総合病院 病床数426床	利用技術・製品 ・ IP-VPN ・ インターネットVPN
2	地域医療連携システムを介したセキュアなインターネットの利用	各医療機関が医療AIの活用する場合に課題となるシステムの導入コスト負担を抑えるため、地域医療連携システムを活用し、医療AIの利用が可能かを検証する。	実証済み 実証期間: 2025/3	東北大病院 病床数1,160	利用技術・製品 ・ CATOクラウド ・ Azure
3	インターネット分離システムを利用したWeb会議および、音声AIサービスの活用	医療AIの利用形態の1つとしてクラウド上にある音声AIの活用を検討しており、端末側マイクデバイスで利用できる新しいインターネット分離ソリューションを試験的に利用し、音声AIの活用やWeb会議が利用可能かを検証する。	実証済み 実証期間: 2024/8~2025/3	東北大病院 病床数1,160	利用技術・製品 ・ RevoWorksBrowser 導入実績 ・ 複数病院に導入実績あり(総数非公開)
4	医師が院外からセキュアにアクセス可能なシステムを利用した電子カルテシステムの活用	医師の働き方改革制度に伴い、これまで院内利用のみが主体であった電子カルテシステムを、医師が院外からセキュアにアクセスできる仕組みも必要になることが想定され、院外からセキュアに電子カルテシステムへアクセスできる仕組みについて検討する。	未実証 既に製品として実運用が行われているため、その内容をヒアリングしレポートに記載	-	利用技術・製品 ・ RDP ・ IP-VPN ・ インターネットVPN
5	遠隔医療システムを活用した手術支援実施	離島やへき地における医療の地域差を縮め、医療の質の向上や患者の利便性の向上のため、遠隔医療の実証を徳洲会が実証していたため、その内容をレポートとしてまとめ、他病院でも活用できるかを検討する。	未実証 既に実証が行われていたため、その内容をヒアリングしレポートに記載	-	5-1 利用技術・製品 ・ kizunaWeb ・ 導入実績: 15病院以上 5-2 利用技術・製品 ・ TELEPRO ・ 導入実績: 病院・大学含む15施設以上

図1 医療機関から外部接続するユースケース一覧

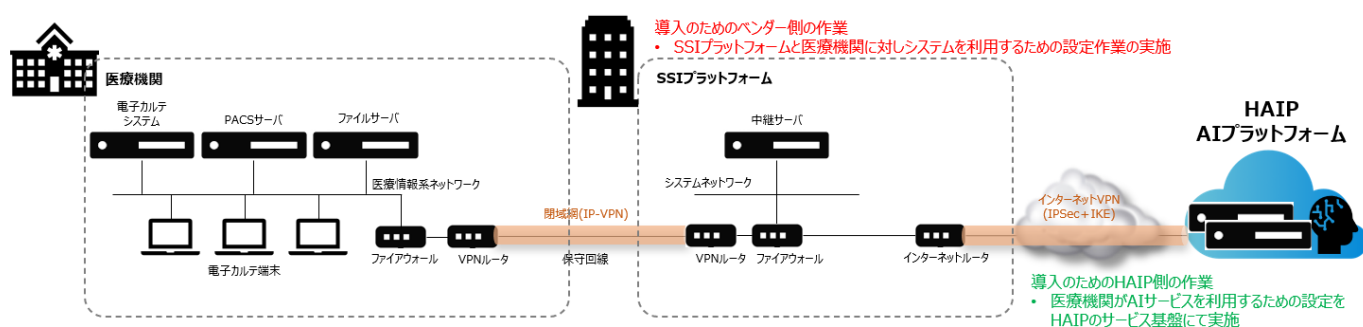


図2 ユースケース1の概要図

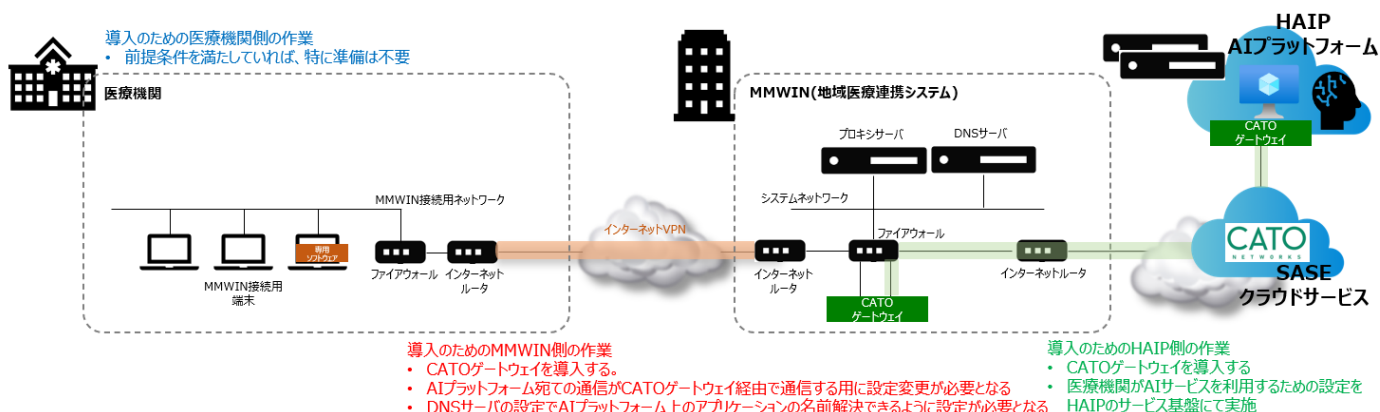


図3 ユースケース2の概要図

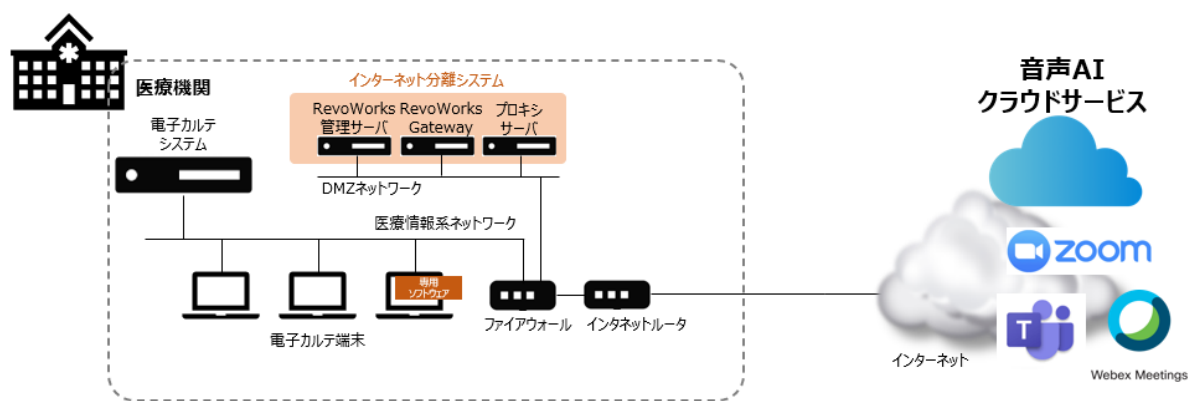


図4 ユースケース3の概要図

構成No	概要	接続元	接続先	接続方法
1	同じ電子カルテ情報を扱うクリニックから電子カルテシステムが存在する医療機関へRDP接続し電子カルテシステムを利用	クリニックの電子カルテ端末	電子カルテシステムが存在する医療機関	クリニックと医療機関を閉域網で接続、RDPを利用し、電子カルテシステムを利用
2				クリニックと医療機関をインターネットVPNで接続、RDPを利用し、電子カルテシステムを利用
3			電子カルテシステムが存在する医療機関の電子カルテ端末	クリニックと医療機関をインターネットVPNで接続、RDPを利用し、医療機関内の電子カルテ端末に接続し、電子カルテ端末経由で電子カルテシステムを利用
4	医師が外出先から医療機関の電子カルテを閲覧	外出用の持ち出し端末	電子カルテシステムが存在する医療機関	外出先の医師の利用端末から医療機関に閉域網を接続、RDPを利用し、電子カルテシステムを利用
5				外出先の医師の利用端末から医療機関にインターネットVPNを接続、RDPを利用し、電子カルテシステムを利用

図5 ユースケース4の構成パターン

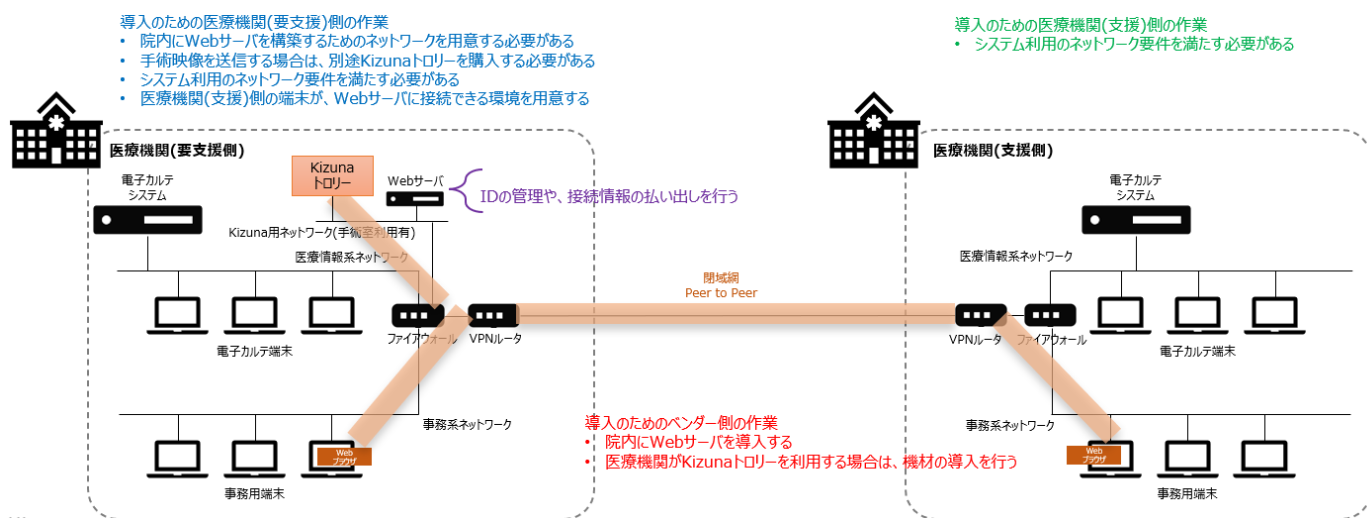


図6 KizunaWeb(ボーダレス・ビジョン社製品)

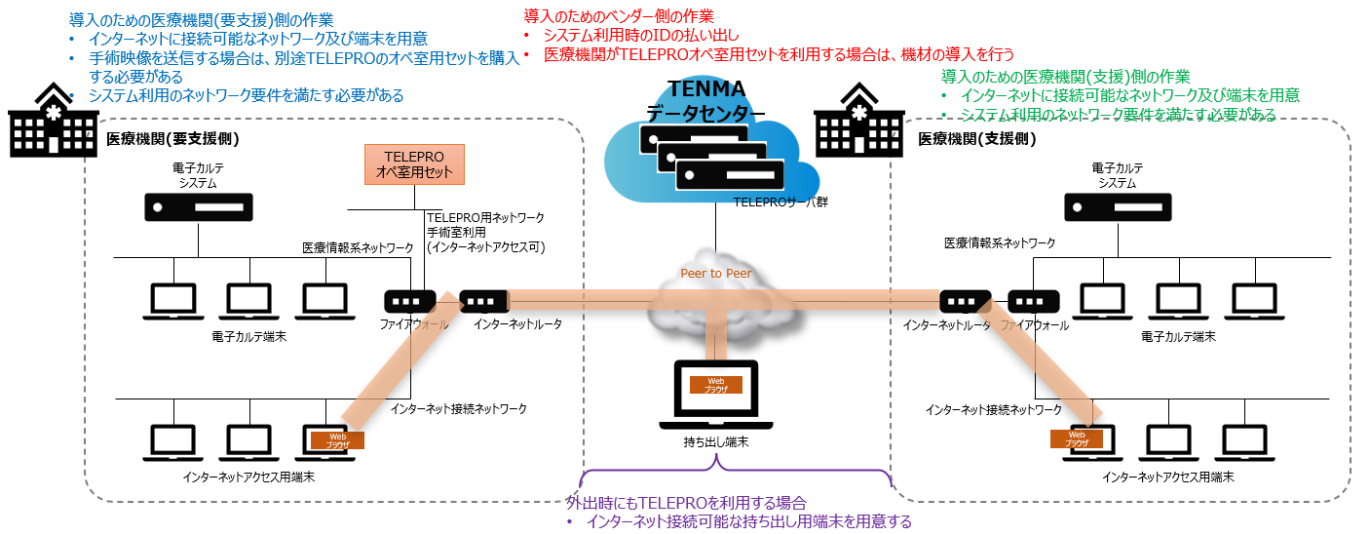


図7 TELEPRO(天馬諮問株式会社製品)