



診療を止めず、医療DXの推進を下支えする 信頼性と性能、セキュリティを兼ね備えた 大規模ネットワークインフラを実現

FTTD(Fiber To The Desktop:光直収ネットワーク)を中心に、医療機関としては画期的な高速ネットワークを整備してきた群馬大学医学部附属病院は、更新を機に、さらなるレスポンス改善と運用性の向上を目指し、Wi-Fi 6 対応のアクセスポイントを1,000台超導入。稼働信頼性と性能、セキュリティといった複数の要素を兼ね備えたネットワークインフラを、フォーティネットのソリューションを活用して実現している。

拠点病院としてどんな事態でも 医療を継続する体制を整備

群馬大学医学部附属病院（以下、群大病院）は北関東有数の拠点病院として、コロナ禍の間も含め地域の高度な医療を担ってきた。規模も大きく、病床数は731床を数え、外来患者は一日平均約1,900名に上るほか、入院患者も平均590名に上る。

そんな大規模かつ高度な医療を支えているのがさまざまな医療システムだ。1988年のオーダリングシステム導入を皮切りに、2009年には電子カルテシステムを導入するなど、ほぼすべての医療業務が電子化されている。2011年の東日本大震災の後に計画停電の影響を受けるといった経験を経て、どのような事態が起きても医療業務を継続して患者の命を守るため、紙ベースでの

導入・構築のポイント

- (1) Wi-Fi 6 対応のアクセスポイントにより、医療業務を妨げない高速ネットワークを実現
- (2) ベンダーを統一することで運用性を高め、障害発生時の時間と工数を削減
- (3) FortiGateとFortiNACを組み合わせ、マイクロセグメンテーションによってセキュリティを強化

運用も行える訓練も実施している。ただ、日々の医療をつつがなくこなす上で各種のシステムはやはり不可欠な存在だ。

一方医療の世界では、コロナ禍も相まってDXが急速に進展している。クラウドサービスを活用して電子処方箋を提供したり、診療報酬の会計処理を行ったりといった動きが進み、クラウドな方針で運用されてきた医療機関のシステムも開かれる方向へと向かっている。それだけでなく、医療システム・機器のメンテナンスのためにリモート接続を許可したり、

医薬品や備品の調達などを担う病院外の組織、いわゆるサプライチェーンと連携するといった形で、実質的に外部との接続は行われてきた。医療DXはその動きをさらに加速させている。

外部に目を向ければ、地政学的な情勢もあって、サイバー攻撃は増加の一途をたどっている。こうした中で群大病院も含め医療機関には、医療を継続するため可用性を確保しつつ、サイバーセキュリティを強化して機密性も保つという、二つの要素の両立が求められている。



国立大学法人 群馬大学医学部附属病院

所在地 群馬県前橋市昭和町3-39-22

1943年、前橋医学専門学校の附属施設として設置される。731床の病棟と1,700名以上のスタッフを擁し、1日1,800名の外来患者と年間2万人の入院患者（2021年度）の診療を行う、北関東有数の拠点病院。システム統合センターは、大学病院としての3機能である臨床・研究・教育を主軸に活動しており、2022年度からは内閣サイバーセキュリティセンター（NISC）の医療分野におけるセブター活動において、セキュリティ領域の幹事を務めている。



国立大学法人
群馬大学医学部附属病院
システム統合センター
センター長 准教授
齋藤 勇一郎氏



国立大学法人
群馬大学医学部附属病院
システム統合センター
副センター長 准教授
烏飼 幸太氏



国立大学法人
群馬大学医学部附属病院
システム統合センター
助教
野口 怜氏

ネットワークは動いて当たり前、音声品質も課題に

どのような組織でもそうだが、大規模な医療機関でも部局ごとに縦割りで電子化やITインフラの整備が進められるケースが珍しくない。「とにかくつながればいい」とその都度拡張していくと、無駄な投資が生じる一方で、使いにくいものになってしまう。しかし群大病院では、「システム統合センター」という名前が示す通り、全体最適を見据えた取り組みを進めてきた。「各部門が勝手に進めているのは全体の整合性がとれません。システム統合センターという名称には、きちんとシステムをつなぎ、全体として利用しやすくしていくという意図が込められています。院内をとりまとめ、分けるべきところは分け、共有できるところは共有する形で最適化しながら、学内の環境を整備してきました」（群馬大学医学部附属病院システム統合センター センター長 准教授 齋藤勇一郎氏）

こうした哲学に基づいて2015年に刷新されたネットワークでは、医療機関としては珍しくFTTD（Fiber To The Desktop：光直収ネットワーク）を整備し、高いネットワーク性能を実現していた。合わせて病院全体のIT資産を洗い出した上でネットワークポロジも整理し、見通しの良いシンプルなアーキテクチャへと変更。障害対応や運用を容易に

し、「止まらない」ネットワークを実現した。

しばしば医療機関のネットワークは、クローズドの神話に頼るか、それともオープンかの単純な二元論で語られがちだ。しかし、「何は守るべきで、何は開いておくべきなのかを踏まえ、適切にセグメンテーションを行って通信を制限できるようデザインすれば、きちんとグラデーションを付けられます」（同副センター長 准教授 烏飼幸太氏）。そうしたコンセプトに基づき、医療業務に必要なレスポンスとセキュリティを実現してきた。こうやってネットワーク環境を整備してきた群大病院でも、やはり課題はあった。

「現場には、車のエンジンをかけたら動くのと同じように、ネットワークは動いて当たり前という感覚があります。無線LANのスピードが少し遅くなったり、ネットワークトラブルがあつたりすると利用者のフラストレーションが溜まるだけでなく、医療の現場も止まってしまうかねません」（同、助教 野口怜氏）

実際、医療の現場では、ささいに思える問題が大きな影響を及ぼす可能性もある。「Webページの表示が遅れるのも使い勝手を損ないますが、特に厳しく要求されるのはストリーミングや音声の品質です。遅延（レイテンシー）によって音が割れ

たり、間延びしてしまうと、重要な薬剤の名前を聞き間違えてしまう恐れもあります」（烏飼氏）

コミュニケーションが途切れ途切れになればストレスがたまり、聞き返すのも手間となるため必要なことを言い出しにくくなるといった二次的な課題も生じる。医療安全の確保においても、セキュリティを保ちつつスピードを保つ、その両立が課題だと捉えていた。

「サービスを提供する上では、稼働信頼性を非常に高くするとともに、動画や音声も含めたリアルタイムのコミュニケーションが快適に行えることが本質的に重要だと考えています」（烏飼氏）

Wi-Fi 6 対応に加え、性能、信頼性、運用性を評価

2023年のネットワーク更改ではそういった観点から、既存のFTTDと既存のネットワークポロジを生かしながらさらなる改善を目指した。

まず着目したのが、ラストワンメートルではないが、デバイスをネットワークにつなぐ無線LANの性能だ。リアルタイムコミュニケーションを快適に行えるよう遅延を抑えた環境を構築したいと考えていたが、ちょうどWi-Fi 6に準拠した機器が登場してきた。

以前から使ってきたフォーティネットの無線LANシステムにもシング



サーバールームで稼働するFortiGate 1800F



天井に設置されたアクセスポイント



コアスイッチ群には、フォーティネットのグループ企業である アラクサラネットワーク製のAX8600S、AX3660Sが導入されている。

ルチャネルという利点があったが、Wi-Fi 6ではネットワーク性能がさらに高まると期待できた。もちろん、運用しやすく稼働信頼性を確保でき、かつコストパフォーマンスに優れている必要もある。これらの条件を満たしたのがFortiAPとコントローラとしてのFortiGateの組み合わせだった。

「Wi-Fi 6と名前が付いていても、製品によってかなり性能差があります。レイテンシーが低いか、通信は安定しているか、コアスペックも含め全体の性能が出るかといった事柄を検証、比較していくと、フォーティネット以外の製品は選べませんでした」と鳥飼氏は述べた。

これまで同様の止まらないネットワークを実現し、セキュリティを確保していく上でもう一つ欠かせない要件が管理性だ。「コントローラ側から接続端末の情報を確認して可視化でき、十分に制御できることも特徴でした。また、機器から出てく

るsyslogを収集し、セキュリティ装置で情報を統合してセキュリティアラートを出せることも考慮しました」（鳥飼氏）

こうして得た情報を元に個別の接続を承認し、ある条件を満たさない端末をネットワークから隔離したり、特定の通信を止めるといった制御を実現するために「FortiNAC」も採用し、FortiGateと連携させることにした。アクセスポイントやスイッチ単位ではなく、個々の端末単位で制御できるため、真の意味でマイクロセグメンテーションを実現できることを評価した。

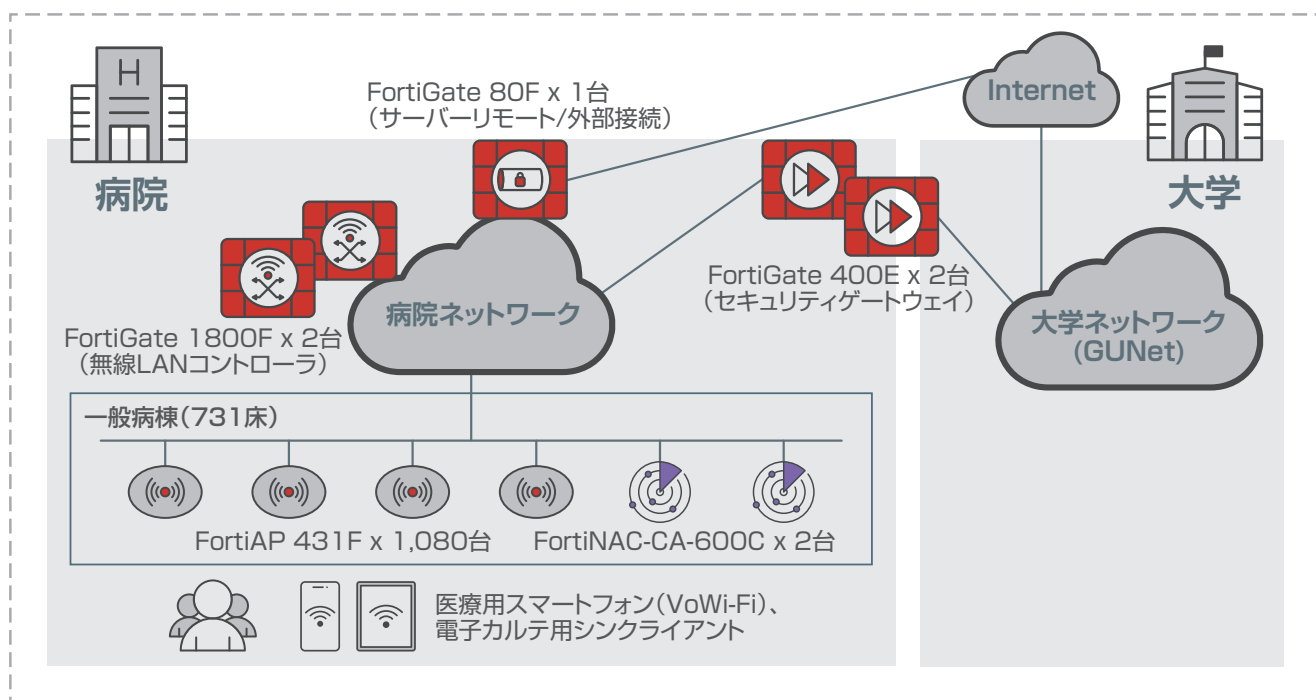
病院のシステムには動かし続けることが求められる。もしトラブルやサイバー攻撃が発生しても、ネットワークすべてを止めてしまうような乱暴な対応はできない。「効果的に範囲を限定して止める能力を持っているかがポイントでした。病院の機能を生かしながら安全を担保するという二つの要素を同時に満たすために、

FTTDのようなネットワークポロジの上でFortiNACを入れ、マイクロセグメンテーションを導入する必要がありました」（鳥飼氏）

待ち時間を大幅に短縮し、障害時の管理工数も削減

群大病院は、2015年の更改時に構築したネットワークポロジを踏襲した上で、1000台以上のFortiAP 431Fiに加え、FortiGateやFortiNACといったソリューションを導入し、レスポンスと運用性、セキュリティのさらなる改善を図った。前回の更改を通してネットワークレスポンスが向上すると業務がどれだけ快適になるかを実感した現場の医療者らも、この方針を支持した。

新ネットワークでは、Wi-Fi 6対応のアクセスポイントを経由し、これまで同様10Gbpsの光回線でアップリンクを構成している。またVLANを活用して医療系ネットワークと学術用ネットワークを一台に集



約しつつ、学術系で発生した大量のデータのダウンロードが医療系の通信に影響を及ぼさないようQoS制御を実施する仕組みも踏襲し、無駄を省きつつ、医療業務をつつがなく継続できる環境を実現した。

FortiAP 431Fでは、ビットレートがこれまでの4倍程度に向上した。「速度の不足に関する声は特に聞こえておらず、スムーズに接続できています」(鳥飼氏)。以前は、音声通話の品質や電子カルテの立ち上げ時間に関するクレームの声もあったが、これらも大きく改善された。「これまで10秒かかっていた電子カルテの待ち時間が2~3秒に短縮されると、一日で5分、10分といった時間が節約できます。群大病院には約2,000人ももの職員がいることを考えると、年間で何億円もの人件費を浮かせるのと同じ効果が得られます」(鳥飼氏)

ネットワークのレスポンス向上は、患者に提供する医療の質の向上に

も寄与するという。「医療は知的作業であるためストレスに弱く、コンピュータがスムーズに回答してくれないと、次にどうするのが思い出せなくなってしまうこともあります。コンピュータを待っている時間は誰の得にもなりません」(鳥飼氏)

また、元々のネットワークポロジも相まって、当初から重視していた可視性も確保できている。「コントローラやアクセスポイントの状態を、リモートから手元で把握できるようになっています。どのアクセスポイントがダウンしているのか、通信負荷が高いのかといった事柄をモニタリングできるため、万一トラブルがあった時の原因特定に役立ち、トラブルシュートまでの時間を短縮化できています」(鳥飼氏)

稼働信頼性の観点からは、極力ベンダーを統一することで管理工数を減らし、サービスレベルを高めるといったメリットにつながると考えている。その場その場で異なるベンダー

の機器を導入していった場合、初期コストは抑えられるかもしれない。だが、どのような機器も故障とは無縁ではない。もしトラブルが発生すると問題の発生場所を特定し、復旧するまでに多くの工数と時間がかかり、医療業務に影響を及ぼしかねない。

「適材適所で機器を選定でき、チューニングできる能力があれば、異なるベンダーの製品を組み合わせることも可能でしょう。ただ、セットでそろえていく方が、同じ管理ツールを利用でき、管理工数が減るメリットがあると思います」(鳥飼氏)

ネットワークの稼働信頼性向上により、わざわざ新たなシステムを導入したり、ワークフローを組み替えるといった手間をかけなくても時間を創出でき、その分を医療DXにつなげることも可能となる。「医療DXに取り組みたくても、目の前のトラブルに追われてそこまで手が回らない病院もあると聞いています。稼働信

頼性を上げることで、医療DXに取り組む余力も生まれると思います」と鳥飼氏は語った。

さらに、医療分野でネットワーク機器等の脆弱性が悪用されたランサムウェア被害が大きく報道されていることについては、「攻撃者は同じ手法で侵入できるものがたくさんある方が効率がいいため、シェアの高い製品を狙ってきます。つまり、シェアのある製品の方が脆弱性報告が出やすい傾向があります」（鳥飼氏）と受け止めている。脆弱性の存在しない機器があり得ない以上、どこか一つが破られても他の部分でカバーする多層防御の考え方を取り入れるとともに、厚生労働省の「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」で明示された医療機関の管理者責任の一環として、設定の誤りや脆弱性をチェックし、修正していく仕組み作りに力を入れるべきだとした。

なお群大病院は2022年12月に、厚生労働省によるサイバーセキュリティの外部監査を受けており、オンプレミス主体の医療機関としては

トップクラスのサイバーセキュリティ対策を実施しているという評価を受けた。「フォーティネットもそのセキュリティの一端を担っていると認識しています」（齋藤氏）

院内Web化も並行して進め、医療DXを着実に推進

医療業界では今、Webを介し、異なる医療機関や施設の間で診療データを連携できるようにするための標準規格として「HL7 FHIR」が策定され、電子カルテ情報の標準化も進んでいる。

群大病院はこうした動きをにらみ、ネットワークインフラの整備と並行して院内システムのWeb化を進めてきた。REST APIを活用し、さまざまなシステムが柔軟に接続できる環境を目指している。院内Web化は、いわゆるゼロトラストセキュリティの考え方に沿ってきめ細かで強固な認証を組み合わせることで、セキュリティ強化との親和性も高いと捉えている。

また8年後に病棟の建て替えを控えることもあり、さまざまな医療機

器やセンサー、ロボットを組み合わせたスマートホスピタル化なども視野に入れている。「さまざまな情報を収集し、AIで解析しようとする、トラフィックは急激に増加します。こうした分散コンピューティングにも耐えるには、ネットワークに求められる性能ももう一桁、二桁高まるでしょう」（鳥飼氏）

そうした要請に応えつつ、患者サービスの向上と医療安全の担保、セキュリティの確保といったさまざまなニーズに応えながら、医療DXを進めていく。

「一連の取り組みは一過性の話ではなく、いきなり実現できるものではありません。可用性と機密性と完全性という多面的な要求に応えられるよう、シンプルで長期的に使えるネットワークをきちんとデザインすることが重要です」（鳥飼氏）。並行して、院内のさまざまな要望をくみ取ってコンセプトを立て、実現できる人材を少しずつ育てていくことも重要であり、腰を据えて五年、十年単位で取り組んでいく計画だ。



FORTINET

フォーティネットジャパン合同会社

〒106-0032

東京都港区六本木 7-7-7

Tri-Seven Roppongi 9 階

www.fortinet.com/jp/contact

お問い合わせ