導入事例

群馬大学医学部附属病院 様

CASE STUDY

サイバー攻撃対策から運用の効率化まで “止まらない病院システム”に必要な医療グレードのネットワークとは

2015年のシステム更新において、コアスイッチと端末を約1,300本の光ファイバで直接つなぐ「FTTD」を導入し、高速レスポンスを実現した群馬大学医学部附属病院（以下、群馬大学病院）。それから7年後の2022年9月、同病院は新たな病院システムを稼働。そこにアラクサラネットワークス（以下、アラクサラ）のネットワーク・マネジメント製品「AX-Network-Manager（AX-NM）」とネットワーク可視化・異常検知ソリューション「AX-Network-Visualization（AX-NV）」を導入した。その目的は、高度化するサイバー攻撃に対応するとともに、運用を効率化し「時間創出」を実現するためだったという。今回は、“止まらない病院システム”に求められる医療グレードのネットワークとは何かについて、同病院 システム統合センターの鳥飼幸太氏に話をうかがった。

患者の命を守るために 必要不可欠な “止まらない病院システム”

――群馬大学病院は2015年のシステム更改によりネットワーク統合を実現し、強固なインフラを構築しました。そして2022年9月に稼働した新たな病院システムでは、ネットワーク構成に大きな変更はなかったと伺っていますが、ポイントはどこにあるのでしょうか。

鳥飼　新システムでは、サイバーセキュリティ対策の強化と運用の最適化に向けて、AX-NMとAX-NVを導入しました。また、“止まらない病院システム”を目指し、これまで物理サーバーで運用していたシステムを仮想統合し可用性を高め、障害発生時の稼働継続を実現しました。さらに、ネットワークを仮想化し、セキュリティサービスと組み合わせたサイバー攻撃対策も実装しています。

――ここまでインフラ統合を徹底して実現した病院はなかなかないように思います。そのねらいはどこにあるのでしょう。

鳥飼　病院システムを止めないことにあります。多くの病院では、システムを更新するたびに「継ぎ足し」でネットワークを強化してきたため、機器同士が相互につながるメッシュ型トポロジーで構成されていますが、結果として構成が複雑になり、パフォーマンスの低下が見られたり、障害時の切り分けに時間がかかったりしています。また、サイバー攻撃を受けた際も、攻撃対象が多くなるため、システムダウンの確率が高くなってしまうのです。よって、障害やサイバー攻撃による影響を最小化したいなら、ネットワークを統合し障害発生の原因や攻撃のターゲットを減らすことが重要です。

そしてセキュリティレベルを高める際には、ネットワークの構成単位を最小化する「マイクロセグメンテーション」が有効です。細分化したセグメントの経路だけをブロックすることで、他のセグメントに影響を与えることなく、被害の拡散を防ぐことができます。この点からすると、当院が2015年のシステム更新でFTTDを導入し、約1300本の光ファイバでコアスイッチと端末を直結したことは、レスポンスや可用性の向上だけでなく、サイバー攻撃対策としても効果的だったといえるでしょう。

企業概要

群馬大学
GUNMA UNIVERSITY

About　群馬大学医学部附属病院

1943年、前橋医学専門学校の附属施設として設置される。現在では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プター活動において、セキュリティ領域の幹事を務めている。
https://hospital.med.gunma-u.ac.jp/

CASE STUDY

医療グレードのネットワークに求められる稼働信頼性の高さを評価し、アラクサラ製品を採用しました

――なぜ“止まらない病院システム”が必要なのでしょうか。

鳥飼　患者さんの命を守るためには必要不可欠だからです。もしシステムが止まり、トラブル対応に忙殺されるようになれば、診療は続けられなくなります。また、ランサムウェアなどのサイバー攻撃を受けた場合、億単位の被害が出る可能性もあり、病院の経営危機に直結します。だからこそ可用性を高めることが重要なのです。

――確かに最近、病院がサイバー攻撃のターゲットになることが増えています。どこの病院も他人事ではないですね。

鳥飼　OECDの情報セキュリティガイドラインでは、情報セキュリティは「機密性」(Confidentiality)、「完全性」(Integrity)、「可用性」(Availability) の3要素からなると定義し、それぞれの頭文字からCIAと呼んでいます。この3要素の中に「可用性」が含まれていることに注目してください。しかし我が国の病院では、「機密性」を守ることだけを考えてセキュリティ対策を導入しているところがほとんどで、システムの二重化やネットワークインフラの強化といった「可用性」がセキュリティ的にも重要だという意識が薄いのです。こうした状況でサイバー攻撃を受ければ、あちこちで火の手が上がり、復旧までにかなりの時間を要することになります。

――群馬大学病院では、何名でシステムやネットワークの管理運用をされているのですか。

鳥飼　システム統合センターは教員3名と医療情報係7名で構成されており、実際に運用を担当しているのは医療情報係の7名です。今のところトラブルが発生することはほとんどないため、トラブルシューティングの負荷も少なく、診療レベルの向上に向けたサポートの提供に集中できています。これだけの規模のシステムやネットワークに少人数で対応できているのは、トラブルの頻度が少なく、またトラブルが起きたとしても速やかに復旧できるからです。迅速なインシデントレスポンスは、日々のシステム運用だけでなく、サイバー攻撃など突発的なトラブルにも有効です。

――群馬大学病院は災害拠点病院に指定されています。そうなると、災害時にも“止まらない病院システム”が求められますね。

鳥飼　災害によってシステムが止まってしまえば、診療もままならなくなります。それゆえ電子カルテシステムとネットワークの稼働信頼性は重要です。たとえば2011年の東日本大震災の際に計画停電が実施されましたが、私たちは自家発電機を使うことでこれを乗り切りました。また、停電対策という意味では、コアスイッチと端末を直接つなぐFTTDを採用しています。これなら間にスイッチが介在しないため、末端の光変換の部分を無停電化しておけば、停電時に使えなくなるリスクもありません。

――ここまでのお話をまとめると、日常のトラブルやサイバー攻撃、災害への対応にはいずれも“止まらない病院システム”が必要ということですね。

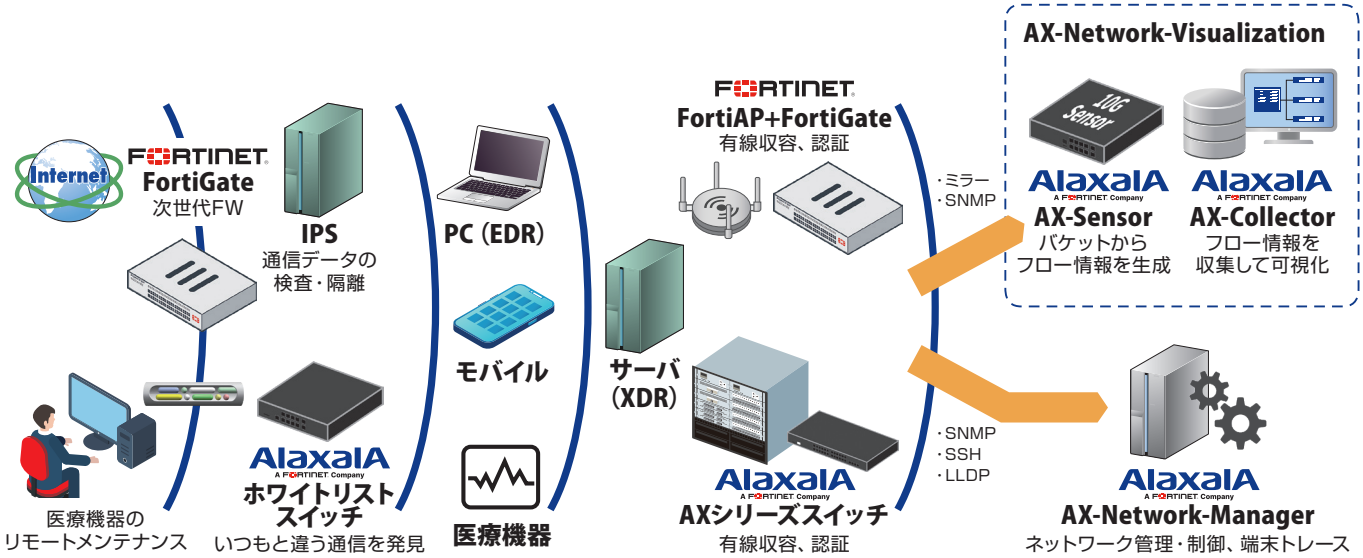
「医療DXとは時間創出である」トラブルを減らすためにもネットワークのシンプル化を

――ところで、近頃では医療分野にもDX導入の動きが出てきているようですが、この点についてはどうお考えでしょうか。

鳥飼　近年、当院では「時間創出」をキーワードに医療システムの整備を進めています。トラブルが減れば、運用担当者はその時間を使ってサービスの向上に注力することができますし、安全な医療の提供に貢献していることを実感しながら働くことができます。つまり、「医療DXとは時間創出である」ということです。

――トラブルを減らすためにはどうすればよ

医療グレードのネットワークセキュリティを実現する多層防御のイメージ



いのでしょうか。

鳥飼　そのためにも資産管理を徹底すること、具体的にはネットワーク構成図をいつでも取り出せるよう整備することが重要です。厚生労働省は2023年3月31日付で「医療機関における医療機器のサイバーセキュリティ確保のための手引書」という通知を発出し、その中で「医療機関は医療情報システムや医療機器がどのようなネットワークを構成し、接続されているかを視覚化したネットワーク構成図を作成すること」としています。現時点では手引書の段階ですが、いずれはガイドラインとして義務化される可能性があります。これに対応するためにも、まずはネットワーク構成図を作成し、院内のネットワークの状態や接続体系を把握することから始める必要があります。

ただし、ネットワーク構成図を作成するだけでは十分ではありません。それをもとに不要なスイッチなどの構成要素を削減し、ネットワークをシンプル化していきましょう。資産の数が少なければ運用管理は楽になりますし、サイバー攻撃からも守りやすくなります。この際、できれば従来のメッシュ型トポロジーから集約型トポロジーに変えて統合することが望ましいと思います。これにより、日常運用におけるトラブルシューティングの負荷が軽減され、サイバー攻撃を受けた際の影響を最小化するマイクロセグメンテーションも可能になります。当院の場合、FTTDでコアスイッチとフロアスイッチを直結したことにより、管理する資産を大幅に減らすことができました。また、光ファイバは25年近くの寿命があり、通電することもないため、重点管理対象から除外することができ、管理面が圧倒的に楽になりました。

医療グレードのネットワークに求められる稼働信頼性の高さを評価

――今回の更改では、前回に引き続きアラクサラ製品を導入いただきましたが、これらの採用の理由はどこにあるのでしょうか。

鳥飼　医療グレードのネットワークに求められる「稼働信頼性」の高さが一番です。コアスイッチに関しては、前回の導入からの7年間で一度も故障したことがなく、ハードウェアの信頼性の高さは折り紙付きです。その上で、壊れたとしてもサービスが停止しないよう二重化、冗長化ができているため安心して使うことができます。

また、今回あらたに導入したAX-NMですが、マルチベンダーに対応し、他社のソリューションと組み合わせて利用できるという点において、アッセンブリーレベルの高さを感じます。トータルでアッセンブルされたものについても稼働信頼性が高いんですね。ネットワークでトラブルが発生した際、アラクサラ製品以外についてもトラブルシューティングに対応可能なので、結果的にダウンタイムの短縮と稼働時間の長期化につながっています。

――そのAX-NMとAX-NVですが、導入の目的はなんでしょうか。

鳥飼　ネットワークのセキュリティ状態を可視化するために導入しました。インシデントレスポンスにおいては、侵入されることを前提に考え、早期検知によって撃退することがポイント

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
准教授 博士（工学）　医学物理士
鳥飼 幸太 氏

となります。両製品があれば、マルウェアなどが内部に侵入してきた際、何が起きたか把握することが可能です。またセキュリティ面以外にも、ネットワーク機器の管理や障害箇所の発見にも効果的です。

――新システムにおいて、アラクサラのソリューションを用いて実現したことをお聞かせください。

鳥飼　今回の導入で実現したセキュリティ対策のポイントは、複数の防御層を用いた「多層防御」を実現したことです。セキュリティチェックのポイントを複数用意することで、一か所の防御層が脆弱性を突かれたとしても、第2、第

群馬大学医学部附属病院様

3の防御層によって迅速に発見・対応することが可能となります。こうした対策を施すことで、ランサムウェアなどによる被害を受けた際に早期対処したり、短時間で医療サービスを復旧したりすることが可能になります。

――具体的にはどのように構成されているのでしょうか。

鳥飼　図のように、外部と内部の境界にはFortinetの次世代FW（FortiGate）を置き、第1層の防御層にIPS（不正侵入防御システム）とアラクサラのホワイトリストスイッチを置いています。ホワイトリストスイッチは、医療機器のリモートメンテナンス用で、あらかじめ登録した正常な通信フロー以外はアラートを上げます。第2層は端末や医療機器が置かれている層で、NDR（Network Detection and Response）によってネットワーク上の通信を監視し、不審な通信を検知します。第3層はXDR（Extended Detection and Response）による攻撃の検知・防御のほか、有線端末はアラクサラのAXシリーズスイッチで、無線端末はFortinetのFortiAPとFortiGateによるネットワーク認証を行っています。

そして、第4層の防御層に採用しているのがAX-NMとAX-NVです。AX-NMでは、ネットワーク機器から各種情報を収集し、機器/回線/端末の状態をグラフィカルに表示することで、トポロジーの把握や端末の追跡に活用します。AX-NVではAX-Sensorでミラーデータを各種フロー情報に加工し、AX-Collectorでフローの可視化と監視を行います。

なお、当病院では複数メーカーの製品を組み合わせて多層防御を実現していますが、第1層から第4層まで、アラクサラ製品とFortinet製品が随所で貢献しています。

――アラクサラの技術力についてはどう感じていますか。

鳥飼　一般的に、私たちがベンダーを変えたくなるのはトラブルが頻発し、原因の究明が進まないときです。短時間でトラブル対応に当たるためには、根本的な原因を推察できる、質の高いエンジニアが揃っていることが不可欠ですが、この点、アラクサラは個々のエンジニアの技術力が非常に高いですね。会社としても、自社製品をよく理解したエンジニアを積極的に育成していこうという意思を感じます。トラブル発生時に業務復旧させるまでの時間を短くすることは、医療グレードのネットワークには必要不可欠な要素ですが、アラクサラが後ろ盾にいることは非常に心強いと感じています。

Node-REDを活用したセキュリティ層の作り込みや医療DX、オートメーションコントロールの推進を検討

――最後に、将来の展望についてお聞かせください。

鳥飼　近々で実施したいこととしては、セキュリティ層の作り込みがあります。セキュリティ面でトラブルが起きたり、何らかのアラートを検知したりした際、それを管理者に通知する仕組みをIoTアプリやAPI開発向けのローコードプログラミング開発ツールであるNode-RED（ノード・レッド）を使って開発し、統合していく予定です。

具体的には、医療的な通信を制御する部分と、サイバーセキュリティを制御する部分を同じ要素として構成するというものです。例えば、診療科の要望で病棟にWebカメラを設置し、許可された通信のみをオープンにする際には、REST（REpresentational State Transfer）を使ってWebサーバーを制御する環境をNode-REDで整備します。これにより、Webカメラの設置台数が増えても、セキュリティを崩すことなくネットワークをコントロールすることが可能になります。また、追加のリクエストに対して短時間に対応できるようにすることで、ネットワークの可用性の向上や、運用時の時間創出を実現します。この点、AX-NMがRESTをコントロールする機能を備えているのはメリットですね。

――その他には何かございますか。

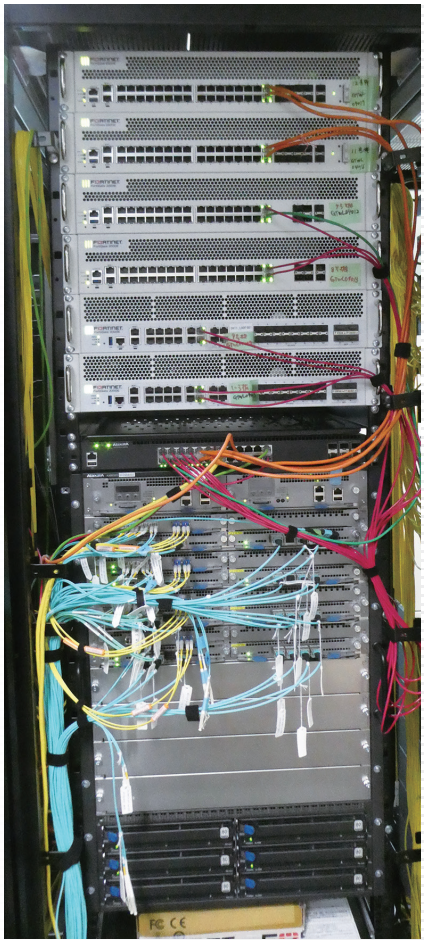
鳥飼　医療DXとしてのFHIR（Web通信）への取り組みや、オートメーションコントロールの実現を考えています。FHIRにおいてもRESTに対応していることが重要で、異なる拠点間やサーバー間のセキュリティ強化、運用の効率化による時間創出に貢献することができます。オートメーションコントロールでは、人が認識しやすいスクリプト言語に置き換えて自動化をやりやすくすることで、運用担当者はより創造性の高い業務にシフトできると考えています。

――最後にアラクサラへの期待をお聞かせください。

鳥飼　医療グレードのネットワークの実現に向けて、さらに技術力を高めていっていただけるとありがたいです。また、病院にふさわしいネットワークトポロジーの浸透を目指し、業界内でリーダーシップを発揮してもらいたいですね。

――ありがとうございました。

コアスイッチ群（AX8600S、AX3660S）と端末を直接接続するFTTD構成



システム全体を支えるAX8600Sとセキュリティを担うFortiGate

アラクサラ ネットワークス株式会社
〒212-0058
神奈川県川崎市幸区鹿島田1丁目1番2号 新川崎三井ビル西棟13階
URL：https://www.alaxala.com/