導入事例

つるぎ町立半田病院

＜医療セキュリティ＞多層的な対策で院内ITを再構築。ランサムウェア被害を教訓にした再出発の軌跡をたどる

つるぎ町立半田病院は2021年にランサムウェアの被害を受けた教訓を踏まえ、アライドテレシスの支援のもとで外部からの不正侵入対策に加え、内部拡散の抑止、リモート接続の集約管理、アクセス権限の分離、ログの可視化といった多層的なセキュリティ強化を段階的に実施。院内ITインフラの防御力と運用体制の信頼性を飛躍的に向上させている。

（左から）
つるぎ町立半田病院
システム管理課
課長
山本 高也氏

アライドテレシス株式会社
四国支社
アシスタントマネージャー
矢田 拓也氏

つるぎ町立半田病院

安心と信頼、そして　地域と共に歩む

課 題

- セキュリティ体制の脆弱性
- 通信状況の把握と監視体制の見直し

採用ポイント

- 対応能力とスキル、適切なアドバイスに対する信頼感
- 既存環境に影響しない対策案

効 果

- 段階的な多層防御でセキュリティ強化
- 信頼性の高いネットワーク環境を実現

地域医療を支える病院、ITインフラを刷新し再出発

つるぎ町立半田病院は、徳島県西部の山間部に位置し、地域の中核医療機関として幅広い診療科を備えている。産婦人科や小児科の常勤体制を維持し、各種検診にも力を入れるとともに、予防医療を通じて住民の健康を支えてきた。「他県の病院も視察して得た情報などをもとに2025年、検診室をリニューアルしました。検診の受診者が増えれば予防にもつながり、何かあった際にもすぐ対応できます」と語るのは、つるぎ町立半田病院　システム管理課　課長の山本 高也氏。

同院は2021年10月、ランサムウェアの被害を受け、電子カルテを含む情報システムが全面停止。復旧までに約2カ月を要し、病院機能は深刻な影響を受けた。以降、外部有識者の助言や公的機関のガイドラインを参考に、情報セキュリティの抜本的な見直しを開始。ネットワーク監視やウイルス対策の強化、バックアップ体制の再構築に加え、アライドテレシスの支援のもとで段階的にITインフラの再設計を進めた。

アライドテレシスを中心に段階的な再設計

半田病院は以前からネットワーク機器を導入するなどアライドテレシスとは付き合いがあった。今回セキュリティを強化するにあたり、複数ベンダーによる複雑なネットワークを構築するのではなく、アライドテレシスを中心にネットワークを一本化することとした。「付き合いが長いこともありますが、対応能力とスキルに対する評価、アドバイスも適切で信頼できるベンダーであることが理由です。有識者会議での賛成も得て決定しました」と山本氏。

まずフェーズ1では、職員が利用する有線インターネット接続に対し、新たなファイアウォールを導入。本装置はアンチウイルスなどのUTM機能を有しており、外部との通信をリアルタイムで監視・制御できる構成である。加えて、侵入経路となった回線は解約し、既存のリモート回線や患者インターネット回線を転用。固定IPの変更もあわせて行うことで、コストを抑えつつ、セキュリティの刷新を実現した。これによりマルウェアの侵入リスクを低減し、病院業務における外部脅威への対応力が向上する。

フェーズ2では、院内約50台のHUBを認証スイッチに刷新し、MAC認証から802.1X認証へ移行。Active Directoryによる認証基盤を整え、802.1X非対応のプリンタはMAC認証で接続を許可している。さらにx930シリーズをAMFマスターとして導入し、既存スイッチの一元管理を実現。VST-APLシリーズによる運用効率の向上とファームウェアの更新も行われた。

また全館Wi-Fi対応となり、「館内どこにいてもどのフロアでも安定してWi-Fiが使えるようになりました」と山本氏は評価する。

さらにサーバー用とプリンタ用のVLANを新設し、機能単位でセグメントを分離することで、内部拡散による被害拡大リスクを抑制。「多要素認証の構築にも積極的に関わってもらいました」と山本氏。すべての電子カルテ用端末に対して認証システムの導入と同時にウイルス対策ソフトをインストールしている。

リモート接続の一本化と認証・監視の強化

フェーズ3では、外部からのリモートアクセスを全面的に見直し、従来複数かつ複数方式であったリモート回線をIPsec VPN方式に一本化するとともに、多要素認証によりセキュリティを向上。ファイアウォールを通じた接続に送信元制限を設け、サーバーからの外部通信は必要最小限な接続とし、不要な外部接続を遮断する構成とした。リモート接続アカウントもすべて再登録し、固定IP回線により接続経路を厳密に制御。「リモート回線を集約して外部からの脅威を大幅に減少させました」と山本氏。外部アクセスは仮想基盤上に構築した中継サーバーを経由させ、その上で各社ベンダーごとにOSやIPアドレスを分離した仮想サーバーを用意。これによりアクセス権限を明確に分離し、院内ネットワークへの接続経路を一本化している。中継サーバー上では証跡管理システムEkran（エクラン）を用いて操作ログを映像でも取得し、ネットワーク機器のログはSyslogサーバーで保管。不正行為や誤操作の追跡性を高めた。

さらに端末の脆弱性管理を強化するため、Windows Updateを集中管理できるWSUS（ダブルサス）サーバーも新設。パッチ適用状況の把握と更新を徹底することでセキュリティの維持向上を図る。同時に脆弱性通知サービスにも加入し、脆弱性によるリスクを最小

限にする運用を行っている。

フェーズ4では、患者と職員それぞれのインターネット利用を用途別に明確化するため、通信構成を再設計。リモート接続用とは別に、インターネット専用として2台目のファイアウォールを新たに導入し、それぞれに異なるセキュリティポリシーを適用可能な体制とした。アクセスポイントではSSIDを分け、無線ネットワークも論理的に患者用と職員用に分離。これにより情報漏洩リスクを抑えつつ、利便性を損なわない構成を実現した。

さらに既存スイッチへのVLAN設定を追加し、ネットワークゾーン単位での通信制御を精緻化。外部向け通信の可視化と不審なアクセスの早期検知を可能とするため、インターネット通信に特化したSyslogサーバーも新たに導入し、不審なアクセスの早期検知体制を整備した。

BCPと未来の医療構想を支えるIT基盤

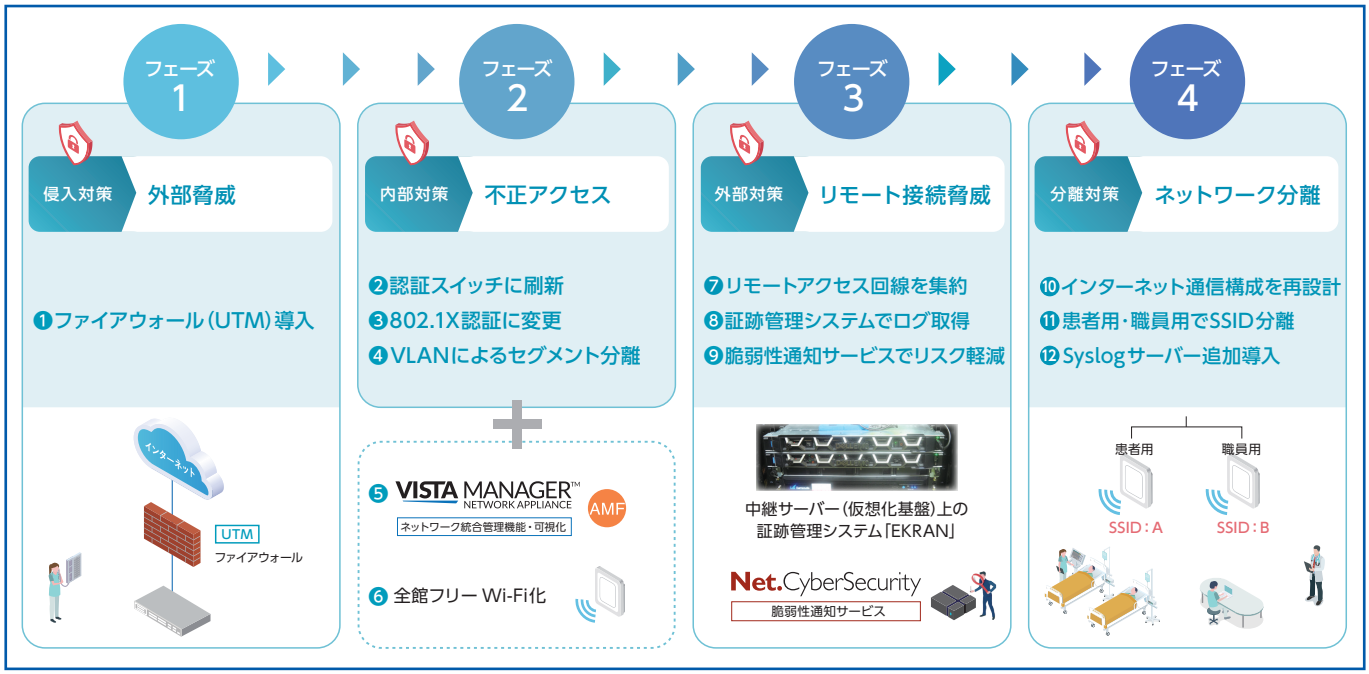
導入した各種セキュリティ対策は、いずれも大きなトラブルなく安定稼働しており、以降ウイルス感染や外部攻撃といった重大な被害も発生していない。日々の運用においても信頼性の高い環境が維持されている。

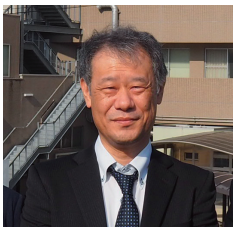
さらに事業継続計画（BCP）に対応するため、バックアップ環境も抜本的に見直されている。HIS系ネットワークとは完全に分離されたNASを構築し、そこにバックアップファイルを保管。システム障害が発生して復旧に時間がかかる場合でも、本番系とは別の安全な経路を使ってバックアップデータを参照できる仕組みが整備された。院内インターネット回線を経由し、ルーターなどを介して接続された専用PCから、診療情報にオフラインでアクセスできる体制となっている。これにより障害発生時でも診療の継続が可能となり、患者への影響を最小限に抑えることができる。

今後の展望について山本氏は次のように語る。「高齢化や人口減少が進む中、患者さんに来てもらうのではなく、私たちが出向く“出張型医療”が必要だと感じています。たとえばアライドテレシスの協力のもと、遠隔診療やドローンによる薬の配送など、ネットワークを活用した新しい医療提供の形が実現できれば面白いですね」。また地域の高齢者はスマートフォンを所持していても通信環境が不十分なケースが多く、そうした地域で医療を支えるには行政の支援も欠かせない。「車やバスの本数が減る中、移動に頼らず、自宅で検診や診療を受けられる体制が整えば、町全体の健康維持にもつながると考えています」。

アライドテレシスは今後も、つるぎ町立半田病院のネットワークインフラとセキュリティ対策のさらなる高度化に向けて、製品・技術・サポートを通じた継続的な支援を行っていく。

多層防御による段階的なセキュリティ対策





つるぎ町立半田病院
システム管理課
課長
山本 高也氏

お客様プロフィール

■つるぎ町立半田病院

開　　設：1949年
管 理 者：病院事業管理者　須藤 泰史
病 床 数：120床

徳島県美馬郡つるぎ町に位置する町内唯一の公立病院。1949年の開設以来、地域医療の中核を担っている。一般病床120床を有し、内科、外科、産婦人科、小児科など多岐にわたる診療科を備えている。
https://www.handa-hospital.jp/

ネットワーク構築などのご質問やご相談、その他のお問い合わせ
https://www.allied-telesis.co.jp/contact/

アライドテレシス株式会社　〒141-0031 東京都品川区西五反田7-21-11 第2TOCビル　https://www.allied-telesis.co.jp/