導入事例

社会医療法人ジャパンメディカルアライアンス 海老名総合病院

Allied Telesis

「サイバー攻撃は侵入を前提とした対策が必要」三層防御からリテラシー向上まで計画的なセキュリティ対策を全面支援

ランサムウェアをはじめとしたマルウェアによる被害は依然として増加し続けており、とくに医療機関をターゲットにした攻撃は後を絶たない。情報漏えいや業務停止に繋がるこれらサイバー攻撃へのセキュリティ対策は喫緊の課題だ。海老名総合病院はアライドテレシスのネットワークを基盤とした、ウィルス対策からネットワークセキュリティ、訓練メールまで幅広いセキュリティ対策を段階的に導入した。

右：アライドテレシス株式会社
執行役員 医療営業本部 本部長
木村 有司 氏

中央：アライドテレシス株式会社
ソリューションエンジニアリング本部
東京プロジェクトマネージメント部
プロジェクトマネージャー
川野 謙 氏

左：アライドテレシス株式会社
医療営業本部 医療営業部 マネージャー
新貝 達朗 氏

右：社会医療法人ジャパンメディカルアライアンス
経営企画本部 情報システム部
兼 業務部 情報システム管理課 係長
飯島 弘之 氏

左：社会医療法人ジャパンメディカルアライアンス
業務部 情報システム管理課
川井 夢子 氏

課題

- ネットワークのセキュリティ強化
- 病院主導でネットワークセキュリティの運用・改善を図る

採用ポイント

- トレンドマイクロ(DDI)×アライドテレシス(AMF-SEC)連携による脅威の検知と自動遮断
- 病院計画に沿った提案と段階的な検証・導入に際しての手厚いメーカーサポート

効果

- 診療部門が気付く前にIT部門が初動対応できるセキュリティ体制を実現
- 訓練メール実施による病院職員のセキュリティリテラシー向上

病院主導のネットワーク基盤を構築

社会医療法人ジャパンメディカルアライアンスが運営する海老名総合病院は、神奈川県海老名市の高度急性期病院。2023年5月には新棟西館をオープンさせ、手術支援ロボットなどの最新技術を取り入れた手術室や高度検査センターなど、医療体制をさらに強化している。

海老名総合病院では、AIを活用した来院前の問診や受診相談、オンライン診療など、新しい技術を活用した医療サービスも積極的に取り入れている。「法人の考え方として、より業務を効率化して、いかに患者様に質の高い医療サービスを提供できるかということに重きをおいているため、先進的な技術はどんどん取り入れています」と語るのは、社会医療法人ジャパンメディカルアライアンス 経営企画本部 情報システム部 兼 業務部 情報システム管理課 係長の飯島 弘之氏。

業務効率化を進める中では、ペーパーレスにも取り組み、成果を挙げているという。「目標値を設けてペーパーレスをはじめとした医療DXに積極的に取り組んでいます」と飯島氏。

また病院ネットワークの充実化も早くから進めており、2020年の更新時にはアライドテレシスのネットワークを採用。AMF（Autonomous Management Framework）や「AT-Vista Manager EX」によるネットワークの統合管理、AWC-CB（Channel Blanket）によるローミングレスの無線環境などを導入している。「ネットワークについては、ベンダー任せにはせず、病院主導での運用・保守を目指しています。例えば監視であれば、システムを共有して、平常時でもこちらから確認ができるようなチューニングをお願いしています」と飯島氏。

トレンドマイクロ(DDI)×アライドテレシス（AMF-SEC）連携で脅威の検知から対応までセキュリティを強化

海老名総合病院では、ネットワーク導入初期のパソコンが入り始めた頃からウィルス対策やファイアウォールなど、基本的なセキュリティ対策は実施してきた。ウィルス対策については、2020年にトレンドマイクロ社の「Trend Micro Apex One」に更改、アライドテレシスがサーバー更新などを支援している。

同時に2010年代から流行が始まったランサムウェアの被害が医療機関でも広がり、ウィルス対策だけなく、ネットワークでセキュリティを担保することが重要という認識が広がってきた。

海老名総合病院でも、そうしたランサムウェアによる医療機関の被害報道や、既存のブラックリスト方式ではゼロデイ攻撃が防げないこと、行政機関からの注意喚起、ファイアウォールやエンドポイントセキュリティの脆弱性情報などを受け、また在宅系訪問事業の効率化、モバイル機器活用拡大などを見据えて、ネットワークセキュリティを検討し始めた。飯島氏は、「ネットワークセキュリティの概念が出てきて、2019年頃には製品も数多く発表されました。そこで、どういった動きをするかなどを確認・検証するために、その中の一つであるトレンドマイクロ社の「Deep Discovery Inspector（DDI）」をトライアル導入しました」と語る。

アライドテレシスの支援のもと、DDIの性能に任せるのではなく、その挙動の詳細な検証を行っている。ベンダーのリモート環境における不正通信の検知やプロキシサーバー経由のリモート通信、悪質な広告、フィッシングサイトの接続・検知、C&Cサーバーへの接続の検知、クラウドストレージサービスの利用検知などを重点項目として、検証を進めた。

さらにDDIの脅威検知の仕組みなどを検証しながら、万一の際の対応・制御の部分についても検討を進め、SDN連携による遮断の検証も始めた。それがアライドテレシスの提案したAMF-SEC（Security）だ。DDIが脅威を検知すると、AMF-SECにより当該端末の通信を遮断して、脅威の拡散を防ぐ仕組みだ。DDI×AMF-SEC連携で検知から対応までの対策を担保する。

AMF-SECによる自動遮断と、導入後も含めたアライドテレシスの支援を評価

他のセキュリティソリューションも比較検討した結果、DDI×AMF-SEC連携による脅威検知と遮断の仕組みを導入することとした。

「DDIを選定したのは、AMF-SECと連携することで通信の自動遮断ができること、既存のネットワーク機器の入れ替えが発生しないこと、既存のエンドポイントセキュリティに影響しないことのほか、コストパフォーマンスや操作性、精度チューニングなども他のソリューションと比較して良かった点です。なにより導入後のアライドテレシスによるサポートや改善相談の対応が良かったと感じています」と飯島氏は言う。

実際の導入では、監視範囲やトラフィック上限を検証により適正に定めて、検知精度のチューニングを行い、検知時の動作や通知、対応を決め、また検知ログとセキュリティ対策の強化施策もあわせて進めた。

「脅威を高中低とレベル分けして、対応を設定していますが、自動遮断や警告通知までに至らないもの、ログに残っているだけの挙動の部分も重要で、毎月ログを精査して、どういった挙動、アラートが多いのかを検証しています」と飯島氏。

アライドテレシスは導入にあたり技術的支援も積極的に行っており、例えばSDN連携の部分で脅威レベルが低い場合でも検知して連携できるようにサポートしている。「今回のプロジェクト導入に関して、アライドテレシスには多大なるサポートと支援を受け、とても感謝しています。」と飯島氏は評価している。

病院職員のリテラシー向上に訓練メールを採用

DDI×AMF-SEC連携による脅威検知と遮断の仕組みが稼働して1年ほど経過しているが、使い勝手も良好だという。社会医療法人ジャパンメディカルアライアンス 業務部 情報システム管理課の川井 夢子氏は、「ひと目見ただけで直感的に操作できるインターフェイスで、自動遮断からの復旧操作も容易です。侵入され、感染が広がって大騒ぎになってからではなく、侵入される前の不正な挙動や通信を検知でき、検知した場合も即時に遮断できる点が良いと思います。運用部門も常に張り付いているわけではないので、自動的に遮断できるのは助かります」と言う。診療部門が気付く前に、IT部門が気付き、初動対応できること、これらの動きを可視化できたことを飯島氏も評価する。

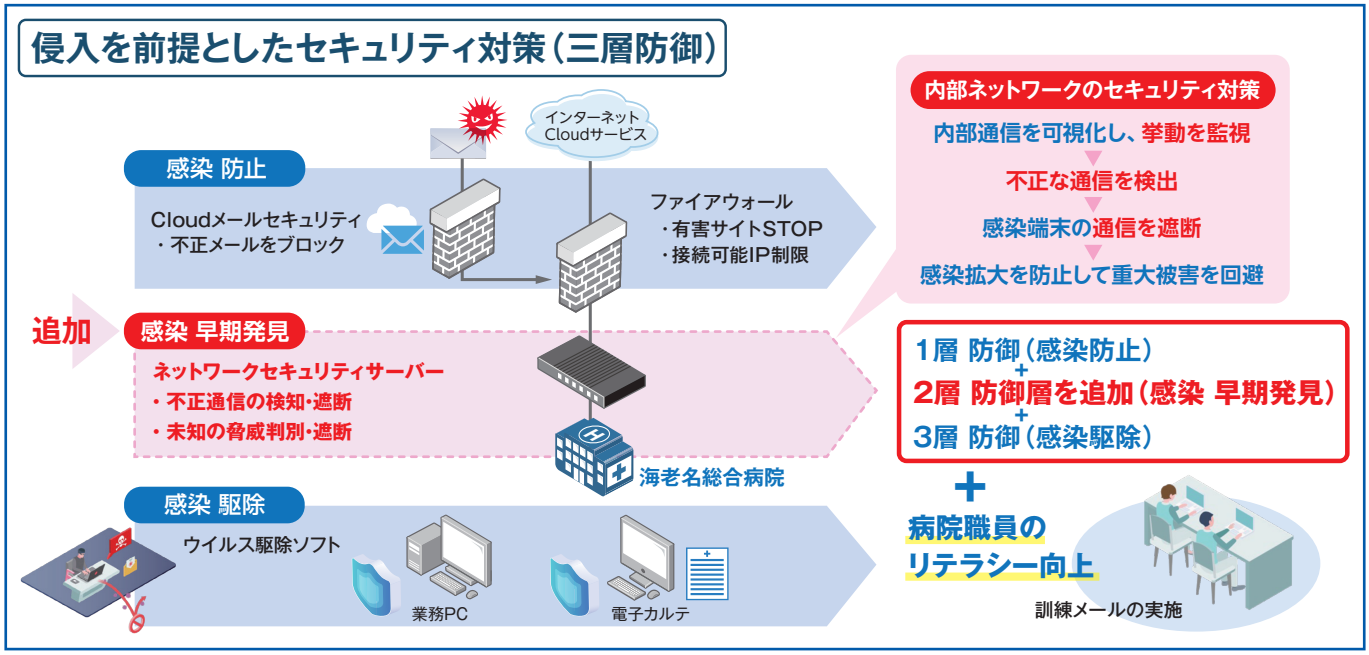
海老名総合病院では、毎月のログ精査、対応の検討の結果、病院職員のさらなるリテラシー向上が必要と考え、訓練メールを実施することとした。アライドテレシスが提案する「PenTestMail」は、フィッシング詐欺メールに対する体験型の訓練を容易に実現するサービスだ。「不正プログラムへの感染経路などを考えると、メール経由の攻撃は軽視できません。なりすましメールや本文のリンクアドレスを不用意にクリックしないなど、リテラシーを向上する必要があります。テスト時は全体の何%かはリンクアドレスをクリックするという結果になりましたが、回数を重ねるごとにその割合は減ることを実証できていますので、今後も続けていく予定です」と飯島氏。

アライドテレシスのネットワーク基盤をベースに、ウィルス対策やファイアウォールなどの基本的な対策から、DDI×AMF-SEC連携による脅威検知と遮断、さらにはログの精査、対応の強化、そして訓練メールの実施による職員のリテラシー向上まで、段階的に病院ネットワークのセキュリティを強化している海老名総合病院。こうした脅威への対策は終わらない。

「DDIのログから脆弱な部分を定期的に課題化して、その解決のためにセキュリティ対策の強化を計画・実施していきます。そうした計画に加え、法人理念の実現を推進するソリューションの導入を検討していきたい」と飯島氏は期待と展望を語った。

アライドテレシスはこれからもジャパンメディカルアライアンスおよび海老名総合病院のネットワークとセキュリティについて、製品や技術、サポートの提供を通じて、積極的に支援していく。

ネットワーク構成イメージ図



社会医療法人ジャパンメディカルアライアンス
経営企画本部 情報システム部 兼 業務部 情報システム管理課 係長
飯島 弘之氏

お客様プロフィール

■社会医療法人ジャパンメディカルアライアンス 海老名総合病院

所在地 ：神奈川県海老名市河原口1320
病床数 ：479床

「仁愛の心で地域の皆様とともに」を理念に、地域に根ざした病院でありつづけるため、24時間365日断らない救急医療の実現を目指す。仁愛の精神のもと、地域の皆様が安心できる医療を提供する、地域密着高度急性期病院。

http://ebina.jinai.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/