社会福祉法人 恩賜財団 済生会

「独立採算」という組織の課題を克服
異なるIT環境を持つ約80病院のセキュリティを統合監視

全国 85 の病院からなる公的病院グループの済生会。各病院は独立採算で運営される体制となっており、IT 環境も病院ごとに独立しています。この構造によって難しくなっていたのがセキュリティの強化です。グループ全体にシステム的な対策を一律に行うことが難しく、本部が行う対策は人的な支援が中心でした。その課題を解決したのが Cisco XDR による統合的なセキュリティ監視です。

社会福祉法人 恩賜財団 済生会

本部事務局
東京都港区三田 1-4-28
三田国際ビルヂング 21 階

開設年
1911 年

主な施設
病院 85 ／診療所 20 ／介護老人保健施設 28 ／
特別養護老人ホーム 54

貧困により医療を受けられない人々を救済するという明治天皇の想いを受けて設立された済生会。公的病院グループとして、経済的貧困だけでなく、様々な困窮状態にある人々を支援する「ソーシャルインクルージョン」を理念に掲げています。

課題

- 規模に関係なく医療機関を標的としたサイバー攻撃が相次いでいる
- グループの各病院は独立採算・個別 IT 環境が基本。本部主導で一律に対策することが困難
- ベンダーごとに構築したリモートアクセス環境など、他のセキュリティリスクへの対応も求められる

ソリューション

- 各病院のネットワーク機器からフローデータを収集し、Cisco XDR で統合的にセキュリティ監視を実施
- 医療従事者をライセンスカウント対象外とする Cisco XDR の医療機関向け特別オファーリングでコストを大幅に圧縮

結果

- 全国の病院を統合 SOC 基盤で監視。病院側の負担を最小限に抑えつつ的確なインシデントレスポンスを実現
- コストや人材面で対策が難しい中小病院も含めてセキュリティレベルを底上げ

今後

- Cisco Secure Access と Cisco Duo を活用し、各病院の保守ベンダーによるリモートアクセスを集約
- Splunk Cloud Platform を応用して医療機器の稼働可視化を検討
- AI などを活用して職員が患者・家族と向き合う時間の拡大を目指す

セキュアな環境のもと
AIやデータの活用に
積極的に挑戦したい

松原 了 氏

社会福祉法人恩賜財団 済生会
済生会保健・医療・福祉総合研究所
理事・所長代理 医学博士

課題

セキュリティリスクの高まりと対策の限界

近年、医療機関を標的としたサイバー攻撃が相次いでいます。長期にわたって診療継続困難に追い込まれた事例も少なくありません。医療機関のセキュリティ強化は、社会全体の喫緊の課題です。

「医療現場でもIT活用が進み、様々なデバイスやシステム、そしてデータがネットワークでつながるようになりました。そのことに比例してセキュリティリスクも増大しています。最新テクノロジーの価値を享受するためにも同時にセキュリティ対策に目を向けなければなりません。もはや医療機関の責務の1つです」と済生会の松原 了氏は指摘します。

かつては、攻撃の多くが大規模な施設を対象としていましたが、現在は多様な施設が攻撃を受けています。「攻撃を受けるのは大きな病院」という考えはもう通用しません。「そうした認識は業界全体に広がっており、日本中にある済生会の各病院でも経営陣やシステム担当者が危機意識を高めています」と済生会の髙橋 洋平氏は話します。

実際、各病院の担当者から「本部で何か対策を打ってくれないか」という相談も増えています。しかし、本部が動くには組織の構造的な限界がありました。

済生会の各病院は独立採算で運営されており、IT環境についても、電子カルテなどの選定、各システムやネットワークの構築、そして日々の運用までを各病院が個別に行うのが前提です。しかも100床以下の病院から数百床を超える病院まで、各病院の規模や状況は様々で、セキュリティにかけられるコストや専任担当者の有無などが大きく異なります。「各病院の状況が異なることから、本部側からシステム的な対策を一律に行うことが難しく、これまでは研修会を開催して情報を提供したり、インシデント対応マニュアルを整備して配布したり、人的な対応を中心に行ってきました」と髙橋氏は振り返ります。

ソリューション

有効な対策を提案できたのはシスコだけ

とはいえ、これからのサイバー攻撃に対抗するには、人的な対応だけでは十分とは言えません。安全性だけでなく効率性の面でも、技術やシステムによる対策は不可欠です。済生会の環境に最適な解決策とは――。髙橋氏は様々な企業に相談しました。しかし、なかなか的を射た回答を得ることはできませんでした。例えば、近年、猛威を振るうランサムウェアのような悪質な脅威に対抗するためにEDR（Endpoint Detection and Response）を導入する企業や組織が増えていますが、済生会の分散したIT環境に同じソリューションを一斉に導入することは現実的ではありません。また、EDRは機器にエージェントをインストールする必要がありますが、医療機器の中には、それが行えないものも多数あります。

そのような状況の中、最適な提案をしたのがシスコでした。具体的に、シスコが提案したのは次のような対策です。

各病院のネットワーク機器から収集したフローデータは閉域網を経由し、新たに設けたデータセンターに集約。クラウド上のCisco XDRにて分析し、統合的なセキュリティ監視を行う。これなら各病院に新たに機器を置く必要がなく、ネットワーク機器がシスコ製品であっても他社製品であっても対応可能です。「導入に向けたスケジューリングや実際の作業もシスコ側で一括対応すると提案してくれました。本部主導の施策で済生会各病院のセキュリティの底上げを図るには、これしかないと感じました」と髙橋氏は言います。

コスト面でも、シスコのプログラムが大きく効きました。1つは、Cisco XDR独自のライセンス体系で、医療従事者（医師・看護師・技師など）をライセンスカウントの対象外とするというものです。「済生会の全職員を数えると数万人規模になりますが、そこから医療従事者を除くことができれば、ライセンスコストを約10分の1に圧縮できます」（髙橋氏）。

もう1つはEA（Enterprise Agreement）契約の活用です。EAは3～5年の単一契約でシスコ製品・サービスをまと

めて調達できる購入プログラムで、ボリュームディスカウントによるコスト削減に加え、契約期間中はライセンスを追加しやすい条件が設定されています。「本部で一括調達し、各病院に按分して年額で案内しています。コストの抑制と平準化につながり、各病院の負担額も計算しやすくなりました」と髙橋氏は続けます。

結果～今後

弱点を生まないために参加を義務化

済生会では、約 80 病院を複数のグループに分け、段階的に Cisco XDR の導入を進めています。グループ全体で統一されたセキュリティ水準を確保するため、本部主導で、この統合セキュリティ監視基盤への参加を義務化しました。「セキュリティ対策は、グループ全体で統一した水準を確保してはじめて意味を持ちます。一部の病院が対策を強化しても、脆弱な病院があれば、それが弱点になってしまう。そのことを伝え参加の理解を得ました」と髙橋氏は話します。

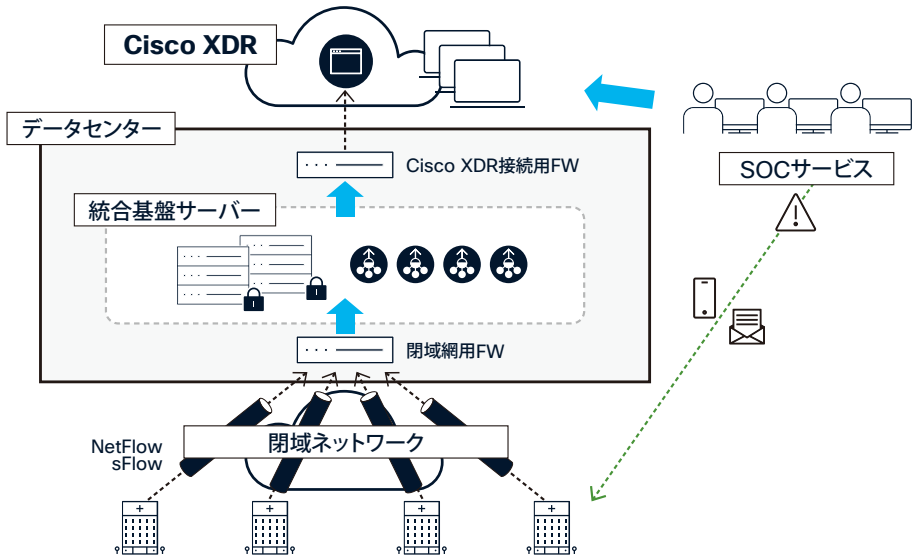
この “強制” は、現場から予想外の歓迎を受けました。特に専任の担当者を置くことが難しい病院では、対策の必要性は認識しながらも、限られた予算の中でどのような対策を講じるべきか判断が難しいという現実がありました。本部が最適解を定め、一斉に展開したことで各病院はスムーズに意思決定が行えたのです。

各病院のネットワークにおける機器の設定変更は、シスコとシスコのパートナーが連携して行いました。「各病院側と個別に打ち合わせを重ね、調整を行いながら進めてくれました。現地の状況を把握したり、日程を調整したりするためのコミュニケーションが大変だったと思いますが、とても丁寧に対応してくれ、安心して任せることができました。また、Cisco XDR の設計と構築も Cisco Professional Service を通じて、製品を熟知しているシスコのエンジニアが行ってくれるなど、私たちの事情を理解した上で最適な導入支援を提供してくれました」と髙橋氏は言います。

日常のセキュリティ監視は外部 SOC に委託

Cisco XDR は、各病院のコアスイッチから NetFlow などのフローデータを閉域網経由で収集し、AI や機械学習を

Cisco XDR によるセキュリティの統合監視



駆使してリアルタイムに脅威分析を実行。内部からの不審なデータ転送、通常とは異なる通信先へのアクセス、マルウェア感染やボットネット活動の兆候といった異常なふるまいを検知した場合は監視担当者にアラートを上げます。

済生会は、この Cisco XDR を中核に据えたセキュリティ監視を、外部 SOC に委託しています。「当初から SOC は外部委託する考えでした。分析と可視化の仕組みを整え、脅威を検知できても、分析結果を正確に判断し、適切な対処を打てる専門人材を各病院が確保するのは現実的ではないからです。緊急度の高いインシデントを検知した際は、外部 SOC から本部と該当病院の担当者に通知が届くことになっています」と髙橋氏は説明します。

構築した統合基盤を新しい取り組みに活かす

このように済生会は、Cisco XDR を活用して、日本中にある病院のセキュリティ監視を統合することに成功しました。現在は、そのために構築した閉域網と統合基盤を別の用途でも活用していく計画を立てています。

1 つ目は、リモートアクセスの集約です。現状、各病院の多くは保守ベンダーごとに個別のリモートアクセス環境を構築していますが、ランサムウェアの主要な侵入経路の 1 つが VPN 機器であることを踏まえ、Cisco Secure Access と Cisco Duo を活用し、整備した統合基盤上にリモートアクセス環境を集約することを考えています。「社会課題を解決するためにシスコが世界各国で展開しているカントリー・デジタル・アクセラレーション（CDA）を活用し、シスコと共に取り組んでいます。グループのリモートアクセス環境を一元管理できればセキュリティリスクをさらに低減できます」（髙橋氏）。

2 つ目は Splunk Cloud Platform によるデータ活用です。Cisco XDR が収集するフローデータは Splunk Cloud Platform で分析されていますが、それをセキュリティ以外の用途でも活用できないか、可能性を探っています。「各病院の医療機器の稼働状況を可視化して、過剰な機器調達の抑制につなげたり、グループ内での資産の有効活用につなげたりできないかと考えています」と髙橋氏は話します。

分散、独立採算という制約の中で、各病院のセキュリティ強化に成功した今回のプロジェクトは、医療グループにおける新たなセキュリティモデルを提示しています。すでに別の医療グループが済生会を参考に同様の取り組みを進めています。

「守りが固まったことで、これまで以上にデジタル活用に積極的に取り組める環境が整いました。AI を活用した業務の効率化や自動化を進めることで、医師をはじめとする職員は、患者さんやご家族に向き合う時間を増やせるかもしれない。各病院とも連携しながら、そうしたチャレンジを続けていきたいと思っています」と松原氏は最後に強調しました。

社会福祉法人恩賜財団 済生会
済生会保健・医療・福祉総合研究所
理事・所長代理 医学博士
松原 了 氏

社会福祉法人恩賜財団 済生会
事業部 デジタル推進課
企画員
髙橋 洋平 氏

社会福祉法人 恩賜財団 済生会
おんしざいだん さいせいかい

40都道府県で、病院や診療所などの医療機関をはじめ、高齢者や障害者の支援、更生保護などにかかわる福祉施設を開設・運営。さらに巡回診療船「済生丸」が瀬戸内海の57島の診療活動に携わっている。
URL https://www.saiseikai.or.jp/

製品 & サービス

- Cisco XDR
- Cisco Secure Access
- Cisco Duo
- Splunk Cloud Platform
- Cisco Secure Firewall
- Cisco Security Cloud Control
- Cisco Unified Computing System
- Enterprise Agreement
- Cisco Professional Service

2606-1-HC