UNIADEX ユニアデックス株式会社

前橋赤十字病院 様

AIによるSOC支援と自動処理で効果的にセキュリティを強化 「医療を止めない」という社会的責任を果たす

サイバー攻撃で医療が停止させられるインシデントが増加していることを受け、前橋赤十字病院はさらなるセキュリティ強化に取り組んだ。そのために導入したのが、ユニアデックスが提案した「Cisco XDR」である。多様な情報を相関分析し、異常なふるまいを早期に検知することでランサムウエアのような悪質な脅威に対応。AIによるSOC支援や他システムと連携した自動処理を行うプレイブック機能によって、限られた人員でも効果的なセキュリティ対策の運用を実装できる点を評価した。

事例のポイント

導入前

- 病院がサイバー攻撃を受けて、診療が止まるインシデントが相次いでいる。社会的責任を果たすためにもセキュリティを強化しなければならない
- 医療用システム・機器はセキュリティ対策ソフトをインストールできない。また、専用のリモートメンテナンス回線が必要といった制約に対応しなければならない
- セキュリティ対策の運用に割くことができる人員は人数・スキルともに限られている。その体制で効果的にセキュリティを強化しなければならない
- 新しいシステムの導入プロジェクトの間も診療は止められない。大きなトラブルを避けてスムーズに導入したい

導入後

- **異常なふるまいをリアルタイムに監視し、Cisco XDRによるインシデントの早期検知を軸に据えた強固なセキュリティを実現**
- **医療システム・機器には手を加えずに、ネットワーク上で異常なふるまいを検知。リモート回線が悪用された場合の備えとしても有効**
- **AIによるSOC支援やバックアップデータの自動生成を活用することで、担当者の負担を大幅に増やすことなくセキュリティ対策の運用を強化**
- **ITインフラに関する豊富なノウハウと丁寧な導入支援によって、大きなトラブルもなく3カ月で導入を完了**

◎お客さまの情報

前橋赤十字病院
Japanese Red Cross Maebashi Hospital

所在地：群馬県前橋市朝倉町389番地1
開設：大正2年3月23日
病床数：555床（一般病床527床、第二種感染症病床6床、精神病床22床）
URL：https://www.maebashi.jrc.or.jp/

大正2年（1913年）の開設以来、時代の要請に合わせて変革を行い、常に新しい病院であることを目指してきた。現在は、基幹災害拠点病院、高度救命救急センター、地域医療支援病院、地域がん診療連携拠点病院、ドクターヘリ基地病院、高次脳機能障害支援拠点機関、地域周産期母子医療センター、エイズ診療拠点病院の指定を受けている。

◎お客さまの声

前橋赤十字病院
病院長
中野 実 氏

**担当者の負担を大幅に増やすことなく
セキュリティを強化できました**

医療を止めないためにセキュリティ強化が欠かせないことは間違いありませんが、病院の本分が医療の提供であるということも事実です。セキュリティの強化だけに多くの人員を割くわけにもいきません。担当者の負担を大幅に増やすことなく、高度なセキュリティを実現できたことは大きな成果です。

前橋赤十字病院
事務部
情報システム課長
市根井 栄治 氏

**豊富な経験に裏打ちされた
導入支援には安心感がありました**

シスコとも密接に連携しながら、あらかじめリスクを洗い出し、トラブルの影響を最小化する計画を立てる。経験を生かしながら、丁寧にプロジェクトを進めてくれるユニアデックスの対応には安心感がありました。

経緯

医療用システム・機器の制約と限られた体制 どのようにセキュリティ強化を図るべきか

「みんなにとってやさしい、頼りになる病院」を理念に掲げる前橋赤十字病院。群馬県では唯一の高度救命救急センターに指定されており、関東で大規模災害が発生した際には救急の要を担う。

社会的責任の大きい前橋赤十字病院にとって、医療を止めないことは重要な使命である。サイバーセキュリティの強化は、そのための取り組みの1つだ。「2020年前後に病院がサイバー攻撃によって診療停止に追い込まれるインシデントが相次ぎ、リスクの大きさが改めて浮き彫りになりました」と前橋赤十字病院 病院長の中野 実氏は言う。

このような状況を受け、同病院はセキュリティの大幅な見直しに着手。特に重点を置いたのがランサムウエア、そして、システム・機器を提供するベンダーが遠隔からメンテナンスを行う際に利用するリモートメンテナンス回線への対策である。

しかし、見直しを進める中で課題に直面した。まず課題となったのが医療用システム・機器の制約だ。「広く知られていますが医療用システム・機器は法律や保障の関係でセキュリティ対策ソフトをインストールすることができません。また、リモートメンテナンス回線にも課題があります。事前申請や端末情報の提供といったルールを設け、病院で用意した回線を利用するようベンダーに要請していますが、一部のシステム・機器はさまざまな事情で例外的な運用を認めるしかない状況です」と事務部 情報システム課長の市根井 栄治氏は言う。

体制面の課題もあった。「IT部門は7人体制で、そのうち3人でネットワークとセキュリティを担当しています。同規模の他の病院に比べれば充実している方かもしれませんが、RaaS(Ransomware as a Service)が象徴するように、サイバー攻撃が組織的に行われ、さらに巧妙化している現在、その人員だけで悪用されている脆弱性などの動向や各セキュリティ対策の機能を理解し、日々のセキュリティ監視、アラートへの対応、インシデント発生時のログ分析や原因特定、そして対処などをスムーズに行うのは非常に困難です。私自身、ネットワークやアプリケーションの分野には一定の経験がありますが、セキュリティの観点でログを分析するには、まだスキルが足りないと感じています」と市根井氏は言う。

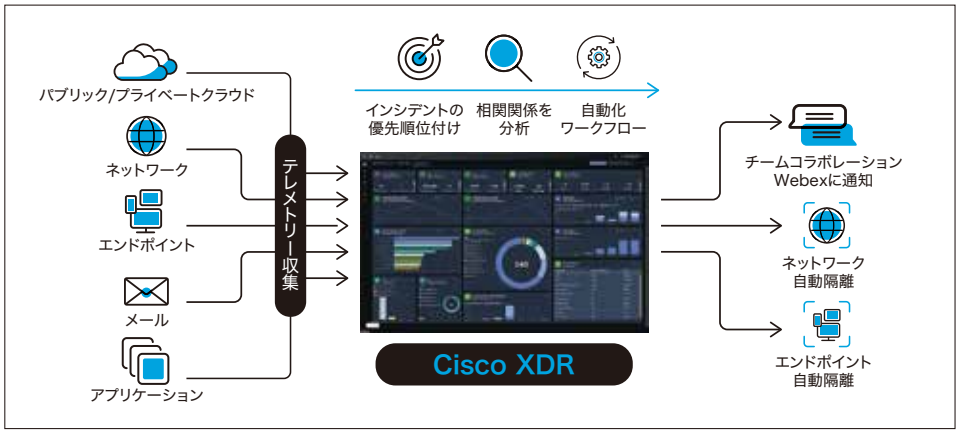
プロセス

AIによるセキュリティ業務の支援 エンドポイントの隔離などの自動処理に期待

課題に対応しながらセキュリティの強化を図るため、同病院はユニアデックスが提案した「Cisco XDR(Extended Detection and Response)」の導入を決めた。

ランサムウエアは、シグネチャーベースの対策や外部からの攻撃を防ぐための対策では対応が難しい。それに対してCisco XDRは、ネットワーク、エンドポイント、クラウド、メール、ID、アプリケーションなど、多様なデータを一元的に収集して可視化や相関分析を行い、異常なふるまいをリアルタイムに検知する。「同じくふるまい検知を行うソリューションにEDR(Endpoint Detection and Response)がありますが、PCやサーバーにエージェントをインストールしなければならないことが多く、医療用システム・機器に適用するのはハードルが高い。一方、Cisco XDRはエンドポイントには手を加えず、通信やネットワークフローを通じて通信量の急増、内部スキャン、未知のC2通信をなど検知するNDR(Network Detection and Response)機能を備えていました」と市根井氏は述べる。

◎Cisco XDRでできること



体制面の課題に対してもCisco XDRが解決策になると考えた。

人員もスキルもまだ十分とは言えないが、同病院は、いずれ自分たちでSOC(Security Operation Center)を運用していくことを視野に入れている。仮に一部を外部委託する場合も具体的な指示を出すなど、主導権を持つ体制を見据えており、その際、Cisco XDRのセキュリティ運用支援や自動化が助けになると期待したのである。

具体的にCisco XDRは、シスコが擁する脅威インテリジェンスリサーチチーム「Talos」の知見を組み込んだAIがログ分析などの調査、検証、危険度のスコアリング、適切な対処方法の提示などを自動的に実行し、セキュリティ担当者を支援する。「インシデントは危険度に応じて1～1000の間でスコアリングされます。膨大なアラートにむやみに振り回されることなく、緊急性の高いインシデントの対応に集中できます」(市根井氏)。

オートメーションというプレイブック機能を活用して、エンドポイントの隔離、IPブロック、アカウント無効化などの処理を自動化することも可能だ。「インシデントを検知したらシスコのWebexを通じて担当者に自動通知するという、シスコ製品同士の連携処理だけでなく、サードパーティー製品とも連携できます。シスコ製品だけに縛られず幅広い選択肢を持つことができ、既存資産の活用にもつながります」と市根井氏は言う。

効果・今後

豊富な経験とノウハウを生かした支援を受け 3カ月でスムーズに導入を完了

現在、Cisco XDRは、約150台のネットワークスイッチからNetFlowを取得し、

インシデントの可視化や相関分析などを行っている。「万が一、リモートメンテナンス回線を悪用された場合も、その後のふるまいから早期に侵入を検知できれば、被害を最小限に抑えるための行動を選択できます。環境が整えば、エンドポイントの情報もCisco XDRに集約し、より統合的な監視や相関分析を行うことも検討しています」（市根井氏）。

オートメーションによる自動処理も積極的に活用しています。例えば、ランサムウエア対策として以前から導入していたイミュータブルバックアップシステムとCisco XDRを連携させた自動処理を実現。Cisco XDRがインシデントを検知すると、即座にバックアップデータを生成するよう設定している。「インシデント発生時、自動的に最新のバックアップが取られていれば、担当者はすぐに影響範囲の把握や原因特定に取りかかることができます。しかも、バックアップデータの存在が保険となり、落ち着いて対処に臨めるはず。スピードだけでなく、担当者の心理面にも有効だと考えています」（市根井氏）。

Cisco XDRの導入期間は約3カ月。非常にスムーズに導入を終えた。

「ITインフラやセキュリティに関して豊富な経験やノウハウを持つユニアデックスのおかげです。例えば、Work Flowによる連携処理を設定する際は、機器のソフトウエアなどにバグがないかを念入りに調査した上で、影響の少ないネットワークセグメントで検証を行いながら丁寧に作業を進めてくれました。ネットフローの収集についても、運用開始後のネットワーク機器の負荷を慎重に見極めて設計してくれ、現在まで大きなトラブルは起こっていません。操作についてもユニアデックスがシスコと密接に連携を取りながら説明会を開催してくれたことで、経験の浅い若いメンバーも苦手意識を持つことなく対応できています」と市根井氏は言う。

このような成果を受けて、同病院はシステムが停止した後の復帰ではなく、インシデント検知直後の対応力を鍛える内容に訓練を変更するなどIT-BCP（ITのBusiness continuity plan）を改定した。CSIRTの定義もインシデント検知を起点に活動するスモールCSIRTと、実際に大きな被害が発生した際にインシデント対応を行うラージCSIRTに分けて整理している。「これでランサムウエアの被害に遭うのなら、他の製品でも回避は難しいだろう。幹部も含めて、そう評価しています」と中野氏は強調します。

今後、同病院はCisco XDRを中心に据えたセキュリティ運用を行いながら、止まらない医療を目指す。また、自身の経験や知見を他の病院と共有するなどして、医療業界全体のセキュリティ強化にも貢献していく構えだ。

UNIADEX
ユニアデックス株式会社
https://www.uniadex.co.jp/
〒135-8560　東京都江東区豊洲1-1-1
Tel：03-5546-4900

ユニアデックスのお客さま事例

2025年6月取材
010901736-0 H2509（100）