前橋赤十字病院

分析、検出、スコアリング、自動処理を実行 AIの力を活用し、止まらない医療を実現

サイバー攻撃で医療が停止させられるインシデントの増加を受け、前橋赤十字病院はセキュリティ強化に取り組みました。新たに導入したのは、多様な情報を相関分析し、ふるまい検知を行う Cisco XDR です。医療用システム・機器の制約や体制面の課題に対応しながら、AI による高度な脅威検知や自動処理によって強固なセキュリティを実現しています。

前橋赤十字病院

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）

「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ことになります。実際、重症患者用ベッド 72 床、うち集中治療室（ICU）24 床という屈指の受入体制を擁している上、緊急時には病院全体が救急外来として機能するように各施設が設計されています。

課題

- サイバー攻撃によって医療が止まるインシデントが相次いでいる
- 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などの制約がある
- 限られた人員でセキュリティ対策を強化しなければならない

ソリューション

- 異常なふるまいをリアルタイムに監視し、検知する Cisco XDR を導入
- エンドポイントには手を加えずにふるまい検知を行える
- AI によるセキュリティ運用支援や自動化に期待

結果

- インシデントの早期検知を軸に据えた新セキュリティで止まらない医療を実現
- AI によるスコアリングのもと担当者は緊急度の高いインシデントに集中
- バックアップデータの自動生成で心理面でも担当者をサポート

今後

- エンドポイントも監視対象に加え、より統合的な監視や相関分析を行いたい
- 他の病院とも知見を共有し、医療業界全体のセキュリティ強化に貢献したい

これで被害に遭うのなら
他の対策でも防ぐのは難しい
そう評価しています

中野 実 氏

前橋赤十字病院
病院長

課題

医療用システム・機器の制約や限られた体制が課題

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す。そのために様々な施策に取り組んでいますが、サイバーセキュリティの強化も、その 1 つです。「病院におけるサイバー攻撃のリスクは以前から指摘されていましたが、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」と前橋赤十字病院の中野 実氏は言います。

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ェア、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す。

しかし、見直しを進める中で課題に直面しました。まず課題となったのが医療用システム・機器の制約です。「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・機器は様々な事情で例外的な運用を認めるしかない状況です」と同病院の市根井 栄治氏は言います。

体制面の課題もありました。社会的にもセキュリティ人材は不足していると言われていますが、閉域網でシステム・機器を運用していることを背景に、長い間、セキュリティリスクは低いと考えてきた医療業界はセキュリティ人材の育成や体制整備が遅れ気味です。「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」と市根井氏は言います。

システムや機器に制約がある病院でふるまい検知を行える

ソリューション

AI によるセキュリティ業務の支援や自動化に期待

課題に対応しながらセキュリティの強化を図るには、どのような方法が最適か――。同病院は調査を行い、複数の方法を比較。最終的にシスコの Cisco XDR（Extended Detection and Response）の導入を決めました。

管理者権限を盗み内部から攻撃する、多様な亜種が登場する、OS の正規機能を悪用するといった特徴を持つランサムウェアは、シグネチャ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困難。異常なふるまいをリアルタイムに監視し、検知する対策が有効です。

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、異常なふるまいを検知するソリューションです。「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 通信などを検知する NDR（Network Detection and Response）機能を備えている。病院でふるまい検知を行うのに最適と判断しました」と市根井氏は述べます。

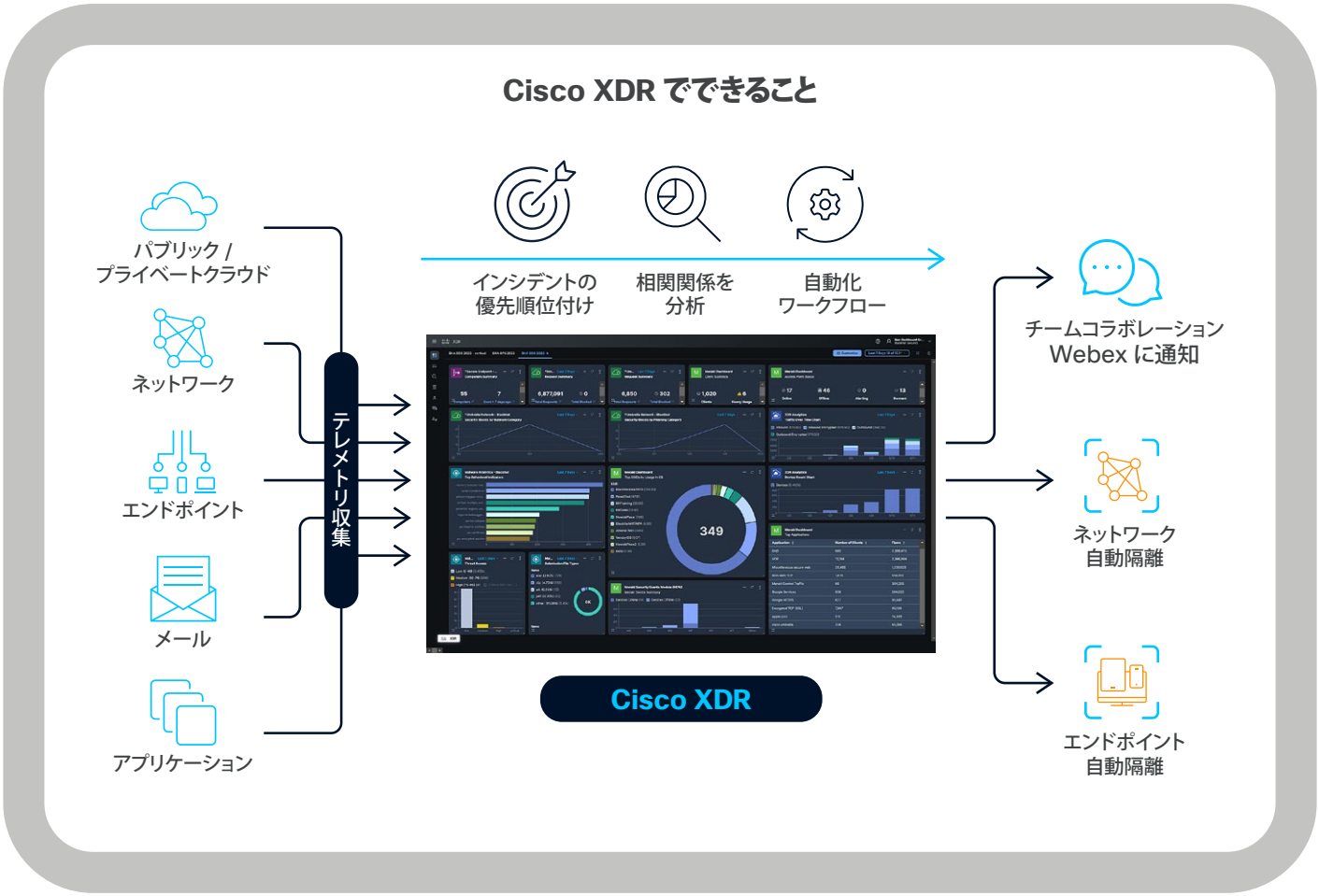
体制面の課題に対しても Cisco XDR が解決策になると考えました。

人員もスキルもまだ十分とは言えませんが、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ます。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す。

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します。「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です。しかも自動処理は、シスコの製品だけでなく他社のシステムと連携させて自動処理を行うこともできます。

「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だけでなく、サードパーティー製品とも連携できる点も評価しました。調査中、多くのベンダーから『複数の製品による多層防御が重要です』とアドバイスされましたが、続けて話を聞くと、そのベンダーから複数の製品を導入することを提案され、『他社製品とは連携できません』と言われたりしました。それでは製品選定の選択肢を大きく狭めてしまいます。一方、Cisco XDR は、シスコ製品だけにしば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」と市根井氏は言います。



結果～今後

インシデントを検知したらバックアップデータを自動生成

同病院のネットワークは、物理的には統合されており、電子カルテを中心とする医療系とインターネット系のネットワークは VLAN で論理分割しています。現在、Cisco XDR は、このネットワークを構成する約 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ます。「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。前述した医療用システムや機器の制約によって現在は行っていませんが、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、ランサムウェ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 Cohesity DataProtect 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、Cohesity DataProtect が即座にバックアップデータを生成するよう設定しています。

「インシデント発生時、自動的に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、落ち着いて対処にのぞめるはず。Cisco XDR と Cohesity DataProtect の自動処理は、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 の導入後、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）を改定しました。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ます。「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。セキュリティ担当者の負担を大きく高めることなく、高度なセキュリティを実現できたことは大きな成果。これでランサムウェ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します。また医療用システム・機器、人員や体制の課題は、同病院だけでなく多くの病院にも共通する課題と捉え、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貢献していく構えです。

前橋赤十字病院
病院長
中野 実 氏

前橋赤十字病院
事務部
情報システム課長
市根井 栄治 氏

前橋赤十字病院
Japanese Red Cross Maebashi Hospital

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。
URL https://www.maebashi.jrc.or.jp/

製品 & サービス

・Cisco XDR

2509-1-HC