The bridge to possible

大阪急性期・総合医療センター

閉域網神話はもう通用しない
ネットワーク可視化で侵入した脅威に素早く対処

ランサムウェアによって診療機能が停止――。大阪急性期・総合医療センターのセキュリティインシデントは、サイバー攻撃が私たちにとって深刻な脅威であることを改めて知らしめました。被害を繰り返さないために、同院が脅威の侵入への備えとして導入したのが Cisco Secure Network Analytics です。

大阪急性期・総合医療センター

所在地
大阪市住吉区万代東 3 丁目 1 番 56 号

開院日
1955（昭和 30）年 1 月

許可病床数
865 床

The bridge to possible

急性期医療から高度な専門医療まで、36 の診療科による総合力を活かした質の高い医療を提供している大阪急性期・総合医療センター。高度救命救急センター、そして大災害に対応する基幹災害医療センターという 2 つの重要な役割も担っており、地域の中核病院として大阪府民の暮らしを支えています。

課題

- 診療系システムがランサムウェアに感染。診療機能の停止に陥った
- 閉域性の高いネットワークは安全と考えられてきたが、境界防御だけでは限界がある
- 医療機器や制御端末は、OS のサポート期間やメーカー保証の関係で対策が困難

ソリューション

- 電子カルテ端末やプリンタ、医療機器の通信を監視しネットワークを可視化する Cisco Secure Network Analytics

結果

- 様々な対策や体制の見直しに加え、Cisco Secure Network Analytics を導入しセキュリティを強化
- 脅威を与える前段の偵察行為から検知して迅速に対処。被害を最小限に抑える
- ネットワークトラフィックを監視する方法は、端末への影響がないため医療機器や制御端末の対策にも有効

今後

- Cisco XDR など、さらにセキュリティを強化できる技術に期待

監視の幅広さ、医療機器や制御端末への対応を評価して Cisco Secure Network Analyticsを選定しました

上野山 亮 氏

地方独立行政法人大阪府立病院機構
大阪急性期・総合医療センター
情報企画室　サブリーダー

The bridge to possible

課題

システムが動かない。ランサムウェア感染で診療機能が停止

サイバー攻撃による被害の報告が後を絶ちません。一般企業はもちろん、電力やガス、石油などのエネルギー関連、金融、鉄道など、社会へのインパクトの大きな重要インフラを狙う攻撃も増えています。医療も、その 1 つです。

攻撃手法としては、システムやデータを人質に身代金を要求してくるランサムウェアの被害が目につきます。また、まずは侵入が容易と思われる組織に侵入して、そこを踏み台に目的の組織に侵入する、いわゆるサプライチェーン攻撃も増加傾向にあるようです。

2022 年 10 月に大阪急性期・総合医療センターを襲ったインシデントも、まさにランサムウェアとサプライチェーン攻撃によるものでした。外部の給食事業者を経由したサイバー攻撃によって、電子カルテを含む同院の総合情報システムに障害が発生。救急診療の受け入れ、初診受付、予定手術を停止せざるを得ない状況に陥りました。

「当直の事務員から『部門システムが動かない』という連絡を受け、サーバ確認を行ったシステム運用管理職員に状況を聞くと、画面に『身代金を払え』というランサムノートが表示されているとのこと。ランサムウェアに感染している可能性が高まり、院内は大いに混乱しました」と同院の上野山 亮氏は言います。

発覚を受け、同院は紙カルテによる対応など当面の診療方針を決定するなど、すぐにインシデントへの対処を開始しました。大阪府立病院機構本部、大阪府、大阪府警、大阪市保健所、内閣サイバーセキュリティセンター、厚生労働省医政局などの各方面にも連絡を入れ、厚生労働省からはサイバーセキュリティ初動対応支援チームが派遣されました。

電子カルテや IT インフラを構築した各 IT ベンダーもすぐに担当者が駆けつけて、原因や影響範囲を調査しました。「ネットワーク担当ベンダーの調査によって、その日のうちに、ランサムウェアを仕掛けた攻撃者が栄養給食管理サーバから侵入していることを特定しました。早朝の午前 4 時台の数分の間に外部の給食事業者との接続回線を通じて大量の RDP を利用したパスワード総当たり攻撃で突破されたことがわかったのです。その情報を基に調査を続け、その給食事業者が踏み台にされていること、その事業者のファイアウォールの脆弱性が悪用されたことなども把握しました」上野山氏。攻撃は、病院が許可したプロトコルと経路、端末を悪用しているため防ぐことが難しいサプライチェーン攻撃だったのです。

シスコ製品でない ネットワーク機器も監視可能

ソリューション

侵入後の脅威を検知。対策が困難な医療機器や制御端末に有効

システムの復旧に向けて、同院は ID ／パスワードや管理者権限、ACL（アクセルコントロールリスト）の設定見直しなど、セキュリティの強化を行いましたが、対応が難しい課題もありました。超音波（エコー）検査装置など、様々な医療機器や制御端末への対応です。

「ネットワークに接続する約 2000 台以上の端末は初期化した上で再接続することを決めたのですが、検査機などの医療機器や制御端末は、メーカー保証の関係で初期化することができません。それらに再び侵入するためのバックドアなどが仕込まれていたら、大きな脆弱性を残すことになってしまいます。そもそも医療機器や制御端末の中には、サポート切れの OS を搭載しているものもあり、どのようにセキュリティを強化するかは、長年、大きな課題でした」と上野山氏は話します。

病院のネットワークは、閉域性が高いことから、セキュリティは外部との境界で対策をしておけば大丈夫と考えるのが一般的でした。そうした背景もあり、医療機器や制御端末の OS のサポート期間などは、そこまで注視されてきませんでした。しかし、今回のように攻撃者は巧妙な手法で境界を突破してきます。「『閉域網神話』は、もはや通用しません。

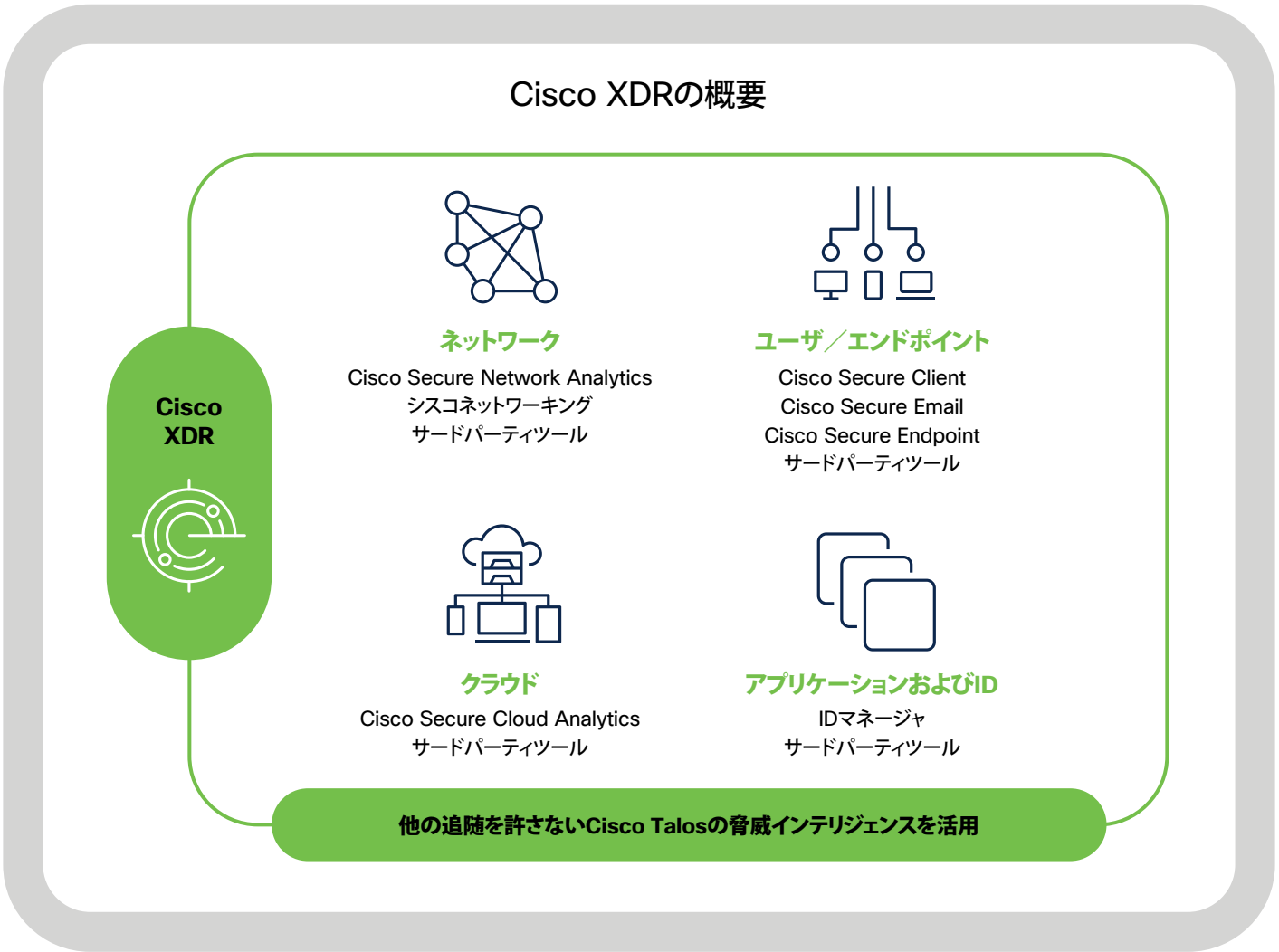
今回のインシデントで、そのことを改めて痛感しました。病院はもちろん、外部業者も含めて、業界全体で意識を変えていく必要があると強く考えています」と上野山氏は言います。

そこで、同院が導入したのが Cisco Secure Network Analytics（SNA）です。

SNA は、NDR（Network Detection and Response）カテゴリに属する製品で、ネットワークトラフィック監視によってネットワークを可視化し、内部の不審なふるまいを検知。脅威が院内に拡散し、手遅れになる前に迅速に封じ込めを支援します。直接対策を施すことが難しい医療機器や制御端末が悪用されても、ネットワーク上で普段とは異なる挙動など、攻撃の予兆を検知して、すぐに対処し、被害を最小限に防ぐことができます。

導入時には、他の NDR 製品との比較も行いましたが、他の製品がコアスイッチを通過するネットワークトラフィックを監視するのに対して、SNA がサーバ間や末端の端末間のトラフィックなども含むネットワーク全体を対象に、よりきめ細かな監視を行うことを高く評価しました。「また、NetFlow と sFlow に対応しており、シスコ製品ではないネットワーク機器も監視対象に含められるため、院内に隅々まで監視網を広げられます。さらに復旧作業時にネットワークから切り離した PC や医療機器の安全性を確認し、再接続する際にも利用しており、すでに動作検証ができていたことも導入を後押ししました」と同院の榎本 純也氏は話します。

ふるまい検知を行う製品としてはネットワークトラフィックを監視する NDR ではなく、エンドポイントで監視を行う EDR（Endpoint Detection and Response）もありますが、



The bridge to possible

前述したとおり多くの医療機器や制御端末はメーカー保証の関係でソフトウェアを追加したりすることができません。また、その端末自体の不正なふるまいは検知できても、他の端末と連動して挙動なども把握できません。頻繁に発生する端末の入れ替えや追加などにも適宜対応しなければならなくなることから、EDR より NDR の方が最適だと判断しました。

結果～今後

攻撃前の小さな調査行動も察知して未然に被害を防ぐ

同院はインシデント発生から 43 日目に外来診療を再開、73 日目には通常診療も再開しました。インシデント発生 4 日後から利用している SNA には大きな手応えを感じています。

「セキュリティ対策が難しい医療機器や制御端末をネットワーク内に多く抱える病院にとって SNA は、非常に有効な対策だと改めて感じています。今回の攻撃において、最初の攻撃行動は早朝の総当たり攻撃ですが、おそらく、それ以前から調査のための様々な行動を行っていたのではないかと考えています。SNA と運用監視サービスによって、そうした小さな不審な挙動も捕捉し、実際の被害が発生する前に対処することができるようになるはず」と榎本氏は話します。上野山氏も「インシデント発生後、他の病院から対策の状況を聞かせてほしいとヒアリングの依頼をよく受けますが、SNA を導入したことは、必ず伝えています」と続けます。

さらに同院はシスコが提案する Cisco XDR（Extended Detection and Response）にも期待を寄せています。

Cisco XDR は、ネットワークだけでなく、エンドポイント、メールなど、さらに幅広い対象を監視し、サイバー攻撃の侵入に備える対策です。シスコが擁するサイバーセキュリティ インテリジェンス＆リサーチ グループ Cisco Talos の知見を有効活用したり、AI（人工知能）によって多様な情報の相関関係を分析したりして、サイバー攻撃の全体像の把握、よりスピーディーな対処、自動化によるセキュリティ担当者の負担軽減など、様々な価値を実現します。「より高度な対策の実現は、当然、考えなければならないことです。費用対効果の見極めなどが必要ですが、選択肢の 1 つとして注目しています」（上野山氏）。

診療の再開に向けて同院が様々なセキュリティ強化を行ったことは、すでに述べましたが、外部業者のセキュリティ監査を強化するなど、体制や運用面でも様々な施策に取り組んでいます。また、そのことを様々な形で発信しながら、サイバー攻撃に備えるとともに、その被害の深刻さ、対策強化の重要性を訴え続けています。同院の経験をムダにせず、社会全体で悪質なサイバー攻撃に立ち向かうために、シスコも同院の取り組みを支えていきます。

地方独立行政法人大阪府立病院機構
大阪急性期・総合医療センター
情報企画室　サブリーダー
上野山 亮 氏

地方独立行政法人大阪府立病院機構
大阪急性期・総合医療センター
情報企画室　主事
榎本 純也 氏

The bridge to possible

急性期医療から高度な専門医療まで、36の診療科による総合力を活かした質の高い医療を提供。高度救命救急センター、そして大災害に対応する基幹災害医療センターという2つの重要な役割も担っており、地域の中核病院として大阪府民の暮らしを支えている。
URL https://www.gh.opho.jp/

製品 & サービス

- Cisco Secure Network Analytics

2406-2311-000-BL