net one

導入事例
セキュリティ

大阪急性期・総合医療センター 様

サイバー攻撃の被害を繰り返さない ネットワーク監視と運用監視サービスで 攻撃者に侵入されても不審な行動をすぐに検知

2022年10月、大阪急性期・総合医療センターはランサムウェアに感染し、診療機能の停止を余儀なくされた。私たちの命や健康までも人質になる――。サイバー攻撃の悪質さや被害の深刻さを改めて感じたインシデントでもあった。現在、同院はセキュリティ対策を強化した上で診療を再開し、再び大阪府民の暮らしを支えている。被害を繰り返さないための対策として、新たに導入したのがネットワンシステムズの提案した「Cisco Secure Network Analytics（SNA）」と運用監視サービスである。

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

ランサムウェアに感染 診療機能の多くが停止

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る。

2022年10月、同院は大きなセキュリティインシデントに遭遇した。サイバー攻撃によって電子カルテを含む総合情報システムが利用できなくなり、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ったのである。

「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、確認に向かった保守ベンダーに状況を聞くと、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 亮氏は言う。

障害は電子カルテにもおよび、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た。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た。

電子カルテやITインフラを構築した各ITベンダーにも、本当にランサムウェアに感染しているのかの確認、感染しているとしたら原因や影響範囲を究明してほしいと依頼をかけた。「既存ネットワークの構築と保守を担当するネットワンシステムズには、ネットワーク機器やファイアウォールのログ調査や各機器の感染状況の確認などを依頼しました」と同院の榎本 純也氏は言う。

依頼を受けたネットワンシステムズは、即座に担当者が現地に駆けつけ調査を開始。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た。「早朝の午前4時台の数分の間に給食業者との接続回線を通じて大量のRDP通信があった。つまり総当たり攻撃で突破されたことがわかりました。その情報を基に調査を続け、外部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）。

対策が難しい医療機器や制御端末に ネットワークふるまい検知で対応

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）の設定を見直すなど、セキュリティの強化に向けた見直しを行った。

しかし、対応が難しい課題もあった。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ある。

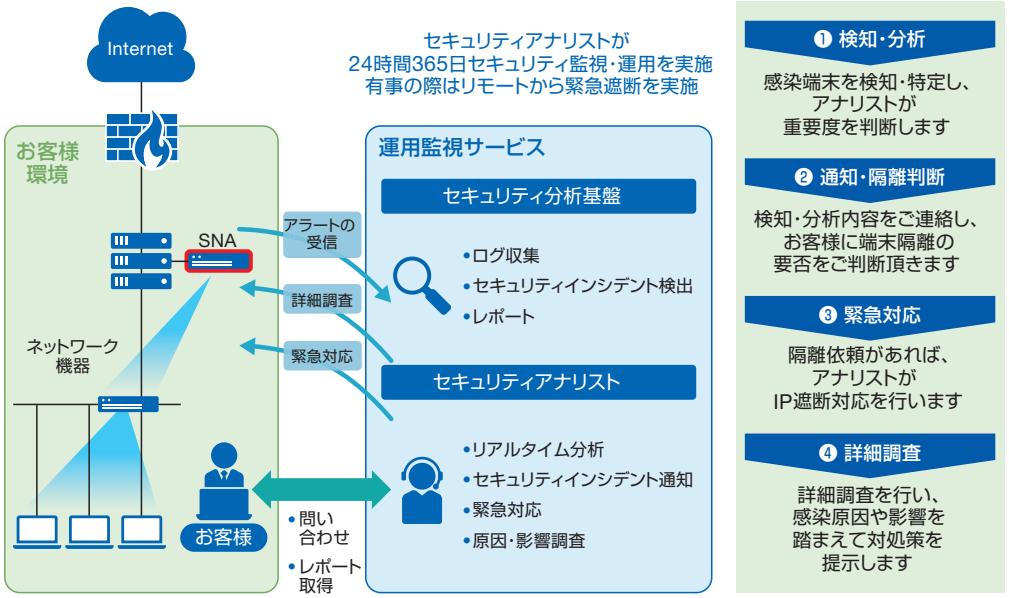
「ネットワークに接続する2,000台以上の端末は初期化した上で再接続することを決めたのですが、検査機の医療機器や制御端末は、メーカー保証の関係で初期化することができません。それらの端末に再び侵入するためのバックドアなどが仕込まれていたら、大きな脆弱性を残すことになってしまいます。そもそも医療機器や制御端末の中には、サ

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、長年の大きな課題でした」と上野山氏は話す。

そこで、ネットワンシステムズが提案し、同院が導入したのが「Cisco Secure Network Analytics（SNA）」である。

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を監視して、ネットワーク内部の不審なふるまいを検知。仮に境界が突破され、脅威が侵入してしまっても迅速かつ的確な対処を支援する。端末自体への対策が困難な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、すぐに対処することで被害を最小限に防ぐことができる。

SNAおよび運用監視サービス提供イメージ



※お客様の求めるレベルに応じて、運用プランをご提案します

加えて同院はSNAと合わせてネットワンシスムズが提案した運用監視サービスも導入した。

「ネットワーク内の不正なふるまいをリアルタイムに検知するSNAを導入しても、人が同じ体制で構えていなければ、導入効果は半減します。私たち職員も思い立ってログを見たりすることはありますが、膨大なログのすべてを常に監視することは現実的には不可能です。そこで外部の運用監視サービスを頼ることにしました」と榎本氏は話す。

具体的にネットワンシステムズが提案した運用監視サービスは、24時間365日の体制でSNAの検知結果を監視。平常時は定期的に提出するレポートで、監視の状況を報告するが、緊急度の高いリスクを検知した際には即座にアラートを挙げる体制になっている。「まだアラートを受けたことはありませんが、監視を任せていることで安心感があります」（上野山氏）。

寄り添って対応を支援
サポート力と技術力に感謝

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た。「インシデント発生直後にすぐに駆けつけ、復旧後の今日にいたるまで、ネットワンは常に私たちに寄り添ってサポートをしてくれました。素早く侵入経路を特定し、原因を明らかにできたのはネットワンシステムズの技術力のおかげ。本当に助かりました」と榎本氏はネットワンシステムズの対応に感謝を示す。

セキュリティ強化のために導入したSNAに対する期待も大きい。

「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。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」と上野山氏は強調する。

インシデントを受けて厚生労働省が医療情報システムの安全管理に関するガイドラインを改変するなど、同院が遭遇したセキュリティインシデントは、その後の医療分野のサイバーセキュリティにも大きな影響を与えた。同院も取引のある外部業者のセキュリティ監査を強化するなど、様々な対策を追加したり、そのことを様々な形で発信したりしながら、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る。被害を繰り返さないために、同院の経験を社会全体で共有し、これからの対策に役立てていきたい。

大阪急性期・総合医療センター
https://www.gh.opho.jp/
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。

ネットワンシステムズ株式会社
〒100-7024　東京都千代田区丸の内2-7-2 JPタワー
https://www.netone.co.jp/

ネットワンパートナーズ株式会社
〒100-7026　東京都千代田区丸の内2-7-2 JPタワー
https://www.netone-pa.co.jp/