「ランサムウェア禍」が地方病院を襲う

国挙げてのサイバーセキュリティ対策が焦眉の急

神戸市議会議員・元国会議員政策担当秘書　岡田裕二

「すべてのファイルが暗号化されました。復元のためにはビットコインを支払ってください。金額はあなたがどれだけ早くメールを送るかで変わります」

22年10月、大阪府内に3ヵ所しかない高度救命救急センターのひとつで、災害拠点病院でもある病床数865床の中核病院「大阪急性期・総合医療センター」（大阪市住吉区）が、「ランサムウェア」と呼ばれる身代金要求型のコンピュータウイルス攻撃を受けた。電子カルテシステムなどの中枢機能が停止し、手術や外来診療の停止を余儀なくされた。復旧させたければ身代金を払えとの冒頭のメッセージがコンピュータの画面に表示され、その後、数ヵ月にわたり病院業務が制限。全診療科の通常診療が再開するには、年を跨ぐ羽目になってしまった。

全世界でランサムウェアの被害が増加している。初期の有名な事例は20年9月、ドイツ・デュッセルドルフの大学病院がランサムウェアによる攻撃の標的になった事例だ。手術は延期、診療はキャンセルされ、入院するはずだった78歳の患者は30キロ以上離れたヴッパータール市にある別の病院に転送され、後に死亡した。この事件は患者の死に関連する世界初のランサムウェア被害として注目を集めた。

20年10月にはフィンランドの心理療法センターがランサムウェアに感染し、4万件以上の患者の個人情報データが流出した。45万ユーロを要求されたが、病院側が支払いを拒否した結果、ネット上に個人情報データが暴露され、「情報を消してほしければ500ドル支払え」と再度脅迫される事態となった。

21年5月にはアイルランド国保HSEが大規模な攻撃を受け、システムを停止。これにより、アイルランド全域で医療サービス提供に混乱が生じた。フランスでも22年にコルベイユ・エソンヌ病院やベルサイユ病院センターが標的となった。

病院以外の公的機関や企業も例外ではない。21年5月には米国最大のパイプライン運営会社であるコロニアル・パイプライン社が攻撃を受け、ハッカー集団「ダークサイド」に対し、500万ドル相当の身代金を支払った。同時期に世界最大級の食肉加工メーカーのブラジル・JBSの米支社も攻撃を受け、身代金として1100万ドル相当を支払ったと発表した。

157年の歴史を誇る米イリノイ州の黒人大学リンカーン・カレッジは、21年12月に攻撃を受けた。新入生募集はおろか、学内データへのアクセス遮断、資金調達に必要なすべてのシステムが機能停止に陥った結果、翌22年5月に閉校した。19年に入学者数が大幅に増え、学生寮の入居者数が過去最多となるなど、最盛期を迎えた直後の惨事であった。

大学のウェブサイトには「リンカーン・カレッジは1887年の経済危機、1912年のキャンパス大火災、1918年のスペイン風邪、大恐慌、第二次世界大戦、2008年の世界金融危機など、多くの困難で厳しい時代を生き抜いてきましたが、今回は違います」と記載。ランサムウェアに葬られた無念さを滲ませた。

日本も例外ではない

日本国内での被害も急増している。よく知られた事例としては、21年10月に起こった徳島県半田病院の事例。ほぼすべての病院機能がダウンし、バックアップも同時に攻撃されたため、早期の復旧は絶望的とされていたが、2ヵ月を待たず機能とデータを全回復させ、関係者を驚かせた。「身代金は支払わない」と表明していた病院だったが、共同通信社の記者がハッカー集団「ロックビット」に取材を試みたところ、あっさりと3万ドルの身代金支払いがあったことを認めた。

そのほか、冒頭の大阪急性期・総合医療センター以外にも、東大阪医療センター（大阪府・21年5月）、日本歯科大学付属病院（東京都・22年1月）、春日井リハビリテーション病院（愛知県・同1月）、青山病院（大阪府・同4月）、鳴門山上病院（徳島県・同6月）、金沢西病院（石川県・同12月）など、病院の大小問わず枚挙にいとまがない。まさに新型コロナウイルス禍で同時進行する「ランサムウェア禍」だ。

こうした全国各地の被害例を受け、主だった公立病院では急ピッチで対策が進められている。例えば、神戸市立中央市民病院では、

①電子カルテ等の医療情報を扱う診療系ネットワークは原則インターネットに接続せずクローズドなネットワークとする。医療機器のメンテナンスなど、限定的に外部と接続する必要がある場合はセキュリティレベルが担保されたVPN回線を使用する

②ファイヤーウォールなどを再構築し、バージョンアップを定期的に行う

③接続できるパソコン等は事前登録制とし、事前にウイスル対策ソフトによる検疫を実施

④USBメモリの使用は必要最低限とし、使用する端末を限ったうえで、専用のUSBメモリのみ利用できるよう設定する。使用時にはウイルス対策ソフトによる検疫を実施する

などの対策を講じている。

しかし、「サイバー攻撃を完全に防ぐことは不可能」という考えに立った対策も重要だ。システム内部にウイルスが侵入しても、ウイルスの不正な動きを早期に検知し、その端末を自動的にネットワークから遮断することで被害を最小限に抑えるEDR（エンドポイント・ディテクション&レスポンス）の導入も進んでいる。必要経費としては、1病院あたり構築費・年間運用費ともに数千万円程度で済むという。

BCP（事業継続計画）の見直しも必要不可欠だ。核となるのはバックアップの確保だ。サーバ等の故障に対応したバックアップはよく行われているが、一度サイバー攻撃に晒されると、バックアップデータも含めてシステム全体が被害を受けるため、バックアップの外部化や多層化が重要だ。

最も論争となり得るのが身代金の扱いだ。世界の事例を見ると、米国ではさっさと身代金を支払い、早期に被害を回復するケースも散見される。逆にフランスのように法律で身代金を禁じている国もある。

日本の場合、法令などの明確な規定はないものの、厚生労働省が22年11月に公表した「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」では、身代金の「支払いは厳に慎むべき」としている。

半田病院の場合、復旧には億単位の経費が必要とされ、何ヵ月もの長期の休業が不可避とされていた。その間、地域住民は医療サービスを受けられない。身代金3万ドルを払いさえすればすぐ復帰できるのであれば、当事者は葛藤に苛まれることだろう。

いずれにせよ地域医療を崩壊に導く深刻なリスクだ。各自治体や法人に任せるのではなく、国として対策を打ち出し、国内の英知を結集させる必要がある。厚労省は医療機関のサイバーセキュリティ対策強化のため、22年12月「医療機関向けセキュリティ教育支援ポータルサイト」なるものを立ち上げたが、これこそコロナ禍に対してアマビエの絵をかざすようなもの。根本的な対策になっていない。

157年の歴史を誇るリンカーン・カレッジの閉校は、日本の地方病院にとって決して対岸の火事ではない。国挙げてのサイバーセキュリティ対策が喫緊の課題だ。

ランサムウェア「Petya」の感染画面