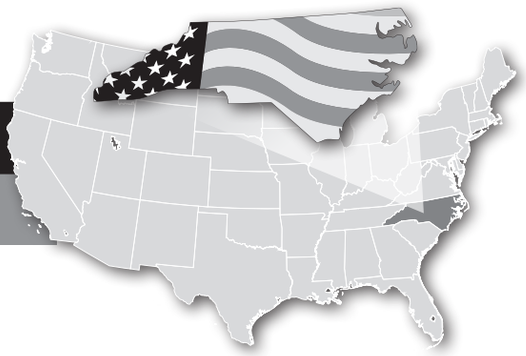

シリーズ
Part 20
（最終回）

米国医療機関に対するランサムウェア攻撃の実態

Cyber Attacks to Healthcare Organizations

ノースカロライナ州保険部認定 SHIIP カウンセラー／アメリカ病院経営士会認定病院経営士
河野圭子
Keiko Kono, RPh, MHA, FACHE

近年、アメリカの医療機関ではランサムウェアなどによるサイバー攻撃が増えてきました。今回は、実際に起きたランサムウェア被害の事例を紹介します。

Cyber attacks by ransomware are increasing in healthcare organizations within the United States. This essay will introduce three actual case studies.

医療機関は狙われやすい

インディアナ州の地域統合医療グループ・ハンコック・ヘルス CEO のロング氏は、自分の病院がランサムウェア攻撃を受けた時、第一に「患者の安全（Patient to be safe)」、第二に「患者個人情報の保持」を考えたと語っています。医療機関は、ランサムウェア攻撃によるシステム停止が即人命にかかわることから、狙われやすいのです。

ランサムウェア（Ransom：身代金）とは、悪意のあるソフトウェアの一種で、感染したコンピュータ内の

Ransomware attack to target providers

Mr. Steve Long, president and CEO of Hancock Health and Hancock Regional Hospital in Indianapolis, Indiana said that when his hospital was hit by a ransomware attack, he thought that his organization should focus on patient safety first and the security of patient information second. Healthcare providers are vulnerable to ransomware attacks which cause life-threatening events.

Ransomware is a type of malware that encrypts the data and blocks access to it unless a ransom is paid.

Ransomware attacks on providers have been increasing

データを暗号化、操作画面をロックしたりして正常に利用できない状態にして、復元のために身代金を要求するものです。

2018年からアメリカの医療機関へのランサムウェア攻撃が増加し、**図表１**のように全米の医療機関への被害も広がっています。次に被害を受けた医療機関の代表的な事例を取り上げます。

ケース１：アルバマ州スプリング・ヒル医療センター

～ランサムウェア被害で初の死亡例になるとされている事例～

ランサムウェア攻撃発覚日：2019年７月８日

スプリング・ヒル医療センターは、ランサムウェアの攻撃を受け、身代金の支払いを拒否し、速やかにネットワークを停止して被害の封じ込め対策を取りました。その結果、院内コンピュータシステム、電子カルテシステムと医療機器がおよそ３週間使用不能になりました。

キッドさんは、病院がそのような状況であることを知らされないで、７月16日に出産のために来院し、分娩室に入りました。ナースステーションでは、胎児心臓モニター監視に支障が出ていたので、胎児は、適切な処置がとられないまま帯頸部巻絡の状態で生まれてきました。乳児は、その時の分娩障害により重度の脳障害を負い９カ月後に死亡しました。

キッドさんは、病院を相手に訴訟を起こし、乳児の死亡原因が、ランサムウェア攻撃に起因することが法廷で

since 2018. The following are three real cases.

Case 1: Spring Hill Medical Center, Alabama

～The first alleged ransomware death～

Incident: July 8, 2019

After Spring Hill Medical Center learned of the ransomware attack, the hospital refused to pay the ransom and promptly shut down their network to contain the incident and protect data. As a result, the hospital's computer system, EMR, and medical equipment were unusable for approximately three weeks.

Ms. Kidd wasn't informed the hospital was struggling with a cyberattack when she went in to deliver her daughter, and doctors and nurses missed several key tests that would have shown that the umbilical cord was wrapped around the baby's neck, leading to brain damage and death nine months later.

Ms. Kidd filed a lawsuit against the hospital and if the allegations are proven; the case would mark the first time a ransomware attack turned deadly. A trial is set for November 2022.

図表１　ランサムウエア攻撃を受けた代表的な医療組織

2020年12月	プラクティス・ファースト・メディカル	ニューヨーク州	患者情報データを含むファイルの不正コピー
2021年５月	スクリプス・ヘルス	カリフォルニア州	電子カルテシステム、予約システム、患者ポータル不能
2021年５月	UF ヘルス	フロリダ州	電子カルテシステム不能
2021年６月	セントジョセフ病院	ジョージア州	電子カルテシステム不能
2021年６月	ネバダ大学医療センター	ネバダ州	個人情報漏洩

立証されると、ランサムウェア攻撃による最初の死亡事件となります。この裁判は、今年（2022年）11月に予定されています。

ケース２：オレゴン州スカイレークス医療センター

～クリーン・バックアップデータが貢献～

ランサムウェア攻撃発覚日：2020年10月26日

スカイレークス医療センターは、半径160キロ内にほかの病院が存在しない地元唯一の基幹病院です。

病院がシステムの異常に気づいたのは、時間外のサポートチームが、IT システムとコンピュータの動作が遅いという電話を受けた後であり、システムは完全にオフラインになっていました。多くのサーバーや PC でランサムウェアが見つかりました。

経営陣の対応

経営陣は、即座に身代金の支払いに応じないことを表明し、院内2,500台のデバイスと600台以上のサーバーをすべてシャットダウンして被害の封じ込め対策を取りました。院内システム、電子カルテシステムは不能、業務系、臨床アプリケーションもオフラインになりました。その間、カルテの記入、処方箋は手書きになりました。

病院はサイバー保険に加入していたので、すぐに外部専門家の派遣を要請し、同時に、院内ネットワーク機器の契約先の Cisco 社を通じて、被害分析と復旧作業の支援を依頼しました。システム復旧に23日を要しました。

後の調査で発覚したランサムウェアの感染源

退職間近の職員が、退職時ボーナスと記載された偽メール（フィッシング・メール）を受け取り、その中の Google Drive へのリンクをクリックしてファイルをダウンロードしました。その時、PC の画面がおかしくなったので、コンピュータを再起動しましたが、このインシデントをセキュリティ部門に報告しませんでした。この

Case 2: Sky Lakes Medical Center, Oregon

～Clean backup data helped speedy data recovery～

Incident: October 26, 2020

Sky Lakes Medical Center is the critical access hospital for residents in the Klamath City area and there are no other hospitals within a 160 km radius.

The hospital was notified by their after-hours support team that computers were running slow and the system was completely offline. Ransomware was found on many servers and PCs.

The management decision

The management team immediately announced that they will not pay the ransom and started to shut down all PCs and servers, about 2,500 devices and more than 600 servers, to limit the spread. As a result, staff was forced to use pen and paper to fill out patient information.

Because of cyber security insurance, the hospital immediately brought an expert team. At the same time, they contacted Cisco for assistance with analysis and recovery.

How did the ransomware enter Sky Lakes Medical Center's system?

Staff coming to the end of his/her employment opened an phishing email and clicked a link to Google Drive and downloaded a file. At the time, the PC screen flashed and restarted the computer, but the incident was not reported to the security department.

時点でランサムウェアが院内システムに侵入しました。

事前対策の重要性

・政府や業界エキスパートが勧告するランサムウェア攻撃に対する復旧計画、システム稼働停止時の手順を確立していた。従って、システム停止時に、必要な情報をどこで入手できるかをスタッフが把握していた。
・クリーン・バックアップ・システムを導入していた。その結果、バックアップデータは不変（暗号化されなかった）だったことが、システム復旧の成功につながった。
・セキュリティ技術を導入していた。特定のイベントとそのデバイスの可視化が可能になった。（ただし、今回の攻撃は、その防護保護サービスを導入している最中であったため、実際に攻撃が発覚されたとき、PC隔離設定はできなかった）
・サイバー保険に加入していた。

Ransomware attack preparation is critical

-Established a disaster recovery plan against ransomware attacks as recommended by the government and industry experts. By following the experts' advice, when the system was shut down, the staff knew where to get the information when they needed it.
-Invested in immutable/clean backups that were not impacted by the ransomware.
-Installed security technology that provided visibility into specific events and their devices. However, since this attack occurred while the company was processing to install this service, it was not possible to use this service.)
-Purchased cybersecurity insurance

システム停止で想定外の出来事

院内のWi-Fiと電子メール送受信不可。Cisco社のウェベックス（Web会議）と個人の携帯電話で連絡を取り合った。

Unexpected event during system shutdown

Wi-Fi and e-mail sending/receiving in the hospital was disabled. The hospital communicated via Cisco's Webex (web conferencing) and personal cell phones.

スカイレークス医療センターから他の医療機関への提言

あなたの組織が外部電子メールの監視やファイアウォールの導入を検討をされているなら、躊躇しないで今すぐ実行してください。このような対策が遅れれば遅れるほど、危険にさらされる可能性が高くなります。

Recommendation to other healthcare organizations

If your organization is considering implementing external email monitoring and firewalls, don't hesitate to do it now. The longer you delay these measures, the more likely you are to be compromised.

ケース３：カリフォルニア州スクリップス・ヘルス

～万全の対策でもやってくる脅威～

ランサムウェア攻撃発覚日：2021年５月１日

サンディエゴの住民にも影響

Case 3: Scripps Health, California

～Well-prepared but the threat isn't going away～

Incident: May 1, 2021

San Diego residents are affected

Scripps Health is based in San Diego, California and operates

スクリップス・ヘルスは、カリフォルニア州のサンディエゴに拠点を置き、５つの病院と19の外来診療施設を運営する地域統合医療グループです（詳細は「医事業務」2020年６月１日号参照）。

ランサムウェア攻撃では、ネットワーク、電子カルテシステム、患者ポータル、さらに病院のホームページも停止し、アリゾナ州の外部バックアップサーバーも影響を受けました。脳卒中など重症患者を近隣病院に転送し、外傷患者の受け入れも一時的にできなくなりました。システム復旧までの４週間は、近隣の病院も過密状態に陥りました。

five hospitals and 19 outpatient care facilities.

The ransomware attacked Scripps and forced their system, EMR, their patient portal, down as well as affected an external backup server in Arizona. Without access to critical IT systems, patients with stroke and critical conditions were transferred to other facilities and their hospitals were unable to accept ER critical patients until the system was restored. It took about four weeks.

患者個人情報も漏洩

ネットワーク上に保存されている文書から147,267人の臨床データ、健康保険情報を含む患者個人情報とそのうち2.5％の人は社会保障番号や運転免許証番号の情報も漏洩しました。後に、この影響を受けた患者さんたちはスクリップスに対して、プライバシー侵害やセキュリティ侵害を理由に複数の訴訟を起こしました。

Personal patient information leaked

The personal information of 147,267 patients was stolen due to this incident. In addition to clinical data and health insurance information, 2.5% of them also had their social security numbers and driver's license numbers compromised. Later, the affected patients filed several class-action lawsuits against Scripps regarding their personally identifiable information and protected health information.

最新情報の公表を控える

スクリップスは、頻繁に最新情報を公開しなかった理由を、「現在の状況では、復旧作業の詳細をオープンにすることで、さらなる攻撃を受けるリスクが高まること。すでに、メディアで報道されている内容を利用して、院内に詐欺的な通信を送信する攻撃者がいる」と説明しています。

Releasing limited updated information

Scripps explained the reason for not releasing frequent updates: Releasing updated information in detail increases the risk of further attacks. Other attackers are already using what is being reported in the media to send scam communications to their organization.

国全体で取り組む

CEO のゴーダー氏は、６月10日付で地元の新聞への寄稿「ランサムウェア被害から学んだこと」で次のように述べています。（抜粋）

この１年、新型コロナウイルスのパンデミックの最前線で、医療機関がコロナウイルス対策に一段落ついたと思われた矢先、サイバーセキュリティの脅威がやってきました。

当院の職員は、緊急事態に備えて訓練を受けています。今回も、ランサムウエア攻撃に対して医師、看護師、スタッフはシステム不能時に、緊急対応計画の手順を実行しました。

しかし、ランサムウェア攻撃の大部分は、海外から平然と攻撃を仕掛けてくるのです。この状況では、我が国の医療機関とすべての機関が、ベストを尽くしても、脅威に立ち向かうには限りがあります。

相次ぐサイバー攻撃から得た教訓の一つは、この問題を管理し、それに立ち向かうための官民パートナーシップの必要性です。米国司法省は、米国政府がサイバー攻撃を国家安全保障に与える脅威として認識し、その捜査をテロと同様の優先順位に引き上げることを発表しました。

元 FBI 特別捜査官で病院セキュリティの専門家は、この脅威に対抗するには、「国家全体」のアプローチであると語っています。政府、法執行機関、民間企業が一体となって協力し、情報源を共有することで、我が国の重要機関とインフラを守ることができるのではないでしょうか。

100年に一度のパンデミック時に国民の健康を守るように、私たちの医療機関、重要なインフラ、学校、企業、政府機関を、犯罪者（サイバー攻撃）から守ることも大切です。

最後に

今回の３つの事例は、医療機関のサイバー攻撃は、人命にかかわり、この問題には官民で取り組む必要性を物語っています。

＊「メディケア相談員が語るアメリカの医療」の連載は、連載の開始とほぼ同時期に新型コロナウイルスの流行からパンデミックになりました。見通しが立たない中、日本から届けられる「医療業務」の特集や対談記事には随分励まされました。今回で、このシリーズの連載は最終回となりますが、新連載からは、さらに読者の皆様にお役にたてる情報を発信していきたいと思います。

医療機関の皆様には、このパンデミックの中、最前線で人命のために医療に従事していただき深く感謝申し上げます。Ⓜ

お断り：英訳は、日本とアメリカの医療制度に違いがあるため、意訳している部分があります。

※本稿の内容は情報提供を目的とするものであり、アドバイスやコンサルテーションを目的としていないことをご了承ください。

●ホームページ：https://e-kono.com ➡
今回の内容に関連する情報やアメリカの医療について紹介しています。

Conclusion

Cyber-attacks have been continuing for healthcare providers in the United States. This essay illustrates three cyber-attacks that caused life-threatening matters. It shows that in order to prevent them, we need the collaboration of the government and private corporations.

＊ This series started almost the same time as the pandemic began. During this pandemic, I was greatly appreciative of the Medical Services journal for encouraging me through their high quality reports. This will be the last article in this series. I look forward to a new series to provide the latest information to readers.

I would also like to express my deepest gratitude to all the healthcare workers for their commitment to patients' care during the pandemic.

Disclaimer: This essay is informational and educational purposes only and not intended to be a substitute for professional advice or consultation. If you seek any legal advice or professional consultation, please contact legal professionals or experts

■ Profile
河野圭子　米国病院経営士会認定病院経営士。薬剤師（日本）。ワシントン大学医療経営学部修士課程修了。フロリダ州サラソタ記念病院にて病院経営フェローシップ終了。アメリカの病院でビジネス開発アナリストや医療機関でボランティアを続けながら全米を縦横断し、現在は８州目のノースカロライナ州で認定メディケアカウンセラーとして活躍中。