人命にかかわるサイバー攻撃の脅威

医療機関向け サイバーセキュリティ対策とは

AMIYA

Index

■ はじめに 2
■ なぜセキュリティのリスクはゼロにならない？ 3
■ 医療機関のセキュリティ対策に重要な2つの考え方 4
■ 医療情報システムのセキュリティ対策 3つのポイント
① インターネット分離
～不正侵入防御 編～ 5
～侵入後の被害拡大防止 編～ 7
② バックアップ 9
③ アクセスログ 11
■ クラウドCSIRTサービス セキュサポ 12

はじめに

「過去の通院履歴がなにもわからない……」インターネットとは分離していたのに、なぜ電子カルテは被害にあったのか？

2021年10月、徳島県の病院がランサムウェアに感染。
この感染により、約85,000人分の患者の電子カルテが暗号化され、「いつ誰がどんな病気で通院し、何の薬を服用していたのか」など、診療に必要な全ての情報を見られなくなるという事態に（図1）。
復旧には約二か月を要し、その間、実質的な機能停止状態となってしまいました。
一般的な病院ネットワークは、メールやインターネットアクセスを目的とした「インターネット用ネットワーク」と、電子カルテや検査システムなどの重要情報を扱う「HIS（Hospital Information System：医療情報システム）ネットワーク」とに分離して運用されています。HISネットワークは外部からの攻撃に備え、インターネットへのアクセスを禁止しています。そのため、電子カルテなどの重要情報へ被害は及ばない想定でしたが……。

しかし現実には、徳島県の病院をはじめ、HISネットワーク内にある電子カルテシステムがランサムウェアに感染した報告が複数上がっています。いったいなぜなのでしょうか。
本ホワイトペーパーでは、「医療情報システムが抱えるサイバー攻撃のリスク」、そして「サイバー攻撃から守る方法」について解説します。

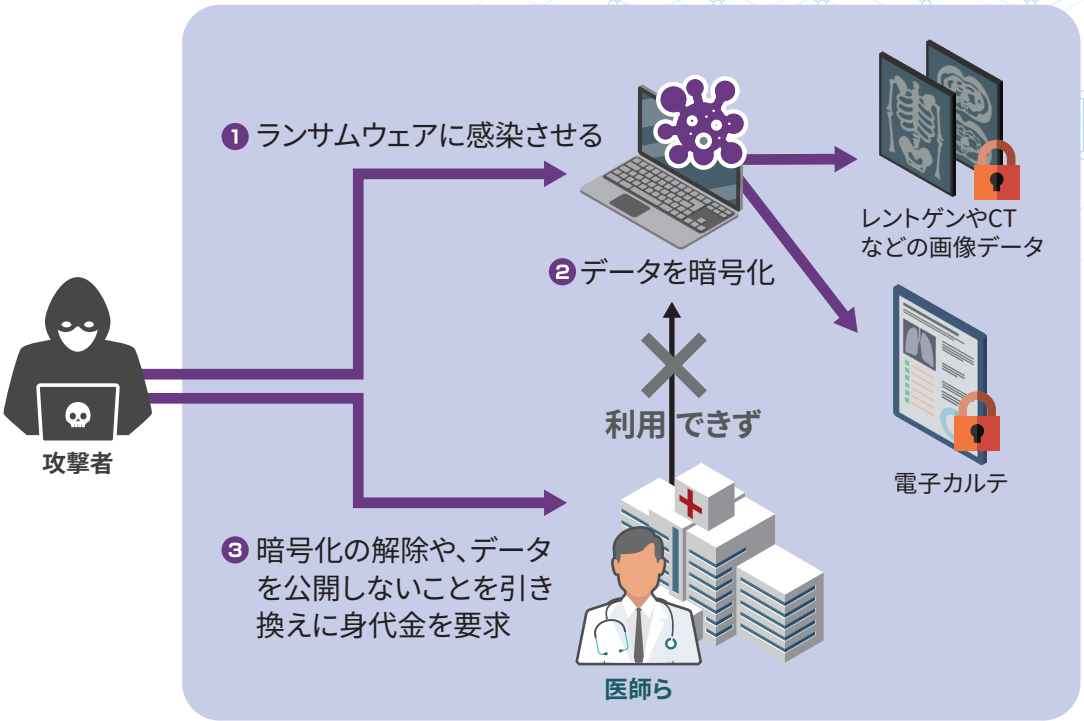

図1：医療機関へのランサムウェア攻撃のイメージ

なぜセキュリティのリスクはゼロにならない？

サイバー攻撃は事業継続を脅かすリスクに

最近のランサムウェアは、重要データを窃取するだけでなく、システムを広範囲に暗号化することで業務停止に追い込み、その事業継続と引き換えに身代金を要求するモデルへと変化しています(図2) 。

例えば、ランサムウェアの代表格である「LockBit 2.0」は、Active Directory(AD)のグループポリシーを悪用することで、Windowsドメイン全体のPC端末を自動的に暗号化する機能が搭載されています。ドメインコントローラーに侵入されたが最後、ドメインコントローラーで管理されるシステムすべてが一斉に被害にあうことになります。

このように、ランサムウェアは広範囲のデータをスピーディに暗号化するよう進化しており、病院ネットワークへ侵入を許してしまうと、医療情報システムが停止し、医療提供できない事態に陥ります。病院にとってシステムや業務の停止は、人命にもかかわる大きな脅威。その脅威に対抗するために、どのような対策を講じるべきか。まずは、その根幹となる「2つの考え方」について次項で詳しく見ていきましょう。

図2:ランサムウェア攻撃の目的の変化

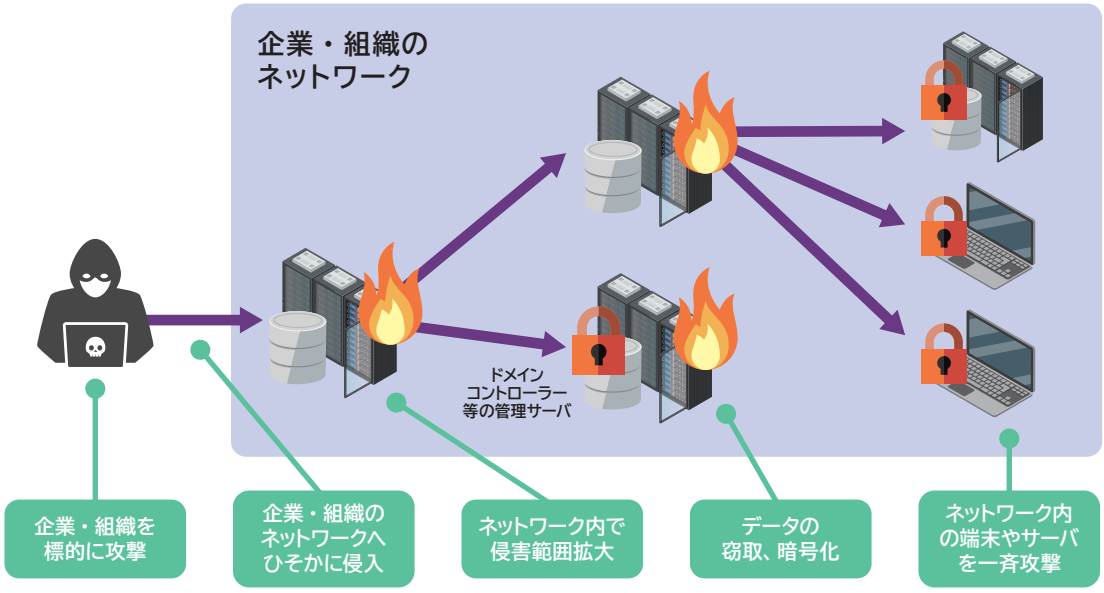

図3:「LockBit2.0」の攻撃手法

医療機関のセキュリティ対策に重要な2つの考え方

①「狙いやすいターゲット」にならないための対策

まず抑えておきたいポイントは、どれだけサイバー攻撃対策をしても「リスク発生の可能性はゼロにはならない」ということ。サイバー攻撃の脅威と対策はイタチごっこの状況で、最新の脆弱性を解消しても、攻撃者は次々と新規の脆弱性を発見し、都度新しい攻撃方法が開発されます。多額のコストをかけたとしても、全てのサイバー攻撃に対応することは事実上不可能と言えるでしょう。

さりとて、攻撃者はセキュリティ対策が不十分な、簡単に攻撃できるターゲットを狙います（図4）。
その方が手間なく目的（ランサムウェアなら重要データの暗号化と金銭要求）を達成できるからです。裏を返せばそれは、セキュリティ対策によってリスクを低減することで、サイバー攻撃のターゲットになる可能性も低くなるということを意味します。

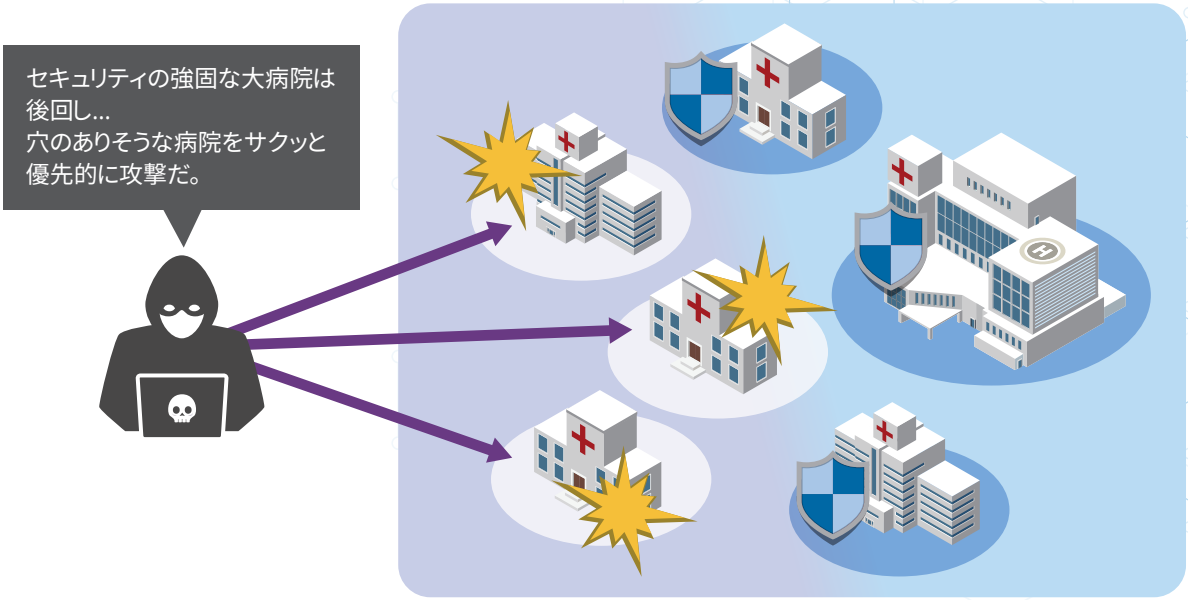

図4：狙いやすいターゲット

②「選択と集中」で効果的なセキュリティ対策

次に重要な考え方は、「守るべき資産を明確にし、その資産が持つリスクに対してリソース（人材、費用）を集中する」ということ。セキュリティ対策費用が潤沢にあり、さまざまな対策を講じられる病院は限られています。限られたセキュリティ対策予算の中で、サイバー攻撃のリスクを最小化するためには、より効果的・効率的な対策を実施していく必要があります。
そのためにはまず、守るべき資産を明確にすることが重要です。

一般的な病院であれば、最優先で守るべき資産にあたるのは「電子カルテなどの医療情報システム、及びそのデータ」ではないでしょうか。特に電子カルテシステムが持つリスクは、システムの停止、データの損失、個人情報の漏洩など、甚大な影響をもたらすものと考えられます。限られたリソースの中で効果的なセキュリティ対策を実現するためには、こうした「より重要度の高いリスクに、優先的にリソースを集中する」と言った考え方が必要です。

医療情報システムの セキュリティ対策 3つのポイント

ここからは具体的な対策として、今あるHISネットワークをベースに、必要最小限の投資コストで実現可能なセキュリティ対策を解説します。ポイントは3つ、「①インターネット分離」、「②バックアップ」、「③アクセスログ」です。一つずつ詳しく見ていきましょう。

①インターネット分離 ～不正侵入防御 編～

病院におけるセキュリティ対策で、コストパフォーマンスに優れる最も強固な対策と言えるのが「医療情報システムをインターネットと分離すること」(図5)です。
ほとんどのサイバー攻撃はインターネットがなければ成立しません。ランサムウェアの代表格である「LockBit 2.0」も、攻撃対象のネットワークにインターネットを経由して侵入するところからすべてが始まるため、インターネットから分離しておけば、”ほとんど”のサイバー攻撃を防ぐことができるでしょう。
しかし残念なことに、前述した通りゼロにはならないのがセキュリティリスク。実際に徳島県の病院では、インターネットと分離していたにも関わらず、ランサムウェアの被害に遭ってしまいました。
なぜか？　答えは明快、「インターネットと完全に分離されていなかったから」です。

	インターネット接続ネットワーク	HISネットワーク
用途	・メール ・インターネット	・電子カルテ ・予約受付システム ・検査システム
個人情報の利用	利用なし	利用あり
インターネット接続の有無	あり	なし

図5:一般的な病院ネットワークの構成

完全なインターネット分離は至難の業

医療情報システムの「リモート保守用VPN」や「地域医療連携ゲートウェイ」、「遠隔地バックアップシステム」など、完全にインターネットと分離できない環境というのが存在します。
またクラウドサービスの普及により、インターネットの利用はこの先さらに広がるでしょう。攻撃者はこの「インターネットと接続せざるを得ないシステム」を経由してサイバー攻撃を仕掛けます。サイバー攻撃の被害に遭う確率を下げるためには、インターネットアクセス可能なシステムのセキュリティを適切に管理することが重要です。

インターネットアクセス可能なシステムの脆弱性に注意

では、運用上インターネットアクセスを許可しなければならないシステムのセキュリティ対策はどうするべきか？まず第一に、「脆弱性への迅速な対応」です。近年増加しているVPN機器を狙ったサイバー攻撃は、VPN機器の脆弱性を突いてきます。増加している要因は主に、「世界中から攻撃ができること（VPN機器がグローバルIPアドレスを持つため）」、「VPN機器の脆弱性が放置された機器がたくさん残っていること」の2つ。この脆弱性に対するセキュリティパッチはメーカーから提供されているため、適用すれば攻撃を防ぐことができるのですが、未適用のまま放置されている機器は今も多く残っています（図6）。
グローバルIPアドレスを持ち、世界中どこからでもその機器へアクセスできるシステムは、より一層、脆弱性を適切に管理する必要があります。

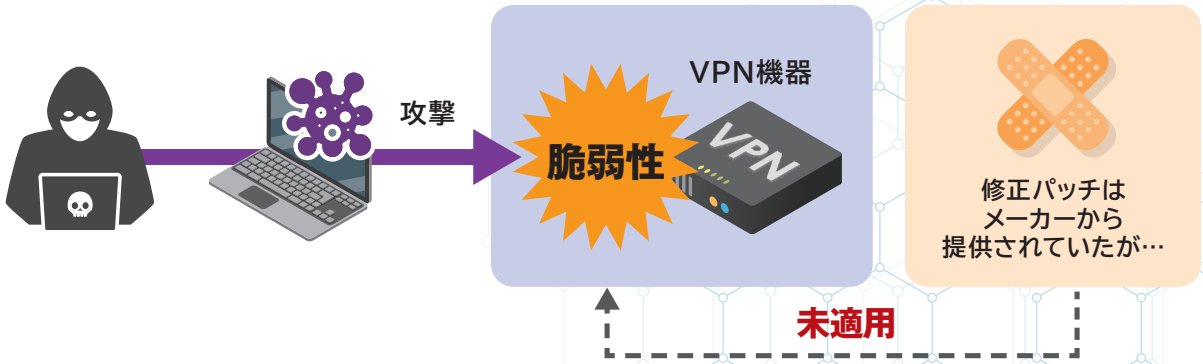

図6：放置される既知の脆弱性

「脆弱性診断サービス」 脆弱性対策に

脆弱性を適切に管理するためには、「脆弱性がある」ことを知るところから始まります。
その方法は二つです。
一つは、「グローバルIPを持つ機器をリスト化し、定期的に公開されている脆弱性について確認する」という方法。これは適切に運用できれば、その機器が持つ脆弱性をゼロにすることができるのですが、機器が増えるほど管理の手間がかかるのが難点です。

もう一つは、グローバルIPをもつ機器に対して「定期的に脆弱性スキャン」をすることです。
半自動的にできるため、機器が増えても手間が増えないことがポイントです。注意点としては「全ての脆弱性を検知できるわけではない」ということ。どうしても漏れは生じてしまいます。とはいえ、攻撃者自身もこの方法で脆弱性のある機器を探していることから、攻撃者と同じ視点で脆弱性をなくしておけば、かなりの確率でサイバー攻撃を防ぐことができるでしょう。

インターネット分離 ～侵入後の被害拡大防止 編～

不正侵入されることを想定に。被害を最小限にする対策とは？

これまでは、HISネットワークに外部から不正侵入されない対策として、インターネット分離とその注意点について解説しました。インターネット分離により不正侵入しづらい環境にはなりましたが、その可能性をゼロにすることはできません。

そこで、不正侵入されたとしても、被害を最小限に（事業継続に影響しない程度に）する対策についても解説します。

定期的なアップデート

サイバー攻撃の常套手段として、不正侵入後、HISネットワーク内のシステムに対してさらに不正アクセスを試み、電子カルテシステムやその他の重要システムへの侵入を企てます。ここで利用されるのが、PCやサーバ、アプリケーションが保有している脆弱性です。その脆弱性をつき、システムの管理者権限を奪取した後、ランサムウェアを実行させます。つまり、HISネットワーク内のシステムに脆弱性がなければ、攻撃者はその先の攻撃をすることはできません（図7）。

HISネットワーク内のシステムも積極的にアップグレードして、脆弱性をなくしていくことがオススメです。

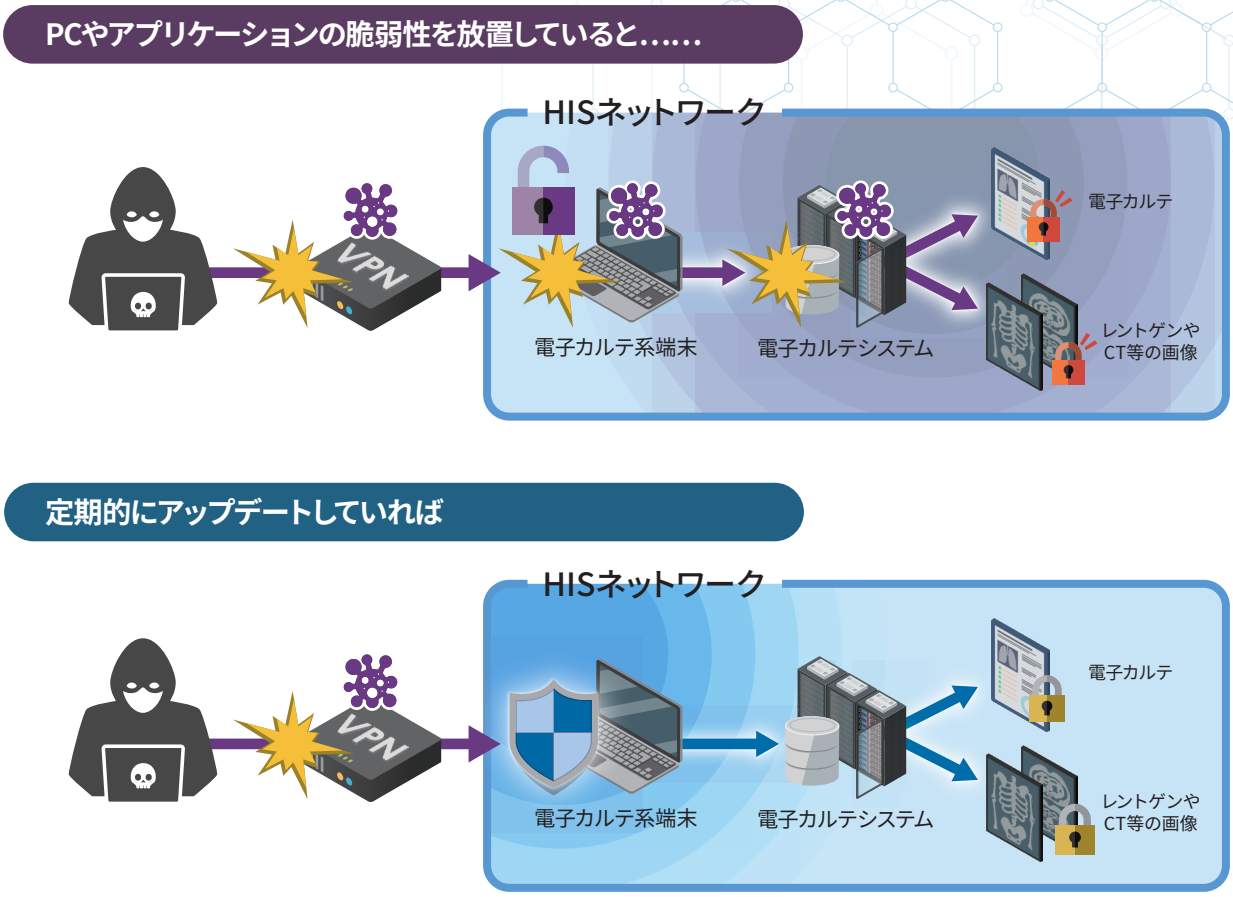

図7：定期的なアップデートの重要性

「Webプロキシ」 アップデート対策に

HISネットワークはインターネット分離が基本原則です。
アップデートさせるためには、安全なインターネットアクセスが必要となりますが、ではインターネット分離しているHISネットワーク内のシステムはどのようにアップデートすればいいのでしょうか。
そこでオススメなのが、Webプロキシの導入です。
Webプロキシは、そのシステムの代わりにWebアクセスをしてくれるシステム。アクセスするサイトを制御できるため、各システムのアップデートパッチのダウンロードサイトのみにアクセスを限定することで、危険なインターネットにアクセスすることなく、定期的なアップデートが可能となります(図8)。
このように、インターネット分離環境におけるインターネットアクセスポリシーはホワイトリスト運用がベースになります。例えば、Windowsのアップデートだけしたいので、インターネットアクセスはWindows Updateサイトに限定するというイメージです。

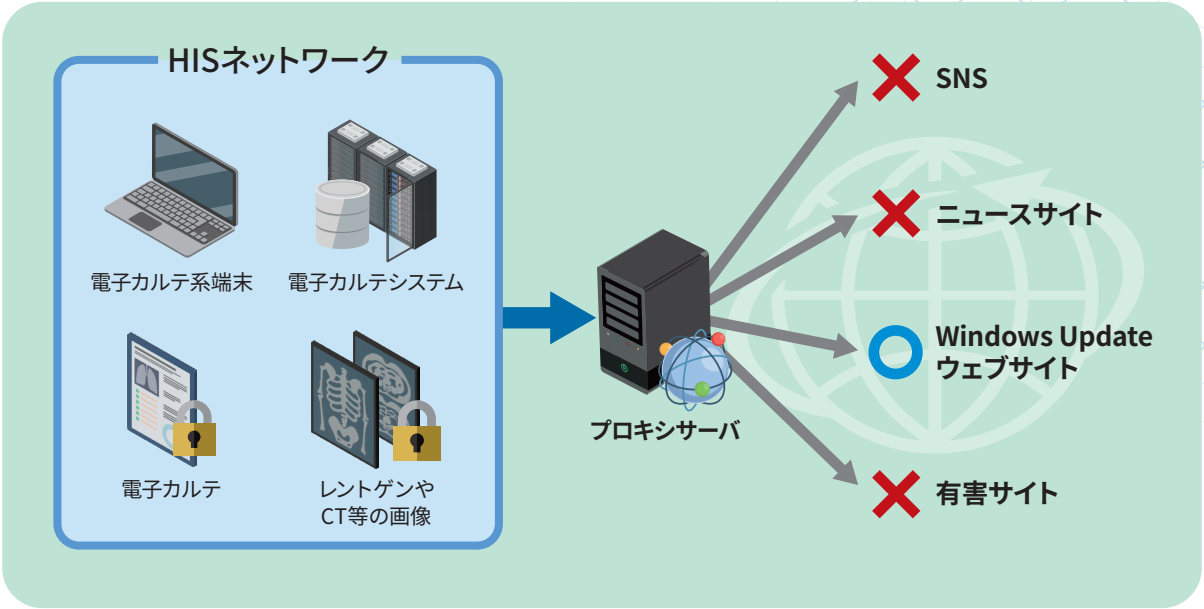

図8:Webプロキシがアクセスできるサイトを制御

「管理者権限の剥奪」 被害拡大防止に

前述したサイバー攻撃の常套手段にある通り、ほとんどのサイバー攻撃は管理者権限の奪取が不可欠です。
サイバー攻撃を完遂するためには、ランサムウェアなどのアプリケーションの実行や設定変更をする必要があり、これらの実行には権限が限定されている標準ユーザーでは不十分だからです。
もちろん標準ユーザーから脆弱性を攻撃して権限昇格するケースも想定されますが、その際にはさまざまな痕跡が残るため、サイバー攻撃を検知することが可能です。ユーザーに不必要なアプリケーションをインストールさせないためにも、標準ユーザーで運用することをオススメします。

② バックアップ

これまで、インターネット分離をテーマに「HISネットワークに侵入させないための方法」、「HISネットワークに侵入されたあと被害を最小限にする方法」をそれぞれ解説しました。ここからは、事業継続に影響を与えないためのさらなる対策として、「重要データのバックアップ」にテーマを移してお話しします。

というのも、ランサムウェアの被害を受けた際には、重要データが暗号化され、診察ができなくなったりと事業継続に多大な影響を及ぼすことが想定されます。万が一被害にあった場合でも、バックアップから重要データを復旧できる体制にしておくことが重要です。

バックアップも暗号化してしまうランサムウェア。その対策は？

そうはいっても、ただバックアップを取得しているだけでは、ランサムウェア対策としては安全と言えません。徳島の病院では取得しているバックアップも含めて、ランサムウェアの被害にあっています。
バックアップの仕組み上、バックアップデータを保存するためにはその端末からバックアップサーバへのディスクアクセスをする必要があります。ランサムウェアはこの経路を悪用し、バックアップもすべて暗号化してしまうのです（図9）。

この状態では、せっかくバックアップを取っていたとしても、感染端末からディスクアクセスできる領域（内蔵ディスク、外付けディスク、ファイルサーバ共有、ネットワークドライブなど）はまとめて被害にあってしまうでしょう。また、ランサムウェア「LockBit2.0」には、ローカルドライブにマッピングされていない隠しパーティションを含むコンピュータ上の全てのボリュームをスキャンし、マウントした上で暗号化する仕組みが搭載されています。

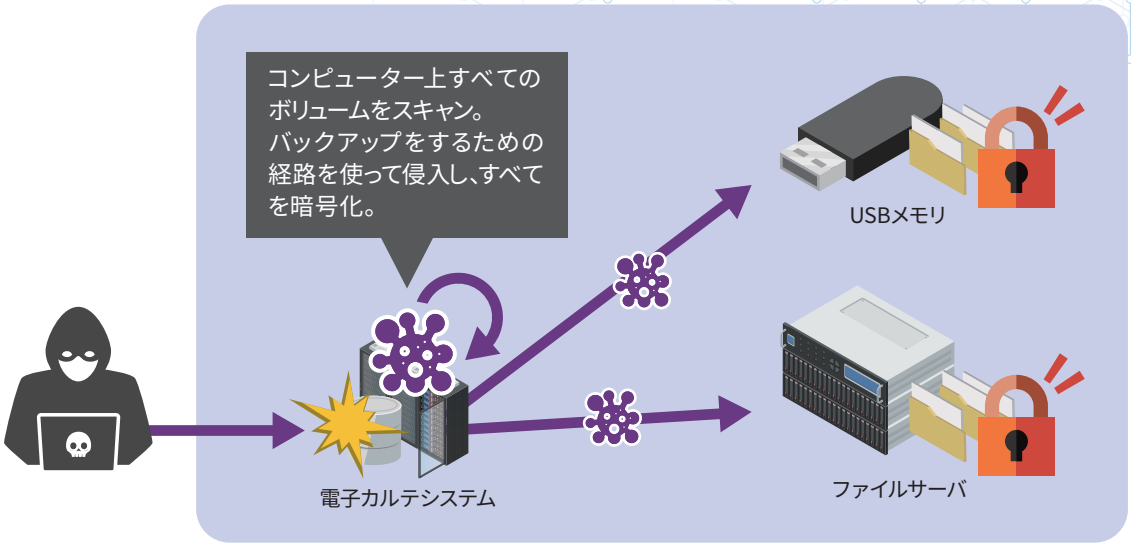

図9：ディスクアクセスの経路を悪用するランサムウェア

3-2-1ルールを適用 バックアップ対策に

データ保護の基本ポリシーとして、アメリカ合衆国国土安全保障省が公表した「3-2-1ルール」。これは、「保護したいデータを3箇所に保持する」、「2つの異なる形態のデバイスに保存する」、「1つをオフサイト(別の場所)に保存する」というポリシー(図10)です。
例えば、業務システムデータをネットワークドライブにバックアップ(一次)し、さらにそれをテープ(異なる形態のデバイス)に書き出すことでオフサイトバックアップ(二次)にも対応するという構成です。

ランサムウェアは、オフサイトに保管されているテープ上のデータを暗号化できません。そのため、もし一次バックアップデータが暗号化されても、テープ上の二次バックアップはから復旧できます。これはランサムウェアなどのサイバー攻撃以外にも、災害やシステム障害などのBCP対策としても有効です。

オフサイトにはクラウドがおすすめ バックアップ対策に

オフサイトにバックアップを取る方法して、オススメしたいのがクラウドストレージへのバックアップです。クラウドならバックアップサーバの運用や初期投資が不要で始められる上、データの削除や上書きを防止できる「オブジェクトロック機能」(図10)が搭載されているものがあります。

クラウドストレージに保管したデータをランサムウェアによって書き替えられることを想定して、「オブジェクトロック機能」でそもそも書き換えられないようにしておくことがポイントです。クラウドストレージ選定の際にはぜひ、この機能が搭載されているかをチェックしてください。

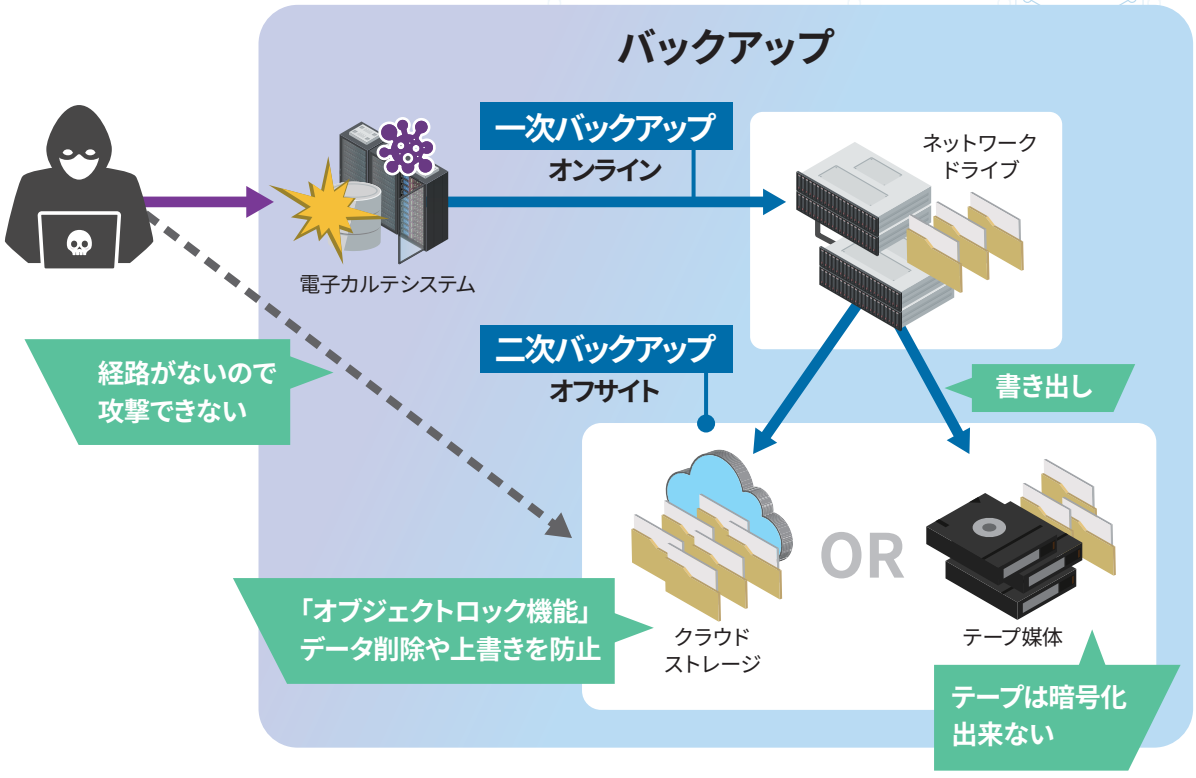

図10:「3-2-1」ルール

③ アクセスログ

それでは最後のテーマ「アクセスログ」を見ていきましょう。アクセスログといえば、個人情報へのアクセスログをシステムから取得し、不正利用がないかを確認することで内部のメンバーが不正をしていないかをチェックするといった、内部不正対策としての側面が有名です。厚生労働省の「医療情報システムの安全管理に関するガイドライン」においても、『個人情報を含む資源については、全てのアクセスの記録(アクセスログ)を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。』と明記されています。しかしこのアクセスログ、内部不正だけではなく、サイバー攻撃についても非常に有用です。システムログがあれば、サイバー攻撃を受けていることにいち早く気づけますし、その予兆を検知することで、サイバー攻撃の最終目的が達成していないタイミングで被害を食い止めることができます。

サイバー攻撃の流れに沿ってログを取得

では、サイバー攻撃を検知する上で、どのようなログを取得するべきでしょうか？もちろん全システムのログを取得しておくことが理想的ですが、現実的ではありません。サイバー攻撃の流れに沿って、そのシステムのログを取得することが最も効率的かつ、現実的と言えるでしょう。HISネットワークへのサイバー攻撃は、「①インターネットとの接点(VPN機器など)から侵入」し、「②サーバやPCへ不正侵入」、「③ランサムウェアなどのマルウェア実行」が一般的な流れになります。そこで、その経路上のシステムからログを取得しておけば、そのポイントごとにサイバー攻撃を検知することができます(図11)。

VPN機器の認証ログを取得しておけば、メンテナンス業者から申請のなかった不正な時間帯のアクセスや海外からのアクセス、大量の認証失敗などが把握できますし、Windowsサーバの認証ログであれば、いつもと違うIPアドレスからのログオンや存在しないアカウントでのログオン試行などがわかります。これらのいつもと違う動きに対してアラートやレポート設定をし、定期的にチェックすることでサイバー攻撃を検知することが可能に。何かあった時の原因分析や証拠のためだけではなく、サイバー攻撃対策としても有効活用できます。

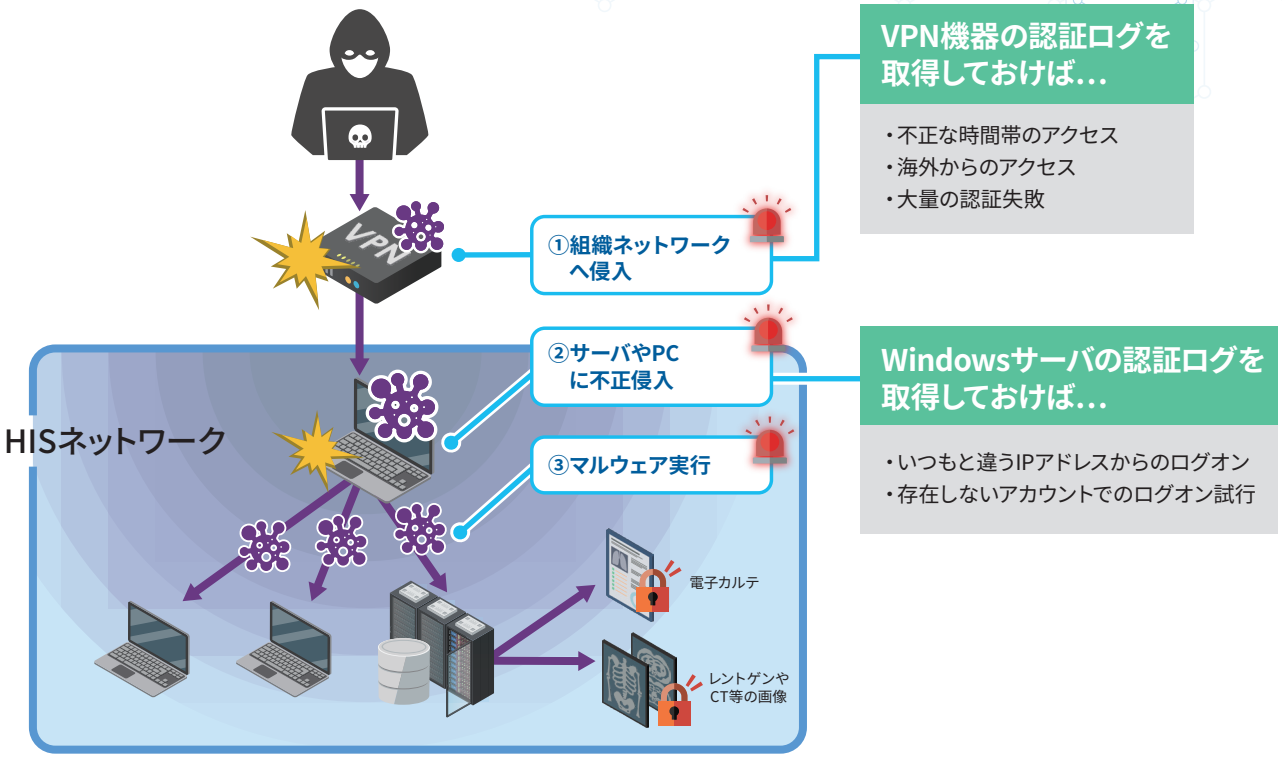

図11:一般的なサイバー攻撃の流れ

おわりに

「サイバーセキュリティ対策に注力したいけれど、人材の確保も予算投資も難しい……」

本資料では主に、医療機関におけるサイバーセキュリティ対策の重要性と具体策についてお話してきました。繰り返しになりますが、サイバー攻撃によって医療システムが停止するということは、最悪の場合、患者様の健康や生命にも関わる問題へと発展します。その危機感から「早急な対策が必要」というのは、誰しも共通の認識としてあるのではないでしょうか。

しかし「そうはいってもね……」という現実があるのも確かです。サイバー攻撃から身を守るためには、対策のためのリソース確保やポリシー策定といった態勢整備、予算策定、サービス選定など、課題がたくさん存在します。「そもそも、何から手をつけてよいかわからない」と出だしからつまずいてしまう医療機関も多いのではないでしょうか。

医療分野のサイバーセキュリティ強化をワンストップで提供 セキュサポ

サイバーセキュリティの専門チームが検知ツールの導入・設計から、インシデント対応までを一貫して実施。
「ポリシー決め」や「リスク分析」といった概念的なセキュリティ対策だけではなく、企業様ごとの環境や業務状況に即した、実現性の高いセキュリティ対策を提案します。

サイバー攻撃対策
お客様環境に検知システムを設置し、サイバー攻撃の常時監視を遠隔で行います。

内部不正対策
内部からの不正を常時監視し、不穏な行動を事前にレポートします。

脆弱性対策
お客様の公開サイトを脆弱性検査し、問題の指摘とその改善を行います。

強化レポート
セキュリティの対策を証明する各種レポートを定期的に提出します。

インシデントレスポンス
攻撃/侵入を検知したら、インシデントレスポンス(原因や影響範囲の調査など)を行います。

サイバー保険
インシデント発生時に起こる過大な調査費用をサイバー保険でカバーします。

セキュリティ相談窓口
不審なメールの安全確認など、セキュリティ上の不明点があれば、相談いただけます。

セキュサポ

セキュリティ専門チームがお客様の環境全体を監視し、ランサムウェア攻撃をはじめとした一連のサイバー攻撃への対策を包括代行。コストと手間を減らしながら最高のセキュリティレベルを月額固定料金でご提供します。

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋
データセキュリティ事業部

TEL：03-6822-9996　E-mail：bv-sales@amiya.co.jp

詳しい製品概要資料はこちら

開発元

AMIYA 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999　FAX: 03-6822-9998

https://www.amiya.co.jp/

販売元