

WATSON Coaching & Consulting Group

医療におけるサイバーセキュリティ Vol.1

現状と基本的対策

A hand holding a glowing digital sphere with the text "CYBER SECURITY" overlaid in a metallic, textured font. The background is dark with some abstract light patterns.

CYBER SECURITY



CONTENTS

はじめに	3
1. サイバーセキュリティとは	4
2. サイバー攻撃被害と今取るべき対処	6
国内医療機関における被害例	7
今とるべき対策	8

はじめに

国内医療機関におけるサイバー攻撃による被害は、増加の一途を辿っている。サイバー攻撃にはいくつかの種類があるが、近年著しく増加が目立つのは暗号化したデータを人質に身代金を要求する「ランサムウェア」と呼ばれるものだ。

医療機関が狙われるのには理由がある。大別すると次の3つが考えられる。

- ① 医療機関はマイナンバー、病歴や投薬歴、患者の個人情報など、情報の転売や恐喝に悪用されやすいデータが大量に存在すること
- ② ITの要員不足や不在などから、他の業界に比べ、OSのアップデートやセキュリティパッチの適用、バックアップ対策などが遅れがちであること
- ③ 医療行為という社会的責任の重い業務であるため、身代金要求に応じやすいと犯罪グループから見られている可能性が高いこと

サイバー犯罪はきわめて攻撃的犯罪であり、ひとたび被害を受ければその影響は甚大だ。攻撃には先ず守りを固めることが何より重要である。

本ホワイトペーパー ではその第一歩を示す。

1. サイバーセキュリティとは

「サイバー」とは、一般にコンピュータやネットワーク上に構築された仮想的な空間のことを指す。わかりやすくするために「インターネット空間上のこと」と捉えて良いだろう。「セキュリティ」とは、危険や脅威から何かを守ることだ。つまり、サイバーセキュリティとはインターネット上に広がるコンピュータのネットワーク空間を利用したさまざまな危険や脅威、リスクなどから身を守ることを意味している。そしてそこで起こる犯罪がサイバーテロやサイバー攻撃、サイバー犯罪などである。

サイバーセキュリティという言葉は2010年前後をターニングポイントとして盛んに使われるようになった。理由は、この頃からサイバー攻撃や関連犯罪が急増したためだ。具体的には、

- ① 攻撃対象が産業界に広まった
- ② 攻撃方法が高度化し、標的を定めた攻撃が急増した
- ③ 国家によるサイバー攻撃、金銭目的のサイバー犯罪が増えた

この頃以降、サイバー領域は犯罪防止及び軍事的な目的からきわめて重要なものとなった。2011年以降、米国ではその安全保障においてサイバー領域は、陸・海・空・宇宙に次ぐ5番目の重要領域とされている。日本においても2013年の「国家安全保障戦略」でサイバー空間への防護が国家戦略に盛り込まれた。以降、サイバーセキュリティは国際政治・安全保障の問題として扱われるようになっていく。

サイバー空間に関するISOの定義

the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

人間、ソフトウェア、およびテクノロジーデバイスやそれに接続するネットワークを用いたインターネット上のサービスのやりとり (interaction) の結果として生じる複雑な環境で、いかなる物理的形態も存在しないもの

— *ISO/IEC 27032:2012

*International Organization for Standardization (国際標準化機構)

International Electrotechnical Commission (国際電気標準会議)

そして、昨今、こうしたサイバー攻撃や関連犯罪が医療分野においても急増しており、厚生労働省も神経を尖らせている。

医療機関においても企業同様にさまざまなサイバーセキュリティ対策が求められるが、まずその前提となる基本的な重要事項を知っておく必要がある。それは次の3つだ。

- ①**機密性 (Confidentiality)**: 情報へのアクセスを認められた者だけがその情報にアクセスできる状態を確保すること
- ②**完全性 (Integrity)**: 情報が破壊、改ざん又は消去されていない状態を確保すること
- ③**可用性 (Availability)**: 情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること

これら3点は「情報セキュリティ」においてきわめて重要とされる基本的要件であるが、サイバーセキュリティにおいても同様に重要となる。

その上で、次の3点への配慮も重要とされる。医療においては患者の健康を預かる観点から尚更重要だと言える。

- ① 健康 (Health)
- ② 安全 (Safe)
- ③ 環境への影響 (Environment)

サイバーセキュリティ対策 3つの重要ポイント

C・I・A

- ①**機密性 (Confidentiality)**
- ②**完全性 (Integrity)**
- ③**可用性 (Availability)**

2. サイバー攻撃被害と今取るべき対処

国内医療機関においてもランサムウェアなどのサイバー攻撃が増加傾向にある。ランサムウェアとは「Ransom（身代金）」と「Software（ソフトウェア）」から生まれた造語だ。医療機関のコンピュータにウィルスを忍び込ませ、データを暗号化して「暗号を解いてほしいければ身代金を支払え」と脅す。「支払わなければ機密データを漏洩させる」と追い討ちをかける。あるサイバーセキュリティ関連企業のレポートでは、2021年にサイバー被害を経験した人は国内で1620万人、世界では4億1500万人と推定されるという。

事態を重く見た厚生労働省は、今年3月1日に「サイバーセキュリティ対策の強化について（注意喚起）」を示し、医療機関をはじめとする重要インフラ事業者等に対し、サイバー攻撃の脅威に対する認識を深めるとともに、リスク低減のための措置等を講じることによりセキュリティ対策の強化に努めるよう要請した。そして4月からは医療を含む14の分野でサイバーセキュリティ対策を講ずることが義務化された。

今、重要なことは、先ずどの医療機関でも対応できることとして、「パスワード管理の徹底」「本人認証の強化」「システム上の対応」「バックアップデータの確保」などを行うとともに、事案が発生した際の対応などを事前に整理・文書化し、院内で周知・徹底しておくことが欠かせない。また、サイバー攻撃は患者への影響も大きいため、日頃からサイバーセキュリティに関する啓蒙活動を推進することが重要だ。医療機関にも情報セキュリティ責任者を配置し、組織的に取り組むことが不可欠である。

サイバー攻撃被害 (2021)

世界： 4億1500万人
日本： 1620万人

HACKED

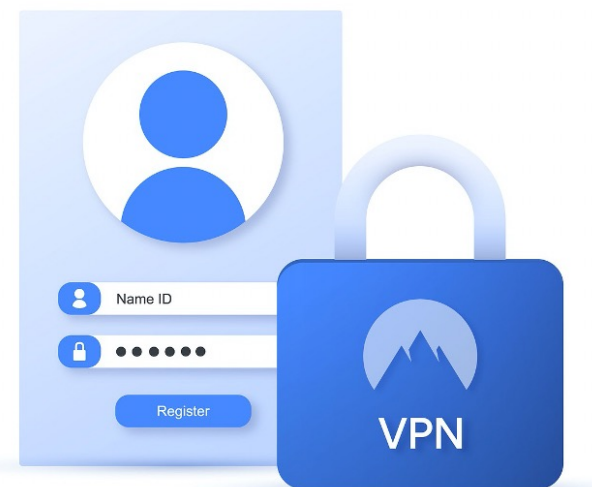
国内医療機関における被害例

すでに多くのメディアが報道しているが、昨年10月、徳島県つるぎ町にある町立半田病院でその被害は発生した。サイバー攻撃を受け、電子カルテが暗号化された。そして院内のすべてのシステムがダウン。病歴、診療歴、投薬歴その他、85000人分の患者情報全てが閲覧不可能となった。

システムはすべて死んだ状態。予約票もない。入院患者のことが何も分からなくなっただけでなく、今日、外来に誰が何時に来るかもわからない。病院にとっても患者にとっても地獄のような日々が2ヶ月も続いた。この間、患者情報はすべて手書きで対応したという。

脆弱と見られたVPNが狙われたようだ。国内の複数の企業・団体などが標的となり、そのうちのひとつが町立半田病院であった。病院、スタッフ、患者、地域、医療ITベンダー。関係者の必死の努力と協力により同年12月末、ようやくシステムは復旧した。

犯人はサイバー犯罪集団であることは間違いなく、世界のどこから攻撃されたのかはわからない。ひたすらに日々の病院運営をこなしてゆくしかない地獄のような2ヶ月。「システムが復旧したときは、本当に嬉しく涙がでた」と報道にあった。



今とるべき対策

今後の被害に備えるために、厚労省や内閣官房など国の複数機関が連名で医療機関に次の対策を求めている。

■ リスク軽減のための措置

- ① 単純なパスワードを使用しない（パスワードの全てまたは一部において、abcd, 1234, 223344, など）
- ② 本人認証を強化する（アクセス権強化、多要素認証活用、使っていないアカウントの削除など）
- ③ IoT機器を含むデバイスを検証する
 - ・VPNをはじめネットワークに接続された機器のセキュリティパッチや更新プログラムを速やかに適用する
- ④ 組織内の周知徹底
 - ・届く予定のないメール、知らない相手からメールの添付ファイルは絶対に開かない。URLも不用意にクリックしない。
 - ・不審なメール等は情報セキュリティ責任者に速やかに報告する
- ⑤ （情報セキュリティ担当は）サーバーの各種ログを頻繁に確認する
- ⑥ （情報セキュリティ担当は）通信の監視・分析、アクセスコントロール等を再点検する
- ⑦ データのバックアップを徹底する（3-2-1ルール適用）

その上で、医療機関は情報部門を強化することが急務となる。情報部門をもたない医療機関は情報部門を早急に設置すべきだ。そして医療機関の規模にかかわらず情報セキュリティ担当者を（外部からの採用を含め）配置する。そうしなければサイバー攻撃への対策を施す術はない。

3-2-1 ルール

321ルールとは、データのバックアップを取る際の理想的な方法のひとつとされる考え方である。

321ルールは「データはコピーして3つ持つ」（二重にバックアップを取る）、「2種類の（種類の異なる）メディアでバックアップを保存する」、「バックアップのうち1つは違う場所で保管する」、という3要素からなる。これを履行することで、保存した記憶媒体に不具合が生じたり、バックアップファイルごと攻撃・抹消されたり、あるいは災害などによってオフィスに立ち入ることができなくなったとしても、データが復旧可能な状態を維持できる。

近年では「SAMAS」をはじめとする凶悪な手口のランサムウェアも登場してきており、データの適切なバックアップは改めて重要視されつつある。

Source: IT用語辞典バイナリ

サイバーセキュリティ対策はお済みですか？

セキュリティソフトを導入するだけでは不十分です。

まず重要なのは、

- ① 院内の危機意識と対策の必要性の認識
- ② 情報管理の現状把握とあるべき姿の理解
- ③ 部門を超えた院内全体の協力体制

セキュリティソフト導入と運用体制の整備は最後のステップです。

伴走型コンサルティングでサイバー犯罪対策立案をお手伝いいたします。

お気軽にご相談ください。

WATSON Coaching & Consulting Group

<https://www.mycoachwatson.com/>

メールでのお問合せもお気軽に info@mycoachwatson.com まで