特集1
今そこにある危機
放射線診療のBCPを考える
Business Continuity Plan

1. サイバー攻撃を考慮したシステム構築の実際

近藤　博史　鳥取大学医学部附属病院医療情報部 / 日本遠隔医療学会会長

孫子の言葉に「知彼知己，百戦不殆（彼を知り己を知れば百戦殆うからず）」とあるとおり，サイバーセキュリティを考える場合，最近のサイバー攻撃の状況を知ることが重要である。その上で，現状の己の状況を確認し，将来を見据えた対策を考える必要がある。

昨今，医療デジタルトランスフォーメーション（DX）と呼ばれるように，今後の医療はインターネット上に広がっていく。オンライン診療もその一つで，医療の対象が感染症から糖尿病，高血圧，高脂血症など生活習慣病に変わり，発症前の“未病”の段階からの介入が患者の人生にも医療費にも有効とわかったため，スマートフォンを使ったモバイル・ヘルス機器の利用が中心となっていく。実際には，「continuous monitoring and timely intervention（連続したモニタリングから適時な介入）」が期待される。治験もインターネットを介した対象者の抽出，治験実施のモニタリングと適時な脱落予防が可能になる。

一方，この変化に対して日本の医療機関は，これまで個人情報保護法対策で閉じたネットワークを使い，ベンダーも医療担当部署にセキュリティ専門家が入っていない状況である。また，大学病院，自治体から診療所，在宅医療，往診，訪問看護，介護支援などの小規模の組織が今後つながっていくことも，サイバーセキュリティを考える上で重要である。

敵を知る

“ボットネット”と呼ばれるサイバー攻撃の仕組みをご存知ない方が多いように思う。ロボットネットの略だが，「クラッカーの自由になるインターネット上の感染したPC群のこと」と言える。メールやホームページなど，種々の方法でウイルスを感染させるが，クラッカーがコンピュータに侵入するための裏口（バックドア）を開け，ウイルス対策ソフトウエアの機能を停止させるなど，多段階的に順次ウイルスを感染させ，自由にできるようにし，静かにしておく。時に感染したPCをスパムメールの踏み台やメール発信に使用し，この多数のPCから標的のサーバに過剰な負荷を与えるDDoS攻撃をし，サーバに入り込むなど種々の活動に使われる。以前，1つのボットネットが摘発されて，鳥取大学のメール数が有意に減少した経験もある。すでに，インターネットにつながったPCの多くが感染しているとも言われている。

ゼロ・トラスト時代のEDR

これまで組織のサイバーセキュリティでは，インターネットからの入口にファイアウオール（以下，FW）を設置して通信制御し，IDS（不正侵入探知システム）やIPS（不正侵入防止システム）などにより通信を監視して，メール添付のウイルス除去，怪しい添付ファイルの分離などでウイルス防御をしていた。同時に，各端末にウイルス対策ソフトウエアを入れ，ウイルスパターンファイルを更新し，端末でのウイルス検知防御もすることで2段階の対策をしてきた。しかし，ここ数年，検出されない亜型ウイルスが増加し，対策ソフトウエアを多重装備するところも出てきている。鳥取大学では，IPSで感染後の大量の流出通信を検知して発覚することも多い。

近年，日本でもランサムウエアの被害が増えた。ランサムウエアは重要ファイルの暗号化を行い，その暗号を解くカギを高額で買い取らせるもので，感染後の大量の流出通信がないのでIPSでも検知防御が困難である。2017年に英国の医療ネットに被害を与えた“WannaCry”はランサムウエアだったが，古いOSの端末サーバ間通信のセキュリティホールをついて暗号化するので，被害を受けた端末，サーバにウイルスが存在せず，検出が難しいことも対策上重要な点だった。2020年から猛威を振るっている“Emotet”は，メール中のURLから感染するため，入口のウイルス検知ができない。ネットワーク経由の接続ID，パスワードやメール自体を収集し，その既存メールにURLを差し替えて送信するなど行うため，探知できる「怪しいメール」と言えない状況になっている。

従来の入口におけるIPSなどのウイルス対策ですり抜けるものが増加したため，内部も安心できない状況から，“ゼロ・トラ

〈0913-8919/21/￥300/ 論文 /JCOPY〉