日本の医療機関におけるサイバー攻撃の事例

金沢大学附属病院において，**各部門で個別に導入したシステムから，他の部門の医療機器にまでマルウェア感染**が広がり，その結果，**レスポンスが遅くなる，動作が不安定になるなど診療業務への影響が発生**した．ウイルス検索・駆除ツール導入後の**ウイルスチェックでは1,000 件近くの不正プログラムが検出**された機器もあった．USB メモリ経由でのウイルスの侵入が原因であった．

2018年10月，奈良県の宇陀市立病院で発生したランサムウェア攻撃であり，これによって**電子カルテシステムが使用できなくなった**．病院側は，サーバを停止させて対応し，復旧までは紙カルテの運用をおこなったとしている．原因としては，**職員が私物のパソコンやネットワーク機器を接続しないという院内のルールを守らなかったこと**が原因の一つとして挙げられている．

2019年5月，多摩北部医療センターの職員端末が不正アクセスを受け，端末内の情報流出の可能性があるメールアドレス宛に連絡するとともに，東京都保険医療公社が不正アクセス被害を発表した．その後の調査により，不正アクセスによる被害は当該職員の職務用PC 端末のメールボックスのみ（ハードディスク，ファイルサーバには被害なし），流出した情報はメールボックス内の一部に留まったと推定（ファイルサーバへの不正アクセスは無し）された．原因は職員へのメールの添付ファイル開封によるマルウェア（Emotet 亜種）感染であった．

2020年12月，福島県立医科大学附属病院は，2017年8月以降，**コンピュータウイルス感染が原因とみられる検査機器の不具合が複数の部署で発生**していたことを公表．現時点で身代金の要求やデータ流出は確認していない．。放射線科では，**CTで胸部を撮影中に管理端末が再起動され，撮影画像を保存できなかった**．また，撮影した**胸部のフィルム画像やレントゲン写真を読み取る際、装置が自動で再起動される状態となり，別室の装置で再撮影**することになった．病院の患者情報などを扱う**情報基盤「医療情報システム」はインターネットと接続されていない**ことから，同病院の担当者は「**私用端末など外部の端末経由で感染した可能性**がある」としている．判明のきっかけは11月に厚生労働省からの照会。厚労省から過去に発生したコンピュータウイルスによる医療情報の消失について確認を求められ、院内で調査したところ、当時のセキュリティ担当部署が作成したインシデントレポートの中に、コンピュータウイルスが関連すると思われるものが11件あった。このうち、放射線撮影装置で再撮影に至ったものを2件確認したという。同病院は発生当時に公表しなかった理由について「**再撮影が発生した情報が院内で共有されておらず、報告できなかった**」と釈明。「患者への影響がなかったとの認識もあった」という。当時も一部の患者には経緯を説明した上で再撮影をしていたが、今回の発表にあたり、該当する患者や関係者には改めて事情を説明した上で謝罪した。

海外の医療機関におけるサイバー攻撃の事例

- 2014年4月から6月にかけて，病院経営を手掛けるCommunity Health Systems は，中国を発信地とするサイバー攻撃を受けた（病院側は，この事実を同年7月に確認）．ハッカーは，OpenSSL フレームワークが抱えるセキュリティ脆弱性を悪用し，仮想プライベートネットワーク（VPN）にログインし，データベース上の患者情報にアクセスしたと考えられる．これにより，同院系列の内科医の診察・治療を受けた約450 万人の個人データ（過去5年分）が流出．流出したデータには，患者の氏名・住所・誕生日・電話番号・社会保障番号が含まれていた．

- 2016年2月にドイツのルーカス病院でマルウェアによるサイバー攻撃

- 2016 年2月12日，南カリフォルニアの病院Hollywood Presbyterian Medical Center は，ランサムウェアによる攻撃を受けたことを公表した．**患者データベース（個人情報，レントゲン写真やCT スキャンのデータ，検査結果等）にアクセスできなくなり**，数多くの患者が治療を受けられず，一部は他の病院に移送されることとなった．電子メールも停止され，医療従事者らはファックスや電話に頼らざるを得ない状況であった．攻撃者に医療機関側対し，身代金として9000 枚のビットコイン （約 340万ドル相当) を要求した．一部を支払ったもよう．

- 2017年5月，英国NHS はランサムウェア「WannaCry」の感染により，**イングランドでは47，スコットランドでは13 の病院で被害**が出ていると報告．一部の病院では手術や診療予約をキャンセル，救急車の受入を拒否．**特に深刻な影響が出たのは，MRIやCT，レントゲンなどの画像データをコンピュータでやりとりする画像診断部門**．保守党政権によるNHS のIT予算削減によるセキュリティ対策の不備が背景との政策論争に発展．

- 2018年1月にはノルウェーの東部南部地域保健局のハッキング，米国ハンコック地域病院でランサムウェア攻撃

- 2020年9月，ドイツのデュッセルドルフ大学病院で発生したランサムウェア攻撃は，救急患者の受け入れ停止を余儀なくされた．**救命処置を受ける予定であった大動脈瘤を患っている78歳の患者は約32km離れた工業都市ヴッパータールの大学病院へ搬送されたがその後死亡**したと報道された．その後、検察当局は死因はあくまでも患者の病状にあり、サイバー攻撃は無関係と結論．

- 2020年10月3日付けのニューヨークタイムズ紙にて、**新型コロナウイルス感染症のワクチンの治験**を含む治験におけるデータ収集等を支援する米国ERT社（eResearch Technology, Inc.）に対して、ランサムウェアを用いたサイバー攻撃が行われ、**治験の遅延が懸念されるサイバーセキュリティインシデント**等の報道

本田大輔：医療分野におけるサイバーセキュリティの文献調査　医機学　Vol．90，No．6（2020）を一部改変

米国ボストンの胎児モニタへの感染事例

- 米国ボストンのBeth Israel Deaconess Medical Centerにおいて、高リスク妊娠の女性向けの**Philips製胎児モニタ装置がマルウェアに感染**した。感染の結果、**装置のレスポンスが遅くなったことが報告されているものの、患者に直接の被害はなかった**。
- Beth Israel Deaconess Medical Centerは、現在、米国でサイバーセキュリティに最も積極的に取り組んでいる病院の一つとなっている。同病院では、15,000の機器が院内ネットワーク上で稼動し、そのうち500の機器が古いOSを利用している。そのため、これらの機器をインターネットから隔離し、院内ネットワークも月1回フルスキャンを実施している。

Philips製胎児モニタ装置の例（Avalon FM40 and FM50 fetal monitors）

医療機器における情報セキュリティに関する調査　医療機器のセキュリティの現状を整理
独立行政法人 情報処理推進機構（IPA）技術本部 セキュリティセンター（2014年4月）

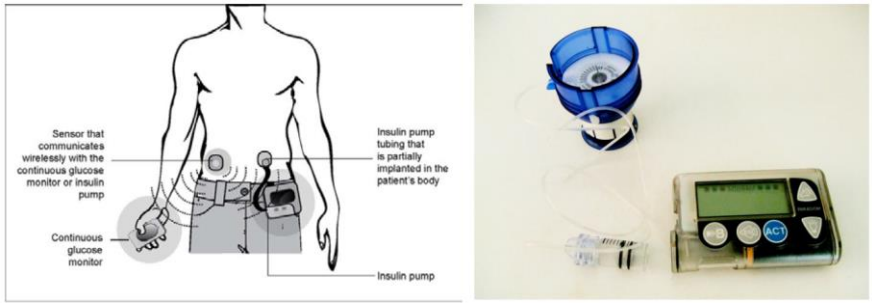
ペースメーカー/ICDの脆弱性事例（Daniel Halperin）

- 2008年、Daniel Halperin（University of Washington）、Kevin Fu（当時University of Massachusetts、現University of Michigan）らにより2008 IEEE Symposium on Security and Privacyでペースメーカー/ICDへのハッキングについて発表された。
- 本事例では**ペースメーカーやICDの機器をリバースエンジニアリングすることにより脆弱性を発見し、その脆弱性を利用して患者情報や診療情報のほか、機器の設定を変更するなどといった攻撃を実施した**ものである。
- Daniel Halperinらによる研究では、**ICDとプログラマのやり取りを、オシロスコープとソフトウェア無線機（USRP：Universal Software Radio Peripheral）を用いて送信波を解析し、暗号化されていなかった通信データから情報を解読し、患者情報などの情報を盗み出すことに成功**した。
- さらに、**市販のソフトウェア無線（USRP）とBasicTXマザーボードを用いて、同じ周波数の波形を送信することによるリプレイアタックを行い、プログラマに進入**し、以下のような攻撃を成功させている。
  - ✓ICD認証を誘発しプログラマからICDの場所、型番やシリアルナンバーなどの詳しい情報を取得
  - ✓患者の情報（名前、診断情報、その他詳細情報）を取得
  - ✓疾患情報など、心臓のデータを取得
  - ✓ICDに登録されている患者名を、GNURadioを使い変更する事に成功
  - ✓イベントログ等を記録するための時間設定の読み取り、再設定に成功
  - ✓心臓に何らかの処置を行う設定、治療設定の削除や変更に成功
- また、論文中では、安全でないソフトウェアアップデートの枠組みや、バッファオーバーフローに関する脆弱性を悪用した攻撃の可能性も示唆するとともに、対策手法の提案も行っている。

医療機器における情報セキュリティに関する調査　医療機器のセキュリティの現状を整理
独立行政法人 情報処理推進機構（IPA）技術本部 セキュリティセンター（2014年4月）

Jerome Radcliffe氏によるインスリンポンプへのハッキング

- 2011年Black Hat にてJerome Radcliffe氏により**インスリンポンプへのハッキングについて発表**。
- 糖尿病患者の治療に用いるインスリンポンプの制御システムに脆弱性を突いて侵入し「致死的な攻撃」を仕掛けることができると発表。具体的には、インスリンを送り込むポンプの無線機能に脆弱性が存在し、それを突くことでポンプ自身を停止においやったり、投与するインスリンの量を外部から操作したりすることが可能。



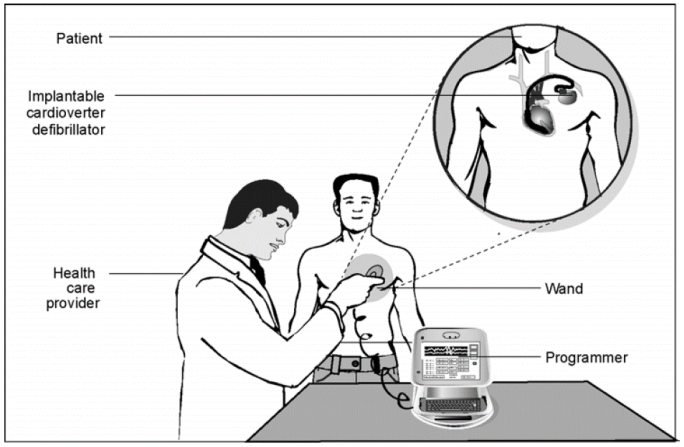
インスリンポンプの通信イメージ（左）と機器（右）（出典：（左）MEDICAL DEVICES FDA Should Expand Its Consideration of Information Security for Certain Types of Devices、GAO、（右）TheRegister Webサイト

- 本研究では、ハッキングのために、インスリンポンプ及びCGMセンサについて、以下の情報を収集
  1. 対象デバイスのマニュアルからの情報を収集し、マニュアルの付録部分にデバイスの詳細情報（パケットのサイズや伝送間隔等）やFederal Communication Commission (FCC) ID を取得
  2. 特許庁Webより機器製造業者を検索し、デバイスの特許情報を取得。デバイスの機能情報や、構成情報の詳細情報が多く掲載
- その結果、CGMセンサでは容易に通信情報の解読が可能であり、インスリンポンプにおいても機器のシリアル番号を取得できれば無線通信により誤った命令を実行できるとしている。CGMセンサ、インスリンポンプそれぞれにおいて、理論上は以下の攻撃が可能であると発表。
  - CGM センサ攻撃例；実際のデータと違う血糖値データを送ることで、インスリン投入量の変化を誘発、正しい血糖値データ受信を妨害し、別のデータを送信
  - インスリンポンプ攻撃例；ワイヤレス機器を用いて、設定の書き換えを行い、意図しない動作を誘発（インスリン投入のタイミングや一回当たりの投入量の変更等）
- なお、2011年10月には、ATMへのハッキングで有名なBarnaby Jack氏により、事前にシリアル番号を取得することなしにハッキング可能であることが示され、ハッキング自体も実演されている。

医療機器における情報セキュリティに関する調査　医療機器のセキュリティの現状を整理
独立行政法人 情報処理推進機構（IPA）技術本部 セキュリティセンター（2014年4月）

Barnaby Jack氏による心臓ペースメーカーへのハッキング

- ATMへのハッキングに加え、2011年にはインスリンポンプへのハッキングを実演したBarnaby Jack氏がBreakPoint security conference 2012（2012年10月）でペースメーカー/ICDへのハッキングについて発表し、ハッキング実演のデモ映像を流した。



ペースメーカー/ICDの治療イメージ（出典：MEDICAL DEVICES FDA Should Expand Its Consideration of Information Security for Certain Types of Devices, GAO,）

- Barnaby Jack氏は、ノートPCを用いて、50フィート（約15m）以内のICD（植込み型除細動器）に830ボルトの電流を流せることをビデオ内で実演した。
- Barnaby Jack氏はペースメーカー/ICDのワイヤレストランスミッタをリバースエンジニアリングすることによりトランスミッタの脆弱性を発見し、ハッキングに利用している。脆弱性は、機器を制御するために必要なシリアル番号等の情報を特別なコマンドにより引き出せるというものである。
- また、ペースメーカーとの無線通信に使われるプログラマに対して不正なファームウェアをアップロードすれば、大量のペースメーカー/ICDへの一斉攻撃も起こり得るとしている。

Roche製の複数の医療機器のSymantec pcAnywhereに関する脆弱性

- Roche製の複数の医療機器で使われているSymantec pcAnywhereに脆弱性があるとして、FDAが2012年6月にEnforcement Report（製品回収情報）を公表した。
- リモートアクセスソフトウェアであるSymantec pcAnywhereの脆弱性を利用して、外部ネットワークと接続している場合に第三者による不正アクセスが行われる可能性があった。
- 対象となる機器は、遺伝子検査製品等に使われているソフトウェア製品AMPLILINK、リアルタイムPCRシステムRoche LightCycler 2.0 Instrument、生化学自動分析装置COBAS INTEGRA 400/400 plus等、複数の医療機器にわたり、リコールのレベルはすべてClass II（一時的健康問題を引き起こすかもしれないか、重大な事故・傷害が稀に発生する可能性のある製品に該当）とされている。

LightCycler® 2.0 Instrument（出典：Roche社Webサイト）

医療機器における情報セキュリティに関する調査　医療機器のセキュリティの現状を整理
独立行政法人 情報処理推進機構（IPA）技術本部 セキュリティセンター（2014年4月）

Roche製生化学自動分析装置のソフトウェア脆弱性

- Roche製の生化学自動分析装置COBAS INTEGRA 400/400 plus Analyzerで使われているOracleのソフトウェアに脆弱性があるとして、FDAが2013年1月にEnforcement Report（製品回収情報）を公表している。
- リコールのレベルはClass III（恐らく健康被害は引き起こさないが、FDAの表示規制に反する製品か、規則に反する製品に該当）。
- 具体的には、装置のデータベースへのリモートアクセスに関する脆弱性であり、OracleのソフトウェアであるTNS-Listenerの脆弱性を利用したリモートアクセスにより、他のDBの登録、既存DBへの読み書きが可能になるというものであった。

COBAS INTEGRA 400 plus（出典：Roche社Webサイト）

医療機器における情報セキュリティに関する調査　医療機器のセキュリティの現状を整理
独立行政法人 情報処理推進機構（IPA）技術本部 セキュリティセンター（2014年4月）