医療DF研究会

医療分野における デジタル・フォレンジックの可能性

和 田　則 仁
慶應義塾大学　医学部　外科学（一般・消化器）

2017年12月12日(火) 11:10～12:10 発表30分; ホテルグランドヒル市ヶ谷 3F 瑠璃の間

医療情報システムの安全管理に関するガイドライン

第1版 平成17年3月
10章、156ページ

第1版 平成21年3月
5章、18ページ

30ページ

医療情報システムの安全管理に関するガイドライン

第５版（平成29年5月）の主な改正点

第4版（平成21年3月）

医療機関等を対象とするサイバー攻撃の手法の多様化・巧妙化、地域医療連携や医療介護連携等の推進、IoT等の新技術やサービス等の普及への対応として、関連する1章や6章を改定するとともに、第4.2版の公表以降に追加された標準規格への対応が行われた。また、平成29年5月施行の改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等への対応が行われた。

改定テーマは以下の13テーマである。

1. **電子カルテの代行入力を時間経過で自動確定することへの言及**：診療録等の代行入力を行う際に、時間経過で自動的に記録確定する運用が認められないことの明確化等、7.1章「真正性の確保について」を改定）
2. **「製造業者による情報セキュリティ開示書」ガイドVer.2.0への言及**：6.2章「医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」において言及
3. **モバイルデバイスへの対応**：院外で利用するソフトウェアを限定することや、他のアプリの影響を受けないこと等といった運用や技術的対策について、6.9章「情報及び情報機器の持ち出しについて」、6.11章「外部と個人情報を含む医療情報を交換する場合の安全管理」に記載）
4. **標的型攻撃への対応**：サイバー攻撃に関して、有事の際を考慮した技術的対策や所管機関への連絡体制や情報共有体制、教育等について6.6章「人的安全対策」、6.10章「災害、サイバー攻撃等の非常時の対応」に追記
5. **TLS1.2によるオープンネットワーク接続への言及**：TLSによりオープンネットワークに接続する場合、「SSL/TLS暗号設定ガイドライン」に基づき適切な設定を行う必要がある旨を6.11章「外部と個人情報を含む医療情報を交換する場合の安全管理」に記載）
6. **小規模医療機関が順守すべき項目の明確化**：医療機関の規模別の運用管理の実施項目例について、6.5章「技術的安全対策」、付表1、付表2を改定）
7. **医療情報システムの対象範囲の検討**：電子的な医療情報を取り扱う介護事業者及び医療情報連携ネットワーク運営事業者を本ガイドラインの対象範囲とする旨を、1章「はじめに」、3.1章「7 章及び9章の対象となる文書について」において明確化
8. **IoTセキュリティへの対応**：総務省、経済産業省、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン」等、各種ガイドライン及び医療の現場の状況を鑑み、6.5章「技術的安全対策」にIoTセキュリティについて記述
9. **2要素認証の採用**：2要素認証の今後の取扱いについて、医療現場への影響を考慮し、猶予期間を設けて段階的に移行を進めること等を6.5章「技術的安全対策」に記載
10. **電子署名の採用**：平成28年度の診療報酬改定において、電子的診療情報提供書の算定要件に保健医療福祉分野の公開鍵基盤（HPKI）による電子署名の採用が盛り込まれたことに合わせ、6.12章「法令で定められた記名・押印を電子署名で行うことについて」を改定
11. **わかりやすさへの対応**：ガイドラインが参照している他の資料の改訂を反映させ、また、分かりやすさの観点から、ガイドライン全体の文書校正や表現等を見直し
12. **規格変更への対応**：規格変更への対応として、5章「情報の相互運用性と標準化について」を改定
13. **個人情報保護法への対応**：平成29年5月施行の改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等に合わせて関連規定を改定

改正個人情報保護法

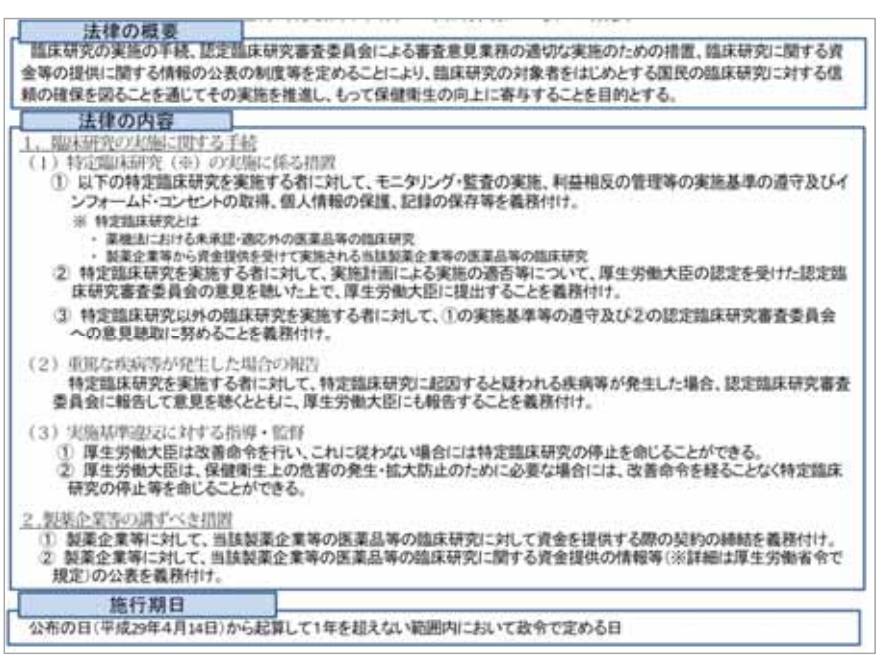
医療・介護関係事業者における
個人情報の適切な取扱いのためのガイダンス

平成29年4月14日
個人情報保護委員会
厚 生 労 働 省

目 次

- 要配慮個人情報の範囲
  （オプトアウトはＮＧ）
- 専門的
- 公共性
- 死者の医療情報
- 予防など周辺分野
- 本人に伝えられない
- 医療従事者のプライバシー

臨床研究法



法律の概要

臨床研究の実施の手続、認定臨床研究審査委員会による審査意見業務の適切な実施のための措置、臨床研究に関する資金等の提供に関する情報の公表の制度等を定めることにより、臨床研究の対象者をはじめとする国民の臨床研究に対する信頼の確保を図ることを通じてその実施を推進し、もって保健衛生の向上に寄与することを目的とする。

法律の内容

1. 臨床研究の実施に関する手続

（1）特定臨床研究（※）の実施に係る措置

① 以下の特定臨床研究を実施する者に対して、モニタリング・監査の実施、利益相反の管理等の実施基準の遵守及びインフォームド・コンセントの取得、個人情報の保護、記録の保存等を義務付け。

※ 特定臨床研究とは
- 薬機法における未承認・適応外の医薬品等の臨床研究
- 製薬企業等から資金提供を受けて実施される当該製薬企業等の医薬品等の臨床研究

② 特定臨床研究を実施する者に対して、実施計画による実施の適否等について、厚生労働大臣の認定を受けた認定臨床研究審査委員会の意見を聴いた上で、厚生労働大臣に提出することを義務付け。

③ 特定臨床研究以外の臨床研究を実施する者に対して、①の実施基準等の遵守及び②の認定臨床研究審査委員会への意見聴取に努めることを義務付け。

（2）重篤な疾病等が発生した場合の報告

特定臨床研究を実施する者に対して、特定臨床研究に起因すると疑われる疾病等が発生した場合、認定臨床研究審査委員会に報告して意見を聴くとともに、厚生労働大臣にも報告することを義務付け。

（3）実施基準違反に対する指導・監督

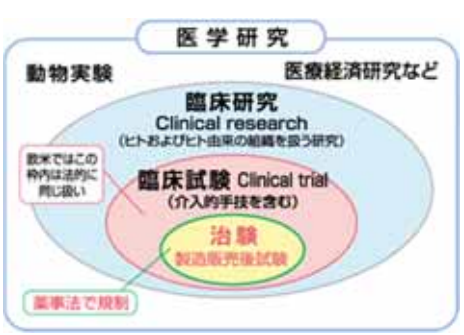
① 厚生労働大臣は改善命令を行い、これに従わない場合には特定臨床研究の停止を命じることができる。
② 厚生労働大臣は、保健衛生上の危害の発生・拡大防止のために必要な場合には、改善命令を経ることなく特定臨床研究の停止等を命じることができる。

2. 製薬企業等の講ずべき措置

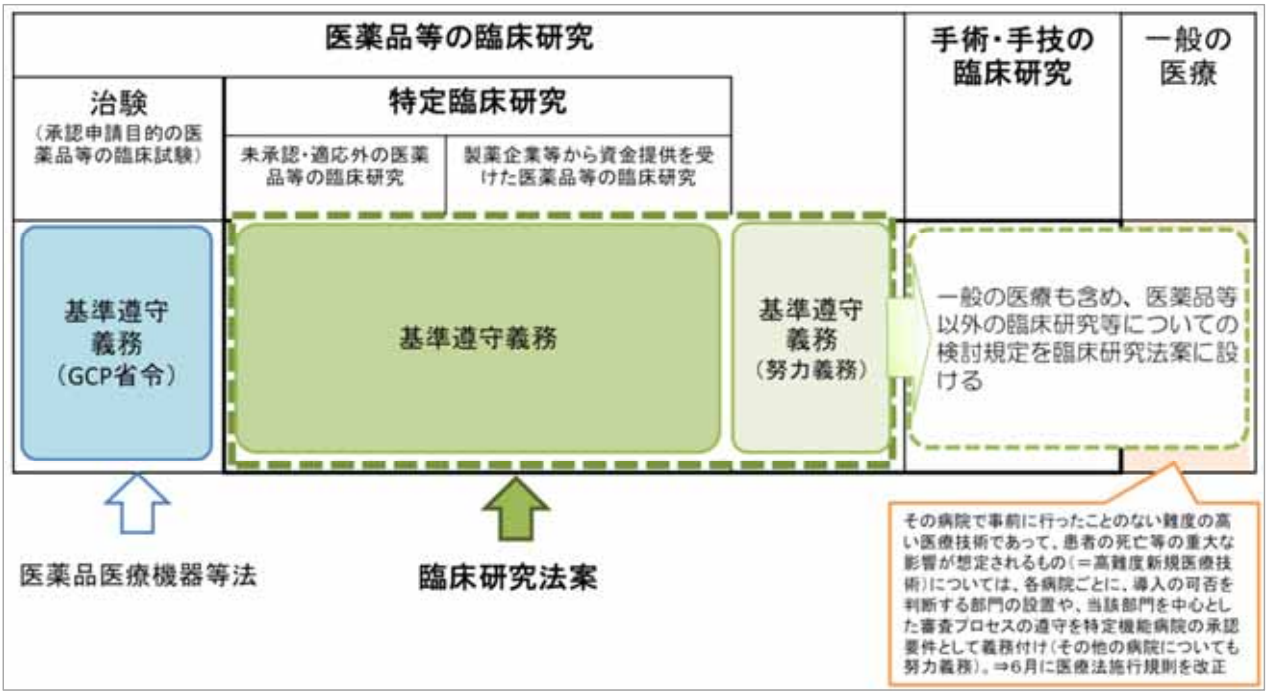
① 製薬企業等に対して、当該製薬企業等の医薬品等の臨床研究に対して資金を提供する際の契約の締結を義務付け。
② 製薬企業等に対して、当該製薬企業等の医薬品等の臨床研究に関する資金提供の情報等（※詳細は厚生労働省令で規定）の公表を義務付け。

施行期日

公布の日（平成29年4月14日）から起算して1年を超えない範囲内において政令で定める日



医療における規制の区分



医学研究に関する指針一覧

1. 人を対象とする医学系研究に関する倫理指針
2. ヒトゲノム・遺伝子解析研究に関する倫理指針
3. 遺伝子治療等臨床研究に関する指針
4. 手術等で摘出されたヒト組織を用いた研究開発の在り方
5. 厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針
6. 異種移植の実施に伴う公衆衛生上の感染症問題に関する指針
7. ヒト受精胚の作成を行う生殖補助医療研究に関する倫理指針
8. 疫学研究に関する倫理指針
9. 臨床研究に関する倫理指針
10. ヒト幹細胞を用いる臨床研究に関する指針

指針等の遵守を厚生労働科学研究費補助金等の交付の条件とし、違反があった場合には補助金の返還、補助金の交付対象外（最大５年間）とする措置を講ずることがあり得る。

デジタル・フォレンジックとは（ＩＤＦのＨＰより）

インシデントレスポンス*や法的紛争・訴訟に際し、**電磁的記録の証拠保全及び調査・分析**を行うとともに、**電磁的記録の改ざん・毀損等**についての分析・情報収集等を行う一連の科学的調査手法・技術を言います。

*コンピュータやネットワーク等の資源及び環境の**不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等**、並びにそれらへ至るための行為（事象）等への対応等を言う。

- ハイテク犯罪や情報漏えい事件などの**不正行為発生後にデジタル機器等を調査**し、いつどこで誰が何をなぜ行ったか等の情報を適切に取得し、問題を解決するインシデントレスポンスとして。
- 定期的にフォレンジックを用いた**監査**を行う事により、**不正行為の発生を抑止**するとともに**発生後の対応を迅速に**行えるようにする、広義の意味でのインシデントレスポンスとして。
- デジタル・データの保全、解析、保管等の**取り扱い手法**に関して適切に行われているかを**議論**する事により、**相互の法的権利を正しく守る**活動として。

医療のデジタル・フォレンジックとは

電子カルテ情報等の不正使用、診療妨害、電子カルテデータの破壊、患者情報漏洩等や医療訴訟に際し、電子カルテ情報の**証拠保全及び調査・分析**を行うとともに、**電子カルテの改ざん・毀損等**についての分析・情報収集等を行う一連の科学的調査手法・技術を言います。

- ハイテク犯罪や医療情報漏えい事件などの**不正行為発生後にデジタル機器等を調査**し、いつどこで誰が何をなぜ行ったか等の情報を適切に取得し、問題を解決するインシデントレスポンスとして。
- 定期的にフォレンジックを用いた**監査**を行う事により、**不正行為の発生を抑止**するとともに**発生後の対応を迅速に**行えるようにする、広義の意味でのインシデントレスポンスとして。
- デジタル・データの保全、解析、保管等の**取り扱い手法**に関して適切に行われているかを**議論**する事により、**医療機関と患者の法的権利を正しく守る**活動として。

医療機関におけるデジタル情報

- 医療情報システム（電子カルテ）
  - 電カル本体
  - ＰＡＣＳ
  - ＤＷＨ
- 部門システム
- 自科検査機器
- ＢＹＯＤ
- 個人で管理するデータ
- 診療外のデータ（研究、教育）

医療のデジタル・フォレンジックとは

電子カルテ情報等の不正使用、診療妨害、電子カルテデータの破壊

患者情報漏洩等

医療訴訟

電子カルテ情報の**証拠保全及び調査・分析**

電子カルテの改ざん・毀損等についての分析・情報収集等

- 犯罪・事件などの**不正行為発生後にデジタル機器等を調査**
- **監査**により**不正行為抑止、迅速対応**
- **取り扱い手法議論**により**医療機関と患者の法的権利を守る**

カリフォルニア州の病院、ハッカーにビットコインで17,000ドルの身代金を支払う （2016年2月17日）

- ハリウッドPresbyterian医療センター
- ランサムウエア
- 「システム正常化の利益最大化のためにやむを得なかった」
- ハッキングによる健康被害の報告はない
- 患者データ流出は確認されていない


Chicago Tribune

California hospital paid $17,000 ransom in bitcoins to hackers

"It is the beginning of a pandemic hitting health systems in the next few years."
Larry Whiteside, Jr. (CEO, Whiteside Security LLC)

http://www.chicagotribune.com/news/nationworld/ct-california-hospital-ransom-hackers-20160217-story.html

ハッカーのウイルス攻撃によりワシントン地区のMedStar病院チェーン麻痺（2016年3月29日）

- MedStar病院チェーン：MDとDCで10病院、30,000人の職員、6,000人の契約医師
- ランサムウエア
- システムをシャットダウン、紙運用に、診療の遅延発生
- 情報漏洩のエビデンスはない
- マルウェアを発見除去に成功


Chicago Tribune

Washington-area MedStar hospital chain paralyzed by hackers' virus attack

WannaCry ransomware attack

- 2017年5月12日から大規模なサイバー攻撃が開始
- 150か国の23万台以上のコンピュータに感染
- 日本：日立製作所、ＪＲ東日本、イオン、本田技研など
- 英国National Health Service (NHS) のシステムが感染
- 一部の病院で診察や手術の予約のキャンセル、救急車の受け入れ不能、画像診断・病理診断の停止
- 解除キー300ドル（3日後に2倍）払った形跡あり

ＵＳＢ紛失事例１

埼玉県立病院医師、患者情報入りＵＳＢ紛失　治療内容など３６００人分（産経ニュース、2017.2.1）

県病院局は３１日、県立循環器・呼吸器病センター（熊谷市板井）の男性医師が患者約３６００人分の氏名や生年月日、処置内容などを保存したＵＳＢメモリーを紛失したと発表した。同局は懲戒処分を検討。第三者による不正使用などは確認されていないとしており、患者らに文書で謝罪する。

同局によると、医師は５０代の幹部で、１月２５日の勤務終了後、処置記録データを自宅のパソコンで整理するため、内部規定に違反してＵＳＢを許可なく持ち出した。本庄市内の飲食店で飲酒後、同僚２人とタクシーに同乗して帰宅途中に、ＵＳＢが入ったセカンドバッグがないことに気付いたという。

データは医師が平成８年以降に担当した約３６００人分。氏名は仮名書きで、診察券番号や放射線検査画像なども保存されていた。ＵＳＢは院内でのデータ移動用で、普段は院内で作業をしていた。同局に対し、医師は「講演会に参加するため急いでいた」と説明している。

既に県警に紛失を届け出ており、防犯カメラ映像などから、同僚の降車時に熊谷市内でバッグごと落とした可能性が高いという。

ＵＳＢ紛失事例２

患者情報含むUSBメモリを紛失 - 茨城県立中央病院（セキュリティーニュース、2017/06/07 ）

茨城県立中央病院の医師が、患者の個人情報を保存したUSBメモリを紛失していたことがわかった。

同院によれば、同院の医師が患者15人分の個人情報を保存したUSBメモリを紛失したもの。氏名や病名、患部の画像データなどが含まれる。紛失した情報の外部流出は確認されていないという。

同院では、対象となる患者に説明と謝罪を行っている。

ＵＳＢ紛失事例３

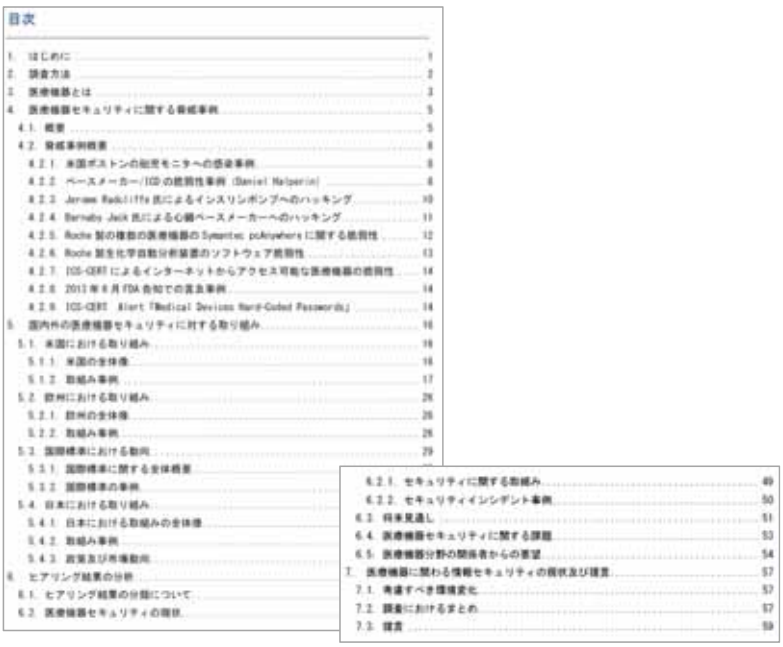
患者の個人情報記録ＵＳＢ紛失　1900人分、北里大東病院（日本経済新聞、2017/01/30）

北里大東病院（相模原市）は30日、神経内科の入院患者約1900人分の氏名や病名などが記録されたＵＳＢメモリーを医師が紛失したと発表した。第三者への情報流出や不正利用は確認されていないとしている。

病院によると、患者のデータ管理を担当する30代の男性医師が19日、神経内科のパソコンにデータを登録するため、院内の一室でＵＳＢを使用。23日に再び使用しようとした際、本来の保管場所にないことに気付いた。院内を捜したが見つからず、27日、遺失物として県警に届けた。

ＵＳＢには2003年３月～今年１月の患者の氏名や性別、生年月日、病名などが記録されていた。病院は今後、患者らに文書で説明し、謝罪するとしている。

IPA 医療機器における 情報セキュリティに関する調査(2014)



セキュリティインシデント及び脆弱性の報告例

分類	事例	概要
インシデント	米国ボストンの Beth Israel Deaconess Medical Center での胎児モニタへの感染[7,8]	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胎児モニタ装置がマルウェアに感染され、装置のレスポンスが遅くなったことが報告されている。患者に直接の被害はなかった。Philips 製とされている。
インシデント	金沢大学附属病院での医療機器のウイルス感染事例[9]	国立大学法人 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、他の部門の機器にウイルス感染が広がり、診療業務への影響が発生。USB メモリ経由での侵入であった。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 1000 件近くの不正プログラムが検出された機器もあったという。
脆弱性	ペースメーカー/ICD の脆弱性[10]	2008 年に Medical Device Security Center によってペースメーカー/ICD（Implantable Cardioverter Defibrillator）へハッキングし、電流を流したり、機器を停止させたりすることが可能という研究結果が発表された。
脆弱性	インスリンポンプへのハッキング（Black Hat）[11]	2011 年 Black Hat にて Jerome Radcliffe 氏が発表。糖尿病患者のインスリンポンプに無線機能の脆弱性を利用して侵入し、投与するインスリンの量を外部から操作するなど「致死的な攻撃」を仕掛けることができることを発表。
脆弱性	インスリンポンプへのハッキング（McAfee FOCUS 11）	Barnaby Jack 氏が、2011 年 McAfee FOCUS 11 でインスリンポンプへのハッキングを実演。
脆弱性	ペースメーカーへのハッキング	Barnaby Jack 氏が、BreakPoint security conference 2012 では、ペースメーカーへのハッキングについて発表し、デモ映像を流した。Black Hat 2013 でもペースメーカーへのハッキングについて発表予定であったが、発表前に死去し、詳細不明となっている。

インシデント	インターネットからアクセス可能な医療機器の脆弱性	ICS-CERT Monthly Monitor （2012 年 8 月号）で報告された医療機器のリモート監視についての警告。実際に、インターネットからアクセス可能な医療機器が大学で見つかり、システム管理者に連絡を取り、是正がなされた。
脆弱性	Roche 製の複数の医療機器で使われている Symantec pcAnywhere の脆弱性[12]	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、Roche 製の複数製品に対して FDA（Food and Drug Administration）が 2012 年 6 月に Enforcement Report を公表。
脆弱性	Roche 製の生化学自動分析装置で利用されている Oracle ソフトウェアの脆弱性[13]	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 のソフトウェアの脆弱性。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。FDA が 2013 年 1 月に Enforcement Report を公表。
インシデント/脆弱性	2013 年 6 月 FDA 告知での言及事例（ネットワーク接続型の医療機器のマルウェア感染や医療機器への無線接続を行うモバイル機器を標的としたマルウェア等）[14]	2013 年 6 月 13 日の FDA 告知「FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks」で言及。ネットワーク接続型の医療機器がマルウェアに感染した事例や、患者の情報やモニタシステム、インプラント機器への無線接続を行うモバイル機器を標的としたマルウェア等が言及されている。
脆弱性	医療機器のハードコードされたパスワード[15]	40 ベンダ 300 の医療機器に関連するハードコードされたパスワードについて 2013 年 6 月に ICS-CERT から Alert が出された。手術用機器や麻酔器、人工呼吸器、薬物注入ポンプ等が関係しており、機器によって遠隔操作が可能とされている。

鑑定の対象資料（ディスカバリー）

- 診療録
  紙カルテ→電子カルテ（プリントアウト）
- レントゲン
  フィルム→ＤＩＣＯＭ（ＣＤ／ＤＶＤ）
- ビデオ
  ＶＨＳ→ＤＶＤ、ＨＤＤ（ＤＶＤ）

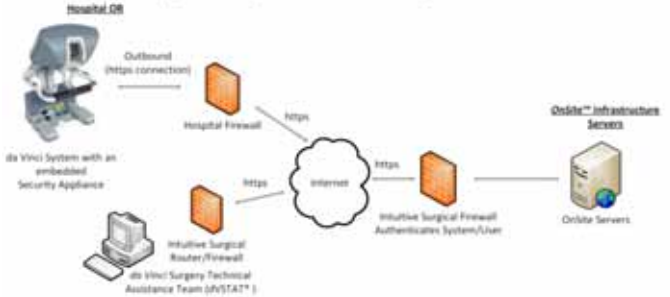
電子カルテのプリントアウトの問題点

- 複写に手間がかかる
- 見るのが大変、場所を取る
- 必要な情報を探すのが困難
- ベンダーごとに様式が異なる
- 検索ができない
- 変更履歴がわかりにくい
- 実際の診療場面を再現できない
- 部門システムのデータがない
- 印刷の範囲が恣意的
- ログの記録はない

ヘルスケア・医療とＩｏＴ

- 在宅医療見守り
- スマートホスピタルライティングシステム
- 服薬支援容器
- スマートウォッチ
- 空気清浄機能付き扇風機
- 衣料型ウェアラブルシステム
- スマート歯ブラシアタッチメント
- 体組成計
- 見守り機能付き電動ポット
- センサー内蔵ベッド
- 糖尿病患者医療支援コンタクトレンズ
- 救命救急補助スマートフォンアプリ

手術ロボットの遠隔支援



Connected Medical Device & IOT Security Summit

後援：
アメリカ臨床工学会
参加型医療学会

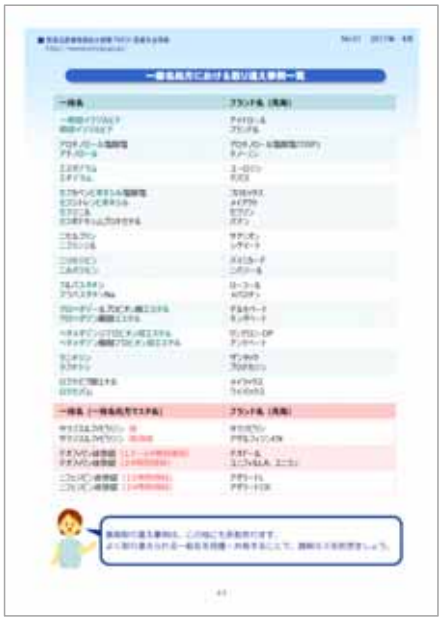
Connected Medical Device & IOT Security Summit

January 25, 2018
08:15 Chairperson's opening remarks
08:45 Keynote address: the economics and ecosystem of the dark web
09:30 Keynote address: MEDSEC vs. St. Jude Medical: implantable devices, vulnerabilities, and the law
10:45 Keynote address: regulatory advances
11:30 US legal and regulatory framework
13:15 Engaging with non-technical stakeholders
15:00 Cognitive devices, internet of hospital things – IoHT, smart devices; safer care
16:30 On the fly contextual security risk management
17:00 Building layers of security for IoT and embedded medical devices
17:30 Innovations in secure IoT medical device application support

January 26, 2018
08:00 Chairperson's opening remarks
08:15 Keynote address: threat modeling 101 – learnings from real design
09:00 Live demo of a medical device replica hack
09:30 Third party risk management for medical devices
10:30 Leveraging exploits to manipulate care workflows
11:30 Utilizing blockchain technology for connected medical device / IoT security
12:00 Panel and audience discussion: where do we go from here?
14:00 Optional post-summit workshop: know thy enemy: securing medical devices in the hacking era

厚生労働省医政局総務課医療安全推進室の通知

PMDAの医療安全情報




PMDA
医療安全情報
No.29 2011年12月
心電図モニタの取扱い時の注意について
POINT 安全使用のために注意するポイント
① テクニカルアラームに関する注意点（電池はがれ）
心電図波形のふれ！


② テクニカルアラームに関する注意点（電池切れ）
受信良好！
受信不良！
電池交換
テレメータ電池確認
BATTERY LOW !


④ その他心電図モニタの適正な使用について
心電図モニタの必要性
適正なアラームの設定
患者さんごとに、心電図モニタの使用目的をチームで検討することが大事ですね。
アラームの適正な設定によって、観察はアラームを頼りすぎることができますね。


PMDA
医療安全情報
No.20 2010年11月
人工呼吸器の取扱い時の注意について（その3）
POINT 安全使用のために注意するポイント
① 使用中の電源に関する注意点について
換気停止！
アラームに気づかずバッテリ駆動に切り替わり、バッテリが充電切れになると、換気停止となり、大変危険です。


使用中の電源の表示例（1）
トレーデル・メディカル・ジャパン（株）
アイ・エム・アイ（株）
コヴィディエン・ジャパン（株）
このように、使用中の電源の表示は製品によって様々です。
使用中の製品の「どこに、どのように」表示されるのか、あらかじめ確認しておきましょう！


② 電源表示の見落とし防止対策の例について
電源表示の見落とし防止のため、電源表示箇所には下のような工夫をすると、気づきやすいですよ！
シールの貼付位置
確認
ランプが点灯
していますか？

まとめ

- 「医療」の特殊事情
- 法律とガイドライン
- インシデントレスポンス事例
- e-Discovery
- IoT／IoHT
- 医療現場での問題・ニーズ