

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



1

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



2

医療情報システムの安全管理に関するガイドライン

- はじめに
- 本指針の読み方
- 本ガイドラインの対象システム及び対象情報
- 電子的な医療情報を扱う際の責任のあり方
- 情報の相互運用性と標準化について
- 情報システムの基本的な安全管理
 - 方針の制定と公表
 - 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
 - ISMS 構築の手順
 - 取扱い情報の把握
 - リスク分析
 - 組織的安全管理対策 (体制、運用管理規程)
 - 物理的安全対策
 - 技術的安全対策
- 人的安全対策
- 情報の破棄
- 情報システムの改造と保守
- 情報及び情報機器の持ち出しについて
- 災害、サイバー攻撃等の非常時の対応
- 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
- 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
- 電子保存の要求事項について
- 診療録及び診療諸記録を外部に保存する際の基準
- 診療録等をスキャナ等により電子化して保存する場合について
- 運用管理について

3



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。

- 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
- 「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
- 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
- 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
- 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
- 小規模医療機関が遵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
- 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

- 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
- 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
- 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 (PKI) 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
- 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
- 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
- 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

4



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

I 本ガイドランスの趣旨、目的、基本的考え方	1
1. 本ガイドランスの趣旨	1
2. 本ガイドランスの構成及び基本的考え方	1
3. 本ガイドランスの対象となる「医療・介護関係事業者」の範囲	1
4. 本ガイドランスの対象となる「個人情報」の範囲	2
5. 個人情報保護委員会との関係	2
6. 医療・介護関係事業者が行う活動の透明性の確保と対外的説明	3
7. 責任体制の明確化と責任・利用範囲の明確化	3
8. 連携への留意事項の明示(取扱い)	4
9. 個人情報に関する取扱い(取扱い)	4
10. 適法性を担保する取扱い(取扱い)	4
11. その他取扱いの確保	5
12. 認定個人情報保護団体における取扱い	5
II 用語の定義等	6
1. 個人情報(法第17条第1項)	6
2. 個人識別符号(法第17条第2項)	7
3. 匿名加工個人情報(法第17条第3項)	6
4. 個人情報の匿名化	11
5. 匿名加工情報(法第17条第4項)	11
6. 個人情報データベース等(法第17条第4項、個人データ(法第17条第5項)、保有個人データ(法第17条第7項))	12
7. 本人の同意	14
8. 取扱いへの制約取扱い	15
III 医療・介護関係事業者の義務等	16
1. 利用目的の特定等(法第17条第1項、第17条第2項)	16
2. 利用目的の通知等(法第17条第3項)	20
3. 個人情報の適正な取扱い、個人データに関する透明性の確保(法第17条第4項、第17条第5項)	22
4. 安全管理措置、取扱いの適正な取扱いの確保(法第17条第6項～第17条第7項)	23
5. 個人データの第三者提供(法第17条第8項)	23
6. 当該事業者への権利の行使(法第17条第9項)	26
7. 第三者提供に係る記録の作成等(法第17条第10項)	27
8. 第三者提供を受ける側の確認等(法第17条第11項)	27
9. 保有個人データに関する事項の公表等(法第17条第12項)	27
10. 本人からの請求による保有個人データの開示(法第17条第13項)	28
11. 訂正及び削除等(法第17条第14項、第17条第15項)	28

12. 開示等の請求等に応じる手続及び手数料(法第17条第16項、第17条第17項)	31
13. 理由の説明、事後的請求、苦情の対応(法第17条第18項、第17条第19項)	31
IV ガイドランスの経過等	33
1. 効果に関する見直し	33
2. 本ガイドランスを施行する事務職員の作成・公開	33
別添1 医療・介護関係法において医療・介護関係事業者の作成・保存が義務づけられている記録	44
別添2 医療・介護関係事業者の活動の範囲で認定される利用目的	46
別添3 医療・介護関係事業者の活動の範囲で認定される主な事例(法第17条第9項に基づく場合)	48
別添4 医療関係機関、介護サービス事業者等に係る付随業務等	71
別添5 医学研究における関連取扱い	73
別添6 LINE S-CO国際宣言等	73

- 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. 臨床研究の取扱いに関する手続

(1) 特定臨床研究(※)の取扱いに係る措置

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。

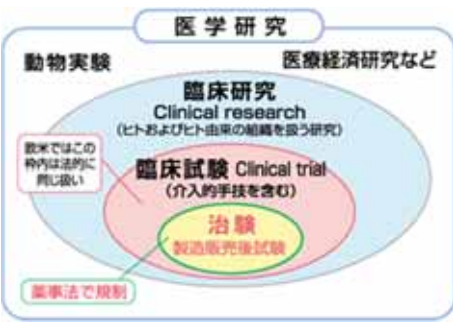
② 厚生労働大臣は、保健衛生上の危害の発生・拡大防止のために必要な場合には、改善命令を経ることなく特定臨床研究の停止等を命じることができる。

2. 製薬企業等の責務に関する措置

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を(※詳細は厚生労働省令で規定)の公表を義務付け。

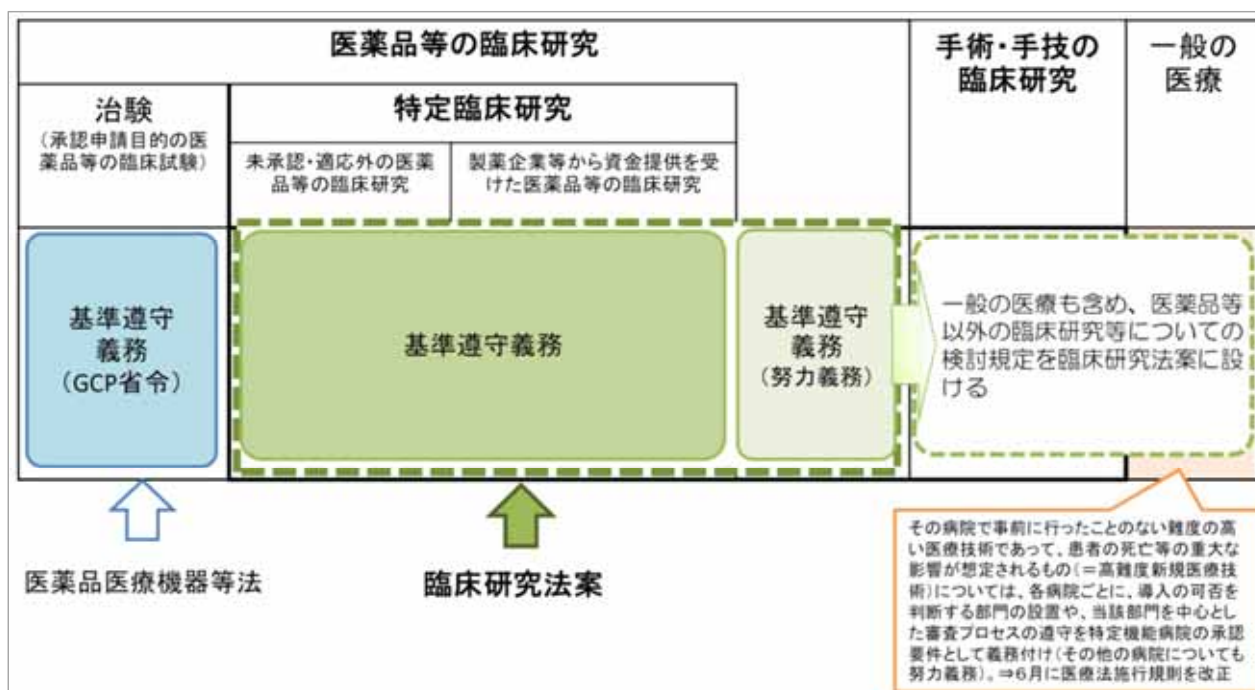
施行期日
公布の日(平成29年4月14日)から起算して1年を超えない範囲内において政令で定める日



1. 動物実験	2. 臨床研究
3. 臨床試験	4. 治療
5. 製薬臨床試験	6. 介入的処置
7. 医療経済研究	8. 動物実験
9. 臨床試験	10. 治療
11. 製薬臨床試験	12. 介入的処置
13. 医療経済研究	14. 動物実験
15. 臨床試験	16. 治療
17. 製薬臨床試験	18. 介入的処置
19. 医療経済研究	20. 動物実験
21. 臨床試験	22. 治療
23. 製薬臨床試験	24. 介入的処置
25. 医療経済研究	26. 動物実験
27. 臨床試験	28. 治療
29. 製薬臨床試験	30. 介入的処置
31. 医療経済研究	32. 動物実験
33. 臨床試験	34. 治療
35. 製薬臨床試験	36. 介入的処置
37. 医療経済研究	38. 動物実験
39. 臨床試験	40. 治療
41. 製薬臨床試験	42. 介入的処置
43. 医療経済研究	44. 動物実験
45. 臨床試験	46. 治療
47. 製薬臨床試験	48. 介入的処置
49. 医療経済研究	50. 動物実験
51. 臨床試験	52. 治療
53. 製薬臨床試験	54. 介入的処置
55. 医療経済研究	56. 動物実験
57. 臨床試験	58. 治療
59. 製薬臨床試験	60. 介入的処置
61. 医療経済研究	62. 動物実験
63. 臨床試験	64. 治療
65. 製薬臨床試験	66. 介入的処置
67. 医療経済研究	68. 動物実験
69. 臨床試験	70. 治療
71. 製薬臨床試験	72. 介入的処置
73. 医療経済研究	74. 動物実験
75. 臨床試験	76. 治療
77. 製薬臨床試験	78. 介入的処置
79. 医療経済研究	80. 動物実験
81. 臨床試験	82. 治療
83. 製薬臨床試験	84. 介入的処置
85. 医療経済研究	86. 動物実験
87. 臨床試験	88. 治療
89. 製薬臨床試験	90. 介入的処置
91. 医療経済研究	92. 動物実験
93. 臨床試験	94. 治療
95. 製薬臨床試験	96. 介入的処置
97. 医療経済研究	98. 動物実験
99. 臨床試験	100. 治療
101. 製薬臨床試験	102. 介入的処置
103. 医療経済研究	104. 動物実験
105. 臨床試験	106. 治療
107. 製薬臨床試験	108. 介入的処置
109. 医療経済研究	110. 動物実験
111. 臨床試験	112. 治療
113. 製薬臨床試験	114. 介入的処置
115. 医療経済研究	116. 動物実験
117. 臨床試験	118. 治療
119. 製薬臨床試験	120. 介入的処置
121. 医療経済研究	122. 動物実験
123. 臨床試験	124. 治療
125. 製薬臨床試験	126. 介入的処置
127. 医療経済研究	128. 動物実験
129. 臨床試験	130. 治療
131. 製薬臨床試験	132. 介入的処置
133. 医療経済研究	134. 動物実験
135. 臨床試験	136. 治療
137. 製薬臨床試験	138. 介入的処置
139. 医療経済研究	140. 動物実験
141. 臨床試験	142. 治療
143. 製薬臨床試験	144. 介入的処置
145. 医療経済研究	146. 動物実験
147. 臨床試験	148. 治療
149. 製薬臨床試験	150. 介入的処置
151. 医療経済研究	152. 動物実験
153. 臨床試験	154. 治療
155. 製薬臨床試験	156. 介入的処置
157. 医療経済研究	158. 動物実験
159. 臨床試験	160. 治療
161. 製薬臨床試験	162. 介入的処置
163. 医療経済研究	164. 動物実験
165. 臨床試験	166. 治療
167. 製薬臨床試験	168. 介入的処置
169. 医療経済研究	170. 動物実験
171. 臨床試験	172. 治療
173. 製薬臨床試験	174. 介入的処置
175. 医療経済研究	176. 動物実験
177. 臨床試験	178. 治療
179. 製薬臨床試験	180. 介入的処置
181. 医療経済研究	182. 動物実験
183. 臨床試験	184. 治療
185. 製薬臨床試験	186. 介入的処置
187. 医療経済研究	188. 動物実験
189. 臨床試験	190. 治療
191. 製薬臨床試験	192. 介入的処置
193. 医療経済研究	194. 動物実験
195. 臨床試験	196. 治療
197. 製薬臨床試験	198. 介入的処置
199. 医療経済研究	200. 動物実験



医療における規制の区分



7



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。

8



デジタル・フォレンジックとは (I D F の H P 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
 - P A C S
 - D W H
- 部門システム
- 自科検査機器
- B Y O D
- 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
- ランサムウェア
- 「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



"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>

13



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
- ランサムウェア
- 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



14



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



U S B 紛失事例 1

埼玉県立病院医師、患者情報入り U S B 紛失 治療内容など 3 6 0 0 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U S B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U S B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、U S B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。U S B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。



U S B 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。



U S B 紛失事例 3

患者の個人情報記録U S B 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U S B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U S Bを使用。23日に再び使用しようとした際、本来の保管場所が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。

U S B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)



目次

1. はじめに	1
2. 調査方法	2
3. 医療機器とは	3
4. 医療機器セキュリティに関する総論事項	5
4.1. 概要	5
4.2. 総論事項概要	8
4.2.1. 米国ボストンの胎児モニタへの感染事例	8
4.2.2. ベースメーカー/ICDの脆弱性事例 (Daniel Nalzer)	8
4.2.3. Jerome Radcliffe氏によるインスリンポンプへのハッキング	10
4.2.4. Barnaby Jack氏による心臓ペースメーカーへのハッキング	11
4.2.5. Roche製の複数の医療機器の Symantec pcAnywhereに関する脆弱性	12
4.2.6. Roche製生化学自動分析装置のソフトウェア脆弱性	13
4.2.7. ICS-CERTによるインターネットからアクセス可能な医療機器の脆弱性	14
4.2.8. 2013年6月FDA告知での調査事例	14
4.2.9. ICS-CERT Alert「Medical Devices: Hard-Coded Passwords」	14
5. 国内外の医療機器セキュリティに対する取り組み	16
5.1. 米国における取り組み	16
5.1.1. 米国の全体像	16
5.1.2. 取組み事例	17
5.2. 欧州における取り組み	26
5.2.1. 欧州の全体像	26
5.2.2. 取組み事例	26
5.3. 国際標準における動向	29
5.3.1. 国際標準に関する全体概要	29
5.3.2. 国際標準の事例	30
5.4. 日本における取り組み	30
5.4.1. 日本における取組みの全体像	30
5.4.2. 取組み事例	30
5.4.3. 政策及び市場動向	30
6. ヒアリング結果の分析	37
6.1. ヒアリング結果の分類について	37
6.2. 医療機器セキュリティの現状	39
6.2.1. セキュリティに関する取組み	49
6.2.2. セキュリティインシデント事例	50
6.3. 対策見直し	51
6.4. 医療機器セキュリティに関する課題	53
6.5. 医療機器分野の関係者からの要望	54
7. 医療機器に関する情報セキュリティの現状及び見直し	57
7.1. 考慮すべき環境変化	57
7.2. 調査におけるまとめ	57
7.3. 謝辞	59



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 ¹⁾	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 ²⁾	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 ³⁾	2008年に Medical Device Security Center によってペースメーカー/ICD (Implantable Cardioverter Defibrillator) へのハッキングし、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) ⁴⁾	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「致命的な攻撃」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 ⁵⁾	Roche製の複数の医療機器で使われている Symantec pcAnywhere の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 ⁶⁾	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横断したマルウェア等) ⁷⁾	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横断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 ⁸⁾	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（ディスクバリー）

- 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

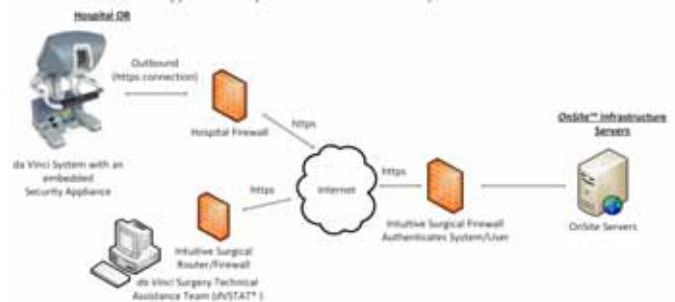
- 在宅医療見守り
- スマートホスピタルライティングシステム
- 服薬支援容器
- スマートウォッチ
- 空気清浄機能付き扇風機
- 衣料型ウェアラブルシステム
- スマート歯ブラシアタッチメント
- 体組成計
- 見守り機能付き電動ポット
- センサー内蔵ベッド
- 糖尿病患者医療支援コンタクトレンズ
- 救命救急補助スマートフォンアプリ



手術ロボットの遠隔支援



1. OnSite™ for the da Vinci System Overview	3
2. Requirements	5
3. Detailed Hardware, Software and Features	6
4. Data Flow Process	7
5. Security and Access Control	7
6. Security Patching Strategy	8
7. Monitoring	8
8. Third Party Audits and Certifications	8
9. Security Administration Roles and Responsibilities	9
10. Antivirus and Malware	9
11. Backup and Recovery	9
12. Storage Management	9
13. Disaster Recovery	9
14. Support Requirements	9
15. Patient Privacy	9
Appendix 1 – System Log	10
Appendix 2 – Optional Wireless Connectivity Kit	10



Connected Medical Device & IOT Security Summit



THE CONNECTED MEDICAL DEVICE AND IOT SECURITY SUMMIT

November 8 - 9, 2017
Best Western Plus Hotel and Conference Center
Baltimore, MD

Supporting Organizations:
American College of Clinical Engineering (ACCE)
The Society for Participatory Medicine

Gold Sponsor: CloudPost Networks

後援：
アメリカ臨床工学会
参加型医療学会

Ben Wilson, MBA, MPH, Vice President, Business Development, Healthcare, CloudPost Networks
To Be Announced, Independent Security Evaluators
Additional Speakers To Be Announced

For information on speaking, sponsorship/exhibition opportunities and registration, please contact:
Suzette Kavanagh, Managing Director, TCBI
Ph: 330.353.3339 Email: skavanagh@tcbi.com

PRELIMINARY AGENDA

DAY ONE, WEDNESDAY, NOVEMBER 8, 2017

8:00 Registration / Sponsor and Exhibitor Showcases / Networking Breakfast

8:15 CHAIRPERSON'S OPENING REMARKS
As the demand for shared health data and interconnected clinical systems rises to meet quality and pay-for-performance needs, the use of personal and commercial IOT is also accelerating. Manufacturers need every viable cybersecurity technique they can muster to protect the healthcare and technology industries, government and the general public, the most important being transparency to the attention of patients and the general public. We must together identify threats, solutions, and realistic paths forward to ensure not just our privacy and security, but the stability of our healthcare industry.

This presentation will offer a summary and analysis of recent concerning and emerging cybersecurity threats in healthcare, from the Malware Protection Medical Center ransomware attack, to St. Jude's, the Anthem Breach, Baltimore, the Equifax breach, and the sale of Australian Medicare records on the web.

Michael Rubin, MBA, Founder & President, Red Hat Healthcare Inc.

8:45 KEYNOTE ADDRESS: THE ECONOMICS AND ECOSYSTEM OF THE DARK WEB
The scourge of the cyber crime ecosystem, and other consequences of leaking virus writing, malware, and ransomware will form the "bad guys" part of our, along with discussion for some threats concerning other threats of our society.

Ben Williams, Chief Architect, IBM Security Systems

9:30 KEYNOTE ADDRESS: MEDSEC VS. ST. JUDE MEDICAL: IMPLANTABLE DEVICES, VULNERABILITIES, AND THE LAW
In 2016, the security research firm Medsec and hedge fund Medsec Waters disclosed the presence of serious vulnerabilities in St. Jude Medical (SJM) implantable cardiac devices. In August 2017, SJM announced a historical recall of approximately 405,000 implantable devices. Dr. Green was one of the outside researchers invited to critique Medsec's findings. This talk will explore the technical aspects of the vulnerability and analyze the long term implications for medical device security.

Matthew Green, PhD, Assistant Professor, Department of Computer Science, Johns Hopkins University

10:15 Sponsor / Exhibitor Showcases & Refreshments 10-11

10:45 KEYNOTE ADDRESS: REGULATORY ADVANCES

The most recent guidance and advice from the FDA on Cybersecurity, Software Development, Post-market surveillance, and the collection of real-world evidence will be presented and discussed.

John F. Murray, Software Compliance Expert, Office of Compliance, CDRH, FDA

11:30 US LEGAL AND REGULATORY FRAMEWORK
Numerous legal obligations have emerged for managing cyber risk for connected medical devices. This session will explore various cybersecurity laws, regulations, and standards governing design, development, deployment, and support for such devices. Learn about legal considerations for incident response and vulnerability disclosure.

Paul Ota, Senior Associate, Hogan Lovells

12:15 Sponsor / Exhibitor Showcases & Lunches

1:15 SESSION TO BE ANNOUNCED

1:45 DISCLOSURE MEDICAL DEVICE CYBERSECURITY VULNERABILITIES: LESSONS LEARNED FROM A MEDICAL DEVICE MANUFACTURER
Participants will hear the on-site behind-the-scenes of one medical device manufacturer coordinated vulnerability disclosure. The talk reveals what really went on behind the scenes and how the manufacturer handled the disclosure. The talk reveals what really went on behind the scenes and how the manufacturer handled the disclosure. The talk reveals what really went on behind the scenes and how the manufacturer handled the disclosure.

12:30 SESSION TO BE ANNOUNCED

3:00 COGNITIVE DEVICES, INTERNET OF HOSPITAL THINGS - IOHT, SMART DEVICES, SAFER CARE
In today's clinical environment, the amount of device information can be staggering and an ever-jamming obstacle to struggling with what it all means. The smart data machine today creates so much data today along with data sharing that create confusion. With the advent of cognitive computing, we now have the ability to create digital agents to address many aspects of this device information tsunami and opportunities to synthesize device data. Cognitive computing at the edge offers the potential to eliminate false alarms, correct data streams for diagnosis, and enable in-real-time predictive care.

The cognitive agents can now live on the instrument, can combine with other systems, and create smart clinical systems that provide continuous monitoring. This self-assembling and cognitive collaboration enables smarter sensing and predictive capabilities not available today.

In addition, with the advent of cognitive computing at the edge, we can enable better systems that can enable new security models. These devices, by bringing AI technology to the device and software, can create smart systems that can detect unusual activity quickly, react and enable ever-changing encryption and security models. This session will cover the evolution of device, the cognitive networking.



Connected Medical Device & IOT Security Summit



THE CONNECTED MEDICAL DEVICE & IOT SECURITY SUMMIT

January 25-26, 2018
Best Western Plus Hotel & Conference Center
Baltimore, MD

REGISTRATION

OUTVIEW
Healthcare providers and medical device companies are currently facing many growing threats, legal concerns, and patient safety challenges as a result of connected devices. Millions of vulnerable and insecure devices are connected from common to all healthcare settings for the first time in the history of the industry. This talk will explore the current state of device and cloud security, the challenges of "black box" medical device security, and the path forward to secure and resilient systems.

SUPPORTING ORGANIZATIONS
ACCE
INCOSE
Participatory
BRONZE SPONSOR
Integra
MIND

CONNECT WITH US
SUPPORTING PUBLICATIONS
Blockchain Healthcare Review
FierceHealthcare
FierceMedTech
Healthcare Guys

- 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

事務連絡
平成28年11月1日付

（都道府県）
各（保健所）
衛生主管官（長）御中

厚生労働省医政局総務課医療安全推進室

画像診断報告書の確認不足に関する医療安全対策について

当院、医療機関において、放射線科へ画像診断を依頼した医師（以下「依頼医」という。）に、画像診断報告書に記載されている内容が適切に伝達されず、治療が遅れにより患者が死亡する事象の報告が続いているところです。

同様の事象に迅速する依頼については、これまで、医療法施行規則（昭和25年厚生省令第36号）第12条に基づき医療事故調査等事象において、公益財団法人日本医療機能評価機構から「画像診断報告書の確認不足」（医療安全情報№48、平成24年2月、別添1）が提出され、注意喚起が図られてきています。

また、同様の操作で生じる他の検査報告書の確認不足についても、「病理診断報告書の確認忘れ」（医療安全情報№24、平成24年10月、別添2）や「パニック値の緊急連絡の遅れ」（医療安全情報№111、平成28年2月、別添3）によって注意喚起を図ってきたところです。

つきましては、画像診断報告書の確認不足を防止するため、別添の内容を御確認の上、貴管下医療機関に対し、改めて周知徹底をお願いいたします。

なお、医療事故情報収集等事象の内容については、公益財団法人日本医療機能評価機構のホームページ（「報告書」タブ）<http://www.med-eval.jp/content/index.aspx?menu=004>、「医療安全情報」<http://www.med-eval.jp/content/info/index.html>）にも掲載されていますことを申し添えます。

公益財団法人 日本医療機能評価機構
医療安全情報 No.71 2012年10月

病理診断報告書の確認忘れ

病理検査を行った際、検査結果の報告書を確認しなかったことにより、治療が遅れた事例が報告されています。

病理検査を行った際、検査結果の報告書を確認しなかったことにより、治療が遅れた事例が報告されています。

検査	確認しなかった検査項目	結果に異常が生じた例
子宮頸癌細胞診	クラス、扁平上皮がん	1例中等
上部消化管内視鏡検査の細胞診	Groupの記載が、	2例中等
	胃の「悪性」所見	2例中等
	胃の癌分化型が、	1例中等
腎臓生検	癌腫が、	1例中等
	癌が、	1例中等
腎臓生検と泌尿器科の癌中継り細胞診	癌がん細胞	1ヶ月以内

公益財団法人 日本医療機能評価機構
医療安全情報 No.62 2012年10月

画像診断報告書の確認不足

事例

当院で依頼した画像診断報告書の確認不足により、治療が遅れた事例が報告されています。

事例が発生した医療機関の取り組み

- 主治医は、放射線科専門医の画像診断報告書を確認する。患者に画像検査の結果を説明する。
- 放射線科専門医は、誤って検査の目的以外の重大な所見を発見した場合、速報した医師に注意喚起する。

総合評価委員の意見

- 入院（特に退院前）、外来を問わず、画像診断報告書が確認できる仕組みを医療機関内で構築する。



公益財団法人 日本医療機能評価機構
医療安全情報 No.71 2012年10月

病理診断報告書の確認忘れ

病理検査を行った際、検査結果の報告書を確認しなかったことにより、治療が遅れた事例が報告されています。

検査	確認しなかった検査項目	結果に異常が生じた例
子宮頸癌細胞診	クラス、扁平上皮がん	1例中等
上部消化管内視鏡検査の細胞診	Groupの記載が、	2例中等
	胃の「悪性」所見	2例中等
	胃の癌分化型が、	1例中等
腎臓生検	癌腫が、	1例中等
	癌が、	1例中等
腎臓生検と泌尿器科の癌中継り細胞診	癌がん細胞	1ヶ月以内

公益財団法人 日本医療機能評価機構
医療安全情報 No.71 2012年10月

病理診断報告書の確認忘れ

事例1

事例2

事例が発生した医療機関の取り組み

総合評価委員の意見

- 重大な所見については、速報確認に留意する仕組みを構築しましょう。

公益財団法人 日本医療機能評価機構
医療安全情報 No.111 2016年11月

パニック値の緊急連絡の遅れ

パニック値の緊急連絡が医師に伝わらなかったため、患者の治療が遅れた事例が報告されています。

検査項目	検査値	異常
グルコース	500mg/dL	患者は糖尿病で、検査時血糖値が異常に高くなり、脱水、意識障害
グルコース	800mg/dL	患者は糖尿病で、検査時血糖値が異常に高くなり、脱水、意識障害
カリウム	6.4mg/dL	患者は腎臓病で、検査時カリウム値が異常に高くなり、呼吸抑制、意識障害

公益財団法人 日本医療機能評価機構
医療安全情報 No.111 2016年11月

パニック値の緊急連絡の遅れ

事例1

事例2

事例が発生した医療機関の取り組み

総合評価委員の意見

- パニック値の緊急連絡が医師に伝わらなかったため、患者の治療が遅れた事例が報告されています。



PMDAの医療安全情報

このページはPMDAの医療安全情報に関するウェブサイトのスクリーンショットです。上部にはPMDAのロゴと「医療安全情報」のタイトルがあります。中央には「PMDA医療安全情報」という見出しがあり、その下に「一般名類似による薬剤取り違えについて」というトピックが紹介されています。右側には「PMDA医療安全情報」の目録がリストアップされています。

このインフォグラフィックは「PMDA医療安全情報」のNo.51 (2017年 9月)版です。テーマは「一般名類似による薬剤取り違えについて」です。POINTとして、薬剤師が一般名と一般名が類似する薬剤を処方する際、類似する薬剤に注意すること、および類似する薬剤が存在することを告知し、薬剤師の注意に留意すること、が挙げられています。また、類似する薬剤のリストが示されています。

このインフォグラフィックは「一般名類似による薬剤取り違えについて」の続きです。類似する薬剤のリストが示されています。リストには「一般名」と「類似する薬剤」の両方が記載されています。また、薬剤師が類似する薬剤を処方する際に注意すること、および類似する薬剤が存在することを告知し、薬剤師の注意に留意すること、が挙げられています。



このインフォグラフィックは「PMDA医療安全情報」のNo.44 (2014年 8月)版です。テーマは「医薬品処方オーダー時の選択間違い」です。POINTとして、処方箋を作成する際に、類似する薬剤を選択しないこと、および処方箋を作成する際に、類似する薬剤を選択しないこと、が挙げられています。また、類似する薬剤のリストが示されています。

このインフォグラフィックは「処方オーダー時の注意 (1)」に関するものです。類似する薬剤のリストが示されています。リストには「薬剤名」と「類似する薬剤」の両方が記載されています。また、薬剤師が類似する薬剤を処方する際に注意すること、および類似する薬剤が存在することを告知し、薬剤師の注意に留意すること、が挙げられています。

このインフォグラフィックは「処方オーダー時の注意 (2)」に関するものです。類似する薬剤のリストが示されています。リストには「薬剤名」と「類似する薬剤」の両方が記載されています。また、薬剤師が類似する薬剤を処方する際に注意すること、および類似する薬剤が存在することを告知し、薬剤師の注意に留意すること、が挙げられています。



PMDA 医療安全情報
fnds 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 センタールアラームに関する注意点（電流は流れ）

- 電流は、電圧力が低下する前に、自動的に交換すること。

電圧は長期間の使用や患者さんの場所などによって変動が低下します。電圧の交換時期についてはメーカーを定める。電圧がけりれる前に交換すること。アラームの発生を軽減することが重要です。

PMDA 医療安全情報
fnds No.29 2011年12月
心電図モニタの取扱い時の注意について

2 センタールアラームに関する注意点（電流は流れ）

- センタールモニタに電圧交換のマークなどが表示されたら、アラームの発報により、当該機種の電圧を速やかに交換すること。

電圧交換の手順

- 電源の切断
- 電源の再接続
- 電池交換
- 充電確認
- 充電完了確認
- 充電完了確認
- BATTERY LOW T

PMDA 医療安全情報
fnds No.29 2011年12月
その他心電図モニタの適正な使用について

4 その他心電図モニタの適正な使用について

心電図モニタの適正使用

OSAL 機器も購入した際でも電圧力に注意してください。（心電図モニターにも電圧力があります）

適正なアラームの設置

心電図機器や患者さんのアラームは、患者の体側に設置していただきます。（心電図モニターにも電圧力があります）

患者さんに近い、心電図モニタの設置は心電図の取扱い時の注意を守っていただきます。

アラームの適正な設置によって、感報はアラームを鳴らすことが出来ます。

本機種の設置方法

- この製品の設置方法は、対応する本機種の取扱説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。
- この機種の取扱いについては、取扱説明書の電圧交換部を参照してください。この機種の取扱いについては、取扱説明書の電圧交換部を参照してください。
- この機種の設置方法は、設置説明書の電圧交換部を参照してください。この機種の設置方法は、設置説明書の電圧交換部を参照してください。

PMDA 医療安全情報 fnds No.29 2011年12月



PMDA 医療安全情報
fnds 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 使用中の電圧に関する注意点について

- 人工呼吸器を使用する際は、AC電源が供給されていることをインジケータなどの表示で常に確認すること。

アラームに気づかずバッテリー充電に気がつかず、バッテリーが充電切れになると、換気停止となり、死の危険があります。

PMDA 医療安全情報
fnds 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）

2 使用中の電圧の表示例（1）

ドレープ・システム（1）

ドレープ・システム（2）

アイズ・アイ（1）

アイズ・アイ（2）

コブディオン・システム（1）

コブディオン・システム（2）

このように、使用中の電圧の表示は製品によって様子です。電圧の表示は「この」・「この」に表示されるので、あらかじめ確認しておきましょう！

PMDA 医療安全情報
fnds 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）

2 電圧表示の異常としり止め対策について

電圧表示の異常としり止めのため、電圧表示の低下のようなエラー状態になったときは、気づかずしてはいけません。

本機種の設置方法

- この製品の設置方法は、対応する本機種の取扱説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。設置方法は、設置説明書の電圧交換部を参照してください。
- この機種の取扱いについては、取扱説明書の電圧交換部を参照してください。この機種の取扱いについては、取扱説明書の電圧交換部を参照してください。
- この機種の設置方法は、設置説明書の電圧交換部を参照してください。この機種の設置方法は、設置説明書の電圧交換部を参照してください。

PMDA 医療安全情報 fnds No.20 2010年11月



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