医療情報学連合大会共催三菱電機展示ルームセミナー
テーマ：電子文書交換・地域医療連携・セキュリティ

医療機器におけるサイバーセキュリティ対策の最新動向

日本光電工業株式会社　技術戦略本部
一般社団法人　電子情報技術産業協会
医療用ソフトウェア専門委員会　委員長

松元 恒一郎

2022年11月20日
第42回医療情報学連合大会
札幌コンベンションセンター201+202会議室

自己紹介

- 日本光電工業株式会社入社
  ー生体情報モニタの開発に従事
  　システム設計，ソフトウェア開発（麻酔関連，薬剤計算処理，アラーム処理等臨床に関連する機能等）
  ー心電計開発，ホルター心電計開発
  ー現在，技術戦略本部
- 2000年頃より医用波形規約の標準化であるMFER（Medical waveform Format Encoding Rules）シリーズ（22077-XX）のISO規格作成
- ISO/TC215 Medical Informatics　WG2/WG4/JWG7　エキスパート
- AAMI/UL 2800-1（Interoperability）プロジェクト　オブザーバー
- DICOM WG32（Neurophysiology Waveforms）オブザーバー
- HL7 Health Care Device WG・Anesthesia WG　メンバー
- 一般社団法人 電子情報技術産業協会（JEITA）ヘルスケアインダストリ部会　医療用ソフトウェア専門委員会　委員長
- 一般社団法人 日本医療機器産業連合会（医機連）
  医療機器サイバーセキュリティWG　副主査，サイバーセキュリティTF，医療ICT推進WG，AI-WG　副主査，
  個人情報取扱対応分科会，プログラム医療機器対応WG規制対応Sub-WG，サイバーセキュリティの不具合報告Sub-WG
- 厚生労働省　「医療情報システムの安全管理に関するガイドライン」改定に向けた調査一式　改定作業班　令和元年～令和2年　構成員
- 経済産業省　産業サイバーセキュリティ研究会WG１『第２層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース　令和元年～令和4年　委員
- AMED 医薬品等規制調和・評価研究事業　データ等の通信機能を有する医療機器開発における相互運用性確保のためのガイダンス策定に関する研究　令和元年～　研究協力者

医療機器のサイバーセキュリティ対応の必要性

- 医療機関

患者カルテ等の情報が電子化されており，個人情報を含む電子情報が医療機関ネットワーク内にてやり取りされる状況.

医療機関のネットワークにおいては，医療情報システムに関するガイドラインとして取りまとめられた「医療情報システムの安全管理に関するガイドライン第5.2版」(令和4年3月)に従って，医療情報システムの適正な運用等を行うことが重要である.

- 医療機器

製品自体の品質・有効性・安全性が担保された上で，使用者による適正使用がなされることにより，医療機器の有効性及び安全性が確保，疾病の診断及び治療等に利用されるIoT機器等の基盤となる通信技術の進歩に伴い，医療機器が医療機関のネットワーク，他の医療機器又は電子機器と接続される機会がさらに増加される.

- 医療機関のネットワークに接続される医療機器が，直接又は二次的に攻撃を受けた場合，その医療機器自体が機能を失う等の障害だけでなく，当該医療機器が接続された医療機関のネットワーク等を介して同様の障害が拡大する可能性が想定される．これらの事象は，診断・治療の遅れ又は誤り等の結果として，患者に健康危害を及ぼすことがある.

医療機器の有効性及び安全性を確保するために
サイバーセキュリティの重要性が増し，持続的な対応が必要

今回は，現在発出されているIoTセキュリティガイドライン，医療機器のサイバーセキュリティの確保について，IMDRF文書を参考に，医療機器の製造販売業者が行うべきサイバーセキュリティへの取り組みについて説明する.

手術室内の医療機器

目次

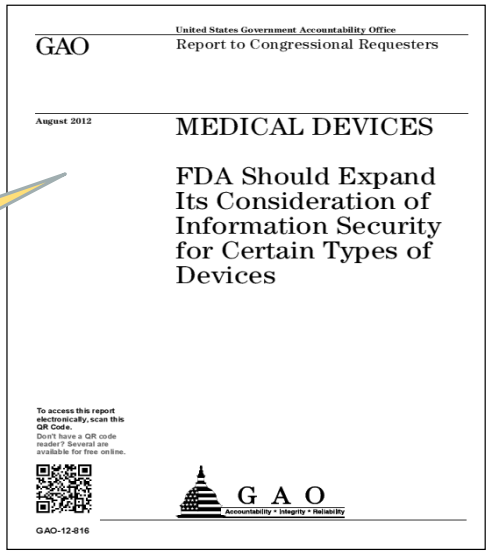
1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

目次

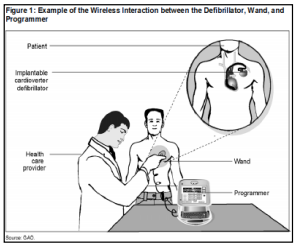
1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

医療機関・医療機器を経由して侵入されるセキュリティリスク

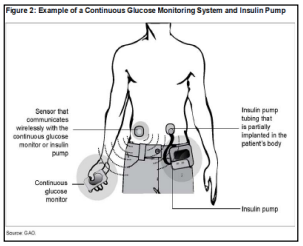
米国医療におけるサイバーセキュリティの警告
2012年8月GAOレポート


United States Government Accountability Office
GAO
Report to Congressional Requesters
August 2012
MEDICAL DEVICES
FDA Should Expand Its Consideration of Information Security for Certain Types of Devices
To access this report electronically, scan this QR Code.
Don't have a QR code reader? Several are available for free online.
GAO
Accountability * Integrity * Reliability
GAO-12-816

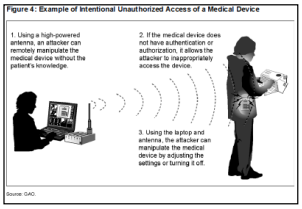
FDAはこのような機器の情報セキュリティへの考慮を拡大すべきだ.



植え込み型除細動器



インスリンポンプ



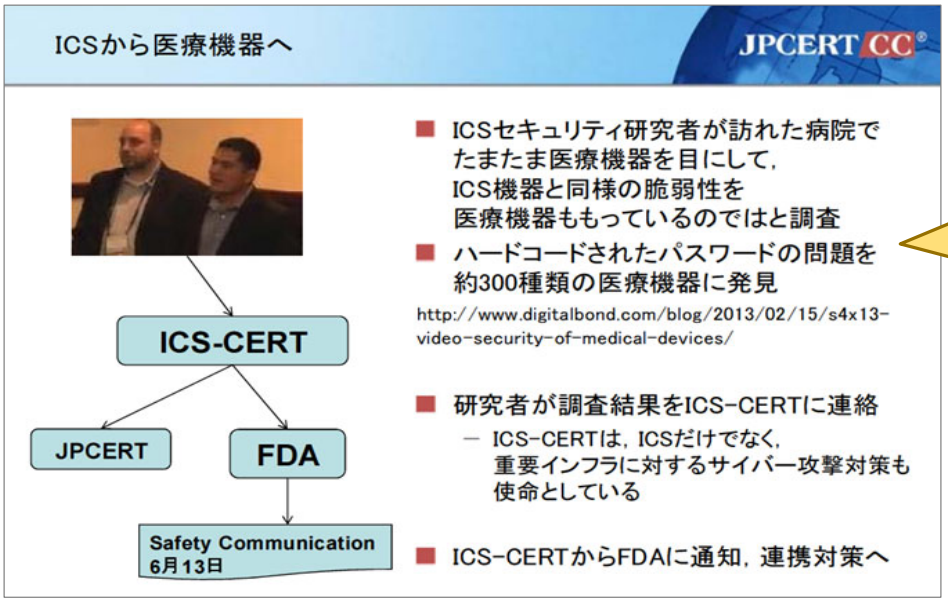
無線接続可能医療機器

GAO: United States Government Accountability Office, 米国政府説明責任局

セキュリティリスクの変遷

2013年　医療機器を調査

- 米国ICS-CERTが医療機器の中にハードコードされているパスワードについて注意喚起(6月13日)
  (約40ベンダーの約300の医療機器)
- FDAがMedical Device Cybersecurityに関するガイダンスのドラフトを公開(6月14日)



ICS-CERT，JPCERT/CC からの医療機器の脆弱性（変更できないパスワード）の指摘を受け，FDAが医療機器製造業者へ注意を勧告.

ICS-CERT(The Industrial Control System Cyber Emergency Response Team) 重要インフラを対象としたサイバーセキュリティ情報の集約，分析を行う機関.
JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）

2014年　医療機器へのサイバー攻撃（標的型攻撃の入口に）

- 医療機器のハッキングは，容易(4月25日)
  （薬物注入ポンプやX線検査装置が容易にハッキングできる）
- 米国の病院に中国からサイバー攻撃、患者450万人のデータが流出(8月19日)
  （狙われたのは，医療機器の開発・研究（治験）データなどの知的財産）

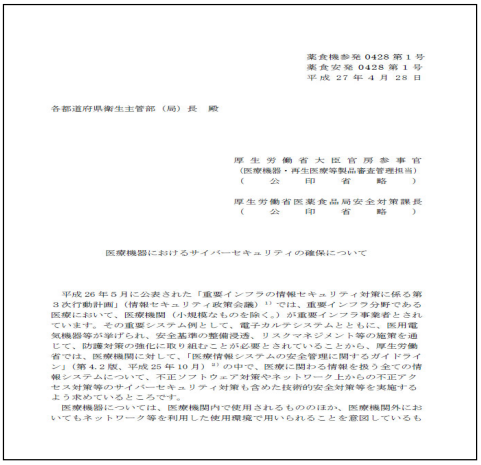
新聞記事と厚生労働省通知


命の情報「セキュリティー甘い」
サイバー攻撃 医療機器 標的
防御体制 日米で差
スキャナー SCANNER

3月開催の医療ハッカソン　実際に医療現場で使われている4種のソフトウェアを対象に解析し，見つけた脆弱性の深刻度を競う競技．制限時間内に100件以上見つかった．
脆弱性：プログラムのミスなどによるセキュリティ上の弱点で，放置するとサイバー攻撃に悪用されやすい．

日本の厚労省は電子カルテなどの医療情報システムの安全管理についてはガイドラインを公表しているが，医療機器についてはない．経産省も2014年規制対象外のヘルスケア製品についてガイドラインを出したが，サイバーセキュリティについては「今後の課題」とした．

医療機器におけるサイバーセキュリティの確保について
（平成27年4月28日）
(薬食機参発0428第1号/薬食安発0428第1号)
https://www.pmda.go.jp/files/000204891.pdf


薬食機参発 0428 第 1 号
薬食安発 0428 第 1 号
平成 27 年 4 月 28 日

各都道府県衛生主管部（局）長　殿

厚生労働省大臣官房参事官
（医療機器・再生医療等製品審査管理担当）
（　公　印　省　略　）

厚生労働省医薬食品局安全対策課長
（　公　印　省　略　）

医療機器におけるサイバーセキュリティの確保について

平成 26 年 5 月に公表された「重要インフラの情報セキュリティ対策に係る第3次行動計画」（情報セキュリティ政策会議）[1]では、重要インフラ分野である医療において、医療機関（小規模なものを除く。）が重要インフラ事業者とされています。その重要システム例として、電子カルテシステムとともに、医用電気機器等が挙げられ、安全基準の整備浸透、リスクマネジメント等の施策を通じて、防護対策の強化に取り組むことが必要とされていることから、厚生労働省では、医療機関に対して、「医療情報システムの安全管理に関するガイドライン」（第4.2版、平成25年10月）[2]のなかで、医療に関わる情報を扱う全ての情報システムについて、不正ソフトウェア対策やネットワーク上からの不正アクセス対策等のサイバーセキュリティ対策も含めた技術的安全対策等を実施するよう求めているところです。

医療機器については、医療機関内で使用されるもののほか、医療機関外においてもネットワーク等を利用した使用環境で用いられることを意図しているも

2015年　医療機関への攻撃

- 病院の侵入に医療機器が悪用される(6月8日)
  （医療機器にバックドア）
- GEの複数の医療機器に複数の脆弱性が公開(7月10日)
- FDAがHospira Lifecare PCA Infusion Systemの利用中止を指示(7月31日)

医療機器のサイバーセキュリティの不備について規制当局が有害事象として警告を発信

■ Symbiq Infusion System by Hospira: FDA Safety Communication
　- Cybersecurity Vulnerabilities

米FDAおよびHospiraは，HospiraのSymbiq Infusion Systemに関するセキュリティの脆弱性を認識した．Hospiraと独立した調査機関によって，当該製品が遠隔的に病院のネットワークを通してアクセス可能であり，権限のないユーザーがポンプの注入量を変更することが可能な状況にあることが確認された．Hospiraは，当該製品の製造，販売を中止し，カスタマーとともに他システムへの移行を実施している．FDAは，医療機関に対し当該システムの使用を中止し，他システムへ移行するよう強く勧めていること，最新の情報について積極的に調査していることなどについて記載．
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

Hospira は，2013年にSymbiq Pumpの生産を終了しているが，未使用のネットワークポート(ポート20/FTP, ポート 23/TELNET)に対してアクセス可能になっていることが分かった．

2017年以降　ランサムウェア「WannaCry」への大規模感染が始まる

2020年6月　Ripple20（IoTデバイス・ネットワーク機器等に影響する脆弱性）

- 米国のTreck社が開発したTCP/IP通信用ライブラリに存在する19個の脆弱性の総称.
- 通信・小売・商社・医療・輸送・工業・エネルギー等広範囲の業界で使用されているとみられている.
- 医療機器に影響がある可能性.

2020年9月　医療機関へのサイバー攻撃

- First death reported following a ransomware attack on a German hospital

独デュッセルドルフ大学病院が，9月10日にランサムウェア攻撃を受けた．同病院が院内の30台以上のサーバに感染したランサムウェア攻撃に対応中に，同病院に救急搬送される予定だった女性患者を受け入れることができず，この患者は30km以上離れた別の病院へ搬送されることになり，死亡．警察が現在捜査中で，ランサムウェア攻撃と病院の稼動停止時間が患者の死亡の直接的な原因であることが判明した場合，捜査を殺人事件に切り替える予定．病院関係者のSNS投稿によると，ランサムウェア感染の原因は，広く使われている商用ソフトウェアの脆弱性で，BSI（ドイツ連邦政府情報セキュリティ局）にインシデントについて報告.

- Massachusetts Hospital Investigates　'Data Security Incident'

米マサチューセッツ州の病院Lawrence General Hospital，9月19日にデータセキュリティインシデントが発生し，同病院のシステムが，36時間オフラインとなった．その間，救急車で搬送されて来た患者は他の病院へ搬送され，病院スタッフは医療フォームに手書きで記入し，電話や対面のミーティングで連絡を取り合った．同病院は現在，フォレンジック会社と協力してインシデントの詳細を調査中で，主要な臨床関連のシステムは復旧し，患者のケアを引き続き行っている.

2021年3月　ENISAとCERT-EUの連携強化

- ENISA and CERT-EU to improve the EU cybersecurity framework
- 欧州サイバーセキュリティ庁（ENISA）と欧州コンピュータ緊急対応チーム（CERT-EU），欧州におけるサイバー脅威やインシデントを予防，検知，対応するための機能と準備を構築・強化するために，互いの業務を支援し，より高い効率性を達成するためのサイバーセキュリティの枠組みを設定する覚書（MOU）を締結.

2021年8月　BlackBerry OSの脆弱性：車の所有者や病院にとって深刻な悪材料

- BlackBerry OS vulnerability is seriously bad news for car owners, hospitals
- BlackBerry社，同社の組み込みOSであるQNXにメモリ関数の使用に起因する複数の脆弱性「BadAlloc」が存在することを認めた.
- 今年初めにこの脆弱を発見したMicrosoft社が，米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）に報告した.
- 数百万台の自動車，病院や工場の重要な機器がハッカーに悪用される可能性がある.
- 厚生労働省からも協調（調整）と情報開示された.

2021年10月　ランサムウェア攻撃：新生児の死をめぐって

- 2019年7月に臍帯を首に巻いて生まれ，9ヶ月後に亡くなった大きな脳損傷を引き起こしたと裁判所文書は述べている.
- 2020年6月に提出された法廷文書では，弁護士は，スプリングヒル医療センターとその親会社がサイバー攻撃を防ぐのに十分なことをしておらず，状況の深刻さを隠すために共謀したと非難している.
- この訴訟は，身代金攻撃が電子機器の故障をもたらしたと主張しており，医師は出産中に子供の状態を適切に監視できず，脳損傷を引き起こした.

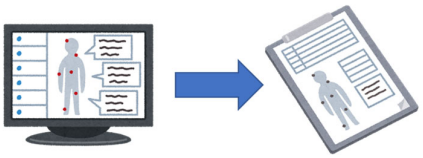
国内のサイバー攻撃の事例

患者，医療従事者へ多大なる影響を及ぼした事例

市立病院（2018年10月）

攻撃の内容

- 電子カルテシステムへのランサムウェア攻撃.
- 電子カルテシステムを全面停止して、紙カルテの運用へ切り替え.
- 停止期間は，2日間.
- 個人情報の漏えいや悪用といった被害報告はなし.



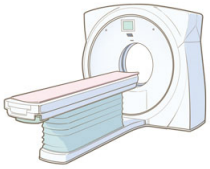
原因

- ウイルスの感染源を特定することはできず.
- しかし，**医療情報システムに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基本的なルールが遵守されなかった**ことによって発生した可能性.

大学病院（2017年　※公表は，2020年）

攻撃の内容

- 検査装置へのランサムウェア攻撃.
- CT撮影中に端末が再起動を起こし，撮影画像が保存されていなかったことで再撮影を施行.
- 撮影した画像の読み取りができなかったことで再撮影を施行.



原因

- **ランサムウェアに感染していた端末を院内ネットワークに接続した**ことによる感染.

AMEDサイバーセキュリティ研究班資料より引用

2021年6月28日　厚労省通知：医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)

- ４月30 日付けで発出された内閣官房内閣サイバーセキュリティセンターからの注意喚起について，改めて貴管内の医療機関に対し周知するとともに，ランサムウェアによるサイバー攻撃の解説及び対策例を参考に関係医療機関に対し注意喚起.

2021年10月　ランサムウェア攻撃：徳島県つるぎ町立半田病院

- 10月31日，電子カルテ他院内システムがランサムウェアに感染し，カルテが閲覧できなくなるなどの大きな被害.
- 調査復旧を請け負った事業者の作業，電子カルテ業者の仮システムの構築，そして、電子カルテより必要に応じて抽出していたデータなどを利用し，令和4年1月4日に通常診療を再開.

2022年10月　ランサムウェア攻撃：大阪急性期・総合医療センター

- 10月31日，電子カルテ他院内システムがランサムウェアに感染し，カルテが閲覧できなくなるなどの大きな被害.
- 通常の外来診療や緊急以外の手術を停止しているほか，救急患者の受け入れもできない状況.
- 11月10日厚生労働省より「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」が発出.
- 攻撃の侵入経路は，医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判明.
- サプライチェーンリスク全体の確認として，自組織のみならずサプライチェーン全体を俯瞰し，発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから，関係事業者のセキュリティ管理体制を確認した上で，関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき脆弱性対策を実施する.

標的型攻撃とは？

従来のウイルスは不特定多数を無差別に攻撃するものが多かったが，標的型攻撃は情報の窃取や破壊などを目的として，特定の企業や組織に向けた攻撃を行う

標的型攻撃のプロセス：

- 興味を引く内容のメールで添付ファイルやURLを開かせる
- 添付ファイルやURLからウイルスを送り込む
- 送り込んだウイルスを利用して攻撃を実施する

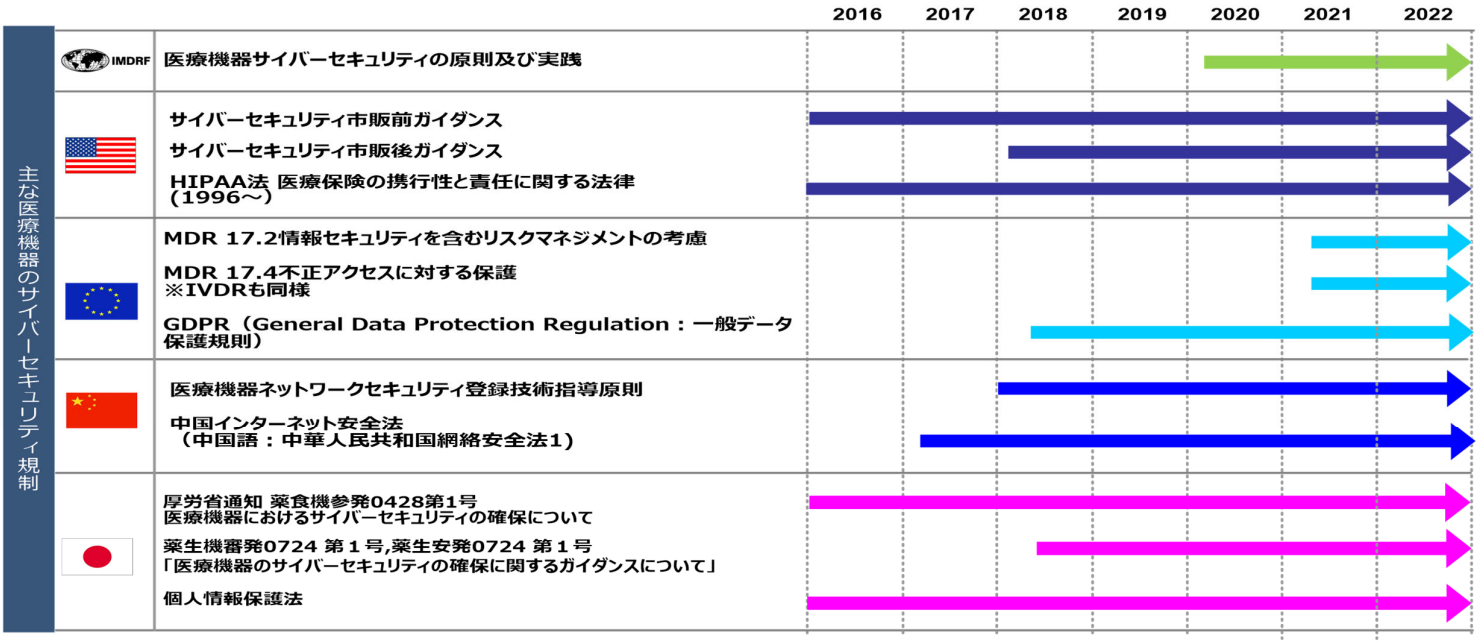
さらに，

- 端末を遠隔コントロールする別のウイルスを送り込む
- 接続可能なマシンにウイルスをばらまく
- アクセス可能なファイルをコピーして外部に送信する

さらにひどいものだと，

- ルート権限を奪取する
- 管理者に成りすましてさまざまな重要機密にアクセスする
  （民間企業などで複数の被害が確認されている）

医療機器サイバーセキュリティ各国の規制の状況



各国とも医療機器に対してサイバーセキュリティの規制要件を要求し始めている.

目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

IoTセキュリティガイドライン

- IoTセキュリティガイドライン ver1.0（平成28年7月）
  IoT推進コンソーシアム，総務省，経済産業省
- 目的
  - IoT特有の性質とセキュリティ対策の必要性を踏まえて，IoT機器やシステム，サービスについて，その関係者がセキュリティ確保の観点から求められる基本的な取り組みを，セキュリティ・バイ・デザインを基本原則としつつ，明確化することによって，産業界による積極的な開発等の取り組みを促すとともに，利用者が安心してIoT機器やシステム，サービスを利用できる環境を生み出す．
  - サイバー攻撃等による被害発生時における関係者間の法的責任の所在を一律に明らかにすることではなく，関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに，その認識のもと，関係者間の相互の情報共有を促すための材料を提供すること．
  - 守るべきものやリスクの大きな等を踏まえ，役割・立場に応じて適切なセキュリティ対策の検討が行われることを期待．

IoTセキュリティガイドライン

■　本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
■　各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	・経営者がIoTセキュリティにコミットする ・内部不正やミスに備える
分析	IoTのリスクを認識する	・守るべきものを特定する ・つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	・つながる相手に迷惑をかけない設計をする ・不特定の相手とつなげられても安全安心を確保できる設計をする ・安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	・機能及び用途に応じて適切にネットワーク接続する ・初期設定に留意する ・認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	・出荷・リリース後も安全安心な状態を維持する ・出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える ・IoTシステム・サービスにおける関係者の役割を認識する ・脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		・問合せ窓口やサポートがない機器やサービスの購入・利用を控える ・初期設定に気をつける ・使用しなくなった機器については電源を切る ・機器を手放す時はデータを消す

IoT特有の性質とセキュリティ

特有の性質

- セキュリティ上の脅威の影響範囲・影響度合いが大きい.
  ネットワークを介して関連する機器・システム，サービス全体に影響が波及.
- 機器のライフサイクルが長い.
  10～20年程度の長期にわたって使用される機器が多く存在.
  セキュリティ対応が不十分になった機器がネットワークに接続されつづける.
- 機器に対する監視が行き届きにくい.
  パソコンやスマートフォン等のような画面がないことから人目による監視が困難.
- 機器側とネットワーク側の環境や特性の相互理解が不十分である.
  相互の使用環境（意図した条件）が未解決のまま相互運用され，想定外のアクセスが発生.
- 機器の機能・性能が限られている（本来機能と見なされていない）.
  小型のウェラブル（センサー）機器等のリソースが限られている場合，暗号化等のセキュリティ対応を適用できない.
- 開発者が想定していなかった接続（使用環境）が行われる可能性がある.
  無線の影響，新たな機器やシステム，サービスの通信が相互に影響する.

IoTセキュリティガイドラインを医療機器に適用する場合

- 5つの指針は，医療機器・システムの製造販売業者とその経営者を対象
  - IoT機器・システム → 医療機器　または　医療機器・システム
    （一部，一般IoT機器を示す場合はIoTのまま）
  - IoTシステム → 医療情報システム
    （一部，一般IoTシステムを示す場合はIoTのまま）
  - IoT機器・システム提供者 → 医療機器・システムの製造販売業者
    （製造業者，販売業者，貸与業者，修理業者）
  - システム・サービス提供者 → 医療機関または医療サービスの事業者
    医療情報システムの事業者
    ネットワーク事業者
- 4つのルールは，医療機器・システムの使用者を対象
  - 利用者（一般利用者） → 患者及びその家族，医師，技師，看護師等

目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

安全管理ガイドラインとサイバーセキュリティガイダンス

安全管理ガイドラインとサイバーセキュリティガイダンスでは目的や位置づけが異なる事から，主体となる組織や適用範囲が異なるので注意．

【医療情報システムの安全管理に関するガイドライン】
医療機関が主体となって医療情報システムの機密性・完全性・可用性を確保するために医療情報システムの安全管理を行う．

※根拠法：個人情報保護法，e文書法

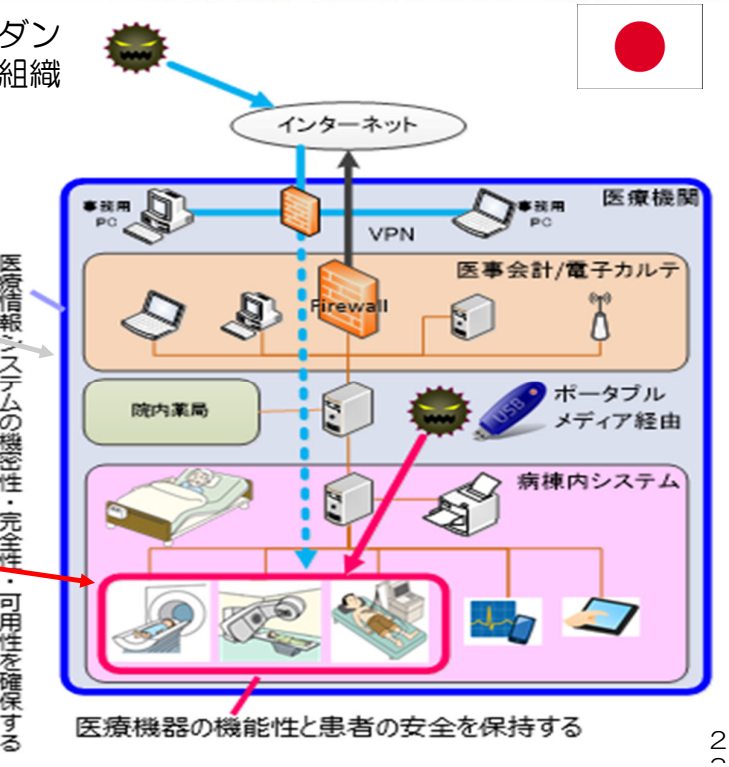
※1 医療情報システムの安全管理に関するガイドライン　第5版（平成29年5月），第5.2版（令和4年3月）公開

【医療機器のサイバーセキュリティの確保に関するガイダンス】
医療機器製造業者が主体となって，サイバーリスクに対する医療機器の機能性と患者の安全を保持する．※医療機関に対して必要な情報提供及び連携を図る．

※根拠法：医薬品医療機器等法

※2 医療機器のサイバーセキュリティの確保に関するガイダンスについて（平成30年7月24日）

JEITA医療機器ソフトウェアの最新技術動向セミナー（2020年2月19日）より引用，一部改変



医療機器におけるサイバーセキュリティの確保について

「医療機器におけるサイバーセキュリティの確保について」　（2015年）
（平成27年4月28日付け薬食機参発0428第１号・薬食安発0428第１号）

①基本的考え方

- 製造販売業者は，サイバーリスクが懸念される医療機器について，サイバーセキュリティを確保する必要がある．
- 医薬品医療機器等法第41条第３項に基づく基本要件基準（平成17年厚生労働省告示第122号）に基づき，サイバーリスクについても危険性を評価し，合理的に実行可能な限り除去することが求められる．
- サイバーリスクが懸念される医療機器の開発に当たっては，リスクマネジメントとして必要な対策を実施し，サイバーセキュリティを確保すること．
- 既に製造販売を行っている医療機器に関しても，同様にサイバーセキュリティを確保することが必要である．

上記が求められている．その上で

②サイバーセキュリティ対応

他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については，サイバーリスクを含む危険性を評価・除去し，リスクマネジメントを行い，使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこととしている．

厚生労働省 医療機器審査管理課
「医療機器のサイバーセキュリティの確保に関する最近の動向」
2020/6/30資料より引用

平成27年4月28日の厚労省通知に書かれた内容

(薬食機参発0428第1号/薬食安発0428第1号)

通知に書かれた具体的な対策①②③	要約
① 他の機器・ネットワーク等と接続して使用する又は他からの不正なアクセス等が想定される医療機器については，当該医療機器で想定されるネットワーク使用環境等を踏まえてサイバーリスクを含む危険性を評価・除去し，防護するリスクマネジメントを行い，使用者に対する必要な情報提供や注意喚起を含めて適切な対策を行うこと． 具体的には，当該医療機器と接続できる範囲を限定する，使用するソフトウェア等は製造販売業者が信頼性を認めたものに限定するなどのような対策が考えられる．	サイバーリスクを評価し，情報提供や注意喚起を含めた対策を行う．
② ①の必要なサイバーセキュリティの確保がなされていない医療機器については，使用者に対してその旨を明示し，他との接続を行わない又は接続できない設定とするよう必要な注意喚起を行うこと．	サイバーセキュリティの確保がなされていない医療機器は，使用者に明示し，他と接続しないように注意喚起する．
③ 「医療情報システムの安全管理に関するガイドライン」を踏まえ，医療機関における不正ソフトウェア対策やネットワーク上からの不正アクセス対策等のサイバーセキュリティの確保が適切に実施されるよう，医療機関に対し，必要な情報提供を行うとともに，必要な連携を図ること．	安全管理ガイドラインを踏まえ，必要な情報を提供し，必要な連携を図る．

医療機器におけるサイバーセキュリティの確保について

「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（2018年）
（平成30年7月24日付け薬生機審発0724第１号・薬生安発0724第１号）

①医療機器に関する検討

- 医療機器を使用する環境（医療機関・医療機関の管理が及ばない環境・特定が困難な環境）を特定．
- 医療機器のネットワーク等への接続方法（無線通信，USB 等の外部入出力ポート）の特定．

その上で

②具体的なサイバーセキュリティに関する対応

- 製造販売業者は，意図される使用環境におけるサイバーリスクに対するリスクマネジメントを実施（リスクが受容可能となるよう，必要な対策を実施）．
- 製造販売業者は，必要に応じて医療機関と連携を取り，保守契約等に基づきサイバーセキュリティの確保を支援することが重要．
- 医療機関と連携を取り，サイバーリスクに伴う医療機器の不具合等の情報の収集を実施（サイバーリスクに伴う医療機器の不具合等の情報も，GVP省令における安全管理情報の一つ）．

厚生労働省 医療機器審査管理課
「医療機器のサイバーセキュリティの確保に関する最近の動向」
2020/6/30資料より引用

ガイダンスの構成

1. 目的
2. 検討が必要となる医療機器及び使用環境の特定
   - 2.1. 対象となる医療機器
   - 2.2. 医療機器の使用環境の特定
     - 2.2.1. 医療機関での使用環境
     - 2.2.2. 医療機関の管理が及ばない使用環境
   - 2.3. 医療機器のネットワーク等への接続
     - 2.3.1. ネットワーク等への接続機器
     - 2.3.2. 無線通信等利用の医療機器
     - 2.3.3. USB等の外部入出力ポート
3. サイバーセキュリティ対応
   - 3.1. 製造販売業者によるサイバーセキュリティ対応
   - 3.2. 使用者によるサイバーセキュリティ対応
4. 市販後の安全性確保について
   - 4.1. 中古医療機器への対応について
5. 使用者等への情報提供
   - 1) 添付文書への記載事項

市販前・市販後にわたる
セキュリティ対応

使用環境を特定するなかで
安全管理ガイドラインに基づく
運用を想定

使用環境，接続機器，通信形態，採用技術，
インタフェースを考慮

・リスクマネジメントの実施
・既製品ソフトウェアも考慮
・セキュリティ対応に関する方針 体制
を確立，情報開示

GVP省令に基づく安全管理の実施(情報の集約
と分析，対策)

医療機器のサイバーセキュリティの確保に関するガイダンス

● 適用範囲

サイバーセキュリティに関するリスクが想定される医療機器が対象

- 機器の特性や使用環境からリスクを有するか判断する
- 医療機器クラス分類（Ⅰ～Ⅳ）は問わない
- 医療機器の構成品として提供される機器も適用対象

参照： 2. 検討が必要となる医療機器及び使用環境の特定
2.1. 対象となる医療機器

● 医療機器の使用環境の特定

サイバーリスクを想定するため医療機器の使用環境の特定が必要

- 使用環境，機器構成，機器間接続(機器間通信)
- 医療機関では安全管理ガイドラインに基づく管理を前提とする
  個人宅等医療機関管理外で利用するケースも考慮する
- 通信やネットワークへの接続，有線/無線，利用通信技術や機器，USB等外部デバイス等
  接続環境に応じたリスクを考慮する

参照： 2.2. 医療機器の使用環境の特定
2.3. 医療機器のネットワーク等への接続

医療機器のサイバーセキュリティの確保に関するガイダンス

- サイバーセキュリティ対応

製造業者によるサイバーセキュリティ対応：

ライフサイクルを通したリスクマネジメント実施と対応方針に基づくセキュリティの維持

- 意図する使用環境に基づくリスクマネジメントの実施と対策
  - 既製品ソフトウェアの考慮も必要
- セキュリティに対応する方針と体制の確立
- 問合せ窓口とサービスに係る取組について開示する事が望ましい

参照： 3. サイバーセキュリティ対応
3.1. 製造販売業者によるサイバーセキュリティ対応

使用者によるサイバーセキュリティ対応：

ライフサイクルを通したリスクマネジメントの実施と対応方針に基づくセキュリティの維持

- 医療機関と連携しサイバーセキュリティの確保を支援
- GVP省令に基づき安全管理を実施

参照： 3. サイバーセキュリティ対応
3.2. 使用者によるサイバーセキュリティ対応

医療機器のサイバーセキュリティの確保に関するガイダンス

- 市販後の安全性確保

GVP省令に基づく市販後の安全管理の実施

- サイバーリスクに伴う医療機器の不具合情報や文献等を収集・調査し，その情報を分析して必要に応じて対策を行う.

中古医療機器への対応

- 中古医療機器においても当該医療機器販売業者に対し適切な指示を行い，サイバーリスクへの対応を実施させる.

医薬品，医療機器等 の品質，有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第１号） 第 170 条

参照： 4. 市販後の安全性確保について
4.1. 中古医療機器への対応について

- 使用者への情報提供

サイバーセキュリティに関する情報を製造業者から使用者へ提供

※機器のセキュリティ上の弱点を取説に書くのは注意！

- リスクに応じて適切な情報提供を行う.
- 使用環境や運用に関する要件，注意喚起，技術的補足事項.
- 問い合わせ窓口やサイバーセキュリティに対する取り組み情報.

参照： 5. 使用者への情報提供

目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

国際整合に向けた組織　GHTF / IMDRF

1992～2012　GHTF（Global Harmonization Task Force）

・参加者：規制当局及び産業界代表者

日本　オーストラリア　カナダ　ヨーロッパ　アメリカ

医療機器規制の基本的なフレームワークに対する多くのガイダンス文書を開発。（基本要件基準，クラス分類ルール等々）

一部は，IMDRFが改定

2011～現在　IMDRF（International Medical Device Regulators Forum）

・参加者：管理委員会は，規制当局
　　作業グループは，産業界も参加

（2020/2/19現在）

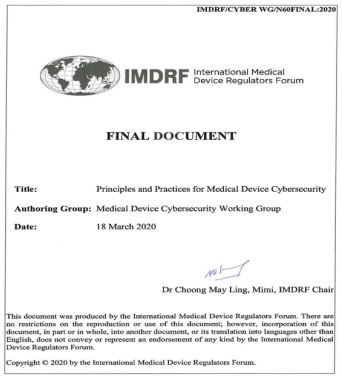
日本　オーストラリア　カナダ　ヨーロッパ　アメリカ

ブラジル　中国　ロシア　シンガポール　韓国

IMDRF サイバーセキュリティガイダンス

Principles and Practices for Medical Device Cybersecurity
（医療機器サイバーセキュリティの原則と実践）

IMDRF/CYBER WG/N60FINAL:2020
2020/03/18付，2020/04/20公開


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity
Authoring Group: Medical Device Cybersecurity Working Group
Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

一般原則

①共同責任
②国際調和
③製品ライフサイクル
④情報共有

1．はじめに
2．適用範囲
3．定義
4．一般原則
5．医療機器サイバーセキュリティの市販前考慮事項
6．医療機器サイバーセキュリティの市販後考慮事項
7．参考文献
8．附属書

- 医療機器（IVD医療機器を含む）のサイバーセキュリティに対する**一般原則及びベストプラクティスについて，全ての責任関係者に対して推奨事項を提供**する．
- **患者危害の可能性を検討することに限定**し，データプライバシーの侵害に関係するようなその他の危害も重要ではあるがこの文書の適用範囲ではない．（規制当局の立場から，**患者への危害と患者の安全性を重視**する．**情報セキュリティを除外**し，直接的に医療機器の安全と性能を含むことを明記する．）
- サイバーセキュリティは，**製造業者，医療提供者，ユーザー，規制当局及び脆弱性報告者を含むすべての利害関係者**の**共同責任**であり，**製品ライフサイクルの全体**を対象とする．
- **市販前の考慮事項**として，**設計インプット，リスクマネジメント，セキュリティテスト，市販後管理の戦略，ラベリング規制当局への対応についての推奨事項を提供**する．
- **市販後の考慮事項**として，**意図する環境における機器の運用，情報共有，協調的な脆弱性の公開，脆弱性の修正，インシデントへの対応及びレガシー医療機器についての推奨事項を提供**する．

- 医療機器サイバーセキュリティの原則及び実践
  Principles and Practices for Medical Device Cybersecurity（N60）
- ガイダンス文書の構成

一般原則
- 国際整合
- トータルライフサイクル（TPLC）
- 情報共有
- 共同責任

↓

市販前考慮事項
- 主に製造業者
- SBOM

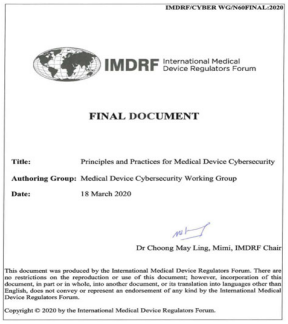
ベストプラクティス

↓

市販後考慮事項
- 様々な利害関係者
  （製造業者、ヘルスケアプロバイダー、患者、規制当局、その他）
- CVD（協調的脆弱性情報開示）
- レガシー医療機器に対する対応

2005年FDA医療機関向けキャンペーン資料より

- 追加の検討（NWIE： 2020年9月開始 24～30か月
  -> パブコメ終了、ほぼ最終）
  - SBOMの導入 / レガシー医療機器に関するフレームワーク


IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity
Authoring Group: Medical Device Cybersecurity Working Group
Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

情報共有の重要性　FDAが示した考慮すべき事項（一部抜粋）

- ユーザー（ヘルスケアプロバイダー，医療提供者（HDO），医療機関）
  - ネットワーク接続する機器の場合，購入前に機器の製造業者から保守計画を確実に入手する.
  - COTSベンダーではなく，サポートのために機器の製造業者に依頼する.
  - MedWatchを使用して，FDAに情報を提供する.
  - 誤動作が発生し，迅速なサポートが行われない場合は，機器の製造業者に書面で（又は口頭で）苦情を申し立てる.

- 製造業者（製販業者）
  - 市販前申請の提出時にCOTS保守計画の詳細を提供する.

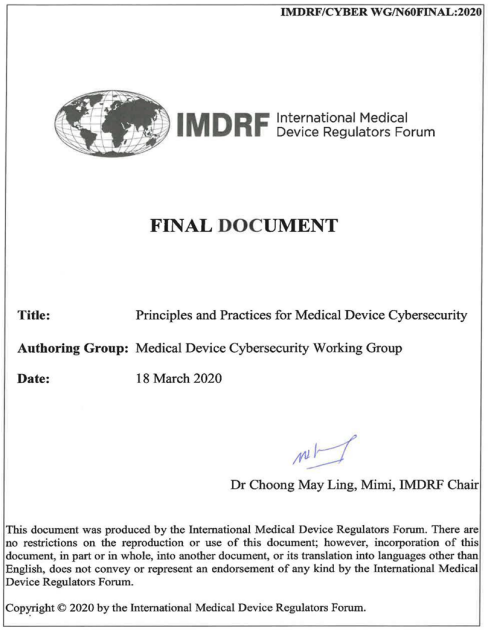
- COTSベンダー
  - 透明性（Transparency）のあるアップデートを提供する.
    医療機器の製造業者（製販業者）が，ユーザー（医療機関）に合わせてアップデートを可能にする.

※　COTS：Commercial-off-the-shelf （既製品で，一般的に購入などにより入手可能な商用製品）

2005年FDA医療機関向けキャンペーン資料より

ガイダンス文書の全体構成

Principles and Practices for Medical Device Cybersecurity
（医療機器サイバーセキュリティの原則と実践）



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

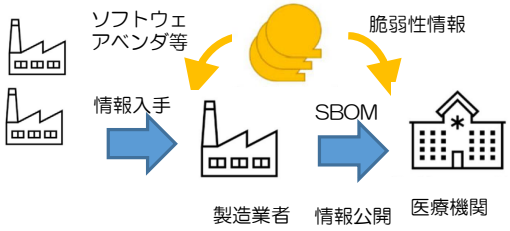
Copyright © 2020 by the International Medical Device Regulators Forum.

1.0	Introduction　（はじめに）	
2.0	Scope　（適用範囲）	
3.0	Definition　（定義）	
4.0	**General Principles　（一般原則）** 4.1 Global Harmonization（国際整合） 4.2 Total Product Life Cycle（製品ライフサイクルの全体） 4.3 Shared Responsibility（共同責任） 4.4 Information Sharing（情報共有）	
5.0	Pre-Market Considerations for Medical Device Cybersecurity （医療機器サイバーセキュリティの市販前考慮事項） 主に製造業者	ベストプラクティス
6.0	Post-Market Consideration for Medical Device Cybersecurity （医療機器サイバーセキュリティの市販後考慮事項） 様々な責任関係者（製造業者，ヘルスケアプロバイダー，患者，規制当局，その他）	
7.0	References　（参考文献）	
8.0	Appendices　（附属書）	

IMDRFガイダンスの3つのキーワード

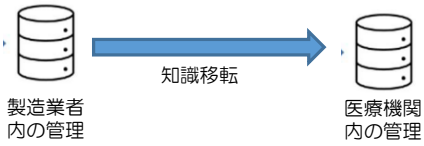
- **Software Bill of Materials（SBOM）**

  医療機器に実装される商用・オープンソース及び市販のソフトウェア部品のサイバーセキュリティに関する情報を提供するための部品表



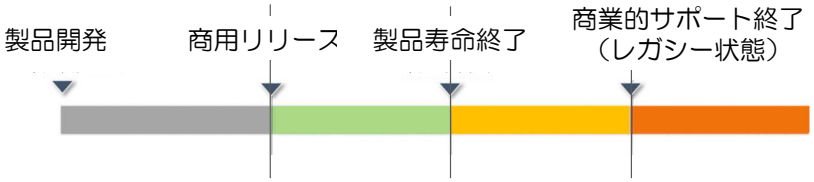
- **Coordinated Vulnerability Disclosure（CVD）「協調的な脆弱性の開示」**

  脆弱性の発見者から情報収集し、関係者間における情報共有などのサイバーセキュリティを確保する各種調整を実施した上で，脆弱性の情報を公開する活動



- **Legacy Medical Device**

  現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器



※サポートレベルは、顧客との契約に応じて異なる

JEITA医療機器ソフトウェアの最新技術動向セミナー（2022年5月）より引用

IMDRFガイダンスにおけるポイント（SBOM）

5.0 Pre-Market Considerations for Medical Device Cybersecurity

5.5.2 Customer Security Documentation

A Software Bill of Materials (SBOM) to inform and support operators regarding the cybersecurity of commercial, open source, or off-the-shelf software components which are included in the medical device. An SBOM creates the necessary transparency via a list identifying each software component by its name, origin, version and build. SBOMs enable device operators (including patients and healthcare providers) to effectively manage their [illegible] and related risks, to understand the potential impact of identified vulnerabilities to t[illegible] to maintain the device's safety a[illegible]ate work with the device manuf[illegible]uirements, and performing appro[illegible]g decisions by providing prospe[illegible] determining potential security [illegible] format, syntax and ma[illegible] me[illegible] th[illegible]

Software Bill of Materials（SBOM）：医療機器に実装される商用，オープンソース及び市販のソフトウェア部品のサイバーセキュリティに関する情報及びサポートを医療機関，顧客に提供するためのソフトウェア部品表

活用：

- 医療機関等が，医療機器及び接続されるシステムに対する脆弱性の潜在的な影響を理解し，医療機器の安全性及び基本性能を維持することが可能．
- 医療機関等が，脆弱性が潜んでいる可能性があるソフトウェアの特定，要件の更新及び適切なセキュリティリスクマネジメントの実施を，医療機器製造業者と協力して促進が可能．
- アプリケーションで使用されているコンポーネントを可視化して顧客に提示し，購入決定に必要な情報を提供することが可能．

SBOMの記載項目

NTIAにおけるSBOM：

1. 作成者情報
   - 業者名
   - 発行日
   - コメント
2. SBOMドキュメント名
3. SBOMコンポーネントのリスト
   - コンポーネント名
   - バージョン
   - コンポーネントサプライヤー
   - 識別子
   - ダウンロード場所
   - 分析されたファイル
   - ライセンス
   - 著作権テキスト

製造販売業者の開発・生産・保守体制等に応じて追加する必要があるかもしれない.

製造販売業者：

管理番号
1. 作成者情報
   - 業者名
   - 発行日
   - コメント
2. SBOMドキュメント名
   - 契約書管理番号
3. SBOMコンポーネントのリスト
   - コンポーネント名
   - バージョン／ビルド
   - コンポーネントサプライヤー
   - 識別子
   - ダウンロード場所／供給方法
   - 分析されたファイル
   - ライセンス
   - 著作権テキスト
   - チェックサム

引用：
NTIA Stakeholder Review Draft (September 4, 2019)
SOFTWARE COMPONENT TRANSPARENCY:HEALTHCARE
PROOF OF CONCEPT REPORT
レポートの「SBOM Generation」から引用

SBOMサンプル

id	*コンポーネントの名称 Component name	*コンポーネントの説明 Component description	*開発者・製造業者名 Developer/manufacturer name	*バージョン番号（該当する場合、メジャーおよびマイナーバージョン番号） Version number (Major and Minor where applicable)	*コンポーネントの種類（OS／ハードウェア／アプリケーション） Component type (operating system, hardware, application)	*共通プラットフォーム一覧(CPE)識別子 Common Platform Enumeration (CPE) identifier	パッチレベル Patch level (Version or date identifying the patch released by the component developer / manufacturer)
1	*Windows 10*	*Operating system*	*Microsoft*	*1903*	*operating system*	*cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*:*:x64:**	*KB4503293*
2	*Adobe Reader DC*	*Software for viewing, searching and printing PDF files*	*Adoble*	*19.008*	*application*	*cpe:2.3:a:adobe:acrobat_dc:19.008.20081:*:*:*:classic:*:**	*N/A*
3	*.NET Framework*	*A runtime execution environment that manages apps that target the .NET Framework*	*Microsoft*	*4.5.2*	*application*	*cpe:2.3:a:microsoft:.net_framework:4.5.2:*:*:*:*:*:*:**	*N/A*
4	*Microsoft Visual C++ Redistributable Packages for Visual Studio*	*Runtime components of Visual C++ Libraries*	*Microsoft*	*2013 update_5*	*application*	*cpe:2.3:osoft:vi udio:20 ate_5:* *:**	

以下の項目は記入を必須とする（先頭が* のもの）
- コンポーネントの名称
- コンポーネントの説明
- 開発者・製造業者名
- バージョン番号
- コンポーネントの種類
- 共通プラットフォーム一覧(CPE)識別子

また項目で記入できないものはN/Aとする.

IMDRFガイダンスにおけるポイント（CVD）

6.0 Post-Market Considerations for Medical Device Cybersecurity

6.3 Coordinated Vulnerability Disclosure

Transparency is an essential building block in cybersecurity because it is difficult to secure what is not known. One mechanism that enhances transparency is coordinated vulnerability disclosure (CVD). CVD establishes formalized processes for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mi... compensating controls and disclosing this information to various stakehold... security information sharin...

- サイバーセキュリティを確保するための手段としての情報開示を示し，医療機関等の関係者においても重要な意味を持つ．
- サイバーセキュリティのインシデントへの準備及び対応に関する透明性を強化する１つの手法として位置付けられている．

Adopting CVD po... impacted technologies to ma... tter protect their medical devices, Health IT infrastructure, and patients.

Engaging in CVD is a responsible course of action for raising awareness to security issues and should be vie... ma...

- 未知の脆弱性を考慮し，セキュアな状態にすることは難易度が高いことから，医療機器の製造販売業者がサイバーセキュリティの脆弱性情報を入手し，それを評価，緩和策及び補完的対策を開発・準備した上で，医療従事者を含む関係者に対して透明性を持って情報開示することが重要である旨が言及されている．

Th... co... fac... should be undertaken as a norm rather than as an exception and medical device stakeholders are encouraged to ask manufacturers about their CVD policies to further catalyze adoption.

IMDRFガイダンスにおけるポイント（レガシーデバイス）

6.0 Post-Market Considerations for Medical Device Cybersecurity

6.6 Legacy Medical Devices

For purposes of this IMDRF guidance, medical devices that cannot be reasonably protected (via updates, and/or compensating controls) against current cybersecurity threats are considered legacy devices. The legacy condition represents an especially complex challenge for the present state of the healthcare ecosystem globally since device cybersecurity may not have been ... in the initial device design and maintenance... ated by the fact that the clinical u... digital technology within medical de... within older analog devices. While be... etwork connectivity in these technologies puts new demands on the device lifetime, which often consists of capital equipment (e.g. scanner hardware) as well as commodity components (e.g. servers, workstations, databases and operating systems).

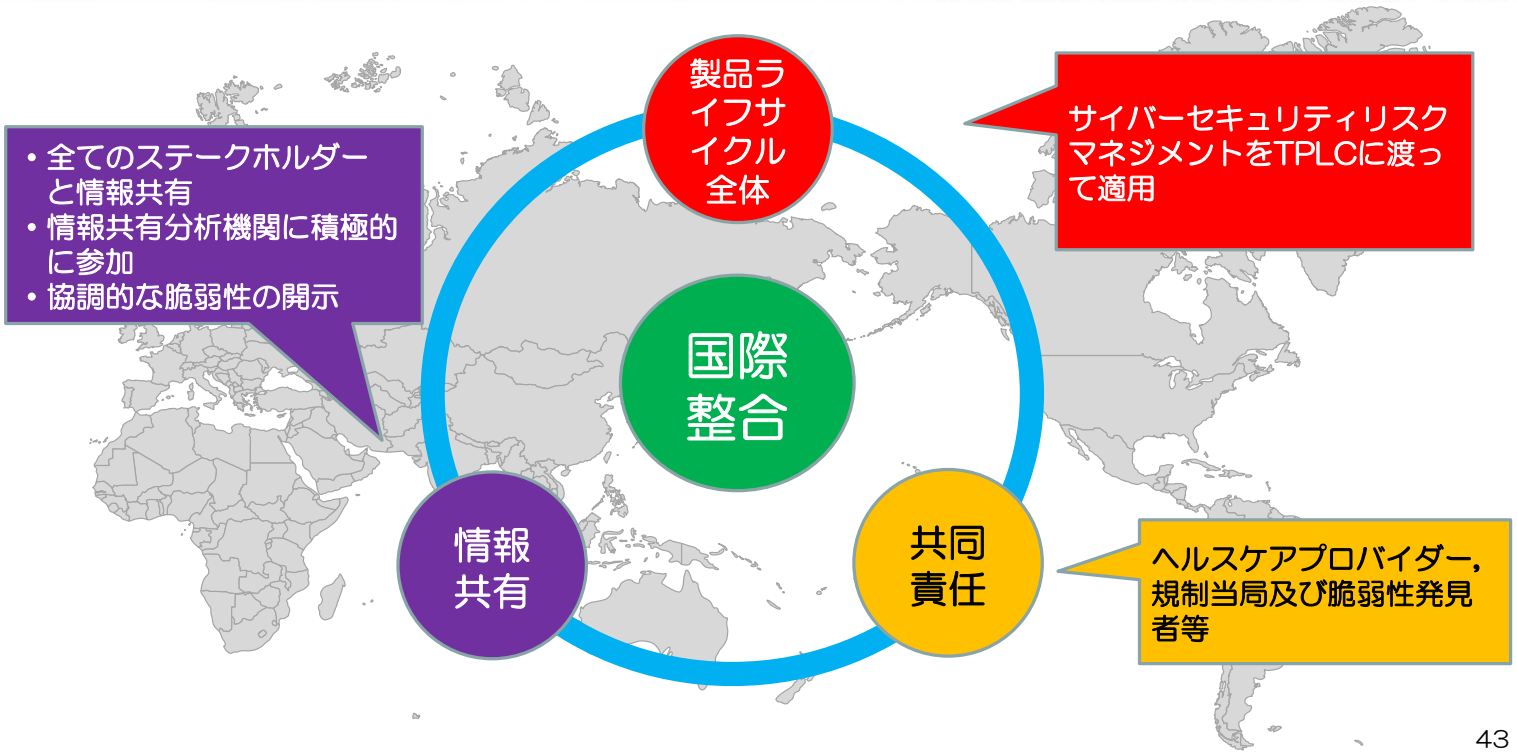
- レガシーデバイス：現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器．

It is important to note, however, that device age is not a sole determinant of legacy status. In other words, a device that cannot be reasonably protected against current cybersecurity threats may be less than five ye... ce m... cy...

- 老朽化の理由のみでその製品がレガシー医療機器であると判断してはならないことも重要（例えば，発売開始から5年以内の医療機器であっても，現在のサイバーセキュリティの脅威に対して合理的な手段で保護できない場合等）
- レガシー医療機器の使用を終了又は段階的に使用を終了するための概念フレームワークについても言及．

A... n ar... re... the norm, and the imbalance observed with respect to the multitude of legacy devices in current clinical use -

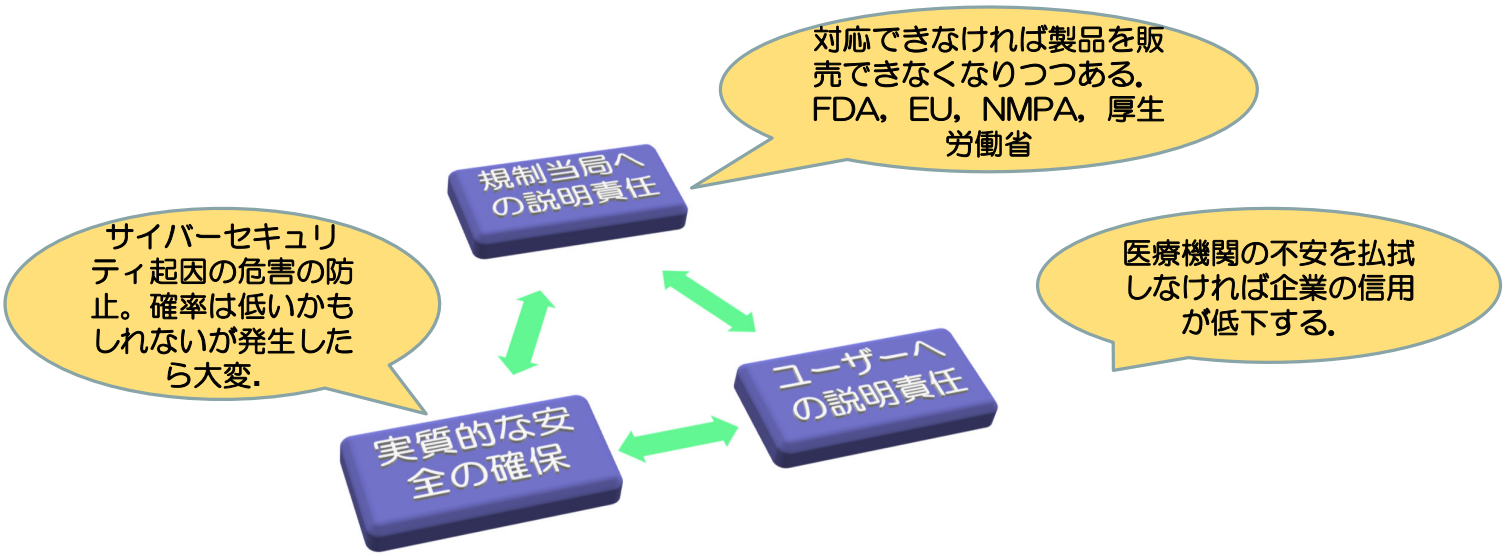
IMDRFガイダンスの一般原則



目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

何故，何のためにサイバーセキュリティに取り組むのか



サイバーセキュリティについて対応しないという選択肢はなくなりつつある．問題は多くの企業が組織的，技術的取り組みについて何をどこまでやればいいのか悩んでいる．

危害にはサイバーセキュリティに起因するものも含まれている

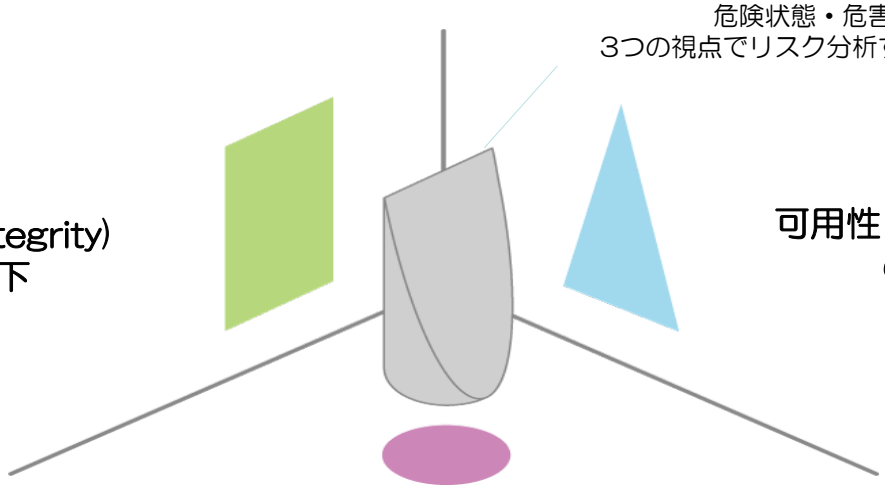
ISO/IEC Guide 51:2014の改定で危害(harm)の定義から physical （身体的）が消えた．

- 危害(harm)の定義
  - 人の受ける（~~身体的~~）傷害若しくは健康障害又は財産若しくは環境の受ける害

サイバー攻撃が原因となりうる傷害や健康被害はもちろんのこと，財産若しくは環境の受ける害に，情報セキュリティのAIC（可用性，完全性，機密性）の侵害により発生する害も含まれると考えれば，患者情報漏洩など機密性の低下も危害に含まれるかもしれない．

可用性，完全性，機密性の低下の視点でサイバーセキュリティのリスクを分析する

危険状態・危害の可能性を
3つの視点でリスク分析すると漏れがなくなる

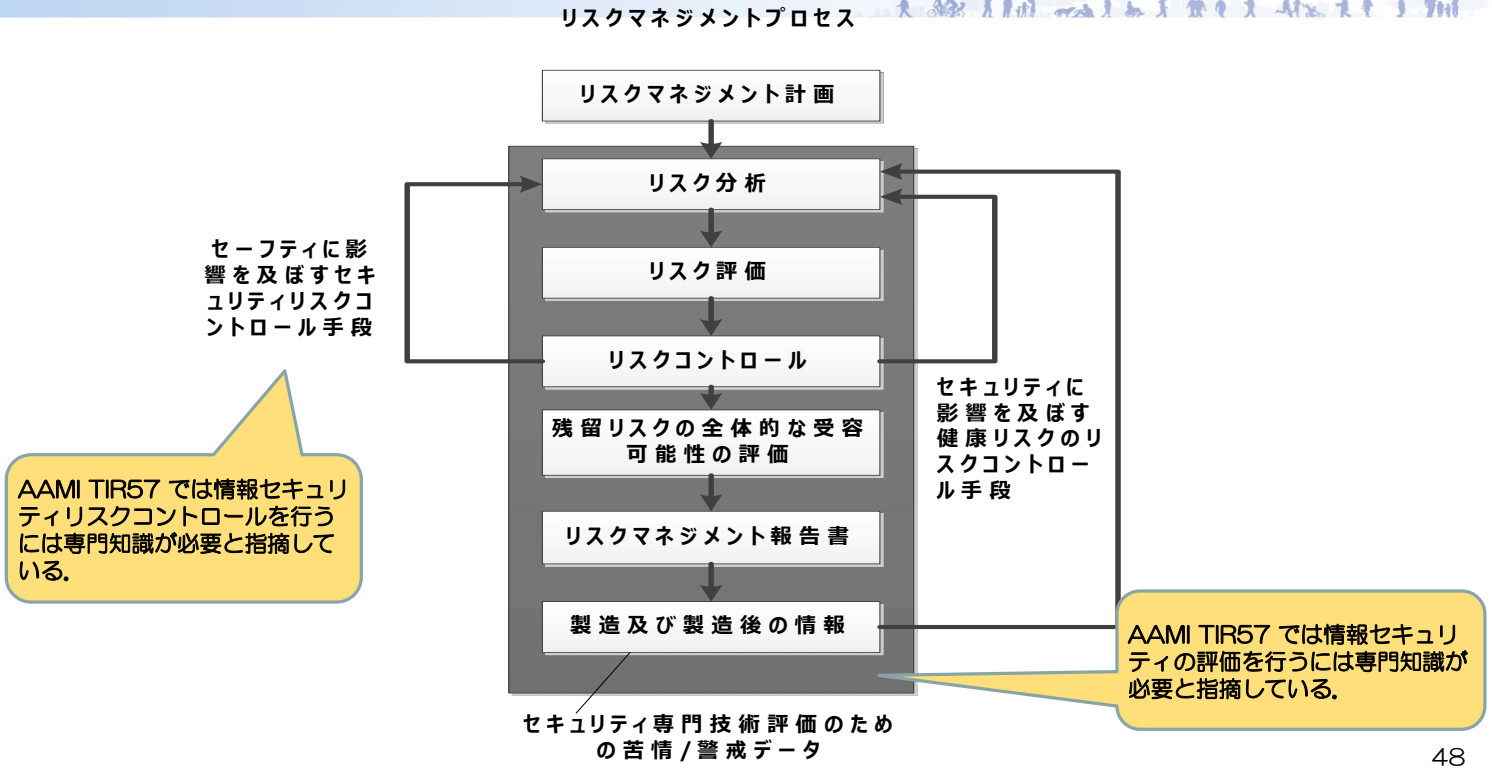


完全性(Integrity)
の低下

可用性(Availability)
の低下

機密性(Confidentiality)
の低下

リスクマネジメントプロセスに組み込む



サイバーセキュリティリスク分析/報告の項目例

- 医療機器の意図する使用（Intended Use）
- 医療機器や構成品，ポータブルメディア，ネットワーク接続環境の説明
- 保護すべき情報資産の内容
- 侵入経路の分析及び脅威のモデリング
- サイバーセキュリティのリスク分析結果
- サイバーセキュリティリスクコントロール手段検証
- トレーサビリティマトリックス
- サイバーセキュリティ残留リスク判定
- 脆弱性の監視計画
- ペネトレーションテスト（侵入テスト）レポート
- サイバーセキュリティバリデーションのレビューワ資格情報
- サイバーセキュリティバリデーションの結果

リスクコントロールのために必要な外部接続機器等がある場合はそれらも接続環境に含める．

サイバーセキュリティリスクマネジメントのまとめ

- 当該医療機器の意図する使用（Intended Use）を確認する．
- 当該医療機器のネットワークシステム構成図（意図する使用環境）を描く．
- I/Fの一覧（I/F仕様，プトロコル，使用者等）とユースケース（そのI/Fを通して何ができるのか）を分析する．
- サイバーセキュリティのリスク分析及びリスク評価（対策前，対策後）を行う．
- リスク分析は情報セキュリティの可用性，完全性，機密性が低下したときの悪用可能性と危険状態と（患者）危害を分析するとよい．
- 危害の重大さの評価レベルは，従来の評価基準（ISO 14971:2007 表D.3-5）と同じにするか，サイバーセキュリティ用に独自の基準を定義するかを考える．
- 脅威の起こりやすさの評価は「確率」ではなく「悪用可能性」を分析することが望ましい．
- 分析したすべてのリスクが受容可となっていることを確認する．

医療機器の製造業者が行うべき事項（研究・開発，市販前）

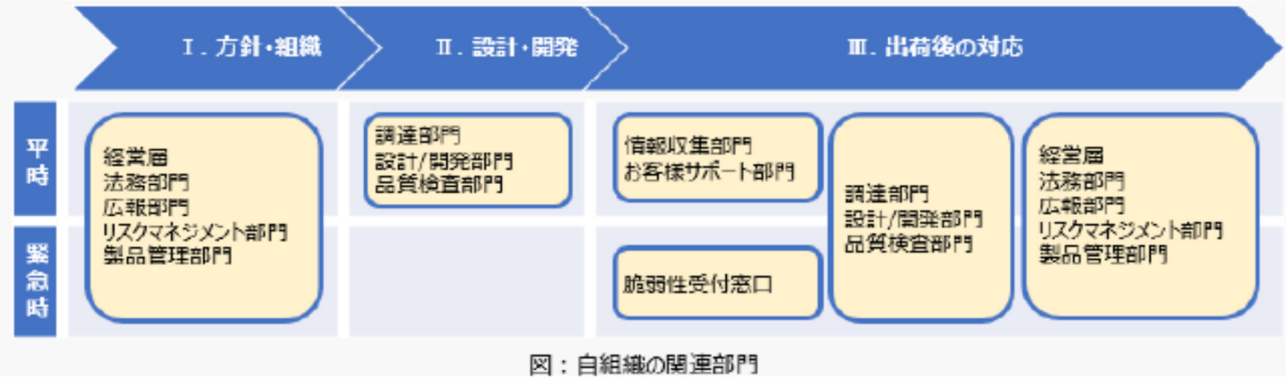
- 技術（設計）的始動と製品セキュリティ
  - 米国FISMA，NIST，DHS及びDoDの動向の習得　（RMF: Risk Management Framework）
  - IMDRF，各国規制要求事項，ガイドラインの習得とリスクアセスメント
  - 製品セキュリティポリシー（ベースライン）及び製品セキュリティ要求事項の決定
  - 基本設計（リスクマネジメントと防御対策の確立）の計画と導入
    - ホワイトリスト型プロテクトツールの導入及びブラックリスト型プロテクトツールによる保守方法確立
    - オープンソースを含むOTSソフトウェアの特定（戦略的選択）及び管理とセキュリティ確保
      （SBOM: Software Bill of Materials, software version: UDI）
    - セキュリティの評価手法・手段の確立と継続的運用（開始）
      （悪用可能性：CVSS，脆弱性検出ツール:例Nessus，侵入試験等）
    - 添付資料（MDS2含む），設計文書
- 仕組み（システム）の構築
  - 企業の情報システムセキュリティマネジメントシステムの適用
    製造所，事業所（ISO 27001： ISMS）
  - 製品セキュリティのための対応組織の設置と継続的運営
    （PSIRT：Product Security Incident Response Team の役割例）
    - セキュリティ情報の収集先の決定（ICS/JPCERT，IPA，サプライヤ等）
    - セキュリティ情報の収集・検知、発見された問題の分類・分析
    - 製品のセキュリティに関連する情報の提供
    - 医療機関を含む社内外の多様なステークホルダとの連携
    - 製品特性に合わせたインシデント対応方針の立案
    - 製品インシデントを発見するための手段・プロセス開発

医療機器の製造業者が行うべき事項（市販後）

- 販売・保守のための技術活動
  - 市販後監視
    - オープンソースを含むOTSソフトウェアの脆弱性管理（PSIRTからの入力）
    - サイバーセキュリティに関連するインシデント等のモニタリング
  - サイバーセキュリティに関する対応
    - セキュリティの評価手法・手段の確立と継続的運用
      （悪用可能性：CVSS，脆弱性検出ツール:例Nessus，侵入試験等）
    - MDS2（Manufacturer Disclosure Statement for Medical Device Security） の提供
    - 米国の主に国防総省（DoD）に関連する施設への納入条件となるATO
      （Authority to Operate：ネットワークにおける運用認定）取得及び取得後の月次報告
      （Nessusによるスキャンを含むSTIG（Security Technical Implementation Guides） の実査による認定で，
      DHA（Defense Health Agency）が実施 https://health.mil/dha）
    - OS等のプラットフォームの更新技術の開発・評価
- 仕組み（システム）の構築
  - 製品セキュリティのための対応組織の継続的運営（PSIRT：Product Security Incident Response Team）
    - オープンソースを含むOTSソフトウェアの脆弱性管理のための契約管理
    - GDPRに基づくSCC（標準契約条項）の締結（欧州）
    - セキュリティ情報の収集・検知、発見された問題の分類・分析
    - 製品のセキュリティに関連する情報の提供
    - 医療機関を含む社内外の多様なステークホルダとの連携
    - 製品特性に合わせたインシデント対応方針の立案
    - 製品インシデントを発見するための手段・プロセスの保守
  - 情報共有の仕組み　ISAO参加と活動（米国）

PSIRT（Product Security Incident Response Team）

体制：多くの部門に関係する



図：自組織の関連部門

◆ インシデント対応準備

インシデント対応管理ポリシーの確立，詳細な対応計画の策定，インシデント対応チームの設立，対応の定期的試験及び練習，対応能力の継続的向上．

◆ コミュニケーション

連絡先窓口情報を顧客に提供．状況共有のための日常的な活動体制を確立し，可能な限り早急に適切な情報を顧客に提供．規制当局その他所轄官庁への報告．

脆弱性対処に向けた製品開発者向けガイド（IPA）
https://www.ipa.go.jp/files/000085024.pdf

目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼） 令和２年５月13日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
厚生労働省医薬・生活衛生局医薬安全対策課長

国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの
原則及び実践に関するガイダンスの公表について（周知依頼）

医療機器のサイバーセキュリティについては、「医療機器におけるサイバーセキュリティの確保について」（平成27年４月28日付け薬食機参発0428第１号、薬食安発0428第１号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）、厚生労働省医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求め、「医療機器のサイバーセキュリティの確保に関するガイダンスについて」（平成30年７月24日付け薬生機審発0724第１号、薬生安発0724第１号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知）により、具体的なリスクマネジメント及びサイバーセキュリティ対策を取りまとめたガイダンスを示し、当該ガイダンスを参考に必要な対応を行うよう、関係事業者等に対する周知を依頼してきたところです。

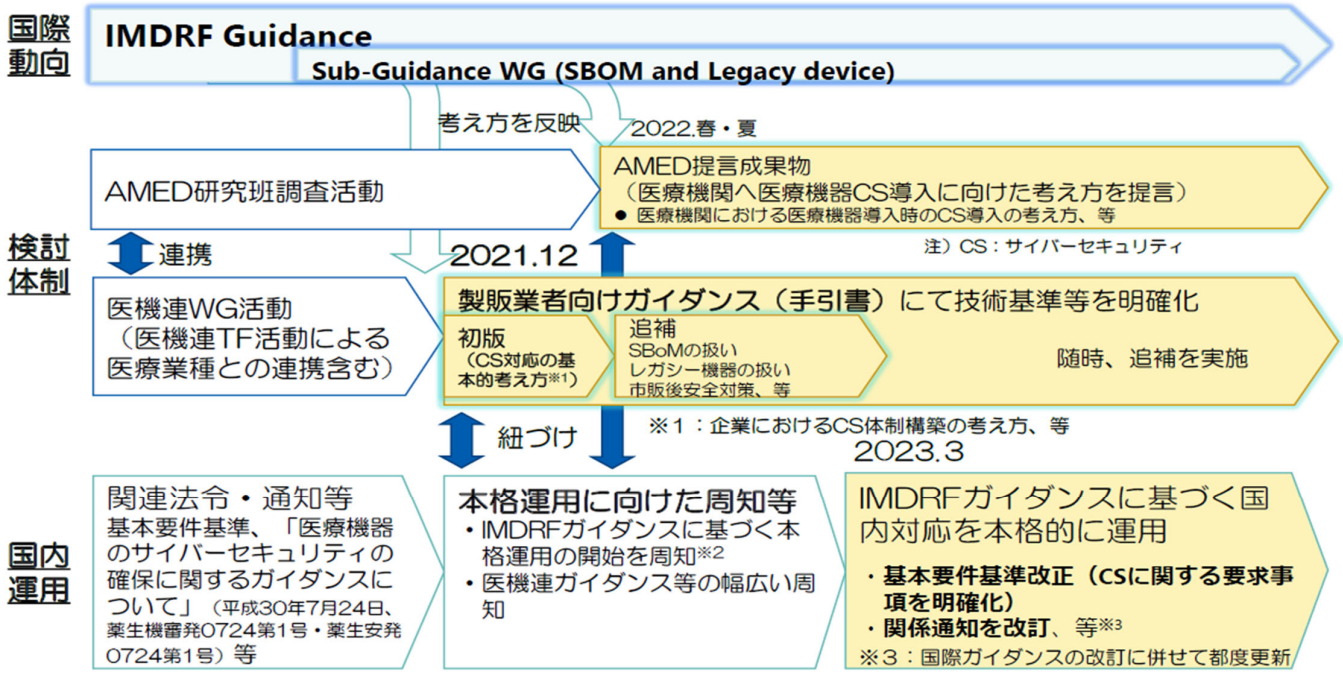
今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、国際医療機器規制当局フォーラム(IMDRF)において、サイバーセキュリティ対策の国際的な調和を図ることを目的として、「Principles and Practices for Medical Device Cybersecurity」（医療機器サイバーセキュリティの原則及び実践）（以下「IMDRFガイダンス」という。）が取りまとめられました。

国際的な規制調和の推進の観点や国境の枠組みを超えて医療機器のサイバーセキュリティに係る安全性を向上させる観点から、我が国においても、今後３年（2023年）程度を目途に、医療機器製造販売業者に対してIMDRFガイダンスの導入に向けて検討を行っているところです。

原文：http://imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
邦訳：http://dmd.nihs.go.jp/cybersecurity/IMDRF_Guidance_Japanese_version.pdf
（国立医薬品食品衛生研究所）

厚生労働省 通知　抜粋

IMDRFガイダンスの国内導入に向けた検討状況
ー今後の予定（2022/8月時点）



※2「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」
（令和３年12月24日薬生機審発1224第１号・薬生安発1224第１号）

医機連サイバーセキュリティ対応WG資料より引用

医療機器のサイバーセキュリティ導入に関する手引書
（2021年12月24日）

IMDRF ガイダンス

1. はじめに
2. 適用範囲
3. 定義
4. 一般原則
5. 医療機器サイバーセキュリティの市販前考慮事項
   - 5.1. セキュリティ要求事項及びアーキテクチャ設計
   - 5.2. TPLCに関するリスクマネジメント原則
   - 5.3. セキュリティ試験
   - 5.4. TPLCサイバーセキュリティマネジメント計画
   - 5.5. ラベリング及び顧客向けセキュリティ文書
   - 5.6. 規制当局への申請に関する文書
6. 医療機器サイバーセキュリティの市販後考慮事項
   - 6.1. 意図する使用環境における機器の運用
   - 6.2. 情報共有
   - 6.3. 協調的な脆弱性の開示
   - 6.4. 脆弱性の修正
   - 6.5. インシデントへの対応
   - 6.6. レガシー医療機器
7. 参考文献
8. 附属書

医療機器のサイバーセキュリティ導入に関する手引書

①共同責任
②国際調和
③製品ライフサイクル
④情報共有

背景
1. 目的
2. 適用範囲
3. 用語及び参考定義
4. 一般原則
5. 市販前考慮事項
   - 5.1. セキュリティ要求事項及びアーキテクチャ設計
   - 5.2. TPLCに関するリスクマネジメント原則
   - 5.3. セキュリティ試験
   - 5.4. TPLCサイバーセキュリティマネジメント計画
   - 5.5. 顧客向け文書
   - 5.6. 規制当局への申請に関する文書
6. 市販後考慮事項
   - 6.1. 意図する使用環境における機器の運用
   - 6.2. 情報共有
   - 6.3. 協調的な脆弱性の開示（CVD）
   - 6.4. 脆弱性の修正
   - 6.5. インシデントへの対応
   - 6.6. レガシー医療機器

文献

目的

- 国際的な規制調和の観点及び国境の枠組みを超えて医療機器のサイバーセキュリティに係る安全性を向上させる観点から策定されたIMDRFガイダンスの要求事項を踏襲.
- 医薬品医療機器等法を遵守し，医療機器の品質，有効性及び安全性を確保するために，製造販売業者が，本邦の医療機器に対して導入するための対応及び組織的な取組みを行うための情報を提供.
- 製造販売業者が適切な対応を実施し，製品ライフサイクル全体（Total Product Life Cycle）を通じサイバーセキュリティに関するリスクを低減し，医療機器製品の安全性と基本性能を確保することで，患者への危害の発生及び拡大の防止に繋げる.

製造販売業者の責任の明確化

適用範囲：サイバーセキュリティが求められている医療機器

- 無線又は有線により，他の機器・ネットワーク等との接続が可能なプログラムを用いた医療機器（ソフトウェア単独で医療機器となる医療機器プログラム（Software as a Medical Device：SaMD）を含む）及びプログラムを用いた附属品等に関するサイバーセキュリティを対象．
- 適用の要否は，医療機器のクラス分類（Ⅰ～Ⅳ）だけで判断すべきではなく，意図する使用環境，サイバーリスクに応じた危害等を考慮したリスクベースアプローチによって判断．
- 患者又はユーザーへの危害が発生する可能性のあるサイバーセキュリティリスクに限定．
  - ✓ 製品の性能に悪影響を与える．
  - ✓ 臨床活動に悪影響を与える．
  - ✓ 誤った診断，治療又は予防に繋がる

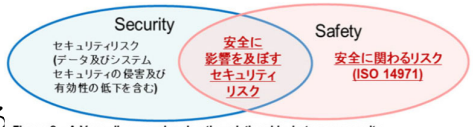
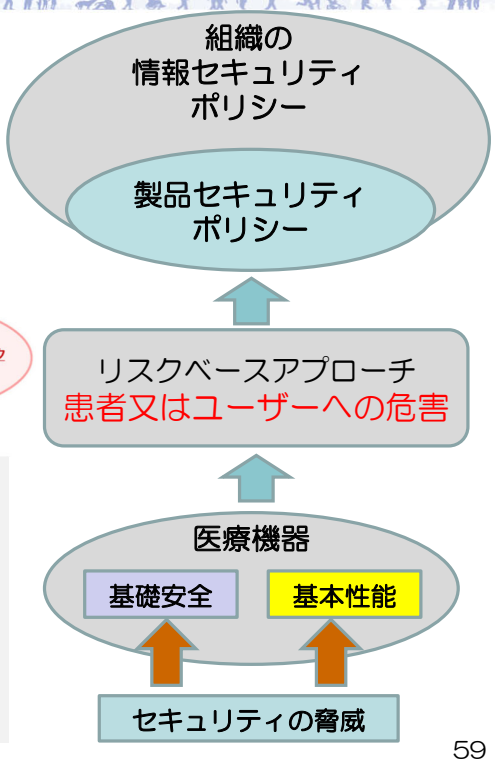


Figure 2 – A Venn diagram showing the relationship between security and safety risks AAMI TIR 57

医療機器は，患者等の個人情報等を扱う医療情報システムの一部としてもみなされるため，データプライバシー等の情報セキュリティに係るリスクへの対応も実施される必要があるが，この文書の適用範囲ではない．情報セキュリティに係る対策については，別途安全管理ガイドライン等を参照する．また，製造販売業者の一般的な企業活動に関するサイバーセキュリティ対応についてもこの文書の適用範囲から除外しているため，医療機器の製造販売業者は，一般的な個人情報の漏洩等の危害についても十分な対応をすることが社会的に求められていることに留意すべきである．



[厚労科研市販後安全対策]サイバーセキュリティに関する研究資料より引用，一部改変

医療機器のサイバーセキュリティ導入に関する手引書ー追補ー

基本　→　実践

背景
1. 目的
2. 適用範囲
3. 用語及び参考定義
4. 一般原則　（4原則）
5. 市販前考慮事項
   - 5.1. セキュリティ要求事項及びアーキテクチャ設計
   - 5.2. TPLCに関するリスクマネジメント原則
   - 5.3. セキュリティ試験
   - 5.4. TPLCサイバーセキュリティマネジメント計画
   - 5.5. 顧客向け文書
   - 5.6. 規制当局への申請に関する文書
6. 市販後考慮事項
   - 6.1. 意図する使用環境における機器の運用
   - 6.2. 情報共有
   - 6.3. 協調的な脆弱性の開示（CVD）
   - 6.4. 脆弱性の修正
   - 6.5. インシデントへの対応
   - 6.6. レガシー医療機器
7. 業許可に関する考慮事項
   - 7.1. 業許可をもつステークホルダーの役割
   - 7.2. リース医療機器の扱い
   - 7.3. 中古医療機器の扱い

附属書（規定）
A. ソフトウェア部品表（SBOM）の扱い

脆弱性マネジメントの視点から、全体を補充
6.4. 脆弱性の修正
- 脆弱性発見（インシデント未発生）でも不具合報告に至る可能性を示す。

6.5. インシデントへの対応
- 緊急対応、予防的活動、不具合報告、情報共有を具体化

6.6.1,6.6.2 をIMDRF追補ガイダンスから補充
6.6.3　補完的リスクコントロール追加

- 製販業者：　関連する製造業者、販売業者、貸与業者に対し必要な情報提供
- 販売業者：　販売時に、規則に従い製造販売業者へ確認
- 販売業者：　医療機関（使用者）に情報提供
- 製販業者が定めたEOLを超えた製品の扱い

IMDRFの追補ガイダンスを基本として追加

6.6.　レガシー医療機器
6.6.1.　TPLCとレガシー医療機器
6.6.2.　TPLCにおける責任・考慮事項
6.6.2.1.　設計・開発段階
6.6.2.2.　サポート段階
6.6.2.3.　限定的サポート段階
6.6.2.4.　サポート終了段階
6.6.3.　補完的リスクコントロールに関する考慮事項

A.　ソフトウェア部品表（SBOM）の扱い
A.1　SBOMの生成
A.2　SBOMの要素と推奨フォーマット
A.3　SBOMの提供
A.4　SBOMの事例

医療機関向け手引書 - 医療機関への周知のために

［背景］
医療機関における医療情報システム及びそのネットワークと医療機器との関係を下図のように提示し，安全管理ガイドラインと現在作成中の「医療機関向け手引書」「製販業者向け手引書」との相互関連性を説明可能な状態にする必要がある．

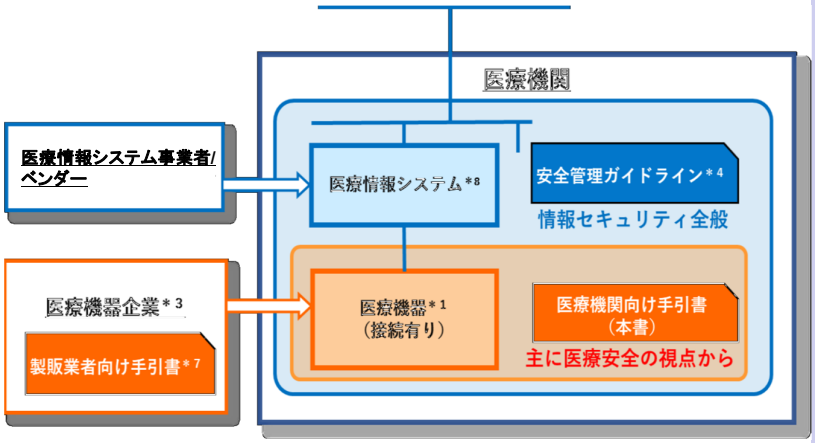


図１ 医療機関向け手引書と安全管理ガイドラインの位置付け（イメージ） 案

- 医療機器へのリモートメンテの方式（ネットワーク経路）
- システム構成図，システム機能構成図，ネットワーク図
- 医療機器の操作者の権限管理
  （医療機器事業者用権限と医療機関の管理者用や一般的な利用者用の分別と権限・制御の設定）
  ※例えば，病院情報システムや病院情報システム端末では，当然ながらシステム管理者（Administrator）とユーザー（Users）などで分け，制御しているのでそれらとの権限コントロールレベル感での整合性を医療機器でもとっていく必要性．（各医療機器でのパスワードなどのセキュリティの設定等）

3省2ガイドライン：医療情報を取り扱う事業者が準拠すべき医療情報の保護に関するガイドラインのこと．厚生労働省，経済産業省，総務省の3省が発行する2つのガイドラインを指すため，そう呼ばれている．具体的には，厚生労働省の「医療情報システムの安全管理に関するガイドライン」，経済産業省・総務省の「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を指す．

「医療機関向け手引書(仮)」の作成

目的，対象者（読者），位置づけ

- 医療機関等で使用される医療機器のサイバーセキュリティを確保することにより，医療安全が確保された円滑な運用に資することを目的とし，医療機関等で必要となる対応について説明する．
  - 医療機関，医療機器製販業者を中心に、すべてのステークホルダーの役割と連携を明確にする．
  - 患者安全(セーフティ)が中心．情報セキュリティ確保との関係にも触れる．
- 主な対象（読者）は，医療機関等（大規模から小規模）の管理者を想定．
  - 大規模施設：経営者，医療機器安全管理責任者，医療情報システム管理者，医療機器・医療情報システム運用担当者．
  - 小規模施設：経営者（業者等に適切な指示を出すために）．

医療機関と製造販売業者が，連携して対応する仕組みの構築が必要

医機連サイバーセキュリティTFで素案を作成中．2023年3月予定．

「医療機関向け手引書(仮)」ー案ー

目次

1. はじめに
2. 本書の目的と対象
    2.1. 目的
    2.2. 本書の対象について
3.サイバーセキュリティ対策について
    3.1. サイバーセキュリティ対策の基本
    3.2. ステークホルダーとの連携
    3.3 製品ライフサイクル全体とリスクマネジメント
    3.4 サイバーセキュリティ対策の国際整合
4. 医療機関の取り組みの実際
    4.1. 医療機器の導入前の準備
    4.2. 医療機器の導入時
    4.3. 医療機器の導入後_運用、管理
    4.4.インシデントへの対応
    4.5.レガシー医療機器への対応
5. おわりに

目次

1. 医療機関・医療機器を経由して侵入されるセキュリティリスク
2. IoTセキュリティガイドライン
3. 医療機器におけるサイバーセキュリティの確保
4. IMDRFサイバーセキュリティガイドライン
5. 医療機器製造販売業者のサイバーセキュリティ対応，リスクマネジメント
6. 医療機器のサイバーセキュリティ対応に関する課題の対応
7. まとめ

まとめ

- 厚生労働省は，平成27年(2015年） 医療機器のサイバーセキュリティに関する通知を発行し，平成30年（2018年）通知に対応するガイダンスを発行した．これが基本となっている．
- 令和2年（2020年）4月，IMDRF サイバーセキュリティガイダンスが公開され，日本では、2023年3月を目途に，医療機器製造販売業者に対して導入が進められる．（日程が早まった）
- 製造販売業者は，開発等市販前から保守・廃棄等市販後まで製品のライフサイクルを対応する必要がある．
- 医療機器のサイバーセキュリティは「規制当局への説明責任（規制要求）」「ユーザーへの説明責任」「医療機器の実質的な安全の確保」という側面から，対応する必要がある．
- 安全に影響を及ぼすセキュリティリスクのリスク低減は必須であり，その他のセキュリティリスクについてもユーザーである医療機関から対応が求められる．
- 製造販売業者は，必要に応じて医療機関と連携を取り，保守契約等に基づきサイバーセキュリティの確保を支援することが重要．

NIHON KOHDEN

ご清聴，有難うございました．

松元　恒一郎
Koichiro_Matsumoto@mb1.nkc.co.jp