JAHIS
健康で豊かな国民生活を保健医療福祉情報システムが支えます

2018年度 業務報告会

# セキュリティ委員会　活動報告

## 医療分野におけるサイバーセキュリティの最新動向

2019年2月4日

セキュリティ委員会

委員長　　茗原　秀幸

# JAHISセキュリティ委員会の対外活動

- セキュリティ委員会では様々な対外活動を実施している。
  - 医療等分野ネットワーク安全管理WG（厚生労働省）
  - 医療情報を受託する情報処理事業者の安全管理ガイドライン改定検討会（経済産業省）
  - 協働の会（JNSA,IPA,JPCERT-CC,JASA）
  - サイバーセキュリティ演習研究会（医業経営コンサルタント協会）
  - etc.
- 今回はその中で第四回協働の会にて発表した「医療分野におけるサイバーセキュリティの最新動向」についてご紹介したい。

# 本日の内容

1. 第三回協働の会でのご説明内容の振り返り

2. 全国保健医療情報ネットワークの必要性

3. 医療機器（IoT）問題とオープンネットワーク

4. 国際標準化の転換点

# 1. 第三回協働の会でのご説明内容の振り返り

# 医療安全と情報セキュリティ

- 従来、医療安全の考え方は国際標準のISO 14971（JIS T 14971）「医療機器-リスクマネジメントの適用」に基づいて行われることが一般的であった。
  - ISO 14971におけるハザード（危害の潜在的な源）の分析においては、「意図する使用および合理的に予見できる誤った使用」を想定し、「予見可能」なものを検討することとなっている。

既存のリスクアセスメントにおいて、「悪意をもった外部からの攻撃」をハザードとして規定することは殆ど行われてこなかった。

- 医薬品・医療機器等法においても、基本的には医療機器単体におけるリスクマネジメントを求めており、組織による多層防御によって実行されるサイバーセキュリティ対策の考え方を持ち込むことは簡単ではなかった。

# 情報セキュリティの観点から見ると…

- サイバーセキュリティを考えるのは医療機器を利用する医療機関
  - 厚生労働省から「医療情報システムの安全管理に関するガイドライン」が発行されている
  - 医療機関が適切なセキュリティ対策を実施すれば医療機関内部にセキュアゾーン（サイバー攻撃に対する一定のセキュリティが確保されたエリア）を構築し、医療機器をセキュアゾーン内で利用することが可能

たとえば基幹系と情報系を完全に分離した場合、
基幹系はオープンネットワークとは隔離され、
基幹系に接続される医療機器はサイバー攻撃の
ターゲットになる可能性を小さくすることが出来る。

# 医療分野においては可用性が重視されている

- 不正アクセス防止のための認証機能は可用性の観点で見ると、むしろ患者安全に影響を及ぼすセキュリティレベルを低下させる。
  - たとえば、不正利用を防止するために利用者認証機能を組み込んだ結果、認証手続きによって対処が数秒遅れたため、患者が死亡することを許容できるかという問題。
- 医療機器が取るべき情報セキュリティ対策として、常にオープンネットワークにさらされている前提の対策を実施することは現実的ではない

オープンネットワーク接続を前提としたセキュリティ対策の強化は、製品コストが上昇するのみならず、利用する側の環境によっては可用性が低下することになりかねない！！

# 医療機器の情報セキュリティ対策の問題点

- 医療機器は医薬品・医療機器等法によって基準適合認証を受けた機器であるため、ソフトウェアのアップデート等内容の変更が発生する場合は変更内容によっては届出あるいは再認証を受ける必要が生じる。
  - 情報セキュリティ対策を追加することで認証の取り直しが発生する可能性があり、簡単に機能の追加変更が出来ない。
  - OSのアップデートや不具合対策のモジュール適用も、当該モジュールに医療機器としての本来機能を損なう別の不具合を内包している可能性があり、十分な検証を行ってからでないと適用が難しい。
- 医療機器の場合10年以上使用されるケースも十分ある。
  - OSにいまだにWindowsXPが利用されている機器も数多く残存

# 日本における厚生労働省の対応

- 2015年4月28日に厚生労働省通知「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」を発出。
  - サイバーリスクについても既知または予期しうる危害として識別し、必要な措置を行うことを製造業者に求めた。

具体的には以下の3点である。（筆者要約：正式には原文を参照願う）

①サイバーリスクを含む危険性を評価・除去し、適切な対策を行うこと。

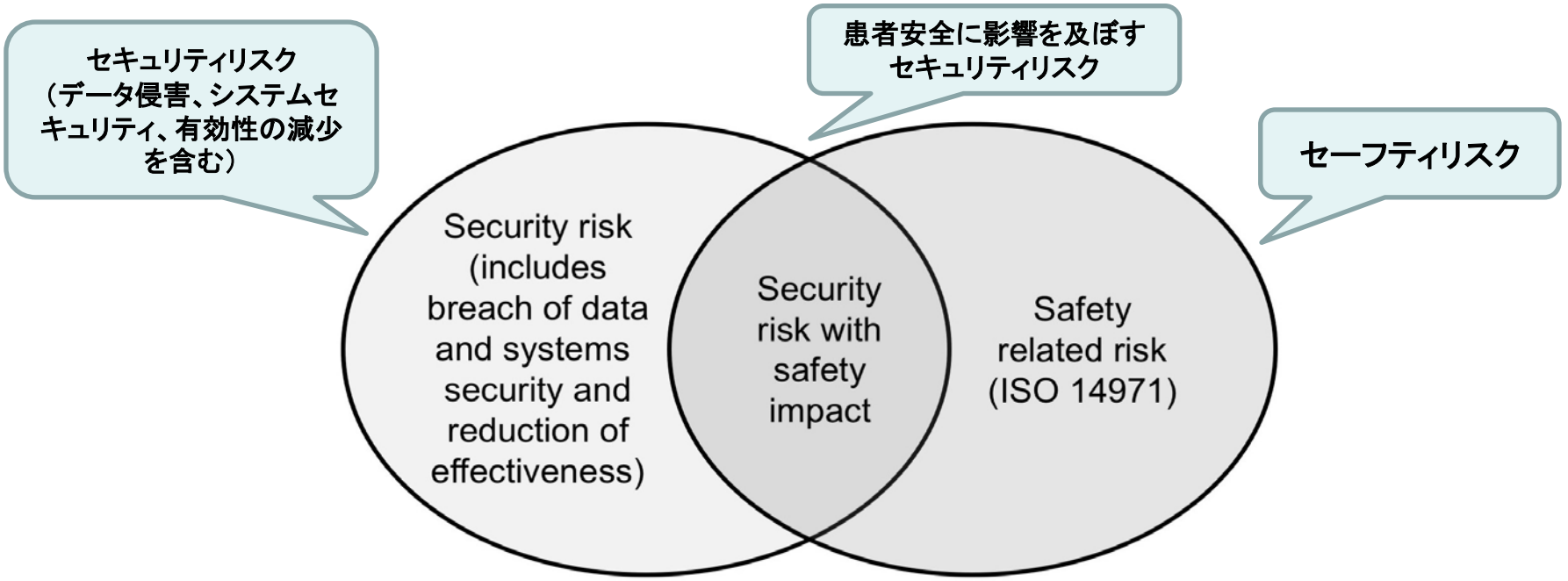
②サイバーセキュリティの確保が出来ていない機器に対する注意喚起を行うこと。

③医療機関においてサイバーセキュリティの確保が出来るように、必要な情報を提供して連携を図ること。

**実は日本においては画期的な通知であった。**

（他の分野ではPL法のような既存の枠組みの中でサイバーセキュリティに対処しようとしていた）サイバーリスクをリスクマネジメントの対象として求めた業種横断的なガイドラインとしては、総務省と経済産業省による「IoTセキュリティガイドライン」があるが、発行されたのは厚生労働省通知の一年以上後の2016年7月である。

# 医療機器の安全性とセキュリティ




AAMI TIR57:2016 Principles for medical device security—Risk management Figure 2

- 患者安全に影響を及ぼすセキュリティリスクを優先的に受容できるまで軽減しなければならない.
- サイバーリスクに対するリスクマネジメントは，ISO14971のスコープ外の事象についても検討の必要がある.（悪意を持った要因）
- 国内については，厚労省から通知「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」（H27.4.28）が出ており，方向性を示している.

# 医療機関と医療機器製造業者の役割分担

**医療機関**
**医療情報システムの事業者（インテグレータ）**

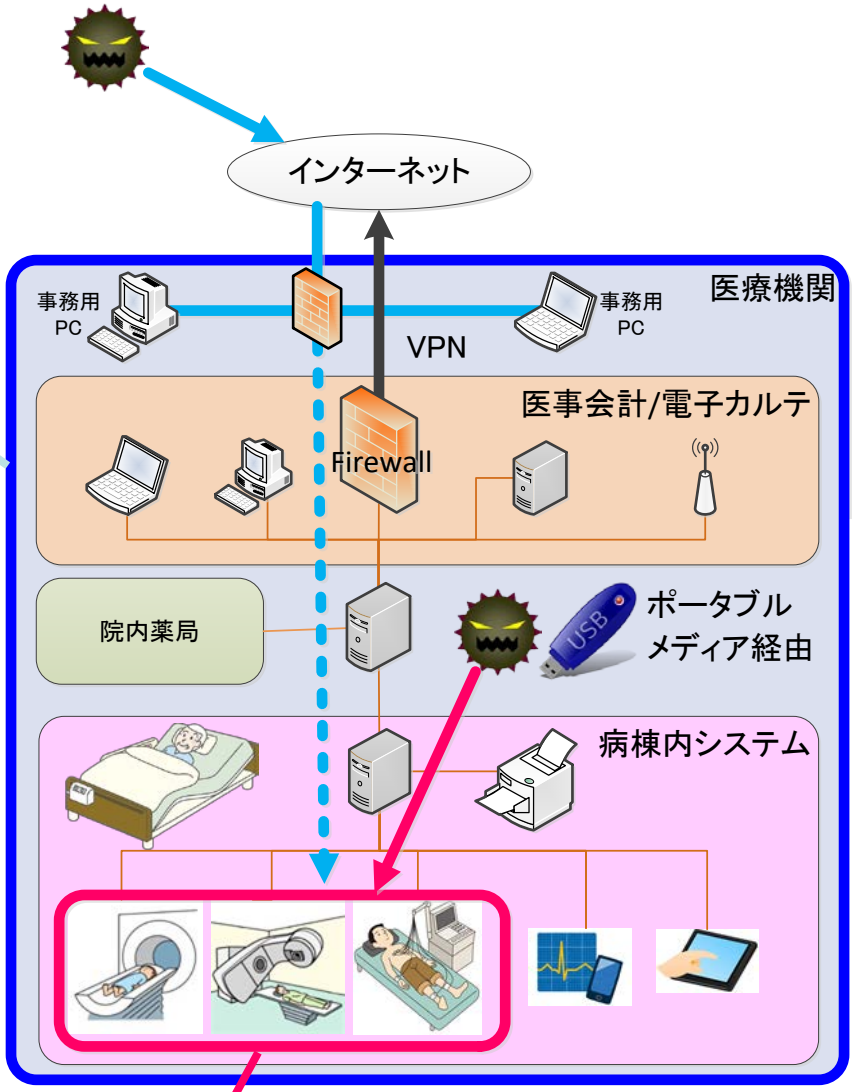
**【安全管理ガイドライン】**
**医療機関が主体となって医療情報システムの機密性・完全性・可用性を確保するために医療情報システムの安全管理を行う.**

http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf

**【サイバーセキュリティ通知】**
**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.**

https://www.pmda.go.jp/files/000204891.pdf

**医療機器の製造販売業者**




医療情報システムの機密性・完全性・可用性を確保する

医療機器の機能性と患者の安全を保持する

# 厚生労働省通知のポイント

既存の実際に使用されているサイバーセキュリティの確保が出来ていない医療機器を許容した上で、残存リスクがある旨を利用者に注意喚起させ、医療機関の組織としての情報セキュリティ対策を施すことで、既存の機器のセキュアゾーン内などでの利用を可能としている。

既存製品の回収のような重大なインパクトを与えず、医療機器製造業者各社に追加のリスクアセスメントを求めることでサイバーセキュリティ対策を啓発する非常にバランスの取れたもの

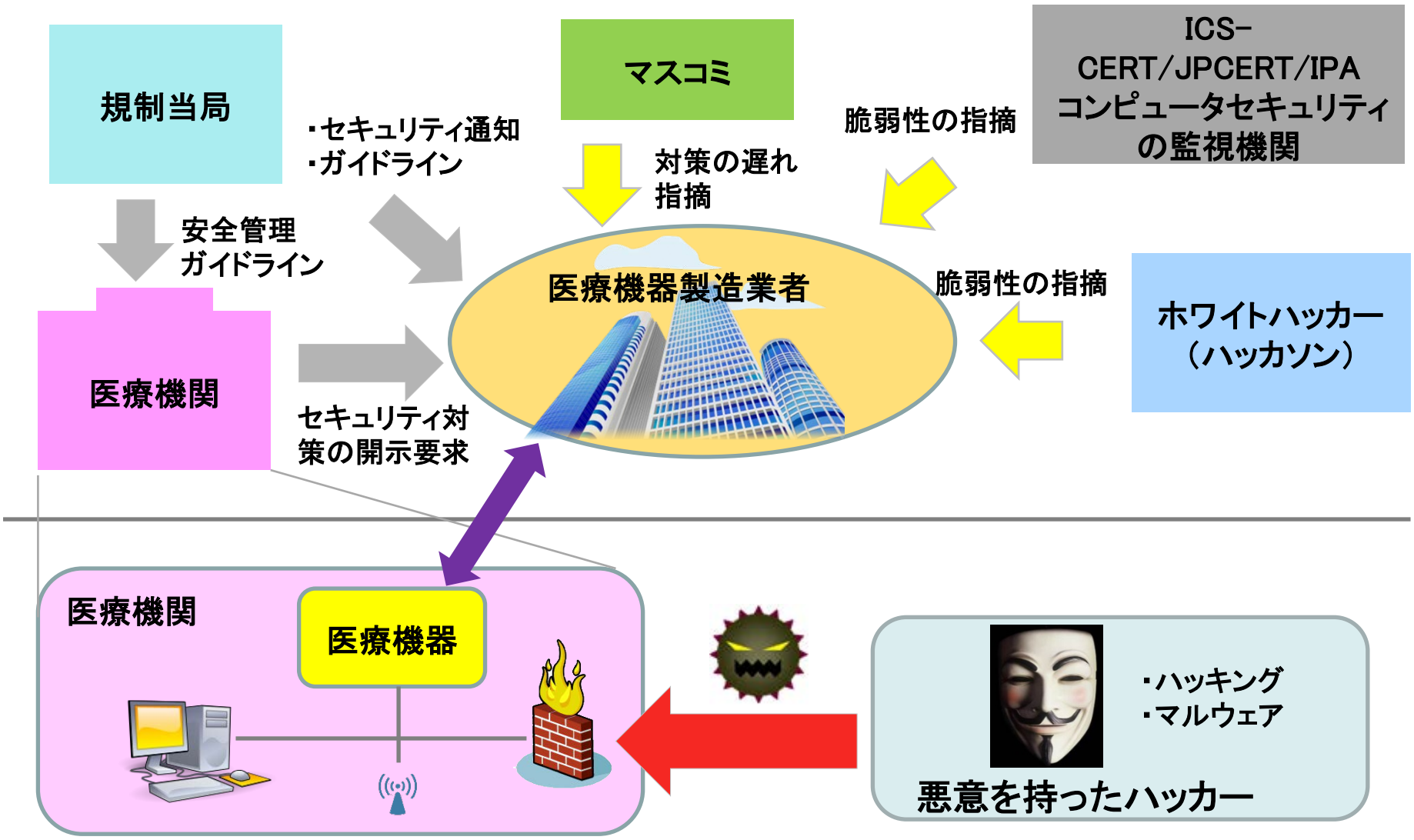
現実の運用においては、医療機器製造業者は「医療機器にどのようなセキュリティ対策が行われているか」を利用者に対して明確にすることが求められており、医療機関は機器単体では未対策な残存リスクに対する防護を組織としての技術的対策や運用的対策などでカバーする必要がある。

# 関係者の協調による対応の必要性

サイバーセキュリティに対処するには、医療機器に対する医療安全を守る医療機器製造業者、組織としての情報セキュリティ対策を行う医療機関、脆弱性情報の分析や情報提供を行うセキュリティの監視機関、規制やガイダンスを提供する国や自治体などが協調して対応する必要があり、どれが欠けても適切な対策を実施できない。

情報共有の仕組みやインシデント発生時のエスカレーションルールの策定など、迅速に対応できる仕組みの構築が求められる。

# 医療機器製造業者を取り巻くサイバーセキュリティ環境



# 2. 全国保健医療情報ネットワークの必要性

# 日本はガラパゴス？

- 日本では厚生労働省が「医療情報システムの安全管理に関するガイドライン」を早くから出版し、チャネルセキュリティ（OSI　1-3層）とオブジェクトセキュリティ（OSI　4-7層）を確保することを求めてきた。
- レセプトオンラインは、チャネルセキュリティとしてIP-VPNもしくはIPsec-VPNの実装を求め、オブジェクトセキュリティとしてTLSクライアント認証を求めており、どちらか一方が危殆化してもサービスを止めない運用が可能となっている。

# SSL/TLSの要求事項

欧米においてはオープンネットワークの利活用が前提となっており、チャネルセキュリティに対する要求は殆どなく、通信経路上のセキュリティにおいてはTLSの採用を求めているが、米国を中心にTLS1.2に限定する動きが出ている。

（DICOMではノード認証においてCRYPTRECガイドラインの高セキュリティ型に暗号スイートを限定する決定がされた）

・米国の医療機関間の情報連携においては、ONCが現在パブリックコメントにかけているTEFCA（Trusted Exchange Framework and Common Agreement ）においてオープンネットワークを前提としつつも、TLS1.2とIPアドレスのホワイトリストによる対応を求めており、チャネルセキュリティに対する考慮がされている。

# TEFCAにおける要求事項（案）

6.2.7 Transport Security.

Each Qualified HIN's security policy shall include the following elements to ensure appropriate data transport security:

(i) Authentication Server Requirements.

(c) Each Qualified HIN shall ensure that message exchanges are secured using TLS/SSL 1.2 X.509 v3 certificates for authentication, and X.509 certificates are used for authentication of all transactions.（TLS1.2が必須）

6.2.8 Certificate Policies.

Each Qualified HIN's security policy shall include the following elements to ensure that all Participant SSL certificates meet or exceed the following criteria:

(i) Key Sizes: The certificate authority shall utilize the SHA-256 algorithm for certificate signatures; and All keys shall be at least 2048 bit.（SHA-384や楕円暗号に対する考慮なし？）

(ii) Certificate Authority: The certificate authority's certificate shall be issued by a mutually trusted certificate authority; and The certificate authority's certification shall not be self-signed.（なんちゃって認証局は許さない）

6.2.9 Policy Binding.

Each Qualified HIN's security policy shall include the following elements to ensure appropriate policy binding by associating the X.509 digital certificate to the trust domain by meeting the following conditions:（PKIでのクライアント認証を求めている）

(iv) An approved trust chain issues the End Entity certificate.

**6.2.12 IP Whitelist.**

Each Qualified HIN shall publish and share all IP addresses that are whitelisted. An IP Whitelist can be implemented by the Qualified HIN's end point only if the result complies with the applicable Qualified HIN Participant's non-discrimination policy. For the purposes of this subsection, an end point will be the web service technical URL hosted by a Qualified HIN that is listed in the online TEFCA directory.（本当にメンテナンスできるのだろうか）

# JAHISオープンネット化の安全性について考える

- オープンネットワークにつながった製品等で隠れた脆弱性が露見した場合、直ちに該当製品全てに対策を講じないとシステム全体の安全性が揺らぎかねない。
  - 対策が遅れたところがセキュリティホールになる
  - 例えば、SSL/TLSのセキュリティ対策でCRYPTREC高セキュリティ型を採用したとしても、隠れた脆弱性がないとは言い切れない
- 危殆化対策としてもチャネルセキュリティによるネットワーク分離は有効な対策ではないか。
  - 対策を講じるリードタイムの確保や対策自体が難しい医療機器へのリスク低減に寄与できるのでは。

# JAHIS 全国保健医療情報ネットワーク

- 厚生労働省の医療等分野情報連携基盤検討会にて2020年の実現に向けて検討中
- セキュアゾーンとして守らなければならない医療の基幹系ネットワークを相互接続するならば、ネットワークそのものもセキュアゾーンに含めてしまえばよい。
- チャネルセキュリティの確保による安全・安心なネットワークの構築が重要
- 情報系やオープンネットワークとの分離によって標的型攻撃などから遮断することが肝要

# 3．医療機器（IoT）問題とオープンネットワーク

# 2020年問題

- XPが残存していることは前回も述べたが…
- Windows7サポート終了に伴う、多くの医療機器の危殆化問題が発生！！

厚生労働省のガイドラインを遵守する医療機関等においてはセキュアゾーンが構築されている。セキュアゾーン内での利用によって、医療機器そのものに脆弱性が残存していても、安全性は医療機関により担保されている…はず。

実は、この状況が、欧米との違いとなっている。

# FDAの危機感？

- FDAは医療機器の製造業者向けのガイダンスなどを立て続けにリリース
- 製造業者に医療機器に対するサイバー対策の追加を求める
- 製品のライフサイクル全体に対する強い要求

多層防御の考え方が無いわけではないが、
医療機器製造業者に対する対応要求が非常に厳しい
他のアクタとの協調について言及すると同時に
機器単体でのサイバー攻撃対策を強く求めていく流れ

# Windows Embedded

- 医療機器を含むIoTの多くが採用する組み込み用OSで医療機器と相性が良い
- 最新はWindows10 IoT
  - サポートはWindows10と同じで18か月（年に2回のアップグレードがあり、サポートが延長される）

（勝手にUGされるので、医療安全面での保証が厳しい）

  - Windows 10 IoT Enterprise LTSC版なら発売から10年保証、ただし10年間機能追加がない

（医薬品・医療機器等法的にはこっちで問題ない）

LTSCの発売から10年は医療機器の発売から10年ではない。
LTSCでも10年以内にサポートが切れるのは同じなので根本的な解決にならない

# アップデート対策

- LTSC版以外のWindows10に一斉アップデートがかかり、基幹ネットワークに瞬間的に莫大な負荷がかかる可能性がある
- 医療機関側が適切に制御しないとネットワークがボトルネックになり、システムが止まるかも？
- アップデートのトランザクションを分離して幹線ネットワークの帯域制御をできるのか

危殆化したOSを持つ医療機器が混在する医療機関の基幹ネットワークにおいてオープンネットワークを用いて最新のモジュールを使って適切にアップデートすることは非常に難しい

# ガラパゴスで良いのでは？

- 結局、チャネルセキュリティを確保してオープンネットワークから分離した環境のほうが安定してシステムが動くのではないか。
- 安全管理ガイドラインにより、セキュアゾーンを構築することが重要だと理解されている日本ならではの環境が作れる可能性がある。
- オープンネットワークを使うための様々な対策は閉域網を作るよりも高額になる可能性がある

厚生労働省の今後の議論に注目したい！

# 4. 国際標準化の転換点

# 前回会議の問題提起

- ドイツがIndustry4.0実現に向けIEC62443シリーズの様々な分野への適用を目指している。
- 医療分野に対して上記のアプローチが行われつつある。
- 日本としてどのように対応するべきか検討する時期に来ている。

# IECサイドのドイツからの提案

## IEC/I SO NP 80001-5-1

Application of risk management for IT-networks incorporating medical device -- Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software -- Part 5-1: Activities in the product lifecycle

**Form 4: New Work Item Proposal**

| | |
|---|---|
| Circulation date:<br>2018-06-08<br>Closing date for voting:<br>2018-08-31 | Reference number: ISO/IEC NP 80001-5-1<br>(to be given by Central Secretariat)<br><br>ISO/TC 215<br>N 2622 |
| Proposer<br>(e.g. ISO member body or A liaison organization)<br>DIN | |
| Secretariat<br>ANSI | |

Circulation　：　2018/06/08
Closing date for voting: 2018/08/31
Draft project plan　：　DIS submission　2019/09/01
Publication　2021/10/20
Liaisons　：　COCIR，DITTA，IEC/TC65 WG10

**Title of the proposed deliverable.**

**English title:**

Application of risk management for IT-networks incorporating medical device -- Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software -- Part 5-1: Activities in the product lifecycle

**French title:**

*(In the case of an amendment, revision or a new part of an existing document, show the reference number and current title)*

**Scope of the proposed deliverable.**

This document specifies activities in the product lifecycle of health software (including those software as/in a medical device) towards the information security of the product.

**Purpose and justification of the proposal***

For health software there are no specific standards regarding the state-of-the-art of lifecycle activities towards information security. There are various standards for the secure operation of connected systems - but few on how to build them in a way that supports security. For different application domains, there are already lifecycle specifications towards information security: E.g. a good overview of lifecycle activities can be found in IEC 62443-4-1, but this standard uses a language referring to the world of industrial automation and control systems (IACS).

*Consider the following: Is there a verified market need for the proposal? What problem does this standard solve? What value will the document bring to end-users? See Annex C of the ISO/IEC Directives part 1 for more information. See the following guidance on justification statements on ISO Connect:*
*https://connect.iso.org/pages/viewpage.action?pageId=27590861*

**Preparatory work** (at a minimum an outline should be included with the proposal)

☒ A draft is attached ☐ An outline is attached ☐ An existing document to serve as initial basis

The proposer or the proposer's organization is prepared to undertake the preparatory work required:

☒ Yes ☐ No

**If a draft is attached to this proposal:**

Please select from one of the following options (note that if no option is selected, the default will be the first option):

☐ Draft document will be registered as new project in the committee's work programme (stage 20.00)
☒ Draft document can be registered as a Working Draft (WD – stage 20.20)
☐ Draft document can be registered as a Committee Draft (CD – stage 30.00)
☐ Draft document can be registered as a Draft International Standard (DIS – stage 40.00)

If the attached document is copyrighted or includes copyrighted content:

☐ The proposer confirms that appropriate permissions have been granted in writing for ISO or IEC to use that copyrighted content.

**Is this a Management Systems Standard (MSS)?**

☐ Yes ☒ No

NOTE: if Yes, the NWIP along with the Justification study (see Annex SL of the Consolidated ISO Supplement) must be sent to the MSS Task Force secretariat (tmb@iso.org) for approval before the NWIP ballot can be launched.

## 提案された成果物の範囲

このドキュメントは，**製品の情報セキュリティに対するヘルスソフトウェア（医療機器としてのソフトウェアを含む）の製品ライフサイクルにおける活動を規定**している．

## 提案の目的と正当性

ヘルスソフトウェアの場合，情報セキュリティに対するライフサイクル活動の最先端技術に関する特定の基準はない．接続されたシステムの安全（secure）な操作のためのさまざまな標準があるが，接続されたシステムの構築においてセキュリティをサポートする方法はほとんど存在しない．異なる応用領域については，情報セキュリティに対するライフサイクル仕様がすでに存在している．**ライフサイクル活動の概要は，IEC 62443-4-1に記載されているが，この規格では，産業オートメーションと制御システム（IACS）の世界を参照する言語が使用されている．**



JAHIS安全性・品質企画委員会資料引用，一部修正

**Indication(s) of the preferred type to be produced under the proposal.**

☒ International Standard ☐ Technical Specification

☐ Publicly Available Specification ☐ Technical Report

**Proposed development track**

☐ 18 months* ☐ 24 months ☒ 36 months ☐ 48 months

**Note: Good project management is essential to meeting deadlines. A committee may be granted only one extension of up to 9 months for the total project duration (to be approved by the ISO/TMB).**

*DIS ballot must be successfully completed within 13 months of the project's registration in order to be elligible for the direct publication process

**Draft project plan (as discussed with committee leadership)**

Proposed date for first meeting: 2018-10-23

Dates for key milestones: DIS submission 2019-09-01

Publication 2021-10-20

**Known patented items (see ISO/IEC Directives, Part 1 for important guidance)**

☐ Yes ☒ No

If "Yes", provide full information as annex

**Co-ordination of work: To the best of your knowledge, has this or a similar proposal been submitted to another standards development organization?**

☐ Yes ☒ No

If "Yes", please specify which one(s):

**A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables.**
**The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized.**

The proposed standard will be structured according to the existing health software lifecycle standards IEC 62304, yet it will specify activities towards information security (rather than product safety). It will not copy specific security methods or techniques but refer to clauses in existing and established information security standards.

**A listing of relevant existing documents at the international, regional and national levels.**

IEC 62443-4-1, AAMI TIR57, FDA 'Content of Premarket Submissions for Management of Cybersecurity in Medical Devices' and 'Postmarket Management of Cybersecurity in Medical Devices' .

**Please fill out the relevant parts of the table below to identify relevant affected stakeholder categories and how they will each benefit from or be impacted by the proposed deliverable(s).**

| | Benefits/impacts | Examples of organizations / companies to be contacted |
|---|---|---|
| Industry and commerce large industry | Clarity on consensus on appropriate activities towards product information security | AAMI, COCIR, DITTA, ZVEI |
| Industry and commerce SMEs | s.a. | s.a. |

ISとすることを意図している.

既存の作業，特に既存のISOおよびIEC成果物との関係，影響について

提案された規格は，既存のヘルスソフトウェアライフサイクル規格IEC 62304に従って構成されるが，製品の安全性（safety）ではなく情報セキュリティへの活動を規定している．特定のセキュリティ方法または技術をコピーするのではなく，既存および確立された情報セキュリティ基準の条項を参照する.

**【参照規格】**

IEC62443-1： Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

AAMI TIR57： Principles for medical device security—Risk management

FDA：

-Content of Premarket Submissions for Management of Cybersecurity in Medical Devices'

-Postmarket Management of Cybersecurity in Medical Devices



JAHIS安全性・品質企画委員会資料引用，一部修正

## まとめ：

- safetyではなくinformation securityが対象.
- 製品ライフサイクルの中での活動を規定.
- ヘルスソフトウエア製品を対象.
- 規制対象・対象外を含む.
- IEC 62443を参考にする.
- 製造者が対象。
- 開発 -> リリース -> 保守まで．導入，臨床利用は含んでいない.
- セキュリティコントロールの技術仕様は，含まない．ここはドイツ（DKE）が，IEC 60601-4-xを準備中

**演者の邪推**

ドイツの世界戦略としてのIEC62443を梃子にしたIndustry4.0の展開に対して、医療分野のサイバー攻撃対策での対応に困っていた米国が医療機器に対する規制強化の流れの中で、製造プロセスにおける管理を目指して手を握った格好に見えなくもない（JWG7コンビナーの米国からドイツへの交代、IEC主導のセキュリティへのScope拡張、製品から組織へのターゲットの変化etc.）

# ISO/TC215PAESTUM会議

- 2018年10月下旬にイタリアのパエスタムにて開催された。ISO/TC215とIEC/SC62Aのジョイントwgであるjwg7はサイバーセキュリティ問題にからむ各種規格群について積極的に議論を実施した。

（他のwgより一週間早く現地入りし、連日議論を行っていた）

# 全体のまとめ

- 医療安全対策は新時代に突入している
- 情報セキュリティに対する過剰な注目と期待
- 医療機関は常に最新の設備で動いているものではない（特に医療機器）
- かじ取りを誤ると大きな社会的損失につながる
  （社会全体としてのコストを見ないと見誤る）
- 本当はどうあるべきなのかを真剣に考えよう

健康で豊かな国民生活を保健医療福祉情報システムが支えます

# ご清聴ありがとうございました