2021年度セキュリティ委員会成果報告

一般社団法人 日本画像医療システム工業会（JIRA)
医用画像システム部会　セキュリティ委員会

報告内容

- **21年度の活動内容**
  - ISO TC215 対応
  - JIRA-JAHIS合同開示説明書WG（MDS-WG）
  - JIRA-JAHIS合同リモートサービスセキュリティWG（RSS-WG）
  - DICOM WG14対応
  - 医療機器のサイバーセキュリティの取り組み
  - その他
- **22年度の活動方針**

ISO TC215 WG4対応

WG4(Security, Safety and Privacy）、及びJWG7(IEC SC62AとのJoint)に対応

- **TC215 WG4会議（リモート開催）のISOエキスパート参加（1～2名）**
  - 2021年　4月13、16日
  - 2021年　6月17日　　Plenary meeting
  - 2021年　8月25、26日
  - 2021年12月16日
  - 2022年　6月6日　　（次回　Plenary meeting）
- **規格検討への取り組み**
  - 重要な規格へエキスパート登録
  - NP/SR投票対応。ドラフトの内容検討、JIRAとしての意見集約
- **委員会関与の規格提案**
  - IEC/ISO TR 81001-5-2(旧IEC TR 80001-2-2)：
    医療機器のセキュリティニーズ，リスク及びコントロールの開示及びコミュニケーションの指針
    ◆ドラフティング作成（SBOM、リモート等）

NP：New work item proposal 新規作業提案
SR: Systematic Review 定期見直し

SBOM：Software Bill Of Materials ソフトウェア部品表

注目の国際規格例

ISO関連

- ISO 27789 (Ed 2)：監査証跡。DICOM Part15、IHE ATNAとの整合性
- ISO/TR 11636　：医療情報インフラとしてのダイナミックオンデマンドVPNについて。リーダーは日本
- ISO/TS 20405　：安全性に関するイベントの監視と分析、報告のフレームワーク
- ISO/DTR 24306　：Personal Health Careシステムのゲートウェイに関するセキュリティガイダンス
- ISO/TS 17975　：個人健康情報の収集、使用、開示に関する同意の原則とデータ要件
- ISO 27799　：ISO/IEC 27002を使用した医療分野における情報セキュリティマネジメント

JWG7関連

- ISO 81001-1　：ヘルスソフトウェアとヘルスITシステムの安全性、有効性、セキュリティ。JIS化
- IEC 80001-1 Ed.2：医療機器等を組み込んだITシステムのリスクマネジメント規格。対訳作成中
- IEC 81001-5- 1　：ヘルスソフトウェアの開発と保守に関するセキュリティライフサイクル要件。JIS化
- ISO/TS 82304-2　：ヘルスアプリの品質ラベル

JIRA-JAHIS合同開示説明書WG（MDS-WG）

- JIRA-JAHIS合同開示説明書WG（MDS-WG）にて、2013年4月に初版発行
  - 現Verは4.0（安全管理ガイドライン第5.1版対応）2021/10発行
- 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」への適合を示すチェックリストと、書き方を示したガイド
- 製造業者が医療機関に対し、医療情報システムの情報セキュリティに関する情報を開示する際に使用(MDS)
- サービス事業者が医療機関に対し、医療情報システムを用いて提供するサービスの情報セキュリティに関する情報を開示する際に使用(SDS)

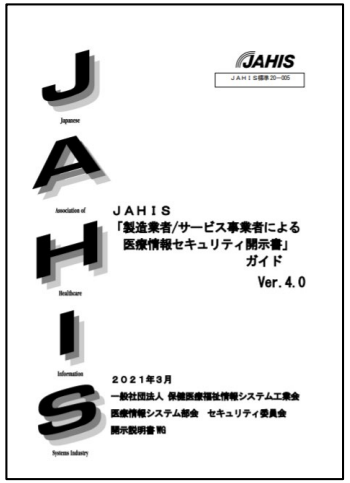
MDS／SDS利用の利点

- 医療機関が製造業者/サービス事業者にセキュリティ機能の説明を求める際の統一した要求形式
- 医療機関にとってのリスクアセスメントの材料
- 製造業者/サービス事業者にとって、安全管理ガイドラインへの適合性の自己評価手段

MDS-WG活動の振り返り

医療情報セキュリティ開示書ガイド（Ver.4.0）の発行

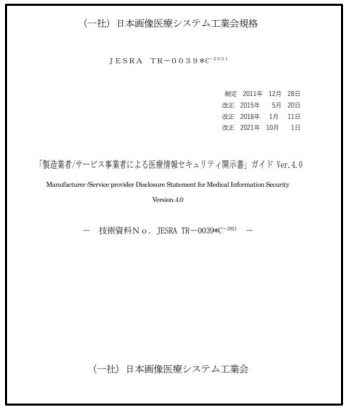
- JAHIS側とJIRA側で公開時期のズレの改善を検討する。
  - JAHIS版：2021年3月発行
  - JESRA版：2021年10月発行
- HELICS審査実施中
  - 安全管理ガイドラインでは不十分な点があるとの意見が出たが、開示書の主旨より安全管理ガイドラインを超えた内容には言及しない方向
  - 上記意見は理解するのでJIRA/JAHISセキュリティ委員会に持ち帰って議論を検討したい。



JAHIS版：2021年3月発行

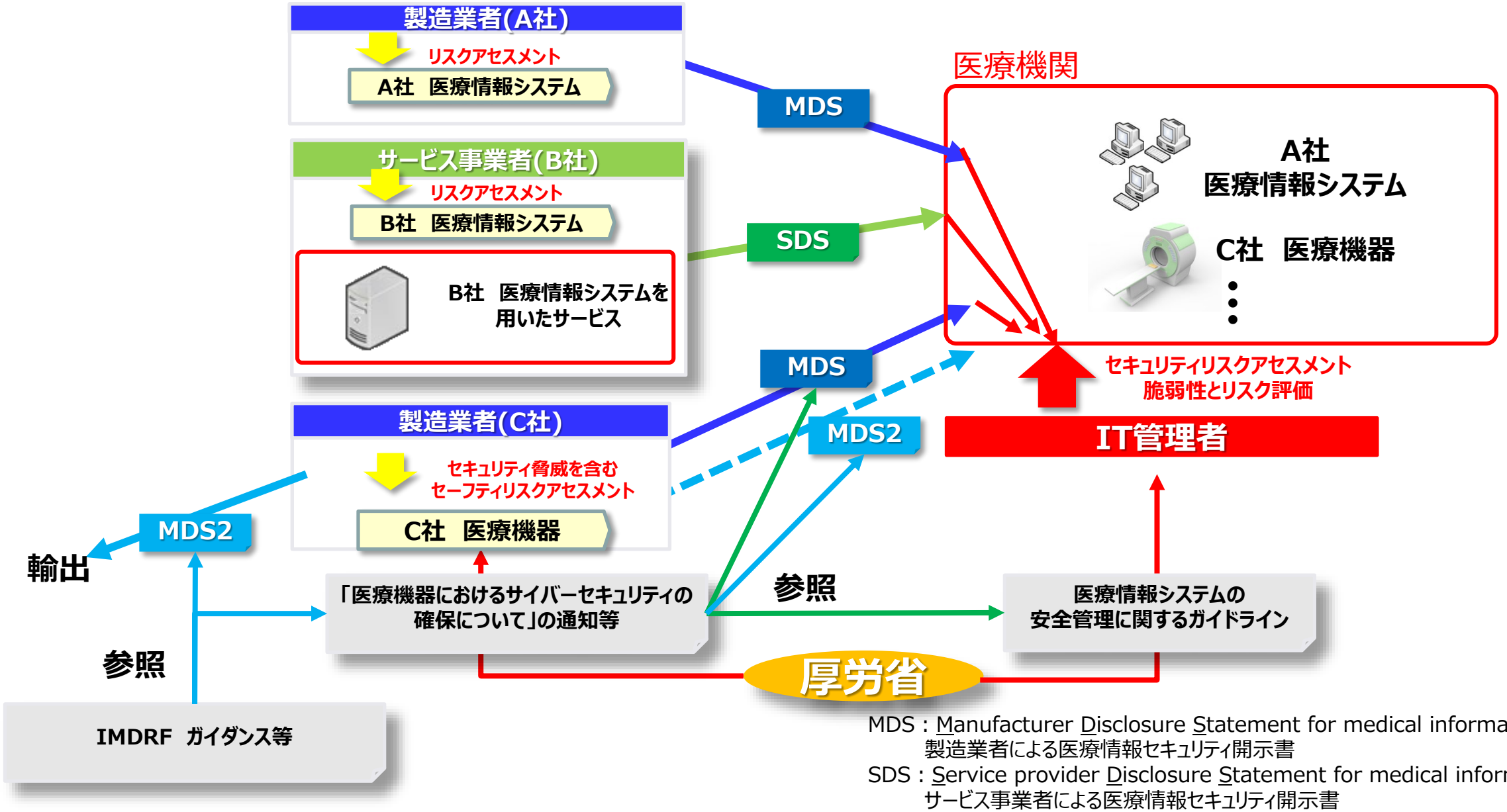
サービス事業者による医療情報セキュリティ開示書（SDS）の講習

- 書き方セミナー（オンライン）を2022年1月28日実施
  - JAHIS/JIRAセキュリティ委員会より講師3名選出



JESRA版：2021年10月発行

MDS/SDS、MDS2の位置付け（MDS-WG）

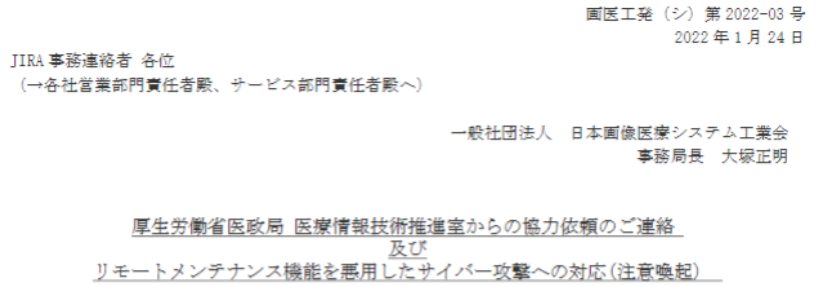


MDS：Manufacturer Disclosure Statement for medical information security
製造業者による医療情報セキュリティ開示書
SDS：Service provider Disclosure Statement for medical information security
サービス事業者による医療情報セキュリティ開示書

リモートサービスセキュリティWG（RSS-WG）

- **リモートサービスセキュリティガイドラインVer.3.0改訂**
  - セキュリティ関連の最新情報に合わせての見直し
  - 3.1版を作成中（JAHIS標準化（3月中）、JESRA版作成（4-5月頃予定））
- **リモートサービスにおける注意喚起とさらなる対策支援**
  - リモートサービス経路を狙ったランサムウェア攻撃が多発*1
    - 「暗号化されたデータの復旧」「データ公開による脅迫」での身代金要請
  - MDS-WGと連携してリモートサービスに対するSDSの記載例作成を予定
  - JIRAは、「厚生労働省からの緊急の医療施設への調査依頼」に関する会員企業への協力依頼と注意喚起を発行(2022/1/24)

*1 国内で2016年以降に少なくとも11病院が「ランサムウェア」による被害を受けているとの報道あり



画医工発（シ）第 2022-03 号
2022 年 1 月 24 日

JIRA 事務連絡者 各位
（→各社営業部門責任者殿、サービス部門責任者殿へ）

一般社団法人　日本画像医療システム工業会
事務局長　大塚正明

厚生労働省医政局 医療情報技術推進室からの協力依頼のご連絡
及び
リモートメンテナンス機能を悪用したサイバー攻撃への対応（注意喚起）

1．厚生労働省医政局 医療情報技術推進室からの協力依頼
2．JIRA からの会員各社へのセキュリティに関する注意喚起
2.1 リモートメンテナンス機能を悪用したサイバー攻撃への対応(注意喚起)
2.2 平時から注意頂きたい事項

https://www.jira-net.or.jp/publishing/jesra.html

●JIRA で参考になる文書 「リモートサービスセキュリティガイドライン Ver.3.0※」(JESRA TR-0034B(最新 2016/8/23))

4) 御社で提供しているリモートメンテナンスサービスで使用しているリモートゲートウェイ(VPN 装置)などにおいて JISRATR-0034 に従い現在もセキュリティが確保されていることの確認をしていただくこと

DICOM委員会と共同で対応中

- **IETF BCP195の改定（2021.3）に伴うTLS Secure Transport Profile の見直し**

  TLS 1.0および1.1の非推奨を受けて、BCP195ベースの3つのプロファイルの見直し検討

  - BCP195 TLS Secure Transport Connection Profile
  - Non-Downgrading BCP195 TLS Secure Transport Connection Profile
  - Extended BCP195 TLS Profile Secure Transport Connection Profile（JIRA 2018提案）

  ↓

  TLS暗号設定ガイドラインVer.3.0.1（Cryptrec/IPA 2020.7公表）

  高セキュリティ型（高い安全性の確保を必要とするケース）の要件を考慮した新たなProfile を提案中

- **CP-2148 Clarify audit trail messages**
  - 監査証跡メッセージの多数の誤植修正を提案

医療機器のサイバーセキュリティの取り組み

- **昨年同様、世界的にランサムウェアの被害が拡大。ヘルスケア分野の全ての利害関係者へのサイバーセキュリティへの取り組みが強く求められている**
  - アイルランドの保健サービス委員会（**HSE**）が「**Conti**」による攻撃を受ける（2021/5）
  - 米インディアナ州の病院Johnson Memorial Health、ランサムウェアによる攻撃を受ける（2021/10）
  - イスラエルの病院Hillel Yaffe Medical Center、イスラエル初の大規模なランサムウェア攻撃を受ける（2021/10）
- **国内では、つるぎ町立半田病院でランサムウェア被害が発生(2021/10)**
  - 電子カルテのデータ約85,000人分がバックアップを含め全て暗号化され、利用不可に（会計システムも利用不可）。システム復旧まで2ヵ月を要する事態となる。
  - 世界的ハッカー集団「ロックビット」の仕業と考えられる。日本では過去にHOYAやカプコンが被害を受けた。
  - 保守用回線・機器を通して侵入された可能性が高い。今後、約2億円をかけてサーバの入替や、システムのセキュリティ向上を予定

サイバーセキュリティに対処するには、医療機器に対する安全を守る医療機器製造業者、医療機器を含む医療情報システムの対策を実施する製造業者、医療情報システムを用いたサービスを提供するサービス事業者、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ません。

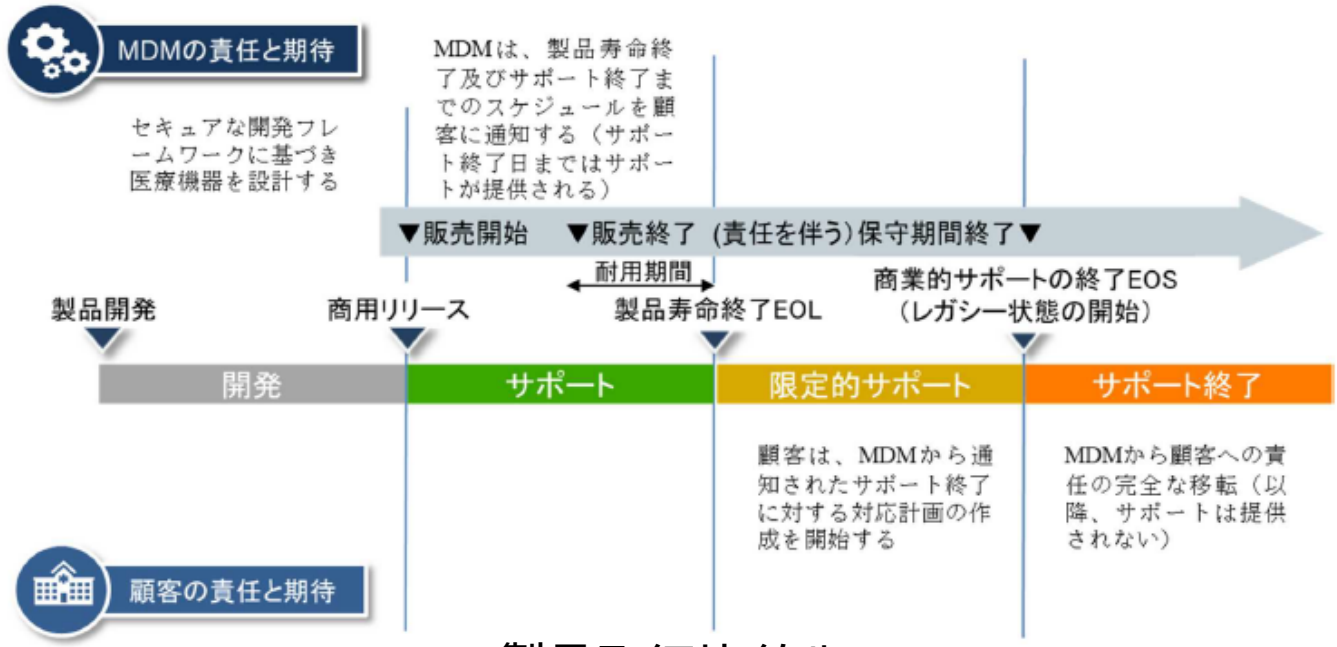
医療機器のサイバーセキュリティの取り組み

「医療機器のサイバーセキュリティ導入に関する手引書」の作成　－2021年12月24日発出－

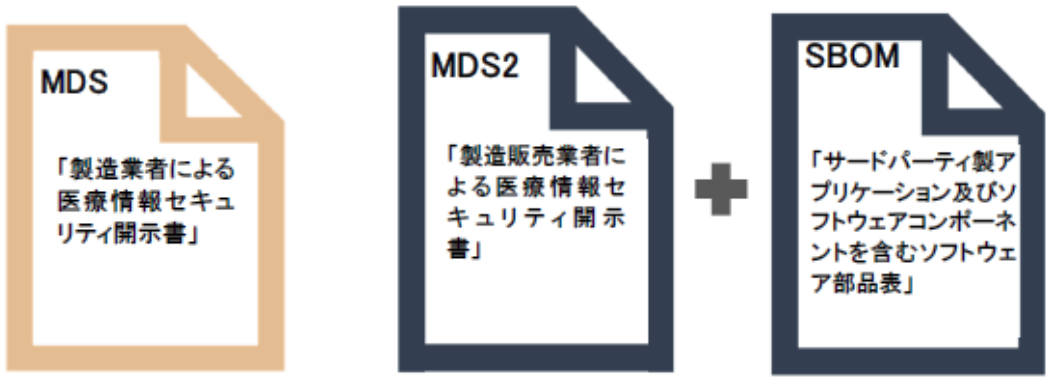
https://www.mhlw.go.jp/hourei/doc/tsuchi/T211228I0070.pdf

- 製版業者向けの手引書。セキュリティ委員会より手引書の作成WGに参画
- 製品ライフサイクル全体に渡って安全性が受容可能なレベルに保たれているかの情報提供を行う
- MDS,MDS2, SBOMのセキュリティ文書を活用し、リスクの把握を行う

※　医療機関向けサイバーセキュリティ手引書（草案作成中）についてもコメント等を提出



製品ライフサイクル



セキュリティ開示文書

その他

各国法規、ガイドライン類に対して情報共有、周知活動を実施

- **IEC TC62/SNAIG**
  - IEC 60050の更新（ヘルスケア分野での用語定義、ヘルスソフトウェア、ネットワーク、サイバーセキュリティ、ロボット、AI等の用語補充）
  - AI/サイバーセキュリティについては日本からSNAIGレポート提出
- **IMDRF AIMD WG**
  - 人工知能関連。JWG7で情報共有
- **FDA-MITA会議**
  - SBOM、レガシー機器、セキュリティポリシーの扱いについて共有
- **IPA CIP Security News**
  - ランサムウェア等、各国のサイバーセキュリティ関連情報の共有

他工業会との協調・連携活動

- 厚労省「安全管理ガイドライン」5.2版改定作業への参画（JIRA/JAHIS/JEITA）
- IMDRF 医機連サイバーセキュリティ対応WGへの参画（JIRA/JEITA）

22年度の活動方針

ISO TC215

- WG4及びJWG7対応も含め、継続的に活動を続ける。

MDS-WG

- セキュリティ対策へのMDSの活用を促進すべく、最新版の安全管理ガイドラインへの対応等を行う。
- 製販企業側、医療機関側が共にMDSによる安全管理の確認が行えるように周知を行う。

RSS-WG

- MDS-WGと連携し、リモートサービスにおけるSDS記載例の作成等を通じて、増加するセキュリティの脅威に対して徹底した対策の促進を普及させる。

DICOM-WG6/WG14

- セキュリティ関連について、継続してDICOM委員会と共同で対応を進める。

医療機器のサイバーセキュリティの取り組み

- サイバーセキュリティ関連についての最新情報を常に収集し共有するとともに、対応について「手引書」制定、普及等を行うことで製販企業側、医療機関側の対策の強化を促進する取組みを実施する。

その他にも、各国法規やガイドラインなどの情報収集を行い、情報提供や対応を行っていく。

御清聴 ありがとうございました。