2022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

- **22年度の活動内容**
  - ISO TC215 対応
  - 医療機器のサイバーセキュリティの取り組み
  - MDS-WG
  - RSS-WG
  - DICOM WG14/WG6/DSC
  - その他
- **23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
主な国際会議への参加は以下

- **TC215 WG4会議へのエキスパート参加（リモート参加）**
  - 2022年　4月28日　（Web開催）
  - 2022年　9月22日　（Web開催）
  - 2023年　1月13日　札幌

- **JWG7会議へのエキスパート参加**
  - 2022年　5月31日-6月1日　（Web開催）
  - 2022年　9月6日-9月8日　ミュンヘン
  - 2023年　1月10日-12日　札幌

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

ISO TC215 WG4／JWG7対応

- **規格検討への取り組み**
  - TC215 WG4、JWG7各々10数件の関連規格をウォッチ
  - 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

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

- **委員会関与の規格提案**
  - IEC TS 81001-2-2：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
    - ◆最終的にTR（技術報告書）からTS（技術仕様書）へ。IEC TS 81001-2-2として規格化
    - ◆NP投票の結果、約160件のコメント有。今後コメント解決を行いDTS案開発を進めていく
    - ◆2024年の秋までにTS発行予定

注目の国際規格例

WG4関連

ISO 27799	医療分野における情報セキュリティマネジメント。
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 **［日本提案］**
ISO 25237	仮名化。SRでの改定が承認。プロジェクトリーダー募集
ISO 21298	機能的および構造的役割。SR承認
ISO 17090-4	HPKIによる電子署名。エキスパート募集がかかる予定

JWG7関連

ISO TS 81001-2-1	アシュアランスケース。TR 80001-2-9から移管
IEC TS 81001-2-2	セキュリティ機能の開示及び運用。DTS案作成へ進む。TR 80001-2-2及びTR 80001-2-8から移管

医療機器のサイバーセキュリティの取り組み

医機連のサイバーセキュリティタスクフォース（TF）、対応ワーキンググループ（WG）活動に参加

- **医機連：サイバーセキュリティTF活動状況**
  - 医療機関における医療機器のサイバーセキュリティ確保のための手引書作成
    - ◆パブコメ終了、3月に手引書発行予定
- **医機連：サイバーセキュリティ対応WG活動状況**
  - 基本要件基準改正施工に関する検討
  - IMDRF サイバーセキュリティWGでのSBOM、レガシー医療機器ガイダンス案の作成
    - ◆パブコメ終了、最終審議を経て3月に文書発行予定
  - 医療機器のサイバーセキュリティ導入に関する手引書（改訂）案作成
    - ◆パブコメ終了、3月に手引書（改訂版）発行予定
  - 経済産業省サプライチェーン・サイバーセキュリティ対策促進事業での実証実験を支援
    - ◆近畿レントゲン工業社製歯科用コーンビームCTでのSBOM作成管理等

対象医療機器：株式会社近畿レントゲン工業様
歯科用コーンビームCT(製品名KR-X SCAN)
https://x-raykinki.co.jp/product_kr-xscan70/

表A-2 SBOMの最小限の要素

要　素	内　容
ソフトウェアコンポーネントのサプライヤーの名前	コンポーネントの作成、定義又は識別を行うエンティティ
ソフトウェアコンポーネントの名前	サプライヤーが定義してソフトウェアユニットに割り当てた名称
ソフトウェアコンポーネントのバージョン	以前のバージョンからの変更を特定するためにサプライヤーが用いる識別子
固有識別子	コンポーネントを識別するために使用する、又は関連するデータベースのルックアップキーとして機能する識別子
コンポーネントハッシュ	コンポーネントのバイナリーを識別するために用いる暗号化ハッシュ
関係	上流のコンポーネントXがソフトウェアYに含まれているという関係を特徴づける情報
作成者名	SBOMエントリーの作成者
タイムスタンプ	SBOMデータの集約を行った日時の記録

医療情報セキュリティ開示書（MDS/SDS）とは

MDS	**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
SDS	**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

- 医療情報セキュリティ開示書ガイド
  - 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

MDS／SDS利用の利点

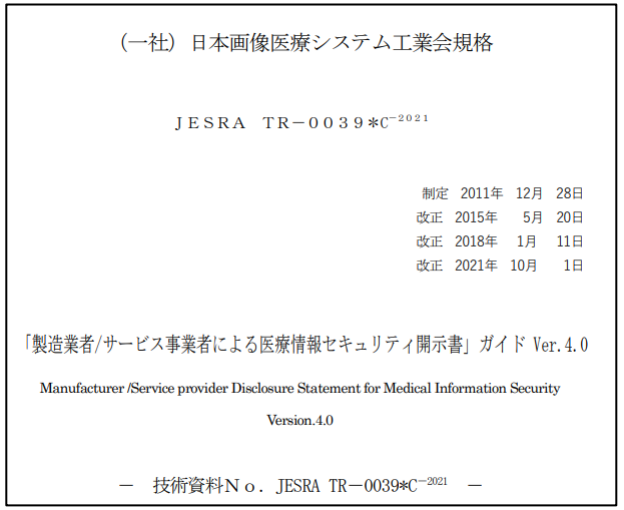
- 医療機関が製造業者/サービス事業者にセキュリティ機能の説明を求める際の統一した要求形式
- 医療機関にとってのリスクアセスメントの材料
- 製造業者/サービス事業者にとって、安全管理ガイドラインへの適合性の自己評価手段

医療情報セキュリティ開示書ガイド

- Ver4.0 JESRA版のHELICS審査完了
  - 「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイドがHELICS指針として採択（2022年9月2日）

MDS/SDS Ver4.1

- JAHIS/JIRA合同MDS-WGにて対応中
  - 「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版への対応
  - 医療情報セキュリティ開示書ガイド Ver4.1原案作成完了(2023年1月)
  - チェックリスト（EXCEL）の条件付き書式の回答選択肢を見直し
    - ✓「はい、いいえ、対象外」のみから、一部の質問に対して「該当、非該当」を適用


（一社）日本画像医療システム工業会規格

JESRA TR−0039*C−2021

制定 2011年 12月 28日
改正 2015年 5月 20日
改正 2018年 1月 11日
改正 2021年 10月 1日

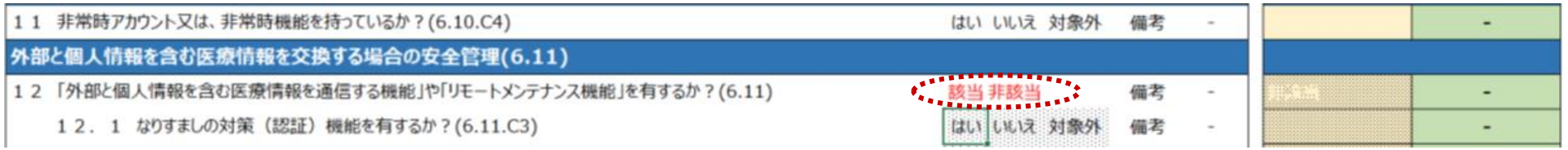
「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.4.0

Manufacturer /Service provider Disclosure Statement for Medical Information Security

Version.4.0

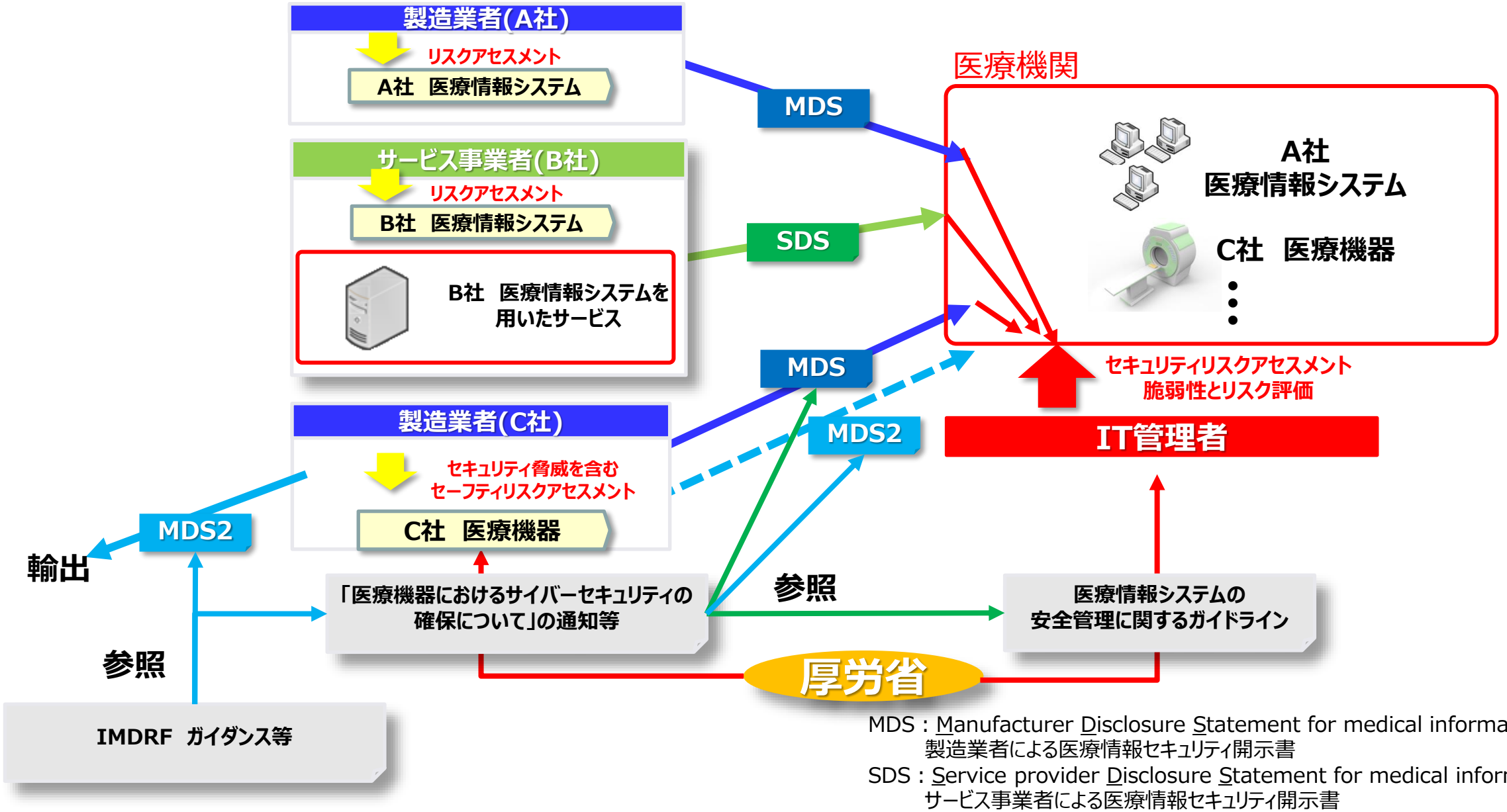
− 技術資料No. JESRA TR−0039*C−2021 −

TR-0039C 製造業者/サービス事業者による医療情報セキュリティ開示書ガイド（2021年10月1日発行）
https://www.jira-net.or.jp/publishing/files/jesra/JESRA_TR-0039C_2021.pdf



MDSチェックリスト例

＜参考＞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

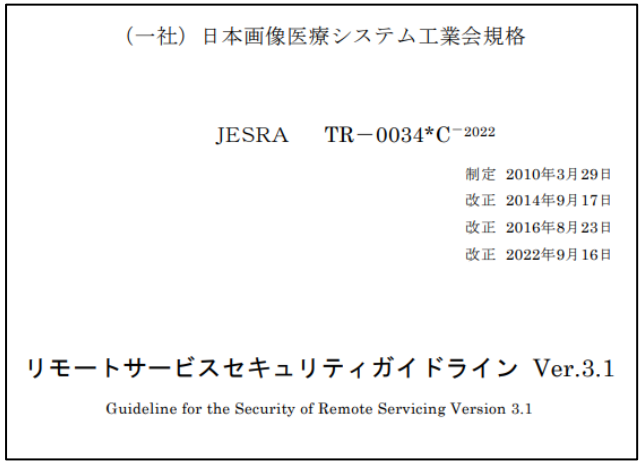
リモートサービスセキュリティWG（RSS-WG）

リモートサービスセキュリティガイドライン

- 改定版Ver.3.1を作成、発行
  - TR0034C「リモートサービスセキュリティガイドライン Ver.3.1」

リモートサービスに特化したSDS記載例作成の検討

- 総務省・経産省の統合ガイドラインのService Level Agreement (SLA)サンプルを参考にサンプルSLAを作成（2022年12月）
- SLAを踏まえたSDS記載例を作成（2023年3月予定）
  - JIRA/JAHIS合同MDS-WGと情報共有し、最終確認段階


（一社）日本画像医療システム工業会規格

JESRA　TR−0034*C−2022

制定 2010年3月29日
改正 2014年9月17日
改正 2016年8月23日
改正 2022年9月16日

リモートサービスセキュリティガイドライン Ver.3.1

Guideline for the Security of Remote Servicing Version 3.1

TR0034C リモートサービスセキュリティガイドライン Ver.3.1（2022年9月16日発行）
https://www.jira-net.or.jp/publishing/files/jesra/JESRA_TR-0034C_r1_2022.pdf

リモートサービスセキュリティのSDS作成では、RSS-WGはMDS-WGと共に活動を進めてきており、今後も必要に応じて関連のあるWG同士で情報共有を行う

- **Sup230 Update BCP Secure Communications Profiles** **<2022.12 Final Text>**

  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の使用を認める旧BCP195ベースの3つのプロファイルをリタイヤとし、
  新BCP195ベースのTLS 1.2以上を必須とする以下2つのプロファイルを定義
  - BCP 195 RFC 8996 TLS Secure Transport Connection Profile
  - Modified BCP 195 RFC 8996 TLS Secure Transport Connection Profile
    ◆TLS暗号設定ガイドラインVer.3.0.1（Cryptrec/IPA）の高セキュリティ型相当 **［日本提案］**

- **CP-2148 Clarify audit trail messages** **<2022.9 Final Text>**

  ◆監査証跡メッセージの多数の誤植修正 **［日本提案］**

DICOM WG14 については、DICOM委員会と協働で対応

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

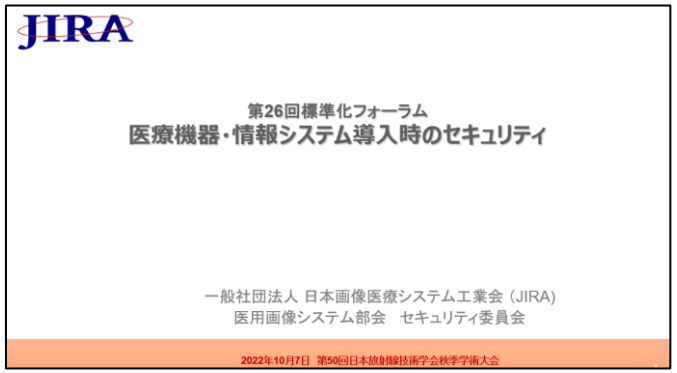
- **IEC TC62/SNAIG※**　※SNAIG：IEC TC62 のソフトウェア、ネットワーク及びAI についての諮問委員会
  - ヘルスソフトウェア、ネットワーク、サイバーセキュリティ、ロボット、AI等での情報を共有
- **IMDRF AIMD WG**
  - 人工知能関連。JWG7で情報共有
- **FDA-MITA※※会議**　※※MITA：米国電気機器製造業者協会（NEMA）傘下の医用画像工学関連機器事業部会
  - SBOM、レガシー機器、セキュリティポリシーの扱いについて共有
- **IPA CIP Security News**
  - ランサムウェア等、各国のサイバーセキュリティ関連情報の共有

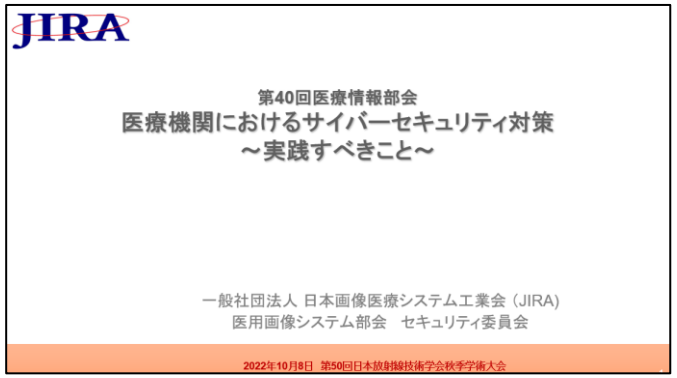
他工業会との協調・連携活動

- 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）

学会・シンポジウム等での講演

- **第50回日本放射線技術学会秋季学術大会**
  2022年10月7日-9日　国際ファッションセンター（東京・両国）
  - 第26回標準化フォーラム
    ◆医療機器・情報システム導入時のセキュリティ
  - 第40回医療情報部会
    ◆医療機関におけるサイバーセキュリティ対策 ～実践すべきこと～





23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。

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、手引書の作成／更新等、TF,WG活動を通じて具体的に製販企業側、医療機関側の対策強化を促進する取組みを実施する。

MDS-WG

- セキュリティ対策へのMDS/SDSの活用を促進すべく、他工業会と協働で安全管理ガイドライン6.0版へ向けたセキュリティ開示書ガイド更新やセミナー活動等を行う。
- 製販企業側、医療機関側が共にMDS/SDSによる安全管理の確認が行えるように周知を行う。

RSS-WG

- リモートサービスにおけるSDS記載例を有効活用し、リモートサービスへの安全対策の促進を行う。
- リモートサービスガイドラインの改定への取り組みを行う。

DICOM-WG6/WG14/DSC

- セキュリティ関連について、 DICOM C/Sのセキュリティ表記等についての周知策等、今後必要となり得る事例を含め、継続してDICOM委員会と協働で対応を進める。

その他、セキュリティに関する情報取集、共有、対策の普及について積極的に活動する。

御清聴 ありがとうございました。