2020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　委員長 葉賀　功

2021/02/19 医用画像システム部会 成果報告会

報告内容

- 20年度の活動内容
  - ISO TC215 WG4対応
  - リモートサービスセキュリティWG(RSS-WG)
  - JIRA-JAHIS合同開示説明書WG(MDS-WG)
  - SPC MDS2対応
  - 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
- 21年度の活動方針

ISO TC215 WG4対応

WG4(Security, Safety and Privacy）を主に、JWG7にも対応

- TC215 WG4会議のISOエキスパート参加（1～2名）
  - 2020年5月　22nd
  - 2020年8月　23nd
  - 2020年10月　24nd＋25nd
  - 2021年1月　26nd
  - 2021年6月　27nd　ワシントンDC（US）　（次回）

- 規格検討への積極的な取り組み
  - 重要な規格へエキスパート登録
  - ドラフトの内容検討、JIRAとしての意見集約
  - NP/SR投票対応

- 委員会関与の規格提案
  - JAHISセキュリティ委員会と合同のリモートサービスセキュリティWG(RSS-WG)で作成したガイドライン(JESRA　TR-0034*B)がベースとなっている
    ISO TS11633-1/TR11633-2の改定提案

注目の国際規格例

ISO関連

- ISO 17090-4：日本提案、デジタル署名に関する規格。改訂作業中
- ISO 17090-5：日本提案、PKI資格情報を使用した認証。2017年発行
- ISO/NP 27789：監査証跡。DICOM Part15、IHE ATNAとの整合性
- ISO/NP TR 21332：クラウドコンピューティング環境のセキュリティ要件とプライバシー要件
- ISO/TR 22696：パーソナルヘルスデバイスの認証に関するガイダンス
- ISO/TS 25238（安全リスク分類），ISO/TS 21547（EHRアーカイブ），ISO/NP 22697（プライバシー保護に関する原則とガイドライン）　etc.

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
- IEC 80001-1 Ed.2：医療機器やヘルスソフトウエアのリスクマネジメント規格
- IEC 62304 Ed.2：ソフトウェアのライフサイクルプロセス規格
- ISO 14971:2019：医療機器リスクマネジメント規格　etc.

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とは

- JAHISセキュリティ委員会との合同WGで作成、JESRA化及びISO化
  JESRA TR-0034、ISO/TS11633-1 / TR11633-2
- 現在、Ver.3.0(JESRA TR-0034*B)
  - 医療機関内の情報機器・システムを遠隔保守するケースのモデル化
  - ISMSの手法に従ったリスクマネジメントの実施例を提示
- Ver.3.0の内容をISOに反映作業中。改定に伴いPart1はTS化
  - TS11633-1は発行済み（ISO/TS11633-1:2019）
  - TR11633-2はDTR投票通過、2021年2月出版完了。

※国際的にも評価の高い規格であり、改定作業と並行して周知活動を予定

- ✓ **ISO/TS 11633-1** Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis （要件とリスク分析）
- ✓ **ISO/TR 11633-2** Part 2: Implementation of an information security management system (ISMS) （ISMSの実装）

JIRA-JAHIS合同開示説明書WG(MDS-WG)

「製造業者による医療情報セキュリティ開示書」ガイドとは

- JAHIS-JIRA合同開示書WGにて、2013年4月に初版発行
  現在Ver.3.0a （JAHIS標準およびJESRA）
  ※安全管理ガイドライン第5.1版対応のMDS Ver.4.0版を準備中
- 製造業者による医療情報セキュリティ開示書の英文の略

  Manufacturer Disclosure Statement for Medical Information Security
- 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することを目的
- MDSを利用することの利点
  - 医療機関が製造業者にセキュリティ機能の説明を求める際の要求書式
  - 医療機関にとって、リスクアセスメントの材料
  - 医療機関にとって、必要な運用的対策の理解が容易に
  - 製造業者にとって、安全管理ガイドラインへの適合性の自己評価手段

MDS-WGの活動

- **20年度の活動内容**

- MDS改定作業（MDS4.0版）
  - サービス事業者向けの開示説明書(SDS)の追加
  - 医療情報システムの安全管理に関するガイドライン第5.1版への対応
- Q&Aの見直し作業（各種セミナーでの意見反映）
- MDSのHELICS申請：MDS改訂版で手続き予定
- 周知活動
  - 2020.8.20　MDS書き方セミナー（JAHISオンラインセミナー）

SPC MDS2対応

MDS2：セキュリティのためのコミュニケーションツール

◆ MDS2は、医療機器製造業者（MDM）と医療提供者（HDO）である機器の所有者/オペレーターの間のコミュニケーションツールとして使用され、潜在的なセキュリティリスクと機能に関連する医療機器に関する技術情報を提供する機器固有の医療機器セキュリティの製造業者開示説明書。

◆ MDS2は、「M-D-S-squared」または「M-D-S-two」と発音。

◆ MDS2の進化：各種セキュリティ要件の取込みによる設問拡大。

- ✓ MDS2-2004（41設問）⇒ MDS2-2013（83設問）⇒ MDS2-2019（240設問）

◆ MDS2-2019の開発

- ✓ 技術的範囲の拡大：セキュリティ管理に関する詳細
- ✓ 包括的なリスクビュー：コンテンツはあらゆる種類のセキュリティリスクを考慮
- ✓ より広範な参加：MITA、MDM、HDO、FDA、その他の利害関係者
- ✓ ソフトウェアの透明性：ソフトウェア部品表（SBoM）に対応
- ✓ ソフトウェアサポート：ソフトウェアアップデートの詳細

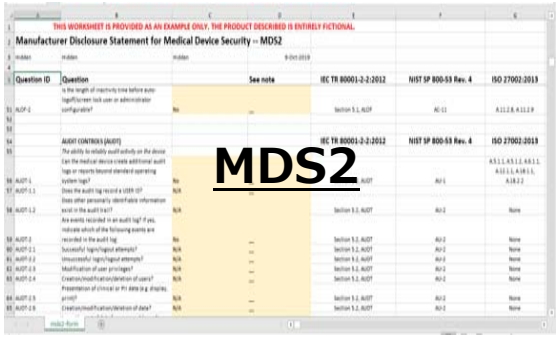
SPC MDS2対応

MDS2：2013版と2019版との比較（設問83⇒240に拡大）

MDS2-2013		MDS2-2019		増減	大幅改定	改訂ポイント(MDS-2019 4.2 Change to question 記載より)
DOC	0	DOC	15	15	○	
MOPD	22	MPII	22	0		用語集の例が更新され、ウェアラブルなどの新しいタイプのデバイスに対処するための質問が拡張されました。 ALOF近接デバイスなどの新しい自動ログオフテクノロジが追加されました。
ALOF	3	ALOF	2	-1		近接デバイスのような新しい自動ログオフテクノロジが追加されました。
AUDT	10	AUDT	30	20	○	1）APIアクセスとデータアクセスの詳細、2）時刻同期、および3）監査ファイルのインポート/エクスポートに対処するための質問が追加されました。リモートサービスはRMOTに移動しました。
AUTH	3	AUTH	8	5		認証タイプの説明が更新されました。
CSUP	2	CSUP	34	32	○	このセクションは大幅に修正されました。更新権限と機能に関する詳細が含まれています。
DIDT	1	DIDT	2	1		利用可能な非識別標準プロファイルへの準拠についての質問が追加されました。
DTBK	1	DTBK	6	5		患者情報以外のデータのカテゴリに対処するために、さらに質問が追加されました。たとえば、システム構成情報のバックアップが含まれます。
EMRG	1	EMRG	1	0		大きな変化なし
IGAU	1	IGAU	2	1		大きな変化なし
MLDP	6	MLDP	15	9		1）どの機能を実行できるか、2）ログおよび通知の対処方法、3）ネットワークプローブの対処方法、および4）ホワイトリストがサポートされているかどうかについての質問が追加されました。
NAUT	1	NAUT	4	3		アクセス制御機能についての質問が追加されました。
		CONN	19	19	○	接続機能について尋ねるために新しいセクションが追加されました。
PAUT	8	PAUT	16	8		多要素認証機能に関する質問が追加されました。
PLOK	1	PLOK	4	3		より多くの種類のロックと物理的な制御に関する質問が追加されました。
RDMP	1	RDMP	4	3		ソフトウェアロードマップについて尋ねるために新しいセクションが追加されました。
		SBOM	8	8		ソフトウェア部品表について質問するための新しいセクションが追加されました。
SAHD	11	SAHD	22	11	○	システムの検証、サイトの設定、およびアップデートプロセスの詳細についての質問が追加されました。
SGUD	2	SGUD	5	3		アクセス制御についての質問が追加されました。
STCF	1	STCF	7	6		質問が修正され、より多くのカテゴリーの詳細が含まれるようになりました。
TXCF	3	TXCF	6	3		デバイス認証に関する質問が追加されました。
TXIG	1	TXIG	2	1		
		RMOT	6	6		リモートサービスと管理機能について尋ねるために新しいセクションが追加されました。
OTHR	3	OTHR		-3		デバイスの製造元に関する追加情報のプレースホルダーとして新しいセクションを追加しました。
CNFS	1			-1		このセクションは、ALOF、AUTH、CVSUP、MLDP、NAUT、PAUT、SAHD、およびSGUDを含む他のカテゴリに含まれている、顧客設定管理に関する質問と質問です。
合計	83	合計	240	157		

SPC MDS2対応

MDS2：リスクアセスメントプロセスでのMDS2の使用


THIS WORKSHEET IS PROVIDED AS AN EXAMPLE ONLY. THE PRODUCT DESCRIBED IS ENTIRELY FICTIONAL.

Manufacturer Disclosure Statement for Medical Device Security – MDS2

MDS2

リスクアセスメント

- **リスク分析**は、危険を特定し、リスクを推定するために利用可能な情報を体系的に使用すること。
- **リスク評価**は、推定されたリスクを所定のリスク基準と比較して、リスクの受容可能性を判断するプロセス

リスク対策/緩和は、リスクが特定のレベルに低減または維持されるように、決定が行われ、対策が実行されるプロセス

リスク監視とは、リスクを低減するか、指定された制限内にリスクを維持するためのリスク管理努力の効果を継続的に監視するプロセス

フィードバックループ

DICOM WG14対応

DICOM WG14(Security)で、DICOM委員会と共同で対応中。

【セキュリティに関わる主なDICOM規格案件】

- DICOM Part 15 への SAFE Profile の追加検討
  SAFE Identity（ヘルスケアにおけるデジタルIDと暗号化の認証機関）WG-14でこの証明書を用いたプロファルの策定について検討中。
- Supplement 211: DICOM web retrieve via ZIP（WG-27）
  DICOMweb Query で検査画像セットをZIP 圧縮して取得する。PS 3.18 “Web Service” に、8.11”Security and Privacy” の追加等。

その他

- DICOM向けのセキュリティに関するホワイトペーパーを検討中。
- NIST SP1800-24 (Securing Picture Archiving and Communication System (PACS) : PACS保護ガイダンス)の情報共有
  ※2020.12.21 Finalバージョン公開

医療機器のサイバーセキュリティの取り組み

諸外国のサイバーセキュリティガイダンスの制定状況

発行日	国名	管轄組織	題目	制定
2016/12/28	米国	FDA	産業および食品医薬品局のスタッフ向けの医療機器ガイダンスにおけるサイバーセキュリティのポストマーケット管理	Final
2018/7/24	日本	厚生労働省	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	Final
2018/10/18	米国	FDA	医療機器のサイバーセキュリティ管理に関する市販前申請の内容 ※再改訂準備中、2021年ドラフト公開予定	Draft
2018/11/13	ドイツ	BSI	BSI-CS 132 ネットワークに接続された医療機器のサイバーセキュリティ要件	Final
2019/6/26	カナダ	Health-Canada	医療機器のサイバーセキュリティに関する市販前のドラフトガイダンス文書	Final
2019/7/18	オーストラリア	TGA	産業用医療機器サイバーセキュリティガイダンス	Final
2019/7/19	フランス	ANSM	ライフサイクルを通してソフトウェアを統合した医療機器のサイバーセキュリティ	Draft
2020/4/20	国際医療機器規制当局フォーラム	IMDRF（International Medical Device Regulators Forum）	医療機器サイバーセキュリティの原則及び実践（IMDRFガイダンス）	Final

- 2017年に世界規模の被害が発生したランサムウェア「WannaCry」は、その後も拡散し、個人や企業、医療機関にまで被害が拡大し、**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。**
- 近年、サイバーテロの急増に伴い、**諸外国からサイバーセキュリティガイダンスが相次いで公表**されており、**IMDRF主導でグローバルなセキュリティ指標の策定が行われ、2020年4月に発出**された。
- 本委員会では、正式版ならびにドラフト版のガイダンス要件の内容把握や和訳作業を通して、**会員企業に対して医療機器製品へのセキュリティ要件情報（詳細、和訳）の共有と周知活動**を行っている。

医療機器のサイバーセキュリティの取り組み

我が国における医療機器のサイバーセキュリティへの取り組み

- **「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：2015年）**⇒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要求。**
- **「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：2018年）**⇒**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。**
- **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**2020年4月に取りまとめられた。**
- **「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日付け薬生機審発0513第1号、薬生安発0513第1号：2020年）**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開始**している。
- **国内での普及・推進活動として、医機連で医療機器サイバーセキュリティ対応WG発足。**
  JIRA（医用画像システム部会セキュリティ委員会、法規安全部会）からWGメンバーとして参画し、IMDRFガイダンス導入の検討を行っている。

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

- Principles and Practices for Medical Device Cybersecurity（IMDRF）
  ※IMDRFガイダンス、2020.4.20発出
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Draft Guidance (US)
- BSI-CS 132 Cyber Security Requirements for Network-Connected Medical Devices（DE）
- Pre-market Requirements for Medical Device Cybersecurity Guidance (CA)
- Medical device cyber security guidance and information for consultation (AU)
- Cybersecurity of medical devices integrating software during their life cycle Draft(FR)
- 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（厚労省通知）
- 医療情報システムの安全管理に関するガイドライン第5.1版（厚労省）※2021.1.29発出
- 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 (総務省＋経産省) ※2020.8.21発出

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改定作業班への参画（JIRA/JAHIS/JEITA）
- 事業者向け3省2ガイドライン策定作業（JAHIS/JEITAとの協調・連携）
- IMDRF 医機連サイバーセキュリティ対応WGへの参画（JIRA/JEITA）

21年度の活動方針

- ISO TC215については、WG4及びJWG7対応も含め、継続的に活動を続ける。
- RSS-WGに関しては、ISO規格改定だけで無く、周知活動にも力点を置くようにする。
- MDS-WGに関しては、製造業者やサービス事業者の周知活動だけで無く、医療従事者（医師、放射線技師など）への周知活動を継続する。
- IMDRFガイダンスをベースにした日本版サイバーセキュリティ手引書の策定作業や周知活動により、会員企業のサイバーセキュリティへの取り組みを推進する。
- DICOM　WG14については、セキュリティ関連の案件が増加傾向にあるため、継続的にDICOM委員会と共同で進める。
- 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。