2019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　葉賀　功

2020/02/21 医用画像システム部会 成果報告会

報告内容

- 19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
  - 各国のサイバーセキュリティガイダンス対応
  - その他
- 20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

- 年２回開催されている会議へISOエキスパートを派遣
  - 2019年4月　イエテボリ（SE）　　1名
  - 2019年11月　韓国テグ（KR）　　1名
  - 2020年4月　ワシントンDC（US）　調整中
- 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, ISO/TS 21547, ISO/NP 22697　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
  - TS11631-1は発行済み（ISO/TS11633-1:2019）
  - TR11633-2はコメント処理完了、DTR投票通過

※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
- 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

● 19年度の活動内容

- MDS改定作業

  サービス事業者向けの開示説明書(SDS)の追加作業検討中

- 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：手続き中
- 周知活動
  - 2019.4　　ITEMちらし配布（医療機関向け）
  - 2019.6.10　MDS解説（JAHISセキュリティセミナー）
  - ~~2020.3.05　MDS書き方セミナー（JAHIS合同セミナー）~~

SPC MDS2対応

MDS2とは

- ANSI/NEMA規格
- 正式名：Manufacturer Disclosure Statement for Medical Device Security
- 現在のバージョン：　ANSI / NEMA HN 1-2019　（2019年10月発行）
- 医療機器のセキュリティ問題の管理におけるセキュリティリスクアセスメントを担当する専門家を支援するためのチェックシートとガイド。
- MDS-WGのMDSチェックリストもMDS2形態を参考にしている。
- 2019年版は、2013年版を基に改訂。新たにSBOM（ソフトウェア部品表）を含む6カテゴリーの設問が追加された。（81⇒216設問）
- サイバーセキュリティ慣行：（例：ISAO加盟 / ISACへの脆弱性の開示）
- IEC/TR 80001-2-2:2012 セキュリティ機能を確立するためのガイダンス、各セキュリティ機能に対処し、プロバイダーのセキュリティ制御オプションの特定
- FDA市販前サイバーセキュリティガイダンス(案)やIMDRFガイダンス(案)でも参照されている、グローバルな技術文書。

MDS2-2019版の構成

IEC 80001-1で医療機器に要求されるリスクマネジメントを行うための規格
IEC/TR 80001-2-2カテゴリ（18項目）＋新項目：RMOT、SBOM、CONN、RDMP、MPII、OTHR

IEC TR80001-2-2:2012セクション	IEC TR80001-2-2 2012名称	2019年版 MDS2カテゴリ	Item Name	コメント
5.1	ALOF	**ALOF**	Automatic Logoff	
5.2	AUDT	**AUDT**	Audit Controls	
5.3	AUTH	**AUTH**	Authorization	
5.4	CNFS	**--**	CONFIGURATION OF SECURITY FEATURES	ユーザ設定の質問をSAHD、SGUD、CSUP、PAUTに移動
5.5	CSUP	**CSUP**	Cybersecurity Product Updates	
5.6	DIDT	**DIDT**	Health Data De-Identification	
5.7	DTBK	**DTBK**	Data Backup And Disaster Recovery	
5.8	EMRG	**EMRG**	Emergency Access	
5.9	IGAU	**IGAU**	Health Data Integrity and Authenticity	
5.10	MLDP	**MLDP**	Malware Detection/Protection	
5.11	NAUT	**NAUT**	Node Authentication	
5.12	PAUT	**PAUT**	Person Authentication	
5.13	PLOK	**PLOK**	Physical Locks	
5.14	SAHD	**SAHD**	System and Application Hardening	
5.15	SGUD	**SGUD**	Security Guides	
5.17	STCF	**STCF**	Data Storage Confidentiality	
5.18	TXCF	**TXCF**	Transmission Confidentiality	
5.19	TXIG	**TXIG**	Transmission Integrity	
--	--	**RMOT**	Remote Service	リモートサービスおよび管理に関する質問を追加（新規）
--	--	**SBOM**	Software Bill of Materials	ソフトウェア部品表の質問を追加（新規）
--	--	**CONN**	Connectivity Capabilities	接続能力を追加（新規）
--	--	**RDMP**	Roadmap for Third-Party Applications and Software Components in Device Life Cycle	ソフトウェアロードマップの質問を追加（新規）
--	--	**MPII**	Management of Personally Identifiable Information	個人識別可能情報に関する質問の管理を拡大
--	--	**OTHR**	Other Security Considerations	他の場所に分類されていないセキュリティリスクの考慮事項または管理（補完的管理策を含む）を製造業者が入力（新規）

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】

CPack-104（CP 35件中、セキュリティ案件の以下4件）

- CP1942 Revise Part 15 Annex F (DHCP)
  DDNS(Dynamic DNS)の解説の明確化など。
- CP1946 Update Part 15 Annex H (add conformance)
  参照RFCの見直しや、DNSのサポートについてのConformance Statementへの記載要求等
- CP1947 Add security considerations for encapsulated formats
  Encapsulated Format についてのセキュリティ考慮事項の追記
- CP1948 Part 10 Format security considerations
  DICOM Part 10フォーマットについてのセキュリティ考慮事項の追記

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検討中。
- NIST SP1800-24 (Securing PACS：PACS保護ガイダンス)の情報共有

サイバーセキュリティガイダンス対応

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	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
2019/10/1	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	Draft

- 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**が進められており、策定動向を継続・注視している。
- 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。

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 Draft（IMDRF）
- 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版（厚労省）
- クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第 1 版(総務省)
- 医療情報を受託管理する情報処理事業者における安全管理ガイドライン（経産省）

他工業会との協調・連携活動

- 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）
- 安全管理ガイドライン改定作業班への参画（JIRA/JAHIS/JEITA）
- IMDRF 医機連サイバーセキュリティWGへの参画（JIRA/JEITA）

20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）への周知も検討する。
- MDS2の2019年度版に関しては、医療機器輸出企業への周知活動により、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。

ご清聴、ありがとうございました。