2018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

報告内容

- 18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
  - その他

- 19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エキスパートを派遣
  - 2018年4-5月　マリンガ(BR)　0名
  - 2018年11月　パエストゥム(IT)　0名
  - 2019年4月　イエテボリ(SE)　1名（予定）
- 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 17090-4
  - 日本提案、デジタル署名に関する。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健康に関するセキュリティ要件とプライバシー要件。エキスパートメンバーにノミネート
- ISO/NP 22696
  - スマートフォンの利用も含めた小型デバイス向けのガイダンス
- ISO/TS 25238,ISO/TS 21547,ISO/NP 22697　etc.
- JWG7関連
  ISO 81001-1,IEC80001-1 Ed.2,IEC 62304 Ed.2　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 TR11633-1/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DTSのコメント処理が終了、まもなく公開予定
  - TR11633-2は次回TC215/WG4会議でディスカッション開始予定

※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
- ✓ ISO/TR 11633-2 Part 2: Implementation of an information security management system (ISMS)

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

○18年度の活動内容

- MDS Ver.3.0a JESRA版の発行（JIRAホームページ公開）
- Q&Aの見直し作業（各種セミナーでの意見反映）
- 医療機関向けのMDS説明資料を準備中
- 周知活動
  - 2018.4　　ITEMちらし配布
  - 2018.5.30　MDS解説（医療機器のサイバーセキュリティセミナー）
  - 2018.6.11　書き方セミナー（JAHIS技術標準セミナー）
  - 2018.10.07　MDS解説（中四国医療情報学研究会）
  - 2018.11.09　書き方セミナー（JAHIS合同セミナー）

SPC MDS2対応

MDS2とは

- HIMSS/NEMA規格
- 正式名：Manufacturer Disclosure Statement for Medical Device Security
- 現在のバージョン： HN 1-2013(リリース版：HN 1-2008)
- 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のチェックリストも形態を参考にしている。
- 現行版はIEC/TR 80001-2-2に準拠している。

- 現在、MDS2の改訂作業が進行中。
  セキュリティ委員会からVoting memberとして参加。下記のコメントを提出し、全てAccept。まもなく、改訂版が公開される見込み。
  - ISO TS11633-1/TR11633-2のReferenceへの追加
  - エディトリアルな語句修正（7項目）

MDS2対応　IEC 80001-2-2

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はセキュリティ機能を下記1-19の項目に分類し、
リスクマネジメントを行うための技術文書

1. ALOF　自動ログオフ
2. AUDT　監査コントロール
3. AUTH　認証
4. CNFS　セキュリティ機能の構成
5. CSUP　セキュリティ製品のアップグレード
6. DIDT　健康データの匿名化
7. DTBK　データのバックアップと災害復旧
8. EMRG　緊急アクセス
9. IGAU　健康データの完全性と真正性
10. MLDP マルウェアの検出/保護
11. NAUT　ノード認証
12. PAUT　個人の認証
13. PLOK　物理的ロック
14. RDMP　機器のライフサイクルにおける3rdパーティ製コンポーネントのロードマップ
15. SAHD　システムとアプリケーションの堅牢性
16. SGUD　セキュリティガイド
17. STCF　健康データストレージの機密性
18. TXCF　送信の機密性
19. TXIG　送信の完全性

IEC 80001-1：Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities
IEC/TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls

DICOM WG14対応

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

日本のCRYPTRECで推奨している暗号スイーツ（12種類）の追加を要望し、Supplement206で下記内容が受け入れられた。
（DICOM2018eで反映）

- Supplement206
  規格書PS3.15の「B.11 Extended BCP195 TLS Profile Secure Transport Connection Profile」として追加。
  - 12種類の暗号スイーツの追加
  - 鍵長はDHE:2048bit以上、ECDHE:256bit以上

その他

・TLSとACME（Automatic Certificate Management Environment）を使ったセキュアなDICOM通信を検討中。

・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。

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

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Draft Guidance (US)
- Pre - market Requirements for Medical Device Cybersecurity Draft Guidance (CAN)
- Medical device cyber security Draft guidance and information for consultation (AU)
- Medical Device Cybersecurity Act of 2017：審議中(US)
- 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）
- 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）
- etc.

19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へ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の改訂に関して国内企業の不利益が発生しないように継続して参加、必要に応じてコメントを行っていく。
- DICOM　WG14についてはSupplement206以降も対応が必要な可能性が高く、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。