2017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　五十嵐　隆史

報告内容

- 17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)
  - 「※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版対応

    ※以下、安全管理GLと表記
  - JIRA- JAHIS合同開示説明書WG(MDS-WG)
  - SPC MDS^{2}対応
  - DICOM WG14対応
  - その他
- 18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
  - 2017年5月　杭州(CN)　1名
  - 2017年11月　リバプール(UK)　0名
  - 2018年4-5月　マリンガ(BR)　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 17090-4
  - 日本提案、デジタル署名に関する。要件追加のため早期SR
- 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.

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
  - TS11633-1がDTS投票を通過
  - TR11633-2のディスカッション・ペーパー準備中

※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/TR 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)

安全管理GL対応

- 5月30日　安全管理GL　第5版発行

医療機関等を対象とするサイバー攻撃、地域医療連携や医療介護連携等の推進、IoT 等の新技術やサービス等の普及への対応と、改正個人情報保護法等への対応

#	改訂内容
1	電子カルテの代行入力を時間経過で自動確定することへの言及
2	「製造業者による情報セキュリティ開示書」ガイドへの言及
3	モバイルデバイスへの対応
4	標的型攻撃への対応
5	TLS1.2によるオープンネットワーク接続への言及
6	第5版の改定内容に沿って付表を更新
7	医療情報システムの対象範囲の検討
8	IoTセキュリティへの対応
9	2要素認証の採用
10	電子署名の採用

・JIRAワークショップでの講演(10月)
・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　の改訂

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(JESRAは発行準備中)
- 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

TOPICS:
安全管理GL第5版で以下の記載がされ、安全管理GLでも有用性が認められた

なお、情報システムで扱われている情報のリストアップやリスク分析及び対策において、その装置のベンダから技術的対策等の情報を収集することが重要である。その際、JAHIS標準及び日本画像医療システム工業会規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」で示されている「製造業者による医療情報セキュリティ開示書チェックリスト」が参考になる。

○17年度の活動内容

- 安全管理GL第5版が発行され、改定内容に対する見直し
- 前バージョンで発見された問題の修正
- チェックシートのExcel化
- Q&Aの発行
- 周知活動　書き方セミナーの開催、ちらしの見直し

※周知活動は今後の18年度の主軸となる予定

MDSのQ&A

「製造業者による医療情報セキュリティ開示書」ガイド　Ver.3.0a

に関するQ&A

（「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」対応）

平成３０年１月

JAHIS -JIRA 合同開示説明書WG

目次

はじめに

本書は「製造業者による医療情報セキュリティ開示書」（以下、MDSとする。）関連セミナー」で寄せられた質問を中心にまとめたものです。

※Qにおける「質問n」の”n”はMDS Ver.3.0aにおける番号を指します。
※本書では厚生労働省の「医療情報システムの安全管理に関するガイドライン」を「安全管理ガイドライン」と記します。
※本書並びに本書に基づいたシステムの導入・運用についてのあらゆる障害や損害について、本書作成者は何ら責任を負わないものとします。

「全体」

Q1．ある病院様より「弊社より納入した医療情報パッケージシステムは、医療情報システムの安全管理に関するガイドラインに対応しているのか？」と回答を求められています。
本ガイドラインについては、どこまでがパッケージシステムに該当し、対応可否の回答をすれば良いのかが判別できない状況にいます。
「製造業者による医療情報セキュリティ開示書」ガイドに「5.2 チェックリスト（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版対応）」がありますが、本チェックリストにある項目が、医療情報システムの安全管理に関するガイドラインの中でパッケージシステムとして対応可否の回答をすべき事項が全て網羅されており、それ以外の項目はパッケージシステムとして関係が無く、対応可否の回答をせずとも良いとの考えで宜しいのでしょうか。

A1．まず大前提ですが「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）に対応すべき対象は、システムベンダーやその医療情報システムではなく医療機関等であるということです。
医療機関等で誤解されている場合があるのですが、医療情報システムが安全管理ガイドラインに対応するのではなく、医療機関等がシステムの持つ機能（技術的対策）とそれに相応した運用的対策を組み合わせて安全管理ガイドラインに対応するものです。必ずしも技術的対策が必須となる訳ではありません。

「製造業者による医療情報セキュリティ開示書」（以下「MDS」と略す。）では安全管理ガイドラインのC項「最低限のガイドライン」の中で、製造業者が提供する個々の医療情報システムの持つ機能（技術的対策）に関して抜粋したものとなっています。
そのため、「MDS」のチェックリストに御社のシステムについて回答したものを提出されれば、基本的には質問された病院様のニーズに応えた事になると思われます。
しかしながら、「MDSの全項目を回答すれば他は考慮しなくてよい」とは言えません。

1

セミナーでの質疑応答や、メールでの問い合わせを元に作成。
必要に応じて適宜更新する。

チェックシートの改善

製造業者による医療情報セキュリティ開示書　チェックリスト　第２版

製造メーカ　：XYZ 株式会社	作成日　：2016 年 1 月 26 日
製品名称　：General-PACS	バージョン　：V1.20R00

医療機関における情報セキュリティマネジメントシステムの実践（6.2）				
1　扱う情報のリストを提示してあるか？（6.2.C1）	(はい)	いいえ	対象外	備考 1
物理的安全対策（6.4）				
2　覗き見防止の機能があるか？（6.4.C5）	はい	(いいえ)	対象外	備考 2
技術的安全対策（6.5）				
3　不正入力防止の機能があるか？（6.5.C3）	(はい)	いいえ	対象外	備考 3
4　アクセス管理の機能があるか？（6.5.C1、6.5.C5）	(はい)	いいえ	対象外	備考
4．1　アクセス管理の認証方式は？（6.5.C1）				
・パスワード認証	(はい)	いいえ	対象外	備考
・生体認証	(はい)	いいえ	対象外	備考 4
・物理媒体認証	はい	(いいえ)	対象外	備考
・二要素認証	はい	(いいえ)	対象外	備考
・その他（具体的な方法を備考に記入してください）	はい	(いいえ)	対象外	備考
4．1．1　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C10-1～6.5.C10-3）	はい	(いいえ)	対象外	備考 5
4．2　アクセスログを出力する機能があるか？（6.5.C6）	(はい)	いいえ	対象外	備考
4．2．1　アクセスログを利用者が確認する機能があるか？（6.5.C6）	はい	(いいえ)	対象外	備考 6
4．2．2　アクセスログへのアクセス制限が出来るか？（6.5.C7）	(はい)	いいえ	対象外	備考
5　時刻情報の正確性を担保する仕組みがあるか？（6.5.C8）	(はい)	いいえ	対象外	備考 7
6　不正ソフトウェア対策を行っているか？（6.5.C9）	(はい)	いいえ	対象外	備考 8
7　無線 LAN を利用する場合のセキュリティ対策機能はあるか？（6.5.C.11）	はい	(いいえ)	対象外	備考 9
情報および情報機器の持ち出しについて（6.9）				
8　ソフトウェアのインストールを制限する機能があるか？（6.9.C9）	はい	(いいえ)	対象外	備考 10
9　外部入出力装置の機能を無効にすることができるか？（6.9）	はい	(いいえ)	対象外	備考 11
10　管理区域外への持ち出しの際、起動パスワード等のアクセス制限を設定できるか？（6.9.C6、6.9.C7）	はい	いいえ	(対象外)	備考

チェックリスト（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版対応）

作成日	2018年1月15日
製造業者	JIRA株式会社
製品名称	General-PACS
バージョン	Ver1.20

						回答欄		
						プルダウン選択（はい/いいえ/対象外）	備考番号の入力(数字)	
医療機関における情報セキュリティマネジメントシステムの実践（6.2）								
1　扱う情報のリストを提示してあるか？（6.2.C1）	はい	いいえ	対象外	備考	1	1. はい	1	
物理的安全対策（6.4）								
2　覗き見防止の機能があるか？（6.4.C5）	はい	いいえ	対象外	備考	2	2. いいえ	2	
技術的安全対策（6.5）								
3　離席時の不正入力防止の機能があるか？（6.5.C4）	はい	いいえ	対象外	備考	3	1. はい	3	
4　アクセス管理の機能があるか？（6.5.C1）	はい	いいえ	対象外	備考	-	1. はい	-	
4．1　アクセス管理の認証方式は？（6.5.C1）								
・記憶(ID・パスワード等)	はい	いいえ	対象外	備考	-	1. はい	-	
・生体認証(指紋等)	はい	いいえ	対象外	備考	4	1. はい	4	
・物理媒体（ICカード等）	はい	いいえ	対象外	備考	-	2. いいえ	-	
・その他（具体的な方法を備考に記入してください）	はい	いいえ	対象外	備考	-	2. いいえ	-	
・上記のうちの二要素を組み合わせた認証	はい	いいえ	対象外	備考	-	2. いいえ	-	
4．1．1　パスワードを利用者認識手段として利用している場合、パスワード管理は可能か？（6.5.C11(1)～6.5.C11(3)）	はい	いいえ	対象外	備考	5	2. いいえ	5	
4．1．2　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？（6.5.C3）	はい	いいえ	対象外	備考	-	1. はい	-	
4．2　利用者別、職種別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考	-	1. はい	-	
4．3　アクセス記録(アクセスログ)機能があるか？（6.5.C7）	はい	いいえ	対象外	備考	6	2. いいえ	6	
4．3．1　アクセスログを利用者が確認する機能があるか？（6.5.C7）	はい	いいえ	対象外	備考	-		-	
4．3．2　アクセスログへのアクセス制限が出来るか？（6.5.C8）	はい	いいえ	対象外	備考	-		-	
5　時刻情報の正確性を担保する仕組みがあるか？（6.5.C9）	はい	いいえ	対象外	備考	7	1. はい	7	
6　不正ソフトウェア対策を行っているか？（6.5.C10）	はい	いいえ	対象外	備考	8	1. はい	8	
7　無線LAN を利用する場合のセキュリティ対策機能はあるか？（6.5.C.12）	はい	いいえ	対象外	備考	9	2. いいえ	9	
情報および情報機器の持ち出しについて(6.9)								
8　ソフトウェアのインストールを制限する機能があるか？（6.9.C9）	はい	いいえ	対象外	備考	10	2. いいえ	10	
9　外部入出力装置の機能を無効にすることができるか？（6.9）	はい	いいえ	対象外	備考	11	2. いいえ	11	
10　管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能もしくは暗号化機能があるか？（6.9.C6、6.9.C7）	はい	いいえ	対象外	備考	-	3. 対象外	-	
災害、サイバー攻撃等の非常時の対応(6.10)								
11　非常時機能又は、非常時アカウントを持っているか？（6.10.C3）	はい	いいえ	対象外	備考	12	2. いいえ	12	
外部と個人情報を含む医療情報を交換する場合の安全管理(6.11)								
12　「外部と個人情報を含む医療情報を通信する機能」や「リモートメンテナンス機能」を有するか？（6.11.C1）	はい	いいえ	対象外	備考	13	1. はい	13	
12．1　なりすましの対策(認証)機能を有するか？（6.11.C3）	はい	いいえ	対象外	備考	-	1. はい	-	
12．2　データの暗号化(SSL/TLS、S/MIME、ファイル暗号化など)が可能か？（6.11.C5）	はい	いいえ	対象外	備考	-	1. はい	-	
12．3　ネットワークの経路制御・プロトコル制御に関わる機能を有しているか？（6.11.C4）	はい	いいえ	対象外	備考	14	2. いいえ	14	
12．3．1　ネットワークの経路制御・プロトコル制御に関わる機能は、安全管理ガイドラインを満たす設定が可能か？（6.11.C4）	はい	いいえ	対象外	備考	-		-	
12．3．1．1　対応している通信方式はいずれか？（6.11.C4、C10）								
・専用線	はい	いいえ	対象外	備考	-		-	
・公衆網	はい	いいえ	対象外	備考	-		-	
・IP-VPN	はい	いいえ	対象外	備考	-		-	
・IPsec－VPN	はい	いいえ	対象外	備考	-		-	
・TLS1.2 高セキュリティ型、クライアント認証	はい	いいえ	対象外	備考	-		-	
12．3．2　ネットワークの経路制御・プロトコル制御に関わる機能の適正さ(図り込み対策を含む)を証明できる文書があるか？（6.11.C4、C10）	はい	いいえ	対象外	備考	-		-	
12．4　リモートメンテナンス機能を有するか？（6.11.C7）	はい	いいえ	対象外	備考	13	1. はい	13	
12．4．1　リモートメンテナンスサービスに関し、不必要なリモートログインを制限する機能があるか？（6.11.C7）	はい	いいえ	対象外	備考	-	1. はい	-	

※YYYY/MM/DD
※文字列
※文字列
※文字列

チェックシートをWORDからExcelにし、見易く、比較が行い易いように変更

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、リビジョンの作業が進行中。セキュリティ委員会からVoting memberとして参加し、コメントの提出を実施

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 Web Services（PS3.18）が長いこと更新されておらず、セキュリティ項目の見直しが必要となり、WG14(Security)が再開され、DICOM委員会と共同で対応を開始。Supplement204が提案された。

- Supplement204での注目点
  - TLS1.0/1.1/1.2対応
    - TLS1.2　高セキュリティモードのみ利用可能とする
    - 利用可能な4つの暗号スイーツの定義
  - コメント内容
    - ISCL protocolの廃止提案
    - CRYPTREC推奨暗号スイーツの追加要望

CRYPTRECの追加は受け入れられなかったがSupplement206として継続案件となり対応中。

Supplement204はコメント付きでLB通過。

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

- SFDAより医療機器ネットワークセキュリティ登録技術審査ガイドラインを発布する通告(中国)
- Medical Device Cybersecurity Act of 2017 (US)
- 欧州医療機器規制　Medical Device Regulation [MDR] (EU)
- 改正個人情報保護法(日本)
- SECURING PICTURE ARCHIVING AND COMMUNICATION SYSTEM (PACS) Cybersecurity for the Healthcare Sector(NIST)
- NEMA Cybersecurity Hygiene Document (CYHG 1-2018)
- JIRAワークショップで安全管理GL第5版に関する講演(10月)
- JART12月号への執筆「外部保存(3省4ガイドライン)について」
- etc.

18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、放射線技師・Drへの周知も検討する
- MDS^{2}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。