

2009年度セキュリティ委員会 活動報告

セキュリティ委員会 委員長
西田慎一郎

2009年度活動内容

- 1) ISO/TC215 WG4(セキュリティ)で検討されている国際標準への対応について
- 2) 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」に対するベンダとしての取り組みについて
- 3) NEMA、COCIRと共同してのグローバルな医療機器セキュリティへの取り組みについて

1) ISO/TC215 WG4(セキュリティ)で検討されている国際標準への対応について

- 年2回開催されている会議へ2名派遣
 - 2008年10月 トルコ・イスタンブール
 - 2009年4月 英国・エジンバラ
 - 2009年10月 米国・ダーラム(予定)
- 規格検討への積極的な参加
 - ドラフトの内容検討、JIRAとしての意見集約
- 日本から規格提案
 - リモートサービスセキュリティ

1) ISO/TC215 WG4(セキュリティ)で検討されている国際標準への対応について

■ リスクマネジメント関連

- TS29321:Application of clinical risk management to the manufacture of health software
- TR29322:Guidance on the use of risk management to ensure the patient safety of health software systems in deployment and use

■ EHR関連

- TS13606-4:Electronic health record communication — Part 4: Security

■ インフラ関連

- TS21547:Security Requirements for Archiving of Electronic Health Records
- IS27789:Audit trails for electronic health records

■ 日本からの提案

- TR11633:Guideline for secure remote services for health systems
- TR11636:Dynamic on-demand virtual private network for health information infrastructure

ISO/TC215 WG4

リスクマネジメント関連

- TS29321:Application of clinical risk management to the manufacture of health software
 - ソフトウェア製造者向けのリスクマネジメントの適用
 - 設計、開発、改良ごとにリスクマネジメントを行い、文書化し、要求に応じて開示することを規定
 - 開発ベンダに対し追加の負担を要求するものであり、米独と協力し反対
 - 投票結果、反対多数で否決
- TR29322:Guidance on the use of risk management to ensure the patient safety of health software systems in deployment and use
 - ソフトウェア利用者向けの患者安全確保のためのリスクマネジメントのガイダンス
 - 上記規格が廃案となったため、本規格も廃案へ

ISO/TC215 WG4

EHR関連

■ TS13606-4:Electronic health record communication – Part4:Security

- CEN(欧州標準化団体)で策定された5つからなるEHRの交換に関する規定の内、セキュリティに関するもの
- ヨーロッパでは国別にEHRの保存や利活用が推進されており、その交換の標準化が急務な課題
- 利用者認証、権限管理、アクセスコントロール、監査証跡などを含む
- 他のISO規格との整合性を検討中
- 本規格に関連し、アクセスコントロールや監査証跡に用いるための「アクセスの目的の分類」規格が新たに提案されてきている

ISO/TC215 WG4

インフラ関連

- TS21547:Security Requirements for Archiving of Electronic Health Records
 - EHRの長期保存(アーカイブ)に関するセキュリティ要件
 - 投票の結果、可決された
- IS27789:Audit Trail for electronic health records
 - 監査証跡に関するセキュリティ要件
 - DICOM Sup95やIHE ATNAと同じ枠組みになる見込み
 - 現在最終ドラフトの審議中

ISO/TC215 WG4

日本からの提案

- TR11633:Guideline for secure remote services for health systems
 - リモート保守におけるセキュリティのガイドライン
 - JESRAである「リモートサービスガイド」および「ガイドライン」を英文化
 - 出版フェーズに進んでいる
- TR11636:Dynamic on-demand virtual private network for health information infrastructure
 - HEASNETのオンデマンドVPNの提案
 - 投票の結果、可決された

2) 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」に対するベンダとしての取り組みについて

■ 個人情報保護法

- －「医療画像データ内の個人情報の取扱について」通知および啓発資料の公開

■ 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 第4版」

- － 作業WGへの参加

■ 認証用HPKIポリシ

- － 作業WGへの参加

3) NEMA、COCIRと共同してのグローバルな 医療機器セキュリティへの取り組みについて

■ SPC(Security & Privacy Committee)活動

- 年1回の会議参加、意見交換

 - 2009年9月 米国・ワシントンDC

- 医療装置セキュリティに関する技術文書の作成・
公開

3) NEMA、COCIRと共同してのグローバルな医療機器セキュリティへの取り組みについて

- 医療装置セキュリティに関する技術文書の作成・公開
 - Break-Glass – An Approach to Granting Emergency Access to Healthcare Systems(緊急時アクセス)
 - Patching Off-the-Shelf Software Used in Medical Information Systems(市販ソフトへのパッチ適用)
 - Management of Machine Authentication Certificates(装置認証)
 - Information Security Risk Management for Healthcare Systems(リスクマネジメント)
 - 他

<http://www.nema.org/prod/med/spc/>

- 日本語訳をJIRAホームページで公開中

<http://www.jira-net.or.jp/commission/system/index.html>

3) NEMA、COCIRと共同してのグローバルな医療機器セキュリティへの取り組みについて

■ 医療機器セキュリティのための製造業者開示説明書 (MDS²)

- NEMA標準
- HIPAA法におけるセキュリティ規則対応のため
- 19個の質問からなるテンプレート

■ 日本語訳をJIRAホームページで公開中

<http://www.jira-net.or.jp/commission/system/index.html>

ご静聴ありがとうございました