2007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

2007年度活動内容

1）国内外のセキュリティ関連規格等への対応

2）画像医療システムに関するセキュリティ関連のガイドライン等の検討

3）画像医療システムに関するセキュリティ関連の情報収集と会員への周知

１）国内外のセキュリティ関連規格等への対応

- ISO/TC215(Health informatics) WG4 (Security)
- DICOM WG14 (Security)
- SPC(NEMA/COCIR/JIRA Joint Security & Privacy Committee)
- 個人情報保護法
- 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」

１－１）ISO/TC215 WG4 への対応

- Risk management関連
  - **Application of clinical risk management to the manufacture of health software**
  - **Guidance on the use of risk management to ensure the patient safety of health software systems in deployment and use**
- EHR関連
  - **Electronic health record communication — Part 4: Security**
- インフラ関連
  - **Security Requirements for Archiving of Electronic Health Records**
  - **Audit trails for electronic health records**
- 日本からの提案
  - **Guideline for secure remote services for health systems**
  - **Dynamic on-demand virtual private network for health information infrastructure**

ISO/TC215 WG4
リスクマネジメント関連

- **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
  - 日本でのソフトウェア薬事とも関連
- **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
  - 上記の製造者から開示される文書を用い、運用上のリスクマネジメントを行うことを推奨

ISO/TC215 WG4
EHR関連

- **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

ISO/TC215 WG4
インフラ関連

- **Security Requirements for Archiving of Electronic Health Records**
  - EHRの長期保存に関するもの
- **Audit Trail for electronic health records**
  - 監査証跡に関するもの
  - DICOM Sup95やIHE ATNAと同じ内容になる見込み

ISO/TC215 WG4
日本からの提案

- **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」を英文化し、提案
  - JAHISと共同のWGでドラフト作成中
- **Dynamic on-demand virtual private network for health information infrastructure**
  - HEASNETのオンデマンドVPNの提案

1－2）DICOM WG14 への対応

- Part 15: Security and System Management Profiles
  - SECURE USE PROFILES
  - SECURE TRANSPORT CONNECTION PROFILES
  - DIGITAL SIGNATURE PROFILE
  - MEDIA STORAGE SECURITY PROFILES
  - NETWORK ADDRESS MANAGEMENT PROFILES
  - TIME SYNCHRONIZATION PROFILES
  - APPLICATION CONFIGURATION MANAGEMENT PROFILES
- Supplement 55: Attribute Level Confidentiality
- Supplement 86: Digital Signatures for Structured Reports
- Supplement 95: Audit Trail Message
- Supplement 99: Extended Negotiation of User Identity

１－３）NEMA/COCIR/JIRA Joint Security and Privacy Committeeへの対応

- 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/security/

１－４）国内法・ガイドラインへの対応

- 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2版」
  - 作業WGへの参加

2）画像医療システムに関するセキュリティ関連のガイド等の検討

- 医療機器に対するリモートサービスにおけるセキュリティガイドラインの検討
- 相互運用性に関するセキュリティ（シングルサインオン、監査証跡）の検討

２－１）リモートサービスセキュリティ（RSS）ガイドライン

- JESRA化完了。HPにて公開中。
  - http://www.jira-net.or.jp/index.htm
- 厚労省「安全管理に関するガイドライン」を受け、リモートサービスにおけるセキュリティの最低限の指針

２－２）相互運用性におけるセキュリティの検討

- シングルサインオン
- 監査証跡
  - MEDIS-DCでの検討委員会に参加
  - 医療機関向けガイドの作成
    - http://www.medical-it-link.jp/

3）画像医療システムに関するセキュリティ関連の情報収集と会員への周知

- JAHIS（保健医療福祉情報システム工業会）セキュリティ委員会との連携
- 情報セキュリティマネジメントシステム(ISMS)への対応
- 医用画像情報に含まれる個人情報の取扱に関しての通達
- CyberRad等でのプレゼンテーション
  - http://www.jira-net.or.jp/index.htm