2010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

2010年度活動内容

1）ISO/TC215 WG4(セキュリティ&プライバシ）で検討されている国際標準への対応

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

3）NEMA,COCIRと共同してグローバルな医療機器セキュリティへの取り組み

1）ISO/TC215 WG4(セキュリティ＆プライバシ)で検討されている国際標準への対応

- 年2回開催されている会議へ2名エキスパート派遣
  - 2010年 5月　ブラジル・リオデジャネイロ
  - 2010年10月　オランダ・ロッテルダム
  - 2011年　5月　フィンランド・クオピオ（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
  - 日本の主張のドラフトへの反映
- 日本から規格提案
  - リモートサービスセキュリティWGで作成したJESRAをTR化→出版済み

ISO/TC215 WG4で検討中の主な国際標準

- EHR関連
  - TS14265 Classification of Purposes for processing personal health information
    （個人健康情報処理の目的分類）
  - TS14441 Security & privacy requirements for use in conformity assessment of EHR systems
    （EHRシステムの適合性評価におけるセキュリティとプライバシ要件）
- インフラ関連
  - IS27789:Audit trails for electronic health records
    （EHRアクセス時の監査証跡）
  - TR16114 Security aspects of Electronic Health Record migration
    （EHRの移行に関するセキュリティ特性）
- 日本からの提案
  - TR11633:Information security management for remote maintenance of medical devices and medical information systems
    （医療機器＆医療情報システムのリモートメンテナンスにおける情報セキュリティマネジメント）
    Part 1:Requirements and risk analysis
    Part 2:Implementation of an information security management system (ISMS)

ISO/TC215 WG4
EHR関連

- TS14265

  Classification of Purposes for processing personal health information

  （個人健康情報処理の目的分類）

  - 英国からの提案。個人健康情報の処理の目的の分類を定義
  - アクセス制御や監査証跡への利用を想定
  - 14種類の目的を定義
  - 投票の結果、賛成多数で成立。出版フェーズに進む
  - JIRAとしては、14種類の内容が妥当かどうかの判断はできないが、このような分類を定義することのメリットはあると判断し「賛成」とした

ISO/TC215 WG4
EHR関連

- TS14441

  Security & privacy requirements for use in conformity assessment of EHR systems

  （EHRシステムの適合性評価におけるセキュリティとプライバシ要件）

  - ブラジルからの提案。EHRシステムの適合性評価におけるセキュリティとプライバシ要件を規定するもの
  - 米国、カナダ、英国、ブラジルで現在使われている規約やガイドラインの内容をまとめ、最低限求められているセキュリティ要件を抽出
  - 小規模のEHRシステムをモデル定義し、そのシステムの要求仕様書(Protection Profile)を例示する

ISO/TC215 WG4
インフラ関連

- IS27789:
  Audit Trail for electronic health records
  （EHRアクセス時の監査証跡）

  - EHRシステム間での情報交換時の監査証跡に関する規格
  - 監査証跡を出力するトリガ（イベントトリガ）と、内容について定義している
  - DICOM Sup95やIHE ATNAと同じ枠組み（RFC3881準拠）
  - 日本から提案したイベントトリガと、その内容がほぼそのまま取り込まれた
  - 今後、DIS投票へ進む

ISO/TC215 WG4
インフラ関連

- TR16114
  Security aspects of Electronic Health Record migration
  （EHRの移行に関するセキュリティ特性）
  - システム更新時のEHRデータの移行に関するセキュリティについて述べた技術文書
  - 移行時のデータの意味的な完全性や、見た目や操作性などのユーザビリティの完全性についての必要性を指摘
  - もちろん、プライバシ保護のための秘匿性にも言及
  - ただし、指摘のみで対策についてまでは含まれない模様
  - JIRAとしては最終版のドラフト待ち

ISO/TC215 WG4
日本からの提案

- TR11633:
  Information security management for remote maintenance of medical devices and medical information systems
  (医療機器＆医療情報システムのリモートメンテナンスにおける情報セキュリティマネジメント)

  - リモート保守におけるセキュリティのガイドライン
  - リモート保守のセキュリティ要件と、モデルにおけるリスク分析の結果を例示
  - JESRAである「リモートサービスガイドライン」を英文化したもの
  - 現在、出版済みである(2009/11)

2）厚生労働省「安全管理ガイドライン」に対するベンダとしての取り組み

- 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をJIRAホームページで公開
- 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４．１版」
  - 作業WGへの参加
  - 2010/2/2公開
- 署名用HPKIポリシ改訂および認証用HPKIポリシ作成
  - 作業WGへの参加

2）厚生労働省「安全管理ガイドライン」に対するベンダとしての取り組み

- 製造業者による医療情報セキュリティ開示説明書に関するWG
  - 「安全管理ガイドライン」の技術的対策の要求事項を適用範囲とする
  - 医療情報システムの製造業者向けに、利用者への開示を目的とした適応性のチェックリスト的な文書の作成
  - 顧客より開示を求められているシステムのセキュリティに関する資料の書式や粒度（どこまで記述すれば十分か）などに対するテンプレートとしての利用を目的

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

- 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

- 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://www2.medicalimaging.org/policy/security.cfm

- 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

- 医療機器セキュリティのための製造業者開示説明書 (MDS^2)
  - 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

ご清聴ありがとうございました