

3. リモートメンテナンスサービスにおけるセキュリティ

(社)日本画像医療システム工業会 システム部会 セキュリティ委員会
野津 勤

近年、医療機器のネットワーク化、医療情報システムは初期導入の段階から一般的普及の段階に移ってきています。それに伴い、医療機器・システムの保守を安全かつ効率的に行うために、医療機関と医療機器・システムベンダ間をネットワークで結び、遠隔からの保守を行うケースが増えてきています。

JIRA((社)日本画像医療システム工業会)セキュリティ委員会では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共同でリモートサービスセキュリティWGを発足させ、医療分野における遠隔保守(リモートサービス)のあり方と、情報セキュリティマネジメントと個人情報保護の視点からリモートサービスのリスクアセスメントを研究し、医療機関と医療機器・システムベンダがそれぞれどのようなセキュリティ対策を取るべきかの検討を行ってきました。

その成果として、2003年度にはJIRA規格としてJESRA「リモートサービスセキュリティガイド」(C0012-²⁰⁰⁴)を、2005年度にはより踏み込んだ内容のJEARA「リモートサービスセキュリティガイドライン」(C0013-²⁰⁰⁶)を制定し、リモートサービスを安全に行うための実践的な指針を示しました。

上記の2つの文書で示されたりモートサービスにおけるセキュリティマネジメントの考え方は、国内に限らずどこでも参考になることから、本WGでは2008年度に、これらの記述から日本固有の法令、制度等に係る部分を取り除いたものを国際標準とすることを考え、ISO/TC215に提案しました。この提案はISO参加各国の賛同を受け、同作業会議における審議と修正を経て、「ISO TR 11633 Part 1&2」として2009年度に出版されました。

本年3月に、上記2文書に「ISO TR 11633 Part 1&2」作成過程で施された修正や新たに加えられた記述に、再度国内での固有の法令、制度等に関する記述を加え直し、従来のガイド(JESRA C0012-²⁰⁰⁴)とガイドライン(JESRA C0013-²⁰⁰⁶)を「ガイドライン ver.2.0」として統合・公開しました。

本ガイドラインでは、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を行い、そのモデルに対してISMS(Information Security Management System)の手法に従ったリスクマネジメントの実施例を示しています。医療機関の管理者、および遠隔保守を行うベンダは、ここでの実施例に倣うことにより、情報資産(特に診療に関する患者の個人情報)を安全かつ効率的に保護することができるようになることを目指しています。