【10】

氏名	羽根田 清文（はねだ きよふみ）
博士の専攻分野の名称	博士（保健学）
学位記番号	第 17710 号
学位授与年月日	平成15年3月25日
学位授与の要件	学位規則第4条第1項該当 医学系研究科保健学専攻
学位論文名	**安全な医療情報システムの構築・運用に必要なセキュリティ対策の最適化に関する研究**
論文審査委員	（主査） 教授 稲邑 清也 （副査） 教授 上甲 剛　教授 村瀬 研也

論文内容の要旨

〔目　的〕

医療情報システムにおいて医療情報を電子媒体として利用する為には、システムに対し医療情報を安全に取り扱う為のセキュリティ対策が必要となる。セキュリティ対策は、本来の業務に付随した装置および作業が必要となるために過度のセキュリティ対策は、システムの利便性を阻害する可能性があり、医療情報システムを適切に運用する為には、過不足ないセキュリティ対策が要求される。また、セキュリティ対策は、システム全体を網羅する必要があり、異なるシステムや施設、あるいは組織と情報を共有する場合には、自システムのみでなく情報を共有する全てのシステムにおいて安全性が確保される必要がある。その為、適切なセキュリティ対策を実施する為には、個々の安全性の評価ではなくシステム全体を網羅し、かつ何れのシステムでも適応可能となる方式が望ましい。

しかし、従来のリスク評価手法は複雑であり、一般的な利用者が的確に理解し、評価することは困難である。複雑なリスク評価およびセキュリティ対策は、利用者にとってもセキュリティ対策方法の理解や操作が煩雑になり効果的な運用が行い難くなっている。

そこで、医療情報システムのセキュリティ対策を簡便かつ容易に最適化する方式を検討し、検討結果を実際の医療情報システムに適応することにより実用化し、また、セキュリティ対策前後のリスクを定量的に表現させることによりシステム間での比較を可能とすることを目的とした。

〔方法ならびに成績〕

本研究による工程を、1）リスク評価、2）被害評価、3）セキュリティ対策、4）実システムへの適用の4工程に分けることにより各工程の意義および役割を明確に評価可能とした。また、工程を分離したことにより変更が発生した場合でも変更箇所は核当工程の必要箇所および関連箇所のみの変更にて対応可能となる。

ここで、1）から3）は、遵守すべき規定や予想されるリスクおよび利用可能な技術などについて検討する基礎的工程であり、4）は、基礎的工程をもとに実システムの運用形態や規模について検討する工程である。

リスク評価は、電子媒体の利用により新たに発生する可能性のある脅威をFault Tree Analysisにより分析することにより、システム全体を詳細かつ定量的に分析する。被害評価は、リスク評価より得た結果を基に、システムの各

箇所における予測される被害を求め、被害を許容限度に制限する為にシステムに最適なセキュリティ対策を提示する。セキュリティ対策は、リスクに応じて適切な対策が可能となるように対策方法を５種類に分類した。また、対策技術の向上などを考慮し各対策をパラメータ化し分類することにより、最適な方法を選択可能とした。

この方式を２種類の医療情報システム（１：広域放射線治療用データベースシステム（ROGAD：Radiation Oncology Greater Area Database）、２：病診連携医療情報システム（広島県立保健福祉大学－広島県立リハビリテーションセンター間画像伝送および診断システム））に適用して、各システムの運用形態を加味したリスクを評価し、評価に基づくセキュリティ対策を実装し運用および運用後の再評価することにより、本方式の実用性を検討した。

セキュリティ対策に必要なコストは、セキュリティ対策を本研究によるリスクの高低に基づいて実装した場合と全てのリスク想定箇所に均等に実装した場合とを比較したところ、広域放射線治療用データベースシステムでは、12%、病診連携医療情報システムでは、50%の改善が認められた。

システムの運用性は、システム運用時の脅威や脆弱性を系統的および個別箇所毎に提示可能となった為、運用規定の作成および各利用者に対するセキュリティ対策に伴う操作等の個別の教示を容易に実施することが可能となった。

研究の途中にてシステムの運用方法や構成内容の変更が発生したが、リスクの再評価およびセキュリティ対策は変更箇所のみの再計算に基づく修正により簡便に対処することが出来た。

〔総　括〕

医療情報システムのセキュリティ対策に関して、システム全体を対象としたリスクを定量的に評価した後、セキュリティ対策を実装した為、システムの運用形態に応じた過不足ない的確かつ効率的な評価および対策が出来た。

リスクの算出のデータとして、一般的なシステムに対する被害データを使用しているが、今後は医療の各分野に特化したリスクを求め、比較することによりそれぞれの医療情報システム特有のリスクについて検討できる可能性を切り拓いた。

論文審査の結果の要旨

本論文は、医療分野の情報システムを構築・運用する為に、解決しなければならないシステムのセキュリティ対策について検討したものである。

医療分野のシステムは他分野のシステムと比較して、情報化が遅れている分野の一つであるが、医療の最適化や効率化の為に、早急なる普及が望まれている。普及を妨げる理由の一つにシステム構築・運用に伴うセキュリティ対策の構築・運用の課題がある。理由として、対策評価に必要な医療情報の価値（医療資産）の把握が困難、および施設内のセキュリティ専門家の不在がある。本研究では、これらの問題点を解消する為に、価値基準、リスク評価およびセキュリティ対策を医療分野に特化することにより解決を図った。

本研究の、独創的な特長として、１）独自モデル作成による全ての医療分野の情報システムへの対応可能、２）医療資産をシステムが被る損額ではなく、医療情報の利用に不可欠な基準への対応度とすることにより基準を脅かす影響度合いとその発生確率にてリスクを算出することにより一般の評価方法では、算出困難な定量的なリスク評価可能、３）基準に基づいた安全許容度を検討し、システムの各事象におけるリスクが許容度から離れているかを定量的に評価し、離れた割合に対して分類し、過不足ないセキュリティ対策を実施したものである。

本方式を実際の２種類のシステム（広域放射線治療用データベースシステムおよび施設間連携医療情報システム）に適用したことにより、システムのリスク評価値に応じたセキュリティ対策の優先度およびコスト配分により、セキュリティ対策を施すことにより既存の方式と同等の安全性を確保しながら、それぞれ 61%、63%の改善が認められ過不足ない最適なセキュリティ対策が実施できた。

本方式を利用することにより、知識および対策コストの問題により医療情報システムの構築に躊躇していた施設への医療情報の有効活用への貢献を高く評価でき、保健学博士の学位に値するものと認める。