平成 27 年度厚生労働科学研究費補助金厚生労働科学特別研究事業
臨床研究の実施状況管理のためのデータベースに関する研究

臨床研究の実施状況管理のためのデータベースのセキュリティ要件

研究者名　藤井　仁、佐々木　美絵、湯川　慶子、佐藤　元 [1)]
1）国立保健医療科学院政策技術評価研究部

研究要旨

目的：本稿では臨床研究の実施状況の管理のためのデータベースの管理主体となることが想定されている厚生労働省、PMDA（独立行政法人医薬品医療機器総合機構）と、国立保健医療科学院のセキュリティ要件を比較し、どこに異同があるのかを明らかにすることを目的とする。

方法：上記 3 機関のセキュリティポリシーを比較し、異同がどこにあるかを明らかにする。また、これらの機関のセキュリティポリシーは、「政府機関のセキュリティ対策のための統一基準」を基に作成されているので、必要に応じてそれとも比較をする。

結果：全体的に見て、3 機関のセキュリティポリシーに大きな相違はなかった。国立保健医療科学院のセキュリティポリシーは厚生労働省のものと同一で、その附則を別途定めている状態であった。ゆえに、3 機関間でのセキュリティポリシーの相違はほとんど見られなかった。

結論：データベースの利用者・管理者側のセキュリティポリシーはいずれも「政府機関のセキュリティ対策のための統一基準」を基底としており、内容が相似しているため統合は比較的容易であると考えられる。しかし、情報の送信者側となる大学等のセキュリティポリシーにはひな形となるものがなく、各機関が独自に策定しているため、将来的なポリシー統合の障壁となりうる可能性がある。

A.研究目的

臨床研究（本稿でいう臨床試験は治験を含まない）の実施状況の管理のために、新しいデータベースの構築が求められている。

その基本設計を考案するうえで重要になるのがセキュリティ要件である。本稿では臨床研究の実施状況の管理のためのデータベース（以後、新 DB）の管理主体となることが想定されている厚生労働省、PMDA（独立行政法人医薬品医療機器総合機構）と、国立保健医療科学院（科学院が保持している臨床試験登録情報データベースと新 DB の連携が求められている）のセキュリティ要件を比較し、どこに異同があるのかを明らかにすることを目的とする。セキュリティ要件に大きな差がなければ、3 機関間でデータを送受信し、参照するシステムの構築は容易になり、逆であれば困難になる。ゆえに本稿はシステム構築の難易を明らかにする。

B.研究方法

厚生労働省、PMDA（独立行政法人医薬品医療機器総合機構）、国立保健医療科学院のセキュリティポリシーを比較し、異同がどこにあるかを明らかにする。また、これらの機関のセキュリティポリシーは、「政府機関のセキュリティ対策のための統一基準」を基に作成されているので、必要に応じてそれとも比較をする。

セキュリティポリシーは

１．総則
２．情報セキュリティ対策の基本的枠組み
３．情報の取り扱い
４．外部委託
５．情報システムのライフサイクル
６．情報システムのセキュリティ要件
７．情報システムの構成要素
８．情報システムの利用

といった構成が一般的である（「政府機関のセキュリティ対策のための統一基準」より）。これをすべて比較すると非常に莫大な量になる。また、すべてを比較することに積極的な意味はない。組織や教育体制についての規定などは、多少の違いがあってもシステム構築に大きな影響を及ぼさ

ないと考えられるからである。ゆえに、本稿では「６．情報システムのセキュリティ要件」に限定して比較する。

(倫理面への配慮)

当研究において、個人データ等を扱っていないので倫理面への配慮は必要ない。

C.研究結果

全体的に見て、厚生労働省と PMDA（独立行政法人医薬品医療機器総合機構）のセキュリティポリシーに大きな相違はなかった。国立保健医療科学院のセキュリティポリシーは厚生労働省のものと同一で、その附則として「国立保健医療科学院研究情報ネットワークシステム情報セキュリティ対策実施手順」を定めている状態であった。ゆえに、3 機関間でのセキュリティポリシーの相違はほとんど見られなかった。

以下、細目について述べる。細目の番号は「政府機関のセキュリティ対策のための統一基準」の附番に則る。

6.1　情報システムのセキュリティ機能

6.1.1　主体認証機能

「政府機関のセキュリティ対策のための統一基準」と 2 機関（厚生労働省、PMDA）のポリシーにほとんど差異はない。厚生労働省のポリシーに注意書きが付加されている程度である（厚生労働省が有する各情報システムの利用者は、行政事務従事者に限られるものでは ない。識別コードと主体認証情報については、利用者の別にかかわらず保護すべきであるが、行政事務従事者以外の者は本ポリシーの適用範囲ではないため、 それらの者に対しては、これを保護するよう注意喚起することが望ましい)。また、PMDA のポリシーには以下すべての項目で基本対策事項が付記されている。

6.1.2　アクセス制御機能

「政府機関のセキュリティ対策のための統一基準」と 2 機関（厚生労働省、PMDA）のポリシーにほとんど差異はない。表現に多少の差異があるのみである。

6.1.3　権限管理機能

「政府機関のセキュリティ対策のための統一基準」と 2 機関（厚生労働省、PMDA）のポリシーにほとんど差異はないが、厚生労働省のポリシーには遵守事項に権限管理の具体的な方策が付記されている（最小特権機能、主体認証情報の再発行を自動で行う機能、デュアルロック機能など)。

6.1.4　ログの取得・管理

「政府機関のセキュリティ対策のための統一基準」と 2 機関（厚生労働省、PMDA）のポリシーにほとんど差異はないが、厚生労働省のポリシーには遵守事項に付記がある（証跡の点検、分析及び報告を支援するための自動化機能、情報セキュリティの侵害の可能性を示す事象を検知した場合に、監視する者等にその旨を即時に通知する機能を必要に応じて設けることの勧告と、証跡の取得と保存に関する但し書きが付加されている）

6.1.5　暗号・電子署名

「政府機関のセキュリティ対策のための統一基準」と 2 機関（厚生労働省、PMDA）のポリシーに大きな差異はない。

差異として、厚生労働省のポリシーには電子署名の鍵の耐タンパー性（外部からのプログラム解析を防ぐ仕組み）と、アルゴリズムの危殆化（暗号解読技術の向上により、既存の暗号レベルの安全性が担保できなくなること）に関する記述がある。

また、「政府機関のセキュリティ対策のための統一基準」と PMDA のポリシーには、暗号技術検討会および関連委員会（CRYPTREC）による安全性と実装性能が確認された暗号リストを参照するよう求めている。

6.2　情報セキュリティの脅威への対策

6.2.1　ソフトウェアに関する脆弱性対策

厚生労働省のポリシーのみ、脆弱性をセキュリティホールと表現している。また、セキュリティホール対策計画を策定するよう要請し、細目を例示している。

(ｱ)　対策の必要性
(ｲ)　対策方法
(ｳ)　対策方法が存在しない場合の一時的な回避方法
(ｴ)　対策方法又は回避方法が情報システムに

与える影響
（オ） 対策の実施予定
（カ） 対策試験の必要性
（キ） 対策試験の方法
（ク） 対策試験の実施予定

6.2.2 不正プログラム対策

表現に多少の差異はあるが、内容はほとんど同じである。厚生労働省のポリシーのみ、システム運用時の取り組みが記載されている。

6.2.3 サービス不能攻撃対策

ほとんど内容は同じであるが、厚生労働省のポリシーのみ、サービス不能攻撃対策への具体策が記されている（通信回線の冗長化など）。また、この節の次に厚生労働省のポリシーのみ、踏み台対策という節が設けられており、第三者によって不正アクセスや迷惑メールの中継地点として、意図しない用途で情報システムが利用されてしまうことのへの対策についての記載がある。

6.2.4 標的型攻撃対策

表現に多少の差異があるが、内容はほとんど同じである。

D.考察

3 機関のいずれのセキュリティポリシーも「政府機関のセキュリティ対策のための統一基準」が基底にあり、表現の違いや記載の濃淡に多少の差異はあるが、統合できない程度の差異ではないと考えられる。よって、臨床研究のための統一セキュリティポリシーの作成は比較的容易であると考えられる。

本システムのセキュリティポリシーの統合に問題があるとすれば、大学や病院など臨床試験の実施、登録機関側のポリシーではないかと考えられる。「大学　セキュリティポリシー」でネット検索した結果の上から５機関のポリシーを確認したところ、「政府機関のセキュリティ対策のための統一基準」よりもはるかに分量は少なく、不十分な内容のものしかなかった。セキュリティ維持のためにポリシーを公開しないと宣言している機関もあり、セキュリティの仕様とポリシーを混同している例も散見できた。

E.結論

新 DB の利用者・管理者側のセキュリティポリシーはいずれも「政府機関のセキュリティ対策のための統一基準」を基底としており、内容が相似しているため統合は比較的容易であると考えられる。しかし、情報の送信者側となる大学等のセキュリティポリシーにはひな形となるものがなく、各機関が独自に策定しているため、将来的なポリシー統合の障壁となりうる可能性がある。

F.研究発表

1. 論文発表
なし

2. 学会発表
なし

G.知的財産権の出願・登録状況（予定を含む）

1. 特許取得
なし
2. 実用新案登録
なし
3. その他
なし