国際標準の参照関係に基づくセキュリティ評価方式における データ移行機能の検討

髙橋 雄志† 勅使河原 可海†
創価大学大学院工学研科†
192-8577 東京都八王子市丹木町 1-236
{e08d5203, teshiga }@soka.ac.jp

あらまし セキュリティ認証取得に対し，国際標準等を基準として対象を評価する．組織では，認証取得に向け，基準達成を確認するセキュリティ評価システムが活用されている．本研究ではこれまで，標準の変化に対応するため，個別の評価ツールではなく，評価基準とする標準の変更のみで標準内容や評価対象の変化に対応した評価ツールを実現するプラットフォームの検討を行ってきた．本稿では，この研究の大目的のひとつであるところの異なる基準をもってセキュリティ評価を行う際に個別のツールを用いなければならないという問題の解決についての検討を行った．データの移行については実験を通してその有効的な移行方法について考察を行った．

A Study on Data Conversion Function of Security Evaluation Method Based on Reference Relationships among International Standards

Yuji TAKAHASHI† and Yoshimi TESHIGAWARA†

† Graduate School of Engineering, Soka University
1-236 Tangi-cho, Hachioji, Tokyo, 192-8577, Japan
{e08d5203, teshiga }@soka.ac.jp

Abstract To obtain acquisition of security attestation, the target organization is evaluated based on the international standards. In the organizations, the security evaluation systems that confirm standards achievement of the platform for the attestation have been used. In order to correspond to changes of the standards, we have been studying a platform that realizes the evaluation tool corresponding to changes of the standards contents and evaluation targets only by changes of the standards used as evaluation criteria. In this paper, we studied the solution to solve the problem that it was necessary to use an individual tool when security was evaluated with different standards. In addition, we discuss the effective data conversion method through the experiment.

1　研究の背景と目的

近年，セキュリティの目的は，組織の資産を守る自己防衛のためのセキュリティから，セキュリティ被害が原因となる二次的な加害者にならないためのセキュリティまで範囲が拡大している．これに伴い，組織の安全性の確保及びセキュリティ対策実施状況を対外的に明示するため，外的機関によるセキュリティ評価をすることが重要視されている[1]．具体的な評価としてISMS 適合性評価制度に基づく情報セキュリティマネジメントシステム（以下，ISMS: Information Security Management System という）認証取得がある．この ISMS 認証は認証制度ができて以来取得件数が増加し続けており，2011 年 8 月 23 日現在で 3,873 件と多くの企業・組織が取得している[2]．

ISMS などのセキュリティ認証の多くは ISO/IEC 27001 や ISO/IEC 27002, JIS Q 15001 といった標準を基準として，その標準に記載されている項目を満たすことにより，組織のセキュリティが確保されていることを保証する．また，組織では認証取得に向け，基準達成を確認するためのセキュリティ評価システムが活用されている[3]．しかし，標準は時代の変化に合わせて頻繁に内容が変更される．中でもセキュリティ関係の標準はまだ充分に試されていないので，ユーザコメントを集め変更が行われる回数が他の標準にくらべて頻繁である．また，取得を目指す認証が異なったり，組織規模などに応じて基準とすべき内容が異なったりする．そうした変化は評価対象組織および評価目的が変わると，認証取得のために，新たな体制を作ってそれぞれの認証取得にあわせて個別のツールや人員を用いてセキュリティ評価をやり直さなければならないといった状況を作りだす原因となっている．そして認証取得のためには多くの時間と労力，費用が必要となり企業活動における人的，金銭的な影響が大きいという問題につながっている．このような問題を解決するために，個別のセキュリティ評価ツールではなく，標準の内容に依存せず，評価対象組織および評価目的の変更に対応した評価ツールを実現する仕組みの必要性が高まってきている．

本研究では，対象となる標準に依存せず，プラットフォームの基本となる標準を整理した基本データの入れ替えだけで他の標準と同様にセキュリティ評価が行えるプラットフォームについて検討を行ってきた[4]．本プラットフォームでは，標準の内容ではなく，その特徴的な構造である階層構造と参照関係に着目し，標準を階層構造に基づいて整理したデータが登録データとなるようにした．また，階層構造と参照関係を利用した評価値計算をすることによって要件の達成を目指すプラットフォームの検討を行ってきた．そして，プロトタイプシステムの開発を行い，ISO/IEC 27000シリーズなどのデータを登録してプラットフォームについて検討を行ってきた[5]．プラットフォームで使用するセキュリティ評価についても同様に，基準とする標準の種類に依存せず，セキュリティ評価が行える必要があり，標準の種類に依存しない評価値算出方式が求められる．これまでの検討でセキュリティ評価について後述する参照ツリーの各構成要素に対して評価に対する影響度を変化させてセキュリティ評価をし，参照ツリーの距離に着目したセキュリティ評価方式について実験を行ってきた結果，距離だけでなく評価項目と各項目の関係により影響度を変えることが有効であるとの知見を得た[6][7]．本稿では，異なる基準を用いてセキュリティ評価を行う際に発生する最初から再評価を実施しなければならないという問題につい基準同士の関係性を利用したデータ移行機能を用いることで解決を目指し，実験および検討をする．

2　標準の分析と活用

2.1　ISO/IEC 27000 シリーズ

ISO/IEC 27000 シリーズとは，国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定する情報セキュリティ規格群である．このシリーズは対象とする範囲が広く，代表的

なセキュリティ問題である，プライバシー，機密，情報技術におけるセキュリティ問題などをカバーしている．従って，あらゆる規模と形態の組織に適用可能であるといえる．

このシリーズのセキュリティ認証を取得するには，まず組織は情報セキュリティリスクを評価し，必要に応じた適切な情報セキュリティ制御を実装することが求められる．また情報セキュリティは固定的なものではないので，ISMS には PDCA サイクル（Plan-Do-Check-Act cycle）による継続的なフィードバックと改善が要求される．多くの標準の策定が予定されており，現在のところ，2011 年時点すでに 9 つが策定済みであり，他にも多くの標準が準備中となっている．ISO/IEC 27000 シリーズは多くの分野においての基準となる標準群となり ISMS に基づく PDCA サイクル運営の重要性を示している．

2.2 ISO/IEC 27001

ISO/IEC 27001 は，ISMS を確立，導入，運用，監視，見直し，維持及び改善するためのモデルを提供することを目的として作成されている[8]．また，ISMS 認証取得時に作成される ISMS 運用マニュアルにおいては，この標準の各項目に示されている内容がセキュリティ要求事項に該当し，そのすべてを網羅している必要がある．ただし，すべての内容についての対策を必要とする訳ではなく，適用対象外のものは対象外であることが明記されていればよい．ISMS 認証の審査の際にはこのマニュアルに基づき各項目への対応状況が審査の対象となる．

2.3 標準の構成

標準では一般的に本文が「章・節・項」のように 3 段階の階層構造で記述されていることが多い．この構成では，章の部分で評価対象を大別し，節の中で評価対象における詳細を記述し，項の中でさらに詳細な内容を記述している．

ただし，個々の項目は独立した項目として記述されているものばかりではなく，その項目の条件や附則事項として，他の項目を参照するように記述されているものが数多く存在している．例えば，ISO/IEC 27001 の「7.1 一般」は本文中で 4.3.3 参照との記述があり，本研究で用いる参照ツリーでは図 1 で示すような形で表現する．

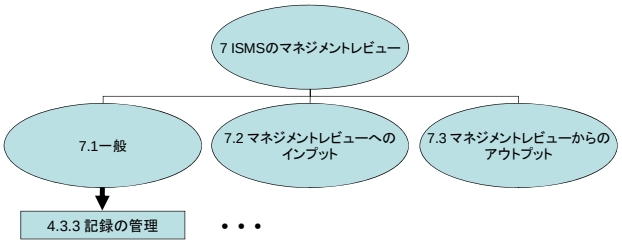

図 1　ISO/IEC 27001 の参照関係の例

2.4 対応策による項目の網羅の困難さと解決策

セキュリティ認証においては，基準を網羅的にカバーする必要があり，構成の各章ごとの枠組みに応じて対応策の実施やリスクの受諾などの対応方針の決定を行っていく流れとなる．その際に，各章ごとにカバーすべき項目をすべて網羅している必要があるため，章ごとの階層構造と各項目からの参照関係を的確に把握する必要がある．しかし，ISO/IEC 27001 に限らず，標準ではこういった参照関係が多く，標準の各項目がカバーすべき内容（項目）が多岐にわたる．そのため，そのすべてを的確に理解し，網羅的な対応策を選択することが困難であるという問題点がある．

そのため，各章で網羅すべきすべて項目を一括管理できることが求められている．標準で本文記述されている階層構造と参照関係は，標準の変更や異なる標準であっても同様の特徴情報として記述されているため，標準の変更や異なる標準であっても同様に特徴情報として扱うことができる，そこで本研究では，階層構造と参照時関係について着目する．そして，階層構造と参照関係を利用することによって，基準が変わっても章ごとに網羅すべき項目を一括管理できるプラットフォームの実現によって問題の解決を図る．

3　プラットフォームの概要

3.1　プラットフォームの構成

本プラットフォームは，データ入力部，データ管理部，スコア計算部の 3 つの部位にわかれている．本プラットフォームの構成を図 2 に示す．データ入力部で，標準の生データと，構造情報，および参照情報の入力をする．データ管理部では，入力された標準の生データと構造情報に基づき整理し，参照情報を用いて参照関係の展開を行い，参照ツリーの構成をする．さらにスコア計算部で計算された評価値の管理もする．スコア計算部では，参照ツリーに基づく参照情報と登録された対応策の施策情報に基づき，評価値計算を行い，データ管理部に計算をしたデータを渡す．また，対応策情報をデータ提供する設定に限りサンプルデータを作成してデータ管理部にフィードバックする．スコア計算部ではサンプルデータを参照しながら対応策の情報入力を行うこともできる．

本稿で追加されたデータ移行機能のために，データ入力部で入力する情報に新たに異なる基準間の対応関係を示す対応情報を追加した．

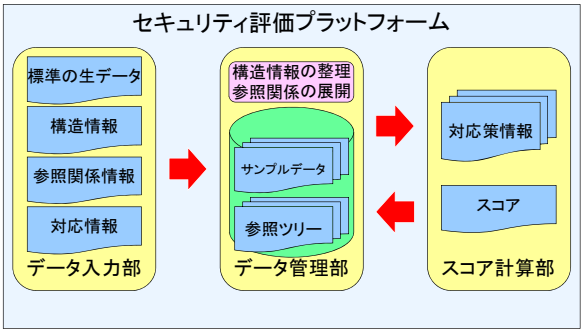

図 2　提案プラットフォームの構成

3.2　プラットフォームの動作

最初にデータ入力部にてデータの入力作業をする．まず標準の生データを登録する．そして，登録したデータに対して 2.2 節で述べた階層構造に基づく構造情報の登録をする．続いて参照関係情報の登録をする．ここで登録をする構造情報と参照情報は，階層に基づく情報と標準本文に記述されている直接的な参照（以下，直接参照という）情報のみが登録される．データの登録がすべて完了したら登録情報をデータ管理部に受渡し次の動作に移行する．

本プラットフォームでは階層をレベルと定義し，章をレベル 1 とし，次の階層をレベル 2 といった形でナンバリングしていき，レベル m はレベル m+1 の項目を直接参照しているとみなす．

そして，他の基準との対応の関係を示す情報がある場合は対応する基準のデータを登録した後に対応情報を入力する．

続いてデータ管理部では登録された情報に基づき参照ツリーを作成する．直接参照の記述がある項目（以下，参照親という）を根とし，記述されている参照すべき項目（以下，参照先という）を葉とするツリーを構成し，基本ツリーとする．基本ツリーの葉となっている項目が別の基本ツリーの根となっている場合に，前者の葉の部分に後者の根を結合して新たなツリーを構成する．また，構成していく中で，ツリーの根からみて同じ項目を参照先として持つ場合がある．この重複する参照関係は，複数箇所で同一項目を参照先として持つ複数参照と，ツリーを構成する際にループが発生してしまうループ参照がある．これらの参照が発生した場合には，その重複が確認された部分を葉として確定させ，ツリーの構成を続けるものとする．このようにツリーの結合を繰り返していき，それ以上結合ができなくなるまで結合を繰り返した最大のツリーを参照ツリーとする．

参照ツリーでは項目間の関係を距離として表現し，直接参照されているものを距離 1 とし，以下参照を繰り返すたびに距離を加えていき要素間の距離とする．こうしてすべての項目について参照ツリーを作成し標準データの管理およびスコア計算部への展開をする．

また，データ移行機能を使うことで異なる標準の対応策情報を変換し，サンプルデータを作成することができる．

スコア計算部ではこの参照ツリーを用いて，セキュリティ評価のための基準を作成する．基準とは，標準の章・節・項を参照親に持つ参照

ツリー全体の評価値を測るためのものである．実際には参照ツリーの情報を用いた対応策施行情報とサンプルデータによる過去の案件での対応策と標準の各項目のマッピングデータの提示を行い，対応策の施行情報の入力を促す．入力された対応策情報と参照ツリーの情報に基づき評価値計算をするものとなる．また，サンプルデータを提供する設定をしている場合に限り対応策と各項目のマッピング情報のうち対応済みとなっているデータをサンプルデータとして取得し，該当する対応策のサンプルデータとしてデータ管理部に送る．データ管理部に送られたサンプルデータは，それ以後該当する対応策について他のユーザ（または案件）で標準とのマッピングを行う際に提示されサンプル情報を参考にしながらマッピング作業を行うことができる．

3.3　プラットフォームの特徴

このプラットフォームでは標準に変更があった場合にデータ入力部での情報更新をする．情報更新の後にデータ管理部で自動的に参照ツリーを再構成し，スコア計算部でスコアの再計算をすることによって変更された標準の内容に沿った再評価をすることができるものである．

また，参照ツリーを構成することによって項目間の関係性を視覚化することができる．この参照ツリーを確認しながら対応策の選択をすることで効果的な対応策を設定することの手助けをすることができる．

サンプルデータの表示機能によって専門知識を十分に有しているとはいえない管理者に知識共有ができる．

データ移行機能によって手間をかけることなく再評価の際に参考となるサンプルデータを作成することができる．

4　データ移行機能の適用

4.1　実験概要

各対応策の状況を『ISO/IEC 27001 附属書A』と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』の二つの視点から対応状況をマッピングして実際にデータ移行を行い，それぞれの基準で各対応策の移行されたデータの状況を調べた．

4.2　情報取得環境

今回の実験では，本学研究における対応策の状況を各基準に基づきマッピング作業を行った．作業は研究室のおける管理責任者を務める学生によって進めたものである．

4.3　実験の流れ

はじめに，ISO/IEC 27001 附属書 A の内容を確認しながら該当する対応策の洗い出し及び状況のマッピングを実施．次に先の工程で洗い出しを行った対応策について，ISMS 認証基準 Ver.2.0 附属書「詳細管理策」を基準として再度状況のマッピングを実施．最後に双方のデータを本プラットフォームのデータ移行機能を使用してデータ変換行って状況の比較を行うといった流れで実施した．

4.4　実験結果

20 件程度の対応策に対して，対応関係がある項目同時で異なる結果を示したものはのべ 120 項目強の項目となった．選択内容が正反対になったもの，片側だけ選択されていたものなどすべてのパターンが発生していた．そして，異なった状況を示した項目の内容を比較し状況の分析を行った．

4.5　実験の考察

分析の結果異なる内容を示した項目には以下の 6 つの特徴と見ることができた．

(1) 項目の内容が詳細に明記された．
(2) 項目の内容が曖昧になった．
(3) 項目の上位の項目の内容が異なるため同じ内容でも指し示すものが異なる．
(4) （指している内容は変わらないが）表現の

違いがある.

(5) 同じ内容のことを別の角度から示している.

(6) 双方の基準で同じ管理分野内に配置されていない.

(1)(2)(3)については表現の幅によって対応状況に変化が出てくる可能性があるので単純にデータを変換するだけではいけないということが見て取れる. また, (4)(5)(6)については被験者の見落としや知識が不十分な時に対応状況を提示することによってエラーを回避することができることが見て取れる.

5 今後の課題

本稿で行った実験では ISO/IEC 27001 に附録として明記されている対比表を用いてデータ移行用の対応情報を作成した. しかし, こうした対応表の存在しない基準同士のデータ移行を行うことができないという課題がある. この課題についてはオントロジーを用いた文書解析などを用いる方法などを検討している.

また, サンプル機能についてもサンプルの収集方法, 信頼性といった根本的な課題が存在する. 現在この課題については技術的な側面ではなく運用的な側面での解決方法を検討している.

6 まとめ

本稿では, データ移行機能を用いて異なる基準を用いてセキュリティ評価を行う際の再評価が必要となる問題についてのアプローチを検討した.

実験により, 見落としや知識の不備などの評価の際に陥りやすい問題について大きな効果が期待できることがわかった. また単純にデータを移行するのではなくサンプルの状態で提示することで表現が細かくなったり, 大まかになったりしたものについての再検討をスムーズに行うサポートができることがわかった.

今後は 5 章で述べた課題に取り組み, 様々なフェーズでの適応を確認し, プラットフォームの有効性を高めていく.

参考文献

[1] 財)日本情報処理開発協会:情報セキュリティマネジメントシステム(ISMS)の国際動向と取り組みの実際＜2004 年版＞, 平成 17 年 5 月

[2] 情報マネジメントシステム推進センター:認証取得組織数推移、認証機関別・県別認証取得組織, http://www.isms.jipdec.jp/lst/ind/suii.html

[3] 独立行政法人情報処理推進機構:セキュリティ設計評価支援ツール V03, http://www.ipa.go.jp/security/fy13/evalu/cc_system/CCtool_V03/secevtoolv03.htm

[4] 高橋雄志, 勅使河原可海:国際標準に基づいたセキュリティ評価プラットフォームの検討, 情報処理学会コンピュータセキュリティシンポジウム 2008(CSS2008) 論文集第 2 分冊, pp.815-819(2008)

[5] 高橋雄志, 勅使河原可海:国際標準に基づいたセキュリティ評価プラットフォームの有効性の検討, 情報処理学会第 46 回コンピュータセキュリティ研究発表会 Vol.2009-CSEC-46, No.13(2009)

[6] 高橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式の検討, 第 142 回 マルチメディア通信と分散処理・第 48 回 コンピュータセキュリティ合同研究発表会, Vol.2010-DPS-142 No.53 Vol.2010-CSEC-48 No.53

[7] 高橋雄志, 勅使河原可海:国際標準の参照関係に基づくセキュリティ評価方式における非専門家への対応策提示機能の検討, マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム論文集, pp.127 - 134

[8] ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005