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研究

Studies of Security Evaluation Platform based on International Standards

08D5203　髙橋雄志　指導教授　篠宮紀彦

ABSTRACT

In order 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 for the attestation have been used, however, they have to use specific security evaluation systems to correspond to changes of the standards. In addition, we need individual security evaluation system when changing of the organization or the position of security evaluation. Therefore, we have been studying a platform that realizes evaluation corresponding to changes of the standards contents and evaluation targets only by focusing changes of the standards used as evaluation criteria. Since all the items should be covered for every field of the standard, there is a problem of the comprehensibility that the reference relation from the structure and each item of the field must be grasped very precisely, We proposed to aggregate items to be covered by using a layered structure and reference relations of the standard, and proposed some methods to evaluate the reference relations. As the results of experiments by using proposed methods, it is recognized covering all items and avoidance of human errors by supplementing technical knowledge and by utilizing visual effects, and the effectiveness of the proposed system is confirmed.

1. 研究の背景と目的

近年，セキュリティ管理の目的の範囲は，組織の資産を守る自己防衛のみから，二次的な加害者になることを防ぐところまで拡大している．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て[1]，多くのセキュリティ標準が策定されている．しかし，個別のセキュリティ認証の取得に関しても対策の項目に対する網羅性の問題や標準に関する専門知識が要求されるといった問題があり，統合的に扱う環境はまだ整っていない．

具体的な認証評価として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，2013 年 8 月 30 日現在で 4,359 件と多くの企業・組織が取得している[2]．同様にコンシューマデバイスの管理に関するセキュリティ技術にも注目されてきている．企業の IT 資産にコンシューマデバイスからアクセスすることは，新しい重大なリスクを伴う．そのため，慎重な計画によって十分なセキュリティプロセスおよびセキュリティコントロールを確実に実現し，機密情報と機密性の高いアプリケーションを保護する必要がある．そのため強力なユーザ認証，アイデンティティライフサイクル管理，Web アクセス管理，情報の保護，および暗号化などの領域を含めて，アイデンティティ/アクセス管理の機能の重要性が高まっており，様々な形での標準化も積極的に行われている[3].

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，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．こういった認証制度では，基準となる標準の網羅性，認証取得担当者の専門知識が不十分なことがあるといった問題がある．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[4]．同様に，IT システムのセキュリティ機能の設計段階で，セキュリティ標準を知識ベースとして用いるシステムの提案もなされている[5]．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，これまでに対象となる標準に依存せず，セキュリティ評価プラットフォームの基本となる標準を整理した生データ（以下，基本データという）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[6]．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，統合的な環境を実現するために重要な，データ移行機能を利用する際には，異なる標準間で同じ内容を指す項目を示す関連情報が定義されている必要がある．しかし，その関連情報が必ずしも定義されているとは限らないという問題がある．そのため自然言語処理の分野で使われているテキスト間の類似度算出手法[7]を応用し各標準の項目同士の類似度から関連性を導き関連情報を取得する実験を行い，その有効性を確認した[8].

本研究では，評価基準となる標準が異なった場合でも，同様にセキュリティ評価を行えるプラットフォームを構築した．そのために，様々な機能の有効性を実験を通して確認した．その中で，基準間の関連情報の作成が，大きな課題であることがわかった．この課題に対して，異なる標準の各項目間の類似度を求めて，その類似度を元に関連情報を作成する手法を提案・検証し有効性を確認することができた．以上のことから，提案したプラットフォームは，異なる標準であっても同様のセキュリティ

評価を行うことができる統合環境が実現できたといえる．

2. 標準の分析と活用

本研究では，ISMS に代表されるセキュリティ管理の基準で広く用いられている PDCA(Plan-Do-Check-Action cycle)サイクルの概念が適応されている ISO/IEC 27000 シリーズとしてまとめられたセキュリティ標準のデータを主に使用して実験並びに検証作業を行ってきた．

このセキュリティ評価プラットフォームは PDCA サイクルのどの場面でしかつかえないというものではなく，用途に合わせて PDCA サイクルのどの場面でも使えるものを目指している．

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，標準では参照を示す記述が多く，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

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 1 に示す．

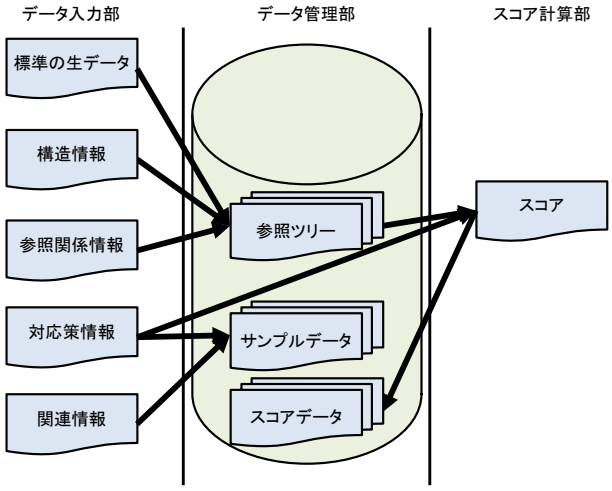

図 1　提案プラットフォームの構成
Figure 1　Structure of proposed platform

データ入力部で，評価基準となる基本データと，構造情報，参照情報，対応策情報および関連情報の入力をする．対応策情報入力時には，データ管理部で作成されたサンプル情報を元にデータ入力を行うことができる．データ管理部では，入力された標準の生データを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（スコアデータ）の管理もする．また，入力された対応策情報または関連情報に基づきサンプルデータを作成する．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．

このプラットフォームを統合的な環境として使用する際には，関連情報と対応策情報を組み合わせて，新しい基準向けのサンプルデータを作成する．このデータ移行機能に使用する，関連情報を自動的に作成することができれば，新たな標準が発表されたり，標準が改版されたりした際に，即座に再評価をすることができるようになる．

4. 類似度算出手法について

本論文で用いている類似度算出手法は，文書の分類や検索に関する研究において，多数の提案がなされている文書間の類似度を算出する手法を用いている．その手法とは，自然言語処理と呼ばれる，文書の内容情報を形式化するために，言語表現からその意味を抽出する処理を行い，形式化された内容情報から文書の内容を近似するものである[7]．まず，類似度算出の対象となる文書を確定し，そのテキスト情報を決定する．次に，決定されたテキスト情報を、奈良先端科学技術大学院大学で開発された「茶筌」[9]などを用いて，形態素解析[7]により形態素に分割する．そして，分割した語から，文書の内容を表す形態素や名詞などの単位で，索引語を抽出する．続いて，文書を特徴付ける上で，あまり役に立たない語を，不要語として削除する．さらに，抽出した索引語がその文書の内容にどれだけ密接に関係しているかを，索引語の重要度として付与するために，重み付けを行う．重み付け手法としては，文書中に出現する索引語の頻度を示す，索引語頻度（TF（Term Frequency））や他の文書中の索引語の分布を考慮した，IDF（Inverse Document Frequency），それらを組み合わせた TFIDF がよく用いられる[7]．最後に，重みによりベクトルや行列で表わされた文書間の類似度を算出する．

5. 各種機能について

本研究ではこれまで 3 章で述べた各機能の有効性の検証のために実験を行ってきた．

5.1　評価値算出手法

評価値算出手法については参照ツリーを用いて参照ツリーの各構成要素に複数パターンの重み付けを行いそれぞれの影響度を変化させた評価値計算を行ってより人の感性に近い値が算出できる評価値算出方法を検討した[10][11][12].

評価値を計算するにあたって参照ツリーの構成要素数および参照ツリーの根となる項目と各構成要素の距離に着目し各構成要素の参照ツリーの根となる項目対する影響度を変更するセキュリティ評価方式を用いて評価値の比較を行った．

最初に構成要素数のみに着目した評価値計算（方式 1）行い，人による評価値と比較したところ，単純な割合では表現できないことがわかった．次に，参照ツリーの距離に着目し，最大距離を取る項目の影響度を 1 とし，評価項目に近づくにつれて影響度を 1 ずつあげていく方式（方式 2）と，評価項目との距離の逆数を影響度とする方

式（方式 3）を用いて検証を行った．その結果，項目ごとに影響度を変えることが有効であることがわかった．そして，それぞれの方式が有効であると，判別された評価項目に対する対応策の状況から各構成要素と評価項目の章が異なるという基準で影響度に変化を加えることによって評価値を改善できるという知見を得ることができた．最後に，着目し，評価項目と構成要素の章が同じ場合に方式 2 を，章が異なる場合に方式 3 を採用する方式 4 を用いて検証実験を行ったところ全評価項目の評価値を改善することができた．

5.2　サンプル提示機能

サンプル提示機能を使用することで，セキュリティ知識が十分に有していない被験者の対策選定のサポートを行うことができるかの検証を行った[12].

検証はロールプレイ実験の形をとり，サンプルデータの作成をセキュリティ認証に関する知識があり，一般セキュリティ業務経験がある筆者が行い，セキュリティに関する一般知識はあるが，セキュリティ認証に関する知識は不十分である本学の大学院生に，対応策が標準のどの項目を満たしているのかを選定する作業を行ってもらった．対象となる組織は被験者が所属する研究室とし，対応策の抽出が終わって現状分析を行う段階である，と仮定した．また，対応策を選択する段階で認証を意識して対策選定が行われていないため，標準の項目を意識して対応策を立てているわけではないという前提でデータを作成および取得している．対応策の有無とは，標準に明記されている要求事項に対する対応が定まっているか否かを示すものとする．

実験後のヒアリングでシステムを使うことにより項目間の関係性の整理を行うことができたこと，サンプルの提示によって自信をもって項目を選択できたことという解答を得られた．また，サンプルにないデータを残した部分については実際の現場にて感じた感覚を信頼して残しているという解答も得られた．このことよりサンプルデータの提示でより的確な対応策の状況を掌握するためのサポートすることができたことが確認できた．

5.3　データ移行機能

データ移行機能については，二つの基準で別々に対策と基準の項目との対応を選択してもらった結果とデータ移行機能を用いてデータ変換した結果を比べることによって管理者の見落としなどのエラーの回避に有効であるかの確認を実験を通して行った[13].

実験では各対応策の状況を『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，対応策がどの項目を満たしているか選択して，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．

実際にそれぞれの基準からみて異なる結果を示した項目を確認すると，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ことがわかり，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わかった．また，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も実験結果から推察することができた．また，同一人物が対策が標準のどの項目に該当しているかを選択しているにも関わらず，データ移行すると一致しないという結果からデータ移行機能の重要性を確認することもできた．

5.4　テキスト類似度を用いた関連情報作成

5.3 の結果からデータ移行機能がこのプラットフォームの重要機能であることがわかった．しかし，このデータ移行機能を使用するためには，基準間の関連情報が定義されている必要がある．しかし，その関連情報が定義されているとは限らない．現状では，関連情報の作成するためには，元となる基準両方に関する知識が必要となり困難な作業となる．また，セキュリティに関する基準は多く存在し，すべての組合せを網羅するとなると膨大な知識と時間，労力が必要となる．そこで本研究では，テキスト間類似度に着目し，基準同士の関係情報を生成実験を行った[14].

初期実験として，最もシンプルな類似度算出手法を用いた実験を行った．最初に，5.3 の実験と同じ標準間の関連情報が明示されている二つの基準を用いて，各項目間の類似度を算出する．算出した類似度を両方の基準からみて同時に最大値をとるものを関連がある項目と定義する．関連がある項目となったものが，明示されている関係をどの程度再現できているのかを調べる．そして，再現できなかったもののうち，「関連付けがあるのに抽出されなかった」ものを FN(False Negative)，「関連付けがないのに抽出された」ものを FP(False Positive)，「間違った項目を抽出した」ものを NG としてそれぞれについて詳細の分析考察を行った．実験結果は

表 1 で示すようになり 80%を超える再現率と 89%を超える確からしさという高い値を示した。

表 1　関連がある項目の再現率と確からしさ
Table 1　Recall and probability of an item with relation

	関連がある項目数	抽出した項目数	OK	FN	FP	NG	再現率	確からしさ
大項目	10	8	8	2	0	0	80.00%	100.00%
中項目	31	28	25	5	2	1	80.65%	89.29%
小項目	116	97	95	19	0	2	81.90%	97.94%

そして，エラー項目を分析することで得られた知見に基づき，さらに精度の高いデータが作成できないか追加の実験を行った[8]．得られた知見とは，項目名と詳細記述に分かれている 場合に，項目名の方が重要な内容を示しているのではないか．もうひとつの知見としては，階層構造を理解することで，項目の内容をより的確にとらえることができるのではないか，ということである．

この実験では，基準の文章構成および標準の階層構造にに着目し，項目名と詳細記述とに分かれて記述されている中項目と小項目について，類似度の算出方法を変えて再現度の向上を目指した．

具体的には，以下に示す方法で類似度を出して，関連がある項目の抽出を行い再現率，確からしさおよびエラー数の比較を行った．

（方式 1）一律 1 の重み付けをする方式

今回の基準にするため初期実験と同じ方式となり，一律 1 の重み付けを行うものとなる．

（方式 2）専門用語数を用いる方式（方式 2）

専門語抽出を行って形態素ごとに分けた際に各項目で「項目名」と「詳細記述」に分けてその専門用語数をカウントすし，その総合計を「項目名」と「詳細記述」のそれぞれで算出する．各形態素に対して項目名は項目名の総計で，詳細記述は詳細記述の総計で割ってそれぞれの形態素の重みとする．

（方式 3）階層構造を用いる方式（方式 3）

まず，手法 1 と同じ方法で，各項目間の類似度を算出する．そして，算出した類似度を，標準の階層構造に基づき積算し中項目，小項目の類似度を改めて算出する．

例えば，基準 A の中項目 1.1 と基準 B の中項目 2.1 の類似度は，手法 1 で算出された基準 A の大項目 1 と基準 B の大項目 2 の類似度と基準 A の中項目 1.1 と基準 B の中項目 2.1 の類似度を掛け合わせた値になる．

それぞれの方式を用いて類似度算出を行って，関連情報を抽出した結果を中項目に関しては表 2，章項目に関しては表 3 のようにまとめた．

表 2　関連がある項目の再現率と確からしさ（中項目）
Table 2　Recall and probability of an item with relation

	関連がある項目の組数	抽出した項目の組数	OK	FN	FP	NG	再現率	確からしさ
手法1	31	28	25	5	2	1	80.65%	89.29%
手法2	31	30	28	3	2	0	90.32%	93.33%
手法3	31	25	23	7	1	1	74.19%	92.00%

表 3　関連がある項目の再現率と確からしさ（小項目）
Table 3　Recall and probability of an item with relation

	関連がある項目の組数	抽出した項目の組数	OK	FN	FP	NG	再現率	確からしさ
手法1	116	97	95	19	0	2	81.90%	97.94%
手法2	116	94	93	22	0	1	80.17%	98.94%
手法3	116	93	90	23	0	3	77.59%	96.77%

手法 1，2 では，小項目について基準 A と基準 B で新たな中項目に属するようになった組を正確に抽出することができた．よって，対象が大きく異なる基準間や基準のメジャーバージョンアップを行った基準の改版チェックを行う際に，使用すると有効だと思われる．また，手法 3 は，今回の手法の中では最も意味的な判定を重視しているものとなるので，同じような文言を多く使用する基準を使う場合や元の基準の構成があまり変化しないマイナーバージョンアップの改版チェック，新しい基準が元の基準の特定のカテゴリ（本実験でいうところの大項目）をトレースする形で作られている場合などに，有効だと思われる．

5.5　機能評価全体を通して

これらの実験によって参照ツリーを使って関係性を視覚化する，サンプルデータを提示するといった視覚的なサポートを行うことによって，セキュリティ評価者が陥りがちなヒューマンエラーを回避できることがわかった．また，テキスト間類似度を使った実験では基準間の関係情報を高い再現率で再現できることがわかり，新たな基準ができた時やローカル基準を作成する際にこの手法を使うことによってよりスムーズに新しい基準に対応するためのサポートができることがわかった．今回の実験で使用した手法 2，3 で，同じ項目の組で関連があると判定された組は，すべて正しい組み合わせであった．そのことから，目的の違う複数の手法を用いて関連情報を作成した場合には，各手法で異なる結果が出た項目の組には，エラーが含まれる可能性がある．このような組に，人の手によるチェックを入れることで，より正確な関連情報の抽出を行うことができると推察される．

6．今後の課題

サンプル提示機能については，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．

基準間の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り，すでに対応表がある基準同士をつかってテキスト間類似度を用いて関連情報を作成する実験を行ってきたが実際に対応表のない基準同士の関連情報作成の実験はまだ行えていないのでそういった実験を行っていく．

これまでの実験でギャップ分析および現状分析のフェーズで実験を行ってきた．しかしそれ以外にもセキュリティ評価実施するフェーズは多く存在する．その他には，詳細リスク分析を行っている段階や，すでに認証取得を行って，PDCA サイクルをすでに運用しているといった段階が，セキュリティ評価をするフェーズに該当する．したがって，その他のフェーズでも組織のセキュリティ評価実験を行い，その時点での有効性の検討をする．

7．まとめ

実験により，参照ツリーやサンプルの提示などによる視覚的なサポートによって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．専門的な知識を有している場合でも見落としてしまう可能性がある潜在的な影響度については参照関係の情報を用いることで評価にしっかりと反映できることが確認できた．また，知識不足の際に起こる可能性がある見落としや勘違いについても参照ツリーやサンプル提示による視覚的な情報は大変有効であることがわかった．

また，サンプル提示機能とデータ移行機能といったように複数の機能を効果的に連動することによってより機能の有効性を高めることができることがわかった．

参考文献

1) 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) TechTarget ジャパンホワイトペーパー：コンシューマデバイスのセキュリティ戦略計画のために考慮すべきポイント，http://wp.techtarget.itmedia.co.jp/contents/?cid=11501
4) 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
5) 芦野他：セキュリティ標準に基づいたセキュリティレベル評価技術の検討，情報処理学会 DPS 154・CSEC 60 合同研究発表会，Vol.2013-DPS-154 No.35 Vol.2013-CSEC-60 No.35
6) 髙橋, 勅使河原：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 CSS2008 論文集第 2 分冊, pp.815-819(2008)
7) 徳永：情報検索と言語処理, 東京大学出版会 (1999)
8) 髙橋他：セキュリティ標準間の関連情報作成手法の検討とその適応, 情報処理学会 CDS 7 研究会, 2013-CDS-7(1), pp.1-8, 2013.05
9) 松本他:形態素解析システム『茶筌』version 2.0 使用説明書 第二版, NAIST Technical Report, NAIST-IS-TR99012 (1999)
10) 髙橋, 勅使河原：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 CSEC 46 研究発表会 Vol.2009-CSEC-46, No.13(2009)
11) 髙橋, 勅使河原：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，情報処理学会 DPS 142・CSEC 48 合同研究発表会，Vol.2010-DPS-142 No.53 Vol.2010-CSEC-48 No.53
12) 髙橋, 勅使河原：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，DICOMO2011 論文集，pp.127 – 134
13) 髙橋, 勅使河原：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，情報処理学会 CSS2011 論文集，pp.666 – 671
14) 髙橋他：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へのテキスト類似度の応用, 情報処理学会 CSEC 58・SPT 4 合同研究発表会，Vol.2012-CSEC-58 No.36,Vol.2012-SPT-4 No.36(2012)