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改善とその適用

髙橋雄志† 篠宮紀彦† 勅使河原可海†

近年セキュリティのトレンドは外部認証機関によりセキュリティが保たれていることを示す事に移ってきた．認証を取得する際には，国際標準などを基準として対象を評価する．認証取得に向け，セキュリティ評価システムが活用されているが，基準の変化に対応する為には，それに合わせて個別のツールが必要であった．本研究では，評価基準とする基準の変更のみで内容や評価対象の変化に対応した評価を実現するプラットフォームの検討を行ってきた．基準が変わった場合に最初から評価し直さなければならないという問題に対し，基準間のデータ移行機能を提案しその有効性と発展性を示してきた．しかし，この機能を使用するためには基準間の関連性を示す情報が必要であるが定義されているとは限らない．これまで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を応用し基準の各項目同士の類似度から関連性を導き，関連を示す情報を取得する方法を提案し，その有効性が確認してきた．本稿では更に再現度を高めるべく，標準の文章構成に着目し，専門用語数に基づく重み付けを行った 5 つの方式の比較を行った．その結果総合的に高い有効性を示す方式を見出すことができた．

Improvement of a Security Evaluation Platform Based on International Standards and its Application

Yuji TAKAHASHI† Norihiko SHINOMIYA †
And
Yoshimi TESHIGAWARA†

1. 研究の背景と目的

近年，セキュリティ管理の目的は，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，2013 年 5 月 13 日現在で 4,277 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現場の状況に合わせた対応が必要となり，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．標準の改定などといっ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，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[4][5][6]．その中で，セキュリティ認証に関する知識が深くないユーザに対して認証取得を意識した対策選定，実施のサポートのために過去の事例に基づくサンプル提示を行う機能や関連情報を用いたデータ移行機能に関する実験を行ってその有効性の検証を行った[7][8]．さらに，データ移行機能についてはサンプル機能と連動させることでより機能の有効性を高めることができる

†創価大学大学院工学研科
Graduate School of Engineering, Soka University

ことがわかった[8]．また，データ移行機能をより有効に活用するために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を応用してデータ移行の際に使用する標準間の関連情報を作成する実験を行って高い再現度を示すことができた[9]．本稿では，文献[9]で行った実験から得られた，項目名の方が少ない文章量で本質的な内容を示していると思われるのでより関連情報を作成する上で重要であると推察できるという知見に基づき類似度算出手法の改良を行いより高い精度での関連情報の作成の為の実験を行った，合わせて専門用語を多く有する方がより重要であるという仮定をした場合の実験も並行して行いそれらの結果をまとめた．

2. 標準の分析と活用

2.1 関連する標準

本稿では，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 ファミリー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．Plan の段階で使用する場合は，現状分析の結果を入力し対策の抜け漏れの確認ができる．Do の段階では対策を実施していく段階で想定していた項目をカバーできないことがわかった場合にそのチェックをすることによって全体としての抜け漏れの確認ができる．Check の段階では対策実施段階で想定されていた通りに各対策が機能しているのかのチェックに利用でき，実際の状況に合わせて対応状況の変更を加えることで抜け漏れの確認ができる．Act の段階では Plan の段階と同様に再設定した対策の対応状況の抜け漏れが確認できる．

2.1.1 ISO/IEC 27000 ファミリー

ISO/IEC 27000 ファミリーとは，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．このファミリーは対象とする範囲が広く，代表的なセキュリティ管理対象である，プライバシー，機密，情報技術におけるセキュリティ課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．

このファミリー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対策を実装することが求められる．また情報セキュリティの運用は固定的なものではないので，ISMS には PDCA サイクルによる継続的なフィードバックと改善が要求される．ISO/IEC 27000 ファミリーは，現在のところ，2012 年末時点すでに 13 種類の標準が策定済みであり，他にも多くの標準が準備中となっている[10]．ISO/IEC 27000 ファミリー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．

2.1.2 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[11]．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，適用対象外のものは対象外であることを示すことを含めて，そのすべてを網羅している必要がある．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．

2.2 標準の構成

関連する標準では一般的に本文が論文における「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．

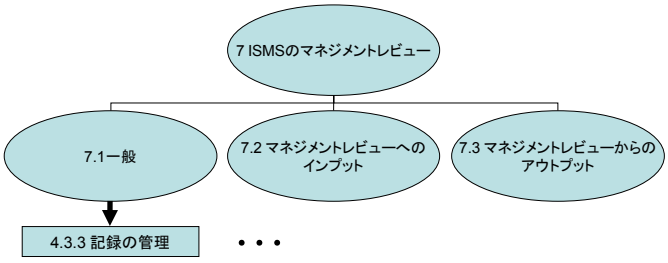

図 1 ISO/IEC 27001 の参照関係の例

Figure 1 Reference-related example of ISO/IEC 27001

2.3 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. 類似度算出について

3.1 類似度算出手法

本稿で用いている類似度算出手法は，近年盛んに行われている文書の分類や検索に関する研究において，文書間の類似度を算出する方法が多数提案されている中でも最も一般的な類似度算出手法を用いている．図 2 に一般的な類似度算出手順を示す．まず，類似度を算出する際に使用する各文書のテキスト情報を決定する（図 2 中①）．次に，決定された各文書のテキスト情報を形態素解析[12]により形態素に分解し，索引語（文書の内容を表す要素）を抽出する（図 2 中②）．形態素解析プログラムは奈良先端科学技術大学院大学で開発された「茶筌」[13]などがある．索引語の単位としては形態素や名詞などが挙げられる．そして，類似度を算出する際にノイズとなる語を不要語として削除する（図 2 中③）．さらに，抽出した語に対して重み付けを行う（図 2 中④）．重み付け手法としては，索引語頻度（TF（Term Frequency））や逆文書頻度（IDF（Inverse Document Frequency）），それらを組み合わせた TFIDF がよく用いられる[9]．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（図 2 中⑤）．

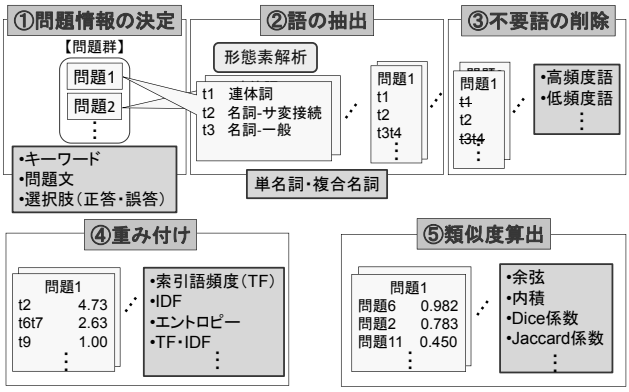

図 2 一般的な類似度算出手順

Figure 2 General procedure of calculating similarity

3.2 応用例

本稿で行った実験は異なる標準を用いて評価する際にすでに評価を行った標準の対応策の状況のデータを活用したいといった要求を想定している．

実験に使用したテキスト間類似度を算出する手法は，コンピュータを教育に応用する「e ラーニング」のうち，特に Web ブラウザやインターネット上の情報やシステムを利用する WBT（Web Based Training）のコンテンツに関する研究の中で同一の知識に関する問題を類似問題群としてまとめる技術としてすでに使われている手法を元にしている[14]．この文献[14]でいう類似問題群とは，それぞれの問題間のテキスト類似度を用いて同一の専門知識を問う問題の集合を指している．本稿ではそれぞれの基準で同一の対応策を求める要件を示す項目を判別する技術としてテキスト間類似度を用いている．

その他の応用例としては，基準となる標準が更新された場合に古い版と異なる章や新たにまとめられた章に移った項目を見つけたり，社内基準などのローカルな基準を作成する時に国際標準などのグローバルな基準を元にしている場合には，どの程度元となる標準の内容を反映できているのか，抜け漏れが発生していないかを確かめたり，すでに社内基準が設けられている場合にセキュリティ認証取得を目指すといった時に現状の基準であればどの程度取得を目指す標準に近い基準を満たしているのかを確認したりするケースを想定している．

4. プラットフォームの概要

4.1 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 3 に示す．

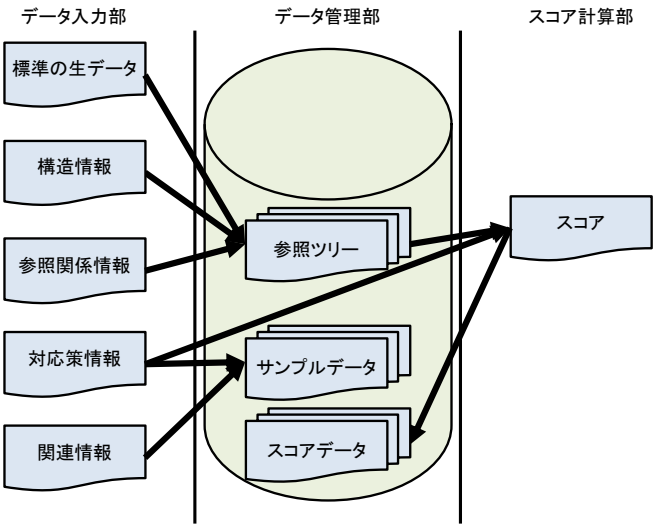

図 3 提案プラットフォームの構成

Figure 3 Structure of proposed platform

データ入力部で，標準の生データと，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（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．

4.2 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．複数の基準（標準）が登録されていてその基準同士に関連があり，それぞれの基準のどの項目とどの項目が同じ観点で対策を必要としているかを示している関連情報が提示されている場合はその情報も登録する．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．本研究ではこのように階層構造も参照関係の一部であるように定義することとする．

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評価値算出のための元データを提供する．

続いて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・項に該当する項目対する評価値であり，それらの項目を参照親に持つ参照ツリーを構成する各要素の対応状況から算出されるものとなる．実際にはデータ入力部で参照ツリーの情報を用いた対応策実施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対応状況のサンプル提示を行い，追加・変更の対応策の実施情報の入力を促す．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，その時データ管理部では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対応状況の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別途保存する．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）で対応状況の入力を行う際に提示されサンプル情報を参考にしながら入力作業を行うことができる．

新しい基準に対して評価を行う際に他の基準との関連情報が登録されている場合はデータ管理部でデータ移行機能を用いて元となる基準の対応状況のデータを元にサンプルデータを作成してデータ入力部で閲覧しながら入力作業をすることができる．

4.3 4.3　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．

5. 類似度による関連情報抽出実験

5.1 実験概要

すでに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．また，今回の実験では作成したデータを専門的な知識が十分ではないユーザに提示することを目的としているため，NG および FP の抑制を優先的し FN の抑制は考えていない．

5.2 実験環境

実験ではすでに関連情報が明示されている『ISO/IEC 27001 附属書 A』（以下，基準 A）と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』（以下，基準 B）の二つを用いてそれぞれの基準から見た各項目の同士の類似度算出を行った．これらを選んだ理由としては ISO/IEC 27001 のドキュメントの附録として対比表が公開されていることの他に国際的なセキュリティマネジメントの基準である ISO/IEC 27001 とその日本の国内版となる ISMS 認証基準 Ver.2.0 を用いることで 3.2 節であげた応用例にもあるように，国際標準と広い意味でのローカル標準としての国内標準の比較が実際に可能であるということを示すことも目的としている．また，具体的な対策に踏み込んだ附属書を使うことで定義などの表現がブレ難いものではなく表現の幅がある内容同士を比較することができ，より適切に有効性を示すことを目的としている．今回は各専門用語に対する重み付けについて，各専門用語に重み付けを行いその重み付けの違いによって関連情報の抽出にどのような差異が生まれるかを確認した．

5.3 重み付けについて

筆者らが行った先行研究の実験で「項目名」と「詳細記述」というように記述が分かれている場合に「項目名」の類似度が「詳細記述」の類似度より関連を示す場合に有効である可能性が高いという考察が行われている[9]．今回の実験ではこの考察に基づき専門語抽出を行った後に各専門用語に重み付けを行って精度の向上を図るものである．

今回の実験では以下の 5 つの方法で重み付けを行いその結果の比較検討を行う．

（方式 1）全ての専門用語に一律の重みをつける

今回の基準となる文献[9]での実験と同じく全ての専門用語に一律 1 の重みを与える．

（方式 2）標準全体の形態素数を用いる場合

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」に分けてその形態素数をカウントする（それぞれ Cnt.name，Cnt.detail とする）．その総合計を「項目名」と「詳細記述」のそれぞれで算出する（それぞれ Sum.cnt.name，Sum.cnt.detail とする）．

方式2Aでは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専門用語の重みとする．

そして，専門用語数が多い方がより重要な内容をしているのではないかという仮定に基づいて重み付けを行う方式の有効性を確認するために，方式 2B では方式 2A とは逆に項目名の各専門用語数を Sum.cnt.detail で，詳細記述の各専門用語数を Sum.cnt.name で割って重み付けをする．

この方式のメリットは各項目で専門用語数の偏りが合っても平均して各専門用語に重み付けができることであり，デメリットとしては各項目の文章量の特徴が反映されないということである．

（方式 3）項目ごとの専門用語数を用いる場合

方式 2 の際に算出した Cnt.name と Cnt.detail を用いて項目ごとに異なる専門用語の重み付けを行うものである．

その内，方式 3A は，方式 2A と同様に各専門用語に対して項目名は Cnt.name で，詳細記述は Cnt.detail で割ってそれぞれの専門用語の重みとする。一方，方式 3B では，方式 2B と同様に方式 3A と逆の要素で割り重み付けを行う。

この方式のメリットは項目ごとの文章量の特徴を反映することができるということであり，デメリットは専門用語数に偏りがあった場合にその影響を大きく受けてしまうということである．

5.4 実験の流れ

（手順 1）各基準の専門用語の抽出

基準 A，B において，「章・節・項」（以下，大項目・中項目・小項目）に含まれる文書間の類似度を算出するためにまず，専門用語抽出システム[15]により，専門用語を抽出する．ただし今回実験の対象となるのは提案している手法で重み付けを変えることができる中項目と小項目のみとなる．そのため大項目については今回の実験の対象外とする．また，各項目の専門用語数をカウントしておく．

（手順 2）各専門用語への重み付け

抽出されたすべての語に対して 5.3 節で述べた 5 つの方法を用いて重み付けを行う．

（手順 3）類似度の算出

手順 2 で作成した各基準のデータを余弦[12]により異なる基準間における類似度を算出する．作業は手順 1 と同様に中項目と小項目についてのみ行う．

（手順 4）関連がある項目の抽出

まず基準Aの各項目から見た類似度最大の項目を抽出する．続いて基準 B でも同様に各項目から見た類似度最大の項目を抽出する．抽出された項目がどちらから見ても一致しているもののみを関連がある項目としてピックアップする．

（手順 5）元データとの比較

手順 4 で抽出した関連がある項目が明示されている関連情報とどこまで一致しているのかを確認する．再現率は「正しく抽出された関連がある項目数」を「関連情報の数」で割ったものとして算出する．確からしさは「正しく抽出された関連がある項目数」を「抽出された関連がある項目数」で割ったものとして算出する．

（手順 6）エラー項目および差分の分析

FP，FN，NG となった項目すべてにおいてその原因分析

を実施する．

そして，重み付けを変えたことによって差が出た組み合わせについてもその原因分析を行う．

5.5 実験結果

(1)　手順 1：各基準の専門用語の抽出

今回の実験で用いた基準 A,B は共に大項目以外は項目名と詳細記述となっていたので，項目名と詳細記述をひとまとめとして専門用語の抽出を行った．その際に項目ごとに専門用語数のカウントを行った．その結果，基準 A では中項目で 2 項目，小項目で 5 項目，基準 B では中項目で 2 項目，小項目で 3 項目が詳細記述の方が専門用語の数が多くなり，また基準 A では中項目で 7 項目，小項目で 7 項目，基準 B では中項目で 6 項目，小項目で 9 項目が項目名と詳細記述で専門用語数が一致した．

(2)　手順 2：各専門用語への重み付け

各項目の専門用語にそれぞれ重み付けを行う．重み付けを行う際に項目名と詳細記述の両方で同じ専門用語が出現した際はより高い重み付けを行う方の重み付けを優先して専門用語に重み付けを行った．方式 1 では先の実験と同様に特別な重み付けを行わず全ての専門用語に同じ重みを与えた．方式 2A，2B では Sum.cnt.name と Sum.cnt.detail を用いて重み付けを行ったため項目ごとに重みのバラつきはなく基準ごとに同じ重み付けとなった．方式 3A，3B では項目ごとの専門用語数にはバラつきがあったため項目ごとの重み付けにもバラつきが生じた．

(3)　手順 3：類似度の算出

手順 2 で 5 つの方式で重み付けを行ったデータを用いて，中項目は中項目，小項目は小項目同士で，各項目総当たりで類似度の算出を行った．

(4)　手順 4：関連がある項目の抽出

基準 A の項目から見て基準 B で類似度最大となる項目でかつ，基準 B から見た時も基準 A の元の項目が類似度最大となる項目の抽出を行った結果を方式ごとにまとめると表 1 で示すようになった．

表 1　関連がある項目数

Table 1　Number of items with relation

	中項目		小項目	
	関連がある項目数	抽出した項目数	関連がある項目数	抽出した項目数
方式1	31	28	116	97
方式2A	31	30	116	94
方式2B	31	25	116	73
方式3A	31	24	116	93
方式3B	31	27	116	75

(5)　手順 5：元データとの比較

手順 4 で抽出された項目を基準 A と B の関連情報と比較を行った結果は表 2 および表 3 で示すようになった．

中項目では方式 2A で FN，NG が減少して再現率と確からしさの両方が方式 1 に比べ改善され，方式 3A では NG が減少し FN が増加したが確からしさが改善された．方式 2B と 3B ではエラーが増加し再現率，確からしさが共に方式 1 に比べて低い値となった．小項目では方式 2A のみが方式 1 に比べて確からしさが改善された．しかし FN が増加しているため再現率は低下した．その他の方式ではエラーが増加し再現率，確からしさが方式 1 に比べて低い値となった．

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 ratio and correctness 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
方式1	31	28	25	5	2	1	80.65%	89.29%
方式2A	31	30	28	3	2	0	**90.32%**	**93.33%**
方式2B	31	25	20	10	4	1	64.52%	80.00%
方式3A	31	24	22	9	2	0	70.97%	91.67%
方式3B	31	27	24	6	2	1	77.42%	88.89%

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 ratio and correctness 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
方式1	116	97	95	19	0	2	**81.90%**	97.94%
方式2A	116	94	93	22	0	1	80.17%	**98.94%**
方式2B	116	73	66	45	2	5	56.90%	90.41%
方式3A	116	93	90	24	1	2	77.59%	96.77%
方式3B	116	75	68	42	1	6	58.62%	90.67%

(6)　手順 6：エラー項目および差分の分析

中項目においては方式 2A，3A にて NG の数の減少が見られた．これは NG となった項目の組が項目名の方が詳細記述の部分よりもその特徴を示していたと推察できる．また，すべての方式で FP として検出された項目と，方式 1，2A，2B で共通して FP として検出された項目がそれぞれ 1 つずつあり詳細を調べた結果，該当する項目に対する大項目および小項目が元データで関連が定義されている項目であることがわかった．概念自体はかなり近いが枠組として別の枠組となっているケースであるとわかった．そして，方式 2A，3A の二つの方式だけで FN となった項目の組について調べた結果その組はその他の組と違って項目名だけ組を判断するのが難しく詳細記述を読んではじめて組が判別できるような内容となっていた．方式 3A，2B のみで FP で検出された項目の組では正しい組では項目名と詳細記述それぞれの専門用語数を調べた結果，項目名の専門用語数が詳細記述よりも多いという想定からはずれている項目であることがわかった．

小項目においては方式 2A・3A にて方式 1 における FN，NG となる項目を多く正しい組で検出できていたが方式 1 で検出できていた組で類似度が低かったものについて FN または NG（方式 3A では FP も含む）のエラーが発生しているために再現度が改善されず，方式 3A については確からしさの改善もされなかった．小項目では中項目以上に専門用語数の差が大きくその影響が大きかったと推察される．重みに直して比較すると最大値は基準 A で 11 倍，基準 B で 16 倍となった．

5.6 実験の考察

総合的には方式 2A が高い再現率と確からしさを示しており，この方式が有効であると考えられる．何故なら今回行った実験により，想定していた専門的な知識が十分ではないユーザに対してより確からしさの高いデータを供給できることになり間違った関連情報を使ってしまう危険性を軽減できたといえる．また，項目名と詳細記述とに分かれて記述されている基準についてそれぞれの専門用語数に基づいて重み付けを行うことで一部のエラーを回避できることがわかった．加えて，各項目の特徴をそのまま反映して類似度算出をするよりも基準全体として平均化して重み付けを行った方がより効果的にデータを抽出できることがわかった．しかし，一部の例外的な記述となっている項目の組については検出することができなかった．

また，小項目のように全体の文章量が多い場合は複数の算出手法でそれぞれ検出できたりできなかったりする項目の組が発生することがわかった．このような場合は複数の手法，例えば方式 1 と 2A のように違う視点で重み付けを行った結果を総合的に判断することにより正しい組を導き出すことも有効であると推察される．

そして，方式 2B，3B といった文章量（専門用語数）が多いほど重要な記述であるといった前提で重み付けを行った方式を試したことによりこのような基準同士の類似度を算出する際には専門用語数によって影響が変わるのではなく意味的な要素を含んで重み付けを行う方が有効であるということがわかった．

6. 今後の課題

今回の実験では項目名と詳細記述のそれぞれに属する専門用語に対する重み付けを変えることで一定の効果をあげることができた．しかし，類似度算出における重み付けの決定方向には他にも専門用語の出現頻度に着目するといったものなど他のアプローチ方法も存在している．今後は他のアプローチが基準同士の類似度算出において有効であるかを検討して有効性の検証をする．

その他にプラットフォーム全体の課題としては以下のものがある．

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．収集方法についてはサンプルの使用条件としてサンプルを使用して作成したデータはサンプルデータとして提出するルールを提案している．サンプルの信頼性についてはサンプルを収集する中央サーバを構築しサーバ側で機械的に信頼性が高いと判断できる基準として同じ対応策について一定件数以上同じ項目に対応していると登録があるものはそのまま採用し，一定数を下回る項目については人の目による確認を行い，その有効性を認めることができたら採用する方式を提案している．

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

本稿では，データ移行機能の充実のために類似度を用いる手法に対して各項目の専門用語数に着目して重み付けを行う手法の実験を行い有効性の確認をした．

実験により項目ごとに重み付けを行うより全体として平均化した重み付けを行った方が有効であることがわかった．これは項目ごとの専門用語数にバラつきがありそのバラつきによる影響を平均化した値を用いることで吸収できたものと推察できた．また，類似度を算出する際には意味的な要素を含んだ重み付けが大事であり単純な文章量では判断できないということがわかった．

今後は 6 章で述べた課題に取り組み，未だ実験を行っていない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) 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) 髙橋雄志, 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) 髙橋雄志, 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) 髙橋雄志, 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(2010)

7) 髙橋雄志, 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(2011)
8) 髙橋雄志, 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データ移行機能の検討，情報処理学会コンピュータセキュリティシンポジウム 2011(CSS2011)論文集，pp.666 － 671(2011)
9) 髙橋雄志, 池田信一，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へのテキスト類似度の応用, 情報処理学会第 58 回 CSEC・第 4 回 SPT 合同研究発表会, Vol.2012-CSEC-58 No.36,Vol.2012-SPT-4 No.36(2012)
10) 情報マネジメントシステム推進センター：国際動向「ISO/IEC 27000 ファミリーについて」 http://www.isms.jipdec.jp/27000family_20121210.pdf
11) ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005
12) 徳永健伸: 情報検索と言語処理, 東京大学出版会 (1999)
13) 松本祐治, 北内啓, 山下達雄, 平野善隆, 松田寛, 高岡一馬, 浅原正幸: 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, 奈良先端科学技術大学院大学 (1999)
14) 池田信一, 高木輝彦, 高木正則, 勅使河原可海：多肢選択式項目の出題パターンと選択肢の類似性に着目した難易度推定方法の提案と評価, 情報処理学会論文誌，Vol.54 No.1, pp.33-44, 2013.1
15) 東京大学中川研究室・横浜国立大学森研究室: 専門用語自動抽出システム，http://gensen.dl.itc.u-tokyo.ac.jp/