Vol.2013-CDS-7 No.1
2013/5/23

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

髙橋雄志[†]　篠宮紀彦[†]　勅使河原可海[†]

近年，多くのセキュリティの脅威に対して自ら対策を行うのみだけではなく，セキュリティ認証の取得といった形で外部認証機関によりセキュリティが確保されていることを証明することはより重要な要素となってきている．そのようなセキュリティ認証を取得する際には，国際標準などを基準として認証すべき対象を評価することになる．また，近年では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おり，様々な標準化も積極的に行われている．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が，標準の変化に対応するためには，基準に合わせてそれぞれ個別のツールが必要であった．そこで，本研究では，このように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の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．

こうしたセキュリティ認証を取得するためにはセキュリティ技術に対する知識と評価に用いる標準に対する知識が問われる，認証取得の担当者が十分な知識を持っている可能性は低く，知識不足の問題が存在する．

こうした問題について，サンプル提示機能を用いてサンプル提示を行うことで知識不足を補うことを提案し，中でも評価対象が変わったり，基準となる標準が更新されたりして基準となる標準が変わった場合に最初から評価しなおさなければならないという問題に対してフォーカスを当て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元となる基準間の関連性を示す情報が必要となるがこうした情報が定義されているとは限らない．

そこで，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標準の各項目同士の類似度から関連性を導き，関連性を示す情報を取得する方法を提案し，具体的な標準を用いて評価実験を行い高い再現度を示すことができその有効性が確認できた．本稿では類似度を算出する際に各語に重み付けを行わない場合，専門用語数によって重み付けをする場合，階層構造による階層的な類似度を用いる場合の 3 つの方法で最終的な類似度を定義する．そして，定義された類似度を元に関連情報の抽出を行いそれぞれの場合での有効性の検証を行った．その結果，それぞれの手法は，関連がある項目の再現率と確からしさに高い値を示したが，手法 2 が総合的に良い結果を出すことができた．さらに，その結果から今後の課題としてセキュリティ標準以外への適応の可能性について考察した．

A Study on the Pertinent Information Creation Methods Between Security Standards and its Application

YUJI TAKAHASHI[†]　NORIHIKO SHINOMIYA[†]
YOSHIMI TESHIGAWARA[†]

It becomes more important for the corporations to be attested by the external certification organizations to demonstrate the corporate security against the many threats including emerging cyber attacks. In order to obtain acquisition of security attestation, the target organization is evaluated based on the international standards. Moreover, in recent years, the security technology about management of consumer devices is focused, and various standardizations are performed positively. 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. 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.

In order to obtain acquisition of security attestation, we need the knowledge over security technology and the related standards used for evaluation. However, it happens that the person in charge of acquisition of security attestation has not enough knowledge, and deficient knowledge becomes a problem.

For solving such a problem we proposed to compensate the knowledge deficiency by using a sample presentation function. When the standards changes or updated, the data conversion method was proposed to the problem that it must reevaluate from the beginning, and the validity has been shown. However, in order to use data conversion method, the information of relationship between the standards is needed.

The method of calculating similarity between texts currently used in the field of natural language processing is applied, and gets information of relationship by calculating similarity between standards. In addition validity of the proposed method is also confirmed by the experiment using an actual standard. In this paper, we proposed 3 methods of calculating similarity to get information of relationship. The method 1 uses flat weighting to each word. The method 2 uses variable weighting corresponding to the number of words. The method 3 calculates the hierarchical similarity by a layered structure. We verified the validity in each method by extracting information of relationship based on the above defined similarity and found that each method showed high recall and probability of an item with relation. In particular, the method 2 showed overall good results. In addition, we considered the possibility to apply our methods to other standards than security standards as a future work from the result.

[†] 創価大学大学院工学研究科
Graduate School of Engineering, Soka University

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 4 月 23 日現在で 4,268 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，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[4]．同様に，IT システムのセキュリティ機能の設計段階で，ISO/IEC 27000 ファミリー，内閣官房情報セキュリティセンターが策定した政府機関統一基準[5]，クレジットカード業界が策定する Payment Card Industry Data Security Standard(PCI-DSS)[6]などの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[7]．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，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[8]．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[9]．そして，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[10][11]．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ことがわかった[11]．この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[12]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てきた[13][14]．本稿では，これまでに検討を行ってきた関連情報を作成手法に加えて標準の階層構造の概念を利用した類似度算出を用いて関連情報を作成し，それぞれの手法のメリット，デメリットの考察を行い，それぞれの手法が最も有効性が高くなるケースの検討を行った．

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-Act）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および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 サイクルの特定の場面でしか使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 **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 シリーズは，現在のところ，2011 年末時点すでに 10 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[15]. 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．

2.1.2 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[16]. 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が示すことを含めて，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　ISO/IEC 27001 の参照関係の例で示すような形で表現する．

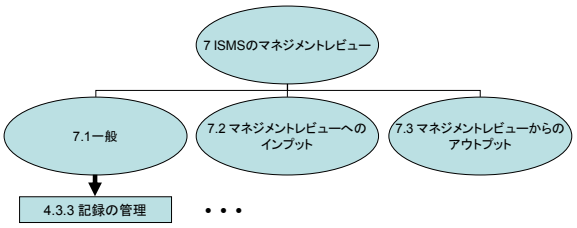

図 1　ISO/IEC 27001 の参照関係の例

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」[17]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 IDF（Inverse Document Frequency），それらを組み合わせた TFIDF がよく用いられる[12]．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 1 中⑤）．

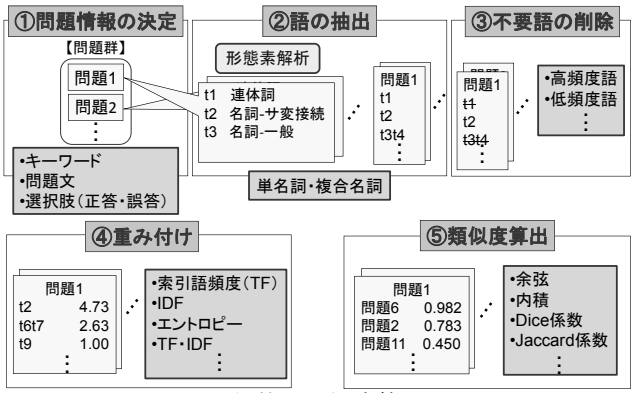

図 2　一般的な類似度算出手順

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．

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．

こういった応用をすることによって，これから新たに定義されていく標準にセキュリティに関する項目を加える際には元からある標準の項目と照らし合わせて要求条件が等しい項目を見つけることができたり，新規の標準を定義する際にすでに定義されている目的を同じくする標準との親和性を確かめたりすることが可能となってくる．

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．

データ入力部で，評価基準となる標準の生データと，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．

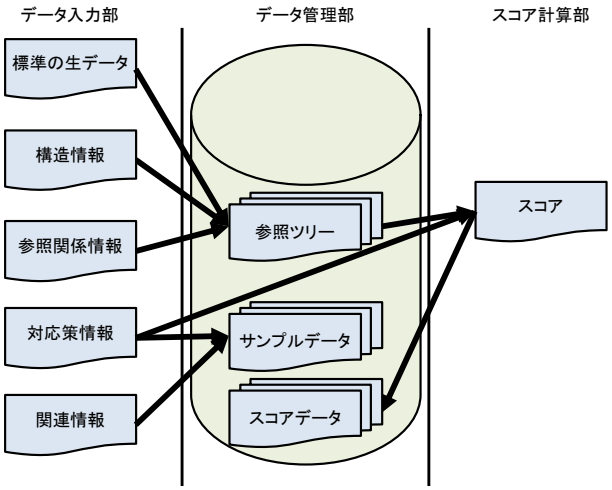

図 3　提案プラットフォームの構成

Figure 3　Structure of proposed platform

4.2 データ移行機能

このセキュリティ評価プラットフォームにおけるデータ移行機能とは，すでにある評価基準（以下，基準 X という）に基づくセキュリティ評価を行ったデータが存在しかつ，これからセキュリティ評価を行う評価基準（基準 Y という）と評価済みの評価基準との間の関連情報が登録されている場合に，評価済みのデータを新しい評価基準向けのデータに変換する機能となる．

はじめに基準 X で通常通り対応策の登録を行い，セキュリティ評価を行う．次に，登録されている基準 X における対応策情報を関連情報に基づき基準 Y のサンプルデータに変換する．この時直接基準 Y の対応策情報に変換せずあえてサンプルの形を取るのは関連情報が定義されていたとしてもより条件が厳しくなっていたり，逆に条件が緩くなっていたり，適応範囲が異なっていたりと一概に同じ対応策で条件を満たせるわけではないということがわかっているからである．

本稿では，このデータ移行機能で用いる関連情報が定義されていない場合に基準間の関連情報を半自動的に作成する手法を検討している．

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評価基準を用いて，各項目間の類似度を算出する．算出した類似度は 0〜1 の値を取る.類似度が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(No Good)としてそれぞれについて詳細の分析考察を行った.

今回の実験では後述する 3 種類の手法で類似度を算出して関連情報の作成を行う．その後，作成された関連情報よりどのような場合にはどの算出手法によって類似度を求めることが有効であるかの考察を行う.

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 という）と『ISMS 認証基準 Ver.2.0 附属書「詳細管理策」』（以下，基準 B という）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（以下，元データという）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 節の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．本実験では各専門用語に対する重み付けについて各専門用語に一律 1 の重みを与えた場合（以下，手法 1 という），各専門用語に基準全体の専門用語数に依存する重み付けを行った場合（以下，手法 2 という），手法 1 で算出した類似度を階層的に掛け合わせた場合（以下，手法 3 という）の 3 種類の類似度から関連情報を作成してそれぞれの再現度の確認を行うものとする.

5.3 実験の流れ

5.3.1 手法 1：一律 1 の重みを与える場合

（手順 1）各基準の専門用語の抽出および重みづけ

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[18]により，大項目それぞれに含まれる専門用語を抽出する．次に，抽出されたすべての語に対して重み付けを行う．本手法では各専門用語に対する重み付けは一律 1 とする．中項目と小項目についても同様の専門用語抽出と重みづけを行う.

（手順 2）類似度の算出

手順 1 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．手順 1 と同様に中項目と小項目についても同様の作業を行う.

（手順 3）関連がある項目の抽出

まず基準 A の各項目から見た基準 B で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基準 A で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 4）元データとの比較

手順 3 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 5）エラー項目の分析

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.

5.3.2 手法 2：専門用語数に基づく重み付けを行う

この手法では文献[13]で行った実験で「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に基づき手法 1 における手順 1 の中の専門用語の重み付けについて以下の重み付けを行う．まず，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．次にその総合計を「項目名」と「詳細記述」のそれぞれで算出する．最後に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.

手順 2 以降の手順は手法 1 に順ずる.

5.3.3 手法 3：類似度を階層的に掛け合わせた場合

最初に，手法 1 の手順 1〜2 に準ずる形で類似度を算出する．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.

手順 3 以降の手順は手法 1 に準ずる.

5.4 実験結果

5.4.1 手法 1

大中小全ての項目について用語抽出を行ってそれぞれ

の専門用語について一律 1 の重みを付けて各項目間の類似度算出を行った．その後関連情報の抽出を行った結果を表 1 に示す．

表 1　関連がある項目数（手法 1）
Table 1　Number of items with relation

	全項目数		抽出した項目数
	基準A	基準B	
大項目	10	10	8
中項目	39	36	31
小項目	133	127	108

そして，抽出した項目の組を元データと比較して分類した結果を表 2 に示す．

表 2　関連がある項目の再現率と確からしさ（手法 1）
Table 2　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%

5.4.2 手法 2

手法 1 と同様の手順で用語抽出を行う．次に大項目は項目名と詳細記述に分かれて書かれていないため専門用語の重み付けは手法 1 と同様に 1 とするが，中小項目については項目名で使われている専門用語数と詳細記述で使われている専門用語数をそれぞれカウントして基準全体の総数を記録する．そして，その比率に合わせた重み付けを項目名と詳細記述の各専門用語に与える．その後の類似度計算，関連情報の抽出，組の分類は手法 1 に準ずる．その結果を表 3 表 4 に示す．

表 3　関連がある項目数（手法 2）
Table 3　Number of items with relation

	全項目数		抽出した項目数
	基準A	基準B	
大項目	10	10	8
中項目	39	36	31
小項目	133	127	108

表 4　関連がある項目の再現率と確からしさ（手法 2）
Table 4　Recall and probability of an item with relation

	関連がある	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	30	28	3	2	0	90.32%	93.33%
小項目	116	94	93	22	0	1	80.17%	98.94%

5.4.3 手法 3

手法 3 では手法 1 で算出した類似度を使って階層的な類似度を算出する．大項目については階層の最上位となるため手法 1 および 2 と同じ結果となった．階層的な類似度を算出した後の関連情報の抽出, 組の分類は手法 1 に準ずる．その結果を表 5，表 6 に示す．

表 5　関連がある項目数（手法 3）
Table 5　Number of items with relation

	全項目数		抽出した項目数
	基準A	基準B	
大項目	10	10	8
中項目	39	36	25
小項目	133	127	93

表 6　関連がある項目の再現率と確からしさ（手法 3）
Table 6　Recall and probability of an item with relation

	関連がある	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	25	23	7	1	1	74.19%	92.00%
小項目	116	93	90	23	0	3	77.59%	96.77%

5.4.4 エラー項目の分析

手法 1，2，3 の結果を比較すると大項目については項目名と詳細記述に分かれているわけでもなく更に上位の概念がないことから差が生じないので，中小項目の分類結果を項目レベル毎の表にまとめると表 7，表 8 に示すようになる．

表 7　関連がある項目の再現率と確からしさ（中項目）
Table 7　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
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 8　関連がある項目の再現率と確からしさ（小項目）
Table 8　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
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%

関連情報を作成する際には FP と NG の二つのエラーが発し，かつそれを間違った組であると認識できないことが一番の問題となるので手法 2 が総合的に良い結果を出すことができたといえる．

大項目，中項目，小項目のそれぞれを見ると文量の少ない大項目では手順 1 における専門用語の抽出時点でより適切な判断をすることができれば，FN のうち 1 つが正しい

組み合わせで導くことができ，もう一方の FN なった項目についても類似語を正しく判別できていれば正しい組み合わせで導くことができたことがわかった．

中項目に関しては手法 2，3 が手法 1 よりも高い確からしさを示すことができていることから，それぞれの手法を使用する適切な場面があることが伺える．手法 1，2 の FP となる項目の組は 2 つとも同じであるが手法 3 では発生していない．これは文言的には大変似ているが関連がない項目で階層を理解していないと判断が難しいケースといえる．また手法 1, 3 の NG となる項目の組は同じで手法 2 では正しい項目の組を抽出している．こちらの場合も文言的に似ているということに変わりは無いが項目名の類似度が高く詳細記述の表記内容によって誤った組を抽出してしまっているものとなる．このエラーは人の目によるチェックで回避することが容易なエラーであるといえる．

小項目については FP となる項目の組は現れなかった．NG となる項目の組については手法 1，2，3 でどの組み合わせでも共通の項目の組はなかった．手法 2 が数としては 1 組と最も少なかったが類似度は 0.470…と比較的高く，手法 3 が数としては 3 組と最も多かったが 0.258…～0.094…と他の手法に比べて非常に低い値を示した．それぞれの項目の組を視認すると類似度が低いことからもわかるように関連がないことが容易に判別できる組となっていた．

5.5 実験の考察

今回は比較的内容の近い基準同士を用いたが，テキスト類似度を用いて関連のある項目を抽出することで高い再現度を得ることができることがわかった．とりわけ抽出された項目の確からしさは非常に高い値を示すことがわかった．また，エラーの原因に文言の解析時に適切な範囲で単語が区切られていないというものがあったり，技術用語を多数使用している故に自動で用語同士が同じ意味を指していると判定できずに類似度が下がってしまい抽出できなかったり，といったものがあった．このことより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用いて基準間の類似度を求めて関連がある項目を抽出する手法が有効であるとわかった．また，類似度の算出方法に意味的な重み付けが工夫を加えることによってより高い再現度，確からしさが得ことができた．

また，今回検証を行った手法の他にも各専門用語の使用頻度などを用いる方法など他にも意味的な解釈をする手法がテキスト類似度を用いた類似問題群作成[19]に使用されているのでそれらを応用することによって結果が変わってくる可能性もある．

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性格に抽出することができたので対象が大きくこと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．

また，今回の実験で使用した手法 2，3 で関連があると判定された同じ項目の組はすべて正しい組み合わせであった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，およびすべての手法で同じ項目の組を示さないものにはエラーが含まれる可能性があるとして人の手によるチェックを入れる必要がある項目の組であると判定することができるものと思われる．

6. 今後の課題

実験ではすでに関連情報がある基準同士の類似度を求めて関連がある項目の抽出を行った．しかし一部の項目について間違った項目への関連を示す（FP および NG）といった問題が発生している．こういったエラーについてより意味的な類似度を求める手法の適応を行うなどで文章解析精度を高めて対応していきたい．

また，プラットフォーム全体の課題としては，これま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を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などが，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ことによって提案プラットフォームが PDCA サイクルのすべてのフェーズで使用できることの確認を行っていく．

7. まとめ

本稿では，セキュリティ評価プラットフォームのデータ移行機能をより有効活用するために，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基準間の各項目同士の類似度を算出した結果から関連性を導き出し関連性を示す情報を取得する実験を行いその有効性について検討した．その際に複数の手法を用いてそれぞれの手法がどういった場面で有効であるかの考察を行った．

関連情報が明示されている 2 つの基準を用いた実験により，高い再現度で，かつ高い確からしさをもつ関連情報を作成できることがわかった．このように関連情報を作成することができればこれまで基準が変わって再評価をしなければいけなかった際のロールバックを軽減することができ

ることがわかった．同様に基準が更新された場合も同じように関連情報を作成することによって更新によるセキュリティの再評価に対しても高い効果を得られるのではないかということがわかった．また，シンプルな類似度算出手法で高い再現度，高い確からしさを示すことができたのでより的確な手法を用いて関連情報を作成することで更に高い再現度，確からしさを得られることが予想される．

そして，今回実験で使用した手法はそれぞれについて利点があり利用目的に合わせて使用することでより大きな効果を得ることができるものであるといえる．今後のコンシューマデバイスやその他のセキュリティに関する新たな標準化の流れで提案した手法を使うことにより素早く新しい標準を理解し活用できるようになると予想される．

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，セキュリティ評価プラットフォーム全体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) 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) 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
5) 内閣官房情報セキュリティセンター: 「政府機関の情報セキュリティ対策のための統一基準群(平成 24 年度版)」について，http://www.nisc.go.jp/active/general/kijun24.html
6) Payment Card Industry Security Standards Council: PCI SSC Data Security Standards, https://www.pcisecuritystandards.org/security_standards/
7) 芦野佑樹，森田陽一郎，小泉純，岡村利彦：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，第 154 回 マルチメディア通信と分散処理・第 60 回 コンピュータセキュリティ合同研究発表会，Vol.2013-DPS-154 No.35 Vol.2013-CSEC-60 No.35
8) 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)
9) 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)
10) 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
11) 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，マ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
12) 徳永健伸: 情報検索と言語処理, 東京大学出版会 (1999).
13) 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)
14) Yuji Takahashi and Yoshimi Teshigawara : Design and Development of a Security Evaluation Platform Based on International Standards, International Journal of Informatics Society, in print
15) 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.or.jp/27000family_20111220.pdf
16) ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005
17) 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『茶茎』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).
18) 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
19) 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