Vol.2012-CSEC-58 No.36
Vol.2012-SPT-4 No.36
2012/7/20

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

髙橋雄志[†]　池田信一[†]　勅使河原可海[†]

近年企業ではサイバーアタックなどの多くのセキュリティの脅威に対して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取得に対し，国際標準等を基準として認証すべき対象を評価する．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が，標準の変化に対応するためには，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．分野ごとにカバーすべき項目をすべて網羅するためにはその分野の構造と各項目からの参照関係を的確に把握しなければならないという網羅性の問題があり，中でも対象が変わったり，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データ移行機能，例えば ISO/IEC 27001 から ISMS へのデータ移行を提案しその有効性を示してきた．しかし，データ移行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．本稿では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その有効性を確認した．

Application of Calculating Similarity Between Texts of a Security Evaluation Platform Based on International Standards

YUJI TAKAHASHI[†]　SHINICHI IKEDA[†]
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. 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. 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. When the standards changes or updated, the data conversion method, for example convert form ISO/IEC 27001 into ISMS, 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. In this paper, 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.

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，2012 年 6 月 6 日現在で 4,066 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

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

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]．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．その結果，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ることができ，評価項目と各項目の関係に着目し影響度の算出方式を変えて評価値を算出する実験も行った[5][6][7]．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[7][8]．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[8]．本稿では，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[9]を応用し標準間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実験を行いその有効性を確認した．

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[10]．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[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．

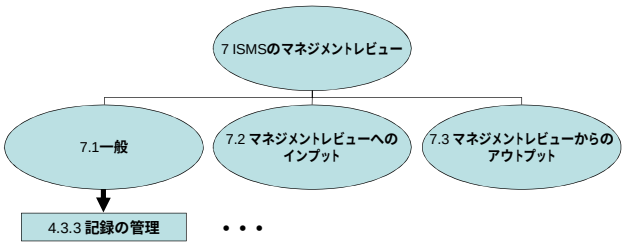

図 1　ISO/IEC 27001 の参照関係の例
Figure 1　Reference-related example of ISO/IEC 27001.

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[9]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」[12]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[9].

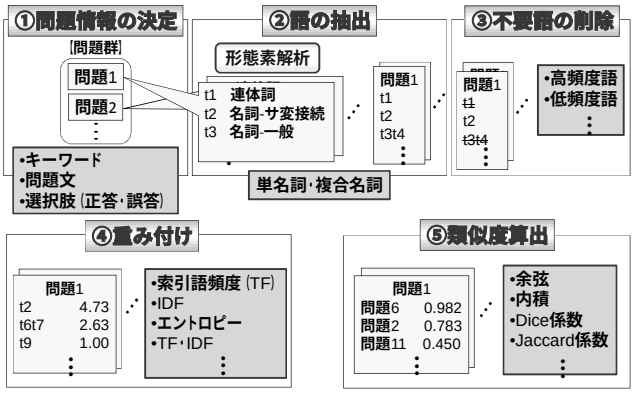

図 2　一般的な類似度算出手順
Figure 2　General procedure of calculating similarity.

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．

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，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．

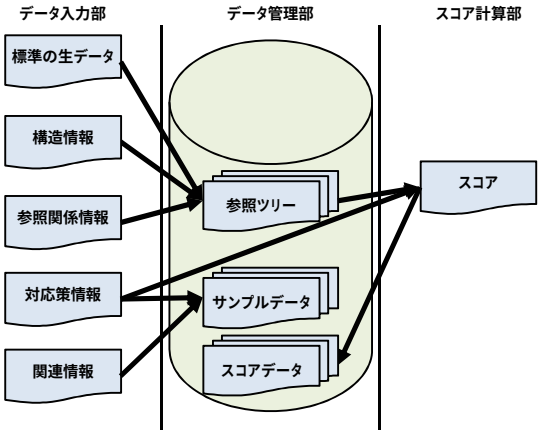

図 3　提案プラットフォームの構成

Figure 3　Structure of proposed platform

4.2 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，図 4 で示すように，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．

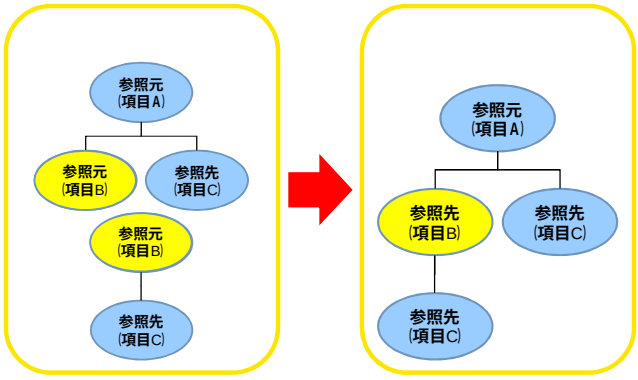

図 4　参照ツリー作成例

Figure 4　Sample of reference tree

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 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．また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．

4.4 プラットフォームのシステム構成

本プラットフォームは Visual Basic を用いてシステム開発を行ってこれまで様々な実験を行ってきた．まずプラットフォーム全体をひとつのプログラムとして構成し，基準と階層構造の情報と参照関係の情報を登録した後に参照ツリーを構成するための情報を作る部分，実際に参照ツリーを表示させる部分，対応策の状況を整理する部分，評価値計算を行う部分をそれぞれ独立したプログラムとして構築している．これらの部分はそれぞれ担当する処理をバックグラウンドで行うことによってシステムの稼働を円滑に行えるようになっている．例えば最初にデータ登録を行った際やデータの変更を行った際に行われる基準全体の参照関係の変更をバックグラウンドで行うことによって変更中であっても過去のデータの閲覧をすることが可能となる．また，参照ツリーの表示，対応策の状況の変更や評価値計算といった処理に時間がかかる部分を独立したプログラムとして稼働させることによってプラットフォームの本体は常に稼働させることができるようになっている．

それとは別に評価値計算の部分を独立させることにより複数の評価値計算方法を導入する（または試す）際にその部分のみを入れ替えることによってスムーズに新しい評価値計算方法に変更することが可能となっている．同様に参照ツリー表示の部分も使用者に要望に合わせたプログラムに差し替えてより使用者の好みに合った表示プログラムを導入することができるようになっている．

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．

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．

5.3 実験の流れ

（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[13]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．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[9]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 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．

5.4 実験結果

(1) 手順 1：各基準の専門用語の抽出および重みづけ

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および重みづけを行った．重みづけについては，今回の実験では，最も単純な手法として 2 進重みを適用している．これは，抽出されたすべての語に対して重み 1 を付与する．

(2) 手順 2：類似度の算出

手順 1 で作成したデータを用いて，大項目は大項目，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．

(3) 手順 3：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は表 1・表 2・表 3 で示すように，大項目で 8，中項目で 31，小項目で 108 件のデータが「関連がある項目」となった.

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

全項目数		抽出した項目数
基準A	基準B	
10	10	8

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

全項目数		抽出した項目数
基準A	基準B	
39	36	31

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

全項目数		抽出した項目数
基準A	基準B	
133	127	108

(4) 手順 4：元データとの比較

手順 3 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 4･表 5･表 6 で示すようになり, 大項目，中項目，小項目の全てで 77%を超える再現率を示し，確からしさはいずれも 90%を超える高い値を示す結果となった.

表 4　関連がある項目の再現率と確からしさ（大項目）
Table 4　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
10	8	8	2	0	0	80.00%	100.00%

表 5　関連がある項目の再現率と確からしさ（中項目）
Table 5　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
36	31	28	5	2	1	77.78%	90.32%

表 6　関連がある項目の再現率と確からしさ（小項目）
Table 6　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
127	108	106	19	0	2	83.46%	98.15%

(5) 手順 5：エラー項目の分析

FN 26 件，FP 2 件，NG 3 件それぞれの組合せについてエラー発生の原因を究明するべく基準 A,B の両方から見た各項目への類似度，各項目の文言を詳細に確認した．その結果エラーを出している項目のほとんどが低い類似度を示していることがわかった.

大項目，中項目，小項目のそれぞれを見ると文章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. 中項目では FP, NG として検出された 3 つの組合せはいずれも類似度が 0.5 を下回る結果となっており低い値を取っている．また，NG となった項目は項目名だけであれば類似度 1 となり完全一致しているが詳細記述の部分を合わせることで類似度が低下しているという結果になった．FN となっている組合せについては NG の時のように項目名が一致または高い類似度を示しているケースもあるが，基準 A，B のどちらから見ても最大類似度が低く片側から見たら最大であるがもう一方から見ると次点や次々点の値を取り僅差で検出できなかったケースと全体的に類似度が低くすべての組合せで 0.5 を下回っているといったケースに分類することができた．小項目については FP となる組合せは現れなかった．が，NG の組合せが 2 つありその両方が片側から見たら最大の類似度を示しもう一方から見るとそれぞれ次点，次々点の類似度を取っているものであった． FN となる組合せは 19 組と比較的多く検出されたが一部の組合せを除けば中項目の時と同じ 2 つのケースに分類することができた.

以上の分析結果より以下の知見を得ることができた.

① 類似度の最大値が 0.5 を下回るような低い値を示す項目は関連する項目がないことが多い
② 記述形式が項目名と詳細記述と分かれている場合は項目名の方の類似度がより重要となってくる
③ 双方からの類似度最大が同じ項目をささず関連を示す項目がないと判断された場合は類似度上位の項目を含めて検討すると関連する項目を検出できる場合が多くある

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．今回類似度の算出にあたりシンプルな方法を用いて類似度の算出を行ったにも関わらず全体を通して高い再現度, 確からしさを示すことができた. 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,類似度の算出方法を改善することによってより高い再現度,確からしさが得られると予想される結果となった.

また，サンプル提示を行うためのデータを作成するという性質上 FP，NG といったエラーについては FN の数がある程度増加しても発生を食い止めることが大事であると思われる．例えば項目名と詳細記述といったように文言が分かれている場合は今回のような重み付けではなく項目名の方が重要視される重みづけを行ったり，基準が階層構造を取っているので上位の項目（小項目に対する中項目や中項目に対する大項目）の関連の検出の有無や類似度を考慮したりといったことで結果を改良できるのではないかと予想される．

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などで文章解析精度を高めて対応していきたい．例えば基準の構成情報となる階層構造や参照関係を示す情報を反映させたり，項目文の構成が項目名と詳細記述に分かれているようなものであれば項目名に対する重み付けを詳細記述部分よりも重くしたりといったような実験を予定している．

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．

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検討している．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ものをサンプルとして配信する仕組みを検討している．その判断基準としては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検討している．

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．

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．

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) 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

Vol.2012-CSEC-58 No.36
Vol.2012-SPT-4 No.36
2012/7/20

8) 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
9) 徳永健伸: 情報検索と言語処理，東京大学出版会 (1999).
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.or.jp/27000family_20111220.pdf
11) ISO/IEC 27001 Information technology - Security techniques - Information security management system - Requirements, 2005
12) 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).
13) 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