情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.3　No.4　22–32 (Dec. 2013)

研究論文

# 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[1,a)]　篠宮 紀彦[1]　勅使河原 可海[1,†1]

受付日 2013年4月25日, 採録日 2013年9月13日

**概要**：近年，組織の安全性の確保およ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．その認証取得のために多くのセキュリティ標準が策定されているが，それらを統合的に扱う環境はまだない．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．個々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る．これらの問題に対して我々は個別の評価ツールではなく，統合的な対策評価を行えるセキュリティ評価プラットフォームを提案してきた．この評価プラットフォームでは網羅性の問題に関しては，セキュリティ標準の特徴である階層構造，参照関係を視覚化することで対処している．また，専門知識に関する問題については，過去のデータに基づくサンプルの作成，提示を行う機能で対応している．さらに統合的な環境を実現するために異なるセキュリティ標準間のデータ移行機能を提供している．このため，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を出す手法を応用し，標準間の関連情報を導き出す方法を提案してきた．具体的な標準を用いて異なる標準間の関連情報の再現を試みて，高い再現率を示したことからその有効性を確認できた．本論文ではこの関連情報を導く実験で得られた知見に基づき，新たに 2 つの手法を提案し比較検証を行った．1 つの手法は文章内で使用されている用語数に着目した重みづけを行う方法であり，もう 1 つの手法は標準の特徴情報のうち階層構造に関する情報を使用する方法である．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，前者の手法が総合的に良い結果を出すことができた．

**キーワード**：国際標準，ISO/IEC 27000 ファミリ，ISMS，セキュリティマネジメント

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

Yuji Takahashi[1,a)]　Norihiko Shinomiya[1]　Yoshimi Teshigawara[1,†1]

Received: April 25, 2013, Accepted: September 13, 2013

***Abstract:*** It becomes more important for the corporations to be attested by the external certification organizations for showing that is keeping security and countermeasure. Lot of security standards is exited for attestation acquisition, but there is still no such environment that provides integrative solutions. Moreover, in recent years, the security technology regarding management of consumer devices is focused, and various standardizations are performed positively. Each security attestation has problems that it requires completeness of countermeasures and specialized knowledge of 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. For solving such problems we provided to completeness of standards by visualizing hierarchical structure and reference relation. In addition, we provided to compensate the knowledge deficiency by using a sample presentation function. Furthermore, we provided to the data conversion function between different security standards in order to get integrative solutions. We proposed that the method of calculating similarity between texts currently used in the field of natural language processing is applied, and it gets information of relationship by calculating similarity between standards. In this paper, we proposed two new methods of getting information of relationship based on the knowledge acquired in the preceding experiment. One method uses variable weighting corresponding to the number of words. The other method calculates the hierarchical similarity by a layered structure. We performed the experiment to compare between these two methods. In the results, 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 former showed overall good results.

***Keywords:*** international standard, ISO/IEC 27000, ISMS (Information Security Management System), security management

## 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．これにともない，組織の安全性の確保およ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 6 月 28 日現在で 4,310 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ともなう．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，ISO/IEC 27000 ファミリ，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十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 [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統合的な環境を提供できるプラットフォームのプロトタイプ開発を行ってきた．そして，実際に ISO/IEC 27000 ファミリ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，その有効性を示してきた [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と分かった [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どうし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 [13], [14]．本論文では，文献 [14] で行った関連情報作成実験を準備実験と位置づけ，そこで得られた知見に基づく新たな手法 2 つを使って，関連情報の生成を行った．1 つは，専門用語数に着目した手法となり，もう 1 つは，標準の階層構造の概念に着目した類似度算出となる．それぞれの手法のメリッ

[1] 創価大学大学院工学研究科
Graduate School of Engineering, Soka University, Hachioji, Tokyo 192–8577, Japan
[†1] 現在，東京電機大学未来科学部
Presently with School of Science and Technology for Future Life, Tokyo Denki University
[a)] e08d5203@soka.ac.jp

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. 関連研究

### 2.1 セキュリティオントロジに関する研究

Secure Business Austria の Fenz らによって Security Ontology [15], [16] を用いた ISO/IEC 27001 に対応したセキュリティ対策を行うための研究が行われている [17]．この研究では，ISO/IEC 27001 の項目を「Hard Fact」と「Soft Fact」に分けて Security Ontology と組み合わせることでセキュリティ対策案選定へと導くものである．また，ここで使われている Security Ontology は，リスク分析の分野での利用を主眼とした研究となっている [18]．この研究は，Security Ontology の作成，有効利用を目的とするもので，我々の研究と違って，認証取得を主眼に置いた研究ではない．また，事前にデータ準備が必要となり，Security Ontology の構築や項目の分類などの事前作業などがこれに該当する．我々の研究では，基準となる標準のデータのみを使用している．そして，認証取得時の項目の網羅性に着目しており，後述の参照ツリーを用いることで，視覚的なサポートを行っている．

### 2.2 セキュリティ対策案選択問題に関する研究

静岡大学の加藤らによって ISMS 認証を意識したセキュリティ対策選定手法についての提案が行われている [19]．この研究では，同大学の中村らによって情報資産，脅威，セキュリティ対策の関係をモデル化し，セキュリティ対策案選択問題を定式化したモデルを使用している [20]．この研究では，情報資産，脅威を網羅する形で結果的に認証に関する項目が網羅できているというものである．

また，このセキュリティ対策案選択問題に関する研究としては，東京電機大の佐々木らによって研究が続けられている，セキュリティ対策に関する意思決定関与者の合意形成を支援するためのツールとなる，多重リスクコミュニケータ（Multiple Risk Communicator: MRC）に関する研究がある [21], [22]．この研究では，認証取得の観点でリスク評価を行っているわけではなく，各関係者同士の合意形成を支援するものである．よって，認証取得を目的とした際に，項目の網羅性が保証されていない．

我々の研究では，提案システムを用いて作られた過去の対策案を提示して，セキュリティ対策案選択問題に対してのサポートを行っている．そのため，過去の案件できちんと標準の各項目を網羅している場合は，網羅性を確保することができる．

### 2.3 セキュリティ標準を意識したセキュリティ評価に関する研究

NEC の芦野らによって政府機関統一基準，PCI-DSS などを評価軸に用いた IT システムのシステム設計に関する研究が行われている [7]．この研究は，我々の目的とする認証取得を目的としたものではない．また，評価に用いるベースのデータとして，標準の内容をナレッジ化する必要がある．しかし，このナレッジ化には，専門的な知識が必要となり，事前のデータ準備が不可欠となる．

我々の研究では，標準の生データと特徴情報のみを使用するので，システムを動かすために，専門的な知識やその知識を用いた事前の準備が必要とならない．

### 2.4 複数標準を用いた統合型システムセキュリティ設計に関する研究

日立製作所の諸橋らによって ISO/IEC 15408 と ISO/IEC 27001 とを併用した統合型システムセキュリティ設計技法の提案がなされている [23]．この研究では，専門的な知識を有するセキュリティの専門家によって双方のセキュリティ機能要件と管理策のマッピングテーブルが作成される．

我々が提案する類似度を用いる手法では，専門的な知識を有するセキュリティの専門家は必要とせずシンプルな手法で，マッピングテーブルを作成することができる．

## 3. 標準の分析と活用

### 3.1 関連する標準

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-Act）サイクルの概念が適応されている，ISO/IEC 27000 ファミリ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分かった場合に，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とお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．

#### 3.1.1 ISO/IEC 27000 ファミリ

ISO/IEC 27000 ファミリとは，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，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．したがって，あらゆる規模と形態の組織に適用可

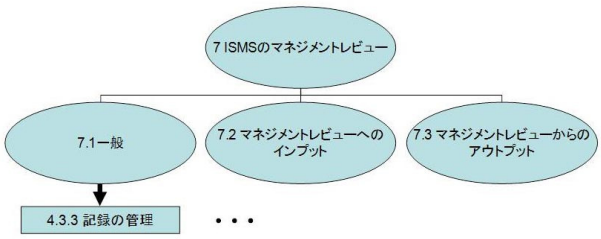


図 1　ISO/IEC 27001 の参照関係の例
**Fig. 1**　Reference-related example of ISO/IEC 27001.

能であるといえる．このファミリ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 ファミリは，現在のところ，2013 年 6 月時点すでに 14 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 [24]．ISO/IEC 27000 ファミリは，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．

#### 3.1.2 ISMS: Information Security Management System

前項の ISO/IEC 27000 ファミリのうち ISO/IEC 27001 は，ISMS を確立，導入，運用，監視，見直し，維持およ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 [25]．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．

### 3.2　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．たとえば，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．

### 3.3　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．具体的には，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．

そのため，各章で網羅すべきすべての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，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．本論文では，標準間の関連情報を抽出するために，テキスト間の類似度を算出する手法を用いている．本論文では，特徴情報のうち階層構造を示す構成情報を用いて，意味的な重みづけを行っている．

## 4.　類似度算出について

### 4.1　類似度算出手法

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 [12]．

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」[26] などを用いて，形態素解析 [12] 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，文書を特徴づけるうえで，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 [12]．最後に，重みによりベクトルや行列で表された文書間の類似度を算出する．

### 4.2　応用例

本論文で行った実験は，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．4.1 節で述べ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もとにしている [27], [28]．この文献 [28] 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．本論文では，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．

したがって，応用例としては以下のものがあげられる．

- 基準となる標準が更新された場合に，旧い版と異なる章や新たにまとめられた章に移った項目の抽出．
- 社内基準などのローカルな基準を作成する際に，国際標準などのグローバルな基準をもとにしている場合に，どの程度もと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の確認．
- すでに社内基準が設けられていて，セキュリティ認証取得を目指すといったときに，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の確認．

このような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る．そして，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，確かめることが可能となる．

## 5. プラットフォームの概要

### 5.1 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 つの部位に分かれている．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，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もと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．

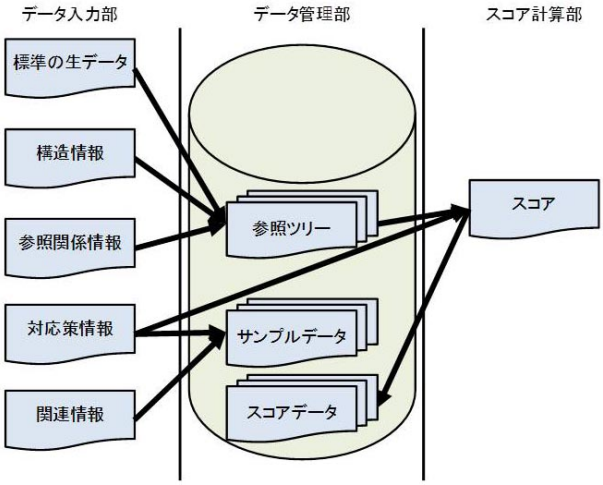


**図 2**　提案プラットフォームの構成
**Fig. 2**　Structure of proposed platform.

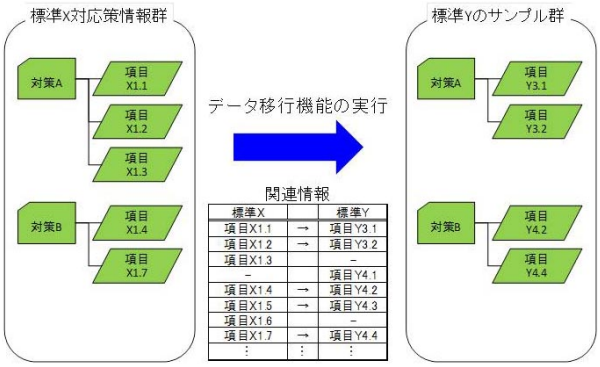


**図 3**　データ移行機能の概念図
**Fig. 3**　Example of Data Convert method.

### 5.2 データ移行機能

本プラットフォームにおけるデータ移行機能とは，ある基準 X に関する対応策情報群が存在し，かつ，別の評価基準 Y との関連情報が登録されている場合に，評価済みの対応策情報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 で通常どおり図 2 の対応策情報の登録を行い，セキュリティ評価を行う．次に，**図 3** で示すよう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 の図 2 のサンプルデータに変換する．この際に，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とる．なぜなら，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とは限らないからである．

本論文では，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．評価実験では，すでに関連情報が定義されている異なる 2 つの標準の各項目どうしのテキスト間類似度を算出することで関連情報の作成を行う．

## 6. 類似度による関連情報抽出実験

### 6.1 実験概要

すでに標準間の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 2 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 の値をとる．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，再現できたものを OK，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．

この 2 つの基準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．そして，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，4.2 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どうし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．

### 6.2 準備実験

文献 [14] で行ったテキスト間類似度を用いて関連情報を作成する（以下，手法 1）実験を本論文での実験の準備実験とする．

#### 6.2.1 実験の流れ

実験の流れは以下に示すものとする．

（手順 1）各基準の専門用語の抽出および重み付け

基準 A，B において，「章・節・項」（以下，大項目・中項目・小項目）の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 [29] 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付けを行う．

（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，基準間の類似度を算出する．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）関連がある項目の組を抽出

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の組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の組が，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．

#### 6.2.2 実験結果

大中小すべ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．項目レベルごとに元の全項目数と抽出した項目の組数を**表 1** に示す．

そして，抽出した項目の組を元データと比較して分類を行った．元データで関連が示されている項目の組数と抽出した組数，結果の分類，再現率，確からしさの関係を**表 2** に示す．

実験の結果，人の作業では見落としが発生しやすい組についても正しく抽出することができた．**図 4** は基準 B で

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

| | 全項目数 | | 抽出した項目の組数 |
|---|---|---|---|
| | 基準 A | 基準 B | |
| 大項目 | 10 | 10 | 8 |
| 中項目 | 39 | 36 | 28 |
| 小項目 | 133 | 127 | 97 |

**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.

| | PI | EI | 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% |

PI：関連がある項目の組数，EI：抽出した項目の組数

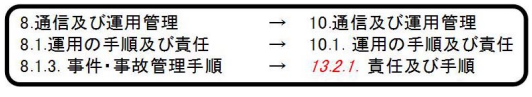


**図 4**　正しく抽出した組の例
**Fig. 4**　Example of combination extracted correctly.

| 項番 | 項目名 | 詳細記述 | | 項番 | 項目名 | 詳細記述 |
|---|---|---|---|---|---|---|
| 9.3. | 利用者の責任 | 情報システムへのアクセス権が、適切に認可され、剥当てられ、維持されていることを確実にするため。 | NG → | 11.2. | 利用者アクセスの管理 | 情報システムへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。 |
| | | | OK → | 11.3. | 利用者の責任 | 認可されていない利用者のアクセス、並びに情報及び情報処理設備の損傷又は盗難を防止するため。 |

図 5　NG となった組の例
**Fig. 5**　Example of combination extracted NG.

| | 類似度 | 判別 |
|---|---|---|
| 6. → 8. | 0 | FN |
| 6.1. → 8.1. | 0.358 | FP |

※6.→8.は本来正しい組だが責任範囲が異なっているため類似度が低い

図 6　FP となった組の例
**Fig. 6**　Example of combination extracted FP.

基準 A とは別の節に移動した項目の組で実際に抽出した組の例である．

#### 6.2.3　実験の考察

準備実験では，最もシンプルなテキスト間類似度を算出する手法を適応したにもかかわらず，高い再現率と確からしさを示すことができた．エラーとなった組で FP，NG となったものに注目して詳細に分析をした結果，以下のような特徴を見つけることができた．1 つ目の特徴は，NG となった組で見られた特徴となる．**図 5** で示すような元データの正しい組では項目名が完全一致していて詳細記述の内容が大きく異なる，という組が複数見受けられた．

2 つ目の特徴は，FP となった組で見られた特徴となる．**図 6** で示すように，文章的には非常によく似ているが上位の概念を確認するとその意味から関連がないことが判別できる組であった．

この 2 つの特徴から，より正確な関連がある項目の組を導くために，項目名の類似度を重視する手法や階層構造の情報を反映させた類似度を算出する手法を試すことが有効であるといえる．

### 6.3　複数の類似度算出手法を用いた比較実験

準備実験で得られた知見に基づき，新たに 2 つの類似度算出手法を使用して，同じ標準の組合せで関連がある項目の組の抽出を行った．

#### 6.3.1　手法 2：項目名をより重要視した類似度算出手法

手法 2 は，準備実験で得た詳細記述より項目名の方の類似度が重要視されるという知見に基づいた手法である．今回使用している 2 つの基準では，中小項目で「項目名」と「詳細記述」というように記述が分かれている．このような場合，「項目名」の類似度が「詳細記述」の類似度より重視されるように専門用語の重み付けを行う．まず，専門語抽出を行って形態素ごとに分ける．その際に，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，各専門用語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．このように各用語への重み付けを行った後に，準備実験と同様に類似度の算出，関連情報の抽出を行う．

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

| | 全項目数 | | 抽出した項目の組数 |
|---|---|---|---|
| | 基準 A | 基準 B | |
| 大項目 | 10 | 10 | 8 |
| 中項目 | 39 | 36 | 30 |
| 小項目 | 133 | 127 | 94 |

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.

| | PI | EI | 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% |

PI：関連がある項目の組数，EI：抽出した項目の組数

#### 6.3.2　手法 3：類似度を階層的に掛け合わせる手法

手法 3 は，準備実験で得られた階層構造の情報を反映させた方が有効である，という知見に基づいた手法である．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．たとえば，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．このように，類似度を算出した後は，手法 1 と同様に関連情報の抽出を行う．

### 6.4　実験結果

#### 6.4.1　手法 2

手法 1 と同様の手順で用語抽出を行う．次に，重み付けの作業になるが，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手法 1 と同様に 1 とする．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．表の各項目の見方については表 1，表 2 に準ずる．

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

| | 全項目数 | | 抽出した項目の組数 |
|---|---|---|---|
| | 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.

| | PI | EI | 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% |

PI：関連がある項目の組数，EI：抽出した項目の組数

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.

| | PI | EI | OK | FN | FP | NG | 再現率 | 確からしさ |
|---|---|---|---|---|---|---|---|---|
| 手法 1 | | 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 | | 25 | 23 | 7 | 1 | 1 | 74.19% | 92.00% |

PI：関連がある項目の組数，EI：抽出した項目の組数

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.

| | PI | EI | OK | FN | FP | NG | 再現率 | 確からしさ |
|---|---|---|---|---|---|---|---|---|
| 手法 1 | | 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 | | 93 | 90 | 23 | 0 | 3 | 77.59% | 96.77% |

PI：関連がある項目の組数，EI：抽出した項目の組数

#### 6.4.2　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．表の各項目の見方については表 1，表 2 に準ずる．

#### 6.4.3　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，さらに上位の概念がないことから差が生じない．中小項目のみが比較対象となるため，分類結果を項目レベルごとの表にまとめると**表 7**，**表 8** に示すようになる．表の各項目の見方については表 2 に準ずる．

関連情報を作成する際には，FP と NG の 2 つのエラーが発生し，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．

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うかがえる．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，階層構造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あるが，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ないが，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．今回の基準の組合せでは，正しい組で項目名が一致していたため，人の目によるチェックで回避することができる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 でどの組合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 NG となった組の中では比較的高く，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分かるように関連がないことが，比較的容易に判別できる組となっていた．

### 6.5　実験の考察

今回は比較的内容の近い基準どうしを用いたが，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率を得ることができることが分かった．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分かった．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分かった．また，類似度の算出方法に意味的な重み付けの工夫を加えることによって，より高い再現率，確からしさを得ることができた．

今回検証を行った手法のほかにも，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 [28] 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．

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，すべて正しい組合せであった．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，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．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．

## 7. 今後の課題

実験では，すでに関連情報がある基準どうしの類似度を求めて関連がある項目の抽出を行った．準備実験で得られた知見に基づく手法では，それぞれの手法で目的に合わせた正しい組の抽出をすることができた．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．そのほかには，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を確認していく．

## 8. まとめ

本論文では，セキュリティ標準を統合的に扱う環境の構築を目指したセキュリティ評価プラットフォームを構築し，そのデータ移行機能をより有効活用するための関連情報作成手法を提案した．そのために，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，基準間の各項目どうしの類似度を算出した結果から関連性を導き出し，関連性を示す情報の取得を行い，有効性について検討した．その際，準備実験で得られた知見に基づき，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．

本実験で使用した 2 つの手法は予想どおりの効果を示し，類似度算出時に意味的解釈を加えることが有効であると示された．しかし，個々の手法だけでは正しい組を再現しきれていないので，複数の手法を利用場面に応じて使い分けることや，組み合わせて使うことでより大きな効果が期待できる結果となった．

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，高い再現率で，かつ非常に高い確からしさを持つ関連情報を作成できることが分かった．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ならなかった際のロールバックを軽減できることが分かった．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，高い効果を得られるのではないかということが分かった．また，シンプルな類似度算出手法で高い再現率と高い確からしさを示すことができた．したがって，より的確な手法を用いて関連情報を作成することで，さらに高い再現率と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の中で，提案した手法を使うことにより，迅速に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 7 章で述べた課題に取り組み，いま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〉(2005.5).

[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，入手先 ⟨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，入手先 ⟨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，入手先 ⟨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，入手先 ⟨http://www.nisc.go.jp/active/general/kijun24.html⟩

[6] Payment Card Industry Security Standards Council: PCI SSC Data Security Standards, available from ⟨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，情報処理学会 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 (2013).

[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，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2011）シンポジウム論文集，pp.127–134 (2011).
[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，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).
[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] Takahashi, Y. and Teshigawara, Y.: Design and Development of a Security Evaluation Platform Based on International Standards, *International Journal of Informatics Society*, *IJIS*, Vol.5, No.2 (2013).
[15] Fenz, S. et al.: Ontology based IT-security planning, *12th IEEE International Symposium on Pacific Rim Dependable Computing* (2006).
[16] Feledi, D. et al.: Challenges of Web-based Information Security Knowledge Sharing, *The 7th ARES* (*Availability, Reliability and Security*) *conference* (*ARES 2012*), pp.514–521 (2012).
[17] Fenz, S. et al.: Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard, *13th IEEE International Symposium on Pacific Rim Dependable Computing*, pp.381–388 (2007).
[18] Ekelhart, A. et al.: Ontology-based Decision Support for Information Security Risk Management, *Proc. 2009 International Conference on Information Networking*, *ICOIN 2009*, pp.80–85 (2009).
[19] 加藤岳久，山本　匠，西垣正勝：教育効果を考慮したセキュリティ対策選定手法の検討，情報処理学会 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.135–140 (2011).
[20] 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45, No.8, pp.2022–2033 (2004).
[21] 佐々木良一，石井真之，日高　悠，矢島敬士，吉浦　裕，村山優子：多重リスクコミュニケータの開発構想と試適用，情報処理学会論文誌，Vol.46, No.8 (2005).
[22] 佐々木良一，日高　悠，守谷隆史，谷山充洋，矢島敬士，八重樫清美，川島泰正，吉浦　裕：多重リスクコミュニケータの開発と適用，情報処理学会論文誌，Vol.49, No.9 (2008).
[23] 諸橋政幸，永井康彦，荒井正人，手塚　悟：ISO15408/ISO27001 統合型システムセキュリティ設計技法の提案，情報処理学会論文誌，Vol.48, No.11 (2007).
[24] 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」，入手先 ⟨http://www.isms.jipdec.or.jp/27000family_20111220.pdf⟩
[25] ISO/IEC 27001 Information technology – Security techniques – Information security management system – Requirements (2005).
[26] 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).
[27] 高木輝彦，高木正則，勅使河原可海：学生が作成した問題の類似度算出手法の提案と評価，情報処理学会論文誌，Vol.50, No.10, pp.2426–2439 (2009).
[28] 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).
[29] 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．

**髙橋 雄志**　（学生会員）

1977 年生．2001 年創価大学工学部情報システム学科卒業．2003 年創価大学大学院工学研究科情報システム工学専攻博士前期課程修了（工学修士）．現在，同大学院博士後期課程在学中．情報セキュリティマネジメントの研究に従事．日本セキュリティ・マネジメント学会学生会員．

**篠宮 紀彦**　（正会員）

1972 年生．1995 年創価大学工学部情報システム工学科卒業．1997 年同大学院工学研究科情報システム工学専攻博士前期課程修了．2001 年同大学院博士後期課程修了（工学博士）．2000 年（株）富士通研究所ネットワークシステム研究所入社．IP ネットワークおよびフォトニックネットワーク管理技術の研究に従事．2005 年創価大学工学部専任講師．現在，同大学准教授．光ファイバセンサネットワーク，自律分散型ネットワーク，グラフ・ネットワーク理論等の研究に従事．2010 年 Best Paper Award, IEEE International Congress on Ultra Modern Telecommunication（ICUMT）．IEEE Circuits and Systems Society，Communications Society，Computer Society，電子情報通信学会，電気学会各会員．

**勅使河原 可海**　（フェロー）

1942 年生．1970 年東京工業大学大学院理工学研究科博士課程修了（工学博士）．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1974～1976 年ハワイ大学アロハシステム客員研究員．1995 年創価大学工学部教授，工学部長等を歴任．2013 年 4 月東京電機大学未来科学部情報メディア学科研究員．ネットワークセキュリティ，e-learning，ユビキタスコンピューティング等の研究に従事．情報処理学会，オペレーションズリサーチ学会各フェロー，情報処理学会平成 23 年度功績賞．創価大学名誉教授．