Vol.2014-CDS-10 No.9
2014/5/23

国際標準間の関連情報を用いた標準固有項目の識別手法

太田 悟[1,a)]　髙橋雄志[2]　勅使河原 可海[2]　篠宮 紀彦[1]

概要：近年，スマートフォンやタブレット端末などの普及に伴い，私物端末を業務に利用する BYOD(Bring Your Own Device) という考え方が，提唱されている．BYOD は，その性質上，個人データと業務データが端末内に混在している可能性が高く，機密情報が漏洩する危険性がある．このため，単純なセキュリティ対策だけでは，業務データのセキュリティを十分に確保することは困難である．そこで，BYOD に使用される私物端末の管理に関するセキュリティ要件の策定や，様々な標準化活動も積極的に行われている．このように，新たなセキュリティ標準が多数策定されているが，複数の標準を統合的に扱う環境はまだない．この問題に対して我々は，統合的な対策実施状況の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．このプラットフォームでは，異なる標準間における対応策のデータ移行機能を提供している．この機能には，異なる標準間において，同一の要求事項を示す関連情報が必要となる．そこで，我々は，情報検索の分野で使われている自然言語処理を応用し，関連情報を作成する手法を提案してきた．本稿では，この手法を用い，ある規格や規定に基づいて作成された標準に含まれる固有の項目を識別する手法を提案する．この手法により，新たに対策を行う内容を明確にし，認証取得を目指す際の支援を行うことを目的とする．提案手法の評価実験から，新しい標準が策定された場合において，新たに対策を行う内容を明確にし，認証取得を目指す際の支援を行うことが可能となることを示した．

キーワード：国際標準，ISO/IEC 27001，ISMS，情報セキュリティマネジメント，マネジメントシステム規格

A method for identifying unique requirements of international standards based on a information management guideline

Satoru Ota[1,a)]　Yuji Takahashi[2]　Yoshimi Teshigawara[2]　Norihiko Shinomiya[1]

Abstract: Recent years, the concept of BYOD (Bring Your Own Device) which has been adopted in the business as those devices are becoming popular, allows employees use personal smartphones and mobile devices at workplace. Since the device used for the BYOD is apt to store both business and private data in various situations, there could occur a risk that the confidential information might be leaked in case that an employee carelessly operates his or her device for private use. For this reason, some security technologies have been developed to manage consumer's devices soundly. And also, there seem no techniques to be establishes that could provide a comprehensive solution to deal with a wide variety of different standards. For solving such a problem, we have studied a platform that can evaluate the state of security measurements independent of any standard. This platform converts the data on the corresponding security measurements mutually among different standards in order to suggest an adequate solution comprehensively. This converting function needs the pertinent information that indicates the common requirements among different standards. Thus, we have applied a method of natural language processing used in the field of Information retrieval. In this paper, we propose a novel method to extract unique requirements in a security standard that are not on other provisions or guidelines. Our method aims at supporting to obtain the certification of some international security standards by clarifying required measurements when a new standard is drawn up based on other provisions or guidelines. This paper demonstrates an experiment to extract the unique requirements from some standards and finds out that the proposed method can clarify the requirements for an existing system.

Keywords: International Standard, ISO/IEC 27001, Security Management, Management System Standard

1. はじめに

近年，組織はサイバー攻撃から情報資産を守る自己防衛だけでなく，踏み台として利用されるような二次的な加害者になるリスクも防ぐ必要もあり，情報セキュリティに対する目的の範囲が拡大している [1]．そのため，組織はそのようなリスクを適切に管理する必要がある．それらのリスク管理について，政府機関や業界団体は IT システムなどに対する満たすべきセキュリティ水準を定めたガイドライン（以下，セキュリティ標準という）を策定している [2]．これに伴い，組織の情報資産に対するリスクへの対策状況を，外的機関からの認証を取得することによって，利害関係者からの信頼を獲得することが重要視されている [3]．

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）認証の取得がある．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，2014 年 3 月 27 日現在で 4,493 件と多くの企業や組織が取得している [4]．

また，近年における，スマートフォンやタブレット端末など（以下，スマートフォンやタブレット端末をまとめて，スマートデバイスという）の普及に伴い，私物端末を業務に利用する BYOD(Bring Your Own Device) という考え方が，提唱されている．BYOD は，私物端末を業務に利用するため，個人データと業務データが混在している可能性が高いが，スマートデバイス使用者の情報セキュリティに対する意識が低く，機密情報が漏洩してしまう危険性がある [5]．また，私物端末上に業務データが存在していなくても，組織の情報資産へ私物端末からアクセスすることは，新しい重大なリスクを伴う．このため，単純なセキュリティ対策だけでは，業務データのセキュリティを十分に確保することは困難である [6]．

そこで，BYOD に使用される私物端末の管理に関して，慎重な計画による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，私物端末上に存在する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，BYOD に使用される端末に関するセキュリティ要件の重要性が高まっており，様々な標準化活動も積極的に行われている [7]．

現在，BYOD の運用手順に関する対策は，組織によって異なる [6]．そのため，BYOD の運用に関する標準が策定され，その認証を取得する際に，組織が既に対応済みである対策と，これから新たに対応しなければならない対策を漏れなく判断する必要がある．

ISMS などのセキュリティ認証の多くは，記載されている要求事項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．こういったセキュリティ標準での要求事項には，保護すべき情報資産の管理体制やセキュリティ対策の基本的な考え方が示されている．また，セキュリティ対策の基本的な考え方は，いかなる組織や IT システムにも対応できるように，汎用的な記述になっている．そのため，適切な対応策の実現には，IT システムとセキュリティの専門知識の両方が要求される．しかし，IT システムの専門知識を持つ人材は不足しており，その中でも特にセキュリティ人材は不足していると言われている [8]．そのため，セキュリティ標準の認証評価時に，取得するセキュリティ標準の要求事項すべてに対策がとられているか分からないという網羅性の問題があげられる．

そこで，認証取得に必要な要求事項の達成度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 [9]．同様に，セキュリティ標準を知識ベースとして用いた IT システムの設計評価システムの提案もなされている [10]．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標準については，変更が行われる回数が他の標準にくらべて頻繁であり，新たなセキュリティ標準も多数策定されている [11]．さらに，組織の規模や製品によって，認証の取得範囲やセキュリティ標準の満たすべき要求事項が異なる．そのような違いにより，認証取得のために新たな体制を作り，それぞれの認証取得にあわせた個別の評価ツールや人員を用いてセキュリティ対策実施状況の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 [12]．このような問題を解決するためには，個別のセキュリティ評価ツールではなく，標準の内容に依存しない統合的なセキュリティ評価ツールを実現する必要性があると考えられる．

これらの問題に対して我々は，統合的なセキュリティ対策実施状況の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 [13]．このプラットフォームでは，異なる標準間における対応策のデータ移行機能を提供している．この機能を実現するために，異なる標準間における同一の対応策を求める要求事項を示す情報（以下，関連情報という）が定義されている必要がある．しかし，その異なる標準同士の関連情報が必ず定義されているとは限らないという問題がある．そこで，情報検索の分野で使われている，自然言語処理を用いたテキスト間の近似度算出手法 [14] を応用し，各標準の項目同士の近似度から，項目の相関を取ることにより，関連情報を作成する実験を行い，その有効性を確認した [15]．

[1] 創価大学大学院工学研究科
Graduate School of Engineering, Soka University
[2] 東京電機大学総合研究所サイバーセキュリティ研究所
Cyber Security Laboratory, The Research Institute of Science and Technology, Tokyo Denki University
[a)] e13m5206@soka-u.jp

本稿では，この関連情報を作成する手法を用い，ある規格や規定に基づいて作成された標準に含まれる固有の項目（以下，固有項目という）を識別する手法を提案する．この手法により，ある規格や規定に基づいて，新しく標準が策定された場合，固有項目を識別することにより，新たに対策を行う内容を明確にすることで，認証取得を目指す際の支援を行うことを目的とする．提案手法の評価実験から，ある規格や規定を基にして，新しい標準が策定された場合において，新たに対策を行う内容を明確にし，認証取得を目指す際の支援を行うことが可能となることを示した．

2. 関連する規格および技術

2.1 マネジメントシステム規格 (MSS：Management System Standard)

MSS とは，組織が特定の目的を達成するために方針，プロセス及び手順を策定し，それらを体系的に管理するための要求事項又は指針を提供する規格である [16]．MSS では，PDCA サイクルに基づいた経営を行うことにより，組織の目標を達成するための力を継続的に改善していくことを求めている．代表的な MSS の標準として，製品やサービスの品質向上のための規格である ISO 9001 や，環境への悪影響を防ぐための規格である ISO 14001，また後述するセキュリティに関する規格である ISO/IEC 27001 などが存在する．これら MSS の標準については，MSS 同士の整合性をはかるために，国際標準化機構によって，MSS の上位構造と共通テキスト (以下，MSS 共通テキストという)，共通用語の定義の指針が開発された [16]．そのため，MSS に基づく標準を新たに策定，もしくは改訂を行う場合においては，常に文献 [16] に記載されている定義に従って作成し，妥当性の評価を行わなければならない．今後，MSS の標準については，MSS 共通テキストに従って策定・改訂が行われるため，我々の提案手法の精度が向上すると考えられる．

2.1.1 ISO/IEC 27001

ISO/IEC 27001 とは，ISMS に関する MSS であり，国際標準化機構と国際電気標準会議の共同によって策定された規格である [17]．この規格は，ISMS に必要な要求事項を規定し，ISMS の開発，実施，改善を支援するための指針から構成されている．そのため，いかなる規模や形態の組織にも適用可能な規格となっている．この規格の認証を取得するために，まず，組織は情報セキュリティに関するリスクを分析，評価し，必要に応じて適切な情報セキュリティ制御を実装する必要がある．また，情報セキュリティの運用は，状況に応じてリスクや対策が変化していくため，他の MSS 同様，PDCA サイクルにより継続的な見直しと改善が要求される．ISO/IEC 27001 は，2008 年からの定期見直しにより文献 [16] に基づき，MSS 共通テキストの内容に沿って改訂が行われ，2013 年 10 月 1 日に ISO/IEC 27001：2013 要求事項が発行された．

また，ISO/IEC 27000 ファミリーとして，ISMS に必要な要求事項である ISO/IEC 27001 を含む様々な規格が検討され，発行されている．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 サイクルによる運営の重要性を示している．ISO/IEC 27000 ファミリーは，2013 年 12 月の時点で 14 種類の標準が策定済みであり，他にも多くの標準が策定中となっている．

2.2 情報セキュリティ対策マップ

NPO 日本ネットワークセキュリティ協会の配下の標準化部会の情報セキュリティ対策マップ WG によって，組織全体の情報セキュリティ対策の状況を確認するための情報セキュリティ対策マップの作成が行われている [12]．この WG では，多くのセキュリティ標準からセキュリティ対策を収集し，対策の構造についてのモデル化，ツリー化を行っている．この WG での対策収集の過程で各セキュリティ標準内での記述や表現，対策の粒度（抽象度），対策を行う時期や対象が異なっていることが指摘されている．その上で，あらゆる対策を同じ表現で記述する正規化や，対策同士を比較できるよう，極限まで対策を具体化させる原子化を行っている．今後，対策の正規化，原子化が行われたセキュリティ標準が新しく策定されるようになれば，我々の提案手法の精度が向上すると考えられる．

2.3 スマートデバイスの業務利用に関するセキュリティガイドライン

日本スマートフォンセキュリティ協会の配下の利用ガイドライン WG によって，スマートデバイスの利用シーンという観点から，企業や組織が考慮すべきセキュリティ上の脅威とその脅威に対する対策を明確化したガイドラインが作成されている [18]．本ガイドラインの前半には，スマートデバイスの特徴や特性，利活用の効果を記載している．そして，後半にはスマートデバイスのセキュリティを，「利用シーン」と「デバイスのライフサイクル」という側面から，管理者が認識しておくべき脅威と対策について述べられている． 各章の「脅威と対策」は、スマートデバイスと PC との違いに焦点を当てながら，多角的な可能性を考慮し，網羅的に述べられており，実際のスマートデバイスの利用目的に照らし合わせて，必要なセキュリティ対策案の選定へと導くものである．本ガイドラインには，「脅威と対策」を整理した付録書により，利用シーン別に必要なセキュリティ対策を検討する際に使用できるものとなっている．

組織が既に対応済みである BYOD の運用に関する対策

と，本ガイドラインの付属書の対策案を比較する事で，これから新たに対応しなければならない対策を漏れなく判断することができると考えられる．

3. 関連する研究

3.1 セキュリティオントロジーに関する研究

Secure Business Austria の Stefan Fenz らによって Security Ontology [19] [20] を用いて 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 [21]．この研究では，ISO/IEC 27001 の項目を「Hard Fact」と「Soft Fact」という２つの要素に分け，それらの要素と Security Ontology を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 [22]．この研究は，Security Ontology の作成と有効利用を目的とするものであり，事前に Security Ontology の構築や項目の分類などのデータの準備が必要となる．

我々の研究では，関連情報の作成時に，セキュリティ標準に記述されている文書を自然言語処理により分析している．しかし，自然言語処理により多数の対応策の中から正しい関連情報を導き出すためには，対応策を実施する時期や対象などを考慮することが必要になる．そこで，Security Ontology を用いて構築や項目の分類などを行うことにより，より正確な関連情報を導き出せると考えられる．

3.2 セキュリティ標準に基づいた IT システム設計支援に関する研究

NEC の芦野らによって政府機関統一基準や PCI DSS（Payment Card Industry Data Security Standard）[23] 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 [10]．この研究では，IT システムの設計書から，IT システム構成のモデル化を行い，それに基づいてセキュリティ標準に準拠した設計がなされているかどうかを評価することを目的としたものである．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，事前にデータの準備が不可欠となる．さらに，評価軸に用いるセキュリティ標準が異なるごとに，ナレッジを再定義する必要がある．

我々の研究では，評価軸に用いるセキュリティ標準が異なる場合において，関連情報を用いることで，認証取得時の支援を目的としている．さらに，関連情報の作成には，セキュリティ標準に記述されている文書を自然言語処理を用いて分析するため，専門的な知識を必要としない．そのため，我々の研究を用いることでナレッジを再定義することが容易になると考えられる．

4. 関連情報の作成について

先行研究では，評価の対象となる標準を整理したデータの入れ替えのみで，他の標準と同様にセキュリティ評価を行なうことができる統合的なセキュリティ評価プラットフォームを提案してきた [13]．このセキュリティ評価プラットフォームの主な機能として，標準の要求事項とそれに基づく対応策のデータを管理する機能，認証取得時における要求事項に対する対応策の達成度の評価機能，過去の事例に基づいたサンプルを提示する機能，そして，異なる標準間のデータ移行機能があげられる．

本稿では，セキュリティ評価プラットフォームにおける，異なる標準間のデータ移行機能に注目する．データ移行機能とは，すでに認証取得済みである標準 X とは異なる標準 Y を用いて認証評価を行う際に，標準 X の対応策の情報を標準 Y の対応策のサンプル情報として提示する機能である．このデータ移行機能を利用する際に，異なる標準間で同じ要求事項を示す関連情報を必要とする．しかし，必ずしも関連情報が定義されているとは限らない，という問題がある．そこで，異なる標準の項目間の相関を取ることで，標準間の関連情報を導出する．

関連情報を作成することにより，異なる標準間において同じ内容の要求事項を判別することが可能となる． 応用例としては以下のことを確認できる．

例 1： 共通する規格や規定を基に，新たな標準を作成する際，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．

例 2： 基準となる標準が更新された場合に，旧版とは異なる章や新たにまとめられた章に移った対応策の項目があるのか．

例 3： すでに組織内基準が設けられており，その組織内基準を用いてセキュリティ認証の取得を目指す際に，現状の組織内基準がどの程度取得を目指すセキュリティ標準の要求事項を満たしているか．

以上のように，新規の標準や項目を定義する際に，もととなる規格や規定の項目と照らし合わせて，要求事項を見つけることで，もとの規格や規定を正しく反映できているか，共通の項目が存在するのか，といったことを確かめることが可能となる．

4.1 相関分析手法

我々は．異なる標準の項目間の相関を取る方法として，文書の分類や情報検索に関する研究分野において行われている自然言語処理によって文書間の近似度を算出する手法を用いている [14]．

はじめに，関連情報算出の対象となるセキュリティ標準を決定し，テキスト情報を取得する．次に，取得したテキスト情報を標準の項目ごとに「茶筌システム」[24] などを

表 1 不要語と索引語

分類	種類	例
不要語	内容語	ある　なる　前　上
	機能語	から　できる　は　を
	接続詞など	したがって　及び　または
索引語	単名詞	組織　パスワード　レビュー
	複合名詞	ネットワーク管理策　管理システム
		セキュリティ基本方針

用いて形態素解析を行い，形態素に分割する．形態素とは，文書の形態素解析によって得られた言語における意味を持つ最小単位のことである．そして，得られた形態素から文書の内容を表す単語を索引語と定義し抽出する．形態素のうち，文書の内容を特徴付ける上で，役に立たない語を不要語として定義し削除する．不要語を削除した項目ごとの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のかを，索引語の重要度として付与するために，重み付けを行う．重み付けの手法として，文書中に出現する索引語の頻度を用いた 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 [14]．その後，各項目の重みをベクトルや行列で表現する．重み付けによって作成した各標準の項目のベクトルや行列の全組み合わせに対して余弦 [14] を計算し，項目間の近似度を算出する．近似度の計算には余弦の他に，Dice 係数や Jaccard 係数などもある [14]．最後に，各セキュリティ標準の項目間の近似度が最大となる項目の組のうち，どちらの標準から見ても一致しているものを相関がある項目の組と定義する．

4.2 不要語と索引語

ここでは，不要語と索引語について詳しく説明する．表 1 は不要語と索引語それぞれについて，いくつかの例を示している．

不要語とは，文章の内容を特徴付ける上で役に立たない形態素のことであり，特定の概念を表す内容語のうち，それだけでは意味の無い語と，語と語の関係を表す機能語と，その他の接続語を指す．これら不要語については相関を取る際に役に立たないため削除する．

索引語とは，文書中からその文書を特徴付けるための形態素のことであり，形態素解析によって得られた形態素から不要語を削除したものである．索引語に含まれる名詞には，単名詞と複合名詞の 2 つの種類がある．名詞のうちそれ以上分割することができない名詞を単名詞と定義し，複数の単名詞から構成される名詞を複合名詞と定義する．例えば，“ネットワーク管理策” という索引語については “ネットワーク” と “管理” と “策” という単名詞から構成される複合名詞であり，“セキュリティ基本方針” という索引語については，“セキュリティ” と “基本” と “方針” という単名詞から構成される複合名詞である．本研究では，このように，セキュリティ標準に基づいて複合名詞を定義した辞書を作成し，形態素解析に使用する．

5. 関連情報を用いた固有項目の識別実験

5.1 固有項目の識別手法

本稿では，4 章で述べた異なる標準の項目間の相関を分析する手法を応用することで，ある規格や規定に基づいて作成された標準に含まれる固有の項目（以下，固有項目という）を識別する手法を提案する．この手法により，ある規格や規定に基づいた新しい標準が策定された場合において，新たに対策を行う内容を明確にする．こうすることで，新たな認証取得を目指す際の支援を行うことができる．

5.2 実験概要

本提案手法の有効性を検証するために，『MSS 共通テキスト』（以下，文書 A という）と，それに基づいて作られた『ISO/IEC 27001：2013 要求事項』（以下，文書 B という）の 2 つの文書を用いて固有項目の識別実験を行う．2 つの文書 A・B から相関がある項目の組を取り除き，残りの項目について分析，考察を行う．

5.3 実験の手順

手順 1： 各文書の索引語の抽出および重み付け
各文書のそれぞれの項目に対して「茶筌システム」[24] を用いて形態素解析を行う．このときに，セキュリティ標準に準拠した複合名詞を定義した辞書を形態素解析に使用する．そうして得られた形態素から不要語を削除し，索引語を抽出する．次に，抽出された索引語に対して重み付けを行う．本手法では，一律 1 の重みを付ける．

手順 2： 近似度の算出
手順 1 によって作成した各文書間の項目の重みの全組み合わせに対して余弦 [14] を計算し，項目間の近似度を算出する．

手順 3： 相関がある項目の組の抽出
はじめに，文書 A の各項目から見た文書 B の項目の中で近似度が最大のものを抽出する．文書 B についても同様に抽出し，相関がある項目の組を抽出する．

手順 4： 固有項目の識別
手順 3 によって得られた相関がある項目の組に該当する文書 B の項目を取り除き，残った項目を固有項目として識別する．

手順 5： 固有項目の比較と分類
実際に人の手により，文書 A と文書 B を比較し，文書 B の固有項目であると考えられる項目と手順 4 によって得られた固有項目の比較し，分類する

表 2 MSS における ISO/IEC27001 の固有項目抽出結果

4.2.b	4.3.c	6.1	6.1.1.a	6.1.1.c
6.1.2	6.1.2.a	6.1.2.a.1	6.1.2.a.2	6.1.2.b
6.1.2.c	6.1.2.c.1	6.1.2.c.2	6.1.2.d	6.1.2.d.1
6.1.2.d.2	6.1.2.d.3	6.1.2.e	6.1.2.e.1	6.1.2.e.2
6.1.3	6.1.3.a	6.1.3.b	6.1.3.c	6.1.3.d
6.1.3.e	6.1.3.f	6.2.c	7.4.d	7.4.e
8.2	8.3	9.1.d	9.1.f	9.3.c.1
9.3.c.4	9.3.d	9.3.e		

表 3 分類結果

固有項目	抽出した項目	OK	NG
33	38	33	5

表 4 OK となった項目

4.3.c	6.1.2	6.1.2.a	6.1.2.a.1	6.1.2.a.2
6.1.2.b	6.1.2.c	6.1.2.c.1	6.1.2.c.2	6.1.2.d
6.1.2.d.1	6.1.2.d.2	6.1.2.d.3	6.1.2.e	6.1.2.e.1
6.1.2.e.2	6.1.3	6.1.3.a	6.1.3.b	6.1.3.c
6.1.3.d	6.1.3.e	6.1.3.f	6.2.c	7.4.d
7.4.e	8.2	8.3	9.1.d	9.1.f
9.3.c.4	9.3.d	9.3.e		

5.4 実験結果

文書 B における，固有項目の識別実験を行った結果，38 項目が固有項目と識別された．識別された項目を表 2 に示す．また，人の手により，文章 B の固有項目であると考えられる項目は 33 項目であった．抽出した項目のうち，正しく固有項目として識別された項目（OK）は 33 項目であり，文書 A と関連があるにも関わらず，固有項目として識別された項目（NG）については 5 項目であった．固有項目の抽出実験の結果を分類したものを表 3 に示す．

5.5 考察

次に，識別された項目の OK，NG それぞれについて，分析を行った．

5.5.1 OK について

はじめに OK となった項目それぞれについて考察を行った．OK となった項目を表 4 に示す．OK となった項目は大別すると 2 つに分けられることがわかった．

種類 1： 文書 B の項目の中でも強く意識するべき項目

はじめの種類として，文書 B の項目の中でも，特に強く意識するべき項目である．これは，4 章「組織の状況」の中にある，他の組織との情報や資源のやり取りについての依存関係の項目，6 章「計画」の中にある，セキュリティアセスメントについての項目と，セキュリティリスク対応についての項目，セキュリティの目的と計画についての項目，7 章「支援」の中にある，コミュニケーションを実施している主体についての項目，9 章「パフォーマンス評価」の中にある，監査を行う主体についての項目であった．種類 1 の固有項目について章ごとに分類したものを表 5 に示す．特に 4，7，9 章の中から識別された項目に関しては，認証を取得する組織と関わりのある他組織についての対策項目であり，情報セキュリティにおいては特に意識しなければならない項目であると考えられる．また，それらの項目は，標準の項目の中でも深いレベルの項目になるため見落としがちになると考えられるが，本提案手法では識別することができた．

表 5 項目の中でも強く意識するべき項目

4 章	組織の状況	他の組織との依存関係 4.3.c
6 章	計画	セキュリティアセスメント 6.1.2 6.1.2.a 6.1.2.a.1 6.1.2.a.2 6.1.2.b 6.1.2.c 6.1.2.c.1 6.1.2.c.2 6.1.2.d 6.1.2.d.1 6.1.2.d.2 6.1.2.d.3 6.1.2.e 6.1.2.e.1 6.1.2.e.2
		セキュリティリスク対応 6.1.3 6.1.3.a 6.1.3.b 6.1.3.c 6.1.3.d 6.1.3.e 6.1.3.f
		セキュリティ目的と計画 6.2
7 章	支援	コミュニケーションを実施する主体 7.4.d 7.4.e
9 章	パフォーマンス評価	監査を行う主体 9.1.d 9.1.f

表 6 種類 1 を追加したことに対する項目

8 章	運用	セキュリティアセスメント 8.2
		セキュリティリスク対応 8.3
9 章	パフォーマンス評価	マネジメントビュー 9.3.c.4 9.3.d 9.4.e

種類 2： 種類 1 を追加したことに対する項目

もう 1 つの種類として分類された項目は，種類 1 の項目を追加したことに対して記述されている項目である．これは，8 章 「運用」の中にある，セキュリティアセスメントについての項目と，セキュリティリスク対応についての項目，9 章「パフォーマンス評価」の中にある，関係者からのフィードバックに関する項目とセキュリティ目的とリスク対応へのレビューについての項目であった．種類 2 の固有項目について章ごとに分類したものを表 6 に示す．8 章については，6 章のセキュリティアセスメントと，セキュリティリスク対応として追加された項目を参照している項目であり，9 章については他組織に関する項目と 6 章に関するレビューに関する項目であった．このことから，種類 2 では PDCA サイクルにおける「Plan」にあたる種類 1 の項目に対する，「Do」と「Check」に対応する項目であると考えられる．

5.5.2 NG について

次に NG となった項目について考察を行った．NG となった項目を表 7 に示す．NG については，本来であれば

表 7 NG となった項目

原因 1	6.1.1.a 6.1.1.c 9.3.c.1
原因 2	4.2.b 6.1

表 8 項目が同じような文言で書かれている場合

文書 B	6.1.1.a	ISMS が，その意図した成果を達成できることを確実にする．	
文書 A	正	6.1.a	XXX マネジメントシステムが，その意図した成果を達成できることを確実にする
	似た項目	5.1.5	XXX マネジメントシステムがその意図した成果を達成できることを確実にする
文書 B	6.1.1.c	継続的改善を達成する．	
文書 A	正	6.1.c	継続的改善を達成する．
	似た項目	5.1.7	継続的改善を促進する．
文書 B	9.3.c.1	不適合及び是正措置	
文書 A	正	9.3.c.2	不適合及び是正措置
	似た項目	10.1	不適合及び是正措置

文書 A と関連がある項目が存在する．しかし相関を分析した時に，近似度が高い項目が発見できなかったため，固有項目として識別されたものである．そのため，なぜ近似度が高い項目が発見できなかったのかについて分析を行った．その結果，エラーとなった原因は大きく 2 つあることがわかった．

原因 1： 項目が同じような文言で書かれている場合

NG と判断された原因の 1 つ目として，相関を分析する際に，本来相関がある項目と同じ索引語を多く使用している項目が他に存在している場合である．原因 1 として考えられる項目とその項目と対応する項目，同じ索引語を多く使用している項目を表 8 に示す．このような場合では，手順 3 で示した処理を行った時に，お互いの近似度が最大となる組合せとして抽出されなかったことにより，固有項目と識別されたと考えられる．そのため，高い近似度が複数存在する場合においては，相関がある項目として抽出する場合には近似度が最大の項目以外の項目についても判断する必要があると考えられる．

原因 2： 詳細記述の分量に差がある場合

NG と判断された原因の 2 つ目は，相関を分析する際に，本来相関がある項目と詳細記述に記載されている分量に差がある場合である．原因 2 として考えられる項目とその項目と対応する項目，それぞれの詳細記述を表 9 に示す．手順 2 で示した処理を行った時に，1 つの索引語がその項目間における近似度に与える影響が少なくなる．そのため，相関があると判断するべき項目との近似度が低くなり，正しく判断されず，固有項目として識別されたと考えられる．4.2.b に関しては，文書 A に対応する項目があるものの，情報セキュリティにおいて考慮すべき事項が注記として追加されているため，近似度が低くなったと考えられる．6.1 に関しては，6 章に新しく節を作成し，固有項目が追加されており，詳細記述が新しい節として項目分けされている．そのために，文書 A の項目との近似度が低くなってしまったと考えられる．これは，文書 A と文書 B の標準の構成が変わり，注記がどの項目に属しているのかについての判断が難しくなったことが原因であると考えられる．そこで，近似度を計算する際に，項目ごとではなく，項番が振っていなくとも，ひとまとまりの文章を 1 つの項目として近似度を算出することで，改善できると考えられる．

表 9 詳細記述の分量に差がある場合

文書 B	4.2.b	その利害関係者の，情報セキュリティに関連する要求事項． 注記 利害関係者の要求事項には，法的及び規制の要求事項並びに契約上の義務を含めてもよい．
文書 A	4.2.2	その利害関係者の要求事項．
文書 B	6.1	リスク及び機会に対処する活動
文書 A	6.1	リスク及び機会に対処する活動 XXX マネジメントシステムの計画を策定するとき，組織は 4.1 規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項のために取り組む必要があるリスク及び機会を決定しなければならない．

6. 今後の課題

実験では，MSS 共通テキストに基づいて作られた標準の項目から，固有項目の識別を行った．関連情報の作成手法を応用することで，正しく固有項目を識別する事ができた．しかし，一部の項目について，本来対応する項目があるのにも関わらず，固有項目として識別されるものがあった．こういったエラーについて，標準の構成を考慮した比較手法や，近似度を算出する際の重み付けなどを考慮して，手法の文章解析精度を高めて対応していきたい．

また，関連情報作成手法の課題として，文章に書かれている意味を考慮して近似度を求めることや，対策を行う時期や範囲などについても考慮した分析手法などの検討も行っていく必要がある．

さらに，実際の対応策データを用いて，組織の対策実施状況などを標準と照らし合わせた実験を行い，本提案手法の評価実験を行い，有用性の確認をしていく．

7. まとめ

本稿では，ある規格や規定に基づいて策定された標準の固有項目を識別する手法を提案をした．そのために，情報検索の分野で使われている，自然言語処理を用いたテキスト間の近似度算出手法を応用し，各文書の項目同士の近似度から，項目の相関を取ることにより，固有項目を抽出する実験を行い，その評価実験を行った．

実験では，ある規格や規定と，それに基づいて作られた標準を用いて，標準の固有項目の識別実験を行うことで，その標準の固有項目を識別することができた．これによ

り，本手法を用いることで，ある規格や規定に基づいて，新しく標準が策定された場合，新たに対策を行う内容を明確にすることができ，認証取得を目指す際の支援を行うことが可能になることがわかった．

そして，今後 BYOD の運用に関する標準が策定され，その認証を取得する際に，本提案手法を用いることにより，必要な対策を漏れなく判断することが可能になり，認証を取得する際に活用できると考えられる．

今後は 6 章で述べた課題に取り組み，手法の改良と追加の実験を行うことで，信頼度と有効性を高めていく．

参考文献

[1] 総務省：情報通信白書平成 24 年度版 (online), 入手先 ⟨http://www.soumu.go.jp/johotsusintokei/whitepaper/h24.html⟩(2012).
[2] 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技術基準 (平成 24 年度版)(online), 入手先 ⟨http://www.nisc.go.jp/active/general/pdf/k305-111.pdf⟩(2012).
[3] 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> , (2004.5).
[4] 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 (online), 入手先 ⟨http://www.isms.jipdec.jp/lst/ind/suii.html⟩.
[5] 情報処理推進機構：2013 年度情報セキュリティの脅威に対する意識調査-調査報告書- (online), 入手先 ⟨https://www.ipa.go.jp/files/000035983.pdf⟩.(2013.12)
[6] 総務省：スマートフォン・クラウドセキュリティ研究会-最終報告-(online), 入手先 ⟨http://www.soumu.go.jp/main_content/000166095.pdf⟩.(2013.6)
[7] 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, (online), 入手先 ⟨http://wp.techtarget.itmedia.co.jp/contents/?cid=11501⟩
[8] 情報処理推進機構：「情報セキュリティ人材の育成に関する基礎調査」報告書について (online), 入手先 ⟨http://www.ipa.go.jp/security/fy23/reports/jinzai/⟩.
[9] 情報処理推進機構：セキュリティ設計評価支援ツール V03 (online), 入手先 ⟨http://www.ipa.go.jp/security/fy13/evalu/ccsystem/CCtoolV03/secevtoolv03.htm⟩.
[10] 芦野佑樹，髙橋雄志，森田陽一郎，島成佳，岡村利彦，勅使河原可海，佐々木良一：セキュリティ標準に基づいた IT システム評価支援ツールの開発，情報処理学会 コンピュータセキュリティシンポジウム (2013.10).
[11] 日本情報経済社会推進協会：情報セキュリティマネジメントシステム 適合性評価制度の概要 (online), 入手先 ⟨http://www.isms.jipdec.or.jp/doc/ismspanf.pdf⟩.
[12] 日本ネットワークセキュリティ協会：情報セキュリティ対策マップ WG 情報セキュリティ対策マップ検討 WG 活動報告 (online), 入手先 ⟨http://www.jnsa.org/seminar/2013/0607/video_t1.html⟩.
[13] 髙橋雄志，篠宮紀彦，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提案，日本セキュリティ・マネジメント学会学会誌 Vol.27, No.2, pp.16-29 (2013.9).
[14] 徳永健伸：情報検索と言語処理, 東京大学出版会 (1999).
[15] 髙橋雄志，篠宮紀彦，勅使河原可海：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 論文誌コンシューマデバイス＆システム 第 3 巻, pp.22-32, (2013.12).
[16] 日本規格協会：ISO/IEC 専門業務用指針，第 1 部，統合版 ISO 補足指針-ISO 専用手順 2013, 入手先 ⟨http://www.jsa.or.jp/itn/pdf/shiryo/isohosoku_taiyaku1304.pdf⟩
[17] 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_20131212.pdf⟩
[18] 日本スマートフォンセキュリティ協会：ガイドライン WG スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン第二版 (online), 入手先 ⟨http://www.jssec.org/dl/guidelines_v2.pdf⟩.
[19] Stefan Fenz et al., *Ontology based IT-security planning,* 12th IEEE International Symposium on Pacific Rim Dependable Computing, 2006
[20] Daniel Feledi et al., *Challenges of Web-based Information Security Knowledge Sharing,* The 7th ARES(Availability, Reliability and Security) conference (ARES 2012), pp.514-521
[21] Stefan Fenz et al., *Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard,* 13th IEEE International Symposium on Pacific Rim Dependable Computing, 2007, pp.381-388
[22] Andreas Ekelhart et al., *Ontology-based Decision Support for Information Security Risk Management,* 2009 International Conference on Information Networking, ICOIN 2009, Proceedings of ICOIN 2009, pp.80-85
[23] Payment Card Industry Security Standards Council: PCI SSC Data Security Standards, 入手先 ⟨https://www.pcisecuritystandards.org/security_standards/⟩
[24] 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).