ISMS と CSMS との関連情報作成の提案

髙橋 雄志[†1]　佐藤 信[†2]　金子 朋子[†3]　加藤 岳久[†4]
間形 文彦[†5]　西垣 正勝[†6]　佐々木 良一[†1]　勅使河原 可海[†1]

概要：近年，様々なシステムはインターネットを介して相互接続しクラウドなどと連携してそれぞれ多様なサービスを提供するようになってきている．これまで情報セキュリティと制御系システムのセキュリティは別々に取り組まれてきていたが，モノのインターネットと呼ばれる IoT の世界では同時に考えていかなければならない．しかし，現状ではまだ，双方を網羅する基準が存在していない．そこで我々はセキュリティ標準間の関連情報を作成する手法を用いて，情報セキュリティの基準である ISMS（Information Security Management System）と制御系システムの基準である CSMS（Cyber Security Management System）の関連情報を作成して共通項や，個別項目の抽出を行って，その親和性について検証をした．

キーワード：セキュリティ標準，ISMS，CSMS

A Proposal of a Pertinent Information Creation between Information Security Management System and Cyber Security Management System

Yuji Takahashi[†1]　Makoto Sato[†2]　Tomoko Kaneko[†3]　Takehisa Kato[†4]
Fumihiko Magata[†5]　Masakatsu Nishigaki[†6]　Ryoichi Sasaki[†1]
Yoshimi Teshigawara[†1]

Abstract: In recent year, a variety of systems has been interconnecting by the Internet, and offer diversified services cooperated with the Cloud. Up to now, securities of the control system and the information system have been considered separately, however, these securities of each system have to be considered together in the circumstance of the Internet of Things. There is not such a standard which covers both security requirements. In this paper, we focus on the two related standards; ISMS (Information Security Management System) which is the standards of the information security and CSMS (Cyber Security Management System) which is the standard of the system control security and create pertinent information by using our developed method to create pertinent information between security standards. In addition, we discuss the compatibility between two standards by extracting the common items and the individual items.

Keywords: Security Standards, Information Security Management System, Cyber Security Management System

1. 研究背景と目的

これまで閉じたシステムであった制御システムや産業システム（FA: Factory Automation）において，ネットワークに接続し状態の監視や生産性の効率向上を図るようになった．このため，例えば電力では DNP3.0，化学プラントでは Modbus，ビル制御系では BACnet といった業界で使われていた独自プロトコルや専用の OS から，情報系ネットワークで使われている汎用プロトコルや Windows や Unix といった汎用 OS が使われるようになりオープン化が進んでいる．特に，SCADA (Supervisory Control And Data Acquisition) や HMI (Human Machine Interface) といった監視制御に使われるようになり，制御システムであっても情報システム同様の脆弱性に対応する必要が出てきた．それだけではなく，PC と監視・制御ソフトウェアとを組み合わせてプロセスの制御・監視を実行する PLC (Programmable Logic Controller) において脆弱性を探す攻撃が行われたり[1]，SHODAN を使って脆弱性のある PLC を見つけ攻撃[2]したりする．

このため制御システムを狙った攻撃が増加しており[3]，これまでの情報システムにおける資産の保護だけでなく，継続性，制御，安定性などから保護する必要が出てきた．

†1 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
†2 東京電機大学
Tokyo Denki University
†3 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
†4 東芝
Toshiba Corporation
†5 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
†6 静岡大学 創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

特に，これまで保護の必要がなかったシステム同士が接続することで新たな脅威が生まれ，新たな対策を考慮する必要が出てきている[4]．例えば，2009 年にイランの核施設で発生した Stuxnet による攻撃は，特定の PLC を狙ったサイバー攻撃である[5]．最近では，2015 年 12 月にウクライナで BlackEnergy と呼ぶマルウェアにより大規模停電[6]が，2016 年 1 月にイスラエルの電力公社がサイバー攻撃により大規模停電を起こした[7].

このため，制御システム業界においてもセキュリティ対策が求められるようになり，業界毎の標準化が進められている．特に汎用制御システムでは IEC 62443 が策定されており，制御システム事業者向けのセキュリィマネージメントである CSMS（Cyber Security Management System）や，組込み機器がセキュアな特性と動作を有するか，セキュリティの設計開発や管理がされていることを示す EDSA（Embedded Device Security Assurance）といった認証制度が日本でも運用されている．

我々は，これらの脅威を呼び起こす原因の一つとして，接続する個々のシステムにおけるセキュリティ基準（または標準）が独立していてうまく連携していないことがあると考える．即ちこれは異なる視点からなるセキュリティの基準同士の連携が取られていないことに起因しているとい言える．

これまでセキュリティ標準に関する研究は多くなされており，数多くの成果が報告されている[8][9][10]．そこで我々は，それらの研究や技術をベースとして拡張を行うことで IoT セキュリティの実現を目指すことを目的とした提案を行ってきた[11]. 本稿では，異なる視点からなるセキュリティ基準同士の連携に関する問題に着目し，これまで我々が研究を行った来た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（以下，提案プラットフォーム）の関連情報作成手法[10]を用いて後述する情報システムに関する基準である ISMS と制御システムに関する基準である CSMS といった異なる視点から策定された標準の関連情報の作成を行った．

2. 関連する規格

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[12]. MSS では，PDCA(Plan-Do-Check-Act)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[12]．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[12] 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．現在 MMS 共通テキストによる標準の改版が行われているが，すべての分野に適応されているとは限らず未だ標準の記述方法についての共通化は完了していない．

2.2 ISMS：Information Security Management System

一般に ISMS として知られている標準に，ISO/IEC 27001 がある．これは，MSS 共通テキストに基づき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[13]. 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[12]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 月に ISO/IEC 27001：2013 要求事項が発行された．日本では JIPDEC による認証制度14があり，認証取得件数は 2016 年 7 月現在で 4,921 件となっている[15].

本稿では，最新版である 2013 年版（以下，ISMS 認証基準）を用いて関連情報の作成を行った．

2.3 CSMS：Cyber Security Management System

CSMS とは，重要インフラなどの制御システムのセキュリティを確保するため，2010 年に IEC（International Electrotechnical Commission: 国際電気標準会議）が国際標準 IEC 62443-2-1 として定めたものである．これは，制御システム製造業者や運用会社に対しセキュリティついて取り組むべき組織マネジメントを規定したものである．日本では, ISMS と同様に JIPDEC が認証機関となり制度を運用している[16]. ISMS が情報システムに対するマネジメントシステムであるのに対し，CSMS はオートメーションおよび制御系システム（IACS：Industrial Automation and Control System）を対象としたサイバーセキュリティマネジメントシステムである．前述のとおり, IACS は専用システムで構成され外部ネットワークから遮断されていた．しかし，IoT 時代の到来により外部ネットワークにつながり, 汎用の OS や通信プロトコルを使うようになったため，セキュリティ上の脅威は無視できないものとなった．日本では，認証制度が 2014 年に始まった[17].

本稿では，JIPDEC によって公開されている CSMS 認証基準（IEC 62443-2-1）サイバーセキュリティマネジメントシステム（以下，CSMS 認証基準）[18]を用いて関連情報の作成を行った．

2.4 ISMS と CSMS の関係

今回着目した ISMS と CSMS の関係は，CSMS 認証基準が ISO/IEC 27001 を参考に，IACS 特有の部分の追加という形で作成されているという関係になる[17]．そのため多くの要求事項に共通が見て取れる．また，ISMS ではセキュリティの 3 要素の機密性（Confidentiality），完全性（Integrity），可用性（Availability）を C.I.A.の順で重視しているが，CSMS では A.I.C.の順で重視し，その他にも HSE（Health: 健康, Safety: 安全, Environment: 環境）も重視するなどの違いがある[17].

3. セキュリティ評価プラットフォーム

提案プラットフォームでは複数の標準を同じ仕組みで評価を行うことを想定している[8]．本稿では，図 1 で示す概念図の関連情報を作成する技術[10]を用いて ISMS 認証基準と CSMS 認証基準の関連情報を作成する．

提案プラットフォームでは，初期の入力データとして標準の生データ，文書構成に基づく章節項といった各項目の構成情報，標準文書内に記載されている参照先といった参照情報を登録する．

複数の標準を登録した際に，標準間の項目同士の関連を示す情報があればそれも登録する．しかしそこで，標準間の関連情報が必ずしも定義されていないという問題が存在する．そういった場合に我々は，自然言語処理を用いた関連情報作成手法を提案している[10][19]．この手法では文書間の相関を求めてより文章的に近しい項目同士を関連情報として抽出している．本稿では，特殊な辞書などを用いずにシンプルな手法のみを用いて関連情報の作成を行うことで，ISMS と CSMS 間の親和性をより明確化することを目指した．

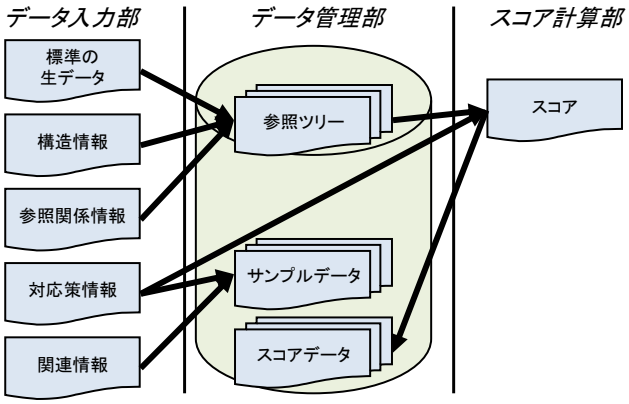

図 1　提案プラットフォームの概念図

Figure 1　Conceptual Diagram of Proposed Platform

3.1 関連情報作成手法

我々は，異なる標準間の関連情報を作成するために項目間の相関を取る方法を用いている．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使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をしている[20].

はじめに，関連情報抽出の対象となる文書（以下，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」[21] などを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[20]．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[20] 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[20]．提案プラットフォームにおける関連情報作成手法では，方式選定段階で最も高い精度を示した余弦を用いた近似度計算を採用している．最後に，各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．抽出された相関がある組み合わせが妥当であると判断された場合，その組み合わせの集合を関連情報とする．

また，相関がある組の妥当性を検証するにあたり，各項目を図 2 で示すように要求事項（Why）を中心とした 5W1H（Why, Who, What, When, Where, How）のセキュリティ文法で分解し比較することも提案している[11].

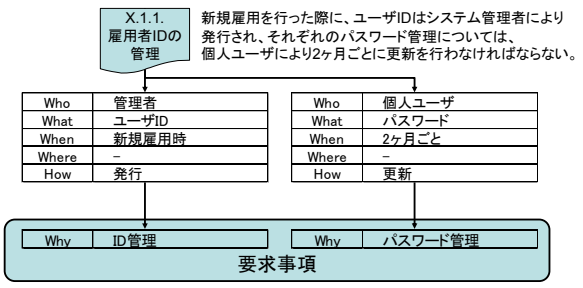

図 2　セキュリティ文法による分解の例

Figure 2　Example of Decomposition by Security Grammar

4. ISMS と CSMS の関連情報作成実験

4.1 実験概要

提案プラットフォームの関連情報作成手法を用いて，ISMS 認証基準と CSMS 認証基準の関連情報を作成する．そして，作成された関連情報から視点の違う標準間の関連情報を作成する際に留意すべき内容の考察を行う．

4.2 実験手順

最初に，提案プラットフォームの関連情報作成手法を用いて，ISMS 認証基準と CSMS 認証基準の相関のある項目の組を抽出する．本実験では，相関がある組を抽出する際に基準間の項目の階層に差があるため項目の階層に関係なく全ての項目を一斉に文書比較を行った．また，使用される形態素の重み付けについても各形態素に一律 1 の重みを与えた．

次に，抽出された組について直接項目内容を確認しその組み合わせが同じ内容を示しているかを判別する．区分としては，違和感が無い組，違和感が有るが間違った組み合わせとまではいかない組（以下，違和感が残る組），同一の内容とするには違和感が有る組の 3 通りに分類した．

そして，それぞれの組み合わせについてどのような特徴があるかの考察を行う．

4.3 実験結果

用語の定義などを除いた ISMS 認証基準の 4 章以降の全 157 項目と CSMS 認証基準の 4 章以降の全 161 項目について項目間の相関を求めた結果， 表 1 で示すように，35 の組み合わせで文書的な相関がありそのうち CSMS 側の 2 項目は ISMS の 2 項目と相関があるという結果を得ることができた．

表 1　ISMS と CSMS の相関情報

Table 1　Correlation Information between ISMS and CSMS

	項目数	相関が見つかった項目数	複数の相関が見つかった項目数
ISMS認証基準	157	35	0
CSMS認証基準	161	33	2

2 項目と相関があるという結果を示した項目は，図 3 で示す 2 項目となり，いずれの項目も ISMS 認証基準では 2 項目に分かれて内容記述されていた項目となる．CSMS 認証基準の 4.4.3.4 にあたる ISMS 認証基準の項目は是正処置に関する項目と，予防処置に関するに分かれており，5.1 にあたる項目は事業計画とその継続に関する項目に分かれて記述されていた．

5.1 事業継続計画

4.4.3.4　是正処置及び予防処理の識別及び導入
--組織は、セキュリティ目的を満たすために
CSMSを変更する適切な是正処置及び
予防処置を、識別及び導入しなければならない。

図 3　複数項目との相関を示した項目

Figure 3　Item of multiple correlation

そして，抽出された項目の組を筆者の目で確認して，分類した結果は表 2 で示すようになり半数は違和感の無い組として抽出されていた．

表 2　相関がある組の内訳

Table 2　Detail of Correlation Information

	違和感		
	無し	残る	有り
組み合わせ数	17	14	4

4.4 考察

①　複数項目との相関を示した組

図 3 で示したような複数項目との相関を示す組が発せ下背景には，項目間の相関を取る際に行った各形態素の重み付けを一律 1 に設定したことが関係していると推察される．これまで我々は，視点が同じ ISO/IEC 27000 ファミリー（以下，27000 ファミリー）[22]と国内の JIS Q 27001 の各文書を比較することを中心に実験を行ってきた[10][11][19][23]．これらの比較実験で使用した標準でも各項目が複数の要求事項を持つことは文献[11]で標準の各項目をセキュリティ文法で分解した際に確認できている．しかし，定義されている関連情報に 1:n または，m:n となる組み合わせがなかったため，詳細な近似度を求める方がよいと判断し形態素の重みづけに関する検討を行っていた．本実験で使用した CMSM 認証基準は ISMS 認証基準の複数の要求事項が図 4 で示すようにひとつの項目に含まれていた．同一比重で含まれている場合と限定されるが，このようなケースでは重み付けを行わない方が良い結果と推察される．

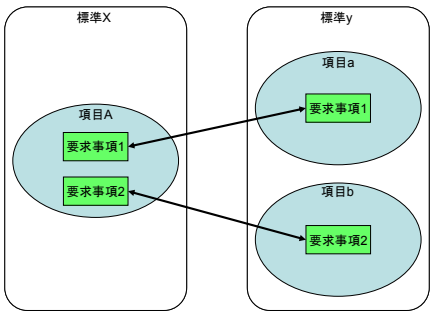

図 4　別の標準で複数要求事項が含まれる例

Figure 4　Example of Multiple Requirements in Other Standard

② 違和感が無い組

目視の結果違和感がない組では，お互いの文章で 3 章までの定義などに記述されている特徴的な用語（以下，専門用語）の使用が少なく一般的な要求中心であることがわかった．また，専門用語が含まれる場合も繰り返し使われず簡素な記述となっている傾向があると推察される．

また，項目の階層が違う項目と相関がある組もあるが，妥当な組み合わせと判断できた．これらは視点が異なることにより，より詳細な内容を示しているか，大まかな内容に集約されているかという違いが出てためと推察される．

③ 違和感が残る組

近似度が低いものも多くセキュリティ文法で分解すると一致しないものもいくつか見つかった．しかし，該当項目の上位または下位の階層の情報から対象範囲などの条件まで確認すると組み合わせとして妥当であるものもあったため，判別は困難ではあるが有効な情報であると推察される．類義語などを定義して専門用語の差異を埋めたり，上位や下位の概念を含めた判断をする仕組みを組み込んだりすることで信頼性をあげることができるのではないかと推察される．

④ 違和感が有る組

抽出されたものとしては数が少なかったが，双方の文章量が著しく異なったり，主要な語は同じであっても目的が異なっていたりと目視であれば妥当な組み合わせとすることが困難な組み合わせであった．傾向としては，セキュリティ文法でいうところの When にあたる部分で相違があることが多いと推察される．

⑤ 抽出されなかった項目

相関がある項目が抽出されなかった項目についてもいくつか特徴的なものがあった．それは，それぞれの基準の専門用語が多く使用されていたものである．本実験では特別な辞書を用いないで，かつ類義語などの定義も行わないずに純粋な文字列比較による近似度を出す形で相関を求めた．その結果，専門用語を中心として記述されている項目については近似度にばらつきが出て双方から見て最大値を取るという条件を満たす組が表れないという状態となった．視点が違うことにより，専門用語として定義される際に同じ語として定義されない可能性があると推察される．例えば ISMS 認証基準では主体の多くを ISMS としているが，同様の内容を CSMS 認証基準では IASC としていたり，ISMS 認証基準では項目へ対処する方法を対応策と記述するが，CSMS 認証基準では対抗策と記述したりするという違うが見られた．同一の視点で策定される場合は，正確な意味を取ることで関連情報の作成精度が上がるが，視点が異なる場合は，正確な意味というよりも同じ目的で使用されている語をまとめることの方が重要であると推察される．

5. 今後の課題

4.4 節に示したように, 視点が同じ基準間の比較と視点が異なる基準間の比較では精度を上げるための技術が異なることが推察される．

今後は，辞書構築に関わる問題として適切な類義語の定義方法や複合名詞の作成方法などに関する問題や，各形態素に対する重みづけに関する問題について検討，提案を行っていきたい．

また，ISMS 認証基準と CSMS 認証基準といった組織レベルの基準だけではなく例えば PCI DSS[24]のような業界標準などについても関連情報作成手法を適用していきたい．

6. まとめ

本稿では，提案プラットフォームの要素技術である関連情報作成手法を用いて ISMS 認証基準と CSMS 認証基準の関連情報の作成を行い，異なる視点に基づき策定された基準を扱うにあたり留意するべき内容について考察を行った．

考察の結果，同じ視点に基づき作成された基準間の比較と異なる視点に基づき作成された基準間の比較では，近似度を求める際の辞書構築に関する課題，各形態素への重みづけに関する課題など本質的な課題は共通しているが解決するためのアプローチを変える必要があることがわかった．

今後は，5 章で述べた課題に取り組み IoT セキュリティに貢献できる技術へと発展させていきたい．

参考文献

[1] 警察庁: 産業制御システムで使用される PLC を標的としたアクセスの観測について，@police, 2015.12.9（オンライン），入手先 <https://www.npa.go.jp/cyberpolice/detect/pdf/20151209.pdf>(参照 2016-8-11)

[2] JPCERT/CC: SHODAN を悪用した攻撃に備えてー制御システム編ー，2015.6.9（オンライン），入手先 <https://www.jpcert.or.jp/ics/20150609ICSR-shodan.pdf>（参照 2016-8-10）

[3] ICS-CERT: NCCIC/ICS-CERT Year in Review (2015)， 2015（オンライン），入手先<https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf>（参照 2016-8-11）

[4] 独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC）：つながる世界のセーフティ＆セキュリティ設計入門～IoT 時代のシステム開発『見える化』～，独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC），(2015-10-7)

[5] WIRED: 核施設を狙ったサイバー攻撃『Stuxnet』の全貌，2012.6.4（オンライン），入手先< http://wired.jp/2012/06/04/confirmed-us-israel-created-stuxnet-lost-control-of-it/>（参照 2016-8-11）

[6] McAfee Blog: ウクライナのサイバー攻撃が示す本当の脅威，マカフィー，2016.1.27（オンライン），入手先 <http://blogs.mcafee.jp/mcafeeblog/2016/01/post-748a.html>（参照 2016-8-10）

[7] ITmedia エンタープライズ: イスラエル電力公社、大規模なサイバー攻撃で「マヒ状態」に，ITmedia Inc. 2016.1.28（オンライン），入手先 <http://www.itmedia.co.jp/enterprise/articles/1601/28/news060.html>（参照 2016-8-11）
[8] 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).
[9] 堀川博史，大谷尚通，髙橋雄志，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝: デルタ ISMS モデルの提案-事故データベースに基づく ISMS の強化-，情報処理学会研究報告コンピュータセキュリティ（CSEC），2015-CSEC-70(24)，pp.1-7 (2015-06-25)
[10] 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).
[11] 髙橋雄志，金子朋子，堀川博史，加藤岳久，間形文彦，西垣正勝，佐々木良一，勅使河原可海：IoT セキュリティにおけるセキュリティ評価プラットフォーム活用の提案，マルチメディア，分散，協調とモバイル(DICOMO)シンポジウム論文集，pp.666-670
[12] 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 第 5 版（オンライン），入手先 < http://www.jsa.or.jp/wp-content/uploads/isohosoku_taiyaku1405.pdf>(参照 2016-08-03)
[13] ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements(2013)
[14] 一般財団法人日本情報経済社会推進協会（JIPDEC）：ISMS 適合性評価制度（オンライン），入手先 <http://www.isms.jipdec.or.jp/isms.html >（参照 2016-08-03）
[15] 情報マネジメントシステム認定センター：認証取得組織数推移、認証機関別・県別認証取得組織数（オンライン），入手先<http://www.isms.jipdec.or.jp/lst/ind/suii.html >(参照 2016-08-03)
[16] 一般財団法人日本情報経済社会推進協会（JIPDEC）：CSMS 適合性評価制度の概要（オンライン），入手先 <http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS120-10.pdf>（参照 2016-08-03）
[17] 一般財団法人日本情報経済社会推進協会（JIPDEC）：CSMS 適合性評価制度の概要（オンライン），入手先 <http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS120-10.pdf>（参照 2016-08-03）
[18] 一般財団法人日本情報経済社会推進協会（JIPDEC）：CSMS 認証基準（IEC 62443-2-1）サイバーセキュリティマネジメントシステム（オンライン），入手先 <http://www.isms.jipdec.or.jp/csms/doc/JIP-CSCC100-10.pdf>（参照 2016-08-03）
[19] 太田悟，髙橋雄志，勅使河原可海，篠宮紀彦: セキュリティ評価プラットフォームにおける国際標準間の関連情報作成手法の提案と実装，情報処理学会第 76 回全国大会(2014-3)
[20] 徳永健伸: 情報検索と言語処理，東京大学出版会(1999)
[21] 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)
[22] 一般財団法人日本情報経済社会推進協会（JIPDEC）：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/27000family_20160617.pdf>（参照 2016-08-07）
[23] 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)
[24] Payment Card Industry Security Standards Council: PCI SSC Data Security Standards（オンライン），入手先 <https://www.pcisecuritystandards.org/security_standards/>（参照 2016-08-08）