Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

ISMS と CSMS の関連情報作成における個別項目抽出に関する考察

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）の相関がある項目の組を抽出した．本稿では，作成過程で作成した形態素解析の結果を分析し類義語や固有項目に含まれる特徴的な語の傾向を分析した．

キーワード：キーワード：セキュリティ標準，ISMS，CSMS

A Study of the Unique Item 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 this paper, we analyzed the result of the morphological analysis made by the pertinent information creation method and found the tendency of the characteristic word included in synonym and the unique item.

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) などに使われ，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 を見つける攻撃も起きたりしている[2].

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．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

†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

Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

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[8].

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[9][10][11]．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[12]．そして，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[11]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間で相関の有る項目の抽出を行い，抽出された組中心に考察を行った[13]．ISMS は全社的な情報セキュリティが対象であるが，CSMS は制御システムに関連するセキュリティに特化している．しかし，後述する 2.4 節で示すような関係から共通している項目もあり，例えば既に ISMS を取得している組織が新たに CSMS を取得しようとする場合，速やかに新たに取り組むべき対策がわかり実施できることが望ましい．即ち，ISMS と CSMS とで取得する際の異同が分かることは，組織にとって重要であり取得コストを下げることにもつながる．本稿では，関連情報作成の際の中間データとなる形態素解析の結果を分析し，類義語や固有項目に含まれるような特徴的な語の抽出，各標準の記述にどのような傾向があるかについて検討を行った.

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[14]. 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[14]．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[14] 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[15]. 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[14]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 があり，認証取得件数は 2016 年 12 月現在で 5,024 件となっている[16].

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

Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

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[17]. 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[18].

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）[19]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[18]．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[18].

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[9]．本稿では，図 1 で示す概念図の関連情報を作成する技術[11]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.

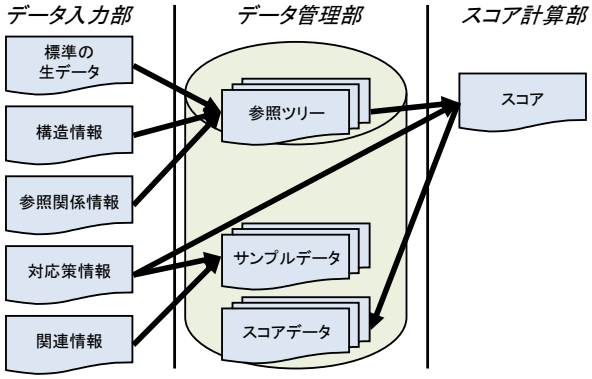

図 1　提案プラットフォームの概念図
Figure 1　Conceptual Diagram of Proposed Platform.

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[11][20]．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．そして，関連情報として抽出されなかった項目が各標準の固有項目となっている可能性が高いことも示している[21]．また，関連情報作成の精度を上げるための辞書構築に関する検討では，形態素解析を実施した際の出現回数に着目し重要な語の抽出をすることができている[22].

本稿では，相関が有る組が抽出されなかった項目を固有項目とみなすために，文献[22]で重要な語を抽出するために行った解析を適応して各項目に関する考察を行った.

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している[23].

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」[24] 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[23] 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[23]．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

Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

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[12].

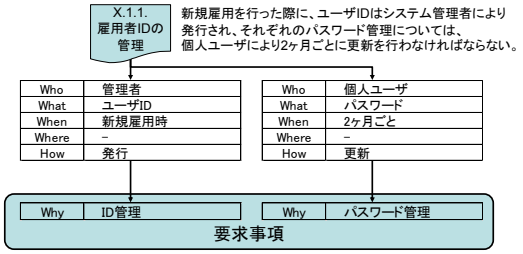

図 2　セキュリティ文法による分解の例

Figure 2　Example of Decomposition by Security Grammar

4.　標準固有項目に関する分析

4.1　ISMS 認証基準と CSMS 認証基準の関連情報の作成

文献[13]では, ISMS 認証基準と CSMS 認証基準に関連情報作成手法を適応し, 相関がある項目の組の抽出を行った．そして，抽出された組み合わせに違和感が有るか否かを確認し，違和感がある組，ない組，一見して違和感があるが妥当であると判断できた組の特徴について考察を行った．この段階では，相関がある項目の組がみつからなかった項目についての詳細な分析を行っていなかったが，評価基準ごとに同じ意味で異なる用語が使用されていることが一部確認できている．

4.2　分析概要

本稿における分析では，関連情報作成手法を適応した際の中間データとなる形態素解析データリストを取得し，顧客分析手法の一つで全顧客を購入金額の高い順に 10 等分し、その売上構成比を分析する分析手法であるデシル分析[25]を行い，10%充足値でデシル値（以下，D 値）を与えて各形態素についての分析を行う．

4.3　分析手順

①　形態素リストの作成

認証基準ごとではなく全体でひとつのテーブルとして形態素, 認証基準名, 項番を要素に持つテーブルを作成する．作成したテーブルをもとに集計リストとして全体としての出現回数，認証基準ごとの出現回数を集計し形態素リストとする．

②　D 値の設定

①で作成したリストに基づき，D 値を全体，ISMS 認証基準，CSMS 認証基準のそれぞれに 10%充足値で出現回数が多い方から順に D01 から D10 まで, 出現回数が 0 となる形態素には DZZ の値を設定する．ただし 10%充足で同じ出現回数の形態素があった場合には上位の値を設定するものとする．

③　各認証基準における DZZ リストの作成

ISMS 認証基準, CSMS 認証基準のいずれかの D 値が DZZ となる片方の認証基準でしか用いられなかった形態素のリストを作成.

④　DZZ リストの分析

③で作成したリストから標準記述方式の特徴などを分析する．また文献[13]の考察で記述した類義語の関する検討も行う．

4.4　分析結果

①　リストの作成

文献[13]の形態素解析の結果をもとにテーブル作成を行い，リスト化を実施した．固有項目を確認するために追加作業として，記号のみの形態素や略語と正式名称などいった不要と思われる要素の削除を行った．今回の組み合わせでは約 700 種類の形態素が使われていた．

②　D 値の設定

全体，ISMS 認証基準，CSMS 認証基準の出現回数に基づく D 値を設定．図 3，図 4，図 5 の図で示すようにすべての場合で上位約 30%の形態素が全体の 80%（D01 から D08）の占めることがわかった．また，各評価基準で D09，D10 の形態素の出現回数は 3 回以下であるため分析の対象外とした．

③　各認証基準における DZZ リストの作成

ISMS 認証基準, CSMS 認証基準のそれぞれの認証基準に基づく D 値が DZZ となる形態素のリストを作成．ISMS 認証基準で DZZ となった形態素は約 400 種類となり，CSMS 認証基準で DZZ となった形態素は約 140 種類となった．それぞれのリスト上位一部を図 6，図 7 に示す．

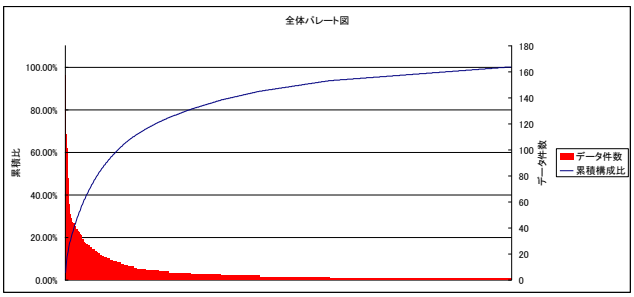

図 3　全体のパレート図

Figure 3　Pareto Diagram of All

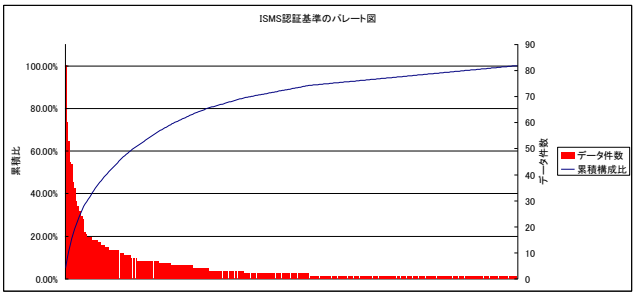

図 4　ISMS 認証基準のパレート図

Figure 4　Pareto Diagram of ISMS Authentication Standard

Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

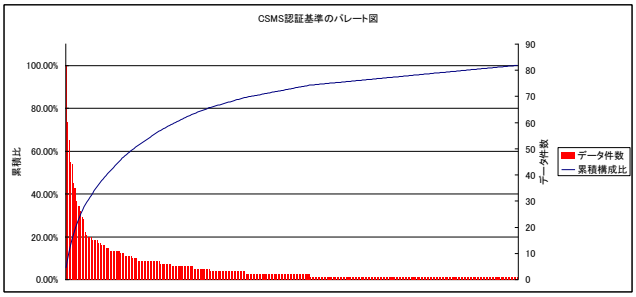

図 5　CSMS 認証基準のパレート図

Figure 5　Pareto Diagram of CSMS Authentication Standard

形態素	ISMS_D値	CSMS_D値	全体_D値
IACS	DZZ	D02	D02
手順	DZZ	D02	D03
サイバー	DZZ	D02	D03
CSMS	DZZ	D03	D04
ポリシー	DZZ	D03	D04
アカウント	DZZ	D03	D05
定義	DZZ	D03	D05
要員	DZZ	D04	D05
詳細	DZZ	D04	D05
導入	DZZ	D04	D05
インシデント	DZZ	D04	D05
制御	DZZ	D05	D06

図 6　ISMS 認証基準の DZZ リスト

Figure 6　DZZ List of ISMS Authentication Standard

形態素	CSMS_D値	ISMS_D値	ALL_D値
ISMS	DZZ	D02	D03
不適合	DZZ	D05	D07
測定	DZZ	D06	D07
注記	DZZ	D06	D07
有効	DZZ	D06	D07
達成	DZZ	D06	D07
人々	DZZ	D07	D07

図 7　CSMS 認証基準の DZZ リスト

Figure 7　DZZ List of CSMS Authentication Standard

④　DZZ リストの分析

ISMS 認証基準の DZZ リストから「IACS，CSMS」といった CSMS 認証基準の特徴的な形態素を検出することができている．同様に CSMS 認証基準の DZZ リストからは「ISMS」といった ISMS 認証基準の特徴的な形態素が検出されている．また，CSMS 認証基準の「要員」に対する ISMS 認証基準の「人々」，CSMS 認証基準における注釈を示す「詳細」に対する ISMS 認証基準で注釈を示す「注記」といった類義語が検出されている．

ISMS 認証基準のリストの方が含まれる形態素が多く，CSMS 認証基準のリストの方が含まれる形態素が少ないことから ISMS 認証基準の方が多くの語を使い文章が構成されていることから，広範囲をカバーしていて細かな内容が記述されていると思われる．このことは認証基準の対象物の差異に一致している．

4.5 考察

関連情報作成手法では，類義語の定義をすることによってその精度を上げることができると考えていた．本稿における分析でも同じように，認証対象の主体（もしくは対象物）を示していて広い意味で同じように使用される形態素同志を類義語と定義することが有効な手段であると推察される．このような語の組み合わせを以後セット語と定義し用いることとする．

ISMS 認証基準と CSMS 認証基準の間では，「IACS，CSMS」に対する「ISMS」，「要員」に対する「人々」，「詳細」に対する「注記」がセット語の候補としてあげることができる．しかし，ISMS 認証基準では「対策」と統一されている形態素でも CSMS では「対抗策」と「対策」のように，近しい内容を示すのに使い分けが行われていたため，この評価基準の組み合わせでは，セット語として定義をすることは不適切と判断した．

5. 今後の課題

本稿で扱った異なる視点からなる評価基準の関連情報を作成する際は，セット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があるので更なる検討，提案を行っていきたい．

4.5 節で示した，「対策」と「対策，対抗策」といったように 1 : n または m : n といった形で使い分けが行われている形態素についてはセット語の定義の可否から検討が必要である．

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カード業界のセキュリティ基準である PCI DSS[26]や，自動車業界の機能安全の基準である ISO 26262[27]等の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，関連情報作成手法を実行する際の中間データである形態素解析の結果を分析し，セット語として定義すべき形態素と，固有項目なる項目に使用される形態素の抽出に関する考察を行った．

分析の結果，比較対象の基準で使用されず比較元の標準で多用されている形態素がセット語として定義すべき形態素や固有項目で使用されている形態素である可能性が高いことがわかった．本稿の分析と文献[13]の実験結果より，評価基準間には用語の不統一といった問題があることがわかり，このような問題が新たな認証を取得しようとする際の大きな障害の 1 つとなっていると考えることができる．

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．

Vol.2017-GN-100 No.31
Vol.2017-CDS-18 No.31
Vol.2017-DCC-15 No.31
2017/1/21

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，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，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，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，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，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，http://www.itmedia.co.jp/enterprise/articles/1601/28/news060.html , (参照 2016-8-11)

[8] CSSC 認証ラボラトリー，http://www.cssc-cl.org/，(参照 2016-12-19)

[9] 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).

[10] 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)

[11] 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).

[12] 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，(2016-07)

[13] 髙橋雄志，佐藤信，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：ISMS と CSMS との関連情報作成の提案，コンピュータセキュリティシンポジウム 2016 論文集，2016(2)，pp128-133，(2016-10)

[14] 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，http://www.jsa.or.jp/wp-content/uploads/isohosoku_taiyaku1405.pdf，(参照 2016-08-03)

[15] ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements(2013)

[16] 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，http://www.isms.jipdec.or.jp/lst/ind/suii.html，(参照 2016-12-12)

[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，http://www.isms.jipdec.or.jp/csms.html，(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 適合性評価制度の概要，http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS120-10.pdf，(参照 2016-08-03)

[19] 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，http://www.isms.jipdec.or.jp/csms/doc/JIP-CSCC100-10.pdf, (参照 2016-08-03)

[20] 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)

[21] 太田悟，髙橋雄志，勅使河原可海，篠宮紀彦: 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，情報処理学会論文誌コンシューマ・デバイス＆システム第 5 巻，pp57-66，(2015-02)

[22] 髙橋雄志，太田悟，間形文彦，西垣正勝，佐々木良一，篠宮紀彦，勅使河原可海: 標準間の関連情報作成のための辞書構築手法の提案，情報処理学会研究報告コンシューマ・デバイス＆システム（CDS），2015-CDS-12(28)，pp1-8，(2015-01-19)

[23] 徳永健伸: 情報検索と言語処理，東京大学出版会(1999)

[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)

[25] デシル分析とは ～ exBuzzwords 用語解説，http://www.exbuzzwords.com/static/keyword_3510.html，(参照 2016-12-19)

[26] Payment Card Industry Security Standards Council: PCI SSC Data Security Standards，https://www.pcisecuritystandards.org/security_standards/，(参照 2016-08-08)

[27] 機能安全（ISO26262）, 一般財団法人日本自動車研究所（JARI）, http://www.jari.or.jp/tabid/112/Default.aspx，(参照 2016-12-13)