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

髙橋雄志[1] 金子朋子[2] 堀川博史[3] 加藤岳久[4]
間形文彦[5] 西垣正勝[3] 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．しかし，相互接続により，セキュリティ上の脅威が大きくなると考えられる．我々は，これらの脅威の原因の一つとして，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）が独立していて連携がとれていないことがあると考える．これらの問題に対して，従来のセキュリティ研究・技術を応用することで問題解決を図ることを提案する．中でも我々が研究を進めてきたセキュリティ評価プラットフォームに関しては，関連情報作成手法に新たにセキュリティ文法による分解，マッチングの作業を追加する実験を行った結果を示す．

Proposal of Security Evaluation Platform Utilization in IoT Security

YUJI TAKAHASHI[1] TOMOKO KANEKO[2] HIROSHI HORIKAWA[3]
TAKEHISA KATO[4] HUMIHIKO MAGATA[5] MASAKATSU NISHIGAKI[3]
RYOICHI SASAKI[1] YOSHIMI TESHIGAWARA[1]

1. 研究の背景と目的

近年，各種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サービスを提供するようになってきている．特に，これまでインターネットに接続していなかった制御機器や家電製品，センサーなどが接続され，様々なデータを収集・分析することで新たなサービスが生まれている．こういった環境をモノのインターネット（IoT: Internet of Things）と呼び，新産業革命という声も上がるくらい大きな期待が寄せられている．しかし，システム間の相互接続という観点からセキュリティに関する脅威は大きな関心事として取り上げられている[1].

IoT でつながるシステムは，従来のスマートフォン，携帯電話，ゲーム機といった情報機器だけにとどまらず，自動車，テレビ，レコーダー，ヘルス機器といった生活機器にまで広がっていく．こうした組み込みシステムがつながることで，単純な情報のやりとりだけではなく，機器の操作も行われるようになり，機器同士が連携して動作をするため意図しない動作を起こさせるセキュリティ被害が起こることが推測される[2].

実際にスマートハウスのセキュリティ事例として，販売された Home Energy Management System（HEMS）の一部のモニタ画面がネット上で見える状態になっていたとの報告がなされている[3]．その他にもスマート冷蔵庫のモニタから連携サービスの情報が搾取されてしまう可能性[4]や，自動車の遠隔操作が成功した事例[5]，電光掲示板を用いた交通システムのデータ書き換えの事例[6]など多くのセキュリティ事象が報告されている．

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．

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[7][8][9]．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．本研究ではこのような拡張を研究・技術の IoTS 化（for IoT Security の意）と定義し，同様に IoTS 化したシステムを IoTS シリーズと定義して【システム・技術名】-IoTS と表現するものとする．

また，我々はこれまで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）の研究をしてきた[7]．この提案プラットフォームでは，異なる標準間の関連情報や，標準の各項目と対応策の対応をデータとして使用している．これらの技術は，IoT セキュリティにおける脅威に対応できる技術であると我々は考える．

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 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
3 静岡大学 創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
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

本稿では，IoT セキュリティを考える上で脅威となる問題とその原因について考察し，注目している研究・技術の IoTS 化の方向性を提案する．そして，実際に提案プラットフォームの IoTS 化を行って，IoT セキュリティの課題に対して有効であることを示す．

2. IoT セキュリティにおける課題および関連研究・技術の IoTS 化

本章では，IoT セキュリティの問題点の中でも特に，相互接続に基づく問題点について注目し掘り下げ，原因を考察し課題を示すと共にいくつかの従来研究・技術の IoTS 化の入り口を示す．

システムの相互接続を行う際に考えられる脅威としては，接続後のシステム全体をカバーする標準がないため，システム全体を評価することが困難であることがあげられる．また，個々のシステムのセキュリティが確保されていたとしても，それぞれの基準でのセキュリティ強度が異なり全体として求められるセキュリティ強度の達していない可能性がある．

こういった個々のセキュリティを示す基準間の差分を埋めるための，従来のセキュリティに関する研究・技術の IoTS 化を以下に示す．

2.1 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[7]．図 1 で示す概念図のマークされている対応策情報と関連情報に関する技術を応用することで IoTS 化を行う．本稿では，この提案プラットフォームの IoTS 化について詳細検討を行った．

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][11]．この手法では文書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が，相関が高いにも関わらず関連情報ではない組が抽出される場合がある．その際には項目の意味を理解する必要があることが確認されている．

そして，対応策の登録では標準の項目と対応策を結びつけるという粒度や視点の違う情報を結びつける必要がある．そこで本稿では，5W1H（Who，What，When，Where，Why，How）からなるセキュリティ文法を定義し粒度と視点が違う情報を主要な要素に分解しつなぎ合わせることとした．前述の関連情報作成手法の問題点も作成された関連情報の多重確認にこのセキュリティ文法を用いることで解決する．

提案プラットフォーム-IoTS では，IoT に接続される各機器の標準間の関連情報を関連情報作成手法で作成し，適時セキュリティ文法による多重チェックを行って標準間の共通項を見つけ出す．これによって IoT システム全体としてのセキュリティ強度を測ることができると推察できる．提案する手法の詳細については 3.3 節に示す．

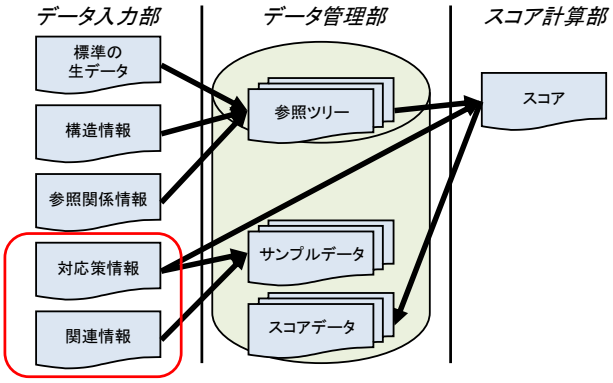

図 1　提案プラットフォームの概念図

2.2 Cybersecurity-Framework

Cybersecurity-Framework とは，米国国立標準技術研究所（NIST: National Institute of Standards and Technology）により提案されていて，プロファイルを作成するためのガイダンスとしてのフレームワークコア，企業における対策その他のバランスを鑑みるために活用できるフレームワークプロファイル，自組織のサイバーセキュリティリスクの特徴を確認・理解するためのフレームワークインプリメンテーションティア*1（以下，ティア）から成り立っている[12]．

我々は IoTS 化の方法として，フレームワークコアを 5 つの機能を最上位にするのではなく，その上に接続機器を並べ階層を増やし，機器ごとのティアの判定に基づき IoT システム全体のティアを判定する形式を提案する．イメージを図 2 に示す．

機器	機能	カテゴリー	サブカテゴリー	参考情報
機器1	特定			
	防御			
	検知			
	対応			
	復旧			
機器2	特定			
	防御			
	検知			
	対応			
	復旧			

図 2　フレームワークコア-IoTS のイメージ

1 サイバーセキュリティリスクを管理する上で，自組織のアプローチの特徴を確認し，理解するための仕組みを提供する要素[12]

2.3 デルタ ISMS

デルタ ISMS とは堀川らによって提案されていて，各組織の事故データベースを用いて，2 回目以降のリスク評価に事故のデータを利用し差分に基づく対策提案を行うものである．また，事故と対策をデルタ ISMS 表という表を用いて表現している[8]

我々は IoTS 化の方法として，事故データベースを組織のものではなく各機器に関する事故事例のデータベースとして，機器導入前と導入後の差分に基づくデルタ ISMS 表を作成し，対策案の提示を行う形式を提案する．

また，本稿では 2.1 節の提案プラットフォーム-IoTS のセキュリティ文法に基づくマッチング結果を表現するためにデルタ ISMS 表と同様の形式の表を用いて表現する．

2.4 CC-Case および CC-Case-i

CC-Case および CC-Case-i とは，情報セキュリティ大学院大学の金子らによって提案されている，コモンクライテリア（CC: Common Criteria）とアシュアランスケースを融合させたセキュリティ要求分析・保証の統合手法である[9].

CC-Case-i の方は，CC-Case にインシデントの考えを加えたものである．また，この手法が IoT に向けて活用できるのではないかという提案も文献[13]で示唆されている．文献内で提案している手法で IoT システム全体を表現することがそのまま CC-Case の IoTS 化となると考える．

2.5 HEMS

HEMS とは，スマートハウスなどでエネルギーの効率化を目的とした管理システムを指す．すでにモニタによって各種エネルギーの使用状況などの見える化が行われていたり，家電機器などの自動制御が行われていたりしている．

しかし，1 章で紹介した事例などが発生しておりセキュリティに関する考慮が必須である．

そこで，IoTS 化としてエネルギー効率とセキュリティ機能を融合させたシステムとすることで IoT セキュリティへの対応ができると考える．

3. セキュリティ評価プラットフォーム-IoTS

この章では，2.1 節で IoTS 化の方向を示した提案プラットフォーム-IoTS についてその適応範囲と拡張を行う技術およびその内容について示す．

3.1 適応範囲

本稿では，2 章にて問題提起したシステムの相互接続時に全体を包括する基準がないという状況を 2 つのケースに分けて考えた．それぞれのケースでどのような形で提案プラットフォーム-IoTS を活用するかを以下に示す．

① 接続されるシステムごとに基準があるケース

独自の基準に基づく評価をすでに受けているシステムが相互接続し，全体システムとして運用されることが想定される．こういった場合には，いずれかのシステムの脆弱性をつかれるインシデントが発生すると推察される．

このようなケースでは，提案プラットフォームの関連情報作成手法を用いることで，接続されているシステム間の関連項目を抽出することができ，強化すべき内容が確認できる．項目間の近似が低いが相関があると判断された組や特殊な表現を含む項目などがある場合は，後述のセキュリティ文法を併用して関連情報の精度を上げるべきであると考える．

② 基準がないシステムが接続されるケース

多くのシステムや機器でセキュリティ基準が定められつつあるがすべての機器が網羅されているわけではなく接続される機器のいくつかに基準が定められていない可能性がある．

こういったケースでは，すでに定められている基準をもとにしてセキュリティ文法に基づく項目の分解を行って比較対象を作成．続いて，基準が定められていない機器の対策をセキュリティ文法にて表現してマッチングを行ってセキュリティ評価を行う．

3.2 関連情報作成手法

本稿用いる関連情報作成手法は，文献[11]にて書かれているものをそのまま使用するものとする．以下に主な手順を示す．

①使用する各標準のテキスト情報を決定
②テキスト情報を形態素解析により形態素に分解
③索引語（文書の内容を表す要素）を抽出
④類似度を算出する際にノイズとなる語を削除
⑤抽出した語に対して重み付け
⑥ベクトルや行列で表わされた文書間の類似度を算出
⑦双方で類似度最大となる組を相関がある組として抽出

3.3 セキュリティ文法

文献[11]で行った関連情報作成手法に関する実験の結果として相関がある組として抽出された組の中に，実際には関連情報ではない組が含まれていた．その項目の文章を確認すると，文言は似ているが人が読み意味を解釈すると異なる内容を示していることがわかるものがあった．そこで得られた知見として意味的解釈により精度があるというものがある．

そこで本稿では，項目の内容を直感的に結びつける手段として 5W1H 分解することを提案する．それぞれの要素は，Who を関する要素，Where を場所に関する要素，When を時系列に関する要素，What をものに関する要素，Why を要求事項，How を手段や方法として定義した．

セキュリティ文法を用いたマッチングでは Why を基準に各要素を比較して要求事項の網羅性と，要求事項に対する対応内容が一致していることの確認を行う．詳細な方法については実験の中で後述する．

4. セキュリティ文法を用いた適応実験

4.1 実験の目的

本実験では，文献[11]で行った ISO/IEC 27001 付属書 A と ISMS 認証基準 Ver.2.0 付属書「詳細管理策」の関連情報を作成する実験で抽出された正しい組と FP（False Positive）となった組をいくつか選び，セキュリティ文法による分解とデータマッチングを行い，関連情報を正しく判別できることを示すことを目的とする．

4.2 実験手順

最初に，基準となる方の標準を分解して 5W1H の各要素に分解する．その際に，各項目を 5W1H 一組に分解する必要はなく，複数の組に分解をしてもよい．

次に，比較対象となる標準項目の要求事項を先に分解した Why の要素から選択してその他の要素についても同様に選択していく．

すべての項目の分解が終了したらデータマッチングの処理に入る．マッチングルールは厳密な判別を行う場合は，5W1H すべての要素が一致している場合だけ該当する要求事項を満たす項目が双方にあるとし，厳密ではなくともよいとする場合には，要求事項に対して 5W1H の要素がどの程度一致しているかを判別するものとする．前者の場合は要求事項に対しての相関は 0 または 1 で表現され，後者は設定要素数分の一致している要素数となる．この相関は項目対項目の相関と，項目と比較対象の標準全体の相関との 2 種類を算出することができる．例えば図 3 のように，標準 X の項目 A は要求事項 1 と 2 を持ち，標準 y の項目 a は要求事項 1 を持ち，項目 b は要求事項 2 を持つような場合である．

各項目における相関は，項目に対する要求事項数分の各要求事項の相関となる．

結果は，マトリクス表で表し縦軸に基準となる標準の項目を置き，横軸に比較対象となる標準の項目を置く．表のクロスした部分は Why が共通となる組の場合は相関を表示する．元の項目が複数項目でカバーされている場合もあり得るので最終行および列に項目全体の相関を表示する．

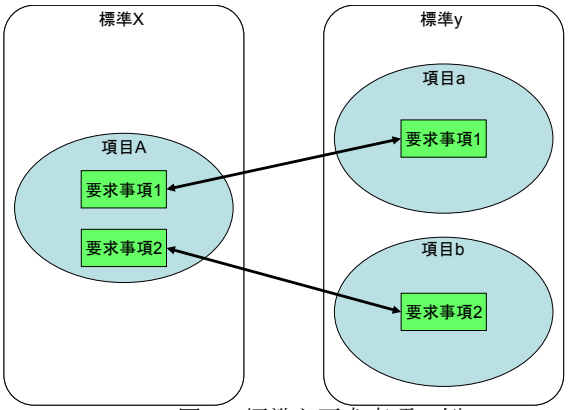

図 3　標準と要求事項の例

4.3 実験結果

本実験では，すでに関連情報作成手法を用いて一度相関を調べている情報を使用するため，手順の中で厳密な判別を行う場合と記述した方式でマッチングを行った．判別に用いた項目の組についての結果は以下の通りである．

①　正しく抽出された組

元となる関連情報が正しく抽出された組にも，相関が高い組と，低い組とに分けることができる．しかし，セキュリティ文法に基づいて分解を行うことでどちらも組も同じ表現に変換することができた．相関が高い組はもともと表現が近いため問題なく同じように分解することができた．そして，相関が低い組については，表現の不統一や装飾後の有無などによって相関が低いとされていたものが多く，表現の修正や装飾をはずしたための分解結果が一致したと考えられる．

②　FP の組

FP として，表現が近いが異なる内容を示している組をセキュリティ文法を用いて分解した結果，分解結果は一致しなかった．実際のデータを確認すると When の要素だけが違ったり，Who の要素だけが違ったりと一部の要素だけが違い要求事項やそれに伴う対処方法が一致しないものであることがわかった．これは文献[11]の中でも考察している「文章の意味によって判別することが必要である」ことにあてはまるといえる．

結論として，セキュリティ文法を用いた分解を行い，マッチングを行うことで異なる表現のセキュリティ文書のマッチング精度を向上させることができたといえる．このことにより，IoT セキュリティの課題としてあげた，異なる標準を持つ機器同士を接続した際に，全体としてのセキュリティ強度の判別に関する問題に寄与し，解決を測ることができる技術として使用できると考える．

5. 考察

本稿では，提案プラットフォーム-IoTS の適応実験を通して従来のセキュリティ技術の IoTS 化で IoT セキュリティへのアプローチを行った．その結果，従来の技術を組み合わせたり，追加のロジックを加えたりすることで IoT セキュリティでも有効な技術とすることができることが確認できた．

また，今回の実験の結果を元にして共通項を作成し，文献[14]に基づく接続されたそれぞれのシステムごとの固有項目を導出して，それらを網羅するような基準を作成して提案プラットフォーム-IoTS の評価基準として用いることで全体評価，繰り返し評価が行えるようなると考える．

IoT の世界では，これまでの情報処理の世界だけに閉じていたよりも用語の違いや粒度の違いといった問題が大きくなると推察される．そのような時に，実験で使用したセキュリティ文法のような共通ルールを用いることで一から

すべてを検査することなくセキュリティ強度を測ることができるようになると考える．しかし，相互接続することによって新たに表れる脅威については更なる検討が必要であると考える．

6. 今後の課題

本稿では，複数のシステムが相互接続する際に IoTS 化するための提案プラットフォームの考え方を示し提案した．今回の実験で IoTS 化を行った技術にとどまらず，その他の研究・技術についても詳細な IoTS 化にむけての検討を行い，IoTS シリーズの充実を目指す．

また，提案プラットフォームそのものについても IoT セキュリティの評価へ使えることを確認するために，近しい標準同士の関連情報の作成だけではなく，セキュリティ系と管理系といった視点の異なる標準間の関連情報の作成にも取り組んでいきたい．

7. まとめ

本稿では，従来のセキュリティ関連の研究・技術の IoTS 化を提案し，提案プラットフォームについて実際に一部の IoTS 化を行った．その結果，多くの従来技術が IoT セキュリティについて有効活用できることを示した．

今後は 6 章で述べた課題に取り組みより安全で安心な IoT セキュリティの実現を目指す．

参考文献

[1] 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)

[2] 辻宏郷: IoT におけるセキュリティの脅威と対策，独立行政法人情報処理推進機構(IPA) 技術本部セキュリティセンター情報セキュリティ技術ラボラトリー（オンライン），入手先<https://www.ipa.go.jp/files/000049819.pdf> (参照 2016-04-27).

[3] 須藤他: 鍵開け・のぞき見…スマートハウスご注意 他人操作恐れ，朝日新聞デジタル（オンライン），入手先<http://www.asahi.com/articles/ASH525J2JH52PTIL00H.html> (参照 2016-04-27)

[4] 鈴木聖子: Samsung の「スマート冷蔵庫」に脆弱性、他人にのぞき見される恐れ, IT media エンタープライズ(オンライン)，入手先<http://www.itmedia.co.jp/enterprise/articles/1508/25/news056.html>(参照 2016-05-06)

[5] 畑中他: 車のハッキングに現実味　遠隔操作でエンジン停止も，朝日新聞デジタル（オンライン），入手先< http://www.asahi.com/articles/ASH974WJ8H97ULFA014.html>(2016-05-06)

[6] ITmedia: 「この先ゾンビ注意」　ハッキングで書き換えられた道路の電光掲示板，ITmedia（オンライン），入手先< http://nlab.itmedia.co.jp/nl/articles/1110/20/news069.html>(参照 2016-05-06)

[7] 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).

[8] 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)

[9] 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).

[10] 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)

[11] 米国国立標準技術研究所 (National Institute of Standards and Technology): 重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版，米国国立標準技術研究所（オンライン），入手先< https://www.ipa.go.jp/files/000038957.pdf >(参照 2016-04-29)

[12] 金子朋子，山本修一郎，田中英彦: CC-Case―コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法，情報処理学会論文誌 55(9)，2134-2148 (2014-09-15)

[13] 金子朋子，髙橋雄志，勅使河原可海，田中英彦: CC-Case を用いた IoT セキュリティ認証方法の提案, 情報処理学会研究報告コンピュータセキュリティ（CSEC），2016-CSEC-72(14)，pp.1-8 (2016-02-25)

[14] 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（CDS），5(1)，pp.57-66 (2015-02-12)