

# 社会インフラシステムを対象とした テンプレート活用型セキュリティ対策立案手法の提案

太田原 千秋<sup>1,a)</sup> 内山 宏樹<sup>1</sup> 井口 慎也<sup>1</sup> 萱島 信<sup>1</sup>

受付日 2016年10月7日, 採録日 2017年6月6日

**概要:** 社会インフラシステムのオープン化にともない, サイバー攻撃数は増加傾向にある. このような状況をうけて, 社会インフラシステムの防護を目的としたセキュリティ設計の実施を要求するセキュリティ標準規格やガイドラインの策定が進んでいる. セキュリティ設計の特徴として, 作業者のセキュリティ知識に依存することがあげられる. 特に適切なセキュリティ対策を検討する対策立案では, 本特徴が大きく影響し, 作業者が限定されることが課題となる. 情報システム分野では, 本課題を解決する手法や, セキュリティ設計や攻撃事例も蓄積されていることから, セキュリティ設計を支援するガイドライン・ツール等が整備されている. しかし, 社会インフラシステムには, リソース上の制限からセキュリティ機能の導入や設定変更等の機能対策の導入が困難な一般的な情報システムと異なる機器が存在する. このため, 情報システムを対象とした従来技術は, リソースが潤沢な情報システムを想定していることから, 従来技術で導出した対策が必ずしも導入可能とは限らないという問題があった. 本手法では, 想定脅威と機器の属性(リソース上の制限等)から, 導入可能性の高い対策をマッピングしたテーブルを準備することにより, 機器の属性を考慮した効果的な対策立案が可能であることを示す. さらに, 情報システム分野における従来技術と対策立案結果を比較することにより, 本手法の有用性を示す.

**キーワード:** セキュリティ対策立案, セキュリティ設計, 社会インフラシステム

## Proposal of the Security Design Method in Infrastructure Systems by Template Application

CHIAKI OTAHARA<sup>1,a)</sup> HIROKI UCHIYAMA<sup>1</sup> SHINYA IGUCHI<sup>1</sup> MAKOTO KAYASHIMA<sup>1</sup>

Received: October 7, 2016, Accepted: June 6, 2017

**Abstract:** As infrastructure systems have introduced general OS and protocol, cyber attacks tend to increase. In response, the security design process is required to be performed. The problem is how precisely the security design process is performed depending on the performers skill. Hence the analysis result is not always precise. In the field of information system, a technique to solve this problem exists. Furthermore, security measure drafting not to need security knowledge is enabled because the example of security design case and the attack case is accumulated. However, in an infrastructure system, the apparatus which is different from the general information system having difficulty in function measures such as introduction and the setting change of the security feature exists from a limit in the resource. Therefore, that may not necessarily introduce measures assigned by the society infrastructure system because the conventional technique for information systems assumes the information system that resource is abundant; had a problem. I show that the effective measures drafting that considered the attribute of the apparatus is possible by preparing for the table which mapped feasible measures derived from an assumption menace and the attribute of the apparatus with respect by this technique. Furthermore, we show the usability of this technique by comparing the measures planning result with the conventional technique in the field of information system.

**Keywords:** security measures planning, security by design, infrastructure system

## 1. はじめに

近年、電力、ガス、水道等の生活の基盤となる社会インフラシステムに対するサイバー攻撃報告数が増加傾向にある [1]。これは、社会インフラシステムの情報化・オープン化が進展し、IT システムに対する攻撃手法の転用が可能になったためと考えられる。社会インフラシステムにおいて何らかの障害が発生した際、死亡事故や環境汚染等といった大きな影響を及ぼすことも可能であることから、テロや国家犯罪の標的となる可能性も否定できない。このような状況を受けて、社会インフラシステムの防護を目的とした、汎用制御システムのセキュリティ標準規格 IEC63443 [2]、や電力システムのセキュリティガイドライン NERC-CIP [3]、NIST IR 7628 [4] 等の分野に応じたセキュリティ規格・ガイドラインの策定が世界的に活発化している。このため社会インフラシステムでは、規格への準拠と社会インフラシステムに固有の特性を持つコンポーネントに対する考慮や、短納期で工数を抑えつつセキュリティ面での品質を確保するセキュリティ設計の実施が求められている。

セキュリティ設計とは、セキュアなシステムを構築するため、分析対象システムにおいて価値があるもの（以降、資産とする）に対して、発生しうる脅威を網羅的に抽出し（以降、脅威分析とする）、抽出した脅威に対して適切なセキュリティ対策を講じる（以降、対策立案とする）一連のプロセスを指す。情報システムでは、インターネットの発展にともない 90 年代後半よりサイバー攻撃の脅威にさらされており、効果的かつ効率的に攻撃を防ぐためのセキュリティ設計手法が検討されてきた。また攻撃事例も多く蓄積されていることから対策のベストプラクティスも存在しており、セキュリティ専門家以外でもセキュリティ設計の実施が可能な環境が整備されつつある。一方、社会インフラシステムは、これまで外部ネットワークと非接続な環境で、独自 OS・プロトコル機器を使用していることから、汎用 OS・プロトコル機器と比較して攻撃発生の可能性は低いため、安全と信じられてきた。そのため、情報システムと比較して、セキュリティ設計の重要性に対する意識が低くセキュリティ設計も重要視されていなかった。よって、社会インフラシステムを対象とした攻撃事例もセキュリティ設計事例も多くは蓄積されていない。よって、社会インフラシステムでは、セキュリティ専門家による脅威分析と対策立案が必要となる。しかし、この対策立案はセキュリティ知識が必要な作業であるため、作業者が限定されてしまう

といった課題がある。この課題を解決しうる情報システムを対象とした既存技術は存在するが、社会インフラシステムに適用してもこの課題は解決できない。なぜなら、既存技術はセキュリティ機能のリソースが潤沢な情報システムを対象としており、対策を導入する機器のリソース等を考慮していない。そのため、情報システムには存在しないセキュリティ機能にリソースを割けないコントローラ/PLC をはじめとする制御システムに適切な対策立案ができないといった課題が存在する。

セキュリティ専門家が過去に実施したセキュリティ分析結果を活用することで本課題を解決するため、「脅威」と「機器の制約（以降、制約とする）」のデータ変換の表現方法を定義し、さらに「脅威」と「制約」と「対策」のマッピングテーブルを用意することで社会インフラシステムに適用可能なセキュリティ対策立案手法を提案する。

以下、2 章では社会インフラシステムを対象とした対策立案の問題点と課題について、3 章では提案手法について、4 章では提案手法の評価結果について示し、最後に 5 章でまとめと今後の課題を述べる。

## 2. 社会インフラシステムにおけるセキュリティ設計の課題

本章では、社会インフラシステムとセキュリティ設計の概要、対策方針立案の従来手法とその課題について述べる。

### 2.1 社会インフラシステムの概要

本稿では、社会や生活を支える公共的な基盤を実現するシステムを「社会インフラシステム」と定義する。具体的には、電力、ガス、水道、交通等、生活に欠かせない基盤を実現するシステムが社会インフラシステムである。

社会インフラシステムが停止すると、大規模停電の発生等、私たちの生活への影響が甚大であることから、業務遂行が最優先される。近年、社会インフラシステムでは、業務効率向上を目的とした IT 技術の利用が進んでいる。たとえば、電力業界ではリアルタイムなエネルギー需要を把握して効率良く電気を送電するしくみを実現するため、国内外の電力会社では IT 技術を使用したスマートグリッドシステムを構築している。このような動きを受け、社会インフラシステムは、情報システムと制御システムを組み合わせられて構成される。表 1 に情報システムと制御システムのセキュリティ面での特徴を示す。表 1 の「セキュリティ機能に割当可能なリソース」に示すとおり、情報システムではほぼ同等のスペックの機器から構成されるが、制御システムでは様々なスペックの機器が存在する。

### 2.2 セキュリティ設計の概要

セキュリティ設計とは、システムやコンポーネントに内在する様々な脅威を洗い出すとともに、その影響度を分

<sup>1</sup> 株式会社日立製作所研究開発グループシステムイノベーションセンターセキュリティ研究部

Security Research Department, Center for Technology Innovation-System Engineering, Research & Development Group, Hitachi Ltd., Yokohama, Kanagawa 244-0817, Japan

a) chiaki.otahara.qv@hitachi.com

表 1 情報・制御システムの特徴 [5]

Table 1 Characteristics of IT system and ICS system.

項目	情報システム	制御システム	
保護対象資産	情報	機能	
リスク顕在化の影響	情報漏えい 金銭的被害 等	人命損失 環境汚染 等	
ライフサイクル	3~5 年	10~20 年	
セキュリティ 三大特性の 優先度	高	機密性	可用性
	中	完全性	完全性
	低	可用性	機密性
セキュリティ機能に 割当可能なリソース	高	高, 中, 低	

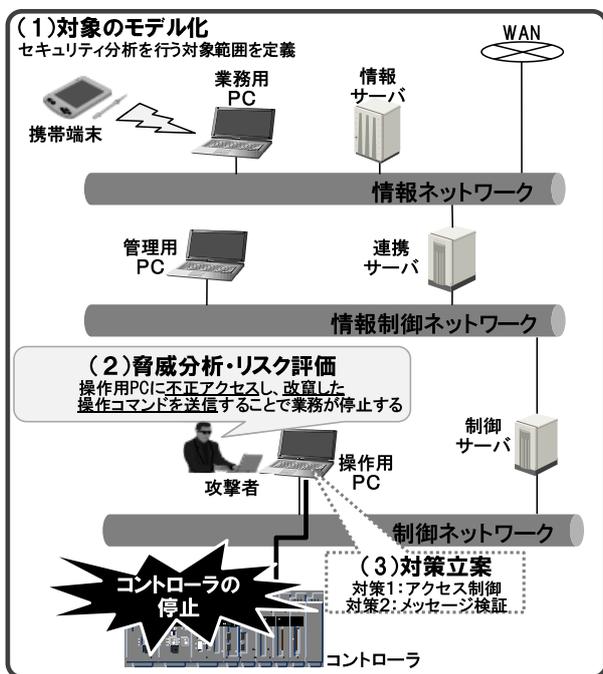


図 1 セキュリティ設計の概要

Fig. 1 Schema of security design.

析・評価し、有効な対策を導き出すための一連のプロセスである。情報セキュリティ国際評価基準 ISO/IEC15408 [6] 等によりセキュリティ設計手順の大枠は規定されている。以下に一般的なセキュリティ設計の概要 (図 1) と手順を示す。

(1) 対象のモデル化

設計対象となるシステムやコンポーネントの範囲や前提条件、保護すべき資産等を定義する。

(2) 脅威分析・リスク評価

設計対象における資産に対して、発生しうる脅威を分析する。脅威事象を網羅的に洗い出す手法として 5W 手法 [7] 等があげられる。抽出した脅威事象は、資産価値と発生確率の観点から、リスクを評価する。

(3) 対策立案

リスク評価の結果に基づき、セキュリティ対策の実施すべき脅威事象の範囲を明確にし、脅威事象の発生要因を分析しセキュリティ対策を立案する。脅威事象の発生要因を分析する手法として ETA (Event Tree Analysis [8]) や FTA (Fault Tree Analysis [8]) 等があげられる。なお、これらの手法は脅威分析に活用されることもある。

社会インフラシステムは一般に大規模であり、セキュリティ設計に膨大な工期を要する。また、セキュリティ設計は、ノウハウの有無により分析結果のばらつきが発生する。特に、対策立案は、セキュリティ知識・セキュリティ設計経験を要する作業であるため、設計者のスキルに依存する傾向が高く、設計時間の短縮と設計品質の均一化が課題となっている。このため、本研究ではセキュリティ設計手順のうち、対策立案を対象とする。

2.3 関連研究

本節では、関連研究として、セキュリティ専門家のセキュリティ設計手順をモデル化することで対策立案を支援する手法と、IPA から発刊されている IoT 開発におけるセキュリティ設計の手引き書に記載の対策立案手法について述べる。

(1) セキュリティ対策選定の実用的な一手法

セキュリティ設計における対策立案手法に関する先行研究として、中村らが提案するセキュリティ対策選定の実用的な一手法 [9] が存在する。本手法は、専門家がセキュリティ対策を決定する際の手順を分析し、資産とその脅威の関係と、脅威と対策の関係を明確化することにより、設計品質の均一化と効果的な対策群の抽出を目指すものである。本手法は、以下を特徴とする。

i. 資産・脅威・制約・対策のモデル化

中村らの提案手法では、品質の均一化するため対策立案の手順を基に、資産と脅威と対策の関係をモデル化している。具体的には、分析対象システム内部の資産 (機器上で動作するソフトウェアや電子情報等) で発生しうる脅威 (STRIDE 手法 [10] の各脅威相当の概念で整理したもの) と対策 (ISO/IEC TR13335 [11], ISO/IEC27000 [12] 相当) との関係を表現したマトリクス表の作成により、資産・脅威・制約・対策のモデル化をしている。モデル化の際、これら 3 項目の関係を「資産と脅威」「脅威と対策」に分けてモデル化している。「資産と脅威のモデル化」では、「PC 上の電子情報」等の資産を横軸、起こりうる脅威「内部者による漏洩・改ざん・破壊・持ち出し・切断」等を縦軸にとり、各資産において発生しうる脅威には「1」、起こりえない脅威には「0」を記載したマトリクス表を作成する。同様に脅威と対策のモデル化でも、脅威を縦軸、対策を横軸にとり、各脅威において對抗策となりうる対策には効果の度合いに応じて「0.7~0.1」、なりえない対策には「0」を

記載したマトリクス表を作成する。これら2つのマトリクスを作成することで、各資産で起こりうる脅威の特定、各脅威の対抗策となりうる対策の特定が容易になり、品質の均一化に大きく貢献する。

## ii. 対策効果の定量的評価

中村らの提案手法では効果的な対策群を抽出し評価するため、対象システムの残存資産価値の総和が高いほど効果的な対策群であると見なし、“資産価値”と“脅威が発生しない確率”と“攻撃成功率(対策導入効果)”から残存資産価値の期待値を定式化している。具体的には、まず(1)で述べた資産と脅威のマトリクス表において、各資産には“資産価値(コスト)”を、脅威には“発生確率”の情報を付与する。同様に脅威と対策のマトリクス表において、各脅威には同じく“発生確率”を、対策にはその対策を導入する“コスト”の情報を付与する。そして、対象システムに存在するすべての資産の“資産価値”と各資産で起こりうる脅威の“脅威が発生しない確率”を考慮したうえで、残存している資産価値の期待値を算出する。そして、対策導入効果から“リスク減少率”を算出し、最終的に対策効果を反映した残存資産価値が高くなる対策群を抽出する。これにより、効果的な対策群の抽出が可能となる。

## (2) IoT 開発におけるセキュリティ設計の手引き

IPAより発行されている「IoT開発におけるセキュリティ設計の手引き[13]」は、セキュリティ設計を担当するIoT開発者に向けた手引きであり、実施例とともに脅威分析・対策立案・脆弱性への対応方法について解説している。詳細を以下に示す。

文献[13]で示されている脅威分析手法は、攻撃ツリーを作成する手法(ETA[8]に相当)があげられている。なお、攻撃ツリーとは、まず回避したい被害を列挙し、その被害を生じさせる脅威を明確化していくものである。また、対策立案手法は、脅威分析における攻撃ツリーの作成により明確化された脅威に対応する対策を立案する手法があげられている。以上より、文献[13]では脅威分析・対策立案で広く用いられるETA相当の分析手法が紹介されている。なお、ETA等の分析による攻撃ツリー作成にはセキュリティ知識やセキュリティ設計のノウハウが必要となる。

## 2.4 従来技術適用時の課題

中村らの提案手法(関連研究(1))を社会インフラシステムに適用すると以下のような課題がある。中村らの手法は、対策を導入する機器のリソース面等の属性を考慮していないため、“サーバ上のデータの暗号化”といったリソースが潤沢な機器を想定した対策を立案している。社会インフラシステムの場合、コントローラやPLCといったセキュリティ機能にリソースを割けない制御機器が使用されている。このような制御機器に暗号化機能を搭載すると、従来の処理時間が増加することから処理遅延や業務停止が発生

する等の問題が起きることがある。以上より、中村らの提案手法を多様な特性を持つ機器から構成される社会インフラシステムに適用した場合、本手法により割り当てられた対策が必ずしも適用できるとは限らない。よって、導入実現性の低い対策が導出されるという課題が存在する

また、文献[10](関連研究(2))で紹介されている手法を適用した場合、脅威分析で抽出した脅威に対して、攻撃ツリーにより導出した脅威発生までの各攻撃に対応する対策を講じる必要がある。文献[10]の手法は、漏れなく対策立案をすることが可能だが、分析者のセキュリティ知識に大きく依存する。そのため、対策立案の課題である、ノウハウの有無により分析結果のばらつきが如実となる。

## 3. テンプレート活用型セキュリティ対策立案手法

本章では、2.4節であげた課題を解決するテンプレート活用型対策立案手法を提案する。

### 3.1 課題の解決方針

従来技術適用時の課題を解決するため、セキュリティ専門家が過去に実施したセキュリティ分析結果(たとえば、5Wによる脅威分析結果やETA/FTAによる対策立案結果等)を活用することで、対策立案を支援する手法を検討することとした。過去事例の利活用を実現するためには、異なる案件のセキュリティ分析結果が比較できるようにする必要がある。そこで、制約を考慮することが可能な「脅威」と「制約」と「対策」パターンを生成し、脅威・制約・対策マッピングテーブルを作成することとした。以下に解決方針の詳細を示す。

#### 1. 脅威と制約の表現方法を定義

脅威・制約・対策マッピングテーブルを用意するための準備として、脅威に関する5W[7]の要素(「脅威発生箇所(Where)」「攻撃者(Who)」「発生タイミング(When)」「動機(Why)」「脅威事象(What)」)から表現される脅威と制約条件に関して、共通基盤となる汎用的なデータ表現への変換するための部品(テンプレート)を作成する。

#### 2. 脅威・制約・対策のマッピングテーブルを準備

対策を導入する機器の制約に応じた対策立案を実現するため、制約条件によって機器を分類、そして制約条件の分類により脅威種別で利用可能な対策手段を選択するテーブルを用意する。

以降、脅威の表現方法に関する詳細を3.2節、脅威と対策のマッピングテーブルに関する詳細を3.3節で述べる。

### 3.2 脅威の表現手法

案件に依存しないマッピングテーブルを作成する準備として、対策立案に必要な情報に関するテンプレートを作成する必要がある。テンプレートの検討にあたり、まず対

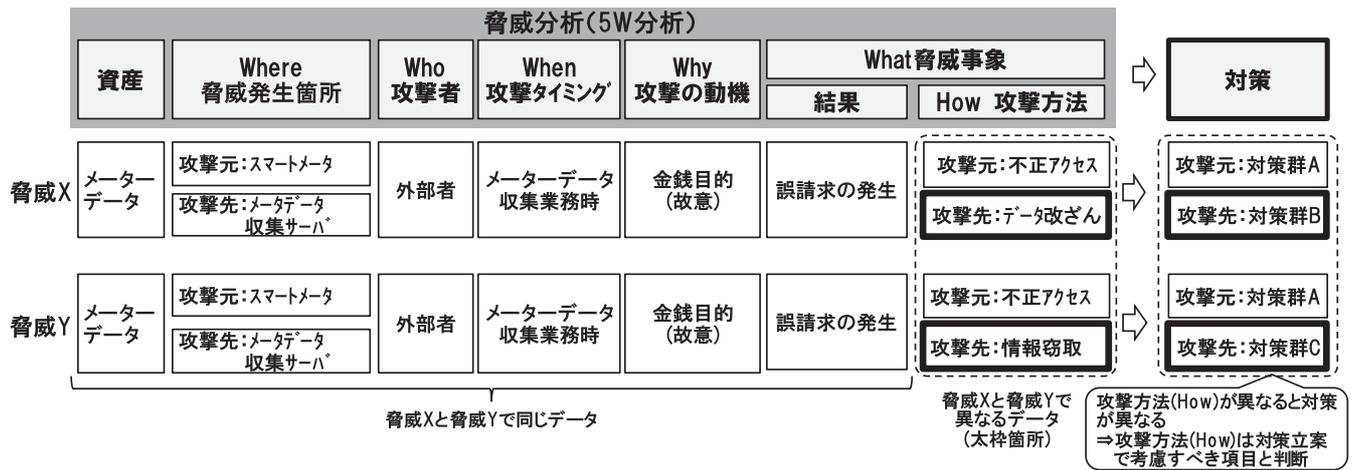


図 2 対策立案時に考慮すべき情報の整理

Fig. 2 Overview of work to organize the information needed to security measure planning.

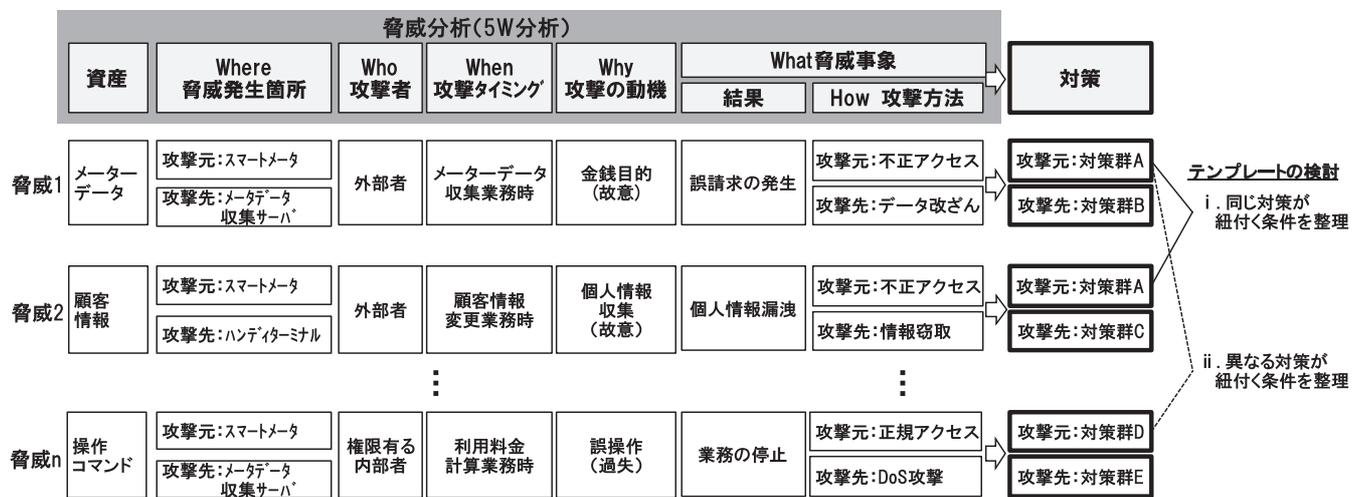


図 3 テンプレート化するべき項目の検討

Fig. 3 Overview of the template study.

策立案に必要な情報を整理することで①テンプレートを作成すべき情報を明確化した後、②テンプレートを検討する。本検討にあたり、セキュリティ専門家がセキュリティ設計を実施した案件 A (電力システムを対象に分析した結果(脅威数が約 1.4 万件規模のシステム))を用いた。詳細は以下のとおり。

①テンプレートを作成すべき情報の明確化

3.1 節で述べたとおり、対策立案では、脅威と制約を考慮し適切な対策を立案する。これら情報のうち、本稿における脅威の定義では、様々な情報から構成されるため、脅威を構成する 5W の項目のうち、対策立案に必要な情報を明らかにすることとした。このとき、過去にセキュリティ専門家が分析した事例の分析結果を用いて、脅威を表現する 5W の項目のうち、どれか 1 つが異なる脅威をいくつか比較し、紐付く対策が異なれば、その項目は対策立案に影響のある項目であると判断する。具体的には、脅威の構成要素の 1 つである「攻撃方法」だけが異なる脅威を複数抽

出し、それらの脅威に紐付く対策を比較する。このとき、紐付く対策は異なるため、「攻撃方法」は対策立案に影響のある項目と見なす(図 2 参照)。同様の確認をすべての項目に対して実施し、対策立案に必要な項目を調査した結果を表 2 に示す。

②脅威分析結果を正規化するテンプレートの検討

①で明らかにした対策立案に必要な各項目のテンプレートの検討にあたり、同様に案件 A の結果を用いて、同じ対策が紐付くときの条件、異なる対策が紐付くときの条件を整理することでテンプレートを検討する(図 3 参照)。過去事例を基に検討した「脅威」のテンプレートを(1)~(5)に、「制約」のテンプレートを(6)にて説明する。なお、これらのテンプレートを用いて「脅威」と「制約」を正規化したものを本稿では脅威特徴と呼ぶこととする。

(1) Where: 脅威発生箇所

過去事例を整理した結果、攻撃経路上のどこかで脅威発生を阻止する対策をうつことで脅威の発生を防止できるた

表 2 対策立案に影響する脅威の構成項目検討結果

Table 2 Study results of the factors that affect the measures planning.

項目	判断結果
資産	資産の種類(情報/機能/物理)が異なっても攻撃方法が同じであれば対策が同じであるため考慮しない
脅威発生箇所(Where)	攻撃元 攻撃先
攻撃者(Who)	攻撃者が外部者か内部者に応じて対策が異なるため考慮する
攻撃タイミング(When)	攻撃タイミング(システムのライフサイクル)に応じて対策が異なることから考慮する
攻撃の動機(Why)	過失か故意かで対策が異なるため考慮
脅威事象(What)	結果
	攻撃方法
	攻撃の結果起きる事象(業務停止/誤操作等)で対策に影響はないため考慮しない
	脅威内容に応じて対策内容も異なるため考慮する

表 3 攻撃経路種別に関する指標

Table 3 Index of the attack path type.

種別	概要
エントリポイント	攻撃者が侵入する機器
ターゲット	攻撃者が最終的に狙う機器

表 4 機器の種別に関する指標

Table 4 Index of the machine type.

種別	概要	
機器	可搬型媒体	持ち運びが可能な機器
	非可搬型媒体	持ち運びができない機器
NW機器	広域ネットワーク対応	インターネット等の広域ネットワークに対応している機器
	狭域ネットワーク対応	Bluetoothなどの狭域ネットワークに対応している機器

め、攻撃者が侵入点とするエントリポイント(攻撃元)とターゲット(攻撃先)のみ考慮する。過去事例を整理したテンプレートを検討した結果、脅威発生箇所となる機器の種類(可搬機器か非可搬機器か等)や攻撃元への侵入方法により対策が異なることから、機器の種類とインタフェース属性は対策立案に必要な情報と見なした。よって、社会インフラシステムを構成する機器名称等のシステム固有のデータを正規化するため、「攻撃経路種別」「機器の種類」と「侵入方法種別」のテンプレートを表 3、表 4、表 5 のとおり定義する。なお、侵入方法種別を考慮するにあたり共通脆弱性評価システム(CVSS) [14]における攻撃元区分(Access Vector)を適用した。

(2) Who: 攻撃者

過去事例を整理した結果、攻撃者が対象システムの従業

表 5 侵入方法の種別に関する指標

Table 5 Index of the intrusion method type.

種別	概要
ローカル	機器への物理アクセスやローカル環境から攻撃する必要がある
隣接	対象機器を隣接ネットワークから攻撃する必要がある
ネットワーク	対象機器をネットワーク経緯でリモートから攻撃可能である

表 6 攻撃者種別指標

Table 6 Index of the attacker type.

種別	概要
外部者	第三者
権限無し内部者	対象システムにおいて、一般ユーザと同等の権限を持つ内部者
権限有り内部者	対象システムにおいて、管理者と同等の権限を持つ内部者

表 7 脅威発生の機会に関する指標

Table 7 Index of threat generation opportunity.

種別	概要
開発	システムの開発時に発生しうる脅威
運用	システムの運用時に発生しうる脅威
保守	システムの保守時に発生しうる脅威

表 8 攻撃の動機に関する指標

Table 8 Index of the attack motive.

種別	概要
故意	悪意を持つ目的・意図のある攻撃
過失	悪意を持たない過失による攻撃

員等の内部者か、対象システムの従業員以外等の外部者かにより対策が異なることが判明した。また、同じ内部者であっても、権限のありなしによって対策が異なるため、攻撃者種別のテンプレートを表 6 のとおり定義する。

(3) When: 脅威発生の機会

過去事例を整理した結果、システム運用時である業務中における対策と保守業務中の対策が異なることが判明した。そこで、脅威発生の機会を一般的なシステムのライフサイクルから検討し、脅威発生機会のテンプレートを表 7 のとおり定義する。

(4) What: 脅威カテゴリ

過去事例を整理した結果、脅威事象を引き起こすまでの攻撃内容に応じて対策が異なる。たとえば、「脅威事象: プライバシ侵害を引き起こす機密情報の漏えい」の対策は「暗号化機能の導入」、「脅威事象: 業務停止を引き起こす機能の改ざん」の対策は「改ざん検知機能の導入」とな

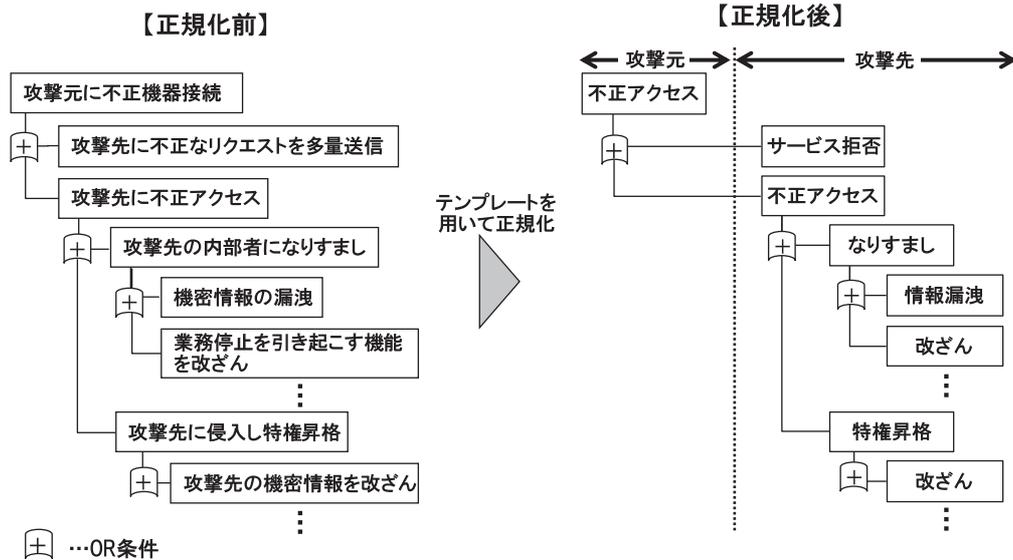


図 4 脅威イベントツリーの正規化例  
Fig. 4 Example of normalized thread tree.

り、攻撃内容に応じて対策は異なってくる。そこで、脅威事象のテンプレート検討にあたり、Microsoft 社が提唱する脅威モデル STRIDE 手法 [10] を適用することとした。STRIDE 手法の STRIDE とは、(1) Spoofing (なりすまし)、(2) Tampering (改ざん)、(3) Repudiation (否認)、(4) Information Disclosure (情報漏えい)、(5) Denial of Service (サービス拒否)、(6) Elevation of Privilege (特権の昇格) で、「STRIDE」はこの 6 つの脅威の頭文字をとったものである。本検討に活用した過去事例を整理した結果、STRIDE に加え、攻撃元と攻撃先への侵入「不正アクセス」または「アクセス」を考慮することで脅威発生までの攻撃方法を正規化できるため、「不正アクセス」「アクセス」+ STRIDE の組合せ攻撃方法を正規化する。具体例としてテンプレートを用いた正規化前後の脅威イベントツリー（攻撃者：外部者）を図 4 に示す。本稿では、ETA [8] における「攻撃方法（本稿における脅威イベントに相当）」を抽出したものを脅威イベントツリーと呼ぶこととする。なお、ETA [8] とは、原因事象の発生後、しかるべき防護機能が機能せず危険事象に至るという過程を解析し、各結節点に対処失敗確率を入れ危険事象の発生確率を定量的に解析するものである。なお、脅威分析への ETA の適用にあたり、「攻撃方法」や「脆弱性」等を考慮してツリー展開していくことで攻撃過程を解析する。各脅威に対して、同様に脅威を引き起こすまでの経緯を表現した脅威イベントツリーを正規化する。

(5) 機器の制約条件

セキュリティ対策は大きく機能対策 (IT 対策)、物理対策、運用対策に分類される。「データ暗号化」等の機能対策はリソースを必要とするため、導入の可否は機器の制約条件が大きく影響する。よって、対策の選定には対策導入

表 9 機器の制約条件に関する指標  
Table 9 Index of restriction of machine.

種別	概要
なし	リソース面や機能変更等における制約なし
小	一部リソース面での制約あり
大	リソース面や機能変更等における制約あり (機能対策の導入が困難)

先の機器の制約条件を考慮する必要がある。そこで、表 9 のとおり機器の制約条件を考慮する。

3.3 脅威・制約・対策マッピングテーブルの検討

脅威・制約・対策マッピングテーブルの作成にあたり、案件 A の分析結果に対して 3.2 節で検討した脅威特徴テンプレートを用いたデータ変換 (正規化) した「脅威」と「制約」の組合せに紐づく「対策」のパターンを検討する必要がある。本パターン作成にあたり、案件 A の脅威分析結果 (約 1 万個の脅威) と対策立案結果を活用し、脅威・制約・対策マッピングテーブルを作成することとした。まず、パターン生成の準備として、「脅威」「制約」情報に対してテンプレート (表 3—表 9) を用いてデータを正規化 (脅威特徴 (表 11) する。次に「脅威特徴」と「対策」頻出するパターンを抽出するため、頻出パターンマイニング手法の 1 つである Apriori アルゴリズム [15] を適用することとした。頻出パターンマイニング手法には、特定の項目に重みを持たせるものも存在するが、各項目がどれくらい対策に影響するかを考慮し重みをつけると複雑になるため、まずはすべての項目が対策立案時に同等に影響すると見なし Apriori アルゴリズムを用いて頻出アイテムパターンを抽出することとした。機械的に頻出パターンを抽出するこ

表 10 脅威分析結果例  
Table 10 Example of threat analysis.

脅威 ID	資産	脅威発生箇所 (Where)		攻撃者 (Who)	脅威発生の機会 (When)	動機 (Why)	脅威事象 (What)	攻撃方法
		エントリポイント	ターゲット					
脅威 1	メーターデータ	スマートメーター	メーターデータ収集サーバ	外部者	運用	金銭目的	誤請求の発生	外部者がスマートメータからメーターデータ収集サーバに不正アクセスし、メーターデータを改ざりする
脅威 2	顧客情報	スマートメーター	ハンディターミナル	外部者	運用	個人情報収集	個人情報漏洩	外部者がスマートメータからハンディターミナルに不正アクセスし、顧客情報を窃取する

表 11 正規化した脅威特徴例  
Table 11 Example of normalized threat analysis.

脅威ID	脅威							機器の制約条件
	脅威発生箇所 (Where)			攻撃者 (Who)	脅威発生の機会 (When)	動機 (Why)	脅威カテゴリ (What)	
	攻撃経路種別	機器の種別	侵入方法					
脅威 1	エントリポイント	可搬型機器	ローカル	外部者	運用	故意	不正アクセス	大
	ターゲット	非可搬型機器	隣接	外部者	運用	故意	不正アクセス改ざん	なし
脅威 2	エントリポイント	可搬型機器	ローカル	外部者	運用	故意	不正アクセス	大
	ターゲット	可搬型機器	隣接	外部者	運用	故意	不正アクセス情報窃取	大

とにより、妥当な「脅威特徴」と「対策」の組合せを比較して、出現頻度が低いことが想定される人的ミスによるはずれ値（不適切な脅威と対策の組合せ等）を取り除くことができる。Apriori アルゴリズムは最小支持度と最小確信度を基に頻出パターン  $X \Rightarrow Y$ （条件部 X:「脅威特徴」、帰結部 Y:「対策」）を生成する。最小支持度 (minsup) とは全トランザクション（全脅威特徴パターン）のうち、どれくらいその要素が含まれるかという割合を示す。最小確信度 (minconf) とは、条件部 X を満たすトランザクション数に対する条件部 X と帰結部 Y の両方を満たすトランザクション数の割合を示す。以下に Apriori アルゴリズムのフローを示す。

1. 頻出アイテム集合の探索

大量のデータの中から頻出アイテム集合、つまり頻出する条件部 X を探索する。このとき、すべてのトランザクションのうち、特定の要素がどれくらい含まれるか支持度 (support) を算出する。入力として与えた最小支持度よりも高い数値であれば頻出アイテムと見なす。なお、支持度の計算式は式 (1) のとおり。

$$\text{support}(X) \geq \text{minsup} \tag{1}$$

今回テンプレートを検討した項目、つまり脅威特徴の組合せから頻出部 X を探索する。今回、過去事例を活用していること、過去事例に対して対策立案に影響する項目のみ抽

出していることから、存在する「脅威特徴」を構成する各情報の組合せを頻出アイテム集合と見なすこととした。

2. 頻出パターンの探索

頻出する条件部 X を探索した後、条件部 X に紐付く帰結部 Y の割合（確信度）を算出する。入力として与えた最小確信度 (minconf) よりも大きい数値であれば頻出パターンと見なす。なお、確信度の計算式は式 (2) のとおり。

$$\text{confidence}(X, Y) = \frac{\text{support}(X \cup Y)}{\text{support}(X)} \geq \text{minconf} \tag{2}$$

以上の処理を繰り返し、過去事例の分析結果からはずれ値を除去した「脅威特徴」（条件部 X）と対策（帰結部 Y）のペアから脅威・制約・対策マッピングテーブルを作成する（表 12）。以上より、脅威・制約・対策マッピングテーブルは、過去事例の脅威分析結果を脅威特徴テンプレートで正規化した「脅威特徴」とそれに紐付く対策から構成される。このテーブルを参照し、「脅威特徴」の各要素が完全にマッチする対策を抽出することで、機器の制約を考慮した対策立案が可能となる。対策立案結果の一例を表 13 に示す。

3.4 提案手法の処理フロー概要と出力結果

本手法の処理フローを図 5 に示す。処理 1 では、脅威分析結果と機器の制約条件に関する情報から、脅威特徴テンプレートを基に、脅威分析結果を正規化する。処理 1 の入

表 12 脅威・制約・対策マッピングテーブルの例  
Table 12 Example of threat characteristic - measure DB.

No.	脅威						機器の 制約条件	対策	
	脅威発生箇所 (Where)			攻撃者 (Who)	脅威発生 の機会 (When)	動機 (Why)			脅威カテゴリ (What)
	攻撃経路種別	機器の 種別	侵入方法						
1	エン트리 ポイント	可搬型 機器	ローカル	外部者	運用	故意	不正アクセス	なし	不要な物理 ポートの 閉鎖
2	エン트리 ポイント	非可搬型 機器	隣接	外部者	運用	故意	不正アクセス	なし	物理認証による 入室管理
3	ターゲット	可搬型 機器	ローカル	外部者	運用	故意	不正アクセス	大	不要な物理 ポートの 閉鎖
4	ターゲット	可搬型 機器	隣接	外部者	運用	故意	改ざん	なし	メッセージ認証による 改ざん検知
5	ターゲット	非可搬型 機器	隣接	権限なし 内部者	運用	故意	改ざん	大	メッセージ認証による 改ざん検知
6	ターゲット	非可搬型 機器	隣接	権限あり 内部者	運用	故意	情報漏えい	なし	データ暗号化
7	ターゲット	非可搬型 機器	ローカル	権限なし 内部者	運用	故意	情報漏えい	中	残留情報削除
...	...	...	...	...	...	...	...	...	...

表 13 対策立案結果の例  
Table 13 Example of measure planning list.

脅威 ID	脅威発生箇所 (Where)	攻撃者 (Who)	脅威発生の機会 (When)	動機 (Why)	脅威カテゴリ (What)	対策
脅威1	スマートメータ	外部者	運用	故意	不正アクセス	・不要なポートの閉鎖 ...
	メーターデータ 収集サーバ	外部者	運用	故意	不正アクセス	・不要なポートの閉鎖 ...
					改ざん	・メッセージ認証による改ざん検知 ...

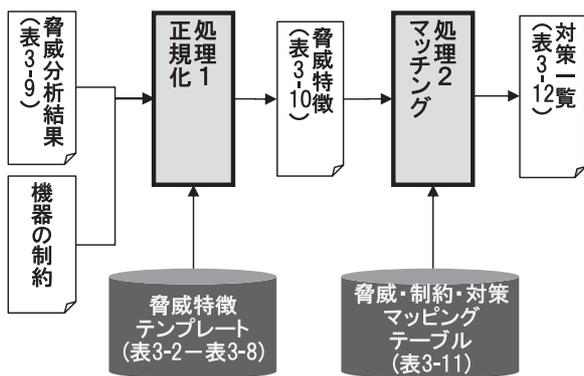


図 5 テンプレート活用型対策立案支援手法の処理フロー  
Fig. 5 Process flow of the security design method in infrastructure systems by template application.

力となる脅威分析結果を表 10 に、出力となる脅威特徴を表 11 に示す。たとえば、表 10 に示す脅威 1 の脅威発生箇所 (Where) に登場する「スマートメータ」は、「攻撃経路種別：エン트리ポイント」「機器の種別：可搬機器」「侵入方法：ローカル」と変換することで正規化する (表 11)。

以上より処理 1 では、共通の脅威特徴テンプレートを用いたデータの正規化により、異なる案件の脅威分析結果とのマッチングをとることが可能となる。

処理 2 では、処理 1 の出力結果である脅威特徴 (表 11) を基に、脅威・制約・対策マッピングテーブル (表 12) を参照し、類似の脅威とそれに紐付く対策を抽出し、対策一覧 (表 12) を出力する。たとえば、表 11 の脅威 1 の 5W と同じ組合せに紐付く対策「不要な物理ポートの閉鎖 (表 12 の No.1)」を抽出していくことで対策一覧 (表 13) を出力する。

#### 4. 評価

本章では、テンプレート活用型対策立案手法の評価結果を示す。

##### 4.1 準備

脅威・制約テンプレートはシステムの分野に依存せず活用することができるが、対策は分析対象システムごとに準拠すべき規格等が異なるため、脅威・制約・対策マッ

表 16 機器 a に関する出力結果  
Table 16 Output of Machine-a.

機器名称	脅威						機器の 制約条件	対策
	脅威発生箇所		攻撃者	脅威発生 の機会	脅威発生 理由	脅威カテゴリ		
	攻撃経路種別	機器の種別						
機器a	ターゲット	可搬型機器	外部者	運用	故意	情報漏洩	大	脆弱なAPIの利用禁止 不要な物理ポートのシールド 耐タンパ実装 起動可能なプログラムの制限

表 14 案件 A, B の概要  
Table 14 Scheme of Project A, B.

項目	案件 A (脅威・制約・対策 マッチングテーブル)	案件 B (入力)
対象システム	電力システム	電力システム
資産数	25 パターン	37 パターン
機器の種別数 (正規化前)	7 パターン	28 パターン
脅威数 (正規化前)	約 14,000 個	約 29,000 個

表 15 案件 A, B の脅威の各項目と制約のパターン数  
Table 15 Number of threat and restriction pattern for project A, B.

項目	案件 A	案件 B
対策実施箇所 (Where)	12 パターン	18 パターン
攻撃者 (Who)	2 パターン	2 パターン
脅威発生の機会 (When)	1 パターン	1 パターン
動機 (Why)	2 パターン (内部者) 1 パターン (外部者)	2 パターン (内部者) 1 パターン (外部者)
脅威カテゴリ (What)	7 パターン	7 パターン

グテーブルの他分野への活用は困難である。そのため、本手法の検証では、脅威・制約・対策マッチングテーブルの生成に活用した案件 A と同じ電力システムかつ同じ規格に準拠した対策の立案を実施した案件 B のデータを使用する。この 2 つの案件の概要を表 14 に、2 つの案件のテンプレートパターンを表 15 に示す。

本手法の処理フローの概要について説明する。本手法の評価に向けて、あらかじめ案件 A の分析結果から脅威・制約・対策マッチングテーブルを作成する。そして、入力となる分析対象システム（本評価では案件 B を指す）の「脅

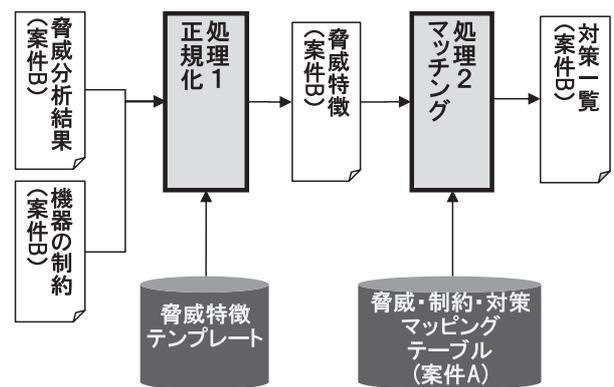


図 6 評価における入出力と DB の概要  
Fig. 6 Outline of input/output and DB used for evaluation.

威分析結果」と「制約」を入力し、脅威・制約テンプレートを用いて情報を正規化する（図 6 の処理 1）。さらに、正規化した入力情報から、同じ脅威・制約の組合せを抽出し、それに紐づく対策を出力する（図 6 の処理 2）。

#### 4.2 評価

本提案手法の出力結果に関する評価にあたり、中村らの提案手法 [9] と比較し、評価する。評価にあたり、案件 B をテストデータとし、リソース上制限がある機器 A に対して、適切な対策を導出するか検証した。脅威イベント「情報漏えい」に対応する対策出力結果の一部を表 16 に示す。なお、表 16 における従来技術 [9] の出力結果は、提案手法との出力結果を比較しやすいよう、脅威・制約・対策マッチングテーブルにおける対策と置き換えた。

従来技術 [9] は、“資産価値”と“脅威が発生しない確率”と“攻撃成功率”から“残存資産価値の期待値”を定式化することで効果の高い対策を定量的に選定することが可能である。しかし、適用対象をリソースが潤沢な情報システムを前提しているため、社会インフラシステムを構成する一部のリソース上の制限がある機器に対して、導入できる可能性の低い「データ暗号化」や「通信データの暗号化」等のリソースが潤沢な機器を前提とした対策が導出されてしまう。このため、対策を導入する段階で再度評価する必要

表 17 提案手法と従来手法の比較

Table 17 Comparison of proposed method and conventional method.

#	項目	提案手法	従来手法
1	対策の網羅的な抽出	○	○
2	対策選定時のコスト	中 (セキュリティ知識が必要)	小
3	対策導入時のコスト	小	大 (導入困難な場合あり)

があり、導入コストが高いと考えられる。

一方、本提案手法では、機器の制約条件を考慮することにより、適用対象機器のリソースに応じた対策を導出可能である。導出した対策の中で効果的な対策を選択するためには対策に関する知識が必要となるものの、適用対象機器へ導入可能な対策に絞り込んで導出していることから、対策導入に関わるコストは小さいと考えられる。

以上の評価結果を表 17 に示す。この結果から、従来手法に比べ提案手法は様々な特性を持つ機器から構成される社会インフラシステムへの対策選定・導入に関わるコストが小さいと考えられ、優位性が高いと考えられる。

## 5. まとめと今後の課題

本稿では、機器の制約を考慮した対策立案を実現するため、脅威特徴テンプレートと、脅威・制約・対策マッピングテーブルを検討した。検討した脅威特徴テンプレートで入力データを変換し、脅威・制約・対策マッピングテーブルを参照することで、機器の制約を考慮した対策の選定を実現するテンプレート活用型対策立案手法を提案した。本手法の評価では、機器の制約を考慮した対策が選定されていることを確認した。

また、本手法の課題として以下があげられる。

### (1) 脅威特徴テンプレートの精度評価

本手法は、共通のデータ変換基盤となる脅威特徴テンプレートを検証した。本手法の評価では、案件 B においても入力となる脅威・制約に応じた対策が出力されていることを確認したが、脅威・制約・対策マッピングテーブルの生成に用いた案件 A と同じ電力システム案件 B をテストデータとして活用したため、他分野のシステムにおいても同様に活用可能か検証する必要がある。

### (2) 出力結果の妥当性評価手法の検討

本手法の検討にあたり、セキュリティ専門家が過去に選定した対策群は適切であるという前提の元、過去事例を活用することで脅威・制約・対策マッピングテーブルを生成した。そのため、出力される対策群の効果を客観的に評価するためにも、リスク低減率に基づく対策選定といった定量的な出力結果の妥当性を評価する手法を考案する必要がある。

ある。

## 参考文献

- [1] ICS-CERT: ICS-CERT Incident Response 2015 (2015), available from [https://ics-cert.us-cert.gov/sites/default/files/Annual.Reports/Year\\_in\\_Review\\_FY2015\\_FinalS508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual.Reports/Year_in_Review_FY2015_FinalS508C.pdf).
- [2] IEC: Industrial communication networks — Network and system security — Part2-1: Establishing an industrial automation and control system security program (2013).
- [3] NERC: NERC-CIP010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments (2013).
- [4] NIST: NIST IR 7628 — Guidelines for Smart Grid Cyber Security (2014), available from <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>.
- [5] IPA: 重要インフラの制御システムセキュリティと IT サービス継続に関する調査 (2009), 入手先 <https://www.ipa.go.jp/files/000013981.pdf>.
- [6] ISO/IEC15408: Information technology — security techniques — evaluation criteria for it security — Part1: Introduction and general model (2005).
- [7] 織茂昌之, 津原 進, 山本倫子, 佐々木良一: 情報システムにおけるセキュリティ対策立案のための計画手法 (2000).
- [8] IPA: 定量的セキュリティ測定手法および支援ツールの開発, 入手先 <https://www.ipa.go.jp/files/000013702.pdf> (2004).
- [9] 中村逸一, 兵藤敏之, 曾我正和, 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).
- [10] Swidersk, F. and Snyder, W.: 脅威モデル—セキュアなアプリケーション構築, 日経 BP ソフトプレス (2005).
- [11] ISO/IEC 13335-1:2004: Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management (2014).
- [12] ISO/IEC: Information technology — security techniques — evaluation criteria for it security — Part1: Introduction and general model (2005).
- [13] IPA: IoT 開発におけるセキュリティ設計の手引き (2016), 入手先 <https://www.ipa.go.jp/files/000052459.pdf>.
- [14] ITU-T: SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyber-security information exchange — Vulnerability/state exchange (2011).
- [15] 元田 浩, 津本周作, 山口高平, 沼尾正行: データマイニングの基礎, オーム社 (2006).



太田原 千秋 (正会員)

2010 年東京理科大学工学部経営工学科卒業。2012 年中央大学理工学部情報工学専攻修了。同年 (株) 日立製作所入社。現在、同社研究開発グループシステムイノベーションセンタ研究員。情報セキュリティ技術、制御セキュリティ技術等の研究開発に従事。電気情報通信学会会員。



内山 宏樹 (正会員)

2001年京都大学工学部電気電子工学科卒業。2003年京都大学大学院情報学研究科通信情報システム専攻修了。同年(株)日立製作所入社。現在、同社研究開発グループシステムイノベーションセンター主任研究員。情報セキュリティ技術、制御セキュリティ技術等の研究開発に従事。電気学会会員。博士(情報学)。CISSP。



井口 慎也 (正会員)

1996年近畿大学理工学部電子工学科卒業。1998年神戸大学工学部自然科学研究科情報知能工学専攻博士前記課程修了。同年(株)日立製作所に入社。



萱島 信 (正会員)

1989年横浜国立大学大学院工学研究科電子情報工学専攻博士課程前期修了。同年(株)日立製作所入社。以来システム開発研究所(現:研究開発グループシステムイノベーションセンター)にてAI技術、オブジェクト指向技術、ネットワーク技術、セキュリティ技術等の研究に従事。現在、同研究所主任研究員。2006年よりIPA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研究員を兼務。電子情報通信学会、AI学会各会員。博士(工学)。