情報処理学会論文誌 Vol.59 No.9 1709–1725 (Sep. 2018)

車載システムを対象とした事後対策向け脅威監視項目の抽出手法および妥当性評価手法の提案

森田 伸義[1,a)] 川口 信隆[1] 井手口 恒太[1] 萱島 信[1]

受付日 2017年11月27日, 採録日 2018年6月8日

概要：車載システムの電動化およびインターネット等を介した車外端末との通信が増加している．これにともない，自動車を対象としたセキュリティ攻撃が危惧されており，実際に車載システムを狙った脅威事例が報告されている．このような脅威への対策として，車載システムのセキュリティ設計/実装時の事前対策だけでなく，セキュリティ運用時の事後対策も重要になりつつある．しかしながら，車載システムは，脅威の監視項目が明確になっていないという課題がある．また，車載システムは，搭載される装置や通信路のリソースが限られており，そのような環境で機能安全を担保するため，設計段階において性能に関する厳しいテスト要求を満たす必要がある．可用性を重視する自動車において，装置の追加や機能の更新による制御機能の性能に対する影響を考慮すると，運用段階で監視装置の追加や監視機能の更新を任意に行うことは現実的ではない．そこで本稿では，事後対策に向けた侵入検知に必要な脅威の監視項目の網羅的な抽出手法および評価手法を提案する．提案手法は，JASO TP15002 に基づくセキュリティ設計において攻撃侵入モデルを用いて，脅威分析で抽出した脅威の攻撃経路を把握し，Fault Tree 分析を用いて各攻撃経路に現れる攻撃による影響を監視項目として抽出，さらに城塞防衛モデルと攻撃侵入モデルを組み合わせることにより，脅威リスクを考慮しつつ，選定した監視項目の迅速性，網羅性，コスト負荷を定量的に評価できることを示した．

キーワード：セキュリティ設計，セキュリティ対策，車載システム

Proposal of Extraction and Validity Evaluation Method of Observe-items for In-vehicle Systems

Nobuyoshi Morita[1,a)] Nobutaka Kawaguchi[1] Kota Ideguchi[1] Makoto Kayashima[1]

Received: November 27, 2017, Accepted: June 8, 2018

Abstract: Recently, computerization and connectivity to external network of in-vehicle systems has been progressing. With the trend, there are big concerns about security attacks aginst vehicles and several attacks were actually reported. To mitigate the attacks, responses to the attackes becomes important, as well as design and implementation of security functions. However, because enough attack cases in automotive domain are not known, it is not clear which events of in-vehicle systems should be monitored. Furthermore, in-vehicle systems must meet stringent requirements on performance to achieve safety functionalities with limited computational power of in-vehicle devices and limited bandwidth of in-vehicle network. Adding devices and functionalities of monitoring to the in-vehicle systems after shipment may affect the performance of the system and therefore is not a practical solution. In this report, we first propose a new security design method that can comprehensively extract events which should be monitored when vehicles are used. Furthermore, we propose a new method that objectively evaluates the validity of the extracted events. The methods include the following features: (1) Visualization of intrusion path using intrusion model and extraction of influences by attack at intrusion path using FT analysis (2) Quantitative evaluation using a new model based on defense layers of castle. We expect that our new approach is effective for security management service in automotive domain.

Keywords: security design, security countermeasure, in-vehicle systems

1. はじめに

自動運転やコネクテッドカーといわれるように，車載システムの電動化およびインターネット等を介した車外端末との通信が増加している．これにともない，自動車を対象としたセキュリティ攻撃が危惧されており，実際に車載システムを狙った脅威事例が報告されている [1], [2], [3].

このような脅威への対応として，自動車を対象としたセキュリティ対策に関する標準規格や法規の整備が進んできている [4], [5], [6], [7], [8], [9], [10]．国内では，2016 年に重要生活機器連携セキュリティ協議会（CCDS）が車載器を対象としたセキュリティガイドライン [4] を策定しており，同ガイドラインでは，車載器を対象とした脅威やリスク，取り組むべきセキュリティ対策についてまとめられている．また，米国では，2016 年に，SAE（Society of Automotive Engineers）や NHTSA（National Highway Traffic Safety Administration）は自動車におけるサイバーセキュリティガイドライン [9], [10] を策定している．SAE が策定したガイドラインでは，セキュリティと機能安全の両方の観点に基づく開発プロセスを検討しており，NHTSA が策定したガイドラインは，脅威分析に基づいたセキュリティ対策を整備すること，利用中の自動車に関する潜在的なサイバーセキュリティインシデントに対してタイムリな脅威の監視と迅速な事後対策を行うことが盛り込まれている．さらに 2017 年に，米国では自動運転車のセキュリティに関する新たな法案が提案された [11]．同法案が施行された場合，NHTSA 等のガイドラインへの準拠が求められる可能性がある．これらの標準規格や法規は米国市場で販売される自動車を対象としており，自動車メーカやサプライヤに少なからず影響があると考える．以上のように，自動運転やコネクテッドカーの実現には，セキュリティ対策が必須になりつつある．

セキュリティ対策では，脅威のリスクを減らすために設計段階で対策を検討する「事前対策」，運用段階で顕在化する脅威を検知する「侵入検知」，顕在化した脅威による被害を最小化する「事後対策」の 3 つの観点で設計から運用にわたって対象システムの保護資産を守ることが有効と考えられている．特に，事後対策を適切に行うためには，攻撃者の侵入を検知できることが重要である．情報系システムでは，このような侵入を検知する仕組みとして IDS（Intrusion Detection System）や IPS（Intrusion Prevention System）が利用されている．ネットワークに IDS や IPS を追加，あるいはその機能を更新することで新たな脅威に対しても一定の効果が期待できる．実際に，産業用制御システムや車載システムを対象とした IDS/IPS の研究 [12], [13], [14] も行われている．

しかしながら，文献 [12], [13], [14] は，IDS/IPS の必要性や導入事例については述べているが，対象システムに対して，監視箇所および監視内容といった監視に関わる要件（以下，監視項目）をどのように導き出すかを説明しておらず，車載システムに IDS/IPS のような侵入検知機能を導入するにあたっても，監視項目が明確になっていないという課題がある．また，車載システムは，搭載される装置や通信路のリソースが限られているとともに，設計段階において性能に関する厳しいテスト要求を満たす必要がある．可用性を重視する自動車において，装置の追加や機能の更新による制御機能の性能に対する影響を考慮すると，IDS や IPS のような侵入検知による対策も設計段階において実施されることが望ましい．

上記の問題を解決するため，本稿では車載システムを対象に，セキュリティ設計段階において事後対策のための侵入検知向け監視項目の抽出手法を提案する．従来の車載システム向けセキュリティ設計手法は攻撃をシステムの境界上で防ぐ事前対策に主眼を置いている．しかし，事前対策が回避され事後対策で攻撃に対処する必要が生じた場合のコストとリスクのトレードオフに関する検討が十分とはいえない．特に，侵入検知に必要な監視項目の網羅性については課題がある．提案手法は，既存のセキュリティ設計手法に基づいて，サイバーキルチェーンモデルの観点で策定した攻撃侵入モデルを導入することで，対象システムで対処すべき脅威の攻撃経路を全パターン抽出し，攻撃の痕跡が残る可能性のある監視項目を Fault-Tree を用いた分析（以下，FT 分析）によって網羅的に抽出する．さらに，城塞防衛モデルと攻撃侵入モデルを組み合わせることで，脅威リスクを考慮しつつ，迅速性，網羅性，コスト負荷の観点で監視項目を定量的に評価する．提案手法により，すべての攻撃経路に対して，攻撃の早期段階で検知可能な監視箇所およびコスト負荷を明確化できる．また，従来手法と比べて侵入検知の回避の可能性を低く抑えることができる．

本稿は以下のとおり構成される．2 章では車載システムを対象としたセキュリティ脅威の監視に関する課題について述べる．3 章・4 章では提案手法の詳細について述べる．5 章では提案手法の有効性および今後の研究課題について議論する．最後に 6 章を本稿のまとめとする．

2. 車載システムにおける侵入検知の課題

本章では，車載システムとセキュリティ設計の概要を述べるとともに，システム監視における関連技術とその課題について述べる．

2.1 車載システムの概要

自動車は，自動車内部の車両制御の連携や情報集約の

[1] 株式会社日立製作所研究開発グループ
Hitachi Ltd., Research & Development Group, Yokohama, Kanagawa 244–0817, Japan
[a)] nobuyoshi.morita.gj@hitachi.com

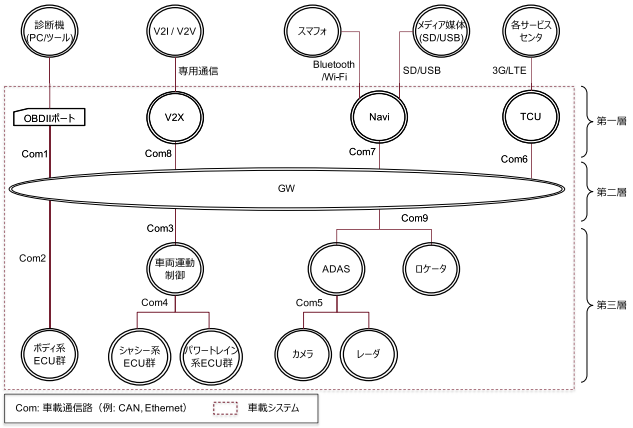

図 1 車載システムの構成
Fig. 1 System architecture of in-vehicle systems.

ため，複数の制御装置（以下，ECU：Electronic Control Unit）が車載ネットワークを介して通信を行うシステム（以下，車載システム）として構築されている．車載システムの例として，戦略的イノベーション創造プログラムにおける「V2X 等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト」では，GW（Gateway）を境界として，車外と直接つながるレイヤと，外部からの情報が GW を経由して接続される車内のレイヤからなる [15]．また，自動運転やコネクテッドカーと称される車載システムでは，複数の ECU からなるネットワークドメインを統合管理する Domain 型 ECU が検討されている [16], [17]．以上を参考として，本稿は，自動運転車における Domain 型 ECU として，各種センサ系 ECU からの情報を収集し，運転を支援する ADAS（Advanced Driving Assistant System）ECU や，走行制御に関るパワートレイン系 ECU やシャシ系 ECU を統合制御する車両運動制御 ECU が導入された構成を車載システムの例として想定する（**図 1**）．想定する車載システムは次の 3 層から構成される．

- 第 1 層

車外と直接つながる ECU（(Navigation ECU：Navi)，TCU（Telematics Communication Unit），V2X），あるいは I/F（診断用 OBD II（On-board diagnostics-II）ポート）

- 第 2 層

第 1 層と第 3 層の間でネットワークドメインを分離する GW

- 第 3 層

走行制御に直接関わる制御系 ECU（パワートレイン系 ECU 群，シャシ系 ECU 群），制御系 ECU を統合管理し，制御指令を出す車両運動制御 ECU，カメラやレーダ等のセンサ系 ECU，センサ系 ECU からの情報に基づいて運転を支援する ADAS，自車の位置情報を計測するロケータ ECU，窓やエアコンを制御するボディ系 ECU 群

また，このような車載システムは，情報システムと比較してセキュリティの観点で**表 1** に示すような特徴がある．

表 1 情報システムと車載システムの特徴
Table 1 Characteristics of IT system and in-vehicle system.

対象システム		情報システム	車載システム
保護資産の対象		情報	機能，情報
主な被害		情報漏えい， 金銭被害　等	人命損失/安全侵害， 情報漏えい， 金銭被害　等
ライフサイクル		3〜5 年	10〜20 年
セキュリティ特性の優先度	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り当て可能なリソース		高	低
アーキテクチャ		制御装置が繋がっておらず，DMZ と FW によって複数の情報系ネットワークドメインから成る構成	GW を中心にネットワークがドメインに分離され，ドメインを統括する Domain 型 ECU が搭載される構成

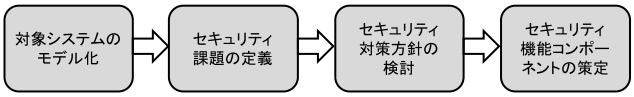

図 2 セキュリティ設計の流れ
Fig. 2 Flow of security design.

表 1 に示すとおり，被害が人命に及ばないように走行制御機能を安全に維持するための可用性を重視したセキュリティ特性，10 から 20 年にわたる長期間の製品ライフサイクル，セキュリティ機能の導入に割当て可能なリソースが乏しいこと，さらに GW を中心にネットワークドメインが分離されるとともに Domain 型 ECU が搭載されるアーキクチャが特徴である．

2.2 セキュリティ設計の概要

車載システムを対象としたセキュリティ設計の一手法として，自動車技術会が発行するテクニカルペーパー JASO TP15002 [18] が普及しつつある．JASO TP15002 は，情報システム分野で利用されている国際標準規格 ISO/IEC15408 [19], [20], [21] を考慮したセキュリティ設計の手順が定義されている．本稿では車載システムの開発に適用することを目標としているため，JASO TP15002 のセキュリティ設計に準拠した手法を検討する．以下に，JASO TP15002 に基づくセキュリティ設計の概要と手順を示す（**図 2**）．

(1) 対象システムのモデル化

対象システムの構造，および守るべき資産（保護資産）の明確化を行い，対象の利用環境を理解するために，対象

システムに関与するエンティティを洗い出すことによりモデル化する．

(2) セキュリティ課題の定義

対象システム内の保護資産に対して発生しうる脅威を分析，運用環境で対策を実施する脅威（前提条件）と，対象システムで対策を実施する脅威に分類し，組織のセキュリティ方針とあわせて整理する．

(3) セキュリティ対策方針の検討

セキュリティ課題に対抗するため，抽出した脅威の発生要因を分析し，セキュリティ対策の方針を検討する．

(4) セキュリティ機能コンポーネントの策定

セキュリティ対策方針を具体化するセキュリティ機能コンポーネントを策定する．

2.3 関連技術

対象システムを監視するためのセキュリティ機能コンポーネントの策定に関する技術として，セキュリティ設計をモデル化することでセキュリティ対策立案を支援する手法について述べる．上記 2.2 節で述べたとおり，セキュリティ設計における対策立案は脅威分析結果に基づいて検討される．脅威分析の手法として，自動車業界にも適用実績のある Attack Tree を用いた脅威分析に基づく手法と，5W 法を用いた脅威分析に基づく手法がある [22], [23], [24]．Attack Tree は自動車の車車間，路車間通信を対象として脅威分析を実施した EVITA プロジェクト [25] で使用された手法である．一方，5W 法は JASO TP15002 [18] において，自動車のセキュリティを確保するための脅威分析手法として掲載されている．以下に，それぞれの手法について述べる．

(1) EVITA プロジェクトにおけるセキュリティ設計

EVITA では，Attack Tree を用いた脅威分析によって脅威を抽出し，抽出した脅威に対して，CC（Common Criteria）の CEM（Common Evaluation Methodology）を基に提案されているリスク評価手法を用いて脅威リスクを評価する方法が開示されている．Attack Tree は，Schneier [22], [23] により考案された手法であり，攻撃者の視点による多段階的な攻撃手法である．EVITA における Attack Tree に基づく脅威分析は，セキュリティの攻撃により侵害されるシナリオを策定し，脆弱性を利用した攻撃の具体的な手順を検討して樹状に展開する．また，EVITA でのリスク評価は，攻撃の結果の深刻度を 4 つの観点（Safety，Financial，Privacy，Operational）で見積もり，これらの観点ごとに攻撃の容易さ（経過時間，経験的知識，システムの知識，期間の時間枠，装置の要素）と組み合わせリスクを見積もることである．ただし，Safety については，運転者による回避可能性であるコントローラビリティを考慮に入れる．

(2) JASO TP15002 におけるセキュリティ設計

JASO TP15002 は，ISO/IEC15408 のセキュリティ設計の流れを踏襲しており，DFD（Data Flow Diagram）によってモデル化された評価対象に対して 5W 法を用いた脅威分析によって脅威を抽出し，抽出した脅威に対して CRSS（CVSS based Risk Scoring Systems）等を用いて脅威リスクを評価する方法が開示されている．5W 法は，脅威の識別に必要な脅威エージェント，攻撃対象資産，攻撃内容に加え，対象システムのライフサイクルに関わる，攻撃の起きるフェーズや攻撃者の種別等を分類整理する．5W 法に必要な情報は，DFD を用いた対象システムのモデル化により明確化した情報を用いて，システマティックに作成できる．CRSS は，情報処理システムに対する脆弱性評価で利用されている CVSS（Common Vulnerability Scoring System）[26] を応用したリスク評価手法である．特に，CRSS では CVSS の基本値（攻撃容易性，資産の影響度）を用いてリスク評価を実施する．

2.4 従来手法適用時の課題

近年の脅威への対策は，入口対策や水際対策だけでは十分といえず，顕在化した脅威を早期に検知し，その被害を最小化する「事後対策」によって，対象システムの保護資産を守ることも必要とされている [27]．迅速かつ正確な事後対策を実現するためには，運用段階で顕在化する脅威を検知する侵入検知が重要である．なぜなら，顕在化した脅威を監視する侵入検知機能がなければ，早期段階での検知および十分な原因解明が困難となり，事後対策を迅速かつ正確に実施できない．IDS としての侵入検知の評価項目として，Milenkoski らは，文献 [28] において検知精度，検知してからレポートまでの期間（迅速性），性能負荷/処理能力，網羅性を用いている．このうち本稿は，車載システム全体の侵入検知として，攻撃経路上における効果的な監視箇所を明確化することに主眼を置き，これに関連する迅速性と網羅性が重要な指標になると考える．

上記 2.3 節に示すとおり，従来のセキュリティ設計は，対象システムで想定される脅威を洗い出すための脅威分析手法や対策優先度を明確化するためのリスク評価手法が提案されている．しかしながら，Attack Tree を用いる EVITA は，分析者が想定するシナリオに基づいて脅威を抽出しているため，対象システムへの侵入口（以下，アタックサーフェイス）がすべて網羅されているか不明確であり，監視すべき脅威が漏れる可能性がある．一方，5W 法を用いる JASO TP15002 は，アタックサーフェイスは明確になっているが，アタックサーフェイスと保護資産の間の攻撃経路は明らかにならないため，脅威の監視項目を特定できない．JASO の手法は，詳細な攻撃方法を抽出する前に，CRSS を用いたリスク評価を実施し，リスク値の低い脅威への対策を許容するため，すべての脅威に対して詳細な攻撃方法を抽出しない．また，リスク値の高い脅威に対しても，セキュリティ機能コンポーネントの要件を策定するが，どこ

に配置するかを対象としていない．

このように，Attack Tree や 5W 法だけでは，車載システムにおける侵入検知として，どのタイミングで検知できるかという迅速性，どの装置が何を監視するという監視項目の網羅性の明確化には至っていない．さらに，事前対策に向けたセキュリティ設計は，リスクの高い脅威に対して，実用的なコストで対応できるセキュリティ機能コンポーネントを策定している．なぜなら，従来のセキュリティ設計手法は攻撃をシステムの境界上で防ぐ事前対策に主眼を置いているからである．しかしながら，事前対策が回避され，事後対策で攻撃に対処する必要が生じた場合のコストとリスクのトレードオフに関する検討が十分とはいえない．特に，侵入検知に必要な監視項目の迅速性や網羅性については課題がある．搭載するセキュリティ機能コンポーネントを絞ることは，侵入検知に向けた監視を阻害する要因となってしまう．このため，監視項目の網羅性を重視しつつコストへの影響を評価できる必要がある．

以上のとおり，侵入検知に向けた脅威の監視項目の抽出は，対象システムに応じた脅威分析に基づいて，解析的に実施できる必要がある．また，車載システムは運用段階で監視装置や機能を導入することは現実的でないため，セキュリティ設計段階で網羅性を重視した脅威の監視項目を抽出し，監視項目の迅速性，網羅性およびコストへの影響を定量的に評価できる必要がある．

【課題】

(1) セキュリティ設計段階で網羅的な攻撃経路を考慮した脅威の監視項目の抽出

(2) 侵入検知に向けた監視項目の迅速性，網羅性およびコスト影響の定量的評価

3. 侵入検知向け監視項目の抽出手法

本章では，上記 2.4 節であげた課題 (1)「セキュリティ設計段階で脅威分析に基づいた網羅的な脅威の監視項目の抽出」を解決するにあたり，既存の事前対策に向けたセキュリティ設計と共存することを目指している．そこで，本稿では自動車業界でも利用実績のある JASO TP15002 をベースに，抽出された脅威に応じてアタックサーフェイスから保護資産までの攻撃経路を明確化することで，より網羅的な脅威の監視項目の抽出手法を提案する．

3.1 課題の解決方針

提案手法は，侵入検知向け監視項目の設計において，車載システムで監視すべき項目を網羅的に抽出するために，車載システムのどこで，どのような脅威に起因する事象が発生するかを明らかにすることとし，下記 3 項目に着目した．

(1) 脅威の対象範囲の明確化

前述のとおり，セキュリティ設計において対象システム

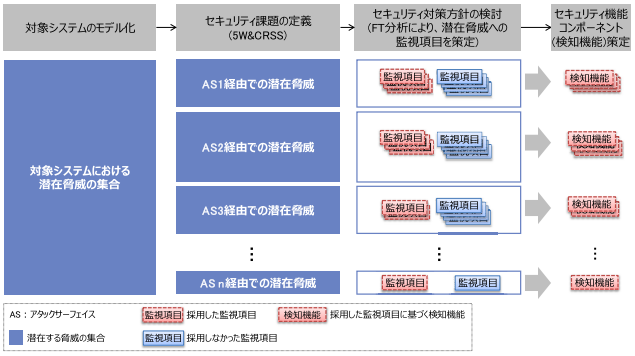

図 3 JASO TP15002 を用いた監視項目の抽出概要

Fig. 3 Overview of extracting observe-items (JASO TP15002).

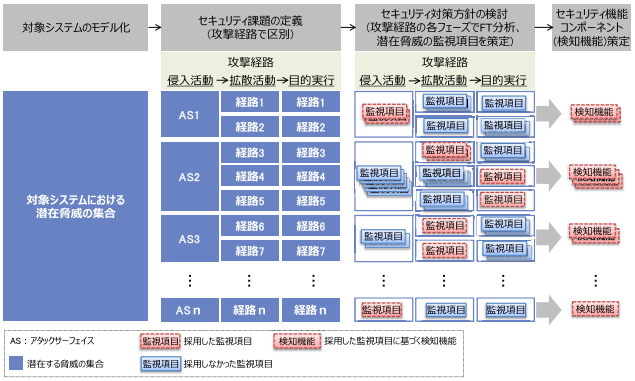

図 4 提案手法を用いた監視項目の抽出概要

Fig. 4 Overview of extracting observe-items (proposal method).

についての脅威を抽出するためには，守るべき保護資産と前提条件（環境での対処）を明確化しなければならない．本稿では，侵入検知向けに監視すべき脅威の対象について明らかにする．

(2) 脅威を引き起こす網羅的な攻撃経路の抽出

JASO TP15002 では，DFD によるシステムモデル化および 5W 法を用いた脅威分析によって，アタックサーフェイスから保護資産に対する脅威の抽出が可能である．本稿では，システム構成と攻撃プロセス（侵入活動，拡散活動，目的実行）を考慮した攻撃侵入モデルを考慮することで，アタックサーフェイスから保護資産に至るまでの攻撃経路（侵入活動，拡散活動，目的実行からなる経路）を網羅的に明らかにすることにより，攻撃の痕跡が残る可能性のある監視項目を明確化する．

(3) 攻撃の痕跡に着目した監視項目（監視箇所，監視内容）の策定

監視項目として監視箇所と監視内容を策定するために，本稿ではアタックサーフェイスから保護資産に至るまでの攻撃経路において，攻撃プロセスの観点で監視可能な攻撃の痕跡を明らかにする．

以上をふまえて，JASO TP15002 を用いて監視項目を抽出する場合と，提案手法を用いた場合の違いを図 3，図 4

表 2 提案手法における脅威の対象範囲
Table 2 Scope of cyber security thread for propose method.

比較項目	JASO TP15002	提案手法
適用目的	事前対策向け	侵入検知向け
対象システム	DFD ベースのシステムモデル	変更なし (事前対策と同じシステムモデルを活用)
守るべき保護資産	各 ECU に搭載される CIA の観点で重要とされる，情報および機能	走行制御に関る制御系 ECU （パワートレイン系，シャシー系）の機能
前提条件	信頼境界を設け，運用や環境による対策を前提として許容する脅威を定義	アタックサーフェイス，保護資産に対する攻撃経路を除外するような前提を設けない

に示す．同じ対象システムを扱うため，対象システムにおける潜在的な脅威は同じになる．図 3 に示すとおり，JASO TP15002 を用いた場合は，アタックサーフェイスから保護資産に対する脅威がアタックサーフェイスごとに抽出され，抽出された脅威ごとに監視項目を抽出する．一方，提案手法を用いた場合は，アタックサーフェイスから保護資産に対する攻撃経路を明確化し，攻撃経路の各フェーズごとに脅威の監視項目を抽出する．図 3，図 4 に示すとおり，JASO TP15002 を用いた場合，攻撃経路が明確になっていないため，システム設計者が選択した監視項目がすべての攻撃経路に対応できているかどうかが不明である．これに対して，提案手法は，攻撃経路を明確にしたうえで，攻撃経路の各フェーズごとに監視項目を明確化することにより，システム設計者は，攻撃経路を網羅的に監視することが可能な監視項目を選択することが可能となる．なお，JASO TP15002 以外の従来研究についても我々が調査した範囲において，同様の手法を提案している研究事例は発見されていない．

以降では，これら 3 項目を考慮した侵入検知向け脅威の網羅的な監視項目の抽出手法の詳細について述べる．

3.2 脅威の対象範囲の明確化

上記 2.2 節で述べたとおり，対象システムにおける脅威の対象範囲は，対象とするシステムモデル，守るべき保護資産，前提条件によって定まる．よって，侵入検知に向けた脅威の対象範囲を明確化するために，これらの項目について提案手法としての対応を**表 2** に示す．

- 対象とするシステムモデル

対象システムについては，本稿で対象とする車載システムは事前対策と侵入検知でシステムモデルに変更はない．仮に，運転手等のユーザが購入後に Navi や走行計測のための装置を追加する場合，そのような装置が追加できることを前提としたシステムモデルに基づいた脅威分析が必要であり，これは侵入検知だけでなく，事前対策に向けたセキュリティ設計においても必要となる．ゆえに，本稿では事前対策と侵入検知とで同じ対象システムを用いることを想定する．

- 守るべき保護資産

事前対策と同等の保護資産の数に対して脅威の監視項目を網羅的に抽出する場合，作業負荷や対策コスト負荷が大きい．リスクの高い脅威に対しては事前対策である程度担保されていることを考慮する場合，侵入検知においてすべての保護資産に対する脅威を監視することは効率的ではない．そこで，情報システムと車載システムの大きな違いとなる人命に影響する脅威にかかわる保護資産を侵入検知向けの保護資産とする．具体的には，自動車にとって走行制御を司る機能が攻撃を受けた場合に，自動車の安全性を担保できなくなり，人命にその影響が及ぶ可能性がある．このため，提案手法では制御系 ECU の機能に保護資産を絞ることにより，作業負荷および対策コスト負荷の低減を図る．

- 前提条件

事前対策に主眼を置く JASO TP15002 では，評価対象は車載システムに限定されており，センタ側のサービス提供者/サーバは安全であることを前提としている．これは脅威分析を実施するにあたり，信頼できる範囲を明確化し，脅威の洗い出しに要する作業負荷を抑えるために行うためである．しかしながら，侵入検知は，設計ミス，実装ミス，運用ミス等によって引き起こされる脅威（例：開発時に使用していたポートが閉じられないまま，攻撃者の侵入を許してしまうケース），あるいは対象システムでは直接対策できないような評価対象外のエンティティ（関与者/関与装置）における前提が覆る事態によって引き起こされる脅威（例：対象システムがダウンロードするアプリセンタにウイルスに感染したアプリを不正にアップロードされるケース）によって，事前対策が十分に機能しないことを考慮すべきである．このため，提案手法はアタックサーフェイスや攻撃経路を絞るような前提条件を設けない．

以上より，提案手法は，対象システムのモデル化は事前対策と同様のシステムモデルを用いて，守るべき保護資産としては走行制御にかかわる制御系 ECU の機能に絞り，前提条件としてはアタックサーフェイスや攻撃経路を絞るような前提を設けない．

3.3 脅威を引き起こす網羅的な攻撃経路の抽出

脅威を引き起こす攻撃経路を網羅的に抽出するため，システム構成と攻撃プロセスを考慮した攻撃侵入モデルを導入することで，アタックサーフェイスから保護資産に至るまでの攻撃経路を明らかにする．システム構成としては，上記 2.1 節で述べた対象システムモデル（図 1）を用いる

表 3 アタックサーフェイスのパターン
Table 3 Pattern of attack surface.

侵入経路			アタックサーフェイスの具体例	
創出アタックサーフェイス	車内	タッピング(通信路に接続されたECUの付替え，通信路自体のタッピング)	AS 1	不正 ECU：攻撃対象同一ドメイン
			AS 2	不正 ECU：GW を介さない別ドメイン
			AS 3	不正 ECU：GW を介した別ドメイン
既存アタックサーフェイス	サービス	ローカル経由	AS 4	リプロサービス／診断サービス(OBD Ⅱ経由で ECU のソフトウェア更新やログ収集するサービス)，アプリインストールサービス（Navi）
		隣接経由	AS 5	V2X サービス，スマフォ/Navi 連携（音楽）
		ネットワーク経由	AS 6	OTA サービス(遠隔のセンタから 3G/LTE 経由で ECU のソフトウェアを更新するサービス)，地図配信サービス，アプリダウンロードサービス(Navi)
	車外	ローカル経由	AS 7	不正端末
		隣接経由	AS 8	不正端末，不正インフラ(不正 V2I)，不正自動車(不正 V2V)，不正センサ
		ネットワーク経由	AS 9	不正センタ

こととした．

一方，世の中でよく知られている攻撃プロセスとしては，ロッキード・マーティン社が提唱したサイバーキルチェーンモデルがある[*1]．サイバーキルチェーンモデルは，情報システムを対象としたモデルであり，「偵察 → 武器化 → デリバリ → エクスプロイト → インストール → Command & Control（C&C）→ 目的の実行」の 7 段階に区分される．さらに，これら 7 段階の区分は，偵察や武器化のような「準備活動」，デリバリ，エクスプロイト，インストールのような「侵入活動」，C&C のような「拡散活動」，目的の実行のような「目的実行活動」の 4 段階に分類できる．このうち，偵察や武器化のような準備活動は車外での活動となるため，車載システムでは監視できない．そこで，提案手法はサイバーキルチェーンモデルを車載システムにおける監視の観点で整理した攻撃侵入モデルを策定し，攻撃侵入モデルと対象システムモデルに基づいた攻撃経路の網羅的な抽出を行うこととした．以下に，具体的な提案手法の詳細を示す．

3.3.1 サイバーキルチェーンモデルに基づく車載システム向け攻撃侵入モデル

サイバーキルチェーンモデルのうち，攻撃プロセスの監視が困難な準備活動を除いた 3 項目について攻撃プロセスを整理する．

(1) 侵入活動

侵入活動は，対象システムのアタックサーフェイスを探して，攻撃コードを用いてターゲットへの侵入を開始，攻撃コードを実行することでアタックサーフェイスとなる装置の足場を確立する．このようなアタックサーフェイスへの侵入パターンとして，対象システムが備える既存の通信 I/F をアタックサーフェイスとするパターンと，対象システムが備える既存の I/F を介さずに，対象システムを改変して新たなアタックサーフェイスを創出するパターンが考えられる．さらに，既存の I/F は，サービスの脆弱性を悪用された場合，物理的につながる I/F ではなく論理的につながる I/F まで侵入されることを想定すべきと考える．そこで，既存の I/F は論理的な I/F としてサービスを考慮し，物理的な I/F として車外からの接続 I/F を想定する．また，JASO15002 を踏襲し，対象に直接つながるローカル経由に加えて，物理的な距離に関係なく 3G/LTE やインターネットを介して攻撃可能なケースをネットワーク経由とし，Bluetooth 通信や V2X 通信等のように近距離通信を介して攻撃可能なケースを隣接経由として区別する．以上をふまえて，図 1 で示した車載システムモデルを対象に，アタックサーフェイスへの侵入パターンを**表 3** に示す．対象システムのアタックサーフェイスとして，AS1 から AS9 までの 9 種類のアタックサーフェイスを定義した．

(2) 拡散活動

アタックサーフェイスに侵入した後に，攻撃目標（制御系 ECU）に攻撃できる最終攻撃元装置まで，中継装置への拡散を繰り返す．ただし，侵入したアタックサーフェイスから攻撃目標に攻撃できる場合，拡散活動は観測されない．

(3) 目的実行活動

攻撃目標に対して，攻撃者が意図した攻撃を実行することにより，保護資産の可用性を損なわせる．

[*1] CYBER KILL CHAIN は，米国 Lockheed Martin Corporation の米国における登録商標または商標です．

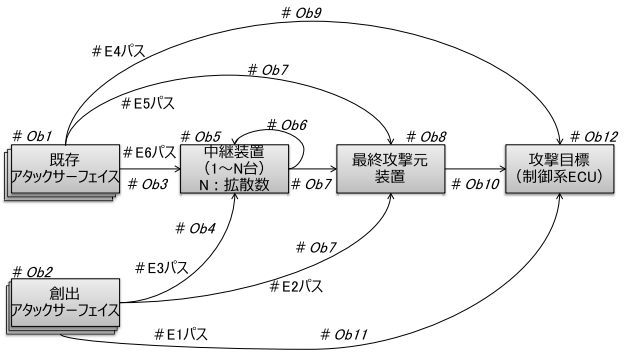

図 5 サイバーキルチェーンに基づく車載システム向け攻撃侵入モデル

Fig. 5 Attack path model for in-vehicle system based on cyber kill chain.

表 4 監視箇所の概要

Table 4 Overview of observe-point.

監視箇所	概要
#Ob1	既存アタックサーフェイス（侵入経路）
#Ob2	創出アタックサーフェイス（侵入経路）
#Ob3	既存アタックサーフェイスから中継装置への拡散経路
#Ob4	創出アタックサーフェイスから中継装置への拡散経路
#Ob5	拡散活動における中継装置
#Ob6	中継装置から中継装置への拡散経路
#Ob7	最終攻撃元装置に対する拡散経路
#Ob8	拡散活動後の最終攻撃元装置
#Ob9	既存アタックサーフェイスから攻撃目標への目的実行経路
#Ob10	最終攻撃元装置から攻撃目標への目的実行経路
#Ob11	創出アタックサーフェイスから攻撃目標への目的実行経路
#Ob12	攻撃目標となる保護資産

以上のとおり，提案手法は侵入活動，拡散活動，目的実行活動からなる攻撃プロセスに基づいた攻撃侵入モデルを活用する．具体的な攻撃侵入モデルを**図 5** に示す．攻撃侵入モデルは，車載通信路のタッピングや車載 ECU の付替えのように，車載システムが本来提供する I/F を迂回したアタックサーフェイス，すなわち攻撃者が新たに創出したアタックサーフェイス（以下，創出アタックサーフェイス）から侵入される#E1 から#E3 までの経路と，既存アタックサーフェイスから侵入される#E4 から#E6 までの経路に分類される．各経路において攻撃の痕跡を観測できる監視箇所として，#Ob1 から#Ob12 の 12 項目を定義した（**表 4**）．

これらの監視箇所は，車載システムの外から車載システムに侵入する経路を侵入経路（#Ob1，#Ob2）とし，車載システム内でさらに侵攻する経路を拡散経路（#Ob3，#Ob4，#Ob6，#Ob7）とし，攻撃目標に対して攻撃を実行する経路を目的実行経路（#Ob9，#Ob10，#Ob11）とする．また，拡散活動で中継される装置を中継装置（#Ob5），拡散活動を経て攻撃対象（#Ob12）に攻撃を行う装置を最終攻撃元装置（#Ob8）とする．本稿では，これらの侵入経路，拡散経路（拡散しないケースあり），目的実行経路を介して攻撃対象（#Ob12）に攻撃を実行する経路を総じて攻撃経路とする．

3.3.2 攻撃侵入モデルを活用した網羅的な攻撃経路の抽出

提案手法は，上記 3.3.1 項で示した攻撃侵入モデルと上記図 1 で示した車載システムモデルを用いることで，対象システムにおける攻撃経路を網羅的に抽出する．具体的には，攻撃目標である制御系 ECU（パワートレイン系 ECU，シャシ系 ECU）を，攻撃侵入モデルの攻撃対象#Ob12 として定義する．このとき，最終攻撃元装置#Ob8 は車両運動制御 ECU に定まるとともに，最終攻撃元装置#Ob8 から攻撃対象#Ob12 に対して目的実行活動の一環で攻撃を仕掛けるための通信路#0b10 は Com4 に定まる．さらに，各アタックサーフェイスについては，表 3 に示したとおり定義できる．これらをふまえて，#E1 から#E6 までの攻撃経路における監視箇所を明確化する．

ここで，対象とする車載システムモデルにおいて，GW は多くの ECU と接続されており，GW が割り当てられる監視箇所によっては存在しえない攻撃経路がある．そこで，GW の監視箇所の候補として，既存アタックサーフェイス#Ob1，中継装置#Ob5，あるいは監視箇所なしに絞った攻撃経路の抽出が効率的となる．また，拡散活動の回数についても拡散しないケース，1 回のみ拡散するケース，N 回拡散するケースが考えられる．これらを考慮した手順を下記に示すとともに，実際に抽出できた攻撃経路を**表 5** に示す．表 5 に示すとおり，対象とする車載システムにおいて攻撃経路は#E1 から#E6 をあわせて 8 つの経路を抽出できることが分かった．これら 8 つの経路は，#E1 から#E6 までの攻撃経路，GW の配置，拡散回数の 3 つの観点を「-」でつなげた識別子で示す．以上より，提案手法を用いることで脅威を引き起こす攻撃経路を網羅的かつ正確に抽出できる．

【攻撃経路の抽出手順】

① 攻撃目標の定義
② 最終攻撃元，および#Ob10 の設定
③ 既存アタックサーフェイスの設定
④ 創出アタックサーフェイスの設定
⑤ #E1 パスの抽出
⑥ #E2 パスの抽出
⑦ #E3 パスの抽出
⑧ #E4 パスの抽出
⑨ #E5 パスの抽出

表 5 攻撃経路の抽出結果
Table 5 Result of attack path.

識別子	GW の配置	拡散回数	攻撃経路
#E1-0-0	なし	—	#Ob2⇒#Ob11⇒#Ob12
#E2-0-0	なし	—	#Ob2⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12
#E3-#Ob5-1	#Ob5	1	#Ob2⇒#Ob4⇒【#Ob5】⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12
#E3-0-N	なし	N	#Ob2⇒#Ob4⇒（【#Ob5】⇒#Ob6⇒・・・）⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12
#E4-0-0	なし	—	#Ob1⇒#Ob9⇒#Ob12
#E5-#Ob1-0	#Ob1	—	【#Ob1】⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12
#E6-#Ob5-1	#Ob5	1	#Ob1⇒#Ob3⇒【#Ob5】⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12
#E6-#Ob5-N	#Ob5	N	#Ob1⇒#Ob3⇒（【#Ob5】⇒#Ob6⇒・・・）⇒#Ob7⇒#Ob8⇒#Ob10⇒#Ob12

表 6 #Ob2 経由の攻撃経路における監視箇所の詳細
Table 6 Detail of observe-point in the attack path from #Ob2.

攻撃経路	#Ob2	#Ob4	#Ob5			#Ob6		#Ob7	#Ob8	#Ob10	#Ob11	#Ob12
#E1-0-0	Com4タッピング										Com4	制御系ECU
#E2-0-0	Com3タッピング							Com3	車両運動制御	Com4		制御系ECU
#E3-#Ob5-1	Com1タッピング	Com1	GW					Com3	車両運動制御	Com4		制御系ECU
	Com2タッピング	Com2	GW					Com3	車両運動制御	Com4		制御系ECU
	Com6タッピング	Com6	GW					Com3	車両運動制御	Com4		制御系ECU
	Com7タッピング	Com7	GW					Com3	車両運動制御	Com4		制御系ECU
	Com8タッピング	Com8	GW					Com3	車両運動制御	Com4		制御系ECU
	Com9タッピング	Com9	GW					Com3	車両運動制御	Com4		制御系ECU
#E3-#Ob5-N	Com1タッピング	Com1	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com2タッピング	Com2	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com6タッピング	Com6	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com7タッピング	Com7	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com8タッピング	Com8	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com9タッピング	Com9	GW	N		N		Com3	車両運動制御	Com4		制御系ECU
	Com5タッピング	Com5	ADAS	GW	N	Ethenet4	N	Com3	車両運動制御	Com4		制御系ECU

（N：複数の拡散対象を示す）

⑩ #E6 パスの抽出
※上記，⑤から⑩の手順は，GW の配置と拡散回数を考慮

3.4 攻撃の痕跡に着目した監視項目（監視箇所，監視内容）の策定

提案手法は，上記表 5 に示す#E1 から#E6 までの 8 つの攻撃経路における各監視箇所（#Ob1 から#Ob12）に対して，攻撃の拡散経路となる箇所（アタックサーフェイス，中継装置，最終攻撃元装置，攻撃目標，通信路）の組合せをすべて抽出する．上記図 1 に示す車載システムに提案手法を適用した結果を**表 6** と**表 7** に示す．表 6 に示すとおり，創出アタックサーフェイスから侵入する経路（#E1 から#E3）では，監視可能な箇所として 15 通りの監視箇所を抽出できた．また，表 7 に示すとおり，既存アタックサーフェイスから侵入する経路（#E4 から#E6）では，監視可能な箇所として 43 通りの監視箇所を抽出できた．各 Table に示すとおり，各監視箇所に複数の監視箇所が割り当てられるケースも抽出できており，提案手法はすべての攻撃経路に対する監視箇所を網羅的に抽出できる．ただし，拡散活動において監視可能な#Ob5 および#Ob6 については，拡散先が 1 カ所に必ずしも特定できないケースを含むため，拡散先になる可能性のある N 個の装置や経路を監視箇所としている．拡散先の「N」は，最終攻撃元装置（#Ob8）と攻撃対象（#Ob12）を除いた，拡散経路上の ECU の個数を示しており，その上限は車内の ECU の個数となり，監視箇所の網羅性を満たす．

一方，監視内容について提案手法は，攻撃プロセスの侵攻を成功させるにあたり，その要因を機能安全設計や脅威分析で利用されている FT 分析を使用する．具体的には，FT 分析を用いて，表 5 に示す各攻撃経路パターンにおける監視箇所（#Ob1 から#Ob12）ごとに，図 5 で示した攻撃侵入モデルにあわせた攻撃方法を定義し，攻撃によって顕在化する可能性のある影響を洗い出し，その影響を監視内容として抽出する．そして，上記 FT 分析の結果と**表 8** で示した攻撃経路における物理的な監視箇所に基づいて，具体的な監視箇所を抽出する．

以上をまとめた監視内容の抽出例を**図 6** に示す．図 6 では，#E4-0-0 における#Ob1 の 3G/LTE 経由で車両運動制御 ECU に対するソフトウェアの更新（以下，OTA（Over The Air））を行う OTA サービスを悪用した侵入活動をモデルに述べる．OTA サービスの概要は，TCU が OTA センタとの通信を行い，TCU を介して GW に対してリプロ用のデータが送られ，GW が受信したデータの正当性を検証した後に，GW から車両運動制御 ECU に対してリ

表 7 #Ob1 経由の攻撃経路における監視箇所の詳細
Table 7 Detail of observe-point in the attack path from #Ob1.

攻撃経路	#Ob1	#Ob3	#Ob5			#Ob6			#Ob7	#Ob8	#Ob9	#Ob10	#Ob12
#E4-0-0	車両運動制御リプロ										Com4		制御系ECU
	車両運動制御OTA										Com4		制御系ECU
#E5-#Ob1-0	GWのリプロ								Com3	車両運動制御		Com4	制御系ECU
	GWのOTA								Com3	車両運動制御		Com4	制御系ECU
#E6-#Ob5-1	Com1不正端末(診断機)	Com1	GW						Com3	車両運動制御		Com4	制御系ECU
	ボディ系ECUリプロ	Com2	GW						Com3	車両運動制御		Com4	制御系ECU
	ボディ系ECUOTA	Com2	GW						Com3	車両運動制御		Com4	制御系ECU
	TCUリプロ	Com6	GW						Com3	車両運動制御		Com4	制御系ECU
	TCUOTA	Com6	GW						Com3	車両運動制御		Com4	制御系ECU
	Naviリプロ	Com7	GW						Com3	車両運動制御		Com4	制御系ECU
	NaviOTA	Com7	GW						Com3	車両運動制御		Com4	制御系ECU
	Navi/スマフォ連携サービス	Com7	GW						Com3	車両運動制御		Com4	制御系ECU
	Naviアプリダウンロードサービス	Com7	GW						Com3	車両運動制御		Com4	制御系ECU
	V2Xリプロ	Com8	GW						Com3	車両運動制御		Com4	制御系ECU
	V2XOTA	Com8	GW						Com3	車両運動制御		Com4	制御系ECU
	ロケータ地図更新サービス	Com9	GW						Com3	車両運動制御		Com4	制御系ECU
	ロケータリプロ	Com9	GW						Com3	車両運動制御		Com4	制御系ECU
	ロケータOTA	Com9	GW						Com3	車両運動制御		Com4	制御系ECU
	ADASリプロ	Com9	GW						Com3	車両運動制御		Com4	制御系ECU
	ADASOTA	Com9	GW						Com3	車両運動制御		Com4	制御系ECU
#E6-#Ob5-N	Com1不正端末(診断機)	Com1	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ボディ系ECUリプロ	Com2	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ボディ系ECUOTA	Com2	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	TCUリプロ	Com6	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	TCUOTA	Com6	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	センタサービス	3G/LTE	TCU	GW	N	Com6	N		Com3	車両運動制御		Com4	制御系ECU
	不正センタ	3G/LTE	TCU	GW	N	Com6	N		Com3	車両運動制御		Com4	制御系ECU
	Naviリプロ	Com7	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	NaviOTA	Com7	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	スマフォ	Bluetooth/Wi-Fi	Navi	GW	N	Com7	N		Com3	車両運動制御		Com4	制御系ECU
	Navi/スマフォ連携サービス	Com7	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	Naviアプリダウンロードサービス	Com7	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	不正メディア媒体	SD/USB	Navi	GW	N	Com7	N		Com3	車両運動制御		Com4	制御系ECU
	V2Xリプロ	Com8	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	V2XOTA	Com8	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	不正V2X装置	V2X通信	V2X	GW	N	Com8	N		Com3	車両運動制御		Com4	制御系ECU
	ロケータ地図更新サービス	Com9	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ロケータリプロ	Com9	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ロケータOTA	Com9	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ADASリプロ	Com9	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	ADASOTA	Com9	GW	N		N			Com3	車両運動制御		Com4	制御系ECU
	不正センサ(カメラ)	光学	カメラ	ADAS	GW N	Com5	Com9	N	Com3	車両運動制御		Com4	制御系ECU
	不正センサ(レーダ)	レーダ	レーダ	ADAS	GW N	Com5	Com9	N	Com3	車両運動制御		Com4	制御系ECU

(N：複数の拡散対象を示す)

表 8 攻撃経路における物理的な監視箇所
Table 8 Physical observe-point in the attack path.

攻撃経路	監視箇所	監視事象	監視可能箇所							
			CGW	TCU	Navi	車両運動制御	ボディ	制御系ECU	ADAS	・・・
#E4-0-0	Ob12	制御系ECU						○		
	Ob9	Com4				○		○		
	Ob1	車両運動制御(リプロ)	○			○				
		車両運動制御(OTA)	○	○		○				

(○：監視可能箇所)

プロ処理を実行することを想定する．このような想定で，#E4-0-0 における#Ob1 を対象とした場合，図 5 において#Ob1 は「侵入活動」を示し，その侵入経路は「車両運動制御 ECU の OTA」となっているため，攻撃方法は，「車両運動制御 ECU の OTA を悪用し，車両運動制御 ECU に侵入する」となり，この攻撃方法に対して，FT 分析による監視内容の抽出結果として 7 項目の監視内容を抽出できる．

4. 侵入検知向け監視項目の評価手法

本章では，上記 2.4 節であげた課題 (2)「監視項目の迅速性，網羅性およびコスト影響の定量的評価」を解決するにあたり，評価項目を明確化するとともに，評価項目に基づく評価手法を提案する．

4.1 課題の解決方針

文献 [28] において迅速性は，検知してからレポートまでの期間として定義されているが，この観点では実装方法や運用体制等にその効果が大きく依存してしまう．このため，提案手法はセキュリティ設計段階でも評価できるように，侵入活動から目的実行活動に至る攻撃プロセスにおける検知のタイミングを迅速性として評価することとした．一方，網羅性については，提案手法は抜け漏れなく攻撃経

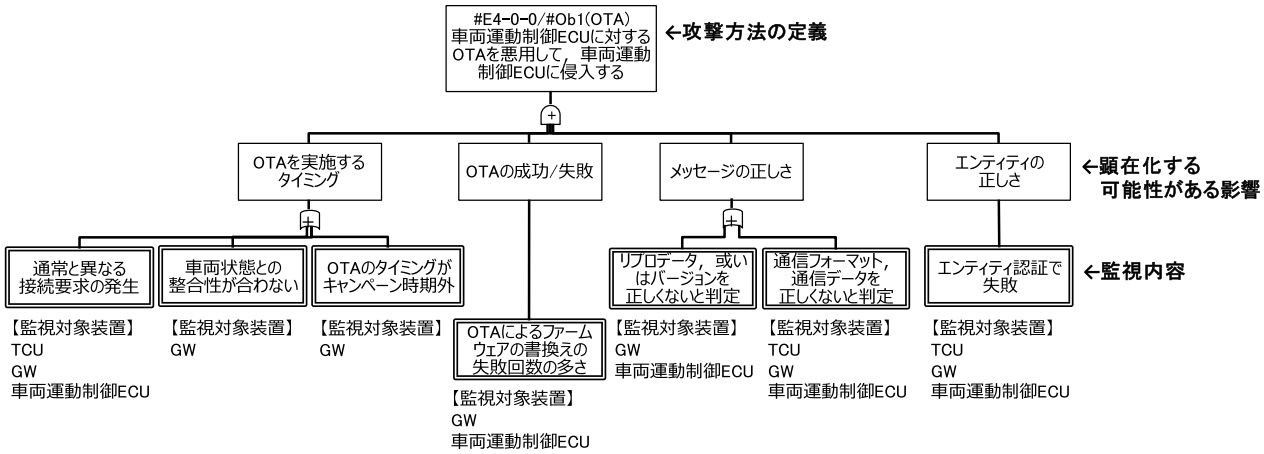

図 6 分析を用いた監視内容の抽出
Fig. 6 Result of FT analysis.

路を監視できることを評価するために，攻撃経路に対する監視可能な経路によって網羅性を評価することとした．監視項目（監視箇所，監視内容）が明確になっていればセキュリティ設計段階でも評価可能である．加えて，提案手法は侵入検知に向けた脅威の監視機能を導入するにあたり，コストに見合わない対処にならないように，脅威のリスクと対処に要するコストも考慮した評価できることを目指す．下記に，提案手法における評価項目の要件を示す．

【評価項目の要件】

(1) 迅速性（攻撃プロセスにおける検知のタイミング）
(2) 網羅性
(3) コスト負荷
(4) 脅威リスクの考慮

また，脅威の監視機能の評価における一手法として，城塞防衛モデルを活用した評価手法が提案されている [29]．具体的には，監視機能を有する製品数に合わせた同心円を描き，円の最も外側をアタックサーフェイス，円の最も中心を攻撃対象とし，攻撃パターンを円弧で区切り，どの同心円で検知できるかを評価する．文献 [29] において，同手法は監視機能を備える複数の製品の監視内容の重複性，独立性を視覚化することに利用されている．そこで，提案手法は上記城塞防衛モデルを参考とし，上記評価項目の要件であげた観点をふまえた評価手法を 4.2 節で示す．

4.2 監視項目の評価手法

提案手法は，図 1 に示した車載システムを対象に，上記 4.1 節で明確化した評価項目を以下の観点で反映した城塞防衛モデルを**図 7** に例示する．

(1) 迅速性（攻撃プロセスにおける検知のタイミング）

同心円を用いて表現される城塞防衛モデルにおいて，円の最も外側をアタックサーフェイス（創出アタックサーフェイス，既存アタックサーフェイス），円の中心を攻撃対象（保護資産：制御系 ECU）に置き換えることが可能

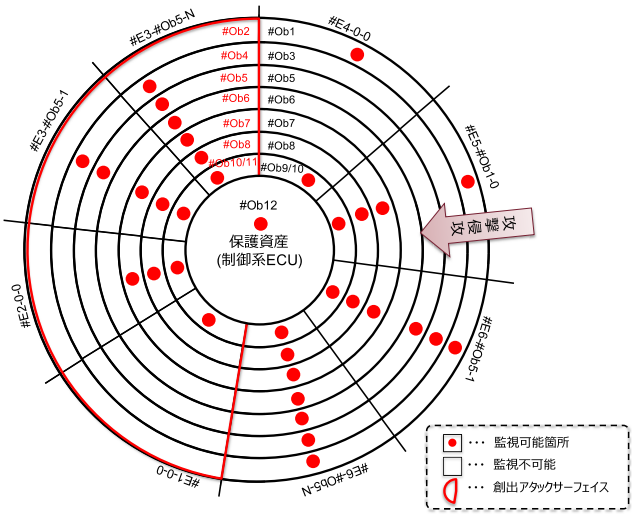

図 7 城塞防壁モデルに基づく評価モデル
Fig. 7 Evaluation model based on defense layers of castle.

である．提案手法は，アタックサーフェイスから保護資産に至るまでの同心円を各攻撃経路における監視箇所として定義する．このとき，攻撃目標に対する経路である#Ob9，#Ob10，#Ob11 を同じレベルに設定する．これにより，攻撃プロセスのどのタイミングで監視可能か（迅速性）を視覚化できる．具体的には，選定した監視項目が属する監視箇所（#Ob1 から#Ob11 のいずれか）から保護資産（#Ob12）までの階層数 r を求め，選定したすべての監視項目に同様の処理を行い，最終的に各攻撃経路 i における最大値 r_i の平均値を算出することにより，平均値が高いほど対象システムにおける監視項目の迅速性が高いと評価できる．なお，図 7 に示すとおり，同心円モデルは 8 つの円から構成されており，r の最大値は最も外側を監視箇所に選定した場合の「8」となり，同心円の中心となる攻撃目標を監視箇所に選定した場合は「1」となり，攻撃経路において監視項目を選定しなかった場合は「0」となる．

$$\text{Rapidity} = \frac{1}{n}\sum_{i=1}^{n} r_i$$

r_i：各攻撃経路 i で選定した監視項目の階層数（最大値）
n：攻撃経路の総数

(2) 網羅性

提案手法は城塞防衛モデルに対して，上記 3.4 節で策定した監視項目をマッピングする．これにより，実際に導入する監視項目を選定した際に，攻撃経路に対する監視項目の抜け漏れの有無を確認するとともに，監視項目の網羅率を算出できる．具体的には，選定した監視項目がカバーできる攻撃経路の数 Observe_path と攻撃経路の総数 Attack_path との割合を算出し，Coverage rate が 100%に近いほど監視項目の網羅性が高いと評価できる．

$$\text{Coverage rate} = \frac{Observe\_path}{Attack\_path} * 100$$

(3) コスト負荷

コストの考え方として，監視項目（監視機能の導入）に紐づいてコストが発生すると考える．上記 (2) のとおり，提案手法は城塞防衛モデルに監視項目をマッピングするため，選定する監視項目に合わせて合計コストを算出できる．具体的には，ある監視項目を実現するセキュリティ機能コンポーネント $Function_i$ と当該機能の実現に要するコスト $Cost_i$ を求め，選定したすべての監視項目について同様の処理を行うことにより，合計コストを算出でき，Cost_t が高いほどコスト負荷が高いと評価できる．

$$\text{Cost}_\text{t} = \sum_{i=0}^{n}(Function_i * Cost_i)$$

$Function_i \in \{1, 0\}$

$Cost_i$：$Function_i$ のコスト

n：選定した監視項目の総数

(4) 脅威リスクの考慮

提案手法は，各攻撃経路で想定される脅威に対して TP15002 で利用されているリスク評価手法（CRSS）を用いてリスク値を算出する．提案手法において算出されたリスク値は，その値に応じて円弧の角度に適用する．これにより，脅威リスクの高い攻撃経路と脅威リスクの低い攻撃経路とでは，監視項目に割り当てられる面積に違いが出る．すなわち，提案手法は脅威リスクを考慮した視覚化が可能となる．なお，どの脅威が顕在化するかは設計段階では判定できない．脅威の発生確率を考慮する手法もあるが，提案手法は安全性を重視して各攻撃経路におけるリスク値の最大値に基づいて円弧の角度 θ（radian）を算出する．具体的には，各攻撃経路における最大リスク値の合計 $Total\_risk\_max$ と，該当する攻撃経路のリスク値の最大値 $Path\_risk\_max$ の割合で算出する．

$$\theta = \frac{Path\_risk\_max}{Total\_risk\_max} * 2\pi$$

図 7 に示した評価モデルにおいて，攻撃経路ごとの円弧の角度は，5W 法によって抽出した脅威に対して，CRSS を用いてそのリスク値を算出した．保護資産はどの攻撃経路でも同じで，制御系 ECU の走行制御機能を保護資産とする．影響度は，可用性と完全性を対象に甚大とした．攻撃容易性区分については，上述したとおり本稿では安全性を重視するため，攻撃容易性区分の最高値を採用した．図 7 に示したとおり，「●」となっている監視箇所が各攻撃経路において監視項目として選定可能となっている．実際には，監視項目は複数の監視内容から成り立っているケースがある．たとえば，#E4-0-0 における#Ob1 では，車両運動制御 ECU の有線でのリプロ，あるいは車両運動制御 ECU の無線経由でのリプロ（OTA）による侵入活動が抽出されており，これらの両方に対して，影響として現れる痕跡を監視項目として選定しなければ，網羅的な監視にはならない．

また，本評価手法の特徴として，早期検知可能な監視項目は，アタックサーフェイスに近い円の外周側となる．円弧の角度を各攻撃経路のリスク値に応じて設定するため，リスクの高い脅威が発生する攻撃経路を監視する場合も円の面積が広くなる．これらを考慮すると，迅速性と脅威リスクを考慮した監視項目の有効性（Effectiveness）は，該当する監視項目の監視箇所（$\#\text{Ob}_j$）とその階層 r_j から算出される面積により評価できる．

$$\text{Effectiveness}(j) = \frac{1}{2}\theta(r_j^2 - r_{j-1}^2)$$

一方，網羅性を重視した場合，少なくとも各攻撃経路は必ず 1 つ以上の監視項目を突破するように監視項目が選定されていることが望ましい．しかしながら，監視項目が増加するとコストも増加するため，これらの関係はトレードオフである．

5. 評価および考察

本章では，上述した提案手法の有効性について評価するとともに，今後の課題について議論する．

5.1 評価

本稿における提案手法の評価として，まず，監視項目の網羅的な抽出について，JASO TP15002 の手法を用いた場合と比較する．また，提案手法はシステム設計者の意図に合わせて監視項目を選択できることを目指しているため，設計者による監視項目の選択に応じて，評価値が正しく推移できることを確認する．

(1) 抽出した監視項目の網羅性

JASO TP15002 は，表 3 で示したアタックサーフェイスを設定し，保護資産に対する脅威を抽出し，脅威に基づく対策としてセキュリティ機能コンポーネントが検討される．JASO TP15002 を用いた手法に対して，上記 4 章で示

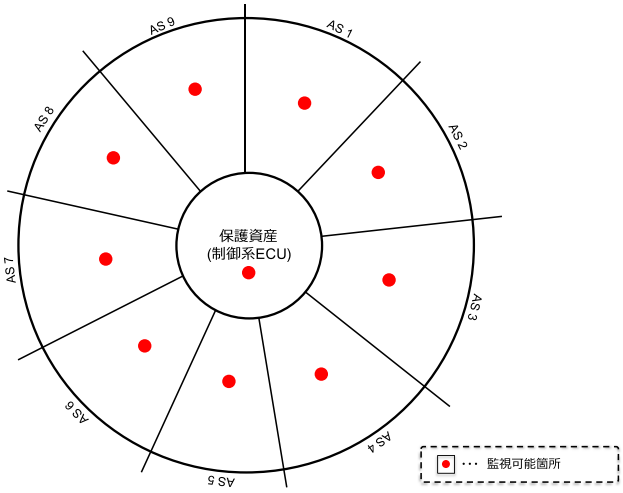

図 8 JASO TP15002 を用いた評価モデルの例
Fig. 8 Evaluation model based on JASO TP15002.

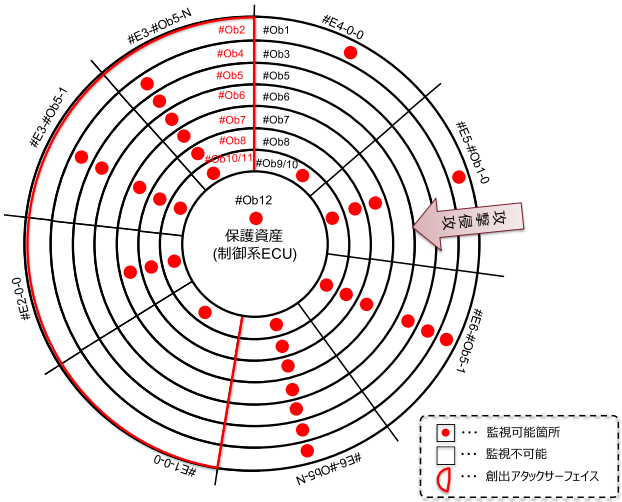

図 9 提案手法を用いた評価モデル
Fig. 9 Evaluation model based on proposal method.

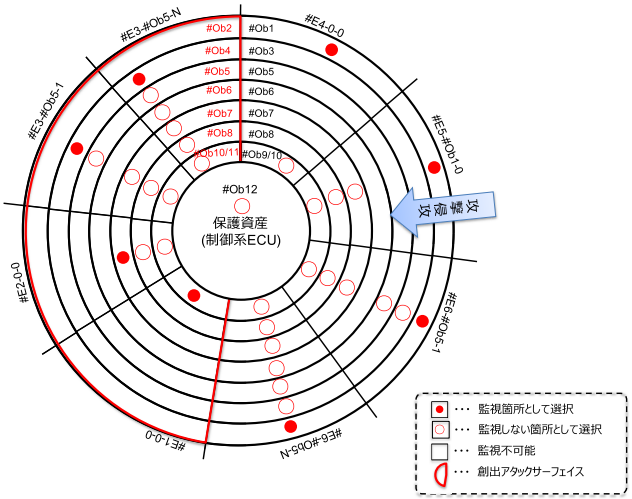

図 10 ケース 1
Fig. 10 Case 1.

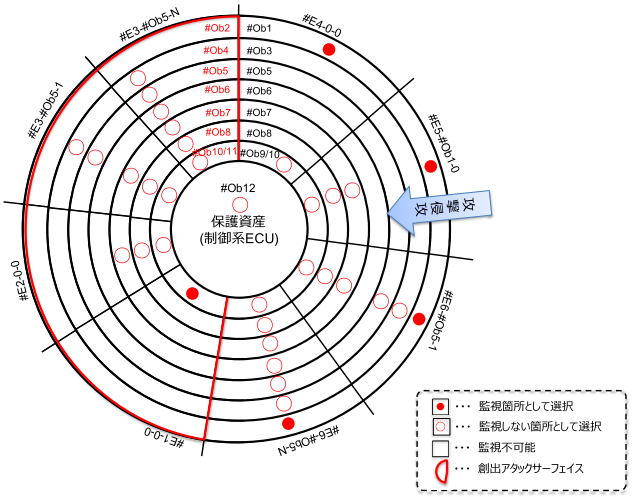

図 11 ケース 2
Fig. 11 Case 2.

した城塞防衛モデルに基づく評価モデルを考える．JASO TP15002 を用いた評価モデルは，表 3 で示したアタックサーフェイス（AS 1 から AS 9）を設定し，アタックサーフェイスから保護資産に対する攻撃を監視することになる（**図 8**）．図 8 に示すとおり，JASO TP 15002 を用いた場合，攻撃経路の抽象度が高くなってしまい，一見すると網羅的に監視できるように見えるが，表 6 や表 7 で示すとおり，同じアタックサーフェイスでも異なる攻撃経路を保護資産に対して攻撃を実行することが考えられるため，システム設計者は網羅的に監視できるかどうか判断できない．

一方，提案手法は**図 9** で示すとおり，表 6，表 7 で示した同じアタックサーフェイスでも異なる攻撃経路も考慮した評価モデルとして表すことができるとともに，攻撃プロセスにおけるどのタイミングでの検知が可能であるかを明示的に示すこともできる．

以上より，提案手法は従来手法と比較して，攻撃経路および攻撃プロセスの侵攻状況の観点で網羅的に監視項目を抽出できる．

(2) 監視項目の選択に応じた評価値の推移

本節では，図 7 で抽出した監視項目に対して，監視項目の選択に応じた 3 つのケースについて提案手法の評価値を比較する．

Case1（**図 10**）：

本ケースは，すべての攻撃経路において，最も外側に位置する監視可能箇所を監視項目として選択する．本ケースは，迅速性と網羅性を意識して選択するケースである．

Case2（**図 11**）：

本ケースは，上記 Case1 に加えて，リスク値の最も低い経路，すなわち上記 4.2 節で示した θ が最も低い値となった 3 つの経路（#E2-0-0，#E3-#Ob5-1，#E3-#Ob5-N）を監視項目から除外する．本ケースは，迅速性と網羅性に加えて，リスクもふまえて選択するケースである．なお，図 1 で示した対象システムに基づく θ の算出結果は，**表 9**

表 9 各攻撃経路における θ の値
Table 9 Value of θ in each attack path.

識別子	各経路における脅威のリスク最大値	同心円における円弧角度（θ）
#E1-0-0	6.6	0.3 π
#E2-0-0	5.8	0.2 π
#E3-#Ob5-1	5.3	0.2 π
#E3-#Ob5-N	5.3	0.2 π
#E4-0-0	6.6	0.3 π
#E5-#Ob1-0	6.6	0.3 π
#E6-#Ob5-1	6.2	0.3 π
#E6-#Ob5-N	6.2	0.3 π

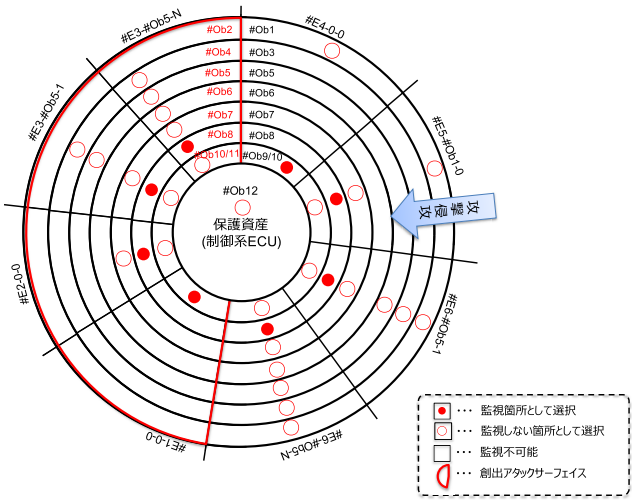

図 12 ケース 3
Fig. 12 Case 3.

に示すとおりであり，リスク値の算出には CRSS を用いた．本稿では，CRSS 方式を用いたが RSMA 方式を用いてもよく，文献 [4] における CRSS 方式と RSMA 方式では出力されるリスク値に多少の差異が見られるため，その影響は攻撃経路ごとの円弧の角度に反映されと予想するが，リスク値の算出手法の優劣は本稿では議論の対象外とする．

Case3（**図 12**）：

本ケースは，最終攻撃元装置（#Ob8），あるいは目的実行経路（#Ob9，#Ob10，#Ob11）を監視項目として選択する．本ケースは，水際での監視項目を選択するケースである．

以上の 3 つのケースに対して，上記 4.2 節で示した提案手法を用いた評価値を算出する．評価値の算出にあたり，本稿では，監視項目ごとに要するコストをすべて等しいものとした．すなわち，コストは監視項目の数に合わせて増加する．実際の開発においては監視項目ごとに実装する機能や必要となる HW 等に依存してコストが異なるため，その差も考慮に入れるべきである．評価結果を**表 10** に示す．

提案手法は，Rapidity と Coverage rate について，各

表 10 各ケースの評価結果
Table 10 Evaluation result of each case.

評価項目	Case1	Case2	Case3
Rapidity	6.5	4.3	2.8
Coverage rate	100%	60%	100%
Cost_t	36 個の監視項目に対応	28 個の監視項目に対応	2 個の監視項目に対応
Effectiveness の合計値	12 π	8.3 π	4.5 π

Case とも図面から視覚的に判断できるとおりの結果が評価できていることが分かる．Cost_t については，表 6 と表 7 を参照し，重複を取り除いた監視項目を対象として算出する．たとえば，表 7 の 4 つの攻撃経路において，#Ob1 に該当する監視項目の総数は 43 件だが，重複を取り除くと 27 件になる．結果として，Case3 が最もコスト負荷が少なく，必要な監視項目が 2 個で済むことが明確になった．一方，Case2 は Case1 よりも 3 つの攻撃経路を監視しないにもかかわらず，Rapidity，Coverage rate，Effectiveness の低下に対して，コスト負荷は下がっていないことも明らかになった．このように，提案手法はコスト負荷についても監視項目数に応じて算出できる．また，本評価では各監視項目の Effectiveness の合計値を算出した．Effectiveness の合計値が大きいほど迅速性と脅威リスクが考慮された監視項目を選択できていることを示す．結果として，Case1 が最も Effectiveness の合計値が大きくなることが明らかになった．

これらをふまえて，提示した 3 つのケースの場合，システム設計者は，コストを気にしない侵入検知を実現しようとした場合，Rapidity，Coverage rate，Effectiveness の合計値が優れた Case1 を選択し，コストの安い侵入検知を実現しようとした場合，Case3 を選択することが望ましいといえる．また，システム設計者は，リスク値の低い攻撃経路を許容して Case2 を選択しても，コスト負荷が Case1 より 20%程度下がるのに対して，その他の評価項目が 30%以上下がるため，Case1 を選択した方が費用対効果が高いといえる．

以上より，提案手法はシステム設計者が選択した監視項目に応じて，迅速性，網羅性およびコスト負荷等の観点で定量的に評価することにより，システム設計者は意図に合った監視項目を選択できる．

5.2 考察

本稿では，上記 2.4 節で設定した 2 つの課題に対して以下の解決策を提案した．これらの解決策により，提案手法は，セキュリティ設計段階で侵入検知向け脅威の監視項目を策定するとともに，策定した監視項目を定量的に評価できる見込みを得た．

【課題 (1)】 セキュリティ設計段階で脅威分析に基づいた網羅的な脅威の監視項目の抽出

提案手法は，JASO TP15002 をベースに侵入検知向けに対象とする脅威の定義として，対象とするシステムモデル，守るべき保護資産，前提条件を明確化した．さらに，サイバーキルチェーンモデルに基づいた攻撃侵入モデルを用いて，対象システムで対処すべき脅威の攻撃経路を全パターン抽出するとともに，痕跡として残る可能性のある監視項目を FT 分析によって網羅的に抽出する．これらにより，提案手法は従来手法と比較して，攻撃経路および攻撃プロセスの侵攻状況の観点で脅威の監視項目を網羅的に抽出できる見込みを得た．

【課題 (2)】 監視項目の迅速性，網羅性およびコスト影響の定量的評価

情報システムで用いられる IDS の監視機能の評価項目を参考に，迅速性，網羅性，コスト負荷，脅威リスクの考慮を評価項目として抽出した．提案手法は，城塞防衛モデルと攻撃侵入モデルを組み合わせ，監視項目をマッピングする同心円型の評価モデルを作成する．本稿では 3 つのケースに対して，提案する評価モデルを用いることにより，迅速性，網羅性，コスト影響を定量的に評価できることを示した．

一方，提案手法を用いた際の作業負荷および監視項目を設置するリソース環境の考慮については議論が必要である．まず，提案手法の作業負荷については，車載システムは，制御プラントのような社会インフラシステムや情報システムと比較して，システムの規模が小さい．また，提案手法はすべての保護資産に対して脅威を洗い出すのではなく，走行制御に関る保護資産に限定することで，対象とする車載システムにおいて抽出すべき脅威を絞ることができる．これらを考慮すると，セキュリティ設計段階での作業負荷の増加を抑えることもできると考える．提案手法は設計情報や前提等を確定すると，機械的に設計できることが期待できるため，ツール化による作業負荷の低減にも取り組んでいきたい．次に，リソース環境の考慮については，車載システムに搭載される ECU のリソースは Navi 等の一部の ECU を除いて潤沢ではない．監視項目を抽出できたとしても，ハードウェアの制約によって実装困難なケースも予想される．このことを考慮すると，リソース環境を考慮した監視項目の選定手法についても取り組んでいきたい．

6. おわりに

本稿では，セキュリティ設計段階で侵入検知に向けたセキュリティ脅威の監視項目を明らかにするために，脅威分析に基づいた網羅的な脅威の監視項目を抽出，抽出した監視項目の迅速性，網羅性およびコスト影響を定量的に評価する手法を提案した．提案手法は，JASO TP15002 に基づくセキュリティ設計において，攻撃侵入モデルを用いて対象システムで対処すべき脅威の攻撃経路を全パターン抽出，痕跡として残る可能性のある監視項目を FT 分析によって網羅的に抽出するとともに，城塞防衛モデルと攻撃侵入モデルを組み合わせることで，選定した監視項目の迅速性，網羅性，コスト負荷を定量的に評価できることを示した．

今後は，提案手法を実施する際の作業工数の削減に加えて，ECU ごとのリソースを考慮した監視項目の選定および妥当性評価を検討することにより，提案手法の有用性をさらに検証していく．

参考文献

[1] 独立行政法人情報処理推進機構：2010 年度制御システムの情報セキュリティ動向に関する調査報告，独立行政法人情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000014121.pdf⟩（参照 2017-11-27）．

[2] 独立行政法人情報処理推進機構：情報家電におけるセキュリティ対策検討報告，独立行政法人情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000014114.pdf⟩（参照 2017-11-27）．

[3] 独立行政法人情報処理推進機構：2012 年度自動車の情報セキュリティ動向に関する調査，独立行政法人情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000027274.pdf⟩（参照 2017-11-27）．

[4] 一般社団法人重要生活機器連携セキュリティ協議会：分野別セキュリティガイドライン車載器編 (2016).

[5] SBD：コネクテッドカーガイド – 法規制編，SBD（オンライン），入手先 ⟨http://www.sbdjapan.co.jp/wp-content/connected_car/pdfs/528-153_IB_J.pdf⟩（参照 2017-11-27）．

[6] UNECE: UN Task Force on Cyber security and OTA issues, UNECE (online), available from ⟨https://wiki.unece.org/pages/viewpage.action?pageId=40829521⟩ (accessed 2017-11-27).

[7] ISO: ISO and SAE International announce agreement to develop technical standards for road vehicles and intelligent vehicle systems, ISO (online), available from ⟨https://www.iso.org/news/2016/11/Ref2137.html⟩ (accessed 2018-04-04).

[8] Auto-ISAC: Automotive Cyber security Best Practices, Auto-ISAC (online), available from ⟨https://www.automotiveisac.com/best-practices⟩ (accessed 2017-11-27).

[9] SAE: *J3061-Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, SAE (2016).

[10] NHTSA: Cybersecurity Best Practices for Modern Vehicles, NHTSA (online), available from ⟨https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf⟩ (accessed 2017-11-27).

[11] U.S. House of Representatives: Highly automated vehicle testing and deployment act of 2017, U.S. House of Representatives (online), available from ⟨http://docs.house.gov/meetings/IF/IF17/20170719/106309/BILLS-115pih-HighlyAutomatedVehicleTesti-U2.pdf⟩ (accessed 2017-11-27).

[12] 中井綱人，山口晃由，清水孝一，小林信博，秦 康祐，佐々木翼，澤田賢治：ライフサイクルに応じた産業用制御システム向けホワイトリスト型侵入検知システムのモデル化とシミュレーション評価，暗号と情報セキュリティシンポジウム 2017 予稿集 (2017).

[13] SAE: NEW NHTSA CYBERSECURITY RESEARCH

PROJECTS: ANOMALY DETECTION SYSTEMS, CYBERSECURITY CONSIDERATIONS FOR HEAVY VEHICLES, AND CYBERSECURITY OF FIRMWARE UPDATES, SAE (online), available from ⟨https://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/SAE/2016/SAE%20G_I_Workshop%20-%20UMTRI%20Carter.pdf⟩ (accessed 2018-04-04).
[14] ESCRYPT: Automotive Intrusion Detection and Prevention System (IDPS) Continuous Protection as part of the Automotive Security Lifecycle, ESCRYPT (online), available from ⟨https://www.concarexpo.com/fileadmin/Redaktion/Dokumente/Praesentationen_ConCarForum_2017/24_escrypt_GmbH_-_Jan_Holle.pdf⟩ (accessed 2018-04-04).
[15] 一般財団法人日本自動車研究所：V2X 等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト，一般財団法人日本自動車研究所（オンライン），入手先 ⟨http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf⟩（参照 2017-11-27）.
[16] 日立オートモティブシステムズ株式会社：ニュースリリース，日立オートモティブシステムズ株式会社（オンライン），入手先 ⟨http://www.hitachi.co.jp/New/cnews/month/2017/10/1024a.pdf⟩（参照 2018-04-04）.
[17] 鳥崎唯之，加藤　遼，芳賀智之，寺澤弘泰，今本吉治，松島秀樹：CAN-Ethernet 混在車載ネットワークにおけるセキュリティ対策の検討と提案，暗号と情報セキュリティシンポジウム 2018 予稿集 (2018).
[18] 公益社団法人自動車技術会：自動車の情報セキュリティ分析ガイド，JASO TP-15002 (2015).
[19] ISO: Information technology – security techniques – evaluation criteria for it security – part 1: Introduction and general model, ISO (2005).
[20] ISO: Information technology – security techniques – evaluation criteria for it security – part 2: Security functional requirements, ISO (2005).
[21] ISO: Information technology – security techniques – evaluation criteria for it security – part 3: Security assurance requirements, ISO (2005).
[22] Schneier, B.: Attack trees: Modeling security threats, Dr. Dobb's Journal of Software, Tools 24, pp.21–29 (1999).
[23] Schneier, B.: Attack Trees, B.Schneier (online), available from ⟨http://tnlandforms.us/cs494-cns01/attacktrees.pdf⟩ (accessed 2017-11-27).
[24] 萱島　信：IoT システム向けセキュリティ要件定義手法の提案，電子情報通信学会論文誌 A，Vol.J99-A, No.2, pp.74–82 (2016).
[25] EVITA: Deliverable D2.1: Specification and evaluation of e-security relevant use cases (2009).
[26] 独立行政法人情報処理推進機構：共通脆弱性評価システム CVSS 概説，独立行政法人情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/security/vuln/CVSS.html⟩（参照 2017-11-27）.
[27] JPCERT/CC：高度サイバー攻撃への対処におけるログの活用と分析方法，JPCERT/CC（オンライン），入手先 ⟨https://www.jpcert.or.jp/research/apt-loganalysis.html⟩（参照 2017-11-27）.
[28] Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. and Payne, B.D.: Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices, *ACM Computing Surveys* (*CSUR*), Vol.48, No.1, pp.1–41 (2015).
[29] Boggs, N., Du, S. and Stolfo, S.J.: Measuring Drive-by Download Defense in Depth. RAID 2014, Research in Attacks, *Intrusions and Defenses*, Vol.8688, pp.172–191 (2014).

森田 伸義 （正会員）

2009 年創価大学大学院工学研究科情報システム工学専攻修士課程修了．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）にて，モバイル端末連携技術，自動車セキュリティ技術等の研究・開発に従事．

川口 信隆 （正会員）

2008 年慶應義塾大学大学院理工学研究科後期博士課程修了．博士（工学）．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）にてサイバーセキュリティおよびマルウェア対策の研究開発に従事．2008 年 IPSJ 論文船井若手奨励賞，2012 年 DICOMO シンポジウム優秀論文賞，2016 年辻井重男セキュリティ論文賞特別賞．情報処理学会 CSEC 研究会運営委員（2013～2017 年），IEICE 論文編集委員（2018 年～）．CISSP，CEH，IEEE，ACM 各会員．

井手口 恒太

2006 年東京大学大学院理学系研究科博士課程修了．博士（理学）．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）にて情報セキュリティおよび暗号技術の研究開発に従事．

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）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）．