情報処理学会論文誌 Vol.58 No.12 1943–1953 (Dec. 2017)

脅威モデリング連携型アタックテストによる車載ネットワーク脅威分析手法

西尾 泰彦[1,a)] 城間 政司[1] 井上 博之[1,2]

受付日 2017年2月28日, 採録日 2017年9月5日

概要：自動車のハッキング事例が国内外で報告される等，車載システムの情報セキュリティの確保が重要な課題となっている．その課題の解決のためには，車載システムに存在する脅威を明らかにし，システムの堅牢性を検証するセキュリティテストが必要となってくる．セキュリティテストでは，脅威分析から導出したアタックサーフェスに基づいたテストが行われることが多く，その作業要素には脅威モデリングとアタックテストという要素が存在する．しかしながら，脅威モデリングとアタックテストは一連の流れで行われるにもかかわらず，従来研究では独立して議論されるケースが見受けられる．本論文では，脅威モデリングとアタックテストを連携させた脅威モデリング連携型アタックテストを提案し，車載システム，特に車載ネットワークの脅威を分析する手法について述べる．本手法の利用ケースは，自動車メーカからアタックテストを依頼された技術者が，依頼元に車載ネットワークの脅威をレポートするまでを想定しており，依頼元メーカにとって提案手法が有効であることを示す．有効性の検証は，一般に行われる脅威分析からアタックテストまでの手順の流れの中で，どの手順に有効かという点で示す．また，技術者が脅威モデリングを行うことなくアタックテストを実施した場合と比較した考察も同時に行う．最終的に，提案手法を用いることで依頼元メーカにとってより有用なレポートを提供できること，脅威モデリングを行わない技術者のアタックテスト結果と同等もしくはそれ以上のアタックテストの効率を維持できること，加えて技術者同士で脅威を共有できるようなテスト手法となることを示す．

キーワード：脅威モデリング，アタックテスト，車載ネットワーク，CAN

An Automotive Network Threat Analysis Method Using Attack Testing Coupled with Threat Modeling

Yasuhiko Nishio[1,a)] Tadashi Shiroma[1] Hiroyuki Inoue[1,2]

Received: February 28, 2017, Accepted: September 5, 2017

Abstract: Recently, several incidents of car hacking have been reported worldwide. Therefore, it is important to ensure automotive system security. To ensure the integrity of these systems, we need to identify the system threats and to examine security testing to verify the system's robustness. Testing based on an attack surface derived from a threat analysis is generally used in security testing process. This process is characterized by two factors, threat modeling and attack testing. A series of these factors is employed in security testing; however, in past studies, the survey of both threat modeling and attack testing is independent. In this paper, we propose an attack testing method coupled with threat modeling and show the application of our method in automotive network threat analysis. The use case of our method is in an attack testing phase examined by attack testers. Further, in this case, they have to report the attack testing results. We show the effectiveness of our method in the phases between threat analysis and attack testing. Furthermore, we evaluate our method quantitatively using a new metric called attack testing efficiency. Finally, we show that attack testers can provide stakeholders with useful reports about automotive network threats by using our method, and they can perform attack testing as efficiently as an expert attack tester. We can share our results with any attack testing engineers.

Keywords: threat modeling, attack test, automotive network, CAN

[1] 重要生活機器連携セキュリティ協議会研究開発センター
Connected Consumer Device Security Council (CCDS), Naha, Okinawa 900–0005, Japan
[2] 広島市立大学大学院情報科学研究科
Graduate School of Information Sciences, Hiroshima City University, Hiroshima, 731–3194, Japan
[a)] yasuhiko.nishio@ccds.or.jp

1. はじめに

Jeep 等の自動車のハッキング事例が国内外で報告され，自動車における情報セキュリティが無視できなくなっている [1]．自動車の情報セキュリティ上の脅威を明らかにし，

© 2017 Information Processing Society of Japan

実証するテストの重要性が高まり，セキュリティ研究者もこのような取り組みを行っている [2], [3]．これらの取り組みでは，効果的なセキュリティテスト，脅威分析からその内容に沿ったアタックテスト，リスク評価といった内容が中心である．しかし，脅威分析とアタックテストに関しては，一連の流れで行われるにもかかわらず，従来研究では独立して議論されるケースが見受けられる．文献 [4], [5] では，脅威モデリングに関して深く考察されているが，アタックテストや攻撃データまでは十分に述べていない．一方，アタックテストの既存研究においてはツールの使い方やテストの手順は解説されているが，どのような脅威や脆弱性をテストすればよいのかという点については言及されていない [6], [7]．Bekrar らの研究 [8] においても，脆弱性パターンという言葉を用いているが，脅威を明確にしたアタックテストを課題にあげており，脅威モデリングとアタックテストの間において関連付けが課題となっている状態である．脅威分析とアタックテストの関連付けが必要な例としては，アタックテスト技術者が，外部の自動車メーカから攻撃者視点でのテストとレポートを要求されるケースがあげられる．脅威モデルのレポートでは脅威の可視化が可能であり，攻撃データのレポートでは脅威の実証が可能である．しかし，脅威モデルのみのレポートでは図としてのイメージに閉じてしまうという欠点があり，攻撃データのみのレポートでは脅威を視覚的にイメージすることが困難であるという欠点がある．脅威モデルと攻撃データの両方をレポートする際においても，その脅威モデルと攻撃データの関連性を明確にしなければならない．このため，自動車のセキュリティテストにおいても，脅威分析とアタックテストの関連付け，つまり連携という課題が存在していると考えられる．

本論文では，上記課題を解決するための脅威モデリングとアタックテストを連携させた脅威モデリング連携型アタックテストを提案する．具体的には，脅威モデリングを XML 等のテキストファイルに変換可能なツールで記述し，XML ファイルを既存のアタック用のツールで使えるデータに変換するまでを手順化する．これにより，自動車メーカが脅威モデルから攻撃データを生成し，アタックテスト技術者の見つけた脅威を容易に再現およびレポートすることに役立てることが可能となる．さらに，提案手法の有効性を評価するために，依頼元の要件に沿った成果を得ることができるか，脅威モデリングを行わない他のアタックテスト技術者が行った場合と同等，もしくはそれ以上のアタックテストの効率を提供できるかの比較評価を行う．

本論文の構成は以下のとおりである．2 章では，セキュリティテスト，脅威モデリングおよびアタックテストに関する既存研究とそれらの問題点について述べる．3 章では，その課題を解決するための脅威モデリング連携型アタックテストを提案する．そして，4 章では，提案手法を車載ネットワークのアタックテストへ適用することについて述べる．5 章では，提案手法を車載ネットワークのアタックテストに適用した場合の評価方法と，評価結果について考察する．最後にまとめと今後の課題とする．

2. 関連研究

2.1 自動車セキュリティのテストに関する既存研究

自動車セキュリティの分野では，Bayer らが紹介するセキュリティテストの枠組みが存在している [9]．その中では自動車セキュリティテストの中でのペネトレーションテストやファジングテストの位置づけを述べている．この内容に鑑み，文献 [2] では効率的な評価手法や評価基準とその問題点について議論している．文献 [3] では，脅威分析およびリスクアセスメントを実施し，セキュリティ対策方針をサイバーセキュリティコンセプトとしてまとめる重要性を述べている．以上のような自動車の情報セキュリティに関する取り組みが，セキュリティ研究者の間で行われている．

2.2 脅威モデリングの既存研究

脅威モデリングの研究の中でも具体的な事例を取り上げた研究には，Myagmer らの手法が存在する [10]．Myagmer らの研究では，ソフトウェア無線機とネットワーク製品の両方で，脅威モデリングのためのベストプラクティスを示している．また，脅威モデリングからセキュリティ要求を詳細化し，そこからセキュリティメカニズムを開発するうえで DFD（Data Flow Diagram）を用いた脅威モデルを構築している．DFD に基づいた脅威モデリングはツール開発や文献化も行われている方法である [5], [11]．

2.3 アタックテストの既存研究

脆弱性を摘出するテストとしては，ペネトレーションテストやファジングテスト等のアタックテストが認知されている [6], [7]．これらのテストは，脆弱性や安全性を脅かす入力データを与え，システムの脅威を識別するテストである．アタックテストにおける攻撃データは通常，ツールが持つ機能や現場で所有するノウハウにより生成される．しかし，未知の脆弱性を検出するためには，システムの脅威や脆弱性を見据え，経験と勘に基づく思考プロセスを必要とする．そこで Bekrar らは，脆弱性のパターンという定義を起点としたテストケース生成に取り組んでいる [8]．このように，脅威モデルや脆弱性のパターンを起点としたアタックテストの研究も行われている．

2.4 脅威モデリングとアタックテストの問題点

脅威モデリングからアタックテストに移行するうえでは，脅威モデリングとアタックテストが連携されていないという問題が存在している．この問題を解決するためには，脅

© 2017 Information Processing Society of Japan

威モデリングとアタックテストを連携させる手順が必要となる．脅威モデリングから攻撃シナリオ，攻撃データ生成という点にフォーカスすると，形式手法によるモデルからのデータ生成に関しては文献 [12] のような研究が報告されている．しかし，文献 [4], [5] のような脅威分析から導出したアタックサーフェスに基づいたテストでは，DFD のようなグラフィカルなモデルが用いられており，これらのモデルとアタックテストの連携に関しては十分議論されていない．この問題を解決するため，本研究では DFD 等の脅威モデリングとアタックテストの連携方法を提案する．

3. 脅威モデリング連携型アタックテスト

2.4 節の問題を解決する脅威モデリング連携型アタックテストを提案する．具体的には，**図 1** のように以下の流れに沿った手順を提案する．以降，図 1 の (1)〜(4) に沿い，DFD による脅威モデリング，脅威モデルの XML 変換，XML 解析結果から攻撃データを抽出，攻撃データの出力，以上の順で説明する．

3.1 DFD による脅威モデリング

DFD による脅威モデリングでシステムの脅威の記述を行う．DFD の記述には DFD のノードに攻撃データ等の文字列を格納できるプロパティ機能が利用可能なツールを用いる．実際には**図 2** のように段階的な詳細化により，DFD 脅威モデルを作成する．この段階的な詳細化は，文献 [4], [15] 等で行われているものを参考にして行う．

Level 1：鳥瞰的視点での脅威モデル

対象システムを図 2 の上段の図のように，1 つのプロセスノードで表す．そして，対象システムと関係する外部エンティティを矢印で結んだ図を作成する．本論文ではこの図を Level 1 と呼ぶ．Level 1 では攻撃者とアセットと呼ばれる 2 つの外部エンティティを持つ．アセットとは，攻撃者の攻撃対象物となる資産，機能，ファイル等を指す．攻撃者は対象システムに攻撃データを送る．対象システムからアセットを指す矢印は脅威の情報を示す．点線の四角はトラストバウンダリを示す．トラストバウンダリとは，対象システムにおいて脆弱性が含まれる可能性がある部分とそうでない部分の境界を表す．以降のモデルにおいても同様である．

Level 2：対象プロセスを詳細化した脅威モデル

次に Level 1 の対象システムのプロセスを詳細化した図を図 2 の中段のように作成する．本論文ではこの図を Level 2 と呼ぶ．Level 1 の対象システムを，エントリポイント，機能 1〜n の処理のプロセスに分解する．ここで n はエントリポイントとつながるプロセスの数とする．エントリポイントから機能 1 への矢印は，機能 1 への攻撃データが送られることを表す．機能 2〜n の処理のプロセスへの矢印に対しても同様である．そして，機能 1 の処理からアセットに対し，脅威の情報を示す．機能 2〜n の処理からアセットに対しても同様である．

Level 3：アタックサーフェスレベルの脅威モデル

Level 2 の機能 1〜n の処理のプロセスをより詳細化した図を図 2 の下段のように作成する．本論文ではこの図を Level 3 と呼ぶ．Level 3 では，脅威やアタックサーフェスを明確にするのに十分な粒度であれば，何階層に分解するかは自由とする．さらに各々のプロセスに攻撃データを格納する領域を，Level 3 の図の右の吹き出しのように設ける．たとえば，機能 1-1 の処理のプロセスにおいてモデリングツールが持つプロパティ機能等で名前と値の属性を入力する．図 2 の Level 3 の吹き出し部分には，機能 1-1 の処理に対して入力されるデータ，たとえばアタックツールのコマンドや引数等が入り，タグ付き値のフィールドに示した値は攻撃対象の ID と攻撃用コマンドへ渡すパラメータ，コマンドの名前および引数の例である．なお，これらの名前と値は，4.2 節の適用例のような検証過程で決定される．このようにして Level 3 の末端のプロセスへの攻撃データの格納が可能となる．

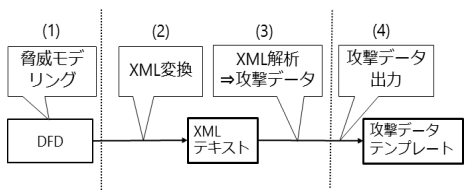

図 1 脅威モデリング連携型アタックテストの概要
Fig. 1 Conceptual diagram of the proposed method.

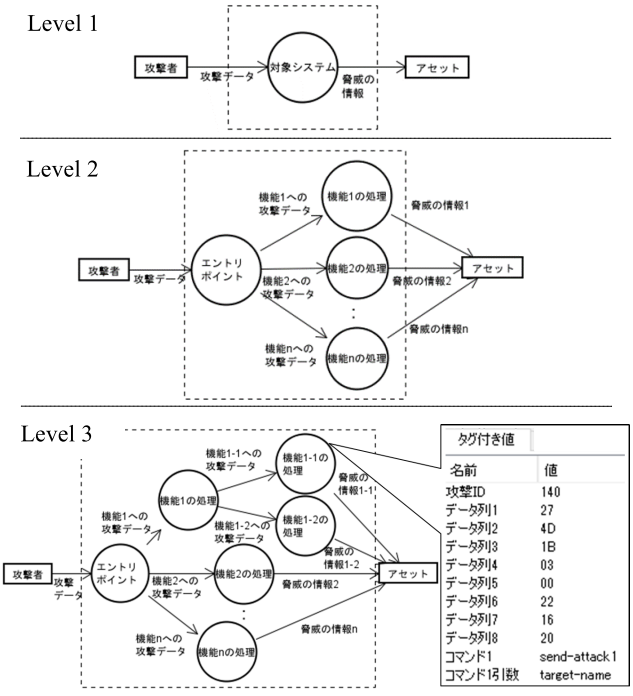

図 2 提案手法の DFD モデル化
Fig. 2 DFD modeling of the proposed method.

© 2017 Information Processing Society of Japan

3.2 脅威モデルの XML 変換

3.1 節で記述した Level 3 の脅威モデルを XML テキストファイルに変換する．この操作は 3.1 節で述べたモデリングツールが持つ XML ファイル出力機能等で可能である．DFD は文献 [5], [11] のツール等で記述される．これらのモデルから攻撃データを生成するうえでは，DFD がグラフィカルなモデルかつ準形式言語であることに注意しなければならない．DFD モデルでは，攻撃データをアタックテストで使用可能なファイルフォーマットへドラッグ，ドロップ，コピー貼り付け等，当該ファイルのフォーマットへ入力できるデータ構造になっていない．このため構造化された XML ファイルという加工しやすい形式にすることで，攻撃データへの変換を可能にしている．そして，構造化されたファイルのどこを読み取ればよいか等の解析手順を整備することで，アタックテストで使用可能なファイルフォーマットに攻撃データを変換することが可能となる．

3.3 XML 解析結果から攻撃データの抽出

変換した XML ファイルを解析し，攻撃データを抽出する．攻撃データの抽出は XPath 等の XML ドキュメントの構文解析機能により行う．たとえば，Level 3 モデルの XML ファイルが**図 3** の XML ドキュメント構成の場合，5 行目青字の機能 1-1 の処理に対し，6 行目の赤字で記載された攻撃用のコマンドである send-attack1，および 8〜16 行目の赤字で示したデータを抽出したい場合は，XPath 等で当該データの抽出を行う．これにより，機能 1-1 の処理の例で格納されている攻撃データを抽出することが可能である．

3.4 抽出したデータのアタックツール用データへの変換と実行

最後に図 3 の下部のように，実際のアタックテスト用のフォーマットで出力する．たとえば，アタックツールへの入力がテキストファイル形式の場合，そのファイル形式で 3.3 節の抽出結果を書き出す．アタックツールがコマンドベースのツールでコマンド名，ターゲット引数，攻撃 ID，攻撃データという入力をとるケースでは，send-attack1 target-name 140 27 40 18 03 00 22 16 20 となる．

以上の 3.1 から 3.4 節までの手順により，脅威モデルから攻撃データを生成することが可能となる．

```
01 <XML.content>
02    <UML:Model>
03       <XML.extension>
04          <UML>
05             <UML name="機能 1-1 の処理">
06                <UML tag="コマンド 1" value="send-attack1" />
07                <UML tag="コマンド 1 引数" value="target-name" />
08                <UML tag="攻撃 ID" value="140" />
09                <UML tag="データ列 1" value="27" />
10                <UML tag="データ列 2" value="4D" />
11                <UML tag="データ列 3" value="1B" />
12                <UML tag="データ列 4" value="03" />
13                <UML tag="データ列 5" value="00" />
14                <UML tag="データ列 6" value="22" />
15                <UML tag="データ列 7" value="16" />
16                <UML tag="データ列 8" value="20" />
17             </UML>
18          </UML>
19       </XML.extension>
20    </UML:Model>
21 </XML.content>
```

```
攻撃データ仕様テンプレート
  send-attack1 target-name 140 27 4D 1B 03 00 22 16 20
```

図 3 XML 変換と攻撃データ生成の例

Fig. 3 Example of XML data conversion and attack data generation.

4. 提案手法の車載ネットワーク脅威への適用

車載ネットワークは多くの ECU（Electronic Control Unit）が接続する複雑なネットワークであり，その脅威の特定とそれを再現する作業は経験と勘に依存し困難をきわめる．このため提案手法を以下に示す車載ネットワーク検証作業に適用し，提案手法に沿って作業することで効率的な脅威と攻撃データの導出，およびアタックテストのレポートの成果物にできることを示す．本論文では，車載ネットワークへの入り口として自己診断端子（以下，OBD2 ポート）を使用する．OBD2 ポートを用いる理由は，同ポートは自動車への搭載が世界各国で義務付けられたことにより義務化以降は標準搭載されているほか，車内に接続用ポートが配備されており検証作業をスムーズに行えるためである．車載ネットワークへの入り口は OBD2 ポートのほかに，各種 ECU，カーナビをはじめとするインフォテインメント機器等が考えられるが，内部の CAN バスに直結するということでは，OBD2 ポートは単なる接点にすぎない．よって，提案手法では，図 2 のエントリポイントのプロセスにこれらの機器のプロセスを置き換えることで，車載ネットワークに直接つながる他の機器を入り口とした場合にも適用可能である．

4.1 車載ネットワークのセキュリティ検証環境

(1) 想定するケース

自動車メーカが外部のテスト技術者にアタックテストを依頼するケースを想定する．自動車メーカは，攻撃者の視点での脅威の洗い出しと，特定した脅威に関するレポートを外部のアタックテスト技術者に対して要求する．なお，車載ネットワークとしては最も一般的な CAN（Controller Area Network）を想定し，ECU どうしが CAN バスを介して接続されているものとする．

(2) 検証目的

CAN バスへの攻撃データの注入によってどのような脅威が存在するかを，ブラックボックステスト方式のペネトレーションテストで確認することを目的とする．

(3) 検証環境

高度な運転支援機能（ADAS）を搭載した自動車の車載ネットワークを想定する．CAN バス上の CAN メッセージを介して，追従走行機能，レーンキープ機能等の自動運

© 2017 Information Processing Society of Japan

転補助システム，エンジン，ギア，アクセル，ハンドル，ブレーキ，計器パネルが制御されるシステムとする．また，OBD2 ポートが車内に設置されているものとする．

実際の車の検証作業はテスト実施者と補助者，モデル作成者という役割を設ける．理由は，車の検証作業においては，CAN メッセージ解析を含むペネトレーションテスト，自動車の操作，脅威分析とそのモデリングを行うためである．

(4) 必要なスキルとツール

テストに最低限必要なスキルとして，CAN に関する知識，CAN バス，CAN ID とペイロードに関する知識，CAN アナライザに関する知識を想定する．必要なツールとしては，ノート PC，CAN アナライザ，CAN メッセージ解析記録のためのワークシートを想定する．

4.2 車載ネットワークの検証の流れ

自動車メーカからの依頼を受けて行う車載ネットワークのアタックテストの手順について述べる．ここでは通常の車載ネットワーク検証と提案手法を用いた場合の 2 点に分けて説明する．なお，本節 (2) 内の太字は，提案手法を用いた場合に通常の車載ネットワーク検証と異なる部分を表す．

(1) 脅威モデリングを用いない場合の検証の流れ

以下に示す要領で CAN メッセージの解析を行う．

① 補助者が，エンジン，ギア，アクセル，ハンドル，ブレーキ，計器パネルを操作する．
② テスト実施者が，CAN アナライザのモニタに反応する CAN メッセージを記録する．
③ モニタリングして見つけた CAN メッセージをテスト実施者が CAN バスに対して注入する．
④ 上記の作業の繰返しから，脅威になりうるメッセージを特定し，レポートを作成する．

(2) 提案手法を用いた場合の検証の流れ

① 3.1 節の方法により脅威モデリングを行う．脅威モデリングは，モデル作成者が行うとする．モデル作成は別の工程のため，実施者や補助者が担ってもよい．なお，脅威モデリングの方法は 4.3 節で述べる．
② 作成した Level 3 の脅威モデルから導き出したアタックサーフェスを参考に，補助者がエンジン，ギア，アクセル，ハンドル，ブレーキ，計器パネルを操作する．
③ テスト実施者が CAN アナライザのモニタに反応する CAN メッセージを記録する．
④ モニタリングして見つけた CAN メッセージをテスト実施者が CAN バスに対して注入する．**モニタに反応があった場合，さらに注入した攻撃データを 3.1 節の Level 3 のモデルの記述に従い格納する．この作業は 4.4 節で述べる．**
⑤ 上記の作業の繰返しから，脅威になりうるメッセージを特定し，レポートを作成する．
⑥ レポート作成においては，3.2 から 3.4 節の手順に沿って攻撃データの生成を行い，生成された攻撃データにより脅威を実証できる脅威モデルをレポートに添える．この作業は 4.4 節で述べる．

4.3 車載ネットワークへの脅威モデリング連携型アタックテスト

Level 1 の車載ネットワーク脅威モデル

対象システムである車載ネットワークを 1 つのプロセスで表現する．車載ネットワークと関係する外部エンティティは，攻撃者および自動車の機能の 2 つとする．この例でのアセットは，自動車の機能とする．自動車の機能とは，エンジンやギア，ハンドル，計器パネル，自動運転機能等を指す．Level 1 の図については，3 章で例示した図 2 の Level 1 とほぼ同じ構成のため割愛する．

Level 2 の車載ネットワーク脅威モデル

Level 1 の車載ネットワークのプロセスを**図 4** のように 10 個のプロセスに分解する．図 4 では，攻撃者が CAN アナライザのコマンドとデータを不正な ECU の処理のプロセスを介し，CAN メッセージ群をエントリポイントに送る．エントリポイントの処理は，OBD2 ポートの処理プロセスとする．理由は OBD2 ポートに解析用の ECU を接続することで，車両診断だけでなく，車載ネットワークにつながる ECU への CAN メッセージの送信も行えるためである．エントリポイントであることを示すために，当該プロセスに EP という記号を与える．そして，OBD2 ポートの処理から CAN メッセージ群を侵入させ，車載ネットワークの処理を介し，車載ネットワークを構成する 7 つの ECU の処理を示すプロセスに侵入する．7 つの ECU の処理を示すプロセスは，攻撃者の視点で図 4 の車載ネットワークの処理から矢印で示される 7 つのプロセスに分解した．これにより，自動車の機能というアセットに対し，不正な CAN メッセージが送られることで予期せぬ脅威が生ずる仕組み

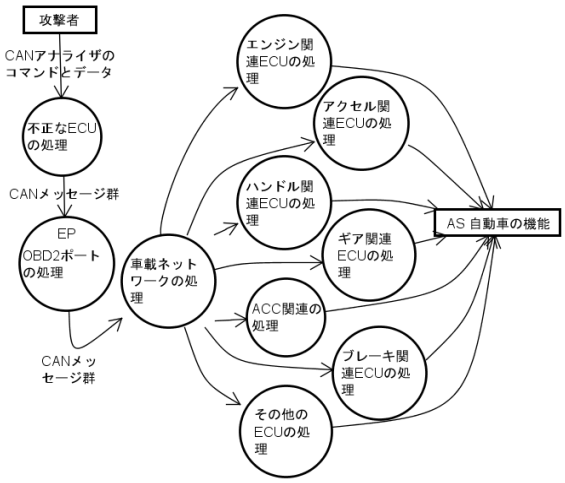

図 4 Level 2 なりすましと DoS 脅威
Fig. 4 Spoofing and denial of service threat of Level 2.

© 2017 Information Processing Society of Japan

を表現することが可能となる．アセットを示すため，外部エンティティである自動車の機能には AS という記号を付与する．EP および AS の意味は，以降の図も同様とする．

Level 3 の車載ネットワーク脅威モデル

図 5 で，Level 2 の車載ネットワークの処理から分岐する 7 つの ECU の処理をさらに細かい粒度に分解する．たとえば，エンジン関連 ECU の処理のプロセスは，エンジンと連動するプロセスであるエンジン回転計等のプロセスに分解する．アクセル関連 ECU の処理等，残りの 6 つのプロセスについても同様に分解する．そして，分解した処理のプロセスごとに STRIDE 分析 [4] で想定される脅威を分析する．図 5 では，**表 1** の STRIDE 分析で脅威の可能性がある ECU の処理のみ Level 2 から詳細化した．図 5 では，攻撃者が CAN アナライザ等でコマンドとデータを悪用し，不正な ECU を用いて OBD2 ポートに攻撃用の CAN メッセージを送るメカニズムを示している．

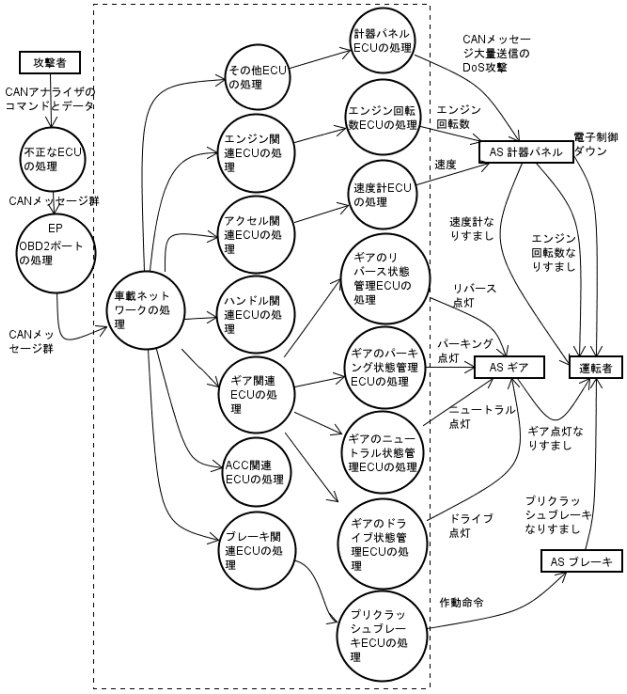

図 5 Level 3 なりすましと DoS 脅威

Fig. 5 Spoofing and denial of service threat of Level 3.

表 1 STRIDE 分析によって洗い出された脅威一覧

Table 1 Records of threats categorized with STRIDE.

分析する処理	STRIDE カテゴリ該否						想定される脅威
	S	T	R	I	D	E	
計器パネル ECU の処理	○	×	×	×	○	×	計器パネルがなりすまされる．大量のデータ送信でダウンする．
エンジン回転数 ECU の処理	○	×	×	×	×	×	エンジン回転計の表示がなりすまされる．
速度計 ECU の処理	○	×	×	×	×	×	速度計の表示がなりすまされる．
ギアのリバース状態管理 ECU の処理	○	×	×	×	×	×	バックしてないのにギアのリバースの表示がなりすまされる．
ギアのパーキング状態管理 ECU の処理	○	×	×	×	×	×	駐車してないのにギアのパーキングの表示がなりすまされる．
ギアのニュートラル状態管理 ECU の処理	○	×	×	×	×	×	ギアのニュートラルの表示がなりすまされる．
ギアのドライブ状態管理 ECU の処理	○	×	×	×	×	×	走行中でないのにギアのドライブの表示がなりすまされる．
ブリクラッシュブレーキ ECU の処理	○	×	×	×	×	×	走行中に予期せぬブリクラッシュブレーキがなりすまされる．

4.4 脅威モデリングからの攻撃データの導出

まず，4.3 節による脅威モデリングを参考にした CAN メッセージ解析を行う．そして，その解析結果を 3.1 節の Level 3 の攻撃データの格納処理にならい，攻撃データをセットする．そして，3.2 から 3.4 節で述べた方法で攻撃データとなる CAN メッセージの生成を行う．**図 6** で，3.2 から 3.4 節の手順に沿い，攻撃データを CAN アナライザに入力する CSV 形式に変換する例を示す．変換した XML ファイルにおいて，速度計 ECU，ギアのリバース状態管理 ECU，プリクラッシュブレーキ制御 ECU に関する攻撃データの該当箇所を例にした抜粋を図 6 の上部に示す．この XML ドキュメント構成で 1，9，21 行目の青字で表した対象へ攻撃する CAN メッセージとして，2，10，22 行目の赤字で記載した CAN ID と，3〜6，11〜18，23〜30 行目の赤字で記載したペイロードに該当する 8 バイトの値を抽出したい場合は，3.3 節の手順同様，XPath 等を用いた XML 解析で攻撃データの抽出が可能となる．これにより，速度計 ECU の処理，ギアのリバース状態管理 ECU の処理，プリクラッシュブレーキ制御 ECU の処理の各プロセ

```
⋮
01 <UML:SubactivityState name="Speed_meter" xmi.id="1n88-4a">
02        <UML:TaggedValue xmi.id="1n8b" value="0D1" tag="CAN ID" />
03        <UML:TaggedValue xmi.id="1n8c-4a" value="6F" tag="B1" />
04        <UML:TaggedValue xmi.id="1n8d-4a" value="02" tag="B2" />
05        <UML:TaggedValue xmi.id="1n8e-4a" value="00" tag="B3" />
06        <UML:TaggedValue xmi.id="1n8f-4a" value="00" tag="B4" />
07 </UML:SubactivityState>
08
09 <UML:SubactivityState name="Reverse_gear" xmi.id="1mwz-4a">
10        <UML:TaggedValue xmi.id="1mx2-4a" value="148" tag="CAN ID" />
11        <UML:TaggedValue xmi.id="1mx3-4a" value="0D" tag="B1" />
12        <UML:TaggedValue xmi.id="1mx4-4a" value="00" tag="B2" />
13        <UML:TaggedValue xmi.id="1mx5-4a" value="00" tag="B3" />
14        <UML:TaggedValue xmi.id="1mx6-4a" value="00" tag="B4" />
15        <UML:TaggedValue xmi.id="1mx7-4a" value="00" tag="B5" />
16        <UML:TaggedValue xmi.id="1mx8-4a" value="00" tag="B6" />
17        <UML:TaggedValue xmi.id="1mx9-4a" value="EE" tag="B7" />
18        <UML:TaggedValue xmi.id="1mxa-4a" value="01" tag="B8" />
19 </UML:SubactivityState>
20
21 <UML:SubactivityState name="Precrash_brake" xmi.id="1mq6-4a">
22        <UML:TaggedValue xmi.id="1mq9-4a" value="160" tag="CAN ID" />
23        <UML:TaggedValue xmi.id="1mqa-4a" value="9E" tag="B1" />
24        <UML:TaggedValue xmi.id="1mqb-4a" value="01" tag="B2" />
25        <UML:TaggedValue xmi.id="1mqc-4a" value="98" tag="B3" />
26        <UML:TaggedValue xmi.id="1mqd-4a" value="00" tag="B4" />
27        <UML:TaggedValue xmi.id="1mqe-4a" value="00" tag="B5" />
28        <UML:TaggedValue xmi.id="1mqf-4a" value="00" tag="B6" />
29        <UML:TaggedValue xmi.id="1mqg-4a" value="00" tag="B7" />
30        <UML:TaggedValue xmi.id="1mqh-4a" value="00" tag="B8" />
31 </UML:SubactivityState>
⋮
```

Bus Traffic File 2 行目，3 行目，7 行目は，3 つの脅威の攻撃データを示す．

Line	N/W	ID	B1	B2	B3	B4	B5	B6	B7	B8
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2	CAN	0D1	6F	02	00	00				
3	CAN	140	00	00	BE	00	00	0F	25	00
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
7	CAN	148	0B	00	00	00	00	00	11	01
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

図 6 車載ネットワーク脅威の攻撃データ生成例

Fig. 6 Example of attack data generation in automotive network threats.

© 2017 Information Processing Society of Japan

スの例で格納されている攻撃データの抽出が可能である．

最後に，4.2 節 (2) のように，攻撃データの生成と脅威の実証が可能な脅威モデルを依頼元へのレポートとするため，CAN アナライザ用のデータフォーマットで攻撃データを出力する．

CAN アナライザの多くは CSV 形式での出力に対応しているため，脅威モデルから抽出した攻撃データの値を，図 6 の下部の CSV 形式で書き込む．

以上，提案手法により，4.2 節の車載ネットワークの検証において，4.3 節の脅威モデリング連携型アタックテストを用いることで，脅威モデルと攻撃データという脅威の実証を行える成果物を提供できることを示した．

5. 提案手法の評価

5.1 脅威分析からのアタックテスト要件に対する評価

依頼元の要件に沿った成果を得ることができるかを評価するために，以下に示す定性評価を行った．

5.1.1 評価方法

要件としては，中小企業のセキュリティに関するケーススタディ [13] にフィードバックできるかによって評価する．このケーススタディを用いた理由は，自動車メーカが外部のテスト技術者にアタックテストを依頼するケースにおいて，自動車メーカのテスト要件や確立された評価基準が広く公開されておらず，アタックテストを行う前段階の脅威分析からアタックテスト要件を作る現状をみると汎用的な例となっているためである．なお，参考にしたケーススタディでは緩和方法すなわち脅威に対する対応策についての手順が含まれているが，アタックテストは脅威の発見までを対象としていることから，緩和方法に関する手順は要件の参考からは除外した．

最終的に文献 [13] を参考に作成した要件 1〜5 に沿って，本提案手法の要件充足についてまとめる．

要件 1　背景情報の収集への貢献：脅威モデル分析を成功させる準備として，背景情報を収集できることとする．

要件 2　脅威モデルの作成と分析への貢献：脅威モデルについてのミーティングで，開発者およびテスト技術者が脅威の発見に役立てられることとする．

要件 3　脅威の確認への貢献：車載ネットワークに対する脅威を特定後，各脅威のリスクにランクを付ける．各脅威への対応方法を決定できることとする．

要件 4　ドキュメントの考慮事項：脅威モデル分析で見つかった事柄と，車載ネットワークへの脅威の影響を軽減するために決定した事柄が文書化されるものとする．

要件 5　脅威モデルの設計との同期の維持：新しい要素を環境に追加する場合は，脅威モデル分析の調査結果を見直し，新しい機能に対する脅威モデル分析を行えることとする．

5.1.2 評価結果

以上 5 つの要件への適合という観点で，4 章の車載ネットワーク検証方法の有用性を評価する．5.1.1 項であげた脅威分析からのアタックテスト要件について，**表 2** のとおり，5 つの要件について要件を満たすことができた．要件 1，2，3 に関しては，DFD で視覚的に脅威を確認することで，要件を満たすことができた．さらに，要件 4 においては，脅威モデルから攻撃データを生成し，脅威を再現しながら検証できる本手法は，文献 [13] にもあるように，品質保証（QA），テスト，サポート，運用担当者の検証ドキュメントになりうる点が要件を満たしているといえる．要件 5 においては，モデル変更だけでなく，関係する攻撃データ部分を更新できることで，アタックテストのドキュメントとして維持できることが，文献 [13] の脅威モデルの同期を維持という点で要件を満たしていると考える．

表 2　脅威分析からのアタックテスト要件と評価結果
Table 2　Requirements from threat analysis and the results.

要件	合否	合否の詳細
1. 背景情報の収集	OK	DFD で視覚的に脅威確認できる
2. 脅威モデルの作成と分析	OK	DFD で視覚的に脅威確認できる
3. 脅威の確認	OK	DFD で視覚的に脅威確認できる
4. ドキュメントの考慮事項	OK	ドキュメントは，品質保証 (QA)，テスト，サポート，運用担当者の検証ドキュメントになる
5. 脅威モデルの設計との同期の維持	OK	モデルのデータ保持部分を変えることで，アタックテストドキュメントとして維持できる

5.2 脅威モデリングを行わない技術者との比較

脅威モデリングを行わない他のアタックテスト技術者が行った場合と同等，もしくはそれ以上のアタックテストの効率を提供できるかを評価するために，以下に示す定量評価を行った．

5.2.1 評価方法

4 章で述べた提案手法による車載ネットワーク検証により，脅威モデリングを行わない他のアタックテスト技術者が行った場合と同等もしくはそれ以上のアタックテストの効率を提供できるかを定量的に評価する．評価には，EVITA の攻撃確率 [14] に技術者のバイアスを取り入れた指標を用いる．EVITA の攻撃確率とは，脅威発見に必要となる攻撃時間，必要な経験，必要な知識，攻撃機会の頻度，攻撃に必要な設備から，攻撃のしやすさを 5 段階で数値化したものである．当該指標をアタックテスト効率と呼ぶ．比較対象として以下の被験者を設定する．なお，被験者の頭文字の M は，被験者の Model の頭文字である．

被験者 M_1：車載ネットワーク解析の指導者．車載ネットワークおよび CAN に関する分野の深い知識を持つ．

被験者 M_2：M_1 の指導を受けた研究員．所有知識は M_1 と同様の分野であるが，知識量は M_1 に劣る．

被験者 M_3：M_1 による 1 日セミナを受講した技術者．M_1 と同様の分野の知識をセミナで習得している．

© 2017 Information Processing Society of Japan

表 3 被験者情報
Table 3 Research participants profile.

被験者	M_1	M_2	M_3	M_4	M_5
役職	大学教員	研究員	大学生	研究員	研究員
役割	研究指導者	M_1 の直属の研究員	M_1 の 1 日セミナーの受講者	M_1 の直属の研究員	M_1 の直属の研究員
事前知識	・情報セキュリティ ・車載セキュリティ	・情報工学	・情報工学	・システム工学 ・アプリケーションサーバ	・システム工学 ・ソフトウェア上流設計 ・UML モデリング
リクルーティング	研究当事者として参加	同左	臨時研究員として雇用	研究当事者として参加	同左
報酬	業務範囲内の報酬	同左	雇用契約内の報酬	業務範囲内の報酬	同左
車載ネットワーク知識	・先行して車載研究 ・外部講演経験有 ・実車デモ歴 5 年 ・公開講座でのデモ可能	・簡易 CAN バス構築可能 ・小型 ECU 操作可能 ・実車デモ歴 3 か月	・CAN バス操作(Linux) ・CAN メッセージ表示 ・CAN メッセージ送受信 ・上記プログラム改変	・CAN バス操作(Linux) ・CAN メッセージ表示 ・CAN メッセージ送受信	・CAN バス操作(Linux) ・CAN メッセージ表示 ・CAN メッセージ送受信 ・DFD による車載脅威モデリング
提案手法利用	なし	なし	なし	なし	あり
場所と設備	近隣の駐車場で運転支援機能(ADAS)を搭載した実験車利用	同左	同左	同左	同左
事前伝達事項	4.2 (1)の手順で脅威を発見すること	同左	同左	同左	4.2 (2)の手順で脅威を発見すること
安全と倫理	所属元の規定の範囲内	同左	2 週間の契約範囲内	所属元の規定の範囲内	所属元の規定の範囲内
制限事項	特になし	同左	同左	同左	同左

表 4 TL_{ij} と C_i の算出表
Table 4 Tables of TL_{ij} and C_i concerned about attacker's level.

準備開始から脅威に関する CAN メッセージの特定までの時間(h)	攻撃時間レベル係数 TL_{ij}
2 時間未満	5
2 時間以上 5 時間未満	4
5 時間以上 10 時間未満	3
10 時間位上 12 時間未満	2
12 時間以上	1

被験者の 1 人月の単価	脅威特定コスト係数 C_i
50 万円未満	5
50 万円以上 100 万円未満	4
100 万円以上 150 万円未満	3
150 万円以上 200 万円未満	2
200 万円以上	1

被験者 M_4：M_1 の指導を受けていない研究員．所有知識は M_1 と同様の分野であるが，知識量は M_2 に劣る．
被験者 M_5：M_1 の指導を受けていないが，提案手法を用いた研究員．所有知識は M_1 と同様の分野で，知識量は M_4 と同等とする．

被験者の背景知識と提案手法を用いるか否かの差異については**表 3** にその詳細を記述した．表の項目については，文献 [16] を参考にした．上記 5 名で，4.2 節で述べた車載ネットワークのアタックテストを実施した．アタックテストの評価は，後述のアタックテスト効率と呼ばれる指標を策定して行う．なお，アタックテスト効率は，脅威ごとの攻撃のしやすさを示す EVITA の攻撃確率に被験者のバイアスを掛け算して算出したものとして以下のとおり定義する．

V_{ij}：被験者 M_i が**表 5** の j 番目の脅威に対して行った場合のアタックテストの効率を指す．以降，この変数をアタックテスト効率と呼ぶ．なお，i は被験者を示す 1〜5 の番号である．j は表 5 の S1〜S9，D1，D2 の 11 件の脅威を指すための 1〜11 の識別番号である．

AP_j：表 5 の j 番目の脅威に対し，文献 [14] を参考に筆者らで算出した EVITA の攻撃確率の値を指す．

B_{ij}：被験者 M_i によって変動する被験者のバイアス係数とする．

表 5 STRIDE 分析によって洗い出された脅威一覧
Table 5 Derived threats list categorized using STRIDE.

STRIDE カテゴリ	想定される脅威	Level 3 内の脅威 ID
S:なりすまし	エンジン回転計がなりすまされる.	S1
	速度計がなりすまされる	S2
	ギア状態がなりすまされる(R, P, N, D)	S3
	プリクラッシュブレーキ制御	S4
	イグニッション OFF 時の鍵の施錠および開錠	S5
	イグニッション ON 時の鍵の施錠	S6
	ホーンを連続で鳴らされる.	S7
	コンプレッサの制御がなりすまされる	S8
	電動パーキングブレーキの解除	S9
T:改ざん	対象除外. CAN メッセージ送信のみでは不可	-
R:否認	対象除外. CAN メッセージ送信のみでは不可	-
I:情報漏洩	対象除外. CAN メッセージ送信のみでは不可	-
D:サービス拒否	DoS 攻撃により計器パネルがダウンする.	D1
	リプレイ攻撃によりエンジンの停止	D2
E:権限昇格	対象除外. CAN メッセージ送信のみでは不可	-

以上の 3 つの変数により，被験者 M_i が j 番目の脅威に対して行ったアタックテスト効率を以下のように定義する．

$$V_{ij} = AP_j \times B_{ij} \tag{1}$$

ここで，攻撃確率 AP_j に被験者 M_i のバイアスを表現するため，B_{ij} の構成要素を以下のように定義する．

TL_{ij}：被験者 M_i が脅威 j を攻撃するのに要する時間のレベルを示す係数．**表 4** の左表のように，攻撃時間により 1〜5 の値をとり，攻撃時間が短いほど効率が良いものとする．攻撃時間は，被験者 M_i によるアタックテストの準備開始から脅威に関する CAN メッセージの特定までとする．

W_{ij}：被験者 M_i が脅威を特定した場合に付与される，被験者のアタックテスト単価により上下する重み係数とする．値は後述する算出ポリシに従う．

以上の 2 つの変数により，B_{ij} を以下のように定義する．

$$B_{ij} = TL_{ij} \times W_{ij} \tag{2}$$

W_{ij} の算出ポリシは，攻撃者のアタックテスト単価を考

© 2017 Information Processing Society of Japan

慮するため，以下のとおりとする．

- W_{ij} は，脅威を見つけた被験者 M_i のみに割り振る．
- それらの合計が 1 になるように，0〜1 の小数値を振る．
- たとえば，脅威 j を被験者 M_1，M_2，M_5 が見つけた場合は，W_{1j}，W_{2j}，W_{5j} で 0〜1 の小数値を振る．理由は，被験者レベルを相対的に表現するためである．
- 脅威を特定できなかった被験者 M_i の W_{ij} をゼロとする．理由は，脅威特定者に価値を持たせるためである．
- W_{ij} は以下の変数により構成する．

C_i：被験者 i による脅威特定のコスト係数とする．被験者の 1 人月の単価を考慮して，表 4 の右表のような算出ポリシにより算出する．C_i のパラメータは，EVITA の各パラメータが 5 段階評価となっていることに合わせて 1〜5 の 5 段階のパラメータをとるようにした．単価の区分についてはアタックツールベンダへのヒアリング結果を基に区分分けを行った．被験者の間には表 3 のような背景知識の差が存在することから，M_1，M_2，M_3，M_4，M_5 の脅威特定コスト係数は，それらの差から生じる被験者ごとの人件費から勘案してそれぞれ $C_1 = 2$，$C_2 = 3$，$C_3 = 5$，$C_4 = 3$，$C_5 = 3$ のように決定した．

$I(i)$：被験者 M_i による脅威の特定度合いを示すインジケータ関数とする．被験者が脅威を起こす CAN メッセージを特定した場合は 1，特定できなかった場合は 0 とする．$I(i)$ の値は，攻撃時間のレベルを示す TL_{ij} の値には依存しない．

上記の W_{ij}，C_i，$I(i)$ の算出ポリシに従い，被験者のアタックテスト単価により上下する重み係数 W_{ij} を以下のように定義する．

$$W_{ij} = \frac{I(i)}{\sum (C_i \times I(i))} \times C_i \tag{3}$$

なお，式 (3) は，5 人の被験者のいずれかが脅威を特定したもののみ評価するため，分母がゼロになる場合は発生しない．

W_{ij} は被験者 M_i が脅威 j を発見した場合，M_i のみが発見した場合は価値が高くなり，他の被験者でも見つけられた場合は，価値が低いという考え方を表している．たとえば，被験者 M_5 のみが脅威 j を発見した場合の W_{5j} は，

$$W_{5j} = C_5/C_5 = 3/3 = 1$$

となり，被験者全員が脅威 j を見つけた場合の W_{5j} は，

$$\begin{aligned} W_{5j} &= C_5/(C_1 + C_2 + C_3 + C_4 + C_5) \\ &= 3/(2 + 3 + 5 + 3 + 3) \fallingdotseq 0.19 \end{aligned}$$

となる．このように，W_{ij} は発見者の少なかった脅威を見つけた場合は最大値 1 に近い数値となり，発見者の多かった脅威を見つけた場合は相対的に小さい数値となる．また，発見者の人件費が低い場合は脅威発見の価値が高いものとして W_{ij} の数値が大きくなり，そうでない場合は価値が低いものとして W_{ij} の数値が小さくなる．すなわち，式 (3) により脅威発見の難易度や発見者の人件費を考慮した重み係数 W_{ij} の算出が可能となる．

以上，式 (3) により，被験者 M_i が脅威を特定した場合の被験者のアタックテスト単価を考慮した重み係数を設定することが可能となる．そして，式 (2) において，被験者が脅威特定に要した時間のレベルと式 (3) のアタックテスト単価を考慮した重みにより，被験者のバイアス係数を表現することができる．最終的に，式 (1) によって EVITA の攻撃確率に被験者のバイアスを考慮することができるため，提案手法を用いた場合とそうでない場合での違いの評価を，式 (1) の指標で評価することが可能となる．

5.2.2 評価結果

表 5 で，被験者 M_1〜M_5 により特定された脅威のすべてを STRIDE カテゴリに分類した一覧を示す．そして，表 5 の 11 件の脅威において，被験者 M_1〜M_5 におけるアタックテストの効率の比較を**表 6** で行った．ここで表 6 の 1 列目の表記では脅威を表す j を略し，被験者のみを添字で示す．アタックテストの効率は，EVITA の攻撃確率に被験者のバイアスを与えた，アタックテスト効率という指標で定量的に比較評価を行った．W_{ij} については，小数点第 2 位までとし小数点第 3 位を四捨五入した値として表示している．その結果，提案手法を用いていない M_4 と同等の能力を持つ被験者 M_5 が提案手法を用いることで，表 6 の下部のとおりアタックテスト効率の合計値および個別傾向において，おおむね M_1 と同等かつ M_4 より高いアタックテスト効率を得られることが分かった．

被験者 M_4，M_5 よりも M_2 のアタックテスト効率が良かった点に関しては，脅威特定にかかるコストが同レベル，

表 6 比較実験結果
Table 6 Comparison results.

	S1	S2	S3	S4	S5	S6	S7	S8	S9	D1	D2
AP	5	5	5	2	5	5	5	5	5	3	3
TL_1	4	5	5	3	5	5	4	4	5	4	1
TL_2	3	4	4	3	4	4	3	3	4	4	1
TL_3	3	3	3	1	3	3	3	1	2	3	1
TL_4	3	2	1	1	3	3	3	1	2	3	1
TL_5	3	3	3	1	4	4	3	3	3	3	1
W_1	0.25	0.25	0.12	0.40	0.12	0.15	0.25	0.25	0.12	0.25	0.40
W_2	0.38	0.38	0.18	0.00	0.18	0.23	0.38	0.38	0.18	0.38	0.00
W_3	0.00	0.00	0.29	0.00	0.29	0.38	0.00	0.00	0.29	0.00	0.00
W_4	0.00	0.00	0.24	0.00	0.24	0.00	0.00	0.00	0.24	0.00	0.00
W_5	0.38	0.38	0.18	0.60	0.18	0.23	0.38	0.38	0.18	0.38	0.60
V_1	5.00	3.75	2.94	2.40	2.94	3.85	5.00	5.00	2.94	3.00	1.20
V_2	5.63	4.50	3.53	0.00	3.53	4.62	5.63	5.63	3.53	4.50	0.00
V_3	0.00	0.00	4.41	0.00	4.41	5.77	0.00	0.00	2.94	0.00	0.00
V_4	0.00	0.00	1.18	0.00	3.53	0.00	0.00	0.00	2.35	0.00	0.00
V_5	5.63	3.38	2.65	1.20	3.53	4.62	5.63	5.63	2.65	3.38	1.80

	M_1	M_2	M_3	M_4	M_5
V_i 合計値	38.02	41.10	17.53	7.06	40.10

© 2017 Information Processing Society of Japan

かつモデル作成のコストをかけなかったためと考えられる．ただし，今回の比較指標の対象外ではあるが，テスト依頼元への説明や技術者間の知識共有という点では，被験者 M_5 が行った脅威モデリングは有用であると考えられる．

6. まとめと今後の課題

本論文では，自動車メーカからアタックテストを依頼された技術者が，依頼元に車載ネットワークの脅威をレポートするまでを想定し，脅威モデリング連携型アタックテストを提案した．本提案手法の有効性を，脅威分析からアタックテストまでにあげた要件のどの要件に有効かを示した．また，技術者が脅威モデリングを行うことなくアタックテストを実施した場合と比較し，同等もしくはそれ以上のアタックテストの効率を提供できることを示した．提案手法は車載ネットワークを介して自動車が制御されてしまう脅威の分析を想定しており，今回攻撃経路として OBD2 ポートを使用した．OBD2 ポートとは別経路の攻撃の例として，車載ネットワークにつながる ECU が乗っ取られて不正なメッセージが注入され，自動車が制御されるような攻撃が考えられる．このような場合には，攻撃のエントリポイントを OBD2 ポート以外の車載ネットワークにつながる ECU に置き換えることで提案手法を適用可能である．ただし，車載ネットワークにメッセージを注入しないような攻撃，たとえばインフォテイメント系の ECU を乗っ取り，ECU に付属するユーザへの画面表示を制御して利便性を損なわせる等の攻撃については，提案手法を適用することが難しい．今後の課題として，これらの車載ネットワークを介さない攻撃についても適用できるよう検討することがあげられる．

謝辞 本成果は沖縄県生活機器セキュリティ基盤形成促進事業の補助を受けて行われました．ここに記して謝意を表します．

参考文献

[1] Miller, C. and Chris, V.: Remote exploitation of an unaltered passenger vehicle, *Black Hat USA 2015* (2015).
[2] 倉地 亮，高田広章，中野稔久，安齋 潤，後藤博喜，中野学，飯沼高明，松島秀樹：自動車の制御システムに対する効率的なセキュリティ評価手法の提案，暗号と情報セキュリティシンポジウム（SCIS2017），pp.1–8 (2017).
[3] 水口大知，杉山 歩，松井康治郎，武田英幸：車載セキュリティガイドライン SAE J3061 に適合したサイバーセキュリティコンセプト構築手順の提案，暗号と情報セキュリティシンポジウム（SCIS2017），pp.1–8 (2017).
[4] Swiderski, F. and Snyder, W.: *Threat modeling*, Microsoft Press, ISBN 978-0735619913 (2004).
[5] Shostack, A.: *Threat modeling: Designing for Security*, John Wiley & Sons, ISBN 978-1118809990 (2014).
[6] Sutton, M., Greene, A. and Amini, P.: *Fuzzing: Brute Force Vulnerability Discovery*, Addison-Wesley Professional, ISBN 978-0321446114 (2007).
[7] Weidman, G.: *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press, ISBN 978-1593275648 (2014).
[8] Bekrar, S., Bekrar, C., Groz, R. and Mounier, L.: Finding Software Vulnerabilities by Smart Fuzzing, *Proc. 2011 4th IEEE International Conference on Software Testing Verification and Validation* (*ICST '11*), IEEE, pp.427–430 (2011).
[9] Bayer, S., Enderle, T., Oka, D.K. and Wolf, M.: Security Crash Test – Practical Security Evaluations of Automotive Onboard IT Components, *Automotive – Safety & Security 2015* (2015).
[10] Myagmar, S., Lee, J.A. and Yurcik, W.: Threat Modeling as a Basis for Security Requirements, *Symposium on Requirements Engineering for Information Security* (2005).
[11] Microsoft: Microsoft Threat Modeling Tool 2016, Microsoft (online), available from ⟨https://www.microsoft.com/en-us/download/details.aspx?id=49168⟩ (accessed 2017-01-31).
[12] Ramaswamy, C. and Blackburn, M.: Automated Testing of Security Functions Using a Combined Model and Interface-Driven Approach, *Proc. 37th Annual Hawaii International Conf.* (2004).
[13] Microsoft：中小企業のセキュリティに関するケーススタディ脅威モデル分析，Microsoft（オンライン），入手先 ⟨https://msdn.microsoft.com/ja-jp/library/aa561499.aspx⟩（参照 2017-02-17）.
[14] Security requirements for automotive on-board networks based on dark-side scenarios, Deliverable D2.3 of EVITA (2009).
[15] Smith, C.: *The Car Hacker's Handbook: A Guide for the Penetration Tester*, No Starch Press, ISBN 978-1593277031 (2016).
[16] Stuart, S.: Common Pitfalls in Writing about Security and Privacy Human Subjects Experiments, and How to Avoid Them, available from ⟨https://www.microsoft.com/en-us/research/publication/common-pitfalls-in-writing-about-security-and-privacy-human-subjects-experiments-and-how-to-avoid-them/⟩ (accessed 2017-06-09).

西尾 泰彦 （正会員）

1997 年広島大学工学部第二類（電気系）卒業．1999 年同大学大学院博士前期課程修了．2002 年同博士後期課程修了．博士（工学）．2002 年株式会社日立製作所ソフトウェア事業部入社．2015 年株式会社チェンジビジョン入社．同年一般社団法人重要生活機器連携セキュリティ協議会（CCDS）研究員（出向）．2017 年より株式会社チェンジビジョン復帰．現在に至る．ソフトウェア信頼性，セキュリティ，安全性モデルの研究に従事．電子情報通信学会会員．

© 2017 Information Processing Society of Japan

城間 政司 （正会員）

2007 年琉球大学工学部情報工学科卒業．2009 年同大学大学院理工学研究科博士前期課程修了．2013 年同大学院理工学研究科博士後期課程単位取得後退学．同年琉球大学医学部附属病院特命一般職員．2016 年より一般社団法人重要生活機器連携セキュリティ協議会（CCDS）研究員，現在に至る．博士（工学）．デジタルアイデンティティ，セキュリティリスクアセスメントに関する研究に従事．

井上 博之 （正会員）

1987 年大阪大学工学部電子工学科卒業．1989 年同大学大学院工学研究科電子工学専攻修了．1989～2000 年住友電気工業株式会社．1998 年奈良先端科学技術大学院大学情報科学研究科博士後期課程単位取得退学，博士（工学）．2000～2007 年株式会社インターネット総合研究所および株式会社 IRI ユビテック．2007 年より広島市立大学大学院情報科学研究科．現在は，同大学准教授．他に，一般社団法人重要生活機器連携セキュリティ協議会研究開発センターチーフ，SECCON 実行委員，セキュリティ・キャンプ全国大会講師等．広域ネットワークにつながる家電や自動車の情報セキュリティについて，その脆弱性やセキュアな通信プロトコルに関する研究開発に従事．電子情報通信学会，IEEE 各会員．

© 2017 Information Processing Society of Japan