Vol.2018-DPS-174 No.1
Vol.2018-CSEC-80 No.1
2018/3/5

膨大な数の自律型モビリティのための基盤の高信頼化に関する検討 ～サイバー攻撃に関する検知の検討～

原田貴史[†1]　諸橋玄武[†1]　伊藤宏樹[†1]

概要：自動走行車をはじめとした自律型モビリティの導入が期待されている．このような自律型モビリティを支える基盤に対するサイバー攻撃により，膨大な数の自律型モビリティに被害が及ぶ恐れがある．本稿では，そのような自律型モビリティ基盤に対するサイバー攻撃の検知について技術検討を行った結果を報告する．自律型モビリティの自動走行には，ダイナミックマップが用いられる．このダイナミックマップのデータには，渋滞情報，道路情報，三次元構造物など，様々な情報が含まれている．これらの情報は，各自律型モビリティから収集された車両の位置情報や速度情報などの情報から生成され，各自律型モビリティから送信される．本検討においては，自律型モビリティとダイナミックマップを生成・配信する基盤との間でやりとりされるトラヒックを分析することで，自律型モビリティシステムの脅威を検知する技術を検討する．より具体的には，膨大な数の自律型モビリティとの間で生じる極めて大量のトラヒックを精度良く効率的に行う方法として多層型分析フレームワークの導入を検討する．また，自律型モビリティシステムのトラヒックを模擬した検証環境上で，同フレームワークを適用した検証実験を行い，その有用性を確認する．

1. はじめに

近年我が国を取り巻く急激な高齢化や人口減少の社会的課題への取り組みとして，過疎地も含めた高齢者の安全・安心な生活や多様な経済活動の生産性確保等に，自動走行技術の実装と，ネットワークを利用した高精度な制御による自律型モビリティ（高信頼・高精度な移動を実現する車両，電動車いす，ロボットなど）の実現が期待されている．自律型モビリティは，様々なセンサー情報などを活用し高信頼・高精度な自動走行を実現するため，ICT 基盤技術との連携が重要となる．具体的には，自律型モビリティに対して低遅延かつ高信頼なデータ処理が不可欠となるため，エッジコンピューティング技術を応用することなどが想定されている[1]．また自律型モビリティシステムは，人命に関わるという観点から安全・高信頼でなければならない．すなわち，自律型モビリティが関わるネットワークにおいて異常なトラヒックの発生を事前に防止する，あるいは，早期に検知し対処する必要がある．

本検討においては，特にこの異常トラヒックの発生が，悪意を持った攻撃者により行われるサイバー攻撃であることを想定し，異常トラヒック発生を迅速に把握する手法について検討する．自律型モビリティシステムにおいて，様々な異常トラヒックによる脅威の発生が想定される．サイバー攻撃による異常トラヒックとしては，DoS 攻撃によるものやアプリケーション上で改ざんされたデータの送付などが考えられる．これらの異常トラヒックの有無を逐次分析することにより，検知する方法について検討する．

2. 自律型モビリティシステムとサービス

自律型モビリティシステムを運用する上でもっとも基本的なサービスとなるのは，自律型モビリティ等から情報を収集し，それに基づいて鮮度と精度の高いダイナミックマップを生成及び配信するサービスである．（以下ダイナミックマップサービスと呼ぶ）

2.1 ダイナミックマップサービス

ダイナミックマップとは，自律型モビリティが，自動走行するために必要な高度な地図情報である．このダイナミックマップは，データの配信される頻度やデータの内容の観点で以下の 4 つに配信するデータを分類することができる．頻度が高く，少量を配信するものから，頻度が低く大容量のデータを配信するものまで存在する．

表 1 ダイナミックマップのデータ分類
（文献[2] p3 を基に作成）

－	頻度	内容
動的情報	1 秒未満	ITS 先読み情報（周辺車両，歩行者情報，信号情報など）
准動的情報	1 分未満	事故情報，渋滞情報，狭域気象情報など
准静的情報	1 時間未満	交通規制情報，道路工事情報，広域気象情報
静的情報	1 ヶ月未満	路面情報，車線情報，三次元構造物など

†NTT セキュアプラットフォーム研究所
NTT Secure Platform Labratories

Vol.2018-DPS-174 No.1
Vol.2018-CSEC-80 No.1
2018/3/5

ダイナミックマップのデータ生成には，様々なケースが検討されている．動的情報については，自律型モビリティから観測された位置情報などのプローブ情報（以下プローブ情報と呼ぶ）を処理して配信する方法，准動的情報は，自律型モビリティから取集されたプローブ情報を，所望の情報に変換するために分析した配信する方法，静的情報は，MMS（モービルマッピングシステム）と呼ばれるような，道路を計測可能な専用車両を用いて収集したデータを配信する方法といったように，データの種類によって様々な情報の収集・生成方法があげられる．特に，動的情報，准動的情報，及び准静的情報は，必要な情報の収集，配信情報の生成，及び配信をダイナミックに行う必要がある．

2.2 自律型モビリティシステムの構成

ダイナミックマップ生成及び配信サービスにおいては，容量が大きい又は，配信頻度が高いといった特徴を持つデータの配信を膨大な数の自律型モビリティとの間で行うという観点からエッジコンピューティングを用いたアーキテクチャが提案されている．エッジコンピューティングとは，クラウドのように中央集権的にデータを配信するのではなく，基地局やモバイル網上に，情報処理リソースを分散配置することにより，モバイル網における中継網を通過するトラヒックを抑え，接続機器から見た応答時間を短縮する技術である．図 1 に示すように，ダイナミックマップサービスのサービスを提供するサーバは，自律型モビリティに近いエッジに分散的に配置されることが想定される．また，システムを構成する構成要素である自律型モビリティ及びエッジサーバ・クラウドサーバの間の通信プロトコルは，TCP /IP などの一般的な IT システムで用いられているプロトコルの使用が想定される．

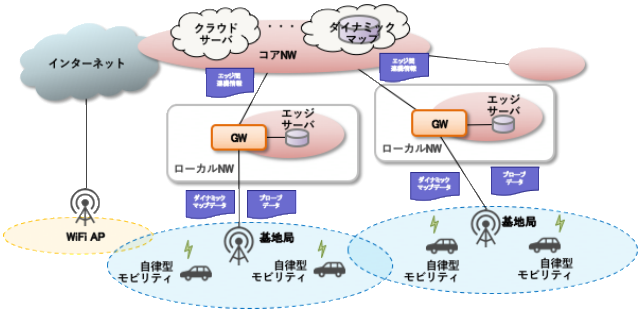

図 1 エッジコンピューティングを用いた自律型モビリティシステムの構成

3. 自律型モビリティシステムの高信頼化

上述したシステムでは，自律型モビリティには，「ネットワークを介して受信する情報」と「モビリティ自身が検知した情報」とを動的に処理し，自律的に移動制御することが求められる．そのため，自律型モビリティの安全性の観点から，自律型モビリティシステムが何らかの不具合により信頼性を失うことは防がなければならない．信頼性を失う要因は，故障，セキュリティに関する攻撃，欠陥（バグ）など様々考えられる．本検討においては，信頼性を失う要因の中でも，悪意のある攻撃者が意図をもって自律型モビリティシステムに対して攻撃を行う，セキュリティに関する攻撃について脅威やその対策について検討していく．

まず，自律型モビリティシステムについて，想定される攻撃者からの脅威を図 2 に例示する．自律型モビリティシステムにおけるネットワークでは，IT システムにおけるネットワーク同様，大量パケットによるネットワーク・サーバ等の機能不全 (以降 DoS 攻撃と呼ぶ) や，クラウドサーバ，エッジサーバ，自律型モビリティのなりすましなど，ネットワークセキュリティにおけるあらゆる脅威が想定される．

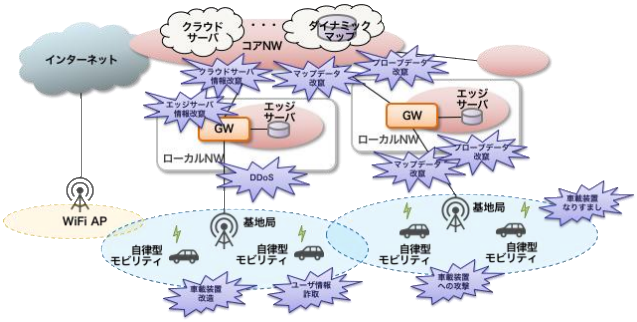

図 2 自律型モビリティシステムに対する想定脅威例

本検討においては，これらの脅威のうち，ゲートウェイからミラーリングされるトラヒックを監視することによって攻撃検知可能なものを対象とする．具体的には，プローブデータの送受信やダイナミックマップデータの送受信などといった自律型モビリティとエッジサーバ間でやりとりされるトラヒックを分析する．これらのトラヒックが，自律型モビリティシステムに対する脅威として顕在化し影響を及ぼすことになる事象としては大きく 2 つある．一方はトラヒックの送信頻度，他方はトラヒックでやりとりされるデータの内容について，何らかの異常が認められることが想定される．例えば，意図的に送信頻度を高くプローブデータを送信する攻撃，意図的にプローブデータの位置情報や速度情報などを改竄して虚偽のプローブデータを送信する攻撃や，不必要に大容量のダイナミックマップをダウンロードする攻撃などが考えられる．こういった脅威に対して，自律型モビリティとエッジサーバの間にあるゲートウェイからミラーリングされるトラヒックを逐次分析することにより，攻撃を検知する方法について検討する．

4. 関連研究

3 章において述べた今回対象とする自律型モビリティシ

Vol.2018-DPS-174 No.1
Vol.2018-CSEC-80 No.1
2018/3/5

ステムにおける脅威と類似した脅威に関するセキュリティ技術は，対象とするサービスは違うもののいくつか存在する．

虚偽のプローブデータの検知に類似する研究として，位置情報ゲームでユーザがゲームを自身に有利に進めるために，ゲームサービス提供者のサーバに対して改ざんした位置情報を送信する攻撃への対策として位置情報を保証する技術がある[2].

プローブデータや，ダイナミックマップデータに限らず，サービス提供者がもつサーバに対して大量のデータを送信することで，サービス提供を不能にする DoS 攻撃が知られており，攻撃内容によって様々な対策が提案されている．例えば，TCP SYN-Flood 攻撃についての検知では，TCP ヘッダの SYN flag や ACK flag の数を分析することにより行われる[4]．さらに，大量のトラヒックを分析する必要のある攻撃検知においては，従来から，監視対象のトラヒックを，フィルタリングするなどして監視対象のデータを削減する工夫が行われている[5].

本検討においては，このような分析を効率的に行う工夫を，複数の分析技術に対して，分析の実装や運用面において効率よく行えるように，新たに該当のトラヒックの分析すべき内容を動的に決定するための尺度である脅威レベルを導入したフレームワーク化を行い，自律型モビリティシステムの系においても，複数の脅威を効率よく分析することができる方式を検討する．

5. 多層型分析フレームワークの提案

文献[4]で述べられているように，トラヒックの内容に応じて監視するトラヒックを絞り込むことは，定常的に大量に流れるトラヒックの分析を行う場合に有効である．多層型分析フレームワークでは，処理コストがより高い詳細な分析は，全トラヒックに対して行わずに必要と推定されるものに対してのみ行うことで，処理の効率化を図る．詳細な分析の要否は，その前段で行った簡易な分析により判定した，当該トラヒックの脅威の度合い（脅威レベル）に応じて決定する．このような分析のフレームワークを，著者らは多層型分析フレームワークと呼んでいる．本フレームワークでは，ある脅威を検知し得る異なるアルゴリズムまたはパラメータを持つ複数の分析を用意し，それらを処理コストが低い順に並べ，実行する．この順序を次数と呼ぶ．ある脅威を検知しようとする際，まず最小の次数を持つ（すなわち，もっとも処理コストの低い）分析を適用し，その結果に応じて脅威度を判定し，次に大きな次数の分析を行うかどうかを決定する．各分析の結果は大きく，陰性，不審，陽性の 3 つの分類に分けられる．分析の結果，陰性とも陽性とも判断できず不審と判定したものに関してのみ，より大きな次数の分析に進む．多層型分析手法においては，このような分析を多層に重ね，陰性，または陽性の判定が確定するまで繰り返す．図 3 のように多層型分析フレームワークに，任意の分析（図中では分析 A，B…）を当てはめることで，複数の脅威に対して分析対象のトラヒックの脅威レベルに応じて効率的な分析を実現する．（図中では陽性判定を赤信号，不審判定を黄色信号，陰性判定を青信号で表す）

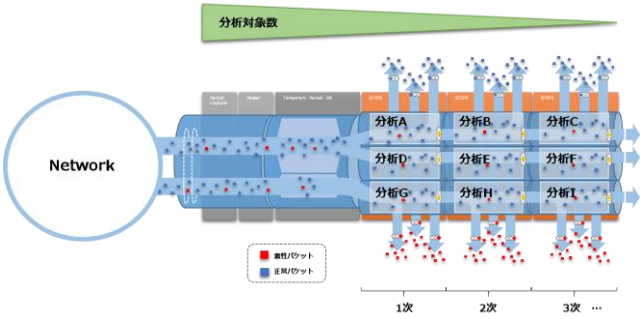

図 3 多層型分析フレームワークの分析振分イメージ

6. 攻撃の想定

3 章及び 4 章で記載したとおり，従来の IT システムにおいても DoS 攻撃は大きな問題となっており，通信のレイヤーやプロトコルに応じた解決策が検討されている．自律型モビリティシステムにおいても，それら解決策が適用可能なものもある．本検討においては，自律型モビリティシステム特有の通信内容を用いた，従来の解決策で対応し難い攻撃に対象を絞り込んだ検討を行う．

6.1 自律型モビリティシステム特有の攻撃

3 章で述べたように，自律型モビリティシステムの攻撃者は，データ送信頻度あるいはデータ内容を操作することで攻撃を行うと想定される．本稿においては，プローブデータの送信頻度を操作し，高頻度化する攻撃を想定するにする．以下，このような攻撃を HFPT 攻撃（High Frequency Probe data Transmission Attack）と呼ぶ．HFPT 攻撃が実現した場合は，プローブデータを正常時の送信頻度よりも高頻度で送信されることになる．そうすることで，複数のセキュリティ上の影響が懸念される．1 つ目は，サービス提供者のサーバのリソースを枯渇されてしまう懸念である．1 台の自律型モビリティだけでなく，複数台の自律型モビリティが連携して，いわゆる分散型攻撃となることで，たとえ，一台一台の頻度がそれほど高頻度化されていなかったとしても，サービス提供者のサーバのサイジング設計値を超えてしまうことになれば，障害が起こりうる可能性がある．2 つ目は，例えサービス提供側のサーバが処理できたとしても，頻度を高頻度化するために，攻撃者が正常な内容のデータが複数送信したり，虚偽の内容を送信することで，生成されたダイナミックマップの信頼性が落とされる

ことも懸念である．

6.2 HFPT トラヒックの想定

HFPT 攻撃を簡単に実行する方法としては，以下の 2 つの手段が考えられる．

- 同一プローブの高頻度送付

自律型モビリティ内の悪意あるプログラム（攻撃者により注入されたマルウェア，もしくは所有者により意図的に改造されたソフトウェア）が，実測されたプローブデータを多数コピーし，それらを高頻度で送付する．

- ランダムプローブの高頻度送付

自律型モビリティ内の悪意あるプログラム（攻撃者により注入されたマルウェア，もしくは所有者により意図的に改造されたソフトウェア）が，プローブデータをランダムに多数生成し，それらを高頻度で送付する．

7. 攻撃の検知

6 章で述べた攻撃の検知方法について検討する．

7.1 正常トラヒックと異常トラヒック

まず，HFPT 攻撃の検知について検討するにあたり，正常トラヒックと攻撃時の異常トラヒックについて整理する．2 章で述べたダイナミックマップ生成のために必要となるプローブデータの正常トラヒックは，図 4 に示すようにほぼ一定間隔で，エッジサーバに対して，自律型モビリティから送信されるものである．ただし，図 5 のように，通信が不安定な場合や，トンネルなど通信が正常に行われなかった際にまとめて再送されるケース考えられる．このような場合は，攻撃ではないが，正常なトラヒック量を上回るトラヒック量となる可能性が考えられる．攻撃時の異常データについても，図 5 と同様なトラヒック量の振る舞いや，連続的に正常なトラヒック量を上回るトラヒック量になることが想定される．

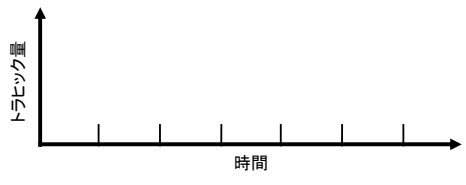

図 4 トラヒック量イメージ A

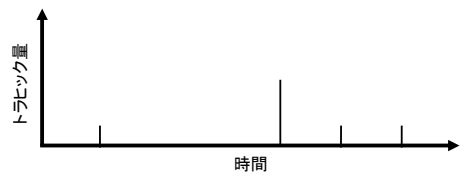

図 5 トラヒック量イメージ B

7.2 異常トラヒック分析

HFPT 攻撃では，攻撃元と攻撃先の通信トラヒック量が正常状態でのそれよりも増加するため，その検知には攻撃元と攻撃先の通信トラヒック量を監視することが有効である．しかし，7.1 節で示したとおり，攻撃発生時以外のトラヒックにおいても，攻撃による異常トラヒックと同様のトラヒック量が観測される可能性があり，これだけでは HFPT 攻撃の検知方法として不十分である．そこで，プローブデータのペイロードが，HFPT 攻撃を意図したものであるかを検査することによって，検知精度を向上させることを考える．すなわち，連続して到着したプローブのペイロードが同一，もしくは，ランダムな値であった場合には，HFPT 攻撃であると判定する検知方法を組み合わせて行う．

8. フィージビリティ検証

本章では，7 章において提案した分析方法を，膨大な数の自律型モビリティが存在する環境に適用した場合に，処理性能の観点から実行可能か否かについて，基礎的なフィージビリティ検証を行う．

8.1 検証目的

本検討においては，期待どおりに検知されているかどうかに加えて，検知の効率性が良いかどうかに着目して検証を行う．そのため，ナイーブに全てのプローブデータを対象に量的分析と質的分析の双方を実施する方法と，多層型分析フレームワークを用いる方法について，同等の検知精度となるように分析処理の閾値を設定した上で，双方の処理時間，すなわち，トラヒック分析の開始から結果を出すまでの時間を指標として比較することにする．

また，本検証において与えるトラヒックの条件は次の通りとする．まず，1 つのエッジあたりのカバー範囲は 1km2，自律型モビリティの車両密度を 1000/km2 を想定しする．プローブデータは，正常時において 100msec 間隔に自律型モビリティからエッジサーバに対して送信されるものとする．また，攻撃を行う自律型モビリティの割合を全体の 1 割，攻撃する際のプローブデータの量は，正常時の 5 倍とし，検証時刻 100 秒から 60 秒ごとに 10 台づつ正常な自律型モビリティが攻撃を行う自律型モビリティへ遷移することを想定する．

8.2 検証に用いる分析アルゴリズムと実装

質的分析については，今回は基礎的な検証として，同一性の確認のみを行う比較的簡易なアルゴリズムを用いる．

- 多層型分析フレームワークを用いる場合

以下のように，1 次の量的分析をパケット通信量の検査，

2 次の質的分析をプローブ同一性の検査とする．パケット通信量とは，トラヒック中の監視対象通信のパケットの数である．

✧ [1 次] IP 別総量分析：

1 秒間隔で，分析検知の対象となるトラヒックであるプローブデータに関するパケットを送信元 IP，送信先 IP 及びポート番号の組み合わせごとに計上したものを，2 秒間隔でスライディングしながら足し合わせ，パケット通信量が明らかに多い場合については，陽性，正常よりやや多い程度は不審と判定する．通常量の範囲内であれば，陰性と判定する．本検証においては，多層型分析フレームワーク処理の効率性を評価するため，TPR = 1 及び FPR = 0 となるトラヒック量の閾値を設定する．また，処理時間の算出に用いる分析開始時刻は，1 秒間隔の中で最初にパケットが到達した時刻とする．

✧ [2 次] プローブの同一性分析：

図 6 におけるセキュリティエンジンにおける最初のパケットの受信時刻(t0)，正常時比較想定個数（n），プローブデータ送出間隔(dt）から規定の範囲を算出し，同一性の比較に必要なプローブを抽出する．また，抽出範囲には，受信時刻のぶれを許容するために，一定程度の余裕(ε）を含ませることとする．比較対象秒数内(検索範囲内)のプローブデータについて比較間隔(e)おきに，t0 におけるプローブデータと時刻，経度，緯度，速度の全ての項目について値が同一であった場合，陽性と判定し，それ以外は陰性とする．今回の検証では，dt = 0.1， n = 30， ε = 1.0 とした．

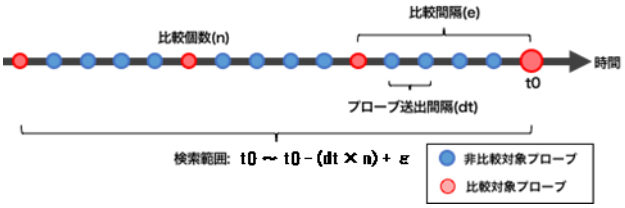

図 6 検知対象プローブの抽出

● ナイーブな方法を用いる場合

ナイーブな方法では，分析対象トラヒックであるプローブデータの全量に対して上記の 1 次分析と 2 次分析の両方を行うこととする．

8.3 検証環境構成とスペック

検証環境は，図 7 に示すように，擬似データ生成系及び多層型分析フレームワークを実現する多層型セキュリティ分析エンジンをスイッチで接続した構成となっている．また，表 2 に示すとおりの諸元の機器を使用する．

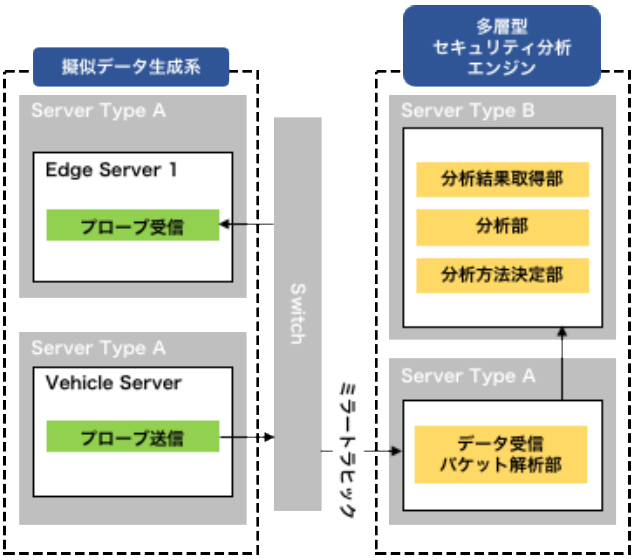

図 7 検証系構成概要

表 2 検証機器諸元

種別	主要スペック
Server Type A	HPE ProLiant DL380 Gen9 CPU：E5-2690v4×2，MEMORY：64GB Storage: 2TB HDD+400GB SSD
Server Type B	HPE ProLiant DL380 Gen9 CPU：E5-2690v4，MEMORY：128G Storage: 2TB HDD+1.6TB SSD
Switch	HPE 5900AF

8.4 擬似データ生成系

擬似データ生成系では，プローブデータのトラヒックを模擬する．1000 台分の送信元を模擬するために，IP エイリアスを用いて仮想 IP アドレスを生成し，その送信元 IP アドレスを用いてプローブデータをエッジサーバへ送信する．この際，プローブデータの中身である位置情報や速度情報は，交通シミュレータである PTV Vissim[6]で事前に作成したものを用い，そのデータを MQTT を用いてエッジサーバへ送信する．攻撃用のプローブデータも同様の仕組みで送付する．

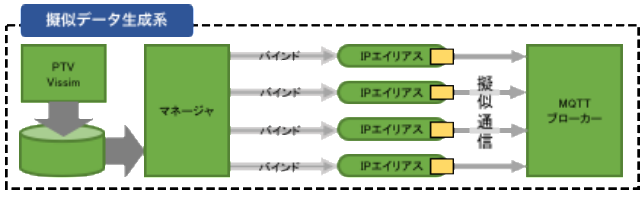

図 8 擬似データ生成系処理フロー

8.5 多層型セキュリティ分析エンジン

多層型セキュリティ分析エンジンとは，多層型分析フレームワークを実装したトラヒック分析ソフトウェアである．

Vol.2018-DPS-174 No.1
Vol.2018-CSEC-80 No.1
2018/3/5

以降，今回の HFPT 攻撃検知における処理フローを例にして動作を説明する．まず，GW よりミラーリングされたトラヒックについて，トラヒック受信解析部は，IPFIX 情報[7]の生成及び，トラヒックから分析に必要なプローブデータの抽出を行う．IPFIX 情報の生成に伴い，1 秒間隔で，トラヒック量を含むエントリデータを生成する（以降，分析対象のデータをエントリデータと呼ぶこととする）．分析方法決定部において，生成されたエントリデータを，1 次分析として量的な分析を行う分析部に渡す．分析部で量的な分析が行われた結果，正常トラヒックと異常トラヒックの区別がつきづらい範囲という判定，つまり不審の判定が出た場合は，分析対象のエントリデータの脅威レベルに応じて，分析結果取得部から 2 次分析を行うために分析方法決定部に戻され，質的な分析を行う分析部に渡され，最終的な検知結果を確定する．この際に，明らかに多量なトラヒック量であった場合には，即時陽性とする．なお，今回の検証においては，予備的な実験から分析部の処理プロセス数を 10 プロセスとした．

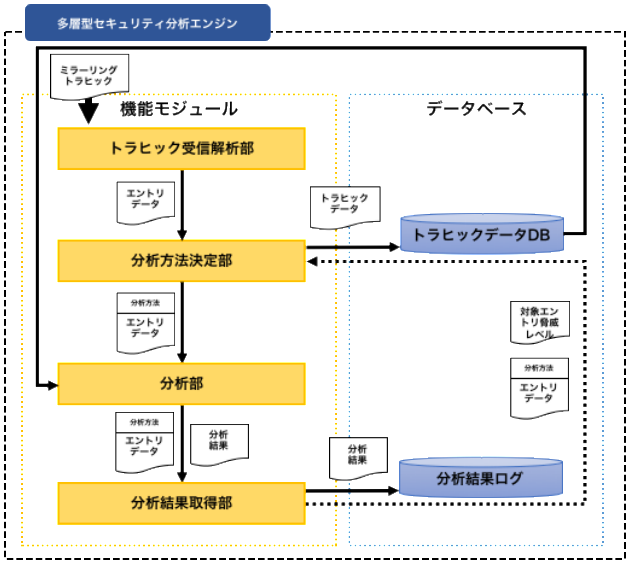

図 9　多層型セキュリティ分析エンジン処理フロー

8.6 検証結果

上記の検証系を用いて，検証を行った結果を以下に示す．

- **多層型分析フレームワークを用いた場合**

多層型分析フレームワーク用いた検知の場合，攻撃を行う自律型モビリティが増加しても，処理時間の最大値，平均値，最小値は，ほぼ一定で検知できていることがグラフからわかる．平均およそ 1.4 秒程度で検知が完了しているが，パケットを計上している時間も含むため，セキュリティエンジン内でのパケットの同一性の比較には 0.4 秒程度かかっていることになる．

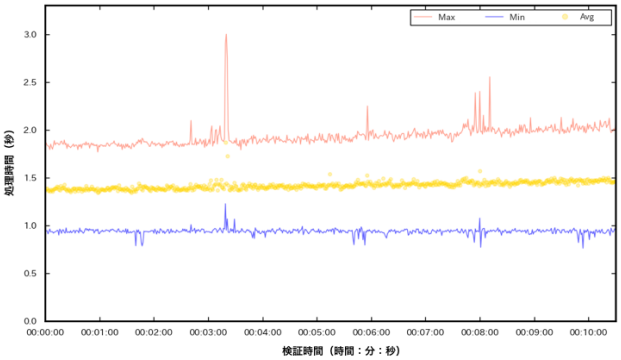

図 10　多層型分析の処理時間

- **ナイーブな方法を用いた場合**

ナイーブな方法を用いた場合，攻撃を行う自律型モビリティが増加するにつれて処理しきれなくなり，処理時間が増加し，検知が遅延していることがグラフからわかる．初期の状態から処理しきれないため，10 分経過時には，処理きれないものかキューにたまり，分析開始から完了まで，400 秒程度かかっていることがわかる．

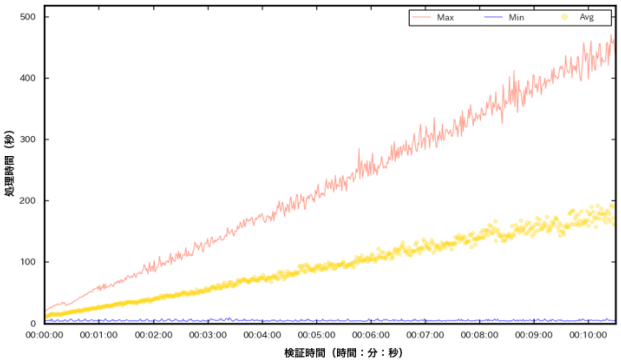

図 11　ナイーブな分析の処理時間

9. 考察と課題

検証の結果から，分析の絞込みが効果的に行われ，分析を同じプロセス数で実施した場合において，より効率的な分析が行われナイーブな方法では処理できない量が処理可能となっていることが分かる．多層型分析の場合，1 次で量的な分析を行っているため，全自律型モビリティが攻撃元となった場合には，ナイーブな分析と同じように全ての自律型モビリティからのトラヒックを分析することになる．

そのため，上記のような効率的な分析を行うことが効果的となるのは，セキュリティ分析のように，多くの監視対象があり，大多数が正常なままである中で，一部少数のみが感染するといったケースである．自律型モビリティの大半が攻撃元となってしまうようなケースは，各自律型モビリティとエッジサーバの対ごとに計上するだけではなく，全体のトラヒックを総合的に監視する必要がある．

10. おわりに

本検討においては，自律型モビリティシステム特有の攻撃として考えられる HFPT 攻撃（High Frequency Probe data Transmission Attack）を検知する手法について検討したそのためのトラヒック分析の方法として，多層型分析フレームワークを用いて量的分析の結果に応じて質的分析を行うか決定する方法と，量的分析と質的分析を常に両方行うナイーブな方法を用いる場合とを大量の自律型モビリティの存在を想定した膨大な量の模擬トラヒックを用いた検証実験により比較評価した．その結果，多層型分析フレームワークを用いることで，ナイーブな方法に比べてより効率的に分析可能なことを示した．自律型モビリティシステム特有の攻撃は，今回検討した HFPT 攻撃のみならず，大容量のダイナミックマップをリクエストする攻撃，虚偽のプローブデータを送信する攻撃などが考えられる．それらの攻撃に対しても，多層型分析フレームワークを用いることでより効率的な攻撃検知が可能であるかどうかを引き続き検証していく．

謝辞 本検討は，総務省委託研究開発「電波資源拡大のための研究開発　膨大な数の自律型モビリティシステムを支える多様な状況に応じた周波数有効利用技術の研究開発　大量の異常通信の検知・抑制による高信頼化技術」の一環で得られた結果を含んでおり，ここに感謝の意を表する．

参考文献

[1] 川村他，自律型モビリティシステム（自動走行技術，自動制御技術等）の開発・実証，ICT イノベーションフォーラム 2018
[2] “戦略的イノベーション創造プログラム（SIP） 自動走行システム研究開発の取組状況“. http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai3/siryou9.pdf, (参照 2018-02-07)
[3] 山口 正他, GPS 情報と WLAN 信号情報を用いた位置証明方式. 電子情報通信学会技術研究報告. IE, 画像工学 112(136), 43-48, 2012-07-12
[4] 倉上弘, DoS/DDoS 攻撃対策（2）情報処理 Vol.54 No.5 May2013
[5] 倉上弘他, 異常トラヒック検出・分析システム, NTT 技術ジャーナル 2008.7
[6] “PTV Vissim 製品情報“. http://vision-traffic.ptvgroup.com/en-us/products/ptv-vissim/, (参照 2018-02-07).
[7] “IPFIX の概要“. https://www.ibm.com/support/knowledgecenter/ja/SSCVHB_1.2.1/collector/cnpi_collector_IPFIX_overview.html, (参照 2018-02-07).