コネクテッドカーはインターネット上から発見可能か？

植田 岳洋[1,*] 佐々木 貴之[2] 吉岡克成[†] 松本 勉[†]

概要：インターネットに接続可能な自動車，いわゆるコネクテッドカーが増加しており，これを狙ったサイバー攻撃の増加が懸念されているが，その実態は明らかではない．本研究では，車載器がインターネットから直接攻撃を受けるケースに着目し，その実態を調査する．まず，第一段階として広域スキャンにより実際に車載器を発見し得るかを検証する．Censys を利用した探索実験の結果，インターネットからアクセス可能な車載器が 5 種 1435 件発見された．これらの車載器の中には Telnet が動作するものも含まれ，サイバー攻撃の対象となる可能性がある．そこで第二段階として，広域スキャンにより得られた機器からの応答を用いて簡易的な低対話型ハニーポットを構築し，攻撃の観測を行った.ハニーポットに対して多くのアクセスと攻撃が観測されたものの実験の範囲では当該機器の車載器として機能を特に狙った攻撃は確認されなかった．今後，前述と同様に外部からアクセスが可能な車載器が増える可能性がある．そこで，広域スキャンによる車載器の発見，発見した機器からの応答の収集，収集した応答を用いたハニーポットの自動構築，当該機器を狙った攻撃の観測といった一連の流れをシームレスに行う，コネクテッドカーに対するサイバー脅威観測フレームワークを提案する．

キーワード：コネクテッドカー，サイバー攻撃観測，車載器，広域スキャン，ハニーポット

Are Connected Cars Discovered from The Internet?

Takahiro Ueda[1,*] Takayuki Sasaki[2] Katsunari Yoshioka[†] Tsutomu Matsumoto[†]

Abstract: As the number of Internet-connected cars (so-called "connected cars") is increasing, there are concerns about the increase of cyber-attacks targeting these cars, but the actual threats are still unclear. In this study, we focus on the case where an On-Board Equipment (OBE) is directly attacked from the Internet and investigate the actual situation. The first step is to verify whether OBE can actually be found by wide-area scanning. In the primary experiment using Censys, the Internet-wide scan system, 1435 devices of 5 different OBE products were discovered. The security of these discovered devices was not optimal, some of which even run Telnet, a well-known target of cyber attacks. Given the result from the experiment, we constructed a simple low-interaction honeypot that imitates one of the discovered OBE products using the responses collected from the actual discovered devices. We have observed frequent accesses and attacks on the honeypot although we could not confirm any attack that specifically targets the device functionality as an OBE. In the future, we should expect more cars being connected and thus targeted. Therefore, we propose a framework for observing cyber threats to connected cars that continuously searches OBE by wide-area scanning, collecting responses from the discovered devices, automatically constructing honeypots using the collected responses, and observing attacks targeting the devices.

Keywords: Connected cars，Observation of cyber-attack，OBE，Wide-scan，Honeypot

1. はじめに

近年，インターネットに接続可能な自動車，いわゆるコネクテッドカーが増加している. 自動車が IoT 機器として，他の自動車や社会インフラとシームレスに接続する事で，安心・安全な交通社会の実現や様々な新サービスの開発が活発化する事が期待されている[1].

一方でインターネット接続することにより，他の IoT 機器と同様にサイバー攻撃の対象となる危険性がある．実際に，コネクテッドカーに対する悪意のある攻撃が増加傾向にある事が報告されているが[2]，その攻撃の実態は明らかになっていない．サイバー攻撃対策のガイドラインやセキュリティ基準を確立し，安心・安全なコネクテッドカーの利用に繋げるために，攻撃実態を明らかにすることは大切である．

コネクテッドカーへのサイバー攻撃の方法としては，インターネットから直接攻撃する，スマートフォンなどを介して攻撃する，信号機や EV の充電所などのインフラを介して攻撃する，コネクテッドサービスを提供している OEM のサーバをのっとることで攻撃する，といったシナリオが考えられる．本研究では，上記の中でも実行が容易で頻度が高いことが予想されるインターネットからの攻撃に着目し，その実態を調査する．

第一段階として，そもそもインターネット接続する自動車，より正確には自動車内の車載器をインターネット経由で発

1 横浜国立大学大学院環境情報学府，Graduate School of Environment and Information Sciences，Yokohama National University
2 横浜国立大学先端科学高等研究院，Institute of Advanced Sciences，Yokohama National University
† 横浜国立大学大学院環境情報研究院/先端科学高等研究院，Graduate School of Environment and Information Sciences，Yokohama National University/ Institute of Advanced Sciences，Yokohama National University
* ueda-takahiro-ny@ynu.jp

見することがどのくらい容易であるかを実験により検証する．コネクテッドカーのインターネット接続方式は，自動車の製造時に通信モジュールを自動車内に組み込む Build-in 型と後付けで通信機能を有する車載器を自動車に取り付けることでインターネット接続を可能とする Retrofit 型の 2 種類が存在するが，現在のコネクテッドカーの多くは Retrofit 型である[11]．そのため，ルータ，ドングル，ドライブレコーダといった Retrofit 型車載器が広域スキャンにより識別可能であるかを検証する．

多くの IoT 機器と同様に，車載器もまた設定や操作を行うための管理インターフェイスを有しているが，これらは特に PC やモバイル端末での操作を行うことが容易な Web インターフェイスとして用意されることが多い．そこで広域スキャンシステムである Censys [3]により収集される大量の Web コンテンツの中から自動車に関連するキーワードを含むものを抽出する．広域スキャンは一般の Web サイトを含めて多様な Web コンテンツを収集するため，自動車関連キーワードを含むものが車載器の Web 管理画面であるとは必ずしもいえない．そこで，同一の車載器の Web 管理画面は互いに類似しているという点に着目し，収集された Web コンテンツをクラスタリングすることで，大きなクラスタを構成する Web コンテンツをもつホスト群を車載器の候補とする．これらの候補についてコンテンツから機器の製造者や製品情報を人手で調査することで車載器を発見する．車載器であることが確定した機器については，そのコンテンツの中から特徴的なキーワードを機器のシグネチャとして選び，再び Censys の広域スキャン結果内を探索し，マッチしたホスト群のクラスタリングを行う．これを繰り返すことで，車載器を検出するためのキーワードを充実させ，多くの車載器の発見を試みる．

5 種類の起点キーワードを用いて上記の手法の評価実験を行った結果，3 種類のキーワードを新たに発見し，最終的に 5 機種 1435 件の車載器が発見された．発見された機器の中には，自動車内部の車載ネットワークにも接続しているもの，認証なしの Telnet が動作しているもの，その機器特有のサービスが稼働しているものなどが存在し，サイバー攻撃の対象となる可能性があることがわかった．

そこでネットワークスキャンツールである Nmap[4]と Zgrab[5]を用いてこれらの機器のポート解放状況，サービスの稼働状況を調べ，これらの機器で動作しているネットワークサービスの応答を収集し，この応答を用いて簡易的な低対話型ハニーポットを構築した．2021 年 4 月 23 日から 2021 年 8 月 13 日まで 1 つの IP アドレスを用いてインターネット上に設置し攻撃の観測を行った結果，IoT マルウェアが感染を広げるために行っている無差別な攻撃は多数確認できたものの，この機器を明示的に狙ったと判断される攻撃は観測されなかった．

今後コネクテッドカーが増加することで，外部からアクセス可能な車載器が増加していく可能性がある．そのため，コネクテッドカーに対する脅威インテリジェンスを収集するフレームワークを提案する．提案フレームワークは広域スキャンにより継続的に車載器を探索する機能と，発見した車載器の応答を用いた簡易的ハニーポットを自動構築する機能，ハニーポットに対する攻撃から特に車載器を狙う攻撃を抽出する機能をもち，これらがシームレスに連携することでコネクテッドカーへのサイバー攻撃の実態を把握する．このフレームワークを利用することにより，インターネット上で広く利用されており実際に外部から発見が可能な車載器をいち早く把握し，それらの機器の利用実態や，それらの機器を狙った攻撃を認識することができる．さらに，車載器を狙った攻撃を観測した場合には，実機等を用いた高対話型のハニーポットの利用により，その実態をより正確かつ詳細に把握することが可能である．

以降では，2 章で関連研究について述べ，3 章で広域スキャンによる車載器の発見方法を説明し，実際のスキャン結果を示す．4 章では 3 章の内容を基に，車載器の発見からハニーポット構築をシームレスに行うフレームワークを提案し,実際にハニーポットによる攻撃観測の試行を行なった結果を述べる.5 章でスキャンを行った結果とフレームワークに対する考察を行い，最後に 6 章でまとめと今後の課題について述べる．

2. 関連研究

2.1 車載器の発見事例

インターネットに接続されている車載器の発見事例として，ホワイトハッカーによるテレマティクスゲートウェイユニット(TGU)である c4max の発見がある[6] ．この車載器はポート 23/TCP で Telnet コンソールが稼働しており，その表示には c4max 特徴である’gps’と‘welcome on console’が含まれているため，インターネット上からこれらの文字列を含む Telnet サービスをスキャンする事で容易に c4max を発見可能である．さらに，このコンソールには認証を行うこと無く侵入可能であり，この車載器が搭載されている自動車を監視，各種パラメータの取得，一部パラメータの制御などが可能であった．

2.2 インターネット上の IoT 機器の探索

インターネット上から IoT 機器を探索する取り組みは世界的に行われている．IPv4 空間全体に対する網羅的な広域スキャンを行い，IoT 機器の検索サービスを提供している Censys[3]，Shodan[7]，ZoomEye[8]がその代表例である．実際に上述した c4max に関しても Shodan を用いて発見されている．また，重要施設の遠隔監視制御に用いられる IoT 機器を発見する手法として，Web ページの類似度によるクラスタリングと施設名などのユニークワードを基に重要 IoT 機器を発見する手法[9]が提案されている．実際にこの手法では複数の重要 IoT 機器が発見されており，それらの

中には脆弱性を持つ可能性があるものも存在し，対策を行う必要がある事が示唆されている．

2.3 IoT 機器の応答を自動的に模倣するハニーポット

IoT 機器への攻撃を観測するためのハニーポットとして，X-pot[10]と呼ばれるハニーポットが提案されている．X-pot は，観測した攻撃の情報を基にインターネット上を広域スキャンする事で攻撃対象となっている IoT 機器を特定し，その Web コンテンツを収集してハニーポットに取り込むことにより，模倣する機器を拡張することができる．これにより，特定の機器を模倣するハニーポットと比較して，より多様な機器を対象とした攻撃の観測やマルウェアの収集に成功している．

2.4 自動車ハニーポットの導入戦略

ハニーポットを用いた自動車へのサイバー攻撃の実態を把握する取り組みも行われている．自動車ハニーポットによる攻撃観測の戦略を示した研究[11]では，4 段階に分けたハニーポットを提案し，1 段階目として低対話型のハニーポットを構築し，攻撃規模の拡大や攻撃手法の高度化が確認される場合，2 段階目として高対話型のハニーポットにより詳細な攻撃の観測を行う必要が出てくると主張している．3 段階については，コネクテッドカープラットフォーム全体を模擬するハニーポットが必要であり，4 段階目になると信号機などの自動車インフラなども含めた自動車関連のネットワーク全体を模倣したハニーネットが必要になると論じている．現在のコネクテッドカーの普及状況から，現状は低対話型のハニーポットでの観測を目指す事が目標となると述べている．

3. Web コンテンツに基づいた車載器の発見方法

本章では，車載器の Web インターフェイスのコンテンツを基に車載器を発見する手法を提案する．

3.1 基本アイデア

車載器の Web インターフェイスを発見する際の課題は，以下の 2 点である．

- 課題 1 : Censys などの IoT 検索サービスを利用し，車載器に関連したキーワードで検索を行うことで，車載器の可能性がある Web ページを特定することが可能である．しかし，車載器を検索するための適切なキーワードは一般的には知られていない．
- 課題 2 : 車載器以外の膨大な数の Web ページの中から車載器の Web インターフェイスを探す必要がある．具体的には，車載器以外の Web ページにも車載器に関連した単語が含まれるため，Censys 等の IoT 検索サービスの検索結果には，車載器以外の一般的な Web サイトも含まれている．

提案手法は図 1 に示すように，1 段階目として Censys のキーワードサーチを利用した Web コンテンツの収集及びクラスタリングと，2 段階目としてクラスタ中からの車載器の発見と車載器で用いられるキーワードの抽出の処理を行うことで，上記の課題を解決し，車載器を発見する．具体的には，同一モデルの車載器は同じ Web コンテンツを持つため大きなクラスタを形成する．よって，車載器の可能性が高いサイズの大きなクラスタのみを調べることで，課題 2 を解決できる．さらに，発見した車載器の Web コンテンツからキーワードを選ぶことにより，課題 1 を解決する．この 2 段階の処理を繰り返し行うことにより，多くの車載器を発見可能である．

3.2 Web コンテンツの収集とクラスタリング

3.2.1 キーワードによる Censys からの Web コンテンツ収集

インターネットからアクセス可能な車載器を発見するために，IoT 機器検索エンジンである Censys を用いる．Censys で自動車に関連するキーワードを検索し，その検索結果を IP アドレスと開いているポート及び稼働サービスの組み合わせのリストとして保存する．このリストを利用して，HTTP 及び HTTPS が稼働しているポートに対して，スキャンツール Nmap を用いてポートスキャンを行い，セッションが確立可能なホストに対して，Web ブラウザを自動的に操作する Selenium[13]を用いてアクセスし HTML ソースを取得する．

初回の検索キーワード(以下，起点キーワードとする)は，過去に購入して調査した車載器の知見を基に選び，2 回目以降は，後述する第 2 段階で発見した機器の Web ページで使用されている単語からキーワードを選択する．

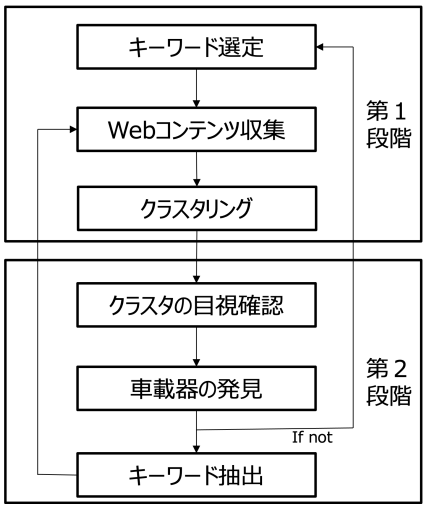

図 1　提案手法の処理手順

Fig. 1　Procedure of proposal method

3.2.2 収集したコンテンツのクラスタリング

Web ページは，Web ページの構造を規定する HTML タグと，Web ブラウザに表示される文字列に分けることができる．このうち，Web ブラウザに表示される文字列は，例えば，GPS の位置情報のように各機器で異なる可能性があるためクラスタリングには適さない．よって，Web ページの

構造を抽出するために HTML タグを抽出し，クラスタリングに用いる．クラスタリングには，fuzzy hash の 1 つである ssdeep[12]を用いて抽出した HTML タグ間の類似度を求め，階層的クラスタリングにより作成されたデンドログラムを閾値 30 でカットすることによりクラスタを生成する．

3.3 クラスタの確認とキーワード抽出

形成された複数のクラスタについて，それぞれの Web ページのコンテンツを目視で確認し，必要に応じて製品情報を Web 検索する等の方法で車載器であるか否かを判定する．判定の基準は Web ページに自動車関連の文字列が明らかに含まれているか，機器の使用用途が自動車内で使うものであるかを調査する事で判定を行う．

ここで車載器が発見できた場合には，発見した車載器の Web ページに用いられている単語から，先ほどとは異なるキーワードを選択し，Web コンテンツの収集とクラスタリングのステップに戻り，車載器の探索を継続する．仮にどのクラスタにも車載器が見受けられなかった場合，Censys で検索する際のキーワードに原因があると考え，別のキーワードを選ぶ事で再び Web コンテンツの収集，クラスタリング，クラスタの目視確認，キーワード選択を繰り返す．

3.4 調査結果

ここでは，提案手法により車載器を探索した結果について述べる．発見した車載器が攻撃の対象となることを避けるために，具体的なキーワードや機種名は開示しない．

提案手法を用いて，5 種類の起点キーワードを用いて調査を行なった結果，車載器を発見可能なキーワードとして新たに 3 種類，車載器として 5 機器，1435 件を発見する事ができた．それぞれの起点キーワードについて，クラスタリングにより生成されたクラスタ数，発見した車載器，発見した車載器から抽出されたキーワードのうち車載器を発見する事ができたキーワードの有無を，表 1 に整理した．具体的には，起点キーワード 1,3,5 を用いて，以下のように車載器を発見することができた．

- 起点キーワード 1 を用いて Web コンテンツの取得とクラスタリングを行うことで 123 個のクラスタを生成し，クラスタの中から車載器 A を発見した．更に，車載器 A の Web コンテンツに用いられている 2 つの単語をそれぞれキーワードとして利用することで，片方のキーワードは 7 個のクラスタを生成し車載器 B を，もう一方のキーワードでは 557 個のクラスタを生成し車載器 C を発見した．車載器 B と C の Web ページに用いられている単語をキーワードとしてさらなる探索を行ったが，新たな機器を発見することはできなかった．
- 起点キーワード 3 を用いて 302 個のクラスタを生成し，その中から車載器 E を発見した．更に，車載器 E に用いられているキーワードを利用して，18 個のクラスタを生成し，その中から車載器 D を発見した．
- 起点キーワード 5 を利用して，4 個のクラスタの中から，車載器 B を発見した．

表 1：探索結果

	起点キーワード	1		2	3	4	5
初期ラウンド	生成クラスタ数	123		191	182	302	4
	発見した車載器	車載器A		-	車載器E	-	車載器B
	発見した機器から抽出したキーワードのうち，新たな機器を発見できたもの	2種類		-	1種類	-	-
第２ラウンド	追加キーワードを利用して生成クラスタ数	557	7	-	18	-	-
	発見した車載器	車載器C	車載器B	-	車載器D	-	-
	発見した機器から抽出したキーワードのうち，新たな機器を発見できたもの	-	-	-	-	-	-

以下では実際に発見した車載器についての特徴を簡単に述べる．

3.4.1 車載器 A

車載器 A は 148 件確認する事ができた．カーテレマティクスに利用される機器であり，HTTP の他にも ssh サービスが動作していた．さらに，ハイポートで不明なサービスが動き，特徴的な応答を持っている事がわかった．また，デフォルトの HTTP ポートと別に HTTP サービスが稼働するポートが存在し，そちらのページでは車載器 A で稼働しているプロセスの一部を確認する事ができた．トップページの情報から車載ネットワークに接続されていると考えられる．

3.4.2 車載器 B

車載器 B は先行研究[6]で取り上げられていた車載器“c4max”であり，363 件発見する事ができた．先行研究においても説明した通り認証なしで Telnet コンソールにアクセスでき，車載ネットワークにも接続している．そのため，攻撃者によって車両情報の取得や一部の機能の制御が行われる可能性がある．

3.4.3 車載器 C

車載器 C は 290 件発見する事ができた．この機器を介すことにより，インターネットから直接に車載ネットワークにアクセスする事ができる．機器自身は，温度や速度，その他の情報を収集しており，OS アップデートなどを遠隔から行うこともできる．

3.4.4 車載器 D

車載器 D は 687 件と今回発見した機器の中で最も数が多かった．自動車内の車載ネットワークと外部のインターネットとを繋ぐゲートウェイとして使用される．HTTP サービスが稼働しており，アクセスするとログイン画面が表示される．その他のポートについては個体差があるが平均して TCP ポートが 2 ポート前後空いている事が多い．

3.4.5 車載器 E

車載器 E は 47 件発見する事ができた．表示されている文字列から車載ネットワークに接続していると予測できるが，

この機器については詳細な情報は得る事ができなかった．

3.5 車載器ではないクラスタ

車載器に関連するキーワードを持つ Web コンテンツを収集した後，クラスタリングを行なっているが，生成されたクラスタを確認すると，その大半は車載器ではなかった．車載器ではないクラスタは大きく 3 つに分ける事ができる．1 つ目は一般的な Web アプリケーションが複数の IP アドレスで動作しており，クラスタが形成される場合である．2 つ目はエラーページである．エラーページはシンプルに作られている事が多いため，全く異なる Web ページである場合でも似た様な作りになり，クラスタが形成される．3 つ目は，一般的な IoT 機器のログインページであり，最も事例が多い．IoT 機器は管理画面で ID と PASSWORD を要求する事が多く，その様な認証画面が多数存在するため，クラスタが形成される．

3.6 提案手法の改良案

提案手法により車載器を発見はできたものの，その網羅性は評価できていない．今後，より多くの機器を発見するために以下の改良案を検討している．

車載器以外のクラスタの削除：3.5 節で述べたように，生成されたクラスタの大半は車載器ではなく，エラーページや一般的 Web ページが含まれていた．この様なノイズとなるクラスタをルールベースでフィルタリングし，探索の効率化を行う．

目視で行っているクラスタの確認の自動化：現状，生成されたクラスタを，一つ一つ目視で確認することにより，車載器か否かの判定を行なっている．クラスタの数が大きくなるほど判定コストが大きくななるため，確認の自動化を検討する．

Web コンテンツに限らないクラスタリング：クラスタリングするコンテンツとして Web コンテンツに限定して調査を行なってきた．調査するプロトコルを拡張することで Web コンテンツに限らず，例えば Telnet のような特定のポートの応答を収集し，その応答をクラスタリングすることで，Web ページを持たない車載器を発見可能にする．

探索手順の変更：提案手法において，起点キーワードを指定して Web コンテンツの収集を行なっていた．この場合起点キーワードを含まないコンテンツは削ぎ落とされてしまう．この削ぎ落とされたコンテンツの中に車載器がある可能性も十分に考えられるため，起点キーワードを指定して Web コンテンツの収集するのではなく，IoT 機器が多く存在する IP アドレスレンジ（例えば，モバイル ISP など）に存在する Web コンテンツを収集することで，より多くの車載器が発見できる可能性がある．ただし，車載器以外のクラスタも多く生成されると考えられるため，上述した車載器以外のクラスタの削除や目視で行っているクラスタの確認の自動化を行う必要がある．

4. 脅威収集フレームワークの提案

３章で示したように，現時点で少なくとも５つの車載器がインターネットからアクセス可能である．今後コネクテッドカーが増加することで外部からアクセス可能な車載器がさらに増加し，より多くの機器がサイバー攻撃に晒されるリスクがある．そのため，車載器に対する攻撃を早期に観測し，対策を行うことを目的として，本章ではコネクテッドカーに対する脅威収集インテリジェンスフレームワークの提案を行う．このフレームワークは先行研究の X-pot[10] の概念を基にしているが，機器の応答収集の手法が異なる．

4.1 基本アイデア

車載器への攻撃の観測には，一般的なサイバー攻撃の観測と同様にハニーポットを利用することが可能である．車載器への攻撃をいち早く観測するためには，インターネットに接続されている車載器を正確に把握し，その機器をハニーポットで模倣できるようにする必要がある．

図 2 に提案フレームワークの基本アイデアを示す．提案フレームワークは，(1)インターネット上の車載器を探索する機器探索部，(2)発見した機器に対しスキャンを行う事で応答を収集する応答収集部，(3)収集した応答を利用して機器を模倣し，攻撃の観測を行う機器模擬部から構成される．提案フレームワークの特徴は，機器探索部でいち早く車載器を把握し，応答収集部でその車載器の Web コンテンツを収集し，機器模倣部が収集した車載器の Web コンテンツを利用することで，様々な車載器を素早く模倣可能な点にある．以降では，各構成要素について詳細を説明する．

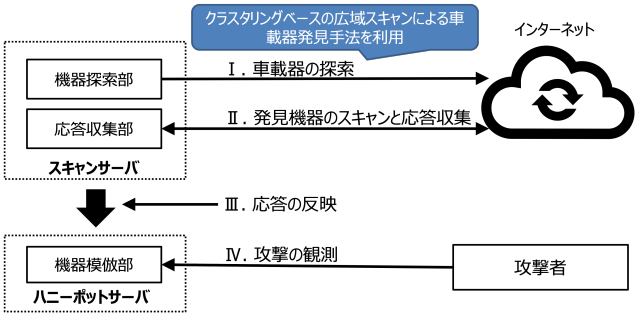

図 2　提案フレームワークの基本アイデア

Fig. 2　Basic idea of proposal framework

4.1.1 機器探索部

車載器を模倣するためには，実際にその車載器を発見する必要がある．現時点で攻撃が行われていなくてもインターネット上から発見可能な車載器であれば，今後サイバー攻撃を受ける可能性があるため，このような車載器をいち早く発見するために，3 章で提案した手法を用いて車載器を発見する．

4.1.2 応答収集部

車載器を模倣する際に，システムのディレクトリ構成，CPU アーキテクチャなどの内部情報まで詳細に作り込む

ことは非常にコストがかかる．これらの内部情報は攻撃者にとって機器への侵入後に得られる情報であり，車載器への侵入を試みる段階においては，表面的な情報のみしか攻撃者は得る事ができない．ここで表面的な情報とは，車載器のポート開放状況や稼働しているサービスの応答などである．そのため，ハニーポットにおいてもこれらの部分のみを模倣していれば，攻撃者が侵入するまでは，あたかも車載器の様に見えるため，攻撃者が興味を持って攻撃する車載器なのか否かを観測する目的には十分である．

応答収集部は，Nmap[4]と Zgrab[5]を用いることによって発見した車載器に様々なポートスキャンをかけることにより，その応答を収集する．

4.1.3 機器模擬部

応答収集部で収集した応答をハニーポットの応答としてハニーポットに追加する．これによりインターネット上から見ると車載器を模擬した動作を行うことが可能である．

4.2 ハニーポットによる観測例

上記の提案フレームワークによるハニーポットの実装例の一つとして，先行研究[6]により発見されている車載器“c4max”を模倣したハニーポットを構築し，2021 年 4 月 23 日から 2021 年 8 月 13 日までインターネット上に公開し観測を行った．観測の結果，IoT マルウェアなどからの自動化されていると思われる無差別な攻撃は多数観測する事ができたものの，この車載器を明示的に狙った攻撃を観測することはできなかった．

5. 考察

車載器のサイバー攻撃リスクの低減．3 章で述べたように，提案した車載器探索手法によって 5 機器 1435 件の車載器を発見した．コネクテッドカーが攻撃を受けるリスクを低減するためには，この様な探索によって発見されない事が望ましい．そのため，車載器の Web コンテンツで不用意に車載器を推測するキーワードを載せない，Web コンテンツのアクセスには認証をかけ，シンプルなログイン画面のみを公開する，特定のアドレス帯にのみ Web コンテンツを公開するなどの対策をとり，発見を未然に防ぐ構成とする事が大切である．

ハニーポットの設置戦略．先行研究[11]にも示される様に，自動車のハニーポットとして，まずは低対話型のハニーポットを作成し，コネクテッドカーに対する攻撃者の興味の度合いや，攻撃者の数を調査し，次のステップで攻撃の詳細を観測する手段として高対話型のハニーポットを作成する戦略は合理的である．4 章の提案手法を用いる事で，インターネット上で広く利用されており実際に外部から発見が可能な車載器をいち早く把握し，それらの機器の利用実態や，それらの機器を狙った攻撃を認識することができる．さらに車載器を狙った攻撃を観測した場合には，実機等を用いた高対話型のハニーポットの利用により，その実態をより正確かつ詳細に把握することが可能になると考える．

また，先行研究[6]で脆弱性が確認されている 1 機器についてはハニーポットを設置したが，観測期間内において攻撃は確認されていない事から，少なくとも現時点でこの機器について高対話型のハニーポットを設置する意義は薄いのではないかと考えられる．しかし，今後この機器が攻撃対象となる可能性があるため，引き続き観測を続ける．

6. まとめと今後の課題

本稿では，クラスタリングと HTML 内のキーワードを組み合わせる事で，インターネット上に存在する車載器を発見する手法を提案した．提案手法を用いた調査の結果，実際に車載器を発見する事が可能であり，8 つの自動車関連キーワードを基に 5 種 1435 件の車載器を発見した．これらの中には車載ネットワークに接続していると思われるものもいくつか存在していた．加えて，インターネットに接続されている車載器への攻撃をいち早く，より多くの機器を対象とした攻撃を観測するための仕組みとして，車載器の発見から低対話型ハニーポットの構築までを自動的に行うフレームワークを提案した．フレームワークを使用した例として，1 機器のみ低対話型ハニーポットで攻撃観測を行った．現時点では，IoT マルウェアが感染を拡大するための無作為なアクセスは多数あるものの，車載器を明示的に狙った攻撃は観測できていない．

今後の課題として，車載器の発見段階におけるクラスタの目視確認の自動化や Web コンテンツ以外を利用したクラスタリング方法の検討による探索性能の向上，今回調査できていないキーワードによる探索が挙げられる．これらの点を改善する事でより多くの車載器を発見し，攻撃実態の把握につなげることを目指す．

7. 研究倫理

本研究は，インターネット上で車載器を発見する事が可能である技術のため，サイバー攻撃に悪用される恐れがある．そのため，発見した個々の機器については特定される事が無いよう詳細情報を匿名化している．本研究は，将来的に発見可能な車載器が出てきた際にいち早く攻撃観測機構を構築し，コネクテッドカーに対するサイバー攻撃の実態を明らかにすることを期待し発表を行うものである．

謝辞

本研究の一部は，内閣府戦略的イノベーション創造プログラム(SIP)第 2 期/自動運転(システムとサービスの拡張)/新たなサイバー攻撃手法と対策技術に関する調査研究の支援を受けて行われた．

参考文献

[1] 富士経済．コネクテッドカー(つながる車)の世界市場の調査．https://www.fuji-keizai.co.jp/file.html?dir=press&file=20061.pdf&nocache．(参照 2021/08/16)

[2] UpStream．UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYVERSECURITY REPORT 2021．https://info.upstream.auto/hubfs/Security_Report/Security_Report_2021/Upstream_Security-Global_Automotive_Cybersecurity_Report_2021.pdf?_hsmi=101240621&_hsenc=p2Anqtz-8p40YfRUbH2ImFBItWnTWLfA_KNjsB2oPKE_L-5OBvfLlaUDZjL-_LbxykqgJH3GK_du0Q6CX07IetDrAKUIe_5GHFew, (参照 2021/08/16)

[3] ‘Censys’， https://censys.io . (参照 2021/08/23)

[4] ‘Nmap’， https://nmap.org．(参照 2021/08/23)

[5] ‘Zgrab’， https://github.com/zmap/zgrab2．(参照 2021/08/23)

[6] Jose Carlos Norte．“Hacking industrial vehicle from the internet “．http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html．(参照 2021/08/18)

[7] ‘Shodan’， https://www.shodan.io．(参照 2021/08/23)

[8] ‘Zoomeye’，https://www.zoomeye.org．(参照 2021/08/23)

[9] 内田佳介，藤田彬，吉岡克成，松本勉．管理 WebUI のカスタマイズに着目した遠隔監視制御用機器の探索手法．暗号と情報セキュリティシンポジウム(SCIS2020)．電子情報通信学会，2020

[10] 加藤誠也，森下瞬，田辺瑠偉，吉岡克成，松本勉，広域スキャンで収集した応答を用いた全ポート待受型 Web ハニーポット．コンピュータセキュリティシンポジウム(CSS)2019，情報処理学会，2019

[11] Yvonne Maria Schmitz ． A strategy for vehicular honeypot. https://www.researchgate.net/publication/333132722_A_strategy_for_vehicular_honeypots．(参照 2021/08/23)

[12] ‘ssdeep’， https://ssdeep-project.github.io/ssdeep/index.html. (参照 2021/08/23)

[13] ‘selenium’． https://www.selenium.dev/ja/documentation/．(参照 2021/08/23)