SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

車載システムに対するデジタル・フォレンジックに向けての一考察 ～車載インフォテイメントシステムについて～

A Study on Digital Forensics for in-vehicle System

味岡 仁雅* 倉地 亮† 佐々木 崇光‡ 黒﨑 雄介* 片山 隆成* 下雅意 美紀*
Yoshimasa Ajioka Ryo Kurachi Takamitsu Sasaki Yusuke Kurosaki Takanari Katayama Miki Shimogai

キーワード 自動車セキュリティ，デジタル・フォレンジック，車載インフォテイメントシステム

あらまし

近年の自動車には多数の電子機器が搭載され，そのサイバーセキュリティについても関心が高まっている．先行研究においては，車載 Event Data Recorder（EDR）に着目し，その電磁的記録が車両へのハッキングの痕跡となり得ることが示された一方，EDR 単体の記録では攻撃の全容を明らかにすることが困難な点が課題とされた．そこで今年度の研究においては，EDR に加え車載インフォテイメントシステムの電磁的記録にも着目することで，デジタル・フォレンジックの精度を向上させる可能性について検討を行った．

本研究においては車載電子機器であるインフォテイメントシステムが不正アクセスを受け，不正な CAN 信号が送出され，事故が誘発された攻撃モデルを想定した．

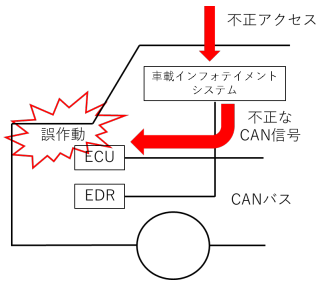

図 1. 想定した攻撃モデル

本攻撃モデルを想定した場合，先行研究のとおり EDR の電磁的記録から，車載ネットワークに攻撃があったことや事故を起点とした経過時間を取得できる可能性がある．一方で，不正アクセスに使用された IP アドレスやアカウント情報，不正な CAN 信号の実データ等については，車載インフォテイメントシステムの電磁的記録を含め広く調査する必要が生じる．そこで本研究においては，攻撃の全容解明に必要と思われる電磁的記録を Five Ws（いわゆる 5W）に沿って分類した上で，現状で取得可能な電磁的記録や今後新たに取得すべき電磁的記録について考察し，表 1 のように整理した．ここで，車載インフォテイメントシステムは Linux ベースの OS が稼働していることを想定している．

表 1. デジタル・フォレンジックにおける電磁的記録

	デジタル・フォレンジックに必要となる電磁的記録	EDR	インフォテイメントシステム	
			既存	新規
When	各イベントの時刻情報	△	○	-
Where	不正なCAN信号の送出元機器	×	×	○
	攻撃対象	△	△	-
Who	攻撃に使用されたアカウント情報	×	○	-
	ハッキングに使用されたIP	×	△	-
What	不正なCAN信号の実データ	△	×	○
	電子機器内で実行されたコマンド	×	○	-

○：取得可能　△：部分的な情報のみ　×：取得不可
※「Why」については推測となる部分が大きいため除外

結果として，車載インフォテイメントシステムにおけるネットワーク関連の syslog や dmesg，アカウント情報としての wtmp や faillog といったログを参照することで，EDR 単体では困難であった攻撃の全体像に関わる電磁的記録を補完できる可能性が示された．加えて，CAN の実データ等を新たに記録する仕組みを設けることで，よりデジタル・フォレンジックの精度を向上できるものと思われる．

* 警察大学校，東京都府中市朝日町 3-12-1，
National Police Academy, 3-12-1, Asahi-cho, Fuchu, Tokyo, Japan.
† 名古屋大学，愛知県名古屋市千種区不老町，
Nagoya University, Furo-cho, Chikusa-ku, Nagoya, Japan.
‡ パナソニック株式会社，大阪府門真市大字門真 1006，
Panasonic Corporation, 1006, Kadoma, Kadoma City, Osaka, Japan.