

# 窃盗犯による車両制御 は可能か？

## 車両防盜システムへの ハッキングアタック



### 車両電子システムのハッキングは新たな盜難手法となり得るか？

本書では窃盗犯が車両システムへのアクセスにコンピューターハッキングを行う危険性について取り上げています。今後採用される車両アーキテクチャや通信を分析し、さまざまな実配線および無線接続でのハッキングの危険性について検証します。ハッキングの危険性については既に注目されており、既存システムの脆弱性が指摘されつつあります。本書では現在のハッキング手法および今後脅威となり得る手法について解説しています。

自動車メーカーおよびサプライヤは新しい通信システム概念を考慮し、現在開発段階にある車両が販売された時点での盜難の危険性について理解する必要があります。本書は窃盗犯による新しい技術の悪用を未然防止する為にお役立ていただけます。



本書では以下のような内容を取り上げています。

- 新しい通信および接続技術によって増す車両の脆弱性の洞察
- 車両アーキテクチャの弱点を検証し、ハッカーによる悪用についての理解
- 車両ハッキングアタック調査チームによる研究で使用されたハッキング手口
- ハッキングに対して防盜上有効なソリューションの提示

詳細に関するお問い合わせは、下記にて承っております。

SBD ジャパン

太田千絵

e-mail : cohta@sbdjapan.co.jp / Tel : 052-253-6202



## 車両ハッキングの脅威が増加

車両技術および車載電子システムは近年急速に進歩しており、車の大部分の機能は電子制御ユニット (ECU) への依存度をますます高めています。車外インフラ (オフボード) との通信レベルの向上に伴い、こうした車両への電子的ハッキング攻撃の脅威が増えています。

こうした技術の発展が車両の性能、排ガス、安全性、利便性の向上・改善に貢献していることは間違いありませんが、コンピューターの専門家は外部と接続している ECU の不正操作に対するセキュリティ対策について懸念を示しています。ナビゲーションやリモート診断と言った便利なシステムには、ネットワークを経由して車両内部の重要な安全・防犯装置と通信できる、あるいは通信するよう設計されているものがあります。

オンボード通信は、多数のアフターマーケット診断用ツールがある点から見ても、不正アクセスを防止するように設計されているとは言えません。脆弱なネットワークへ車外からの接続を可能にすることは、ハッカーに CAN Bus のオフボードシステム又は通信プロトコルを攻略し、車両の重要なセントラルシステムへ不正にアクセスするチャンスを与えてしまう可能性を高めます。これまでの調査でも実配線および無線接続でのハッキングが可能である事は明らかで、エンジン、ブレーキ、イグニッションなどの制御が可能となっています。

想定されるハッキングアクセス経路

車両接続	アクセスポイント	所要技術レベル	必要な侵入/接近レベル	接続の難しさ
実配線	OBD ポート	高	車内	難
	CAN ケーブル	高	車内	中
	HEV 充電ケーブル (データ転送兼用設計の場合)	未知 (まだ実用化されていない)	車外	未知 (まだ実用化されていない)
無線	RF 通信	高	リモート (狭域)	中
	SMS メッセージ	高	リモート (広域)	中
	Bluetooth	中	リモート (狭域)	難
	インターネット	低	リモート (広域)	容易

車両防犯上のリスクレベル: ■ 高 ■ 中 ■ 低

出典: SBD, 2011 年

車載電子システムや無線通信を追加することでハッカーが侵入する可能性が増します。自動車メーカーやサプライヤはこのレベルの操作を防止する為のセキュリティプロトコルを組み込む必要があります。本書では車へのアタック手法としてのハッキングについて取り上げ、現在のハッキング技術と、今後 7 年を見据えた車両アーキテクチャと発生し得るアタック手法とツールについて考察・検証しています。

SBD では、車両ハッキングが将来的に脅威になる可能性があるとしており、窃盗犯に悪用される可能性のある通信経路からセキュリティと安全システムの分割、防御性に優れた強固なオンボードシステムソフトウェア開発、設計の初期段階からのセキュリティ対策などを推奨しています。

本書では以下のような疑問について解説しています。

- 車両ハッキングは現時点で脅威なのか？
- 車両へハッキング攻撃が成功した場合に可能となる操作は？
- 車両ハッキングは容易に行えるのか？どのような知識・設備が必要なのか？
- システムの統合とオープンなアーキテクチャのハッキングへの影響は？

# »» ...know what tomorrow brings

## 目次

1. 要旨
  - 1.1 はじめに
  - 1.2 結論
  - 1.3 推奨事項
2. アーキテクチャの弱点
  - 2.1 実線接続
  - 2.2 無線接続
  - 2.3 車両技術
    - 2.3.1. インフォテインメント
    - 2.3.2. テレマティクス
  - 2.4 アクセス経路のまとめ
3. 新しい技術および動向
  - 3.1 車両側
  - 3.2 インフラ
  - 3.3 窃盗ツール
4. 車両ハッキングアタック
  - 4.1 調査研究1: 接続型車両制御ユニット
  - 4.2 調査研究2: TPMS (タイヤ空気圧監視システム)
  - 4.3 調査研究3: 警察の車載監視システム
  - 4.4 一般のハッキング事例
  - 4.5 有効なハッキング手口のまとめ

## 5. ハッキングのリスク

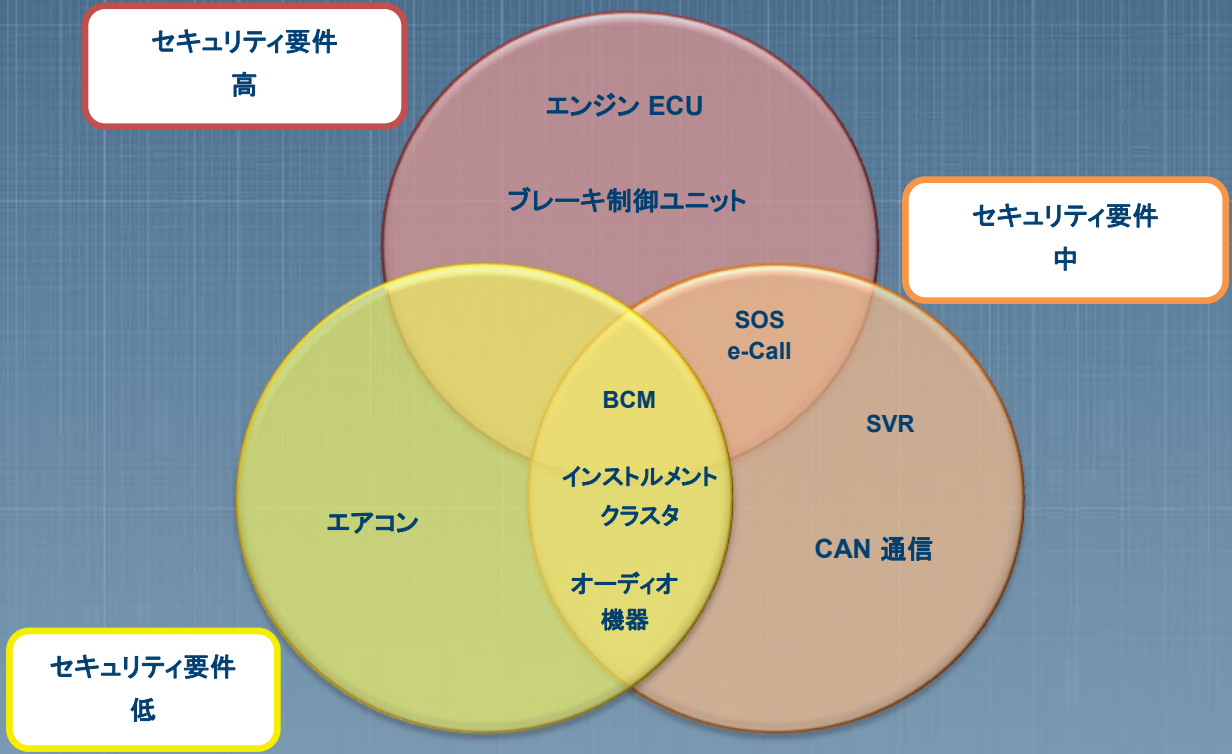
- 5.1 ハッキングが今後深刻な脅威となる理由
- 5.2 車両の制御

## 6. 防盜性向上策と防護策

### 図表一覧

- 図 1. CANアーキテクチャの発展
- 図 2. インフォテインメントシステムの接続性拡大
- 図 3. テレマティクス通信ルート
- 表 4. 想定されるハッキングアクセス経路
- 図 5. 隊列走行システムのコンセプト
- 図 6. TPMSアタックツール
- 表 7. 有効なハッキングアタックの手口
- 図 8. 車両ハッキングのリスク: 現在と将来
- 図 9. 車両オンボードシステムの重要度分類
- 図 10. ECUパーティショニング: ボデー制御モジュール

車両オンボードシステムの重要度分類



# SBD の基本理念

SBD は 1995 年の設立以来、自動車業界向け技術動向調査レポートやエンドユーザー調査といったサービスをグローバルに展開し、お客様の戦略構築をサポートしています。

SBD の技術エキスパートチームが、お客様の状況を正確に把握し、各国の市場ニーズ・技術要件の理解と費用対効果の高い製品開発を支援します。

## 本書の著者について



クレイグ・ベスト: 自動車セキュリティ テクニカルアナリスト

ラフバラ大学で自動車工学を専攻し、自動車設計に関する幅広い知識を有する。SBDの各プロジェクトでは広範な調査に携わり、SBD独自の調査データベースの分析・管理も担当している。現在は世界の盗難統計と自動車技術情報を専門に手掛けている。

## 本書のご購入形態

※下記は税抜価格です

レポート名	日英対訳版 製本+PDFレポート
窃盗犯による車両制御は可能か? 車両防盜システムへのハッキングアタック (SBD/SEC/2312)	¥ 405,000

お問い合わせは下記まで

SBD ジャパン

担当: 太田 千絵

Eメール: [cohta@sbdjapan.co.jp](mailto:cohta@sbdjapan.co.jp)

Tel: 052 253 6202

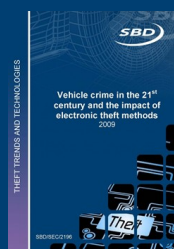
## 関連サービス

車両盗難アタック対策をより強固なものにするために

SBD の製品テストサービスを、貴社製品に対する最新盗難手法の脅威の検証にお役立てください。自動車セキュリティおよび認証・テスト基準に関する知識と経験をもとに、明確な戦略アドバイスを提供し、実際の盗難手法に対して有効な防盜対策の策定をサポートします。

SBD の製品テストおよび開発サポートサービスの詳細につきましては **SBD ジャパン** ([太田/cohta@sbdjapan.co.jp/052-253-6202](mailto:cohta@sbdjapan.co.jp)) までお問い合わせください。

## 関連レポート



今世紀の車両犯罪と電子的盗難手法による影響

車両盗難の傾向は、地域レベルの小規模グループから、国際的な規模で活動する、より本格的な犯罪組織によるものへと移行してきています。さらに現在では診断用、修理業界向けの自動車セキュリティシステム情報に、独立企業がアクセスできるようになっています。SBD では、自動車業界および関連業界に、変わりゆく盗難傾向についての認識と次世代自動車に対する新たな防犯戦略の必要性を促す目的から、本書を発行しました。

レポート番号: SBD/SEC/2196