



SBD 2021年Q4版  
サイバーセキュリティ最新動向ガイド  
発行年月：2022年1月  
148ページ | CYB905-224

## 目次 (2021年Q4版)

### はじめに 要旨 車への攻撃

車両の内部ネットワークおよびアプリケーションに関連する攻撃の分析 (Teslaの走行データ保管システムからのデータ抽出、ブートローダーセキュリティをバイパスするEMFIパルス攻撃、CAN周辺クロックへのCANnon攻撃、他2015年以降に発表された攻撃事例32件を掲載)

### バックエンド/スマートフォンアプリへの攻撃

バックエンドおよびその他のオフボードシステムに関連する攻撃の分析 (Pod PointのEV充電アプリユーザーにデータセキュリティリスク、Schneiderの充電ステーションのリモートroot化、他2016年以降に発表された事例18件を掲載)

### 自動車エコシステム全体における攻撃

OEMの組織全体および自動車サプライチェーンに関連する攻撃の分析

## 関連レポート

### サイバーセキュリティ法規制ガイド

レポート番号: CYB539

本書「サイバーセキュリティ法規制ガイド」では、法規制が車載およびオフボードの自動車システムのどの部分にどのような影響を及ぼすのかについて詳細な分析を行う。欧州、米国、中国、日本における政府の義務化、ガイドライン、標準による影響および機会を特定。これら以外の国においても法規制に関する重要な進展が見られた場合は適宜、情報を提供する。



Cyber Security

レポート番号: CYB905

# サイバーセキュリティ 最新動向ガイド

UNECE WP29自動車サイバーセキュリティ法規では、サイバーセキュリティ管理システムのプロセスによりセキュリティが適切に考慮されていることを証明することが求められ、それにはリスク管理や対策だけでなくサイバーセキュリティインシデント事例の脅威や脆弱性情報などのモニタリングも含まれます。

UNECE法規のAnnex 5 では、脅威に関連する脆弱性および軽減策を車両やバックエンドサーバー、通信の脅威など7つのカテゴリでリスト化しており、OEMはそれらを考慮する必要があります。

本レポートでは、自動車のハッキング事例を挙げながら、それらがAnnex 5 のどの項目に該当するかを分類しており、こうした情報が自社製品にどのように関連するのかを参照することが可能です。またそれらの事例に対し、サイバーセキュリティゴールおよびセキュリティ要件を含めた脅威の緩和策の推奨策、ISO21434で採用されることになるCAL(Cybersecurity Assurance Level)での基準も含めて整理しており、ハッキング事例を技術面およびリスク管理面の両方からわかりやすくまとめています。

### 対象市場

欧州 北米 中国  
日本 グローバル その他

### レポート発行頻度

  ①  
毎年更新 四半期更新 ワンタイム

### レポート形態

     
PDF PowerPoint Excel Online

### ページ数

  
130+

# 実際のハッキング事例を分類・解説

アセット	サブアセット										
車両	キー FOB										
利用される脆弱性											
コードの署名、キー FOB のファームウェア更新の認証、ペアリングのセキュリティの欠如											
SBD の ASDL 脅威 レーティング	<table border="1"> <tr> <td>1. 深刻</td> <td>2. 重要</td> <td>3. 中</td> <td>4. 低</td> <td>5. なし</td> </tr> <tr> <td>✓</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	1. 深刻	2. 重要	3. 中	4. 低	5. なし	✓				
1. 深刻	2. 重要	3. 中	4. 低	5. なし							
✓											
WP.29 の表 A1 に記載された脅威の説明を参照											
大分類	小分類										
<ul style="list-style-type: none"> <li>4</li> <li>6</li> </ul>	<ul style="list-style-type: none"> <li>7</li> <li>26</li> </ul>										
セキュリティ制御による脅威の緩和											
サイバーセキュリティの目的	サイバーセキュリティの要件	対象	要件カテゴリー	CAL							
BCM のキー FOB ペアリングプロセスをセキュアなものにする	キー FOB のペアリングに使用される認証情報が有効であることを確認する	BCM	ソフトウェア	1	2	3	4				
ファームウェアコードに Tesla の改ざんに強い暗号署名があることをキー FOB で確認する	キー FOB のファームウェア更新にコード署名を導入する	キー FOB	ソフトウェア				✓				

UNECE 法規の要求に沿った形で資産を定義

脅威レベルを5段階でレーティング

UNECE の Annex5 に基づく脅威分類を表記

脅威の緩和策を ISO21434 で採用される CAL (Cybersecurity Assurance Level) の分類に基づき記載

※本書「COSICによるTesla Model XのBLEキー攻撃」ページより

# SBDカスタマーポータル

ご契約いただいたレポートへはお客様専用ポータルサイトからアクセスいただけます。

100+ Reports published per year  
50k+ Slides of insights, forecasts & data  
4,000+ # of auto professionals who access our reports

ポータルサイトのアカウントはご契約企業ごとに作成され、ご契約企業に所属する方であれば登録ユーザー数に制限はございません。

ご契約状況の確認や、ポータルサイトへの新規ユーザー登録をご希望の場合は、SBD Automotive ジャパンまでお問い合わせください。



SBDカスタマーポータル

## 本書に関するお問合せ・お見積り依頼

### 「サイバーセキュリティ最新動向ガイド」

お問合せ・お見積り依頼



サンプルレポートの無料ダウンロード



2021年Q4版  
サイバーセキュリティ最新動向ガイド

発行年月：2022年1月  
レポート番号：CYB905-214