

WP.29/2020/79制定で義務化される セルラ通信を使用する車載機向け サイバーセキュリティ脆弱性評価方法

シグナリングテスト MD8475B

コネクテッドカーの普及に伴い重要性を増すサイバーセキュリティ

近年、自動車にセルラ通信を使用した車載器が搭載され、交通情報の取得や遠隔での車両状態監視、スマートフォン連携などのサービスを提供するアプリケーションが展開されています。

こういったアプリケーションを使用して、運転がより快適で安全なものになるような取り組みが各自動車メーカ、車載器メーカによって行われています。しかし、自動車がより便利になる一方で、サイバー攻撃に対するセキュリティ面での問題が顕在化しており、自動車のセキュリティ脆弱性評価が重要性を増しています。

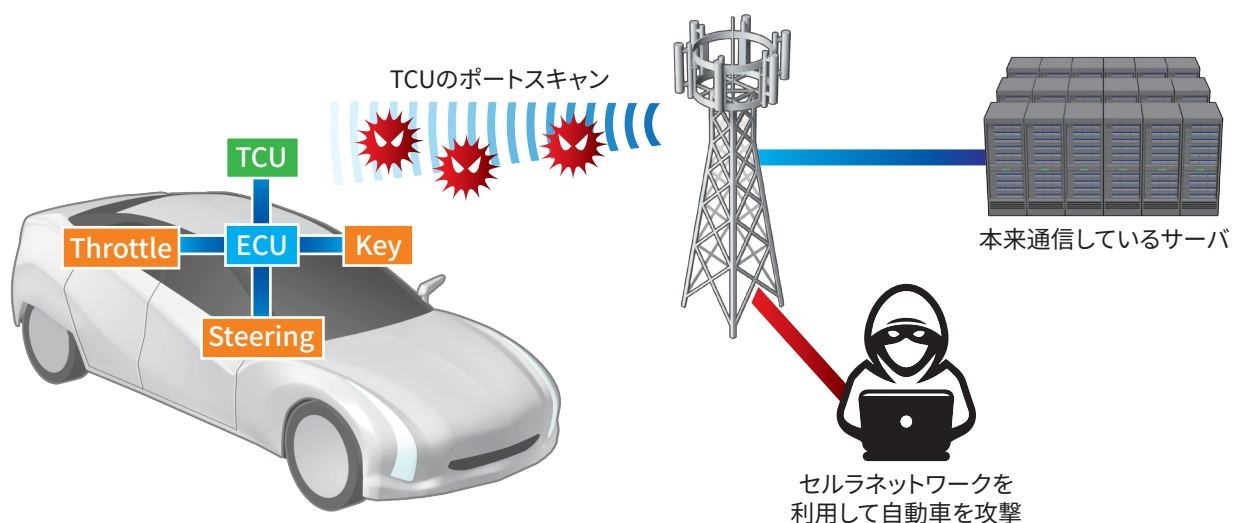


図1：TCUへのポートスキャンを使用したサイバー攻撃

実際にTCU (Telematics Communication Unit) へポートスキャンを実施して、自動車の制御を乗っ取るといったようなサイバー攻撃を受けるリスクがあります。セルラ通信を利用したサイバー攻撃の例として、下記のような事例が報告されています。

- ・ 自己診断用ポートのドングル経由による、SMSでの自動車遠隔操作
- ・ CS (Circuit Switched) フォールバックを悪用した、音声通話、SMSの乗っ取り

義務化されるWP.29/2020/79の認証プロセス

自動運転技術の進歩に伴い、サイバーセキュリティは、ますます重要な課題となっています。

国際連合・国連欧州経済委員会のもとに設立された自動車基準調和世界フォーラム WP.29は、サイバーセキュリティに関する規則、ECE/TRANS/WP.29/2020/79を制定し、ISO/SAE 21434で具体的な規格を定義します。各自動車メーカーや車載器メーカーには、法規と規格に則った組織とシステムづくり、また、自動車には型式認証が求められます。



アンリツの基地局シミュレータ MD8475Bを利用したセキュリティ脆弱性評価

サイバーセキュリティに脆弱性がある自動車が出回ってしまうと重大な事件や事故に繋がりがねません。

アンリツは、基地局シミュレータ MD8475Bを利用した、セルラ通信経由での車載器向けサイバーセキュリティ脆弱性評価方法を提案いたします。

アンリツの基地局シミュレータ MD8475Bとサイバー攻撃模擬ソフトウェアを組み合わせることにより、実環境と同等の条件下で、セルラ通信経由のサイバー攻撃の耐性を評価できます。

* 組み合わせ可能な製品、評価可能な脆弱性については、担当営業にお問い合わせください。

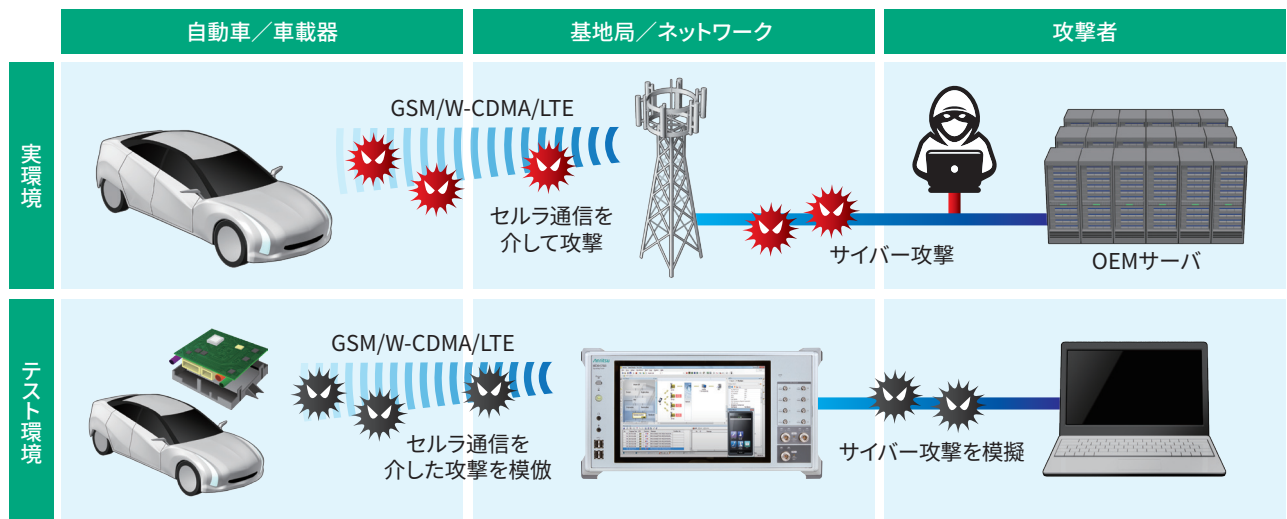


図2：実環境とテスト環境

他サイバーセキュリティ評価への応用

MD8475Bは、さまざまなセキュリティ評価システムと組み合わせることができ、ポートスキャン以外のサイバー攻撃に対する脆弱性の評価にも応用できます。

アンリツは現在、DoS攻撃や、なりすましSMS、ファームの改ざんといったさまざまな無線環境下での脆弱性診断を実現する取り組みを実施しております。