知って欲しい防犯対策

自動車盗手口【CAN インベーダー】

公益社団法人　日本防犯設備協会　自動車・オートバイ委員会

＜はじめに＞

テレビのニュースその他マスコミなどで高額車両盗難の事件をよく耳にするようになりました。

その中では近年様々な盗難手口の名称が出てきています。リレーアタック、コードグラバー、キープログラマー等々。それらの中でも特に最近話題になっているものに「CANインベーダー」があります。

CANインベーダーは比較的短時間に自動車を盗むことが可能なツールであるというのが特徴で、海外で購入ができるという情報があります。これらによりCANインベーダーによる犯罪が増えてきているのだろうと考えています。

＜CANインベーダーはどういうもの?＞

CANは「Controller Area Network」の略称で、自動車で一般的に使用されている通信です。

元々は車両の自己診断機能（OBD2）の標準化に伴い利用されるようになり、現在ではほとんどの自動車に使用されています。CANは各機能ユニット間で通信信号を並列接続（バスライン）し、それらユニットを制御します。例えば、スピードメータ、ヘッドライト、エアバッグ、ミラー調整などのあらゆる制御機器には同じ信号線に様々な通信データが行き来しています。CANインベーダーではCANに接続して同様に接続されている、ドアの鍵モータ、エンジン制御のユニットらを動かしてしまおうというものです。

しかし本来、エンジンは容易に始動できないように暗号化された信号をもって制御しています。CANインベーダーの中には特種な信号データを出力することによりエンジン始動を可能にしているものがあります。CANの通信線だけですので簡単に接続可能で、ドアを開錠し、エンジン始動がいかに容易にできてしまう事がおわかりになることでしょう。CANへの接続は比較的容易な前輪フェンダー部を外してヘッドライトユニットへの配線を利用するケースが多いようでカーメーカーは対策を急いでいるとの情報を得ています。

＜対策は?＞

どの分野のセキュリティでもそうですが、完璧に安全!というものはありません。守る側、盗る側の知恵比べのようものが繰り返されているのが実情です。自動車標準装備のセキュリティは、犯人らにはその解除方法が知られる可能性があります。このＣＡＮインベーダーはまさしくその例であり、最近になってから容易に解除されてしまうようになりました。自動車に装備されている機器は、「同じ場所」「同じ配線」「同じ機能」で標準化されているので、犯人にとって盗む作業も標準化でき容易になります。その中において、盗る側にとっての「面倒さ」は防御効果が高めです。下記のような複数のセキュリティ対策を組み合わせて施すことはその意味で適っています。

・機械（物理）的ロック装置（タイヤロック、ハンドルロックなど）
・通信型駐車監視機能付ドライブレコーダー
・後付カーアラーム装置
・位置情報装置（ＧＰＳ通信機など）
・駐車場所（ゲート、防犯カメラなど）

ハンドルロック

タイヤロック

＜まとめ＞

ＣＡＮインベーダーは直接車両のコンピューター制御にアタックされる手口であるため、ユーザーがＣＡＮインベーダーについて直接の対策をするのは困難です。前述ように複数のセキュリティ対策をすることで結果、ＣＡＮインベーダーからの被害を受けるリスクを減らすことが現状の得策です。

また、自動車盗難に合わないためには、従来からの基本的な対策や注意を怠らないこともとても重要になります。

その他の盗難手口であるリレーアタック、コードグラバー、キープログラマー等については、「自動車セキュリティガイドＶＯＬ.3」を参照ください。