特集● IoT、Big data と交通／論説

コネクティッドカーのセキュリティ

竹森敬祐*

スマートフォンやネットワークと連携することで、遠隔操作や自動運転を実現するコネクティッドカーへの期待が高まる中で、つながるが故のサイバー攻撃への脅威が指摘されている。車両のセキュリティ対策には、製造～利用～廃棄までの長いライフタイムの中で、さまざまな開発者、所有者、整備員が関わる特有の難しさがある。本稿では、車両セキュリティに関わる組織論と技術論を概観し、特に技術の基本となるElectronic Control Unit（ECU）向け鍵管理、Virtual Private Network（VPN）の構築、セキュアな診断・リプログラミングについて掘り下げてみる。

Security for Connected Car

Keisuke TAKEMORI*

Smartphone apps can be used to control multiple functions of a car as well as providinga self-driving mode that is controlled via remote systems. As a lifetime of a car is very long cyber-attacks can be a serious threat. Adding security countermeasures can be proven difficult due to i various developers, owners, and maintenance operators participating in the creation of the car. In this paper, security management systems and techniques to combat cyber-attacks for the connected car are surveyed. Basic security techniques, i.e., cipher-key management of electronic control units (ECUs), virtual private network (VPN), secure diagnosis and reprogramming, will be discussed.

1．はじめに

スマートフォン（以下、「スマホ」とする）から車載エアコンなどの遠隔操作、走行ログの収集による開発支援、通信と交通インフラが連携する自動運転など、車両にスマホがつながり、車両がネットワークにつながるコネクティッドカーへの期待が高まっている。しかし、外部機器やネットワークと連携するが故に、サイバー攻撃へのリスクが潜在する。2010年ころから、研究レベルでの攻撃事例が多く発表されるようになり、リモートPCからの侵入や運転操作の乗っ取り、成り済ましスマホからの不正操作などが報告されてきた[1)～7)]。もし、ちまたを走る車両にこうした攻撃が突然仕掛けられると、人命、財産、プライバシーが脅かされることになる。このため事前の防御、攻撃の検知、迅速な回復などの対策が喫緊で求められている。しかし、車両のセキュリティ対策の設計には、製造～利用～廃棄までの長いライフタイムの中で、さまざまな開発者、所有者、整備員が関わる特有の難しさがある。特に、サプライヤー（以下、SUP）、車両メーカー（以下、OEM）、板金店の間で、電子制御装置（Electric Control Unit：ECU）の組み付け、交換、リプログラミングをセキュアに行う必要があり、暗号鍵の管理、セキュアな通信、診断ツールや作業の管理が課題となる。

本稿では、昨今の車両に対する攻撃事例を振り返るとともに、セキュリティに関する組織論と技術論について公開資料から概観する。その中から、セキュリティ技術の基本となる(i) ECU向け鍵管理、(ii) 車外とのVirtual Private Network（VPN）通信、(iii) セキュアな診断・リプログラミングについて、例を挙げて掘り下げてみる。(i)～(iii) を適切に設計・

* 株式会社KDDI総合研究所
KDDI Research, Inc.
原稿受付日　2017年6月16日
掲載決定日　2017年7月19日

実装することで、他に実現したい機能やサービスへの応用も可能になる。

2．車両に対する攻撃事例

2－1　偽のECUを取り付けるローカル攻撃

自動運転が期待されるコネクティッドカーでは、正規のECUに、正規のソフトが搭載され、正規品以外のECUから制御を受け付けない仕組みが必要である。しかし、診断ポートから、Controller Area Network（CAN）を便利にモニター・制御するアフターマーケット品が出回る中で、こうした物品の不具合や悪意の制御への不安がある。また、CANのハーネスをタップして、偽のCANパケットを注入する攻撃や、ECUコードの改ざんによる運転妨害が実験レベルで検証されるようになってきた[1)～6)]。

2－2　スマホ連携の弱点を突くリモート攻撃

スマホから車載Wi-Fiスポットへ接続し、ドアロック解除を行えるサービスがある。これに対して、悪意のWi-Fiスポットが偽の公開鍵証明書をスマホに渡して組み込ませ、スマホからの車両操作の通信をこのWi-Fiスポットに引き込むことで、スマホと正規のサーバーとの間に割り込むMan-in-the-Middle攻撃が発表された[7)]。この攻撃で、サーバーからスマホに発行されるアクセス認証子であるトークンが盗聴され、盗んだトークンを用いて成り済ましスマホからドアロックが解除された。

2－3　不正な診断・リプログラミング

販売店や板金店で行われている診断･リプログラミングの構成を**Fig. 1**に示す。診断ポートに専用のツールを接続し、セキュリティアクセスの認証を経て、Central GWで隔たれた先にあるECUの診断やリプログラミングを行う。使い方次第で、速度リミッターの解除や燃調変更によるエンジン出力の増加、安全運転支援システムの解除など、望ましくないリプログラミングが可能である。ローカルな作業であり、誰が、どの車両に、何を実施したのか、OEMで把握できず、故障や事故発生時の原因の切り分けが難しくなる課題がある。

3．サイバーセキュリティのベストプラクティス

車両に対するさまざまな攻撃実験を受け、米国運輸省（National Highway Traffic Safety Administration : NHTSA）から、“Automotive Industry Cybersecurity Guidance”として、OEMにおける開発プロセスや体制構築の在り方、具体的なセキュリティ技術対策について公表された[8)]。**Table 1**に項目を列挙する。

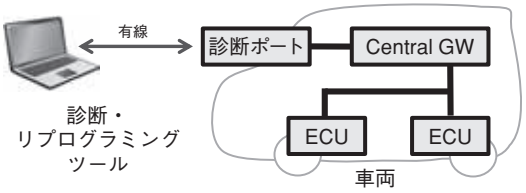

Fig. 1　診断･リプログラミングツールによるローカルなメンテナンス

Table 1　NHTSAセキュリティベストプラクティス

1	Vehicle Development Process with Explicit Cybersecurity Considerations（セキュリティを考慮した開発プロセス）	
2	Leadership Priority on Product Cybersecurity（優先決め）	
3	Information Sharing（情報共有）	
4	Vulnerability Reporting/Disclosure Policy（脆弱性の公表）	
5	Vulnerability / Exploit / Incident Response Process（インシデントレスポンス）	
6	Self-Auditing（自己監査）	
	1	Risk Assessment（リスク評価）
	2	Penetration Testing and Documentation（ペネトレーションテスト）
	3	Self-Review（自己レビュー）
7	Fundamental Vehicle Cybersecurity Protections（セキュリティ要素技術）	
	1	Limit Developer/Debugging Access in Production Devices（開発者の制限）
	2	Control Keys（鍵管理）
	3	Control Vehicle Maintenance Diagnostic Access（診断アクセスの保護）
	4	Control Access to Firmware（F/Wの保護）
	5	Limit Ability to Modify Firmware（不正なリプログラミング対策）
	6	Control Proliferation of Network Ports, Protocols and Services（通信サービスの制限）
	7	Use Segmentation and Isolation Techniques in Vehicle Architecture Design（ネットワークの分離）
	8	Control Internal Vehicle Communications（制御信号の保護）
	9	Log Events（ログの収集と監査）
	10	Control Communication to Back-End Servers（サーバー -to-車両間のセキュアな通信）
	11	Control Wireless Interfaces（無線インターフェースの管理）
8		Education（社員教育）

本稿では、上記に紹介した対策技術のうち、特に重要な鍵管理、セキュアな通信、セキュアな診断･リプログラミングについて事例を挙げて、次章から掘り下げてみる。

4．ECU向け鍵管理

車載ネットワークの堅牢化に向け、CANパケットへのCipher-based Message Authentication Code（CMAC）付与や[9),10)]、正規ECUの認証、ECUコード

のリモートリプログラミングなどの研究開発[11)～13)]が進められている。これらを実現するには、ECUへの暗号鍵の設定･管理が必要となる[14)]。本章では、車両向けセキュアエレメントの代表格であるSecure Hardware Extension（SHE）に準拠したマイコンへ安全に鍵を設定する際の考え方を紹介する。

4－1　SHE

初めに、SHEレジスターに設定する鍵とその略号、鍵の役割を**Table 2**にまとめる[15)、16)]。

- MASTER_ECU_KEY（MEK）
  MEK、BMK、KEY_nを更新するための鍵。
- BOOT_MAC_KEY（BMK）
  Start／Endアドレスで指定される一つのコード領域に対するセキュアブートの期待値（CMAC）を算出する鍵。BMの更新にも用いられる。
- BOOT_MAC（BM）
  セキュアブートの期待値（CMAC）。
- KEY_n
  CMAC算出もしくは暗号･復号のいずれかの用途を指定して、総計10個まで設定される鍵。例えば、KEY_1にCMAC算出用の鍵（MAC）を、KEY_2に暗号･復号の鍵（ENC）を設定する。
- RAM_KEY（RMK）
  RAMに一時的に設定して利用する鍵。電源OFFで消去されるが、高速アクセスが可能。

4－2　鍵設定の単位

次に、鍵の設定単位について考える。もし統一的な鍵を全ての車両やECUに設定してこれが漏えいした場合には、CMACやECU認証の危殆化が全車両に及んでしまう。では、セキュリティを重視して、全てのECUに異なる鍵を設定する場合には、SUPやOEMの生産ライン、市場での保守作業、CANでのCMAC検証において、個々のECUを識別しながら鍵を特定する煩雑な対応が必要となる。車両間で異なるものの、車両内のECU間では共通の鍵を設定する場合、漏えい時の影響は対象車両のみとなり、鍵管理も車両単位で良いことから、生産や保守、CMAC検証が比較的容易となる。これらの考察を**Table 3**にまとめる。MEK、MAC、ENCは、車両単位で発行するのがリーズナブルといえよう。

次節より、正規ECU／コードの認証、車両単位での鍵の設定、板金店での交換ECUへの鍵の設定について考える。

4－3　SUPでの鍵設定

SUPでは、ECUが正規品であること、コードを改造されていないことを保証するために、鍵更新に利用されるMEK、セキュアブートに利用するBMKとBMに、SUPごとに割り当てられた鍵と、これから算出される値を書き込んでおくと良い。MACとENCは、初期値のままで良い。この様子を**Fig. 2**に記す。

Table 2　SHE準拠の鍵管理レジスターとその用途

	鍵更新	暗号復号	CMAC	セキュアブート
MEK	✓			
BMK	✓			✓
BM				✓
KEY_n	✓	✓	✓	
RMK		✓	✓	

Table 3　MEK、MAC、ENCに関する設定の単位

単位	管理の容易性（コスト）	漏えい時の影響（セキュリティ）
OEM	OEM単位で鍵を設定する。全車両のECUで同じ鍵を持つ。 コスト：小	攻撃者の解析結果が、他車両まで影響する。 影響：大（リコール）
車両	車両単位で鍵を設定する。車両内のECUは同じ鍵を持つが、他車両とは異なる鍵となる。 コスト：中	漏えい車両の全ECUを制御できる。ただし、解析者の自己責任の範ちゅうと見なされ得る。 影響：小（該当車両）
ECU	ECU単位で鍵を設定する。全てのECUで異なる鍵を持つ。 コスト：大	漏えいECUを制御できる。重要なECUが狙われると車両単位と同じ影響となる。 影響：小（該当車両）

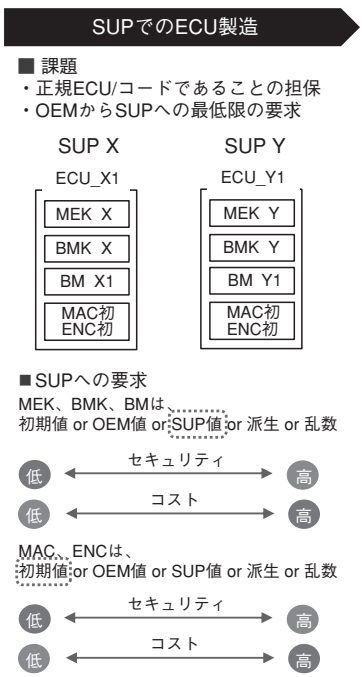

Fig. 2　SUPでの鍵設定の一例

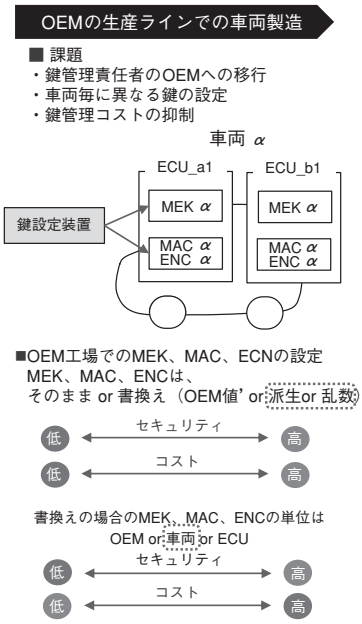

Fig. 3　OEM生産ラインでの鍵設定

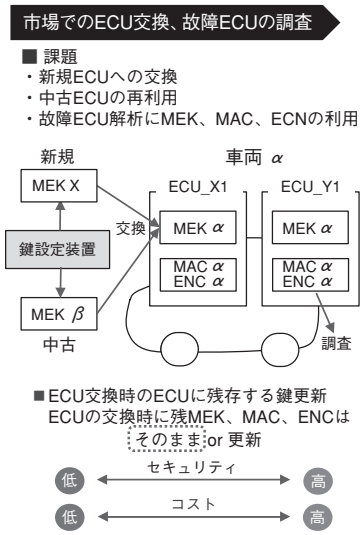

Fig. 4　販売店／板金店での鍵設定

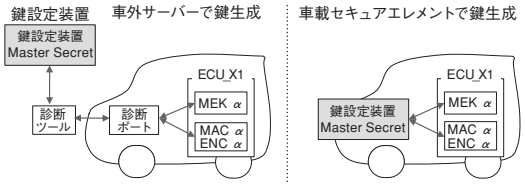

Fig. 5　サーバー型鍵生成と車載型鍵生成

4－4　OEMでの鍵設定

前節で、SUP鍵もしくは初期値が書き込まれたECUがOEMに納品される。ここで、走行安全やデータ通信に関わるMEK、ENC、MACについて、OEMしか知らない鍵へと置き換えることで、鍵管理の責任者をSUPからOEMへ移行する必要がある。その際、車両単位の鍵に書き換えることで、漏えい時の影響を抑える。

そこで、出荷車両のセキュリティに関わるMEK、MAC、ENCを、OEM以外の第三者が知り得ないように、MEKについてはSUP固有値から、MACとENCについては初期値から、個車鍵へと更新する。更新は、車両単位で、安全性とコストに鑑みて乱数鍵もしくは派生鍵とする。ここで派生鍵とは、派生する際の種として、OEMが秘匿管理するMaster Secretと、車両識別子（Vehicle Identification Number : VIN）の組み合わせから、

派生鍵＝ダイジェスト（Master Secret、VIN）

のように生成される鍵である。OEMがMaster Secretを安全に管理しておくことで、ECU交換の際に、板金店からVINの通知を受けると、当該車両に設定されている個車鍵を算出して通知できる、メンテナンスに適した特性を持つ。この様子を**Fig. 3**にまとめる。

4－5　販売店／板金店での鍵設定

ちまたを走る車両のECUが故障した場合には、販売店や板金店で新品もしくは中古品のECUへと交換する必要がある。その際、新たに取り付けられるECUに設定されているMEK、ENC、MACの鍵値を使って、該当車両の鍵値へと書き換える必要がある。この様子を**Fig. 4**に示す。

Fig. 4では、鍵設定装置が新品もしくは中古のECUに設定されているMEK、ENC、MACを把握して、これを用いて対象車両の個車鍵を設定する様子を示している。もし派生鍵が設定されている場合には、対象車両のVINから車両 α の個車鍵を算出できる。その際、新品ECUへと交換する場合は、SUP鍵や初期鍵を用いて個車鍵 α を書き込むと良い。中古ECUへと交換する場合は、旧車両 β のVINを鍵設定装置に入力することで、旧個車鍵を算出でき、これを用いて対象の個車鍵 α に書き換える。

4－6　サーバー型と車載型の鍵設定装置

Fig. 5に、鍵設定装置を、車外のサーバーとするモデル、車両に搭載するモデルを示す。

サーバー型は、攻撃者の目に触れにくい長所があ

る半面、車両と鍵設定装置を接続する必要があり、OEMの生産ラインへの影響や、世界中に分布する販売店や板金店に通信ネットワークを整備する必要がある。通信を利用できないへき地で、簡単にECUを交換できない課題がある。

車載型は、鍵設定装置が攻撃者の目に触れやすい短所がある。特に、Master Secretと鍵の派生関数を内包する鍵設定装置の場合、これらの漏えいに対する脅威が潜在する。その半面、鍵設定が車両内で自己完結するため、OEMの生産ラインへ与える影響が小さいこと、販売店や板金店、もしくはへき地でのECUの交換作業の手順が変わらないなどの長所がある。

4－7　ECU向け鍵管理の考察

本章では、正規ECUの認証、CANパケットへのCMAC付与、ECUコードのリモートリプログラミングなどで必要となるECU向け暗号鍵の設定について、さまざまなモデルを振り返ってみた。鍵設定には、SUPとOEMの責任境界を勘案しつつ、安全性とコスト、市場保守のバランスを加味することが重要である。鍵設定サーバーを守り切ることで鍵管理の安全性を保つ考え方、セキュアエレメントの堅牢性を頼りに車載化して、生産や保守の担保を軽くする考え方などがある。

5．通信のセキュリティ

本章では、車両-to-サーバー、車両-to-サーバー-to-スマホ間のVPNを堅牢にする仕組みについて考える。なお、スマホ-to-車両をWi-FiやBluetoothによる近距離無線を介した直接的な接続構成は、脆弱性が露見した場合において、すぐに停止させるなどのリカバリーが難しく、人命や財産の侵害に至りかねない車両には望ましいモデルとはいえないため、ここでは検討から外す。

以下では、まず初めに暗号の強度について振り返り、その後、車両-to-サーバー、車両-to-サーバー-to-スマホ間のVPNの構築について、図例を挙げて考えてみる。

5－1　暗号アルゴリズムと鍵長

VPNの構築には、RSAに代表される認証や鍵共有、AESに代表されるデータの暗号化が欠かせない。IPAから、各種アルゴリズムと鍵長の耐性について、2030年を基準に利用の可否が報告されている[17]。AES128は、2030年以降も安全とされているが、RSA2048は、新規車両への適用は不可であり、既存車両の互換性のためには許容とされている。鍵長は長いほどセキュリティ強度は高まるが、処理時間を要し、非力なマイコンではメモリ使用量の関係から動作が不安定になる。これから出荷され、そこから10年以上のライフタイムを持つ車両に搭載される暗号アルゴリズムと鍵長について、設計と運用指針をあらかじめ決めておく必要がある。

例えば、VPNをRSA2048で構築しつつ、これとは独立したAES128の事前共有鍵を用いて、データの暗号化を併用する。ライフタイムの短いスマホやPCでは、VPNだけで十分であったが、車両についてはデータの暗号化を追加するなどの多層防御の考え方もあり得る。

この他、まずはRSA2048を適用しつつ、2030年ころに、通信サービスの見直しと併せて暗号アルゴリズムを強化するために、高性能なTelecommunication Unit（TCU）へと交換するなどの計画もあり得る。

5－2　車両-to-サーバー間のVPN

車両-to-サーバー間のVPNの構築には、サーバー認証、クライアントである車両認証を経たVPNの構築が必要である。その際の認証に用いる鍵は、堅牢なセキュアエレメントで保護する必要がある。この様子を**Fig. 6**に示す。**Fig. 6**では、TCUとサーバー間で、サーバー公開鍵証明書／秘密鍵とクライアント公開鍵証明書／秘密鍵を用いたVPNの構築と、サーバーと車両が事前に共有された共通鍵を持つVPNの構築について記している。

公開鍵／秘密鍵を用いるVPNの場合、車両ごとにクライアント証明書の発行と、ペアを成す秘密鍵を安全に保持する仕組みが必要である。Certification Authorityの公開鍵証明書を安全に管理しつつ、高い堅牢性を有するSIMやTPMなどのセキュアエレメントクライアント秘密鍵を保管すると良い。

事前に共有された共通鍵を用いるVPNの場合、車両ごとに異なる共通鍵の発行と、安全に保持する仕組みが必要である。これについても同様に、堅牢

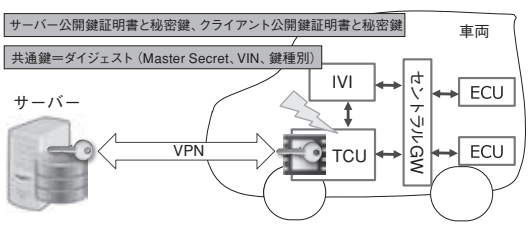

Fig. 6　車両-to-サーバーのVPN

なセキュアエレメントで管理すると良い。SIMを用いたVPNの構築の事例については、携帯通信事業者の世界的な業界団体であるGSMAから、ホワイトペーパーが公開されている[18]。

なお､本来であれば､通信を行う車載アプリとサーバー間でエンド-to-エンドのVPN構築が望ましい。しかし、アプリ内に鍵を安全に隠し込む難しさや、隠し込めない場合にアプリを搭載するIn-vehicle Infotainment（IVI）やECUの個々にセキュアエレメントを搭載するコスト的な課題がある。そこで、車載ネットワークは信頼できると仮定して、車両からの出口であり、SIMを搭載するTCUで、VPNを終端する考え方もあり得る。

5－3　車両-to-サーバー -toスマホ間のVPN

車両にとって、成り済ましスマホからの操作を受け付けるわけにはいかない。そこで、正規のスマホと車両を安全にバインドする仕組みについて、**Fig. 7**の処理シーケンスを例に考えてみる。

【初期設定フェーズ】

1）IVIやインパネの画面に、サーバーのURL、当該車両のVIN、車両が発行したトークンを含む２次元バーコードを表示し、スマホで読み取る。
2）車両とサーバー間で VPNを構築する。そして、VINとトークンを通知することで、スマホがサーバーへアクセスしてくることを知らせる。
3）スマホとサーバー間でVPNを構築する。そして、SIM／スマホ固有の識別子であるICCID/IMEI、２次元バーコードで読み取ったVINとトークンをサーバーに送付する。
4）サーバーは、車両から送られてきたVINとトークンと同じ値であることを確認する。
5）車両操作の際のアクセス認証に用いるパスワードをスマホから設定させる。デフォルト値としてトークンとしておき、これをユーザーに変更させても良い。そしてサーバーは、ICCID/IMEI、VIN、パスワードを管理する。

【操作フェーズ】

1）スマホとサーバー間でVPNを構築する。そして、スマホからサーバーへICCID/IMEI、パスワードを送付する。
2）サーバーは、ICCID/IMEIとパスワードでスマホを認証し、バインドされているVINを確認する。
3）サーバーから車両にSMSを送付するなどして、車両を呼び起こし、サーバーへのVPN構築を促す。
4）スマホからサーバーへ車両の操作コマンドを送付し、サーバーはこれを車両へ転送する。
5）車両は操作コマンドを実行し、結果をサーバーへ返送する。サーバーはこれをスマホへ転送する。

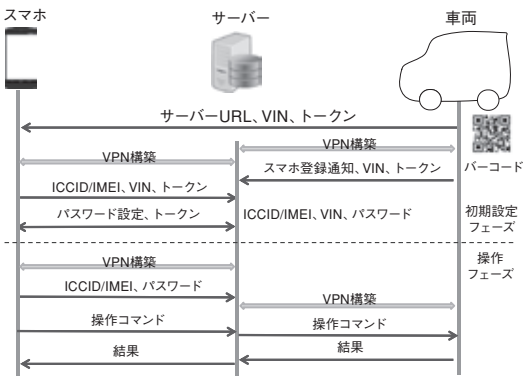

Fig. 7　スマホと車両のバインド･シーケンス

6．診断・リプログラミング

現在、ECUの診断やリプログラミングは、整備士が専用のツールを診断ポートに接続して、ローカルな作業として行われている。この場合、誰が、どの車両に、何を行ったか、ログを一元管理できるようにはなっていない。

本章では、作業員を認証し、診断・リプログラミングの認可を与える仕組みについて、**Fig. 8**を例に紹介する[19]。その際、診断ツールが主体となってコマンドを発行する構成と、Webサーバーが診断・リプログラミングの主体となる構成の二つを例に考える。なお、管理サーバーと車両には、認証・認可のための暗号鍵を生成する種となるMaster Secretと暗号鍵生成式を安全に保持するためのセキュアエレメントを具備するものとする。また、正確な日付も保持できる仕組みを持つものとする。

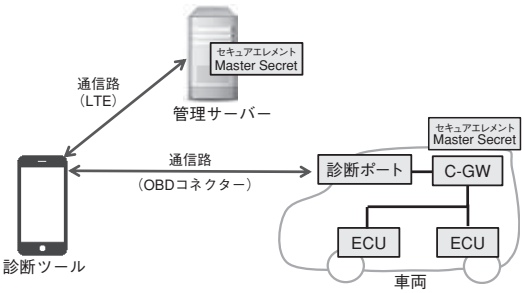

Fig. 8　サーバー連携型の診断･リプログラミング

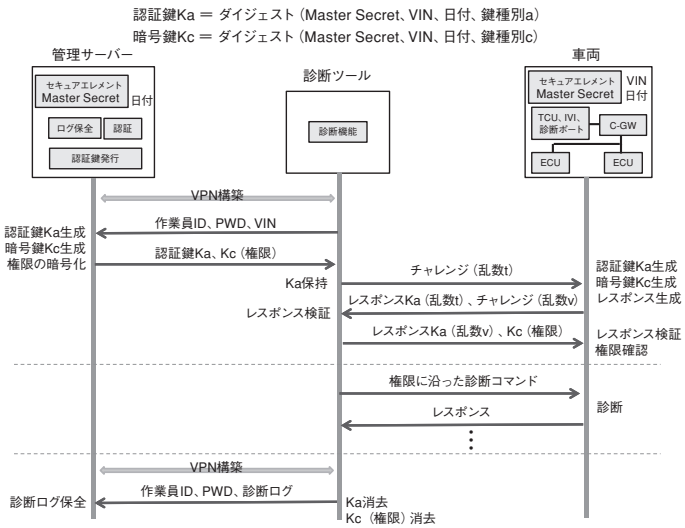

Fig. 9　認証･認可型のローカルツール主体の診断･リプログラミング

6－1　ローカル診断・リプログラミング

ここでは**Fig. 9**を例に、診断ツールから管理サーバーに、作業員ID、パスワードによる認証を経て、VINと日付から生成される鍵を用いて、ローカルで行われる診断･リプログラミングを認可する処理シーケンスについて考える。

【作業員の認証フェーズ】

1）診断ツールと管理サーバー間でVPNを構築する。以後、診断ツールとサーバー間の通信は、VPNを通じて行われるものとする。
2）作業員が、診断ツールから管理サーバーへログイン（ID/PWD）を行う。このとき、診断対象車両のVINをサーバーへ通知する。
3）サーバーは、K＝ダイジェスト（Master Secret、VIN、日付、鍵種別）で算出される認証鍵Kaと暗号鍵Kcを生成する。
4）サーバーは、認証鍵Kaと、作業員の暗号化された権限Kc（権限）を診断ツールに返信する。

【診断ツールの認証フェーズ】

1）診断ツールから車両へ、チャレンジ（乱数t）を送付する。
2）車両は、K＝ダイジェスト（Master Secret、VIN、日付、鍵種別）で算出される認証鍵Kaと暗号鍵Kcを生成する。
3）車両は、認証鍵Kaで、レスポンスKa（乱数t）を生成する。
4）車両から診断ツールへ、レスポンスKa（乱数t）、チャレンジ（乱数v）を送付する。
5）診断ツールは、認証鍵Kaでレスポンスka（乱数t）を検証し、かつレスポンスKa（乱数v）を生成する。
6）診断ツールから車両へ、レスポンスKa（乱数v）と、暗号化された権限Kc（権限）を送付する。
7）車両は、認証鍵Kaでレスポンスka（乱数v）を検証し、暗号鍵Kcで権限を復号する。

【診断フェーズ】

1）診断ツールから車両へ、作業員の権限に合わせた診断コマンドを発行する。
2）車両から診断ツールへ、診断結果が送付される。

【診断ログ保全と完了処理】

1）診断が終了すると診断ツールと管理サーバーの間でVPNを構築する。
2）診断ツールは、VIN、診断ログを管理サーバーへ送付する。
3）診断ツールは、認証鍵Ka、Kc（権限）を消去する。管理サーバーは、診断ログを保全する。

ここで、認証鍵KaとKc（権限）を消去する理由は、これらを蓄積しておき、車両の日付を認証鍵KaとKc（権限）が発行された日に狂わせることで、いつでも診断・リプロを行えてしまう攻撃を防ぐためである。

作業員によっては、サーバーへの完了処理を行わないこともあり得る。これに対しては、次回の診断の際にサーバーへアクセスするタイミングで、前回の診断結果を送付して、不要となった認証鍵KaとKc（権限）を消去する仕組みを設けると良い。

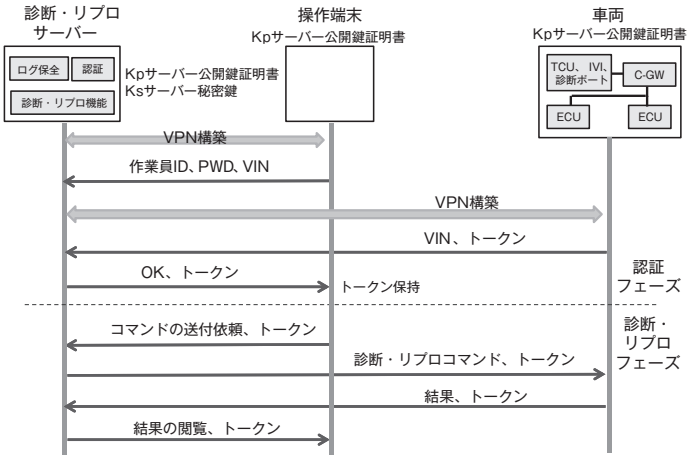

Fig. 10　認証･認可型のサーバー主体の診断・リプログラミング

6－2　リモート診断・リプログラミング

ここでは**Fig. 10**を例に、診断機能を管理サーバーに搭載して、管理サーバーから発行される診断･リプログラミングコマンドを操作ツールで中継して車両に届ける処理シーケンスについて考える。

【作業員の認証、準備フェーズ】

1）操作端末と診断･リプログラミングサーバー間のVPNを構築する。以後、操作端末とサーバー間の通信は、VPNを通じて行われるものとする。
2）作業員が､操作端末からサーバーへログイン(ID/PWD）を行う。その際、対象となる車両のVINを通知する。
3）操作端末を土管として、車両とサーバー間のVPNを構築する。以後、車両とサーバー間の通信は、VPNを通じて行われるものとする。
4）車両からサーバーへ、VINとトークンを送付する。
5）サーバーから操作端末へ、トークンが渡される。これを診断･リプログラミングのセッション管理に用いる。

【診断･リプログラミングフェーズ】

1）作業員は、サーバーから操作端末に送られてくる診断･リプログラミングのウェブ画面を通じて、車両へのコマンドを、トークンを添えて要求する。
2）サーバーは要求されたコマンドを、トークンを添えて車両へ送信する。
3）車両で診断･リプログラミングコマンドが実行され、結果を、トークンを添えてサーバーへ返送する。
4）サーバーから操作端末へ結果が送られる。

7．おわりに

本稿では、コネクティッドカーのセキュリティ対策として、組織論と技術論があることを概観し、中でも重要な鍵管理技術、セキュアなVPN構築技術、認証･認可型の診断･リプログラミング技術について、図例を挙げて考えてみた。長いライフタイムの中で、さまざまな開発者、保守者、所有者が関わる車両のセキュリティを一貫して守るためには、暗号アルゴリズムの選定に始まり、セキュアエレメントの搭載、ログの保全や認可のためのサーバー連携を考える必要がある。

脆弱性の発覚や時間の経過に伴いセキュリティ技術の危殆化も進む。本稿では深掘りできなかったが、技術だけでは解決できない組織論としてのインシデントレスポンス体制の構築、セキュリティ考慮の開発プロセスの整備、ログの定期的な監査についても、併せて考えていく必要がある。

参考文献

1）Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T. : Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy, May, 2010
2）Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. : Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security, August, 2011
3）畑正人、田邉正人、吉岡克成、大石和臣、松本勉

「不正送信阻止：CANではそれが可能である」情報処理学会、CSS2011、pp.624-629、2011年10月
4）Miller, C. : Adventures in Automotive Networks and Control Units, DEF CON 21, August, 2013
5）Miller, C., Valasek, C. : Survey of Remote Attack Surfaces, July, 2014
6）Miller, C., Valasek, C. : Remote Exploitation of an Unaltered Passenger Vehicle, Black Hat USA 2015, August 2015
7）「スマホの通信を乗っ取って自動車を解錠してエンジンをかける脆弱性が発覚、GMはすでに対処済みを発表」Gigazine、2015年７月31日
►http://gigazine.net/news/20150731-ownstar/
8）NHTSA: Cybersecurity Best Practices for Modern Vehicles, October, 2016
►https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf
9）竹森敬祐、溝口誠一郎、川端秀明、窪田歩「セキュアブート＋MACによる車載制御システム保護」電子情報通信学会、ITS研究会、2014年９月
10）AUTOSAR: CANへのMAC付与、2014年10月
►http://www.autosar.org/fileadmin/files/releases/4-2/software-architecture/communication-stack/standard/AUTOSAR_SWS_SecureOnboardCommunication.pdf
11）Idrees, M. S. : Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates, In Communication Technologies for Vehicle, pp.224-238, Springer, 2011
12）Klimke, M. : Secure and seamless integration of Software Over the Air（SOTA）update in modern car board net architectures, 13th ESCAR EU, November, 2015
13）溝口誠一郎、竹森敬祐、川端秀明、窪田歩「セキュアなリモートリプログラミング方式の実装」情報処理学会、CSS2016、2E1-2、2E3-2、2016年10月
14）竹森敬祐、溝口誠一郎、窪田歩「車載ECU向け暗号鍵管理」電子情報通信学会、SCIS2017、2017年1月
15）STMicroelectronics : Introduction to the Cryptographic Service Engine（CSE）module for SPC56ECxx and SPC564Bxx devices
►http://www.st.com/content/ccc/resource/technical/document/application_note/f6/9a/a2/ed/e5/3a/48/37/DM00075575.pdf/files/DM00075575.pdf/jcr:content/translations/en.DM00075575.pdf
16）EVITA Project: Hardware Security Module
►http://www.evita-project.org/
►http://www.evita-project.org/Publications/AEHR10.pdf
17）IPA「SSL/TLS暗号設定ガイドライン」2015年8月
►https://www.ipa.go.jp/files/000045645.pdf
18）GSMA : Solutions to Enhance IoT Authentication Using SIM Cards（UICC）, Using a SIM Card to Verify the Integrity of Firmware Updates
►http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/cl_iot_authenticate_report_web_11_16.pdf
19）竹森敬祐、溝口誠一郎、窪田歩「サーバー型セキュア診断・リプログラミングシステム」電子情報通信学会、ITS研究会、ITS2016-91、2017年3月