クルマのサイバー攻撃対策技術

近年，インターネット経由などで遠隔から自動車を不正に操作できることを実証した実験が発表されるなど，自動車へのサイバー攻撃は現実社会において深刻な問題となっており，自動車の安心・安全を守るセキュリティ対策技術が早急に求められています．本稿では，世の中の自動車のセキュリティ対策技術の動向，およびNTTセキュアプラットフォーム研究所の自動車のセキュリティ評価技術や対策技術の取り組みについて紹介します．

田中　政志（たなか　まさし）　/高橋　順子（たかはし　じゅんこ）
大嶋　嘉人（おおしま　よしひと）
NTTセキュアプラットフォーム研究所

自動車へのサイバー攻撃

近年，自動車のシステム化が進み，自動車のさまざまな機能が車載ネットワーク上に接続された多数の車載制御コンピュータであるECU（Electric Control Unit）によって電子制御されています．また，車載機器が外部のネットワークとつながることで，コネクティッドカーや自動運転など外部の情報を活用した多種多様な自動車サービスの創出が期待されています．

一方で，自動車のシステム化や車載機器と外部ネットワークの接続が急速に進んだ結果，自動車においてもサイバーセキュリティが大きな問題となりつつあります．近年，世の中に影響を及ぼした自動車へのサイバー攻撃に関する事例を以下に紹介します．

■電子キー偽造による自動車盗難

現在の多くの自動車には，盗難防止システムであるイモビライザーが搭載されています．イモビライザーは，電子キー内の電子チップと車両側のマイコン間で暗号演算による認証を電子的に行い，認証が通ればエンジンを始動できるというシステムです．この認証にメーカ独自の暗号アルゴリズムを用いているものがあり，攻撃により認証に用いる秘密鍵が不正に入手できるという報告もされています．

■OBD2ポート経由の車両の不正操作

自動車の診断を行うインタフェースであるOBD2（On Board Diagnosis second generation）ポートに，データ取得用デバイスおよびPCを接続し，車内通信でやり取りされるメッセージ〔CAN（Controller Area Network）メッセージなど〕を取得・解析することで，そのときの自動車の挙動と合わせて該当メッセージの意味を推測することが可能です[1]．推測に基づいて偽造したメッセージをPCから挿入することで，ブレーキやハンドルを運転者の意図に反して操作したり，スピードメータ表示を改ざんしたりできることが実際の自動車で実証されました．

■遠隔からの車両の不正操作

2015年にクライスラーの「Cherokee」をインターネット経由でハッキングして遠隔地からブレーキなどの操作をする実験に成功したことが発表されました[2]．自動車内のOBD2などの通信インタフェースに直接触れることなく，遠隔からカーナビシステムを経由して自動車へ侵入し，制御にかかわるシステムを不正に作動させたことは自動車業界に大きな衝撃を与えるとともに，100万台規模のリコールという大きな被害を与えました．

上記の事例のように，自動車へのサイバー攻撃は財産や生命を侵害する問題を引き起こし，現実社会に多大な影響を与えます．よって，安心・安全な社会インフラの実現に向けて自動車のサイバー攻撃に対するセキュリティ対策の取り組みが求められています．

次に，自動車のサイバーセキュリティに関する対策技術の動向とこれまでのNTTセキュアプラットフォーム研究所の取り組みについて紹介します．

自動車のセキュリティ対策技術の動向

近年発売されている自動車で一般的になりつつある車載システムの構成とセキュリティの観点からの階層分類を**図1**に示します．

■車載システムの構成

⑴　階層1

階層1は，外部と通信を行う役割を持ち，モバイルネットワークやWi-Fiなどの近接無線通信機器，あるいは，車々・路車間通信（V2X通信など）機器と接続し，外部と通信を行う外部通信機器から構成されます．

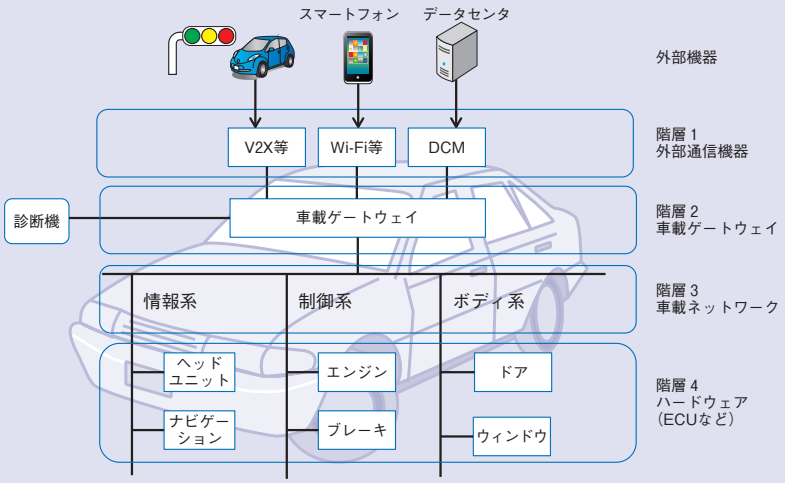

図1　車載システムの構成と階層分類

⑵　階層2

階層2は，車載システム全体を制御する役割を持ち，階層1を経由して行われる外部と車内のECUとの間のメッセージ交換，あるいは，車載ネットワークの間をまたいだ車内のメッセージ交換を制御する車載ゲートウェイで構成されます．

⑶　階層3

階層3は，ECU間でやり取りされるメッセージを伝送する役割を持ったネットワーク（車載ネットワーク）であり，カーナビなどが属する情報系や，ブレーキなどが属する制御系，ドアロック機能などが属するボディ系など，ECUの用途や役割に応じて複数の車載ネットワークに分割して配備されます．CANやLIN（Local Interconnect Network）など，系に応じた車内通信プロトコルが採用されます．

⑷　階層4

階層4は，エンジンや，ブレーキ，ドアロック機能など自動車の各コンポーネントを制御し，各種機能を実行するECUなどから構成されます．

■各階層のセキュリティ

⑴　階層1（外部通信機器）のセキュリティ

通信先である車外のシステムが信頼できる，あるいは，通信することがあらかじめ許可された相手であることを確認したり，それ以外の車外システムとの通信を遮断したりするための認証ならびにアクセス制御が挙げられます．また，車外システムとの間で確立した通信路上で盗聴されたり，不正なメッセージが挿入されたりすることを防ぐための通信路の暗号化も必要になると考えられます．

⑵　階層2（車載ゲートウェイ）のセキュリティ

車外システムと車載ネットワークの間，あるいは，異なる車載ネットワークの間において，許可されたメッセージのみが流れることを保証するフィルタリングや，ECUが暗号化や認証に用いる鍵を管理する鍵管理，車内で流れるメッセージにセキュリティ異常が発生していないかを監視・検知する異常検知などが挙げられます．

⑶　階層3（車載ネットワーク）のセキュリティ

ECU間で伝達されるメッセージが書き換えられたことを検出する改ざん検知，盗聴されることを防ぐ暗号化などが挙げられます．

⑷　階層4〔ハードウェア（ECUなど）〕のセキュリティ

ECUに搭載されるプログラムに脆弱性をつくり込まないコーディング作法であるセキュアプログラミング，ファームウェアやOSが改ざんされていないかを起動時に検証するセキュアブートなどが挙げられます．

今後，自動車の通信ネットワークへの接続がより一般的になり，多種多様なネットワーク型のサービスが提供されるに従い，サイバー攻撃も高度化・巧妙化していくことが想定されます．ITシステムのセキュリティ対策と同様に，自動車に対しても階層ごとのセキュリティ技術を組み合わせた多段的，多層的な防御策を施すことが必要と考えられます．

自動車のサイバー攻撃に対するNTTの取り組み

■取り組み概要

NTTセキュアプラットフォーム研究所では，自動車がサイバー攻撃に対してどれだけの耐性を有しているかを評価する安全性評価技術や，前述の階層1～4のセキュリティをベースとした対策技術の研究開発を実施していま

す．ここでは，自動車の制御に関連したセキュリティ評価技術と対策技術の例として，階層3のセキュリティに関連する，車内通信プロトコルLIN上で不正挙動を誘発する攻撃技術とその対策技術，および階層4のセキュリティに関連する，イモビライザー用の認証プロトコルに対する安全性評価技術と対策技術の研究事例を紹介します．

■LIN上での不正挙動を誘発する攻撃技術および対策技術

近年，車載ネットワークのセキュリティに関する研究が多く行われていますが，そのほとんどがエンジン，ブレーキなどの制御に利用されているCAN通信上でのセキュリティ評価や対策法に関するものです．一方，ステアリング，シートおよびドアなどの制御に用いられているLINを攻撃者が不正操作し，意図的に操作できれば非常に脅威となるものの，LIN通信上での不正な挙動を誘発する攻撃への耐性の有無や必要な対策法は明らかになっていませんでした．そこで私たちは他社と共同で，LIN通信上での不正な挙動を誘発する攻撃法やその対策法を提案しました[(4)]．

LINは，マスタースレーブ方式で通信が行われます．マスターノードが実行させたい処理のIDを含むヘッダを送信し，IDに該当する送信・受信スレーブノードがデータを送信・受信します．また，LINのエラーハンドリング機構に関して，エラー検知後の処理はLIN仕様では定義されていないため，処理内容はアプリケーションに依存します．例えば，自身が送信したデータとバス上のデータが異なる場合にエラーを検出し，データの送信を停止し，次のヘッダを待つといった単純な処理を実装する場合もあります．私たちはこのエラーハンドリング機構の特徴を利用することにより，受信スレーブノードに不正データをあたかも正しいものとして誤認識させ，不正な挙動を誘発できることを示しました．具体的には，攻撃者はバスを監視し，ヘッダ受信後の正しいデータ送信（図2①，②）に同期して，不正データを挿入・衝突させることによって（図2③），エラーハンドリング機構によって正しいデータ発信を停止させます．正しいデータ発信が止まるとともに不正な挙動を誘発するデータを挿入し，それを受信スレーブノードに正しいデータとして誤認識させることが可能になります．このようにして，運転者の意図に反する挙動を誘発することが可能なことを明らかにしました．

この攻撃への対策として，データ内で重要な意味を持つ値の配置を工夫する方法や，通信エラーが発生した際には異常を通知するメッセージをLINバス上に伝送させて不正データを上書きすることでそのデータを受信することを防ぐ対策方法を考案しました．

■イモビライザー用の認証プロトコルに対する評価技術および対策技術

2010年に，メーカ独自の暗号アルゴリズムに代わり，デファクトスタンダードであるAES暗号を利用したオープン仕様のイモビライザーで利用される認証プロトコルが提案されました．この認証用プロトコルは理論的な解析による脆弱性は発見されていませんでした．しかし，私たちの研究により，暗号の実装攻撃の一種である故障利用解析攻撃を応用することによって，電子キー内部に格納された認証に利用する秘密鍵を暴けることが明らかになりました[(3)]．本対象のプロトコルでは，電子キーが過酷な利用環境下であっても，電子キー内部に格納された

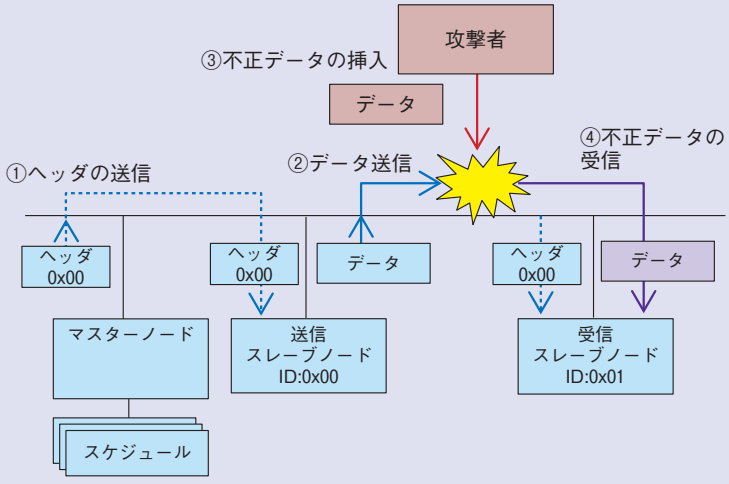

図2　LIN通信上での攻撃法の概要

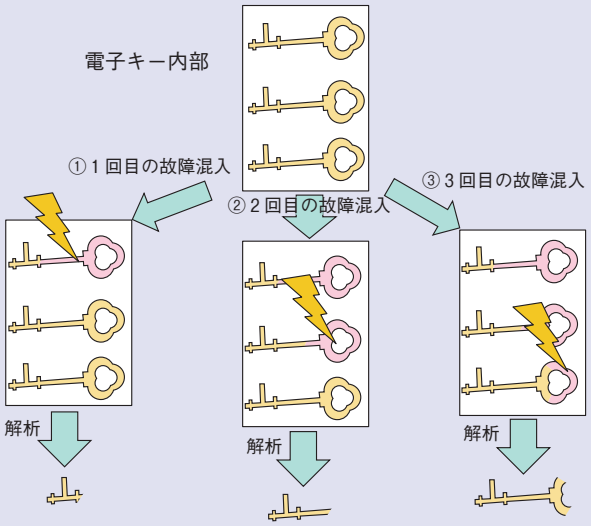

図3　故障利用解析攻撃の概要

秘密鍵が壊れにくくなるように，電子キー内に同じ値の3つの秘密鍵を格納し，これを順次に利用することで冗長化を行っています．私たちはこの事実に着目し，故障利用解析攻撃に用いられる故障混入方法で，電子キー内部の電子チップに格納されている3つの秘密鍵に各々特定のデータ変化を引き起こし（**図3**①～③），そのプロトコルの応答結果を解析することで，秘密鍵を徐々に特定する方法を考案しました（図3の「解析」部）．

本認証プロトコルの方式は，自動車が電子キーを認証するUnilateral方式と，自動車と電子キーが相互に認証するBilateral方式の2パターンがありますが，提案攻撃法を用いることにより，Unilateral方式の場合は現実的な時間で秘密鍵の特定が可能であること，Bilateral方式の場合は攻撃に利用できる電子キーの数などによっては秘密鍵の特定が可能であることを明らかにしました．さらに，提案攻撃手法への対策法として，各々の秘密鍵を利用して計算した暗号化結果を事前に比較することにより，秘密鍵の値が変化していないかを確かめる方法などを考案しました．

今後の展開

自動車は今後，自動運転やコネクティッドカーを実現するために，ますます多機能化すると予測されています．それに伴い，サイバー攻撃の侵入口の多様化や，攻撃の手口が高度化していくと考えられます．NTTセキュアプラットフォーム研究所では，車載ネットワークや車載システムのセキュリティに関する研究開発を今後も継続的に実施し，次世代の自動車の安心・安全に必要となるサイバー攻撃対策技術を提供していきます．そして，自動車と車外システムを接続する安全な通信インフラや，クラウドなどと連携した自動車向けセキュリティサービスの実現に貢献していきます．

■参考文献

(1) C. Valasek and C. Miller：“Adventures in Automotive Networks and Control Units,” DEFCON 21, Las Vegas, U.S.A., August 2013.
(2) C. Valasek and C. Miller：“Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA, Las Vegas, U.S.A., August 2015.
(3) 高橋・福永：“イモビライザー用の認証プロトコルに対するフォールト攻撃手法とその対策,” 信学論（A），Vol.J99-A，No.2，pp.106-117，2016.
(4) J.Takahashi, Y.Aragane, T.Miyazawa, H.Fuji, H.Yamashita, K.Hayakawa, S.Ukai, and H.Hayakawa：“Automotive Attacks and Countermeasures on LIN-Bus,” IPSJ Journal, Vol.25, Feb. 2017.

（左から）大嶋　嘉人/ 高橋　順子/
田中　政志

コネクティッドカーは将来の社会インフラの重要な要素になると考えられます．安心・安全なモビリティ社会の実現に貢献する自動車セキュリティ技術の研究開発を進めていきます．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
TEL　0422-59-3212
FAX　0422-59-2971
E-mail　scpflab@lab.ntt.co.jp