車載制御ネットワークCANへの不正メッセージ挿入防止技術

セキュリティーとリアルタイム性を確保したCAN通信システムを構築

電子化が進む自動車では，サイバー攻撃が脅威となっています。車載制御ネットワークとして広く普及しているCAN（Controller Area Network）の仕様は，セキュリティー機能が十分でないため，サイバー攻撃につながる不正メッセージを挿入されるおそれがあります。一方，暗号技術に基づくメッセージ認証で不正メッセージの挿入を防ぐ既存の対策では，リアルタイム性が損なわれます。

東芝は，リアルタイム性を損なわずにセキュリティーを確保するために，送信端末が受信端末と共有する疑似乱数（以下，秘密乱数と呼ぶ）をCANの通信フォーマットの拡張領域に埋め込み，受信端末が秘密乱数を照合して不正メッセージの挿入を防止する技術を開発しました。

自動車へのサイバー攻撃

2010年に自動車を標的としたサイバー攻撃が起こりうることが実証されて以来，様々なサイバー攻撃事例が報告されています。特に，市販の自動車を遠隔操作した2015年の事例では，140万台ものリコールにつながり，社会問題になりました。

車載制御ネットワークCAN

自動車の制御ネットワークでは，CANが利用されています。CANは，ISO（国際標準化機構）で標準化された信頼性の高い通信プロトコルです。自動車以外にも船舶や，医療機器，産業機器など多方面で利用されています。

CANでは，各ECU（Electronic Controller Unit）が，事前に割り当てられたID（識別情報）を利用してメッセージをブロードキャスト通信しています（**図1**）。現状のCANの仕様はセキュリティー機能が十分でないため，不正メッセージが挿入されると，自動車は遠隔操作の脅威にさらされます。そのため，CAN通信におけるセキュリティーの確保が必要不可欠になります。

不正メッセージ挿入防止の既存技術

メッセージ認証コード（MAC）は，通信の認証に広く利用されており，メッセージの改ざんや不正メッセージの挿入を防ぐことができます（**図2**）[1]。しかし通常のCAN通信（**図3**(a)）に比べ，MAC付きCAN通信（図3(b)）は，送信ECU側のMAC生成処理と受信ECU側のMAC認証処理が必要になるため，以下の二つのデメリットが生じます。

(1) 低性能なECUでは，ソフトウェアで実装したMAC認証は負担が大きく，処理に時間が掛かります。その結果，大量の不正メッセージを送る攻撃（DoS（Denial of Service）攻撃）を受けると，ECUが処理を実行しきれず正しく動作しない可能性があります。MAC認証専用のハードウェアを追加することで解決できますが，製品コストが増大します。

(2) MAC情報がCANメッセージの狭いデータ領域（8バイト）を占用するため，通信能力が低下します。例えば，4バイトのMACを使用すると通信能力は半減します。

開発技術の特長

東芝は，正規のECUが共有する秘密乱数によるメッセージの認証方式を開発してこれらの課題を解決するとともに，その技術を2016年11月にESCAR（Embedded Security in Cars）Europe Conferenceで発表しました。送信ECU側は，共通鍵と固定長のビット列であるシードから計算される秘密乱数を，CANの拡張ID領域に埋め込んで送信します。受信ECU側は，ブロードキャストされたメッセージを受信します。ハードウェアフィルターで拡張ID領域の情報とみずから計算した秘密乱数を照合し，両者が一致する場合はメッセージを受信します。一方，一致しない場合は受信したメッセージが不正なECUから送信されたものと判断し，瞬時に通信を遮断します。また，各ECUがメッセージの送受信の合間に秘密乱数を更新することで，リアルタイム性を確保します（**図4**）。

一方，MAC認証と異なり，秘密乱数を用いた認証ではメッセージの改ざんは検出できません。その代わりにCANの仕様では，送信ECU側はCAN上の信号をモニタリングし，通信エラーが生じると通信を無効化するので，この機能によって，メッセージの改ざんを防止できます。

システム構築に向けて

今回開発した技術では，同一CANに接続された全てのECUが同じ秘密乱数を使用する必要があります。そのため，この技術を用いたシステムの構築には，秘密乱数を生成するためのシードの初期化と更新，及び秘密乱数の更新の同期という二つの課題があります。そこで，セキュアなゲートウェイ（GW）が秘密乱数を同期させるための情報を，中央管理するシステム（**図5**(a)）を考案しました。

このシステムでは，GWがECUと共通鍵を共有することで，MAC認証や暗号通信により秘密乱数を生成するためのシードの初期情報や更新情報を安全に転送します（図5(b)）。

秘密乱数を同期して更新するため，GWが秘密乱数を診断情報として定期的に送信します（図5(c)）。各ECUは，診断情報が自己の秘密乱数と異なる場合には，同期エラーが発生したと判断して，GWに同期要求を送信します（図5(d)の左）。その後，ECUはMAC認証や暗号通信を用いてGWから同期情報を安全に受信し，回復処理を実行します（図5(d)の右）。

今後の展望

今回開発した方式は，CANのリアルタイム性と通信性能を損なうことなく，不正メッセージの挿入をソフトウェア実装で防ぐことができます。今後は，CANコントローラーにこの技術をハードウェア実装することで，より機能改ざんが困難で信頼性が高いシステムを構築し，性能評価を進めます。

文　献

(1) AUTOSAR Release 4.2.2: 2015. Specification of Module Secure Onboard Communication.

夏　　徴帆
技術統括部
研究開発センター
コンピュータアーキテクチャ・セキュリティラボラトリー

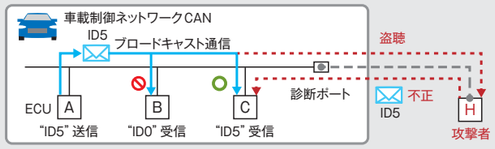

図1. 車載制御ネットワークCAN ― 診断ポートを経由して，ブロードキャスト通信されたメッセージを盗聴されたり，不正メッセージを挿入されたりするおそれがあります。

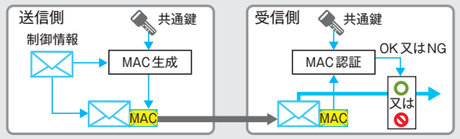

図2. MAC認証技術 ― MAC認証を利用して，不正なメッセージの挿入を防ぎます。

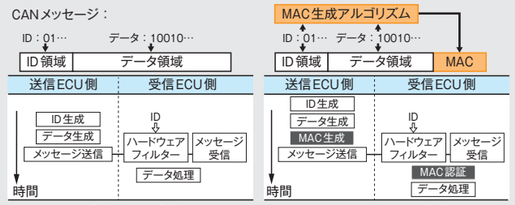

図3. CAN通信の従来技術 ― 通常のCAN通信に比べてMAC付きCAN通信では，MAC認証をしてメッセージが改ざんされていないことを確認してからデータを処理するため，リアルタイム性が損なわれます。

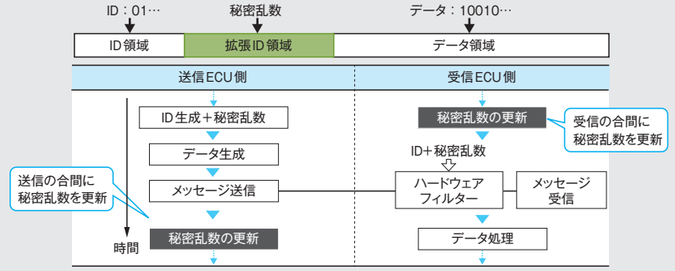

図4. 秘密乱数を利用するCAN通信 ― 通信ごとに更新される秘密乱数を照合してメッセージを受信することで，不正メッセージの挿入を防ぎます。

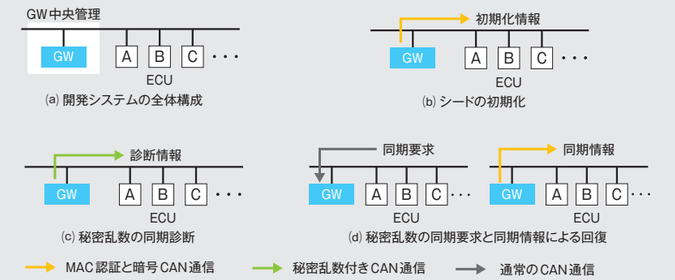

図5. 今回開発した技術を用いたCAN通信システム ― CANに接続されたECUをGWが中央管理することで，秘密乱数を生成するためのシードの初期化や，診断情報を利用した秘密乱数の同期診断，同期エラー発生時の秘密乱数の同期要求と同期情報によるエラーからの回復などを行います。