車載通信向け通信シーケンス番号の再同期方式

森田　伸義[†1]　井手口 恒太[†1]　萱島 信[†1]

概要：車載通信として利用されている CAN プロトコルにおける通信メッセージの改ざん対策として，アプリ層での MAC を用いたメッセージ認証の仕様策定が進んでいる．リプレイ攻撃対策も考慮した従来のメッセージ認証方式では，通信メッセージとシーケンス番号に対する MAC を算出する．しかしながら，同方式は車載制御装置の予期せぬ電源消失等の異常によってシーケンス番号の同期ずれを引き起こし，通信メッセージを正しく認証できなくなる恐れがある．そこで本稿は，車載システムに異常が発生したとしても，メッセージ認証による通信が継続可能な仕組みを提案する．提案方式は，新たに導入する異常用カウンタを用いた再同期メッセージにより，通信用シーケンス番号の同期回復を低コストで実現できるとともに，異常用カウンタに要するメモリ使用量が十分に実用的である見込みを得た．

キーワード：自動車セキュリティ，CAN，MAC，リプレイ攻撃，シーケンス番号の再同期

A Method of Resynchronization of the Communication Sequence Number for Automotive Networks

Nobuyoshi Morita[†1]　Kota Ideguchi[†1]　Makoto Kayashima[†1]

Abstract: In the automotive on-board system, automotive ECU (Electronic Control Unit) and CAN (Controller Area Network) which connects the ECU have been widely used. However, since attacks on CAN have been recently reported, countermeasures against the threat of information security are increasingly required. One of these threats is a message tampering. Generally, a countermeasure using a MAC (Message Authentication Code) is effective against such an attack. AUTOSAR suggests a countermeasure using a MAC for automotive on-board system, too. However, this countermeasure for automotive on-board system does not mention the processing when errors (ex. ECU's power down) occur in a car. ECUs can not synchronize sequence number of communication message due to these errors. By this cause, the security solution on CAN must make effective use of environment in which errors occur. Therefore, in this report, in order to continue above countermeasure when errors occurred in a car, we propose a new method. This method includes the following features: This method does not need special devices such as NTP server and RTC (Real Time Clock). This method uses the resynchronization message using the different counter that is updated when an error occurs. According to our experimental results, the proposed method makes continue above countermeasure when errors occurred in a car. We expect that our new approach is effective for automotive on-board system.

Keywords: Automotive security，CAN，MAC，Replay attack，Resynchronization of the Communication Sequence Number

1. はじめに

Connected Car と呼ばれるように，車載システムはインターネットなどの外部ネットワークとつながることにより，センタシステムからインターネット経由でユーザに様々なサービスを提供するようになりつつある．Connected Car 向け車載システムは，車内の車載制御装置（以下，ECU：Electronic Control Unit）と外部システムとの間でネットワークを介した情報交換を行い，システムを構成する物理的な機器の制御を実施する．このため，従来の閉じた車載システムとは異なり，外部からのセキュリティアタックに対する備えが重要になってきている [1][2][3].

外部からのセキュリティアタックの事例として，特に，Controller Area Network（以下，CAN[4]）プロトコルを用いた車載システムでは，OBDⅡ（On-Board-Diagnostics Ⅱ）ポートのような車載ネットワークに直接繋がっているインタフェースに不正な装置が接続され，意図的に改ざんされたメッセージを混入されることにより，自動車の安全走行を脅かす危険性が指摘されている[5]．通常，外部ネットワークと繋がる車載システムへの最も基本的な対策はネットワークに対するアクセス制御である．しかしながら，上記脅威事例[5]で指摘されているように，自動車内部に侵入できる可能性を払拭できず，車外ネットワークからの通信に対するアクセス制御を設けるだけで完全に車載ネットワークへの侵入を防止できるとは限らない．このため，基本的な暗号機能，特に改ざん検知機能によって車載ネットワークの安全性を高める対策による多層防御が必要になると考える．

一般的な改ざん検知機能として，各装置間を流れるメッセージに対して MAC（Message Authentication Code）を付与することで不正なメッセージを検知する方式が普及している．自動車業界における動向としても，ECU 向け OS

†1 株式会社日立製作所
244-0817　神奈川県横浜市戸塚区吉田町 292 番地
Hitachi, Ltd.,
292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa, 244-0817, JAPAN.

（Operating System）として検討されている AUTOSAR（AUTomotive Open System ARchitecture） OS では，AUTOSAR 4.2.2 の Secure Onboard Communication（Sec OC）モジュールに，MAC を用いたメッセージ認証の仕様が盛り込まれている．AUTOSAR におけるメッセージ認証の仕様は，MAC の生成に用いる入力情報および MAC を含めた通信メッセージのデータ構造については言及されているが，異常発生時の対処については言及されていない[6]．同仕様はリプレイ攻撃への対策のために，通信用のシーケンス番号を MAC 算出の入力値として用いている．このため，同仕様に基づいて実装された ECU は，例えば ECU の予期せぬ電源消失が発生した場合，通信用のシーケンス番号の同期がずれてしまう可能性がある．一旦，通信用シーケンス番号の同期がずれてしまうと，以降に受信した通信メッセージを正しく認証できなくなる．これは可用性を重視する自動車の走行制御に対して，無視できない影響を及ぼす恐れがある．そこで本稿は，車載システムに異常が発生したとしてもメッセージ認証を用いた通信が継続できるように，通信用シーケンス番号の再同期方式を提案する．

以下，第 2 章では車載システムに対するセキュリティとして，想定する脅威と既存の対策技術について述べ，第 3 章では車載通信むけメッセージ認証の課題を述べる．そして，第 4 章ではメッセージ認証に用いる通信用カウンタの再同期方式を提案し，第 5 章では提案方式の有用性について評価し，第 6 ではまとめと今後の課題について述べる．

2. 車載システムに対するセキュリティ

車載システムでは，代表的な通信プロトコルとして CAN プロトコルが普及している．CAN プロトコルは，複数の通信網を介した大容量データの高速通信といったニーズに応えるために開発されたシリアル通信プロトコルである．その後，CAN プロトコルは ISO（International Organization for Standardization）11898 および ISO11519 で規格化されている．本章では，CAN プロトコルについて 2.1 節で述べ，CAN プロトコルで想定される脅威とその攻撃方法について 2.2 節で述べ，既存の CAN プロトコルへの対策について 2.3 節で述べる．

2.1 CAN プロトコル

CAN プロトコルは，2 線式差動電圧方式でデータを伝送する．同方式は 2 本の通信線の電位差によって信号を伝える方式で，電位差が大きい状態をドミナント「0」と呼び，電位差が小さい状態をリセッシブ「1」と呼ぶ．CAN プロトコルはすべての ECU がマスタとして動作するマルチマスタ方式であり，複数の ECU が同時にドミナントとリセッシブを送信した場合，ドミナントが優先される仕様となっている． このような CAN プロトコルでは，ECU 間でデータを送受信する際にデータフレームを使用する．データフレームは，ID フィールド（CAN ID），データ長を示す DLC（Data Length Code），送信するデータ本体が格納されるデータフィールド，誤り検出符号の CRC 等から成る（Fig. 2-1）．ID フィールドに格納する識別子（CAN ID）は，各通信メッセージの ID を表すだけでなく，当該通信メッセージの優先度も示しており，CAN ID の値が小さいほどその通信メッセージの優先度は高くなる．送信データは，データフィールドに格納し，1 つのデータフレーム（1 メッセージ）を用いて最大 8Byte のデータを送信できる．

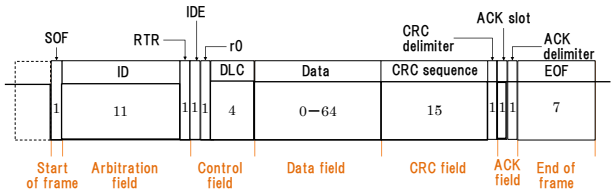

Fig. 2-1 CAN データフレームの構造

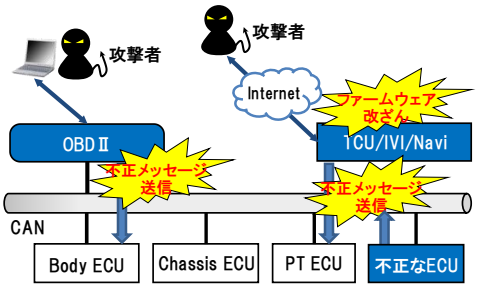

Fig. 2-2 CAN バスを介する攻撃とそのエントリポイント

また，CAN プロトコルは，バス型ネットワークを前提としており，バスに接続されるすべての ECU にメッセージを一斉送信（ブロードキャスト）する性質を有しており，各 ECU は自身が管理する CAN ID を含んだ通信メッセージを取得する．CAN バスが空いている状態で最初に送信を開始した ECU が送信権を取得する．同時に複数の ECU が送信を開始する場合は通信調停が行なわれ，最も優先度の高いメッセージを送信する ECU が送信権を取得する．このため，同時に複数の ECU がデータを送信する場合，上記通信調停により，CAN ID の小さい値の通信メッセージが優先される．

2.2 想定する脅威と攻撃方法

上記 2.1 節で述べた通り，CAN プロトコルは送信元を示す情報を含まない．このため，例えば，OBD Ⅱ ポートのような CAN バスに直接メッセージを送信可能な I/F を有する車載システムにおいて，CAN プロトコルを用いた通信路に不正なメッセージが送信された場合，正規のメッセージになりすまされる危険性がある（Fig.2-2）．このような CAN プロトコルの脆弱性を狙った不正なメッセージの混入として，本稿では 3 つの脅威事象を対象とする（Table 2-1）．

Table 2-1　想定する脅威事象

#	脅威事象
Threat1	OBD II ポートのような車載ネットワークに直接繋がっているインタフェースに不正な機器を接続し，不正な機器が不正なメッセージを CAN バスに送信することで，ECU の誤動作や動作停止を引き起こす.
Threat2	車外のサーバやデバイス等と連携する Navigation ECU（以下，Navi）等のファームウェアを改ざんし，改ざんされた Navi が不正なメッセージを CAN バスに送信することで，ECU の誤動作や動作停止を引き起こす. ※ただし，攻撃者は鍵情報を取得できない想定
Threat3	正規の ECU が不正な ECU に置き換えられ，不正なメッセージを CAN バスに送信することで，ECU の誤動作や動作停止を引き起こす.

さらに，本稿では上記脅威事象において，CAN バスに対する不正なメッセージの混入を，攻撃に使用される通信メッセージの内容によって，次の 2 つの攻撃方法に分類する．前提として攻撃者は ECU 間の通信を傍受し，各 ECU にメッセージを送信できるものとする．また，攻撃者は傍受したメッセージに含まれるデータを自由に変更できるものとする．

(1)　総当り攻撃

総当り攻撃は，攻撃者が事前にメッセージを傍受（或いは，予め対象車両における CAN プロトコルの通信フォーマットを取得）し，制御用データが取りうるすべてのパターンのメッセージに改ざんし，その改ざんしたメッセージを CAN バス経由で ECU に送信するものである．

(2)　リプレイ攻撃

本稿におけるリプレイ攻撃は，攻撃者が事前にメッセージを傍受し，任意のタイミングでその傍受したメッセージを CAN バス経由で ECU に送信するものである．

2.3 既存の CAN 向けメッセージ認証

上記 2.2 節で示した攻撃方法，「総当り攻撃」，および「リプレイ攻撃」への対策として，改ざん検知機能による解決が有効とされている．一般的な改ざん検知機能として，各装置間を流れるメッセージに対して MAC を付与することで不正なメッセージ検知する方式が普及している．

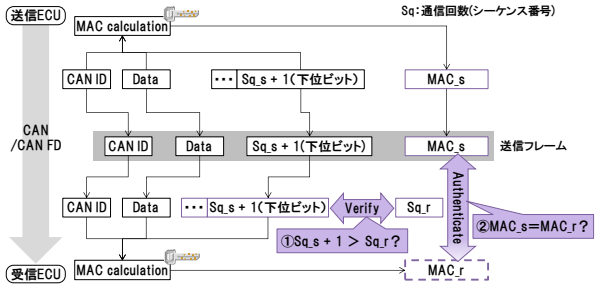

Fig. 2-3　AUTOSAR に基づくメッセージ認証の概要

特に，車載システム向けメッセージ認証として，AUTOSAR では CAN プロトコルにおけるメッセージ認証の仕様が策定されている．

AUTOSAR の仕様では，リプレイ攻撃対策用の通信用シーケンス番号（Sq）の下位ビットのみを送信フレームに付与する方式が盛り込まれている（Fig. 2-3）．以下，AUTOSAR の処理概要について述べる．

- 事前処理
  - ① 送信 ECU と受信 ECU で MAC の算出に用いる鍵を共有
  - ② 送信 ECU と受信 ECU で通信用の Sq を共有（同期済み）
- 送信時処理
  - ① 送信時に Sq_s（上位ビット ‖ 下位ビット）を更新（例：Sq_s ⇒ Sq_s + 1）
  - ② CAN ID，制御に用いるデータ，Sq_s + 1 に加えて，予め送受信 ECU 間で共有される鍵を用いて MAC_s を算出
  - ③ 「CAN ID」，「制御に用いるデータ（Data）」，「Sq_s + 1 の下位ビット」，「MAC_s」から成る送信フレームを生成し，受信 ECU に送信
- 受信時処理
  - ① 受信した Sq_s + 1 の下位ビットと，Sq_r の上位ビットを合わせた Sq_s + 1（Sq_r の上位ビット ‖ 受信した Sq_s + 1）と，Sq_r を比較し，受信した通信メッセージの最新性を検証
    ※Sq_s + 1 の下位ビットで桁上がりが発生する場合，Sq_r の上位ビットに 1 を加算
  - ② 受信した CAN ID，Data，Sq_s + 1（Sq_r の上位ビット ‖ 受信した Sq_s + 1 の下位ビット）に加えて，予め送信 ECU/受信 ECU 間で共有される鍵を用いて MAC_r を算出し，受信した MAC_s と MAC_r が一致していることを検証
  - ③ 上記①と②の検証によって通信メッセージの正しさが確認された場合のみ，Sq_r を更新するとともに，受信した制御データに基づく制御処理を実行

3. 車載通信向けメッセージ認証技術の課題

自動車は，様々な環境（マイナス数十度～数十度の気温，湿度，電子ノイズ）において，20 年近く運用されることが想定されている．このため，自動車における機能安全の分野では，予期せぬ異常が発生してもフェールセーフ機能によって自動車の走行制御を維持し続けることが検討されている．同様に，ECU に実装したセキュリティ機能についても，予期せぬ異常が発生した場合の車載システムに及ぼす影響を検討する必要がある．そこで本章では，車載システムで起こりえる異常について 3.1 節で定義し，異常が発生した場合のメッセージ認証の課題について 3.2 節で述べる．

3.1 異常の定義

本稿では車載システムで想定する異常として，「ECU の予期せぬ電源消失（Table 3-1)」，および「一時的な通信途絶（Table 3-2)」のケースについて定義する．一方，揮発性メモリや不揮発性メモリで格納される状態が保証されない場合は，プログラムそのものが正しく動作しない恐れがある．このような直ちに修理する必要があるケースは故障とし，本稿が想定する異常の対象外とする．

Table 3-1　ECU の予期せぬ電源消失

分類	補足説明
異常内容	ある ECU が予期せぬタイミングで電源を消失し，その後再起動によって復帰する．
通信用シーケンス番号への影響	電源を消失した際に，その通信用シーケンス番号の最新値をロストしてしまう． ※不揮発性メモリの書き換え回数の上限を，一般的に言われている数万回から十数万回程度とした場合，自動車の運用年数に対して, CAN プロトコルの通信回数は上記書き換え上限を大幅に上回ってしまう. ECU のコストを考慮すると，単純に不揮発性メモリの容量を増やすことは望ましくないため，メッセージ認証に用いる通信用シーケンス番号は揮発性メモリに格納されると想定する．
異常検知方法	ECU には予め予期せぬタイミングで電源が消失した場合，の事象が障害ログに残る仕組みとなっており，再起動時に障害ログを確認することで異常を検知できる．

Table 3-2　一時的な通信途絶

分類	補足説明
異常内容	一部の受信 ECU が一時的に通信メッセージを受信できず，一定期間経過 ※一時的でない場合は故障とし，本稿の対象外となる．
通信用シーケンス番号への影響	上記 2.3 節で述べた AUTOSAR のメッセージ認証方式のように，通信用シーケンス番号の下位ビットのみを送信フレームに付与する実装において，下位ビットで表現できる以上の期間通信途絶が発生した場合，通信用シーケンス番号の同期を取れなくなってしまう．
異常検知方法	CAN ID の周期情報に基づいて，一定時間を経過しても通信が届かない場合，異常として検知できる．

3.2 課題

上記 3.1 節で定義した異常が発生した場合，Table 3-1 および Table 3-2 に記載した通り，通信シーケンス番号はその影響を受けることになる．このため，送受信間の通信用シーケンス番号の同期ずれが発生してしまう．一旦同期ずれが発生してしまうと，受信 ECU は以降に送信 ECU から受け取った通信メッセージを正しく認証できなくなるため，自動車の走行制御に多大な影響を及ぼしてしまうという問題がある．このような事象を引き起こさせないために，車載システムに異常が発生したとしてもメッセージ認証を用いた通信を正しく継続できるように，通信用シーケンス番号の同期回復が必要である．

情報系システムにおける通信用シーケンス番号の同期回復方式として，IPsec（IP Security Protocol）では，IKE（Internet Key Exchange）プロトコルに基づく SA（Security Association）の更新が行なわれる[7]．しかしながら，IKE プロトコルを用いる再同期方式は, CAN プロトコルではサポートされていない．また，再同期プロトコルを導入する場合は，車載システムという低リソース環境での利用を考慮すると，処理負荷が小さい方式が求められる．その他にも，送受信装置間で共有されるタイムスタンプを用いた解決策が考えられる．しかしながら，タイムスタンプを用いる再同期方式は，各 ECU が時刻を管理できる必要がある．Navi のような一部の ECU を除いて ECU には時刻管理を行なう RTC（Real Time Clock）のような特殊な装置は搭載されていない．また，車載システムには情報系システムにおける NTP（Network Time Protocol）サーバのような時刻を管理する機構は搭載されていない．このため，タイムスタ

ンプを活用する解決策には，上記のような機構を追加する必要があるため，車載システムのコストが高くなってしまう．

以上より，車載向けメッセージ認証を実用化するための課題を纏めると次の通りである．

(1) 処理負荷が小さいこと

(2) 車載システムに新たな装置を追加しないこと（低コスト）

4. シーケンス番号の同期回復方式の提案

通信用シーケンス番号の同期回復は，大きく 2 つのステップからなる．1 つ目のステップは異常を検知することであり，もう一つのステップは検知後に通信用シーケンス番号の同期を回復することである．このうち本稿は，検知後の回復手法について新たに提案するものである．

提案方式は，電源を消失しても値を失わない不揮発性メモリの特徴を活用する．ただし，上述した通り不揮発性メモリには書き換え回数の制限がある．このため，通信用シーケンス番号を揮発性メモリではなく，不揮発性メモリで常に管理する場合，CAN プロトコルにおける通信のように 1ms 間隔で通信が行なわれる車載通信環境では，約 20 年と言われている自動車のライフサイクルを通して不揮発性メモリが正しく動作し続けることは保証されない．そこで，不揮発性メモリの書き換え回数の制限を遵守しつつ，同期を回復できる方式を提案する．具体的には，揮発性メモリで管理される通信用シーケンス番号（通信回数に応じて更新）に加えて，異常発生（検知）回数に応じて更新される異常用カウンタを不揮発性メモリに新たに導入する．そして，提案方式は異常の発生によって通信用シーケンス番号の同期ずれが起きた際，異常用カウンタを用いた再同期依頼メッセージを同期対象となる ECU に送信することで，通信用シーケンス番号の同期を回復することを特徴とする．以下では，通信用シーケンス番号（Sq）の一部を送信フレームに付与するメッセージ認証を例として，提案方式の処理概要を述べ，通常時の処理概要を Fig.4-1 に，異常発生後における同期回復の処理概要を Fig.4-2 にそれぞれ示す．

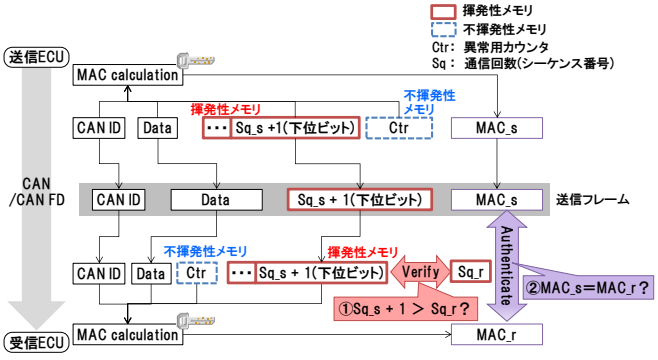

Fig. 4-1 提案方式を用いたメッセージ認証の概要（通常時）

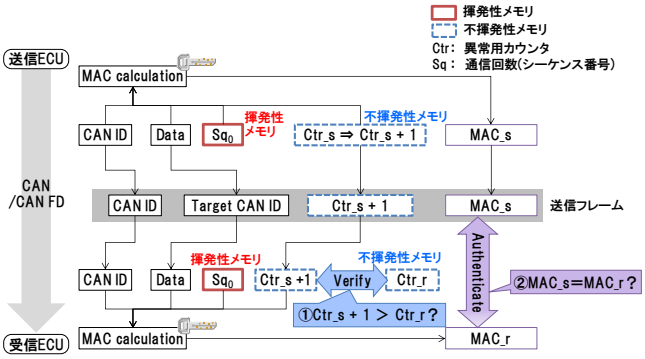

Fig. 4-2 提案方式による同期回復の概要（異常発生後）

(1) 通常時の処理概要

➢ 事前処理

① 送信 ECU と受信 ECU で MAC の算出に用いる鍵を共有

② 通信用の Sq に加えて，送信 ECU/受信 ECU は異常検知時に更新される異常用カウンタ（Ctr）を予め共有（同期済み）

➢ 送信時処理

① Sq_s を更新（例：Sq_s ⇒ Sq_s + 1）

② CAN ID，制御に用いるデータ，Sq_s + 1 と Ctr_s に加えて，予め送信 ECU/受信 ECU 間で共有される鍵を用いて MAC_s を算出

③ 「CAN ID」，「制御に用いるデータ」，「Sq_s + 1（下位ビット）」，「MAC_s」から成る送信フレームを生成し，受信 ECU に送信
通信メッセージ量を削減するため，Ctr_s を送信フレームに載せない

➢ 受信時処理

① Sq_s + 1（上位ビット ‖ 下位ビット）と Sq_r を比較し，受信した通信メッセージの最新性を検証

② 受信した CAN ID，制御に用いるデータ，Sq_s + 1 に加えて，Ctr_r と予め送信 ECU/受信 ECU 間で共有される鍵を用いて MAC_r を算出し，受信した MAC_s と MAC_r が一致していることを検証

③ 上記①と②の検証によって通信メッセージの正しさが確認された場合のみ，Sq_r を Sq_s + 1 の値に更新するとともに，受信した制御データに基づく制御処理を実行

(2) 異常発生後における同期回復の処理概要

➢ 事前処理

① 送信 ECU と受信 ECU で MAC の算出に用いる鍵を共有

② 通信用の Sq に加えて，送信 ECU/受信 ECU は異常検知時に更新される異常用カウンタ（Ctr）を予め共有（同期済み）

- 送信時処理
  ① 異常検知時に，不揮発性メモリから取得した Ctr_s を更新（例：Ctr_s ⇒ Ctr_s + 1）
  ② 同期依頼専用 CAN ID, 同期対象となる CAN ID, Ctr _s + 1 に加えて，予め定められたルールに基づいて更新した Sq_s(例：初期化 Sq0)と，予め送信 ECU/受信 ECU 間で共有される鍵を用いて MAC_s を算出
  ③ 「同期依頼用 CAN ID」,「同期対象となる CAN ID」,「Ctr _s + 1」,「MAC_s」から成る送信フレームを生成し，受信 ECU に送信（通信メッセージ量を削減するため，Sq_s を送信フレームに載せない）
  ※同期依頼メッセージを送信できたことを確認した後に，更新した Ctr_s（即ち，Ctr _s + 1）を不揮発性メモリに格納
- 受信時処理
  ① 同期依頼専用 CAN ID を認識した場合，その通信メッセージを受信
  ② 自身が同期対象 CAN ID（Target CAN ID）を管理している場合は③以降の処理に進み，管理対象外の場合は処理を終了
  ③ 受信した Ctr _s + 1 と保有する Ctr _r を比較し，受信した通信メッセージの最新性を検証
  ④ 受信した，同期依頼用 CAN ID，同期対象となる CAN ID，Ctr _s + 1 に加えて，予め定められたルールに基づいて更新した Sq_r（例：初期化 Sq0）と，予め送信 ECU/受信 ECU 間で共有される鍵を用いて MAC_r を算出し，受信した MAC_s と MAC_r が一致していることを検証
  ⑤ 上記①と②の検証によって通信メッセージの正しさが確認された場合のみ，Ctr _r を Ctr _s + 1 の値に更新予め定められたルールに基づいて Sq_r を更新（例：初期化 Sq0）することで安全に送信 ECU と同期可能

以上の処理により，提案方式は安全に通信用シーケンス番号の同期を回復できる．また，提案方式は特殊な装置を用いることなく，一般的な揮発性メモリと不揮発性メモリを利用することで実現できるため，十分に低コストで通信用シーケンス番号の同期回復を実現できる．

5. 評価および考察

本章では，提案方式の有用性について評価する．まずは，通信用シーケンス番号の再同期に関する異なるアプローチとして，鍵更新に基づく再同期方式との比較について 5.1 節で述べる．また，提案方式は AUTOSAR の仕様に対して，不揮発性メモリに異常用カウンタを追加導入するため，そのメモリ使用量に関する考察を 5.2 節で述べる．

5.1 提案方式の比較評価

本稿では，AUTOSAR で仕様策定されたメッセージ認証を ECU に実適用するために，異常発生時の通信用シーケンス番号の同期ずれに対して，再同期メッセージによる解決策を提案した．一方で，異なるアプローチとして，メッセージ認証に用いる鍵を更新することによって，利用する通信用シーケンス番号を初期化し，強制的に同期を回復する方式がある[9]．本稿で提案した異なる 2 系統のカウンタに基づく再同期メッセージを用いた同期回復方式と，鍵更新を用いた通信用シーケンス番号の初期化方式について比較する（Table 5-1）．

基本的に処理の重い暗号演算による処理負荷の点で，提案方式は鍵更新方式と比べて優位になると考える．仮に，鍵更新方式が暗号アクセラレータを用いた場合，処理負荷はクリアできたとしても今度はコストが高くなり，メッセージ認証の対象となるようなすべての ECU に適用することは困難と考える．

Table 5-1　提案方式の比較評価

比較項目	提案方式	鍵更新方式
アプローチ	異なる 2 系統のカウンタに基づく，通信用シーケンス番号の再同期メッセージを用いた同期回復	鍵更新による通信用シーケンス番号の初期化による同期回復
処理負荷（通信負荷は同等になるため，暗号演算で比較）	○ MAC の生成/検証（各 1 回）	× MAC の生成/検証（各 1 回），メッセージの暗号化/復号（送受信で各 1 回），鍵生成（生成側で 1 回）
セキュア HW に要するコスト	○ 1 系統の鍵をセキュア HW で管理	△ 2 系統の鍵をセキュア HW で管理

5.2 不揮発性メモリの使用量に関する考察

CAN プロトコルは, 同時に通信バスにメッセージを送信した場合，通信調停によって値の小さい CAN ID が優先される仕様となっている．提案方式は，通信シーケンス番号を MAC の算出に用いており，通信調停が発生した際の MAC の再計算を避けるため，CAN ID ごとに通信用シーケンス番号を保持する．加えて，提案方式は異常用カウンタを新たに導入しており，異常用カウンタについても同様に CAN ID ごとにカウンタを保持する．また，CAN プロトコルにおける制御メッセージの送信周期は CAN ID ごとに決められている．送信周期の早い CAN ID の場合，その送信周期は 1ms 間隔となるメッセージもあり，自動車のライフサイクルとして考えられる 20 年間では，2^{40} 回以上の通信が発生する．

以上の条件において，提案方式は，CAN ID ごとに異常用カウンタ用の不揮発性メモリが最大で 40bit 追加できれば十分である．ここで，メッセージ認証が適用される ECU で管理される CAN ID の数が，送信用と受信用を合わせて 200 個程度のケースを考える．即ち，ECU で 1Kbyte の不揮発性メモリが必要となる．ECU として利用されるマイコンの例として, ルネサス社製マイコンの RH850F1L がある[8]. 同マイコンでは，2MByte の不揮発性メモリが搭載されており，新たに追加される異常用カウンタで使用する 1Kbyte は全体の 0.05％で済む．これより，同マイコンを利用した ECU において，提案方式は少ないメモリの使用量で効果が見込める．

6. まとめと今後の課題

本稿は，想定する 2 つの異常，「ECU の予期せぬ電源消失」，および「一時的な通信途絶」に関して，異常発生時にメッセージ認証に用いる通信用シーケンス番号の同期がずれたとしても，通信用シーケンス番号を再同期可能な方式について述べた．

提案方式は，RTC のような特殊な装置を用いずに，通信用シーケンス番号に加えて，異常用カウンタを不揮発性メモリに格納し，これらの異なる 2 系統のカウンタに基づく再同期メッセージによる同期回復を特徴とする．また，提案方式は，鍵更新による再同期方式と比較して処理負荷を小さくできるとともに, ECU の候補となるマイコンを対象に，新たに追加する異常用カウンタに要する不揮発性メモリの使用量が十分に低コストであることを示した．今後は提案方式の実用化に向けて下記課題への対応を試みる予定である．

- 起動タイミングの異なる ECU への対応
  異なるタイミングで起動する ECU に対する提案方式の適用について検討する
- 再同期依頼メッセージの最適配信
  CAN プロトコルのブロードキャスト通信の活用や，ECU による同期処理の集中管理等，再同期依頼メッセージの最適配信について検討する．

参考文献

[1] IPA.”2010 年度 制御システムの情報セキュリティ動向に関する調査報告”, https://www.ipa．go.jp/files/000014121.pdf，(参照 2016-07-20).
[2] IPA.”情報家電におけるセキュリティ対策 検討報告”, https://www. ipa. go. jp/files/000014114. pdf, (参照 2016-07-20).
[3] IPA．”2012 年度 自動車の情報セキュリティ動向に関する調査”， https://www.ipa.go.jp/files/000027274.pdf, (参照 2016-07-20).
[4] Bosh．”CAN Specification Version2.0”, http://esd.cs.ucr.edu/webres/can20.pdf，(参照 2016-07-20).
[5] Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno. : Experimental Security Analysis of a Modern Automobile, 2010.
[6] AUTOSAR，Specification of Module Secure Onboard Communication，AUTOSAR Release 4.2.2.
[7] 馬場達也．マスタリング IPsec．オーム社，2006.
[8] ルネサス製 RH850 F1L. http://japan.renesas.com/products/mpumcu/rh850/rh850f1x/rh850f1l/index.jsp，(参照 2016-07-20).
[9] 菅島健他.”セキュアかつ効率的な車載鍵管理の提案“．暗号と情報セキュリティシンポジウム(SCIS)，2016.