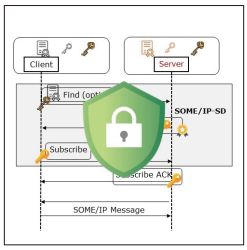


車載イーサネットのセキュリティ拡張プロトコルの提案

A Proposal of Security Extension Protocol for Automotive Ethernet

上田　浩史* Hiroshi Ueda
倉地　亮* Ryo Kurachi
高田　広章 Hiroaki Takada
井上　雅之 Masayuki Inoue
上口　翔悟 Shogo Kamiguchi
和田　健治 Kenya Wada

近年、自動車の電子制御システムにもイーサネットの搭載が進んでおり、自動車の電子制御システムに適したサービス指向プロトコルとしてSOME/IP（Scalable service-Oriented MiddlewarE over IP）プロトコルが採用されてきている。SOME/IPプロトコルではサービスを探索するためのプロトコルであるSOME/IP-SD（Service Discovery）プロトコルを実行した後、サービスを受信することが可能となる。しかしながらその一方で、SOME/IP-SDプロトコルの保護が十分でなくセキュリティリスクがあることが課題となっている。このため、本稿ではSOME/IP-SDプロトコルに対する保護を実施するための拡張プロトコルについて提案する。さらに、提案プロトコルを評価し、他のプロトコルよりも優位であることを示す。

Ethernet and SOME/IP (Scalable service-Oriented MiddlewarE over IP) have been increasingly applied to modern vehicles. Although SOME/IP serves as an automotive middleware solution for control message transmission, it lacks security measures, making it vulnerable to various attacks. To address this issue, we present a security extension protocol for automotive Ethernet. Furthermore, we evaluate the protocol and demonstrate its effectiveness.

キーワード：自動車セキュリティ、車載ネットワーク、車載イーサネット、SOME/IP

1.　緒　　言

近年、自動車に搭載される機能が増加するにつれ、自動車内の電子制御システムは複雑化し、ECU（Electronic Control Unit）と呼ばれる制御用コンピュータが多数搭載されるようになっている。また、自動車に搭載されるセンサが高機能化されるにつれ、大容量の通信プロトコルが必要となり、車載イーサネットが注目されている。車載イーサネット通信では、リアルタイム性を確保するために、物理層やMAC (Media Access Control) 層を拡張した様々なプロトコルが提案されている。さらに、その上位層のプロトコルとして、より柔軟な制御システムを構成するために、SOME/IPプロトコルが提案されている[(1)]。従来の電子制御システムでは静的に配置された機能が、各ノードからブロードキャストされるデータを受信することにより実現されている。その一方で、SOME/IPプロトコルでは電子制御システム上の機能配置を柔軟にするため、動的にノードに配置された機能からサービスを受信することを前提としている。従って、SOME/IP通信を開始する前に、SOME/IP-SDを実行する[(2)]。しかしながら、SOME/IP-SDによる動的な接続を確立する場合、セキュリティ上の課題が存在する。このため、本稿では2つのノード間の通信を安全な方法で確立するための拡張プロトコルを提案する。また、本稿では様々なセキュリティプロトコルとの比較を行い、提案プロトコルの必要性を議論する。

2.　SOME/IPプロトコルとその関連研究

2−1　SOME/IPプロトコル

SOME/IPプロトコルは、自動車のソフトウェアプラットフォームを標準化する業界団体のAUTOSAR (AUTomotive Open System ARchitecture) により仕様が策定された通信プロトコルである。この通信プロトコルの特徴は、サーバクライアント通信を想定しており、クライアントが動的にサービスを実行するサーバを探索し、接続することにより通信チャネルを確立するプロトコルである。このサービス探索のためのプロトコルをSOME/IP-SDプロトコルと呼ぶ。サーバとクライアントの通信チャネルが確立した後は、サーバがクライアントに対して**図1**に示すSOME/IPメッセージを送信することによりサービスが開始される。

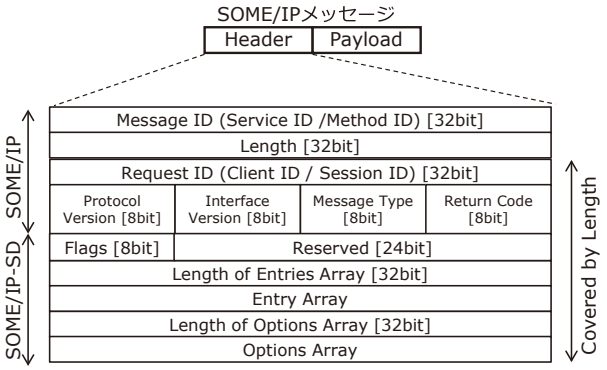


図1　SOME/IPメッセージのフォーマット

2−2　SOME/IP-SDプロトコル

SOME/IP-SDプロトコルでは、サーバ、クライアントのいずれのノードも起動時に実行するシーケンスが定義されている。クライアントは起動後、サービスIDを指定しFindメッセージを送信しサーバからの応答を待つ。サーバはクライアントからのFindサービスが、自身が実行するサービスIDが指定される場合には、Offerサービスによりクライアント側にサーバへの接続情報を付与して応答する。Offerサービスを受信したクライアントはOfferサービスにて通知されたサーバの接続情報を利用し、Subscribeメッセージを送信し接続を要求する。サーバは、Subscribe Eventgroup AckあるいはSubscribe EventGroup Nackを用いて接続の可否を応答する。このとき、Subscribe Eventgroup Ackが返れば、SOME/IP-SDでの接続が完了したものとして扱われ、以降はSOME/IPメッセージにてサービスを受信することができる。この動作については**図2**に示すとおりであり、Subscribe Eventgroup Ackが返却されるまでがSOME/IP-SDプロトコルであり、以降はSOME/IPメッセージにてデータの送信が行われる。

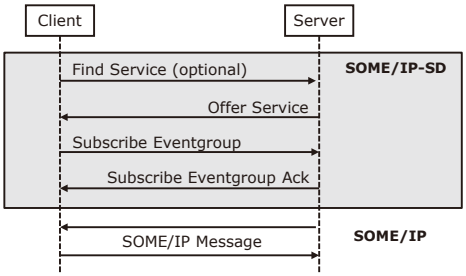


図2　SOME/IP-SDのシーケンス

2−3　SOME/IP-SDプロトコルの脅威

SOME/IP-SDプロトコルは、前述するような動的に接続確立が要求される通信プロトコルであるため、以下の攻撃方法が想定される。

（攻撃方法1）不正なクライアントによる盗聴

もし攻撃者がネットワークに接続している場合、攻撃者はSOME/IP-SDプロトコルで通知される情報を盗聴することにより、各サービスをどのノードが実行しているのかを把握することができる。このため、SOME/IP-SDプロトコルに対して、秘匿性を確保する手段が必要と考えられる。

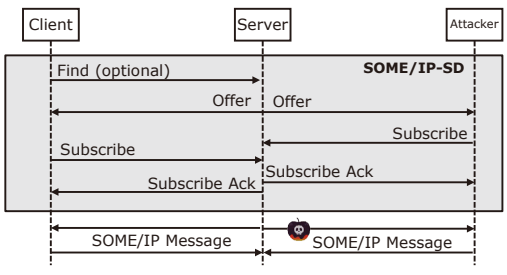


図3　SOME/IP-SDにおける盗聴

（攻撃方法2）中間者攻撃

SOME/IP-SDでは任意のメッセージを事前の認証なしに送信することができるため、ネットワークに接続する攻撃者によって、データやコマンドを注入され、悪用される可能性がある。この具体的な攻撃方法としては**図4**に示すような中間者攻撃が挙げられる。正規のサーバから送信されるOfferサービスを攻撃者のノードの情報に書き換えて送り付けることにより、クライアントを攻撃者が制御するサーバに接続させ、異常なデータを送り付けることが可能になる。

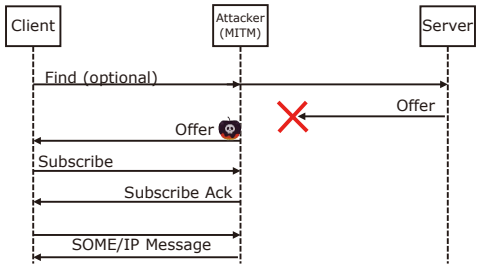


図4　SOME/IP-SDにおける中間者攻撃

（攻撃方法3）コピーキャット攻撃

論文 (3) にて、コピーキャット攻撃と呼ばれる攻撃方法が言及されている。コピーキャット攻撃は、正規のサーバがOfferサービスを送信するのを待ち、その後すぐに攻撃者が自身のエンドポイント情報を含むOfferサービスを送信することにより実現される攻撃であり、クライアントが後から送信されたOfferサービスを実行する性質を利用して、攻撃者の偽サーバに誘導する攻撃方法である。この攻撃では、前述する（攻撃方法1）と（攻撃方法2）の組み合わせにより実現され、攻撃者は正規サーバのOfferサービスを盗聴した上、偽サーバになりすますことで、クライアントに異常なデータを送り付けることが可能になる。

2−4　脅威の対抗策と関連研究

また、SOME/IPに対する脅威を排除するために、以下のような対抗策が議論されている。

（対抗策1）メッセージ認証子による保護

AUTOSARでは SecOC（Secure Onboard Communication）と呼ばれる仕様が規定されており [(4)]、従来の車載制御ネットワークでも既に利用されている。このため、車載イーサネットに関してもSecOCに対応しMAC（Message Authentication Code）を付与することで各メッセージを保護する手法が考えられている。しかしながら、この方法では安全な場所にて事前に書き込まれた共通鍵を保持することが前提であり、この共通鍵が漏洩する場

合には効果がない。つまり、通信オーバーヘッドが最も少ないという利点を持つが、共通鍵が漏洩した場合は効果がないことが課題である。

（対抗策2）TLS による保護

セキュアなノード間の通信を確立するために、民生機器ではTCPに対してTLS※1、UDPに対してDTLS※2が用いられることが多い。しかしながら、TLSはサーバとクライアントの両方に相応の計算処理を課すため、計算機資源の限られた組み込み機器には計算量が大きすぎる可能性がある。さらに、高いリアルタイム性が要求される自動車のようなアプリケーションにおいて、SOME/IP-SDを実行する他に、TLSで接続を確立しなければならない場合には、アプリケーションが開始するまでの時間が長すぎることが課題である。

さらに、既存研究として、以下のような対抗策が議論されている。

まず、福田らは、車載制御システムにセッション管理サーバを立てることによりセッション管理サーバが代理で認証する方式を提案している[(5)]。この方式では、セッション管理が一元化され、それらのログを管理することが容易である一方で、セッション管理サーバが動作しない場合にはすべての通信が確立できなくなる可能性があるうえ、通信確立までに時間がかかるという課題がある。

次にIorioらは、SOME/IPメッセージを保護するための認証プロトコルを提案している[(6)]。この手法は、クライアント証明書とサーバ証明書を用いて、すべてのクライアントとサーバの間でユニキャストによるハンドシェイクを実施することを前提としており、Findメッセージをブロードキャスト（あるいはマルチキャスト）しない。このため、サービス数やノード数が増加するとメッセージが多くなることが課題である。

Zelleらは、SOME/IPプロトコルのセキュリティ分析を行い、改良プロトコルを提案している[(3)]。この手法では、Offerサービスに対して、起動後セッション開始前にOfferサービス通知側で生成されたセッション鍵（共通鍵）を共有することにより実現される。また、この手法ではグループ鍵を用いることで、Offerサービスを保護することを可能にしている。しかしながら、毎回起動時にセッション鍵の共有を行うまでは通信を開始できないことと、クライアントからのFindサービスに対応していないため、サーバのOfferサービスの定期送信頻度を上げないと、接続開始が遅くなることが課題である。

このように、様々な手法が提案されているものの、SOME/IP-SDプロトコルに完全に互換し、セキュリティ強度を高める手法はこれまでに提案されていない。このため、本稿ではSOME/IP-SDプロトコルに互換したうえで、より通信オーバーヘッドを低減しつつセキュリティ上の安全性を高める通信方式を提案する。

3.　提案方式

本章では、SOME/IPのための安全なノード間通信チャネルを確立するためのプロトコルを提示する。我々の提案方式では、サーバとクライアント間で通信を確立する際に実行されるSOME/IP-SDに着目し、サーバクライアント間での通信保護を実現するものである。以降では、その要件を述べ、設計したプロトコルの概要について述べる。

3−1　要件

車載制御システムならではの幾つかの要件が存在する。

（要件1）少ない通信オーバーヘッド

車載制御システムは分散制御システムであるため、起動時の通信は混みあうことから、起動時の通信オーバーヘッドを低減することは重要である。このため、セキュリティを担保するための通信が多数行われると通信確立までの時間が長くなることが懸念される。したがって、通信オーバーヘッドが極力低減できる方式が必要となる。

（要件2）Findサービスの保護

クライアントは起動後、マルチキャストにてFindサービスを実行することでサーバからの応答を待つ。特に、サーバからのOfferサービスの受信を待ち続けるよりも、Findサービスを用いる方が通信確立までの時間を短くできる可能性が高い。このため、Findサービスをマルチキャストで実行することを前提とした保護方法が必要となる。

（要件3）セキュリティレベルを設定可能であること

従来の車載制御システムでは、ノード間の通信をすべて暗号化することは行われていない。このため、暗号化したい通信と暗号化しなくてもよい通信に分類できると考える。ゆえに、それぞれのサービスごとにセキュリティレベルを定義し、暗号化の有無や暗号方式を変更できる仕組みが必要と考えられる。

3−2　セキュアな通信チャネルの設計

TLSまたはDTLSをSOME/IPに適用する場合、いくつかの課題がある。まず、SOME/IPのハンドシェイクでは、クライアントからのマルチキャストによりサービスを実行するサーバがどこに配置されているのか探索する必要がある。この時、クライアントはサービスIDなどのサービスグループ情報を暗号化せずに配信する。

このため、攻撃方法1であげるような盗聴により、システム上の構成情報が漏洩することが懸念される。さらに、盗聴されたサービスグループ情報を用いて、攻撃方法2にある中間者攻撃で、クライアントに偽のメッセージを送信することが可能になり、攻撃方法3であげられるコピーキャット攻撃が実行される恐れがある。

次に、静的な秘密鍵（共通鍵）を各ノードに持たせることにより、MACを使ってSOME/IPメッセージの安全性を確保する方法もある。このような場合、SOME/IPメッセージの改ざんに対しては保護できるものの、サービスの内容が漏洩する恐れがある。また、前述したように、共通鍵を静的に保持し続ける方法では、漏洩後の安全性が確保でき

ない。このため、サーバ証明書やクライアント証明書を用いて、送信元を認証・認可することも必要と考える。

さらに、SOME/IP プロトコルとの完全な互換性を実現するため、ユニキャストメッセージに加えてマルチキャストメッセージも保護する必要がある。特定のサービスインスタンスに属するメッセージを保護するため、事前に共有される共通鍵を用いる。この1つの共通鍵はセッション確立前にすべてのノードの安全な場所で共有されることを想定する。この事前に共有された共通鍵を使用し、Find サービスを保護することで、安全性が増し、既存手法に比べてサービス確立までの時間を短縮することができる。

以上を踏まえ、我々の提案するプロトコルでは、事前共有された共通鍵とサーバ証明書、クライアント証明書を用いる方式を提案する。この提案プロトコルの特徴は、従来の SOME/IP プロトコルに完全に互換し、Find サービスや Offer サービスを保護することである。以降では提案方式の鍵の管理について説明したうえで、提案するプロトコルを説明する。

3−3　鍵の管理

共通鍵、サーバ証明書あるいはクライアント証明書を各ノードに事前に配布することを前提としている。このため、これらの初期鍵は工場などの安全性の高い場所にて書き込まれる必要がある。その上で、SOME/IP-SD プロトコルの実行時、Find サービスの保護のために共通鍵を用いる。また、証明書を用いて相互認証することにより、サーバおよびクライアントのなりすましから保護することを目的とする。従って、**図5**に示すように、各ノードにはクライアントとサーバのいずれかの役割が割り当てられており、各ノードは秘密鍵とそれに対応する証明書（サーバ証明書あるいはクライアント証明書）を保持しているものとする。

さらに、共通鍵の更新については、接続が確立された後、各ノードにて更新することを想定する。このため、この共通鍵は SOME/IP-SD にて接続が確立される度に更新され、不揮発メモリに保存される。

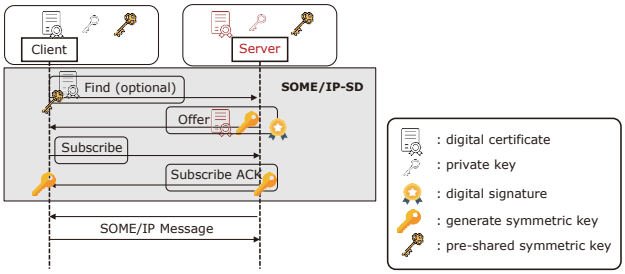


図5　本提案手法における鍵の管理とシーケンスの概要

3−4　提案プロトコル

本提案プロトコルは、基本的にはハイブリッド暗号方式を採用し、SOME/IP-SD に適用したプロトコルである。しかしながら、Find サービスを保護するために、事前に共有された鍵を用いることが他のプロトコルと大きく異なる。より具体的には、以下のようなプロトコルである。

図5に示すように、まずクライアントは Find サービスを送信する際、クライアント証明書を付与した上、事前共有鍵を用いて暗号化を行った上で MAC を付与することで盗聴と改ざんから保護する。Find サービスを受信するサーバは事前共有鍵を用いて MAC の検証と復号を行い、クライアント証明書が信頼できるルートにより発行されたかどうかを検証し、正しいクライアントからの要求であることを確認する。

次に、サーバは要求してきたクライアントに対し Offer サービスを通知する前に、クライアントが要求するサービスを提供可能か事前に与えられたリストに従い確認した上で、セッション鍵（共通鍵）を生成する。このセッション鍵をクライアント証明書に付与される公開鍵を用いて暗号化し、クライアントに Offer サービスを応答する。この手順により、対応する秘密鍵の所有者であるクライアントのみが復号できることが保証され、セッション鍵の機密性が確保される。

さらに、Offer サービスには、その真正性と完全性を保証するため、応答全体に対するデジタル署名を付与する。次にクライアントが Offer サービスを受信すると、送信されてきたサーバ証明書を検証し、正規のサーバであることを確認する。最後に、サーバ証明書から抽出した公開鍵を用いてデジタル署名の有効性を確認し、一致した場合は自身の秘密鍵を用いてセッション鍵を復号し、以降の通信で利用する。Subscribe Eventgroup および Subscribe Eventgroup Ack は秘匿性を持たせるため、セッション鍵により暗号化し送信するものとする。

3−5　サービスの保護レベル

一方、SOME/IP-SD によるセッション確立後、通常の SOME/IP メッセージで送信する場合、サービス単位で保護レベルを設定することができるものとする。保護レベルについては、基本的には、クライアント証明書内に対応可能な保護レベルを記載することにより実現されるが、サーバが保持する事前に与えられたリストにより制御されることも想定する。このため、攻撃などにより通信が不安定な場合にはサーバから保護レベルを変更することも可能となる。サービスの保護レベルについての一例を**表1**に示す。

表1　サービスの保護レベルの一例

保護レベル	サービス保護策
0	なし
1	メッセージ認証コードによる改ざん防止
2	暗号化と改ざん防止
3	暗号化とデジタル署名による保護

4. 評　　価

本稿では、2つの観点での評価を実施する。まず、実機を用いて通信オーバーヘッドを測定する。次に前述する対抗策や関連研究との比較について述べる。

4−1　評価環境

評価環境は**図6**に示すとおりであり、2台のRaspberry Piと1台のスイッチングハブを用いた。なお、プロトコルは、vsomeip[7]を用いて実装を行った。

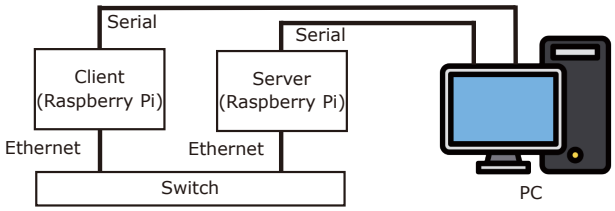


図6　評価環境の構成

4−2　評価結果1：通信オーバーヘッドの評価

評価としては、実機上でのスループットを測定し、通信オーバーヘッドについて考察した。比較対象としては対抗策1.メッセージ認証による保護（MAC）と対抗策2.TLSによる保護（TLS）を想定する。測定は各クライアント側からのFindサービスとOfferサービスによる応答を受信するまでの時間とした。なお、対抗策1（MAC）ではFindサービスとOfferサービス以降の手続きがない点、対抗策2（TLS）については事前にTLSの通信保護手続きを行う必要があることから、通信オーバーヘッドが大きくなる点に注意されたい。そのうえで、各方式に対して100回計測し、その平均、最小値、最大値を記載している。

測定結果については**表2**に示すように、従来手法と比べて、十分に低い通信オーバーヘッドで実行できているといえる。

表2　SOME/IP-SDのセッション確立時間（ms）の比較

		対抗策1 (MAC)	対抗策2 (TLS)	提案手法
計測時間	最小	25.990	95.784	45.164
	平均	26.778	95.983	46.552
	最大	28.206	99.245	48.655

4−3　評価結果2：既存する対抗策や関連研究との比較

まず、既存する対抗策である対抗策1（MAC）と対抗策2（TLS）の2つと提案方式を比較した。比較結果については、**表3**に示すとおりである。クライアント認証（観点1）とサーバ認証（観点2）について、対抗策1（MAC）では考慮されていないことが課題である。次に、他ノードの鍵漏洩の影響（観点3）については、共通鍵をベースとする対抗策1（MAC）では他ノードから漏洩した鍵により自ノードになりすましをされてしまう可能性があるため、セキュリティ上の安全性は相対的に低いといえる。さらにセッション確立時間（観点4）については、前述した評価結果より、対抗策2（TLS）では相対的に長くなることが課題である。これらの結果から、提案手法は他の対抗策と比較し、十分に優位であると結論付けられる。

表3　対抗策1，2と提案手法の比較

観点	対抗策1 (MAC)	対抗策2 (TLS)	提案手法
1.クライアント認証	× (なし)	○ (あり)	○ (あり)
2.サーバ認証	× (なし)	○ (あり)	○ (あり)
3.他ノードの鍵漏洩	× (影響あり)	○ (影響なし)	○ (影響なし)
4.セッション確立時間	○ (短い)	× (長い)	△ (比較的短い)

次に、他の関連研究との比較として、論文 (6) と論文 (3) の手法との比較を述べる。**表4**に示すとおり、いずれの手法も、クライアント証明書、サーバ証明書を用いることが想定されており、観点3までは大差がないと考える。一方、観点4についてはFindサービスの扱いに差がある。より具体的には、論文 (6) ではFindメッセージをブロードキャストできないため、サービスを実行する可能性のあるノードに対してユニキャストでFindサービスを送信する必要がある。このとき、すべてのサーバの候補とのセッションが確立している必要があり、サーバの候補が多数存在する場合には通信量が膨大になることが課題である。また、論文 (3) ではFindサービスは保護せずに使用しないものと考えられる。この場合、サーバからのOfferサービスにより通信が開始される場合のみが想定され、高い頻度でOfferサービスを送り続けなければならないため、通信オーバーヘッドが大きくなる可能性がある。このため、提案手法がFindサービスに対応しつつ、相対的に短い時間でセッションが確立できると考える。従って、セキュリティとリアルタイム性のトレードオフとしては最適なレベルであると考えられる。

最後に、既存手法との差異として、**表4**に挙げられる観点5と観点6について説明する。まず、Findサービスの保護（観点5）については、論文 (6) ではユニキャストを用いることにより保護されているが、論文 (3) ではFindサービスを使用しない。SOME/IPプロトコルの仕様上、Findサービスはオプションであるものの、クライアントが必要とするサービスグループ情報の漏洩につながるため、Findサービスを保護することは重要である。また、通信の接続

開始の起点としてもFindサービスは重要であるため、保護すべきと考える。一方、Offerサービス以降の保護手法については、ほぼ同様の保護を行っており、いずれも差がないと考えらえる。つぎに保護レベルの変更（観点6）については、本提案手法以外に言及される論文はなく、事前に与えられたサービス保護レベルにて保護することが想定されている。しかしながら、SOME/IPのサービスごとに保護レベルを変えたり、クライアントや通信路の状態に応じて、保護レベルと動的に変更させることは有効と考える。

これらの結果より、セキュリティとリアルタイム性のトレードオフを保ちつつ、SOME/IP-SDを保護する手法として、本稿で提案する手法が有効であると結論付ける。

表4　既存研究との比較

観点	論文 (6)	論文 (3)	提案手法
1. クライアント認証	○ (あり)	○ (あり)	○ (あり)
2. サーバ認証	○ (あり)	○ (あり)	○ (あり)
3. 他ノードの鍵漏洩	○ (影響なし)	○ (影響なし)	○ (影響なし)
4. セッション確立時間	× (長い)	△ (比較的長い)	○ (比較的短い)
5. Findサービスの保護	△ (ユニキャスト)	× (なし)	○ (あり)
6. 保護レベルの変更	× (なし)	× (なし)	○ (あり)

5. 考　察

本稿で言及したSOME/IP-SDプロトコルの保護手段の他にも、いくつかの手段が存在する。例えば、IPSecやMACSecを用いた保護手段が考えらえる。IPSecやMACSecを用いる場合、車載要件を満たしたスイッチなどが必要であり、コスト制約の厳しい車載制御システムへの適用は比較的遠い将来になるのではないかと考えられる。しかしながらその一方で、コストを追加することにより、より安全にできる可能性も有る。このため、今後の課題として、本稿では述べられなかった他の保護手段との比較が挙げられる。

6. 結　言

本稿では、セキュリティとリアルタイム性の良いトレードオフを実現するため、SOME/IP-SDの拡張プロトコルを提案した。FindサービスとOfferサービスのシーケンスに対して適切な保護策を施し、既存手法よりも通信オーバーヘッドを低減した方式である。さらに、通信を保護するためのサービス保護レベルを導入することにより、様々な保護手段を動的に変更できることを示した。

今後は、実車への適用、他の保護手段との比較についても議論する予定である。

用 語 集

※1　TLS

Transport Layer Security：インターネットなどのコンピュータネットワークにおいてセキュリティを要求される通信を行うためのプロトコルで、認証・暗号化・改ざんの検出の機能を提供する。多くの場合、コネクション型のトランスポート層プロトコル（通常はTCP）とアプリケーション層の間で使われる。

※2　DTLS

Datagram Transport Layer Security：TLSに基づくプロトコルであり、トランスポート層がUDPの場合にもTLSと同様のセキュリティを確保する目的で設計された。

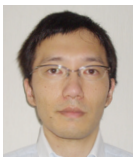
参 考 文 献

(1) SOME/IP Protocol Specification, AUTOSAR FO R22-11 (2022)
(2) SOME/IP Service Discovery Protocol Specification, AUTOSAR FO R22-11 (2022)
(3) D. Zelle, et al., “Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods,” The 16th International Conference on Availability, Reliability and Security, Vienna, Austria (2021)
(4) Specification of Secure Onboard Communication Protocol, AUTOSAR FO R20-11 (2020)
(5) 福田 ほか、「セッション管理サーバによるSOME/IPセキュリティの検討」、ETNET2021、pp1-8 (2021)
(6) M. Iorio, et al., “Protecting In-Vehicle Service : Security-Enabled SOME/IP Middleware,” IEEE Vehicular Technology Magazine, Vol. 15, No.3, pp.77-85 (2020)
(7) vsomeip https://github.com/COVESA/vsomeip

執　筆　者

上田　浩史*：㈱オートネットワーク技術研究所
グループ長

倉地　　亮*：名古屋大学
特任准教授
博士（情報科学）



高田　広章：名古屋大学
センター長・教授
博士（理学）

井上　雅之：㈱オートネットワーク技術研究所
主幹

上口　翔悟：㈱オートネットワーク技術研究所

和田　健治：㈱オートネットワーク技術研究所

＊主執筆者