Vol.2013-ITS-53 No.6
2013/6/14

テレマティクス対応セキュリティシステムの構築

小林 信博[†1]　三澤 学[†1]　泉 幸雄[†1]　坂上 勉[†1]

近年，車載情報システムの高度化が進み，車外の IT システムと通信・連携することでサービスを提供するテレマティクスが注目を集めている．一方，通信路を経由して外部から車載情報システムに侵入，攻撃する手法が報告されており，新たな情報セキュリティ対策が必要となっている．我々は，車載情報システム特有のセキュリティ要件について整理するとともに，外部からの不正アクセスを防止し，車の正常動作を確保する際に必要となるセキュリティ対策技術について検討を行った．特に，リソースの制限される車載装置において，テレマティクスで必要とされる認証機能を搭載する為に，車外のセキュアサーバとの連携ならびに動的なホワイトリストとその効率化に関する方式を考案した．そして，評価システムを開発し，システムの基本性能について評価を行ったところ，その有効性について確認できた．

Proposal of telematics security system

NOBUHIRO KOBAYASHI[†1]　MANABU MISAWA[†1]
YUKIO IZUMI[†1]　TSUTOMU SAKAGAMI[†1]

In this paper, we examined security requirements peculiar to in-vehicle information systems, and considered security countermeasures necessary to prevent unauthorized access from outside and to ensure normal movement of cars. In order to implement an authentication function required by telematics in in-vehicle devices with limited resources, we devised a method for in-vehicle devices to cooperate with a secure server outside, and an efficient method for dynamic white lists. We developed an evaluation system and evaluated the basic performance of the system, thereby having confirmed the effectiveness of our methods.

1. はじめに

近年，携帯電話網に代表される遠隔通信サービスのエリア拡大や普及にともない，クルマをネットワークに接続することで，多様なサービス提供者により運用されるオープンなシステムと協調・連携するテレマティクスという概念が注目を集めている．これまで，クルマと外部との通信を利用したサービスとして国内において普及してきた ETC(Electronic Toll Collection)あるいは DSRC(Dedicated Short Range Communication)等の ITS システム(Intelligent Transport System)は，特定の管理団体による適切な運用がなされ，クルマとの通信相手となる装置も限定的であった．また，クルマの内部には，エンジン制御やドアロックを司る多数の ECU(Electronic Control Unit)が配置され車載ネットワークを構築していた．この車載ネットワークには，CAN(Controller Area Network)[1][2]や LIN(Local Interconnect Network)[3]等の自動車特有の通信方式が利用されており，外界からは隔離され独立のネットワークとなっていた為に，外部からの攻撃は難しいと考えられてきた．

しかし，テレマティクスの概念を取り入れることによってクルマが外部のネットワークと繋がることとなり，一般の IT システム同様に車載情報システムへ攻撃が及ぶとして警鐘が鳴らされている[4]．更に，Checkoway らの報告[5][6]によれば，3G 携帯電話経由でのクルマ外部から車載ネットワークへの不正侵入とクルマの制御をおこなう攻撃が実証されている．

車載情報システムは，その基幹をなす車載ネットワークに各種の ECU，センサ，アクチュエータ，情報機器などが接続されるが，これらは機能から「1. 基本制御機能」「2. 拡張機能」「3. 一般的機能」の三つに分類される[4]．「1. 基本制御機能」はクルマのセーフティに密接な「走る・曲がる・止まる」の基本かつ必須の機能である．「2. 拡張機能」は運転支援及び快適性向上のための機能であり，テレマティクスや ITS もここに位置づけられる．「3. 一般的機能」は携帯型カーナビなどドライバー等による持ち込み機器や後付のエコメータが該当する．テレマティクスの利用により，「1. 基本制御機能」への直接的な攻撃の脅威が発生することは考えにくいが，「2. 拡張機能」を踏み台にした間接的な攻撃が行われる可能性が課題とされている[4]．

上記課題に対して，本論文では，テレマティクスのセキュリティ対策の一つとなる認証に着目し，オープンなネットワーク環境に適した X.509v3 形式[7]の証明書を用いてセキュアな車載システムを実現する方式について提案する．

本論文では，2. にてテレマティクス対応セキュリティシステムの要件分析とセキュア化の課題，3. にて外部のセキュアサーバとの連携による失効管理ならびに認証強度の長期維持に対応した強固な認証と，セキュアサーバとの通信途絶を考慮し動的なホワイトリストとを備えたセキュリティシステムの実現方式の提案をおこない，4. にて本方式を適用した評価システムの開発，5. にて評価システムを用い

†1 三菱電機株式会社
Mitsubishi Electric Corporation

たシステムの基本性能の評価結果について述べ，6. にて結果を考察し，最後にまとめを行う．

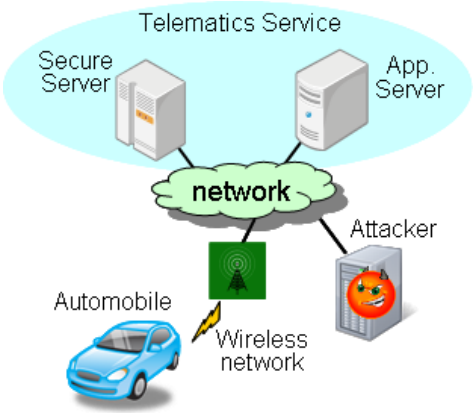

図 1　提案システム構成概略

Figure 1　Components of Proposal System.

2. テレマティクス対応セキュリティシステムの要件分析とセキュア化の課題

2.1 テレマティクス対応セキュリティシステムの要件分析

テレマティクスの概念を取り入れることにより車載情報システムが外部のネットワークと繋がることとなり，多様なサービスによる付加価値の向上が期待できる半面，人命に重大な影響を与える脅威をもたらす恐れがある．

一方，システム外部からの不正アクセス対策の一つとして，主体が客体の正当性を検証する“認証”が知られている．我々はクルマの外部からの攻撃に対抗する為のセキュリティを検討するにあたり，車載情報システムの動向分析[4] にて挙げられた「ネットワーク接続」,「オープン化」,「安全快適機能」を念頭に置き，中核をなす対策技術として，特にこの認証に着目している．

また，現在インターネットに代表されるオープンなネットワーク環境において，セキュリティを確保する認証の枠組みとして普及している技術の一つに PKI（Public Key Infrastructure）[8]が挙げられる．一般的な PKI では，信頼できる第三者機関として位置付けられた認証局（CA：Certification Authority）から X.509v3 形式の証明書が発行される．証明書の所有者は，これを利用することで，自分の身元の正当性を相手に証明することができる．この X.509v3 形式の証明書は，インターネット上で各種サービスを提供している SSL/TLS[9]サーバの認証や，サーバとクライアント間の VPN（Virtual Private Network） 接続を行う IPsec[10]の認証等に広く利用されている．そのため，クルマがテレマティクスのサービスを利用する場合にも，現在インターネット上で普及しているネットワーク上のサービスと同様の認証方式を採用することが，早期展開ならびに各種サービスとの融合によるシナジー効果を発揮する上で，有利であると考えられる．また，クルマの将来を見据えた場合にも，EV（Electric Vehicle） への搭載が必要となる車載充電装置と外部の充電スポットとの間の通信のセキュリティとして， SSL/TLS を利用する IEC 15118[11]の標準化作業が進められている最中である．

一方，X.509v3 形式の証明書には有効期間が定められており，証明書の所有者が秘密に保持する秘密鍵の意図せぬ漏洩による被害の抑制や，計算量的な安全性に基づくセキュリティ強度の確保を，CA による証明書の再発行（更新）により実現している．また，秘密鍵の漏洩事故発生等の理由により有効期間内に証明書を失効させる為に，CA が定期的に CRL（Certificate Revocation List）を発行し， CRL の発行時点における証明書の有効性が確認できる仕組みが導入されている．更に，X.509v3 形式の証明書は，スケーラビリティ確保の観点から階層構造に対応している．信頼点（Trust Anchor）となる階層構造の最上位に位置するルート認証局（root CA）の証明書から，その下に繋がる多段の中間認証局（intermediate CA）の証明書，および最下層に位置する所有者（主体者）のエンドエンティティ証明書（End Entity Certificate）に至る信頼の連鎖（Chain of Trust）が，各証明書に含まれる上位 CA の署名情報により検証することが可能である．

次に，運用期間，利用環境，用途の観点から，PC やサーバ等の IT 機器とクルマとの特性の違いについて，比較を行う．

国内におけるクルマの平均使用年数に関する推移[12]によれば，普通乗用車で 12.56[年]となっており，PC メーカ各社が公表している補修用性能部品の保有期間から推定される PC の使用年数 6～8[年]よりも長期に渡る安全性の確保が求められると考えられる．従って，開発期間の猶予も含めると 20 年先（2030 年）を見越したセキュリティ強度の確保を，車載装置に対するコストインパクトを抑えつつ考慮する必要がある．

また，利用環境を考えると，屋内の整備された環境で稼動する PC やサーバと異なり，クルマは広域の屋外を高速に移動しながら稼動する．基本的にはクルマが走行する為の道路が整備された場所となるが，都市部でのトンネルや立体交差，地下駐車場，そして山間部や僻地においては，テレマティクスの前提となる外部ネットワークとの通信品質の悪化や途絶が発生する恐れがある．同時に，外部ネットワークを提供･運用する通信事業者･回線事業者の事情，あるいはバックボーンとなるインターネットのベストエフォート型のサービス特性から，クルマと目的とするサーバとの通信不能状態が発生することも想定される．

更に，クルマの用途を考えると，我々が生活を営む社会のなかで，法令[13]に基づき運転者が業務として運転することが基本となることから，運転者や乗員，そして歩行者に対する人体・生命の安全確保を最優先事項として取り扱

う必要がある．従って，情報システムにおける機密性（Confidentiality），完全性（Integrity），可用性（Availability）の各セキュリティに対する優先度が C.I.A の順となるのに対し，重要インフラの制御システムが可用性を最も重視[14]していることと同様, A.I.C の順番でセキュリティを考えていく必要がある．

以上から導かれるテレマティクス対応セキュリティシステムの要件を以下にまとめる．

要件 1.
テレマティクスにおけるセキュリティ確保の為に，
インターネットで普及している認証方式の採用が有利
要件 2.
クルマの長期運用に対応したセキュリティ強度の
確保が必要（目標：2030 年までの安全性維持）
要件 3.
身体・生命の安全を第一に通信途絶時の可用性を重視したセキュリティ機能の実現が必要

これらの要件を念頭に，テレマティクス対応セキュリティシステムの方式検討を行う必要がある．

2.2 セキュア化の課題

前節の要件に基づき，インターネットで普及している SSL/TLS あるいは IPsec 等のセキュリティプロトコルにおいて X.509v3 形式の証明書を用いた認証を実現する為には，その認証機能の内部で証明書検証の処理が必要となる．一般的な証明書検証の検証項目を以下に示す．

① 証明書の有効期間内であること
　… 現在時刻と有効期間を比較
② 証明書の内容が期待通りであること
　… 証明書の拡張領域の内容を確認
③ 証明書への上位 CA の署名が正しいこと
　… 証明書に上位 CA が付与した署名の検証
④ 認証パスの構築・検証に成功すること
　…証明書の信頼の連鎖が検証者の信頼点に到達すること．各 CA の証明書の証明書検証を含む．
⑤ 証明書が失効していないこと
　… CRL 等の失効情報を入手して確認

上記項目のうち，①～④については，検証に必要な証明書が相手から提供される場合，クルマ内部で処理を完結することが可能である．一方，⑤の処理は，各証明書を発行した CA から発行される CRL を入手し，その CRL 自身の正当性の検証を行う必要がある．

CRL は有効期限内に失効した全ての証明書が記載される為，膨大なサイズになる可能性がある．また，CRL は CA 毎に発行されることから，検証に必要な CRL 全てをクルマにダウンロードする為の通信時間，通信トラフィックが発生する．このような課題に対して，CRL のサイズ削減を目的として，前回発行時からの差分となる証明書のみを含めて発行するデルタ CRL という方式[7]も存在するが，この方式では過去の CRL 情報を全てクルマ側のデータベースに保存しておく必要があり，その保存領域の確保や管理が課題となる．

⇒【課題 1.】認証に用いる証明書の失効の検証が困難

また，クルマの長期運用に対応したセキュリティ強度を確保する為には，暗号アルゴリズムを適切に利用することが必要となる．セキュリティの根幹をなす暗号アルゴリズムは，素因数分解問題や離散対数問題などその安全性の根拠となる数学的な問題の困難性に依存する宿命を持ち，解読技術や計算機の処理能力の向上により，長期的には危殆化の必然性を有することが指摘されている[15] [16] [17]．既に我々は，暗号危殆化への対策の 1 つとなる鍵の更新に関する安全性について考察し，RSA 暗号アルゴリズムの公開鍵長 1024[bits] について，2020 年には現実的な更新間隔での運用が困難との結果を得ている[18]．従って，2030 年を視野にセキュリティ強度を確保するには，それ以上の鍵長となる 2048[bits], 4096[bits]が必要となるが，その場合には検証項目③の計算処理時間が増加することとなる．

⇒【課題 2.】長期的な安全性確保の為の鍵長増加に伴う処理性能の低下

以上で述べた要件と課題との対応関係を表 1 に示す．

表 1　要件と課題の対応関係
Table 1　Comparison between requirement and problem.

要件	【課題 1.】	【課題 2.】
要件 1.	該当	－
要件 2.	－	該当
要件 3.	該当	該当

3. 提案方式

3.1 方針

2.の結果を考慮し，本論文では，クルマが車外のセキュアサーバと連携して，X.509v3 形式の証明書を用いた認証に基づくセキュアな車載システムを実現する方式について検討していく．

以下，図 2 に示した本提案方式における認証処理の概略をもとに説明する．

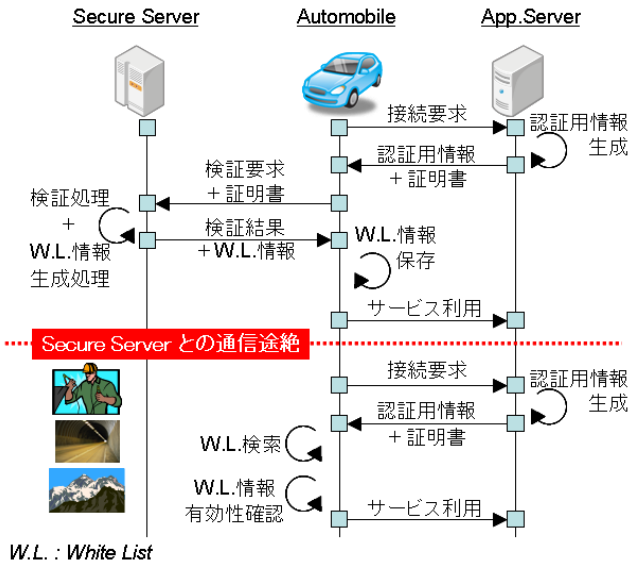

図 2　提案方式における認証処理概略

Figure 2　Authentication Procedure of Proposal System.

3.2 セキュアサーバとの連携による証明書検証

まず，課題 1. の対策として，失効確認を含む証明書の検証処理を，クルマのかわりにセキュアサーバにて実行することとする．このセキュアサーバは，クルマにとってのTTP（Trusted Third Party）として取り扱う．証明書検証に必要な検証項目を，サーバ側で処理する既存のプロトコルとしては，OCSP（Online Certificate Status Protocol）[19]が知られているが，検証項目②～④の処理には対応していない．一方，SCVP（Server-based Certificate Validation Protocol）[20]および DVCS（Data Validation Certificate Server）[21]では，全ての項目をサーバ側で処理することが可能となり，クルマ側の処理を大幅に削減できることとなる．従って，SCVP あるいは DVCS に相当するクライアント機能をクルマ側に，サーバ機能をセキュアサーバ側に搭載することとする．セキュアサーバは，クルマと比較して豊富な計算リソースを持たせることが可能であるとともに，クルマがテレマティクスに利用する無線通信と比較すると高速で信頼性の高い通信インフラを備えていると想定される．従って，失効状態を含む証明書検証を高い処理性能と信頼性をもって実施することができると考えられる．

また，長期的な安全性確保の為の鍵長増加に伴う処理性能の低下という課題 2. に対しても，同様にサーバ側の高い処理能力を活用することで，カバーすることができる．更に，セキュアサーバ側の処理として，証明書の検証結果から，クルマとセキュアサーバとの通信途絶時に利用する後述のホワイトリストに登録する W.L.情報（検証キャッシュ）を生成し，検証結果とともにクルマに提供することとする．

3.3 動的なホワイトリストを用いた証明書検証

要件 3. に述べたように，テレマティクスのセキュリティ機能には通信途絶時の可用性が求められる．そこで，クルマが単独で検証項目⑤を含む証明書検証を実施可能とする為に，ホワイトリストを用いることとする．このホワイトリストには，セキュアサーバにて正当性が検証された証明書に関する情報（W.L.情報）を登録する．W.L.情報には証明書の有効期間や CRL の次回更新日時（nextUpdate）を考慮した W.L.情報そのものの有効期限を含めることとし，証明書検証処理とあわせてセキュアサーバ側で生成することにより，クルマ側の追加処理を不要とする．クルマに蓄積されたホワイトリストは，W.L.情報により動的に更新され，常に最新の状態に保たれる．そして，通信途絶等の理由によりセキュアサーバとの連携不能時には，クルマがこのホワイトリストと証明書のマッチングにより，検証項目の①～⑤に相当する処理を簡略化して行うことが可能となる．従って，通信途絶時にも安全性の確認された証明書に基づく認証によって，セキュリティ機能の可用性が担保できる．

また，ホワイトリストを用いた証明書の有効性の確認処理は，証明書そのものを W.L.情報として用いることにより，ASN.1 形式で格納されている証明書情報のデコードをすることなく，バイナリレベルでのマッチングで処理することも可能である[22]．しかし，ホワイトリストに登録する証明書の枚数に比例してその記憶領域が必要となるため，クルマの限られたリソースへの影響が懸念される．証明書の署名アルゴリズムとして現在一般的な RSA 暗号を利用する場合，安全性と密接に関係する鍵長[23]が，証明書所有者の公開鍵（subjectPublicKeyInfo の subjectPublicKey）ならびに，CA の署名値（signatureValue）のサイズに影響を及ぼす．CA と EE が同一の鍵長を利用するケースでは，RSA 2048[bits] で 512 [octet]，RSA 4096[bits] で 1024 [octet] の格納領域が証明書の内部に必要になる．

そこで今回は，ホワイトリストのサイズ削減の為に，証明書のハッシュ値を生成し，これを W.L.情報として利用することとする．一般的に証明書のサイズは，利用する鍵長や格納される情報により不定ではあるが，上記公開鍵や署名値の合計以上となることは確実である．一方，ハッシュアルゴリズムとして SHA-256 を用いる場合，ハッシュ長は 32[octet]に固定となり，証明書そのものをホワイトリストに登録する場合よりも必要な記憶領域を削減することが可能となる．

4. 評価システムの開発

提案方式を実装したテレマティクスシステムの評価システム構成について図 3 に示す．

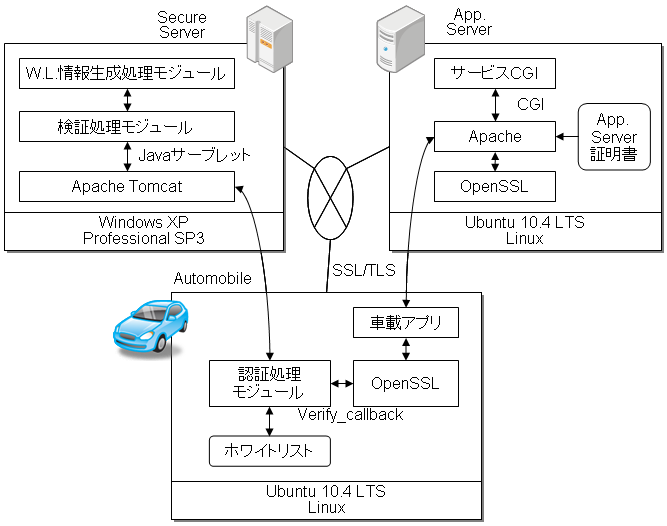

図 3　評価システム構成
Figure 3　Components of Evaluation System.

評価システムには，テレマティクスサービスを提供するアプリサーバ(App. Server)，テレマティクスサービスを利用する車載情報システム(Automotive), 車載情報システムと連携するセキュアサーバ(Secure Server)の各装置が存在する．車載情報システム(Automotive)を模擬する PC 上に，アプリサーバをセキュアサーバと連携して認証する為の機能を，認証処理モジュールとして実装した．また，セキュアサーバ上に，車載情報システム上の認証処理モジュールからの検証要求に対応する証明書の検証処理モジュールおよび W.L.情報生成処理モジュールを実装した．そして，これらの各装置を 100BASE-TX ネットワークで接続する構成とした．表 2 に各装置の仕様を示す

表 2　評価システム装置仕様
Table 2　Specifications of Evaluation System.

装置名称	プロセッサ	動作周波数	RAM	OS
車載情報システム.	Intel Core2 Duo	2GHz	1GB	Ubuntu 10.4 LTS Linux
セキュアサーバ	Inter Core2 Duo	2GHz	2GB	Windows XP Professional SP3
アプリサーバ	Intel Core Duo	1.8GHz	1GB	Ubuntu 10.4 LTS Linux

4.1 車載情報システム

車載情報システムには，OpenSSL[24]ライブラリを利用して，アプリサーバからテレマティクスサービスを模擬した情報を SSL/TLS 経由でうけとる車載アプリを搭載した．また，OpenSSL ライブラリが通信相手となるサーバの認証の為に SSL/TLS プロトコルに基づき実施する証明書検証に関して，本提案方式を実装した認証処理モジュールを OpenSSL の検証コールバック(verify_callback)として呼び出すこととした．従って，SSL/TLS に対応済の車載アプリの場合，本提案方式を実装する為に追加する処理は，認証処理モジュールの検証コールバック登録処理のみとなる．

認証処理モジュールは，アプリサーバの証明書のハッシュ値を算出し，ホワイトリストに登録された W.L.情報の中から一致する証明書のハッシュ値を検索する．一致した W.L.情報が有効期限内の場合には，検証成功と判定し，その他の場合は，セキュアサーバに対して証明書の検証を要求する．そして，セキュアサーバの応答が検証成功の場合は，セキュアサーバの生成した W.L.情報をホワイトリストに登録し，検証失敗の場合は，アプリサーバが不正であると判定する. 表 3 にホワイトリストに登録する W.L.情報のデータフォーマットを示す.

表 3　W.L.情報のデータフォーマット
Table 3　Data Format of White List Information.

データ名称	サイズ
登録状態（済/未）	1 [octet]
証明書ハッシュ値（SHA-256）	32 [octet]
有効期限（YYYYMMDDhhmmss）	14 [octet]
登録日時（YYYYMMDDhhmmss）	14 [octet]

4.2 セキュアサーバ

セキュアサーバには，車載情報システムの認証処理モジュールから証明書検証要求とともに証明書を受け取り，証明書の検証処理を実施する検証処理モジュールを実装した．また，W.L.情報として正当性が検証された証明書の SHA-256 ハッシュ値と有効期限を生成する W.L.情報生成処理モジュールを実装した．各モジュールは，セキュアサーバに搭載した Apache Tomcat[25]のサーブレットとして実現した．また，検証処理モジュールのトラストアンカーとしてアプリサーバの証明書を発行した認証局のルート証明書を登録した．

4.3 アプリサーバ

Apache[26]および OpenSSL により SSL/TLS 対応の WEB サーバをアプリサーバとして実装した．また，テレマティクスサービスを模擬した情報を車載アプリへ提供する為にサービス CGI を実装した．WEB サーバには，アプリサーバ用の証明書（公開鍵長: RSA 2048[bits]）を登録した．

5. 評価

開発した評価システムを用いて，車載情報システムにおける認証処理モジュールの性能評価を行った．

5.1 認証処理モジュールにおける証明書検証

評価システムを用いて，認証処理モジュールにおける証明書検証の性能評価を行った．認証処理モジュールにおける下図に示した各処理の処理時間を測定した．

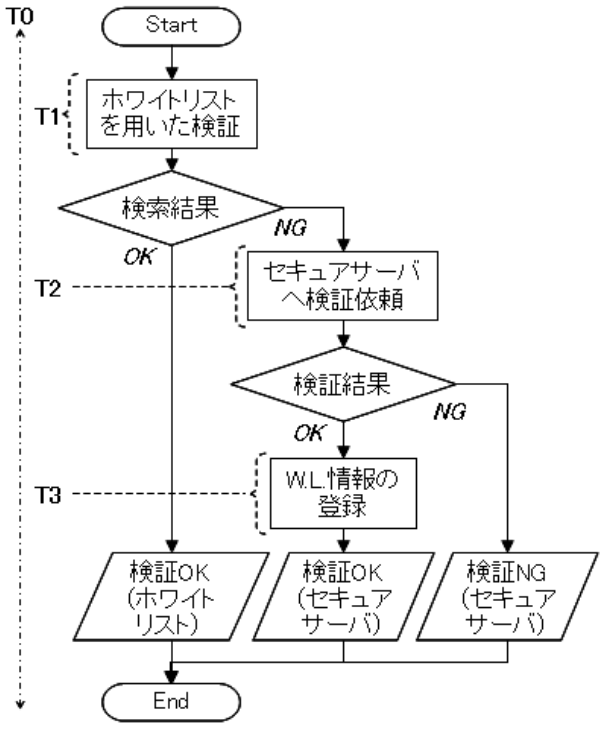

図 4　処理時間の測定対象
Figure 4　Target Functions of Evaluation.

(1) **T0:認証処理モジュール全体処理時間**
- 検証コールバック全体

(2) **T1:ホワイトリストを用いた検証処理時間**
- アプリサーバの証明書のハッシュ値算出
- ホワイトリストの検索
- 有効期限の確認
- 期限切れ W.L.情報の削除

(3) **T2:セキュアサーバへの検証依頼処理時間**
- 検証要求の生成および送信
- 検証結果の受信および解析

(4) **T3:W.L.情報のホワイトリストへの登録処理時間**
- ホワイトリストへの W.L.情報の登録

認証処理モジュールにおける証明書検証の性能評価結果について表 4 に示す．

評価結果について確認したところ，ホワイトリストに登録されている W.L.情報に一致するアプリサーバの証明書の検証処理が 169.3[usec]かかっており，そのうち T1 の処理時間が 32.8[usec]であることが確認できた．

そして，ホワイトリストに含まれずセキュアサーバにて正当性が検証された場合の検証処理が 247.0[usec]かかっており，そのうち T1 の処理時間が 33.5[usec]，T2 が 163.6[usec]，T3 が 19.4[usec]であることが確認できた．

更に，ホワイトリストに含まれずセキュアサーバにて無効と判定された場合の処理時間が 214.3[usec]かかっており，そのうち T1 の処理時間が 33.5[usec]，T2 が 173.8[usec]であることが確認できた．

また，本機能はほぼリアルタイムで完了する処理であることが確認できた．

表 4　認証処理モジュールにおける性能評価結果
Table 4　Evaluation Result of Authentication Function.

処理結果	T0 [usec]	T1 [usec]	T2 [usec]	T3 [usec]
検証 OK (ホワイトリスト)	169.3	32.8	－	－
検証 OK (セキュアサーバ)	247.0	33.5	163.6	19.4
検証 NG (セキュアサーバ)	214.3	33.5	173.8	－

6. 考察

5.に示した評価結果を確認したところ，アプリサーバの認証における証明書検証処理が，最大 247.0[usec]で完了することが確認できた．また，検証対象の証明書がホワイトリストに登録されている場合，169.3[usec]で検証処理を完了することが確認できた．従って，本提案方式によれば，強固なセキュリティによる安全性と，セキュアサーバとの通信途絶時の可用性に加えて，通常時においても処理時間を約31%高速化することが可能になるという利点が確認できた．

また，クルマが時速 100[km/h]で移動している場合を想定すると，上記処理中に移動する距離は，1[cm]未満であり，本提案処理をクルマに適用することで，安全な運行に重大な影響を及ぼす処理遅延を招く可能性は低いと考えられる．

なお，今回の評価システムは，有線での理想的な通信環境を備えていたが，実システムでは T2 の処理時間における通信そのものの占める時間が増大することが予想される．従って，クルマとセキュアサーバのネットワーク上の距離を狭め，TCP 通信における往復遅延時間(Round Trip Time)を短縮する等の考慮が必要と考えられる．また，ホワイトリストの有効期限切れや，新たに接続するアプリサーバの認証におけるオーバーヘッドを低減・解消する方策について，更に考慮していく必要がある．

7. おわりに

本論文では，クルマがセキュアサーバと連携して，X.509v3 形式の証明書を用いた認証に基づくセキュアな車載システムを実現する方式について提案し，その評価システムを開発した．まず，クルマにおいて認証に用いる証明書の失効状態の検証が困難であるという課題に対して，セキュアサーバと連携することにより，サーバ側の豊富な計算リソースおよび無線通信よりも高速で信頼性の高い通信インフラを利用して失効状態を含む証明書検証を実施することができることとした．また，長期的な安全性確保の為の鍵長増加に伴う処理性能の低下という課題に対しても，同様にサーバ側の高い処理能力を活用することで，カバーすることができる．更に，可用性の面からセキュアサーバとの通信途絶を想定し，証明書の検証結果を動的なホワイトリストとしてクルマ側に蓄積することで，クルマ単独での安全な検証処理を可能とした．加えて，ホワイトリストに登録する W.L.情報として，証明書そのものを利用するのではなく，証明書のハッシュ値，および証明書の有効期間をふまえた有効期限を利用することで，クルマの限られたリソースへの配慮と処理負荷の軽減を図った．

上記結果に基づき，評価システムを開発し，システムの基本性能について評価を行った．評価結果を確認したところ，アプリサーバの認証における証明書検証処理が，最大 247.0[usec]，検証対象の証明書がホワイトリストに登録されている場合，169.3[usec]で検証処理を完了するという結果が得られ，有効性について確認することができた．

本方式によって，テレマティクスシステムにおけるセキュリティ確保の為に，インターネットで普及している認証方式が活用可能となり，早期展開ならび各種サービスとの融合によるシナジー効果の発揮が期待できる．また，車載装置のコストインパクトを抑えつつ長期にわたるセキュリティ強度の確保が可能となる．更に，通信途絶などの障害が発生した場合でも，セキュリティ機能の可用性を確保することが可能であり，クルマの誤動作等により身体・生命の安全が損なわれる事態を回避可能と考える．また，今回ターゲットとした車載情報システムは，各種移動体システムの構成要素として共通な為，本方式をクルマ以外の様々な制御系組込み機器にも広く適用することが可能である．

参考文献

1) the International Organization for Standardization: Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling, ISO 11898-1:2003 (2003)
2) the International Organization for Standardization: Road vehicles -- Low-speed serial data communication -- Part 1: General and definitions, ISO 11519-1:1994 (1994)
3) LIN CONSORTIUM: TECHNICAL OVERVIEW, http://www.lin-subbus.org/
4) 独立行政法人 情報処理推進機構セキュリティセンター: 2011 年度 自動車の情報セキュリティ動向に関する調査 (2012)
5) Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage: Experimental Security Analysis of a Modern Automobile, Proceedings of IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 447-462 (2010)
6) Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno: Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Association, Proceedings of the 20th USENIC conference on Security (2011) http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf
7) The Internet Engineering Task Force: RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2008) http://tools.ietf.org/html/rfc5280
8) The Internet Engineering Task Force: RFC5246 The Transport Layer Security (TLS) Protocol Version 1.2 (2008) http://tools.ietf.org/html/rfc5246
9) Carlisle Adams, Steve Lloyd: Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, MACMILLAN TECHNICAL PUBLISHING (1999)
10) The Internet Engineering Task Force: RFC4301 Security Architecture for the Internet Protocol, (2005) http://tools.ietf.org/html/rfc4301
11) the International Organization for Standardization: Road vehicles -- Vehicle to grid communication interface -- Part 2: Network and application protocol requirements, ISO/IEC DIS 15118-2 (2012)
12) 一般財団法人 自動車検査登録情報協会: わが国の自動車保有動向 車種別の平均使用年数 推移（昭和 51～平成 24 年）(2012) http://www.airia.or.jp/number/pdf/03_32.pdf
13) 国家公安委員会（警察庁 交通局）: 道路交通法, 昭和 35 年 6 月 25 日 法律第 105 号 (1960) http://www.npa.go.jp/syokanhourei/houritsu.htm
14) 独立行政法人 情報処理推進機構セキュリティセンター: 重要インフラの制御システムセキュリティと IT サービス継続に関する調査, pp.62 (2009) http://www.ipa.go.jp/security/fy20/reports/ics-sec/rep_main_fy20.pdf
15) 独立行政法人 情報処理推進機構セキュリティセンター: 暗号の危殆化に関する調査 報告書 (2005) http://www.ipa.go.jp/security/fy16/reports/crypt_compromize/documents/crypt_compromize.pdf
16) 小林 信博, 米田 健: 長期運用可能な機器認証方式, IEICE, Symposium on Cryptography and Information Security (2010)
17) National Institute of Standards and Technology: Recommendation for Key Management Part 1: General (Revised), Special Publication 800-57, Special Publications (800 Series), pp.66 (2007)
18) http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
19) 独立行政法人 情報処理推進機構セキュリティセンター:「安全な暗号鍵のライフサイクルマネージメントに関する調査」に関する報告書 (2008)
20) The Internet Engineering Task Force: RFC2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (1999) http://tools.ietf.org/html/rfc2560
21) The Internet Engineering Task Force: RFC5055 Server-Based Certificate Validation Protocol (SCVP) (2007) http://tools.ietf.org/html/rfc5055
22) The Internet Engineering Task Force: RFC3029 Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (2001) http://tools.ietf.org/html/rfc3029
23) 独立行政法人情報通信研究機構: CRYPTREC 報告書 電子政

府推奨暗号の利用方法に関するガイドブック (2007)
http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf
24) 小林 信博, 中川路 哲雄: ユビキタス PKI 高速化手法について, IPSJ, Multimedia, Distributed, Cooperative, and Mobile Symposium 2003 (2003)
25) OpenSSL:
http://www.openssl.org/news/.
26) Apache Tomcat:
http://tomcat.apache.org/.
27) The Apache Software Foundation:
http://www.apache.org/.
28) 小林 信博, 三澤 学, 泉 幸雄, 坂上 勉: テレマティクス対応セキュリティシステム, IEICE, Symposium on Cryptography and Information Security 2013 (2013)