特集論文

テレマティクス対応セキュリティ技術

小林信博* 三澤 学*
坂上 勉*
泉 幸雄*

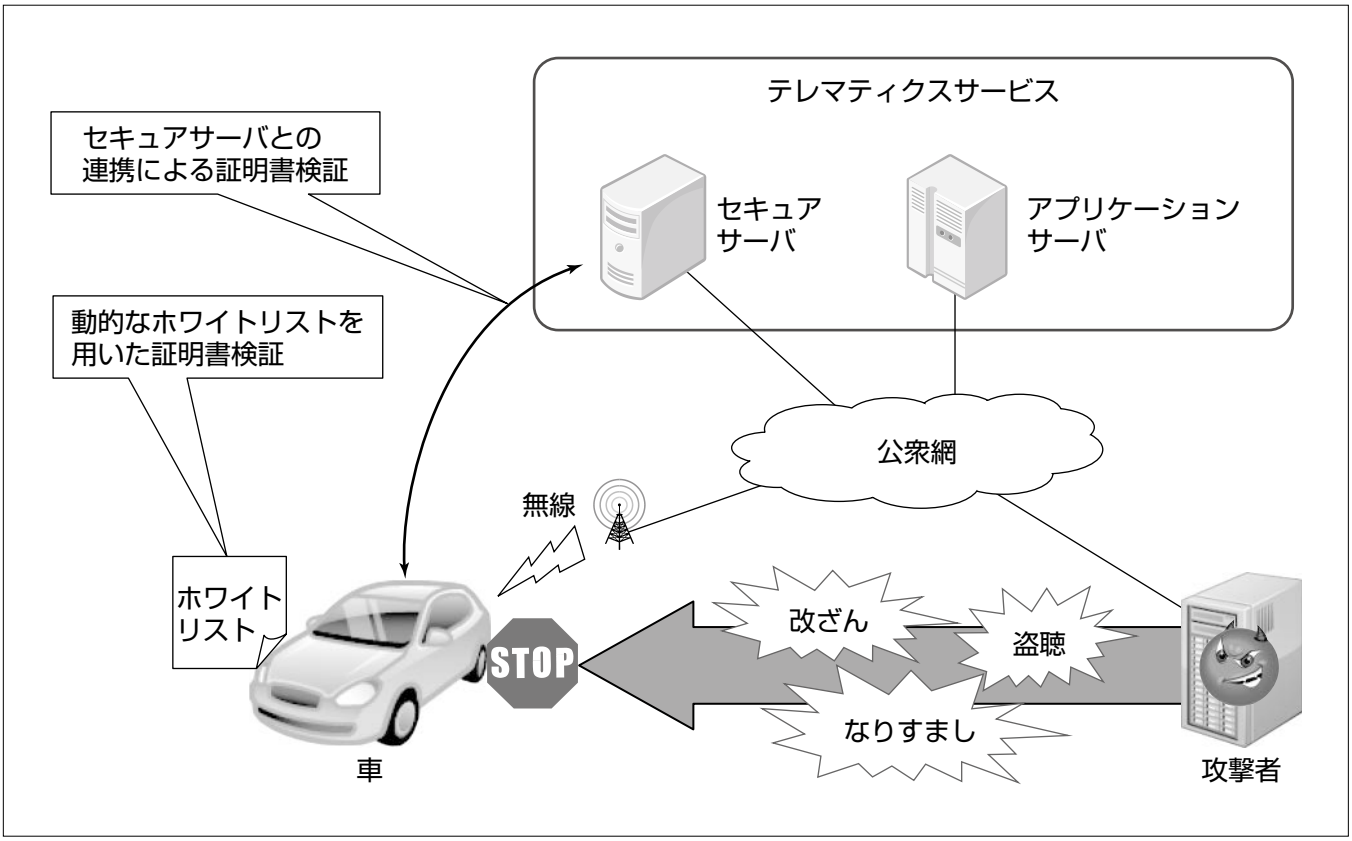
Applying Information Security Technology to Telematics Systems

Nobuhiro Kobayashi, Tsutomu Sakagami, Yukio Izumi, Manabu Misawa

要 旨

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求められている。車載情報システムに適用する情報セキュリティ対策には，クルマの利用環境を考慮した，長期運用に対応可能であり，かつ，可用性を重視したセキュリティ機能の実現が必要である。また，車載情報システムの早期展開と各種サービスとの融合によるシナジー効果を発揮させるためにはインターネットで普及している認証方式を利用することが有利である。

本稿では，車載情報システム特有のセキュリティ要件と課題を整理するとともに，そのセキュリティ対策技術として，車載情報システムが証明書の失効状態を確認するため，豊富なリソースと信頼性の高い通信インフラを利用可能なセキュアサーバと連携する証明書検証方式と，セキュアサーバとの通信途絶時に可用性を確保するため，セキュアサーバで正当性が検証された証明書に関する情報を動的に生成してホワイトリストとして用いる証明書検証方式について述べる。この技術によって，インターネットで普及している認証方式を活用しつつ，車載情報システムへのコストインパクトを抑えた長期にわたるセキュリティ強度の確保が可能となる。さらに，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できる。



テレマティクス対応セキュリティ技術のシステム全体像

テレマティクス対応セキュリティ技術では，サーバ側の豊富なリソースと信頼性の高い通信インフラを利用することで，失効状態を含む証明書検証が可能となり，鍵長増加に伴う処理負荷を軽減できる。また，セキュアサーバで正当性が検証された証明書に関する情報をホワイトリストとして保持することで，証明書検証に要する車側のリソースの削減や処理負荷を軽減し，クルマ単独での安全な検証処理が可能となり高い可用性を維持できる。

*情報技術総合研究所

1. まえがき

近年，携帯電話などの遠隔通信サービスの普及に伴い，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って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。これまで国内で普及してきたETC（Electronic Toll Collection System）又はDSRC（Dedicate Short Range Communication）等のITS（Intelligent Transport Systems）システムは，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つかさどる多数の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）やLIN（Local Interconnect Network）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ため，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，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[1]。さらに，遠隔通信経由で車載ネットワークへ攻撃できることが実証されている[2]。

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，情報機器等が接続されるが，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3つに分類される[1]。

①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もここに位置付けられる。③は携帯型カーナビなどドライバなどによる持込み機器や後付けのエコメータが該当する。テレマティクスの利用によって①基本制御機能への直接的な攻撃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[1]。

この課題に対して，**図1**に示すスコープから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[3]の証明書を用いてセキュアな車載情報システムを実現する方式について提案する。

2. 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

2.1.1 インターネットで普及している認証方法の採用（要件1）

テレマティクスの概念を取り入れることによって，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おそれがある。

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。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で，セキュリティを確保する認証の枠組

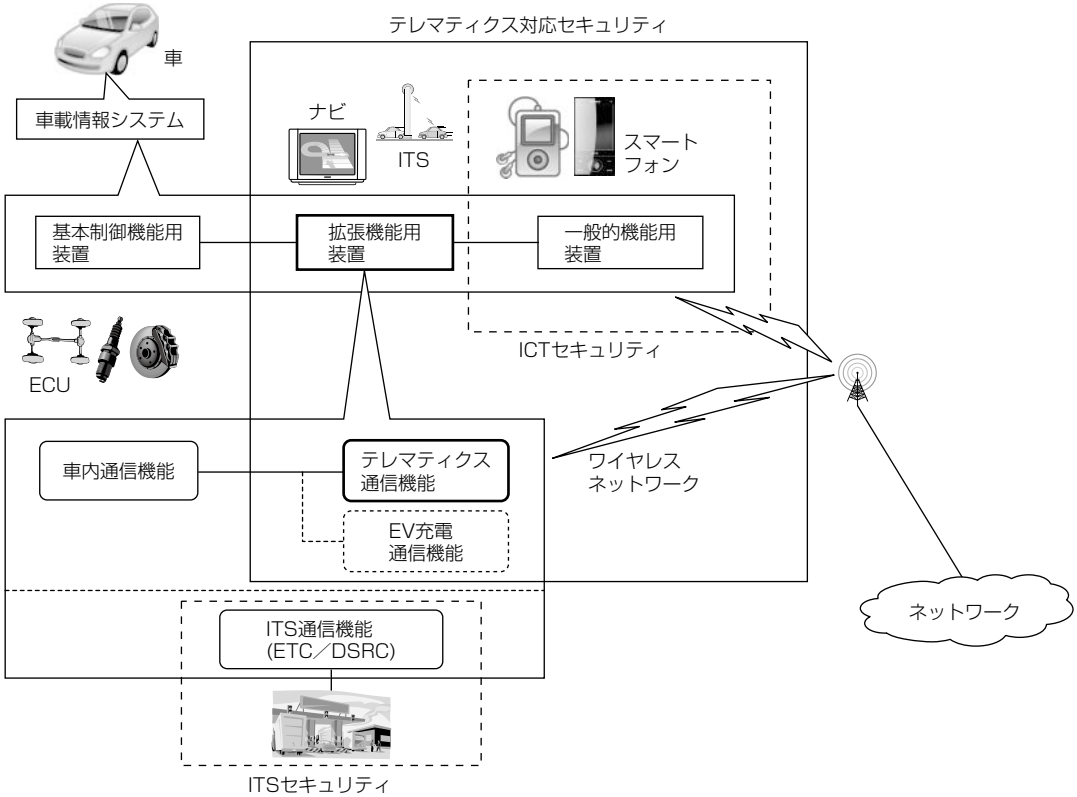


図1．テレマティクス対応セキュリティのスコープ

みとして普及している技術の一つにPKI(Public Key Infrastructure)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(Certificate Authority：CA)からX.509v3形式の証明書(証明書)が発行され，この証明書を利用することで身元の正当性を相手に証明することができる。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(Secure Socket Layer)／TLS(Transport Layer Security)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(Security Architecture for Internet Protocol)の認証に広く利用されている。したがって，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)用車載充電装置と外部の充電スポットとの通信のセキュリティとして，SSL／TLSを利用するIEC 15118の標準化作業が進められている最中である。

一方，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プライベートキーの意図せぬ漏洩(ろうえい)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によって実現している。また，プライベートキーの漏洩事故発生などの理由によって有効期間内に証明書を失効させるために，CAが定期的に証明書失効リスト(Certificate Revocation List：CRL)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。CAの階層構造によってスケーラビリティを確保できる。

2.1.2　長期運用に対応したセキュリティ強度の確保(要件2)

パソコンやサーバ等のIT機器とクルマとの特性の違いについて，運用期間，利用環境，用途の観点から比較する。統計によればクルマの平均使用年数は，普通乗用車で12.56年となっており，パソコンの使用年数6～8年よりも長期にわたる安全性の確保が求められると考えられる。したがって，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。

2.1.3　安全を第一に可用性重視のセキュリティが必要(要件3)

クルマの利用環境を考えると，屋内の整備された環境で稼働するIT機器と異なり，広域の屋外を高速に移動する。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(へきち)，さらに，離島では，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おそれがある。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，又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。

さらに，クルマの用途を考えると，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。したがって，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。

2.2　セキュア化の課題

2.2.1　認証に用いる証明書の失効の検証が困難(課題1)

2.1節の要件に基づき，証明書を用いた認証を実現するためには，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次に示す。

(1)　証明書の有効期間内である
(2)　証明書の拡張領域の内容が期待通りである
(3)　証明書への上位CAの署名が正しい
(4)　認証パスの検証に成功(信頼の連鎖が信頼点に到達)
(5)　証明書が失効していない(CRLの入手と確認)

これらの項目のうち，(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ため，膨大なサイズになる可能性がある。また，CRLはCAごとに発行されることから，全てをクルマにダウンロードするための通信時間，通信トラフィックが発生する。

2.2.2　長期的な安全確保のための鍵長増加に伴う処理性能の低下(課題2)

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ためには，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って，長期的には危殆(きたい)化の必然性を持つことが指摘されている。既に我々は，暗号危殆化への対策の一つとなる鍵の更新に関する安全性について考察し，RSA(Rivest，Shamir，Adleman)暗号アルゴリズムの鍵長1,024ビットについて，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。したがって，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2,048ビット，4,096ビットが必要となるが，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。

2.3　要件と課題の対応

2.1節と**2.2節**で述べた要件と課題について，要件1を実現するためには課題1を，要件2を実現するためには課題2を，さらに要件3を実現するためには課題1と課題2を解決する必要がある。

3. 提 案 方 式

2章で述べた要件と課題を考慮し，この章では，クルマがテレマティクスサービスの一つとなるセキュアサーバと連携して，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。次に，**図2**に示したこの提案方式における認証処理を基に述べる。

3.1　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，クルマのかわりにテレマティクスサービスの1つとなるセキュアサーバで実行することとする。このセキュアサーバは，クルマにとっての信頼できる第三者機関として取り扱う。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)，SCVP(Server-Based Certificate Validation Protocol)，DVCS(Distributed Version Control System)が知られている。このうち，OCSPは**2.2.1項**で挙げた検証項目(2)～(4)の処理には対応していない。一方，SCVP及びDVCS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。したがって，プロトコルの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，豊富な計算リソース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ため，失効状態を含む証明書検証を高い処理性能と信頼性を持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ため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。さらに，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.(White List)情報を生成し，検証結果とともにクルマに提供することとする。

3.2　動的なホワイトリストを用いた証明書検証

2.1.3項の要件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，クルマが単独で証明書検証を実施可能とするため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，セキュアサーバで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.情報には認証パス上の各証明書の有効期間やCRLの次回更新日時を考慮した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って，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.情報によって動的に更新され，常に最新の状態に保たれる。そして，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って，**2.2.1項**で挙げた検証項目(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。したがって，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。なお，恒久的な信頼対

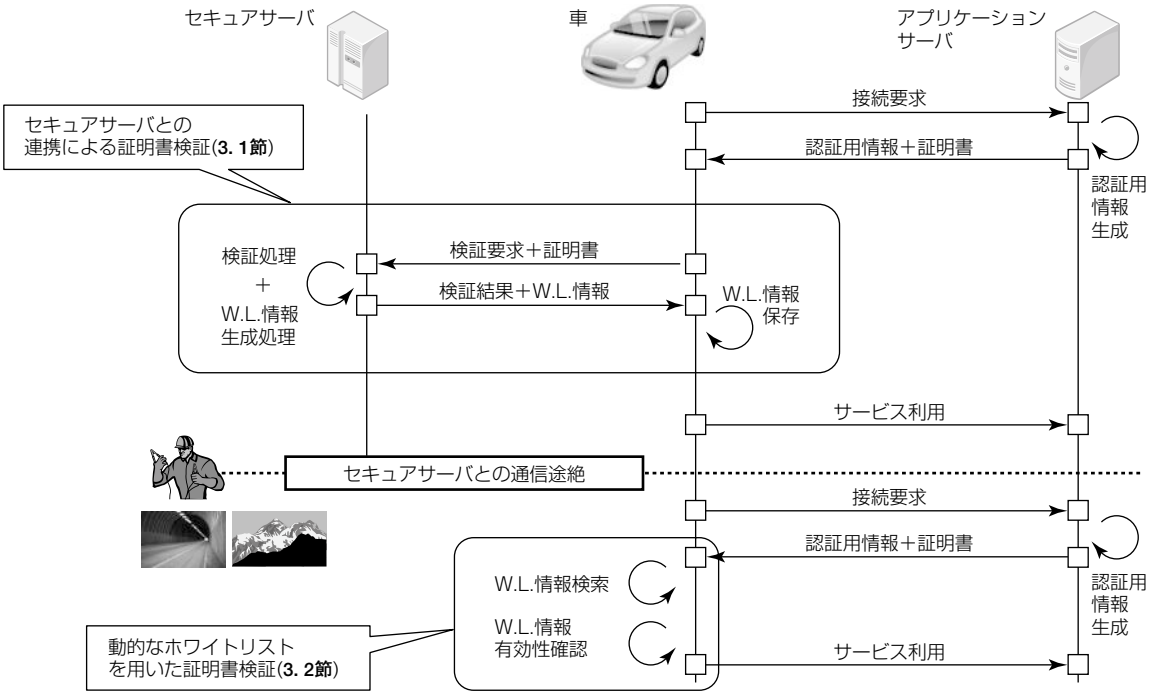


図2．提案方式における認証処理

象としてカーメーカーなどのW.L.情報を事前にプリインストールしておくことで，セキュリティサーバを利用しないシステム構成の場合にも，クルマ側の処理負荷軽減のメリットを得る事が可能である。

3.3 ハッシュ値を用いた省リソース化

車載装置のマイコンは，その性能だけでなく搭載するメモリ量によってコストが増減する。メモリの使用量として支配的なW.L.情報として，証明書そのものを用いると，枚数に比例して記憶領域が必要となり，クルマの限られたリソースへの影響が懸念される。そこで，証明書のハッシュ値をセキュアサーバで生成し，W.L.情報として提供することとした。

省リソース化の効果について試算した結果を次に示す。なお，証明書に含まれる暗号・署名に関連する情報を除いた主体者名などの記載情報は1,000octetとする。また，試算用パラメータは次のとおりとする。

⑴ PKIにおける信頼モデル：CA 2 階層
⑵ 公開鍵暗号アルゴリズム：RSA 2048
⑶ W.L.情報算出用ハッシュアルゴリズム：SHA 256 (Secure Hash Algorithm 256bit)

試算の結果，暗号・署名に直接関係するデータは，19.7%(1,536octet→302octet)まで削減された。さらに，証明書 3 つ分の記載情報(1,000 × 3 octet)を加味したW.L.情報全体としては，6.7%(4,536octet→302octet)まで削減されることが確認できた。

このことから，この方式をリソース制限の厳しい車載装置へ適用することは十分可能であると考える。

4. む す び

クルマがセキュアサーバと連携して，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た。まず，クルマで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って，サーバ側の豊富な計算リソース及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ため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。さらに，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，及び証明書の有効期間を踏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。試算によってデータを 7 %弱に削減できることが確認できた。今後は，提案方式に基づくシステムの試作と評価を行い，有効性を確認する予定である。

参 考 文 献

⑴ (独)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) http://www.ipa.go.jp/files/000024413.pdf
⑵ Stephen Checkoway，et al.：Comprehensive Experimental Analyses of Automotive Attack Surfaces, Proc. of the 20th USENIX conference on Security (2011) https://www.usenix.org/legacy/events/sec11/tech/full_papers/Checkoway.pdf
⑶ The Internet Engineering Task Force，Network Warking Group RFC5280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile (2008) http://tools.ietf.org/html/rfc5280