社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（39）
2005－CSEC－28（39）
2005／3／23

携帯電話スマートキーを活用した車操作権限の貸与方式の提案

齋藤 和美† 太田 英憲† 松田 規† 伊藤 隆† 辻 宏郷† 米田 健†

†三菱電機株式会社 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1
E-Mail: †{kazumi, hidenori, norim, takashim, hirosato, tyone}@iss.isl.melco.co.jp

あらまし 近年, 自動車の新しいキーレスエントリーシステムとしてスマートキーが利用され始めているが, 車を他人に貸与する場合は, 従来と同様にキーを手渡しする必要があり, 他人に悪意があれば車や車内の付属物などが盗難される恐れもある. 本発表では, 携帯電話をスマートキーとして用い, 携帯電話を介して所有者から借用者に車操作権限を発行することによって, 車を貸与する方式を提案する. 更に, 提案方式は, 車操作権限に制限を付与することによって, 安全性および柔軟性を向上する.

キーワード 権限委譲, 携帯電話, 認証, アクセス制御, 公開鍵暗号, 自動車

A Proposal of Method of Lending Car Operation Privilege by Using Cellular Phone as Smart Key

Kazumi SAITO† Hidenori OHTA† Nori MATSUDA† Takashi ITO†

Hirosato TSUJI† and Takeshi YONEDA†

†Mitsubishi Electric Corporation, Information Technology R&D Center,
5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan
E-Mail: †{ kazumi, hidenori, norim, takashim, hirosato, tyone}@iss.isl.melco.co.jp

Abstract In recent years smart keys are being applied to cars as an advanced keyless entry system. However, when lending a car to someone, handing a physical key over to him/her is still needed, which might cause a robbery of the car or its accessories. In order to lend a car without handing a physical key, in this paper, we propose a method of using a cellular phone as a smart key. By this method, lending a car is realized by transferring operation privilege from the owner's phone to the borrower's phone. Furthermore, owner can set restrictions of car operation privilege in order to improve safety and flexibility.

Key words delegation privilege, cellular phone, authentication, access control, public key cryptosystem, car

1. はじめに

近年, 自動車(以下, 車と呼ぶ)のドアロック・アンロック, エンジン始動・停止などの操作にスマートキーを用いたシステムが増加している. 従来のキーレスエントリーシステムでは, ドアロック・アンロック時は物理的な鍵に付属しているスイッチを押下, エンジン始動・停止時は物理的な鍵を挿入するものであるのに対して, スマートキーシステムでは単に車のドアノブやイグニッションボタンの押下を行うだけで自動的に車のドアロック・アンロック, エンジン始動・停止操作が可能である. このようにスマートキーの利用は, 利

用者の操作性の向上をもたらしているが，例えば，車を所有者以外の者に貸与する場合は，物理的な鍵と同様にスマートキーを手渡しし，操作の全権を委ねることとなり，物理的な鍵と同程度の安全性と操作性を提供するものとなっている．スマートキーのような電子的な鍵を車に適用する場合に，このような安全性と操作性を向上するために，2 章に示すような幾つかの方式が提案されている．しかし，操作権に制限を付与できるがキーの手渡しを必要としたり，携帯電話を用いて操作権を遠隔で貸与できるが携帯電話以外にサーバを必須としたりするなどの課題が残っている．今回，我々は，携帯電話をスマートキーとして活用し，安全且つ柔軟に車を人に貸与する方式について検討したので，ここに報告する．本稿では，まず，スマートキーの現状と課題およびセキュリティ要件について述べる．次に，今回提案する貸与方式について述べる．最後に，提案方式のセキュリティ要件への対応についての考察を記す．

2．現状と課題

本節では，スマートキーを用いた車操作の現行方式の概要と課題，関連する研究概要について述べる．

2．1 現状の方式

現在の車操作におけるスマートキー方式の概要を図 1 に示す．

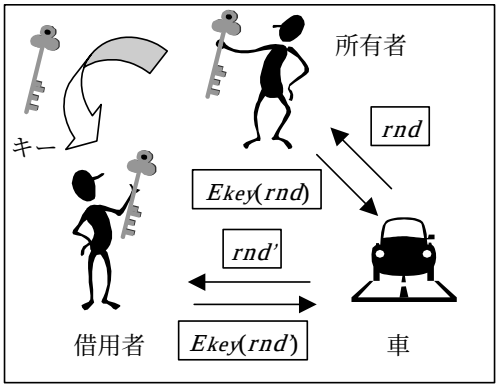

図 1：現在のスマートキー方式概要

車の所有者(以下，所有者と呼ぶ)は，所有する車に対して操作を行うためのスマートキーを保持している．スマートキーと車を稼動するための制御装置には，予め工場において生産時などに固定の共通鍵が埋め込んであるものとする．例えば，所有者がドアノブに触れてドアを開けようと車操作を開始すると，車の制御装置は乱数(*rnd*)を生成してスマートキーに送信する．スマートキーは，受信した *rnd* を保有している共通鍵(*key*)を用いて暗号化し(*Ekey*(*rnd*))，車の制御装置に送信する．車の制御装置は，保有している *key* を用いて，受信した *Ekey*(*rnd*)を復号し，先に生成した *rnd* と復号した乱数とを照合する．乱数どうしが一致した時のみ，ドアをアンロックする．
次に，所有者が車を借用する人(以下，借用者と呼ぶ)に対して車を貸与する場合は，所有者が保持するスマートキーを借用者に手渡しすることによって貸与する．借用者は，所有者と同様に車を操作することが可能である．

2．2 課題

このように，現在のスマートキー方式は，車を人に貸与する場合，従来の物理的な鍵と同様の貸与方式を用いているため，以下のような問題が存在する．
借用者が使用するスマートキーは，所有者の保持するスマートキーであるため，所有者と同等の権限を用いて車を操作することが可能である．例えば，ホテルや旅館などの宿泊施設では，車のキーを施設の従業員に預けて，車を所定の位置に駐車してもらう場合，車を盗まれる恐れがある．また，運転免許を持たない者や子供にキーを預けた場合，誤って車を発進してしまう恐れもある．また，借用者が遠隔地にいる場合には，キーを手渡しする必要があるので不便である．

2．3 関連研究

これら問題に対する解決方法として，幾つかの方式が提案されている．例えば，参考文献[1]に記載されている方式では，スマートキーを複数個用意する．各キーは，異なる機能権限が付与されており，所有者は，借用者毎に許可する機能を判断し，その機能に対応するスマートキーを渡す．この方式によって，借用者に一定の機能制限を与えることができる．しかし，詳細な機能制限を与えるとするとスマートキーの数を増加する必要があり運用上困難が伴う．また，キーを手渡しする必要がある．参考文献[2]に記載されている方式では，携帯電話をスマートキーとして活用する．所有者は借用者の情報をサーバに登録した後，借用者にサーバへのアクセス情報を連絡する．借用者は，アクセス情報を用いてサーバに接続し，車操作に必要な情報をダウンロードする．この方式を用いることによって，所有者と借用者が離れた

場所にいても借用者は車を操作することが可能となる. しかし, 所有者と借用者は共にサーバに接続する必要があり, サーバの障害や負荷発生時など通信困難な場合においては, 利用が難しい.

3. セキュリティ要件

本節では, スマートキーの現状と課題を踏まえ, スマートキーのセキュリティ要件について述べる.

(1) 所定外の車へのアクセス防止

複数の車を所有している場合, 借用者が許可していない他の車を操作することを防止する必要がある.

(2) リプレイアタックによるなりすまし防止

所有者と借用者, 車と所有/借用者間の通信を第三者が傍受し, 取得したデータを用いて関係者になりすまして車を操作することを防止する必要がある.

(3) キーの複製による不正利用防止

キーの情報が複製されることによって, 車を不正に利用されないように考慮する必要がある.

(4) キーの紛失/盗難による不正利用防止

物理的にキーを紛失/盗難されることによって, 車を不正に利用されないように考慮する必要がある.

(5) 遠隔地にいても安全に車を貸与

借用者が遠隔地にいても, 所有者は安全に車を貸与できることが望まれる.

(6) サーバ不要の簡易な構成

サーバとの通信状況や負荷状況を考慮すると, サーバを必要としない簡易な構成であることが望まれる.

(7) 操作権限の木目細かな設定

所有者が車を貸与する様々な状況に対応するためには, 操作権限を柔軟に設定できることが望まれる.

4. 提案方式

借用者が遠隔地にいても, サーバを介さない簡易なシステムを用いて, 所有者が車操作の機能を木目細かに制限することができる貸与方式を提案する.
本節では, 提案方式のシステム構成概略, 車を人に貸与するための車操作権限委譲手順, 車の所有者や借用者が車を操作するための車操作手順について述べる.

4.1 システム構成の概略

今回提案する車操作におけるスマートキーシステムの概要を図 2 に示す.

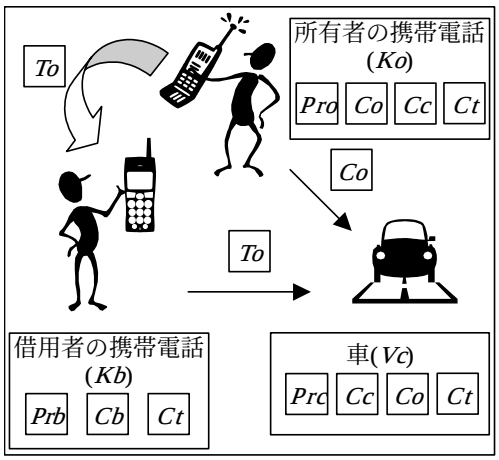

図 2:提案のスマートキー方式概要

所有者は所有する車の操作を行うためのスマートキー機能を持つ携帯電話(*Ko*)を保持する. 例えば, 車を購入する際に, 販売店の専用端末に *Ko* を接続してスマートキー機能を実現するプログラムやデータをダウンロードする. *Ko* に格納するデータは, 所有者の秘密鍵(*Pro*), *Pro* に対応する公開鍵(*Puo*)を含む証明書(*Co*), 車の公開鍵(*Puc*)を含む証明書(*Cc*), *Co* および *Cc* を発行したメーカの証明書(*Ct*)とする.
借用者も所有者と同様にスマートキー機能を持つ携帯電話(*Kb*)を保持する. 例えば, 自身が車を購入する際または車を借用する際に, スマートキー機能を実現するために必要なプログラムやデータをダウンロードする. *Kb* に格納するデータは, 借用者の秘密鍵(*Prb*), *Prb* に対応する公開鍵(*Pub*)を含む証明書(*Cb*), *Cb* を発行したメーカの証明書(*Ct*)とする.
車メーカは, 車(*Vc*)を出荷する際に車が動作するために必要なプログラムやデータを *Vc* に格納する. データは, 車の秘密鍵(*Prc*), *Prc* に対応する公開鍵(*Puc*)を含む証明書(*Cc*), *Cc* を発行したメーカの証明書(*Ct*)とする. また, 販売店において, 所有者の公開鍵を含む証明書(*Co*)も格納する.

4.2 車操作権限貸与手順

所有者が携帯電話を用いて借用者に車を貸与する手順を図 3 に示す.

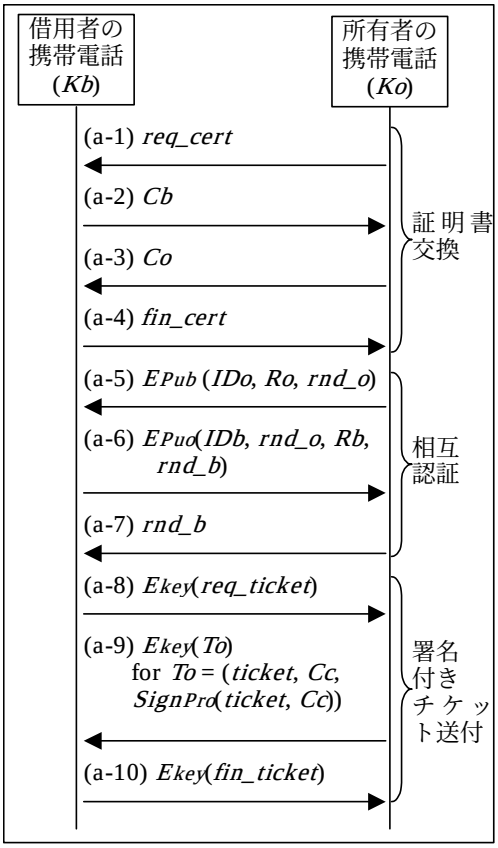

図 3:車操作権限貸与手順

(1) 証明書交換

借用者の携帯電話(*Kb*)は所有者の携帯電話(*Ko*)から借用者の証明書送信要求(*req_cert*)を受信すると, 借用者の証明書(*Cb*)を返信する. *Ko* は上位の証明書(*Ct*)を用いて *Cb* を検証する. 検証に成功すると, 所有者の証明書(*Co*)を *Kb* に送信する. *Kb* は上位の証明書(*Ct*)を用いて *Co* を検証する. 検証に成功すると, 証明書受信完了通知(*fin_cert*)を返信する.

(2) 相互認証

次に *Ko* は所有者を示す識別子(*IDo*), 共通鍵生成用乱数(*Ro*), 相互認証用乱数(*rnd_o*)を生成する. ここでは *IDo* は *Co* のイシュア名とシリアルナンバーとする. *Ko* は *IDo*, *Ro*, *rnd_o* を借用者の公開鍵(*Pub*)を用いて暗号化し *Kb* に送信する. *Kb* は借用者の秘密鍵(*Prb*)を用いて復号し, *Co* を用いて *IDo* を検証する. 検証に成功すると, 借用者を示す識別子(*IDb*), 共通鍵生成用乱数(*Rb*), 相互認証用乱数(*rnd_b*)を生成する. ここでは *IDb* は *Cb* のイシュア名とシリアルナンバーとする. *Kb* は *IDb*, *rnd_o*, *Rb*, *rnd_b* を所有者の公開鍵(*Puo*)を用いて暗号化し *Ko* に送信する. *Ko* は所有者の秘密鍵(*Pro*)を用いて復号し, *rnd_o* を検証し, *Cb* を用いて *IDb* を検証する. 検証に成功すると, *rnd_b* を返信する. *Kb* は *rnd_b* を検証する. 検証に成功すると, *Kb* は次の手順に進む.

(3) 署名付きチケット送付

Kb は *Ro* と *Rb* を用いて共通鍵(*key*)を生成する. ここでは *Ro* と *Rb* を連結して生成したハッシュ値の先頭から鍵長分の長さのデータを *key* とする. *Kb* は *key* を用いてチケット要求(*req_ticket*)を暗号化し *Ko* に送信する. *Ko* は *Kb* と同様に *Ro* と *Rb* から生成した *key* を用いて復号し, *req_ticket* を確認する. 次に *Ko* は借用者に車操作権限を与えるためのチケット(*ticket*)を作成する. チケットは *Cb*, 操作許可情報, 操作制約情報, チケットの有効期限から構成される. 操作許可情報はドアのロック･アンロック, エンジン始動･停止など借用者に許可する車操作の機能を含む情報である. 操作制約情報は走行距離, 走行範囲など借用者に許可する車操作の制限を含む情報である. *Ko* は *Pro* を用いて *ticket* と車の証明書(*Cc*)の署名を生成する(*SignPro*(*ticket, Cc*)). *Ko* は *key* を用いて署名付きチケット(*To*)を暗号化し *Kb* に送付する. *Kb* は *key* を用いて復号し, *Puo* を用いて署名を検証する. 検証に成功すると, *To* を格納し, *key* を用いて暗号化したチケット受信完了通知(*fin_ticket*)を *Ko* に送付する. *Ko* は *key* を用いて復号し, *fin_ticket* を確認する.

4．3 所有者の車操作手順

所有者が携帯電話を用いて車を操作する手順を図 4 に示す.

(1) 証明書交換

車(*Vc*)は定期的に応答要求を送信している. 所有者が *Vc* に接近すると, 所有者の携帯電話(*Ko*)と *Vc* との間で通信リンクが確立される. 所有者がドアノブに接触するなどの車操作を開始すると, *Vc* は証明書送信要求(*req_cert*)を *Ko* に送信する. *Ko* は所有者の証明書(*Co*)を返信する. *Vc* は上位の証明書(*Ct*)を用いて *Co* を検証する. 検証に成功すると, 車の証明書(*Cc*)を *Ko* に送信する. *Ko* は上位の証明書(*Ct*)を用いて *Cc* を検証する. 検証に成功すると, 証明書受信完了通知(*fin_cert*)を返信する.

(2) 相互認証

次に *Vc* は車を示す識別子(*IDc*), 共通鍵生成用乱数(*Rc*), 相互認証用乱数(*rnd_c*)を生成する. ここでは *IDc* は *Cc* のイシュア名とシリアルナンバーとする. *Vc* は *IDc*, *Rc*, *rnd_c* を所有者の公開鍵(*Puo*)を用いて暗号化し *Ko* に送信する. *Ko* は所有者の秘密鍵(*Pro*)を用いて復号し, *Cc* を用いて *IDc* を検証する. 検証に成功すると, 所有者を示す識別子(*IDo*), 共通鍵生成用乱数(*Ro*), 相互認証用乱数(*rnd_o*)を生成する. ここでは *IDo* は *Co* のイシュア名とシリアルナンバーとする. *Ko* は *IDo*, *rnd_c*, *Ro*, *rnd_o* を車の公開鍵(*Puc*)を用いて暗号化し *Vc* に送信する. *Vc* は車の秘密鍵(*Prc*)を用いて復号し, *rnd_c* を検証し, *Co* を用いて *IDo* を検証する. 検証に成功すると, *rnd_o* を返信する. *Ko* は *rnd_o* を検証する. 検証に成功すると, *Ko* は次の手順に進む.

(3) 操作開始要求送信

Ko は4. 2(3)と同様にして *Rc* と *Ro* を用いて共通鍵(*key*)を生成する. ここでは *Rc* と *Ro* を連結して生成したハッシュ値の先頭から鍵長分の長さのデータを *key* とする. 次に *Ko* は *key* を用いて操作開始要求(*req_start*)を暗号化し, *Vc* に送信する. *Vc* は *Ko* と同様に *Rc* と *Ro* から生成した *key* を用いて復号し, *req_start* を確認し, 動作を開始する.

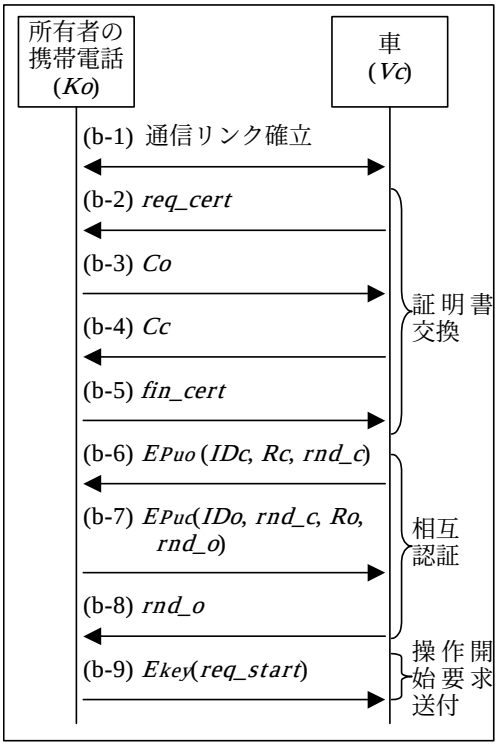

図 4:所有者の車操作手順

4．4 借用者の車操作手順

借用者が携帯電話を用いて車を操作する手順を図 5 に示す.

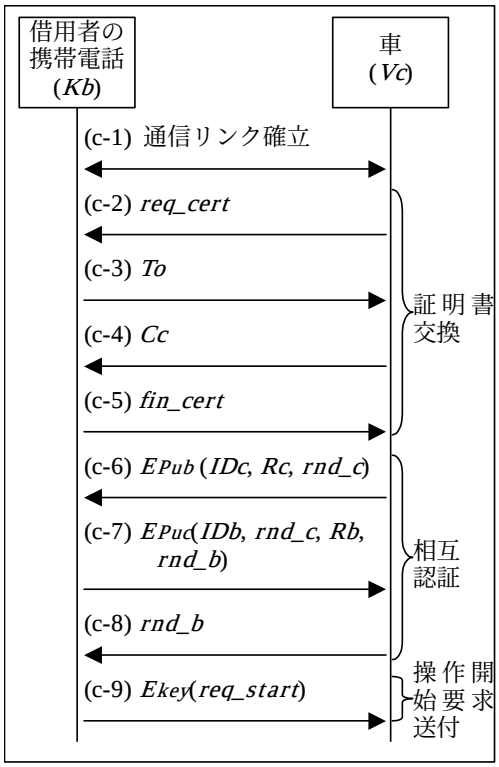

図 5:借用者の車操作手順

(1) 証明書交換

所有者が携帯電話を用いて車を操作する手順と同様に, 車(*Vc*)と借用者の携帯電話(*Kb*)との間において通信リンクが確立され, 借用者が車操作を開始すると, *Vc* は証明書送信要求(*req_cert*)を *Kb* に送信する. *Kb* は署名付きチケット(*To*)を返信する. *Vc* は所有者の証明書(*Co*)および上位の証明書(*Ct*)を用いて *To* の署名を検証する. 検証に成功すると, *Vc* は *To* に含まれる車の証明書(*Cc*)を検証する. また, 現在時刻を取得し, *To* に含まれるチケットの有効期限を過ぎていないことを検証する. 検証に成功すると, *Cc* を *Kb* に送信する. *Kb* は上位の証明書(*Ct*)を用いて *Cc* を検証する. 検証に成功すると, 証明書受信完了通知(*fin_cert*)を返信する.

(2) 相互認証

次に *Vc* は車を示す識別子(*IDc*), 共通鍵生成用乱数(*Rc*), 相互認証用乱数(*rnd_c*)を生成する. ここでは *IDc* は *Cc* のイシュア名とシリアルナンバーとする. *Vc* は *IDc*, *Rc*, *rnd_c* を借用者の公開鍵(*Pub*)を用

いて暗号化し *Kb* に送信する. *Kb* は借用者の秘密鍵(*Prb*)を用いて復号し, *Cc* を用いて *IDc* を検証する. 検証に成功すると, 借用者を示す識別子(*IDb*), 共通鍵生成用乱数(*Rb*), 相互認証用乱数(*rnd_b*)を生成する. ここでは *IDb* は借用者の証明書(*Cb*)のイシュア名とシリアルナンバーとする. *Kb* は *IDb*, *rnd_c*, *Rb*, *rnd_b* を車の公開鍵(*Puc*)を用いて暗号化し *Vc* に送信する. *Vc* は車の秘密鍵(*Prc*)を用いて復号し, *rnd_c* を検証し, *Cb* を用いて *IDb* を検証する. 検証に成功すると, *rnd_b* を返信する. *Kb* は *rnd_b* を検証する. 検証に成功すると, *Kb* は次の手順に進む.

(3) 操作開始要求送信

Kb は所有者の場合と同様にして *Rc* と *Rb* を用いて共通鍵(*key*)を生成する. ここでは *Rc* と *Rb* を連結して生成したハッシュ値の先頭から鍵長分の長さのデータを *key* とする. 次に *Kb* は *key* を用いて操作開始要求(*req_start*)を暗号化し, *Vc* に送信する. *Vc* は *Kb* と同様に *Rc* と *Rb* から生成した *key* を用いて復号し, *req_start* を確認する. 次に *Vc* は現在時刻を取得しチケットの有効期限を過ぎていないこと, これから開始する操作が操作許可情報において許可された機能であること, 操作制約情報に触れないことを確認して, 動作を開始する.

5. 考察

本節では, スマートキーのセキュリティ要件における提案方式の対応状況について述べる.

(1) 所定外の車へのアクセス防止

提案方式では, 車側において借用者の携帯電話から送信されたチケットに含まれる車の証明書を検証するため, 借用者は所定の車のみアクセスできる.

(2) リプレイアタックによるなりすまし防止

提案方式では, 相互認証時に乱数を用いることによってデータの再利用を防止している.

(3) キーの複製による不正利用防止

提案方式では, キーの情報を携帯電話に内蔵される UIM などの IC カードチップに格納することにより, 複製を困難にすることができる.

(4) キーの紛失/盗難による不正利用防止

提案方式では, 携帯電話のパスワード/認証機能を利用して, 他人の利用を防止することができる.

(5) 遠隔地にいても安全に車を貸与

携帯電話と公開鍵暗号を用いて, 所有者と借用者間, 車と利用者間を相互に認証しているので, 第三者のチケットの不正利用などを防ぎ, 安全に貸与できる.

(6) サーバ不要の簡易な構成

車の操作権限を貸与する場合, 携帯電話を介して所有者から借用者にチケットを発行するので, 貸与毎にサーバに接続する必要がない.

(7) 操作権限の木目細かな設定

チケット中に借用者に許可する操作機能と制限範囲を任意に設定するので, 従来よりも詳細な設定が可能である. また, 所有者は, 携帯電話を用いて使い慣れている普段と同じ入力操作によって操作権限を設定できる.

6. おわりに

携帯電話をスマートキーとして用い, 安全且つ柔軟に車操作権限を貸与する方式について提案した. 今回の提案では, スマートキーのセキュリティ要件を満足することを目的とした. 今後は, 性能要件を特定し, その要件を満たす H/W 構成の特定, 暗号方式の選定, 通信プロトコルの改良を行う. また, スマートキーの紛失/盗難時などへの対策についても更に検討していく所存である.

参考文献

[1] 大滝 清和, 日本国特許庁公開特許公報, 特開 2004-25937, “電子キーシステム”, 2004.
[2] 梅田 文雄, 日本国特許庁公開特許公報, 特開 2004-88339, “識別コード配信システム、識別コード配信方法及び識別コード配信用プログラム”, 2004.
[3] Colin Boyd, Anish Mathuria, “Protocols for Authentication and Key Establishment”, Springer, 2003.
[4] 中井 登, 平野 文人, 加藤 高明, 荻野 光弘, “二輪車用盗難抑止装置(イモビライザー)”, YAMAHA MOTOR TECHNICAL REVIEW, No.36, 2003-9.