特殊ハードウェアに依存しない車両スマートフォンキーシステムの提案と検討

2016SC005 渕将成　2016SC011 濱村京太郎
指導教員：石原靖哲

1　はじめに

従来の自動車キーを使わず車両にアクセスし，エンジンを始動する新たな方法として，スマートフォンを利用する方法に期待が寄せられている．現在使用されているスマートキーは自動車の近くでのみ利便性が発揮できるが，車両スマートフォンキーシステムでは遠隔からでもエンジンの始動やドアの開閉，空調機能などを利用することが可能となる．その反面，車両スマートフォンキーシステムを使用すると，サイバー攻撃を受ける可能性がでてくるため，その対策が必須である．

スマートフォンからの情報漏洩に耐性を有する車両キーシステムについて過去に竹内らが研究している．しかし，竹内らの提案システムは鍵情報がパスワード特有の脅威から漏洩しないことが前提である．日常生活に応用するにはパスワード特有の脅威についても考慮しなければならない．

そこで本研究では，竹内らが除外した，パスワード特有の脅威からの鍵情報の漏洩を阻止するという観点と，車両スマートフォンキーシステムに共通して存在する問題であるスマートフォン内の情報を書き換える攻撃やスマートフォンを盗難されても車両の安全性が確保されるという観点で，特殊ハードウェアに依存せず，利便性にも考慮した方式を検討する．車両スマートフォンキーシステムの概要を図 1 に示す．本研究の前提として，すべてのスマートフォンが SIM を持っているものとする．そして，認証に成功したらユーザは自動車のあらゆる機能を利用できるようになる．自動車がユーザを認証する方法としてワンタイムパスワードを利用した方式を検討する．自動車とユーザが持つスマートフォンはあらかじめ鍵情報を共有しておくこととする．尚，パスワード特有の脅威を覗き見，フィッシング，使い回し，推測とする．

また，自動車がスマートフォンを認証するという方式を用いるとスマートフォンを盗難された際，直ちに自動車も盗難されてしまうため，自動車がスマートフォンを介してユーザを認証することとする．そのため，ユーザが入力した情報がスマートフォンを介して自動車に送信され，自動車は受信した内容をもとにユーザの認証を行うことを前提とする．

2　関連研究

車両スマートフォンキーシステムは現在特殊ハードウェアを利用するもの，バーチャルキーを利用したもの，パスワードを利用したものがある．

カーシェアリングサービスを提供している会社では特殊ハードウェアを利用する仕組みを導入している．この仕組みでは初回のみ自動車の解錠に会員カードを利用してユーザを識別し，解錠したらそれ以降は車内にある物理的な鍵を用いて自動車を利用する．しかし，特殊ハードウェアを利用する仕組みは一般車に普及することは困難である．

バーチャルキーを利用した仕組みでは管理者や所有者の元にマスターキーを置きながら，利用者はスマートフォンで受信したバーチャルキーでドアロック解除およびエンジン始動までを可能にする．この仕組みでは，スマートフォン内の情報を書き換える攻撃に対して安全性が確保できないことが考えられる．

パスワードを利用した仕組みとしては竹内らが提案した方式 [4] がある．竹内らの論文では，短いパスワードを使用したとしてもスマートフォンからの鍵情報の漏洩に耐性を持たせることができる，LR-AKE[3] を適用したスマートフォンキーシステムを提案している．その手法ではパスワード特有の脅威への対策が不十分であり，実用的なものとするためには，この観点についても考慮する必要がある．

3　既存のユーザ認証方式と車両スマートフォンキーシステムへの適用

3.1　ユーザ認証方式の分類

ユーザ認証方式には，持っているものを用いて認証する「所持認証」，ユーザが知っていることを用いて認証する「知識認証」，ユーザ自身の特徴を用いて認証する「生体認証」の 3 つがある [2]．本研究では，特殊ハードウェアに依存しない認証方式の検討を行うことから，「生体認証」は除外し，「所持認証」と「知識認証」の 2 つについて検討する．この節では所持認証から SMS 型，知識認証からパターン型と位置情報型を取り上げる．

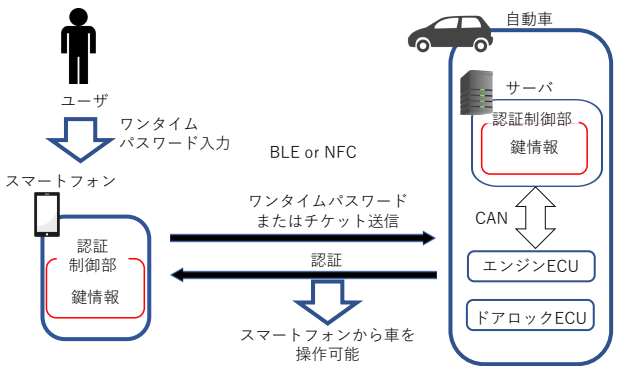

図 1　車両スマートフォンキーシステム概要

3.2　SMS を利用したアウトオブバンド認証方式

アウトオブバンド認証方式とは，2 種類の通信路を介して認証を行う方式である．この方式はその一例である．

車両スマートフォンキーシステムへと応用する場合は，BLE または NFC と携帯電話の回線の 2 種類の回線を用いる．また，はじめに ID を作成し電話番号とともに自動車のサーバに登録しておく必要がある．自動車側は ID で誰が認証要求をしているのか識別する．認証要求を行っているユーザを識別したら自動車はそのユーザ宛てにショートメールを用いてワンタイムパスワードを送信する．ユーザは BLE 回線等を用いて自動車にワンタイムパスワードを送信する．自動車が送信したワンタイムパスワードとユーザが送信したワンタイムパスワードが一致していたら自動車はユーザを認証する．この方式は覗き見，フィッシング，使い回し，推測に強く，盗難に弱い．

3.3　位置情報型ワンタイムパスワード方式

位置情報型ワンタイムパスワード方式は，予め用意しておいた乱数表を用い，何行何列から何桁といった表の中の位置をパスワードとして使用する方式である．乱数表の共有の方法として紙で配布する方法と電子的に共有する方法が考えられる．

車両スマートフォンキーシステムへと応用する場合は，電子的に共有する際の盗聴の恐れを考慮し，自動車の利用者が最初に利用する際に紙の乱数表を配布するのがよいと考えられる．また，同じ乱数表を使い続けると使用している乱数表が知られるリスクが高まるため，乱数表は数年に一度新しいものに変更する．この方式ではまずユーザが認証要求を行い，自動車は認証要求をしたユーザに対しワンタイムパスワードにする位置を送信する．ユーザは手元の乱数表と要求された位置からワンタイムパスワードを生成し，自動車に送信する．自動車が想定したワンタイムパスワードとユーザが送信したワンタイムパスワードが一致していたら自動車はユーザを認証する．この方式は使い回し，盗難，推測に強く，覗き見，フィッシングに弱い．

3.4　パターン型ワンタイムパスワード方式

パターン型ワンタイムパスワード方式 [1] はマトリクス状の乱数表からあらかじめ決めておいた「パターン（マスの位置と順番)」に沿って文字を抽出し，つなげることでワンタイムパスワードを生成する方式である．表示される乱数表は認証のたびに変更されるためワンタイムパスワードとして運用することができる．

スマートフォンキーシステムへと応用する場合は，ユーザは自動車購入時にパターンを作り自動車に登録する必要がある．ユーザは自動車に自らの ID を送信することで認証要求をすることとし，自動車側は受信した ID で誰が認証要求をしているのか識別するものとする．認証要求を行っているユーザを識別したら自動車はそのユーザに毎回異なる乱数表を送信する．ユーザは登録したパターンと乱数表からワンタイムパスワードを生成し，自動車に送信する．自動車が想定したワンタイムパスワードとユーザが送信したワンタイムパスワードが一致していたら自動車はユーザを認証する．この方式は覗き見，盗難に強く，フィッシング，使い回し，推測に弱い．

知識認証 / 所持認証	位置情報型 ワンタイムパスワード方式	パターン型 ワンタイムパスワード方式
時刻同期型 ワンタイムパスワード 方式	× スマートフォン内に ユーザ乱数が必要	× 大人数になると時刻のずれが 発生する スマートフォン内にユーザ乱 数が必要
生成回数型 ワンタイムパスワード 方式	× スマートフォン内に ユーザ乱数が必要	× 大人数になると回数の同期の 手間 スマートフォン内にユーザ乱 数が必要
SMS型 ワンタイムパスワード 方式 （ボイスコールを含む）	○ スマートフォン内に ユーザ乱数が不必要	○ スマートフォン内に ユーザ乱数が不必要

図 2　ハイブリッドの検討表

4　車両スマートフォンキーシステムの提案

4.1　自動車の使用方法の現状と分類

現在，自動車はマイカーとしてだけでなく，レンタカーやカーシェアリング，カーリースなど様々な場面で利用されている [5]．それらの場面に適した車両スマートフォンキーシステムを提案することでユーザの利便性向上が期待できる．

本研究では，安全性に考慮した上で場面に応じた利便性や現実性に合ったシステムを目指す．そこで，自動車がネットワーク接続が可能な場合と不可能な場合の 2 つの場面に分けて考える．また，それぞれの場面において自動車の利用方式を以下の 2 方式に分類する．

- 個人向け方式:「所有者」と「利用者」が同じもしくは「所有者」が「利用者」に含まれる場面で用いられる方式．具体的には，個人または家族で自動車を所有し，使用する場面向けの方式である．
- シェア方式　:「所有者」と「利用者」が異なる場面で用いられる方式．具体的には，レンタカーなど自動車の貸し借りをする場面向けの方式である．

4.2　提案方式の検討

従来の単一なユーザ認証方法では強固なセキュリティとは言い切れない．知識情報なら忘却や漏洩，所持情報なら紛失や盗難といった問題が存在する．そこで互いの問題点を補完しあう多要素認証を実現することでより安全性を高めることを目指す．

多要素認証を実現するために，知識認証の位置情報型とパターン型の中から 1 つ，所持認証の時刻同期型，生成回数型，SMS 型の中から 1 つ選ぶとき，全部で 6 通りが考えられる（図 2 を参照)．

時刻同期型，生成回数型を使用する組み合わせを考えた

場合，スマートフォン内にユーザごとの乱数を保存する必要があり，スマートフォン内の情報を書き換える攻撃を受けたときの耐性がない．また，大人数で使用する場合，時刻のずれや生成回数のずれも懸念されるため，提案するシステムに適切でないと判断した．

SMS 型を使用する組み合わせを考えた場合，スマートフォン内に情報を保存する必要がなく，スマートフォン内の情報を書き換える攻撃に対して耐性を有する．また，時刻のずれや生成回数のずれもないため適切であると判断し，この方式を用いたものを提案する．

以下では紙面の都合によりネットワーク接続が可能な場合の車両スマートフォンキーシステムのみ説明する．

4.3 ネットワーク接続が可能な場合の車両スマートフォンキーシステム

自動車がネットワーク接続可能な場合，第三者のサーバを設置する必要がなく，コストを抑えることができる上，信頼できるサーバがない場合でも成り立つ利点がある．

4.3.1 ネットワーク接続が可能な場合の個人向け方式

この方式は所持認証の SMS を利用したアウトオブバンド認証方式と，知識認証の位置情報型を組み合わせたハイブリッド型であり，多要素認証を実現している．

この方式では，SMS 方式の弱点である盗難を，盗難に強い位置情報型で補完し，位置情報型の弱点である覗き見，フィッシングを，これらの脅威に強い SMS 型で補完する．SMS 型単体，位置情報型単体の時に比べて，互いの弱点を補いあい，強みをつぶしていないため，元の方式の良さがなくなっていないことが分かる．

所持認証の SMS 型と組み合わせる選択肢として位置情報型以外にパターン型があるが，パターン型と比べて強みが多い位置情報型を用いるのがよいと判断した．

個人が利用する場合は乱数表の発行枚数が少なく流出のリスクも低く抑えることができるため，位置情報型を適用する．

ネットワーク接続が可能な場合の個人向け方式の認証までの流れを以下に示す（図 3 を参照）．

1. ユーザが認証要求を行う
2. 自動車側がユーザに SMS でワンタイムパスワードにする位置を送信する
3. ユーザ側と自動車側は 2 の情報と乱数表よりそれぞれワンタイムパスワードを生成する
4. ユーザ側から自動車側にワンタイムパスワードを送信する
5. ユーザ側が送信したワンタイムパスワードと自動車側が生成したワンタイムパスワードと一致していたら認証する

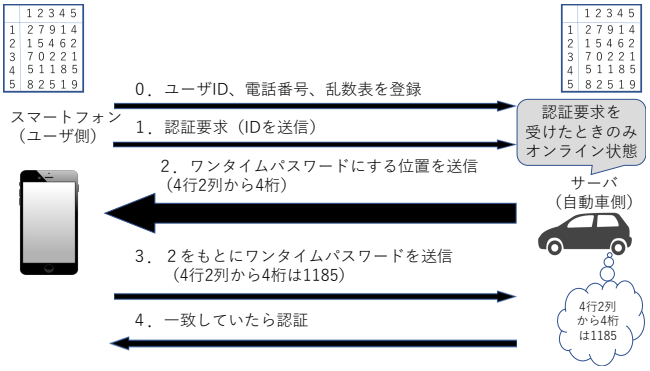

図 3　ネットワーク接続が可能な場合の個人向け方式の概要

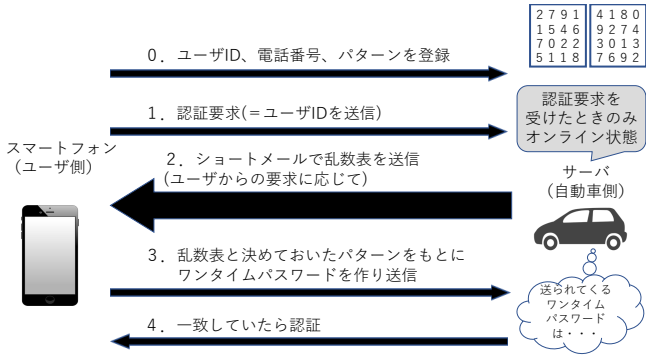

図 4　ネットワーク接続が可能な場合のシェア方式の概要

4.3.2 ネットワーク接続が可能な場合のシェア方式

この方式は所持認証の SMS を利用したアウトオブバンド認証方式と，知識認証のパターン型を組み合わせたハイブリッド型であり，多要素認証を実現している．

SMS 方式の弱点である盗難を，盗難に強いパターン型で補完し，パターン型の弱点であるフィッシング，使い回し，パターンの推測を，これらの脅威に強い SMS 型で補完する．SMS 型単体，パターン型単体の時に比べて，互いの弱点を補いあい，強みをつぶしていないため，元の方式の良さがなくなっていないことが分かる．

位置情報型は乱数表を紙で配るため，大人数が利用する場合には乱数表の流出のリスクが高まる．そこで，パターン型をこの方式に適用する．

ネットワーク接続が可能な場合のシェア方式の認証までの流れを以下に示す（図 4 を参照）．

1. ユーザが認証要求を行う
2. 自動車側がユーザに SMS で乱数表を送信する
3. ユーザ側と自動車側は 2 の情報と登録したパターンからそれぞれワンタイムパスワードを生成する
4. ユーザ側から自動車側にワンタイムパスワードを送信する
5. ユーザ側が送信したワンタイムパスワードと自動車側

が生成したワンタイムパスワードと一致していたら認証する

5 セキュリティ評価

5.1 想定する脅威

4.3 節で提案した 2 つの方式における脅威として，自動車の不正利用を目的とする攻撃と，自動車を利用不可にする可用性への攻撃の 2 つを考える．

攻撃者は正規のユーザへのなりすましに成功することで自動車の不正利用が可能となる．パスワードが盗取されている場合，攻撃者はパスワード情報を持って自動車に近づき，スマートフォンに正規のユーザのパスワードを入力することができれば，正規のユーザになりすますことができ，自動車を不正利用することができる．自動車の不正利用を目的とする攻撃として，パスワード特有の脅威から正規のユーザのパスワードを盗取する方法と，スマートフォン内のパスワード情報を直接盗取する方法，スマートフォンそのものを盗取する方法，攻撃者がスマートフォン内の情報を書き換えた後にユーザと自動車サーバの通信を盗聴することでパスワードの候補を絞ることを可能にする方法が考えられる．可用性に関する攻撃方法としてスマートフォン内の情報を無効な値に書き換える方法が考えられる．提案した方式がこれらの攻撃に対して耐性を有するか評価する．尚，個人向け方式とシェア方式とでほぼ同様の議論となるため，個人向け方式についてのみ取り上げる．

スマートフォンと自動車サーバとで鍵情報は予め共有してあるものとし，自動車サーバからの情報の漏洩は評価から除外する．

5.2 想定する攻撃への耐性

ネットワーク接続が可能な場合の個人向け方式はワンタイムパスワードを用いる方式のため，パスワードを推測することは不可能である．また，同様の理由でワンタイムパスワード入力時に覗き見をされたとしても安全性が確保される．さらに，乱数表を覗き見られてしまったとしても電話番号を登録していないと SMS が受信できないため，車両の安全性が確保される．

電話番号をフィッシングされても，その攻撃者に SMS が送信されることはないため，フィッシングに対して安全性を確保できる．また，送信したワンタイムパスワードをフィッシングされ，乱数表が知られてしまっても，同様の理由で車両の安全が確保される．

スマートフォンそのものを盗難する方法については，スマートフォンが盗難されたとしても，乱数表がないとワンタイムパスワードを作れないため車両の安全性が確保される．

ユーザは秘密の情報を一切登録しないため，使い回しによる他のシステムから秘密の情報が漏洩するリスクは存在しない．

この方式ではスマートフォン内に秘密の情報を登録していないため，スマートフォン内のパスワード情報を直接盗取する方法や，攻撃者がスマートフォン内の情報を書き換えた後にユーザと自動車サーバの通信を盗聴することでパスワードの候補を絞ることを可能にする方法，スマートフォン内の情報を無効な値に書き換える攻撃に対して耐性を有する．

5.3 自動車の不正利用への攻撃対策

攻撃者が適当に打ち込んだパスワードで認証されてしまう可能性もある．そこで複数回誤ったパスワードを入力したことを検知した場合，認証を一定期間中止するなどの対策を行えば十分に安全性を確保することができる．

6 まとめと今後の展望

6.1 まとめ

本研究ではパスワード特有の脅威への耐性を考慮したうえで，車両スマートフォンキーシステムに共通して存在する問題にも考慮し，特殊ハードウェアに依存しない車両スマートフォンキーシステムの検討を行った．自動車がネットワーク接続が可能な場合と不可能な場合の 2 つの場面に分けて考え，それぞれの場面において自動車の利用場面を 2 場面に分類し，場面に応じた利便性や現実性に合ったシステムを提案した．提案したシステムに対してセキュリティ評価を行い，なりすましによる自動車の不正利用や，スマートフォン内の情報を書き換える可用性への攻撃に対して致命的な脆弱性がないことを確認した．

6.2 今後の展望

今回の提案では自動車サーバへの攻撃や通信妨害による可用性への攻撃は提案システムに限らない攻撃方法であるため除外したが，これらの脅威についてはシステム全体で対策が必要である．

また，本研究ではシステムの提案とセキュリティの評価を行ったが，セキュリティ評価を行う際に数学的に証明する必要があると考えられる．

参考文献

[1] パスロジ株式会社. https://www.passlogy.com/corporate.

[2] 関 良明他. ネットワークセキュリティ. 共立出版株式会社, 2017.

[3] 古原 和邦他. 漏洩に強いパスワード認証とその応用. シンセシオロジー, Vol. 7, No. 3, pp. 179–189, 2014.

[4] 竹内 恭平他. スマートフォンからの情報漏えいに耐性を有する車両キーシステム. 暗号と情報セキュリティシンポジウム，2E2-1, 2019.

[5] 北村 清州他. データから読み解く自動車の使われ方の変化. IBS Annual Report 研究活動報告, pp. 13–20, 2018.