

周囲のスマートフォンを利用する個人認証技術の提案

藤井 薫^{1,a)} 稲葉 宏幸¹

概要：情報化社会の進展に伴い、利用者の正当性を確認する個人認証技術の重要性が高まっている。特に、身近な情報機器であるスマートフォンの安全性向上は重要な課題であり、その認証方式として、パスワードを用いる知識認証方式や、指紋や顔を用いる生体認証方式等が採用されている。これらの既存技術は、いずれも利用者個人が持つ情報や特性を利用する方式であるが、本研究では個人が有する社会性に着目した新たな方式を考える。具体的には、利用者の周囲に存在する友人等のスマートフォンを利用して認証を行う方式を提案する。これは、被認証者の周囲にその友人や家族等、信頼できる利用者が多数存在する状況であれば、被認証者は本人である可能性が高いと予想されることに基づいている。さらに、そのような状況は攻撃者にとっても、窃盗や覗き見などの攻撃を行いづらく、より安全と考えられる。提案方式は、このように周囲に信頼できる利用者が一定数以上存在する場合に、パスワード等を入力せずに認証する方式であり、多くの利用者が複数の信頼できる人間と一緒に行動することが多いことを利用する利便性の高い認証方式である。

キーワード：個人認証技術，人間関係，スマートフォン，Bluetooth Low Energy，デジタル署名

Proposal of Personal Authentication Using Surrounding Smartphones

KAORU FUJII^{1,a)} HIROYUKI INABA¹

Abstract: With the progress of the information society, the importance of personal authentication technology is increasing. Particularly, improving a safety of smartphones is an important issue. Therefore, several authentication methods such as knowledge authentication methods and biometric authentication methods are known. These existing technologies use the information or characteristics of individual users. In this study, we consider a new method that focuses on the social relations between individuals. Specifically, the method uses smartphones that are owned by user's friends surrounding the user. This is based on the fact that there is a high possibility that the person to be authenticated is the person himself / herself if there are many reliable users such as friends and family around the person to be authenticated. Furthermore, it is harder for adversaries to perform attacks such as theft and peeping. The proposed method authenticates without entering a password when there are a certain number of reliable users in the surrounding area. It is an easy-to-use authentication method that uses the fact that many people live with their reliable people.

Keywords: personal authentication , personal relationships , smart phone , Bluetooth Low Energy , digital signature

1. はじめに

近年、情報化社会が益々進展し、様々な場面で利用者の正当性を確認するために個人認証技術の重要性が高まって

いる。なかでも、スマートフォンの普及率は年々増加しており、そのロック解除に様々な方式が採用されている。個人認証技術は、知識認証方式、所有物認証方式、生体認証方式の三つに大きく分類される。スマートフォンのロック解除方式には、既存技術としてパスワード認証のような知識認証方式が広く普及しているが、ブルートフォース攻撃や辞書攻撃など様々な攻撃が問題となっている。その対策

¹ 京都工芸繊維大学 大学院 情報セキュリティ研究室
Kyoto Institute of Technology , Security Laboratories
^{a)} fujii15@sec.is.kit.ac.jp

として、パスワードの桁数や文字の種類を増やすなど、複雑なものに設定することが挙げられる。しかし、利用者の記憶負担が重くなるという問題がある。一方で、指紋認証や顔認証のような人間の持つ身体的特徴を利用する生体認証方式も、近年多く利用されている。利便性が高い一方、変更が困難であることや偽造の可能性が指摘されている。

2. 既存技術

スマートフォンのロック解除に広く用いられている既存の個人認証技術とその問題点について述べる。

2.1 パスワード認証方式

あらかじめ数桁の文字列をパスワードとして登録しておき、認証時に入力値が登録されたパスワードと一致するかどうかで本人確認を行う。パスワード認証の利点として、導入コストが低いことや変更が容易であることが挙げられる。一方、利用者の記憶に負担がかかる点や、他の認証方式に比べると認証に時間がかかり利便性の面で劣るという欠点がある。

2.2 指紋認証方式

人間の指紋は他人と一致する可能性は極めて低いため、認証に用いられている。認証時は指をセンサーに当てるだけでよいので、認証操作に時間や手間がかからないという利点がある。ただし、手袋をしているときや指が濡れているときには認証できないという欠点がある。また、ドアノブなど、誰でも触れる場所から簡単に指紋を採取できるため、シリコンのような身近にあるものを用いて偽造可能という報告もある [1], [2]。

2.3 顔認証方式

顔画像から目立つ特徴を抽出することで識別する。例えば、顔の各部位の相対位置や大きさ、目、ほお骨、あごの形などが特徴として利用される。近年では三次元センサを用いた三次元顔認証も行われており、より精度が向上している。ただし、マスクなどにより顔が隠れているときは認証できないという欠点がある。また、3D プリンタにより製作された顔の模型を用いても認証できることが判明している [3]。

3. 提案方式

3.1 概要

提案方式は、スマートフォンのロック解除の際に用いることを想定する。利用者が信頼する人物の所持するスマートフォンが定期的に発するパケットを、個人の認証に利用することを考える。自分自身の近くに、友人や家族のような信頼できる人間が複数いる状況は被認証者が本人である可能性が高く、さらに、攻撃者にとってそのような状況は

攻撃を行いづらく安全と考えられるからである。提案手法は、このように周囲に信頼できるユーザー (Reliable User, 以下 RU とする) が一定数以上存在する場合に、パスワード等を入力することなく認証する方式である。

3.2 Bluetooth Low Energy

提案方式において、スマートフォンを識別するために Bluetooth Low Energy (BLE) を用いるため、本節で説明する。

3.2.1 概要

BLE は近距離無線通信技術である Bluetooth の ver4.0 から追加された低消費電力モードである。大量のデータを高速で伝送するような使い方には不向きだが、速度がそれほど要求されないような環境下で長時間運用が必要な場合に適している。[4]

3.2.2 通信方法

BLE には、ブロードキャストという通信方法が定義されている。これは、ある BLE デバイスから周囲に存在する全ての BLE デバイスに対して、一方的にデータを送信するための通信方法である。ある BLE デバイスが一定周期 [5] でデータを発信し続け、別の BLE デバイスがそれをスキャン、受信する。この通信方法において、データを発信するデバイスをブロードキャスター、データを受信するデバイスをオブザーバーと呼ぶ。また、ブロードキャスターが発信しているパケットのことをアドバタイズパケットと呼ぶ。アドバタイズパケットには、仕様で定められた範囲内であれば、任意のデータを設定することができる。なお、ブロードキャスターが発信するデータは、不特定多数のオブザーバーによって受信されるため、一般に機密性を要求されるようなデータのやり取りには不適である。一般的にアドバタイズパケットの中に含まれているデータとしては企業識別子や UUID などが挙げられる。

3.2.3 通信可能距離

BLE における通信可能距離は、仕様上は 30m 以上の距離まで届くとされているが、物理的な障害やノイズの影響、低い消費電力で運用するために、実際には 5m 程度 [4] となる。受信端末側が、受信した電波強度を測る指標として、RSSI (Received Signal Strength Indication) があり、良好な無線接続を行うために十分な信号を受信しているかどうかの判断に用いられる。RSSI は相対的な指標であり、大きいほど良い品質の信号とされている。目安として、 $-70[\text{dBm}]$ から $-30[\text{dBm}]$ の値であれば望ましいとされている [6]。実用上は、5m から 10m 程度の距離なら信頼できる品質でパケットをやりとりできる。

3.3 提案方式 (基本方式)

本節では提案方式の詳しい説明を行う。提案方式は、周囲に信頼できるユーザー (RU) が一定数以上存在する場合

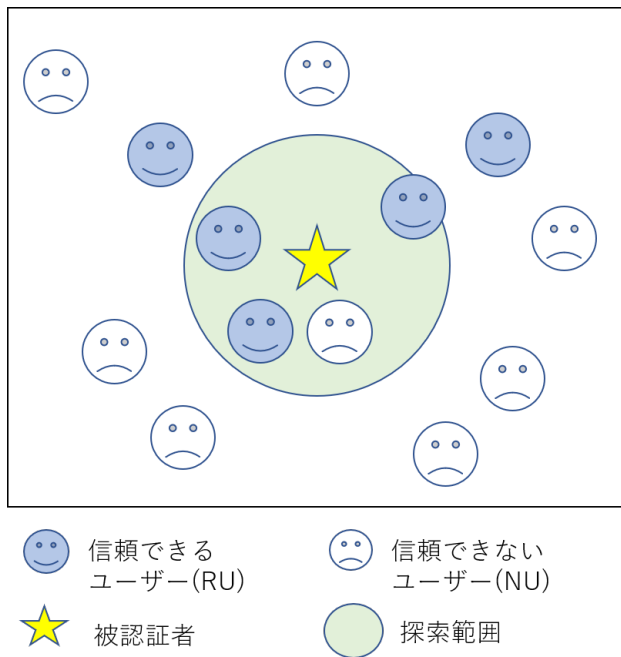


図 1 提案方式の例

Fig. 1 Example of proposed method.

に、パスワード等の入力なしに認証する方式である。なお、提案方式では前提条件として以下を仮定している。

- ユーザーはスマートフォンを所持している
- スマートフォンは常に BLE アドバタイズパケットを発している
- 利用者には多数の RU が身近に存在する
- RU は利用者に対し攻撃を行わない
- RU は利用者への攻撃を防ぐような行動をとる

事前に、利用者は自らの RU を選定し、RU が所持するスマートフォンの情報を、自分のスマートフォンに登録する必要がある。そして、認証時に RU のアドバタイズパケットを認証可能人数以上受信することができ、かつ、RU の人数が周囲のユーザー数に対して一定割合以上であれば、認証成功とする。RU でないユーザー (Non Reliable User, 以下 NU とする) は、窃盗などの攻撃を行う可能性があるため、NU が多く存在する状況はリスクがあると考えられる。このような状況下では、パスワード認証など他の認証方式を用いる必要がある。例として、図 1 を用いて説明する。

図 1 の被認証者がスマートフォンのロック解除を行おうとしている。このとき、探索範囲に RU が 3 人、NU が 1 人存在するとする。仮に、認証可能人数を 2 人、必要とする RU 数の割合を 0.3 とすれば、RU 数は 2 を超えており、さらに RU の割合は 0.75 であるので認証成功となる。逆に、認証可能人数を 4 人以上の値に設定していた場合は、図 1 の状況では認証失敗となり、被認証者は他の認証方式を用いることになる。

3.4 アルゴリズム

提案方式のアルゴリズムを説明する。機器の識別にはアドバタイズパケットに含まれる UUID を利用する。

3.4.1 事前登録

提案方式における、事前登録の手順を以下に示す。

- (1) 利用者が複数の RU を選定する。
- (2) (1) で決定した RU のスマートフォンが発するアドバタイズパケットをキャプチャする。
- (3) (2) でキャプチャしたアドバタイズパケットに含まれる UUID のハッシュ値を求め、利用者のスマートフォンにリストとして保存する。

上記 (3) で完成したリストを $List_{RU}$ とする。

3.4.2 認証時

提案方式における、認証時の手続きについて説明する。

- (1) 利用者のスマートフォンが受信可能なアドバタイズパケットをキャプチャする。
- (2) (1) でキャプチャしたアドバタイズパケットに含まれる UUID のハッシュ値を求める。
- (3) (1), (2) を一定時間 (L とする) 繰り返し、リスト ($List_{All}$ とする) を作成する。
- (4) $List_{All}$ の要素で、 $List_{RU}$ に格納されているものの個数を Cnt_{RU} 、そうでないものの個数を Cnt_{NU} とする。
- (5) Cnt_{RU} が閾値 (Th_A) 以上、かつ $Rate_{RU}$ が閾値 (Th_B) 以上であれば認証成功となる。なお $Rate_{RU}$ は式 (1) で定義される。

$$Rate_{RU} = \frac{Cnt_{RU}}{Cnt_{RU} + Cnt_{NU}} \quad (1)$$

3.5 実装と実験

提案システムの実装を、3.4 節に基づいて行った。なお、簡単のため UUID のハッシュ化は行っていない。このプログラムの動作を確認する実験を行った。その結果と考察を述べる。

3.5.1 実験内容

事前準備として、実験協力者らは所有するスマートフォンやタブレット端末に、iBeacon パケットを発するアプリケーション^{*1}をそれぞれインストールする。これにより、自由に UUID を設定でき、送出電波強度 (Tx Power) が -56[dBm] のパケットを送出できる。発信されたパケットを PC でキャプチャし、正しくそれら进行处理できることを確かめた。実験は計 3 回行う。全ての実験で共通して、受信電波強度を示す RSSI が -70[dBm] 以上のものをキャプチャするように設定している。なお、Tx Power が -56[dBm]、RSSI が -70[dBm] 以上という条件では、半径約 5m 以内の地点から発されたパケットをキャプチャすることができる。各実験の目的、実験時のパラメータを以下に示す。

^{*1} <https://itunes.apple.com/jp/app/beacon%E5%85%A5%E9%96%80/id1088591228?mt=8>

● 実験 1

正しくパケットをキャプチャし、処理できることを確認する。 $Th_A = 3$, $Th_B = 0.3$, $L = 10$ [秒] とし, $List_{RU}$ の要素数を 0~7 の範囲で変更する。

● 実験 2

L が小さい場合でも、問題なく処理できることを確認する。 $Th_A = 3$, $Th_B = 0.3$ とし, L を 5, 3, 1[秒] と変更する。 $List_{RU}$ の要素数は 7 に固定して行った。

● 実験 3

認証失敗となったときに、その原因が正しいか確認する。 $L = 1$ [秒] とし, Th_A , Th_B を変更する。

実験 1, 2 では 7 台の端末, 実験 3 では 3 台の端末で実験を行った。

3.5.2 実験結果とその考察

実験 1, 2, 3 の結果を、それぞれ表 1, 2, 3 に示す。

実験 1 では、全てのパケットのキャプチャに成功し、それらの処理も正しく行えている。実験 2 では、 $L = 1$ [秒] という最も短い時間でも、正しく処理が行えることが確認できる。1 秒以内に認証が行えれば、利便性の面で特に問題ないと考えられる。実験 3 では、 Cnt_{RU} が Th_A 未満の場合と、 $Rate_{RU}$ が Th_B 未満の場合のうち、どちらか一方のみを満たしていても認証失敗を出力することが分かる。これらの実験から、確実にアダプタイズパケットをキャプチャでき、認証処理を高速かつ正確に行えることが分かった。

表 1 実験 1 の結果

Table 1 Result of Experience 1.

$List_{RU}$ の要素数	Cnt_{RU}	Cnt_{NU}	$Rate_{RU}$	出力
0	0	7	0.00	失敗
1	1	6	0.14	失敗
2	2	5	0.29	失敗
3	3	4	0.43	成功
4	4	3	0.57	成功
5	5	2	0.71	成功
6	6	1	0.86	成功
7	7	0	1.00	成功

表 2 実験 2 の結果

Table 2 Result of Experience 2.

L [秒]	Cnt_{RU}	Cnt_{NU}	$Rate_{RU}$	出力
5	7	0	1.00	成功
3	7	0	1.00	成功
1	7	0	1.00	成功
1	7	0	1.00	成功

3.6 基本方式の考察

提案方式（基本方式）の利点と問題点を示す。

表 3 実験 3 の結果

Table 3 Result of Experience 3.

Th_A	Cnt_{RU}	Th_B	$Rate_{RU}$	認証失敗原因
3	2	0.3	0.67	$Cnt_{RU} < Th_A$
2	2	0.8	0.67	$Rate_{RU} < Th_B$

3.6.1 利点

● 利便性が良い

特定の状況下では利用者は認証操作を意識することなくロックを解除できる。例えば、旅行時やオフィス内のように複数の RU と一緒に行動するような場合には非常に有効と考えられる。

● RU のスマートフォンの紛失に気付くことができる

十分な数の RU が近くにいるにも関わらず認証できないときは、RU の誰かがスマートフォンを落としたり盗まれたりしている恐れがある。このような状況に、すぐに気付くことができる可能性がある。

● 盗難被害に強い

スマートフォンを盗難されたとしても、RU が近くにいなくて認証できない。なお、多数の RU のスマートフォンと自分のスマートフォンを同時に盗難されてしまった場合は認証可能であるが、そのような状況は起こりにくいと考えられる。認証可能人数 Th_A を大きくすることにより、この攻撃に対するリスクをさらに減らすことができる。

● 覗き見攻撃や録画攻撃に強い

本方式は、知識認証方式のように秘密情報を入力する必要がないので、これらの攻撃で直接情報を盗まれることはない。

● RU のリストを柔軟に変更できる

利用者は所持するリストを変更することによって、認証に用いる RU を変更することができる。自身の生活や環境の変化に応じて RU を選定することができる。また、RU を攻撃者に知られてしまったときにも変更することができる。

● 本人が認証できない状態でも認証できる可能性がある

本人である利用者が認証できる状況にないが、スマートフォンはあるという状況であれば、認証できる可能性がある。例えば、怪我で意識不明になるなどで本人が認証できなくなってしまった場合でも、家族などの親しい間柄であれば RU の推定が可能であろう。このような状況ならば、家族は RU の協力を得て、認証できると考えられる。

3.6.2 問題点

● RU 情報の漏洩

スマートフォンに格納していた RU の情報が、ウイルス感染などにより漏洩してしまうことが考えられる。提案方式では、RU 情報をハッシュ化して保存するの

で RU の情報がすぐに知られることはない。ただし、攻撃者が RU の候補リストを有している場合には RU が判明する危険はある。

- アドバタイズパケットの偽造
アドバタイズパケットを偽造する攻撃が考えられる。この攻撃について以下に詳しく考察する。
- 利用者が認証する瞬間に、周囲にあるアドバタイズパケットを傍受し偽造する
RU の特定は難しくても、利用者が認証している瞬間を狙ってアドバタイズパケットを傍受する攻撃が考えられる。しかし、攻撃者が傍受する位置は利用者の位置からはある程度離れた位置にいると考えられるため、全く同じパケット群を入手できるとは考えにくい。ただし、何度かこれを繰り返し、それらの共通部分を求めることで RU を特定できる可能性はある。
- 適当なパケットを大量にブロードキャストする
適当なアドバタイズパケットを大量にブロードキャストして、認証処理を重くさせる攻撃が考えられる。しかし、このような状況は近くに悪意を持った攻撃者がいる可能性を利用者に知られることになるので、攻撃者にとって得策ではないと考えられる。
- BLE を OFF にして利用者に接近する
RU 率が低いときに認証失敗となるが、NU がアドバタイズパケットを発さないようにして利用者に近づき、窃盗などの攻撃を行うことが考えられる。こうすれば RU 率に影響を与えないため、NU が周囲に多数存在しても認証できる可能性がある。

4. 提案方式の改良

第3節で述べた基本方式は、アドバタイズパケットが偽造可能であることを利用した攻撃への対策が不十分と考えられる。また、RU 率は攻撃者がアドバタイズパケットを発さない場合には無効な指標になってしまう。これらから、本節ではその改良案としてデジタル署名を用いる方式を考える。

4.1 改良方式

事前準備として、被認証者は信頼できるユーザー RU の公開鍵 Kp を入手しておき、公開鍵リスト $List_{Kp} = \{Kp_i\}$ として保存しておく。実際の認証時には以下のような手順で認証を行う。なお、チャレンジビット列とは、認証の都度異なる値になるようにランダムに設定される値である。

- (1) 被認証者がチャレンジビット列 (Ch) をブロードキャストする。 Cnt_{RU} を 0 に初期化する。
- (2) Ch を受信した周囲のスマートフォンが、 Ch に対する署名 σ をブロードキャストする。
- (3) 被認証者が $List_{Kp}$ 中の全ての公開鍵 Kp を用いて署名 σ を確認し、正しい署名があれば Cnt_{RU} を 1 だけ

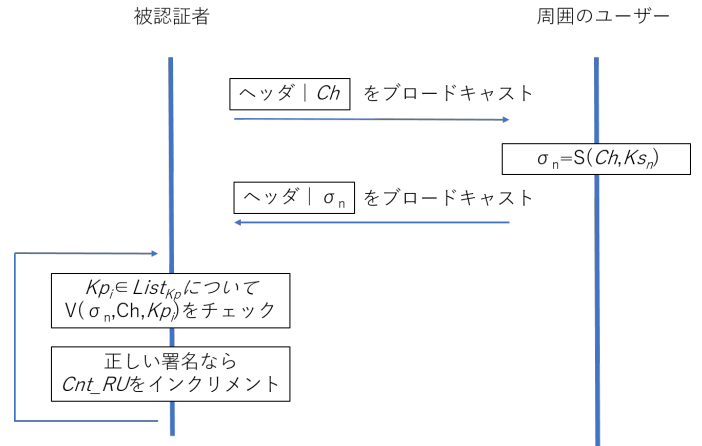


図2 鍵を用いた方式の認証時の流れ

Fig. 2 Flow of authentication using digital signatures.

増加する。

- (4) 受信した全ての署名 σ に対し (3) を行い、制限時間 L 内に Cnt_{RU} が認証可能人数 Th 以上になれば認証成功とする。制限時間 L を超えると認証失敗とする。
- 認証時の流れを図2に示す。ヘッダには本方式を用いることを示す内容が含まれているものとする。

なお、チャレンジビット列を用いるため、毎回ブロードキャストされるパケットの内容が異なる。従って、攻撃者によるリプレイ攻撃は行えない。

4.2 改良方式の考察

基本方式における問題点であった、アドバタイズパケットの偽造が可能である問題を、デジタル署名を用いることで解決できた。通信は全てブロードキャストされ、チャレンジビット列とその署名のみを送信するため、攻撃者に有益な情報を盗まれるリスクはないと考えられる。

また、手順 (3) において、RU の情報を攻撃者から秘匿するために、周囲のユーザーから送られるパケットには対応するユーザー ID が明記されていないため、正しい署名が得られるまでリスト中の全ての公開鍵を試行することになる。対象が不特定多数の場合はこの方式は非現実的であるが、本方式において公開鍵のリストの要素数は高々数十程度だと考えられる。従って、全ての鍵で確認をしても現実的な時間内に確認が可能であると考えられる。

5. まとめ

本論文では、既存の個人認証技術とは異なり、自分自身の所有物ではないものを認証に用いる方式を提案した。提案方式は、周囲に存在する友人などのスマートフォンを用いて個人認証を行う。本方式によって、利便性に優れた認証を行うことができ、さらに、信頼できるユーザーが複数存在すれば、彼らによってある程度攻撃を抑止する効果も期待できる。考察の結果、様々な場面で本方式が有効であ

ることが分かった。今後は、スマートフォンで認証を行うアプリケーションを実装し、評価実験を行う。

参考文献

- [1] Apple Geek LABO : <https://apple-geeks.com/iphone-58-2783>(2019/8/22).
- [2] 牧野武文 : <https://the01.jp/p0006463/>(2019/8/22).
- [3] 佐藤岳大 : iPhone X の顔認識「Face ID」が 3D プリントのマスクで突破される , <https://pc.watch.impress.co.jp/docs/news/1091311.html> (2019/8/22).
- [4] Bluetooth Low Energy, https://ja.wikipedia.org/wiki/Bluetooth_Low_Energy(2019/8/22).
- [5] FIELD DESIGN INC. : https://fielddesign.jp/technology/ble/blespec_advertise/ (2019/8/22).
- [6] IBS JAPAN CO., LTD. : <https://www.ibsjapan.co.jp/tech/details/metageek-solution/understanding-rssi.html> (2019/8/22).