M-023

近距離通信を用いた親子端末の連携を鍵とするスマートフォン認証

Smartphone Authentication Based on Cooperation between Parents' and Children's Terminals Using Short-Range Communication

岸里 正樹† 高井 昌彰‡
Masaki Kishisato Yoshiaki Takai

1. はじめに

スマートフォンからのネットショッピングやアプリのインストールなど，子どもが単独でそれらの操作を行うことが望ましくない状況では，監督者である親が子どものネット利用を見守り，利用を適正に制限することが必要である．

子どもの利用する端末にロックをかけ，必要に応じて親が解除を行うという簡単なアプローチにおいては，ロックの解除キーとしてパスコードや画面を指でなぞるパターン認証を用いた場合，子どもが親の操作を背後から覗き込むことによって解除キーを容易に盗み取ることが可能である．

本稿では，上記の問題を防ぎ，安全かつ手軽に，親が子どもを見守りながら認証を行うことを目的として，スマートフォン端末の Bluetooth 機能を利用し，親と子どもの端末同士を一定距離内に近付けて連携させることで子どもの端末のロック解除を実現する認証システムについて述べる．

2. システム設計

2.1 認証の流れ

本システムでは，複数の端末を，認証を経て許可の権限を与える親端末と，許可を受ける子端末の 2 種類に分けて連携させる．一連の認証動作は，端末同士の接近を要する第一段階と，親端末で操作を行う第二段階に分けられる．

第一段階では，親端末が周辺のデバイスを検索し，子端末を発見した際に，電波の受信強度をもとに子端末までの距離を推定する．両端末が物理的に一定距離内に接近していない場合，認証の第二段階に進むことはできない．

第一段階の認証を通過した後，親端末での第二段階の認証操作を行う．これを通過することをもって，子端末のロックが解除され，目的の操作を行う権限が与えられる．

また，一度端末同士を近づけて認証が完了し，子端末に権限が与えられた後であっても，親端末と子端末が一定距離以上離れてしまった場合には，再び端末同士の接近と認証動作を要求する．

2.2 第一段階の認証

はじめに親端末は Bluetooth を用いて近くにあるデバイスをスキャンする．その中から予め登録しておいた子端末が発見されると，RSSI（電波の受信強度）をもとに端末間の距離測定を開始する．

RSSI 値を s，距離を r とすると，RSSI から端末間距離の概算値への変換は次式で求めることができる[1].

r = 10^((距離 1m のときの RSSI - s) / (10 * 2.0))

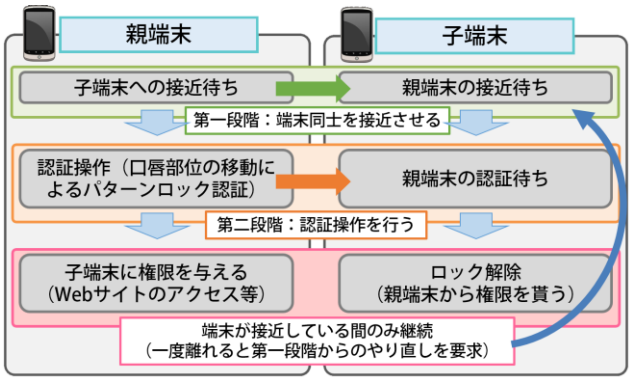

図 1 システムの構成図

算出した距離を用いて，親子端末が接近しているかどうかの判定を行う．予め設定した閾値よりも小さければ，端末同士が接近していると見なし，Bluetooth のペアリングを行い，認証の第二段階に移行する．

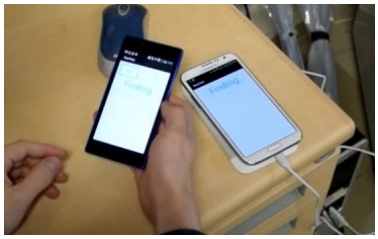

図 2 第一段階の認証（端末の接近）

2.3 第二段階の認証

第二段階の認証方法として，パスコードやパターンロック等といった従来の簡易な認証方法を利用すると，第 1 章で述べたように，子どもによるショルダーハック等のリスクを回避できない．

そこで，顔面の口唇部位の移動による認証システム[2]を用いることとする．このシステムは，まず図 3 のように顔面をカメラ方向に向けたまま口唇部位だけを連続的に上下左右へと移動させ，スマートフォン端末のカメラでその動きを認識する．システムは口唇部位の動きを図 4 に示すような格子パターン上での移動ベクトルの列へと変換することで，従来のパターンロック認証と同様の機能を実現するものである．

この認証システムを用いることによって，ショルダーハックや，スマートフォン画面上の指の痕跡から認証キーを読み取ることを防止しながら，親端末の認証を安全に行うことができる．

† 北海道大学大学院情報科学研究科, Graduate school of Information Science and Technology, Hokkaido University
‡ 北海道大学情報基盤センター, Information Initiative Center, Hokkaido University

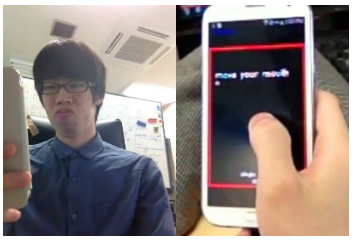

図 3 口唇部位の移動

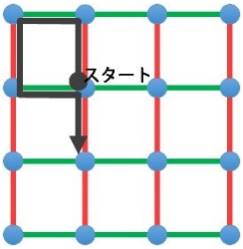

図 4 格子状パターンロック

2.4 一対多及び多対多での利用

連携を行う対象である親端末と子端末は，必ずしも一対一の対応に制限されるものではない．例えば，1 台の親端末が複数台の子端末に対して同時に権限を与える場合や，複数台の親端末が全て許可しなければ子端末に権限を与えないようにする場合，あるいは，複数の親端末のうち 1 台でも許可すれば子端末に権限を与える場合など，多様な連携が想定される．

親端末と子端末のいずれかが複数台であっても，第一段階，第二段階の認証に必要な条件が複数台に対するものに変わるのみである．

3. 実行結果

3.1 親子端末における動作結果

親端末 1 台と子端末 1 台を連携させ，認証動作を行った際の動作画面の例を図 5 に示す．ここではロック解除後に子端末が利用可能となる機能としてショッピングサイトの閲覧を想定している．また，実装したシステムを用いて認証の各段階に要する時間を計測した結果を表 1 に示す．

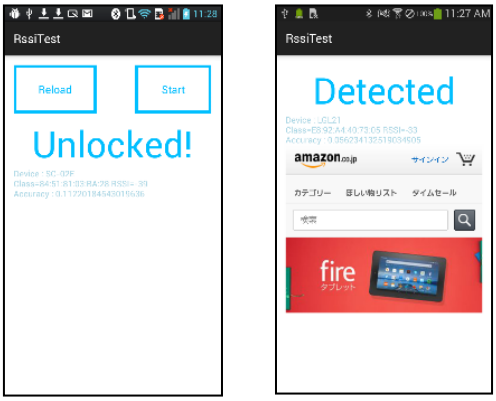

図 5 親子端末の動作画面（端末検出とロック解除）

実験において，端末 2 台を両方とも移動させていないにもかかわらず，更新のたびに RSSI 値が大きく変動する現象がしばしば見られた．その結果，端末同士が近くにあっても親端末が子端末を発見できず，接続に時間を要することがあった．一方，端末同士がはじめから離れている場合には，近いと誤認識することはなかった．現在の実装では，子端末を発見できない場合に，親端末が Bluetooth の発見待ちをリセットし，接近の検知処理を再実行している．

動作	所要時間(s)
端末接近～口唇認証開始 （閾値設定：22cm, 配置距離：10cm）	15.61
口唇認証 （操作開始～ロックの解除） パターン：↑←↓→↓	10.89
ロック解除～再ロック （閾値設定：22cm, 配置距離：100cm）	11.56

表 1 認証の各段階に要する時間（10 回の平均値）

また，Bluetooth のペアリングを行っている際に RSSI 値を取得することができない状況も見られた．この場合も，ペアリングのリセットを行うことで再び取得が可能になるが，値の更新が遅れ，認証動作のリアルタイム性が失われてしまう問題点がある．安定して RSSI 値を取得できる実装方法を検討する必要がある．

3.2 動作環境

本認証システムを動作させるスマートフォンには，親端末として au LGL21(OS：Android 4.0.4, CPU：1.5GHz(4C), Bluetooth：4.0)，子端末として Docomo SC-02E(OS：Android 4.3, CPU：1.6GHz, Bluetooth：4.0)を用い，本システムの開発言語には Java を用いた．表 1 に示した所要時間はこの動作環境で測定されたものである．

4. まとめと今後の課題

本稿では，スマートフォン端末同士を一定距離内に近付けることでロックの解除を行うことのできる認証システムについて述べた．第 2 章では親子端末の連携による認証プロセスに重点を置いた実装について述べたが，認証の完了後も親が継続して子どものネット利用を見守ることのできる機能の実現を現在検討している．子端末に対しブラウジングを許可した際には，ブラウザのスクリーンショットを親端末に定期的にサンプリングして送信し，また，アプリのインストールを許可した際には，そのアプリの詳細な情報を親端末に送信するといった機能が例として考えられる．

また，親子間におけるフィルタリング以外の応用として，一般の PC 等の利用開始時にユーザ認証を行う際の鍵としてユーザのスマートフォンを用い，本システムと同様の連携を行うことで，口唇部位の移動を認証キーの入力方法とした安全なユーザ認証の実現が考えられる．

その他，安定した RSSI 取得方法の改善，他プラットフォームへの移植と処理高速化は今後の課題である．

参考文献

[1] Erin-Ee-Lin Lau, Boon-Giin Lee, Seung-Chul Lee, Wan-Young Chung: "Enhanced RSSI-Based High Accuracy Real-time User Location Tracking System for Indoor and Outdoor Environments", (http://www.s2is.org/Issues/v1/n2/papers/paper14.pdf, 参照：2016/6/21).

[2] 岸里正樹, 高井昌彰: 口唇領域の動きの画像認識を用いたスマートデバイス向けパターンロックシステム”, 第 14 回情報科学技術フォーラム（FIT2015）, M-031, Vol.4, pp.363-364（2015）.