空間依存情報を用いた場所ベース認証方式

蜂谷 達郎[1]　萬代 雅希[1]

概要：本論文では空間依存情報を用いた認証システム（SmartLocAuth）を提案する．SmartLocAuth では，特定の場所における空間依存情報を利用することにより場所ベースの認証を行う．空間依存情報とは場所に依存する情報であり，無線 LAN のアクセスポイントからの Service Set Identifier（SSID）や環境音などが挙げられる．従来の場所ベースの認証では Global-Positioning System（GPS）を用いるのが一般的だが，SmartLocAuth では GPS を用いないため，GPS では正確な位置情報が取得できない屋内でも利用できる．更に GPS を搭載していない機器でも利用可能である．本論文では空間依存情報として SSID を用い，SmartLocAuth を Android OS 4.0 の Galaxy Nexus に実装し，登録時間と認証距離を評価をする．評価の結果，認証に成功する範囲は登録地点から 5m 以内で限定でき，SmartLocAuth が認証方式として有効であることを確認する．

Location-based Authentication –SmartLocAuth–

Tatsuro Hachiya[1]　Masaki Bandai[1]

1. 緒論

持ち運びが可能な機器としてタブレットやスマートフォンのようなモバイル端末あるいはラップトップ PC などが利用されているが，その中には機密情報が含まれていることが多い．そのため，他人にモバイル端末やラップトップ PC を操作させないように，パスワードなどが広く利用されている．しかし，モバイル端末やラップトップ PC の所有者本人しか操作し得ない状況にも関わらず，認証の度にパスワード入力などの煩雑な作業をしなければならないのは非常に面倒であり，パスワードを設定しない原因にもなっている [1]．パスワード以外にも様々な認証方式が研究されているが，その多くは個人をベースにした認証である．また，場所ベースの認証には Global-Positioning System（GPS）を利用するものが多く，ラップトップ PC など GPS が搭載されていない機器では利用することができない．

本論文では空間依存情報を用いた認証システム（SmartLocAuth）を提案する．SmartLocAuth では，特定の場所における空間依存情報を利用することにより場所ベースの認証を行う．空間依存情報とは場所に依存する情報であり，無線 LAN のアクセスポイントからの Service Set Identifier（SSID）や環境音などが挙げられる．従来の場所ベースの認証では Global-Positioning System（GPS）を用いるのが一般的だが，SmartLocAuth では GPS を用いないため，GPS では正確な位置情報が取得できない屋内でも利用できる．更に GPS を搭載していない機器でも利用可能である．本論文では空間依存情報として SSID を用い，SmartLocAuth を Android OS 4.0 の Galaxy Nexus に実装し，登録時間と認証距離を評価をする．評価の結果，認証に成功する範囲は登録地点から 5m 以内で限定でき，SmartLocAuth が認証方式として有効であることを確認する．

2. 関連研究

コンピュータにおける認証とは，コンピュータを操作する際，操作者にコンピュータを操作する権利があるか確認する作業のことである．認証の方式は図 **1** のように分類できる [2]．認証方式には個人ベースの認証と場所ベースの認証がある．

個人ベースの認証とは，認証者が認証に成功すべき人（以下，正規ユーザ）かどうかを確かめることによる認証である．現在でも様々な認証方式に関する研究が行われてい

[1] 上智大学
Sophia University
Chiyoda, Tokyo 102–8554, Japan

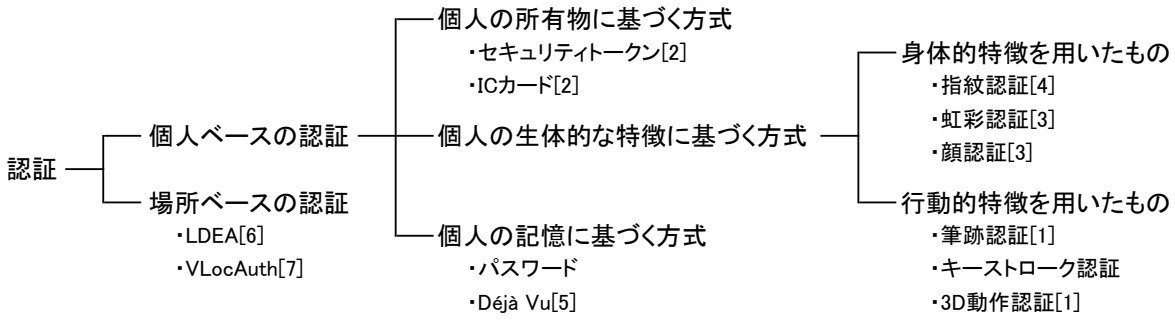

図 1　認証方式の分類

るが，その多くは個人ベースの認証である．また，我々が日常の生活で利用することが多いのは個人ベースの認証である．具体例として IC カードによる認証，指紋認証，パスワード認証などが挙げられる．

一方場所ベースの認証とは，認証者が認証に成功すべき場所にいるかどうかを確かめることによる認証である．本研究では場所ベースの認証に注目する．代表的な場所ベースの認証は以下の三つである．

一つ目は GPS と Toleration Distance（TD）を用いた認証である [6]．TD とは誤差の許容範囲のことである．GPS だけを用いて認証を行う場合，位置情報に誤差が生じるため認証に成功するべき場所でも失敗することがある．そこで TD を用いることにより，GPS による位置情報の誤差の問題を解決する．例えば TD = 5m と設定すると，GPS が示した位置情報から半径 5m の範囲までは認証可能になる．このように TD を設定することで，GPS が示す位置情報が本来の位置と異なっていても，認証に成功すべき場所で失敗することはない．

二つ目は VLocAuth である [7]．VLocAuth では場所ベースの認証方式として GPS のみではなく，ユビキタスカメラを利用する．VLocAuth では，認証者の GPS による位置情報を含む範囲を撮影するユビキタスカメラを用いて，本当に認証者は GPS の示す場所にいるのかを確認することで認証を行う．図 **2** に VLocAuth の認証を示す．具体的な認証手順は以下の通りである．

(1) 認証者は GPS による位置情報を Authentication Server(AS) を経由して Camera Server(CS) に送信
(2) CS は受け取った位置情報を含む範囲を撮影できるユビキタスカメラに位置情報を転送
(3) 移動中の認証者の GPS による位置情報を含む範囲を，ユビキタスカメラが撮影
(4) 認証者が移動した際の GPS による位置情報とユビキタスカメラに映る動きが一致していれば認証成功

ただし VLocAuth はユビキタスカメラが設置されていること，圏外ではなく通信可能な環境下であることを前提としている．そのため，ユビキタスカメラが設置されない自宅や研究室，職場などの屋内や，通信不可能な環境下で利用

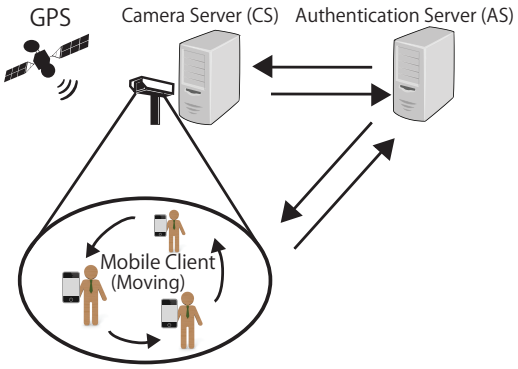

図 2　VLocAuth の認証

することができない．

三つ目は位置と速度を利用した認証である [8]．位置と速度を利用した認証では，ある地点から移動する際の通過地点，および移動速度を用いることにより認証を行う．なお位置情報を取得するためには GPS を用いる．例えば，地点 A から地点 B，C，D を通過して地点 E に到達する場合を考える．地点 E で認証に成功するには，地点 B，C，D を指定された速度で通過しなければならない．あらかじめ地点 A を出発してから地点 E に到達するまで通過地点，および各通過地点を通過する際の速度を登録する．

以上のように，既存の場所ベースの認証では GPS を用いる必要がある．そのため，GPS が搭載されていない機器では利用することができない．更に屋内など GPS によって正確な位置情報が得られない場所において利用できないことが課題である．

3. 提案方式

本論文では，空間依存情報を用いた場所ベースの認証 (SmartLocAuth) を提案する．SmartLocAuth は場所ベースの認証方式でありながら，GPS を用いることなく認証を行うことができる．そのため，GPS では正確な位置情報が取得できない屋内でも利用できる．また，モバイル端末に限らず GPS を搭載していないラップトップ PC などの機器でも利用できる．

本章では SmartLocAuth のアルゴリズムを説明した後，SmartLocAuth の実装について説明する．

3.1 空間依存情報

SmartLocAuth では，特定の場所における空間依存情報を利用することにより場所ベースの認証を行う．空間依存情報とは場所に依存する情報であり，無線 LAN のアクセスポイントからの Service Set Identifier(SSID) や環境音 [9] などが挙げられる．ここで，SSID とは無線 LAN におけるアクセスポイントの識別子のことであり，最大 32 文字までの英数字を任意に設定できる．無線 LAN は電波を使って通信するため，有線 LAN とは異なり混信が生じる可能性がある．そのため，混信を避けるために SSID が利用される．無線 LAN の電波は限られた範囲にしか発信されない．つまり場所によって検出される SSID は異なるため，空間依存情報として SSID を用いることは有効であると考えられる．

環境音とは，音声や音楽以外の動作音など身の回りの音である．場所によって環境音は異なる．例えば，賑やかなレストランにおける環境音と，一人で部屋にいるときの環境音は異なる．環境音は音声や音楽を除いた音であり，同じ場所において環境音の類似性が高いと考えられる．以下では空間依存情報として SSID を用いる場合を考える．

3.2 SmartLocAuth のアルゴリズム

認証機器において，SmartLocAuth では SSID の登録および認証時に登録 SSID リストと認証 SSID リストを用いる．SmartLocAuth のアルゴリズムは SSID リストの登録時の処理と認証時の処理の二つがある．

- 登録時の処理
  - (1) 認証機器が周辺の SSID を T_A 秒の間取得
  - (2) 取得した SSID と SSID 毎の信号受信強度（RSSI）の平均値を登録 SSID リストに追加
- 認証時の処理
  - (1) 認証機器が周辺の SSID と各 SSID に対する RSSI を取得
  - (2) 取得した SSID と各 SSID に対する RSSI を認証 SSID リストに追加
  - (3) 認証 SSID リストと登録 SSID リストを比較し，一致率 P を算出
  - (4) 一致率 P が指定した割合 P_{th} 以上（$P \geq P_{th}$）であれば認証成功，P_{th} よりも小さいとき（$P < P_{th}$）は認証失敗

認証時の処理で求める一致率 P を以下のように定義する．

$$\text{一致率 } P = \frac{\text{一致数 } P_{num}}{\text{認証 SSID の数}} \times 100 \qquad (1)$$

一致数 P_{num} は以下のように定義する．

$$\text{一致数 } P_{num} = \text{認証 SSID の中で登録 SSID リストに含まれていて，かつ } R_{ave} - R_{th} \leq R_{auth} \leq R_{ave} + R_{th} \text{ を満たす認証 SSID の数}$$

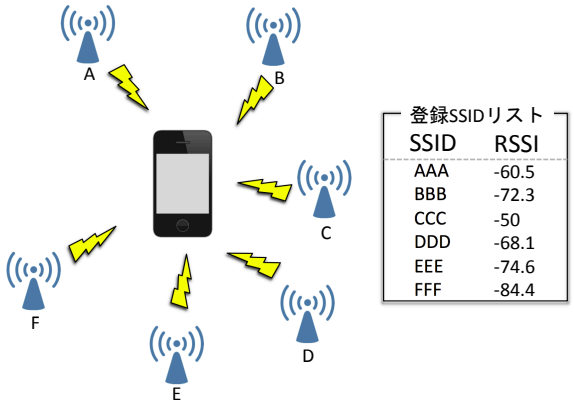

図 3　SmartLocAuth の登録方法

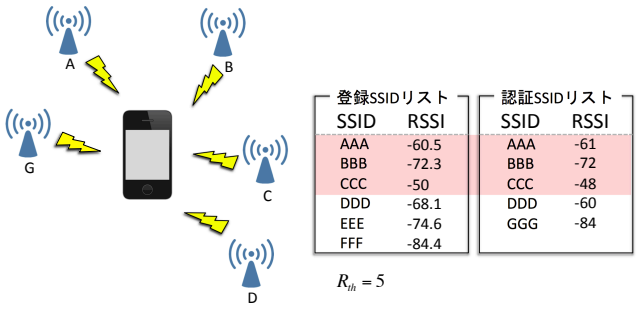

図 5　SmartLocAuth の認証方法

を満たす認証 SSID の数

R_{th} は RSSI の閾値，R_{ave} は各登録 SSID の RSSI の平均値，R_{auth} は各認証 SSID の RSSI を表す．

図 3 に SmartLocAuth における登録時の処理の例を示す．認証機器の周辺にアクセスポイント（AP）が 7 個存在し，各 AP の名前を A，B，…，G とする．登録時の処理において，T_A 秒間 SSID を取得した結果，A〜F から 6 個の SSID（AAA，BBB，…，FFF）が検出されたと仮定する．この 6 個の SSID と各 SSID に対する RSSI の平均値が登録 SSID リストに追加される．

図 5 に SmartLocAuth における認証時の処理の例を示す．ここで $R_{th} = 5$，$P_{th} = 80$ とする．認証時の処理では，E の SSID である EEE と，F の SSID である FFF が検出されず，AAA，BBB，CCC，DDD，GGG の 5 個の SSID が検出されたと仮定する．この 5 個の SSID と各 SSID に対する RSSI が認証 SSID リストに追加される．登録 SSID リストと認証 SSID リストを比較すると，AAA，BBB，CCC，DDD の 4 個の SSID が登録 SSID リストと認証 SSID リストの両方に含まれていることが分かる．この 4 個の SSID の中で $R_{ave} - R_{th} \leq R_{auth} \leq R_{ave} + R_{th}$ を満たす SSID を調べる．AAA，BBB，CCC の 3 個の SSID では条件を満たすが，DDD の RSSI は $-60 > -68.1 + 5$ であるため条件を満たさないことが分かる．よって，一致率 $P = 3/5 \times 100 = 60$ となる．今回，$P_{th} = 80$ と設定したので，$P_{th} > 60$ となるため認証に失敗する．

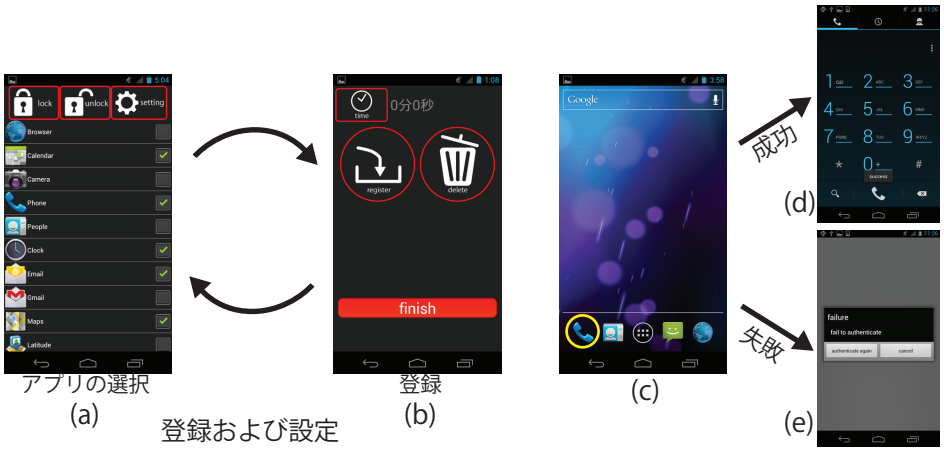

図 4　SmartLocAuth アプリの画面

3.3　SmartLocAuth を使ったアプリケーション

SmartLocAuth の利用方法は二つある．一つは SmartLocAuth のみを認証に用いる方法であり，もう一つは SmartLocAuth で認証できない際に他の認証方式を併用する方法である．

SmartLocAuth のみを認証に用いる場合，SmartLocAuth で登録処理を行った場所でしか認証機器を利用することができない．つまり登録処理を行った場所にいる人なら認証機器を利用することができる．そのため利用例として，社外へ持ち出し禁止の機密情報などが挙げられる．ある会社の社員しか閲覧することのできない機密情報に対し，パスワードを利用する場合と SmartLocAuth を利用する場合を比較する．パスワードを利用する場合，機密情報を閲覧するたびに社員はパスワードを入力しなければならない．また，機密情報閲覧専用のパスワードを設定する場合，社員はそのパスワードを新たに記憶する必要があり，各社員が社内で既に利用しているパスワードを機密情報の閲覧に利用する場合，パスワード管理が面倒になる．更に，パスワードが外部に流出した際には，社外の人に閲覧される危険性がある．一方 SmartLocAuth を利用する場合，機密情報を閲覧するためにパスワード入力のような面倒な認証作業は必要ない．また，社員は新たにパスワードを記憶する必要がなく，パスワード管理が楽である．SmartLocAuth のみを認証として利用できない例として，スマートフォンの画面ロックなどが挙げられる．画面ロックに対して SmartLocAuth のみを用いた認証を適用すると，SmartLocAuth の登録を行った場所以外ではスマートフォンを利用できなくなる．

SmartLocAuth で認証できない際に他の認証方式を用いる場合，SmartLocAuth は認証作業を容易にすることができる．モバイル端末やラップトップ PC の所有者本人しか操作し得ない状況にも関わらず，パスワード入力などの煩雑な作業を行うことは非常に面倒である．SmartLocAuth は認証機器の所有者本人しか操作し得ない状況で，自動で認証作業を行うために SmartLocAuth が利用できる．使用例として，スマートフォンの画面ロックやアプリケーションのロック，あるいはラップトップ PC 内の特定のファイルやソフトのロック，ログイン画面での認証などが挙げられる．

3.4　SmartLocAuth の実装

SmartLocAuth をスマートフォンに実装する．実装する機器は Android OS4.0 の GALAXY NEXUS である．スマートフォンで SmartLocAuth を利用する場合，SmartLocAuth を適用する対象は二つある．一つはスマートフォン内の任意のアプリケーション，もう一つはスマートフォン自体のロックつまり画面ロックである．本論文ではスマートフォン内の任意のアプリケーションをロックする方法を実装する．なお，本論文で実装する，SmartLocAuth における空間依存情報の登録および認証を行うアプリケーションを SmartLocAuth アプリと呼ぶ．

SmartLocAuth アプリの画面を図 4 に示す．

- 登録時の処理
  - (1) SmartLocAuth アプリを起動しロックするアプリケーションを選択する (a)
  - (2) 周辺の SSID と RSSI 情報を取得する (b)
- 認証時の処理
  - (1) 今，電話アプリケーションが SmartLocAuth アプリによってロックがかけられているとする．
  - (2) 電話アプリケーションを起動する (c)
  - (3) バックグラウンドで認証時の処理が実行される．
    - もし認証に成功すれば電話アプリケーションを利用することが可能である (d)
    - もし認証に失敗すれば電話アプリケーションはロックされたままである (e)

以上から分かる通り，認証のためにユーザが行う作業は全くない．

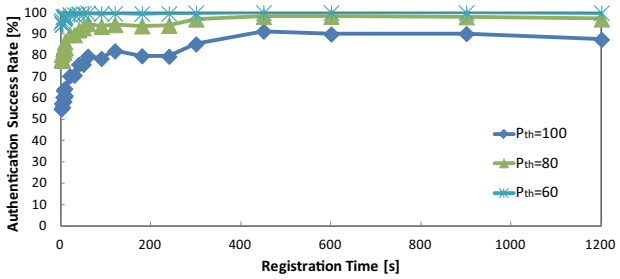

図 6　登録時間と認証成功率の関係

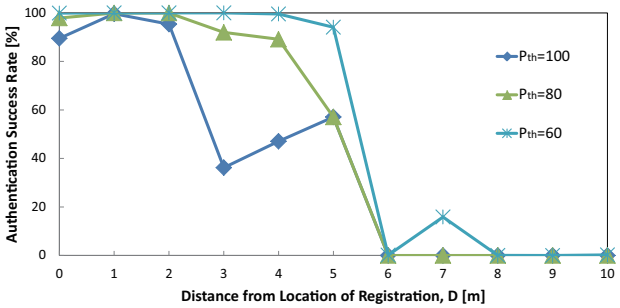

図 7　登録地点からの距離と認証成功率の関係

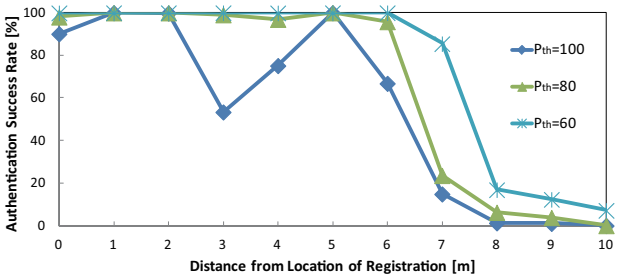

図 8　登録地点からの距離と認証成功率の関係（RSSI を用いない場合）

4.　性能評価

本章ではスマートフォン上に SmartLocAuth を実装し，性能評価を行う．登録時間と認証成功範囲の二つを評価する．なお，本論文の評価では Android OS 4.0 の GALAXY NEXUS を用いる．

4.1　登録時間に関する評価

図 **6** に登録時間に対する認証成功率を示す．認証成功率の定義は以下の通りである．

$$\text{認証成功率} = \frac{\text{認証に成功した SSID リストの数}}{\text{認証に用いた SSID リストの数}}$$

評価方法は以下の通りである．

(1) 登録時間 T_A =1，2，3，4，5，6，7，8，9，10，20，30，40，50，60，90，120，180，240，300，450，600，900 と設定
(2) 各登録時間 T_A において登録処理を実行
(3) 登録地点と同じ場所で，各登録時間 T_A の登録 SSID リストに対して 5,000 回の認証作業を実行
(4) 認証成功率を算出

以上の 4 ステップを 10 回行い，各登録時間 T_A における認証成功率の平均値を算出する．

図 6 に，登録地点における認証成功率が 95%以上となるのに必要な登録時間 T_A を評価する．図 6 より，$P_{th} = 60$ の場合は $T_A \approx 5$ 秒の登録時間が必要であり，$P_{th} = 80$ の場合は $T_A \approx 240$ 秒（約 4 分）の登録時間が必要であることが分かる．これに対し，$P_{th} = 100$ の場合，T_A は 900 秒（15 分）よりも長時間必要である．以上より、登録時間 T_A を長くするほど認証成功率が向上し，中でも P_{th} =60，80 が実用的であることが分かる．登録時間 T_A を長くするほど認証成功率が向上する理由として，同じ場所にも関わらず，電波の状態により取得できる時もあればできない時もある SSID が存在することが挙げられる．T_A を長くするとより多くの SSID が登録できるため，P_{th} を大きく設定しても高い認証成功率を実現できる．一方で，P_{th} を低く設定するほど短い登録時間で高い認証成功率が得られる．

4.2　認証成功範囲に関する評価

登録地点からの距離に対する認証成功率を求める評価方法は以下の通りである．

(1) 登録時間を $T_A = 900$ と設定
(2) 登録処理を実行
(3) 登録地点から Dm 間隔で離れた地点において，$R_{th} = 16$ と設定し 5,000 回の認証作業を実行
(4) 認証成功率を算出

以上の 4 ステップを 10 回繰り返し，各距離における認証成功率の平均値求める．

図 **7** に登録地点からの距離に対する認証成功率を示す．図 7 より，$P_{th} = 100$ の場合は登録地点における認証成功率は約 90%であるが，登録地点から 3m 離れた地点では認証成功率が約 40%になり，登録地点から 6m 以上離れると認証成功率が 0%になる．よって，$P_{th} = 100$ の場合は極めて限定された範囲でのみ認証に成功することが分かる．$P_{th} = 80$ の場合は登録地点から 2m 離れた地点までは認証成功率が 100%に極めて近く，登録地点から 6m 以上離れると認証成功率が 0%になる．$P_{th} = 60$ の場合は登録地点から 5m 離れた地点までは認証成功率が 100%に極めて近いが，登録地点から 8m 離れた地点でも認証成功率は 0%ではない．そのため，$P_{th} = 60$ の場合は $P_{th} = 80$ や $P_{th} = 100$ と比較して認証範囲が限定されていないと言える．

次に認証成功率を求める際に RSSI を用いない場合を図 **8** に示す．図 8 と図 7 と比較すると，登録地点から 2m 離れた地点までは全く同じ結果となる．しかし図 8 では，$P_{th} = 100$ および $P_{th} = 80$ では登録地点から 7m 離れた

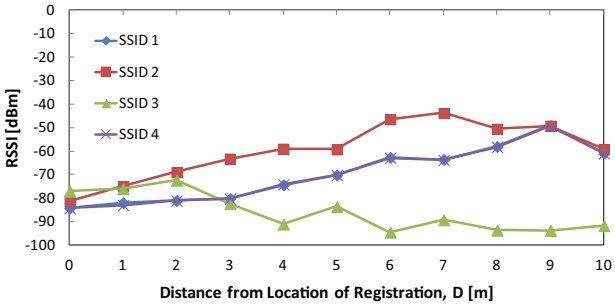

図 **9**　登録地点からの距離と RSSI の関係

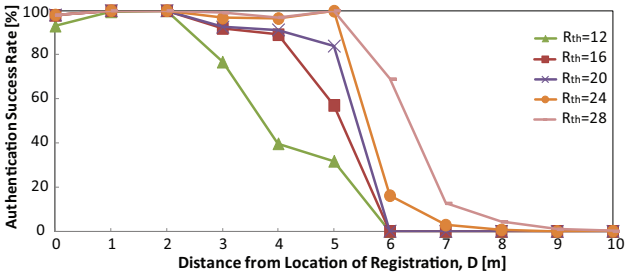

図 **10**　各 R_{th} における登録地点からの距離と認証成功率の関係

で認証成功率が約 20%にまで減少するが，認証成功率が 0%となるのは $P_{th} = 100$ なら登録地点から 8m 離れた地点，$P_{th} = 80$ なら登録地点から 10m 離れた地点である．また，$P_{th} = 60$ の場合は登録地点から 10m 離れた地点でも認証成功率は約 10%である．よって，RSSI を用いない場合は，RSSI を用いる場合と比較して認証範囲が限定されていないことがわかる．したがって，一致率を求める際に RSSI を用いること，つまり (1) 式が有効であると言える．

一致率を求める際に RSSI を用いることが有効である理由を示すために，図 **9** に登録地点からの距離に対する各 SSID の RSSI の関係を示す．この評価では，登録地点から Dm 間隔で離れた地点において，SSID およびその RSSI を 1 秒間隔で 5,000 回を取得し，各 SSID に対応する RSSI の平均値を求める．なお，図 9 に載せる SSID は登録地点から 10m 離れた地点まで検出され続ける SSID である．図 9 において，距離が登録地点から移動することにより RSSI が変化する．RSSI が大きくなるのはアクセスポイント (AP) に近づくときであり，RSSI が小さくなるのは AP から遠ざかるときである．例えば図 9 の SSID2 では，登録地点から 7m 離れた地点に近づくにつれて RSSI が大きくなり，7m 地点から 10m 地点に近づくにつれて RSSI が小さくなる．このことから SSID2 の AP は登録地点から約 7m 離れた地点に存在することが分かる．以上より，AP からの距離によって RSSI の値が変化することが分かる．よって，SmartLocAuth において RSSI を使うことは有効であると考えられる．

続いて，RSSI の閾値 R_{th} を評価する．図 **10** に，登録時間 $T_A = 900$，$P_{th} = 80$ としたときの，登録地点からの距離に対する認証成功率を R_{th} 毎に示す．評価方法は以下の通りである．

(1) 登録時間を $T_A = 900$ と設定
(2) 登録処理を実行
(3) R_{th} =12，16，20，24，28 と設定
(4) 各 R_{th} において 5,000 回の認証作業を実行
(5) 認証成功率を算出

以上の 5 ステップを 10 回繰り返し，各 R_{th} における認証成功率の平均値求める．まず，登録地点における認証成功

図 **11**　GPS のみ

図 **12**　GPS+WIFI

率を調べる．$R_{th} = 12$ のときは $R_{th} \geq 16$ のときよりも認証成功率が低い．認証に成功すべき場所では高い認証成功率であることが望ましいため，$R_{th} = 12$ は不適切である．次に，登録地点から 6m 離れた地点における認証成功率を調べる．$R_{th} \leq 20$ のときは認証成功率が 0%なのに対し，$R_{th} = 24$ のときの認証成功率は約 15%，$R_{th} = 28$ のときの認証成功率は約 70%である．登録地点以外で認証に成功することが望ましくない．つまり認証に成功する範囲は狭い方が望ましいので，$R_{th} \geq 24$ は不適切である．最後に $R_{th} = 20$ と $R_{th} = 16$ を比較すると，登録地点から 3m 離れた地点までは認証成功率が等しいが，登録地点から 4，5m 離れた地点では $R_{th} = 16$ のときの方が認証成功率が低い．したがって，$R_{th} = 16$ が R_{th} の設定値として最適である．

以上より，登録時間と登録地点における認証成功率はトレードオフ関係にあることが分かる．つまり，登録時間が長くなるにつれて登録地点における認証成功率が高くなり，登録時間が短くなるにつれて登録地点における認証成功率は低くなる．トレードオフ関係の中で，$P_{th} = 80$，$R_{th} = 16$ と設定するのが最適であることが分かる．

最後に GPS を用いる既存の認証方式において，認証者が屋内にいる場合にどの程度の誤差が生じるのかを調べる．図 **11** と図 **12** は iPhone4 の Google Maps を屋内で用いるときの誤差を示す．青い点は GPS が示す現在地，水色の円は誤差範囲，紫色のピンは実際の現在地である．図 11 は GPS のみを使用する場合であり，図 12 は Wi-Fi を ON にして GPS を使用する場合である．GPS のみを使用する

場合，実際の位置と GPS が示す位置は約 300m 以上の誤差があり，誤差範囲の半径は約 1,700m である．また GPS と Wi-Fi を用いる場合，実際の位置と GPS が示す位置は約 20m の誤差があり，誤差範囲は半径約 70m である．したがって，GPS を用いた認証方式を屋内で利用する場合，Wi-Fi を用いた場合であっても，認証が狭い範囲に限定できないことがわかる．

5. 結論

本論文では GPS を用いない場所ベースの認証方式として，空間依存情報を用いる認証システムである SmartLocAuth を提案した．空間依存情報として本論文では無線 LAN のアクセスポイントからの SSID を用い，登録時間と認証距離を評価した．評価の結果，登録時間と登録地点における認証成功率はトレードオフ関係にあることが分かった．トレードオフ関係の中で，一致率の閾値 $P_{th} = 80$，RSSI の閾値 $R_{th} = 16$ が SmartLocAuth を利用する上で最適であることが分かった．登録時の処理にかかる時間は約 4 分であった．認証に成功する範囲は登録地点から 5m 以内であることより，SmartLocAuth の認証方式としての有効性を確認した．

今後の課題は登録時間を短くすることである．また，本論文では環境依存情報として SSID のみを用いたが，それに加えて環境音や時間など様々な環境依存情報を組み合わせることにより，登録時間を短縮できると考えられる．

参考文献

[1] 石原進, 太田雅敏, 行方エリキ, 水野忠則, “端末自体の動きを用いた携帯端末向け個人認証,” 情報処理学会論文誌, 46(12), pp. 2997-3007, 2005.

[2] 山本匠, “利便性と安全性を兼ね備えた画像認証方式の実現,” 博士論文, 静岡大学, 2010 年.

[3] 湯浅秀一, 和田山豊, 藤井明宏, “実用化が進む生体認証技術,” 沖テクニカルレビュー 65, 第 207 号, Vol. 73, No. 3, Jul. 2006.

[4] A. Jain, L. Hong, and R. Bolle, “On-Line Fingerprint Verification,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314, 1997.

[5] Rachna Dhamija, Adrian Perrig, “Dj Vu: A User Study Using Images for Authentication,” *9th USENIX Security Symposium*, pp. 45-58, Aug. 2000.

[6] Hsein-Chou Liao and Po-Ching Lee. “A New Data Encryption Algorithm Based on the Location of Mobile Users,” *Information Technology Journal*, 7 (1), pp. 63-39, 2008.

[7] Hsein-Chou Liao and Po-Ching Lee. “A Novel Vision-based Location Authentication Approach in a Ubiquitous Camera Environment,” *Information Technology Journal*, 9 (8), pp. 1571-1584, 2010.

[8] 角田雅照, 伏田享平, 三井康平, 亀井靖高, 後藤慶多, 中村匡秀, 松本健一, “位置と速度を利用した移動体向け認証方式の提案,” MoMuC2006-55, pp. 11-16, November, 2006.

[9] 山口雄大, 大島直樹, 巽孝介, P. Ravindra De Silva, 岡田美智男, “NEXUS+:ネットワークを介した仮想クリーチャの共有による他者とのつながり感の創出,” インタラクション 2011, pp. 331-332, Mar. 2011.