

# ライフスタイル認証における IP アドレス情報の利用について

重田 信夫<sup>†1</sup> 佐治 信之<sup>†2</sup> 山口 利恵<sup>†1</sup>

**概要:** モバイルインターネットの普及やオンラインでの決済等のサービスで、スマートフォンの活用が進んでいる。利用者が様々なオンラインサービスを受けるために、個人認証として ID とパスワードや生体情報などが広く使われている。しかしながら、こういった方法ではユーザーにパスワードの適切な管理や追加の操作などの特別な負担を求めることがある。ライフスタイル認証は、個人の行動履歴情報を活用することにより、ユーザー利便性を損なわずに安全性の高い認証手法を提案してきた。2017 年に実施した実証実験において、5 万人規模のデータを集約した。実験では、スマートフォンに搭載したアプリで、端末情報、GPS 情報、Wi-Fi 情報を収集し解析を進めてきた。

これに加えて、今回は実証実験で収集した IP アドレスデータを、ライフスタイル認証で利用するための考察を行った。本稿ではこの結果を報告する。

**キーワード:** ライフスタイル認証, 位置情報, IP アドレス, スマートフォン, プライバシー保護

## Consideration on Utilization Method of Global IP Address Information in Lifestyle Authentication

NOBUO SHIGETA<sup>†1</sup> NOBUYUKI SAJI<sup>†2</sup> RIE Shigetomi YAMAGUCHI<sup>†1</sup>

**Abstract:** The use of smartphones is progressing with services such as spread of mobile Internet and online payment. ID, password, biometric information, etc. are widely used as individual authentication for users to receive various online services. However, with such a method, there are cases where a user is required to apply a special burden such as proper management of passwords and additional operations. Lifestyle authentication has proposed a highly secure authentication method without losing user convenience by utilizing personal action history information. In the field trial carried out in 2017, data of 50,000 people scale was aggregated. In the experiment, we have been collecting and analyzing terminal information, GPS information and Wi-Fi information with an application installed on a smartphone.

In addition to this, we examined the use of IP address data collected in the demonstration experiments for lifestyle authentication. This paper reports this result.

**Keywords:** Lifestyle Authentication, location information, IP Address, Smartphone, Privacy protection

### 1. はじめに

近年、スマートフォンの普及により EC サイトの利用が増えている。このようなサービスを利用するにあたり、個人認証手法として ID とパスワードが使われることが多い。この認証方式では、情報の漏洩に伴うなりすましの問題や、パスワードの適切な管理や利用の都度入力を求められるユーザービリティの問題がある。これらの欠点を補うため、行動履歴を用いたライフスタイル認証を提唱してきた。2017 年 1 月から約 3 ヶ月半の期間で実施した実証実験においては、スマートフォンの各種センサーを用いて位置情報や Wi-Fi 情報を収集するためのスマートフォンアプリ (MITHRA アプリと呼ぶ) を使い GPS 情報や Wi-Fi 情報を使った分析を進めてきた[1][2][3][4]。

スマートフォンの GPS 情報などで収集される位置情報を分析すると、その人の行動が分かり、その日々の変化か

らその人の固有の習慣性が見出される。この習慣性から人物を特定することが出来れば、それを認証として利用するというのがライフスタイル認証の発想である。

今回、GPS 情報に頼らなくても同様に行動の習慣性把握に IP アドレスが使えるか確認のために、先の実証実験のデータをあらためて分析することとした。

### 2. 行動分析として IP アドレスを利用する狙い

#### (1) 狙い

ライフスタイル認証では、行動履歴情報として、GPS 情報や Wi-Fi 情報などを中心に解析が進められた[5][6][7]。GPS 情報が利用可能であれば、高精度の位置を割り出すことができるため、行動履歴の蓄積や習慣性の解析に有益な情報が得られる。

当然のことながら、GPS 情報を使うためには、スマート

<sup>†1</sup> 東京大学大学院情報理工学研究科  
Graduate School of Information Science and Technology,  
The University of Tokyo

<sup>†2</sup> 筑波大学, 株式会社コードノミー, 株式会社インフォコーパス  
University of Tsukuba, Codenomy Inc., Infocorpus Inc.

フォン等の GPS 機能が必要である。また、利用者には精度の高い位置情報を収集することに対する心理的負担も懸念される。

そこで、IP アドレスを使用した行動履歴が使えるれば、スマートフォン以外の GPS 非搭載の IoT デバイスやセンサーを利用することも可能となり、ライフスタイル認証に向けた利用の幅が広がる可能性がある。

## (2) 利用する IP アドレスの性質

IP アドレスとは、インターネットに接続するすべての機器の接続のキーとなる情報であり、スマートフォン等は必ず IP アドレスを割り当てられている。

通常、キャリアや ISP から割り当てられるのは、グローバル IP アドレスと呼び、端末を全世界でユニークに識別することが可能である。

ところが、この IP アドレスを使って端末を識別しようとする場合、端末と IP アドレスの対応関係は一般に固定的ではない。つまり動的に変化する IP アドレスとなる。スマートフォンの場合、例えば地理的位置が変化した際などに IP アドレスも変化する例も知られている。

我々は、この IP アドレスが場所や接続環境によって変化する性質に着目して、その所有者の固有の行動パターン、つまり個人の習慣性を見つけるための一手段として利用したい。

このために我々は、IP アドレスとその利用者の位置情報がある程度関連する性質を利用する。具体的には IP アドレス利用者の国、都市、インターネットサービスプロバイダ (ISP) といった情報にマッピングするデータベースサービス[8]を利用した。

ただし、ある程度位置が特定できたとしても、モバイル端末では常に位置が変化することから、位置情報の精度が低くなることは当然想定される。

## 3. 検証内容

### 3.1 収集データ

まず 2017 年に実施した実証実験で収集したデータから、有効な IP アドレス情報がどれだけ得られるかを確認する。対象は、MITHRA アプリを搭載して情報を送信された、73 58 人分のデータとする。

含まれる IP アドレス情報は、Android スマートフォンの場合、5 分間隔で収集したものであり、iOS スマートフォンの場合、前回測位からの移動や基地局の変化をトリガーとして収集したもの。1 日分のデータを 1 件としてアップロードする[3]。今回、これらの収集された IP アドレス情報の精査と予備分析を行い、有効な情報がどれだけ収集できるかを確認する。

## 3.2 データのスクリーニング

### (1) キャリアが提供するグローバル IP アドレス

スマートフォン・キャリアが提供するモバイルデータ通信 (3G や 4G 等) 網を使ったインターネットアクセスでは、通常、動的なグローバル IP アドレスが割り当てられる。

この場合、タイミング等により割り当ての IP アドレスが変わるのが一般的である。変更のタイミングは、スマートフォンの電源を入れ直した場合や、キャリアが管理する基地局エリアを移行した場合などと言われている。

### (2) プライベート IP アドレスの除去

公衆 Wi-Fi 接続スポット、家庭内および企業内ネットワークなどでは、DHCP (Dynamic Host Configuration Protocol) により、プライベート IP アドレスが動的に割り当てられることが一般的である。プライベート IP アドレスは、インターネットアクセスする場合は、グローバル IP アドレスとのネットワークアドレスの変換 (NAT: Network Address Translation) を行うため、外部の IP アドレスとの対応関係は一定でなく、また同じプライベートアドレスが多くの環境 (ネットワークセグメント) で用いられることから、アドレスのユニーク性もない。このため行動履歴の分析に使用することはできないので、元データからプライベート IP アドレスを除去する前処理が必要となる。

### (3) リンクローカル IP アドレスの除去

リンクローカル IP アドレスは、DHCP サーバー機能を持たないネットワークセグメントにおいて、自動的に割り当てられる IP アドレスであり、ネットワークセグメントを超えてユニークであることが保証されない。このためプライベート IP アドレスと同様に元データからリンクローカル IP アドレスを除去する前処理が必要となる。

## 3.3 アドレスの管理者および位置情報の特定

- 上記の前処理で得られた IP アドレスから Whois 検索をし、アドレス管理者を知る。有効なアドレスレンジ、ホスト名等を知る。
- IP Geolocation 技術を活用して、IP アドレスの位置情報 (地域や都市名等) を得る。

ただし全国規模の ISP では位置特定の精度は低くなるのが一般的である。これは保有するアドレスプールをどのようにに内部利用しているかを公表していないためとみられる。例えば全国規模の ISP サービスでは、インターネットとの相互接続点 (POI: Point of interface) の位置が東京であれば、あるアドレス範囲はすべて東京と示されることがある。

一方、地域 ISP では、サービス提供エリアからある程度の地域性の確認も可能である。

## 4. 分析の実施

### (1) IP アドレスの抽出

元データには、IPアドレスのデータそのものが収集できていないケースもあった。これは被験者のスマートフォンの環境やアプリ起動状況などの使い方に依存するとみられる。これらのIPアドレスが含まれないデータを除外する。

### (2) プライベートアドレスの除去

DHCP (Dynamic Host Configuration Protocol) により割り当てられる以下のプライベート IP アドレスを除去する。

【除外アドレス】

10.0.0.0～10.255.255.255

172.16.0.0～172.31.255.255

192.168.0.0～192.168.255.255

### (3) リンクローカルアドレスの除去

APIPA (Automatic Private IP Addressing: IP アドレス自己割り当て) による以下のリンクローカルアドレスを除去する。

【除外アドレス】

169.254.0.0～169.254.255.255

### (4) 有効でないグローバル IP アドレスの除去

Whois 検索に登録がない、または何らかの理由で IPlook up ができないものを除去する。

ここまでの処理(1)～(4)の結果、有効なグローバル IP アドレスを含む 105 人分の情報 (全体の 1.427%) が得られた。

### (5) 位置情報への変換

IP アドレスから位置情報を得る。商用サービスとして位置情報を売る会社もあるが、ここでは無料で利用できる Maxmind の GeoIP サービス (IP アドレスから地理情報を確認することができるサービス) [8]を活用した。

## 5. 考察

### (1) 有効なグローバル IP アドレスが得られたケースが少ない理由

理由として DHCP の利用が多い (プライベート IP アドレスが多い) ことが挙げられる。(NAT 配下では外部のインターネット側アドレスを収集していない)

### (2) グローバル IP アドレスが得られた場合の課題

グローバル IP アドレスは主にキャリア回線からのものであり、キャリアや ISP は、アドレスの利用方法に関しては情報公開がない。一般的に言われていることでは、アドレスプールから、地域ごとや負荷バランスを考慮して割り当てる等が行われるため、全国規模でアドレス再配

置も頻繁にあると見られる。つまり位置情報との関連においては、地域との相関性が低く出る傾向がある。

### (3) IP アドレスから分かる位置情報

大雑把な場所 (都市名レベル) まで得られる。参考として、市販の有料サービスとしての位置情報提供では独自の情報収集により精度を高め、随時情報をアップデートすることで位置信頼性の確保を図っているが確実性は低い。(例 位置に関して、半径 25km 程度の円範囲で示す等)

### (4) 位置の精度について

参考とした Maxmind の GeoIP サービス[8]では、位置精度を公開している。独自の収集情報や複数の情報との組み合わせにより位置精度を確保していると考えられる。

表 1 日本：半径 25km 圏内での位置解決について

サービス名	正しく解決	誤った解決	未解決
GeoLite2 City	45%	43%	12%
GeoIP2 City	52%	34%	15%
GeoIP2 Precision City サービス	52%	34%	15%

今回参考とした、GeoLite2 City サービスの精度[9]は、25 km 圏内にいない確率 (誤る確率) も 43% と相当高い。因みに範囲 100km 圏内では以下となっている[9]。

表 2 日本：半径 100km 圏内での位置解決について

サービス名	正しく解決	誤った解決	未解決
GeoLite2 City	66%	22%	12%
GeoIP2 City	70%	15%	15%
GeoIP2 Precision City サービス	70%	15%	15%

データの信頼性、誤りに基づく影響を考えると、行動パターンの特定につながる情報は単独では得られにくいと考えられる。

## 6. 分析で得られたデータの傾向について

我々の目的は、IP アドレスから正確な位置を特定することではなく行動習慣性の確認の一要素として IP アドレスの利用を考察してきた。

絶対位置の精度よりも、アドレス変化の特徴を考察した結果は次の通りの傾向がみられた。(表 3 参照)

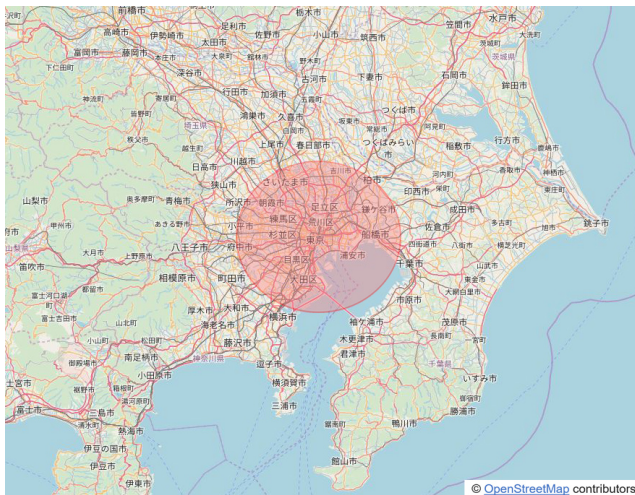
表 3 アドレスから得た位置情報の特徴

ケース分類	内容	件数	比率
A) 1 拠点型	存在拠点がほぼ一か所に絞られるもの	46	43.8%
B) 2 拠点型	存在拠点が二か所に分かれるもの (例えば、居住地と職場等生活拠点が2か所で、その間の移動が推定される)	8	7.6%
C) 県内型	ほぼ県内に位置が集中するもの	2	1.9%
D) 圏域型	関東圏、関西圏など、人口集中エリアにほぼ重なるもの	7	6.7%
E) 広域分散型	上記よりも広域に分散するもの。行動範囲が広い人のデータと見ることができ、その比率が高いことと、位置に飛び地が生じる場合があることから、実際の移動があったのか、誤情報が含まれるのか、判断は難しい。	29	27.6%
F) 海外型	海外の場所を含むもの	13	12.4%
	合計	105	

其他的なデータ例を図示する。

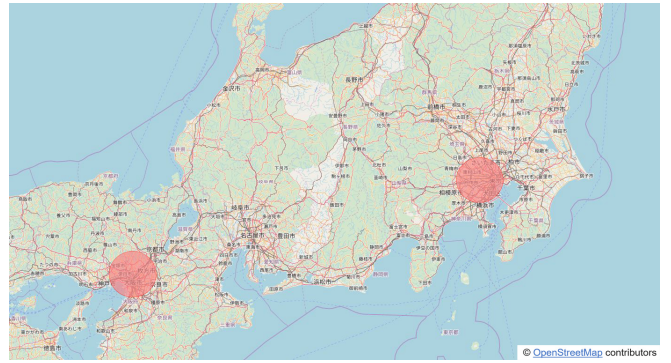
- ケース A の一か所を拠点とするとみられる位置情報の例を示す (図 1 参照)。
- ケース B の二か所を拠点とするとみられる位置情報の例を示す (図 2 参照)。
- ケース D の主に関東圏一帯を拠点とするとみられる位置情報の例を示す (図 3 参照)。
- ケース E の広域の活動拠点とするとみられる位置情報の例を示す (図 4, 図 5 参照)

図 1 A) 1 拠点型の事例



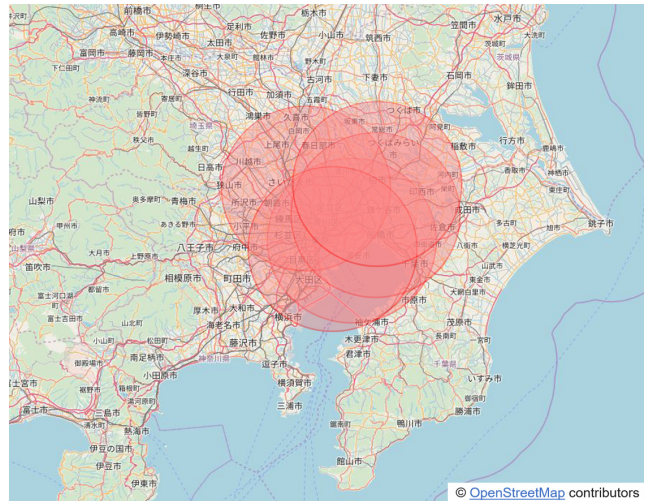
拠点が 1 箇所に限られるもの。データ数が十分にあれば位置情報の信頼性はあるとみられる。このケースの場合は東京大学で使用されているアドレスが含まれるため、位置はほぼ正確であることが確認できた。

図 2 B) 2 拠点型の事例



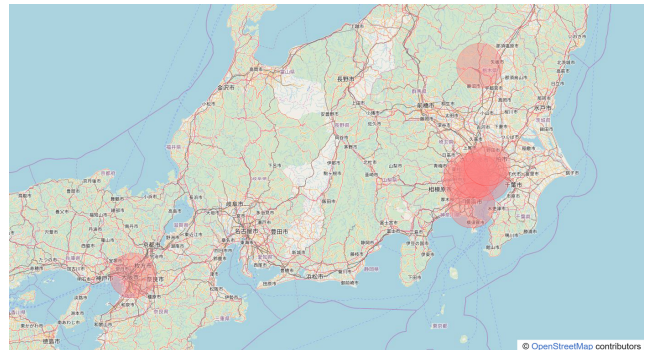
拠点が 2 箇所に限られるもの。アドレスから得た位置情報からは 2 つの拠点の位置情報が複数存在しており、両方の場所に関連することが想定される。

図 3 D) 圏域型の事例



位置のブレはあるが、ほぼ関東中心部 (東京・千葉・神奈川・埼玉) に限定して分布する。生活圏がここにあることは容易に推定できるが、個々人の分解能は低い。同様の事例では、ほぼ円が重なり合う。

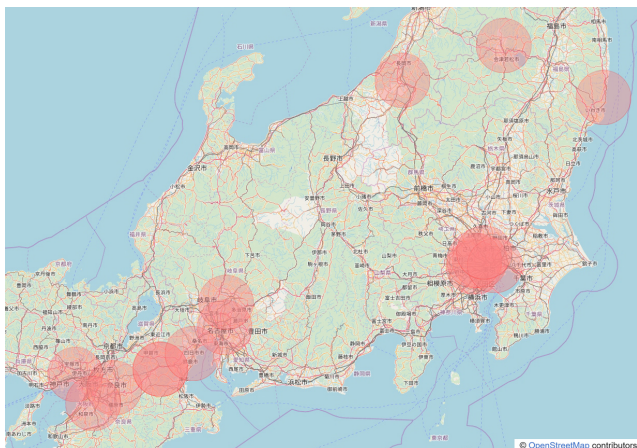
図 4 E) 広域分散型の事例 1



関東圏を中心に活動しているが、離れたエリアにも移動した可能性がある。実際に広域での行動実績があるのか、アドレスからの位置精度のゆらぎによるノイズかは、この情報からだけでは確定できない。



図 5 E) 広域分散型の事例 2



これも関東圏を中心に活動しているが、関西圏でも広い動きが見える。ノイズよりも実際の行動履歴が表れていると推定される。

## 7. まとめ

IP アドレスから正確な位置情報を得ることが我々の目的でないが、IP アドレスの変化から行動をとらえ、ライフスタイル認証に使えるようにするためには、実用的な位置情報の精度や、行動の習慣性の確認が必要であろう。

この意味では、現状は単独で IP アドレスデータを使用することは難しいと思われる。

今後、他の要素との組合せなどで新たな利用法を検討する必要がある。

## 参考文献

- [1] 鈴木宏哉, 小林良輔, 佐治信之, 山口利恵: ライフスタイル認証実証実験-MITHRA プロジェクト-, SCIS2017 暗号と情報セキュリティシンポジウム, No. 4D2-1(2017).
- [2] 鈴木宏哉, 小林良輔, 佐治信之, 山口利恵: ライフスタイル認証実証実験レポート-MITHRA データセット-, マルチメディア、分散、協調とモバイル(DICOMO2017)シンポジウム, No. 1H-2(2017).
- [3] 鈴木宏哉, 小林良輔, 山口利恵: ライフスタイル認証モデルの提案とその評価に向けた実証実験, 日本ソフトウェア科学会第 34 回大会[一般 11-3-L](2017).
- [4] 小林良輔, 佐治信之, 山口利恵: ライフスタイル認証の活用事例とその検証: 低リスクシナリオ, コンピュータセキュリティシンポジウム 2017 論文集, 2017
- [5] 鈴木宏哉, 山口利恵: 倫理審査, 同意取得, アプリ審査の壁を越えて…ライフスタイル認証実証実験の履歴収集に関して, コンピュータセキュリティシンポジウム 2017 論文集, Vol.2017, No.2.
- [6] 疋田敏朗, 小林良輔, 鈴木宏哉, 山口利恵: MITHRA プロジェクトの移動履歴データの解析, マルチメディア, 分散協調とモバイルシンポジウム 2017 論文集, 2017, 231-238
- [7] 小林良輔, 山口利恵: MITHRA データセットで Wi-Fi 個人認証その 1, マルチメディア, 分散協調とモバイルシンポジウム 2017 論文集, 2017, 239-244

- [8] “GeoIP データベース&サービス: 業界をリードする IP 情報収集” <https://www.maxmind.com/ja/geoip2-services-and-databases>, (参照 2017-08-01).
- [9] “GeoIP2 City 精度” <https://www.maxmind.com/ja/geoip2-city-accuracy-comparison>, (参照 2017-08-15).