東海大学大学院 2012 年度 修士論文

Bluetooth のスキャニングからのロケーション プライバシ侵害のリスクについて

On the risk of location privacy violation via Bluetooth scanning

指導教員　菊池 浩明 教授

東海大学大学院工学研究科情報理工学専攻

1 BDRM033 横溝 健

目次

第1章 はじめに

1.1. 背景

近年，Bluetooth を利用した近距離無線通信が盛んに行われるようになってきた．これは Bluetooth を内蔵した Android 携帯や iPhone といったスマートフォンが携帯電話市場でシェアを伸ばし年々出荷台数が増加傾向にあるためである．Bluetooth を用いることで携帯電話とワイヤレスヘッドセットなどの周辺デバイスをワイヤレスで接続することができ，Bluetooth 内蔵のデバイスを持ち歩くユーザは増加の傾向にある．

Bluetooth を用いた通信ではその仕様上，デバイスに割り当られた MAC アドレスが暗号化されることなく通信が行われている．この MAC アドレスは外部から容易に観測することができる．Bluetooth で行われる通信は近距離ものであり，ユーザは実際にデバイスを持ち歩いている可能性が高く，観測される MAC アドレスの移動履歴はユーザの移動履歴に近い．この MAC アドレスと位置情報，時刻などの情報とともに観測することでユーザのロケーションプライバシ上のリスクがある．折尾ら[1]は MAC アドレスとその他の情報を 5 台のロガーで収集し，ロケーションプライバシ上の脅威を示した．しかし，彼らの手法では特定のデバイスを追跡したため，一般にはどの程度の脅威があるか判断がつかない．

1.2. 目的

本稿では，Bluetooth MAC アドレスの 定点観測実験を行い，観測されるBluetooth 数と通過人数の相関を求めることで，Bluetoothのスキャニングからのロケーションプライバシ侵害のリスクを明らかにすること．

第2章 関連研究

2.1. 従来研究

ロケーションプライバシ考慮する研究には，暗号化・匿名化・秘匿化と様々な手法がある．本章では，それらの手法について述べ，本研究の位置づけを述べる．

2.1.1. アノニマイズドされた行動履歴に基づく行動パターン検索方式の提案[2]

川田らは,ユーザの行動履歴から,プライバシ保護を行いつつ検索精度の高い行動パターン検索を行うために,アノニマイズされたユーザの特徴を示す行動パターンを用いた検索方式を提案した．この方式では,実データである緯度・経度,時間,性別,年齢が含まれたユーザの個人情報から，アノニマイズされた行動パターンを生成する．この生成した行動パターンを検索するシステムの構築を行い,実際の行動履歴と比較しながらアノニマイズされた行動パターンの匿名性と検索精度について評価も行なわれている．

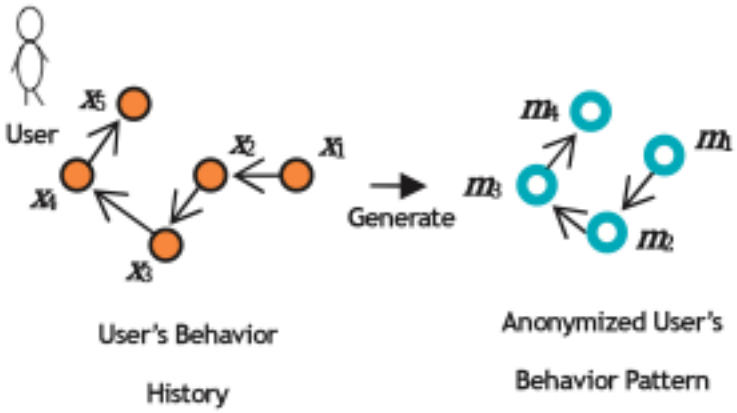

図2．1 アノニマイズド行動パターンの生成[2]

2.1.2. ロバストな突き合わせが可能な位置情報の秘匿化手法の提案[3]

牛田らは,秘匿化された地点情報を用いて,クラウド上で位置情報の連携サービスを行う連携サービス業者が各移動体の存在した位置を知ることなく,同時刻に同じ地点に存在した移動体同士を突合せる秘匿突合せ技術の提案した．この手法を用いることで,位置情報の測位の際の誤差に対応できる,ロバストな突合せが可能である．

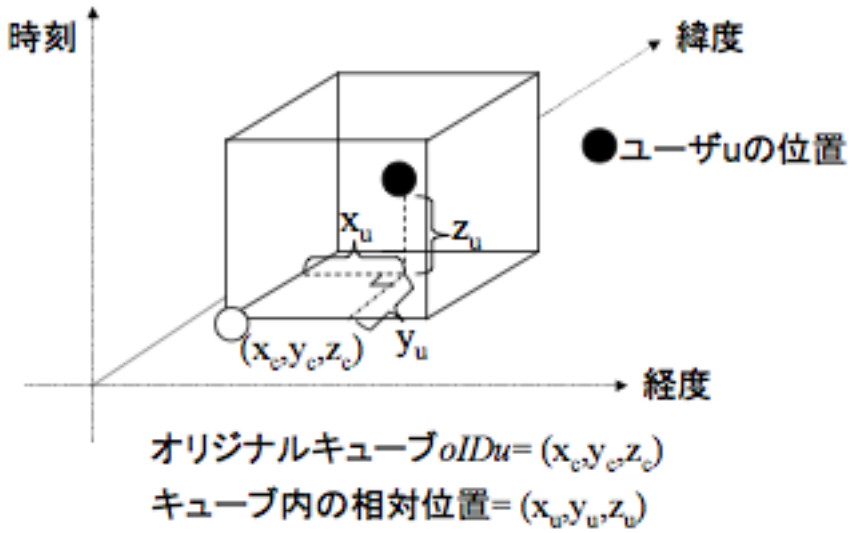

図2．2 オリジナルキューブIDとキューブ内の相対位置[3]

2.1.3.　粒度の動的変更による位置匿名性についての考察[4]

中西らは，公開した位置情報を悪用された場合の被害を抑えるために，公開する位置情報にユーザの望む匿名性を付加するサービスフレームワークを提案した．このフレームワークは，ユーザの望む程度の匿名性を満たすよう，公開する公開する位置情報の粒度をユーザが任意に指定できる．匿名性が高いほど位置情報の悪用は困難となり，ユーザ自身でプライバシを保護できる．

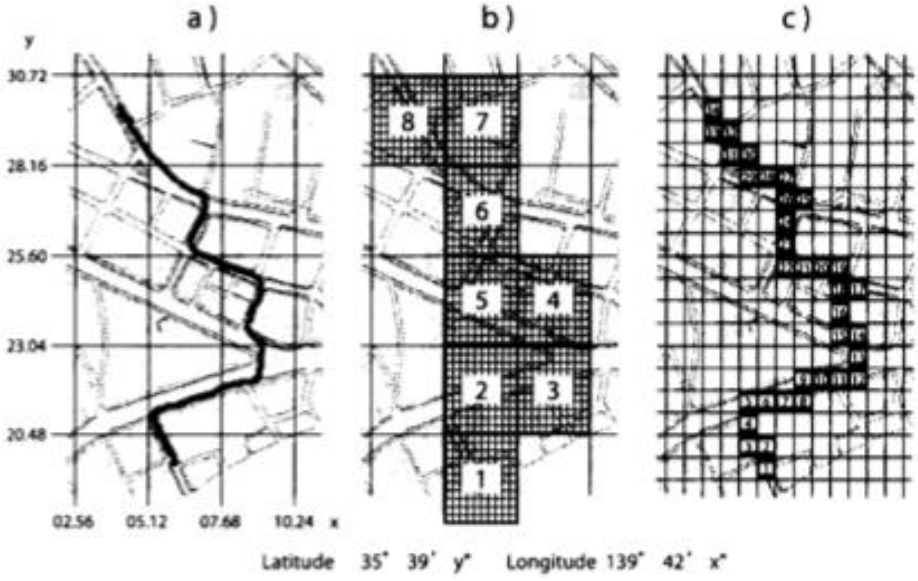

図 2．3 公開値情報例[4]

2.2. 本研究の位置づけ

先に紹介した 3 つの研究は，どれもユーザが自ら位置情報をサービス側に提供した場合に，位置情報の漏洩や悪意のあるサービス側によって起こりうるロケーションプライバシ侵害を防ぐものである．

本研究は，ユーザは自身の位置情報を発信しておらず，悪意のある第 3 者が勝手に観測した Bluetooth MAC アドレスと観測位置を突き合わせることで，ユーザのロケーションプライバシ侵害がどの程度起こりうるか調査するものである．

第3章 要素技術

本章では，Bluetooth の仕様と観測に用いた Bluetooth プロトコルスタックの BlueZ について解説する

3.1. Bluetooth

Bluetooth は，携帯電話やヘッドホンといった各種デバイスやマウス，キーボードなどシステムコンポーネントに接続に使用される近距離無線通信規格の 1 つである．規格の策定は Bluetooth Special Interset Group(Bluetooth SIG)が行なっている．

Bluetooth の名称はエリクソン社の研究者がつけたもので，デンマークとノルウェーを交渉で無血統一した Bluetooth（青歯王）の異名をもつデンマーク王ハーラル 1 世ゴームソンに由来している．

Bluetooth は 2．4GHz 帯を利用し，利用する周波数をランダム変える周波数ホッピングを行ないながら半径 10m-100m 内の Bluetooth 搭載機器と無線通信を行なう．IrDA と比較すると，Bluetooth は意識せずに常時接続したままでの使用状況に適しており物や壁などの障害を気にせず接続できる．しかし，IrDA は障害物があると接続できないため意識して接続する必要がある．

Bluetooth では，１つのマスタとなる端末と 1 つ以上のスレイブとなるワイヤレスネットワークを構築し通信を行なう．コンピュータネットワークに例えると，マスタはサーバ，スレイブはクライアントに相当する端末である．このマスタとスレイブから構成されるネットワークをピコネットとよび，同じピコネットに属する Bluetooth 端末同士は同期している状態である．図 3.1 にピコネットの構成例を示す．

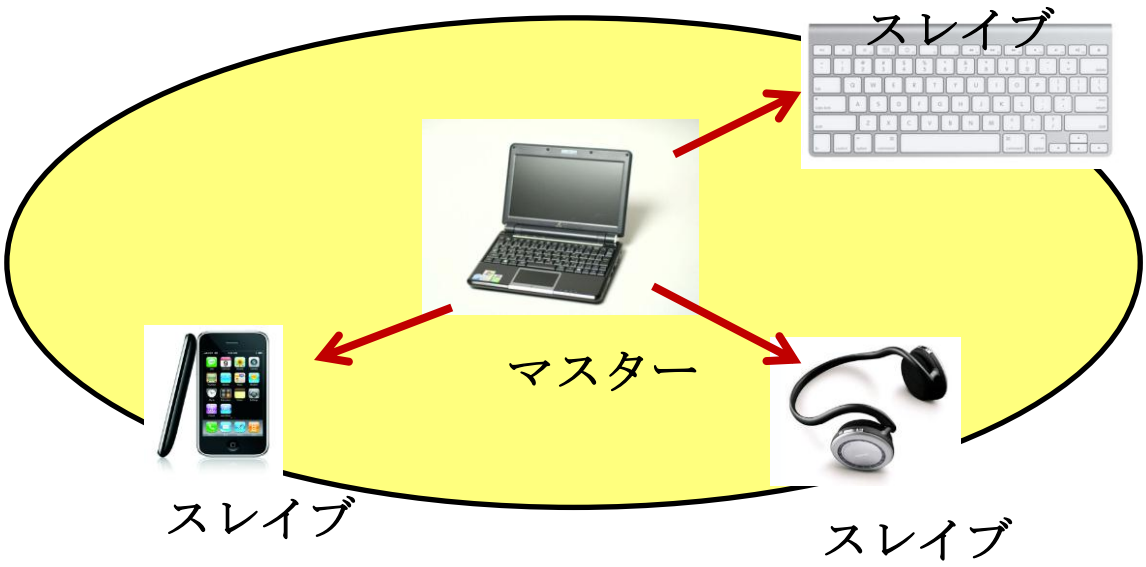

図 3．1　ピコネット構成

全ての Bluetooth デバイスにはそれぞれの固有の ID として，48 ビットの MAC アドレスが製造時に割り当てられる．Bluetooth デバイス同士で通信を行うときはこの MAC アドレスを交換してお互いに識別する．このため Bluetooth でバイス同士はお互いに認証し通信可能な状態になっていなくても MAC アドレスの交換は行われる．

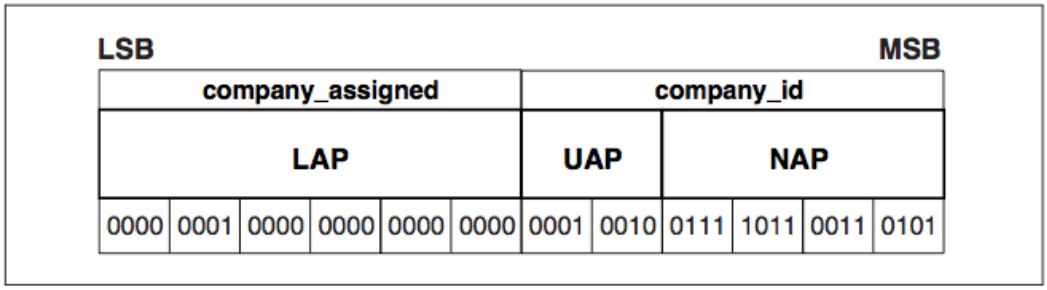

図 3．2 Bluetooth MAC アドレスのフォーマット[5]

3.2. BlueZ[5]

Linux 用のオープンソースによる Bluetooth プロトコルスタックである．デバイスドライバとしての Linux カーネルモジュールと，ソフトウェアから利用するためのライブラリを含んでいる．

3.2.1. hcitool

hcitool は，Bluetooth 接続を設定し，Bluetooth デバイスにいくつかの特殊なコマンドを送信するために使用される． 表 3.1 に hcitool のコマンド一覧を示す.

表 3. 1 コマンド一覧

コマンド名	実行内容
dev	ローカルデバイスを表示
inq	リモートデバイスの検出 検出された全てのデバイスのアドレス，クロックオフセット，デバイスクラスを表示
scan	リモートデバイスの検出 検出された全てのデバイスのアドレス，デバイス名を表示
name <bdaddr>	アドレスのリモートデバイス名前を表示
info <bdaddr>	アドレスのデバイス名，バージョン，サポートを表示
cmd <ogf><ocf>[parameters]	ローカルデバイスへの任意の HCI コマンドを送信
con	アクティブなベースバンドコネクションを表示
cc [--role=mis] [--pkt-type=<ptype>] <bdaddr>	アドレスのリモートデバイスとベースバンドコネクションを作る
dc <bdaddr>	アドレスのリモートデバイスとベースバンドコネクションを削除する
sr <bdaddr> <role>	リモートデバイスのマスタまたはスレイブのベースバンドコネクションの役割を切り替える
cpt <bdaddr> <packet types>	アドレスのデバイスのベースバンドコネクションのためのパケットの種類を切り替える
rssi <bdaddr>	アドレスからの受信信号強度を表示
lq <bdaddr>**tpl** <bdaddr> [type]	アドレスのデバイスに接続するための品質を表示
tpl	アドレスのデバイスに接続するための送信電力

	レベルを表示
afh <bdaddr>	アドレスのデバイスに接続するための AFH チャンネルマップを表示
lst <bdaddr> [value]	値がない場合，アドレスのデバイスに接続するためのリンク監視にタイムアウトを表示
auth <bdaddr>	アドレスのデバイスに接続するための要求の認証
enc <bdaddr> [encrypt enable]	アドレスのデバイスに接続するための暗号化を有効または無効
key <bdaddr>	アドレスのデバイスに接続するためのコネクションリンクキーの切り替え
clkoff <bdaddr>	アドレスのデバイスに接続するためのクロックオフセットを表示
clock <bdaddr> [which clock]	アドレスのデバイスに接続するための時間を読む

第4章 実験

本章では，Bluetooth によるプライバシ侵害の程度を明らかにする目的で行なった 3 つの実験を概説する．

1. 保有と使用状況のアンケート調査
2. 通過人数とデバイス検出率
3. 測定地による検出率の比較

4.1. 実験 1 保有と使用状況調査

4.1.1. 実験目的

どれだけのユーザが Bluetooth 対応端末を保有しているか，また探索可能であるか調査すること

4.1.2. 実験方法

アンケート調査を実施した．実施環境を表 4.1 に示す．アンケート内容を図 4.1 に示す．実験環境を表 4.2 に示す．

表 4.1 実験環境

期間	1/6-1/8
対象	学生 90 名
場所	東海大学学生食堂


Bluetoothの認知度や利用状況について調査をしています
問1
Bluetoothを知っていますか
知っている
知らない
問2
あなたは Bluetooth 対応機器を持っていますか
持っている
持っていない
分からない
問3
持っているBluetoothのスイッチが入っているか
ON
OFF
問4
持っている Bluetooth 対応機器はどのようなものですか（複数回答可）
携帯電話
ノートPC
マウス
キーボード
ハンズフリー
ワイヤレスヘッドホン/イヤホン
ワイヤレスヘッドセット
USBアダプタ
その他
問5
問3で「その他」を選択した方は,こちらにそのBluetooth対応機器を記入してください
過去の回答から選ぶ：

あるいは：

図 4．1 アンケート用紙

4.1.3. 実験結果

アンケート結果を以下に示す.

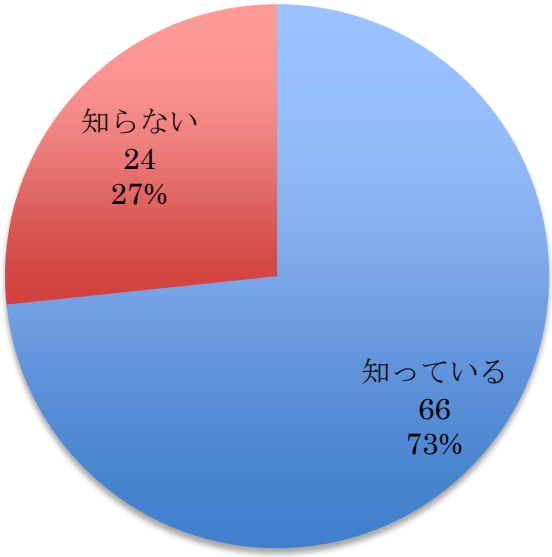

図 4. 2 問 1 Bluetooth の知っているか

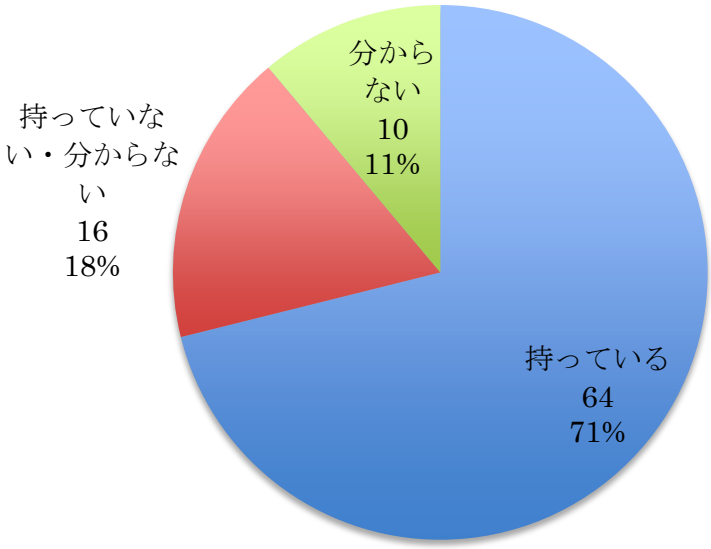

図 4. 3 問 2 Bluetooth 対応端末を持っているか

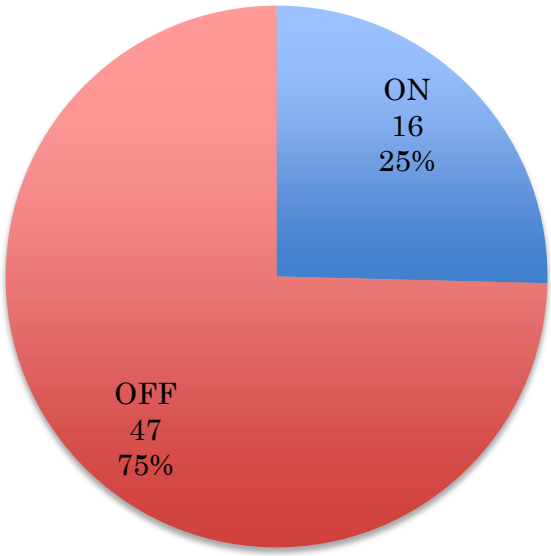

図 4. 4 問 3 持っている Bluetooth のスイッチが入っているか

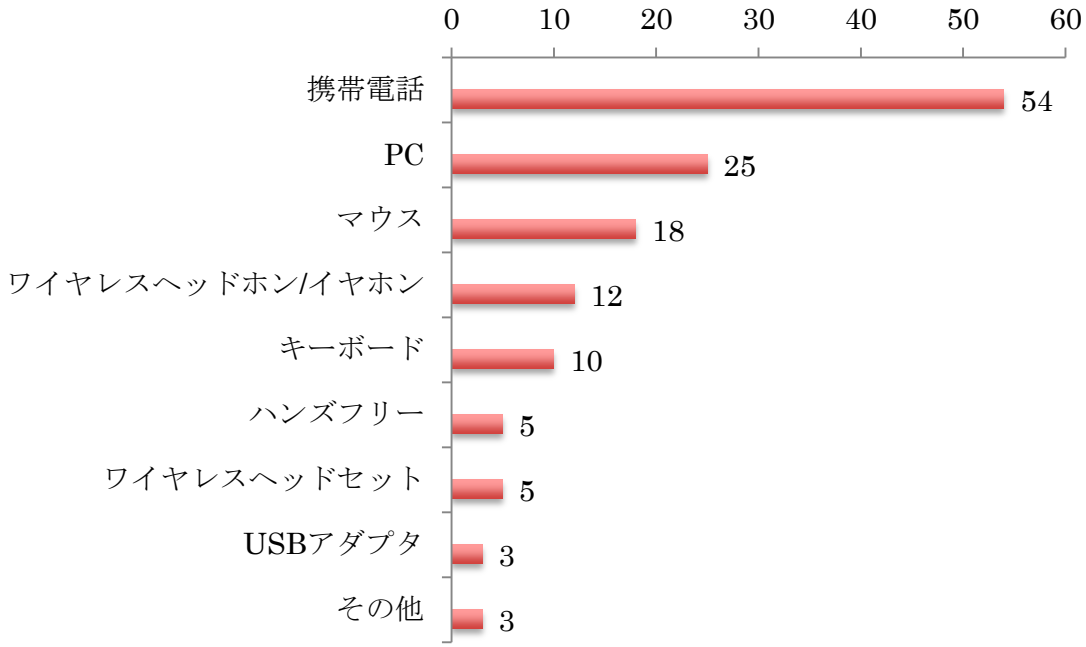

図 4. 5 問 4 持っている Bluetooth 対応端末

4.2. 実験 2 Bluetooth 数と人数の相関

4.2.1. 実験目的

Bluetooth の検出数と通過人数の相関を調査すること.

4.2.2. 実験方法

情報系の学生が在籍しするため Bluetooth を利用頻度が高いと思われる東海大学高輪校舎で, hcitool scan コマンドを用いて, 半径 10m 以内の Bluetooth MAC アドレスを検出する. 同時に通過人数をカウントする.

4.2.3. 実験環境

OS: Ubuntu 12. 4. 1LTS(VM)

Bluetooth: Bluetooth v4. 0

場所: 東海大学高輪校舎 1 階エントランス

日時: 1/15 8:30-18:00

4.2.4. 実験結果

総通過人数 942 人, 検出できた Bluetooth 数 1496 個でそのうちユニークなものは 15 個であった. 10 分ごとの通過人数における検出数を図 4. 2. 4. 1 に示す. 最小二乗法より検出率は 0. 0126 である. 近似曲線が緩やかに増加していることから通過人数に応じて観測できる Bluetooth 数が増えることが分かった.

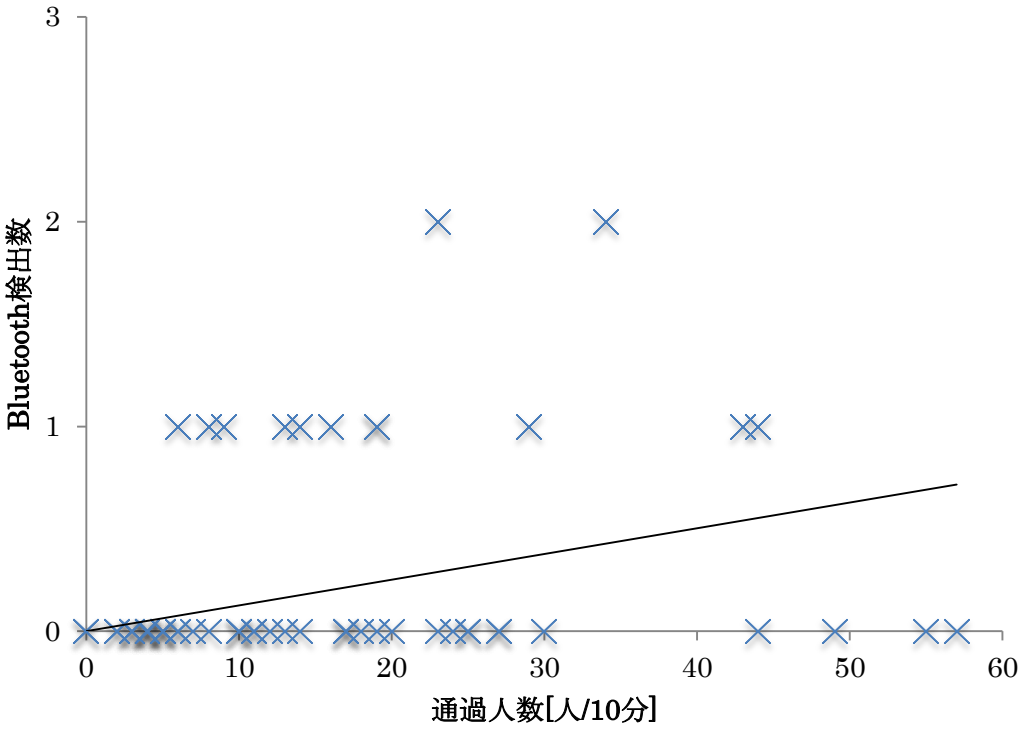

図 4. 6 10 分ごとの通過人数と Bluetooth 検出数

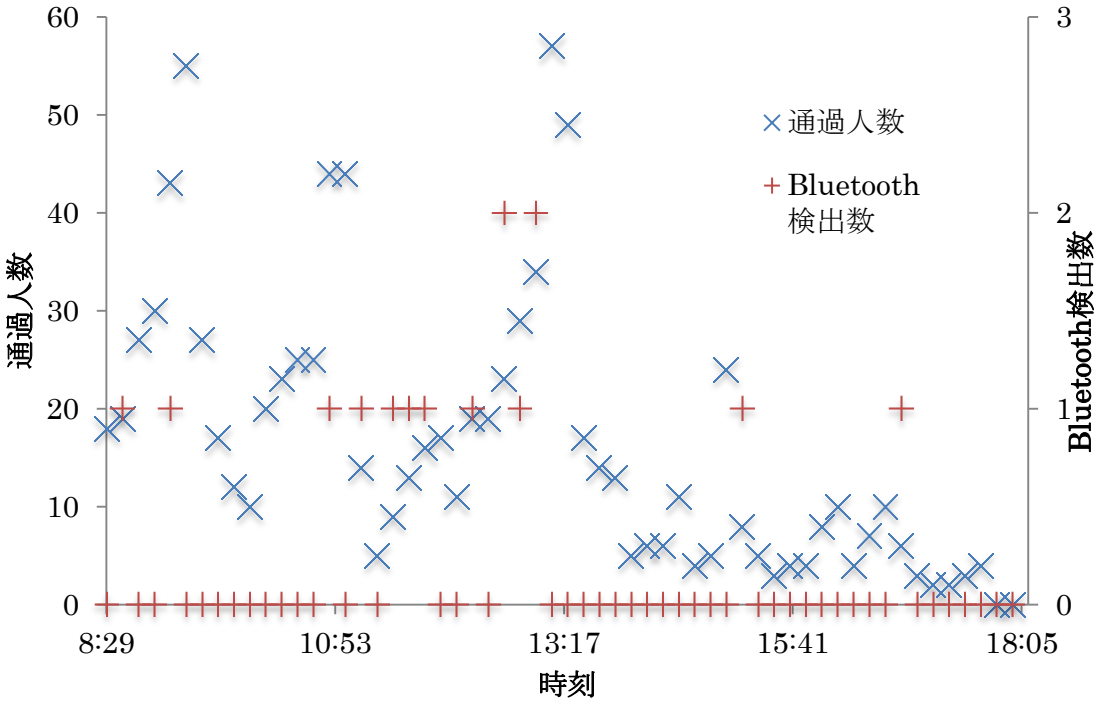

図 4. 7 10 分ごとの通過人数と Bluetooth 検出数

累計通過人数と累計 Bluetooth 検出数の変化を比較した.

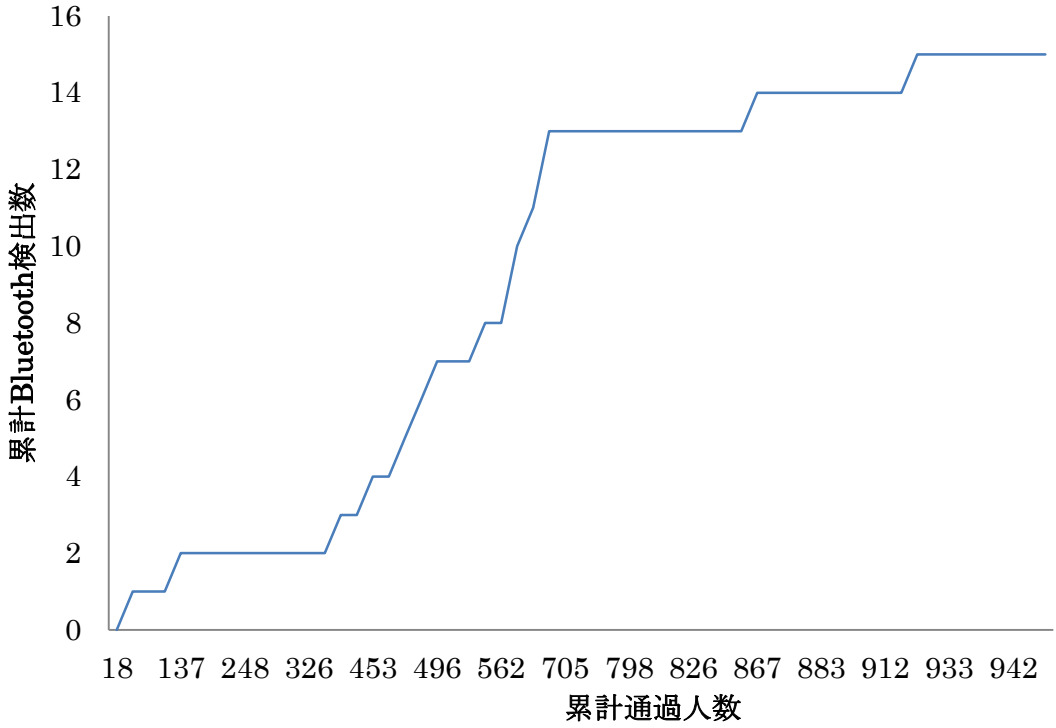

図 4. 8 累計通過人数と累計 Bluetooth 検出数

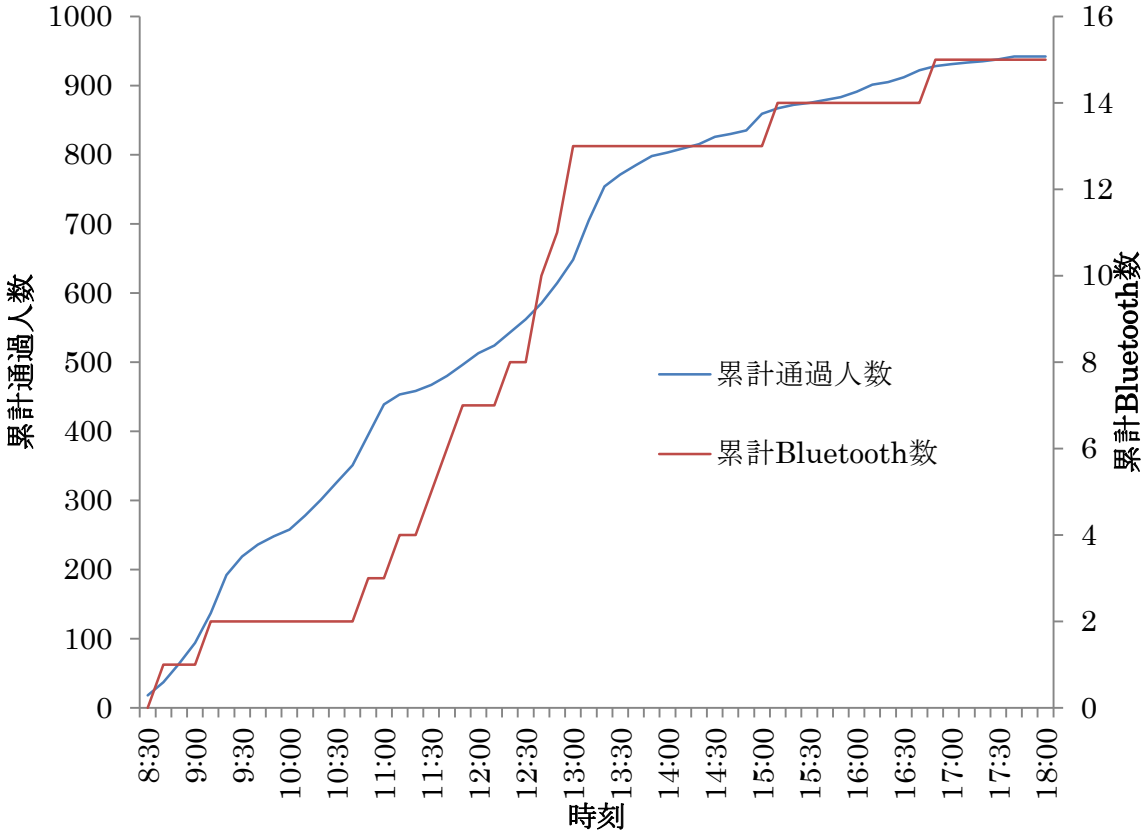

図 4. 9 10 分ごとの累計通過人数と累計 Bluetooth 数

4.3. 実験 3 場所による相関の違い

4.3.1. 実験目的

観測地点によって相関に違いがあるかを確かめる.

4.3.2. 実験方法

駅ビルが直結していることで家族連れが多いたまプラーザ駅と,通勤通学に利用される白金高輪駅で, 実験 2 と同様に hcitool scan コマンドを用いて, 半径 10m 以内の Bluetooth MAC アドレスを検出する. 同時に通過人数をカウントする.

4.3.3. 実験環境

OS: Ubuntu 12. 4. 1LTS(VM)

Bluetooth: Bluetooth v4. 0

場所: 東急田園都市線たまプラーザ駅

日時: 1/16 16:30-19:00

場所: 東京メトロ南北線白金高輪駅

日時: 1/17 9:15-10:05

4.3.4. 実験結果

たまプラーザ駅の累計通過人数は 4968 人でユニークな Bluetooth 検出数は 136 台であった. 検出率は 0. 0269 である. 白金高輪駅の累計通過人数は 3476 人でユニークな Bluetooth 検出数は 22 台であった. 検出率は 0. 0058 である.

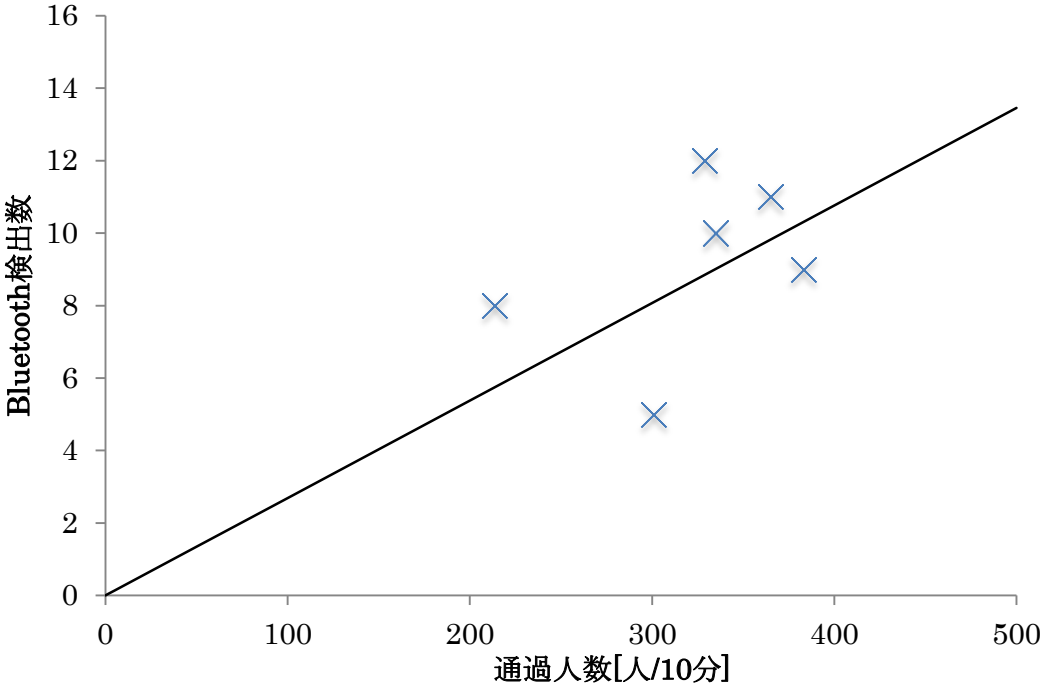

図 4．10 10 分ごとの通過人数と Bluetooth 検出数(たまプラーザ駅)

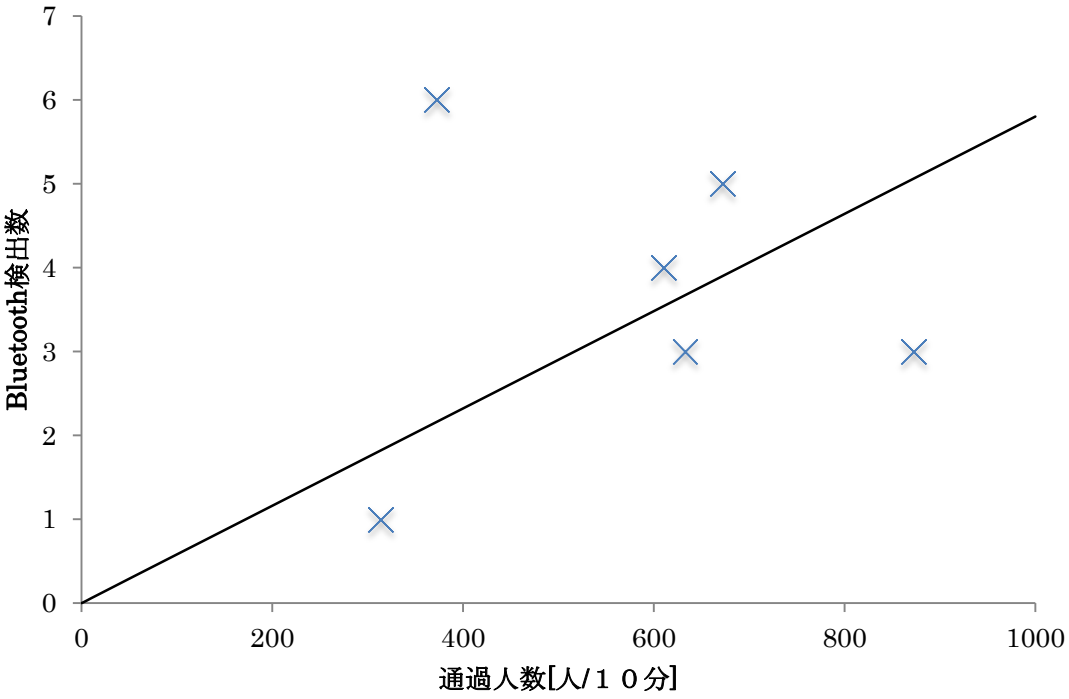

図 4．11 10 分ごとの通過人数と Bluetooth 検出数(白金高輪駅)

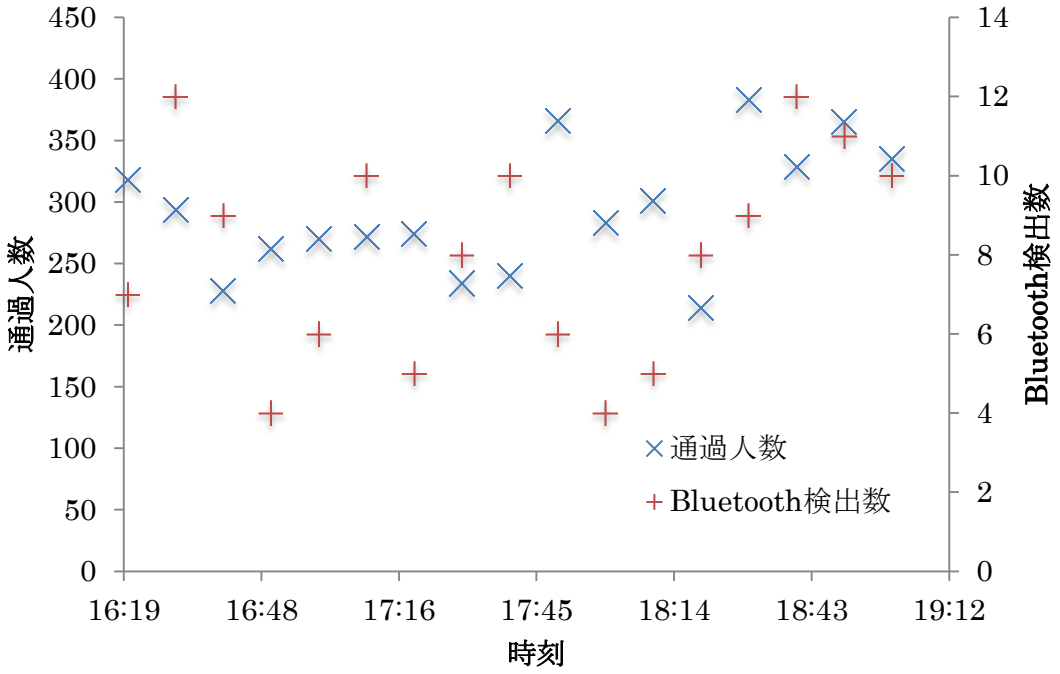

図 4. 12 10 分ごとの通過人数と Bluetooth 検出数(たまプラーザ駅)

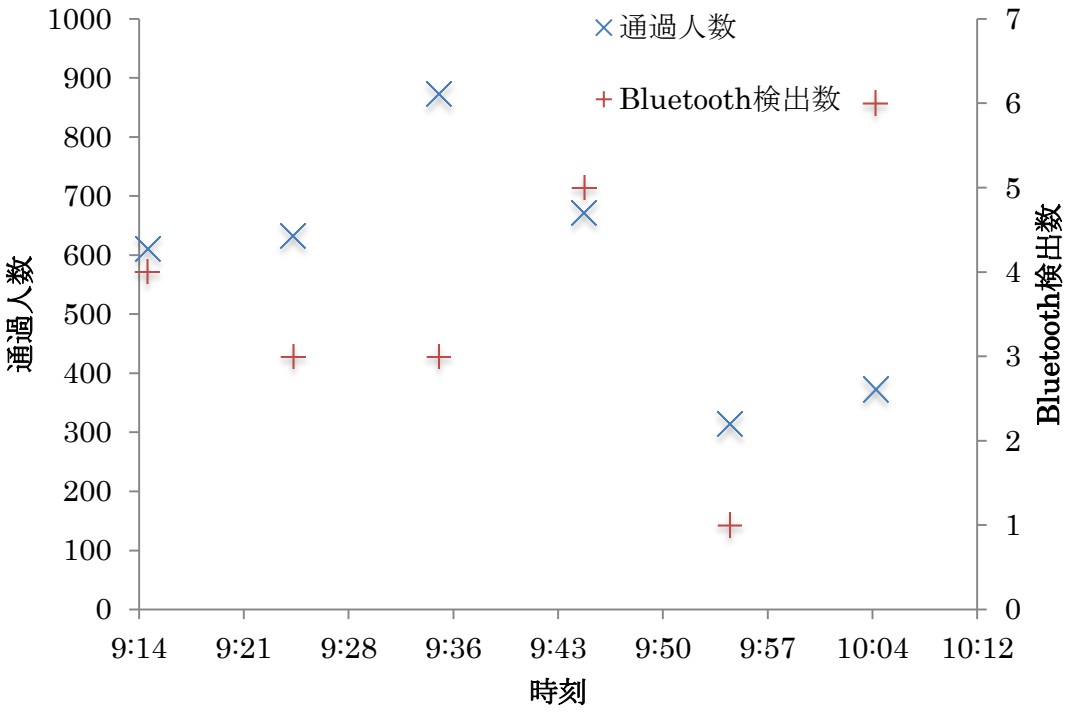

図 4. 13 10 分ごとの通過人数と Bluetooth 検出数(白金高輪駅)

累計通過人数と累計 Bluetooth 検出数の変化を比較した.

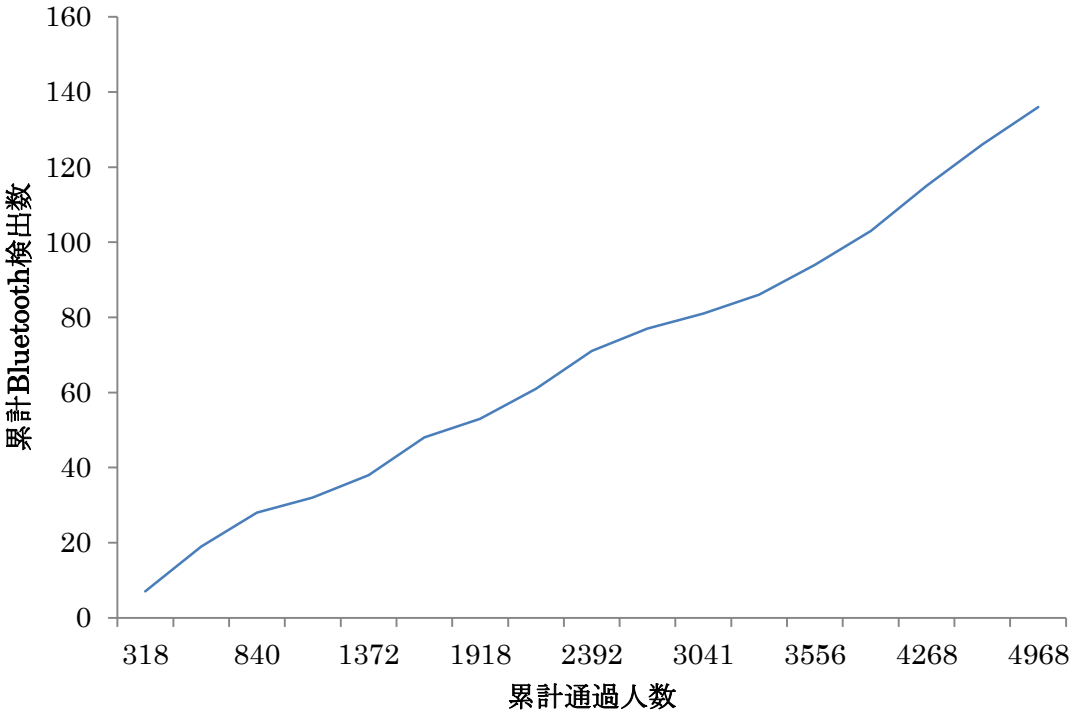

図 4. 14 累計通過人数と累計 Bluetooth 検出数(たまプラーザ駅)

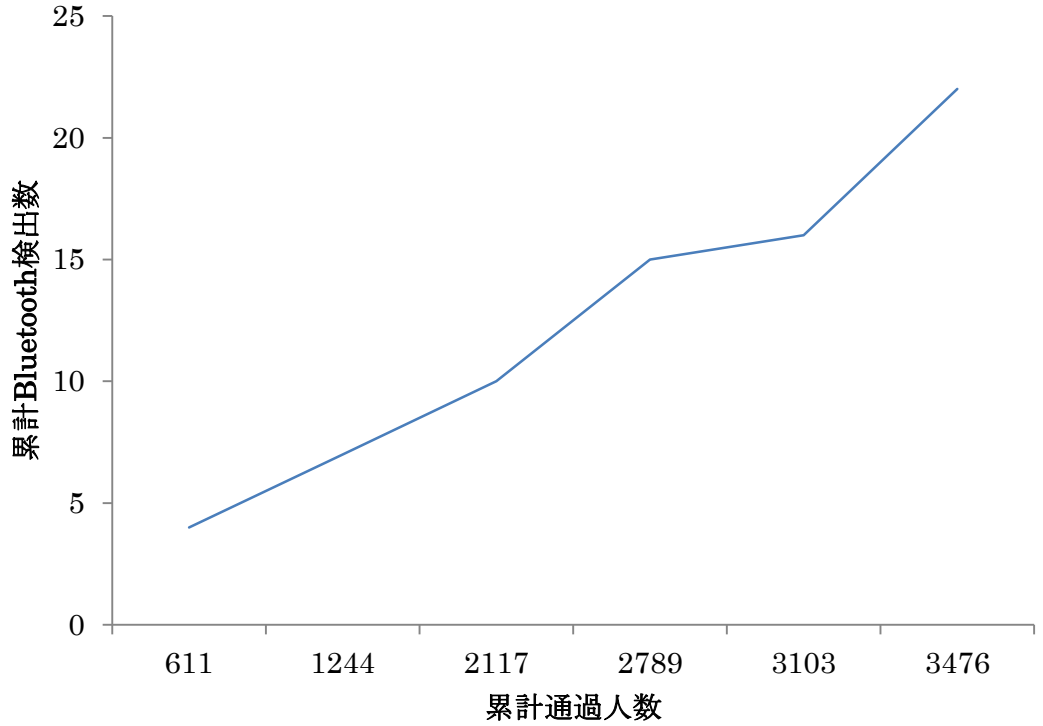

図 4. 15 累計通過人数と累計 Bluetooth 検出数(白金高輪駅)

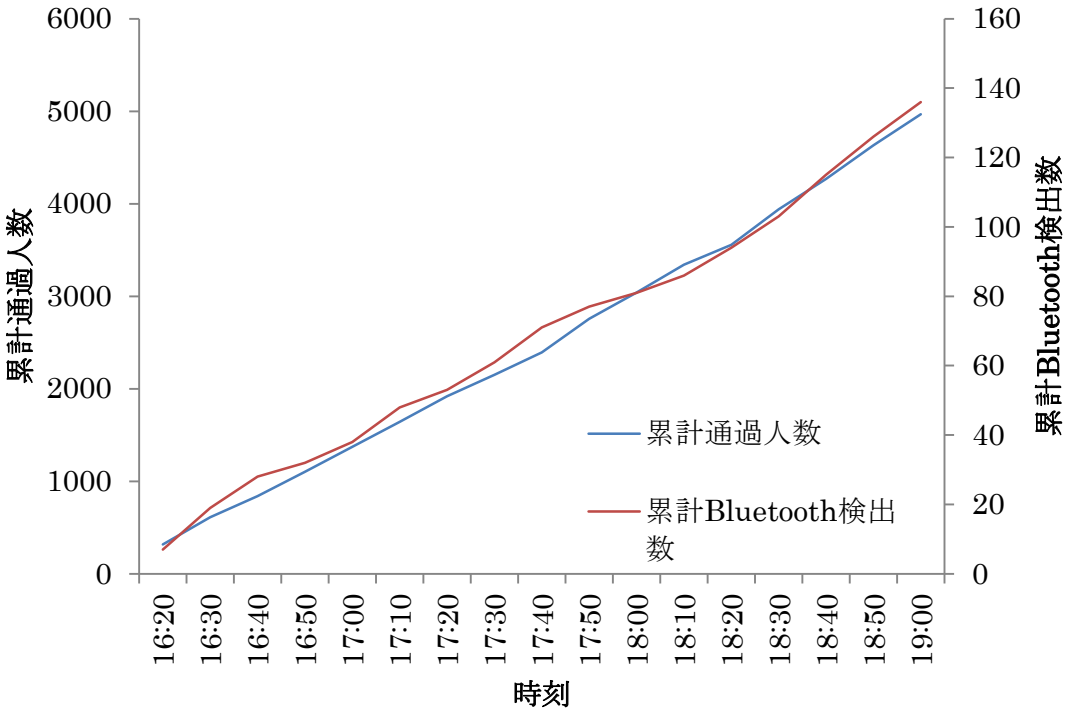

図 4. 16 10 分ごとの累計通過人数と累計 Bluetooth 数(たまプラーザ駅)

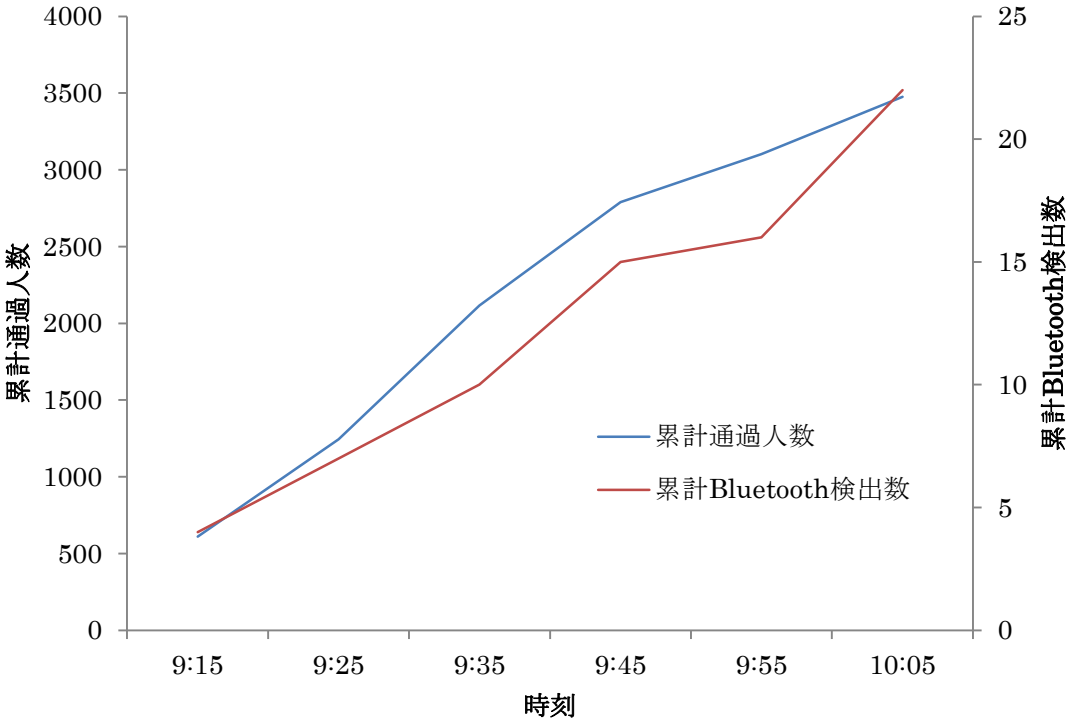

図 4. 17 10 分ごとの累計通過人数と累計 Bluetooth 数(白金高輪駅)

scan コマンドではMACアドレスだけでなく,デバイス名も取得できるためそこからメーカーを類推できる．図 4.18 はメーカーごとに Bluetooth 検出数を比較したものである．

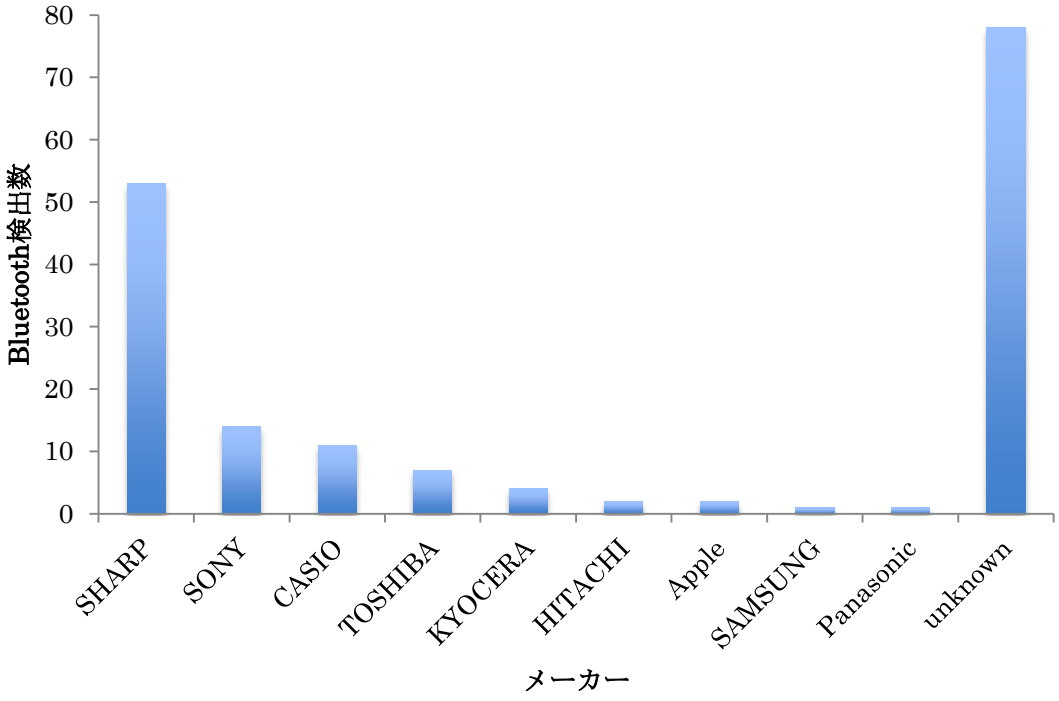

図 4．18　メーカー別 Bluetooth 検出数

表 4．2　携帯種別台数

ガラパゴス携帯	84 台
スマートフォン	11 台

第5章 考察

実験 1 の問 1，2 より Bluetooth の認知率，所持率ともに約 7 割で差がないことが分かった，問 3 より，スイッチを OFF にしている学生が多いのは，電池の消耗を抑えるためであると考えられる．また，25%の学生がスイッチを ON にしていることが分かるが，これは問 2 で Bluetooth 端末を持っていると答えた学生 64 名の 25%である．そのため，実際は 90 人の学生のうちだと 18%である．

実験 2 では実験 1 の問 3 より，Bluetooth の検出率は 18%であろうと予測されたが，実際に検出できた割合は 1．3%であった．これは，ヘッドホンやマウスなどの端末は，一度ペアリングを行なうとペアリングを切断するまで探索可能状態にならないためであると考えられる．

実験 3 では実験 2 と比較して，検出率が変化するため測定地によって相関が変化することが分かる．低くても 0．0058 の確率で Bluetooth を検出できるため，Bluetooth のスキャニングからのロケーションプライバシ侵害のリスクがあることが言える

図 4．18 で検出された Bluetooth 対応端末をメーカーごとに比較したが，SHARP が圧倒的に多かった．実験 1 問 3 でスイッチを OFF にしている理由は，スマートフォンの電池の消耗を抑えるためで，実際に検出された Bluetooth 対応端末のほとんどもガラパゴス携帯であった．ガラパゴス携帯ならスマートフォンと比べて電池が長く持つためである．そのため，SHARP が初期設定で Bluetooth のスイッチを ON に設定していても，ユーザが気にせずそのまま使っていること多いためだと考えられる．

勝手に検出されない対策としては Bluetooth を使わないときは常に OFF にし，使うときのみ ON にすることが最も簡単で有効である．また，最新の iOS ではペアリングしていない状態でホーム画面に戻ると，自動的に OFF になる仕様になっているため，OS のアップデートをし，常に最新の状態にしておくことも有効である．

第6章 おわりに

6.1. 結論

本稿では，Bluetooth MAC アドレスからロケーションプライバシ侵害のリスクがあるかを，検出される Bluetooth 数と通過人数の相関を明らかにすることで調査した．アンケートの結果，検出できる Bluetooth 数は通過人数のうち 18%と予測された．実験の結果，検出できる Bluetooth 数は通過人数の 1．3%であった．このことから，Bluetooth のスキャニングからのロケーションプライバシ侵害のリスクがあると考えられる．対策としては Bluetooth を使わないときは常に OFF また，iPhone なら OS を常に最新の状態にしておくことも有効である．

6.2. 今後の課題

今後は測定地や時間に連続性を持たせ，ユーザの行動履歴を観測できるかを調査する必要がある．

また，MAC アドレスから Bluetooth の検出も可能であることから，総当たり攻撃をしたときどの程度検出できるか調査する必要がある．

参考文献

[1] 折尾 彰吾, 上田 浩, 上原 哲太郎, 津田 侑, ”ワイヤレスデバイスのもたらすロケーションプライバシーに関する一考察”, コンピュータセキュリティシンポジウム(CSS2012), pp. 262-269, 2012.

[2] 川田 正明, 小川 克彦, ” アノニマイズされた行動履歴に基づく行動パターンの提案”, 情報処理学会論文誌 50(4), 1251-1261, 2009-04-15.

[3] 牛田 芽生恵, 伊藤 孝一, 小櫻 文彦, 福岡 俊之, 津田 宏, ”ロバストな突き合わせが可能な位置情報の秘匿化手法の提案”, 暗号と情報セキュリティシンポジウム(SCIS2012), 3D2-2, 2012.

[4] 中西 健一, 高汐 一紀, 徳田 英幸, ”粒度の動的変更による位置匿名性についての考察”, 情報処理学会論文誌 46(9), 2260-2268, 2005-09-15.

[5] Core Version4.0, Current Master TOC, Publication Data:30 June 2010.

[6] BlueZ, http://www. bluez. org/ (2012/12/12 参照).

[7] bluecove - Java library for Bluetooth - Google Project Hosting, http://code. google. com/p/bluecove/ (2012/12/14 参照).

[8] The Java Community Process(SM) Program - JSRs: Java Specification Requests - detail JSR# 82, http://jcp. org/en/jsr/detail?id=82.

謝辞

本論文を執筆するにあたり多くの方々から多大なる御指導と御援助を賜りました.

特に, 研究に関わらず私を導いて下さった東海大学情報通信学部通信ネットワーク工学科菊池浩明教授に最大の感謝を申し上げます.

また, 本研究を推進するにあたって, 度重なる御指導を頂いた東海大学情報理工学部情報科学科内田理准教授に多大なる感謝を申し上げます.

そして, 実験用のプログラムを作成してくれた東海大学情報通信学研究科情報通信学専攻大久保成晃氏に深く感謝致します. また, 実験に協力して下さった方々と, 二年間ともに学生生活を楽しんだ研究室の仲間に感謝申し上げます.

最後に, 大学院まで行かせていただき, 常に応援してくれた家族に感謝の意を表するとともに, 謝辞とさせて頂きます.

付録　A. Bluetooth の長期的収集

東海大学情報通信学研究科情報通信学専攻の大久保の作成したプログラムを用いて，Bluetooth による研究室内の入室者の収集を行なったので，ここに示す．

A.1 実験目的

研究室内で検出される Bluetooth の数から，学生の研究室の利用状況を調査すること．

A.2 要素技術

Java で Bluetooth を動かすためには bluecove[7]というライブラリのパスを通す必要がある．

A.2.1 bluecove

Java で Bluetooth を動かすには JSR 82: Java™ APIs for Bluetooth[8]という仕様がある．JSR 82 自体は Java で Bluetooth を動かす仕様だけを定義しているので，実際の JSR 82 の実装として bluecove を使用する．

A.3 実験方法

本実験では，Java を用いて Bluetooth の収集を行なった．研究室に設置した収集用の PC から収集した Mac アドレス，デバイス名，取得日時を研究室のサーバに送り，csv 形式にて出力．

A.4 収集期間

12/17-1/13

A.5 結果

Bluetooth の検出結果を以下に示す．

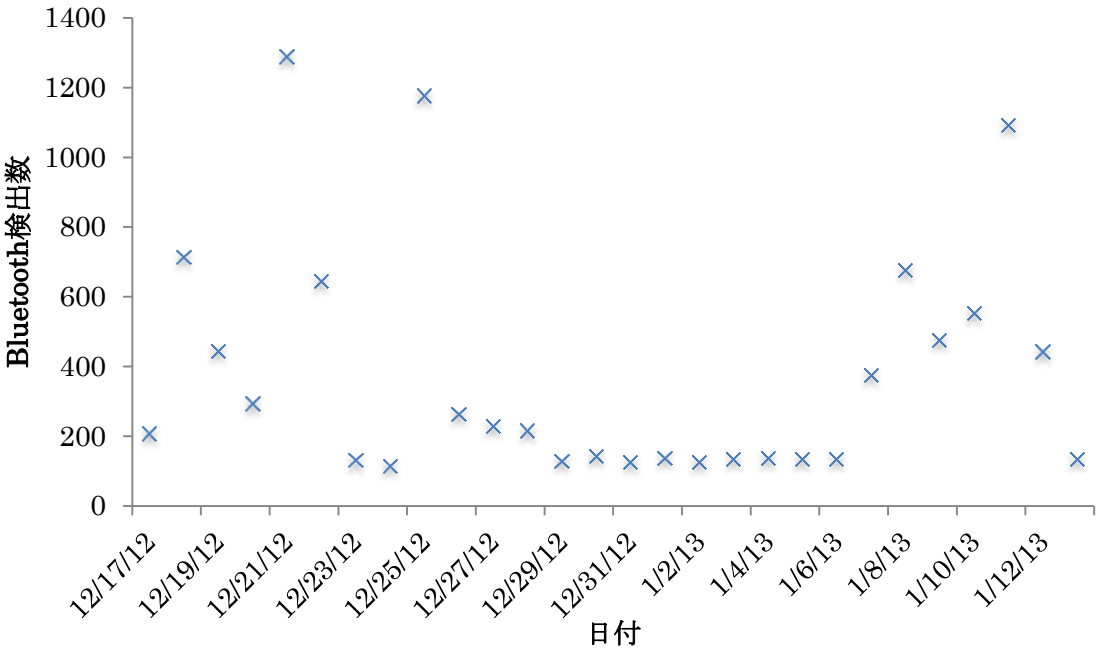

図 A.1　日別 Bluetooth 検出数

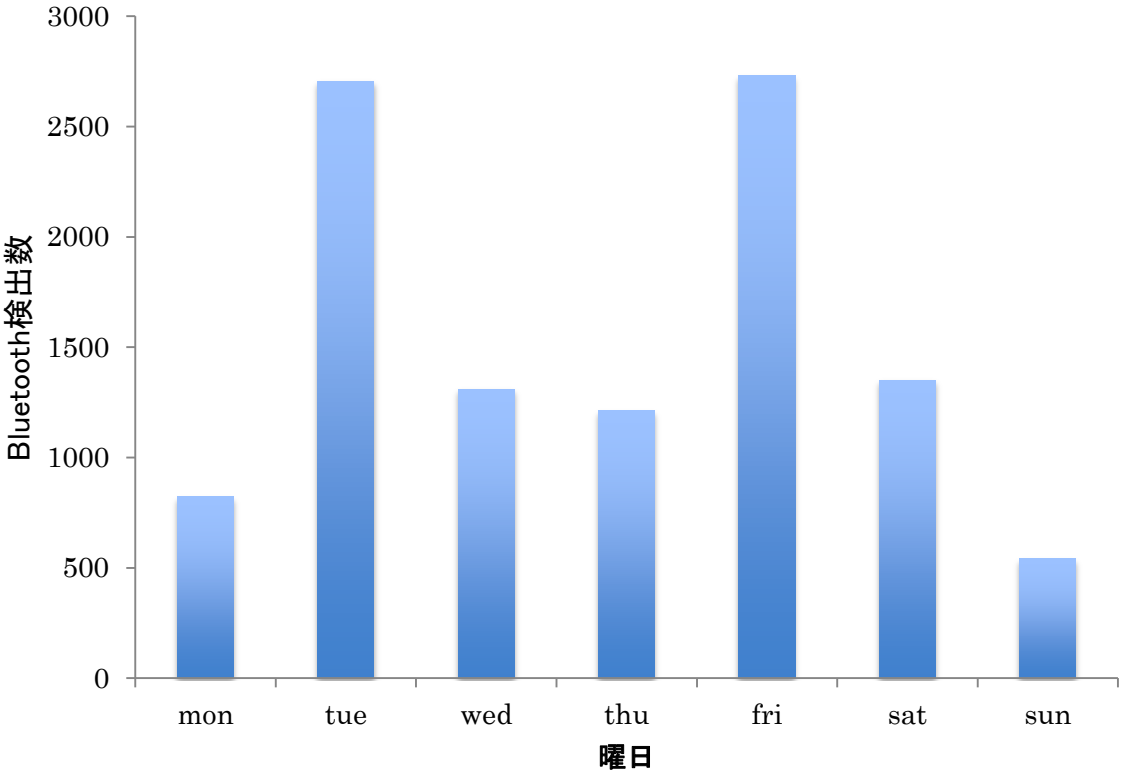

図 A.2　曜日別 Bluetooth 検出数

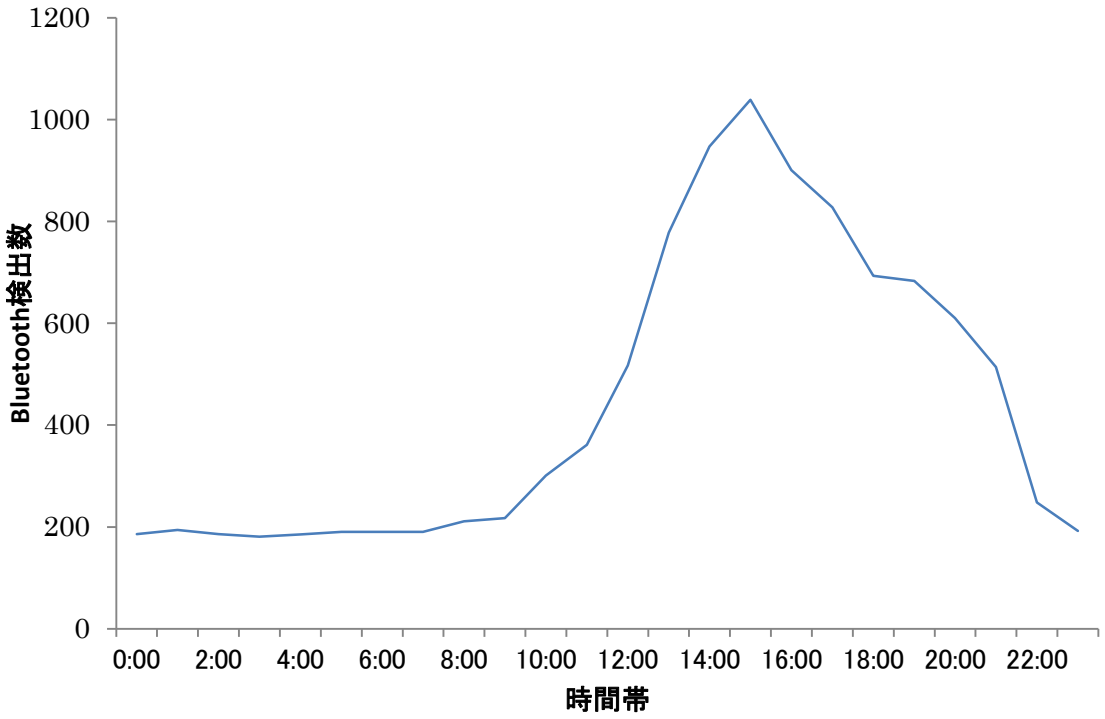

図 A.4　時間帯別 Bluetooth 検出数

A.6 考察

図 4．1，4．2 より火曜日と金曜日はゼミがあるため，学生が集まり Bluetooth の検出数が多くなっている．日曜日と月曜日の変化は少なく，連続して休む学生が多いと考えられる．

図 4．3 より，12 時から 13 時の 1 時限に掛けて学生が増えている様子が見える．また，17 時から 18 時と 20 時から 22 時帰宅のピークが発生していると考えられる．夜中も検出されているものはサーバ兼用で動かしている PC があるためである．

本実験の際は，研究室の PC の Bluetooth のスイッチも ON にしていたため，PC の起動時間も考慮すれば，利用頻度の高い PC，学生の好みの PC を調べることも可能であると考える．