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問題に関する一考察

折尾 彰吾† 上田 浩‡ 上原 哲太郎§ 津田 侑†

†京都大学 大学院情報学研究科
606-8501 京都市左京区吉田本町
{orio, tsuda}@ipe.media.kyoto-u.ac.jp

‡京都大学 学術情報メディアセンター
606-8501 京都市左京区吉田二本松町
uep@media.kyoto-u.ac.jp

§NPO 法人 情報セキュリティ研究所
646-0011 和歌山県田辺市新庄町 3353-9 Big-U 104 号
uehara@tetsutaro.jp

あらまし スマートフォンやオーディオプレーヤ，ヘッドセットなどに代表される，Wi-Fi や Bluetooth を用いてワイヤレス通信を行うことのできるデバイスを，多くの人が日常的に持ち歩いている．一方これらのワイヤレス通信ではその仕様上，デバイス固有に割り当てられた MAC アドレスが暗号化されることなくやりとりされており，これは外部から容易に観測することができる．この MAC アドレスを位置，時刻その他のデータと紐付けて収集することによって，ユーザのロケーションプライバシーが暴露されるおそれがある．本稿では，実際に MAC アドレスの収集実験を行った結果を述べるとともに，この脅威を低減・回避する手法について考察する．

A Study of Location Privacy Issues Brought Down by General Wireless Devices

Shogo ORIO† Hiroshi UEDA‡ Tetsutaro UEHARA§ Yu TSUDA†

†Graduate School of Informatics, Kyoto University
Yoshida Honmachi, Sakyo-ku, Kyoto 606-8501, JAPAN
{orio, tsuda}@ipe.media.kyoto-u.ac.jp

‡Academic Center of Computing and Media Studies, Kyoto University
Yoshida Nihonmatsu-cho, Sakyo-ku, Kyoto 606-8501, JAPAN
uep@media.kyoto-u.ac.jp

§The Research Institute of Information Security
#104, Big-U, 3353-9 Shinjo-cho, Tanabe-shi, Wakayama 646-0011, JAPAN
uehara@tetsutaro.jp

Abstract Many people are equipped with wireless devices which interact with each other through Wi-Fi or Bluetooth connection, as typified by smartphones, audio players or hands-free headsets. In these wireless connections, by specifications, these devices exchange their unique MAC addresses in the clear; these addresses can be observed without difficulty by third parties. This raises concerns that users' location privacy may be disclosed by gathering these MAC addresses correlate with other information: time, location, etc. In this paper, we show the actual result of gathering MAC addresses and discuss effective method for mitigation or avoidance of this privacy risk.

1 はじめに

1.1 ワイヤレスデバイスの普及

Android 端末や iPhone に代表されるスマートフォンは，携帯電話市場において急激にそのシェアを伸ばしている．国内では 2010 年ごろから本格化したスマートフォン市場であるが，その出荷台数は年々増加傾向にあり，その成長は今後さらに拡大していくと考えられている [4].

スマートフォンの利用においてはその自由度の高さから，ユーザが自分好みのアプリケーションをインストールしてカスタマイズすることが一般的である．例えば，スケジューラを導入して PDA のように使う，GPS と地図アプリケーションによって PND のように使うといったように，ユーザのライフスタイルに合わせて通話機能に限定されない様々な利用法が存在する．また Bluetooth[1] を利用することでワイヤレスヘッドセットなどの周辺デバイスを接続できることから，利用するユーザによってその構成は様々である．

通信回線についても，従来は携帯電話キャリアが提供する 3G 回線を端末毎に利用することが一般的であったが，スマートフォンやラップトップ PC 等のモバイル端末を複数所有するユーザやより高速な回線を望むユーザなどによって，モバイルルータと呼ばれる携帯型の無線アクセスポイントを利用し，手持ちのデバイスを Wi-Fi (ワイヤレス LAN; IEEE 802.11[2]) 接続して運用する例も見られるようになってきた．

このほか，オーディオプレーヤやカーナビゲーションシステムなどにおいても Wi-Fi，Bluetooth への対応が進み，デバイス操作やデータ更新などをワイヤレスで行えるものが増えている．このように従来のあらゆる携帯デバイスが Wi-Fi や Bluetooth によってワイヤレス化され，ますます多くのユーザがこのようなデバイスを持ち歩くようになっている．

1.2 プライバシーリスク

一方，このような携帯デバイスで Wi-Fi や Bluetooth を利用することはその仕様上，重大なプライバシーリスクを抱えている．具体的にはこれらのデバイスが有する，

- ユーザのライフスタイルに密着したデバイスの移動履歴は，一般にそのデバイスを所有するユーザの移動履歴に近似できる．
- Wi-Fi や Bluetooth による無線通信の際に用いられるデバイス固有の MAC アドレスが外部から容易に観測できる．

という 2 つの性質から，このアドレスを位置や時刻などの情報とともに観測・収集することでユーザの位置に関するプライバシー情報が暴露されるおそれがあるという問題である．

本稿ではこの問題を明らかにするため，ある地点で観測できる MAC アドレスをその位置情報等とともに収集する実験を行い，ユーザのプライバシー情報が暴露される危険性を明らかにする．また上記のような方法によって現実となるロケーションプライバシー上の脅威を回避・低減する手法について考察する．

1.3 本稿の構成

本稿は以下のように構成されている．第 2 章でロケーションプライバシーに関連する研究や事例を紹介し，第 3 章では実際に行ったアドレス収集実験とその詳細について述べる．実験により明らかとなるロケーションプライバシー上の脅威やその脅威を回避・低減する手法について第 4 章で考察し，第 5 章で結論を述べる．

2 ロケーションプライバシー問題

2.1 関連研究

Krumm は，ユーザの位置情報を利活用したサービスの広がりに関連して，ロケーションプライバシーの概念や位置情報の漏洩が引き起こす脅威とその対策に関して広く調査している [3].

測位の方法に関して，GPS や Cricket[1] のようにデバイス外部からの位置ビーコンをもとにデバイス上で自位置を計算するインサイドアウト

[1] http://cricket.csail.mit.edu/

の測位と，Ubisense[2]のようにデバイスの発するビーコンを基に周囲のインフラがデバイスの位置を計算するアウトサイドインの測位に分類されている．また位置計算を外部に依存しデバイス内部だけで完結しないアウトサイドインの測位の方が，より漏洩リスクが高いとされている．これはアウトサイドインの測位の場合，ユーザ（のデバイス）だけでなくサービスのインフラもユーザの位置を知ることができ，時にはユーザの意思に反して位置情報を取得することができるためである．

加えて，ユーザの位置情報が収集された場合，それが仮に匿名のデータであったとしても，計算による行動パターンの分析によってそのユーザの属性（実名や居住地・勤務先等）が暴露される脅威が示されており，さらにそれらによってユーザの将来の位置を予測することも可能であるとされている．

2.2 現実の脅威となった事例

各種センサーや通信機能を搭載したデバイスを常時持ち歩くということは，プライバシー上の危険をはらんでいる．2011 年に大きなニュースとなったカレログ[3]がひとつの例である．

Android アプリケーションとして実装されたこのツールは，GPS 等から得た位置情報，端末から得られる通話履歴や電池残量など，インストールされた端末の移動・利用履歴をロギングすることで，ユーザの行動ログを得ようとするものである．このアプリケーションについては各方面からの批判や指摘の結果，端末にインストールして動作するという仕様上，利用規約や導入時の本人確認の強化するなどの方法でプライバシーの問題を回避した．

しかし前述のようにスマートフォンはその性質上，そのユーザの生活に密着した利用がされていることが多く，ユーザはデバイスを肌身離さず持ち歩く傾向がある．そのため，デバイスのログがそのままユーザの行動ログに近似できるという性質は依然存在している．

実際，カレログ以上に多彩な機能を提供する Cerberus[4]や AndroidLost[5]といった Android アプリケーションも公開されている．これらのツールはデバイスの追跡や遠隔操作を可能とするものであり，GPS による追跡はもちろんデバイスのカメラ等を制御することも可能である．これらの機能はデバイスの紛失や盗難に備えたものであるとされているが，その強力な機能から，ユーザに無断で第三者にインストールされた場合の脅威はカレログ以上であると指摘されている．

2.3 ワイヤレスデバイスの持つ潜在リスク

これまでに述べたような Wi-Fi デバイスおよび Bluetooth デバイスには，それらのインターフェースごとに固有で割り当てられた MAC アドレスがある．このアドレスを利用し，通信相手を識別した上でワイヤレス通信を実現している．また原則として，デバイスが製造されてから廃棄されるまでこのアドレスが変更されることはない．さらに，一般にワイヤレス通信の内容は上位レイヤーで暗号化されていることが多いが，MAC アドレスは最も低レイヤーのアドレスであるため，通信においてこのアドレスを暗号化することができない．

これはつまり，「Wi-Fi や Bluetooth を用いて無線通信を行っているデバイスは，そのデバイス固有の ID を外部から容易に観測・収集され得る」ということを意味する．このことから，測位を意図したものではない通信パケットであってもそれを位置ビーコンとして利用することができ，2.1 節で触れたアウトサイドインの測位が可能となることから，Wi-Fi や Bluetooth を用いて通信を行うデバイスにはその仕様上，単に通信を行うだけで第三者に自身の位置情報を取得され得るという潜在的なリスクがあると言える．

[2] http://www.ubisense.net/
[3] http://karelog.jp/
[4] https://www.cerberusapp.com/
[5] http://www.androidlost.com/

2.4 鉄道利用者の乗降パターン追跡実験

ワイヤレスデバイスの通信による脅威を実際に示すものとして，独立行政法人産業技術総合研究所・高木浩光氏のブログ記事がある [6]．これは，山手線の車内で観測できる Bluetooth デバイスの MAC アドレスを収集し，得られたデータを分析することで乗客の乗降パターンを追跡するというものである．この実験では位置情報を同時に観測することは行われていないが，観測時刻と山手線の運行スケジュールの関係を考慮することで，乗客の乗降パターンを詳細に追跡できていることが確認できる．

またこの記事によると，山手線を 4 周する間，時間にして 4 時間程度で 1,154 個の MAC アドレスを検出し，またそれぞれ異なる日に行われた予備テストを合わせた 4 回の観測の中で，同一の MAC アドレスを 2 件検出したとされている．これは以前に観測したものと同じデバイスが観測範囲内に再び現れたということを意味しており，それぞれの位置・時刻において同じ人物が近くにいた可能性が高いと推測できる．

この実験は 1 台のロガーによる収集を短時間行ったものであるので，深刻なプライバシー情報の暴露には至っていない．しかし，同様の実験を多数のロガーを用い長期に渡って続けることで，深刻なロケーションプライバシー問題を提起するより多くの実データを得ることができると考えられる．

3 フィールド実験

3.1 実験の詳細

3.1.1 データ収集

京都大学学術情報メディアセンターの教員 4 名，同大学院情報学研究科の博士課程学生 1 名の合計 5 名の実験協力者が，次項で述べるロガーアプリケーションをインストールしたデバイスを携帯しデータを収集した．収集期間は月曜日から金曜日までの平日 5 日間を 1 セットとした合計 2 セット 10 日間で，協力者はロガーアプリケーションを起動させた状態で日常の通勤・通学・学内移動といった行動をとった．

ただこの実験では，ロガーアプリケーションの起動中は協力者の移動履歴がすべて記録されることになるため，実験に協力することで協力者のロケーションプライバシーが詳細に暴露されるという問題がある．そこで，協力者のロケーションプライバシーを考慮し，特に行動を秘匿したい場合等において協力者の判断で任意にロガーをオン／オフすることを認めている．

3.1.2 ロガーアプリケーション

実験用に，Android デバイス上で動作するロガーアプリケーションを開発した．このアプリケーションは Android 2.1[5] 以上のデバイスで動作する．ロガーは Android サービスとして動作し，サービスが起動している間，周囲に存在する Wi-Fi, Bluetooth デバイスを一定時間毎にスキャンし，観測したデバイスの情報（表 1）を記録する．さらに，Android によって提供される GPS およびネットワーク測位の情報を利用して自身の移動履歴（表 2）を記録する．

このロガーアプリケーションは Android の一般ユーザ権限で利用できる API のみを利用して実装されている．そのため，収集可能なデバイス情報は，SSID をブロードキャストしているアクセスポイントモードの Wi-Fi デバイスと discoverable（発見可能）モードの Bluetooth デバイスに関する情報である．

root 権限を取得した Android デバイスやモバイル PC などを用いて通信パケットを詳細に解析することで上記に限定されないより多くのデバイスの情報を取得することが可能となると考えられるが，ここでは敢えて制限の厳しい一般ユーザ権限のアプリケーションとして実装している．これは，特別な知識や技術がなくても他者のプライバシー情報を暴露でき得ることや，悪意がなくとも例えばマルウェアとしてインストールされた場合の脅威を実証することを意図したものである．

なお取得した情報のうちデバイスの MAC アドレス（BSSID）についてはデバイスの同定のみを目的とし，万一この実験において収集したデータが漏洩した場合に問題が拡大すること

表 1: 取得するデバイス情報

Wi-Fi	Bluetooth
システム時刻	システム時刻
スキャン開始時刻	スキャン開始時刻
BSSID*	MAC アドレス*
SSID	デバイス名
認証, 暗号化方式等	デバイスクラス
信号強度	
使用周波数	

* 値そのものではなく SHA-1 によるダイジェスト値

表 2: 取得する位置情報

GPS	ネットワーク測位
システム時刻	システム時刻
GPS 時刻	
緯度，経度，高度	緯度，経度，高度
精度	精度
速度，進行方向	

を防ぐため，MAC アドレスそのものではなく SHA-1 によるダイジェスト値を記録している．

3.1.3 実験用デバイス

本実験のデータ収集において，Android 2.3.4 を標準搭載した Sony Ericsson Mobile Communications 社製のスマートフォン，Xperia ray を使用した．本機種は一般の携帯電話販売代理店や家電量販店等で入手可能なものである．

3.2 実験結果

3.2.1 収集したデータ数

前節で述べた実験の結果，同一のデバイスを連続して観測したものも含め延べ 125,567 件の Wi-Fi デバイス，12,757 件の Bluetooth デバイスを観測し，このうちユニークなものは，Wi-Fi デバイス 17,355 件，Blutooth デバイス 1,535 件であった（表 3, 4）．ここで，観測されたデバイスの中には複数のロガーによって観測されたデバイスも存在するため，ロガー毎のユニークデバイス数の合計と全体でのユニークデバイス数は一致しない（表 3, 4 中 * 印）．

表 3: 収集したデータ数（Wi-Fi）

ロガー	ログ件数	ユニーク
#1	23,388	2,004
#2	1,847	666
#3	20,865	3,970
#4	22,868	4,013
#5	56,599	10,489
合計	125,567	17,355*

表 4: 収集したデータ数（Bluetooth）

ロガー	ログ件数	ユニーク
#1	3,680	307
#2	652	109
#3	1,854	248
#4	4,440	383
#5	2,131	636
合計	12,757	1,535*

* ロガー毎のユニークデバイス数の合計とは一致しない

4 考察

4.1 ロケーションプライバシー上の脅威

収集した表 3, 4 のデータのうち，複数のロガーに共通して観測されたデバイス数を集計したところ，Wi-Fi デバイスは 2,407 件，Bluetooth デバイスは 105 件であった（表 5）．

特に，ロガーで観測されたデバイスが Wi-Fi 92 件，Bluetooth 2 件であり．このうち Bluetooth デバイスについては，後述するフレンドリ名を利用することで行動パターンを分析することなくユーザを特定することができた．

また，上記デバイスを観測した位置についても，収集したログにより特定することが可能である．今回の実験ではデバイス数を集計するのみにとどめているが，これらの情報を元にターゲットを絞り，さらに詳細な追跡を行うことも可能である．

表 5: 複数のロガーに観測されたデバイス数

ロガー台数	Wi-Fi	Bluetooth
2	1,498	71
3	530	27
4	287	5
5	92	2
合計	2,407	105

4.2 脅威を回避・低減する手法

4.2.1 脅威の原因

このようなプライバシー上の脅威の根本的な原因は，2.3 節で述べたように，MAC アドレスがデバイス固有とされていることにある．外部から容易に観測することのできる MAC アドレスが唯一不変のものであるという性質を有するため，MAC アドレスを用いて外部からデバイスを同定することが可能となり，固定 ID[7] の問題が発生する．つまり MAC アドレスの一意性が解消されない限り，位置情報が暴露されるリスクを回避することはできない．

4.2.2 MAC アドレスの定期的な変更

仕様上，MAC アドレスは割り当てられるインターフェイスに唯一固有のものとされているが，実際上は通信範囲内で MAC アドレスの衝突が起こらない限りは唯一固有でなくても（通信範囲外に重複する MAC アドレスを持つインターフェイスが存在したとしても）通信に影響はない．そこで一つの解決策として，利用する MAC アドレスを次々に変更しながら通信を行うことで，第三者に観測されたとしてもデバイスの追跡を困難にすることが考えられる．

Wi-Fi においては，仮に通信中に MAC アドレスを変更したとしても，Layer-3 以上では従来通りの通信が期待できる．具体的には，アドレスを変更する度に ARP によるアドレス解決を再試行すればよいと考えられる．

ここで，アドレス解決を再試行する際の通信を傍受された場合，変更前のアドレスと変更後のアドレスを関連付けることで引き続き目的のデバイスを追跡することが可能となる．しかしそれが可能となるのはあらゆる地点に無数のロガーが存在する場合や，既にある程度ユーザが特定されており常に近距離で追跡されている場合である．このような状況では，仮に MAC アドレスを変更することでこれに起因する脅威を回避したとしても他の方法でユーザを追跡することが可能であると考えられるため，本稿では考察の対象としない．

ただ，暗号通信プロトコルである WPA-PSK が鍵生成に MAC アドレスを利用するように，仕様上 MAC アドレスを参照する必要があるプロトコルが存在する場合，その実装によっては特別な対応が必要になる可能性がある．また MAC アドレスを用いてデバイス認証を行うシステムも存在するため，注意が必要である．

Bluetooth においても同様の手法によってプライバシーリスクを低減できると考えられるが，Bluetooth デバイスの場合，接続相手のデバイスの MAC アドレス（BD_ADDR）やリンクキーを互いに記憶しておくことによって次回からのデバイス認証を省略することのできるペアリング機能が存在する．複数台のデバイスとのペアリング設定（マルチペアリング）を行うことも一般的であるため，単純にアドレス変更を行うだけでは，そのときオフラインであるデバイスとのペアリングが解消されてしまうため，この点に関して考慮が必要である．

4.3 初期設定や仕様の問題

4.3.1 Bluetooth デバイスのフレンドリ名

今回の実験で収集したデータ，特に Bluetooth デバイスに関する情報において，いくつかの興味深い特徴があった．

Bluetooth デバイスは，そのデバイスを表すフレンドリ名（表 1 中「デバイス名」）を持っている．入力インターフェイスを持つデバイスではユーザが任意に設定できることが多く，また多くの場合その規定値はメーカーによって定められた値となっている．

4.3.2　携帯電話の場合

Bluetooth デバイスのうち携帯電話に注目すると，フレンドリ名が取得できたものは全体で 600 台あり，これらのフレンドリ名が初期値である機種名のまま変更されていないと仮定すると，そのメーカーに偏りが見られた．目視で確認したところ，観測した 600 台のうち A 社製の携帯電話が 317 台でもっとも多く，以下 B 社製が 53 台，C 社製が 41 台であり，この 3 社で全体の 7 割弱を占めていた．

この結果は携帯電話の国内シェアの傾向とは一致しておらず，このことから，これまでに出荷されたこれらのメーカーの携帯電話では，初期設定で discoverable（発見可能）モードに設定されているか，discoverable モードを自動的に解除する機能用意されていないのではないかと推測できる．さらには，初期設定で Bluetooth が有効化されている可能性も考えられる．

discoverable モードに設定されたデバイスは，今回開発したロガーのように周辺のデバイスを検索するデバイスに対して応答する．このことはデバイスの追跡をより容易にするため，デバイスのペアリングを行う時にだけ discoverable モードに設定し，ペアリングが完了したらすぐに解除するのが望ましい．

4.3.3　コンピュータやスマートフォンの場合

コンピュータやスマートフォン等においては，フレンドリ名にユーザの名前が含まれているものが多く観測された．例えば,「折尾彰吾のコンピュータ」「ORIO-PC」のようなものである．これは問題のデバイスに搭載されている OS が，フレンドリ名の規定値を「（ユーザ名）の（製品名）」やマシン名としていることが原因であると考えられる．

携帯電話の場合と同様に目視で確認したところ，フレンドリ名が取得できた 135 台のうち，半分以上の 72 台にユーザの名前（姓，名）と思われる文字列が含まれていた．さらにそのうち 34 台はユーザのフルネームと思われる文字列が含まれていた．

ユーザの名前が分かると本人の特定がより容易になり，プライバシー上の脅威がさらに大きくなる．基本的には変更できない MAC アドレスとは異なり，フレンドリ名はユーザによって任意に変更できることも多いため，外部に公開される可能性のあるフレンドリ名にはユーザの名前を含めないようにすることで，この問題は回避できる．

4.3.4　メーカー仕様の重要性

前述のように，基本的にこれらのデバイスではユーザによって設定を変更できるため，設定変更によって脅威を回避することができ，問題は少ないと考えられるかもしれない．しかし操作に不慣れなユーザによる意図しない操作によってデバイスが discoverable モードに設定された場合を考慮し，一定時間でモード変更を自動的にキャンセルする仕様や，外部に公開される可能性のあるフレンドリ名の初期値にユーザ名を含めない仕様にしておくことが重要であると考えられる．

5　おわりに

5.1　まとめ

Wi-Fi デバイスや Bluetooth デバイスにはその仕様上，唯一不変の MAC アドレスが割り当てられているが，これらのワイヤレス通信においてこのアドレスは外部から容易に観測できる．本稿ではこれを固定 ID を伴った位置ビーコンとして利用できると考え，これにより可能となり得るロケーションプライバシー上の脅威について述べた．

上記を実証するため，まず周囲に存在するデバイスの MAC アドレスを位置その他の情報と紐付けて収集するロガーアプリケーションを開発した．また実際にこのアプリケーションを用いて上記の情報を収集する計 10 日間のフィールド実験を行い，結果を分析することでロケーションプライバシー上の脅威を示した．

これらの脅威を回避・低減する手法として，MAC アドレスを変化させながら通信する仕組みの必要性を提言した．

また実験によって収集したデータから，初期設定や仕様が適切でないおそれがあるデバイスが多く存在することが分かった．さらにこの性質を利用することで，少ない数のデータからでもユーザを特定した上で，そのユーザのデバイスを追跡することができることが分かった．

5.2 今後の展望

ロガーアプリケーションをインストールした 5 台のデバイスを用いて 10 日間の実験を行いデータを集計した結果，合計 2,512 台のデバイスを異なるロガーで観測できたことが分かった．今後，より多くのデバイスでより広範囲，長期間のデータを収集したい．

また本稿では複数のロガーに共通して観測されたデバイスを集計したのみであるため，ユーザを追跡でき得るデバイスが実験協力者の行動範囲の中に上記の台数存在することが示されたのみである．しかし併せて収集した位置や時刻等の情報を用いることでユーザの行動パターンを分析することで，より深刻なプライバシー情報を暴露することが可能であると考えられる．

この脅威に関して，MAC アドレスを変化させながら通信することで脅威を低減・回避する手法を提言したが，この手法を実機に実装し実験によって有効性を確認することは現実的でない．そのため，ユーザの行動やロガーの移動，MAC アドレスを変更するタイミング等を数理モデル化しシミュレーションを行うことで，提言した手法の妥当性を確認したい．またこの手法を Wi-Fi と同様に Bluetooth に適用すると設定したペアリングが無効になる場合がある問題があるため，この問題を解決して安全に Bluetooth 通信を実現する手法を新たに提案する必要がある．

参考文献

[1] Bluetooth Special Interest Group. *Specification of the Bluetooth System (2.1)*, 2007.

[2] IEEE. IEEE 802.11 wireless local area networks. `http://www.ieee802.org/11/` Accessed: July 1, 2012.

[3] John Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13:391–399, 2009.

[4] MM 総研. スマートフォン市場規模の推移・予測（12 年 3 月）. `http://www.m2ri.jp/newsreleases/main.php?id=010120120313500` Accessed: July 1, 2012.

[5] Android Open Source Project. Android 2.1 platform. `http://developer.android.com/about/versions/android-2.1.html` Accessed: July 1, 2012.

[6] 高木 浩光. Bluetooth で山手線の乗降パターンを追跡してみた. `http://takagi-hiromitsu.jp/diary/20090301.html` Accessed: July 1, 2012.

[7] 上原 哲太郎. Web や携帯電話における固定 ID とプライバシー問題. **システム制御情報学会誌**, 54(6):236–241, 2010.