1W-04

スマートフォンアプリケーションの動作状況を利用したフォレンジック手法の検討

諏訪部　功吉†　　田中　英彦†
情報セキュリティ大学院大学†

1. はじめに

総務省が発表した「平成 28 年度版情報通信白書」[1]によれば，「携帯電話・PHS」の世帯普及率は 95．8%であり，「携帯電話・PHS」の内数である「スマートフォン」は 72．0%と普及が進んでいる．また多くのスマートフォンには GPS センサーや加速度センサー，温度センサー等の各種センサーが搭載されており，これらのセンサーを活用するアプリケーションも日々増えている．このためインターネットだけでなく，スマートフォンを使用して音楽を聞いたり，SNS やチャットアプリを使用したりするなど，スマートフォンを肌身離さず持っている人は多くなっていると言える．

ただスマートフォンを持つ人が増えたことで，様々な場面でモバイル・フォレンジックを行う機会も増えているとも言える．しかしこれらスマートフォンにはインターネットや E-mail などの機能に加え，様々なアプリケーションをインストールでき，パソコンと同様の機能を有しているものの，パソコンやサーバに対するフォレンジックとモバイル・フォレンジックとは異なる．

現在のモバイル・フォレンジックでは，専用ソフトウェアの自動解析機能だけでは「十分な解析をした．」とは言えない．これはスマートフォンにインストールされたアプリケーションが，許可された範囲で開発者が自由にデータを保存することが可能なため，そのデータの中にもフォレンジックの結果として必要なデータが保存されている場合があるにもかかわらず，専用ソフトウェアの自動解析機能だけでは解析者に必要なデータであることを示すことができていないからである．

本研究では，フォレンジック用のソフトウェアの自動解析機能を使用せず，スマートフォンにインストールされたアプリケーションが記録したデータに着目して行うモバイル・フォレンジックの手法を提案する．

2. 関連研究

デジタル・フォレンジック研究会では，デジタル・フォレンジックについて「インシデントレスポンスや法的紛争・訴訟に際し，電磁的記録の証拠保全及び調査・分析を行うとともに，電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言います．」と定義[2]している．またデジタル・フォレンジック概論[3]では，フォレンジックをする対象を，パソコン，ネットワーク，モバイル，その他の電子機器の 4 種類に分類して説明しており，本研究ではモバイル・フォンレジックを対象とする．

Forensic method using data recorded by smartphone applications
†Koukichi SUWABE , †Hidehiko TANAKA
†Institute of Information Security

2.1. モバイル・フォレンジック

現在のスマートフォンやタブレットなどのモバイル端末は，パソコンに近い機能を持っており，基本的な構成についてもパソコンと同様であると言える．しかしフォレンジックの観点からは，パソコンのハードディスクに当たる補助記憶装置が手軽に取り出せないという点で大きく異なっており，従来の補助記憶装置を取り出してデータを複写するという手法を使用することができない．またスマートフォンやタブレットでは，インストールされるアプリケーションの権限を厳しく管理されていることが多く，パソコンのように新たに専用アプリケーションを実行しても，メモリ上データを取得することは困難である．このためモバイル端末からデータを取得するには，そのモバイル端末の基本ソフトである Android や iOS を作成した Google 社や Apple 社が提供している，バックアップ用のソフトウェアを使用するという方法が一般的であり，モバイル端末とパソコンとでは「データの収集」という過程について大きな差がある．

2.2. 先行研究

スマートフォンに対するフォレンジックについては，白石ら[4]は企業の情報漏洩対策の際にフォレンジックが必要であるとして，企業が社員にスマートフォンを渡す前に，専用のフォレンジックのためのアプリケ ーションを事前にインストールしておき，スマートフォン内のデータに優先順位をつけて，継続的にそのアプリケーションでデータを取得するという手法を提案している．

また SNS に投稿した際の位置情報に関する研究も行なわれている．森國ら[5]は SNS の位置情報付きツイートから，各エリアで単語出現頻度を学習し，その結果を用いて単語フィルタリングをすることで，位置情報を付加していない投稿に対してツイート投稿位置を推定して，位置情報を付与する手法を提案した．また論文中で，SNS を用いた位置推定手法を大きく，投稿内容を用いて推定を行うコンテンツベース手法，ユーザ友人関係を用いて推定を行うグラフベース手法，それらを組み合わせる手法の 3 つに分類している．

スマートフォン内のデータを使用せず，観測により行動を把握する手法として，吉村ら[6]は Wi-Fi や Bluetooth 通信が，デバイス固有に割り当てられたアドレスが暗号化されることなくやり取りされていることに着目し，これらのデータを観測位置や時刻などの情報と紐付けて，継続的に観測することで，ユーザの位置履歴や行動パターンを特定することが可能であることを示した．フィールド実験で 4 ヶ月間データを集めて，そのデータをデバイスのアドレスで名寄せし分析することで，位置を追跡できるデバイスの存在を明らかにした．

また Stefan Maus ら[7]はスマートフォンに記録されたアプリケーションのデータから，緯度経度や住所などの位置情報を取得するため，「latitude」「longitude」などの単語によるフィルタリングを用いる手法を示し，実際に

アプリケーションから，住所情報を抽出可能なことを示している．またこれらで取得可能な情報量を増やすことで，捜査機関に有用なデータとなることを述べているが，実証はされていない．

本研究の提案手法は追加のアプリケーションをインストールしない点，継続的な観測や，SNS などの外部の情報を使用せず，スマートフォンから得られる情報だけを用いる点で上記研究とは異なる．またスマートフォンに記録されたアプリケーションのデータに着目する点については Stefan Maus らと同様であるが，実際のデータに本研究の提案手法を適用し，市販されているモバイル・フォレンジックの専用ソフトウェアと結果を比較することで，本研究の提案手法の優位性を示す．

3. 提案手法

本研究の提案手法ではスマートフォンなどにインストールされたアプリケーション（以下アプリケーション）が独自に保存しているデータを調査した．特に本研究ではアプリケーションが独自に保存している「スマートフォンの場所に関わるデータ」に着目して調査を行い，対象としたアプリケーションが記録したデータの形式やファイルパスを調査して，実際のデータを抽出した．

4. アプリケーションの調査

インターネット上の様々な統計情報を収集している statista 社が公開している情報[8][9]によれば，Google Play で公開されているアプリケーションの数は 2016 年の時点で 240 万件を超えており，App Store で公開しているアプリケーションの数は 2016 年の 6 月には 200 万件を超えている．また日々新しいアプリケーションが公開されていることを考えると，これら膨大な数のアプリケーションを全て調査することは不可能である．

本研究では，平成 28 年 6 月 12 日時点の日本向けの Google Play において無料でダウンロード可能な，上位 540 位のアプリケーションのうち，位置情報の権限を要求する 187 個のアプリケーションを対象とし，そのアプリケーションの中から，データがバックアップ可能かどうかを調査し，バックアップ可能なアプリケーション 137 件を対象とした．

緯度経度の保存形式は整数値の場合や小数値の場合がある．また時間であれば，UnixTime もあれば，年月日時分秒が記載されている場合もあるため，データの確認は目視によるものとした．

5. 調査結果

OS に Android 6.0 を搭載した LG 製の Nexus5X を検証用端末として，実際にインストールしたアプリケーションからデータを確認した．データの収集については基本ソフトの Android を作成した Google 社が提供しているバックアップ用のソフトウェアである「Android Debug Bridge」[10]を使用してバックアップファイルを取得し，その確認には「Oxygen Forensic Suite」[11]を使用した．

位置情報の権限を要求し，データが取得可能な 137 種類のアプリケーションを確認した結果，位置情報等が記録されていたアプリケーションは 17 種類であった．この調査結果を用いて位置情報等を Google Map に表示した像を図 1 に示す．図中の「📍」マークは緯度経度情報を地図上に示したものである．Android Debug Bridge で取得したバックアップファイルを市販のツールの自動解析機能で解析したところ，表示することはできなかった．

図 1. 位置情報等を Google Map で表示

6. まとめ

本研究により，モバイル・フォレンジック専用ソフトウェアの自動解析では発見できなかった値を抽出できることを実証した．本研究では例として「所有者の場所に関わる情報」を挙げて示したが，アプリケーションのデータを詳細に解析するという手法は，他の情報についても可能であるし，また他のモバイル端末に対しても同様である．例えば接続時の IP アドレスや無線 LAN の SSID 等の抽出も可能であろう．

今後は本提案手法を他の端末やデータについて実証し，適用可能であることを示す必要があると考えている．

参考文献

[1] 総務省，「平成 28 年版 情報通信白書｜インターネットの普及状況」，http://www.soumu.go.jp/johotsusintokei/white-paper/ja/h28/html/nc252110.html(2016.11.15 アクセス)
[2] デジタル・フォレンジック研究会，「デジタル・フォレンジックとは」，https://digitalforensic.jp/home/what-df/ (2016.11.15 アクセス)
[3] 羽室英太郎，國浦淳，「デジタル・フォレンジック概論」，東京法令出版 (2015)
[4] 白石陽，三科貴，高橋修：フォレンジック技術を利用した携帯端末のための証拠保全手法，情報処理学会論文誌 Vol.54 No.1 91-102
[5] 森國泰平，吉田光男，岡部正幸，梅村恭司：ツイート投稿位置推定のための単語フィルタリング手法，情報処理学会論文誌データベース Vol.8 No.4 16-26 (2015)
[6] 吉村豪康，折尾彰吾，上田浩，上原哲太郎，津田侑，山村智英，野村怜一：Wi-Fi/Bluetooth 通信が引き起こす位置プライバシー問題に関するフィールド実験，信学技報 IEICE Technical Report SITE2012-71,IA2012-109 (2013)
[7] Stefan Maus, Hans Höfken, Marko Schuba：Forensic Analysis of Geodata in Android Smartphone，International Conference on Cybercrime, Security and Digital Forensics （ 2011 ）
[8] statista 社，「Google Play Store: number of apps 2009-2016 | Statistic」，https://www.statista.com/statistics-/266210/number-of-available-applications-in-the-google-play-store/(2016.12.13 アクセス)
[9] statista 社，「Apple App Store: number of available apps 2016 | Statistic」，https://www.statista.com/stati-stics/263795/number-of-available-apps-in-the-apple-app-store/(2016.12.13 アクセス)
[10] Google 社，「Android debug bridge」，https://devel-oper.android.com/studio/command-line/adb.html (2016.12.21 アクセス)
[11] Oxygen Forensics，「Oxygen Forensics Suite」，https://www.oxygen-forensic.com/en/ (2016.11.21 アクセス)