Vol.2013-IS-125 No.9
2013/9/13

スマートフォン・フォレンジックのための通話録音アプリケーションの提案

古川 敬久[†1]　千石 靖[†1]

概要：スマートフォン・フォレンジックサービスでは、削除された発信履歴・着信履歴などの通話履歴の復元やメール・SMS などのメッセージ復元などの調査を行うことができる。企業内部で情報漏えいが起こり、スマートフォン・フォレンジックによってデータを収集する時、発信履歴・着信履歴などの通話履歴を示すのは電話をした事実だけのため、情報漏えいに繋がるかは不明確である。そこで本研究では、企業で支給されるスマートフォンを対象にし、容易に削除できない通話録音アプリケーションを提案する。

キーワード：デジタル・フォレンジック,スマートフォン,スマートフォン・フォレンジック

The propose of call recording application for smartphone forensic

TAKAHISA FURUKAWA[†1]　YASUSHI SENGOKU[†2]

Abstract: Smartphone forensic services can extract the incoming and outgoing call history and can restore messages such as those exchanged through SMS and e-mail. When information leakage occurs within a company, data is collected through smartphone forensics to identify the perpetrator; however, call history information is insufficient, as the mere fact that a phone call was placed or received does not amount to information leakage. In this paper, We propose a call recording application targeted at smartphones paid for by the company.

Keywords: Digital forensic, smartphone, Smartphone forensic

1. はじめに

近年デジタル・フォレンジックに対する意識が高まっている。デジタル・フォレンジックとは、インシデントレスポンスや法的紛争・訴訟に対し、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・技術を言う。なお、インシデントレスポンスとは、コンピュータやネットワーク等の資源および環境の不正利用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為や事象等への対応等を指す。金融庁では 2010 年に経営破たんした日本振興銀行が破たん前に意図的に電子メールを削除し、捜査を妨害した例もあることから、情報隠しの検査を強化するために、フォレンジックシステムを導入することを決定した[1]。

コンピュータ・フォレンジックの手順としては、まず調査対象となるコンピュータのハードディスクを専用の機器を用いて物理的にコピーする。ディスクのセクタを残らずコピーするため、完全に同じハードディスクを作成することができる。次にコピーされたハードディスクに保存されているファイルや、Web ブラウザが利用するキャッシュをもとにアクセス履歴や、レジストリ情報をもとに USB メモリなどの利用状況を調査し、可能な限り復元する。可能な限りというのは、デジタル・フォレンジックではパソコンのハードディスクに残ったデータ本体や削除されたデータの残骸、データ処理の際に使われる別の領域に残された痕跡などを復元し、時系列に合わせていくのだが、ディスク上のビット列が一度でも変更された場合、復元が難しくなるためである。しかし、デジタル・フォレンジックを用いることで復元が可能となった事件は多くある。

主な事例としては、ライブドア事件[2]と大相撲八百長問題[3]が挙げられる。ライブドア事件とは、虚偽の有価証券報告書の提出をはじめ株式市場に虚偽情報を流し、ライブドアおよびその役員等が同社株価及び関連会社株価を不当に高く吊り上げ、その結果、本来あるべき株価よりも高い株価で購入させられた一般投資家が多大な損害を被った事件である。当時の報道によれば、家宅捜査が行われると察した事件関係者は虚偽情報などのメールを削除し、重要なファイルも削除されていた。デジタル・フォレンジックによりデータセンターに設置されたサーバでメールの流れを押さえ、押収した経営陣のパソコンを解析して問題のメールを把握した。大相撲八百長問題の発端は、警視庁が行っていた野球賭博に関する捜査で押収された携帯電話のなかに、八百長を持ちかけるメールが見つかったというものである。端末上で削除されていたメールのデータを復元するのにデジタル・フォレンジックの技術が使われており、電子情報におけるフォレンジック技術を知らしめることにもなった。強制捜査で押収すれば、そのなかに被疑者が隠そうとする証拠をみつけることもあり得るため、これはフォ

†1 金沢工業大学大学院工学研究科
Graduate School of Engineering, Kanazawa Institute of Technology

レンジック・ツールが有効に使われたケースであった。

犯罪捜査だけではなく、企業内部の不正調査にもデジタル・フォレンジックは活用される。様々な企業でフォレンジックの調査サービスを行っている。たとえば、既存顧客からの指摘で、顧客情報と技術情報が競合他社に持ち出されていることが発覚し、アクセスログ、メールの送受信履歴など意図的な隠ぺい工作の証拠データをデジタル・フォレンジック技術により検出したため損害賠償請求に至った事例などが挙げられる。

2011 年情報セキュリティインシデントに関する調査報告書[4]によると、表 1 からインシデント・トップ 10 の原因は「内部犯罪・内部不正行為」「不正アクセス」「不正な情報持ち出し」と故意を含んだ原因が目立つ。図 1 より 2011 年の漏えい原因比率として、内部犯罪・内部不正は全体の 1.7%を占めていた。図 2 では漏えい原因別 1 件あたりの漏えい人数を示している。原因比率として内部犯罪・内部不正は低いにも関わらず、1 件当たりの漏えい数は 3 番目に高いことから発生時の影響が多大であることがわかる。以上からデジタル・フォレンジックは重要な手段として必要とされていることがわかる。

表 1：規模の大きいインシデント・トップ 10

No.	漏えい人数	業種	原因
1	165 万 7131 人	金融業，保険業	不正な情報持ち出し
2	136 万 8307 人	金融業，保険業	管理ミス
3	100 万 7052 人	生活関連サービス業，娯楽業	不正アクセス
4	20 万 3731 人	情報通信業	不正アクセス
5	15 万 8248 人	金融業，保険業	内部犯罪・内部不正行為
6	12 万 8307 人	金融業，保険業	管理ミス
7	12 万 4900 人	金融業，保険業	管理ミス
8	9 万 2408 人	金融業，保険業	内部犯罪・内部不正行為
9	7 万 3000 人	卸売業，小売業	内部犯罪・内部不正行為
10	7 万人	情報通信業	誤操作

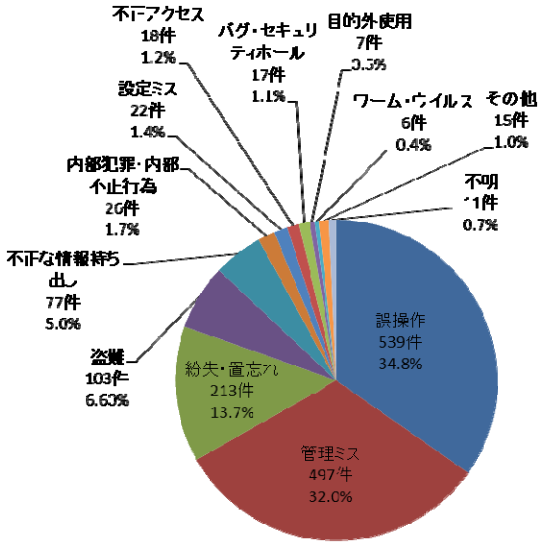

図 1　漏えい原因比率（件数）

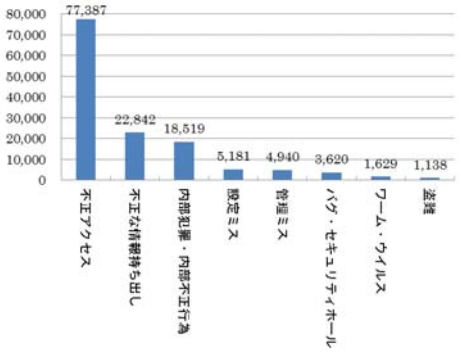

図 2　漏えい原因別 1 件当たりの漏えい人数

1.1 スマートフォン

年々スマートフォンの普及率は増加しつつある。スマートフォンが普及し始めた理由としては、従来の携帯電話と違い様々なアプリケーションを導入することが可能であり、より高速になった通信により様々な情報を常に収集することが可能になり、スマートフォンのインターフェイスをユーザの思い通りに変更可能になったなどが挙げられる。図 3 によると、世帯別の通信機器保有状況では、スマートフォンが平成 23 年末の約 30%から平成 24 年末では約 50%まで急増しタブレット端末は平成 23 年末の約 9%から平成 24 年末では約 15%に伸びている[5]。よって今後もスマートフォンとタブレット端末の世帯保有率が上昇することが予想される。2013 年スマートフォンセキュリティ協会の第一回スマートフォン企業利用実態レポート[6]から、図 4 は主に情報通信業と製造業 33 社の会社支給のスマートフォンの導入状況を示している。8 割以上がスマートフォンを支給され業務に利用している。一般的な企業対象のスマートフォン導入配布状況[7]は 27.2%であり、それより多い結果となったのは、スマートフォンセキュリティ協会参加企業が主に情報通信業と製造業からの回答のためである。IPA(情報処理推進機構)による 2013 年 4 月～6 月のウイルス・不正アクセス関連の相談総件数は 3,800 件であり、そのうちスマートフォンに関する相談が 110 件であった。2013 年の 1 月～3 月は全体 3,300 件のうちスマートフォンに関する相談が 85 件であり、2013 年 1 月～3 月と 2013 年 4 月～6 月を比べるとスマートフォンに関する相談は 29.4%の増加となった[8]。これより、今後企業で支給されるスマートフォンによるフォレンジックも考慮していかなければならない。

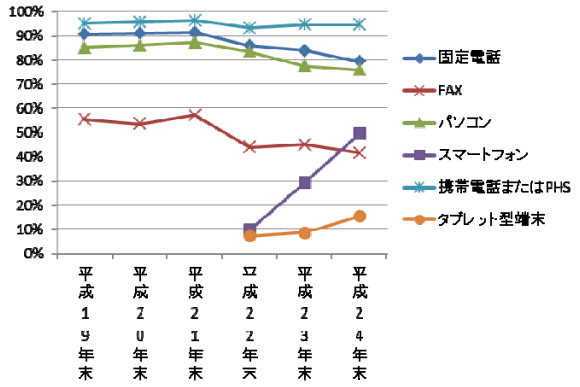

図 3　主な情報通信機器の世帯保有状況グラフ

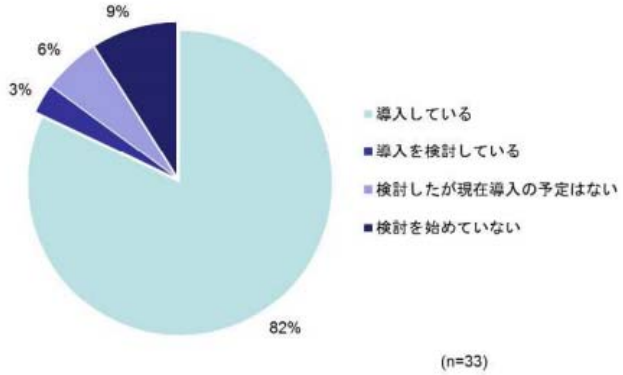

図 4　会社支給のスマートフォン導入状況

2. スマートフォン・フォレンジック

2.1 既存システム

株式会社ボイスサイバーテクノロジーズ・ジャパンでは通話録音システムとして Me(エム・イー)[9]という製品を提供している。Me はスマートフォンと固定電話で記録された録音データをサーバで一元管理するシステムである。しかし、スマートフォンで通話録音は可能だが、確認は全てサーバ上で行なわなければならない。

本研究ではスマートフォンを対象とし、ユーザが録音データを聞くことができ、アプリケーションを容易に削除できないことを可能にする。さらに、提案システムを用いてスマートフォン・フォレンジック調査に対して支援することを目的としている。

現在、スマートフォン・フォレンジックサービスを行っている企業はいくつか存在する。以下に主な調査対象を記す。

- 通話履歴調査
- メール・SMS 復元調査
- 電話帳復元調査
- 画像データ復元調査
- 使用者の位置情報履歴調査

たとえば、企業内部で情報漏えいが起こり、スマートフォン・フォレンジックによってデータを収集する際、発着信の通話履歴が示すのは電話をした事実だけであり、情報漏えいに繋がる会話を行ったかは不明確である。

そこで本研究では、企業で支給されるスマートフォンを対象にし、容易に削除できない通話録音アプリケーション(以下録音アプリケーション)を提案する。

3. 提案する通話録音アプリケーション

3.1 録音アプリケーションを使用する企業条件

録音アプリケーションを利用する際、企業条件を設定しなければ、取引先、企業イメージなど多くの被害が発生する。そのため、本研究では以下の前提条件と後述するアプリケーションと録音データの条件から企業が使用するアプリケーションとして成り立たせる。

- 従業員に会社配布のスマートフォンを持たせ、使わせる
- 個人で使用するスマートフォンは出勤時に預けるなどして使わせない

3.2 個人情報保護法に関する注意点

個人情報保護法令の法 2 条 1 項によると通話内容をデジタル機器に録音したデータの中に氏名や顧客番号など特定の個人を識別できる内容が含まれていれば、個人情報に該当する。本研究の録音データには顧客情報や従業員の名前が録音される可能性が高い。そのため、個人情報に該当する。個人情報の取り扱いは、利用目的の特定(法 15 条)、目的外利用の制限(法 16 条)、不正な取得の禁止(法 17 条)、利用目的の通知・公表(法 18 条 1 項)の義務が課せられる。個人情報のうち、個人情報データベース等を構成するもの(法 2 条 4 項)を個人データという。個人情報データベース等とは、個人情報を含む情報の集合物であり、特定の個人情報を容易に検索できるように体系的に構成したものをいう(法 2 条 2 項、政令 1 条)。録音データをサーバに残すか、クラウド上で管理するかは今後検討する。どちらの保存方法でも、日付・電話番号等による検索は可能である。そのため、個人データに該当する。個人データの取り扱いについては、正確性の確保(法 19 条)、安全管理措置(法 20 条)、従業者・委託先の監督(法 21、22 条)、第三者提供の制限(法 23 条)の義務が課される。個人データのうち、個人情報取扱事業所が、開示、訂正、追加または削除、利用の停止、消去および第三者への提供の停止を行うことのできる権限を有するものであり、6 か月を超えて保有するものであることを保有個人データという(法 2 条 5 項)。保有個人データに当たるときは、開示(法 25 条)、訂正(法 26 条)、利用停止等(法 27 条)の義務が課される[10]。そのため、6 か月を超えて保有している場合は、保有個人データに該当することとなり、開示等の対象となるため、データ保存期間の把握が重要である。

3.3 訴訟に関する問題

無断録音に対する意見は明確に解説した文献がなく、

様々な法律事務所でも意見が分かれている。訴訟で証拠として提出された場合、無断録音されたデータが法律上問題となる。刑事訴訟では、厳格な証拠制度があり、無断録音データの会話内容は原則として証拠としては使えない。しかし民事訴訟の場合では、刑事訴訟法のような厳格な証拠能力の規定はなく、当事者が事実を証明するために提出した証拠の証拠能力は原則として存在することになる。

以上から、アプリケーションと録音データの条件を以下に記す。

- 通話を自動的に録音する
- 録音データは通話終了後自動的に保存されるようにする
- 日時と通話相手が表示される
- 通話相手に録音されていることを明示する
- 誰でも必要時は録音データを聞くことができる
- 録音データは従業員が改ざん・削除できないようにする
- アプリケーションは従業員が容易に削除できないようにする
- 録音データは 6 か月後、削除を検討可能にする

以上の条件から、個人情報保護法令にも対応でき、従業員が常駐または外出している場合も録音することができる。さらに、通話相手に録音する旨を伝えた場合、刑事訴訟や民事訴訟で通話録音データは証拠能力が存在し、裁判時などに証拠物として提出することができる。

3.4 プリインストール化

本研究の録音アプリケーションでは従業員に容易に削除できないようにするためプリインストール化を行う。プリインストールとは、Android 端末やパソコンなどにあらかじめソフトウェアをインストールしていることである。Android 端末ではアドレス帳、電話帳、Google 社が提供しているフリーメールサービス Gmail などが挙げられる。

手順としては、アプリケーションの拡張子が.apk の場合、PRODUCT_COPY_FILES は system/app 以下にコピーするように記述する。記載するファイルはビルド時に読み込まれる mk ファイルにしソースをビルドすることでプリインストール化できる。

3.5 録音アプリケーションの利点

録音アプリケーションを導入することで情報漏えいの疑いがあり、さらに日時などの情報が判明している場合、クラウドやサーバに保存されている通話履歴から疑いのある人物を絞り込み、通話内容で人物を特定することができる。また、従来のスマートフォン・フォレンジックツールで発信履歴、着信履歴などの通話履歴やメール・SMS、画像データなどを復元する過程で疑いのある人物が特定できた場合でも、クラウドやサーバに残されている録音データの通話履歴や通話内容を調査することでより短時間に証拠物として裁判所に提出することができる。

録音されていることを社員に意識させることにより不正の抑止力となる。さらに重要な会話でも録音していると認知させることで会話終了後に確認できることにより聞き忘れや覚え間違いが無くなるという安心感や誤ったことは伝えてはいけないという責任感もでき、顧客とのコミュニケーションの信頼性向上につながる。

他にも顧客対応が良く、褒められた会話や対応が悪くクレームを生み出す原因となった会話を録音することで顧客対応の向上につながる。

さらに、新人教育でも実際の会話を元に教育することで問題の意味や価値を知ることができるため、教育の質が向上する。

顧客が購入後の保険や製品についての説明が購入前に聞いた情報と違うという苦情が発生した場合、従業員が購入前にどのような説明をしたのかを把握することができるため、言った言わないの水掛け論を未然に防ぐことができる。

従業員が会話内容を把握することで誤った説明や説明不足を早期に発見し対策することが可能となる。

3.6 録音アプリケーションの欠点

プリインストール化を行っても、従業員にプリインストールアプリを削除するアプリケーションをインストールされた場合、対処が不可能となる。サーバの保守などの業務を行っている企業であると、緊急に業務が発生した場合、直接保守を行っている企業ではなく、自社に出向かなければならないため対応が遅れる場合がある。従業員が不正を行い、さらにどの時期から不正を行ったかが不明確の場合、録音データを記録している期間の最初から調べなければならないため、膨大な作業量となる。

4. 通話録音アプリケーションの考察と課題

本研究はスマートフォン・フォレンジックを対象にし、通話録音アプリケーションの構築を想定している。スマートフォン・フォレンジックに対する利点がスマートフォン・フォレンジックサービスを行っている企業の通話履歴だけでなく、録音データをサーバやクラウドに保存することでより証拠性の高いデータを確保できる点などが挙げられる。しかし、スマートフォン・フォレンジックを対象としなくても、録音データを保存することで業務の効率化などの利点があり、スマートフォン・フォレンジックを対象とした通話録音アプリケーションを構築する有用性が十分とはいえない。そのため、スマートフォン・フォレンジックの対策となる有用性を今後調査、検討する。

スマートフォンを支給している企業は情報通信業と製造業の割合は多く見られたが、他の業種でも情報漏えいや内部犯罪、内部不正は起こる可能性はある。さらに、録音アプリケーションの利点は情報通信業、製造業に限らず多く

の業種に当てはまるため、他業種の企業に対するスマートフォン支給率やスマートフォンに対する意識も調査しなければならない。

録音アプリケーションの欠点では、従業員にプリインストール化を解除できる不正なアプリケーションのインストールを防ぐため、定期的にスマートフォンを回収することで防ぐことができる。また緊急に業務が発生する場合、事前に従業員にスマートフォンを貸出し、一定期間後回収することで防ぐことができる。

システム構築ではスマートフォンに標準で備わっている通話アプリケーションが起動された時に通話録音アプリケーションの起動や、通話データの保存先、通話終了時に通話データ保存の自動化、通話データの削除対策などを検討、構築していかなければならない。

5. まとめ

本稿では、既存のフォレンジックサービスを提供している企業が行っている通話履歴だけではなく、通話を録音することにより、履歴だけでは判断できない情報を得ることでスマートフォン・フォレンジック調査を支援するスマートフォン・フォレンジックのための通話録音アプリケーションを提案した。調査から、フォレンジックの有用性、スマートフォンの保有率、企業のスマートフォンの支給率からスマートフォン・フォレンジックのための通話録音アプリケーションが必要とされていることがわかった。今後は構築に向けて、他の業種でも有用性を示し、システム条件をより向上させる必要がある。

参考文献

1) 金融庁の「フォレンジック」システム導入を受けてフォレンジック関連銘柄に注目
http://www.zaikei.co.jp/article/20120129/93725.html
2) ライブドア事件
http://itpro.nikkeibp.co.jp/article/tousei/20060529/239322/
3) 大相撲八百長問題
http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=315&continue=on
4) 2011 年情報セキュリティインシデントに関する調査報告書
http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.2.pdf
5) 総務省　平成 24 年通信利用動向調査ポイント
http://www.soumu.go.jp/johotsusintokei/statistics/data/130614_1.pdf
6) 第一回スマートフォン企業利用実態調査レポート
http://www.jssec.org/dl/ResearchReport2012_v1.pdf
7) 株式会社 MM 総研　法人ユーザにおける携帯電話/スマートフォンの導入配布状況(2012 年度版)
http://www.m2ri.jp/newsreleases/main.php?id=010120121113500
8) IPA コンピュータウイルス・不正アクセス届出および相談受付況[2013 年第 2 四半期(4 月～6 月)]
http://www.ipa.go.jp/security/txt/2013/q2outline.html
9) 株式会社ボイスサイバーテクノロジーズ・ジャパン　Me
http://www.voicecyber.co.jp/
10) 個人情報の保護　個人情報保護法令
http://www.caa.go.jp/seikatsu/kojin/houritsu/index.html