1E07 先端事例をもとにした携帯電話犯罪の抑制

○伊藤卓朗（知的財産研究推進機構／慶應大政策・メディア研），
及川博道（知的財産研究推進機構／宮城大事業構想学），西村邦裕，杉村武昭（知的財産研究推進機構），
玉井克哉（東大先端研），岩崎匡寿（知的財産研究推進機構），西村由希子（東大先端研）

1. 本研究の背景と目的

近年、急速に普及した携帯電話は、単に移動式の電話端末として用いられるにとどまらず、メールやインターネット接続、デジタルカメラ、電子マネー、ポイントカード、音楽・動画再生、TV 視聴などの機能が次々と追加され、高度に多機能化している。さらに、こういった携帯電話端末の多機能化と平行して、その利用方法も複数の機能を組み合わせるなどして多様化が進んでおり、携帯電話は多機能移動個人端末「ケータイ」へと進化してきた。本研究を開始した 2004 年当時は、1999 年の NTT ドコモによる i mode サービスの開始をうけて、携帯電話が急速にインターネットへと近づき始めていた。また、日本では第三世代規格を用いたサービスの普及が進み、世界との次世代通信方式の共通化が進められた。

一方、当時既に世界的に普及していたインターネットでは、悪用や犯罪などの問題が国内外で表面化し始めていた。その際、パスワードの盗難やサーバ攻撃など、専門的知識を用いた操作が一般へと情報流出することにより問題が拡大・拡散する傾向にあった。また、インターネット上ではその技術的特性から、問題が国境を容易に越えて世界中に広がる事が常であった。携帯電話においては、日本でほぼすべての新製品に搭載されるようになっていたデジタルカメラ機能が、その機能をすぐに使い始めた若年層を中心に、雑誌や図書などから必要な情報を画像データとして複製し保存する、デジタル万引きと呼ばれる新しい犯罪を生み出した。

ケータイの新機能・新サービスにおいて、既に社会問題化した負の効果については事業者が対応しているものが多いが、潜在的な問題に対しては使用者に対してほとんど配慮がなされていない。そこで本研究では携帯電話の普及と機能の高度化・複雑化によって生じるべき将来の問題を未然にとらえ、予め適切な対応策を考案することによって、それが社会にもたらしうるマイナスの効果を極小化することを目的とした。そのため、問題が国境に縛られずにインターネットからケータイへ、若年層を中心とした先端ユーザから一般ユーザへと移行すると予測し、問題の発生源となるインターネットと先端ユーザの動向を調査する事により、ケータイで起こりうる問題を初期段階で発見出来るとの仮説を立てた。また、発生を予測、または発見した問題について、社会への影響を追跡調査した。

2. 予測した問題

1. 端末の再起動を必要とするバグ

初期のインターネット社会では、インターネットブラウザの普及に伴ってその技術的欠陥を突き、使用者を混乱させるような行為が横行した。例えば、インターネットブラウザの新規ウインドウを永遠に開き続けさせて端末を使用不能に陥らせるプログラムや、表示とは違った場所へと導くリンクなどである。これら自体は経済的に大きな被害を及ぼす事は無かったが、その後、利便性の高いサービスや技術を悪用し

たインターネットブラウザ上でのユーザネームや暗証番号の盗難へと発展し、現在では世界中で大きな経済的被害が報告されている。

2004年にPCと同様のインターネットサイトに接続出来るブラウザ（以下、フルブラウザ）を搭載したPHSが人気を博したのを受けて、携帯電話市場にもフルブラウザが登場した。そのため、著者らは初期のインターネット社会で起こったような利用者が操作不能になるような問題が起こりうると予測した。

2. 市販ソフトウェアによる暗証番号解読

第二世代（PDC）携帯電話の暗証番号は4ケタの数列であった。そのため、組み合わせは最大で9999通りであった。また、使用者の多くが自分、もしくは自分以外の誕生日などの日付（365通り）を暗証番号として設定しており（1)、その場合は容易に暗証番号を推測できた。さらに、PCを使って暗証番号を解読できるソフトが、数多く販売、または配布されており、PC初心者であっても容易に使用できた。一般的には、暗証番号解読が家族間や友人間など、近しい人間関係で行われていた。しかし、著者らはその利用の拡大をもとにした犯罪的個人情報流出の危険性を予測した。

3. 不正バイオメトリクス認証

2で述べた問題の解決策の1つとして、バイオメトリクス認証の1つである指紋認証機能の搭載が提案され、2003年より一部の携帯電話で実用化された。指紋認証技術は、ほぼすべての人間が独自の特徴を持つとされる指紋によって操作している人を特定する技術である。指紋による個人特定は、古くから犯罪捜査に使用されるなど、その有用性は実証されている。しかし、携帯電話に搭載された指紋認証機構は、市販のゼラチンを使うなどして容易に不正認証を得る事が可能である事が早くから報告されていた（2)。しかしながら、携帯電話事業者はその安全性を大きく広報したが、危険性について消費者に対して十分な説明がなされていなかった。著者らは、指紋認証を初めとするバイオメトリクス認証が、その利用拡大により高額商品や金融サービスにも使われ始めると、不正認証を用いた犯罪が発生すると予測した。

4. RFIDハッキング

RFIDとは、微小な無線システムによる認証機能であり、EdyやSuicaとしてサービス化されているFelicaが世界で初めて世界標準セキュリティ機構を取り入れて実用化されたRFIDである。現在、Felicaはおサイフケータイとして、携帯電話のほとんどの新機種に搭載されている。Felicaの内部情報は、大きく暗号化された電子マネー部分と市販のカードリーダで内容を読み込める使用履歴などを保存する部分に分ける事ができる。つまり、後者は情報の安全性が保証されておらず保存する情報は第三者に容易に閲覧される。さらに、RFIDの無線通信を前提としている技術的特性から、カード保持者に気づかれずにその情報を閲覧する事も容易である。電車や買い物などの履歴は個人の行動追跡を補助できるために、著者らは特にストーカーにより悪用される危険性を予測した。

3. 予測後の追跡調査結果及び事業者・自治体等に対する提案事項

1. 端末の再起動を必要とするバグ

初めに、技術的に可能であるかどうかを確認するために、複数のフルブラウザと端末を用いて実証実験を行った。その結果、PHS 一機種の標準搭載フルブラウザである簡単なプログラムを仕掛けたサイトにアクセスすると、電池を外さないと対処できない状況に陥る事がわかった。

また、2006 年 7 月にはケータイ Shion と呼ばれる日本語入力システムで特定の言葉を変換しようとすると、一切の操作を受け付けなくなる、または予期せず再起動するという欠陥が見つかり、1047 万台が修理を要した (3)。

これまでの調査では、こういったケータイにおける現象を悪用した犯罪は確認されていないが、ケータイの機能が多様・複雑化する中では、思いがけない欠陥が大規模に見つかる可能性は捨てきれない。そのため、事業者は使用者に対して問題が起きた時の対処方法を周知するとともに、問題が発見された場合に素早くそれを使用者に伝え、迅速に問題に対処する仕組みを整えておく必要があると考えられる。

2. 市販ソフトウェアによる暗証番号解読

複数のソフトの暗証番号解読機能を用いて暗証番号の解読を試みたところ、数十秒で第二世代携帯電話の暗証番号を明らかにできた。実際に、携帯電話の暗証番号を解読し、その暗証番号を使ってキャッシュカードやクレジットカードから金銭を不正に引き出された被害が二件報告された (4, 5)。

現在発売されている第三世代携帯電話は、ほとんどが 8 ケタの暗証番号を採用しており、さらに外部接続からの暗証番号解読が困難な構造になっている。また、使用者に対する暗証番号管理の啓蒙により、使用者のセキュリティに関する関心も高まっている。しかし、一方で第二世代携帯電話を使用している人は未だに数多くおり、金融機関など暗証番号を管理する他の団体とも協力してよりいっそうの啓蒙活動が必要であると考えられる。

3. 不正バイオメトリクス認証

現在、ケータイや PC など多くの電子機器に指紋認証機能が採用されている。また、金融機関などでは静脈認証機能を用いた ATM が実用化されるなど、バイオメトリクス認証は確実に社会に普及し始めた。ところが海外では、持ち主から切り落とした指を使用して指紋認証を突破し、高級車を盗難するという残酷な事件が報告された (6)。

今後、日本でも金融機関や金融サービスと融合したケータイなどにバイオメトリクス認証が普及すると、強盗や盗難が被害者の殺傷や誘拐を伴うようになる可能性がある。そのため、バイオメトリクス認証にだけ頼って良いのかを犯罪心理学や社会行動学なども踏まえてよく議論する必要があると考えられる。

4. RFID ハッキング

初めに、第三者が RFID 保持者の情報にどれほど簡単にアクセスできるかを確認したところ、厚手のコート越しでもかざしただけで簡単に情報を読み出す事ができた。切符や財布として使えるようになった事から利便性を求めてケータイをバッグの外側のポケットに入れる人は女性を中心に多く、そのような場合、第三者が保持者に気づかれずに定期的に情報を閲覧できる可能性は非常に高い。

この問題に対しては、一部の端末において特定のボタンを押した時のみ RFID が使用可能になる機構の導入が行われ始めた。しかし、使用者への啓蒙はほとんど行われておらず、事業者は今後積極的に安全な

使用方法を使用者に周知させる必要があると考えられる。

4. まとめ

本研究で予測した 4 つの問題のうち、実際に携帯電話を用いた犯罪として表面化したのは、「市販ソフトウェアによる暗証番号解読」のみであった。しかしながら、ケータイは関わらないものの、実際に海外で犯罪が確認された「不正バイオメトリクス認証」や、問題発生の可能性が実証された「端末の再起動を必要とするバグ」と「RFID ハッキング」、と予測したすべての問題が現実なる危険をはらんでいると証明された。

これまでに発生した、または著者らが予測した、ケータイに関わる問題を総合的に考えると、問題に対処するために大きく 3 つの方法が考えられる。第一は、通話のマナーの改善など利用者が中心と解決すべきものである。第二は、デジタル万引き防止のためのシャッター音の付加など事業者が中心となって解決すべきものである。第三は、犯罪として明らかに社会的問題となり公的制度の整備が必要なものである。そのため、今後ケータイに融合していく技術や先端ユーザの使用方法の動向を、より広範囲に、そして長期的に調査をつづけ、上記 3 つの問題に分類することで、ケータイを利用した犯罪に対して迅速な対応が可能になり、問題が拡大・拡散するのを抑制することができると考える。

ケータイは子供と老人を除くほとんどの国民が保持しており、なにか問題が起きた場合に、大きな犯罪や混乱に発展する可能性がある。そのため、このように先端事例をもとに携帯電話犯罪を抑制する社会的な仕組みが必要であると考える。

※本研究の一部は、株式会社 NTT ドコモ モバイル社会研究所との共同研究として実施した。

引用

(1) 岩崎匡寿他、「利用者から見た携帯電話の安全性に関する意識調査」、第 21 回研究・技術計画学会、2006

(2) 田辺壮宏他、「携帯機器に搭載された指紋照合装置は人工指を受け入れるか」、SCIS 2005（暗号と情報セキュリティシンポジウム ）、2005

(3) NIKKEI NET、「みられまくっちゃ」で不具合・シャープ製携帯 1047 万台を修理: http://it.nikkei.co.jp/mobile/news/index.aspx?n=MMITfa000024072006

(4) RBB TODAY、ケータイ盗難に注意…暗証番号解読機が出回る?: http://www.rbbtoday.com/news/20050818/24898.html

(5) 共同通信社、侵入先で暗証割り出す　パソコン接続、被害 2 億: http://flash24.kyodo.co.jp/?MID=RANDOM&PG=STORY&NGID=soci&NWID=2006060801004476

(6) BBC NEWS、Malaysia car thieves steal finger: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm