



行き届いたサービスか、 プライバシー保護か？

昨年9月号の本コラムではWeb世界のセキュリティについて問題が起こっているが、皆の努力で改善されるのではないかと希望を込めて書いた。安全対策についてはやっと本気に取り組みが始まったようだが、技術の標準化では、期待していた Sender ID 技術が特許の関係で IETF で不採択になり、あまり進んでいない。その間に事件の件数は増え続けている。今回は米国における ID 窃盗やプライバシーについてとり上げる。



◆個人情報の保護

日本では個人情報保護法が今年の4月から施行された。罰則規定などはこれから決めるようだが、多方面に影響を及ぼしている。一方、米国では個人情報 (ID) 窃盗がますます問題となっている。他の国でも程度の差はあれ、状況は同じようだ。技術の急速な進歩によって社会システムのデジタル化が急速に進んでいるにもかかわらず、一般の人にとって安全に使えるほどセキュリティが確立していないからだ。

個人情報はプライバシーとはどう違うのだろうか。常識的には個人情報はすべてプライバシー概念に含まれるように思えるが、法律的にプライバシー権として保護されるのは非公開情報だけである。個人情報とは、個人を識別できる情報のことで、公開情報も含まれる。この定義では、技術がさらに進歩すると、バイオメトリック情報や RFID 情報などを含め、対象となる情報は拡大していく。また、プライバシー権として保護されるはずの非公開情報も、インターネット社会では後で触れるように公開情報を集めて分析すれば推測できる。個人情報をきちんと保護することはますます重要になる。

◆米国の情報漏洩の現状

昨年度米国で ID 窃盗による詐欺の被害にあった消費者は約 930 万人、被害総額は 526 億ドルに及ぶという調査会社の報告がある。その手口は、PC や紙ファイル、郵便物など個人情報の書かれた媒体の盗難という従来の

手口が大半を占める。インターネットを利用したフィッシングやハッキング (正確にはクラッキングだが、誤用が流布している)、スパイウェアなど技術的に高度なものはまだ比率は小さいが、今後増加が予想される。

・フィッシング、ファームング

フィッシングは昨秋日本でも出現したが、米国ではその後も増加を続け、被害が拡大している。対策団体 APWG (Anti-Phishing Working Group) の集計によれば、報告されたフィッシングのサイト数は今年2月で2,600 サイト以上もあり、サイトの継続期間は平均 5.7 日だという。フィッシングメールも昨年7月から月 26% で増加し、2月には 1.3 万件になった。標的は主に金融機関や大手のオンラインショッピングのサイトであるが、対象が広がって、たとえば、人気小説「ハリーポッター」の最新本の販売を騙るフィッシングサイトも現れた。

対策としては、2種類以上の個人認証手段を使うなり、予防的スキャンソフトを使うなどすれば一定の効果があるが、広く普及するのに時間がかかる。なお、攻撃の主要なターゲットの1つである eBay では、利用者のアイデアを取り入れて、今年から利用者への連絡を電子メールを使わず、マイメッセージという独自の機能でメッセージを伝達する方法を取り入れた。

新たな手口も話題になっている。それはファームング (Pharming) と呼ばれ、騙しメールを使わない手口である。DNS サーバに仕掛け (DNS ポイズニング) を組み込んで、ユーザが正しい URL を使っても本来アクセスしたい Web サイトから偽の Web サイトに自動的に誘導される。この DNS ポイズニングは高度な技術が必要なのであまり広まらないという専門家の意見もあるが、本当に楽観できるのだろうか。少なくとも DNS への信頼性が問題になれば、インターネット全体への信頼が揺らぎかねず、心理的影響は大きい。最近、Microsoft も自社のサーバ OS に緊急にパッチをあてるよう要請している。

・ハッキング、スパイウェア

ハッキングやスパイウェアによる情報漏洩も多い。昨年10月に UC Berkeley にあるカリフォルニア州政府のデータベースに進入され、140 万人分の住民の個人情報が流失する事件があった。今年1月にはバージニア州の George Mason 大学が攻撃され、教授や学生の個人情報が 3 万人分が持ち出された。携帯電話会社 T-Mobile でもシ

米国富士通研究所

松尾 和洋 kmatsuo@fla.fujitsu.com



コラム
アメリカ IT まわりの話題

システムに侵入され、多量の顧客情報が盗まれた。

スパイウェアも色々話題を賑わしている。知らないうちに個人の行動を監視するソフトを組み込まれ、その情報を特定のあて先に送信するもので、当初はオンライン広告に必要な情報を吸い上げる目的で Claria 社が開発したが、それを悪用すれば個人情報やプライバシー情報をこっそり盗むことができる。スパイウェアでどれだけの個人情報が漏洩したかの実態はほとんど把握できていない。大手 ISP 業者 EarthLink の推定では、ネットワークに接続された PC の 90% にスパイウェアが入っており、1 台あたり平均 25 種類もあるという。

◆PC の盗難

個人情報を満載したノート PC の盗難は、どこの国でも頻発している。米国での最近の例をいくつか列挙する。カリフォルニア州の Delta 血液銀行で昨年 12 月に 10 万人の献血者の個人情報の漏洩、UCLA でも 14 万 5,000 人分の献血者の情報漏洩、UC Berkeley では 10 万人の卒業生、大学院生、過去の入学志願者の情報漏洩などなど。簡単な盗難で大量の情報が漏洩するので緊急の対策が必要だ。他人が簡単に情報を読めないような仕組みを記憶装置や PC に組み込むことは技術的には可能だから、そういった装置を広く普及させれば、これらのケースはかなり防げるはずだ。

◆プライバシーをどう考える？

ID 窃盗などの不法な手段だけでなく、普段の日常的な行動からも個人情報やプライバシー情報が他人の手に渡っている。たとえば、オンラインショッピングの先駆者である Amazon.com 社では、同社のショッピングサイトでの顧客の全行動をすべて記録している。それらのデータを分析すれば、顧客の好み、家族構成、交友関係、行動パターンなどプライバシー情報が分かる。ユーザは、それらの情報を使った行き届いたサービスを受けられる。それを高く評価するか、あるいは、気味が悪いと感じるかは、人によってさまざまだ。もちろん、相手がどの程度信用できるかによって感じ方はまったく変わってくる。

同様のことは Google などの検索サービスにもある。多くの人が便利なので Google の検索に頼っている。あまり意識せず使っている検索のキーワードや見たサイトの内容などのデータが記録されている。最近 Google 社は Google デスクトップ検索や G メールなど便利なサービスを積極的に提供して、多くのユーザを獲得しようとしている。実際に使ってみるととても便利だ。ただ、それらのサービス、特に G メールについては、プライバシーの面で問題があると指摘されている。Amazon.com 社の場合と同様に、個人情報を提供してカスタマイズすれば、

便利なサービスが使える。それを喜んで受け入れるか、プライバシーの侵害だと問題にするかは、なかなか微妙な問題である。

先進的なマーケティングの世界では共通して同じような情報収集と分析をするので、サービスを提供している企業の責任は重い。米国では、プライバシー規約なるものを利用者に同意させて、サービスを提供することにより、サービスを正当化している。このやり方がどの程度法的に有効かははっきりしない。

◆政府の対応

米国では、個人情報の盗難とそれを悪用した犯罪について、その被害額も含め、一括して扱うところはなく、FTC (Federal Trade Commission) が苦情や犯罪の届け出や報告をまとめているだけである。したがって、事件を報告しない企業もあるから、発表される数字は全体のうちの一部にしか過ぎない。

日本の個人情報保護法に相当する米国の法律は、1968 年に制定され、1984 年に改定された「電気通信プライバシー法」である。この法律は、それまでの通信傍受法を電子メール、携帯電話、コンピュータ通信などの電気通信手段に拡大して、プライバシー保護を適用させたものである。さらに広いプライバシー保護については、一般、オンライン、金融、医療など個別の分野ごとに法律が制定されている。それも連邦政府と州政府がそれぞれ別個に制定しており、込み入っている。州権の強い米国では、ID 窃盗のようなネットワーク犯罪の場合、犯人と被害者が別の州の場合がほとんどで捜査が難しい。それを改善する動きも始まっている。

インターネットが社会基盤になった現在、安全を支える技術がますます重要になっている。今後は、社会とのかかわりをもっと意識した研究開発が必要とされる。

参考文献、参考 URL

- 1) 松尾和洋：Web 世界を安全にする試み、情報処理、Vol.44, No.9, pp.970-971 (Sep. 2004) .
- 2) ID 窃盗の調査報告：http://www.javelinstrategy.com/reports/2005ReportBrochure.pdf
- 3) APWG サイト：http://antiphishing.org/
- 4) ファーミング紹介記事：http://www.wired.com/news/infrastructure/0,1377,66853,00.html
- 5) 検索サイトの問題点指摘記事：http://www.wired.com/news/privacy/0,1848,67062,00.html
- 6) ID 窃盗のより詳しい報告：http://www.jpssa.or.jp/info/04/20050405_us_it_softmarket.pdf

(平成 17 年 4 月 13 日受付)

【訂正】本年 1 月号に書いた「医療現場の情報化」で述べた連邦政府の医療関係の法律 HIPAA の制定は、1996 年でした。お詫びして訂正します。