神戸大学経済経営研究所
Research Institute for Economics & Business Administration – Kobe University
■コラム　RIEB ニュースレターNo.143　2014 年 10 月号

# 財産を守る

神戸大学　経済経営研究所
日本学術振興会　特別研究員 PD　佐藤　健治

2013 年 7 月から TBS 系各局で放送されたテレビドラマ『半沢直樹』は今世紀最高のドラマ視聴率を記録したそうだ[1]。放送から 1 年以上経った今なお半沢直樹シリーズの小説は書店で平積みになっているし、池井戸潤氏の他の文庫本が大きなコーナーを作っているところも多い。売れ行きは絶好調のようだ。今年の春、「もうそろそろミーハーとは思われないだろう」と思って読み始めた矢先にドラマ『ルーズヴェルト・ゲーム』の放送開始。やめるにやめられないのでブームに流されることにする。気づいたときには現在手に入る小説はすべて読んでしまっていた。とにかく面白いのだ。

池井戸氏の小説には銀行組織の闇を小気味良く描いた良作が多い。いくつかの物語に共通して現れていたためだろうか、大きな展開の中での小さな描写が強く印象に残っていた。銀行に個人情報に関する問い合わせをすると、電話番号を調べて折り返し連絡するようになっているというのだ。この描写をふと思い出したのは最近になって次のような話を聞いたからだろう。

Y 氏は所属先から機密性の比較的高い個人情報を送るよう指示を受けた。その所属先では VPN (Virtual Private Network) というインターネット技術を使って自宅と組織内ネットワークとの間に暗号化された通信経路を構築できる。さらに、特に機密性の高い情報については IC 職員証に埋め込まれた個人証明書によって認証を行うという二重のセキュリティが用意されている。このシステムをもって安全に登録できるはずの当の個人情報は、Y 氏が長期休暇中ということもあって電子メールで送ったのだという。

広く知られている話だが、電子メールが通信経路の全部で暗号化されている保証はない。部外者である以上、この個別の事例についてとやかく言うことはないが、難解でよく分からない新しい技術よりも使い慣れたものの方が信じるに値するという誤解は普遍的なようだ。技術者が「100%安全」と宣伝する訳にはいかないから一般ユーザーにとって学習意欲の湧くものではないのだろう。

---

[1] http://www.videor.co.jp/data/ratedata/junre/01drama.htm [2014 年 10 月 1 日閲覧]

一般論として、離れた 2 つの場所の間で情報をやりとりする際には、悪意の第三者の存在を無視することはできない。池井戸小説の電話対応であれば個人情報を不正に盗もうと「なりすまし」をする人物であり、インターネットであれば盗聴・改ざんを行う攻撃者である。池井戸小説における電話対応は、電話口の人物が本当にその人物かを確認するために（確実かどうかは別として）登録済みの電話番号にかけ直すか、あるいは顧客でなければ所属先の代表番号に掛けて当人を呼び出してもらう。Y 氏の所属先では、情報送信者と受信者のなりすましを防止するための認証技術と、盗聴や改ざんを防止する暗号化技術を用いた情報伝達の仕組みが提供されている [2]。

受信者の部分だけを取って比べてみれば、これらは同じ目的であることが容易に想像できるだろう。銀行では登録データの正しさが口座開設時の本人確認によって担保されているし、顧客でない場合は所属先が身元保証を行っている。一方で、ウェブサイトが認証機関による認証を受けていることをどれくらいの人が意識しているだろうか？

新しい技術に対する無自覚が社会問題に発展することもある。ウェブサイトのなりすましによる詐欺はフィッシングといって、不正なサイトの数は昨年ごろから急速に増加している。ID とパスワードやクレジットカード情報を抜き取るために本物によく似た偽サイトを作って誘導するのだ。平成 25 年度に確認されたフィッシングサイトは 2,522 件に上り [3]、インターネットバンキングによる不正送金事犯に関して言えば平成 25 年の認知件数 1,315 件、被害額約 14 億 600 万円と、この数年で大幅に増加している [4]。これを受けて日本の主要な銀行はウェブサイトで不正なサイトに注意するよう大々的に呼びかけるようになった。

---

[2] まったくの余談であるが、池井戸潤氏は暗号解読を物語に織り込んで小説『最終退行』（小学館文庫）を書いている。

[3] フィッシング対策協議会『フィッシングレポート 2014』 https://www.antiphishing.jp/report/pdf/phishing_report_2014.pdf . 日本でのフィッシングサイト数は世界的に見ればまだ小さいものであるが増加傾向を無視することはできない。 参考： APWG “Phishing Activity Trends Report 1st Quarter 2014” http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf

[4] 警視庁広報資料『平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について』 https://www.npa.go.jp/cyber/pdf/H260131_banking.pdf . 最近、2014 年 1 月から 7 月までの期間における京都府下の被害額が前年同期比のおよそ 7 倍に達したとの報道があった。全国的にも今なお増加傾向にあると見て間違いないだろう。 http://sankei.jp.msn.com/region/news/140917/kyt14091707030002-n1.htm [2014 年 9 月 22 日閲覧]

フィッシング詐欺に対する対策として周知されてきた方法は、ほとんどが標準的と言っていいようなものだ。あやしいリンクはクリックしない、ソフトウェアを最新版に保ち、個人情報を入力する際には暗号化の有無、サイトのアドレスや証明書を確認する。より巧妙な手口にはセキュリティソフトの対応を待つしかないだろうが、自分でできることがまったく無駄になる訳ではない。例えば、パスワードの使い回しをやめるだけで少なくとも被害の拡大を避けられる[5]。

もっとも重要なことは、犯罪の手口、その対策に関する新しい情報をときどき仕入れておくことだろう[6]。急速な技術革新の中に生きる私たちにとって自らの財産を守るためには新しい知識を身につけることが必要であり、それは同時に社会厚生に直結している。望ましい市場環境の下では自己利益の追求は社会全体を豊かにする。これはよく知られた経済学の命題であるし、言うまでもないことだが詐取が横行しているような世の中は望ましくない。財産を守るための学びは社会の豊かさのために必要なのだ。

---

[5] 何らかの方法で不正に入手された ID・パスワードを使って様々なサイトへのログインを試みる「パスワードリスト攻撃」の被害は継続的に発生している。独立行政法人情報処理推進機構と一般社団法人 JPCERT コーディネーションセンターは 2014 年 9 月 17 日より「STOP!! パスワード使い回し!!」キャンペーンを展開し、一般ユーザーへの呼びかけを行っている。
https://www.jpcert.or.jp/pr/2014/pr140004.html [2014 年 9 月 22 日閲覧]

[6] 今年は情報セキュリティのニュースが大きく取り上げられたように思う。ベネッセホールディングズの個人情報流出事件は言うまでもなく、より技術的な問題としては OpenSSL の Heatbleed 脆弱性の話題や、もっと最近では bash の脆弱性に関する話題が夕方のニュースでも報道されていたほどだ。