応専

9

菊池 浩明
東海大学

日本を元気にするセキュリティ技術

正直に告白すると，震災復興で日々の暮らしでさえ大変というときにICTも情報セキュリティもないだろうと思っている．震災のときには，電話よりもTwitterやSNSが役に立ったという話もよく聞いたが，それは少なくともネットが使える安全な場所にいた人たちの話で，被災地の様子や震災のニュースを入手するのに有益であっただけで，Twitterで壊れた道路が直ったり放射能汚染が止められたりしたわけではあるまい．私が専門とする個人情報保護やプライバシー保護技術は避難所の現実の前には消し飛んでしまう．それどころか，原発内部で遠隔操作のロボットは故障して止まったというし，インフラがないところで真価を発揮するはずのアドホックネットワークは使われたという話すら聞かない．重機を駆使して被災地への道を切り開くボランティアの力強さやネットワークを駆使して義援金を募る支援団体の活動の前で，ICTができることははるかに小さく，震災直後ラジオで繰り返し流れて子供たちを元気づけたアンパンマンマーチに遠く及ぶまい．

だから筆が進まないという言い訳から始めてしまったが，そんな後ろ向きの姿勢をしかるかのように，中央大の今井先生が「想定外」についての情報セキュリティの観点からの考察をされていた[1]．想定外の事態が生じたというのは，そもそも脅威の洗い出しが不十分でリスク評価が完全でなかったことを表しているのであるから，失敗の言い訳にはしてはならない．情報セキュリティ対策としてできることは，リスクや驚異の見落としを極力少なくするための暗号化のモデル化や適宜見直しをするループを作ることであるが，それでも暗号処理時間や電力消費量の観測から秘密鍵を推測するサイドチャネルアタックや偽造指紋によるバイオメトリクス認証装置のなりすましなどの「想定外」が示すように完全に安全にはできない．想定外を想定し，起こり得ることは起こると考え，我々が常に考慮しなくてはならない鉄則を，情報セキュリティの15の法則にまとめている．この15条だけでも面白いので一読を勧める．まったく同感である．言い訳をしている場合ではない．

情報セキュリティ技術が日本を元気にするためにできることは何か？　記憶の片隅に引っかかっていたのは，震災後の被災者登録に関する記事[3]であった．津波によって戸籍を含むほとんどすべての書類を流され，電子データを格納していたサーバは水没してしまった陸前高田の市庁舎や町役場での奮闘を綴ったものである．遺体の火葬許可手続きという急を要する悲しい手続きから，震災中の希望となった出生届，日々の暮らしに必要な金融機関に本人を証明する身分証明．震災直後に市庁が果たすべき役割は多い．仮庁舎では，急ごしらえでデジタルカメラの写真に町長の割り印を押した手作りの本人証明書で対応したり，近郊の役所に代用の書類発行の応援を頼んだりしたという．頼りになるはずの住民基本台帳の電子データはサーバとともに水の中に消え，業者のバックアップに残っているやや古いデータを元に復元にあたったというくだりが，ICT技術者のはしくれとして悲しい．

情報セキュリティ，信頼性工学の基本に帰るならば，データベースは十分な冗長化を行い，十分に分散した施設で安全に管理されていなくてはならない．耐故障性を備えた近郊の役所や出張所でも，被災した庁舎と同等のレベルで均一のサービスを提供できなくてはならない．さらに，最新の技術を考えるな

らば，十分な帯域を備えたネットワーク環境でクラウドコンピューティングによるサービスが導入できるだろう．クライアント側の負担を低減して，ネットワークさえ復旧すればサービスが機能するというクラウドが市庁舎にあればいいのに，とすぐに連想した技術者は私だけではあるまい．防災に優れた各種住民サービスを提供する電子的な役所の設計を，この機会にこそ考えるべきであろう．

すぐにでも適用できるICTもある．住民基本台帳ネットワーク（住基ネット）と共通番号制度「マイナンバー」の活用である．2011年12月28日の朝日新聞は，福島第一原発事故の福島県の住民150万人への賠償金の支払いに，東京電力と経済産業省が住基ネットの活用を検討していることを報じている[4]．150万人という膨大な数の申請書を処理するためには大規模なコールセンタが必要になる．そこで，住所，氏名，生年月日，性別が登録されている対象地区への在住の証明が容易な住基ネットに着目して，被害者が住民票の写しを用意することなく，賠償金の請求をできるようにしようというものである．住基ネットには本来，個人情報の流出と目的外利用を禁止する原則があるが，市町村が個人情報保護条例を改正すれば適用できる．東京電力という一企業が情報管理を厳密に実施し，法令順守に努めることが条件であるが，震災対応で余裕のない東京電力にとっても渡りに舟であろう．住民も住民票のために何度も市庁舎に足を運ぶ必要はなく，ウィンウィンではないか．

便利な仕組みには裏側があり，拙速に進めては歯止めが効かなくなる，という慎重論もある．ならば，なおさら，現在検討が行われている共通番号制度（マイナンバー）の検討を進めるところであろう．2011年6月の「社会保障・税に関わる番号制度に関する実務検討会」では「社会保障・税番号大綱―主権者たる国民の視点に立った番号制度の構築―」を公表して，年金，医療，福祉，税務を用途とする共通番号＝マイナンバーを発表している．関連法案が通れば，2015年に利用が始まる．内部犯によるマイナンバーの漏えいに対しては，リンクコードと呼ぶ一時的な符号を発行して使い捨てにする情報連携基盤と監査を行う第三者機関を主な対策として提言している．技術的な中身や背景は，文献2）が詳しい（私のつけ焼き刃もこの本の受け売りである）．セキュリティ屋のはしくれとして，国家による情報統制やプライバシー侵害のリスクは承知しているが，すでに日本は震災の痛手から脱原発への舵を切った．プライバシーと震災に強い元気な社会のためには，今度はマイナンバーに対してもその利用の覚悟を決める必要があると考える．

そもそも，e-Japanをうたって進めてきた電子政府の現状は満足いくものではない．インターネットの黎明期に夢見たような，すべての電子メールに公開鍵証明書による署名を付けて正式に利用できる社会になったというのに，（私の場合）その機会は年に1回の確定申告のe-Taxに限られていて，ほかに利用することは許されていない．自治体ごとに異なるICカードを購入しなくてはならず，引っ越ししたらカードリーダを買い替えなくてはならない．ブラウザにすでにVeriSignの認証局が設定されているのに，公的個人認証の発行者となる地方自治体が自己署名したルート証明書を新たに登録しないと使えない．公開鍵証明書の中に入っていると思っている貴方の名前は単なるコメントで，所有者名（Common Name）には申請時刻が無味乾燥に格納されている．これでは，証明書の中の公開鍵が泣いていよう．リスクを恐れず，「想定外」を想定し，安全に安心して暮らしていくための真の電子政府を今こそ再設計すべきであろう．

電子化の推進とともに忘れてはならないことがある．被災者のプライバシーである．2011年10月，福島県の18歳までの子供たち36万人を対象とした甲状腺検査が始まった[5]．食品から取り込まれた放射線ヨウ素は甲状腺に集まり，子供は特に甲状腺がんになりやすいと言われているためである．対象は震災当日に0歳から18歳だった全県民で，県外に避難しても対象に含まれ，検査は定期的に生涯続く．発病のリスクだけではなく，この子供たちが受けるかもしれない偏見や差別，根拠のないいじめが心配

でならない．現に，赤十字血液センターの献血制限を誤解した検診医によって，福島県出身者が献血を断られる事例が起きている[7]．かといって，低放射線と疾病の相関を正しく知ることは，被災者の健康管理や医療対策のためには必須の重要な機微情報である．疫学調査は止められまい．この相反する要請を満たして子供たちのプライバシーを守るためには，最強の情報セキュリティ技術が必要である．単なるメールアドレスが配送間違いで漏えいしたのとはわけが違う．

そのセキュリティ技術には，前述したリンクコードなどの追跡を防止するプライバシー保護に加えて，暗号プロトコルによるプライバシー保護データマイニングがあげられる．この解説については，たとえば文献8）に譲るが，代表的な手法は準同型性を満たした公開鍵暗号技術を組み合わせて，データを秘匿したままでさまざまな解析アルゴリズムを適用するものである．その実現のためには入力データの各ビットに高度な暗号化を施すなどの計算コストや大規模な記憶装置が必要な点が大きな課題であったが，疫学調査はそれだけのコストに値するプライバシーである．入力データを秘匿したままで検査ができるのならば，生活習慣や各種の医療データについてのさまざまな相関をきめ細かく明らかにして，より精度の高い医療モデルや治療に活用されることが期待されている．我々の研究グループでも，低放射線従事者のリストとがん罹患のリストを入力にして，そのがん率が公開されている一般的な率と比較して統計的に有意かどうかだけを判定するプロトコル[6]を提案して，この研究を始めたところである．

さて，アンパンマンマーチに勝てるか情報セキュリティ．

参考文献

1）今井秀樹：情報セキュリティと「想定外」，IEICE Fundamental Review, Vol.5, No.3, pp.198-204 (2011).
2）前田陽二，松山博美：国民ID制度が日本を救う，新潮新書 (2011).
3）「戸籍を，埋葬を／住民データも水没，庁舎なき役所奮闘　東日本大震災」，朝日新聞，2011年3月27日朝刊，p.31 (2011).
4）「賠償に住基ネット活用／東電・経産省・事務量削減狙う」，朝日新聞，2011年12月28日朝刊，p.1 (2011).
5）「子ども甲状腺検査開始／福島36万人対象・生涯継続」，朝日新聞，2011年10月10日朝刊，p. 38 (2011).
6）佐藤，菊池，佐久間：プライバシーを保護した放射線疫学調査システム，情報処理学会研究報告，Vol.2011-CSEC-54, No.25, pp.4-7 (2011).
7）「福島男性の献血を「拒否」／「遺伝子に傷」という誤解」，AERA，2011年6月13日，p.24 (2011).
8）Vaidya, J., Clifton, C. W. and Zhu, Y. M. : Privacy Preserving Data Mining, Springer (2006).（嶋田　茂，清水將吾による和訳あり，シュプリンガージャパン，2010).

（2012年1月23日受付）

■菊池 浩明（正会員）　kikn@tokai.ac.jp
東海大学情報通信学部教授．博士（工学）．CSEC研究会前主査．ネットワークセキュリティ，暗号プロトコルの研究に従事．本会フェロー．