電子政府-電子自治体の「安全性」問題
――ヌーワー報告への検閲に「技術」はどう答えるか

西邑　亨
（JCA-NET）

「ハッカー」レポートへの総務省の検閲

2004 年 11 月 12 日、東京で開かれたネットワーク・セキュリティに関する国際的な技術セミナー（pacsec.jp/core04：主催は日本事務局の（株）SIDC、およびカナダの dragostech.com。総務省や日本ネットワークセキュリティ協会などが後援）で、総務省の強い「要請」を受けてひとつの技術レポートの発表が中止された。ネットワークセキュリティ・コンサルタント（ハッカー）のイジョビ・ヌーワーさん（アメリカ／セキュリティラボ・テクノロジーズ社 CTO：最高技術責任者）が予定していた、「Inside Juki Net」と題するレポートだった。

事前に配布されたセキュリティラボ・テクノロジーズ社の日本語プレスリリースによれば、この技術報告の内容は、彼が技術スタッフとして参加した長野県の「住基ネットに係る市町村ネットワークの脆弱性調査」（安全確認実験。2003 年 9～11 月実施）の結果をふまえた「住基ネット」の情報セキュリティに関する技術報告という。

朝日新聞（2004 年 11 月 12 日）などは、総務省が同報告の「修正」を求めた主要な理由を、

・住基ネットと庁内 LAN を混同している。
・脆弱（ぜいじゃく）性を具体的に示すおそれがある。

の 2 点だったとしている。

このうち後者については、実験実施スタッフであったヌーワーさんの長野県と交わした守秘義務契約の存在について総務省は十分認識している。しかし「守秘義務」の範囲を合理的論理的に判断することで「住基ネット」に関する情報をできるだけ開放的に扱おうとする長野県と、これを行政側が完全にコントロールすることで情報を閉鎖的に扱おうとする総務省（市町村課）の間には、大きな温度差がある。ヌーワーさんは発表が中止されたセミナー当日の記者会見で、「私はプロのセキュリティ・コンサルタントなので、日本の市民のセキュリティを損なうことはしない」と語っていた。アメリカ的なビジネス常識では、それですむことだ。

古くからある官僚的体質の問題――日本社会全体に見られる説明責任が定着していないという状況の典型的な事例といえるだろう。むろん、こうした不規則的な行政によるコントロールが今回有効に働いてしまった要因は、この技術セミナーを総務省が「後援」していたことにあった（そのコントロールを受け入れなければならなかった日本側主催者、SIDC の事情も、一部で指摘されている）。朝日新聞に対して総務省は「内容は総務省が後援している以上、適当でなかった」と語っている。

しかし前者の「要求」――「住基ネットと庁内 LAN の切り分け」は、「住基ネット」の安全性／危険性を考えるとき、技術的にはより本質的な問題を含んでいる。住基ネットに接続されている「市町村庁内 LAN」に情報セキュリティ上の脆弱点が発見されたことを、「住基ネットの脆弱性」と考える必要があるか否か、という問題だ。これはそのまま、国と自治体が相互接続されるネットワーク――「電子政府-電子自治体」全体の情報セキュリティ強度の確保や、個人情報保護／プライバシー保障の問題でもある。

明確ではない「住基ネット」の範囲

情報セキュリティ強度を評価する上で、「住基ネット」と「市町村庁内 LAN」を別の存在としてとらえる考え方は、「住基ネット」の設計／構築を主導した総務省市町村課に顕著な考え方だった。すでに、2003 年 12 月に長野県が安全確認実験の中間報告を公開したとき、総務省の反論としてこの考え方は強く打ち出されている。

「……実際に住基ネット本体へは侵入されておらず、また、指定情報処理機関の本人確認情報はまったく問題ない状況であるにもかかわらず、庁内 LAN の脆弱性を住基ネット本体の安全性の問題であるかのように取り上げるなど、事実と異なる情報が喧伝されている。」（「長野県が実施した『市町村ネットワークの安全性調査』を受けての対応」2003 年 12 月、総務省住民基本台帳ネットワークシステム調査委員会）

「住基ネット」ということば――それは、技術的には「システムとして考慮された全体」を指すはずだが――と、ここで使われている「住基ネット本体」ということばは、実は明確に使い分けられていない。

確かに、管理・運営を委託されている（財）地方自治情報センターの直接コントロールが及ぶ範囲を区切ることは可能だろう。その範囲は、確定しにくい部分もあるが、とりあえず全国サーバー・全国ネットワーク・都道府県サーバー・都道府県ネットワーク・市町村の都道府県ネットワーク側ファイヤーウォール（県調達ファイヤーウォール）などということになる。だからこれを総務省のように「住基ネット本体」と呼ぶことには、「制度的な根拠」があるのかもしれない。

「住民基本台帳ネットワーク基本設計書　第 2 版」（2000 年、（財）地方自治情報センタ

ー）の記載範囲は少し広く、長野県の実験で脆弱性が指摘された CS サーバーや CS クライアントほかを含んでいる。しかし最近の総務省の発言では、CS サーバーや CS クライアントを含まないとしているように見える。

いずれにしろ、例によって「玉虫色」だ。

「ネットワーク」の考え方

とはいえこの議論は、「住基ネット」の情報セキュリティ対策の視点からはさほど意味のある区分ではない。厳重なセキュリティ対策を実施している企業や国の機関のシステムは、しばしばインターネットからの侵入を受けているが、侵入者は企業などの管理範囲外にいる。

「住基ネット」の CS サーバーと通信をしている既存住基サーバーは、市町村の庁内 LAN に置かれている。庁内 LAN の情報セキュリティ対策が、（ファイヤーウォールの向こう側にある）CS サーバーや都道府県サーバー、全国サーバーなどの情報セキュリティ対策（運用されている個人情報の保護）において考慮されなければならないのは、いわば技術常識の話だ。

現実に運用されている全国規模の行政システム（住基ネット）において、情報セキュリティ対策における「制度的な区分」と「技術的な連続性」の間での対立（少なくともヌーワー報告が中止されるような齟齬）が起きている。だが、この対立は、民間が主催する国際的な技術カンファランスの報告をブロック――検閲するほど緊張した（本質的な）「対立」なのだろうか？　私には、そしておそらく情報通信技術に関心を持つ日本の市民の多くにも、とうていそうは見えない。

報告を封じられた当事者であるヌーワーさんは、彼の Web サイト（英語サイト：http://www.ejovi.net/）で次のように書いていた。

「私はただそのシステムを改善し、より安全にするために、何がベストかを提唱したかっただけです。しかし総務省は、その安全性をいかに改善するかということに限った提案が、住基ネットが問題点を持っていることを示すものだと思いこみ、これ（住基ネットに問題があることそのもの）を認めることを拒否したのです。彼らに言うのは残念だが、しかし住基ネットには確かに問題がある。しかし同時に、良いニュースとしては、そのような技術的問題は容易に解決できるということだ。」（住基ネット差し止め訴訟弁護団仮訳。以下同じ。カッコ内は訳注）

システムやネットワークは、常に情報セキュリティ上の脅威を受けており、それを完全に免れることはできないだろう――これが、技術の側が前提とする考え方だ。そして「住基ネットには確かに問題がある」が、実験で見つかった「問題は容易に解決できる」というのが、彼の技術者としての結論だった。しかし彼は、今回の「検閲」の経過を受けて次

のような（技術論を越える）指摘を、彼の結論に追加せざるを得なかった。

「しかしながら住基ネットの最も大きな問題は、技術的なものではなく、問題があること自体を総務省が認めないことだ。もしも、政府が問題点を指摘する者に耳を傾けようとしないならば、システムはどうやって安全になるのだろうか？」（同前）

「行政」の考え方

「庁内 LAN」の脆弱性が、「住基ネット本体」の脆弱性とは関係がないかのように取り扱おうとする総務省市町村課の態度を、技術的な発想で理解することはおそらくむりだ。そこには、システムとしての物理的論理的な連続性があきらかに存在しているのだから。

とはいえ、総務省市町村課のセキュリティ対策の重点が「市町村庁内 LAN」に向けられていることはよく知られている。市町村課は早い時期から、自治体自身の手で情報セキュリティの状況を自己点検するために「チェックリスト」を提供し実施してきた。補助金の支給や職員研修の実施を含むいくつかの自治体支援も行っている。

彼らは「庁内 LAN に問題がある」ことは否定していない。むしろ対策の強化を支援している。そして、それらが「住基ネット本体」の脅威となっていることも「承知して」いる。ただしこの問題は、「行政区分上は、あくまでも自治体の問題」（自治事務上の問題）なのだ。だから、この問題をほんとうに理解していないのは市町村の側だ。

そして、「住基ネット」の運用を円滑に継続するためには、「市町村の理解」は大きな障害になる。「住基ネット」に脅威を与えていることを市町村が理解しその対策に自らの責任（資金）と判断（能力）で取り組もうとすれば、「資金難」と「技術能力の不足」による早期対策の不能のために、一部の自治体は「住基ネット」への接続を断念（切断）せざるをえない。多くの関係者が指摘するように、現在のようなシステム設計がされた「住基ネット」に参加するには、総合的なシステム運用能力が不足している市町村は多数ある。その動きは、主要な「国-自治体をつなぐネットワーク」である LGWAN（総合行政ネットワーク）などにも影響する。従って、国・総務省の政策全体が大きな影響を受ける。

差し迫った個人情報漏洩の危険－－吉田証人尋問

今から考えれば、このヌーワー報告中止事件の予兆は、10 月 15 日東京地裁で開かれた「住基ネット差し止め訴訟」（第 1 次訴訟。原告は斎藤貴男さん、被告は中野区、東京都、国、（財）地方自治情報センター）における吉田柳太郎さん（長野県の安全確認実験の実施監督者）の証人尋問に現れていたのかもしれない。

この証人尋問は、昨年末になって裁判長が、「原告の個人情報が漏洩する差し迫った危険がなければ、早期に結審したい」とする方針を示したことへの、原告・市民側の対応として提案されていた。いくつかの紆余曲折があったが、結果的には、当時大きな注目を集め

ていた長野県の安全確認実験の結果が、2004 年 7 月になって県から東京地裁に証拠として提出されたことを受けて、法廷が採用した中立的な証人として吉田さんが証言することになった。

この証人尋問で注目されたのは、被告国側が、長野県の実験結果に対してどのように反論するか――実験が指摘した主として「庁内 LAN の脆弱性」が「住基ネット」（本体）の「危険性」を示すものではないことを、どのように立証しようとするか、だったと言えるだろう。これが成功すれば、長野県の実験結果は何ら「住基ネット本体」における「差し迫った個人情報漏洩の危険」を証明するものではなく、単に「市町村の庁内 LAN における脆弱性の問題」だということになる（と、総務省市町村課は主張するだろう）。

実際、被告・国代理人の証人尋問は、一貫して、

・「住基ネット」（本体）に対する侵入は行われていない

ことを立証（むしろ強調）する内容だった。吉田証人らの実験内容は、国の言う「住基ネット本体」に対しては「ノックすらしていない」範囲のものだったから、彼らの意図はあらかじめ満たされることが予定されていた。

「行政の考え方」によれば、吉田証人の証言は、「住基ネット本体」に対する脅威を論理的に推定させるもの――「可能性」を指摘しただけに「すぎない」。裁判所の示した考え方は「差し迫った個人情報漏洩の危険」の立証だから、被告・国側の主観（「行政の考え方」）によるなら、被告に有利な証言が得られたことになるのだろう。

「可能性」と「危険性」

法廷証言後吉田さんは、「『可能性』という言葉を法廷で何回も使いましたけど、それは『危険性』という言葉で表現した方がよかったかなぁと、すごく思っています。」と述べている。

「原発の裁判でも、ことごとく国が勝ち続けてきたけれども、現実に原発は臨界事故を起こしたし、冷却パイプが破断して被爆したり死んだ人もいる。『0.00001％の可能性は、危険性じゃないんだ』と国は言ってきたことになるのだけど、実際に問題が発生して人の命も失われてしまった、多くの人が被爆してしまった。

『危険性』というものの次元は『原発』も『住基ネット』も同じだと思う。『裁判勝ったけど、ごめんね。0.00001％だけど事故起きちゃったんだ、まちがってました！』と言わなければいけない。結果がどうあれ、ゴメンナサイすることによって広く問題を認知するということがだいじだと思うのですよ。そこからアクションが起こるのですから。」

「問題が認知されない」という指摘は、ヌーワーさんのメッセージの中にもあった。重ねて引用しておこう――「しかしながら住基ネットの最も大きな問題は、技術的なものではなく、問題があること自体を総務省が認めないことだ。もしも、政府が問題点を指摘する者に耳を傾けようとしないならば、システムはどうやって安全になるのだろうか？」

「可能性――論理的推測」は、「危険性」を定量的に評価するひとつの指標だ。「個人の意図的な侵入・漏洩」といった偶発性に強く依存する情報システムのセキュリティでは、なおのこと「危険性」は「論理的推定 ――可 能性」の中にしか存在しえない。安全への道はいつも、「問題の認知」から始まる。

＊吉田柳太郎さんのセキュリティ論については『地域住民と自治体のための　住基ネット・セキュリティ入門』（吉田・西邑著、七つ森書館刊、2004 年）参照。

行政による「100%安全はない」の理解

「行政の考え方」が変わってきている兆候もないわけではない。たとえば「電子政府推進シンポジウム 2004 東京」（セキュアな電子政府を推進する会主催、毎日新聞社など後援）における元官房副長官石原信雄さんの発言に、毎日新聞はこうコメントする。

「石原氏は『反対派には 100%完璧でないと駄目だという意見もあるが、ある程度まで（安全性が）行き、大局的にみて住民のサービスレベルを向上させるなら技術を導入する決断が必要だ』と述べた。

一昨年から昨年にかけて、住基ネット導入にあたり片山虎之助総務相（当時）は、『住基ネットはクローズドで安全』と繰り返し主張。反対派に対しては『あらぬ想定をして、安全ではないとか世の中を惑わす』と切り捨てた。住基ネットへの賛否はともかく、セキュリティーに万全はないのは常識であり、こうした主張を続ける総務省を批判する声が出ていた。石原氏の発言は、官僚社会でも、ようやく当たり前の意見を人前で出せる風潮の表れであり、今後、議論の深化が期待される。」（毎日 Interactive、2004 年 10 月 6 日）

「今後の議論の深化」を、私も期待している。

実際問題として、昨年秋以降、国はすでに片山総務大臣の路線から転換していた。前述したように、「市町村庁内 LAN の脆弱性」は、政府によって認識されている。現在の問題は、「技術を導入する決断」を下すための「セキュリティ強度の要件」（対策と監査の要件）および「残余リスク」を地域住民（個人）が引き受けざるを得ない事実を行政側がどう認識するかというところにある。そしてこの「決断」をする（責任を負う）のは誰か？ ――国か都道府県か市町村か、それともデータ主体者である地域住民か？ ―なのだ。

とはいえ、あいかわらず「行政の考え方」は支配的だ。「ネットワークの考え方」は見えていない。政府関係者が示しているものは、「物理的論理的な連続性」によって「市町村庁内 LAN の脆弱性は住基ネット全体の脆弱性につながる」という事実の認知ではない。それは、「100%安全はないが、住基ネット本体はある程度まで（安全性が）行っている。市町村庁内 LAN には問題があるので対策を実施している」というレベルを越えない。市町村の

対策がある程度進んだとして、「住基ネット」（全体）について「ある程度まで（安全性が）行く」のはいつのことなのだろうか？

市町村の数は現時点で約 3000 ある。「統一的均質的なセキュリティ構築」を行うとした総務省市町村課の戦略（「住基ネット推進協議会」の決定）は、「3000 の自治体のそれぞれの事情」によって破綻しているが、これに代わる戦略、実効的な方法論は市町村課にはない。

技術を持っているのは政府ではない－－展望

原発問題や医療問題などで典型的なように、従来の課題では、「技術」（技術者）は明らかに政府のコントロール下に置かれていた。そこでは、「技術論」ではなく「政策論」がすべてを決定している。

しかし、新しいネットワーク技術の分野では、そうした関係はまだ未成熟だ。長期にわたって情報通信技術の供給を大手エレクトロニクスメーカーだけに依存してきた政府、少なくとも情報通信政策を所管する総務省は、IT 技術の主力を担うベンチャーやその技術者集団に対する影響力をまだ確立していない。

電子政府-電子自治体の構築を軸とする e-Japan 戦略の遂行に必要な技術は、主要に、ベンチャーたちが持っている（従来の大手エレクトロニクスメーカーは、技術的に「遅れている」がために衰退した）。現在ベンチャーの囲い込みが日本政府によって精力的に進められているが、電子政府による「『特需』見込めず」と日経新聞（2004 年 8 月 24 日）が論評する状況で、技術も技術者も「行政の考え方」にやすやすと囲い込まれるわけにはいかない。国際的な技術とビジネスのリアリズムの中で、新分野の「技術」が容易に囲い込めるものではないことを、日本政府は切実に理解することになるかもしれない。

いずれにしても、ベンチャーとその技術者に彼らの技術論の正当性を担保するのは、「住基ネット」に限って言えば、本人確認情報の「データ主体者」―地域住民なのである。

追記　イジョビ・ヌーワーさんは、その後総務省に対して、「表現の自由」を侵害したとして国家賠償訴訟を起こした。また、吉田証言に対して被告国側は、反論のための新たな承認を申請することはないとの方針を、11 月末の東京地裁における進行協議で示したとのこと。

掲載：月刊「技術と人間」2004 **年** 12 **月号**

（株）技術と人間　電話 03-3260-9321