宇治市の住民情報データ流出事件を経験して

――― 住民情報データ流出事件の教訓 ―――

木村　修二

はじめに

宇治市では、９９年５月に２１万件の住民情報データが流失していたことが発覚した。古典的で幼稚な不正行為であったので、発覚から約１週間で、流失ルートの解明からデータの回収・消去までを行うことができた。市では再発防止策をまとめ、制度的な保障としての個人情報保護条例の改正と、実態的な保障としての情報セキュリティシステムの構築に取り組んだ。

この事件発覚直後から再発防止策をまとめ推進してゆく過程で考え続けた。一体何に失敗したのか？どう対応すべきか。

１．「情報セキュリティ」への疑問

（１）事件発覚直後からマスコミは、「個人情報のずさんな管理で流出」という表現が跋扈した。また識者のコメントとして「信頼できる事業者の選定」に失敗とか、「本番の生データの持ち出し」を批判されることが多数見受けられた。しかしこれらは、事件が起こったという結果から原因を語っている結果解釈でしかなく、再発防止策にはならないことに気づかされた。同じことを行っている数多くの自治体では事故が発生していないのだから。

宇治市が全国最下位のセキュリティ水準であったなら、事件発生は自業自得と納得もいくが、悪くても全国平均値程度ではあったと思っている。世界最高の堅牢さを誇るところでも事件は発生の報道も目にすることがある。情報セキュリティの水準と故の発生とは相関関係があるかと考えれば、相関関係を見出すことができない。情報セキュリティの向上に努めても事故は防止できないことになる。

事件のあと当然のごとく再発防止策に取り組むが、しかし情報セキュリティを向上させれば事件は防止できるのか、という基本的な疑問を抱いていた。

（２）再発防止策は対症療法的であってはならないし、事件はなぜ発生したのか、なぜ事故が起きたのか、因果関係を解明しつつ、普遍化することを通じて、根源的な再発防止策を構想することを想定した。しかし、事件発生の個別具体的な、因果関係のある根拠は見出せなかった。結局、くだけた言い方になるが、「悪い奴がいた」「悪いことができる環境だった」という、ごく一般的な２つの条件がそろえば事件はどこででも起こると理解せざるを得なかった。だから再発防止策はこの条件を排除することが課題となった。「悪い奴」を排除できればいいが、職員だけでなく委託業者の社員その他

多くの人が関わるのであるから、また職員研修が全職員すべてに浸透して意思改革を達成できると想定することは不可能としか思えないことから、たった１人の「悪い奴」を排除する手法たりえない。だから、「悪いことができない環境」を技術的セキュリティで最大限に構築し、やむを得ない部分だけ、強力な抑止力で対応することを再発防止策の基本とした。マネジメント系の情報セキュリティを後景に退け、技術的セキュリティに前面に力を傾注した。

（３）情報セキュリティの水準と事故の発生とは相関関係がないし、情報セキュリティの向上に努めても事故は防止できないのは、事件は管理者側の対策よりも攻撃者側の要素、つまり「攻撃者の執着心と技術力」によると理解した。だから、攻撃を「できなくする」ことが可能であるならば、事件を防止することができる。それが「悪いことができない環境」ということである。

システム管理者が自らの権限だけで整備できる領域が唯一対応可能な領域である。それ以外の領域には無限の脅威が存在する。だからこの領域を完全に分離することからはじまる。だから一般に語られる情報セキュリティの体系ではなく、実効性のある別の体系を模索せざるを得なかった。

２．「情報セキュリティ」の理念の再確認と直後の対応

自治体の情報管理の原則は、情報公開制度と個人情報保護制度である。これらと無関係に情報セキュリティといわれるものがあるわけがない。

被害者（情報主体）の意思を考慮せずに、加害者（情報保有者）だけで対策を考えることにはならないし、情報セキュリティは、情報主体の権利保障を内包しなければならない。だから、情報公開条例・個人情報保護条例の下に情報セキュリティを構築すべきであると再確認した。

（１）情報セキュリティの理念

情報主体のプライバシーの権利を保障すること、それに市民の知る権利を保障すること、これが情報セキュリティの目的である。だからプライバシー保護制度から情報セキュリティシステムに要請される課題は、機密性・完全性・可用性といわれる自己完結的な内部統制系統だけでなく、これに、外部にいる情報主体（市民）の自己情報コントロール権を貫徹し、その意思・コンセサスに基づいて内部統制をさせることである　さらに外部の情報主体が、自らのどんな個人情報が蓄積され、どう管理され、どう利用されているかを、自らが監視できなければならないと考えた。

（２）だから、情報主体が安心して自らの個人情報を提供できるためには、情報主体が自ら安全性を判断するための情報（セキュリティ情報）をすべて開示しなければならない。また、情報主体がセキュリティの水準を決定し、情報保有者は、情報主体の意思に従って、それを実現する。これがデータ保護からプライバシー保護への転換であると考えている。

（3）特に留意すべきは、情報システムの導入によりその利便性等の利益を享受するのは情報保有者であるが、その情報化による個人情報漏洩の危険性を負担するのは情報主体であるということである。情報主体にとって利便性を感じられない情報システムでは危険性だけを負担させられることになる。このような関係のもとでは、「１００％のセキュリティはない、事故は起きる」ということはできない。またセキュリティと利便性はトレードオフの関係だからということもできない。これでは情報主体の理解はられない。

（4）個人情報が流出したことが発覚したとき、まず考えることは被害がどこに発生するか、どう救済するかである。情報主体である市民１人１人にどんな被害が発生するかは情報保有者は想定できない。市民の個人情報を流出させ、流通をコントロールできなくなったのであるから、あとは市民自らで防衛していただく以外に方法はない。すべてを公表し１人１人に防衛をしていただかざるを得ない。事件の概要や流出経路等だけでなく、流出したデータの元データが保存されていたので、各個人に流出したデータを開示した。

組織の利益を優先するのではなく、被害者である市民の利益を優先し、すべてを公表することにしたのである。

3．事件はなぜ起きたか、なぜ続発するのか

① 企業に大量の個人情報の需要があるから、供給されているだけである。不正であるか否かに関わり無く、需要があるから供給される。このような不愉快な社会を変しないかぎり個人情報流失事件はなくならない。だから情報セキュリティの取り組みは、再発防止策のごく一部でしかない。

② 爆発的な情報化の進展の基礎的な技術であるインターネットの技術それ自体が脆弱性を抱えている。

③ 特に深刻なのが、危険なアプリケーションが日々量産され、稼動していることである。

このように個人情報漏洩事件の発生の原因は社会システムにあるから、情報保有者が個別に情報セキュリティの対策を進めるだけでは不十分である。

4．技術的セキュリティシステムの体系化をめざしての試論

（1）磁気情報とそれ以外の情報の対策の体系は異なる。また大量漏洩対策の体系と少漏洩対策の体系とは異なる。まず最も危険な磁気情報の大量漏洩対策を機軸とする。

大量漏洩は、紙にプリントするか、外部媒体に書き出すとか、ネットワーク上に書き出すとか、「書き出す」ことで発生するのであるから、最後の出口を規制する。

自治体の保有する情報は、ほとんどが市民の個人情報であるから、重要性のランク付けを行い、取り扱いに差を設けることは有効ではない。どの情報を守るか？と問う

ことから始めるのではなく、自らの権限で整備できる範囲にあるネットワーク全体というように、物理的に守るべき範囲（ＬＡＮ内部）を確定することから始める。情報という形のないものは守れない。情報を搭載しているもの、つまりパケットも含めた機器類・媒体を守ることで、結果として情報が守られるのである。

このようにすることで安価でシンプルなシステムになったと考えている。

（２）庁内ＬＡＮのどこに個人情報漏洩のリスクが存在するかは、個別のリスク分析ではなく、どこのＬＡＮにも妥当する普遍的課題を克服することからはじめる。

通信しようとしている機器の相互認証と、データ部の暗号化、ＩＰアドレス隠蔽、パケット改ざん検出、送信元なりすまし回避、リプライ攻撃防止などである。さらに後述するが、マイＩＰアドレスによるルーティグで、アクセス規制を行うこと、また無許可パケットを排除するなど、通信での対策が可能な範囲は広くかつ安価で強力である。

次に、クライトンアトの機能制限を行うが、これはクライアントの機能を一旦剥したのちに、操作者個人が有する権限にあわせて、クライアントの機能を付与する。さらに、外部媒体への書き出し、ネットワーク上への書き出しをできなくする。

このような組み立て方を「図　具体的な手法の体系図」に示す。これにそれぞれのでの深さが付け加わるのであるが、たとえば、操作者認証３系統にするとか、より堅牢なセキュリティソフトを導入するとかである。

（３）無限の脅威を有限の脅威へ

「無限の脅威」を「有限の脅威」に転換する手法を施し、「有限の脅威」に対する防止策を講じる。防止策が不可能な部分は局所化し、別系統の強力な抑止策を施す。

１）無限の脅威

無限の脅威は管理下にあるＬＡＮの外と内にある。インターネットと接続した場合には、世界の向こうに匿名の無限の脅威が存在する。イントラの中には管理者が許可していない機器が接続されることで匿名の無限の脅威が発生する。誰が何をどんな技術でしようとしているかが全くわからない。

２）外部の無限の脅威

自らの管理下にないネットワークと接続する場合には、その先に無限の脅威がある。不正侵入が行われても仕方がない接続と位置づけた。無限の脅威に対する防衛であるから相手方を想定することができないので対応のしようがない。あえて対応しようとすれば、多額のコストを投入し、今現在採用できる最大限の防衛策を施すことになるが、いたちごっこといわれる対策に追われることになる。無限の脅威から防衛することは「あきらめる」という手法が最も現実的でかつ有効であると考える。

この対応は間違っているとは考えている。しかし他に対応策が思いつかなかった。安全なインターネットへの接続の方法を求めて検討を続けたい。

3）ＬＡＮ内部の無限の脅威

イントラは管理下にあるので、まずこの特定の「許可を受けた人」しか参加できないような仕組みを構築する。無許可の機器を接続できなくすること、または無許可の機器が送信するパケットを消去することができること、パケットが解読できないことが実現できれば、内部の無限の脅威は排除することができる。

ＬＡＮ内部のサーバだけを守ろうとした場合には、ＬＡＮ内部の無限の脅威を抱えつづけることになる。

4）有限の脅威へ

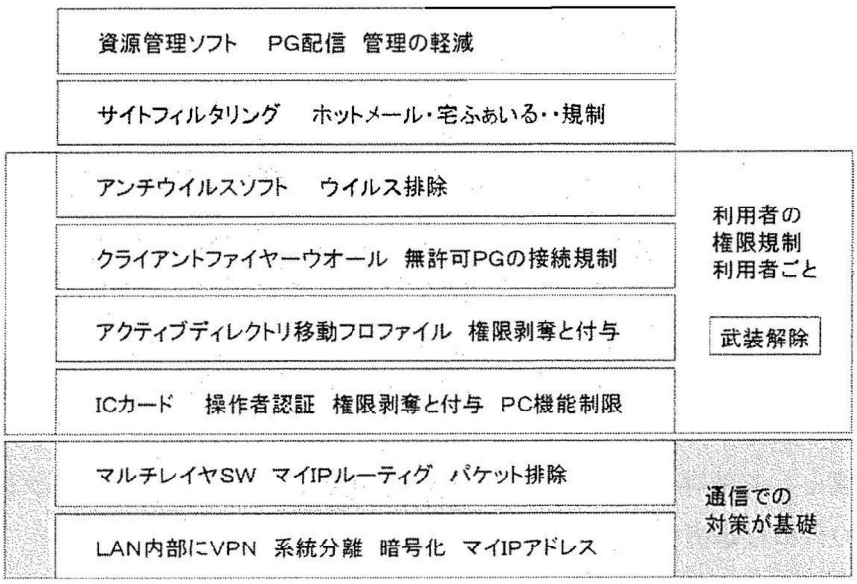
ＬＡＮに接続される機器（パソコン）の使用できる機能を管理者が全権をもって管理することができれば、無限の脅威を有限の脅威に転化することができる。管理者が権限を付与する方式であるならば、利用できる技術を管理下におくことができる。

5）系統の分離

自らの管理下にない回線と接続する無限の脅威を有する系統（外部接続系統、インターネットなど）と管理下にある有限の脅威しか存在しない系統を分離することとした。もしも分離しなければ無限の脅威を引き継ぐことになる。

系統の分離にはＶＰＮによる論理的な分離を採用することとした。物理的に別回線とすると、系統の間の情報流通も行わなければならない（インターネットで収集した情報を業務で使用するなど）のであるから、「媒体交換方式」による外部媒体の接続の危険性か、クライアント内部での蓄積された情報の流通か、どちらが安全かという比較となる。媒体交換方式は操作者の不正行為を防止することは不可能で個人情報が不正コピーにより流出する可能性がある。

具体的な手法の体系図



ここに掲げたすべての項目を網羅的に実施して、初めて「できなくする」の端緒になる。どれかが欠けていれば、「情報セキュリティの向上と事件発生に相関関係はない」という世界に引き戻される。情報セキュリティでは、もっとも脆弱な部分の水準が全体の水準であるから、１点豪華主義は馴染まない。

（４）役割分担の明確化

情報基盤である通信、クライアント、サーバなどで実施する課題とアプリケーションで実現する課題を分離する。これが情報システムの構築の根本問題で、たとえばアプリケーションの流通も可能となる。通信での安全性の確保とアプリケーションでの安全性の確保の機能を分離し、それぞれの果たすべき役割を明確にすること。重複を回避して運用面も含めたトータルコストの縮減を図る。

５．最後に

（１）情報主体の自己情報コントロール権としてのプライバシーの権利と知る権利を保障するという情報セキュリティの理念を確認したことで、たとえば組織内部の不正行為者の摘発ではなく、情報主体の被害救済を第一義的な目的とするのであるから、技術的セキュリティに求められる要件も異なってくる。個人情報保護法では、個人情報は「利用目的」にそった管理が要請されることとなった。これは情報主体の意思に基づく利用であり、情報システム内部に外部の情報主体の意思を取り込める仕組みが不可欠である。

（２）宇治市ではＩＣカードと連動したＩＰ－ＯＶＥＲ－ＩＰのＶＰＮを構築し、職員個人がマイＩＰアドレスを持つなど、ＬＡＮ内部の実名性を確保した技法を実装してきた。情報セキュリティを強化するためには、ネットワークの中での匿名性を排除し、実名によるトレーサビリティを確保する方向の確立をめざしている。

しかし往々にして匿名性は弱者の自己主張、内部告発の手段であるという側面を考えると、匿名が直ちに悪とは思えない。

実名のネットワークが確立されればされるほど、それと同時に匿名性の確保されたネットワークもまた不可欠になってくると考えている。またネットワーク管理者にも知られないことはプライベートな通信の原則で、匿名の空間、実名の空間は並存し、利用者がそのネットワークの特性を理解して利用できることが要請される。

匿名性の陰でうごめく悪意ある者を排除するために、匿名性という盾に護られてしか自己主張できない弱者までも排除することは健全な社会とは思えない。犯罪が全くない過剰防衛社会では窒息するだろう。実名性確保のための技術開発が大きく発展しているが、匿名性を確保する技術も開発されるべきと考えている。

両者が社会基盤として並存しなければならないと考える。どのネットワークに接続するかは利用者の自由な選択である。