

4- 6. 吉田柳太郎委員

【IT 社会の「メリット闇」】

コンピュータネットワークは現代の怪獣、モンスターです。それは、社会に非常に大きな影響を及ぼす存在になっています。有名芸能人が自分のホームページで、状況によってはプロダクション事務所を離れると宣言すれば、社長が辞任し三〇代の役員が社長に就任することになったりします。ホームページの意見が、企業の株価を急落させる要因となる時代なのです。

そういう時代のなかで、国は万全の体制と対策で IT を国家戦略として推進するとしてきました。たとえば、二〇〇一年一月 IT 戦略本部が策定した「e-Japan 戦略」では、「我が国が五年以内に世界最先端の IT 国家となる」ことが目標とされています。その構想には、IT の推進によって新規雇用が生まれ、高度情報社会によってすべての国民が一律に大きなメリットを享受できる……といったバラ色の表現ばかりが並んでいました。

しかし IT には本質的に、深くて目には見えない深海のような闇が広がっているのです。

各省庁のホームページの改ざんや海外からの攻撃、電子個人情報の漏洩、誹謗中傷掲示板の存在、対策を誤れば人事や株価にまで影響を及ぼすネットワーク社会……。長野県「安全確認」実験の結果をふまえて発言してきたことや、個人情報保護の観点で指摘した内容はコンピュータネットワーク社会が生みだしてきた、この深い闇の部分の指摘することだったつもりです。しかし、長野県本人確認情報保護審議会や長野県安全確認実験の経験をふまえて発言してきた論点に対する、マスコミを中心とした各界の反応は穏やかなものではありません。

- ・具体的な危険が起こっていないのに安全性を問題視することが問題だ。
- ・具体的な危険性を示せないなら黙っている。
- ・IT 推進にブレーキをかける行為である。
- ・国家プロジェクトに君ごときが意見を言う立場にない。
- ・米国の著名な団体の意見なら聞く耳はあるが、長野県の田舎審議会の委員から意見をされる覚えはない。

繰り返しますが、IT 社会はバラ色だけではありません。もちろんメリットはたくさんある。本当の意味で社会に IT が活用されることを切望しています。だからこそ、それを実現するためには「IT の闇」にしっかり目を向けて行くべきなのです。分かりにくいからとか、国が安全と言っているからということで問題すら認識しない状態では、ほんとうの意味での IT の活用はできるはずがありません。

たとえば、IT 社会は新たな差別を生むものです。

あらゆる情報を入手することの手間は格段に減りました。現在は、検索エンジンを使うことができれば、ほぼ入手できない情報はないとも言われる状況にあります。そのため、IT を活用して情報を得る人と、IT を活用しない人あるいはできない人との間での、情報の乖離は急速に広がり埋まらなくなっているのです。そこにさまざまな新しい差別が生まれ、拡大していく素地が存在しています。

ネットワーク上で情報を共有し活用する「IT 社会」と、人間と人間が直接触れ合うことで情報の占有的利用が行われてきた従来型の社会とでは、他の社会（コミュニティ）との接点で公開される情報の量と質が、格段に異なっています。そして、国や自治体のそれぞれの行政執行組織は、明らかに「人間と人間が直接触れ合う」型の社会です。

それでも、IT 化推進で先行した国はまだまだといえます。成功しているとは思えないまでも、国はそれなりに「IT を活用して情報を得る」ことで「ネットワーク社会における勝ち組」になろうとしています。ところがここで「IT 社会の深い闇」に落ち込んでいるのは、多くの自治体なのです。

それらの自治体には、「検索エンジンを使えば入手できる」レベルの「情報セキュリティ」や「個人情報保護」のための対策についてすら、情報を入手したり活用したりすることができていません。国と自治体の間には、「IT 社会の深い闇」から生み出される新たな差別がすでにできあがってしまっているのです。

……これが、長野県での本人確認情報保護審議会における自治体の実地調査や安全確認実験を通じて見聞してきた、多くの自治体の現実でした。

本当の意味で社会に IT が活用されるためには、IT 社会の浸透によって新たに生まれる「闇」に対して、適切で強力な対策が必要です。そうすることではじめて、多くの国民ができるだけ安全に日々をすごせるような IT 社会を作り上げていくことができます。

リスクを承知で危険なスポーツを楽しむ方々に危険だからやめろ！などという話をしているわけではありません。リスクを正しく認識することを棚上げにして法律を作り、実行すべき時期が来たからと言って、準備ができていないにも関わらず「安全」だということにしてスタートすることは、IT 社会では通用しません。IT 社会に一度解き放たれた情報は二度と回収できないからです。

言ってしまうと「住基ネット」は、財政能力もある、技術能力もある、責任能力もある自治体が先行して導入すればよいシステムです。その導入、運用ノウハウを後に続く自治体に提供できれば、広がりもでてくるはずですが、ところが現実には、そうではありません。安全対策を十分に行えない自治体が問題を抱える存在であることは、今や総務省も認めています。それは地方交付税支出の事務連絡を出している点からも明らかです。

だから住基ネットの議論は、「安全 / 危険」の話ではありません。ネットワーク社会の「メリットと闇」をどう読み取るかがポイントとなる議論なのです。多くの情報セキュリ

ティ技術者・研究者からは、現在の住基ネットをめぐる国（総務省市町村課）の議論は、技術以前の「超低レベル」のものに見えています。つまりここで必要とされているのは、議論の質的転換なのです。

ネットワーク社会の「メリットと闇」を直視した、広範な社会的議論が、的確なポイントを押さえるものとして深化されて行くなれば、住基ネットは現在のものとは本質的に異なるシステムになっていくでしょう。

情報セキュリティの問題を考えることは、実は「IT 社会の闇」に対する適切で強力な対策を考えることそのものなのです。

先般、静岡県のある役所でパソコン十台と現金七〇万円の盗難が発覚しました。社会教育課、国民年金課、総務課などのノートパソコンだそうです。市役所の夜間警備は守衛二人で行っていて、防犯装置などは設置されていないとのことでした。

これでも個人情報の漏洩はありえないと言えるのでしょうか。この事件では、そもそも個人情報保護論議以前の問題が露呈しています。安心とはそもそも何なのでしょうか。

国民の、地域住民のキビ情報が入っているコンピュータを運用、管理しているのに警備保障会社にも入っていないことがまかり通っていたことが明るみになっています。

この文章をまとめている読売新聞の朝刊一面にも、社会保険庁がITゼネコンと呼ばれる企業に106億円もの契約外の支払いをしていたことが指摘されました。内容がわからないので誰も確認をしないでいわれるがままに支払いを続けてきたことも露呈しました。

マスコミは、長野県本人確認情報保護審議会と総務省の平行線の議論と書き続けました。徹底的な間違いは、住基ネットの範囲を定義している長野県本人確認情報保護審議会と数年前から話をするたびに範囲が狭くなる総務省側の認識の違いを指摘すべきだと考えています。

個人情報保護の観点からの議論をしているのであって、論理的に別でも物理的につながっている「庁内にある既存住基サーバは住基ネットではない」と主張すること自体に総務省側の無理があることを指摘しなければなりません。

[あたまの転換]

情報漏洩が発覚しても毅然とした態度でいいわけができません。

なんでもかんでも怖いと言っているつもりはありません

何でもかんでも怖いと言っているつもりはいっさいありません。住基ネットがなくなればいいという話をしてきたつもりもありません。それなのにいろいろなところで、

「住基や背番号に反対しているやつの話なんか聞く耳はない！」

などと言われたりします。先般も長野県内で、市町村のみなさんを対象とした説明会をしましたが、田中知事とは異なるお考えを持つ自治体の課長さんなどから

「住基ネット自体の侵入が心配だったんだ。でも実験では侵入に失敗しているじゃないか。世間を混乱させたのはおまえなんだから謝罪しろ」

というおしかりをいただきました。私の話が、おっしゃるように理解されてしまっているのであれば、そうした混乱 誤解をさせている責任の一端は私にもあるのだということで、反省をし、おわびをしたいということで謝罪しました。それで、私が頭を下げた写真を使って、

「彼はまちがってたんだ」

という報道がされるわけです。マスコミの報道というものも、もうちょっと何とかならんのかと思うのですが、なかなか正確に報道していただけません。

私が言っていることはどういうことかと言いますと、

国が安全だと言っているから、コンピュータシステムは万全で安心できるから、

どんどん使いましょうというわけにはいかない。

ということです。なぜかという、コンピュータのネットワークっているんなところに問題があるからなのです。

「自治体が守り通す、賠償を含めて責任を負う」と言えますか

自治体のみなさんへの説明会などで、こんなご意見をよくいただきます。

「とどのつまりは何だ？ 結論聞かせてくれ。長野の話はもういいんだ！」

結論は何かと言うと、住民のみなさんの個人情報を預かっている自治体さんそれぞれが、「私のところは絶対に完璧に守り通す、何か問題があっても賠償責任も含めて全部負う、その所存で運用しているのだから、何があっても心配ない、大丈夫なんだ」と言い切れるかどうか、ということだと思います。

「言い切れるから心配してもらわなくてもかまわないんだ」と言われるところは、どんどん推進されるのがいいと思います。ただし、住民の方が窓口に来て、

「僕の個人情報漏れた。あなたは担当責任者としてこの問題にどういうふうに責任とってくれるんだ？」

首長はどのような形で謝罪をし、責任をとるのか？

「お金がありませんとか、伝票がなくなりましたとか、書類を紛失したという話じゃない。僕の個人情報どんどん漏洩していったんだ。僕のプライバシーに対してあなたの自治体ではどういうふうに責任をとってくれるのか？」

と言われたときに、賠償訴訟というものが起きます。日本弁護士連合会の先生方もいろいろなケースを考えられておられるのですが、どうも頭を下げるだけではすまない。

「そんな問題は、世間一般的には起こっていないのだから、そんなこと起こるはずがないんだ」というようなお話もありますが、来年の4月には個人情報保護法が施行されます。今後は自治体も例外なくコンプライアンス（規定やルール）が問われることになります。さらに、アカウントビリティ（説明責任）やトレーサビリティ（情報追跡）といった、フォレンジック（法的根拠になる証拠）が問われることになります。米国ではSOX法（コンプライアンスに関する責任者の個人責任追及法）も始まりました。日本も近々同じことが求められるようになり日本の法も経済産業省が音頭をとり整備が始まっています。

来年の4月からは個人情報保護法も施行されます。自治体も例外ではありません。

危険性がゼロでない限り「あり得ない脅威論」なのだと放置することはもはや不可能です。

住民から賠償請求がされたとき窓口で毅然とした対処ができますか

情報が漏洩してしまう危険性をゼロにすることは、技術的にも論理的にもできません。

窓口で「俺の個人情報漏洩の賠償を支払え」という人が何万人と来ても、毅然とした態度で対処ができるようにしておく必要がある、ということです。

その毅然とした態度で対応ができるようにするということはどういうことかと言うと、きちんと窓口で「いいわけ」ができるかどうかです。

たとえば、こんなふうがいいわけができるでしょうか

「僕のところはここまでやりました。その証拠がここに記録されています。正直言うと僕にもよくわかっていません。でも、わからないなりに一生懸命やってたんです。職員は勉強会も行った。わかんないなりに試験も受けて、やっぱり落ちて、それでもうまくいかないなりに一生懸命やった記録がこれなんです。

だから、あなたが問題があったと言ってる 月○日の記録もここにあります。これを見てください。

何が書いてあるか、僕には分かりません。でも、機密保持の誓約にあなたが今サインしてくれるんだったら、ご覧になっていただいてけっこうです。それで、問題がどういうことだったかを追求してください。

僕の責任がゼロだとは言いません。幾分の責任はあると思います。でも、僕が一〇〇%悪いという話になりますか？ 僕は一生懸命やりましたけど、あなたに、僕が一〇〇%悪いと言われる覚えはありません。その比率がどこかということは法廷でどうぞ」

こういう話を窓口ですれば、相手は「おまえは一〇〇%全部悪い」と言えないわけです。これが結論です。

ところが今、実際の市町村の状況はどうなっているのでしょうか 多くの自治体では「国がだいじょうぶだと言ってます。僕に言われてもわかんないので上長に聞いてください」

という話になります。そこで、責任のある上長に僕が「あなたは対策をどうしてましたか？ これ、ルールどうなっていましたか？」と聞くと、

「そんなの俺に聞くな。問題があったらポチポチ直せばいいんだ。

はじめから否定するようなやつの話なんて問題外だ。議論になるか。出てけ！」

こうおっしゃる方が少なからずおられます。対策の記録も、セキュリティ管理のルール(運用細則など)も、たぶんどこかにそれなりのものがあるのでしょうか。だけど責任ある上長が把握していないし、理解もしてない。だから記録もルールも窓口の苦情に対して有効に使えません。コンプライアンス的に問題なのです。

そういう状況です。

毅然とした態度で「いいわけ」をするためにとにかく「パッチ」をあてましょう！

「あたまの転換」をしてください。

より安全で安心できる状態に持っていく一〇〇%はそもそもないので、できるだけお金をかけずにいろんなことをやる、ということです。

具体的には、まず、とにかくパッチをあてることです。「パッチ」というのは、プログラムの「つぎあて」です。プログラムの穴(セキュリティホール)をふさぐ小さなプログラムですね。

マイクロソフト社からセキュリティ対策のパッチが出たら、その日の内にあてるのがベストです。そうしておいたら、誰にもなんにもつっこまれる筋合いのない話です。マイクロソフト社が対策をたてていない未知の攻撃を受けたら、それはもうしょうがないです。だけど、マイクロソフトが公表した既知の攻撃だけは、せめてその日に対策しておかなければいけないと考えています。

問題発生時に、かならず「いいわけ」の材料のひとつになるからです。これをきちっとやっておけば、みなさんのネットワークはかなりよくなります

そこから次にどうしていくかを考えながら、最終的には、
たくさんのお金をかけてシステムやネットワークを維持運営し続けていかなければなりません。

【セキュリティ対策の限界】

セキュリティレベルを 100%にできないのはなぜか

小学校六年生程度の日本語を読む力があれば、他人のコンピュータを乗っ取ることができてしまいます

「IT のセキュリティ対策にはまったくお金をかけませんでした」となると、セキュリティレベルはどうでしょうか

書店で簡単に入手できる「ハッカーになろう！」とかいうタイトルの本が一〇〇〇円かそこらで売っています。そういう本を読んでいくと、

小学校六年生くらいから中学レベルの日本語を読む力があれば、
絶対に他人のコンピュータが乗っ取れるくらいの知識が、「おまけの CD-ROM」で付いてきます。

これはほんとの話です。

まったくお金をかけなかったら、セキュリティレベルはゼロ。

だからセキュリティ対策はしないとはいけません。でも、三〇万円お金をかければ、セキュリティレベルはがーんと上がるんです。もうちょっと行こうかということで「六〇万円かけましょう」となると、セキュリティレベルは ガガ～ン と上がります。

だけど、「一億円かけました、一〇〇兆円かけました」……セキュリティレベルは絶対に一〇〇%になりません。

なりようがない。「セキュリティレベルの限界」があるためです。

ソーシャルエンジニアリングこれやられると、盗れない情報なんてありません

「ソーシャルエンジニアリング」とは、ケビン・ミトニックという男をご存知でしょうか

彼は「ハッカー」です。「世界でみんなが知ってたハッカー」でした。で、彼はある日考えます。

「どこにだってどんどん入れる。俺は天才だ。だからどんな情報でもお金にできるし、知的好奇心を満足させることができる。」

そこで彼は、こともあろうにアメリカの FBI 犯罪者リストというデータベースに侵入します。犯罪者の顔が正面とか横から写されていて、住所とか年齢とか全部は知っている、そんなデータベースのデータをポーンと抜いてきて、インターネット上のホームページで誰でも閲覧できる場所に置いたのです。

それでアメリカ政府はアタマにきて、彼を追いかけてまわすことになります。

彼は逮捕されて牢屋に入ります。そこで五年間生活して、二〇〇三年の一月にやっと出てきました。彼がその時何を考えたか、「このまま同じことを繰り返しても、きっと捕まる。そうだ、俺はこのノウハウを売ろう」ということになりまして、彼のノウハウを本にします。それが『欺術』岩谷弘訳・ソフトバンクパブリッシング刊、二〇〇三年。原題 "The Art of Deception") という本です。この本にはいろいろなことが書いてありますが、その中心は「ソーシャルエンジニアリング」です。

みなさんの経験の中にも、相手から「こいつは口がうまいな」とか「こいつは信用できねえな」とか思われてしまったことがあると思います。相手は心をガチャンと閉ざします。閉ざしてしまったら、「こいつには絶対に俺のことは教えない」となります。そうなるとどんな話をして、よっぽどでない限り、個人の情報は教えていただけることがありません。それはあり得ない。敵とみなしたやつには何もあげないし何も教えない、何も話してやらない こうなります。みなさん共通の、人間の心のシステムがそうできている。

だけれども、同僚が困ってる、仲間が困ってる、きのうお世話になったなになにさんが困ってらっしゃる そうなると人間はどうするかというと、みんな幼いときから教育を受けていますので、「困ってる人を助けなさい」と教わってきています。僕も、小さな頃おばあちゃんにもよく言われました。「知らない人にはついて行くな。でも、困っている人は助けなさい」 こうなるのですね。

どういうことが起きるかといいますと、たとえば日弁連に電話をかけます。本当の目的は「大江先生の携帯番号が知りたい」ということなのですが、

「清水先生いらっしゃいますか？」

という話から始めます。

「清水先生は今日はちょっといらっしやいません」

「そうですか。じつは清水先生に書類を送りたいのがあって、ファックスの番号教えていただけないでしょうか」

「そうですか。私ではちょっとそんなことお教えできるか判断できる上司がいませんので、お答えしかねます」

こうなるわけですね。だけれども、

「そうですか。じゃあ大江先生にいつもお世話になっているんですが...」

「あ。大江先生にはいつもお世話になってるんですよ...」

「じゃあ、大江先生の携帯番号は...えっと〇九〇の六四.....ああ、ちょっと今忘れた。大江先生の番号、今わかります？ だったらそこから清水先生のファックスの番号教えてもらうんで.....」

ここまでくれば、

「ええと、六四七のお.....」

と始まってしまうわけです。

全く関係ない話を振っておいて、後から言った話がほんとうの目的です。なんか言ううちに「この人知ってる人で、そういえば聞いたことある声だなあ」なんて気分になると、教えちゃうものなのですね、人間って。「吉田さんてそういえばいつも日弁連でしゃべってるし、清水さんも大江さんも知ってらっしゃるって言うし、困ってるんだからいいか」と、こうなるわけです。

人間って不思議なもので、「言っちゃいけないよ」と言われたことを言ってしまうと、心の中にずっと引っかかっています。「ああ、言っちゃったなあ。なんていいわけしようか」.....長い間忘れません。でも、人を助けたこと、困っている人によいことをしたときはすぐ忘れるようにできています、心の仕組みがそうなっている。

ケビン・ミトニックの『欺術』には、そういう、人間の心の隙間をいかに突けば人間はしゃべってくれるか、どんな情報でも手に入れられるかということが、ことこまかに、ゼーんぶ書いあります。すごい本です。読んでびっくりしました。ここまで言っちゃうの？.....これをやられると、盗れない情報なんてありません。もう絶対、犯罪ですね。

というわけで、『欺術』にはソーシャルエンジニアリングということが、細かく、わかりやすく、日本語で解いてあります。お時間があればぜひご一読ください。

人間の心から情報が漏れていくことを一〇〇%止めることはできません

このソーシャルエンジニアリングに対するセキュリティ対策に限界がある

ためだ、という話になります。人の心には鍵はかけられません。よかれと思ってやった行為まで、「おまえはまちがっている」と責めることはできない。そのひとを責めるのであれば、何を言っははいけないのか、何が危険なのかということをおあらかじめことこまかにみなさんに通知して、問題の起こりうる危険性のある事項をみなさんが正しく理解しているという状態でなければならないはずだ。

でも、そうしたことを国はおざなりにして、

「自治体のみなさんで考えるべきことだから自治事務なんです。国はそれに口を出しません。自治体の箸の上げ下げまで国が意見を言うはずがありません」

みたいなことをまことしやかに言います。もちろん、やれと言ってるのは国です。なのに「口を出しません」と言う。何をしゃべっちゃいけないか、どういうことをしゃべったら問題になるか、情報漏洩につながる行為とはこういうことだ、ということを国は具体的に示していないのです。

人間の心から、口から情報が漏れていくことを一〇〇%止めることはできません。アメリカの国防総省だってできませんね。できるはずがありません。それができる生き物って、この地球にはいないのです。

できないようになっている。

これがソーシャルエンジニアリングです。

よって、セキュリティレベルには限界があるのですね。心の隙間にあるセキュリティホールは埋めることができません。

人的ミスによるセキュリティホールと未知のセキュリティホール

人間の心から、口から情報が漏れていくのは、「人的ミスによるセキュリティホール」の一種とも考えられますが、それ以外にも「人的ミス」はたくさん起きています。「人的ミス」を完全に防止することは、やっぱり人にはできないようになっているのです。

[セキュリティの限界]

「未知のセキュリティホール」が存在します。

セキュリティ対策は、やみくもにやっているわけではなくて、すでにわかっている「既

「未知のセキュリティホール」を埋めるために実施しているのです。でも、世の中には「未知」の穴もたくさんあります。単純に、知られていないから「脅威ではない」と言うわけにはいきません。少なくとも、新たなセキュリティホールが発見されてから、実際の対策が実施されるまでの間はまったく無防備です。

この問題はとくに、自治体のパソコンやサーバに使われている Windows などの基本ソフト（OS）のセキュリティホールが、毎月のように新たに発見されていることと深く関係してきます。

いずれにしても、どれだけお金をかけても「実現できるセキュリティレベルには限界がある」ということになっています。

「未知のセキュリティホール」を使って不正侵入はできる

「マイクロソフト社がパッチを公表する前の『未知のセキュリティホール』を突いてサーバを乗っ取ることなんかできないのに、それをやると吉田は言っている。あいつはウソツキだ」という話が、一部の人たちの間で言われているそうです。でも、マイクロソフト社がパッチを公開しているもの以外を「未知のセキュリティホール」だと言うのであれば、「未知のセキュリティホール」を突いてサーバを乗っ取るとは、実は誰にでも可能です。

現実のマイクロソフト社が自分たちでパッチ対策を実施するプロセスはどうなっているかという点、社内ですら脆弱性（セキュリティホール）を認知して改善対策としてパッチを公表する」というパターンと、ぜんぜん違う他人（利用者など）から「指摘を受けて確認したらセキュリティホールがあったので対策プログラムを作って公開する」というパターンの、二つがあります。ところがマイクロソフト社は今や巨大企業になって、世界中にそのマジョリティを広げてしまっています。そのため、従来なら利用者がセキュリティホールを発見した場合、マイクロソフト社に知らせて改善を求める人がほとんどでしたが、巨大化して動きが鈍くなっているのです。

「マイクロソフトがまたやってるよ。こないだも注意したのに対策できてないじゃないか。もう報告なんてしないで、こういう問題があるって公表してしまうぞ！」

というホームページが、実は世界中に山ほどできています。そういうサイトはいっぱいあり、著名なサイトがいくつかが決まっています。たとえば、eEye 社（<http://www.eeye.com/html/>）などが一番有名です。

そこを見たら、今マイクロソフトが対策パッチを作れていない脆弱性にはどんなものがあるか、一覧できます。そういう環境がすでにインターネット上の公開された場所にできている。ここには、

「マイクロソフト社が、対策パッチを公表できていないセキュリティホールはこれだけあります。こうすればこの脆弱性を突くことができます」

という情報が、ずらっと並んでいる。だから、「マイクロソフト社がパッチを公表する前におまえが知ってること自体、おかしいんだ。情報入手先を明らかにしろ！」とか言われても、「あなた、eEye社のホームページ、知らないの？」という話になる。セキュリティ関係者ならeEye社のことを知っていてあたりまえなのです。

ネットワーク上にはそういう情報があるわけで、私が特殊な技能を持っているわけでも何でもない。ちょっと英語が分かるとか自動翻訳ソフトを使ってやれば、どんな人でも分かるような情報として「未知のセキュリティホール」の情報はパブリックな場所、インターネット上で公開されているのです。

だから、マイクロソフト社が公表していないセキュリティホールは、知ることができます。その脆弱を突いて、管理者権限を乗っ取る方法まですぐに分かります。技術に精通していればよりリアルに具体的に分かります。

したがって、マイクロソフト社がパッチを公開したら即座にあてるとするのは「最低限の防御」でしかないですね。マイクロソフト社が「緊急です、パッチをあててください」と言っているにもかかわらず対応していないということでは、いいわけもできません。損害賠償の全責任を負わなければいけない、ということですね。「だって、メーカーが公表していないものすら、インターネット上で公表されているんだから！」という理屈です。

[セキュリティ対策の基本]

やっておかなければならないことはなにか

事前の対策 + 有事の対策これが理想的なセキュリティ対策の考え方です

最も重要なことは「危機管理」の観点で対策に取り組むことです。セキュリティ事故を一〇〇%防止することはできないから、「危機をできるだけ回避する対策」と、実際の「危機に対処する対策」で、二段階の危機管理をするという考え方です。

(1) 事前の対策 : 「 有事の可能性をできるだけ低くする 」

まず「事前の対策」として、

論理的にあらゆる「有事の可能性」を洗い出し、ひとつひとつに対する対策を考えて実施することが必要です。これはやはり、ベンダー(納入業者)さんの技術の方、みなさんの

お仲間のコンピュータに明るい方.....いろんな方の複数の知恵を出しあって、取り組んでください。ベンダーさんまかせでは、やっぱりうまくいきません。

できるだけ問題が小さくなるように机上で問題をつぶしていくということ 有事の可能性をできるだけ低くするために何をすればよいかをまず考えて、その結果にもとづいた強固なシステムを作り、継続してそれを維持してください。

(2) 有事の対策 : 「 有事の被害をできるだけ小さくする 」

それでもなにか起こります。さきほどのソーシャルエンジニアリングもそうですが、こういうところに問題があるか勉強し続けたいといけません。でも情報を漏らすことはかならずあります。だからリカバリーオペレーション 問題があったときに、被害をできるだけ小さくするためにどうリカバリーするかということが非常に重要な問題になってきます。

「その場でネットワークケーブルを抜ける」ルールを作ってください

「事前の対策」が十分でないまま、現に全国の自治体でシステムは動いています。

で、「有事」が発生したとします。

「問題が起こってる？ 誰かがこのコンピュータに侵入しているみたい」

.....「みたい」じゃなくて、きっと入っているんですね。

「情報をとってるみたい.....もしかしたらデータベースの情報、抜かれてる、かも.....」

さあどうしよう？ となると、上長に報告しなければなりません。でも上長は席を外している。誰かに聞いても「止めていい」って言ってくれそうな人はどこを見てもいません。どうしよう.....と思っている間に情報は、ずーと、ずーと、抜かれている。

ではどうしたらいいか

問題があると気づいた時点で、コンピュータに勝つ絶対の方法がひとつだけあります。

「ネットワークケーブルを抜く」

ことです。

コンピュータは疲れません。だから人間よりも早く、いろいろな計算をして結果を出してくれる。だけどコンピュータは万全ではないし、完全でもないし、神様でもありません。ただの計算機、電卓のばけものです。こういうやつらに人間が絶対に勝つ唯一の方法が「コンセントを抜く」ことなのです。電気を与えなければ、コンピュータはただの箱、鉄のか

たまりだけれども、「リカバリーオペレーション」として「コンセントを抜く（電源を切る）」ということを決めて（定義して）おかないと、後から問題になります。

「おまえ、誰の責任で抜いたんだ！ 誰がOKって言ったんだ！」

と叫ぶ人が絶対います。

「コンピュータもわかってないで勝手なことしゃがって、どうしてくれるんだ。

窓口業務止まったじゃないか」

そんなこと言われるんですが、情報が出てしまって四〇億円払わされるんじゃないのですね。コンセント抜いた方がよっぽど安くつきます。二〇~三〇万円払えば、ベンダーさんが、がたがたガタガタ言いながら収まるようになっていきます。どっちが差し引き得ですかを判断しなくてはいけないのです。その場で判断することは難しいならルールで決めておけばよいということなのです。

確かに多くの方にめいわくをかける。窓口の業務も止まるでしょう。でもそこでは、毅然とした態度で

「情報漏洩の可能性があります。今コンセントを抜いてその危険性をくい止める努力をしています。まことにもうしわけありませんが、みなさんにはお時間をいただきたい」

こう言うしかないわけです。

多くの方のみなさんの個人情報を守るの方が大切なはずで、目の前のお客さんがどなりちらすからといって、それに従っていたら、残りの何十万人の方のみなさんの情報が出ていってしまう。最終的に差し引きしたらどちらが安いのか判断できるようにしないと行けない。だからこそ、リカバリーオペレーションとして、気づいた人がその場で対処するルールを作っておかないといけません。

住民の方のみなさんの情報を守るために線を抜いたのに誰かにぶーぶー言われる筋合いはありません

今、僕は極論を言ってます。要はコンピュータを孤立させることですから。

「その場で線を抜く」ルールをはっきりと決めておかないと、勝手に抜いたとか、誰の判断で抜いたんだとか、誰が抜けと言ったのかとかという話になる。でも「誰が抜けと言ったのか」という話ではありません。何が起きているかの方がだいじなのです。そういうことをあらかじめルール（規定）にしておかないと、後で問題になります。

だからここできちっと、「それでも何か起こるから」とう有事の対策を考えておかなければならないということですね。要は、

誰の責任もないようにしておかないといけない

のです。住民のみなさんの情報を守るために線を抜いたのに、誰かに苦言を言われる筋合いはない、ということです。誰も悪者にならないように、ルール化しておく。それをぜひとも大きな声で言って実施してください。

たとえば税の「消し込み」のような業務はすごくセンシティブですね。税金払うと自分のところに「消し込み」がされます。それがたとえば三〇〇〇人分、まだデータベースに書き込まれる前に「飛んじやった」となると、お金のことですから大変です。それをきちんとなおそうと思ったら、一行ずつ目で確認するほかありません。そうしますと、一日一万人以上の窓口に来られる自治体の場合、こういう手間のかかる確認の作業が一日六人の自治体と比べて圧倒的に多くなる。

むろん、その後本当にそれがきちんと戻ったか、途中で消えているものがないか、という確認があります。それはやっぱり、職員のみなさんにやってもらわないといけないわけです。おそらく業者も手伝ってやるということになりますが、それをやっても何億円にはなりません。でも、このくらいのコストはかかる。だけど「ネットワークケーブル」を抜かないで全部情報漏洩してしまったら何億円になる。ということです。

「運用・管理状況に対するコンサルティング」はベンダーさんが仕様書まで書いている自治体では必須です

オーディットをやることで器械やネットワークがどうなっているかはわかった。では運用だとかルールはどうなっているのか？

器械はルールにマッチした動きをしているのだろうか？

器械はちゃんと動いているけどわれわれの運用がちゃんとできていないのではないかな？

ということで現状を評価しようというのが、「運用・管理状況の評価」です。でも、自分たちのやっていることを自分たちで評価するのは難しい。中規模以下の自治体では、ネットワークのデザインは仕様書までベンダーさんに書いてもらっているところがほとんどという実情だと思います。何の器械を買ってどういうネットワーク構成にするかということ自体を、ベンダーさんに全部書いてもらっているわけですから、そもそも自治体自身に現在動いているネットワークが分かるわけないのです。その上担当はぐるぐる替わっている。「前任者がやりました、そんなもの俺に分かるわけねえ」ということになります。そこで、

第三者に客観的に「運用・管理」について評価してもらいましょう。

同時にアドバイスもいただきましょう。

ということが大切になってきます。

「あなたの既存のネットワークのセキュリティレベルを評価しました。器械は五段階評価の4ですが、運用がぜんぜんでたらめなので、総合レベルでは2しかあげられません。落第点ですね」

「では、どこを直したらいいの？」

という相談ができる相手を見つけないといけません。これが、

「運用・管理状況に対するコンサルティング」

です。で、コンサルタントとディスカッションすることによって、セキュリティのレベルを上げていくことができるようになってくると、実は必然的に、現在のネットワークのデザインに「セキュリティ上のボトルネック」が見つかってきます。そのため「ネットワークのこの部分は意味がないですね。この部分はこういう構成にした方がいいですね」という話が出てくるのですが、そこから始まるのが、

「既存ネットワークデザインの改善」の相談ということになります。

オーディットのようなある程度おまかせ可能なサービスとは違って、運用・管理のコンサルティングは、ツーウェイの「相談」です。担当者とコンサルタントが相談して、納得したら担当者が実行する　そういうものがコンサルティングです。

「相関分析」の重要性をぜひ理解してください

運用・管理状況の評価をする上で、ネットワークがどのように運用されているかを調べるだけではなくて、「あなたのネットワークが日々どのようなセキュリティ上の脅威にさらされているか」も調べる必要があります。それを明らかにするのが「相関分析」です。

これはけっこうめんどろな作業なのですが、「相関分析の実施」ということを、ぜひみなさんの認識として持っていていただきたいと思っております。何の話かというと、

ネットワークは「一つの器械」のように思いますが、実はたくさんの器械で構成されているわけです。たとえば「ルータ」という器械があります。ネットワークの出入り口です。電話線を使って LAN の間を接続するときの出入り口には「ダイヤルアップルータ」が使われます。

それから「ハブ」とか「スイッチ」と呼ばれる器械があります。ネットワークケーブルを分岐・合流させる装置です。

「サーバ」があります。WEBサーバやメールサーバ、データベースのサーバなどいっぱいある。

「ファイアウォール」もあります。自治体によっては「不正侵入検知システム」があるかもしれません。

ほかにもいろいろな器械が使われています。たくさんの器械でネットワークは構成されているわけですね。こういう器械は一個ずつが「ログ」というそれぞれの器械の動作の記録をはき出しています。それから、システムの運用上の記録があります。たとえば「サーバールーム（重要機器室）の入退室記録」のような記録が作られているはずです。

何か問題が発生したとき、たとえば不正侵入を受けたときには、そういう、記録を全部集めてきて、時系列に並べて相互につじつまが合っているかじっくり時間をかけて分析していきます。分析は専門技術者が行います。これが「相関分析」です。これをやれば、実際に何が行われたかが分かってきます。「やられた」というサーバのログだけを見ても分かりません。プロ中のプロが分析しても「たぶんこうだろうな」ということぐらいしか分からないので、本当にすべてを知ろうとしたら、今言いましたルータやスイッチやサーバなどの全部の記録を集めてきて、「相関分析」をします。

「管理・運用の評価」の中で行う相関分析の実施は、たぶん不正行為が行われていない時のログを集めて行う分析ですが、それでもいろいろなことが分かります。

たとえば、相関分析の結果、「入退室記録もないのに、祝日の深夜にデータベース更新がかけられていた」ことが分かるかもしれません。よく調べてみると、この入退室記録は実は別の部屋のもので、サーバールームの入退室記録は完備されていなかった、ということが分かるかもしれません。逆に、今まで気づかなかったデータベースの不正な書き換えが発見されるかもしれません。不正侵入には至らなかったけれど、サーバが乗っ取られそうになっていたことが分かって改善点が指摘される場合もあるでしょう。ネットワークに対する日常的な脅威の現実が明らかにできるわけです。

もう一つ重要なことは、

相関分析に必要とされている記録（ログ）が、意図した手段によってきちんとそろえられるかどうかを確認することです。これがうまくできないということは、ネットワークのどこかに問題があるか、あるいは管理や運営のどこかに問題があることを意味しています。そのために、「何か起きた」とき相関分析によってネットワークの何を改善すればよいかを明らかにすることができない。ということがないように、きちんと確認しておいてください。「ログ」そのものも法廷で記録として通用するような正確で改ざんされていないことを担保することも必要になります。デジタルフォレンジックが問われるでしょう。

実は、この「相関分析」をリアルタイムで行うことは「究極のセキュリティ監視」だと言われている、つい最近になって製品も発売され、自治体のみなさんも注目しています。

何か困ったときに相談できる人を作っておいてください

セキュリティ対策のサービスメニューとして、「緊急レスポンス」も広く活用されています。

何か困ったときに相談できる人、技術的に明るい人、具体的に親身になってくれる人
それをキチンと作っておくということです。ベンダーさんの方かもしれませんし、緊急レスポンスを外部の技術者にアウトソースする場合もあるでしょう。自治体職員の中で特にシステムやネットワークに詳しい人、職場の上司かもしれません。そういう人を作っておく、ということが非常にだいじだということです。

「なんかおかしいんだけど、どうすればいいの？」

ということを、その場ですぐに相談できる。最初に、どんなアクションを起こせばいいのか　ファーストエイドと呼ばれている一番最初の手当てを相談できる相手を作ることです。で、相談する相手を作るということは、

「すぐに相談する」というルールを作る

ということです。とにかく、今何かおかしい　という時に一番最初の手当てを施すのが緊急レスポンスですが、「する」というルールを持っていなければ、「おかしいなあって思って見てたんですが、やっぱりなんかおかしくなってるんですか」で終わってしまいます。

重要なのは「ネットワークケーブルを抜いてください！」と言ってもらえる相手を作っておく、そう言ってもらえるルールを作っておく、ということですね。そうしておけば、被害を小さくすることができる、たくさんの住民のみなさんが被害を受けなくてすむ。担当者も悪者にならないですむ。

そういうサービスを利用できるようにしておけば、メニュー化されているし、契約書なり規則なりがあってルール化されているわけですから、安心してアクションが起こせます。

住基ネットとそれに物理的に接続された自治体のネットワークのセキュリティを考えた場合、二十四時間三六五日の「セキュリティ監視」は必要です。そんなにお金のかかることをと言われる方も多いのではないかと思います、理由は簡単です。

九時　五時の勤務時間には誰かがシステムを見ている可能性が高いので、「何かが起きて気づくかもしれません。でも、たいていのサーバは二十四時間運転されています。誰もいない深夜に「何かが起」っても誰も気づきません。翌朝になっても誰も気づかないかもしれません。だから二十四時間のセキュリティ監視は必要なのです。「うちのサーバ

は、時間がくるとタイマーで電源を切るから大丈夫だ」という自治体さんがあるかもしれませんが。でも、確実にタイマーで電源が切られていることが保障されているのでしょうか？

これが、二十四時間のセキュリティ監視が必要になる理由です。ネットワークを運用するには、お金がかかります。

ここで少し、「リアルタイム相関分析」について考えてみたいと思います。

リアルタイムで実施することは、人間わざではできません。分析する情報の項目が、ルータ、ファイアウォール、不正侵入検知システム、各種サーバなどのログや警報などすごい数になっています。それらを並列で見比べて、つじつまが合っているかどうかを人間の目で瞬時に判断することはとうていできません。器械にやらせるしかない作業です。

そんなリアルタイム相関分析によるセキュリティ監視が、つい最近になって数社から提供され始め、注目されています。リアルタイム相関分析が、必要とされる情報のすべてにわたって実施できたら、確かに究極のセキュリティ監視と言えるでしょう。きちんと動作すれば、本当のプロ中のプロでなければ侵入に成功しなくなります。

しかし「リアルタイム相関分析」は、現在ようやくサービスとして出始めたところです。まだまだ、コスト、クオリティ、チューンアップの手間など、課題はたくさんあります。

それでも実害は発生するのだとしたら、「最終的なリスクヘッジは保険しかない」

さて、お金もかけ勉強もして、必要なセキュリティ対策をかなりのレベルで実施しました。でも、セキュリティは一〇〇%ではないので残余リスクが残っています。

……とういことで、「保険」はその残余リスクをヘッジする究極の対応策です。

最近日本の保険会社が、自治体を含めて上場会社にだけ、個人情報漏洩に対する保険を作りましょうということを言っています。二月半ばの日本経済新聞だったと思います。ところがその二日後に、「四五〇万人の個人情報漏洩」と報道されて、保険会社は大変な状況ですね。「やるといったけどやばいぞ……」

「保険」というものは究極の考え方です。アメリカのCIAやFBIのITセキュリティのコンサルタントをしているカウンター・ペインという会社があります。この技術責任者をしている取締役は、ブルース・シュナイアーという暗号の世界では「神様」と呼ばれている男がいるのですが、彼が言っています ITセキュリティの究極は保険だ。人に依存しても無理、器械に依存しても無理。最終的なリスクヘッジは保険しかない 彼の『暗号の秘密とウソ』（翔泳社刊、二〇〇一年）という本の中に書かれていることです。

「パッチがあてられない」というのはウソです

先日、ある講演会で出た質問に、

「パッチあてると言うけど、『パッチあてたら動かなくなっても知りませんよ』と業者に言われました。だからパッチなんてあたらなと言われたけど、なんで？」

というものがありません。

これ、ウソです。

パッチはあたるんです。で、プログラムが動かなくなったら、それは業者の責任ですそれはもう、まちがいありません。はっきりしています。

でも、業者はそう言う。なぜかというと、技術者は後ろ向きの仕事はしたくありません、作って納めたら終わりなんです。でも、パッチをあてるたびに、納めたプログラムの全部の機能をひとつひとつ動かして、「収税消し込み動作 OK、……」ってやらないといけな。機能のありとあらゆる組み合わせの作業項目表を作って、ここはまる、これはいけた、これもいけた という形でチェックしないと、「プログラムが動かなくなる」ことを予測できないのです。こういうチェック作業は何も新しいものを生みません。後ろ向きの仕事です。だから技術者はやりたくない。

営業課長さんあたりがお客さんのところで「パッチあてて」と言われて「はい、見積ってみます」と答える。ところが帰ってきて技術担当に相談するとういわれます。

「えー、そんなのやるの？ やるんだったら、僕、会社辞めるもんね」

そんなわけで

「わかったわかった。何とか断ってくるからよお、どう言えば断れるんだ？」

「そんなのやったら、業務のプログラム、動かなくなっても保障できないって言ったらいいんじゃないですかあ」

「じゃあそう言うよ」

というわけで営業課長さんはお客さんにそう言う。

「何とかお客さんは納得してたからさ、お客さんとの話はずっとそれで通せよ！」

「わかったあ」

という話に業界ではなっているのです。これが真実です。でも、パッチがあたらなようなプログラムを納めた業者が悪いんです。ここだけは覚えておいてください。

これは当然、住基ネットの業務用プログラムの問題だけではなく、既存住基やそのほかの事務処理で使っているプログラムでも同じです。そこまで含めて「全国いっせい

に、パッチをあてる方法」を考えておく必要があったのです。

簡単ではありません。でもやっぱりパッチは、きちんとあててください。

緊急対策

委託業者とのサービスレベル・アグリーメント：SLAを確認してください

これは何かと言うと、自治体のみなさんをいかに守れるか、という問題です。損害賠償が求められたとき、「ここまでやってたんですけどダメでした」と言って責任を分ける切り札がこれです。

業者の方にアウトソースしたときの、サービス上の契約書に、
どこまでが役所の仕事で、どこまでが業者さんの仕事です という、
「責任分界点」がはっきりと書かれているかどうか
という問題です。

現実の市町村の契約には、「サービスレベル・アグリーメント」はほとんど書かれていません。自治体のなかで今までSLAを明記してきたところというのは、たいへん少ないのです。人口が三〇〇万人以上いるような自治体なら、業者さんの方から喜んで作ってくるのですが、そうでなければSLAは書かれていないでしょう。

これがないと役所のみなさんは守れません。窓口で被害を受けた住民のみなさんから、「やっぱりお前たち、何も考えてなかったんだろう！ だからこんな問題が発生したんだ」

こう一方的に言われるに決まっています。いいわけできません。だからみなさん、現在の責任分界点がどうなっているかをぜひ確かめてください。

日本の行政機関や自治体は、「性善説」で永年にわたって業者との関係を構築してきました。だから「SLAなんて今さら作れない。コミュニケーションコストだって無視できないし」という声も強い。でも、これって、ただのナニワブシです。

ネットワーク管理者と協力関係を作り上げるために

さて、セキュリティ対策をうまく実施していくために、「ネット管理者」の立場についてもご理解をいただきたいと願っています。「ネット管理者」はつらいです、本当につらいです。

よく言われます。

「情報化の利便性とセキュリティのバランスをちゃんと取ってね！」

そんなのネット管理者に分かりません。システムを運用する人が「何をどれだけ守りたい」のか、「利便性をどれだけ犠牲にしてもセキュリティを優先するのか」を決めてください。それはネット管理者が勝手に決めることじゃありません。

「ウチのセキュリティはだいじょうぶかね？」

そんなことネット管理者に聞かれてもこまります。私がどんなに一生懸命働いたって、セキュリティは一〇〇%にならないのですから、情報漏洩はいつだって起きる可能性があるのですね。

人手と予算は？

コスト削減をまっさきに求められるのがネット管理者です。

年中多忙なのに、でも評価は？

事故は起きなくて当然、なんかあれば「お前のせいだ」となる。セキュリティはそもそも利益を生まないのですね。だから個人情報の保護と運用の板挟みにあいます。

そして情報収集に終わりはありません。ハッカーさんとのイタチごっこ、新しい技術がつぎつぎと出てくる。

お前技術担当だろう！

知っていて当然のように扱われます。迷惑千万です。

だから問題発生でスキルが疑われることになる……

「お前、本当はたいしたことないんじゃないか？」

ネット管理者なんてそんなものなのです。押しつけられてもこまります。だからみんな考えないといけない問題なのです。セキュリティはネット管理者だけに押しつけるような問題じゃない、ということですね。

パッチは、無料でできる有効なセキュリティ対策です

パッチって何？どうやってパッチをあてるの？

マイクロソフト社は「パッチ」について、ホームページで次のように説明しています。

インターネットにはウイルスや、ハッカーなどからの不正アクセスといったさまざまな危険性があります。コンピュータのセキュリティ対策を行わないとこれらの問題により、

ウイルスに感染したり、ハッカーなどの不正なユーザーから個人情報盗まれるといった被害を受ける可能性があります。これらの被害を受けないようにするためにもセキュリティ対策が大切です。セキュリティ対策を行うためには次に紹介する対策を行うことをお勧めします。Windows Update は、コンピュータの状態を診断して、Windows を常に最新の環境に整えるオンラインサポート機能です。こまめに行うことで、ウイルスが悪用するセキュリティホールを修正し、悪質な攻撃に負けない頑丈な環境を構築します。これがパッチ対策です。

(http://www.microsoft.com/japan/security/security_bulletins/より)

これを読むと、「不正アクセスを受ける危険性」はインターネット上に一般的に存在しているかのような印象を受けるかもしれませんが、少なくともここで公開されているパッチが修正しようとしている「セキュリティホール」は、マイクロソフト社のプログラム開発に問題があって発生したものです。マイクロソフト社はこのミスに責任を取るため、対策用の「パッチ」を作って公開しています。

これは自動車の「リコール」とよく似た考え方だと言ってさしつかえないと思うのですね。自分で作ったものに自分で問題を発見しました、だからこうしてください ということです。自動車だったら「部品を交換させていただきますので、お近くのサービス店においでください」ですが、Windows の場合は「自分で対策をしてください」という話になっているのです。

「パッチ」は、プログラム（ここでは Windows やそれに付属しているインターネットエクスプローラーなど）のミスが原因となって攻撃を受ける可能性がある時、そのプログラムを書き換えて攻撃を受けないように修正する小さなプログラムです。自宅のパソコンなどでは、Windows Update の機能などを使って自分で適用する（パッチをあてる）ことができます。でも、企業や自治体の中で使っているパソコンやサーバの場合は、自分で勝手にパッチをあてることはできないようになっているのではないかと思います。その場合はネットワーク管理者がパッチをあてるか、「こういう手順でパッチをあててください」という指示をみなさんに出している「はず」です。

Windows のパッチってどのくらいあるのか

では、このような脆弱性の問題 修正プログラム（パッチ）は、何個あるのかというと.....パソコンをお持ちの方は、ホームページブラウザ（インターネットエクスプローラーなど）で次のURLにアクセスして、ゾツとしてください。めっちゃくちゃあるんです。だから大変だということなんです。

http://www.microsoft.com/japan/technet/security/current.asp?sel_id=Windows+2000&

info=ALL&optTop=all

(このURLは将来無効になるかもしれません。その場合は、マイクロソフト社のトップページから「セキュリティ」および「その他のセキュリティ情報」などをキーワードにして探してください)

このページには、住基ネットのCSサーバやCS端末で一般的に使われているWindowsに関連するセキュリティ対応「パッチ」だけで、

二〇〇四年八月四日現在 一一五件

が公開されています。このページ全部の「パッチ」の総数は

三〇八件

でした。

皆さんがいま使っておられるサーバやパソコンなどの基本ソフト(OS)と呼ばれている一番重要なプログラムには、いくつか種類があります。マイクロソフト社の基本ソフトはWindowsと呼ばれていますが、それにもWindowsNT 4.0、Windows2000、WindowsMe、WindowsXP だとか、Windows2000 Server、Windows2000 Server Advanced などいっぱいあります。パソコンやサーバー用の基本ソフトを発売しているのはマイクロソフト社以外にも数社あって、MacOSとかLinuxといったそれぞれ独自の種類の基本ソフトを提供しています。

皆さんがお使いの基本ソフト(OS)がその内のどれかを調べて、Windowsの場合はここにある該当するパッチが、いまだこまであたっているかを調べてみてください。すでに使っている方がほとんどだと思いますが、Windows Update という機能を使うと、自動的にこれを調べてくれます。

Word や Excel などにもパッチがあります。あててください

それから、このページで公開されているいろいろなセキュリティ情報(パッチ)には、「Microsoft Word」とか「Microsoft Excel」などと書かれているものも含まれています。何かというと、CS 端末もそうですが、パソコンがWindows2000 などを使っていてWindowsのパッチはあててあるから安心だと思っていると、Microsoft Word などマイクロソフト社のワープロや表計算用などのプログラムが使われていて、いやらしいことにこれにもパッチがあるのですね。それがあたっていないと、まあ中級以上のコンピュータ乗っ取りが大好きなお兄さんたちが「Wordの脆弱性がある！」と言って管理者権限を奪取する、ということが起こります。

非常にやっかいです。Windows(基本ソフト:OS)のパッチをあてているだけではダ

めで、ほかにアプリケーション(プログラム)が動いていると、そのアプリケーション自体の脆弱性を突いて管理者権限がとれることがあるのですね。

これはマイクロソフト社のプログラムに限りません。たとえば常識的に考えれば、住基ネットのCSサーバやCS端末で動いている住基ネットの業務用プログラムにだって、セキュリティ対策の「パッチ」はあるはずですよ。おそらく「バージョンアップ」とか「機能追加」という形で、地方自治情報センターから配布された「追加プログラム」に含まれていると考えていいでしょう。

[情報セキュリティ 10 原則]

できないことはしない、しなければ問題は発生しない

最後に、みなさんといっしょに考えてきた情報セキュリティについて、「10原則」という形でまとめてみました。

この「原則」は僕の発明ではありません。

RSA 暗号システムというものの開発者アディ・シャミア博士というセキュリティの専門家がいます。彼の「原則」は、彼が講演の中でしばしば言っていたことばを、そのまままとめたものです。僕が付け加えたことは、これの 1 番だけ。あとは全部シャミア博士が言っていたことです。

原則 パーフェクトなセキュリティを求めるな

100%は求められないよ！ ということです。何か必ず起こると考えて、「有事の対策」を立ててください。

原則 まちがった解を解くな

問題はシステムやネットワークの上で起きるとは限りません。銀行の小切手詐欺の内、ネット犯罪被害は10%です。むしろ問題の90%は、ネットワーク以外の場所で発生していたりするので。

だから、僕が怖いと言ってるのは、ネットワークの何もかもが怖いと言っているわけではないのです。そこを勘違いされないようお願いいたします。

原則 全体でセキュリティの問題を考える

ここ一カ所だけ安全だったらいいという話じゃないのですね。ほかにつながっていると

ころもぜーんぶ見ないと、何にもならないですよ、という話です。それと、ネットワーク管理者や業者まかせにしてもいけないのです。

原則 暗号のかけ過ぎは正しくない

何でもかんでも「良く」しちゃうと、やりすぎになります。やりすぎでもうかるのはベンダーさんだけです。

原則 高価にするな（何かを買えばすむ話ではない）

やっぱりやりすぎはダメ、ということですね。業者さんがこんなふうに勧めるかもしれません。

「不正侵入検知システムがあったらいいって言ってますからね。長野はうるさいんですよ。長野に文句言われないようにしましょう。どうぞこの器械買ってください。三〇〇万円です！」

そんなものすぐ買う必要はないのです。

まずパッチをあてればいいのです。パッチは「無料でできるセキュリティ対策」ですね。これを忘れていくらお金をかけたって、初心者さんにやられます。パッチから始めてください。ものを買うのはその検討後にしましょう。

原則 防御ラインは一つだけでは意味がない

ファイアウォールがあるから安全だ そんな話はウソです。いろんなところから、統合的に、多角的にものごとを考えてみましょう。

原則 アタックがあることを忘れるな

プロ中のプロ以外は、いきなり本丸にはたどり着けません。チョロチョロと兆候があるのですね。それをみのがしていたらダメです。そこで防ぐのが皆さんの仕事になるのだと思います。でも、今の自治体にそんなことができるのか、というところが問題なのですが……。

原則 システムを信じるな

国が安全だと言ってることを鵜呑みにしてると大変なことになります。

原則 人を安易に信じるな

これは「ソーシャルエンジニアリング」のことですね。何を言ってもいいか、何を言っ
てはいけないか これをはっきり「ルール(規定)」にしておいてください。

原則 できないことは、するな！

「できないことはしない」

これが一番正しいことなのかもしれません。僕はそう思って生きております。だからでき
ないことは「すみません、できません」と言います。

「でも、お前できるみたいに言っただろう！」

「僕じゃなかったら、できる人はいると思います」

そういう話なんですね。僕にはそんな能力はないです。頭もそんなに賢くないと思いま
す。でも、こういうことはやっとなきゃいけないんだろうな、ということはわかります。
だからできないことはしない。しなければ問題は発生しない 僕はそう思っています。

最後に

マスコミなどからはさんざんに書かれるという経験をしてき吉田ですが、捨てる神あれ
ば拾う神ありで、少数ながら吉田の活動に「がんばれ」と激励をくださった自治体の担当
職員の皆さんに感謝したいと思います。数行の激励メールに励まされたことが、吉田のダ
イナモを回してきました。

現場を担当する自治体職員や民間のネットワーク管理者のみなさん、そして住基ネット
の問題の解決に強い関心を寄せている地域住民と自治体議会議員のみなさんの努力に少
しでも役立つことを切に望みます。

下記書籍の本文から内容を抜粋しています。

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

吉田柳太郎・西邑亨著 / [七つ森書館刊](#)