市町村ネットワークの脆弱性調査の結果説明

アジェンダ

～長野の実験で何がわかったのか～

1．実験によって直接わかったこととは
2．事実から類推する想定される危険とは
3．なにを問題視しているのか
4．どうすればよいのか
5．なにをもって良しとするべきなのか

吉田柳太郎

1．実験によって直接わかったこととは

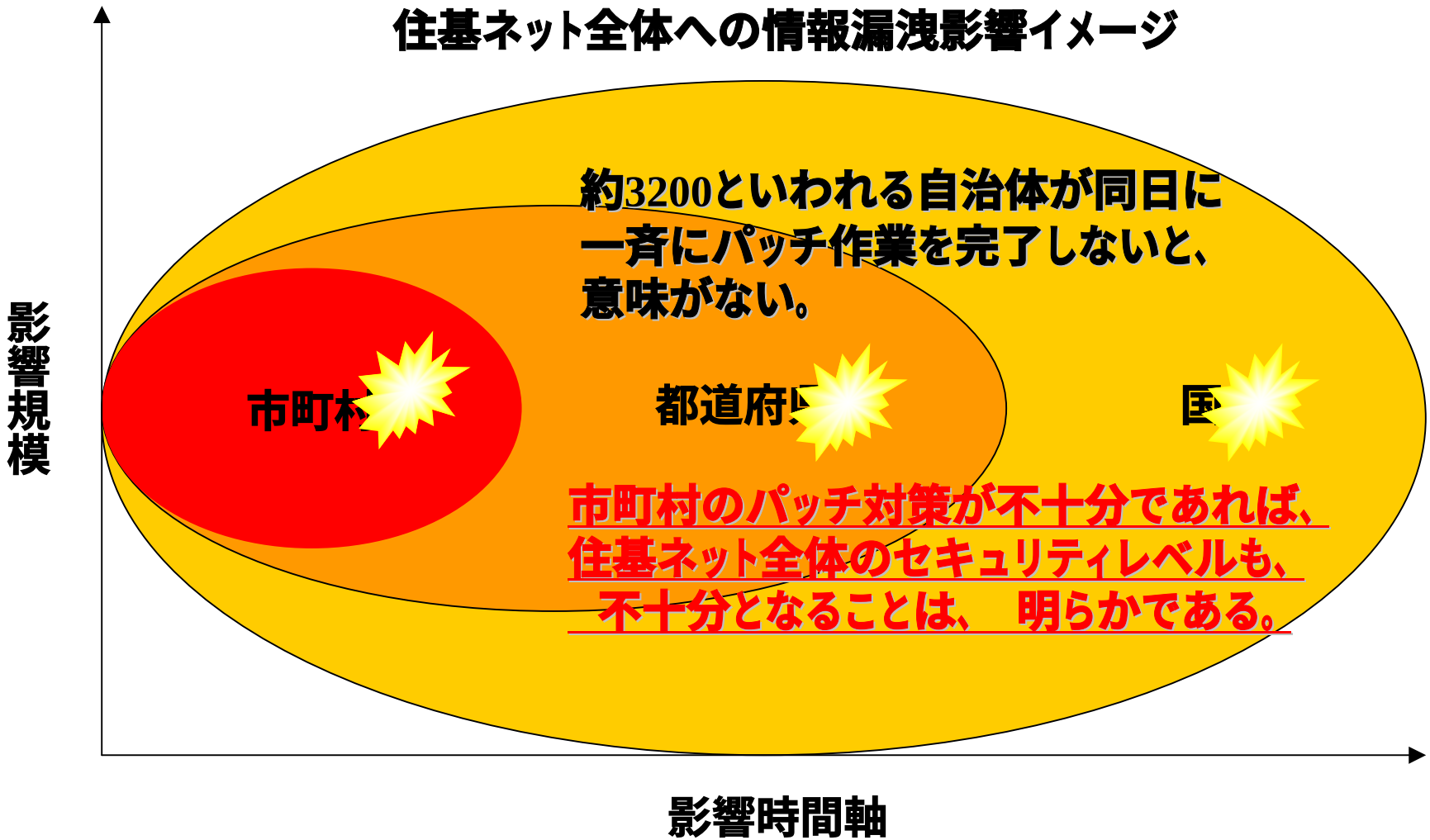
～目に見えない脅威論は、非現実なのか～

- 既存住基ネットワークはパスワード管理がなされていない。
- サーバーと端末は、パッチが対策が最新でない
- ファイアーウォールを信じ切って安心している。
- 自治体にはネットワークに詳しい担当職員がいない。
- 自治体の現状のネットワークを正確に管理、把握できていない。
- 国の想定どおりの理解と対策は行えていない。

2．事実から類推する想定される危険とは

フラクタル理論にみる住基ネット全体の問題を考える

- **全国一斉にパッチがあたっていないと意味がない。**



3．なにを問題視しているのか

～最低限の今できる対策は、取り急ぎパッチをあてること～

A ： パッチ対策

1. パッチがあたっていれば、とりあえず最低限の安全は保てる。

- **CSサーバーやCS端末のみのパッチ対策では意味がない。**
- **庁内ネットワークの端末や既存住基を含むサーバー群すべてに最新のパッチ対策が最低限必要**
- **パッチさえあたっていれば、最低限のいいわけには、なりうるはず。**

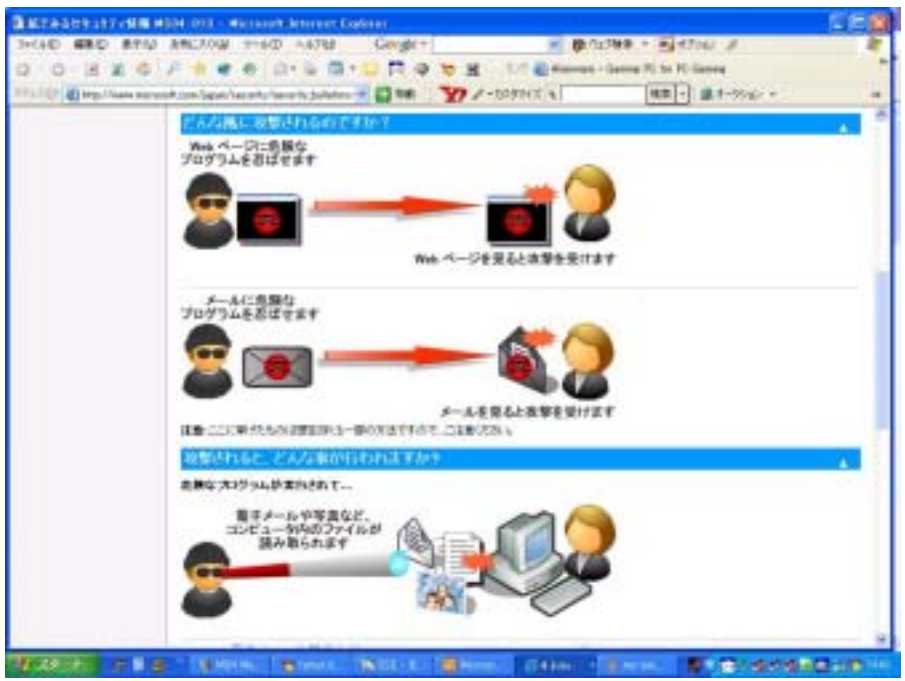
2. 全国の約３２００の自治体が一斉に同時にパッチを当てなければ意味がない。

3. 既知のパッチがあたっていても、未知の驚異には役に立たないことは理解しておく。（プロ中のプロには役に立たない）

パッチ（つぎはぎ）とはなにか

1. 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。
コンピューター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が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、ウィ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。～ＭＳ社ホームページより文書抜粋～

http://www.microsoft.com/japan/security/security_bulletins/



脆弱性を発見してもメーカーに報告しない

～そもそも、報告、通告の義務はない～

1．Windowsは世界でもっとも利用されているOSになりましたが世界中で利用され急激に大きくなったため、
最初は善意で脆弱性を見つけた技術者もメーカーに報告していましたが、最近は脆弱性を発見しても
メーカーに報告せずに自分で脆弱性をつく手法やプログラムを構築しメッセンジャーやチャットを通じて
流通させています。

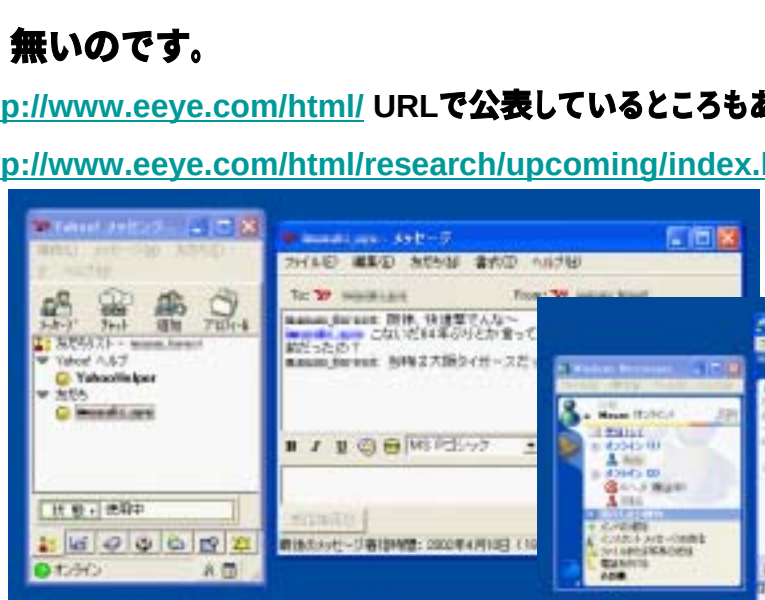
2．このため、メーカーのパッチ対策ソフトをあてて対策を実施し安心していても、メーカー自身が脆弱性を発見し
対策パッチを構築し公表するまでの間は、脆弱性にパッチ対策を打つことが、できないのです。

3．スキルのあるエンジニアたちは世界中に分布し且つ、一瞬にして情報やツールを入手し続けるのでパッチ対策が
万全の対策とはいえなくなってきています。

4．つまり、万全なセキュリティ対策などは存在せず、常に最新の情報を収集、解析、対応を繰り返す以外に方法は
無いのです。

http://www.eeye.com/html/ URLで公表しているところもある。

http://www.eeye.com/html/research/upcoming/index.htm



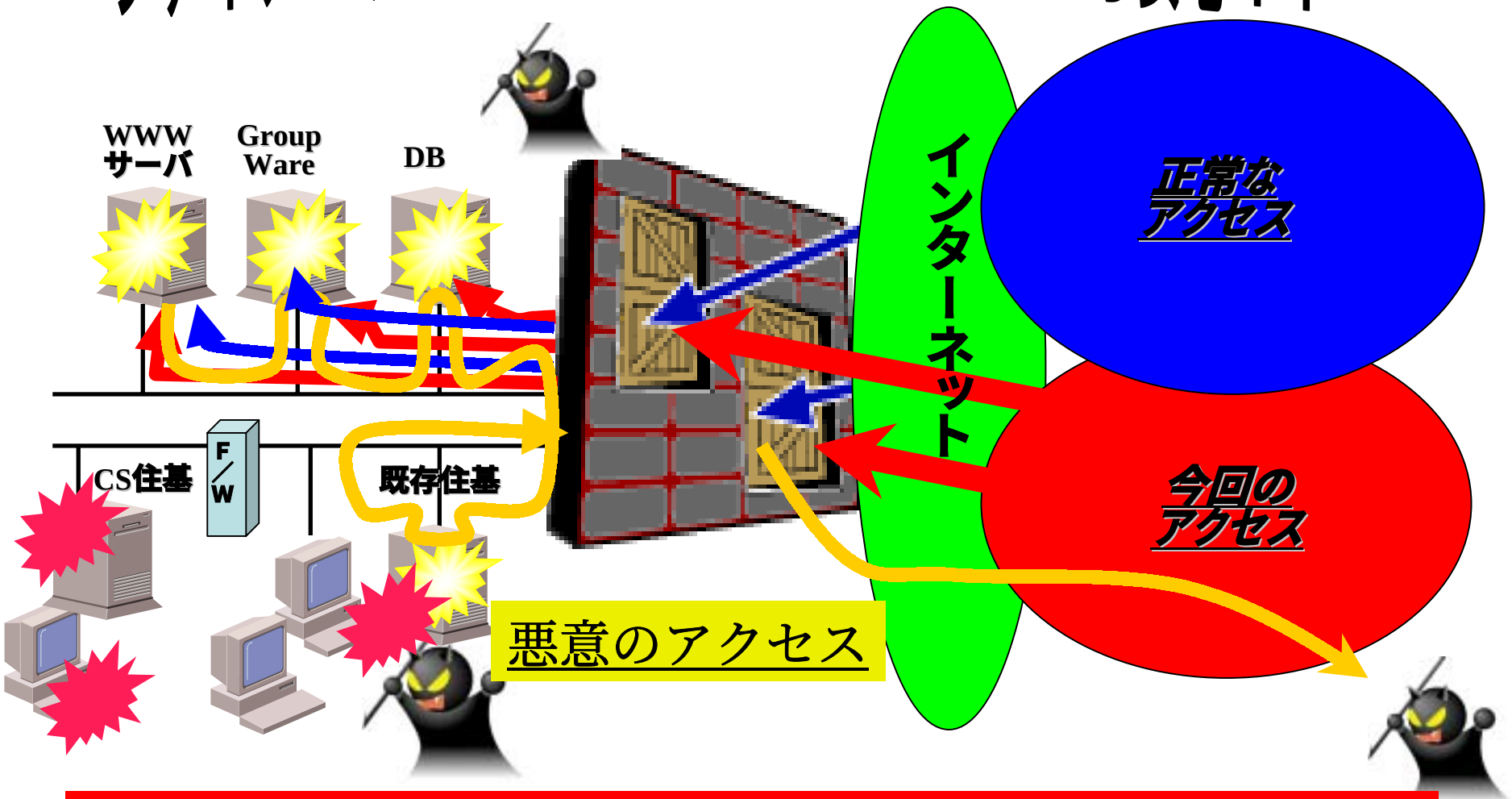
3．なにを問題視しているのか

～ファイアーウォールは突破の問題ではない～

B ： ファイアーウォールを理解する

～通信自体の危険性や不正なアクセスか否かはファイアーウォールでは判定できないのです～

ファイアーウォールが突破されていない？から安心？！



これを突破していないと表現するのが正しいのでしょうか

３．なにを問題視しているのか
～十分な説明もなく安全と、うたうべきではない～

１．８月の長野県個人情報保護審議会ですでに本人確認情報保護改善案を
具体的に提案している。

２．国の部分はテストしていないので安全かどうかは解らない。

そもそも、ドアもノックしていない。

３．LASDECの２４時間監視の質は民間業者で行えば年間３００万円以下で

有名大手が手がけているレベルでしかない死活監視のみとわかった。

４．このレベルでは不正なアクセスを検出すらできないことも明らかにできた。

５．国の部分が守られているから住基ネット全体が安全という話にはならない。

既存住基の内容を改竄し転出すればＣＳサーバーに１４情報が移動し

転出先の既存住基そのままコピーされ住基ネットのなかを４情報以外の

データーが流されている。

3．なにを問題視しているのか
～物理的に目に見える範囲の問題ではない～

6．出先施設の安全性は不十分であった。簡単に庁内LANに入れた。
庁内施設の安全性確保だけでは不十分で、遠隔施設の安全性も確保する必要がある。とくに出先からISDNによる公衆回線で庁内ＬＡＮ接続しており住基ネットが公衆回線に接続されていることが明らかになった。
発信者番号チェックやコールバック機能だけでは不十分である。

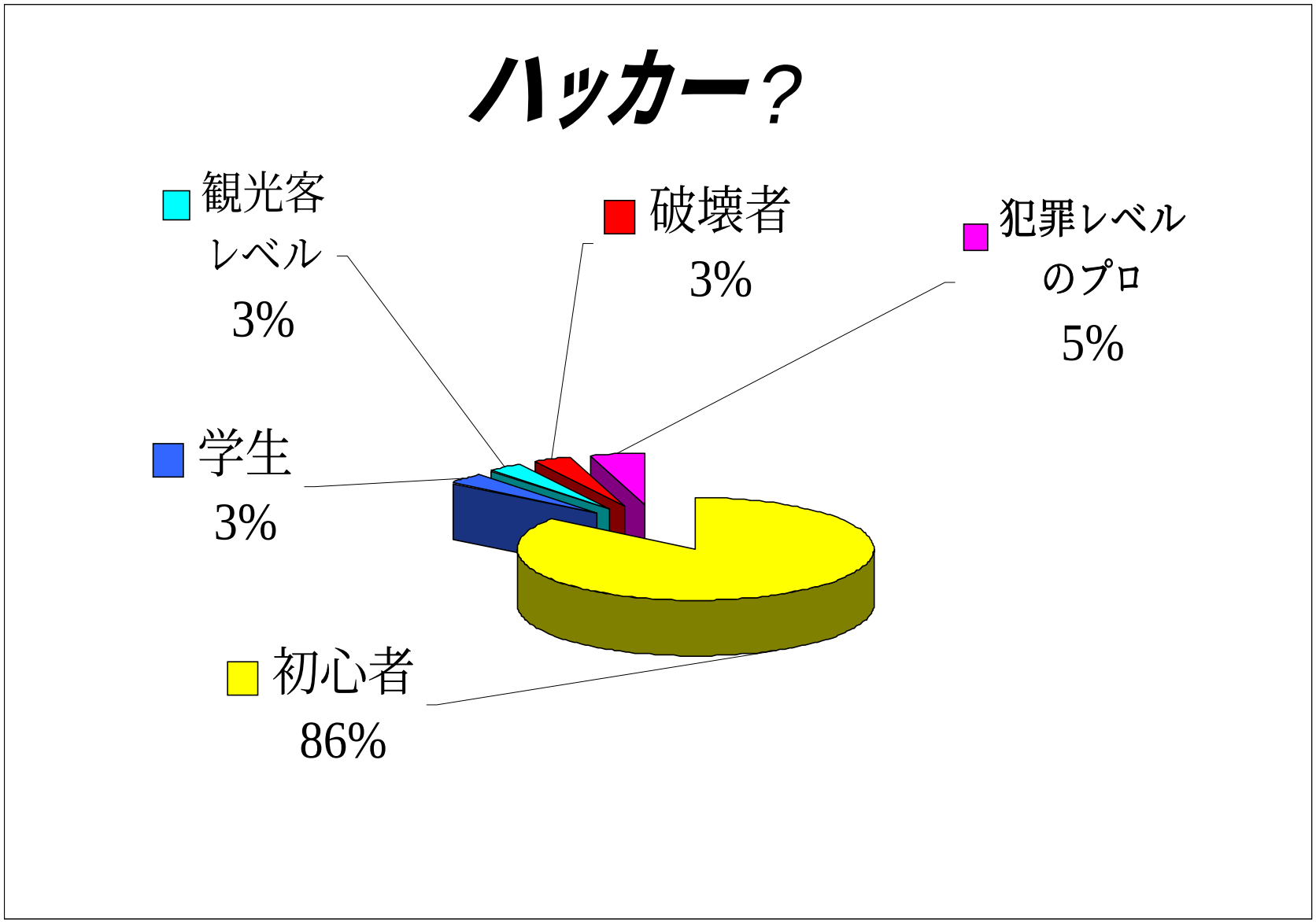
7．ラックの鍵を持ったことは実験の価値がないとの声が多いが実際には庁内であれば場所に関係は無く、どこからでもアプローチは同じである。

8．他の都道府県の多くは未だ長野県レヴェルには達していない。

9．今後より具体的な対応策を今回の実験を受けて精査して提案したい。

3．なにを問題視しているのか

～現状では、初心者レベルのアッタクで十分侵入を許してしまう状態～



3．なにを問題視しているのか

初心者に管理権限を奪われればお粗末

～コンピューターの脆弱性を突いてくるのは興味本位の子供たちが増えている～

1．雑誌や書籍に付録としてついてくるCD-ROMやDVD-ROMは、小学生や中学生で十分理解できる内容といえます。

2．専門的な知識は必ずしも必須とはいえず、パッチ対策が不十分であれば十二分に管理者権限を奪取されかねない。

3．つまりプロ中のプロだけがネット犯罪を起こすのではなく、低年齢化が加速しており、罰則を強化しても未成年で罪を問うことも難しくなってきているのです。

4．どうすればよいのか①

～ありもしない脅威論で済ませられない～

1．安全性を具体的に説かなければ安心できるものではない。

2．国の安全性の根拠情報を公表することがセキュリティホールになるという声があるが、
驚異の可能性を調査した長野県の実験結果を具体的に公表することの方がセキュリティホールになることは明らかであり、国の安全性を立証することの方が先に行われるべき行為である。

3．今般の長野県に対する報告書が公開されることで、それ自身がセキュリティホールとなる可能性を払拭できない。

4．これらはコンピューターの専門家でないとわからない問題ではなく極々初心者でも、良く考えれば、簡単に理解できる仕組みである。

5．技術論をいくら加速させても技術的なセキュリティ対策のみではカバー仕切れない。

6．世界でも日本でも多くの人間が、コンピューターを操作しているが操作していることと、
基本的なことを理解しているということは別だということです。

＜事実＞http://www.yomiuri.co.jp/net/feature/014/20040619fe02.htm

２００２年秋、世界中のインターネットが重大な危機に見舞われたことは、あまり知られていない。
ハッカーが、ネットの基幹コンピューターである「ルートサーバー」に、電子的な一斉攻撃を仕掛けた。
世界にはたった１３台の名前解決サーバー存在しておらず　一時７台がダウンした。

4．どうすればよいのか②
～驚異に対応する安全性の詳細を説くべき～

7．法律ができて、実行すべき時期が来たから、実は万全の準備ができていないにも関わらず、できる、安全だということにして、スタートすることはこの世界では通用しない。

8．隅々まで、安全性を確認しなければならないにもかかわらず、一部分だけでなぜ良しとしているのかが重大な問題である。

9．ＢＳＥでも全頭検査といっているのに、長野県の一部でさえ重大な問題が浮かび上がってきたにもかかわらず全体が安全といえるものではない。

10．ＬＡＳＤＥＣには、そもそも扉もノックしていないので国側が侵入されていないのは当然であるにもかかわらず、安全を強調するの暴言でしかない。

11．安全、危険の話ではなく、どう読み取るかがポイントの議論であると考える。

12．にもかかわらず、特殊性やリスクを考えないで、こういった制度を全国一律に行政に採用するのは、本質的に問題である。

4．どうすればよいのか③
～驚異に対応する安全性の詳細を説くべき～

13．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行えば良い
システムが住基ネットであり、そのノウハウを後に続く自治体に指導してゆければ、
広がりもある。

14．安全対策を十分に行えない自治体は、問題の旨、今や総務省も認めている。
地方交付税支出の事務連絡も出している点でも明らかである。
国は元々の範囲を超えていることを許容し理解している。

15．むしろ、安全はどのように、確立されているのかを国自身が確認しなければならない。
逆の発想で考えるべき議論です。

16．全国の端末が安全を担保されなければ、安全は国として保証できない。

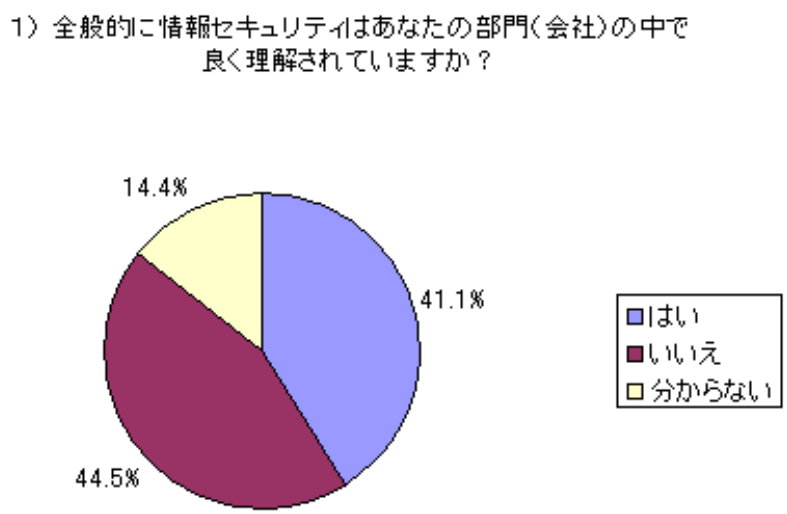
17．鍵のかかる部屋も、全国で徹底されていない。
全国すべての安全確認を自己申告のアンケートで立証できるはずがない。

18．物理的にも危険な状態を数多く自身の目で確認した。
間違いなく長野県だけでなく、全国の他のところにもたくさん問題があるはず。
そんな、なかを個人情報が飛び交うことを安全といえるはずがない。

5．なにをもって良しとするべきなのか

～ネット管理者は辛い！～

- あるエンドユーザ意識調査
- 難しい情報セキュリティ
  - 利便性とセキュリティのバランス
  - 担当者の悩み
    - 上司の問い掛け『ウチのセキュリティは大丈夫かね？』
    - 人手と予算は？コスト削減を真っ先に求められるのに…
      - 年中多忙で評価は？
      - 何もなくて当然、何か起これば…
    - セキュリティは利益を生まない…
    - 個人情報と運用の板挟み
    - 情報収集に終わりはない
    - 知っていて当然・・・
    - 問題発生でスキルが疑われる



http://www.iaj.or.jp/bukai/isec/survey/200002/

5．なにをおもって良しとするべきなのか
～性悪説にたつこと～

- 何から手をつければ良いのか？
  - 即座に実行すべきこと
    - パッチをあてる。(常に最新でなければ意味がない)
      ＜サーバーＯＳだけでなくＦＷやルーターに至るまで管理が必要＞
    - パスワードは厳格に管理する
    - 設定見直し
    - 委託業者とのSLAの確認
  - 多少時間をかけて検討すべきこと
    - 現状評価を定期的に行う
    - ポリシーの立案･実行
- 防御はどうすれば良いのか？
  - セキュリティ対策を実装したシステム構築･運用 (維持)
    - 最新バージョン管理
    - 設定の合理性を追求する
    - 保険をかける
    - SLAを厳格にする
    - 生体認証も偽装は可能、完璧は無い
      http://www.yomiuri.co.jp/net/feature/014/20040617fe01.htm
    - ルールーや罰則を作るだけでは無意味

5．なにをもって良しとするべきなのか
～性悪説にたつこと～

「性善説」では絶対に防げない

1．機密情報を守る性悪説セキュリティ対策

- 「内部セキュリティ対策」の構造を理解する
- 内部からの「不正アクセス」を防ぐ仕組み作り
- 漏えいを検知し再現できる仕組みをつくる
- 「抑止力」になるルールとモラールの確率

2．F/Wがあるから安全という技術神話は崩れた。

3．波田町はなぜ今は安全だったのか

- インターネットと分離が無意味だったのではなく、サーバを完璧に守ったことが今回はたいへん有効だった
  サーバやPCのセキュリティホール対策が重要ということであり、
  不具合が見つかったら直せばいい、という考えは技術的には
  通用しない。

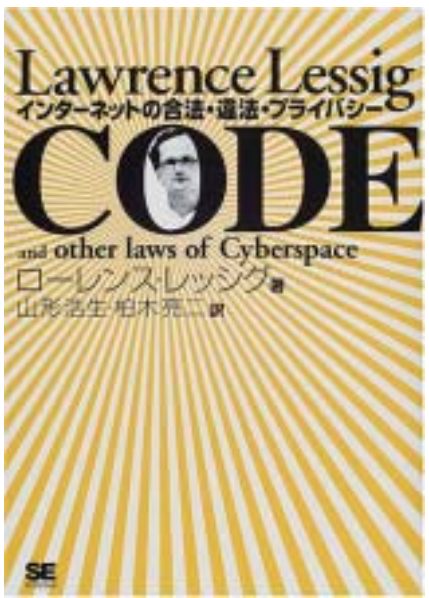
まとめ

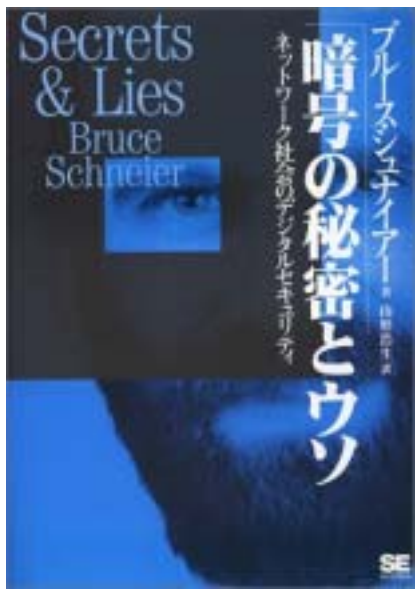
①パーフェクトなセキュリティを求めるな
②間違った解を解くな（銀行のネット犯罪被害は小切手詐欺の１０％）
③全体でセキュリティの問題を考えろ
④暗号の掛け過ぎは正しくない
⑤高価にするな（何かを買えば済む話ではない）
⑥防御ラインは1つ（FW)だけでは意味がない
⑦アタックがあることを忘れるな
　（いきなり本丸からは狙えない、兆候を見逃すな）
⑧システムを信じるな
⑨人を安易に信じるな
⑩出来ないことは、するな！

～ＲＳＡ暗号システムの開発者であるアディ・シャミア博士の講演より一部抜粋～

参考になる書籍群ほか

- CODE — インターネットの合法･違法･プライバシーローレンスレッシグ山形浩生訳
- 欺術 (ぎじゅつ) 史上最強のハッカーが明かす禁断の技法ケビン･ミトニックウィリアム･サイモン
- 暗号の秘密とウソBruce Schneier (著, 山形浩生訳)
- リトル★ハッカー「ハッカー」になった子供たちダン･ヴァートン山形浩生訳





参考になる映画

■■映画編

○エネミー・オブ・アメリカ
http://www.amazon.co.jp/exec/obidos/ASIN/B00005EKWM/qid=1089958723/sr=1-1/ref=sr_1_2_1/250-4123517-1345057

『ワイルド・ワイルド・ウエスト』のW・スミス主演のサスペンス・アクションが再発売。
国家の陰謀に巻き込まれ、命を狙われる身となった弁護士の苦闘を描く

○ザ・インターネット
http://www.amazon.co.jp/exec/obidos/ASIN/B0000CD7OW/qid=1089958846/sr=1-1/ref=sr_1_2_1/250-4123517-1345057

すべてがコンピュータに管理される高度情報化社会を舞台に、見えない敵にたった一人で立ち向かうヒロインの姿を描いた、
サンドラ・ブロック主演で贈るサスペンス。

○ザ・ハッカー
http://www.amazon.co.jp/exec/obidos/ASIN/B00005LMSH/qid=1089958892/sr=1-1/ref=sr_1_2_1/250-4123517-1345057

実際の事件を基にしたパニック・サスペンス。天才ハッカー、コンピュータ保安問題の専門家、FBI捜査官の、3者の攻防を描く。
『スクリーム』のS・ウーリッチ主演。

○マイノリティ・リポート
http://www.amazon.co.jp/exec/obidos/ASIN/B0000QX4B6/qid=1089958929/sr=1-1/ref=sr_1_2_1/250-4123517-1345057

2054年のワシントンDC。犯罪予防局の刑事ジョン・アンダーソンは、予知能力者・プリコグの透視により、次々と犯罪を未然に防いでいた。
ところがある日、プリコグが透視した犯人の名がジョンだったことから、彼は予防局に追われる立場に追い込まれる…。

○スニーカーズ
http://www.amazon.co.jp/exec/obidos/ASIN/B0001ZX0YM/qid=1089959044/sr=1-1/ref=sr_1_2_1/250-4123517-1345057