～Winnyなんて氷山の一角！？～

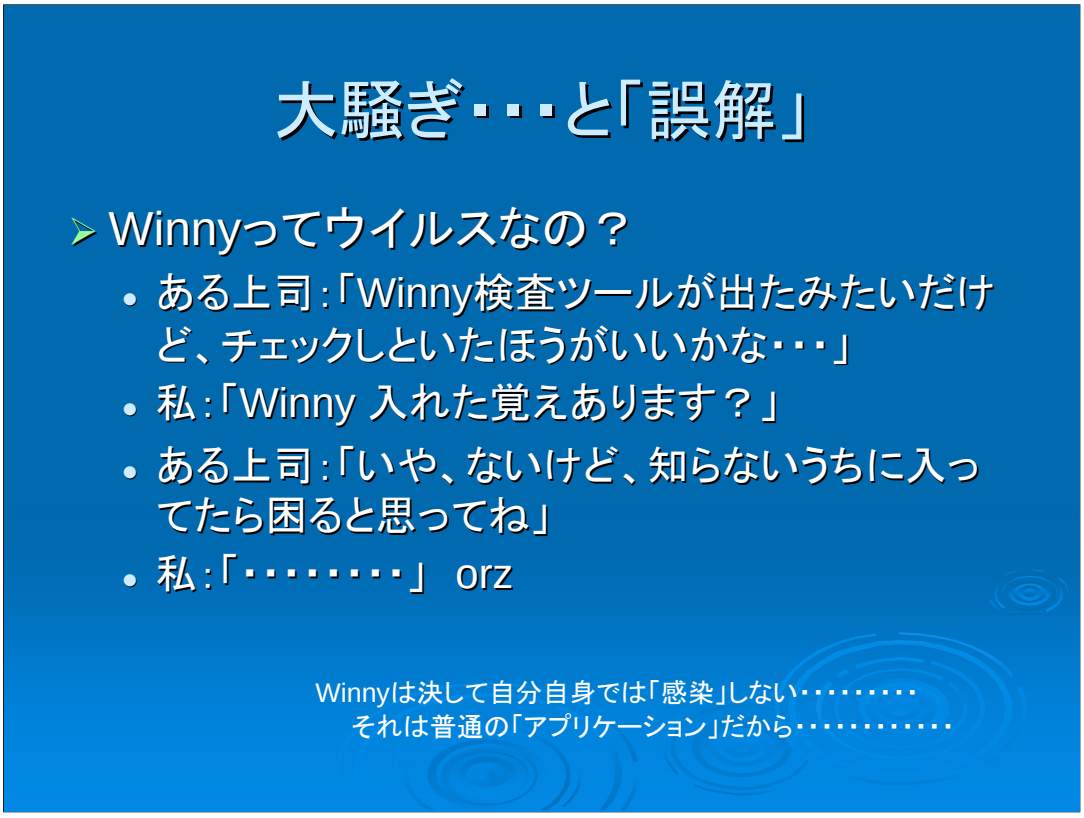
情報漏洩がおきる本当の理由

住商情報システム株式会社　情報システム部
二木真明
(NPO日本ネットワークセキュリティ協会幹事、技術部会長)

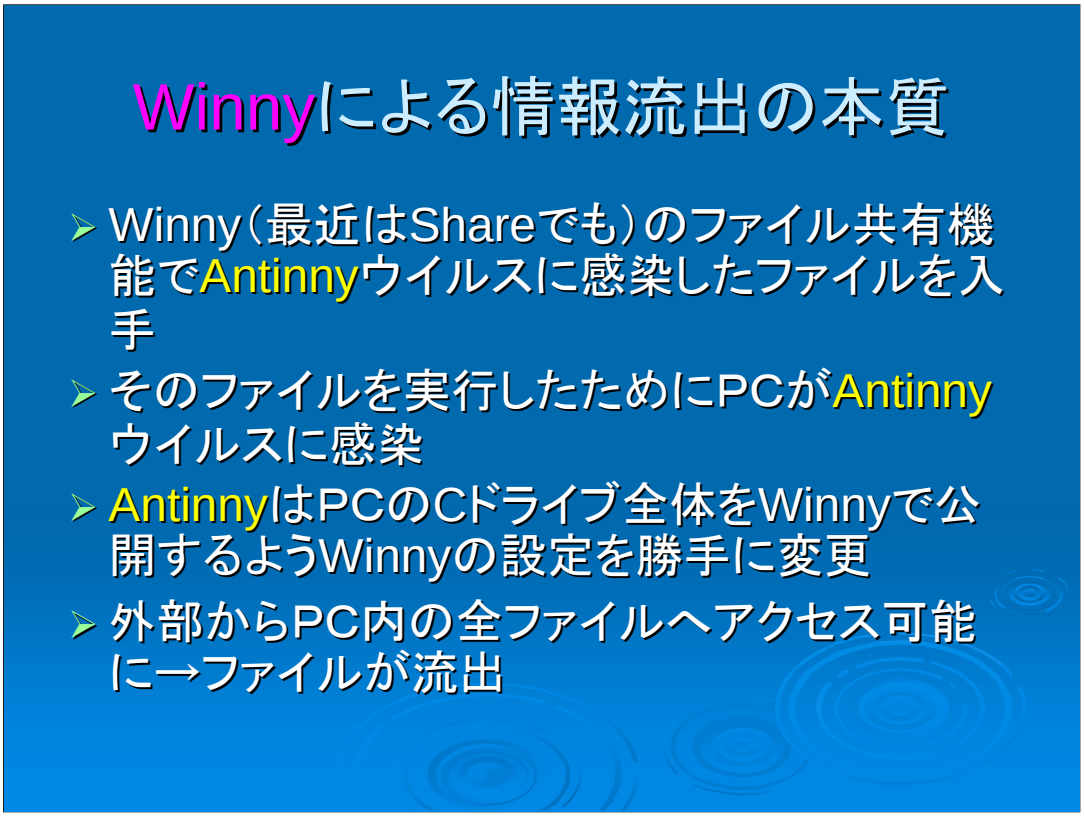
官民・産学を問わない”Winny”事件

- 米軍三沢基地　個人情報流出
- KDDI顧客情報流出
- 海上自衛隊　機密情報流出
- 東京地裁書記官のPCから個人情報が流出
- 北海道武蔵女子短期大学　合否情報流出
- ボーダフォン　基地局関連個人情報流出
- 北海道職員の個人情報流出
- ・・・・・・・・・・

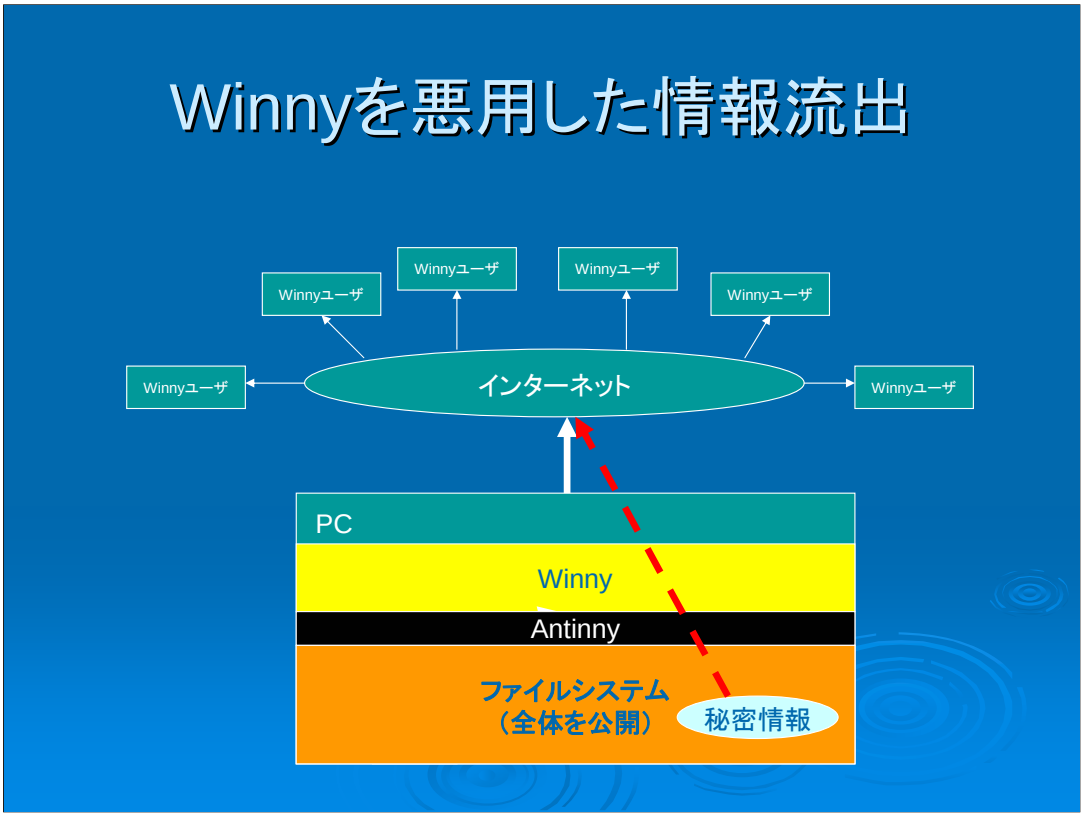
まさに日本全国、Winnyに困惑、狼狽・・・というのが実際だろう。いまやWinnyは「悪」の代名詞となりつつある。官民・産学を問わず、多くの組織が”Winny”規制に走る中、実はもっと大きな問題が「Winny問題」に矮小化されてしまっていたりしないだろうか・・・。



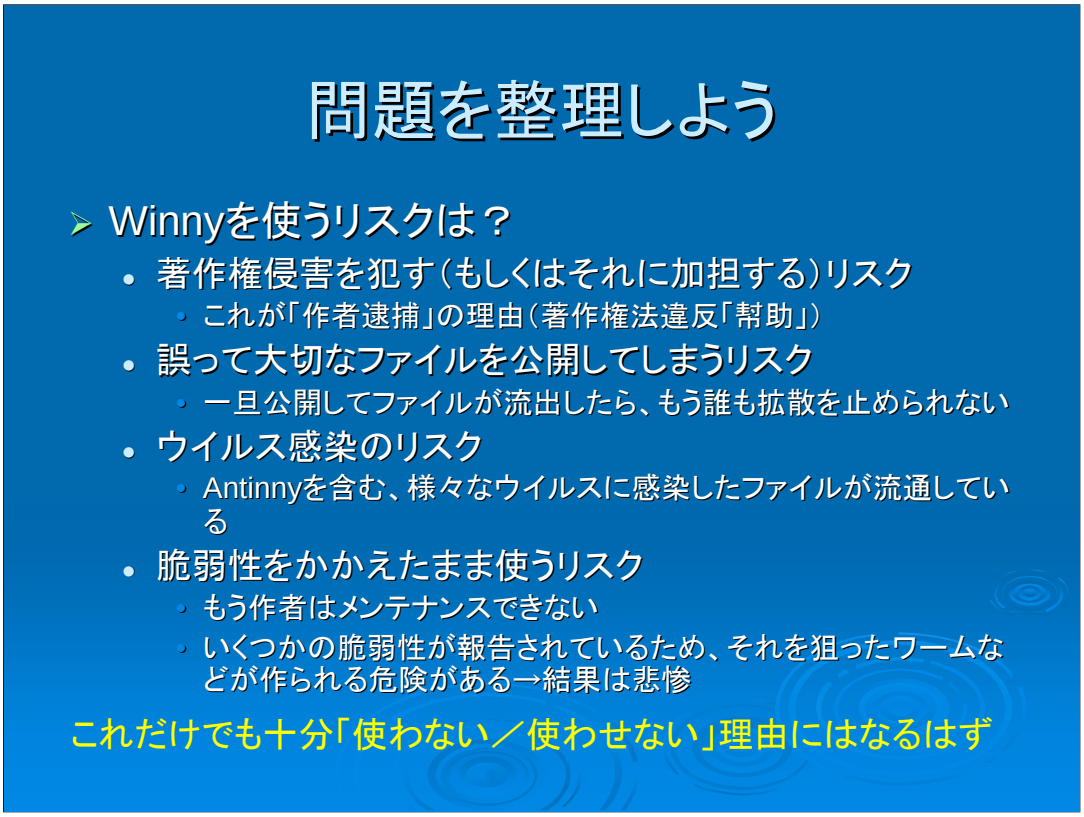
たとえば、これは実際にあった話だが、Winnyを「ウイルス」のように伝染していく（恐い）不正プログラムだと思っている人も少なくない。この例は、決して「おバカな上司」の例ではなく、WinnyやAntinnyウイルスをよく知らない普通の人なら、この騒ぎをみて陥りかねない誤解だと思っている。



Winny から情報が流出する過程は、このようなものだ。Winnyを使っているから情報が流出したのではなく、Antinnyというウイルスに感染したことが直接の原因である。もちろん、Winny（最近はShareも対象になるが）を使っていなければ、Antinnyは悪さをできないし、そもそもAntinnyを拾ってしまう危険も少ない。だが、この「ウイルス感染」という事実があまり強調されていないことが、今後の展開において危険な要素となる可能性がある。

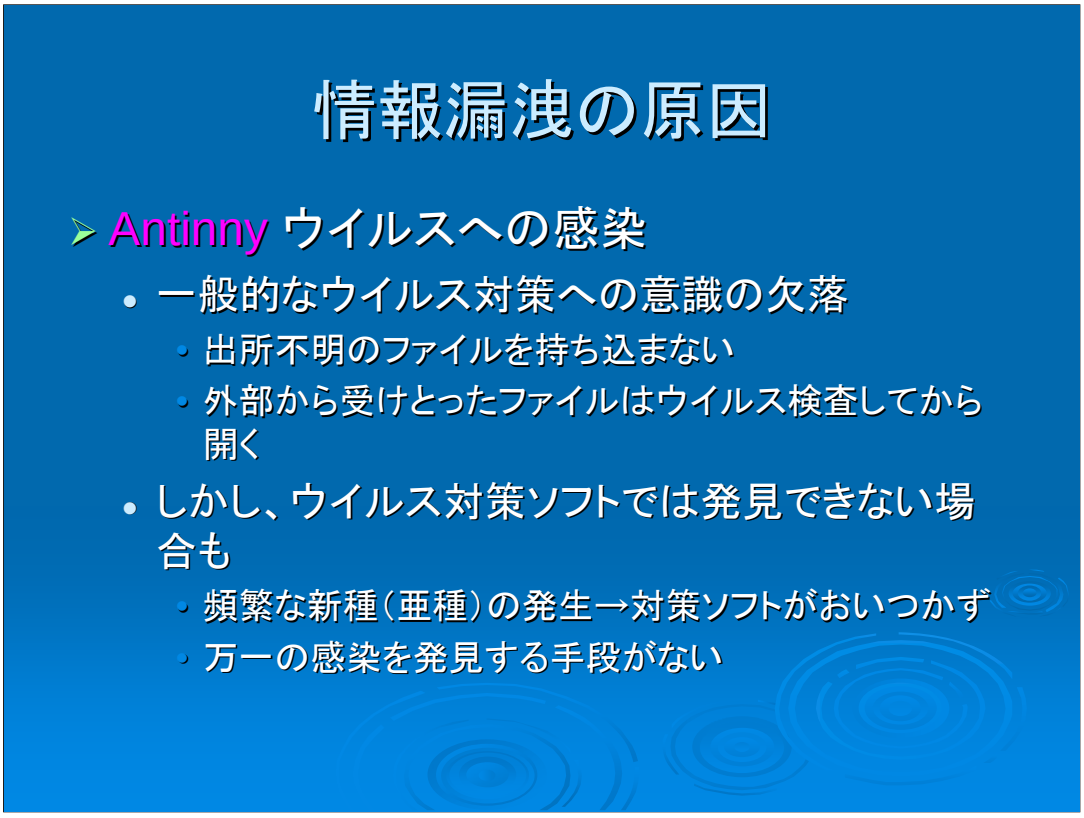


先のページの図を模式化すればこのようになるだろう。



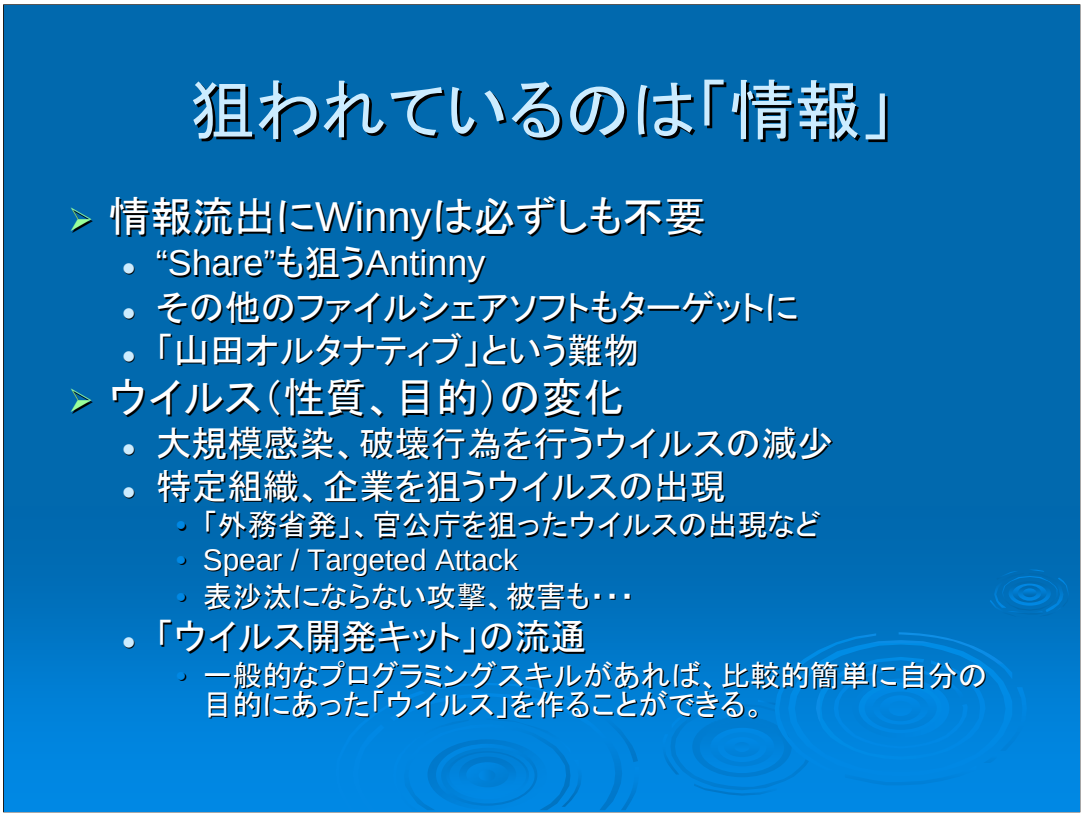
ここで問題を整理してみる。

もちろん、Winnyを使うこと自体にも様々なリスクがある。情報漏洩を一旦脇においたとしても、これだけの理由があれば、Winnyを「危険なプログラム」と位置づけるに十分な理由となるに違いない。だから、組織のみならず個人もがWinnyを使わないようにする、というのは、一般論から言えば理にかなったことだろう。



一方で、「ウイルス（Antinny）感染」という問題だけを考えてみれば、これは一般にいわれているウイルス対策の基本ができていないということにほかならない。

但し、「ウイルス対策」の概念はここ数年で大きく変わっている。ウイルスの進化と拡散の速度が非常に速くなり、いまやウイルス対策ソフトは万能の防具とはなりえなくなった。ウイルス感染に長い間気付かない可能性も高くなってきている。



Antinnyはたまたま、winnyという既存のアプリケーションが作ったネットワークを使って情報を流出させた。これは、winnyネットワークの特性を考えると極めて有効な流出方法だが、P2P技術をベースとしたファイル交換ソフトには、同様の特性があるため、ウイルスに狙われやすい。しかし、一方で、まだまだ稚拙なものだが、「山田オルタナティブ」と呼ばれるウイルスは、もはやこうしたファイル交換ソフトを使わずに情報流出を手引きする。Winnyに気をとられていると、知らない間に別の危険を見逃してしまう可能性も高いのだ。

また、ウイルスを作る側の動機も変化しつつある。愉快犯的な大規模感染のデモンストレーションは最近では少なくなり、一報で、特定の組織や業界を狙って、ウイルスが送り込まれるといった事件が起き始めている。このような小規模な感染を狙ったウイルスは、もはやウイルス対策ソフトではほとんど検知できない。

このような状況を考えると、今後の情報漏洩（流出）（というよりも、情報窃盗犯罪といったほうがよい）にこのようなウイルスが使われる可能性は極めて高いといえる。ウイルスの製作は特殊な技術と思われがちだし、実際にこれは高度な技術だが、最近では「ウイルス開発キット」のようなものがインターネット上で流通している。犯罪者に少しプログラミングの経験があり、こうしたキットを入手できれば、自分の目的にあわせたウイルスを作ることは、いまや困難ではない。

実際にもしかしたら、誰も気付かない情報漏洩事件が、日本の企業で頻発しているのではないか・・・・これが杞憂に終わって欲しいと心から思う。

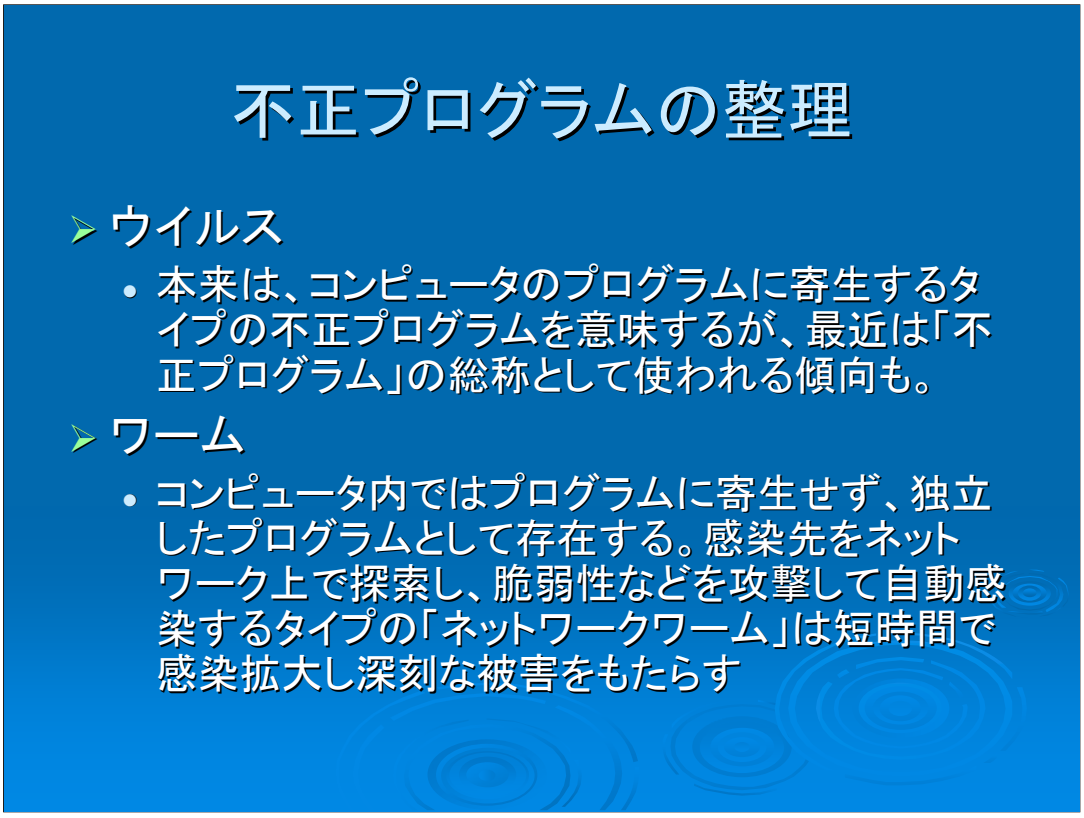
恐いのは「ウイルス」＝不正プログラム

- 山田オルタナティブ
  - 感染するとPCのCドライブをWindowsのファイル共有でアクセス可能にしてしまう
  - そのPCのインターネット接続IPアドレスを「2ちゃんねる」掲示板に書き込み
  - PCが常時接続されていると、知らない間に情報を外部から参照されてしまう
  - ルータ、ファイアウォールが入っていても安心できない＝（今後は）UPnP悪用の可能性もある

これが「山田オルタナティブ」の動きだ。

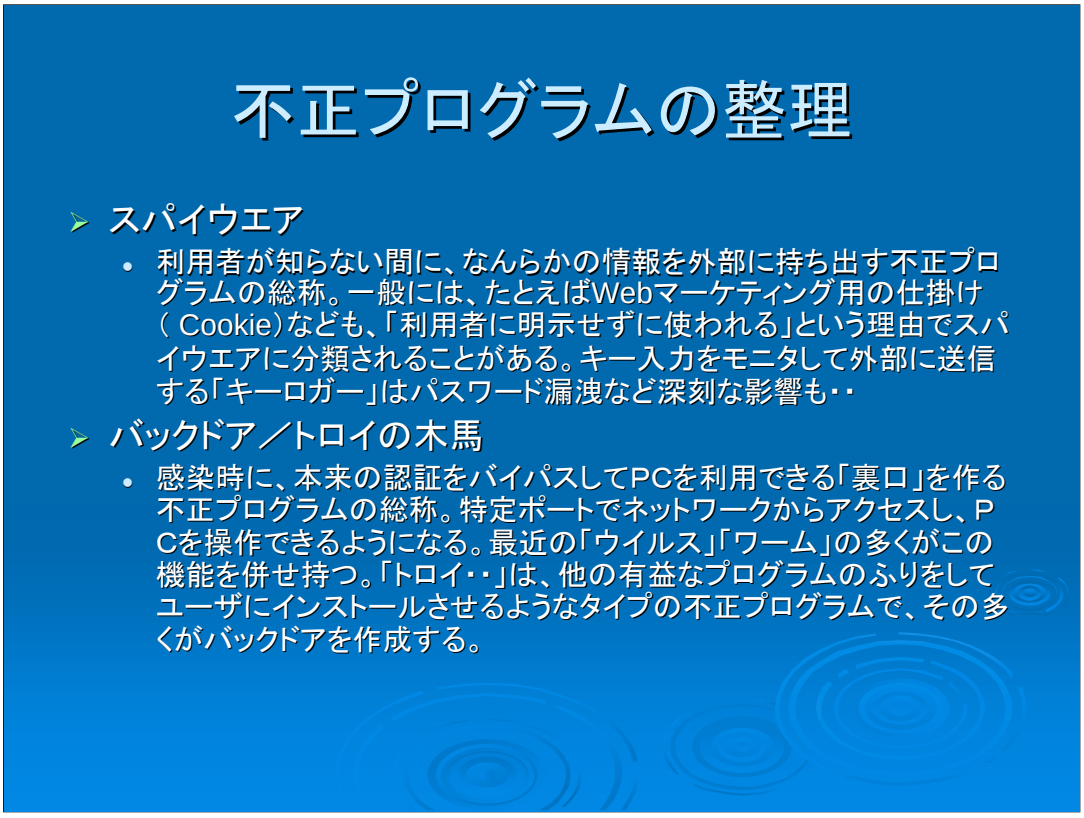
これは、まだまだ「愉快犯的」なものである。しかし、この情報書き込み先が2ちゃんねるではなく、犯罪者のサーバだったら・・・と考えると、事態はかなり深刻だ。

このウイルスが作れた、ということは、同様の、より悪質なウイルスも、これをベースに簡単に作れるからだ。



ここで、ウイルス＝不正プログラム関連の言葉を少し整理しておこう。

マスコミには様々な言葉が氾濫し始めているが、多少混乱も生じている。過度の不安や、過小評価を避けるためにも重要なことだ。

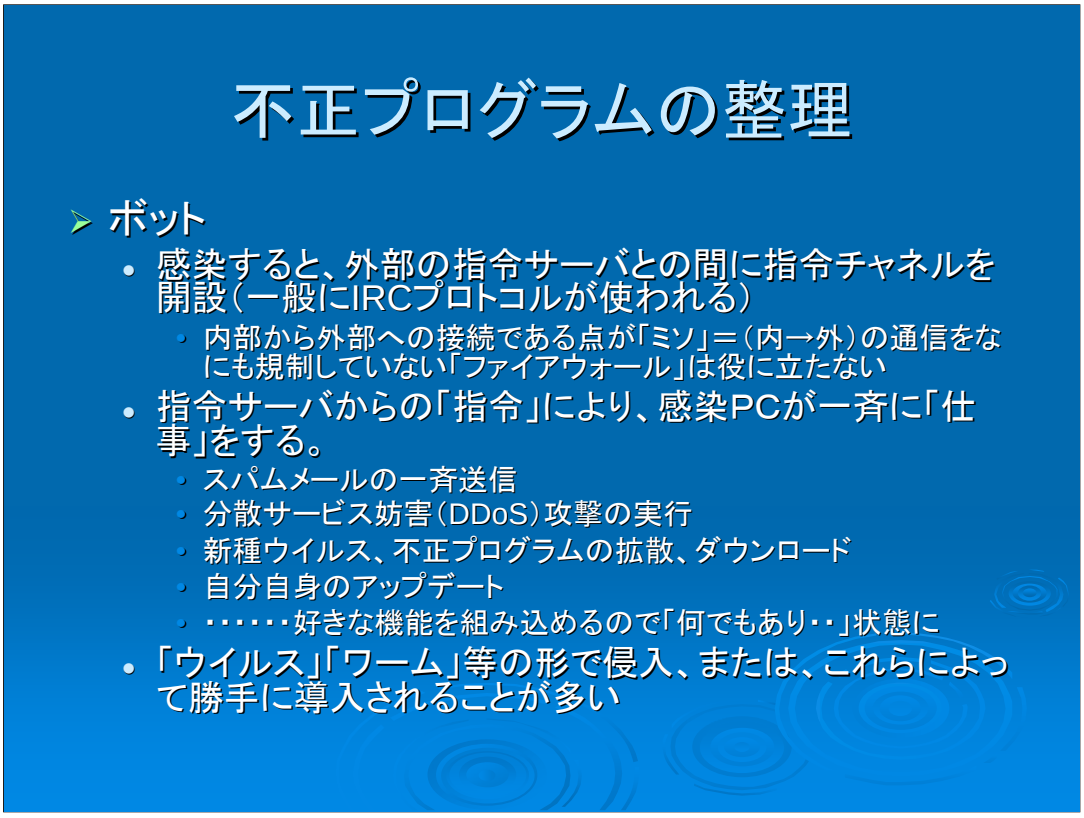


スパイウエアの位置づけは、かなり広い。「スパイウエア対策ソフト」は一部の商品や、Webマーケティングに使われる手法をも、「スパイウエア」として分類しているが、その理由は「ユーザが知らないうちに、なんらかの情報を外部に提供する」というスパイウエアの定義に基づいている。従って、スパイウエアに分類されるものには実害のほとんどないものから、キーロガーのような、深刻な問題をひきおこすものまで、様々なものが含まれる。

バックドアは、たとえば特定の通信ポートで待ち受けて、接続者に本来の認証を経ないでPCの操作を許してしまうような仕掛けである。現在のウイルスやワームの多くが、副次的にこうしたバックドアを作る機能を持ち、またそうしたウイルスが作ったバックドアは他のワームなどの攻撃対象になったりもする。

トロイの木馬は、たとえば「便利なツール」をインストールしたら、実はバックドアが出来ていた・・・というように、別の目的のツールに見せかけて、もしくは潜んで、不正な操作をするタイプの不正プログラムで、多くの場合はバックドアを密かに設置するような目的で使われる。いわゆる「トロイの木馬」に兵士が隠れて城塞を内部から攻撃した話と同じような形だ。

バックドアを悪用するためには、基本的にはそのコンピュータに接続可能なネットワークに攻撃者が存在する必要がある。たとえば、社内ネットワークにいるPCの場合、ファイアウォールがあるため外部からの接続は困難だ。しかし、このようなPCが、たとえばノートPCで、外部に持ち出してインターネットに直接接続すると、外部から侵入される危険が生じる。

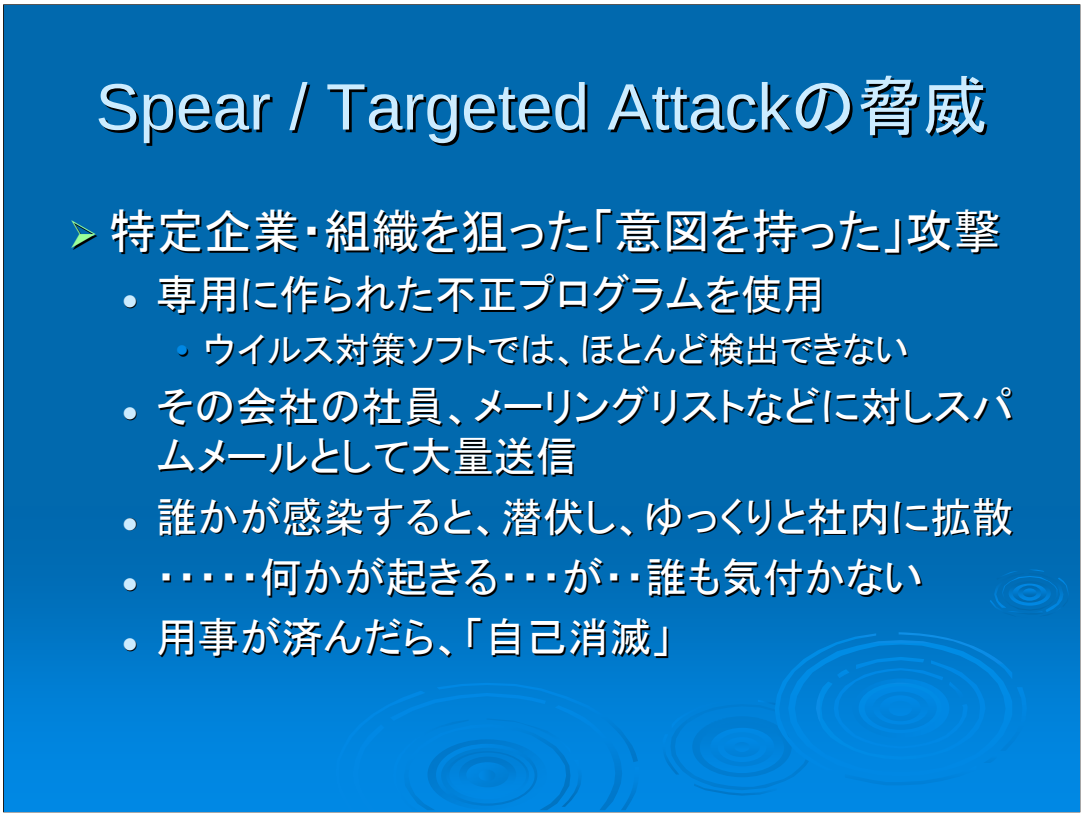


ボットは、ある意味で最もタチの悪い不正プログラムと言える。

外部からPCをリモコンできてしまう上、指令チャネルを内部側から接続するため、ファイアウォールがあっても接続できてしまう可能性が高くなる。また、自分自身のアップデートや任意のプログラムのダウンロードなどの機能をもつため、一旦入られてしまうと、なんでも好きなことができてしまうため、非常に危険だ。また、それ自体は何も派手な動きをしないから、簡単には発見できない。

このようなボットが多数接続された「ボットネット」は、スパムメールの送信ツールとして使用されたり、特定のサイトに対して過大な負荷をかける分散型のサービス妨害攻撃（DDoS）などに利用されている。しかし、これを特定の企業や組織への攻撃に利用するようなことも可能だ。密かに侵入して拡大し、ある日突然、活動を開始して情報システムをマヒ状態に陥れることもできる。

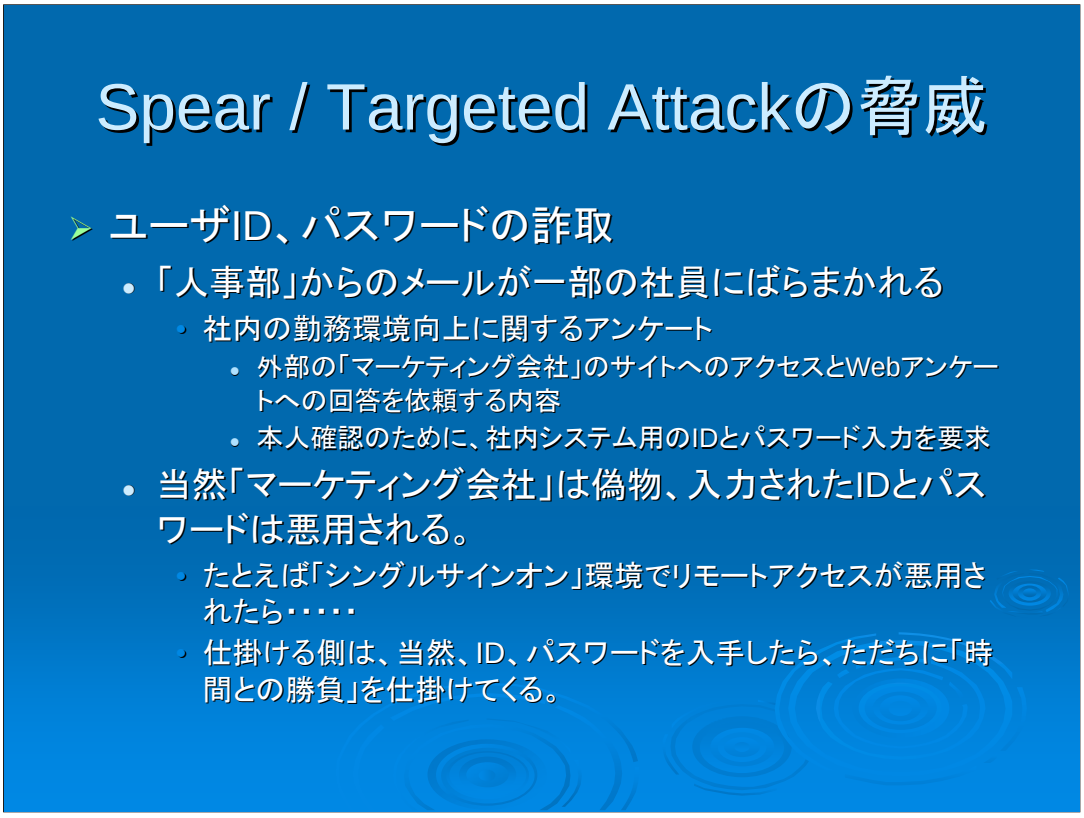
これが、各国政府や警察などが、サイバーテロの道具として危険視し、対策を検討しているゆえんである。



かつて、ネットワークからの攻撃は、「これみよがし」的なものだったし、その動機は「自己顕示」「技術的チャレンジ」といったものだった。しかし、いまや「営利目的」の攻撃・・・つまりは「ハッカー」というよりは「泥棒」による攻撃、が多くなっているため、その手段やありかたも様変わりしている。

「専用ウイルス」の怖さを考える上で、これはいい例だろう。

大きな会社では、不審なメールを開いてしまう人は少なからず存在する。最低一人、そういう人がいれば、犯人は目的を達成できる可能性が高い。このような「オーダーメイド」ウイルスは、ウイルス対策ソフトメーカーに検体が届かないため、ウイルス対策ソフトでの検知は困難である。「未知ウイルス検知機能」に期待する人もいるが、それは間違いだ。なぜなら、ウイルス作者は最新のウイルス対策ソフトを簡単に入手できるし、自分のウイルスが検知できないことを確認することができるからである。

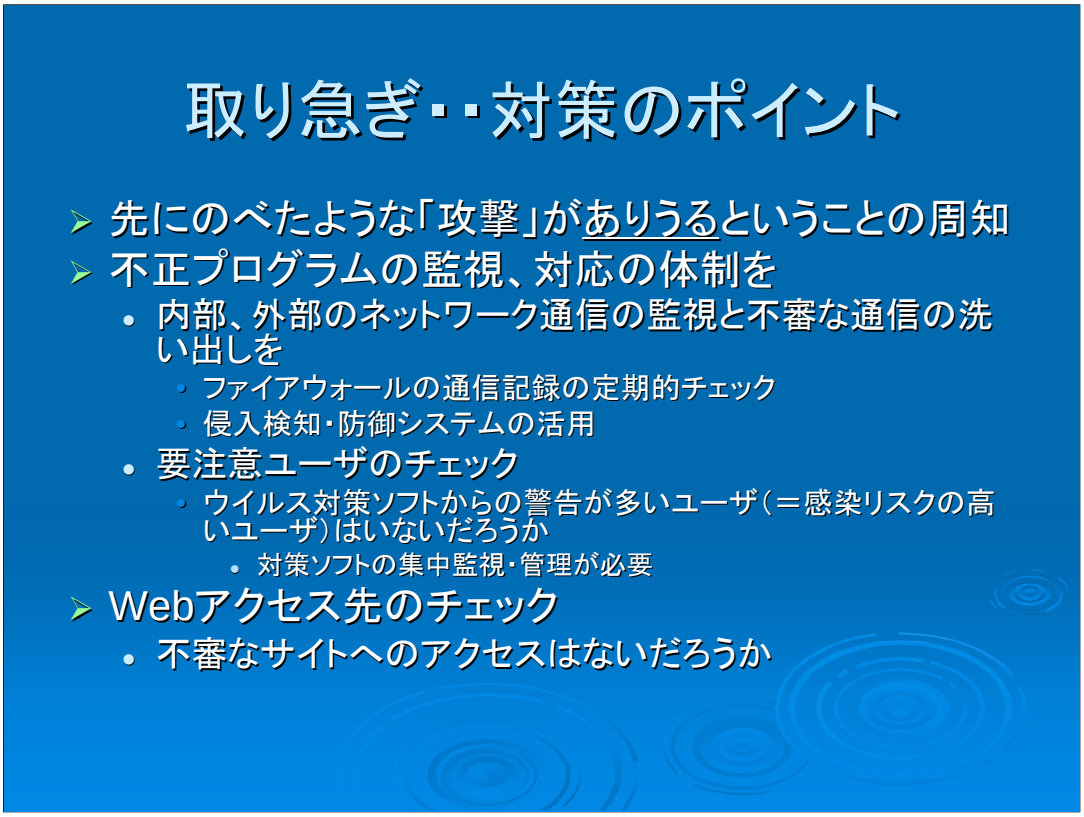


たとえば、こんな例も考えられる。

犯人は、狙っている会社がシングル・サインオン環境を構築していることを知っている。そして、社員のリモートアクセス用にSSL-VPNを使用していて、そのIPアドレスも入手できている。あとは、誰かのアカウントを盗むことができれば・・・・。という場合に、こんな手段を使うこともできるだろう。

ウイルス付きメールを開いてしまう人があとをたたないのと同様に、このようなタイプの攻撃（古典的には、電話での詐欺のようなものがあるが・・・）にひっかかる人も少なくはないだろう。

攻撃者にとっては、パスワード入手後は、いかに素早く仕事を終えるかという時間との勝負だ。それゆえ、このようなことをする攻撃者は、この仕掛けを動かす前にすべての準備を整えているだろう。たとえば、このようなメールが社内にばらまかれたという事実を対応部署が知った時点では、すべてが終わっている可能性も高い。

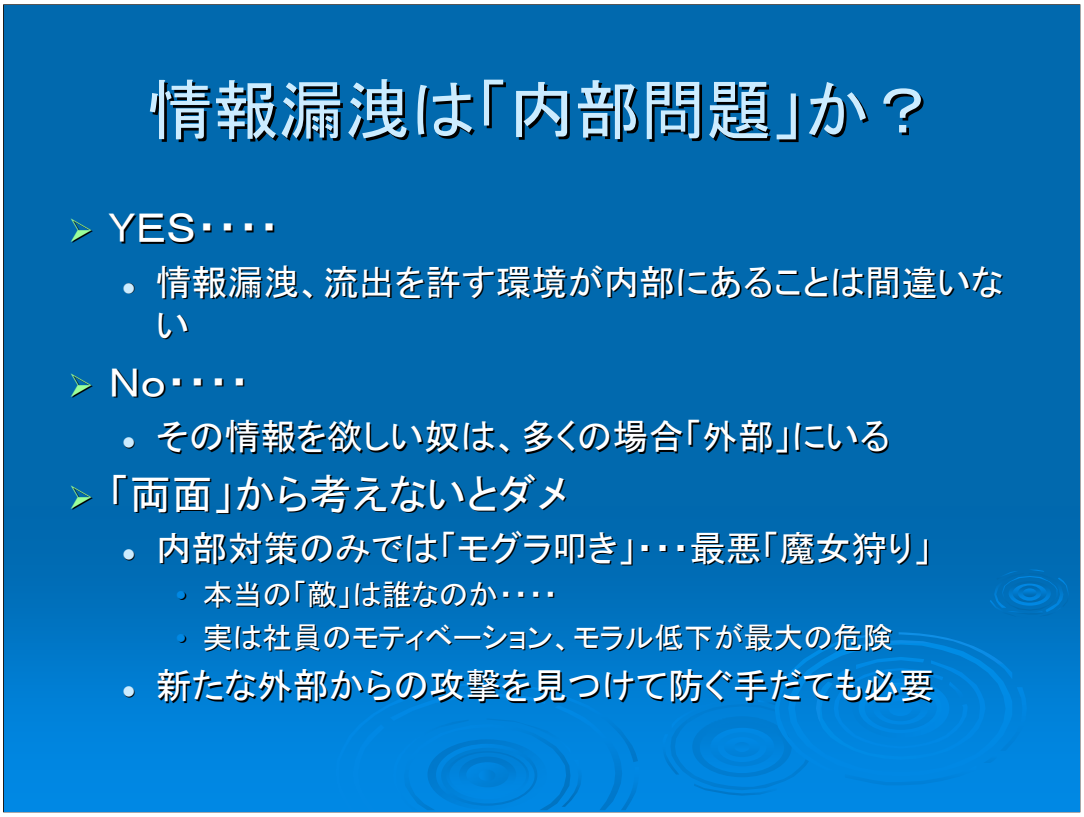


不正プログラム対策は、「予防」「検知」「駆除」の3つのフェーズすべてでの対応が必要。

予防対策の決め手はないが、ユーザに注意を促すことで、こうした攻撃を受けてしまうリスクをかなり減らすことができる。既知ウイルスに対しては、ウイルス対策ソフトは十分に有効だ。しかし、未知ウイルス、特に特定の目的を持ったウイルスに対しては無力であると考えたほうがよい。ただ、役に立つ使い方もある。ウイルス感染しやすいユーザは、既知のウイルスに対しても感染寸前でウイルス対策ソフトに救われるケースが多いと考えられるから、このような警告を多く出すユーザは「要注意」としてマークしたり、再教育する必要がある。これをやるためには、状況をつかむためウイルス対策ソフトを集中管理する仕組みが必要になる。

次に、万一（‥という以上の確率ではあるが）侵入を許した場合、それらをどのようにして見つけるかという点。通信の監視やチェックを地道にやるしかないのが実情だ。

Webアクセスでウイルスを拾ったり、詐欺的なサイトに引っかかる可能性があるため、Webサイトのアクセス先をチェックしておくことも必要だろう。単純にアクセス先だけならば、ファイアウォールのログを集計すれば収拾できるし、Webフィルタリングソフトなどを利用して、より厳密に調査したり、不要なサイトへのアクセスをコントロールすることも有効な対策だ。



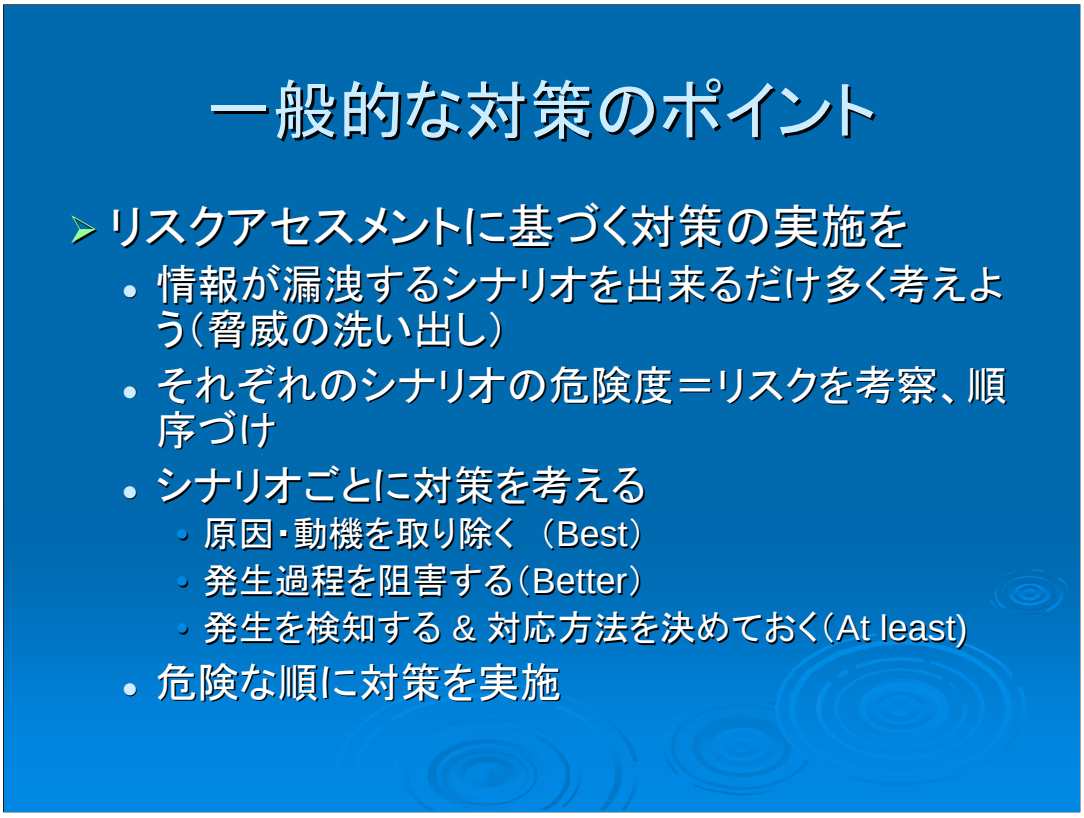
情報漏洩は、内部に問題があって発生するが、その情報をほしがる相手は外部にいる点にも注意が必要。内部対策は重要だが、やりすぎて社員のモティベーションを下げるようなことになれば、外部の犯罪者の「思うつぼ」になる危険がある。会社への反発心から外部の犯罪者に手を貸すケースも多いからだ。ルーズだからといって特定の人間を必要以上に「つるし上げる」ようなことは避けた方が賢明だろう。魔女狩りのようになってしまっては大変だ。

同時に、外部からの攻撃手法もより巧妙になっている。内部ばかりに気を取られていると、知らないうちに重要な情報を盗み取られてしまうことにもなりかねないので注意が必要。

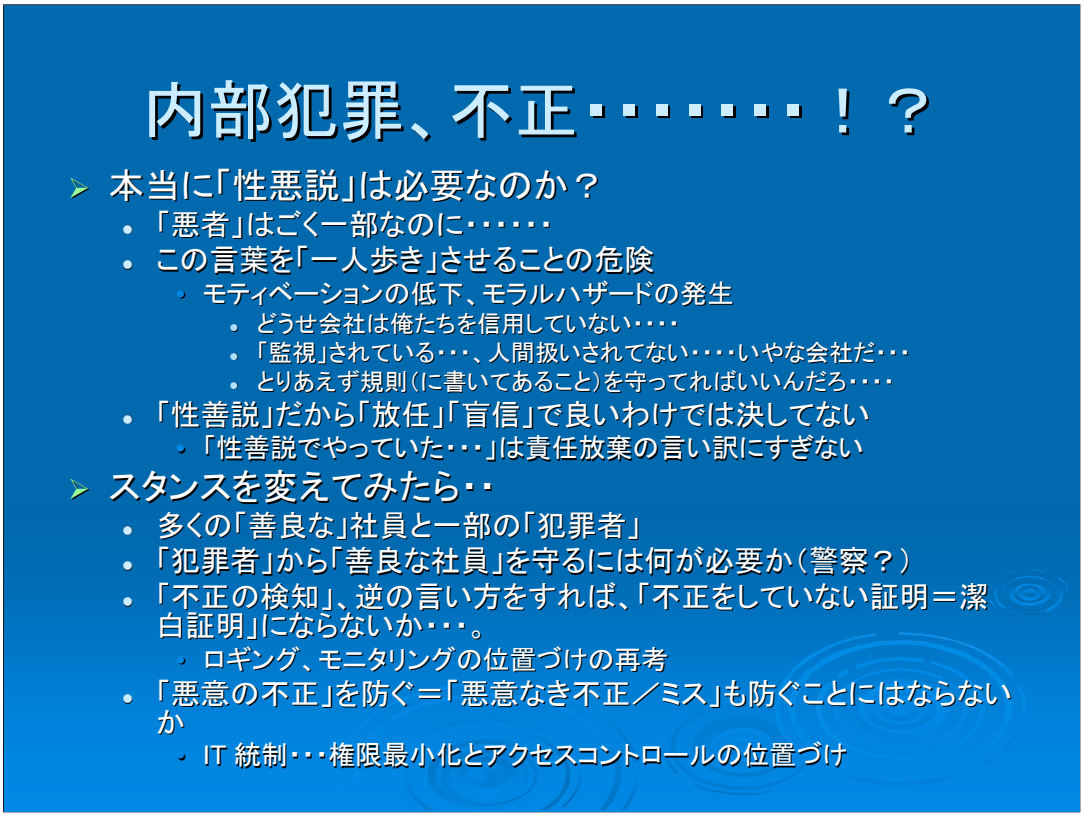
ある調査

- “CSI/FBI Computer Crime and Security Survey”
  - 2005年、2006年調査では、セキュリティ事件の「内部」「外部」比は拮抗している
- 「情報セキュリティ調査から見た日米比較」
  - 情報セキュリティ大学院大学　内田助教授
  - CSI/FBI surveyと同じ調査を国内で実施
  - 2005年までの調査では国内でも米国同様に「内部」「外部」の比率は拮抗している
- 内部犯行がことさらに強調されて報道されていないだろうか・・・・・という疑問

「内部犯罪」「外部犯罪」比率が議論されるとき、「内部犯罪がほとんど・・・」と言われるがこれは本当だろうか。これらの調査では、必ずしもそうではないことが見て取れる。内部対策、外部対策ともにバランスをとって行っていくことが重要なのだ。



一般論だが、（費用対効果的にも）有効な対策を講じていくには、リスクアセスメントという作業は欠かせない。ふんだんな予算があるわけではないから、当然、リスクの高い部分から対策をとらなければならないし、対策の結果、どの程度リスクが減ったかという点も、対策をきちんと評価するためには不可欠だ。



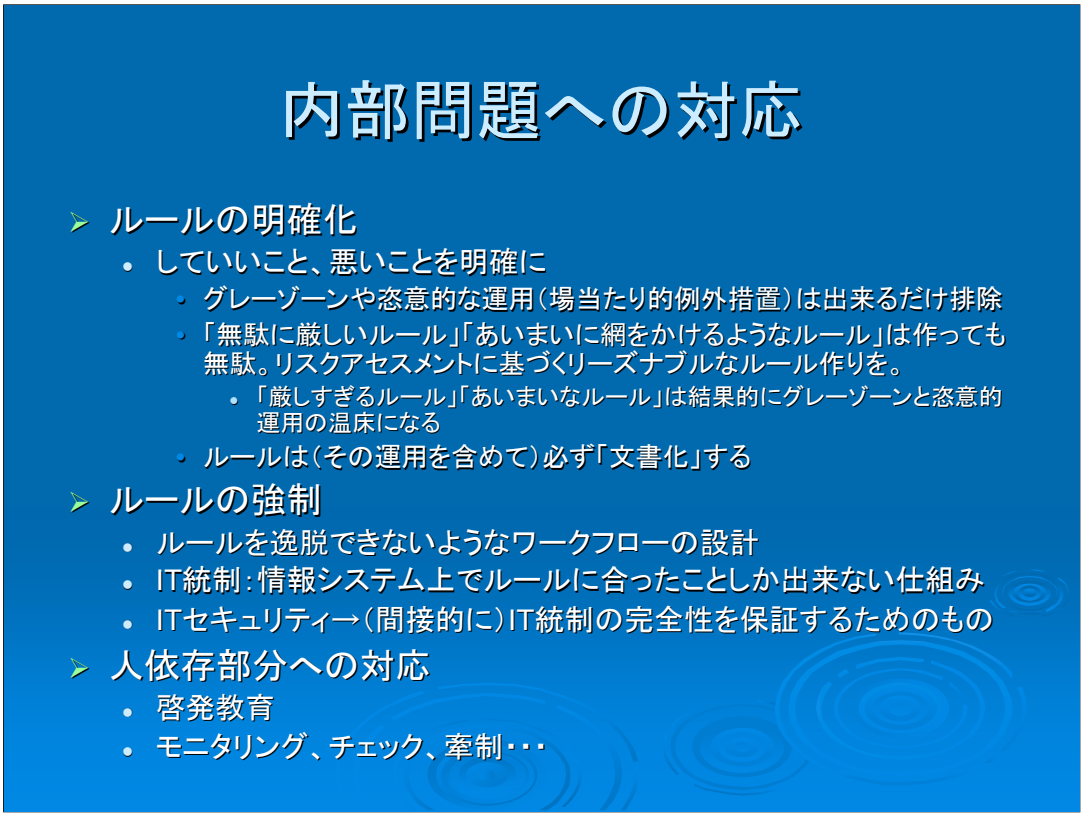
最近、セキュリティ対策は「性悪説」で、という言葉をよく耳にするが、これには危険な要素が含まれている。「性悪説」という言葉の本来の意味とは異なる使われ方だが、言葉が与える印象はより「悪い」。はたして、ことさらに「性悪説」なる言葉を叫ぶことが、セキュリティに強化に繋がるのだろうか・・・・。

これはそういう問題提起である。

「性悪説」とは、生まれついての善人はいないという考え方だ。この言葉を聞いた人の多くが、「みんな悪人だ」ということだと解釈する。たとえば刑務所ならばともかく、一般の会社でこの言葉を使うのは、よほど慎重にしたほうがいいと思う。会社を「刑務所」化してしまえば、何がおきるかは自明だろう。必要なのは、普段は善良な人が「悪の道へ走る」のをどう防ぐかということである。または、ごく一部の悪人と善人をどう区別し、善人を悪人からどう守るかという課題であるはずだ。よく、これまでは「性善説」でやっていた、これからは「性悪説」で・・というようなことを記者会見などで言っているのを見るが、これは自分が責任放棄をしてきたことの言い訳に過ぎない。「性善説」であっても、放任や盲信はしてはいけないからだ。

モニタリングや各種の規制は必要だが、それらは「社員を疑う」からではなく、「無用な疑いをかけられない、もしくは晴らす」ために使えるのだし、結果として一部の悪者から善良な社員を守ることにつながるのだという点を強調すべきだろう。

セキュリティ対策のかなりの部分が、どうしても「善良な社員」の努力に依存せざるをえない。それを考えると、安易にこうした言葉を使って、善良な社員まで敵に回してしまう愚は避けたいところだ。



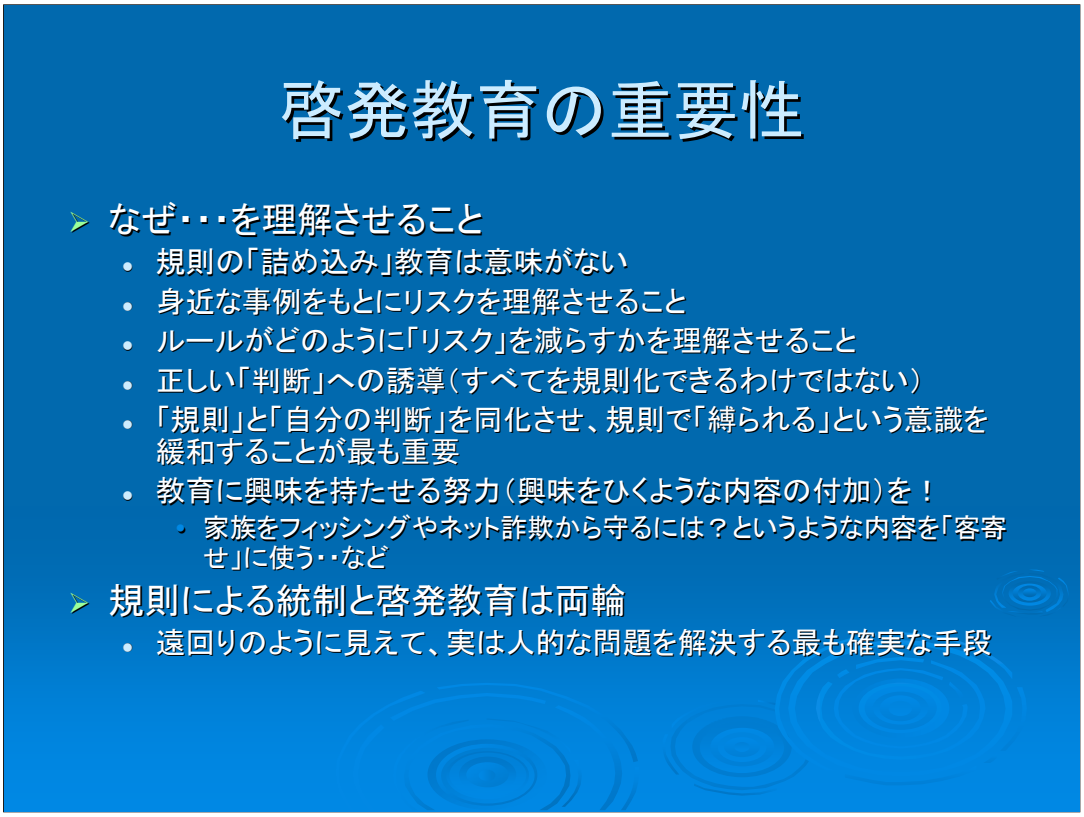
統制を確実に行うためには、論理的で明確なルールが必要だ。たとえば厳しすぎるルールは、「業務効率が落ちる」「業務ができない」という理由で、例外ができやすい。利益を上げることが使命の営利企業にとっては、仕事が進むことが最優先事項だからだ。また、そのような例外ができる過程では、恣意的な運用が行われやすい。声の大きな部署が例外扱いをいっぱい獲得する・・・といった状況では、規則の信頼性そのものが揺らぐ。また、基準があいまいなままで、おおまかに網をかけるようなルールも結果的には、厳しすぎるルールと同じような状態に陥りやすい。

ルールは、きちんとしたリスク分析に基づいて、本当に必要な内容を記述するようにしたい。また、ルールは、その運用方法なども含め、きちんと文書化して周知おく必要がある。

ルールを決めるだけでは、不十分な場合も多い。ルールを実効的なものするためには、仕事のワークフロー自体をルールに基づいて変える必要もあるだろう。その上で、その仕事がシステム化されるのであれば、システム上で確実にルール遵守を保証するような仕組みを作り込む。これがいわゆるIT（システム）統制の考え方だ。しかし、その前提となるのは、規則に沿った形で最適化されたワークフローの存在である。

内部統制は情報セキュリティとからめて語られることが多いが、セキュリティ対策は内部統制を直接には保証しない。あくまで、システム統制をかいくぐった処理が出来ないような仕組みを作ることで、間接的に統制の完全性を保証する点に注意が必要だ。もちろん、これは重要なことである。

どれだけIT化しても、人に依存する部分はのこる。人にルールを守らせることは、一般に難しい。これを確実にするために、啓発教育や、チェック、牽制といった考え方が必要になる。しかし、真に重要なのは、この啓発である。



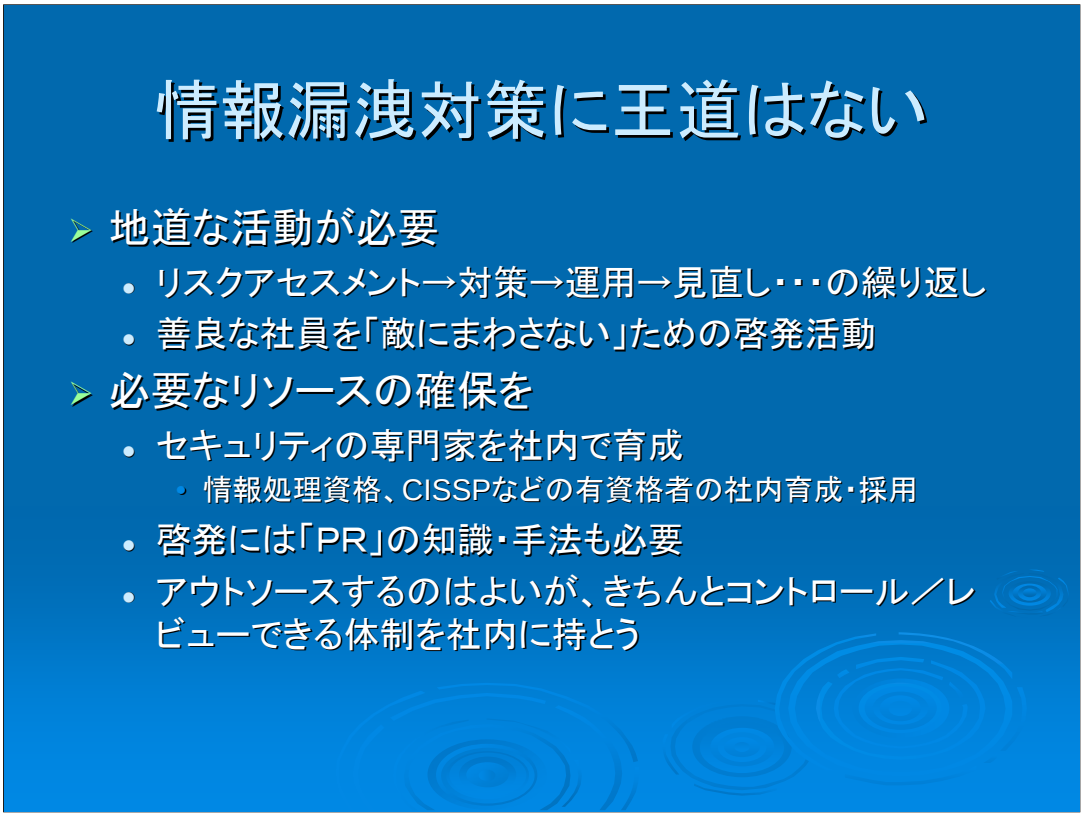
日本の会社の情報セキュリティなどについての社員教育は、特に個人情報保護法施行後、社内規則の詰め込み的に行われるケースが多くなったように思う。コンプライアンスという冠がつくことで、どうしても「規則を守れ！」というのが中心に座ってしまうからだろう。

規則詰め込みの弊害は言うまでもなく「思考停止」だ。「規則にあることだけを守っていればいい」といった、ある種のモラルハザードを引き起こす危険もある。

本当に必要な教育は、規則がなぜ必要かを実感させるものだ。規則で決められるまでもなく、自分の判断としてそれを実行できるようになれば、規則で縛られるといった窮屈感は、かなり緩和できるだろう。規則がどんどん増えていきそうな昨今、これは社員のモティベーションを維持する上でも重要だ。このような作業が難しいことは承知の上だが、結局は必要になることだ。

ある米国のコンファレンスで講演者が言ったことが印象的だ。

「この人たちにはどれだけ言ってもわからない、説明しても無駄だ・・・、こう思った瞬間、あなたはセキュリティ管理者として自殺している」



実際に、自社内でこうしたことをやりはじめてみると、地道にやるしかないな、というのが実感。少ないリソースで対策を進めていこうとすれば、「皆様のご協力」がないと絶対に無理。多くの善良な社員を敵に回すようなことをしては、仕事が成り立たない。どうしたら彼らに自発的に協力してもらえるかを常に考えておく必要があると思う。

セキュリティにかかわらず、日本企業のITはアウトソース中心のようだが、少なくともセキュリティだけは、絶対に「丸投げ」できない部分。先に挙げた日米比較調査でも、セキュリティに関するアウトソース率は日米で最も差が出たものの一つ。米国では、多くの会社でアウトソース率は10%未満。

先日のNetSecコンファレンス（米国フェニックスで開催）でも、アウトソースに関するセッションがあって、その中で、「自分たちの要求事項をアウトソース先にすべて満たしてもらおうとすれば、自社で体制を持つより割高になることもしばしば・・」という話が聞かれた。多くの企業でセキュリティ専門の組織が確立している米国ならではの議論かもしれないが、数年後は日本もそうなっている可能性が高いと思う。

各企業が自分たちでリスクアセスメントを行った結果として対策を考える場合、リスクを許容限度におさめる対策という視点でアウトソース先に要求をぶつければ、ある種オーダーメイドのサービスになってしまうため、どうしても割高になるのだろうと推測する。きちんとしたセキュリティのマネジメントが行われるようになれば、日本でも同様のことが起きてくるに違いない。

アウトソースは決して悪ではないが、その目的はコストダウン。しかし、セキュリティの形は自分たち自身が決めないと、最終的に責任が取れない。丸投げした結果、重大なインシデントが発生しても、アウトソース先は責任を負わない（負えない）からだ。自分たちがきちんとコントロールし、チェックできる形でアウトソースを考える必要がある。そのためには、少なくとも最小限必要な専門家は自社内で確保し、責任を持てる地位を与えた形で体制を作っておく必要があるだろう。

啓発教育については、「教育」独特のノウハウがあるため、アウトソースしたほうがよいケースもあるだろう。しかし、社員とセキュリティ組織との間の関係を考えれば、定期的に face to face のコミュニケーションの場を持つことは悪いことではない。これも完全に人任せにせず、適宜、自社の担当が首を突っ込んでいく必要があるだろう。

このような体制は一朝一夕ではできない。しかし、数年後、こうした形を他に先んじて作ることができた企業が社会的に大きな評価を得ることになるかもしれないということは、考えておくべきだろう。

参考資料

- 「パンドラの箱を開け」
  あなたは自社ネットワーク利用の現実を知っていますか？
  - Interop 2006 セキュリティパビリオンでの講演より
  - http://www.kazamidori.jp/SECURITY/pandra-interop06.pdf
- ・不正プログラム対策と侵入検知、防御技術
  - Internet Week 2005 チュートリアル　T13より
  - http://www.nic.ad.jp/ja/materials/iw/2005/proceedings/
- CSI/FBI Computer Crime and Security Survey 2005
  - CSI Website : http://www.gocsi.com/
- 第3回情報セキュリティ調査
  - 情報セキュリティ調査からみた日米情報セキュリティ比較
  - 情報セキュリティ大学院大学　助教授　内田勝也
  - http://www.uchidak.com/chuo/2006_Japan_CSI.pdf

ご清聴ありがとうございました

二木真明　（ふたぎ　まさあき）

住商情報システム株式会社
情報システム部　部長付　（情報セキュリティ担当）
ネットワーク・セキュリティソリューション事業部　担当部長

NPO 日本ネットワークセキュリティ協会幹事　技術部会長

CISSP (Certified Information Systems Security Professional)
情報セキュリティアドミニストレータ
futagi.masaaki@scs.co.jp