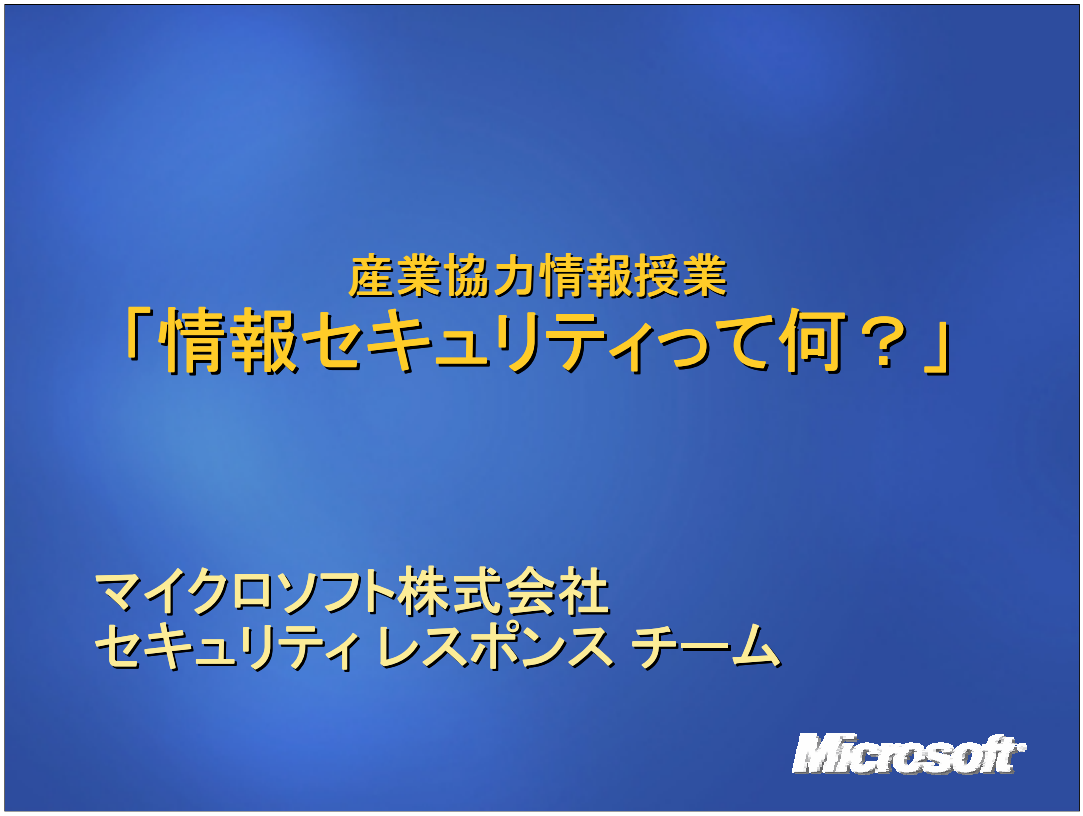
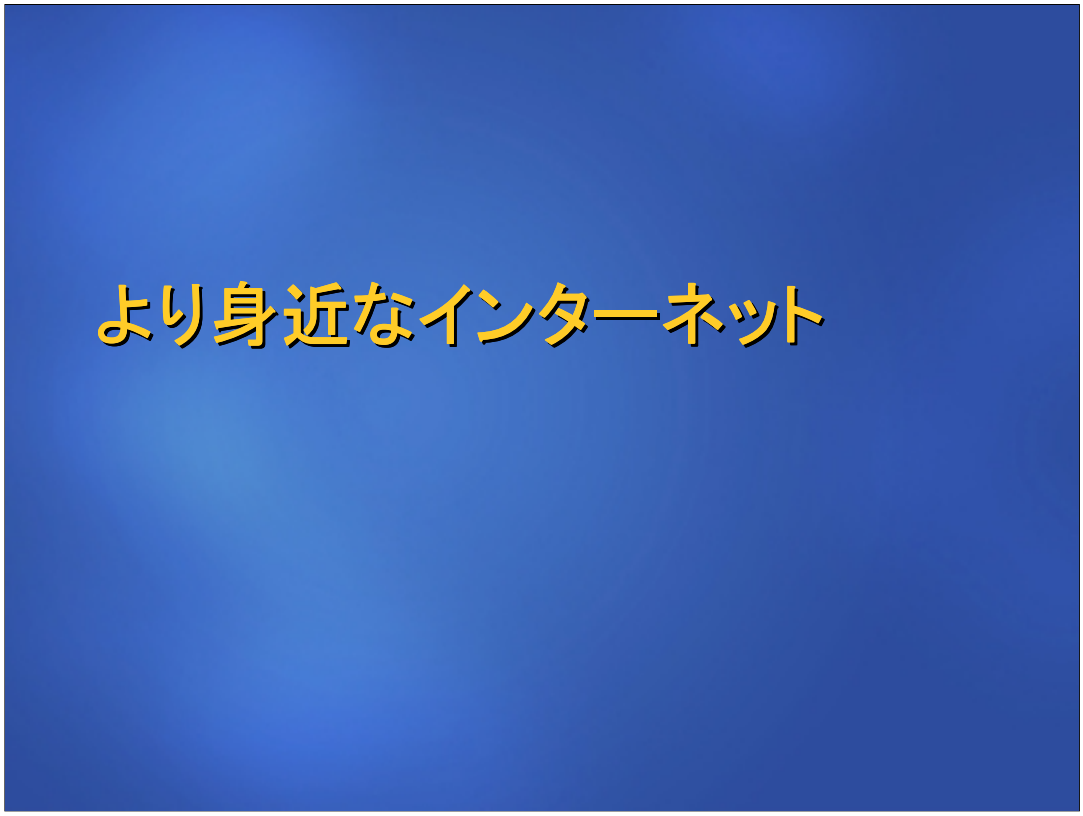

産業協力情報授業
「情報セキュリティって何？」
マイクロソフト株式会社
セキュリティ レスポンス チーム
Microsoft

講師用

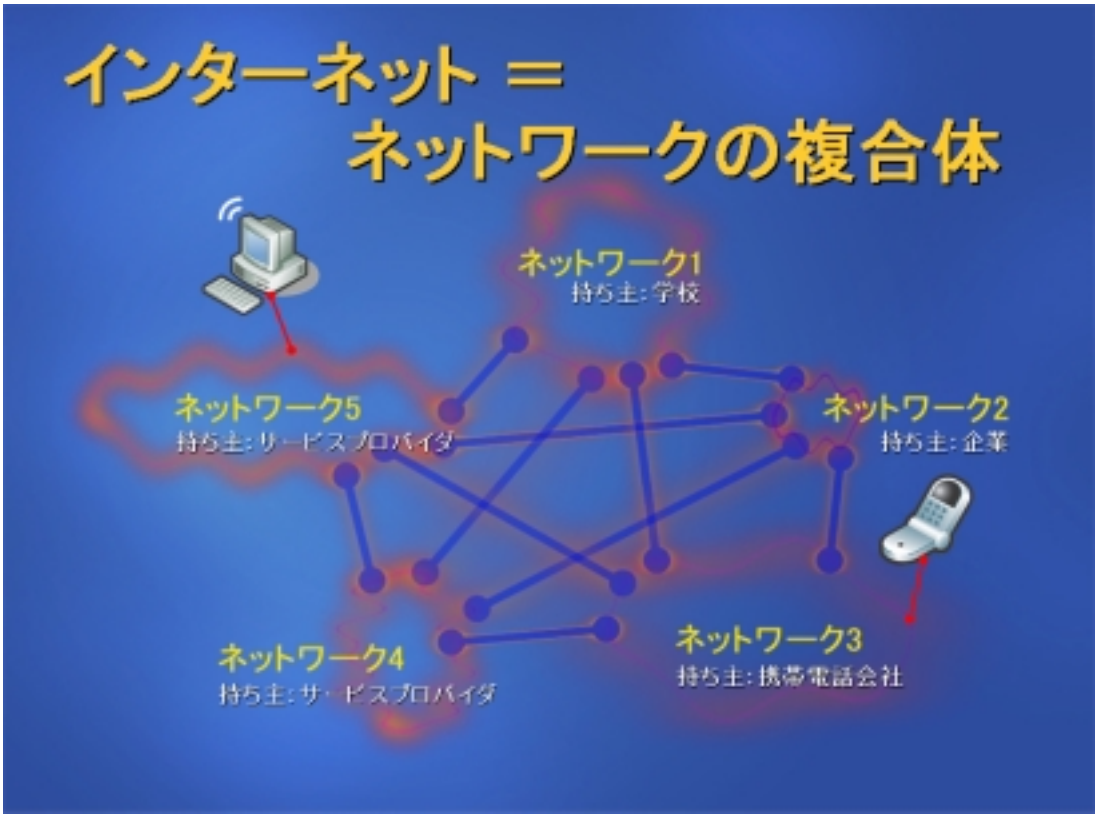
＜1時限目＞



“インターネット” については、いろいろなところで耳にされていることでしょう。

ほとんどの方が、パソコンや携帯電話などで利用した経験があるでしょうし、既に世界中に広がったインターネットは、直接利用をしていなくても、どこかで恩恵を受けているもので、生活に無くてはならない基盤として活用されています。

ここでは、情報セキュリティを考える上で、必ず理解しなければならないインターネットの基礎的な考え方と、数々の機器がつながった仮想的な世界についての理解してください。



インターネットと聞くと、パソコンなどを壁のソケットと接続すると、電話線を伝って接続されるネットワーク、という漠然としたイメージを持っている方が多いと思います。

しかし、実際のインターネットは非常に高度で複雑な仕組みで動いているのです。

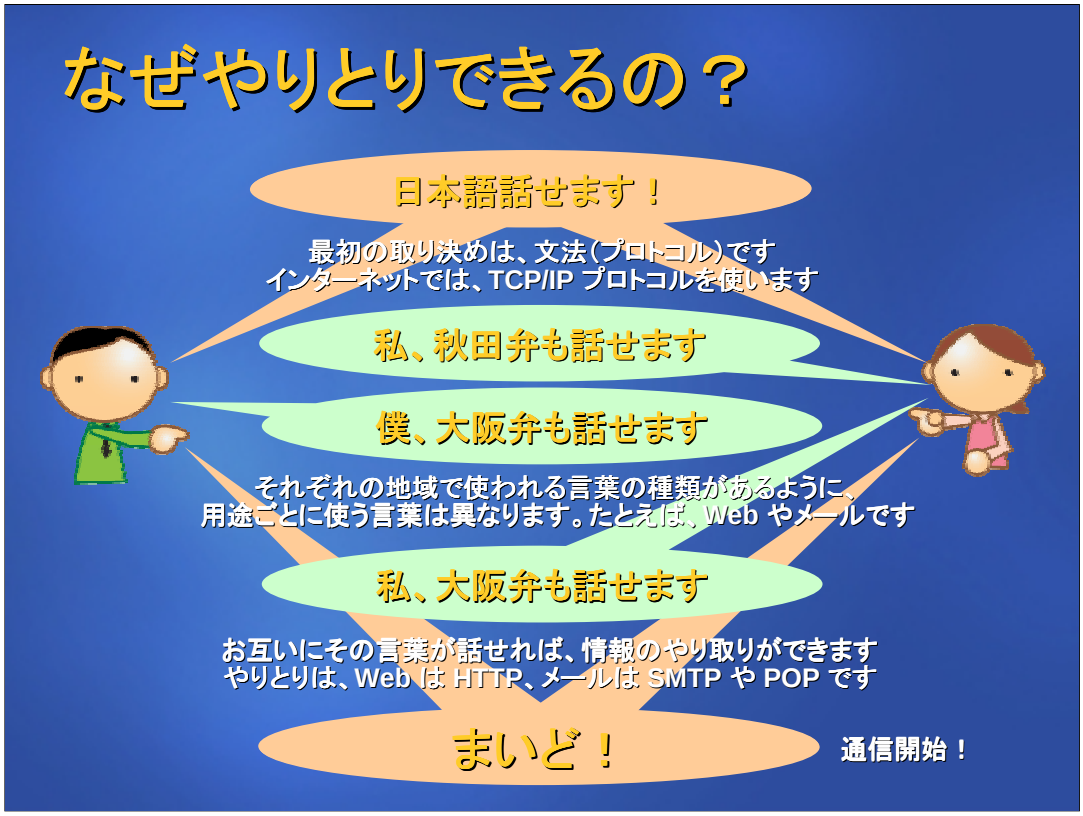
インターネットとは、何か決められたネットワークがただ存在するのではなく、どこかの会社が運営しているものでもありません。アメリカ国防省高等研究計画局 (ARPA) が最初にネットワークを組み立て、アメリカの広大な国土の中で、情報の受け渡しを円滑に行うために活用が始まったものです。

当初インターネットは、ARPA-NET と呼ばれていましたが、全米科学財団 (NSF) がこのネットワークを使用し始め、主に研究用途での使用が広がりました。そのころネットワークとは、小さな区域でのネットワークである、ローカルエリアネットワーク (LAN) と LAN を接続するワイドエリアネットワーク (WAN) が主流でしたが、より効果的な情報のやり取りを行うため、ARPA-NET へ、これらのネットワークを接続することが加速してゆきます。

結果的に、いくつものネットワークが相互に接続されることとなり、巨大なネットワークが出来上がった、これがインターネットの前身となります。

つまり、インターネットは、様々に管理されたネットワークがそれぞれ相互に接続された、ネットワークの複合体といえるのです。

インターネットは、ネットワークの（ 複合体 ）です。



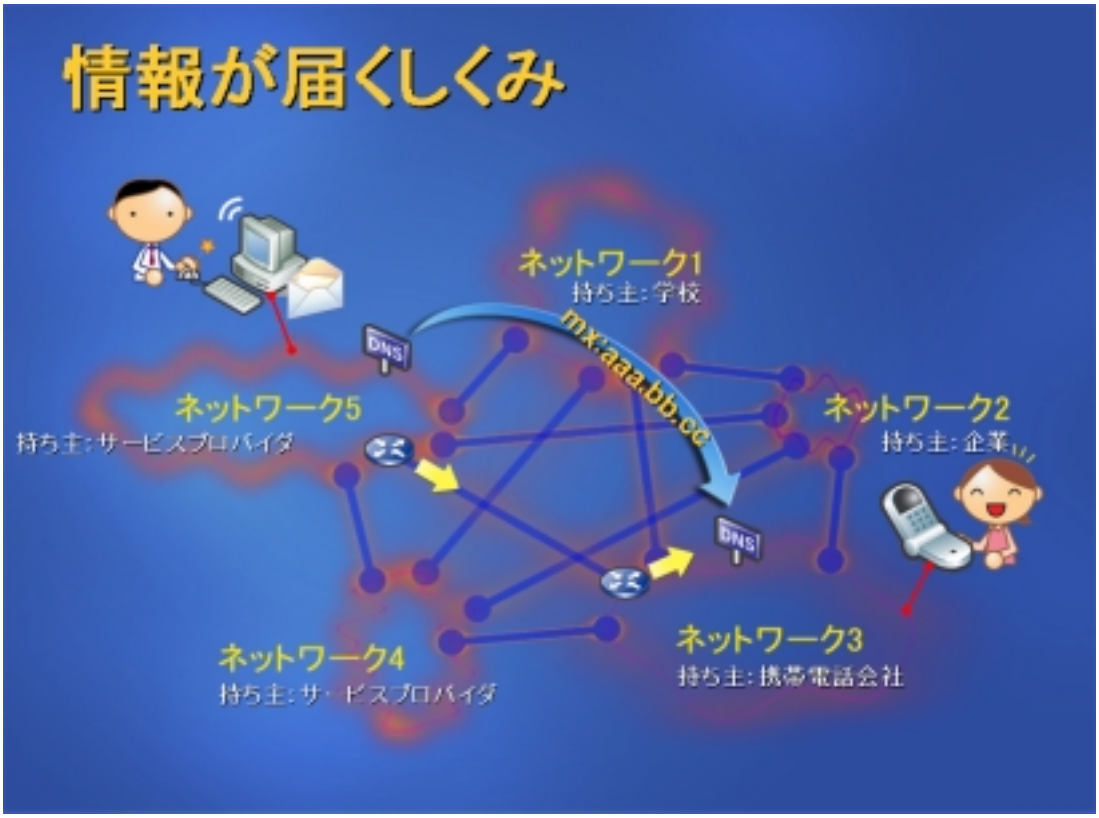
ところで皆さんは、なぜ壁のソケットにパソコンを指して、ネットワークを利用できると思いますか？

実は、ネットワークで情報のやり取りをするには色々な決まり事があり、全員がその取り決めに従って通信をすることにより、接続性を確保しています。これらの取り決めは、Request for Comment (RFC) と呼ばれる資料にまとめられています。インターネットは、色々な国や色々な機器がつながる多様性に富んだ世界です。そのため、基本的には“他者にやさしく、自分に厳しく”がマナーとされています。つまり、他者から自分宛に送られた情報のなかで、理解することができるものはできる限り受け入れ、逆に他者が理解できる内容を自分からは送るようにすべき、と言うものです。

このやり取りは、視点を変えると、私達の語学に通じるものがあります。コミュニケーションは、双方が理解しなければ成り立たないと言うことです。私達が会話をするときに、いくつもの取り決めがあります。まずは、日本の文法を知ること。これがもっとも重要なことですね。日本語の主語、述語、目的語の並び順などは、皆さん生まれたときから学んでいる取り決めです。インターネットでは、TCP/IP という取り決め（プロトコル）があります。この取り決めは、最低限これを理解できないとコミュニケーションが成り立たないものです。

しかし、日本語の文法を理解していても、単語を理解し、話す話題や会話のルールなどを知らなければ、会話は進みません。日本は狭いと言われていますが、国内の方言は大変多くのものが存在しています。同じように、日本語が話せた上で、それぞれの地域の方言となるプロトコルが存在します。それが Web やメールなどに代表されるアプリケーションプロトコルです。このように、プロトコルが理解できるプログラムを使用すれば、インターネットを介していろいろなサービスを受けられるようになります。

インターネットで情報をやり取りする取り決めを
(プロトコル）と呼びます。



インターネットでやり取りされる情報の取り決めについて理解できましたが、まだ良く分からない点があるでしょう。

なぜ、複数のネットワークがつながっているのに、メールや Web へアクセスできるのか？ということです。

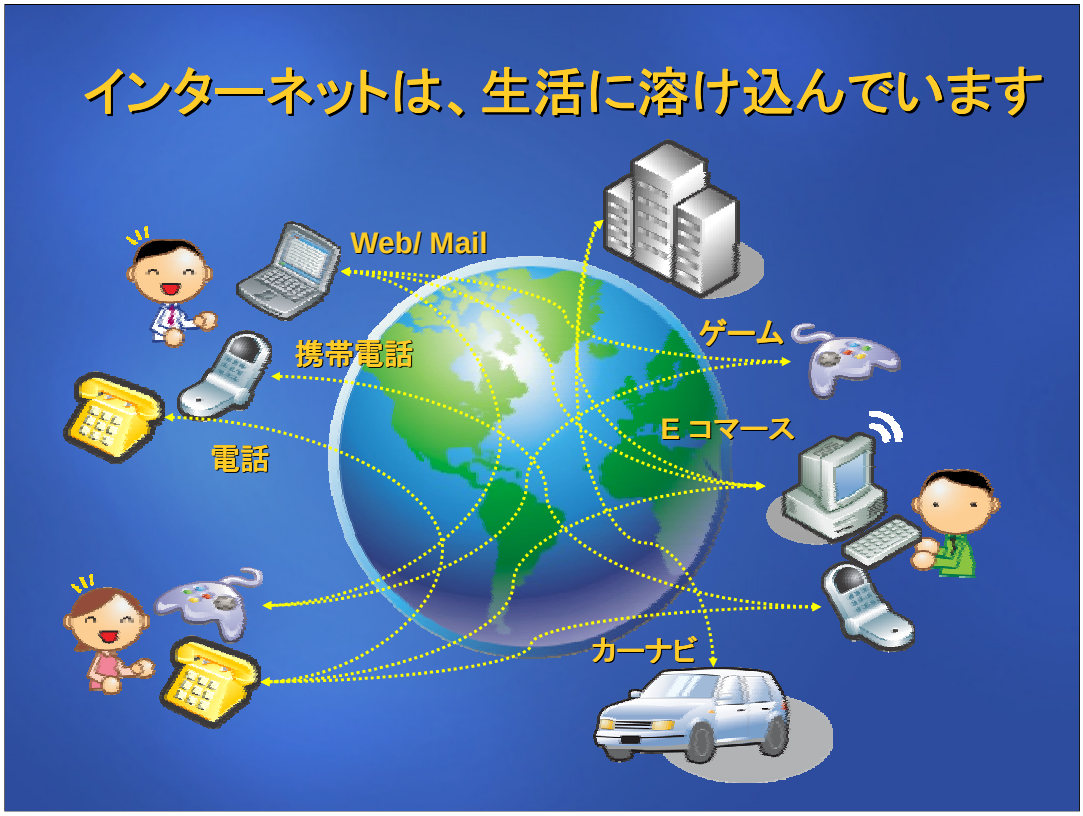
機器をインターネットに接続するときに、そのネットワークの持ち主はインターネット上の住所とも言える、IP アドレスと言うものを手に入れています。これは、東京都のなになに市、といったいくつもの住所が集まった地域の情報に近いものです。この住所を、ネットワークに接続する機器に対して貸し与えるのです。

IP アドレスというのは、0 から 256 までの数字を、4つ並べて決定されます。たとえば、192.168.0.1 のような形式です。しかし、これでは人間には分かりにくいので、分かりやすい別名をつけることが出来ます。これがドメイン名とホスト名なのです。先ほどの東京都なになに市に相当するのは、aaa.bb.cc といったドメイン名で、メールであれば、アットマーク (@) の前にメールアドレスが入ります。

コンピュータは、ドメイン名から IP アドレスを割り出すことができ、これはドメイン ネーム システム (DNS) と呼ばれているソフトを使用して行います。相手先のドメインが分かれば、そこに接続することは簡単です。

上の絵では、メールを送ったときに、そのメールの内容が携帯電話の女性に届く流れを示しています。左の男性がメールを送ると、そこから DNS を使用して、接続先のメールのサーバーを特定できます。メールサーバーが特定できたら、そこにメールの情報を送るわけですが、このとき、ネットワークとネットワークを接続するルーターという機械が、何処にそのメールの情報を転送すればよいのかを判断して、交通整理をしてくれるのです。こういったネットワークを介して、メールは届けられるのです。

TCP/IP と呼ばれるルールを利用することによって、
(ネットワーク) 上の通信は行われています。



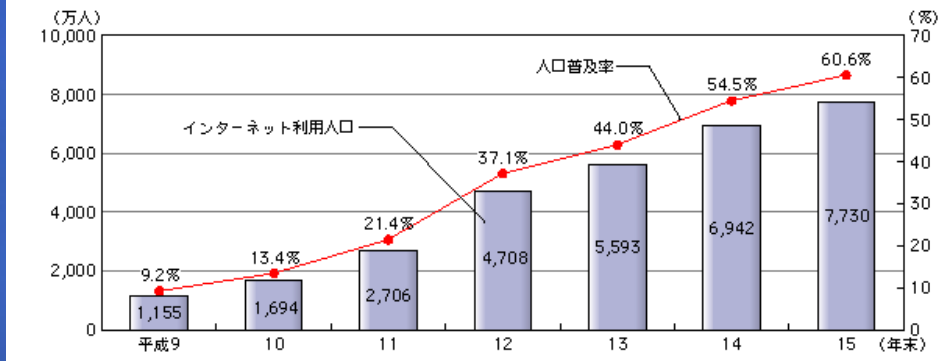
インターネットの仕組みが分かると、条件さえ満たせば誰でも参加できるネットワークだと言うことが分かることと思います。

たとえば、Web やメールのやり取りも、携帯電話やゲーム機とやり取りできますし、電話も今ではインターネットを介して接続されることがあります。さらに、ネットワークゲームが流行ったり、電子商取引やカーナビの地図の入手など、いたるところで使用されているのです。

ネットワーク同士を接続することが、ここまで可能性を広げることを誰が想像したでしょうか？

インターネットを利用すると、ホーム (ページ) を見るだけではなく、メールを送信したり遠隔地の友達とゲームをすることなど便利なサービスが利用できます。

どのくらい普及していると思いますか？



※1　上記のインターネット利用人口は、パソコン、携帯電話・PHS・携帯情報端末、ゲーム機・TV機器等のうち、1つ以上の機器から利用している6歳以上の者が対象
※2　平成15年末の我が国の人口普及率（60.6%）は、本調査で推計したインターネット利用人口7,730万人を、平成15年末の全人口推計値1億2,752万人（国立社会保障・人口問題研究所「我が国の将来人口推計（中位推計）」）で除したもの（全人口に対するインターネット利用人口の比率）
※3　平成9～12年末までの数値は「情報通信白書（平成12年までは通信白書）」より抜粋。平成13年末、14年末の数値は、通信利用動向調査の推計値
※4　推計においては、高齢者及び小中学生の利用増を踏まえ、対象年齢を年々拡げており、平成12年末以前の推計結果については厳密に比較できない（平成11年末までは15～69歳、平成12年末は15～79歳、平成13年末から6歳以上）

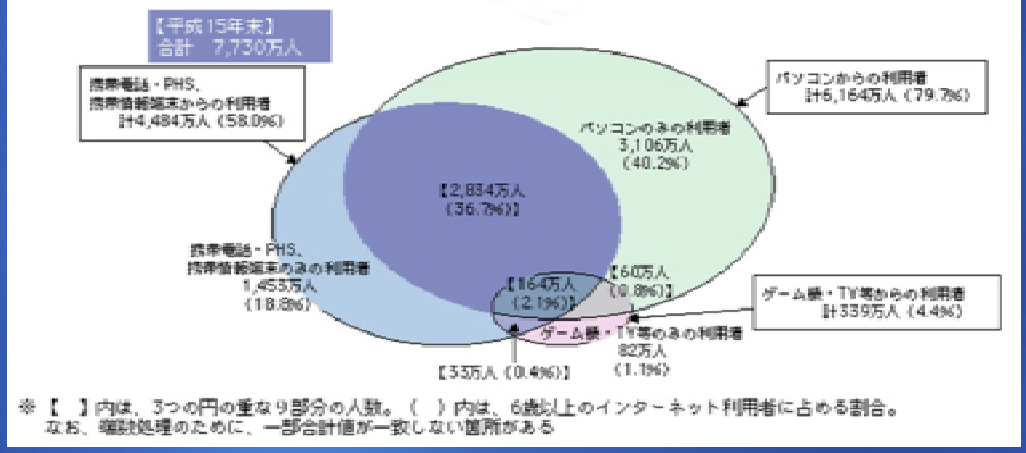
総務省　平成16年版　情報通信白書
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

ちなみに、インターネットの使用者は、まさに右肩上がりの発展を続けています。

携帯電話などの機器の増加や、テレビなどの家庭電化製品もインターネットに接続されています。

家庭電化製品の中でも、冷蔵庫やポットなども今後インターネットを介して、通信を行うことになるかもしれません。

その内訳は？



総務省　平成16年版　情報通信白書
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

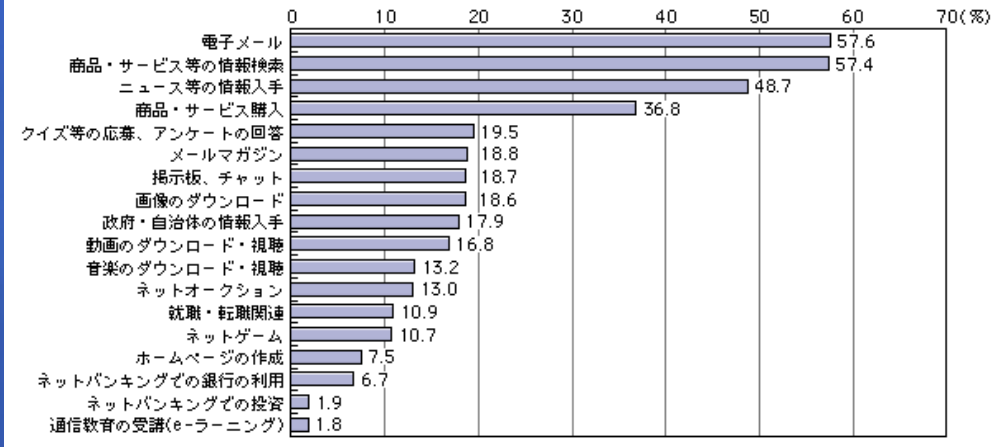
接続される機器の割合と分類です。

多くの方が複数の機器を使ってインターネットの便利さを体験しています。なんと7730万人の人が既に活用をしているのですから、国民の半数は直接的にインターネットに参加しているわけです。その内の80%近くがパソコンからの接続を行っていて、ついで58%が携帯からの接続を行っています。

今後は、ゲーム機がインターネットに接続することが当たり前となり、携帯やパソコンはもはやネットに繋がることが前提の世の中になってきました。

機器の中で2番目にインターネット利用者が多いのは（携帯電話）です。

利用の動機は？



（出典）総務省「平成15年通信利用動向調査」

総務省　平成16年版　情報通信白書
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

この情報は、使用者がインターネットを利用する動機をまとめたものです。

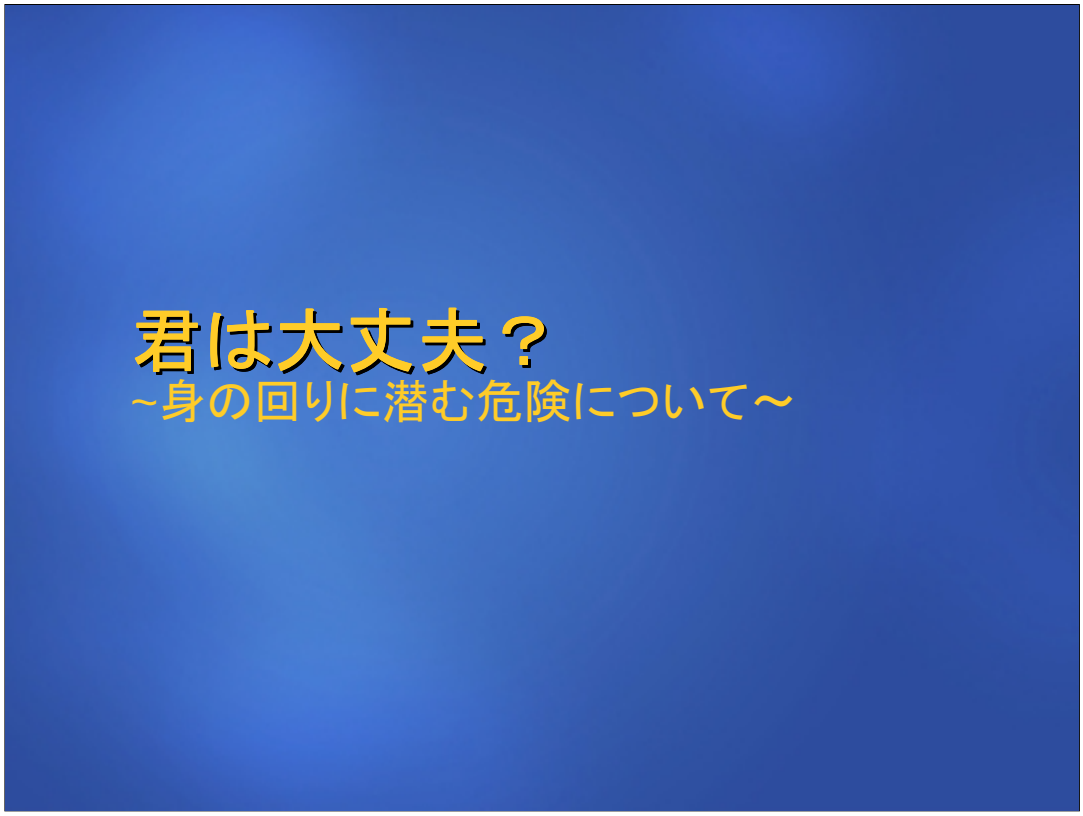
電子メールや、情報の検索に使っているわけで、コミュニケーションや、情報の入手を行うツールとして目覚ましい発展を続けています。注目すべきは、その使用用途が非常に多方面に渡って満遍なく分布していることです。パソコンの用途は多目的です。いくつもの情報をパソコンで手に入れ、さらに不足分を別のツールから入手していることが分かると思います。

インターネットの普及により、皆さんの生活が変化してきていることを感じている方も、この授業で知った方もいると思います。インターネットは、今後もよりいっそうの広がりを見せ、受けられるサービスも充実し、これまで以上に無くてはならないものになってくることは間違いありません。

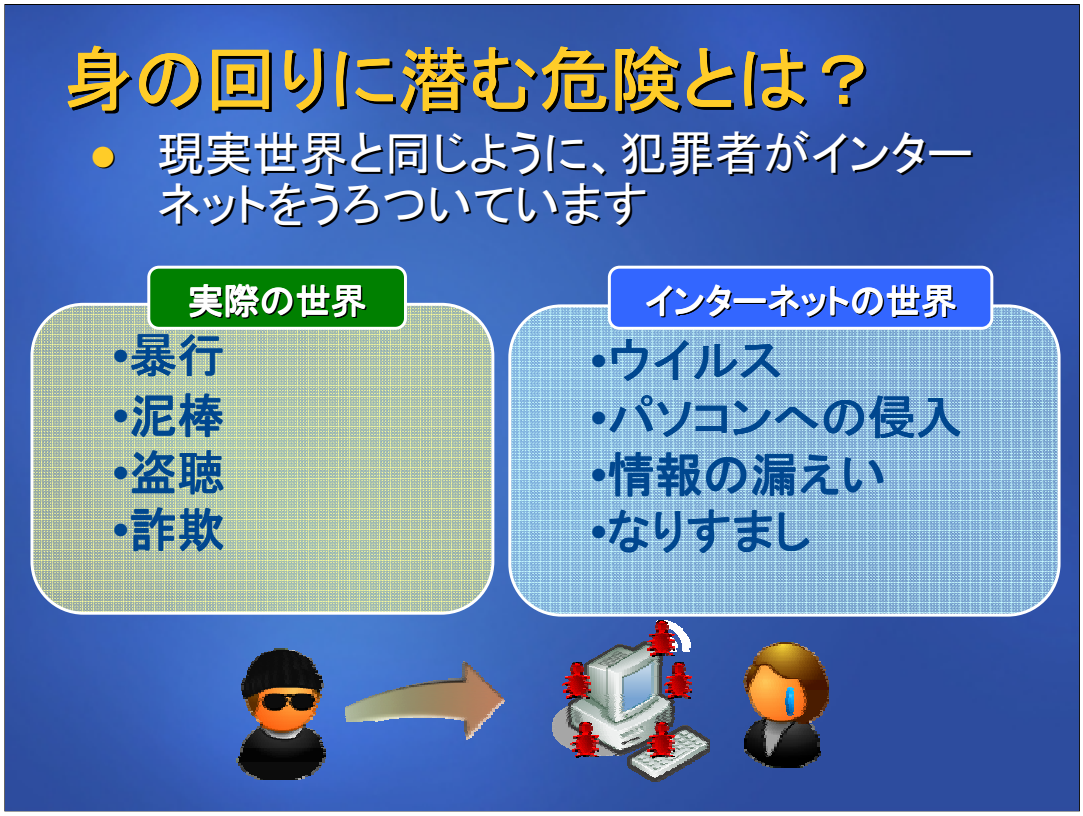
しかし、多くの人が参加し一般化することは、別の側面からみると現実世界の道路のように、参加者を拒みにくくなっているという事を意味します。たとえば参加者が悪意をもった方であっても、悪意がある事実を把握することは不可能です。夜の歓楽街のように人が集まるところには、それを狙った悪い考えを持つ人が引き寄せられるのは、世の常と理解してください。

現実の世界とインターネット上の仮想的な世界は、似通った点と異なる点があります。人と人がコミュニケーションをとったり、ショッピングをしたり、ゲームで楽しんだり映画見るなどが可能になると共に、犯罪というものも徐々に一般化してきています。これとは別に決定的に異なる点は、インターネットの先の使用者の特徴がほとんど情報に盛り込まれないことです。たとえばメールは、文字によるコミュニケーションですし、実際に住んでいる住所なども公開されません。しかも本名も公開しないことが多いため別の人になりすますなど、インターネットの匿名性に隠れた犯罪が発生することがあるのです。

インターネットの匿名性に隠れ、他人に（ なりすまし ）た犯罪が発生



ここからは、インターネットを利用する上で、気をつけなければならない危険について理解しましょう。転ぶと痛いことを知らなければ、転ばない努力はしないものです。危険について正しく理解をすれば、その対処方法もしっかり理解できるはずです。



実際の世界とインターネットの世界を比較して、どのような危険が潜んでいるのか、考えてみましょう。

インターネットの世界にも、実際の世界と同じように犯罪者が存在し、みなさんを騙して利益を得ようとうろついています。

実際の世界では、泥棒や詐欺、盗聴などの犯罪があります。最近ではオレオレ詐欺というのが、テレビでも取り上げられ、多くの被害が出ています。

インターネットの世界ではどうでしょうか。実は現実の世界に近い種類の犯罪が身の回りに潜んでいるのです。

暴行事件は、コンピュータや大切な情報を消したり使えなくなってしまう、財産への被害に近いでしょう。

泥棒も同じく、ID やパスワード、大切な情報や、ソフトウェアの製品キーの情報などが盗まれてしまう犯罪を指します。

盗聴は、現実世界でも発生している犯罪ですが、ネットワークにおいても非常に高度な技術を駆使すれば、インターネット上で流れている情報を取り出し盗聴が行われる可能性があります。

最後に、詐欺のほとんどはオレオレ詐欺のように。使用者の心に訴えかける犯罪となります。また、ID やパスワードを盗まれてしまった場合にも、詐欺

インターネットに流れる情報を盗む犯罪を（盗聴）という。

（パスワード）とは、ID と共に使用され、本人だけが知っている情報を指します。

オレオレ詐欺をご存知でしょうか？突然電話を掛けてきて、“オレだよ！大変なことに巻き込まれたので至急お金を振り込んでくれ！”といった緊急事態を感じさせる電話をしてくるわけです。電話を受けた人は、誰からの電話かを想像してついついに自分の子供の名前などを相手に伝えてしまいます。自分が確認したことが。自分自身に暗示を掛けてしまい、その後はその相手を当の本人だというように信用してしまうものです。

そんな訳がないと考えるでしょうが、実際に同様の手口で沢山の被害者を出してしまっているのです。

コンピュータの世界では、そのまんま本人が送信したようにしてメールなどを送信することができます。また、使ってもいない有料のインターネット サイトになりすまし、架空請求でお金をだまし取るようなメールが送られてくる可能性があります。

使っても居ない料金を請求する詐欺を（架空請求）詐欺という。

現実の世界で、自分の名前を告げずに相手を信用させる詐欺を（オレオレ）詐欺という。

現実の世界では、泥棒が家から何かを盗もうとしたときに、最終的に家に侵入して金目のものを持ち去ると思います。ただ、侵入をするにも、警官や近所の人の目をかいくぐったり、塀を乗り越えたり、番犬が居ないかを確認したりしなければなりません。また、家に鍵がかかっていたら、素早く開錠するためにピッキングという行為を行うことになります。

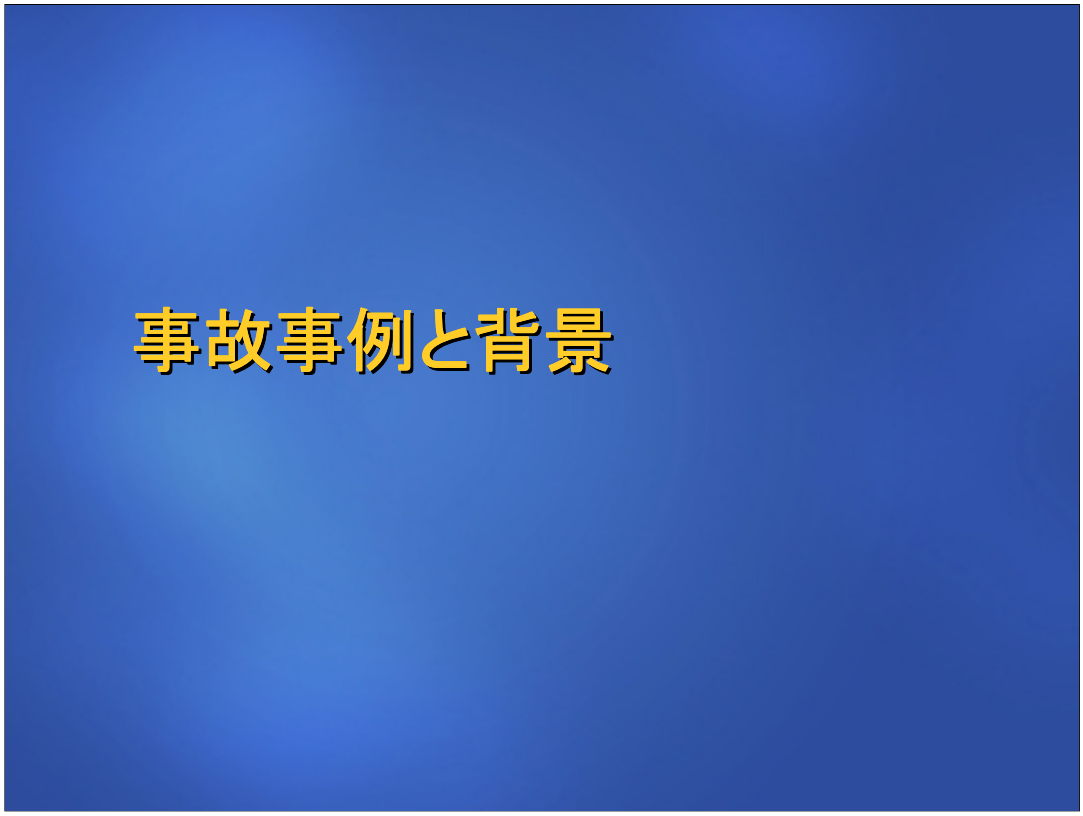
このような幾重にも乗り越える障害が、現実の世界には存在するわけですが、インターネット上には使用者が知らなければ対策できない事柄がとても多いのです。

ウイルスがメールで送られてくるのは、郵便や宅配便の配送係が家にやってきたのと同じです。普段皆さんは、彼らを家に招き入れる前に、信頼できる人かを確認するでしょう。ウイルスのメールの場合には、突然メールソフトに送られてきてしまいます。そのまま内容を信用すると、それは配送係を無条件に信用することと同じなのです。

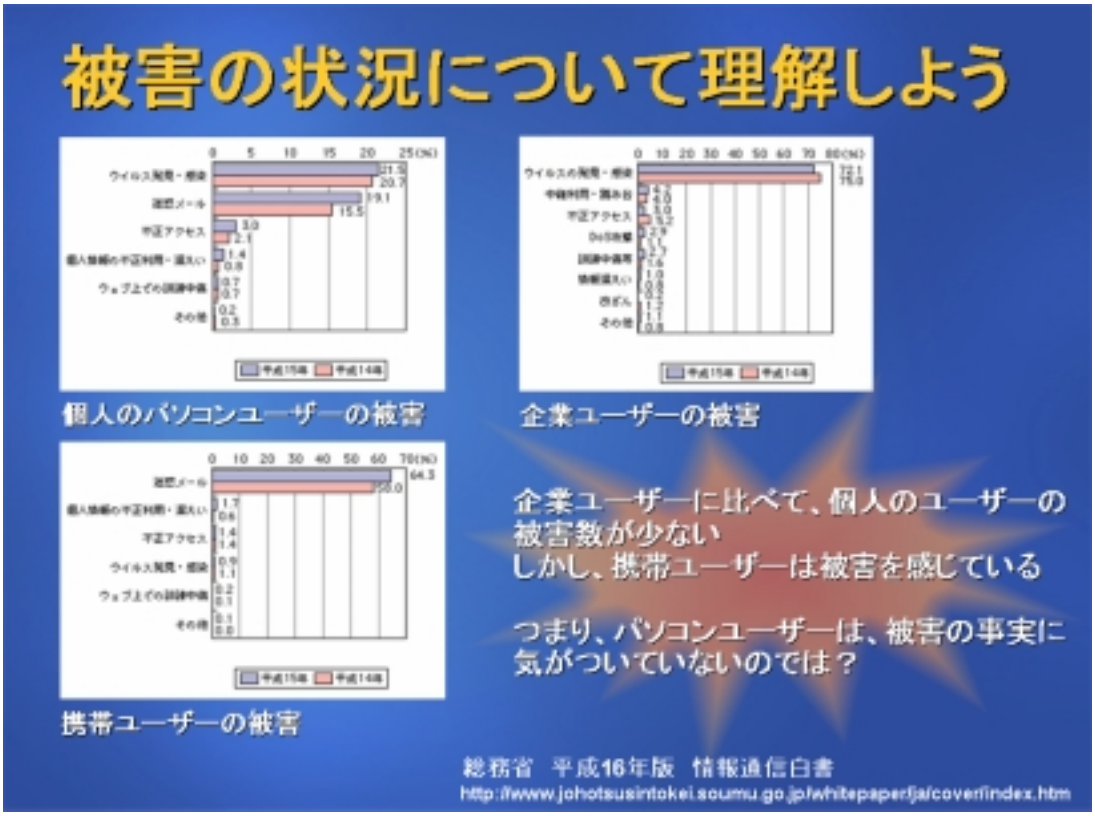
ハッキングとは、現実の泥棒と同じように、誰にも見つからずに家に侵入する行為です。家に入ってしまった泥棒は、住人に見つかる前に目的のものを探すことでしょう。ハッキングを行う犯罪者も、同じように発見されないように行為を行います。

とはいえ、現実と大きく異なるのは、盗まれるものが物理的なものではないために、現金や宝石が無くなるわけではありません。写真や重要な情報がコピーされて持ち出されたり、口座情報なども盗まれると危険な情報です。さらに、ほとんどの場合このようなコンピュータの犯罪は、情報が無くなるわけではないので、使用者は気がつかないのです。

犯罪者が、コンピュータに侵入することを（ハッキング）という。



コンピューターセキュリティの世界では、犯罪による被害が出ることを、“事故”と呼びます。ここでは、実際に発生している被害を理解して、より具体的なイメージを掴んでください。



それでは、どのくらいの情報機器の使用者が、このような犯罪行為について認知しているのかを見てみましょう。

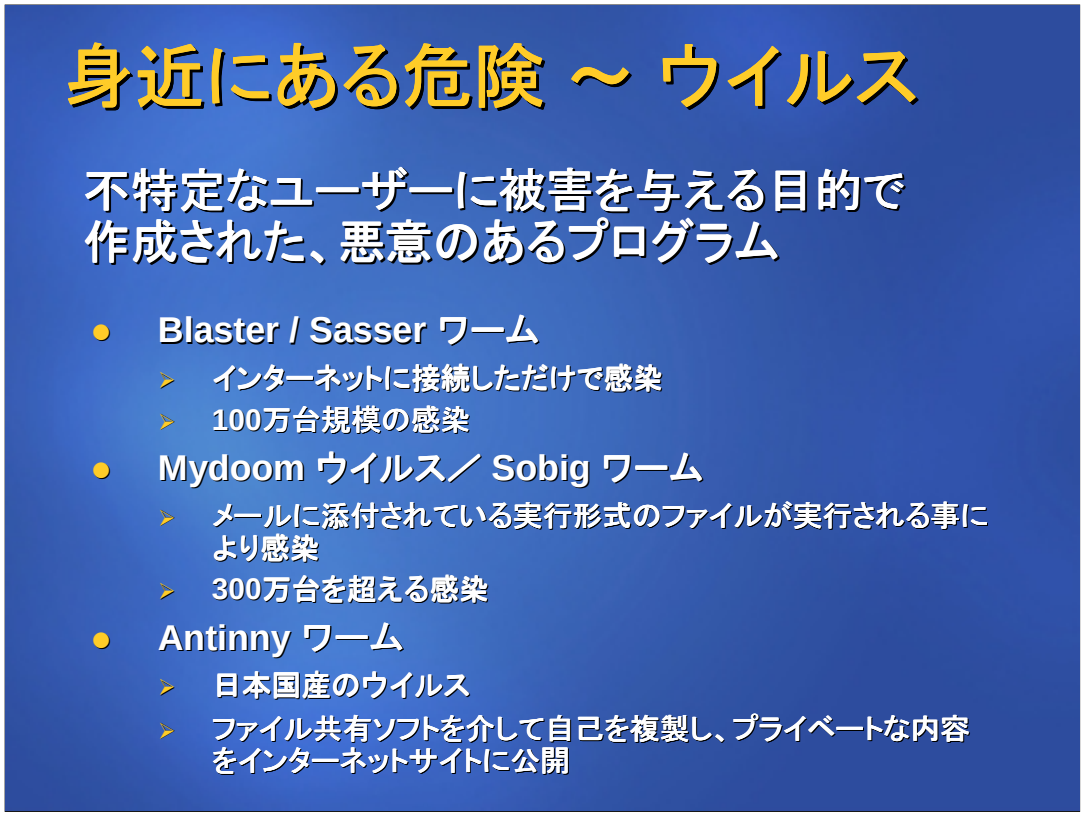
まず、左上のグラフにあるように、個人のパソコン使用者のうち、20%程度が、迷惑メールやウイルスの被害に遭っていることが分かります。また、企業のパソコンユーザーの被害に関しては、個人よりも圧倒的に多くの被害を認識しているようです。

この二つを見て気になることは、企業のようにしっかりと対策をしている方こそ被害顕著に現れているということです。

また。同じく個人も含まれている携帯電話のユーザーの被害として、迷惑メールの被害などがとても高い認知度となっています。これは迷惑メールの送信により、通信費という実害につながっていることも原因と考えられます。

つまり個人のパソコンユーザーも、被害の認知することは可能ですが、実際には被害にあっていても気がついていない可能性があります。

なお、ここに現れない被害者として、アダルトサイトなど他人に知られたくないサイトで被害にあっている方なども、相当数いると言われています。



実際に発生している被害で、一番大きな割合を占めるのは、コンピュータウイルスによる感染です。コンピュータウイルスは、その名の通り、自分自身を他のコンピュータに複製します。これを感染活動と呼んでいます。

ウイルスとは、一般的にコンピュータ上のファイルなどに自分自身をコピーして、コンピュータそのものに被害を与える目的で作成されるプログラムです。

ワームとは、ウイルスの一種なのですが、異なるのは自発的に他のコンピュータへの感染活動を行う点です。メールを介したものやネットワーク上のコンピュータに無差別に感染活動を行います。感染したコンピュータを増やすことが目的になっていて、基本的には破壊活動は控えめです。

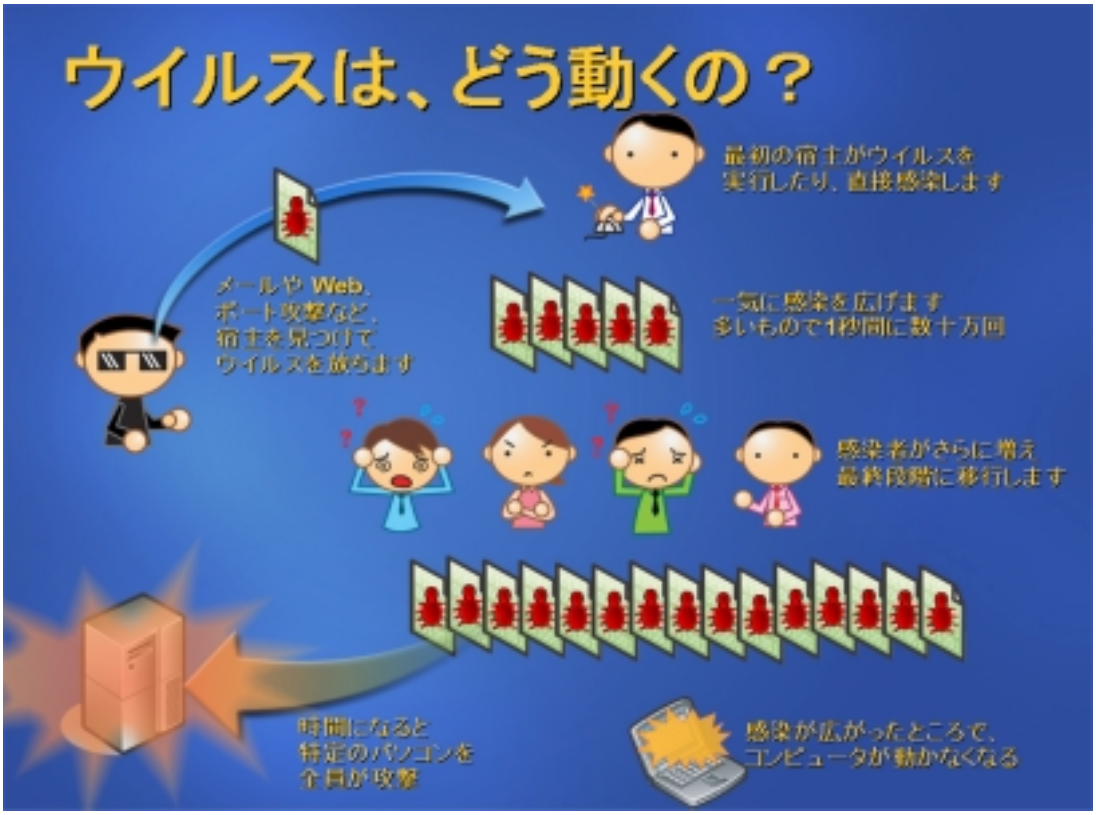
上のスライドにあるワームは、どれも桁違いの感染能力を持っていて、世界で数百万の被害を出したものです。

Blaster ワームは、コンピュータの世界に、セキュリティに弱いパソコンをインターネットにつなぐと感染する、という常識を作ったものです。

Sobig ワームは、何の変哲も無い添付ファイルがあるだけのメールなのに、大勢のパソコンユーザーがうっかり実行してしまいました。

また、Antinny ワームは、日本だけで使用されているファイル共有ソフト上で感染被害をもたらしたものです。日本だけで使用されているソフト用に開発されていることから分かるように、日本人が開発したと言われています。

コンピュータに被害を与える目的で作られた
プログラムを（コンピュータウイルス）という。

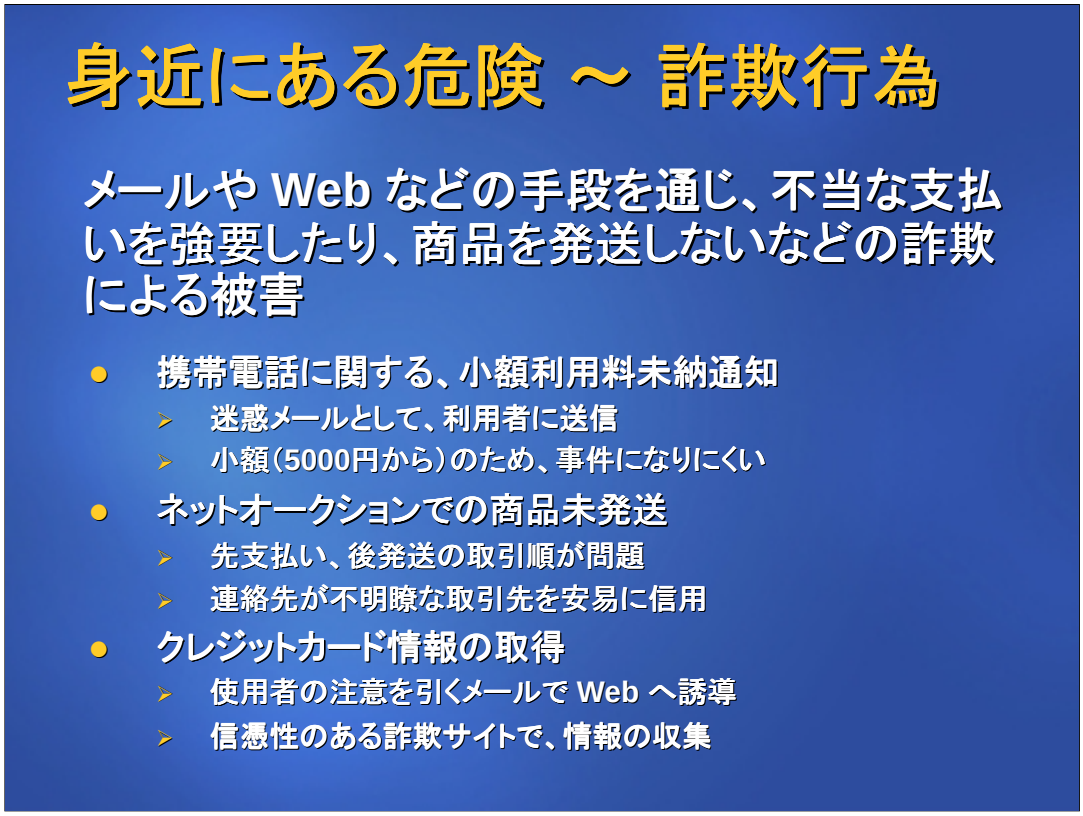


ウイルスの感染に関しては、ウイルスを作成した人が、最初に感染させる人を選んで、被害を発生させるところから始まります。

最初に感染した人のパソコンでは、その後知り合いやインターネットにつながっている人に攻撃を始めます。しかしこのとき、ほとんどの感染した人は自分が感染していることを知らないのです。時間が経過するごとに、感染した人が増えてゆきます。

最初の感染者から、次の感染者へ、その連鎖が延々と続いた結果、百万人単位での感染者が発生する被害が、これまでも何度も確認されています。

そして、ほとんどのウイルスが、感染被害を広めた後に、そのコンピュータを停止させたり、全部のプログラムがあらかじめ決められたサーバーをいっせいに攻撃を開始します。これにより、攻撃を受けたサーバーが応答をしなくなるなどの現象が発生します。



次に、インターネット上で今も行われている詐欺行為について説明します。

現実の世界でも、電話での勧誘や訪問販売を模した詐欺など、頻繁にニュースなどで取り上げられています。しかし、インターネット上の詐欺は、なかなかその実態が明らかにならないものです。

上にある幾つかの事例は、実際に発生した被害の例です。

最初にあるのは、携帯電話の使用料金に関する未納通知を模した、架空請求詐欺となります。実際には使っていない料金の滞納についての請求書が、電子メールで多くのユーザーに送信されています。この詐欺では、迷惑メールとして多くのユーザーに、料金の未納通知を行い、期日を過ぎると訴えるという内容が記載されています。その多くが5千円から1万円と、支払えない額ではないことが特徴です。

また、皆さんが良く利用されるネットオークションでも、詐欺が相次いでいます。購入代金を振り込んでも商品が送られてこないというのが代表的なものです。今のオークションでは、エスクローサービスといって、中間業者が商品の受け取りから支払いまでを一括して行い、商品が確実に届くことを保障しています。これを使用していない場合、落札した人が自分で出品者の信頼性を調べなくてはならないのです。

また、ここ最近、フィッシング (Phishing) 詐欺というものが増えています。この詐欺は、インターネットの利用者に対して、メールなどを通じて緊急の事態もしくは特をする情報を伝え、信頼した使用者がアクセスをした先のサーバーで、クレジットカードやその他個人の大切な情報を収集するというものです。実際の被害も出始めており、今後注意が必要な犯罪になっています。

また、注意すべきは、友人や知り合いの個人情報（名前、電話番号、住所、メールアドレスなど個人を特定できる情報）を無断で提供した場合、あなたも詐欺の幇助という罪に問われかねないのです。

現在増加している詐欺の一つに、クレジットカードや個人情報を収集しようとする（フィッシング）詐欺があります。

詐欺行為は、上記のような手順で行われるのが一般的です。

まずは、犯罪者が被害を受けてしまう人の連絡先を入手を試みます。この連絡先は、昨今の個人情報の漏えいや名簿の販売を行っている業者から不正に入手します。たとえば、携帯電話に関する詐欺の場合、携帯電話の契約者の名簿を入手するといったように、最も当てはまる人の情報を集めるわけです。このほかにも、大量な迷惑メールを送信し、その返信が帰ってきたメールアドレスを記録したり、インターネットから入手することもあります。

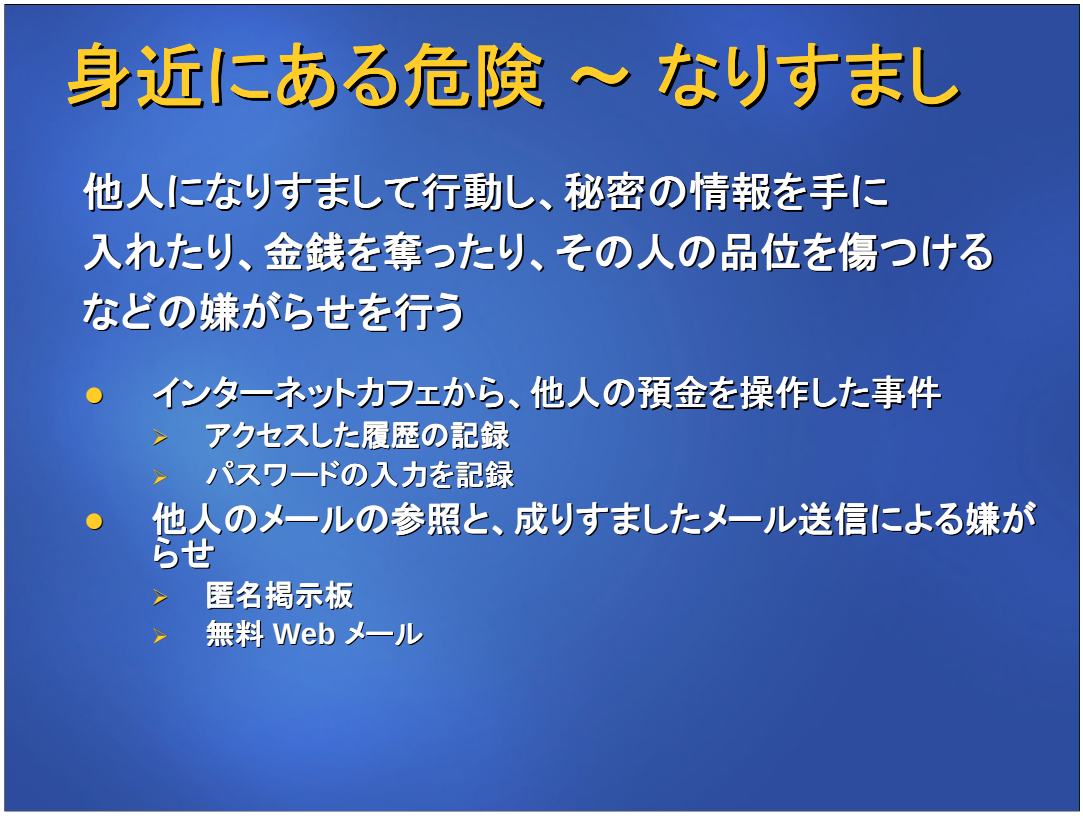
続いて、被害者を信用させるようなメールを送信します。この内容には、架空の住所や裁判所など、読んだ人を信用させるような工夫が行われています。このような信用をさせるようなテクニックを、ソーシャルエンジニアリングといいます。また、送信先が女性や低年齢の方の場合には、脅し文句が用いられたり、男性の場合にはアダルトサイトのふりをした内容などが送られることがあります。

このようなメールを受け取った方は、内容を信頼したり驚いたりして、すぐにお金を振り込んだり、偽者のサーバーへ、使用者の重要な情報を提供したりしてしまうわけです。

たとえば、クレジットカード情報が犯罪者に渡った場合、ある程度そのような情報が集まった段階で、一気に金銭的な犯行に及びます。個人上の場合、特に身体的な特徴の情報がある場合には、名簿業者に販売したりすることになります。さらに、インターネット上でサインなどを行った結果、購入の意思がない商品が送られてくるなどの被害につながります。

(スパム) メールは、営利目的のメールを無差別に大量配信されます。

(迷惑) メールは 個人(情報漏えい) により入手したメールアドレスに対して送信されることがあります。



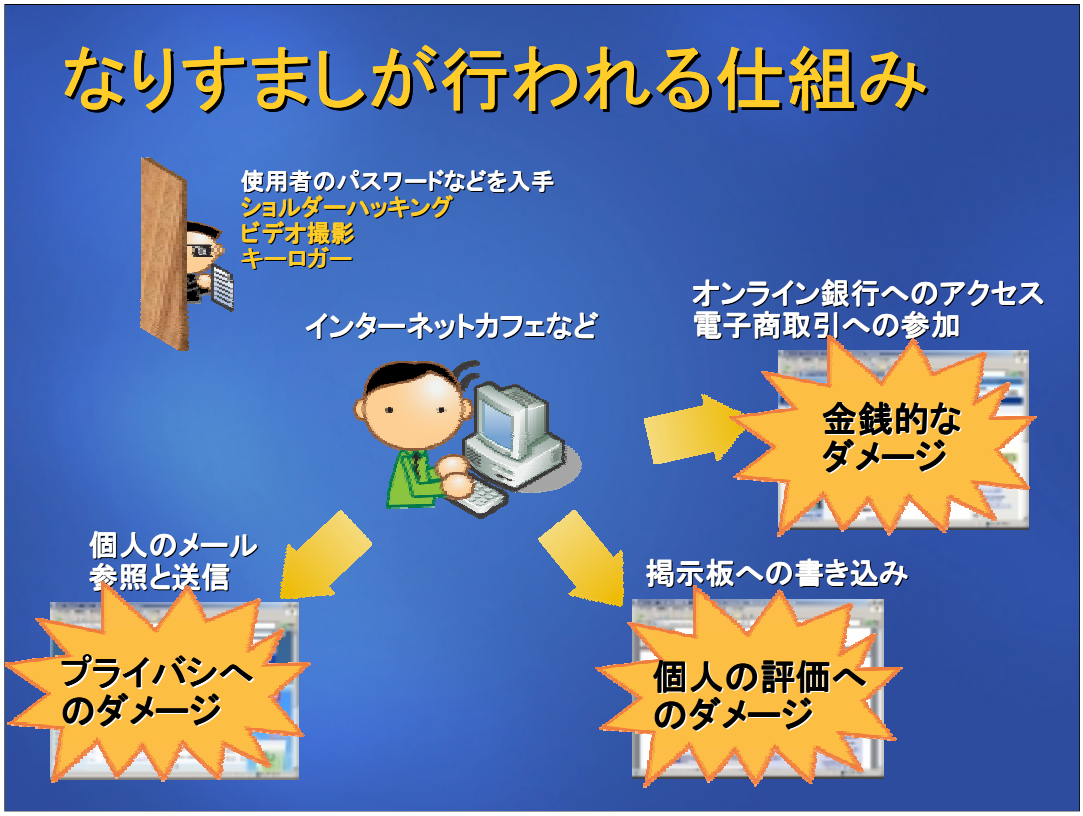
頻繁に被害報告があるものに、なりすまし被害というのがあります。インターネットが匿名性が高いことは皆さん理解していると思います。しかし、銀行や会員サービスなどを受ける場合には、個人を特定できる情報でサービスを受けることでしょう。

インターネットカフェや、知らない人のパソコンなどを使ったときに、自分の ID やパスワードが犯罪者に漏れてしまい、結果として会員サービスで勝手に買い物をされたり、酷いときには銀行の口座から全額が振り込まれてしまったりします。

ID やパスワードを犯罪者が入手する方法はいくつもあります。たとえばパソコンに、キーロガーというキーボードの入力内容を記録するソフトを入れたり、ソーシャルエンジニアリングの手法として、肩越しにキーの入力内容を見たり、ビデオカメラを隠して設置して、あとでその内容から情報を得たりします。また、パソコンの使用者の電話番号が分かっていれば、アクセスした銀行員や電子商取引サイトの管理者を装って、アカウントの情報を聞き出すなどの手法も発生しています。

ここまでは、会員サービスに関するものでしたが、インターネットならではの匿名掲示板や無料のメールサービスなどを狙った犯罪として、たとえばその本人になりすました発言をしたり、本人のメールの中身を読んだり、本人になりすましたメールのやり取りなどを行うなどの被害も発生します。金銭の被害は無いことがほとんどですが、精神的な被害はとても甚大となります。

インターネットの匿名性に隠れ、他人に（なりすま）した犯罪が発生している。

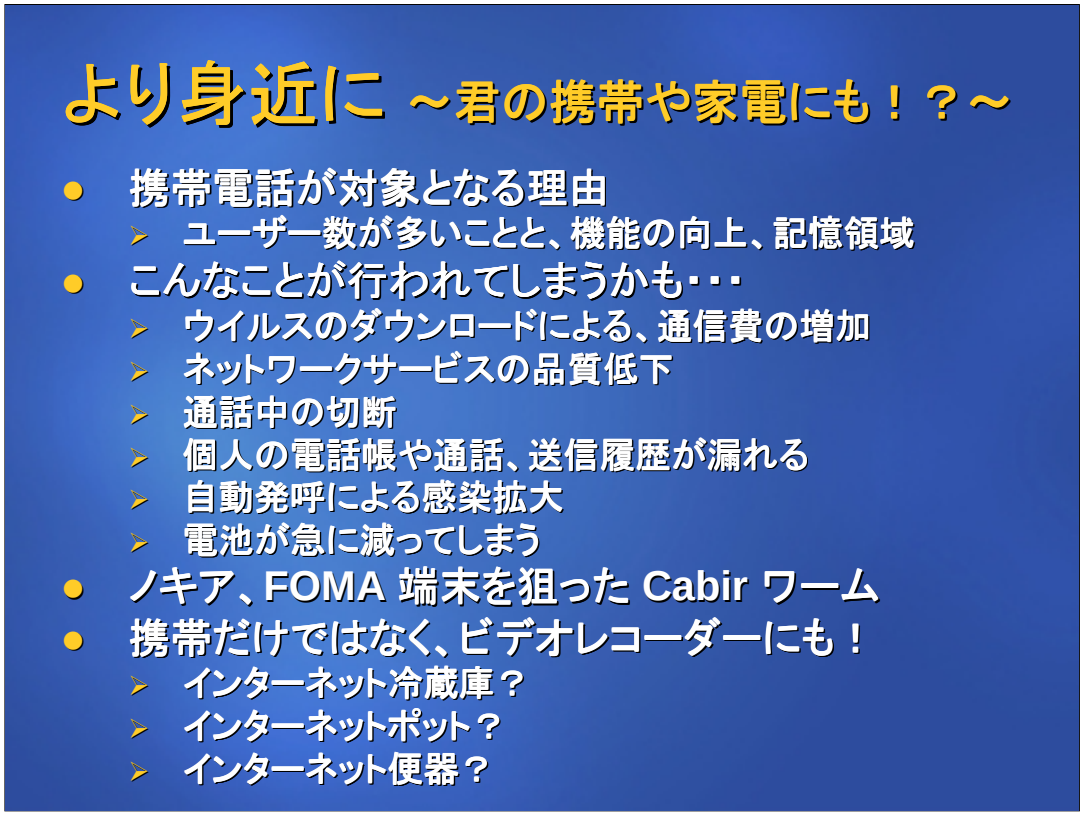


なりすまし被害は、誰もがパソコンを使える場所で行われることが多いといわれています。もちろん、メールのアカウントの情報などを別の手段で手に入れることもあり得ます。犯罪者は、その人が操作しているパソコンから情報を奪うことを常に考えています。キーの入力の順や、キーロガーなどを使用する場合もあります。

この結果、オンライン銀行や、電子商取引サイトでの金銭的な被害や、個人の大切な情報を盗み見られたり、掲示板をつかった個人の評価へのダメージなどが考えられるのです。

これらの手順は、ほとんどの場合非常に古典的なものです。しかし、人間の心の隙を突く犯罪は、今後も無くならないということは、現実の世界にも当てはまることでしょう。

キーボードの入力を常にチェックし、ID やパスワードを盗む (キーロガー) というソフトがあります。



ここまで説明したように、インターネットにまつわる危険は、常に私達の身近にあります。しかし、パソコンを使用していなければ大丈夫、と思っているとより危険なのです。

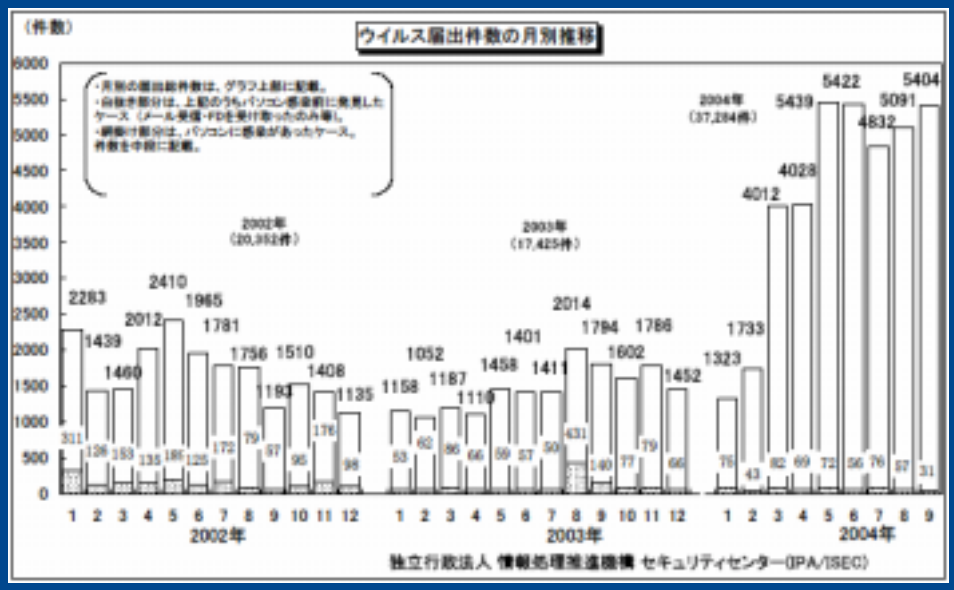
たとえば、携帯電話上で動作するウイルスが発生した場合を考えていましょうウイルスの作者は、多くの人が使用している機器を狙うことが知られています。今の市場の伸びを考えると、携帯電話が最も着目されているわけです。その証拠に、携帯電話各社ように、ウイルス対策ソフトが現在開発されている状況なのです。多くの人が使っているだけではなく、携帯電話が持つ機能や、ウイルスが動作するための性能も向上してきています。

もしも携帯電話で不正なプログラムが動作してしまった場合ですが、上にあるような非常に危険な状況が考えられます。もちろん、携帯電話会社では、そのようなプログラムが動かないように工夫をしていますが、将来的に安全性と便利さのどちらを取るかの決断によっては、状況が悪化することも考えられます。

実際、海外で発生した例ですが、ノキアや FOMA 端末が使用しているオペレーティングシステムに感染するタイプのウイルスが発見されています。このウイルスは、なんと近寄っただけで感染活動を行うといわれています。

ここでは携帯電話を取り上げましたが、ハードディスクビデオレコーダーの高機能化に伴い、コンピュータ犯罪の標的になってしまった例もあります。以前世間を賑わせたインターネット冷蔵庫は、商品の賞味期限の情報をインターネットから取得していました。また、インターネットポットは、ポットの使用回数を、ご老人の生活状況の把握に使っています。もしかすると、今後はインターネット便器といったものが出てくるかもしれません。

残念ですが、状況は悪化しています

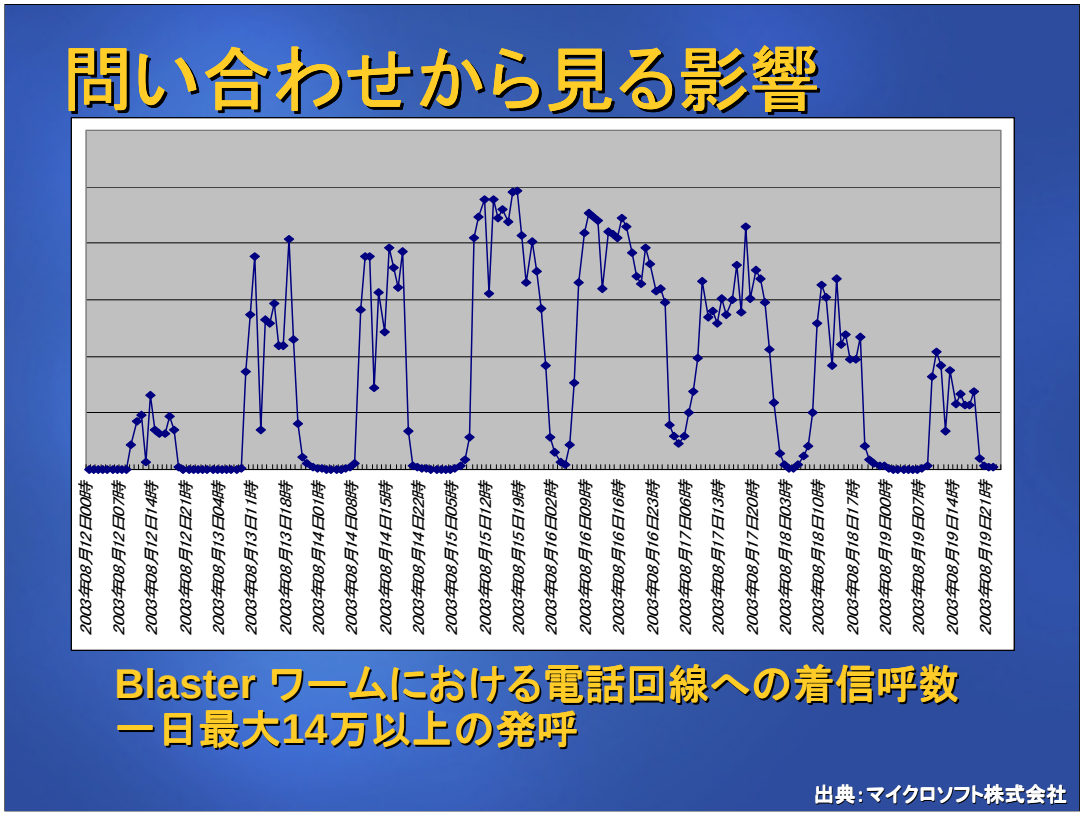


IPA/ISEC 9月の発見届出状況（詳細）
http://www.ipa.go.jp/security/txt/2004/documents/virus-full0410.pdf

このグラフは、IPA というウイルスによるセキュリティ被害の届出を行う組織が公開した資料です。

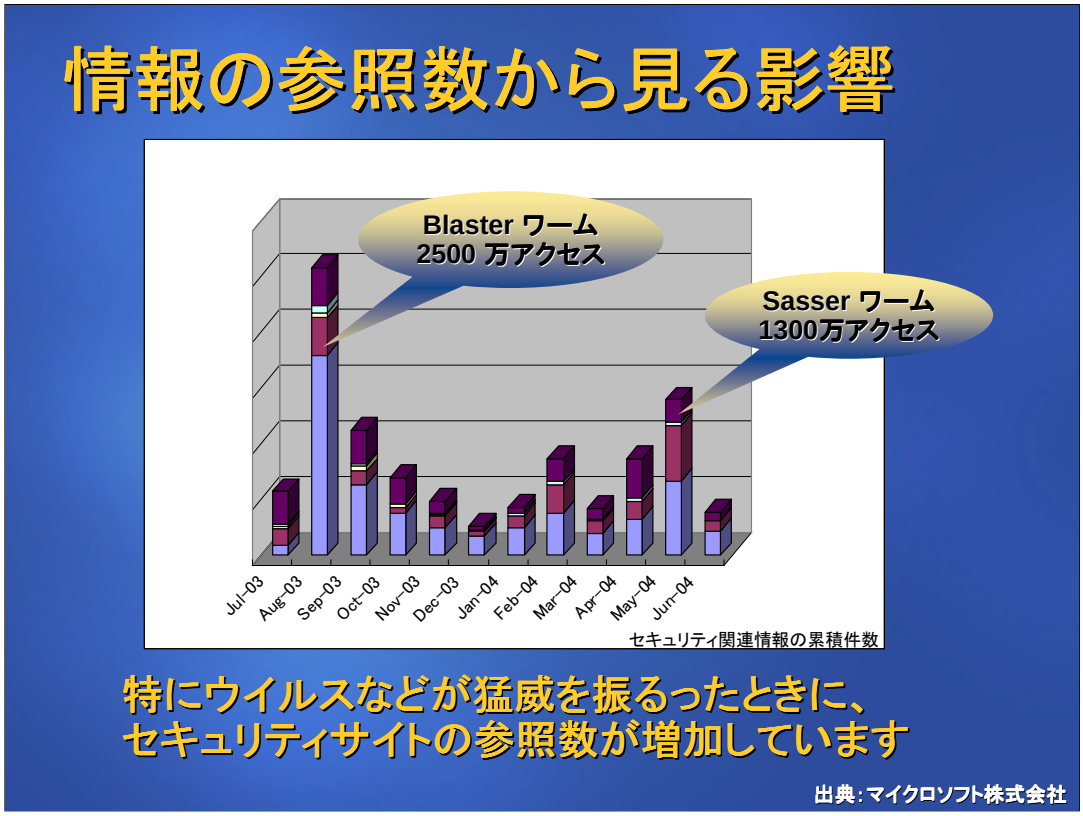
2004年3月あたりから、急激に被害の報告件数が増えています。被害の報告は必ず行わなければならないものではないですし、前述したように被害にあっていることを知らないパソコンの使用者もいることを考えると、氷山の一角といえます。

この資料には、詐欺の犯罪などは含まれていません。そのため、より深刻な被害はさらに沢山あることを覚えておいてください。



このグラフは、マイクロソフトの無償電話窓口に掛けられた電話の数を示しています。

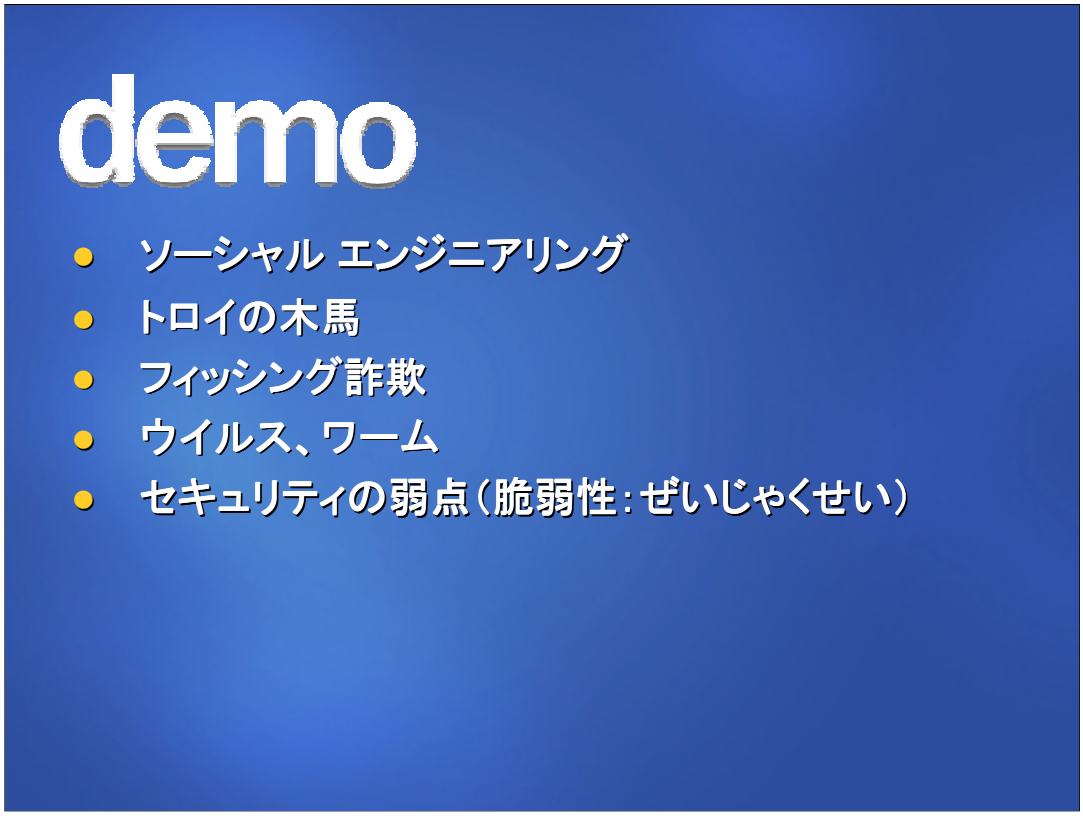
最大で、一日14万以上の電話が掛けられ、電話回線は NTT の回線交換局で輻輳状態になりました。もちろん、何度も掛けなおした方がいたためにこのような数の発個数になっています。初めて自宅でパソコンを使用している方がウイルスの被害に遭った事例として、象徴的な事故でした。



このグラフは、マイクロソフト日本法人の Web サイトにアクセスされた数を示しています。セキュリティに関する情報だけを抜き出しているため、より移り変わりが顕著になっています。

大きなセキュリティの事故が発生すると、一気にアクセスの数が増え、Blaster ワームが発生したときには、マイクロソフトの情報に他社のリンクを追加すると、リンクの追加先のサイトが停止してしまうなどの現象に発展しました。

しかし、のど元を過ぎてしまえば忘れてしまうようで、その後のアクセスは低下しています。セキュリティの情報は常に最新のものが提供されていますので、ぜひ定期的に参照してほしいと思います。



それでは、デモンストレーションを行います。

このデモンストレーションでは、日ごろ話に聞くウイルスが、どのように皆さんに忍び寄るか、または、侵入などを行う犯罪者が、どのようにその行為を行うのかをお見せします。

ソーシャルエンジニアリングとは、皆さんの心の隙に付け入る攻撃です。ほとんどの場合、人間は人を信じるとその人の言うとおりに動いてしまうものであることを理解してください。

トロイの木馬とは、受け取った人を巧みに信じさせ、問題のあるプログラムなどを実行させてしまうものです。ソーシャルエンジニアリングと、ウイルスの合体したものと理解してください。

フィッシング詐欺は、同じくメールを受けた人を脅したり、信頼させたりして不正な Web サイトに引き込み、犯罪の餌食にします。

ウイルスやワームは、皆さんご存知の通りですね。

あとは、ソフトウェアに潜むセキュリティ上の弱点とは何者か、それを理解していただきたいと思います。

正体を偽ってコンピュータへ侵入し、データの消去や他のコンピュータの攻撃などの破壊活動を行なう (トロイの木馬)と呼ばれる不正なプログラムがあります。

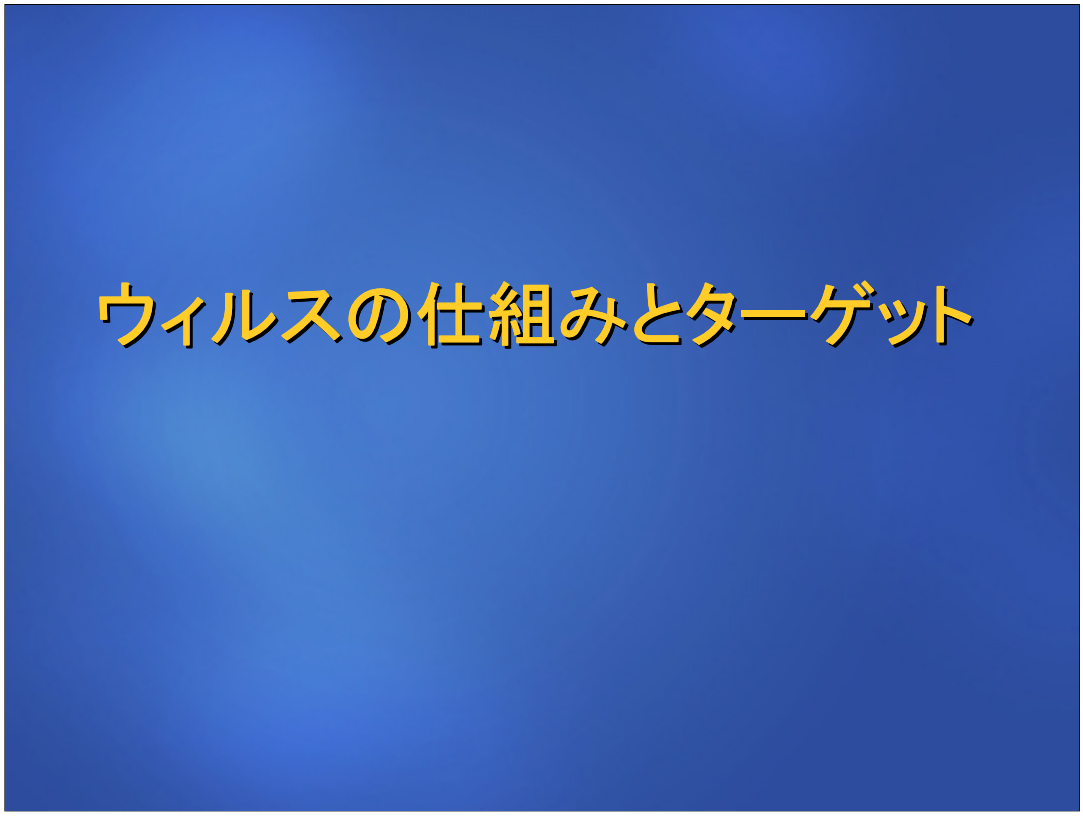
まとめ

- インターネットは、既にライフラインとなっています
- 犯罪の被害は、増え続けています
- さらに巧妙化するコンピュータ犯罪の手口は
  1. 使用者の心の隙を誘うもの
  2. コンピュータの弱点を狙うもの

どうやったら防げるのか？

（2時限目で学習します）

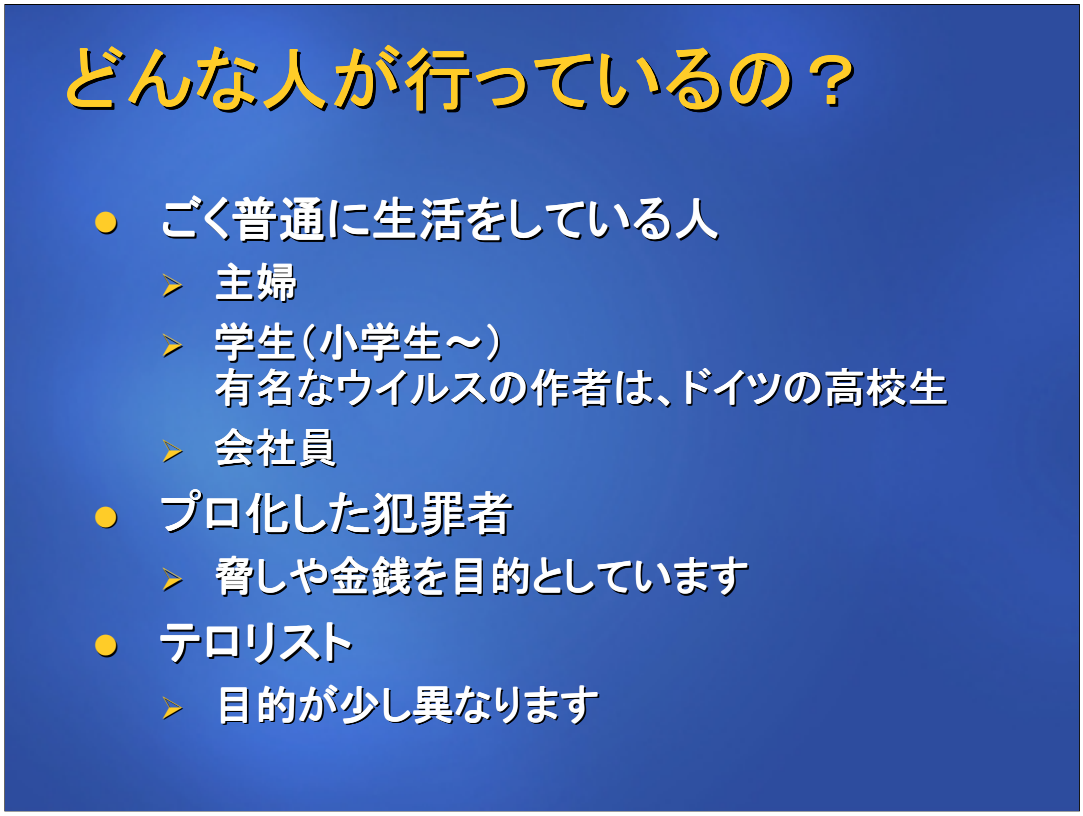
＜2時限目＞



既にウイルスの動作については説明を行いましたが、もう少しその背景について理解してください。

何事を行うにも動機があります。

犯罪と分かっていて手を出してしまう背景を理解し、自分が同じような過ちを犯さないよう、また攻撃側の視点に立って、自分の安全を守ることを目的としています。



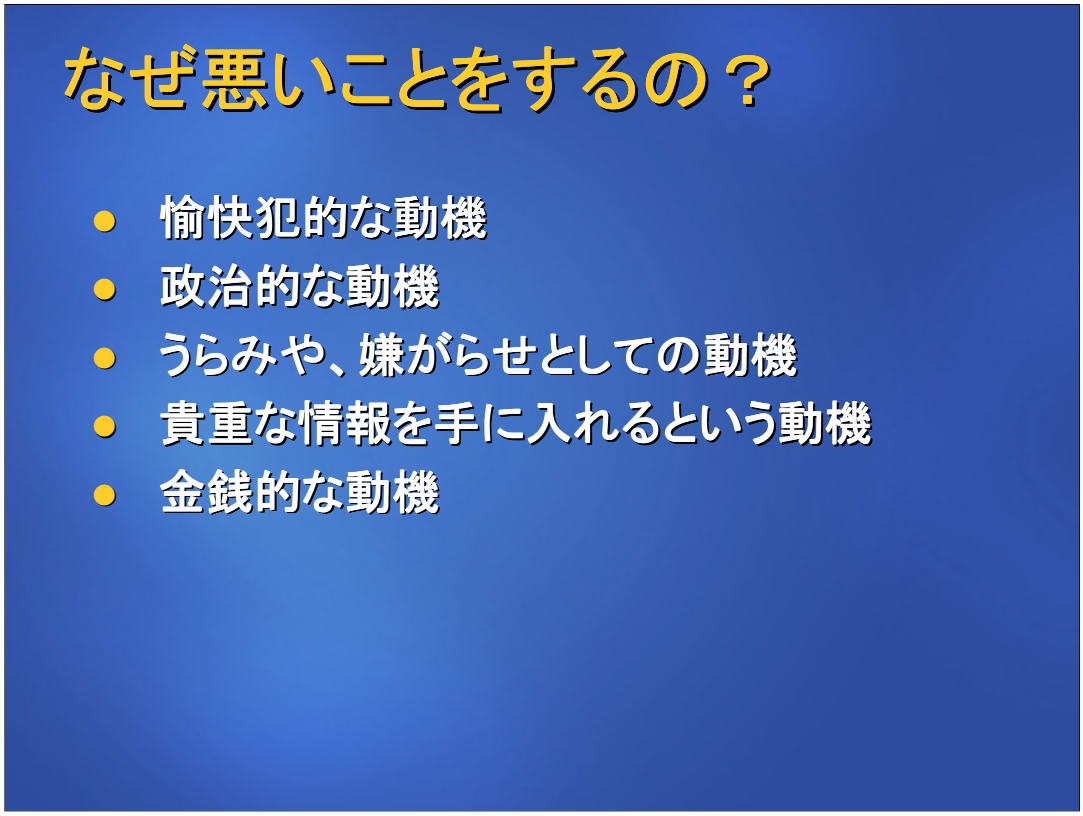
では、実際にどんな人が犯罪に手を染めているのでしょうか。これまでに検挙された数少ない例を見てみると、総じて一般の市民であることが分かります。

映画であるような、家に閉じこもったハッカーといったイメージは、実際の犯罪者には当てはまらないことが多いのです。共通することは、強い恨みや金銭が関わっていること以外、好奇心が強かったり、時間があったりということです。

最近顕著になっているのは、低年齢化ということが上げられます。インターネット上には、様々なツールが公開されていて、それらのツールを実行して犯罪を犯した小学生が居たり、Sasser ワームの開発者や、Blaster ワームの改造を行った者は、皆さんと同じ高校生なのです。

尚、テロリストやスパイといった特殊な目的を持つ凶悪犯は、特に注意を払われている存在といえます。何しろ、危険を冒して建物に侵入せず、情報を盗めるわけですから。

2004年のゴールデン ウィークに世界中で流行した Sasser ワームの開発者は(高校生) です。



なぜインターネット上で犯罪を働くのか、ということに関しては、いろいろな理由があるといわれています。その多くは、自己顕示欲を満たすためと言われていますが、それだけではない要素もあります。

愉快犯的な動機

度を過ぎた、いたずらの感覚

知らない家の呼び鈴を鳴らして、遠くから眺めるようなもの

政治的な動機

主張を犯罪の手口で表現

国際情勢に呼応した、嫌がらせ

個人的なうらみによる動機

他人のイメージや、資産へのダメージ

競合に対する嫌がらせとしての動機

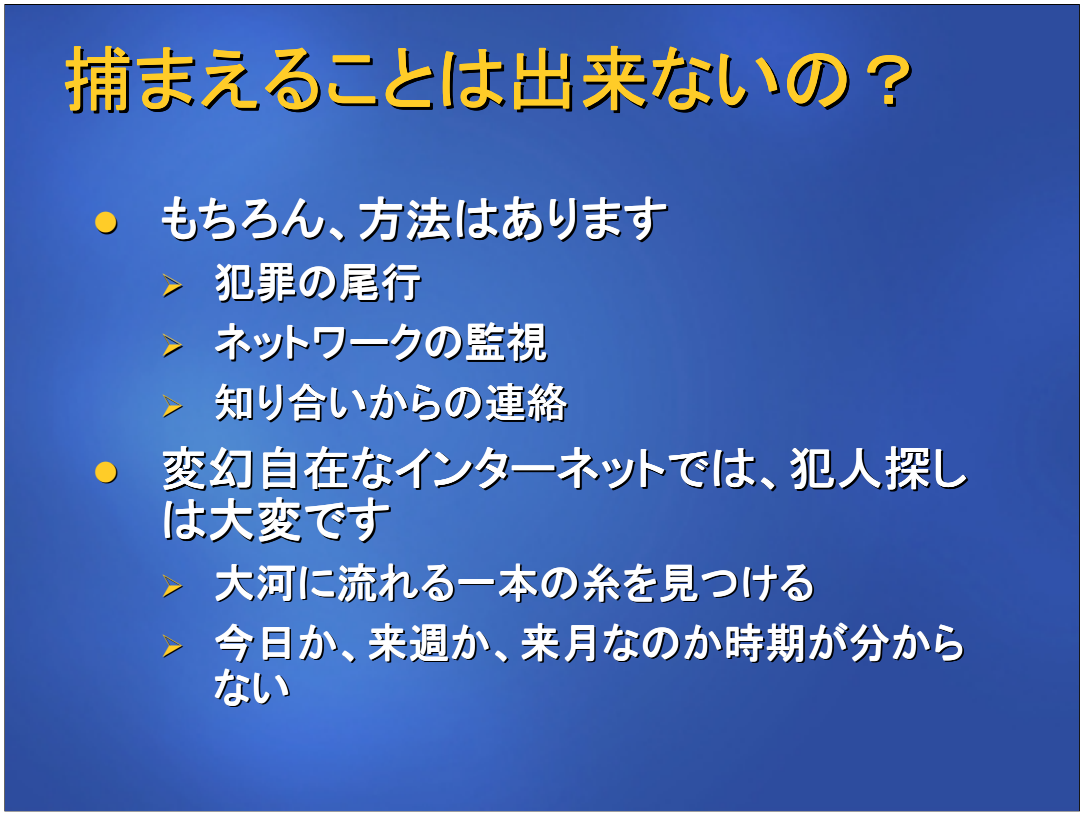
商売敵へのダメージにより、自社を有利にする

貴重な情報を手に入れるという動機

新しいビジネスを盗み、競争を有利に運ぶ

金銭的な動機

個人情報や企業秘密などを楯にした恐喝



では、犯罪者を確実に捕まえることは出来ないのか、という疑問も湧きますが、現時点では技術的に完全な対処というのは難しいといわれています。なぜなら、彼らは踏み台といわれる善良な市民のパソコンを経由して悪事を働くからです。

踏み台というのは、セキュリティに弱いコンピュータの操作を手に入れて、そこから他のコンピュータに対して攻撃を仕掛けることを指します。そのため、犯人を見つけても、それは善良な市民のコンピュータだった、といったことが考えられるのです。

トレースバック技術の進歩

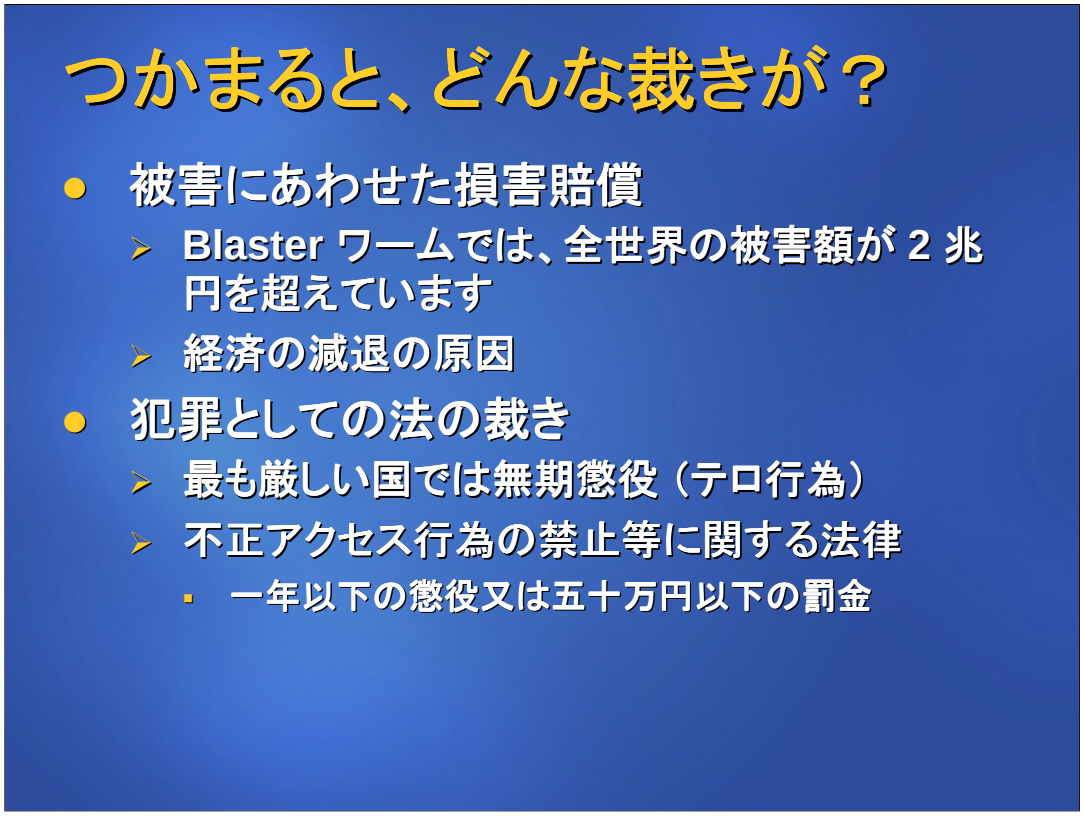
トレースバックとは、実際に攻撃が行われたときに、情報の流れてくる経路を逆算して犯人を特定します。現在基礎研究の最中です。

ネットワークの監視

現在、警察などの国家機関や、大手のネットワークサービスプロバイダ、セキュリティ関連企業などによって、インターネット上で不正が行われている統計をとっています。もしウイルスなどが確認されたら、そこから細かな情報の分析を行っています。

知り合いからの連絡

ウイルスなどの犯罪者は、集団行動することが多いといわれています。そこで、懸賞金など知り合いの犯罪を通告するような仕組みが、国外では行われています。そして、これが元で Blaster/ Sasser/ Netsky 作者などの検挙につながっています。



インターネット犯罪は、ほとんどの場合自動的に実施されます。自動的に被害を与え続けるプログラムにより発生する被害額は、天文学的な数字になってしまうのです。

被害額の算出は、一般的に以下のように考えられています。

復旧にかかる人的労力

企業の社会的ダメージ

システム停止による機会損失

信用低下による受注減など機会損失

情報資産の喪失

法的な裁きも徐々に揃ってきました。

国によって異なる基準

最も厳しい国では無期懲役

不正アクセス行為の禁止等に関する法律

一年以下の懲役又は五十万円以下の罰金

被害損害賠償の金額は、戦争に匹敵するほどのものとなっています。

Blaster ワームでは、被害総額 2 兆円以上

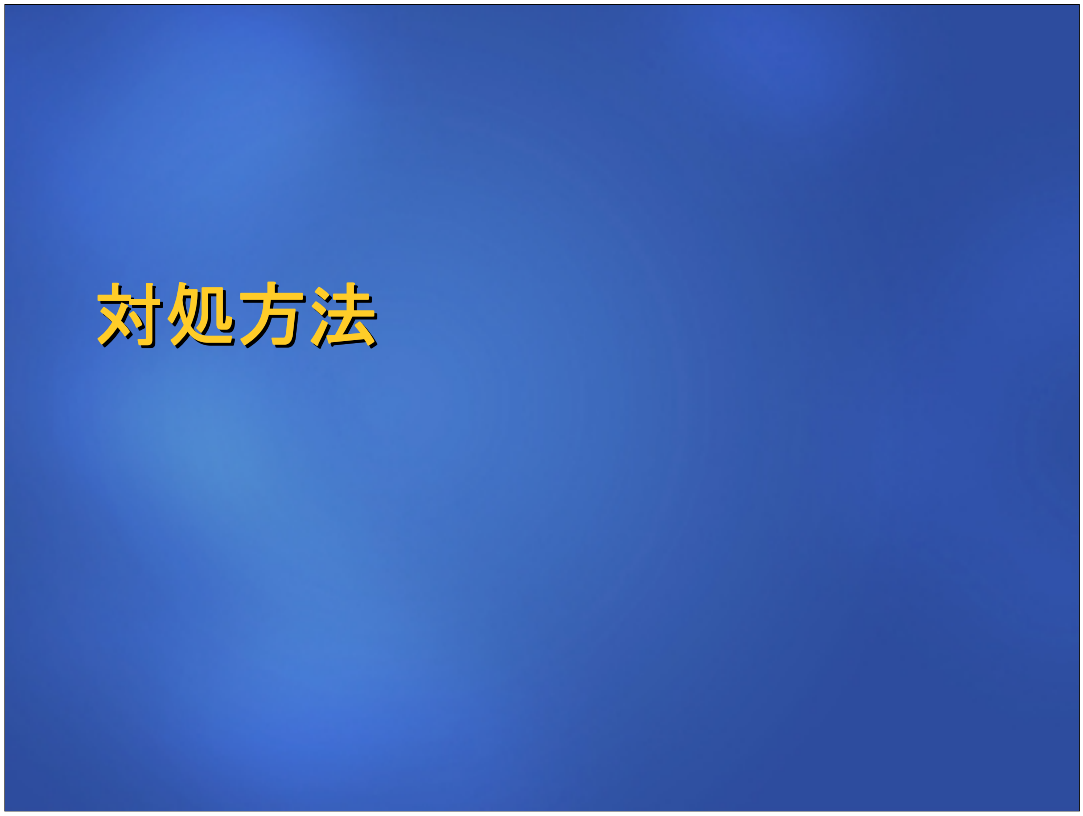
大企業での損害額は数億を超える

個人が受け止められる影響度ではない

現実世界では、限られた範囲への犯罪となる

ネット世界では、全世界に広がる犯罪へ発展

このような犯罪を犯してしまうと、取り返しがつかないのですよ。



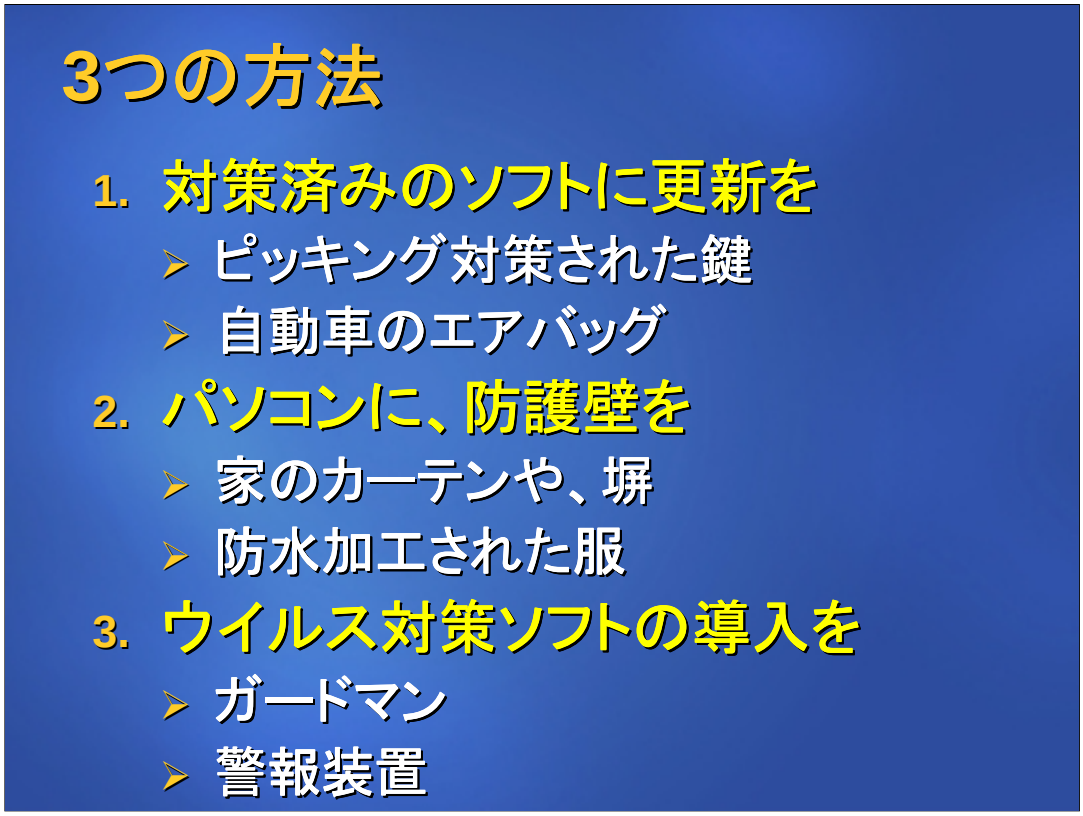
ここまで、インターネット上で実際に行われている犯罪に関するお話の一部を、理解してきました。これらの話は少し怖いと思いますし、なんとなくインターネットに参加するのが嫌になったかもしれません。

インターネットは本当に便利で、どんどん身近になってゆくことに間違いはないのです。来るべき将来に備え、現状としっかり向き合い、使用者と、産業界が協力して対策を行ってゆくべき課題なのです。

現実の世界では、犯罪から身を守るためには色々な取り組みが必要です。鍵を新しいものに変えたり、ガードマンを雇ったり、どうしても危険が無くならない時には、保険に入ったりするわけです。

しかし、インターネット上の犯罪のほとんどは、思ったより簡単に対策することが可能なのです。やり方さえ理解すれば、誰でも行えます。

ここからは、今後もインターネットを楽しく、便利に使うための方法について説明をしますので、しっかり理解してください。



パソコンの安全を守るには、3つの方法をすべて行うことが重要だとされています。

まず一つ目は、パソコンのソフトウェアに、犯罪者に付け込まれる弱点がある場合、まずはその弱点をなくすことから始まります。これは、ピッキング犯罪に弱い鍵を、新しい強い鍵に付け替えるのと似ています。また、交通事故で体を守るために、シートベルトやエアバッグを追加していることと似ています。

ソフトウェアは物体ではありません、皆さんが新しいより安全なソフトウェアに生まれ変わらせることが簡単に出来るのです。そして弱点が無くなったソフトウェアは、今までの機能をより安全に使い続けることができるのです。

続いて二つ目は、パソコンに犯罪者が入り込まないように防護壁を作ります。家を建てるときに、勝手に侵入者が入らないよう、または入るときに不審に感じさせるよう、塀を作りますね。また、窓ガラスにはカーテンをして中が見えないようにもしています。新しいお気に入りの服には、防水加工して水が染みるのを防ぎます。このように、外部からの侵入に強くなるような対策を行うのです。

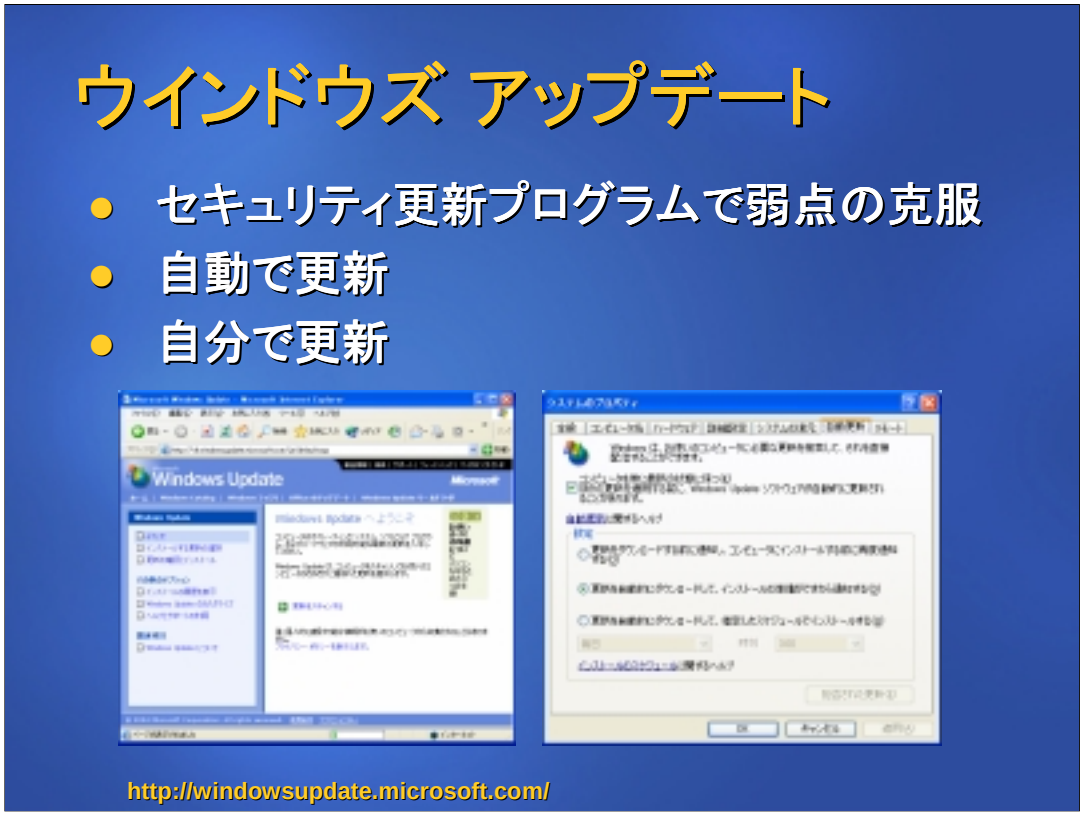
最後に三つ目ですが、犯罪者を発見するために、パソコンの中にガードマンを雇ったり警報装置を付けます。これは水際対策というもので、最後の最後に、不審なソフトウェアが入り込むのを防ぐのです。

この3つの手順について、説明をしたいとおもいます。

最初に行うことは、パソコンのソフトを常に最新の状態にして、セキュリティの弱点の対策を行うことが重要です。マイクロソフトの場合、ウィンドウズ アップデートや、オフィス アップデートという機能を用いることで、この弱点の対策を行うことができます。

現実の世界では、ピッキング犯罪に弱い鍵が話題となり、危険を感じた方々が新しい対策が施された鍵に付け替えを行いました。また、新しく家を建てるときには、すでに対策されたものを取り付けることと思います。しかし、鍵の場合には、使用者がお金を払ってこれらを購入しなければなりませんでした。なぜなら、ピッキング犯罪が無ければ、この鍵は鍵としての機能を果たしているのですから。ソフトウェアの場合にも同じように、機能としては問題なく動作するのですが、インターネット上の犯罪に弱い部分は対策を行わないと付け入る隙を与えてしまいかねません。

ウインドウズアップデートとオフィスアップデートは、インターネットにつながっていれば誰でも対策を進めることができます。



ウィンドウズアップデートはどのように行うのか、知っている人がいらっしゃるかもしれませんが、実は2種類の対策方法があるのです。

ひとつは、自動更新機能です。たとえば、インターネットに接続している状態でパソコンを使用しているとき、自動更新機能を有効にしている場合には、皆さんが見ている画面の裏側で、更新プログラムを入手して、更新を行う手前まで準備をしてくれるのです。準備ができたら、あとは皆さんが更新の許可をするだけで完了します。あまりに簡単で驚きますが、これもインターネットの危険に対応するために、パソコンが発達した成果なのです。

また、自動更新を使用しなくても、最新の状態に保つことができます。それは、ウインドウズアップデートサイトに自分で接続をして、新しい更新が無いかを調べる方法です。このように書くと、なんだか面倒な作業に思えますが、上の画像にあるように、いくつかのボタンをクリックするだけで対処が出来ます。注意しなければならない点は、皆さんが更新を確認する作業を忘れてしまうことです。月に一度は交信の状況を確認することを継続して行ってください。

オフィス アップデート

- オフィス アップデートは、自分で更新

http://office.microsoft.com/ja-jp/officeupdate/default.aspx

この前に説明をしたのは、ウインドウズの更新を行う方法でしたが、多くのユーザーが使用しているオフィスシリーズは、ウインドウズとは異なる方法で最新の状態にする必要があります。

オフィスアップデートというサイトでは、皆さんが使っているオフィスを調べて、必要な更新プログラムを選んで対策を薦めてくれます。

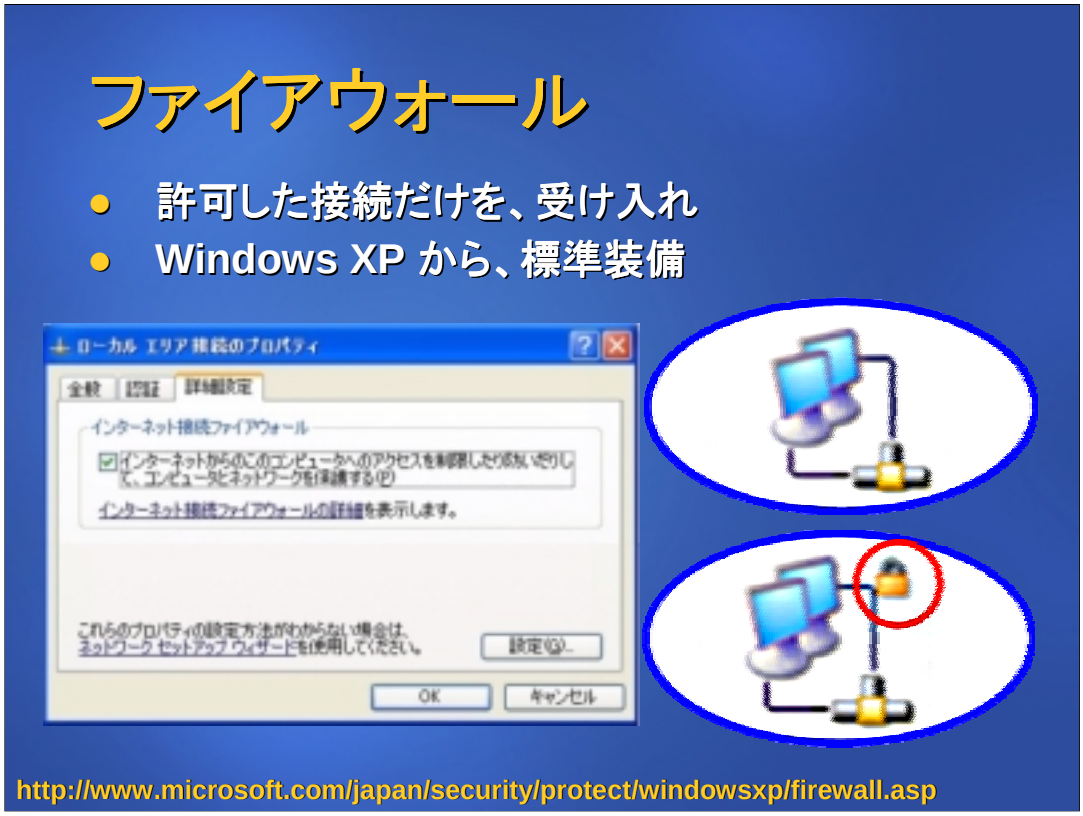
こちらには自動更新の機能はありませんが、現在マイクロソフトではオフィスも自動で更新できるように、さらに改良を加えているところです。

次に行う対策は、パソコンに防護壁作り上げることです。

防護壁がなぜ必要なのかわかりますか？先に説明したように、家に塀がないと侵入者が簡単に家に近づけるのと同じように、防護壁がないとパソコンに侵入する隙を作ってしまいかねないのです。

コンピュータの世界では、この防護壁のことをファイアウォールと呼んでいます。ファイアウォールは、皆さんが明らかに許可した通信以外をストップする機能を提供するものです。たとえば、ウイルスの攻撃は皆さんのパソコンがファイアウォールで守られていれば、突然何かを行われてしまうことはほとんど無くなるといわれています。過去にあった Blaster ワームなどは、このファイアウォールが有効であればパソコンに何も影響を与えなかった、つまり防ぐことが出来たのです。

もちろん、皆さんが使いたいソフトウェアがあるのでしたら、そのソフトウェアの動作を調べて通信を許可することができます。



このファイアウォールは、インターネットがとても危険な状況になる前の製品には含まれていません。マイクロソフトの製品であれば、Windows XP というソフトウェアから搭載されるようになったのですが、その前の製品では、別途ソフトウェアを購入しなければならないことを理解しておいてください。

Windows XP を使用している方は、上の画面にあるファイアウォールを有効にするボタンをクリックするだけで、対策を完了できますので、ぜひこの優れた機能を使用してみてください。

もしも今まで使っていたソフトウェアが動かなくなってしまった場合、ソフトウェアを販売している会社に聞いてみたり、インターネットで情報を探してみましょう。どうしても対策方法が無い場合以外は、出来るだけ使用を続けるようにしてください。

Windows XP 以前の Windows を使っている方は、次に説明をするウイルス対策ソフトの上位版を購入すると、そこに機能が含まれていることがほとんどですので、購入することをお勧めしています。

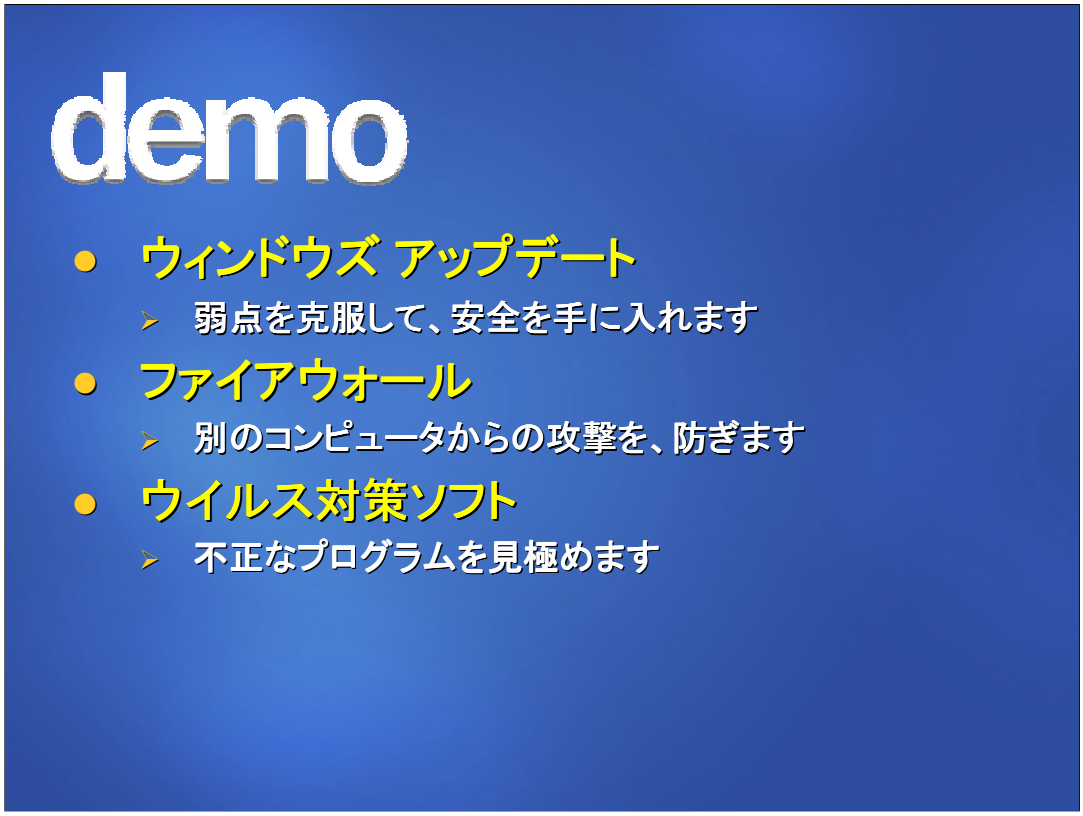
最後に 3 つめのウイルス対策ソフトについて説明をします。

ウイルス対策ソフトは、その名前のとおり。ウイルスや不審者が侵入しないように監視するガードマンの役目と、ウイルスに侵入された場合に、そのウイルスを駆除する役目を果たします。

ウイルス対策ソフトを正しく使用するためには、ウイルスの手配リストともいえる情報を常に最新の状態にしなくてはなりません。この手配リストは、パターン ファイルとか定義ファイルと呼ばれていますが、最近のウイルス対策ソフトは、この手配リストを自動的に最新のものに置き換えてくれるようになっています。手配リストが新しいものになっていなければ、新しいウイルスが侵入しようとしてやってきたときに、そのプログラムがウイルスだと気づかずに侵入を許してしまったり、感染したウイルスを駆除できなかったりします。それどころか、最近のウイルスはこのウイルス対策ソフトを停止したりするので、その後対策が正しく行えなくなったりします。ウイルス情報をもったファイルを最新にしておくことが最も大切なことです。

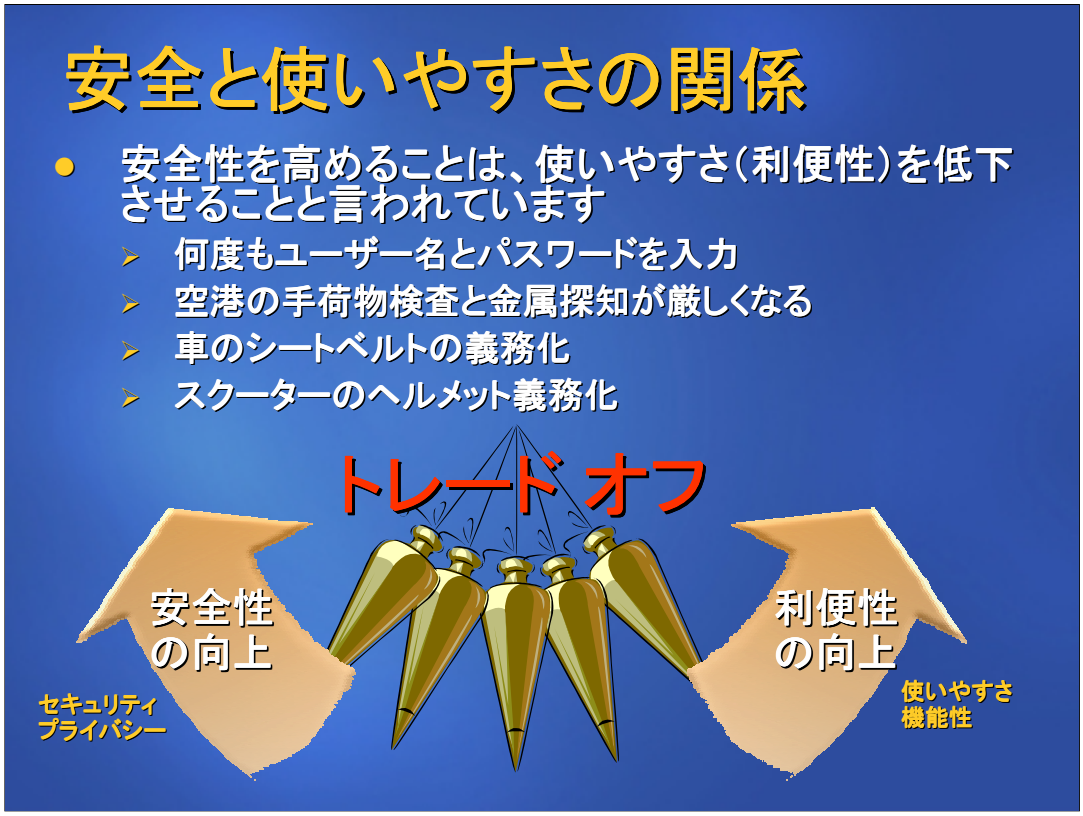
もうひとつ注意が必要な点は、パソコンに付属しているウイルス対策ソフトは、期間が決められた期間限定版です。使用できる期間が切れる前に、使用許可の更新を行ってください。

この対策だけは、残念ながら有料となります。しかし、ガードマンを雇うとおもえば、十分に支払うだけの価値があるのではないでしょうか。



それでは、今度はセキュリティ対策に関するデモンストレーションを行います。
このデモンストレーションでは、1時間目に行ったいくつかの攻撃を、いかに防ぐことが出来るかを確認してゆきたいと思います。

ウインドウズアップデートで弱点をなくした Windows に攻撃を加えるとどうなるのか。
ファイアウォールが正しく動作していると、外部からの侵入行為がどのように防がれるのか。
ウイルス対策ソフトが動いていると、どのように攻撃が停止させられるのか。
これらを実際に体験していただきます。



ここまでの説明で、インターネット上の危険と、その対策方法を説明してきました。

皆さんも内容に関しての理解ができたのではないかとおもいます。

皆さんがコンピュータを使用する理由は、危険への対策をするためではなく、ワープロや表計算、Web の検索などを行うためのはずです。ソフトウェアを開発する会社も、皆さんが使いやすいように様々な工夫をしてきているのです。

しかし、使いやすくすればするほど、そこに付け入る隙ができてしまいます。

家に入るのに鍵を開けるのが面倒だからといって、鍵を掛けない人はいないと思います。最近はテロの影響で、空港のチェックが厳しくなっているのは聞いたことがあるでしょう。車のシートベルトもそうです。昔はスクーターに乗るのにヘルメットは要りませんでした。

そうなのです、危険への対処をするには、残念ながら、使いやすさなどを犠牲にしなければならないのです。これをトレードオフといいます。

マイクロソフトでは、これまで紹介した3つの対策を簡単に、今までどおり使いやすく、できないかを考えて開発したのが、Windows XP のサービスパック 2 という更新ソフトです。

このソフトを皆さんの Windows XP に入れると、様々なセキュリティの向上に役立つ機能や、設定の変更が行われます。

上の画面は、セキュリティセンターという機能ですが、ここまでお話した対策が分かりやすくまとめてあり、皆さんがうっかり対策し忘れることを防いでくれます。

Windows XP サービスパック2では、ネットワーク、Web の閲覧、メール、ソフトウェアの持つ弱点を、独自の方法で安全に使えるようになっています。

まとめ

- 安全性と、利便性の両立は、トレードオフの関係
- 巧妙化するコンピュータ犯罪の手口への対策
  - 使用者の心の隙を誘うもの
    - ウインドウズ アップデート
    - ウイルス対策ソフト
  - コンピュータの弱点を狙うもの
    - ウインドウズ アップデート
    - ファイアウォール

最後に

コンピュータとインターネットは、とても便利な反面、危険も潜んでいます

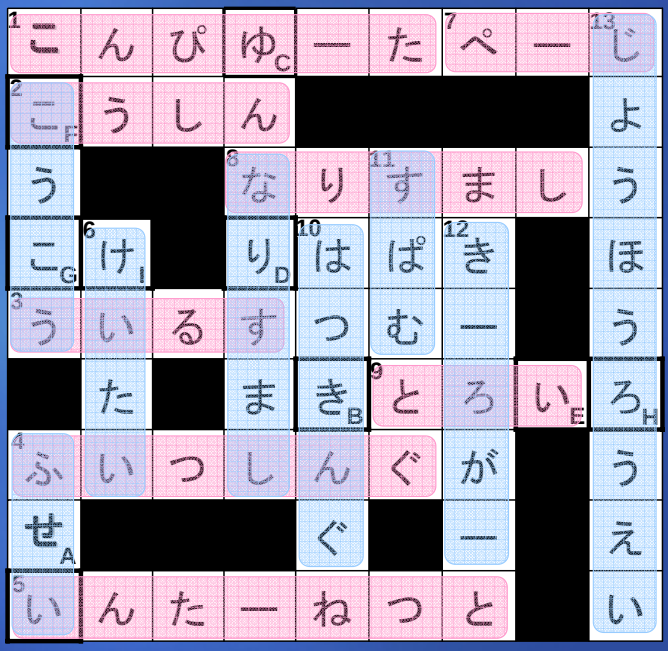
対策は簡単ですが、行動を起こさないと誰も守ってくれないのです

授業で習った対策を行えば、ほとんどの危険から身を守れますので、継続して実施してください

でも、一番大事なことは、危険に近寄らないなど、皆さんのこころがけなのです。

ソフトウェアを安全に利用するためには (継続) することが大切です。

まとめ(クロスワードパズル)



ヨコのかぎ

1. 皆さんの目の前にあります。これを使って情報を検索したりします。
2. 新しくすること。英語で言うとUpdate
3. 風邪と同じで感染しますが、マスクでは防げません。
4. 皆さんは引っかからないでね。お魚は釣れません
5. これで世界につながっています。
7. ホーム〇〇〇からいろいろな情報を調べます。
8. 「おれおれ」って誰?
9. トロイアの故事からこう名づけられました。ブラピ主演で映画にも

タテのかぎ

2. 皆さんは〇〇〇〇生
4. 〇〇〇請求・〇〇〇アクセス、正しくない行為をこういいます。
6. 最近はこれにもウィルスが。電車の中ではマナーモードにしようね。
8. あかずきんちゃんの狼はおばあさんに〇〇〇〇〇ました。
10. 他人のコンピュータに侵入すること。「カッコウはコンピュータに卵を産む」名著です。
11. 〇〇〇メールは迷惑です。ハワイではおにぎりの具にもなっています。
12. キーボードから入力されたパスワードなどを盗みます
13. 個人情報はどこから知られてしまうのでしょうか。

解答

A せ B き C ゆ D り て E い 対策は

皆さんの F こ G こ H ろ が I け が一番大事です

2004年10月22日初版発行
2004年10月28日第2版発行
発行：マイクロソフト株式会社
制作：マイクロソフト株式会社　セキュリティレスポンスチーム
著作：マイクロソフト株式会社