経営講演会

講 演 録

『中小企業のサイバーセキュリティ』

（ 2020 年 11 月 30 日 講演 ）

講 師 東京電機大学研究推進社会連携センター 顧問 客員教授

佐々木 良一 氏

RESONA りそな中小企業振興財団

講 師　東京電機大学研究推進社会連携センター 顧問 客員教授 佐々木 良一 氏

◆プロフィールご紹介

●主な経歴

1971 年 東京大学医学部保健学科卒業

1971 年 株式会社日立製作所入社。システム開発研究所にてセキュリティ技術、ネットワーク管理システム等の研究開発に従事

1981 年　東京大学大学院 博士課程修了（工学博士）

2001～2018 年 東京電機大学教授

2020 年　東京電機大学研究推進社会連携センター　顧問　客員教授（現職）

●主な受賞

2002 年　情報処理学会論文賞受賞

2007 年　総務大臣表彰

2017 年　総務大臣表彰

2017 年　電子情報通信学会マイルストーン表彰　等

●主な委員

日本セキュリティ・マネジメント学会会長、

内閣官房サイバーセキュリティ補佐官等を歴任

●主な著書

「IT リスクの考え方」岩波新書 2008 年等

この講演録は、2020 年 11 月 30 日に YouTube ライブで Web 配信した、当財団主催の経営講演会を収録・編集したものです。なお、財団ホームページにも掲載しております。（https://www.resona-fdn.or.jp）

1. 中小企業におけるセキュリティ対策の現状

2020 年 1 月、サイバー攻撃による三菱電機の情報流出の可能性が報道されました。また、最近話題の**ランサムウエア**、データを勝手に暗号化して、お金を払ったら元に戻してあげると脅迫する攻撃、これがますます巧妙かつ悪質になっています。例えばゲームメーカーのカプコンが数億円、あるいは十数億円を要求されているといわれております。

新聞に出るのは大企業が多いのですが、中小企業が関係ないということではありません。日本損害保険協会が実施した「中小企業の経営者のサイバーリスク意識調査 2019」では、中小企業の経営者・役員 825 名から回答があり、そのうち約 2 割はサイバー攻撃の被害の経験があり、被害額が数千万円を超えるものもあるという結果になっています。

一方、中小企業におけるセキュリティ対策としては、「OS やソフトの脆弱性管理、ウイルス対策ソフトの導入」は約 52%の企業で実施していますが、「現在、サイバー攻撃に対する対策はしていない」ところが 24%あるということも明らかになっています。

また、「貴社の経営課題について、優先度の高いものをお選びください」という問いに対しては、「サイバーリスクへの対応」に注目している経営者は、非常に少ないのが現状です。

2. セキュリティの基礎

サイバー攻撃をする攻撃者には、「部外者」と「部内者」がいます。**部外者**としては「**クラッカー**」、新聞等では**ハッカー**と書くことが多いのですが、これは、面白半分でサイバー攻撃をする人たちです。また「**スパイ**」には、産業スパイや国家スパイもあります。そして「**テロリスト**」です。それから、4 番目が「**犯罪者**」です。これは金銭目的で攻撃する人たちで、典型的な例が、先ほどのカプコンに対するランサムウエア攻撃だろうと思います。

また、従業員などの**部内者**ですが、一般的に、犯罪の成功確率は部外者よりも部内者のほうが高くなります。一方、攻撃の数からいうと、外からのほうが圧倒的に多いわけです。

ただ、情報の流出による被害については、昔は部内者のほうが多いといわれていたのですが、最近は外からの攻撃が増え、かつ巧妙になってきたこともあって、アメリカの大手電気通信事業者ベライゾンの調査によると、部外からの攻撃による成功の数が多くなっています。部外者、部内者、両方にちゃんと対応していく必要があるということでしょう。

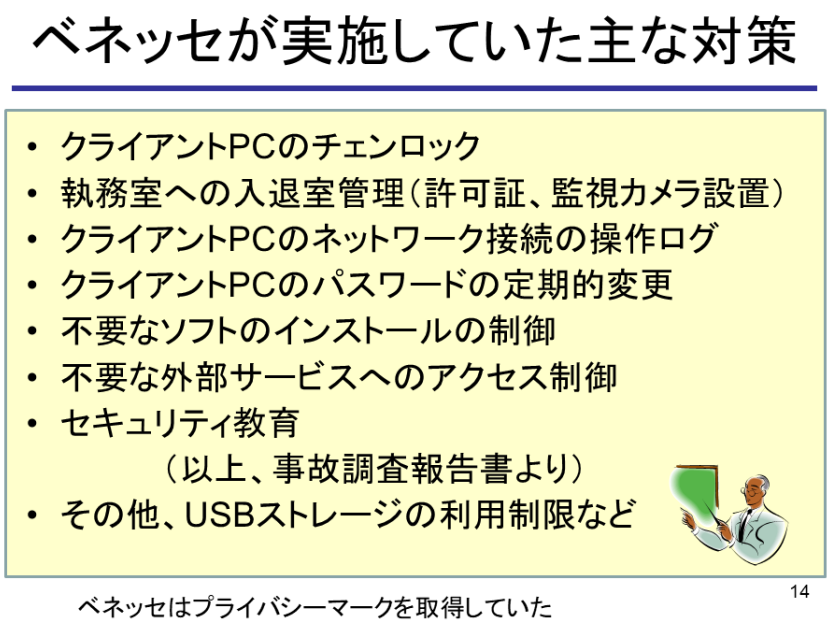
ベネッセ個人情報流出事件

部内者による攻撃の典型的な例として、今から 5 年ぐらい前に、ベネッセコーポレーションからの情報漏洩事件があります。同社は、いろいろな試験や講義を受けた顧客の個人情報を、顧客の同意を得て保管していました。その個人情報を管理していた系列企業の外部委託者であった被告が、情報をスマホにコピーして持ち出し、名簿業者に販売したのです。

実はベネッセのセキュリティがいいかげんだったわけではありません。まず系列会社からベネッセのデータベースサーバーへのアクセスは監視されており、不審なアクセスには

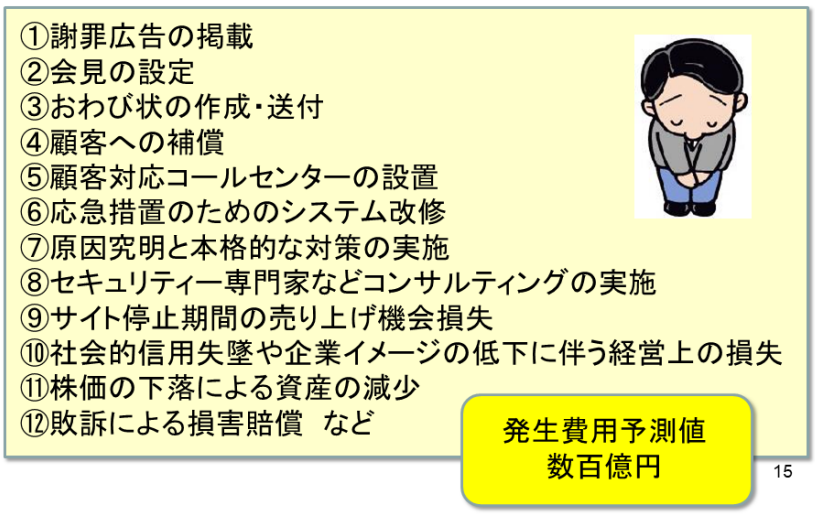
警告が出る仕組みでした。しかし、被告は正規のアクセス権を持っていたため、システム側でも気付かなかったようです。また PC からスマホにコピーできない仕組みになっていましたが、新しいスマホではたまたまコピーできたということでした。

これ以外にも、入退出の監視カメラを置いたり、クライアント PC からネットワークへの接続の際には操作ログを取ったり、いろいろな対策をしていました（図 1）。



（図 1）

こういう事件が起こると、謝罪広告の掲載だとか会見の設定、おわび状の作成、送付、顧客への補償等々から、最終的には社会的信用の失墜や株価の下落、裁判に敗訴した場合の損害賠償などを考えると、数百億円の被害が出てしまうケースがあるわけです（図 2）。



（図 2）

このベネッセの事件では、漏えいした情報は 3,500 万件分もあったということですから、おわび状を郵便で出すだけでも億円単位になってしまいます。

内部不正に対する防止策

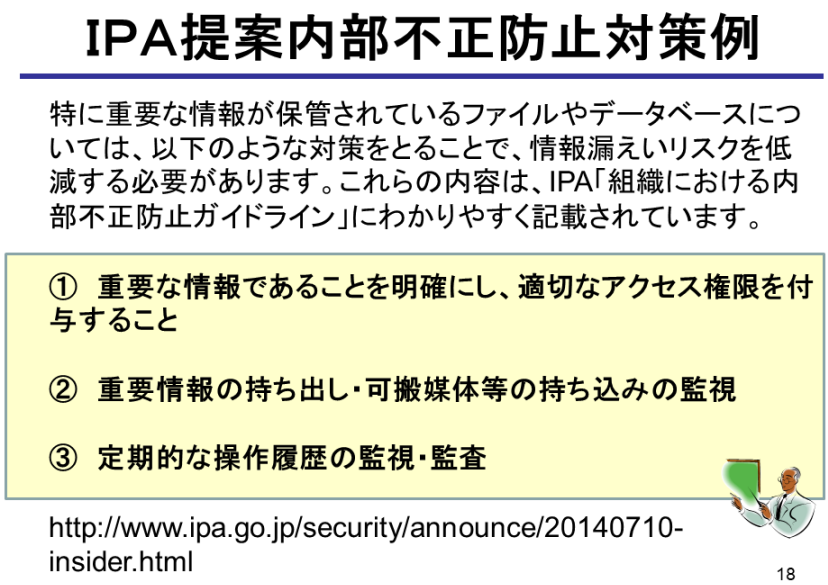
内部不正の動機は、『**情報セキュリティ白書 2013**』(IPA=独立行政法人情報処理推進機構)によれば、「不当な解雇通告を受けた」「給与や賞与に不満がある」「社内の人事評価に不満がある」などが挙げられています。しかし、こういうことを思う人をゼロにするのはほとんど不可能に近いわけですから、いろいろな形での対策が必要になるわけです。

内部犯罪の人たちは、「恨み系」か「金銭目的系」の 2 つに分かれるといわれています。

恨み系では、その会社のシステムを破壊したり、データを壊したり、情報流出も、外部に知られたら困る文書などをオープンにするようなケースが多くなります。

それに対して金銭目的系は、システムを悪用してお金を手に入れたり、情報を流出させると脅してお金を要求したりするという形です。

IPA では、こうした内部不正への対策等も提示しています（図 3）。ざっくり言うと、「**重要な情報であることを明確にし、適切なアクセス権限を付与すること**」、それから「**重要情報の持ち出し・可搬媒体等の持ち込みの監視**」をすること、そして「**定期的な操作履歴の監視・監査**」をすることが必要だとされており、これをぜひ意識していただければと思います。



（図 3）

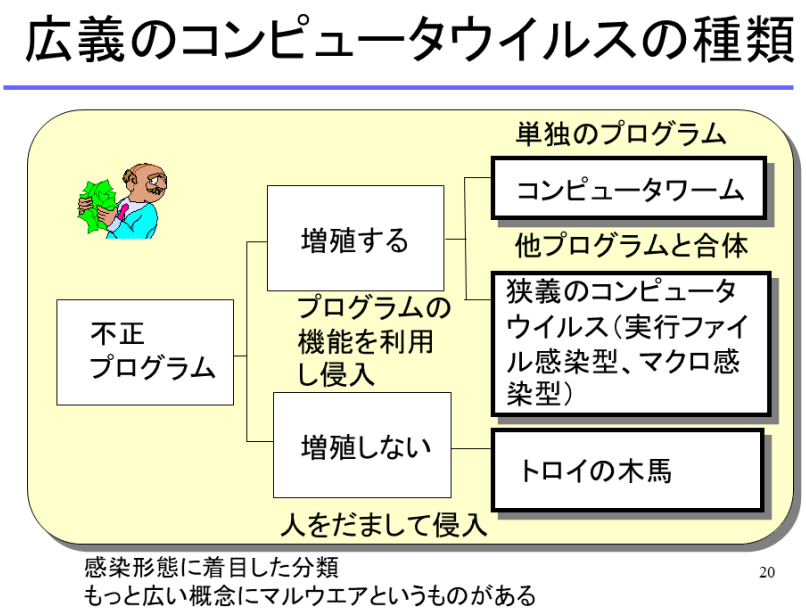
間接的攻撃に対する防止策

部内者の他にも、部外者に対する対策も必要になります。部外者による攻撃は、大きく「直接的攻撃」と「間接的攻撃」に分けることができます。**直接的攻撃**というのは、自分でネットワークを経由して、相手の PC やサーバーに入っていって、情報を取ってきたり壊したり

する攻撃です。

それに対して**間接的攻撃**というのは、ソフトウエアを相手のコンピューターに送り込むことによって、ファイルへの攻撃、データの取得・破壊をやらせます。これがいわゆるコンピューターウイルスとかマルウエアとか呼ばれるものです。

こういう不正プログラムは、大きく、「自分自身をコピーして増殖できるもの」と、「増殖機能を持たないもの」に分けられます。増殖する機能を持たないタイプは、例えばこれは面白いゲームですよなどと人をだましてダウンロードさせ、遊んでいるうちに不正なプログラムを送り込みます。これが「**トロイの木馬**」といわれるマルウエア、広義のコンピューターウイルスの一種です（図 4）。



（図 4）

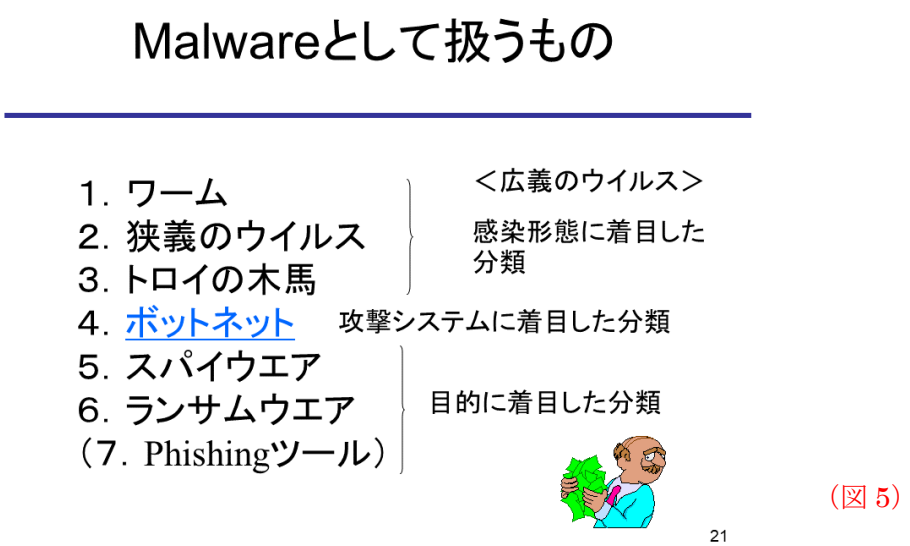
それに対して、増殖する機能を持つものは、相手の PC やサーバーにあるプログラム上の弱点を突いて入り込み、プログラムの機能を利用して自分自身をコピーするとともに、不正を行います。

増殖する機能を持つものには、そのプログラム単独で不正を行うことができる「**コンピューターワーム**」と呼ばれるものと、自分自身では不正はできませんが、他のプログラムと合体することで不正が可能になる、いわゆる狭義の「**コンピューターウイルス**」の 2 つのタイプがあります。

今はトロイの木馬が一番多く、その次がコンピューターワームで、狭義のコンピューターウイルスはだいぶ減ってきています。ですから、だまされないようにすること、コンピューターワームが侵入してくるセキュリティホールを作らないように、セキュリティパッチといわれるプログラムを常に新しいものに更新することをしっかりやっていくことが必要になります。

広義のコンピューターウイルスというのは、感染形態に着目した分類ですけれども、攻撃システムに着目した分類としては「**ボットネット**」がありますし、目的に着目した分類では、

「スパイウエア」だとか、先ほどお話ししたランサムウエアなど、いろいろな分類のしかたがあります（図 5）。



（図 5）

ボットネットの「ボット」は、ロボットの略だそうですが、これは PC やいろいろなコンピューター装置にウイルスを感染させて、その PC などをロボットのように自由に操れるようにするものです。そうしておいて、攻撃者は指令サーバーを経由し、感染したボット PC などを操作して攻撃を仕掛ける。

例えば、本当の発信者が分からないようにして迷惑メールを送る場合がこのケースです。あるいは「**ＤＤｏＳ**」といって、1 カ所に、いろいろなところから大量のパケット(データの小さなかたまり)をぼんぼん投げつけて、PC やサーバーを動けなくする攻撃がありますけれども、これも攻撃者が、指令サーバー経由で多数のボット PC を操って行います。

それから目的に着目した分類では、先ほどのスパイウエアやランサムウエアのほかに、「**フィッシングツール**」といって、メールを送り、そこから不正なサイトに誘導しておいて、そのサイトで感染させる攻撃もあります。

フィッシングツールの手口

私のところに、ファーストバンクから来たという外見で、フィッシングメールが届きました。メールの本文には、文中の「here」という部分をクリックし、別なサイトに飛んで、パスワードをすぐに変えるように書いてあります。このフィッシングメールは、途中まで操作しただけでは危険はないという情報を得ていましたから、実際にクリックしてみました。そうして誘導されたサイトは、本物のファーストバンクのサイトと区別がつきません。

そのサイトで、適当な ID とパスワードを入れてログインボタンを押してみました。そうすると、「Network Error (tcp_error)」、つまり、ネットワークが故障しているという表示が出てきました。ただ、このエラー表示自体がニセモノで、攻撃者が OS のメッセージに似せ

て表示させたものです。

本来の ID とパスワードを入力すれば、その時点で攻撃者に口座情報が盗み取られます。ですから、エラー表示を見て、「今ネットワークの調子がおかしいなら、後でもう一度やってみよう」と思っているうちに、攻撃者は、あなたの口座から送金してしまうわけです。

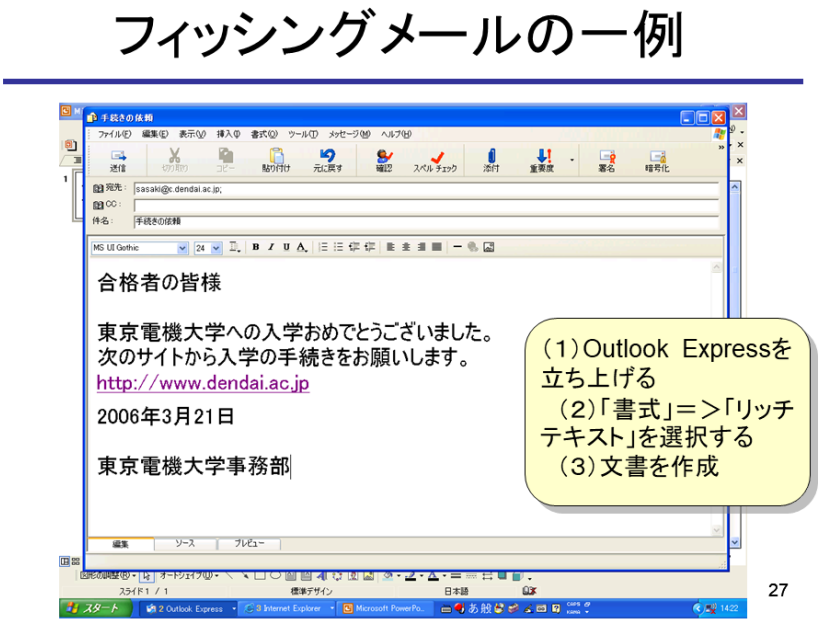
基本的には ID とパスワードだけでお金を動かせるらしいアメリカと違い、日本の場合は口座の暗証番号も入れなければならないものもあるため、日本では、暗証番号を入れる窓があったり、一度さらに別のサイトに飛ばしたりするものもあるようです。

実は簡単に作れるフィッシングメール

私は、偽メールを作るのがどのくらい大変か調べるために、試しに作ってみたことがあります。少し古いですが、「書式」から、「リッチテキスト」を選んで、文書を作成します。

ちなみに、昔はこういう情報は一切教えませんでした。今、ハッカーズサイトでは、不正の方法や、不正のためのプログラムが多数置いてあって、どんどん攻撃が高度化しています。そこで、我々もその攻撃方法を知り、対策も学ぼうとなっているわけです。

さて、リッチテキストでデータを作ると、ウェブサイトなどを作るための HTML 形式で保存されます。リンク先として例えば“http://www.dendai.ac.jp”と入力して、飛び先だけを例えば“http://www.nisenodendai.ac.jp”に換えることができます。そうすると、メールに表示されている「東京電機大学」のアドレスをクリックしたつもりなのに、「偽の東京電機大学」に飛んでしまうことになるわけです（図 6）。

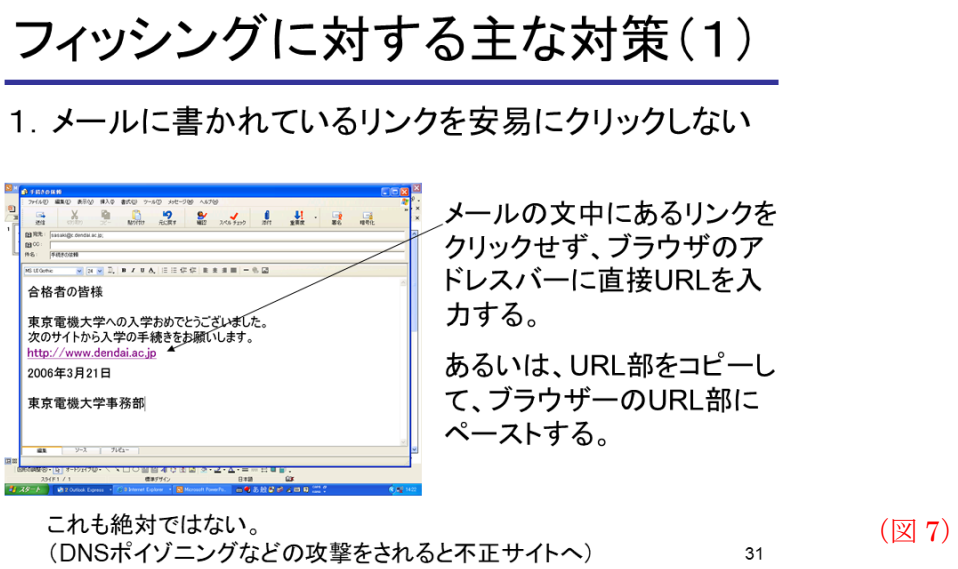


（図 6）

ただ、“nisenodendai.ac.jp”などといったドメイン名を登録するのは結構大変なので、実際には、IP アドレスという数字を羅列したネットワーク上のアドレスを入れているケースが多いかと思います。いずれにしても、フィッシングメールは、意外と簡単に作れます。

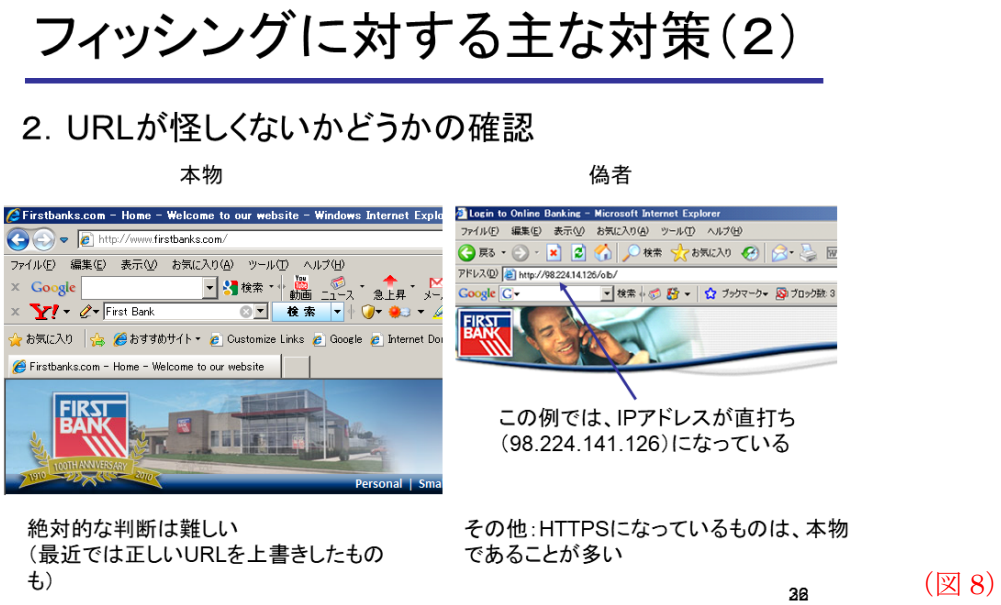
フィッシングに対する主な対策

フィッシングメールにはいろいろな対策を、組み合わせてやっていくことが必要です。まず、メールに書かれている URL は直接クリックせず、URL 部分をコピーして、ブラウザのアドレスバーにペーストして、移動します（図 7）。これだけで、メールの表示とは別のところに飛ばされる可能性はかなり下がると思います。ただ、これも絶対ではなく、「**DNS ポイズニング**」というかなり高度な攻撃をやられると、やはり危険なページに飛んでいきます。



（図 7）

飛んでいった先のデザインなどでは危険性を判断できません。ただ、偽ページではアドレスが社名などのドメイン名でなく、数字が連続した IP アドレスのことが多いです（図 8）。



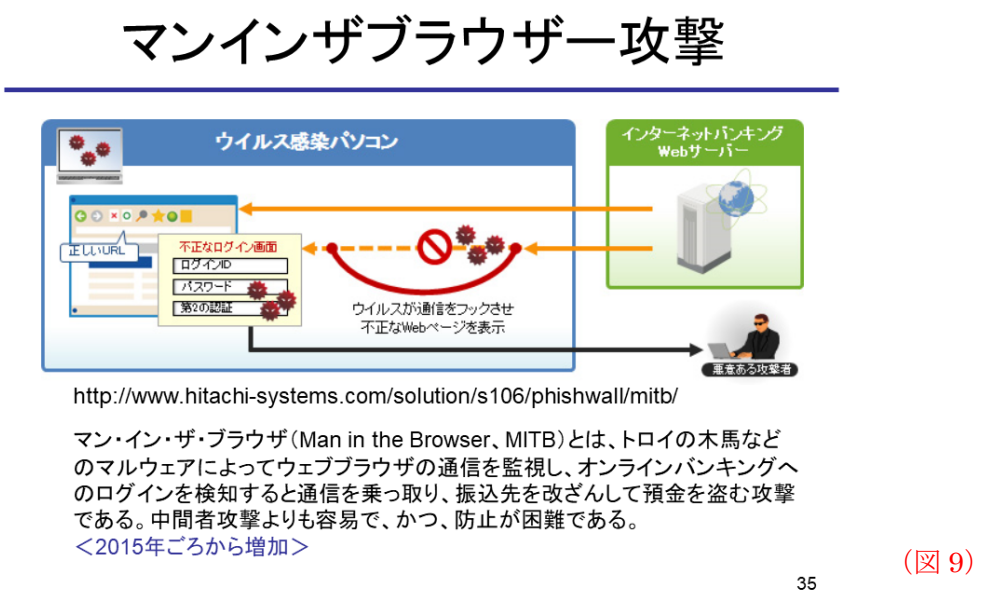
（図 8）

また、フィッシング対策機能を備えたセキュリティソフトも結構出てきています。今は保護率が 90%を超えるものも増えているようですが、本物のサイトに「危険」というアラートが上がることは少なくありません。そのため、アラートに慣れて、これは大丈夫だろうと思って入ると実はフィッシングサイトだった、ということもあるので、難しいところです。

そのため、どれか一つに頼るのではなく、今言ったような三つのやり方を組み合わせてやっていくのがいいと思います。

防止が困難なマン・イン・ザ・ブラウザ攻撃

それから、最近はもっと巧妙になっていて、偽サイトに行かなくても攻撃されてしまう例もあります。例えば、インターネットバンキング用の端末にウイルスを送り込む「**マン・イン・ザ・ブラウザ**」攻撃です。この攻撃では、送り込んだウイルスが、インターネットバンキングの利用者にはインターネットバンキングサーバーにつながっているように見せるとともに、インターネットバンキングサーバーには正規の利用者がアクセスしているように見せて、実はその間に入ったウイルスが攻撃をします（図 9）。



（図 9）

例えば、ユーザーがインターネットバンキングサーバーに対して、A 銀行に 100 万円送金という依頼をする。するとウイルスが、B 銀行に 1,000 万円送金と変換して送るわけです。インターネットバンキングサーバー側は、それを正規ユーザーの依頼と信じて、B 銀行に 1,000 万円送金し、ユーザーに取引内容を返します。これをユーザーが見ると不正がバレるので、ウイルスは、A 銀行に 100 万円送金済み、と書き換えてユーザーに見せるのです。

こういった攻撃は 3～4 年前にずいぶん流行り、一時期減っていったのですが、最近、また増えてきているようです。

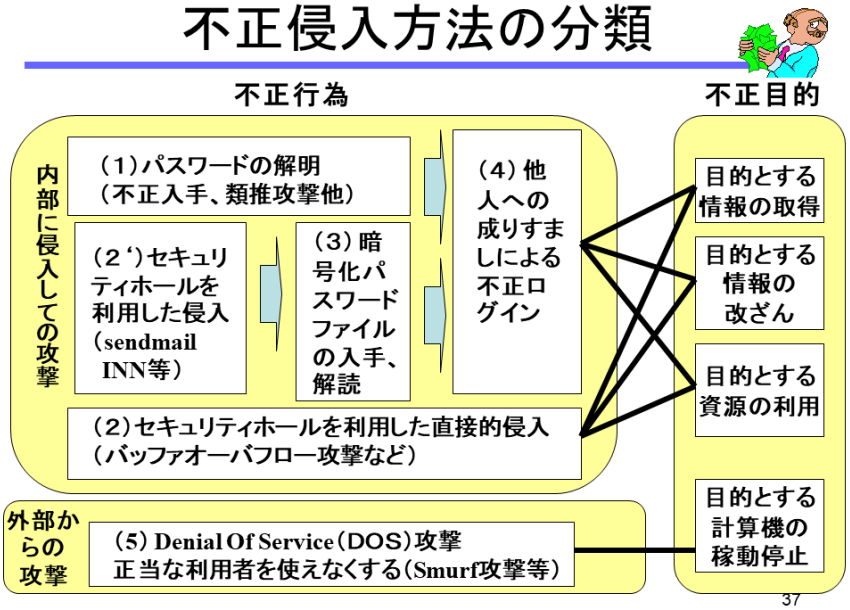
このように、サイバー攻撃にはさまざまな種類があります。ドコモ口座の不正引き出しの

ような問題はこれとは少し違いますけれども、お金が絡むところにはいろいろな知恵を出す人がいるため、十分注意する必要があります。

攻撃者と攻撃方法の分類ということに戻ると、ここまで述べたようなウイルスを使ったもの以外に、「**直接的攻撃**」があります。これは、インターネット経由で相手のサーバーとか PC の中に入っていって行う攻撃です。攻撃のやり方を、ざっくりまとめてみます。

相手の内部に侵入しての攻撃として、一番分かりやすい例は、本人確認のためのパスワードを不正に入手したり、類推したりすることで、他人になりすまして不正にログインし、目的とする情報を取ったり、情報を改ざんしたりするものです。

また最近では、セキュリティホールを突いた攻撃が増えてきており、OS やアプリケーションソフトの脆弱性を突いて、そこに対して外から悪さを仕掛けることによって、他人になりすましたり、あるいは相手のコンピューターを自由自在に動かせるようにしたりするケースもあります。外部からの攻撃ということでは、先ほども述べた、パケットをどんどん送りつけて他からアクセスできなくする「**ＤｏＳ攻撃**」というような攻撃もあります(図 10)。



(図 10)

サイバー攻撃に対するリスクマネジメント

セキュリティを対策フェーズで見ていくと、「**平常時**」には、どういったコンピューターがあるかを把握する「**資産管理**」や「**リスクアセスメント**」を行う「**特定**」というフェーズがあります。同じく平常時の「**防御**」というフェーズでは、「**アクセス制御**」や暗号化などの「**データセキュリティ**」が含まれます。「**平常時**」と「**非常時**」の境目となる「**検知**」フェーズは、異常検知するための「**モニタリング**」をして、異常があったらそれをアラートとして上げるなどの「**検知プロセス**」が必要です。それから、異常が発生した非常時には、「**対応**」と「**復旧**」というフェーズがあり、それぞれ事前の「**計画**」が必要になるとともに、事後には「**分析**」や「**改善**」等を進めなければなりません。

ここまでを踏まえて、どういう対策をしていくかを明確にしようとすると、リスクを考慮したアプローチが必要になってきます。工学分野の確率論的リスク評価では、通常、次のように定義します。

リスク=損害の大きさ×損害の発生確率

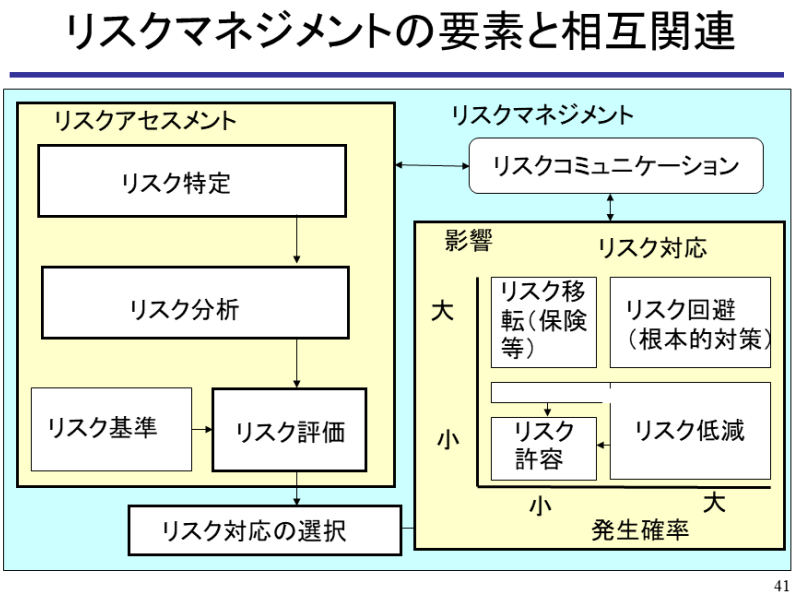
これはある意味合理的で、例えば、発生確率が一緒ならば、損害が大きいほうが困るのでリスクが大きくなるのは当たり前ですし、損害の大きさが同じであれば、発生確率が大きいほうが困るためにリスクが大きくなる、ということです。

それから、IT の分野では、以下のような別の定義もあります。

リスク=情報価値×脅威×脆弱性

ただこれは、「損害の大きさ」がだいたい「情報価値」に相当し、「損害の発生確率」は「脅威×脆弱性」と置き換えられますので、基本的には同じことを言っているのだと思います。

そうしたリスクにどう対応するのかということでは、全体としては、「**リスクマネジメント**」をきちんとやっておくことが必要になります（図 11）。リスクマネジメントの中心になるのが、「**リスクアセスメント**」です。リスクアセスメントというのは、「**リスクの特定**」を行ってどういうリスクがあるのかを明確にし、「**リスク分析**」をしてリスクの大きさを定量的、あるいは準定量的に把握し、「**リスク基準**」と比べて「**リスク評価**」をすることです。このリスクアセスメントの結果によって、「**リスク対応**」を選択していくことになります。



（図 11）

リスク対応については、発生確率も影響も小さいリスク事象については、リスクを「**許容**」します。

それから、「**リスク低減**」という対応があり、これは、発生確率や影響が少し大きい場合については、ある程度のリスク対策をすることで許容範囲までリスクを下げるものです。

また、発生確率は小さいけれども、起こると影響が大きいリスクに対しては、「**リスク移**

転」といって、対策は採らずに保険などに加入し、何か起こったら保険で対応します。

もう一つ、「**リスク回避**」という対応もあります。これは抜本的対策、根本的対策ともいわれていますが、現状ではリスクから逃げ切れない場合に、業務形態などを変えて対応しようというものです。例えばウェブを使い、個人の顧客に課金する業務形態はよくあります。しかし個人情報を持つと、もともとの取引は少額でも、情報漏えい被害が出るとそれを超えた損害賠償を要求されるという大きなリスクを抱えてしまいます。そのようなケースでは、個人情報を持たないようにするために少額の課金をあきらめ、広告等で収入を得ようといった形で、業務形態を変えていくのも選択肢の一つです。

こうしたリスクアセスメントとリスク対応においては、いろいろな部署間のリスクコミュニケーションが必要になるため、以上のように選択肢を整理しておくと、自分たちが今どうすればいいのか決定しやすいと思います。

アクセス制御技術の概要

サイバーリスクを低減する上で「アクセス制御」が広く使われています。これは要するに、重要な情報が入っているところに関係者以外は近づけないようにすることです。

アクセス制御には「**ユーザー認証**」技術と、その人が許された以上の侵入をしようしたらブロックする「**狭義のアクセス制御技術**」という機能があります。ユーザー認証、本人確認のための技術としては、「本人の知識」を利用するパスワード認証、「本人の持ち物」を利用する ID カード認証、「本人の身体的特徴」を利用する指紋認証などがあります。

一時期、静脈認証が話題になった時に、身体的特徴を利用するものがいいといわれましたが、必ずしもそうではなく、それぞれに長所、欠点があります（図 12）。

表　ユーザ認証方式の比較

No	認証の根拠	例	長所	短所
1	知識	暗証番号 パスワード	実装が容易	忘れる危険性 類推が可能
2	持ち物	磁気カード ICカード	偽造が困難	なくする可能性 特別な読取装置が必要
3	身体的特徴（バイオメトリックス）	指紋 声紋 虹彩 網膜パターン	他人の偽造が困難 確実性が高い	プライバシー問題 変更が不可能 特別な装置が必要

44

（図 12）

身体的特徴を利用するものは「**バイオメトリクス**」ともいいますが、これの問題点は、他人が偽造した場合に変更ができないという点です。例えばパスワードなら変えることができますが、自分の指紋を変えることはできません。

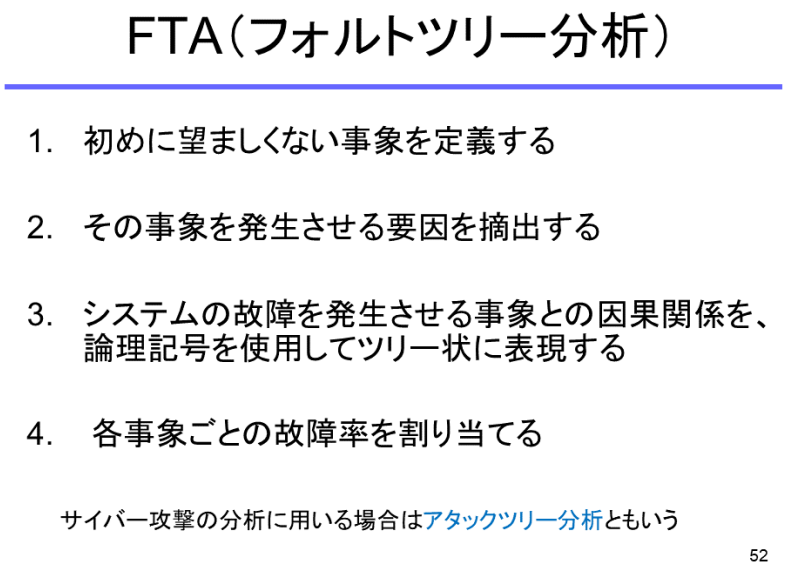
かつて、身体的特徴を利用する認証も万全ではないことを示すために、学生に実験をさせたことがあります。2009 年当時、NTT ドコモの生体認証機能付き携帯電話が 19 機種ありました。内訳は顔認証が 12、指紋認証が 6、音声認証が 1 でした。それぞれ 1 台ずつ用意してさまざまな条件で認証するかどうか試してみました。普通にやると、指紋認証、顔認証、音声認証とも本人を本人として認めます。

ところが、例えば、人工指では指紋認証されるのでしょうか。また、カメラで顔認証するタイプの携帯に、持ち主本人の顔写真をかざしてみたらどうでしょう。それから、同じ携帯を 2 台用意し、1 台の画面に持ち主の顔写真を表示し、それをもう 1 台のカメラで写すと認証されるのか。音声については、テープレコーダーの録音で試してみました。

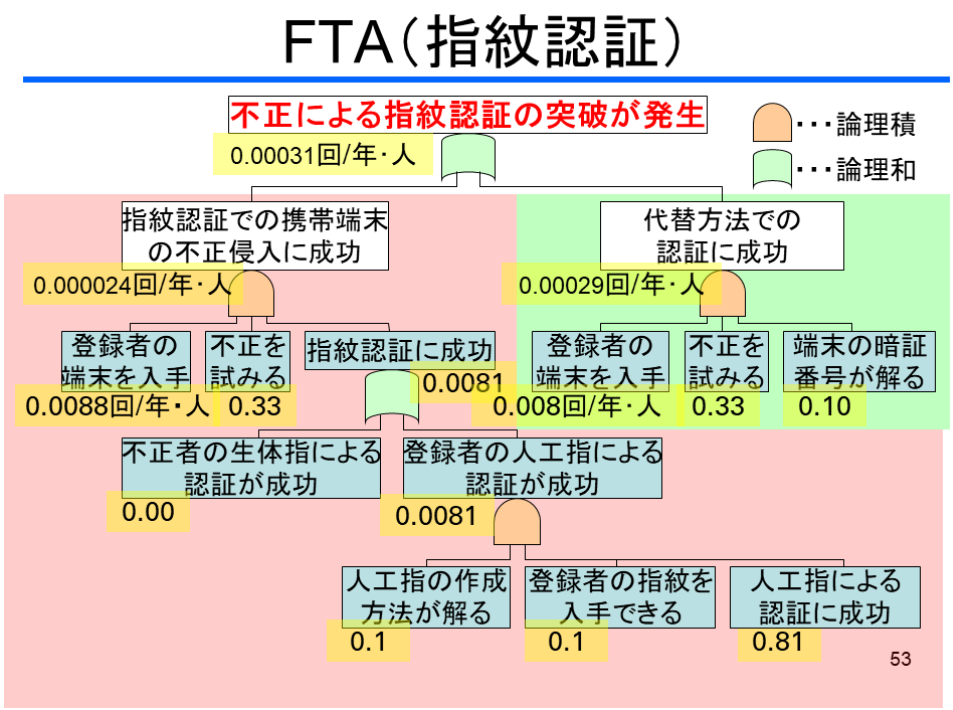
結論としては、いずれも 80%を超える確率で本人と認証されます。特に、携帯に表示させた顔写真で認証させたケースでは、認証成功率は 97%に達しました。これらのことから、いわゆる生体認証も、過度に信頼するのは適当ではないと思います。

生体認証技術の限界と危険性

ただし、これは自分のスマホや携帯を、誰かに渡したり盗られたりした時の問題ですから、現実的にはどのぐらい起こる可能性があるのか、フォルトツリー分析をしてみました（図 13、図 14）。



（図 13）



（図 14）

細かい説明は省きますけれども、例えば、人工指による不正な認証が成功する確率は、先ほどの実験結果等の数字を入れて計算すると、1 人当たりで 3,000 年に 1 回ぐらいとなります。その意味では、それ自体はあまり心配することはないという結論になりますが、日本は 1 億人の人口がありますので、やはりリスクや対策をよく考えておく必要があるでしょう。

もう一つ、先ほどの実験は 2009 年の古いデータですけれど、2020 年ではどうでしょうか。実は現在でも同様なリスクは存在し、さらに 4K テレビ、8K テレビなどのデータを使えば、3D プリンターなどで人工指を作ることは、そう難しくはありません。

では、「**静脈認証**」ではどうでしょう。静脈認証は指紋などより安全性が高いといわれていますが、過信は禁物です。最近の研究で、市販のデジタルカメラで撮った指の画像を使ったものがあります。この画像の元データには赤外線領域も記録されています。それを特殊な方法で加工すると、赤外線領域の画像から、指の静脈の形が読み取れることが確認されています。こうした研究結果はメーカーも把握しており、その対策も採られているので多くの場合は問題ないと思いますが、いずれにしても過信は禁物です。

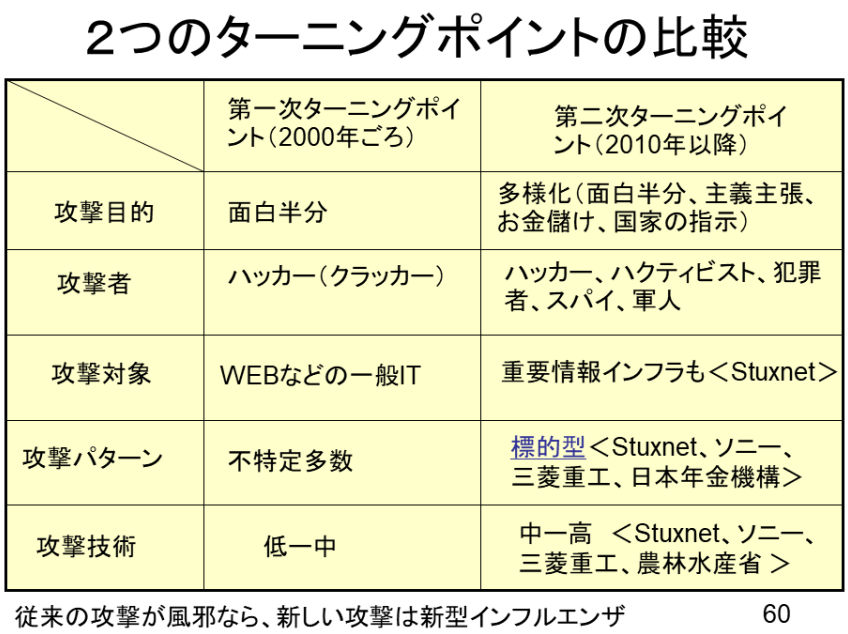
そのため最近は、指紋認証とパスワードとを組み合わせるなどの **2 要素認証**をやるべきであると一般的にいわれています。

3. サイバー攻撃の動向

次に、サイバー攻撃の動向についてお話しします。

サイバー攻撃について、私は、2 つのターニングポイントがあったと考えています。1 番目が 2000 年頃、2 番目が 2010 年頃です。2000 年には、科学技術庁のホームページの改ざん事件が起こり、大騒ぎになりました。われわれセキュリティの専門家は、こういうことは

起こりうると思っていたのですけれども、一般の人には非常にショックだったらしく、この頃からセキュリティ対策が注目されてきております（図 15）。



（図 15）

2010 年には、**Stuxnet**(スタックスネット)というものが出現しています。これは、「ネット」という名前ですが、実はウイルスです。通常状態では Windows PC から Windows PC に感染するだけですが、核燃料製造用の遠心分離機を動かすソフトに行き着くと暴れ出し、遠心分離機の回転数を異常にします。これによって、当時イランにあったといわれる遠心分離機は 5,000 台とも 3,000 台ともいわれていますが、そのうちの 1,000 台が壊れてしまい、イランの核開発が 1 年以上遅れたのではないかといわれています。

これは今では、アメリカとイスラエルが組んで、やった攻撃であるというのが定評になっていますが、こういう非常に高度な攻撃も行われているわけです。日本の場合はそれほどでもありませんが、三菱重工や日本年金機構に対するものは同じ標的型攻撃となっています。

従来の攻撃は面白半分中心でしたが、お金もうけや国家の指示などの明確な目的を持った攻撃が増えています。攻撃者も、ハッカーとかクラッカーに加え、犯罪者、スパイ、軍などが参入してきました。それから攻撃は、ウェブなどの一般的なメディアが対象だったものから、重要インフラなども攻撃の対象になるようになり、さらに攻撃パターンが、不特定多数から特定少数、標的型と呼ばれるものが増えてきて、攻撃も非常に高度になっています。

日本年金機構への標的型攻撃

2015 年の 5 月、ウイルス付きの添付ファイルをメールで送り込む方法で日本年金機構への攻撃が行われました。送り込まれた 124 通のうち、開けてしまった人はわずか 4 人です。従来は、それを開けた PC の持ち主だけが被害に遭ったのですが、最近の攻撃は、その PC の利用環境を調べて、外部の C&C サーバー（指令サーバーともいいます）にデータを強制

的に送るようになっています。これは、攻撃者が自由に操ることができるサーバーです。

そして C&C サーバーから感染した PC に、その環境に最適な攻撃ツールをダウンロードさせたり、あるいは、バックドアを仕掛けて後から何度でも入れるようにしておいて、他の PC やサーバーに侵入させて情報を取り出したりといったようなことをやっています。

そうした経緯でデータが外に出ていくわけですが、直接攻撃者のところに行くのではなく、攻撃者が自由に操作できるようにしたサーバーのところに送らせておいて、後から取りに行く。しかも、取りに行く時は匿名通信路を使うことで、本当の攻撃者は追跡できない仕組みになっていたため、いまだに犯人は捕まっていないようです。

こういうことが起こると、日本は遅れているという非難が沸き起こるのですが、実はそうではなくて、ちょうど同じ頃、アメリカの連邦政府の人事管理局でも個人情報が 2,210 万件も取り出されたという事件がありました。それだけ攻撃は簡単で、守備は難しいということです。

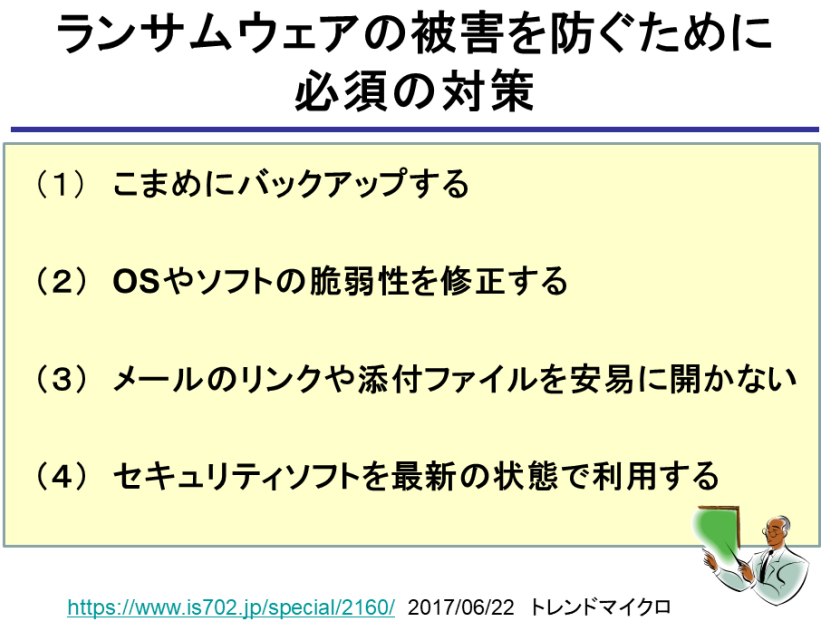
今後予想される被害の大型化と多様化

今後、どういう形で攻撃が進展していくかということを考えてみました。一つは「**被害の大型化**」という問題です。3 年ほど前に、コインチェックという仮想通貨の取引所から、580 億円相当の仮想通貨が不正に取り出されるという事件がありました。これはいまだに戻ってきていないのですが、こういう仮想通貨絡みでの犯罪は今後も続くし、それに伴って被害額は非常に大きくなっていくだろうと類推することができます。

それから 2 番目が、「**被害形態の多様化**」です。従来の攻撃が「機密性の喪失」という、個人情報等を盗まれるといったことであったのに対して、今後、「**完全性や可用性の喪失**」、つまり情報の内容を変えられたり、あるいはコンピューターを使えなくしたりするような攻撃が増えてくると考えられます。この典型的なものが、先ほど申し上げたランサムウエアです。これは、データの暗号化、つまりデータを書き換えるという意味では完全性の喪失ですし、データを使えなくするという意味では可用性の喪失となり、従来の情報漏えいのような形の、機密性の喪失とは違った形の攻撃となります。

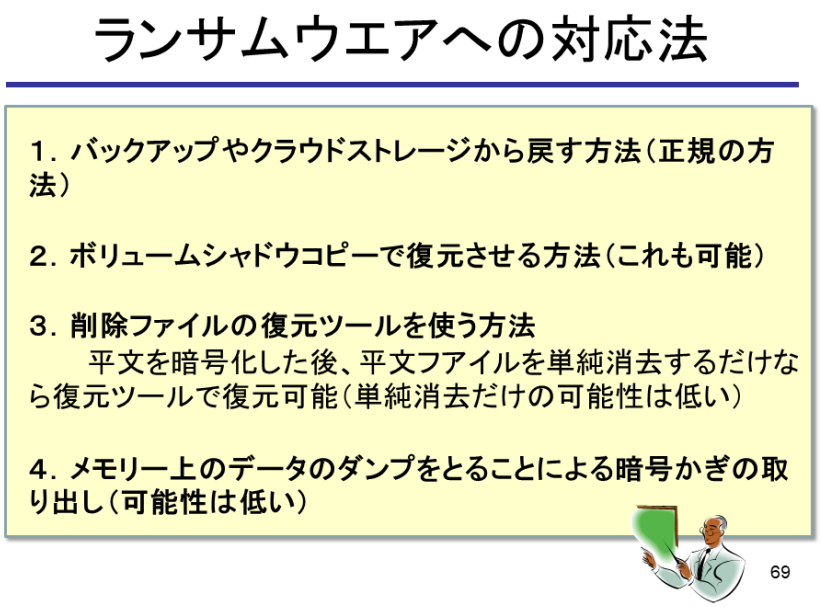
ランサムウエアへの対策と暗号化への対応

ランサムウエアへの対策は、「**小まめにバックアップを取る**」ということに尽きます。それから、防御策は、「**OS やソフトの脆弱性を修正**」しておくことです。この二つはぜひやっていただきたいと思います。また、先ほどの、「**メールのリンクや添付ファイルを安易に開かない**」、「**セキュリティソフトを最新の状態で利用する**」ことも重要になってきます（図 16）。



（図 16）

もし、ランサムウエアに情報を暗号化されてしまった場合は、バックアップやクラウドストレージから戻すのが正規のやり方です。ボリュームシャドウコピーを使って復元する方法もあります。実は OS の中には、プログラム等が変更された履歴が残っているため、それをうまく使うと復元できる場合があります。最新のデータは感染しているので使えませんが、少し古いコピーを使えば感染する少し前の状態を復元できる可能性があります（図 17）。



（図 17）

それから、削除ファイルの復元ツールを使うのも一つの方法です。ただ、元の平文データを単純消去するようなランサムウエアは、最近は減ってきています。

また、メモリー上のデータのダンプを取ることで、暗号鍵を取り出せることもあります。

ただこれも、最近は攻撃側も賢くなっており、かなり難しいようです。

日本の IPA などもサポートメンバーとなっている国際的な組織「The No More Ransom プロジェクト」では、ランサムウエアの調査研究を行うとともに、暗号化されたデータを復号するツールの提供なども行っています。

それから、ある業者に頼むと暗号化されたデータを復元できる場合があるという噂があります。この業者は、裏で脅迫者と交渉し、お金を払って復号ツールを手に入れ、被害に遭った会社には身代金にさらに上乗せした金額を請求した上で、脅迫者から手に入れたことを隠して、その復号ツールでデータを復元するようです。

最近のランサムウエアによる攻撃はさらにいやらしくなっており、まず不正な方法でデータの平文を詐取し、それから元のデータを暗号化してきます。そうしておいて、お金を払わないと、平文の部分を少しずつ外部に公開していくのです（図 18）。このケースでは請求金額も億の単位になってきているといわれています。

（図 18）

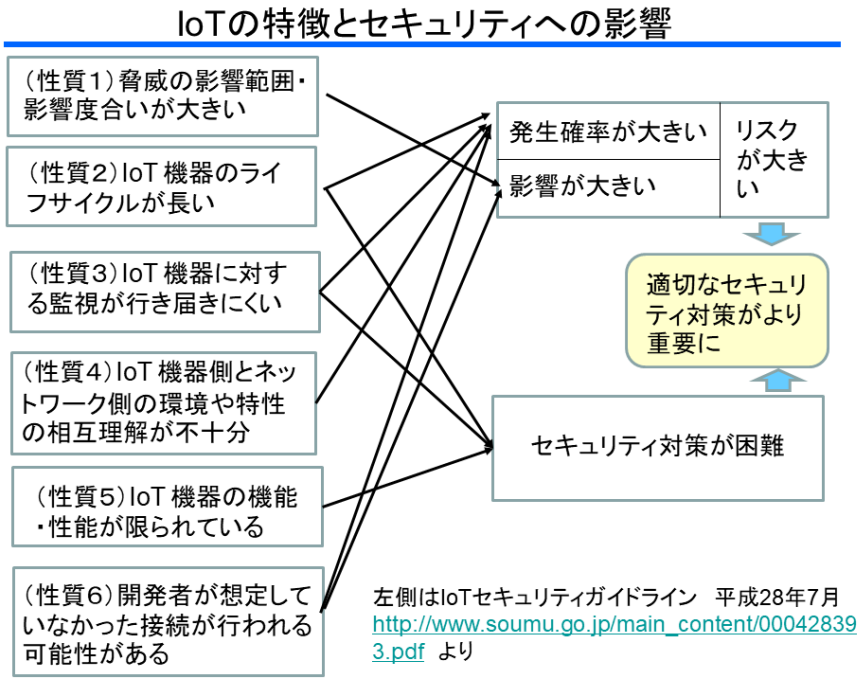
ランサムウエアによる攻撃に対して、身代金を払うか払わないかについては、いろいろな議論があります。しかし、「**身代金を払ってもサイバー犯罪者が約束を守る保証はどこにもない**」こと、「**身代金の支払いはサイバー犯罪者にさらなる攻撃のための資金を与えることになる**」こと、それから「**身代金を支払ったことが理由で、別の犯罪や脅迫に巻き込まれる危険性もある**」ことなどから、身代金を払うのはやめましょうというのが基本です。

IoT の特徴とセキュリティへの影響

それから、「攻撃対象の多様化」として、PC などから IoT などへ対象が拡大していくことも予想されます。今後、IoT (Internet of Things) で、家や、いろいろなものがインターネットにつながっていき、それがセキュリティ上のいろいろなリスクになり得るのです。

総務省と経済産業省が作成した「**IoT セキュリティガイドライン**」では、IoT 機器に特有

の性質として、「脅威の影響範囲・影響度合いが大きいこと」など 6 つを挙げています（図 19）。それをセキュリティという面から整理すると、いずれもリスクの増大や、セキュリティ対策の困難化につながっており、適切なセキュリティ対策がより重要になります。



（図 19）

しかも、従来の PC などに対する攻撃では被害は「セキュリティの喪失」だけでしたが、IoT の場合は医療事故や交通事故、事故による環境影響や健康影響、さらに企業の業務停止など、「セーフティーの喪失」も起こりうるため、対策が非常に重要になってきています。

自動車もインターネットにつながりつつあり、アメリカのセキュリティカンファレンス Black Hat USA 2015 では、数マイル離れた自宅から携帯電話のネットワークを経由して、自動車のハンドルを操作し、ブレーキを無効化することに成功したことが発表されました（図 20）。

（図 20）

またアメリカの高速道路では、インターネット接続の交通標識が「GODZILLA ATTACK!」「TURN BACK」ゴジラが攻撃、引き返せ、と書き換えられてしまいました。もし災害など本当に起こりうる内容だったら、行く車と帰る車で大事故につながりかねないわけです。

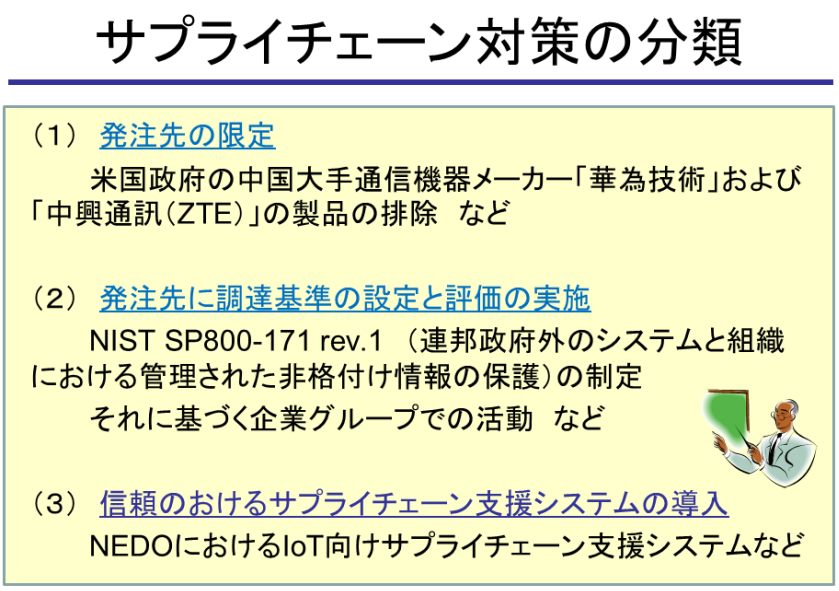
それから、ウェブカメラだとか、家庭用ルーターなどの IoT 機器が攻撃の踏み台になることも心配されています。実際、3 年ぐらい前に Mirai というマルウエアによって多数のウェブカメラがボット化され、それらのウェブカメラから標的サーバーへのパケット攻撃により複数のウェブサイトがダウンしたといわれています。

情報機器のサプライチェーンにおける脅威

さらに、IoT 機器やシステムの、サプライチェーンにおける脅威も心配されています。実際にアメリカで、海外から調達した通信機器（ファーウェイ製といわれています）が深夜に勝手に動き出して、本国にデータを送信したという疑惑が持たれています。

情報システムのサプライチェーンでは、例えば部品ベンダーや製品ベンダーがハードを作り、ソフトウエアベンダーだとかがシステムを構築していく。そういう中で、例えば部品ベンダーになりすまして、ハードウエアトロイといって、悪いことをする回路を勝手に入れ込まれる心配や、脆弱性のあるソフトだとか不正機能を持つソフトを組み込まれる危険性もあります。さらには、神奈川県では廃棄業者による情報の持ち出し事件がありました。

こうした状況に対応し、サプライチェーン対策が重視されるようになった結果、公的機関や大手企業は、情報システムの部品、ハード、ソフトを購入するに当たって、いろいろな条件を付けるケースが出てきています（図 21）。一つは「**発注先の限定**」で、例えばアメリカ政府は、ファーウェイの製品は購入しない対応を始めています。



（図 21）

また、発注先に、「**調達基準の設定と評価**」を実施して、あるレベル以上の対策をしてい

るところからしか買わないといったような動きも出てきています。ただ、かなり厳しい基準を設けているところもあり、中小企業では対応が難しい場合も出てくるかもしれません。

そのため、「**信頼のおけるサプライチェーン支援システムの導入**」が必要となりますが、国家間の対立がある中で、一番の課題であるハードウエアトロイを見つけられるのか。サプライチェーン対策によるコスト上昇を誰が負担するのか、エコシステムは存在するのか、こういう難しい問題が出てきますが、今はまだ、試行錯誤しているという状況です。

攻撃者の多様化・高度化

それから今後、「攻撃者の多様化・高度化」も予想されます。攻撃者には、団体、テロリストもありますし、犯罪者も国に準ずる組織もあるという状況が生まれています。2018 年のサイバー攻撃の目的は、金銭目的が 76%、スパイ活動が 20%弱でした。2020 年度では、金銭目的が 86%ぐらいに増加し、中小企業は関係ないとはならなくなってきています。サイバー攻撃は、麻薬売買などと並んで割の良い犯罪だといわれています。これは設備投資が要らず、捕まりにくいためで、今、犯罪組織がどんどん参入してきているようです。

『フューチャー・クライム -サイバー犯罪からの完全防衛マニュアル-』(マーク・グッドマン著、松浦俊輔訳)には、先進的サイバー犯罪組織には最高経営責任者、最高情報責任者の他に、研究開発部門や、コンピューター開発やウイルスの品質保証部門もあると書いてありました。なぜかというと、今は攻撃者が分化していて、攻撃依頼者、攻撃実行者、攻撃ツールの提供者、コーディネーターと分業になっているからです。そのため攻撃ツール提供者は、犯罪者に買ってもらうために、信用第一で色々な対応をするようになっているのです。

また、攻撃も国際的になってきて、国際的指名手配になるケースが増えてきています。

さらに怖い話としては、イスラエル軍が、イスラム過激派のハマスによるサイバー攻撃を阻止するために、そのアジトと目されるガザ地区の建物を空爆したという新聞記事が出ていました。サイバー攻撃を防ぐための物理的攻撃というのが、現実的に起こりつつある現在、日本はどうしていくのかという議論をしっかりしておかないと、物理的戦争のリスクにつながりかねないという問題も生まれつつあります。

4. 中小企業のためのセキュリティガイド

最後になりましたが、中小企業のためのセキュリティガイドという話をしていこうと思います。経営者向けには、私が座長を務め、経済産業省と IPA が協力して作った「**サイバーセキュリティ経営ガイドライン**」があります。それからもう一つ、中小企業向けには「**中小企業の情報セキュリティ対策ガイドライン第 3 版**」が、やはり IPA から出ています（図 22）。この第 3 版はなかなかよくできているので、今日はこれを中心に紹介させていただきます。

中小企業の情報セキュリティ対策ガイドライン第3版の概要（1）

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

（図 22）

https://www.ipa.go.jp/files/000055520.pdf

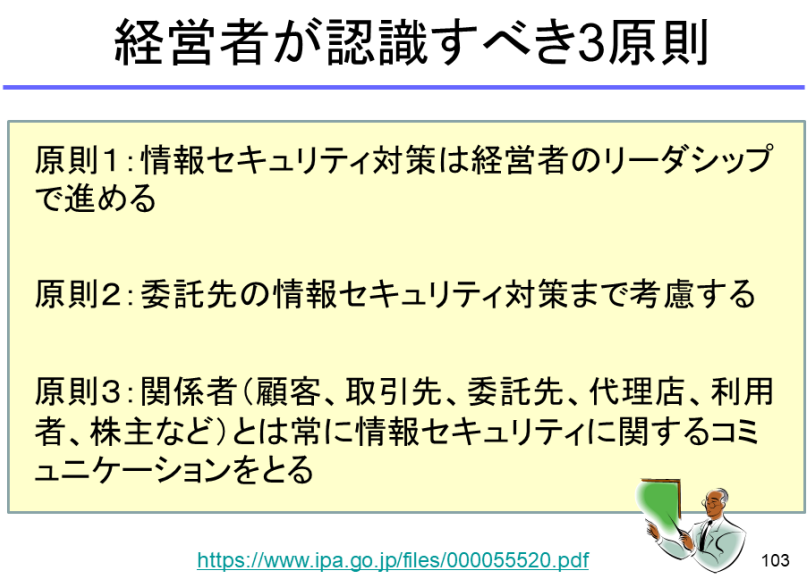
「中小企業の情報セキュリティガイドライン第３版」は、本編の第１部が経営者編、第２部が実践編で、付録がたくさん付いています。経営者編は、経営者が何をしなければならないのか、実践編では、具体的に組織として何をやらなければならないかを解説したものです。

まず、「経営者の皆様へ」では、「情報セキュリティ対策は、経営に大きな影響を与えます!」と書かれています。影響の一つは「金銭的損失」です。ウイルス感染で、業務が停止して数千万円の損失を出した例や、個人情報の漏えいで損害賠償などが生じる場合もあります。次に「顧客の喪失」。顧客情報の流出などで顧客が離れていきます。そして業務システム事故によるインターネット遮断などによって「業務の停滞」が起きたり、従業員のみを罰して管理者が責任を取らなかったりすれば、働く意欲の低下など「従業員への影響」も心配されます。

「経営者の皆様へ」の２番目では、「対策の不備により経営者が法的・道義的責任を問われます!」と、少し脅しが入っています。「法的責任」としては、「個人情報保護法」「マイナンバー法」「不正競争防止法」「金融商品取引法」「民法」などがあります。また、「関係者や社会に対する責任」としては、会社役員が会社法上の責任を問われる可能性があり、最近は株主代表訴訟などでかなり多額の損害賠償を請求される場合も出てきています。

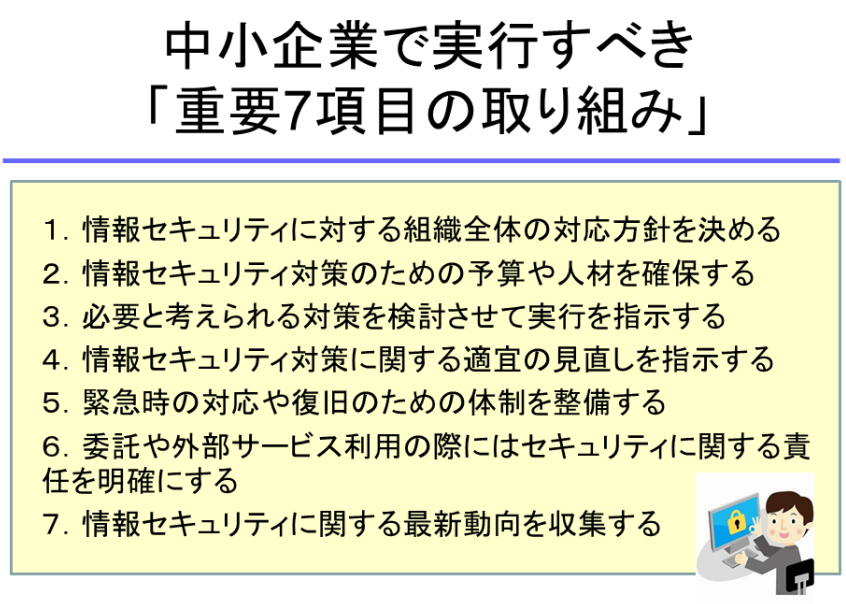
これらを受けてガイドラインでは、「**経営者が認識すべき『3 原則』**」が示されています（図 23）。**原則 1** は、「情報セキュリティ対策は経営者のリーダーシップで進める」。要するに、経営者の責任です、他人任せでは駄目ですということです。**原則 2** は、「委託先の情報セキュリティ対策まで考慮する」で、サプライチェーン全体で考えていきましょうと

ことです。**原則 3** は、「関係者とは常に情報セキュリティに関するコミュニケーションをとる」こと。顧客、取引先、委託先、代理店、利用者、株主などの関係者と、常に情報セキュリティに関するコミュニケーションをとる必要があります。この三つの原則は、非常に大事なことですので、ぜひ頭に入れておいていただければと思います。



（図 23）

次に示されているのが、「**実行すべき『重要 7 項目の取組』**」です（図 24）。まず「情報セキュリティに対する組織全体の対応方針を決める」。次に、「情報セキュリティ対策のための予算や人材を確保する」。これは大事なことです。続いて、「必要と考えられる対策を検討させて実行を指示する」こと。4 番目は、「情報セキュリティ対策に関する適宜の見直しを指示する」ことで、サイバー攻撃というのは日々変わりますから、変化への対応が必要です。

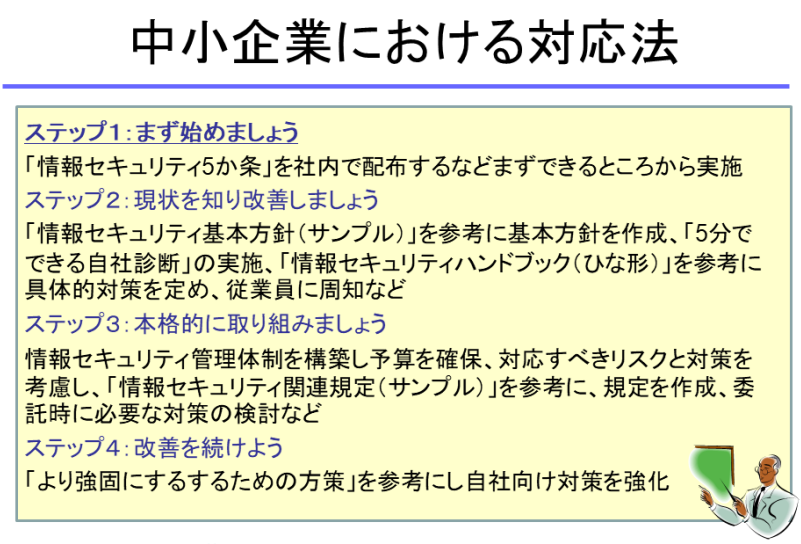


（図 24）

それから、「緊急時の対応や復旧のための体制を整備する」ことも必要ですし、「委託や外部サービス利用の際にはセキュリティに関する責任を明確にする」必要があります。最後は、「情報セキュリティに関する最新動向を収集する」ことが必要です。

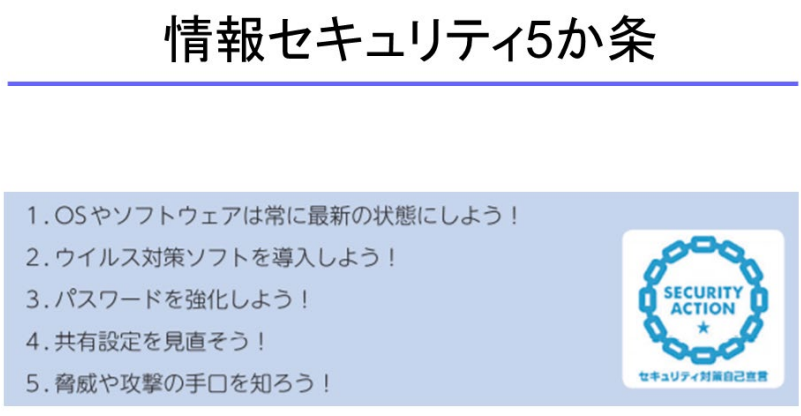
まず「情報セキュリティ 5 か条」を配布する

次の「実践編」は 4 つのステップに分けられており、できるところから徐々にやっていきましょうという組み立てになっているのは、このガイドラインのいいところだと思います（図 25）。



（図 25）

ステップ 1 では、まず「**情報セキュリティ 5 か条**」を社内で配布するなどで、まずできるとこからやってきましょうということが挙げられています（図 26）。



（図 26）

「情報セキュリティ 5 か条」とは、「OS やソフトウエアは常に最新の状態にしよう!」などの五つで、これをプリントして配りましょうというわけです。例えば、社内 LAN の中で、他の PC とお互いファイル共用できるような機能を持たないようにするとか、ここでは触れていませんが、一つの管理サーバー端末を共有の ID とパスワードでみんな利用できるような設定はリスクが高いのでやめましょうということです。

2 番目のステップは、現状を知り、改善しましょうということで、「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成し、「5 分でできる!情報セキュリティ自社診断」を実施して、「情報セキュリティハンドブック(ひな形)」を参考に具体的対策を定め、従業員に周知しましょうということが書かれています。

付録の「情報セキュリティ基本方針」のサンプルを参考にすれば、それほど専門知識がなくても最低限のものはできますから、ぜひ作成したほうがいいと思います。

「**情報セキュリティ自社診断**」は、25 項目の設問に答えていくことで、自社の情報セキュリティの強みと弱みをチェックできるようになっています（図 27~図 29）。例えば「パソコンやスマホなど情報機器の OS やソフトウエアは常に最新の状態にしていますか?」という問いに対し、実施しているなら 4 点、一部実施していれば 2 点で、実施していなければ 0 点、分からないならマイナス 1 点という形でチェックしていくと、自分たちはトータルとしてどのくらいのレベルなのか分かるようになっており、なかなかよくできています。

5分でできる情報セキュリティ自社診断（1）

実施状況の把握

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1

https://www.ipa.go.jp/files/000055520.pdf 109

（図 27）

5分でできる情報セキュリティ自社診断（2）

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1

https://www.ipa.go.jp/files/000055520.pdf

（図 28）

5分でできる情報セキュリティ自社診断（3）

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？	4	2	0	−1

（図 29）

https://www.ipa.go.jp/files/000055520.pdf

111

「情報セキュリティ自社診断」には「解説編」として、それぞれの項目の対策の概要も書かれているので、ここで自社に必要な対策を決定。それを「情報セキュリティハンドブック(ひな形)」に落とし込んで、従業員に配布することになります。

「情報セキュリティ関連規程」は、できるところから

ステップ 3 は、「本格的に取り組む」ですが、これをすべて実際にやるのはなかなか大変です。まずセキュリティの「管理体制の構築」をし、「IT 利活用方針と情報セキュリティの予算化」を行い、対応すべきリスクと対策を考慮し、「情報セキュリティ規程の作成」、さらに「委託時の対策」を検討するという手順ですが、前の基本方針に対して、こちらはより具体的に記述することになります。

ガイドブック付録の「情報セキュリティ関連規程(サンプル)」では、全部で 50 ページぐらいありますが、サンプルをベースにやれるところまで作ってみて、徐々に充実させていきましょうということだろうと思います。

そして規程を作ったら、日々「点検と改善」が必要となり、セキュリティをより強固にするための方針を決めて、毎年改善を続ける必要があります。

4 番目、最後のステップとして挙げられているのが「より強固にするための方策」です。ここでは、「情報収集と共有」「ウェブサイトの情報セキュリティ」「クラウドサービスの情報セキュリティ」などに対策の範囲を広げていきましょうということが書かれています。ここまでになると、大企業でもできていないところもありますけれど、ステップ 2 までは、ぜひ早くやってほしいと思っています。

サイバーセキュリティ対策は経営者の責任

IPA では「**サイバーセキュリティお助け隊**」という事業で、相談窓口を設定するとともに、対策機能を設置して、攻撃に遭った場合のサポートなどを行っています。

ここでの推奨は、UTM（Unified Threat Management）の導入です。UTM にはファイアウォールや VPN、コンピューターウイルス対策、不正検知対策、ウェブコンテンツフィルタリングという、セキュリティに必要な一通りの機能があります。意外と安価で、PC 接続は 10 台から 30 台ぐらいで月額数千円、買い切りで 20 万円ぐらいからあるようです。UTM はいろいろチェックしてくれて、何か攻撃があった時には、アラートが会社だけでなく、外部のセキュリティ専門組織である**ＳＯＣ**（Security Operation Center）にも飛んでいく。UTM の販売会社が SOC の機能も持っていることが多く、また損害保険とセットになっているものもありますから、これなら中小企業でも対応できるかと思っています。

「**サイバーセキュリティお助け隊**」サービスは、2019 年度に国の実証事業として実施され、中小企業約 1,000 社が参加しました。そして、実際にサイバー攻撃を防ぐ効果があったことが認められています。

サイバーセキュリティ対策は、中小企業も含めて経営者の責任と見なされる時代になっていることも踏まえ、ぜひ認識を新たにしていただきたいと思います。

ご清聴ありがとうございました。

（2020 年 11 月 30 日（月） YouTube ライブによる Web 配信）

RESONA りそな中小企業振興財団

The Resona Foundation
For Small And Medium Enterprise Promotion

〒141-0021
東京都品川区上大崎三丁目２番１号
Tel. 03-3444-9541　Fax. 03-3444-9546
URL: https://www.resona-fdn.or.jp
E-mail: staff@resona-fdn.or.jp