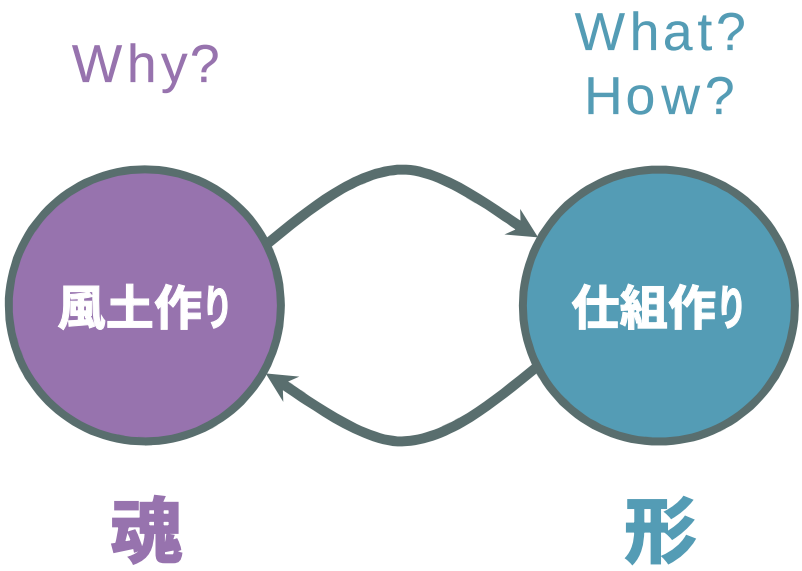
経営者の皆さん！

情報セキュリティ対策は十分ですか？



丸山　満彦

2010 年 03 月 05 日 版

経営者の皆さん！　情報セキュリティ対策は十分ですか？　2010 年 03 月 05 日版

目　次

経営者のみなさん、情報セキュリティ対策は十分ですか？

「多くの組織では、まだまだ情報セキュリティ対策が行われていない」と、専門家は指摘します。なぜ情報セキュリティ対策が十分に行えないのでしょうか。組織が情報セキュリティ対策を自発的に行うようにするためにはどうすればよいのか。なかなか難しい問題です。本書ではこの点について、今まであまり話されていなかった視点から考えていきたいと思います。

第１回　情報セキュリティのための「風土作り」と「仕組作り」

人間が「何かをする」場合、その前に「何かをしたい」という「動機」があるのが普通です。情報セキュリティの場合はどうでしょうか。情報セキュリティ対策を自発的にしたいとあなたは思うでしょうか。これから説明しますが、情報セキュリティ対策をすることは人間にとって不自然な行動なのです。「情報セキュリティ対策を自発的にする」ことは人間の普通の行動ではありません。この理解がなければ、情報セキュリティ対策を組織に浸透させることは難しいでしょう。では、どうすれば組織の中の人々が自発的に情報セキュリティ対策をしていくようになるのでしょうか。これから、「風土作り」と「仕組作り」という視点から情報セキュリティマネジメントを考えてみたいと思います。

人間として不自然な行為を行わせる難しさ　知りたいという欲望は人間の本能

人間は生物です。まず、ここから出発したいと思います。人間には五感つまり、視覚、嗅覚、聴覚、味覚、触覚があります。見る、嗅ぐ、聴く、味わう、触るですね。人間はこれらの五感をなぜ持っているのでしょうか。それは、生物として生きていくために必要だからでしょう。これら五感は、すべて「知る」ためにあるのです。環境を認識し、つまり情報を収集し、最適な行動をとれるようにするために人間には五感が存在しているのです。五感を使っていろいろな情報を知ろうとすることは人間の DNA に刷り込まれた本能なのだろうと思います。

また、高度に社会化された環境に生きる現代人は、知的好奇心、意思疎通の必要性、社交的でありたいと思うこと、信頼し信頼されたいと思うことなどの衝動からより多くの情報を収集したいと考えます。他の仲間が知っていることを知らないままでいることは気持ちが良いものではありません。企業でも、仕事が円滑に進むように情報が容易に検索でき、関係者の中で共有できるようにしようと努めていることでしょう。この傾向は、現場の職務分掌を明確にせず、現場で情報共有を進めながら仕事をする傾向の強い日本の社会構造では顕著にでてくるでしょう。このように人間が社会的活動を行うためにも人間は情報を集めて様々なことを知ろうとするのです。

つまり、情報を収集するということは、人間として、生物的な生存、社会的な生存の可能性を高めるための手段なのです。情報保護の難しさは、まさにここにあります。情報セキュリティ対策を進めるということは人間の本能に逆らうことをさせることなのです。従って、人間は自発的には情報セキュリティ対策を行おうとはしません。情報セキュリティ対策をするようにするための何か別の「しかけ」が必要となるのです。

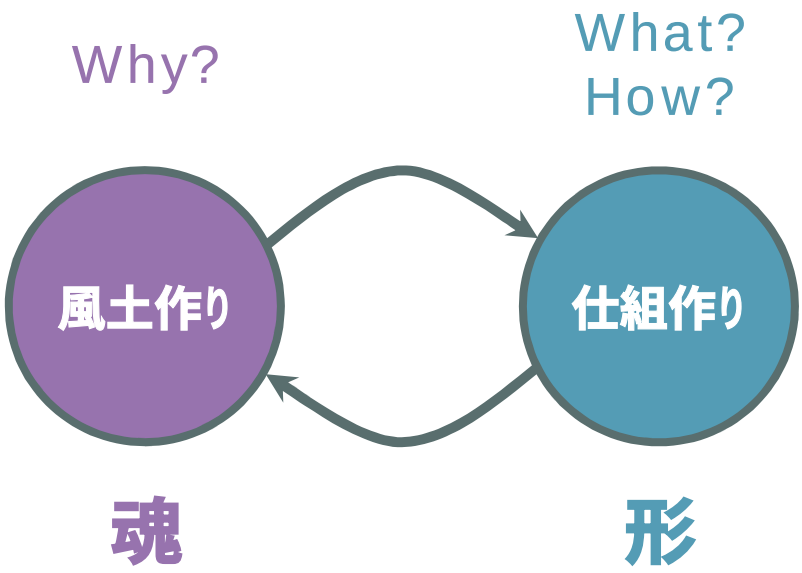
風土作りと仕組作り

組織において情報セキュリティ対策を進めるための「しかけ」の基本的な考え方は、「風土作り」と「仕組作り」です。「風土作り」とは、組織のメンバーが情報セキュリティ対策を行っており、改善の必要性がないのかと自然と考えている状態を作ることです。「仕組作り」とは、組織のメンバーが適切に情報セキュリティ対策を実施しつづける状態にすることです。

風土作りには、なによりも組織のトップの意識が重要となります。組織のトップが事業特性を考慮し、事業における情報セキュリティの重要性を組織のメンバーに伝えていくこと必要があります。これは、長期間にわたる地道な取り組みの結果生まれていくものです。情報セキュリティを行うことが「社風」として組織のメンバーに認識される必要があります。

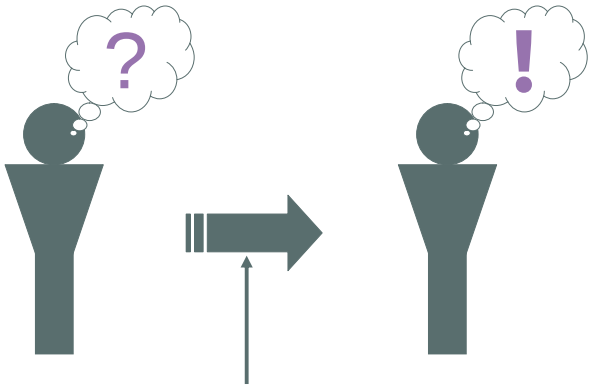
仕組作りは、マネジメント・システム作りともいえます。組織のトップが方針と手続を示し、メンバーがそれを順守していくことになります。

風土作りと仕組作りは車の両輪のようなもので、どうちらかが欠けてもいけません。仕組作りが「形を作る」ことであるとすれば、風土作りは「魂を入れる」ことに相当します。情報セキュリティ・マネジメント・システム（以下、「ＩＳＭＳ」といいます。）を構築しても形骸化するという話がよくありますが、ＩＳＭＳというのははじめから形であり、形骸化して当然なわけです。問題は、風土作りを行っていないことなのです。武術において形が重要視されるように形から入って魂を入れるという方法でも、意識を高めてから形を作るという方法でもよいのですが、いずれにせよ、両方がそろって初めて意味のある情報セキュリティ対策が実施されることになることを忘れてはいけません。



風土作りは改革

情報セキュリティ対策を実施することは、人間の自然な欲求に逆らうことですから、とりわけ「風土作り」が重要です。その際には、なぜ情報セキュリティ対策をしなければならないのかを、組織のメンバーに納得させる必要があります。そのため、情報セキュリティの必要性を理解させるための教育が必要となります。例えば、個人データが漏えいすると、漏えいされた個人に対してどのようなことが起こるのか、組織は監督官庁からどのような処分をうけるのか、裁判になればどのようなことが起こりうるのか、社会から組織はどのような制裁をうけるのか、漏えいした本人は、どのような処分をうけるのかを理解させる必要があります。情報セキュリティ対策を実施するのは人間ひとりひとりですから、それを行う意味を十分に理解させ、強い動機付けをしなければならいのです。この風土作りは、それぞれの組織がすでに持っている組織風土に加える形で行います。どんな組織であっても風土作りは改革となります。組織のメンバーに共感されるような方法で行わなければ成功はしません。人の意識を変える改革ですから、トップの力の見せ所です。一過性ではなく、しつこくしつこく動機付けを行わなければなりません。

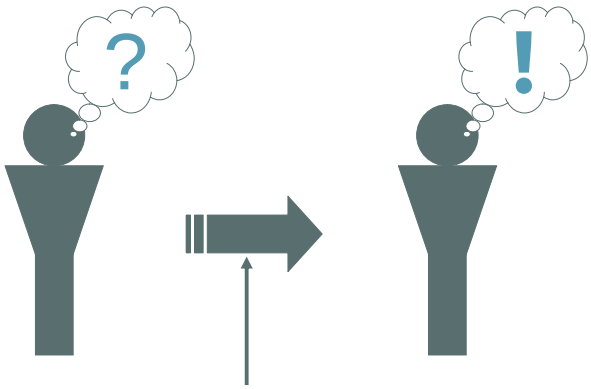


守れる仕組作りが重要

人が情報セキュリティ対策をする気になっても、具体的に何をすればよいのかがわからなければ具体的な行動に移れません。そこで、「仕組作り」が必要となります。仕組作りの第一歩はトップによる方針の伝達です。情報セキュリティポリシーといわれるものです。「なんだ、そんなものとっくにあるよ」という経営者がいるかもしれませんが、よく読み返してください。本当に情報セキュリティポリシーになっていますか。あなたの組織のメンバーに「情報セキュリティに対してどのように考え、どのような考え方で行動すべきか」という強いメッセージが含まれていますか。その組織の事業特性にあったその企業ならではのメッセージになっているでしょうか。

トップが方針を示した後は、その方針を現場で具体化するために、標準となる規定を決めます（ここまでを方針という場合もあります）。規定ができた後は、各現場で実行するために手続きに落とす必要があります。この手続きは 2 種類あります。一つは情報セキュリティ対策をするための手続き（例えば、ユーザのＩＤ登録手続など）、もう一つは既存の業務プロセス（例えば、マーケティングやプログラム開発など）に情報セキュリティ対策を組み込む手続きです。このような手続きは現場で実現不可能なものであってはなりません。できないルールほど有害なものはありません。守れない方針や手続があれば、守れる方針

や手続まで守らなくてもよいという風土を作ってしまいます。部分的に守れない方針や手続があれば、それは必ず例外処理として取り扱い、必ず守れる方針や手続にしてください。



おまけ：情報セキュリティも内部統制

平成 18 年 5 月に施行された会社法により、委員会等設置会社に義務付けられていた内部統制システムに関する事項の取締役会決議の実施が大会社にも適用されるようになり、また、金融商品取引法により平成 20 年 4 月 1 日開始事業年度より財務報告に係る内部統制の評価と監査の制度が上場企業等に適用されることになったことから、内部統制が注目を浴びています。情報セキュリティ対策を実施することは、「業務の有効性及び効率性」に係る内部統制との結びつきが強いですが、個人データが漏えい、改ざん等されないようにするという面では、「事業活動に関わる法令等の遵守」に関係する内部統制に関連し、財務会計データの改ざん等がされないようにするという面では、「財務報告の信頼性」に関係する内部統制といえます。従って、内部統制を構築するという観点から、情報セキュリティ対策を実施するということも重要なことになります。

内部統制のデファクトスタンダードといわれているトレッドウェイ委員会支援組織委員会（ＣＯＳＯ）により公表された「内部統制の基本的枠組みに関する報告書（以下「ＣＯ

ＳＯ内部統制報告書」といいます。)」の内部統制の構成要素に当てはめると「風土作り」は主に「統制環境」にあたります。一方、「仕組作り」はそれ以外の「リスクの評価」、「統制活動」、「情報と伝達」及び「モニタリング」にあたります。

第２回　風土作りのために　経営者の本気度が試される

第一回では、情報セキュリティ対策を行うことは本能に反することであり、それを行わせるためには特別な仕掛け、つまり情報セキュリティ対策を行おうとする「風土作り」と「仕組作り」が必要という話をしました。風土作りには経営者の意識が重要となること、仕組作りはマネジメント・システム作りであることを説明しました。そしてその両方が車の両輪のように回って情報セキュリティが達成されることを説明しました。「風土作り」と「仕組作りは」それぞればらばらに行われるのではなく、両者があいまって行われなければなりません。第二回では、「風土作り」についてもう少し考え、次回に説明する「仕組作り」との関係についても簡単に説明しておきます。

情報セキュリティを社風にする

情報セキュリティ対策において「風土作り」が成功した状態とはどのような状態をいうのでしょうか。これがわかれば、情報セキュリティ対策をするための目標が明らかになります。風土作りが成功した状態とは、いちいち「情報セキュリティ対策は重要です。みなさん、情報セキュリティ規定をよく読んでルールを守ってください。」といわなくても、組織のメンバー全員が情報セキュリティ対策を実践している状態といえます。

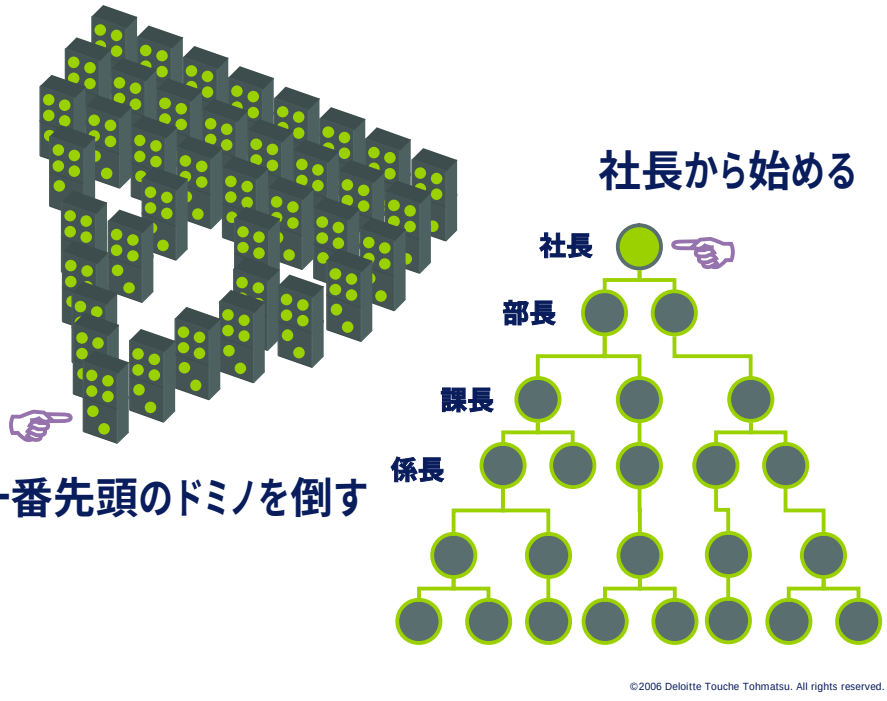
言葉にすれば簡単ですが、実際にこの状況を作り出すのは困難です。今のあなたの組織ではどうでしょうか。経営会議の資料に情報の秘密区分が記されているでしょうか？どのような物理的セキュリティ対策が行われているか理解しているでしょうか？

風土作りのゴールは、情報セキュリティ対策が重要であるという社風にすることです。組織のベクトルをトップから今年組織に加わったメンバーまで合わせることです。品質にこだわる会社、自由に意見がいえる開放感のある会社、仕事を丁寧にきっちりする会社、従業員がのびのびと働ける会社、いろいろな社風の会社があると思います。みなさんの会社にもそれぞれの社風というのがあるはずです。通常それは、組織の中の人にいる人にとっては空気のような存在で意識されないかもしれません。「個人情報、他社の情報、自社の情報を大切に取り扱う会社」こういう会社ですと、組織の構成員全員が当たり前のように

いえる会社となれば成功です。情報セキュリティ対策をすることは不自然な行為であることを考えると、社風として定着させるのは大変ですが、それは不可能なことではありません。では、どうしたらよいのでしょうか。

一番先頭のドミノの先頭を倒す

風土作りは改革です。組織の構成員全員に情報セキュリティに対する意識を高めるにはどうしたらよいのでしょうか？2000 個のドミノがあるとします。この 2000 個のドミノ全部を最もよく倒す方法はどうすればよいでしょうか。ドミノをひとつひとつ倒す人はいないでしょう。普通の人であれば、ドミノを並べて一番先頭のドミノを倒すでしょう。



組織図を眺めてみてください。社長は部長を、部長は課長を、課長は係長を、と必ず上から下に階層ができていますね。すなわち、社長が変われば組織は変わるわけです。人間をドミノにたとえるのは気が引けますが、社長が変われば、ドミノ倒しと同じで組織全体が変わります。そして、それは社長にしかできないことです。社長にしかできないことがある。だから社長は社長ともいえます。

「日本の会社では、中堅の管理職が部下を指導しつつ、経営者に新しい戦略や計画を提案しているので中堅の管理職が反対するようなことをトップはできない。」という意見があるかもしれません。「欧米の会社はトップが命令すれば、下は従うけど、日本ではそう単純でもない。」という意見があるかもしれません。もちろん、人の価値観を変える話でもあるわけですから、「組織のトップがいったことをすべて理解して、納得して、明日から行動しなさい。」と、いうはなしではありません。現実はドミノ倒しのように、パタパタとリズミカルに倒れていくわけではありません。しかし、組織のトップがまず変わらないと組織のメンバーの意識は変わらないということは事実です。「風土作りは社長から」です。トップの本気度が試されます。

腑に落ちなければ人は行動しない

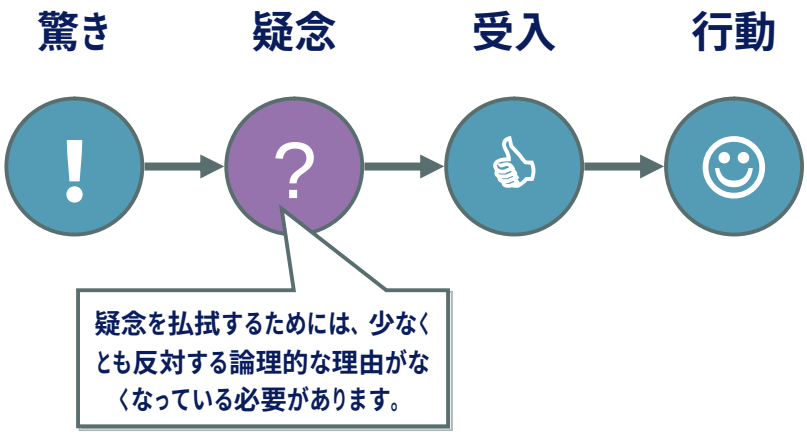
組織のトップの意識が変われば、その「思い」を伝えていく必要があります。その思いを効率よく確実に伝えていくためには「仕組み」が必要です。これは次回に説明します。今回は、伝えられた人がその意図に納得する、腹に落ちる、腑に落ちるようにするためのポイントを説明したいと思います。

人間は、自分が納得していないことを他人にさせられるのは苦痛です。それが自分の利害と関係する場合は特にそうです。黒いカラスを前に「カラスは白い」といわされることは、普通の人にとっても心地よいものではありません。カラスの専門家（いるのかどうかは知りませんが）にとってはもっと苦痛でしょう。昨日まで「直行直帰でもいいからできる限りたくさんの仕事をとってこい」といわれつづけていた営業担当者に対して、「今日からは仕事をとることも重要だが、ウイルス対策ソフトのバージョンが最新であることを毎朝確認しろ」と急にいわれても、心の底から「はい、わかりました。すぐに今日からそのようにします。」とはなかなかいかないものです。

指示を受けた後、その指示内容を実行するまでに、「納得するプロセス」が必要となります。この納得するプロセスは、ある程度時間がかかるプロセスです。まずは、新しいことを指示された場合、人は「驚き」を覚えます。その次にくるのが、「疑念」です。本当にそれでよいのだろうか、自分はそれでどうなるのだろうか、という思いです。この「疑念」が晴れると、新しい概念を「受入」、それを実現するためには自分は何をすべきかを考える

ことができます。そして、新しい概念に基づく「行動」に移ることができます。

この一連のプロセスの中で一番時間がかかるのが、「疑念」を払拭することです。本人が新しい考えを受け入れることに反対する論理的な理由がなくなっている必要があります。例えば、営業担当者が「営業ノルマはそのままで、情報セキュリティ対策をするために追加で時間をとられるのではないか。」といったことを感じたとします。その時に社長が、「情報セキュリティ対策を実施するために慣れるまでは一日 30 分は余計に時間がかかるだろう。したがって、営業担当者のノルマは、７％カットする。」といわれれば、納得するかもしれません。しかし、「営業担当者のノルマはそのままで変更しない。営業担当者は裁量営業だから残業代も出さない。」といわれれば、しばらくは様子をみておいて、「他の営業担当者がやり始めたら自分もしよう」という結論になるかもしれません。他の営業担当者がやり始めるたらしぶしぶ受け入れて、行動をしようということになります。



「動機付け」と「できる対策の提示」が必要

疑念を払拭するために最も効果的な方法は、情報セキュリティ対策をすることが本人にとってもメリットがあることを理解してもらうことです。つまり、動機付けが重要となり

ます。次に、実現可能と思われる情報セキュリティ対策の提示することです。やる気があって、できる対策が提示されている。こういう状態にもっていけば、人は自然と情報セキュリティ対策をするようになります。もちろん、「理論的にはそうだけど、具体的に動機付けをするのが難しい。」という話はあります。では、動機付けをどのようにすればよいのかについて考えていきましょう

情報資産の重要性を認識させるのが王道

現場の担当者が情報セキュリティ対策を積極的にはしない理由は主に次の３つです。

1. 意思疎通をしたいという人間の欲求と情報保護という欲求は衝突する。
2. 情報資産の価値について通常は認識していないので、それを保護するという感覚になりにくい。
3. 人間は、有形資産の保護には慣れているが、情報という無形資産の保護にはなれていない。

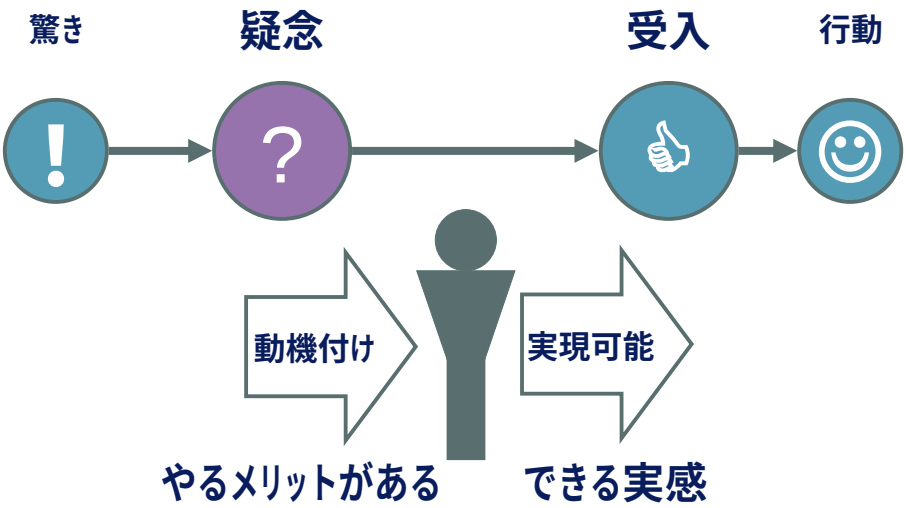
情報セキュリティ対策を行わせるための王道は、情報資産の価値を認識させ、それを保護させることにモチベーションを持たせることです。しかし、それはそんなに簡単なことではありません。情報はスーパーで売っているわけではないし、あるのが当たり前になっているので、正しくその価値を認識するのが難しいからです。その場合は、別の方法で組織の構成員を動機付けしていく必要があります。

どのような動機付けが効果的か、これは純粋にマネジメントの問題です。動機付けは、個々の人それぞれの価値観により変わります。価値観が近い人が集まっている組織では、動機付けは比較的容易に行えますが、多様な価値観を持つ人々からなる組織では、価値観が近いグループ毎に分けて動機付けを考える必要があります。金銭的な動機付けで動く場合もあれば、自由に活動できることで強く動機付けが働く場合もあります。さまざまな動機付けの要素の中から最も効果的な動機付けの要素は何かを検討する必要があります。例えば製造業では、営業部門、管理部門、工場部門、開発部門に分けて動機付けを考えなければならないかもしれません。

組織の構成員をどのように動機付けるかは、直接情報セキュリティ対策をすることではありません。多くのセキュリティ専門家が見逃しがちな視点です。しかし、情報セキュリティマネジメントを行うという視点では最も重要なポイントです。ある会社では、人事制度まで変更しています。

実現可能な対策の提示

また、実現可能な対策の提示も重要です。「そんな対策できるわけがない」と思えば、人はとりあえず反対します。次回の仕組作りでも触れますが、実現可能な対策の提示は違反に対する懲罰とも関係する重要な問題です。また、セキュリティ対策の実効性の問題としても、100%の対策を 50%の人しか実行していない場合と、50%の対策を 100%の人が実行している場合、どちらがセキュリティ対策の実効性が上がっているのかを考えてみれば実現可能な対策の提示が重要なことは明白です。セキュリティ対策を行っていないとその行っていないレベルが組織のセキュリティレベルとなるからです。できていない対策というのは、実際に実現可能かどうかは別として、実現可能な対策と認められていないことが原因となっている場合がほとんどです。実現可能と思わせる対策の提示が重要となります。



みんなはトップの本気度をみている

「情報セキュリティ対策をしっかり行う」という風土作りは改革です。したがって、トップがまず変わらなくてはなりません。また、トップの指示を受けた組織のメンバーがそれを受け入れなくてはなりません。組織のメンバーは、トップが情報セキュリティ対策にどの程度本気で取り組んでいるのかをみて、それに応じて、どの程度対応するのかを決めるでしょう。トップが本気であることを示せば、組織の風土が変わります。風土が変われば、セキュリティ対策が定着します。いちいち「情報セキュリティ対策は重要です。みなさん、情報セキュリティ規定をよく読んでルールを守ってください。」といわなくても、組織のメンバー全員が情報セキュリティ対策を実践している状態になります。

今回は、情報セキュリティの話ではない内容が多くなりました。結局、セキュリティも経営課題のひとつであり、特殊なものではないということです。情報セキュリティも他の経営課題と同じように当たり前にマネジメントをすることが重要であるということです。

以　上

第３回　仕組作りのために　いまさら情報セキュリティポリシーの作り方

第１回では、情報セキュリティ対策を行うことは本能に反することであり、それを行わせるためには特別な仕掛け、つまり情報セキュリティ対策を行おうとする「風土作り」と「仕組作り」が必要という話をしました。第２回では、「風土作り」のポイントを説明しました。情報セキュリティをする社風を作ることが重要となるが、組織のトップの意識を構成員に伝えていくことが重要なこと、その際に、腑に落ちる理由と、実行できる対策の提案が必要なことを説明しました。第３回からは、「仕組作り」つまり、情報セキュリティマネジメント体制作りの説明をします。その際に、情報セキュリティポリシーが要となります。今回は仕組作り、特に情報セキュリティポリシーの話をします。

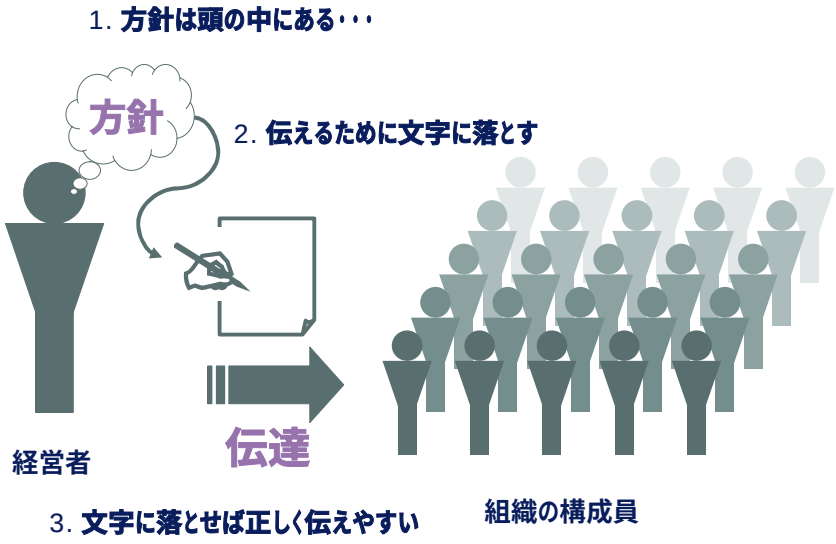
情報セキュリティポリシーは文書のことではない

第１回で仕組作りの第一歩は経営者による方針の伝達という話をしていますが、その方針が情報セキュリティポリシーです。ここで重要なポイントは、「ポリシー（方針）は文書ではない」ことです。「えっ」と思われる方がいるかもしれませんので、もう少し丁寧に説明します。

情報セキュリティポリシーは方針であって、設計思想に近いものです。頭の中にあるものです。トップが情報セキュリティポリシーを持っているというのは、トップの頭の中に、その組織にあるべき情報セキュリティの設計思想があるということです。しかし、情報セキュリティポリシーがトップの頭の中にあるだけでは組織のメンバーには見えません。見えなければ理解されません。そこで、トップは頭の中にある情報セキュリティポリシーを文書にして組織のメンバーに理解されるようにしなければなりません。それが、情報セキュリティポリシー文書です。トップは、情報セキュリティポリシーを文書にして組織のメンバーに伝達します。つまり、方針を伝達するために文書が必要という関係です。

「情報セキュリティポリシーがありますか？」と訪ねると「情報セキュリティポリシーはすでに定めています。」といって情報セキュリティポリシーの文書を見せてくれます。しかし、それが本当の情報セキュリティポリシーかどうかは文書を見るだけではわかりませ

ん。文書を見るだけではトップの頭の中からでてきたその組織における情報セキュリティの設計思想であるかどうかはわからないからです。



情報セキュリティポリシーとは何か

さて、それでは情報セキュリティポリシーとは何かを考えましょう。

すでに説明していますが、情報セキュリティポリシーは、情報セキュリティに関する会社の方針、設計思想のようなものです。「顧客の個人情報のセキュリティは優先的に対策を実施する」、「製品原価に関する情報は重要情報とする」といったビジネス上の要請事項と「外部からのアクセスポイントは最小限とする」、「共有 ID は認めない」といったリスク対応上の要請の２種類の要請があることに注意する必要があります。この２種類の要請はリスクアセスメントを実施する際に意識しなければならないこととなります。

よい情報セキュリティポリシーとは

情報セキュリティポリシーは、それがあることによって事業の成功につながるものでなければなりません。また、情報セキュリティに対するリスクを低減する必要があります。逆にいうとそういうものでなければなりません。情報セキュリティポリシーは組織の目標を達成するための手段だからです。したがって、よい情報セキュリティポリシーは事業を成功に導くものです。それでは「よい情報セキュリティポリシー」とはどのようなものでしょうか。以下に７つのポイントを挙げます。

１．情報や情報システムの価値の順位付けに役立つっている
２．情報セキュリティ戦略、計画、及びその導入を進める基礎となっている
３．経営者、管理者、従業員、協力者にとって、明確かつ首尾一貫した行動規範である
４．規定、ガイドライン、業務マニュアルとともに、評価の尺度となっている
５．外部の利害関係者に対する、明確かつ首尾一貫した意思表明となっている
６．組織全体のリスクマネジメントを達成するための要素となりえている
７．法令及び規制に準拠するのに役立っている

この７つのポイントは網羅的なものではありませんが、このようなポイントを押さえたセキュリティポリシーになっているかどうかという視点で、皆さんの組織の情報セキュリティポリシーを見直してみてください。

情報セキュリティポリシーを文書化するわけ

はじめに「情報セキュリティポリシーは文書ではありません」と説明しました。しかし、「組織のメンバーに正しく伝えるためには情報セキュリティポリシーを文書にしなければならない」と説明しました。そこで、「正しく伝える」ということをもう少し丁寧に説明します。

情報セキュリティポリシーを文書にするのは次のような理由からです。

１．すべての関連する人々（外部の利害関係者も含みます）に情報の取り扱いの方針を正しく理解してもらい、正しい取り扱いを行ってもらえる。
２．情報を守ることは本能に反することで、その必要性が直観的にわかりにくいので文字にして説明する。
３．情報の取り扱いに関する価値判断は明確でないことが多いため、それを明確にする。

したがって、情報セキュリティポリシー文書を読むと、情報の取扱方針が正しく伝わるものでなければならないことになります。皆さんの会社や組織にある情報セキュリティポリシー文書の内容はどうでしょうか。内容が情報セキュリティの取扱方針を示しているものか（ポリシーが適切か）、それが正しく伝わる書き方になっているか（文書化が適切か）、２つの視点から確認してみてください。

よい情報セキュリティポリシーの特徴

さて、情報セキュリティポリシーの内容について考えてみましょう。よい情報セキュリティポリシーには次のような特徴があります。このような特徴は、およそポリシーとよばれるものすべてに共通する話です。

(1) 簡潔でわかりやすい

第一に、簡潔でわかりやすくないとだめです。誰にでも直感的にわかるような書き方が必要です。専門用語を多用しないで下さい。たとえば、
「情報セキュリティとは、情報の機密性、完全性、可用性を確保することで、・・・」と書くよりも、
「情報セキュリティ対策とは、重要な情報が漏えいしたり改ざんされないようにするために、また、重要な情報システムが必要なときにいつでも正しく使えるようにするために行う対策です。」
のほうがわかりやすいですね。

(2) 組織に適合している

一般的な雛型を利用して情報セキュリティポリシー文書を作ることがあります。それ自体を否定するわけではありません。しかし、その雛型の前提となっている環境があなたの組織と同じであるかどうかを確認しなければなりません。前提となっている環境が違うのが通常でしょうから、必要な部分は適切に変更して、組織に適合したものにしなければなりません。そうでなければ、具体的な業務マニュアルを作る際に矛盾がでてきてしまいます。

(3) 実施可能である

前回の風土作りでも説明しましたが、やる気になった人の目の前に実施可能な対策があれば、それは実施されます。ところが、せっかくやる気になったのに、目の前に実施できそうもない情報セキュリティポリシーがあればどうなるでしょうか。やる気までそがれてしまうかもしれません。一度失ったやる気を元に戻すのは大変です。したがって、実施可能なポリシーを作るということは重要なことなのです。守らせる側に多大な努力（例えば給料に見合わないような努力、多大な事前準備が必要、高度な知識が必要）を要求するポリシーは実施されないと思うべきです。「会社のデータは自宅に持ち帰らない」という方針を示したとします。今まで直行直帰していた外回りの営業担当者は、毎朝会社に行き必要な書類を持ち出し営業に出かけ、会社に戻って書類を置き、自宅に戻るというように行動を変更する必要があります。しかし、その際に、会社に寄るための時間が余計に掛かることを計算してあげる必要があります。例えば、稼動可能時間が減少するわけですから営業ノルマを削るなどの配慮が必要です。方針の内容が悪いのではなく、それが、守る側に多大な努力を押し付けているところが問題なわけです。

(4) 遵守を強制できる

違反した場合に懲罰の対象とできなければ、実効性が伴いません。その際のポイントは、「適切な権限により懲罰の対象とできること」と「違反したか、していないかの判断がつくこと」が重要となります。例えば、労働組合等と交渉し、懲罰の対象とすることを規定として承認していることが求められます。また、判断基準が不明確なためその行為が、情報セキュリティポリシーに（これは、方針レベルではなく、業務マニュアルレベルで規定されているかもしれません）違反しているか、違反していないかが不明確になってしますのであれば問題です。

(5) 段階的な導入も考える

「情報セキュリティポリシーが本日の取締役会で承認されました。このポリシーは明日から適用されます。皆様、必ず守ってください」。新しく導入を決めたセキュリティ対策については、すぐにできる対策と、守るために準備が必要となる対策があります。状況によっては、段階的な導入をすべきです。例えば、システム変更が必要となる対策については、1 年間の猶予をするとか、方針はすぐに適用しても懲罰については、1 年間の猶予を認めるといった感じです。個人情報保護法の導入は、基本法部分と個別法部分にわけて二段階で行われましたね。社内の規定等も同様です。

(6) 前向きに取り組める

モチベーションとも関係してきますが、禁止事項が羅列されたポリシーというのは、読んでいてつらいものです。もちろん、禁止事項が必要な場合もありますが、できる限り「～すること」という書き方が望ましいです。

(7) 絶対や完全は用いない

外部の利害関係者にも提示するものであれば、「絶対」や「完全」といった表現は用いないようにすべきです。用いるべきときは、慎重にすべきです。「達成したい目標」と「達成しなければならない遵守事項」とは違います。社内のメンバー示す方針であれば達成したい目標を提示するということでよいのですが、外部に提示する場合は、達成しなければならない遵守事項のみを提示すべきです。達成しなければならない遵守事項が守れなかった場合は、責任問題となります。「絶対」や「完全」といった表現はできる限り使わないようにすべきです。

(8) リスク受け入れの概念がある

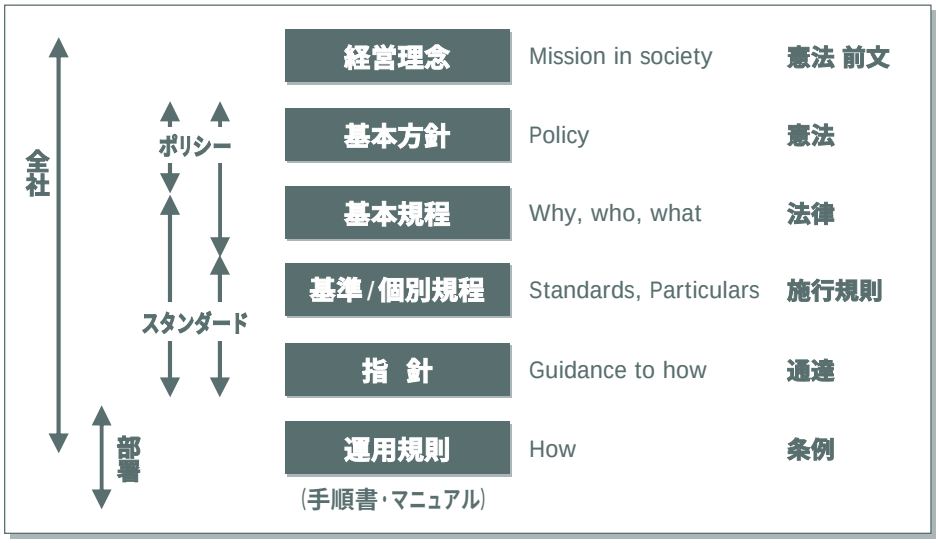
100%のリスクの低減はできません。リスクを受け入れるということも必要です。リスクを受け入れるということは、セキュリティ対策をあきらめるということです。すべての人間の行動に共通のことですから当然なのですが、あらためて文字に落とすとなると気が引けるかもしれません。しかし、リスクを受け入れるという選択肢もあることを明確に意識することが重要です。

(9) あらゆる形態の情報をカバーする

守る対象は、情報とそれを取り扱うシステムです。ここがポイントです。情報とそれを取り扱う媒体は別です。時々、紙情報はすでに文書管理規程で定めているという理由で、情報システムで使われる情報に関してだけ情報セキュリティポリシーを定めている場合があります。あるべき姿は、情報と情報システムの取り扱いを定め、その場合に文書という媒体の取り扱いを決めるという考え方です。

(10)　内容とその詳細度が妥当である

情報セキュリティポリシーについて、ここまで詳細さについて説明せずにきました。情報セキュリティポリシーはその名のとおり
方針です。方針は設計思想なのでそれだけでは細かい状況に応じた対応はできません。そこで、より詳細な行動指針や規範が求められる場合があります。その階層を明確にし、状況に応じた詳細さで規定することが重要です。そのためには、上位の方針をより具体的にした詳細なものを業務における適用指針や要求事項として定めていくことになります。一般的には次のようになります。



(財) 関西情報センター　ISMSセミナー
元松下電器産業株式会社　法務本部　IT・情報セキュリティ担当顧問
現長岡技術科学大学教授淺井氏の資料より

また、これらの規定等の承認を誰が行うのかも階層に応じて決めることになります。

文書化のポイントは、必要なだけ文書化することです。文書にしなくても誰でも正しくできることは文書にする必要はありません（例えば、一般のドアであれば開け方のマニュアルなんて作りません。しかし特殊な構造の扉や、緊急用扉については開け方の説明が必要となるでしょう）。

今回は、このあたりで終わりにします。次回は、体制の話をしていきます。

第 4 回　情報セキュリティと組織体制　CISO は必要か？

第 3 回は「仕組作り」の第一弾として、情報セキュリティポリシーの話をしました。今回は、情報セキュリティと組織体制の話です。特に、最高情報セキュリティ執行役といわれる CISO（Chief Information Security Officer）が必要かという話などをしていきたいと思います。巷では、CISO が必要だという話が多いですし、実際に CISO を設置している企業も増えているよう思います。私もセキュリティ関係の人と名刺交換をすることが多いのですが、「CISO です」と名刺を渡してくれる人も時々います。でも、本当に CISO が必要なのか。そんなことを思っている経営者の方も多いと思います（ひょっとしたら、CISO の人が今回の連載を読んでいるのかもしれませんが・・・）。ということで**今回は、情報セキュリティの組織体制作りと CISO の話**です。

ISMS の構築が必要

情報セキュリティ対策が適切に継続的に整備され、運用されつづけるためには、**情報セキュリティ対策が行われるような管理体制をつくることが重要**です。このような管理体制を情報セキュリティ・マネジメント・システム、ISMS といいます。「あれっ。ISMS といえば、国際標準となり、JIS にもなった認証制度のことじゃないの？」と思う経営者の方がいればかなり情報セキュリティに詳しい方でしょう。確かに情報セキュリティ・マネジメント・システムに関する認証基準と JIS Q 27001 があります。でも ISMS は JIS Q 27001 のことではありません。JIS Q 27001 は、ISMS のベストプラクティスといわれるものを JIS 規格にしたものに過ぎません。あなたの組織の ISMS が必ずしも JIS 規格に従わなくてもよいわけです。重要なことは、情報セキュリティ対策が適切に継続的に整備され、運用されつづけるようになることです。対外的に説明が必要な場合には、ISMS の認証を取得することで説明はしやすくなります。それだけのことです。

組織は戦略に従い、戦略は組織に従う

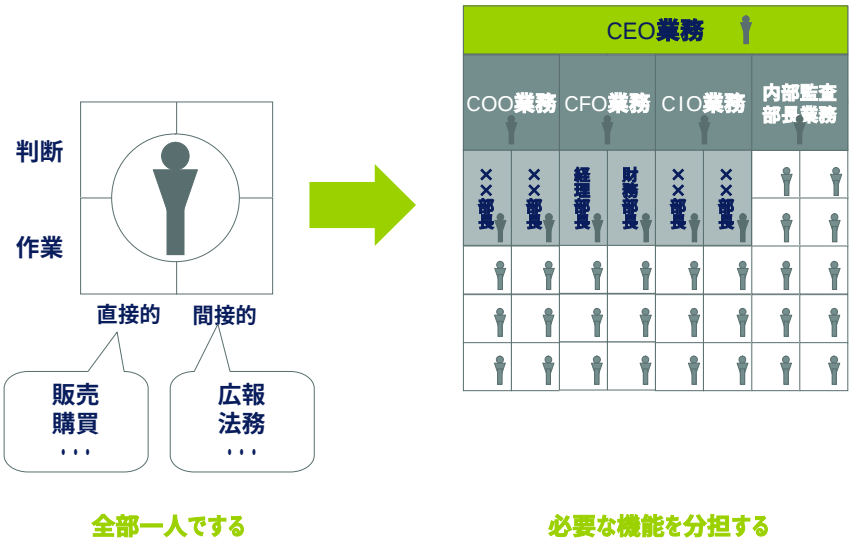
あなたの組織にもっともふさわしい ISMS をどのようにつくるか。これが本章のテーマです。**組織をどのようにデザインするかは、何をしたいかに依存します**。当たり前ですが、目標達成のために組織をデザインするということです。あなたの組織が何を使命として存在し、何を達成しようとしているか、そのための基本的理念は何か、そういうことが重要となります。このような基本的理念の情報セキュリティの側面が情報セキュリティポリシーとなります。つまり、情報セキュリティポリシーを達成するためにどのような、戦略が必要かを考え、その戦略を実行するためにはどのような組織がふさわしいか、これが ISMS をデザインするための第一歩です。目標達成のためにもっともふさわしい組織設計の正解というものはありません。業務の内容や種類、従業員等の人数や勤務形態、組織の地域的広がり等、さまざまな要因を考える必要があります。また、それらの条件は時とともに変化します。絶対的な正解はありませんが、誤った組織を作ってしまうと目標を達成できずに失敗しますので、ポイントは押さえておく必要はあります。

儲けるための組織体制とリスクを減らすための組織体制

ISMS のための組織をどのように作ればよいのかについて、考えてみることにします。あなたが一人で商売をしているとしましょう。あなたは、事業に関するすべての判断や作業をしなければなりません。営業方針を決める必要もありますが、営業もしなければなりません。お客さんが、「掛売りでお願いします」といえば、掛売をすべきか、代金引換にすべきかの判断もしなければなりません。掛売りをすれば売上増加に結びつき利益が増えるかもしれませんが、代金回収ができなくなる可能性もあります。さて、ここで２つの視点が生まれました。ひとつは**判断と作業という視点**です。もうひとつは、**目的達成に直接的に関係する判断や作業**（例えば、儲けること、販売することなど）と**目的達成を間接的に支援する判断や作業という視点**です。**目的達成を間接的に支援する判断や作業という**業務は間接業務と一般的には言われます。間接業務は更に、代金回収ができなくなることを防ぐという損害の発生等を防止する業務と、マーケティングのようにより効率的売上を上げるような業務の有効性・効率性を向上させる業務の 2 種類があります。組織の成長に合わせ

てこれらの業務を分化させ、それぞれの業務を人に割当てていくことになります。なお、間接業務を専門にする人を集めて組織化した部門は、間接部門と呼ばれたりします。

　下の図を見てください。もともと一人でしていた業務は、業務を拡大するために分化させていかなければなりません。それぞれの人が升目の中で仕事をしていくために、責任と権限が任されます。これが職務分掌と職務権限です。多少の濃淡はあれ、組織に必要な職務はもれなく埋めつかされなくてはなりません。



CISO の仕事は何か？

　さて、このように経営者がしなければならない機能を分解していった場合に、CISO はどのような業務を担うことになるのでしょうか。それは、定義次第です。職務分掌規程でどのような職務を担うのかを定義し、職務権限を規定し何ができるのかを決めることになります。具体的な職務や権限は情報セキュリティ管理規程などで規定されるかもしれません。ところが、実は CISO を設けている企業の職務内容や権限を確認すると曖昧な場合があります。認証を取得するために CISO を設置しただけで、実はその職務や権限が明確になっていないのです。例えば、「CISO は、当社の情報セキュリティに関連する業務全般を統括し、情報セキュリティに関する責任を担う。」と規定されていたらどうでしょうか。具体的にどの

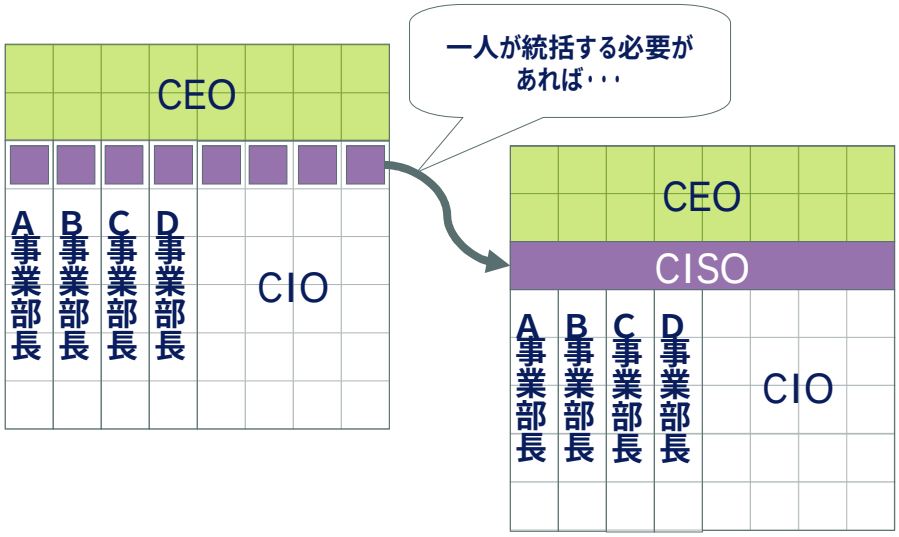
ような職務と権限があるのかよくわかりません。そもそも、情報セキュリティの定義が「情報の機密性、完全性、可用性を確保すること。」と定義されている情報セキュリティ管理規程が多いことをあわせて考えると、**CISO の仕事は明確にされていない場合が多い**ようです。

これは、情報セキュリティの位置づけが明確でないからです。情報セキュリティという言葉には、情報の保護が目的としてあるのですが、その実現手段の多くの部分が情報システムの脅威対策であるので、どうしても情報システム対策ということで、CISO は情報システムを統括する執行役である CIO(Chief Information Officer)の下のイメージになりがちですがそうでしょうか。

情報の保護という意味では、CIO の仕事の範囲だけではもれがでます。各業務の現場（例えば、マーケティングの現場）での情報の保護が範囲外となるからです。そういう意味では、リスク統括責任者である CRO（Chief Risk Officer）の職務の一部を補佐する役割というほうが収まりがよい場合もあるでしょう。CRO がいない組織は、リスク管理がそれぞれの業務の責任者に分担されていることになり、その統括は最高執行責任者である CEO（Chief Executive Officer）又は COO（Chief Operation Officer）がすることになります。

みなさんの組織では CISO は必要ですか

CISO が必要かどうかは、CISO の仕事を誰かに統括する必要があるかということに尽きます。各現場の責任者の仕事として分割しその統括を CEO や COO に任せるほうが効率的かつ効果的であればそうすればよいのです。



一人で統括するほうが情報セキュリティ対策を効率的かつ効果的に実行に移せるのであれば、CISO を設置すればよいでしょう。例えば、各事業部長は売上増加や利益率アップのための仕事にできる限り集中したほうが効果的な運営ができる場合、各事業部長の意見を調整し組織全体として統一した情報セキュリティ対策を実施したい場合などがそれにあたるでしょう。とくに情報セキュリティの業務は IT に関する専門的な知識が必要となる場合も多いのでできる限り専門家に任せたほうが効果的にできる場合が多いと思われます。もし、一人で CISO をするには業務が少なすぎるのであれば、例えば CIO の業務と兼務させるという方法もあります。しかし、CIO と CISO はその業務の目的が異なります。場合によっては CIO と CISO の利害が対立することもあるでしょう。そのような場合は、わけるほうがよいかもしれません。

それでは、まとめです。あなたの組織では CISO が必要ですか。次のような場合は、CISO の設置を検討してください。

1．**組織全体として情報セキュリティに関わるリスクを統一的に統制したい**場合

2．各事業部長が直接業務に専念し、**情報セキュリティに関する業務を別の責任者に統括させるほうが組織全体の業務が効率的かつ効果的に行える**場合

組織作りは経営者の大切な仕事です。この後は、経営者自身の判断にお任せするほうが

良いようですね。今回は、このあたりで終わりにします。次回は、「リスクアセスメントの仕方とやめ方」の話をしていきます。

第５回　リスクアセスメントの仕方とやめ方（１）リスクアセスメントをする前に理解しておくべき５つのポイント

第４回は「仕組作り」の第二弾として、「情報セキュリティと組織体制　CISO は必要か」という話をしました。CISO という役職がはやりだからといってつくるのではなく、組織全体として情報セキュリティに関わるリスクを統一的に統制したいのか、事業部長が直接業務に専念し、情報セキュリティに関する業務を別の責任者に統括させるほうが組織全体の業務が効率的かつ効果的に行えるのか、といった観点を踏まえて作る必要があるという話をしました。

さて、**今回は情報セキュリティ対策を考える上で重要となる「リスクアセスメント」の話**をしたいと思います。「リスクアセスメントをどうすればよいのかわからない」、「情報セキュリティリスクはどのように算定すればよいのか」、「リスクアセスメントをどこまで詳細にすればよいのかわからない」という相談をうけますが、みなさん難しく考えすぎだと思います。今回は、経営者であれば誰にでもできるリスクアセスメントの話です。今回は、リスクアセスメントをする前に理解しておくべきポイントを５つ説明し、最後にリスクアセスメントのやめ方の話をします。

リスクアセスメントをする前に理解しておくべき５つのポイント

ポイント１：リスクアセスメントはビジネス感覚で行い、テクニカル感覚では行わない。
ポイント２：定量的にリスクアセスメントができるという幻想をすてる。
ポイント３：リスクアセスメントはビジネスからプロセスの順で行う。
ポイント４：リスクアセスメントをする責任者はビジネスオーナである。
ポイント５：ビジネスオーナが重要性判断を、脆弱性判断は取扱者が行う。

この５つのポイントを押さえておけば、情報セキュリティのリスクアセスメントはそん

なに難しいものではないと思います。

リスクアセスメントはビジネス感覚で行うことが重要

リスクアセスメントを行う目的は、ビジネスを成功させるためであり、会社のリスクが実際どの程度あるかを正確に算定し論文を書くことではありません。目的はビジネスを成功させることで、その手段のひとつとしてリスクを算定するのです。この両者の関係は当たり前のことです。しかし、実務でリスクアセスメントを始めると目的と手段の連鎖の中で「リスクをどのようにすれば正確に算定できるのか」というテクニカル論に議論が落ちていってしまうことが多いようです。情報セキュリティのリスクを考える場合、テクニカルで客観的な情報に基づいて判断していくことも重要です。しかし、経営判断をするために必要となる情報を全て網羅的に収集できると思う人はいないでしょう。もしできれば、経営者は必要ないということです。結局**リスクアセスメントは、経営者としてのビジネス感覚で決めるしかない**のです。経営者は、中国に子会社を設立すべきかどうか、他社を買収すべきかどうかなど、情報セキュリティ以外の大きなリスクに立ち向かっています。情報セキュリティのリスクもそれと同じく経営感覚で対応すればよいわけです。

定量的なリスクアセスメントはできない

リスクアセスメントの教科書には、「リスクはできる限り定量的に算定し、評価するほうがよい」と書いているかもしれません。しかし、こと**情報セキュリティについては定量的にリスクを算定することはできない**と思ってください。

リスクを算定するための数式として、

リスクの大きさ＝影響度×発生可能性

という数式が説明に使われていることが多いでしょう。数式を持ち出されると、リスクを客観的に評価できるように思いますが、そんなことはありません。上記の数式は単なる概念を説明するために持ち出されているといってよいでしょう。「(純粋) リスクというのは、ある事象が与える影響度と、その事象の発生可能性によって大きさを測ると考えるとわかりやすいでしょう。」といった程度のものです。また、情報セキュリティの分野では、次の数式もよく使われます。

リスクの大きさ＝情報資産の価値×脅威の発生の可能性×脆弱性の程度

これも同じです。いずれもリスクの大きさについて概念的に説明するための方便にすぎませんから、上記の数式を利用してリスクを定量的に測定するのは馬鹿げた話です。とりわけビジネスの視点にたったリスクアセスメントは経営上のリスクに対して、自らの資源をどの分野から優先してどの程度使うのかを決めることです。そう考えれば、定量化の必要性もある程度でよいことがわかってくると思います。繰り返しリスクの評価をしているうちにある程度のリスクについての目安がついてくると思ってください。

経営者はもともと数式では導けない課題について意思決定をする人なのですから、自分の経営センスにもっと自信をもって対応すべきでしょう。

リスクアセスメントはビジネスからプロセスの順で行う

3 番目のポイントは、リスクアセスメントを行う場合、2 つの視点があるということです。ひとつは、ビジネスの視点です。もうひとつはプロセスの視点です。ビジネスの視点というのは、どのような事業領域、リスク項目のリスクが大きいのかを把握するために行うものです。リスクアセスメントをする順番はビジネスの視点から行い、次には業務プロセスレベルのリスクアセスメントをします。現場で情報セキュリティのリスク分析を行う場合、情報資産の棚卸と称して、サーバルームにある情報資産を順番に数えていったり、情報システムに保存されているデータやプログラムの棚卸をいきなり始める場合がありますが、そのような方法ではコストがかかりすぎます。まずは、ビジネスの視点からどのような情報セキュリティ上のリスクがあるのかを考えることが重要です。ビジネスの視点からみて重要性のない部分にまで詳細なリスク分析をする必要はありません。ISMS 認証を部門で取得する場合は、実はこのような経営の視点からのリスクアセスメントを既に行っているといえます。ビジネスの視点からみて重要な情報や情報システムが存在する部門をマネジメントの単位としてみなして ISMS の認証範囲を決めることは、すでにリスクアセスメントをしているといえます。これがある意味ビジネスの視点からみたリスクアセスメントの例で

す。次に、業務プロセスにしたがってリスクを洗い出していきます。経営資源は限られていますから、経営上の優先順位に従って、経営資源を利用するのが当たり前です。リスクアセスメントを行うということは、経営資源の割当ての優先順位付けを行うことであるという意識をもう少しもったほうがよいでしょう。**ビジネス上の重要な分野から情報セキュリティに取り組むことが重要です**。

リスクアセスメントをする責任者はビジネスオーナである

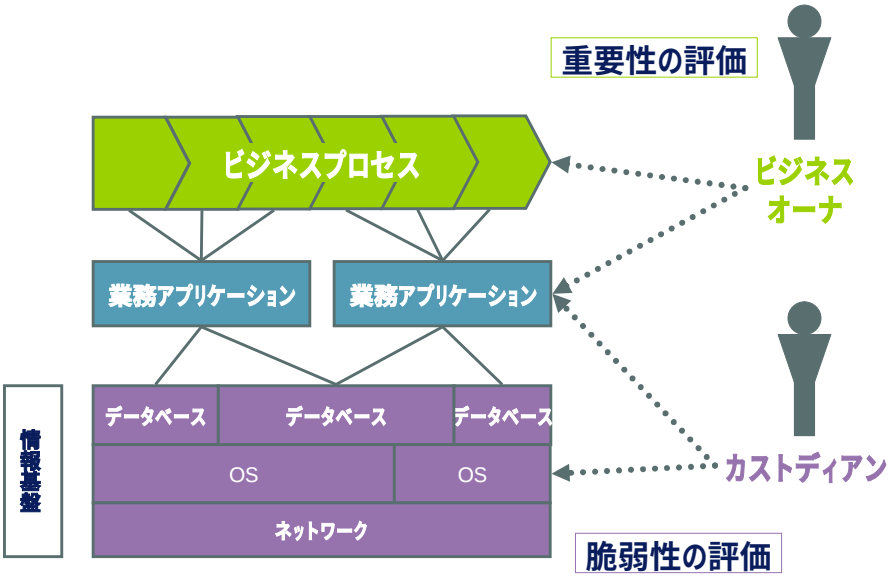
4 つ目は業務プロセスレベルでの情報セキュリティのリスクアセスメントをする場合のポイントです。業務プロセスレベルでのリスクがどの程度でどこまで受け入れるかを決めるのはビジネスオーナです。情報システム部門の人が、情報セキュリティのリスクアセスメントができないと悩んでいる場合がありますが、それは当然です。情報システム部門は情報システムが処理をしているビジネスが成功するか失敗するかについての直接的な責任を負っていません。だから、情報システムの障害がどれだけビジネスに影響を及ぼすのか、つまりどれほどのリスクがあるのかを評価することができないのは当然なのです。業務プロセスレベルでの情報セキュリティのリスクアセスメントは、ビジネスの重要性、そのビジネスに及ぼす情報等の影響度などを考慮して、**ビジネスを遂行する責任者、つまりビジネスオーナが最終的に責任を持つ**ことになります。従業員の人事情報のリスクアセスメントは人事部長が、通信販売事業部で利用する個人情報のリスクアセスメントは通信販売事業部長がリスクアセスメントをする責任があるということです。

ビジネスオーナが重要性判断を、脆弱性判断は取扱者が行う

では、情報システム部長はリスクアセスメントにおいて何もすることが無いのでしょうか？そんなことはありません。情報システム部長の責任を考える前に、オーナとカストディアンという考え方を説明します。カストディアンというのは、執事という意味です。ビジネスオーナに仕え、ビジネスを裏で成功に導くいわば裏方さんです。ビジネスオーナが行う業務の執行を代わってしてくれる人ということです。「最も売上高の多い顧客を選定し

たい」とビジネスオーナである営業部長が思った場合、カストディアンは顧客名簿と売上明細を調べて最も売上高の多い顧客の名前をビジネスオーナに提供します。今では人間が売上明細の帳簿をめくって調べるのではなく、情報システムが検索してくれます。情報システムがカストディアンともいえるのですが、その情報システムを管理している人がカストディアンということになります。**ビジネスオーナはビジネスやそのビジネスで利用する情報の重要性に応じた判断を行うことができます。一方、脆弱性については情報を取り扱う場面での責任者がその判断を行うことになります。**営業管理部で顧客名簿を業務委託先にＦＡＸ送信する場合の情報セキュリティに関する脆弱性、例えば、誤った番号に送付してしまう可能性の評価を行うのは、営業管理部になります。顧客マスターデータを管理している情報システムに関する脆弱性、顧客マスターデータが変更権限を有していない人により改ざんされる可能性は、顧客マスターデータを管理している責任者が評価することになります。多くの場合、顧客マスターデータの管理は情報システム部門が行っています。したがって、情報システム部門が脆弱性によるリスクの発生可能性を評価することになります。

気をつけなければならないのは、情報ネットワークなど多くの業務に対して影響を与える情報システムの場合のリスクの評価です。社内のネットワークが止まれば多くの業務に影響が及びます。影響するビジネスがどの程度あるかについての判断は情報システム部門でなければできません。ビジネスプロセスがどのような業務アプリケーションを利用していて、その業務アプリケーションがどのような情報基盤（たとえば、社内ネットワーク）を利用しているかを把握し、リスクアセスメントに反映していく必要があります。



リスクアセスメントのやめ方

「リスクアセスメントはどこまで詳細にしたらよいのか」つまり、「リスクアセスメントのやめ方」の話を最後にします。リスクアセスメントは、ビジネス感覚ですればよいので、経営者がこの程度でよいと思ったところまですればよいのです。**最初から完璧を求めると悩みます。最初は 60 点でよいわけです。**100 点がとれないからまったく何もしないというよりも、60 点でもよいので少し前に進むほうが重要です。経験を積んでいく中で誤りがあると思えば、少しずつ修正していけばよいのです。リスクアセスメントもマネジメントプロセスの中で改善していけばよいわけです。情報セキュリティ対策をどの程度すればよいかを決定することもビジネス上の判断であるということを常に意識しておけば、経営者自身が納得できるところで自信をもってリスクアセスメントをやめればよいのです。

まとめ

それでは、まとめです。今回は情報セキュリティ対策を考える上で重要となる「リスク

アセスメント」の話としてリスクアセスメントをする前に理解しておくべき５つのポイントを説明しました。リスクアセスメントは、テクニカルな正確性を追及するのではなく、ビジネスの視点で経営者の視点で自信をもって行えばよいという話をしました。

　今回は、このあたりで終わりにします。次回は、「継続的なセキュリティマネジメントの実施に向けて」と題して継続的なセキュリティ対策の重要性の話をします。

第 6 回　継続的なセキュリティマネジメントの実施に向けて（１）周知・教育・訓練の重要性

第 5 回は情報セキュリティ対策を考える上で重要となる「リスクアセスメント」の話をしました。「リスクアセスメント」を実施する際にはリスク正しく計量しようとするのではなく、経営の視点から行えばよいということを説明し、リスクアセスメントについての５つのポイントを説明しました。

今回は継続的なセキュリティマネジメントの実施に向けて重要となってくる「**周知・教育・訓練**」の話をしたいと思います。「継続的なマネジメントの実施に向けて一番重要なのは、PDCA の C の部分、つまり監査じゃないの」と思う人がいるかもしれません。確かに、監査も重要ですが、監査よりも教育のほうがより重要です（監査の話は次回にしようと思います）。また、「なんだ、教育か。うちの会社では、セキュリティに関する e-learning 教育を全ての従業員と派遣社員に受けさせているよ。記録も全部とっているので、うちの会社は万全だ。」という人がいるかもしれません。形式的な面では万全かもしれませんが、実効性が上がっていないと意味がありません。というか、実効性が上がらない教育というのはコストをかけて貴重な従業員の時間を無駄にしているということになります。効果的に教育をすることが重要です。今回はこの連載の第 1 回「情報セキュリティのための「風土作り」と「仕組作り」」、第 2 回「風土作りのために経営者の本気度が試される」、第 3 回「仕組みの作りのためにいまさら情報セキュリティポリシーの作り方」の話も交えながら話をしていきます。

ほとんどの組織は周知・教育・訓練の本当の重要性がわかっていない

いきなり、挑戦的な始まりですが、これはほとんどの組織で当てはまっていると思います。次のような質問を考えてみましたので、みなさんの組織の場合はどうでしょうか。

1.　情報セキュリティポリシーを作るために要した費用や労力よりも情報セキュリティポ

リシーを実行してもらうための教育等に要した費用や労力のほうが多い。
2. 経営者が情報セキュリティポリシーの周知・教育・訓練を積極的に支援してくれている。経営者自らが教育を受けている。
3. 周知計画、教育計画、訓練計画があり、毎年実行されている。

情報セキュリティポリシーを作り終わった段階でプロジェクトチームが解散してしまい、教育は付け足しのように行われている組織が多いのではないでしょうか。第 1 回、第 2 回で説明したとおり、新たなポリシーの導入は風土改革ですから、情報セキュリティポリシーを守るために従業員等への動機付けが必要です。そのための方法としてこれら周知・教育・訓練というものが重要となります。

周知・教育・訓練

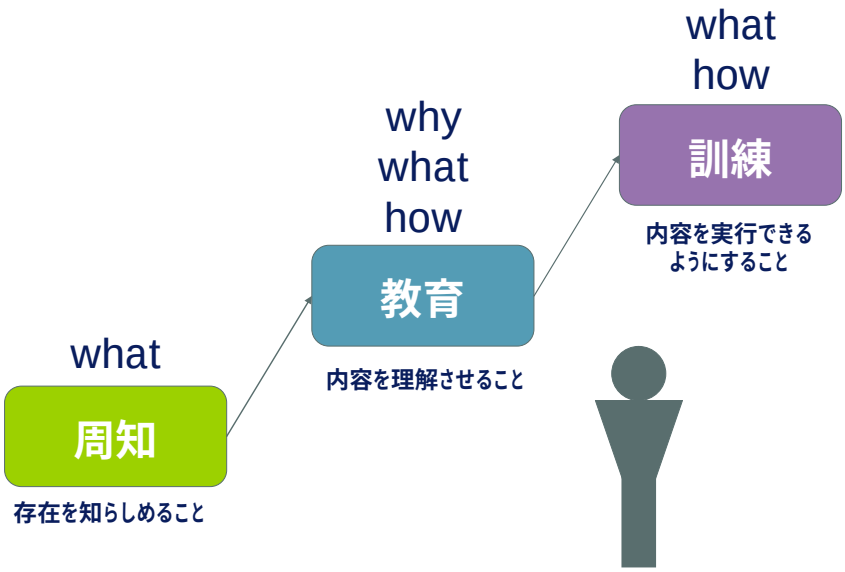
まず、この３つの用語を区別して使うことにします。皆さんの組織では、別の定義がされているかもしれませんが、ここでは、次のように定義します。

周知：存在を知らしめること
教育：内容を理解させること
訓練：内容を実行できるようにすること

第 2 回で新しい指示を受けた後、人間が、驚き、疑念、受入、行動というステップを踏むという話をしました。そして、「それを本当にしなければならないのか」という疑念を払拭し、新しい指示を受入れるためには、それを行う動機付けが必要という話をしました。腑に落ちなければ行動につながりません。この**腑に落ちるようにする仕掛けのひとつが周知や教育**です。

また、第 2 回では、腑に落ちた段階で実現可能な対策が提示されているとそれは実行に移されやすいという話もしました。具体的な手順書があればよいでしょう。しかし、文書だけ読んでも、その本意が伝わらないかもしれません。また、具体的にやらないと実行できないかもしれません。具体的に実行に移すためには、教育と訓練が必要となります。特

に複雑なことをさせる場合は、訓練が重要となります。



周知は従業員に対する広報　その存在を知らなければ始まらない

　まず周知が重要です。情報セキュリティ対策を組織に根付かせようとする場合、情報セキュリティ対策の存在やその重要性を従業員等にまず知ってもらわなければなりません。また、情報セキュリティポリシーを策定した場合も、それを守ってもらうためにはその存在を知ってもらわなければなりません。「知らないものは存在しないに等しい」のです。情報セキュリティポリシーを策定したことを周知させるために多くの組織で、「通達文書を各部署の部長に発信した」、「社内ウェブサイトのトップページにリンクした」、「社長名で全員にメールをした」という事例があります。これは立派な周知の方法です。ただ、私がそこで気になるのが、「それで本当に本意が伝わったか」ということです。ただ、社内ウェブサイトのトップページにリンクしただけであれば、本意が伝わらない場合が多いのではないでしょうか。「最近、何か新しいパソコンのルールができたみたいだね。ちょっと開いてみたけどよくわからなかったよ。ところで、今日のお昼はどこに行く？・・・」で話は終わってしまうかもしれません。これでは情報セキュリティポリシーができたことはすぐに

忘れ去られてしまいます。

例えば、全社的に情報セキュリティの重要性を周知させる場合には、どのような媒体を使って、誰に、いつ、周知させていくかといった周知計画を立案して実施していくことになります。周知の段階では、具体的な内容を理解してもらうための教育に進むために従業員などに「**動機付けを行う**」ことに焦点を当てる必要があります。周知は、従業員などに対する情報セキュリティの広報やマーケティングと考えればよいでしょう。

教育　なぜ、何を、どのように

周知・教育・訓練は、それぞれ重要ですが、なかでもその**中核をなすのは、教育**です。教育と周知や訓練との関係を整理すると、周知は教育のために必要な作業であり、訓練は、教育の結果、理解してもすぐにできないことをできるようするためのものといえます。

教育というのは簡単なものではありません。例えば、情報セキュリティポリシーを理解してもらうための教育計画を立案する場合、誰に、何を、どのような手法や教材を使って、どの程度の費用で行うのかということを明確にしなければなりません。また、ひとつひとつの教育カリキュラムを**どの程度の理解レベルの人をどの程度まで引き上げるのかを明確にして立案**しなければなりません。単に「e-learning なら手軽にできるから」という理由で教育をしても教育効果はあがりません。

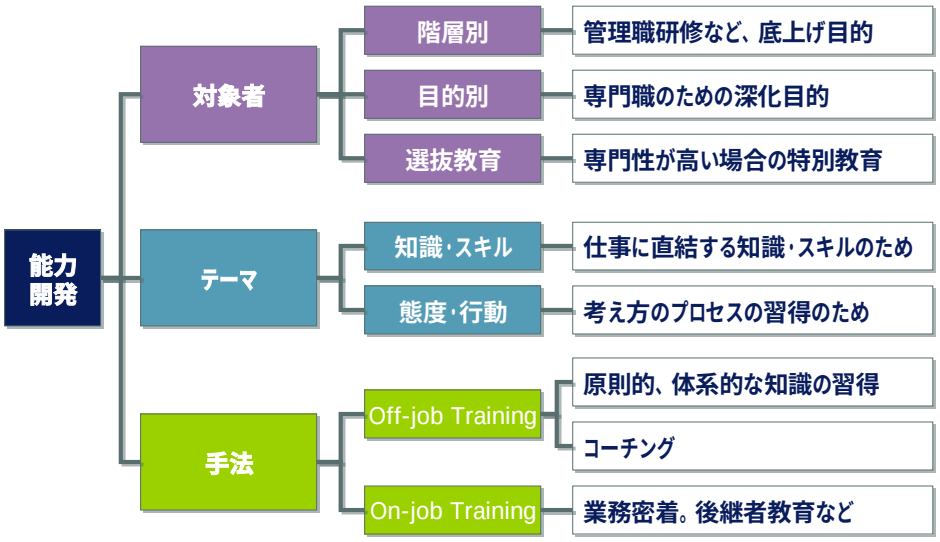
誰が	外部講師
誰（対象者）に	全従業員
何（テーマ）を	個人情報保護の重要性に関する知識
何（媒体）を使って	パワーポイント 配布資料
どのような手法で	45分の講義方式

訓練　体で覚えないとできない

訓練は、教育のうち「どのようにするか（HOW）」の部分を強調したものと考えてください。簡単なことは聞いたらすぐにできます。しかし、聞いただけではできないこともあります。車の運転マニュアルを読んだだけでは車が運転できないのと同じです。複雑で、多くの判断が求められるような手順を確実に実行するためには、座学だけでなく実際に訓練を通じて「体で覚える」ことが重要です。特にとっさの行動は体が覚えていないとできません。**緊急対応時の情報セキュリティ対策は訓練が重要**となります。

教育・訓練は能力開発

教育・訓練は能力開発プログラムの一部と考えてください。対象者、テーマ、手法という観点から整理してみましたので、参考にしてください。



成功のポイント

最後に周知計画、教育計画、訓練計画を立案する際の留意点を挙げておきます。大きな組織にとっては必要なことでも小さな組織では必要でないこともあります。組織で重要と思うことから順番に実践してみてください。

- 教育等で、あなたの組織をどのような状態にすべきかという目標を明確にし、それぞれの個人に対して**必要となる知識・技能を明らか**にしてください。
- 目標を達成するための、組織内の**キーとなる組織や人は誰かを特定**してください。
- あなたの組織にある**既存の教育インフラを活用**してください。新人研修、部門における技能研修、管理職研修といった既存の教育インフラに情報セキュリティをテーマとした研修を組み込むことが効果的です。
- **他の教育と組みあせることでより効果的な場合**がないか検討してください。例えば、ソフトウェア開発技法の 3 時間研修の最後の 20 分間にソフトウェア開発時におけるセキュリティ上の留意点という内容を盛り込むことでより効果的な研修効果が期待できるでしょう。
- **教育手法**としてどのような方法でメッセージを伝えるのが適切かを目的またはカリキ

ュラム毎に考えてください。例えば講義形式で教育を行うだけでなく、合宿でディスカッションをしながら研修を行う、クイズ形式の e-learning を使う、研修終了後にテストをするなど、いろいろな手段がありえます。ただし、手段に力を入れすぎるのは禁物です。ビデオは効果的な媒体ですが、そのために多くの時間を費やして全体計画が遅れるのは本末転倒です。

- 一般論や原則論に終始せずに**自らの組織の失敗体験や成功体験を取り上げ**、自社の成功・失敗体験を共有することも考慮してください。身近な事例によりメッセージを強く伝えることができます。また、具体的にどのようにすれば良いのかを理解することができます。
- **研修はできる限り楽しく**してください。情報セキュリティというテーマは人間の本能に逆らうことをさせることですから、多くの人は否定的な態度から入ります。つまらないテーマと思う人も多いでしょう。研修がつまらなければ、メッセージが聴衆の心に届きません。ただし、失敗事例の登場人物を茶化したり、情報セキュリティがつまらないものと思わせるような発言はしてはいけません。情報セキュリティは重要な経営のテーマなのです。
- 研修終了後に記念品を渡すことも効果的な場合があります。例えば、情報セキュリティに関する簡単なメッセージを記したボールペン、マウスパッド、クリアファイルなどを配布するということも考えてみてください。
- 必要であれば外部講師を活用も考えてください。外部講師に話してもらうことにより、研修全体に緊張感を与えることができます。ただし、外部講師に対して、内部講師以上に組織内部の事情に合わせた研修を期待することはできません。
- 販売されている教育コンテンツは網羅的に要点をまとめているので、多くの人にすばやく情報セキュリティに関する基礎的な知識を獲得してもらうという目的には向いている場合もあります（コンテンツ次第ですが・・・）。ただし、組織の事情に合わせたものではないために、その効果には限界があることも理解してください。

まとめ

今回は、「継続的なセキュリティマネジメントの実施に向けて（１）周知・教育・訓練の

重要」というテーマで、周知・教育・訓練の重要性について説明しました。情報セキュリティポリシーを策定するのと同じように、従業員等がその周知や理解をできるようにすることに力を注いでください。

次回は、「継続的なセキュリティマネジメントの実施に向けて」の第二弾として自己評価・監査について説明したいと思います。

第 7 回　継続的なセキュリティマネジメントの実施に向けて（2）自己評価と監査で改善につなげる

第 6 回は継続的なセキュリティマネジメントの実施に向けて重要となってくる「周知・教育・訓練」の話をしました。周知により意識付けを行い、教育を通じて理解させ、訓練によって確実に実施できるようにする。そのためには、周知・教育計画等を立案し、実施していくことが重要であると説明しました。

さて、今回は、継続的なセキュリティマネジメントの実施に向けて（2）として、**自己評価と監査**の話をします。今回紹介する方法は、まずセキュリティ対策の実施者が自らの実施状況を確認・評価し、かつ、実施者とは第三者の立場から監査を実施することにより、改善につなげるという方法です。

チェック機能の重要性

継続的なセキュリティマネジメントの実施のためには、経営者が指示したことが適切に行われていることを確認する必要があります。それを保証するのが PDCA の C の部分、つまり点検の部分です。点検し、確認した結果を経営者にフィードバックすることにより不備が是正され、目標が達成されます。とかく日本の会社では、指示を出しっぱなしにする経営者が多いようですが、それではだめです。指示した経営者は、「指示を出しているので実行されているはず」と考えがちです。また、「私は部下を信頼している。わざわざ確認するまでもない。部下を信じられない上司は部下からも信頼されない」と考える人もいるでしょう。しかし、指示をしたからといって必ずしもできているわけではありません。担当者が不正をしている場合もありえます。また、単純にミスをしている場合もあります。**指示の出しっぱなしではなく、指示をしたことを確認することが重要**です。担当者も第三者に確認をしてもらって、問題がないという結論を得たならば胸をはって「指示されたことはできている」と言うことができます。指示をした経営者のためにも、指示を受けた担当者のためにもチェック機能というのは重要なのです。

自己評価と監査（独立的評価）

情報セキュリティ対策等が行われていることを確認する方法には、

- 実施者等が確認する自己評価
- 実施者等と直接的な指揮命令関係のない第三者による独立的評価（

の２つの方法があります。自己評価については、

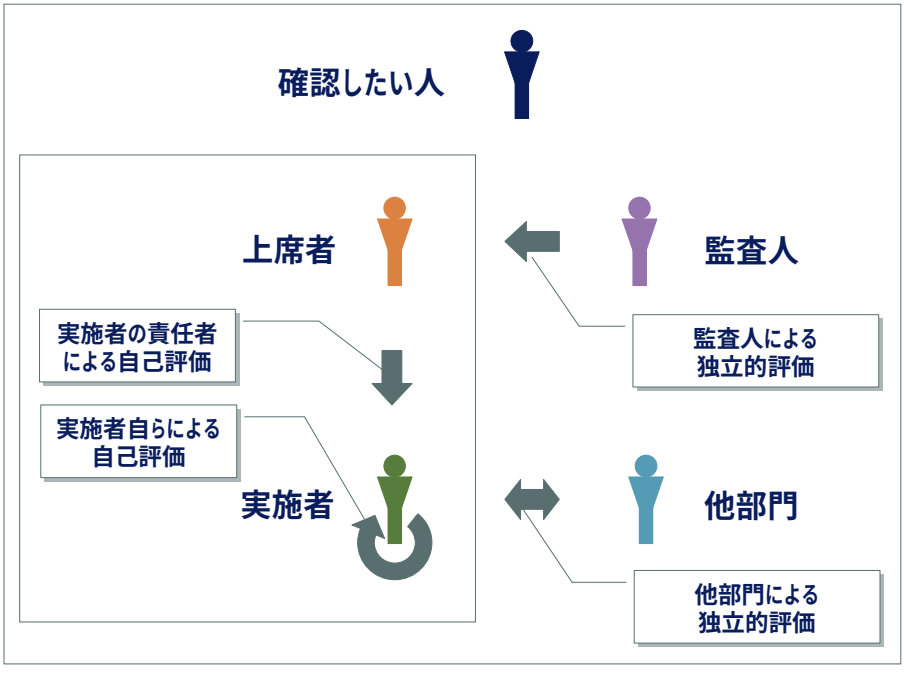
- 実施者自らが確認する自己評価
- 実施者の責任者が確認する自己評価

の２つがあります。

第三者による確認、つまり独立的評価には、

- 専門的に独立して評価をする監査人による確認（監査）
- 別の部門による確認（相互確認）

の２つがあります。



自己評価と独立的評価の長所と短所

自己評価と監査はどちらも対策の実施状況を確認する方法ですが、それぞれ長所と短所があります。自己評価は、自らが確認することですから自分が勘違いをしている場合や不正をしている場合は正しく報告されないことになります。一方、第三者による独立的評価の場合は、実務に精通していない評価者、セキュリティの知識や能力のない評価者による確認が行われてしまう場合があります。

	長所	短所
自己評価	• 実務に精通しているために効率的、効果的に評価することができる	• 不正を見逃す可能性がある • 本人の勘違いにより誤った報告をする場合がある
独立的評価	• 客観的に評価できる。 • 実行者の意図的な不正を発見することができる	• 実務に精通していない評価者が評価した場合、誤った報告をする場合がある • セキュリティの知識や能力のない評価者が誤った報告をする場合がある

両者の長所短所を考えると実務的に両者の短所を補うように組み合わせて実施することが効果的になります。特に**大きな組織な場合は、監査人だけすべてをカバーすることは難しいので自己評価の活用が有効**だと思います。

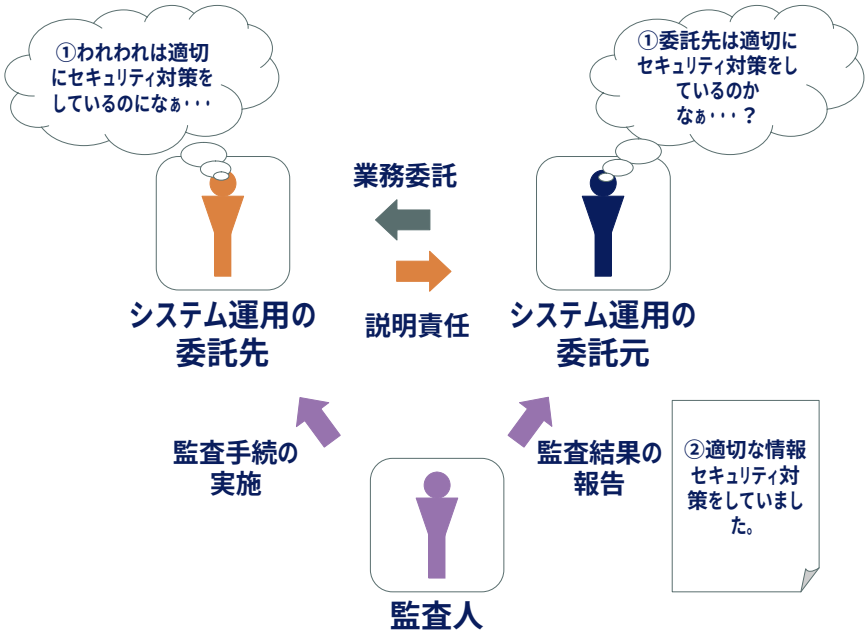
助言型監査と保証型監査

次に監査について、もう少し説明します。監査には改善のための監査と、説明責任を果たすための監査の２つがあります。前者を助言型監査、後者を保証型監査と言います。

助言型監査は、経営者が指示したことが行われているかを確認し、行われていなければその不備を指摘しつつ、不備を是正するための改善案を提示し、**改善を促進させる**ことにあります。助言型監査は、監査人の専門的能力を背景に、客観的な視点での助言が求められるものです。例えば、経営者が自社の情報セキュリティ対策の整備状況が十分か、運用上の問題はないかを確認し、不備があれば改善しようと思っている場合は、専門的の能力に重点をおいて、情報セキュリティ調査や検査をする外部の会社に委託する助言型監査が考えられます。

保証型監査は、利害関係者に対する説明責任を果たすために利用します。保証型監査は、監査の客観的な立場を背景に、専門的能力を活用して情報セキュリティ対策が適切に行わ

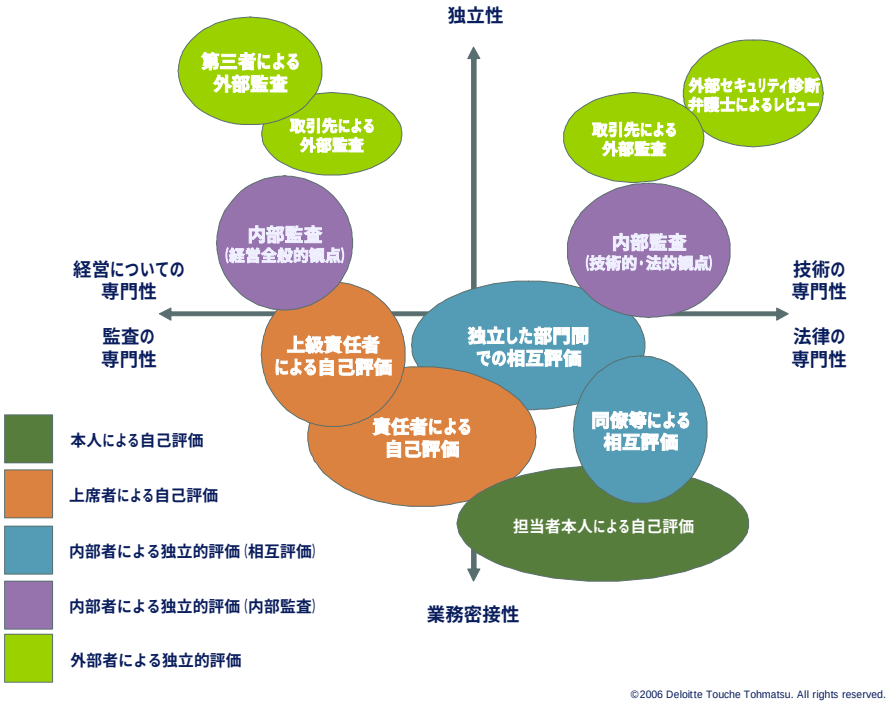
れていること等を評価し、保証します。例えば、情報システムの運用を委託している会社が委託元の会社から情報セキュリティ対策の実施状況についての説明を求められた場合、監査法人等の外部の第三者に監査をしてもらい、問題がないことを報告してもらう保証型監査が考えられます。保証型監査のイメージを図に表すと次のようになります。登場人物が 3 名（図の場合は委託元、委託先、監査人）登場するところが特徴です。



上記の例は、社内の指示を出す人と、指示を受けて実施する人の間でも同じ関係がなりたちます。指示を受けた人が正当に業務を行っていることを監査人が保証することにより、指示を受けた人の説明責任が果たせることになります。

成功のポイント

継続的セキュリティマネジメントの実施には、確認する機能が重要となりますが、今までの話を評価する主体と評価を受ける主体の「独立性の観点」、「評価する主体の専門性」の観点から分類すると次の図のようになります。



それぞれの方法にはそれぞれ長所短所がありますから、うまく組み合わせて実施することが重要となります。

まとめ

今回は、「継続的なセキュリティマネジメントの実施に向けて（２）自己評価と監査で改善につなげる」というテーマで、セキュリティ対策の実施者が自らの実施状況を確認・評価し、かつ、実施者とは第三者の立場から監査を実施することにより、改善につなげることの重要性とそのポイントを説明しました。

次回第 8 回は、「備えあれば憂いなし　災害復旧はまず計画から」として災害復旧計画の立案のポイントについて説明したいと思います。

第 8 回 備えあれば憂いなし　災害復旧はまず計画から

第 7 回は継続的なセキュリティマネジメントの実施に向けて（２）として、自己評価と監査の話をしました。自己評価をベースとして、さらに第三者による監査を受ける方法を説明しました。今回は、「備えあれば憂いなし　災害復旧はまず計画から」として**災害復旧計画の立案のポイント**について説明します。今回の対象は、情報システムの災害復旧計画の立案とします。本来ならば情報システムの災害復旧計画は、事業継続計画の一部として策定されるものです。しかし、今回は災害復旧計画に絞って考えることとします。

地震！・・・そのときあなたは何ができますか

背中に「ドン」と突き上げるような衝撃を受けて目が覚めました。その直後、ガタガタと建物が揺れだし、戸棚から食器が飛び出し床に落ちて割れる音が聞こえてきました。揺れは数分で止まりましたが、まだ床が揺れている感じがします。揺れが止まるとあたりは再び静寂に包まれました。ゆれが収まってからしばらくして、はじめに台所に行きました。食器の半分は床に落ちて割れています。余震があるかもしれないし、停電もしているので片付けるのはあきらめました。とりあえずパジャマにジャンパーを羽織って、マンションから出てみました（当時、尼崎市の武庫之荘に住んでいました。後で知ることになるのですが、震度５か６のようでした）。外では、信号が消えた道（中津浜線）を車がライトをつけながらゆっくりと走っています。他の家からも何人か人が出てきていました。まだ暗いので様子がよくわかりません。寒いこともあって、再び家に戻りました。なぜか突然「水」と思い、お風呂に水をはりました。水洗トイレの水だけでも確保していないと大変なことになると思ったからです。しかし、断水は２週間程度続き、お風呂の水だけでは足りませんでした。7 時前に空が明るくなってきたので再び外の様子を見に行きました。電柱が何本か傾いていたり、アパートや家が崩れていたり、傾いています。これはかなり大規模な災害だろうと直感で思いました。近所の人（普段は同じマンションでもほとんど挨拶しかしませんでしたが）と少し話をしました。とにかくじっとしているしかないだろうということでした。幸いなことにマンションは無事でした。その日は平日でお客さんと会う予定が

ありましたが、会社に行っている場合ではないだろうなと思いました。**まずは、家族の安否確認です。**家族や親戚が、宝塚や東灘区に住んでいました。近くだったの同じような状況になっているだろうなぁと思い電話をかけましたが、混雑していてつながりません（結局、翌日に仙台にいる弟をハブにして連絡がとれました)。電気が止まっているのでテレビがつきません。情報がまったく入りません。近所のコンビニエンスストアに行きましたが、人が結構並んでいたので、あきらめました。しばらく近所を歩きました。救急車、消防車、パトカーが時々サイレンを鳴らしながら走り去りました。古い家やアパートの中には全壊しているものもありました。壊れた家の前で、そこの住民と思しき人が呆然として立っていました。しばらく歩き回った後、再び家に戻りました。

夕方になると幸いなことに電気がきました。真っ先にテレビをつけました。ヘリコプターからの映像です。神戸の町から煙が立ち上がっていました。高速道路がなぎ倒されていました。そのとき始めて神戸で地震があったことがわかりました。「1,000 人以上は死亡者が出ただろうなぁ」と直感で思いました。死亡者や負傷者の数が各市町村区別に発表されていました。親戚のいた東灘区の死亡者の数も、最初はわずか（わずかでもないのですが）数十名だったと思います。「この人数ならたぶん入っていない。」と思いました。しかし、時間がたつとどんどんと死亡者の数が増えていきます。100 名を超えました。「大丈夫だろうか」。電話もつながらないので安否がわかりません。**死亡者の数が増えるたびに不安になり落ち着きません。**（結局、東灘区だけでも死亡者は約 1,500 名となりました)。その日は不安の中、早めに布団にもぐり寝ることにしました。時々余震がありましたが、本震以上の揺れはないだろうと自分に言い聞かせました。地震当日はお菓子と食パンだけを食べたように思います。

翌日、再び目を覚ましました。朝方に台所の食器の破片を片付けました。半分くらいが割れていました。しかし、家があるだけましでした。昼くらいには水が止まりました。マンションの貯水槽にある水がなくなったのです。武庫之荘の駅まで歩いていきました。途中、何軒か家やアパートが半壊、または全壊になっていましたが、テレビでみる惨状と比べると、かなりましだなぁと思いました。でも、駅前のマンション（８階建くらいだったと思います）の１階の駐車場部分が完全につぶれているのを見てびっくりしました。「倒れないのだろうか」。このマンションはしばらく、そのままの姿でたっていました。武庫之荘の駅につくと、なんと電車が走っていました。会社にいけるなぁと思いながら家に戻りました。しかし、家に戻ると相変わらず、水道もガスも止まっていました。

結局、２０日に会社には行きました。線路から見える家々でも被害を受けて傾いている家がいくつかありましたが、大阪に行くにつれて傾いた家も減っていきました。大阪は多少バタバタとしていましたが、何事もなかったかのような様子でした。会社の同僚とは、お互いの安否の情報を聞きました（幸いなことに、最終的に全員無事であることが確認できました)。大阪では、普通に生活ができます。水も当たり前のように出ます。ガスも来ています。でも、戻ると水もガスもない生活です。幸いなことに鉄道がつながっていましたので、いざとなれば大阪に行けました。その後、親戚、友人やその家族などの安否がじ少しずつわかってきました。結局、知り合いで亡くなったのは一人だけでした。会社の有志が夙川や神戸で被災した会社の人に水を送りに行ったりしました。

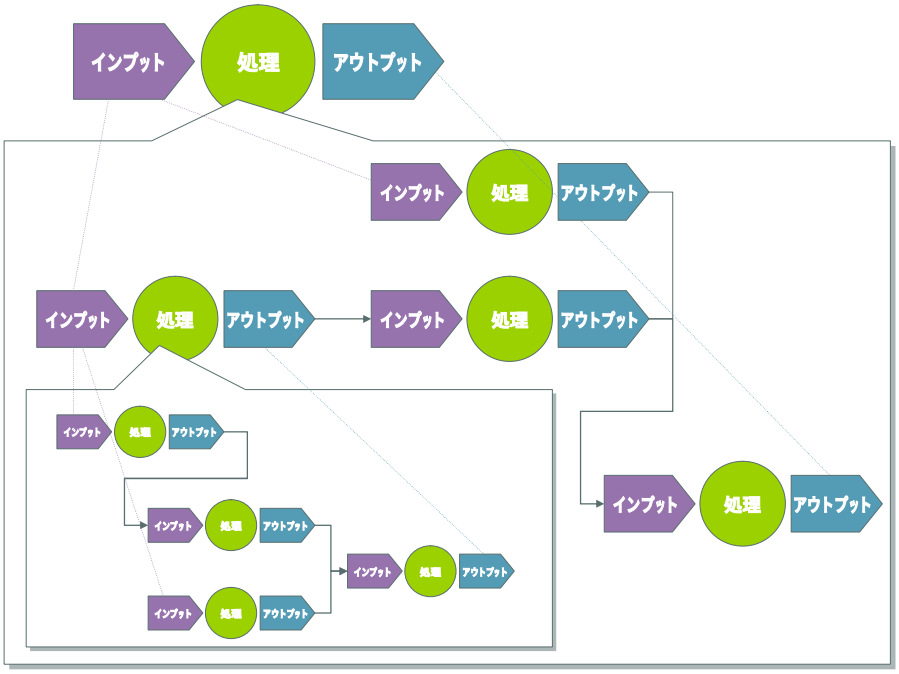
翌週には、被害が激しく交通の便が悪い地域に住んでいる人を除きほぼ全員通勤してきました。

災害復旧計画を立案するまえに・・・

(1) ある機能を実現させるプロセスとその連鎖

災害復旧計画を考える場合に重要なことは、**事業はその目的を達成するための機能の集まりと考え、機能とその機能間の連鎖を復旧させること**と考えることです。

機能を実現することは、プロセスからアウトプットを生み出すということです。アウトプットを生み出すためにはインプットと処理が必要となります。ひとつの処理はさらに複数の処理の連鎖に分解することができます。つまり、ある処理は、複数の処理の連鎖の階層から成り立っているといえます。このような入れ子関係は、極端に言えば CPU 上の電子レベルの振る舞いにまで分解できますので、実務的には目的が達成できる対策が決められるレベルでこのような分解は終了します。



機能を実現するためには、インプットを確保し、正しい処理ができるようにする必要があります。インプットの確保ができなかったり、処理が正しく行われなかった場合、期待されたアウトプットはでないので、プロセス全体として機能不全に陥ることになります。

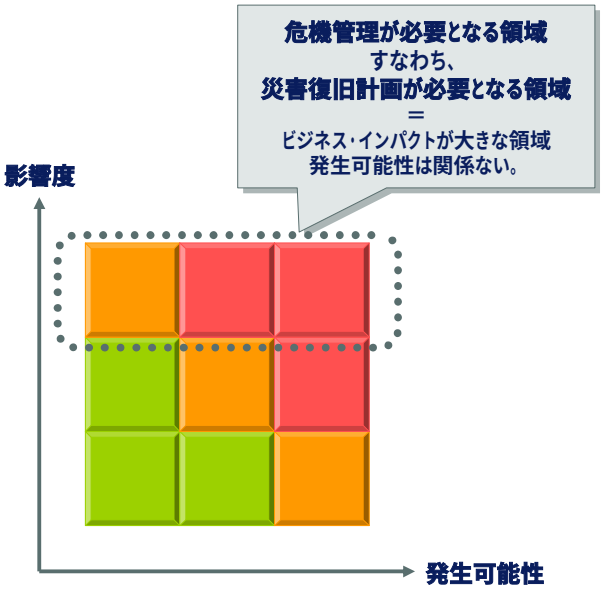
このように考えれば、災害復旧計画は、機能を実現するためのインプットが絶たれ、又は、正しい処理ができなくなった場合の対応手順を備えるということになります。一般的には、代替的なインプットをどのように確保するのかということが重要になります。

データセンタで行われているデータ処理に必要なインプット（例えば、電力、要員、通信回線、情報）が絶たれた場合にどのようにして、そのイ**ンプットを回復させたり、代替させることができるのか**ということを考えることになります。

(2) 災害復旧計画が必要となる場合

災害復旧計画は、どのようなリスクが顕在化した場合にたてるべきでしょうか？災害復旧計画は、危機管理の一部です。危機管理では、重大な損失につながる事象が発生した場合にいかに損失を少なく抑えるかが重要となります。したがって**災害復旧計画は、発生可能性が少なくても影響度が大きな事象の発生に備えて策定すべきです。**災害復旧計画の立

案にあたっては、ビジネスインパクト分析を行いますが、それはまさにどのような事象が起こった場合に影響が大きいのか、つまり危機管理が必要となる分野を特定するために行われるのです。

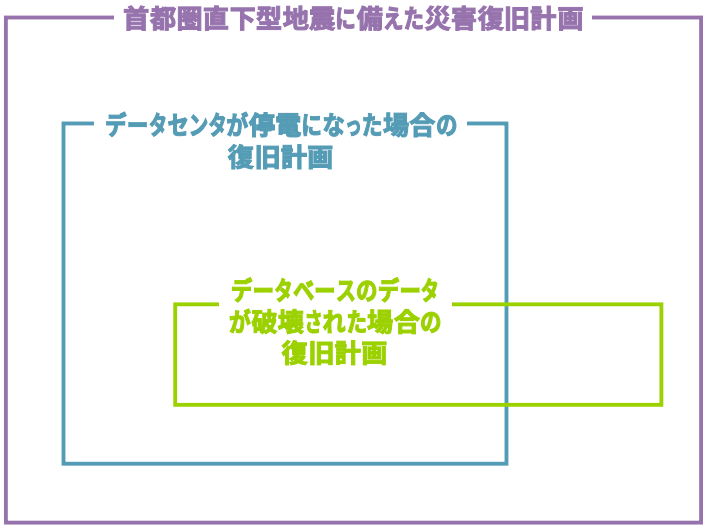


インターネット通信販売のみで営業を行っている会社の場合は、コンピュータ機器の故障により注文受付ができなくなるということは、事業に与える影響が非常に大きいといえます。したがって、コンピュータ機器の故障による注文受付ができなくなる場合の対策をあらかじめ考え、そのような自体に直面した場合の復旧計画を立案することが重要となるでしょう。

また、災害復旧計画を考える場合はどのような事象が発生した場合に、どのようなことがその後起こるのかを想定していくことが重要となります。例えば、首都直下型地震が発生し、首都機能が麻痺した場合に備えた災害復旧計画を立案するのか？それとも、データセンタが停電になった場合の対応計画を立案するのか？、データベースのデータが破壊された場合の復旧計画なのか？その対象を明確にする必要があります。

一般に、**大きな災害に対する復旧計画は、より小さな事故等からの復旧計画を含みます。**首都直下型地震が発生した場合に備えた災害復旧計画には、データセンタが停電になった場合の復旧計画や、データベースのデータが破壊された場合の復旧計画も含まれることに

なります。



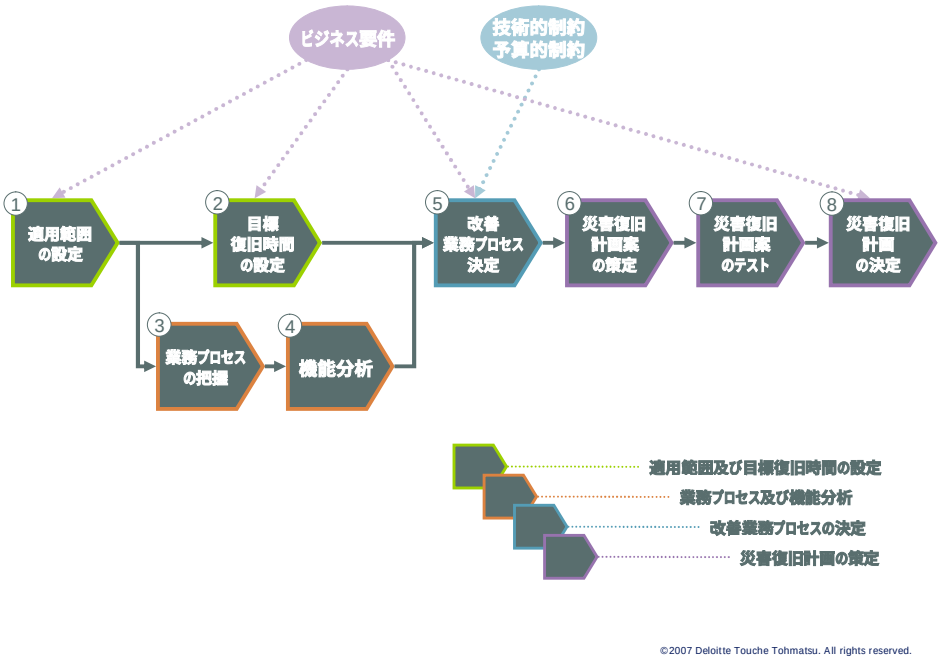
このような関係を理解すれば、おのずとわかってくることがあります。それは、データベースのデータが破壊された場合の復旧計画が存在しないのにいきなり首都圏直下型地震に備えた災害復旧計画を立案することは困難ということです。

次にどのような考え方で災害復旧計画を立案すればよいのかを説明することにします。

災害復旧計画の立案手順

災害復旧計画、事業継続計画等の策定手順については、内閣府の事業継続ガイドライン、経済産業省の事業継続計画(BCP)策定ガイドライン、中小企業庁の中小企業 BCP 策定運用方針、英国規格の BS25999 事業継続管理のためのガイドライン等の様々な参考資料がありますので参考にしていただきたいのですが、ここでは、次の４つのプロセスに分けて災害復旧計画の立案手順を示します。

1. 適用範囲及び目標復旧時間の設定
2. 業務プロセス及び機能分析
3. 改善業務プロセスの決定
4. 災害復旧計画の策定



(1) 適用範囲及び目標復旧時間の設定

災害復旧計画を定める範囲及び、**目標とする復旧時間の設定**を行います。これは、ビジネスの観点から行われることになります。例えば、東京都江東区にあるデータセンタの情報処理サービス機能を災害復旧計画の範囲と定義し、その機能が停止した状況から目標復旧時間内に復旧するための災害復旧計画を立案することになります。なお、データセンタの情報処理サービス機能の中でも緊急性が高いものと高くないものがありますので、目標復旧時間は複数設定することもありえます。例えば、月末に行われるバッチ処理の機能は、月初であれば緊急度が高くありません。一方オンライン処理されるものは、緊急度がより高いでしょう。したがって、目標復旧時間を複数設定することにより、緊急度の高い機能をより早く復旧するような災害復旧計画を立案することになります。

(2) 業務プロセス及び機能分析

適用範囲となる機能を実現する**業務プロセスを分析**していくことになります。まず業務

プロセスに含まれる活動を識別します。その活動に含まれるインプット（経営資源等）、処理、アウトプットを把握します。次にそれぞれの活動の依存関係を分析します。その際に、リスクに対して実施されている対策も併せて識別し、**シングルポイント（二重化されていない部分）の識別、クリティカルパスの識別**をします。

(3) 改善業務プロセスの決定

現在の業務プロセスを改善せずに災害復旧計画を立案することは通常ありません。業務プロセス及び機能分析の過程で改善すべきポイントが識別されますので、それを改善したのち又は改善しながら災害復旧計画を立案することになります。

(4) 災害復旧計画の策定

災害復旧計画は、**テストによる検証**をして、問題点がないことを確認し、確定します。情報システムを開発する場合と同じです。このように新しいプロセスが適切に機能するかどうかはテストしてみなければわかりません。テストの手法には机上テストと実地テストがあります。その実効性が非常に問われることになるので、実地テストをし、テストの過程で発見された問題点を改善しながら最終的に承認を得て災害復旧計画を確定させることになります。

成功のポイント

機能が停止したときに確保すべきインプットは何か、それをどのように確保するのか、そして、**テスト**をしなければなりません。災害復旧計画の文書は必要となります。しかし、実効性のない文書は意味がありません。テストはしっかりとしてください。そうすると本当に重要なことが見えてくると思います。成功のポイントとして、本当に重要なことを最後に説明したいと思います。

本当に重要なことは、**従業員等に対する愛情**です。人がいなければできないことが非常

に多いです。**安否確認システム**を必ず導入してください。安否がわからなければ、その後の災害復旧計画は意味がありません。次に、いつ仕事に復帰できるかの情報を確実に入手することです。本人は元気でも家族や親族が被災していれば会社にはいけません。近所の人が被災していれば、近所で救援活動を手伝っているかもしれません。最悪の状況になった場合は、おそらくどんな事業継続計画も無意味かもしれません。

そういう観点からいえば、できるところから少しずつ災害復旧計画を立案することが重要です。まずは、安否確認システムが有効に機能するかテストをする。データバックアップのリカバリー計画や、停電時のバックアップ用発電機への切り替え計画などを立案し、それが確実に行えるかテストをする。それらの結果から問題点を抽出し、改善していく。そういう地道な災害復旧計画を策定し、テストを繰り返すほうがよいと思います。それらが確実にできるようになってからより総合的な災害復旧計画を立案していく。

極端に最悪なシナリオに従って事業継続計画を立案することも必要かもしれませんが、まずは**足元を固めること**が重要です。

まとめ

今回は、「備えあれば憂いなし　災害復旧はまず計画から」というテーマで、災害復旧計画の立案のポイントを説明しました。

次回第９回は、「新しいリスクへの対応」について説明しようと思います。

第 9 回　新しいリスクへの対応（変化するリスクに対応する）

第 8 回は「備えあれば憂いなし　災害復旧はまず計画から」として災害復旧計画の立案のポイントについて説明しました。機能を復旧させることが重要であり、その機能を生み出す資源、とりわけ人が重要であること、できる部分から災害復旧計画を立案することが重要であること、文書の策定より訓練に時間をつかうことなどを説明したつもりです。今回は、「**新しいリスクへの対応（変化するリスクに対応する）**」として、変化するリスクにどのように対応すればよいのかについて考えてみたいと思います。

IT は発展途上？変化がはやい

情報セキュリティマネジメントはリスクマネジメントの一部です。そういう意味では、現金が従業員に着服されるというリスクを考え、そのリスクに対してどのような対策を導入すべきかを考えることと大差はありません。情報セキュリティがちょっと特別であるのは、IT に関係する部分が大きいということです。IT について重要な点は、**変化が速い**ことです。新しい IT がつぎつぎと生まれます。また、IT を利用した新しいサービスも次々と誕生してきています。

新しいソフトウェアは便利かもしれませんが、十分なテストが実施されずにバグが残ったままリリースされているかもしれません。特にそのバグが管理者権限をのっとることができるようなバグであれば、セキュリティ上の問題となるでしょう。

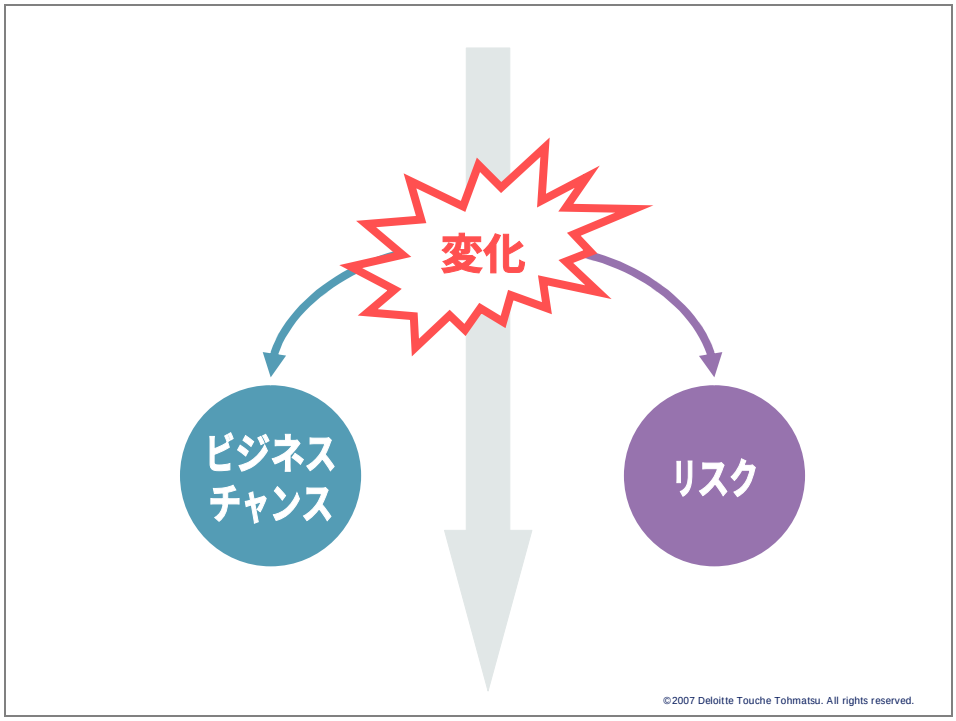
新たなサービスもこの数年で大きく増えました。ウェブメールは大変便利なサービスです。どのパソコンからも ID とパスワードによりメールを受送信することができます。しかも、無料でこのようなサービスを提供している企業も多いですね。しかし、ウェブメールを利用した意図的な情報漏えいをどのようにして予防するのか、また、どのようにしてそれを発見すればよいのかという新たな情報セキュリティ上のリスクも生じました。ウェブメールを読んだ際に一時的に保存された添付ファイルがインターネットカフェのパソコンに消去されずに残ってしまうかもしれません。

また、最近始まったサービスとして、ソーシャルネットワークがあります。ソーシャル

ネットワークはある程度閉じたネットワークを前提としていて、仲間うちで日記を交換したり、メールを送受信したりできます。自分の日記を公開できる範囲を自分の友人、友人の友人までと明確にできたりします。しかし、このようなソーシャルネットワークの中で、次のような事件がおこりました。ある企業の男性社員が彼女の裸の写真をソーシャルネットワーク内の日記に載せてしまいました。それが話題となりました。その男性社員の名前が明らかにされ、会社名もでてしまいました。結局、男性社員は会社から去ることになりました。会社としても決してよいイメージが消費者に残ったとはいえません。また、インサイダー情報や企業秘密と思われる情報がソーシャルネットワーク内の日記に書かれたりする場合もあるようです。

変化が生じるところにチャンスとリスクあり

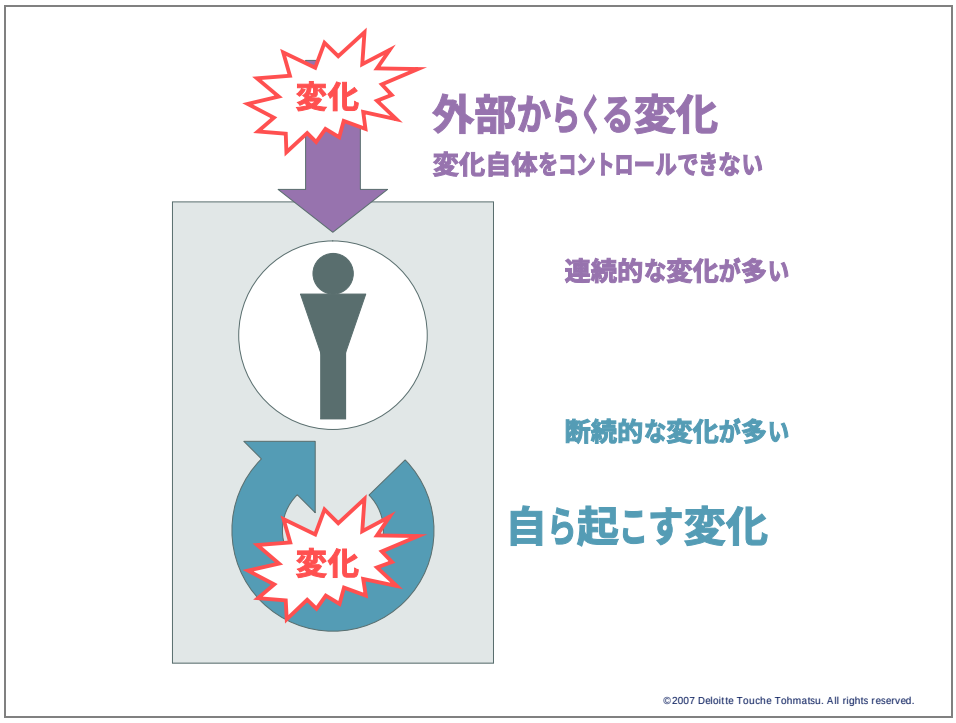
このような新しいサービスが生まれることより、ビジネスチャンスが広がります。しかし一方、変化は新たなリスクも生みだします。**チャンスとリスクは双子のようなもの**です。変化が生じたら新たなリスクを識別する。これが重要です。



さて、このような変化は、自ら起こす場合もありますが、外部からくる場合もあります。

変化を自ら起こす場合は、変化が起こることが事前に想定できるので変化するタイミングでリスクを識別し、必要となるキュリティ対策を実施することになります。たとえば、ウェブアプリケーションを利用した消費者向けの販売サイトを立ち上げた場合、クロスサイトスクリプティング等の脆弱性に気をつける必要があり、そのための情報セキュリティ対策を設計し、導入する必要がでてきます。システム開発を外部委託する場合は、委託に伴う新たなリスクを識別して、対処しなければなりません。

外部からくる変化は変化自体を自らコントロールできません。したがって、まず変化を識別することが重要となります。変化には**断続的な変化**と**連続した変化**があります。外部環境の変化はあまり断続的に変化しないので、気づかないうちにリスクが少しずつ増大しているということもありえます。

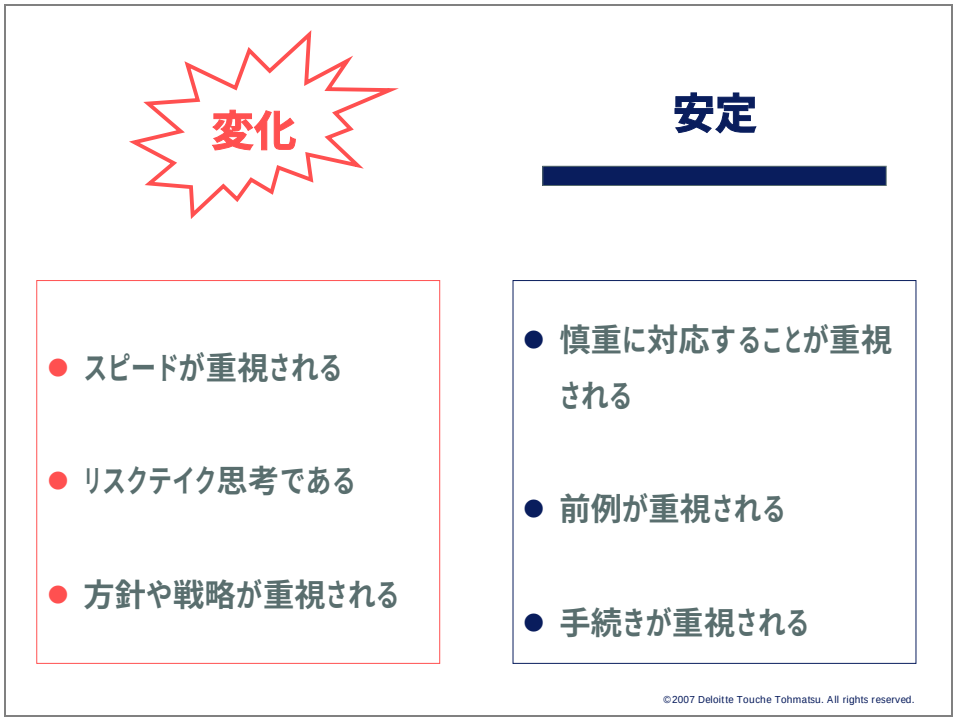


たとえば、外部記憶媒体の大容量化にともなうリスクの変化を考えてみましょう。10 数年前の外部記憶媒体はフロッピーディスクという 1.4Mb ほどの容量しかありませんでした。しかし今では、USB ポートにさせば数 Gb の容量の情報を保存できる USB メモリーがあります。何千万人分の個人情報の抜き取りなんてできないと思っていたら、それ以上の個人情報が胸ポケットに入ってしまう時代です。10 年前であれば、コンピュータルームの大きな場所を占めていた数十ギガバイトのハードディスク装置も、手のひらにのる大きさになりました。事故がおこってから、「確かに、大量の個人情報が USB メモリーを使うことによっ

て抜ける。」と気づいても遅いわけです。「変化が生じるとリスクが変わる」。どのような変化がおこっているのか、どのような変化をしようとしているのか、それについてどのようなリスクが新たに生じて、どのようなリスクが少なくなっているのかを常に考える「クセ」をつけることが重要です。このような**「クセ」をつける**ことは、日ごろの意識付けで養っていくことが重要です。

変化に追従できるマネジメントスタイルが重要

次に IT は変化が速いということが、マネジメントスタイルや対策を立案するときにどのように影響するのかについて考えてみることにします。IT の変化について組織運営も追従できなければなりません。もともと**変化が速い業界では、変化への対応できるようなマネジメントスタイルがとられている**はずです。変化に対応できるようなマネジメントスタイルでは、たとえば、「スピードが重視される」、「リスクテイク思考である」、「方針や戦略が重視される」といった特徴があります。一方、変化が少ない環境に最適化されたマネジメントスタイルでは、「慎重に対応することが重視される」、「前例が重視される」、「手続きが重視される」といった特徴があります。どちらのマネジメントスタイルがよいという問題ではなく、環境に応じた適切なマネジメントスタイルがあるわけです。今まで変化の少ない環境にあり、それに適したマネジメントスタイルをとっていた組織は変化への対応力が弱く、情報セキュリティマネジメントが十分にできないかもしれません。注意する必要があります。



情報セキュリティマネジメントが適切にできなければ、適切なセキュリティ対策もとれません。次に対策を考える上でのポイントを説明します。

対策を考える場合はリスク指向の原則ベース

結局、情報セキュリティ対策を考える場合に重要となることは、変化が速い IT 及び IT を利用したサービスの変化を識別し、その変化から生じる新たなリスクを把握し、対策をとり続けることです。変化が速い場合の対策のポイントは

1．　**リスク指向**

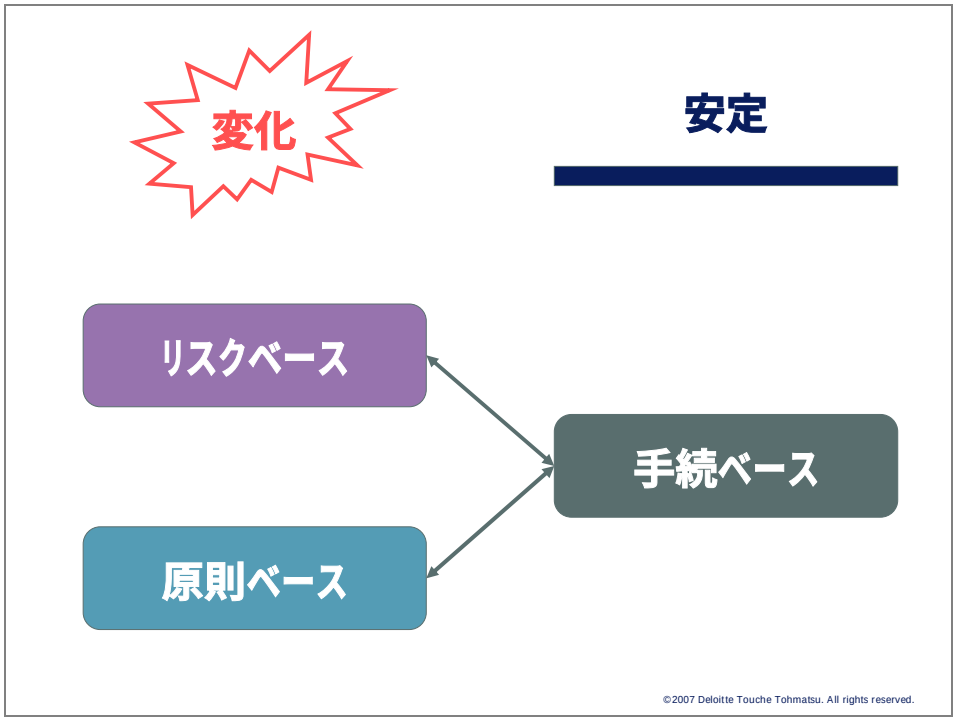
2．　**原則ベース**

です。

リスク指向というのは、どのようなリスクがあるからどのような情報セキュリティ対策を採るべきかという、対策をとるための目的であるリスクを常に意識することです。

次に原則ベースというのは何でしょうか。原則ベースというのは、英語では Principal Base といいます。対比される概念は、手続ベース、Procedure　Base です。IT 及びそれを利用したサービス等の変化が速いのでリスクも当然変化が速いわけです。変化するリスク

に適時に対応するためには、手続レベルではなくその手続を規定するより上位概念である原則ベースでものごとを考えるべきです。たとえば、社内のネットワークに接続する場合は 8 文字以上のパスワードにより認証するということに重きを置くのではなく、社内のネットワークに接続する場合は適切な方法で本人を認証しなければならないということに重きを置くべきです。



想像力が重要

　個人レベルでは、リスクについて意識するクセが重要となりますが、同時に**想像力も働かなくてはなりません**。たとえば、サーバ管理を迅速にするために「データセンタ内のコンソール端末による管理から、管理者のノートパソコンを使ったリモート管理に変更する」場合を考えてみましょう。変更前のコンソール端末はデータセンタ内で物理的に保護されていたわけですが、変更後のコンソール端末は管理者のノートパソコンであり、物理的な保護というのは無い状況となっています。そうすると、ノートパソコンを紛失（電車への置き忘れ、ひったくり、家で盗難される等）する可能性が生じ、可用性及び機密性の観点から新しくリスクが生じることになります。変化についてどのようなリスクが新たに生じ

るかについては、想像力を働かせる必要がありますが、想像力を働かせるためのポイントは、タブーを設けずに自由に考えることです。たとえば、上記を例について私が思いついたリスクをそのままに羅列してみます（すべてのリスクを網羅的にあげているわけではありません）。

１．ノートパソコンのテンキーの下にキーロガーを仕掛けられ、認証パスワードが漏えいする。
２．自宅の無線ＬＡＮが盗聴又はケーブルタッピングされ、認証パスワードが漏えいする。
３．喫茶店で PC を利用している際に、ショルダーハッキングされて認証パスワードが漏えいする。
４．誤って不正なソフトをダウンロードし、サーバ等の設定情報が漏えいする。
５．自宅で空き巣にあい、PC が盗まれ ID とパスワードが解析されえて判明してしまう。

この例は、ノートパソコンに関するリスクなのでそれほど難しくないかもしれません。皆さんも次のような変化が起こった場合にどのようなリスクが新たに生じるか想像してみてください。変化についてはレベル感が異なるものを整理せずに並べています。

- 在宅勤務を認める
- 事務所の端末をデスクトップ型からノート型に変える
- シンクライアントを導入する
- 部門毎に職場に設置していたファイルサーバを廃止し、すべてデータセンタのサーバに変える
- 構内のＬＡＮを無線ＬＡＮに変える
- シングルサインオンを導入する
- 会社の基幹システムを汎用機からウェブベースのオープンシステムに変える
- システム運用子会社を売却する

まとめ

今回は、「新しいリスクへの対応（変化するリスクに対応する）」というテーマで、「変化に対応することが重要である」ということを中心に説明しました。

次回第 10 回は最終回です。今までのまとめという意味も含めて「ヒトに始まりヒトに終

わる」と題して、ＩＴ技術がどこまで進歩しようが情報セキュリティの問題も最後はヒトの問題であることを説明しようと思います。

第 10 回　人に始まり人に終わる　エラーや不正を防ぐために・・・

第 9 回は「新しいリスクへの対応（変化するリスクに対応する）」として、変化するリスクにどのように対応すればよいのかについて考えました。IT は変化が激しいので、その変化にタイムリーに追従できるマネジメントスタイルが情報セキュリティマネジメントでは重要となります。またセキュリティ対策は、リスク指向の原則ベースで考えることが重要となります。変化するリスクを考える場合には、タブーを設けずに想像力を働かせることが重要となります。このように変化への対応が情報セキュリティマネジメントでは大切になります。さて、最終回となる第 10 回はふたたび人に焦点を当て、エラーや不正を防ぐためには何に気をつけないといけないかを説明します。

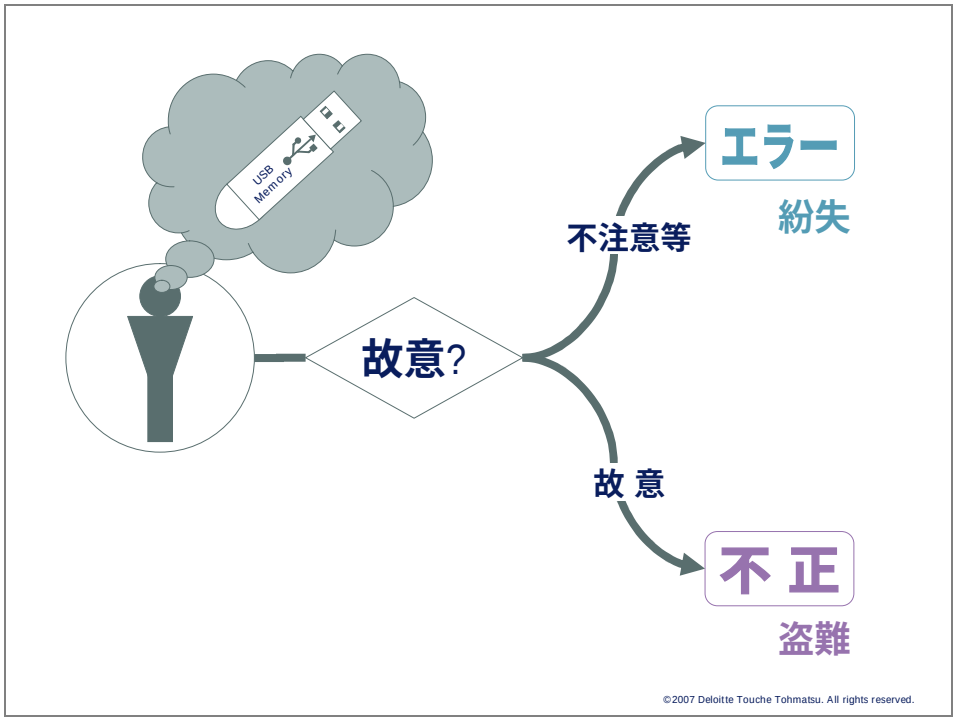
本能に逆らったことを当たり前のようにするために（エラーや不正が起こらないように）

この連載コラムは個人の生物的な存続、社会的な存続の可能性を高めるために情報を収集しようとすることは本能であり、情報を保護することと相容れない部分があるという話からはじめました（第１回）。本能に逆らうことを自然に行わせるためには、「風土作り」と「仕組作り」が両輪となって機能しなければならないという話をしました。「風土作り」は仏に魂を入れること、「仕組作り」は仏を作ることに似ています。仕組みを作るのも人間ならば、それを守るのも守らせるのも人間です。コンピュータが自動的にセキュリティ対策をするとしても最後はやはりどこかで人間が関与しなければならないわけですから、まさに情報セキュリティは人に始まり人に終わるわけです。**人である以上必ず誤り（エラー）をします。また、場合によっては意図的に情報漏えいをしたり改ざんをしたりするかもしれません。**個人情報を漏えいした企業の方が、「内部者による不正は防ぎきれない」とつぶやいていたのが記憶に残っています。もちろん、人間のエラーや不正を 100%防ぐことは無理です。しかし、できる限り減らすようにすることは可能です。そして常にそれをしつづけることが重要です。最後はやはり人が砦となりますから人に焦点をあてた対策を考えることが重要です。エラーや不正による漏えい、改ざん等を起こさないようにするためのポ

イントを最終回としてまとめたいと思います。

エラーと不正は対策が異なる

はじめに、エラーと不正の違いについて整理しておきます。**エラーと不正の違いは、意図的であるかどうかということです。**意図的に情報を漏えいさせるのは不正、意図的ではなく漏えいしてしまったのはエラーとなります。情報漏えいはエラーでも不正でも起こります。しかし、対策を考える場合は、エラーに対する対策と不正に対する対策は別々に考えるべきです。



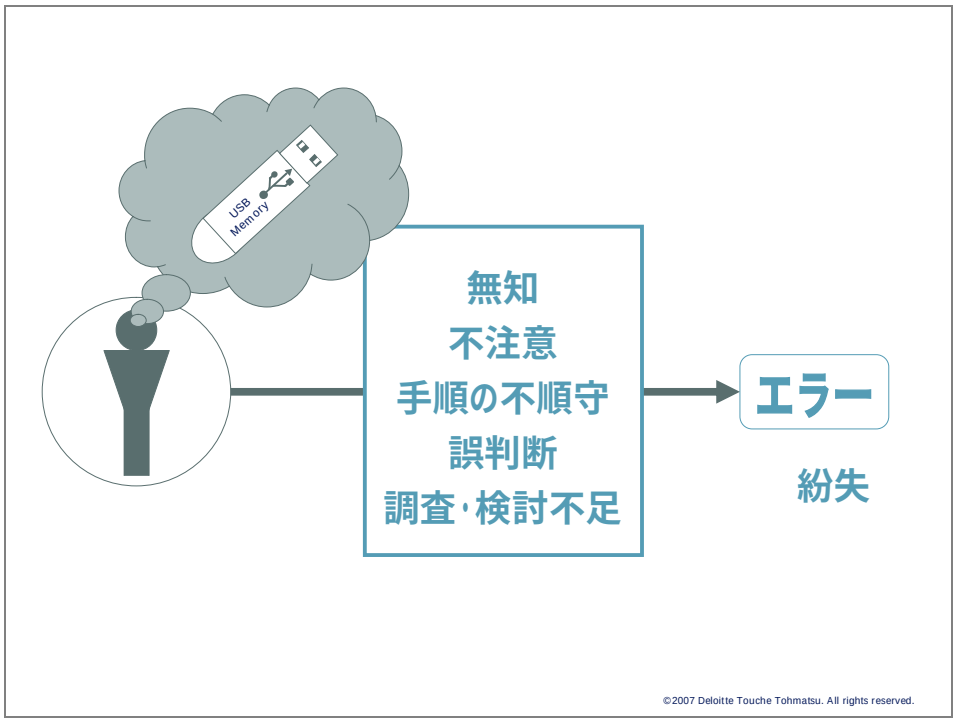
エラー対策には教育・訓練と仕組みのセットで行う

個人に起因するエラーの原因には、主に

- 無知
- 不注意

- 手順の不順守
- 誤判断
- 調査・検討不足

などがあります（JST　畑村委員会作成）。これらは**教育や訓練を行うことによりある程度防ぐことができます。**しかし、さらに**仕組みとしてこれらの原因が起こりにくくすることが重要です。**人間はどれだけ注意をしていても不注意でエラーを起こすことはあるし、誤った判断をすることがあるからです。



USB メモリー等に個人情報を格納し紛失するというエラーを起こさないようにするためには、そもそも USB メモリー等の紛失をしないように注意をするだけでなく、USB メモリー等が紛失しにくいように USB メモリー等を必ず首からぶら下げるようにするという方法も考えられます。USB メモリーは小さいので紛失しやすいということを理解していれば、そもそも USB メモリーに情報を保存できないように PC を設定したり、必ずシステム的に USB メモリーに保存する場合には暗号化するような仕組みを導入することも効果的でしょう。また、エラーが起こる前には必ず「ひやりはっと」事例があるものです。たとえば、「USB メモリーがかばんの中に無かった。でも、よく探したら机の引き出しに無意識に入れていた」といった事例です。このような事例を積み重ねることにより、USB メモリーは首にかけると

いう方法を考えることができるようになります。USB メモリーの例はわかりやすいですが、たとえば退職者の ID を消去し忘れたということがあった場合には、必ず人事部門から情報システム部が連絡をうけて ID の有効期限を退職日に設定し、その設定した結果を人事部門に戻し、人事部門が退職日の諸手続きの中で確認するという仕組みを導入することにより退職者の ID の消去を確実にできるようになります。このように、**「ひやりはっとデータベース」や「失敗事例データベース」を構築することにより同種同類の失敗の再発を防止できるようになります。**

コラム１：「高名の木登り」

徒然草【百九段】

高名の木登りといひし男、人を掟てて高き木に登せて、梢を切らせしに、いと危く見えしほどは言ふ事もなくて、おるゝ時に、軒たけばかりになりて、「あやまちすな。心して降りよ」と言葉をかけ侍りしを、「かばかりになりては、飛び降るとも降りなん。如何にかく言ふぞ」と申し侍りしかば、「その事に候ふ。目くるめき枝危きほどは、己れが恐れ侍れば申さず。あやまちは安き所になりて、必ず仕る事に候ふ」と言ふ。

本当に重要な情報はそれを取り扱う人が慎重に対応するために案外適切に取り扱われているものです。本当に重要な情報を誤って漏えいさせるようなことは案外起こりにくいものです。むしろ危ないのは、普段当たり前のように使っているそれよりもちょっと重要性の低い機密情報かもしれません。たとえば、人事評価情報は誰でも気をつけて取り扱いますが、重要な経理情報を案外ぞんざいに取り扱っている場合があります。本当に重要な情報は大切に取り扱うが、普段何気なく使っている重要性がちょっと落ちる機密情報の取り扱いにむしろ注意することが重要かもしれません。

コラム２：「才子、才に倒れる」

優れた才知を持っている人は、自己過信に陥ってとかく失敗するものである。

組織には、PC スキルの高い人が何人かはいるものです。知識も十分あり、普段は適切な対応できています。しかし、人間である以上誤りはあるものです。特にスキルの高い人は、心の油断から思わぬ事故を起こす場合があります。また、IT 環境は変化が早いですから知識の陳腐化しやすいです。昔は PC スキルが高く情報セキュリティに対する知識が豊富だったかもしれませんが、今はそうでないこともありえます。したがって、どんなにスキルが高い人であっても一定の教育・訓練を受けることは必要であり、重要です。

不正対策は、動機、環境、正当化の３つがポイント

そもそもアクセス権限を持った人が個人情報をサーバから USB メモリー等にコピーし、持ち出すといった事件がよく起こります。いわゆる内部犯行と言われるものです。このような意図的である不正を防ぐためにはどうすればよいかが常に問題となります。

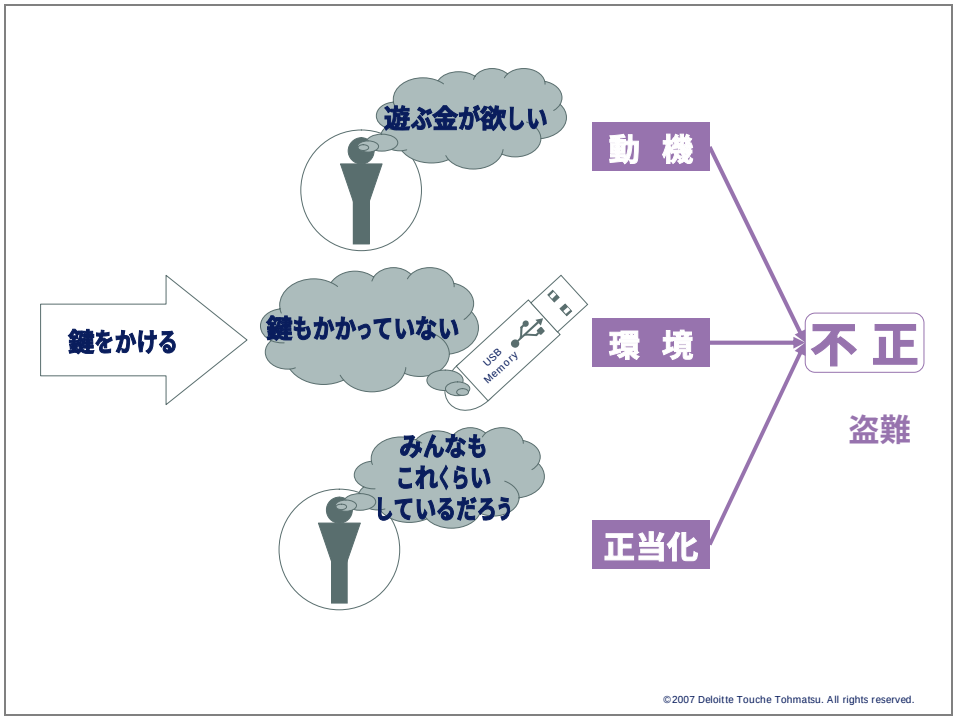
まずは、仕組みで担保する方法から考えます。不正の防止を仕組みで担保する方法の一つが、デュアルコントロールという方法です。必ず二人そろわなければ何かをできない仕組みです。たとえば、核ミサイルの発射ボタンは二人が同時にスイッチを起動しないと発射できない（と、映画では見ましたが本当のことは知りません。）という仕組みです。当然、二人が共謀すれば不正が起こるわけですが、一人でするよりもかなり不正が起こる確率は減ります。しかし、頻繁に行われる作業においてこのようなデュアルコントロールを導入するのは実務的に無理があります。そこで、**動機、環境、正当化という３つのキーワードを使った不正を防止する方法**を考えましょう。

一般に不正は、

- 不正を起こす**動機を持つ人**、
- 不正をすることが**できる環境**、
- 犯した不正を**正当化できる状況**

がそろえば起こりやすいといわれています。たとえば、「遊ぶ金が欲しい」と思っている人がいて、「会社の机の上に 100 万円の札束がおいてあり、だれも見ていないし、誰がとったか気づかない」という環境があって、「いつもサービス残業でこき使っているんだからこの

くらいのお金をもらって当然」という正当化できる状況がそろっていれば、おそらく机の上の 100 万円の札束はとられてしまうでしょう。



注意しなければならないのは、この中で**会社側が直接コントロールできるのは「環境」だけ**であることです。お金を金庫に入れるといった方法をとることにより不正が起こせない環境を作ることができます。しかし、完全にはできないことがあります。そこで、直接的ではないが、**「動機」を抑止する**といった方法をとることが考えられます。たとえば、ビデオカメラが設置されていて、盗むと必ず見つかって必ずつかまるということがわかっていれば、100 万円は取られにくくなるでしょう。最後は、「正当化」です。自分が行っている不正を自分の中で正当化できる状況をなくすということです。たとえば、きれいな壁には落書きをしづらくても、あちこちのかべに落書きがあれば、「ちょっとくらい落書きをしてもいいや」という気持ちになり落書きをしてしまうということです。「1 枚の割れたガラスを放置しておくと、他のすべての窓ガラスが割られてしまう」というブロークンウィンドウズ理論は正当化と関係があるでしょう。誰もが情報セキュリティ規定を遵守している状況であれば、一人だけ規則を破るのは難しくなるでしょう。しかし、多くの人が守っていないルールは「赤信号、みんなで渡ればこわくない」ということで、誰一人守らなくなります。

まとめ

最終回の今回は、「人に始まり人に終わる　エラーや不正を防ぐために・・・」というテーマで、エラーと不正を防ぐためのポイントを中心に説明しました。

ＩＴがどこまで進歩しようが最後に情報セキュリティを担うのは人です。もちろん、人が起こすエラーを減らすためにＩＴを活用して有効かつ効率的にセキュリティ対策をすることは重要です。しかし、人の問題を解決しなければ最後の最後で情報セキュリティは維持できません。**「人は城　は石垣　人は堀」。その人に働きかけるのは経営者です。経営者が積極的に情報セキュリティの維持にとりくまなくては情報セキュリティの問題は解決しません。**

これまで 10 回にわたって情報セキュリティについて連載してきました。すべてを言い尽くせたわけではありませんが、みなさんのお役に少しでも立てれば幸いです。私が今まで述べてきたことは、どれだけ技術が進歩しても普遍的な問題です。そして、情報セキュリティ以外の経営課題についての対応にも参考になることだと思っています。

長い間、お付き合いいただきありがとうございました。

以　上

修正履歴

2010 年 03 月 05 日　公開