企業における情報セキュリティリスクマネジメント
（暫定稿 2008/4/4）

財団法人日本情報処理開発協会

情報セキュリティ総合的普及啓発シンポジウム

2008 年 2 月 21 日（木）

講演 5 「企業における情報セキュリティリスクマネジメント」

情報ネットワーク法学会（IN-Law）

佐藤　慶浩（日本ヒューレット・パッカード株式会社）

●スライド１：

講演内容

●リスクマネジメントとは
●リスクマネジメントと業務の関係
●リスクマネジメントの集中管理
●リスクマネジメントとしての情報セキュリティ
●情報セキュリティの傾向と課題

●すぐに使える推奨資料

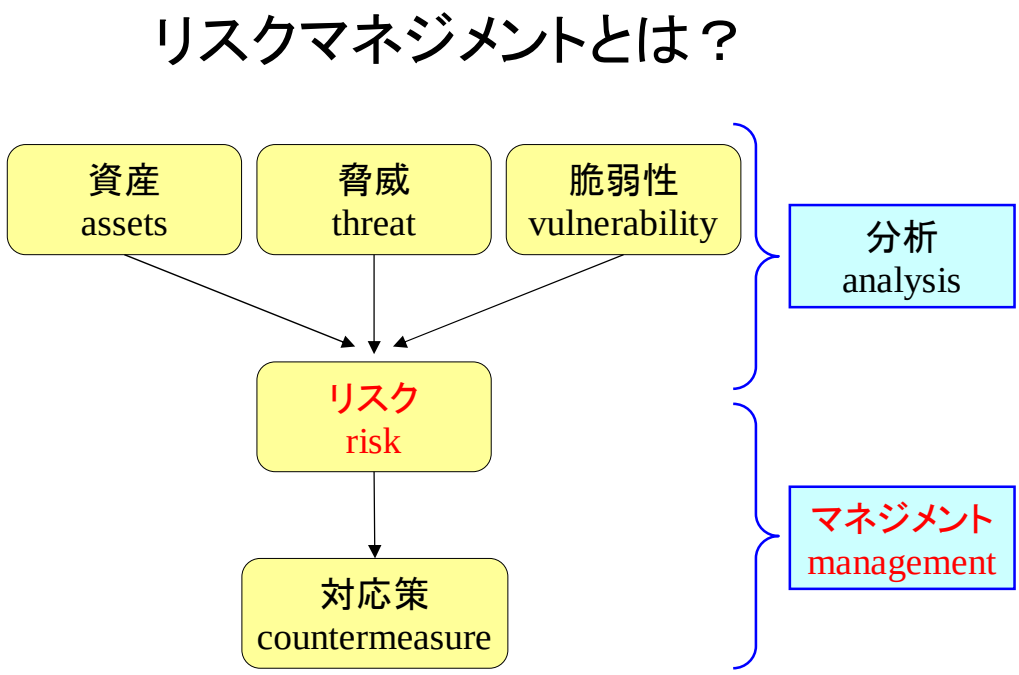
 1

情報ネットワーク法学会の佐藤と申します。表題のとおり「企業における情報セキュリティリスクマネジメント」という形で紹介を進めさせていただきます。

ご紹介する内容の目次ですが、リスクマネジメントという表題になっているので、少し復習がてらにリスクマネジメントの基本的なところの紹介。次に業務の関係。リスクマネジメントは今、エンタープライズリスクマネジメント（ERM）などと称して集中管理化できないか､企業などで検討が進んでおります｡それに関しての考え方を少しご紹介します。

それから、今回は全体のセミナーが情報セキュリティにかかわるものなので、リスクマネジメントとしての情報セキュリティという形でご紹介させていただきます。最後に少し情報セキュリティの傾向と、昨今の諸般の対策の課題を整理させていただければと思います。

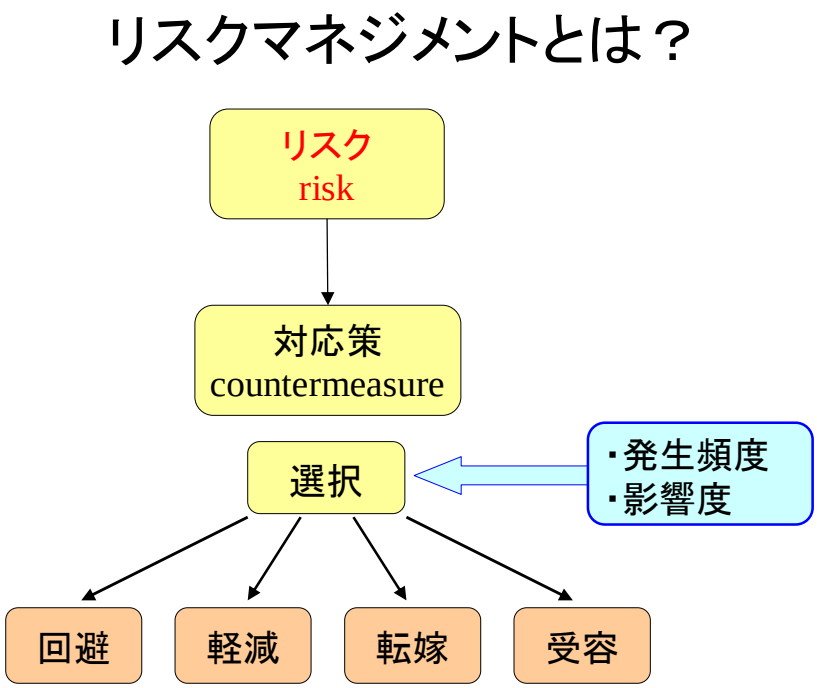
●スライド２：



最初にリスクマネジメントの復習です。リスクマネジメントそのものに関しての定義はいろいろありますけれども、これはその一例で CRAMM というところのものです。書き方、言葉が微妙に違ったりしますが、大方の考え方はここに書いてあるようなものだと思います。資産が存在し、そこに何らかの脅威があって、そこに脆弱性があるという形で考えた場合、この資産と脅威と脆弱性が合わさって何らかのリスクが生じる。生じたリスクに対して何らかの対応をするという考え方になろうかと思います。

上の前半の部分を一般的にリスク分析、リスクアナリシスと言ったりします。そのリスク分析が終わったあと、そのリスクに何らかの処置をいたしますので、その部分をリスクマネジメントと呼ぶかと思います。この部分の切り分け方は、先ほどご紹介したとおり、幾つかいろいろな考え方がありますが、基本的にはこのようなことを頭に思い浮かべればいいだろうと思います。

●スライド３：



では実際にリスクにどう対応するのかというところも、それぞれに特徴はありますが、大まかにはここに書いてあるような、何らかの選択を行うという考え方になっていると思います。そのリスクに対して回避行動を取るのか、軽減するのか、転嫁するのか、それを受け入れるのかという考え方です。

この場合、選択基準としてはそのリスクが発生する頻度、影響度です。それが１年に１回起こる問題なのか、それとも毎日起こるかもしれないことなのかが発生頻度です。仮に起こった場合、それが最終的には金額に換算できれば一番分かりやすいのですが、結果的には 100 万円の損害になるのか、１億円の損害になるのかというところです。

この発生頻度と影響度を考えた上で、そのリスクに対して回避する。何らかのことをやろうとしていた場合、やることによって発生するリスクであれば、やることそのもの諦めるのが回避です。

軽減は、リスクがあるのは承知しているけれども、何らかのリスクがもし発生した場合にはその影響度が減るように何か工夫をしよう。あるいは本来３日に１回起きそうだということであれば、それを何らかの形で１カ月に１回に発生頻度を下げる工夫をしようというものが軽減になります。

転嫁は、実際にはリスクに対して主体的な対応はせず、一番分かりやすい例は保険に加入することです。ですから、リスクが発生した場合に備えて、その影響度、例えば万が一事故が起きてしまえば 1000 万円の被害が出るということであれば、1000 万円の補償を得られるような保険に加入する。実際に事故が起きた場合に保険で担保するのが転嫁になります。

受容は言葉にしてしまうと乱暴なのですが、承知の上で何もしないで受け入れる。起こったら起こったときで､その被害を払うということで受け入れてしまうという考え方です。これらを選択することを通常、リスクの対応と呼んでいるかと思います。

ここまでがリスクマネジメントの基本ですけれども、基本的にはリスクマネジメントそのものに会社の目的があることはありません。次のスライドでは、リスクマネジメントと会社の目的である業務との関係をちょっと考えて、整理をしてまいります。

こちらに書いてありますが、先ほどのスライド２の図でお分かりのとおり、脅威と脆弱性によってリスクが生まれます。ですから資産だけがあって、脅威もなければ脆弱性もない場合であれば、その資産に対してリスクは生じないことになります。脅威だけあってもリスクは本来生じません。脅威があって、それに対して脆弱な部分があれば、それが合わさって資産と脅威と脆弱性の三つ、いわば三拍子そろってリスクが生まれることになります。

●スライド４：

リスクマネジメントと業務の関係

脅威と脆弱性によりリスクが生まれる

脅威や脆弱性を生じる事象の分類:

- ・業務によらない事象
  - ・人為的な事象　→無許可のアクセス・・・
  - ・人為的ではない事象　→自然災害・・・
- ・業務による事象
  - ・業務の不作為による事象　→注意不足・・・
  - ・業務の作為による事象　→故意、過失・・・

 4

その際、脅威や脆弱性がどうして生じるのかを少し分解いたしますと、このリスクマネジメントの対応を体系化というか、分別することができるようになります。まず一つの大分類は、その脅威や脆弱性が業務によって起こるのか。業務でない、業務の知らないことで起こるのかというところで分けたものが第１分類です。

そのような意味で、最初は業務によらない事象。業務上何かをするからリスクが生じているわけではないという場合、さらにそれを二つに分けています。まず人為的な事象。人の問題によって起こる場合です。どちらかというと悪い人に悪いことをされてしまうということが一つあります。「無許可のアクセス」と書いてありますが、その他にも幾つか例があろうかと思います。もう一つは人為的ではないものです。人がやるものではない。例としましては自然災害等が、それによって起こるリスクになろうかと思います。これは業務によらない事象を分けてみたところです。

次に業務によって起こる事象も当然あります。この業務によって起こる事象は、先ほどのスライド３でいいますと、場合によっては回避という形で、その業務自体を諦めることによってリスクを完全に回避することができる場合もあるものです。

これに関しては二つに、今度は切り方をちょっと変えてあります。業務の不作為、やら

ないことによる事象です。何かやるべきことをやらなかったことによって、そのリスクが生じる場合。ですから、言葉にしますと注意不足などで起こるかもしれません。もう一つは、一番下に書いてあるのが何かをやってしまうことによって起こることです。これには故意や過失の場合もいろいろあろうかと思います。そういった意味で不作為による事象は、少しくだけた言い方をすれば、やらなければならないことをやり忘れたときに起こります。業務の作為による事象は、やってはいけないことをやってしまった場合に起こるリスクと分けることができます。

今ここで分けた分類は、実際には二分岐法で分けております。これは一見羅列のようですが、完全に網羅性を持っています。業務によるのかよらないのかで、イエス、ノーで分かれております。業務によらない場合は人為的なものか、そうでないかでイエス、ノーで分かれております。下のものは業務による事象のうち、やらなくて起こることか、やって起こることかですから、これもイエス、ノーですので、基本的には物事をイエス、ノー、イエス、ノーで分解していった場合、それには網羅性がありますので、そういった意味でこのカテゴリーを使うことができます。

これは何でもいいわけですけれども、このリスクマネジメントに関して、リスクを整理する際に漠然とリスク対策だと考えていると、ここにちょっと書いただけでも明らかに種類が違います。自然災害の問題と故意で起こることはリスクの種類が全く違いますので、種類が違うものをまとめて全部、何か整理しようとしても、それは抽象的な結果しか得られません。

これは一つの例ですが、何らかの分類をした上で、それに対してばらばらになったものをより具体的に考えていくことが必要だと思います。ただ、ばらばらにする際に注意しなければいけないのは、ばらばらにする方法が網羅性を持っていないとすき間が生じてしまう。せっかく考えたことがすき間に陥ってしまうと大変です。

そういった意味では、網羅性のある分類の仕方で一番簡単なやり方は二分岐法です。イエス、ノー、イエス、ノーで分解していく限り、本来すき間はありません。ただイエス、ノーの判断に若干グレーなゾーンとか、かぶるゾーンが出てくるかもしれませんので、網羅性はあるが重複性がないかというと、場合によってはあることになります。ただ、この類のことを考える場合には、重複性を排除するよりはむしろ網羅性の方を担保させたほうがいいと思いますので、あまり重複性にはこだわらなくてもいいのではないと考えております。

本来はこの資料の４種類、一項一項をリスクマネジメントとして企業は考えていかなければならないのですが、本日は時間の都合もあるので、最後の下線がひいてある「業務の作為による事象」という、４番目だけをこのあと分解します。残りの３つも別途考えなければならないのですが、このあとの資料には含まれていないのでご承知おきください。

●スライド５：

リスクマネジメントと業務の関係

・「業務の作為による事象」以外は、
リスク対応策は、本来業務と独立又は区別できるリスク対応業務となる。

・「業務の作為による事象」は、
リスク対応策は、業務そのものに内在する。
当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

 5

先ほどの続きになりますが、リスクマネジメントと業務の関係の中で、業務の作為による事象以外は、先ほど他に置いておいたものです。これらのリスク対応策は、実は本来業務と独立または区別できるリスク対応業務となります。

これはどのようなことかといいますと、スライド４の下線の付いていない３つは、それに対して、もし回避策以外の対策を取ろうとすれば、それはかなり明確に業務と本来のビジネス､企業であれば事業のための処理とは異なるリスク対策をするための業務というか、作業という形で明確に分かれます。今、自分は事業の、ビジネスのための仕事をしているということと、片やその三つの部分に対応するため、そうではなくリスク対応のために何か手を動かしているのだというところが明確に分かる内容が多いです。

それに対して、業務の作為による事象とは、そもそも仕事をすることによってリスクが生じているので､この仕事そのものとリスク対策そのものを明確に分離できるかというと、

できないわけです。ですから、この部分のリスクを管理しようとすると、厳密には回避策しかない。一体化しているということです。言葉にしてみますと業務そのものに内在していると言うことができます。

そう考えてみると、その業務が仮に標準化されている、もっと分かりやすく言えば文書化されていたとします。すると、机上でその業務のリスク管理を手順化することができます。朝来てから夕方帰るまで、やることが手順書で決まっている。「朝９時に何をしなさい」「９時半に何をしなさい」「10 時に何をしなさい」と全部、書いてあって、仮にそのとおりにやっているとしましょう。すると、紙に書いてある内容を確認し、紙の内容の中に「こういうことをやったら、こういうリスクが生じる」と思えば、そこにこういったリスク対策をしましょう。朝９時に来たときにやる仕事に対して、こういうリスクが生じると分析されるのであれば、そのときにこういうことを注意しましょう。あるいはこういうことをしましょう。あるいはこういうことはやめましょうということを紙にどんどん書き込んでいけば、この業務に対する内在したリスクの対応は明確になっていきます。

●スライド６：

リスクマネジメントと業務の関係

当該業務手順が標準化されていれば、その標準にリスク対応策を適用することができる。・・・はず。

一方で、非標準化手順、すなわち、裁量業務については、リスクマネジメントの集約が困難である。と考えるべき。

なぜなら、手順を裁量しているのが業務担当者である限り、業務担当者がリスクの分析やリスク対応策の選択をする部分があるため。

 6

ただ、そのはずなのですが、実際にそうなるかというところをちょっと検証したいと思います。先ほどのスライドの文章の下に続けていますが、一方で非標準化手順を考えてみ

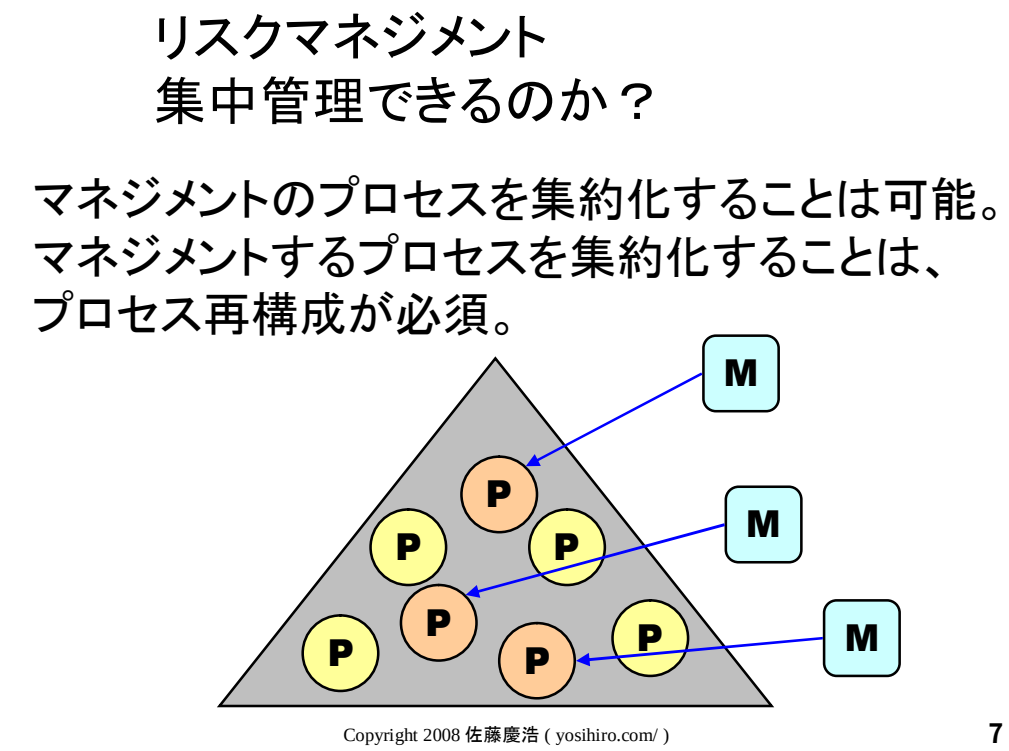
ます。９時から５時までやることが全て手順化されている一方で、そういった手順ではない仕事はどうだろうか。

何を言わんとするかというと、作業の成果物などが約束されている。ですから「今日１日でこういう成果物を出しなさい」「出すためにどういうことをするか､自分で考えてやりなさい」。だから、９時から５時までのあいだを手取り足取り、指示書はないけれども、最終的にこういう成果を出すのだと言われているような裁量業務についてはリスクマネジメントの集約が困難です。

先ほどのような標準化の紙があれば、９時から５時までやることを紙に書き、その紙に書いてあることに対して生じるリスクの対応策を逐次考えていけばいいのですが、そもそも何をやるか分からない。しかも、それは業務としてやることなので、それ自体を止めるわけにもいかないといった場合です。

そういった場合、その手順を裁量しているのが業務担当者である限り、業務担当者にリスクの分析やリスク対応策の選択をしてもらうしかありません。非常に乱暴に区分しておりますけれども、分かりやすく言うとそのようなことになります。仕事すること自体でリスクが生じているといったら、それに対して標準化ができるものは、やっている内容に関して文書上、精査することですが、そもそもどのような手法でやるかは本人に任せているという場合に関しては、その本人にリスクの分析と対応を逐次やってもらわなければいけない。そのような形になろうかと思います。

●スライド７：



リスクマネジメントを、そういった意味でエンタープライズリスクマネジメント（ERM）という言葉がありますが、会社組織として集中的に管理することができるかといった場合、実はこれはできるとも言えるし、できないとも言えると思います。それは言葉を非常にていねいに取り扱う必要があります。マネジメントのプロセス、手続きを集約化することはおそらく可能でしょう。マネジメントするための作業そのものを集約化することは、おそらく難しいでしょうということです。

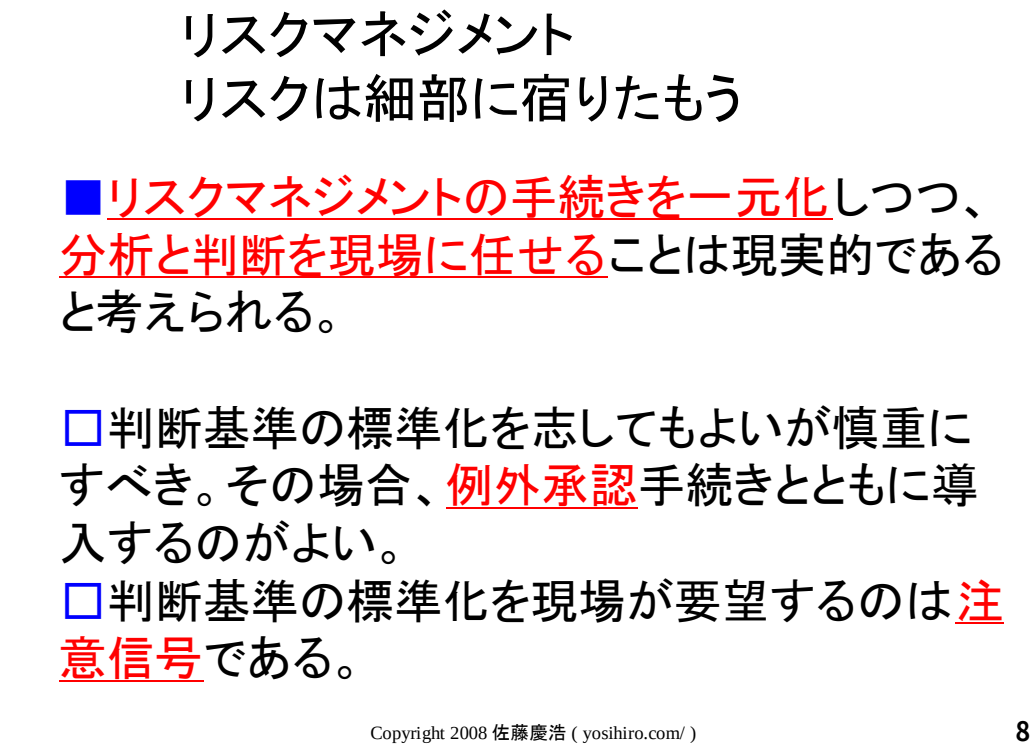
Ａさんが任された仕事において、Ａさんがやる仕事によって生じているリスクのマネジメントをＢさんが実施できるかというと、論理的にはあり得ません。Ａさんの本来業務をＢさんが持っていかない限り、Ａさんが仕事をすることで生じているリスクですから、Ａさんに手を動かして対応させなければならないわけです。

ですから、マネジメントするプロセスを集約化することは、プロセス再構成が必須です。これはできないというか、そのリスク分析の結果、先ほどの頻度と影響度が非常に大きければ、今申し上げたＡさんの仕事を取り上げてＢさんにやらせるという英断は、本来は選択肢の中にあるわけです。

ですから、今まで本人任せにしていたことが、実はリスクが非常に大きいとなれば、そ

れを完全に本人任せにするのではなく、一部、例えばところどころやっている内容のチェック作業だけをＢさんが横から同時にやる、あるいは横で見ていることはあり得ます。それをプロセス再構築とまでは言いませんが、業務手順そのもののプロセス再構成することまでやれば、マネジメントするプロセスそのものを集約化することはできます。実際にはそのマネジメントそのものを本人の作業なくして、あるいは本人の判断なくして、誰かが取って代わって、どこか別の場所で集中的に集約することは、ある意味、論理上あり得ないことになります。

●スライド８：



今のことをもうちょっと平たい言葉にすると、マネジメントのプロセスを集約化することは可能だろうと言っていたものは上になりますが、簡単に言うとリスクマネジメントの手続きを一元化することはできるでしょう。リスク分析をしたら、このような対応を取りなさいというガイドラインなりルールを設けておく。ルールを読んで、実際の作業はやはり本人にやってもらうということであれば、できるでしょう。その大前提として、分析と判断は現場に任せるということを意味しています。

ただ、その場合に判断基準が必要です。分析と判断は現場に任せるのですが、ERM という言葉を聞くと、分析基準と判断基準の標準化を何となく志してみたくなるのです。特

にその管理部門系の人は、そのようなことをやりたくなったりします。それが判断基準の標準化を志しても良いが、慎重にしたほうがいいのではないか。

なぜかというと、そもそも標準的な作業手順のものは、その標準作業手順書を紙の上で分析し、対応を書き込めばいいわけです。それができていないということは、この対象は非標準作業です。非標準作業に対してリスクの分析の基準や判断基準だけをピン留めした場合、業務のやり方、作業の内容が担当者によって柔軟ある行動をされたときに、すべてを想定してあらかじめ考えておくということができるか。できたら作業が標準化できるということで、パラドックスというか、ぐるぐる回ってしまいます。

そのような意味で、あくまで分類した考え方で行けば、非標準化の部分はそもそも作業が標準化されていないことを意味しているのだから、分析基準、判断基準だけを標準化することは、そこで現場の自由度、柔軟性を奪うと考える必要があります。

ただ、それを言ってしまったら何もできなくなりますので、それに備えて例外承認手続きを必ず注入する。ですから、あらかじめ想定された分析基準、判断基準はこうだった。ただ、実際に日々現場の業務をやってみたら、その判断基準では業務そのものが止まってしまう可能性が出た。そのときはルールを破るのか、ルールを守って業務を中止するのかといったときに、例外承認は得られるようにしておく。「判断基準はこうなのだけれども、判断基準にだけ従っていたのでは業務が止まってしまいます。でも、私は業務を続けた方がいいと思いますがどうでしょうか？」という場合を想定しておく。それはすなわち先ほどの選択でいうとリスクを軽減または転嫁、回避しろといっているものを、リスクを受容することになります。リスクがあることを承知で業務を続けることになりますので、それを例外承認として設ける必要があります。その際には、やはり手続きを一元化することができます。手続き者は現場ですけれども、手続き承認の基本的な手続きのやり方を一元化することはできます。

そういった形である程度、標準化していってもいいのですが、これは最後にきりがあるというところを、もう少し深掘りしてみたいと思います。判断基準の標準化を現場が要望しなければ、本当は任されるわけです。「分析と判断もあなたに任せてあるのですよ」「会社として、とうてい受容できないようなリスクが生じるようなことはしないように業務をしてくださいね」と言っておいた上で、適宜、毎日分析と判断をしていけば、本当は回るわけです。

その場合、とはいえ判断基準が欲しい、判断基準をくれと言われがちです。ただ、この

判断基準の標準化を現場が要望するのは注意信号です。分析能力とか判断能力がないということを自ら言っているようなものです。その人に、そのリスクが生じる業務を任せていること自体を再検討しないければならないという注意信号になります。それが本人に判断能力がないから、判断を示してくれと言っているのであれば、リスクの判断基準を標準化するのではなく、業務を標準化してしまうほうが賢明ということになろうと思います。あるいは先ほどのように、リスクに遭遇するような部分に関しては、本人にやはり分析判断を任せないということです。

ということで、このリスクマネジメントの手続きを一元化することは、とても意味があります。ただ、標準化された業務以外のところに対して、リスクマネジメントそのものを会社で集中管理することに関しては非常に慎重にやらないと、決めたことが形骸化するか、決めたことを真に受けてやったために業務に支障が出るかのどちらかになってしまいます。

その際に例外承認をうまく回していけば、例外承認の部分を集約し、そこで担保するやり方は一つの手法です。その場合、例外承認をどう承認するのかの判断基準をやはり紙に書きましょうということにすると、今言ったような弊害があるかもしれないので、このやり方を否定はしませんが、非常に慎重にやったほうがいいです。

慎重にやって、最後はやはり例外承認の中にさらに例外承認が生じるかもしれませんが、最後は人に行き着くことはしょうがないという諦めがあったほうがいいです。最後の行き着く先が文書なり、ルールや基準に落ち着く形で動くことはないと思ったほうがいい。最後はどこかで人が判断するという考え方に、若干乱暴ですが割り切ってしまったほうがいいのではないかと思います。

●スライド９：

リスクマネジメント

JIS Q 2001「リスクマネジメントシステム構築のための指針」より
「発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合には、そのグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当者を定めてもよい。」

拙著 参考記事:
翔泳社Webサイト
リスクは集中管理できるのか　～企業における法対応とITのバランス～
http://www.itcomp.jp/a/article.aspx?aid=153

 9

ここまでの二つに割る割り方も乱暴ですし、その後の進め方のとらえ方も乱暴なのですが、今、申し上げたことは邪道なのかといいますと、JIS 規格の中にリスクマネジメントシステム構築のための指針、2001 があります。この中の文言も発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合は、すなわち先ほどのような分類化して、その上でその分類化されたグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当者を定めても良い。だから最後は人に委ねても良いという考えも示されています。

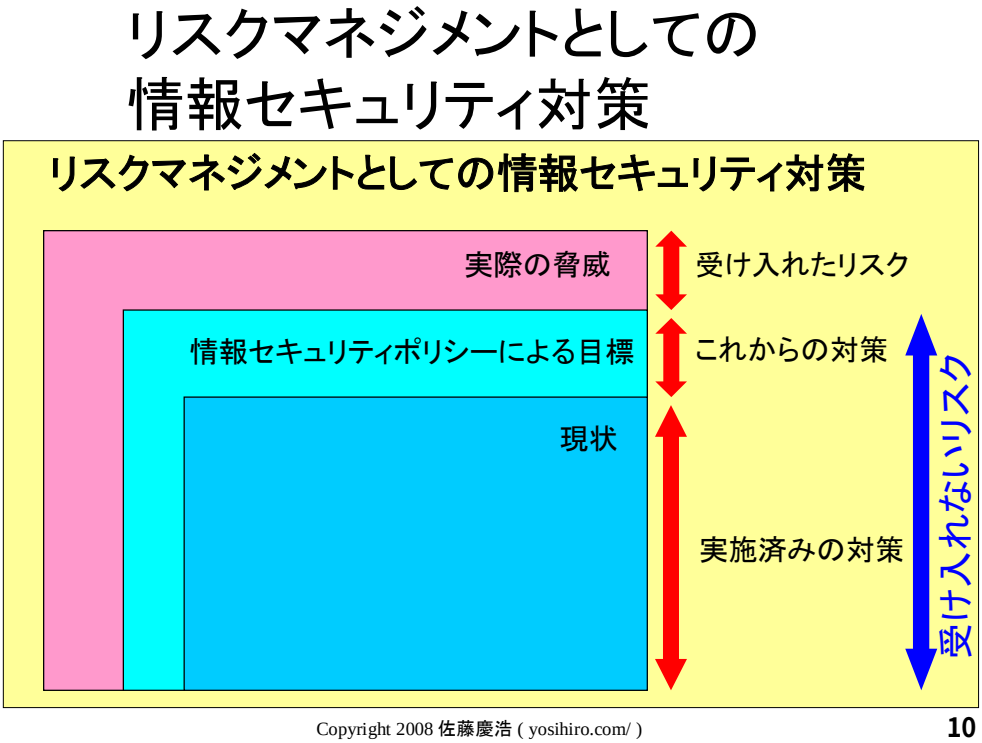
ですから ERM などを導入した際に、文書化してそれを整然と標準化することはとても意義のあることですが、だからといって最後に人の判断に頼ってしまうことをあまり否定しないほうがいい。最後は人に任せる部分があってもいいと考えてもいいのではないでしょうか。

これについては、スライド９の下に紹介してある記事で、読みものとして書き改めておりますので、もしご興味があれば、そこのところをご参照ください。

リスクマネジメントに関しては、今、申し上げた考え方で整理をした上で、さらになるべくリスクマネジメントのうち、対応に関しての作業を最適化するためには集約化したほ

うがいいという世の中の流れ、それはいいでしょう。ただ集約化といった場合、手続きを一元化することと、実際の対応策を担う実施策を集約化することは違うものだと分け、できる範囲のことをやって、できないものはやはり集約できない、分散していると考えてもいいのではないかということをご紹介しました。

●スライド１０：



話はここからがらりと変わりまして、それらのことで何らかのリスクマネジメント体制が会社の中に確立した場合、情報セキュリティ対策との関係を少し整理してみたいと思います。

情報セキュリティ対策は、おおむね情報セキュリティポリシーなるものを目標設定として定めた上で、それに対して実施するわけですけれども、その情報セキュリティポリシーによって定めた目標とリスクマネジメントの関係を少し考えてみます。

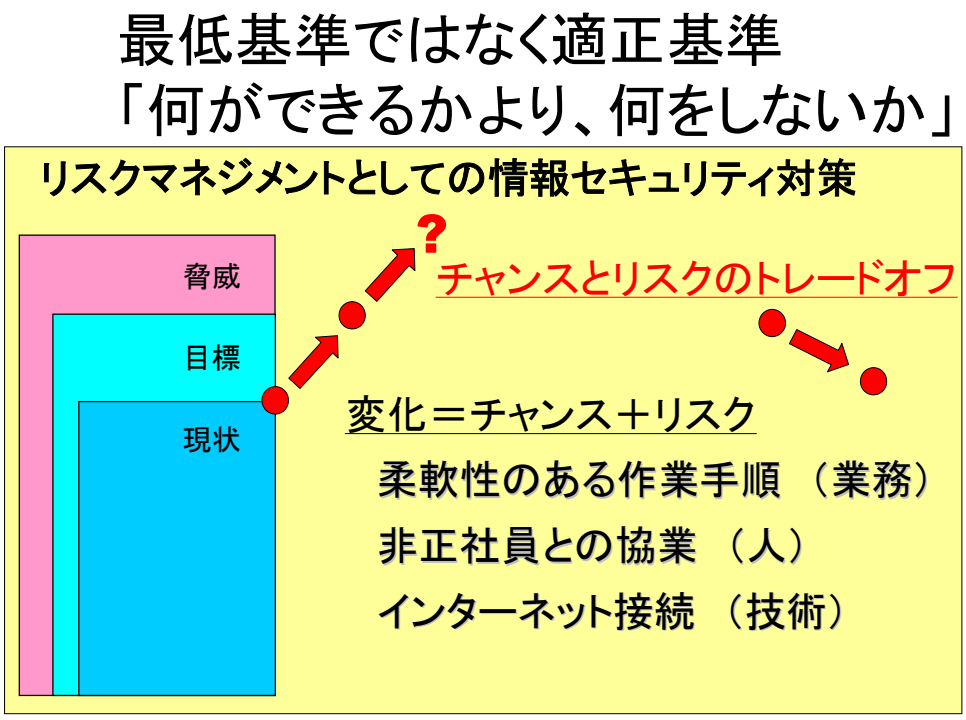
セキュリティポリシーで定める目標は通常、現状より若干高い、背伸びをしたところに定めるのが一般的です。そう考えてみますと、情報セキュリティポリシーによる目標の高さが、このスライドの高さだとしますと、現状のやっている対策の高さは実施済みの対策ということになります。すると、セキュリティポリシーの目標から現状を引いたものは、やってはいないけれども、これからやることを決めた対策ということになります。

片や目標に対して、例えばそれほど大きくない事業をやっているところが、銀行とか通信会社と同じくらいのセキュリティ対策をやるかといったら、そこまでやる必要はないわけです。それは先ほどのリスク分析等によってここまでなら受容できる。あるいは自分の会社には影響度がない。頻度が高いなどの理由で異なります。目標とは実際の脅威に対してすべて対応するわけではなく、何らかの目標値を設定しているので、先ほどのリスク管理で言えば目標よりも高いレベルはリスク対応の選択で受容したということです。「受け入れました」「そのリスクの対策はしません」「それが起きたときにはしょうがないでしょう」「そのときに起きてから考えましょう」ということで、上の部分が受け入れたリスクになります。

すると、逆に目標設定は何によって定まるかというと、受け入れられないリスクだと判断されたものに対して回避するのか、転嫁するのか、軽減するのか、何らかの選択肢を講じるわけです。そういった意味では、受け入れられないリスクそのものが情報あるいは情報システムなどの情報セキュリティポリシーの対象とする範囲によりますけれども、その対象とする範囲のものに対してリスク分析をした結果、受け入れられないと分析し、判断したものが、すなわち情報セキュリティポリシーの目標の高さということになります。

ここで一つのポイントは、受け入れられないと判断したのであれば、少なくとも世界一の対策をしていない限りは、受け入れたリスクは残っているのだと考えるべきです。

●スライド１１：



その場合に時系列でちょっと考えてみます。こちらのスライドになりますが、現状がここでした。目標がここですといっていますから、右のほうに時間が流れるとすれば、右肩上がりで上がるわけです。例えば１年間でセキュリティポリシーを達成しようとすれば、今日よりも１年後には上がっているわけです。すると、１年後に上がったのなら、２年後はどこに行くのでしょうか。上がるのでしょうか、下がるのでしょうか。

今日に対して目標が上がっているのだから、上がるように思えるのですが、実際にはここに書いてある幾つかのキーワードをリスク分析という考え方で考えてみます。先ほどもちょっと触れておりますが、柔軟性のある作業手順です。すなわち作業手順をすべて標準化し、非標準化手順を極力なくして現場判断をさせないことに対して、現場判断をさせるのはリスクが増えているのでしょうか、減っているのでしょうか。

例えば 20 年前、15 年前であれば、基幹系の情報システムに対して非正社員がその情報にアクセスすることは全く考えられませんでした。しかし、今は派遣社員、委託社員、アルバイト、パートの方に基幹系の情報にアクセスさせずに仕事をさせることができる会社があるでしょうか。非正社員との協業です。例えばインターネット接続もそうですが、インターネットがブラウザで普及したのはここわずか 10 年ほどですが、15 年前に銀行の勘

定系システムに間接的であるとはいえ、外部のネットワークがつながることが考えられたでしょうか。考えられません。そんなリスクは受け入れられなかった時代があるわけです。

そう考えてみますと、実はこの目標設定はセキュリティポリシーを立ててやる直後の状態は上がるのですけれども、その後、ビジネスの要求によって一般的にはリスクは受け入れる側が伸びる、目標は下がると思ったほうがいいのです。「変化＝チャンス＋リスク」となっておりますけれども、銀行においては全く受け入れられなかったリスクを取ることで、インターネット上でお客様へのサービスを提供するというビジネスチャンスを得たわけです。ビジネスチャンスを得るためにリスクを取ることは、今の企業では積極的に行われている判断です。そういった意味では、いったん立てたセキュリティポリシーは厳密には新しいビジネスチャンスを求める際、そのつど受け入れるリスクが増えている可能性のほうが高いと考えられます。

すると、チャンスとリスクのトレードオフということが重要になってまいります。このことに非常に注意しながら目標設定を考えたほうがいい。短期的に理想郷を作り、その次に理想郷がさらに理想化していくのかというと、むしろ足を引っ張られるのであれば、ここにあまり高い目標設定をするよりは、現実的な目標設定をした上で、さらに下がることに備えていろいろなリスク管理を考えていくという考え方もあります。

そういった意味で、表題にしておりますが、今どきは最低基準ではなく適正基準という考え方が求められています。以前であれば「セキュリティ対策は少なくともこれだけはしてください」というところ、最低ラインだけが決まっていました。だから「ベースライン型」と言ったりします。

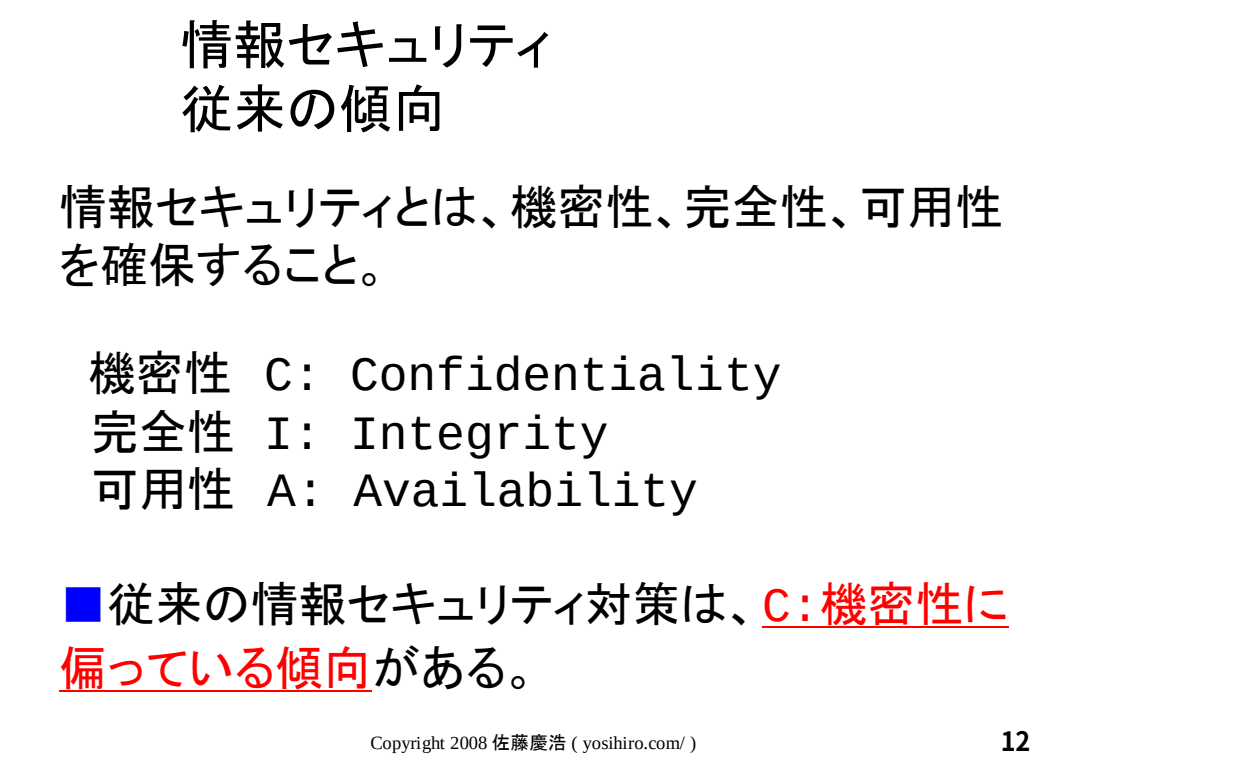
「最低これだけはしてください」という言葉の裏側には「もっとやることはウェルカムですよ」「もっとやれるのだったら、よりもっとやることはどうぞ皆さんご判断ください」ということがあったのですが、今これは適正基準になっています。「このレベルで対策してください」「やり過ぎはやめてください」。低くなるのは当然リスク管理として、会社として受け入れられないけれども、ではそのリスクをより軽減することは幾らでも高くしていいのかというと「それはやり過ぎないでください」「ある幅の中に収まってください」と適正基準化しています。

そういった意味で情報セキュリティ対策の場合、何ができるかよりも、何をしないかの判断のほうが重要です。このことはしないと決めることがあれば決めていかないと、基本的にはこの部分で何らかの支障を生じるという考え方が、一つあるのではなかろうかと考

えております。

以上が情報セキュリティとリスクマネジメントの関係になったかと思いますけれども、このあと情報セキュリティの従来の傾向に少し触れた後、もう１回、リスクマネジメントに話を戻したいと思います。

●スライド１２：



こちらのスライドにありますが、情報セキュリティは一般的に機密性、完全性、可用性を確保することだと言われておりまして、それぞれの英語の頭文字を取って CIA と呼ばれております。従来の情報セキュリティ対策は、少しＣの機密性に偏っている傾向があると言われ始めております。

●スライド１３：

情報セキュリティ
今後の方向性

CIAからAICへ
□実際には、Cに加えて+Iさらに+A
□しかし、CとIとAの要求が相反する場合にトレードオフを図る必要に迫られる。
□情報セキュリティを直接トレードオフすることはできない。リスクのトレードオフとなる。
■情報セキュリティマネジメントシステムにおいては、+I&+Aによって、対策そのものに加えてリスク評価が重要になる。

 13

今後の方向性として、これをあえて言うのであれば、CIA から今 AIC へ移ったほうがいいのではないかと言われています。ただ、この言葉は順番をひっくり返す意味ではありません。実際には CIA でやったＣの対策が、もしある程度のレベルまで達したなら、そのレベルは落とさずにＩとＡはプラスアルファして成長させようという意味合いです。ですから、今までやってきたＣをないがしろにして、CIA のＣを AIC にするということではありません。

ただ、ＣとＩとＡの要求が相反する場合、トレードオフを図る必要に迫られます。一般的には CIA のうち、Ｃをやり過ぎると業務に支障があります。Ａは可用性ですから、情報の安定性です。安定性を上げることは業務に支障が出ることにはなりません。業務にとってはむしろプラスです。そういった意味では、ROI を得ようと思えば得ることもできます。そのようなことがありますので、ＣとＩとＡに関してはどれかを高めると、実は他のどれかがマイナスに動く可能性があります。

すると、どちらを優先するのかということが起きますので、どちらを優先するということは、片仮名で言うとトレードオフということになります。その際、情報セキュリティの対策、Ｃをこの高さでやっています。今、Ａをこの高さでやっています。Ａを上げようと

思うとＣが下がるのです。これを情報セキュリティ対策の先ほどのセキュリティポリシーの目標設定のレベルとして、トレードオフすることは実際には不可能に近いです。

何をトレードオフできるかというと、リスクのトレードオフです。先ほど申し上げたセキュリティの要件とは、Ｃがこの高さであるということは、このＣがこの高さであることによってこのリスクが受け入れられないと定まっているわけです。Ａが今この高さであることは、このリスクは受け入れらないと定まっているので、これとこれがこのように動くときにはセキュリティの対策レベルをトレードオフするのではなく、こちらにあったリスクの受け入れられない範囲を上げる代わりに、こちらのリスクでは受けられないと言っていたものを受け入れる。この受け入れが増える部分に関してトレードオフをする必要があります。

情報セキュリティマネジメントシステムにおいては、この＋Ｉ、＋Ａ、すなわち CIA から AIC に移るためには、対策そのものに加えてリスク評価が非常に重要になってまいります。そのような意味で、情報セキュリティ対策のうち、実は CIA のＣしか行わない場合、あまりリスク評価をシビアにやらなくても、だいたい同業、同種、同業態のところと同じぐらいのことをやっておくと、まあまあ何とかなる場合もあります。ただ CIA が絡みますと、これは各企業の中でそのリスクのトレードオフを行い、自分が決めければならない問題です。

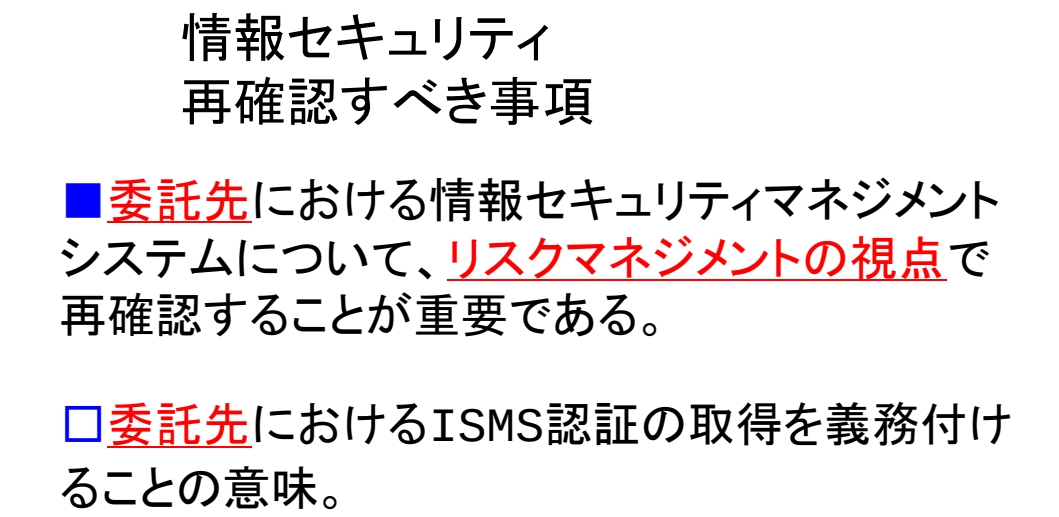
先ほど申し上げたように、銀行さんがインターネットバンキングを始めたとき、インターネットに足を踏み出すのか踏み出さないのかは、隣の銀行を見て決める問題ではありません。自分の銀行はそのリスクを取ってでもインターネットのサービスをやろうと思うのか、やろうと思わないのかという自分の問題になりますので、その場合、組織ごとのリスク評価が非常に重要になってきます。

実際には ISMS の認証等がありますが、しつこいようにリスク評価をまずやれと繰り返し言うわけです。そのリスク評価がちゃんとできている組織、ちゃんとした上でセキュリティレベルが決定している組織は、その後、このトレードオフが生じた場合にリスクのところを見直し、そのトレードオフをビジネスの要求とのトレードオフにかなり容易に結び付けることがでます。これをあいまいに行っている企業は、セキュリティ対策のレベルを直接トレードオフしなければならないことになりますので、そのときに困ってしまうわけです。

可用性を上げるために機密性の担保を下ろすけれども、どちらが大切なのだろうと言わ

れても、どうにもなりません。両方大切だとしか言いようがないのです。すると、どうなるか。Ｃが落とせないならＡが上げられない。Ａが上げられないということは、何らかのビジネスチャンスを諦めるしかないのです。これを上げないということは、リスクを回避する選択肢を取るということですから、基本的には新しいビジネスに臨めないことになろうかと思います。

●スライド１４：

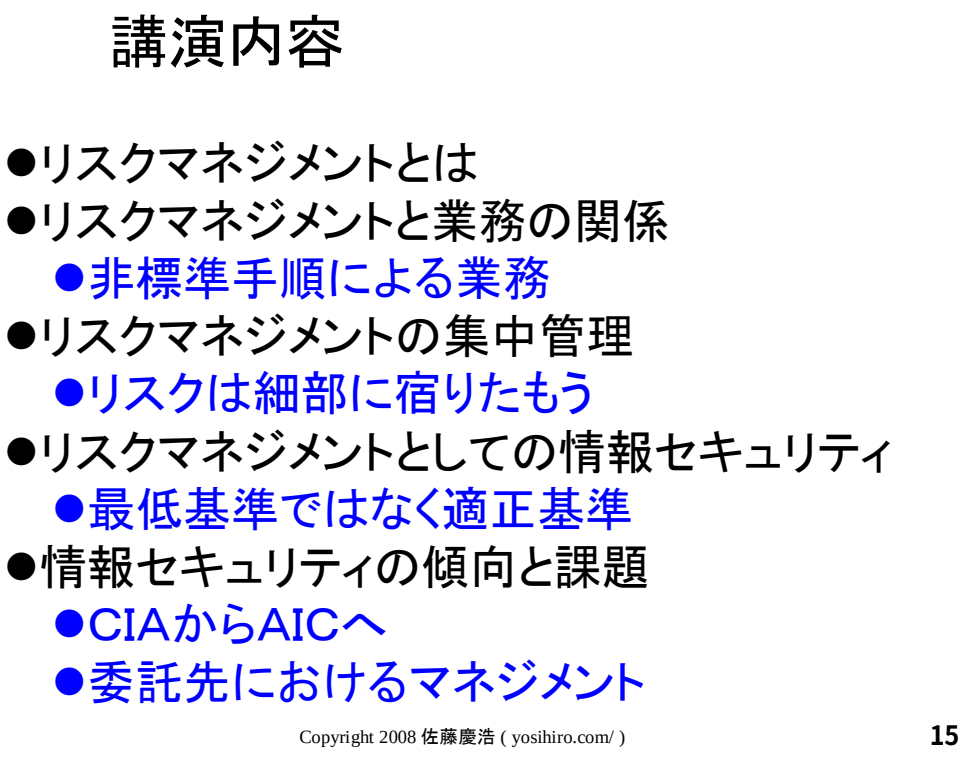


次に、委託先に関して、このリスクマネジメントの視点で再確認することが重要になろうかと思います。例えばここは一つの例ですが、委託先に対して ISMS 認証の取得を義務付けたとしましょう。その場合、リスク評価は誰がすべきか。今日このご紹介、ご説明を聞いた方は自明ですね。委託先が行ったリスク評価を使うなどということは無意味です。

委託先に対して行うのであれば、自社がやったリスク評価の結果を相手に指示し、ISMS を仮に自分の会社で取っていたとしたら、そのとき行ったリスク分析の結果に基づき、改めて委託先のセキュリティ対策レベルを設定してもらわなければならない。委託先側がやった、しかも委託先における ISMS 認証の取得は通常、発注前ですから、発注する前の状態で委託先が自分の会社のためにやったリスク分析に基づいて行っている対策だけに頼ることは意味がないのです。

ですから、この部分はこれからの課題になってくると思います。これをまともにやろうとすれば、コストに跳ね返ってきますので、高いコストを請求されてしまいます。そこまでやるのか。あるいは委託先に ISMS 認証を取らせるのではなく、自分の会社で取っている ISMS 認証のマネジメントシステムの配下に委託先を置くほうが、むしろ自然かもしれません。この部分は今、一つの解があることではないと認識していますが、ここのところで勘違いしてしまうと、委託先にただ「ISMS 認証を取ってこい」と指示することは、あまりよろしいことではないと言えるかと思います。

●スライド１５：



以上、お時間を頂いて「リスクマネジメントとは」から始めてご紹介いたしましたが、時間の関係で若干、早口で進めてまいりました。お手元の資料には色が付いておりませんが、スライドではそれぞれの項目のキーワードを改めて文字に起こしてあります。

リスクマネジメントと業務の関係、ポイントは非標準手順による業務を少していねいにやらなければならないというところです。それからリスクマネジメントの集中管理。業務の最適化、リスクの最適化として、集中管理はぜひとも進めるべきですが、リスクは同時に細部に宿りたもうと書いていますが、完全に１ヵ所にすることはできないと思ったほうがいいのではなかろうかというところです。

それからリスクマネジメントと情報セキュリティの関係は、先ほどの例のように密接な関係があるとともに、徐々に対策が増えていくという幻想にとらわれず、最低基準ではなく適正基準という考え方をしていく必要があろうかと思います。

それから、今後の傾向として、CIA から AIC の観点が最近は求められております。このために事業継続計画の策定といったことが最近、多く取り上げられているのは、この理由によるところだと思います。

また、昨今の企業において委託先を使うことは多くの局面で出てくるので、委託先におけるマネジメントをどう位置付けるのかを非常に注意深く考えないと、ここが形骸化してしまって、事実上リスクを転嫁しているのに等しい状態になってしまうかもしれません。すると、それは保険会社との関係という感じで委託先と付き合っているのか、丸投げしていて本当にいいのかということがあります。

●スライド１６：

すぐに使える推奨資料

「先進企業から学ぶ事業リスクマネジメント 実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

情報セキュリティに限らない、企業におけるリスクマネジメント全般について検討すべきことを紹介している。
300ページと分量が多いが、図を多用し、企業事例にも具体的にふれてわかりやすく解説しているため、読むのにストレスはない。

以下のWebから無償ダウンロード可能
http://www.meti.go.jp/policy/economic_industrial/report/downloadfiles/g50331i00j.pdf

 16

以上のとおり、今日はリスクマネジメントということでご紹介してまいりました。冒頭のところで一例、CRAMM のモデルだけを取り上げましたが、実は経済産業省の報告書に、ここに書いてあるようなものがあり、下に書いてあるウェブサイトから PDF がダウンロードできるのですが、これはリスクマネジメントの教科書的なものとして非常に有益です。

政府が出した報告書なので、まず 300 ページと聞いただけで、読む気がなくなってしまい、１ページ目を開く気持ちがなくなってしまうのですが、この実践テキストに関して申しますと、むしろ本屋さんで売っている 300 ページのリスクマネジメント教科書がただでもらえると思えば、これは安いです。これをご覧いただくと、今日の私の講演は特定の手法だけを引用していますが、これは中立的にいろいろな手法を述べています。しかも、書籍を購入して勉強するのに比べれば無料です。

Ａ４、１ページ両面にしても１ｃｍちょっとあるので、印刷してホチキスで綴じるのも大変ですが、先ほど言ったように書籍だと思えばこれはありがたいです。ただでこの厚みの書籍がもらえるのだと思えば、ふだん払っている税金をこういうところで取り返してもいいですから、ぜひ一読ください。自分で読まなくても、今日ご参加の皆様で部下のいる方であれば、ダウンロードして部下に渡す、部下に「読め」という形でもいいかと思います。

●スライド１７：

すぐに使える推奨資料

「先進企業から学ぶ事業リスクマネジメント 実践テキスト」
平成17年3月　経済産業省
（事業リスク評価・管理人材育成システム開発事業）

目次
1. リスクマネジメントとは
2. 事業リスクマネジメントシステム構築及び維持のための体制
3. リスクマネジメント方針
4. リスクマネジメント計画の策定
5. リスクマネジメントの実施
6. リスクマネジメントシステムに関する評価、是正・改善

 17

その実践テキストの目次だけ挙げておりますが、オンラインがありますので、そのオンラインの中で印刷してご覧いただければと思います。

●スライド１８：

情報ネットワーク法学会
http://in-law.jp/
随時、入会受付中

発表資料のダウンロード
http://yosihiro.com/go/2008-02-21-inlaw

私のほうからの講演は以上ですが、私の所属しておりますネットワーク法学会という学会では随時、入会を受け付けております。今日発表したようなことを勉強会という形で随時、行っておりますので、もしご興味があれば、当学会にもご入会いただけましたら幸いです。

あと本日の資料、稚拙なものですが、書いてある URL から電子ファイルをダウンロードできるようにいたしますので、もし必要であればダウンロードしてお使いいただければと思います。