特 集

「BL-QE登録組織 情報交換会 in 東京」セミナーレポート❸ 〈全４回〉

おがたコンサルティング代表 緒方 健氏

全４回にわたってお届けしている『BL-QE登録組織 情報交換会 in 東京』セミナーレポート（2019年12月 BL東京本部にて開催）。今回は基調講演のまとめとして、「情報セキュリティの核心」に迫ります。マネジメントやリーダーシップをどのように機能させてIT活用をしていけばいいのか、さらに持続可能な情報セキュリティマネジメントシステムを構築していく上で最も大切なことにも触れて頂きましたのでお伝えします。

基調講演

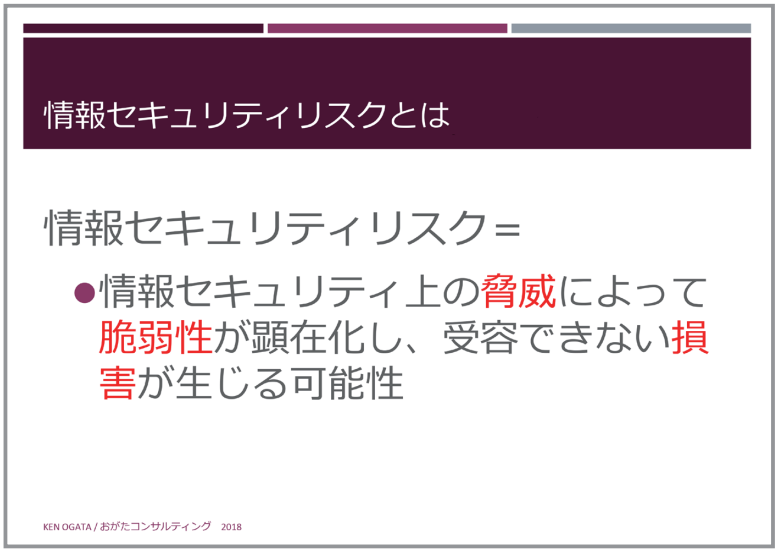
『マネジメントとリーダーシップに資するIT活用』

3 科学して対策を有効に保ち続ける。それが「情報セキュリティの核心」

ここまで、情報化社会におけるこれからの経営戦略とマネジメントの考え方、そして情報セキュリティとは何かという基本的なお話をさせて頂きました。ここからは、それらの話を総まとめにして、様々な情報セキュリティリスクに対してどのように考え、マネジメントシステムを構築をしていけばいいのかを一緒に考えていきましょう。

結局のところ「リスク」って何？

よくリスク、リスクって言いますが、情報セキュリティリスクというものは一体何なのかというと、教科書的な定義ではこうなっています。



注記１
情報セキュリティリスクは、脅威が情報資産のぜい弱性又は情報資産グループのぜい弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じる。

JIS Q27000:2019
情報技術ーセキュリティ技術ー情報セキュリティマネジメント　用語

ここでちょっと気をつけて頂きたいのが、すでにISMS認証をされている会社様はご存知だと思うのですが、例えばISO9001で出てくるリスクと、ISMSで出てくる情報セキュリティリスクというのは別物なんですね。定義自体が違うということで、用法が被ったりする際には注意して頂きたいところではあります。

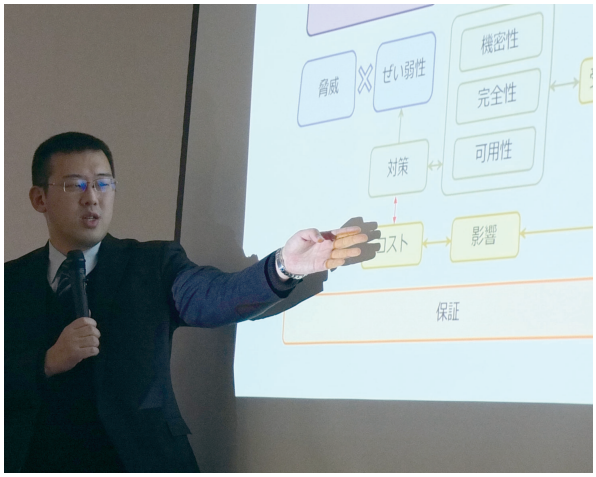
情報セキュリティリスクとは、「脅威」と「脆弱性」の重なり合いです。脅威と脆弱性という2つの要素が重なり合うことによって、事故や何らかの損害が発生するということです。この考え方は、例えば労働安全の場面でも同じです。

職場の使用機材について一定の危険な部分があった場合に、そういった危険なものがあるにも関わらず危険行動を取ったことによって何らかの被害や損害、怪我をするとか死ぬといったことが発生してしまうと。そのような考え方は、リスクアセスメントでは大体共通になっていると思います。

すべての対策は「とりあえず」。脅威と脆弱性の関係

では、どのようにして立ち向かうのかということですが、完璧なものはありません。対策はすべて「とりあえず」です。時代によって変わります。以前はこういうやり方が有効だったという話があっても、それは大体賞味期限2~3年ぐらいだと思ってください。今はもうそのやり方はでは完全に無理とか、その暗号方式では完全にデータを抜かれちゃいますよということがあったりします。

それに対して、例えば国がいろいろルールを定めて欲しいみたいな言い方もよくされます。でもそれは無理なんですね。なぜかというと、ちょっとここで強調しておきたいのは、ガイドライン通りにやっていたことをもって司法上の免責にはならないということです。これ、大きな誤解があるんですけれども。国のガイドラインを守っていたと主張すること自体をもって、「守っていたのならしょうがないね」と免責になるということはない、という風に覚えておいてください。国としてはこういう風に考えていますということを提示しただけのことで、自分達に関係のないところについてはやらなくていいし、逆にとても重要だと思っていることについては、ガイドラインがこのレベルでいいというようなことを書いていても、もっと突き詰める必要があるということです。

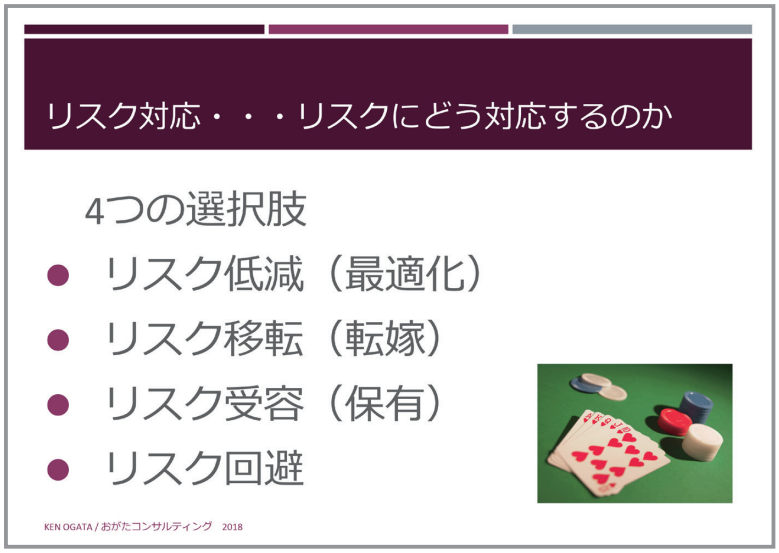


リスク対応には扱うものに合わせてメリハリが必要

セキュリティレベルというのは、情報セキュリティリスクに応じて自分達で考えて決定しなければなりません。何をどこまで守るかというのも、一つの戦略です。

例えばゲノム情報みたいなものとか国の機密だとか、そういったものを取り扱うとなると漏れたら大変だから二重にも三重にもやらないといけないかもしれませんが、それ以外のそうでもないという時にはそれなりに、という感じですね。そういう風にいわば対策にもメリハリをつけていくというのが必要になってくるということです。

そこでどう対応するか、選択肢は以下の4つになります。



注記２
リスクへの取組みの選択肢
- リスクを回避すること
- ある機会を追求するためにそのリスクを取ること
- リスク源を除去すること、起こりやすさ若しくは結果を変えること
- リスクを共有すること、又は情報に基づいた意思決定によってリスクを保有すること

JIS Q 9001:2015
6.1 リスク及び機会への対応

リスクを下げるというのは一般的によくされている手法です。リスクを転嫁するというのは、例えばそれまでは社内にサーバーを置いて管理していたが、これからはプロの管理に任せようということでクラウド化するとかですね。クラウド化はリスクの移転になります。

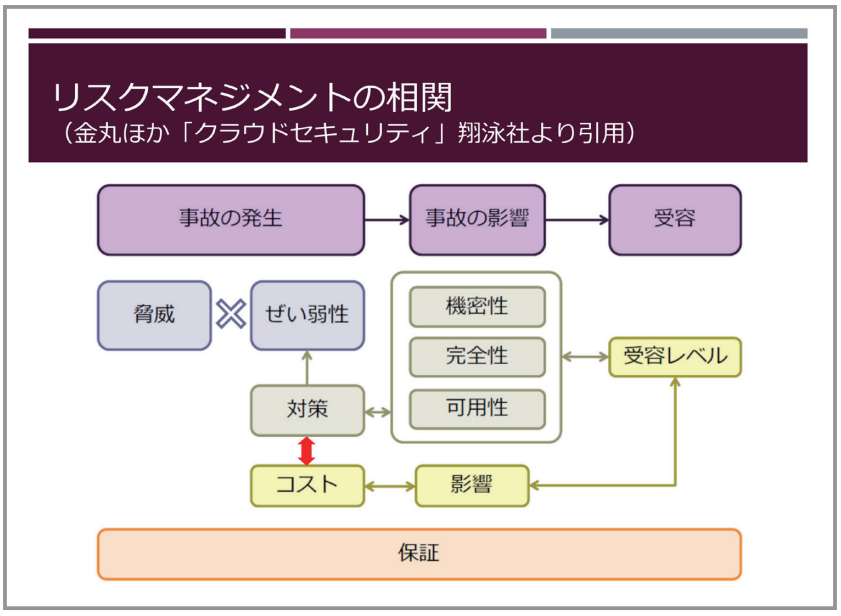
保険をかけることもそうです。もしも建物が津波とか火事でやられた時のために保険をかけておくことは、そのリスクを保険会社に被せているということになりますから。

あとはリスク受容、リスクを呑むということですね。このリスク受容というのは必ず発生します。リスクゼロというのはあり得ないので、一定のリスクは受容せざるを得ない。

そして最終的にはリスク回避というのがあります。もうこんなに危ないことは手を出さないでおこうという、この４つの中から判断することになります。

ISMSは対策を有効にし続けるための仕組み

ここまでのおさらいをしますと、情報セキュリティには脅威と脆弱性というものがあり、その２つが重なることによって事故が発生します。この事故が発生して機密性･完全性･可用性に対する影響が出ます。もし事故が起きたら対処して、その影響を受容レベルまで下げないといけません。そして事故が起こる前でもそのリスクを見立ててきちんとそれが受容レベルまで落ちるように対応しなければなりません。



上記図の赤矢印は私が入れたものですが、個人的にはここが重要だと考えています。というのは対策にはどうしてもコストが掛かります。その対策に関するコストと影響、事故の影響も勘案して対策を立てていくことになります。これはマネジメントのレベルというよりは、戦略的判断の部分になってくるでしょう。

ISMSなら管理責任者として、プライバシーマークだったら代表者も承認が必要になってきます。こういうリスクがあるということはわかりました、それでこれについては呑みます、こういった手立てをします。これについてはもう、リスクが高いので避けますといったことは、最終的には会社の戦略的判断として行うということです。

情報セキュリティも単純化･分業化･標準化が基本

情報セキュリティでは最近リーガルの話も非常に多く、ISMSでも様々な法令の特定を行っています。その中には個人情報保護法があったり、著作権法などがあったりしますが、著作権法がなぜ出てくるかというと、要は盗用などをしないためです。第三者の発信する情報を勝手に盗用して使ったとなると、大変なことになります。例えば著作権法的に問題のない形でデザインするなどのルールを決めて、ちゃんと規定に則っているか、則っていないか、定められた要件に当たるか当たらないかという最低限のブレない判断をするだけで済むようにしていきます。

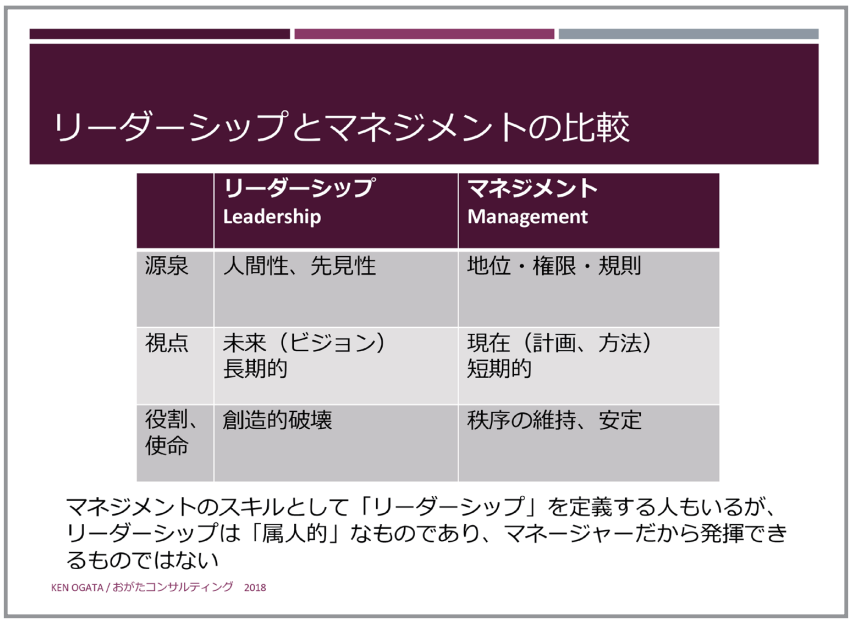
それが「セミナーレポート①『管理型からデータ活用型へ――21世紀型のマネジメントとは?』単純化･分業化･標準化で物事の再現性を確保する」のところで申し上げた「単純化」ということになります。そしてこの判断を「分業化」させていきます。法的な判断というのは、皆が弁護士としてやっているわけではないから法的な判断ができるわけでもないし、皆がセキュリティをやってるわけではないので、セキュリティの個々の実装などは専門の部隊にやらせましょう、そこで決めたルールのもとで現場ではやらせましょうということで、守るルールの中身も分業化していくとことになります。

しかしこれが行き過ぎると、とにかくルールを守っていればいいんだということになったり、手順の

ための手順がどんどん増えたりと、冒頭から申し上げてきたようなマネジメントの弊害が発生する場合があります。それをどういう風に解決していくかということで、一つの対策として「リーダーシップ」の重要性についてお話したいと思います。

マネジメントの弊害を打ち破るのは「リーダーシップ」

組織が仕事をする時に、誰もが好きにやっても良いというようなことだったら、全然パフォーマンスは上がりません。かといって、あまりガチガチに締め付けてしまうと今度はやる気を無くしてしまいます。ですので、ストレスというものは適度に掛けないといけません。マネジメントというものはストレス方向に動きますので、あまりやり過ぎるとパフォーマンスが行き過ぎてしまうので、それをリーダーシップで少し呼び戻す必要があります。



リーダーシップはミッションからビジョンへ向かうためのエンジンと言えるかと思います。それをうまく方向性を間違わずに誘導していくのがマネジメントになります。ただしリーダーシップは結構属人的なもので、マネージャーになれば即発揮できるというものではありません。そのためにリーダーシップ教育などがあるのですが、リーダーというものは単にリーダーシップだけやればいいという訳ではなく、フォロワーシップもやらなければならないとよく言われています。

フォロワーは、そのリーダーのもとで従うということです。リーダーはそれぞれの場面に応じて変わったりします。そうなるとある時はＡさんがリーダーだったが、次の時はＢさんがリーダーということになる。そうなるとＢさんがリーダーシップを執る時はそれまでリーダーだったＡさんはＢさんのフォロワーに回るということですね。リーダーをやるとフォロワーシップもできてくるし、フォロワーをちゃんとできる人はリーダーシップもうまくやれる人、そういう形で相乗効果がうまく出てくると言われています。

マネジメントが行き過ぎた時に起きる「官僚制の逆機能」のような弊害を打ち破る方法の一つとして、社員にリーダーシップを持たせることは非常に大事だというお話をさせて頂きました。

ISMSは対策を有効にし続けるための仕組み

情報セキュリティ対策には物理的な対策、技術的な対策、そして何より人や組織の対策があります。一番メインになるのは当然漏れない、壊れないようにするための対策ということになりますが、さらに考えておかなければいけないのは、漏れても壊れても損害が発生しないようにするための対策です。かつ対策を一度有効にやっただけではダメで、対策が有効であり続けるための対策が必要になります。

情報セキュリティマネジメントシステムとは、まさにその対策を有効にし続けるための仕組みのことで、マネジメントシステムはそれ全部を包括･包含するものになるわけです。これは一番ベーシックな部分で、この辺の話がわかっていないと、単にITの機材を入れても局所的なものになってしまいます。その前提となるお話ということで、「ITをほとんど話さないITの話」で話をさせて頂きました。（一同 笑）

何かまだモヤモヤされているところもあるかと思いますので、その辺りは質疑応答でディスカッションしながら適宜お答えできればと思います。ありがとうございました。

緒方 健氏　プロフィール

おがたコンサルティング代表。情報セキュリティ、個人情報保護、ISO、知的資産経営に関する コンサルティング、監査･認証審査を行っている。　経産省高度情報処理技術者、プライバシーマーク主任審査員、医療情報技師、行政書士な どの資格を有し、国の医療系研究プロジェクトのセキュリティアドバイザー等を務める。