特 集

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

おがたコンサルティング代表 緒方 健氏

2019年12月9日、東京飯田橋にあるベターリビング東京本部7F会議室で『BL-QE登録組織 情報交換会』が開催されました。刻々と変化する情報セキュリティへの取り組み方だけでなく、その基本となるマネジメントの考え方についてふれた大変意義ある内容でした。そこで当日ご出席になれなかったBL登録組織の皆様にもぜひお伝えしたく、情報交換会の内容を全４回に分けてお届けしています。本レポートはその２回目となります。

基調講演

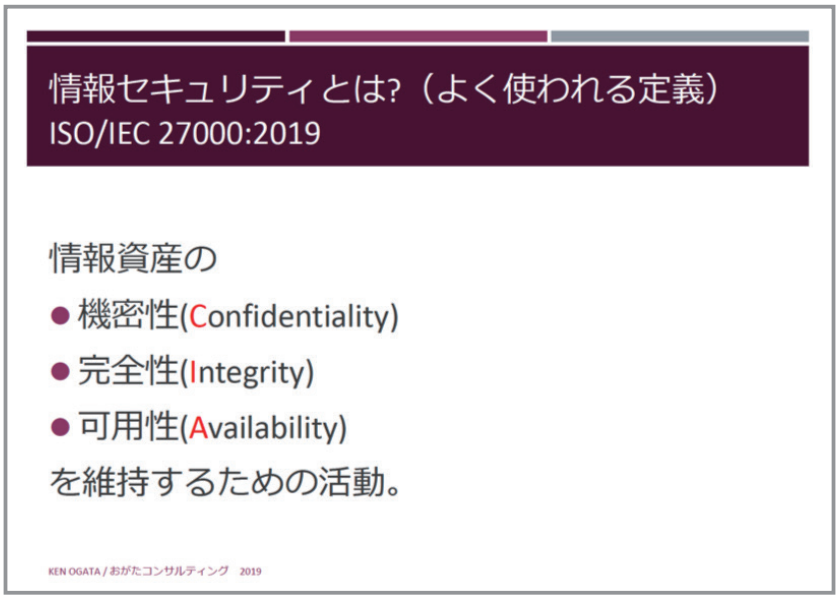
『マネジメントとリーダーシップに資するIT活用』

2 情報のリスクマネジメントは「根性ではなく科学」

さて、前半は現在のIT化において「管理そのものが目的」になってしまっていないかというお話と、目的･目標をもって活用させる「情報化」に進化させていくことの重要性、そして経営戦略とマネジメントの基本的な考え方についてお話ししてきました。後半はマネジメントの一例として、IT化に不可欠な要素「情報セキュリティ」のお話をさせて頂きます。

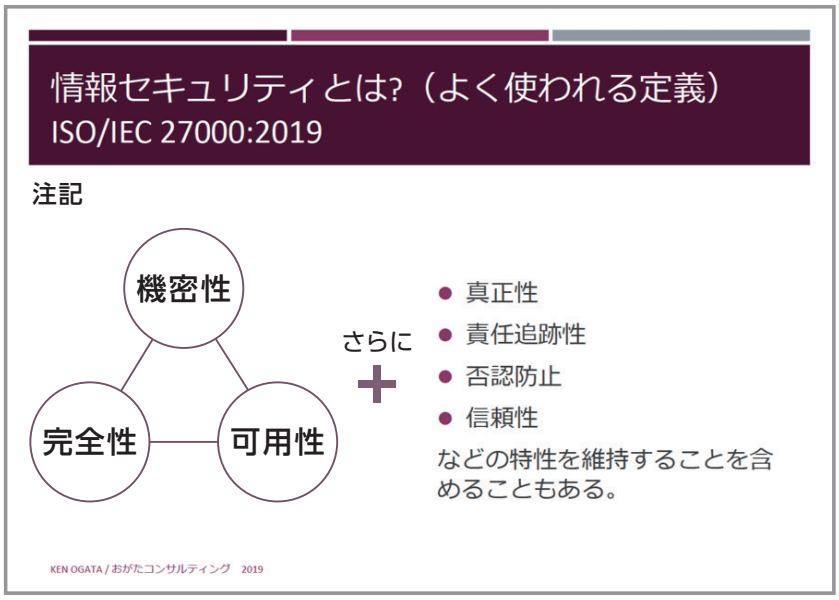
情報セキュリティの定義と特性について知る

まず「情報セキュリティ」とはいったい何かというと、教科書的な定義はこちらになります。



要は秘密を守るということが「機密性」。では「完全性」とはどういうものかというと、あるべきものがあるべき形で１から10まで揃っている状態、つまり欠けがないということですね。そして使いたい時に使いたいだけ使えるというのが「可用性」です。

これをちゃんと確保しておくための活動というのが、情報セキュリティです。しかし、これだけの要素では足りないということで、次のような特性を維持することを含める場合もあります。



「真正性」とはつまり、これが本物であるということをしっかり担保するということ。そして「責任追跡性」は誰が書いたものであるかというのを、きちんと明確化しておくこと。「否認防止」というのは、自分が作っていないというのを言わせないこと。これは責任追跡性と表裏の関係なので、２つ一緒にする場合もあります。

あとは「信頼性」です。いろんな仕組みがあるとかシステムがあるとか言うけれども、それはきちんと稼働するのか、ということですね。電源が止まってもバックアップ電源があるから大丈夫とか、そういった形でちゃんと使えますよ、ということを信頼させること。これらの特性が情報セキュリティの大切な要素であると、考えられています。

「情報」セキュリティか？「サイバー」セキュリティか？

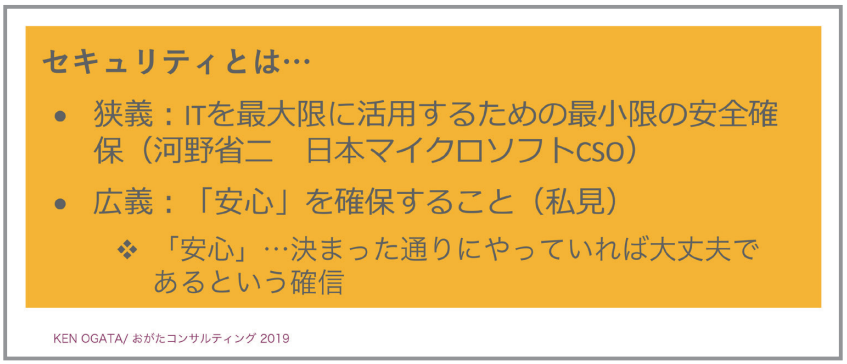
少し脱線しますが、「情報セキュリティ」と似た言葉で「サイバーセキュリティ」という言葉を皆さんも聞かれたことがあると思います。その２つは何が違うのかというと、人はいろいろなことを言いますが、「サイバーセキュリティ」は基本的に紙が対象にはならなくて、「情報セキュリティ」は紙に書かれた情報も対象になる。大体この辺りでのコンセンサスは得られてると思います。ただ、これにあまり大きな意味はありません。正直どちらでもいいという話です。ISMSはInformation Security Management System＝情報セキュリティマネジメントシステムですね。だから紙も入ります。

アメリカでは政策上サイバーセキュリティという言葉を使いたがります。なぜかというと、アメリカはセキュリティというのを自分たちの情報を守るための手段としてだけではなく、一つの産業として興す

という遠大な目標があるからなんですね。

これは皆さんの会社に置き換えても、情報の何をどこまで守るかということ自体が、売り物になる場合もあります。例えばデータセンター企業などでは、当社はこれだけの地震に耐えられますとか、ISMSとプライバシーマークの両方を持っていて、米国公認会計士協会からSOCの2、3を取得していますといったように、認証を並べることがあります。認証を積極的に取得し開示していくこと自体を、広告宣伝や会社の差別化要素にしていくということなら、それも一つの戦略です。

セキュリティレベルは相手との関係性で決まる相対的なもの



「安心」と「安全」という言葉があります。私がここであえて「安心」という言葉を使ったのは、結局セキュリティというのは個人の信頼とか感情といった、そのあたりの話になるからです。

例えばカルテの情報を落としたとか、ある県で起こった行政文書流出のように自分の納税情報が載っていたとなると大騒ぎしますけど、たとえば名刺のようなものなら時折落ちていたりしますよね。名刺1枚落ちていたからといって大騒ぎする会社もあれば、それほど大騒ぎしない人もいる。その辺の温度差は必ずあるわけです。

そういった類の事故対応というのは、いい、悪いの問題ではなく、相手との関係性などで決まってくる相対的なものだということです。信頼や感情的にこれは許せるかどうかというところで実際のセキュリティレベルが決まってくるわけなんですね。

例えば公的なセクター、役所などでは信頼として要求されるレベルが非常に高いですね。相手にする人も、どんな人を相手にするかわからないというのがあるので、そこの部分での対応レベルというのは自然と高くなるということです。その中で「安心」を確保する対象というのは、実は中の人たちのことを申し上げています。

「安心」それは決まった通りにやっていれば大丈夫であるという確信

これがマネジメントシステムの中でいろいろルール化をして、皆に教育して浸透させることの目的です。

さきほど申し上げたように、セキュリティのレベルというのは極めて相対的なものです。相対的ということは、裏を返すと何をどこまでやっていいかわからないということになります。その判断を個々の人間に任せるのは危険ですし、社員ごとに当然判断はブレます。また現場の社員さんたちは、そんな怖いことはできないということになります。

ですから、ちゃんと決めて社長が承認したルールに基づきその通りにやったということであれば、もしその下でなにか起こったとしても、それは個々の社員のミスではなくて、それ相当にやったという前提があれば、ルールが悪かったということになります。つまりそれは、組織の責任ということになります。ですので、情報セキュリティにはいわば組織の人たちを守るといった目的もあるわけですね。そこが「決まった通りにやっていれば大丈夫であるという確信」です。

ただ、ルールを守らせることばかりに傾注すると、本来の目的を忘れてルールを守ること自体が目的となってしまい、顧客不満足を生んで逆にパフォーマンスの低下を招き、新たな管理の強化を生む、という「官僚制の逆機能」と呼ばれる現象が起きがちです。

これを打破するためには、リーダーになる人が先程のVision、Mission、Value[※1]に照らして適切な介入を行う必要があります。ある意味、時にはマネジメントを壊さねばならないのがリーダーシップです。これについては後ほど詳しく述べさせて頂きます。[※2]

※1　参照: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?』10年後の姿・やるべきこと・価値観をもとに戦略を立てる
※2　参照:セミナーレポート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』マネジメントの弊害を打ち破るのは「リーダーシップ」

ゼロリスクは無理。自分たちが責任を持てる程度を保つことがポイント

情報セキュリティにおける安全というのは程度的なもので、それは自分たちが責任を持てる程度に、というのがポイントです。なぜかというと、ゼロリスクというのは無理ということですね。情報を扱うということは、必ず一定のリスクが発生します。

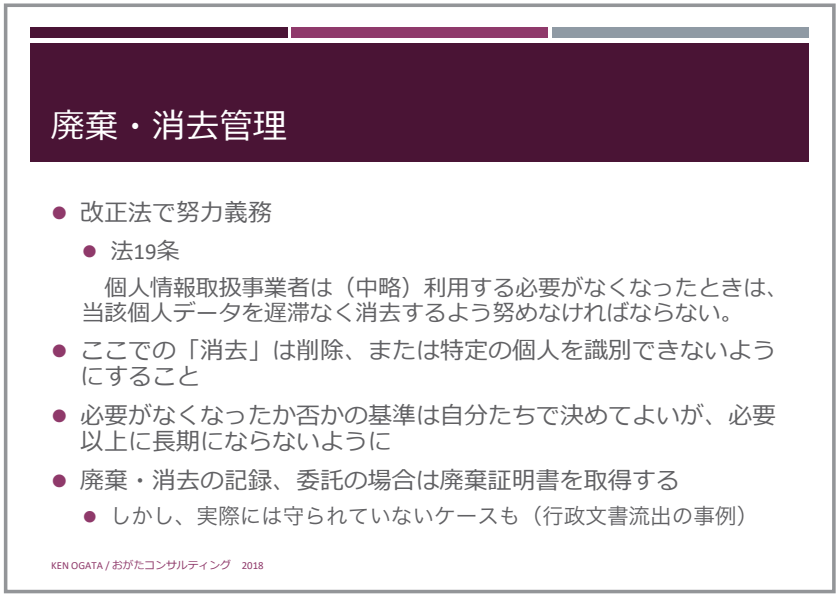
情報が漏れないよう、例えば模式的に鉄のカプセルみたいなものに入れてしまうと考えると、一応安全だけれども使うためには、穴を開けないといけないですよね。穴を開ければ当然そこには、穴という脆弱性がリスクの要素として、出てくるわけです。

ISMSでは建物のセキュリティの話をする際に、地震の震度をいくらまで耐えられるようにしますか、というのがあります。例えば、震度8とか9クラスの地震なら地面にアンカーを打ち込んでも無理ですよね。だとすると、建物が崩れてしまうくらいの地震がきたらこの会社も機能停止しているはずだから、とりあえず震度6くらいまではなんとかなるように、ちゃんと補強された部屋に入りましょうとか、サーバー等は固定しましょうみたいな、そういった話になるわけです。そういうことをちゃんと、会社の判断として責任が持てる程度に保たれている状態というのが、大事になってきます。

そして「根性ではなく科学」である必要があります。情報でも環境でもリスクマネジメントというのは全部それだと思います。誰がやっても結果が同じになるようにという再現性の話です。リスクマネジメントとはそういうことなんですね。

個人情報の廃棄･消去のベストな方法とは？

次は情報の廃棄･消去の管理の方法についてです。現状の個人情報保護法では、利用する必要がなくなった時は当該個人データを遅滞なく、消去するよう努めなければならないと定められています。ここでいう「消去」とは「削除または特定の個人を識別できないようにすること」です。



例えば個人情報が書き込まれたハードディスクがどこかに売られてしまったら、そこからデータを抜かれてしまう可能性がありますよね。ですから、もしハードディスクの廃棄･消去を外部に委託する場合は、廃棄証明書を取得するのがいいでしょうということになっています。しかし実際に起こった行政文書流出事件のように、廃棄の約束が守られていないケースがあるのも実状です。そのため物理破壊するか、暗号化した上で廃棄する対策をとる自治体や組織も出てきました。

また完全消去ソフトというものもあります。アメリカ国防総省（DoD）の方式で3回上書きとか、アメリカ国家安全保障局（NSA）方式で上書きみたいな方法もありますが、それでも確実ではないというのが最近の研究です。データを100％完全に復元するというのは無理ですが、データの残骸みたいなものを一部濾し取れれば脅迫としては十分ですよね。そういった意味では完全な消去というのは無理だろうと言われています。

ですから、結果的にはハードディスクは消耗品で使い捨てと考えた方がいいのかもしれません。完全消去よりは物理破壊の方が確実だと思います。もしも私が相談を受けたらそういう風にお答えします。

それではハードディスクではなく、クラウドならどうでしょうか。ご存知の通りクラウドは全世界にデータセンターがあって、分散して情報を保管しています。そのため仮に手元でデータを消去したとしても、実はどこかのサーバーには残っているわけです。自分達でも分かりません。分からないけど、どこかに残っている、抽象的にはそうです。

そのため今とられている重要書類などを消去する方法としては、特定の個人を識別できないようにすればいいので、暗号化して鍵を捨てるということになっています。そうすると情報を呼び出せなくなるので捨てたことになるわけです。クラウドでは消去に変わる手段として、そのような方法がとられています。

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。