<タイトル>

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—EA がもたらす最適化とは ～

<リード>

さまざまな法例や規制への対応が求められるようになった企業の IT 部門。企業のメインテーマである「ビジネス」という大前提を崩さずに、コンプライアンスを進めていくにはどうすべきか？—日本ヒューレット・パッカードで個人情報保護対策室長を務める佐藤慶浩氏に、コンプライアンスと IT のバランスについて話を訊いた。

<本文>

■異なるコンプライアンスを IT に取り込む

—企業を取り巻く法対応とそれに伴う IT の現状と課題について、見解をお聞かせください。

まず、IT に限らず広い視点からいうと、マネジメントサイクルとして PDCA というのがあります。

今多いのが、個人情報対策 PDCA、SOX 法対策 PDCA、情報セキュリティ対策 PDCA・・・といったように、コンプライアンス側の PDCA として複数の PDCA を設けてしまっているケースです。複数の PDCA の間で整合がとれない。あるいは、気付いてみたら職場には、SOX 法責任者、個人情報管理責任者、文書管理責任者、防災責任者とあって、3 人しか人がいない部署に 10 個ぐらい役割があります、というようなことが起こっています。会社にとっての PDCA は 1 つというのが理想です。そこにいろいろなコンプライアンスが入る。とはいえ、PDCA をやるためにビジネスをやるわけではないので、その PDCA に対してビジネスをどう合わせていくのか。この部分は IT に限らず、もう少し広い枠組みで考える部分です。

IT に関していえば、今までだと、たとえば「売り上げを伸ばす」といった目的のために IT をつくるという、いわばビジネスの目的に対する手段として IT がありました。ところが、コンプライアンスで考えると、何か IT のシステムがあって、コンプライアンスに適合させなければならないといったときに、コンプライアンスのことをそんなに気にしなくてもよかった時代に比べると、目的以外の制約に合わせて構築するというアプローチに変わったということですね。

—コンプライアンスは IT の目的ではないということでしょうか？

コンプライアンスのための手段を IT でつくるというときは、コンプライアンスが目的になるので、今までの IT 構築の考え方と同じです。

しかし、今いわれているコンプライアンスというのはむしろ、何らかの目的がある IT システムがコンプライアンスを満たすようにしなければいけない。そのITシステムの目的ではないことになります。要件としてコンプライアンスを見なければいけない。ここが、これまでの IT 構築と違うところです。IT化されたものがまずあって、それに加速的に複数のコンプライアンスに対応しなければいけなくなった。

この 2 つの点を咀嚼するのがこれからの IT 部門なり、IT なりの課題ではないでしょうか。

目的のための手段として IT をつくる際に、要件を満たすということを一緒に取り込まなければいけない。

どうやって取り込むかに関しては、方法はおおむね限られていると考えています。

まず、コンプライアンスの観点でどういうことをしなければならないのかという要求事項を出す人がいます。その人は逆にいえば、あまり他のことは考えないでそれだけ出します。

次の人が、IT にそれをどう取り込むのか、あるいはそれを取り込んだことで他に弊害が起きないのか、といったことでレビューをします。この作業は、アーキテクチャ・レビューといって、他との整合性を図りながらシステムの設計図を見ていくという作業です。

最後に、これらの結果をビジネス側で受け入れられるかどうか。IT システムは通常は企業の場合だと、何らかのビジネスの目的のために存在しています。そこでビジネス側が、新しいアーキテクチャになってもいいのか、あるいは利便性が落ちたり、使い勝手が悪くなっていいのか、それでいいのか受け入れる、3 つの段階を回していくという方法です。

それぞれの段階で、何か問題があったら差し戻します。たとえば、アーキテクチャ・レビューの結果、コンプライアンスに確認したいことがあれば、コンプライアンスの人に戻ることもあるし、あるいはコンプライアンスを満たすための要件はそろい、整合の問題が生じることはないといいうことがわかったが、一番大切な部分であるビジネスの目的に対してどういう影響があるのか、場合によっては、コンプライアンスはよくなったけど、ビジネスができなくなるということでは差し戻しになるかもしれない。

「目的の手段」としてだけ IT があった時代は、目的を達成できるかということでよかったのですが、今は、オープンシステムによるアーキテクチャ上の整合性、コンプライアンスからくる要求事項、そしてビジネス目

的達成という 3 つの観点で考えることが求められているのではないでしょうか。

—最初の段階でコンプライアンス要件を出す人、あるいは最後の段階でビジネス的な判断をする人というのは、横断的に連携する必要はなく、アーキテクチャ・レビューを行う人が、いわゆる「横串」の役割を果たすということでしょうか。

連携できればそれに越したことはないのですが、割り切ってしまえば、必ずしも連携しなくてもよいということです。会社の方針として、横串を刺すことが決まっていれば、もともとアーキテクチャ・レビューをする人は、横串のためにいるので、その人が吸収します。たとえば個人情報保護のコンプライアンスがあって、SOX のコンプライアンスがありました、というときに、その要求をそこでミックスするのではなくて、それぞれの要求はそのまま直接出す。それをアーキテクチャのところで吸収し、どうやって横串を刺すかは、アーキテクチャが考えるという考え方でやるのがいいと思います。

すごく多様性のある人がいれば、もしかしたら全部を 1 人でできるかもしれませんが、実際には、最近出ているようなコンプライアンスの問題に対応できる 3 つの能力を兼ね備えた人をアサインするのは難しいでしょう。でも、コンプライアンス担当の人、アーキテクチャ・レビュー担当の人、ビジネス・アライメント担当の人がそれぞれの役割を担うのはそんなに大変じゃない。コンプライアンス対応の人は、乱暴な言い方をすれば、アーキテクチャのことは知らなくてもいいと、割り切るというやり方はあってもよいと思います。

■異なる要件を横断的に捉える

—なるほど。横串を刺す部分が肝のようですね。この部分についてもう少し、詳しくお聞かせください。

ソリューションの言葉だと、EA（エンタープライズ・アーキテクチャ）と呼ばれているものです。日本はおろか、米国でもまだ本格的に立ち上がっているところは少ないです。ITに関係するところとしては、IT アーキテクトと呼ばれる人がいます。これはそういった部署があるというよりは、IT の中の役割の名前ですね。

IT アーキテクトの人にコンプライアンスをしなさいというのは、コンプライアンスが 1 つくらいならできるかもしれませんが、今のように複数ある場合、現実的ではありません。いくつも出てくるようだったら、そこはコンプライアンスの人に任せる、というようなことがいいのではないかと思います。

アーキテクチャの人は、もともと横串を刺すことのプロです。コンプライアンスのプロではないけど、横串を刺すことのプロなので、その人にコンプライアンスの要求事項を与えてITに横串を刺してもらうと、結果的にコンプライアンスに横串を刺すことになるわけです。

現在の日本企業のコンプライアンス対応を見ていると、この 3 段階をまたいだことを人や部署に期待をしてしまっている場合が多いですね。これは非常に難しいことだと思います。

—先ほど、「コンプライアンスは IT の目的ではない」とおっしゃっておられましたが、今日の IT ベンダーのアプローチを見ると、コンプライアンスのための IT といったスタンスが多く見受けられます。目的があって、コンプライアンス要件を満たす IT という考え方は基本なのかもしれませんが、そういう意見が表立って出てくることが少ないような気がします。

コンプライアンス対応そのものを支えるシステムというのもあります。たとえば社内教育の受講管理システムなどがあります。

また、ERP は業務処理そのものを管理するために用いられる IT ですがコンプライアンスにも対応できる。なので、ERP を強化しておくと、コンプライアンス対応をしやすい。

SOX 対応だけで考えると、SOX 対応をいかにこなすかということでパンク寸前になっている企業があるかもしれませんが、むしろそのシステムをビジネスにどう生かすかといったことを併せて考えていくのがいいと思います。

SOX だと結局経理システムの完全性(Integrity)を正確に保ちその説明責任を果たすということです。説明責任を果たすためには、本来法律は求めていないけれど、ほぼリアルタイムに経理状況がわかるシステムはビジネスにも役立ちます。法律の要件だけでいえば、別に年度末にチェックすればいいんです。でも、1 年間やったことを年度末にまとめるのではビジネスにはほとんど貢献しない。そうではなく、日々の業務の中で、経理処理が可視化されていると違ってきます。たとえば、収支計算書は年度末に作成するわけですが、それは経理処理がIT化されていなかったときの常識であって、経理そのものとそれを取り巻く様々な処理がIT化されている現在は、今日時点の収支計算書をリアルタイムで見れてもよいわけです。それができれば、現場レベルのキャッシュフロー・マネージメントができるようになります。

それをわざわざ寝かせておいて、365 日たってから処理するとなると、まさに SOX 法対応用のコンプライアンス・システムの構築になってしまいます。これは現場のビジネスからするとなんの役にも立たないんで

すね。

以前は商品には利益率が割り振ってあって、それを売る営業部門には、売り上げ目標が設定され、それを達成すると定率の利益が得られるということを前提にしていました。しかし、いまどきは、そんな単純なことではなくなっています。企業にとって必要なのは、売り上げ倍増だけでも、コスト半減だけでもない。その差額である利益を向上させることだとすれば、その判断材料となるキャッシュフローを現場が「見れる」ようにするということは、コンプライアンスではなく、ビジネスツールとして考えることができ、営業管理のツールとして非常に役立つ感じですよね。そのあたりのことまでやれれば、コンプライアンス用のシステムにならないと思います。

—コンプライアンス目的の IT にならないようにするには、アーキテクチャの部分が問われることになりそうですね。このアーキテクチャの部分がない会社も多いと思うんですが、こうしてみるとアーキテクチャがないとうまくいきませんね。

アーキテクチャがなくても最終的にコンプライアンスの要求を満たせばいいのですが、それでは共通でやることが限られコストがすごくかかると思いますね。EA があれば確実にできますが EA なしでできている企業もあります。属人的ですが、コンプライアンスのこともわかっていて、ビジネスのこともわかっているというようなスーパーマンがIT戦略を立案し実践しているような人がいて頑張っている場合です。日本だとそういうケースが多いのじゃないでしょうか。スーパーマンが多いというか、スーパーマンが期待されてしまっているというか。しかし、ここまで技術の進化が早まり、コンプライアンスもビジネスも多様化してくると、それはそろそろ限界じゃないかと思います。

■リスクは細部に宿りたもう

—今、企業の間では、法対応を超えた取り組みとして、リスクを統合して管理していこうという流れがありますね。統合的リスクマネジメント（ERM： Enterprise Risk Management）と呼ばれたりしています。この 3 段階の仕組みは、ERM とはまた違うのでしょうか。

流れは違うわけではないのですが、まず、ERM については、現在のところ抽象的な説明が多くて具体的

な説明がないように思うので、多くの人はプロセスをフレームワークにするものだと勘違いしがちです。僕の意見は少数派かもしれませんが、プロセスを一番外側のフレームワークに置くのはちょっと教科書的だと考えています。なぜなら、企業はリスクマネジメントのためだけにあるわけではないからです。それだけじゃ現場は動かせない。コンプライアンス対応、リスクマネジメント対応といったものは、たとえば、SOX 対応のように何か新しいコンプライアンス対応が出た時には勢いで一瞬何とかなりますが、それを将来的に継続する必要があります。だから、リスクマネジメントで業務を分析するのではなく、リスクは業務の随所に埋まってます、「リスクは天空にいる」のではなく「リスクは細部に宿りたもう」という考え方の方が現実的なのではないでしょうか。

—それは、いわゆる ERM の「まずリスクを棚卸しする」というのとは真逆の考え方ですね。

そうですね。リスクアセスメント、リスクの棚卸しを時間的空間的に集中してやるというのはあまり現実的だとは思えないですね。時間的というのは、PDCAのライフサイクルのどこかの時点で、空間的というのは、企業の中の特定の部署でするということです。そうではなくて、コンプライアンス担当はコンプライアンス問題に遭遇したときにコンプライアンスに違反してしまった場合のリスクを考える。アーキテクチャ担当はアーキテクチャを見直す必要が出たときにアーキテクチャが矛盾してしまった場合のリスクを考える。ビジネス担当の人は、用意できたものがビジネスに対して矛盾してしまった場合のリスクを考える。

つまり、リスクマネジメントのプロセスが外側にあるのではなくて、プロセスは随所にあって、リスクの程度判定は一番近いところにいる人がやるという考え方です。組織としては、リスクの大きさに応じて受け入れを選択する際の承認手続きを一律に決めておく。このやり方の欠点は判定が属人的にしかならないということでしょうか。担当者の判断ミスでリスク判定を誤る可能性があります。しかし、だったら、そこを属人的じゃなくできるのか？という割り切りかもしれないですね。リスクの程度判定そのものは、各部署に任せることになります。そこを集約して、リスクマネジメントの担当部署のようなところをつくってまとめて判定するということとは真逆の考え方ということになります。

たとえば、個人情報保護対応は顧客満足度向上の目的にぶら下げます。そして SOX 対応は現場の経理のビジュアライズ、つまり、生産性向上にぶら下げます。まずその目的の下で必要なことを考える。

顧客満足度を向上させるためには、利用目的の通知に関してどういう文言がよいかとか、同意を得られなかったときにどうするのか、顧客満足度の観点でまず答えを出します。その後に答え合わせとしてコンプラ

イアンスを持ってくるわけです。その結果、法律よりも厳しいレベルが自らの答えだったのであればわざわざレベルを下げる必要はない。それは顧客満足度向上のために必要なのだから。逆に、企業が自分で出した答えがコンプライアンス要件よりも低かったらこれは上げなくてはならない。そのように答え合わせとして考えるのがいいのではないでしょうか。

そう考えると、リスクマネジメントのプロセスというのは、個々の処理とか、個々のイベントの中に内在するのであって、どこか外にあるものではないと思うんです。

確かに、「リスクマネジメントを企業の要にすべし」といって、プロセスを一番外側に持っていこうという意見も多いことは確かです。ただ、実際の企業事例としてプロセスを一番外側に持ってくるっていうのはあまり聞いたことがないですね。

それは結局、リスクマネジメントのプロセスを集約なんてしたら、どこでリスクとビジネスのバランスを取るのか、ということだと思うんですね。ノンリスクでビジネスができるのかという話です。ビジネスをする局面でリスクに遭遇したときに、ビジネスを捨てる覚悟がある企業は集約すればいいですが、なかなかそういう時代ではないと思いますね。

ERM はまだ成熟してはいないので、実践的な話として、僕がいうようなタイプの ERM もあるし、異なるタイプの ERM もあって、どちらがいいというわけではないと思います。それは自社にあったやり方を見つけていくのでよいと思います。

—ありがとうございました。（聞き手・文／小泉真由子）

＜インタビュイー＞
日本ヒューレット・パッカード株式会社
個人情報保護対策室　室長
佐藤慶浩氏

＜プロフィール＞
1990 年、日本ヒューレット・パッカード(株)入社。
1997 年以後は、通常のコンサルティング活動の他に、各種の講演をしている。
2004 年 6 月、個人情報保護対策室長に着任。
2004 年 11 月、ヒューレット・パッカードのプライバシー・オフィスに所属し、日本のチーフ・プライバシー・マネージャとして全社施策の推進にあたる。
詳細は、http://yosihiro.com/profile/ にて紹介。