

Protiviti Japan Report

セキュリティマネージメント

1 形から入ったセキュリティも実を獲る時代へ

近年、インターネットの普及と共に企業が直面するセキュリティ環境は大きく変貌を遂げました。従来からある汎用機と呼ばれるコンピュータの世界は、通信手順(プロトコル)がコンピュータベンダー独自のものを利用していたため、外部から不正に侵入しようにも、入り込む手段がないために、セキュリティといえどもっぱら内部のセキュリティを考慮していれば良かったのです。ところが、95年以降インターネットが普及してからは、コンピュータ同士の通信手順がTCP/IPという標準的かつオープンなプロトコルに取って代わり、コンピュータ同士の接続が飛躍的に容易になったのと同時に、外部から不正に侵入する行為も同様に飛躍的に容易になりました。つまり、この10年でセキュリティは内部の管理中心から外部の管理まで幅を広げなければならなくなりました。ところが、残念なことに、この大きな環境の変化に迅速に対応を取られている企業は多くなく、90年代後半以降、様々なセキュリティに関する事故・事件が多発しています。そのような中、情報セキュリティの大切さに関する認識が徐々に高まり、この2-3年の間には、情報セキュリティポリシーを作成する企業が増えました。情報セキュリティポリシーとは、本来は会社として情報セキュリティをどのように捉え、どのように取り組むのか?を方針としてまとめあげた文章であり、情報セキュリティへの取り組みの第一歩となります。つまり、会社が主体として、会社の各種「情報」に関する様々な客体(情報の取り扱いルールや外部からの脅威など)をどのように取り扱うか?を定め文章にするものです。ということは、主体である「会社」は企業ごとに業種・プロセス・文化・風土も違えば、そもそも別の法人格ですし、客体となる事象も会社ごとに異なるはずですが、しかしながら、これまで多くの企業が作成してきた情報セキュリティポリシーは、「雛形」をベースにしたカスタマイズによる文章で、形式的に情報セキュリティポリシーを整えた、に過ぎないケースが多かったろうと思われる。そこに大きな落とし穴が潜んでいるのです。

形式的に揃えた情報セキュリティポリシーの問題点は、企業の業務の実態に則していない、あるべき姿を規程として採用したために業務が回らなくなる、その結果守れないルールが出来上がり、違反行為が横行し、ポリシーが有名無実化してしまう等があげられます。今、企業は自らの情報セキュリティに面と向かい、自社にとっての情報セキュリティとは何か?をもう一度見つめ直し、実のある「情報セキュリティ管理」を目指す段階に差し掛かっているといえるでしょう。

2 情報セキュリティ管理(ISMS)とは

情報セキュリティ管理(別名ISMS : Information Security Management System)という言葉が一般的に使われるようになったのは、2002年の4月にスタートしたISMS認証プログラムの貢献が大きいです。ISMS認証プログラムはISO17799というISOで規格化された情報セキュリティ管理に関するガイドラインをベースに日本のJIS規格がJISX5080として策定したガイドラインを基に、JIPDEC(日本情報処理開発協会)が日本に見合った形のISMS基準に焼き直し、その基準に則した情報セキュリティ管理体制を運営している組織に認証を付与するということです。また、ISMSの原型となったISO17799は英国の規格であるBS7799をベースにしており、元を辿れば英国の情報セキュリティ管理に関する規格が今や世界的な模範となっているのです。

さて、次に情報セキュリティ管理(ISMS)の内容について触れたいと思います。情報セキュリティ管理は、情報セキュリティに関するPlan Do Seeのマネジメントプロセスを確立し運営維持することです。上述した情報セキュリティポリシーはこのPlanの中で作成される成果物となります。情報セキュリティ管理のプロセスの例をJIPDECのISMSを例にとりてご説明しますと、

1. ISMSの確立
2. ISMSの導入および運用
3. ISMSのモニタリング
4. ISMSの改善

のPlan Do Check Act の4つの管理プロセスを回すこととなります。ここで、余談になりますが注意の必要な事がありますので解説を加えておきます。管理プロセスをPlan Do See の3段階で表現するケースと、Plan Do Check Actのように4段階で表現するケースがあります。最近では4段階で表現されることが多いですし、一見すると、どちらも同様のことを言っている様なのですが、この違いを明確に認識しておくことが、管理プロセスを成功に導く第一歩となります。両者の違いは、役割で分けているのか、機能で分けているのか、の違いになります。つまり、3段階の表現は、「役割」で分けているのです。Plan(企画の役割)、Do(実行の役割)、See(モニタリングの役割)となるわけで、企業の実際の組織や担当に対して役割を与える際には、この3段階の表現が適します。また、4段階の表現は、「機能」で分けていることとなります。Plan(企画機能)、Do(実行機能)、Check(モニタリング機能)、Act(改善の企画・実施機能)となり、ここでいうActは実は管理プロセスが1周したあとのPlanとDo の機能を別出しで表現しているにすぎません。従って、4段階の表現を使用したときに、仮に1周しか回らない管理プロセスならば理解し易い表現ですが、通常は何周も回る管理プロセスであり、この場合には、冗長な表現になっていることに注意が必要です。また、4段階の表現をそのまま役割と勘違いして、実組織に当てはめようとすると、当然ながら冗長な分が実際の組織には適合せず、機能不全に陥ることは明白です。

3 情報セキュリティ管理体制の確立

それでは、次に情報セキュリティ管理体制を確立する方法について見ていきます。ここでは、JIPDECのISMS確立基準を例に、情報セキュリティ管理体制をどのように確立していくか、の構築プロセスをご説明します。まず、最初に実施するのが“1.今から取り組む情報セキュリティの対象範囲を明確にする”ことです。企業であれば当然、全社的な取組みを想定するわけですが、そもそもここでいう全社とはどの範囲を含むのか？例えば、“子会社やグループ会社を含むのか？”、“連結対象会社は含むのか？”、“業務の委託先を含むのか？”といった組織的な範囲を決めなければなりません。また、“情報システムのセキュリティだけなのか？”、“文章管理などを含めたセキュリティなのか？”といった情報の種別で区切る範囲などを明確にする必要があるということです。範囲の明確化の大切さは、言葉で書くとうりですが、実際に範囲を決定することは、非常に難しい作業となります。難しい原因としては、情報セキュリティ管理体制構築プロジェクト自体の権限・役割が不明確であったり、全社的な合意が取られていない場合に、各組織の抵抗にあたり、またプロジェクトメンバーが全ての組織、業務、情報を理解できていない場合に、そもそも範囲を決定する能力がない、などが考えられます。ですから、情報セキュリティへの取組みを成功させるための第一の要因としては、情報セキュリティの対象範囲を明確に決定できるプロジェクトチームを結成することと言えるでしょう。

2番目に実施するのは“2.情報セキュリティポリシーを策定する”ことです。ここでいう情報セキュリティポリシーは、1.で定めた対象範囲における情報セキュリティへの取組みの方向性と行動指針を基本方針として取りまとめたものであり、会社が事業を行うにあたって前提となる法的な要求事項や製品、サービスを提供する際の契約上の義務事項などを考慮した内容となります。また、情報セキュリティ管理体制を確立するにあたっての組織、体制、プロセスの整備方針を含んだ内容となります。さらには、“会社が置かれた現状の環境において情報セキュリティに関するリスクがどの程度あるのか？”を評価するリスクアセスメントの方針および評価基準を定義した内容を含む必要があります。情報セキュリティ管理体制の構築に、リスクアセスメントを行う必要があるということに、唐突感をお持ちの方もいらっしゃるかもしれません。そこで、少し余談にはなりますが、“なぜリスクアセスメントが必要なのか？”、そして“重要なのか？”ということについて解説を加えておきます。リスクアセスメントは、情報セキュリティのみならず、様々な管理プロセスに有効なアプローチです。その理由は、大きく次の4点に表されます。

1: 網羅性を確保するため

日常業務の中で、過去の経験から想定できるリスクに対して場当たり的に対応を施すのに比べて、リスクアセスメントを実施することは、潜在するリスクを網羅的に洗い出すことが可能となり、結果として『想定外であった』『起こるとは思わなかった』といった事態を回避することが可能となります。

2: どこまでやれば良いかを見極めるため

そもそも企業が抱える全てのリスクに対して一様に対策を施すことはコスト的にも、人的リソースの面でも不可能です。従って、限られた資源の中で最大限の効果のある対策を施すためには、リスクアセスメントを行い、リスクに対して優先順位付けを行ったうえで、対処することが必要となります。

3: 実効性・効率性のある対策を打つため

リスクアセスメントを行わずに、経験に基づき直感的に対応すると、リスクを過小評価した結果、有効に機能する対策にならない場合があります。また、その逆にリスクを過大評価した場合には、過剰な対策を施してしまう場合もあります。そういった、経験と感に頼った対応ではなく、リスクアセスメントを行うことで、リスクの大きさや真の原因(源泉となるリスク)を見極めることが可能となり、より効果のある対策を効率よく選択できることとなります。

4: 自己証明を果たすため

リスクに対する投資(対策)の説明責任を果たすためには、『なぜ』『なんのために』当該投資が必要なのかを自己証明できる手続きを踏まなければなりません。リスクアセスメントはまさにその『なぜ』『なんのために』を導き出す作業となります。

以上のように、情報セキュリティ管理に取り組むにあたって、リスクアセスメントを行うことが、肝要となるのです。

続いて、3番目に実施するのは、“3.リスクアセスメントについて体系的な取組み方法を策定する”ことです。ここで、リスクアセスメントの体系的な取組み方法を策定する、とあるのは、リスクアセスメントにはいくつかの手法が存在しますので、その中から、企業が置かれた環境に見合った最適なアセスメント手法を選択することが大事になるからです。また、リスクアセスメントの目的の一つが、どこまで対応するのか、というリスクの許容水準を導出することであり、説得力のあるリスクの評価基準や論理的かつ体系的な方法を特定することが必要となります。リスクの評価は一般的に、リスク発生の可能性とリスクが発現した際のビジネスへの影響度を用いて、優先順位をつけることとなります。この発生の可能性と影響度合いにどのような重み付けを行うかという基準を決めておく必要があるわけです。

リスクアセスメントの取組み方法を策定した後は、“4.リスクの識別”を実施します。リスクの識別に必要な要素は、そもそもセキュリティを維持する主体としての「情報」、それから「情報」を取り扱う客体としての社内の業務プロセス、また「情報」に対して影響を及ぼす客体としての脅威(ペリル)、また脅威を顕在化する業務プロセス上の根本原因である脆弱性(ハザード)の4つとなります。つまり、リスクの識別は、どのような「情報」に対して、その「情報」が取り扱われるプロセス上で、どのような「脅威」が存在し、その脅威が顕在化する原因としてどのような「脆弱性」があるのか、を洗い出すことです。(これらの洗い出し作業を通称リスクシナリオの導出と表現することもあります。)ここで肝心となるのは、あくまでも情報を取り扱うプロセス上の脅威や脆弱性を洗い出すことです。一般的な情報セキュリティリスク識別のアプローチ(JIPDECのISMSも同様)では、「情報」、「脅威」、「脆弱性」の3つの要素を識別するに留まっています。3つの要素でリスクシナリオを構成すると、どうしても漠然としたシナリオしか導出できません。例えば、顧客情報(情報)が、誰でもアクセスできる環境にあり(脆弱性)、社員が不正に持ち出し漏洩する(脅威)、というように、非常に抽象的なシナリオしか描くことができません。実は、現在多くの会社が取られているリスク識別の手法は、ここに大きな問題が潜んでいるのです。情報セキュリティをコンピュータシステム中心に捉える手法が世の中に多く出回っているために、情報を取り扱う業務プロセス要素を洗い出す作業を省略してしまっているのです。たしかに3つの要素でリスクを識別することは、情報セキュリティ管理体制構築プロジェクトを主に担当する情報システム部門の担当者だけでも作業が可能であり、簡便な手法の一つと言えます。しかしながら、本来は情報を取り扱う業務プロセスを識別しなければ、情報がどのように脅威にさらされ、どのような脆弱性によって、漏洩、改ざん、滅失されるのか、といった具体的な原因には辿り着けないはずで、上記の例に業務プロセスの要素を加えると、どのようなシナリオに変貌するかというと、顧客情報(情報)を利用して、新製品案内のダイレクトメールを送付する宛先リストを作成している途中に、誰でもアクセスできる共有フォルダー(脆弱性)に保存してしまい(プロセス)、本来はこのリストにアクセス権限を持たない社員の不正持ち出しによって顧客情報が漏洩する(脅威)、というように何が問題なのかにより具体的に把握できるシナリオを導出できます。具体的な原因が明らかでないリスクの識別は、具体的な対策を検討できない、中途半端な結果を導き出してしまいます。3つの要素だけで対策を検討すると、データを暗号化する、アクセス権限を厳格に設定する、データを持ち出せないよう出力媒体に統制機能を導入する、など大掛かりな体系的な仕組みが浮かんでしまいます。ところがプロセス要素を含めて対策を検討すると、顧客情報を取り扱うプロセスでは、共有フォルダーは使用しない、という運用上の対策も想定できます。業務プロセス上の脆弱性を洗い出す作業は、業務部門の力を借りなければ実現しません。したがって、全社的に業務部門を巻き込んで、リスク識別に取り組む必要があります。効率的な対策を導入するには、システムのなもの、人的な運用上のものを組み合わせて検討することが重要です。そのためにもプロセス要素を取り入れたリスクの識別をお勧めします。

セキュリティマネージメント

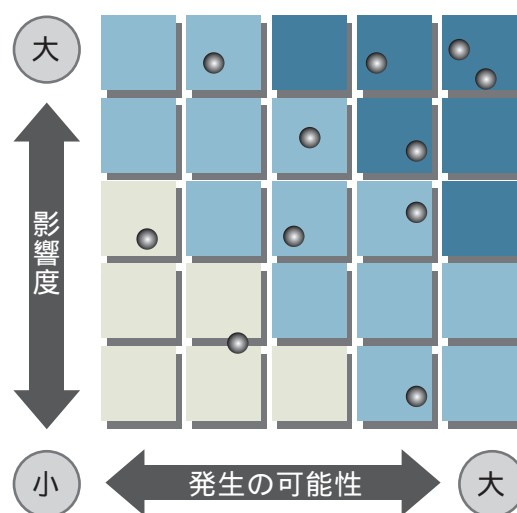
情報セキュリティへの取組みを成功させるための第二の要因は、情報を取り扱う業務プロセスの洗出しを省略せずに、業務部門を巻き込んで管理体制の構築を推進することと言えるでしょう。

リスクの識別が終了した後は「5.リスクアセスメントの実施」となります。リスクアセスメントの実施とは、4.のリスクの識別で洗い出されたリスクシナリオについて、情報セキュリティの3要素(機密性・完全性・可用性)が確保できなくなる可能性と、問題が発生した場合の影響度合いを、1.で策定した基準をもとに評価することです。評価結果は一般的にリスクマップ(右図参照)と呼ばれる、発生の可能性と影響度の2つの軸で表された2次元の表にプロットし、優先順位付けを行います。

続いて、5.で評価した結果を受けて「6.リスクの対応方針の決定」を行います。リスクの対応方法には、リスクを、受け入れて維持する(テイクする)軽減する、回避する、他のものに移転する、があります。したがって、5.でアセスメントしたリスクの現状に、会社としてどのように対応するかを評価し、決定することになります。リスクの現状が受け入れ難いものであれば、軽減、回避、移転、の中から対応方法を選定します。また、現状が許容できる場合には、現状のリスクの程度を維持するための対応を考えることになります。

リスクの対応方針が決まると、次に「7.具体的なリスク対応策の検討および導入」を行います。6.で決定した方針に則って、リスク対応の具体的な施策を検討します。リスクを軽減すると決めたリスクシナリオに関しては、どの程度までリスクを軽減するのかを明確にし、リスクの根本原因に対して最も効果的、効率的な対策をシステムの、人的、物理的なものを組み合わせて検討します。ここで、リスクを軽減することについて解説を加えておきます。リスクを軽減するとは、リスクの発生の可能性を軽減すること、リスクの影響度合いを軽減することの2つの側面があります。通常リスクを軽減するという場合は、発生の可能性を軽減することになります。なぜならば、影響度合いを軽減することは現実的に難しいからです。例えば、顧客情報が漏洩した場合の影響を考えた場合、顧客のセンシティブなプライバシーに関する情報を取り扱わないことにより、万が一情報が漏洩した場合においても、影響度は軽減できます。(情報漏洩による損害賠償額は漏れた情報のプライバシー度合いに関係することから)しかしながら、実際にセンシティブな情報を取り扱わないで、業務の遂行が可能であるかどうか、という問題は残るため、一概に取り扱わないことで影響度を軽減するという選択は難しくなるわけです。また、情報漏洩によって会社の風評が劣化し、売上が激減するといったリスクを考えた場合において、減少する売上金額を現実的に極小化するためには、あらかじめこういった事態に備えて保険を掛けるくらいしか手立てはありません。このようにリスクを軽減するとは発生の可能性を軽減することを中心に対策を考えます。ファイアーウォール、識別認証ツール、暗号化ツールなどのセキュリティ製品を導入することは、脆弱性を補完することであり、結果としてリスクが発現する可能性を抑えるという考え方に基づいています。また、リスクを受け入れる選択をしたものについては、ただそのまま放置しておけば良いわけではありません。受け入れるレベルにある現状のリスクを現在のままに維持する対策を検討し、導入しなければなりません。

図1 リスクマップのイメージ



セキュリティマネージメント

さて、ここまでの手順で、情報セキュリティ管理体制の構築を行ったあとは、構築した体制を運用、継続することになります。“ 8.情報セキュリティ管理体制の運用 ”の実施です。1.から7.までのプロセスを経て情報セキュリティ管理の枠組みを構築しても、情報セキュリティリスクがゼロになったわけではありません。リスクを軽減する活動を行ったとしても、残存しているリスクはあるわけで、運用フェーズでは、それら残存リスクの状況をモニタリングすることが重要となります。“ 許容したはずのリスクが増大していないか? ”、“ リスクを軽減するために導入した対策が有効に機能しているのか? ”を監視し、問題がある場合には速やかに対応と取るための手続きを構築しておく必要があります。

4 情報セキュリティ管理体制構築支援

プロティビティでは、情報セキュリティ管理に取り組もうとされているお客様を様々な形でご支援します。

5 情報セキュリティ管理方針策定を支援するサービス

支援内容は、お客様が情報セキュリティへ取り組むにあたり、まず現状はどのレベルなのか、また会社としてどのレベルを目指すのか、という方針を決定するフェーズで、プロティビティのコンサルタントがお客様の現状を評価し、お客様の経営戦略、事業環境などを踏まえた上で、目指すべき方向性をお客様と一緒に導出する内容となります。

図2 目指すべき情報セキュリティレベルの例

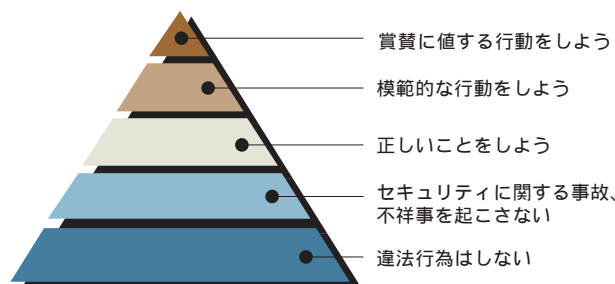


図3 情報セキュリティリスクマネジメントの成熟度で見た目標レベル

ステージ	能力の特徴	セキュリティの観点
最適化 Optimized	(継続的改善) リスクマネジメントが競争優位の要素として活用される	<ul style="list-style-type: none"> ・前者的セキュリティリスク管理が実行されている。 ・積極的にリスクを活用(テイク) ・知識の蓄積と共有
マネジメント Managed	(リスクの予測可能) リスクが評価され、全社で包括的に管理される	<ul style="list-style-type: none"> ・セキュリティリスクを予測可能な評価方法の確立 ・リスクとリターンとのトレードオフについての徹底的な討論
定義・制度化 Defined	(プロセスの標準化) プロセス・基準が定義され、制度化される	<ul style="list-style-type: none"> ・スタンダード、プロシージャの導入 ・標準化された作業 ・スタンダードに基づいたセキュリティインフラの導入
反復 Repeatable	(規律ある状態) 反復可能なプロセス 基本方針の確立	<ul style="list-style-type: none"> ・セキュリティポリシーが策定される ・共通言語 / 適任者の選任 ・定義された作業 ・初期のセキュリティインフラ導入
初期段階 Initial	(場当たりの) 傑出した社員への依存 制度的な機能の欠如	<ul style="list-style-type: none"> ・責任が不明確 ・場当たりの対応 ・主要な人への依存

6 情報セキュリティリスクアセスメントを支援するサービス

支援内容は、お客様が取り組む情報セキュリティ管理の中で、セキュリティリスクの識別、リスクアセスメントの実施、のフェーズにフォーカスし、プロティビティのリスクコンサルタントがお客様の環境に見合ったセキュリティリスクの識別方法、アセスメント方法を提供する内容となります。プロティビティでは、リスクアセスメントを効率的に実施するためのフレームワークを保有しており、ツールを利用し、短期間で精度の高い合意形成を構築する手法を提供します。 リスクアセスメントワークショップ(またはセッションとも呼ぶ)を開催し、下記の手順でリスクの識別、評価を実施します。

関係する経営者や担当者にセッションへご参集いただく

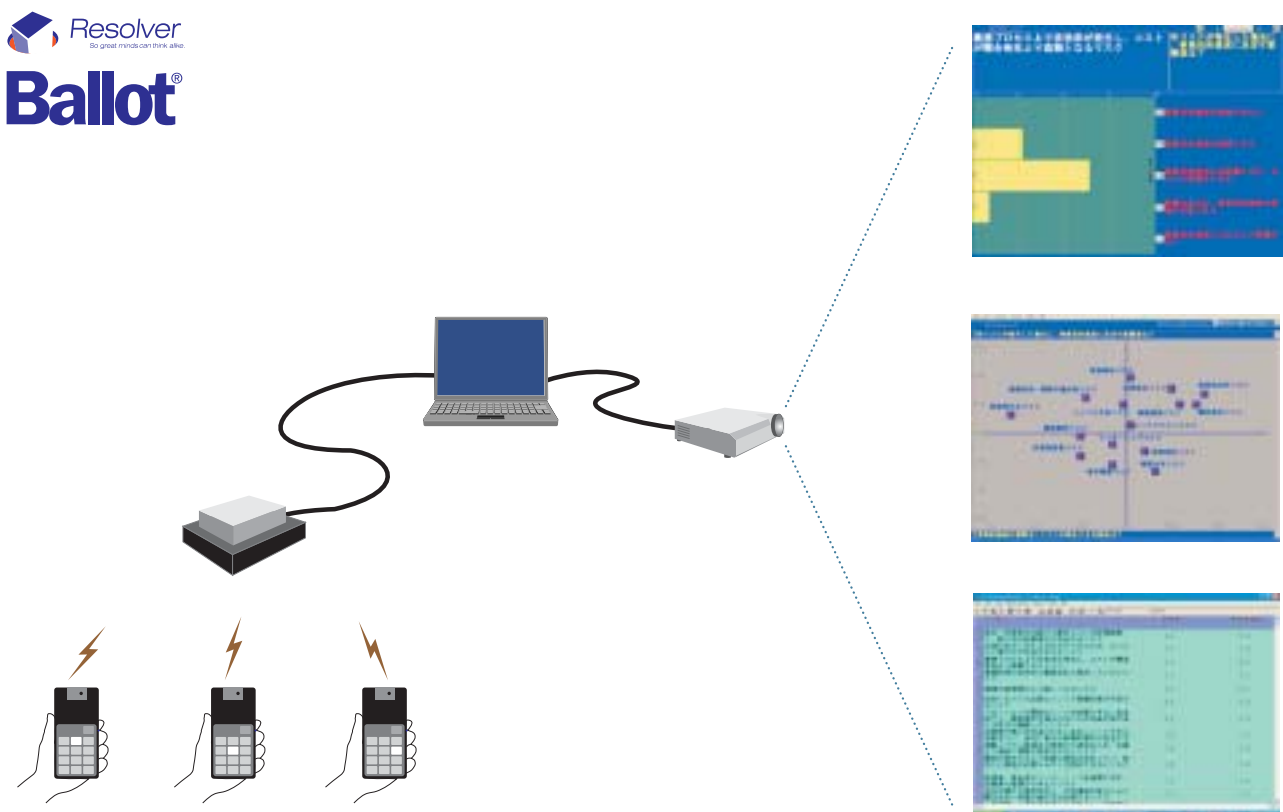
プロティビティのコンサルタントがナビゲート役を努め、お客様におけるセキュリティリスクやビジネスリスクについて、プロティビティが用意するフレームワークをベースに討議していただく

セッション参加者に、お客様におけるリスクの発生の可能性と影響度を評価していただく

評価にあたっては、専用の投票ツール(Ballot)を使用し、討議だけでは拡散しがちな議論を効率的に収束させ合意形成に導きます

参加者の協議結果および優先順位付けの投票結果はプロティビティがレポートにまとめてご報告

図4 リスクアセスメント支援ツールのイメージ



7 情報セキュリティ管理のモニタリングを支援するサービス

支援内容は「“ 情報セキュリティの対策(コントロール)が有効に機能しているか ”の評価」、「“ 情報セキュリティポリシーやスタンダードに準拠した業務運営を行っているか ”の診断」をプロティビティのセキュリティコンサルタントおよび提携する情報セキュリティのエキスパートが実施する内容となります。

主な診断内容

- セキュリティ対策(コントロール)の有効性レビュー(リスク軽減度合いの評価)
- セキュリティプロセスの準拠性レビュー(ポリシー・プロシージャーへの準拠性を評価)
- 脆弱性レビュー(不正侵入テスト、パスワードクラッキング、アクセスコントロールレビュー、など)
- レビュー結果を基にしたマスタープランの見直しとコントロールの修正提案

8 情報セキュリティ統合管理システム

プロティビティは自社開発の情報セキュリティ管理を支援するリスク管理支援ツール(PGP: Protiviti Governance Portal)を提供しています。これまで、情報セキュリティ管理体制を構築するとなると、情報資産の洗い出し、リスクアセスメント、コントロールのデザイン・導入、モニタリング、といった一連のマネジメントプロセスを、ほとんど手作業の管理(Officeツールでのデータ化が精一杯)が実状であり、管理体制を運営すること自体に大きな工数が必要となっていました。また、マニュアル管理のために、一度行ったP D C Aのマネジメントサイクルを次年度以降回そうとしても、過去の履歴や現状のステータスがデータベース化されていないことから、継続的な改善活動が難しいのが現状でした。

プロティビティがご用意するリスク管理支援ツールは、特に情報セキュリティ管理専用というわけではなく、広範なリスク管理にご活用いただけるプラットフォームです。

つまり、管理対象(セキュリティ・コンプライアンス・品質・環境・など)が変わってもご利用いただけるようにデザインしています。

PGPの特徴

PGPは情報セキュリティ管理のフェーズ毎に以下のようなご活用が可能です。

- 情報資産の洗い出し: 情報資産を入力、DBとして管理
- 社内組織の整理: 社内組織を入力、DBとして管理
- 業務プロセス分析: 各種業務プロセスを入力、DBとして管理(プロセスフロー描画機能あり)
- 業務プロセスの中の業務タスク(1つ1つの作業)を入力、管理対象としてDBで管理
- リスク認識: 業務タスクに関連するリスクシナリオを入力、DBとして管理(タスクとリスクの関連付け、リスクシナリオとリスクモデルとの関連付け)
- リスクの評価: リスクシナリオの源泉となるリスク(脆弱性)および脆弱性が現実となるリスクドライバーをリスクシナリオに関連付けしDBで管理
- コントロールのデザイン: 脆弱性およびリスクドライバーに対するコントロールを設計後、入力しDBとして管理
- モニタリング: コントロールの評価結果を入力し、コントロールの有効性 リスクの軽減度合い、をDBとして管理
- 経営(マネジメント)からの現状ステータス照会機能: 情報、プロセス、組織、リスク、コントロール、どの観点からも情報セキュリティの現状を照会可能(セキュリティリスク管理状況の可視化の実現)

9 情報セキュリティ管理支援サービスを必要としているお客様の例

以下に列挙する事項に心当たりのあるお客様は、早急に弊社の情報セキュリティ管理支援サービスの導入をご検討されることをお勧めいたします。

お客様の会社は、正式に情報セキュリティポリシーを有していない

お客様の会社は、情報セキュリティポリシーを作成しているが、情報システム中心に策定したため、全社的なセキュリティ文化の醸成につながっていない

お客様の会社の情報セキュリティ管理は、法制度対応のレベルに留まっている

お客様の会社には、情報セキュリティやリスク管理に関する深い知識と技術を持った人材がいない

情報システム会社に情報セキュリティの支援を委託し、技術的な対策ばかりが進んでおり、人的な対策、教育などが遅れている

ISMSは構築したが、統合的なシステム管理ツールは使用していない

お客様の会社は、外部の第三者から何らかの保障(サービスアグリーメント、品質保証、など)を求められている

お客様の会社は、個人情報を取り扱っている