2008年10月

コスト、複雑さ、リスク: 未来企業のためのセキュリティー

目次

はじめに

IBMの動向調査レポートであるIBM Global CEO Study『未来企業におけるIT部門のあるべき姿:The Enterprise of the Future』[1]によると、CEOやその他の上級ビジネスリーダーらは、新たなビジネス設計、破壊的イノベーションおよび継続的な経済のグローバリゼーションなどの変化によって、期待感に満ちた新たなビジネス環境の活性化と推進が行われると予測しています。CIOには、ITのアプリケーション、サービスおよびインフラストラクチャーを、融通の利く自動化された環境へと変革し、お客様の組織がますます動的になっている市場の機会を活用できるようにする責任があります。

多くのCIOと同じように、お客様も、ITセキュリティーとコンプライアンスがこのビジョンにとっての大きな障害になるかもしれないと感じていることでしょう。いずれにしても、その立場上、技術的変化の力が、すでにセキュリティーやコンプライアンスのコストと複雑さを大幅に押し上げていることを目の当たりにしていると思います。変化は、すぐにセキュリティーのアンチテーゼと見なされがちですが、将来はさらに大きな変化が待ち構えています。「リスク管理やビジネス継続性を完全にコントロールにはどうすればよいのだろうか」、そして「自分達の適応力を改善し、セキュリティーやコンプライアンスの目標が変化し続けていく場合に、リスク、複雑さおよびコストのバランスを効果的に取っていくにはどうすればよいか」といった問題が、まず頭に浮かびます。お客様はきっと、セキュリティーやコンプライアンスの問題がすべて、簡単に解決してくれればいいのにと思っていることでしょう。

非常に長い間、セキュリティー技術はITインフラストラクチャーやアプリケーションおよびプロセスのメインストリームから離れて開発、配備されてきました。その一方でベンダーは、それをどのようにメインストリームに統合すべきか、あるいはそれによってビジネス・プロセスがどれほど複雑になるのかといった問題に、ほとんど注意を払って来ませんでした。セキュリティーやコンプライアンスのコストは、間違いなく、IT予算の3倍の速さで高騰し続けるでしょう。

ハイライト

CIOは、未来の企業において変化の作用因子となりつつ、その変化がセキュリティーやコンプライアンスにどのように影響していくかという点にも対処していく必要があります。

未来の企業では、セキュリティーおよびコンプライアンスのソリューションを考案、応用および管理する方法を大幅に変革する必要があります。そのためには、お客様の組織にとって新たなタイプのセキュリティー・パートナーの登場が求められます。この新たなパートナーは、変革の力があるセキュリティー・ベンダーとして知られており、セキュリティー業界に長いことかけていた強力なベンダーのリーダーシップを提供するものです。このようなリーダーシップには、セキュリティーとコンプライアンスに関する新たなビジョンをサポートするために必要な最先端のセキュリティーの専門知識、幅広いITの専門知識、そして深みのあるリソースが含まれます。

この新たなビジョンは、お客様やお客様の組織によって共有されます。お客様の協力により、変革の力があるセキュリティー・パートナーは、次の3つの課題に対応してくれます。その3つとは、1) リスク管理を再定義して簡素化し、常に変化し続ける環境においてリスク、複雑さおよびコストのバランスをどのように取っていくかという点において、より明確な指針を示してくれる、2) シームレスな統合とビジネス主導という点を兼ね備えた総合的なセキュリティー・ソリューションの配備における最適な柔軟性を実現する最先端のセキュリティー調査、製品およびサービスなど、包括的なセキュリティーの枠組みおよびポートフォリオを提供する、3) リスクのライフサイクルを圧縮して簡素化し、セキュリティーのコストおよび複雑さを長期的に緩和する、ということです。

最終的に、このような変革を行うとセキュリティー技術が既存のインフラストラクチャーとビジネス・プロセスにしっかり統合されます。これにより、企業の資産としてのセキュリティーをめぐる管理が強化されるほか、セキュリティーとコンプライアンスの簡素化やコストの削減が実現し、進化し続けるお客様のビジネス・ニーズにより効果的に対応できるようになります。

傾向: 変化の力がITセキュリティー/コンプライアンスを高額で複雑なものに

セキュリティーの「パーフェクトストーム」に集約された5つの主要な力により、リスク環境は常に変化し続けています。つまり、複雑化とコストの増加も続いているということになります。

ハイライト

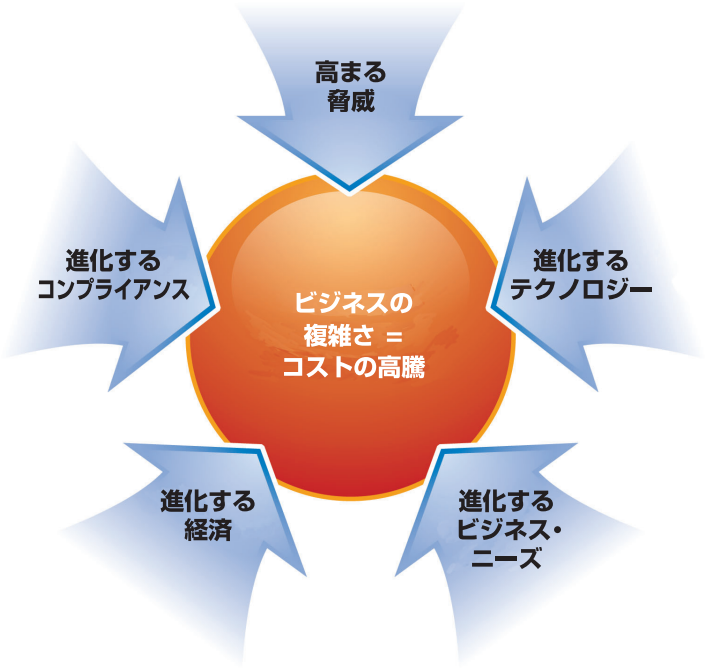

図1: 変化の5つの主要な力

社内外の複数の変化の力が、セキュリティーとコンプライアンスのコストおよび複雑さに直接的な影響を及ぼしています。

1. 高まる脅威

セキュリティーとコンプライアンスは、昔からこれほど複雑だったわけではありません。1980年代と1990年代のほとんどにおいて、ITセキュリティーは主にウィルス対策とファイアウォールで構成されていました。この比較的狭い技術範囲でも、多額のセキュリティー予算がかかりました。しかし近年になると、サービス妨害攻撃、ルートキット、ボットネット、ブラウザー・ベースの攻撃、スピアフィッシングやホエーリングなど、多岐に渡る脅威が出現しました。急速に変化するこのような背景については、IBM Internet Security Systems™ X-Force® Threat Reportに詳しく記載されています[2]。脅威の性質も進化し、単なるいたずらではなく政治的な動機および利益追求型の動機が明らかになっています。最新の脅威により、専門家による配備や管理が必要な新たなスタンドアロンのエージェントやアプライアンスが登場しました。これらのソリューションの多くが徐々に標準化され、スイッチ、サーバー、OSおよびその他のインフラストラクチャー・コンポーネントに組み込まれるようなっているといっても、さらに新たな脅威が発生し、それには新技術への新しい資本投資が必要となります。これらの新技術の資金は、既存のセキュリティー・ソリューションのコストですでに逼迫している予算から捻出しなければなりません。

図2：さまざまな種類の脅威の増加

2. 進化するコンプライアンス

組織にとってのセキュリティー関連の規制や業界のコンプライアンスに関する負担も、膨張を続けています。これらの指令の対象は、業界、国、および州などにより、さまざまに異なります。多くの管轄区域では、準拠違反があれば企業が民事罰および刑事罰の対象となるリスクを抱えることになります。したがって、上級経営陣にとってコンプライアンスは、予算の優先順位の協議の中で譲れないものとなり、通常は、同じ資金プールの中で予算を分け合う他のセキュリティー・イニシアチブよりも優先されることになります。

3. 進化するテクノロジー

仮想化、Web 2.0、サービス志向アーキテクチャーおよびクラウド・コンピューティングなどの技術の進化により、企業の境界線が拡大を続け、新たなビジネスの相互関係の道筋が確立されています。このような破壊的イノベーションは、新たなリスクの出現や、古いセキュリティー・モデルや投資の弱体化の原因にもなります。この場合、新たな対策が必要となり、ITに関する新しいコストや管理の問題が発生することになります。

ハイライト

4. 進化する経済

グローバル化された経済の力学により、ますます予算が苦しくなっています。ウォール街や世界の金融市場の最近の不安定な状態は、石油加工や住宅ローンの利率から為替レートといったさまざまな経済的要因の影響がグローバリゼーションによっていかに加速、増強され得るかということを、劇的に実証するものでした。乱高下の幅がそれほど酷くないとしても、世界経済の状況を受けてCIOは、セキュリティーおよびコンプライアンスの戦略および業務の調整を余儀なくされています。たとえば、諸外国の政府はそれぞれ独自の規制要件を提示し、グローバルな事業経営により24時間業務を行わなければならず、セキュリティー・ソリューションでは幅広い地理的条件、言語、法的要因および文化的要因に対処しなければなりません。

5. 進化するビジネス・ニーズ

ますます企業は、変化する市況に迅速に対処しなければならなくなっています。場合によってこれは、合併や吸収、または流通方法の変更といった戦略的動きを意味することもあります。あるいは、単にテクノロジー、人材およびその他の資産を適用し、社内の生産性の向上、サプライヤーとの協力の改善、およびお客様との関係の強化を実現するためのクリエイティブな方法を求めるという場合もあります。これらの項目にはたいていの場合、機密情報の可能性があるデータの共有が含まれているため、リスクの心構えに影響が及ぶ可能性があります。

CIOの最大のニーズ

リスク、複雑さ、およびコストのバランスをとること

上述した変化の力はどれも、計画と予算という点においてセキュリティーやコンプライアンスを非常に難しく、とらえどころのないものとしてしまうものです。

変化し続けるリスク、コストおよび複雑さのバランスを保つことは、CIOのセキュリティー疲労の原因となり、最終的に誤った選択をしてしまう恐れもあります。

したがって、企業にとって非常に重要なものであるにもかかわらず、ITセキュリティー/コンプライアンスはたいていの場合、散漫であり、管理上の負担になるものだとみなされてしまいます。お客様はきっと、こんなものがなければいいのに、と思っていることでしょう。しかしこれは避けることができないCIOの責任ですから、お客様は、複雑さを管理することができ、リスクが受容できるものとなる予算の絶妙なポイントを探さなければなりません。リスク、複雑さ、およびコストのバランスを取るという仕事は、これらの5つの変化の主な要素も、ほとんどがお客様の責任だということから、さらに難しいものとなっています。

データおよびITインフラストラクチャーのビジネスバリューがこれほど高くなったことはかつてありません。CIOであるお客様は、これらの戦略的資産を守るために、増え続ける一連のセキュリティー対策を管理していかなければなりません。しかし、セキュリティーはお客様の仕事の1つの側面でしかなく、お客様はその他のITの責務にも幅広く責任を負っているほか、お客様のリソースにも限りがあります。

セキュリティーやコンプライアンスの課題の複雑さや過酷なサイクルを考えると、CIOは「セキュリティー疲労」に陥る傾向があり、コストや労力を抑えるために近道をしようとするケースが多く見られます。

そこで、最も低いコストでコンプライアンス監査をするためだけの特定のソリューションを採用したものの、リスクは十分に緩和されなかったり、CIOがベンダーの数を減らすことでコストの削減を行おうとしたものの、特定のベンダーの製品やスキルがどのようにビジネス・ニーズと合致しているかという分析が不十分だったり、といった事態が生じます。

コストに対する対策のほとんどが、複雑さとリスクの両方に何らかの影響を与えることになります。

図3: 複雑さによるコストの緩和策がリスク・レベルを上げる恐れがある

セキュリティーを犠牲にせずにソリューションの簡素化に対する即応的なアプローチを生み出すような方法、つまり「即応的簡素化」によって複雑さおよびコストのバランスを取ることは、引き続き難しいものとなっています。常に変化するリスクや規制の環境にその場しのぎで対応する限り、セキュリティーが犠牲になってしまいます。差し当たりは圧力を受けて行われる安易な決定によって、短期的な予算の懸案事項は解消されるかもしれませんが、それによって多くのリスクに十分に対処しきれず、望まれない重大な結末を招いてしまうことになります。

では、より簡単にこのバランスをとるにはどうすればよいのでしょうか。より明確で目的主導の選択をするには、どうすればよいのでしょうか。私たちは、セキュリティー・ベンダーの役割と、それらのベンダーが現在ジレンマにどのように関係しているかを検討しなければなりません。

ベンダーの責務

リスク、複雑さ、およびコストの適切なバランスの維持に関しては、責任が最終的にはCIOおよびCISOで止まっています。しかし、多くの場合、ITセキュリティーとコンプライアンスに関するフラストレーションや混乱の責任は、セキュリティー・ベンダーの玄関先にあると考えることができます。何年にも渡り、純粋なセキュリティー企業が複雑で既存のITシステムとの互換性もない新たなテクノロジーを生み出してきました。これらのソリューションを開発するベンダーには、それらをお客様のためによりシンプルで安価なものにするための動機付けがほとんどありませんでした。

したがって、「セキュリティー・プロバイダー」の責任を想定するインフラストラクチャー・ベンダーは存在しても、それらをスイッチやサーバー、アプリケーションなどに機能としてバンドルするようになるまでには、セキュリティー・ソリューションの成熟と大幅なコモディティー化を待たなければなりません。それらのベンダーには概して、最新のテクノロジーを提供したり、セキュリティーやコンプライアンスの戦略に関する専門的ガイダンスを提供したりするほどの的を絞った専門知識ガ不足しています。

今までのところ、いずれのカテゴリーからも、ITセキュリティー・リスクのライフサイクル全体を通じ、コストおよび複雑さをトータル的に削減する責任を負うベンダーは出ていません。大部分が、お客様の責任に委ねられています。今こそ、より多くのことを期待し、求めてもよい時期です。

ハイライト

未来企業のためのセキュリティー変化に対応

お客様の課題は、IBM Global CEO Study『未来企業におけるIT部門のあるべき姿: The Enterprise of the Future』にまとめられています。この資料によると、CIOは「CEOに並ぶ重要な役割として企業全体に目を配りつつ、自身のIT担当機関の中でも『変化のリーダー』として変革を促進し、『変化の作用因子』として変革を実践」していく責任を負うことになります。

未来企業作りに対応し、それをサポートするために、CIOであるお客様は、変化に付き物のあつれきを緩和するお手伝いをしていく必要があります。変化は実際に成長や機会を推進する力となる場合もありますが、変化がリスクに影響を及ぼし、セキュリティーやコンプライアンスがお客様にとって最も悩ましい責務となる場合もあります。

ビジネスのコストや複雑さを削減するには、変化に際し、リスクおよびコンプライアンスの管理をより持続的なものとし、一貫してビジネス主導の方向性を保つことが必要です。従って、ITの規律として、セキュリティーを、お客様ができないことを定義する阻害的技術から、お客様のビジネスの目的のために必要なものを実行するための力を与えてくれる実現技術へと変革する必要があります。

未来の企業では、セキュリティーおよびコンプライアンスを、阻害的技術から実現技術へと変革することが求められます。

これは、非常に大きな仕事です。企業の中の変化の作用因子としてお客様ができることは多くありますが、セキュリティーやコンプライアンスの真の変革のためには、さまざまな種類のセキュリティー・プロバイダーが必要となります。

変革の力があるセキュリティー・プロバイダーの出現

未来の企業は、セキュリティー業界における変化を促す役割を想定した規模やコミットメントを提供してくれるベンダーを求めています。従来の各種セキュリティー・ベンダーとは異なり、変革の力のあるプロバイダーは、セキュリティー技術をITのメインストリームへ導き、リスクのライフサイクル全体に対して説明責任を負うために必要な特性を有するものとなります。

- *ITインフラストラクチャーのあらゆる側面に関する専門知識*
- *セキュリティーの研究開発におけるリーダーシップ*
- *セキュリティーの製品およびサービスの奥深さと幅広さ*
- *幅広い統合の専門知識とビジネス・コンサルテーション*
- *テクノロジーとビジネス・プロセスの整合における専門知識*
- *グローバルな展開*
- *財政面での強さと持久力*

ハイライト

変化の力のあるプロバイダーは、これらの特性を活用し、以下の3つの主要課題に対応していかなければなりません。

1. 絶え間ない変化に対応するためにリスク管理を再定義し、簡素化する

本資料で先に詳しく述べたように、リスクの心構えにおける絶え間ない変化により、固定的な予算に対して重み付けする必要があるセキュリティーやコンプライアンスのニーズのリストが増大しています。CIOは自身の脅威に対する心構えについてより明確かつ包括的な見解を持つよう求められているため、セキュリティーの意思決定におけるガイダンスが不足しています。 結果的に、見せかけの経済に基づいた優先順位や、実際のビジネスの目的から切り離された優先順位を確立してしまう場合が多くなっています。問題の一部は、単純に、変化の5つの主な要因がリスクに影響を及ぼす様々な経過についての情報不足にあります。 従来のベンダーは、複数の変化のベクトルに対する意見を提供することはほとんどありません。

セキュリティー・ニーズを評価し、優先事項に対して支出するための完全なビジネス中心の枠組みをお客様に提供するために、変革の力のあるセキュリティー・プロバイダーは企業のリスク管理を、非常に洗練され、かつダイナミックな形式で再導入することになります。これにより、あらゆる主要な変化の要因が考慮されるとともに、ベンチマーキングのプロセス、成熟度モデル、業界のベスト・プラクティスおよびその他の要素に盛り込まれ、リスクを実際のビジネス目標へ影響を及ぼすものとして評価する、完全でより正確な企業のリスク・プロファイルが生まれます。

変革の力のあるセキュリティー・プロバイダーは、より幅広く、ビジネス主導の一連のソリューションを提供するとともに、市場でのリーダーシップや説明責任も兼ね備えていなければなりません。

これは、セキュリティーおよびコンプライアンスの計画および管理から圧力や当て推量をほとんど排除する、継続的かつ順応的なリスク管理のアプローチです。より賢明なビジネス主導の意思決定を行うことにより、お客様はセキュリティー関連のコストや複雑さを、現在だけでなく長期的によりうまく管理できるようになります。

2. シームレスでビジネス中心のソリューションを実現するセキュリティーの枠組みとポートフォリオを提供する

従来、セキュリティー技術は、狭い目的に特化して、別個に開発され、大きなITインフラストラクチャーの中の、狭く定義されたサイロの中で適用、管理されてきました。未来の企業へと向かう道筋の中では、このアプローチは持続可能なものではありません。主なリスクの課題（支払カード業界のデータ・セキュリティー標準など）により、企業のインフラストラクチャーの大部分、および不可欠なビジネス・プロセスに統合すべき複数のセキュリティー領域における技術が必要となります。包括的なソリューションを多数のソースによる技術とつなぎあわさなければならない場合、コストおよび複雑さを抑えることはできません。

変革の力があるセキュリティー・パートナーは、シームレスかつ効果的な、優れたセキュリティーおよびコンプライアンスのソリューションを提供しなければなりません。まず、以下のような5つの主要なセキュリティー領域を網羅する有効なセキュリティー製品の幅広いポートフォリオが必要です。

1. 人とID
2. データと情報
3. アプリケーションとプロセス
4. ネットワーク、サーバーおよびエンドポイント
5. 物理的インフラストラクチャー

次に、変革の力のあるパートナーは、ソリューションをお客様独自のビジネス要件に合わせることができなければなりません。これには、ビジネスやアプリケーションの詳しい知識と、優れた技術ソリューションをお客様独自のインフラストラクチャー環境およびビジネス・プロセスにしっかりと統合するためのリソースが必要です。

最後に、このようなパートナーは、お客様がセキュリティーおよびコンプライアンスについて常に先を見据えていられるようにし、変化の力がリスクに対処するための力を凌ぐことがないようにするために、セキュリティーの研究開発の最先端にいなければなりません。

図4は、このような総合的なセキュリティーのエコシステムを簡単に図示したものです。

図4: 総合的なセキュリティーの枠組み

3. セキュリティー・リスクにおけるライフサイクルの圧縮と簡素化

セキュリティーは製品でしょうか、それとも特徴でしょうか。リスクのライフサイクル全体に渡るということで、その答えは「両方」ということになります。図5に示すように、あらゆる具体的なリスクに対するソリューションは通常、別個の独立したセキュリティー製品として立ち上げられます。これは、コストが高く複雑なものである場合があります。ほとんどの場合、ソリューションは変遷し、次第に標準化されて最終的にはITインフラストラクチャーに統合される特徴となります。ITインフラストラクチャーに組み込まれる特徴として、セキュリティーは安価なものとなるほか、成熟度が上がり、機能の自動化も進むようになります。

変革の力があるプロバイダーは、この製品から特徴までのライフサイクルを圧縮して簡素化し、変化の力によってお客様のリスクの心構えが常に変化する状況においても、セキュリティーのコストと複雑さをよりうまく管理できるようにしてくれます。

このようなプロバイダーはまず、ライフサイクルの「変遷」段階における役割を果たします。それはつまり、セキュリティー・ソリューションを効果的なテクニック、ミドルウェア、パートナーシップおよびコンサルティングの能力を使ってより迅速に「特徴」の段階に進めることです。

ハイライト

将来的には、より多くのセキュリティーおよびコンプライアンスのソリューションを、当初から既存のインフラストラクチャーやビジネス・プロセスへのシームレスな統合を意図して設計するようにしなければなりません。

次に、これは長期的に見てより重要なことですが、変革の力のあるパートナーは設計によりさらに圧縮されたライフサイクルを提供していきます。セキュリティーおよびインフラストラクチャーの両方の技術に関する製品の開発、統合および管理の能力を擁し、優れたパートナー両端からプロセスを加速させていきます。この時の方法としては、インフラストラクチャー・システムの中のセキュリティーの特徴およびセキュリティーを実現する枠組みを常に追加し続けること。そして、可能な限り設計時にセキュリティー・ソリューションを組み込むこと、あるいは既存のITインフラストラクチャーおよび管理システムにセキュリティー技術を簡単に統合できるソリューション・アーキテクチャーを実現することが挙げられます。

最後に、変革の力があるセキュリティー・パートナーは、セキュリティーの変革の破壊的影響からお客様の組織を守り、管理されたサービスとして多くのセキュリティーおよびコンプライアンスのソリューションを提供することにより、より大きな戦略的柔軟性を提供します。

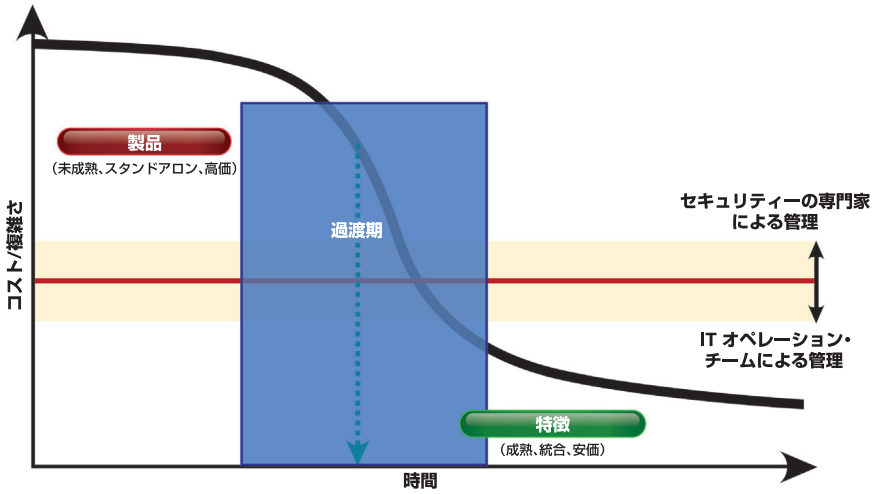

図5: リスクのライフサイクルを巡るコストと複雑さの縮減 ほとんどの企業では、製品、過渡期、および特徴というライフサイクルのあらゆる段階にあるセキュリティー・ソリューションが見られます。

結論

将来的なセキュリティーおよびコンプライアンスは、未来企業に対応するものでなくてはなりません。つまり、一般的にセキュリティーの複雑さとコストを増大させる原因となる、破壊的イノベーション、グローバリゼーションおよびその他の変化の力を網羅するものということになります。求められている変革とは、異色の新技術を、メインストリームのITアーキテクチャーの一部として簡単に管理できる、安定していて安価なセキュリティーの特徴へと移行させるのを促すようなものです。

ハイライト

ポイントは、変化を続けるリスク環境に起因するセキュリティーおよびコンプライアンス管理の痛みや不確定要素の大部分を排除することです。

その道筋は明確かつ説得力のあるものです。つまり、セキュリティーおよびコンプライアンスを既存のITインフラストラクチャーに移し、標準的な管理プラットフォームおよびビジネス・プロセスに統合することです。最も重要なのは、トータル的なリスクのライフサイクルという観点から将来的なリスクのイノベーションを追求することです。このアプローチは、ビジネスのコストや複雑さの絶え間ない変化による影響を緩和し、ビジネスの継続性を改善するために不可欠なものです。

これは、お客様の力だけでは対処できない仕事です。つまり、お客様の組織には、リスクの心構えを評価し、セキュリティー・ソリューションの統合と常に変化するリスク/複雑さ/コストのバランスのあらゆる側面を維持するために必要な専門の人材を維持する余裕がありません。さらに、取引のある古いベンダーには優れたソリューションを提供するだけのリソースがありません。

IBM: 変革の力があるセキュリティー・パートナー

IBMは、グローバルに展開し、市場の変革の力があるセキュリティー・パートナーとなるべき幅広い能力とビジョンを兼ね備えた組織です。

この動的な環境を確保することは非常に大きな仕事であり、そのためには幅広く、コミットメントの確かなベンダーが必要です。IBMには、変革の力があるセキュリティー・プロバイダーの役割を担うためのリソース、専門知識およびビジョンがあります。IBMが未来の企業を実現するパートナーとして、そしてプロバイダーとして、お客様がその確保を行うお手伝いをさせていただくことは合理的な選択肢となりますので、IBMの特徴をご検討ください。それは、先に述べた、変革の力のあるセキュリティー・パートナーとして不可欠な要素としての以下のような要件を満たすものです。

- *ITインフラストラクチャーにおける包括的な専門知識*
- *セキュリティーの研究開発におけるリーダーシップ*
- *セキュリティーの製品およびサービスの奥深さと幅広さ*
- *幅広い統合の専門知識とビジネス・コンサルテーション*
- *テクノロジーとビジネス・プロセスの整合における専門知識*
- *グローバルな展開*
- *財政面での強さと持久力*

IBMは、リスク管理の再定義と簡素化を行います。

市場の調査および分析、技術開発およびビジネス主導のソリューション統合における現場での専門知識により、IBMは、ビジネス環境におけるリスクの展開に対して深みのある見解を提供します。これにより私たちは、お客様が直面するリスクのより明確で優れた評価を提供するとともに、より効果的なセキュリティーおよびコンプライアンスの戦略を提供します。たとえば、IBM Client Security Readiness Methodology では、お客様がリスク、複雑さおよびコストのバランスを取るためのビジネス主導の理論的基盤を確立するお手伝いをしていきます。

IBMは、トータル的なセキュリティーの枠組みとソリューションのポートフォリオを提供します。

IBMは、幅広く深いソリューションのポートフォリオを提供します。その範囲は、5つの主要なセキュリティー領域に渡り、シンプルなポイントとなるソリューションから包括的な管理されたサービスまで、あらゆる物が網羅されています。最も重要なのは、ソリューションおよび納入する代替物の幅広い組み合わせにより、最大限の制御が実現するため、お客様の戦略を独自の要件に合わせてカスタマイズできるという点です。

IBMは、セキュリティー・リスクのライフサイクルを圧縮し、簡素化します。

IBMのセキュリティーおよびコンプライアンスの製品ロードマップは、ますます、未来の企業のビジョン、つまり、ITセキュリティーが全体として絶え間ない変化に対応し、それを実現させるという方向性を取るようになっています。製品の研究開発、戦略的買収、およびチャネルや技術パートナーの開発において、私たちはセキュリティーやコンプライアンスのソリューションをより統合されたものとし、かつ、ITのインフラストラクチャーやビジネスの実践における有効な部分とするよう、努めています。

未来の企業とは、絶え間ない変化に特徴付けられる素晴らしい目的地です。そこでは、特にセキュリティーとコンプライアンスの分野において、刺激的なプロの挑戦が約束されています。それには多くの段階を経なければなりませんが、自信を持って先に進んでいただけると思います。なぜなら、IBMがお客様の味方だからです。

詳細情報

セキュリティー/コンプライアンスをITインフラストラクチャーおよびビジネスの実践に統合し、それらにおける有効な一部分とすることによって企業のリスク、コストおよび複雑さの軽減をサポートするIBMのセキュリティー・ソリューションに関する詳細については、日本IBMの営業担当員またはIBMビジネス・パートナーにお問い合わせいただくか、次のWebサイトをご覧ください。**ibm.com**/services/jp/cio

日本アイ・ビー・エム株式会社
〒106-8711
東京都港区六本木 3-2-12

Produced in Japan
October 2008

[1] IBM Global CEO Study『未来企業におけるIT部門のあるべき姿:The Enterprise of the Future』**ibm.com**/services/jp/cio/pdf/cio_implications_whitepaper.pdf

[2] X-Force Trend Report - **ibm.com**/services/us/iss/xforce/midyearreport/

CIW03050-JPJA-00