IBM Global Technology Services
Thought Leadership White Paper

2012 年 4 月

情報技術リスク管理をサポート

組織全体での取り組みが必要

目次

はじめに

情報技術 (IT) が企業運営の中核を担うまでに進化を遂げた今、IT リスクがビジネスに与える影響は増大する一方です。今や IT に何らかの事象が発生すると、ビジネス機能全体に影響が及ぶことになります。今日、システム障害やインフラストラクチャー障害のほか、データの損失や破損、データ・アクセス不能といった事態は、組織の生産性に重大な影響を与えかねません。このホワイト・ペーパーは、IT リスクがビジネス機能全体に及ぼす広範な影響を組織により深く理解してもらうことを目的としています。このホワイト・ペーパーでは、考慮すべきさまざまなリスクのタイプ、そしてこうしたリスクを効率的に管理するには、なぜ「リスク軽減」と「特定のビジネス・プロセスが創出する価値」とのバランスを取ることが必要になるのかについて説明しています。

課題への取り組み

かつてないほど多くの課題を抱え、組織ではビジネスに対する IT リスクの管理にさらに力を注ぐ必要が生じています。それにもかかわらず、IT プロフェッショナルを対象とした 2010 年の調査では、IT リスク軽減に対する組織全体の取り組みについて、回答者の 34% が「平均的」または「不足」と評価していました。[1]

ISACA (情報システムコントロール協会: IT や情報システムの専門家のための国際的な非営利団体) は、IT リスクを「企業内での IT の使用、所有、運用、関与、影響、採用に関連するビジネス・リスク」と定義しています。[2]

ほとんどの組織では、ほんの一握りのビジネス・プロセスが大半の事業収入や企業評価に貢献しています。IT リスクを完全になくすということは現実的ではありませんが、特定のプロセスがビジネスにもたらす価値に基づいて、リスク軽減の選択肢をバランス良く配分することは道理にかなっているといえるでしょう。

ビジネス・プロセスとテクノロジーは相互に依存しており、包括的なリスク管理ソリューションを構成する非常に重要な要素であることを、企業の上級幹部や経営陣は認識する必要があります。このことを理解していれば、IT リスク・マネージャーやビジネス・プロセスのリーダー、その他のリスク利害関係者との作業もしやすくなり、IT リスクに対処するテクノロジーを効果的かつコスト効率の高い方法で計画、実装、管理できるようになります。この基本的なことを理解していない組織では、次のような結果に陥る可能性が高くなります。

- **重大なリスクを見落とす。**経営幹部は、業務リスクの監視を事業部門 (LOB) のリスクに最も密接に関連するマネージャーに委任することもできます。しかし最終的に、企業全体で確実にリスクを特定、軽減、最適化する責任を負うのは経営幹部です。
- **受任義務を適切に果たせない。**経営責任者には、自社の中核となるビジネスを維持し、保護することが求められます。
- **ビジネス・プロセスの脆弱 (ぜいじゃく) 性を放置する。**放置することで損失につながりかねない業務リスクからビジネス・プロセスを保護することで、信頼性の高い業務運営を実現できます。
- **収益が低下する。**壊滅的ではない「運用」停止でも、累積すれば組織のビジネスに大規模な経済的影響を与える可能性があります。
- **悪い評判を生む。**問題が発生した場合、メディア露出により、組織のブランドと事業上の信用に後々まで影響が及ぶ可能性があります。

リスクのタイプ

IT リスクには、ありふれたものから想定外のものまで、発生の確率も影響の度合いもさまざまな脅威が伴います。これらの脅威は、データ起因リスク、ビジネス起因リスク、イベント起因リスクの 3 つに分類できます。

データ起因リスク: データ起因リスクは多くの場合、ITの観点から最も注目されます。一般に、データ起因リスクは、その他のリスクよりも発生頻度が高くなりますが、発生による損失額は比較的小さいといえます。事業継続性やビジネスの可用性という点ではビジネス起因リスクと重なる部分もありますが、このリスクでは、システムやデータといったレベルにフォーカスしています。

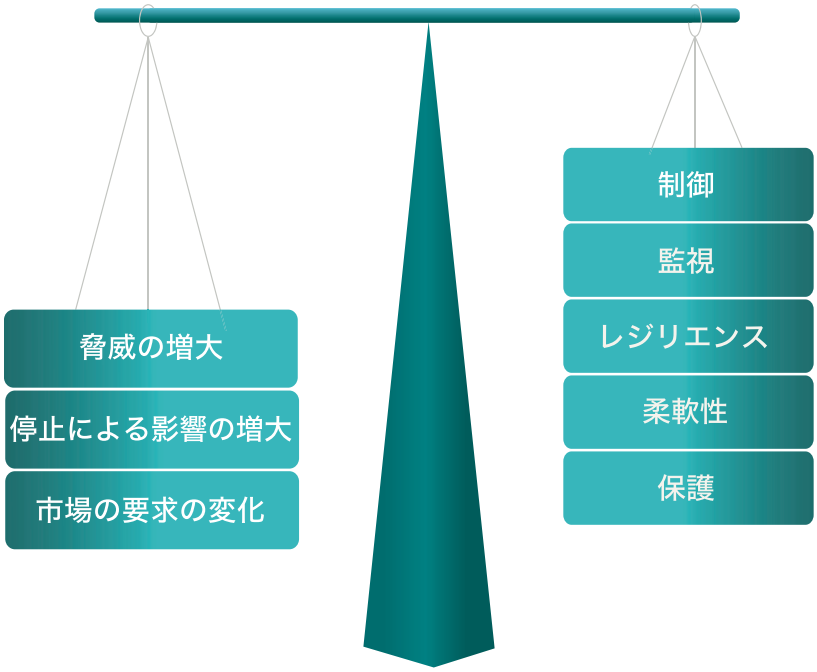

図 1: ビジネス・プロセスのもたらす価値とリスク軽減とのバランスを取る

ビジネス起因リスク: ビジネス起因リスクは、事業継続性と企業運営に直接影響を及ぼします。ビジネス起因リスクは一般的に、データ起因リスクと比べて戦略的な性質があり、ビジネス全体に悪影響を及ぼすため、組織の取締役は通常ビジネス起因リスクに最も関心があります。

イベント起因リスク: 組織の労働力、プロセス、アプリケーション、データ、インフラストラクチャーを混乱させるイベントはすべて、イベント起因リスクに分類されます。イベント起因リスクは、事業の継続性と実現性に影響を及ぼします。

効果的な IT リスク管理ソリューションの開発

自社の収益を伸ばし損益の改善を図るために、既存のテクノロジーを活用してより適切なコンプライアンスの結果を出そうと企業が注力するにつれ、IT リスク管理の重要性は高まります。

IT リスクを効果的に管理するには、次のことが必要です。

- IT サービスの中断や停止が、重要なビジネス・サービスにとってどの程度の脅威や影響となり得るかを評価する
- ビジネスに対する IT リスクを効果的に特定し、評価する
- IT リスクの適切な管理に必要な戦略を定義する
- 継続的な IT リスク管理とガバナンス・プログラムを定義し、実装する
- IT リスクを常に監視し適切なアクションをタイムリーに取ることで、ビジネス・サービスに対するリスクを軽減する

IT リスク軽減を達成するには、プログラムを「管理とガバナンス」、「影響評価」、「計画と設計」、「実装とテスト」、「監視」という 5 段階で構成します。

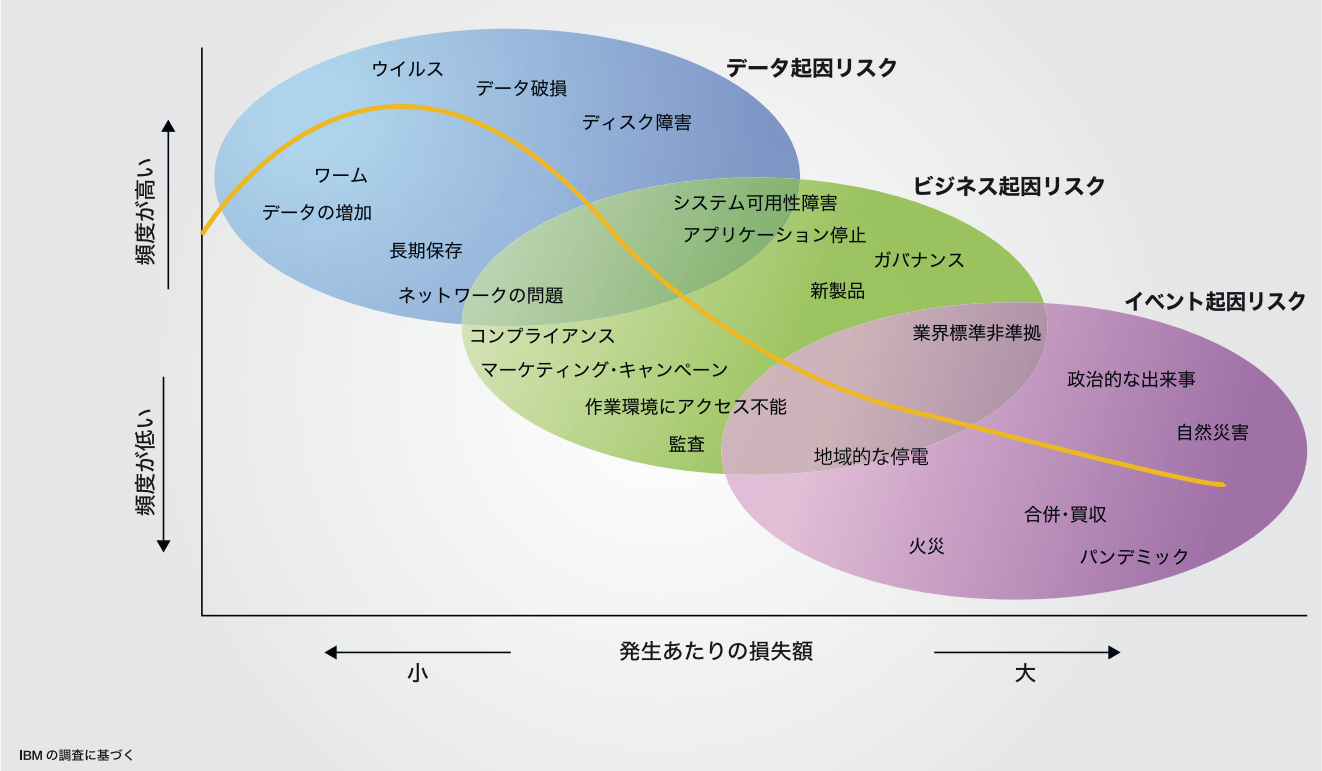

図 2: リスクをタイプ別に示したグラフ

管理とガバナンス: ビジネス状況、IT 機能、IT コストはいずれも、時間とともに変化します。IT リスクの管理とガバナンスは、IT リスクへの適切な取り組みを長期にわたって維持するプロセスです。主な要素には、次のものがあります。

- 役割と責任を明確にしたポリシーを作成し、社内のリスク管理プログラムと関連させて「リスク」の背景を確立する
- IT リスクについて重要リスク管理指標 (KRI) を定義する (測定・監視が可能な指標とし、企業のリスク・プロファイルの変化を早期に警告できるようにする)
- IT リスク管理に関する考慮事項を社内の業務プロセスに組み込む
- IT リスク・プロファイルについて評価、報告、通知を行う
- IT リスクを再評価し、軽減戦略を適宜更新する

影響評価: 影響評価の最初のステップでは、組織が直面する可能性のある IT リスクの0タイプを明確に特定して評価し、リスク・イベントに対してどの程度迅速に対応できるかを正確に把握します。影響評価は、継続的なプロセスであり、次のものがあります。

- 組織に価値をもたらす主要なビジネス・サービスを定義し、それらのサービスの価値を定量化する
- ビジネス・サービスを、サービス提供に必要とされるビジネス・コンポーネントに分解する
- 特定のビジネス・コンポーネントが機能しない場合にサービスが受けるビジネス上の影響を明確にする
- 脅威発生の可能性や発生した場合の影響を評価し、ビジネス・コンポーネントに対する最も重大な脅威と関連リスクを定義する
- ビジネス・コンポーネントに対する影響に基づいてビジネス・サービスの影響を特定する
- 定義済みのリスクを軽減するために、組織の「リスク選好度 (risk appetite)」を理解した上で、コスト効率の高い適切な戦略を確立し、実装する
- 外部リスク依存関係を特定し、セキュリティー侵害発生時に組織とシステムがどのように対応するかを決定する

計画と設計: 計画と設計の段階では、IT リスク管理に必要な軽減戦略を策定します。この段階では、次を実行します。

- 事業継続性、災害復旧、危機管理に関する計画を戦略的に定義し、停止発生時に重要なオペレーションをいかに維持するかを特定する
- 組織の IT 環境として、ビジネス要件ベースのアーキテクチャーを設計する
- IT リスク管理に対する投資とビジネス価値とのバランスを最適化する

実装とテスト: 実装とテストの段階では、計画の有効性を検証し、弱点を特定します。主な要素は次のとおりです。

- テスト計画を作成し、テストを実行し、「あるべき姿」と「現状」のギャップを特定し、修正案を提案する
- IT とビジネス・ニーズを統合する
- IT リスク・ソリューションが最新かつ実行可能なものであることを確認する

監視: KRI を継続的に監視することで、リスク・レベルの変化を特定できるようになるため、リスクが顕在化して主要なビジネス・サービスに影響を及ぼす前にアクションを取ることが可能になります。IT リスク監視をうまく機能させるには、次の要素が必要です。

- IT サービス・コンポーネントを、サポート対象のビジネス・サービスにマッピングする
- 異常の可能性を示す KRI しきい値を定義する
- 適切なエージェント (ユーザーとテクノロジーの両方) にアラートを送信するメカニズムを実装し、予防措置や修正作業を実行できるようにする

IBM の提供するサービス

IBM のセキュリティー・サービスとレジリエンス・コンサルティング・サービスを利用すると、現行のIT リスク管理アプローチに存在する改善すべきギャップと領域を特定できます。IBM のレジリエンシーおよびセキュリティーの専門家は、国際標準化機構 (ISO) などの業界標準を活用して環境を深く理解し、セキュリティーとレジリエンスのフレームワークの定義を支援し、評価で使用する個々の付随事実のレビューを行い、修正や継続的な改善に必要なロードマップの提供を支援します。

IT リスク・ソリューションの再評価

リスクと脅威は絶え間なく変化しています。そのため、定期的にリスクを見直し、ポリシーと管理の妥当性と有効性を再検討する必要があります。対処すべき課題には、次のものがあります。

- **企業運営上、IT 関連のビジネス・リスクと企業全体のリスク管理をどのように調整するか**
- **リスク管理上のコストとメリットのバランスを取る場合、どのような課題に直面するか**
- **日常的に継続して行う重要なプロセスであると理解し、組織的に取り組んでいるという事実をどのように実証するか**
- **障害やセキュリティー違反が発生した場合、ビジネスを最大のリスクにさらすビジネス機能やビジネス・プロセスはどれか。そうしたビジネス・プロセスはどの程度IT に依存しているか**
- **IT に起因するビジネス・プロセス中断のリスクと、中断による経済的な影響や信用上の影響を十分に評価し、軽減しているか**

IBM® レジリエンシー・コンサルティング・サービスは、組織固有の IT リスク管理ニーズに合わせて柔軟にソリューションを調整し、提供します。IBM は、ソリューションの評価、計画、設計、作成、実装、テストを支援し、複数のビジネス機能全体にソリューションを統合できるようにします。IBM のベンダー中立的なアプローチでは、業界のベスト・プラクティスと構造化された手法を活用することで、IT とインフラストラクチャーのリスクをより明確にし、ギャップを特定し、IT リスク管理戦略がより包括的でコスト効率の高いものになるよう支援します。

IBM セキュリティー・サービスでは、IBM のセキュリティー手法を活用し、組織で使用されているセキュリティー・メカニズム(ハードウェア/ソフトウェア・システム、ネットワーク、データベース、従業員が使用しているもの) の評価を支援します。IBM は、担当マネージャーや従業員と面談を行うことでビジネス・プロセスを理解し、組織全体のデータとアプリケーションが、現行の運用管理でどの程度効果的に保護され使用されているかを把握します。

IBM をお勧めする理由

業務リスクやビジネスの停止を事前に特定、把握、管理、対応する必要のあるお客様に、IBM は IT リスク管理サービスを提供します。IBM のソリューションは、組織が事業を継続し、自社のブランドをより確実に保護できるように、またサービス提供者として顧客やパートナーからの信頼を維持できるように支援します。IBM は、業界や IT のベスト・プラクティスを活用して、組織の IT リスク管理ニーズをより的確に把握し、セキュリティー機能が充実したリスク管理計画の作成を支援することで、組織固有の脆弱性やコンプライアンス要件に対処し、全体的なリスクやコストを軽減できるようにします。企業の IT ソリューション分野におけるグローバル・リーダーとして、IBMはこれからも製品とサービスを開発し、進化し続けるリスク管理ニーズに対応していきます。

詳細情報

IBM のセキュリティー・サービスやレジリエンス・コンサルティング・サービスの詳細についてご確認ください。

IBM セキュリティー・サービスの詳細については、次の Web サイトをご覧ください。
ibm.com/itsecurity

IBM レジリエンシー・コンサルティング・サービスの詳細については、次の Web サイトをご覧ください。**ibm.com**/bcdr2012

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19-21

Produced in Japan
April 2012

[1] IBM CIO Risk Study、2010 年 6 月

[2] ISACA Web サイト (http://www.isaca.org/Pages/Glossary.aspx?tid=4326&char=I)
2011 年 6 月 23 日時点の情報

Please Recycle