

信頼をより確かなものへ

さまざまな皆様とともに社会の発展に貢献していくためにも、信頼をより確かなものにする経営の基盤づくりが欠かせません。全世界にわたるさまざまなリスクの管理と有事における事業継続への対策、そしてIBMのビジネスの根幹にかかわる情報セキュリティーやコンプライアンス（法令遵守）強化に努めています。

リスク・マネジメントと事業継続

リスク・マネジメント

未知のリスクを事業計画に反映する — ERM*

IBMでは、米国本社が主導するエンタープライズ・リスク・マネジメント（ERM）という手法で全世界のIBMの戦略の策定と実行、事業活動におけるリスクを管理しています。日本では、社内の主要機能および製品・サービス事業に責任をもつ役員で構成されるERMステアリング・コミッティ（Steering Committee）において、日本IBMの事業リスクの特定、影響度分析を行い、リスクの優先順位を決め、担当責任者を決定します。これらのリスク項目を危機管理体制や各事業部に助言し、リスクの最小化の検討、実施をします。例えば、情報セキュリティーに関するリスク、自然災害に対するリスク、社内の資産の活用に関するリスクなどが2010年に挙げられたリスクの一部です。

ERMを通じて、経営層が日本だけでなく世界中のIBMのリスクについて同じ認識を持つと同時に、継続

的な成長を確保するために、全社でリスクを管理し、悪い影響が起こる前に最善の策を決定し、事業計画に反映することを実現しようとしています。

*ERM（Enterprise Risk Management）戦略的意思決定や業務遂行上の意思決定を増強する組織的かつ統合的なリスク・マネジメントのアプローチのこと

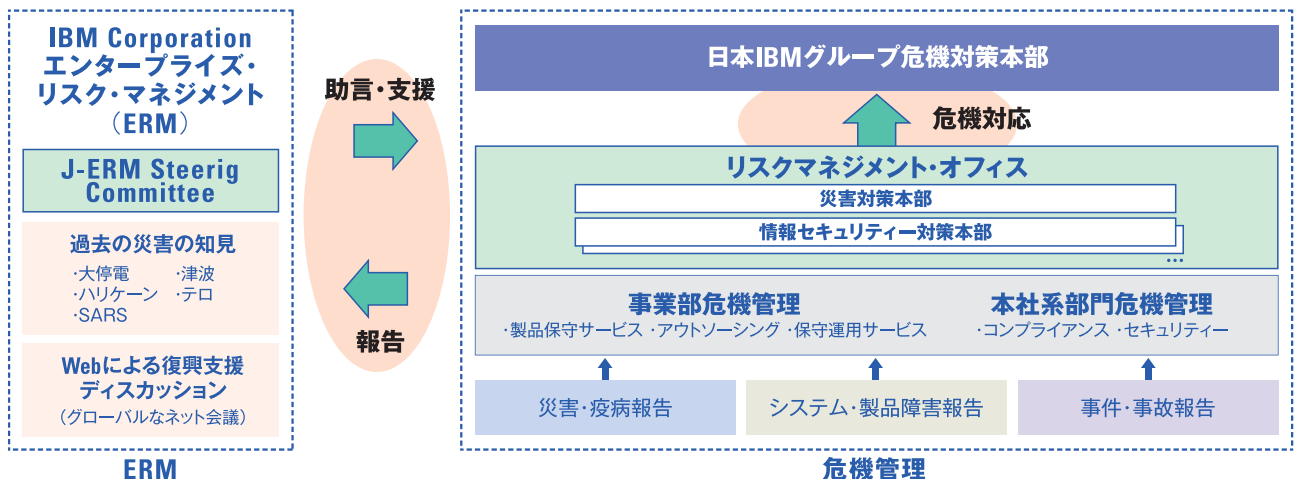
悪い影響を最小限にとどめる — 危機管理

日本IBMでは、2006年より危機管理体制として設置された日本IBMグループ危機対策本部のもと、既知のリスクに対応する「全社災害対策本部」「情報セキュリティー対策本部」「組織別緊急対応体制」が設置されています。日常的なトラブルや問題に対しては、それぞれのチームが対応しますが、ハイ・リスク事案や全社での判断が求められる事案については、危機対策本部で会社としての対応の検討を行います。これらの事案を通じて、不確定な要素はERMステアリング・コミッティに報告し、リスクの特定へと連携します。

取り組み 社員安否確認システム

危機管理の一環として、2007年の新潟県中越沖地震の経験に基づき、2008年より社員安否確認シス

図1：リスクマネジメント/危機管理体制



テムを日本IBMグループ内に導入しました。このシステムは、携帯電話と社内システムのLotus Notesを連携させたもので、グループ内の社員を対象とし、年に数回の訓練を実施しています。このシステムは、地震などの災害時を想定したメニューと新型インフルエンザのような疫病を想定したメニューがあります。2010年には、新型インフルエンザの流行を想定した訓練が行われました。

安否確認システムは、全社員を対象に実施しています。中でも技術部門においては、技術員の安否確認状況をもとに、いち早く被災地への技術員の派遣指示にもつなげています。

事業継続

IBMは、世界各国で天災、テロ、感染症などの非常事態を経験する中で、自社やお客様、そして社会の被災に対し常に適切に対応してきました。設備、テクノロジー、アプリケーションとデータなど、ITやITインフラにかかる領域だけでなく、ビジョンと戦略、組織、プロセスといったビジネスや企業を構成する層に対して不慮の事態を想定して対策を検討しています。図2にあるような企業における6つの層に対して、IBMでは、①脅威の想定 ②ビジネス影響分析 ③想定脅威に対する課題分析 ④対策概要検討 ⑤対策実施計画 ⑥対策実施 ⑦対策管理 ⑧対策管理の評価 という8つのプロセスで、事業継続計画(BCP)の管理をしています。

2006年より着手した新型インフルエンザへの対応では、この脅威が広範囲かつ長期間にわたり影響を

及ぼすことから、全IBMで対策に取り組みました。特に、BCPについては、世界中のIBMで対策を検討し、立案しました。

現在でも、当時のBCPをベースに脅威の想定を随時見直し、対策を強化しています。継続してBCPを見直すことで、その間に変更されたプロセスやルール、組織、アプリケーション、テクノロジー、ITインフラ、設備に対応した計画を維持しています。

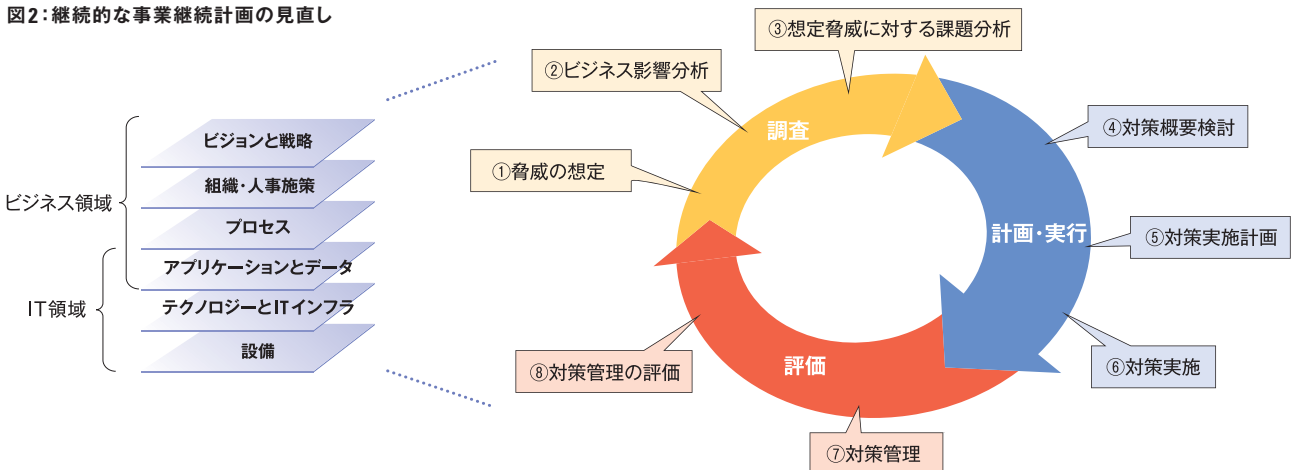
インテグリティの取り組み

日本IBMグループは、インテグリティを実践し、定着させるための取り組みを、社長、部門長、管理者、社員が一丸となって推進しています。インテグリティとは、「誠実な行動・ビジネス」を意味する言葉です。法令遵守はもとより、広く企業倫理の向上を図るための施策を継続的に行い、お客様や社会からの信頼を確かなものとしていくよう努めています。

IBM企業行動基準

社員一人ひとりが遵守すべき行動規準を「ビジネス・コンダクト・ガイドライン(BCG)」という形でまとめ、全社員がこれに従って行動するよう求めています。BCGは社員がIBMのビジネスを行うにあたって、個人としてすべきこと、してはいけないことの判断基準を示すものです。BCGは毎年更新され、日本IBMグループに所属するすべての社員は、入社時に、また入社後は毎年一度、BCGを熟読した上で同意の署名を行います。

図2: 継続的な事業継続計画の見直し



BCG違反者に対しては解雇を含む厳正な処分がなされます。

BCGはIBMのWebサイトで公開されています。

URL
● <http://www.ibm.com/jp/ibm/bcg/>

ビジネス・インテグリティ研修

社員一人ひとりが「インテグリティなくしてビジネスなし」という強い決意を持って業務を遂行していくために、日本IBMグループに所属する全社員を対象に、毎年、ビジネス・インテグリティ研修を実施しています。この研修はイントラネットにより実施され、研修の都度、社員一人ひとりの理解度が確認されます。

またすべてのライン管理者を対象にした集合研修も行っています。これは過去の具体的事例に基づき、管理者として取るべき行動を自ら考えたとともに、グループ討議を通じて適切な判断や部下への指示を行えるようにするためのより実践的な研修です。

さらに、このような活動により、社員と組織の中にビジネス・インテグリティを重視する意識、風土が定着していることを確認するため、全世界で、毎年2回、定期的に社員に対する意識調査を実施し、その結果に基づいたアクションを取っています。

日々のビジネス遂行のための インテグリティ三原則

- 常に、事実、数字などの情報を、**正確に記録し報告**をすること
- どんなに急いでいても、自らの権限を超えて独断に走ったりせずに、判断に困ったときは、**所属長や関連の責任部門に、まずは相談**すること
- 過去の事例をもとに、自分が似たような状況に遭遇した際には、どのような危険が待ち受けているかを予測しながら、**常に慎重に行動**をすること

情報セキュリティ

日本IBMグループは、情報セキュリティがビジネスの根幹にかかわるものであること、また我が国では2005年4月の個人情報保護法施行以降、個人情報の取り扱いに対する国民の意識が高いことを十分認

識し、日頃から情報セキュリティの対策を推進する取り組みを実践しています。

情報セキュリティ・マネジメント体制

日本IBMグループは、IBMコーポレーションの規定および日本IBMの規定に基づき、日本IBMグループ全体で取り組むべきセキュリティ施策を体系化し、チーフ・インフォメーション・セキュリティ・オフィサー(CISO)と情報セキュリティ委員会を中心とする体制を確立して、情報セキュリティ・マネジメント・システム(ISMS)を実践しています。

また、昨年に引き続き全社方針である「重大事故ゼロ」をはじめとして、重要な情報資産を守るために必要なセキュリティ目標を設定し、日本IBMグループ全体でそれらの達成度を可視化して実践しています。

日本IBMグループのISMS統一認証

日本IBMおよび日本IBMグループ会社16社は、全従業員が参加するISMS統一認証を取得しており、同じ方針・ルール・仕組みに基づいてISMSの構築・運用を行っています。日本IBMグループ全体のセキュリティ・レベルの維持および向上に努め、お客様に提供する価値を進化・深化させてこれまで以上に信頼されるパートナーとなることを目指します。



ITを活用した情報セキュリティの推進

取り組み1 スマートデバイス(スマートフォン)による社内IT利用

日本IBMでは、社員向けにスマートデバイス(スマートフォン)を活用した社内ITリソースへのアクセスサービスを提供しています。

スマートデバイスとIBM社内ネットワークをインターネット回線の仮想プライベート・ネットワークを介して接続し、社内のメール、カレンダー、電話帳などを利用します。データはブラウザ経由で閲覧するのでスマートデバイスには保存されず、セキュアな



利用が可能です。

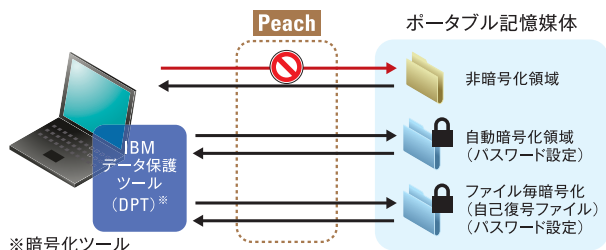
その他、USBメモリーキー一つで任意のPC上でセキュアな環境で社内業務を遂行できる仕組みなど、セキュリティに配慮し、新しいテクノロジーを取り入れたより柔軟性の高い作業環境を提供し、社員の業務の生産性向上を図っています。

取り組み2 全従業員の業務用PCのセキュリティ強化

情報セキュリティ・マネジメントを確実に、しかも効率的に実施するために、ITインフラの重要性がますます高まっています。世界中のIBMの従業員全員のクライアントPCには、遵守すべきセキュリティ要件を満たしているかどうかを自動的に点検するツール(Workstation Security Tool)を導入しています。このツールはIBMが開発したものであり、これによって、万が一従業員がPCを紛失しても、保管している情報が外部に流出したり等の事態が発生しないよう、日常的に点検と管理がされています。また、業務で使用するすべてのPCには、HDD全体を暗号化するツールを導入し、情報資産保護に努めています。

取り組み3 ポータブル記憶媒体のセキュリティ対策の強化

近年USBメモリーや外付けHDDなどのポータブル記憶媒体に関連した事件・事故が見られます。日本IBMグループでは、ポータブル記憶媒体への情報の書き出し時に自動的に暗号化するツールを開発し、業務用PCに導入しています。



健全なインターネットの発展のために

日本IBMでは、大変残念なことに、2008年にお客様にご迷惑をおかけした個人情報漏えい事件が発生しました。しかし一方で、その対応に全社を挙げて徹底的に取り組むことで情報の流出を最小限に抑え、また関係諸機関やセキュリティ関連団体と優れた連

携を行ったことにより、当社の情報セキュリティー推進室の社員が経済産業省より表彰を受けました。

平成22年度情報化促進貢献
経済産業省商務情報政策局長表彰「情報セキュリティ促進部門」(1件)

表彰の理由は、ファイル共有ソフトによる情報漏えい事件を受けて、事件の対処に関する経験を講演やセミナー等を通して積極的に共有する活動を行い、またセキュリティ・オペレーション・センター(SOC)や関係諸機関の間の連携に大きく貢献しているというものです。その活動を通して、興味本位な情報漏えいや情報の拡散は許さないという社会全体の強い姿勢を示すことにもなりました。

IBMのセキュリティ・オペレーション・センターでは、世界6カ所のセンターと連携して、24時間365日セキュリティに関する監視活動を行っています。今回の表彰では、この活動も評価をされました。

日本IBMではさらに、事件への対応により得られたさまざまなノウハウを、実績に裏打ちされたコンサルテーション、セキュリティ・ソリューションとしてお客様に役立てていただけるように、積極的な活動を行っています。

プライバシー(個人情報の取り扱い)

日本政府は現在、社会保障・税に関わる番号制度および国民ID制度の導入の検討を進めており、その番号制度における個人情報保護の有効な仕組みを検討するワーキング・グループを設置しています。従来の法制度におけるさまざまな問題点を洗い出し、プライバシーに十分配慮した法規制と安全なITシステムとの連携によって実現される、現実的なリスクに応じた柔軟で合理的な個人情報保護制度の確立が期待されます。その過程において、IBMはグローバルでの経験やノウハウを持つ企業として、海外のID管理やデータ保護にかかわる取り組み事例や、新技術やシステム開発においてプライバシーの保護機能を初期段階から織り込むPrivacy by Designの考え方、さらに先進的なセキュリティ技術の利用など、さまざまな個人データをプライバシーに十分配慮した革新的な方法で活用することを提案していきます。