

信頼を確かなものとするために

IBMers Valueを具現化するとともに、ステークホルダーの皆様への責任を果たす基礎として、コンプライアンス・企業倫理を社員一人ひとりへ徹底する取り組みや、さまざまなリスクの予防と発生時の適切な対応およびビジネスの根幹にかかわる情報セキュリティの強化に日ごろから取り組んでいます。

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グループ全体で推進しています。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基準を「ビジネス・コンダクト・ガイドライン」(以下「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。

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のウェブサイトで公開されており、どなたでも参照することができます。

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

● 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、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るe-ラーニングの形で実施され、研修の都度、社員一人ひとりの理解度を確認することとしています。

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るとともに、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実践的な研修です。

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**すること

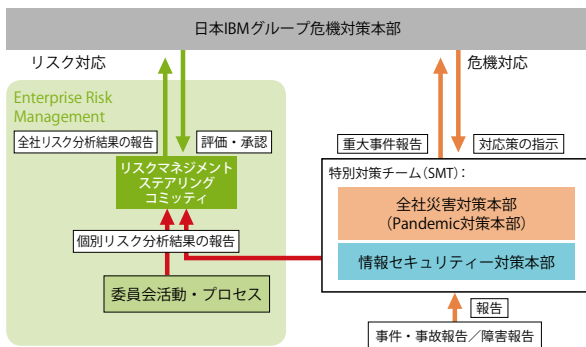
リスクマネジメント

● ERM

IBMは、全世界の事業活動におけるリスクをエンタープライズ・リスク・マネジメント(ERM*)という手法で管理しています。米国本社が主導し、各地域および各事業部が同じリスク分析手法と判断基準を用いて、リスクの特定や優先順位付け、原因分析を行い、IBM全体へのリスクの影響を評価しています。これにより、経営に対する影響を最小限に食いとどめ、継続的な成長を確保するための最善の策を決定することを実現しています。

日本IBMグループでは、図の危機管理体制を設け、リスクマネジメント・ステアリング・コミッティにおいて、ERMの手法を用いて日本におけるリスクの集約と分析を行い、その結果を世界中のIBMと共有しています。

日本IBMグループ危機管理体制



日本のリスク事象の多くは他の地域と共通していますが、地震の多発や大都市に機能が密集している点など、日本特有の条件も留意しています。

* ERM (Enterprise Risk Management) とは、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

● 事業継続

IBMは世界各国で電力不足、暴風雨、洪水、津波、テロ、感染症などの非常事態を経験する中で、自社、お客様、ひいては社会の被災に対し常に適切に対応してきました。

お客様のデータセンターが被害を受けた場合に、お客様業務が継続できるよう、24時間365日の監視サービスや保守サービスを提供しています。また、パブリック・クラウドとして高品質かつ安全性の高いIBMデータセンターでは、お客様のサーバーやPCのデータを自動的にバックアップし、監視するサービスにより、お客様の事業継続を支援しています。

日本IBMは、2008年から2009年まで(社)電子情報技術産業協会 (JEITA) 情報政策委員会新型インフルエンザ・タスクフォースの主査を務め、事業継続に関する政府への提言、業界のガイド作成などをリードしてきました。このJEITAの活動については評価され、特定非営利活動法人事業継続推進機構 (BCAO) より、2009年度BCAO優秀実践賞が授与されています。

社員安否確認システム

日本IBMグループでは2007年の東日本大震災の経験に基づき、2008年より社員安否確認システムを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ています。年に数回の訓練を実施し、訓練の回数を増すごとに回答率が上がってきています。

重大なリスク事象が発生した場合、本システムを活用して短時間で社員や家族の安全を確認し、あわせてお客様へのサービスを継続できるよう平時から備えています。



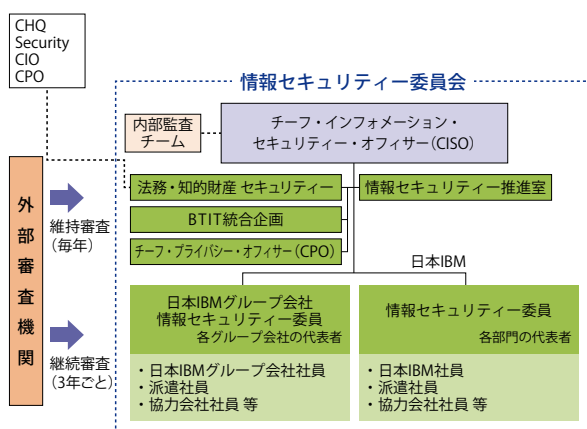
安否確認画面のイメージ

情報セキュリティ

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、また我が国では特に2005年4月個人情報保護法の施行以降、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を強化するための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

米国本社の規定および日本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、全社方針である「ハイリスク・インシデント*1のゼロ」をはじめ、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。

2009年11月、日本IBMおよび日本IBMグループ会社17社は、全従業員が参加するISMS統一認証を取得しました(登録証番号: JQA・IM0258)。グループ全体で共通の方針・ルール・仕組みに基づいてISMSの構築・運用を行い、セキュリティ・レベルの維持および向上に努めていきます。

● ITを活用した情報セキュリティの推進

取り組み①

全従業員のクライアントPCのセキュリティ強化

世界中のIBM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ための、IBMが開発したツール (Workstation Security Tool) を導入しています。仮に万が一従業員がPCを紛失しても、保管している情報が外部に流出する等の事態が発生しないよう、このツールにより日常的に点検と管理がなされています。また、より機密性の高い情報を保管する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②

ポータブル記憶媒体のセキュリティ対策の強化

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・事故の再発を未然に防止するため、ポータブル記憶媒体への情報書き出し時に暗号化を強制するツールを開発し、業務用クライアントPCに導入しています。

取り組み③

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・サービスを開始しました。スマートフォンとIBM社内ネットワークをインターネット回線上のVPN*2を介して接続し、社内のWeb業務アプリケーション、メール、カレンダー、電話帳などが利用できます。データはブラウザ経由で閲覧するのでスマートフォンには保存されず、安全で信頼性の高い利用が可能です。

● ビジネスにおけるセキュリティの徹底

日本IBMのビジネス遂行に当たっては、協力会社(委託先会社)との協業は欠かせません。お客様に信頼いただける価値を提供するためには、情報セキュリティについて、日本IBMの取り組みの

みならず、協力会社にも十分配慮していただくことが必要です。

そのため、日本IBMと協業する協力会社には、下記のような対応を確実に実施していただき、ともにお客様へのセキュリティ確保に努めることとしています。

- セキュリティに関する条項を含む誓約書を交わし、その実施状況について定期的な点検を行う。
- 日本IBMから委託した業務に使用するPCは日本IBMから貸与することとし、協力会社のPCは持ち込み禁止とする。
- 業務から離任する際は、使用したPCや外部記憶媒体の残留情報の徹底削除を義務付ける。

● 健全なインターネットの発展のために

日本IBMは、特にビジネス分野における健全なインターネットの発展のために、次のような社外の協議会の一員として積極的な活動を行っています。

● 安心安全インターネット推進協議会 P2P研究会

Winnyなどに代表される匿名P2Pファイル共有ソフトウェア*3を研究し、ファイルの流通の原理の解明や抑制の技術などを開発しています。開発された技術は実際の情報漏えい事故に適用され、多くの実績を残しています。

● 日本セキュリティオペレーション事業者協議会 (ISOG-J)

セキュリティ事業者間の連携に必要な情報を定義し、また法律問題を取り上げて研究するなど、インターネットに対する攻撃をさまざまな技術を持った企業が連携して防御する仕組みを構築しています。

*1 例えば重大な情報漏えい事故のような、お客様や企業にとって影響度の高い事故のこと

*2 Virtual Private Networkの略。公衆回線をあたかも専用回線であるかのように利用できるサービスのこと

*3 Peer to Peerファイル共有ソフトのこと。インターネットを介して不特定多数のコンピューターの間でファイルを共有するソフトウェアの総称

プライバシー（個人情報の取り扱い）

Smarter Planetの実現に向け、さまざまなデータを革新的な方法で活用することになりますが、その際、プライバシーとセキュリティへの十分な配慮を忘れてはなりません。特にプライバシーの観点からの個人情報の保護については、各国・地域で文化が異なるように、その規制の方法も異なります。この状況で、世界規模のサービスを提供するには、国境を越えたデータの保護に関して、柔軟かつ円滑なルールが必要です。

2010年は日本でAPEC*会議が開催されますが、IBMはその会議に産業界から参加し、政府とともに、有効なルール作りへ積極的に取り組んでいます。

* アジア太平洋経済協力 (Asia-Pacific Economic Cooperation) の略

