

経営の基盤

企業の存立の基盤であり、すべての企業活動の前提となる企業倫理の向上、リスクマネジメント体制の構築と
不断の活動、情報セキュリティの向上に努めています。

インテグリティ

昨今、企業経営環境の厳しさが増す中、コンプライアンスや内部統制の重要性とそれに対する関心はますます高まっています。

インテグリティとは「清廉、誠実」を意味する言葉です。日本IBMグループではインテグリティの取り組みにより、単に法令遵守にとどまらず広く企業倫理の向上をも目指すことで、社会から信頼される企業としての社会的責任を果たしてまいります。

IBM企業行動基準 (ビジネス・コンダクト・ガイドライン)

IBMでは、お客様をはじめ社会のIBMに対する信頼と期待に応えるため、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」(BCG)という形でまとめています。

BCGは社員がIBMのビジネスを行うにあたって、個人として何をなすべきで何をなすべきでないかの基準を示すもので、社員はBCGによって社員としてのあるべき姿を確認することができます。

日本IBMグループに所属するすべての社員は、法令遵守はもちろんのこと、より高い倫理基準であるBCGを遵守するため、毎年更新されるBCGを熟読し、同意を行います。

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。

なお、IBMのBCGはウェブで公開されています。

WEB <http://www.ibm.com/jp/ibm/bcg/>



ビジネス・コンダクト・ガイドライン

コンプライアンス委員会

2003年10月、日本IBMグループの企業価値・企業品質向上を目指し、コンプライアンス委員会が発足しました。

具体的な委員会活動としては、年間の全社インテグリティ推進計画の策定、インテグリティ研修の立案と実施、社内の各種規定を整理した「社内規定解説書」の作成、社内向けコンプライアンス相談窓口の運営、内部統制の充実のための社内プロセス改善提案活動などを行っています。

これらに加え2008年には、日本IBMグループ各社について、法令遵守状況の調査と四半期ごとの点検などを実施しました。

インテグリティ研修

日本IBMグループでは、「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すべく、グループに所属する全社員を対象にインテグリティ研修を実施しています。

研修では、全社員を対象として、イントラネットによるe-ラーニング研修を実施し、その理解度を確認しています。

また2008年には、すべてのライン管理者を対象にした集合研修も行いました。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、グループ討議を行うことで、管理者一人ひとりが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。

2009年も引き続き法令違反や社内規定違反を絶対に許容しない (Zero Tolerance) ということ、社員一人ひとりにしっかりと浸透させ、さらなる啓発の促進・充実を図ってまいります。



e-ラーニングによるインテグリティ研修

社内での問題提起・通報制度

IBMでは、会社に関する懸念事項や社員個人では解決できない問題について、社員が会社に提起・通報し、解決を求めることができる全世界共通のプログラムとして、Concerns and Appealsが設けられています。

Concerns and Appealsには以下の2種類のプログラムがあり、社員は適したプログラムを選択し、問題を提起することができます。

このプログラムを利用する社員に対し、報復ととられるような行為をした場合は、どのような立場にある社員であっても厳しい措置がとられることになっています。

● Open Door (オープン・ドア)

社員が、社員個人に影響を与えるマネジメントの決定やアクションについて問題提起し、調査を求めることができる制度です。業績評価、昇給の決定、不当な処遇などが提起の対象となります。例えば提起した社員が公正に扱われているか、などについての調査が実施され、必要に応じ是正措置が取られます。

その結果は、通常、その問題を扱った役員が直接提起者に面談し、回答されます。

● Confidentially Speaking (コンフィデンシャルリー・スピーキング)

IBMの方針や施策に関する疑問、社内プロセスの問題、あるいはBCG違反が疑われるような事柄について、社員は所定のプロセスにより問題を提起・通報することができます。提起者が誰であるかは、全社でただ一人、当プログラムのコーディネーターにしか分からない運用となっています(匿名性の保証)。

調査結果は、提起者へe-メールで回答されます。

リスクマネジメント

日本IBMグループは、グループの経営に影響を及ぼすさまざまな危機、リスクへ適切に対応する体制を設けるとともに、IT事業者として危機発生時の事業継続のため、必要な備えを行っています。

危機管理体制

危機管理体制として危機対応プロセスおよびリスク対応プロセスを設けています。これにより、各種危機発生時の緊急対応を行うとともに、平時においてはリスク軽減策の充実を図っています。

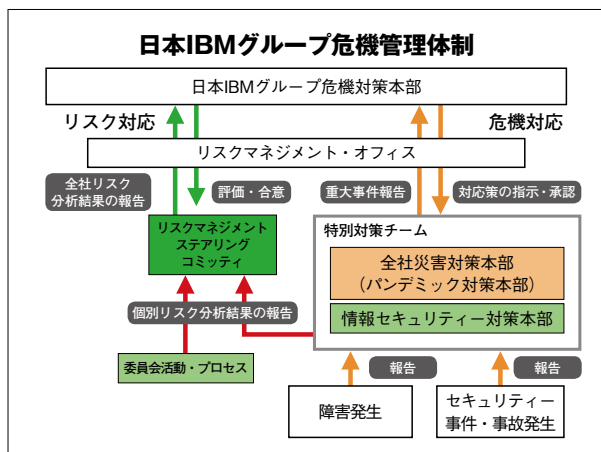
● 危機対応プロセス

製品障害や情報セキュリティに関する事件・事故、自然災害など、日本IBMグループ経営全体に影響を及ぼす危機が発生した場合、日本IBM社長を本部長とする危機対策本部は、最高意思決定機関としていち早く状況を把握し、全社的な視点から対策の実行を指揮します。

危機対策本部の下に設置された特別対策チームは、危機発生時の対応のみならず、既知の特定の危機についてその予防策やリスク低減策を立案します。

● リスク対応プロセス

グループ全社に潜むリスクは、平時より特別対策チームや個別の委員会活動およびプロセスで分析・評価の上、危機対策本部の諮問機関であるリスクマネジメント・ステアリング・コミッティにおいて協議します。危機対策本部は、グループ経営全体に影響を及ぼす重点対応リスクの決定、対応策の承認を行います。



事業継続

IBMでは、これまで世界各国で、電力不足、暴風雨、洪水、津波、テロ、感染症など重大な事態が発生した際に適切に対応してきました。またこれらの潜在的発生可能性への備えも行っています。

IBMコーポレーションは、2005年末、各国IBMに新型インフルエンザ対策立案を指示し、日本IBMでは、2006年年初よりIBMのグローバル・ガイドや日本政府の行動計画、ガイドラインに従い、感染拡大防止に努めるとともに、社会・経済を停滞させないよう、事業継続計画を立案し、継続してその実行性を確認しています。

また日本IBMはお客様のビジネス・プロセスにおける情報システムの継続を実現するため、業界団体である(社)電子情報技術産業協会(JEITA)情報政策委員会においてタスクフォースをリードし、2008年8月、その検討結果を取り入れた提言が政府へ提出されました。*

現代の社会機能は、情報システム・インフラに依存しており、特に、保守・運用サービスは要員やスキルに左右され、一社だけの対策では社会機能の継続を実現することはできません。引き続き、IBMグループや取引先企業とともに、さらにはJEITAをはじめとする業界団体を通じて新型インフルエンザ発生時の事業継続について協議し、万全を期することとします。

* <http://home.jeita.or.jp/is/committee/infopolicy/080826Influenza/>
2008年8月25日、「情報システム産業の視点での新型インフルエンザ対策に関する提言」がJEITAのホームページで公開されるとともに経済産業省に提出されました。

日本IBMのパンデミック*対策

基本方針

- ・ 職場における社員の安全衛生の確保
- ・ お客様への影響の最小化
- ・ 社会への支援を最大化

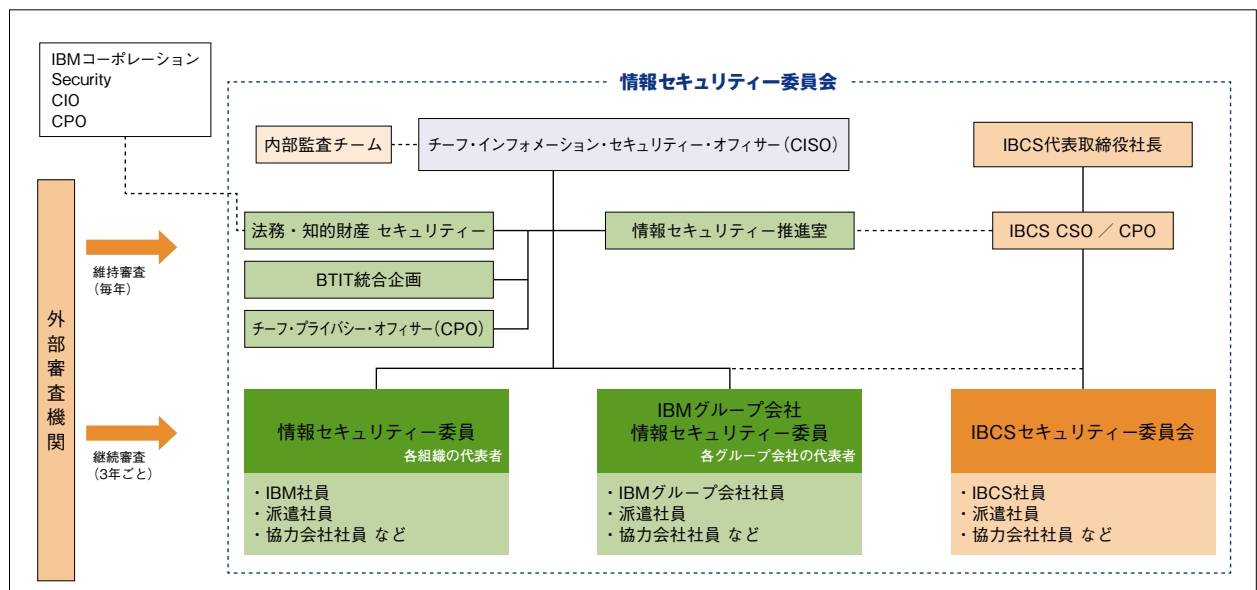
国内感染拡大期、まん延期の対応

- ・ 感染拡大防止のために出社を制限 → 在宅勤務を推進
- ・ 一部の事業所を閉鎖
- ・ 安全を維持しつつ、国民の最低限の生活維持のための業務を継続

*パンデミック：新型インフルエンザ等の感染症の世界的大流行

情報セキュリティ

日本IBMグループは、これまでIBMが長年培ってきた体系的かつ包括的な情報セキュリティの施策を基に、情報セキュリティ・マネジメント・システム (ISMS) を確立してきました。このISMSを基盤として、お客様の最も信頼されるパートナーとして、お客様に提供する価値を最大化していくため、常に情報セキュリティの強化に努めています。



情報セキュリティ・マネジメント体制

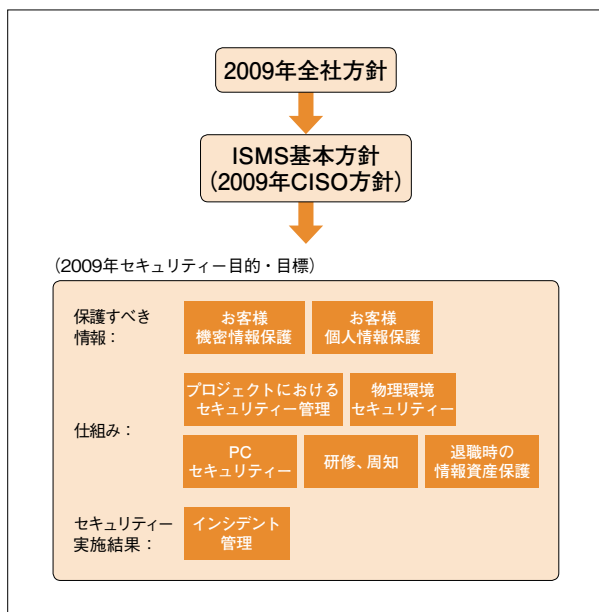
情報セキュリティ・マネジメント体制

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、グループ全体で遵守すべきセキュリティ対策を体系化し、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ISMSを実践しています。（前頁図参照）

全社方針と「セキュリティ目的・目標」の見える化

全社方針である「ハイリスク・インシデントのゼロ」を実現すべく、8項目の「セキュリティ目的・目標」を設定し、全グループでそれらの達成度の「見える化」を実践しています。

「見える化」の仕組みとして、達成度を評価するための目標値および改善アクションを決定するための指標を設定して実施しています。具体的には、お預かりしているお客様情報や個人情報の管理状況、PCやポータブル記憶媒体の管理状況、ワークスペース・セキュリティの遵守状況、セキュリティ教育の受講等を数値化して、グループ全体の基準やルール遵守状況を確認し、また改善活動を実施するトリガーとしています。



全社方針およびCISO方針を実現するためのセキュリティ目的・目標

全社・全グループ参加のISMS統一認証

日本IBMグループでは、これまで日本IBMの全部門、日本IBMグループ会社の一部、およびIBMビジネスコンサルティング サービス (IBCS) において、個々にISMS認証を取得してきました。

2009年は、全社・全グループ参加の日本IBMグループISMS統一認証取得を目指します。

ISMS統一認証の狙いは、日本IBM、IBCSおよび日本IBMグループ各社が、同じISMSの仕組み・ルールに基づいてISMS構築・認証活動を行うことにより、全社・全グループのセキュリティ・レベルを向上させ、お客様に提供する価値を最大化していくことにあります。

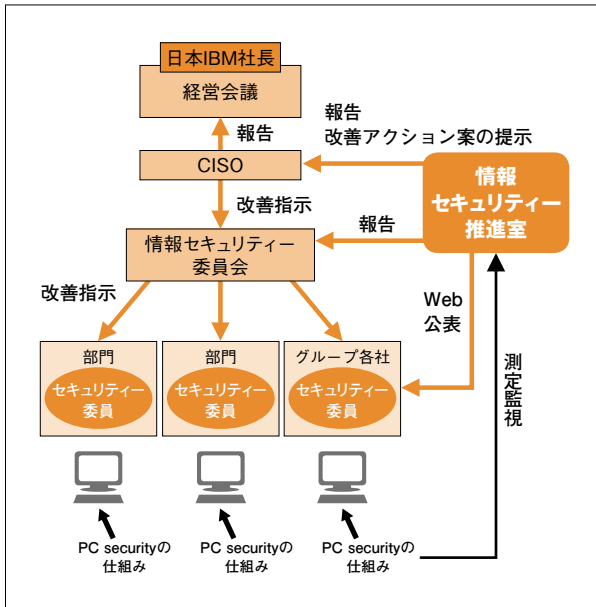


【ISMS登録マークおよびJIPDEC認定マーク】

ITを活用した情報セキュリティの推進

事例1 全従業員のクライアント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、例えば、外部からの不正な侵入を許さないために、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ないように、日常的に遵守状況が点検されています。



ツールと改善活動の概念図

事例2 ポータブル記憶媒体のセキュリティ対策の強化

近年、USBメモリーや外付けハードディスク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グループは、ポータブル記憶媒体使用時に、強制的に暗号化するツールを開発し、業務用クライアントPCからポータブル記憶媒体に情報を書き出す場合には暗号化することを強制する仕組みを導入しています。

プライバシー

IBMのプライバシー規定は今から30年以上前に作られたものですが、それは2005年4月に施行された日本の個人情報保護法の定める要件を満たしています。IBM企業行動基準(BCG)では、プライバシーおよび個人情報の取り扱いが定義されており、世界中のIBM社員はその内容を毎年確認し、同意しています。

IBMでは、ポリシーや基準を定めるだけでなく、ITを用いて、お客様情報および社員個人情報の適切な管理に努めています。個人のPCや記憶媒体、サーバーでの個人情報の保管状況を検索する個人情報検索支援ツールを社内でも活用し、定期的に点検を行うプロセスを確立しています。また、個人情報の管理状況について、情報のリスクに応じて、管理状況を分析するツールを用いて、定期的に監査しています。

プライバシー規定

