リスクマネジメント

**社会の信頼と期待に応え、事業を継続的に営んでいくために、
リスクの把握とそれに対処する体制を整えています**

リスクマネジメントへの取り組みを強化

サントリーのリスクマネジメントは、各カンパニー、各部門等、業務執行レベルでのPDCAサイクルに基づく自己管理を原則としています。各担当取締役は、その対応について責任をもち、重要なリスク案件については取締役会またはグループ経営戦略会議へ報告、付議することになっています。

経営全般にわたる重要なリスクについては、取締役会の委嘱を受けた「コンプライアンス」「品質保証」「個人情報保護」「環境」「ARP」の各委員会が、専門的な見地から全社横断的にリスクの分析・評価を行い予防策を講じるとともに、その強化を図っています。

なお、サントリーではリスクマネジメントに関わる体制・状況について、定期的にグループ監査部による監査を行い、指摘があった場合には直ちに改善策を講じる体制としています。

情報セキュリティ体制を強化

サントリーグループは情報セキュリティポリシーのもと「個人情報や機密情報の安全管理と漏洩防止」「情報セキュリティ遵守意識の維持・向上」「情報システムの安全かつ円滑な稼動の堅持」のために適切なセキュリティ対策を講じています。

2005年には「不正競争防止法」が一部改正施行されたほか、経済産業省から「情報セキュリティガバナンス」の考え方が提示されるなど、企業のセキュリティ強化に対する社会的要請はますます高まっています。そのことを認識し、サントリーは今後、「セキュリティ」「情報の活用」「事業継続性の維持」という3つの観点から、グループ全体で従来以上に厳格かつ適切な情報管理を進めます。そのために、「ルールの再構築・徹底」「教育・啓発活動」「監査」といったPDCAサイクルに沿って取り組みを進めていける体制の整備に2005年12月から取り組んでいます。

●機密情報の管理・保護

経済産業省の「営業機密管理指針」を参照しながら、個人情報を含む機密情報の管理体制の構築を進めています。

物理的・技術的管理の強化

商品開発センターに加え、2005年に、サントリーワールドヘッドクォーターズ(お台場オフィス)および赤坂オフィスにIDカードを用いた入館管理システムを導入しました。また、全社の情報システムに、このIDカードとパスワードによる認証機能を追加し、アクセス管理を強化しました。

この他、情報漏洩防止のためのパソコン持ち出し制限、社外からの不正アクセス・攻撃防止のためのファイアーウォール設定など情報管理を徹底しています。


お台場オフィスの入館管理システム

人的・法的管理の強化

2003年10月に情報システム利用上の詳細規定をまとめた「情報システムセキュリティ保持規定」を、翌年11月に「サントリーグループ機密情報管理規定」をそれぞれ制定。機密情報の管理に関するグループ全体での基本的な規定を明文化しました。

また、これら規定を確実に遵守していくために、2004年にはグループの全従業員を対象にe-ラーニングを実施したほか、各種機密情報の管理に関する情報をイントラネット上に掲載して周知徹底を図りました。

さらに、全従業員は、2005年から毎年提出する「コンプライアンス誓約書」によって機密情報を適切に管理することを誓約しています。


eラーニング画面

●お客様の個人情報を保護

サントリーグループ各社は、事業活動の中で、商品の販売促進キャンペーンへご応募いただいたお客様や健康食品などの通信販売をご利用のお客様をはじめとする多くの方の個人情報をお預かりしています。

これらの大切な個人情報を守るため、サントリーは2001年4月に「プライバシーポリシー※」を定めて適切な取り扱いに努めてきました。

2004年4月には、個人情報保護体制を一層強化していくため、「個人情報保護委員会」を設置。個人情報保護法・ガイドラインなどに基づき、e-ラーニングによる従業員教育を実施するなど、グループ全体で個人情報保護に取り組んでいます。

※ サントリーの「プライバシーポリシー」URL
http://www.suntory.co.jp/privacy/

キャンペーン履歴管理システム

キャンペーンについては、業務委託先との間で機密保持契約書を締結したうえで、「キャンペーン履歴管理システム」によって情報の入手から廃棄に至るプロセスを管理しています。
また、保管が必要な個人情報は、社内に構築されたデータベースで一元管理するなど、お客様の情報を確実に保護するよう努めています。

通信販売顧客の情報管理

通信販売顧客の情報は、通信管理センター内に整備した専用のクローズドシステムで一元管理し、センターへの入退出者については静脈認証により厳重に管理しています。
2005年度は、これらの仕組みの整備・強化に加え、社内に保管していた個人情報の峻別・廃棄とその実施確認、「個人情報保護法」に関わる従業員および業務委託先などへの教育・研修、各部署・グループ会社・キャンペーン事務局の監査などに取り組みました。


通信管理センターの静脈認証

知的財産権を活用・尊重

社会における知的財産に対する意識の高まりや国による数々の施策により知的財産の重要性は年々増してきています。サントリーは、2003年に知的財産権を統括する部署として「知的財産部」を設置し、製品や技術の研究・開発を通じて獲得した成果を知的財産として権利化・活用し、サントリーならではの高付加価値商品を継続して供給するための活動を進めています。
また、研究・開発活動の現場に密着して、情報収集に努め、他人が保有する知的財産権に配慮し、それを侵害しないよう留意しています。たとえば、新しい技術の採用にあたっては他社の特許が存在しないか、また商品名の採用に関しては、類似商品が登録されていないかなどを調査し、他人の知的財産権に類似するか否かの判断にあたっては、必要に応じて専門家の意見も仰いでいます。

クライシスマネジメント体制を整備

会社にとっての危機を未然に防ぐための「リスクマネジメント」とあわせて、万一、危機的状況が発生した場合に備えておく「クライシスマネジメント」も重要です。サントリーでは、2003年12月に「有事対応基本方針」を策定。この方針に沿って、危機が発生したときに、迅速な意思決定と情報伝達、具体的かつ適切な対処ができる体制の強化を進めています。
なお、「有事対応基本方針」では、お客様をはじめとするステークホルダーの安全を最優先とすること、適切な情報開示を行うこと、全従業員が当事者意識をもって速やかかつ誠実に対処することなどを定めています。

クライシスマネジメント体制の例

●製品品質問題

製品の品質や表示に問題が発生した際に、迅速な対応によってお客様の被害を最小限にとどめ、損害の影響を極小化することを目的に、対応マニュアルを策定しています。この中の基本方針として「お客様の安全・安心を最優先すること」「一貫して誠実に対応すること」「適切な情報開示を行い説明責任を果たすこと」を明記。あわせて、問題発生時の対応体制と判断基準、再発防止策を確実に実施することなどを明確にしています。

●大規模地震

大規模地震が発生した場合には、従業員に対して本人および家族の安全確保を最優先するとともに、会社への安否連絡をすることを定めています。また、「対策本部」を設置し、その下に、総務部、人事部を中心に「対策本部事務局」を設置します。対策本部事務局では、主として従業員や家族の安否情報の確認や被害情報の収集・整理などを実施します。また、各部が作成している災害発生時の活動方針に沿って実施する「事務所機能復旧」「情報システム復旧」「救援物資等手配」「生産機能復旧」「得意先・地域社会支援」などの活動と連動します。これらの体制や手順については、総務部のイントラネットの「防災」欄の「震災時危機管理体制について」に掲載し、従業員がいつでも確認できるようにしています。
さらに、災害発生時にも重要事業をできるだけ中断せず、ステークホルダーに対する責任を果たしていくために、生産、物流、情報システム等について事業継続計画(BCP)を策定しています。