リスクマネジメント体制

基本姿勢

会社にとって重大な危機が発生し、または予見される際に、機敏かつ的確に対応し、健全な企業活動を維持することができるよう、CSR会議を中心とした危機管理体制を構築しています。

リスクマネジメント推進体制

リスクマネジメントに関しては、「CSR会議」の中で審議・報告されています。リスクマップを作成し、重要度・緊急度に応じた層別を行っています。災害時などには、全社防災対策本部を立ち上げるなど、迅速に防災体制を確立できるように準備・訓練を進めています。

リスクマネジメント・ガイドライン

当社は、危機管理規程および危機の態様に応じた各種規程を策定・周知しています。また、経営環境の変化や事業を取り巻く新たなリスクが想定されるときには、万全の体制が取れるように、逐次見直しを行うよう定めています。2016年1月の事故を踏まえ、初動対応・社内外の連携を高めていきます。

教育・啓発

全ての階層別研修に「リスクマネジメント（危機管理）」のカリキュラムを設け、CSRの中での位置づけと重要性に加え、自社における危機事例などの紹介を行い、リスク感性を高めると共に、予防・再発防止と発生時の初動行動などについて周知を行っています。

防災対策

東日本大震災後、「大震災対策検討委員会」を立ち上げ、社員の安全を第一に、ソフト安全・ハード安全・生産復旧の3つの分科会を置いて震災対策強化を進めるとともに、事業継続マネジメント（BCM）のブラッシュアップを進めています。
2015年は、それぞれの分科会において下記の対策を行いました。

ソフト安全分科会

人がより安全に避難できるようにするために

①継続的な「防災ニュース」の発行による社員啓発の実施
②負傷者搬送なども含めた実戦的な避難訓練の定期的な実施
③備蓄食料等の充実　など。

ハード安全分科会

建物や構築物の震動による人的被害を防止するために

①安全に避難できるよう建物内外の更新・拡充　など。

生産復旧分科会

早期にお客様に製品をお届けできるように

①揺れや液状化による致命的な被害を防止するための設備の補強（継続中）
②国内外グループ、仕入先、同業など広い範囲での代替生産の検討
③少人数の出勤でも重要生産ラインを操業できるよう、要素技術、キーマンの育成
④情報システム、データのバックアップ対応　など。

防災体制図

歩道灯

情報セキュリティ

基本姿勢

機密事項とは、開示・漏洩等により会社が不利益を被る情報または第三者を利する情報・製品・施設であり、かつ情報セキュリティ推進体制に定める機密管理責任者による開示制限の指定を受けた全ての情報・製品・施設であって、形式を問いません。なお、正当な手段で入手した他社の機密事項も含むものとしています。

情報セキュリティ・ガイドライン

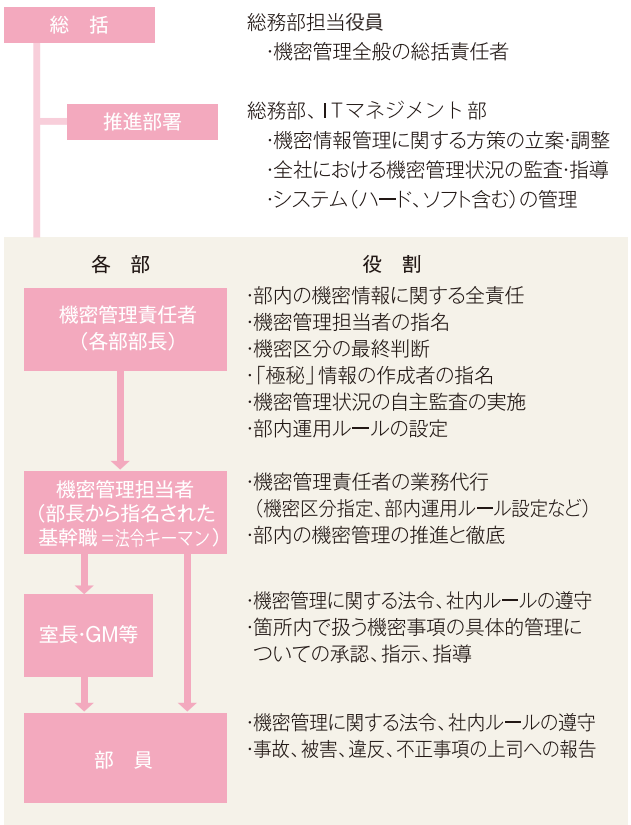
当社は、機密管理や個人情報の漏洩を防止するため、文書・データの管理手順、メールの送受信、PCおよびその周辺機器の管理基準・手順に関する規程を定めています。

(規程の例)
- 文書管理規程
- 機密管理規程
- 情報開示規程
- 個人情報保護規程　など

当社およびグループで発生する情報やお客様、お取引先様、その他関係者および社員などから入手した情報を取り扱う際には、社内規程に従って適切に取り扱い、厳正に管理しています。

情報セキュリティ推進体制

各部管理体制と役割



情報セキュリティ

機密管理の重要性を認識し、適切に情報管理が行えるよう、オールトヨタセキュリティガイドライン(ATSG)に基づき、社内体制の整備・システム的な規制・ルールの周知・教育・点検などを行っています。
社外に発信されているメールの情報に問題がないか、社員が社内情報を不用意に持ち出さないか、USBメモリやカメラなどの情報機器の取り扱いに問題はないかなど、リスクマネジメント担当部門で監査を実施(強化)しています。
グループ会社に対してもオールトヨタセキュリティガイドライン(ATSG)を展開し、アイチグループ全体で情報セキュリティを向上させる取り組みをしています。

情報監査実績

メール監査	22件	パスワード設定漏れ パスワード本文記載 個人端末への送信
手荷物点検	5月:3件 10月:2件	許可申請帳票の不備など

情報セキュリティの啓発と教育

CSR会議の中で、役員層に対して当社グループの機密管理レベルの現状と課題・取り組み状況を報告し、経営課題として共通認識を持つようにしています。
社員については、日常業務でパソコンを使用する者全員に対し、「情報セキュリティチェックリスト」による情報機器の扱いや各種ルールについてのチェックを実施しています。そしてその結果に基づき、各部門での教育・所属長からの指導を行っています。
また、社会で発生している機密漏洩事故事例をニュース形式で展開し、また社内にてコンピュータ・ウィルスなどが確認された場合には、全社に注意喚起を行うなど、機密管理意識の啓蒙を図っています。