リスクマネジメント

基本的な考え方　2010年の一連のリコール問題を踏まえ、トヨタはリスクマネジメント体制の強化を図ってきました。同年6月に「リスクマネジメント委員会（現 サステナビリティ会議およびESG委員会）」を設置し、グローバル並びに各セクションにリスク責任者を任命するなど、事業活動において発生するリスクを予防・軽減するための活動にグローバルで取り組んでいます。

推進体制・仕組み

グローバルリスクマネジメントの責任者として「グローバルCRO（チーフリスクオフィサー）」を設置し、重要リスクの掌握、グローバル重大有事対応の統括・指揮を行っています。その下には、各地域を統括する「地域CRO」を配置し、地域ごとのリスクマネジメント体制を構築しています。

また、社内のヘッドオフィス（経理・調達など）では機能別リスク担当として各本部長・各部門リスク責任者を、各カンパニーでは製品別のリスク担当として各プレジデント・各カンパニーリスク責任者を任命し、各地域本部や各セクションが相互に連携・サポートしあえる体制をとっています。

グローバルリスクマネジメントの統括の仕組みとして、「ESG委員会」において、リスク予防のアクションにつなげるという目的で、事業活動を妨げるリスクを徹底的に洗い出し、現状直面する重要リスク項目の確認・報告などを行います。

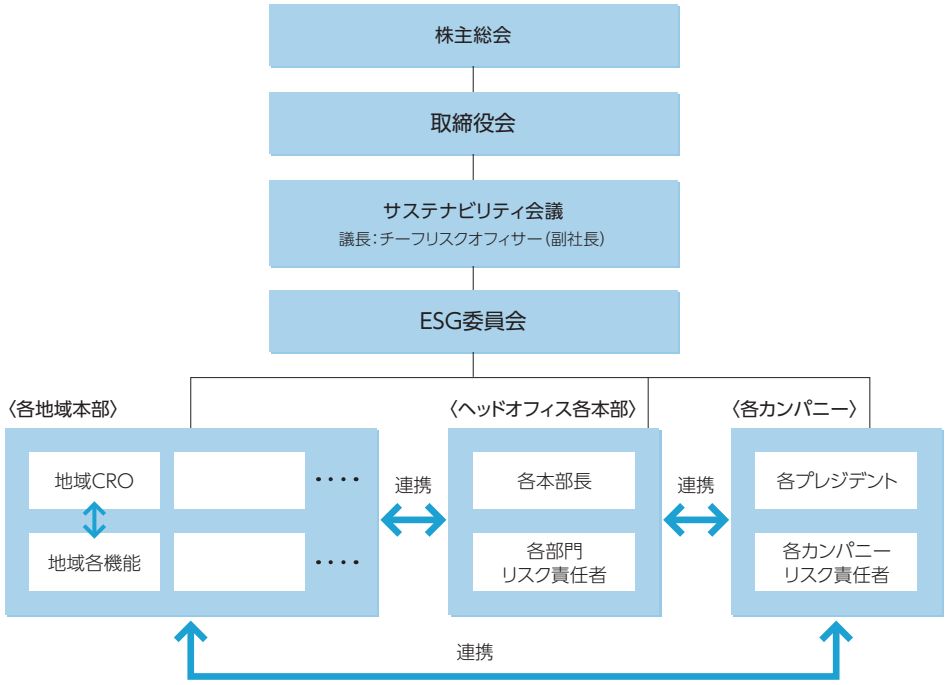
さらに、業務執行の監督としての「サステナビリティ会議」において、ESG委員会の結果を報告しています。

なお、近年、企業においてリスクが増大している「情報セキュリティ」「BCM（事業継続マネジメント）」については、特段の取り組みを進めています。

トヨタの事業などのリスクについては、投資家の判断に重要な影響を及ぼす可能性のある「市場および事業に関するリスク」「金融・経済のリスク」「政治・規制・法的手続・災害などに関するイベント性のリスク」を有価証券報告書に記載しています。

有価証券報告書　Web https://www.toyota.co.jp/jpn/investors/library/negotiable/

推進体制



情報セキュリティの取り組み

近年、サイバー攻撃が巧妙・複雑化しています。会社の機密情報や情報システムのほか、ネットワークでつながる工場設備や自動車などの制御に関するシステム（車載システムなど）も、サイバー攻撃のターゲットとなっており、トヨタにおける情報セキュリティの重要性は高まっています。
トヨタは、このようなサイバー攻撃の脅威に対し、お客様の安全・安心を確保し、個人情報などのお客様の財産を守ることを社会的責務として捉え、ガバナンスおよびリスクマネジメントの観点から、情報セキュリティ強化に向けてさまざまな活動に取り組んでいます。
2016年6月には、情報セキュリティに対する基本的な考え方や取り組み姿勢を明確にし、TMCおよびTMCの子会社が一体となって情報セキュリティに取り組むことを目的として、「情報セキュリティ基本方針」を定めました。

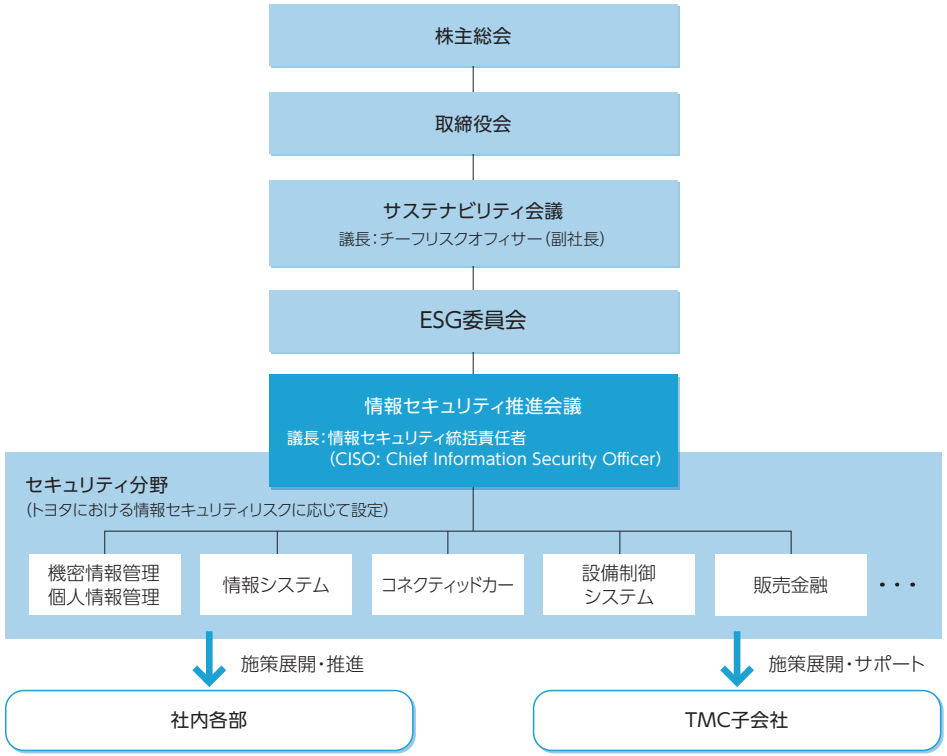
情報セキュリティ方針（トヨタの基本的な姿勢）

① 法令遵守
② 安定した経営基盤の維持
③ 安全な商品・サービスの提供
④ 安全なサイバー空間づくりへの貢献
⑤ 情報セキュリティマネジメント

情報セキュリティ基本方針 Web https://www.toyota.co.jp/jpn/sustainability/governance/risk-management/pdf/information-security-policy.pdf

推進体制・仕組み

情報セキュリティ統括責任者のもと、セキュリティ分野ごとに責任者を配置し、活動を推進しています。
また、各セキュリティ分野の活動内容や全体の共通課題については、情報セキュリティ推進会議で共有・検討し、トヨタ全体の情報セキュリティの向上を図っています。



情報管理の取り組み

トヨタは、内部からの情報の漏洩防止や近年増加するサイバー攻撃に対応する仕組みとして、TMCおよびTMCの子会社・関連会社を対象とした「オールトヨタ セキュリティ ガイドライン（ATSG）」を定め、情報セキュリティの徹底に取り組んでいます。

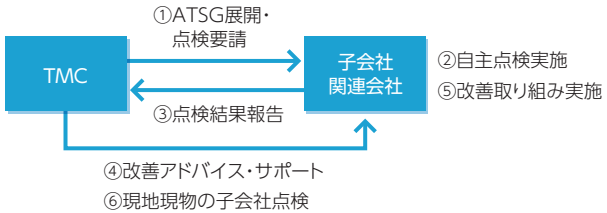
ATSGでは、取り組むべき対策として、組織的管理策、人的管理策、技術的管理策、物理的管理策のほか、事件・事故発生時の対応体制の整備を定めており、さまざまな観点からの情報セキュリティ確保につなげています。なお、昨今の環境変化や高度化するサイバー攻撃に対応するため、ATSGは定期的に見直しをしています（最新改訂2018年4月）。

また、ATSGによる各社の情報セキュリティの取り組み状況の点検を年1回実施することにより、各社の情報セキュリティの継続的な維持・向上に努めています。さらに2018年度からはTMCによる現地現物の子会社点検活動も開始し、改善に取り組みます。

オールトヨタ セキュリティ ガイドライン（ATSG）

① 組織的管理策（体制・ルールの整備など）
② 人的管理策（従業員への教育など）
③ 技術的管理策（ネットワーク対策など）
④ 物理的管理策（入退室管理など）
⑤ 事件・事故発生時の対応体制の整備

子会社、関連会社へのATSG推進の仕組み



個人情報については、一人ひとりへの教育により法令遵守・適切な取り扱いを周知徹底しています。2017年は改正個人情報保護法（日本）、GDPR（欧州）[*1]などへの対応に取り組みました。今後とも個人情報保護に努めます。

自動車関連については、自動車メーカーが参加するサイバーセキュリティ攻撃事例の情報を共有する組織「Auto-ISAC[*2]」にも日米で加盟し、最新動向を確認しながらサイバーセキュリティ向上に努めています。

＊1 GDPR（General Data Protection Reglation）：EU一般データ保護規則
＊2 Auto-ISAC（Automotive Information Sharing & Analysis Center）：自動車情報・共有分析センター

トヨタ流事業継続マネジメント（BCM）

東日本大震災やタイの洪水などの大規模災害においては、トヨタは自社が直接的な被災をしていないにもかかわらず、生産が長期間にわたり継続できない事態に陥り、販売・サービスの両面でお客様にご迷惑をおかけしました。

昨今は「南海トラフ巨大地震」の発生が危惧されていますが、その被災想定エリアにトヨタグループの主要機能が集中しており、大規模地震が起きた場合は生産や物流などに甚大な影響が生じると予想されます。

そうした万一の場合に備え、トヨタが策定しているのが、限られたリソースで事業の早期復旧を実現するための「事業継続計画（BCP[*3]）」です。

トヨタは、「いい町・いい社会」づくりへの貢献という目的のもと、災害時は行動規範にのっとって復旧に取り組むこととし、2016年4月に発生した「熊本地震」でも、このBCPに基づき対応に当たりました。

＊3 BCP（Business Continuity Plan）

トヨタの行動規範（災害時の優先順位）

1	2	3
人道支援（人命第一、救援）	被災地（地域）の早期復旧	自社の業務・生産復旧

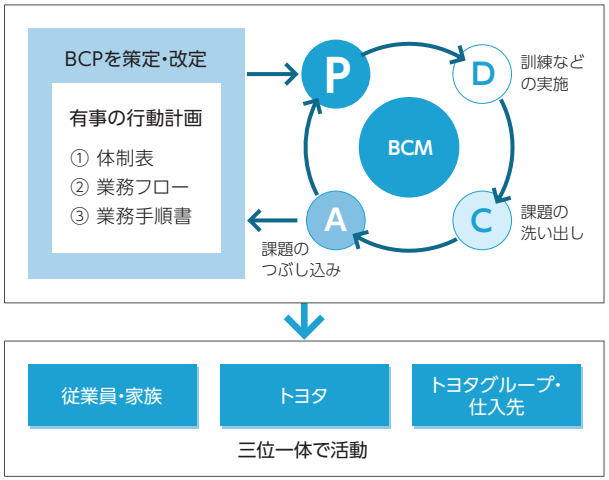
トヨタのBCM活動

トヨタのBCPは、訓練などによりPDCA[*4]を回して改善を行うことで、その実効性を高め続けています。

この活動を「事業継続マネジメント（BCM[*5]）」と位置付け、「従業員・家族」「トヨタグループ・仕入先」「トヨタ」が「三位一体」となった活動として推進しています。

こうしたBCPの策定・見直しの過程を通じて有事に強い人材を育成し、平時から危機に強い組織・職場・個人づくりを目指しています。

＊4 PDCA：Plan（計画）・Do（実行）・Check（評価）・Action（改善）を繰り返すことによって、業務を継続的に改善するサイクル
＊5 BCM：Business Continuity Management



人道支援、被災地（地域）の早期復旧

災害時は、行動規範にのっとった地域復旧を優先させるという活動の実行性を高め、災害に強いまちづくりに貢献するため、トヨタは行政との包括的な災害支援協定を締結しています（豊田市、みよし市、田原市、裾野市）。そのなかで、人道支援・地域復旧支援は行政との相互協力のもとで実施することとし、あらかじめBCPの中に織り込んで体制を整備するとともに、行政との合同訓練を実施するなど、平時からの備えを進めています。
主な支援内容は下記のとおりです。その他、指定避難場所用施設の提供など、行政ごとに締結している内容もあります。

主な支援内容

① 災害発生時の救援・救護活動
② 大規模震災時における一時避難場所の提供
（被災した地域住民の受け入れ）
③ 食料・飲料水・生活物資などの行政（市民）への提供
④ 市設置の救援物資など受け入れ施設における荷役支援
⑤ 地域インフラ（上下水道、道路など）復旧工事などに必要な用地の提供
⑥ 社員の地域復旧活動への参画

サプライヤーと一体となった災害に強いサプライチェーンの構築

これまでトヨタは「1．人道支援」「2．被災地の早期復旧」「3．自社の業務・生産復旧」の優先順位の考え方に基づき、復旧支援をしてきました。特に東日本大震災以降は、さらなる初動迅速化、復旧早期化を目指し、各国・各地域でサプライヤーと一体となった「災害に強いサプライチェーンの構築」に努め、平時からの「サプライチェーン情報の見える化」と「災害に備えた対策」を推進してきました。
日本における「サプライチェーン情報の見える化」では“日本のモノづくりを守る”という思いのもと、非常に機密性の高い情報をサプライヤーからご提供いただき、データベース（RESCUE*システム）を構築しました。トヨタは、各社の情報について守秘義務を厳守しつつ、災害時に有効活用するための定期訓練をサプライヤーと共に実施。2016年4月に発生した熊本地震に加え、2018年5月の大阪北部地震、6月の西日本豪雨の際も活用されました。
本システムは汎用化され、活動事例を含めて日本自動車工業会を通じて他社へも展開しており、災害に強いサプライチェーン基盤構築の一助となっています。
海外でも各国・各地域で、サプライヤーと一体となった同様の取り組みが進められています。

＊ RESCUE：REinforce Supply Chain Under Emergency

サプライチェーン情報を保有するRESCUEの仕組み