第9章 危機管理の徹底

第9条

市民生活や企業活動に脅威を与える反社会的勢力の行動やテロ、サイバー攻撃、自然災害等に備え、組織的な危機管理を徹底する。

背景

（1）多様化・複雑化する脅威

企業のグローバル化の進展に伴い、市民生活や企業活動に影響する脅威が多様化、複雑化している。例えば、反社会的勢力の活動は、広域化、不透明化するとともに手口も巧妙かつ多岐にわたり、悪質化の傾向を強めている。また、テロ組織による悪質な行為が多発し、経営トップや従業員をはじめ幅広いステークホルダーが巻き込まれ、大変痛ましい事態が発生している。

さらに、サイバー犯罪やサイバーテロといったサイバー攻撃が世界的規模で頻発するようになった。

その他にも、地震災害や豪雨による洪水、土砂災害、火山噴火など、世界各地で広域かつ甚大な被害をもたらす自然災害が多発し、深刻な人的・物的被害が生じている。

こうした危機に対して、企業は、危機管理体制の確立とともに、組織的な対応を図ることが求められている。また、個社のみならず、多様なステークホルダーと連携し、取り組みを強化することが不可欠となっている。

（2）企業における反社会的勢力との対決姿勢、一切の関係遮断

「暴力団員による不当な行為の防止等に関する法律」（暴力団対策法）の施行、都道府県による暴力団排除条例の制定などにより、市民や企業の間で暴力団排除意識が大きく進展し、暴力団の社会的孤立が進んだ。

しかし、近年では、暴力団が、その威力を明確に誇示して利益や便宜供与を要求することは減少する一方、通常の取引関係を装って企業活動に介入する傾向が強まっている。この結果、暴力団排除志向の高い企業であっても、暴力団などであると知らずに結果的に経済取引を行ってしまう可能性がある。また、暴力団関係企業や暴力団周辺者を利用するなどした資金獲得活動や犯罪も絶えない。このように、暴力団をはじめとする反社会的勢力による市民、企業、行政を対象とする暴力行為、違法・不当行為は、健全な市民生活や企

業活動にとって脅威となっている。

そのため、企業に対しては、引き続き、反社会的勢力との一切の関係遮断を計り、反社会的勢力に不当な利益を得させないように努めることが求められる。各企業は、社会的責任を強く認識するとともに、企業防衛に努め、社会正義に反する行為を許さず、反社会的勢力とは、断固として対決する基本方針を確認し、広く社会に宣言するとともに、社内体制の整備や従業員の安全確保を行い、関係する外部機関と積極的に連携して対策を組織的に実行しなくてはならない。

（3）テロへの対応

近年、宗教的過激主義、極左思想、移民・外国人排斥を含む極右思想などに基づくテロリズムが国際的に活発化している。空港や地下鉄駅など不特定多数の人が集まる場所や外国人が多く訪れる観光地などで、銃撃や自爆テロといったテロ事件が頻発している。過激派組織「イスラム国」（IS）の勢力は弱まってきているとみられる一方で、テロの実行主体者が、イスラム過激思想に影響を受けた若者や、組織とは関係なく単独で動く人物である場合の増加が指摘されている。

また、日本国内においても1995年３月に発生したオウム真理教の地下鉄サリン事件では大変痛ましい被害が発生するなど、国内テロへの警戒も怠ることはできない状況にある。

（4）サイバーセキュリティ対策の急務

サイバー攻撃による企業からの技術情報などの流出、国民や経済活動に大きな影響を及ぼす情報システムや重要インフラ、生産ラインなどの制御システムの停止など、企業におけるサイバー攻撃の被害件数は増加傾向にあるばかりでなく、影響の範囲も多岐にわたっている。

また、特定の企業や組織の機密情報を狙う「標的型攻撃」や企業のサーバーを踏み台にして国民や事業者を狙う「水飲み場型攻撃」では、プロの集団の巧妙な手口により、攻撃を受けていてもそのことに気づかない企業は少なくない。国家が関与する攻撃もあることから、国の防衛・外交努力が重要ではあるが、攻撃対象となる民間企業も主体的に対策を進める必要がある。

サイバーセキュリティ対策の中核拠点
（サイバーセキュリティ・ファクトリー）の構築
（提供：日本電気）

9-1 組織的な危機管理体制を整備する。

基本的心構え・姿勢

緊急事態が発生した場合のことを想定し、速やかに適切な対応がとれるよう、危機管理体制を整備しておく。

具体的アクション・プランの例

1 緊急事態に対応する社内体制を構築する。

❶ 平時より経営トップを長とする対策本部の設置を準備する。

a. 対策本部のメンバー、任務、機能などを明確化する（規程整備）。メンバーは広報部、総務部、人事部、法務部、顧問弁護士、その他関連部門のスタッフを含むようにする。

b. 対策本部と現場を含めた情報連絡・指揮命令系統を明確化する

❷ 危機管理マニュアルを作成する。マニュアルに記載すべき事項は次の通り。

a. 会社の危機管理に関する方針、基本理念

b. 緊急事態発生時の経営トップの役割

c. 緊急事態発生時の管理体制、関連組織の業務と権限

d. 連絡体制

e. 基盤インフラの確保

f. 従業員一人ひとりの行動マニュアル

g. その他、自社の業容・業態に即した対応要領

［ポイント］

- 自社の事業上のリスクを棚卸しし、発生しうるリスクの具体的事例を解説する。
- 個々の事態において、是非すべきこと、絶対すべきでないことを整理、分類した上で、箇条書きで表記する。

2 緊急事態への対応に関する研修、訓練を実施する。

❶ 一般従業員、管理職など階層別に、また管理部門、営業部門、製造部門、研究部門などの部門別に研修を実施する。

❷ 緊急事態の発生を想定し、対策本部の設置や関係部門との連絡、広報対応などについての訓練を実施する。

❸ 緊急事態発生時の経営トップによる報道機関への対応に関するメディアトレーニングを実施する。

9-2 反社会的勢力を排除する基本方針を明確に打ち出し、社内体制を確立する。

基本的心構え・姿勢

反社会的勢力に毅然とした態度で臨み、付け入る隙を与えない企業活動を実践することは、健全な市民社会の形成に寄与するとともに、企業価値の毀損の防止につながる。企業活動に重大な脅威を与える反社会的勢力との関係根絶のため、経営トップは、反社会的勢力との関係を完全に遮断し、断固としてこれらを排除する決意を社内外に明らかにする。同時に、反社会的勢力による組織暴力に対しては、「恐れない」「金を出さない」「利用しない」「交際しない」、いわゆる「三ない運動＋1」を基本として、自ら、社内体制を確立する。

具体的アクション・プランの例

1 経営トップが反社会的勢力との絶縁を宣言する。

❶ 経営トップは、反社会的勢力と関係を遮断し、断固としてこれらを排除する決意を明確に社内外に宣言する（絶縁宣言）。

❷ 経営トップ以下、組織全体として遵法意識を高め、社会的良識を備えた善良な市民としての行動規範を確立し、遵守することにより、企業活動のあらゆるレベルで反社会的勢力との結びつきを阻止し、健全な企業風土を醸成する。

2 反社会的勢力の排除に向けた社内体制を確立する。

❶ 反社会的勢力は、社会的信用を重視する企業に巧妙に付け込み、法的対抗手段の行使をためらわせる。そこで、業務の適正を確保するために必要な法令遵守・リスク管理事項として、反社会的勢力による被害防止を内部統制システムに位置づけた上で、担当部署を設置するとともに社内の諸規則や組織的対応体制を整備し、社内規則に基づいて民事・刑事の両面から法的対抗手段を行使できるよう、社内体制を整備する。

a. 平素からの備えと問題解決能力の維持・向上が必要である。反社会的勢力との一切の関係遮断を図るために必要な内外の関連情報を一元的に管理するとともに、常に外部専門機関と連携し、問題解決のための指導・支援を行う組織を用意し、人材の育成に努める。

b. 常に危機管理意識を維持し、反社会的勢力に付け入る隙を与えないよう、反社会的勢力からのアプローチに対応する社内規則や業務マニュアルを策定し、教育・研修に努める。また、組織的対応の実効性を確認するために、業務監査を強化する。

参考

＜９－２、９－３共通＞

- 「警察白書」2015年　国家公安委員会・警察庁
- 「世界一安全な日本　創造戦略」2013年　犯罪対策閣僚会議
- 「暴力団対策に関する有識者会議報告書」2012年　警察庁
- 「東京都暴力団排除条例」2011年　東京都
- 「企業活動からの暴力団排除の取組について」2010年　犯罪対策閣僚会議暴力団取締り等総合対策ＷＴ
- 「企業が反社会的勢力による被害を防止するための指針について」2007年　犯罪対策閣僚会議
- 「いわゆる総会屋対策の推進について」1997年　いわゆる総会屋対策のための関係閣僚会議
- 「総会屋等への対応について警察庁からの要請」1997年　経団連
- 「当面の総会屋等への対応策について」1997年　経団連
  （http://www.keidanren.or.jp/japanese/policy/pol142.html）

9-3 反社会的勢力による被害防止のために、全社を挙げて法に則して、関係団体とも連携して対応する。

基本的心構え・姿勢

反社会的勢力の組織暴力に対しては、対応する役員、従業員が孤立することが最も危険である。反社会的勢力による不当要求は、人の心に不安感や恐怖感を与えるものであり、何らかの行動基準などを設けないままに担当者や担当部署だけで対応した場合、要求に応じざるを得ない状況に陥ることもあり得る。対応窓口には常に複数名で対応できるよう人材を配置し、全社を挙げて迅速かつ組織的に対応する仕組みを構築する。

商取引にあたっては、取引相手の属性をチェックし、契約や取引約款などに暴力団排除条項を設けるなど、反社会的勢力の排除に徹底して取り組む。

被害を受けた場合には、警察に被害届を提出する。企業の落ち度や不祥事を理由に不当要求が行われた場合にも、速やかに事実調査と原因究明を行うとともに、関係者の法的責任を明確にした上で躊躇せず警察に被害届を出すなど、毅然として法に則した解決を図る。

反社会的勢力との裏取引や事実隠蔽は、反社会的勢力による被害を拡大させ、企業の存続に関わる問題を引き起こすことから、絶対に行わない。

反社会的勢力の排除のために、平素から警察の組織犯罪対策部局、暴力追放運動推進センター、民事介入暴力を専門とする弁護士、業界団体連絡会など、関係団体との信頼関係を構築する。反社会的勢力により被害を受けるおそれがある場合には、速やかに関係団体と連携し、法的対抗措置を行使する。

具体的アクション・プランの例

1 警察など関係機関と緊密に連携し、迅速かつ組織的に対応する。

❶ 社内に窓口部署と警察など関係機関との通報担当責任者を設置する。また、報告ルートと指揮命令系統を整備し、平素から緊密な連携を保つ。

❷ 業界ごとのデータベースや警察、暴力追放運動推進センターなどから情報収集を行い、反社会的勢力の情報管理・評価に努め、取引相手の属性のチェックに活用する。また、反社会的勢力に関する情報は一元的に管理・蓄積し、適切に活用する。

❸ 平素から自社の対応方針に従い、研鑽に努める。反社会的勢力との接触にあたっては、対応の初期段階から相手方の特定に努め、会話や面談の録音・文書化、ビデオ撮影などの記録化を行い、法的対抗措置として活用する。

❹ 取引関係を通じた被害防止のため、契約書や取引約款などに暴力団排除条項を導入する。また、自社株の取引状況や株主の属性情報を確認するなど、株主情報の管理を適切に行うとともに、反社会的勢力による株式買占め防止に努める。

❺ 相手方が反社会的勢力であるかどうかについて、常に注意を払う。反社会的勢力とは知らずに何らかの関係を有してしまった場合には、相手方が反社会的勢力であると判明した時点や反社会的勢力であるとの疑いが生じた時点で、速やかに担当部署に連絡し、組織的に連携して関係を解消する。

❻ 正体を隠した反社会的勢力の介入事例、傾向、対応マニュアルなどを全社的にストックし、従業員全体に周知徹底を図る。

❼ 総会屋対応については、平素から警察との意思疎通を図り、利益供与要求罪に該当するような不当要求行為に対しては、その前兆を察知した段階で迅速に通報し、適時、適切なる指導と支援を要請する。

2 裏取引や事実の隠蔽は、絶対に行わない。

❶ こちら側の落ち度を理由とする取引先からの不当要求に対しては、法的責任を見極めて適切に対応するとともに、裏取引は絶対に行わない。

❷ 企業活動や役員・従業員など個人の不祥事を理由とする反社会的勢力による不当要求に対しては、問題の内容に応じて、対外公表を含めて適切に対応するとともに、要求は断固として拒絶する。

❸ 反社会的勢力による被害については、内容や被害額の如何にかかわらず、直ちに警察に被害届を出す。また、事件化に躊躇することなく法的な対抗手段に訴えるなど、あらゆる刑事的・民事的な対抗策を講ずる。

3 平素から警察などの外部機関との信頼関係を構築する。

❶ 担当窓口部署は、警察など外部機関の連絡先と担当者を確認し、情報交換に努め、平素から信頼関係を構築する。また窓口担当者は、不当要求防止責任者講習をはじめとする各種講習を受講するなどして、民事介入暴力への対応能力の維持向上に努める。

❷ 志を同じくする企業・団体と連携、情報交換を行う。また、特防連（公益社団法人警視庁管内特殊暴力防止対策連合会）や、各県の暴力追放運動推進センター、企業防衛協議会などの暴排活動に参加する。

❸ 契約書や取引約款などにおいて暴力団排除を規定するモデル条項を業界間で協力して作成し、普及させる。

❹ 反社会的勢力情報を集約した業界ごとのデータベース構築などに協力する。

4 有事の際は、外部機関と連携し、企業と関係者の安全を確保する。

❶ 反社会的勢力への対処にあたっては、弁護士などを通じ、内容証明郵便の送付、各種の不当行為を禁止する仮処分の申し立て、債務不存在確認訴訟や損害賠償請求訴訟の提起など、あらゆる法的措置を活用する。

❷ 警察から責任追及に向けた協力要請があった場合、躊躇することなく被害届を提出し、犯罪捜査に積極的に協力する。

❸ 株主総会に関しては、平素から情報収集に努めるとともに、利益供与要求の前兆段階から警察に通報し、指導・支援を要請する。

❹ 反社会的勢力からの不当な要求に対応する窓口部署担当者の安全確保に努める。

9-4 テロの脅威に対する危機管理と対策に取り組む。

基本的心構え・姿勢

国内外を問わず、テロなどの事件・事故に巻き込まれる可能性が高まっていることを踏まえ、企業ならびに従業員は、まずは自分の身は自分で守るとの意識を持ち、それぞれが日本企業や日本人が置かれている状況を正しく理解した上で、情報収集や安全対策を行うことが、これまで以上に重要となってきている。

具体的アクション・プランの例

1 リスクの洗い出し・評価

❶ テロや犯罪リスクを洗い出し、それぞれのリスクを評価し、優先的に対策を講じるリスクを決定する。

a. 一般的にリスク評価の尺度は、「リスクが顕在化した場合の影響度」「リスクが発生する頻度」「リスクへの対策状況」などが用いられることが多いことに留意する。

b. 適正なリスク評価を行うには、的確な情報収集と分析が不可欠であり、最近のテロの動向やテロ対策の動向などの把握、的確な対策実施のための現地調査なども必要に応じて行う。

2 テロ対策の構築

❶ 上記リスクの洗い出し・評価を行った後は、具体的なテロ対策を検討し、対策を実行する。

a. テロ対策に向けた体制構築や危機管理マニュアルの策定や既存マニュアルの見直しなどを行う。

b. 海外危機管理において最も困難な判断を迫られる海外拠点からの緊急退避に関して、現地駐在員や帯同家族を急ぎ避難させる事態を念頭に、緊急退避計画を事前に作成することに努める。

3 教育・訓練

❶ 危機管理体制の構築において最も重要なのは、リスクに適切に対応できる人材であることを認識し、危機管理体制の整備や危機管理マニュアルの策定に加え、リスクに対応できる人材の育成、教育、訓練を実施する。

a. テロを想定したシナリオに基づいた訓練（本社および現地の対策本部が情報収集、緊急対策の実施、業務継続のための施策の検討などを模擬体験する訓練）を実施する。

b. 訓練を通じ顕在化した問題点を改善し、いざという時に機能する危機管理体制を構築する。

参考

- 「海外安全ホームページ」外務省
  （http://www.anzen.mofa.go.jp/）
- 「国際テロリズム要覧（Web版）」公安調査庁
  （http://www.moj.go.jp/psia/ITH/index.html）
- 「危機管理対策の心得」警視庁
  （http://www.keishicho.metro.tokyo.jp/kurashi/heion/antep_mpd.files/kikikanritaisaku.pdf）
- 「東京防災」（テロ・武力攻撃については同資料の 164～ 167ページ）東京都
  （http://www.bousai.metro.tokyo.jp/1002147/index.html）
- 「東京 NBC災害対策マニュアル（概要版）」
  （http://www.bousai.metro.tokyo.jp/taisaku/1000061/1000883.html）
- 「国民保護ポータルサイト」内閣官房
  （http://www.kokuminhogo.go.jp/pc-index.html）
- 「米国国務省 /海外渡航情報」
  （https://travel.state.gov/content/passports/en/alertswarnings.html）
- 「英国外務省 /海外渡航情報」
  （https://www.gov.uk/foreign-travel-advice）

9-5 サイバーセキュリティの確保に努める。

基本的心構え・姿勢

情報ネットワーク環境を脅かすサイバー攻撃が年々増加し、その手口も巧妙化し続けている。現在、サイバー攻撃の脅威は世界規模となり、ますます社会経済活動や国民生活に深刻な影響を及ぼすリスクとなっている。

こうした状況の中、企業はサイバーセキュリティが経営に大きな影響を与えるリスクの一つであると認識し、経営者のリーダーシップのもとで必要な経営資源を投入して十分な対策をとることが求められる。また、被害にあうことを想定し、早期の検知や対応・復旧を行う必要がある。

具体的アクション・プランの例

1 サイバーセキュリティ対応方針の策定と管理体制の構築

❶ 経営者がサイバーセキュリティリスクを認識し、対応方針（セキュリティポリシー）を策定し宣言する。

❷ サイバーセキュリティリスク管理体制を、企業活動の全般にわたって、海外拠点・グループ企業を含めて構築し、役割と責任を明確にする。その際に、特定、防衛、検知、対応、復旧の５つの機能を考慮する。

2 サイバーセキュリティのリスクの認識と対策の実施

❶ 守るべき資産やそれに対するサイバー攻撃のリスクを特定し、対策を行う。その上で、それらを見直し、改善・維持する。

❷ サイバーセキュリティに関する脆弱性診断などの外部監査を実施する。

❸ 委託先のサイバーセキュリティ対策を実施および状況把握する。

❹ 経営会議や取締役会での定期的な報告討議を行う。

3 資源確保

❶ サイバーセキュリティリスク対策のための資源（予算、人材など）を確保する。

❷ サイバーセキュリティ人材の育成と、従業員向けセキュリティ研修を行う。

4 情報収集・情報共有

❶ 業界内の情報共有組織などへの加入を検討する。

❷ 各種団体が提供するサイバーセキュリティに関する情報を入手し、必要な対応をとる。

❸ 関係官庁・組織・団体と平時から信頼関係を培い、インシデントの情報共有を促進する。

5 緊急時の対応準備

❶ サイバー攻撃の初動対応手順や緊急連絡体制を整備する。

❷ インシデント発生時に原因解析や影響範囲調査等を行う。インシデント対応の専門組織（CSIRT）を設置する。

❸ 定期的かつ実践的な対応訓練や演習を実施する。

❹ 経営者への報告ルート、各国法定報告義務の内容、市場への公表内容やタイミングなどについて事前に検討する。

参考

- 「高度情報通信ネットワーク社会形成基本法」2000年 12月制定
- 「サイバーセキュリティ基本法」2014年 11月制定
- 「サイバーセキュリティ戦略」2015年 9月
- 「サイバーセキュリティ経営ガイドライン」2015年 12月　経済産業省
  (http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf)
- 「サイバーセキュリティ対策の強化に向けた提言」2015年 2月　経団連
  (http://www.keidanren.or.jp/policy/2015/017.html)
- 「サイバーセキュリティ対策の強化に向けた第二次提言」2016年 1月　経団連
  (http://www.keidanren.or.jp/policy/2016/006.html)

9-6 災害発生時に備えた体制を構築し、対応する。

基本的心構え・姿勢

災害発生時において、企業は、まず「従業員とその家族の安全を確保」し、「事業活動の維持継続・早期復旧」に注力する必要がある。そのため、企業は「BCP」（事業継続計画：Business Continuity Plan）を策定し、それを実効あるものとするべく、定期的に訓練を実施することなどが求められる。

また、被災した地元地域との共生は、地域社会の一員であり地域の従業員や取引先に支えられている企業にとって重要であることから、地域の救援・復旧にできる限り積極的に取り組むことも必要である。

さらに広域かつ甚大な大規模災害に対応するため、個社だけでなくグループ企業や取引先・サプライチェーン、他社・業界団体などのステークホルダーと連携し、社会全体として災害からの被害を最小化することが重要である。

具体的アクション・プランの例

1 平常時からの取り組みで、災害対応能力を向上させる。

❶ 自社が見舞われる可能性のある危機事象（地震、津波、洪水など）を洗い出す。
❷ 災害対策組織を構築する。
❸ 緊急物資の備蓄・確保の体制を整備する。
❹ 帰宅困難者対策を講じる。
❺ 災害発生時の初動マニュアルを策定する。

2 災害に対するBCPを策定し、事業継続の実効性を高める。

❶ 地震、津波、洪水、感染症など各種災害の内容に応じたBCPを策定するとともに、「結果事象型」のBCPも検討する。
❷ 施設の耐震化、災害に強い通信手段の確保など、施設・設備の強化を行う。
❸ クラウド技術、テレワークの推進など、最先端技術を活用する。
❹ 定期的に、課題発見型で実践的な訓練を行い、現場力向上を図る。
❺ 外部機関や国際規格などを参考にした評価を行う、また実際に機能するPDCAサイクルの構築などにより運用体制を確立する。

3 多様なステークホルダーと連携・協力し、業界や社会全体として被害の最小化を図る。

❶ 企業内・グループ内において、災害発生時のコミュニケーション体制を構築するとともに、グループ内横断のBCP体制を検討する。

❷ 業界としてのBCP・BCM（事業継続マネジメント：Business Continuity Management）に関するガイドラインを策定する、また合同訓練の実施など、業界団体主導による備えを充実させる。

❸ 取引先のデータベース化や見える化、取引先とのBCP共有や協定締結によりサプライチェーンの強化を図る。また、自社サプライチェーンを構成する中小規模事業者への支援を行う。

❹ 自治体との災害連携協定を締結する、また「DCP」（地域継続計画：District Continuity Plan）を策定するなど地域などとの連携を行う。

❺ 11月5日の「世界津波の日」などを契機に、津波防災訓練の実施、普及啓発を促進する。また、訓練の実施にあたっては、地域全体での共同訓練の実施も検討する。

「世界津波の日」（11月5日）に関する津波防災訓練
（提供：大成建設）

参考

- 「企業間のBCP/BCM連携の強化に向けて」2014年2月　経団連
  （http://www.keidanren.or.jp/policy/2014/010.html）
- 「企業の事業活動の継続性強化に向けて」2013年2月　経団連
  （http://www.keidanren.or.jp/policy/2013/014.html）
- 「新型インフルエンザ対策に関する提言」2008年　経団連
  （http://www.keidanren.or.jp/japanese/policy/2008/043.html）
- 「企業の地震対策の手引き」2003年7月　経団連
  （www.keidanren.or.jp/japanese/policy/2003/070/tebiki.pdf）
- 「事業継続ガイドライン　ーあらゆる危機的事象を乗り越えるための戦略と対応ー」
  2013年8月　内閣府（防災担当）
  （http://www.bousai.go.jp/kyoiku/kigyou/keizoku/sk_04.html）