一般社団法人 日本DPO協会

2021年3月25日

企業価値を創造する コンプライアンス経営

―情報法コンプライアンスとクライシス・マネジメントを中心として―

関西大学 社会安全学部

教授・博士（法学） 髙野 一彦

企業価値を創造するコンプライアンス経営

1. 法が企業に求めるコンプライアンスと
   内部統制適合的法務

2. 情報に関するリスク

3. 贈賄に関するリスク

4. 企業価値を創造するコンプライアンス

5. Crisis Management（危機管理）

   まとめ

１．

法が企業に求めるコンプライアンスと内部統制適合的法務

内部統制システムの基本となる法制度

会社法

2000年7月　大和銀行株主代表訴訟事件判決

「取締役会はリスク管理の大綱を決定し、代表取締役及び業務担当取締役は、リスク管理体制を具体的に決定する職務 」

2002年4月　神戸製鋼株主代表訴訟事件判決

「大企業の取締役には不正行為防止のための**内部統制システム**を構築すべき法律上の義務がある」

その他、ヤクルト本社株主代表訴訟（2004年12月）など

善管注意義務の一類型として
過去の代表訴訟から定立

2005年6月　会社法　成立

内部統制システムの構築の基本方針の決定、開示が義務化

金融商品取引法

アメリカ

2001年　9.11同時多発テロ
ワールドコム事件
2002年　エンロン事件
2002年　サーバンス・オクスリー法

内部統制システムの構築と有効性の評価に関する報告義務

世界的
な潮流

日本

2006年6月　金融商品取引法　成立

「確認書」、「内部統制報告書」の提出義務

内部統制（Internal Control）
- ✓業務の適正を確保する仕組み（会社法）
- ✓財務報告の信頼性及び適正な開示（金融商品取引法）

内部統制システムの基本となる法制度

	会社法	金融商品取引法（J-SOX）
主目的	**業務の適正を確保するための体制整備** **（＝内部統制システム）**	**財務報告の信頼性の担保** **（＝内部統制報告書の提出と監査の義務化）**
法の要請	**会社法施行規則（2006.2.7）** 1．情報の保存と管理 2．**リスクマネジメント** 3．取締役の業務執行の効率性確保 4．**コンプライアンス** 5．**グループ会社の上記確保の体制** **2014年成立の改正会社法では、グループ管理を法文明記** **2015年 コーポレートガバナンス・コード改訂** **2021年 コーポレートガバナンス・コード改訂（予定）**	1．内部統制報告書の提出 経営者は、財務報告に係る**内部統制の有効性を評価し報告**する。経営者は有価証券報告書記載事項について**確認書を提出**する。 2．外部監査 監査法人は提出された内部統制報告書の有効性を検証する。

その他・・・
公益通報者保護法の受付体制　⇒　間接的な対応体制確立の義務
個人情報保護法の安全管理措置義務　⇒　情報セキュリティーの確立

コーポレート・ガバナンスと内部統制＝OS（基本ソフト）

①親会社自身のコーポレートガバナンス

取締役会の経営監視機能の確立
適法性を確保する仕組みの構築

②子会社のガバナンス

親会社による子会社の意思決定への関与

③内部統制の共通基盤

リスクマネジメント体制、およびコンプライアンス体制の構築

④個別リスク対策（コンプライアンス・プログラム）

個別法ごとのコンプライアンスプログラムの策定と、
グループ横断的な運用

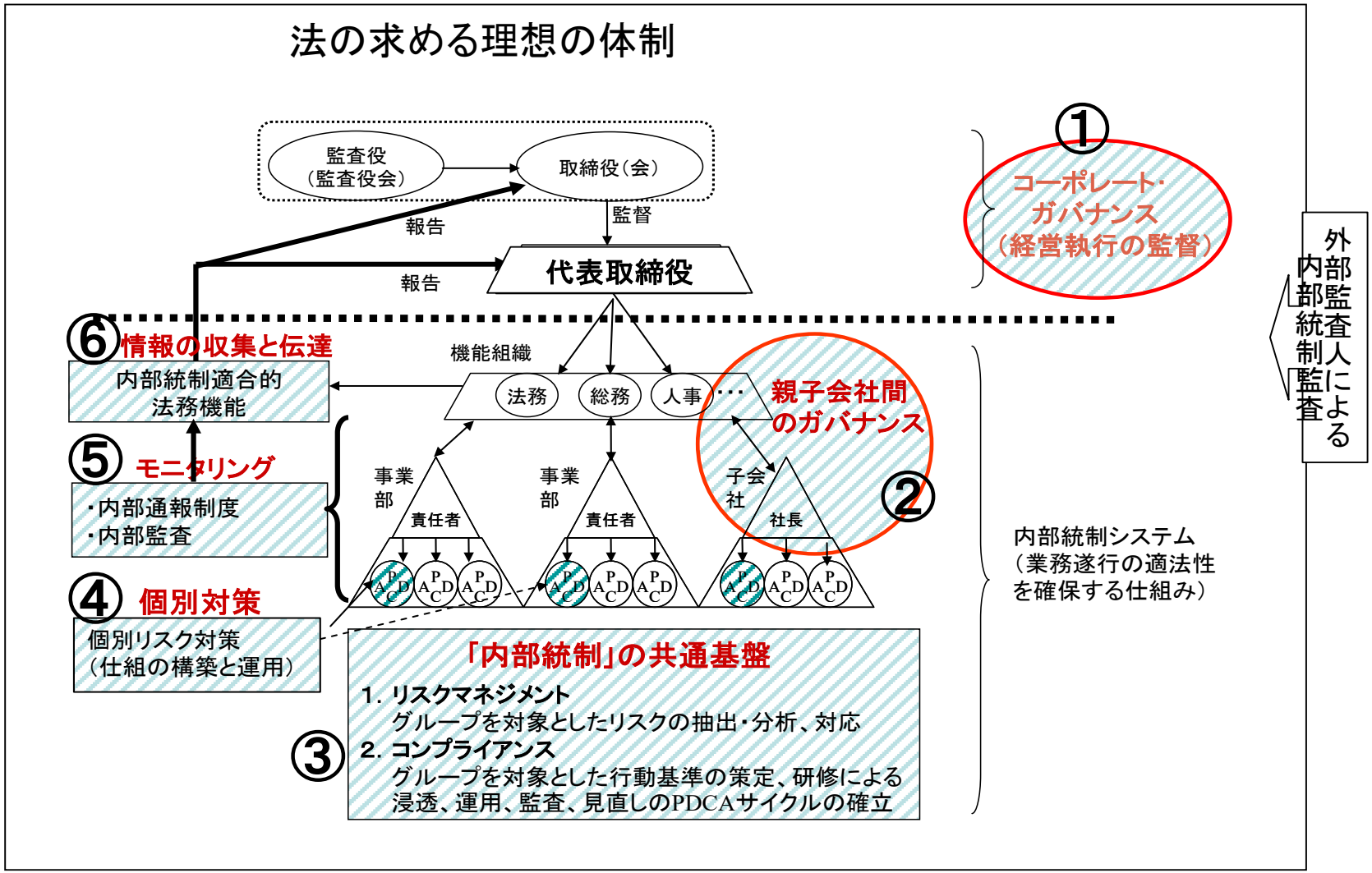
⑤モニタリング

内部通報、内部監査などのモニタリング諸制度
の定立と運用

⑥情報の収集と伝達

グループ全体のネガティブ情報が一元管理され、
定期的に代表取締役・取締役会に報告する仕組み

内部統制システムの全体像

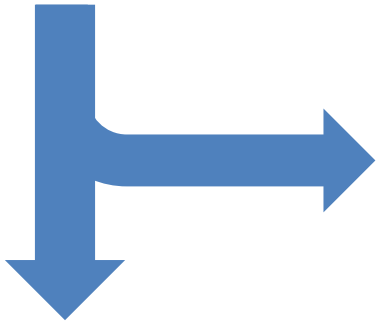


出典：拙著『情報法コンプライアンスと内部統制 第2版』（ファーストプレス、2008）

内部統制システム ≒ コンプライアンス ＋ リスクマネジメント

企業法務論の視座からのコンプライアンス部門の変遷

	法務部門	CSR・コンプライアンス部門
1980年代	総務部文書課から 法務部が独立	
1990年代	臨床法務→予防法務	1990年代　環境・社会貢献部門の新設
2000年初頭	予防法務→戦略法務	2002年　経団連「企業行動憲章」CSR元年 企業倫理部門、CSR部門の新設
		2005年　会社法成立 多くの会社で、法務部から コンプライアンス部門が独立
		2015年　国連サミット・SDGs採択
		現在　サステナビリティ推進部に改組し、 経営戦略に関与（C製薬、K電力など）



出典：1965年から5年ごとに経営法友会が実施している「会社法務部実態調査」、及びBERC法令部会の研究報告などをもとに著者作成

コンプライアンス＝経営のマネジメントシステムであり、企業価値創造のエンジン

近年の企業不祥事・事故の傾向

1. 情報に関する事件・事案
   情報流出事件　⇒　教育B社事件（2014年）、日本N機構事件（2015年）・・・
   利活用の事案　⇒　就職情報サイトの情報提供事案（2019年）、交通系カード事案（2013年）

2. 外国法の域外適用
   FCPAの摘発強化
   2016年　精密O社事件、FCPA違反で約740億円の罰金
   2018年　電機P社事件、同309億円の罰金
   GDPRの発効
   2019年1月、フランスCNILは検索G社に5千万€(約62億円)の制裁金
   2019年7月、イギリスICOはホテルM社に9920万£(約135億円)の制裁金

3. 子会社、協力会社などの取引先が直接の原因だが、グループのクライシスとして親会社が対応するケースが散見される。

コンプライアンス経営の課題

1. 風通しの良い社風づくり
   親会社＞子会社＞協力会社、経営層＞現場　の温度差の解消

2. 危機に強い会社づくり
   事故・不祥事が発覚した時の迅速なクライシス対応体制の整備

2.
情報に関するリスク

情報に関する事件

2004年　インターネットY社 顧客情報流出事件　460万件（内部者の窃取）

2006年　行政機関 「秘」扱い情報流出事件（ウイニー）

2007年　印刷D社　個人情報流出事件　863万件（委託先社員の窃取）

2007年　自動車部品D社　技術データ流出事件　13万点の図面（従業員の窃取）

2009年　生命保険A社　顧客情報漏えい事件　13万件（委託先からの流出？）

2011年　電機S社子会社　7000万人を超える個人情報が流出（ハッキング）

2012年　鉄鋼S社　営業秘密の不正取得でポスコなどを提訴（元従業員）

2013年　鉄道J社　乗降履歴データの第三者提供

2014年　出版B社　顧客情報流出事件（委託先社員の窃取）

2017年　チケット販売P社　カード情報等流出、630万円分の不正利用発覚

2019年　就職情報サイト運営R社　内定辞退をAIで予測し他社に販売

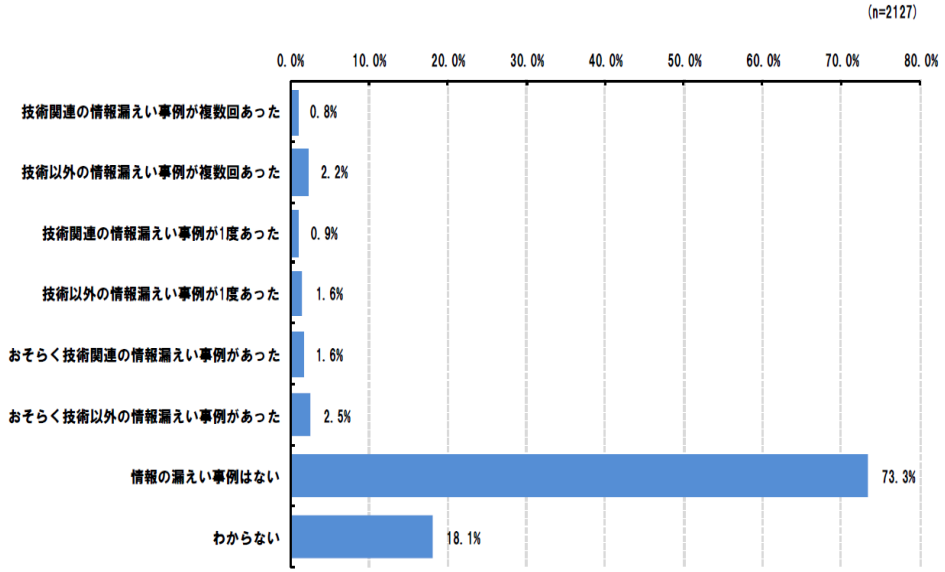
✓ 大きな事件は、内部者による情報の不正取得が目立つ
✓ 最近は積極的な情報の利活用の結果、炎上する事件が散見される

情報流出の発生頻度

営業秘密の流出

過去5年間で営業秘密の漏えいが
「あった」と回答した企業は8.6%

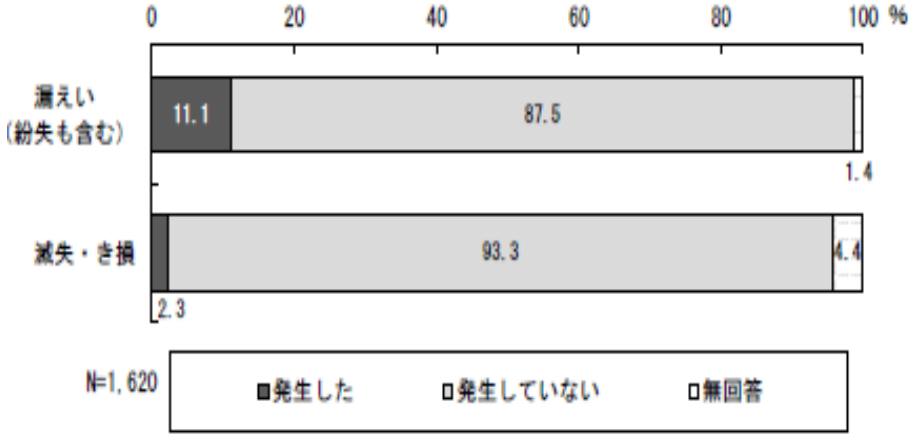
中途退職（正規社員）による漏えい24.8%
取引先・共同研究先による漏えい：11.4%



出典：　情報処理推進機構「企業における営業秘密管理に関する実態調査」（2017年）

個人情報の流出

個人情報の漏えい（含む紛失）が
「あった」と答えた事業者は11.1%



出典：個人情報保護委員会「個人情報の保護に関する事業者の取組実態調査」（2018年）

「情報流出」は、他のリスクに比べて、発生頻度が極めて高い

情報漏えいとリスク

個人情報漏えいと損害
①訴訟リスク　＝　本人のプライバシー侵害
②罰則リスク　＝　個人情報保護法違反
③損害賠償リスク　＝　契約違反により取引先より請求
③株主代表訴訟リスク　＝　管理体制の不備による損害
④その他　＝　被害者への補償、業務ストップ、信用喪失など

近年の情報漏えい事件
Y社　＝　450万人顧客情報流出（2004）⇒　損失29億円
A社　＝　13万件顧客情報流出（2009）⇒　損失69億円
B社　＝　3504万件（2014）　⇒　特別損失約260億円を計上

損失額：Y社は経産省資料、A社・B社は報道による

大きな損害＝『情報セキュリティー』は経営上の重要マター

法的制裁

	法律名	禁止行為
刑事	刑法	窃盗 業務上横領 背任など
	不正競争防止法	営業秘密侵害罪
	不正アクセス 禁止法	不正アクセス行為
	電気通信事業法、 電波法など	通信事業者による 通信の秘密の侵害
	秘密保持法	職務上の秘密の漏示 (公務員,弁護士など)
民事	民法	不法行為
	不正競争防止法	営業秘密の不正取得

個人情報保護法、プライバシー権など

※ただしケースの行為時は、2003年成立の個人情報保護法が適用されます。

不正競争防止法

「不正競争防止法」による、「営業秘密」の保護

差止請求権、損害賠償請求権、信用回復措置請求権

「営業秘密」の概念

①秘密管理性：	秘密として管理している
②有用性：	経済的に有用な情報であること
③非公知性：	公に知られていない情報であること

争点は、「秘密管理性」

秘密管理措置

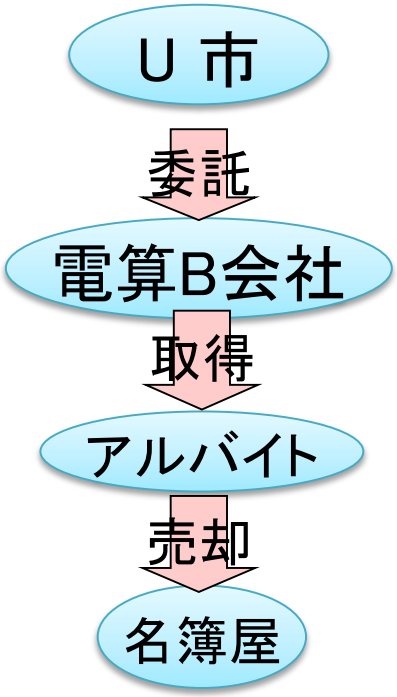
①秘密管理意思	⇒	営業秘密が一般の情報と区分されている
②認識可能性	⇒	営業秘密であることを明らかにしている

出典：営業秘密管理指針　（2015年1月28日全部改訂）

営業秘密の秘密管理性が争点になった81 件の裁判で、秘密管理性を認めた判例は23 件（28.4%）。「営業秘密管理指針」2010、8頁

2015年、経済産業省「営業秘密管理指針」の改訂

京都府 U 市住民基本台帳データ流出事件



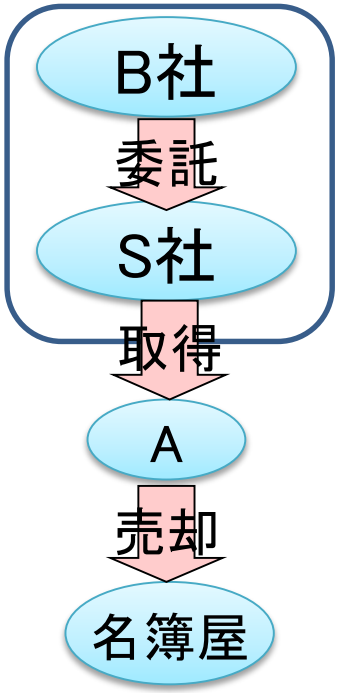
1999年5月
U市の住民基本台帳データ約22万人分が流出した事件。
U市がメンテナンスを委託していた電算業者の下請会社B社のアルバイト大学院生が、児童検診用データを自身が所有する光磁気ディスク（MO）にコピーして持ち出し、インターネット上で名簿業者に売却、約23万円の利益を得ていた。

刑事：
アルバイト大学院生は不起訴処分。
現行刑法では、自己所有のMOへデータをコピーしても、データが財物でないため不可罰となった。また同市個人情報保護条例にも該当の処罰規定なし。

民事：
3人の住民がU市を提訴。使用者責任に基づきU市の賠償義務を認めた
慰謝料1人1万円、弁護士費用各5千円と遅延損害金

2003年の改正不正競争防止法に、営業秘密侵害罪を加入

教育B社　顧客情報流出事件



2014年6月末

顧客からの問い合わせで、顧客情報流出の疑いが浮上。
⇒社内調査の結果、3504万件の個人情報流出を確認。

2014年7月

情報処理を委託していた100%子会社S社に常駐していた、
システムエンジニアAが、事件発覚から約2週間後に
不正競争防止法違反（営業秘密侵害罪）容疑で
異例のスピード逮捕
⇒　アクセス制限・客観的認識可能性の証明

2015年3月

260億円の特別損失を計上、1995年の上場以来初めての赤字

B社は、情報セキュリティーへの莫大な投資を行い、また個人情報保護にも
極めて積極的に取組んでおり、先進企業として学会でも認知されていた。

悪意を持った者の持ち出し行為は情報技術上、予防は困難
→　流出時の「被害拡大防止」の対策をとれるかどうかが重要

改正個人情報保護法

2015年改正　個人情報データベース等不正提供罪の新設

改正個人情報保護法 第83条
個人情報取扱事業者（略） 若しくはその従業員又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、1年以下の懲役又は50万円以下の罰金に処する。

2020年改正　個人情報データベース等不正提供罪

法人に対しては、罰金刑の最高額を、1億円以下に引き上げる（法人重科）
ただし行政制裁は継続的な検討課題とした。

参考：不正競争防止法の営業秘密侵害罪の罰則

① 個人：懲役10年以下、罰金2000万円以下（海外3000万円）、犯罪収益没収
② 法人：5億円以下（海外重罰10億円）、犯罪収益没収
③ 二次取得者以降も処罰対象

どのような情報管理を行えば良いか？

1. 社内の情報を棚卸し、重要な情報とそうでない情報に峻別
2. 重要な情報は、「営業秘密」としての法的な保護をうけられるような管理を行う。

秘密管理措置

①営業秘密が一般情報から合理的に区分されていること

②当該情報について営業秘密であることを明らかにする措置

3. グループ横断的な責任者（CIO又はCPO）と専任管轄部署を設置し、

①従業員教育

②秘密保持契約、競業避止義務契約の締結

③従業者の監視（内部通報、業務監査、メールモニタリングなど）

④見直し、

のPDCAサイクル（Plan/Do/Check/Action）を運用する

重要な情報は「法的保護」を受けられるような管理を行う

2020年6月5日成立　改正個人情報保護法の論点

個人情報保護法 附則第12条の規定、「3年ごと見直し」に基づく2020年改正

1. 個人情報に関する個人の権利の在り方
   目的外利用、不正な手段による取得等に限定されていた利用停止等（利用の停止又は消去）の無限定化の検討
2. 漏えい報告の在り方
   個人情報の漏えい報告は、わが国では法的な義務ではないが、GDPRでは「データ侵害通知」として72時間以内の監督機関への報告が義務
3. 個人情報保護のための事業者における自主的な取組を促す仕組みの在り方
   個人データ取扱責任者の設置、PIAなど
4. データ利活用に関する施策の在り方
   匿名加工情報の利活用を促す、利用しやすい制度の検討
5. ペナルティの在り方
   罰金額を上げるべきか、課徴金を導入すべきか検討
6. 法の域外適用の在り方及び国際的制度調和への取組と越境移転の在り方など

2020年6月5日成立　個人情報の保護に関する法律等の一部を改正する法律（概要）　出所：個人情報保護委員会

■ 平成27年改正個人情報保護法に設けられた「**いわゆる３年ごと見直し**」に関する規定（附則第12条）に基づき、個人情報保護委員会において、関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施。

■ 自身の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点から、**今般、個人情報保護法の改正を行い、以下の措置を講ずる**こととしたもの。

改正法の内容

１．個人の権利の在り方

- **利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和**する。
- **保有個人データの開示方法**（※）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

（※）現行は、原則として、書面の交付による方法とされている。

- 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。
- ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

２．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。

- **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

３．事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、**企業の特定分野（部門）を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

４．データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した「**仮名加工情報**」を創設し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。
- 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

５．ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

（※）命令違反：6月以下の懲役又は30万円以下の罰金
→ 1年以下の懲役又は100万円以下の罰金
虚偽報告等：30万円以下の罰金 → 50万円以下の罰金

- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**（法人重科）。

（※）個人と同額の罰金（50万円又は30万円以下の罰金）→ 1億円以下の罰金

６．法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。
- 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

※　その他、本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

補足　欧州司法裁判所のSchremsII 事件Judgmentの概要

2020年7月16日、欧州司法裁判所は、SchremsII事件においてEU-US Privacy Shieldは無効と判断

✓国家安全保障目的で米国が運用する監視プログラムは、EU域内から移転される個人データに対しても実施される可能性があるため、EU-US Privacy Shieldは、EU基本権憲章で保障されている個人データの本人の基本権（私的生活・家庭生活および個人データの保護）を侵害する

✓EU-US Privacy Shieldにおけるオンブズパーソンは、その独立性と米国諜報機関の命令権による拘束から考えると、EU法と同等の法的救済を保障していない

2019年 日・UEデータ保護の十分性の相互承認 ⇒ 2021年に見直し

2021年の個人情報保護法改正

※ 論点は、国際的整合、行政機関法等との合体、条例2000問題

3.
贈賄に関するリスク

ゴムB社事件

2004年～2007年の間、B社は国営企業との関係を構築していたエージェントを通じて、国営企業の職員に取引総額の一定割合の支払いを行った。
B社は、現地エージェントに対して、国営企業の職員へ支払う金額（合計約1億5000万円）を上乗せして、販売手数料を支払っていた。

2007年、B社の担当部長は米FCPA違反等により逮捕、翌年懲役2年の実刑及び8万ドルの罰金が科せられた。
2011年9月15日、B社は米司法省と2800万ドルの支払いで和解した。その後、同社は司法省の調査に全面的に協力すること、大規模なコンプライアンス体制の改善を行うことなどとし、和解金が減額された。

精密O社事件

O社は、米子会社などを通じて、中南米の複数の国・公営病院の職員らに対し、機材購入を目的とした賄賂を渡していた。
2016年3月、O社は、米司法省と罰金・和解金として計6億4600万ドル（約736億円）を支払う合意をした。

2016年3月3日朝日新聞朝刊「罰金など736億円支払いへ（略）」

アメリカ海外汚職行為法（FCPA）の概要

アメリカ海外汚職行為法（The Foreign Corrupt Practice Act）の中の
「外国公務員贈賄禁止条項」（法78条DD-1～3）

主体：　1．NYSE、NASDAQの上場会社等
2．アメリカ市民・居住者等、アメリカに主たる事務所を有する会社等
とその役員、従業員、代理人等
3．アメリカ国内の通信手段を用いて贈賄行為を行ったもの

禁止：　1．外国公務員、政党・政党職員、候補者等に対して
①職務執行に影響を与える、②職務違背行為を誘導する、
③不正利益を供与する、④あっせんをさせる、ことを目的として
金銭の申し出、支払い、その約束などを行う行為。
2．エージェントなどの仲介者に対して、前項の行為をさせ（又は誘導する）

例外：　「ファシリテーション・ペイメント」
日常的な政府活動の履行などを目的とした少額の金銭の支払いは適用外

「FCPAに関する当局の摘発・訴追姿勢は、かなり強気である。SECとFBIが、FCPAに特化した専門組織を設置」している。（出典：外国公務員贈賄規制法制に関する海外動向調査、35頁）

訴追件数（司法省・SEC 総計）、2005年 12件、2007年 38件、2009年 51件、2010年 56件・・ 年120～200件の調査

参考：　FCPAガイドライン「A Resource Guide to the U.S. Foreign Corrupt Practices Act」

参考：連邦量刑ガイドライン

（1）犯罪の予防、または発見のための**規準と手続の規定**

（2）（A）組織を支配する権限を有するもの（取締役会など）は、法令遵守と企業倫理プログラムの内容と運用を熟知し、また運用と効果を確認すること。

（B）組織の上級幹部の者が、その組織はこのガイドラインに沿って、効果的な法令遵守と企業倫理プログラムを持っていることを確実にする。特定の上級幹部の者が、**法令遵守と企業倫理プログラムの総合的な責任者**として任命されていること。

（C）その責任者は、法令遵守と企業倫理プログラムの日々の運用責任を負う。その責任者は定期的に、また適切に、組織の上級幹部、執行役、または事業部長などに報告すること。またその責任者は、運用責任を果たすために、予算、適切な権限、取締役会などに直接コンタクトをとる機会を与えられなくてはならない。

（3）組織は、犯罪、その他法令遵守と企業倫理に反する行為に関与した者が、組織の実質的な権限を与えられることのないよう、合理的な努力をすること。

（4）（A）組織は、法令遵守と企業倫理プログラムに関する従業者の役割と責任に関する情報伝達の実質的な手順と方法により、定期的に周知する合理的なステップをとらなければならない。**全役職員に法令遵守規準や手続に関する情報を効果的に周知徹底**すること

（B）上記（A）は、上級幹部、執行役、事業部長、従業者に対して行い、適切な場合はエージェントに対しても行う。

（5）組織は次の合理的なステップを踏まなければならない。

（A）**モニタリングと監査**によって、法令遵守と企業倫理プログラムを確かなものにする。

（B）法令遵守と企業倫理プログラムの効果を**定期的に評価**する。

（C）従業者またはエージェントが、実際の犯罪またはその可能性について通報するシステムで、**通報者に報復などが及ぶおそれのない、匿名または秘密保持のためのメカニズム**を有したものを持つこと。

（6）法令遵守と企業倫理プログラムは、それが機能するためのインセンティブを有し、そして違反した者および法令違反を発見できなかった者に対する処分を規定し、継続的な強制力をもたせること。

（7）犯罪が発見されたとき、組織は適切に処置し、また違反行為の再発防止のために**法令遵守と企業倫理プログラムを修正**するなどの適切な措置をとること。

(1)文書化（可視化）、(2)(3)組織・権限の明確化、(4)従業者の教育・訓練、(5)(A)および(B)監査、(5)(C)内部通報、さらに(7)継続的改善

罰金額が400%～5%の間で変動

イギリス贈賄法 （Bribery Act 2010）

2010年、それまでの贈賄防止3法を廃止し、外国公務員に対する贈賄罪、商業組織の贈賄防止策懈怠罪を加えて、包括的な贈収賄罪を新設。
2011年7月1日発効。
※内容は米国FCPAに比べ、以下に特長がある。

第1条　贈賄罪
人が他人に対して、職務行為を不適切に遂行させることを意図し、金銭上その他の利益の提供を供与等する行為

特長1：公務員に限定されず、一般の私人も対象となる。

特長2：「職務行為の不適切な遂行」の判断基準とは、「イギリスの合理的な一般人ならば同様の職務を遂行する上で、「誠実性」「公平性」「信頼性」が期待されており、これを裏切る行為の誘導を意図する利益の提供を「贈賄」と定義

例：　私立病院の職員への贈賄なども対象となる
（ただし現在のところ摘発事例はない）

イギリス贈賄法（Bribery Act）の概要

第7条　贈賄防止策懈怠罪
会社の関係者（役員、従業員、エージェント、子会社など）が贈賄行為を行った場合、防止のための「適正な手続」を立証できなければ、会社に本条が適用される。（法人罰）

特長3：　贈賄防止懈怠罪：

行為者による贈賄行為が発生したとき、企業が贈賄行為を防止する「適正な手続き」を実施していなければ、自動的に可罰される可能性がある

「Bribery Act 2010 Guidance」（2011年3月30日）

1. 経営者によるコミットメント
2. 定期的なリスク評価の実施と文書化
3. 関係者※1の調査
4. 関係者※1への研修による周知
5. モニタリング（関係者の監視）
6. モニタリングに基づく改善

「贈賄防止策懈怠罪」の抗弁

※1関係者＝当社役員、従業員、エージェント、子会社など

アメリカFCPA・イギリスBribery Actへの企業の対策

アメリカ「A Resource Guide to the U.S. FCPA」、イギリスの「Bribery Act 2010 Guidance」の要素を加味した、コンプライアンス・プログラムの策定と運用

1. 経営者による宣言	贈賄行為を行わない旨の意思表示
2. 責任者、専管部署	コンプライアンス・プログラムの定立と運用、 事業を展開する諸国の法制度の確認と報告など
3. リスク・アセスメント	グループ、エージェント等の関係者を含めて評価
4. ルールの策定　企業グループ行動基準への明記⇒ガイドラインの策定	
5. 運用	役員・従業員、子会社、エージェントなどへの研修 （特にアメリカは教育訓練プログラムの整備と実施を重要視） エージェントなどとの契約に贈賄禁止条項を加入
6. モニタリング	内部通報、業務監査、取引先アンケートなど
7. 改善	定期的な経営トップ等への報告と指示に基づく改善
8. クライシス対応　発生時の	報告、調査、処罰、などの一連のクライシス 対応ルールの整備と運用

※2019年3月のFCPAガイドライン改定により、①経営陣の関与、②顕著な利益、③社内蔓延、④常習性等がなければ、量刑ガイドラインの罰金50%軽減。　事後的でも協力すれば25%軽減。

贈賄予防は然ることながら、訴追時に、法人としての違法性を阻却し、又は罰金額を抑えるためのマネジメント・システム

４.
企業価値を創造する
コンプライアンス

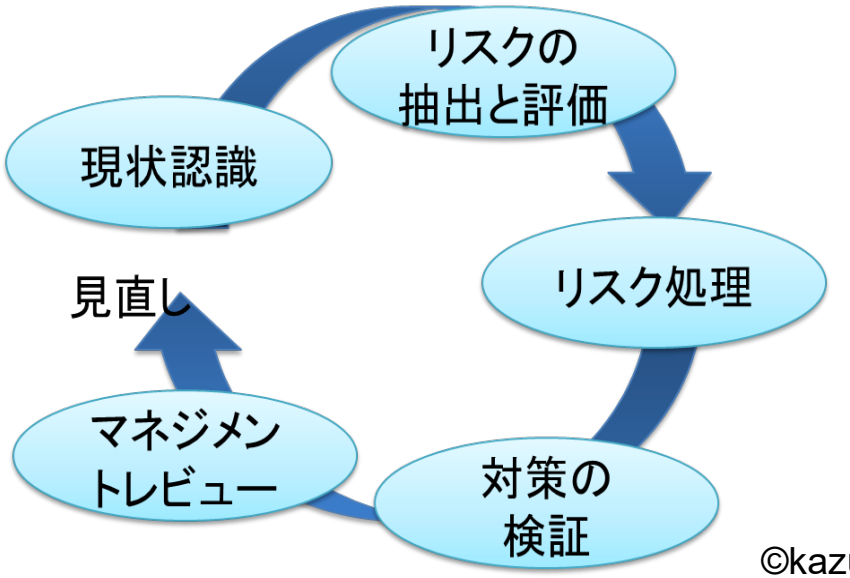
リスクマネジメントとは

リスクの顕在化を抑えつつ、企業を持続的に成長させることが、経営の目的である「株主価値の増進」に寄与　⇒　リスクマネジメントは経営者の役割

リスクマネジメントの定義

企業を取り巻く様々なリスクを予見し、①そのリスクがもたらす損失を予防するための対策、②不幸にして損害が発生した場合の事後処理対策等を、効果的・効率的に講じることによって、事業の継続・安定的発展を確保していく企業経営上の手法

引用：インターリスク総研『実践リスクマネジメント―事例に学ぶ企業リスクのすべて―』経済法令研究会、2002年）



2016年　電機S社の事例

2007年三重県中部地震（M 5.4）で震度5強、亀山工場（液晶パネル）に被害なし。

大阪・堺泉北コンビナート建設に際し、過剰な安全投資　（1兆円超）を行った結果、経営破綻し、外国企業の傘下に。

河田惠昭「平成30年の4連続災害とBCP」2018年、2頁

限られた経営資源（人・もの・金）を、有効にRM投資を行うため、重要リスクを選定する。

リスクの種類と対策

	経済的リスク（取引先の倒産等）	人的リスク（労災等）	物的リスク（地震等）	社会的リスク（戦争等）	法的リスク（法令違反・違法行為等）
リスクファイナンス	貸倒れ引当金の計上等	労災保険等	地震保険・火災保険等	予防不可能 ・クライシスマネジメントに特化	予防不可能 ・保険の免責要件 ・引当金計上不可能
リスクコントロール	与信管理 契約上の転嫁	コンプライアンス・プログラム	契約上の転嫁		コンプライアンス・プログラム
クライシスマネジメント	債権管理 クライシスマネジメント	コンプライアンス・プログラム クライシスマネジメント	クライシスマネジメント	クライシスマネジメント	コンプライアンス・プログラム クライシスマネジメント

コンプライアンス・プログラム

1. グループ横断的な責任者、専任管轄部署の設置
   リスクアセスメントにより重要リスクの選定と、グループ横断的に
   重要リスクを主管する責任者、専任管轄部署の設置

2. 規程策定
   重要なリスクについて、規程・ガイドライン等のルールを策定

3. 役員・従業者教育
   対象は当社の役員・従業者、エージェント、子会社など広く実施

4. 運用とモニタリング
   ネガティブな情報を収集する仕組み
   内部通報ライン、コンプライアンス監査、従業者・取引先アンケートなど

5. 経営者への報告と改善

6. 情報公開
   重要リスクは有価証券報告書の「事業等のリスク」・四半期報告で開示
   CSRレポート等で任意に開示

コンプライアンス・プログラムの設計・運用上のポイント

1. マネジメント・システムへの発想の転換

「コンプライアンス＝法令遵守」は間違い

「コンプライアンス・プログラム＝法的リスクのマネジメント・システム」であり、
「コンプライアンス＝企業価値創造のエンジン」

2. コンプライアンス・プログラムの効果

（1）企業防衛の視点からの運用

✓発生時の損失最小化

クライシス発生時に法人としての違法性の阻却、罰金・課徴金の減額、又は損失の低減を目的としたコンプライアンス・プログラムの運用とエビデンスの収集

※概ね、国内＝レピュテーション、海外＝罰金・制裁金、損害賠償

✓抑止効果

経営者による宣言、規程などのルールの整備、従業員研修、モニタリングなど、一連のPDCAサイクルを回すことにより、従業員のリスク感度を高め、発生を抑止する。

（2）迅速なクライシス・マネジメント

経営者による事件・事故などの「ネガティブ情報」の収集と迅速な対応が損失を極小化

GDPR データ侵害通知（31条1項、32条）＝72時間以内の報告等

「風通しの良い社風」をどうのように作るのか？

親会社＞子会社＞協力会社の温度差

親会社と子会社・協力会社が「理念」や「価値観」を共有する取組み

経営層＞現場　の温度差

経営層と現場が「理念」や「価値観」を共有する取組み

例：電力K社 「CSRキャラバン」 取締役は2016年までの5年間で約260回の現場訪問
ガイシN社 「CSRトークライブ」 日本ガイシ・グループ会社従業員との双方向コミュニケーションイベント、2017年度は9回実施
ウィッグA社　国内・海外に多店舗展開をしており、経営陣が現場を訪問することは不可能
⇒スーパーバイザー制度：経営指導とクレド・価値観の共有を行う専門職、など

「風通しの良い社風」の醸成１

理念や価値観を共有する継続的な取組み

ビデオ会議システムによる価値観の共有→コロナ禍で生まれた新たな可能性

「風通しの良い社風」をどうのように作るのか？

心理的安全性（psychological safety）
⇒人間関係において安全であるというチーム共通の信念

Amy Edmondson（1999）, *Psychological Safety and Learning Behavior in Work Teams*, Administrative Science Quarterly, Vol. 44, No. 2, pp. 350-383

働きがいのある会社ベスト100（Fortune） Google社は2014～2017で1位

「Project Oxygen」（2009年）
⇒マネージャーの役割と仕事に関する調査プロジェクト

「Project Aristotles」（2012年～）
⇒生産性の高いチームの特性を明らかにするプロジェクト

心理的安全性の確保＝自分が自分らしく働ける環境、自己認識・自己開示・自己表現ができる場を作ること ⇒ 組織効率の向上

参考：ピョートル・フェリクス・グジバチ「世界最高のチームーグーグル流「最少の人数」で「最大の成果」を生み出す方法ー」朝日新聞出版、2018年

「風通しの良い社風」の醸成2

働く人が「ありのままの自分」でいられる職場作りは、企業価値の持続的向上を経営の目的としている経営者・経営幹部にとって、「役割」そのもの

コロナ禍で見えてきたビデオ会議システムの可能性

1. ビデオ会議システムによる従業員教育

　　会社・事業所の垣根を越えた従業員研修（exグループ各者の部長研修）

2. ビデオ会議システムによる価値観の共有

　　経営層研修（ex世界各国の子会社役員の研修、クライシス・トレーニング）

　　経営者によるCSRキャラバン、買収した企業の同質化など

⇩

ビデオ会議システムによる遠隔研修・コミュニケーションを採り入れることで、移動を伴わず、均質な従業員教育、価値観共有活動を行うことができる

⇩

組織としての帰属意識を醸成するため、オンライン教育のみならず、定期的なリアル集合研修を組み合わせて、「ハイブリッド」なカリキュラムに

企業でのビデオ会議システム、その他の可能性

✓取締役会　＝　海外在住者、障がい者などの社外役員の選任が可能に

✓緊急危機対策本部　＝　ネット接続ができれば集合しなくとも開催可能

✓ビデオ・カウンセリング　＝　顧客とのカウンセリングのオンライン化、など

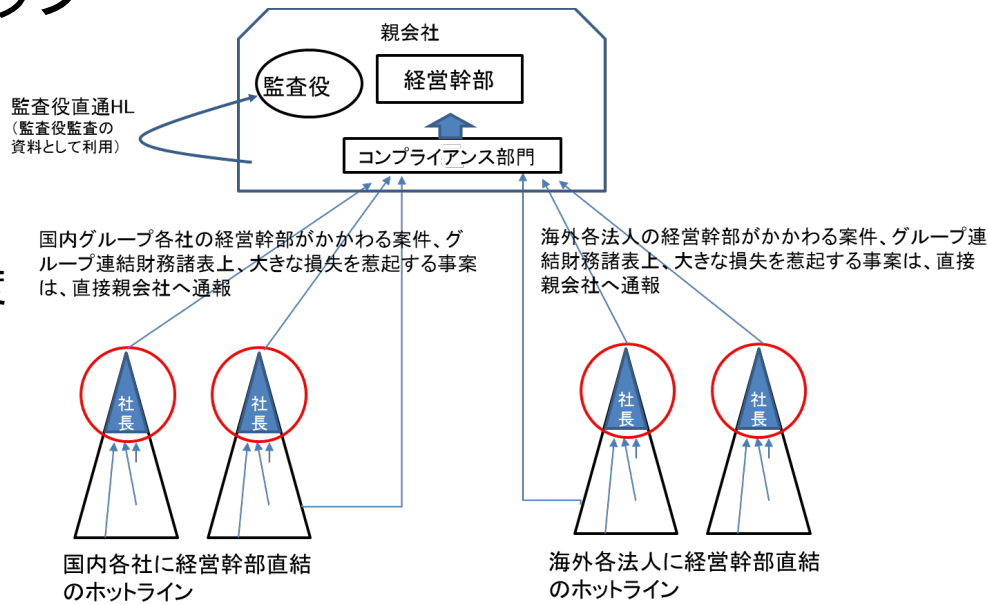
「危機に強い会社」をどうのように作るのか？

3．内部通報制度をブラッシュアップ

「内部告発」ではなく「内部通報」

✓子会社・協力会社、取引先、OB・OG
　など、広めに通報を受け付ける通報制度
✓通報者が通報をためらわない匿名通報制度
✓経営者の問題を通報するラインの設置など

例：食品A社：経年での通報制度の有効性調査
　　教育B社、機械E社：「監査役直通HL」など



4．クライシス・マネジメント

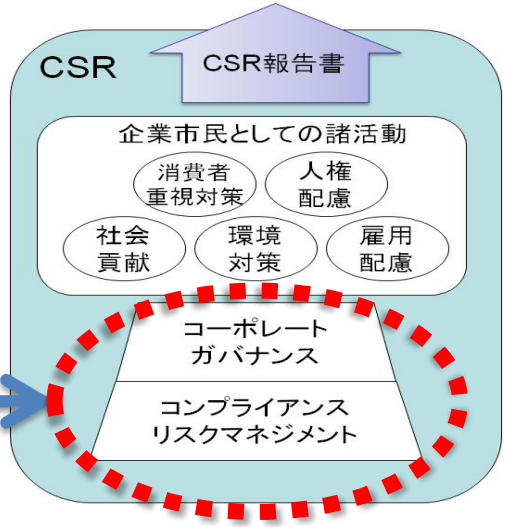
経営者を対象に、クライシス発生を想定したトレーニングを定期的に行う。
　例：製鉄N社、教育B社、衣料G社などのクライシストレーニング、電力K社のシビアアクシデント
　　トレーニング、鉄道J社のシナリオ非提示型訓練など、経営者を対象としたトレーニング

クライシス発生時の対応すべき事項をまとめた「チェックリスト」
　例：化学A社グループ「危機管理ハンドブック」、鉄道J社「危機対応チェックリスト」など

コンプライアンスと企業価値

CSR経営の基盤としてのコーポレートガバナンスと内部統制システムの確立

Dow Jones、Ethibel等の評価会社による評価



Dow Jones Sustainability Indexes
Powered by Dow Jones Indexes, STOXX Ltd. and SAM

Sustainability Assessment Questionnaire（質問書）の構成

Economic dimension ： 32問
Environmental dimension： 31問
Social dimension： 36問

→ コーポレートガバナンス
リスクマネジメント
コンプライアンス

日本における2020年3月末のESG投資残高は、
2兆180億ドル（約310兆円）
出典：日本サステナブル投資フォーラム(JSIF)

比較：アメリカ：11兆9千9百億ドル(約1250兆円)
※2018年、全投資の25.7% 出典：田村怜・石本琢「ESG投資の動向と課題」2020年

→ 企業価値向上の経営目的に合致

Crisis Management（危機管理）

エスカレーションルール

迅速に事故情報が企業グループ経営トップに報告される仕組みづくり

1. 事件が発生したら、エスカレーションルールに基づき、報告する。

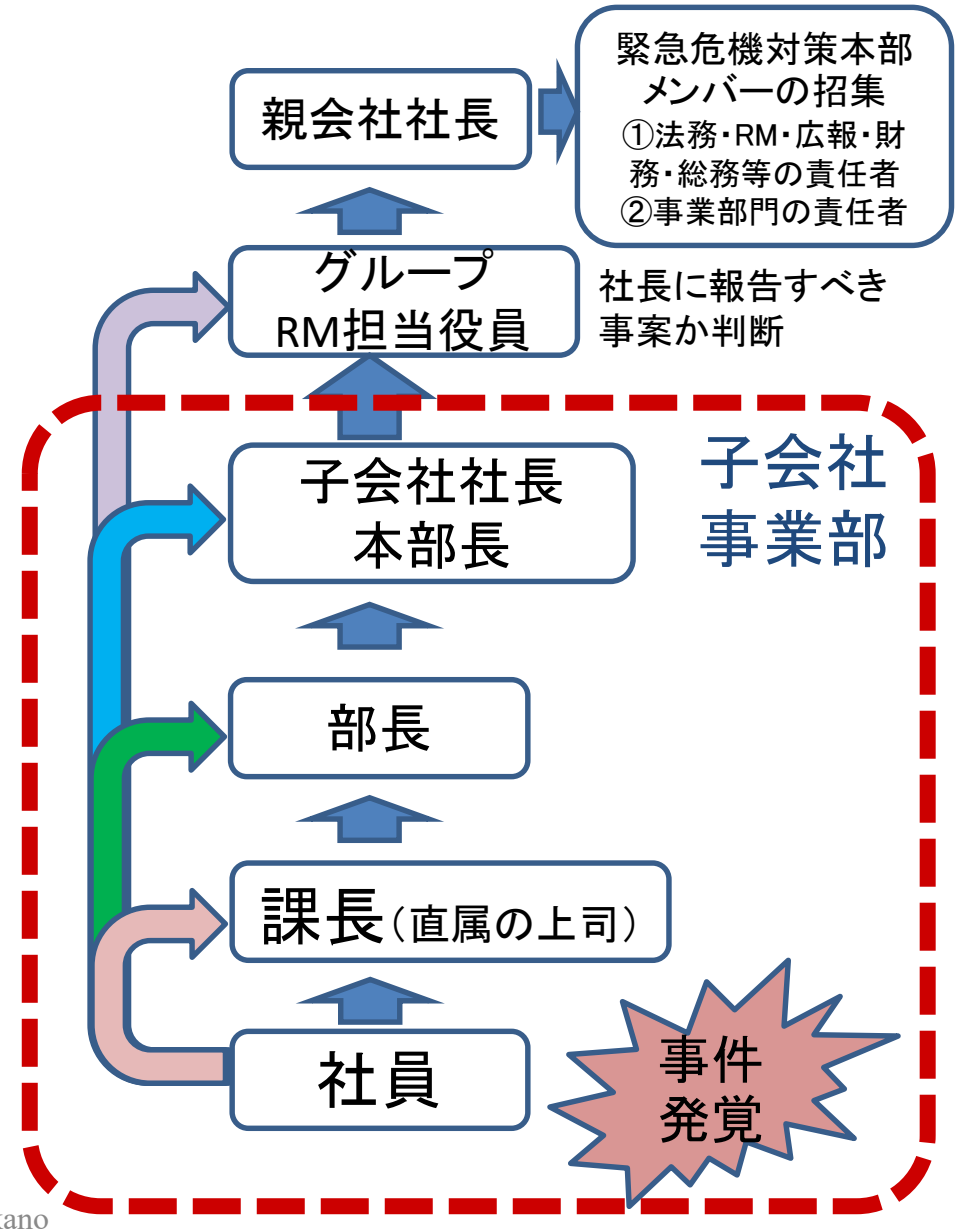
   ✓まず上司に報告
   ✓上司が不在の場合は、その上の上司に報告
   ✓その上の上司が不在の場合は、さらに上の上司に報告

2. 経営トップには、事件発生から24時間以内に報告を行う。

3. 事件かどうか、また重大な案件かどうか迷う場合も、まず報告する。

4. 報告したことは責めず、報告しなかったことを譴責する。

5. 不正案件で上司が関わっている場合は、内部通報ラインに報告。



危機管理体制のチェックポイント

1. 事前対策

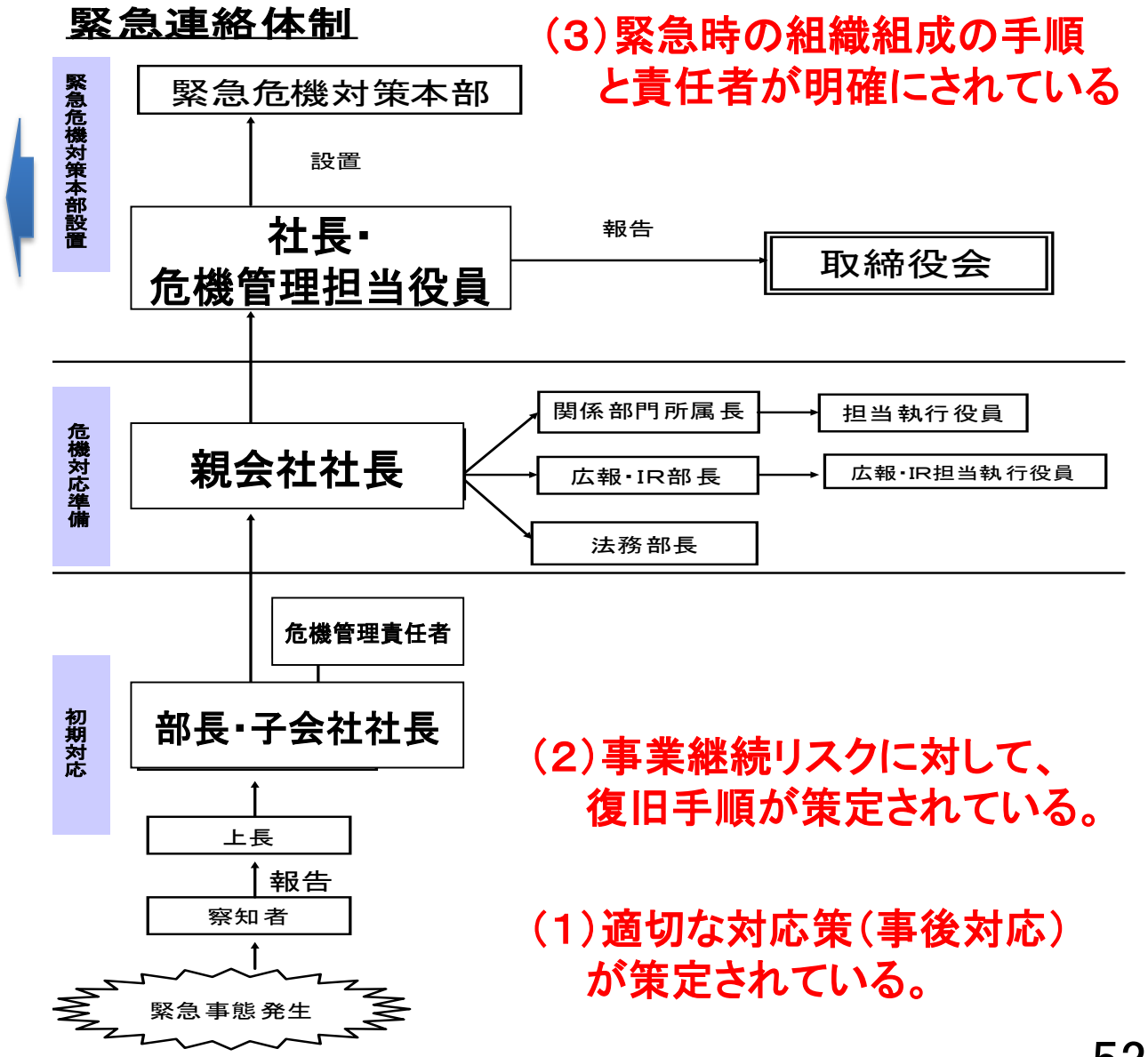
①グループ・RM基本方針
グループとして対応する
事象と方針の決定

②クライシス対応規程
事業継続計画の策定

2. 事後対応（対策本部）

①情報収集
②基本方針の表明
③個別対応

・顧客対応（被害者対応）
・従業員対応
・施設対応
・株主対応
・取引先対応
・行政対応
・マスコミ対応
：



（3）緊急時の組織組成の手順
と責任者が明確にされている

（2）事業継続リスクに対して、
復旧手順が策定されている。

（1）適切な対応策（事後対応）
が策定されている。

クライシス・シミュレーション・トレーニング

社長をはじめとした取締役・監査役のトレーニング（子会社も参加）

テーマ：個人情報流出、製品事故、ネット炎上、感染症、大規模地震など

1. 初期対応

第一報を受けた事業部門・子会社の責任者が、事実確認、原因究明などを行う。

2. 社長報告と危機対策本部の設置

企業グループの重要リスクと判断した場合、親会社の社長に緊急危機の発生を報告。
社長は、緊急危機と判断した場合はメンバーを招集して危機対策本部を設置する。

3. 危機対策本部での対応

危機対策本部長（社長）は、対応の基本方針を決定。
基本方針に基づき個々の対応を行う（被害者、顧客、行政、取引先、マスコミ、株主対応など）

4. マスコミへの公表

ポジションペーパー等の準備をして模擬記者会見。

クライシス・シミュレーション・トレーニングのポイント

1. いかにリアリティーのあるシナリオを作れるか
   ⇒　参加者が「これは訓練だから」と思ったら効果が半減

2. 1年に1回必ずトレーニングを実施することを規程にして親会社の取締役会で決議をしておく。

3. 運営はリスクコンサルタントや弁護士などの専門家に委ねる

社長や役員からのプレッシャーを廃する
1. 定期的な運営を担保する
2. 指摘したいことは、「専門家」を介して言う

企業における実施事例

鉄道会社：　役員向けシナリオ非提示型訓練　（地震）
電力会社：　シビアアクシデントトレーニング（発電所事故）
　　ブラインドシナリオトレーニング（地震BCP）
鉄鋼メーカー、衣料メーカー、飲料メーカー、有料老人ホーム事業など
　　クライシス・シミュレーション・トレーニング
　　（製品事故、情報漏洩、感染症、パンデミックなど）

まとめ　企業の情報法コンプライアンス部門の今後

1. 「情報法コンプライアンス」、「情報セキュリティ」が、企業価値の向上に寄与する時代、情報法コンプライアンス部門の社内プレゼンスがますます向上

⇒コンプライアンスの取組は、法のクロノロジー研究、比較法研究は当然ながら、経営学分野との学際研究から、マネジメント・システムとして実装する必要あり

2. 企業における個人情報の管理は、競争法ではなく個人情報保護法による保護が、利活用にも好影響

⇒コンプライアンス経営の視点から、企業からの立法提案が必要ではないか