内部統制から見た
プライバシーガバナンス

英知法律事務所
弁護士　森　亮二

○○ガバナンス

○○ガバナンス？

- ガバナンスとは、もともと「統治」という意味の英語 “governance”。
- 様々な文脈で使われて（濫用されて）多義的な言葉となっている。
- 「ITガバナンス」「情報セキュリティガバナンス」などのように使うときは、企業その他の組織において、IT戦略や情報セキュリティが正しく確保される仕組みが作られて機能していることをいいます。
- **○○が正しく確保される仕組みが作られて機能していること**

○○ガバナンス？

経済産業省
Ministry of Economy, Trade and Industry

文字サイズ

サイト内検索

ホーム | 経済産業省について | お知らせ | 政策について | 統計 | 申請・お

政策について ▸ 政策一覧 ▸ 安全・安心 ▸ 情報セキュリティ政策 ▸ 情報セキュリティガバナンス確立促進事業 ▸ 情報セキュリティガバナンス

印刷

情報セキュリティガバナンスの概念

情報セキュリティガバナンスの概念・定義

情報セキュリティガバナンスとは、「企業における情報セキュリティガバナンスのあり方に関する研究会報告書」において、「コーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」と定義されました。

平成20年6月公開の「産業構造審議会情報セキュリティ基本問題委員会 中間とりまとめ（PDF形式：323ＫＢ）」の中で、「企業経営の主目標は、株主、顧客、取引先、従業員、社会等の利害関係者に対して責任を果たすこと、つまり、「企業価値の向上」及び「社会的責任の遂行」にあり、これを支える重要な取組の一つにリスク管理が位置づけられる。様々なリスクの内、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み*を構築・運用することを情報セキュリティガバナンスと位置づける。（*経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを指す）」と、その概念の一層の明確化を図りました。

プライバシーガバナンスの必要性

- 「情報セキュリティガバナンス」は、経産省の2008年のガイドライン※の公表後、間もなく「やらないとダメ」に。

- 手堅く役立つものをガイドラインにするので、それほど新しいものが出るわけではない。　　e.g.　IPAの十大脅威は2006年から

- プライバシーガバナンスもそうなるのではないか。

※　　産業構造審議会情報セキュリティ基本問題委員会中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～

背　景

- 「プライバシー問題」で炎上すると様々な問題が生じる（代表者謝罪、役員交代、事業廃止等）

- その一方で**何が炎上するのか分からない**。個人情報保護法だけ確認してもダメ。　⇒　e.g.　リクナビ事件

北風

- 株主や債権者等に対して、「プライバシー問題」で役員が「**内部統制**」に関する義務違反で責任を負うことがありうるのではないか。

- 情報セキュリティの不備で漏えいしたらまずいことになったが、同じことがプライバシーについてもあるのではないか。

太陽

- そろそろプライバシー保護で差別化が図れるのではないか。

ガバナンスと「内部統制」

ガイドブックの構成

3. 経営者が取り組むべき三要件

そもそも、株式会社の経営者は、善良な管理者としての注意義務（善管注意義務）を負う。かかる**善管注意義務には、会社の規模に応じたリスク管理体制の構築も含まれる**。したがって、かかる体制の不備により、損失が発生した場合には、関連部署の担当の役員だけでなく、その他の役員も損害賠償責任を問われることとなりうる。デジタル・トランスフォーメーションを推進する企業にとっては、パーソナルデータの管理と適切な利用は重要な業務執行であり、**適切な内部統制の構築ができないことにより、漏えいや炎上の結果として企業に損害が発生する場合には、その損害の責任を経営者個人が問われうることになる点に注意が必要である**。

以上の観点から、企業の経営者には、プライバシー問題を競争力の要素として、重要な経営戦略上の課題として捉えるとともに、コーポレートガバナンスとそれを支える内部統制の仕組みを企業内に構築・運用することが求められる。

プライバシーガバナンス実現のために、経営者がまずすべきことは、以下の3点である。

要件１：プライバシーガバナンスに係る姿勢の明文化

要件２：プライバシー保護責任者の指名

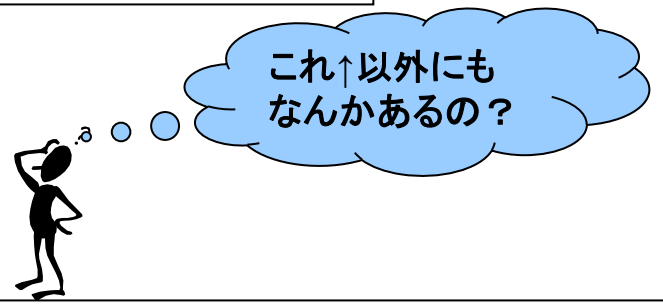
要件３：プライバシーへの取組に対するリソース投入

裁判例における「内部統制」

内部統制とは何か

3つの内部統制の法的根拠

- 金融商品取引法 → 内部統制報告制度
- 会社法
  - 第362条4項等 → 業務の適正確保体制決定義務
  - 取締役の善管注意義務 → 判例の内部統制構築義務



判例における内部統制 – 大和銀行事件

大和銀行事件（大阪地裁H12.9.20）

【事案】

- 大和銀行ニューヨーク支店の従業員Aが同行に無断で簿外取引を継続した結果、同行に巨額の損失を与えたことつき、**取締役12名に対し、1人あたり830億円から75億円という巨額の損害賠償が命じられた株主代表訴訟事件である。**
- Aはトレーダーとして、米国財務省証券（以下「財務省証券」）を他の証券会社との間で売買し、その資金手当てのため、大和銀行が業務上保管していた顧客および大和銀行自身の財務省証券を順次売却した。
- Aの違法行為は、(a)トレーダーとしての財務省証券の簿外取引と(b)保管中の財務省証券の無断売却の二つに分けられる。

- 2つの事件

＜甲事件＞

内部統制システムの不備によって見過ごされた簿外取引自体により、11億ドルの損失を会社に与えたこと

＜乙事件＞

簿外取引と発覚後の隠ぺい行為を理由として米国当局から刑事訴追を受け、罰金の支払を命じられるとともに弁護士費用を支出して3億5000万ドルの損失を会社に与えたこと

- 取締役固有の違法行為・・・

  隠ぺい！　→　違法行為(c)

判例における内部統制

- はるか離れた米国のトレーダーを取締役が直接監督するのは無理。それでも裁判所は、不正行為を防止する「仕組み」（＝内部統制）ができていなかったことについて取締役に責任があるとして、巨額の損害賠償責任を認めた。
- このため「内部統制」がおそろしいものとして一躍有名に・・
- 内部統制とは、「会社が営む**事業の規模、特性等に応じたリスク管理体制**」
- 担当取締役でないこと、組織的・物理的に距離があること等により、直接の監督義務違反が否定される事案でも、内部統制構築義務違反により責任が認められる場合がある。
- 今のところ、プライバシー問題の「炎上」について取締役の責任が認められた事案はないが、時間の問題かも…

判例における内部統制 – ダスキン事件①

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

【事案】

- 食品衛生法に違反する添加物を含んだ肉まんを販売した会社が、その事実が報道されたことなどにより多額の損失を生じたことについて、取締役・監査役が善管注意義務違反に基づく損害賠償を求められた株主代表訴訟。

- 同社の委託先の業者が違法添加物を使用した肉まんを製造し、同社はこれに気づかずに当該肉まんを販売をしていたところ、違法添加物が使用されている旨の通報を受けた。担当取締役2名は、この通報を受けた後、事実確認を行い、違法添加物の使用を知ったにも関わらず、肉まんの販売を継続する決定を行った。また、通報者に口止め料6300万円を支払った。

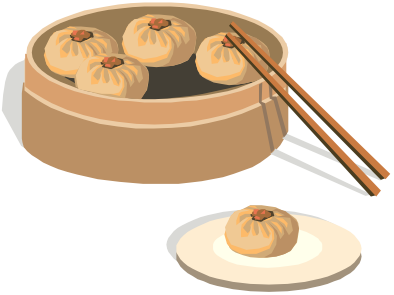
- 後日、この事実が報道されるなどしたため、同社は、フランチャイジーに対する営業補償など総額105億6100万円の出費を要することとなった。

- 本訴原告は、取締役による善管義務違反を多数主張したが、中でも目を引くのは、内部統制構築義務に関連した複数の請求原因を立てていることである。

判例における内部統制 – ダスキン事件②

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

① 違法添加物混入！！



② 通報（脅迫？）

③ 口止め料

④ 担当取締役らによる販売継続の決定

⑤ 取締役会に判明するも「積極的には公表しない」

判例における内部統制 – ダスキン事件③

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

【事案】ー原告の主張

(a) 違法添加物が使用されることがないようなリスク管理体制を構築すべき義務。

(b) 違法な添加物の使用を知った担当取締役がその販売の継続を決定したことについて、違法行為を発見した役員・従業員がどのように報告し行動すべきか等についてのマニュアルを作成し周知徹底すべきであり、さらに、違法行為等があれば即座にコンプライアンス部門等を通して取締役会に報告される体制を構築すべき義務。

(c) 担当取締役が通報者に口止め料を払ったことについて、取締役等が恐喝等違法行為の疑いがある事実を認識した場合には、直ちにコンプライアンス部門に報告し、同部門は必要な調査をした上、取締役会に報告するという体制を構築すべき義務。

(d) 違法行為を認識したら，直ちに違法添加物を食べさせた消費者に被害回復を申し出る体制を構築すべき義務

(e) その他善管注意義務違反多数

判例における内部統制 – ダスキン事件④

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

【原審の判断】

- (a)については、①従前、冷凍ワンタンの仕入れ取引があり、取引引開始に先立ってその品質管理状況を検討したうえで取引を開始したこと、②当該供給業者が肉まんに類似した製品の製造販売実績を有しており、これまで冷凍ワンタンについて品質上の問題が発生したことはなかったことなどから、品質管理のために必要な措置を講じていなかったとはいえないとした。

- 次に(b)と(c)については、**ダスキンは、当時、担当取締役は経営上の重要な事項を取締役会に報告するよう定め、従業員に対しても、ミスや突発的な問題は速やかに報告するよう周知徹底しており、違法行為が発覚した場合の対応体制についても定めていたこと、**

実際に起こった食中毒に関する企業不祥事を取り上げた啓発セミナーも開催していたこと、などから、ダスキンにおける違法行為を未然に防止するための法令遵守体制は、本件販売当時，整備されていなかったとまではいえないと判断した。

- さらに(d)については、原告は、体制の内容等を何ら具体的に主張しないため、主張自体失当であるとされた。

- 結局内部統制構築義務違反の主張はすべて棄却、(e)のうち、当時の専務取締役が違法添加物の混入の可能性を認識しながら、当時の最高責任者である取締役会会長兼社長に報告をしなかった点のみが善管注意義務違反にあたるとされた。

判例における内部統制 – ダスキン事件⑤

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

【控訴審の判断】

- 一転してすべての取締役の責任を認めた。
- (a)違法添加物が混入されないような体制の構築義務違反、(b)混入判明後に販売が継続されないような体制の構築義務違反、(c)恐喝者に対して口止め料を支払うようなことのない体制の構築義務違反については、原審同様すべて否定。
- 混入・販売を知った後、「積極的には公表しない」という意思決定を行ったことは「消極的な隠蔽行為」である。
- 違法添加物の混入を知りつつその事実を秘して販売を継続するといった問題が発生した場合には、自ら進んで事実を公表して、すでに安全対策がとられて

問題が解決していること、隠蔽が過去の問題であって克服されていることを印象づけることによってしか、消費者の信頼を取り戻すことはできない。

- メディアや世論が隠蔽について敏感であり、隠蔽自体が大々的に取り上げられて、企業の信頼が大きく損なわれることがありうるのであり、本件取締役らの判断は「到底『経営判断』というに値しない」。

【最高裁の判断】

取締役らの上告棄却！

判例における内部統制 – ダスキン事件⑥

ダスキン事件（大阪地裁H16.12.16）
（大阪高裁H18.6.9、最高裁H20.2.12）

＜原審の教訓＞

- 今後の株主代表訴訟等においては、発生した不適切な行為・結果を逐一捉えて、取締役にはそのような行為・結果を防止すべき体制の構築義務違反があったとする主張がなされる可能性あり。しかしながら

直接の監督義務

①直接の監督義務違反が認められる場面では内部統制構築義務違反を問題にする余地がない。

→ ジャージー高木乳業事件

内部統制構築義務

②構築すべき内部統制の内容が具体的・合理的なものでなければ、そのような主張が認容されることはない。

＜控訴審の教訓＞

- **「違法添加物の混入を知りながら販売を継続する」という最悪の不祥事であったにも関わらず、事件の発生自体（混入、販売継続、口止め料の支払）を防止すべき内部統制構築義務違反は、第一審判決同様、認められなかった。本件で善管注意義務違反が認められたのは、すべて混入の事実を認識した後にとられた行為**についてであり、その中心は、「隠蔽への誘惑」に負けたことによる責任。

- 内部統制は取締役に結果責任をもたらすものでもない。重大な不祥事が判明しても、取締役は、善管注意義務違反に問われるとは限らない。実のところ、勝負はそこから・・

ガイドブックにおける特徴的な内部統制

ガイドブックの構成

3.経営者が取り組むべき三要件

3. 経営者が取り組むべき三要件

そもそも、株式会社の経営者は、善良な管理者としての注意義務（善管注意義務）を負う。かかる**善管注意義務には、会社の規模に応じたリスク管理体制の構築も含まれる**。したがって、かかる体制の不備により、損失が発生した場合には、関連部署の担当の役員だけでなく、その他の役員も損害賠償責任を問われることとなりうる。デジタル・トランスフォーメーションを推進する企業にとっては、パーソナルデータの管理と適切な利用は重要な業務執行であり、**適切な内部統制の構築ができないことにより、漏えいや炎上の結果として企業に損害が発生する場合には、その損害の責任を経営者個人が問われうることになる点に注意が必要である**。

以上の観点から、企業の経営者には、プライバシー問題を競争力の要素として、重要な経営戦略上の課題として捉えるとともに、コーポレートガバナンスとそれを支える内部統制の仕組みを企業内に構築・運用することが求められる。

プライバシーガバナンス実現のために、経営者がまずすべきことは、以下の3点である。

要件１：プライバシーガバナンスに係る姿勢の明文化

要件２：プライバシー保護責任者の指名

要件３：プライバシーへの取組に対するリソース投入

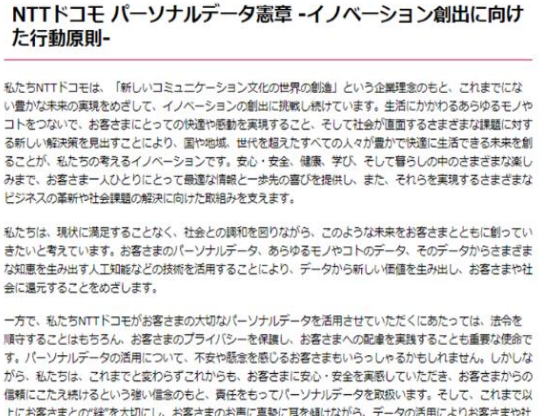
3. 経営者が取り組むべき三要件

要件１：プライバシーガバナンスに係る姿勢の明文化

- **企業が**それぞれの企業理念の下、一貫した姿勢で**消費者のプライバシーを守っていくことは、商品やサービスの品質を向上させ、社会からの信頼の獲得、ひいては企業価値向上に繋がる**。
- 経営者はプライバシー問題への取組を経営上の重要事項の1つと認識し、**プライバシー保護の軸となる基本的な考え方や姿勢を明文化し、組織内外に知らしめることが必要**。
- トップダウンで浸透させることで、組織全体にプライバシー問題への認識を根付かせることができる。公表することで消費者やステークホルダー（株主、取引先等）からの信頼を高める根拠となる。
- 経営者には、明文化した内容に基づいてプライバシー問題に取り組むことへのアカウンタビリティ確保が求められる。
- 明文化の具体的な形としては、**宣言の形をとったプライバシーステートメントや、組織全体での行動原則などを策定するケースもある**。

事例：NTTドコモ パーソナルデータ憲章の公表

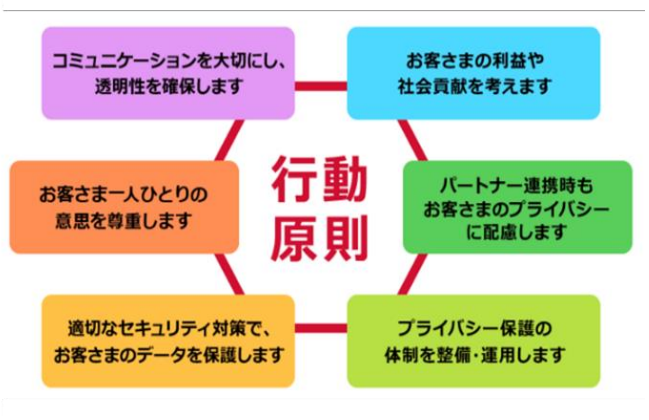
株式会社NTTドコモでは、「パーソナルデータ憲章―イノベーション創出に向けた行動原則―」を作成し、公表している。このパーソナルデータ憲章は、株式会社NTTドコモが「新しいコミュニケーション文化の世界の創造」という企業理念の下、これまでにない豊かな未来の実現をめざして、イノベーション創造に挑戦し続けていること、社会との調和を図りながら、未来をお客様と共に創っていきたいと考えていること、パーソナルデータの活用に当たり法令順守はもちろん、お客様のプライバシーを保護し、配慮を実践することも重要な使命であることなどを宣言し、行動原則として6つの原則を提示している。


NTTドコモ パーソナルデータ憲章 -イノベーション創出に向けた行動原則-

私たちNTTドコモは、「新しいコミュニケーション文化の世界の創造」という企業理念のもと、これまでにない豊かな未来の実現をめざして、イノベーションの創出に挑戦し続けています。生活にかかわるあらゆるモノやコトをつないで、お客さまにとっての快適や感動を実現すること、そして社会が直面するさまざまな課題に対する新しい解決策を見出すことにより、国や地域、世代を超えたすべての人々が豊かで快適に生活できる未来を創ることが、私たちの考えるイノベーションです。安心・安全、健康、学び、そして暮らしの中のさまざまな楽しみまで、お客さま一人ひとりにとって最適な情報と一歩先の喜びを提供し、また、それらを実現するさまざまなビジネスの革新や社会課題の解決に向けた取組みを支えます。

私たちは、現状に満足することなく、社会との調和を図りながら、このような未来をお客さまとともに創っていきたいと考えています。お客さまのパーソナルデータ、あらゆるモノやコトのデータ、そのデータからさまざまな知恵を生み出す人工知能などの技術を活用することにより、データから新しい価値を生み出し、お客さまや社会に還元することをめざします。

一方で、私たちNTTドコモがお客さまの大切なパーソナルデータを活用させていただくにあたっては、法令を順守することはもちろん、お客さまのプライバシーを保護し、お客さまへの配慮を実践することも重要な使命です。パーソナルデータの活用について、不安や懸念を感じるお客さまもいらっしゃるかもしれません。しかしながら、私たちは、これまでと変わらずこれからも、お客さまに安心・安全を実感していただき、お客さまからの信頼にこたえ続けるという強い信念のもと、責任をもってパーソナルデータを取扱います。そして、これまで以



（出典）https://www.nttdocomo.co.jp/info/notice/pages/190827_00.html

3. 経営者が取り組むべき三要件

要件２：プライバシー保護責任者の指名

- プライバシーガバナンスの実現には、経営者による関与と明文化した内容の具体的な実践が不可欠。そのために、**経営者は、組織全体のプライバシー問題への対応の責任者を担当幹部（プライバシー保護責任者）として指名し、経営者が姿勢を明文化した内容を実現するための責任を遂行させる**ことが必要。
- その際には、**プライバシー保護責任者の責任範囲を明確にし、プライバシー問題の発生を抑止するために必要な権限も与える**必要がある。
  - プライバシー保護責任者は、**GDPRでいうところの、強い独立性が担保されているデータ保護オフィサー（DPO）とは必ずしも同じものとは限らず**、役員が担うこともありうる。
- 経営者は、プライバシー保護責任者から報告を求め、評価をすることで、組織の内部統制をより効果的に機能させる。

要件3：プライバシーへの取組に対するリソースの投入

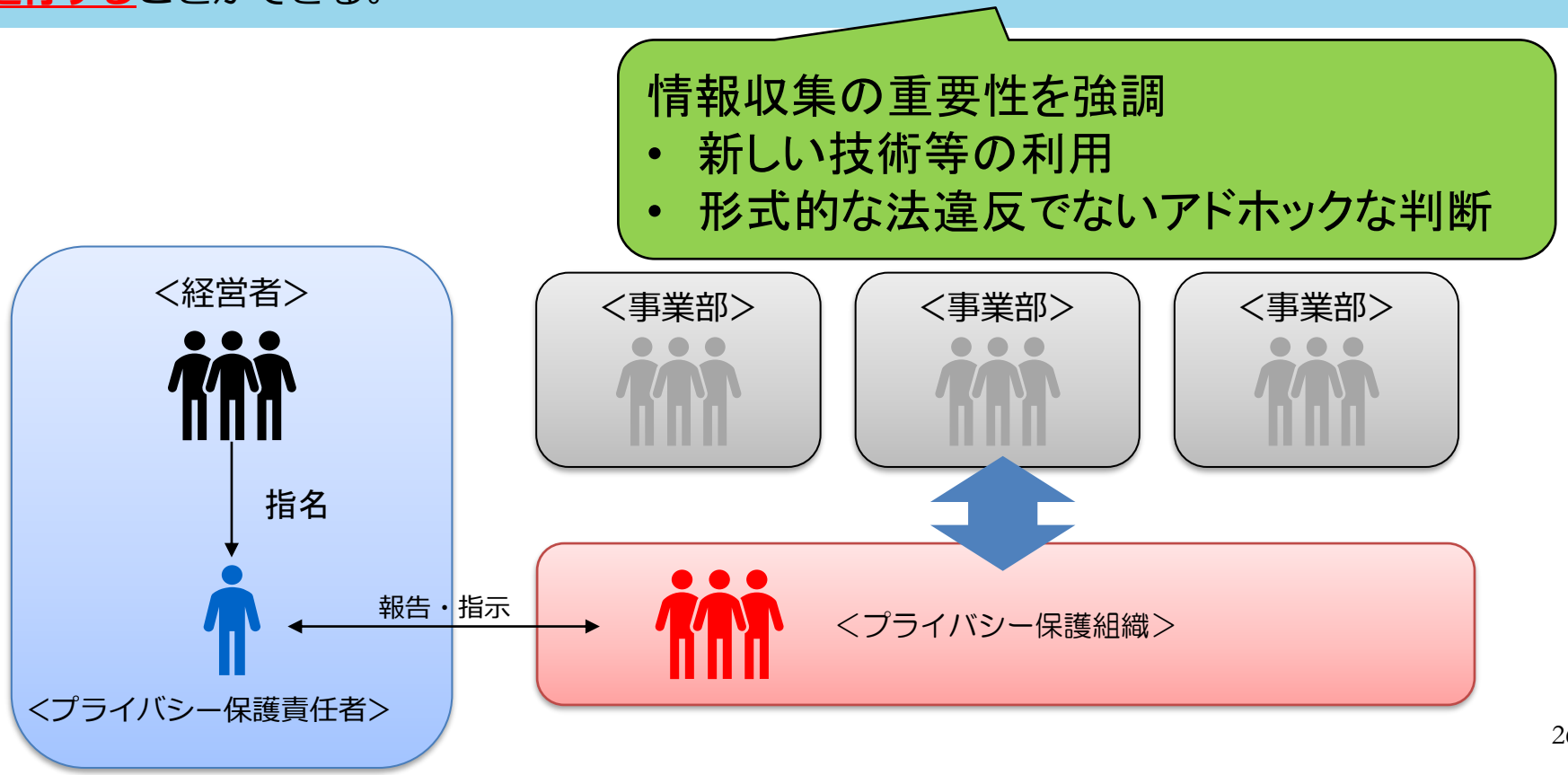
- 経営者は、明文化した姿勢の実践のため、**必要十分な経営資源（ヒト・モノ・カネ）を投入**することが求められる。プライバシー問題に対応するための体制の構築や、十分な人員の配置、人材の確保・育成等を実施することが必要。
- プライバシーに係る対応は、事後的に追加するものではなく、事前に検討され、戦略、事業、システムへ組み込まれるべきもの。また、プライバシー問題は、経営状況や外部環境に必ずしも依存せず、常時発生する可能性がある。そのため、**必要なリソースが継続的に投入され、取組自体の継続性が高められる**ことが期待される。

4.プライバシーガバナンスの重要項目（4.1~4.3）

4．プライバシーガバナンスの重要項目（4.1体制の構築）

■ プライバシーガバナンスの機能として、**各部門の情報を集約し、事業におけるプライバシー問題を発見することが求められる**。さらに、**対象となる事業の目的達成とプライバシーリスクマネジメントを両立**するために、**対応策の多角的な検討**が必要。

■ **プライバシー保護責任者の下で、中核となる組織を企業内に設ける**ことが望ましい（＝**「プライバシー保護組織」**）。プライバシー保護組織を設けることで、**社内の新規事業部門との密なコミュニケーションの醸成や、社外有識者などからの関連情報の収集、多角的な対応策の検討を遂行する**ことができる。



4．プライバシーガバナンスの重要項目（4.1体制の構築）

プライバシー保護責任者の役割

- プライバシー保護責任者は、**経営者が明文化した姿勢等の実践のための方針の確立及び体制の構築を進め、当該方針の実施を徹底**する。
- 経営者に対し報告を行い、経営者が明文化した内容と合致しているかを絶えず確認する。

プライバシー保護組織の役割

- 企業内の各部門から新規事業やサービス内容に関する**様々な情報を集約**し、**プライバシー問題が消費者や社会に発現するリスクを見つける**。そのために、各部門と日頃から接点を持つとともに、プライバシー保護組織の存在を企業内に周知徹底する必要がある。
- プライバシー問題は、個人的な感じ方の相違や、社会受容性がコンテキストや時間の経過で移り変わることから、**常に関連する情報を収集**する。
- **対象事業の目的を実現**しつつ、プライバシーリスクに対応するために、**多角的に対応策を検討**する。
- 新規事業や新規技術を開発する部門とともに、**他部門と円滑な連携を図ることが重要**。
- **プライバシー問題が発生した場合の初動や**、その後の再発防止策の策定等の**事後対応について**、事業部門と連携して情報を集約・検討し、**プライバシー保護責任者へ報告・指示を仰ぐ**。
- プライバシー問題に係る検討をした際の**情報を履歴として蓄積し、活用**できるようにしておく。

4．プライバシーガバナンスの重要項目
（4.1体制の構築～4.2運用ルールの策定と周知）

4.1 内部監査部門や第三者的組織の体制構築

- **内部監査の体制を構築**するなど、**独立した立場からモニタリング・評価**することで、社内の取組を徹底し、**社外からの信頼を更に高める**。
- また、**第三者的な立場の外部の有識者からなるアドバイザリーボード、諮問委員会などを設置**し、評価・モニタリングを受けることも検討すべき。有識者の専門的かつ客観的な意見を、経営者や社員へフィードバックする体制・仕組みを構築することで、組織全体としてプライバシー問題への意識を高めることも可能。

4.2 運用ルールの策定と周知

- 構築した体制が実質的に機能するためには、サービスや技術が開発・提供される前に、プライバシー保護責任者やプライバシー保護組織によってプライバシーリスクが把握され、適切な検討がなされる必要がある。そのような**運用が徹底されるためのルールを、プライバシー保護責任者の責任の下、組織内で策定しておく**ことが重要。
- 例えば、**プライバシー保護のための対策や、「どのタイミング」で「誰が」プライバシーリスクを評価するかなどの観点から、ルール化**することが望ましい 。ただし、画一的な対応を招かぬよう、原理・原則の理解や定着を心掛けるとともに、継続的に内容の見直し・修正を行うなどのメンテナンスも必要。
- プライバシー保護責任者やプライバシー保護組織は、ルールを組織全体に周知徹底する必要がある。

4.3 企業内のプライバシーに係る文化の醸成

■ プライバシーガバナンスを実質的に機能させていくためには、プライバシーリスクに適切に対応できる企業文化を組織全体で醸成することが不可欠。**企業に所属する従業員一人一人が、当たり前のようにプライバシーに関する問題意識を持ち、消費者や社会と向き合った丁寧な対応をしていく状態が望ましい**。

■ **このような企業文化**を根付かせるためには、経営者やプライバシー保護責任者が発信し続けるなど、継続的な取組が必要。こうした取組は、社内の専門人材育成の基盤となる。

統制環境とは

残念ながら、COSO レポートでは、「統制環境」という用語そのものについて明確に定義を与えていない。しかし、多くのページを費やしてその概念を説明している。それらを要約して、**「組織の気風を決定し、組織を構成する人々の統制に対する意識に影響を与え、内部統制の他の4 つの構成要素の基礎をなすとともに、規律と構造を提供する」**としている。多少乱暴かもしれないが、日本に古くからある「企業風土」もしくは「企業文化」に非常に近い概念であると言えそうである。

デロイトトーマツのウェブサイトより

まとめ

北風

- 会社だけでなく役員個人の責任にもなり得る。
- リスク管理体制の中身は、事業の規模に応じたものであり、裁判所の判断は厳しいものではない。
  ⇒　できるところから
- ガイドブックが紹介する特徴的な内部統制
  - 方針の明確化「〇〇原則」「●●憲章」
  - 体制構築の際は、情報収集に力点を
    ⇒　新しい技術、変化する受容性
  - 企業文化も重要

ご清聴ありがとうございました