コンプライアンス研修

講師　ジャイロ総合コンサルティング（株）

西村伸郎

JAIRO
ジャイロ総合コンサルティング

内容

- コンプライアンスの基礎
- 個人情報保護とは
- 事例で学ぶ

コンプライアンス経営の本質

ＣＳＲとは

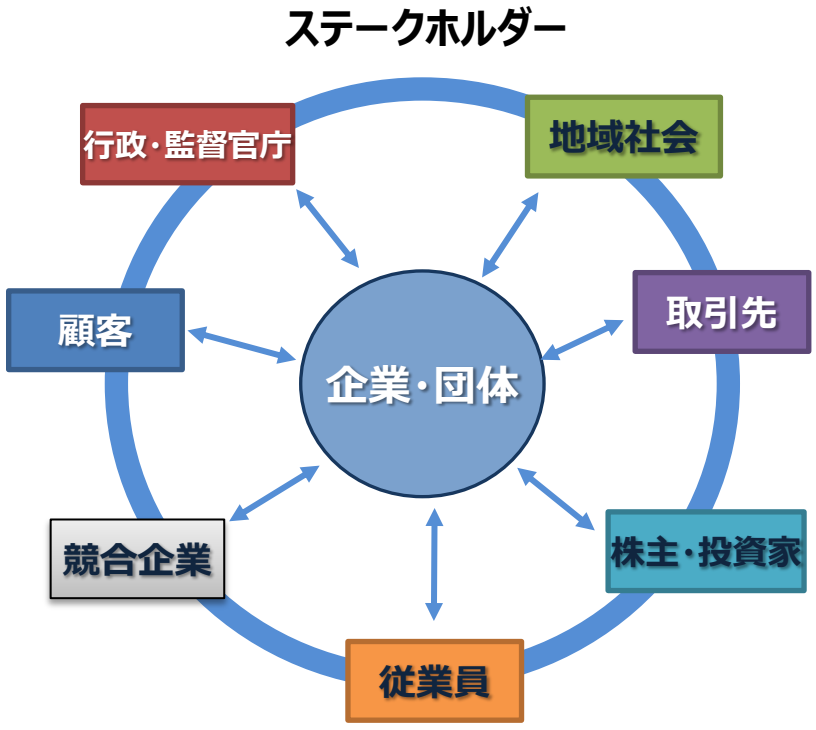
ＣＳＲ（企業・団体の社会的責任）は、企業・団体の活動が単に法令に適合しているだけではなく、社会にとって望ましいとされる価値基準に照らして倫理的であり、誠実であることを求めている。そのような企業・団体でなければ、もはや社会から信頼も尊敬もされず、製品やサービスに対する顧客や消費者の支持も得られない。

企業・団体の役割と目的

事業活動（製品・サービスの提供など）を行い、
→ 利益を生み出し、
→ 利害関係者（ステークホルダー）に還元しながら、維持・発展する

社会の一員として存在

→ 創業の思い、経営理念、社是・社訓を元に
→ 自組織の存在意義、役割を明確にし
→ 従業員との価値観・志・思いを融合し
→ 社会的なモラル・期待に応える



コンプライアンスと個人情報保護

① 個人情報漏えい、営業秘密漏えい

② ハラスメント（パワハラ、セクハラなど）

③ データ改ざん・偽装

④ 粉飾決算、経費の不正請求、脱税

⑤ 労務上の不正行為

⑥ 他社との不適切な関係（過剰接待等）

⑦ 下請いじめ（下請法違反）

⑧ 営業上の不正行為（架空売上、物品の横流し、談合）

JAIRO ジャイロ総合コンサルティング

個人情報とは

名称	定義	説明
個人情報	生存する特定の個人を識別できるもの、および個人識別符号	例えば、次です • 本人の氏名、生年月日や連絡先などを組み合わせた情報 • 防犯カメラに記録された情報など本人を判別できる映像データ • 本人氏名が含まれるなどから、特定の個人を識別できる録音データ • 氏名・会社名が含まれるなどの理由から、特定の個人を識別できるメールアドレス
個人データ	個人情報の内、特定の個人情報を検索できるよう体系的化したもの	コンピュータで管理されているか、紙で管理されているかを問わず、個人情報を一定の規則で整理・分類し、特定の個人情報を容易に検索できるように目次、索引などによって順番に並べているもの
保有個人データ	個人データのうち、個人情報取扱事業者に開示・訂正・消去等の権限があるもの	保有個人データ取扱い事業者は、本人からの請求に応じて、個人情報を開示、訂正、利用停止等しなければならない。また、以下の5点に関してHPに公表するなどして、本人の知り得る状態にしておく必要がある。 • 事業者の名称 • 利用目的 • 請求手続きの方法 • 苦情の申出先 • 加盟する認定個人情報保護団体の名称

個人情報保護法を知る①

- **ＩＴ化の進展**：　不正アクセスやウィルスなどによる情報セキュリティへの脅威が高まる。
- **流出事件が続発**：一旦流出すると、プライバシーの侵害など取り返しのつかない被害を及ぼす恐れがあり、多くの人に不安が高まる。
- **SNSの普及**：　炎上など取り返しのつかない事態につながる危険性が高まる。

個人情報保護法の趣旨

- 個人の権利・利益の保護と個人情報の有用性とのバランスを図る。

個人情報保護法を知る②

法的整備の進展

プロバイダ責任制限法
（2002年5月施行）

ネット上の掲示板などで誹謗中傷を受けたり、個人情報を掲載されて、個人の権利が侵害された場合、プロバイダ事業者・管理者に対して、削除を要請できる。

不正アクセス禁止法
（2002年5月施行
2012年改正）

- 他人のID・パスワードを奪取・盗用し、他のコンピュータへのアクセスを行うことが犯罪
- ソフト上のセキュリティ上の弱点を攻撃し、プログラム改ざんやコンピュータを不能に追い込んだりする行為を禁じる。

個人情報保護法
（2005年4月施行）

- 5000件以上の個人情報を個人情報データベース等として所持し用いている事業者は個人情報取扱事業者となる。
- 予め本人の同意を得なければ、個人データを第三者に提供してはならない。

改正
（2017年全面施行）

改正
（2022年全面施行）

例外事項

- ①法令に基づく
- ②人の生命、身体又は財産の保護のため
  - 警察などの捜査情報を求められる場合
  - 事故・災害時など緊急性がある場合
- ③公衆衛生の向上又は児童の健全な育成の推進
  - 児童虐待の恐れがある場合
- ④国の機関・地方公共団体が法令の定める事務を遂行する
  - 税務署からの問い合わせや国勢調査

不正競争防止法
（1934年制定）

2015年改正
（営業秘密である個人情報を入手したものも処罰対象に）

個人情報保護法改正（2017年施行）の概要

改正の背景

グレーゾーンが拡大、ビッグデータへの対応、グローバル化への対応

個人識別符号

① ＤＮＡ、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋など特定の個人を識別可能な情報

② 公的な番号（マイナンバー、パスポート、基礎年金番号、免許証番号、保険証の被保険者番号等）


マイナンバー


パスポート

運転免許証


指紋認識データ

匿名加工情報

匿名加工情報（特定の個人を識別することができないように個人情報を加工した情報であって、当該個人情報を復元することができないようにしたもの）の類型を新設し、個人情報の取扱いよりも緩やかな規律の下、自由な流通・利活用を促進


個人情報

匿名加工情報


識別できない

個人情報取扱事業者の範囲

取り扱う個人情報の数が5000人分以下である事業者も規制

個人情報保護法改正（2022年施行）の概要

改正の背景

個人の権利意識の高まり、保護と利用のバランスの推進、国際的な制度調和・連携

本人の請求権の拡充

① 利用する必要がなくなったとき
② 重大な漏えいなどが発生したとき
③ 本人の権利または正当な利益が害される恐れがあるとき

事業者の義務・公表等事項の追加

① 漏えいなどが発生した場合
② 本人への通知も義務化

仮名加工情報の創設

① 匿名加工情報に加え、個人情報の加工の程度を抑え利活用しやすい「仮名加工情報」
② 法令による場合や共同利用を除き、第三者提供を行うことができない

短期保有データの保有個人データ化※

6か月以内に消去される短期保有データは「保有個人データ」に含まれる

法令違反時のペナルティ強化

※ 保有個人データとは、個人情報取扱事業者が開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有している個人データ

事業者および個人が守るべきルール①

事業者が守るべきルール

① 個人情報を取得・利用する時のルール

⇒ 個人情報を取得した場合は、その利用目的を本人に通知、又は公表する（あらかじめ利用目的を公表している場合を除く）

② 個人情報を保管する時のルール

⇒ 情報の漏えい等が生じないように安全に管理する

③ 個人情報を他人に渡す時のルール

⇒ 個人情報を本人以外の第三者に渡すときは、原則として、あらかじめ本人の同意を得る

④ 個人情報を外国の第三者に渡す時のルール

⇒ 外国の事業者についても原則適用（第三者が個人情報の体制整備し、あるいは委員会が認めた国であること）

⑤ 本人から個人情報の開示を求められた時のルール

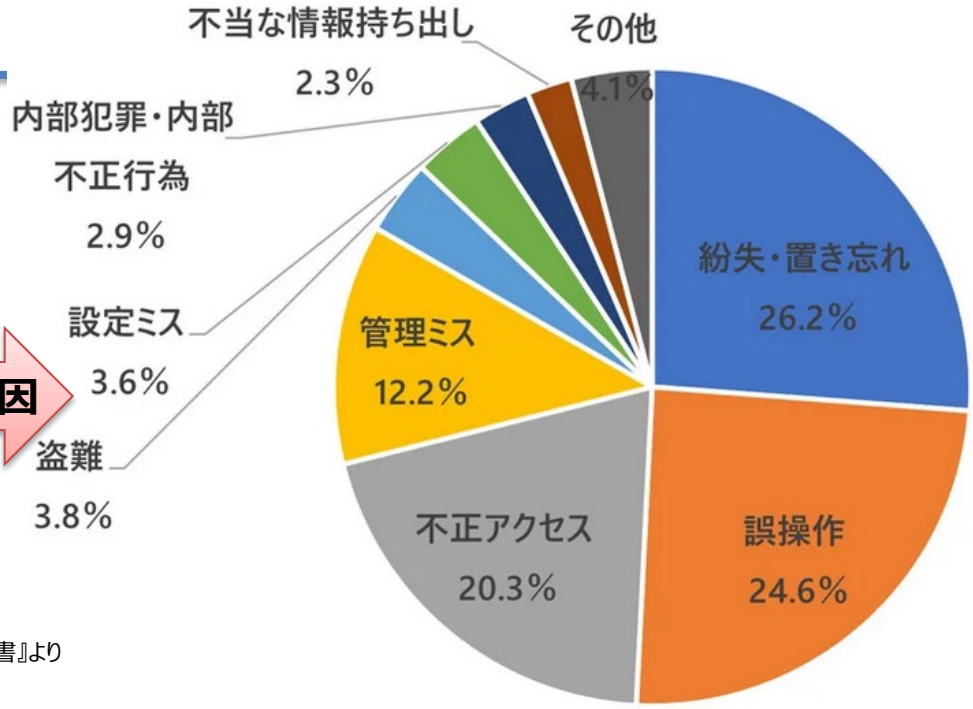
⇒ 本人からの請求に応じて、個人情報を開示、訂正、利用停止等する

個人情報の漏えい

情報漏えい事件の現状

漏えい人数	561万3,797人
インシデント件数	443件
想定損害賠償総額	2,684億5,743万円
一件あたりの漏えい人数	1万3,334人
一件あたり平均想定損害賠償額	6億3,767万円
一人あたり平均想定損害賠償額	2万9,768円

その原因



『2018年情報セキュリティインシデントに関する調査報告書』より

情報が漏洩した結果、企業や団体はどうなるか？

- **直接的損害**
  - **刑事罰** — 6か月以下の懲役または30万円以下の罰金 **（→ 22年改正で厳格化）**
  - **民事賠償** — 1人当たり数千円～数万円の賠償（過去の判例）
- **間接的損害**
  - **信用低下** — 信用が低下することによって、新規受注や取引停止
  - **復旧コスト** — システムやデータの検証に要するコスト
社内エンジニアの稼働工数や外注費の発生
  - **業務効率低下** — 殺到する問い合わせへの対応

業務内で情報漏えいを防ぐには

紛失・置き忘れ

- 外部に情報（PC、メモリ、書類等）を持ち出さない
- 情報の持ち出しルールの徹底・遵守
- PC、スマホのパスワードやロック
- 外部での会話にも注意　など

誤操作・管理ミス・設定ミス

- 他による宛先のダブルチェック（電子メールやFAX）
- 情報廃棄ルールの厳格化（シュレッダーなど）
- パスワードの定期的な変更、および外部への非開示
- 添付ファイルの暗号化　など

盗難・不正な情報持ち出し

- アクセス制限（権限の付与）
- アクセス履歴・操作履歴の定期的な監視
- 職場環境や処遇の見直し　など

不正アクセス

- セキュリティーソフトをインストール
- ファイル共有ソフトを利用しない
- インストールできるソフトを制限
- ファイアウォールの活用 など

事例演習①

AさんがFacebookに書き込んでいる内容が少々問題になっている。取引先として訪問した企業名と社内風景の写真を時折アップしているようで、そこでアップされたある企業の社員が、たまたまそれを目にして、「大丈夫ですか？」と我が社に連絡してきた。内容自体は特に悪口でもないし、秘密事項にも触れていないようなので、大きな問題にはしたくない。しかし、ことがことだけに放置するわけにはいかない。

何が問題ですか。また、どのような影響があると思われますか。

会社として、このような事態を今後発生させないためにどうするべきですか。

- SNSなどでの炎上は、決して特殊な人だけの話ではない。
- 一時期に話題になった、バイト先の店で悪ふざけをしてSNSに投稿し、炎上してしまう「バイトテロ」のように、お店側から訴訟されるなど大きな問題に発展する場合がある。
- 一度ネット上で公開された内容は完全に削除するのは難しい。
  他者や他団体に迷惑のかかる可能性がある場合は、SNSへの投稿を控える。

事例演習②

B社はネット通販を中核事業に据えています。B社のECサービスは、ある大手IT企業の会社のクラウドサービスを利用していますが、B社内これらクラウドサービスに十分な人員を割くことが出来ず、営業担当の方が片手間で行っているのが実情です。
ある日のことお客様から、「お宅のECサイトのあるページから、多くの人の個人情報が表示されていますよ。大丈夫ですか？」という連絡を受けました。

何が起こったのだと思いますか。また、何が原因だと思いますか、考えられることを挙げてください。

- クラウドサービスとして、オンラインストレージ、Zoomなどの会議システム、Gmailなどのメールシステム、さらに専用SWも多く導入されています。
- クラウド サービスはインターネット経由で利用するため、セキュリティ面のリスクに注意が必要です。また、サービス提供元の状況（例えば、サービス終了）に自社が影響を受けることもリスクの 1 つです。

私たちが行うべきこと

個人で行うべきこと

- 情報管理の重要性を認識しておく
- 自身が扱う個人情報は何かを再確認する
- 不審に思うことがあれば、他に知らせる・相談する

組織で行うべきこと

- 規程・ルールを最新の状況に合わせる
- 技術的安全管理策を講じる
- 基本方針・ルールの一般層への浸透策を施す