令和6年度

人権研修問題研修講演会

「個人情報漏えい問題と人権」

大阪企業人権協議会
特任講師（大阪府人権擁護士）

金井　敬三

◆企業等が管理する「情報」と「情報セキュリティ」

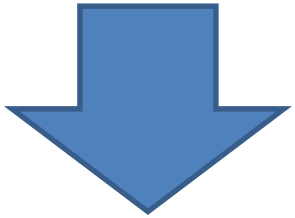
○個人情報
- **顧客情報**
- 従業員の人事情報　など

○プライバシー情報
- **病歴情報**
- 国籍・民族に関する情報　など

○営業秘密
- 技術情報（ノウハウ等）
- 取引先情報（顧客情報等）
  など

○その他知的財産関連の情報など
- 特許情報、著作物　など

これらの情報をしっかりと管理し、漏洩を防ぐために取り組むこと



「情報セキュリティ」

◆組織に求められる「情報モラル」とは？

人権尊重のための情報モラル

「情報を取り扱う際に求められる考え方と行動」

個人の尊重

人格の尊重　・プライバシー　・名誉・信用　・表現の自由

安全への配慮

・個人情報保護
・情報セキュリティ
・リテラシー教育

社会的公正への配慮

・消費者保護、知的財産権保護
・デジタル・ディバイド対応　等
（様々な「情報格差」の解消）

【1】

個人情報保護法について

（2005年4月施行、2017年5月改正施行
以降原則3年毎見直し）

◆「個人情報保護法」について

①国および地方公共団体の責務等を明らかにすると共に、
事業者の遵守すべき責務等を定める。
個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。（第1条要約抜粋）⇒ どうバランスを図るか？

②プライバシーとの関係
プライバシーとは「個人の私生活に関する事柄や、それが他から干渉されない状態を要求する権利の総称」

個人情報保護法では「プライバシー保護」という文言はない。
従って、プライバシー侵害による個人の権利利益の救済は、従前通り、民法上の不法行為や刑法上の名誉棄損罪等によって図られることが基本となる。

法的問題としての個人情報保護の全体像

○「個人情報の保護に関する基本方針」

○「個人情報保護法」

○関連法（職業安定法（求職者等個人情報）、プロバイダ責任制限法　不正競争防止法　著作権法　等）

○ガイドライン（通則編・外国第三者提供編・確認記録義務編・匿名加工情報編）・金融関連分野・医療関連分野・情報通信関連分野等については、別途のガイドライン等がある

○事業者毎の「個人情報保護指針」・・・「プライバシーポリシー」

○認定個人情報保護団体（民間団体）制度・・43団体（2024年）
・民間事業者の自主的な取組みを尊重し、個人情報の適正な取扱いを確保目的とする民間団体を認定し一定業務をすることを認め支援するようしている。

「個人情報保護法」の関連年表（4つのポイント）

法改正対応　等	重大な出来事や社会状況
1988年　行政機関個人情報保護法制定 プライバシーマーク制度運用開始	
1999年　「改正住民基本台帳法」成立	
2003年　「個人情報保護法」（2005年施行）	1964年　「宴のあと」事件東京地裁判決 「プライバシー権」認知～憲法13条
	1980年　OECD「プライバシー8原則」提示 ①目的明確化　②利用制限　③収集制限 ④データ内容　⑤安全保護 ⑥公開　⑦個人参加　⑧責任　①（矢印）
2013年　「マイナンバー関連法」成立	
2015年　「個人情報保護法」改正（2017年施行） ・個人情報の定義明確化 ・情報漏洩対策強化 ・ビッグデータの利活用推進　②（矢印）	2014年　「パーソナルデータの利活用に関する制度改正大綱」公表 2015年　「日本年金機構」漏洩事件
2016年　「個人情報保護委員会」設置	2016年　EU「一般データ保護規制（GDPR）」
2021年　「デジタル庁」設置	2019年　「リクナビ」事件
2022年　「個人情報保護法」改正 ・罰則強化（2020年12月前倒し施行） ・個人の権利の強化（本人同意 等） ・漏洩時の報告・本人通知の義務化　③（矢印）	2020年　コロナ禍における日本社会のデジタル化遅れ露呈 ・給付金手続き不調、行政の印鑑問題 医療やオンライン教育での遅れ顕著 ・「個人情報保護法制2000個問題」　等　④（矢印）
2023年　「個人情報保護法」改正 ・「デジタル社会形成整備法」に関連し、行政・自治体の法律の統合・共通化等	◆「超スマート社会」の到来・本格化 ～IoT・SNS・AI 等の社会浸透～

◆個人情報の定義

（第2条）個人情報とは、生存する個人に関する情報

ｉ）当該情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別できるもの

（例）氏名に加え、生年月日、連絡先（住所、電話番号、メールアドレス）、会社における職位又は所属情報で氏名と組み合わせたもの、防犯カメラ記録情報、官報、電話帳、新聞、ホームページ、SNS等で公にされている特定の個人を識別できる情報

ⅱ）個人識別符号が含まれるもの（政令等で個別に指定）

①身体の一部の特徴を電子計算機のために変換した符号

（DNA、顔、虹彩、声紋、歩行の態様、指紋・掌紋　等）

②サービス利用や書類において対象者毎に割り振られる符号

（旅券番号、基礎年金番号、運転免許証番号、住民票コード　マイナンバー、各種保険証　等）

◆「要配慮個人情報」とは？

○（第2条第3項）「要配慮個人情報」とは、本人に対する不当な差別や偏見その他の不利益が生じないように、その取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう

①人種　②信条　③社会的身分　④病歴　⑤犯罪の経歴　⑥犯罪被害の事実　⑦身体障害、知的障害、精神障害等心身の機能障害　⑧健康診断等の結果　⑨医師等が行う指導、診療等の内容　⑩被疑者・被告人として刑事事件手続きが行われた事実　⑪少年法に規定する保護事件に関する手続きが行われた事実　⑫ゲノム情報

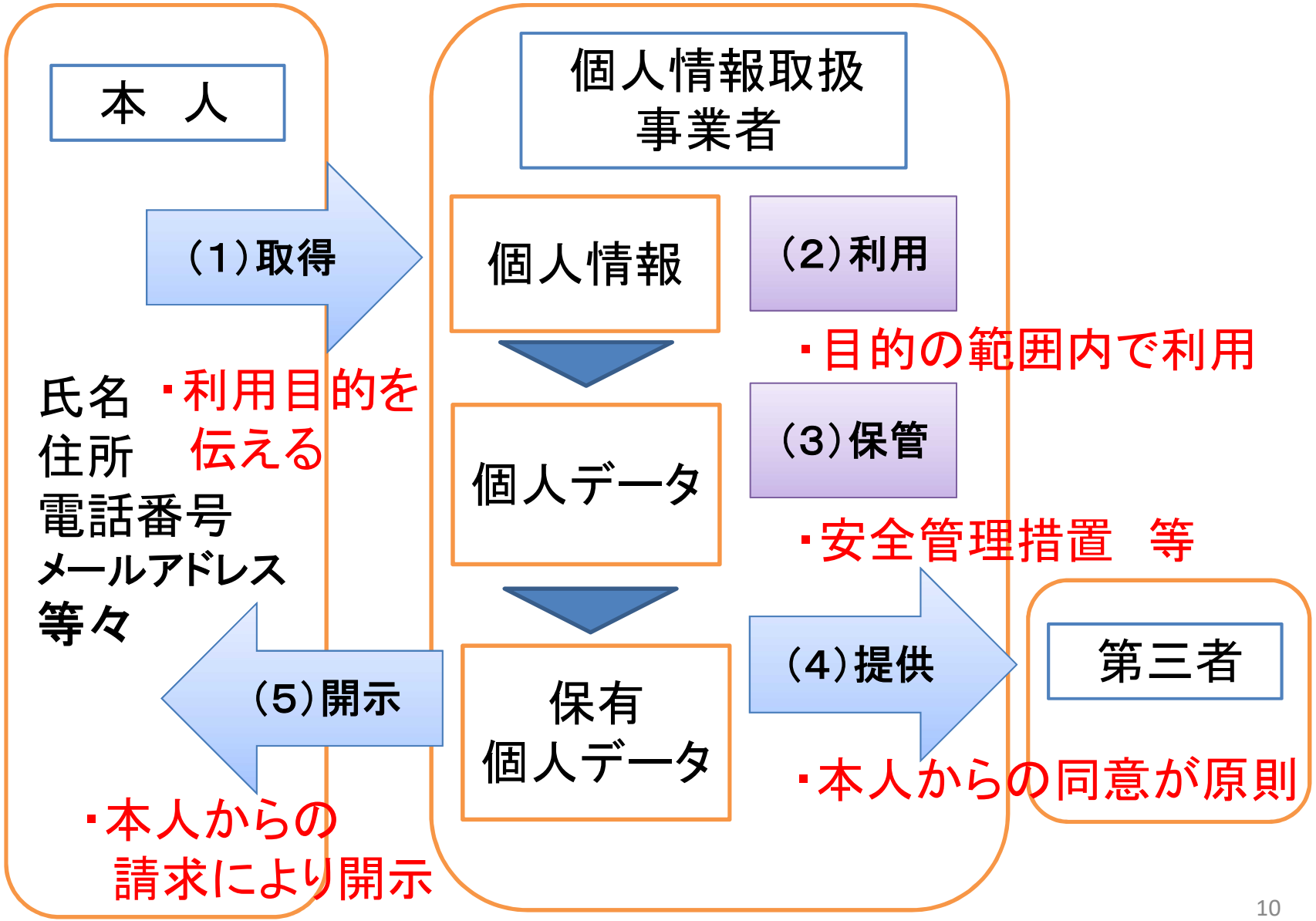
○取得や第三者提供に当たっては、事前に本人の同意が必要

○要配慮個人情報が含まれる個人データの漏えいが発生した場合には、個人情報委員会への報告及び本人への通知等を行う必要がある

⇒　自社で扱っている書類や個人データ等の管理は厳格に！

（特に従業員等の病歴、心身の機能障害、健康診断の結果　等）

◆個人情報取り扱いの基本ルール（5原則）



◆事業者における個人情報取り扱いの対策ポイント

①取得　・本人に対して、利用目的をできる限り分かり易く具体的に示す
・直接の利用目的に合わない、個人情報を取得しない
・十分な判断力を有しない子供などからの取得は、原則的にしない

②利用　・情報を取得するときに伝えた利用目的以外に個人情報を使わない
・誤送信、誤操作による情報漏洩が起きないようチェック体制を作る
・第三者提供が必要な場合は、利用目的に開示する
・後から第三者提供が必要になった時は、改めて本人の同意を得る

③委託　・委託先の安全管理体制を確認して委託契約を結ぶ（「委託元責任」）
・契約書の取り扱いルールが適切に行われているか定期的に確認
・委託先での個人情報の社外への持ち出しを禁止する
・システム開発時に個人情報の実データは（安易に）使わない

④保管　・社内のどこにどのような個人情報があるか整理し把握・点検する
・物理的安全管理措置、技術的安全管理措置を継続的に講じる

⑤問い合わせ　・窓口（担当部署）を明示して、存在を周知する
・開示要求等に応えられるよう個人情報を全社的に整理して管理

◆物理的安全管理措置（盗難対策 等）

参考

ⅰ．個人データを取扱う区域の管理

・個人データを取扱うことのできる従業者及び本人以外が、容易に個人データを閲覧できないような措置を講じる

ⅱ．機器及び電子媒体等の盗難等の防止

・個人データに係る機器、電子媒体、書類等を施錠できるキャビネット、書庫等に保管する

ⅲ．持ち運び時の対策

・パスワードの設定、個人データの暗号化、目隠しシールの添付、施錠できる搬送容器の利用等の対策を行う。置き忘れにも注意！

・従業員のスマホに入っている個人情報への対策にも留意

ⅳ．削除、廃棄

・書類の廃棄は、焼却、シュレッダーによる処理等復元できないように対処

・機器、電子媒体等はデータ削除ソフトウェアの利用や物理的破壊を行う

・責任者が廃棄を確認する

◆技術的安全管理措置

参考

AI時代到来の中、技術環境は日進月歩の状況！

ⅰ．アクセス制御とアクセス者の識別と認証

・個人情報を含むファイルにID/パスワードを設定する　等

ⅱ．外部からの不正アクセスの防止

・ウィルス対策ソフト等の導入および常に最新の状態にしておくこと（追っかけ子の常態化、世界レベルでのアクセス）

・最新の事件等を勘案し、適切なセキュリティ技術を選択・運用する（専門事業者等との連携）　等

ⅲ．システム利用時の漏えい防止

・メール添付ファイルへのパスワードの設定を行う　等

◆2022年4月1日改正施行のポイント

詳細は次頁

①漏えい等が発生し個人の権利利益を害するおそれが大きい場合、
委員会への報告及び本人への通知が義務化（現在は努力義務）

⇒　万が一に備え、漏えい等報告・本人通知の手順の準備を！

②個人の権利拡充
（利用停止・消去等の請求権、電磁的記録の提供　等）

⇒　安全管理措置の公表やデータ開示請求等への備えを強化

③利活用の推進（「仮名加工情報」の新設・・・ビッグデータ活用推進）

④ペナルティの厳罰強化…罰則引き上げ（特に法人対応強化）

⑤リクナビ事件再発防止（第三者提供時の事前本人確認の義務化）

⑥その他（法の域外適用・越境移転、不適正利用禁止　等々）

◆個人情報保護制度の官民一体化等(2023年4月改正施行)

◆漏えい等報告（委員会宛）・本人への通知の義務化

【漏えい等報告の義務化対象事案】

- 要配慮個人情報の漏えい
- 不正アクセス等による漏えい
- 財産的被害の恐れがある漏えい

} これらの類型は件数に関わりなく対象

- 一定数以上の（1000件超）大規模な漏えい

○要配慮個人情報の漏えい	・病院での患者の診療や調剤情報を含む個人データを記録したUSBメモリーを紛失 ・従業員の健康診断結果データ漏えい
○財産的被害のおそれがある漏えい	・クレジットカード番号を含む個人データ漏えい ・送金や決済機能のあるウェブサービスのログインIDとパスワードデータ漏えい
○不正の目的をもって行われた漏えい	・不正アクセスにより個人データが漏えい
○1000件を超える漏えい	・システムの設定ミス等によりインターネット上で1000人以上の個人データが閲覧可能な状態

◆委員会への報告は、速報（5日以内）、確報（30日以内）の2段階で必要

【2】

個人情報の漏えい問題と対策

【近年の情報漏えい状況】

①外部からの攻撃多発（サイバー攻撃やウィルス感染等）

・国家レベルでの介入、止まらない技術の高度化

②内部不正～今も頻繁に続く、企業の個人情報流出～

・社員や退職者、また委託先職員等さまざま

・大手損害保険会社（契約者情報250万件流用）等

③それでも一番多い「ヒューマンエラー」！

・人間による漏えい（“うっかりミス”など人は間違うもの）

・まだまだ残る“紙文化”（紛失、誤送付等、人は間違う）

④インターネット（SNS等）による情報流出の増加

・スマホ・パソコン等の普及の中、規範意識不十分

◆情報セキュリティ脅威2023

順位	個人	前年順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSNS等を使った脅迫・詐欺の手口による金銭要求	3位	標準型攻撃による機密情報の搾取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等のニューノーマルな働き方を狙った攻撃	4位

注　出典（（独法）情報処理推進機構より、次頁以降資料も同様）

◆フィッシングによる個人情報等の詐取

公的機関や金融機関、ショッピングサイト、宅配業者等の有名企業を騙るメールやSMSを送信し、正規のウェブサイトを模倣したフィッシングサイト（偽のWebサイト）へ誘導することで、認証情報やクレジットカード情報、個人情報を入力させ詐取する行為

攻撃者に詐取された情報を悪用されると金銭的被害等が発生する。具体的には、個人情報を販売されたり、詐取した認証情報で不正送金したり、物品を購入・転売したりすることで金銭を得ている

「警察庁2023レポート」によれば、2023年のインターネット関連の不正送金事案による被害件数は　5,578件（前年比391％増）、被害総額は約87.3億円
届け出件数においては約119万件と過去最高となっている

◆ランサムウェアによる被害

～組織の規模や業種は関係なし！次の標的はあなたの組織～

ランサムウェアはウィルスの一種。攻撃者はPCやサーバーを感染させ、様々な脅迫により金銭を要求する
さらに、攻撃者は複数の脅迫を組み合わせることで、攻撃を受けた組織がシステムを復旧するために金銭を支払うことを検討せざる得ない状況を作り出そうとする

【脅迫内容】

① PCやサーバーのデータを暗号化其の復元かと引き換えに金銭要求
②重要情報を窃取し、金銭を払わなければ情報を公開すると脅迫
③金銭を支払わなければ、感染事実を被害者の利害関係者に連絡する

【攻撃手口】

「OSやアプリケーション等のソフトウェア、VPN等の脆弱性を悪用してネットワークから感染」、「公開サーバーに不正アクセスして感染」「メールから感染（添付ファイルやリンク等）」等、様々な手口で侵入感染させる

●2022年230件、2023年197件、2024年は上期114件と高水準!（警察庁）
被害の予防対策、被害を受けた時の対応など整備・強化が必要

◆情報セキュリティ対策の基本

参考

攻撃の手口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウィルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

◆複数の脅威に有効な共通対策

①パスワードを適切に運用する　②情報リテラシー、モラルを向上させる
③メールの添付ファイルの開封や、リンク、URLのクリックを安易にしない
④適切な報告/連絡/相談を行う　⑤インシデント対応体制を整備し対応する
⑥サーバーヤクライアント、ネットワークに適切なセキュリティ対策を行う
⑦適切なバックアップ運用を行う　等々

◆個人情報漏えい事例（内部不正、ヒューマンエラー）

2023年10月　大手通信会社

（原因）元派遣社員がクライアントから預かっていた顧客情報を不正に持ち出した

（内容）顧客の氏名、住所、電話番号などの個人情報900万件流出。
盗んだ個人情報は、名簿業者に送付・売買し、2000万円以上の利益を得たと推察される

2022年4月　インフラ企業

（原因）緊急対応に関係する顧客データを委託先の会社にメールで送信した際、誤って関係のない個人情報を誤送信した

（内容）約12,000人分の個人情報流出。キャパシティーを超えた業務量が原因

2022年6月　尼崎市

（原因）全市民約46万人の住民基本台帳や生活保護受給世帯の口座情報などが流出

（内容）臨時特別給付金事務受託企業の再々委託先の社員が、データを無断で持ち出し、居酒屋で泥酔。バックアップ用のUSBメモリーを鞄ごと紛失

◆「2023年度「個人情報保護委員会」年次報告」

1）漏えい件数　　民間事業者　1万2120件（57%増）
　　行政機関等　　1159件（約10倍に増）

2）漏えい情報種類　～以下「民間事業者」の報告数値～
　・顧客情報（83.5%）、従業員（6.7%）、その他（13.3%）

3）情報の形態
　・紙媒体のみ（82%）、電子媒体のみ（12.2%）　の順

4）報告義務該当自由
　・要配慮個人情報を含む（89.7%）、財産的被害のおそれ（0.7%）
　　不正の目的をもって行われたおそれ（8.1%）、1000人超（4.6%）

5）漏えい原因
　・ヒューマンエラー（人的ミス）が90%近くを占める！
　　～ 誤交付（61.8%）、誤送付（16.5%）、紛失（4.3%）　の順

■ヒューマンエラーの防止対策

- 組織の個人情報の取扱いの規定・ルールを守る
- PCメール等の技術力・リスクリテラシーの向上を図る
- ヒューマンエラー発生リスクの高い方法による情報移転は、特に慎重に扱う
  - ファックス利用における注意事項
  - 個人情報は外に持ち出さない ⇒ 厳正なルールが必要
    （書類、USBメモリー、メールでのファイル転送　等々）
- 個人情報の漏洩の恐ろしさを認識する
- 個人情報を大切にする意識・習性を身につける。（社員教育）
  - 危険が潜在していることを認識する
  - 平気で個人情報が他人に知られる状況に置く
  - 公の場で人の個人情報の話を大声で話す

個人情報漏えいの責任・影響と人権侵害

◆個人情報を漏えいしてしまったら

・原因追求、問合せ対応、公表準備などに膨大な時間を費やす
・実際には、漏えい者が特定できなかったり漏えい者に賠償責任や履行能力が無いなどを理由に、企業に賠償責任を追及するケースが多い
・漏えい数によっては、厳しい問題指摘、責任追及そして多額のお詫び料も支払うことも多い

⇒　信用失墜、イメージダウン、存続危機　など

◆個人情報を漏えいされた人たちは・・・場合によっては

・執拗な勧誘の電話・メール等による精神的苦痛
・平穏な日常生活が脅かされる　＝　人権侵害　等を理解する

◆企業（組織）は、「加害者」（「被害者」であっても）になる

隠すのはダメ！ 迅速に、被害発生状況確認や原因を特定し法に従がって、被害者に連絡し、対応に最善をつくすこと

◆求められる組織としての管理ポイント

①**責任者を明確**にし、**管理体制等を周知・徹底**

②日常業務の中の重要事項として、漏洩等の異常は、**（報・連・相）の対象**として徹底

③**セキュリティ対策の基本をはずさず、強化を**！

・研修・教育等での意識改革の継続、点検強化

・帳票やファイル等の日常管理ルール厳正化

（持ち出し禁止、アクセス制限、PSW管理・・・）

・パソコン等のウィルスソフト等は最新状態に！

・外部委託はしっかり相手先を把握する　等々

【３】

インターネット（ＳＮＳ等）の利用拡大と人権問題

注）ＳＮＳとは、
　　ソーシャルネットワーキングサービスの略

◆インターネット上での人権侵犯事件状況！

＜インターネット上の人権侵犯事件（新規開始）＞

	2013年	2018年	2023年
インターネット上の人権侵犯	957件	1,910件	1,824件
うち　プライバシー侵害	600件	849件	542件
うち　名誉棄損	342件	667件	415件

（出典法務省）

〇2023年の当該事件の処理は、被害者自らが削除依頼する方法を教示するなどの「援助」が半数近くを占めるが、人権擁護機関が違法性を判断したうえで、プロバイダ等に対し削除を求める「要請」を行った件数は449件。また、2023～25年の3年間の「要請」のうち、削除対応された件数は954件で、その割合は69.08%。

◆ネット上の誹謗・中傷・デマ

インターネットで自身の意見を自由に発信できることが一般的になった今、自身の発信で他者を誹謗・中傷したりデマで社会的混乱を引き起こしたり等問題となる場合が増えている。発信した内容によっては裁判沙汰になったり、経済的損失を被ったりすることもある
また、AI技術の発達により嘘か本当か見分けのつかない情報が錯綜することもあり、一層注意が必要
要因としては、「匿名での発信なら、身元を隠せると誤解する」、「第三者が、悪意の有り無しに関係なく、真偽を確認せずに拡散してしまい、伝言ゲームのように別の第三者がさらに拡散させることで広がっていく」 などが考えられる

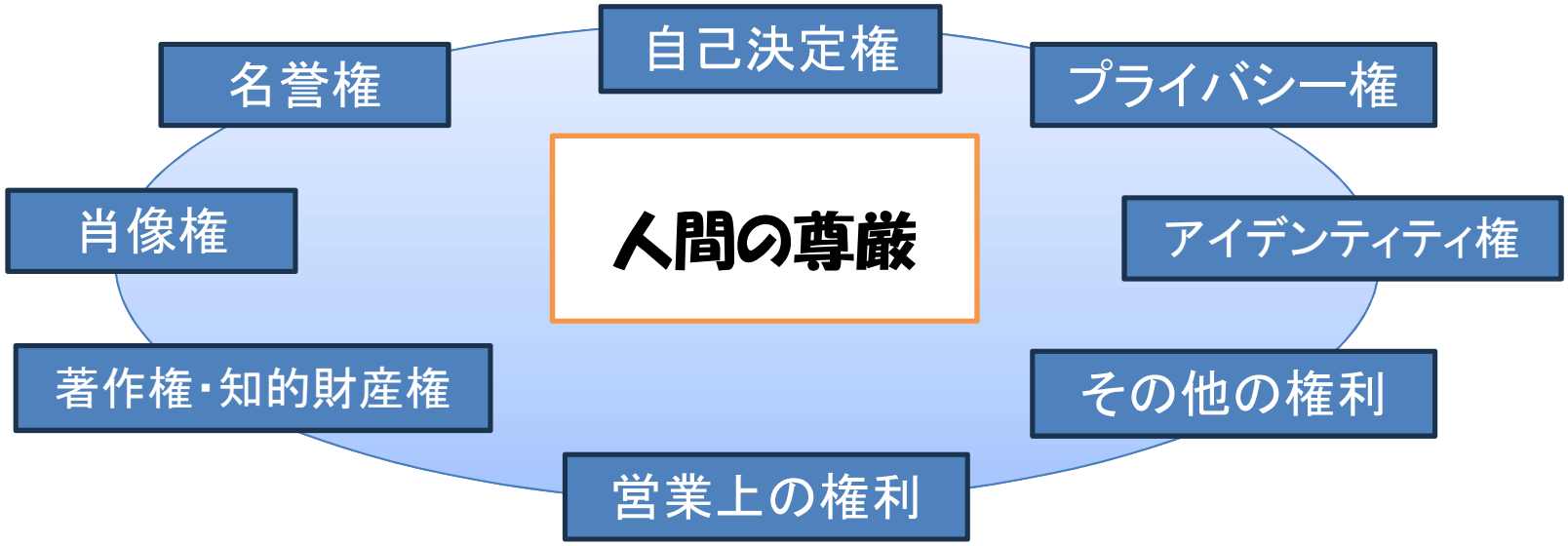
05

- **SNS上の誹謗・中傷問題が拡大し社会問題化。行政も対策を強化している。（侮辱罪の厳罰化、発信者情報開示請求 等）**
  また、プロバイダーへの要請・連携も強化しているが・・・

●一層の情報社会の充実に向けた規範や制度作りが不可欠！

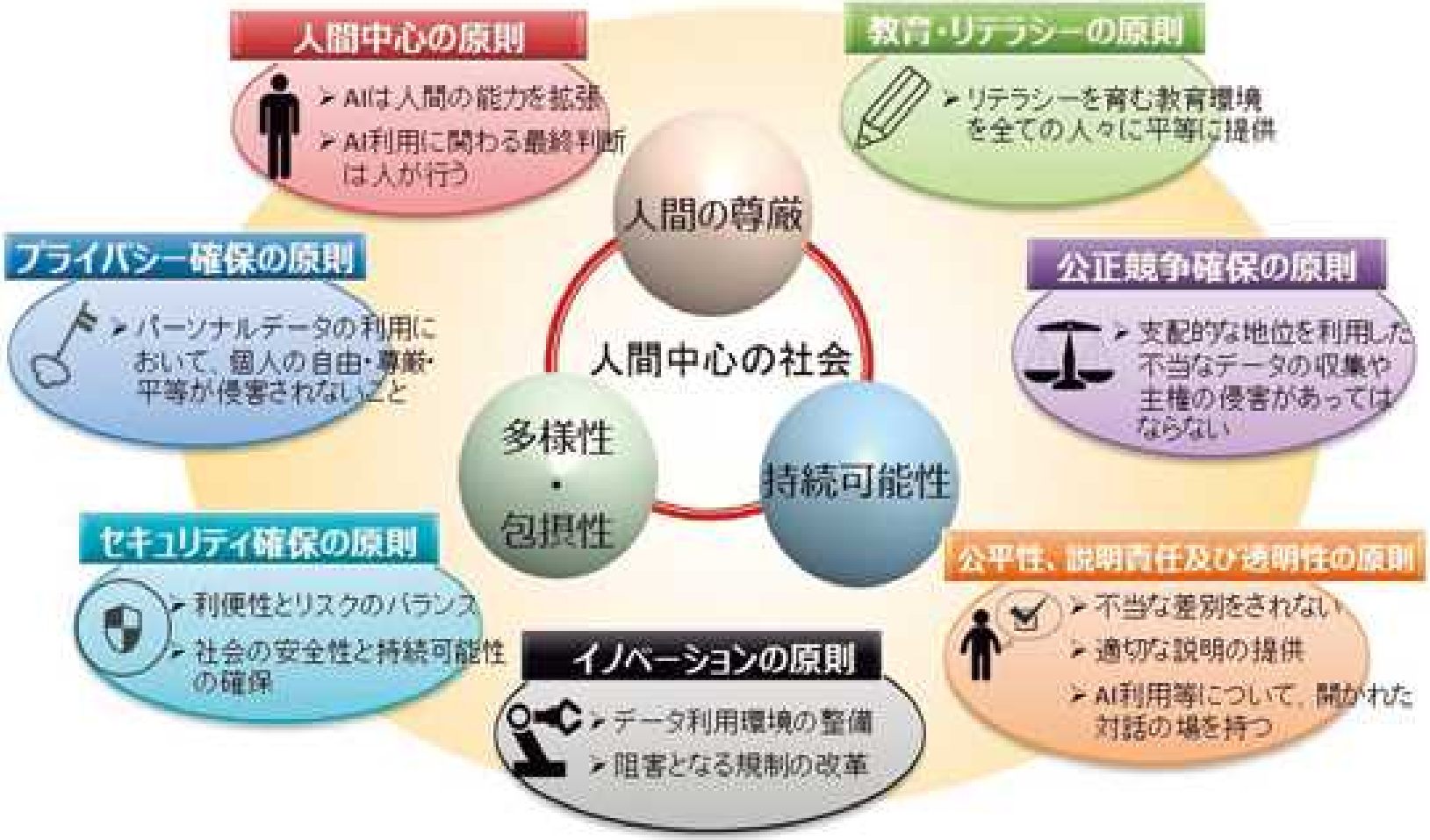
◆インターネット利用による権利侵害

①情報発信による他人の権利の侵害
②ソーシャルメディア等による自分の権利の侵害
③インターネットサービスを介した消費者取引の増大と
　新たな消費者被害の出現
④AIの急速な進展・拡大の中で、人間の尊厳を守る！



参考

人間中心のAI社会原則の概要



（2019年内閣府「統合イノベーション戦略推進会議」より抜粋）

■SNS利用のポイント 「自覚と責任」

〇ネット社会の現状（本質）を理解する

たとえ、個人間のやりとりであっても、SNS＝「公」の場であり、次の特質を理解する

①真偽に関わらず、すべての記録や個人情報が未来永劫残される。削除は容易でない

②誰でもアクセス・発信可能

③瞬時に伝播する（スピード、拡散範囲）

④匿名性（？） 本当の匿名性はない

〇人のネット社会に対する意識が技術の発展に追いついていないことが、ゆがみの原因のひとつ

つまり、本質は使う側の問題ともいえる

今、社会的規範作りが喫緊の世界的課題！

（再掲）

◆求められる「情報モラル」とは？

人権尊重のための情報モラル

「情報を取り扱う際に求められる考え方と行動」

個人の尊重

人格の尊重　・プライバシー　・名誉・信用　・表現の自由

安全への配慮

・個人情報保護
・情報セキュリティ
・リテラシー教育

社会的公正への配慮

・消費者保護、知的財産権保護
・デジタル・ディバイド対応　等
（様々な「情報格差」の解消）

◆組織における情報モラルの構築（まとめ）

1. 情報モラルに関する組織のポリシーを策定
   「基本方針」・・・経営者が自社の基本的な考え方と姿勢を示す
   「行動基準」・・・基本方針を実現するためにとるべき行動や対策の指針
   「運用ルール」・・・行動基準を日常業務に落とし込んだ実施マニュアル
2. 情報の棚卸しとリスクの把握（人権DDの「未然防止」に該当）
   自社の扱っている情報を洗い出し、人種、安全、社会的公正等の視点から
   どのようなリスクと脅威を抱えているか検討・評価し、回避・軽減策を講じる
3. 社内の情報モラル啓発取り組み
   ・各自の職務・役割・責任に応じた内容で、研修・啓発活動の継続的実施
4. 最新の事故情報等を収集し、適切なセキュリティ技術選択を！
5. 対策の評価・見直しの組織的仕組作り（「PDCAサイクル」）
6. 問題発生時の体制づくり（トップの率先取り組み）

ご清聴ありがとうございました！

明るく活気に満ちた社会
であり続けるために、
お役に立てれば大変嬉しいです