ZeroBIO研究プロジェクト

第1回ワークショップ「生体情報のプライバシー」

バイオメトリクスの利用と個人情報保護法

筑波大学大学院　図書館情報メディア研究科
助教授　新保　史生

バイオメトリクスの利用に伴う法的課題

- a）予測不能な目的での利用（Function Creep）の問題
- b）監視手段としての利用に関する問題
- c）同意原則に基づく利用と透明性の確保の問題

検討事項

①法制度
　バイオメトリクスの利用に係る法整備の問題

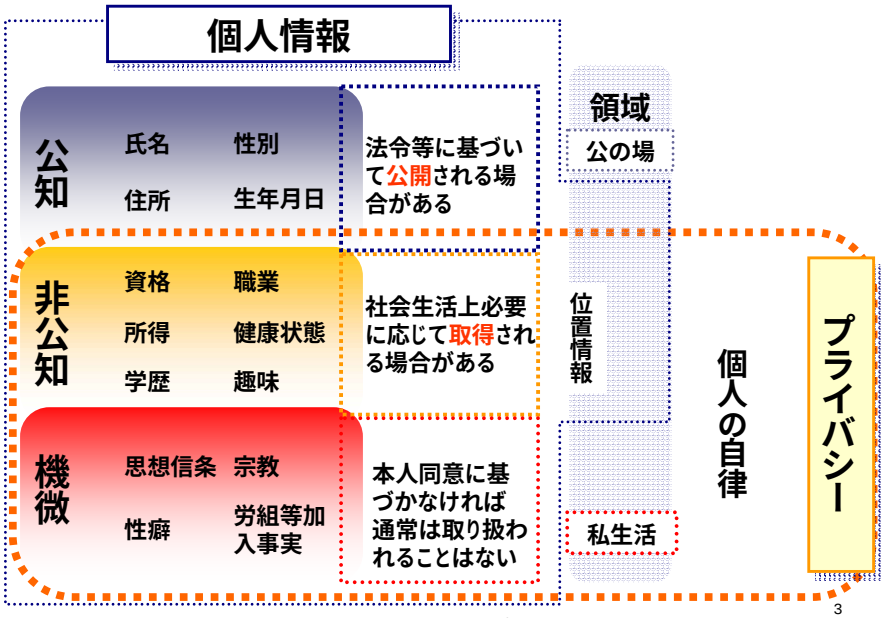
②指針や課題解決のための枠組みの方向性
　バイオメトリクスの利用に係る基本的な枠組みや指針の策定、諸課題への対応のあり方

③技術的検討課題
　耐タンパ性やPETsの利用など

OECD, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY, COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, BIOMETRIC-BASED TECHNOLOGIES,(30 June 2004).

BIOVISION, Privacy Best Practices in Deployment of Biometric Systems(2003)を参考に作成

個人情報とプライバシーの関係



個人情報の取扱い及びプライバシー保護との関係における問題

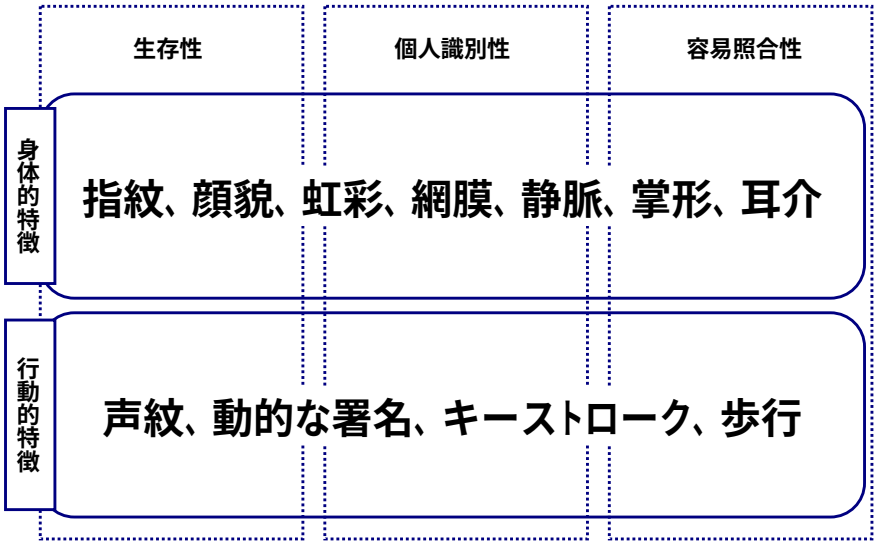
- 1－1　個人情報の取得及び利用にあたっての問題
  - バイオメトリクスを利用するにあたって取得される個人情報
  - 必要最小限のバイオメトリック･データの取得
    - 最低限度の個人データの保有
  - プライバシー侵害リスクの低減のための対応
  - なりすましへの対応
- 1－2　公正かつ適法な処理
  - 取得対象となる個人情報の特定
  - バイオメトリクスの利用目的の明確化
- 1－3　過剰利用や差別助長のリスクへの対応
  - バイオメトリック･データの本来の利用目的を逸脱した利用に伴う個人の権利利益の侵害
  - バイオメトリクスを用いた認証を利用できない身体的障害に起因する差別
  - 誤った本人拒否･他人受入に伴う問題

個人情報の取扱い及びプライバシー保護との関係における問題

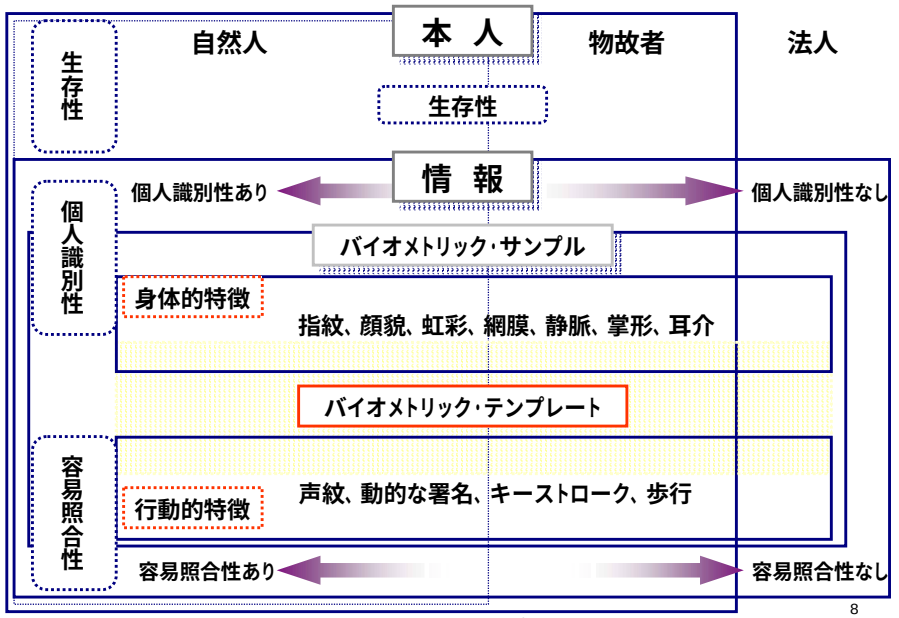
- 1－4　センシティブ･データの取扱い
  - テンプレート以外に副次的に取得される個人情報の問題
  - 副次的情報の抽出に伴いセンシティブ･データを結果的に取得してしまう場合の問題
- 1－5　他の情報との照合や関連づけ（マッチングやリンケージ）の問題
  - バイオメトリック･データと他の個人情報との結合
  - 他の組織が保有する情報との結合や共同利用に伴う問題
- 1－6　バイオメトリック･データの自動処理に伴う問題
  - 特定個人の情報の自動集積や追跡に伴う問題
  - 一度取得されたデータが際限なく自動処理されることによる問題
- 1－7　バイオメトリクスを利用したモニタリングの問題
  - 1対1認証と1対N認証それぞれの場合の問題
- 1－8　バイオメトリック･データの安全管理
  - サーバ認証とクライアント認証モデルそれぞれにおける個人データの安全管理上の問題

バイトメトリクスの利用と個人情報の取扱い

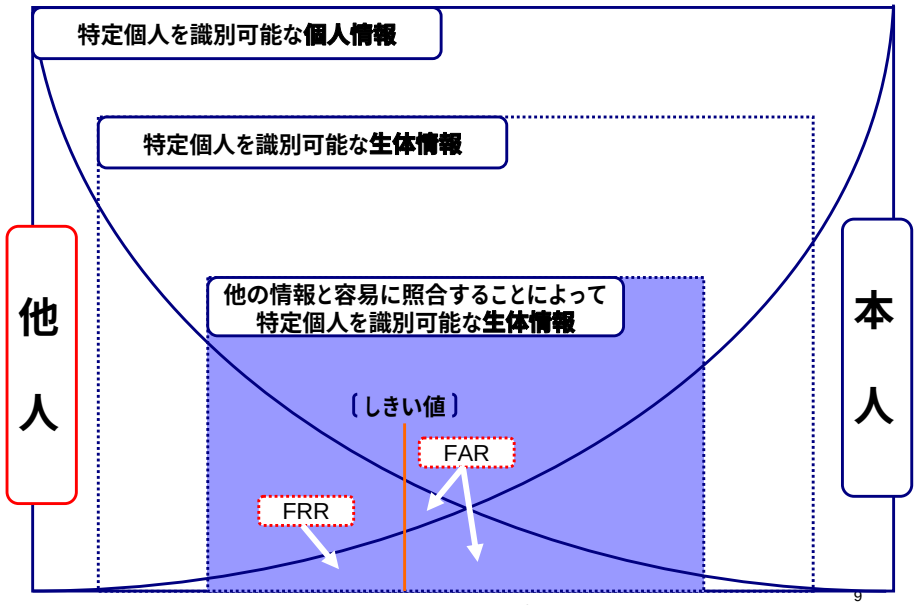
バイオメトリック・データと個人情報



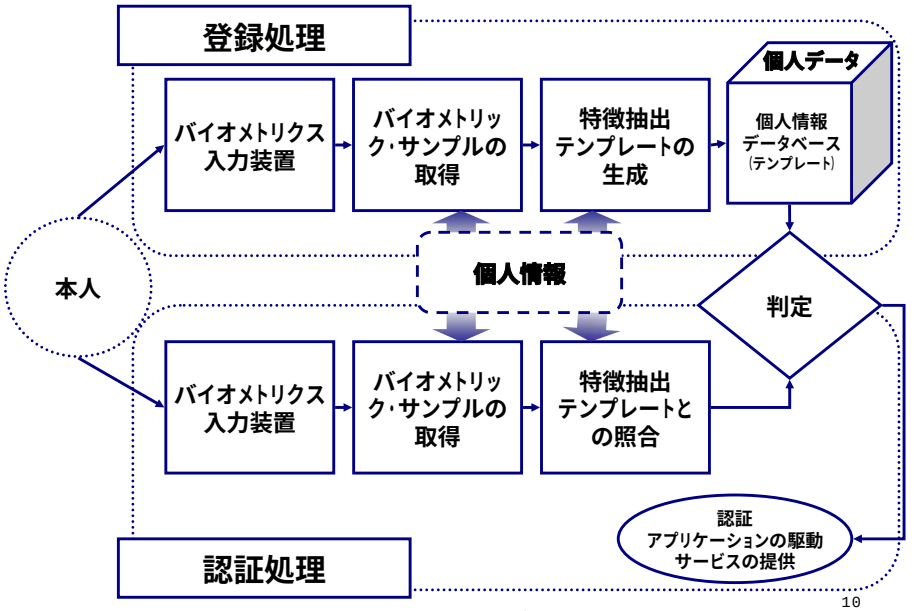
バイオメトリック・データと個人情報



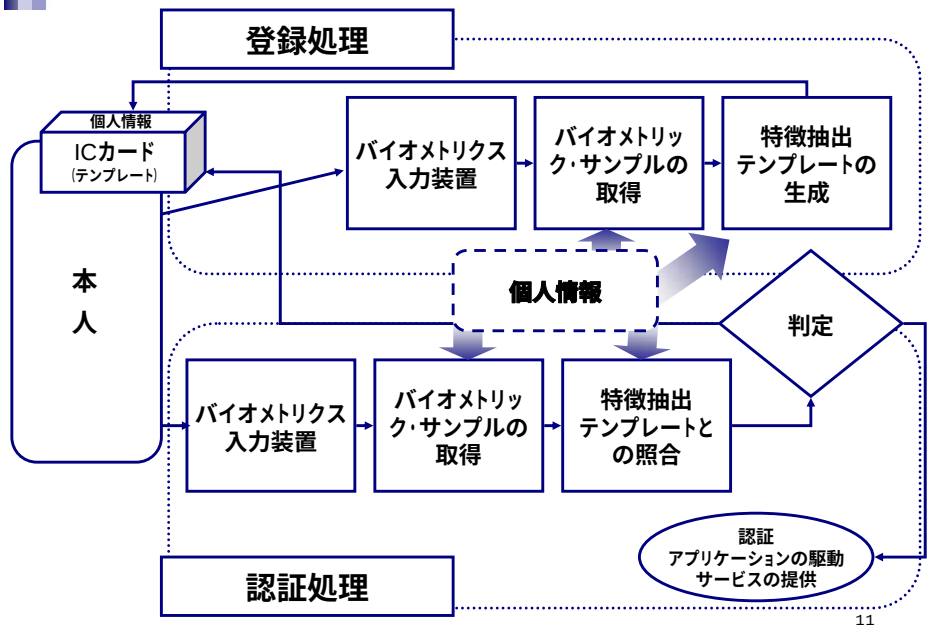
FAR/FRRと個人識別性



サーバ認証モデルにおける個人情報（個人データ）への該当性

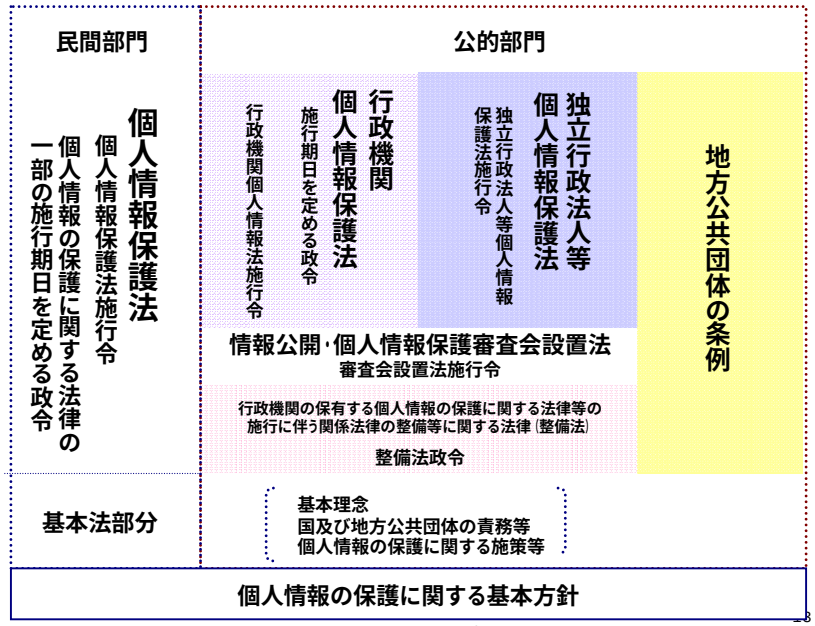


クライアント認証モデルにおける個人情報の取扱い

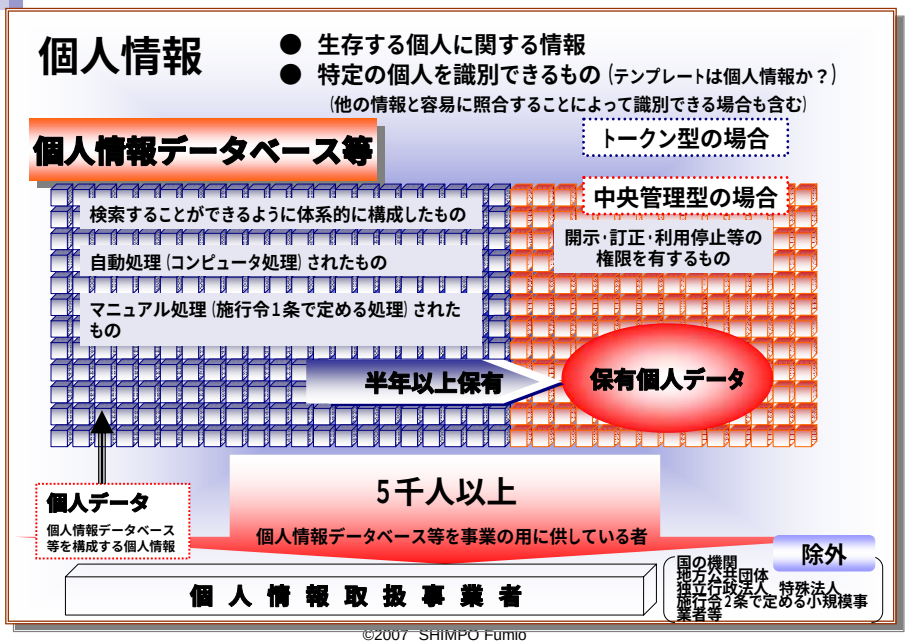


個人情報保護制度

個人情報保護制度



バイトメトリクスの利用と個人情報の取扱い



3　個人情報取扱事業者の義務

個人情報

- **利用目的の特定、利用目的による制限**（15条、16条）
  個人情報を取り扱うに当たり、その利用目的をできる限り特定
  特定された利用目的の達成に必要な範囲を超えた個人情報の取扱いの原則禁止
- **適正な取得、取得に際しての利用目的の通知等**（17条、18条）
  偽りその他不正の手段による個人情報の取得の禁止
  個人情報を取得した際の利用目的の通知又は公表
  本人から直接個人情報を取得する場合の利用目的の明示
- **苦情の処理**（36条）
  個人情報の取扱いに関する苦情の適切かつ迅速な処理

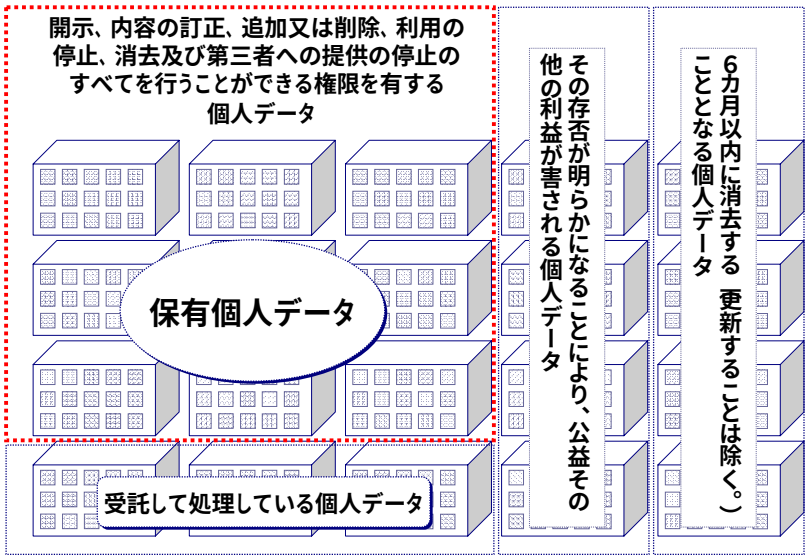
個人データ

- **データ内容の正確性の確保**（19条）
  利用目的の達成に必要な範囲内で個人データの正確性、最新性を確保
- **安全管理措置**(20条)
  個人データの安全管理のために必要かつ適切な措置
- **従業者・委託先の監督**（21条、22条）
  従業者･委託先に対する 必 要かつ適切な監督
- **第三者提供の制限**（23条）
  本人の同意を得ない個人データの第三者提供の原則禁止

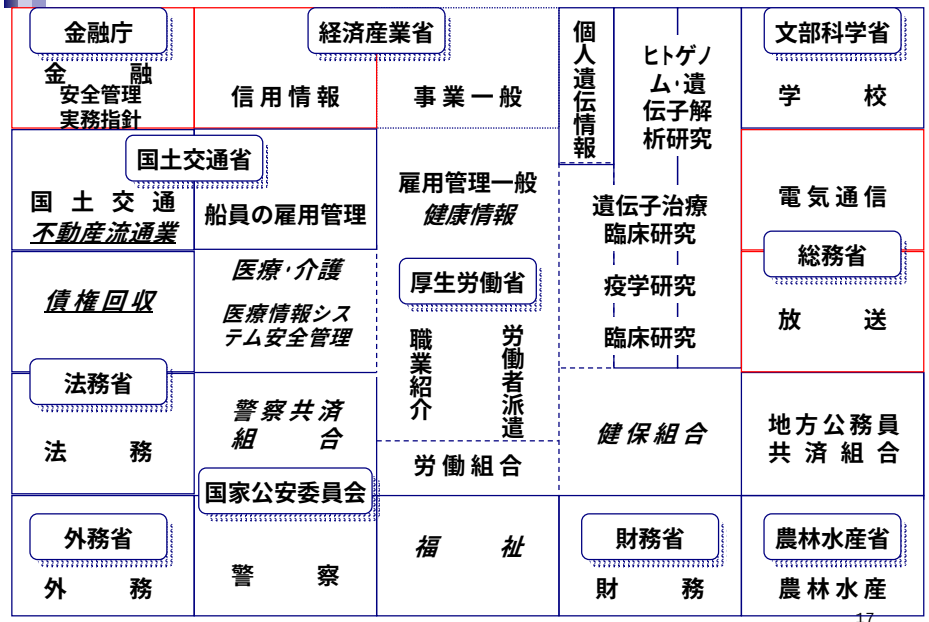
保有個人データ

- **保有個人データ事項の公表等**（24条）
  保有個人データの利用目的、開示等に必要な手続等についての公表等
- **開示、訂正等、利用停止等**（25～27条）
  保有個人データの本人からの求めに応じ、開示、訂正等、利用停止等
- **理由の説明**（28条）
  本人関与に関する理由の説明
- **開示手続、手数料**（29条、30条）

保有個人データとして管理するバイオメトリック・データの限定の必要性



バイオメトリクスの取扱いに関するガイドライン（指針）



＊斜体は通達／下線は通知

「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」

平成17年1月6日金融庁告示第1号

基本方針の整備

取扱規程の整備

点検・監査規程の整備

外部委託規程の整備

センシティブ情報に該当する生体認証情報の取扱いに関する特別の措置

センシティブ情報の取扱いに関する特別の措置

管理段階ごとの安全管理に係る取扱規程

安全管理措置に係る実施体制の整備

安全管理措置等についての実務指針の概要

- **センシティブ情報に該当する生体認証情報の取扱いに関する特別の措置**
  - □なりすまし登録防止
  - □必要最小限の取得
  - □生体情報の消去
  - □不正認証防止措置
  - □代替措置の厳格性
  - □分別管理
  - □保存時の暗号化
  - □外部監査等

安全管理措置等についての実務指針の概要

- **センシティブ情報の取扱いに関する特別の措置**
  - □ガイドラインに定める目的のみの取得、利用
  - □取扱者の必要最小限の限定、アクセス制御
  - □本人同意取得及び本人への説明
  - □必要に応じた外部監査等

バイオメトリクスの利用と個人データの安全管理

取得・入力

移送・送信

利用・加工

保管・バックアップ

消去・廃棄

従業者の役割・責任の明確化

※個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。

個人情報保護管理者の設置

作業責任者の設置及び作業担当者の限定

個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）

情報システム運用責任者の設置及び担当者の限定

個人データを取り扱う情報システム

部署毎の役割と責任の明確化

個人データの取扱いに係わるそれぞれの部署

監査実施体制の整備

監査責任者の設置

報告連絡体制の整備

代表者への報告

個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合

個人データの漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合

※個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい。

漏えい等の事故による影響を受ける可能性のある**本人**への情報提供体制の整備

主務大臣及び**認定個人情報保護団体**等への報告

漏えい等の事故発生時

整備

運用

個人データの取扱いに関する規程等

個人データを取り扱う情報システムの安全管理措置に関する規程等

個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等

個人データの取扱の委託

受託者の選定基準

委託契約書のひな型等

監査証跡の保持

個人データに関する情報システム利用申請書

特定の従業者に特別な権限を付与するための権限付与申請書

情報システム上の利用者とその権限の一覧表

建物等への入退館（室）記録個人データへのアクセスの記録

教育受講者一覧表　等

個人データの取扱い状況を一覧できる手段の整備

個人データの取扱い状況を一覧できる手段

- 取得する項目
- 保管方法
- 通知した利用目的
- アクセス権限を有する者
- 保管場所
- 利用期限
- その他個人データの適正な取扱いに必要な情報

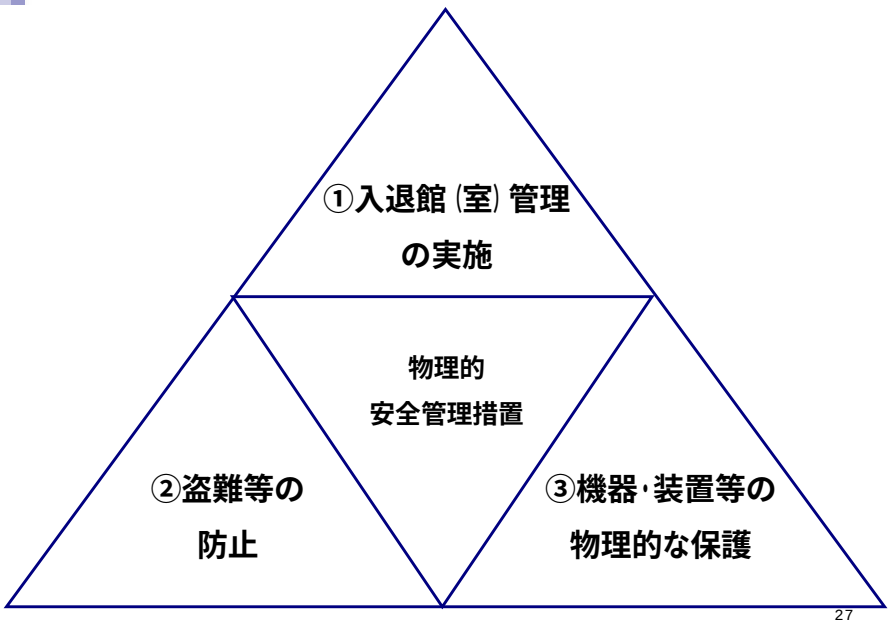
整　備

個人データ取扱台帳の内容の定期的な確認による
最新状態の維持

人的安全管理措置

1. ①なりすましによる登録の防止
2. ②従業者に対する教育･訓練の実施
3. ③個人データを取り扱う従業者の雇用契約時及び委託契約時における非開示契約の締結

物理的安全管理措置



技術的安全管理措置

- ①個人データへのアクセスにおける識別と認証
- ②個人データへのアクセス制御
- ③個人データへのアクセス権限の管理
- ④個人データのアクセスの記録
- ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
- ⑥個人データの移送･送信時の対策
- ⑦個人データを取り扱う情報システムの動作確認時の対策
- ⑧個人データを取り扱う情報システムの監視

認証装置の共有と個人データの共同利用

ア）共同して利用される個人データの項目

共同して利用するバイオメトリック・サンプル／テンプレート
認証装置を利用するための登録者・利用権者本人に関する個人データ

イ）共同利用者の範囲

認証装置を共同して利用する者の範囲

ウ）利用する者の利用目的

共同して利用する個人データのすべての利用目的

エ）個人データの管理について責任を有する者の氏名又は名称

認証装置の管理について責任を有する者

変更 → 本人同意

変更 → 通知／本人の知り得る状態に置くこと

開示等の求めへの対応

本人

利用目的の通知

開　示

訂　正

追　加

削　除

利用の停止又は消去

第三者への提供の停止

開示等

訂正等

利用停止等

個人情報取扱事業者

個人情報の漏えい等に対する法的責任

個人情報の漏えい等の態様

内的要因

外的要因

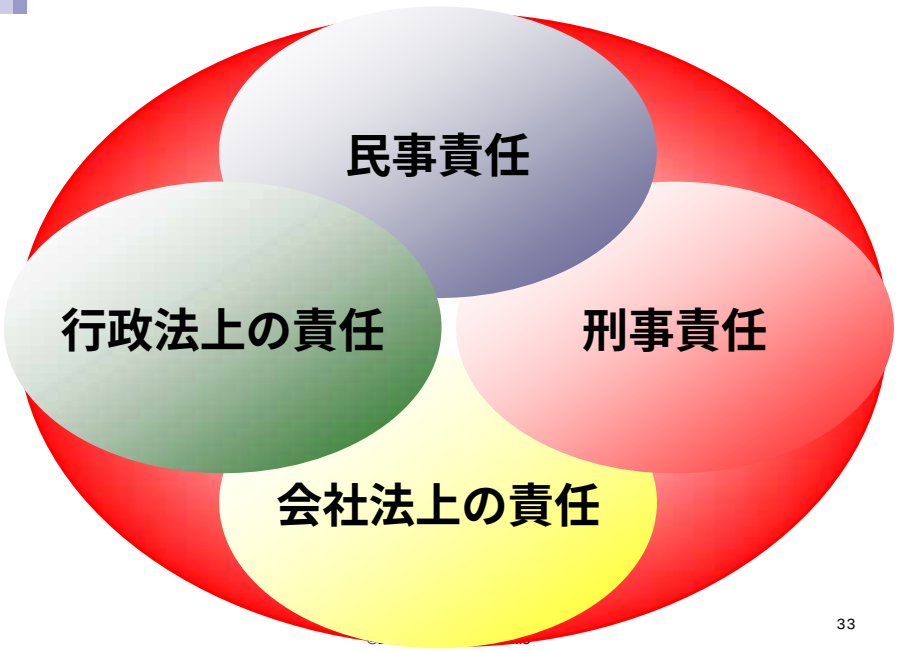
- 従業者の故意による漏洩
- 従業者の過失による漏洩
- 外部委託業者等による故意の漏洩
- 外部委託業者等の過失による漏洩

人的要因

- ウィルス感染による個人情報の毀損・滅失
- ワームの繁殖による個人情報の漏洩
- 内部システムの欠陥による漏洩
- 外部システムの欠陥による漏洩
- 外部委託等によって構築したシステムの欠陥による漏洩
- 不正アクセスによる漏洩
- 災害による情報の滅失、き損

システム的要因

法的責任の類型



リスク管理と経営者の責任(取締役・監査役のリスク管理義務)

大和銀行株主代表訴訟第一審判決(大阪地判平成12年9月20日)

健全な会社経営にあたってのリスク管理体制の整備義務

健全な会社経営を行うためには、目的とする事業の種類、性質等に応じて生じる各種のリスク、例えば、信用リスク、市場リスク、流動性リスク、事務リスク、システムリスク等の状況を正確に把握し、適切に制御すること、すなわちリスク管理が欠かせず、会社が営む事業の規模、特性等に応じたリスク管理体制(いわゆる内部統制システム)を整備することを要する。

取締役会によるリスク管理体制の導入の決定

重要な業務執行については、取締役会が決定することを要するから(商法260条2項)、会社経営の根幹に係わるリスク管理体制の大綱については、取締役会で決定することを要し、業務執行を担当する代表取締役及び業務担当取締役は、大綱を踏まえ、担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う。

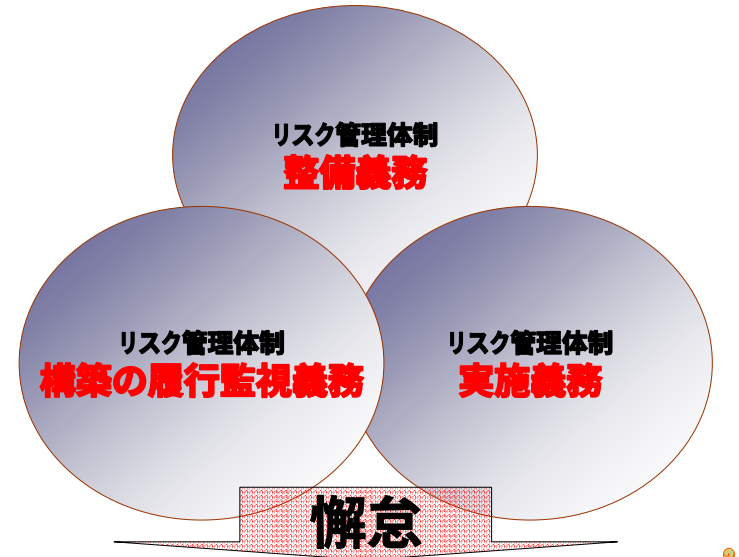
リスク管理体制の整備及び実施に関する取締役の義務

取締役は、取締役会の構成員として、また、代表取締役又は業務担当取締役として、リスク管理体制を構築すべき義務を負い、さらに、代表取締役及び業務担当取締役がリスク管理体制を構築すべき義務を履行しているか否かを監視する義務を負うのであり、これもまた、取締役としての善管注意義務及び忠実義務の内容をなすものと言うべきである。

監査役によるリスク管理体制の監視義務

監査役は、商法特例法22条1項の適用を受ける小会社を除き、業務監査の職責を担っているから、取締役がリスク管理体制の整備を行っているか否かを監査すべき職務を負うのであり、これもまた、監査役としての善管注意義務の内容をなすものと言うべきである。

リスク管理に係る取締役の善管注意義務及び忠実義務の内容



取締役の善管注意義務及び忠実義務違反として
会社に対する損害賠償責任

会社法の定める内部統制システムの構築の義務化

取締役の職務執行が法令･定款に適合すること

会社の業務の適正を確保するための体制の構築の基本方針の決定を義務付け

株式会社の業務の適正を確保する体制

①取締役の職務の執行に係る情報の保存及び管理に関する体制

②損失の危険の管理に関する規程その他の体制

③取締役の職務の執行が効率的に行われることを確保するための体制

④使用人の職務の執行が法令及び定款に適合することを確保するための体制

⑤当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

プライバシー侵害による法的責任

「『宴のあと』事件」判決（東京地判昭和３９年９月２８日判時３８５号１２頁）

プライバシーの権利

私生活を**みだりに**公開されないという法的保障ないし権利

プライバシー侵害による不法行為の成立要件

①公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること

② 一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること

③ 一般の人々に未だ知られない事柄であること

「宴のあと」事件以前にプライバシーの権利について言及した判例

「大阪証券労組保安阻止デモ事件」（大阪高判昭和３９年５月３０日判時３８１号１７頁）

国民の私生活の自由が国家権力に対して保障されていることを知ることができる。ここから**プライバシーの権利**を導き出すことができるであろうが、もとより無制限なものではない。

人はその承諾がないのに自己の写真を撮影されたり世間に公表されない権利（肖像権）を持つとすれば、それは**プライバシーの権利**の一つとして構成することができる。

その他、モデル小説とプライバシーが問題となった事例

「『名もなき道を』事件」判決（東京地判平成7年5月19日判時1550号49頁）

「『石に泳ぐ魚』事件」判決（東京地判平成11年6月22日判例時報1691号91頁）

情報照会への対応と法的責任

「京都市前科照会事件」判決（最判昭和５６年４月１４日民集３５巻３号６２０頁）

前科及び犯罪経歴（以下「前科等」という。）は人の名誉，信用に直接にかかわる事項

前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有する

市区町村長が，本来選挙資格の調査のために作成保管する犯罪人名簿に記載されている前科等をみだりに漏えいしてはならない

市区町村長が漫然と弁護士会の照会に応じ、犯罪の種類、軽重を問わず、前科等のすべてを報告することは、公権力の違法な行使にあたると解するのが相当

正確性の確保と法的責任

京都地裁平成１５年１０月３日判決

大手消費者金融が債務者と間違えて支払の催促をしたため、原告の個人情報を抹消し，今後支払催促をしない旨の約束をしたにもかかわらず，再度債務者と間違われて支払の催促をされ，これにより精神的損害を被ったとして，不法行為に基づく損害賠償を求めた事件

個人情報の取扱い

氏名（漢字氏名とカタカナ氏名），生年月日，自宅電話番号，住所，勤務先等の個人情報を端末に登録して社内記録として保存

全国信用情報センター連合会加盟の信用情報機関及び同連合会と提携する信用情報機関並びに株式会社シーシービー（これらを以下「関連信用情報機関」という。）に提供

Aが貸金債務の履行を延滞

債務の支払催促

Aの連絡先不明

住民票の写しの交付請求

氏名が類似した別人の住民票を京都市が交付

住民票記載住所をもとにNTTの電話番号案内で自宅電話番号を調査

電話番号と住所を修正

督促状を送付

取り違えが判明

誤情報の抹消を約束

社内端末 抹消せず

関連信用情報機関 登録状態が継続

再度支払催促

正確性の確保と法的責任（判決の要旨）

被告及び関連信用情報機関が取得した原告本人の個人情報

原告のカタカナ氏名，住所及び電話番号

個人識別のための単純な情報

他人に知られることを望まない情報
取得先が消費者金融業者

法的保護に値する

抹消するとの約束に違反

＋

少なくとも1年数か月間にわたりその個人情報を保有し続けた

自己情報コントロール権としての原告のプライバシー権を侵害

自己の個人情報が悪用されて社会的に不利益を受けるのではないか等と強い不安感を抱き続け，もって精神的損害を被ったことが認められる

不法行為が成立

個人情報保護法に基づく責任
従事者の義務・罰則（公的部門）

注：民間部門（個人情報取扱事業者）については、
個人データの漏えい等を直接処罰の対象とする
罰則規定は置かれていない。

従事者の義務

業務に関して知り得た個人情報の内容

みだりに他人に知らせること

不当な目的に利用

従事者の義務違反

従事者の義務の対象となる個人情報

業務に関して知り得た個人情報

コンピュータ処理　マニュアル処理

すべての個人情報が対象となる

公知の個人情報

非公知の個人情報
（他人に知られ**ていない**情報）

機微な個人情報
（他人に知られ**たくない**情報）

秘匿性（個人の秘密）

プライバシー

行政機関等個人情報保護法の罰則規定

罰則規定

- 罰則規定の内容
  - (1) 正当な理由なく個人の秘密に属する事項が記録された個人情報ファイルを提供したとき
  - (2) 業務に関して知り得た保有個人情報を自己若しくは第三者の不正な利益を図る目的で提供又は盗用したとき
  - (3) 職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集したとき

罰則規定の構成

個人情報 第55条
- ●専らその職務の用以外の用に供する目的
- ●職権を濫用して個人の秘密を収集

保有個人情報 第54条
- ●業務に関して知り得た保有個人情報
- ●自己若しくは第三者の不正な利益を図る目的で提供又は盗用

個人情報ファイル 第53条
- ●正当な理由なく
- ●個人の秘密に関する事項が記録された個人情報ファイル
- ●提供

罰則規定第５３条の適用対象となる個人情報