

ユビキタス環境における プライバシー問題 - 監視社会化の動向を踏まえて -

筑波大学 図書館情報学系 助教授
新保 史生

2004年2月19日(木) 15:00-16:00

知的コミュニティ基盤研究センター
研究談話会

ユビキタス環境



監視社会

におけるプライバシー侵害の特徴

トレーサビリティと
プライバシー侵害の危険性

新たな監視・追跡技術の開発によって、本人が不知・不識のうちに、容易かつ効率的に監視や追跡を実施することが可能になったことによって生ずるようになった問題

既存の監視・追跡手段の利用機会の増加と
常態化に伴うプライバシー意識の希薄化

監視・追跡手段が日常的にあらゆる場面で利用される結果、監視される側が、そのような環境に順応してしまうことによって生ずる問題

顕著な例

ネットワーク
監視

クッキー
スパイウェア
各種ログ
ウェブビーコン
固有の識別アドレス
KLS(キーロガー)

非接触型の
監視技術

ICカード
RFIDなど

監視カメラ

街頭防犯カメラシステム
Nシステム(自動ナンバー読み取りシステム)
成田空港・関西空港税関の顔貌認識カメラ
街頭緊急通報システム(スーパー防犯灯)
商店街など、地域コミュニティにおける監視カメラの設置
民間の事業者による防犯目的での設置

民間の事業者による効率的なマーケティング実現の手段 / 政府による監視手段

監視手段の利用機会増加の背景

公共の安全確保

国の安全保障

犯罪捜査

マーケティングの
変革

政府による監視手段利用の正当化の根拠

犯罪発生率の増加やテロ対策
現実の脅威の予防と解決がなされる
ことへの社会的期待の増大


社会的に導入を求める理由の存在

ユビキタス・マーケティングの実現

民間事業者における監視手段活用の推進

新技術の開発、技術障壁の解消

監視技術の高度化、小型化、ネットワーク化、低価格化等による導入の容易性
効果的な情報分析技術の開発
各種認識技術（虹彩、顔貌、指紋、声紋など）やフィルタリング技術の高度化



米国における最近の導入例 (9 / 1 1 以降)

US-VISIT

米国出入国状況表示技術
U.S. Visitor and Immigrant Status Indicator Technology
顔貌・指紋の登録とデータベース化

MATRIX

州際間対テロ情報交換パイロットプロジェクト
The Multistate Anti-Terrorism Information Exchange
テロ関連情報のデータ・マイニングと情報共有

ASDIS / ASRS

データマイニング及び航空保安計画
Data Mining and Aviation Security (NASA)
航空データ統合システム (**Aviation Security Data Integration System**)
航空安全報告システム (**Aviation Safety Reporting System**)
テロ脅威予測プログラム

CTS

戦闘地域監視計画
Combat Zones That See
米国の国内走行全車両の追跡・分析システム

CAPPS

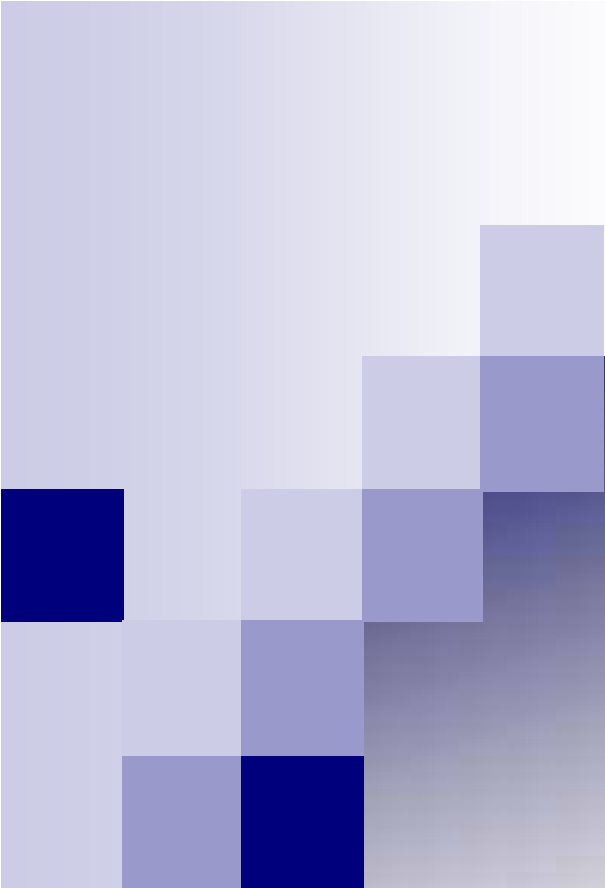
搭乗者事前自動識別システム
Computer Assisted Passenger Prescreening System
政府保有データベース登録情報との照合による搭乗者危険度評価

TIA

テロ情報認知システム
Terrorism Information Awareness system

TSWG

テロ対策技術支援局(CTTSO)の監督のもと
テロ対策技術の開発を行うプロジェクト
Technical Support Working Group



監視社会が進むと、
何が問題になるのか？

■ プライバシーの権利

- 監視技術利用と個人のプライバシーの権利の保障
- 個人情報保護の問題
- 電気通信役務の提供と監視手段の利用(電気通信事業法上の義務)
- 監視カメラの設置をめぐる問題

■ 表現の自由

- 公の場において個人が情報を取得する行為(知る権利)
- 営利的な表現の自由の制約(商業広告の制限)、営利目的での個人情報の販売の規制
- 政府による個人の監視による匿名性の喪失と集会結社の自由との関係

■ 通信の秘密の保障

- ネットワークにおける監視技術利用の問題
- 各種監視ソフトの利用による電子通信の監視
- スニッファーの問題
- スパイウェア(ペスト)の問題
- スпам対策のためのフィルタリング技術の利用
- ネットワーク監視と固有識別アドレスの利用
- インタフェース上の固有の識別番号
- IPv6環境におけるGUIDの利用
- アプリケーション固有のID

■ 法の下での平等

- 特定対象者に限定した監視活動の実施と公平性の問題

■ 適正手続の保障

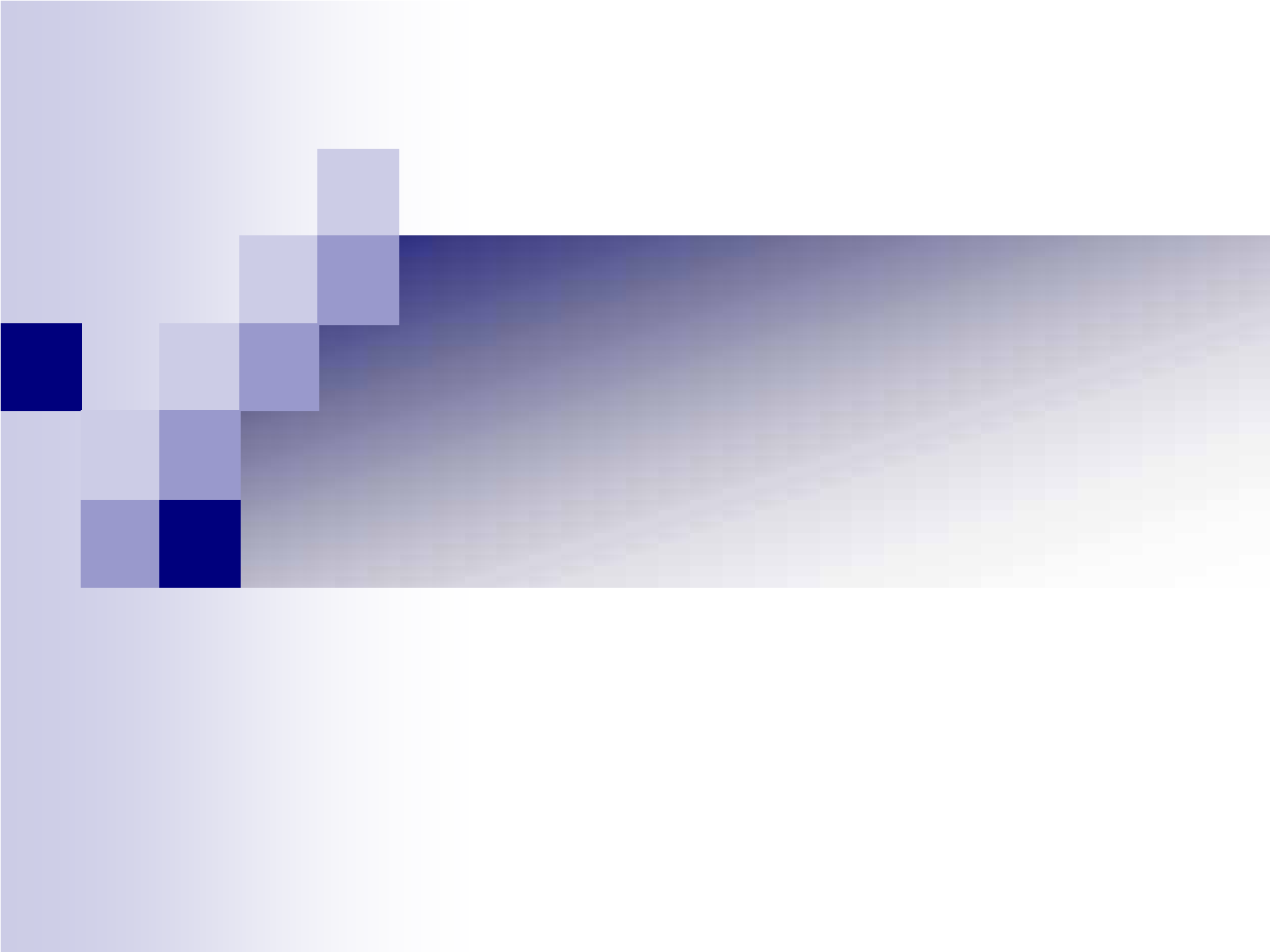
- 捜査手段としての監視技術の利用
- 自己負罪拒否特権
- 各種監視技術の政府による利用(仮釈放、保護観察中の人物の監視など)

- **不法行為法、消費者契約法、特商法との関係における問題**
 - 個人情報不正利用・漏洩
 - 過度な監視技術の利用と人格権侵害
 - CRMの活用による過度の広告の受領
 - オプト・アウトによる個人情報の利用の一般化
 - 情報倫理の欠如
- **製造物責任法**
 - 監視技術の開発・利用に伴う製造物責任
- **著作権法**
 - 技術的保護措置の補完としての監視技術の利用
 - P2P等を利用したインターネット上の著作権侵害者及び侵害行為の特定のための監視

■ 犯罪捜査、犯罪予防を目的とした監視技術の利用

- 通信傍受
 - DCS 2000
 - キーロガー (KLS)
 - NSAによる9カ所のIX (Internet Exchange) への「スニッファー」ソフトのインストール
- RFID、電子透かし、ビーコンの利用による追跡
 - RFIDの利用とトレーサビリティ電子透かしを利用した紙幣の偽造防止と追跡
 - ウェブ上で用いられる1ピクセルのタグ (ウェブビーコン)
- 特定人物を対象とした監視活動とストーカー規制法
- マネーロンダリングや脱税の防止を目的としたオンライン取引の監視
- センサーを用いた捜索 (検証) (非物理的な捜索・押収の問題)
 - a) 透視装置の利用
 - 熱感知投影装置 (Thermal Imaging) = ホットスポットの感知
 - テンペストの問題
 - b) 非接触型の身体検査
 - X線投射による検査をめぐる問題
 - c) スマート・ダスト
 - ユビキタス環境において空気中に浮遊するセンサーを利用した監視
- 監視技術利用の正当化の根拠との関係における問題
 - 法執行機関による個人識別性の向上と効果的な法執行
 - テロ対策
 - サイバーテロ対策
 - 公共の安全確保の必要性
 - 犯罪発生率の増加

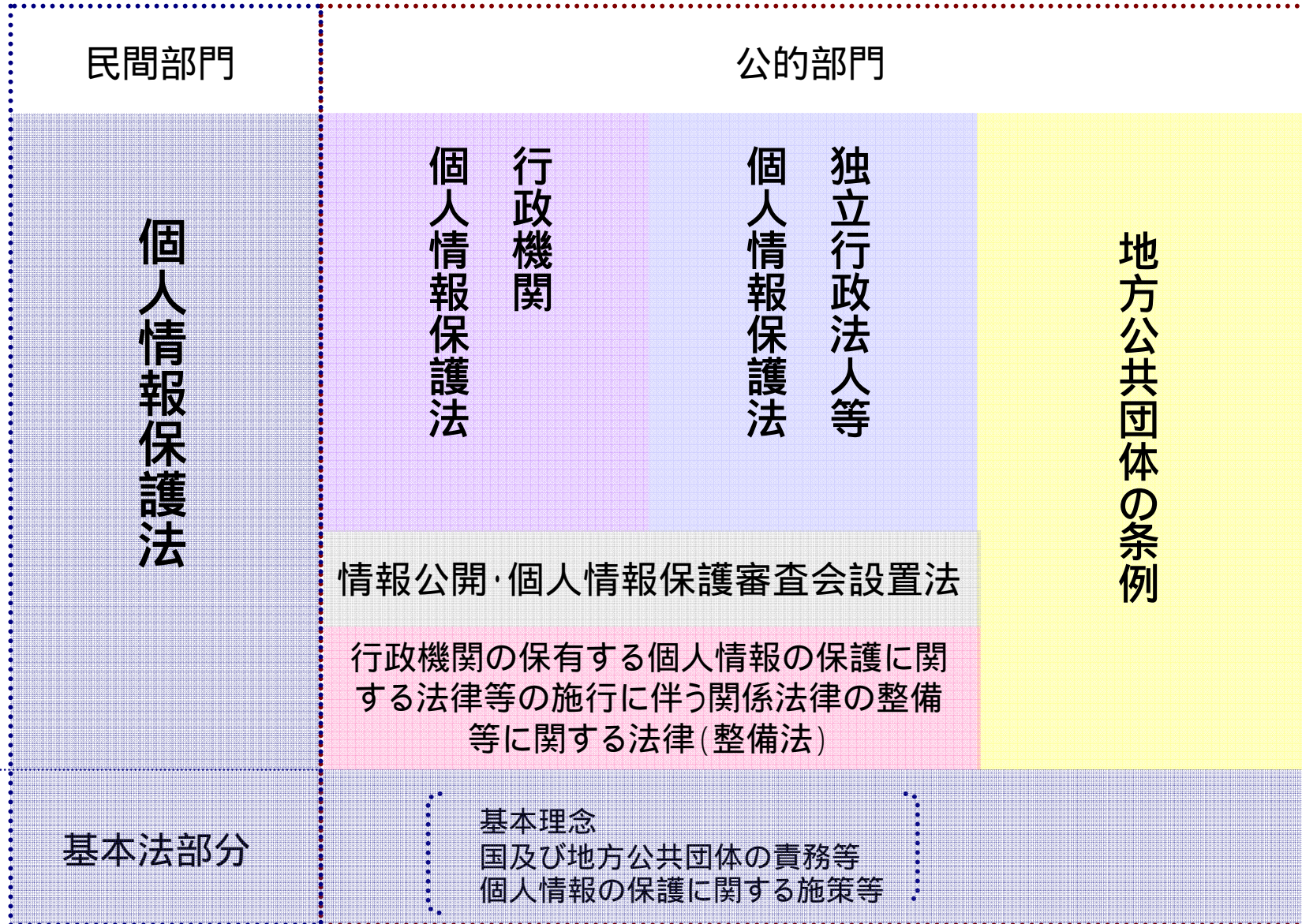
- **道路交通法、道路運送車両法、道路法**
 - ITSの普及とプライバシー
 - Nシステムの運用をめぐる問題
 - オービスによる自動速度取締に関する判例
 - 車両搭載のブラックボックスによる車両情報のリアルタイム追跡
 - GPSを利用した車両位置確認システムと道路交通法違反者に対する対応
 - GPSを利用して速度超過違反車両の燃料供給を停止するシステムの開発(イギリス)、車両の移動記録の捕捉
- **個人情報保護法**
 - 監視技術の利用に伴う個人情報の不正利用と主務大臣の関与



個人情報保護法上の問題



個人情報保護制度



定義関係

個人情報

生存する個人に関する情報
特定の個人を識別できるもの

(他の情報と容易に照合することによって識別できる場合も含む)

個人情報データベース等

検索することができるように体系的に構成したもの

自動処理(コンピュータ処理)されたもの

マニュアル処理(政令で定める処理)されたもの

監視技術を用いて
取得・捕捉する情報
における
個人識別性の有無

訂正・利用停止等の
権限を有するもの

半年以上保有

保有個人データ

個人データ

個人情報データベース等を構成する個人情報

5千件以上

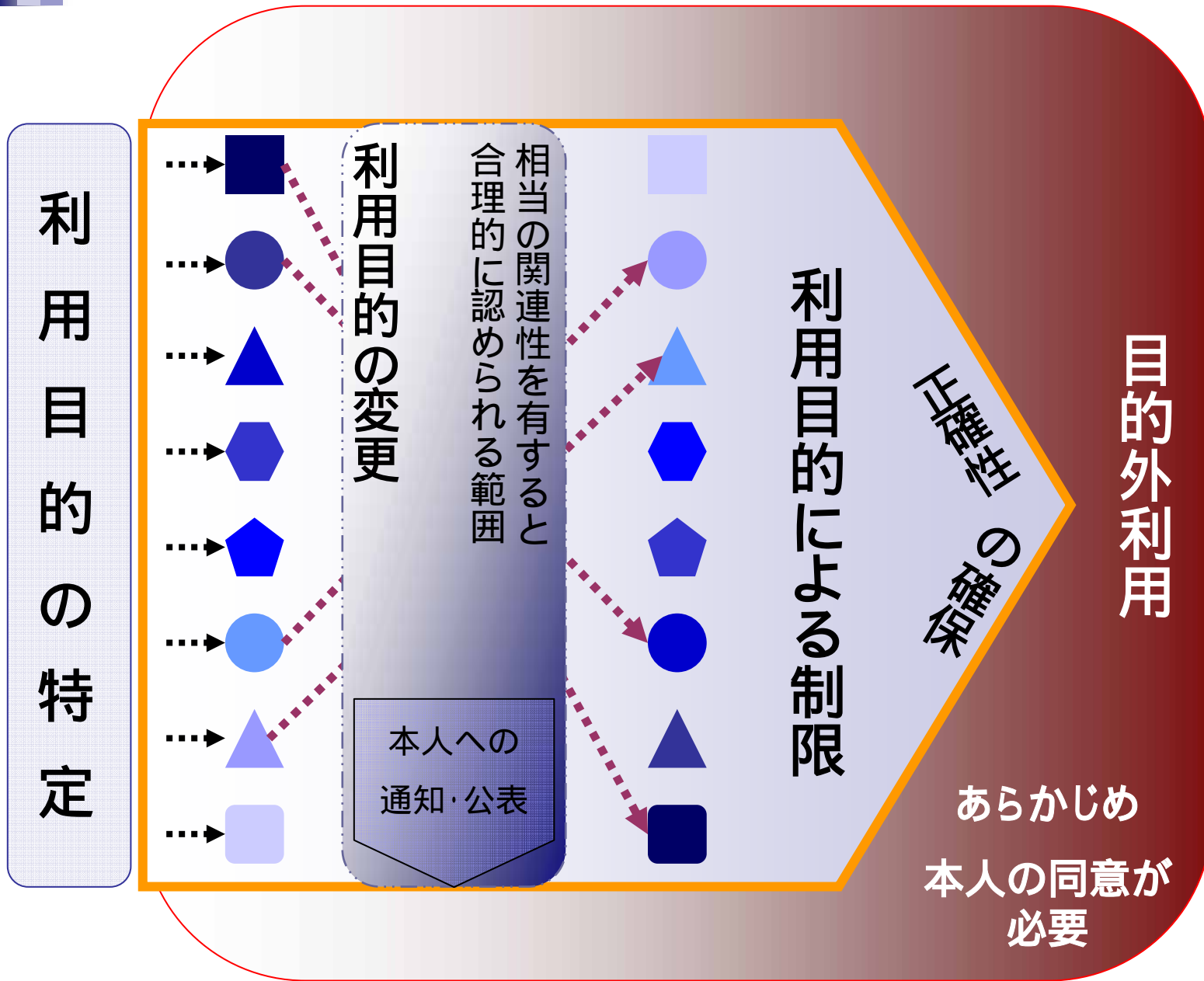
個人情報データベース等を事業の用に供している者

個人情報取扱事業者

国の機関
地方公共団体
独立行政法人
特殊法人
政令で定める小規模事業者等

除外

利用目的の特定、利用目的による制限



除外

法令に基づく場合
人の生命、身体又は財産の保護
公衆衛生の向上又は児童の健全な育成の推進
公的事務の遂行

個人情報取得関係

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む

直接書面取得

間接取得

利用目的

明示

あらかじめ

個人情報の取得

取得後速やかに
通知又は公表

除外

本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
公的事務の事務を遂行することに対して協力する必要がある場合
取得の状況からみて利用目的が明らかであると認められる場合

第三者提供の制限

個人情報取扱事業者

原則

本人の同意

適用除外

法令に基づく場合
人の生命、身体又は財産の保護のために必要がある場合
公衆衛生・児童の健全な育成の推進のために特に必要がある場合
公的事務への協力

オプトアウト

本人の求めに応じてオプトアウトすることとしている場合

オプトアウトの要件

1. 第三者提供すること
2. 個人データの項目
3. 提供の手段又は方法
4. 求めに応じた提供停止

変更

委託先への提供

合併等に伴う提供

共同利用

共同利用の事実
個人データの項目・利用目的
利用する者の範囲・管理責任者名

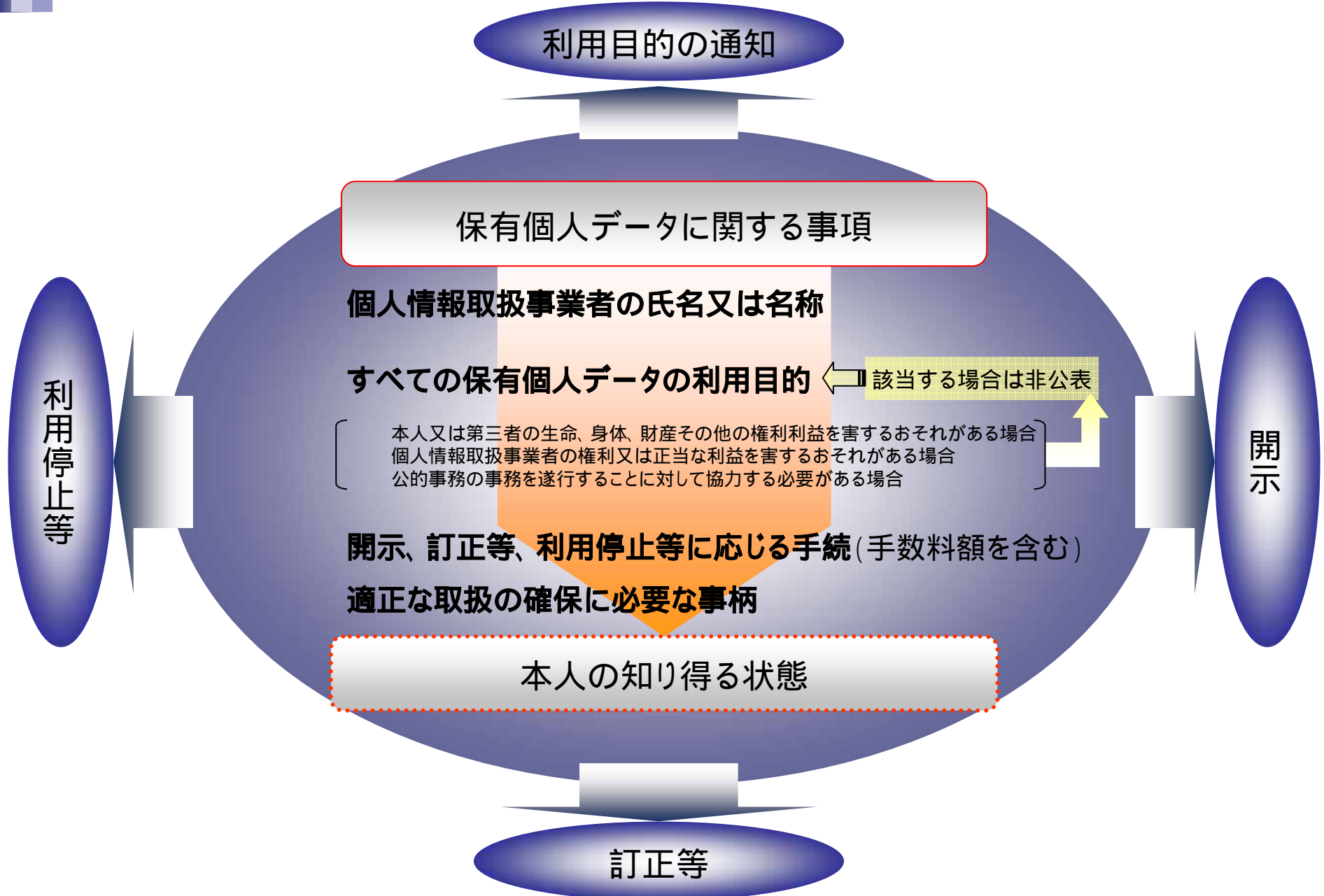
あらかじめ本人に通知 または 容易に知りうる状態に置くこと

第三者

第三者提供に該当せず



保有個人データの公表、開示、訂正、利用停止等



- **バイオメトリクス(生体情報認証技術)の利用**
 - 虹彩、指紋、顔貌等
 - バイオメトリクスの問題(二つの側面)
 - 1. 変更不可能であること
 - 2. 取得する個人情報のセンシティブ性が高いこと
 - 政府の場合(FBIのCODIS「DNA記録システム」やアイスランドの医療情報データベース)

- **医療情報データベースの構築**
 - ヒトゲノム・遺伝子解析
 - 24種類の染色体に遺伝情報が蓄えられている。(アデニン(A)、グアニン(G)、シトシン(C)、チミン(T)の4種類の塩基配列で構成されるDNA) **究極の個人情報**
 - 一定範囲のヒトの細胞等(特定胚)の作成、譲受又は輸入及びこれらの行為後の取扱いの適正確保の必要性
 - ヒトに関するクローン技術等の規制に関する法律

■ 競争法上の問題

- 不正競争防止法、独占禁止法、景品表示法
 - 米国の場合は不公正または欺瞞的取引としてFTC法に基づく行政処分の対象
 - ダブルクリック事件
 - Real Jukebox事件
 - GeoCities事件
 - Intel Chip ID事件
- 過去の米国の暗号規制と情報法制化における各種規制

■ 労働法上の問題

- 職場における監視の実施とプライバシー
 - 電子メールモニタリング事件(国内判例2件)
 - 職務遂行能力の把握、職務専念義務・企業秩序維持のための監視の実施に伴う問題
 - 職業上の秘密保持義務との関係

■ 国際法上の問題

- 宇宙法
 - 衛星監視システムの利用
 - 高精細衛星画像の民間利用
- 国際情報法
 - エシュロン(UKUSA同盟)



まとめ

監視社会化の道を歩み続ける政府

様々な監視技術の開発と導入を進める民間の事業者

利用実態や運用体制の
不透明さへの懸念

プライバシー侵害や個人情報の
不適正な利用にあたるとの指摘

導入しなければならない
様々な社会的要求や国際的背景の存在



監視社会

監視技術の高度化

監視機会の増加

従来からの監視技術を用いて行われる監視
(単なる街頭監視カメラなど)

監視機会の常態化

新たな技術手段が最大の脅威ではなく、
その利用が一般化した監視社会を所与の前提として
受け入れてしまう社会状況が真の脅威