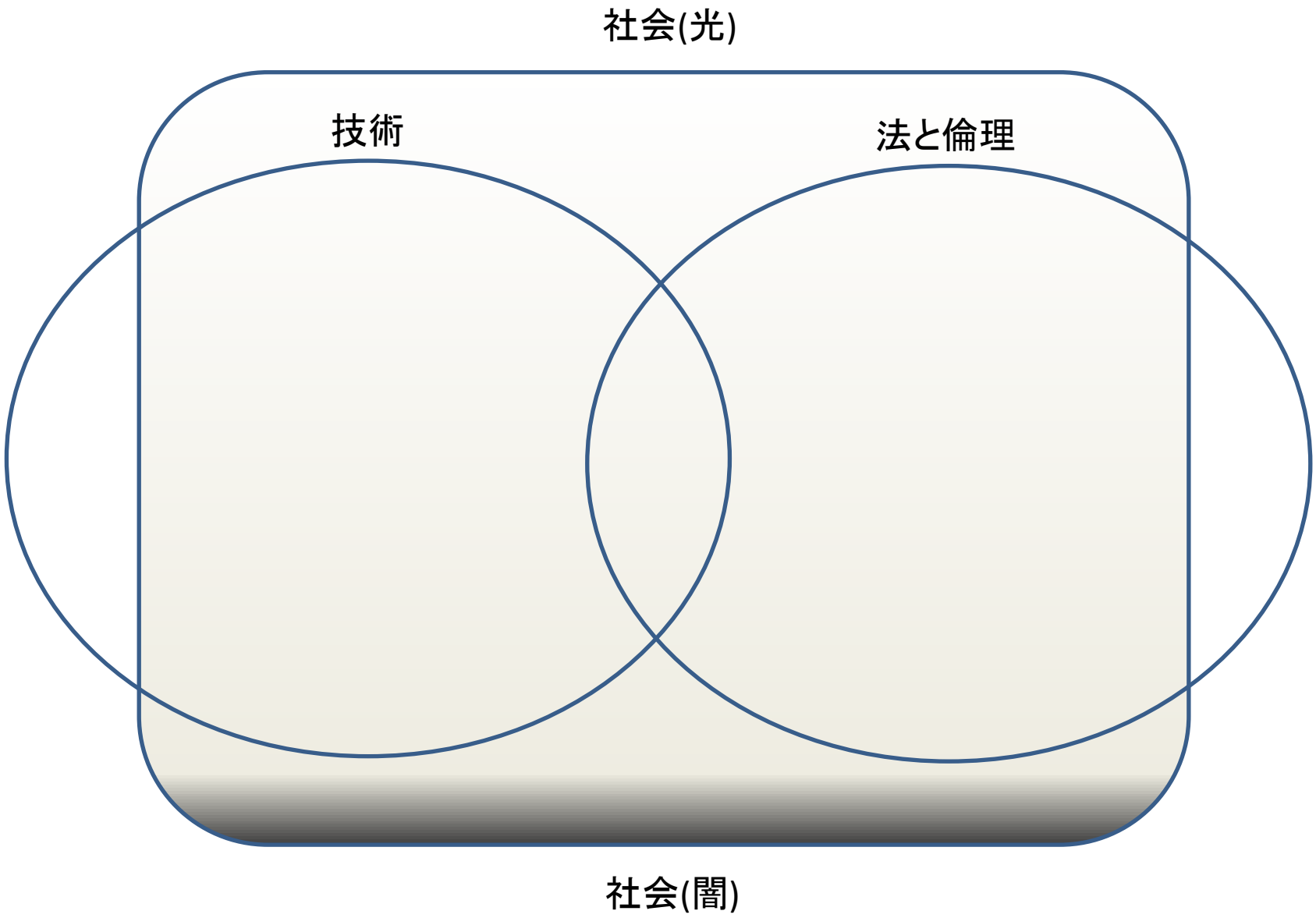
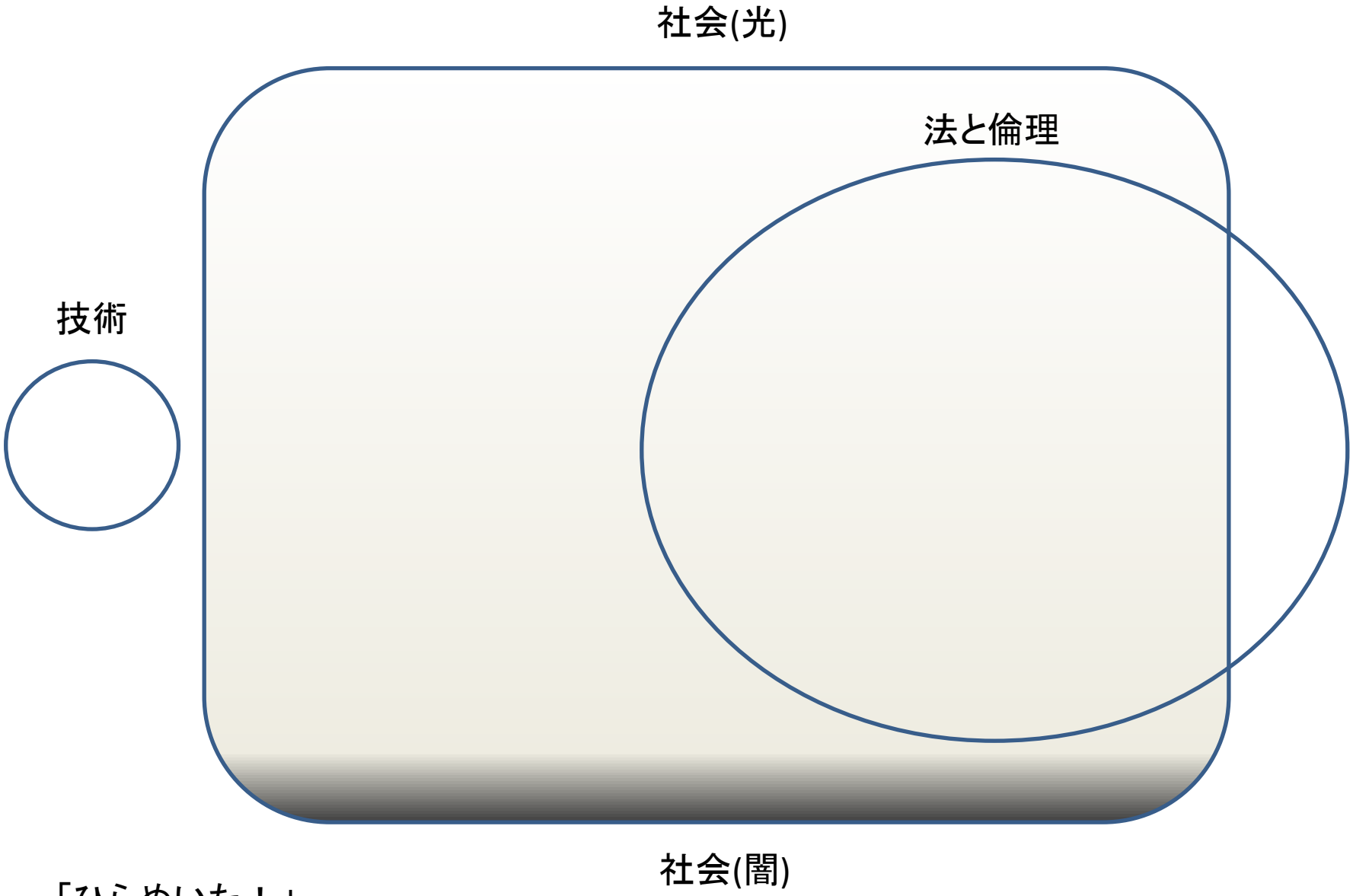
情報セキュリティと情報倫理

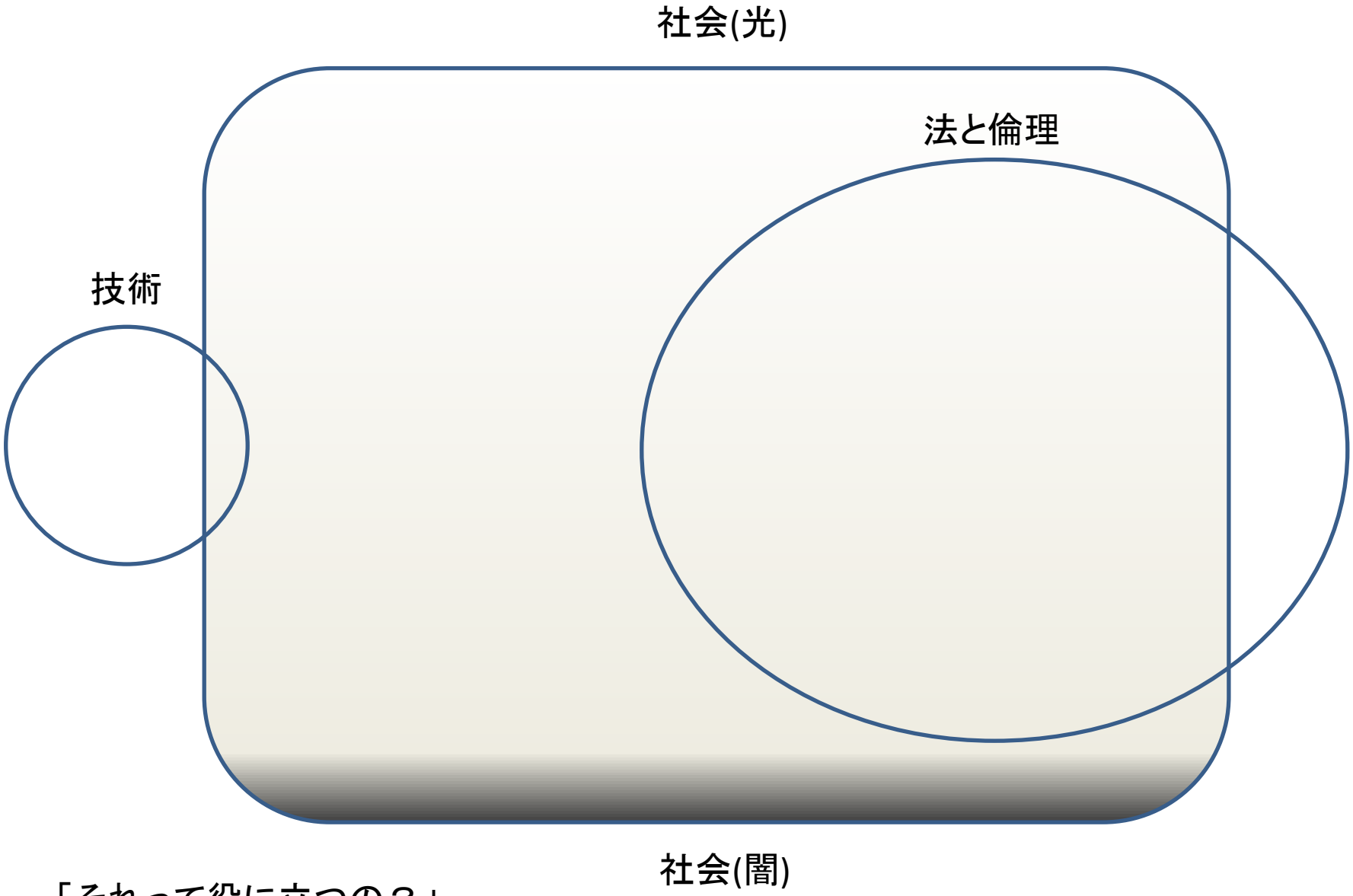
第2回　プライバシーと個人情報

2022/10/07

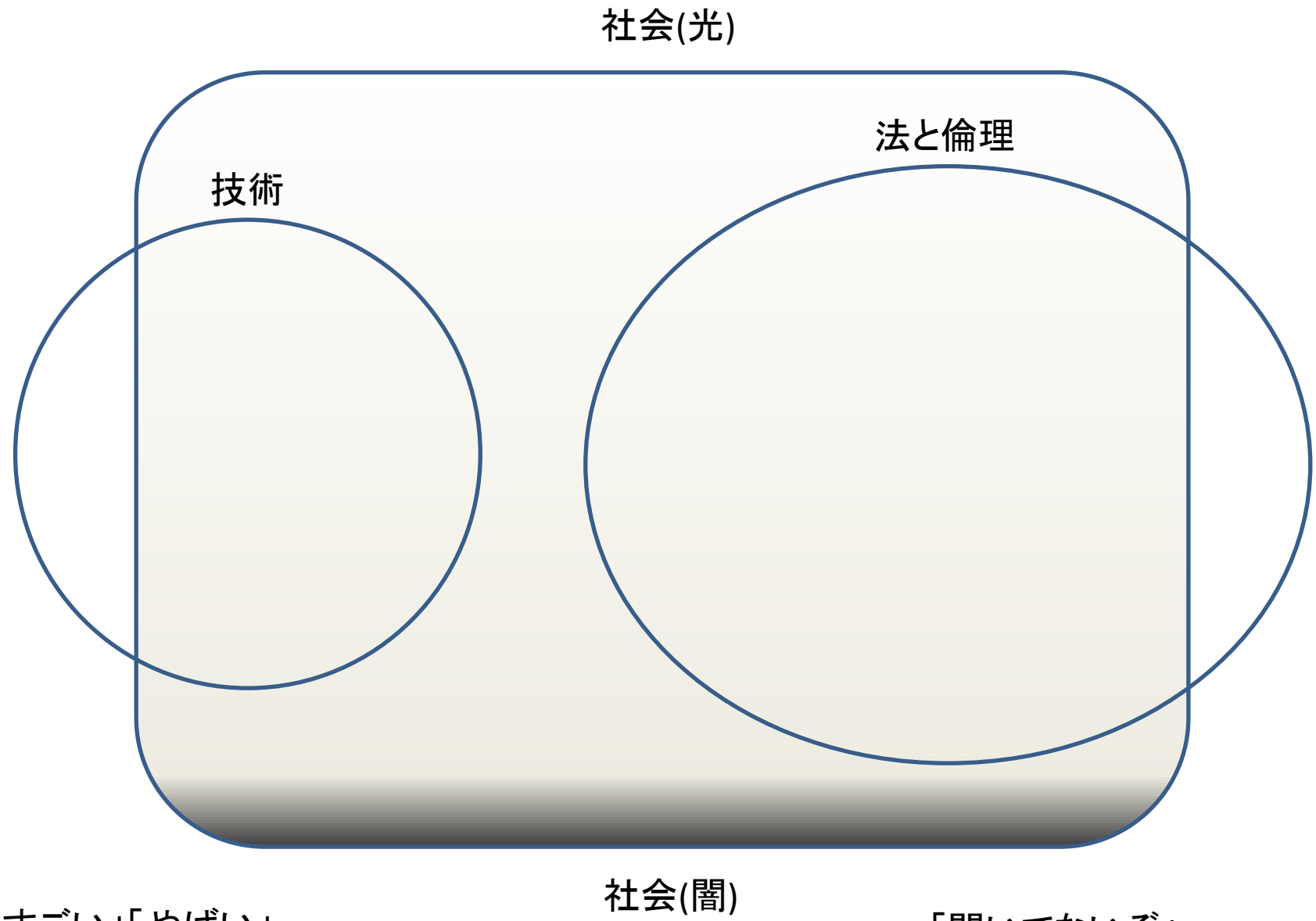

社会(光)
技術
法と倫理
社会(闇)

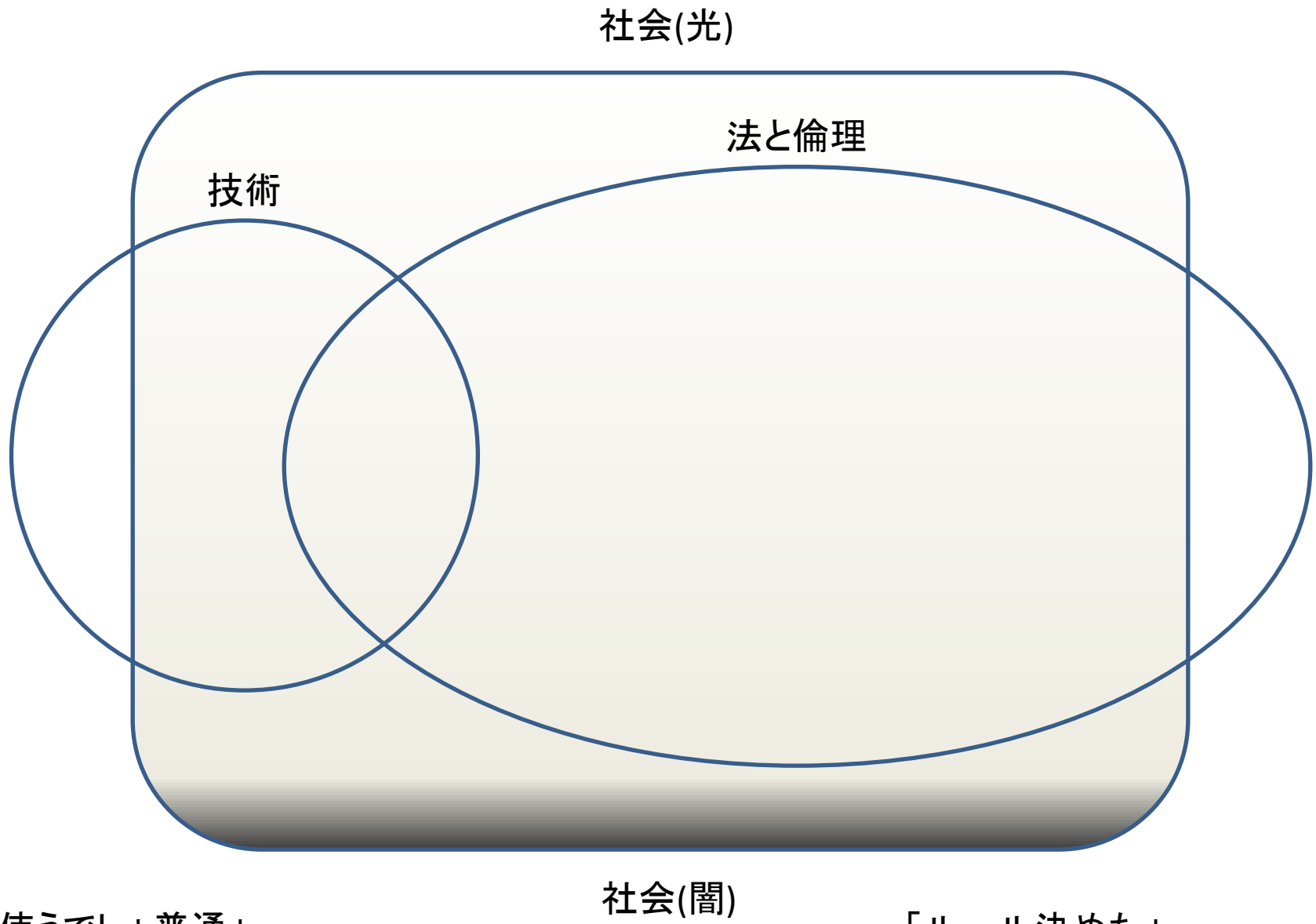


「ひらめいた！」



「それって役に立つの？」

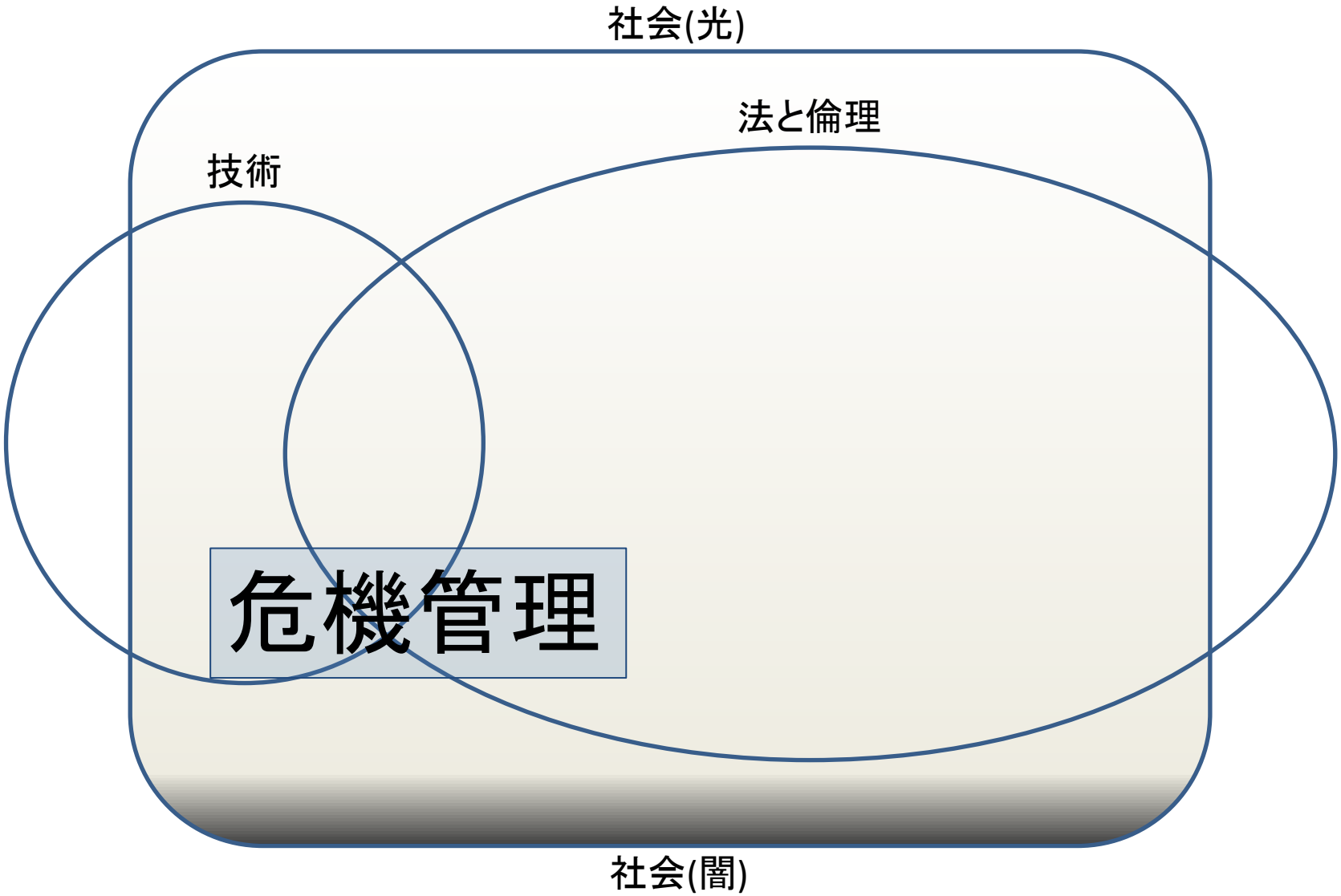

社会(光)
法と倫理
技術
社会(闇)
「すごい」「やばい」
「何じゃこれ」
「聞いてないぞ」
「どうしてこんなことに…」



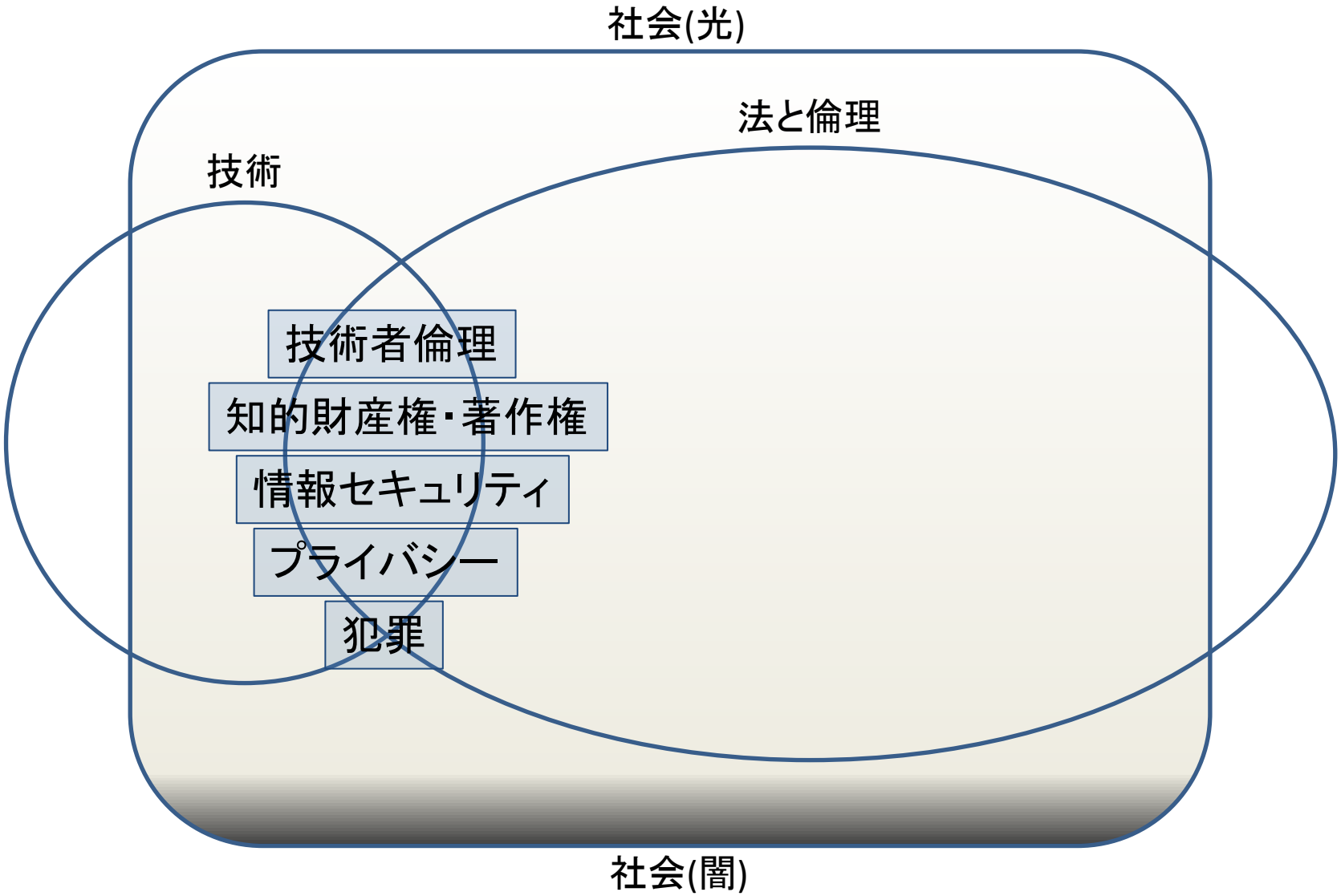
「使うでしょ普通」
「どうするのこれ？」

「ルール決めた」

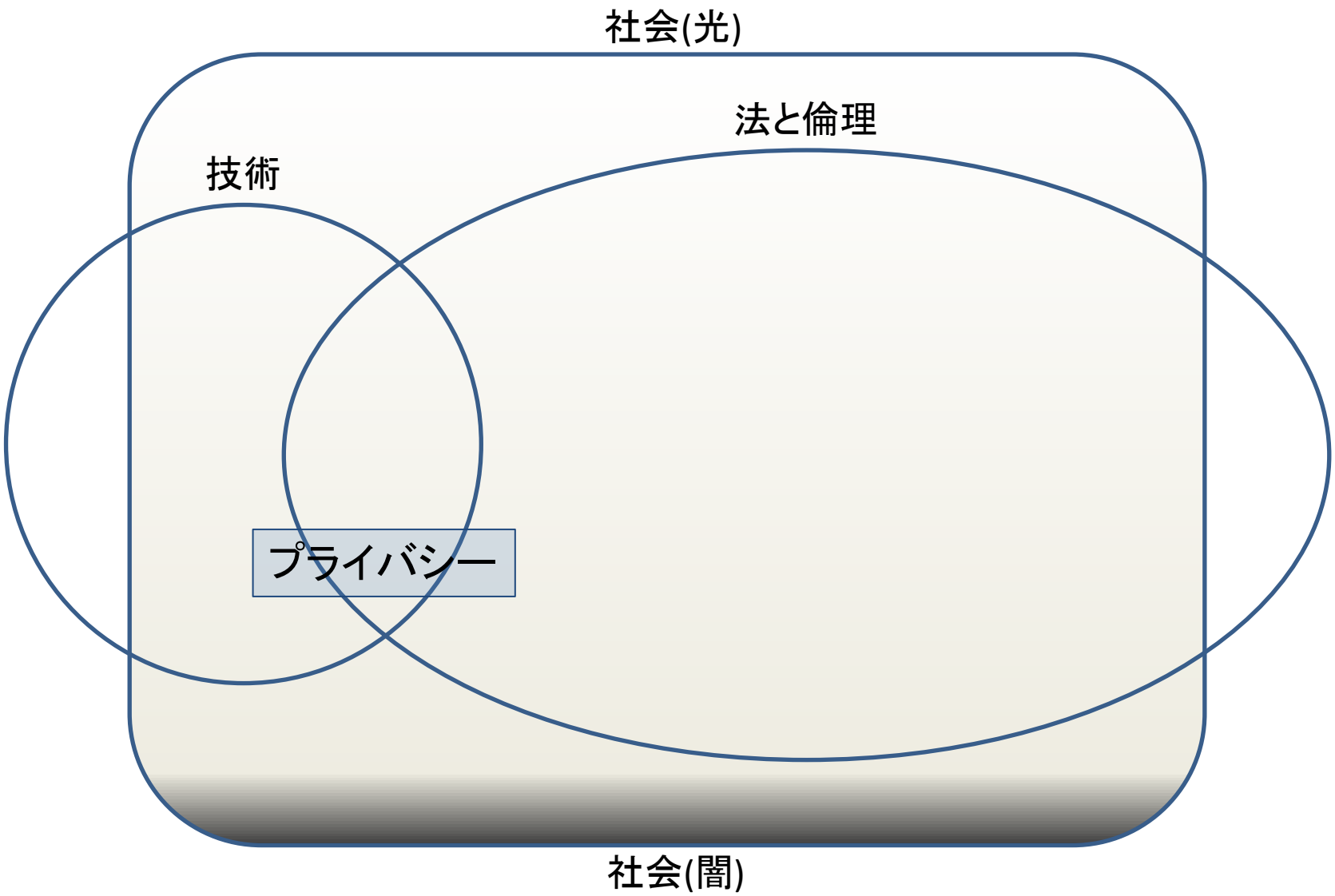
身につけたい能力



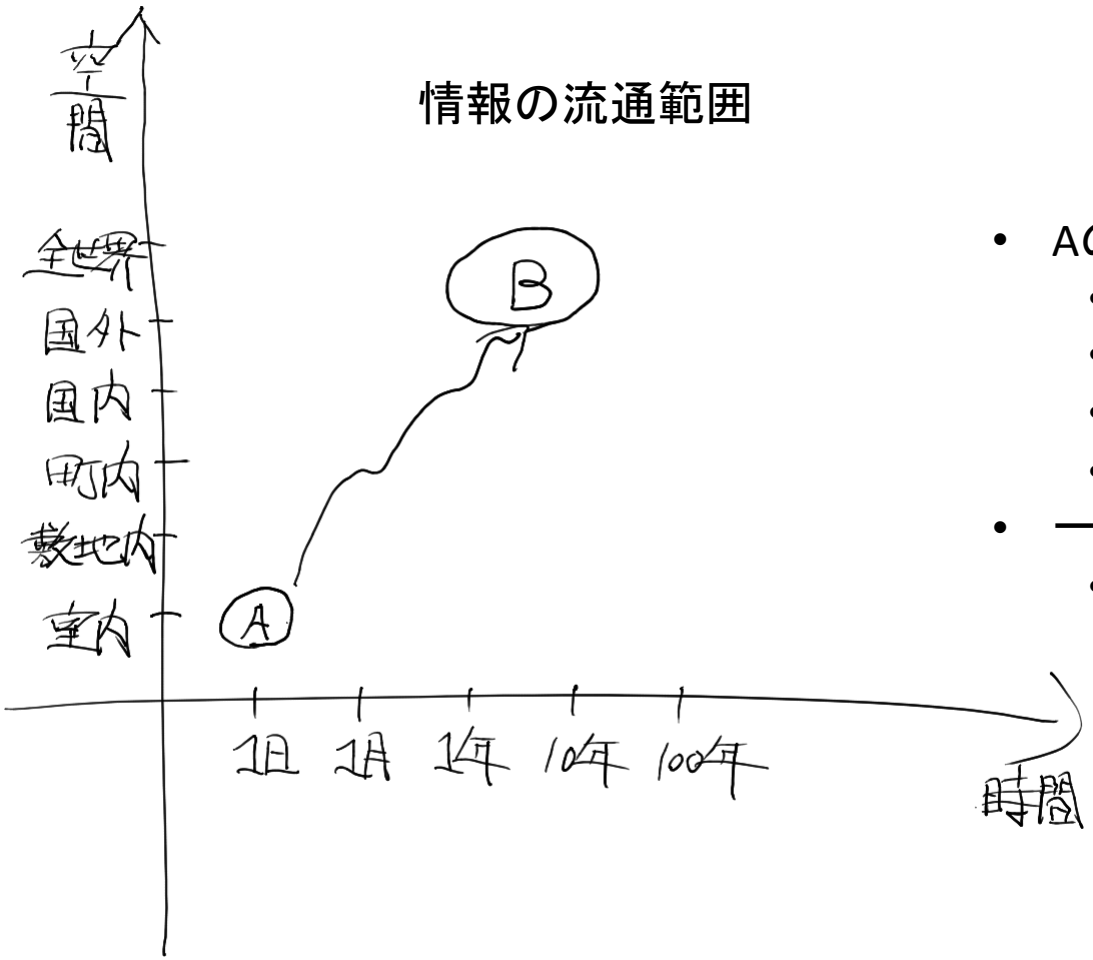
本科目でカバーする内容



今日の内容



何が問題なのか？



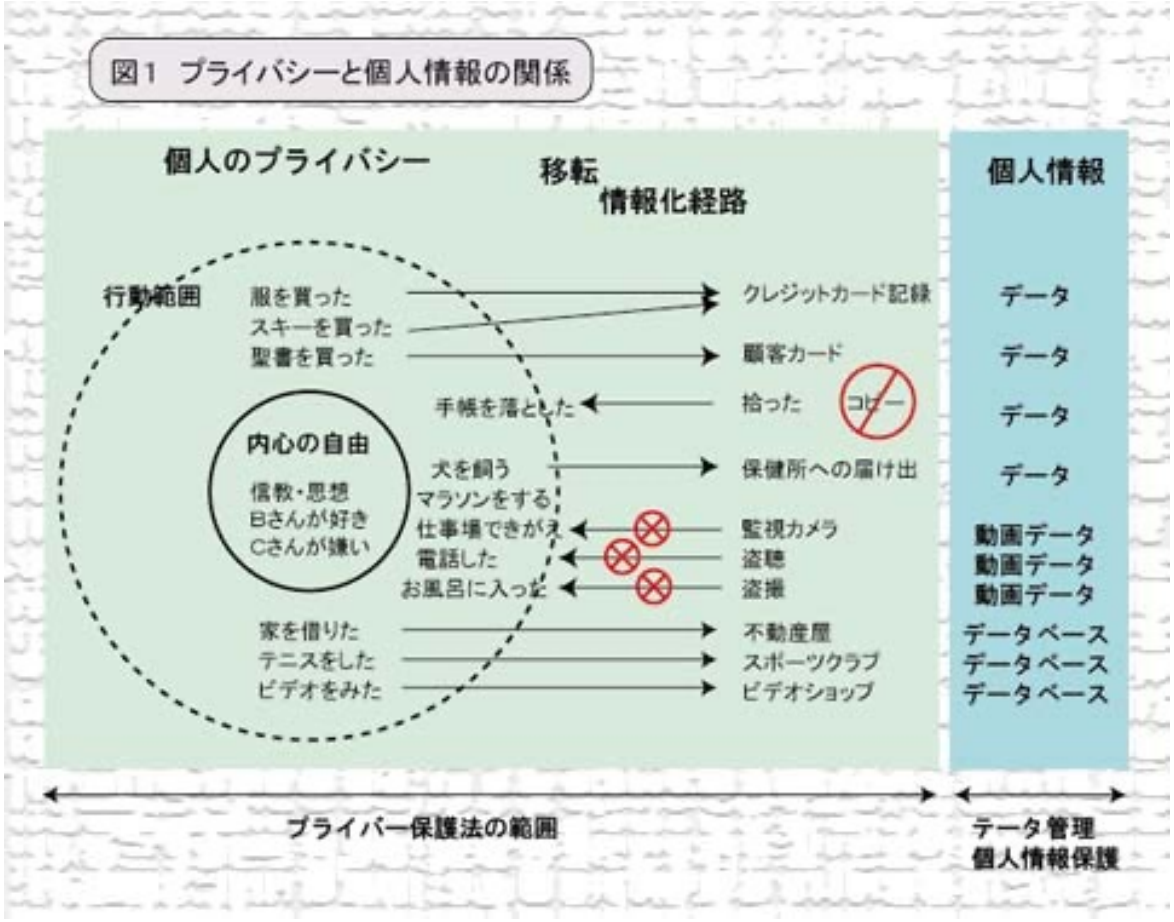
- Aのつもりが実はBだった
  - いつの間にか記録される
  - 意図されない用途に使われる
  - 間違って伝わる
  - 一度出た情報を削除できない
- 一体何がプライバシーなのか？
  - 卒業文集はプライバシーか？

プライバシー権

1. 侵入からの自由(消極的プライバシー権)
   - 一人にしておいてもらう権利
2. 監視からの自由
   - 尾行、観察、盗聴からの自由
3. 自己情報のコントロール(積極的プライバシー権)
   - 自己に関する情報の提供に関する決定権

「内心の自由」が根幹にある

プライバシーと個人情報の関係



出典：http://www.asahi-net.or.jp/~VR5J-mkn/point/privacy/

プライバシーは守れる？

- 人付き合いで伝わってしまう情報
  - 服装,髪型,持ち物,人柄,etc
- 契約上、情報を伝えざるをえないケース
  - 賃貸契約,保険,クレジットカード,etc

大原則：完全なプライバシーは存在しない

例：緊急時連絡網

- 全員の携帯電話番号を資料で配付
  - 「自分の番号は教えたくない」という人がいたら？
  - 諦める？
- Moodleに登録済みの人
  - 「緊急時連絡網に番号を載せる」に投票

https://moodle.cis.kit.ac.jp/mod/choice/view.php?id=230294

医療記録

- 医療情報の機密性は高いと信じられている
  - ex.ある種の病気であることを知られたくない
- 電子化によるプライバシー保護
  - カルテの必要部分のみ閲覧許可
- 完全には秘密にできない
  - 健康保険による点数処理
  - 医者，看護師，薬剤師，検査技師…
  - 生命保険

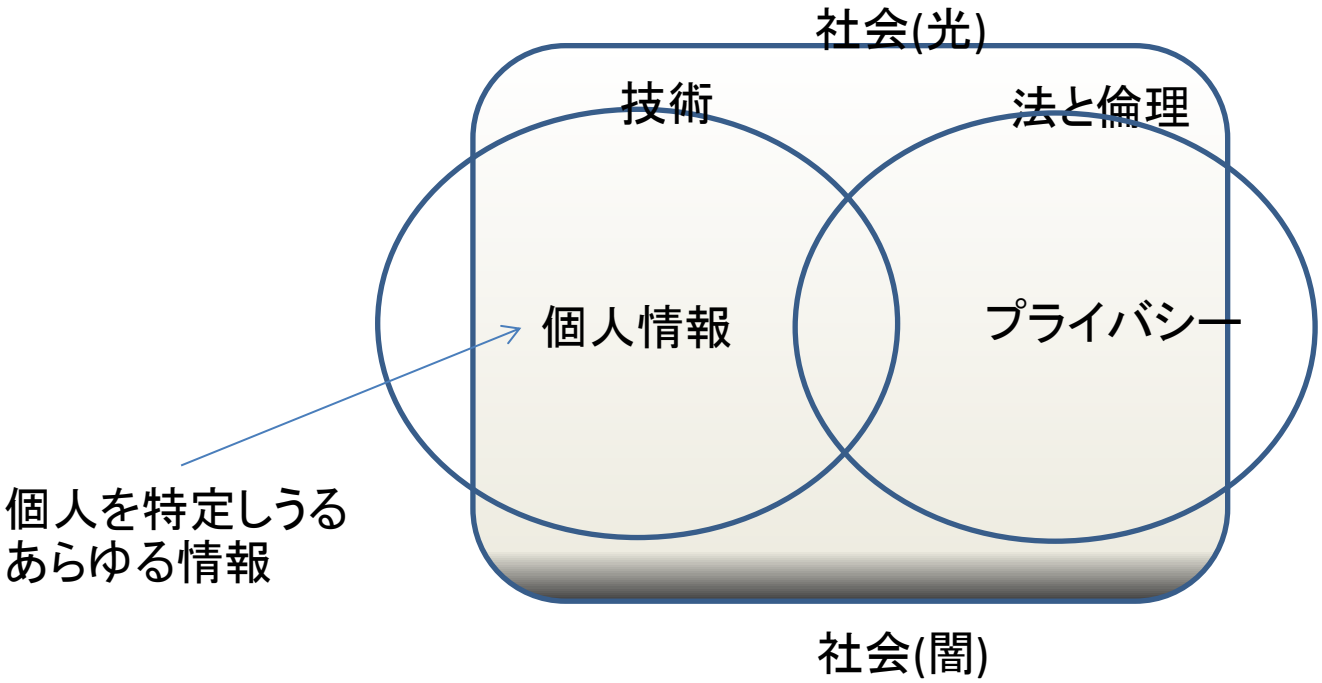
プライバシーはどの程度守られるべき？

- 何でも保護すればいいわけではない

- どういう守り方がよいか？

プライバシーと個人情報

- プライバシーと個人情報は同じ物？
  - 日常会話では両者を同一視することも
  - 概念としては別のもの
    - プライバシーは「権利」、個人情報は「情報」



ミニレポート

- この一週間の生活を振り返り、自分のプライバシーに関係するどのような情報が収集されているか、またそれによってどのようなメリット・デメリットを受けているか、個人の視点と社会の視点から述べよ。
- 提出先：Moodle
- ∝切：10/14(金)　16:10

トピック

- コンピュータ技術の影響
- 行政活動とデータベース
- 消費者情報
- プライバシーの保護に関する法・規制

情報化以前はどうだったか？

- 旧東ドイツ　秘密警察シュタージ
  - スパイや密告者
  - コンピュータ無しで600万人分の思想・行動調査
  - 隣人・同僚・友人・家族
- ゴミ
  - 各種書類，買物明細など
- 監視カメラの映像
  - 従業員が(人手で)監視

情報化が進むとどうなるか？

情報技術の危険性

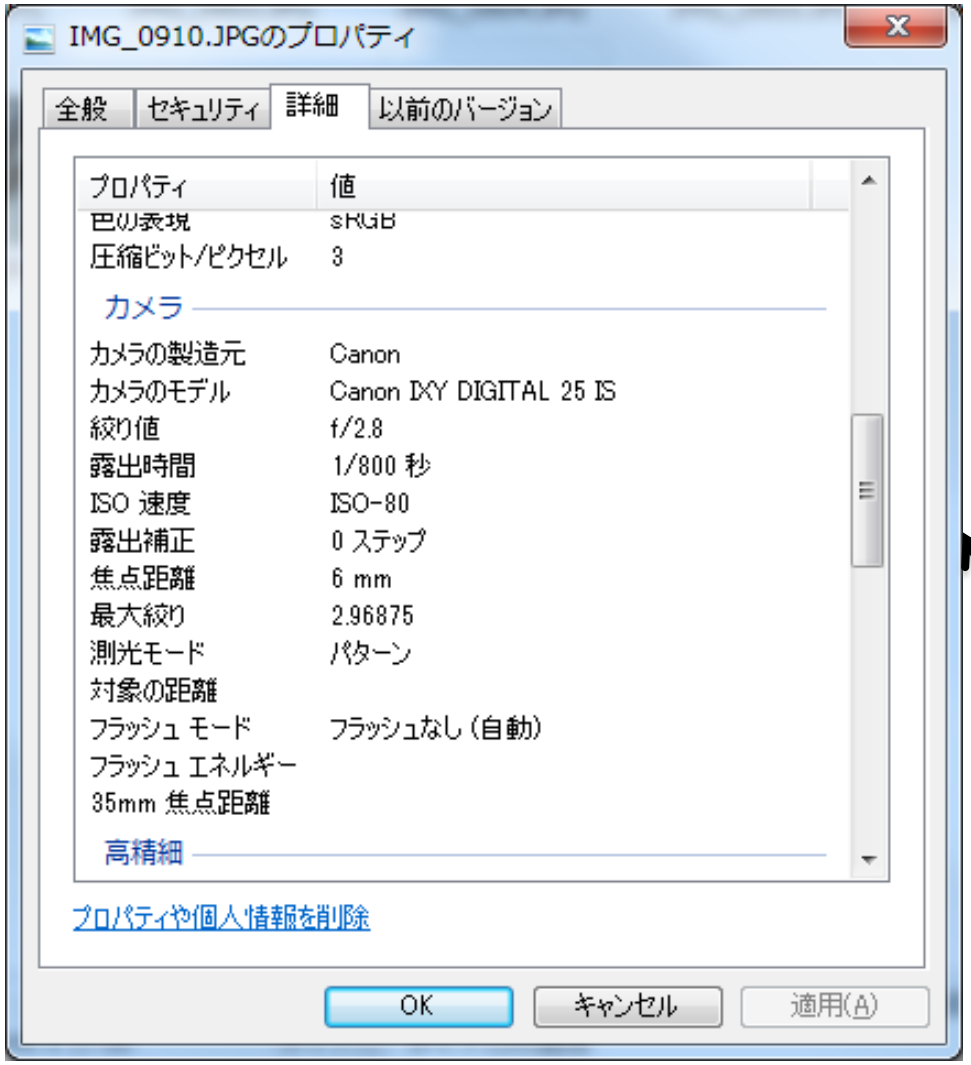
- 情報へのアクセスが容易
- 情報が残り続ける
- 見えざる情報収集
  - 同意を与える機会がない
    - 例：発信者番号
  - 何の情報を集めているかよく分からない
    - 例：メンバーズカード
    - 例：WebブラウザのCookie

トレーサビリティとプライバシー

- 個人の行動と紐付いたIDが勝手に読まれる
  - 例：RFIDタグのついたキーホルダー
  - 例：無線LAN端末のMACアドレス
    - Wi-FiのMACアドレスはもはや住所と考えるしかない
- IDが変更困難だとプライバシー問題に
  - 例：自動車のナンバープレート
  - 例：いつも使うスマートフォンで場所が筒抜け

- Q:AirTagではどのような対策がされている？

デジカメで撮った写真の付加情報



撮影日時だけでなく

撮影場所も…

Webで公開すると？

個人情報の流用

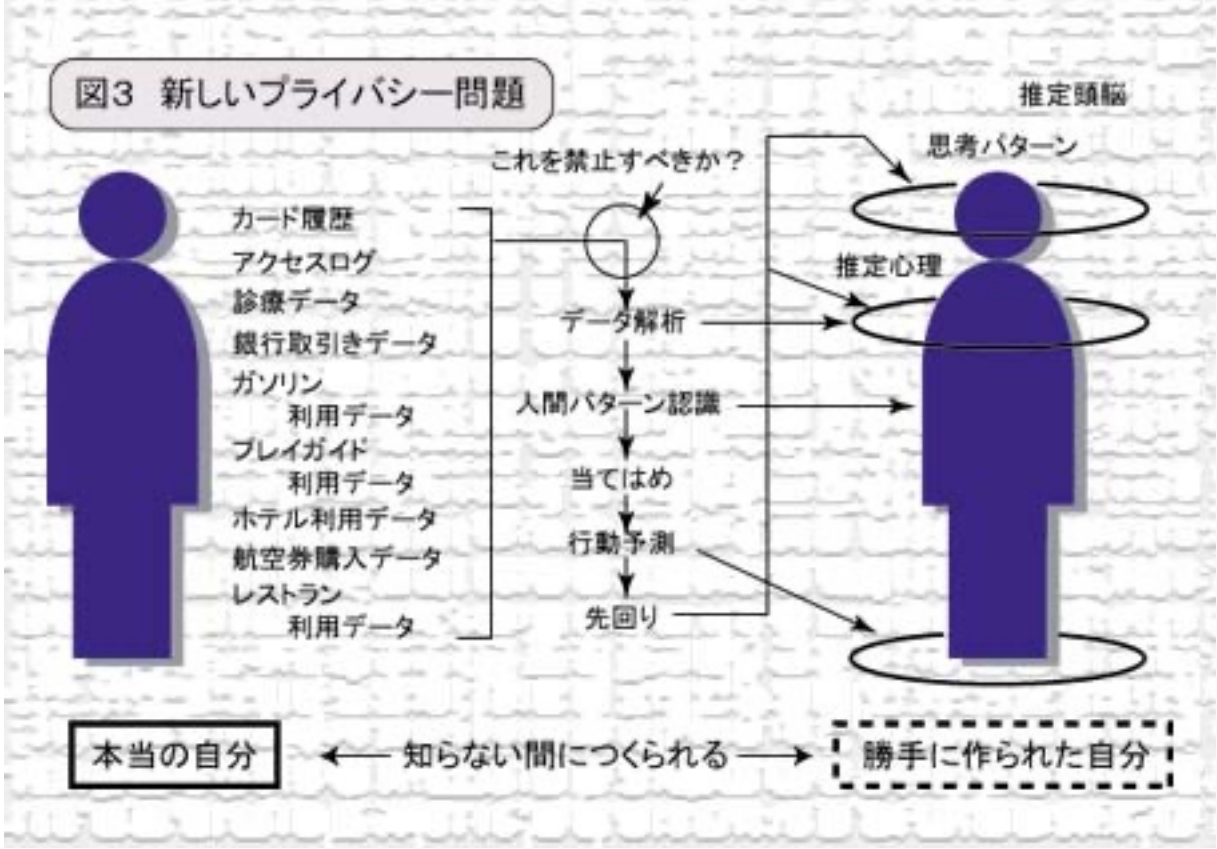
- 過去のSNSの投稿分析
  - 過去何年にもわたる発言の分析
- データベース間のマッチング
  - 例: (ID,年齢,身長,体重)×(ID,年収)→(ID,年齢,年収)
  - 例: (ID,住所)×(ID,年収)→(ID,住所,年収)
- 個人のプロファイリング
  - ある傾向をもった人物の抽出
  - 例:要注意人物の抽出

米国の事例

- スーパーマーケット「ターゲット」の事例(2012)
  - 出産が近い顧客にベビー用品のクーポンを送付
  - 高校生の娘がいる父親がクーポンを受取り激怒
    - 実は娘は本当に妊娠していた
- 「ターゲット」の手法
  - 買い物の特徴から妊娠を予測
    - 香り付きローションから無香料ローションに乗り換え
    - サプリメントの買いだめ
  - 出産予定日も高精度で予測

元記事：How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

情報化によるプライバシー問題例



出典: http://www.asahi-net.or.jp/~VR5J-mkn/point/privacy/

リクナビ問題(2019)

- リクナビDMPフォロー社(グループ企業)
  - リクナビ上の行動履歴などをもとに、内定辞退率を予測。34社に内定辞退スコアを提供(販売)
  - 対象者：7万4878人
    - 「リクナビ2019」会員のうち12,330人
    - 「リクナビ2020」会員のうち62,548人
- 利用規約に説明はあったか？
  - 「*採用活動補助のための利用企業等への情報提供*」
  - 同意を得ていなかった学生:7,983人

リクナビ問題への反応

- 「リクナビDMPフォロー」は8/4付で廃止
- 大学側の反応
  - 一部私大でリクナビと絶縁宣言
    - 「信頼関係がなくなった」
- 個人情報保護委員会から勧告・指導
  - 一部学生から同意を得ていないことが問題
- 東京労働局から行政指導
  - 職業安定法の指針に違反
    - 「特別な理由のない個人情報の外部提供」に該当
  - 同意の有無によらず違反

行政活動とデータベース

政府（内閣・行政機構）とデータベース

- 行政機構のもつ多数のデータベース(DB)
  - コンピュータマッチング
    - 異なるDBから情報を結合・参照
    - ex.納税DBと給付金DB →不正受給の発見
  - コンピュータプロファイリング
    - 特定の行動に親和的な人間の性質を決める
    - ex.脱税の逮捕歴のある人の納税パターン
- 行政機構のDB誤用は深刻な脅威
  - 権力性が高い(提供を拒否できない)
  - センシティブな情報が多い(戸籍など)

行政機構とデータベース例

- IRS(内国歳入庁)
  - 納税データを持つ
  - Compliance2000: 車両登録機関，個人信用調査会社，不動産登記簿，新聞記事，船舶登録情報，職員雇用記録，免許発行記録などを統合
    - 納税未申告者，収入が正確で無い人などの捕捉
- FBI 全米犯罪情報センター(NCIC)
  - 指名手配犯，盗品，行方不明者などのデータ
  - 入力，利用が野放図だった
    - 誤った情報による誤認逮捕
    - 特定思想者の動向調査
      - 情報が蓄積されると最初に意図されなかった目的に流用されがちな典型例

米国: 社会保障番号(SSN)

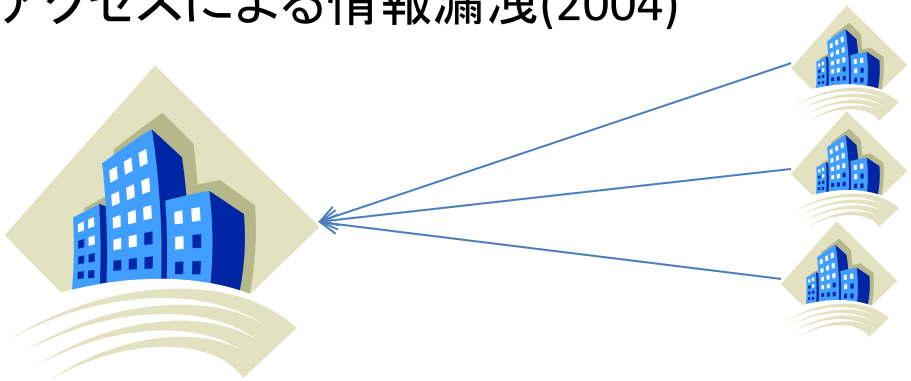
- SSN(Social Security Number)
  - 1936年　社会保障プログラム専用として発行
  - 1961年　納税者ID(IRS)
  - 1976年　地方税，福祉，自動車関係
  - 1988年　出生証明に親のSSNを提供
    - 仕事，所得歴，信用報告，運転歴，銀行口座..
- SSNの濫用
  - 名前とSSNで，ほぼ個人が識別(特定)できる
  - SSNは必ずしも一意ではない
  - 偽造，詐欺，信用の失墜，その他の問題多数

行政系DBの安易な連携の問題点

- 正当な業務 vs プライバシーへの不当な脅威
  - 脱税者の分は納税者が負担している？
    - 脱税者の(強引な)捕捉方法が必要
  - 無実な人が不当な扱いをうける？
- 推定無罪→推定有罪になりかねない
  - DBの処理で疑わしい→無実を示す必要?
- →権力の濫用に繋がる可能性が高い

民間企業からの情報購入

- 保有データベースに含まれていない個人情報
  - 自分たちで収集しようとすれば議論沸騰
    - もしかしたら違法行為
  - 集める代わりに民間企業から購入
    - LexisNexis Risk Solutions社(旧ChoicePoint社)
      - 個人情報会社を12社以上買収,100億件以上の情報保持
      - 少なくとも35の政府機関が顧客
      - 不正アクセスによる情報漏洩(2004)



行政管理DBに対する期待と不安

- 行政のサービスや能力が拡大する
  - 犯罪を減少させる
  - すべての人に納税をさせる
  - 自発的に遵法している人には脅威はない
  - 公務員は，正当，公正，誠実に執行

- →行政はどのようにしてうまく，自身のデータベース内の個人情報を保護し，自身のプライバシールールに従うのか？

- 誰が見張り番自身の見張りをするのか.

政府は大丈夫？

- 1974年プライバシー法は守られていない
  - 連邦政府が保有する記録中のデータは、それが収集される合法な目的との「関連性と必要性」が認められる範囲内にとどめなければならない
  - 本人の同意無しに個人情報を提供してはならない
- 連邦政府Webサイトの80%がプライバシー法に違反(1997)
- NCIC(全米犯罪情報センター)のDB乱用
  - 私立探偵に情報転売
  - 元彼女の居場所を突き止め殺害

メディアの誤送付

- デンマーク(2015)
  - データCDの誤配送
    - デンマーク統計局のはずが中国のビザ申請局へ
  - 中身：国民520万人分の社会保障番号＋健康データ
    - ガンや糖尿病、精神疾患などに関する診断結果
    - 氏名・住所は含まれず
  - 受け取った職員は荷物を開封
  - データは暗号化されていなかった

元記事：Five million Danish ID numbers sent to Chinese firm
国民ほぼ全員分の個人情報が手違いで中国へ送られるハプニングが発生

消費者情報

DBと営業活動

- 消費者情報は氾濫ぎみ
  - 懸賞に応募
  - 保証の為のユーザ登録
  - 店舗でのポイントカード
  - 電子マネー
- データマイニング(data mining)
  - 消費者情報の分析
  - 顧客にあわせたダイレクトメール
  - 消費者プロファイルの作成→新顧客の発見

危険にさらされる消費者情報

- DB上の取引データが莫大である＝脅威
  - クレジットカード利用履歴→行動・所在
    - 電子マネー(Edy/iD, SUICA/ICOCA, おサイフ携帯,..)
  - 通販履歴→趣味・嗜好
- 気づきにくいメタ情報の付与
  - EXIF情報（デジタルカメラ用の画像ファイルの規格）: 撮影日時などの付加情報を記録可能
- 提訴によって顧客情報の開示を求められる
  - 不必要な提示，必要以上の提示
- 漏洩による安全性への脅威
  - 消費者プロファイルを企業に送付
    - 入力従事者自身による漏洩・悪用

Facebookの事例

- 適正に入手したユーザ情報を転売(2016)
  - Facebookの5000万人の個人情報、トランプ陣営が不正利用か
  - ケンブリッジ・アナリティカ廃業へ　フェイスブックデータ不正収集疑惑で
  - フェイスブック＆ケンブリッジ・アナリティカ事件の問題点と教訓
- 脆弱性による情報流出(2018)
  - 「Facebook、5000万人の情報が流出か」

プライバシーとダイレクトメール

- ダイレクトメール(DM)はプライバシー侵害か？
  - 侵入からの自由を侵害しているのは確か.
  - 顧客にあったDMなら歓迎されやすい.
- 受け取ったDMの処理の片付けコスト増
- DMにより余計な出費をしてしまう？
- 自己情報のコントロールの権利を侵害している場合がありえる
  - いったん第三者利用に同意すると取り消すのが困難
- 同意無くDMを送付すること＝違法とは言えない(通常の郵便物との区別がつかない)

Q:ターゲット広告はありがたい？

- 良い点
  - 無駄な広告が減る→宣伝費の節約→値下げ
  - 自分にあった商品/サービスを見つけられる
- 悪い点
  - 受け取ったチラシ・カタログを捨てる手間
  - 欲しくない物でも買ってしまう
  - 精神的苦痛
    - 赤ちゃん用品/子供用品
    - 子供が亡くなった後も送られてくる

子供とWeb

- 子供特有の危険
  - 家族・友人の情報を教えてしまう
  - 犯罪者との接触ルートになりうる
- 子供のオンラインプライバシー保護法(米2000)
  - 親からの明確な同意がない限り、13歳未満の子供から個人情報を収集してはならない

信用情報

- 本来の用途
  - クレジット申込者の評価
  - 支払い実績、訴訟、破産など
- 他の用途での利用
  - 採用応募者の身辺調査
- 懸念事項
  - もし信用情報に誤りがあったら？
    - 住宅ローン、自動車ローン、就職etc

Q:古い個人情報は消されるべきか？

米Equifax社の情報漏洩事件(2017)

- 消費者信用情報会社大手3社の1つ
  - 住所,免許証番号,クレジットカード支払い履歴等
- 事件の概要
  - 米個人情報機関最大手Equifax、1億4300万人の社会保障番号など漏えい
    - Equifaxの最大1億4300万人分の情報漏洩、原因は半年前のStruts2脆弱性
  - 大量データ流出のEquifax、さらに別な機密情報にアクセス可能な状況

個人の行動に関わるデータ

- いつ/どこで/誰と/何を
  - 検索履歴,購買履歴,アクセス履歴
  - 移動履歴,操作履歴
- 趣味・嗜好・健康状態等の推定に利用可能
  - パーソナルデータによる新サービスの創出
  - データの扱いについて社会的な合意が必要
    - Suica分析用データの社外提供(2013)
      - JR東日本にて分析用データに加工→日立製作所にて分析
      - 「事前説明無し」と批判→中止へ

行動履歴とプライバシー
情報倫理デジタルビデオ小品集より

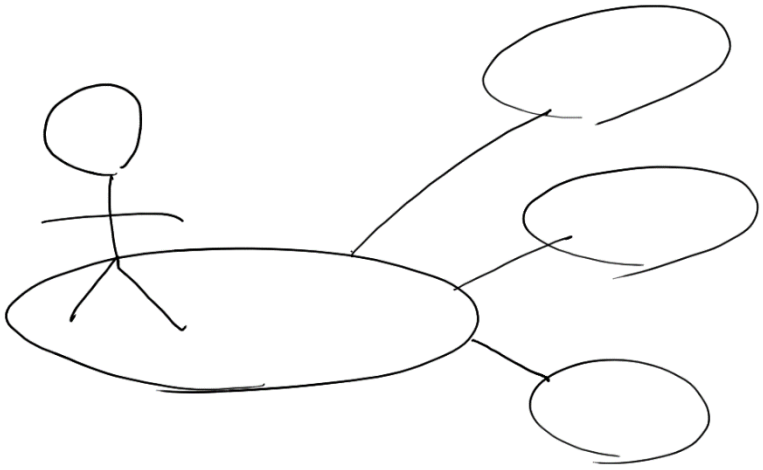
- 情報倫理デジタルビデオ小品集について
- ポイントを貯めると個人情報が流出
  - 物語編(約3分)
    - どうすればよかったのか
    - どうすればよいか
  - 解説編(約3分)

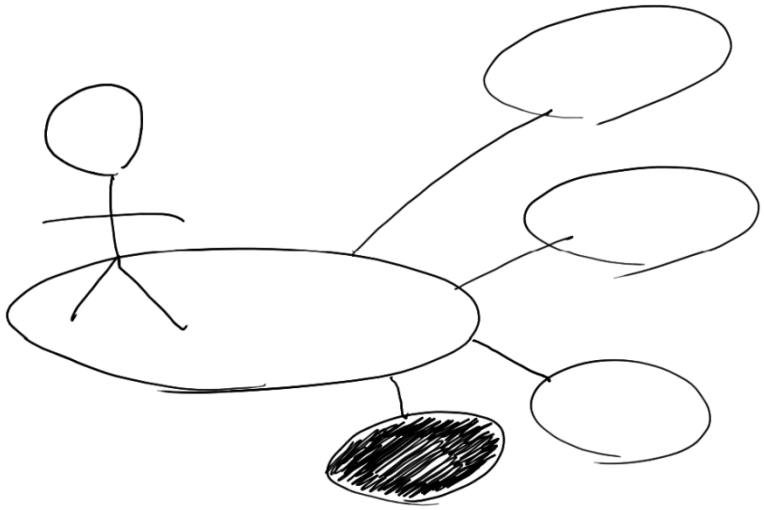
データ収集・利用の原則

1. インフォームドコンセント
2. データ利用範囲の選択肢の提供
   - オプトイン方式
     - 利用者が明示的に利用を選択
   - オプトアウト方式
     - 利用者が明示的に拒否を選択
     - 何もしなければ同意と見なされる

オプトアウトの問題

- 提携先企業でのデータ利用に同意すると・・・
  - 提携先企業は刻々と変わっていく





個人情報のプライバシー原則

- 必要なデータのみ収集すること
- 何の情報をいつ収集し、どう利用するか本人に通知すること
- オプトアウト手段、第三者提供拒否の手段を提供すること
- センシティブなデータは強い保護を用いること
- データは必要な期間のみ保持すること
- データの正確性・安全性を確保すること
- 自分のデータを修正できること

企業の動き

- プライバシーポリシーの公開
  - ex. Googleのプライバシーポリシー
- 最高プライバシー保護責任者の設置
- オンライン広告掲載サイトの選別
  - 適切なプライバシー保護を行わないサイトへの掲載中止

プライバシーの保護：法と規制

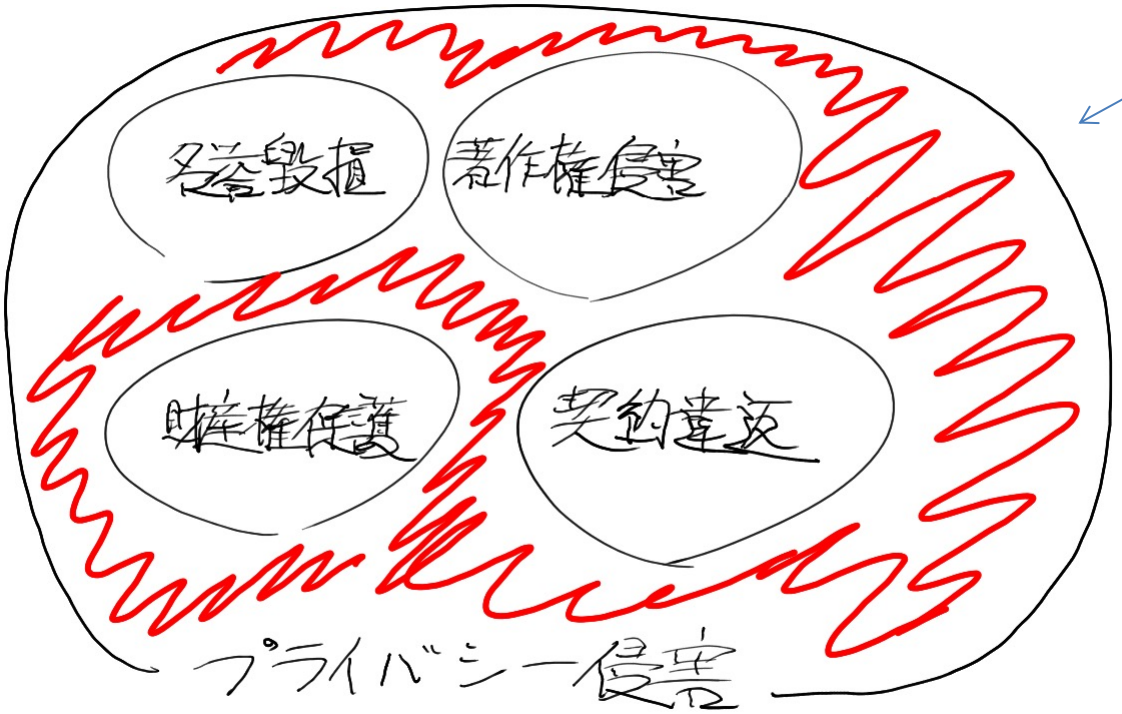
プライバシー問題の法的救済

- 我々はどんな権利を持つべきか？
  - 見解１:プライバシーは別個の権利として保護されるべき
  - 見解２:プライバシーの侵害は他の権利の侵害とみなすべき

見解1:不可侵の人格

- Warren&Brandeisの見解(1890)
  - 人々には自身に関する事実や写真の公表を禁止する権利がある

隙間で多くのプライバシー侵害が起きている

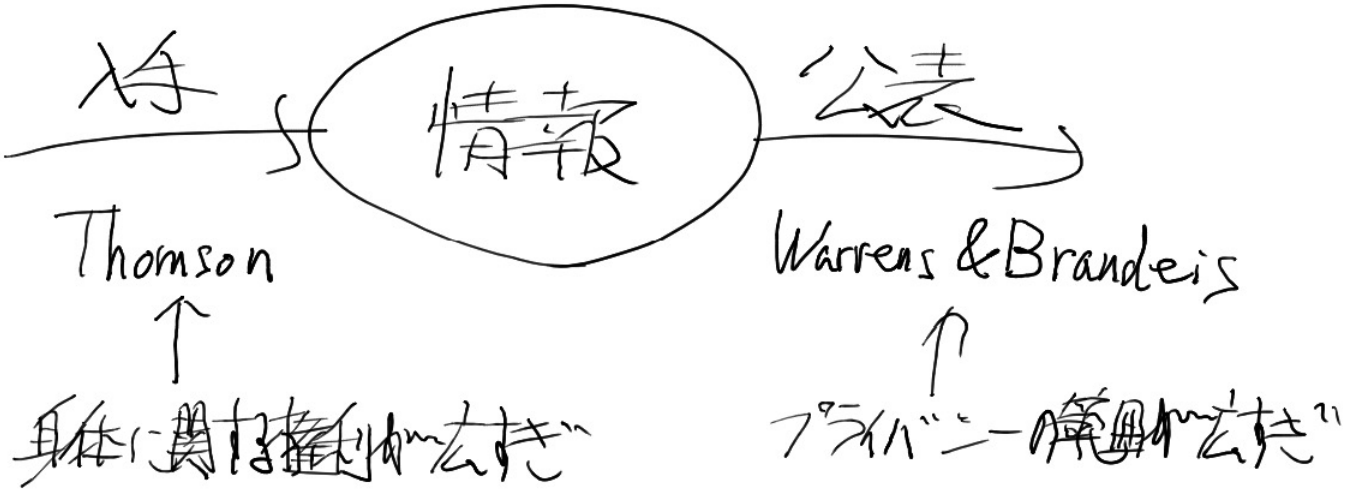


見解2:既存の権利でカバー可能

- Thomson (1975)
  - 「プライバシーの侵害は他の何かの権利の侵害によって生じる」
  - 所有権：所有物を勝手に見たり撮ったりしてはダメ
  - 身体権：体を誰に見せるかを決定する権利
    - 会話を誰に聞かせるかを決める権利
    - 公共の場では権利を放棄している状態
  - 秘密をばらす行為は？
    - 秘密保持の合意の侵害
    - 事前に秘密保持の同意をせずに話すのは軽率

両見解の整理

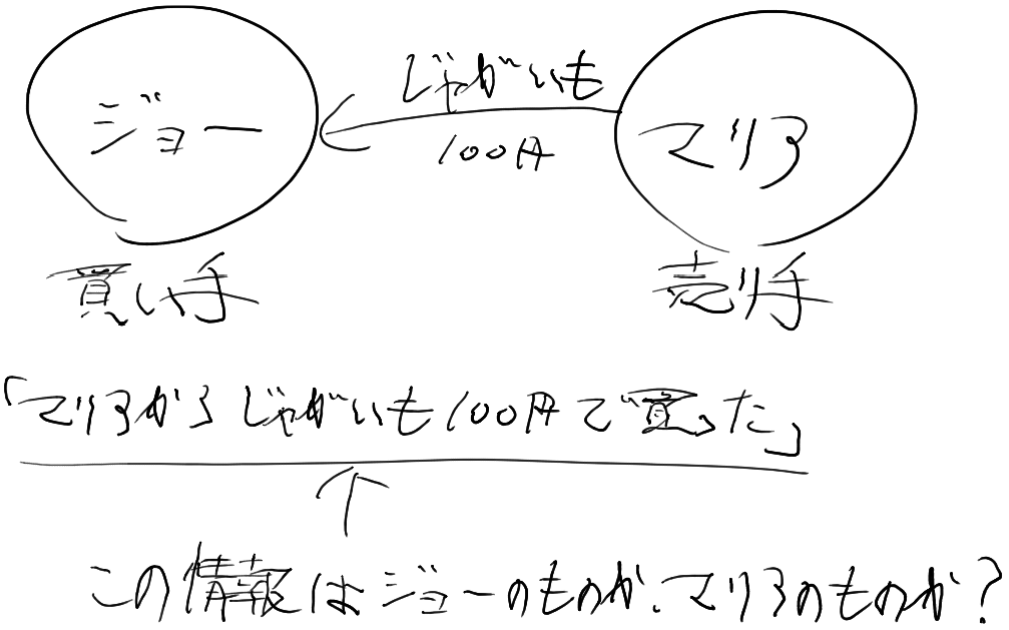
- 入手が問題か、公表が問題か



本人が同意した情報の入手・公表はプライバシー侵害ではない

取引に関する情報の所在

- 当事者が複数いるとどうなる？



- 情報のコントロール権はどちらにあるか
  - 売り手に権限がある？買い手に権限がある？

消費者取引情報の規制

- 個人-企業間の取引も個人間の取引と同じ？
- 2つの見解
  1. 自由市場論
  2. 消費者保護論

自由市場論

- 消費者の権利と能力を尊重
  - 法は最低限の基準を定めるだけ
  1. データの他者への開示を明確に告知すること
  2. 個人情報を開示する契約を結ぶ自由
  3. 言論および営業の自由

     自主的かつ非侵入的でない方法で入手した事実の開示を禁ずるべきでない
  - 市場が幅広い選択肢を提供するのを認めるべき
    - 立法者が前もって消費者のニーズを知るのは不可能

消費者保護論

- 危惧
  - 企業による個人情報の濫用
    - ex.企業はオプトインを義務づけられるべき
  - 知識・判断力・関心の欠如
    - ex.消費者はリスクについて十分理解していない
- 消費者の状況
  - 企業と交渉の余地はない
    - 真意に反して個人情報の開示に同意
  - 企業がプライバシーポリシーを守る保証はない
  - プライバシー保護技術は完全ではない

規制は正解か？

- サービスの減少
  - 規制：１３歳未満の子供から情報収集するには親の同意が必要
  - 結果：子供向けサービス(メール等)の廃止
- コストの増大
  - 法遵守のコストに年間６～１０万ドル
  - 小企業には大きな負担

法律上の潜在的な問題点

- 個人情報の所有権を認めるべき？
  - 「事実」を「所有」することはできるのか？
  - あなたの誕生日は誰のもの？？？
- 言論の自由との衝突
  - 「取引」に関する「事実」の伝達を禁じる法律は？

各国におけるデータ保護規制

OECDプライバシーガイドライン

収集制限の原則	個人データ収集方法は適法かつ公正で、当人に通知や同意をする事
データ内容の原則	個人データを利用目的の範囲内で利用する事と、その範囲内で個人データの正確さや最新さを規す事。
目的明確化の原則	個人データ収集以前に収集目的を特定し、目的変更の際も目的を特定する事。
利用制限の原則	当人の同意や法令に基づく場合以外は、個人データを目的外使用してはならない事
安全保護措置の原則	不正利用、漏洩、改竄等に対する対策を講じる事。
公開の原則	個人データの利用方針を公開し、これに基づく事。さらにデータ管理者と個人データの所在地を示す事
個人参加の原則	データ管理者が自身の個人データを保有しているかを確認し、保有している場合にはそのデータを当人に教えるすべを提供する事。データ管理者がこれらを拒否する場合はその理由を提示し、異議申し立てができるようにする事。
責任の原則	データ管理者が以上7つの原則を実施する責任を有する事

出典: Wikipedia プライバシー保護と個人データの国際流通についてのガイドライン

EUにおけるプライバシー規則

- EUデータ保護指令
  - 個人データ処理に関する包括的プライバシーポリシー
  - EU内で個人情報を扱う団体・事業主は届け出が必要
  - 適切な制度を持たない国への個人データ移転を禁止
  - 違反には制裁金
    - ソニープレイステーションネットワーク個人情報流出事件(2011)
  - EU加盟国間で法律にばらつき
- EU一般データ保護規則(GDPR,2018年施行)
  - 加盟国間のばらつきを解消
  - 消去権(忘れられる権利),データポータビリティ,等
  - EU市民を相手にするEU外の団体・事業主にも適用

保護対象の個人情報

- 氏名,個人識別番号
- *位置データ*
- オンライン識別子
- 身体的・生理的・遺伝的・精神的・経済的・文化的・社会的アイデンティティに特有な1つまたはそれ以上の要素

アメリカにおけるプライバシー規則

- 領域・業種毎(医療、金融、etc)に規制
  - 包括的な個人情報保護法は存在しない
  - 公的部門はプライバシー法(1974)を制定済み
  - 民間部門は自主規制が基本
    - Google(データ収集・解析), Apple(「我々はやらない」)
- 州によっても規則が異なる
- 個人情報全般の監督機関は存在しない
  - 連邦取引委員会が消費者プライバシー保護担当

個人情報の保護に関する法律の概要
第1章　総則

- 目的（1条）
  - 高度情報通信社会の進展に伴い個人情報の利用が著しく拡大
    → 個人情報の有用性に配慮しつつ、個人の権利利益を保護
- 定義（2条）
  - 個人情報：生存する個人に関する情報（識別可能情報）（＜ー詳細次ページ）
  - 個人情報データベース等：個人情報を含む情報の集合物
    （検索が可能なもの。一定のマニュアル処理情報を含む）
  - 個人情報取扱事業者：個人情報データベース等を事業の用に供している者
    （国、地方公共団体等のほか、取り扱う個人情報が少ない等の一定の者を除く）
  - 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
  - 保有個人データ：個人情報取扱事業者が開示、訂正等の権限を有する個人データ
- 基本理念（3条）
  - 個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであり、その適正な取扱いが図られなければならない。

出典：http://www.mhlw.go.jp/shingi/2004/06/s0623-15g.html

個人情報とは
（個人情報の保護に関する法律第二条）
（平成一五年五月三十日法律第五十七号，最終改正：平成二十一年六月五日法律第四十九号）

- この法律において「個人情報」とは、生存する個人に関する情報であって、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することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

改正個人情報保護法

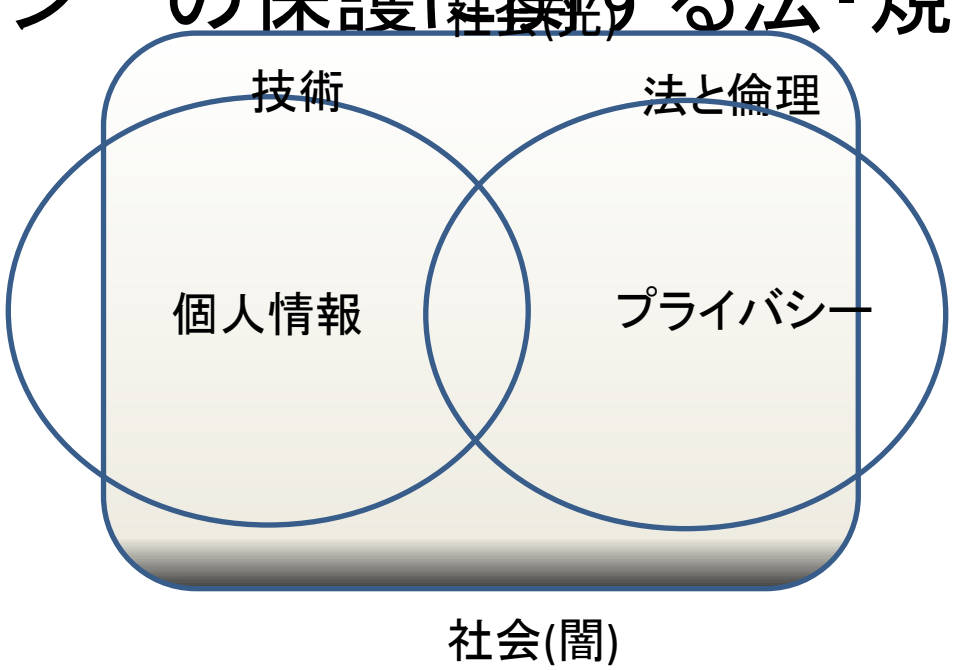
- 平成27年9月公布。平成29年春施行
  - 3年ごとに見直し。(2020年6月公布,2022年4月施行)
- 特定の個人を識別できるもの
  - 従来(氏名、住所、生年月日)＋個人識別符号
  - 改正案:指紋データ、顔認識データ、遺伝子データ、旅券番号、免許番号をカバー
- 他の情報と容易に照合することができるもの
  - 改正案:購買履歴、移動履歴をカバー
- 「匿名加工情報」の導入
  - 適切に匿名化されたデータの取り扱い
- 「要配慮個人情報」の導入

要配慮個人情報

- 特に配慮を要する情報
  - 不当な差別、偏見、不利益を招くおそれがあるもの
- 説明(個人情報ハンドブックp.27)
  - 人種、信条、社会的身分、病歴
  - 犯罪歴、犯罪により害を被った事実
  - 健康診断などの結果
- 取得には本人の同意が必要

今日のまとめ

- コンピュータ技術の影響
- 行政活動とデータベース
- 消費者情報
- プライバシーの保護に関する法・規制

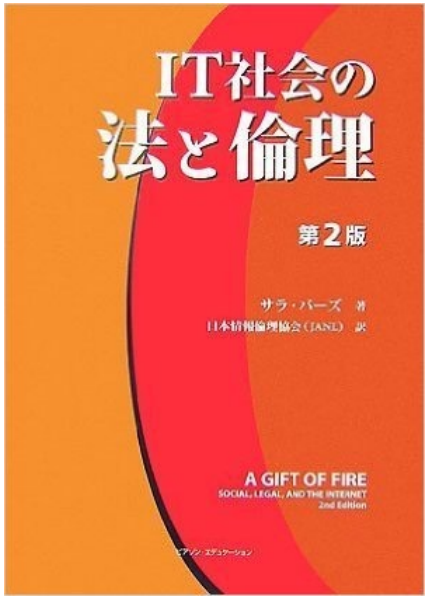


参考文献

- パーソナルデータの衝撃
  - 一生を丸裸にされる「情報経済」が始まった

ダイヤモンド社
ISBN:978-4478064832

- IT社会の法と倫理



ピアソンエデュケーション
ISBN:978-4894714304