情報セキュリティポリシーと個人情報保護の取り組み

武蔵大学情報システムセンター
小野成志

あらまし

- 情報セキュリティポリシーとは
- 個人情報保護法とは
- 情報セキュリティと個人情報保護の関係
- 若干の事例

情報セキュリティポリシー

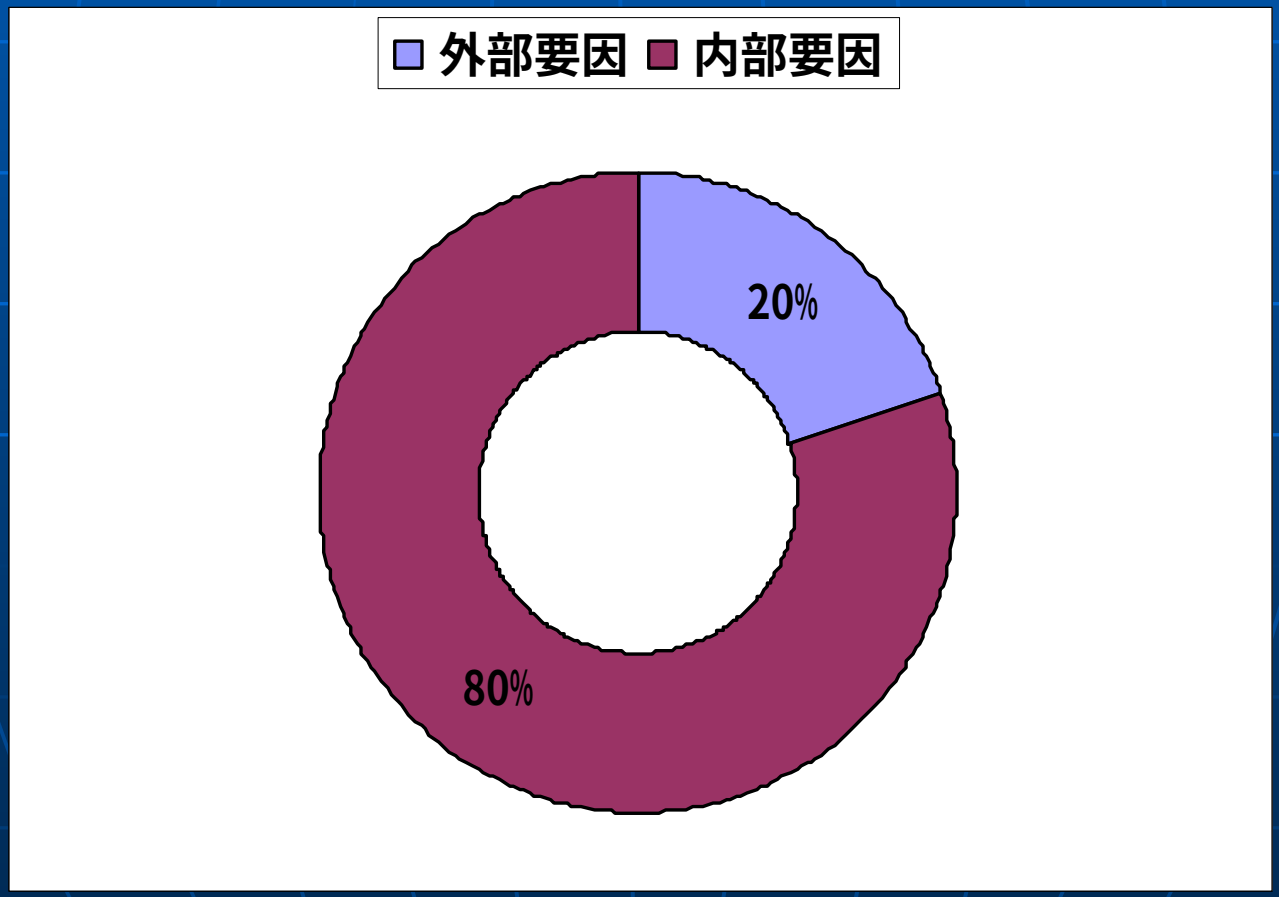
- 情報資産の保全
- システム管理者だけのセキュリティ対策から全ユーザの取組むセキュリティ対策へ
- 内部からのセキュリティ侵害対策

大学における情報資産

- 事務システムの価値は高い
  - 個人情報
  - 入試情報
  - 財務情報等
- 教育システムの価値は相対的に低い
  - 電子メール
  - 個人情報の一部

潜在的な脅威

- セキュリティ侵害の80％は内部から



情報セキュリティの本質

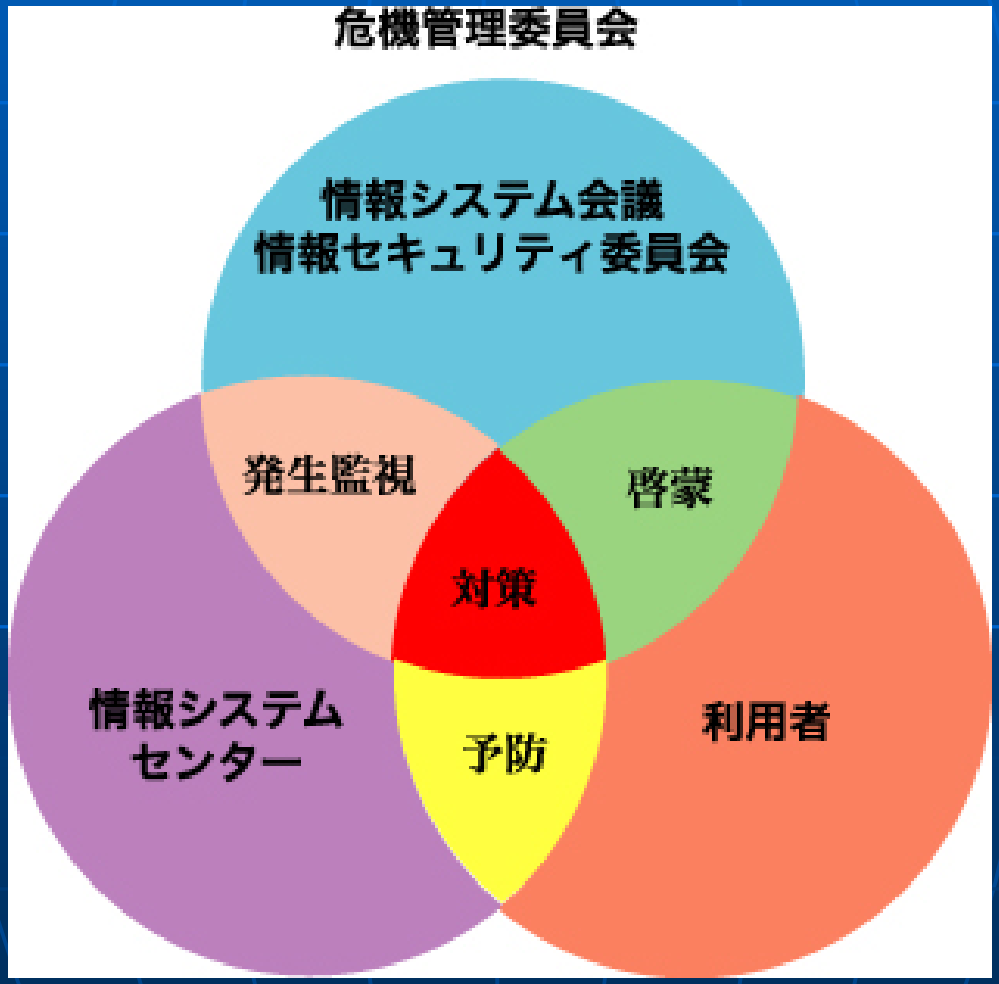
- PCが極めて高性能になった
- 善意だが未熟な内部ユーザ
- 悪意のある内部ユーザ

⇒組織的な対応が必要

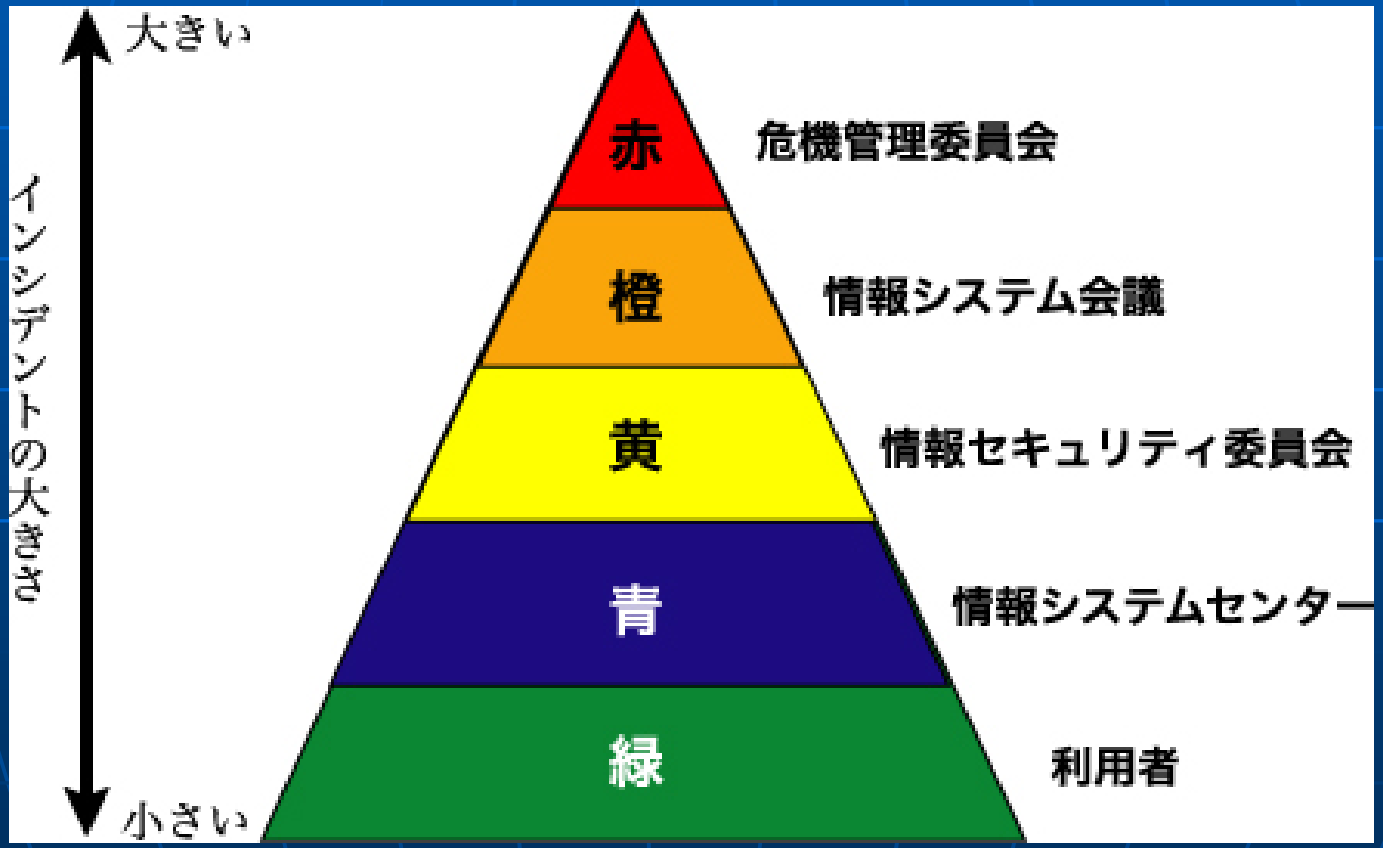
武蔵大学の事例

- 組織
- 対策
- 監査
- ポリシー見直し

情報セキュリティの組織



インシデントの区分


大きい
インシデントの大きさ
小さい
赤
危機管理委員会
橙
情報システム会議
黄
情報セキュリティ委員会
青
情報システムセンター
緑
利用者

インシデント状態：低い

- 通常はこの状態
- ユーザが主体
- インシデントの兆候に注意をはらう

インシデント状態 注意

- インシデントが発生している
- 情報セキュリティ委員会から注意喚起
- 情報セキュリティ担当やシステム担当は特別な注意が必要な場合もある。

インシデント状態：　高い

- 被害の発生
- システムの一部の運用停止
- 利用制限
- 情報セキュリティ委員会が対応

インシデント状態：重大

- 深刻な被害
- 基幹LANの停止または制限
- 財務的措置の発動
- 情報システム会議が対応

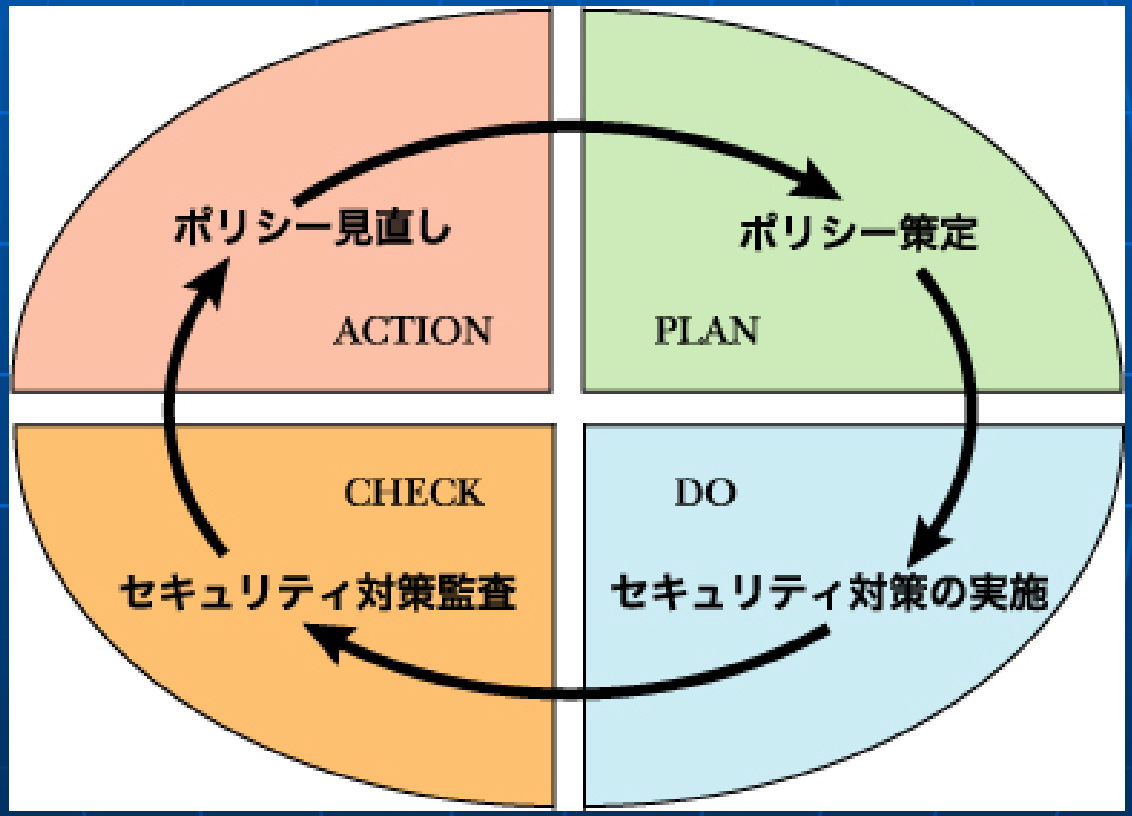
インシデント状態：深刻

- 深刻な被害
- 法的措置に対する対応
- マスコミ対策
- 危機管理委員会が対応

武蔵大学では高いまで

- ワームの侵入
  - 全教員に注意喚起のメール
  - ダイヤルアップサーバ停止
  - 研究室立ち入り調査
  - 大学院生室立ち入り調査
- 制度やシステムの未整備のため駆除まで時間を要した。

セキュリティのPDCA



システム監査の実施

- 内部監査の実施
- 外部監査の実施
  - セキュリティ会社の利用

ポリシーの見直し

- ポリシーは年に一度は見直される
- タイムリーな修正もある

セキュリティポリシー下の個人情報

- 情報システムからの漏洩を防ぐ
- 情報漏洩の被害にfocus

損害額はどのくらいか

- １９９８年早稲田大学での江沢民講演会名簿事件では1万円／件（２００２年東京高裁）
- １９９８年宇治市情報漏洩1万5千円／件（２００１年大阪高裁）
- 2003年度ジャパネット高田では1万5千円／件

JNSAの試算

- 電子メールで最大4,000円／件
- 基本4情報に付加される情報によっては30万円／件
- 平均4万5千円／件

（2003年度セキュリティインシデントに関する被害報告）

個人情報保護からみると

- 損害額が問題なだけではない

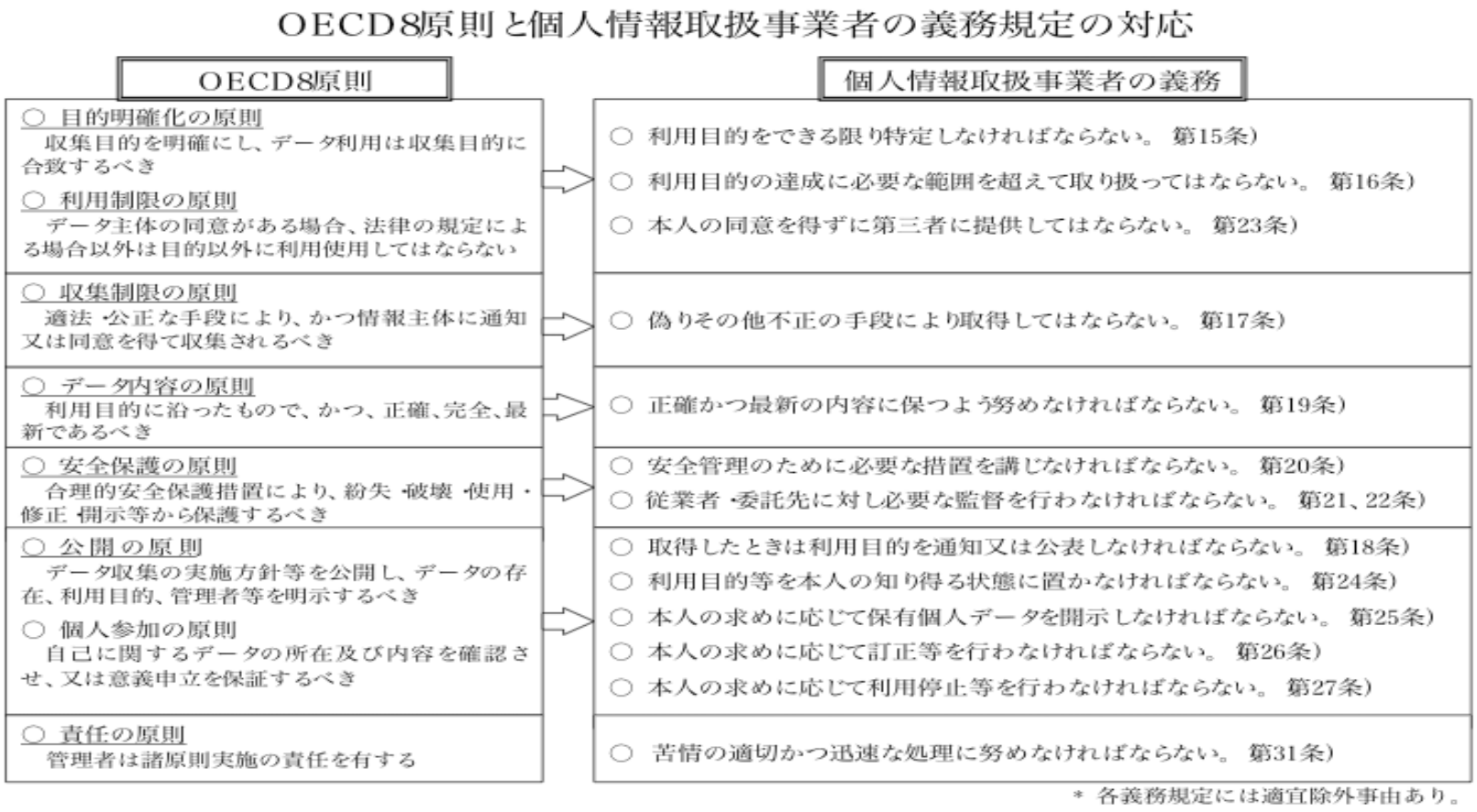
個人情報保護法の特色

- ミニマムスタンダード
- 解釈の余地が多い

個人情報保護法理解のリソース

- OECD８原則
- 個人情報の保護に関する法律
- 同施行令
- 個人情報保護法の概要（内閣官房作成）
- 文部科学省告示（パブリックコメント中）
- 経産省ガイドライン
- 個人情報保護に関するコンプライアンス・プログラムの要求事項(JISQ15001)

OECD８原則と個人情報保護



内閣官房作成

概要

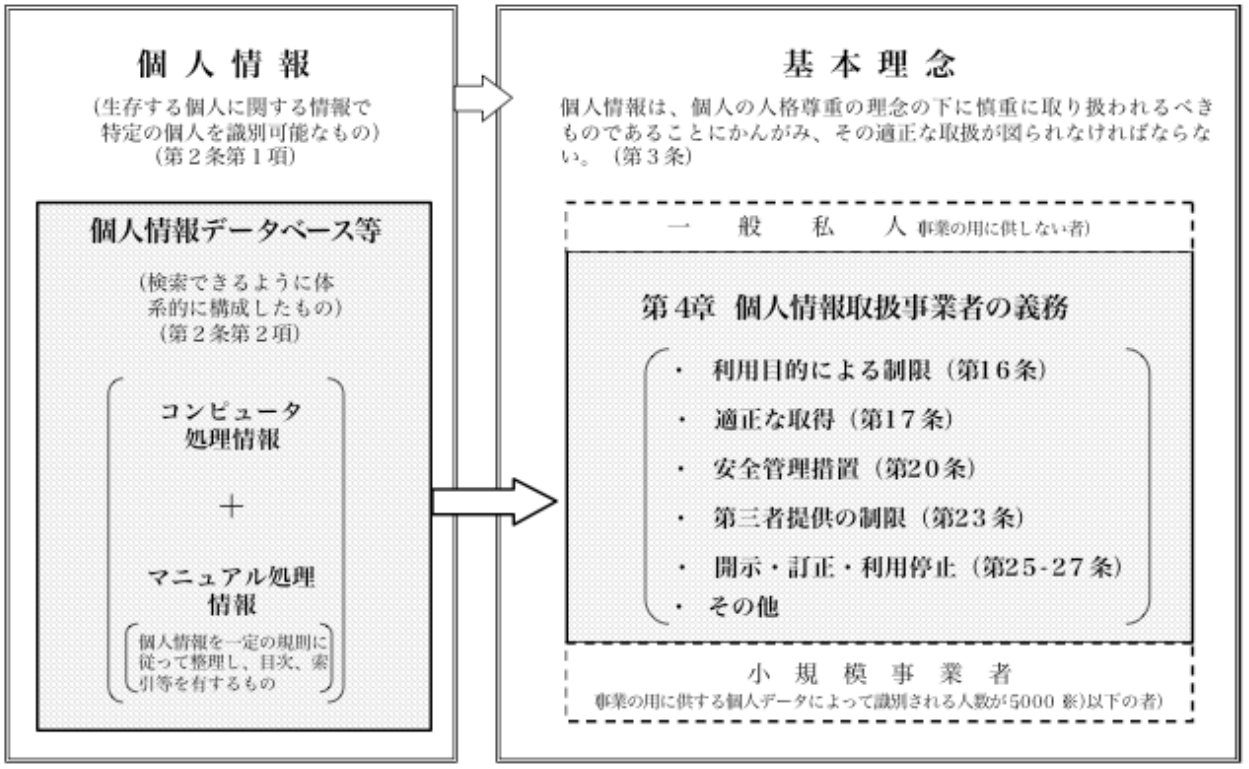
- 平成15年5月30日一部施行
- 2年以内に全面施行
- 個人情報を取り扱う事業者が遵守すべき義務
- 個人情報データベース等が対象

施行令での定め

- 平成17年4月全面施行
- データベース以外にも名簿等が対象
- 5000件以上の個人情報を有する事業者が対象

個人情報と事業者の範囲

4. 事業者の遵守すべき個人情報の取扱いのルールについて
(1) 対象となる個人情報、事業者について
① 対象となる個人情報、事業者の範囲



※市販のカーナビや電話帳をそのまま利用する場合、これらに含まれる個人データによって識別される人数は算定に含まれない。

内閣官房作成

個人情報データベース

- 個人情報を含む情報の集合物
- 電子計算機を用いて検索可能な体系的に構成したもの
- 個人情報を容易に検索可能な体系的に構成したもの

個人情報の定義

- 生存する個人に関する情報
- 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。

生存する個人の情報

- 生存中の遺族親族に関わる情報は保護される

個人情報に当たらないもの

- 死亡した個人に関する情報
- 法人の情報
- 個人を特定できない情報
  - 匿名化された情報

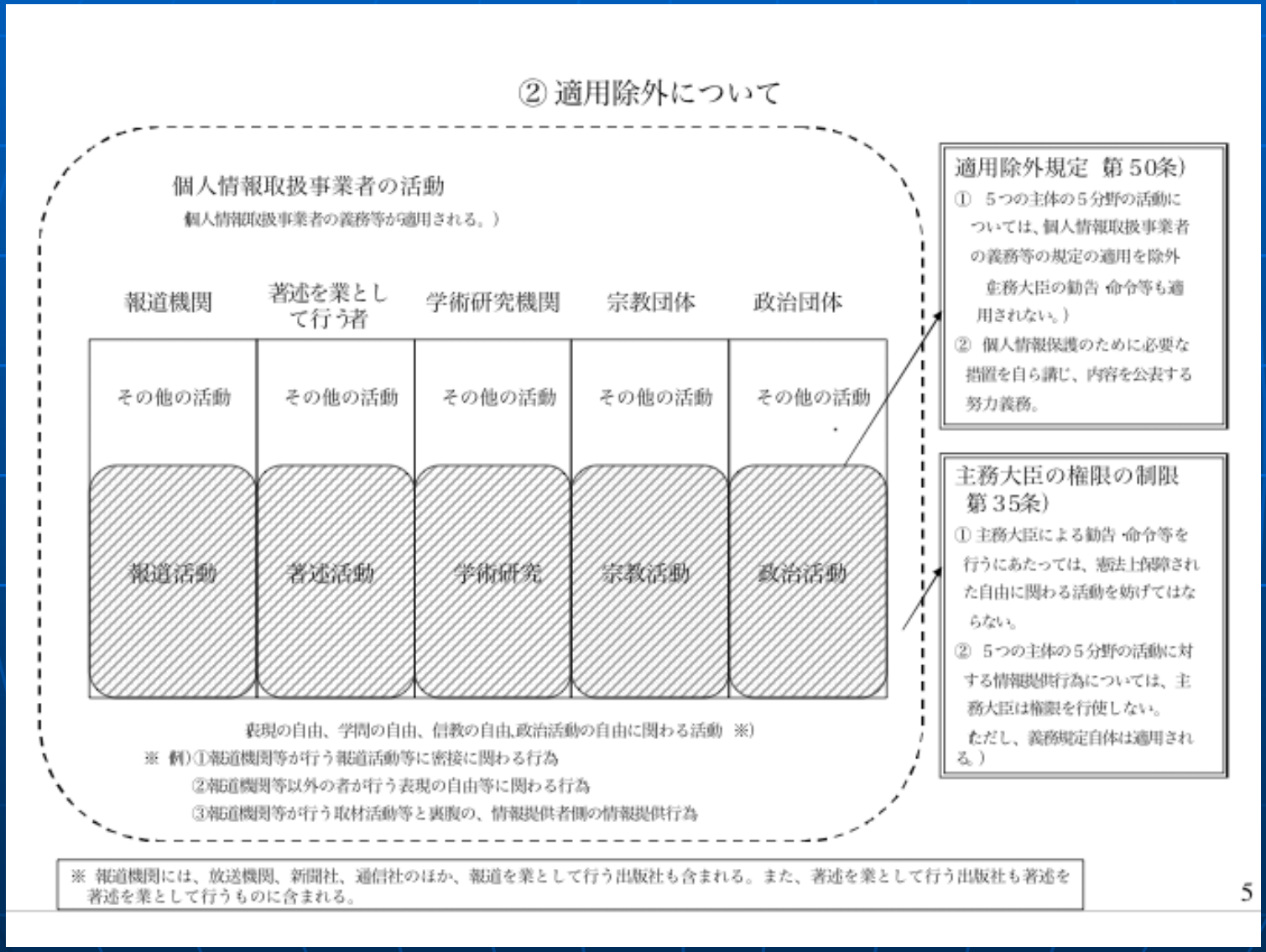
事業の用に供する

- 特定の目的をもって反復継続して遂行される同種の行為の総体を指し、営利、非営利の別を問わない

容易に照合できる情報

- 受験番号、学籍番号をキーに検索できる情報
- アカウント情報、アンケート調査結果

適用除外規定



内閣官房作成

大学での個人情報

- ほとんどすべてが対象となる

センシティブ情報（JISQ15001）

- 思想，信条及び宗教に関する事項。
- 人種，民族，門地，本籍地（所在都道府県に関する情報を除く。），
- 身体・精神障害，犯罪歴，その他社会的差別の原因となる事項。
- 勤労者の団結権，団体交渉及びその他団体行動の行為に関する事項。
- 集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項。
- 保健医療及び性生活。

センシティブ情報の扱い

- そもそも扱うべきではない
- 情報流失に対する責務は重い

利用目的の明確化

- 利用目的をできる限り特定しなければならない。（１５条）
- 利用目的の達成に必要な範囲を超えて取り扱ってはならない。（１６条）
- 利用目的を通知又は公表しなければならない。（１８条）
- 利用目的を変更したときが通知又は公表しなければならない。（１８条）

不正取得の禁止

- 偽りその他不正の手段により取得してはならない。（１７条）

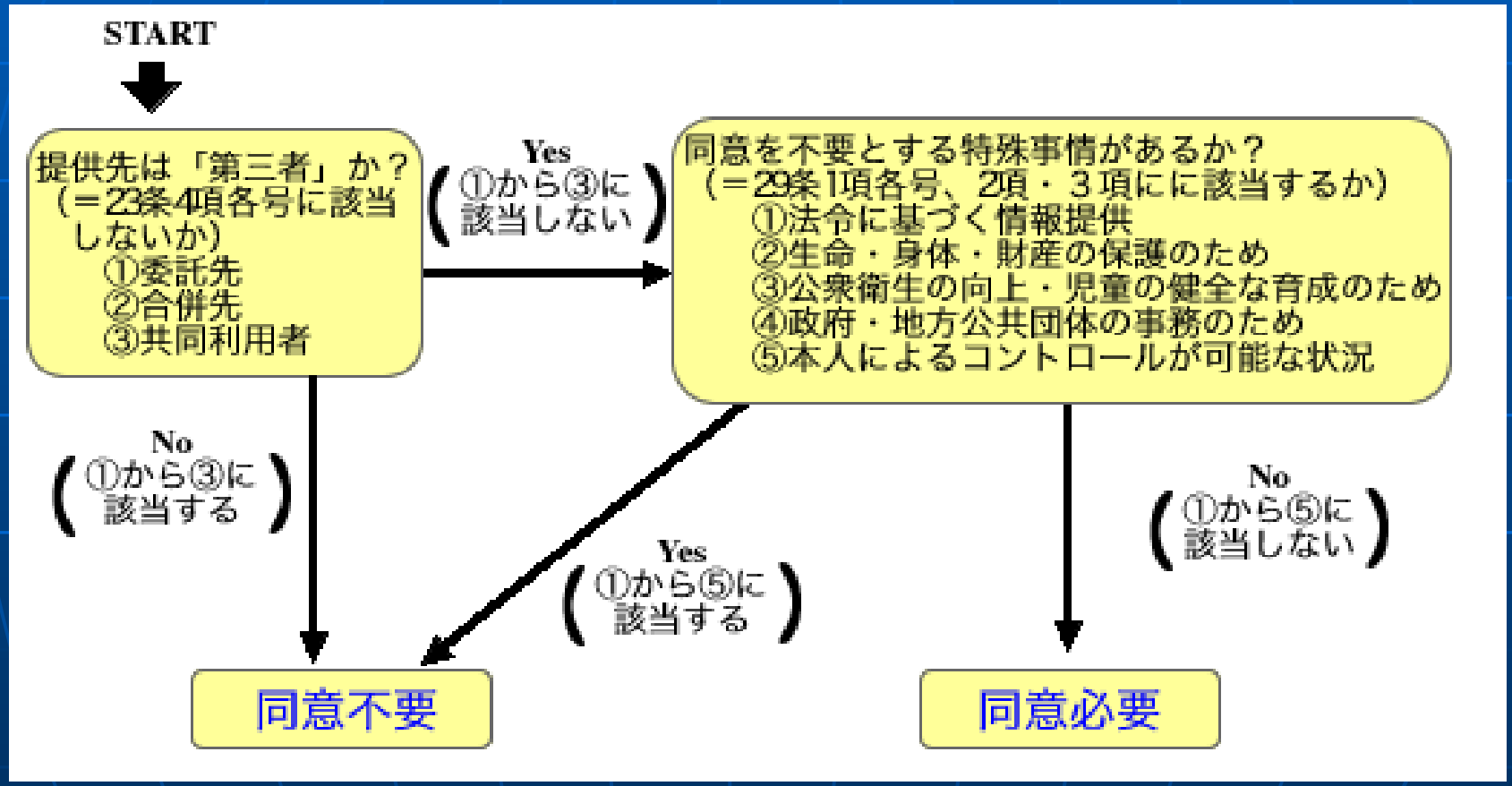
個人情報の管理

- 正確かつ最新の内容に保つよう努めなければならない。（１９条）
- 安全管理のために必要な措置を講じなければならない。（２０条）

第三者供与

- 本人の同意を得ずに第三者に提供してはならない。（２３条）
  - 共同利用についてあらかじめ同意を得ている範囲での提供は適用外
  - 利用目的達成のための業務委託の際の提供は適用外
  - 合併等による事業継承時の提供は適用外。

第三者への提供


START
提供先は「第三者」か？
（＝23条4項各号に該当しないか）
①委託先
②合併先
③共同利用者
Yes
（①から③に該当しない）
同意を不要とする特殊事情があるか？
（＝29条1項各号、2項・３項にに該当するか）
①法令に基づく情報提供
②生命・身体・財産の保護のため
③公衆衛生の向上・児童の健全な育成のため
④政府・地方公共団体の事務のため
⑤本人によるコントロールが可能な状況
No
（①から③に該当する）
Yes
（①から⑤に該当する）
No
（①から⑤に該当しない）
同意不要
同意必要

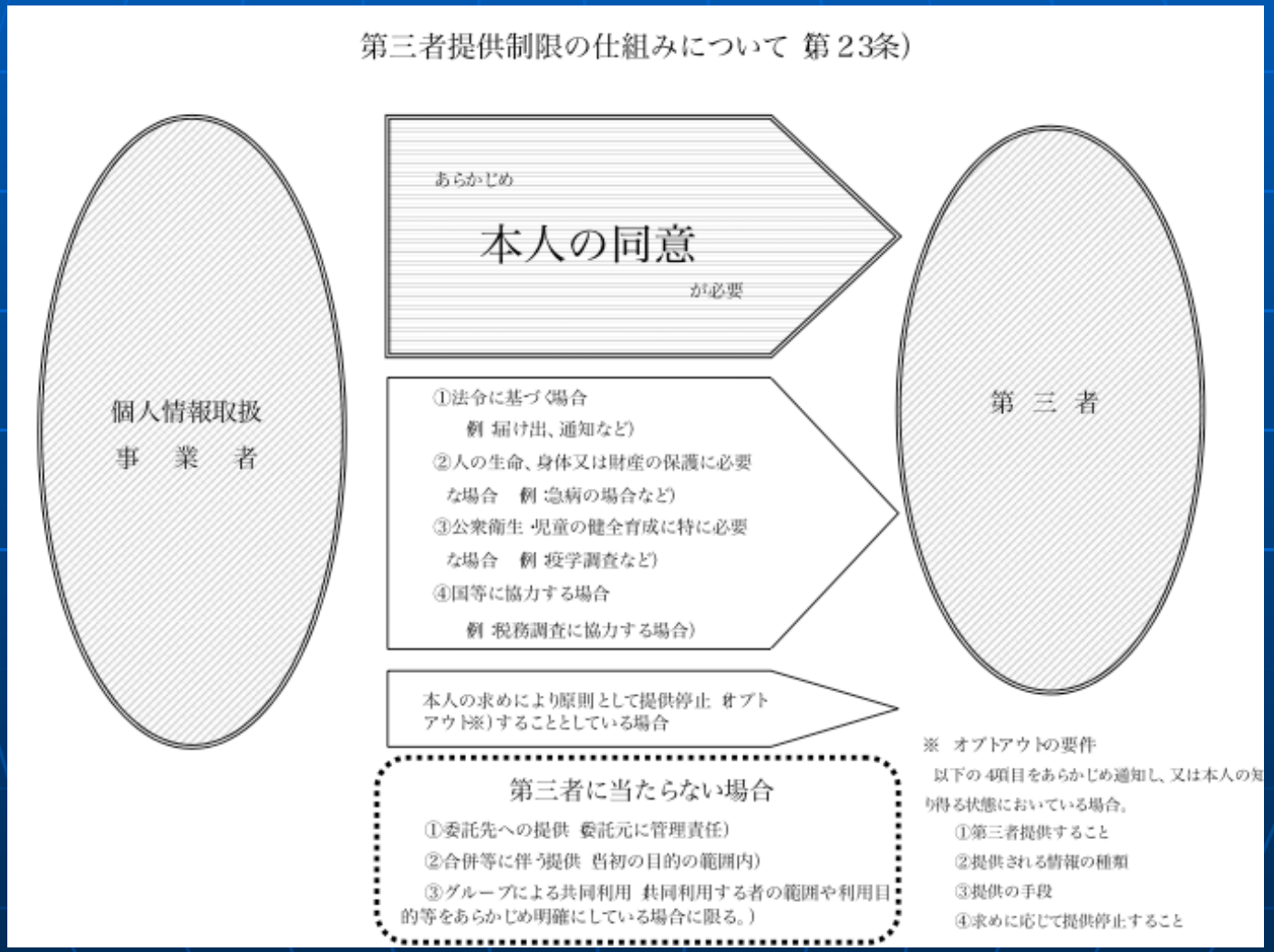
本人の関与

- 事業者名、利用目的等を本人の知り得る状態に置く（２４条）
- 本人の求めに応じて保有個人データを開示（２５条）
- 本人の求めに応じて訂正等を行なう（２６条）
- 本人の求めに応じて利用停止等を行う（２７条）
- 適切かつ迅速な苦情の処理に努める（３１条）

本人の知りえる状態

- 以下の項目を本人に通知
  - 第三者への提供を利用目的とすること。
  - 第三者に提供される個人データの項目
  - 第三者への提供の手段又は方法
  - 本人の求めに応じて提供を停止すること（オプトアウト）

第三者提供制限



内閣官房作成

例外処理

- 合理的な理由がある場合は、応じない決定も可能（本人に対し、遅滞なく、その旨を通知しなければならない）

監督

- 従業者・委託先に対し必要な監督を行わなければならない。（２１条、２２条）

委託業者への対応

- 秘密保持契約の締結
- 定期的な会議での点検
- 議事録の作成
- データを廃棄した誓約書

罰則

- 主務大臣からの勧告
- 6ヶ月以下の懲役、30万円以下の罰金
- 従業員が行なった違反にたいしては、事業者も罰則の対象

文部科学省の告示

- 成績管理
  - 管理者の設置
  - モラル教育
- 成績の開示
  - 本人または代理人に対しても慎重な取り扱いを求めている
- 第三者への提供
  - 同窓会等への提供基準

同窓会名簿

- 同窓会の本来の目的で利用する分には対象にならない（法18条4項4号）
- 名簿を使って商用のDM発送した
  - 同窓生が提供した場合は対象にならない。
  - 学校が提供した場合は対象となる

クラブ活動等

- 学校のクラブ活動の名簿は、クラブ活動が一般にいう「事業」に当たらないとして対象外になる。（156回国会質問答弁より）
- ゼミ演習活動は事業活動の一部のため法の範囲

事業者対象外

- 学校のクラブ活動の名簿は、クラブ活動が一般にいう「事業」に当たらないとして対象外になる。（156回国会質問答弁より）
- 学術研究目的は適用除外だが、その範囲は明確ではない

情報セキュリティと個人情報

- 情報セキュリティから見た個人情報
  - 情報資産の一部として位置づけ
  - 漏洩を守るべきもの
- 個人情報から見た情報セキュリティ
  - OECD８原則のうちの対策の一つ
  - 個人の権利保護

OECD8原則からみた情報セキュリティ

- 収集制限の原則　×
- 情報内容の原則　△
- 目的明確化の原則　×
- 利用制限の原則　×
- 安全保護の原則　○
- 公開の原則　△
- 個人参加の原則　×
- 責任の原則　×

情報セキュリティの責任分担

- CIOは不可欠
- 組織毎の責任者が必要

個人情報の責任分担

- Chief Privacy Officer(CPO)が必要
- 個人情報システム毎の管理者と監督者が必要

CIOとCPO

- 利害はしばしば相反する
- CIOは情報資産を内部の関係者から守る
- CPOは個人の権利を内部の関係者から守る

武蔵大学の取り組み

- 個人情報に関する勧告
- 責任者の設置
- 新入学生への入学前の告知

個人情報保護責任者の設置

- 総括的な責任はCIO
  - CPOとの分離ができていない
- 教員は各学部長、職員は総務部長
  - 組織単位での大まかな責任者

新入学生への開示

- 執務上必要な限りでの利用（利用目的限定）
  - 利用目的限定が不十分
- 共同事業者の開示（同窓会父母の会）
  - 監督方針が曖昧

To do…

- 情報セキュリティから独立した個人情報保護ポリシーの策定
- 責任、権限関係の確定
- 成績管理ポリシーの策定
- 在学生へのアナウンス
- 共同事業者、委託業者に対する監督方針

…