

個人情報保護法と企業の対応

管理者が留意したいコンプライアンス・
プログラムの最新論点

ニフティ(株) 法務部 鈴木 正朝

はじめに

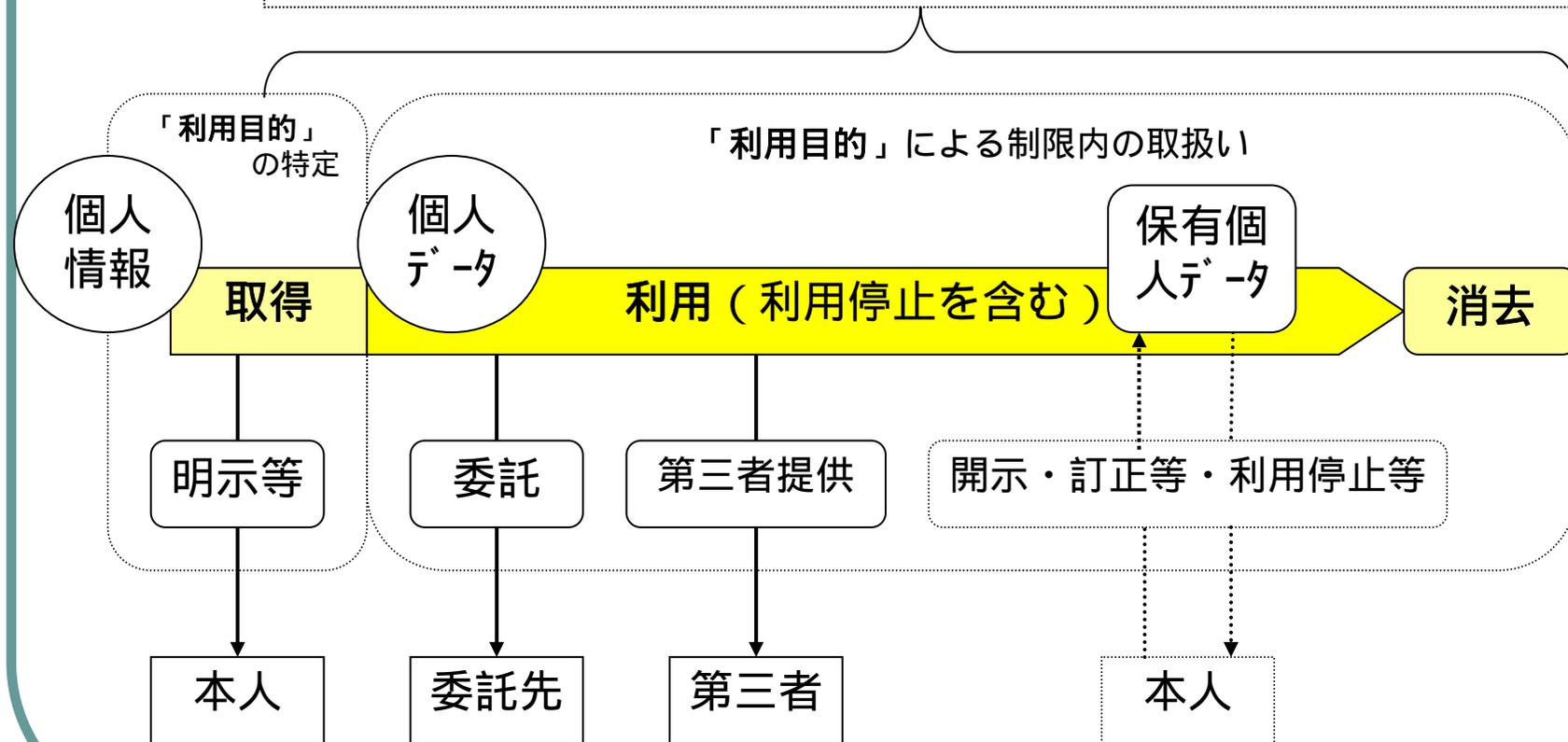
- 個人情報保護法は実験的法律
- 人・物・金に関する社内制度
- 人・物・金に関する法制度
- 情報に関する社内管理制度
- 情報に関する法制度
- コンプライアンス・プログラムの考え方

論点「個人情報」は誰のものか？

- 「個人情報」とは？ (定義の確認)
- 「個人情報」の帰属性を論じる意味
 - 手帳に記載された個人情報
 - ネット上を漂う個人情報
 - 遺伝子に関する個人情報
- 物権法制 (ex. 所有権) とのアナロジー
 - 知的財産権法制 (ex. 著作権) とのアナロジー
- 自己情報コントロール権的発想の根源

論点「個人情報」のライフサイクル

「個人データ」の管理（安全管理措置、従業員の監督、委託先の監督）



1. ビジネスプランと個人情報のライフサイクル

- **個人情報の特定**
- **当該部門の個人情報を取り扱う業務を全て特定する。**
- **当該業務ごとに個人情報の取得から消去に至る個人情報のライフサイクルを確認する。**

2. 個人情報取得

(1) 利用目的の特定

- 利用目的をどのように特定しているかを確認する。

(2) 直接取得の場合における利用目的の明示

- 利用目的を本人にどのように明示しているかを確認する。

(3) 間接取得の場合における利用目的の公表・通知(及び契約の確認)

- 直接本人から取得するのではなく、社内の顧客DB等から取得する場合、利用目的の範囲内で取り扱っているかを確認する。
- システム連携などにより社内外の個人データを自動的に取得していないかどうかを確認する。

3. 個人情報利用・管理

- (1) 個人情報(個人データ)の委託と委託先の監督
- 個人情報の委託先(再委託先を含む)をすべて特定する。
 - 個人情報の取扱いに関して委託契約(または覚書等)を締結しているか確認する。
 - 委託先従業者との誓約書の取得状況を確認する。
 - 個人情報の授受の方法を確認する。
 - 委託契約終了時の措置として個人情報の取扱いを確認する。
 - 委託先の選定基準を確認する。

3 . 個人情報(個人データ)の利用・管理

(2) 個人情報(個人データ)の第三者提供

- 個人情報を第三者に提供していないかを確認する。
 - システム連携などにより、個人データが取引先、提携先に自動的に送信されていないかどうかを確認する。
 - 電子メールアドレスを提携先に提供していないかどうかを確認する。

3 . 個人情報利用・管理

(3) 従業員の監督

- 各従業員がPC及びその他の媒体(紙を含む)で取り扱っている個人情報をどのように管理しているか。
- 監視ツールの適用

(4) 安全管理措置

- 情報セキュリティ対策
- ISMS制度(ISO/IEC17799)と法

5. 個人情報情報の消去

(1) 個人情報情報の保有期間

- 当該個人情報情報の保有期間を確認する。

(2) 消去の方法

- 消去の定義とその方法を確認する。

(3) 利用停止の方法

- 利用停止の定義とその方法を確認する。