

## 個人情報保護と 保健医療分野のプライバシーマーク制度



(財)医療情報システム開発センター  
プライバシーマーク付与認定審査室  
相澤直行

Ver. 20031105



## 患者からみた病院でのプライバシー

- 情報に関するプライバシー
  - 入院しているかどうかの情報
  - ナースステーションにある患者の名前が並んだボードが廊下から見える
  - ベッドの上に名前、主治医、診療科などを表示
- 生活面でのプライバシー
  - 視覚面、聴覚面、嗅覚面
- その他プライバシー
  - 外来の「中待ち」
  - 会計や投薬時の呼び出し
  - 受付や入院時の書類記入時
  - 給食内容

## プライバシーの権利

- プライバシーの権利とは
  - 諸権利の中で最も包括的で、かつ、文明人が最も価値があるとする権利
    - 一人にしておかれる権利
    - 自分に関する情報は自分でコントロールする権利
- プライバシーの権利の特徴
  - プライバシーの侵害は回復が困難
  - 何がプライバシーかの判断基準を定めることは困難

## プライバシー 個人情報

- 個人に関する情報であって
  - 氏名、生年月日その他の情報
  - 個人に付された番号、記号その他の符号
  - 個人の画像もしくは音声など
    - により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り、当該個人を識別できるものを含む)
- 個人情報の具体例
  - 氏名、性別、生年月日、住所、勤務先、学歴、家族構成、本籍地、電話番号、電子メールアドレスなど
  - 銀行等の口座番号、クレジット番号、健康保険番号、免許証番号、パスポート番号、住民基本台帳番号など
  - 趣味・嗜好、購買履歴、**保健医療情報**など
  - 肖像、声

# 個人情報の基本分類

個人情報の基本分類

レベル	個人情報の種類
最も低いレベル	日常生活を送る中で意識的に提供しているもの 氏名、住所、電話番号、年齢、家族、配偶者、勤務先など、個人の基本属性情報
基本的に知られたくないレベル	金融や資産などに関する個人信用情報、趣味・嗜好、身体特性、交友関係、学歴・結婚歴、性格判断、心理テストなどの情報
最も知られたくないレベル	個人医療情報、カルテ、看護記録、検査記録、レセプトなどの医療関連情報、人種・民族・門地・本籍地、信教・政治的見解、労働組合への加盟、保健医療・性生活などの <b>センシティブな情報</b>
その他	日常的に意識せずに提供している無意識提供情報。 例えば、クレジットカードの利用により、カード会社と加盟店に蓄積する購買記録など

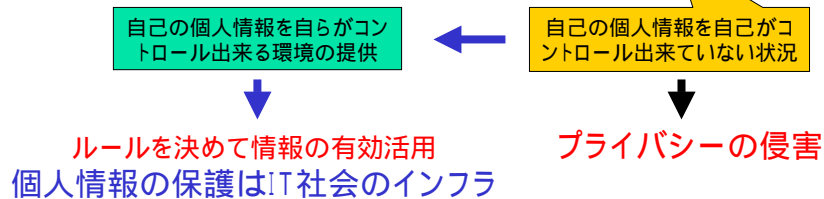
～電子商取引推進協議会(ECOM)の分類による～

# 個人情報の保護はIT社会のインフラ

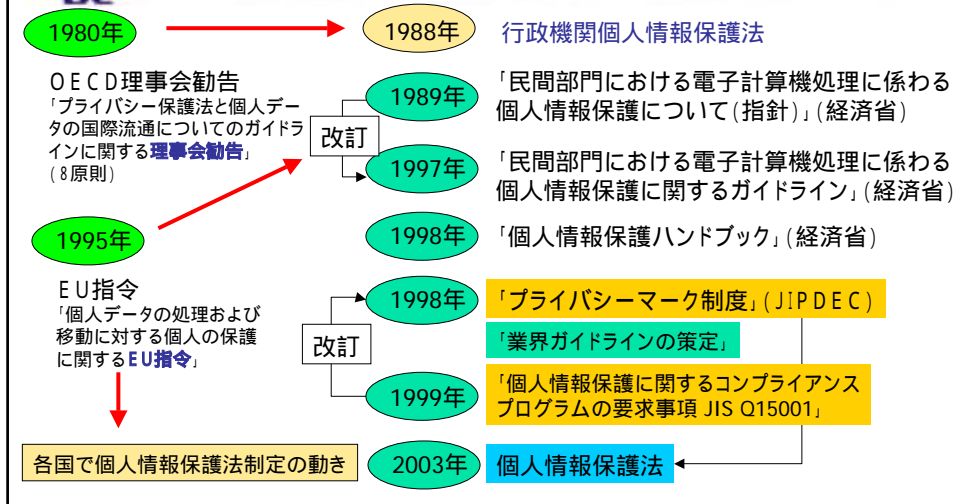
ネット上では故意・過失のいずれにせよ、リアル環境に比べて極めて大量の個人情報が瞬時に漏洩してしまう危険性を持っている

**個人情報のリスク**

- 知らない間に集められる……………不正な収集
- 知らない間に使われ・売買される……………不正な利用
- 誤ったまま使われる……………入力ミス、改ざん、破壊
- 世の中に無秩序に漏えいされる……………漏えい



# 個人情報保護に関する動向



## OECDの個人情報保護8原則

OECD理事会勧告(1980年)

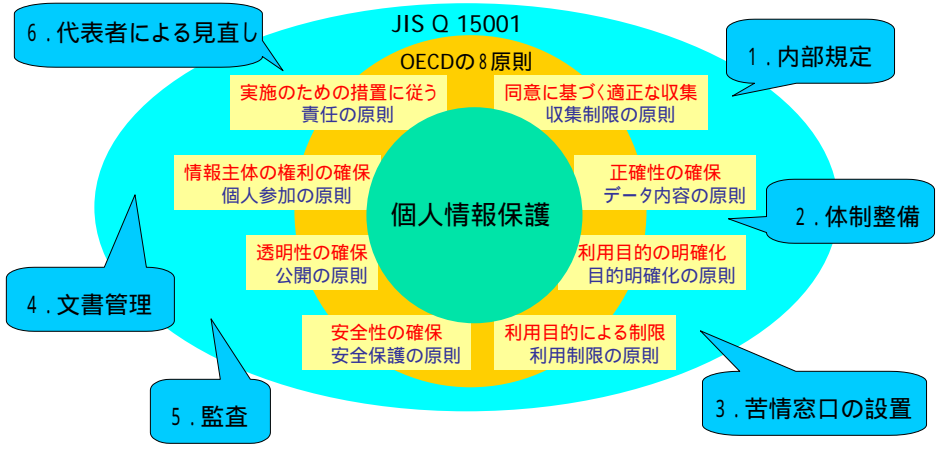
1. **収集制限の原則**：同意を得た個人データのみ限定する
2. **データの正確性の原則**：正確、完全かつ最新のものに保つ
3. **目的明確化の原則**：データの利用目的は収集時に定められる
4. **利用制限の原則**：明確化された目的のみに利用される
5. **安全保護の原則**：合理的な安全保護措置によって保護される
6. **公開の原則**：個人情報に関連した開発、慣行、ポリシーおよび連絡先情報を公開する
7. **個人参加の原則**：情報主体のコントロール下におく
8. **責任の原則**：上記の諸原則を実施するための措置に従う責任を有する

### JIS Q 15001(1999)の追加事項

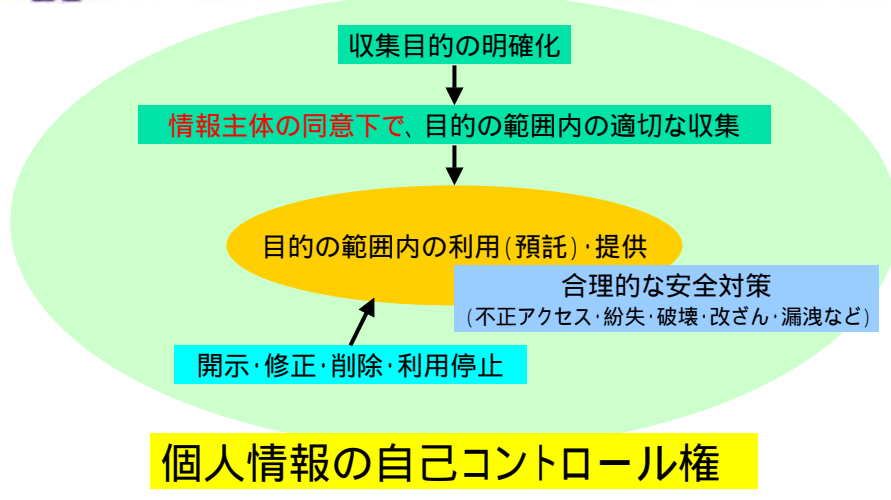
1. 内部規定
2. 体制整備
3. 苦情窓口の設置
4. 文書管理
5. 教育・監査
6. 代表者による見直し

# JIS Q 15001 コンプライアンス・プログラムの概念

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



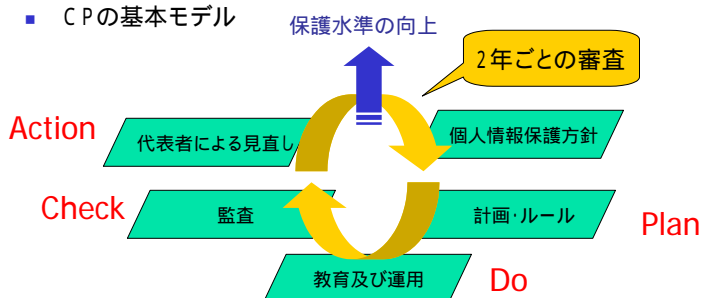
## 個人情報保護とは



# 個人情報保護に関するコンプライアンスプログラム (JIS Q 15001) とは



- 個人情報保護を実践するためのマネジメントシステム
  - 個人情報保護の基本方針を策定・公表
  - 運用ルールを定め、教育・監査の計画を立案
  - 教育し、ルール通りに個人情報を取り扱う
  - ルール運用の監査を行う
  - 運用ルールの見直しを行う
- CPの基本モデル



# JIS Q 15001の要求事項



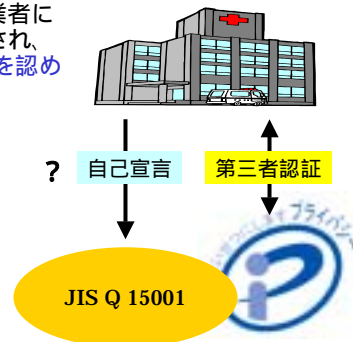
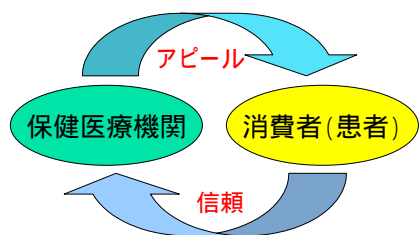
- 4.1 一般要求事項
- 4.2 個人情報保護方針 合理的な安全対策
- 4.3 計画
- 4.3.1 個人情報の特定
- 4.3.2 法令及びその他の規範
- 4.3.3 内部規定
- 4.3.4 計画書
- 4.4 実施及び運用 収集目的の明確化  
情報主体の同意
- 4.4.1 体制及び責任
- 4.4.2 個人情報の収集に関する措置
  - 4.4.2.1 収集の原則
  - 4.4.2.2 収集方法の制限
  - 4.4.2.3 特定の機微な個人情報の収集の禁止
  - 4.4.2.4 情報主体から直接収集する場合の措置
  - 4.4.2.5 情報主体以外から間接的に収集する場合の措置
- 4.4.3 個人情報の利用及び提供に関する措置
  - 4.4.3.1 利用及び提供の原則
  - 4.4.3.2 収集目的の範囲外の利用及び提供の場合の措置
- 4.4.4 個人情報の適正管理義務
  - 4.4.4.1 個人情報の正確性の確保
  - 4.4.4.2 個人情報の利用の安全性の確保
  - 4.4.4.3 個人情報の委託処理に関する措置
- 4.4.5 個人情報に関する情報主体の権利
  - 4.4.5.1 個人情報に関する権利
  - 4.4.5.2 個人情報の利用又は提供の拒否権
- 4.4.6 教育
- 4.4.7 苦情及び相談
- 4.4.8 コンプライアンス・プログラム文書
- 4.4.9 文書管理
- 4.5 監査 開示・修正・削除  
利用停止
- 4.6 事業者の代表者による見直し

目的の範囲内の利用 (預託)・提供

開示・修正・削除  
利用停止

## プライバシーマーク制度とは

- 個人情報についてJIS Q 15001に則った適切な保護措置を講ずる体制を整備している事業者(保健医療機関)であるかを審査認定し、認定された事業者には、その旨を示すプライバシーマークが付与され、事業活動に関してプライバシーマークの使用を認める制度



## プライバシーマーク取得の メリット・デメリット

- メリット**
  - 国民からの信頼
  - 委託元からの信頼
- デメリット**
  - 人的、物的リソースの確保が必要
    - コンサルタント、管理コスト、専任の担当者、入退管理システム、セキュリティ対策ソフト……
  - 社会からの見る目が厳しくなる
    - 漏洩事故による社会的信用の失墜

## 制度の実施体制

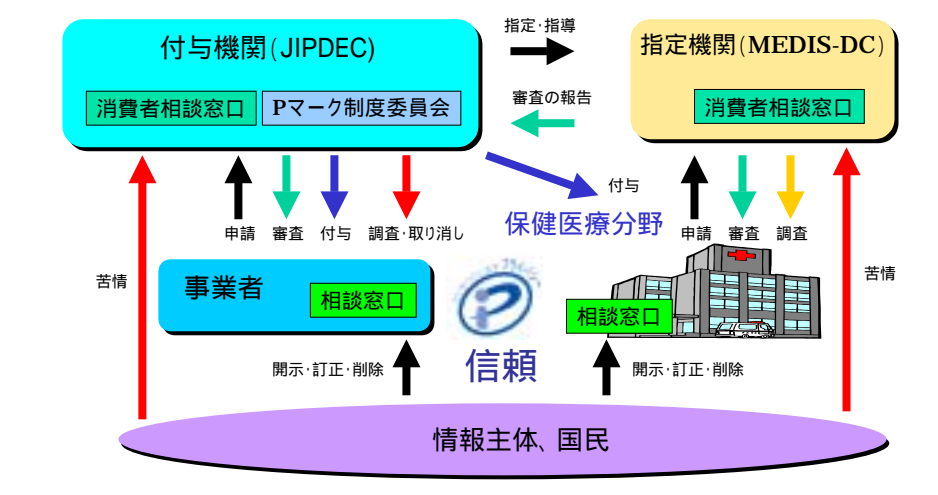
- プライバシーマーク制度は以下の2種類の機関で運営される
  - プライバシーマーク付与機関(付与機関)
    - 財団法人日本情報処理開発協会(JIPDEC)(A)
  - プライバシーマーク付与認定指定機関(指定機関)
    - 社団法人情報サービス産業協会(B)
    - 社団法人日本マーケティング・リサーチ協会(C)
    - 社団法人全国学習塾協会(D)
    - 財団法人医療情報システム開発センター(E)
- 付与機関と指定機関の仕事(\*は付与機関のみの仕事)
  - 事業者からのプライバシーマーク付与の申請を審査して認定すること
  - 消費者からの苦情を受け付けること
  - プライバシーマークを付与すること\*
  - 指定機関を指定すること\*
  - プライバシーマーク制度の維持\*

## 保健医療分野のプライバシーマーク付与の対象

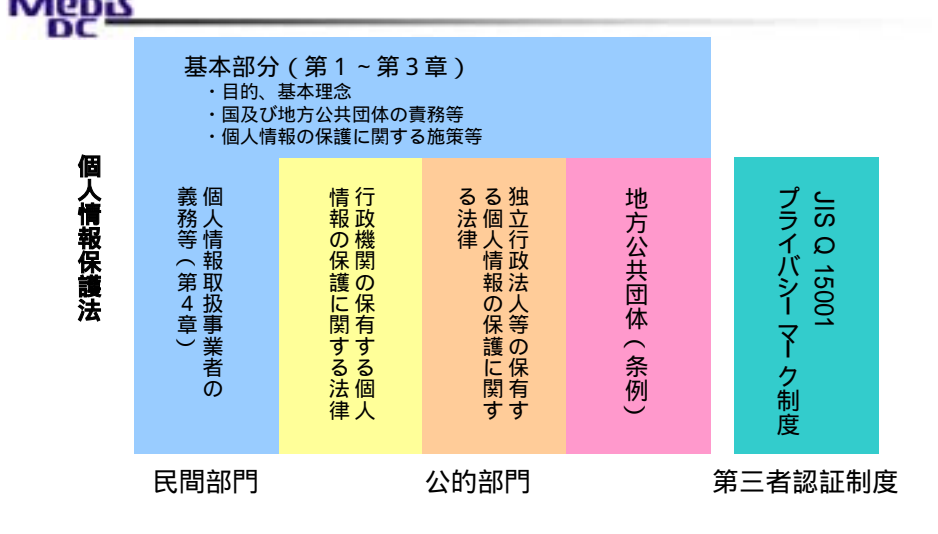
- 国内に活動拠点を有する事業者で、「医療機関の認定指針」の適用範囲とする保健・医療に関する事業を主に営む者を対象とする
  - 例えば、病院、診療所、その他保健・医療に関連する事業等を営む事業者が該当します。
- さらに次の条件を満たしている事業者
  - JIS Q 15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」および「医療機関の認定指針」に準拠したCPを定めている
  - CPに基づき個人情報の適切な取扱いが実施され、または実施可能な体制が整備されている(教育 運用 監査 見直し)
  - 欠格事項に該当しない事業者



## 保健医療分野のプライバシーマーク制度



## 個人情報保護制度





## 個人情報保護法と JIS Q 15001 (プライバシーマーク制度)

- ミニマムスタンダード
  - 事業者による自主的な保護措置の上乗せの可能性を排除していない  
JIS より高いレベルの措置
- 取扱データ件数による適用除外
  - 「特定の個人の数」の合計が過去6ヶ月以内のいずれの日においても5千を超えない者  
JIS 除外なし
- 全ての個人情報に等しい規制
  - 個別法の制定を求めている(第6条)
  - 個人信用情報分野、医療情報分野、電気通信関連情報分野  
JIS センシティブ情報の原則収集禁止
- 出口規制(オプトアウト)
  - 目的外利用、第三者提供にのみ情報主体の同意を求めている  
JIS 入口出口規制(オプトイン)



## 診療情報の開示について

- 診療情報は個人情報保護法の対象
  - 原則として本人からの開示の求めに応じる義務がある  
JIS 同様
- 問題点
  - 適用対象除外となる小規模の診療所が生じること
  - 死者の個人情報が遺族による開示請求の対象とならない場合がある  
JIS 原則として全てが対象
- 訴訟への対応
  - 医事紛争を前提とする場合は、指針の範囲外「診療情報の提供に関する指針」(日本医師会1999年)
  - 訴訟を前提としていることのみを理由に診療録の開示を行わないことは適当でない「診療に関する情報提供の在り方に関する検討会」(厚生労働省2002年)  
JIS 病院のポリシーとして明確にしておく必要がある

## 診療情報の提供等に関する指針

- 厚生労働省通知(医政発0912001号、平成15年9月12日)
  - 診療情報の提供等に関する指針の策定について  
<http://www.whoirei.mhlw.go.jp/hourei/doc/tsuchi/150916-a.pdf>
  - 診療情報の提供等に関する指針(別添)  
<http://www.whoirei.mhlw.go.jp/hourei/doc/tsuchi/150916-b.pdf>
- 提供(開示)対象はカルテだけではない(2)
  - 処方箋、手術記録、看護記録、検査所見記録、X線写真、紹介状、...
- 診療の提供は患者の同意が原則(4)
- 提供(開示)を拒める理由は2つだけ(8)
  - 診療情報の開示が、第三者の利益を害する恐れがある場合
  - 診療情報の開示が、患者本人の心身の状況を著しく損なう恐れがある場合
- 死者の情報も遺族へ提供(9)
- 診療情報の提供(開示)に関する規程の整備を求めている(12)

<http://privacy.medis.jp/>



## 参考図書



**医療の個人情報保護とセキュリティ**  
開原成允、樋口範雄[編]、有斐閣( ¥2,415)



**個人情報保護法の解説**  
園部逸夫 / 編、藤原静雄 + 個人情報保護法政研究会 / 著  
ぎょうせい( ¥3,333)



**逐条個人情報保護法**  
藤原静雄、弘文堂( ¥2,000)