# 個人情報保護法 あっぷでーと

@

Internet Week 2004

セキュリティホール memo ML BoF

タイムインターメディア

リスク管理室

太田 敏文

# はじめに

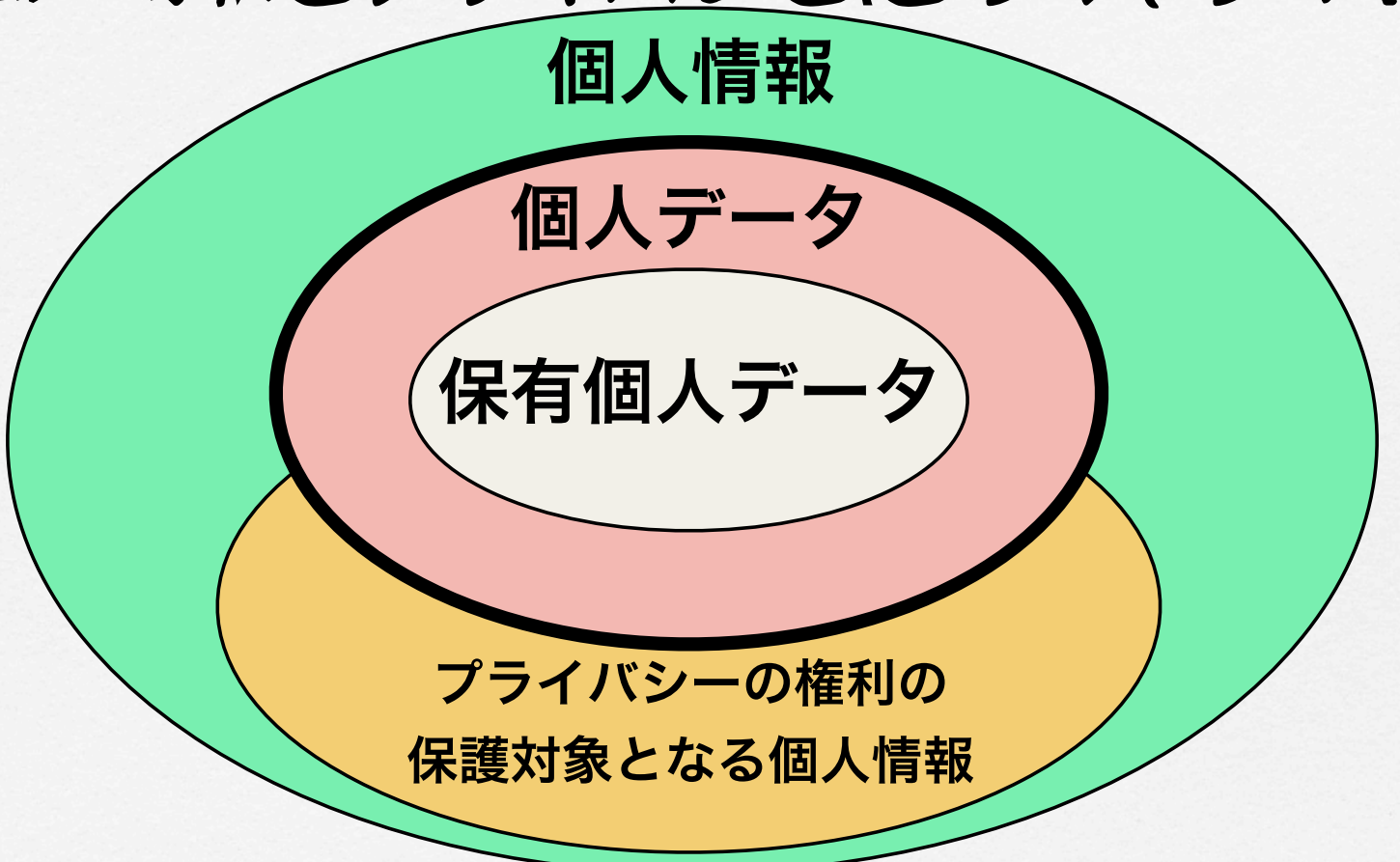
- こんなんでましたけど？(up date)
- あれから一年たちました
  - あと半年を切りましたが…
    - まだ間に合うのかな？
    - どうすれば間に合うの？
- 私のところはだいじょうぶ？？
  - ホントかなー？

# こんなんでてますぅ

- 各主務官庁からのガイドライン
  - 厚生労働省
    - 医療と雇用管理
  - 通商産業省
    - 製造業からサービス業
  - 総務省
    - 放送・通信事業者

ところで…

# 個人情報とプライバシとどうちゃうの？



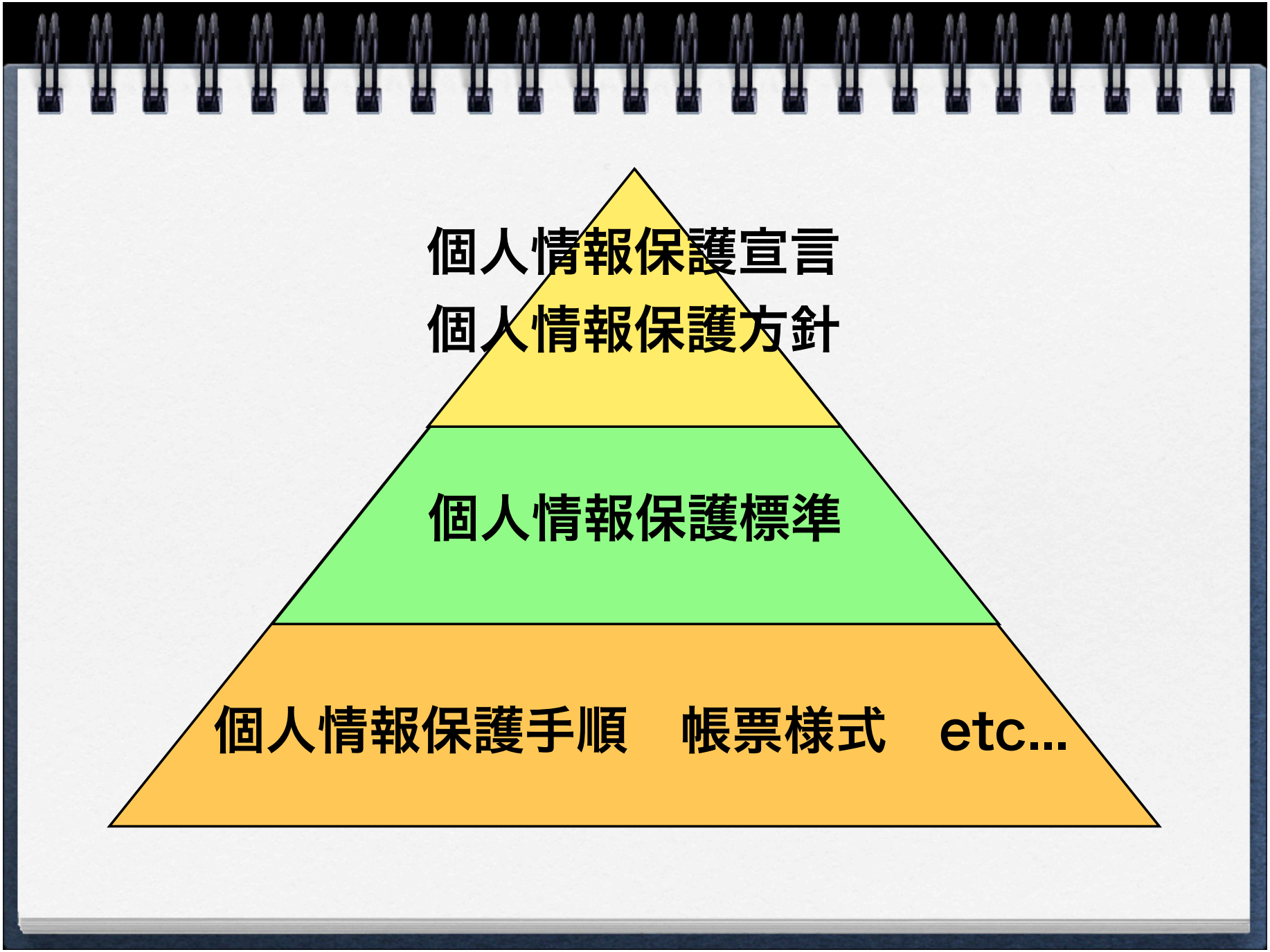

岡村　久道　著「個人情報保護法入門」より引用

# あと半年ありませんが…

- まだ間に合います(たぶん)
  - でも「根性」は必要ですよ ^^;
  - 年末までに文書、帳票類を整備(Plan)
  - １月までに実施開始(Do)
  - ２月までに実施状況の監査(check)
  - ３月までに文書、帳票類の改訂(Act)

# 文書、帳票の整備って…

- とーっても大変じゃない？ですか？
  - はい、大変です(泪
  - だから「頂上」と「麓」を攻めましょう
    - 頂上
      - 個人情報保護宣言
    - 麓
      - 個人情報取り扱い基本手順


個人情報保護宣言
個人情報保護方針
個人情報保護標準
個人情報保護手順　帳票様式　etc...

# 個人情報保護法の全面施行にあたっての
# 従業者の基本的な行動指針について

2004/11/29
リスク管理室

## 1．この文書の目的

この文書は、株式会社タイムインターメディア（以下当社）の第８期の最重要課題の一つである個人情報保護法の全面施行に対し、これに対応するために必要となる当社全従業者の最も基本的な行動指針を示す物です。法令の施行は2005年４月１日からですが、それまでに以下に述べる行動指針をよどみなく遵守できるようになるためにも、本文書の公開とともに全従業者の励行への協力をよろしくお願いいたします。

## 2．この文書の適用対象

この文書は、当社業務に従事する全従業者（役員、社員、準社員、契約社員、および協力会社社員、アルバイト、インターンなど）に例外無く適用します。

## 3．遵守事項

当社業務における全従業者は、以下の基本的行動指針を遵守しなければなりません。

### 1．入館証の常時携帯と提示

社屋構内に立ち入る際には「入退出標準」に基づき、入館証を常時提示した状態で立ち入ること（２００５年１月より実施予定）

### 2．アカウントの自己管理

・当社構内で使用するコンピュータ （当社備品・私物を問わない）には必ずパスワードロック（いかなる場合でも使用を開始する前に必ずパスワード認証が必要となる状態）をかけること
・いかなる事情においても共用アカウントの作成は、これを認めない
・いかなる事情においても他者へのパスワードの開示は、これを認めない

### 3．クリアスクリーンの励行

業務中に一時離席をする場合には、使用中の端末をログアウト（ログオフ）するか、パスワードロックされるスクリーンセーバを起動すること

### 4．クリアデスクの励行

業務中に一時離席をする場合には、机上に広げている書類等はフォルダ、またはバインダ等に収納してから離席すること

### 5．紙メディアの自己管理

・プリントアウトした書類は直ちにプリンタトレイから回収し、常時バインダ、フォルダなどに収納した状態で利用をする事
・使用目的が完了し、バインダやフォルダなどから外した書類はただちにシュレッダーで裁断して破棄すること
・会議メモ、ホワイトボードのハードコピーなどは、議事録などの作成が終了した時点でシュレッダーで裁断して破棄すること

### 6．業務情報の帯出許可申請

ノート型パソコンまたは磁気メディア（FD, HD, MOその他）、メモリディスク（CFその他）、PDA、ネットワーク装置（いずれも備品・私物を問わない）に業務上のデータ（顧客情報、見積書、仕様設計書、プログラムコード、試験報告書、顧客とのメールなど）を格納し携帯する場合には、別途定める「業務情報帯出標準」に従い「業務情報帯出許可申請書」を上長に提出し、その許認可を得ること

### 7．終業点検の励行

終業時には以下の項目をチェックし、対応作業を実施してから退出すること

1）作業の為に一時的に作成したファイルやメモがそのまま残されていないか
2）ログイン（ログオン）状態のまま遊休しているアカウントが残っていないか
3）机上に書類やメモがむき出しのままで置かれていないか
4）無用に通電しているモニタ、PC は無いか

### 8．定期点検の励行

・上記基本的行動指針の遵守励行につき、毎偶数月末に自己点検を実施すること
・遵守励行を支障する問題があった場合には「基本的行動指針障害報告書」を提出し、その問題の組織的な解消について協力すること

## 4．例外規定

この文書には例外規定を認めません。

## 5．罰則

この文書の基本的行動指針を遵守しなかった場合、別途定める罰則標準に基づく罰則の適用を受ける事があります。

# …でも「ひとごと」でしょ？

- だうと！
  - 大概の事業者が個人情報取扱事業者に当該するものと覚悟しましょう
    - 政令の定義は非常に厳しいです
  - 万一当該しなかったとしても…
    - 結局は何らかの態勢の整備が必要なのです

報告の徴収

助言・勧告・命令

主務官庁

個人情報
取扱事業者

情報主体

報告

監督・指導

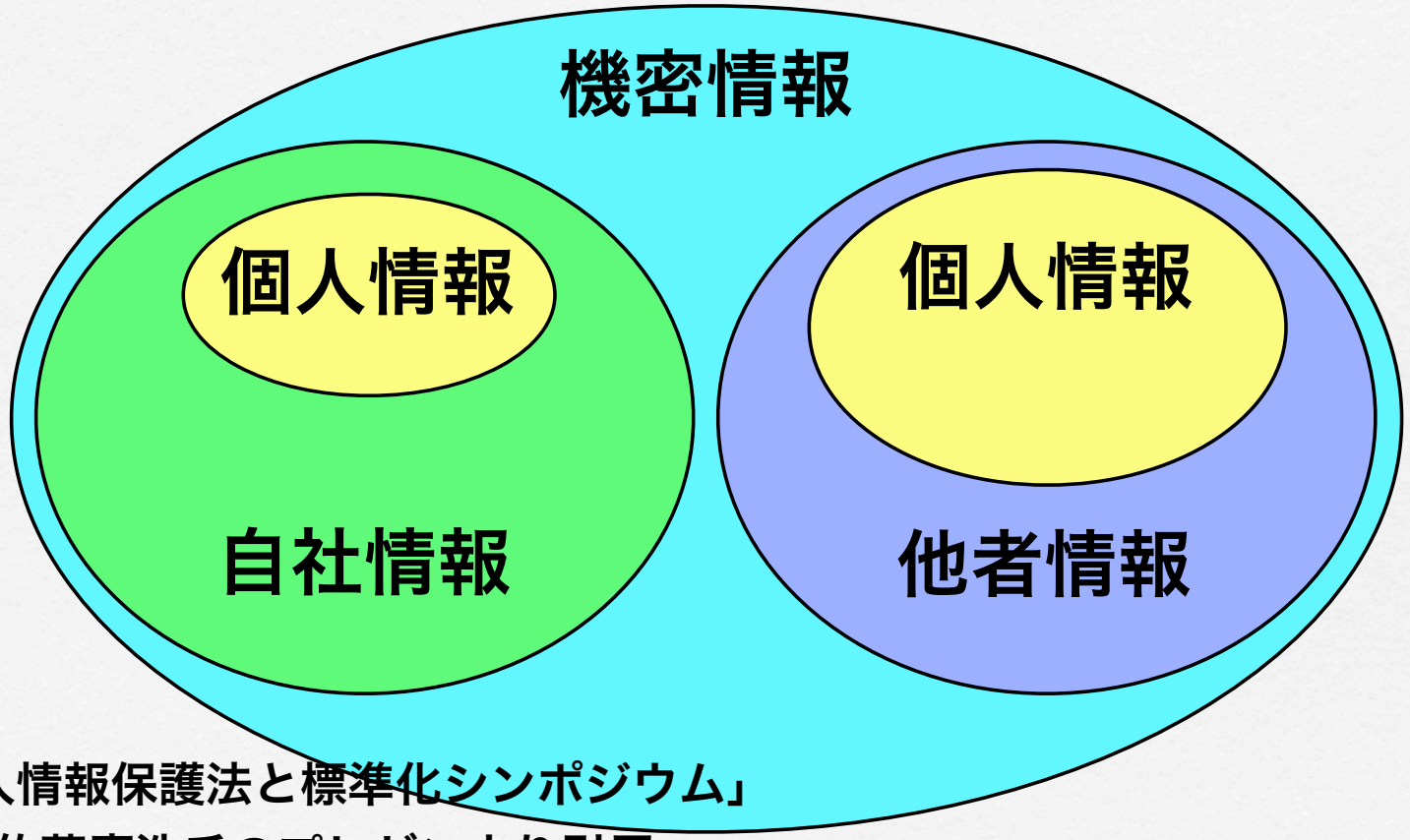
協力・委託
会社

協力会社

# さぁ、どうしましょうか？

- こういう場合には資源の整理が有効です
  - 今、どのようなものを持っていて
  - 何を管理する必要があるのか？
  - 何を使う事ができるのか？

# もう一度資源を整理！




「個人情報保護法と標準化シンポジウム」
佐藤慶浩氏のプレゼンより引用

## すなわち！

- 機密情報保護の管理態勢が確立できていれば、個人情報保護対策はそのフレームワークに個人情報保護特有の要件を追加することで実現できる

# 機密情報保護標準

基本的にライフサイクルに対応する

機密情報入手標準

機密情報保管基準　→　廃棄

機密情報利用標準

これらに基づき手順書や帳票等を整備

# 「アドオン」するものは？

- オプトイン／オプトアウトの管理です
  - オプトイン
    - 個人情報を収拾する時点において「情報主体」の同意があること
  - オプトアウト
    - 個人情報を利用したことに対して「情報主体」の異議表明がないこと

# まとめ

- 個人情報保護法対応は個別対応
  - 「コピペ」じゃだめ！
- 対応が除外される可能性は無いと考える
- 情報セキュリティ管理＋αで行ける
  - まだなんとかなる
- 定常的な改善の継続の確保が必要

# 参考文献・資料など


リスクマネジメントシステム構築のための指針 JIS Q 2001

情報セキュリティマネジメントの実践のための規範 JIS X 5080

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
JIS Q 15001

個人情報保護法セキュリティ実践マニュアル ISBN4-8443-1858-6

個人情報保護法と標準化シンポジウム配布資料

JPSA会員向け個人情報保護対策 ハンドブック

ISMS 認証基準(Ver.2.0) -JIP-ISMS100-2.0


あんど すぺしゃる さんくす つー『みかちゃん ふぉんと』!