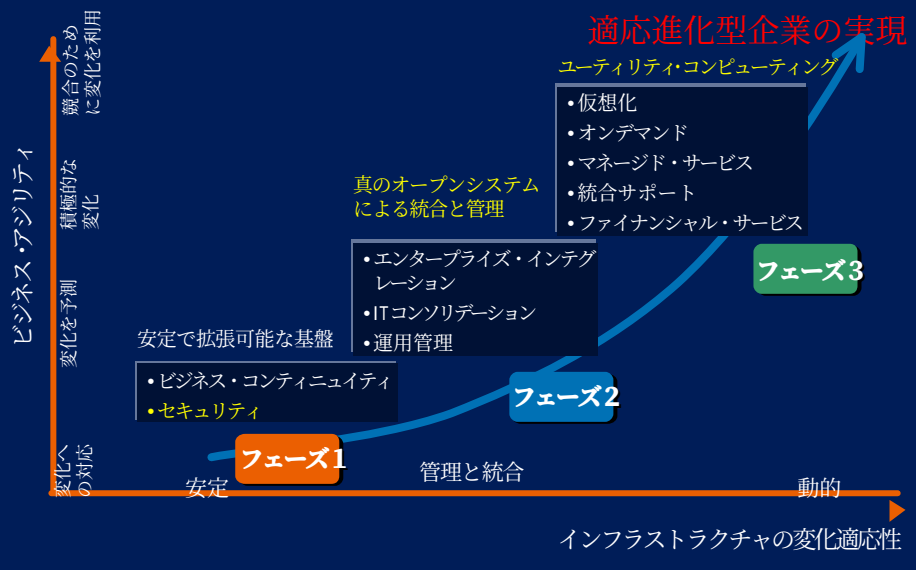
事故想定社会における企業のセキュリティ・マネジメント

個人情報保護と情報セキュリティ対策

日本ヒューレット・パッカード株式会社
個人情報保護対策室　室長
佐藤慶浩

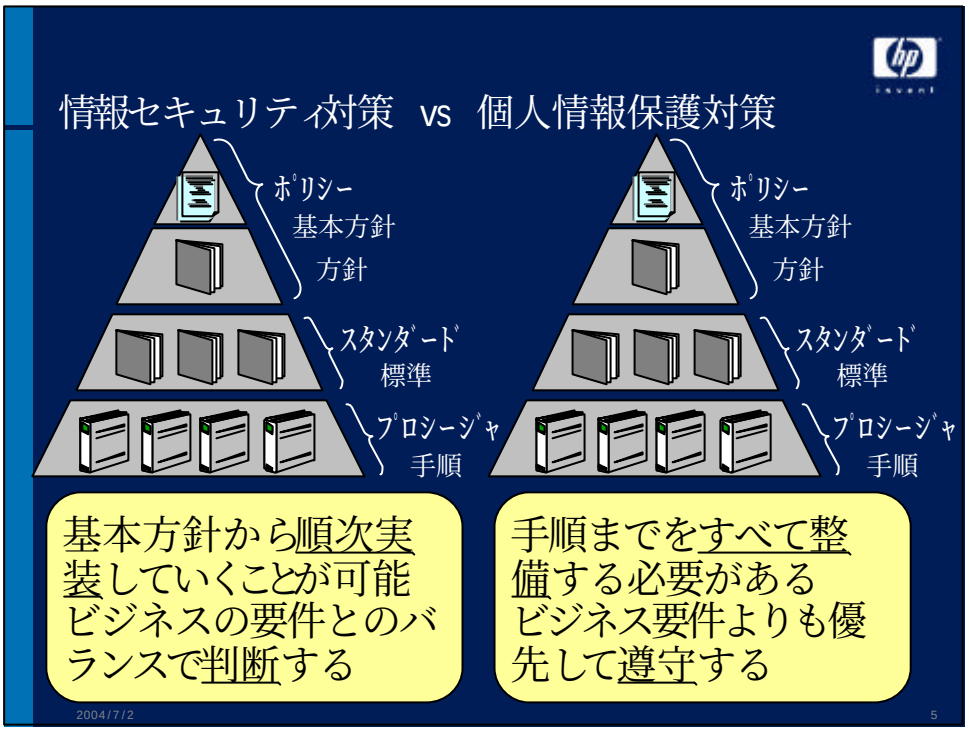
適応進化型企業（アダプティブ・エンタープライズ）

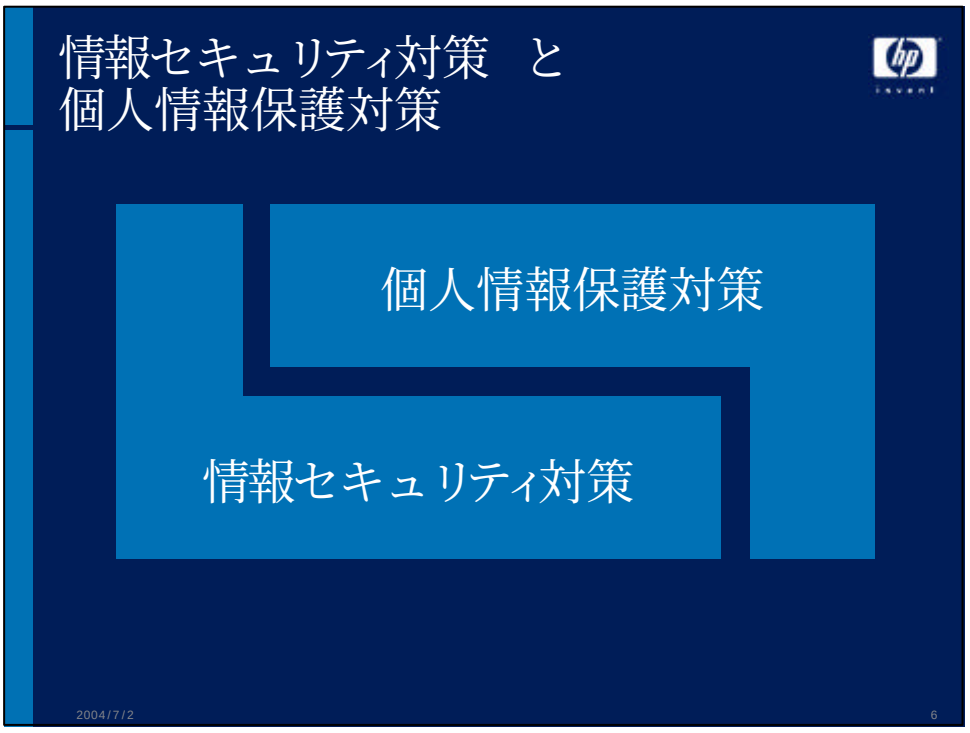


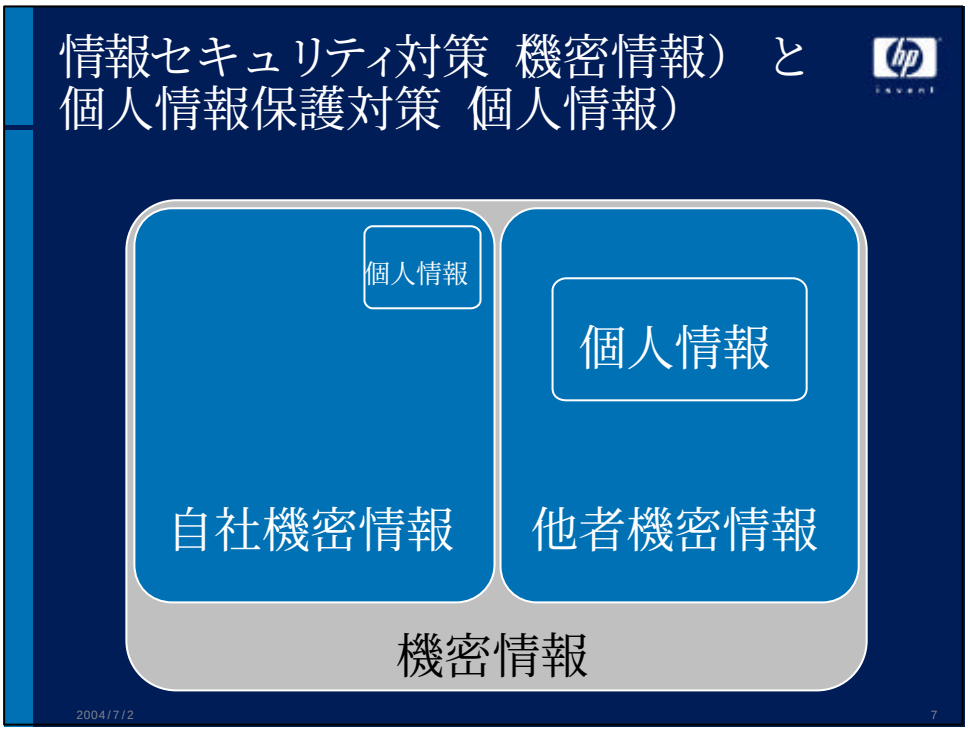
2004/7/2　2

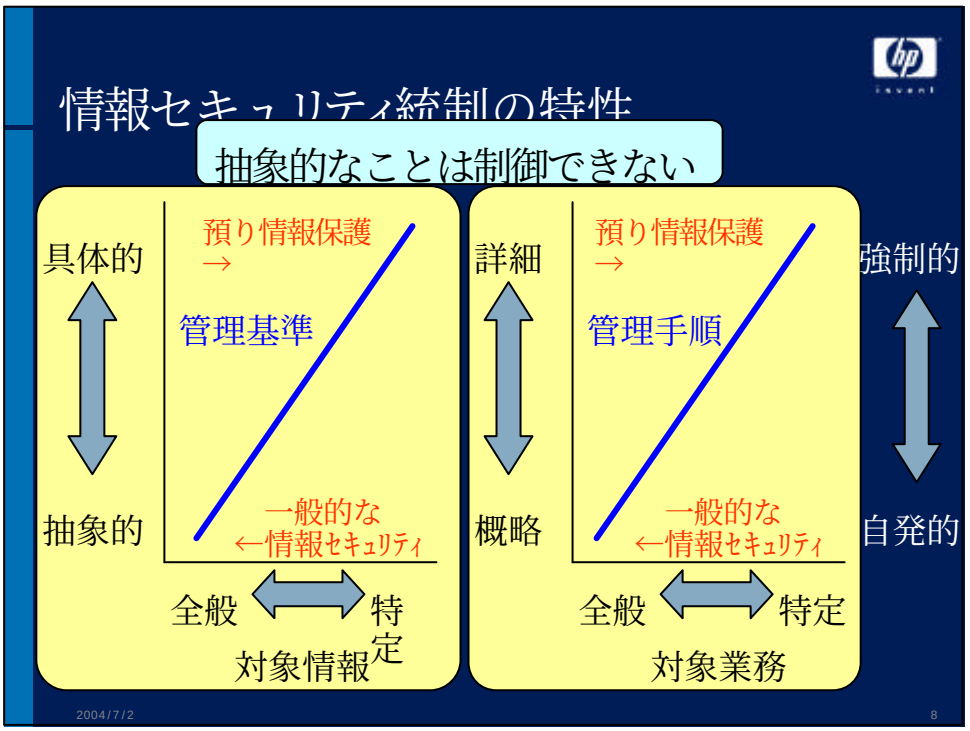

個人情報保護と情報セキュリティ対策
個人情報保護対策確立までのロードマップ
- 外部支援サービスの活用
- 啓発 •教育 •訓練
個人情報保護法と委託関係
まとめ
hp


個人情報保護と
情報セキュリティ対策


情報セキュリティ対策 vs 個人情報保護対策
ポリシー
基本方針
方針
スタンダード
標準
プロシージャ
手順
基本方針から順次実装していくことが可能
ビジネスの要件とのバランスで判断する
ポリシー
基本方針
方針
スタンダード
標準
プロシージャ
手順
手順までをすべて整備する必要がある
ビジネス要件よりも優先して遵守する
2004/7/2
5


情報セキュリティ対策 と
個人情報保護対策
個人情報保護対策
情報セキュリティ対策
2004/7/2
6


情報セキュリティ対策（機密情報）と
個人情報保護対策（個人情報）
個人情報
個人情報
自社機密情報
他者機密情報
機密情報
2004/7/2
7


情報セキュリティ統制の特性
抽象的なことは制御できない
具体的
預り情報保護
→
管理基準
抽象的
一般的な
←情報セキュリティ
全般
特定
対象情報
詳細
預り情報保護
→
管理手順
概略
一般的な
←情報セキュリティ
全般
特定
対象業務
強制的
自発的
2004/7/2
8

個人情報のライフサイクル

個人情報の取得
- 利用目的・情報移転の了解を事前に得る
- 必要最低限の取得→使用予定のないものは取得しない

個人情報の保管
- 情報漏えい・書き換えの防御
- 情報格付け、ｼｽﾃﾑ格付け：所在の管理、視認性の確保

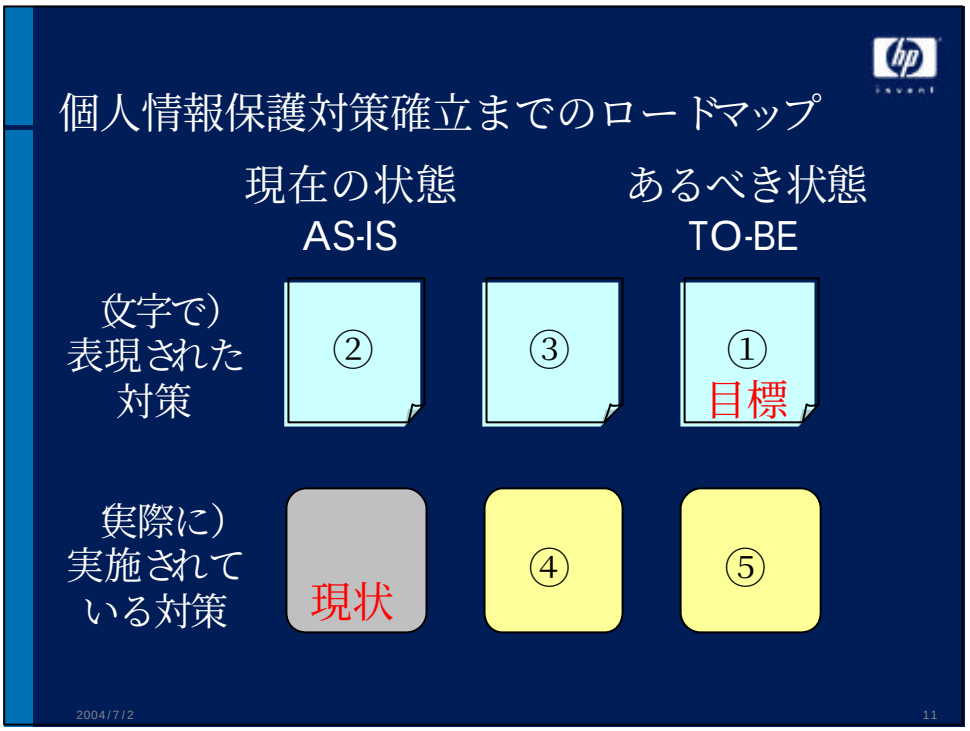
個人情報の加工
- 情報格付けの継承、ｼｽﾃﾑ要件の継承

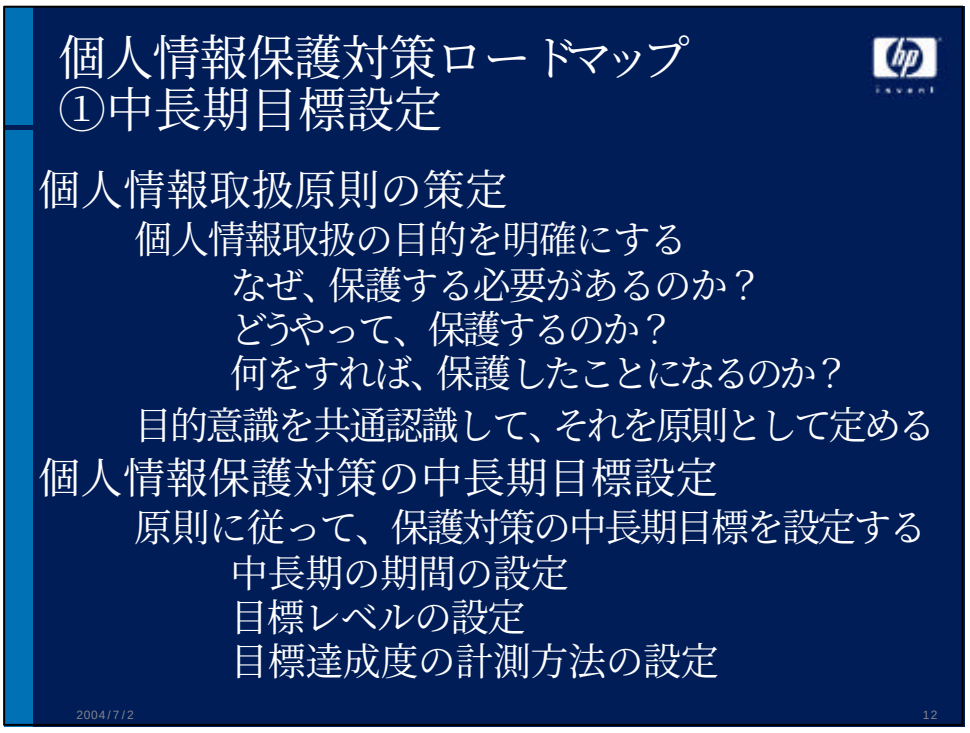
個人情報の利用
- 利用者の制限（無許可者からのアクセス防御）
- 最小情報、最小数量の利用制限（許可者の最小権限）
- 取扱い手順の明確化（許可者の注意義務）

個人情報の廃棄
- 廃棄手順の明確化（電子化前後の廃棄手順を含む）

2004/7/2 9

個人情報保護対策確立までのロードマップ


個人情報保護対策確立までのロードマップ
現在の状態
AS-IS
あるべき状態
TO-BE
(文字で)
表現された
対策
②
③
①
目標
(実際に)
実施されて
いる対策
現状
④
⑤
2004/7/2
11


個人情報保護対策ロードマップ
①中長期目標設定
個人情報取扱原則の策定
個人情報取扱の目的を明確にする
なぜ、保護する必要があるのか？
どうやって、保護するのか？
何をすれば、保護したことになるのか？
目的意識を共通認識して、それを原則として定める
個人情報保護対策の中長期目標設定
原則に従って、保護対策の中長期目標を設定する
中長期の期間の設定
目標レベルの設定
目標達成度の計測方法の設定
2004/7/2
12

個人情報保護対策ロードマップ ②現状把握

個人情報取扱状況の把握
- 現状の実態を把握する
  - 意識の把握
  - 関係者の把握
  - 情報の把握
  - システムの把握
  - 運用の把握
  - 契約の把握

2004/7/2 13

個人情報保護対策ロードマップ ③短期目標設定

個人情報保護対策の短期目標設定
- 現状と中長期目標の間で短期目標を設定する
  - 中長期内での優先度の選定
  - 範囲の設定
    - 短期の期間の設定
    - 対象とする業務、組織、情報の設定
  - 制約条件の設定
    - 現場が受け入れ可能な条件
  - 前提条件の設定
    - 組織的支援が可能な条件
  - 目標レベルの設定
  - 目標達成度の計測方法の設定

2004/7/2 14

個人情報保護対策ロードマップ ④短期目標達成

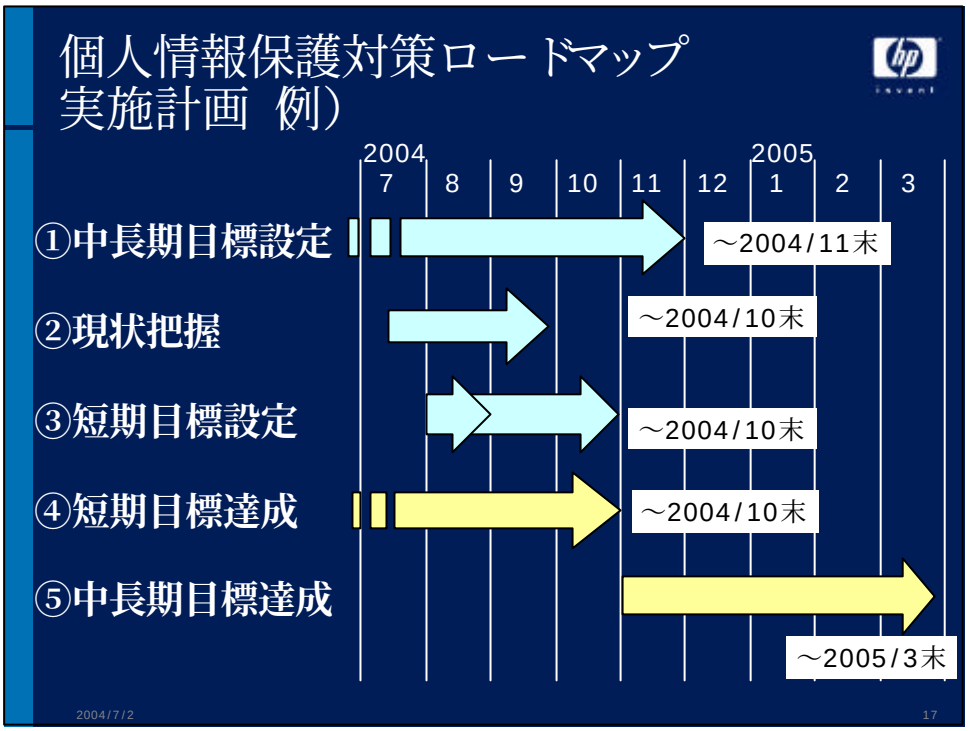
- 個人情報保護対策の短期目標達成
  - 短期内での優先度の順位付け
  - 短期目標の達成
    - 人的対策の実施
      - 啓発、教育、訓練
    - プロセス的対策の実施
      - 方針、手引書、手順書の整備
    - 技術的対策の実施
      - システム等の変更、導入
    - 目標達成度の計測
      - 人/プロセス/技術の計測準備と実施

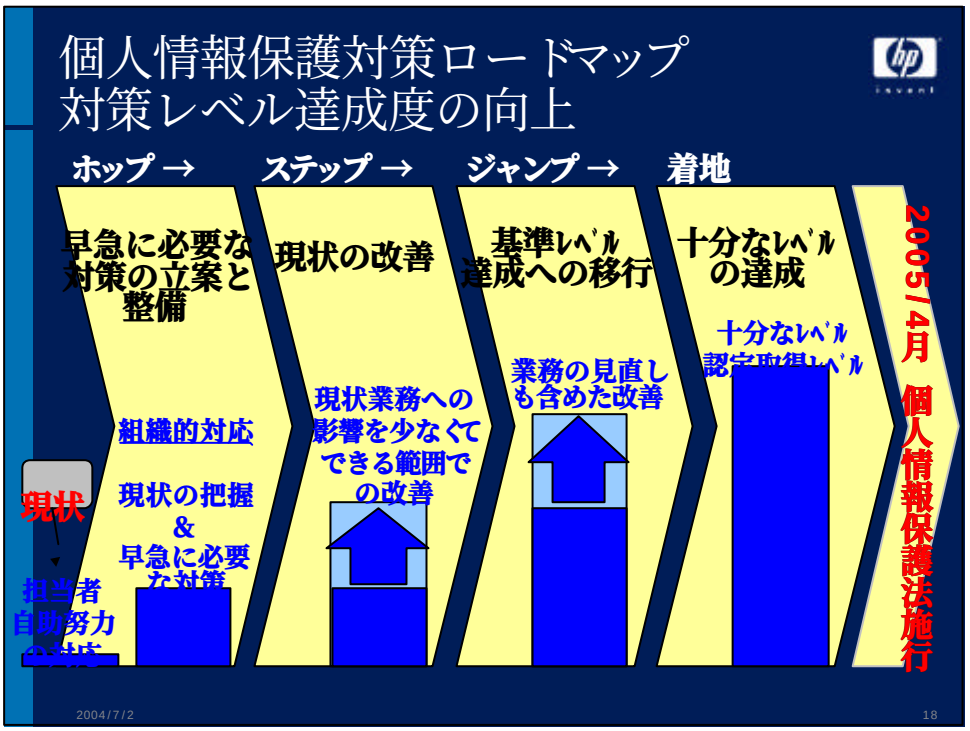
2004/7/2 15

個人情報保護対策ロードマップ ⑤中長期目標達成

- 個人情報保護対策の中長期目標達成
  - 中長期目標の達成
    - 範囲の拡大
      - 全業務、全組織、全情報を対象とする
    - 制約条件の解消
      - 現場が受け入れるのに必要な支援
    - 前提条件の拡大
      - 個人情報保護に必要な全面的支援
    - 目標達成の公的認証取得の検討
  - 達成レベルの継続性の確保
  - 中長期目標の見直しと向上

2004/7/2 16


個人情報保護対策ロードマップ
実施計画（例）
2004
2005
7
8
9
10
11
12
1
2
3
①中長期目標設定
～2004/11末
②現状把握
～2004/10末
③短期目標設定
～2004/10末
④短期目標達成
～2004/10末
⑤中長期目標達成
～2005/3末
2004/7/2
17


個人情報保護対策ロードマップ
対策レベル達成度の向上
ホップ →
ステップ →
ジャンプ →
着地
早急に必要な対策の立案と整備
現状の改善
基準レベル達成への移行
十分なレベルの達成
2005/4月 個人情報保護法施行
組織的対応
現状の把握
&
早急に必要な対策
現状
担当者自助努力
現状業務への影響を少なくてできる範囲での改善
業務の見直しも含めた改善
十分なレベル
認定取得レベル
2004/7/2
18

外部支援サービスの活用

支援サービスの利用範囲

	助言	資料作成	文書清書
①中長期目標設定	■	□	□
②現状把握	■	■	□
③短期目標設定	■	■	□

	計画	設計	実施支援
④短期目標達成	□	□□□	□□□
⑤中長期目標達成	□	□□□	□□□

個人情報保護対策　≠　情報漏えい対策

2004/7/2　20

事故対応

事故対応　≠　事後対応

事故の発生を完全に防止することはできない。
　不正アクセス＝無許可アクセス＋権限アクセスの濫用

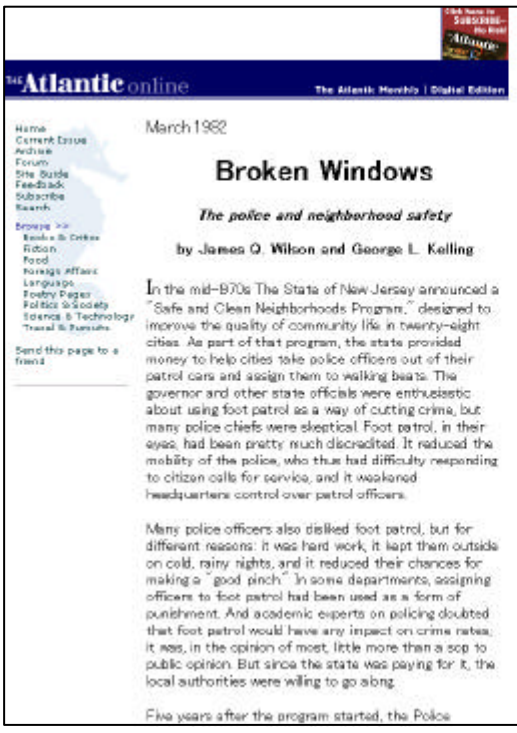
事故の発生を想定した、体制の確立が必要。

社内の危機管理体制などと整合を図るのがよい。

遅延なき対処（ノン・ストップ・プロセス）の確立＝
事前計画の策定と、例外対応の整備。
　事前計画 :計画に沿った処理、役割分担、全員連携
　例外対応 :計画に沿わない処理、役割排除、個別判断

2004/7/2　22

啓発 ・教育 ・訓練



The Atlantic online — The Atlantic Monthly | Digital Edition

March 1982

Broken Windows

The police and neighborhood safety

by James Q. Wilson and George L. Kelling

In the mid-1970s The State of New Jersey announced a "Safe and Clean Neighborhoods Program," designed to improve the quality of community life in twenty-eight cities. As part of that program, the state provided money to help cities take police officers out of their patrol cars and assign them to walking beats. The governor and other state officials were enthusiastic about using foot patrol as a way of cutting crime, but many police chiefs were skeptical. Foot patrol, in their eyes, had been pretty much discredited. It reduced the mobility of the police, who thus had difficulty responding to citizen calls for service, and it weakened headquarters control over patrol officers.

Many police officers also disliked foot patrol, but for different reasons: it was hard work, it kept them outside on cold, rainy nights, and it reduced their chances for making a "good pinch." In some departments, assigning officers to foot patrol had been used as a form of punishment. And academic experts on policing doubted that foot patrol would have any impact on crime rates; it was, in the opinion of most, little more than a sop to public opinion. But since the state was paying for it, the local authorities were willing to go along.

Five years after the program started, the Police

凶悪犯罪を防止
することはできるか？

情報セキュリティの
重大違反を防止
することはできるか？

人が業務を遂行して
おり、人が違反する
→完全に防止する
ことはできない。

ブロークン・ウインドウズ理論

第１段階
　落書きが放置されていると罪悪感が薄れやすくなる
第２段階
　軽犯罪が多発し治安が悪くなる
第３段階
　警察の監視がないと判断され、より凶悪な犯罪者が寄り付く
第４段階
　犯罪がエスカレートし凶悪犯罪が発生する

対策
(1)落書きを徹底的に消す
→警察や住民の監視があるというメッセージ
→軽い気持ちで罪を犯す人が減少する
(2)軽犯罪の取締りを強化する
→小さな犯罪も許さないという姿勢をアピール
→犯罪を起こそうと思う人間は近づかない
→凶悪犯罪は発生しなくなる

2004/7/2 25

訓練

「HPウイルス予防訓練サービス」を損保ジャパン様が導入第 1段階

2004/7/2 27

個人情報保護法と委託関係

個人情報保護法ガイドライン（経済産業省の例）

第20条　（安全管理措置）
- 組織的安全管理措置
  - 情報のライフサイクル（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）
- 人的安全管理措置
  - 教育
- 物理的安全管理措置
- 技術的安全管理措置
  - 5A（Authentication, Access Control, Administration, Auditing, Assurance）

2004/7/2　29

個人情報保護法ガイドライン（経済産業省の例）

第22条　（委託先の監督）

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない。
「必要かつ適切な監督」には、委託契約において委託者である個人情報取扱事業者が定める安全管理措置の内容を契約に盛り込むとともに、当該契約の内容が遵守されていることを、予め定めた間隔で定期的に確認することも含まれる。

個人情報保護法ガイドライン（経済産業省の例）

第23条　（第三者への提供）

事業者は、雇用管理に関する個人データの第三者への提供に当たって、次に掲げる事項に留意するものとすること。
（1）提供先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこととされていること。
（2）当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。但し、当該再提供が、法第二十三条第一項第一号から第四号までに該当する場合を除く。
（3）提供先における保管期間等を明確化すること。
（4）利用目的達成後の個人データの返却又は提供先における破棄若しくは削除が適切かつ確実になされること。
（5）提供先における個人データの複写及び複製（安全管理上必要なバックアップを目的とするものを除く。）を禁止すること。

委託関係において あってはならないこと

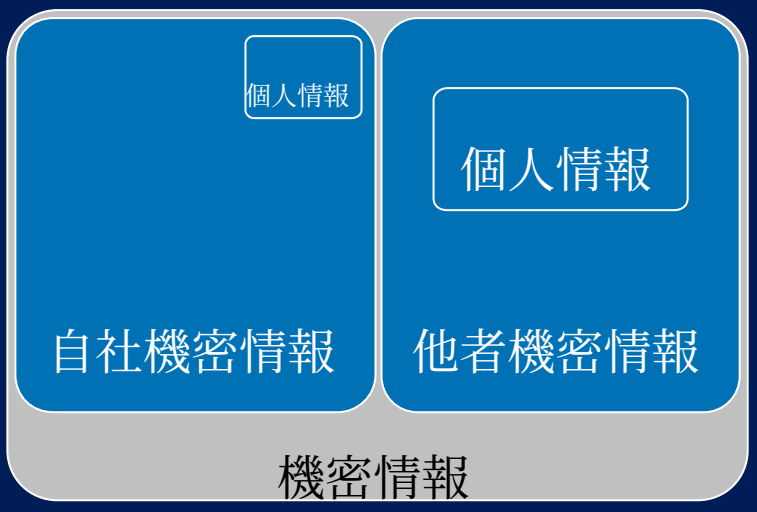
委託関係において、発注者が安全管理措置を具体的に示さず、結果責任としての賠償責任だけをリスク転嫁することは、健全な社会を形成するとは思われない。

リスクの転嫁の連鎖だけが発生する
- 具体策がないまま見積もりをする
- 適正にするところは費用が高くなる
- 適当に対応するところは費用が安くなる
- 発注者としての具体策がないため、費用以外での評価ができない

リスクが潜在化するだけ
- 粗悪業者が蔓延し、事故が発生するその日まで、リスクが温存されるという社会になる危険性がある。

2004/7/2 32

情報セキュリティ対策（機密情報）と 個人情報保護対策（個人情報）



2004/7/2 33

委託関係において配慮すべきこと

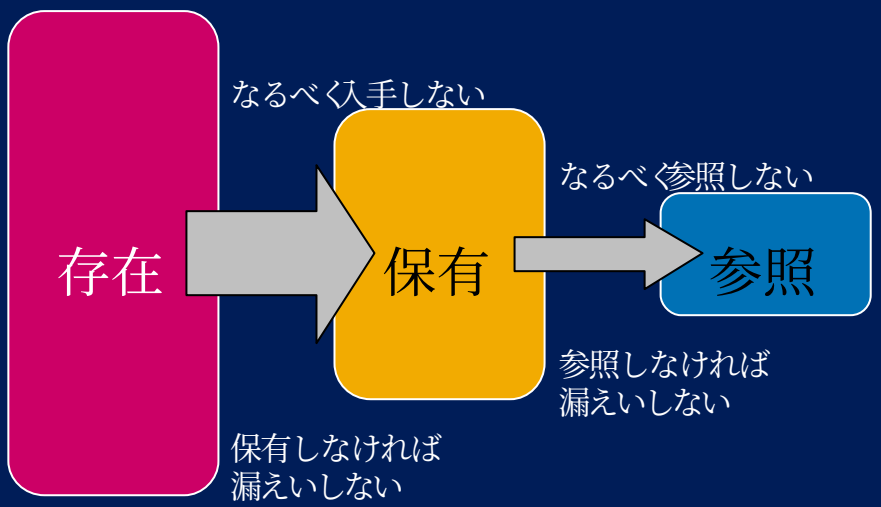
委託発注者は、一次的な個人情報取扱事業者である。

発注者は、自身の安全管理措置を具体的に定めて徹底する。
発注者は、安全管理措置を発注時に具体的に示す。
受注者は、指示された措置に必要な対策を具体的に設計し、必要な費用を見積もる。
双方が、個人情報の保護に必要な運用体制（情報受け渡しプロトコル）を確立する。

なぜなら、顧客は、一次的な個人情報取扱事業者を信頼して個人情報を預けているのであって、

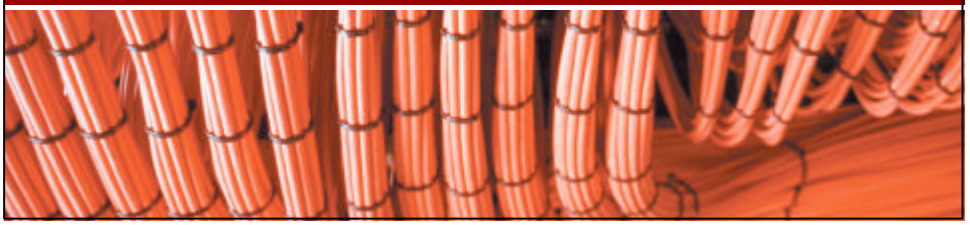
2004/7/2 34

情報漏えい防止の基本原理



2004/7/2 35

まとめ



個人情報保護の企業における位置付け

企業の目的：　個人情報の活用
企業への要件：個人情報の保護

個人情報の保護だけを目的とするのではなく、
個人情報を適切に取扱う（保護し活用する）ことを目的として、保護をその１つの要件として位置付け、それに必要な対策を検討します。
お客様が自らの個人情報を自社に預けていただいていることの期待に応えるために、必要な施策をすべきです。

2004/7/2　37


invent
本日の講演資料
http://yosihiro.com/speech/