日本HPにおける個人情報管理対策

2006年9月25日

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
チーフ・プライバシー・マネージャ
佐藤　慶浩

2006/9/25版

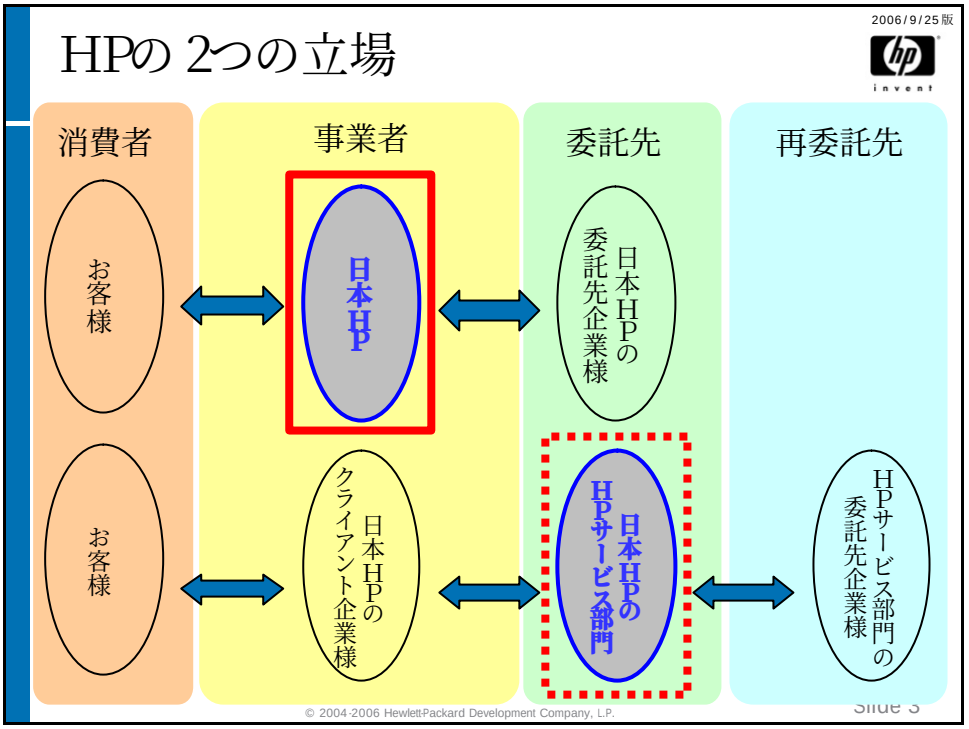
講師略歴 (http://yoshihiro.com/profile/)

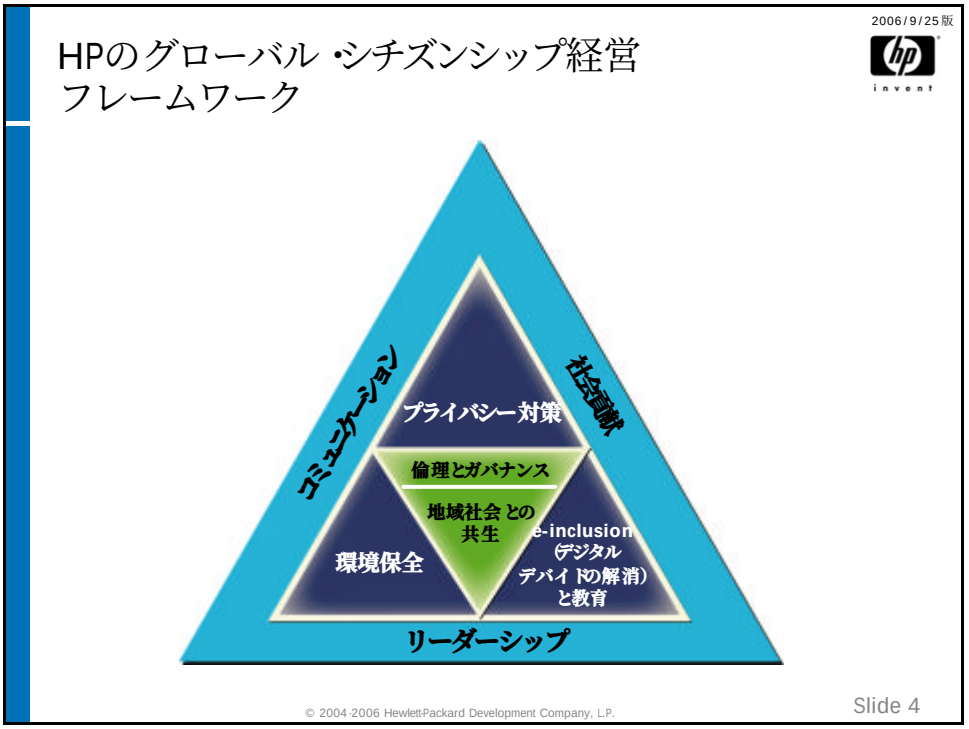
佐藤　慶浩　（さとう よしひろ）
日本ヒューレット・パッカード株式会社　個人情報保護対策室　チーフ・プライバシー・マネージャ
併任
- 情報処理推進機構（www.ipa.go.jp/）セキュリティセンター　非常勤研究員(2000/12～)
- 内閣官房 情報セキュリティセンター（www.bits.go.jp/） 内閣参事官補佐(2004/7/15～)

略歴
1990 年、日本ヒューレット・パッカード(株)入社。
2004 年6月、個人情報保護対策室長に着任。
2004 年11月、ヒューレット・パッカードのプライバシー・オフィスに所属し、日本のチーフ・プライバシー・マネージャとして全社施策の推進にあたる。

委員等
- 情報処理学会（www.ipsj.or.jp/） 正会員(1998～)
- NPO 日本ネットワークセキュリティ協会（www.jnsa.org/） 理事(2000/4～2004/5)
- 金融情報サービスセンター（www.fisc.or.jp/）セキュリティポリシー研究会 委員(2001～)
- ISO/IEC JTC1 国際標準セキュリティ委員会 委員(2001～)
- 杉並区住民基本台帳ネットワークシステム調査会議（www.city.suginami.tokyo.jp/）技術専門委員(2002/7～)
- 情報ネットワーク法学会（www.in-law.jp/）理事(2002/5～)
- 経済産業省　セキュリティホールに関する法律の諸外国調査委員会　委員(2003)
- 総務省　セキュアOSに関する調査研究会　構成員(2003/4～2004/3)
- 情報処理推進機構（www.ipa.go.jp/）情報システム等の脆弱性情報の取り扱いに関する研究会　委員(2003～)
- セキュアOSと基盤ソフトウエアに関する研究会（secure-os.yosihiro.com/） メンバー(2003～)
- 内閣官房 情報セキュリティ対策推進室 セキュアOS検討委員会 委員(2003～)
- NPO オープンソースデベロップメントラボ（www.osdl.jp/） Enterprise Linux for Public Sector ワークショップ メンバー(2004/2～)
- NPO デジタル・フォレンジック研究会(www.digitalforensic.jp/) 理事(2004/8～)
- 経済産業省 e-文書法 検討委員会委員(2004/11～)
- 経済産業省 個人情報保護ガイドラインQ&A集検討会 委員(2005/4～)
- 日本情報処理開発協会 ISMS技術専門部会 委員(2006/5～)

Slide 2


2006/9/25版
HPの 2つの立場
消費者
事業者
委託先
再委託先
お客様
日本HP
日本HPの委託先企業様
お客様
日本HPのクライアント企業様
日本HPのHPサービス部門
HPサービス部門の委託先企業様
© 2004-2006 Hewlett-Packard Development Company, L.P.
Slide 3


2006/9/25版
HPのグローバル・シチズンシップ経営
フレームワーク
コミュニケーション
社会貢献
プライバシー対策
倫理とガバナンス
地域社会との共生
環境保全
e-inclusion（デジタルデバイドの解消）と教育
リーダーシップ
© 2004-2006 Hewlett-Packard Development Company, L.P.
Slide 4

2006/9/25版

HP における取り組み
プライバシー原則 principles

hp社のプライバシー原則

1997 年～

- お客様自身のデータについては、お客様が制御（コントロール）できるものとします
- 信用を向上し、その結果としてビジネスを伸ばすような選択肢をお客様に提供します
- お客様とhp の関係についての決定権はお客様にあるものとします
- 最高のインテグリティ（誠実さ）のある行動を、業務と供給者、協業者において実施してもらいます
- CRM ではなく、CMR(Customer Managed Relationship) を行ないます

Slide 5

2006/9/25版

HP における取り組み
プライバシー基本原理 fundamentals

hp社のワールドワイド・プライバシーポリシーの基本原理

告知 (notice)

選択 (choice)

アクセス (access)

正確性 (accuracy)

管轄外への転送 (onward transfer)

セキュリティ(security)

施行/監視 (enforcement/oversight)

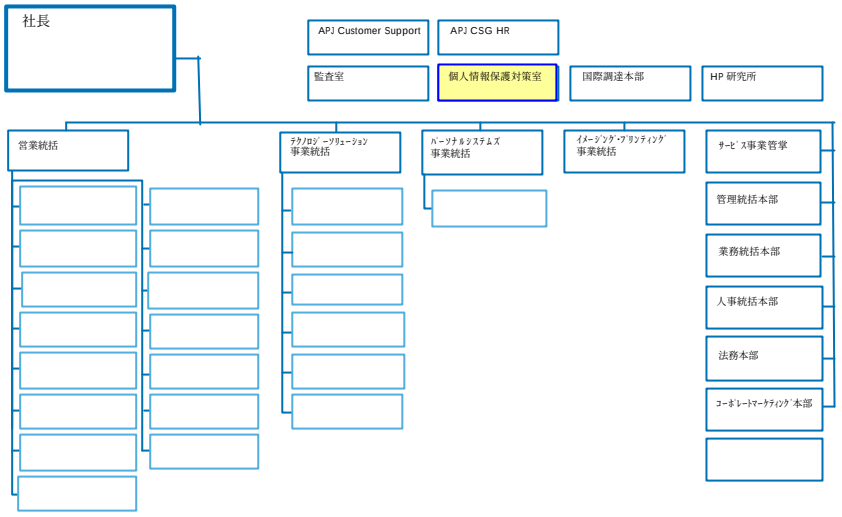
hp では
同一の基本原理を
グローバルに適用

onward transfer は、safe harbor 協定で定義。
米国では企業合併の際の連邦確認項目でもある。

Slide 6

2006/9/25版

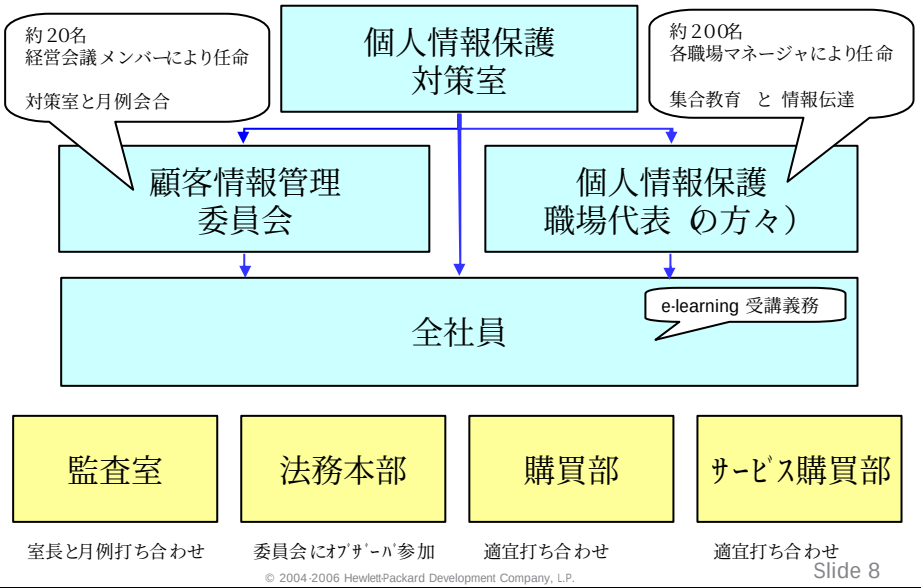
日本ヒューレット・パッカード株式会社 組織図



Slide 7

2006/9/25版

個人情報保護対策　日本HP体制



Slide 8

2006/9/25版

個人情報保護の企業における位置付け

企業の目的：　個人情報の受諾目的内での活用
企業への要件：個人情報の保護
＝個人情報の目的外使用の防止

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。

→　個人情報適正取扱施策

Slide 9

2006/9/25版

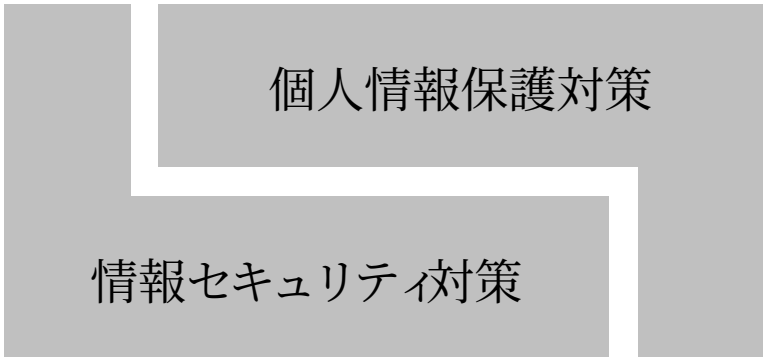
個人情報○×対策」という言葉

- コンプライアンス（順法）としての
  個人情報保護法対応
- 情報セキュリティ・リスク管理としての
  個人情報漏洩防止
- ビジネスに役立てるための
  個人情報活用施策

Slide 30

2006/9/25版

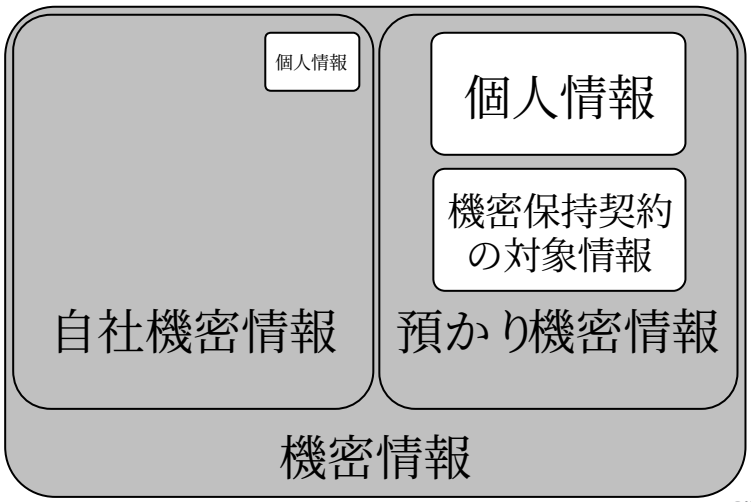
情報セキュリティ対策　と
個人情報保護対策



Slide 31

2006/9/25版

個人情報と機密情報の関係



Slide 32

2006/9/25版

経済産業省
個人情報保護法ガイドライン 第20条

http://yosihiro.com/infosec/index.html#security_architecture

- **つぎはぎシステムを防ぐセキュリティアーキテクチャ**
- **5A (Authentication, Access Control, Administration, Auditing, Assurance)**

2006/9/25版

内閣官房情報セキュリティセンター
政府機関情報セキュリティ統一基準

http://www.nisc.go.jp/active/general/kijun01.html

- **政府機関の情報セキュリティ対策のための統一基準**（2005年12月版［全体版初版］）解説書

2006/9/25版

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。

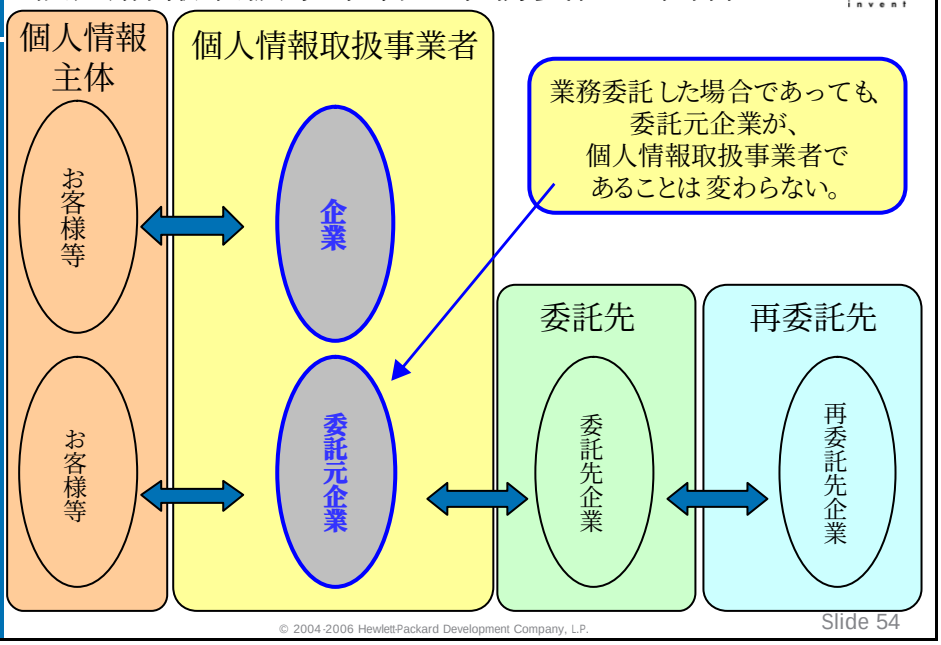
発注者は、自身の安全管理措置を具体的に定めて徹底する。
発注者は、安全管理措置を発注時に具体的に示す。
受注者は、指示された措置に必要な対策を具体的に設計し、必要な費用を見積もる。
双方が、個人情報の保護に必要な運用体制（情報受け渡しプロトコル）を確立する。

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、委託先に責任転嫁されることを期待していない。

Slide 53

2006/9/25版

個人情報取扱事業者と業務委託の関係



Slide 54

2006/9/25版

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

結果責任だけを押し付けると、自社の周囲に粗悪業者が蔓延し、事故が発生するその日まで、リスクが温存される危険性が高まる。

2006/9/25版

委託先への誤った管理

- 委託先に意味もなくプライバシーマーク認証取得を指示する

→愚の骨頂

- 委託先にISMS認証取得を指示する

→誤解されやすい

個人情報取扱事業者として、社外への丸投げ体質は許されない。

リスク転嫁策のように思われるが、事故発生後のことを考えれば、それが正しくないことは、すぐにわかること。

さらに、現場での責任意識・危機管理意識の希薄化を招くため、むしろ、百害あって一利なし。

2006/9/25版

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、法第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行わなければならない。

・「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。なお、優先的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

・委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意する。

2006/9/25版

まとめ

個人情報に関する企業における対策は、
・お客様
・関連企業の従事者
・従業員に関する者
に関するものの3つに大別できる。
そのうち、お客様に関する個人情報に関する対策は、お客様に対して、
・「個人情報を適切に保護しているという安心感の向上」
・「個人情報を利用した各種販売促進活動における満足度の向上」
を管理することだと言える。
→社内個人情報保護ガイドラインの公開 (http://www.hp.com/jp/pip)

参考：
「法律から始めない個人情報保護対策」
科学技術振興機構発行　情報管理　2006年8月号 (VOL.49 NO.5)
http://johokanri.jp/vol49-05/index.html

参考資料