個人情報保護対策

2009年11月13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
佐藤　慶浩

自己紹介 (http://yosihiro.com/profile/)

2009/11/13 版

佐藤　慶浩
日本ヒューレット・パッカード　個人情報保護対策室　室長
（併任）内閣官房 情報セキュリティ指導専門官

個人情報保護に関する社外活動
- JIPDEC　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ運営要領改正委員会　委員
- (社)ｺﾝﾋﾟｭｰﾀｿﾌﾄｳｪｱ協会　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ審査判定委員会　委員
- JIPDEC　ISMS適合性評価制度技術専門部会　委員
- 杉並区　住基ネット運用監視委員会　委員
- 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

2009/11/13 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

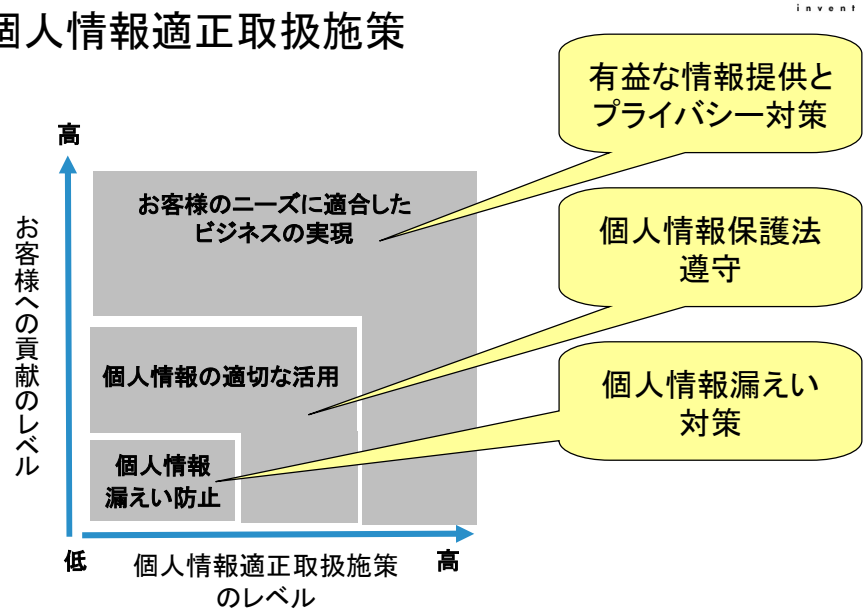
個人情報保護対策とは、個人情報を適切に取扱う（保護し活用する）ことを目的として、その目的達成における要件の1つとして保護を考えるものとして位置づけられます。
お客様が自らの個人情報を自社に預けていただいていることの期待に応えるために、必要な施策をすべきです。

→個人情報適正取扱施策　の方が直感的な言葉です。

Slide 3

2009/11/13 版

個人情報適正取扱施策



Slide 4

2009/11/13 版

「個人情報〇×対策」という言葉

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

Slide 5

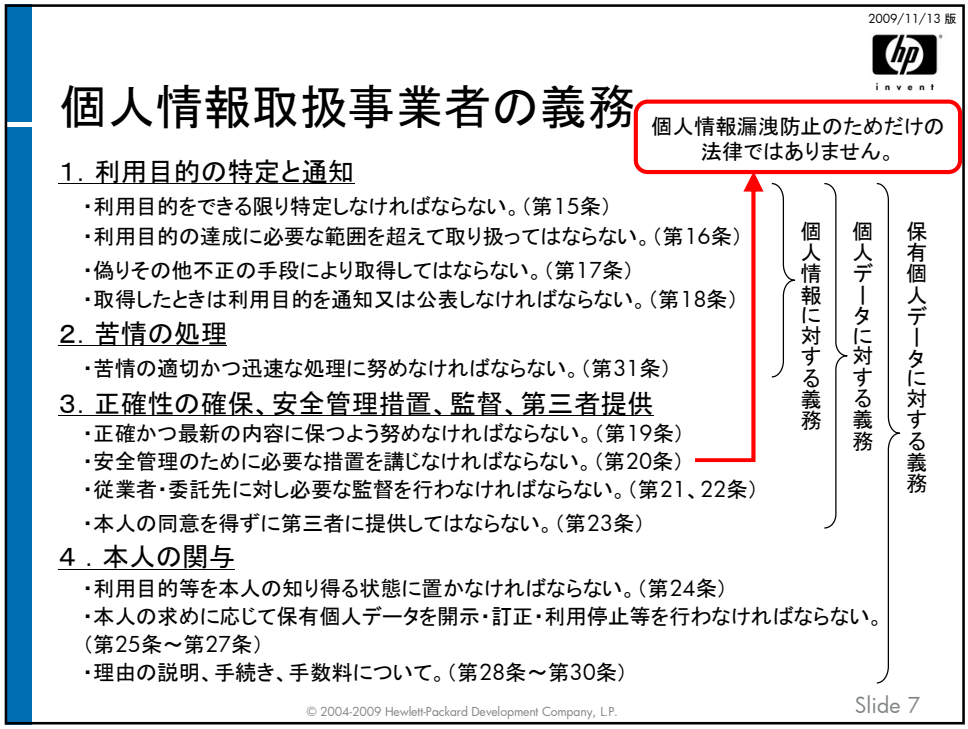
2009/11/13 版

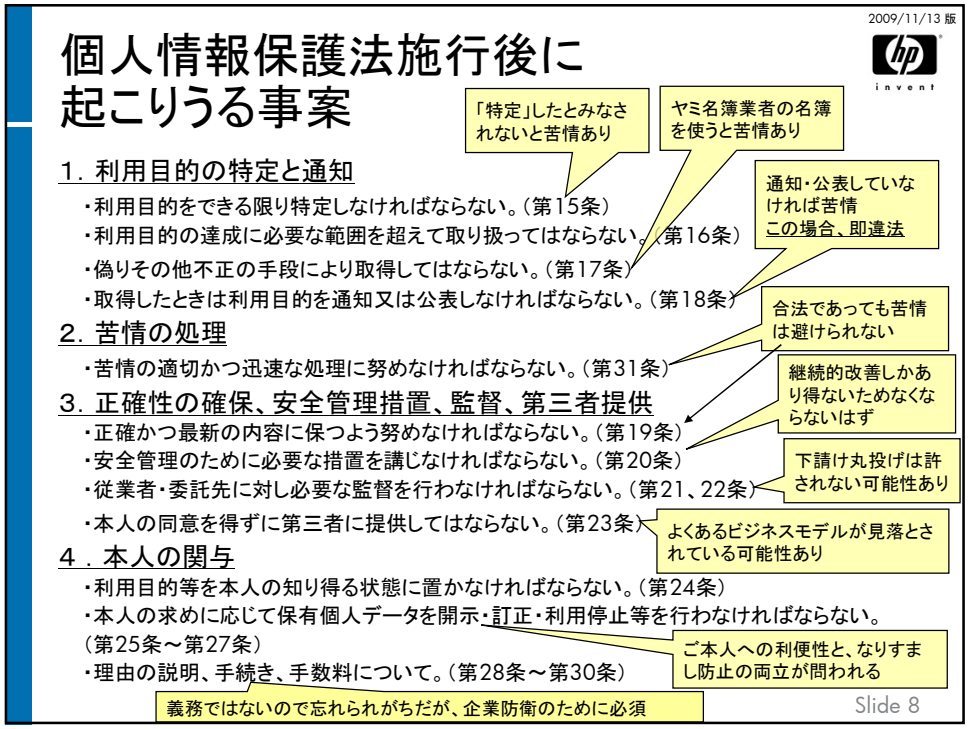
「個人情報〇×対策」という言葉

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

© 2004-2009 Hewlett-Packard Development Company, L.P.

Slide 6





2009/11/13 版

個人情報保護法のガイドライン

内閣府　国民生活局
個人情報の保護に関するガイドラインについて

http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

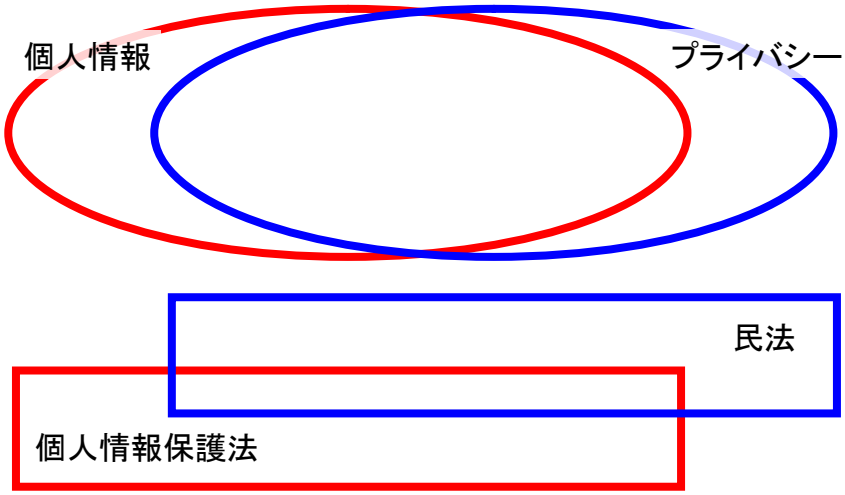
法律の内容を知っておくための参考書籍

これだけは知っておきたい　個人情報保護（525円）
　岡村久道・鈴木正朝著　日本経済新聞社

Slide 9

2009/11/13 版

個人情報保護法へのコンプライアンス？ →特定の法律だけを検討しても不十分



出典:「個人情報保護法とコンプライアンス・プログラム」鈴木正朝 著
商事法務 出版 ISBN4-7857-1191-4

Slide 10

2009/11/13 版

個人情報の定義のおける留意点

一般的に使われる「個人情報」という用語で考えればよいが、以下の点に注意するとよい。

- 電子、非電子のいずれも対象
- 従業員も対象
- 法人等の連絡先情報も対象
- 公知の情報も対象

Slide 11

2009/11/13 版

プライバシー侵害

プライバシーの侵害による不法行為の成立要件

- 公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること
- 一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること
- 一般の人々に未だ知られない事柄であること
- その他、被害者が公開により不快、不安の念を覚えること

『宴のあと』事件判決（東京地判昭和39年9月28日）より
出典：新保史生先生 http://hogen.org/research/paper/jp/

Slide 12

2009/11/13 版

個人情報保護に関係する法令等

省庁	日付	内容
総務省	－	迷惑メールに係る対応方策の検討について（論点整理）
	－	独立行政法人などの保有する個人情報の保護に関する法律に係る 行政手続における情報通信の技術のりように関する法律施行規則
	－	行政機関等個人情報保護法（個人情報保護関連5法の概要）
	－	放送受信者等の個人情報の保護に関する指針
	－	電子タグに関するプライバシー保護ガイドライン
	－	損害保険会社に係る個人情報保護指針（個人情報指針）について
	H16.9.14	「行政機関の保有する個人情報の適切な管理のための措置に関する指針」及び 「独立行政法人等の保有うする個人情報の適切な管理のための措置に関する指針」
	H16.8.13	「放送分野における個人情報保護の基本的な在り方について」の公表
		特定電子メールの送信の適正化等に関する法律（ 迷惑メール防止法 ） 改正
経済産業省	H14.6.21	特定商取引に関する法律施行規則の改正について（電子メールによる一方的な商業広告の送りつけへの対応）
	H19.～	電子商取引等に関する準則改訂案
財務省	H16.10.25	財務省の所管する事業者等.個人情報の保護に関する法律 （個人情報の取得等、管理etca0

http://www.soumu.go.jp/menu_hourei/d_shinjigyou.html

Slide 13

2009/11/13 版

日本における 法令等のコンプライアンス （私見）

合法＝法の条文とおり従う

→目標（理想的）

法の条文とおりではなくても違法ではない場合もある

→欧米にあまりない概念

違法とならない程度＝社会通念上遜色のない最善策を実施していれば違法とはならない場合もある

脱法＝法律に触れないような方法で、実際は、法が禁止していることを犯すこと （広辞苑より）

→発覚すれば企業として致命的 →絶対にしてはならない

Slide 14

2009/11/13 版

個人情報保護に関する法対応との「付き合い方」

法律の対応として難しく考えるよりは・・・

お客様に対するビジネスマナーとして考えるのがとりかかりやすい。(と思います。)

そう考えてみると、かなり当たり前のことが要求されているだけです。

マナーを守らない人が多いと法令等により規制されてしまいます。

法律では、5000件以上の個人情報を所有する事業者に限定されていますが、それ未満の規模の会社でもビジネスマナーとして実践するのがお勧めです。

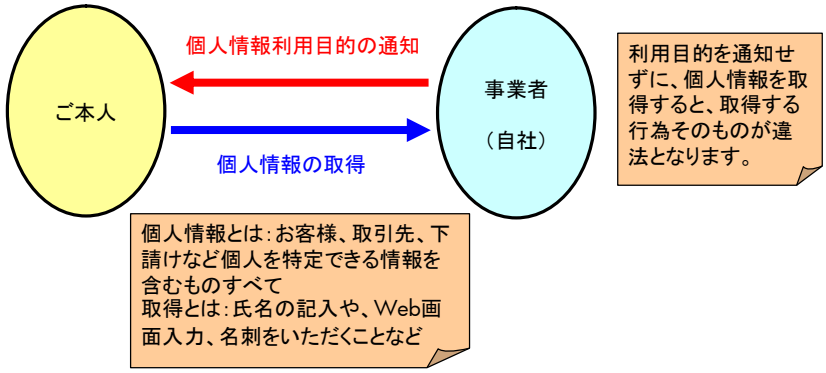
Slide 15

2009/11/13 版

個人情報保護対策「利用目的の通知」

個人情報を取得する際には、必ず、「利用目的」を取得時にご本人に知らせなければなりません。

「利用目的」の表記方法は会社の標準を作るのも一例。その場合には、個々の社員が「利用目的」を勝手に作文しないようにします。

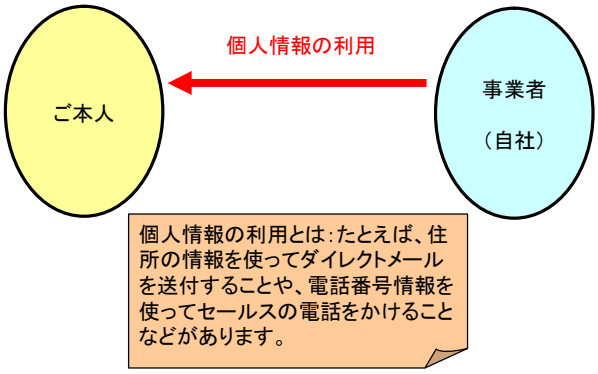


Slide 16

2009/11/13 版

個人情報保護対策
「利用目的の範囲内での利用」

個人情報を利用する際には、ご本人に知らせた「利用目的」を達成する範囲内だけで利用しなければなりません。

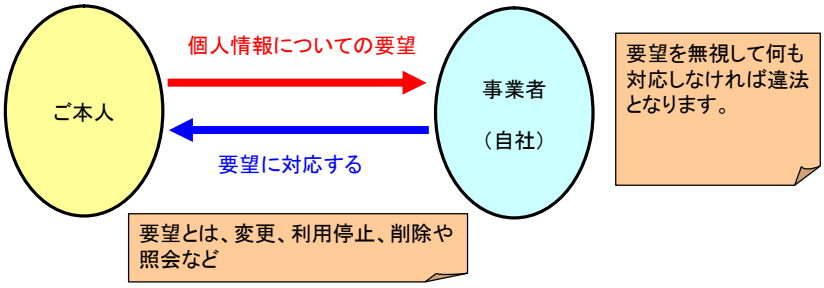


Slide 17

2009/11/13 版

個人情報保護対策
「ご要望に応じる」

個人情報についてご本人からご要望があれば、それに対応しなければなりません。

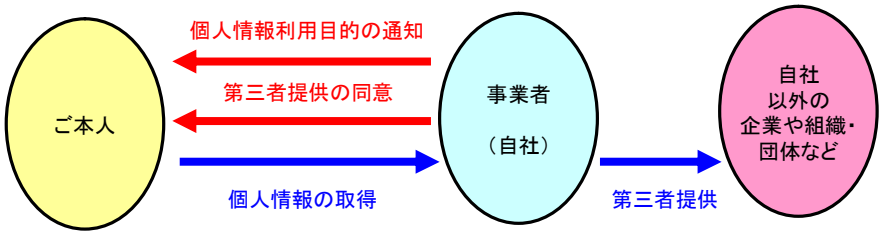


Slide 18

2009/11/13 版

個人情報保護対策
「第三者提供の同意」

個人情報を自社以外に提供する(参照させる)際には、ご本人から、予め「第三者提供の同意」を得なければなりません。



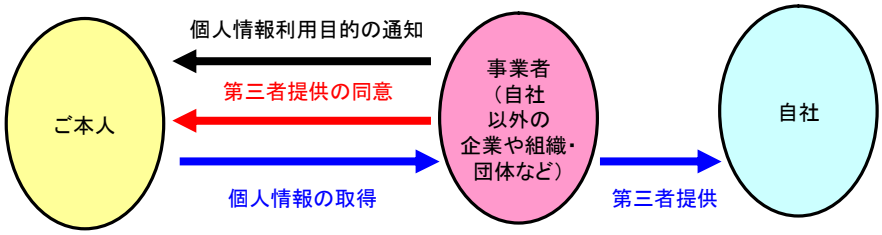
ご本人から第三者提供の同意を予め得ずに、個人情報を自社以外に提供すると違法になります。
イベントやセミナーの共催であっても、例外ではありません。
業務を社外に委託している場合には、その旨を通知したり同意を得たりする必要はありません。

Slide 19

2009/11/13 版

個人情報保護対策
「第三者提供の同意」

個人情報をご本人以外から取得(入手)する場合には、自社に対する第三者提供の同意を予め得てもらったものに限ります。



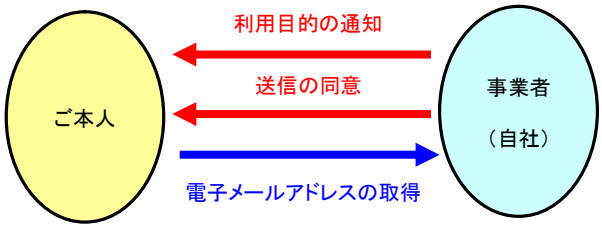
ご本人以外から取得する場合には、最初に取得する人が、事業者以外への第三者提供の同意を得る必要があります。
第三者提供の同意を得ていないものを取得すると、提供を受けた者は不正入手という違法になります。
イベントやセミナーの共催であっても、例外ではありません。
名簿業者も同様です。

Slide 20

2009/11/13 版

個人情報保護対策
「電子メール送信の同意」

電子メールを送信する場合には、予め同意を得なければなりません。



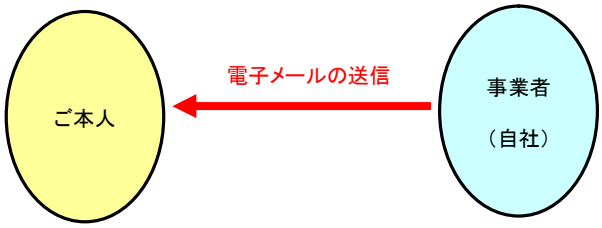
ご本人から電子メール送信の同意を予め得ずに、電子メールを送信すると違法になります。
実際には、「特定電子メール（≒広告宣伝メール）」に該当する内容の電子メール送信だけが対象です。

Slide 21

2009/11/13 版

個人情報保護対策
「電子メール送信時の記載項目」

電子メールを送信する場合には、必要な項目を記載して送信しなければなりません。



電子メールを送信する場合に、必要な項目を記載していなければ違法になります。

必要事項:
a) 送信責任者の氏名・名称
b) オプトアウト手順（連絡先メールアドレスやウェブページのURLなど）
c) オプトアウトができることの説明
d) 送信責任者の住所
e) 問い合わせ先（電話番号、メールアドレスなど何らか）

http://yoshihiro.cocolog-nifty.com/postit/2008/11/post-1186.html

Slide 22

2009/11/13 版

オプトイン／オプトアウト

HPのポリシー

オプトイン（同意原則）

個人情報を取得する際に、利用目的についての合意を得て、それに従って利用する

明示オプトイン：「同意するなら○○してください」

→確認を取れなければ、不同意として扱う

EU,USでのベースライン

暗黙オプトイン：「同意しないなら○○してください」

→確認を取れなくても、同意とみなす

オプトアウト（利用停止）

個人情報保護法の要件

個人情報を利用する際に、利用停止の手段をご本人に通知し、ご要求により利用を停止する

Slide 23

2009/11/13 版

オプトイン・フラッグ

４つのメディアを区別

- 電子メール　（オプトイン）
- ＦＡＸ　（オプトイン）
- 電話　（オプトアウト）
- 郵便　（オプトアウト）

ステータス

- Ｙ　（同意）
- Ｎ　（不同意）
- Ｕ　（未確認）
- Ｉ　（利用禁止）

ID	電子メール	FAX	電話	郵便	氏名	連絡先
1	Y	Y	Y	Y	佐藤	・・・
2	Y	U	N	U	鈴木	・・・
3	Y	N	N	N	田中	・・・
4	I	I	I	I	伊東	・・・

●事業部間連携
●本人確認手段
→お客様ご本人による情報管理

Slide 24

2009/11/13 版

「個人情報〇×対策」という言葉

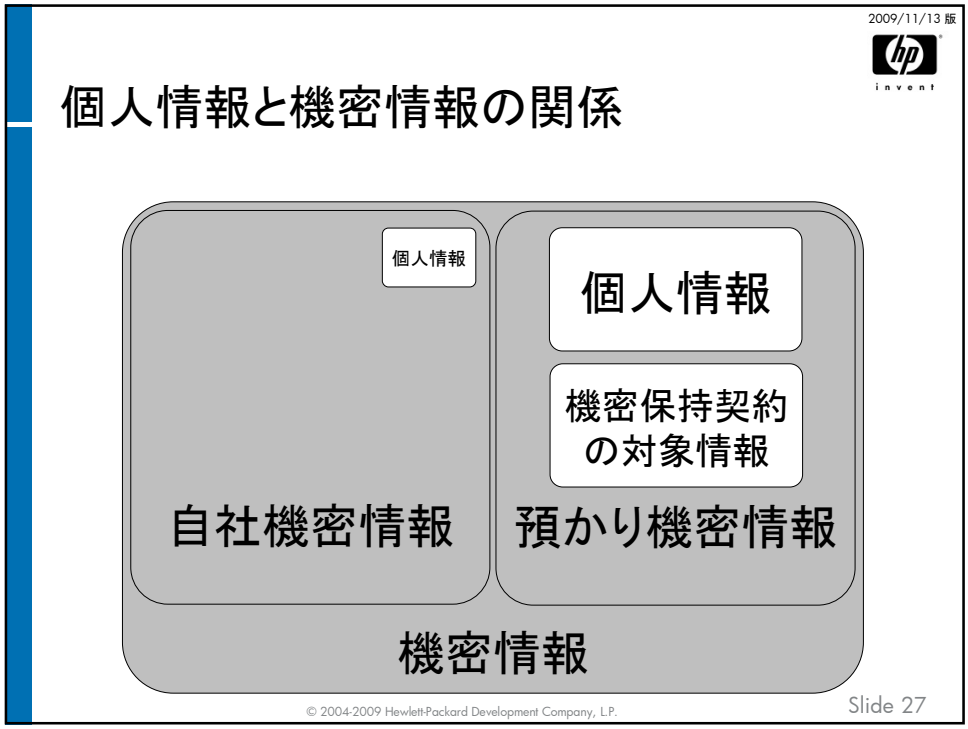
- コンプライアンス（順法）としての
  個人情報保護に関する法対応
- 情報セキュリティ・リスク管理としての
  個人情報の漏洩防止
- ビジネスに役立てるための
  個人情報の活用施策

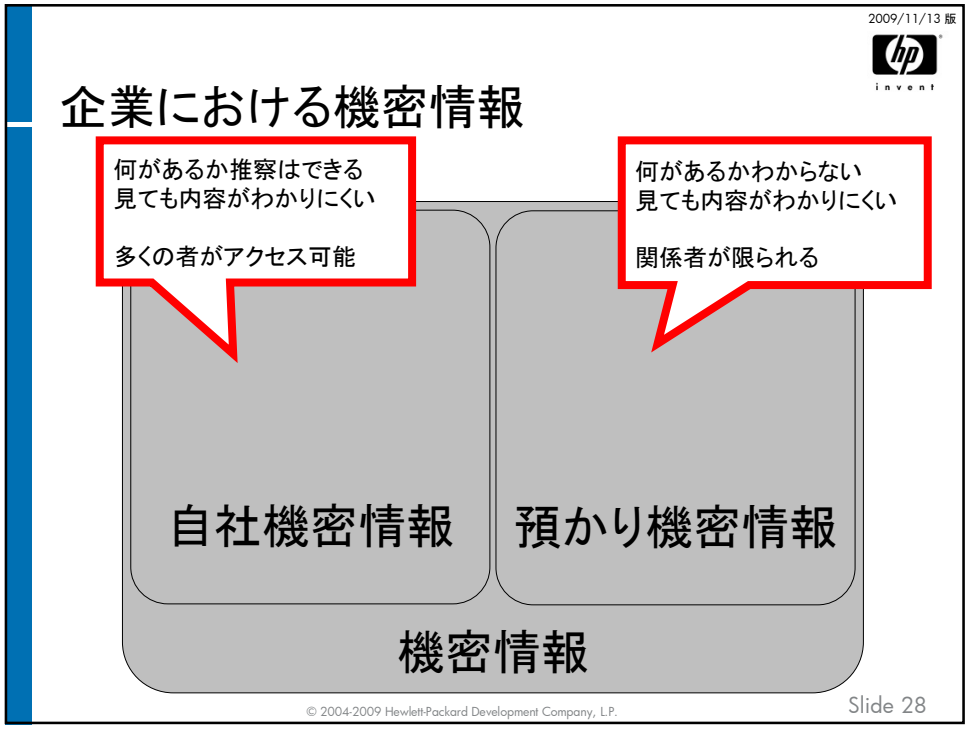
Slide 25

2009/11/13 版

情報セキュリティ対策　と
個人情報保護対策

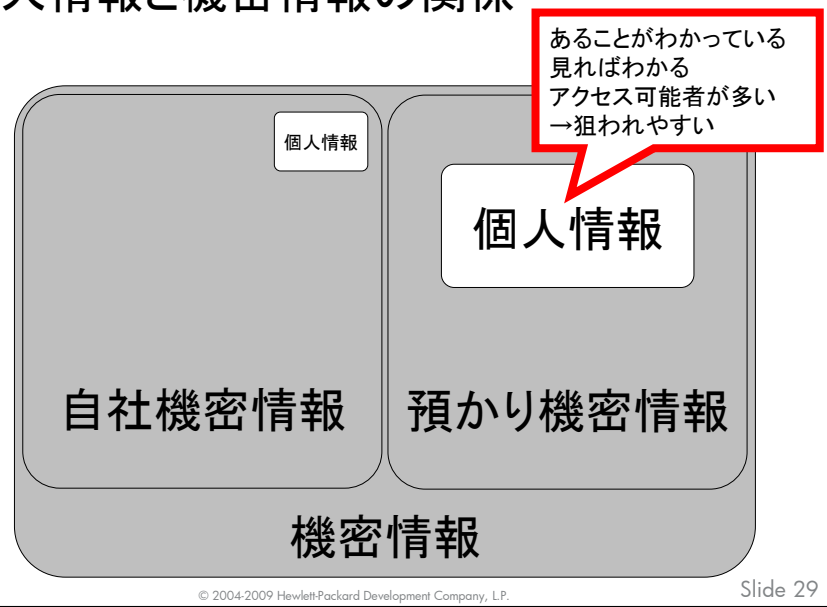
Slide 26





2009/11/13 版

個人情報と機密情報の関係



Slide 29

2009/11/13 版

管理の不徹底が顕在化した
新たな脅威技術が登場したわけではない

- 企業において機密情報管理が徹底していなかった。
- 個人情報の漏洩でそのことが顕在化した。

- 管理が不十分であったとは言い切れないが、不徹底が潜在的にあった。

- 企業内外の情報に対する価値観や環境の変化。
- 現代の企業は、変化に対応することで安定する必要がある。（変化しないことが安定ではない）

Slide 30

2009/11/13 版

個人情報保護法第20条 安全管理措置 と ガイドライン

経済産業省ガイドライン
・個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のため、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び技術的な安全管理措置を講じなければならない。

組織的 安全管理措置	人的 安全管理措置	物理的 安全管理措置	技術的 安全管理措置

Slide 31

2009/11/13 版

経済産業省 個人情報保護法ガイドライン 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)

Slide 32

2009/11/13 版

経済産業省 個人情報保護法ガイドライン 第20条

56ページにわたり、具体的な指針が書かれているが、特に20条　安全管理措置については、11ページを割いて詳述している。

20条のガイドライン（抜粋）

1. 組織的措置
2. 人的措置
3. 物理的措置
4. 技術的措置：
   1. 個人データへのアクセスにおける識別と認証
   2. 個人データへのアクセス制御
   3. 個人データへのアクセス権限の管理
   4. 個人データのアクセスの記録
   5. 個人データを取り扱う情報システムに対する不正ソフトウェア対策
   6. 個人データの移送・通信時の対策
   7. 個人データを取り扱う情報システムの動作確認時の対策
   8. 個人データを取り扱う情報システムの監視

Slide 33

2009/11/13 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)

Slide 34

2009/11/13 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対策統一基準

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（初版2005年12月、最終改訂2009年2月）
- 解説付きの「解説書」を参照していただくことをお勧めします。

Slide 35

2009/11/13 版

IPA（情報処理推進機構）http://www.ipa.go.jp/
中小企業向け情報セキュリティ対策

- **5分でできる！自社診断パンフレット**
- **5分でできる！自社診断シート**

http://www.ipa.go.jp/security/manager/know/sme-guide/index.html

Slide 36

2009/11/13 版

個人情報のライフサイクル

①個人情報の取得・入力
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
②個人情報の移送・送信
宛先間違え、遺失、盗聴などの予防や防止、被害の軽減対策など
③個人情報の利用・加工
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)
情報格付けの継承、システム要件の継承
④個人情報の保管・バックアップ
情報漏洩・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
⑤個人情報の消去・廃棄
廃棄手順の明確化(電子化前後の廃棄手順を含む)

Slide 37

2009/11/13 版

「個人情報○×対策」という言葉

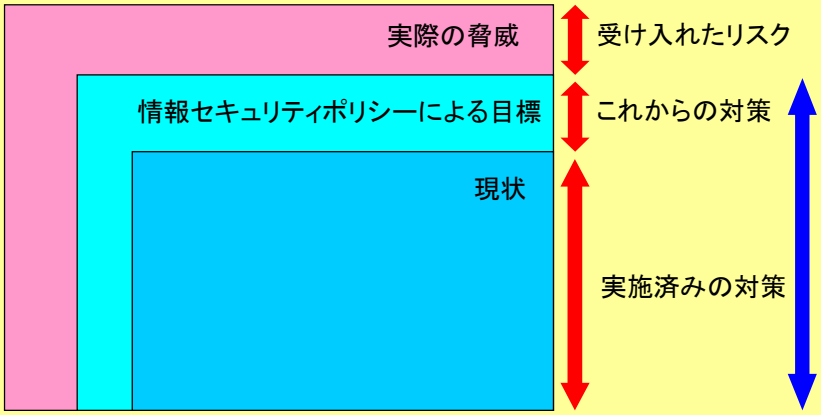
- コンプライアンス(順法)としての
  個人情報保護に関する法対応
- 情報セキュリティ・リスク管理としての
  個人情報の漏洩防止
- ビジネスに役立てるための
  個人情報の活用施策

Slide 38

2009/11/13 版

最低基準ではなく適正基準
「何ができるかより、何をしないか」

ビジネス・リスク対策としての情報セキュリティ施策

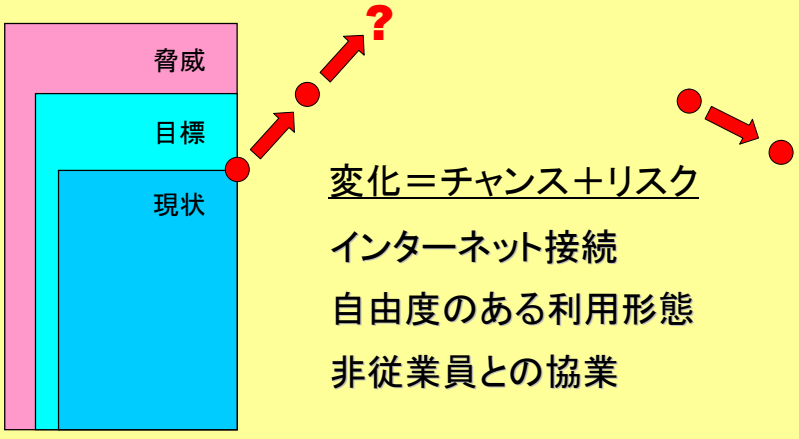


Slide 39

2009/11/13 版

最低基準ではなく適正基準
「何ができるかより、何をしないか」

ビジネス・リスク対策としての情報セキュリティ施策



変化＝チャンス＋リスク

インターネット接続

自由度のある利用形態

非従業員との協業

Slide 40

2009/11/13 版

個人情報管理でのポイント
～顧客に提供する情報の品質改善～

合法であっても問い合わせは来る
→問い合わせにて、合法を納得させられなければ、苦情になる
→問い合わせを軽減するために、施策や説明、同意の有無をわかりやすくする

数撃てば当たる的な販売促進活動は自滅する
→利用停止要求を軽減するために、提供する情報の品質を改善し、継続して情報提供して欲しいと思われる情報の発信をする

Slide 41

2009/11/13 版

情報セキュリティ
情報活用と情報保護のバランス

情報は活用するためにある

情報セキュリティ偏重の過度の情報保護は禁物
情報活用が、企業における情報保持の目的
情報保護は、目的達成のための条件であり義務であるが、目的ではない
情報活用と情報保護のバランスをはかる情報セキュリティ施策とすべき

コスト低減に貢献しないセキュリティ対策は要注意

ITセキュリティ施策をROIで考えてはいけない
IT施策におけるTCO削減は避けれない
TCO削減に貢献する、ITセキュリティ施策でなければ実効性は高まらない
セキュリティ対策のひとつは単純化。単純化はコスト低減になるはず。
逆にコスト低減になっていないということは、複雑化をもたらしている危険信号。
ITの最適化計画の中でセキュリティ対策に取り組むべき

Slide 42

2009/11/13 版

情報セキュリティ
情報活用と情報保護のバランス

守れるルールだけが、守られる。

必ず遵守できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的に企業のセキュリティレベルを向上することができる。
できることの他に、できれば望ましいようなルールを混在させて、「ルールは必ずしも守らなくても良い」という意識を持たれることは好ましくない。
具体的な遵守方法が十分検討されていないようなルールを設けることは論外。
ビジネスの要求に即したバランスを保つルールを設けることが重要。

性善説を前提。性悪説も想定。

性善説を前提とする。その上で、性悪説についても想定する。ことが重要。
性善説であれば、「ルールは守られる」というところから検討し始めることができる。
性悪説への対策は、ルールを守っている性善説の人達によって実施する。しかない。

Slide 43

2009/11/13 版

まとめ

Slide 44

2009/11/13 版

「個人情報〇×対策」という言葉

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

Slide 45

2009/11/13 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」
をビジネスマナーの向上として取り扱うすること。

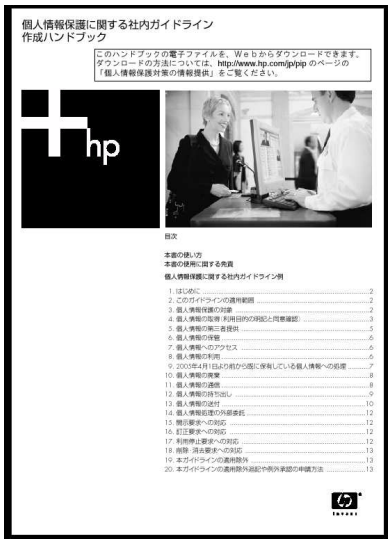
参考：
●社内個人情報保護ガイドラインの公開 (http://www.hp.com/jp/pip)
●「法律から始めない個人情報保護対策」
科学技術振興機構発行　情報管理　2006年8月号 (VOL.49 NO.5)
http://www.jstage.jst.go.jp/article/johokanri/49/5/49_225/_article/-char/ja/

訂正

Slide 46

2009/11/13 版

参考：日本ヒューレット・パッカード 個人情報保護に関する社内ガイドライン


個人情報保護に関する社内ガイドライン
作成ハンドブック

このハンドブックの電子ファイルを、Webからダウンロードできます。
ダウンロードの方法については、http://www.hp.com/jp/pip のページの
「個人情報保護対策の情報提供」をご覧ください。

目次

本書の使い方
本書の使用に関する免責
個人情報保護に関する社内ガイドライン例

Slide 47

invent

本資料のダウンロード
（本資料で紹介したウェブページ）

http://yosihiro.com/go/2009-11-13-tori