個人情報保護対策

2010年11月26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/)

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

ｽﾗｲﾄﾞ：2　©2010

個人情報保護法の位置づけ

自動車の運転と道路交通法の関係に似ています。

道路交通法を守るために運転するわけではありません。
安全な運転をするための（最低限の）ルールが道路交通法で定められています。
自分のためにすること（速度制限など）と、他の人のためにすること（方向指示器の点灯など）で、他の人も安全になり、結果的に自分もまた安全になることで、安全に自動車を利用することができるようになります。

ｽﾗｲﾄﾞ:3 ©2010

個人情報保護法の位置づけ

事業者による個人情報の利用について安心してもらうための法律です。

安心してもらうための（最低限の）ルールが個人情報保護法で定められています。

安心してもらうことによって、事業者は個人情報を利用することができるようになります。

ｽﾗｲﾄﾞ:4 ©2010

個人情報保護法の位置づけ

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。）

そう考えながら内容を理解すると、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。

ｽﾗｲﾄﾞ:5

ご紹介する内容

個人情報保護法の説明が、道路交通法の学科教習だとすると、
これからご紹介するのは、安全運転教習です。

ｽﾗｲﾄﾞ:6

用語:個人情報取扱事業者

法律では、５０００人分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、それ未満の規模の事業者でもビジネスマナーとして実践するのがお勧めです。

事業者には、企業だけではなく、学校や、機関、任意団体（町内会や同窓会など）も含まれます。

用語:個人情報

一般的に使われる「個人情報」という用語で考えればよいですが、以下の点に注意するとわかりやすいです。

①電子、非電子のいずれも対象
②お客様以外も対象（業者担当者、従業員、採用面接者などもすべて含む）
③法人等の連絡先情報も対象
④公知の情報も対象

個人情報保護対策 「法律による主な義務」

個人情報保護法
- 利用目的の通知
- 利用目的の範囲内での利用
- ご要望に応じる
- 第三者提供の同意

http://www.caa.go.jp/seikatsu/kojin/index.html

特電法（特定電子メールの送信の適正化等に関する法律）
（通称、迷惑メール防止法）
- 電子メール送信の同意
- 電子メール送信時の記載項目

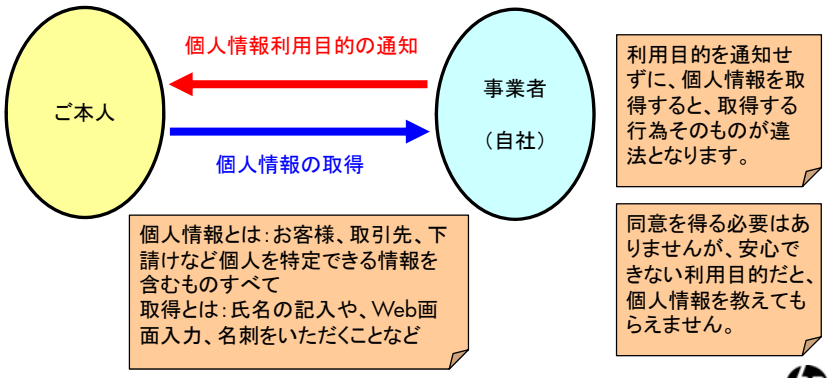
http://www.caa.go.jp/representation/index.html#m03

個人情報保護対策 「利用目的の通知」

個人情報保護法による義務

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。

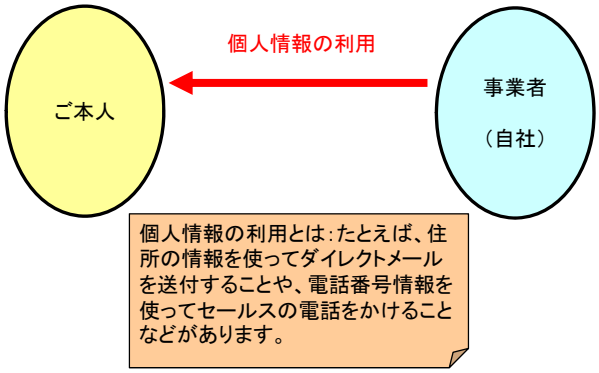
「利用目的」の表記方法は会社の標準を作るのも一例。その場合には、個々の社員が「利用目的」を勝手に作文しないようにします。



個人情報保護対策
「利用目的の範囲内での利用」

個人情報保護法による義務

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。

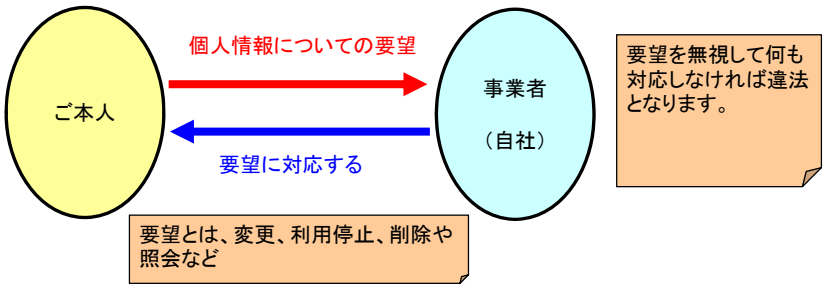


スライド：11　©2010

個人情報保護対策
「ご要望に応じる」

個人情報保護法による義務

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。

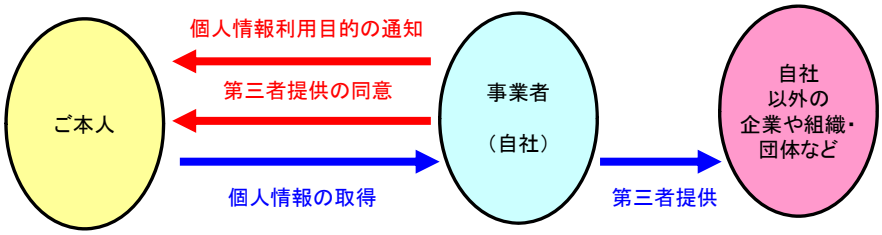


スライド：12　©2010

個人情報保護対策「第三者提供の同意」

個人情報保護法による義務

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。



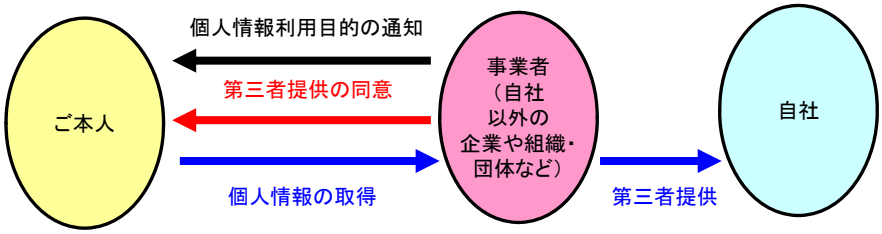
ご本人から第三者提供の同意を予め得ずに、個人情報を自社以外に提供すると違法になります。
イベントやセミナーの共催であっても、例外ではありません。
業務を社外に委託している場合には、その旨を通知したり同意を得たりする必要はありません。

スライド：13　©2010

個人情報保護対策「第三者提供の同意」

個人情報保護法による義務

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。



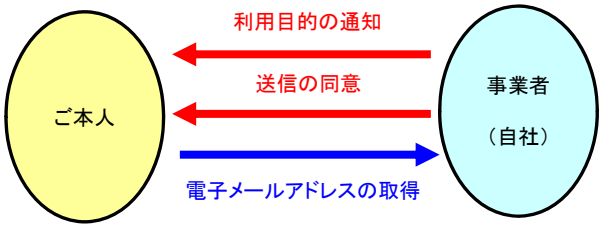
ご本人以外から取得する場合には、最初に取得する人が、事業者以外への第三者提供の同意を得る必要があります。
第三者提供の同意を得ていないものを取得すると、提供を受けた者は不正入手という違法になります。
イベントやセミナーの共催であっても、例外ではありません。
名簿業者も同様です。

スライド：14　©2010

個人情報保護対策「電子メール送信の同意」

特電法（迷惑メール防止法）による義務

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。



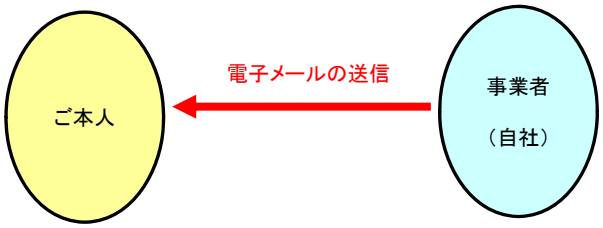
ご本人から電子メール送信の同意を予め得ずに、電子メールを送信すると違法になります。
実際には、「特定電子メール（≒広告宣伝メール）」に該当する内容の電子メール送信だけが対象です。

ｽﾗｲﾄﾞ：15　©2010

個人情報保護対策「電子メール送信時の記載項目」

特電法（迷惑メール防止法）による義務

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

ｽﾗｲﾄﾞ：16　©2010

同意を得る／利用を断られる オプトイン／オプトアウト

オプトイン（同意原則）

同意を得る方式には2種類あります。

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

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）

個人情報の利用を断られたことにより、利用しない又は利用を停止する

スライド：17　©2010

個人情報と同意状態の管理

例：

連絡手段で区別

- 電子メール（同意必要）
- ＦＡＸ
- 電話
- 郵便

状態値

- Ｙes（同意）
- Ｎo（不同意）
- Ｕnkown（未確認）
- Ｉsolate（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	・・・

検討事項：

●部署ごとの管理の場合、部署間連携方法

●お問い合わせ時の本人確認手段

スライド：18　©2010

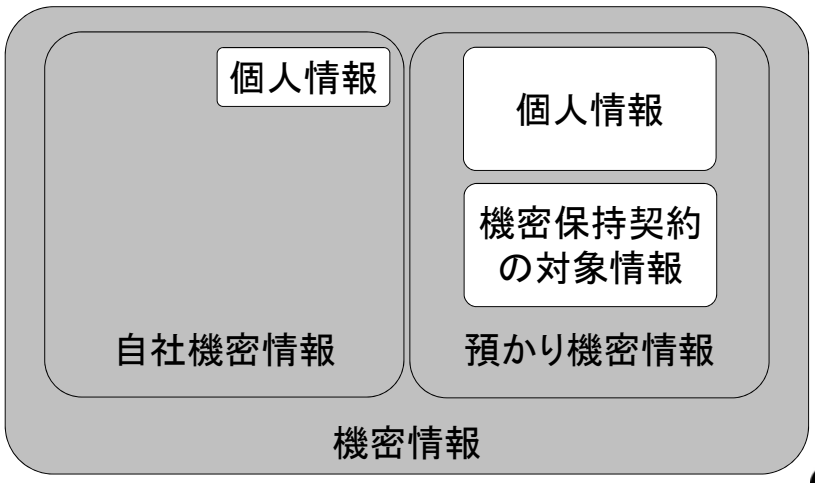
参考:
法律から始めない個人情報保護対策

科学技術振興機構発行
情報管理　2006年8月号 (VOL.49 NO.5)

http://www.jstage.jst.go.jp/article/johokanri/49/5/49_225/_article/-char/ja/

個人情報の安全管理措置

個人情報と機密情報の関係



情報管理の不徹底の顕在化

新たな脅威が登場したわけではない

- 機密情報管理が徹底していなかった。
- 個人情報の流出や紛失等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。
- 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）

スライド：21　　©2010

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

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

- **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**

スライド：22　　©2010

個人情報のライフサイクル に沿った安全管理措置

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）

ｽﾗｲﾄﾞ：23 ©2010

個人情報管理でのポイント ～お客様にお届け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、利用目的だけではなく利用頻度・方法や安全対策、オプトイン（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
→オプトアウト（利用停止）要求を軽減するために、お客様に連絡する情報（ダイレクトメールの内容など）の品質を改善し、継続して連絡して欲しいと思われる情報をお送りする

ｽﾗｲﾄﾞ：24 ©2010

利活用と保護のバランスを取るには？

守れるルールだけが、守られる。

実施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、結果的にルール遵守を定着させることができる。
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、「必ずしも守らなくてもよいルールもある」という意識を持たれることは好ましくない。
遵守するための具体的な実施方法が明確になっていないルールを設けることは避ける。
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。

スライド：25　©2010

利活用と保護のバランスを取るには？

性善説を前提にして性悪説も想定する

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と考えることが重要。

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ことを忘れてはいけない。

スライド：26　©2010

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ｶﾞｲﾄﾞﾗｲﾝ作成ﾊﾝﾄﾞﾌﾞｯｸ

http://yosihiro.com/go/hp/privacybook
からPDFファイルをダウンロードできます。

ｽﾗｲﾄﾞ：27　　©2010

まとめ

用語の注意点
法律による主な義務
オプトインとオプトアウト
個人情報と同意状態の管理
個人情報の安全管理措置
　個人情報と機密情報の関係
　新しい脅威ではない
　ライフサイクルに沿った管理
利活用と保護のバランス
　守れるルールだけが守られる
　性善説を前提にして性悪説も想定する

http://yosihiro.com/speech/#2010-11-26

ｽﾗｲﾄﾞ：28　　©2010