プライバシー対策の特徴：

情報セキュリティ対策との違いについて

2012年5月17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
佐藤　慶浩

あるシンポジウムのアンケート結果から

■プライバシーや個人情報保護の対策には、情報流出対策や不正アクセス対策などの情報セキュリティ以外の対策として、どのようなことがあるか具体的に2つ以上ご存知ですか？

1．はい　　2．いいえ　　3．よくわからない

24名

「はい」の場合、
ご存知のものを2つだけ具体的にお書きください：

回答数　57名

正解＝13名 (23%)

個人情報保護対策

利用目的の特定

利用目的の本人への通知

利用についての本人からの同意獲得

第三者提供の際の本人からの同意獲得

本人からの要求（訂正、利用停止等）への対応

安全管理

など

弊社のﾏｰｹﾃｨﾝｸﾞ/営業担当者向けﾄﾚｰﾆﾝｸﾞ

HPの基本的な考え方
個人情報のライフサイクル
個人情報の利用
個人情報の安全管理措置

弊社のﾏｰｹﾃｨﾝｸﾞ/営業担当者向けﾄﾚｰﾆﾝｸﾞ トレーニング目的

以下の手順について、適切な手順を理解すること。

- お客様からお名前や連絡先（以下、お客様情報）を入力や記入していただき入手する際の手順
- 入手したお客様情報の保管と顧客データベースへの登録等の手順
- 顧客データベース等で管理しているお客様情報の利用手順
- お客様情報の入手に日本HP以外が関係（セミナーやイベントを他社と共催など）する場合の手順
- お客様情報をプロモーションで利用する際の手順

目次

お客様情報の取り扱い

- HPの基本的な考え方
- 個人情報のライフサイクル
- 個人情報を使ったプロモーション

HPの基本的な考え方

HPの基本的な考え方

個人情報保護　＝　プライバシー保護

個人情報の適切な取り扱い

文字が*イタリック体(斜体)*になっている箇所は、日本HP独自の呼称や制約です。
（以下、この資料において同じ。）

プライバシー保護とは、何？

プライバシー保護対策
Privacy protection measures

- 個人情報についてプライベートなことを詮索しない。
- 個人情報を利用目的の範囲内でだけ使う。
- 個人情報の漏洩を防ぐ。
- 個人情報を本人が好まないことに使わない。

ホテルで、PRIVACY PLEASE をドアノブに吊るしたときの期待は？

●私についてプライベートなことを詮索しないでください。

●私の名前を内緒にしてください。

●私が宿泊の支払いに使うクレジットカード番号を内緒にしてください。

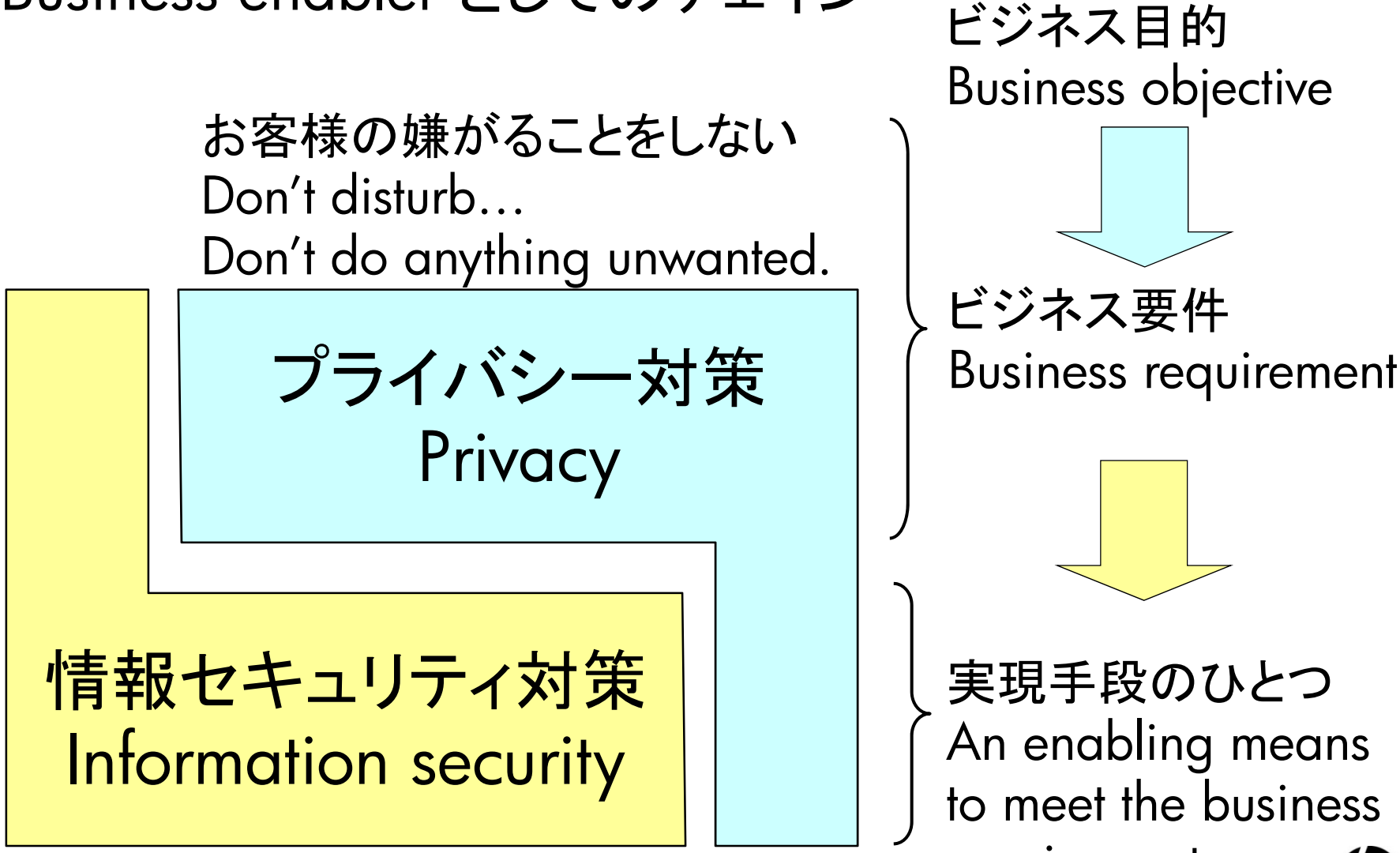
●私の邪魔をしないでください。

プライバシーとは・・・
「私の邪魔をしないでください」

プライバシーとは、本人が選んだ係わり合いだけで、それ以外の干渉を受けない権利
privacy is the right to be left alone and associate with whom you choose

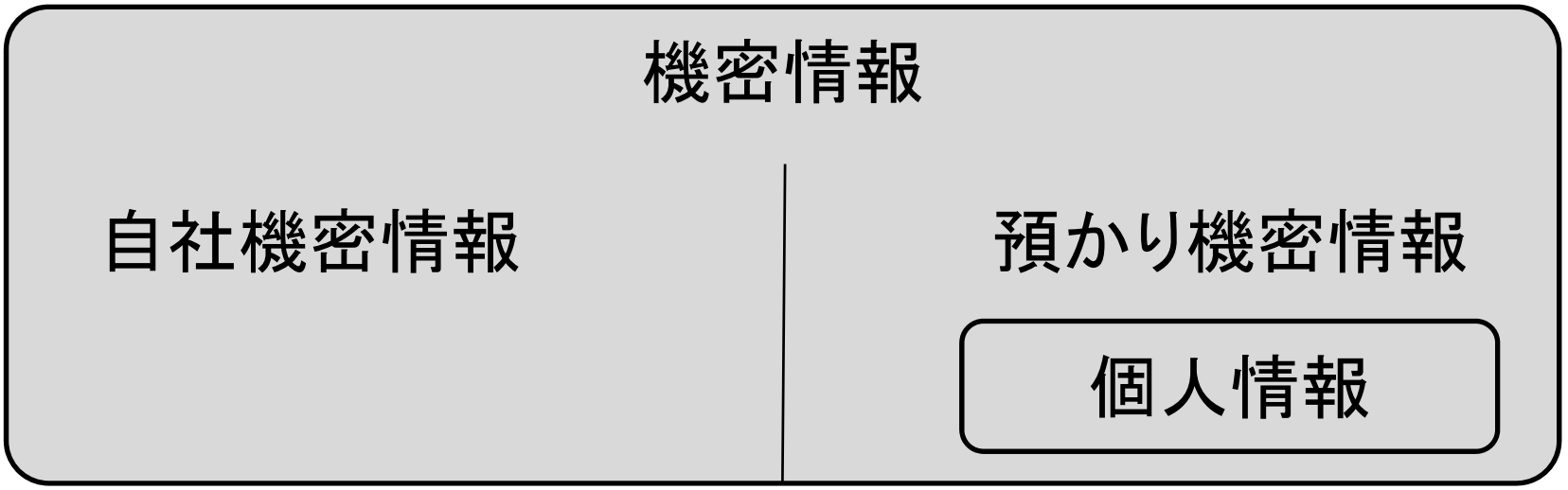
プライバシー対策は、個人データの適正かつ丁重な使用
privacy is the fair and respectful use of personal data

HPにおけるプライバシーとセキュリティ対策
Business enabler としてのチェイン



個人情報は　預かり機密情報　として取り扱う

・機密情報には、大きく分けて、自分の情報と、他から預かっている情報の２種類がある。



参考：機密情報とは

http://bit.ly/kimitsujouhou

http://yoshihiro.cocolog-nifty.com/security/2004/12/post_2.html

個人情報のライフサイクル

個人情報のライフサイクル

- 個人情報の属性
- 個人情報の入手
- 個人情報の登録
- 個人情報の保管
- 個人情報の通信・移送
- 個人情報の提供（←共用・共同利用）
- 個人情報の廃棄・消去

お客様情報(＝個人情報)の属性
お客様への連絡に用いる属性

氏名

役職名

部署名

会社名

住所　＝　郵送による連絡で用いる属性

電話番号　＝　電話による連絡で用いる属性

eMailアドレス　＝　eMail送信による連絡で用いる属性

FAX番号　＝　FAX送信による連絡で用いる属性

お客様情報の入手
入手の形態：一次的と二次的

一次的入手

日本HPがご本人から入手し、かつ、
ご本人は日本HPに提供したと認識している入手方法。
入手作業について業務委託先を経由してもよい。※

二次的入手

一次的入手以外の入手方法。
例）イベント・セミナー等の共催会社から入手
例）名簿業者から入手

※業務委託契約に付帯契約（個人データ保護契約）の*追加締結が必要*。→機密保持対象が異なるため、業務委託契約の機密保持条項だけでは不十分。

文字が*イタリック体（斜体）*になっている箇所は、日本HP独自の呼称や制約です。
（以下、この資料において同じ。）

お客様情報の入手
一次的入手

利用目的の通知

セールス用途であれば「全社共通標準文言」を、それ以外であれば「業務連絡文言」を記載すること。

同一書面（同一ページ）に記載すること。

利用目的の同意（オプトイン）取得

電子メールアドレスとFAX番号を入手する場合には、*明示的な同意確認を得ること。*

住所と電話番号については、*必ずしも同意確認を得なくて構わない。*

お客様情報の入手
二次的入手

二次的入手の同意取得

一次的入手者からHPにお客様情報を提供することについて、
一次的入手者が、ご本人から同意を事前に得る必要がある。

その際に、
一次的入手と同じ「利用目的通知」「利用目的同意取得」をご本人に通知・確認する必要がある。

HPは、一次的入手者が上記を実施することについて「事前に」約束してもらう必要がある。

お客様情報の入手
入手する項目

セールス用途であれば、以下の項目を入手する。

氏名、役職名、部署名、会社名

住所、電子メールアドレス、電話番号、FAX番号

その他、お客様情報DB登録に必要な項目

それ以外の用途（＝*業務連絡*※）であれば、その用途に必要最小限の項目だけを入手する。

業務連絡に用いない項目を入手してはならない。

例）FAX送信しないなら、FAX番号を入手しない。

※*業務連絡*：法第18条4号4項「取得の状況からみて利用目的が明らかであると認められる場合」に該当するが、社内ガイドラインの定義を必ず参照のこと。

お客様情報の入手
同意（＝オプトイン：Opt-in）取得の方法

明示的同意（Explicit Opt-in）確認

「同意していただけるなら、～～してください。」という確認方法。ご本人が能動的に「～～する」ことによってのみ、同意を確認する方法。

デフォルト・オフとも言われる。

暗黙的同意（Implicit Opt-in）確認

「同意しないなら、～～してください。」という確認方法。→「～～しないなら、同意したとみなします。」と暗黙に確認する方法。

デフォルト・オンとか、みなし確認とも言われる。

同意を明示的に取得すると、同意率が下がる可能性があるが、後日に「同意したつもりはなかった」という苦情を避けられやすい。

お客様情報の入手
同意（＝オプトイン：Opt-in）取得率の向上

お客様に同意をしていただきやすい文章で取得する必要がある。

「HPからの製品案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内を1ヶ月間に最大1回お送りしてもよろしいでしょうか？」

目的や頻度を限定すれば、同意取得率は向上する場合がある。

目的が広ければ、色々な目的に使えるが、同意取得率が低下する場合がある。

お客様情報の登録

お客様情報は、原則として お客様情報DB に登録しなければならない。

お客様情報DB の登録ガイドラインに従う。

利用目的の同意取得結果を正しく登録する。

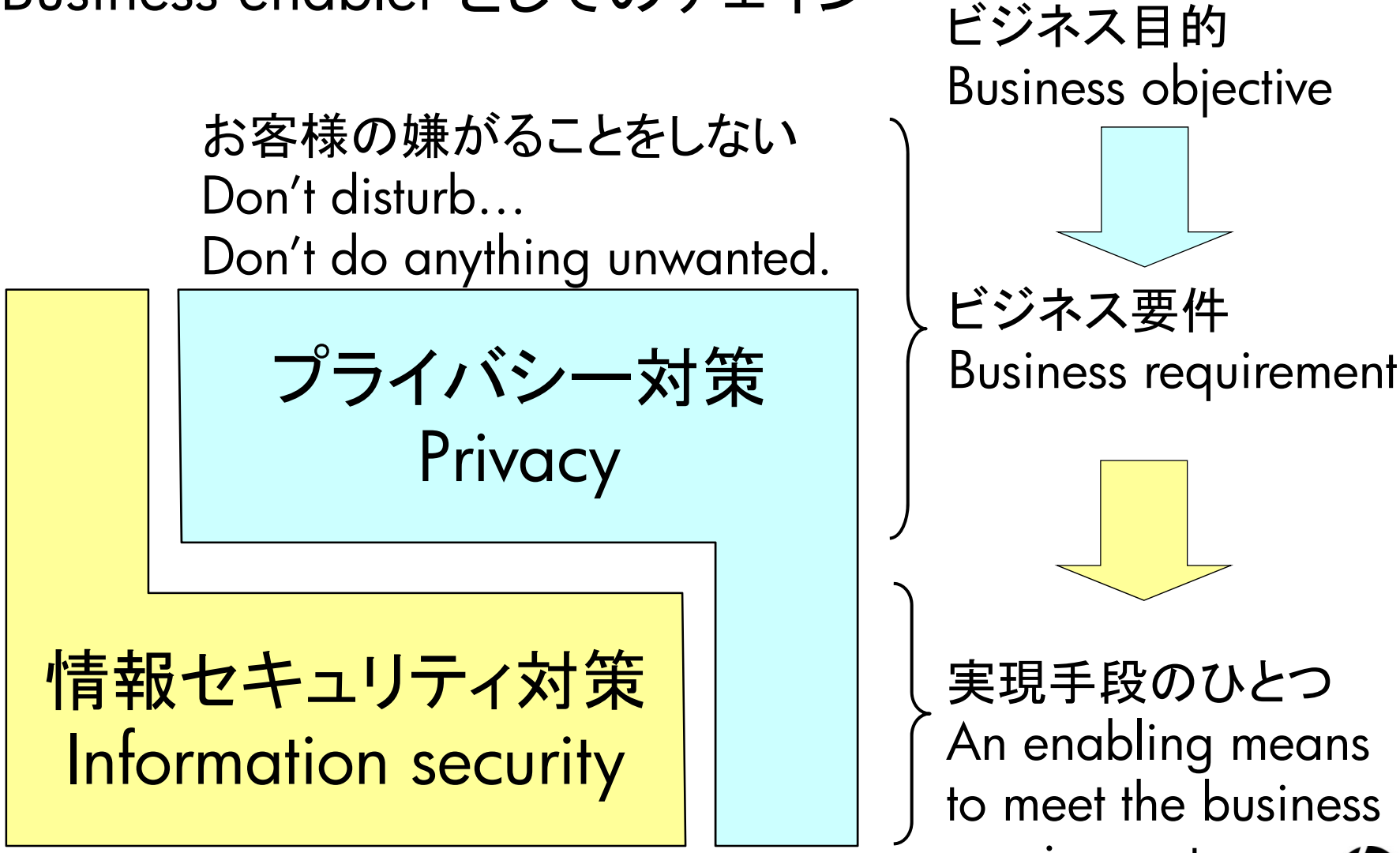
お客様情報の保管

お客様情報の保管は一時的にだけ許される。

→恒常的（1ヶ月以上）保管は お客様情報DB に登録すること。

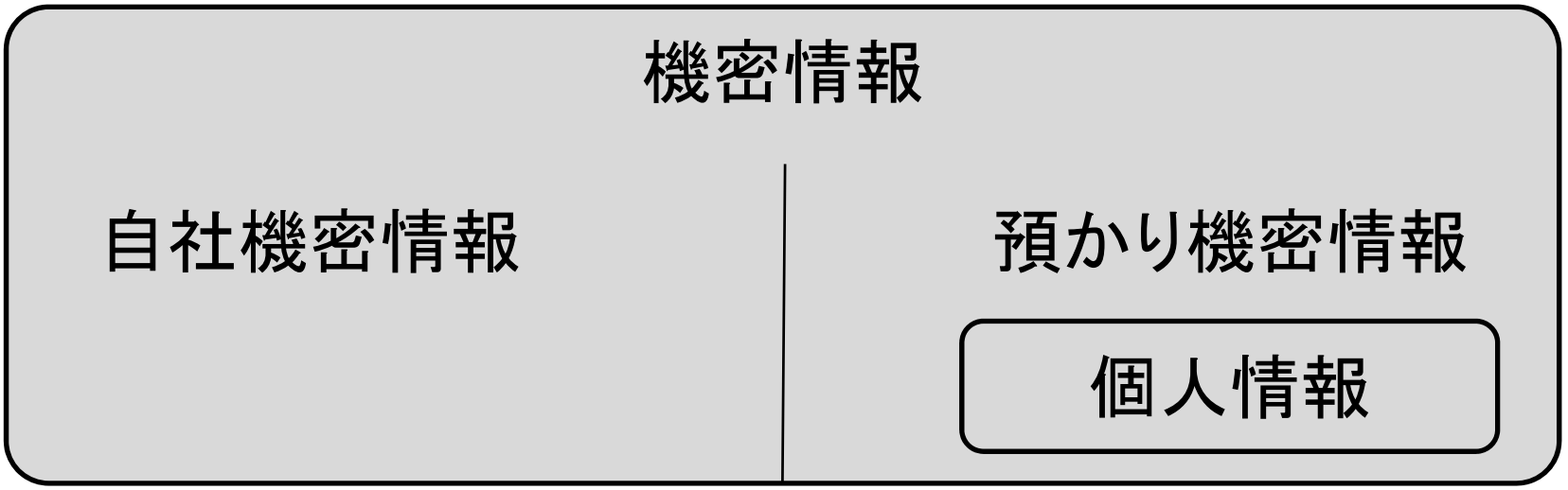
HP秘(HP Confidential)として保管する。

HPにおけるプライバシーとセキュリティ対策
Business enabler としてのチェイン



個人情報は　預かり機密情報　として取り扱う

・機密情報には、大きく分けて、自分の情報と、他から預かっている情報の２種類がある。



参考：機密情報とは

http://bit.ly/kimitsujouhou

http://yoshihiro.cocolog-nifty.com/security/2004/12/post_2.html

機密保持契約書 と 個人情報保護契約書における機密保持条項 との違い

機密保持契約書
- 機密情報を提供者が特定
- 業務達成目的の範囲内で関係者の取り扱いを許容
- 業務達成目的の範囲内で主体的に利活用される

個人情報保護契約における機密保持
- 個人情報を受領者が認識
- 取り扱い者は業務の直接従事者に制限
- 主体的な利用は一切禁止

お客様情報の保管
HP秘(HP Confidential)としての対策

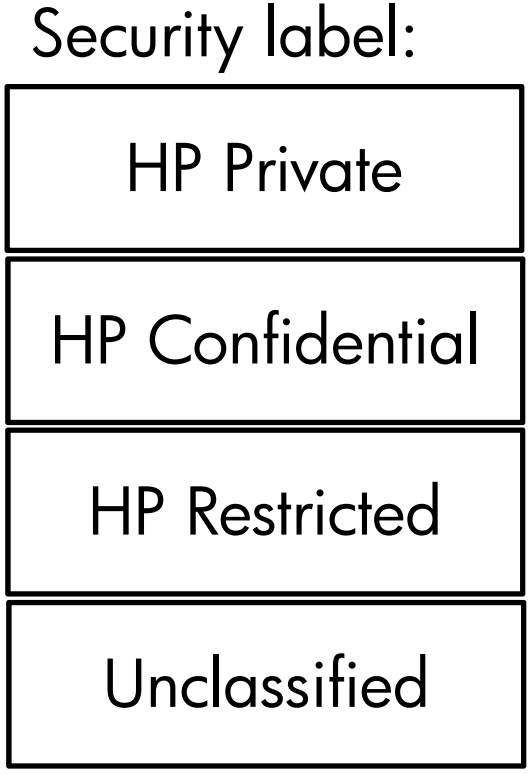
HP業務外秘(HP Restricted)としての対策は不十分である点に注意。

・*アクセス制限が必須*

・*社外通信は暗号化（S/MIME）が必須*

→パスワード保護は条件によっては不十分

詳細については、社内個人情報保護ガイドラインを参照。



お客様情報の通信・移送

通信

専用ウェブサイトを利用する

宛先指定間違えに注意する

暗号化やパスワード保護を適切に行なう

移送

通信と同様

紙媒体と電子媒体にはそれぞれ特徴がある

紙媒体：漏洩防止の技術的対策が困難

電子媒体：複製防止の技術的対策が困難　など

特徴に合った対策を行なう

お客様情報の提供

HP以外（業務委託先を除く）に提供する場合には、例外なく、ご本人から事前に同意を得なければならない。→その際、*明示的*同意確認を得ること。

*提供先の利用目的をご本人に通知する*こと。

利用目的の同意取得をするかは、提供先のポリシーによる。

★他社との間で、お客様情報について、共用・共同利用という考え方をしない点に注意。個人情報保護法にある「共同利用」は、「共同で利用する」という一般的な意味ではなく、法律の要件を満たした限定した利用方法である点に注意。

お客様情報の廃棄・消去

廃棄

書面：シュレッダー又は社外秘ごみ箱

記録媒体：データ抹消又は破壊

消去

データ抹消（ *フリーソフト eraser を使用*すること）

詳細については、社内個人情報保護ガイドラインを参照。

個人情報の利用
（お客様情報を使ったプロモーション）

お客様情報を使ったプロモーション データ抽出・照合

Privacy preference（＝オプトアウト＆オプトイン）の確認

オプトアウト（利用停止）の有無の確認

お客様の連絡先（住所、電話番号、電子メールアドレス、FAX番号）について、オプトアウトの申し出がないことを確認しなければならない。

オプトインの状態の確認

*電子メールアドレスとFAX番号については、オプトインを得ていること*を確認しなければならない。

プロモーションに使えないデータベース

Privacy preferenceの管理機能のないデータベースにあるお客様情報はプロモーションに使ってはならない。

お客様情報を使ったプロモーション
データ抽出・照合

Privacy preference（＝オプトアウト＆オプトイン）の値（フラッグ）と状態

Y (Yes)：明示的オプトインを得た

N (No)：オプトインを拒否された　又は
オプトアウトされた

U (Unknown)：オプトインの確認をしていない

I (Isolated)：データの削除要求をされた

お客様情報を使ったプロモーション
コンタクト・ポリシーの管理

住所（*YまたはUにコンタクト可能*）

DM（郵送によるダイレクトメール）

→担当者許可制　＋　送付届出制

電話番号（*YまたはUにコンタクト可能*）

テレセールス（テレマーケティング）

→ガイドライン遵守

電子メールアドレス（*Yのみにコンタクト可能*）　※オプトイン必要

eDM（電子メールによるダイレクトメール）

→原則として発行を集約

FAX番号（*Yのみにコンタクト可能*）　*※オプトイン必要*

FAX送信によるセールスや案内

→（ガイドライン作成中）

お客様情報を使ったプロモーション
データ更新

お客様からのフィードバックを適時かつ正確にデータ更新すること。

登録データの変更（住所変更など）

利用停止（＝オプトアウト）状態の更新

お客様からの「～～してください。」という依頼については、「HPとして、～～させていただきます。」と受け止めること。

→「自分又は自部署が～～する」のでは不十分な点に注意すること。


SUPPORT ANGELS
NEXT
starring AKB48


SUPPORT ANGELS
NEXT
starring AKB48

篠田 — 大島 — ？


ココロ オドル タッチ

お客様情報を使ったプロモーション データの廃棄・消去

プロモーション実施後は速やかに、適切な廃棄・消去を徹底すること。

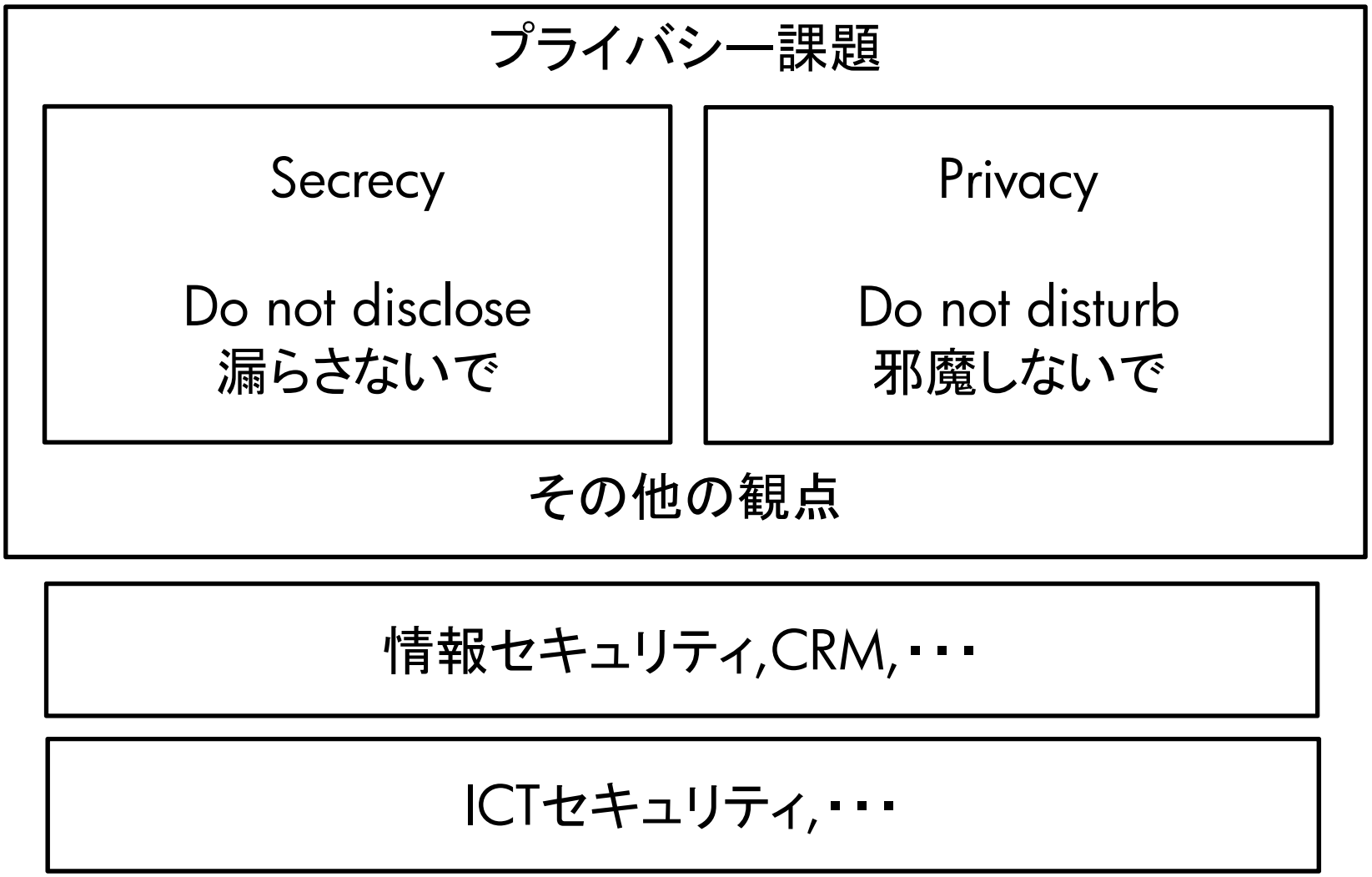
お客様情報は、動的なもので利用期限付き情報だという認識が必要。

まとめ

プライバシー対策の特徴：
セキュリティ対策との違いについて

・利用目的の特定
・利用目的の本人への通知
・利用についての本人からの同意獲得
・第三者提供の際の本人からの同意獲得
・本人からの要求（訂正、利用停止等）への対応

プライバシー対策とセキュリティ対策の関係



まとめ

情報セキュリティ対策と個人情報保護対策の違い

- 利用目的の特定
- 利用目的の本人への通知
- 利用についての本人からの同意獲得
- 第三者提供の際の本人からの同意獲得
- 本人からの要求（訂正、利用停止等）への対応