個人情報保護対策と情報セキュリティ対策の国際標準化動向と企業実務

個人情報保護対策と情報セキュリティ対策の関係を整理し、双方の効率的な運用方法に関して、ISO/IEC国際会合での動向と、企業実務とについて、BYODやソーシャルメディア利用対策も交えての解説

2012年11月22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

発表者紹介

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード　個人情報保護対策室　室長
元　内閣参事官補佐・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
　消費者庁　個人情報保護法説明会　講師
　JIPDEC　プライバシーマーク推進センター　非常勤研究員
　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
これまでの関連活動
　経済産業省 個人情報保護ガイドラインQ＆A集検討会　元委員
　JIPDEC　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ運営要領改正委員会　元委員
　(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　元委員
その他
　http://yosihiro.com/profile/

目次

個人情報保護対策と情報セキュリティ対策
個人情報保護対策の弊社事例紹介
プライバシー・バイ・デザイン
国際規格動向
BYOD（参考情報紹介のみ）

個人情報保護対策と情報セキュリティ対策

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取得

第三者提供の際の本人からの同意取得

本人からの要求（訂正、利用停止等）への対応

安全管理

など

個人情報保護対策の弊社事例紹介

プロモーション業務トレーニング

2012年11月19日 REV1

日本ヒューレット・パッカード株式会社
CRM（カスタマ・リレーションシップ管理）委員会

この資料の取り扱い

機密指定が明記されているスライド以外については、社外に開示して構いません。

プロモーション業務に従事する社外の委託先などについては、本資料で説明されている遵守事項の周知と徹底をお願いします。

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

プロモーション業務トレーニング
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
- ●まとめ

●景品表示法

●ブランディング

●ソーシャルメディア利用

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。

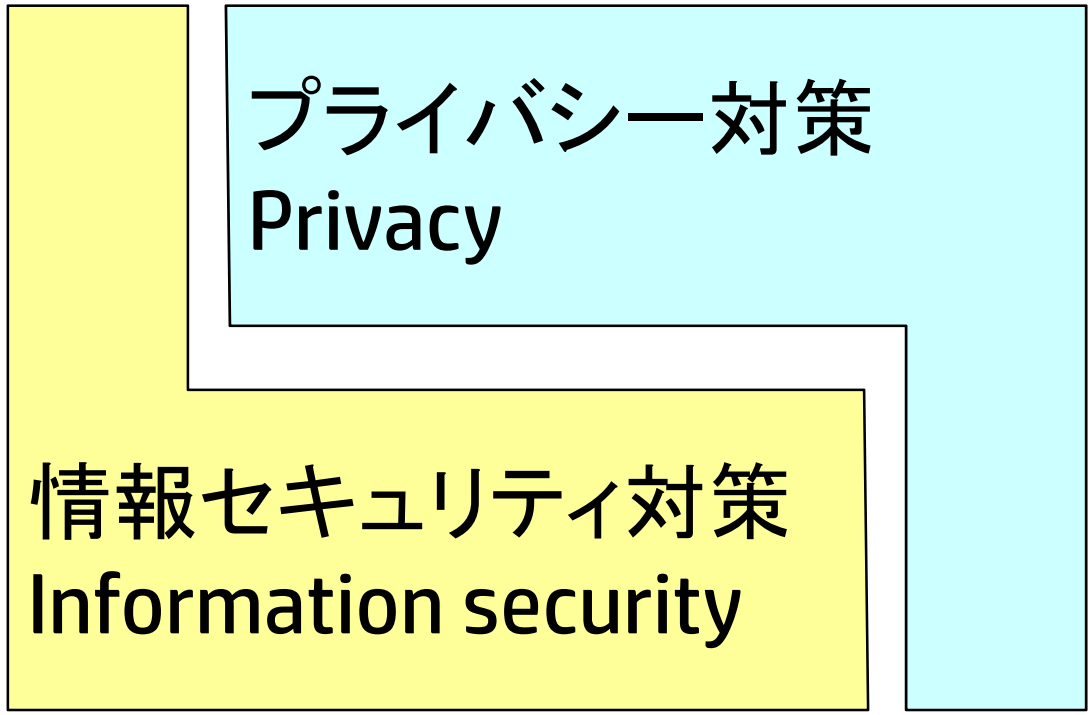
●私の邪魔をしないでください。

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



ビジネス目的
Business objective

ビジネス要件
Business requirement

実現手段のひとつ
An enabling means
to meet the business
requirement

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
- 個人情報の廃棄・消去
- 個人情報の提供

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。

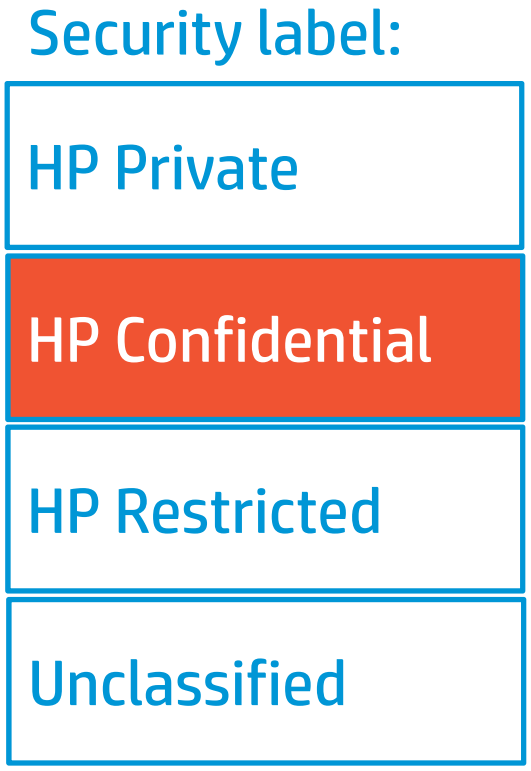
HP秘(HP Confidential)として保管する。

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。

お客様情報の提供

業務委託先以外への提供

業務委託先（サプライヤ）への提供

お客様情報の提供
業務委託先以外

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・共同利用や第三者提供を利用目的にする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。

お客様情報の提供
業務委託先

HP以外を業務委託先（サービス・サプライヤー）に提供して、業務を委託する場合には、例外なく、PDPA（個人データ保護契約）を事前に締結しなければならない。

→CDA又はNDAなどの機密保持契約書や契約書の機密保持遵守条項では、不十分であることに注意してください。

お客様情報の提供
業務委託先

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

相手方との予めの合意に基づき締結日をさかのぼって構わない

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

締結日をさかのぼることはできない

個人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の管理及びコンタクトポリシー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。

★お客様情報は、静的なものではなく利用期限付き情報だという認識が必要。

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
媒体の種類ごとのガイドライン

電子メールアドレス（Yのみにコンタクト可能）
eDM（電子メールによるダイレクトメール）
→担当者許可制　＋　送付届出制
※迷惑メール防止法遵守が必要
住所（Y又は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


DMガイドライン

電話番号（Y又はUにコンタクト可能）
テレセールス（テレマーケティング）
→コンタクト・スクリプトの準備が必要


テレマ・ガイドライン

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
→実施する場合は個人情報保護対策室に連絡

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。

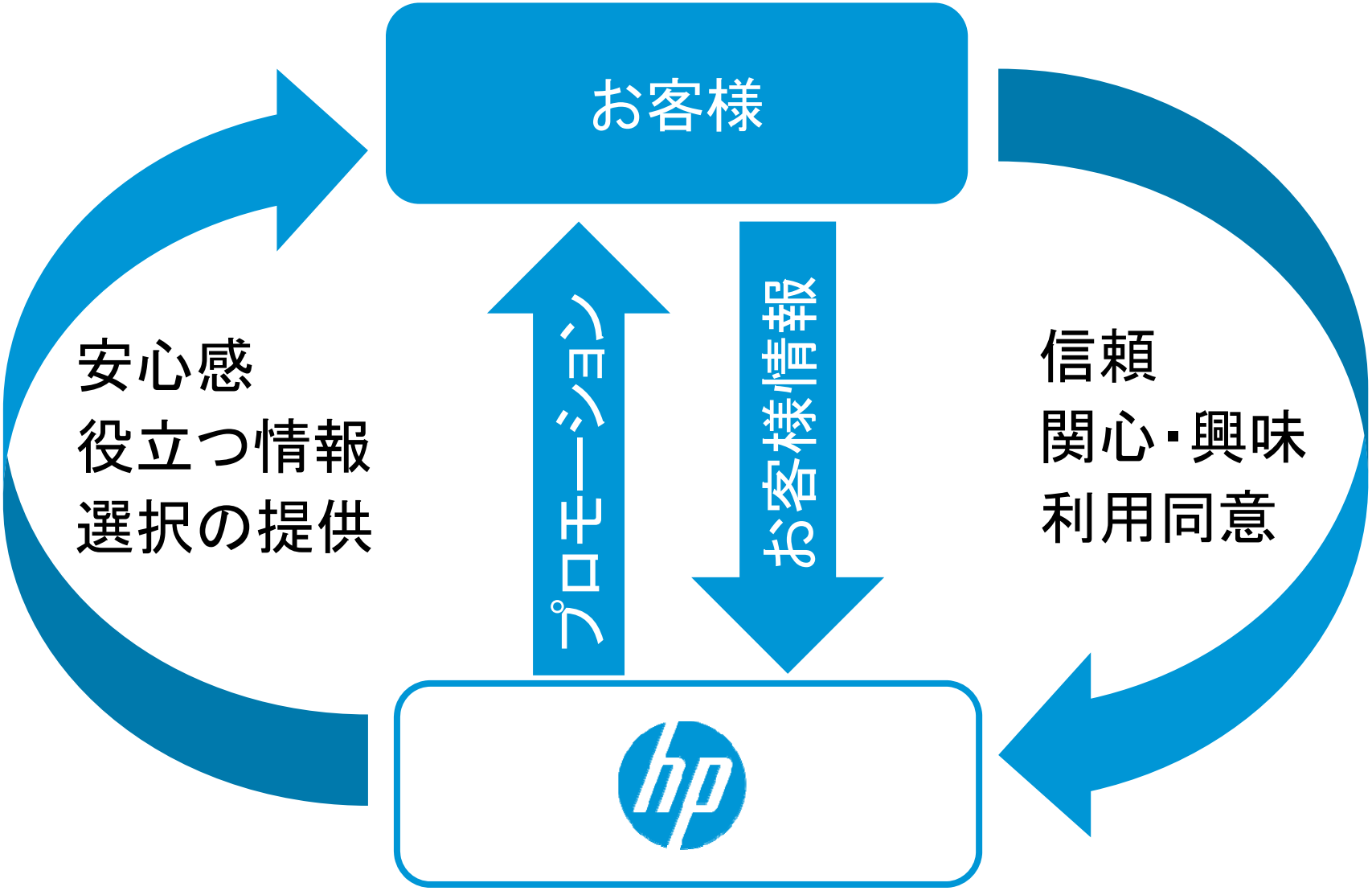
お客様情報を使ったプロモーション
データの廃棄・消去

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、静的なものではなく利用期限付き情報だという認識が必要。

まとめ

まとめ



まとめ

お客様情報をいただくとき

利用目的の記載

利用同意の取得

共催等の他社と連携するときには特に注意

お客様情報を使うとき

利用停止の対象者ではないことの事前確認

※部署単位だけでなく全社での確認も必要

利用停止したいと思われない連絡方法と内容

基本は、マナーの再確認、安心感に留意

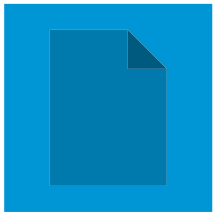
利用停止する準備

※部署単位だけでなく全社での停止にも備える

ガイドラインと問い合わせ先

ガイドライン
　@hp
　　個人情報保護
　　　ガイドライン

問い合わせ先
　@hp
　　個人情報保護
　　　お問い合わせ
　　　　CRM委員会委員



景品表示法トレーニング

2012年11月

日本ヒューレット・パッカード株式会社
法務・コンプライアンス統括本部

プロモーション業務に関する
その他のガイドライン

2012年11月

日本ヒューレット・パッカード株式会社

プロモーション業務に関するその他のガイドライン：
ブランディング

プロモーション業務をするときに知っておくべきガイドラインとしては、以下のようなものがあります。これらがすべてではないですが参考にしてください。

HPはHouse of brandsではなくBranded House

略

プロモーション業務に関するその他のガイドライン：ソーシャルメディア業務利用ガイドライン

HP Restricted

ソーシャルメディアを業務で利用する場合には、メディアごとに異なる手続きとトレーニング受講が必要です。

略

プロモーション業務トレーニング

おわり

2012年11月19日 REV1

日本ヒューレット・パッカード株式会社
CRM（カスタマ・リレーションシップ管理）委員会

ソーシャルメディアの
業務外利用ガイダンス

～思わぬトラブルに遭わないために～

日本ヒューレット・パッカード株式会社

2012年10月26日

ソーシャルメディアの業務外利用ガイダンスの作成方針

社員などの読者をしらけさせない

言い回し

・会社としてのリスク対策を前面に出した文章とせず、個人の被害予防を基本にする。それが結果的に会社業務にも影響することについては、くどくど書かずに、本人の想像力に委ねられることは委ねる。読者に「また何かの禁止事項か」「私生活にまで会社リスクの話しか」というように「しらけさせない」ことに留意する。

・疾病予防の注意喚起のような言い回しを心がける

例）「風邪の予防は油断大敵」とは書くが、

→「風邪で欠勤されると業務に支障がある」という書き方をしないのと同じ。

「感染症は他人への感染を防ぐため出社せず自宅療養を」とは書くが、

→「社内に感染させると業務に支障がある」という書き方をしないのと同じ。

開示範囲

以下の理由で、基本的に非機密情報として作成する

・正社員だけでなく、常駐非正社員や、非常駐の業務委託先への展開を視野に入れる

・事故発生時に会社の取り組みを示す必要が出た場合に、社外に開示できるものにする

（つづく）

ソーシャルメディアの業務外利用ガイダンスの作成方針
社員などの読者をしらけさせない
（つづき）

付加的な情報提供

疾病予防は言われなくても当然のこと。

風邪や感染症に自らなりたい人はいない。

そのような当たり前のことについて、付加的情報を収録する。

・「そんなこと知ってる」という情報だけではなく、

・「なるほど」「え？そんなこともあるのか」という気付きを与える情報を提供する。

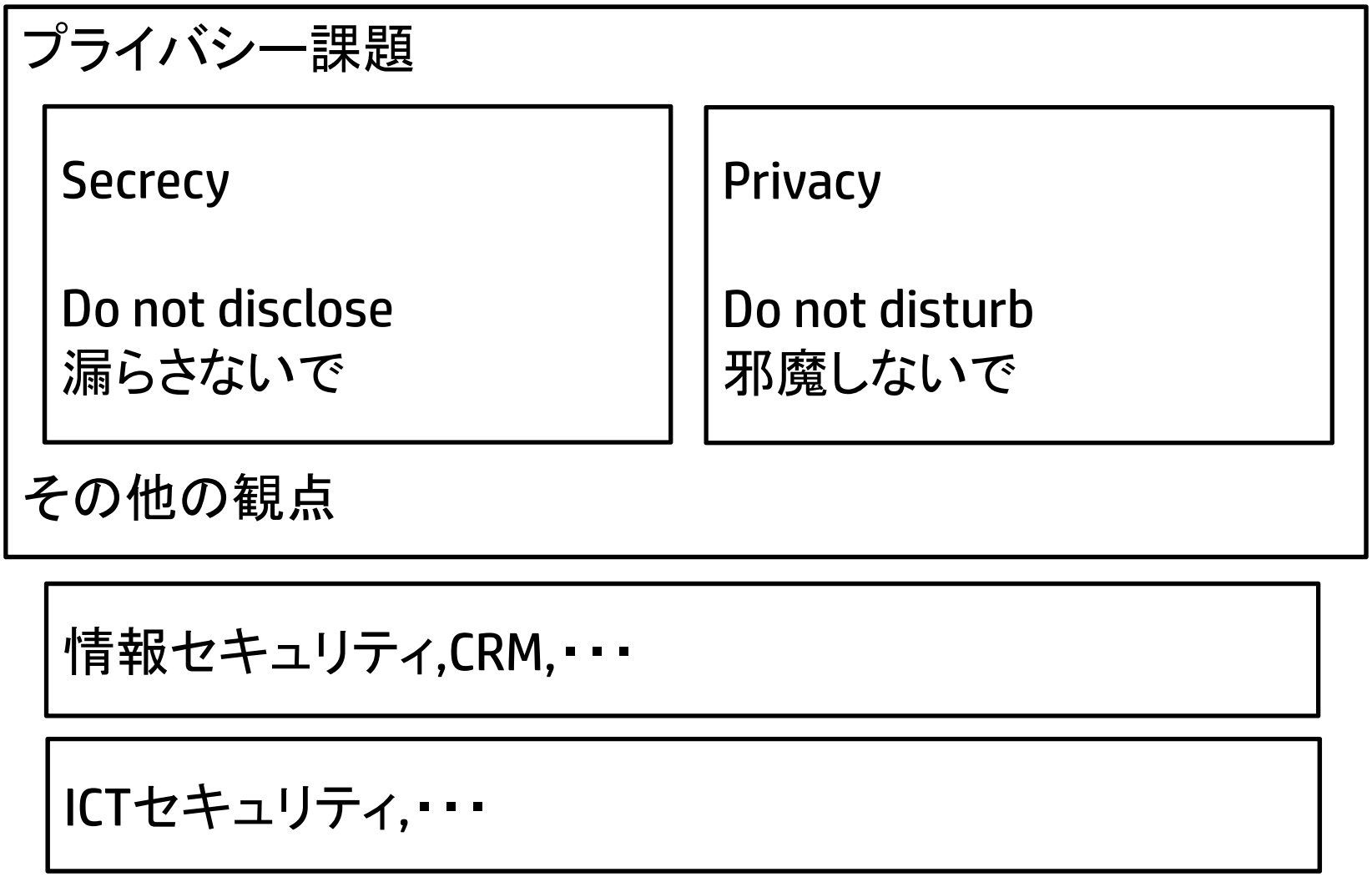
量的付加情報

・気付きにくい項目を紹介することによる、
注意点の網羅性向上のための付加的な情報提供

質的付加情報

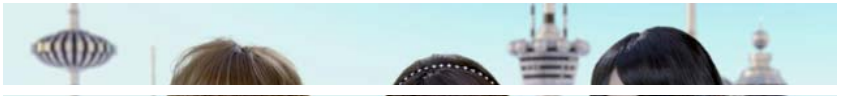
・気付いているはずの項目に対して具体的な被害状況を紹介することによる、
深刻さの理解度向上のための付加的な情報提供

プライバシー対策とセキュリティ対策の関係



プライバシー・バイ・デザイン

篠田 — 大島 — ？



国際規格動向

国際規格化の動向　http://bit.ly/jtc1sc27

ISO IEC/JTC 1/SC 27 Information technology -- Security techniques
WG5 Privacy, Identity management and Biometrics

プライバシー関連で発行されている規格

ISO/IEC 29100:2011 Privacy framework　→無料化を検討中

プライバシー関連で作成中の規格

ISO/IEC FDIS 29115 Entity authentication assurance framework (ITU-T X.1254)

ISO/IEC DIS 29191 Requirements for partially anonymous, partially unlinkable authentication

ISO/IEC CD 29101 Privacy architecture framework

ISO/IEC WD 29190 Privacy capability assessment model

ISO/IEC NP 27018 Code of practice for data protection controls for public cloud computing services

ISO/IEC NP 29134 Privacy impact assessment – Methodology

プライバシー関連で審議中の案件

SP on Privacy / Personal Information Management Systems (PIMS)

SP on Privacy impact assessment

SP on Study period on Privacy seal programs

SP on Documentation of data deletion principles

規格審議の協力者　絶賛　募集中です

SC27国際規格の審議は、研究者以外でも会費（年間1口70万円～）を払って規格賛助員になることで基本的にどなたでも参加できます。

情報処理学会情報規格調査会ホームページ
http://www.itscj.ipsj.or.jp/

参考：
SC27　WG5のプライバシー関連のいくつかの規格の意見交換
情報ネットワーク法学会プライバシー国際規格研究会
※SC27の未公表の審議内容を参照することはできません

いわゆる BYOD

弊社事例紹介

IT Initiative Day - HP Enterprise Security（2012年10月17日開催）

「モバイルとクラウドを最適化するHP社内IT環境の作られ方」

企業のIT環境を取り巻く課題として、新しい技術への対応を効果的かつ効率的に運用していく必要があります。これらの課題について弊社では、日頃お客様からのご要望に応じた個々の解決策の提案をしていますが、HP社の社内では、全体像をどう位置付けてIT 改革に取り組んでいるのかを、プロジェクト管理、クラウド技術の活用、BYODやソーシャルメディア利用などについて管理と技術の両面から具体的な事例を含めて紹介します。一般解ではありませんが、ある条件下での最適解の事例として参考にしていただければと思います。

資料・録音等

http://yosihiro.com/speech/#2012-10-17

目次

個人情報保護対策と情報セキュリティ対策
個人情報保護対策の弊社事例紹介
プライバシー・バイ・デザイン
国際規格動向
BYOD（参考情報紹介のみ）

発表資料のダウンロード

http://yosihiro.com/

お問い合わせ

twitter

http://twitter.com/4416sato