個人情報の利用と保護の実務

2012年2月20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
（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　元委員
その他
　http://yosihiro.com/profile/

発表内容

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

本日のスライド:
http://yosihiro.com/go/2012-02-20-aichi

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
- 個人情報の入手
- 個人情報の登録
- 個人情報の利用
- 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（←共用・共同利用）
- 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。

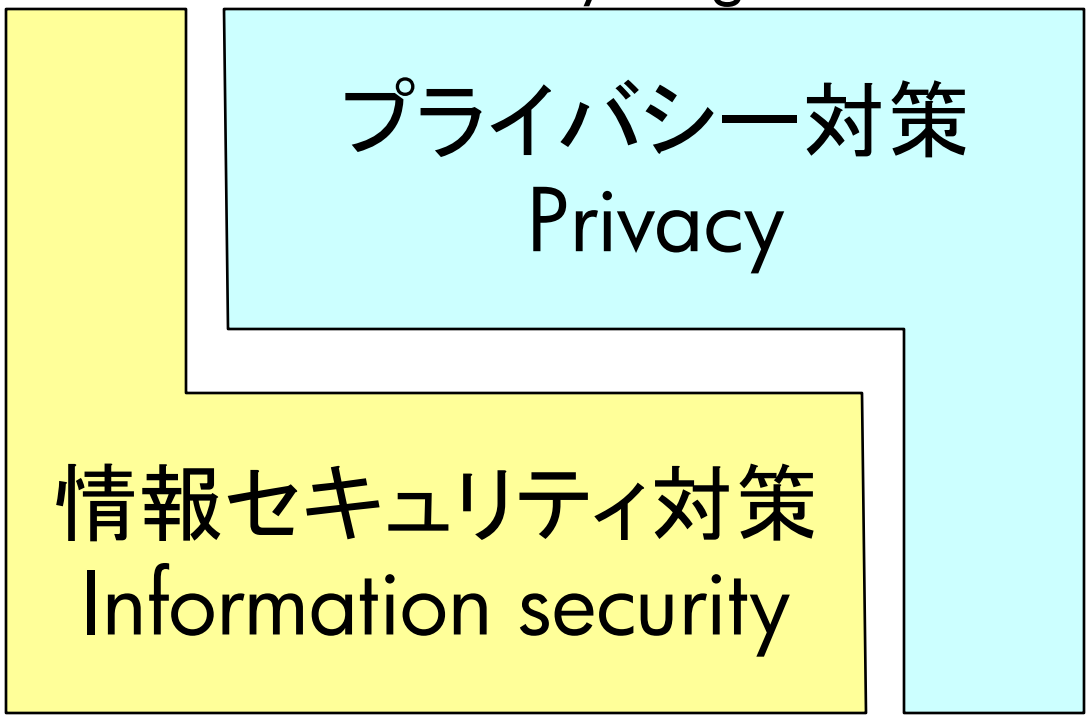
●私の邪魔をしないでください。

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



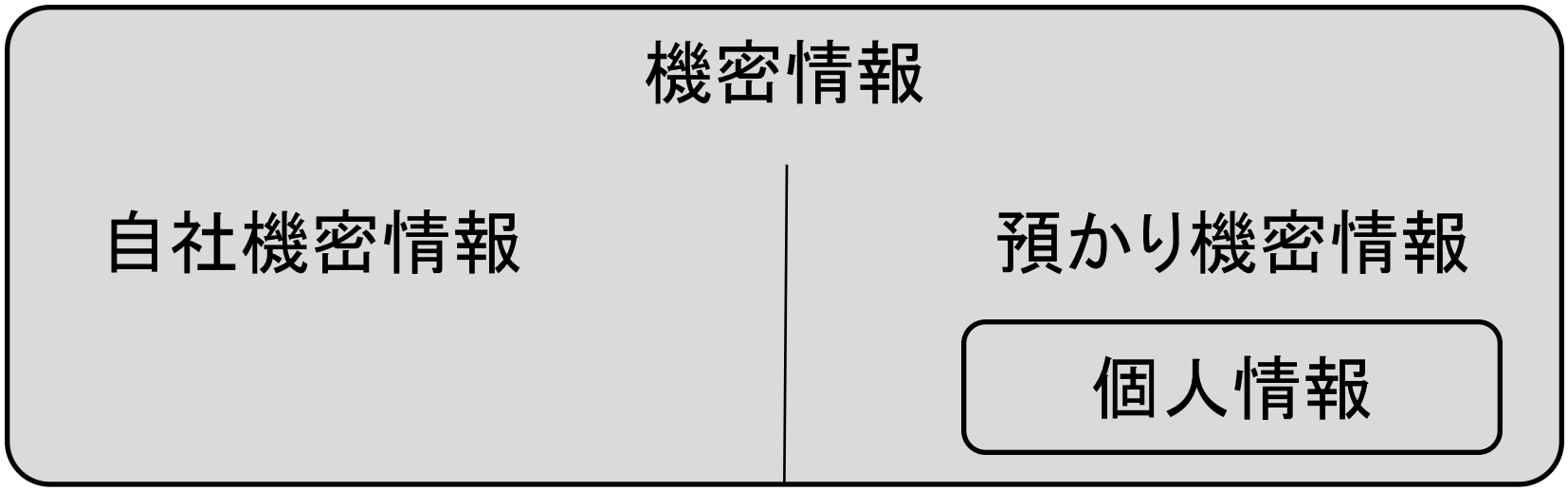
ビジネス目的
Business objective

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。

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。

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。

個人情報の安全管理措置

- 暗号化とパスワード保護
- 情報の通信や移送ー秘密分散

暗号化とパスワード保護の違い

- 質問：人に見られたくない物をしまうとしたら、どちら？
  ①ジュラルミンケースに、１桁の番号錠が付いている
  ②木箱に、５桁の番号錠が付いている

デモ

暗号化とパスワード保護の違い

・頑強な箱には、頑強な錠前を付けないと意味がない。

参考：「暗号化」と「暗号で保護する」を使い分ける
http://bit.ly/angou-de-hogo
http://yoshihiro.cocolog-nifty.com/postit/2006/09/post_e9f0.html

暗号化とパスワード保護の違い

パスワード設定のルール例
　８文字以上の英小文字、大文字、数字、記号の組合せ
　できれば12文字以上
　　12文字以上で手入力の場合、区切ると入力が容易
　　例）G!8T-X#3f-H8dU
　忘却しないための注意も必要
　　パスワードの記録は他人にわからない内容ならOK
　　語呂合わせにして、語呂を記載するなど
　　保管目的の重要なパスワードは記載して金庫に保管
ランダム生成ソフトの利用
　例） http://yosihiro.com/go/rpg

秘密分散の紹介

・機密情報の安全な保管・移送に有益な技術

秘密分散
例）1080という数字を分散する

単純：10と80に分割する
　→10か80を知られると半分の情報がわかってしまう
ちょっと複雑：1080を20x54に分割する
　→20か54を知られると、その倍数であることがわかってしまう

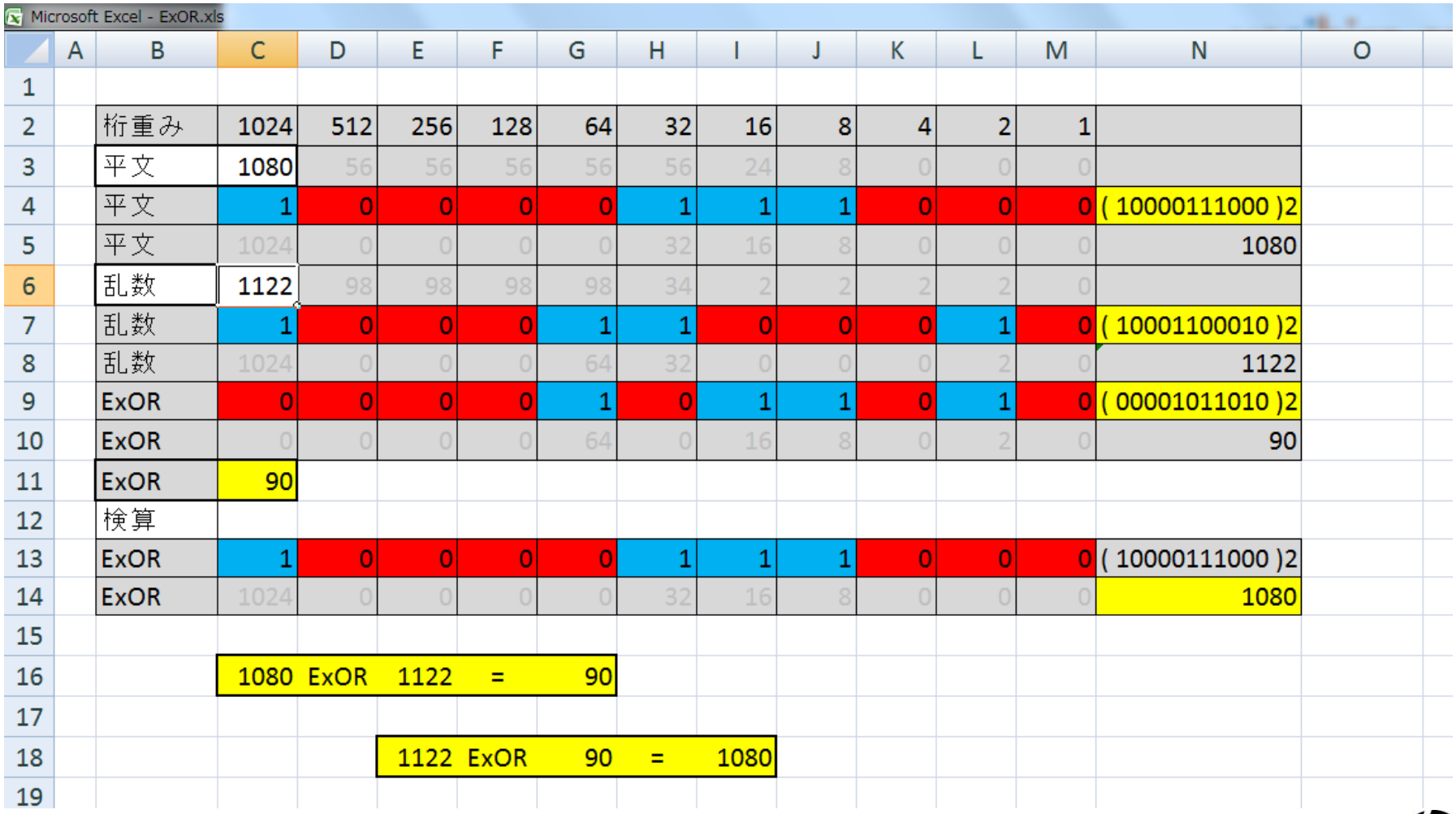
秘密分散の紹介

・機密情報の安全な保管・移送に有益な技術

秘密分散
例）1080という数字を分散する

実際には2進数にして排他的論理和という計算をします
排他的論理和(Exclusive OR, ExOR)の特性
A ExOR B = C ← Bを乱数にするとAがBとCに分散
B ExOR C = A ← BとCからAを復元できる

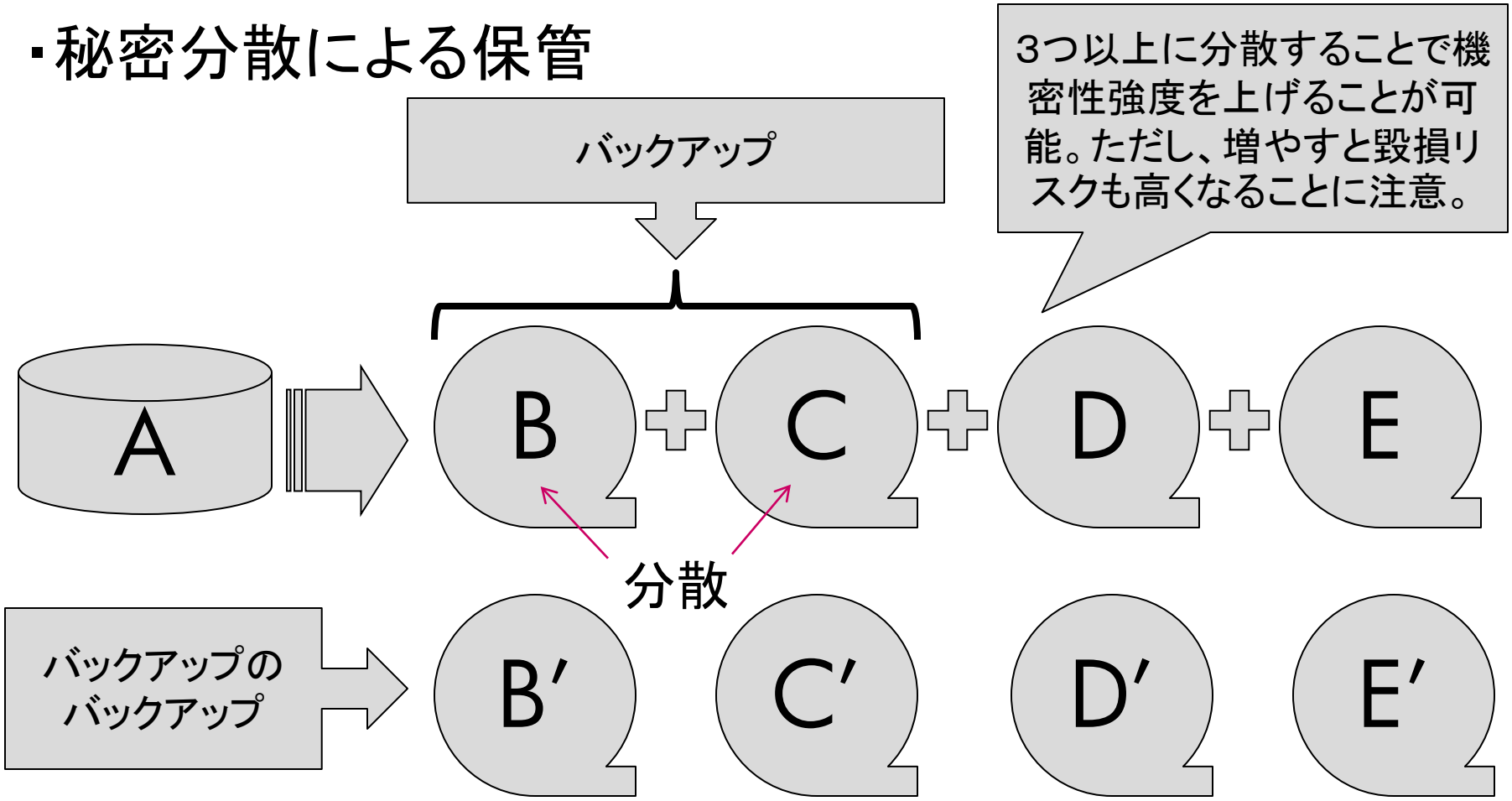
秘密分散の紹介



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2		桁重み	1024	512	256	128	64	32	16	8	4	2	1		
3		平文	1080	56	56	56	56	56	24	8	0	0	0		
4		平文	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
5		平文	1024	0	0	0	0	32	16	8	0	0	0	1080	
6		乱数	1122	98	98	98	98	34	2	2	2	2	0		
7		乱数	1	0	0	0	1	1	0	0	0	1	0	(10001100010)2	
8		乱数	1024	0	0	0	64	32	0	0	0	2	0	1122	
9		ExOR	0	0	0	0	1	0	1	1	0	1	0	(00001011010)2	
10		ExOR	0	0	0	0	64	0	16	8	0	2	0	90	
11		ExOR	90												
12		検算													
13		ExOR	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
14		ExOR	1024	0	0	0	0	32	16	8	0	0	0	1080	
15															
16			1080 ExOR 1122 = 90												
17															
18					1122 ExOR 90 = 1080										
19															

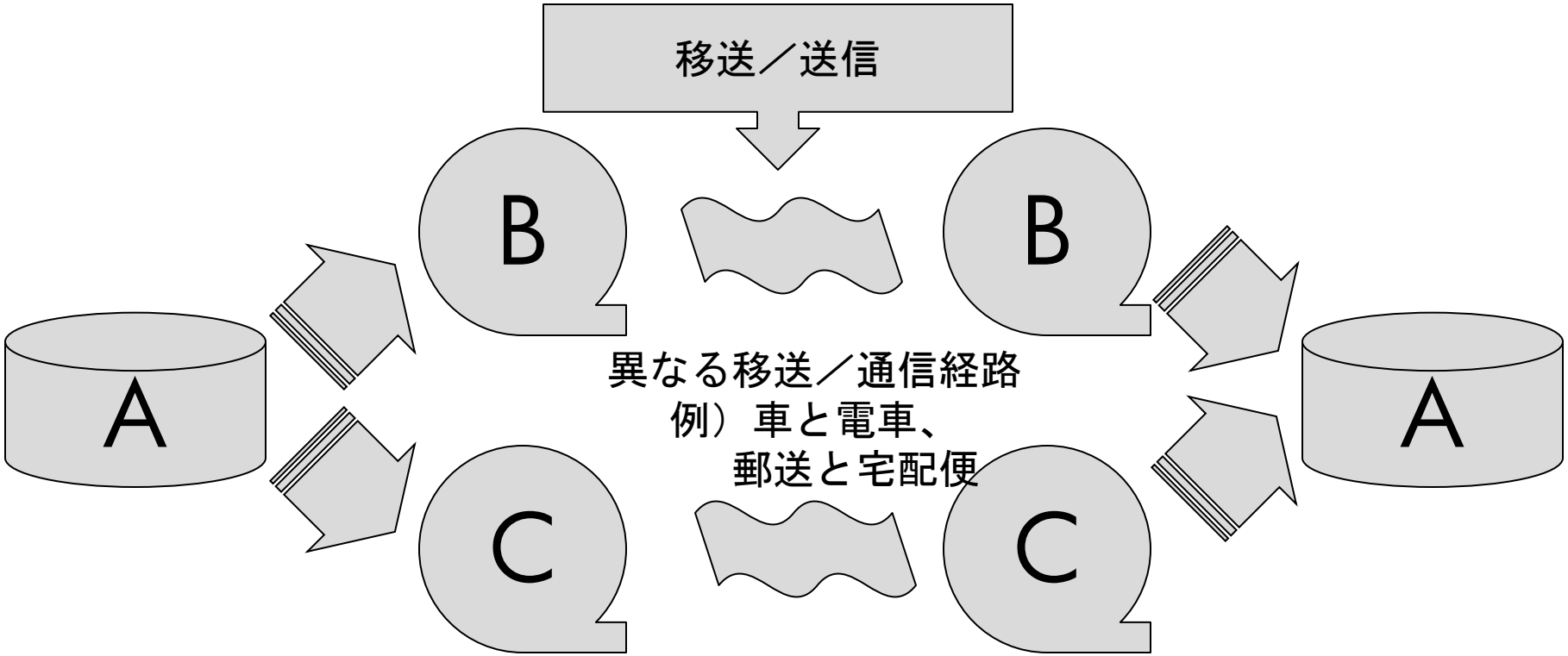
秘密分散の紹介

- 秘密分散による保管



秘密分散の紹介

・秘密分散による移送／送信



Bの安全な移送／送信完了を待ってから
Cを移送／するのが望ましい→同じ経路も検討可

秘密分散の紹介
機密ファイルの移送の具体的手順

・作業用PCで機密ファイルを秘密分散ソフトを使って、FILE-AとFILE-Bに分散する。
・作業用PC上の機密ファイルを抹消ソフトで抹消する。
・FILE-AとFILE-Bをそれぞれ CD-Rに書き込む。
・FILE-Aを移送する。
・FILE-Aの移送が完了してから、FILE-Bを移送する。
・到着地の作業用PCでFILE-AとFILE-Bを使って機密ファイルを復元する。
・2枚のCD-Rは到着地で破壊する。
・移送先で機密ファイルの保管ができたら、作業用PC上のすべてのファイルを抹消ソフトで抹消する。

秘密分散の紹介
機密ファイルの移送の具体的手順

・作業用PCで機密ファイルを秘密分散ソフトを使って、FILE-AとFILE-Bに分散する。
・FILE-AとFILE-Bをそれぞれ CD-Rに書き込む。
・作業用PC上の機密ファイル、FILE-A、FILE-Bを抹消ソフトで抹消する。
・FILE-Aを移送する。
・FILE-Aの移送が完了してから、FILE-Bを移送する。
・移送先のPCでFILE-AとFILE-Bを使って機密ファイルを復元する。
・2枚のCD-Rは移送先で破壊する。（破壊してもらう。）

秘密分散の紹介
機密ファイルの移送の具体的手順（PCを持参）

・作業用PCで機密ファイルを秘密分散ソフトを使って、FILE-AとFILE-Bに分散する。
・FILE-AだけをCD-Rに書き込む。
・作業用PC上の機密ファイルとFILE-Aを抹消ソフトで抹消する。
・FILE-Aを移送する。
・FILE-Aの移送が完了してから、作業用PCを持参する。
・移送先に持参した作業用PCでCD-RにあるFILE-AとPC内にあるFILE-Bを使って機密ファイルを復元し、提出する。
・FILE-AのCD-Rは移送先で破壊する。
・移送先で作業用PC上のFILE-Bを抹消ソフトで抹消する。

発表内容

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

本日のスライド:
http://yosihiro.com/go/2012-02-20-aichi