JAPiCO
一般社団法人 日本個人情報管理協会

オフィス四々十六

個人情報保護対策と情報セキュリティ対策の共通点と相違点

2017年3月9日

佐藤　慶浩

発表者紹介

佐藤慶浩（さとう　よしひろ）
フリーランス・コンサルタント

オフィス四々十六（ししじゅうろく）　代表
一般社団法人　日本個人情報管理協会（JAPiCO）理事
一般財団法人　日本情報経済社会推進協会（JIPDEC）客員研究員

元　株式会社 日本HP アジア地域プライバシーオフィサー
元　日本ヒューレット・パッカード株式会社　ITセキュリティソリューション事業部アジア地域マネージャ
元　内閣官房情報セキュリティセンター（NISC）　内閣情報セキュリティ指導専門官（民間併任）

【その他】　**https://よしひろ.com/profile/**

発表内容

JIS Q 15001に基づく個人情報保護マネジメントシステムにおいて、情報セキュリティ対策をどのように位置づけて連携していくのかについてご説明いたします。

【1】個人情報保護対策と情報セキュリティ対策の違い

【2】両対策の連携方法

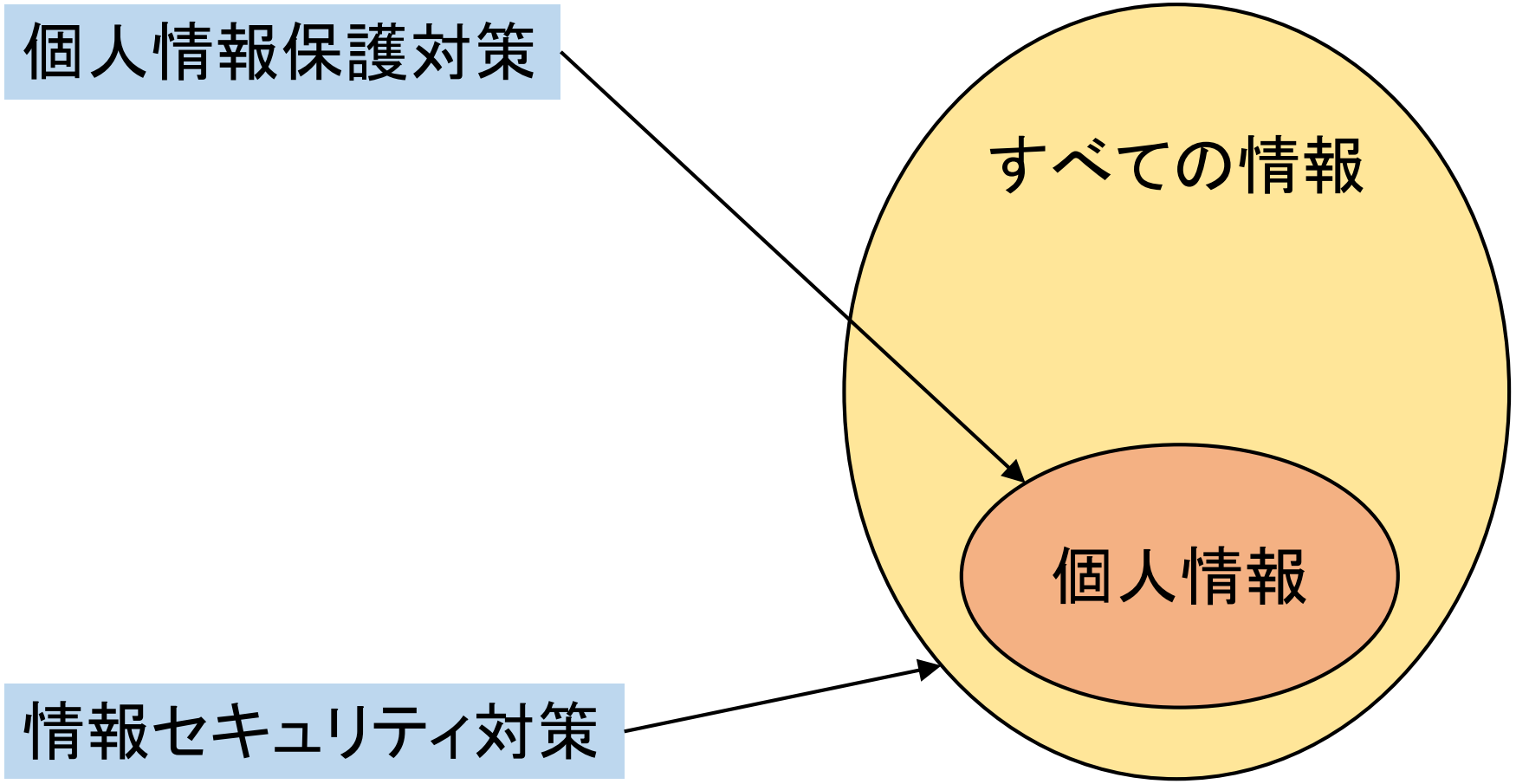
【3】個人情報保護マネジメントシステムの計画

【１】
個人情報保護対策と情報セキュリティ対策の違い

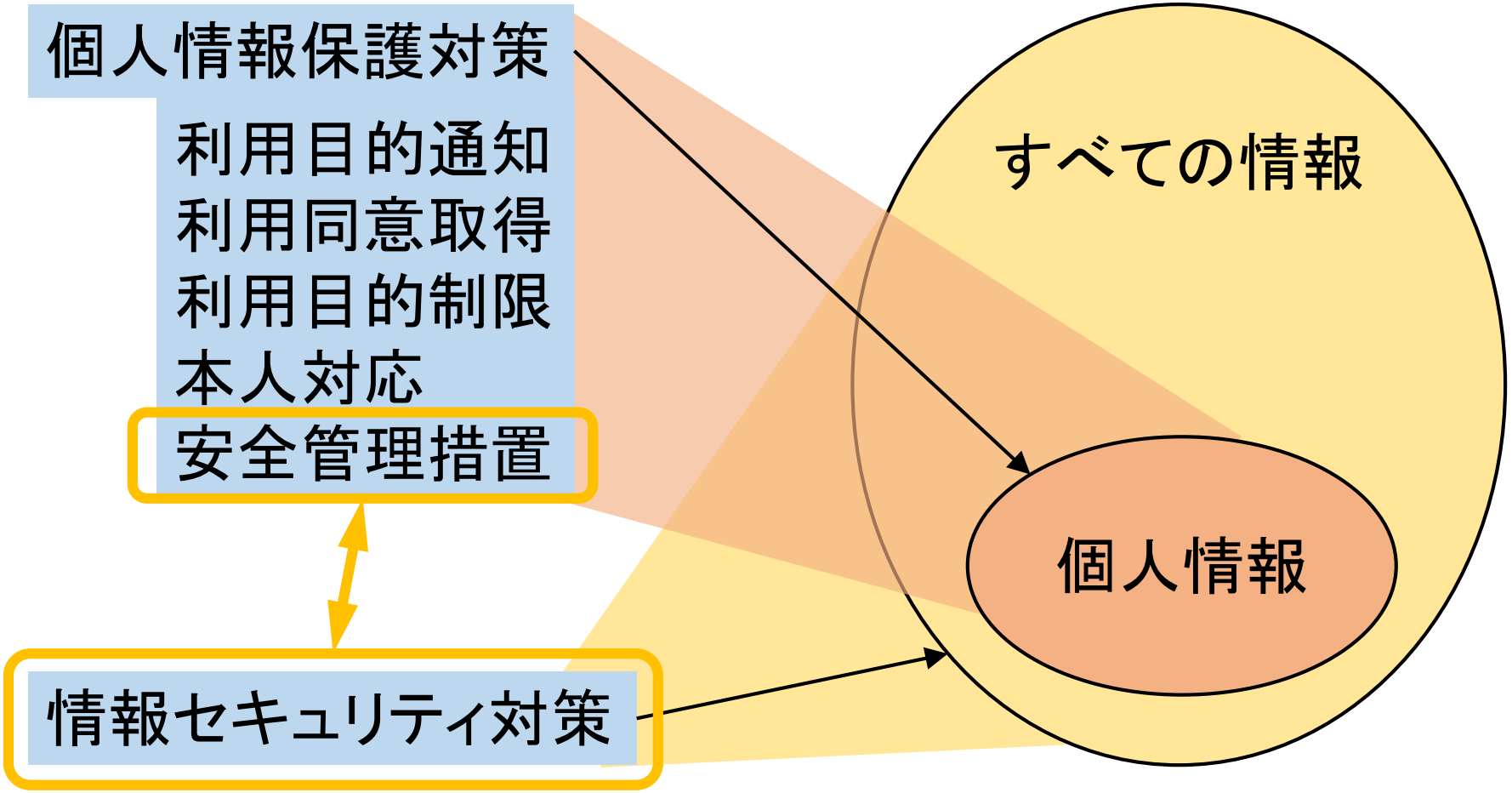
【２】
両対策の連携方法

【３】
個人情報保護マネジメントシステムの計画

対策する対象情報の違い



対策する内容の違い



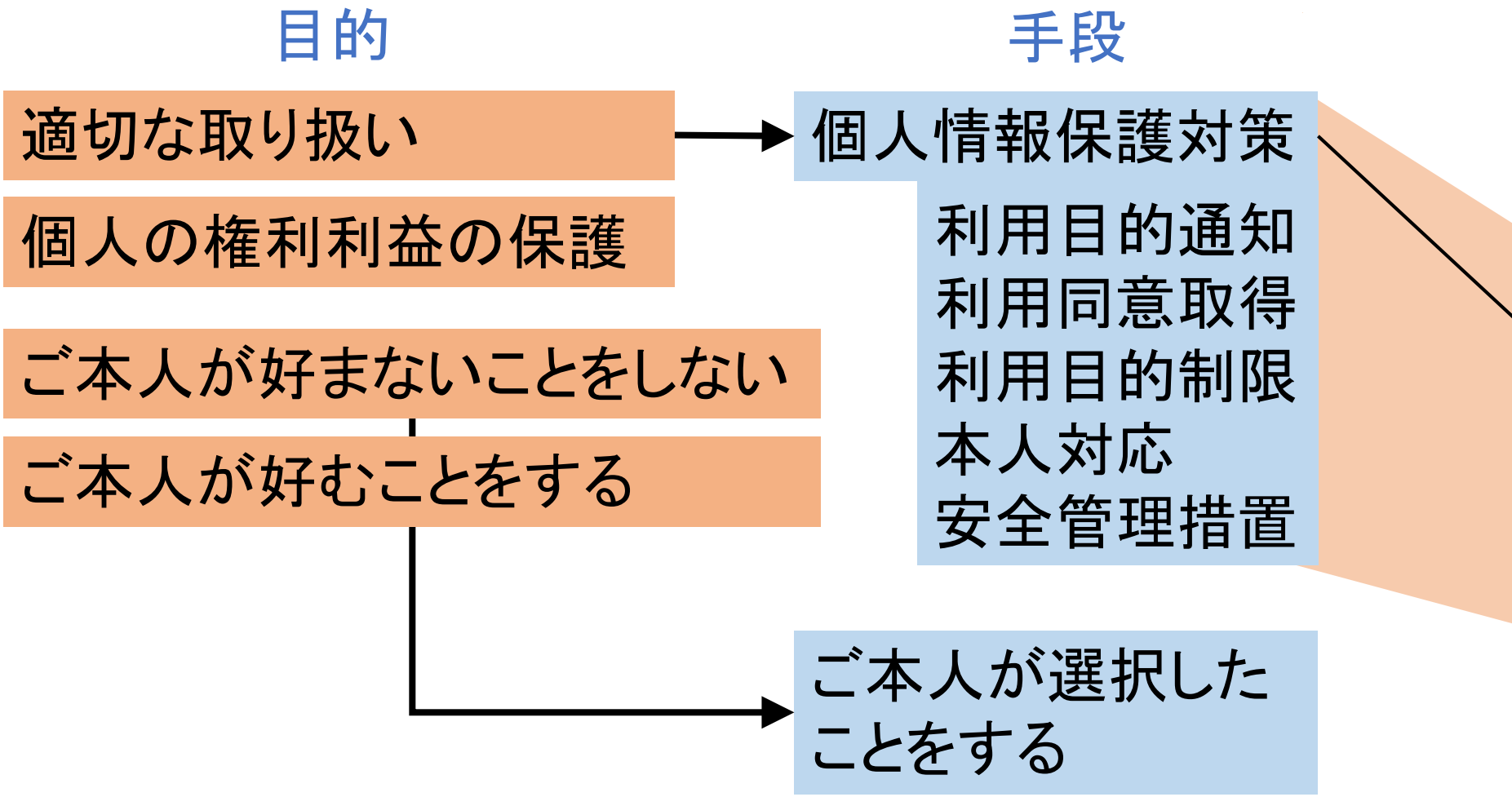
対策する目的の違い

目的	手段
適切な取り扱い 個人の権利利益の保護	個人情報保護対策 利用目的通知 利用同意取得 利用目的制限 本人対応 安全管理措置
機密性・完全性・可用性の維持	情報セキュリティ対策

個人情報保護対策の目的

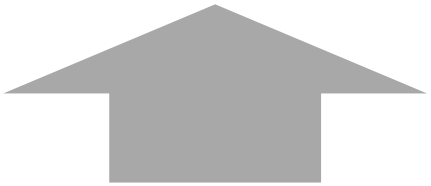
目的	手段
適切な取り扱い 個人の権利利益の保護	個人情報保護対策 利用目的通知 利用同意取得 利用目的制限 本人対応 安全管理措置
ご本人が好まないことをしない ご本人が好むことをする	
機密性・完全性・可用性の維持	情報セキュリティ対策

個人情報保護対策の目的を実現する手段



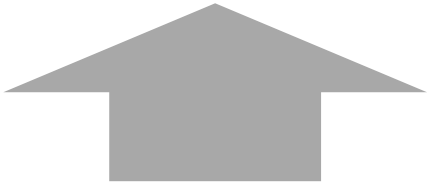
ご本人が好まないこと･･･とは？

ご本人をXXにしない　　･････自主的な目標



ご本人を不安にさせない　　改正法の

→　情報取得制限･････要配慮個人情報要件



ご本人を邪魔しない

→　利用目的制限･････法律上の最低水準

同意取得方式の区別

明示的同意取得（デフォルトオフ方式）

同意についての何らかの行為を求めて、その行為があった場合に限って同意を取得したと判定する

例）同意するなら、□にチェックを記入してください。

□　同意する

暗黙的同意取得（デフォルトオン方式）

同意しないための何らかの行為を求めて、その行為がなかった場合に限って同意を取得したと判定する

例）同意しないなら、□にチェックを記入してください。

□　同意しない

例）同意しますか？

☑　はい　　□　いいえ

表 3　明示的または暗黙的同意取得の特徴

同意取得方式	長所	短所
明示的同意取得方式	• 初期の同意取得状態が安定する • プライバシー対策に誠実な印象を与える	• 同意取得率が低くなる • 実際には不同意の意思がないのに見落としによって不同意になる
暗黙的同意取得方式	• 初期の同意取得率が高くなる • 確認画面が簡潔な印象を与える	• 事後の不同意が発生する • そもそも同意したつもりはなかったというトラブルが発生する

表 4　明示的または暗黙的方式を区別した同意状態値の例

同意状態値	同意状態の意味
Y （大文字 Yes）	明示的同意： 明示的に同意を確認した結果，同意を選択した
y （小文字 yes）	暗黙的同意： 暗黙的に同意を確認した結果，不同意を選択しなかった
N （No）	不同意： 同意を確認した結果，不同意を選択した
U （Unkown）	未確認： 同意をいまだ確認していないまたは同意を確認した結果，同意も不同意も選択しなかった

メディア・パーミッションとコンテンツ・パーミッション

同意取得の細分化の例

メディア・パーミッション

連絡先情報のどの項目を使って、どのメディアで連絡をするのか

- 住所を使った郵送の利用同意
- 電話番号を使った電話の利用同意
- メールアドレスを使ったメール配信の利用同意

コンテンツ・パーミッション

連絡先に、どのような内容（コンテンツ）の連絡をするのか？

- パソコン製品のご紹介
- プリンタ製品のご紹介
- 顧客満足度調査のお願い

同意事項と同意状態値の例

表6：ご連絡先に弊社製品のご案内をしてよいですか？→はい
表7：弊社パソコン関連のご案内をメール配信してよいですか？→はい
表7→表8：プリンタ関連案内を郵送→プリンタ関連案内の郵送は不要という反応
表9：弊社プリンタ関連のご案内を郵送してよいですか？→はい

表 6　同意事項と同意状態値の例（1）

同意事項		同意状態値
メディア	住所	Y
	電話番号	Y
	メールアドレス	Y
コンテンツ	パソコン関連ニュース	Y
	プリンタ関連ニュース	Y

表 8　同意事項と同意状態値の例（3）

同意事項		同意状態値
メディア	住所	N
	電話番号	U
	メールアドレス	Y
コンテンツ	パソコン関連ニュース	Y
	プリンタ関連ニュース	N

表 7　同意事項と同意状態値の例（2）

同意事項		同意状態値
メディア	住所	U
	電話番号	U
	メールアドレス	Y
コンテンツ	パソコン関連ニュース	Y
	プリンタ関連ニュース	U

表 9　同意事項と同意状態値の例（4）

同意事項		同意状態値
メディア	住所	Y
	電話番号	U
	メールアドレス	U
コンテンツ	パソコン関連ニュース	U
	プリンタ関連ニュース	Y

顧客情報管理データベースのテーブルの例

表 12　顧客情報管理データベースのテーブルの例

ID	氏名	住所	電話番号	メールアドレス	取得日時 更新日時	取得状況	同意状態値					地域	隔離フラッグ
							メディア・パーミッション			コンテンツ・パーミッション			
							住所	電話番号	メールアドレス	パソコン関連ニュース	プリンタ関連ニュース		
01	鈴木一郎	○○	03～	suzuki@ example.com	2001/2/3	A12345	Y	Y	Y	Y	Y	日本	
02	佐藤二郎	○○	03～	sato@ example.net	2002/3/4 2013/7/8	B34567 E76543	U	U	Y	U	Y	日本	
03	田中花子	○○	06～	hanako@ example.org	2003/4/5	A12345	Y	N	U	Y	Y	日本	
04	高橋三郎	○○	06～	takahashi@ example.jp	2004/5/6 2013/9/10 2014/3/2	C23456 G87654 H01234	Y	N	Y	U	U	日本	
05	山本愛子	○○	03～	aiko@ example.net	2005/6/7 2013/7/8	D45678 E76543	N	N	N	N	N	日本	オン
06	John Smith	△△	1234	john@ example.edu	2010/9/8	Z98765	U	U	U	U	U	US	

表1と表2に照合して取得状況と通知した利用目的を必要時に確認する

データ汚染時に部分的な除染ができる

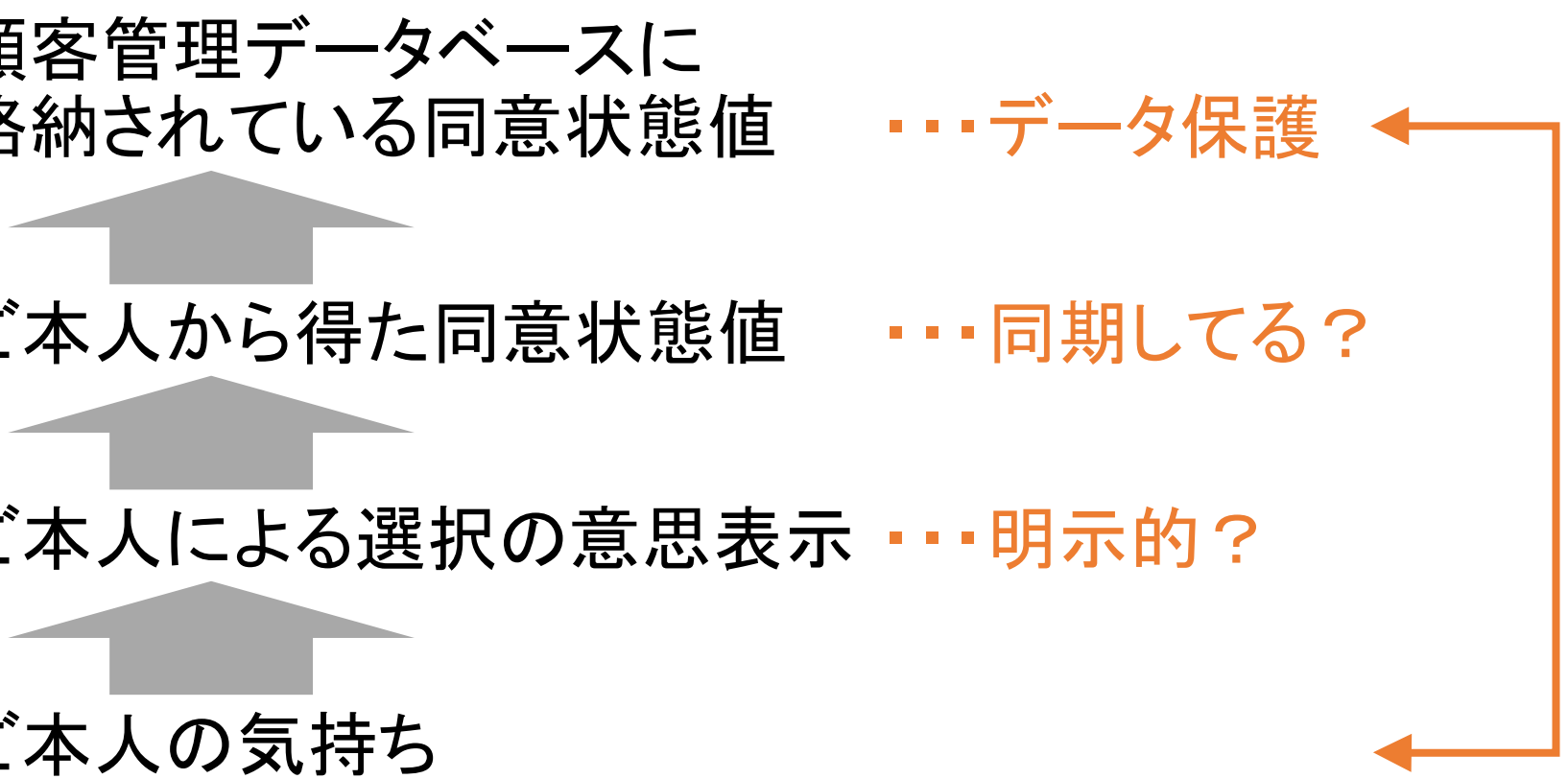
表3～9に基づいて同意状態値を保持する

表11に基づいて同意状態値を更新する

表10に照合してデータ利用の可否を判断する

削除の代替

ご本人が好んでいること



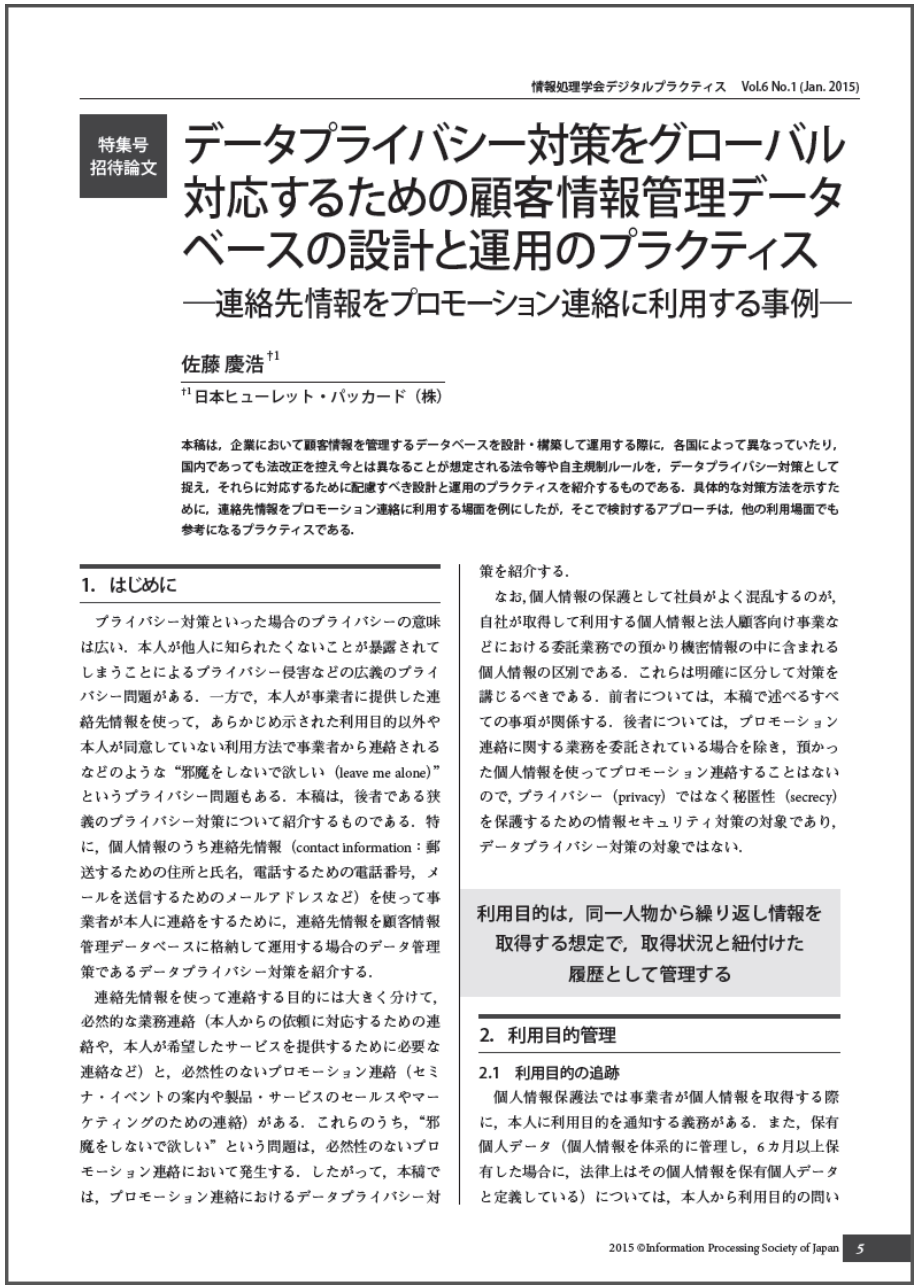
【参考資料】

情報処理学会
デジタルプラクティス
Vol.6 No.1 (Jan.2015)

デジタルプラクティス　検索

招待論文

データプライバシー対策をグローバル対応するための顧客情報管理データベースの設計と運用のプラクティス



情報処理学会デジタルプラクティス　Vol.6 No.1 (Jan. 2015)

特集号
招待論文

データプライバシー対策をグローバル対応するための顧客情報管理データベースの設計と運用のプラクティス

―連絡先情報をプロモーション連絡に利用する事例―

佐藤 慶浩[†1]
[†1]日本ヒューレット・パッカード（株）

本稿は，企業において顧客情報を管理するデータベースを設計・構築して運用する際に，各国によって異なっていたり，国内であっても法改正を控え今とは異なることが想定される法令等や自主規制ルールを，データプライバシー対策として捉え，それらに対応するために配慮すべき設計と運用のプラクティスを紹介するものである．具体的な対策方法を示すために，連絡先情報をプロモーション連絡に利用する場面を例にしたが，そこで検討するアプローチは，他の利用場面でも参考になるプラクティスである．

1. はじめに

プライバシー対策といった場合のプライバシーの意味は広い．本人が他人に知られたくないことが暴露されてしまうことによるプライバシー侵害などの広義のプライバシー問題がある．一方で，本人が事業者に提供した連絡先情報を使って，あらかじめ示された利用目的以外や本人が同意していない利用方法で事業者から連絡されるなどのような“邪魔をしないで欲しい（leave me alone）”というプライバシー問題もある．本稿は，後者である狭義のプライバシー対策について紹介するものである．特に，個人情報のうち連絡先情報（contact information：郵送するための住所と氏名，電話するための電話番号，メールを送信するためのメールアドレスなど）を使って事業者が本人に連絡をするために，連絡先情報を顧客情報管理データベースに格納して運用する場合のデータ管理策であるデータプライバシー対策を紹介する．

連絡先情報を使って連絡する目的には大きく分けて，必然的な業務連絡（本人からの依頼に対応するための連絡や，本人が希望したサービスを提供するために必要な連絡など），必然性のないプロモーション連絡（セミナ・イベントの案内や製品・サービスのセールスやマーケティングのための連絡）がある．これらのうち，“邪魔をしないで欲しい”という問題は，必然性のないプロモーション連絡において発生する．したがって，本稿では，プロモーション連絡におけるデータプライバシー対策を紹介する．

なお，個人情報の保護として社員がよく混乱するのが，自社が取得して利用する個人情報と法人顧客向け事業などにおける委託業務での預かり機密情報の中に含まれる個人情報の区別である．これらは明確に区分して対策を講じるべきである．前者については，本稿で述べるすべての事項が関係する．後者については，プロモーション連絡に関する業務を委託されている場合を除き，預かった個人情報を使ってプロモーション連絡することはないので，プライバシー（privacy）ではなく秘匿性（secrecy）を保護するための情報セキュリティ対策の対象であり，データプライバシー対策の対象ではない．

利用目的は，同一人物から繰り返し情報を取得する想定で，取得状況と紐付けた履歴として管理する

2. 利用目的管理

2.1 利用目的の追跡

個人情報保護法では事業者が個人情報を取得する際に，本人に利用目的を通知する義務がある．また，保有個人データ（個人情報を体系的に管理し，6カ月以上保有した場合に，法律上はその個人情報を保有個人データと定義している）については，本人から利用目的の問い

【参考資料】

経済産業省
Ministry of Economy, Trade and Industry

商務情報政策局　情報経済課

平成26年10月17日(金)

「オンラインサービスにおける消費者のプライバシーに配慮した情報提供・説明のためのガイドライン」

http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html

概要

経済産業省では、パーソナルデータの利活用に当たって重要な消費者と事業者の間の信頼関係の構築を促進するため、平成25年度にパーソナルデータの取得時における消費者への情報提供・説明を充実させるための「評価基準」を取りまとめ、公表しました。

今般、経済活動のグローバル化の進展を踏まえ、この「評価基準」を、国際的にサービスを展開する事業者の参考に資するものとすべく、「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」を取りまとめました。本ガイドラインの国際規格化に向けて取組んでいきます。

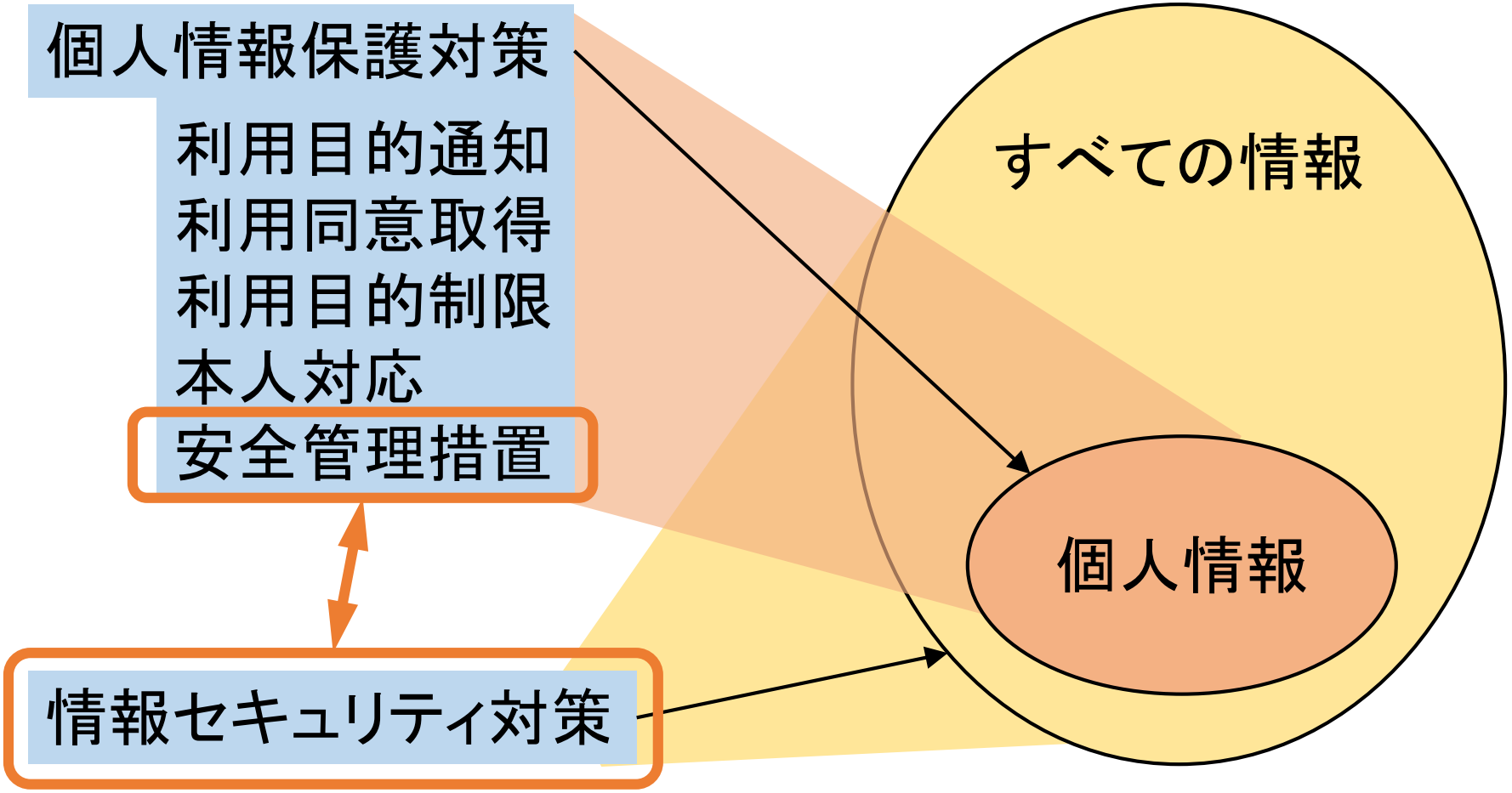
ISO/IEC 29184 Guidelines for online privacy notice and consent

【１】
個人情報保護対策と情報セキュリティ対策の違い

【２】
両対策の連携方法

【３】
個人情報保護マネジメントシステムの計画

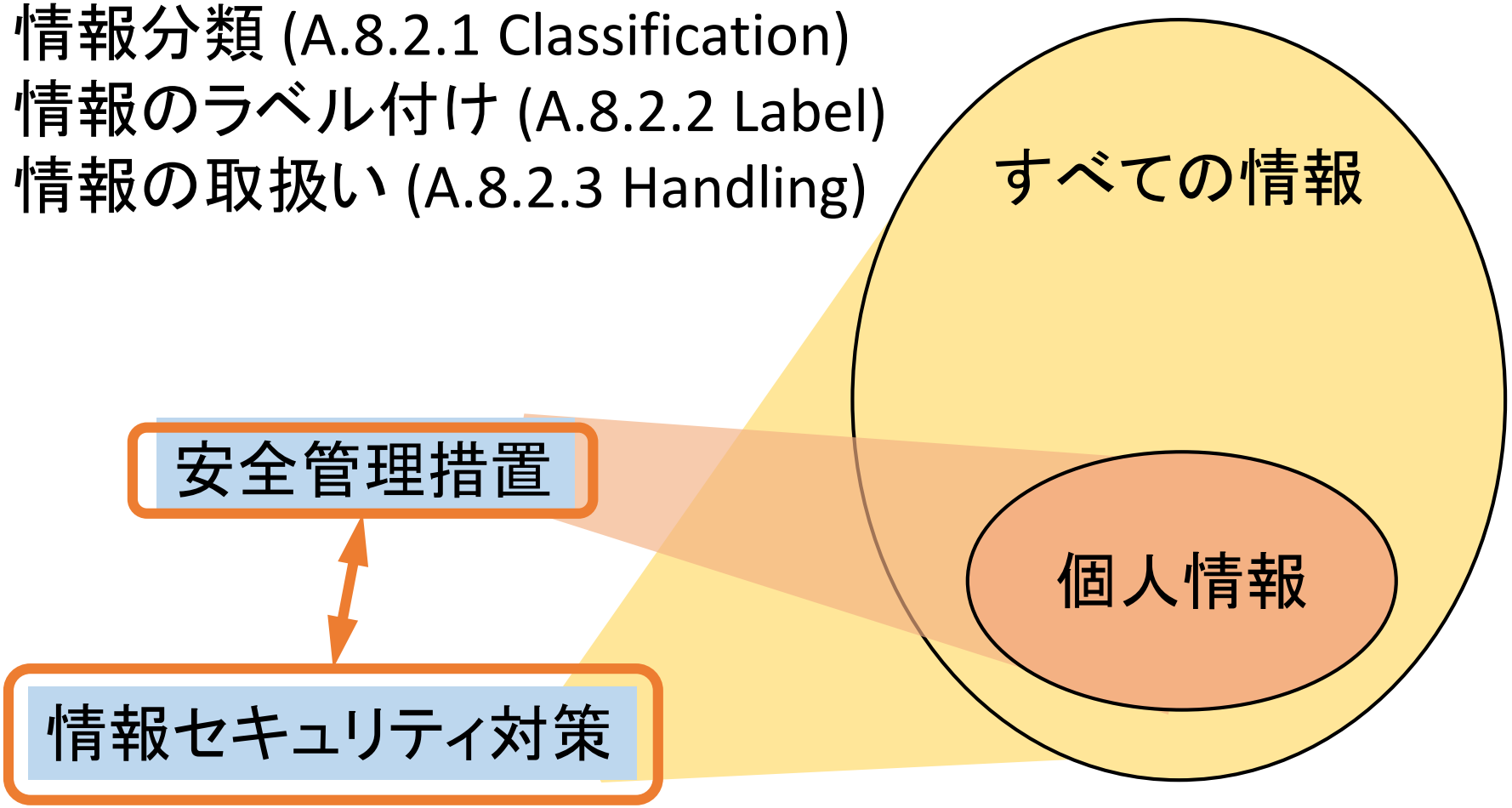
対策する内容の違い



個人情報安全管理措置と情報セキュリティ対策

JIS Q 27001:2014(ISO/IEC 27001:2013)

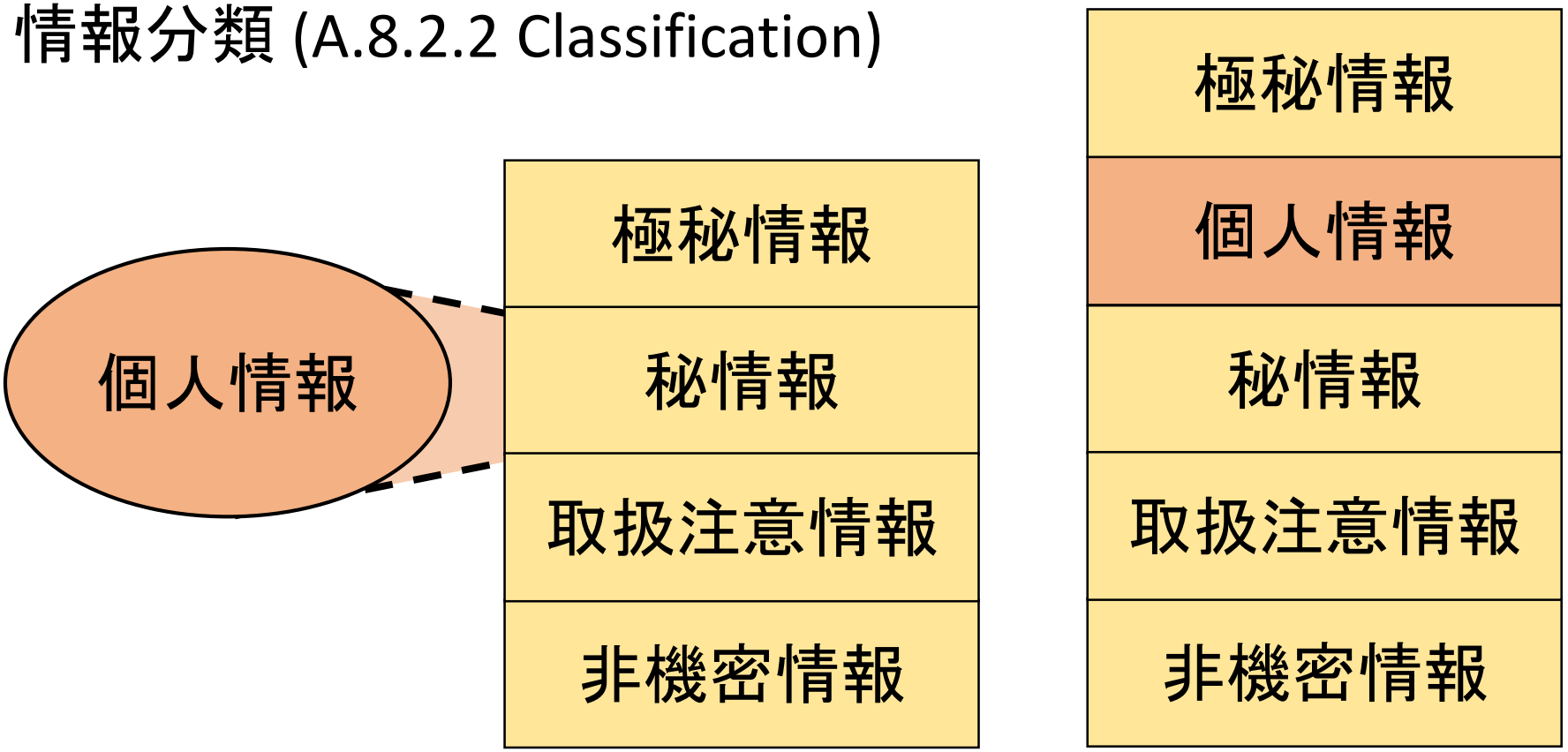
情報分類 (A.8.2.1 Classification)
情報のラベル付け (A.8.2.2 Label)
情報の取扱い (A.8.2.3 Handling)



個人情報安全管理措置と情報セキュリティ対策

JIS予定なし (ISO/IEC 29151:2017発行予定)

情報分類 (A.8.2.2 Classification)



既存対応方式

新規作成方式

個人情報安全管理措置と情報セキュリティ対策

JIS予定なし (ISO/IEC 29151:2017発行予定)

情報分類 (A.8.2.2 Classification)

情報のラベル付け (A.8.2.3 Label)

8.2.3 Labelling of Information

Implementation guidance for the protection of PII

発表時点で未発行の規格文書のため
規格文章については不掲載です

個人情報安全管理措置と情報セキュリティ対策

JIS予定なし (ISO/IEC 29151:2017発行予定)
情報分類 (A.8.2.2 Classification)
情報のラベル付け (A.8.2.3 Label)
情報の取扱い (A.8.2.4 Handling)

8.2.4 Handling of assets
Implementation guidance for the protection of PII

発表時点で未発行の規格文書のため
規格文章については不掲載です

機密保持契約書と個人情報保護契約書の違い

一般的な契約書の例であって、実際には契約条文によって決まります。

	機密保持契約書	個人情報保護契約書
対象情報の特定	機密情報の特定は情報提供者の責任	個人情報の特定は情報受領者の責任
受容リスクの判断	対策の受容リスクは委託先が判断する	対策の受容リスクは委託元が判断する
契約締結日	契約締結日をさかのぼることができる場合がある	契約締結日はさかのぼることができない場合がある

※特定の容易性、ワークフローの自由度、利用継続性

【１】
個人情報保護対策と情報セキュリティ対策の違い

【２】
両対策の連携方法

【３】
個人情報保護マネジメントシステムの計画

個人情報保護マネジメントシステム

マネジメントシステム

→　継続的な改善

→　計測できないものは改善できない

個人情報保護マネジメントとしての計測指標

例）

利用同意率の向上　　Opt-in rate

利用停止率の軽減　　Opt-out rate

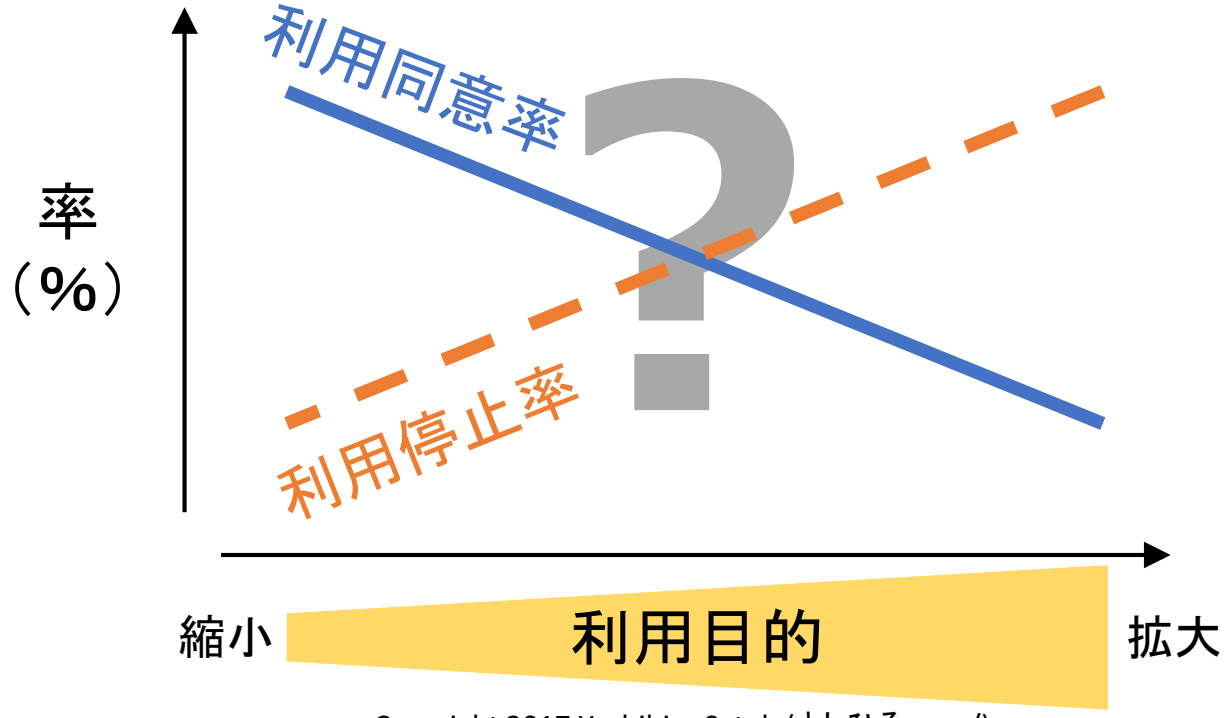
利用目的の拡大

→　方針に基づく目標設定

個人情報保護マネジメントの計測指標

利用同意率の向上
利用停止率の軽減
利用目的の拡大

方針に基づく目標設定
↓
仮説と検証による目標改善



個人情報保護マネジメントシステム

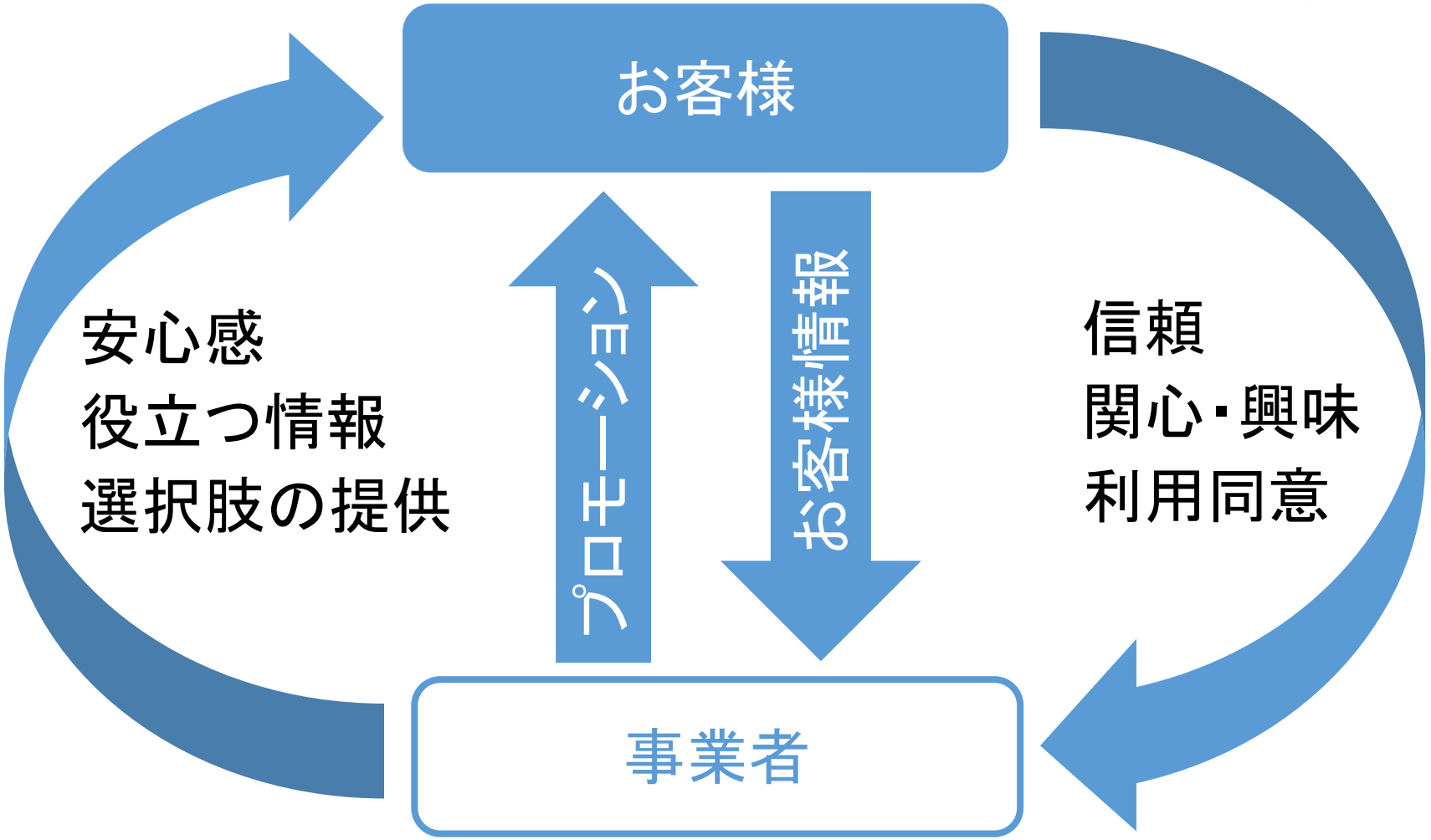
方針に影響を与える要素

- マス・マーケティング／ダイレクト・マーケティング
- その他

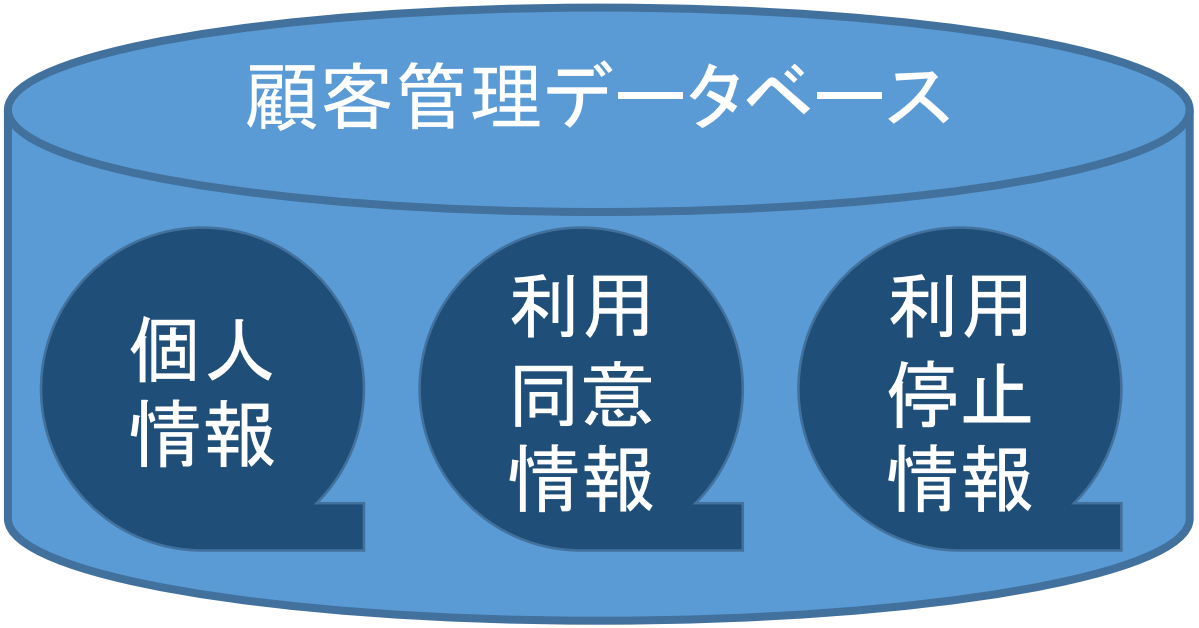
目標設定に影響を与える要素

- エンゲージメント率
- データクレンジング頻度
- その他

個人情報のライフサイクル

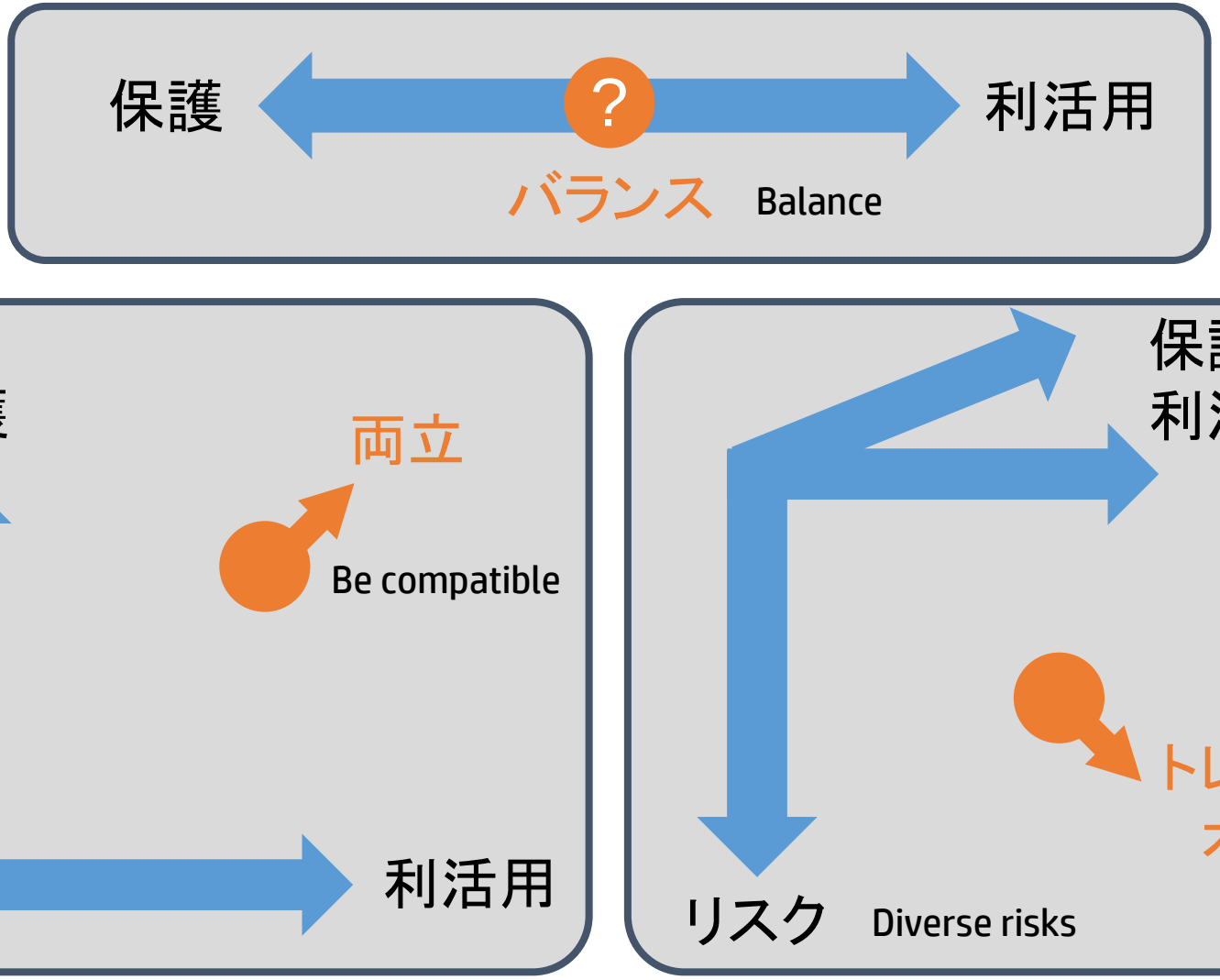


個人情報のリスク管理



流出	汚染	滅失	・・・リスク
機密性保護	完全性保護	可用性保護	・・・リスク軽減策

個人情報の保護と利活用の両立



発表内容

JIS Q 15001に基づく個人情報保護マネジメントシステムにおいて、情報セキュリティ対策をどのように位置づけて連携していくのかについてご説明いたします。

【1】個人情報保護対策と情報セキュリティ対策の違い

【2】両対策の連携方法

【3】個人情報保護マネジメントシステムの計画