データベース・セキュリティ・コンソーシアム
第12回DBSC春のセミナー

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

2016年5月30日

株式会社 日本HP
チーフ・プライバシー・オフィサー
佐藤慶浩

自己紹介

佐藤　慶浩（さとう　よしひろ）

Asia Region Privacy Officer / Privacy Office / HP Inc.
Chief Privacy Officer / HP Japan Inc.
Data Protection Officer / HP Singapore Inc.

元　内閣参事官補佐（民間併任）
　（内閣官房　情報セキュリティセンター　情報セキュリティ指導専門官）

【社外の活動】

内閣官房　IT総合戦略本部パーソナルデータ検討会技術検討ワーキンググループ

経済産業省

消費者向けサービスにおける通知と同意・選択のあり方検討WG 委員

消費者向けｵﾝﾗｲﾝｻｰﾋﾞｽにおける通知と同意・選択に関するｶﾞｲﾄﾞﾗｲﾝ検討委員

厚生労働省　医療等分野における番号制度の活用等に関する研究会　元構成員
杉並区　情報公開・個人情報保護審議会委員
世田谷区　情報公開・個人情報保護審議会　元構成員
JIPDEC　ISMS適合性評価制度技術専門部会　委員
ISO/IEC JTC1/SC27 WG5 プライバシー小委員会　元主査、現エキスパート
情報ネットワーク法学会　元副理事長、現理事

【その他】　http://よしひろ.com/profile/

資料

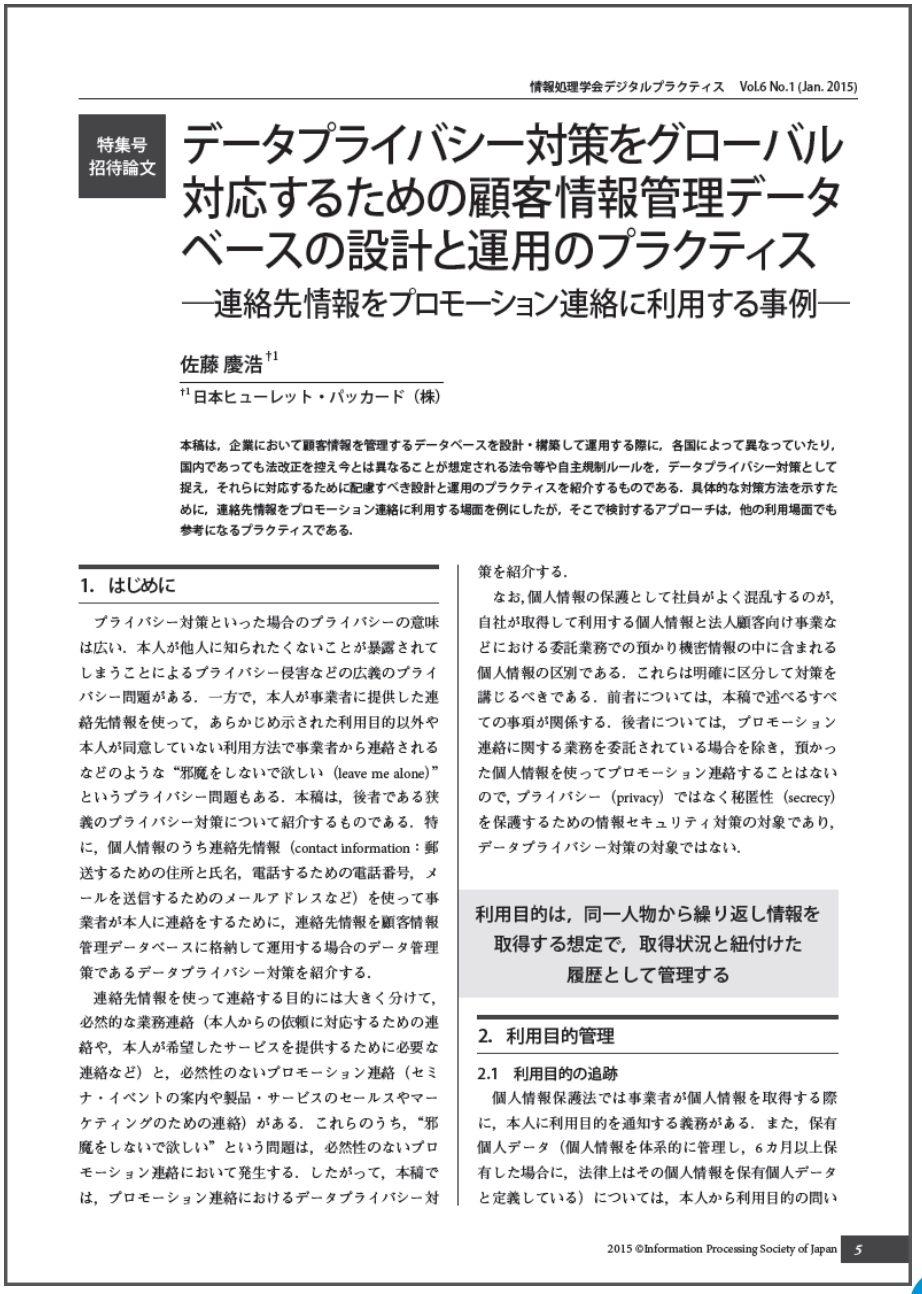
情報処理学会
デジタルプラクティス
Vol.6 No.1 (Jan.2015)

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

佐藤慶浩
日本ヒューレット・パッカード（株）



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）と，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

2015 ©Information Processing Society of Japan　5

目次

1. なぜ、グローバル対応？
2. 利用目的の履歴管理
3. 同意取得状況の管理
4. グローバル対応

グローバル対応の紹介をする目的

個人情報保護法改正に対応することと、グローバル対応する話しと何の関係があるのか？

グローバル対応：
　A国の法令要件に対応、B国の法令要件に対応

法改正対応：
　日本国の法改正前の要件に対応、改正後の要件に対応

地域による違いか時期による違いかでしかない
そして、A国もB国もいずれは法改正する

データプライバシー対策の基本

利用目的の通知

個人情報の利用目的を通知する。
通知した利用目的の範囲内だけで個人情報を利用する

ポイント：法人は1部署とは限らない。1人につき一回の取得とは限らない。

利用の同意取得

個人情報の利用について同意を得た場合は、
同意を得た利用の範囲内だけで個人情報を利用する

2. 利用目的の履歴管理

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

利用目的と取得状況の履歴管理

表 1　利用目的文言番号の例

利用目的文言番号	利用目的文言
JP001	弊社からの製品ニュースをお送りするため
JP002	弊社からのパソコン関連ニュースをお送りするため
JP003	弊社からのプリンタ関連ニュースをお送りするため

表 2　取得状況番号の例

取得状況番号	取得状況	通知した利用目的文言番号
A12345	2001/2/1 開催のセミナへの申し込み登録	JP001
B34567	2002/3/3 開催のセミナでのアンケート記入	JP003
C23456	2004/1/5 ～ 5/5 開催のキャンペーンへの登録	JP001

利用目的と取得状況の履歴管理

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
01	鈴木一郎	○○	03～	suzuki@ example.com	2001/2/3	A12345
02	佐藤二郎	○○	03～	sato@ example.net	2002/3/4 2013/7/8	B34567 E76543
03	田中花子	○○	06～	hanako@ example.org	2003/4/5	A12345
04	高橋三郎	○○	06～	takahashi@ example.jp	2004/5/6 2013/9/10 2014/3/2	C23456 G87654 H01234
05	山本愛子	○○	03～	aiko@ example.net	2005/6/7 2013/7/8	D45678 E76543
06	John Smith	△△	1234	john@ example.edu	2010/9/8	Z98765

データプライバシー対策の基本

利用目的の通知

利用の同意取得

個人情報の利用について同意を得た場合は、
同意を得た利用の範囲内だけで個人情報を利用する
個人情報の利用について不同意を得た場合は、
不同意されてない範囲内だけで個人情報を利用できる

ポイント：

同意取得が法的義務でなくても、不同意の管理は不可避で、初期値を同意ありにした同意管理が必要。

意思と意思表示と意思確認は必ずしも一致しない。

３．同意取得状況の管理

同意取得は
連絡先項目ごとに、
確認の有無と確認方法が
わかるように管理する

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

（参考）みなし同意

明示的同意取得（デフォルトオフ方式）
暗黙的同意取得（デフォルトオン方式）

みなし同意（同意したものとみなしますと通知するだけ）

　明示的または暗黙的同意取得方式のように何らかの行為を促す選択肢を与えないで，同意を取得したとみなすと表示だけすることを，みなし同意と呼ぶ．

みなし同意を，同意を取得したとして取り扱うことは適切ではない．すなわち，同意を取得したことにならないという意見があることに留意すべきである．

本稿では，みなし同意は同意取得ではないという意見を尊重し，方式は2通りとしたが，確認結果をすべて未確認として扱うしかない第3の同意取得方式とみなす数え方も考えられる．

（参考資料）

経済産業省　商務情報政策局　情報経済課
Ministry of Economy, Trade and Industry

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。

同意取得方式ごとの取得者における長所と短所

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

同意取得方式を区別した同意状態値

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

同意確認の状況と同意状態値

□ 同意する
□ 同意しない

同意しますか？
□ はい

☑ 同意する

□ 同意しない

表 5　同意確認の状況と同意状態値

同意確認の状況				同意状態値
同意について確認した	同意と不同意の選択肢を示した	同意をあらかじめ選択してない	同意を選択した	Y
			不同意を選択した	N
			どちらも選択しなかった	U
		同意をあらかじめ選択しておいた	同意をそのままにした	y
			不同意を選択した	N
	同意の選択肢だけを示した	同意をあらかじめ選択してない	同意を選択した	Y
			同意を選択しなかった	U／N
		同意をあらかじめ選択しておいた	同意をそのままにした	y
			同意を取り消した	N
	不同意の選択肢だけを示した	不同意をあらかじめ選択してない	不同意を選択しなかった	y
			不同意を選択した	N
		不同意をあらかじめ選択しておいた	不同意を取り消した	Y
			不同意をそのままにした	N
同意について確認していない				U

同意を得ていない状態の3類型

表 5　同意確認の状況と同意状態値

同意確認の状況				同意状態値
同意について確認した	同意と不同意の選択肢を示した	同意をあらかじめ選択してない	同意を選択した	Y
			不同意を選択した	N
			どちらも選択しなかった	U
		同意をあらかじめ選択しておいた	同意をそのままにした	y
			不同意を選択した	N
	同意の選択肢だけを示した	同意をあらかじめ選択してない	同意を選択した	Y
			同意を選択しなかった	U／N
		同意をあらかじめ選択しておいた	同意をそのままにした	y
			同意を取り消した	N
	不同意の選択肢だけを示した	不同意をあらかじめ選択してない	不同意を選択しなかった	y
			不同意を選択した	N
		不同意をあらかじめ選択しておいた	不同意を取り消した	Y
			不同意をそのままにした	N
同意について確認していない				U

すべての N

①同意確認をした結果として不同意を選択された

②同意確認をした結果として同意を得られなかった

③同意確認をいまだしていない

（参考）第5の状態値：Isolation

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

I （Isolation）	隔離： アクセスできない状態にする

COLUMN

個人情報削除のパラドックス：「俺の個人情報の削除は完了したか？」と問われて「完了しました」と答えたら「俺が削除依頼したと分かるということは俺のことが削除されていないじゃないか」と矛盾を指摘されることになる．そう問われたら「どなたですか？　何のことですか？」と答えれば矛盾はなくなり，問合せ者は「いや．気にしなくていい．この問合わせは忘れてくれ」と納得する．

実際には弊社では，削除依頼を受け付けた際に受付番号を発行する．受付番号は削除作業の進捗管理にだけ使い個人情報と直接は紐づけない．すべての削除を完了した後は，受付番号だけを単独に履歴として残す．ご本人から作業進捗を問われた場合には，受付番号だけを教えてもらい，その受付番号の進捗状況を回答する．

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 ←U
	電話番号	U ←U
	メールアドレス	Y ←Y
コンテンツ	パソコン関連ニュース	Y ←Y
	プリンタ関連ニュース	N ←U

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

４．グローバル対応

同意状態を各国の
利用可否要件に
対応させることにより、
グローバル対応する

同意状態値と法令等の要件に沿った利用の可否

同意取得原則
オプトイン原則
U＝不可

明示的同意取得原則
（デフォルトオン禁止）
y＝不可

表 10　同意状態値と利用可否

同意状態値		利用の可否			
		日本		A 国	E 国
		プライバシーマーク認証取得事業者	その他の事業者		
住所	Y	可	可	可	可
	y	可	可	可	不可
	N	不可	不可	不可	不可
	U	不可	可	可	不可
電話番号	Y	可	可	可	可
	y	可	可	可	不可
	N	不可	不可	不可	不可
	U	不可	可	可	不可
メールアドレス	Y	可	可	可	可
	y	可	可	可	不可
	N	不可	不可	不可	不可
	U	不可	不可	可	不可

同意状態値の更新ルール

表 11　同意状態値の更新ルールの例

取得した値	既存の値	値の更新方法
Y	Y, y, N, U	Y
N	Y, y, N, U	N
y	Y	Y
	y, U	y
	N	N
U	Y, y, N, U	更新しない

別方針の例

明示的同意の継承方針の例

Y → y

不同意の継承方針の例

N → y

既存値の継承方針の例

Y → U　　Y → Y

y → U　　y → y

N → U　　N → U

同意の有無について、ご本人からの明示的意思変更がなければ、それまでの確認結果を変更しない。という方針の例

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

まとめ

まとめ:データプライバシー対策の基本

利用目的の通知

個人情報の利用目的を通知する。
通知した利用目的の範囲内だけで個人情報を利用する
ポイント:法人は一人ではない。一人につき一回ではない。

利用の同意取得

個人情報の利用について同意を得た場合は、
同意を得た利用の範囲内だけで個人情報を利用する
個人情報の利用について不同意を得た場合は、
不同意されてない範囲内だけで個人情報を利用できる
ポイント:同意取得が法的義務でなくても、不同意の管理は不可避で、初期値を同意ありにした同意管理が必要。
意思と意思表示と意思確認は必ずしも一致しない。

まとめ：利用目的と同意状態の管理

法令等の要求事項を直接的に管理するのではなく、それらを間接的に吸収できるシステムを設計・構築し運用するとよい。

法令等の要求事項への対応は、ITシステムや運用手順において、セマンティクス（コーディング）として実装するのではなく、パラメータとして実装する。

法令等の要求事項の変化は、パラメータの変更だけで対応できるようにする。（例：表10）

まとめ:データプライバシー対策の基本→応用

利用目的の通知　→　第三者提供の通知

提供内容

個人情報の~~利用目的~~を通知する。

提供内容　　提供

通知した~~利用目的~~の範囲内だけで個人情報を~~利用~~する

利用の同意取得　→　第三者提供の同意取得

提供

個人情報の~~利用~~について同意を得た場合は、

提供　　提供

同意を得た~~利用~~の範囲内だけで個人情報を~~利用~~する

発表資料のダウンロード

http://よしひろ.com/

お問い合わせ

http://twitter.com/4416sato