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

合わせがあった場合には対応する義務がある．

それらを遵守するために，顧客情報管理データベースの個人レコードには取得時にどのように利用目的を通知したかを管理する必要がある．しかし，個人レコードごとに利用目的文言を文章で格納するのは効率が悪い．

連絡先情報の利用目的文言について会社としての標準文言を定めるのがよい．標準文言といっても，あらゆる取得状況において単一共通の文言にする必要はなく，いくつかの定型文にすればよい．その上で，取得する際に定型文から選ぶことにして，定型化せずに作文することを禁止すべきである．それであれば，顧客情報管理データベースでは，利用目的の文言そのものを格納する必要はなく，定型文に割り振った番号を格納することができて効率的である．利用目的文言番号の例を表1に示す．

しかし，実務上は，利用目的文言番号だけを管理するよりも，その連絡先情報をどのような状況で取得したのかまでを含めて後から分かるようにする方がよい．たとえば，イベントの参加申し込みをしてもらったのか，セミナ参加時にアンケートに記入してもらったのかなどの状況である．それらの取得状況に付番をして，番号ごとにどのような状況での取得であったのかと，その取得に際して通知した利用目的文言番号または文言そのものを，顧客情報管理データベースとは分けて紐づけて管理することで，顧客情報管理データベースには，取得日と取得状況番号だけを格納するとよい．取得状況番号の例を表2に示す．

このとき，個人情報の取得は，同じ人から繰り返して取得する場合があることを想定すべきである．たとえば，イベント申し込みですでにデータベースに登録された人が，後日別のセミナに参加してアンケートに連絡先を再び記入して提出していただくということもある．そのため，取得状況番号の格納は1人につき1つではなく，履歴として格納するべきである．

通知した利用目的の追跡のために，取得状況を個人レコードごとに履歴として管理することが必要である．

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

2.2　データ汚染時のデータ除染

万が一，取得時に利用目的の通知を怠っていたり，次章で紹介する同意取得状況に不備がある状態で顧客情報管理データベースに登録されてしまった場合には，後からそれらの不適切な個人レコードだけを削除や修正する必要がある．そのように不適切な個人レコードが混入することをデータ汚染と言う．データ汚染した場合には，汚染しているデータだけを抽出してデータ除染する必要がある．部分的なデータの除染ができないと，最悪の場合は，データベースのすべてのレコードが利用できなくなってしまう．

データ除染ができるようにするためにも，取得状況を個人レコードごとに履歴管理することが必要である．

同意取得は，連絡先項目ごとに，確認の有無と確認方法が分かるように管理する

3.　同意取得管理

3.1　事前同意の要否と同意管理の必要性

個人情報保護法では事業者が個人情報を取得する際に，本人から同意を得るのは第三者提供する場合などに限られている．しかし，保有個人データについては，個人情報の取得後に本人からの求めに応じて利用停止などの対応をする義務がある．また，迷惑メール防止法（正式通称:特定電子メールの送信の適正化等に関する法律）において，いわゆる広告メール（法では特定電子メールとして定義されている）を送信するためには，メール送信についての同意を本人から事前に得る義務がある．本人から知らされたメールアドレスであっても，事前に同意を得ずに，広告メールを送信することは違法である．

仮に，事前同意が不要であっても，事後に不同意の依頼があれば法令等の義務がなくとも業務として対応する必要がある．データベースの処理として考えた場合には，事前同意が不要な場合とは，同意状態の管理が不要にな

るわけではなく，同意状態値を格納できるようにした上で，その初期値を同意にできるということでしかないのである．

したがって，事前同意が不要な場合でも，同意状態を管理することが必要である．

3.2 メディア・パーミッションとコンテンツ・パーミッション

連絡先情報には，住所や電話番号，メールアドレスなどがあるが，これらは連絡のための媒体の種類であることから，それぞれの項目をメディアという．プロモーション手段として考えた場合に，新聞広告というメディアを使うのか住所を使ってダイレクトメールというメディアを使うのかということである．

メールアドレスについては事前同意が求められていることからも分かるとおり，少なくとも，メディアごとに同意状態を分けて管理する方がよい．すなわち，メールアドレス利用の同意状態と，住所や電話番号など他のメディアの同意状態を分けて管理するということである．メディアを分けていないと，メールアドレスの同意を得られないと電話もできなくなってしまうからである．メディアごとの同意状態をメディア・パーミッション（メディア別許可）という．

メディア・パーミッションを得る際に，利用目的に即して包括的に同意を得るのと，連絡する内容を限って同意を得ることが考えられる．たとえば，「パソコンのご案内をお送りしてもよいか？」という確認と，「プリンタのご案内をお送りしてよいか？」という確認を分けるということである．連絡する内容を分けた同意状態をコンテンツ・パーミッション（内容別許可）という．

法律上は，このように同意状態を細分化して管理することは求められていない．同意だけの観点からすると包括的に得た方が広範に利用できるようになるため，事業者にとって有益だと思うかもしれない．しかし，同意を得るという行為をして，結果的に同意をしてもらえないと，不同意を得てしまったことになることもある．つまり，同意を得る行為は，不同意を得る行為と表裏一体なのである．その意味で，包括的に同意を得ようとすると，包括的な不同意を得たことになる場合もあり得る．そうなると，その人へのプロモーション連絡は一切できなくなるのである．そのように，不同意の観点もあることに着目し，不同意を細分化するために，確認する連絡内容の細分化が役立つ場合がある．

たとえば，あるお客様はパソコンを購入した直後なのでパソコンに関する案内なら不要だが，プリンタに関する案内なら欲しいと思うかもしれない．そのような場合には，パソコンに関する案内の同意をあえて確認しないことによって，不同意を得る可能性をなくすことができる．同意を得ようとしなければ，能動的には不同意を得ることもないのである．

また，事後に利用停止を希望された場合にも，部分的な利用停止ができることで，すべての内容の利用停止を避けることができる場合もある．

このように連絡内容を細分化した同意の選択をご本人ができるようにすることで，部分的な同意取得の機会を増やしたり，利用停止などを部分的な不同意にとどめることができたりする場合もある．メディア・パーミッションとコンテンツ・パーミッションを組み合わせて事業に最適化することが重要である．

3.3 明示的同意取得と暗黙的同意取得

同意を取得する方法について，法律上は指定されていないが，同意の取得方法には，明示的同意取得と暗黙的同意取得の2通りある（コラムも参照）．

明示的同意取得とは，同意を取得するために，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ことである．たとえば，「同意するならチェックボックスにチェックマークを記入してください」と確認して，チェックマークを記入されたときにだけ，同意を取得したものとして扱い，記入がなければ同意を取得できなかったとして扱う方法である．

暗黙的同意取得とは，同意を取得するために，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ことである．たとえば，「同意しないならチェックボックスにチェックマークを記入してください」と確認して，チェックマークを記入されなかったならば，同意を取得したものとして扱う方法である．

Web画面の場合には，逆に「□同意する」というチェックボックスを表示しておいてあらかじめそこにチェックを入れた上で，「同意しないならチェックマークを外してください」と確認することも暗黙的同意取得になる．そのため，明示的同意取得方式と暗黙的同意取得方式を，それぞれ，デフォルトオフ方式とデフォルトオン方式と呼ぶこともある．

同意の取得率を高くしようとする観点からは，暗黙的同意取得方式が優位に思うかもしれないが，実際には，それぞれに一長一短がある．明示的同意取得方式と暗黙

的同意取得方式の特徴を整理したものを表3に示す.

3.4　同意状態値の定義

同意確認の有無と，同意確認をした場合にその確認方法が明示的方式か暗黙的方式かを区別して同意状態を管理するための値の例を表4に示す.

これらの同意状態値が，どのような同意確認状況の結果として登録されるのかを表5に示す.

3.5　同意状態の運用方法

メディアとコンテンツによる同意状態の細分化と同意状態値の定義をした上で，同意確認の結果をどのように格納して，どのように利用するかについて紹介する．たとえば，メディア・パーミッションとして，住所，電話番号，メールアドレスの3つを，コンテンツ・パーミッションとして，パソコン関連ニュースとプリンタ関連ニュースの2つに細分化した例を紹介する.

「ご記入いただきましたご連絡先に弊社からの製品紹介をお届けしてもよろしいでしょうか？」という文言で確認した結果, 同意を確認できた場合の例を表6に示す. この例は単純にすべての同意状態値がYになるので，すべての利用が可能になる.

少し確認文言を限定して,「ご記入いただきましたメールアドレスに弊社からのパソコン関連の製品紹介をお届けしてもよろしいでしょうか？」という文言で確認した結果，同意を確認できた場合の例を表7に示す.

表7の同意状態のとき，パソコン関連の紹介をメールで送信することができるのは当然である．では，プリンタ関連の紹介を郵送することはできるのだろうか．それができるかどうかは，これらの連絡先を取得する際に通知した利用目的の内容による．個人情報保護法では，利用目的を通知すれば同意を取得しなくても利用すること

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

COLUMN

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.

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

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

ができるので，「ご記入いただきましたご連絡先は，弊社からのパソコンおよびプリンタ関連の製品紹介をお送りするために利用いたします」と通知等をしてあれば，同意取得がなくても送ることができる．

先に，同意状態を細分化する利点を紹介したが，表7の同意状態のときに，プリンタ関連の製品紹介を郵送した結果として「パソコン関連の郵送物は不要だ」という反応があった場合には，**表8**のように同意状態を細かく更新することができる．

また，同じ利用目的通知をしているときに，「ご記入いただきましたご住所に弊社からのプリンタ関連の製品紹介をお届けしてもよろしいでしょうか？」という文言で同意を確認できた場合の例を**表9**に示す．

表9の同意状態のときに，パソコン関連の紹介をメール配信できるだろうか．これはできない．なぜなら，メール送信については事前同意を取得することが法律上求められているからである．

3.6　同意状態値と利用可否

このことは，同意状態値がY（同意）またはN（不同意）の場合には，それを利用できるかどうかが明白であるのに対して，U（未確認）の場合には，法令等などによって利用できるか否かが決まることを意味する．たとえば，プライバシーマーク認証を取得している事業者は，メールアドレスだけでなく，住所や電話番号も事前同意を得るということを対外的に自主宣言しているため，Uの値では郵送も電話もできない．

以上のように，同意を得ていない状態には，同意確認をいまだしていない場合と，同意確認をした結果として同意を得られなかった場合，同意確認をした結果不同意を選択された場合の3種類があり，それぞれ異なるものである．そして，どの場合に利用できるかどうかは，法令等や自主規制ルールの定めによって最終的に決まるのである．メディアごとの同意状態値と対応するメディアをプロモーション連絡に利用できるかの可否の関係を**表10**に示す．

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 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 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

同意状態値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

3.7　グローバル対応

プロモーション連絡に関するデータプライバシー対策のグローバル対応に必要なことは，同意状態と利用可否の関係を各国の法令ごとに対応させることである．たとえば，表10のメールアドレスの同意状態値がUで同意未確認の場合に，日本ではメールによるプロモーション連絡は違法だが，米国では（州によって異なる場合があるが）違法ではない．そのように，同意状態値によって，各国の法令等での利用可否を対応させることでグローバルに対応することができる．したがって，顧客情報管理データベースでは，同意状態値（メディア・パーミッシ

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

ョンとコンテンツ・パーミッション）を格納し，その値を表10の利用可否と対応させてから利用することにより，法令等の要件に対応することができる．そのように管理すれば，同じデータベースの運用で，各国の法令等を遵守することができ，グローバルな事業に使えるのである．このように，データベースでは，利用ができるか否かではなく，同意の有無だけでもなく，同意確認の有無と確認方法を値として格納し，その状態値によって利用できるかを判断することによりグローバルに対応するのがよい．なお，このようにすれば，国内であっても法令等に変更があった場合にすぐに対応することができ，グローバル対応に限らず有用である．

3.8　再取得時の同意状態値の更新

連絡先情報を再取得した場合に，新たに取得した同意状態値に単純に更新するのではなく，既存の値との関係で，どのような値に更新するかのルールを決める必要がある．更新ルールの例を**表11**に示す．

表11から分かるとおり，取得した値がYまたはNの場合には,取得した値で既存の値を上書きして更新する．Uを取得した場合には，既存の値を更新しない．暗黙的同意取得方式であるyについては，既存値に応じて更新方法を決めてもよい．表11では既存値のYとNを残す例を示したが，yに上書きすることもできる．どのようにするかは事業者が検討して決めればよい．

また，このとき，既存の値YまたはyをNに更新するということは，それまで取得した同意が失われ利用できなくなるということである．このことから，既存の値がYまたはyの人に，改めて同意を確認すると，不同意取得の機会を作ってしまうため，同意を確認しない方がよいということが分かる．同意を確認すれば，同意が継続されるか失われるかのどちらかで，同意が増えることはないからである．

4. レコードの利用停止と削除

国内では，個人情報保護法に保有個人データの削除についての努力義務があるため，個人情報の削除について事業者が比較的安易に応じる傾向があるが，事業者としては個人情報の削除には慎重に対処しなければならない．事業のために取得した個人情報は，事業として法令等遵守のために必要な記録や証拠保全の必要がある場合や，個人情報削除のパラドックス（コラムを参照）のような問題もあるからである．

法的義務ではないが，削除についてはできる限り応じるべきであり，そのひとつの手段が，レコードの隔離である．

レコードに隔離フラッグ（Isolated flag）を設けて，隔離フラッグが設定されたレコードについて，データの参照担当者のみでなくデータ更新担当者からも，レコード指定や検索など一切のレコードへの参照ができなくして，限定した特権者だけに参照を許すようにするのである．ご本人からの利用停止の依頼には，データ更新担当者が隔離フラッグを設定することで，その瞬間から，データ更新担当者も参照できないようにする．つまり，データ更新担当者は隔離フラッグを設定できるが，解除はできないようにするのである．

その後，特権者が隔離フラッグの設定されているレコードについてご本人からの依頼状況などを確認した上で，最終的に対処方法を判断するということに隔離フラッグを用いることができる．

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

5. テーブルの例

これまで述べたことをまとめたテーブルの例を**表12**に示す．このテーブルと表1，表2，表10とを併用することで顧客情報管理データベースとして運用することになる．

6. 同意状態値更新の部門間連携

事業者内で単一の顧客情報管理データベースに集約する場合には，それをテーブルとして管理すればよい．しかし，複数のデータベースで管理する場合には，それらの連携が必要である．

この連携は技術的に行うことも，運用で行うこともできる．技術的にできるならば，データベース間を接続して，それぞれの同意状態値が同期するようにする．しかし，それができるのであれば，同意状態値のテーブルを集約してしまうほうが効率的である．それができずに複数のテーブルを共存させるのであれば，運用上で各デー

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	

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．

タ更新担当者が，同意状態値と隔離フラッグの更新を連絡しあって更新することもできる．

いずれにしても注意しなければならないのは，本人による同意状態値の依頼を，どのように解釈するかである．たとえば，ダイレクトメールを送った反応として「今後はダイレクトメールは不要だから止めて欲しい」と依頼されたとする．ダイレクトメールを送った部署の人は，自分の送ったダイレクトメールについてのコンテンツ・パーミッションをNに更新することは，すぐにできるだろう．しかし，相手はメディア・パーミッションとして，他の部門からのダイレクトメールも停止する依頼をしたと思っているかもしれない．利用停止に際しては，どの範囲の停止を希望しているのかを丁寧に確認して，それに見合った同意状態値を部門間で連携して更新する必要がある．

本人の同意状態値の更新の期待範囲が部分的か全社的かは，場合によるが，連絡先情報そのもの，すなわち住所や電話番号などについては，部分的な更新よりは全社的な範囲になるため，その点においても顧客情報管理データベースはなるべく集約する方向で検討するのがよい．

以上のように連絡先情報とデータプライバシー対策に必要な同意状態値と隔離フラッグの運用に注意すべき点は多い．したがって，業務アプリケーションソフト内に連絡先情報を格納すると複雑な連携が必要になるため，業務アプリケーション内には連絡先を保管せずに顧客IDなどを使って顧客情報管理データベースと紐づけて，運用することが効率的である．

7. おわりに

企業におけるプライバシー対策に法令等で何をどう求めるのか，それに対して業界は自主規制を含めてどう対応するのかについて，世界の各地で多くの議論が繰り返されている．このように要求事項が多様化し，なおかつ変化している中で，IT部門がすべきことは，議論の中でどの個所が変化しており，どの個所は定着しているのかを見極めることである．そして，変化している個所についての結果に一喜一憂する必要はないのである．ITシステムの中でその変化をパラメータとして集約できるようにすることで，要求事項が変わったときに俊敏に対応できるように備えることが重要なのである．本稿は，

企業におけるプライバシー対策のうち，データプライバシーに限定し，さらに，連絡先情報をプロモーション連絡に利用する場面を事例として紹介した．その場合であれば，同意取得の取得方法を表4と表5に集約でき，取得している同意状態値をどのように取り扱うかを表10に集約できた．そのようにすることで，プライバシー対策の要件がどのように変化しても，データベースシステムそのものの設計見直しや再構築は不要となり，グローバルに対応できるシステムになるのである．以上のように，企業におけるプライバシー対策をITシステムとして具体的に検討する場合には，プライバシーの範囲を絞り，利用場面に沿った内容で検討し，変化に個別に対応するのではなく，変化を吸収できるシステムを設計・構築し運用することが，企業に求められていることなのである．

参考文献

1）佐藤慶浩：機密情報とは，http://yoshihiro.cocolog-nifty.com/security/2004/12/post_2.html
2）個人情報の保護に関する法律
3）特定電子メールの送信の適正化等に関する法律

佐藤 慶浩（正会員）yoshihiro.satoh@hp.com
日本ヒューレット・パッカード（株）チーフ・プライバシー・オフィサー／エヴァンジェリスト．1990年日本ヒューレット・パッカード（株）入社．アジア地域のITセキュリティ事業統括，米国の開発部門および英国の研究所などに従事した後，2004年から現職．社外では，IPA，JIPDECの非常勤研究員の他，2004～2012年まで内閣官房情報セキュリティ参事官補佐・指導専門官を併任．2015年度に予定されている個人情報保護制度改正については，政府の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委員として参加した．

採録決定：2014年9月29日
編集担当：茂木　強（(独）科学技術振興機構）