個人情報保護法改正のポイントとパーソナルデータ利活用に向けた匿名加工

亀石 久美子（かめいし くみこ） /廣田 啓一（ひろた けいいち）
藤村 明子（ふじむら あきこ） /間形 文彦（まがた ふみひこ）
大田 幸由（おおた ゆきよし）
NTTセキュアプラットフォーム研究所

パーソナルデータの利活用によるさらなる産業振興と，プライバシ保護の両立をめざし，2015年に個人情報保護法が改正されました．本稿では5つの改正ポイントと，NTTにとっても新たなビジネス創造につながる「匿名加工情報」の制度について説明するとともに，NTT独自の安全性と有用性を両立するPk-匿名化技術，および最新の研究状況を紹介します．

パーソナルデータ利活用に関連する法制度の動向

ビッグデータやパーソナルデータの利活用と，適法かつプライバシに配慮した規律が求められる中，2015年に個人情報保護法が改正され（以下，改正法*1, (1)），2017年5月30日の全面施行に向けた準備が政府主導で進められています．個人情報保護に関する法令の体系を**図1**に示します．一番下に位置する個人情報保護法を基にガイドライン等によって具体化される構成になっており，特に実務担当者が見ておくべき項目は，中ほどから上に位置する「個人情報の保護に関する法律についてのガイドライン」(2)，省庁ガイドライン，認定個人情報保護団体*2指針です．

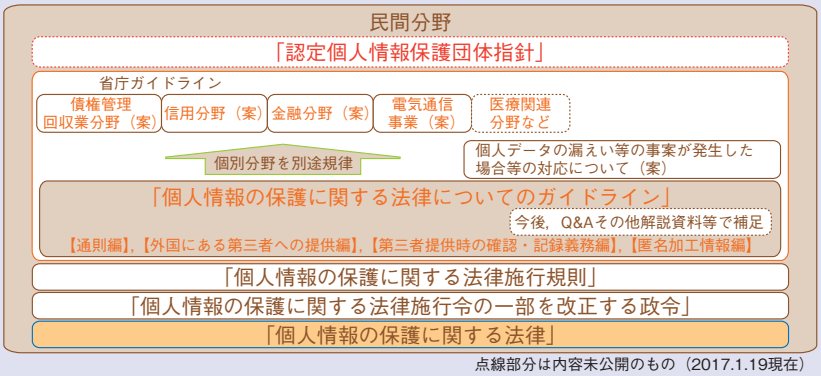
認定個人情報保護団体指針は，従来あまり意識されてこなかったかもしれませんが，今回の法改正で，特に「匿名加工情報」の取扱いに関する事項の追加と，対象団体への指針遵守のための指導・勧告が義務化されたため，重要になっています．NTTグループを対象とする認定個人情報保護団体には，一般財団法人日本データ通信協会（デ協）と一般財団法人日本情報経済社会推進協会（JIPDEC）などがあります．

個人情報保護法の改正ポイント

個人情報保護法の改正のポイントについて，政府資料を基に作成した**図2**を用いて，特に実務への影響が大きいと思われる5点を挙げ，公布済みの施行政令・施行規則の内容を踏まえて説明します．

(1) 個人情報の定義の明確化：「個人識別符号」の導入（改正法 第2条第2項）

情報単体で特定の個人を識別できるものとして「個人識別符号」の概念を導入し，氏名などの情報がなくても個人情報とされることになりました．具体的には指紋や顔認証，静脈などのデータや，マイナンバー・旅券番号・運転免許証番号，基礎年金番号など公的な番号が定義されています．例えば，指紋認証機能付きUSBメモリやスマートフォン内部に保存されている認証用の指紋データも単体で個人情報になるため，企業内での取扱い規定について確認する必要が出てきます．



点線部分は内容未公開のもの（2017.1.19現在）

図1 改正個人情報保護法令の体系

*1 改正法：個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律．

*2 認定個人情報保護団体：個人情報の適正な取扱いなどを目的とし，対象事業者の苦情処理や情報提供を行う民間団体で，分野ごとに現在42団体があります．各団体が関連する省庁が策定するガイドラインを基に指針を策定し公開しています．

⑵ 「要配慮個人情報」（改正法　第２条第３項）

要配慮個人情報とは，人種，信条，社会的身分，病歴等，その取扱いによっては差別や偏見を生じるおそれがあるため，特に慎重な取扱いが求められる個人情報を類型化したもので，いわゆる機微情報のことです．改正後は，本人の同意なく要配慮個人情報の取得ができなくなるため，企業で健康に関する簡易なアンケートなどで病歴を問う場合に同意取得が必要になります．

⑶ 「匿名加工情報」（改正法　第36～39条）

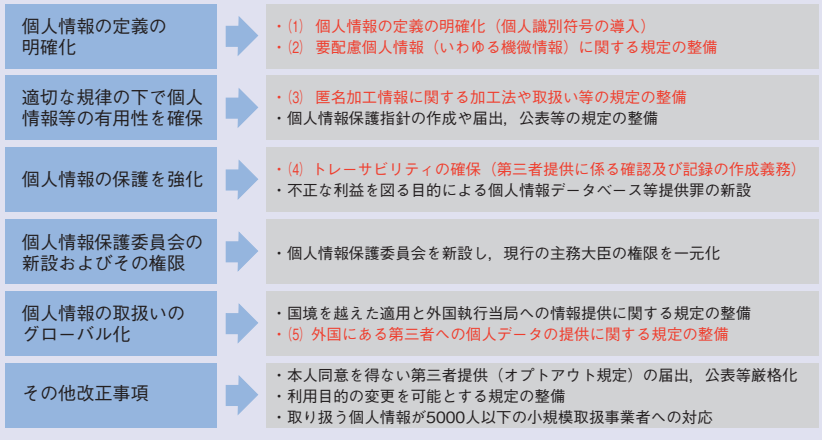
個人情報を特定の個人を識別することができないように加工し，かつ，当該個人情報を復元することができないようにしたものを「匿名加工情報」と定義し，一定の規律の下流通できるようにする制度です．個人情報の第三者への提供には本人の同意取得が必要ですが，匿名加工情報は本人の同意取得が不要というメリットがあります．

⑷ トレーサビリティの確保（第三者提供に係る確認及び記録の作成義務）（改正法　第25，26条）

事業者が他者と個人データの授受を行う場合に，取得経緯の確認，授受した情報の項目や提供年月日などの記録が義務付けられました．不正な手段によって入手・流出した個人情報が，転々流通することの防止を意図しています．既存の契約形態が委託か，第三者提供かの確認や，必要に応じて，ログ取得機能の追加が必要になります．

⑸ 「外国にある第三者」への個人データの提供（改正法　第24条）

「外国にある第三者」とは外国に所在する者で法人等を含む（自社の海外支店等は該当しない）と定義され，その外国にある第三者に個人データを提供する場合，原則本人の同意がないと個人データを提供できないというものです．ある海外法人の提供するクラウドサービスに社員の個人情報の取扱いを委託する場合にも，原則本人の同意取得が必要になります．例外として，個人情報保護委員会が定める外国の企業であることや，APECの越境プライバシールール（CBPR: Cross Border Privacy Rules）に基づく認定を取得した外国企業であれば本人の同意が不要[3]とされています．

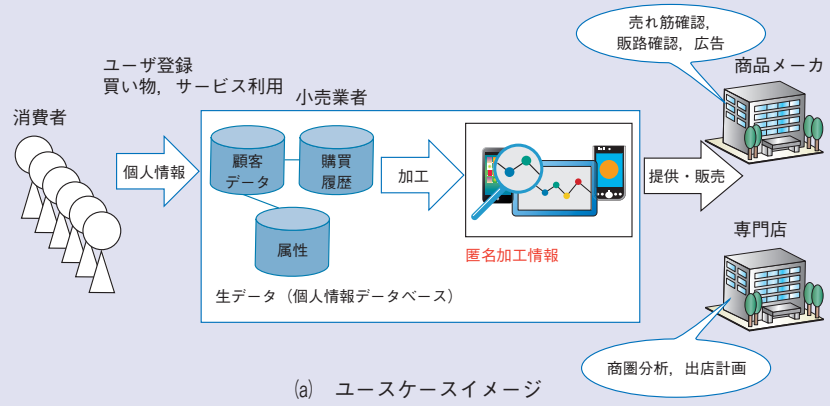


出典：http://www.cas.go.jp/jp/houan/150310/siryou1.pdfより作成

図２　個人情報保護法の改正のポイント

「匿名加工情報」の活用による新規ビジネスの創出

「匿名加工情報」は個人情報を加工した情報ですが，第三者への提供には本人同意が不要というメリットがある



⒜　ユースケースイメージ

① 生データ（個人情報）

顧客ID	登録日（YYYYMMDD）	氏名	住所（郵便番号，詳細な番地まで）	生年月日（YYYYMMDD）	性別（男/女）	購買履歴（日時，購入明細）	購入経路（1:店頭，2:ネット）	支払方法（1:現金，2:クレカ）	属性1（宅配利用）	属性...

加工
・氏名等の個人特定につながる項目の削除，置換
・数値を丸めるなどの処理

② 匿名加工情報

仮ID	住所（町丁目まで）	年齢（10歳刻み）	性別（男/女）	購買履歴（年月，カテゴリ）	購入経路（1:店頭，2:ネット）	属性1（宅配利用）	属性...

③ 統計情報

商品カテゴリ	世代別購入額（201x年○月～○月，○市）							
	10代	20代	30代	40代	50代	60代	70代以上	合計
食　品								
日用品								

⒝　データセットの加工イメージ

図 3　匿名加工情報のイメージ

ため，うまく活用することで新たなビジネス創出が期待できます．

匿名加工情報を活用するユースケースイメージを**図 3** ⒜に示します．消費者は小売業者にユーザ登録を行い，小売業者から商品を購入したり，サービス利用をすることにより，小売業者に顧客データ，購買履歴などの生データが蓄積します．これを小売業者が加工し，加工データを商品メーカ，専門店などの他者に提供・販売し，他者は売れ筋や販路の分析，出店計画に利用することが考えられます．この提供・販売するデータを匿名加工情報とする活用が考えられます．

データの加工イメージを図 3 ⒝に示します．①の表では，小売事業者は顧客IDでユーザを管理し，顧客データとして登録日，氏名，住所，生年月日，性別を登録しています．さらに顧客IDごとに購買履歴（日時，購入商品の詳細や金額），購入経路（店頭・ネット経由），支払方法（現金・クレジットカード），宅配サービスの利用の有無などを管理しているとします．現行法では本人同意なく他者に提供できるのは③統計情報ですが，統計情報よりももう少しきめ細やかなデータへ加工して使うことを考えます．

生データから氏名や住所などの個人特定につながる情報を削除，または丸めて個人が分からないようにし，いつ，どんな商品カテゴリの商品を買ったか，ネット販売を利用したかどうかが分かるデータ②に加工します．②は，例えば商品メーカで売れ筋確認，興味ある商品カテゴリが想定した顧客層に受けているか，宅配の利用が多いか否かなど，マーケティングへの活用が見込まれます．

研究所の匿名化技術

改正法における匿名加工では，「特定の個人を識別することができないように」個人情報を加工することが求められます．特定の個人を識別することができないことを証明するのはとても難しい問題であるため，実際には「あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することを求めるものではなく，少なくとも，一般人及び一般的な事業者の能力，手法等を基準として当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるもの」[4]とされています．

具体的な匿名加工の方法や基準については，前述の指針等によって今後業界ごとに決められることになりますが，例えばガイドラインの匿名加工情報編[4]や匿名加工情報作成マニュアル[5]では，一般化，トップ（ボトム）コーディング，ノイズ付加などの方法が示されています（**表**）．実際にこれらの方法を使って匿名加工を行う際には，利用するパーソナルデータのユースケースを明確化し，情報の項目に対して識別子，属性，履歴の仕分けを行って，個人識別等にかかるリスクを抽出し，どのような加工方法を適用するかを検討することが必要です．

匿名加工したデータを実際のビジネスで活用するためには，特定の個人を識別することができない匿名性を満たすのと併せて，データを有効に活用できる有用性がなるべく高くなるように加工することが重要です．NTTセキュアプラットフォーム研究所では，k-匿名性という評価尺度を基準として，こ

表　匿名加工情報の加工にかかわる手法例

手法名	概　要
項目削除・レコード削除・セル削除	加工対象となる個人情報データベース等に含まれる個人情報の記述等を削除するもの．
一般化	加工対象となる情報に含まれる記述等について，上位概念もしくは数値に置き換えること，または数値を四捨五入などして丸めることとするもの．例えば，購買履歴のデータで「きゅうり」を「野菜」に置き換えること．
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して，特に大きいまたは小さい数値をまとめることとするもの．例えば，年齢に関するデータで，80 歳以上の数値データを「80 歳以上」というデータにまとめること．
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後，グループの代表的な記述等に置き換えること．
データ交換（スワップ）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えること．
ノイズ（誤差）の付加	一定の分布に従った乱数的な数値を付加することにより，他の任意の数値へと置き換えること．
疑似データ生成	人工的な合成データを作成し，これを加工対象となる個人情報データベース等に含ませること．

出典：個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」より作成

れを確率的な尺度に置き換えたPk-匿名性というNTT独自の評価尺度に基づく匿名化技術を開発しました[6]．これは，項目の値を確率的に書き換えるランダム化という処理に基づくもので，k-匿名性と同等の安全性を持つことが数学的に証明された世界初の手法です．Pk-匿名性に基づく匿名化では，値を確率的に書き換えているため，元のデータとは違うものになりますが，確率に基づくベイズ推定という方法を使って統計的に元のデータに近いデータに加工することができます．k-匿名化でよく使われる一般化という加工方法では，例えば「きゅうり」を「野菜」と変えることでデータの細かさが変わるのに対し，Pk-匿名化では「きゅうり」を「トマト」のように細かさを変えずにデータを書き換えるので，若干の誤差は許しつつ，データの細かい分布を見たいマーケティングなどの分析において有用であると考えています．

NTTセキュアプラットフォーム研究所では，これら匿名化技術の研究開発を進めるとともに，実際にデータを持っている事業者との共同研究や実証実験，国内における匿名化技術に関するコンテストへの参加などを通じて，多様なデータの匿名化に関する技術的ノウハウを蓄積し，改正法の施行に合わせたサービス提供の準備を進めています．

今後の展開

2017年2月ごろには，改正法の関連ガイドラインや認定個人情報保護団体指針の改定作業が進む一方，企業の個人情報保護関連の規定類の見直しや，有用なデータを匿名加工情報にして活用するビジネスの検討が進んでいるかと思います．私たちは，法制度関係の動向を踏まえながら，法制度と技術の両面からNTTグループ内での技術支援と，学会活動等の対外活動を引き続き行っていきます．

■参考文献

⑴ 日置・板倉：“平成27年改正 個人情報保護法のしくみ，” 商事法務，2015.
⑵ http://www.ppc.go.jp/
⑶ 個人情報保護委員会：“個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編），” 2016.
⑷ 個人情報保護委員会：“個人情報の保護に関する法律についてのガイドライン（匿名加工情報編），” 2016.
⑸ 経済産業省：“事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（「匿名加工情報作成マニュアル」）Ver1.0，” 2016.
⑹ Focus on the News：“ビッグデータ時代における新たなパーソナルデータ匿名化システムを開発――高度にプライバシを保護したままに，データの利用価値を高いままとする，” NTT技術ジャーナル，Vol.26，No.5，pp.51-52，2014.

（左から）間形 文彦/ 藤村 明子/
亀石 久美子/ 廣田 啓一/
大田 幸由

個人情報保護法の改正により，匿名加工情報というパーソナルデータ利活用のための新たな制度ができました．この制度の利用や匿名化技術の活用を検討中のご担当者からのご相談をお待ちしています．

◆問い合わせ先
NTTセキュアプラットフォーム研究所
企画担当
TEL 0422-59-3212
FAX 0422-59-2971
E-mail scpflab@lab.ntt.co.jp