Deloitte.
デロイト トーマツ

個人情報保護法改正・グローバルな法制度とシステム

2015年10月29日

デロイト トーマツ リスクサービス株式会社
北野 晴人

目次

グローバルな法制度と最近の話題

グローバルにみた関連法制度は変化しています

アジア諸国で法制度が確立

欧州（EU加盟国およびEEA加盟国）

- EU Data Protection Directive / EUデータ保護指令
- Member State Data Protection Law / データ保護に関する国内法

米国

【連邦レベル】
- 米国消費者プライバシー権利章典
- HIPPA / 医療保険の相互運用性及び説明責任に関する法律
- GLBA / 金融サービス近代化法
- Telemarketing and Consumer Fraud and Abuse Prevention Act（DoNotCall） 等

【州レベル】
- マサチューセッツ州プライバシー保護法 Mass 201 CMR 17（2010年3月）

マレーシア

- Personal Data Protection Act 2010（2013年11月施行）

韓国

- 個人情報保護法（2011年9月施行）

台湾

- 個人資料保護法（2012年10月施行）

香港

- Personal Data Privacy Ordinance / 個人データ（プライバシー）条例

フィリピン

- Data Privacy Act of 2012 / 2012年データプライバシー法

インド

- Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 / 合理的な保護手段及び手続き並びにセンシティブ個人情報に関する情報技術規則（仮訳）

シンガポール

- Personal Data Protection Act 2012 / 2012年個人データ保護法（2014年7月施行）

世界的なプライバシー保護法制の動向には3つのトレンドが存在します

地域によって特性が異なる

欧州 （EUデータ保護指令）	「個人の権利」として厳格に保護する流れ ■ 1995年に成立～今後は「規則」化に向かう ➢ 域外適用 ➢ 罰則強化・消去する権利などの特徴的な内容
アメリカ合衆国	個別法と州法が中心（規制が緩いわけではなく訴訟は厳しい） ■ 分野ごとの規制（HIPPAなど） ■ 州法で対応（California SB 1386、Mass 201 CMR 17など） ■ 包括的な法制度制定の動きも出てきている
アジア各国	国際的な経済交流を視野に入れた急速な法整備 ■ 欧州型（シンガポールなど）とそれ以外（台湾など） ■ 国外持ち出しを禁止する国の増加 ■ 欧州とのビジネスやメディカルツーリズムの進展

欧州司法裁判所 によってセーフハーバー無効の判決が出されました

EU-USセーフハーバー関連の報道

■**The Court of Justice declares that the Commission's US Sate Harbor Decision is invalid（PRESS RELEASE No 117/15）**

米国の公的機関は、セーフハーバー協定の対象外となっている。さらに、国家安全保障、公の秩序及び法秩序に基づいて求められる用件は、セーフハーバー協定に優先している。（略）このような理由から、**裁判所はセーフハーバー協定は無効**であると判断する。

The Court observes that the Commission did not make such a finding, but merely examined the safe harbour scheme.

Without needing to establish whether that scheme ensures a level of protection essentially equivalent to that guaranteed within the EU, the Court observes that the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it.

Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements.

The United States safe harbour scheme thus enables interference, by United States public authorities, with the fundamental rights of persons, and the Commission decision does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference.

For all those reasons, the Court declares the Safe Harbour Decision invalid.

出所：http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

EUデータ保護指令とセーフハーバー無効の問題（1）

EUデータ保護指令では個人情報の域外持出しは原則禁止

法令名称		EUデータ保護指令 / EU Data Protection Directive
概要		① 一元的な基本法。各構成国は、EUデータ保護指令に基づいて国内法を定める義務を負っている。 ② 各構成国に第三者機関が存在し、立ち入り調査権を含む、強い権限を持っている。 ③ 個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護が目的。 適用対象は、EU構成国ですが、域外の第三国への個人データの移転を規制している。
域外移転	原則	域外移転時の制約（第25条）が定められている。 「十分なレベル」※の保護措置を確保している場合には、域外移転が可能とされている。
	例外	域外移転時の例外（第26条）が定められている。 明確な同意の取得、**拘束的企業準則（BCR）や標準契約（SCC）**などがある。
留意事項 （考慮事項）		2012年1月に欧州委員会は、「一般データ保護規則（案）」を発表しており、2015年6月に開催される閣僚理事会での検討・承認後、成立することが予定されている。 規則（案）では、忘れられる権利及び削除権の創設、拘束的企業準則の明文化、段階的な行政上の制裁金制度等が整備される予定であるが最終的な案はまだ変わる可能性もある。

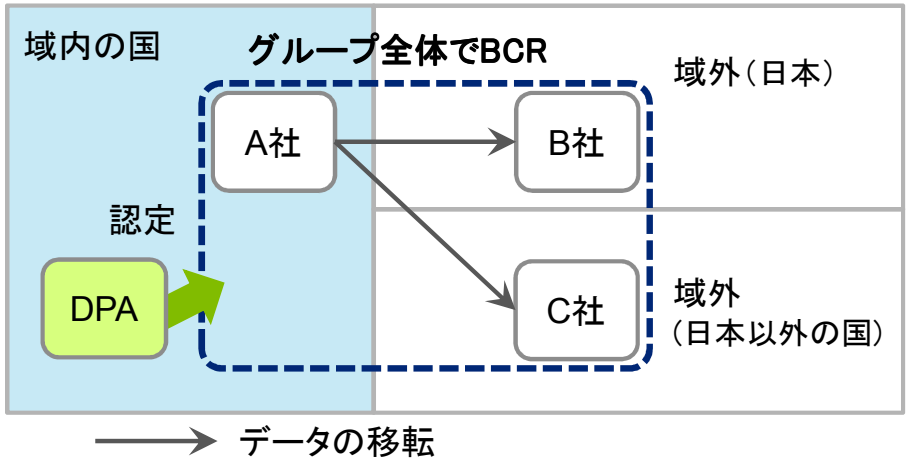
※「十分なレベル」にあるとして、EUから認定を受けている国々は、以下のとおりです。下記以外の国々にデータを移転するには、第26条に基づいた対応が必要です。
スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージー島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド

EUデータ保護指令とセーフハーバー無効の問題（2）

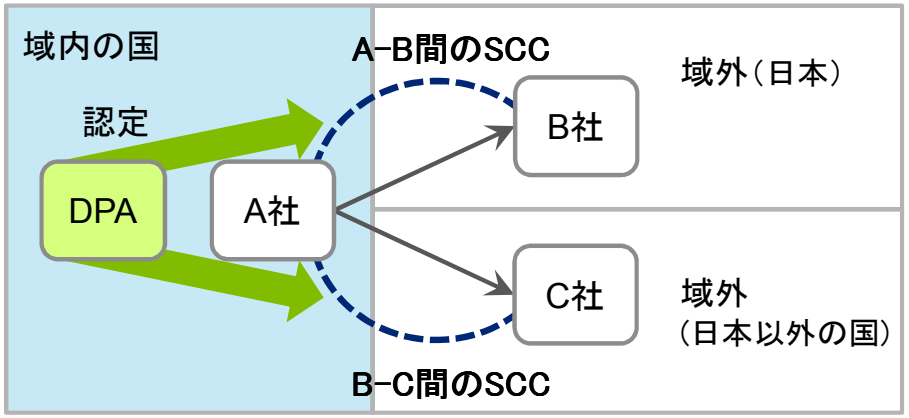
例外条項に基づいた域外移転の主な方法

方 法	概 要
明確な同意の取得	✓ データ主体の**個々人から**個人情報移転に関する明確な同意を得る。
拘束的企業準則 **（BCR: Binding Corporate Rules）**	✓ **グループ内で統一された情報管理を実施している場合**に選択できる。 ✓ その情報管理の方法を文書化し、DPAに申請して承認を得る。これによりグループ企業を包括した個人データ移転が認められる。 ✓ DPAに提出する文書には、SCC（下記参照）と比べて**情報管理に関する詳細な記載**が求められ、外部専門家の助力が必要になる場合が多い。
標準契約 **（SCC: Standard Contractual Clauses）**	✓ **所定の契約フォーマットを使用して、DPAへの届出・申請・承認取得等を行う。** 個別契約を交わした企業間のみに適用される。 ✓ ①セットⅠ、②セットⅡ、③CtoPの3種類のフォーマットがある。

BCRの例



SCCの例



EUデータ保護指令とセーフハーバー無効の問題（3）

29条作業部会の見解

■ **2016年1月末までに解決策が見つからなければ、DPAsは必要かつ適切な措置を講じる**
（Statement of the Article 29 Working Party 2015年10月16日）

DPAsは、SCCやBCRがまだ利用可能であることを考慮し、個人データ主体の保護のため、苦情に基づいた調査の実施は行わない。もし、2016年1月末までに、米国当局においてなんらの適切な解決策が見出すことができない場合、データ保護機関は、全ての必要かつ適切な措置を講じる予定である。セーフハーバーに関するCJEUの決定後に行われている移転は、不法なものである。

In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals.

If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions.

（略）In any case, transfers that are still taking place under the Safe Harbour decision after the CJEU judgment are unlawful.

出所：http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

個人情報保護法改正と実務・システム

個人情報保護法の改正案が可決・成立しました

改正案の概要（マイナンバー関連の改正案と同時に成立）

個人情報の定義の明確化	・個人情報の定義の明確化（身体的特徴等が該当） ・要配慮個人情報（いわゆる機微情報）に関する規定の整備
適切な規律の下で個人情報等の有用性を確保	・匿名加工情報に関する加工方法や取扱い等の規定の整備 ・個人情報保護指針の作成や届出、公表等の規定の整備
個人情報の保護を強化	・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） ・不正な利益を図る目的による個人情報データベース等提供罪の新設
個人情報保護委員会の新設及びその権限	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化
個人情報の取扱いのグローバル化	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
その他改正事項	・本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化 ・利用目的の変更を可能とする規定の整備 ・取り扱う個人情報が5,000人以下の小規模取扱事業者への対応

出所：内閣官房「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案」

海外への個人情報の第三者提供

改正24条（外国にある第三者への提供の制限）

現行法第23条5項
各号は除かれて
いないことに注意

以下の2つの条件どちらも満たさない外国の第三者に個人情報を提供する場合には、「外国の第三者に情報を提供する」ことについて本人からあらかじめ同意を得なければならない、としている（以下2つのどちらかを満たせばよい）。

- 日本と同等の水準で個人情報が保護されている、と認められた国にある
- 日本の個人情報取扱事業者と同じような個人情報保護の体制を整備している

25/26条に沿った
運用が海外側で
必要

海外への持ち出しが発生

- 「認められた国」を選ぶ
- 海外側の環境を整備する
- 同意を取得する（情報提供の同意とは別）

- 人事制度のグローバル化のため
  グローバルな人事システムを構築し、
  海外にデータセンターを持つクラウド
  を利用したい
- 日本の顧客データを海外の委託先
  で分析してサービスを提供したい。

第三者提供の際の記録と確認

改正25条（第三者提供に係る記録の作成等)・26条（第三者提供を受ける際の確認等）

第25条
第三者提供を行う側

個人情報を第三者へ提供する際、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。また一定の期間、記録を保存しなければならない。

第26条
第三者提供を受ける側

個人情報の第三者提供を受けた場合は、当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名、及び当該第三者による当該個人データの取得の経緯を確認しなければならない。

第三者提供がある場合

- **提供する側も、提供を受ける側も、記録と確認を行う仕組みを作る必要がある（契約・システム）**

■ 販売・マーケティング目的のセミナーにおいて参加者の個人情報を、本人の事前同意を得た上で、主催社から協賛各社（スポンサー）に提供したい

要配慮個人情報の新設

改正2条（定義）・17条（適正な取得）

オプトアウト方式は
認められていない
ことに注意

第2条
この法律において「要配慮個人情報」とは、本人の**人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実**その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

第17条
個人情報取扱事業者は、次に掲げる場合を除くほか、**あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。**
一 法令に基づく場合
二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
五 当該要配慮個人情報が、本人、国の機関、地方公共団体、第七十六条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
六 その他前各号に掲げえる場合に準ずるものとして政令で定める場合

EUデータ保護指令における「special categories of data」「sensitive data」と呼ばれているものと似ている。EUデータ保護指令では人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟に関する情報を漏えいする個人データの処理、もしくは健康又は性生活に関するデータの処理を原則、禁止している。

出所：「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案」新旧対照表

個人情報データベース提供罪の新設

改正83条（第7章　罰則）

第83条
個人情報取扱事業者（その者が法人（法人でない団体で代表 者又は管理人の定めのあるものを含む。第八十七条第一項において同じ）である場合にあっては、その役員、代表者又は管理人）若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベースなど（その全部又は一部を複製し、又は加工したものを含む）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、**一年以下の懲役又は五十万円以下の罰金**に処する。

行政機関向けは
現行法でも刑事罰
がある

窃盗罪はまず適用
できないことに注意

情報漏えい対策

- **技術的な要素は今までと何ら変わらない**
- **営業秘密と主張できるシステムが望ましい**

- ■ 内部関係者による情報漏えいなどが起きた場合の直接的な刑事罰
- ■ 不正競争防止法、威力業務妨害、不正アクセス禁止法との比較が必要（営業秘密の証明等）

個人情報保護委員会の新設

欧州データ保護機関に似た強い権限

- 番号法（マイナンバー法）に基づく特定個人情報保護委員会が改組されて個人情報保護委員会になる予定。（2016年1月の見込み）
- 「内閣府設置法（平成十一年法律第八十九号）第四十九条第三項の規定に基づいて、個人情報保護委員会（以下「委員会」という。）を置く。」とされており、内閣総理大臣の所轄となる。
- 改正によって新設された各種の制度などについては、個人情報保護委員会が規則として詳細を定めることになっている部分が多い
- 立ち入り調査権を含む、強い権限が付与される予定であり、現在は各産業分野ごとに現行法では主務大臣が行っている監督業務を一元的に集約して担うことになる。

個人情報保護委員会

- **各種の政令等を確認する**
- **第三者提供時の届出**
- **立ち入り調査についての危機管理体制作り**

- 各種届出などが必要になるため、手続きに注意して業務を行う必要がある。
- 問題が発生した際は報告する必要が発生したり、調査を受けたりする。

まとめ

活用と保護のバランスを検討

1 グローバルな個人情報の移送に注意しましょう

2 要配慮個人情報の取り扱いに注意しましょう

3 技術的安全管理措置は従来と変わらずしっかり実施しましょう

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約8,500名の専門家（公認会計士、税理士、弁護士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約220,000名を超える人材は、“making an impact that matters”を自らの使命としています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

有限責任監査法人トーマツ 東京事務所 エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited