

EUデータ保護指令改定の動き

～国境を越えるデータ移転の課題～

2012年10月3日

一般社団法人 電子情報技術産業協会
クラウドビジネス推進研究会
情報政策委員会 国際活動WG 主査
白川 幸博

JEITA

Japan Electronics and Information Technology Industries Association

【構成】

【1】 EUデータ保護指令について

- プライバシー保護の歴史
- EUデータ保護指令とは
- 日本企業にとっての問題点

【2】 EUデータ保護指令改定について

- EUデータ保護指令改定とは
- 日本企業にとっての問題点

【3】 データ保護制度の国際的潮流について

- EU、米国、OECD、APEC

【4】 JEITAにおける対応について

- EUデータ保護指令改定案に対する意見
- 国際的潮流をふまえたプライバシー保護とデータ活用のバランスのあり方検討

【1】 EUデータ保護指令について

1-1. グローバルなクラウドサービスの法的課題（データ外部保存の視点）

プライバシー保護

（EUデータ保護指令 等）

政府によるデータ閲覧

（米国愛国者法 等）

外国為替及び外国貿易法

（戦略的物資・技術の輸出規制）

不当競争防止法

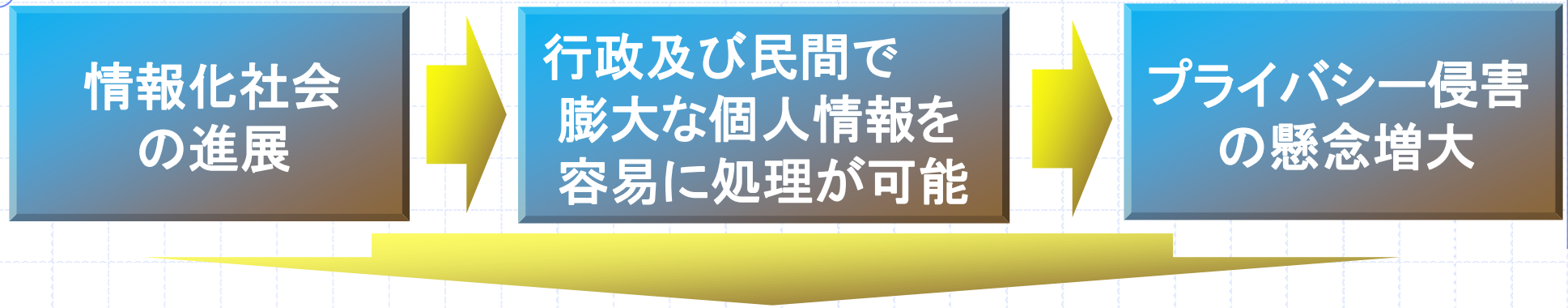
（営業秘密管理）

知的財産権や著作権保護

**各国に保存された
データベースに関する
裁判管轄権**

等々

1-2. プライバシー保護の歴史とEUデータ保護指令



1970年代

- 欧州各国(スウェーデン、ドイツ、フランスなど)及び米国において、プライバシー保護のための法律が多く制定

1980年以降

- 国際機関／多国間でのプライバシー・フレームワークが制定
 - OECD 1980 プライバシーガイドライン
 - **EU 1995 EUデータ保護指令**
 - APEC 2004 プライバシー・フレームワーク


※日 本…1988 行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
1989 民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン(通産省→民間部門へ)
1997 同ガイドライン改正 ⇒ **プライバシーマーク制度**(現在はJISQ15001:2006基準)
2003 **個人情報保護法**

1-3. EUデータ保護指令とは(1)

- 「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令(95/46/EC)」
1995年10月24日 (EUデータ保護指令)

指令の趣旨及び特記すべき内容

- EU及びEEA加盟国に、個人データの処理に対する自然人の基本的
人権及び自由、特に**プライバシー権の保護**を要求
- そのうえで、加盟国間の個人データの自由な流通を促進

- 
- 第三国**が個人データに関する十分なレベルの**保護**を保証すると認められない場合、**個人データの移転は制限**される。(第25条)
 - 日本は、その十分性を認められていない。**
 - 個人データ移転の制限には例外規定あり。(第26条)

1-4. EUデータ保護指令とは(2) <個人データのEU域外移転に関し>

欧州委員会の十分性認定国

- スイス、カナダ、アルゼンチン、イスラエル、* 米国セーフハーバー・スキーム、ガーンジー、マン島、ジャージー(左記3つ: 英国王室属領)、フェロー諸島(デンマーク自治領)、オーストラリア(条件付)

* 米国セーフハーバースキーム

- ・ 米国商務省が中心となりセーフハーバー原則と呼ぶ自主規制を策定、EUとの交渉で認めさせた。
- ・ 企業が当該規制遵守を自己宣言し、米国商務省が認証、企業名を「セーフハーバーリスト」に公示。(2011年7月現在2716社)。違反企業は連邦取引委員会(FTC)が不公正取引として制裁。

第26条 (第三国規定の例外)

- 保護内容が規定されている一定の**標準契約書**の締結など

1-5. EUデータ保護指令とは(3)

EUデータ保護指令

EU+EEA加盟国(合計30カ国)に
国内法規を要求

- ・公正かつ適法な利用
- ・利用目的の明確化
- ・個人情報の正確性
- ・本人の同意の上での取得・利用
- ・特定カテゴリーの個人情報の利用禁止
- ・セキュリティ対策
- ・その他

EU+EEA

A国



公共機関・
民間企業

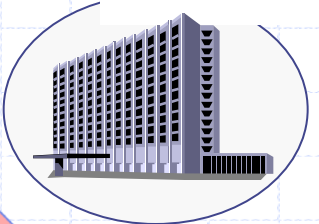
B国

C国

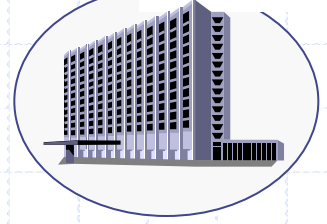
- 以下事項を本人に通知
- ・データ管理者
 - ・個人情報の利用目的
 - ・第三者への提供
 - ・アクセス権、訂正権
 - ・その他

第三国が個人情報に関する
十分なレベルの保護を保証
する場合のみ、
移転を許可
(第25条)

第三国



第三国



監督機関

- ・独立
的な監督
機関の
設置
(第28条)

- ・個人情報への
アクセス権、
訂正・削除
する権利の
保証

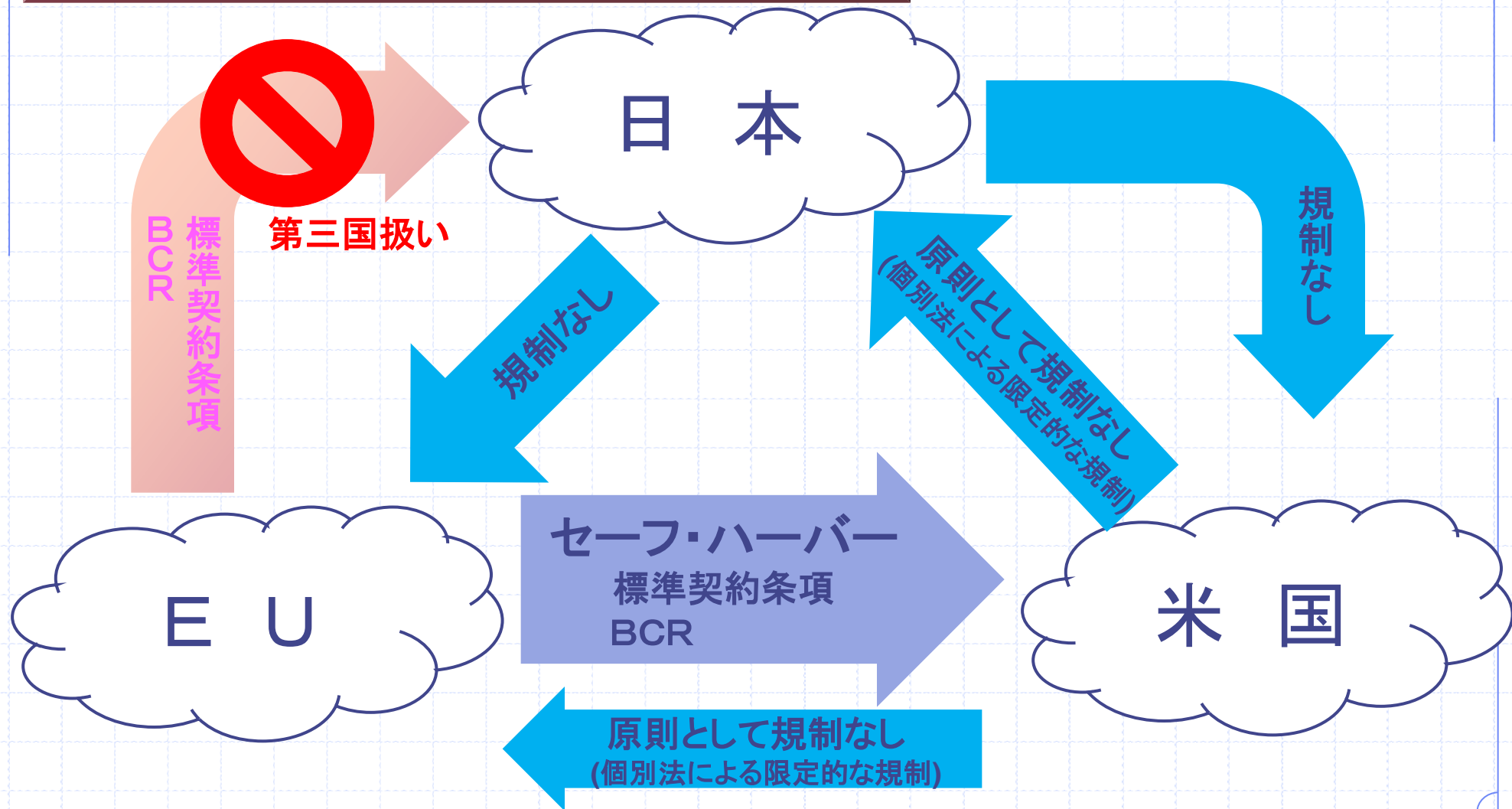
利用者

域内での個人情報の
自由な移転は
認める

1-6. EUデータ保護指令とは(4) <日本企業にとっての問題点>

EU域外への個人データの移転について

(出典:慶應義塾大学 総合政策部
新保准教授資料より)



【2】 EUデータ保護指令改定について

2-1. EUデータ保護指令改定について

- 2012年1月：欧州委員会が「EUデータ保護規則案」を公表

改定の背景

- ・急速なICT技術の進歩とグローバル化の進展による**リスク拡大**
(SNSサイトやクラウドコンピューティング、個人データ収集方法の高度化)
- ・現行のデータ保護スキームに対する**企業の不満増大**

改定の方針

- ・**「指令」から「規則」へ**
(EU加盟国が、「指令」に準拠した国内法を各国でそれぞれ整備する現状から、各国一律で遵守すべき共通ルールとする方向)

今後の予定

- ・欧州議会と連合理事会の審議後、2013年夏～14年に採択の見通し
- ・採択から2年後に発効の見込み

2-2. EUデータ保護指令改定とは(1)

改定の内容(追加された義務)

●第3条 EUデータ保護規則の域外適用

- EU域外企業であっても、EUに居住するデータ主体(個人)のデータを取り扱う管理者に対しては規則が適用される。(EUに居住する個人に商品やサービスを提供している場合等)

●第4条 個人データの範囲

- 個人データの定義は「データ主体に関する全ての情報」として現行指令と変わらないが、個人識別可能なデータとして、「位置データ」と「オンライン識別子」追加。

●第7条 明確な同意の取得

- プライバシーポリシーが分かりにくいため本人の同意が形式的なものに陥っている現状を踏まえ、同意を明確に取得することの義務、また同意を撤回できる権利を保障する義務を追加。

2-3. EUデータ保護指令改定とは(2)

改定の内容(追加された義務)

●第11条 透明で適切なプライバシーポリシーの提供

□現行EU指令にも本人への利用目的等の通知義務があるが、企業のプライバシーポリシーが煩雑で分かりにくい現状を踏まえ、新たに「透明性」の義務を追加。

●第17条 忘れられる権利、同意を撤回する権利

□現行EU指令の第12条にも消去する権利が規定されているが、これを精緻化。現行では、データが不正確だったり不法に収集された等の理由がないと消去できないが、改定案では本人が同意を撤回すれば消去が可能。

●第18条 データポータビリティの権利

□利用者が例えばSNSサービスを他のサービスに切り替える際など、管理者に妨害されることなく、自分の個人データを一定のフォーマットで入手し、他のサービスに移転する権利を保障。

2-4. EUデータ保護指令改定とは(3)

改定の内容(追加された義務)

●第23・30条 データ保護・バイ・デザイン/バイ・デフォルト及び処理のセキュリティ

- 処理の方法を決定するとき及び処理を実施するときの両方において、最新技術や実装コストを考慮し、技術的及び組織的な対策と手順を実行しなければならない。

●第31・32条 データ違反時の監督機関及び本人への迅速な報告・連絡

- 個人データ違反 (personal data breach、紛失・盗難・漏洩・不正利用等) があつた場合、その発見後、可能な限り24時間以内に、監督機関に報告する義務を新設。報告項目は、漏洩データ等の対象人数・データ項目、漏洩等の影響を軽減するために個人等が取るべき対処策、発生した事態(結果)、管理者が取る予定の対応策等。24時間以降に報告する場合は、遅れたことについて正当な理由付けが必要。また、監督機関への報告後、不当な遅滞なく本人へも連絡することが必要。

2-5. EUデータ保護指令改定とは(4)

改定の内容(追加された義務)

●第33条 データ保護影響評価の実施

- プライバシーリスクが高い個人データ処理(経済状況、位置情報、医療健康情報、遺伝子情報、生体情報、監視カメラ情報等を取扱う場合)について、データ保護影響評価(プライバシー影響評価に該当)を義務付け。

●第35条 データ保護オフィサーの設置

- 公共部門及び民間部門(大企業等)におけるデータ保護オフィサーの設置を義務化。

●第79条 監督機関による課徴金

- EU規則への違反に対して、最大で100万ユーロ、又は企業の場合には最大で年間世界売上の2%の罰金が課される。

2-6. EUデータ保護指令改定とは(5)

改定の内容(緩和内容)

●EU域内でのデータ保護ルールの一元化

- 単一のEU規則を各加盟国に直接的に適用すること。
(加盟国毎のルールに合わせなくても良い為、企業にとってコスト削減可能)

●データ処理に係わる監督機関への通知義務の廃止

- 企業にとってコスト削減可能

●ワンストップサービスとしての監督機関

- 多国籍企業の監督機関とのやり取りは、主要拠点の国の監督機関に一本化。

●BCR(拘束的企業準則)の手続き簡素化

- BCRについては、従来複数の監督機関(3箇所)の承認が必要であったが、新規則では、1つの監督機関の承認を得られれば良い。

2-7. EUデータ保護指令改定とは(6) <日本企業にとっての問題点>

現行指令

- ・ 第三国(日本)へのデータ移転制限は継続
(データ保護の十分性認定に至らず)

指令改定

規則強化

- ・ データ保護の権利強化
(忘れられる権利、データポータビリティ、違反時の義務や罰則等々)
- ・ 強化規則の域外適用
(現行指令はEU域内設備でデータ処理を行う場合のみ適用が、域外企業へも適用に)

規則緩和

- ・ EU域内ルールの一元化
- ・ データ処理の監督機関への通知義務廃止
- ・ BCR手続きの簡素化 等々

<日本企業にとっての問題点>

- ・ データ移転制限によるグローバルな**事業活動の制約**(例外規定対応への多大なコスト負担等の負荷含む。
ex. グローバル人材活用の為の従業員データの日本本社への移転対応など)
- ・ 事業活動の抑制や萎縮により**革新的サービスの提供の妨げ**
- ・ EU域内事業拠点を含め、強化規則対応のための**多大な負荷**

<EU域内日本企業にも裨益>

- ・ 規則対応や手続きの簡素化による**コスト削減含む負荷の軽減**

【3】 データ保護制度の国際的潮流について

3-1. データ保護制度の潮流について <各国・各機関>

各国・各機関における制度見直しの動き

EU

- ・1995年10月 EUデータ保護指令 採択
- ・2012年 1月 EUデータ保護規則案 公表

米国

- ・1974年 プライバシー法(連邦行政機関を対象) 制定
- ・民間分野は自主規制中心
- ・2012年2月 消費者プライバシー権利章典 公表
- ・2012年3月 FTCのプライバシー・フレームワーク 公表

OECD

- ・1980年 プライバシーガイドライン 採択
- ・現在、プライバシーガイドラインの見直し中(2013年改正予定)

APEC

- ・2004年 APECプライバシー・フレームワーク 採択
- ・2011年 越境プライバシールール 採択

3-2. 米国のプライバシー・フレームワーク(1)

①ホワイトハウス「ネットワーク化された世界における消費者データプライバシー」

- 2012年2月公表、「消費者プライバシー権利章典」7原則を含む
 - 米国のFIPPs(公正な情報取扱い8原則)を現代風にアレンジ
 - あくまで「原則」のみであり、「ルール」までは規定せず
 - 権利章典という「原則」については立法勧告を受けているが、「ルール」については業界ごとの行動規範を策定、自主規制を行う
 - EUデータ保護規則案とは「原則」は共通する部分も多いが、「ルール」が法規制か、自主規制か、の面で異なる

3-3. 米国「消費者プライバシー権利章典」 7原則

1. 個人のコントロール

●消費者は、企業が自分からどのような個人データを収集し、どのように利用するかについてコントロールする権利を有す。

2. 透明性

●消費者は、プライバシー及びセキュリティ・プラクティスに関して容易に理解でき、アクセスできる情報の提供を受ける権利を有す。

3. コンテキストの尊重

●消費者は、自分が個人データを提供したコンテキストと統合的な仕方で企業がデータを収集し利用し提供することを期待する権利を有す。

4. セキュリティ

●消費者は、個人データのセキュアかつ責任ある取扱いを受ける権利を有す。

5. アクセスと正確性

●消費者は、使用可能なフォーマットで、またデータのセンシビリティ、及びデータが不正確であった場合に消費者が負の影響を受けるリスクに適合した仕方で、個人データにアクセスし、修正する権利を有す。

6. 焦点を絞った収集

●消費者は、企業が収集及び保持する個人データに合理的な制限を設ける権利を有す。

7. 責任(Accountability)

●消費者は、企業が消費者プライバシー権利章典への遵守を保証するための適切な措置を伴って、それらの企業による個人データの取扱いを受ける権利を有す。

3-4. 米国のプライバシー・フレームワーク(2)

②FTC「急速に変化する時代における消費者プライバシーの保護」(1)

● 2012年3月公表、民間分野のプライバシー・フレームワーク

ー 対象企業（別途、対象除外の条件もあり）

- ・特定の消費者、コンピュータ、又はその他の端末に無理なくリンク可能な消費者データ(reasonably linkable data)を収集したり利用したりする全ての企業等(commercial entities)に適用

**※「個人データ」＝「個人等に無理なくリンク可能なデータ」
(reasonably linkable data)**

企業が次の3つの条件を満たせば、「無理なくリンク可能なデータ」ではない。

- (i) データが脱-識別化されたことを保証する合理的な措置を取っている
- (ii) 当該データを再識別化しようとしないうちに公的にコミットしている
- (iii) データ受領者が当該データを再識別化しようとすることを契約で禁止している

3-5. 米国のプライバシー・フレームワーク(2)

②FTC「急速に変化する時代における消費者プライバシーの保護」(2)

ー 要求するベストプラクティス

①プライバシー・バイ・デザイン、②選択の簡略化、③透明性の向上

ー 実施勧告

①立法勧告

・FTCは、議会にベースラインとなるプライバシー立法を考慮するように要求しており、またデータセキュリティとデータブローカーに関する立法を再度要求

②5つの重点領域

・FTCは、2013年にかけて下記領域での自主規制の取組みを促進
(i)「※Do Not Track」、(ii)モバイル、(iii)データブローカー、
(iv)巨大プラットフォームプロバイダー(ISP,OS,ブラウザ,ソーシャルメディア等)
(v)実施可能な自主規制行動規範の促進

※Do Not Track: 行動ターゲティング広告ネットワークに対して、自分のオンライン行動のトラッキングを拒否できるメカニズム。

3-6. OECDのプライバシーガイドライン見直し

OECDプライバシーガイドライン（1980年採択）

- プライバシー8原則含む。日本の個人情報保護法の基盤ともなっている。
 - ・収集制限の原則
 - ・データ内容の原則
 - ・目的明確化の原則
 - ・利用制限の原則
 - ・セキュリティ保護措置の原則
 - ・公開の原則
 - ・個人参加の原則
 - ・責任の原則

OECDプライバシーガイドライン見直し（2013年見直し版公表予定）

- ソウル閣僚宣言（2008年）において、「技術、市場、利用者行動の変化とデジタル・アイデンティティの重要性の拡大の観点」から、ガイドラインの見直しが要求され、現在取り組み中。2013年に見直し版を公表予定。
- 8原則自体は変更せず、ガイドラインに新たな項目を追加する見通し。
 - ・企業によるプライバシー・バイ・デザインの実施
 - ・十分な権限を持った監督機関の設置 等

3-7. APECの越境プライバシールール(CBPR)

APECプライバシールール・フレームワーク(2004年採択)

- 9つのプライバシールール原則から成る。

越境プライバシールール執行のための協力取決め(CPEA)(2010年発効)

- APEC内で、各国のプライバシールール執行機関のネットワークを通じて、プライバシールール法令の国境を越えた執行協力を行うための取決め。これまで、カナダ、オーストラリア、中国香港、ニュージーランド、米国、日本の執行機関が参加。

APECの越境プライバシールール(CBPR)(2011年11月公表)

- APEC内で、企業・組織が国境を越えて個人データを移転するためのルール。
- 個人データを越境移転しようとする企業は、APECのプライバシールール9原則に基づく行動規範を開発し、責任団体による第三者認証を受ける必要がある。
- 責任団体は公的機関でも民間団体でも良いが、APECによる認定が必要。

【4】 JEITAにおける対応について

4-1. JEITA(電子情報技術産業界)における対応について

短期的対応

- EUデータ保護規則案への意見発信
 - 意見書作成
 - 国内外の関係機関と連携
 - EU関係先への意見提示

中・長期的対応

- 日本におけるプライバシー保護のあり方を業界の視点で検討
 - 世界的なプライバシー保護の潮流把握と国際的調和の検討
 - 新たな時代におけるデータの保護と活用の最適なバランス検討

4-2. 短期的対応(EUデータ保護規則案への意見(1))

基本的スタンス

□人、物、金、情報といった経営資源が国境を越えて流通する時代の企業活動におけるグローバルなデータ保護のルール

- ・第一に、解りやすく透明であること
- ・第二に、国内外を問わず公平であり調和が取れていること
- ・第三に、実行可能であり実効性があること
- ・第四に、企業活動を過度に抑制したり企業に過剰な負担を強いるものではないこと

□以上のような観点から、各国間または国際機関の場で関係者による議論が活発に行われ、現代の社会環境に適合した個人データの保護と活用に関する国際的なフレームワークが形成されていくことを望む

4-3. 短期的対応(EUデータ保護規則案への意見(2))

逐条ごとの意見(要望)概要

●第3条 EUデータ保護規則の域外適用

- 例えば、商品やサービスの提供範囲にEU加盟国が含まれない旨をサイト上で明示している場合は適用対象とならないなど、適用対象とみなされない為の条件の明確化

●第4条 個人データの範囲

- 識別番号、位置データ、オンライン識別子等の「グレー」なデータがどのような場合には個人データとみなされないか、すなわち管理者や処理者があるデータに対してどのような措置を行っていれば当該データの処理にあたって個人データとして保護することの義務を免除されるかを明確化

●第7条 明確な同意の取得

- プライバシーポリシーの透明性を高めるためには、本人が同意を与える「データ処理の目的」について、内容を分類して標準化し、プライバシーポリシー内では目立つ形で表示するようにすべき

4-4. 短期的対応(EUデータ保護規則案への意見(3))

逐条ごとの意見(要望)概要

●第7条第4項 従業員データの合法的処理

□雇用者が正当な目的で**従業員データの処理を行う際の処理の合法性**は、第6条第1項(b)の「データ主体が当事者であるような契約の履行のために、又は契約締結に先立ちデータ主体の請求に対処するために処理が必要なとき」または第6条第1項(f)の「管理者が追求する正当な利益の目的のために処理が必要なとき」のいずれかの適用によって担保されると考えられるが、もしそうであるならば、その旨を明示してほしい。

●第17条 忘れられる権利、同意を撤回する権利

□**消去対象となる個人データの範囲**は、民間企業が個人データの処理を伴う製品やサービスを開発する上で、とりわけ個人データの管理方法を設計する上で、データ主体の消去請求に対して適切な措置を取れるようにするために極めて重要である。したがって、これについては**委任法令や実施法令等の中で明確化**してほしい。

4-5. 短期的対応(EUデータ保護規則案への意見(4))

逐条ごとの意見(要望)概要

●第18条 データポータビリティの権利

- 個人の権利を保護するために一定の形式で入手できるデータは、本人のプロフィール情報(氏名、性別、年齢、住所、写真、趣味等)や書き込み内容に限定するべきであり、本人のサイト閲覧履歴や購買履歴といったログデータまで対象とするべきではない。

●第23・30条 データ保護・バイ・デザイン/バイ・デフォルト及び処理のセキュリティ

- このような委任法令・実施法令においては、民間企業の事業内容や事業規模に応じて過度の経済的負担とならないように、実行可能な技術の適用に配慮した合理的な標準や基準を策定してほしい。また、民間の標準化団体を含む国際的な場での議論やコンセンサスとも調和の取れたものとしてほしい。

4-6. 短期的対応(EUデータ保護規則案への意見(5))

逐条ごとの意見(要望)概要

●第31・32条 データ違反時の監督機関及び本人への迅速な報告・連絡

- 個人データ違反の発見の第一報(データ違反の種類、分かる範囲での概要、およびデータ保護オフィサーの連絡先)は24時間以内に行うとしても、別途規定された詳細内容については内部でのオーソライズが取れ次第、不当な遅滞なく監督機関に通知するといった、より実行可能な要件に変更してほしい。
- データ主体への影響が軽微であるために監督機関への通知や本人への連絡の義務が免除されるケースについて、明確化してほしい。

●第39条 認証メカニズム、データ保護シールについて

- 今後、EUのレベルで当該制度を具体化していくにあたっては、さまざまな国々の既存制度を参考にして頂き、とりわけそれらの制度との相互承認に向けた検討を行って頂きたい。

4-7. 短期的対応(EUデータ保護規則案への意見(6))

逐条ごとの意見(要望)概要

●第41条 第三国移転と十分性決定

- 日本のプライバシーマークと、第39条にいう欧州レベルのデータ保護シールとの相互承認が行われた場合には、**プライバシーマークの認証**を受けているということが、第42条第1項にいう「**適切な安全管理措置**」に該当するようにしてほしい。
- または、**プライバシーマーク等のデータ保護シールの認証**を受けることが、第41条第1項にいう第三国内の特定の処理分野に対する**十分性決定の条件の1つ**となりうると思われるが、もしそうなのであれば、第41条第2項の中にデータ保護シールに関する記述を追加するなど、条文の中で**その旨を明示**してほしい。
- グローバルで活動する企業は、国境を越えて消費者の個人データを処理する機会がますます増えているため、このような**データ移転に関して、二国間のみならず、マルチリージョン間で調和され、統一された移転方法を必要**としている。このような観点から、中長期的には**データ保護に関する国際基準が整備され、EUにおける十分性決定(第41条)や適切な安全管理措置(第42条)との調和が図られることが望ましい**。

4-8. 短期的対応(EUデータ保護規則案への意見(7))

逐条ごとの意見(要望)概要

●第44条 従業員データの第三国移転

- 日本企業でにとっては、従業員データのみに限って、雇用契約の履行等の正当な目的でEU域内の現地法人から日本の本社に移転するケースが多い。
このようなデータ移転において場合は、**個人の権利が侵害されるリスクは低い**と考えられるため、標準契約条項やBCRよりも**簡易な移転方法**として、例えば本人がデータ移転について同意した場合も可能であることを明示してほしい。

●第79条 監督機関による課徴金

- 年間世界連結売上の2%という課徴金の上限額は過大であるため、**絶対額としての上限額を設けて**ほしい。
- 違反を救済するための監督機関への協力の度合いに応じて決めるものとする」とされているが、その具体的な算定基準は示されていない。第79条において欧州委員会による詳細規定(委任法令や実施法令)の策定は特に予定されていないようだが、このような詳細規定等において**課徴金の具体的な算定基準をぜひ明確に**してほしい。

4-9. 中長期的対応(プライバシーの保護とデータ活用のバランスのあり方検討)

日本国内

★国際的潮流をふまえながら、
プライバシーの適切な保護と
データ活用のバランスのあり方
を検討していく。

- 個人情報保護法の検討
- プライバシーマークの検討 等

個人のコントロール権

プライバシー影響評価

マイナンバー法

第三者機関

プライバシー・
バイ・デザイン

匿名化技術

クラウドサービス

ビッグデータ活用

...

...

国際的潮流

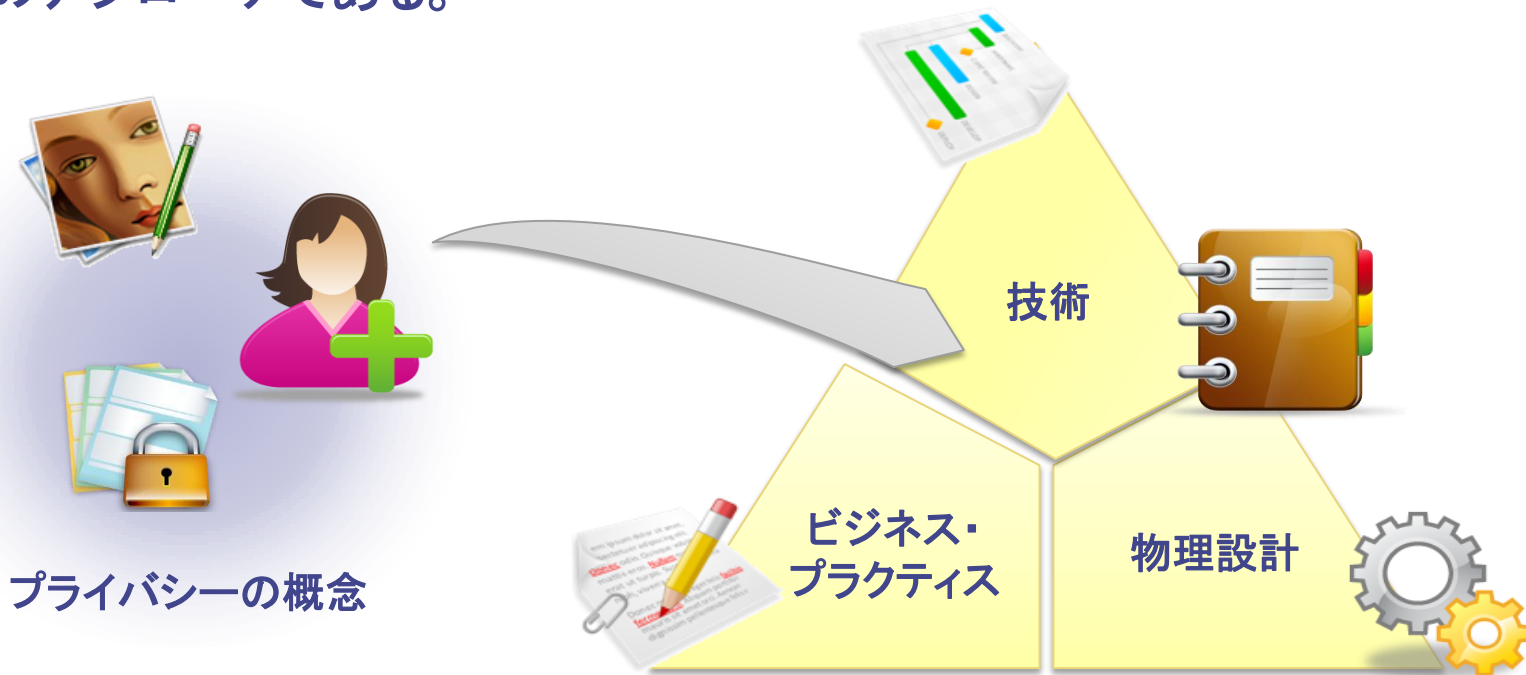
- 欧米等の動向
 - EUデータ保護規則
 - 米国 消費者プライバシー
権利章典 等
- 多国籍機関の動向
 - OECD、APEC 等
- 国際標準の動向
 - ISO 等

【ご参考:プライバシー・バイ・デザイン(PbD) (1)】

■ プライバシー・バイ・デザインとはどういうものか？

JIPDEC

- 1990年代に、オンタリオ州情報・プライバシー・コミッショナーのアン・カブキアン博士が提唱。
- プライバシー・バイ・デザインは、「技術」「ビジネス・プラクティス」「物理設計」のデザイン仕様にプライバシーを埋め込むことで、プライバシーを保護するためのアプローチである。



【ご参考:プライバシー・バイ・デザイン(PbD) (2)】



■PbDの7つの基本原則

- ◆ 7つの基本原則を実践することで、「プライバシーの確保」「個人の自己情報に対するコントロール」「組織の持続可能な競争的利点の獲得」が実現できる。

The 7 Foundational Principles <http://privacybydesign.ca/about/principles/> (2009年)

原則	内容
事前的／予防的	プライバシー侵害が発生する前に、それを予想し予防すること。
初期設定としてのプライバシー	プライバシーを保護することを当たり前の機能として最初から組み込まれていること。
デザインに組み込む	プライバシー対策を、システムおよびビジネス・プラクティス、社会基盤にまで組み込むことで最適化される。
ゼロサムではなく、ポジティブサム	ポジティブサムの「WIN-WIN」のアプローチをとることで、セキュリティとプライバシーを両立させる
徹底したセキュリティ (ライフサイクルを保護)	情報のライフサイクル全体を通してプライバシー対策を行う。
可視性／透明性	情報技術、組織や社会基盤の中でプライバシー対策がどのようになっているか可視化する。また、企業組織の理念、目標に対して独立した検証(第三者による監査など)を行い、透明性を高める。
ユーザーの尊重	個人の利益を尊重し、適切な通知、権限委譲、およびユーザープライバシー対策について選択可能な状態で提供する。

【ご参考:プライバシー・バイ・デザイン(PbD) (3)】

■PbDに基づいた全身イメージングの例

【ビジネス・プラクティス】

- 不安や不信を抱く旅行者には、この検査を拒否し、これまでの金属探知機等による検査を選ぶ自由が与えられる。

【技術】

- 裸に近い画像を外形表示に変換して表示される。
- 画像は保存せず破棄される。



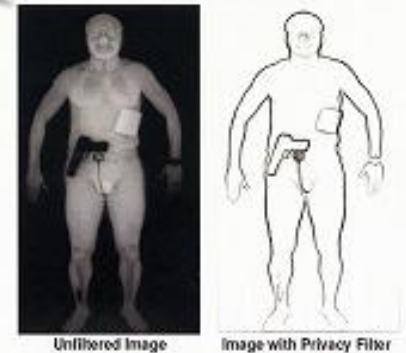
チェック



異常

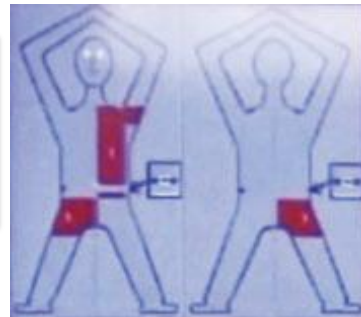


Smart Check 参考画像



【技術】

- 変換された画像をさらにあいまいにした画像で確認する。



【物理設計】

- 監視員は搭乗客が見えない場所(別室)で分析し、搭乗客と画像を見比べることが出来ない。
- 搭乗客と同性の監視員が作業。
- 携帯電話持ち込み禁止。

プライバシー・バイ・デザインは、世界的に認められている

ご静聴有難うございました。

JEITA

Japan Electronics and Information Technology Industries Association