資料3

EU、米国における
個人情報・プライバシー保護等に関する制度の
概要

プライバシー保護に関する制度（EU）

個人データ保護指令（95年）
「個人データ処理及びデータの自由な移動に関する個人の保護に関する指令（95/46/EC）」

分野横断的な個人情報保護に関する規制

（主な内容）
（1）データ内容に関する原則（特定された明示的かつ適法な目的のための取扱い等）
（2）データ取扱いの正当性の基準（データ主体の明確な同意等）
（3）センシティブデータ※の取扱い ※人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入、健康又は性生活に関するデータ
（4）データ主体のデータへのアクセス権
（5）取扱いの機密性及び安全性
（6）第三国への個人データの移転に関する規律（第三国が十分なレベルの保護措置を確保していることを条件とする等）
（7）独立した監督機関

e-プライバシー指令（02年、09年改正）
「電子通信部門における個人情報の処理とプライバシーの保護に関する指令（2002/58/EC）」

電子通信部門に関する個人データ保護指令の特則

（主な内容）
（1）通信の秘密保持
（2）Cookieの利用に当たって内容を明示しオプトインによる利用者同意を求める
（3）ロケーションデータを利用する際にオプトインによる利用者同意を求める

英国
データ保護法

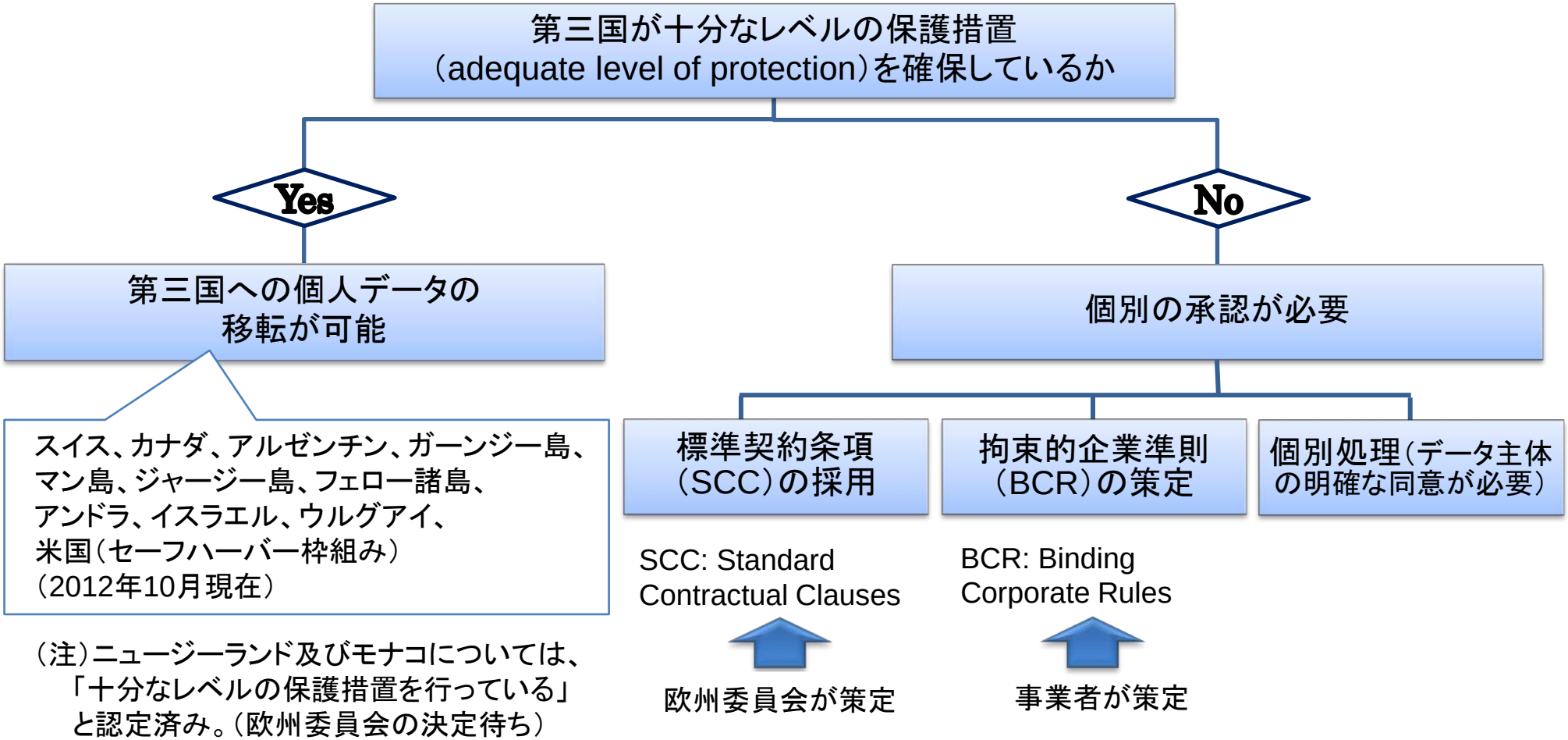
フランス
情報処理、情報ファイル及び自由に関する法律

ドイツ
連邦データ保護法

イタリア
個人データの処理に関する個人その他の主体の保護に関する法律

等

EUから第三国への個人データ移転



個人データ保護規則の枠組み

個人データ保護指令（1995年）

↓

e-プライバシー指令（02年、09年改正）

- 急速な技術進展
- 情報の共有・収集の規模の劇的な増加

↓

個人データ保護規則案（12年1月）

立法手続きを開始

① EU域内における規制の単一化・簡素化

② より強固な個人データ保護ルールの整備

③ データ保護に関するグローバルな課題への対応

- 国内法制化の不要な「規則」に変更
- 一国からの承認を得れば、他国の当局からの承認は不要
- データ保護当局間の調査協力のメカニズム

より強固な個人データ保護ルール(②)

事業者

個人データ

個人

「プライバシー・バイ・デザイン」原則

- 新サービスの導入時、データ保護への考慮の義務付けの導入
- 個人の権利や自由に対するリスクを伴う個人データの取扱いを行うに当たって、当該取扱いが個人データの保護に対して与える影響度の評価(PIA: Privacy Impact Assessment プライシー影響評価)を実施する必要がある旨の規定
- 「データ保護職員」の任命義務(250人以上の従業員の雇用などの要件を満たす事業者が対象)

個人データ漏えい時の通知義務

- データ保護当局に対しては可能な場合24時間以内に、個人に対しては当該個人プライバシー等に悪影響を及ぼす可能性がある際には遅滞なく通知

忘れられる権利

- データ削除に関する現行法令における個人の権利をより明確化するとともに、データ管理者は、ネット上での個人データへのリンクやコピー・複製された個人データについて、当該個人から削除要求があった場合、当該要求を(それらデータを扱う)第三者に対して通知するなど、あらゆる合理的手段を講ずる義務がある旨規定

データ持ち運びの権利

- 共通化されたフォーマットで電子的に自らのデータのコピーをデータ管理者から取得できるとともに、自らのデータをあるアプリケーションから別のアプリケーションに移転させることができる権利について規定

同意の明示

オプトイン原則

- 個人データの取得に当たって必要な同意は明示的な(explicit)ものであることを要する旨の規定

プライバシー・バイ・デザイン

プライバシー・バイ・デザイン（PbD：Privacy by Design）

カナダ　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1990年代に開発した概念

7つの基本原則

1. 事後的ではなく、事前的；　救済的でなく予防的
2. 初期設定としてのプライバシー
3. デザインに組み込まれるプライバシー
4. 全機能的　－　ゼロサムではなく、ポジティブサム
5. 最初から最後までのセキュリティ
   － すべてのライフサイクルを保護
6. 可視性と透明性　－　公開の維持
7. 利用者のプライバシーの尊重
   － 利用者中心主義を維持する

プライバシー影響評価（PIA：Privacy Impact Assecemnet）

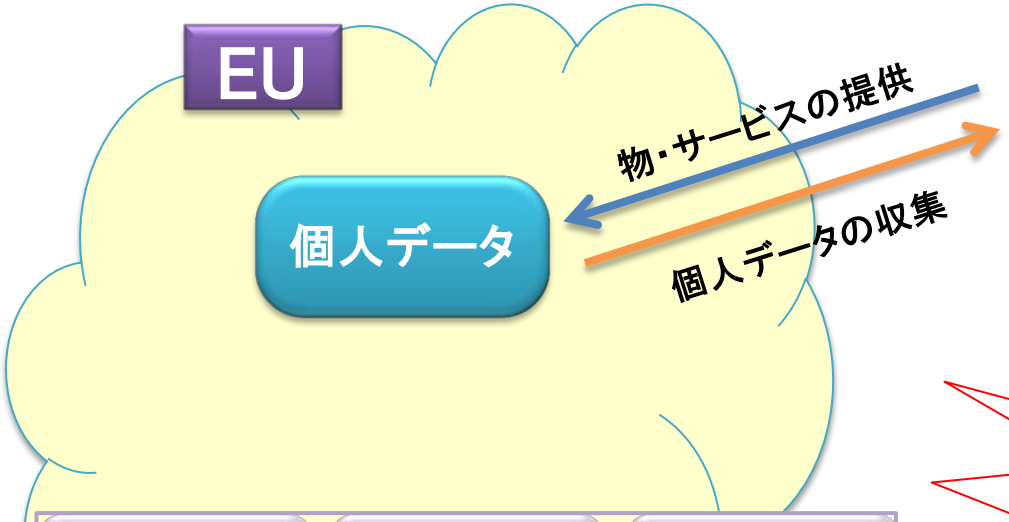
個人情報の収集を伴う情報システムの導入にあたり、プライバシーへの影響度を「事前」に評価し、その構築・運用を適正に行うことを促す一連のプロセス

プライバシー・バイ・デザインの実施プロセス

1. プライバシー要件を作成する
2. 個人に関する情報の流れを確認する
3. プライバシー要求仕様を開発する
4. プライバシー要求仕様を設計に盛り込む
5. 開発方法へ適用する
6. テストして確認する

プライバシー影響評価（PIA）を活用

個人データ保護に関するグローバルな課題への対応（③）



域外事業者

- 個人データ保護規則の域外適用
- EU域内に代理人を置く必要（一定の要件を満たす場合）

規則に違反した場合（域内事業者を含む）

制裁（課徴金）

最大で、100万ユーロ、又は事業者の全世界での売上高の2%相当額の課徴金

	現指令 →	規則案
標準契約条項（SCC）	データ保護当局の承認	承認不要
拘束的企業準則（BCR）	少なくとも域内3国の当局の承認	域内の一当局からの承認
個別処理	各国当局の承認	保護当局の事前承認

プライバシー保護に関する制度（米国）

分野横断的な個人情報保護法は存在しない

政府部門	健康情報等	信用情報	通信分野	金融部門	児童のプライバシー
	（民間部門）				
プライバシー法（Privacy Act of 1974）	医療保険の相互運用性及び説明責任に関する法律（HIPPA）	公正信用報告法(FCRA)	電子通信プライバシー法（ECPA）	金融サービス近代化法（Gramm-Leach-Bliley Act）	児童オンラインプライバシー保護法（COPPA）

自主規制

セーフハーバーの枠組み（2000年7月）

商務省

セーフハーバー原則

① 告知：利用目的等の告知
② 選択：オプトイン、オプトアウトの機会の提供
③ 第三者への提供：告知と選択の原則の適用等
④ セキュリティ
⑤ データの完全性
⑥ アクセス；開示、訂正、変更、削除請求
⑦ 執行

企業

- セーフハーバー原則遵守の宣言
- プライバシーポリシーを公表
- セーフハーバー原則の遵守の確約書を商務省に提出
- 商務省は当該企業名等をウェブサイトに掲載

FTC

【違反行為が発覚した場合】

- 「不公正又は欺瞞的な行為又は慣行(unfair or deceptive acts or practices)」（FTC法第5条）として、排除措置・課徴金等の対象
- 民事責任も問われる。

消費者プライバシー権利章典

米国政府発表：“ Consumer Data Privacy in a Networked World ” (12年2月23日)

個人プロファイリングを念頭

「消費者プライバシー権利章典」(A Consumer Privacy Bill of Rights)

1　個人による管理　：消費者は、自分の個人データを企業が収集し、それを使用する方法について管理する権利を有する。

2　透明性　：消費者は、プライバシー及びセキュリティの企業実務に関する情報に容易に理解しアクセスできる権利を有する。

3　経緯の尊重　：消費者は、企業が、自分の個人データを、自分が情報を提供した経緯に沿う方法で、収集、使用、開示することを期待する権利を有する。

4　セキュリティ　：消費者は、個人データを保護し、責任持って処理する権利を有する。

5　アクセス及び正確性　：消費者は、使用可能な形式で、また、データの機微性及びデータが不正確であった場合に消費者に悪影響を与える危険度に応じた方法で、個人データにアクセスし訂正する権利を有する。

6　対象を絞った収集　：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る。

7　説明責任　：消費者は、この権利章典の遵守を保証するための適切な措置を講じる企業によって個人データが処理される権利を有する。

Do Not Track（オプトアウト原則）

関係者間プロセスの強化

- 行動規範を採用するかどうかは企業が最終判断
- 遵守を公言した企業が違反した場合、FTCは行動規範に基づき、執行可能。

連邦取引委員会（FTC）の執行能力の向上

国際的な相互運用性の促進

- 相互認証・執行協力が必要

FTCによる消費者プライバシーの保護の取組み

FTC報告書（12年3月）
“ Protecting Consumer Privacy in an Era of Rapid Change ”

米広告業界は反発

IE 10(MS)、Mozilla（FF）は、DNTをデフォルト

対象企業

- 特定の消費者、コンピュータ、その他デバイスと合理的に関連付けられる消費者データを収集したり、利用したりする企業(commercial entity)
- ただし、年間5,000名未満の消費者のセンシティブでない消費者データのみを収集し、かつ、その消費者データを第三者と共有しない企業については含まれない

企業行動枠組み

① 計画的なプライバシー保護の実施 (Privacy by Design)
② 消費者への簡潔な選択肢の提供
③ 透明性の確保

FTCによる支援 (2013年末までを想定)

① 追跡拒否(Do Not Track)
② 携帯電話
③ データ販売業者(ブローカー)
④ 大規模プラットフォームプロバイダー
⑤ 法執行可能な自主規制規範の推進

・FTCは規制導入に前向き
・個人情報検索サイト Spokeo に対して 80 万ドルの罰金（12年6月）

プライバシー保護に関する主要6社による自主的な取り組み

主要6社

アップル、アマゾン、グーグル、
ヒューレッド・パッカード
マイクロソフト、リサーチ・イン・モーション

共同声明
（12年2月）

カリフォルニア州司法長官
カマラ・ハリス氏

アプリケーション開発者

提供

・プライバシーポリシーを提示
（パーソナルデータの収集方法・用途・提供先を示す）

モバイルアプリマーケット事業者

・アプリケーション開発者が、アプリケーションを提出する際、そのプライバシーポリシーへのリンク又はテキストを提出できるようにする

購入

・利用者が、アプリケーションの購入時等にアプリケーションストアからプライバシーポリシーにアクセスできるようにする

消費者

（注）主要6社は、国境を越えたサービスも提供できるため、本質的にグローバルな効果を有する。

米国・EU間の政策対話

○ 米国ブライソン商務長官とEUレディング欧州委員会副委員長が共同声明を発出（2012年3月19日）
○ 以下の3点について、米国とEUが認識を共有。
・個人情報保護に係る個人の権利促進と商業情報プライバシー制度の相互運用性の円滑化への責任
・セーフハーバー協定の枠組みが、さらなる相互運用性の向上のための出発点となること
・プライバシーの課題への対応策についてのグローバルなコンセンサス作りへ向けて取り組むこと

（共同声明の抜粋）

「米国及びEUは、個人情報を保護するための個人の権利の促進及び商業的な情報プライバシー制度の相互運用性の円滑化への責任感を明確に共有する。」（第1段落）

「データ保護におけるより強力な環大西洋の協力は、消費者の信用を高め、グローバルなインターネットエコノミーの持続的成長、進化する環大西洋のデジタル市場を促進する。」（第2段落）

「双方は、両者で、また、国際的なパートナーとともに、プライバシーを保護するための相互認証の枠組を創設するために協力して取り組むことにコミットしている。双方は、個人情報保護の分野における基準は、国境を越えた情報・物・サービスの自由な流通を円滑化するものであるべきと考えている。」（第4段落）

「我々は、次々に生じるプライバシーの課題への対処策についてのグローバルなコンセンサス作りに向けて、他国の利害関係者とも一緒に取り組んでいきたいと考えている。」（第5段落）

「米国とEUは、セーフハーバー協定に関する各々のコミットメントを改めて確認する。この枠組みは、さらなる相互運用性の向上のための有益な出発点である。・・・(中略)・・・欧州委員会及び商務省は、この枠組みが前進的にアップデートされるよう、引き続き米EUの緊密な協力に期待する。」（第6段落）