資料 7

諸外国における現状

平成２４年２月８日

事務局

諸外国等における個人情報保護制度及び監督機関

	法律名（制定年）	主な監督機関名 （設置年）	法的位置付け
米国	連邦プライバシー法（1974年制定） 連邦取引委員会（FTC）法 公正信用報告法（FCRA） 金融サービス近代化法(GLBA) 児童オンラインプライバシー保護法(COPPA) 等	連邦取引委員会（FTC）（1915年） ※その他多数の機関が関わっている。	独立行政委員会 （委員数：５人）
カナダ	連邦プライバシー法（1982年制定） 個人情報保護及び電子文書法（PIPEDA法）（1999年制定）	連邦プライバシー・コミッショナー（1982年）	特殊オンブズマン （プライバシー・コミッショナー：１名）
EU	1995年個人データ保護指令 2002年e-プライバシー指令	欧州データ保護監督官 29条作業部会	
英国	1998年データ保護法 （1984年データ保護法を改正）	情報コミッショナー （2001年、前身は1984年）	女王から独立した単独法人 （情報コミッショナー：１名）
仏国	情報処理、情報ファイル及び自由に関する法律（1978年制定／2004年改正）	情報処理及び自由に関する国家委員会（CNIL）（1978年）	独立行政委員会 （委員数：17名）
ドイツ	連邦データ保護法(2009年度最終改正）	連邦データ保護・情報自由監察官（1977年） 州プライバシーコミッショナー等	連邦議会によって選任され、大統領が任命（監察官：１名）
韓国	個人情報保護法（2011年） 情報通信網利用促進及び情報保護等に関する法律（1999年制定／2001年改正）	個人情報保護委員会 （2011年）	諮問機構と行政機構の両者の性格を有する（委員数：15名）

（消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書（平成23年3月）」に基づき、総務省作成）

１．米　国

連邦取引委員会(FTC)法　第5条の概要

連邦取引委員会(FTC: Federal Trade Commission)

- 米国では、個人情報・プライバシー全般を所轄する統一的な第三者機関は存在せず、各個別法において分野別の個人情報に関する第三者委員会が定められている。
- 連邦取引委員会(FTC)は、消費者保護に関する職務・権限(FTC法第5条で規定)を担う独立の機関として消費者のプライバシー保護を図る。
- インターネット上の個人情報全般に関しては包括的な立法が行われておらず、FTCが業界全体を監視しつつ、自主規制を促す形でルール形成。

連邦取引委員会法(FTC法)第5条(a)

- 以下の行為を禁止:
  ①不公正な競争方法(unfair methods of competition)
  ②不公正・欺瞞的行為又は慣行(unfair or deceptive acts or practices)

  → ②で禁止される行為又は慣行には、消費者のプライバシー侵害、不適切な広告表示も含まれる。
- 違反行為に対する措置: 差止請求(第5条(a)(2))、排除命令(第5条(b))、民事制裁金(1万ドル以下)(第5条(m)(1)(A))

オンライン・プライバシーの規律

- **オンライン広告との関係**
  オンライン広告のプライバシー問題について、FTCは自主規制中心の対応を行う姿勢を示してきた中で、サービス運営者のプライバシー・ポリシーを重視。プライバシー・ポリシーに反する行為を行った企業に対しては、FTC法第5条に基づき民事訴訟を提起し、差止めや賠償金の支払い等を求めている。

  ⇒ *自主規制への規律付けとして、FTC原則(4原則)を策定*

米国FTCスタッフレポート（4原則）（2009年2月）

対象

- オンライン行動広告（異なる時間に行われたオンライン上での消費者の行動を追跡することにより消費者個々の嗜好に合わせた広告を提供すること）が対象。
- First Party Advertising（※1）、Contextual Advertising（※2）は対象外。
- PII（個人識別情報）と非PIIを区別しない。（どちらも対象）
- 特定の個人や使用するPCや機器に合理的に関連づけが可能となる、オンライン行動広告向けのデータが対象。

※1：第三者とデータが共有されない、自己のサイト内でのデータを使用した広告
※2：広告が一回の訪問履歴や検索結果のみにより行われる広告

4原則

①透明性及び消費者による管理

行動ターゲティング広告のために情報を収集する全てのWeb サイトは、消費者をターゲットとした広告に提供するためのデータが収集される詳細を、明確、かつ、消費者にとってわかりやすく、その目を惹きやすい形で提示しなければならない。また、そのような目的で情報が収集されることの可否を消費者が決定できるようにしなければならない。データ収集が伝統的なウェブサイト外で行われる場合、上記の原則を満たす代替的な方法を提供しなければならない。

②消費者のデータに対する合理的なセキュリティ、データ保持の原則

行動ターゲティング広告のために消費者の情報を収集または保存するあらゆる企業は、当該データに対して合理的なセキュリティを施さなければならない。セキュリティは、データセキュリティ関連諸法や連邦取引委員会によるデータセキュリティ執行のための行動等と同じく、データの機微の程度、当該企業の事業遂行の性質、当該企業が保有するリスク、当該企業が合理的な可能なセキュリティのレベルに応じて決定される。また、当該データは、正当な事業の遂行や法執行において必要な期間に限り保持されるべきである。

③プライバシーに関する同意の実質的変更に当たっての事前の同意再取得

連邦取引委員会が本原則の執行および普及活動で明らかにしたとおり、消費者のデータの取り扱い方および保護の仕方について、企業が消費者との間に行った合意は、仮に事後プライバシーポリシーを変更したとしても遵守しなければならない。そのため、取り決めに定めた利用法と実質的に異なる方法で当該データを用いようとする企業は、事前に影響を受ける消費者から同意を得なければならない。本原則は、企業の買収に当たってデータの収集、使用、共有方法に実質的な変更が生じた際にも適用される。

④行動ターゲティング広告のための機微情報の使用に対する事前同意（または使用の禁止）

企業は機微情報を用いた行動ターゲティング広告を受け取ることについて事前に消費者から同意を得て機微情報を取得した場合に限り、当該広告を行わなければならない。

米国FTC　予備スタッフレポート（2010年12月）
～急速に変化する時代における消費者プライバシー保護～

対象

➢ 特定の消費者、PCやその他端末と合理的に関連付けることが可能な消費者データを収集、または利用するすべての商業主体が対象

新たな枠組みの原則

①Privacy by Design：ビジネス設計段階からのプライバシー保護
→ 企業は、全社かつ商品・サービス開発の前段階で消費者プライバシー保護の取り組みを促進すべき

②Simplified Choice：選択する権利の簡易化
→ 企業は、消費者の選択する権利を分かりやすくすべき
→ 一般的に容認されない行為に対しては、消費者データの収集や利用に先立ち有意義な選択をする権利を提供
→ オンライン行動広告に関して、業界全体を網羅する包括的な消費者の選択する権利を実現する「Do Not Track（追跡拒否）」制度（※）を提案
（※）その手法として、消費者によるサイト毎の登録ではなく、ブラウザ・ベースでの対応を提案

③Greater Transparency：さらなる透明性の確保
→ 企業は、プライバシー告知のさらなる明確化、簡潔化、標準化を行うべき
→ 企業は、消費者データへの合理的なアクセスを提供すべき
→ 企業はデータ収集時点で告知した方法と異なる方法で消費者データを利用する場合、消費者の明示的な合意を得なければならない

パブリックコメントにより提出された意見（450件以上）をFTCは現在考慮中

商務省　消費者オンライン・プライバシー保護に関するグリーンペーパー（2010年12月）
～インターネット・エコノミーにおける商用データ・プライバシー及びイノベーション: 動的政策枠組み～

概要

- 商務省のインターネット政策タスクフォース（IPTF: Internet Policy Task Force）による政策提言の報告書インターネットの持つイノベーション、雇用創出、経済成長への効用を確保しつつ、いかに消費者のオンライン・プライバシーを保護していくかについての政策提言の報告書
- 現在のプライバシー保護法制ではインターネット上での個人情報の利用の進展に十分追いついておらず、FTCが取り組んでいる個人のオンライン・プライバシー保護も十分に機能しているとは言い切れないため、枠組みの見直しが必要

主な提言

◎プライバシー権利章典(Privacy Bill of Rights)として公正情報行動原則(FIPPs: Fair Information Practice Principles)の検討
→FIPPsには、事業者による消費者情報の利用についての透明性確保、データ収集の必要性とそのデータ利用方法の説明、データの明確な利用範囲、監査システム等による説明責任等の向上も盛り込むべき
→国土安全保障省(DHS: Department of Homeland Security）は2008年、1974年プライバシー法基づくFIPPs８原則を採択
８原則：①透明性、②個人の参加、③目的限定、④データ最小化、⑤利用制限、⑥データ品質及び完全性、⑦セキュリティ、⑧説明責任及び監査。

◎プライバシー行為規範(Privacy Codes of Conduct)の検討とプライバシー保護政策室の設置
→同室は、インターネット政策タスクフォースの職務を引き継ぎ、様々な利害関係者との対話を開催するとともに、商用データのプライバシー保護政策の専門機関として機能すべき

◎技術革新と貿易拡大のためのグローバルな相互運用性の導入

◎セキュリティ侵害(breach)報告制度のハーモナイズ

◎クラウドを想定した電子通信プライバシー保護法(ECPA: Electronic Communications Privacy Act)の見直し
→電子通信プライバシー保護法をクラウド等に対応したプライバシー保護となるよう見直すべき。個人のプライバシーを保護し、消費者データへの非合法アクセスや消費者データの公開を取り締まるべき

2. 欧　州

EUにおける個人データ保護に関する制度

主な制度

- **1995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）」**
  （EU個人データ保護指令）
- **2002年「個人情報の処理と電子通信部門におけるプライバシーの保護に関する指令（2002/58/EC）」**
  （e-プライバシー指令）
  →（1）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、
  （2）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　　等
- **2009年「Telecom Reform Package」（e-プライバシー指令の一部改正）**
  →（1）利用者に対するCookie及び個人情報の利用についての分かりやすい説明による事前通知を義務づけ
  （2）利用者のより容易な自己の情報のコントロールに向けた改善
  （3）個人情報の使用目的の明示と目的外使用の禁止

- **EU個人データ保護指令第29条に基づくデータ保護作業部会**
  （1）検索サービス提供会社の検索ログ保存期間に関して審議。09年2月、個人特定可能なIPアドレスがあるログファイル保存期間を6ヶ月とすることで米国主要検索事業者と合意。
  （2）09年6月SNSにおける個人情報保護に関する報告書を公表。EU域外のSNS事業者であっても指令適用を受けうる

EU「個人データ保護規則」案の公表（2012年1月25日）

- より強固な個人データ保護ルールの整備（「忘れられる権利」、「プライバシー・バイ・デザイン」原則等）
- データ保護に関するグローバルな対応（EU域内居住者向けの場合、域外事業者による個人データ取扱いにも法令効力）
- その他：課徴金（企業の全世界での売上高の最大2%相当額）　等

EU個人データ保護規則案の概要①

■ EUの個人データ保護に関する現行基本法令(「個人データ保護指令」(※))に代わる新法令(「個人データ保護規則」)案が、1月25日に公表。1995年の現行法令の採択以来、初の抜本改正。

規則案の概要

※ 個人データの取扱いに関する市民の基本的権利及び自由(特にプライバシー権)の保護、EU加盟国間での個人データの自由な流通の確保の2点を目的とする法令。

◆ 規則案のポイント(現行指令からの主要改正点)は以下のとおり。

(1) EU域内における規制の単一化・簡素化

- EU法令が全加盟国に同一に適用されるよう、国内法制化の不要な「規則」に変更　※EU規則は各国に直接適用
  - ➢ 従来は、各加盟国個別の法制化によってルール適用の在り方に差異が存在
- 事業者による事務負担(行政手続等)の簡素化
  - ➢ 事業者がEU域内のうち一のデータ保護当局の承認を得れば、他国の当局からの承認を不要とする制度を導入
- EU加盟国のデータ保護当局間の円滑な協力メカニズムの創設
  - ➢ EU加盟国のデータ保護当局は、他の加盟国の当局からの求めに応じて調査等の協力を行う制度を導入

(2) より強固な個人データ保護ルールの整備

- 個人データ保護に関する個人の権利の強化
  - ➢ 忘れられる権利(個人の求めに応じ、ネット上にアップロードされた個人データの削除の義務化)の導入)
  - ➢ データポータビリティ(個人がサービスを乗り換える際、事業者は当該個人がアップロードしたデータを当該個人に引き渡す)について規定)
  - ➢ 個人データの取得に当たって必要な同意は明示的な(exploit)ものであることを要する旨の規定　等
- 事業者による個人データ処理に関する説明責任の強化
  - ➢ 「プライバシー・バイ・デザイン」原則(新サービスの導入の際、あらかじめプライバシー対策の考慮を求める)の導入
  - ➢ 個人データの取扱いに当たって、当該取扱いに係るリスクの影響度評価を実施する必要がある旨の規定
  - ➢ 「データ保護官」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
- 個人データのセキュリティの強化
- データ保護に関する個人の権利行使方法の改善
  - ➢ EU加盟国のデータ保護当局の独立性及び権限の強化、行政及び司法による救済策の強化

EU個人データ保護規則案の概要②

（３）データ保護に関するグローバルな課題への対応

- EU域内の居住者に物品・サービスの提供を行う場合、**域外の事業者による個人データの取扱いにも法令の効力を及ぼす**ための規定を整備
  - 一定要件を満たす域外事業者はEU域内に代理人を置くべき旨の規定等導入）
- EU域内から域外の第三国への個人データの転送に関するルールの明確化・簡素化
  - 原則（第三国が十分なレベルの個人データ保護を確保していると欧州委員会が認めた場合に限り、EU域内から当該第三国に対して個人データの転送を行うことが可能）に変更はないが、欧州委員会の認定の基準の一部（独立した監視機関の必要性等）を規則において明記
  - BCR（拘束的企業準則（Binding Cooperate Rules））に基づく個人データの（十分性が認定されていない第三国への）転送に関するルールを簡素化[企業がBCRについてEU域内の一の規制当局から承認を得れば十分である旨を規定]するとともに、BCRが満たすべき要件を規則において明記
  - 標準データ保護条項（Standard Data Protection Clauses。欧州委員会又は加盟国データ保護当局が採択したもの）に基づく個人データの（十分性が認定されていない第三国への）転送については、承認は不要である旨を規定
  - データ管理者とデータ処理者の間の（個別の）契約条項（Contractual Clauses）に基づく個人データの（十分性が認定されていない第三国への）転送については、加盟国のデータ保護当局の承認が必要である旨を規定
  - （BCR等の）長期的・構造的な方法によるものだけはない（アドホックな）個人データの転送に関するデータ保護当局の事前承認についても規定

（４）その他

- 新たな制裁の導入（企業の全世界での売上高の**最大2%**相当額の課徴金）
- 「欧州データ保護ボード」の設置（現行データ保護指令第29条に基づく作業部会を改組）　　等

3. OECD

OECDプライバシーガイドラインの見直しについて

プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告（1980年9月）
（OECDプライバシーガイドライン）
8原則（①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、
⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則）
⇒世界の多くの国の個人情報保護法の立法にその考え方が採用される

・グローバル・ネットワークにおけるプライバシー保護に関する閣僚宣言(1998年）
・プライバシー・オンライン：政策及び実際的ガイダンス(2003年）

インターネット経済の将来に関するソウル閣僚宣言（2008年6月）
プライバシーガイドライン等の適用を「変化し続ける技術、市場動向と利用者の行動及びデジタルアイデンティティの重要性増大に照らして」OECDにおいて評価することを要請

インターネット経済に関するハイレベル会合（2011年6月）
インターネット政策制定の原則に関するコミュニケ

プライバシーガイドライン制定後30年経過した状況変化

・インターネットの発展　クラウドコンピューティングの発展
・収集、利用、保存される個人データの量の増大
・社会的経済的利益の価値とプライバシーに対する脅威
・個人データのグローバルな利用可能性

グローバルに相互運用可能なプライバシー枠組み検討の必要性
⇒ボランティアグループにおいて、議論の枠組みとなる文書を作成中