野村総合研究所

パーソナルデータの保護と利用

2013年2月28日

株式会社野村総合研究所
ICT・ﾒﾃﾞｨｱ産業ｺﾝｻﾙﾃｨﾝｸﾞ部
兼　未来創発センター金融・社会システム研究室

小林慎太郎

はじめに

■スマートフォンやソーシャルメディアの普及とともに、個人に関するデータ（パーソナルデータ）が日々大量に生成されるようになった。ビッグデータビジネスが推進される一方で、データの不正利用をはじめとするプライバシー侵害事件が頻発し、ネット社会への不安が高まっている。

■さらに、センサーネットワークが発達すると、大量のパーソナルデータが生成され、流通するようになる。このデータは個人情報に該当するのか、或いは、個人情報に該当しなければ自由に利用できるのかといった課題を、多くの日本企業は抱えている。

■ビッグデータは、次代の成長領域と目される一方で、プライバシーへの対処が大きな課題の一つである。安心してパーソナルデータを利用・提供できる社会に向けて、生活者の意識変化や欧米の政策動向を踏まえ、「個人情報」の範囲に収まらない「プライバシー」をめぐる課題を指摘し、利用ための適切な保護のあり方を提起する。

本日の発表内容

1. 個人情報とプライバシー

2. ネット社会で生じるプライバシー侵害事件

3. 米国、EUそれぞれの規制強化の動き

4. パーソナルデータの保護と利用のあり方

個人情報、個人に関する情報、プライバシー

■個人情報

- 生存する個人に関する情報であって、当該情報に含まれる　氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）【個人情報保護法による定義】

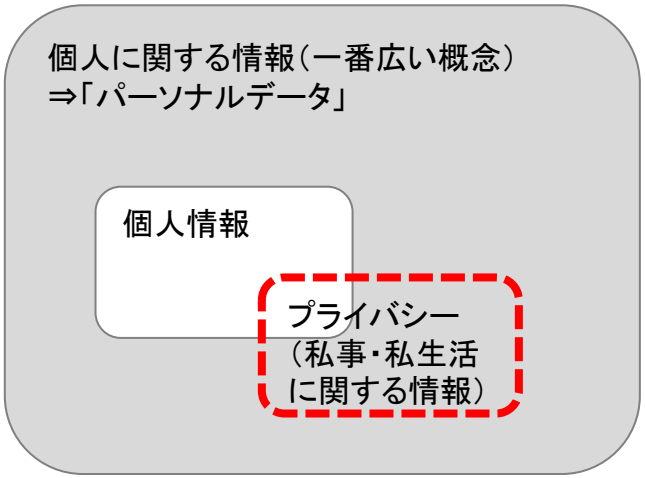
■個人に関する情報（パーソナルデータ）

- 個人に関連する情報を指す最も広い集合
- 個人情報はその集合の一部

■プライバシー

- 個人や家庭内の私事・私生活。個人の秘密。また、それが他人から干渉・侵害を受けない権利【小学館「大辞泉」の引用】
- 法令上の定義はない。

個人情報、個人に関する情報、プライバシーの関係



日米欧のプライバシーに関する規範の起源

■日本：「宴のあと事件」に基づくプライバシー侵害の要件（1964年）

- 私生活上の事実または私生活上の事実らしく受け取られるおそれのあること
- 一般人の感受性を基準として当該私人の立場に立った場合公開を欲しないであろうと認められること
- 一般の人々に未だ知られていないこと

■米国：　ウィリアム・プロッサー（不法行為の権威）によるプライバシー侵害の4類型（1960年）

- 一人で他人から隔絶されて送っている私的な生活状態への侵入
- 知られたくない私的な事実の公開
- 一般の人に誤った印象を与えるような事実の公表
- 氏名または肖像を、自らの利益のために登用すること

■EU：「人権と基本的自由の保護のための条約」第8条で規定されるプライバシー権（1950年）

- (1)すべての者は、その私生活、家族生活、住居および通信の尊重を受ける権利を有する。
- (2)この権利の行使に対しては、法律に基づき、かつ国の安全、公共の安全もしくは国の経済的福利のため、混乱もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他者の権利および自由の保護のため民主的社会において必要な場合以外、公的機関による干渉があってはならない。

ネットをとりまく環境変化が、消費者の個人情報に関する不安を助長し、企業の対応を難しくしている。

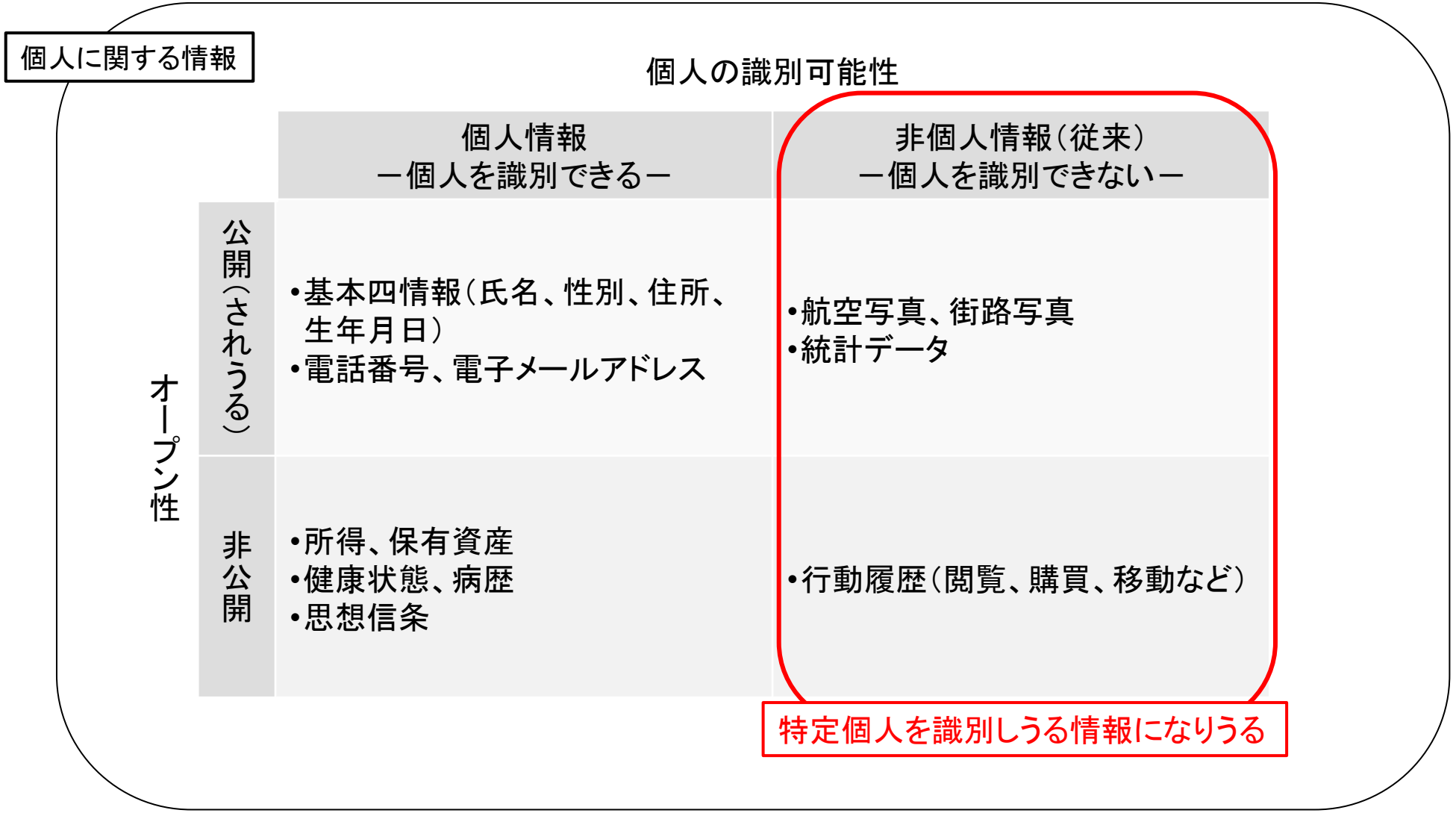
■「容易照合性」（他の情報と容易に照合することができ、それにより特定の個人を識別することができるかどうか）を判断基準に、個人情報と非個人情報が区別されている。

■しかし、3つの環境変化によって、容易照合性による区分は意味をなさなくなりつつある。

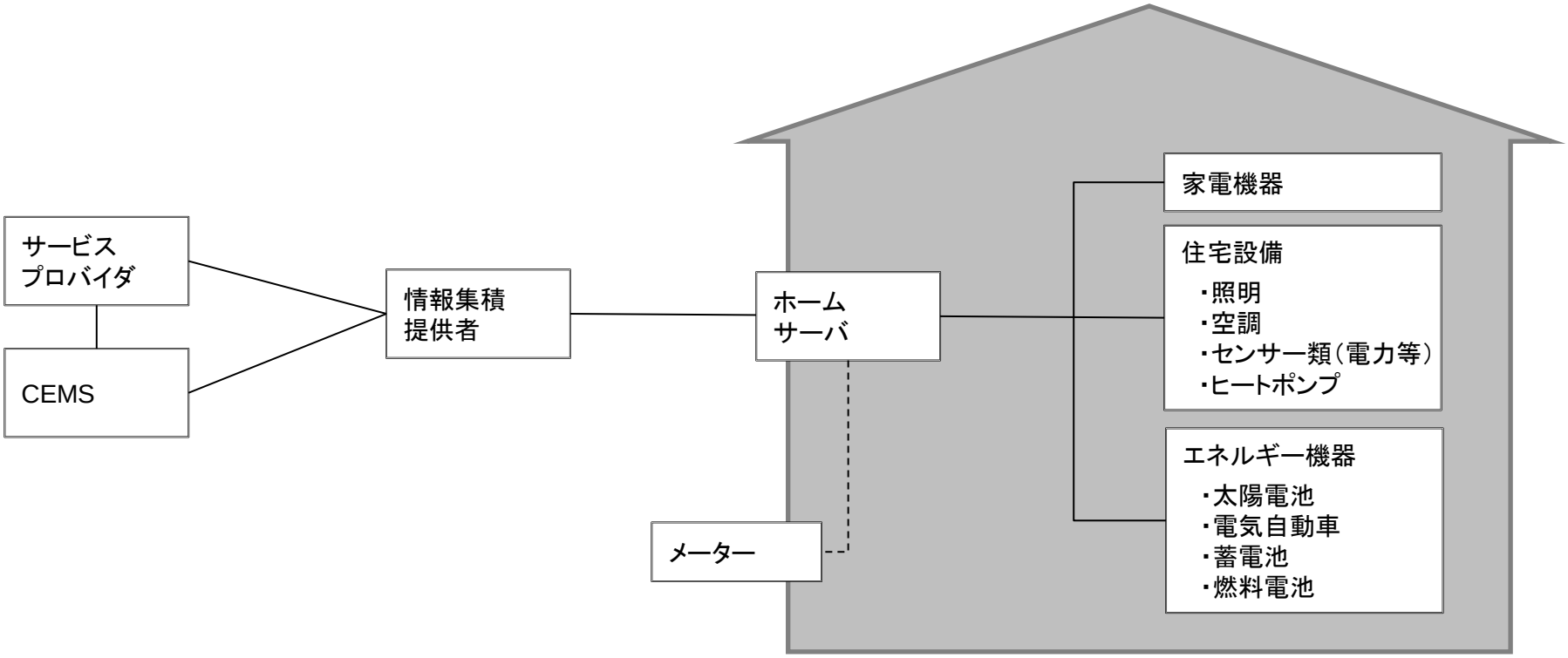
① スマートフォンの普及　⇒行動履歴等の個人に関する情報が大量に自動生成されてネット上を流通
② Facebook等の普及　⇒本人、友人が書き込んだ個人情報そのものがネット上に増大
③ ビッグデータの台頭　⇒ネット上の大量データを処理することで個人の識別が可能に

■これまで非個人情報とされていたものであっても、個人の識別が容易にできる社会となると、消費者はプライバシーが脅かされ、企業は従来の個人情報保護対応の見直しが必要となる。

これまで非個人情報とされていた情報が、他の情報との照合により個人を特定しうる社会になりつつある。



スマート関連ビジネスで収集するデータも、特定の個人を識別する情報となりうる。



行動履歴から特定個人の識別が可能になる事例

■Netflix（全米最大のオンライン映画配信・DVDレンタル事業者）の事例

- 2006年にNetflix社は、顧客の嗜好に合わせて、映画をお勧めする同社のアルゴリズムの精度を向上させることを目的に、100万ドルの懸賞金を掲げたコンテストを実施。同社のアルゴリズムよりも10%以上、推薦精度を向上させた応募者が、懸賞金を獲得できるというルール。
- コンテストの応募者へ、匿名化した約50万ユーザーの過去6年にわたる視聴履歴データを提供。
- コンテスト開始の2週間後に、テキサス大学のグループが、その匿名データから、一部の特定個人を識別したことを発表。
- Netflixは、2回目のコンテストを予定していたが、プライバシー侵害の指摘を受けてとりやめた。

出所）Paul Ohm” BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION” UCLA LAW REVIEW 1701 (2010) より作成

従来の個人情報保護では、ビッグデータ社会におけるプライバシー問題に対処することが困難である。

■個人情報保護法は、「個人情報を保護することで、個人の権利利益を保護する」ことを謳っている。しかし、

- 個人情報と非個人情報とを明確に区別することは難しい。
- ネットビジネスで自動的に収集されるデータは、非個人情報であってもプライバシー侵害につながる可能性がある。
- 非個人情報は、本人の知らぬ間にデータが第三者へ提供され、本人の行動追跡や、人物像を描かれるプロファイリングに利用されている。

⇒ 従来の個人情報保護では、ビッグデータ社会におけるプライバシー問題に対処することが困難。

⇒ 「個人情報」の保護から、「プライバシー」の保護へ、対応の見直しが必要。

１．個人情報とプライバシー

２．ネット社会で生じるプライバシー侵害事件

３．米国、EUそれぞれの規制強化の動き

４．パーソナルデータの保護と利用のあり方

ネットビジネスで生じたプライバシー侵害事件とその類型

国	日本		米国	
サービス名（事業者）	ビューン（ビューン社）	AppLog（ミログ社）	Google Buzz（Google社）	Facebook（Facebook社）
事件の概要	タブレット端末等で、新聞・雑誌の電子版を定額料金で購読できるサービス。 ユーザーの同意なく、閲覧履歴がサーバーに送信されていたことが問題になった。	ユーザーのアプリの使用状況を監視・取得するプログラム。 ユーザーへの説明が不十分なまま、端末にインストールされた全てのアプリの起動履歴情報を、サーバーに送信していたことが問題になった。	ツイッターに類似したミニブログサービス。 ユーザーの事前同意を取得せずに、「Gmail」の情報を「Google Buzz」の初期設定時のユーザー名等に利用したこと等が問題になった。	ソーシャルネットワーキングサービス。 ユーザーに通知することなく、非公開に設定していた情報の公開設定を変更した点、外部アプリ事業者へユーザ情報を提供した点などが問題になった。
事件の顛末	2012年初、ユーザーへの告知文において閲覧履歴の利用目的を明示して同意取得することに変更して対処。	プライバシー侵害による社会的信用喪失のため、2012年4月に会社を清算、解散。	サービスはユーザーの支持を得られず2011年末に終了。監督機関から事業者として是正措置を命じられた。	2011年末に監督機関から事業者として是正措置を命じられた。
問題の類型	✓ 事業者の認識不足やセキュリティ対策が不十分だったことによる問題		✓ 法制度の規制等が曖昧な領域に対する事業者の挑戦による問題	

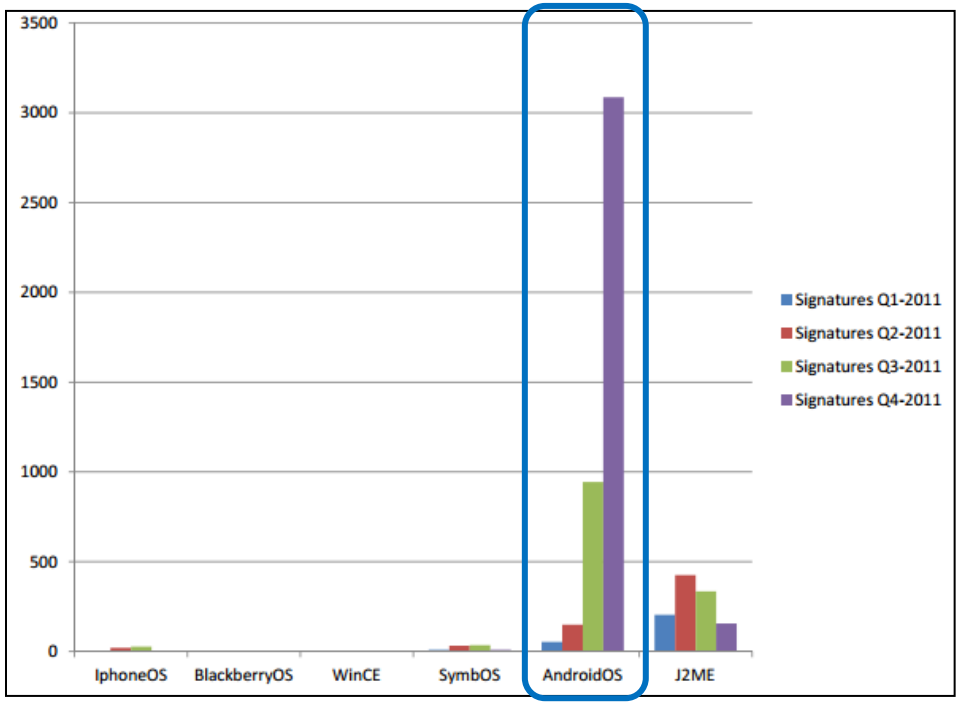
【類型1】
スマートフォンの急速な普及に伴って、過渡的に生じている問題。セキュリティ対策の普及等によって次第に解消されうる。

【類型2】
個人情報やプライバシーの保護に関する制度のあり方が問われている。

2011年後半から、Androidにおける不正アプリが急増

- 2011年度で、Android OS向けアプリで確認された不正アプリは4,000件以上。
- Android OS向けアプリの公式マーケットで発見された、下記の不正アプリのダウンロード件数は7万回以上。

モバイルOS向けマルウェア数



出所）日本スマートフォンセキュリティ協会
「マルウェア対策WG 活動報告」（2012）

Androidの公式マーケットで発見された不正アプリ

項番	特徴	アプリ配布場所における名称	インストール後の名称
1	有名なアプリ、ほかのスマートフォンOSで人気のアプリ名を含む	ウォーリーを探せ the Movie	ユーチューブ動画
		うまい棒をつくろう！ the Movie	youtube 動画まとめ
		ギャングハウンド the Movie	グラビア動画
		スヌーピーストリート the Movie	笑える動画
		チャリ走-the Movie	ようつべ動画まとめ
		ぴよ盛り the Movie	面白動画まとめ
		メガ盛ポテト the Movie	芸能動画
		空手チョップ! The Movie	ニコニコ動画まとめ
		大盛モモ太郎 the Movie	youtube 動画
		桃太郎電鉄 the Movie	ようつべ動画
		魔界村騎士列伝 THE MOVIE	暇つぶし動画
		連打の達人 the Movie	ユーチューブ動画まとめ
2	個人的嗜好をくすぐる文字列を含む	FC2動画まとめ the Movie	怖い動画
		けいおん-K-ON!動画	アニメ動画
		スク水動画まとめ	美人動画
3	実用性を感じさせる文字列を含む	3D 視力回復 THE MOVIE	泣ける動画

出所）IPA
「コンピュータウイルス・不正アクセスの届出状況【2012年4月分】について」

米国連邦取引委員会(FTC)は、Google、Facebookへの是正措置として、長期にわたる第三者監査を義務付け

FTCによる「Google Buzz」事件への措置

- ✓今後20年間、総合的なプライバシー保護プログラムを実施、**第三者による監査**を隔年で実施
- ✓US/EUのセーフ・ハーバー協定に準拠した消費者のプライバシー保護に違反する行為を禁止

FTCによるFacebook事件への措置

- ✓プライバシープログラムの実施、**第三者による監査**を、20年間隔年で実施すること
- ✓ユーザーが情報を消去又はアカウントを停止した場合は、Facebookによる制御によって、適切な期間のうちに、秘匿された情報にアクセスできなくする手段を講じること

しかし、個人に関する情報の活用への挑戦は続いている。

複数サービスのポリシーの一元化、
初期設定における公開範囲の拡大
・・・

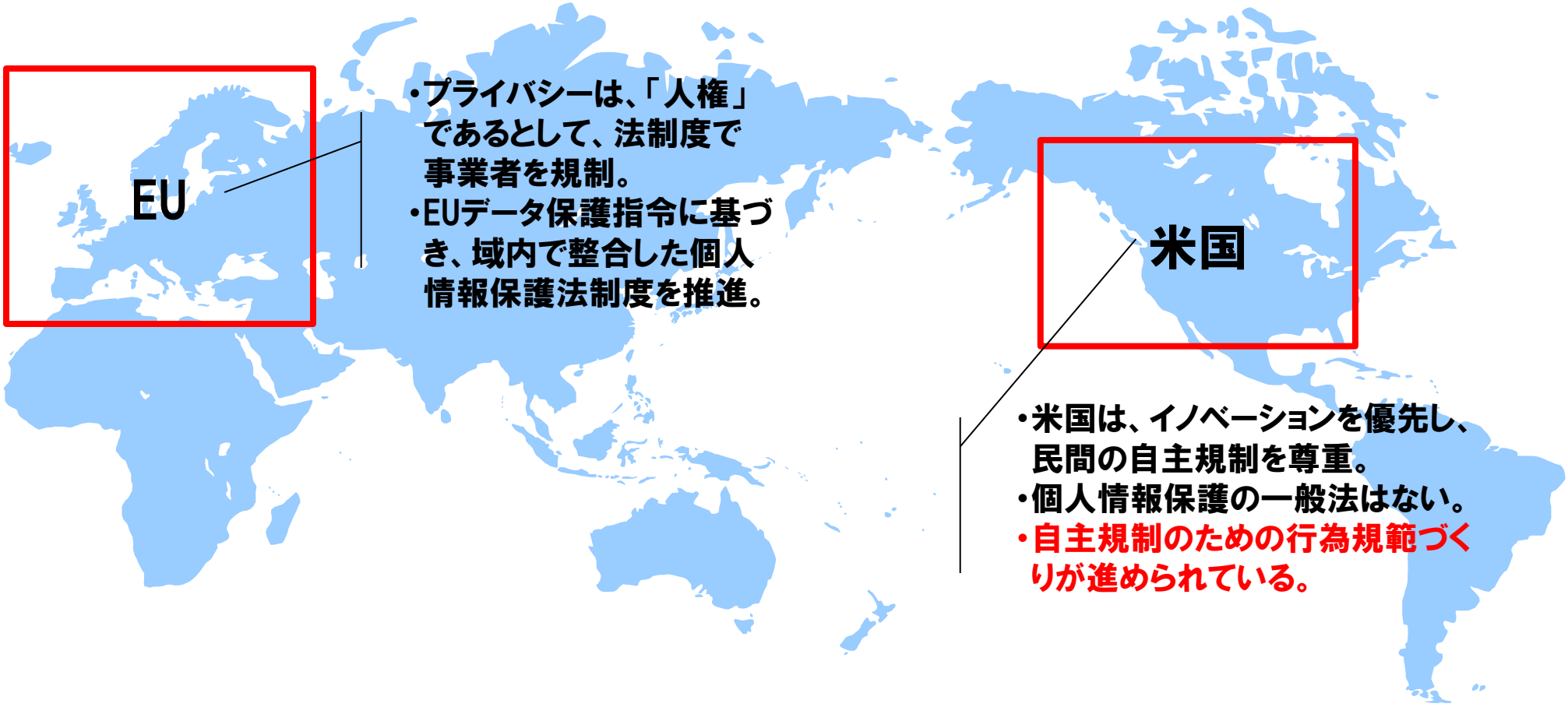
１．個人情報とプライバシー

２．ネット社会で生じるプライバシー侵害事件

３．米国、EUそれぞれの規制強化の動き

４．パーソナルデータの保護と利用のあり方

法制度で規制するEU、自主規制を尊重する米国



2012年初、欧米ではプライバシー保護法制の見直しが大きく進展

■2012年1月、EUでは「EUデータ保護指令（1995）」を刷新した、「EUデータ保護規則案」を発表。EU全域で、厳格なプライバシー保護を推進。

■2012年2月、米国では「消費者プライバシー権利章典」にオバマ大統領が署名。消費者のプライバシー権利を明確化することで、事業者の自主規制に留まらない政策の展開を示唆。

欧米におけるプライバシー法制化の動向

	2011年まで	2012年
EU	● 統一の指令に基づき、構成国がそれぞれ国内法化。 • EUデータ保護指令：95/46/EC	● 「指令」ではなく、「規則」に格上げして、EU全域で統一の法令を適用 • EUデータ保護規則案：General Data Protection Regulation
米国	● プライバシー保護をセクター別に規定 •公正信用報告法：FCRA(1970) •医療保険の相互運用性と説明責任に関する法律：HIPAA（1996）、 •子供のオンラインプライバシー保護法：COPPA（1998） •グラム リーチ ブライリー法：GLBA（1999） 等	●セクターに留まらない消費者のプライバシー権利を明確化。 • 消費者プライバシー権利章典：Consumer Privacy Bill of Rights（2012）

「人権」としてのプライバシー保護をオプトイン※で強化するEU

■EU内事業者が果たすべき義務の追加、EU市民にサービス提供をするEU外事業者に課される義務の新設、「忘却される権利」「データ・ポータビリティ権利」などが新設された。

名称		EUデータ保護規則案
基本思想		人権保護
同意取得の在り方		オプトイン（本人の事前同意の取得を義務化）
特徴	**「自己情報コントロール権」**	透明なプライバシーポリシー（11条）や明示的な同意の取得（7条）、自己情報への容易なアクセスの保証（15条）に加え、**「忘却される権利」（17条）等を通じ、消費者の自己情報コントロール権を強化。**
	セキュリティ	プライバシー強化技術（30条）やプライバシー認証制度（39条）の促進に加え、同規則違反時における、24時間以内の監督機関への届け出義務（31条）等を明示。
	データ管理者の責任	**プライバシー侵害の予防対策をサービス設計段階から講じる「プライバシー・バイ・デザイン」**原則（23条）や**機微情報に係るデータ保護影響評価**（33条）等を通じて、データ管理者の説明責任を強化
	異議申し立ての権利	自動プロファイリングをされた異議申し立てを行う権利（19条）および、**「自動プロファイリングのみに依拠して評価されない権利」**（20条）を規定
	子どものプライバシー	**13歳未満の子どものデータの取扱いについては、親権者の事前同意を義務付け**（8条）
	非EU地域への言及	EU内に事業所がなくとも、EU市民を対象としたサービスを展開する事業者を規制対象と規定（3条）

※オプトイン：事前にユーザーの明示的な同意を取得してから個人情報を利用するルール

プライバシー保護と産業振興の両立を試みる米国

■米国の法制度では、消費者の「自己情報コントロール権」を明確化。また消費者は、自身が意図した脈絡（コンテクスト）に沿って、事業者による個人データの収集・利用・開示が行われることを期待する権利も包含。

名称		消費者プライバシー権利章典
基本思想		産業振興
同意取得の在り方		オプトアウトを容認（本人からの苦情申入れがあった場合における対応を義務化）
特徴	**個人によるコントロール**	消費者は、事業者が収集する**自身の個人データおよび利用目的について、コントロールする権利**を有する。
	透明性	消費者は、事業者によるプライバシーおよびセキュリティ遵守に関する情報について、**容易にアクセスし理解できる権利**を有する。
	脈絡（コンテクスト）の尊重	消費者は、**自身が意図した脈絡（コンテクスト）に沿って、**事業者による個人データの収集・利用・開示が行われることを**期待する権利**を有する。
	セキュリティ	消費者は、個人データが安全に管理され、責任を持って扱われる権利を有する。
	アクセスおよび正確性	消費者は、機微情報や不正確なデータが本人にリスクを与えるような場合、適切かつ利便性の高い方法で、**本人のデータにアクセスし修正する権利**を有する。
	適切な範囲の収集	消費者は、事業者が収集および保持する個人データを適切な範囲に留める権利を有する。
	説明責任	消費者は、個人データが、本権利章典に沿って取り扱われる権利を有する。

EUはCookie指令でオプトイン規制を指向
米国は”Do Not Track”という自主規制

EU

■ 2002年の電子プライバシー指令（2002/58/EC）でCookieの事前同意（オプトイン）を原則とした。この段階では、オプトアウトも許容の範囲。

■ しかし第三者Cookie等によるプライバシー侵害が生じているとして、2009年の改正指令（通称「Cookie指令」）により、ユーザーの事前同意がなければ、Cookie等は利用できない、又はCookie等を拒否する機会をユーザーにわかりやすく提示しないといけないことを義務付け。

■ 指令に基づき、EU構成国は、国内法化して実施。ただし、英国では一部オプトアウトも実質的に認める運用を行っている。

※Cookie:Webサイトの提供者が、Webブラウザを通じて訪問者のコンピュータに一時的にデータを書き込んで保存させるしくみ。
Cookieにはユーザに関する情報や最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができる。

※オプトアウト：事前にユーザーの明示的な同意を取得せずに、ユーザーの個人情報を利用し、本人からの求めに応じてその個人情報の利用を停止するルール。

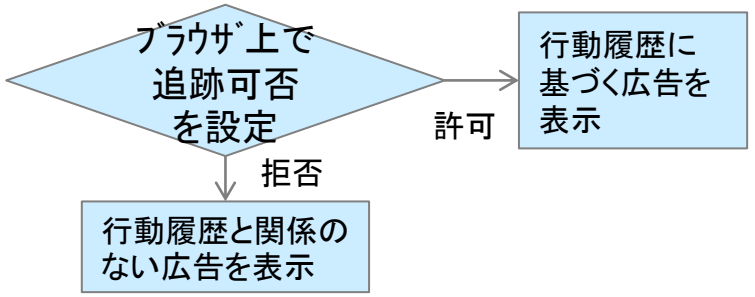
米国

■ 米国では2000年代後半から、“Do Not Track”（追跡禁止）という仕組みによる、オプトアウトを基調とする自主規制を推進。

■ しかし、2012年3月に連邦取引委員会（FTC）は、自主規制が十分でないとして、Do Not Trackの監督強化を宣言。

■ これを受け、Microsoftは2012年6月にインターネットエクスプローラーで“Do Not Track”を初期設定で”on”にする計画を発表。広告業界は、このMicrosoftの動きに反対している。

“Do Not Track”の仕組み

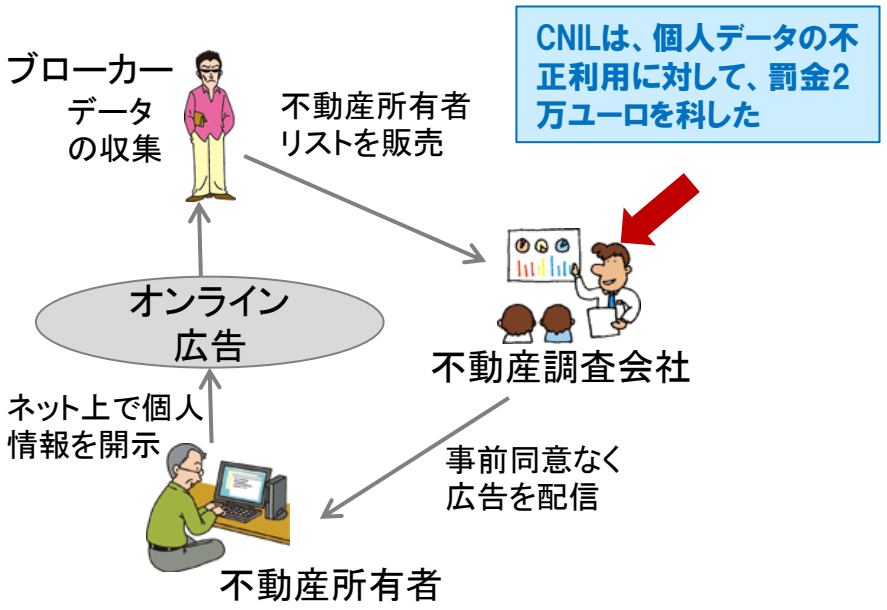


EUは「プロファイリングされない権利」の創設によって、米国はデータブローカーに対する罰則によって、規制を強化

EU

■ EUデータ保護規則案（2012年1月）では、本人の個人的側面の評価や、本人の業績、経済状況、位置、健康、個人的志向、信頼性、行動などを、「プロファイリングされない権利」を創設。

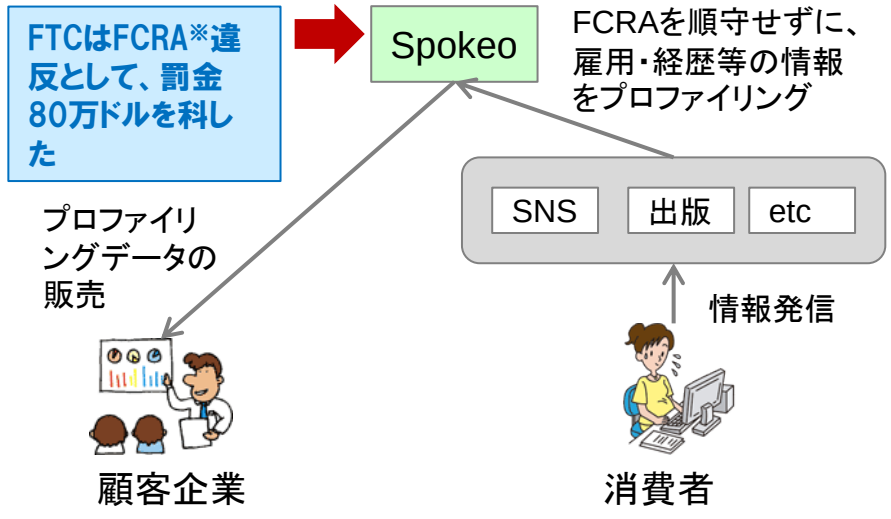
■ フランスの第三者機関（CNIL）は、ブローカーのデータを利用して広告配信をした不動産事業者に、初めて罰則を科した。



米国

■ 連邦取引委員会（FTC）は、2012年3月、消費者の権利を守るため、データブローカーの規制立法を示唆
- FTCは、”Online Profiling: A Report to Congress”(2000)において、本人がプロファイリングを受けることの可否や収集されたデータへのアクセス性・安全性の担保が推奨されているが、事業者の自主規制に留まっていた。

■ 2012年6月、プロファイリングデータの販売を行ったSpokeoに対し、FTCは80万ドルの罰金を初めて科した。



※公正信用報告法

EUは、親権者の同意義務付けと「忘却される権利」を創設、米国は現行法の監督を強化

■米国では1990年代から、13歳未満の子どものインターネットサービス利用に関する親権者同意が義務付けられていたが、2012年にはEUも同様の規定を策定し、欧米の足並みがそろった。

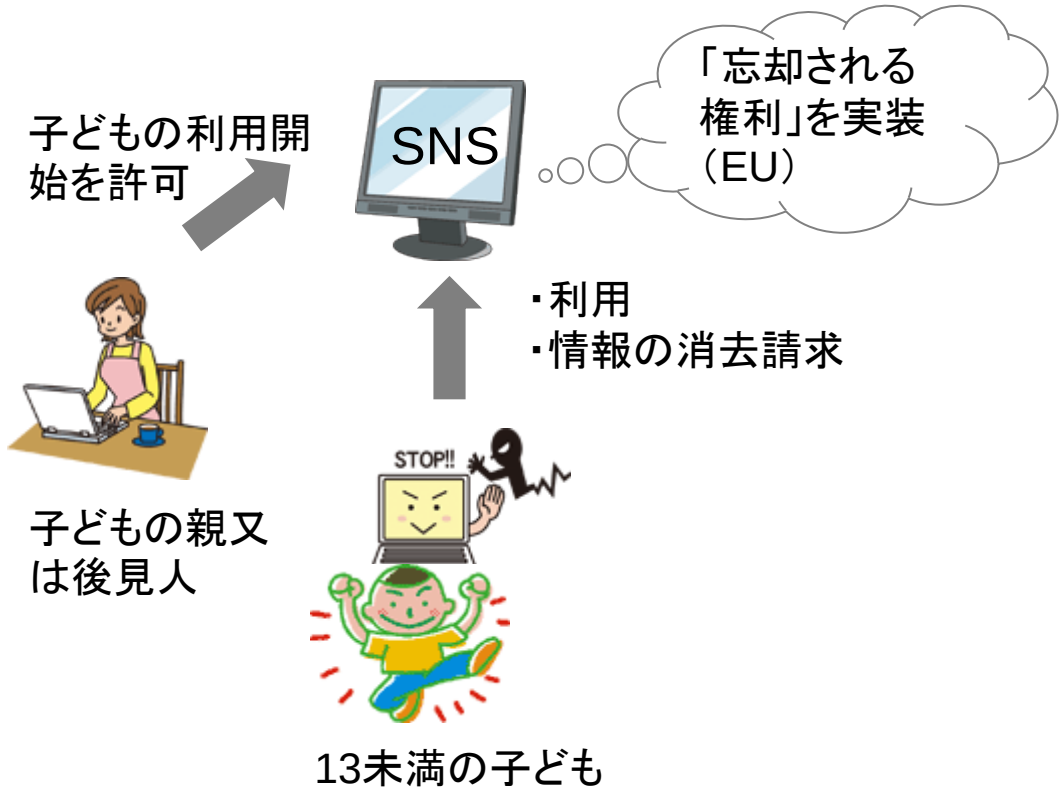
EU

■ EUデータ保護規則案では、13歳未満の子どもの個人データの処理に、親権者の同意取得を義務付け。
■ また、「忘却される権利」の創設によって、SNS事業者等の個人データ管理者に対し、第三者へのデータのリンクや、当該データのコピー、複製を消去することを本人が要請できることに。

米国

■ 米国ではCOPPA（1998）によって、13歳未満の子どもによるインターネットサービスの利用に親権者の同意を義務付け。
■ しかし、法令が守られていないことから、監督が強化される見込み。

子どものSNS利用に親権者の同意が必要に



1．個人情報とプライバシー

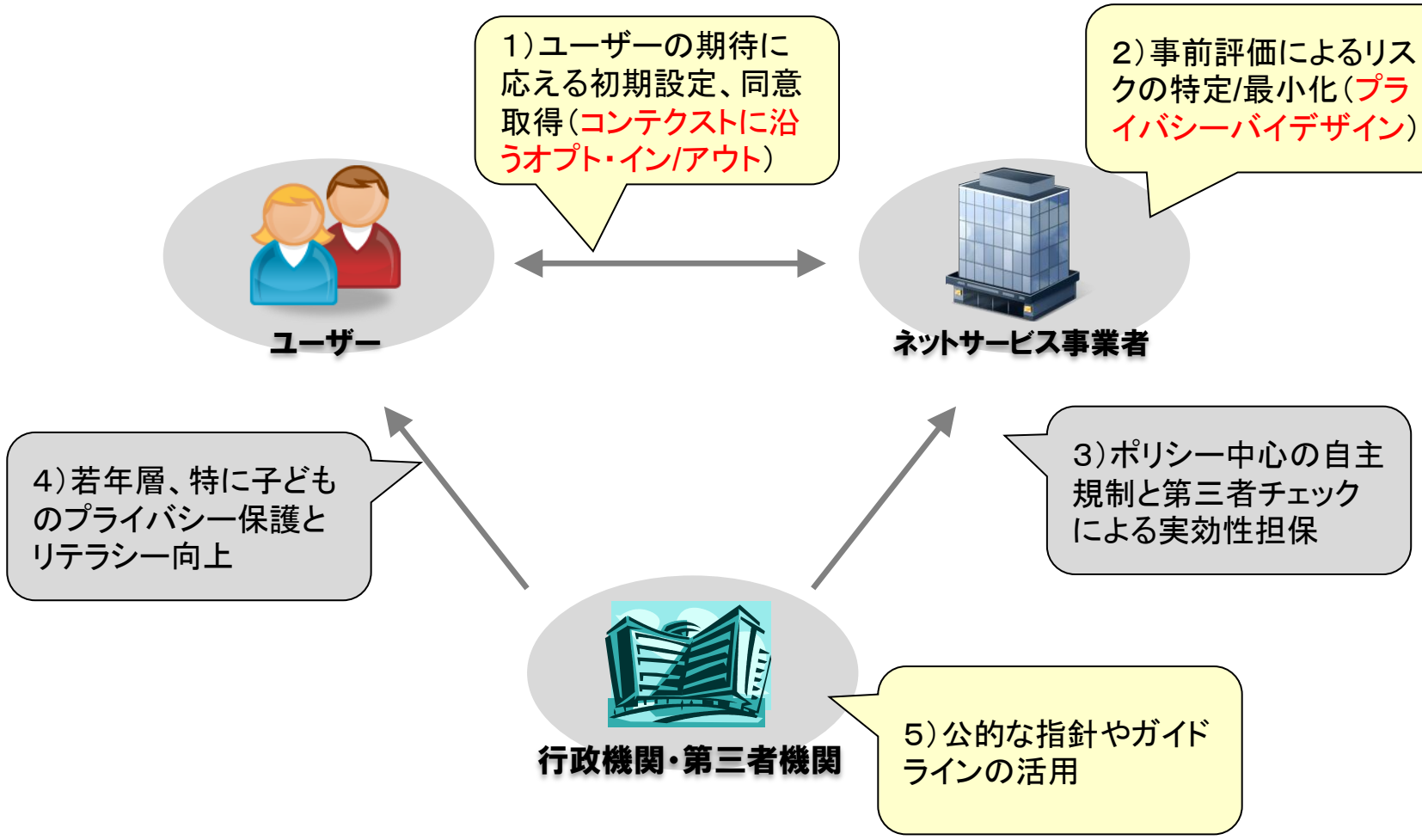
2．ネット社会で生じるプライバシー侵害事件

3．米国、EUそれぞれの規制強化の動き

4．パーソナルデータの保護と利用のあり方

パーソナルデータの保護と利用を実現させるための要点

本日は、1)、2)、5)について紹介する。



1)ユーザの期待に応える初期設定、同意取得（コンテクストに沿うオプト・イン／アウト）

■コンテクスト（脈絡）に沿って、ユーザーが期待する（ユーザーが驚かない）情報の取得、利用・提供の範囲を評価する。

■評価結果に基づき、①プライバシー設定の初期設定へ反映する、②同意取得すべき場面を設定する、③通知文を簡潔にする。

（例）

①SNSにおける個人情報の公開範囲の初期設定を「友人」までとする。

②軽微なポリシー変更（管理体制の変更など）はオプトアウトで行い、当該サイト以外へ情報を提供する時はオプトインで本人の同意を取得する。

③同意取得の通知文において、「アフターサービスに利用する」などの一般的に受容される内容を省略する。

■プライバシー設定を、機械（情報システム）が判読して自動的に対処する仕組みを導入する

- 日本版“Do Not Track”の導入
- プライバシー保護のレベル分けを、例えば、「高・中・低」の3段階で設定するなど、P3P※プロジェクトを教訓として実装が容易な機械判読によるプライバシー設定とする。

※P3P（Platform for Privacy Preferences）は、Webサイトの運営事業者がプライバシーポリシーを、サイトを訪問する個人のコンピューターのツールが自動的に解読できるよう、記述方式を標準化した仕様である。実装が難しく普及していない。

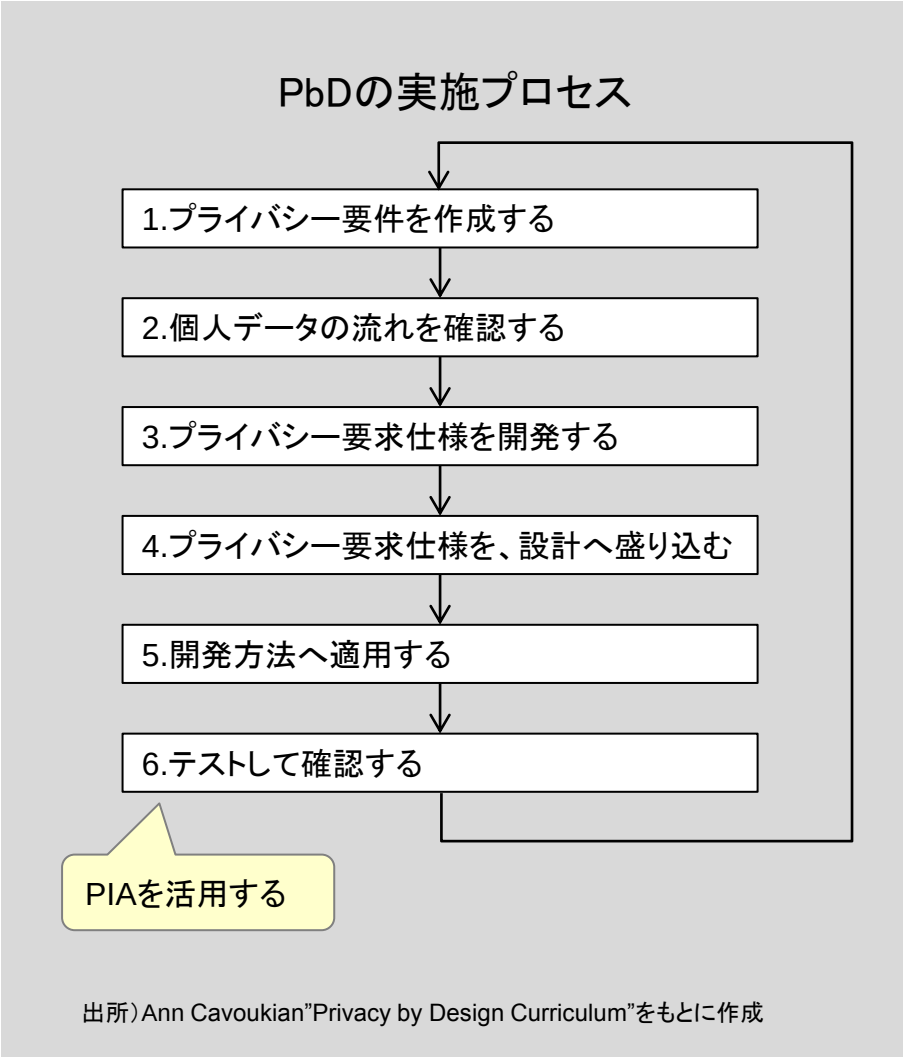
2）事前評価によるリスクの特定、最小化
（プライバシーバイデザイン）

■サービス開始に当たって、発生する可能性があるプライバシー侵害を、事前評価してリスクを特定し、最小化する取組であるプライバシーバイデザイン（Privacy-by-Design, PbD）を実施する。

■PbDを実践する手法として、プライバシー影響評価（PIA）を活用する。

- 米国、カナダ、オーストラリア等では電子政府プロジェクトに伴って、行政機関に義務づけられている。
- EUの新データ保護規則案では、PIAの実施が官民問わず、義務づけられている。
- マイナンバー法では、「情報保護評価」として行政機関に義務づけられる予定。

■経済的損失リスクを定量把握する。これにより、対策コストを見積もる。



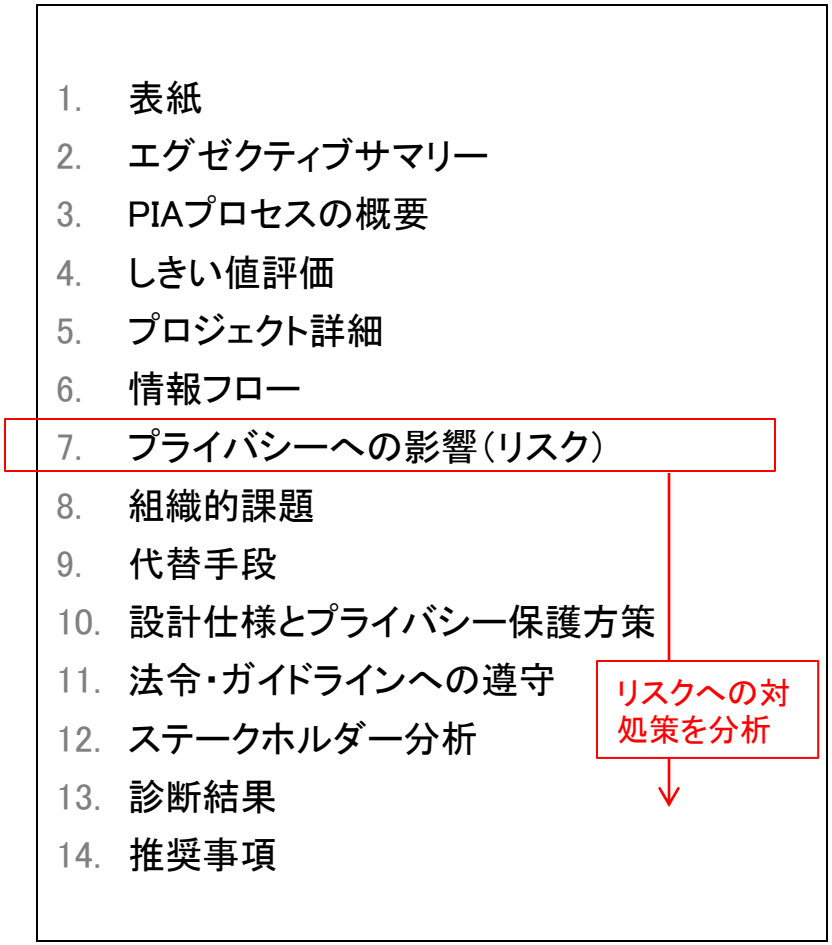
出所）Ann Cavoukian"Privacy by Design Curriculum"をもとに作成

EUの事例：
リスク評価を中心に対策を検討するPIAフレームワークを提供

- 欧州委員会が、民間コンサルに委託して、プライバシー影響評価（PIA）の在り方を調査。成果は、PIAF（Privacy Impact Assessment Framework）としてとりまとめられた。PIAのテンプレートが示されている。

- PIAは、複雑になりすぎると実効性が低下するとし、PIAFでは、最低限盛り込むべき要点を整理している。

欧州委員会によるPIAテンプレート



5）公的な指針やガイドラインの活用

■総務省では、スマートフォンの利用者情報の取扱いに関する指針を示し、業界や事業者の自主的な取組を促進している。

■社会保障・税の番号（マイナンバー）制度では、プライバシー保護に重要な仕組みが誕生予定。

- 個人番号情報保護委員会（第三者機関） 2013年6月に設立予定
- 情報保護評価（PIA）制度　情報保護評価の指針は、2013年3月末に公表予定

スマートフォン利用者情報取扱指針の基本原則

基本原則

① 透明性の確保

対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

関係事業者等は、その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは同意取得を行う。また、対象情報の取得停止や利用停止等の利用者関与の手段を提供するものとする。

③ 適正な手段による取得の確保

関係事業者等は、対象情報を適正な手段により取得するものとする。

④ 適切な安全管理の確保

関係事業者等は、取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要・適切な措置を講じるものとする。

⑤ 苦情・相談への対応体制の確保

関係事業者等は、対象情報の取扱いに関する苦情・相談に対し適切かつ迅速に対応するものとする。

⑥ プライバシー・バイ・デザイン

関係事業者等は、新たなアプリケーションやサービスの開発時、あるいはアプリケーション提供サイト等やソフトウェア、端末の開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計するものとする。

利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うものとする。

出所）総務省　利用者視点を踏まえた ICT サービスに係る 諸問題に関する研究会「スマートフォンを経由した利用者情報の取扱いに関するWG　最終取りまとめ・スマートフォン プライバシー イニシアティブ」（2012年8月）

パーソナルデータの利用拡大に向けた政府の動きが見られる

■規制改革会議

- 「ビッグデータビジネスの普及（個人情報の利用制限の見直し）」を課題として認識。

「 個人情報保護法においては、原則として、個人情報の取扱いには、その利用目的を特定するとともに、目的外利用の際には、あらかじめ本人の同意を得ることが義務付けられている。いわゆるビッグデータビジネス（様々な分野のデータの蓄積、組合せによって新たな価値を創出するもの）の普及を促進する観点から、**「個人情報」の定義を明確化するとともに、収集した個人情報について、個人を特定できない状態にした場合には、個人情報保護法の適用対象とはせず、第三者への提供や目的外利用を可能とすべきではないか**。」

■総務省 「パーソナルデータの利用・流通に関する研究会」

- プライバシー保護等に配慮したパーソナルデータ（個人に関する情報）のネットワーク上での利用・流通の促進に向けた方策について検討.

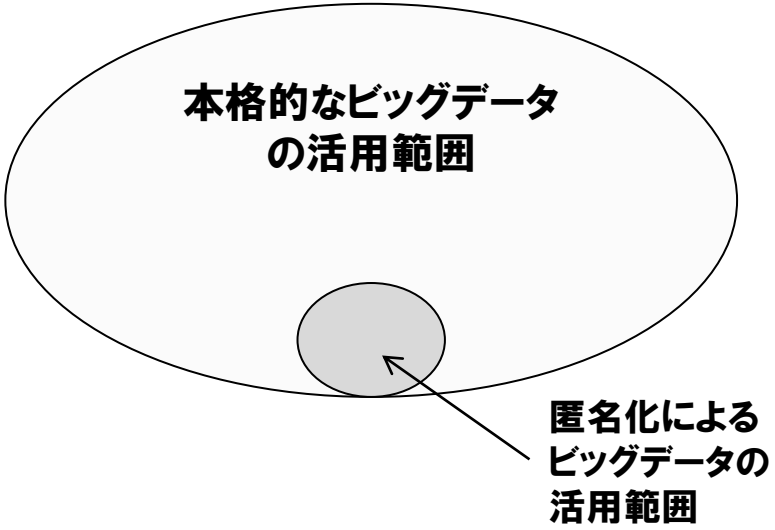
■経済産業省「IT融合フォーラム パーソナルデータワーキンググループ」

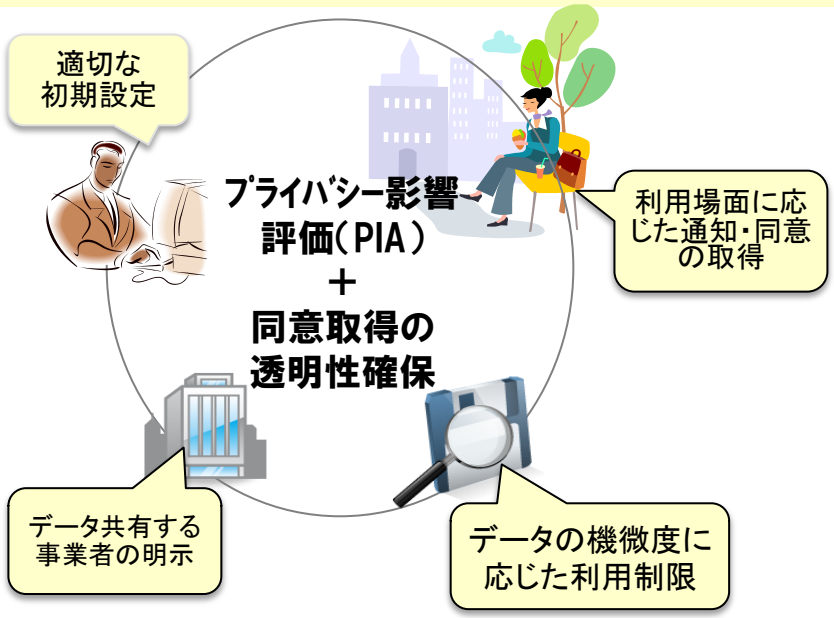
- データ活用による新産業創出のため、個人情報、プライバシー等に関する課題の対処策を検討。

本格的にビッグデータ活用するためには、プライバシー影響評価（PIA）と同意取得における透明性確保が不可欠。

■匿名化はビッグデータ活用の一里塚。
- 規制改革会議等、匿名化のルール整備を推進中。
- しかし、匿名化しても、他の情報との再結合による個人の識別リスクは残る。
- 強い匿名化処理をすると、ビジネス価値の乏しいデータになる。

■PIAを実施し、同意取得の透明性を確保することで、活用の幅は広がる。
- 欧米は、PIAの実施、同意取得の透明性確保のルール作りを指向。
- 消費者がリスクを理解し、自ら判断して同意することのできる仕組みが必要





本日のまとめ

- SNS、スマートフォン、ビッグデータビジネスの台頭によって、従来の個人情報保護では対処できないプライバシー保護の問題が拡大している。

- パーソナルデータの利用に関するプライバシー侵害事案は国内外で多数生じている。

- 米国、EUともに、2012年初にプライバシー法制の改正案を発表。米国が自主規制、EUは法制による規制強化を指向するも、同じ問題意識に基づいて対処を模索している。日本の法制への影響も大きい。

- 本格的にビッグデータ活用をするためには、プライバシー影響評価（PIA）の実施と、同意取得における透明性確保が求められる。