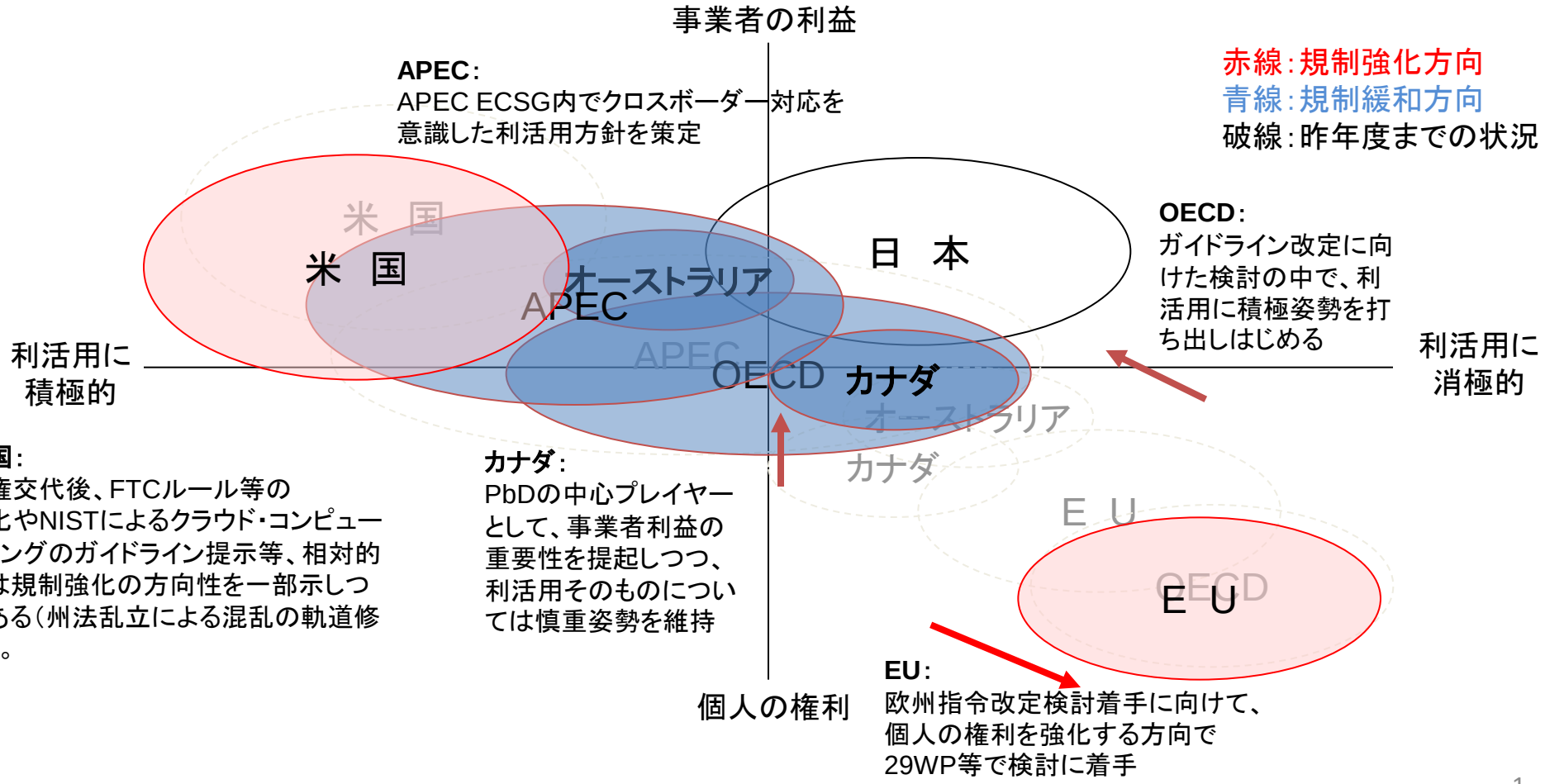
資料4

# パーソナルデータに関する海外動向

2012年11月
経済産業省
商務情報政策局

# パーソナルデータに関する国際動向①

EUの『データ保護規則案』や、米国の『消費者プライバシー権利章典』に見られるように、欧米では、パーソナルデータに関する議論が積極的に行われており、欧米共にパーソナルデータの活用が新産業創出の際に重要な役割を果たすと明示している。ビッグデータ時代を迎える中、消費者保護と産業創出の新たなバランスの在り方を模索している。






経済産業省調査事業「平成23年度_匿名化クラウド社会実装の推進事業報告書」をベースに作成

# パーソナルデータに関する国際動向②



2011年頃からパーソナルデータに関し、国際的に活発な議論が行われており、欧米各国でプリンシプルの発信、制度設計が進んでいる。

**① EU**

2012年1月、1995年に制定したデータ保護指令の包括的な改正に向けた「EU個人データ保護規則案」が提案され、「データ・ポータビリティの権利」や「忘れてもらう権利」を認め、また、各国のデータ保護機関の権限強化を図る、個人データ保護のためのEUフレームワークの設置が掲げられている。EU域内の事業者に対しては義務を追加し、EU域外の国に対してもデータ移転にあたって「十分なレベル」の個人データ保護を要請する、個人情報保護の分野では極めて影響力の強いフレームワークである。

**② 米国**

2012年2月、「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」を公表。①消費者プライバシーの権利章典（Consumer Privacy Bill of Rights）、②執行可能な行動規範の策定に向けた多様な利害関係者との協議の促進、③連邦取引委員会の執行強化、④グローバルな相互運用（interoperability）について言及。
また、米国では「サイバースペースにおける信頼できるアイデンティティのための国家戦略」という国内向けの戦略を打ち出し、インターネットを単なるツールとしてではなく、陸、海、空、宇宙と同じように、サイバー空間として位置付けている。

**③ イギリス**

ビジネス・イノベーション・職業技能省が、消費者が企業の保持している自身のパーソナルデータにアクセスし、そして利用しやすくするというプロジェクトである消費者権限付与戦略『より良い選択：より良い取引』の中で、midataのためのプランを策定。
midataはイギリスの主要企業、政府、消費者団体が共同で進めているプロジェクトであり、消費者が企業・政府の持つ個人データにアクセスできる権利を消費者に与えることを目的にしている。

# パーソナルデータに関する国際動向③



| | EUデータ保護規則提案 | 米国消費者データ・プライバシー権利章典 | OECDプライバシー・ガイドライン見直し案 |
|---|---|---|---|
| 公表時期 | 2012年1月 | 2012年2月 | 2013年（予定） |
| 目的 | 自然人の基本的権利及び自由、特に個人データの保護への権利保障 | ネットワーク化された技術における消費者データ・プライバシー保護 | プライバシー及び個人の自由の保護 |
| 適用範囲 | EU市民の個人データの処理、EU域外でも商品・サービス提供またはモニタリングは該当 | 消費者のデータ・プライバシーを主な対象 | 官民問わず、個人データに適用 |
| 本人の権利 | 本人同意、忘れられる権利、データ・ポータビリティが追加 | 消費者プライバシー権利章典、公正な情報慣習の原則に基づく7原則 | 8つの基本原則に変更なし |
| 事業者の義務 | データ保護バイ・デザイン、<br>データ保護違反通知義務、<br>データ保護影響評価、<br>データ保護担当者の設置など | Do-Not-Track原則などを用いたプライバシー強化技術、執行可能な行動規範の策定 | プライバシー・マネジメント、セキュリティ違反の通知の導入、プライバシー・リスク評価に基づく保護措置など |
| データ移転 | 十分性の要件の具体化、<br>拘束的企業準則の明記 | グローバルな相互運用（相互認証、利害関係者との対話と行動規範の策定） | 越境プライバシー法執行の協力促進 |
| 監督・執行 | 独立性の確保、相互支援、欧州データ保護委員会の設置 | 連邦取引員会の権限強化 | プライバシー執行機関の設置 |

宮下紘「プライバシー・イヤー2012」Nextcom Vol.12 2012 Winter

参考①

# 各国・地域の状況

# 各国・地域の事例①　EUデータ護規則案の概要

1995年の「個人データ処理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指令（95/46/EC）」の指令から規則へ格上げ。EU法を加盟国へ直接適用し、EU域内でのデータ保護ルールを一元化。2013年夏から2014年にかけて採択される予定。

## ①EU域内における規制の単一化・簡素化

- 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

## ②より強固な個人データ保護ルールの整備

| | |
|---|---|
| **事業者** | プライバシー・バイ・デザインの原則 |
| | 個人データ漏えい時の通知義務 |
| **個　人** | 忘れてもらう権利 |
| | データ・ポータビリティの権利 |
| | 同意の明示（オプト・イン原則） |

## ③データ保護に関するグローバルな課題への対応

【参考】 日本の個人情報保護法とEUデータ保護規則の比較

日本の個人情報保護法は、以下に挙げるような多くの点で、EU 規則案よりも規定が緩やかでああると言える。

- **対象事業者（個人情報取扱事業者）の範囲が狭い**
- **第三者提供など一定の場合を除いて本人の同意取得が必要とされていない**
- **特定カテゴリの情報（特定機微情報）の取扱いに関する規定がない**
- **開示・訂正・消去請求権が本人の権利として明示的には認められていない**
- **ダイレクトマーケティングに対する異議申立の権利がない**
- **プロファイリングを受けない権利の規定がない**
- **個人情報漏洩時等の報告・連絡義務がない**
- **第三国への個人情報移転を禁じていない**
- **独立的な監督機関（第三者機関）に関する規定がない**
- **司法救済を求める個人の権利が規定されていない 等**

# 各国・地域の事例②　米国　消費者プライバシー権利章典

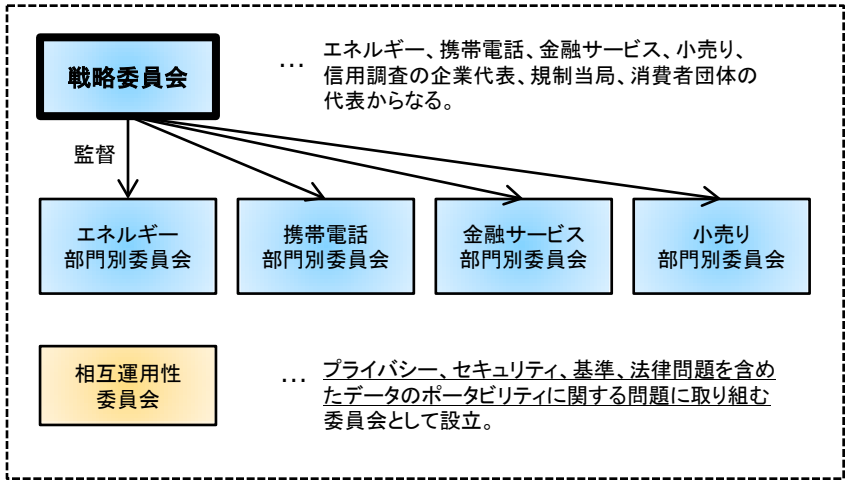


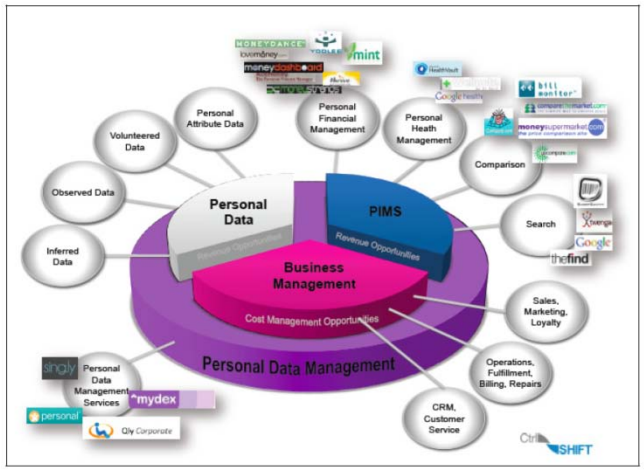
米国の通称ホワイトペーパーと呼ばれる2012年2月に公表された「ネットワーク化された世界における消費者のデータプライバシー」から2章「消費者プライバシー権利章典」7原則として記述。OECD8原則を現代風にアレンジし、民間分野でのベースラインとなるプライバシー法令として議会に立法勧告。立法化は2013年になる予定。

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、どのようにそれを利用するかについてコントロールを行使する権利を有する。
2. **透明性**
   消費者は、プライバシー及びセキュリティ・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る。
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整合的な仕方で、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る。
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る。
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る。
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る。
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る。

# 各国・地域の事例③　英国 midata

midataとは、消費者に関するデータを保持している企業に、ポータブルで再利用が可能な（電子的な）形式で、そのデータを本人に公開し直すことを促進する、英国政府プロジェクトであり、世界的に見て初めての、個人データの使用について消費者の管理権限を強化する、政府ベースのイニシアティブ。ビジネス・イノベーション・業技能省、及びエネルギー、小売り、携帯電話、金融の各部門の主要企業が推進している。



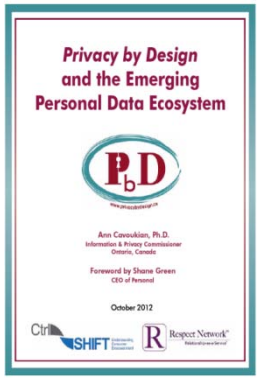




| | |
|---|---|
| **消費者データの権限強化** | • 個人が自らの消費者情報を使用する原則を認め、支持する。<br>• 組織が収集する個人の取引、やりとり、利用状況に関するデータ含めた個人の消費者データにその個人がアクセスしてライ利用できることは、この原則が具体化される際に必要不可欠であることを認める。 |
| **消費者データの透明性** | • 消費者に対して保管した個人情報の記述が正確で最新であることを維持し、消費者がこれを利用できるようにする。 |
| **消費者データへのアクセス** | • ポータブルで再利用可能な安全でプライバシーに配慮したやり方で、消費者のデータを消費者に公開しなおすための自由な方法を開発し、これをサポートして促進させる。 |
| **消費者データのセキュリティー** | • データの改竄とプライバシーの侵害の危険を最小限に抑制する。（個人のデータが安全かつセキュアにアクセス、転送、保存、利用、更新、共有されることを保証することを含む）<br>• 個人が理解し、信頼できる方法で個人データにアクセスし、利用し、共有することを個人に認める枠組みを創出する手助けをする。この枠組みは個人の利益を保護し、個人が自らの目的に個人データを使用する権限を個人に与える。 |
| **消費者データのイノベーション** | • “midata”が新しい消費者情報サービスのイノベーションのための基盤を創出している事実を認め、歓迎する。<br>• 消費者と企業の全体的な利益を探求し、提供する。 |

# 【参考】Privacy by Design

Privacy by Designとは、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り、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。

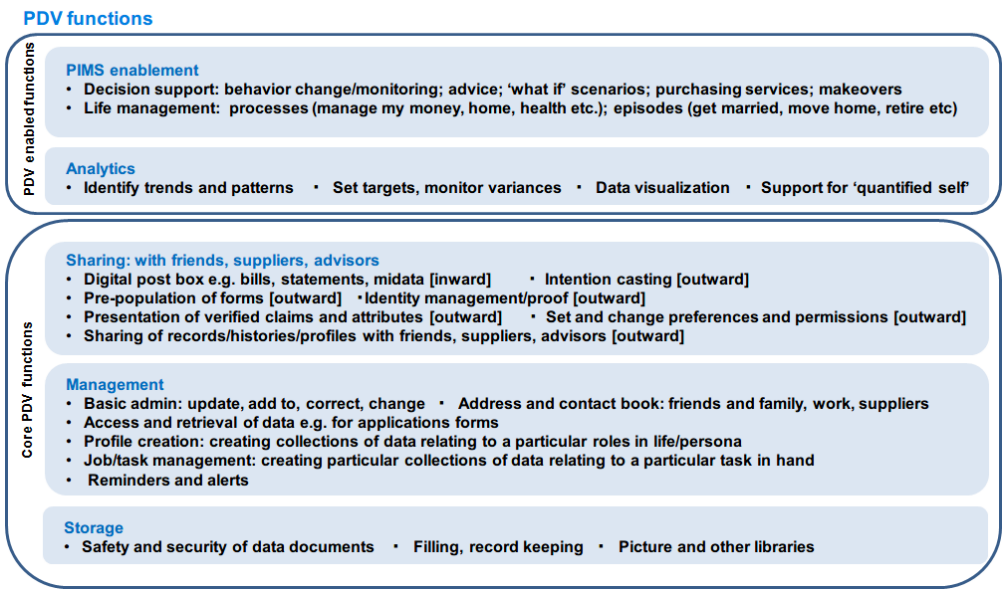
個人の情報を集め、個人がその情報にアクセスし、利用させるためのエコシステムの構築を目的とした事業者主体のコンソーシアム（Personal Data Ecosystem Consortium）が、ベンチャー企業を中心に組成され、PbDに沿った実装モデルを議論が為されている。




| 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されているか**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。 |

主な参加企業

bitWORLD　reputation.com　connect.me　personal　mydex




図PVD　構成図

参考②

# 海外における実ビジネスの事例

# パーソナルデータに関するビジネスの国際動向①

2011年頃から、パーソナルデータを集積して、2次利用するモデルが増加している。


**Infochimps（ http://www.infochimps.com/ ）**

【事業概要】

◎集積データのマーケットプレイスを提供（現在登録されているデータ種類は14000件。内2400件が有料データ）

◎販売時の手数料（平均30%）が収益

【パーソナルデータの取り扱い例】

・イリノイ州内400万人の電話番号リスト（200 USD）

・カナダの弁護士7万人リスト（125 USD）

・米国のアラブ研究者が、自著 “What Arabs Think”で用いたアンケートのデータ

【調査結果】

・公開が認められていないデータの一つとして、「当該個人から未承諾である個人を特定するデータ」が指定されている。

・データの品質を保持するために、一件ずつスタッフが人力による確認を行なっている。

・複製制限については「規約による制限」となっている。

・価格設定については「それぞれのユーザに一任」など


**Demdex（ http://www.demdex.com/）**

【事業概要】

◎行動ターゲティング広告などに用いるための、ユーザ動態データの提供・流通事業者

【パーソナルデータの取り扱い状況】

・収集するデータは基本的に個人を特定するデータは含まないとしている。中心は、オンラインでのサイト閲覧履歴等に関するデータ

【調査結果】

・顧客1人につき保管するデータ量に応じて月額料金を徴収している。

・金額は概ね訪問者1人/月あたり1セント程度であった。それぞれのユーザについては40種類程度の行動変数が取得されていた。

**※参考※**
2011年にAdobe社が買収し、Adobe社の広告サービスとしてサービスを継続中

# パーソナルデータに関するビジネスの国際動向②



**Bluekai（ http://www.bluekai.com/ ）**

【事業概要】

◎匿名データの取引を中心とするデータ売買の取次ぎ事業（ 北米では毎月約300万の利用者）

【調査結果】

・サービスは2種類

① Data Exchange

：パートナー企業から提供を受けているデータを顧客が購入できるシステム（主にアドバタイズに利用されている）。データ更新は頻繁。

②Data Management Platform

：データ解析サービス。顧客のウェブサイト解析（どのページにアクセスがされているか、どのページで訪問者が閉じているかや、何のデバイスで見られているか　など）が中心であるが、最近は事業者がデータ持ち込んで解析を依頼されるケースも増えている。

・プライバシーに関わる部分が残されているデータは取引等を行わない。

①名前、住所などは勿論の事、1個人の医療記録や金銭面に関するもの

②Minor （18歳以下、日本における未成年者）のものと思われるデータが発見された場合は、収集および分析対象から除外。

・全てのデータは独自のアルゴリズムを用いたツールによる審査を受けてから売買の対象になる。


**Allow（ http://i-allow.com/ ）**

【事業概要】

◎ 個人情報を販売し、情報を提供した個人には売り上げの70%を手数料を支払っている。

【パーソナルデータの取り扱い状況】

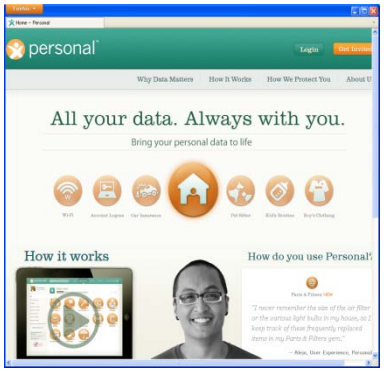
・『個人情報の積極的換金を支援する』方針を明確に打ち出している。

【調査結果】

・ サービス登録はイギリス国民に限定されている。

・「保険」「携帯電話」「クレジットカード」に関する問いの価値が高い。

# パーソナルデータに関するビジネスの国際動向③




**Personal.inc（ http://www.personal.com ）**

【事業概要】

◎個人に関する情報を、保管、共有するサービスを無料で提供する。

【調査結果】

・提供するサービス

①保管（自身の情報を保管する）

②共有（家族、友人などと情報を共有する）

③販売（自身の情報を販売する）

・利用者が預けたデータから利益を得ることを選んだ場合は、Personal社はデータ販売を行い、手数料として10%以下を徴収し、利用者へ支払うというビジネスモデル。


**STATZ（ http://www.statz.com/ ）**

【事業概要】

◎利用者が自信で登録したパーソナルデータを匿名化して販売する。

【調査結果】

・プライバシー3原則を提示

Effective（識別データの要素は、プライバシーや機微性があるため、転送・格納された要素は、データに匿名化や強い暗号化によって加工される）

Open（機微な識別可能データ要素、匿名化・暗号化の方法、匿名化の対象となるべきデータを明示）

Verifiable（最も良い効果を得るためには、実際の顧客の生データとフィルタされたデータを比較することである）

| 要素 | プライバシーレベル | | |
|---|---|---|---|
| Name | 4 | | |
| Street Address | 4 | | |
| City | 5 | | |
| State | 5 | | |
| Zip | 5 | | |
| Zip +4 | 4 | | |
| Country | 5 | | |
| Phone # | 3 | | |
| Birthdate | 3 (never presented in cle form) | | |
| Age | 5 | Device model | 5 |

データ要素は、固有のプライバシーリスクがあり、組合せによってリスクも高くなる。

レベル1：データを削除する

レベル2：一方向性（ハッシュ）関数によって暗号化する

レベル3：匿名化によって（1:1から1:10000へ）あいまいにする。（電話番号なら下4桁を削除することで、1:1から1:10000として識別リスクを下げる）

レベル4：双方向のアルゴリズムにより暗号化（データの所有者がアクセス権を提供するまでは暗号化されたままとなる）

レベル5：生データ

**※参考※**

STATZに関しては、2011年調査当時はサービスを提供していたが、その後大手IT企業に買収され、現在はサービスをおこなっていない。