MyData Japan 2019
オープンスペース講演

信頼される安心を、社会へ。
SECOM

個人中心のアプローチに欠かせない ユーザブルプライバシー ～動向と課題～

セコム株式会社 IS研究所

坂本一仁

2019.5.15

自己紹介 - 研究内容

「人」の観測

- プライバシー保護ツールのユーザビリティ
- プライバシー侵害の感じ方
- 使いやすい認証・認可技術
- 効果的なアカウンタビリティ

「Web」の観測

- プライバシー保護機能の効果測定
- 広告配信状況の調査
- 人物属性を模した大規模なWeb巡回調査
- 大規模サイバー攻撃の調査

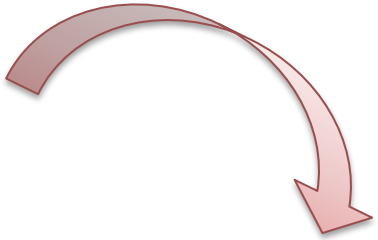
- ユーザが管理できる行動ターゲティング方式
- Malvertisingに対するセキュアな広告配信方式

使いやすい仕組みやツールの提案

MyData Japan

MyDataの原則について

私たちはパーソナルデータに対する**個人中心**のアプローチに向けた取り組みを推進しています。 個人が自身のデータについて十分に理解し、**主体性と主導権**を持って、自らのためにパーソナルデータを活用できる世界を目指しています。 この価値観を共有し、**パーソナルデータのパラダイムを逆転**させる MyData Japan の活動にぜひ参加してください。
MyDataへの宣言に署名し、このパラダイムシフトを推進しましょう。

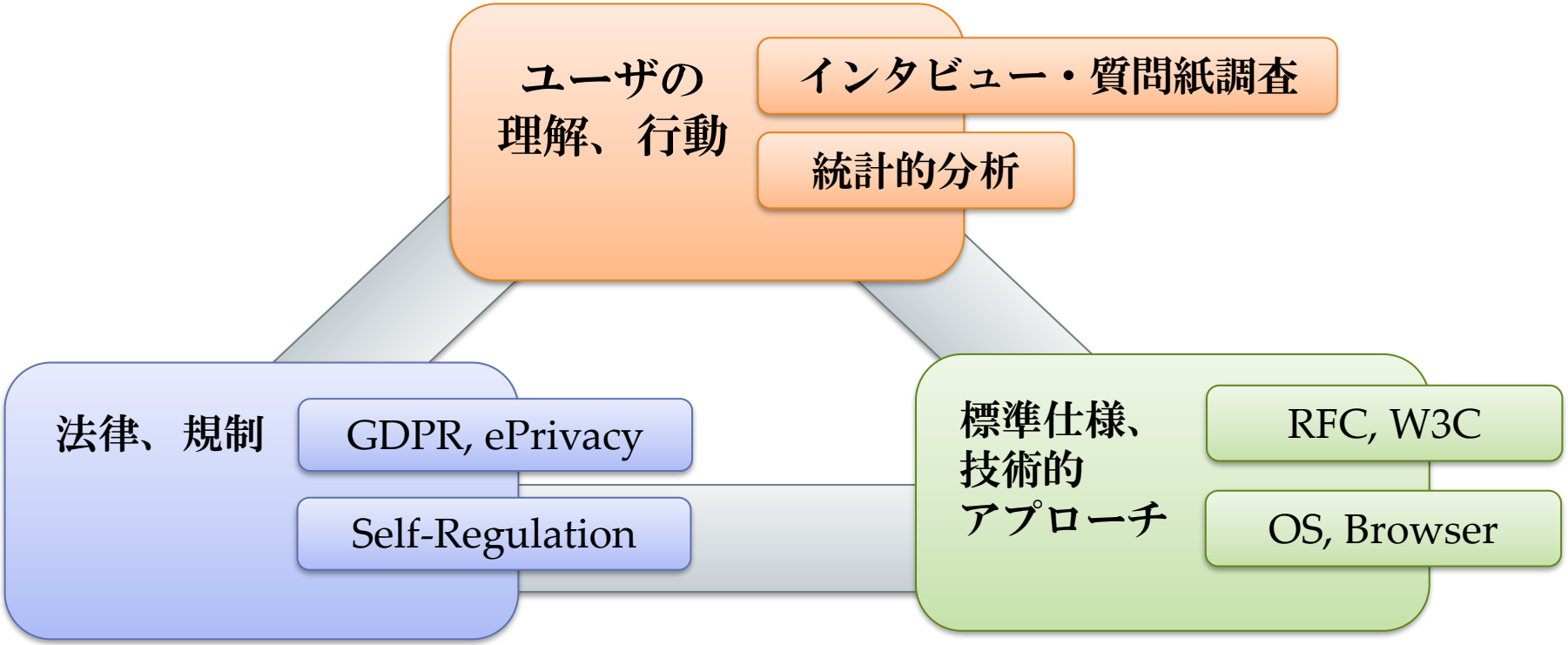


Usable Privacy
ユーザブルプライバシー

Usable Privacy

- 明確な定義はない？
  - あえて言うと、自身のプライバシーの状態を理解できて向上できるもの
- 2000年前半ぐらいから研究されている
  - 第一人者：Lorrie Cranor (CMU)
  - 心理学、行動科学的アプローチ
    - ユーザは何ができるか、何を不快に思うか、より良いツールは何か
- 日本では流行っていない
  - MyData Japanや情報銀行の取組みと関連して盛り上がることを期待

ユーザブルプライバシーを取り巻く現状



目次

- ユーザブルプライバシー関連の歴史
  - これまでの取組みと失敗事例
- ユーザブルプライバシーについてわかってきていること
  - 研究動向、ユーザの行動・感じ方
- 情報銀行で考えるユーザブルプライバシー
  - これからのこと

目次

- **ユーザブルプライバシー関連の歴史**
  - **これまでの取組みと失敗事例**
- ユーザブルプライバシーについてわかってきていること
  - 研究動向、ユーザの行動・感じ方
- 情報銀行で考えるユーザブルプライバシー
  - これからのこと

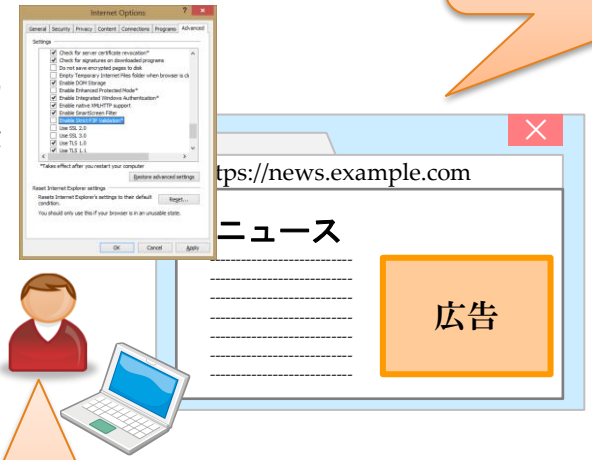
P3P: Platform for Privacy Preferences Project

W3C勧告 since 2002

・P3Pの複雑な仕様への準拠
・対応サイトが増えない

・XMLポリシー作成が大変
・法的な強制がない

User Agent



・内容の理解が困難
・プライベートモードでいい

ニュースサイト
news.example.com

P3P検証

/policy.xml

コンパクトポリシー送信

P3P: CP="UNI CUR OUR"

```
<META xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY-REFERENCES>
  <EXPIRY max-age="172800"/>

   <POLICY-REF about="/P3P/Policies.xml#first">
    <INCLUDE>/*</INCLUDE>
    <EXCLUDE>/catalog/*</EXCLUDE>
    <EXCLUDE>/cgi-bin/*</EXCLUDE>
    <EXCLUDE>/servlet/*</EXCLUDE>
   </POLICY-REF>

   <POLICY-REF about="/P3P/Policies.xml#second">
    <INCLUDE>/catalog/*</INCLUDE>
   </POLICY-REF>

   <POLICY-REF about="/P3P/Policies.xml#third">
    <INCLUDE>/cgi-bin/*</INCLUDE>
    <INCLUDE>/servlet/*</INCLUDE>
    <EXCLUDE>/servlet/unknown</EXCLUDE>
   </POLICY-REF>

 </POLICY-REFERENCES>
</META>
```

ターゲティング広告オプトアウト

- **広告事業者団体の自主規制ガイドライン*に準拠する実装**

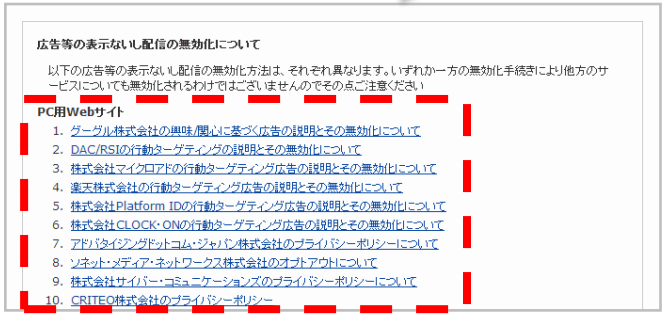
* AAAA and ANA and BBB and DMA and iab: Self-Regulatory Principles for Online Behavioral Advertising (2009)

ほとんどのユーザは覚えていない

全て確認するには年間で200時間以上かかる

アイコンやフレーズ

プライバシーポリシー


広告等の表示ないし配信の無効化について

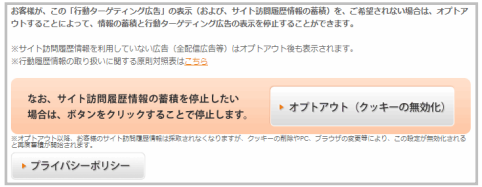
以下の広告等の表示ないし配信の無効化方法は、それぞれ異なります。いずれか一方の無効化手続きにより他方のサービスについても無効化されるわけではございませんのでその点ご注意ください

PC用Webサイト

1. グーグル株式会社の興味/関心に基づく広告の説明とその無効化について
2. DAC/RSIの行動ターゲティングの説明とその無効化について
3. 株式会社マイクロアドの行動ターゲティング広告の説明とその無効化について
4. 楽天株式会社の行動ターゲティング広告の説明とその無効化について
5. 株式会社Platform IDの行動ターゲティング広告の説明とその無効化について
6. 株式会社CLOCK・ONの行動ターゲティング広告の説明とその無効化について
7. アドバタイジングドットコム・ジャパン株式会社のプライバシーポリシーについて
8. ソネット・メディア・ネットワークス株式会社のオプトアウトについて
9. 株式会社サイバー・コミュニケーションズのプライバシーポリシーについて
10. CRITEO株式会社のプライバシーポリシー

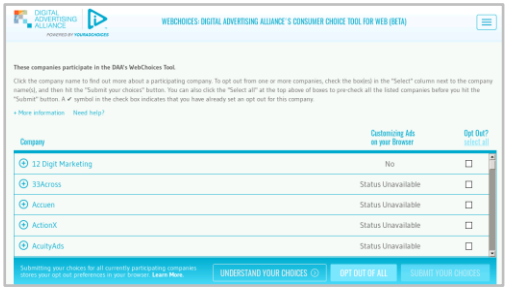
出典：livedoor利用規約 <http://www.livedoor.com/rules>

個別オプトアウト



出典：MicroAd <http://send.microad.jp/w3c>

一括オプトアウト



出典：DAA: WebChoices <http://optout.aboutads.info>

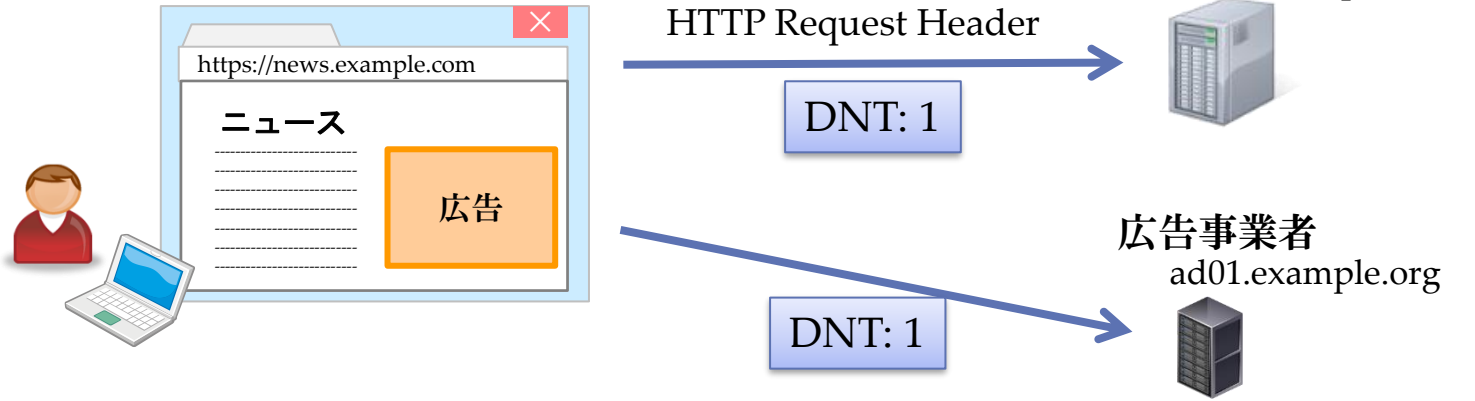
多くのユーザがオプトアウトの意味を誤解

Do Not Track (Tracking Preference Expression)

W3C Note (Recommendationではない)

・各ブラウザはとりあえず設定機能がある

・DNTを尊重して対応するかどうかは事業者しだい
・法的な強制がない



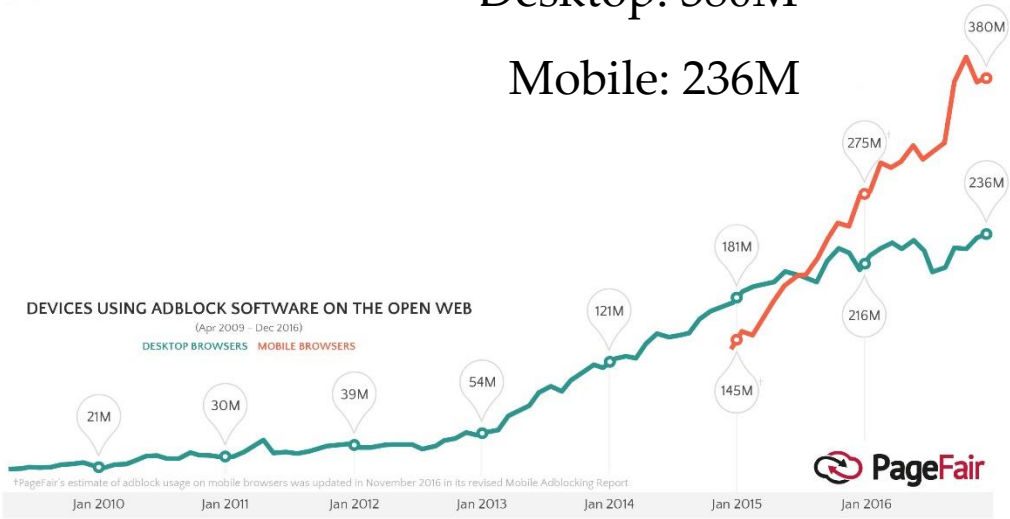
広告ブロッキングツール (成功事例?)

インターネットユーザの11%, 約6億デバイスが広告ブロッキングツールを導入*

* PageFair: The state of the blocked web - 2017 Global Adblock Report -

Desktop: 380M

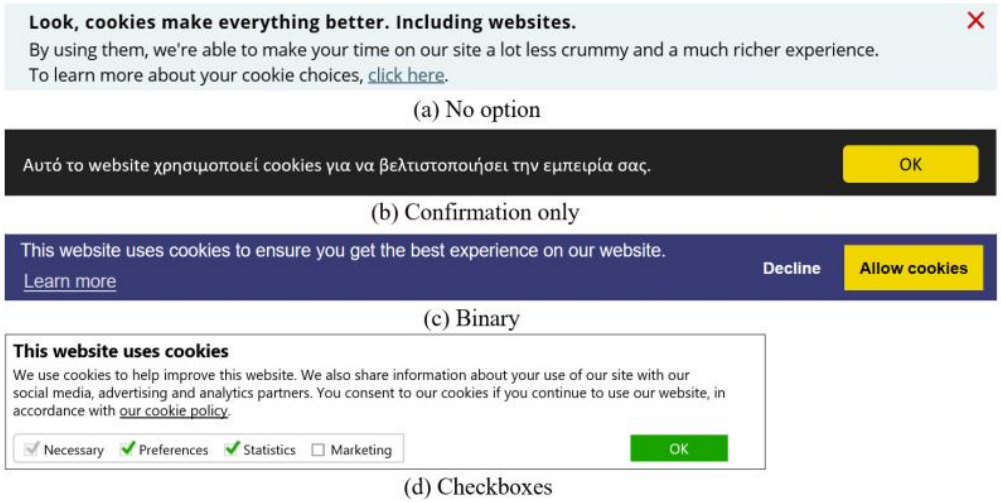
Mobile: 236M

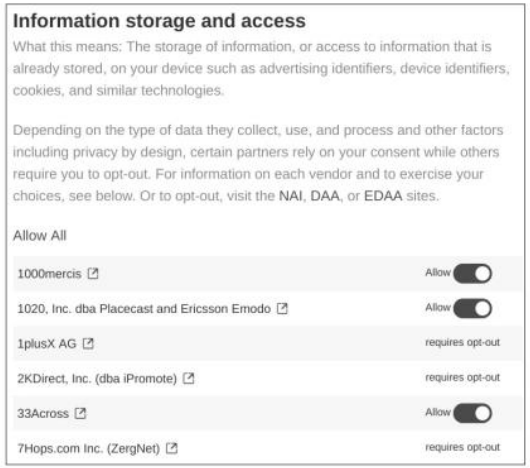


Cookie同意通知

GDPRの影響* （Cookieがパーソナルデータとなったため）

邪魔、不快に思う、大体の人は無視している



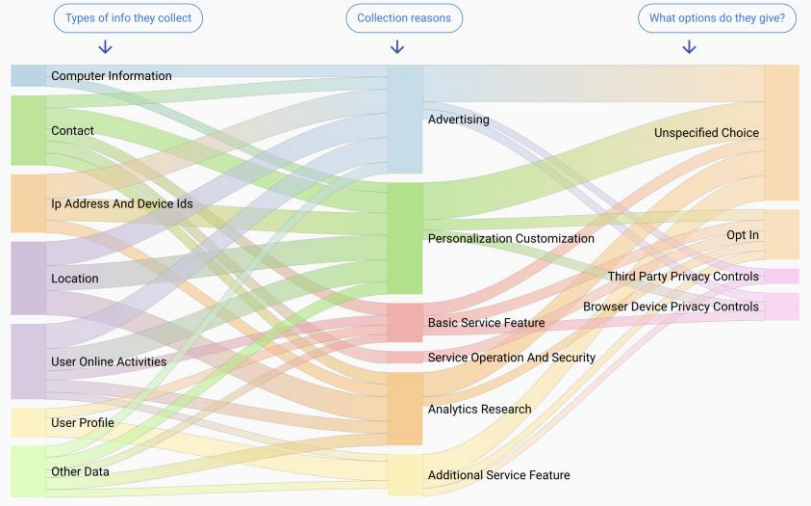


* Martin Degeling, et al.: We Value Your Privacy… Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy (NDSS2019)

Polisis – Pribot (最新の取り組み)

The Usable Privacy Policy Projectの成果物の一つ

Polisis: DLベースのPolicy解析器



データは何か　　目的は何か　　何ができるか

Pribot: Policyに対する質問に答えてくれるBot

https://pribot.org/polisis

目次

- ユーザブルプライバシー関連の歴史
  - これまでの取組みと失敗事例
- **ユーザブルプライバシーについてわかってきていること**
  - **研究動向、ユーザの行動・感じ方**
- 情報銀行で考えるユーザブルプライバシー
  - これからのこと

Webにおけるユーザブルプライバシー研究

ツール	構成要素	機能面
オプトアウトツール	アイコンとフレーズ	(認識)
	プライバシーポリシー	(認識)
	個別オプトアウトサイト	意思表示
	一括オプトアウトサイト	意思表示
ブラウザ/OS設定	Cookie制御	識別子制御
	Cookie削除	識別子制御
	プライベートブラウジング	識別子制御
	Do Not Track (DNT)	意思表示
	広告用識別子	意思表示
ブロッキングツール	アクセス制御	識別子制御
	Tracking Protection List	識別子制御
プライバシー設定	プロファイリング属性編集	意思表示

- **意思表示型**

  何らかの文字列を送信しユーザの意思を伝える方式

  - オプトアウトツール
    - Cookie: optout=1
  - DNT
    - HTTP Header – DNT: 1

- **識別子制御型**

  主に匿名性を保つ方式

  - Cookie制御/削除
  - ブロッキングツール

出典：坂本一仁, Webトラッキングにおけるユーザブルプライバシーの調査 (CSS2017)

研究論文サーベイ調査

論文	ユーザ調査				調査ツール	
	調査集団	調査数	調査方法	教育	プライバシーツール	要素
Beliefs and Behaviors (2010) McDonaldとCranor	大学関係者 Mturk	14 314	インタビュー 質問紙	なし なし	オプトアウトツール ブラウザ/OS設定	アイコンとフレーズ 一括オプトアウト Cookie削除
Icon Study (2010) Hastakら	オンライン調査	2604	質問紙	なし	オプトアウトツール	アイコンとフレーズ
Smart, Useful, Scary, Creepy (2012) Urら	大学近隣住民	48	インタビュー	あり	オプトアウトツール	アイコンとフレーズ
Communicate to Users (2012) Leonら	MTurk	1505	質問紙	なし	オプトアウトツール	アイコンとフレーズ
Why Johnny Can't Opt Out (2012) Leonら	大学近隣住民	48	インタビュー	あり	オプトアウトツール ブラウザ/OS設定 ブロッキングツール	一括オプトアウト Cookie制御/削除 DNT アクセス制御 TPLs
What do they know about me? (2015) Raoら	大学関係者 MTurk	8 100	インタビュー 質問紙	なし なし	プライバシー設定	プロファイリング編集
(Do Not) Track Me Sometimes (2016) Melicherら	大学近隣住民	35	インタビュー	あり	ブロッキングツール	-

Why Johnny Can't Opt Out (2012) *

- 9つのプライバシーツールのユーザビリティを調査
  - それぞれ5ユーザずつインタビュー調査
- 結果
  - オプトアウトツール（広告アイコンクリック→サイト上で操作）
    - ほとんどのユーザが自力でタスクを完了できない
    - オプトアウトの効果は正しく理解されていない
  - ブラウザ設定
    - プライバシー設定は表示できるが、専門用語に苦戦
  - ブロッキングツール（広告ブロック）
    - インストールは問題ないが、カスタマイズは困難

[*] Leon et al.: Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising (CHI 2012)

What do they know about me? (2015) *

- プライバシー設定についてインタビューおよびオンライン調査
  - ユーザの反応や意見を分析
- 結果
  - 「プロファイリング結果の利用方法がよくわからない」
  - 「設定変更の効果がよくわからない」
  - 「仕組みが難しく理解が困難」
  - 「多量のプロファイリング結果を編集できない」

出典：Googleの広告設定（講演者のあるアカウント）

[*] Rao et al.: What do they know about me? Contents and concerns of online behavioral profiles (2015)

ユーザの特性についてわかってきたこと

- Webトラッキングとプロファイリングの説明とユーザの理解度

  実験中に教育を行っている過去の研究から

  - ユーザは基本的なCookieの仕組みやWebトラッキングの仕組みは理解できる
  - 高度な内容（閲覧履歴やキャッシュとの違い、事業者の識別）は難しい
  - 基本的な仕組みを理解していても各種ツールの適切な利用は困難

- 複雑な内容の理解、高度な設定はできない(やらない)
- 自分の都合の良いように理解する

目次

- ユーザブルプライバシー関連の歴史
  - これまでの取組みと失敗事例
- ユーザブルプライバシーについてわかってきていること
  - 研究動向、ユーザの行動・感じ方
- **情報銀行で考えるユーザブルプライバシー**
  - **これからのこと**

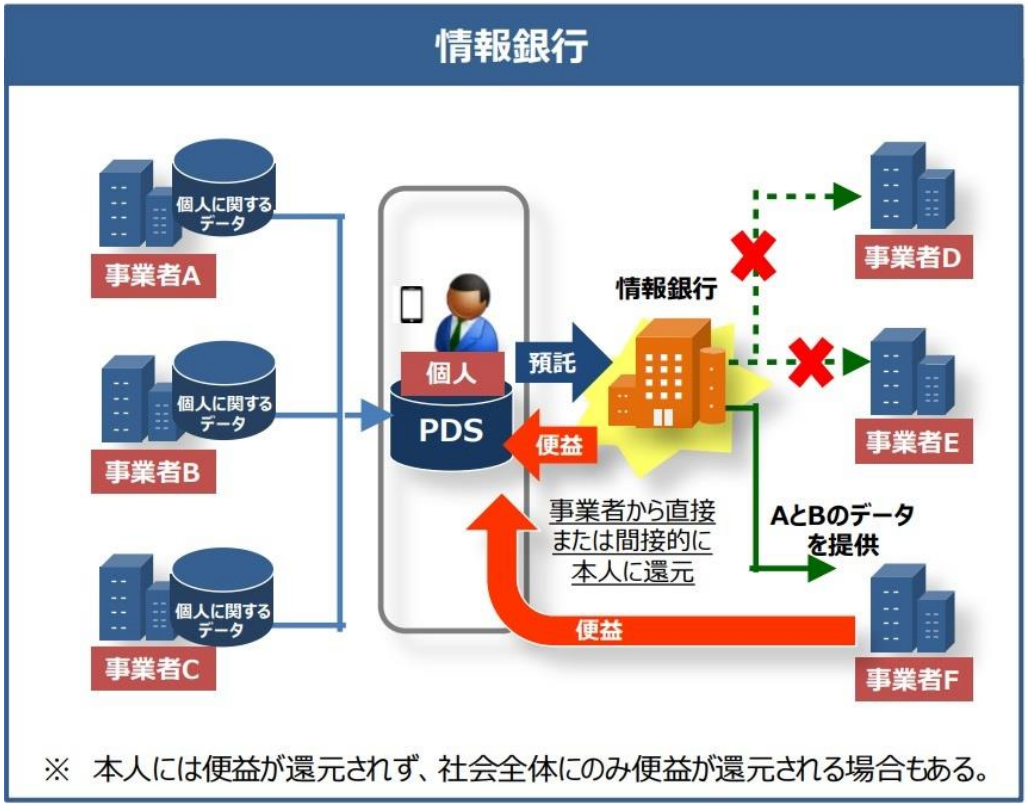
MyData Japan (再掲)

MyDataの原則について

私たちはパーソナルデータに対する**個人中心**のアプローチに向けた取り組みを推進しています。 個人が自身のデータについて十分に理解し、**主体性と主導権**を持って、自らのためにパーソナルデータを活用できる世界を目指しています。 この価値観を共有し、**パーソナルデータのパラダイムを逆転**させる MyData Japan の活動にぜひ参加してください。
MyDataへの宣言に署名し、このパラダイムシフトを推進しましょう。

情報銀行とユーザブルプライバシー

事業者データを
個人が自発的に
収集・統合
できるか



個人が適切に
提供できるか

または信託の
報告を理解
できるか

出典：内閣官房IT総合戦略室「AI・IoT時代におけるデータ活用ワーキンググループ」

ユーザの主体性と主導性

- ユーザが利用できるか
  - アプリの工夫である程度は解決可能
  - しかし高度な操作・設定は難しいかもしれない
- ユーザが意味を理解して利用できるか
  - 自分のデータを提供するという基本的なところは理解可能
  - データ種別の違い、データから推測できることは理解が困難
- ユーザがプライバシーと便益のバランスを取れるか
  - データを理解し、推測される結果を予測できなければ困難
  - 情報銀行が受託者として適切にハンドリングする必要

情報銀行で起こりそうなこと

- ユーザの期待(誤解?)とサービス実態の乖離は必ず起きる
  - この情報を提供したつもりはない
  - なぜこの案内が送られてくるのか

    ⇨ ユーザへのフォローアップが大切

- 難しすぎて使えない
  - なんだかやっぱり仕組みがよく分からない
  - 登録/インストールしてからのハードルが高い

    ⇨ 平均的なユーザが使えるものから
    徐々に理解を促し、便益を提供する

情報銀行は何を目指す？

- Users are products
  - いくつかの大手事業者はユーザのデータを利用しつつプライバシー設定機能を豊富に提供している
- Users are customers
  - いくつかの大手事業者は差別化戦略としてユーザのプライバシー保護強化を宣言している

まとめ

- ユーザブルプライバシーに関する過去の事例を紹介
  - 過去の取組みの多くは失敗している
- ユーザブルプライバシー研究からわかってきたことを紹介
  - 平均的なユーザは多くのことをできない
- 情報銀行でのユーザブルプライバシーを議論
  - 情報銀行は仕組みが複雑（なのでそのままだと失敗する可能性）
  - ユーザビリティを向上させる工夫が必須