野村総合研究所

資料３

諸外国におけるパーソナルデータ流通のための自主規制ルールづくりの動向

2016年5月12日

株式会社野村総合研究所
ICT・メディア産業コンサルティング部　兼　未来創発センター

小林慎太郎

内容

- なぜ、行動規範等の自主規制ルールやマルチステークホルダープロセスの活用が期待されるのか
- 諸外国における自主規制ルールの事例の紹介
  - 米国
  - オランダ
- 今後の議論に向けて

なぜ、行動規範等の自主規制ルールやマルチステークホルダープロセスの活用が期待されるのか

■ データの種別で保護すること、本人の同意に依存することの限界

- 「個人情報」への該当性が不明確なパーソナルデータは、プライバシーリスクが千差万別。
  - かつての「(仮称)準個人情報」(端末ID、IPアドレス、行動履歴等)
  - プロファイリングによる推定データ
- IoTの台頭で、データそのものよりも、コンテキスト(ものごとの経緯)が、よりプライバシーリスクを大きく左右するように変化。その一方で、実効性のある本人同意の取得はより困難に。

⇒データの取扱い(行動)で保護を考えることが必要。ただし、分野ごとのより専門的なプライバシーリスクの評価と対応が求められる。

⇒行動規範(Code of Conduct, CoC)等の自主規制ルール

■ ステークホルダーが多種多様

- モバイル、ソーシャルネットワーク、ビッグデータでは、キャリア、プラットフォーマー、分析事業者等の様々な主体がサービスの提供に関与
- さらにIoTの台頭で、自動車、住宅、家電など、消費者へのタッチポイントが増大し、メーカーがステークホルダーに新たに加わった

⇒サービス提供に関与する一連の事業者が、消費者代表や監督機関と連携して消費者保護のあり方を考えることが必要。

⇒マルチステークホルダープロセス(MSP)

改正個人情報保護法では、認定個人情報保護団体が、「個人情報保護指針」として自主規制ルール作成に努めなければならない、とされている。

■ 改正個人情報保護法　第53条（個人情報保護指針）

- １項　認定個人情報保護団体は、対象事業者の個人情報等の適正な取扱いの確保のために、個人情報に係る利用目的の特定、安全管理のための措置、開示等の請求等に応じる手続その他の事項又は匿名加工情報に係る作成の方法、その情報の安全管理のための措置その他の事項に関し、**消費者の意見を代表する者その他の関係者の意見を聴いて、この法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成するよう努めなければならない**。
- ２～４項略

（参考）パーソナルデータの利活用に関する制度改正大綱（平成26年6月24日，高度情報通信ネットワーク社会推進戦略本部）

Ⅱ 制度改正内容の基本的な枠組み

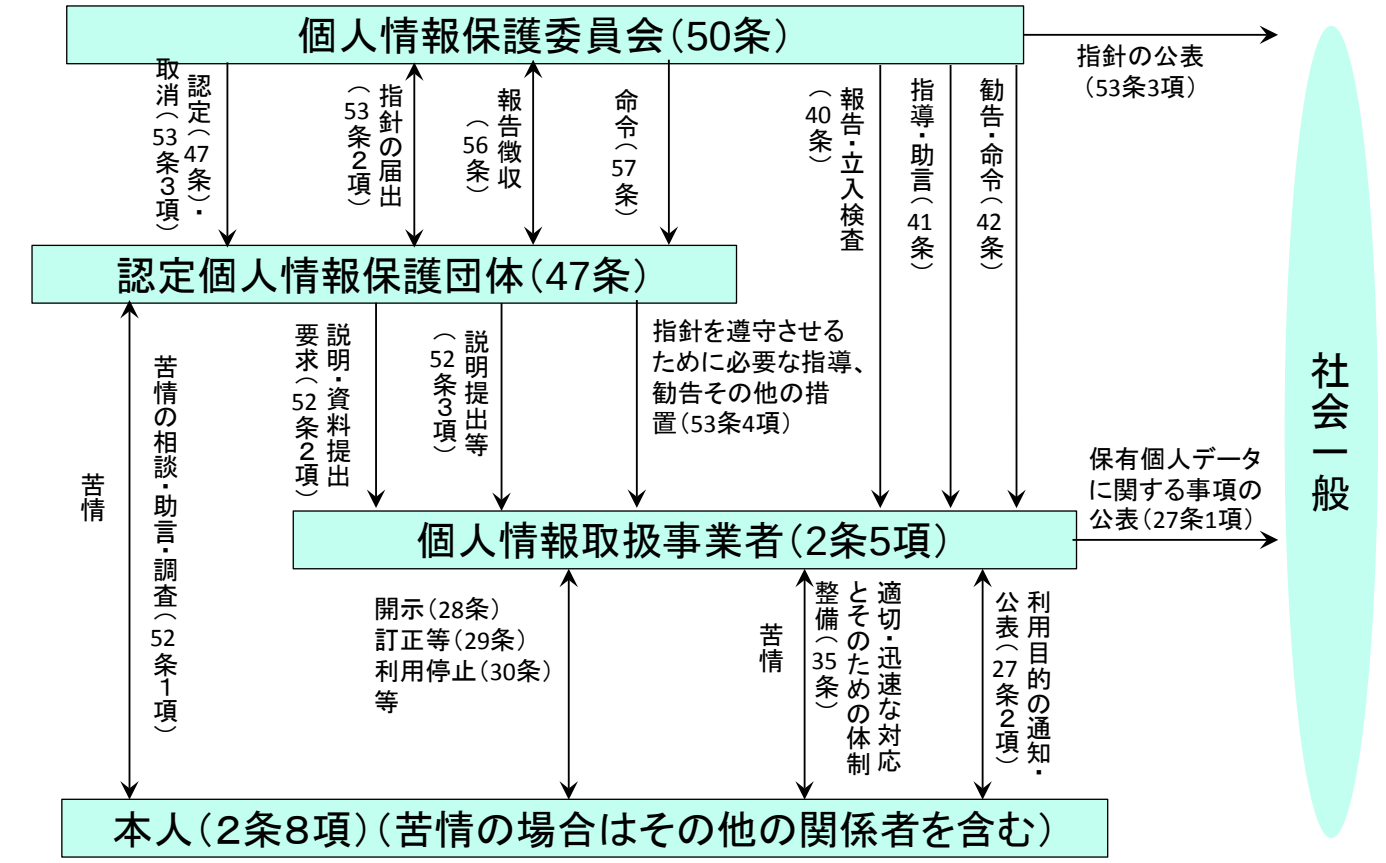
１ 本人の同意がなくてもデータの利活用を可能とする枠組みの導入等

２ 基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用

グレーゾーンの内容や個人の権利利益の侵害の可能性・度合いは、情報通信技術の進展状況や個人の主観等複数の要素により時代とともに変動するものであることから、これらに機動的に対応することを可能とするため、社会通念等も踏まえつつ、法律では大枠を定め、具体的な内容は政省令、規則及びガイドラインにより対応する。また、これと併せ**民間の自主規制ルールの活用を図る**こととする。

３ 第三者機関の体制整備等による実効性ある制度執行の確保

個人情報の取扱いに関する委員会と認定個人情報保護団体の役割



※「指針」:「個人情報保護指針」のこと

出所）関啓一郎「ポイント解説　平成27年改正個人情報保護法」ぎょうせい（2015年）

諸外国における個人情報の保護と活用に係る自主規制ルールの事例

国	自主規制の例	作成主体	法的根拠	公的機関の関与
米国	モバイルアプリの通知に関する行動規範	アプリ開発協会、消費者団体等のマルチステークホルダー	なし（ただし、FTC法5条の執行対象）	商務省電気通信事業庁（NTIA）が主導。執行機関（FTC）もオブザーバで参加。
米国	デジタル広告に関する自主規制プログラム	DAA（米ネット広告団体） ※執行主体はBBB（民間の消費者保護機関）	なし（ただし、FTC法5条の執行対象）	執行機関（FTC）の方針が尊重されている。非公式な相談対応がなされている。
EU	スマートメータのプライバシー影響評価（PIA）のフレームワーク	スマートメーター関連事業者	EUデータ保護指令27条	EU構成国の監督機関によるWP（29条委員会）が、審査・承認。
EU	データ保護に関するクラウドサービス提供者の行動規範（作業中）	クラウド産業グループ	EUデータ保護指令27条	同上（ただし、現状は審査の途中段階）
オランダ	業界別の行動規範	製薬、生命保険、医療保険、通信販売、スマートメーター、探偵等の各業界団体	オランダ・個人情報保護法	個人情報保護の監督機関（CBP）が行動規範の内容を審査・承認。
シンガポール	生命保険会社におけるパーソナルデータの取扱いに関する行動規範	生命保険協会	なし	個人情報保護の監督機関が作成時に意見・示唆を提供。 監督機関のウェブサイトに掲載。

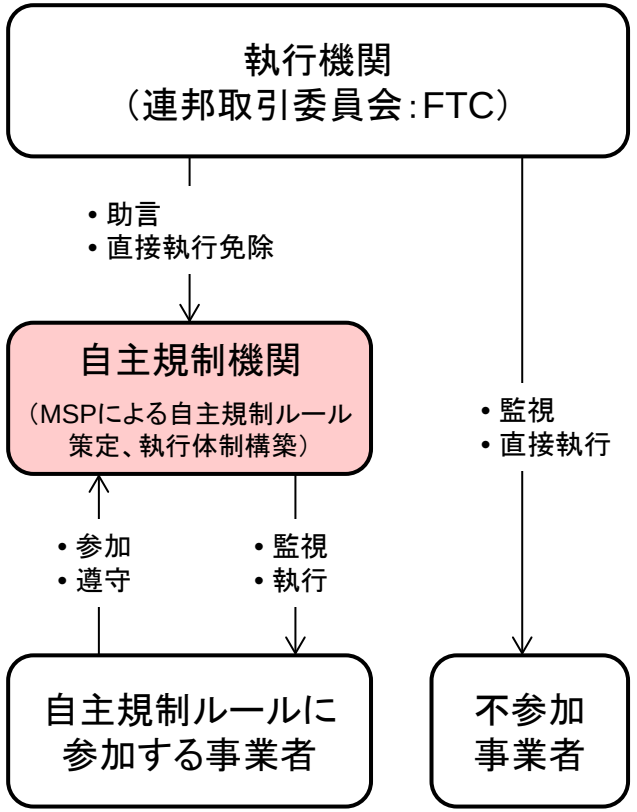
米国商務省・電気通信情報局（NTIA）によるマルチステークホルダープロセス（MSP）

■ 自主規制の構造的な問題
- 団体に参加する事業者の都合のいいようにルールが作られる。
- 執行体制に独立性が欠けて、エンフォースメントが機能しづらい。
- 不参加企業が出る（正直者が損をする）。

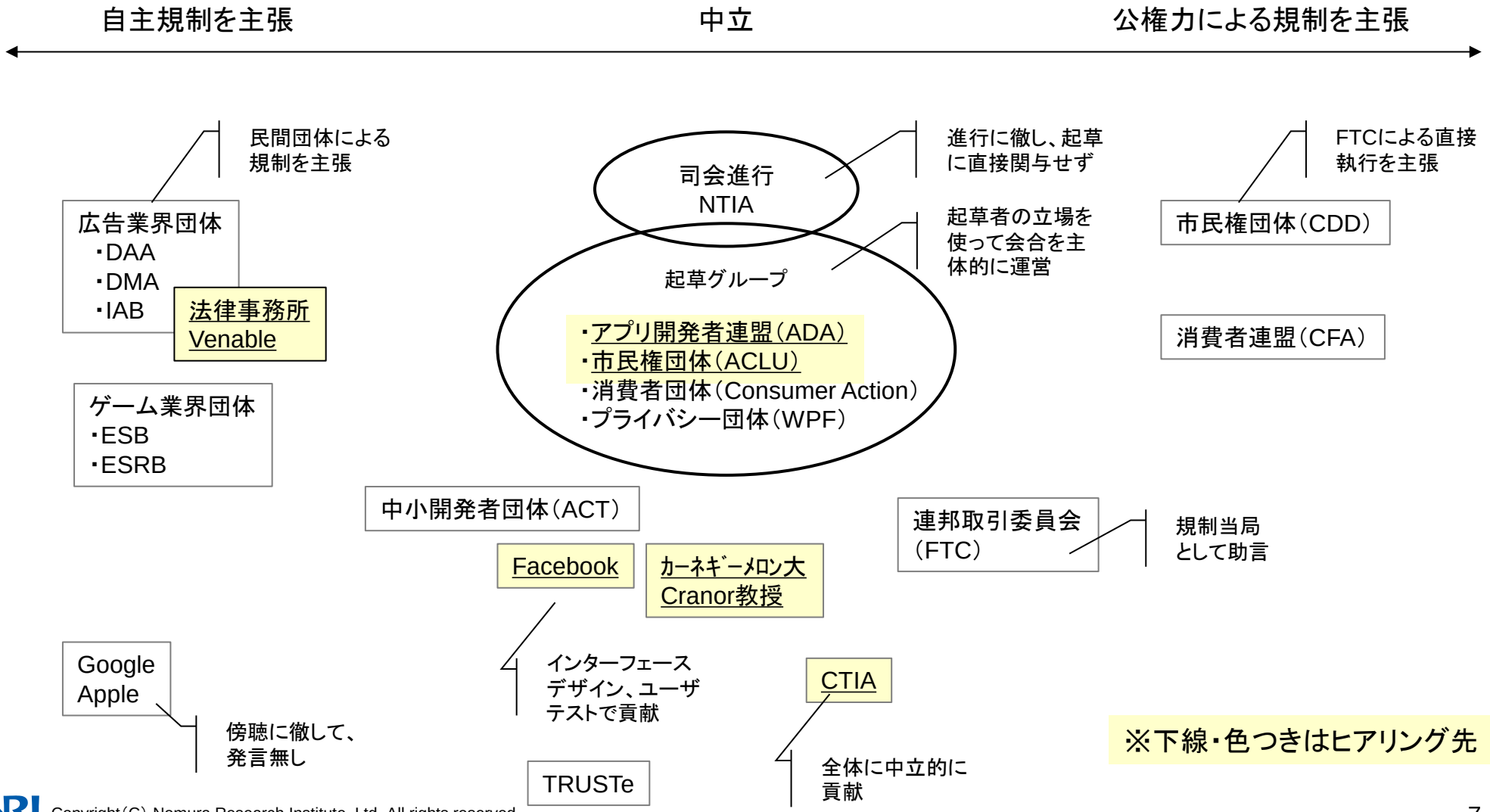
■ NTIA・MSPは、自主規制の問題を解消するため、ホワイトハウスの指示を受けて取り組まれた。
- 多様なステークホルダーの意見を調整。
- 執行機関が、MSPに参加して意見や助言をする。
- ルールへの参加事業者は、直接執行を免除される。
  ※最終的に、FTCは直接執行免除を約束せず。

＜事例＞
- モバイルアプリの通知に関する行動規範
- 顔認証技術に関する行動規範
- セキュリティ脆弱性の開示に関する行動規範

NTIA・MSPによる自主規制スキーム（目標像）



モバイルアプリの通知に関する行動規範のマルチステークホルダープロセス参加者の関係



MSPの長所、課題等

■ 起草グループ

（MSPの長所）

- オープンで、透明であること。誰でも参加でき、議論がみえるため、正当性を打ち出すことに寄与する。（ADA）
- ルール構築を、立法措置及び行政機関主導の取組に比べて迅速に行える。（ADA，ACLU）

（MSPの課題等）

- 参加者には、各分野の確固とした代表性が求められる。消費者団体、業界団体など、誰の利益を代弁しているのかが明確である必要がある。（ACLU）
- 目的・意義の方向性が異なるステークホルダーを多く参加させすぎたことで、メリットであるスピーディさが失われてしまった。（ADA)
- 真に消費者のことを考えているステークホルダーのみにするべきだった(ACLU)

■ その他の参加者

（MSPの長所）

- 検討と制度の構築が通常の法制度に比べ迅速に行える。政府が直接的に運営しようとすると、公示等の様々な手続きが求められることになってしまうため、時間がかかる。（CTIA）

（MSPの課題等）

- 一部の個人的な関係が大きく影響を与えすぎた。重要な協議や議論がMSP外で行われていた。(CTIA)
- 参加者が、それぞれ代表している団体の規模を考慮した意見の集約がなされていない(Venable)
- 意思決定のプロセスが不透明。議事録を始めドキュメントの回覧等が不十分。会議に毎回出席できない遠方の参加者への配慮が必要。（CMU）
- 取りかかりの段階で、何が明確なゴールであるか定義が必要。（CMU）

ルール作りのためのMSP運用上の要諦（日本への示唆）

1. ゴールの明確化

- 予め、何がゴールであるか 、どのような状態になれば完了なのか、明確な定義が必要。

2. オープン性の確保

- 議論の経緯、論点は、極力オープンにする。
- 毎回の参加が難しい参加者もいるため、資料共有、議事録の回覧等により情報共有・公開に努める。

3. 非公式な会合の活用

- 一堂に会する場以外に、各ステークホルダーと個別の調整を行うことで、意見調整を図る。
- ただし調整の対象を、一部のステークホルダーに偏らないよう配慮が必要

4. 執行機関／行政機関の関与

- 執行機関の見解を考慮しながら検討する。
- 行政機関の関与を通じて、議論を円滑化する（NTIAの果たした役割）。

5. 参加者の代表性への配慮

- 消費者団体、業界団体など、誰の利益を代弁しているのか、また、参加者が、それぞれ代表している団体の規模を考慮した意見の集約を行う。

6. 執行性の確保（アメとムチ）

- 参加する（ルールを遵守する）ためのインセンティブが必要。
- あわせて、ルールに拘束力を持たすための仕組み（監視機関やペナルティの設置など）が必要。

＜参考＞　モバイルアプリの通知に関する行動規範（2013/7/25版ドラフト）

■ 簡易通知画面での明示情報

（収集するデータ要素）

- 生体情報（指紋、顔認識、署名、声紋）
- ブラウザのログ（閲覧したWebサイトのリスト）
- 電話、テキストのログ（発信・着信した電話又はテキストメッセージ）
- 連絡先（SNSのコンタクトリスト、電話番号、住所、電子メールアドレス）
- 金融情報（クレジット、銀行、取引データなど）
- 健康、医療、治療情報（診療請求情報、健康ウェルネス測定情報）
- 位置情報（過去・現在の正確な位置、行動履歴）
- ユーザファイル（カレンダー、写真、テキスト、ビデオなどのデバイスに格納されている情報）

（データ共有する外部事業者）

- 広告ネットワーク事業者
- 通信キャリア
- 消費者データの再版事業者
- データ分析事業者
- 政府機関
- OS・プラットフォーム事業者
- 他のアプリ
- ソーシャルメディア事業者

（簡易通知画面の例外）

- アプリ機能の維持・改善・分析に用いる場合
- ネットワーク通信に用いる場合
- ユーザの認証
- 広告の頻度を制限する場合
- ユーザやアプリのセキュリティや完全性保護の場合
- 法令を遵守するための場合
- ユーザのデバイス上でユーザにアプリを利用できるようにする場合（OSへ対応する場合）

＜参考＞ モバイルアプリの通知に関する行動規範（2013/7/25版ドラフト）

- 簡易通知画面のデザイン要素
  - A) テキスト又はアイコン・シンボルで表示
  - B) テキストの詳細情報を別画面等で表示
  - C) 所定のデータ項目以外について、小さい文字で表示してよい
  - D) 実現可能な場合、アプリ開発者を同一画面上に太字テキストで表示
  - E) 消費者が容易に簡易通知画面から詳細情報へ遷移できる
  - F) テキストとフォントがはっきりしている
  - G) 簡易通知はアプリから容易にアクセスできる
  - H) 簡易通知は、ユーザアプリのインストール前に要求しなくてよい
  - I) アプリ開発者は、データ収集やデータ共有の方針に大きな変更を加える場合は、消費者に通知して同意を取得する

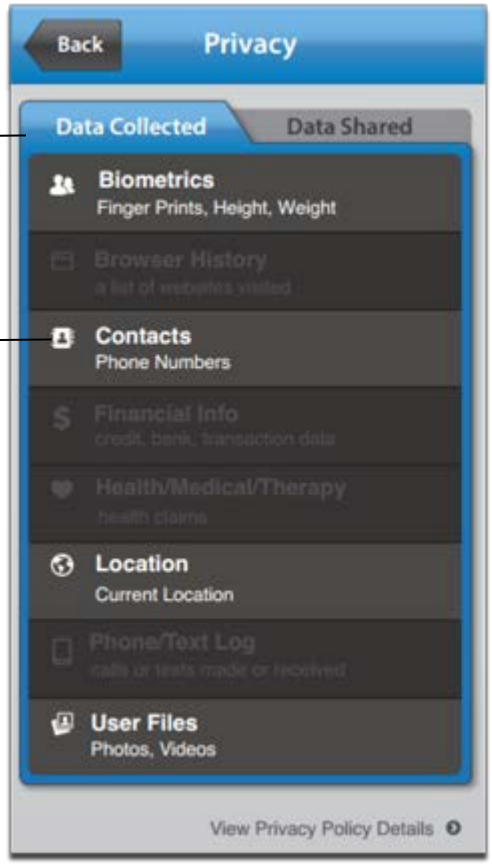
- データ利用ポリシー、利用規約、プライバシーポリシー（正規版）とのリンク
  - 簡易通知画面に加えて、関係するアプリ開発者・提供者は、データ利用ポリシー、利用規約、プライバシーポリシー（正規版）へ消費者が容易にアクセスできるようにする

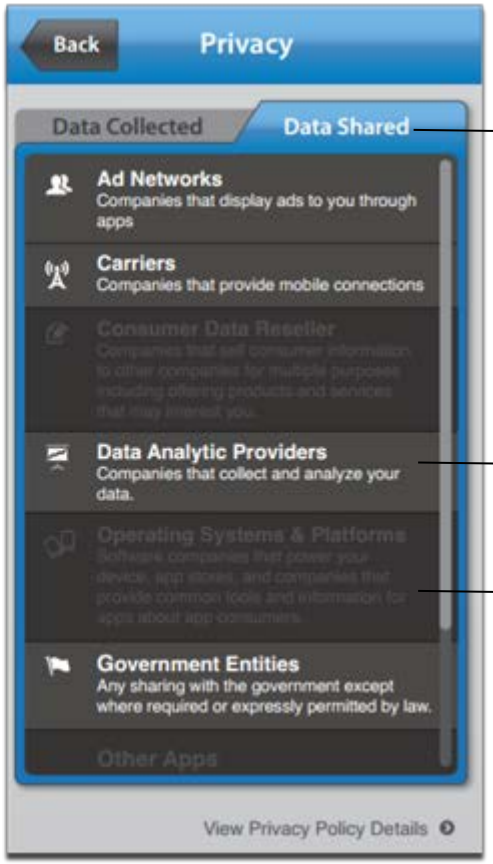
＜参考＞MSP終了後に作成されたモバイルアプリの通知画面のインターフェースデザイン

モバイルアプリの通知画面のデザイン

取得するデータ
項目を表示

データ項目を
アイコンで表示





データを共有する
外部事業者カテゴリを表示

共有する事業者を
ハイライト表示

共有しない場合は
グレイアウトして表示

出所）NTIAウェブサイトの情報をもとに作成

オランダでは、個人情報保護の領域で、業界ごとの行動規範（CoC：Code of Conduct）が、20年以上運用されている。

- オランダは、1989年個人情報保護法において、業界団体が起草して、オランダ個人情報保護の監督機関（CBP）が認定する行動規範の制度を導入。
  - オランダ社会が信用（TRUST）で回っていて、自主規制が尊重されていることが背景にある。ドイツと異なる。
  - オランダでは、信頼が非常に重要視され、このため企業が設置するコンプライアンスオフィサーの地位は高い。ジェネラルマネージャーよりも高いことがある。オランダの伝統。
- 行動規範が作成されている業界の例（過去の20種以上作成されている。）
  - 製薬
  - 生命保険、医療保険
  - 通信販売
  - エネルギー（スマートメーターに関する取扱い）
  - 探偵　　等
- 行動規範は、法律の条文を解釈して、実際にデータ処理する規範を示したもの。行動規範に基づくと、データ処理の遵法性を確信できる（CBPから直接執行を受けることなく個人情報を取り扱うことができる）。
  - CBPが行動規範の遵守状況をチェックすることはない。
  - 業界団体の中には、会員企業における行動規範の遵守状況の自己評価の報告を受けているところもある。
  - 業界に加盟していなくても、行動規範を活用してもよい。
- 行動規範の有効期限は5年。

出所）CBP、オランダ製薬工業協会（Nefarma）、オランダ保険協会（VvV）へのヒアリング（NRI自主調査2015年）に基づく。

オランダの行動規範の審査プロセスと考え方

審査プロセス

- 民間団体がCBPに申請。CBPは申請を受理してから13週間以内に事前評価結果（Preliminary Decision）を出す。
- その後、6週間のパブリックコメントにかける。
- パブリックコメント終了後は、どのパブリックコメントをどのように取り入れるかは、先ずCBPが検討し、申請者である民間団体に指示を出す。
- 民間団体は再度行動規範を修正してCBPに提出する。
- CBPは再修正案を審査し、最終評価結果を出す。承認された場合は、官報に公示される。
- 全工程は、ペーパーワークが基本で、ドラフト提出から6ヶ月以内に終えなければならない。

審査の考え方

- 行動規範を作成するプロセスにおいて、民間団体とCBPとの間で話し合いが行われるが、これを交渉と呼ぶのは適切ではない。CBPは、基本的権利を保護するための機関で有り、基本的権利は絶対なものであり、交渉可能なものでは無い。基本的権利に照らして、適切かどうかを判断する。交渉のように、取引をするようなことはありえない。
- 民間団体が作成したドラフトに対して、CBPは書面で、改善すべき点等を回答する。
- その後、CBPは、民間団体を招集し、改善すべき点の解説をする。民間団体からもデータ取り扱いの意味について解説をうける。前述のとおり、これは交渉ではなく、改善すべき点等を明確にするために行う。
- データ処理をする場合、なぜその処理が必要なのかをクリアにしなくてはならない。CBPは民間団体に対して、人々が理解できるように、データ処理の理由を明確化することを求める。
- 民間団体はその後ドラフトを修正し、CBPに提出する。

出所）CBP、オランダ製薬工業協会（Nefarma）、オランダ保険協会（VvV）へのヒアリング（NRI自主調査2015年）に基づく。

製薬、保険業界の事例

■ オランダ製薬工業協会（Nefarma）の事例

（作成）

- 行動規範は、Nefarmaが2人、CBPが2人の4人がドラフトの作成に関与。ドラフトは、Nefarmaの委員会に諮り、承認を得た後に、CBPに承認申請をする。
- ドラフト作成段階で、医療協会、先端製薬社会、患者消費者連盟（NPCF）に照会をかけている。このうち、NPCFは、消費者を代表する機関と見なすことができ、Nefarmaの行動規範は、消費者代表の意見を反映しているものということができる。
- ドラフト作成段階で主要なステークホルダーから意見をとりいれているので、パブリックコメントをしても、大きな変更が必要となることはない。

（運用）

- 会員企業の自主的な運用に任されている。Nefarmaが会員企業をチェックすることはない。そもそもNefarmaの行動規範を採用する際に、公式な署名プロセスはない。実質的に誰が使ってもよい。
- この結果、Nefarmaの会員にならずに、Nefarmaの行動規範を利用するフリーライダーはいるだろう。

■ オランダ保険協会（VvV）の事例

（作成）

- VvVがドラフトを作成し、CBPに提出する。作成にあたって、CBPに相談している。
- パブリックコメント期間の終了後、CBPは意見をふるいにかけ、VvVに対して、修正指示を出す。修正対応は、反映しないと行動規範を承認してもらえないことになるので、クリティカル。
- ドラフト作成段階では、消費者代表は関与しない。パブリックコメントを通じて消費者や一般の意見を収集し、反映する。

（運用）

- 各会員企業に、チェックリストのようなものを提示して、自己評価を依頼し、報告を受けている。毎年1回。
- CBPが、この自己評価プロセスに関与することはない。自己評価結果を求めることもない。
- 規範はオランダ国内でしか有効でない。

出所）CBP、オランダ製薬工業協会（Nefarma）、オランダ保険協会（VvV）へのヒアリング（NRI自主調査2015年）に基づく。

今後の議論に向けて

1. 行動規範等の民間自主ルールは、法令等を補完する仕組みとして活用していくべき
   - IoTの台頭で、データの種別で保護すること、本人の同意に依存することが限界に来ており、データの取扱い（行動）で保護を考えることが必要。ただし、分野ごとのより専門的なプライバシーリスクの評価と対応が求められ、法令等の枠組みでは対処が難しい。
   - 行動規範は、プライバシー保護の分野で世界的に活用されており、日本でも改正法でできた「個人情報保護指針」の活用を促進する仕掛け、あるいは、民間の自主ルール作成を支援する施策を推進するべき。

2. マルチステークホルダープロセスは、国が民間を伴走しながら取り組むべき
   - 米国のマルチステークホルダープロセスは政府と民間がともに試行錯誤の最中。日本においても、初期段階では国が積極的に関与して、わが国の制度・慣習に適した方法を追求していくことが必要。
   - 例えば、法53条「消費者の意見を代表する者その他の関係者の意見を聴いて」は、業界やサービスの特性に応じて、検討会、パブリックコメント、消費者アンケートなどの方法を適切に組み合わせて実施していくのはどうか。

3. ルール作りは、プライバシー保護の原則、フレームワークを使って考えていくことが大事
   - 定型的な取り扱い義務の定められている個人情報と違って、ビッグデータ／IoT活用では、相手との関係や背景や状況などの“コンテキスト”によって、対応を考える必要がある。
   - プライバシー保護の基本に立ち返って、OECD8原則やISO/IEC 29100プライバシーフレームワークを活用してバランスよく取り組むことが大事。

＜参考＞ OECD8原則

OECD8原則

原則	原則の内容
目的明確化	収集目的を明確にし、データ利用は収集目的に合致するべき
利用制限	データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない
収集制限	適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき
データ内容	利用目的に沿ったもので、かつ、正確、完全、最新であるべき
安全保護	合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき
公開	データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき
個人参加	自己に関するデータの所在及び内容を確認させ、又は異議申立を保証するべき
責任	管理者は諸原則実施の責任を有する

出所）個人情報保護法制化専門委員会（2000年）

＜参考＞ ISO/IEC 29100 プライバシーフレームワーク

ISO/IEC 29100 プライバシーフレームワークの11原則

原則	OECD8原則との対応	主な内容
1. 同意と選択	対応する原則はない。	本人に、明確で分かりやすくアクセスしやすい選択の仕組みを提供し、データ処理に対する同意を取得する。 本人が同意時に、自分の好みにあった設定をできるようにする。
2. 目的の正当性と詳述	「目的明確化の原則」に対応	OECD8原則と同等
3. 収集の制限	「収集制限の原則」に対応	OECD8原則と同等
4. データ最小化	対応する原則は無い	データの処理を必要最低限にする。 処理する者を最低限にする。 個人の特定、他データとの照合、属性推定を制限する。
5. 利用、保持、開示の制限	「利用制限の原則」に対応 保持や廃棄の制限がより明確になっている。	正当な利用目的の範囲の中で、データの利用、保持、開示をする。 必要最低限の期間だけデータを保持し、期間が過ぎたら安全に廃棄するか匿名処理をする。
6. 正確性と品質	「データ内容の原則」に対応。 プロファイリングに伴うリスク対策を含意している。	利用目的に沿ったもので、正確、完全、最新のものとする。 不正確なデータによって、個人に実害が生じうる場合は、特に重要。
7. オープンさ、透明性、通知	「公開の原則」に対応	OECD8原則と同等
8. 個人の参加とアクセス	「個人参加の原則」に対応	OECD8原則と同等
9. 説明責任	「責任の原則」に対応	OECD8原則と同等
10. 情報セキュリティ	「安全保護の原則」に対応	OECD8原則と同等
11. プライバシー法令遵守	対応する原則は無い	個人情報・プライバシー保護の関連法令を遵守する。

出所）小林慎太郎「パーソナルデータの教科書」日経BP