

米国における顔認識技術の商用利用と プライバシー保護について

2016年9月
(株)国際社会経済研究所
小泉 雄介

米国調査概要(2016年6月下旬実施)

- 調査目的
 - 米国における顔認識技術の商用利用の実態と法令・ルール化の動向に関する調査
- 訪問先機関

国名	訪問先機関	概要
米国	National Telecommunications and Information Administration (NTIA: 電気通信情報局)	米国商務省傘下の組織。顔認識技術の商用利用に関するマルチステークホルダープロセスを主催。
	U.S. Government Accountability Office (GAO: 米国会計検査院)	連邦議会の下で調査を行う組織。顔認識技術の商用利用とプライバシー問題に関する報告書を発行。
	Federal Trade Commission (FTC: 連邦取引委員会)	民間分野における個人情報取扱いを監督する第三者機関。顔認識技術のベストプラクティスに関する報告書を発行。NTIAのマルチステークホルダープロセスにも参加。
	National Retail Federation (NRF: 全米小売業協会)	小売店における監視カメラ・顔認識利用(防犯利用、マーケティング利用)についても所轄。
	International Biometrics & Identification Association (IBIA: 国際バイオメトリクス・アイデンティフィケーション協会)	生体認証技術ベンダー企業とユーザ企業から成る業界団体。NTIAのマルチステークホルダープロセスにベストプラクティス案を提出。
	Consumer Federation of America (CFA: 全米消費者協会)	顔認識技術の商用利用に関するマルチステークホルダープロセスに参加していたが、他の消費者団体とともに2015年6月にプロセスから離脱表明。

1. 顔認識技術の商用利用の状況

2. 顔認識技術の商用利用に関する法令・ルールの検討状況

米国における顔認識技術の商用利用の状況(1/4)

- 米国では、(日本に比べて)[商業施設における顔認識技術の利用が進んでいる訳ではない](#)。利用が進んでいるのは、SNSにおける写真のタグ付けや、スマートフォン等へのログイン時の本人確認の用途である。

(1) 比較的利用が進んでいる利用方法

• ① 写真の識別/照合と整理

- [SNSにおける写真のタグ付け](#) (Facebook、Google)
 - FacebookのTagSuggest機能(顔照合)
 - 利用者がアップロードした写真に人物が含まれる場合、既に当該利用者と「友人」関係にある人については、その人が誰であるかの「タグ」を「サジェスト」する機能である。
 - 2012年にFacebookはこの機能を一時中断したが、2013年に再開された。
- PC内の写真アルバムの整理(自分の子どもの写真等)

• ② セキュアなアクセス

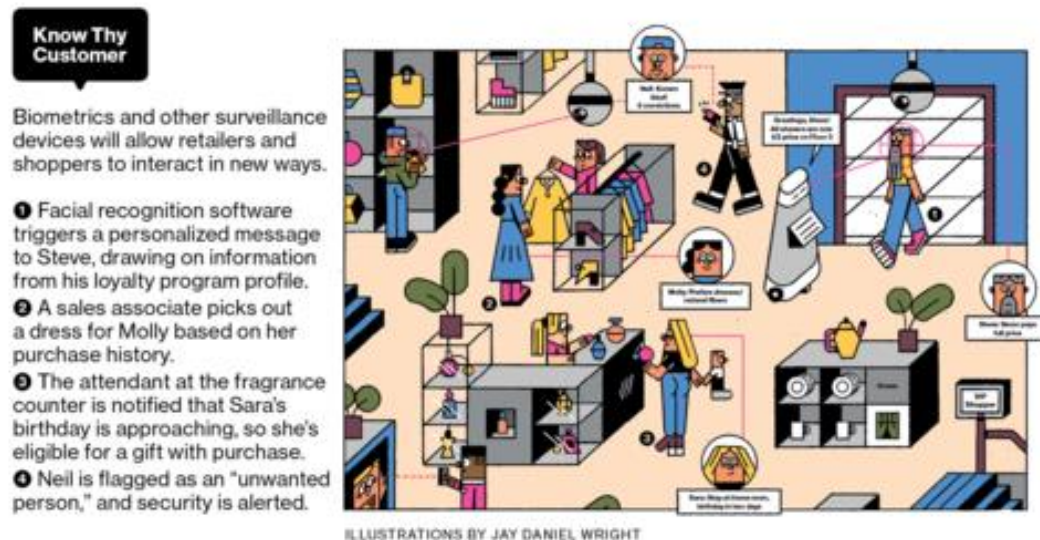
- PCやスマートフォンへのアクセス(アンロック機能におけるパスワードの代替)
- [モバイルペイメント](#)
 - マスターカードは「selfie pay」という、スマホサイトでのクレジットカード決済時に顔認識で本人確認するアプリを開発。カナダのモントリオール銀行がコーポレートカード利用者向けに、2016年夏から導入。
- 建物内のセキュアなエリアへの物理的アクセス
 - A社では会社の受付で従業員や常連のビジターを顔認識を用いて見分けている。
 - B社では、駐車場のゲートに警備員がいて写真付きIDを見せるが、車の窓越しに顔認識をしてID写真と照合できるかを実験している。

米国における顔認識技術の商用利用の状況(2/4)

(2)パイロット(試験運用)中／一部実用化された利用方法

③セーフティとセキュリティ

- **小売店**: 窃盗防止目的で、顔認識ソフトウェアを備えた防犯カメラシステムを試験運用(書店や衣料品店等)。来店客の画像を、**既知の万引き犯**や犯罪組織メンバー等の画像DBと比較する。マッチングした場合、警備員や管理者にアラートが送られ、当該人物に関する既知の情報が送られる。
- **カジノ**: 既知のギャンブル詐欺犯や犯罪組織メンバー等を識別するために利用している。カジノは顔認識のメジャーユーザーである。カジノ内で歩ける場所が決まっているので、顔画像を撮りやすい。
- **金融機関**: 幾つかの金融機関の防犯システムにも、強盗容疑者等を識別するために顔認識ソフトウェアが組み込まれている。
- **アパートメント**: 顔認識システムにより住民と非住民を識別。



図の出典:
Bloomberg記事

米国における顔認識技術の商用利用の状況(3/4)

(2)パイロット(試験運用)中／一部実用化された利用方法

④マーケティングと顧客サービス

- 電子看板：既に顔認識技術が一部で利用されている。閲覧者の性別、年代といった属性を推定し、それに応じたターゲット広告を提示する。小売店や広告者はリアルタイムで、消費者に関連する製品やセールを表示することができる。将来的には電子看板を用いて顧客の氏名を識別したり、過去の購買履歴やその他の個人情報に基づいてターゲット広告を行なったりすることも想定されるという。
- 小売店における電子看板以外の用途としては、顧客の店内での動線を追跡して商品レイアウトの変更等の顧客サービス改善のために利用することや、既存顧客が入店した際に店員にアラートを送ることも想定できるという。これらは現時点での利用というよりは、将来的なポテンシャルのある用途である。
- NRFによると、米国ではこれらの用途はまだ模索中であり、進み方がゆっくりしている。
- あるベンダー企業は、小売店舗でリピーター顧客にポイントを付与する際に顔認識を使うパイロット実験を行っている。例えば、バーでビールを頼むとき、オプトインで登録してもらい、1回目がギネスだったら、2回目もギネスを勧めたりする。これは、個人に向けたターゲット広告の1つの方法とも言える。

※Bloomberg Intelligenceによれば、米国においてはWalmart、Macy's、Giorgio Armaniが、欧州においてはBenettonが顔認識技術を検討もしくはテストしているという。Macy'sとBenettonは公式にはそれを否定した。

※顔認識技術は旧来のブリック&モルタルの小売店にとって、オンラインショッピングサイト(顧客からより多くのデータを取得できる)との競争において必要であるという。

小売店舗における利用事例： Saks Fifth Avenue

- 「米国の高級百貨店Saks Fifth Avenueは、2016年にカナダ・トロントに新店舗をオープンした。この店では、世界で最もアグレッシブで最先端な店内セキュリティと顧客サーベイランスの手法がとられている。
- カナダの小売企業においては年間46億ドルの「シュリンケージ(万引きや内部犯行によって商品が盗まれ、在庫数が減少すること)」が発生しているが、組織的小売店犯罪はこの約半分を占める。
- Saksは[小売店での紛失防止](#)において、より議論が多く、潜在的に侵害的な方策、すなわち[顔認識ソフトウェアの早期導入者](#)である。顔認識技術は最近までは、物理的世界では、主に空港セキュリティ、国境管理、カジノ、警察で使用されてきた。
- 小売店用の顔認識アプリケーションにおいては、カメラで撮られた個人の顔は顔特徴データに変換され、過去の万引き犯や犯罪者のDBと照合される。[米国の店舗の中には、万引き容疑犯に対して警察に知らせる代わりに写真撮影許可のオプションを与えるところがある](#)。これらは全て、ネットワーク化された高解像度のセキュリティカメラと急速に進歩した分析機能の出現によって可能となった。
- 2014年に開催された紛失防止カンファレンスでのあるプレゼンで、Saks親会社の資産保護システム担当シニアマネージャーは、顔認識ソフトウェアの導入経験を語った。この新しい技術のいくつかの制約を示しながらも、彼は「求める結果は間違いなく得られる」と語った。Saksの全ての店舗のカメラはネットワーク化され、ニューヨークの本社で映像を見ることができる。
- [どのように見られるかを心配して、大手小売店は顔照合を行っていることをほのめかさないように注意深い態度を取ってきた。Saksは顔認識ソフトウェアを使っているか否かについてのコメントを拒否した。」](#)

(The Guardian記事“Revealed: how facial recognition has invaded shops – and your privacy”(2016年3月3日)より抄訳)

小売店舗における利用事例： Nordstrom

（顔認識ではなく、スマホWiFi機能の利用事例）

- 2012年10月から2013年5月頃まで、大手百貨店のNordstromが、EuclidというスマートフォンWiFi通信機能を利用したサービスを、全米の17店舗でトライアル。
 - Euclid: スマートフォンのWiFi機能を用いて顧客の店内での動きを追跡するサービス。
- 顧客のスマートフォンのWiFi機能がONになっている場合、店舗内のセンサーがスマホの識別情報を収集できる。顧客がどの店舗を訪問し、どのくらい滞在したかをモニターできる。ただし、異なる店舗間で顧客を追跡したり、スマホ所持者の個人情報を識別したりはできない。
- Euclidを使うことにより、混雑時のスタッフ配置を増やしたり、商品のレイアウトを変更する際の判断材料にできるという触れ込みであった。
 - ショーウィンドウを見てから店内に入る顧客のカウントができる。ショーウィンドウのディスプレイを変えることで店内に入る顧客をどのくらい増やせるかの測定に役立つ。
 - 顧客の店内での滞在時間を測定できる。また、店内での顧客トラフィックを測定することにより、曜日や時間帯におけるトラフィックの増減をより正確に予測できる。
 - Euclidは1センサー当たり月額200ドルの料金。
- Nordstromは店舗の入口に、スマホのWiFi機能をOFFにすることによりオプトアウトできるとの消費者向け通知を掲示していた。
- しかし、マスコミ報道もあって、顧客からはネガティブな反応を受け、約半年間のトライアルの後に同サービスを停止した。

米国における顔認識技術の商用利用の状況(4/4)

- ⑤その他

- 顔画像検索:

Googleには「この画像と類似した画像を探す」画像検索機能がある。

- 出会い系サイト:

いくつかの出会い系サイトは顔認識技術を利用し、あるユーザが最も魅力的と感じる顔の特徴を割り出し、同様な特徴を持った個人を会員データベースから検索している。

- 記憶補助:

スマートフォン用の記憶補助アプリ。相貌失認患者などに対して、面会者の氏名等を教えてくれる。

- ギャンブル依存症治療プログラム(カナダの事例):

患者の自己申告によるプログラム。患者が登録した顔写真をカジノに提供し、来店してしまった際に出て行ってもらようようにする。

【ご参考】 米国における新たな顔認識サービス

- Facedeals

- Redpepperという米国テネシー州の広告企業が2012年に開発し、2013年1月にFacedeals社として独立。同年からパイロット実施。



写真の出典: techcrunch.com

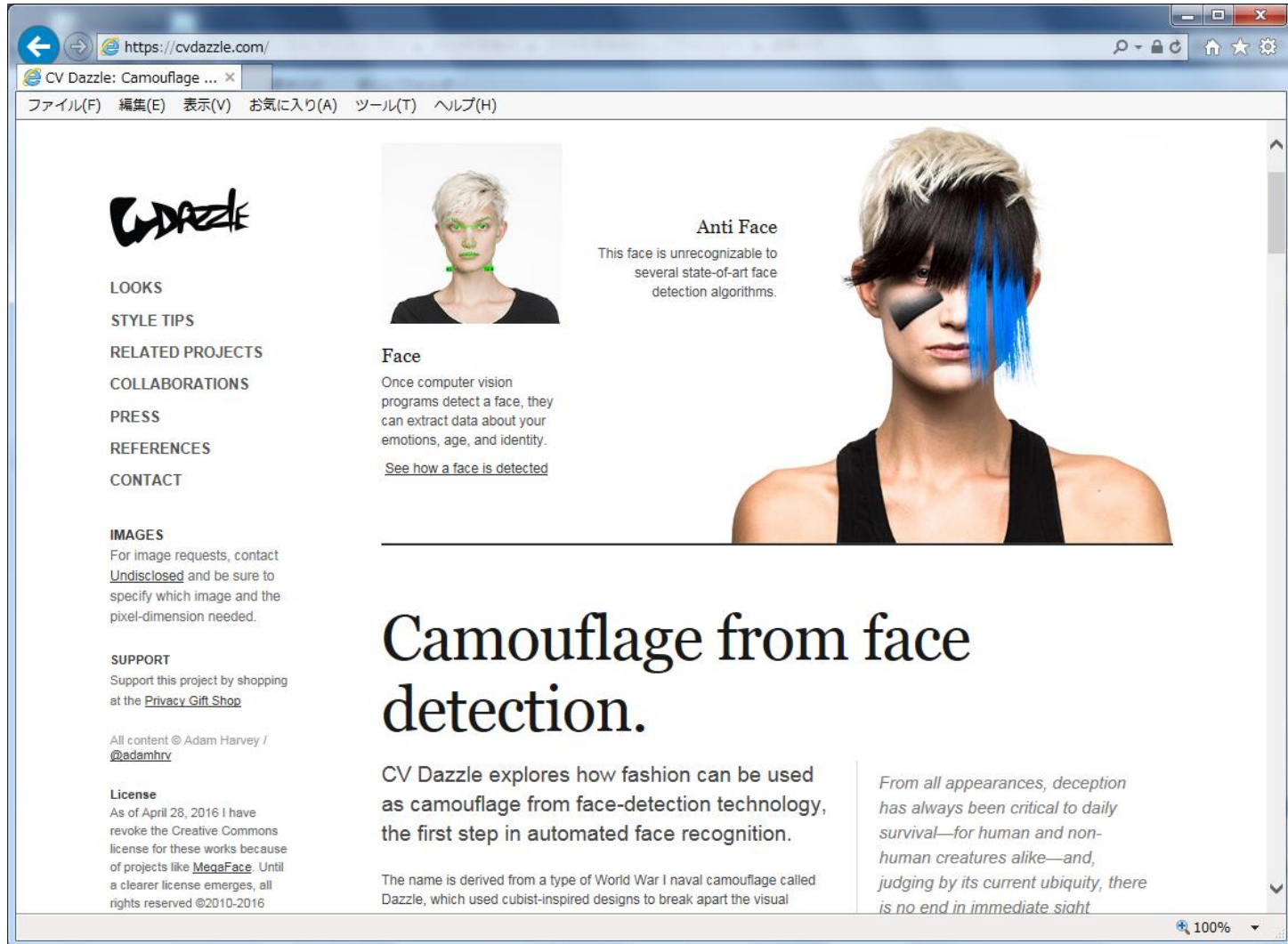
- 利用方法

- 利用者はFacedealsアプリ(Facebookの連携アプリの1つ)をスマートフォンにインストールする。
 - ※同アプリをFacebookが公認しているわけではない。
- Facebookアカウントでログインし、自分の写真や「いいね」履歴データを同アプリが利用することを許可する(オプトイン)。
- サービスに参加するレストランやバーに専用カメラが設置され、顔照合により利用者が識別され、自動的に「チェックイン」する。
- 利用者の「いいね」履歴に合わせた割引等のオファーがスマートフォンに送信される。

- 2016年現在、実サービス開始には至っていない模様。

【ご参考】 顔認識を避ける方法

- cvdazzle.comというサイトでは、監視カメラでの顔認識を避けるためにカモフラージュする方法(メイクアップ方法)が掲載されている。



【ご参考】 英国の状況

- 2015年にITサービス企業Computer Services Corporation (CSC)が英国で150の小売店および約2000人の消費者に対して行った調査では、英国の小売店の27%が顔認識を使用していると推定されている。
- 衣料品店は特に積極的であり、59%が何らかの形態の顔認識を使っているという。
- 消費者の56%は顔認識技術が何なのか知らないと回答。33%が顔認識技術について知っているが、プライバシー侵害的であると回答。
- 消費者の71%は、自分の性別・年齢層・店内での滞留時間といった情報を記録する技術に対して居心地が悪い、又はあまり居心地が良くないと回答。
- CSCによれば、伝統的な小売業者はオンラインショッピング企業への対抗手段として、顔認識技術を用いた顧客行動の分析を行おうとしている。オンラインでは周知の通り、ショッピングサイト内で利用者の閲覧行動や購買行動は追跡されている。

※欧州では、いくつもの高級ホテルや高級小売店が、来店時にVIPやセレブを識別して望ましい対応を行うために顔認識を使用しているという。

※欧州の或る大きなショッピングセンターでは1日に15000人の来店客をスキャンし、既知の顧客にはターゲット化された広告を送ることができるという。(GAO報告書より)

米国において顔認識技術の商用利用が進まない理由 (1/2)

- 全米小売店協会NRF(利用企業の観点)
 - 米国の小売店もマーケティング・顧客サービス目的での顔認識技術の利用を模索しているが、顧客の反応への懸念があるために、外国に比べると動きが鈍い。
 - 大手百貨店Nordstromは、店舗内での顧客の動線をスマートフォンを通じて追跡すると掲示したところ、顧客からネガティブな反応を受けた。
 - 企業のライアビリティや訴訟されるリスクが課題となっており、これによって皆が尻込みしている。
 - 米国でもメディアからの批判的記事が契機となって一般人の批判が高まるという「炎上現象」がよくある。企業はブランドを傷つけない、プライバシーを守りたいので導入に消極的になる。
 - 顔認識技術に価値はあるが、まだ社会的な下地ができていない。
 - 米国では恐れより利便性が勝った時に、市民が受容する。現状は恐れが強いのかというと、まだそこまでも行っていない。顔認識技術が十分に認知されていないので、一般市民の意見が形成されていない。現時点では、小売店 vs 消費者団体の構図にしかならない。それほど使われていないので、一般市民の反対運動も起こっていない。
 - ジェネレーションギャップもある。2000年世代(18歳～34歳)はプライバシーを気にしていない。それに対し、年配層はプライバシーを守りたい。

米国において顔認識技術の商用利用が進まない理由 (2/2)

- IBIAおよび会員企業(ベンダー企業の観点)
 - セキュリティ目的・不正防止目的で顔認識を使用する場合、それを公表すると万引き犯が回避するので公表しないという小売店もある。
- FTC(監督機関)
 - 顔認識技術の正確性や、導入コストの問題かもしれない。普及啓発が足りないからかもしれない。
 - SNS企業(Facebook等)が写真タグ付け機能に関して州レベルで訴訟されるという事件もあった。これらも背景にあるかもしれない。
 - 技術は開発されているが、市場の受け入れの準備が整っていないのではないか。顔認識サービスに対して、怖いと思われていることもある。
- その他の機関
 - American Bankers Associationによると、ある主要な銀行では顔認識技術を強盗容疑者の識別のために使っているが、他の2つの主要な銀行は正確性に懸念があるため金融機関では広範には使われてないという。

顔認識技術の商用利用に対するプライバシー懸念 (1/2)

- 公共空間での匿名性の喪失

- 顔認識技術は急速に正確性の面において改善を続けている。また、個人はSNSその他のインターネットサイトに何十億もの写真をアップロードし続けており、顔画像(しばしば氏名その他の個人情報とリンクされている)の巨大なレポジトリが構築されている。これら2つのトレンドを結び付けることにより、いつか、公共空間の広範な範囲でほとんど全ての個人を識別することが技術的に可能になるかもしれない。(GAO報告書)
- 路上で出会った人の写真をスマートフォンや眼鏡型ウェアラブル端末等で撮影し、オンライン上の「顔照合サービス」で個人の身元を特定したり、住所情報を得たりする。照合には、例えばSNSにアップロードされている写真とプロフィール情報を用いるサービスが実現すると、路上・駅・店舗といった公共空間での匿名性が脅かされうる。(FTC報告書)
- 商業施設で遠隔で識別されることがより一般的になると、個人によっては商業施設を訪れたり、ショッピングしたりすることを不快に感じるかもしれない。また、個人が誰かを識別するのみならず、誰と一緒にいるかも分かってしまう。(GAO報告書)

- 現実世界(オフライン世界)での個人の追跡

- 現時点では、商業施設では顔認識は消費者を広範囲で追跡するためには使われていないが、将来的に顔認識技術が広範囲に使われるようになり、企業が互いに顔認識データを共有するようになれば、カメラのネットワークが様々な場所での消費者の動きを容易に追跡できるようになる。(GAO報告書)
- SNSにおける顔認識の利用に比べ、多くの消費者やプライバシー擁護者は物理的世界における顔認識や生体認証プロファイリングの利用の方が問題があると考える。クッキーやブラウザのキャッシュは削除することができ、SNSや携帯電話の設定は変えることができる。しかし、公道を歩いているときやショッピングモールを歩いているときのプライバシー設定は存在しない。自分の顔データを削除することもできない。(The Guardian記事)

顔認識技術の商用利用に対するプライバシー懸念 (2/2)

- カメラが個人を識別し、自動的に行動を追跡し、笑顔や怒りと言った表情を検出する。常連客が駐車場にきたことを認識し、好みの駐車スペースに誘導する。顧客がショッピングモールに入場すると服装を識別し、各店舗のオファーや過去の購買履歴等に基づいて店舗をサジェストする。店舗のウィンドウにはカスタマイズされた広告が表示されたり、店舗へのアクセスが自動的に拒絶されたりする。顧客に合ったレストランもサジェストされる。[映画「マイノリティ・リポート \(2002年\)」的な世界の出現](#)。(EU指令第29条作業部会WP193)
- 個人が気付かない場面で顔認識技術が利用されること
 - 他の生体認証技術と異なり、[顔認識技術は遠隔かつ本人の認識がなくても顔画像を取得しうる](#)。また、消費者が通知を受け、オプトアウトの選択肢を与えられていたとしても、街中の様々な施設や場所で顔認識技術の利用が増加するにつれて、その選択肢の行使は難しくなりうる。(GAO報告書)
- 誤照合
 - ある人の顔画像が誤照合され、例えば[万引き犯と誤って識別された場合、個人にとって不利な情報が長期的に様々な商業システムに伝播する](#)恐れがある。(GAO報告書)
- 差別待遇
 - 顔認識システムから得られた情報に基づいて、[特定グループの消費者に差別的な取扱いがなされる恐れがある](#)。ある消費者団体は、性別や人種、年代といった分類の目的で顔認識技術が利用されることに懸念を表明。それらの属性データはプロファイリング(ある個人の傾向について推定するために、個人の属性や行動パターンを利用すること)につながり、例えば特定グループの消費者への価格差別につながる恐れがある。(GAO報告書)
 - [小売店からの顔認識の要求に同意しない個人が、特定製品やサービスへのアクセスを拒否される](#)可能性がある。(GAO報告書)

1. 顔認識技術の商用利用の状況

2. 顔認識技術の商用利用に関する法令・ ルールの検討状況

米国のプライバシー・フレームワーク

- 従来のフレームワーク

- 行政分野は1974年プライバシー法、及び2002年電子政府法により規制。
- 民間分野は、HIPAA(医療保険)、電子通信プライバシー法、金融サービス近代化法、FCRA(公正信用報告法)、児童オンラインプライバシー保護法などの個別法により個別分野を規制するセクトラル方式。
- 個別法により規制されない、大多数の民間企業に対しては、自主規制を推奨。企業のプライバシーポリシーに虚偽の記載があれば、FTC法の第5条(不公正な競争方法及び不公正・欺瞞的な行為又は慣行の禁止)によってFTCが法執行を行う。

- FTC(連邦取引委員会)による法執行の例

Googleに対する法執行 (2012年8月)	GoogleとFTCは、閲覧履歴収集に関するグーグルの虚偽説明および前回の同意内容への違反を理由として、制裁金2,250万ドルをFTCに支払うということで同意。
Facebookに対する法執行 (2011年11月)	同社のプライバシーポリシーに違反して個人データを第三者に提供していたとして、同社に対して包括的なプライバシープログラムの導入と、外部監査人による20年間に渡る評価を命令。
Googleに対する法執行 (2011年10月)	Google Buzzのサービスが同社のプライバシーポリシーに違反していたとして、同社に対して包括的なプライバシープログラムの導入と、外部監査人による20年間に渡る評価を命令。

米国のプライバシー・フレームワーク

• 近年の動向

① ホワイトハウス「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」

- [2012年2月](#)公表。通称ホワイトペーパー。
- 商務省のドラフト報告書(グリーンペーパー: 2010年12月)がベース。
- [「消費者プライバシー権利章典」7原則](#)を含む。
 - 内容的には米国のFIPPs(公正な情報取扱い8原則。OECDの8原則とほぼ同じ)を現代風にアレンジしたもの。
 - [民間分野に対する「原則」を規定しているが、細かい「ルール」までは規定していない。](#)
 - [原則\(権利章典\)については立法勧告](#)を行っている。
 - [ルールについては各関係者で集まって業界ごとの行動規範](#)を作り(マルチ・ステークホルダー・プロセス)、自主規制を行う。

※EUデータ保護規則(GDPR)とは「原則」は共通する部分も多いが、[「ルール」が法規制なのか、自主規制なのかの面で異なる](#)。ただし、ルールに対する「法執行」は、米国の方が厳しいとも言われている。

② FTC「急速に変化する時代における消費者プライバシーの保護」

- [2012年3月](#)公表。FTCのドラフト報告書(2010年12月)がベース。
- [民間分野に要求するルール\(自主規制\)の一般的内容を規定](#)している。

ホワイトハウス「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」

・ 報告書の構成

エグゼクティブ・サマリー

I. 序論

II. 消費者プライバシー権利章典

III. マルチステークホルダー・プロセスによる行動規範の開発

IV. FTCによる法執行の強化

V. 国際的な相互運用性の促進

VI. 消費者プライバシー法令の立法化

VII. 連邦政府のリーダーシップ

VIII. 結論

・技術やビジネスモデルの発展によって生じたプライバシー問題に対処し、消費者の信頼を向上させるために、「消費者プライバシー権利章典」を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。

・7つの原則で構成。

- ・特定の産業分野ごとに、権利章典に準拠した行動規範を開発。
- ・商務省のNTIAが旗振り役となる。
- ・ある行動規範を採用(遵守)するか否かは、企業の自由裁量。

・「消費者プライバシー権利章典」が立法化されなかった場合：
→「行動規範を遵守する」という企業のコミットメントに違反があれば、FTC法の第5条によって法執行を行う。

・「消費者プライバシー権利章典」が立法化された場合：
→上記に加え、FTC(及び州の司法長官)には、消費者プライバシー権利章典を直接的に執行する権限が与えられる。ただし、行動規範を遵守する企業には「執行セーフハーバー」として、消費者プライバシー権利章典の直接的執行が免除される。

FTC「急速に変化する時代における消費者プライバシーの保護」

- 民間分野のプライバシー・フレームワークとして、(a)の条件に該当する企業に対して、(b)のベストプラクティスを実施することを要求。

- (a)対象となる企業

- 特定の消費者、コンピュータ、又はその他の端末に無理なくリンク可能なデータ(reasonably linkable data)を収集したり利用したりする全ての企業等(commercial entities)に適用される。
- ただし、当該企業が年間5000人未満の消費者からの非センシティブなデータしか収集しておらず、かつそれらのデータを第三者と共有していない場合は除く。
- 「保護対象となる個人データ」=「個人等に無理なくリンク可能なデータ(reasonably linkable data)」

企業が次の3つの条件を満たせば、「無理なくリンク可能なデータ」ではない。

- (1) データが非識別化されたことを保証する合理的な措置を取っている。
- (2) 当該データを再識別化しようとしないうちに公的にコミットメントしている。
- (3) データ受領者が当該データを再識別化しようとすることを契約で禁止している。

- (b)要求されるベストプラクティス

- ① プライバシー・バイ・デザイン
 - ② 選択の簡略化(コンテキストの尊重)
 - ③ 透明性の向上
- A. 一般に受容された取扱い(コンテキストと整合的な取扱い)に対しては、消費者に事前に選択を提供する必要はない。
— B. それ以外の取扱いに対しては、消費者に選択を提供すべき。

【ご参考】FTCが民間企業に要求するベストプラクティス

①プライバシー・バイ・デザイン

- 企業は、自社組織全体を通じて、また製品やサービスの開発のあらゆる段階で、消費者プライバシーを促進すべきである。
- 企業は、自社のプラクティスに、データセキュリティ、合理的な収集制限、妥当な保持・廃棄、データの正確性といった実質的なプライバシー保護を組み込むべきである。

②選択の簡略化

- A.選択を必要としないプラクティス(一般に受容されたプラクティス)

企業は、当該取引のコンテキストや消費者との関係と整合的な、若しくは法令によって要求されたり特別に許可されているプラクティスにおいて消費者のデータを収集したり利用したりする場合は、消費者に事前に選択を提供する必要はない。

(1)製品やサービスの遂行 (2)内部オペレーション (3)詐欺の防止 (4)法令順守と公共目的 (5)ファーストパーティ・マーケティング

- B.その他のプラクティスに対しては、企業は消費者に選択を提供すべきである

選択を必要とするプラクティスのために、企業は、消費者が自分のデータに関して決定を行う時点及びコンテキストで選択を与えるべきである。企業は、(1)データが収集された時点とは実質的に異なる仕方で消費者データを利用する場合、または(2)ある目的でセンシティブデータを収集する場合には、事前に肯定的で明示の同意を得なければならない。

③透明性の向上

- A.プライバシー通知

プライバシー通知は、プライバシー・プラクティスをよく理解したり比較したりできるように、より明確で、より短く、より標準化されたものであるべきである。

- B.アクセス

企業は自社が保持する消費者データへの無理のない(reasonable)アクセスを提供すべきである。アクセスの範囲は、データのセンシティブ度やその利用の性質に釣り合ったものであるべきである。

- C.消費者の教育

全てのステークホルダーは、商業的なプライバシー・プラクティスに関わる消費者を教育する努力を拡大するべき。

【ご参考】FTCによる実施勧告

- FTCはまた、同報告書で下記2点の実施を勧告

① 立法勧告

FTCは、議会にベースラインとなるプライバシー立法を検討するように要求しており、またデータセキュリティとデータブローカーに関する立法を再度要求。

② 5つの重点領域

FTCは2013年にかけて、下記5つの領域での自主規制の取組みを促進。

1. 「Do Not Track」

- 行動ターゲティング広告ネットワークに対して、自分のオンライン行動のトラッキングを拒否できるメカニズム。
- これまで、複数のブラウザベンダーが、オンライン行動を追跡しないようにウェブサイト要求できるブラウザベースのツールを開発。
- また、W3CがDo Not Trackのための共通のウェブプロトコルを開発中。
- DAA(デジタル広告アライアンス)が、消費者がアイコンのクリックを通じてアクセスでき、行動ターゲティング広告に関する情報を得たりそこからオプトアウトするためのツールを開発した。さらに、DAAはクレジットや雇用のような二次的な目的で消費者のデータを利用することを防止することや、追跡に関してブラウザ上での設定を通じて消費者が行った選択を守ることにコミットした。

2. モバイル

3. データブローカー

4. 巨大プラットフォーム・プロバイダー(ISP、OS、ブラウザ、ソーシャルメディア等)

5. 執行可能な自主規制行動規範の促進:

商務省(NTIA)のMSHPを通じた特定産業分野ごとの行動規範の開発にFTCも参画。

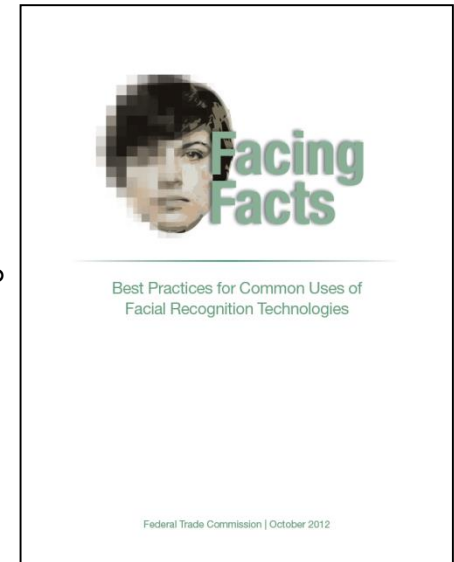
【ご参考】 消費者プライバシー権利章典法案ドラフト

- 消費者プライバシー権利章典法案ドラフト (Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015)
 - 2015年2月27日にホワイトハウスが公表
 - 個人データの定義で以下を例示
 - A.氏名
 - B.住所、メールアドレス
 - C.電話番号、FAX番号
 - D.社会保障番号、納税番号、パスポート番号、免許証番号等の政府発行ユニーク識別番号
 - E.指紋、声紋等の生体識別子
 - F.以下を含むユニークな継続的識別子
 - ネットワーク端末をユニークに識別する番号
 - 商業発行の識別番号、サービスアカウント番号(金融口座番号、クレジットカード番号、デビットカード番号、ヘルスケアアカウント番号、小売アカウント番号等)
 - ユニークな自動車識別子(自動車識別番号、ナンバープレート番号等)
 - 個人のサービスアカウントへのアクセスに必要な情報(セキュリティコード、アクセスコード、パスワード等)
 - G.個人のコンピュータや通信端末のユニークな識別子またはそれに関する情報
 - H.その他、個人データの定義に該当するデータ
 - ただし、以下は個人データから除外する
 - 「De-identified data(FTC 3条件に相当)」「削除データ」「従業員情報」「サイバーセキュリティデータ」
 - 対象組織から以下は除く
 - 「連邦・州政府機関」「商業能力を持たない自然人」「いずれの12か月の期間も、1万未満の個人や端末のデータしか取扱わない者、または従業員が5名以下の者」等

FTCの顔認識技術の商用利用に関するレポート

- FTCレポート “Facing Facts”

- FTC(連邦取引委員会)では[2012年10月](#)にスタッフレポート “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies”を発行。
- 2012年3月のFTCレポートの3原則を顔認識サービスに適用。
すなわち、[顔認識技術を商用目的で用いる企業に対して、以下の3つの原則に基づくサービス設計を行うように勧告](#)。
 - (1) プライバシー・バイ・デザイン
 - (2) 選択の簡略化
 - (3) 透明性の向上
- 2011年12月のFTC主催「Face Factsワークショップ」やそれに続くパブリックコメントでの検討結果をまとめたもの。
- FTCが本レポートで勧告するベストプラクティスは既存の法的要求事項を越えているかもしれないが、越えている範囲についてFTCが現行法の下で法執行を行うことは意図していない。
- また、本レポートは顔認証技術の商用利用のみを対象とし、セキュリティ目的での利用や法執行機関・政府機関による利用については対象外。
- FTCコミッショナー5名のうち1名が本レポートに異議を表明している。



FTCの顔認識技術の商用利用に関するレポート

- FTCレポート“Facing Facts”（続き）
 - 顔認識技術は、遠距離からでも消費者を検知でき、消費者に気付かれることなく消費者の映像を収集し、処理することが可能である。
 - 顔認識技術の将来利用とプライバシー懸念
 - 路上やショップのような公共スペースにおいて匿名の個人を特定(identity)したり、オンライン上の匿名の写真を識別(特定)したりすることに顔認識技術が使用される可能性が最大のプライバシー懸念。
 - カネギー・メロン大学の2011年の研究では、デートサイト上の匿名の写真が、顔認識技術によりFacebook上のプロフィール付き写真と照合され、個人が特定された。
 - 顔認識技術を使用する企業の責務
 - 顔は消費者のユニークな識別子であり、置き換えることができないため、当人に密接に連結(link)しており、プライバシー保護措置が必要。
 - 顔認識技術を使用する企業は、顔検出や属性推定、顔照合などいかなる目的で使用するにせよ、消費者との関係のコンテキストにおいて適切なプライバシー保護を実施すべき。
 - この結論は、2012年3月のFTCレポートにおける、「企業は特定の消費者やコンピュータその他の端末に無理なく(reasonably)連結可能ないかなるデータに対してもプライバシー保護を実施すべき」という立場と整合的である。

FTCの顔認識技術の商用利用に関するレポート

- FTCレポート“Facing Facts”（続き）
 - FTCは顔認識技術を用いる企業に対して、以下の3つを勧告
 - (1) プライバシー・バイ・デザイン
 - 合理的な安全管理措置を取ること。 – 適切なデータ保持・廃棄のプラクティスを行うこと。
 - 顔認識製品やサービスを実装する際の情報のセンシティビティ(ex.設置場所)に配慮すること。
 - (2) 選択の簡略化／(3) 透明性の向上
 - 例えば、カメラ機能付きの電子看板(デジタルサイネージ)は、通常の電子看板と外見上は区別しにくいので、生体技術の使用に当たっては、その旨を消費者に明確に告知(notice)し、嫌な消費者はその看板を避けられるようにすべき。
 - また、顔認識機能を使用するSNSは、消費者に自分の顔特徴データは収集しないことや顔認識機能で利用しないことを選択を与えたり、当該機能をいつでもOFFにしたり既に収集された自分の顔特徴データを削除できるようにすべき。
 - さらに、以下の場合には、消費者から事前に明示的な同意を取得すべき。
 - データ収集時に消費者に示した利用方法と異なる方法で顔画像や顔特徴データを利用する場合(目的外利用)。
 - 匿名の映像から消費者を特定するために顔認識技術を使用する場合(一種の目的外利用)。
- 幾つかの業界団体(電子看板業界等)は既に行動規範等を発行
 - POPAI(Point of Purchase Advertising International's Digital Signage Group)の行動規範(2010年8月)
 - Digital Signage Federationの自主的なプライバシーガイドライン(2011年2月)
 - これらの自主規制プログラムに参加した企業が違反した場合には、FTCはFTC法第5条により法執行可能

顔認識技術に適用されうる法律

○ 連邦法

- FTC法第5条(不公正な競争方法及び不公正・欺瞞的な行為または慣行の禁止)

- 欺瞞的な行為または慣行(deceptive act / practice):

企業のプライバシーポリシーに虚偽の記載があれば、FTCはFTC法第5条に基づき、当該企業を訴追できる。

- Ex. 顔認識技術を使っていないと表明しながら、実際には使っていた場合
- Ex. 顔認識技術で取得したデータを第三者提供しないと表明しながら、実際には提供していた場合

- 不公正な行為または慣行(unfairness act / practice):

企業のプライバシーポリシーに記載がない場合であっても、企業が消費者に実質的な損害を引き起こした場合には、FTC法第5条が適用されうる。

- ビデオ隠し撮り防止法(Video Voyeurism Prevention Act of 2004):

- 個人の「私的領域」の写真を、本人の同意なく、意図的に撮影することを犯罪とする。
- 私的領域の定義には個人の顔は含まれないが、小売店の試着室・トイレなど、商用空間の一定箇所でのカメラ設置を規制しうる。

顔認識技術に適用されうる法律

○ 州法

- テキサス州とイリノイ州は、顔認識技術で取得された顔特徴データを含む生体認証識別子の商用利用に明示的に対処したプライバシー法を制定している。
 - テキサス州下院の委員会報告書では、生体認証データが徐々にアイデンティティ窃盗のターゲットとなっており、安全保護の必要があるという。
 - イリノイ州の州議会は、生体認証技術の利用はビジネス分野（決済など）やセキュリティ検査分野で拡大しており、この技術の影響は十分に認知されていないという。
- テキサス州とイリノイ州の法律は両者とも、以下の内容を含む。
 - 個人の生体認証識別子の取得に先立ち、民間企業・民間団体は本人の同意を得なければならない。
 - 生体認証識別子を保有する企業・団体が、それらを第三者に提供することを禁じる。ただし、法執行機関への提供や、本人が請求または承認した金融取引を遂行するための提供の場合は除く。
 - 生体認証データの保持に関する規定を含む。生体認証データの保護に関する要件や、一定期間後の生体認証データの破壊など。
- その他、コネティカット州でも法案を審議中。

※イリノイ州のBiometric Information Privacy Actは2008年に通過した。Facebookのロビー活動を受けて、Terry Link州上院議員により2016年5月26日に修正法案が提出された。同修正法案は、ソーシャルメディアで使われている写真タギング技術を同法の適用から除外するというもの。しかし、消費者団体の反対により同法案は撤回されたとのこと。

基本的な個人情報保護法の立法化の見通し

- 民間分野を包括的に規制する基本的な個人情報保護法
 - 現状、連邦レベルでは存在しない。
 - 2012年2月のホワイトハウス報告書で立法勧告がなされ、2015年2月にはホワイトハウスが消費者プライバシー権利章典法案ドラフトを公表したが、議員からの法案提出はなされていない。
- 今後の見通し
 - 現状では[大統領と連邦議会の仲が悪い](#)ため、よほど重要な法案でないと立法化されない。(NTIA)
 - 包括的なプライバシー法は将来的にもできないと考える。なぜなら、米国における法律の基本的な構造はセクション別のアプローチである。[米国では法律は危機モードにならないと制定されない](#)。例えば、1980年代に最高裁判事候補のビデオレンタル記録をマスコミがごみ箱から見つけて暴露した事件があった。これを契機にビデオプライバシー保護法が制定された。(GAO)
 - FTCとしては包括的なプライバシー立法の支援はしているが、近い将来にできる見通しはないと考えている。(FTC)
 - 米国でうまく行っていないのは政治的な理由であり、すなわち共和党と民主党が拮抗しているので、なかなか進まない。(NRF)
 - 業界団体に比べ、消費者団体の声が法律になることが難しいのは、業界側のリソース・予算・人が多いため。製造物責任法など、危機がないと法律ができない。[プライバシーメルトダウンがないと、法律はできないのではないか](#)。ただ、業界も一枚岩ではない。Microsoftは包括的なプライバシー法がむしろ業界のためになるとして、賛成している。(CFA)

顔認識技術の商用利用に関するマルチステークホルダープロセス

- マルチステークホルダー・プロセス (MSHP)
 - 2012年2月のホワイトハウス報告書(消費者プライバシー権利章典含む)において、特定の産業分野ごとにマルチステークホルダー・プロセスを通じて消費者プライバシー権利章典に準拠した行動規範を開発することを推奨。
 - 商務省のNTIA(電気通信情報庁)が旗振り役として指名された。
 - 当該分野で行動規範が開発されたとしても、その行動規範を採用(遵守)するか否かは、企業の自由裁量に委ねられている。
 - 行動規範を採用した企業は、違反時にはFTC法第5条により執行されうる。
 - オバマ政権のいう「消費者プライバシー権利章典」が立法化された場合には、MSHPで策定された行動規範を遵守する企業には「執行セーフハーバー」として、「消費者プライバシー権利章典法」の直接的執行が免除されるというメリットが考えられていた。
 - 第一弾はモバイルアプリの透明性(2012年7月開始。2013年7月に行動規範を策定)。
 - 上記「消費者プライバシー権利章典」の立法化の見込みがないため、このモバイルアプリの行動規範を採用した企業は多くないという。

顔認識技術の商用利用に関するマルチステークホルダープロセス

• 顔認識技術に関するマルチステークホルダー・プロセス

- 第二弾として2014年2月から開始。誰でも参加できるオープンミーティングであり、連邦政府広報に掲載。Webキャストも実施。
- 消費者プライバシー権利章典に準拠した顔認識技術の商用利用に関する行動規範の開発が目的であった。
- 全15回の開催を経て、2016年6月14日に完了。その1年前の2015年6月16日には消費者団体9団体が共同声明を発表し、MSHPから脱退。
- 消費者団体が脱退した直後に業界側関係者のみで1回開催したが(2015年7月)、次の回の開催までは時間を空けた(2016年3月)。
 - 2つの理由があり、1つは消費者団体が戻ってくるための時間的猶予を与えなかったことであり、もう1つは業界にドキュメントを用意させるためである。
- 結局、消費者団体は戻ってこなかったが、2016年3月に再開し、同年6月14日に業界側関係者のみで合意。当初目的は行動規範の策定であったが、業界側の意思により、ベストプラクティスを策定した。

※「行動規範」と「ベストプラクティス」の違い

- 行動規範: 企業が採用(ポリシーで公表)すると、FTC法第5条で法執行可能になる。
- ベストプラクティス: 啓発や情報提供が目的。企業が目標とするレベルを明示化する。ベストプラクティスをポリシーで公表する企業はないので、FTCによる法執行が及ばない。

顔認識技術の商用利用に関するマルチステークホルダープロセス

- 参加者(発表者)は以下の団体等。
 - 政府機関
 - 商務省のNTIA(電気通信情報庁)(主催者)
 - Federal Trade Commission(FTC)
 - 外国の政府機関
 - カナダ・オンタリオ州情報プライバシーコミッショナー事務所
 - フランスCNIL
 - 企業
 - Paycasso
 - Animetrics
 - Motorola
 - FaceFirst
 - Kairos
 - Microsoft
 - A Novetta Solutions Company
 - 業界団体
 - Online Trust Alliance
 - Identity Counsel International
 - Interactive Advertising Bureau
 - International Biometrics & Identification Association(IBIA)
 - Marketing Research Association
 - NetChoice
 - Internet Association
 - 消費者団体
 - Center for Democracy & Technology
 - Consumer Federation of America(CFA)
 - ACT
 - American Civil Liberties Union(ACLU)
 - Center for Digital Democracy
 - TechFreedom 等
 - 大学
 - Carnegie Mellon University
 - UCLA
 - Rutgers Business School

顔認識技術の商用利用に関するマルチステークホルダープロセス

- 2015年6月16日に[Consumer Federation of America](#)は他のプライバシー保護団体と[共同声明](#)を発表し、[顔認識技術の商用利用に関するマルチステークホルダープロセスから脱退する](#)と宣言した。
- 共同声明によると、「我々は、NTIAのプロセスが、顔認識技術の利用に対して十分な保護を与えるようなプライバシールールを生み出しそうだとは思わない。我々は、多くのコンテキストにおいて、[消費者の顔認識は個人が肯定的にそれを許可している場合のみ実施すべき](#)だと確信している。しかし直近のNTIA会合（MSHP会合）では、[産業界の関係者は、消費者の許可に基づく場合のみ顔認識を用いるべきとするいかなる具体的なシナリオにも合意しなかった](#)。（・・・）我々は、この脱退が、消費者のプライバシーを保護する効果的な交通規則を開発する手段として、マルチステークホルダープロセスの有効性を再評価する必要性のシグナルとなることを望む」とのことである。
- また、Consumer Federation of Americaの消費者保護・プライバシー担当理事であるSusan Grant氏は、「（マルチステークホルダープロセスは）本質的に欠陥のあるプロセスである。なぜなら、企業の現行または将来のビジネスの制約となるかもしれないいかなる決まり事にも、企業が合意するインセンティブはないからである」と述べている。
- NTIAは2015年6月15日に、[これらプライバシー保護団体（消費者団体）抜きで、マルチステークホルダープロセスを継続する](#)と述べた。実際に2015年7月28日には、プライバシー保護団体抜きで第13回会合が行われ、[以下の2つの団体から提出された行動規範案が検討](#)された。
 - (1) NetChoice（eコマースの業界団体）
 - (2) International Biometrics Industry Association（バイオメトリクス産業の業界団体）

【ご参考】 業界団体によるルール案

(1) NetChoiceの指針案 (Stakeholder Draft of Guidelines for the Collection and Use of Facial Recognition)

- 透明性
 - 顔認識技術を使用する組織は、顔認識データ(顔特徴データを含む)の収集と利用に関する当該組織のポリシーを、本人に利用可能とするべきである。
 - 顔認識技術の使用に関する通知は、顔認識技術が用いられる時点かそれ以前に与えられるべきである。あるいは、組織が本人に顔認識データの利用をコントロールするための適切な選択を提供している場合には、顔認識技術が用いられた後に通知が与えられてもよい。
- コントロール
 - 顔認識技術を使用する組織は、顔認識データを第三者に提供する場合には、有効なコントロール手段を本人に与えるべきである。
 - 顔認識データをアクセス拒否 (barrier to access) に用いる場合には、当該措置に異議申し立てする機会を本人に与えるべきである。
- 顔認識データの提供
 - 以下の場合に顔認識データを提供する場合には、本ガイドラインの制限は適用されない。
 - 本人の同意がある場合
 - 人の死や身体的危害を避けるために必要な場合
 - 令状 (warrant) や召喚状 (subpoena) など、法的要求に従うために必要な場合
 - 防犯目的のみで利用される場合
- 利用の制限
 - 顔認識技術や顔検出技術、顔認識データを非合法・違法な取扱いのために利用してはならない。
- 適用範囲
 - 本ガイドラインは、媒体に関わらず、あらゆる顔認識技術の使用に適用される。ただし、「利用の制限」を除き、本ガイドラインは顔検出(※顔特徴データの作成を伴わない、顔検出および属性推定を指す)技術の使用には適用されない。

【ご参考】 業界団体によるルール案

(2) International Biometrics Industry Associationのベストプラクティス案 (Discussion Draft Privacy Best Practice Recommendations For Commercial Biometric Use)

- 透明性
 - 透明性には2つの要素が含まれる。
 - (i) プライバシーポリシーの存在と、それが利用可能であること。
 - (ii) 顔認識技術が用いられることの通知。
 - バイオメトリック技術が特定個人の識別には用いられない場合、例えば人間の検出・カウントや属性推定に用いられる場合には、コンテキストに合致した一般的な通知を行うべきである。
 - 他方、顔照合のために顔認識システムが用いられる場合は、以下の項目を考慮に入れ、個別の通知を行うべきである。
 - 自発的な登録であるか、強制的な登録であるか
 - バイオメトリクスデータ以外にどのような個人データが取得され、保存されるか
 - どのようにデータが保存され、利用されるか
 - こうしたプロセスが、登録される個人にどのようなリスクや損害をもたらしまうるか
 - 当該データ利用は消費者の合理的な期待に適合しているか
- その他、OECDプライバシーガイドライン8原則に基づき、以下の原則が挙げられている。

– 収集制限の原則	– 目的明確化の原則
– 公開の原則	– 利用制限の原則
– 安全保護措置の原則	– データ内容の原則
– 責任の原則	– 問題解決と救済措置 (個人参加の原則に対応)

MSHPで策定されたベストプラクティス(原文)

Privacy Best Practice Recommendations For Commercial Facial Recognition Use

- These “Privacy Best Practice Recommendations for Commercial Facial Recognition Use” serve as general guidelines for covered entities. The fundamental principles underlying the recommendations are based on the Fair Information Practice Principles (FIPPs) .
- [It is left to implementers and operators to determine the most appropriate way to implement each of these privacy guidelines.](#)
- Given the numerous existing uses in widely different applications (such as authentication, social media and physical access control), as well as potential uses, specific /detailed practices are not feasible or practical across this wide spectrum.
- [These best practices are intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies.](#)
- This document is intended to provide a general roadmap to enable entities using facial recognition technologies by recognizing differing objectives, risks and individual expectations associated with various applications of these technologies.
- [These principles do not apply to the use of a facial recognition for the purpose of aggregate or non-identifying analysis.](#) For example, [when facial recognition technology is used only to count the number of unique visitors to a retail establishment or to measure the genders or approximate ages of people who view a store display \(for marketing research purposes\), those practices are outside the scope of these principles.](#)
- [These best practices do not apply to security applications, law enforcement, national security, intelligence or military uses,](#) all of which are beyond the scope of this document.

MSHPで策定されたベストプラクティス(原文)

○ Definitions

- Covered Entity – Any person, including corporate affiliates, that collects, stores, or processes [facial template data](#). Covered entities do not include governments, law enforcement agencies, national security agencies, or intelligence agencies.
- Unaffiliated Third Party – Any person other than (1) a user of a covered entity's products or services; (2) a covered entity's employees; (3) an entity under common control or ownership with a covered entity; or (4) a vendor or supplier to a covered entity when such vendor or supplier is used to provide a product or service related to facial template data.
- Facial Template Data – A unique facial attribute or measurement generated by automatic measurements of an individual's facial characteristics, which are used by a covered entity to uniquely identify an individual's identity or authenticate an individual when the individual accesses a system or account. Data that has been reasonably de-identified and the underlying document from which the data came is not facial template data and therefore is not covered by these best practices.
- Facial Recognition Technology – A computer program used to compare the visible physical structure of an individual's face with a stored facial template to confirm an individual's claimed identity or to uniquely identify an individual.
- Security Applications - Loss prevention and other applications intended to detect or prevent shoplifting, fraud, misappropriations or other malicious and criminal activities.

○ Transparency

- [Covered entities are encouraged to make available to consumers, in a reasonable manner and location, policies or disclosures describing such entities' practices regarding collection, storage, and use of facial template data](#). Covered entities are encouraged to update their policies or disclosures when they make material changes to their facial template data management practices. Generally, policies or disclosures should describe, if applicable, and/or in the appropriate context:

MSHPで策定されたベストプラクティス(原文)

- the reasonably foreseeable purposes, or examples, for which the covered entity collects and shares facial template data or uses facial recognition technologies;
- the covered entity’s data retention and de-identification practices;
- and, if the covered entity offers the ability to review, correct, or delete facial template data, the process to accomplish such actions.
- Where facial recognition technology is used on a physical premises that a covered entity controls, such entity is encouraged to provide concise notice to consumers that facial recognition technology is present, and, if contextually appropriate, where consumers can find more information about the covered entity’s use of facial recognition technology.

○ Developing Good Data Management Practices

- When covered entities formulate their facial template data management practices, and before covered entities deploy facial recognition technology, they are encouraged to consider the following factors:
 - Voluntary or involuntary enrollment;
 - Type of non-facial recognition sensitive data being captured and stored;
 - How that data will be stored and used;
 - Whether facial template data may be used to determine a person’s eligibility for, or access to, employment, healthcare, financial products or services, credit, housing, or insurance;
 - Risks and harms, if any, this process may impose on the enrollee;
 - Reasonable consumer expectations with regard to the use of the data.

MSHPで策定されたベストプラクティス(原文)

○ Use Limitation

- Covered entities that use facial recognition technologies to determine an individual's identity are encouraged to provide the individual the opportunity to control the sharing of their facial template data with an unaffiliated third party that does not already have this information.

○ Security Safeguards

- Covered entities should take measures to protect covered data by implementing a program that contains reasonable administrative, technical, and physical safeguards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the facial template data." Covered entities are encouraged to take reasonable steps to periodically assess their facial template data protection measures consistent with the sensitivity of the use of the data.
- When appropriate, covered entities are encouraged to consider whether these measures should include limiting the individuals or applications that may access facial template data.

○ Data Quality

- Covered entities are encouraged to take reasonable steps to maintain the integrity of the facial template data they collect.

○ Problem Resolution and Redress

- Covered entities are encouraged to provide a process consumers can follow to contact the entity regarding its use of facial template data.

各ステークホルダーが考える望ましいルールの内容(1/3)

	業界団体	消費者団体	監督機関(FTC)
ルール／ ルール案 の名称	“Privacy Best Practice Recommendations For Commercial Facial Recognition Use” (NTIAのMSHPの成果物)(2016年6月) https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recognition.pdf	“An Ethical Framework for Facial Recognition” (NTIAのMSHPへの消費者団体ACLU提出資料)(2015年6月) https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf	“Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies” (FTCのスタッフレポート)(2012年10月) https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialechprpt.pdf
ルールの 対象	顔特徴データの商用利用 (万引き防止等のセキュリティ目的での利用は除く。また、 属性推定や人数カウントのみの利用も除く)	顔認識技術の商用利用	顔認識技術の商用利用 (セキュリティ目的での利用は除く)
通知・公表 方法	(1)企業は、合理的な方法かつ場所で、消費者に対して以下の取扱いについて記載したポリシーまたは通知(notice)を入手できるようにすることが推奨される。 ・顔特徴データの収集 ・顔特徴データの保存 ・顔特徴データの利用 (2) 顔認識技術が物理的施設で使用されている場合は、企業は顔認識技術が使われていることについて簡潔な通知(notice)を消費者に提供することが推奨される。 またコンテキスト的に適切である場合には、消費者がどこで当該企業の顔認識技術の使用に関する 詳細情報 を得られるかについて消費者に提供することが推奨される。	(1)企業は、本文書に挙げる諸原則を遵守するために、以下の項目を含めてポリシーを記載しなければならない。 ・データの保持期間 ・データの利用方法 ・データへの政府機関のアクセス ・アカウントビリティを保証するために必要な技術仕様 (2)企業は、 顔認識が作動中である場合は、個人に対して目立つ形で通知(notice)しなければならない。	※顔認識機能付きの電子看板の場合 通常の電子看板と外見上は区別しにくいので、 顔認識技術の使用に当たっては、その旨を消費者に明確に通知(notice)し、嫌な消費者はその看板を避けられるようにすべきである。

各ステークホルダーが考える望ましいルールの内容(2/3)

	業界団体	消費者団体	監督機関(FTC)
<u>本人の事前同意</u>	【IBIAへのヒアリングより】 <u>消費者向けに適切に通知・公表を行っていれば、顔特徴データの取得・保存時の本人同意は不要。</u> 【NTIAへのヒアリングより】 ・事前同意は、小売店の中など、消費者が顔データを取られて顔認識に使われているとは思わないような場合は難しいので、企業側は賛成していない。 ・FacebookのようなSNSではオプトインが可能だが、店舗などでは難しい。不可能ではないが困難であるため、<u>事前同意を必要とすると、店舗で不特定多数の顧客の顔特徴データを取得して顔照合を行うことは事実上不可能</u>となる。 ・ただし、顔特徴データの利用について消費者も認知できるような場合(テーマパークでチケットを買う場合等)、店舗であっても事前同意は可能となる。	・<u>消費者の顔特徴データや顔写真をデータベースに保存する場合には、事前に書面での本人同意を得なければならない。</u> 【CFAへのヒアリングより】 例えば、VIP顧客が来店したことを知るために顔照合を行う場合、<u>ロイヤルティカードなどの申し込み時に同意を取ることができる</u>。顔照合を条件にはいけないが、顧客側で選択できるようにすればよい。あるいは店で顔照合を使います、こんなメリットがありますというチラシを配り、その店のWebサイトで自発的にサインアップして写真を登録する方法が考えられる。	以下の場合には、消費者から事前に明示的な同意を取得すべきである。 (1)データ収集時に消費者に示した利用方法と異なる方法で顔画像や顔特徴データを利用する場合(目的外利用)。 (2)匿名の顔画像から消費者を特定するために顔認識技術を使用する場合(一種の目的外利用)。
<u>訂正・消去する権利</u>	企業が個人に自分の顔特徴データを<u>閲覧・訂正・消去する権限を与えている場合には、ポリシーや告知(disclosure)において、その実施プロセスを記載すべき。</u>	個人は自分の顔特徴データにアクセスしたり、それを<u>訂正・消去したりする権利が与えられなければならない。</u>	(顔検出機能を用いた眼鏡店サイトや顔照合機能を用いたSNSサイトの事例では、自分の顔画像や顔特徴データを消去できるようにすべきとされている。)

各ステークホルダーが考える望ましいルールの内容(3/3)

	業界団体	消費者団体	監督機関(FTC)
プライバシー・バイ・デザイン	企業が顔特徴データの管理方法を策定する際には、また顔認識技術を実装する前には、<u>以下の要素を考慮することが推奨される</u>。 (1)顔特徴データの登録は任意か強制か (2)取得され保存されるセンシティブデータの種類(顔認識データ以外) (3)データの保存方法および利用方法 (4)顔特徴データは、雇用・医療・金融商品・金融サービス・クレジット・住宅・保険への個人の資格やアクセスを決定する際に利用されるか否か (5)登録された個人にもたらされるリスクや損害(もしあれば) (6)顔特徴データの利用に関する消費者の合理的な期待	企業は、倫理的かつプライバシープロアクティブな顔認識システムを運用するために、本文書に挙げる諸原則(伝統的な「公平な情報取扱い原則(FIPPs)」に基づくもの)を<u>採用しなければならない</u>。	プライバシー・バイ・デザインとして、顔認識技術を使う企業に<u>以下を勧告</u>。 (1)消費者の顔画像や顔特徴データに対して合理的な安全管理措置を講じること。 (2)適切なデータ保持・廃棄の取扱いを行うこと。 (3)顔認識製品やサービスを開発する際に情報のセンシティビティ(ex.設置場所)に配慮すること。
<u>子どもに対する配慮</u>	(子どもの顔特徴データの取得等に関する配慮については記載がない。)	(1)企業はティーンエイジャーに対して顔認識システムを使用する場合には特別な事前注意を行わなければならない。ティーンエイジャーに通知(notice)し、インフォームドコンセントを取得する際には、企業は<u>ティーンエイジャーの年齢や理解レベルについて考慮しなければならない</u>。 (2) <u>13歳未満</u>の子どもに対しては、証明可能な<u>親の同意</u>を得なければならない。	例えば顔認識機能付きの電子看板を開発する企業は、その設置場所について注意深く配慮し、トイレ・ロッカールーム・医療施設・<u>子ども集まる場所等のセンシティブなエリアへの設置は避けるべき</u>である。

各ステークホルダーが考える望ましいルール of 形態(1/2)

	業界団体	消費者団体	監督機関(FTC)
望ましい ルールの形 態	<u>ベストプラクティス</u>	<u>顔認識を規制する法律</u>	<u>基本的な個人情報保護法の下での 行動規範</u>
(顔認識に 関する) MSHPの存 在意義	【IBIAへのヒアリングより】 MSHPIは有効。	【CFAへのヒアリングより】 (1)MSHPはルールを決めるための適切な方法 ではない。なぜなら、 <u>決められたルールはあくま で自主的なものであり、企業がそれを守るイン センティブがない。また、そもそも企業が自分た ちを縛るような厳しいルールを作るようなインセ ンティブがない。したがって、法律が必要である。</u> (2)MSHPの実施にあたって、行動規範という呼 び方は誤解を招くので、ベストプラクティスと呼 ぶべきと提唱してきた。なぜなら、 <u>行動規範と いってもNTIAがフォローアップするものではな い。</u> どの企業が行動規範を採用するのか、行動 規範をきちんと遵守するのかをチェックするわ けではない。	【FTCへのヒアリングより】 (1)MSHPは難しい問題に対するソリュー ションを、色々な関係者を集めて探そうと いうもの。 (2)顔認識技術に関するMSHPがうまく行 かなかったのは、 <u>業界側が妥協するた めの強力なインセンティブがなかったからで はないか。業界にとっては法律制定の可 能性が強力なインセンティブとなる。その 場合、業界としては適切な行動規範があ れば、法律によるレギュレーションを免れ ることができるためである。今回は立法化 の恐れがなかったため、行動規範策定の インセンティブが働かなかった。</u>

各ステークホルダーが考える望ましいルール of 形態(2/2)

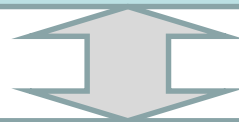
	業界団体	消費者団体	監督機関(FTC)
MSHP で 策定されたベストプラクティスの意義	【IBIAへのヒアリングより】 ・IBIA 等の業界団体はベストプラクティスに対する賛成意見を公表。 ・IBIAがベストプラクティスを支持したのは、<u>既に顔認識のアプリケーションが沢山あり、今後も増えていくことを考えると、ベストプラクティスを策定することが唯一の現実的な手段である</u>ため。 ・ベストプラクティスを参考にして、ベンダー企業とユーザ企業とがどうするかを考えていくべき。ベンダー企業はベストプラクティスを推奨はするが、実際に顔認識技術を使うのはユーザ企業である。 ・<u>技術の応用を事前に制限することはイノベーションを阻害する。</u> 【NRFへのヒアリングより】 ベストプラクティスを守るかはNRFの会員企業による。NRF全体として守る訳ではなく、個々の企業に依存する。	【CFAへのヒアリングより】 「ベスト」プラクティスと呼ぶ価値のないものが出来上がっている。消費者団体が脱退した時点で予想していた通り、弱体化したベストプラクティスができた。	【FTCへのヒアリングより】 NTIAのMSHPで策定されたベストプラクティスは、あくまで推奨であり要求ではないため、あまり意味がない。
民間分野を包括的に規制する基本的な個人情報保護法の必要性	【IBIAへのヒアリングより】 賢明な法律があれば、公共の場でバイオメトリクスを利用しても消費者も安心できるし、ベンダー企業も将来を見据えた技術を開発できる。企業があまり萎縮しないように、技術的進歩を消費者視点とのバランスを取っていくことが重要。ベストプラクティスはその一歩である。今後は、連邦政府の関与や、法律作りも必要になると考える。	【CFAへのヒアリングより】 ベストプラクティスや単なる自主規制では企業がそれらを守るインセンティブがない。消費者を守るために最低限の法律は必要。	2012年のFTCスタッフレポートにおいて、連邦議会に対して包括的なプライバシー立法を検討するように勧告を行っている。

小売店ユーザ企業とベンダー企業の感覚の違い

○ 商業施設における顔認識サービスの普及促進のためには、どうしたらよいのか？

- 小売店の業界団体（NRF）

- 顔認識技術の小売店での利用は、米国ではまだ模索中。普及促進のためには成功事例が必要。
- 顔認識を使って誘拐犯を逮捕できた、テロリストを予防できたなど（商用利用に限らず）事例の積み重ねが必要だ。
- 政府のガイドラインが妥当なものであれば、すなわち利便性とプライバシーとのバランスが取れたものであればヘルプフルである。そのようなガイドラインがあれば、顔認識技術の商用利用も進むのではないか。



- ベンダー企業の業界団体（IBIA）

- 顔認識技術は成熟してきているので、放っておいても使われていくのではないか。
- かつては利用に尻込みしていたが、最近では加速度的に利用が進んでいる。今後、何もしなくても利用が進むと思う。アイデンティティを確認する手段としては非常に強力な技術である。政府は顔認識の利用に躊躇があるが、消費者にはアレルギーがなくなっている。10年前とは違う状況だ。
- 消費者への啓発が必要とは考えている。例えば、SSN（社会保障番号）が漏えいした場合と、バイオメトリクスデータが漏えいした場合とで、消費者への影響は異なる。今後、IBIAでプライバシーフォーラムを開き、プライバシーとバイオメトリクスについて啓発したい。

まとめ

- 米国では、(日本に比べて)商業施設における顔認識技術の利用が進んでいる訳ではない。ただし、SNS・スマートフォンOS等では利用が進んでいる。
- 防犯目的での顔認識技術の利用は、一部の小売店・カジノ・金融機関で開始されている。
- 顧客の店内での動線を追跡して商品レイアウトを変更することや、既存顧客が入店した際に店員にアラートを送るといったマーケティング目的での利用は、今後期待されている。
- 商業施設での利用が十分に進まない理由は、ユーザ企業がレピュテーションリスクを恐れているため。消費者の顔認識技術に関する認知度・理解度も高くなく、マスコミ報道等に煽られた漠然とした不安感がある。社会的に受容されるための下地がまだ整っていない。これらの点は、日本と類似している。
- 米国の法律体系は、民間分野全体を規制する個人情報保護法(基本法)がない点で、日本とは異なる。基本法がなく、その立法化の可能性もないことから、業界側に法執行可能な行動規範を作成することのインセンティブ(行動規範の遵守によって直接的な法執行を免れる等)が働かず、今回のNTIAのMSHPはベストプラクティスの策定にとどまった。

まとめ

- 日本では、顔認識技術に関する商用利用ルールがなく、社会的なコンセンサスもないため、企業がレピュテーションリスクを恐れて利用に二の足を踏んでいるのが実態であり、何らかの共通ルールの策定が望まれる。
- 商用利用ルールは消費者のプライバシーに配慮したものであるとともに、顔認識技術を利用する企業にとって実現可能なものでなければならない。また、将来的なサービス開発やイノベーションの足枷となるものであってならない。そのさじ加減は難しいが、米国（FTCの報告書）や欧州（EU指令第29条作業部会の意見書、英国ICOの指針）などの先行事例は参考になるだろう。
- ルール策定のプロセスについては、米国の事例を見れば必ずしもフラットなマルチステークホルダープロセスが機能するとは限らない。関係者間の利害が一致しない場合に、一段上の立場から差配し、意見を収斂させるための「強制的な」メカニズムが内在していないからである。その意味で、国によるガイドラインの策定は、それがバランスの取れたものであるならば、事業者にとっても望ましいことである。また、顔認識技術の認知度・理解度向上のために、消費者向けの周知・啓発も重要となろう。