

# 個人識別性/識別可能性と いわゆる「FTC3要件」

—個人識別性を巡る米国の議論動向を踏まえて—

駒澤大学GMS学部 松前恵環

1

## 報告の流れ

はじめに

1. いわゆる「FTC3要件」とは
2. FTCにおけるこれまでの議論動向
3. 米国の関連法制・法学説の動向

おわりに

2

## はじめに—日本でのいわゆる「FTC3要件」への注目

### ■近時、「パーソナルデータ」を巡る日本の議論において、いわゆる「FTC3要件」が注目を集める

- ◆ 総務省「パーソナルデータの利用・流通に関する研究会報告書」(2013年)
- ◆ IT総合戦略本部「パーソナルデータに関する検討会」での立法措置としての「日本版FTC3要件」の導入に関する提言(2013年) 等

### ■意義と課題

- ◆ 意義: 個人情報の保護と利用のバランスを目指す試み
- ◆ 課題: 「日本版FTC3要件」の法制・政策への導入の是非・程度  
「個人識別性/識別可能性」を巡る議論との関係 等



今後、いわゆる「FTC3要件」の背景や、米国の法領域における議論の整理・検討等を行う必要

3

## 1. いわゆる「FTC3要件」とは

4

## 米国連邦取引委員会（FTC）の2012年の報告書

### 「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)

*'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers'* (2012)

#### ■ プライバシー保護のための新しいフレームワークを提唱

##### ■ 主な内容:

- ◆ プライバシー・バイ・デザイン (Privacy by Design)
- ◆ 消費者への簡潔な選択肢の提供 (Simplified Choice)
- ◆ 透明性の確保 (Transparency)

##### ■ 適用範囲:

- ◆ フレームワークの適用対象事業者

「このフレームワークは、**特定の消費者、コンピュータ、その他のデバイスに合理的に結び付けられ得る消費者のデータ**を、収集または利用する、すべての事業者に適用される。ただし、年間5,000名未満の消費者からセンシティブでないデータのみを収集し、かつ、そのデータを第三者と共有しない企業は、この限りでない。」

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, vii (2012).

5

## 適用範囲に関する報告書の記述：いわゆる「FTC3要件」

「最終フレームワークの下では、事業者のデータは、**当該事業者がそのデータについて3つの重要な保護措置を実施している場合は、特定の消費者またはデバイスに合理的に結び付けられ得ることとはならない。**」

- ◆ 「事業者はそのデータの非識別化を確保するために合理的な措置を講ずるべきである。」
- ◆ 「事業者は、そのデータを非識別化された形態で保有及び利用し、そのデータの再識別化を試みないことを、公に約束すべきである。」
- ◆ 「事業者がかかる非識別化されたデータを他の事業者に提供する場合には、それがサービス提供事業者であろうとその他の第三者であろうと、その事業者がデータの再識別化を試みることを契約で禁止すべきである。」

※個人を識別可能なデータと、ここで説明した非識別化のための措置を講じたデータの双方を保有及び利用する場合には、これらのデータは別々に保管すべきである。

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 20-21 (2012).

6

## 第1要件と「合理的な措置」の解釈

事業者はそのデータの非識別化 (de-identified) を確保するために合理的な措置を講ずるべきである。

### ■ 非識別化を確保するための合理的な措置

- ◆ 「事業者は、当該データが、特定の消費者、コンピュータ、その他のデバイスに関する情報を推測するために合理的に用いられない、または、合理的にそれらに結び付けられないという、正当な信頼の合理的なレベル (reasonable level of justified confidence) を達成しなければならない」

### ■ 「正当な信頼の合理的なレベル」

- ◆ 何が「正当な信頼の合理的なレベル」にあたるかは、個々の状況—「利用可能な方法及び技術」「問題となっているデータの性質」「(データが)利用される目的」などによる
- ◆ 例えば、企業が外部にデータを公表しているか否かはこの判断に影響する

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 21 (2012).

## 第2要件と「FTC法5条」の執行

事業者は、そのデータを非識別化された形態で保有及び利用し、そのデータの再識別化 (re-identify) を試みないことを、公に約束すべきである。

### ■ 公表に反した再識別化→FTC法5条の下での提訴の対象に

#### ■ FTC法5条:

- ◆ 「不公正または欺瞞的な (unfair or deceptive) 取引行為・慣行は違法である」 (15 U.S.C. Sec. 45(a)(1).)
- ◆ これに該当する場合、民事罰、差止命令、損害賠償請求の可能性
- ◆ プライバシー・ポリシー違反の他、情報漏えいの際の安全管理措置、更に近時は透明性の確保についての執行も見られる

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 21 (2012).

## 第3要件と‘Netflix’の例

事業者がかかると非識別化されたデータを他の事業者に提供する場合には、それがサービス提供事業者であろうとその他の第三者であろうと、その事業者がデータの再識別化を試みることを契約で禁止すべきである。

### ■ 提供先となる第三者の監督

- ◆ 契約条項の遵守状況を監視し、契約違反に対して適切に対処するために、「合理的な監督」を行うべきである

### ■ Netflixに対するFTCの調査

- ◆ Netflixは、計画を中止
- ◆ 以後、同様のデータを第三者と共有する場合には、「その利用に関する特別の制限について契約で合意した研究者にアクセスを限定する」とともに、データが消費者の再識別のために用いられることを防止するために、複数の「運用上の安全措置」を実施することに

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 21-22 (2012).

9

## 2. FTCにおけるこれまでの議論動向

10

## FTCにおける消費者プライバシー保護の主な取組み

- 1970年代: プライバシー保護に関する取組みを開始
- 1990年代半ば: オンラインプライバシーに関する取組み
  - ◆ 「オンライン・プライバシー」に関する二つの報告書
  - ◆ 「オンライン・プロファイリング」に関する二つの報告書
  - ◆ 「通知・選択(‘notice and choice’)アプローチ」の採用
- 2000年代: オンライン・オフラインの融合への対応
  - ◆ 「具体的な損害に基づいた(‘harm-based’)アプローチ」の採用
  - ◆ データ漏洩、ID窃盗、スパム等の問題への取組み
- 2000年代後半～2010年代: 新たな技術・サービスへの対応
  - ◆ 「オンライン行動ターゲティング広告」に関する報告書
  - ◆ これまでのアプローチの見直し→新しいフレームワークの提唱

U.S. Federal Trade Commission, *FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, 3-22 (2010).

11

## 「個人情報/個人識別可能情報」を巡るFTCの議論動向

### 「プライバシー・オンライン: 議会への報告」(1998年)

*‘Privacy Online: A Report to Congress’* (1998)

- 「個人情報(personal information)」は以下の二つの情報のカテゴリを含む
  - ◆ 「個人識別情報(personal identifying information)」(氏名、住所、eメールアドレス等)
  - ◆ 「その他の個人情報(other personal information)」または「市場分析のように個人を識別しない形態での集積に利用したり、消費者の詳細な個人プロフィールを作成するために個人識別情報と結び付けて利用したりし得る」「人口統計データや嗜好データ」(年齢、性別、所得水準、趣味等)

U.S. Federal Trade Commission, *Privacy Online: A Report to Congress*, 20, 31, 47 (n 19) (1998).

12

## 「個人識別性/識別可能性」を巡るFTCの議論動向

### 「プライバシー・オンライン: 電子市場における公正な情報慣行 : 議会への報告」(2000年)

*'Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress' (2000)*

#### ■「個人情報(personal information)」は、以下の二つの情報のカテゴリーを含む

- ◆ 個人を特定(locate)または識別(identify)するために用いられる「個人識別情報(personal identifying information)」(氏名、eメールアドレス、住所、電話・FAX番号、SSN、クレジットカード番号等)
- ◆ 「個人を識別しない情報」(non-identifying information)(年齢、性別、学歴、収入、趣味等、それだけでは(他の情報と組み合わせることなく)個人を特定・識別するために利用できない情報)

U.S. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, 9, 46 (n 53, 54) (2000). 13

## 「個人識別性/識別可能性」を巡るFTCの議論動向

### 「オンライン・プロファイリング: 議会への報告」(2000年6月)

*'Online Profiling: A Report to Congress' (June 2000)*

#### ■「個人識別可能情報(PII: personally identifiable information)」と「非個人識別可能情報(non-PII)」の区別に言及

- ◆ ‘PII’: 特定の個人に結び付け得るデータであって、氏名、住所、電話番号、eメールアドレス、社会保障番号(SSN)、運転免許証番号のような情報を含むが、それに限られない
- ◆ ‘non-PII’ であっても、‘PII’ と結び付けられるおそれ  
← オンライン広告事業者による、クッキーやWebバグを用いた情報収集を巡る懸念

U.S. Federal Trade Commission, *Online Profiling: A Report to Congress*, 2-6, 10-17 (June 2000). 14

## 「個人識別性/識別可能性」を巡るFTCの議論動向

### 「オンライン・プロファイリング：議会への報告(Part 2)」(2000年7月)

*'Online Profiling : A Report to Congress Part 2'* (July 2000)

- 6月の報告書における「個人識別可能情報(PII: personally identifiable information)」と「非個人識別可能情報(non-PII)」の定義を引き継ぐ
- 「透明性は、‘non-PII’及び‘PII’いずれの収集・利用にも関連する問題である」
  - ◆ ‘non-PII’についても一定の配慮を求める「NAI原則」を紹介

U.S. Federal Trade Commission, *Online Profiling : A Report to Congress Part 2* (June 2000).

15

## 「個人識別性/識別可能性」を巡るFTCの議論動向

### 「オンライン行動ターゲティング広告のための自主規制原則」(2009年)

*'FTC Staff Report: Self-Regulatory Principles for Online behavioral Advertising'* (2009)

- 「個人識別可能情報(PII: personally identifiable information)」と「非個人識別可能情報(non-PII)」との伝統的な区分の意義の減少 (※それぞれの定義については、2000年6月の報告書を踏襲)
  - ◆ ‘PII’と‘non-PII’との結合可能性
  - ◆ ‘non-PII’に基づいた個人の識別を容易にする技術の進展
  - ◆ 単体では匿名であっても他の情報と結び付けられることで個人を識別し得る情報の存在 (※AOLの例)
  - ◆ ‘non-PII’に関する消費者の懸念
- 適用対象となるデータ
  - ◆ 「オンライン行動ターゲティング広告のために収集されるあらゆるデータであって、特定の消費者、コンピュータまたはデバイスに合理的に結び付けられ得るもの」

U.S. Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online behavioral Advertising*, 20-26 (2009).

16

## 「個人識別性/識別可能性」を巡るFTCの議論動向

### ■2009年報告書における「合理的に結び付けられ得る (reasonably could be associated)」の意義

「情報が特定の消費者やデバイスに『合理的に結び付けられ得る』ものか否かは、**実際の状況や、利用可能な技術によって決まるが、例えば以下のような情報を含む**」

- ◆ 合理的な努力によって、消費者のウェブサイトの登録情報と結び付けられ得るクリックストリームデータ
- ◆ 特定の個人を識別し得るのに十分詳細なプロフィールに結び付けられた匿名データ
- ◆ 特定の消費者に結び付けられないが、パーソナライズされた広告やコンテンツを特定のデバイスに配信するために保管され利用される、行動プロフィール

U.S. Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 25 (2009).

17

## 2010年の事前報告書の公表

### 「急速な変化の時代における消費者プライバシーの保護【事前報告書】」 (2010年)

*'Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers'* (2010)

#### ■プライバシー保護のための新たなフレームワークを提示

#### ■「個人識別可能情報 (PII: personally identifiable information)」と「非個人識別可能情報 (non-PII)」との区分の妥当性の低下

- ◆ 公に利用可能な情報の増加
- ◆ 「再識別化」の可能性⇒「非識別化」された情報、「匿名化」概念の変容  
※Netflixの例

#### ■適用対象となるデータ: ‘PII’に限定されない

- ◆ 「このフレームワークは、特定の消費者、コンピュータ、その他のデバイスに合理的に結び付けられ得る消費者のデータを収集または利用するすべての事業者に適用される。」

U.S. Federal Trade Commission, *Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, 35-43 (2010).

18

## 2010年報告書へのパブリックコメント：適用範囲について

パブリックコメントの主な内容(例)	
賛成意見	<ul style="list-style-type: none"> <li>・「匿名の」データの再識別化可能性に照らせば、消費者やデバイスに合理的に結び付けられ得るデータを適用範囲とすることは支持される</li> <li>・個人から引き出されるすべての情報は何らかの保護に値する 等</li> </ul>
反対意見	<ul style="list-style-type: none"> <li>・PIIを含まないデータの収集及び利用に伴うリスクは、PIIの場合とは異なる</li> <li>・新フレームワークの「結合可能性」基準は、過度に曖昧で現実的でない可能性がある</li> <li>・十分な時間と資源があれば、いかなるデータも個人に結び付けられ得る</li> <li>・すべてのデータに同等レベルの保護を要求することは、容易に個人を識別するデータの収集を回避したり、収集及び利用するデータを非識別化するための措置を講ずる企業のインセンティブを低下させるおそれがある 等</li> </ul>
限定付けを要求するもの	<ul style="list-style-type: none"> <li>・特定の消費者、コンピュータまたはデバイスに実際に結び付けられたデータに適用範囲を限定すべき</li> <li>・識別可能な消費者に合理的に関連付けられる可能性があるデータに適用範囲を限定すべき</li> <li>・契約や内部管理によって特定の消費者に結び付けられないデータは適用範囲から除外すべき 等</li> </ul>

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 18-20 (2012). 19

## 2012年の報告書といわゆる「FTC3要件」の提示

### 「急速な変化の時代における消費者の保護」

*‘Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and PolicyMakers’ (2012)*

- パブリックコメントを踏まえ、2010年報告書の適用範囲を見直し
- 適用範囲に関する変更点：
  - ◆「合理的な結合可能性基準」の明確化として、非識別化のための3要件を追加
  - ◆適用対象となる事業者の限定
- 「合理的な結合可能性基準」の明確化の意義：
  - ◆「当該基準が過度に広範であるという懸念」への対応
  - ◆事業者に、「特定の消費者またはデバイスに結び付けられる可能性の少ない態様でデータを収集・利用するインセンティブ」を与え、それによりプライバシー保護を促進
  - ◆事業者に公の約束を求めることで「説明責任」を果たさせる

U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 22 (2012). 20

### 3. 米国の関連法制・法学説の動向

21

#### 「個人識別/個人識別可能性」と米国のプライバシー保護法制

##### ■米国のプライバシー保護法制の特徴:

- ◆ 民間部門を規律する包括的なプライバシー法は存在せず
- ◆ 分野ごとの個別の立法と自主規制で対応

##### ■米国のプライバシー保護法制における「個人情報 (PI: personal information)」ないし「個人識別可能情報 (PII: personally identifiable information)」概念

- ◆ 各法律により、用語・定義とも不統一
- ◆ 1990年代半ばからは‘PII’がよく用いられるように
- ◆ 一般的にEUの ‘personal data’ より範囲が狭いと言われる

##### ■現行法制における ‘PII’ 概念への依存

- ◆ ‘PII’ のカテゴリに含まれる情報は保護され、このカテゴリに含まれない情報は保護されないという「二分法 (dichotomy)」

See e.g., Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U.L. REV. 1814 (2011).

22

## HIPAAプライバシー規則における「非識別化データ」の利用

### ■HIPAA プライバシー規則

- ◆ 「医療保険の相互運用性と説明責任に関する法律」(HIPAA: Health Insurance Portability and Accountability Act of 1996)に基づき、保険社会福祉省(HHS: Department of Health and Human Services)が制定
- ◆ 「非識別化された保健情報(DHI: de-identified health information)」の利用・開示について規定

### ■DHI:

- ◆ 「個人を識別しない、または、その情報が個人を識別するのに利用され得ると信ずるにつき合理的な根拠を提供しない、情報」
- ◆ 以下の二つの場合に非識別化
  - 「統計学基準」:統計学者等が個人識別可能性がないと公式に決定
  - 「セーフ・ハーバー基準」:個人に関する18項目識別子の削除  
(45C.F.R.Sec.164.502 (d)(2), 164.514 (a), (b).)

「ここ40年間、立法者は、表立って利益衡量を行うことを免れるための完璧な特効薬—匿名化—を活用してきた。」

Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1736 (2010).

23

## 「再識別化」のリスクを巡る近時の法学領域の学説

### ■理論上のリスクの指摘は既に1990年代にも(J. Kang)

- ◆ 匿名化された情報など、一見特定の個人が識別されないと解される情報であっても、「文脈(context)」や「付加的な調査(additional research)」など、「総合的な状況(totality of circumstances)」によって個人を識別され得る場合もある  
Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1206-1211 (1998).

### ■クッキー、IPアドレスなどの個人識別可能性・要保護性を巡る議論

### ■近時、「再識別化」を巡るコンピュータ技術者の研究の法学領域への導入

- ◆ 「再識別化」が問題となった具体的事案(AOL、Netflix等)の発生と、これらを契機としたコンピュータ技術者の研究等
- ◆ これらの議論を法学領域に導入して、「匿名化」に警鐘(P. Ohmら)

24

## おわりに—まとめと若干の考察

### ■技術の進展により増幅する「個人識別性/識別可能性」判断の困難

- ◆ 理論上の困難はこれまでも認識
- ◆ 近時、具体的事案の発生と、これを契機とする技術者の研究により、「再識別化」という用語とともに注目を集める

### ■「個人識別性/識別可能性」を巡る米国の制度や議論の特徴

- ◆ 「個人情報/個人識別可能情報」等、関連する用語やその定義の不統一
- ◆ いわゆる「FTC3要件」
  - 保護対象となる情報の拡大とセットで論じられているもの
  - FTCの強力な執行力を背景とするもの

### ■情報の性質の「文脈依存性」→分類の難しさ

- ◆ 「個人識別/識別可能情報」:「動的な」概念
  - その範囲画定は個々のケースにおける文脈に依存せざるを得ないことに加え、技術の進展により今後も変化していく蓋然性が高い
- ◆ 柔軟・弾力的な対応を可能にしておく必要

25

ご清聴どうもありがとうございました。

26