Empowered by Innovation NEC

プライバシー保護のトレンド ご紹介

2013/2/14

日本電気株式会社

宮川　伸也

本講演の内容

1. プライバシー保護を考えるにあたって
2. プライバシー侵害の事例紹介
3. プライバシー保護に対する取り組み

プライバシー保護を考えるにあたって

個人情報保護法における「個人情報」の定義

第二条一項

- この法律において「個人情報」とは、**生存する個人**に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により**特定の個人を識別することができるもの**(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう。

個人情報＝?プライバシー保護すべき情報

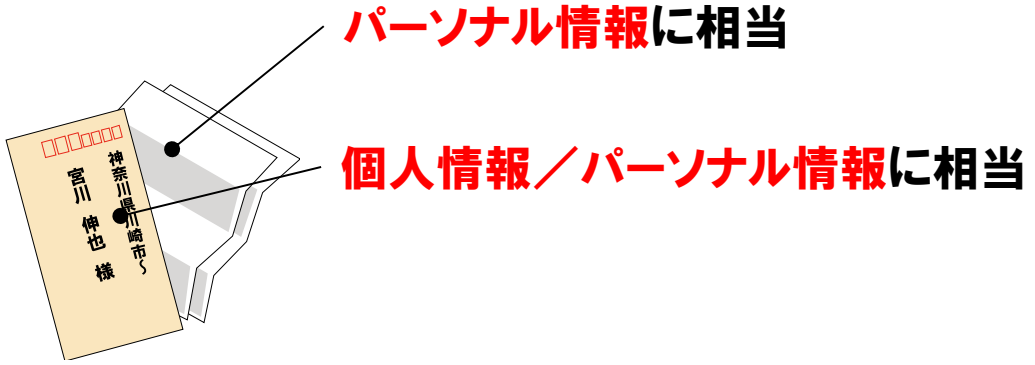
プライバシー保護が必要な情報(パーソナル情報)とは何か？

パーソナル情報のだいたいの解釈 (『宴のあと』事件」判決より)

- 個人の私生活上の事実 (事実らしく受け取られる事柄を含む)を示す情報
- 私人としては、通常は公開を望まない情報
- 公知になっていない情報

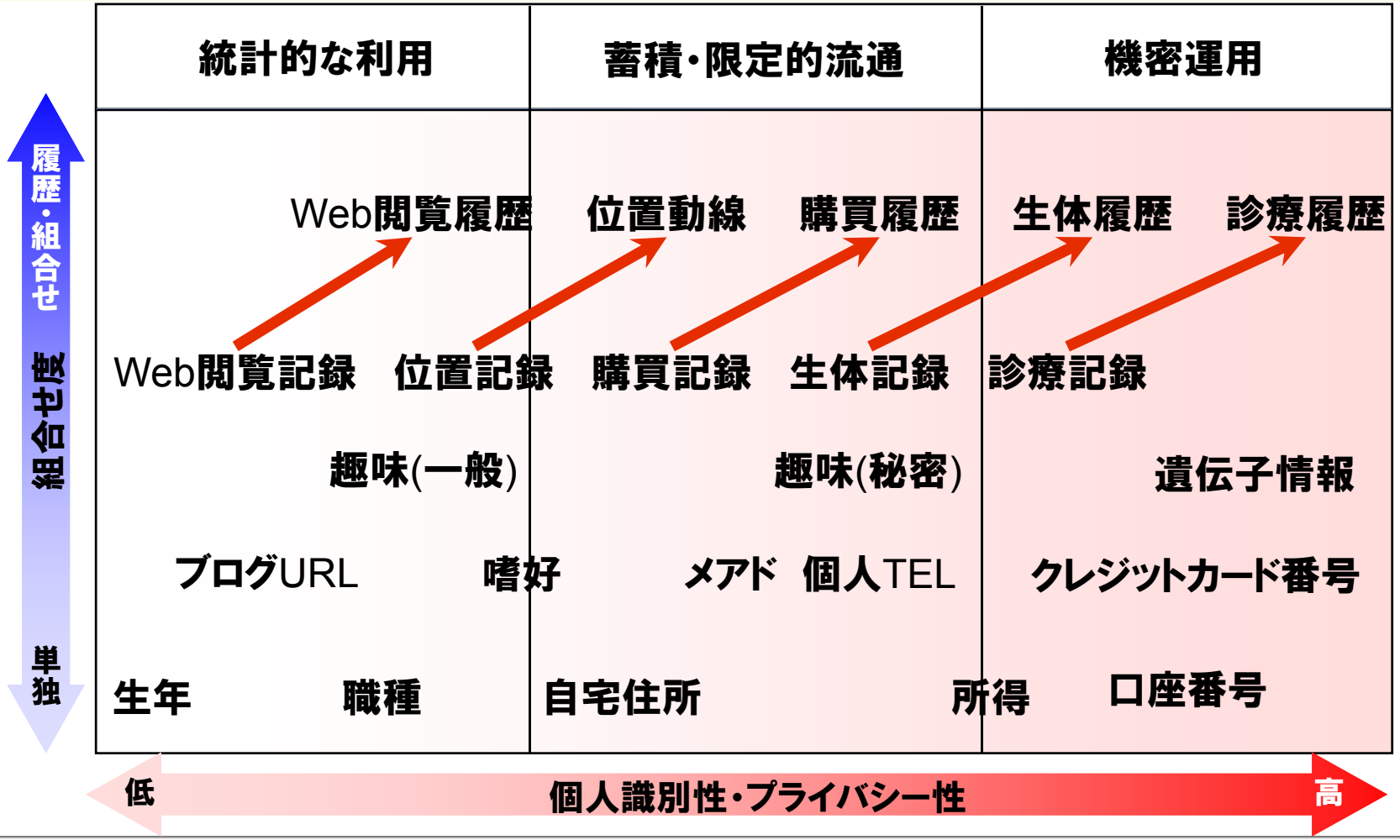
要するに…

- パーソナル情報は、個人情報保護法で定義される個人情報とは次元が異なる
- その人が公開したくないと思っている私的な情報であれば、個人情報である／なしに関わらず、その情報はパーソナル情報
- パーソナル情報の解釈は、人によって違う



パーソナル情報の個人識別性・プライバシー性

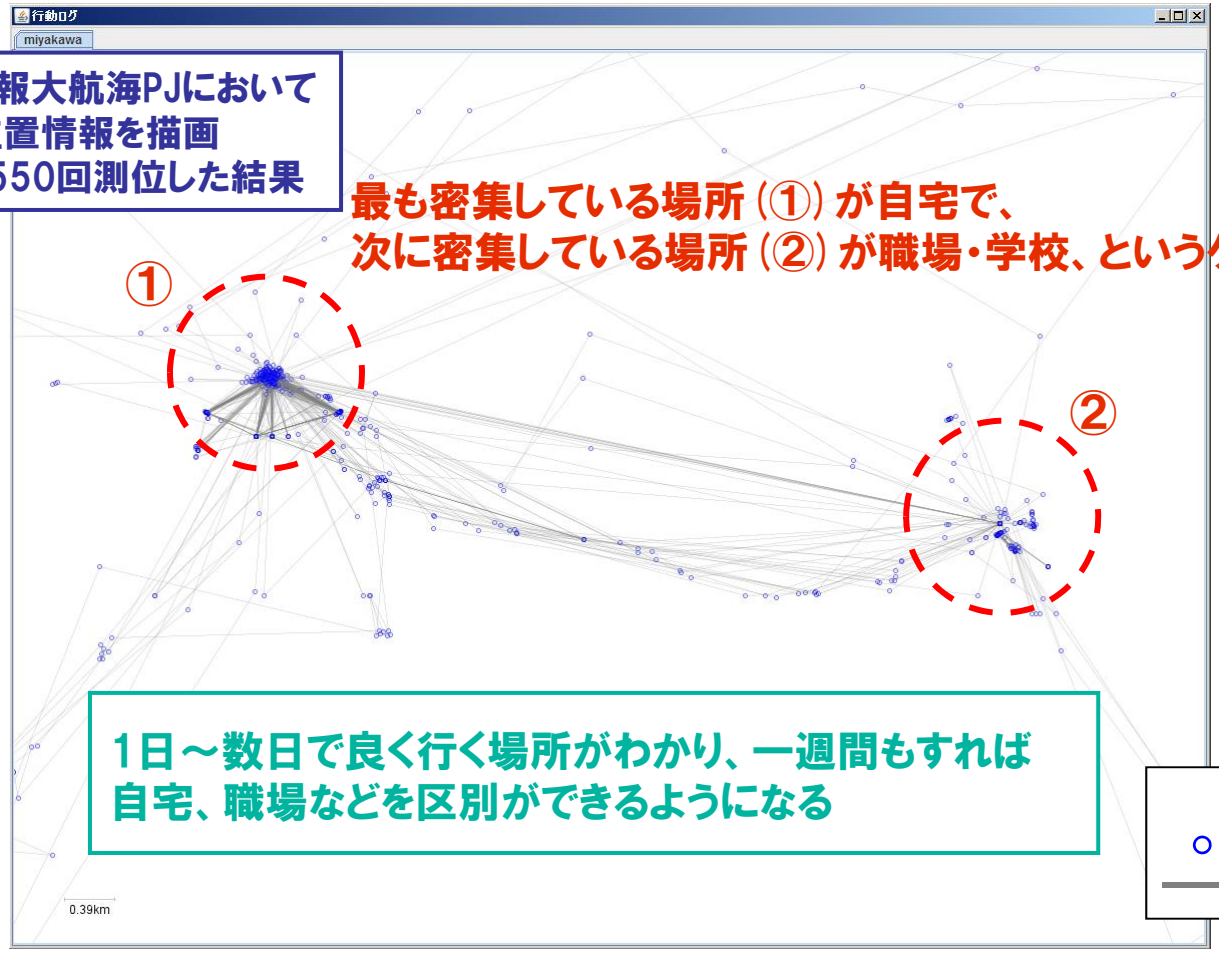
パーソナル情報の個人識別性とプライバシー性は多様であり、組合せによって個人識別性やプライバシー性が変化する場合もある



位置情報はパーソナル情報？

頻繁に提供された位置情報から最も測位された場所からユーザを特定でき、
誰がどこに行ったかが分かるためパーソナル情報として扱われるべき

経済産業省 情報大航海PJにおいて
収集した私の位置情報を描画
約2ヶ月間に3,550回測位した結果



最も密集している場所（①）が自宅で、
次に密集している場所（②）が職場・学校、というケースが多い

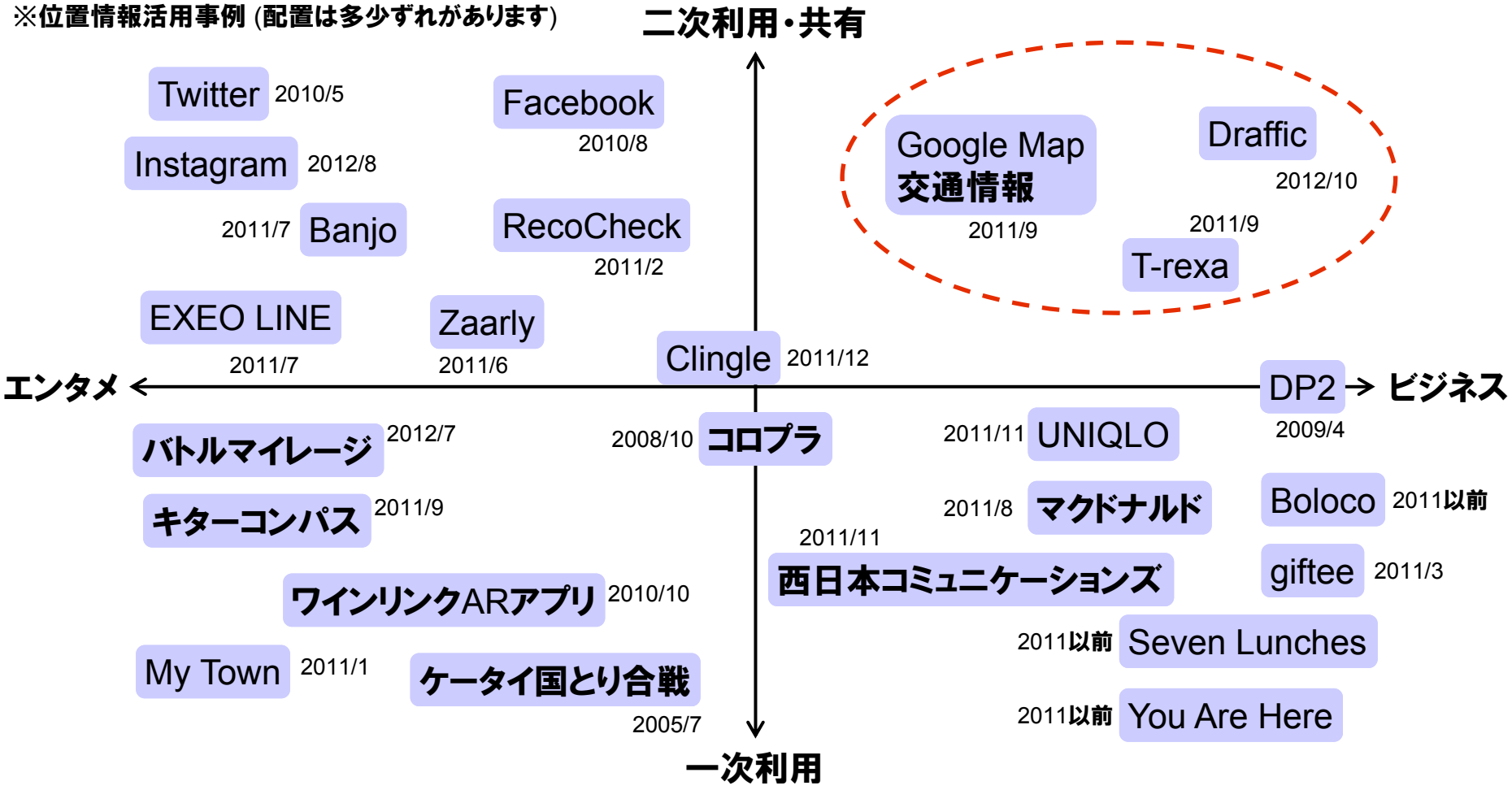
1日～数日で良く行く場所がわかり、一週間もすれば
自宅、職場などを区別ができるようになる

凡例
位置（緯度・経度）
位置間の移動

プライバシー侵害の事例紹介

パーソナル情報(位置情報)を活用したビジネスの広がり

パーソナル情報を活用したサービスは、以前はゲーム系が多かったが、最近は
二次利用・共有でビジネスに活用するケースも増えている

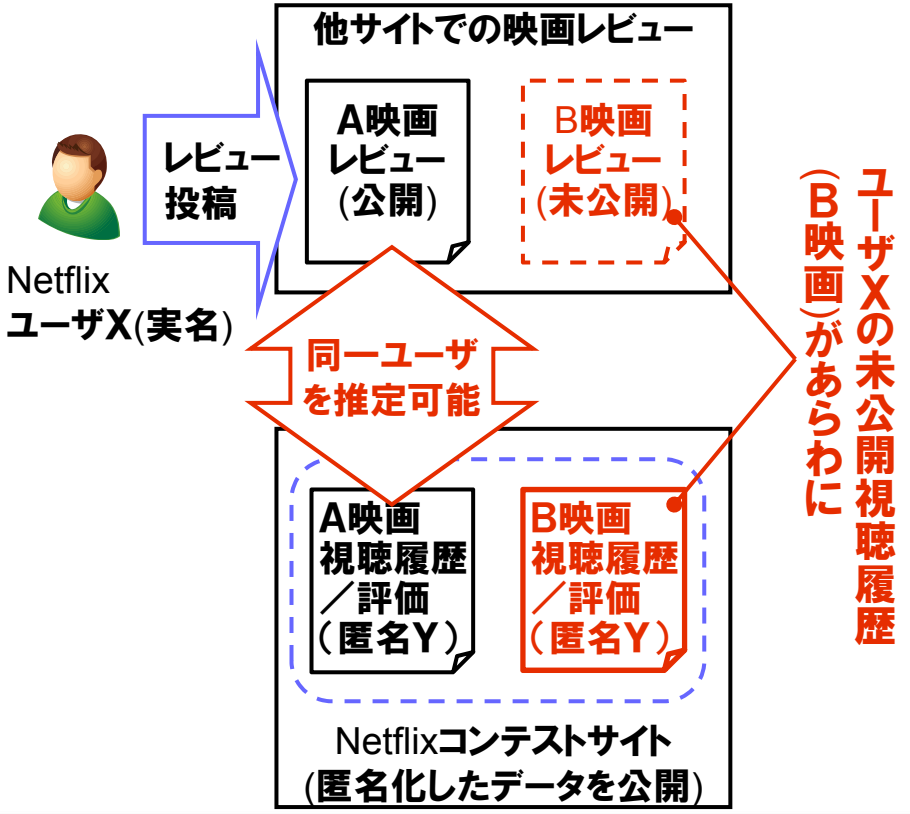


パーソナル情報公開における問題事例：Netflixコンテスト

- Netflix社はユーザの嗜好に合わせて映画をお勧めするアルゴリズムのコンテストのために、**約50万人のユーザの視聴履歴と評価を匿名化して公開**
- 特定ユーザの視聴履歴を類推できることから訴訟問題にまで発展
- 同社は予定していた**2回目のコンテストを中止**

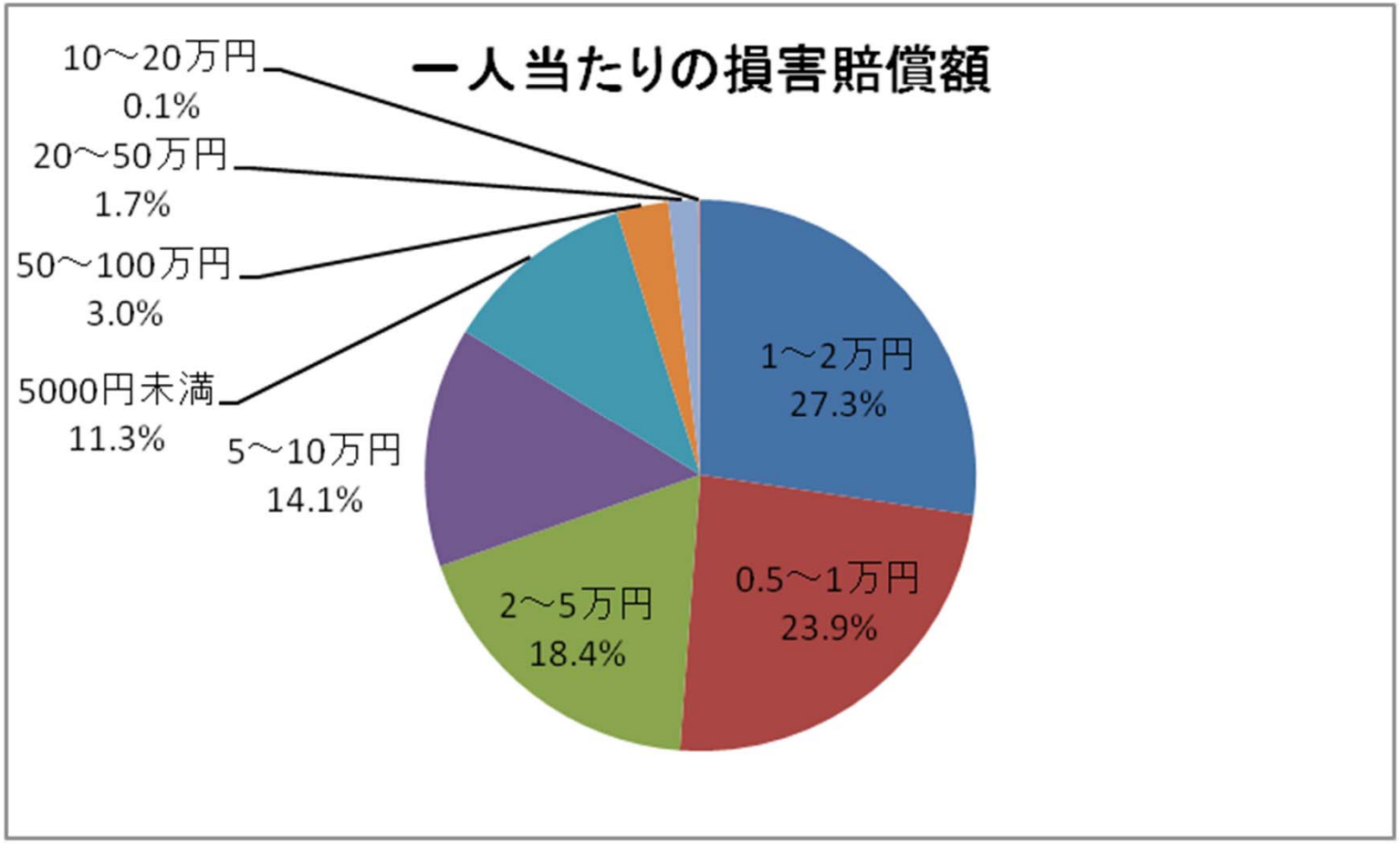
※Netflix社：全米最大のオンライン映画配信、DVDレンタル企業

Netflixコンテストサイトにおいて
ユーザの映画レビューを公開



パーソナル情報漏えいの損害賠償額

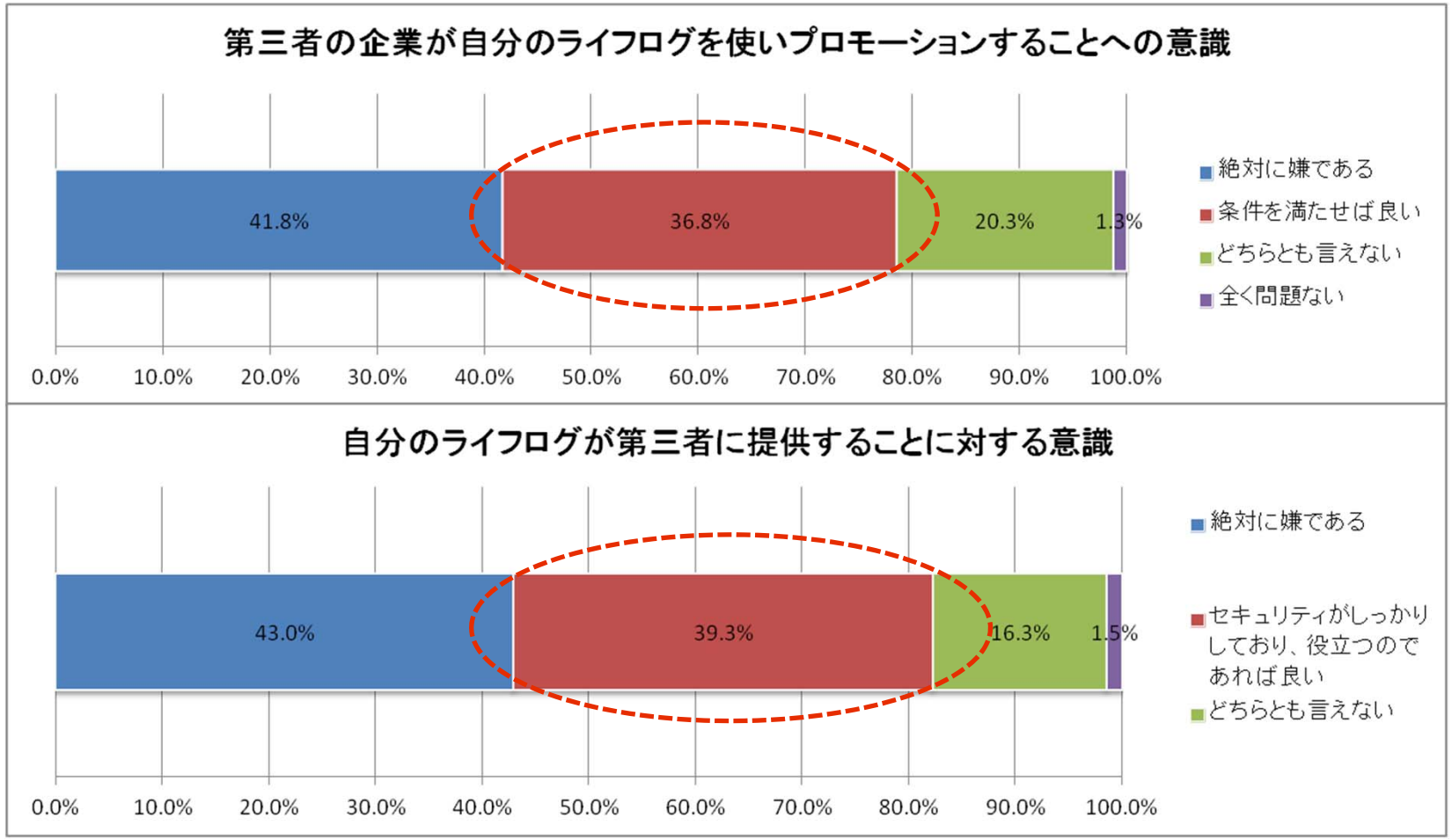
情報の機密性・プライバシ性や被害人数にもよるが、漏えいした際には莫大な損害賠償額になる他、社会的信用を損なうことになる



2011年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～NPO 日本ネットワークセキュリティ協会、2012/9/20発行)から引用

エンドユーザの意識

パーソナル情報を安全に管理していることをアピールすることで、第三者に利用されることを肯定的に感じるユーザを増やせる

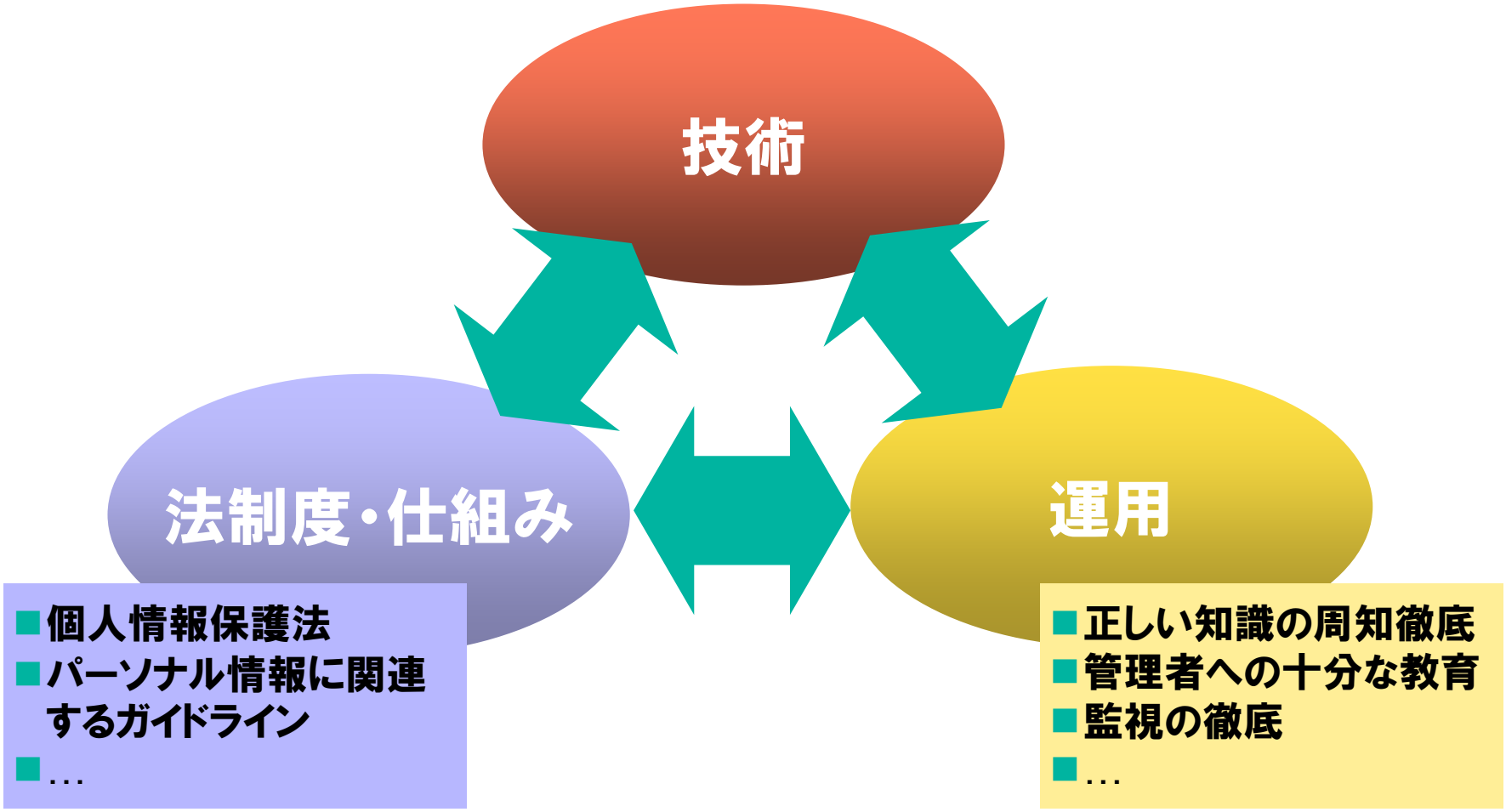


2011年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～から引用

プライバシー保護に対する取り組み

パーソナル情報を保護するためのアプローチ

パーソナル情報を保護するためには、保護の基準や指針となる**法制度や仕組み**が不可欠。それを基に、**技術**ばかりでなく、**適切な運用**が必要



各国のパーソナル情報の法制度

近年のプライバシーへの関心の高まりに対して、先進国ではプライバシー保護が強化されつつあり、各新興国においても法規制が整備されつつある

	日本	EU	米国	新興国
現状	■ 日本国憲法で、古典的なプライバシー権を規定 ■ 個人情報保護法で、個人情報のみに積極的プライバシー権を規定	■ EUデータ保護指令で、アクセス権、ユーザの同意、データ最小化の要件、データ管理者に課されるガバナンス上の様々な義務を規定	■ 連邦レベルでの包括的な個人情報保護法・プライバシー法は存在せず ■ 一部の業界では法令が定められ、その他は自主規制やガイドラインで対処	■ 2010年頃からOECDガイドラインに基づく法制度を整備
今後の動き	■ 匿名化に関して事業等分野ごとのガイドラインが整備されることを日本再生加速プログラムで後押し	■ EUデータ保護規則で、オプトイン原則の明確化、罰則規定の厳格化、忘却される権利の提示	■ 消費者プライバシー権利章典に基づき、ネット上等のパーソナル情報の扱いにおいて、個人の権利が具体化される見込み	■ 先進国の動きに追従する可能性があるが、現状では不明

ご参考：政策動向

オープンデータ／匿名化された個人情報の流通・活用に関して、具体的な取組みが行われ始めている

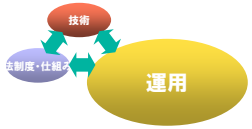
オープンデータ関連

- **電子行政オープンデータ戦略**　by IT**戦略本部** (2012/7)
- IT**融合フォーラム 公共データ**WG**発足** by **経産省** (2012/8)
- DATA METI**構想** by **経産省公共データ**WG (2012/10/4)
- **パーソナルデータの利用・流通に関する研究会** by **総務省** (2012/10/30～)

個人情報活用自由化関連

- 2012**年度経団連規制改革要望** (2012/9)
- **日本再生加速プログラム@閣議決定** (2012/11)

プライバシーに関連する規格

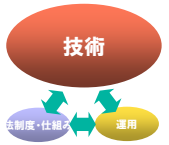


プライバシーに関する規格は、セキュリティ全般からプライバシー保護の詳細へ、開発・運用ばかりでなく、規格・設計まで広範囲に規定されている

	企画	設計	開発	運用
セキュリティ		コモンクライテリア (ISO15408, 2005) ・情報技術セキュリティ評価基準 ・情報セキュリティに関連した製品及びシステムの設計と実装を評価するための規格		第三者適合性評価制度 ISMS (ISO 27001, 2005) ・情報セキュリティマネジメントシステム ・情報システム、データ、それらを管理する環境・体制に対するリスクアセスメントの規格
プライバシー	PIA (ISO 22307, 2008) ・プライバシー影響評価 ・プライバシーリスクを事前に評価するリスク管理手法			PMS (JIS Q 15001, 2006) ・個人情報マネジメントシステム ・事業者が個人情報の取扱いを適切に行う体制を整備していることを認定するための規格 個人情報保護法 (2005)／個人情報保護ガイドライン

プライバシー影響評価ハンドブック、公立大学法人首都大学東京、産業技術大学院大学、2012を参考に作成

プライバシー保護技術の分類



分類		技術
データに対する保護	曖昧化による保護	①データ匿名化
		②ランダム化
	暗号化による保護	③マルチパーティプロトコル
		④準同型性暗号
クエリー結果に対する保護		⑤差分プライバシー

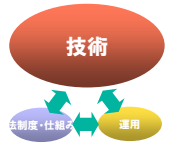
データに対する保護

- パーソナル情報全体を公開することを前提とし、パーソナル情報を加工してプライバシを保護

クエリー結果に対する保護

- パーソナル情報を検索、分析することを前提とし、その際に実行されるクエリーの結果を加工・制御してプライバシーを保護

データ匿名化 (k-匿名化とℓ-多様化)



データ匿名化(k-匿名化、ℓ-多様化等)は、データ自体を加工し、ユーザの準識別子を知る閲覧者に対してセンシティブ属性を知られないようにする技術

A病院のカルテデータ（元データ）

No.	ZIPコード	年齢	国籍	病状
1	13068	28	ロシア	心臓病
2	13068	29	アメリカ	心臓病
3	13053	21	日本	感染病
4	13053	23	アメリカ	感染病
5	14853	31	アメリカ	風邪
6	14853	37	インド	風邪
7	14850	36	日本	がん
8	14850	35	アメリカ	がん

準識別子 ／ センシティブ情報

k-匿名化 準識別子の組合せが同じユーザをk人以上にする

No.	ZIPコード	年齢	国籍	病状	
1	13068	28-29	*	心臓病	k=2
2	13068	28-29	*	心臓病	
3	13053	21-23	*	感染病	k=2
4	13053	21-23	*	感染病	
5	14853	31-37	*	風邪	k=2
6	14853	31-37	*	風邪	
7	14850	35-36	*	がん	k=2
8	14850	35-36	*	がん	

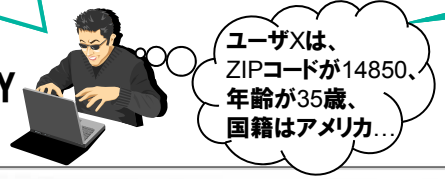
ℓ-多様化 準識別子の組合せが同じユーザのセンシティブ情報をℓ通り以上にする

No.	ZIPコード	年齢	国籍	病状	
1	130**	21-29	*	心臓病	ℓ =2
2	130**	21-29	*	心臓病	
3	130**	21-29	*	感染病	ℓ =2
4	130**	21-29	*	感染病	
5	148**	31-37	*	風邪	ℓ =2
6	148**	31-37	*	風邪	
7	148**	31-37	*	がん	ℓ =2
8	148**	31-37	*	がん	

ユーザXは、レコード8で、「がん」なんだな

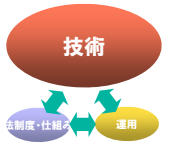
ユーザXは、レコード7と8のどちらか分からないけど、とにかく「がん」なんだな

？ユーザXは、レコード5～8のどれか分からない。「風邪」なのか？「がん」なのか？



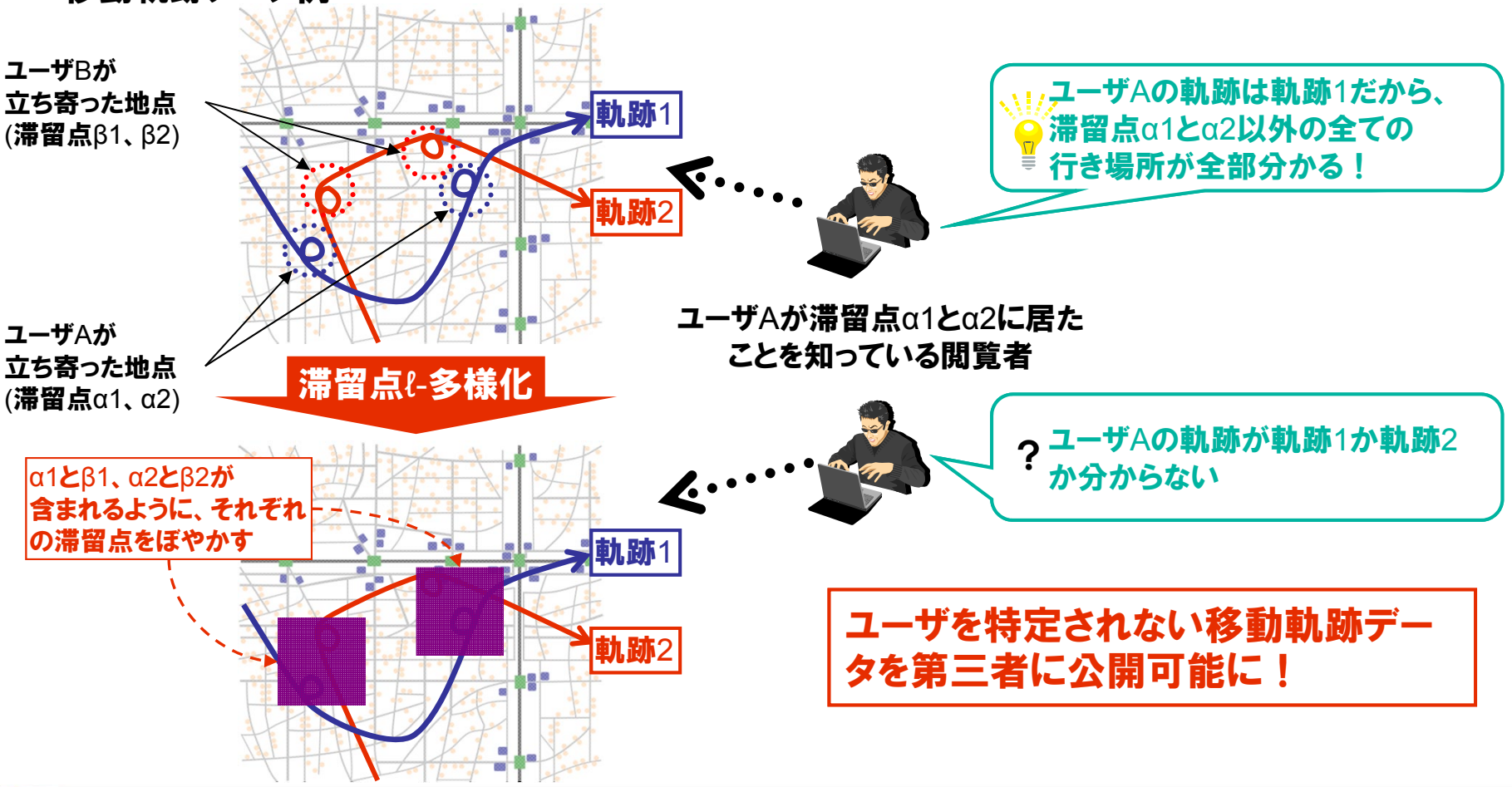
A病院に通うユーザXの準識別子を知る閲覧者Y

移動軌跡に対する匿名化



移動軌跡データは経路解析(ある施設を利用したユーザの経路分析等)に有用であるが、第三者に公開する場合、プライバシー漏えいを防ぐことが重要

移動軌跡データ例



まとめ

リスク

- 蓄積されたパーソナル情報が漏えいする事件・事故が増えており、漏えい時には、莫大な損害賠償や社会的信用損失が伴う
- 漏えいの防止には限界があるため、データのプライバシを保護し、安全に管理していることをアピールすることが、ユーザの安心感につながる

法制度

- 様々なパーソナル情報が各国の法制度やガイドラインで保護対象になる可能性が高く、今後の動向に注視する必要がある

各社動向

- これまではパーソナル情報を限定的に使うことが多かったが、最近は統計利用等のさらなる活用事例が増えている
- その際には、個人を特定できないような対策(運用、技術採用)を行う企業が増えている

パーソナル情報の活用が注目されているが、リスクの回避と法制度への対応のために、個人のプライバシーを保護することが重要になる