

認定保護団体指針の 匿名加工基準策定に向けて

国立研究開発法人 産業技術総合研究所
高木 浩光

最近の経緯

- 5月20日 前回本シンポジウム
 - JILISによる情報公開請求で開示された資料を紹介
 - 政府はB説？これを否定する内閣法制局長官の指摘を紹介
 - 仮ID問題に言及 仮IDは不要だったのでは
- 6月4日 日記「匿名加工情報は何でないか・後編」
 - 法制局長官指摘で法案が根本的に変更されていたことを発掘
- 6月17日 情報法制シンポジウム（JILIS）
- 7月22日 日記「匿名加工情報は何でないか・後編の2」
 - 法制局長官指摘で「ひっくり返った」とする明確な根拠を発掘
 - 「復元することができないように」が実は重要だと判明
- 9月14日 情報処理学会FIT
 - 終了後、森・高橋両氏と仮IDの不要性について議論

匿名加工の基準は結局曖昧なまま

- 必要条件はいくつも示されたが
 - 十分条件的なものは全然示されていない
- 5月のJIPDECの指針は匿名加工の基準を示さなかった
 - これからするとしている
- 認定保護団体の指針で具体的な基準を示したものはない
 - いずれも施行規則と委員会ガイドラインのコピペ
- これから具体的な基準を示す指針が期待されている
 - いくつかの具体的なデータ流通のケースで、認定団体があるところでは指針を示せるかも
- 十分条件的な基準を作ろうにも
 - 法律の条文解釈からして曖昧なところがある

法の条文解釈で曖昧

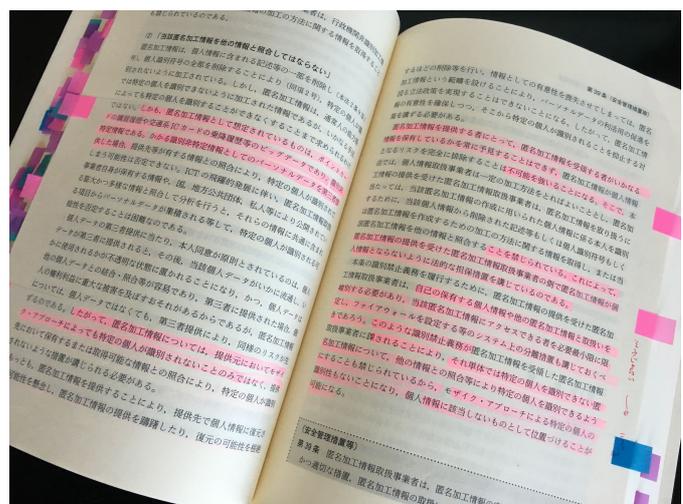
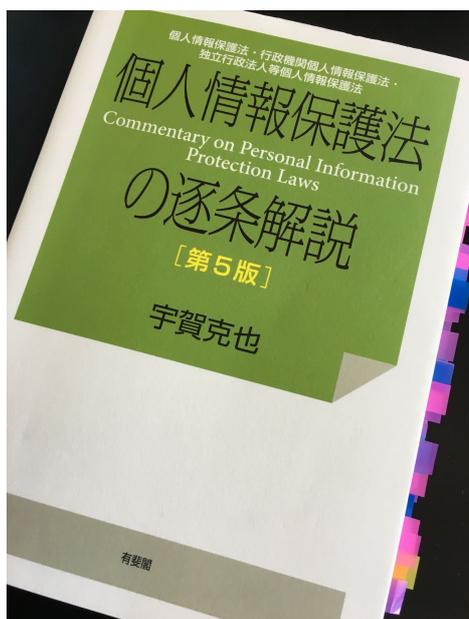
- 解釈が定まらないと基準の妥当性を誰も言えない
- 「匿名加工情報は個人情報でない」とされるが
 - A説 非個人情報でない限り匿名加工情報となり得ない？
B説 匿名加工情報に加工すれば非個人情報ということになる？
 - 高木浩光「匿名加工情報の制度概要と匿名加工基準の規則案」ビジネス法務16巻11号17頁以下（2016年9月）
 - B説では
 - 36条5項の規定により、作成者において、匿名加工情報を元の個人情報と照合することが禁止されるから、「容易に照合することができ」が否定されるという考え方
 - B説に基づくと
 - 仮名化だけで常に非個人情報ということにできてしまう
 - データセット照合は一切考慮しなくてよいことに……
 - 施行規則19条5号はそれを否定している……？

総務省視聴者プライバシー保護WG

- JEITA意見
 - 「詳細時刻情報を丸めるという考え方は再考いただきたい」
 - 「提供先での再識別のリスクは、法的に禁じることをもって十分とする
と考えることはできないか」
 - 「外部観測性はないため、個人の特定につながるリスクが一般的にありうるかには疑問がある」
 - B説に基づく加工基準の考え方を主張
- JEITA意見に対するWG事務局見解（6月7日）
 - 「法で再識別が禁止されていることをもって加工方法の基準を緩和することは、制度趣旨に照らすと適切ではない」
 - 「通常の方法により特定できないような状態にすることを求めるという規律を課した上で、さらに再識別の禁止を課しているものであって」
 - B説を否定する方向性

宇賀・逐条解説第5版

- B説で書かれているが……



- 「復元することができないように」を説明していない

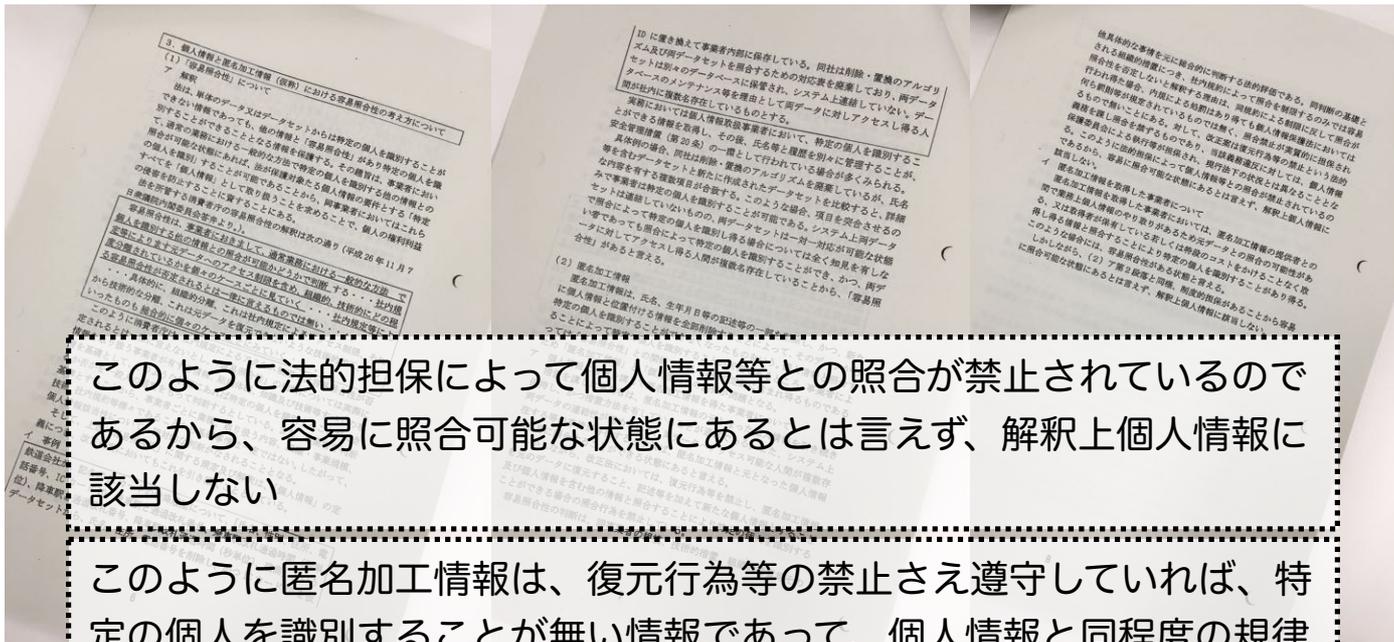
「復元することができないように」とは？

- 当初は飾りだと思っていた
 - 瓜生編1問1答では、識別できないようにと復元できないようにとは同じことが並べて書かれているように見えた
- 加工内容ではなく組織的管理措置のこと説
 - 前掲ビジネス法務で高木
 - 「②の「識別できない」と③の「復元できない」は、それぞれ誰にとってできないという意味か。……③は加工に限らず「できないようにしたもの」であり、解説書によれば「できないような状態にすること」を言うと言われる。この「状態」とは、組織的管理措置も含まれ、他の情報を加えることで復元可能となるような状態にしないを作り出さないことを求めるものと理解できる。このような管理は、法36条5項及び38条が求めている。
- そうじゃなかったことが開示資料で判明

立案段階で存在した旧案と新案

- 内閣法制局長官がひっくり返す前の案
 - 規制緩和する案だった
 - まさに仮名化するだけでOKとする案だった
 - 個人識別符号を削除すれば突合リスクを排除できるという考え方
 - 個人識別符号を広めに入れる前提だった
 - 照合禁止の義務により容易照合性は解消するとする解釈を導入
- 内閣法制局長官がひっくり返した後
 - 仮名化でOKとする案を撤回
 - 「復元することができないように」を定義の要件に追加
 - 規制緩和にならないことが認識されていた様子
 - 躊躇せずできるようにするものであって、基準の明確化こそが肝であることが整理文書に書かれている

旧案の説明資料



このように法的担保によって個人情報等との照合が禁止されているのであるから、容易に照合可能な状態にあるとは言えず、解釈上個人情報に該当しない

このように匿名加工情報は、復元行為等の禁止さえ遵守していれば、特定の個人を識別することが無い情報であって、個人情報と同程度の規律を課すことまでは求める必要のないものである。

- 2014年11月時点の案に対する説明資料である点に注意

条文も成案とは異なるものだった

- ボツになった旧案

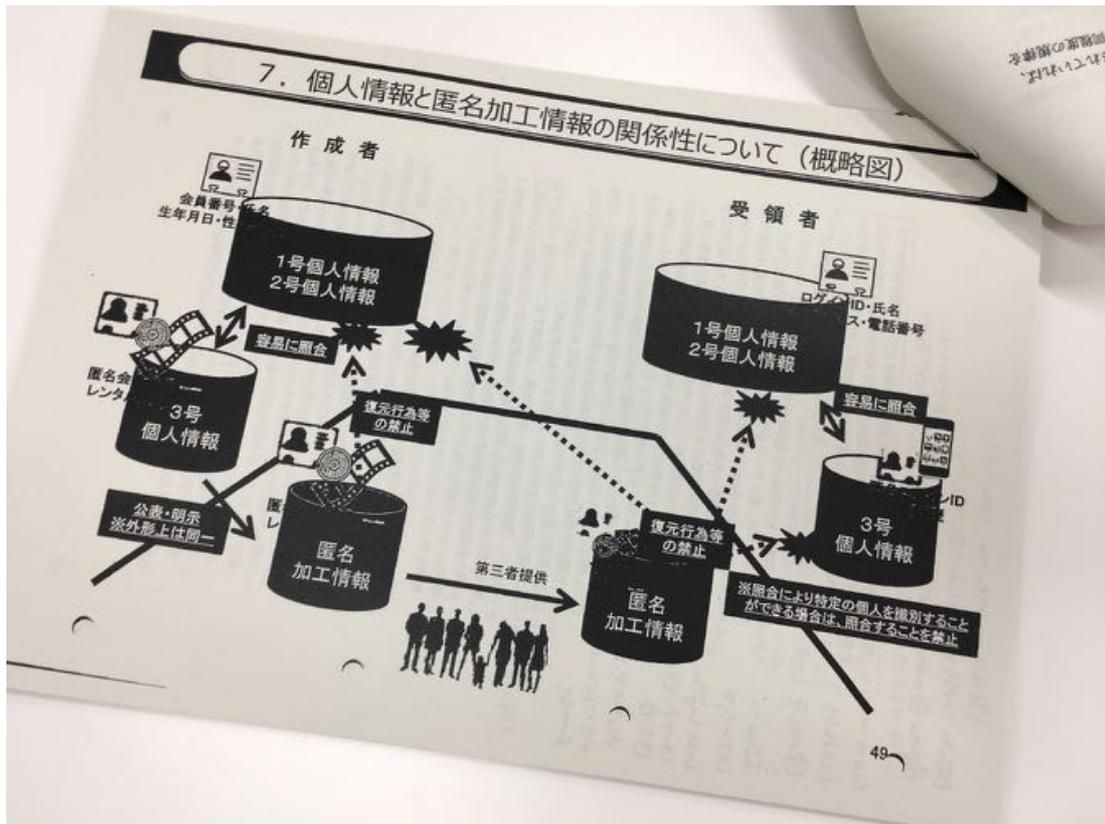
第2条 この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

- 一 当該情報に含まれる氏名、生年月日その他の記述等（第2号に規定する個人識別情報を除く。以下同じ。）により特定の個人を識別することができるもの
- 二 特定の個人に関する身体の一部若しくは一部を用いて電子計算機の用に供するために作成され、又は旅券の番号（略）を含むもの
- 三 個人情報取扱事業者において、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又は個人識別情報を識別することができることとなるもの（第7項に規定する措置を講じた者以外が取り扱う場合における当該措置に係る匿名加工情報を除く。）

7 この法律において「匿名加工情報」とは、生存する個人に関する情報であって、次の各号に掲げる個人情報に当該各号に定める措置を講じて得られるもの（略）及び第1項第3号に該当するものをいう。

- 一 第1項第1号に該当する個人情報 氏名、生年月日その他の記述等の全部又は一部を削除すること（他の情報に置き換えることを含む。）により、特定の個人を識別することができないようにすること。
- 二 第1項第2号に該当する個人情報 個人識別情報を全部削除すること（他の情報に置き換えることを含む。）

旧案の説明資料



これに対する内閣法制局長官の指摘

2014年12月1日

個人情報保護法

長官指摘 (12月1日)

まだ粗いので、19日に公表というのは難しいのではないかと

○ 指紋データ等 (1)

どのような基準でこのカテゴリーに入れるものを抽出するにすること。また、つまみ食いみたいになるのは不可であるカードについても、店で個人識別ができるデータと共に管理グループに入れるべきである。他方、身体特性については、ほはないのだから、個人識別に足りるものに限定すべきでこれら二つは、考え方が異なるので分けて書くこと。

○ 匿名加工情報 (2)

復元禁止の規制で対応しようというのは無理がある。個人情報に戻りかねないものが容易に流通することになるのは危険すぎる。加工者が第三者に提供する時点で、復元ができないように、個人識別情報にたどり着けないように、加工しなければならないことにすべきである。(容易照会もできないような形で提供すべきである)

その上で、加工者と二次的な利用者は分けて規制を設けるべきである。

○ 要配慮情報 (3 (1))

2014年12月16日

個人情報保護法骨子案

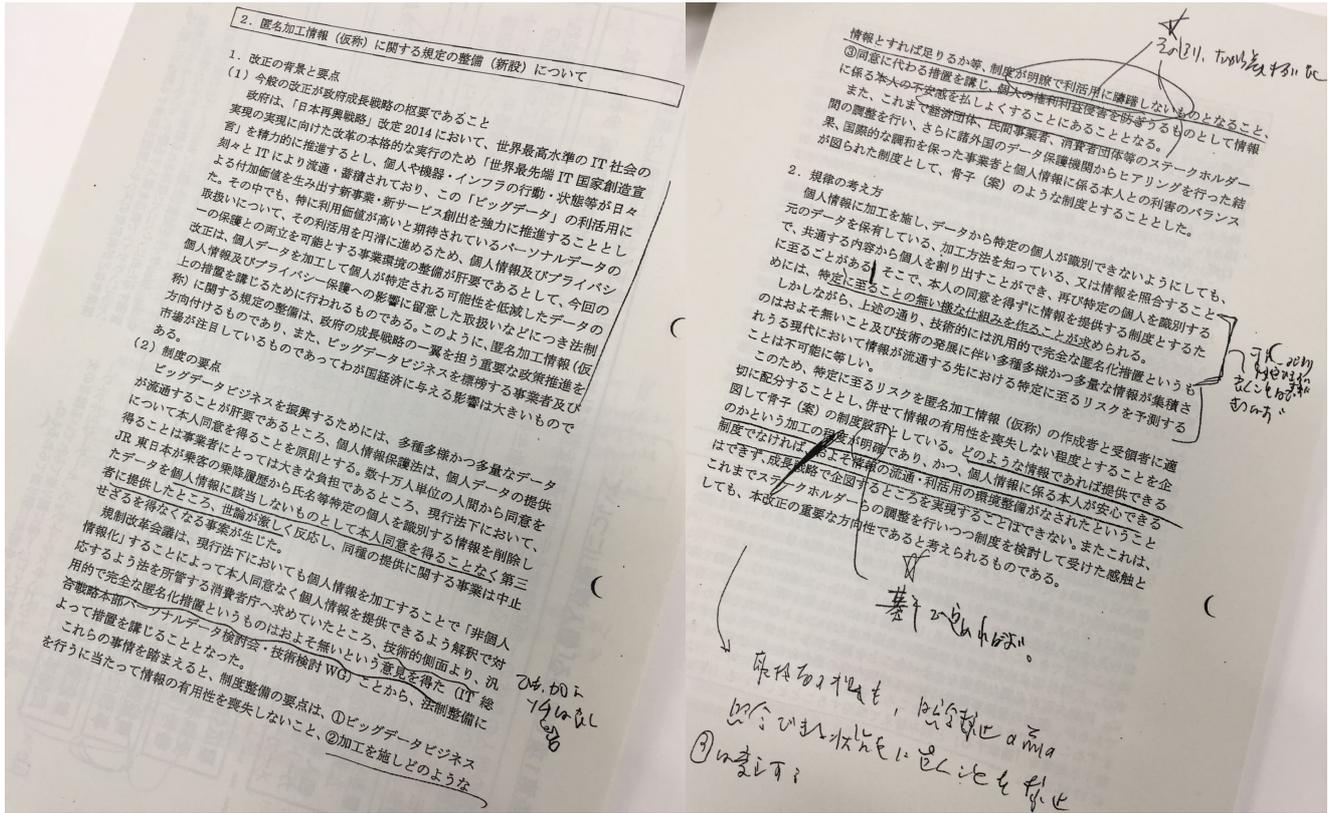
長官御指摘事項 (12/16)

匿名加工情報の加工は、その情報から個人情報が辿れないことが重要。そこで、「容易に」ではなく、「復元ができないように」とすること。漏洩防止は、加工とは別途記載することにして、「その他の復元を可能とする情報」は、復元ができると強調しているようなのでやめること。

なお、条文審査の時でよいが、1 (2) の書面は、カードなどが読めるように、また、書面上に記載されずに電磁的に記録されるものが読めるように工夫すること。

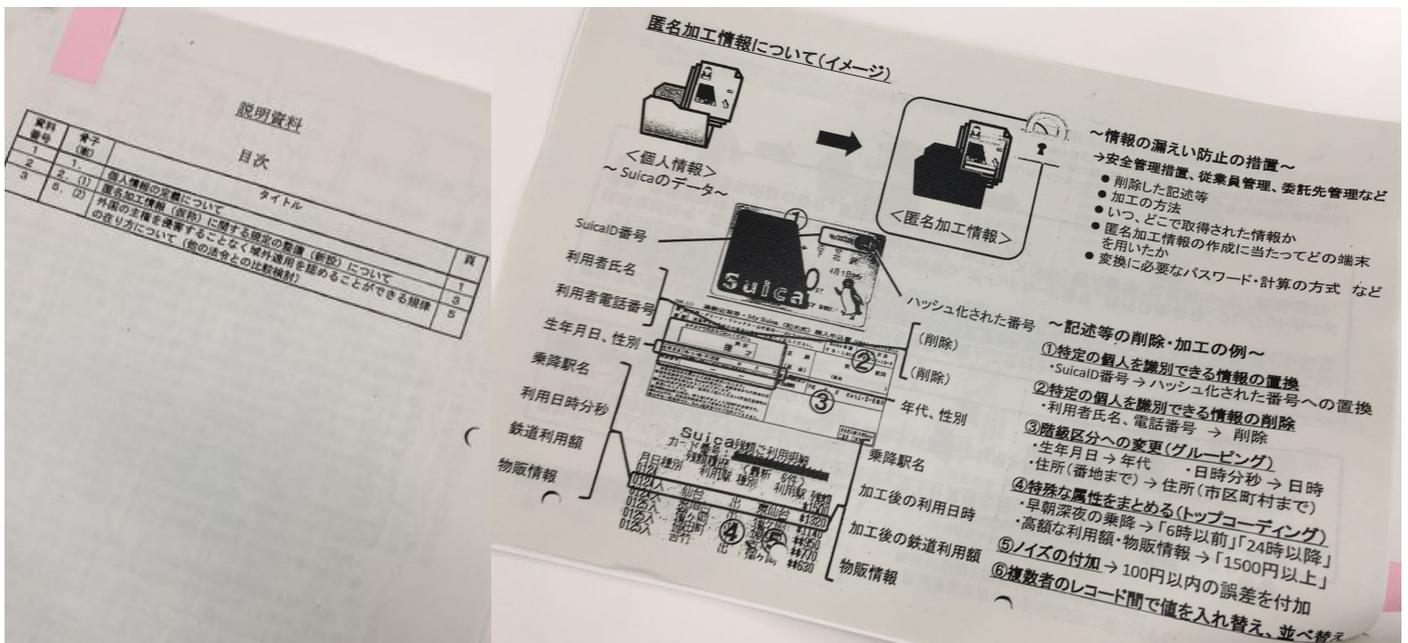


長官指摘後の再整理 (新案)



長官指摘後に作成された資料

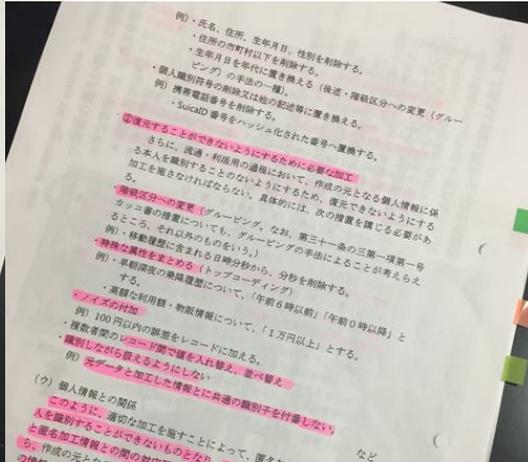
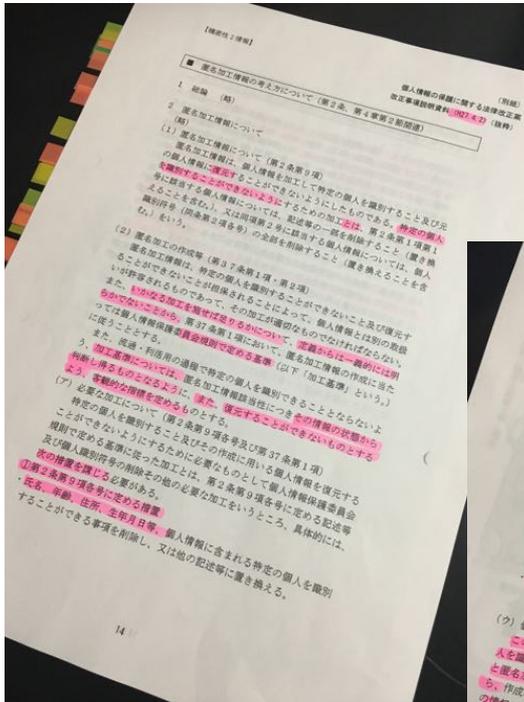
- ③～⑥の加工方法は長官指摘前には想定していなかった
- ③グルーピング、④トップコーディング、⑤ノイズの付加、⑥値を入れ替え・並べ替え



後の説明資料

● 2015年4月2日「改正事項説明資料（抜粋）」

- 「①2条9項各号に定める措置」として、記述等の削除等と個人識別符号の削除等だけが記載
- 「②復元することができないようにするために必要な加工」として、「グルーピング、トップコーディング、ノイズの付加、並べ替え」が記載



- 1号措置が「一部を削除」となっていて「全部又は一部を削除」となっていないのは、①の想定で定めたからではないか

- 5号基準による加工が記述等の全部を置き換える必要がある場合、1号措置に該当しないものというようになってしまう件

加工措置と加工基準の対応関係

長官指摘前

匿名加工情報定義 2014年10月24日案

生存する個人に関する情報であって、次の各号に掲げる個人情報に当該各号に定める措置を講じて得られるもの（…）及び…ものをいう。

1号措置

氏名、生年月日その他の記述等の全部又は一部を削除すること（他の情報に置き換えることを含む。）により、特定の個人を識別することができないようにすること。

2号措置

個人識別情報を全部削除すること（他の情報に置き換えることを含む。）

3号措置なし

3号個人情報単体はそのまま加工せずとも匿名加工情報となる

1号基準

特定の個人を識別することができる記述等の全部又は一部を削除…

2号基準

個人識別符号の全部を削除すること（…置き換えることを含む。）

3号基準

措置を講じて得られる情報とを連結する符号…を削除すること（…

4号基準

特異な記述等を削除すること（…置き換えることを含む。）

5号基準

…を構成する他の個人情報に含まれる記述等との差異その他の…

長官指摘後

匿名加工情報定義 2015年1月26日案

個人情報を加工して得られる個人に関する情報であって、次の各号に掲げる当該個人情報に当該各号に定める措置を講じて特定の個人を識別することができないようにし、かつ、当該個人情報を復元することができないようにしたものをいう。

特定の個人を識別することができないようにする措置

1号措置

当該個人情報に含まれる記述等の一部を削除すること（他の記述等に置き換えることを含む。）

2号措置

当該個人情報に含まれる個人識別符号の全部を削除すること（他の記述等に置き換えることを含む。）

復元することができないようにすること

施行規則19条 2016年10月

法第36条第1項の個人情報保護委員会規則で定める基準は、次のとおりとする。

1号基準

特定の個人を識別することができる記述等の全部又は一部を削除…

2号基準

個人識別符号の全部を削除すること（…置き換えることを含む。）

3号基準

措置を講じて得られる情報とを連結する符号…を削除すること（…

4号基準

特異な記述等を削除すること（…置き換えることを含む。）

5号基準

…を構成する他の個人情報に含まれる記述等との差異その他の…

改正趣旨説明の変遷

- 長官指摘前の案では
 - 改正前では、元データとの容易照合性により、氏名等を削除しても依然として個人情報であるため、提供できないところ、改正により、再識別禁止の義務を課すので、容易に照合することはできないこととなり、匿名加工情報に加工すれば法律上、非個人情報ということになる……というような説明
- 成立した改正法では
 - 匿名加工情報は、特定の個人を識別できないように、かつ、元の情報に復元できないように加工したものであるから、基本的には非個人情報であるが、完全にそのように加工することは困難なところ、再識別禁止の義務も課されるのでこれと相まって、非個人情報ということになる……というような説明

ボツ案の説明文書に基づく誤解説

- 宇賀逐条解説5版（前掲）の説明はボツ案ベース
 - ボツになった旧案の説明資料（2014年11月）を下地にして書かれている（比べるとそっくり）
 - だから「復元できないように」の説明がない
- 第二東京弁護士会編「Q&A改正個人情報保護法」（新日本法規, 2015年10月）
 - ボツ案ベースの説明
 - 情報公開請求した開示資料に基づくと明示されているが、法制局長官による「ひっくり返し」があったことは見抜けなかったもよう
- 他の解説書は……
 - この論点に踏み込まず何も言っていない

依然はっきりしない点

- 「各号に定める措置を講じて」はどこまでに掛かる？

9 この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であつて、当該個人情報を復元することができないようにしたものをいう。

- **α解釈** (前掲の図)

- 「復元することができないように」は各号の措置とは独立の要求
 - 文理的にはこちらでは？ (前掲2015年4月2日付資料はこの前提で記載)
 - 施行規則19条4号・5号は「復元できないようにする」ことを求める

- **β解釈**

- 各号の措置は「復元することができないように」も求めている
 - 皆さん、こっちだと思ってなかった？
- 施行規則19条4号・5号は「特定の個人を識別することができないように」と「復元することができないように」の両方を求める

α解釈とβ解釈

α解釈の場合

匿名加工情報定義

個人情報を加工して得られる個人に関する情報であつて、次の各号に掲げる当該個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないようにし、かつ、当該個人情報を復元することができないようにしたものをいう。

特定の個人を識別することができないようにする措置

1号措置
当該個人情報に含まれる記述等の一部を削除すること (他の記述等に置き換えることを含む。)

2号措置
当該個人情報に含まれる個人識別符号の全部を削除すること (他の記述等に置き換えることを含む。)

復元することができないようにすること

施行規則19条

法第36条第1項の個人情報保護委員会規則で定める基準は、次のとおりとする。

1号基準
特定の個人を識別することができない記述等の全部又は一部を削除…

2号基準
個人識別符号の全部を削除すること (…置き換えることを含む。)

3号基準
措置を講じて得られる情報とを連結する符号…を削除すること (…

4号基準
特異な記述等を削除すること (…置き換えることを含む。)

5号基準
…を構成する他の個人情報に含まれる記述等との差異その他の…

β解釈の場合

匿名加工情報定義

個人情報を加工して得られる個人に関する情報であつて、次の各号に掲げる当該個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないようにし、かつ、当該個人情報を復元することができないようにしたものをいう。

1号措置
当該個人情報に含まれる記述等の一部を削除すること (他の記述等に置き換えることを含む。)

2号措置
当該個人情報に含まれる個人識別符号の全部を削除すること (他の記述等に置き換えることを含む。)

施行規則19条

法第36条第1項の個人情報保護委員会規則で定める基準は、次のとおりとする。

1号基準
特定の個人を識別することができない記述等の全部又は一部を削除…

2号基準
個人識別符号の全部を削除すること (…置き換えることを含む。)

3号基準
措置を講じて得られる情報とを連結する符号…を削除すること (…

4号基準
特異な記述等を削除すること (…置き換えることを含む。)

5号基準
…を構成する他の個人情報に含まれる記述等との差異その他の…

照合による識別を含まないのか

- この「特定の個人を識別することができないように」の「識別」は容易照合による識別を含まないのか

9 この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であつて、当該個人情報を復元することができないようにしたものをいう。

- 括弧書省略説
 - 規則19条5号は元データと容易照合できなくすることを求める
 - β 解釈と整合的
 - α 解釈なら、規則19条5号は容易照合できなくすることと復元できなくすることの両方を求めているということに
- 明示的非含意説
 - α 解釈と整合的
 - 規則19条5号は復元できなくすることのみを指す

行政機関法では

- 「特定の個人を識別できない」の明確化括弧書がある

8 この法律において「非識別加工情報」とは、次の各号に掲げる個人情報（…）の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができない（個人に関する情報について、当該個人に関する情報に含まれる記述等により、又は当該個人に関する情報が他の情報と照合することができる個人に関する情報である場合にあっては他の情報（当該個人に関する情報の全部又は一部を含む個人情報その他の個人情報保護委員会規則で定める情報を除く。）と照合することにより、特定の個人を識別することができないことをいう。…）ように個人情報を加工して得られる個人に関する情報であつて、当該個人情報を復元することができないようにしたものをいう。

- 記述等により OR 他の情報と照合することにより
- ここからの類推では基本法も括弧書省略説とするのが自然
 - ただし謎の括弧書がある

もう決めないといけない

- ここを曖昧にしている限り匿名加工基準は定まらない
- 括弧書省略説で行くしかないのでは
 - α 解釈か β 解釈かはどちらでもよい
 - 明示的非含意説で行くとしても、 α 解釈で結局は（ほぼ）同じことを求めることになる
 - 法制局長官指摘は、容易照合もできないようにと求めている
- 明示的非含意説で行きたい人々の言い分（推察）
 - 元データと「容易照合できなくする」要件は厳しすぎて、有用性を残す加工が不可能になる……とと思ってない？
 - 結局それは「容易照合」をどういうものとするか次第
 - 今から「容易照合」の解釈を確定させていけばいい話
 - これまでも曖昧なままで来ているのだから

容易照合の解釈

- 極端な解釈
 - どんな加工をしても元データと常に容易照合可能
 - Suica事案を例にデータセット照合説を採用した上で、解消できないから匿名加工情報制度により法的に容易照合性を無効化するとして立案されたのが、ボツとなった旧案
 - 技術的無理解又は政治的意図による悲観説
- k-匿名（全列QI）基準説
 - k-匿名性の指標を借りて、全列QIとして $k \geq 2$ としたとき非個人情報となるとした見解
 - 1個でも元データと1対1対応する要素が存在したら $k=1$ になってしまう
 - これは過剰な加工要件だといってよいのでは
- 提案したい解釈
 - ファイル単位でAとBがもっばら照合できることをいう

もっぱら照合できるとは

- もともと容易照合はファイル単位の照合を指していた
 - 昭和63年法からの伝統
 - 「当該行政機関が保有する他のファイル又は台帳その他のものと照合することにより識別できるものを含む」（初期案ではこうだった）
 - 過去の国会答弁でもそれに該当する例示により説明されており、要素である1つの個人情報単位での照合は問題にされていない
- ガイドラインQ&A Q1-15（旧経産省改Q14）も同旨
 - 事業者の各取扱部門が独自に取得した個人情報を取扱部門ごとに設置されているデータベースにそれぞれ別々に保管している場合において、ある取扱部門のデータベースと他の取扱部門のデータベースの双方を取り扱うことができないときには、「容易に照合することができ」（法第2条第1項）ないといえますか。（→ yes）
 - これも、ファイル単位でもっぱら照合できるのでなければ容易照合なしとした見解と言える

その意味での容易照合をなくす加工

- ノイズ付加、サンプリング、グルーピング……など
 - 元データ一意の全解消は必須ではない
 - 例えば、ランダムサンプリングでは、k-匿名指標でk=1になる確率が、そこそこあるし、ノイズ付加でも確率0ではない
- この解釈における容易照合性解消の実質的意義は何か
 - **当該個人の人格から切り離された情報となるということ**
 - 匿名加工情報定義中の「個人に関する情報であって」の「個人に関する情報」は個票（record）のことを指すが、もはや「架空の個人」に関する情報（record）となっているもの
 - ありふれた情報であれば、誰か具体的なある個人の情報ということにはもはやならない
 - 観測者の思い込みは問題としない（実際に元データ一意であっても）
 - 「ありふれた」の基準をどうする
 - 背景母集団における一意性は要考慮

同種の議論

- 情報公開法制定時の不開示情報としての個人情報
 - 部分開示規定
 - 「氏名、生年月日その他の特定の個人を識別することができることとなる記述等の部分を除くことにより、公にしても、個人の権利利益が害されるおそれがないと認められるときは、……」
 - 氏名等を削除すれば開示していいのか？
 - 「反省文」「カルテ」を例に、本人の人格に関わる情報であるから、開示することはできないとする意見が記録されている
 - 「誰のものかわからないからいいのでは」との意見に対して、「本人にとっては自分のものだわかる」という意見が出ていた
 - これをどう考えるか
 - 例えば、外性器の写真はどうか
 - 外部観測性がないから匿名加工情報ということでいいのか？
 - 本人には「俺のじゃないか」とわかる
 - 内臓の写真なら本人もわからないからいいのか？ ……。

数理的なモデルが必要

- だがまだやっていない

国際的整合性

- EU一般データ保護規則（GDPR）での匿名化
 - 「anonymous information」について前文26に記載あり
 - singling out = 一人ひとりを区別
 - determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, **such as singling out**, either by the controller or by another person to identify the natural person directly or indirectly.
 - 氏名等を削るだけは仮名化（pseudonymisation）であり、personal dataであるとされる
 - 「追加的な情報の利用によってある個人に属するものとなり得るものは、依然として識別可能な個人の情報とみなすべき」
 - 「Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person」
- 結果的に日本の匿名加工情報はEUの anonymous information 相当のものとなったのではないか
 - 仮名化しただけでは匿名加工情報にならないということ

残る問題

- 仮IDによる元データとの容易照合
 - 委員会事務局レポートは、仮IDを残して提供することを許容
 - ただし繰り返し提供するときは危ないから気をつけろと書かれている
 - 連結仮名化に該当、元データとの容易照合性があることに
 - EUでは、pseudonymised dataであり、モロにpersonal dataに該当
- 仮IDを残したいのか
 - 残したいが故に、明示的非含意説をいう人がいたのでは
- なぜ仮IDが残ったのか
 - ボツになった旧案では連結可能仮名化での提供を予定していたので、氏名や元IDのハッシュ化を想定していた
 - 法制局長官指摘でひっくり返ったときにこの点を気にしなかった様子
- 仮IDは不要では

以下は前回本シンポジウムからの再掲

仮ID問題

- 開示資料には鍵付きハッシュ関数によるIDの例がある
 - これは連結仮名化（連結可能匿名化）であり、消費者庁見解で言う「対応表」を残す場合に当たり、個人情報の提供であると言うべき

①～⑥の措置により、元の情報を復元することができない理由について

①について
 Suica番号に付加する符号(ソルト)が提供者において秘密に保管されていること、また、ハッシュ値から元の符号(Suica番号又はソルト)が推知できないことから、Suica番号を復元できないこととなるもの。

<Suica番号>	<ソルト>	ハッシュ化	<ハッシュ値>
JE305 1485 9840 2145 +	ut1h7r	あらかじめ定められた公知の計算手順に基づいて、元の符号を一定の符号(ハッシュ値)に置き換え	897a7e9fe9de73e42efb1e266d1749fc
JE307 7238 8212 5091 +	k3g6jt		ac3f07c8ffd225fc03d02f27f5c88918
JE305 1485 9840 2145 +	ut1h7r		897a7e9fe9de73e42efb1e266d1749fc

提供者において秘密に保管

※Suica番号のみをハッシュ化すると、取り得るハッシュ値を受領者がすべて事前に計算して照合できてしまうため、ソルトを提供者において秘密に保管し、ハッシュ化の際にこれをSuica番号に付加することで、受領者による事前の計算ができないようにするもの。
 ※同一のSuica番号(及び付加されたソルト)については常に同一のハッシュ値が出力されるもの(緑字部分)。

- ちなみにこれを「ソルト」と呼ぶのは暗号技術用語として誤り

事務局レポートでは

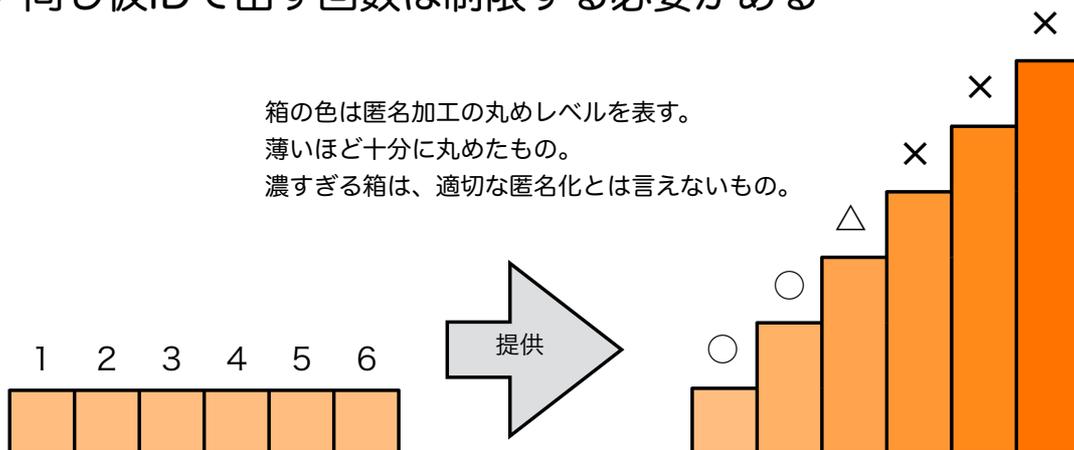
- 鍵付きハッシュ関数の鍵を残す方法を認めてしまった
 - 【ハッシュ関数による置き換えについて】
 - 「……ハッシュによる仮ID生成に当たっては、（氏名+秘密の文字列）、（氏名+電子メールアドレス+秘密の文字列）といったように、鍵となる秘密の文字列を付加した上でハッシュ化をすること（いわゆる鍵付きハッシュ関数の利用）が望ましい²⁴。」
 - このハッシュID（仮ID）を付けたまま匿名加工情報取扱事業者に提供することを認めてしまっている
 - 消費者庁見解に反し、違法な個人データの提供では？
 - 照合禁止義務により容易照合性が消えるとする解釈をとるのは、内閣法制局長官の指摘を無視しているのでは？
- そもそも仮IDなんて要らないのでは？
 - 作成段階で何らかの仮IDが技術的に必要なのは理解できるが、提供時に残して提供する必要性は何か

仮IDのリスクは散々議論されてきた

- 経産省「匿名加工マニュアル」での議論
 - 仮IDをそのまま残して提供する案に対して、有識者が反発
- NIIの有識者WG報告書（2017年2月21日）
 - (ウ) 同一事業者複数回提供・複数事業者提供
 - 「同一の本人に同じ仮IDを付して同一の提供先に複数回提供する場合には、当該提供先において当該本人に関する情報が順次累積されることを考慮して、2回目以降の加工を行うべきである。」
- 委員会の事務局レポートでは
 - 【仮IDへの置き換えについて】
 - 「また、同じ事業者に複数回にわたって匿名加工情報を提供する場合は、同一の人物の情報が蓄積され続けることにより、元の個人情報に係る本人を識別できるリスクが高くなることも想定される。したがって、同一事業者への提供であっても、定期的に仮IDを変更することが望ましい。
なお、仮IDが不要である場合には、再識別リスクを低減する意味からも、仮IDへの置き換えを行わないことが望ましい。」

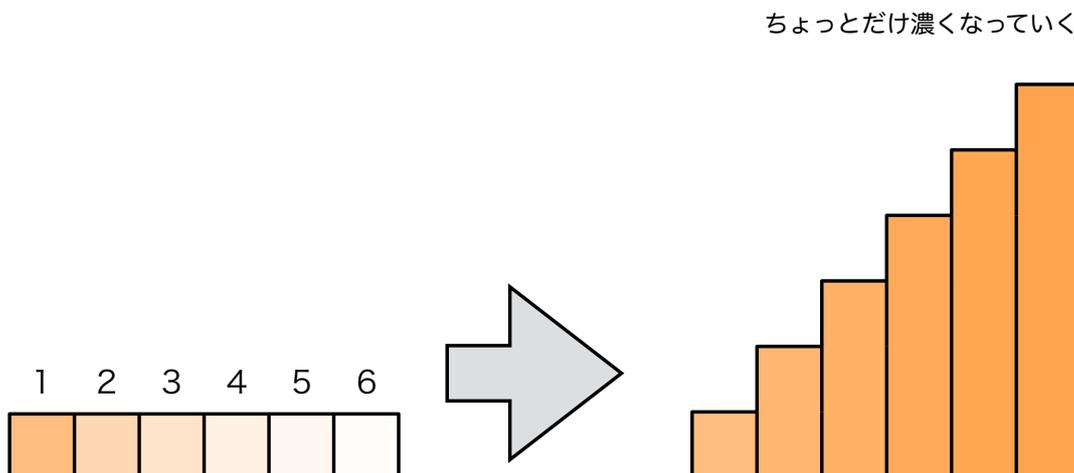
仮ID運用の悪い例

- 同じ仮IDで繰り返し提供すると
 - 受領者側で蓄積されて再識別リスクが高まる
 - 1回目の提供時に適切なレベルで丸めた匿名加工をしたとして
 - 2回目の提供時に同じレベルで丸めた匿名加工をすると、受領者側で両者を合成したものが、適切なレベルの匿名加工とは限らなくなる。
 - 同じ仮IDで出す回数は制限する必要がある



対策した例（無計画な場合）

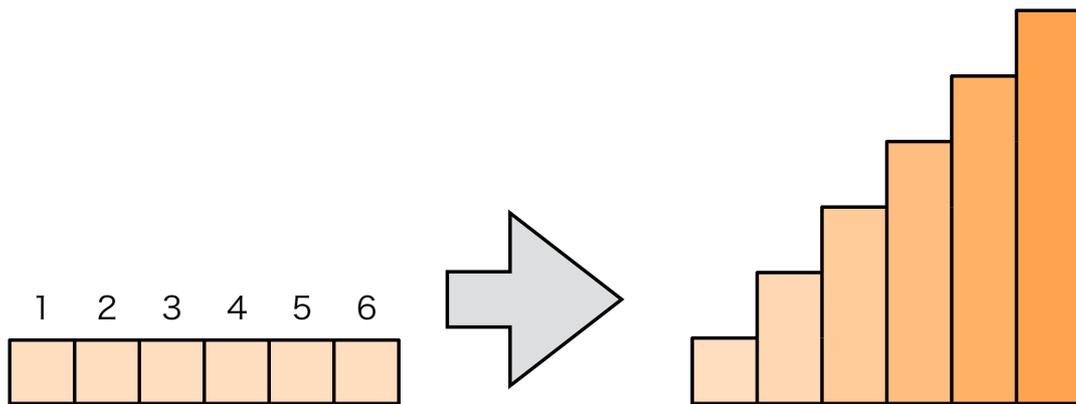
- 同じ仮IDで繰り返し提供するなら
 - 2回目以降は、どんどん薄めていく（丸めレベルを高めていく）必要がある
 - 前掲NII報告書が指摘しているのはこれ



対策した例（計画的な例）

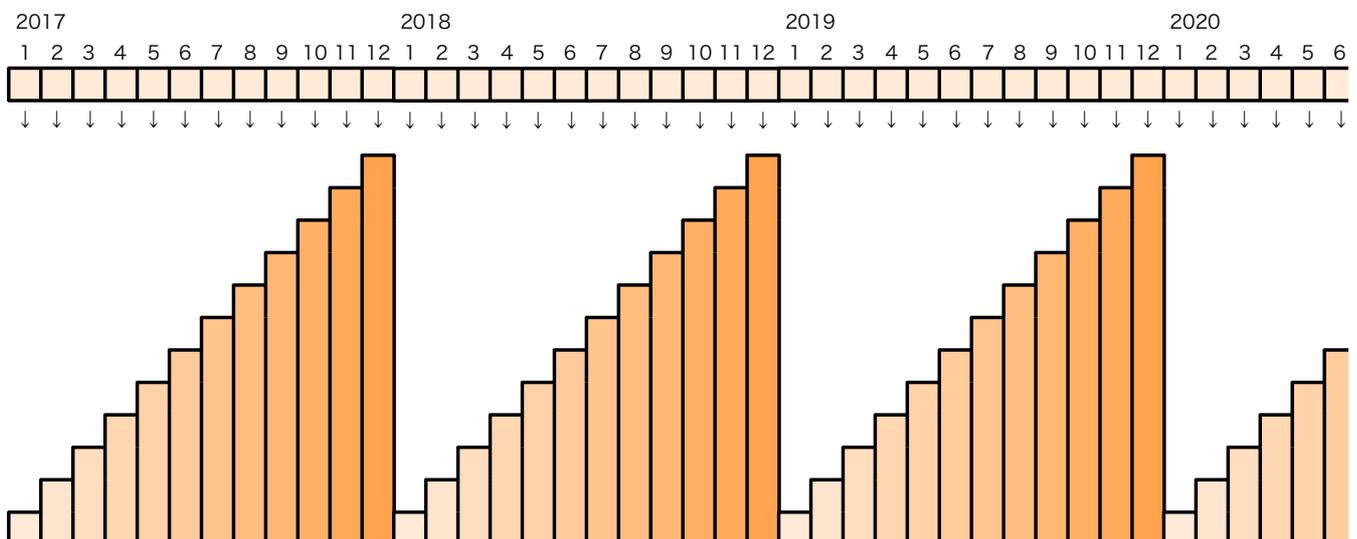
- 同じ仮IDで繰り返し提供するなら
 - 提供回数を事前に決めて、最終的に蓄積されたものが合成されたときに、適切な丸めレベルとなるよう、初めから十分に丸めた匿名加工をして提供する。

最終回で最大限に濃いデータを得たい
 （その前の段階でも、できた分から早めに、できることなら得たい）



連続して得たい？

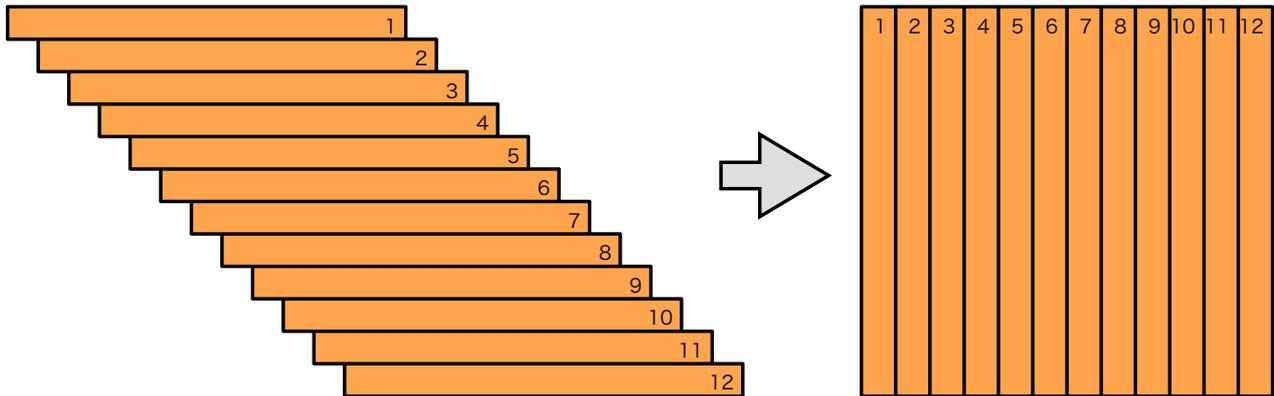
- 月次レポートを延々得たい場合
 - 仮IDを定期的にはリセットする？
 - 例えば毎年リセットする場合



連続して得たい場合

- 毎月、過去1年分のデータを最適に匿名加工して、仮IDなしで提供すればよいただけの話
 - 仮IDは要らない！（毎回リセット、対応表保管せず）

繰り返し用いられる共通のIDがないので蓄積されない



ただし、履歴データ自体によるマッチングが可能とならないように、加工する必要あり