別紙 1

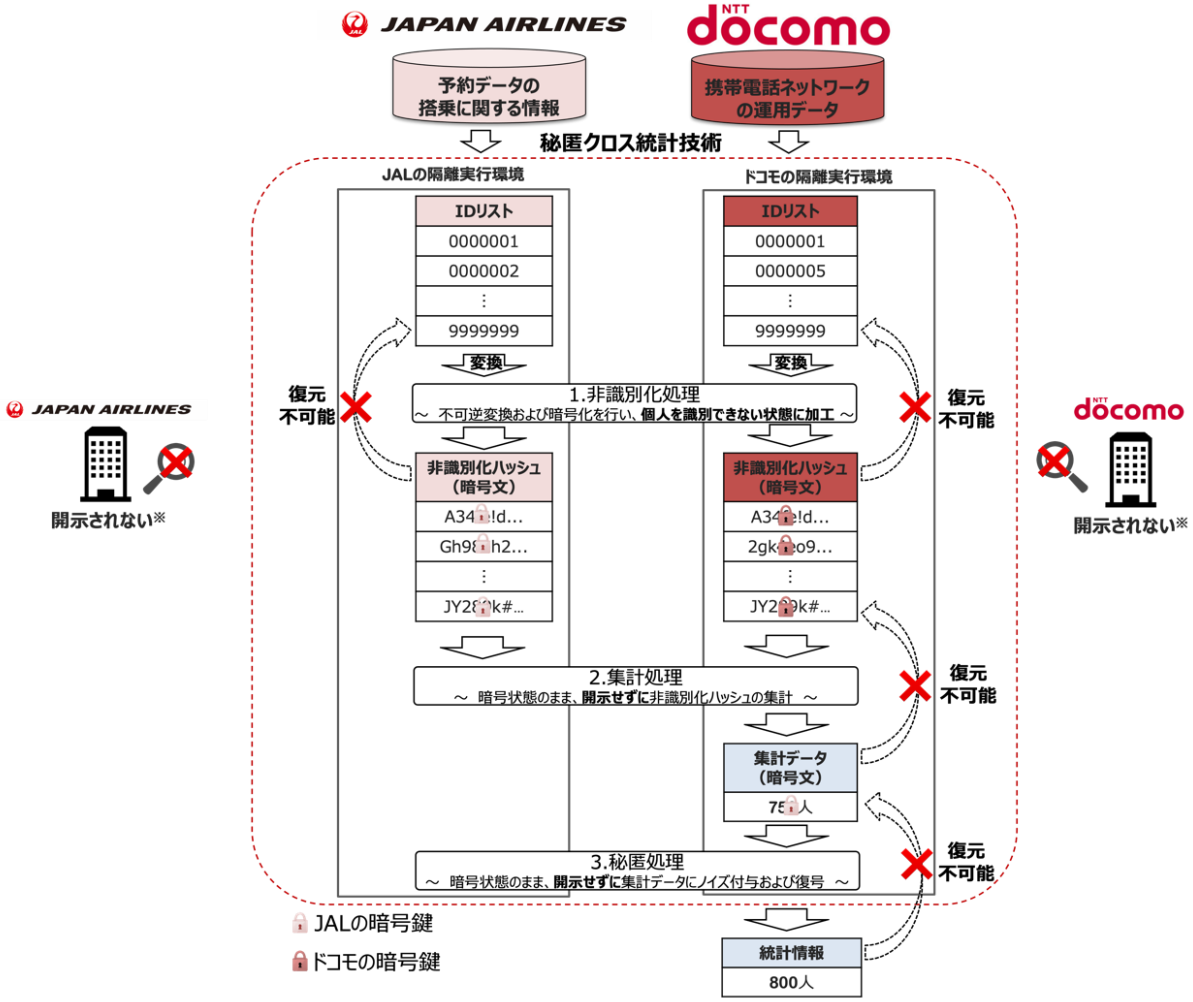
「秘匿クロス統計技術」の概要

概要

秘匿クロス統計技術は、相互にデータが開示されない状態で安全な統計情報を作成することを可能にする、NTT グループが推進する次世代 ICT 基盤構想「IOWN®」の構成技術です。本実証実験では、本技術を用いて、JAL、ドコモが、各社が保有する同じ形式の ID リストをそれぞれの安全な処理環境（隔離実行環境）で、非識別化処理（不可逆変換および暗号化）により、個人を識別できない状態に加工したうえで、暗号状態のまま集計処理と秘匿処理を実施します。

この統計情報は、集団の人数のみをあらわす人口統計情報であり、作成される統計情報以外の情報は JAL、JAL カード、ドコモのいずれも確認することはできません。
本技術の安全性は、NTT 社会情報研究所の研究成果である高速・安全なデータ結合処理技術※1 に加えて、ドコモが保有する差分プライバシー※2 に基づくプライバシー保護技術を併用することで実現しています。

本技術は、「モバイル空間統計」のガイドラインに準拠しており、非識別化処理、集計処理、秘匿処理を通じて統計情報を作成します。また、モバイル空間統計ガイドラインの中でご案内している「運用データ利用停止手続き」を行っているお客さまのデータは、本実証実験において利用しません。



※開示されないとは、一連の処理を人の目に触れることなく機械が行なうことを保証することを指す

本実証実験における秘匿クロス統計技術の処理の流れ

※1 データを暗号化したまま処理できる暗号方式（準同型暗号）を応用し、複数の主体が各々持つデータを互いに開示せずに、データ結合処理と統計情報の作成を行う技術です。

※2 特定の背景知識や攻撃能力をもつ攻撃者に対しても安全性を保証できることを目的として作成されたプライバシー保護の強度を定量的に測る指標です。なお、米国国勢調査においても、「差分プライバシー」を用いた保護手法が採用されています。

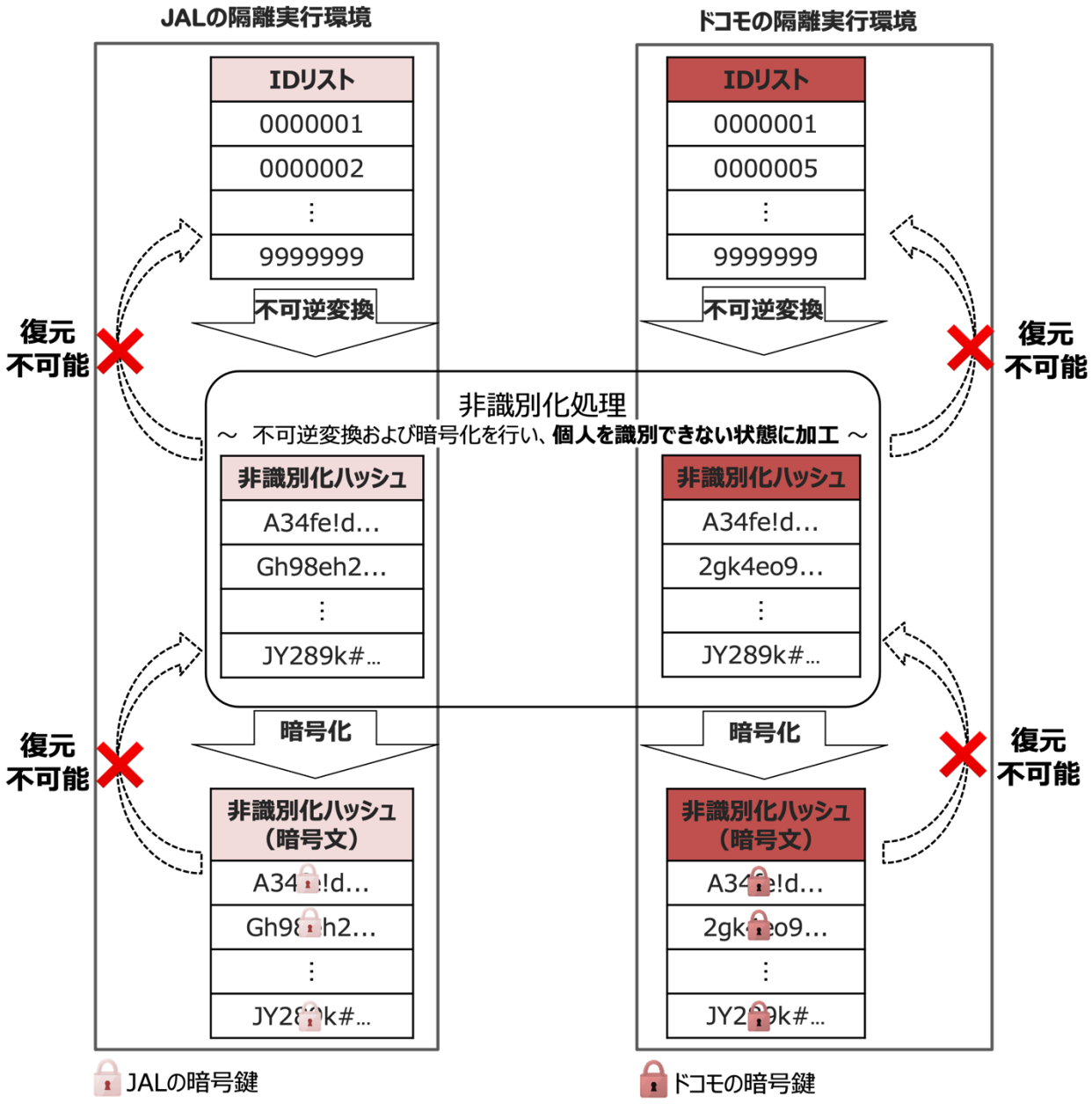
*「IOWN®」は、日本電信電話株式会社の商標又は登録商標です。

別紙 2

「秘匿クロス統計技術」における各種処理

1. 非識別化処理

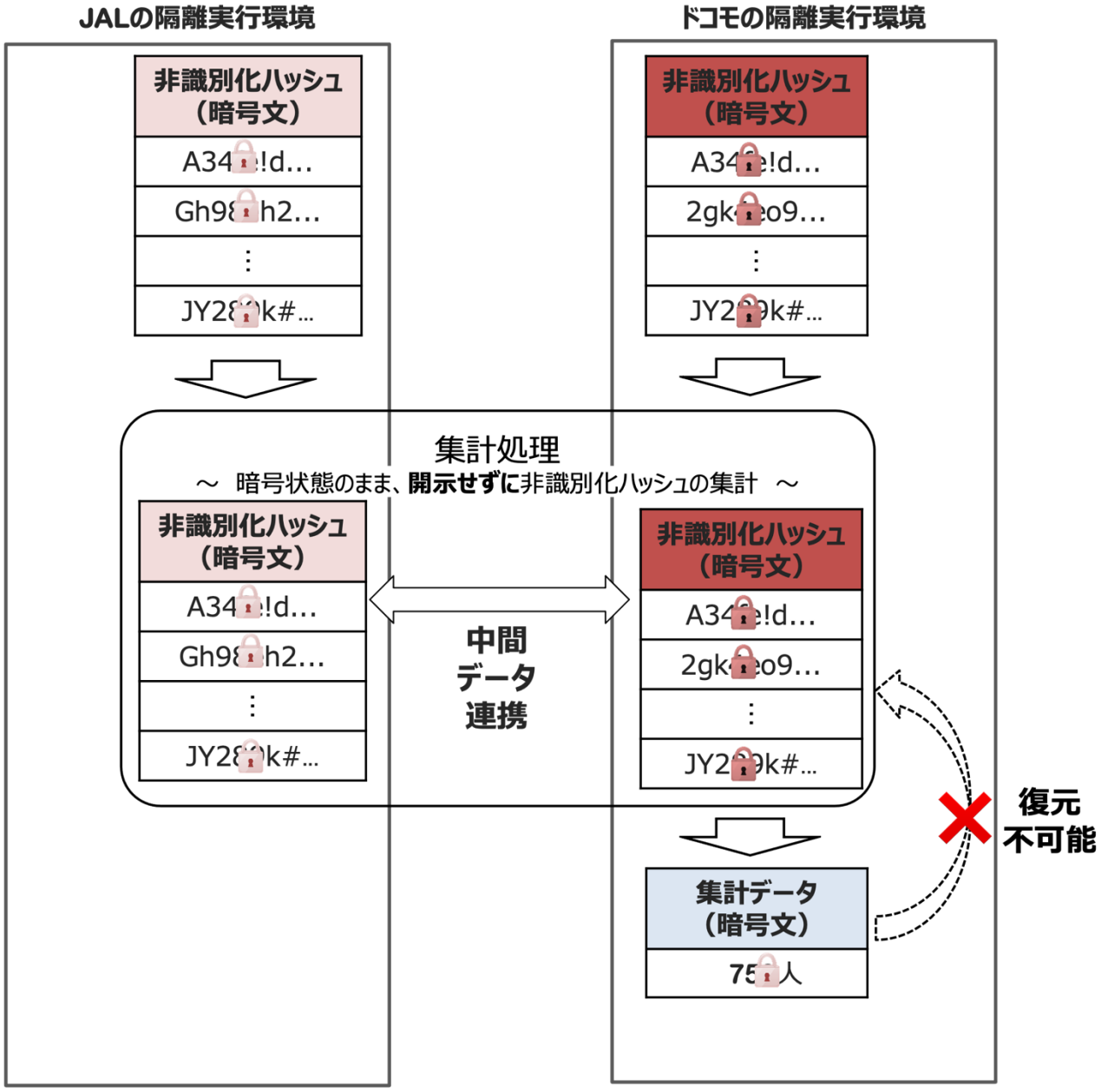
各社が保有する ID を不可逆変換し、非識別化ハッシュを得ます。不可逆変換では非識別化ハッシュからの ID の復元を防止するため、ID にソルト（乱数）を付与し、一方向関数により非識別化ハッシュを得た後、ソルトの破棄を技術的に保証します。その後、各社のそれぞれの暗号鍵で、非識別化ハッシュの暗号化を行います。以上の処理により、各社のデータを集計する前の時点でも、データを保有する各社自身でも不可逆に個人を識別できない状態になります。



2. 集計処理

非識別化処理の段階で施された暗号状態のまま、両者の共通する非識別化ハッシュ（暗号文）の個数を集計し、集計データ（暗号文）を得ます。非識別化ハッシュ（暗号文）および集計データ（暗号文）は各社それぞれの暗号鍵により暗号化されているため、集計処理の途中で集計相手のデータが開示されることはありません。

なお、集計データには非識別化ハッシュを含みません。また、集計データから非識別化ハッシュの復元は不可能となります。



3. 秘匿処理

集計処理で得られた集計データ（暗号文）に暗号状態のまま、差分プライバシーに基づくノイズ（暗号文）を付与した上で復号し、統計情報を得ます。この統計情報は集団の人数のみをあらわす人口統計情報であり、お客さま個人を特定することはできません。