資料5

NTT

Innovative R&D by NTT

調査票情報等の二次的利用における秘密分散・計算技術の適用可能性

2018年1月24日

NTTセキュアプラットフォーム研究所

1. NTTの秘密計算技術・システムのご紹介

秘密計算とは

Innovative R&D by NTT

**データを秘密に（暗号化）した状態のまま、
各種計算（含、統計値算出）できるセキュリティ技術**

データ所有者

機密データ

年齢	性別	身長	体重
57	男	154.8	71.7
45	男	179.9	70
53	女	156.3	51.1
77	男	169.2	63
59	男	175.2	67.1

データ登録

秘密計算システム

意味のないデータに変換して保管

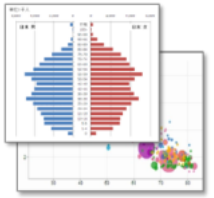
年齢	性別	身長	体重
oeiaIJ30fe	3rjaU($hj	JP"(Rh3h	JU#$H(h
fek3)j3pa	j3aj)H"op	Mj3i8Y$h	J"IY#HO!
fkap039K	3j32IHO"	j("h2Z8H"	jri3hr8"IU
kfea0o23	U#(Jd39	aQjDP"(H	jI#O"(DH
fk3o3494	j3(")D"H	(hjd2oh(	j3"(h2ho

元データを復元せずに計算

計算要望

計算結果

データ利用者



統計データ

データ登録者以外は
元データを知ることなく
分析結果を得られる

【比較】通常の暗号化の場合

機密データ

年齢	性別	身長	体重
57	男	154.8	71.7
45	男	179.9	70
53	女	156.3	51.1
77	男	169.2	63
59	男	175.2	67.1

データ登録（暗号化）

機密データ（暗号化）

年齢	性別	身長	体重
oeiaIJ30fe	3rjaU($hj	JP"(Rh3h	JU#$H(h
fek3)j3pa	j3aj)H"op	Mj3i8Y$h	J"IY#HO!
fkap039K	3j32IHO"	j("h2Z8H"	jri3hr8"IU
kfea0o23	U#(Jd39	aQjDP"(H	jI#O"(DH
fk3o3494	j3(")D"H	(hjd2oh(	j3"(h2ho

復号

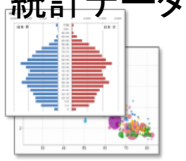
機密データ

年齢	性別	身長	体重
57	男	154.8	71.7
45	男	179.9	70
53	女	156.3	51.1
77	男	9.2	63
59		.2	67.1

計算

計算結果

統計データ



計算のために
元データを復元

データ漏洩のリスク有

NTT

NTTの秘密計算システム（データ保管）

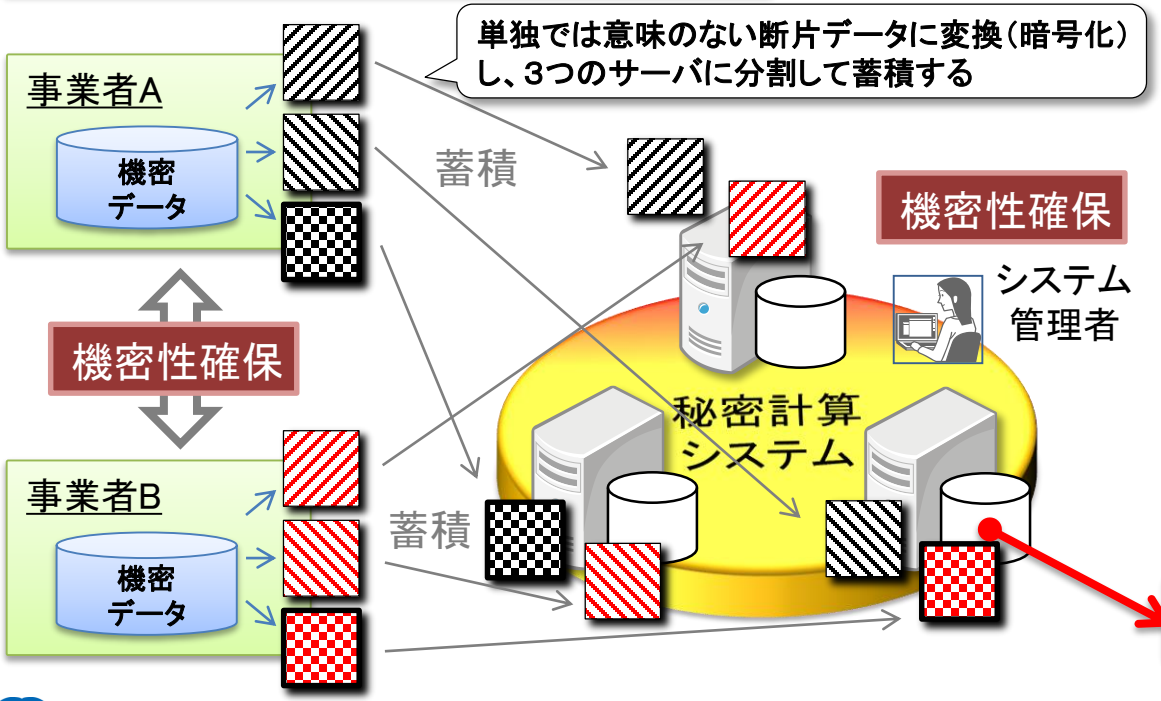
Innovative R&D by NTT

データを単独では意味のない複数の断片データに変換する秘密分散技術（ISO国際規格※準拠）を採用し、機密性と可用性の高いデータ保管を実現

《機密性》1つ1つの断片データからは元データの復元が一切不可能

《可用性》災害等で1つの断片データを失っても、残りの断片データから失った断片データを再現することが可能

事業者（機密データ保有者）



鍵を用いた暗号化と比べると・・・

✓ **高い安全性を継続**

計算機性能の向上や暗号解読技術の進歩により安全性が損なわれることがないようにデータを保管

✓ **鍵の漏洩リスクゼロ**

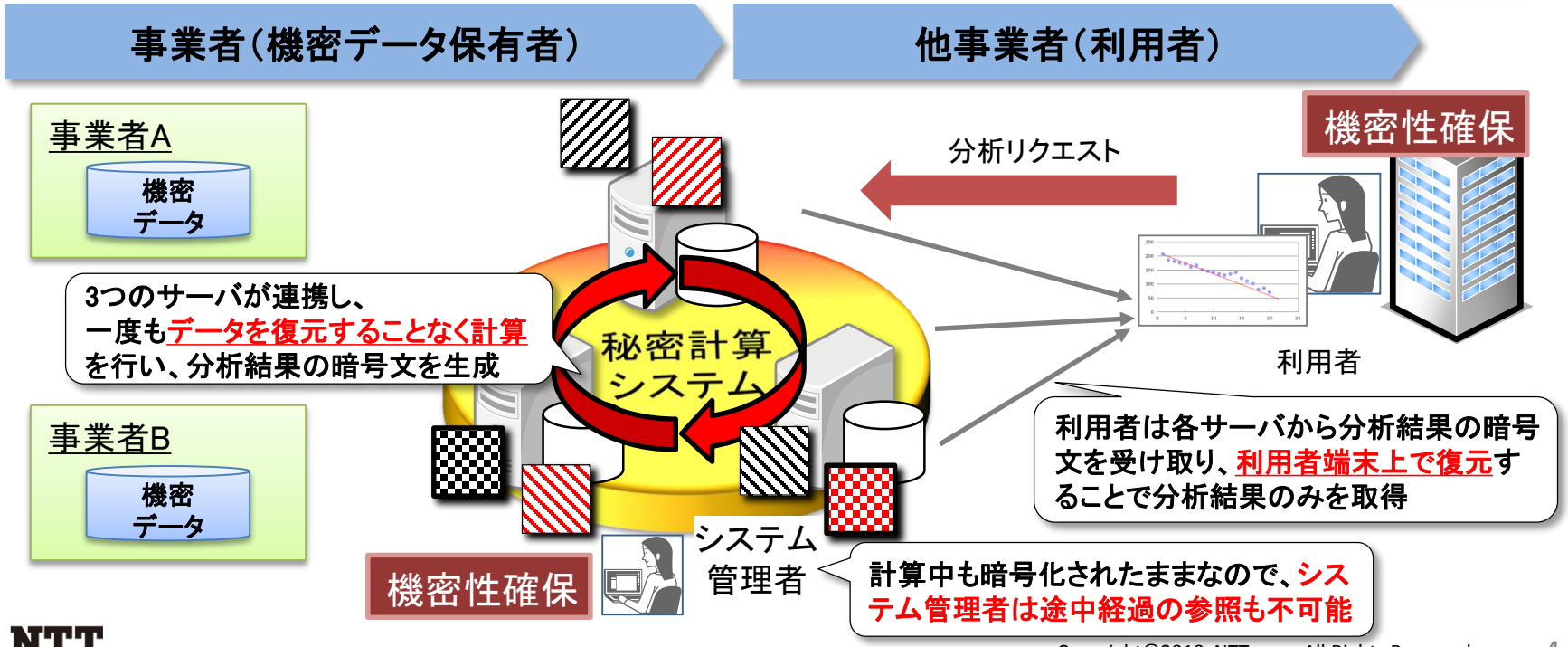
鍵管理が不要であるため、鍵の漏洩による暗号解読リスクがなく、運用の手間を削減できる

※ISO/IEC: 19592-2 “Information technology -- Security techniques -- Secret sharing -- Part 2: Fundamental mechanisms”（ISO/IEC JTC 1/SC 27/WG 2発行）

NTTの秘密計算システム（データ分析）

一度もデータを復元せずに計算し、元データの機密性を確保したまま分析

- 秘密計算の課題であった**処理速度を劇的に向上（世界最速）**
- **世界トップレベルのデータ件数を実用的な時間内で取り扱い可能**
- **汎用的な集計・基本統計演算機能**を有し、統計解析ソフト’R’のI/Fから利用可能（他のI/Fもご要望に応じて追加可能）
- **複数の登録データを暗号化したまま統合（Append）や結合（Join）する機能**とマルチテナント対応により、保有者の異なるデータの安全な統合分析が可能



2. 調査票情報等の二次的利用における秘密分散・計算技術の適用可能性

調査票情報の二次的利用

国民・企業の情報管理意識が高まっている中、調査客体の信頼性を確保しつつ、調査票情報等の提供及び活用の要望に柔軟に対応していくに当たっては、よりセキュアな環境において、調査票情報等の有効活用に取り組む必要がある。

「公的統計の整備に関する基本的な計画」の変更に係る答申（平成29年12月19日） ３統計の利活用促進・環境改善 (1)調査票情報等の提供及び活用の推進 より抜粋

現在

調査票（個票）情報

○高度な公益性	○学術目的　○高等教育	
調査票情報の提供	オーダーメード集計	匿名データ

受領形態	電子媒体	オンサイト
提供先	行政機関等	研究者

今後の可能性

①管理するデータの増加
　⇒ **管理業務のアウトソーシング、クラウド利用**による自己管理設備のスリム化
②二次的利用の利用件数の増加
　⇒ 提供元・提供先双方の**申請処理の効率化・負荷軽減**が必要
③提供先や提供形態（リモートサイトアクセス、オンデマンド集計等）の拡大
　⇒ 提供先・形態に合わせた**適切なセキュリティ対策**が必要
④調査票情報と他のデータ（行政記録情報や民間ビッグデータ等）との統合分析
　⇒ 重要データの**秘匿とデータ統合の両立**が必要

秘密計算の適用可能性

秘密計算の「データを暗号化して保存・処理」や「元データ（個票）を参照不可」という特徴を利用し二次的利用に貢献

将来図(可能性)