\Orchestrating a brighter world

NEC

秘密計算のPWS2018での議論と最近の動向

NEC セキュリティ研究所
竹之内隆夫

2019年3月7日 PWS Meetup@明治大学

© NEC Corporation 2019

はじめに

本日の発表の趣旨

- 匿名加工情報では実現できない複数組織でのデータ結合を秘密計算技術で安全に実現できるのでは？

CSS/PWS2018@長野にて、秘密計算技術を用いたセキュアなデータ結合に関する企画セッションを実施

- 新潟大学 須川先生（座長）
- 宮内・水町 IT法律事務所 宮内先生
- NTT 藤村さん
- 日立コンサルティング 美馬さん
- **NEC 竹之内**

CSS/PWS2018でのセッション内容の振り返りつつ、
最近の議論動向を説明

© NEC Corporation 2019

目次

PWS2018の議論

１．秘密計算への期待（私見）

組織間での個人データの安全な共有への期待

個人に関するデータを組織間で結合・分析することは、社会的な価値を創出できると期待されているが、プライバシ等の課題が存在

データの共有分析による価値創出

- 例：米国の医療は、病院・介護者・製薬会社などがデータを共有して活用できれば、**毎年3000億ドル以上**の価値を生み出せる。[1][2]

データ共有の狙い	創出価値(億ドル)
生活習慣の改善	700-1000
医療・介護の連携	900-1100
最適な医療の選定	500-700
費用対効果の検証	500-1000
創薬・実証の加速	400-700
合計	3000-4500

データ共有の主な阻害要因

1. 個人のプライバシー保護：
   個人の同意なく、個人情報の**第三者への提供は禁止(違法)**

2. 競争力の源泉になる秘密情報：
   企業や研究機関は、データを**競合に開示するのを嫌う**

[1] McKinsey Global Institute, *Big data: The next frontier for innovation, competition, and productivity*, 2011年5月

[2] McKinsey Global Institute, *The 'big data' revolution in healthcare — Accelerating value and innovation*, 2013年1月. Exhibit 4.

© NEC Corporation 2019

安全なデータ結合分析による社会課題解決

組織間での安全なデータ流通を「技術」と「制度」で実現し、様々な社会課題を解決

疾病と運動の
相関分析による
予防医療

ヘルスケア分野

観光客の行動と購買
傾向分析による
おもてなし

観光分野

金融情報の
結合分析による
不正送金検知

金融分野

・・・・・

複数組織のデータを
結合した分析結果だけを提供

秘密計算技術

制度整備

複数組織の機密データを相互に開示せずに結合

投薬・疾病履歴、
ゲノム情報など

医療機関

運動量情報

ヘルスヘア企業

銀行残高
送金情報など

金融機関

位置情報
購買情報など

キャリア、ECサイトなど

・・・・・

© NEC Corporation 2019

2．秘密計算のユースケース・制度

PWS2018の各セッション概要と本発表の概要

- ①宮内先生：契約/制度を整理し、秘密計算が有用な場面を検討
  ⇒ 特に有用な場面は、組織間での個人データの結合・分析か

- ②藤村さん：個人データの組織間の結合における法制度の議論状況
  ⇒ 秘密計算等の技術を前提とした新制度を検討してもよいのでは？

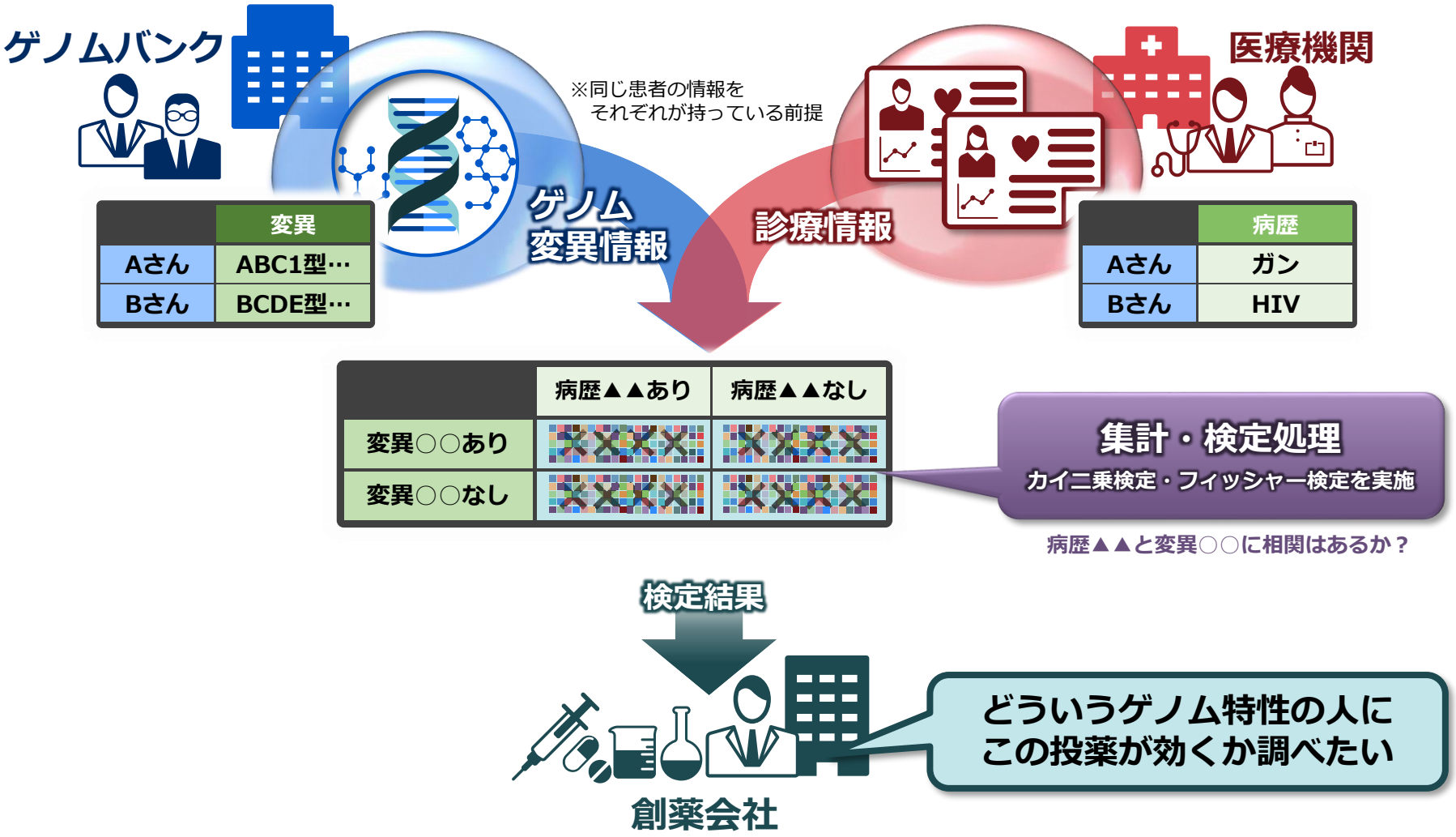
- ③美馬さん：韓国の事例（信頼のおける第3者を置くモデル）
  ⇒ 信頼のおける第3者機関のモデルで本当に良いのか？

- ④竹之内：秘密計算の技術・ユースケースなどを整理

© NEC Corporation 2019

【典型的ユースケース】１：１での個人レコードを結合した医学分析

複数の医療機関の同一人物のデータを結合して分析し、医学研究に活用

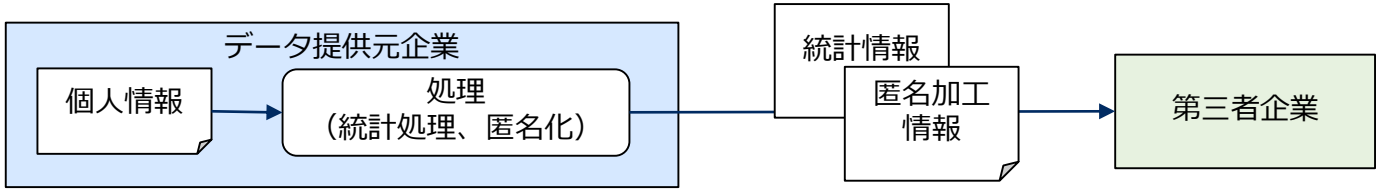


© NEC Corporation 2019

匿名化技術では不十分

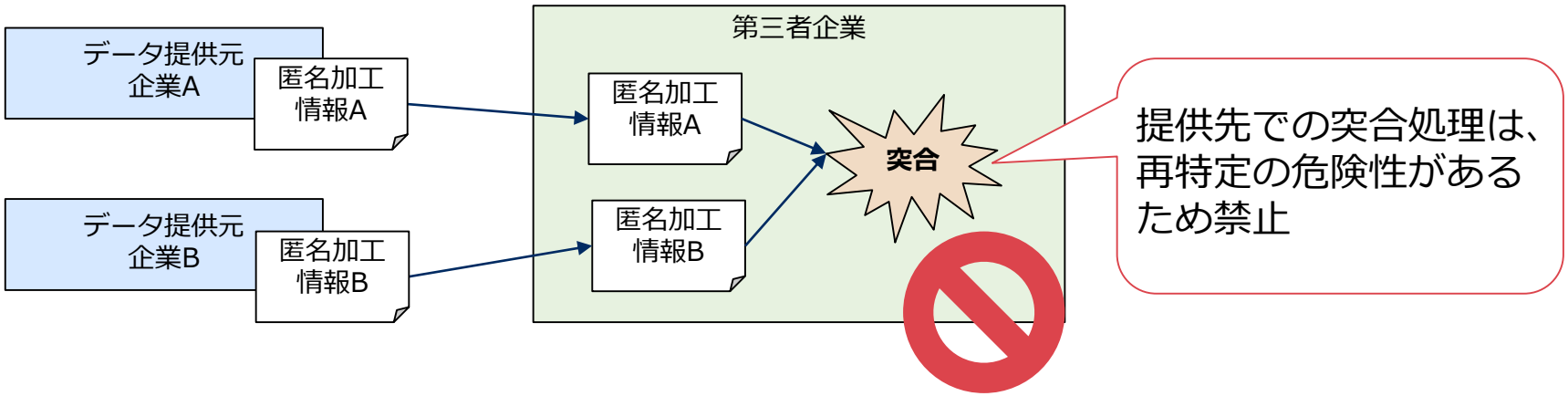
匿名化技術では、組織間でのデータ結合分析への対応は困難

匿名加工情報や統計情報であれば第三者企業へ提供可能
(匿名加工情報の場合は一定の条件がある※1)



※1: オプトアウトへの対応、提供先での突合処理の禁止、など

匿名化は、複数組織のデータを結合することは想定していない

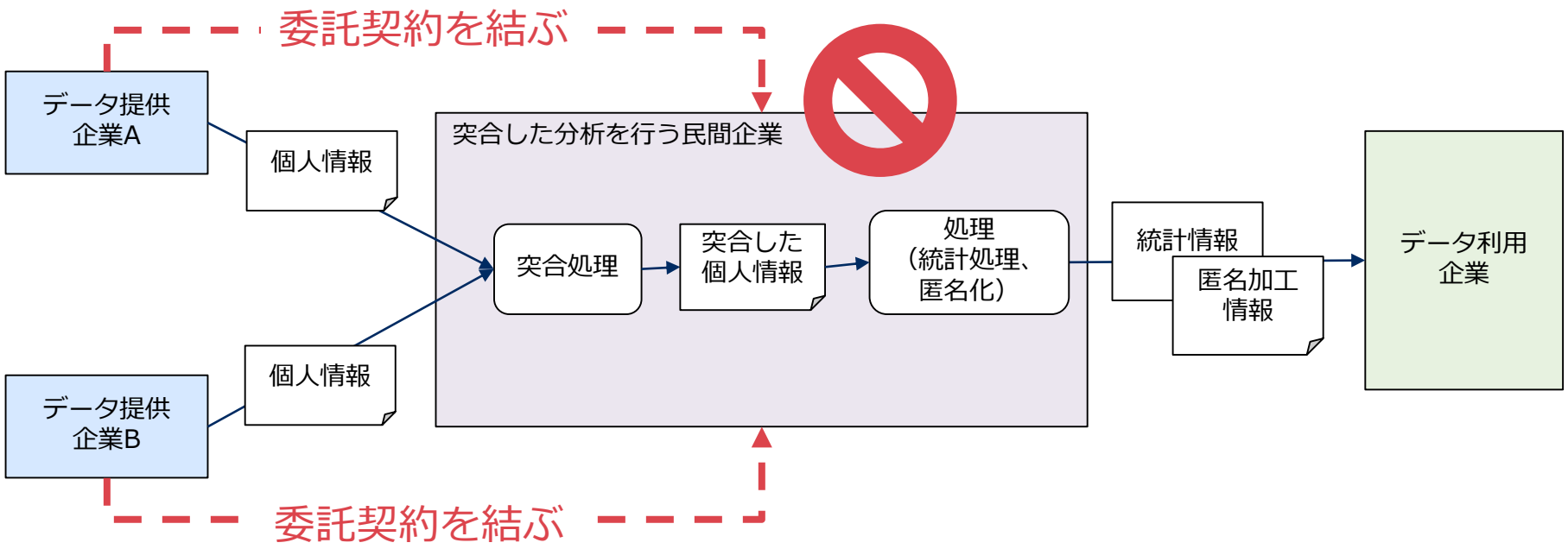


© NEC Corporation 2019

委託契約でもデータ結合は禁止

委託契約先で異なる委託元の個人情報を突合することは禁止

委託契約先で突合処理は禁止

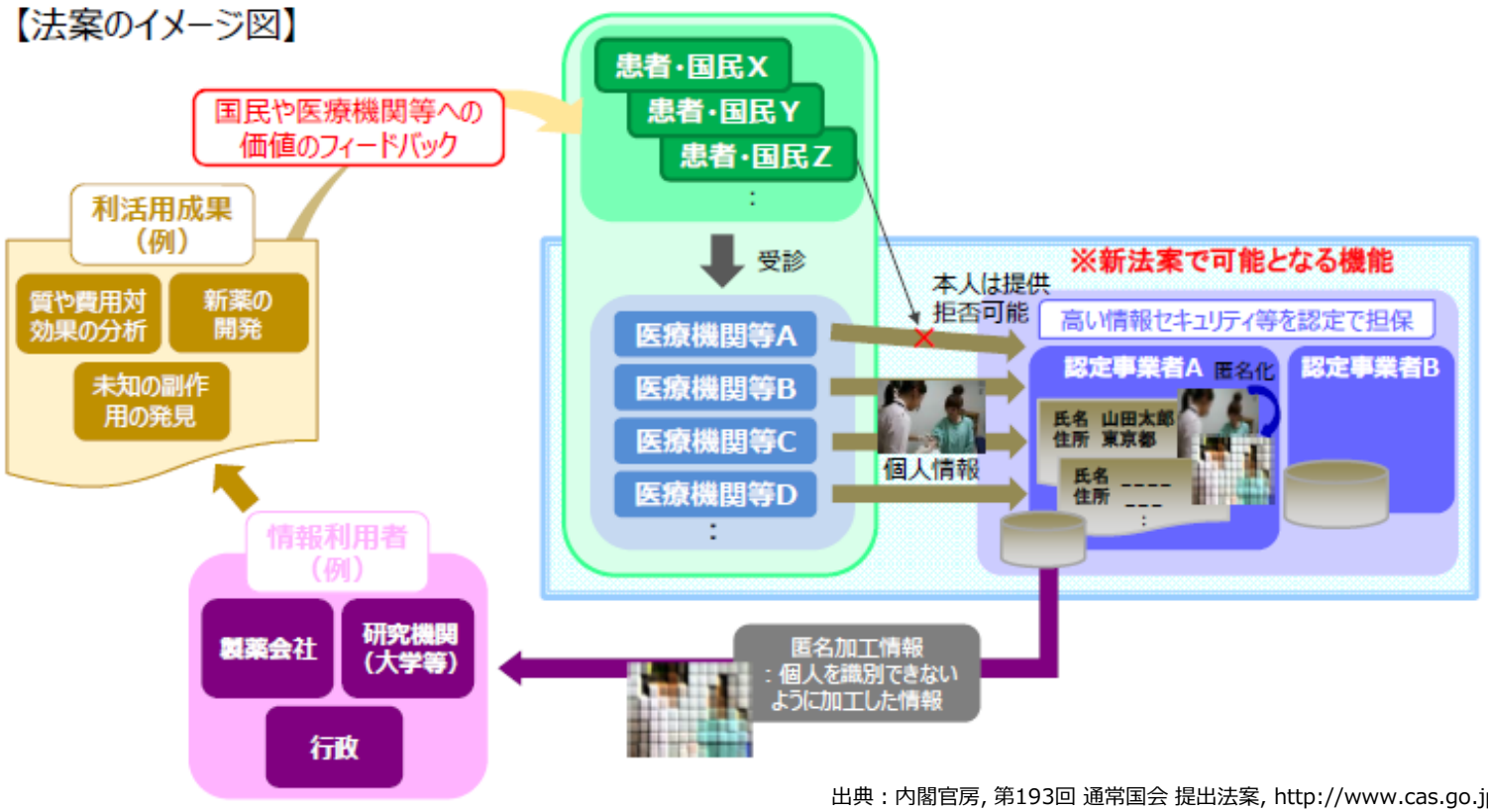


※同意を取るなどが必要

© NEC Corporation 2019

医療分野における法制度：次世代医療基盤法

次世代医療基盤法※1が成立し、一定の基準を満たした「認定匿名化加工医療情報作成事業者」に対して、医療情報を収集・結合し、匿名化※2して提供可能となる※3



出典：内閣官房, 第193回 通常国会 提出法案, http://www.cas.go.jp/jp/houan/193.html

※1 「医療分野の研究開発に資するための匿名加工医療情報に関する法律案」（次世代医療基盤法案）2017年4月可決、5月公布

※2 次世代医療基盤法は「匿名加工情報」ではなく「匿名加工医療情報」である。詳細は未定。

※3 あらかじめ本人に通知することや、提供先では他の情報との照合は禁止されることなどの条件がある

© NEC Corporation 2019

再掲：目指すユースケース

医療情報に限らず、組織が保有する様々な機密データを、**相互に開示せずに結合した分析**を実現し、組織を越えたデータ活用による新たな知見を獲得

疾病と運動の
相関分析による
予防医療

ヘルスケア分野

観光客の行動と購買
傾向分析による
おもてなし

観光分野

金融情報の
結合分析による
不正送金検知

金融分野

・・・・・

複数組織のデータを
結合した分析結果だけを提供

秘密計算技術

制度整備

複数組織の機密データを相互に開示せずに結合

投薬・疾病履歴、
ゲノム情報など

医療機関

運動量情報

ヘルスヘア企業

銀行残高
送金情報など

金融機関

位置情報
購買情報など

キャリア、ECサイトなど

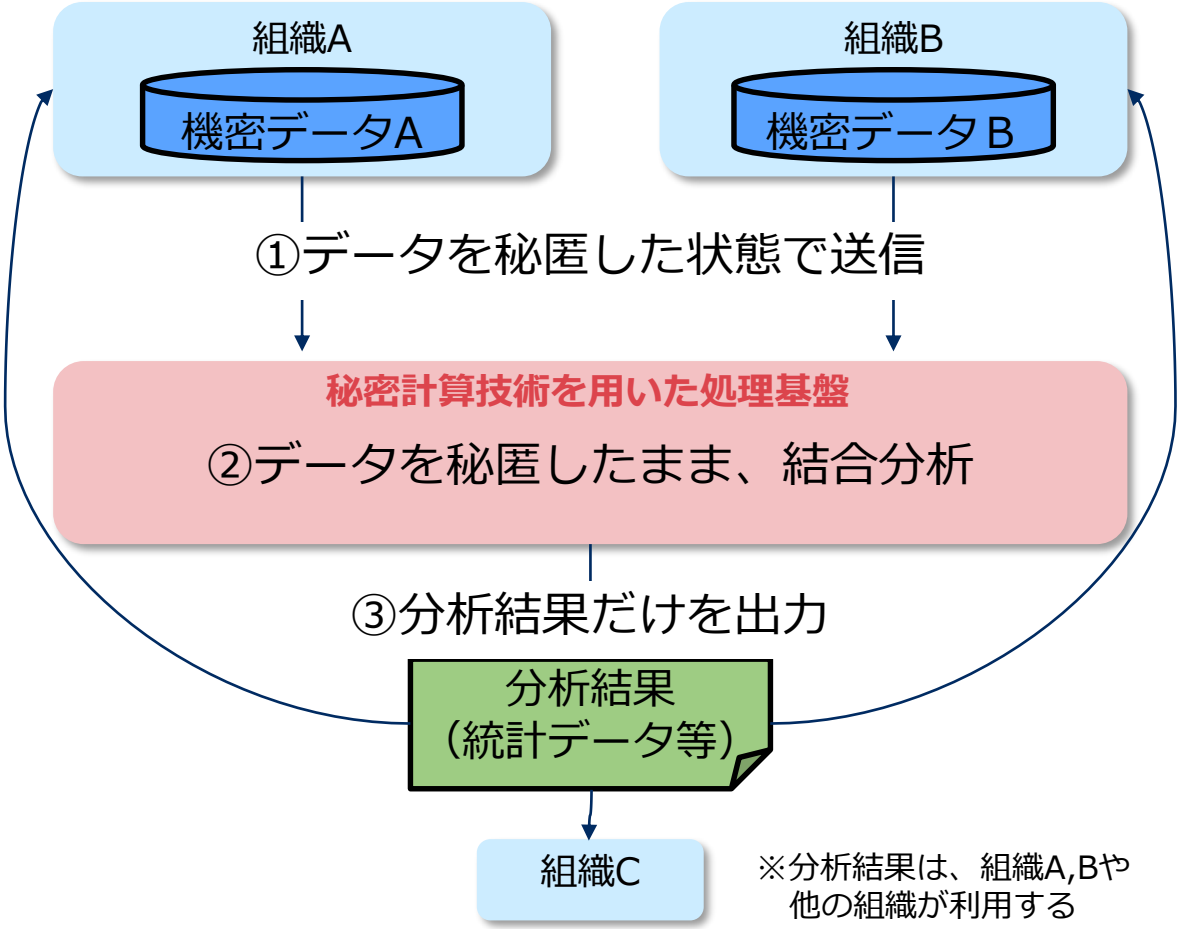
・・・・・

© NEC Corporation 2019

3．秘密計算の方式整理

秘密計算技術の概要

- 秘密計算とは、データを秘匿したまま処理できる技術
- 異なる組織のデータを、組織外に元データを一切開示せずに、データを結合した分析が可能

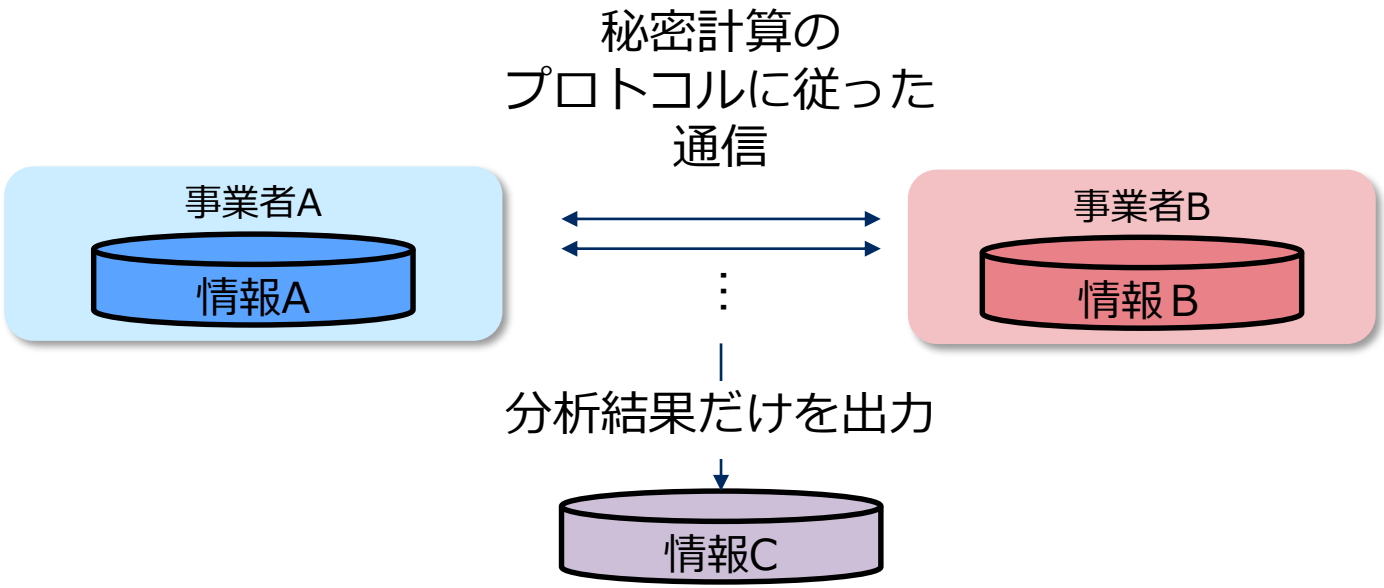


© NEC Corporation 2019

秘密計算の安全性

秘密計算では、各事業者は、出力以上の情報は得られない

モデル



安全性：

- 事業者Aは、情報C以上の情報は得られない。
- 事業者Bは、情報C以上の情報は得られない。

© NEC Corporation 2019

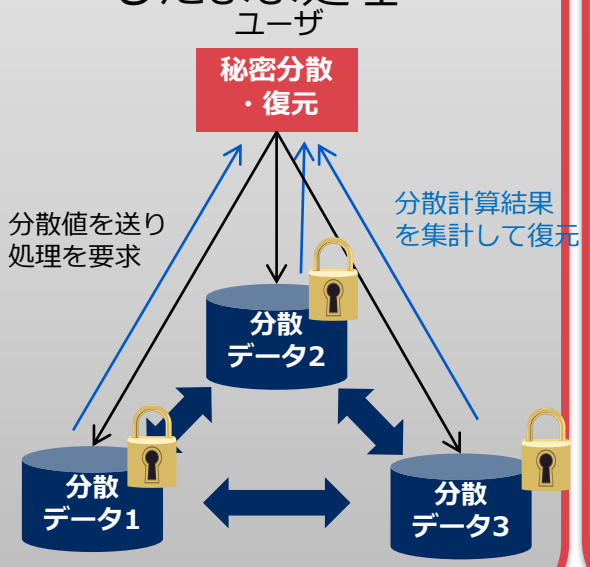
秘密計算技術の様々な方式

秘密計算には様々な方式があるが、本セッションでは「秘密分散方式」と「準同型暗号方式」について説明

秘密計算

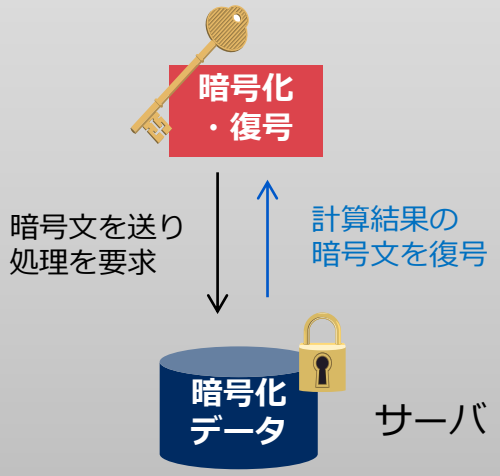
秘密分散を利用した方式

データを秘密分散したまま処理



準同型暗号を利用した方式

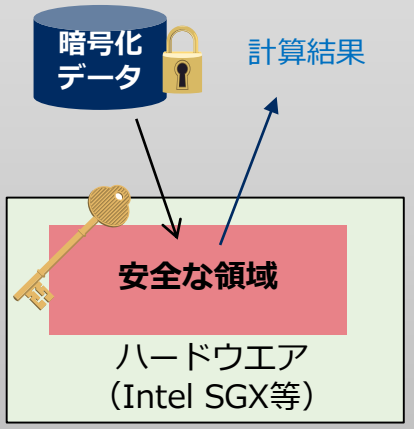
データを暗号化したまま処理



ハードウエアを利用した方式

(Trusted Execution Environment等)

ハードウエア上の安全な領域で処理



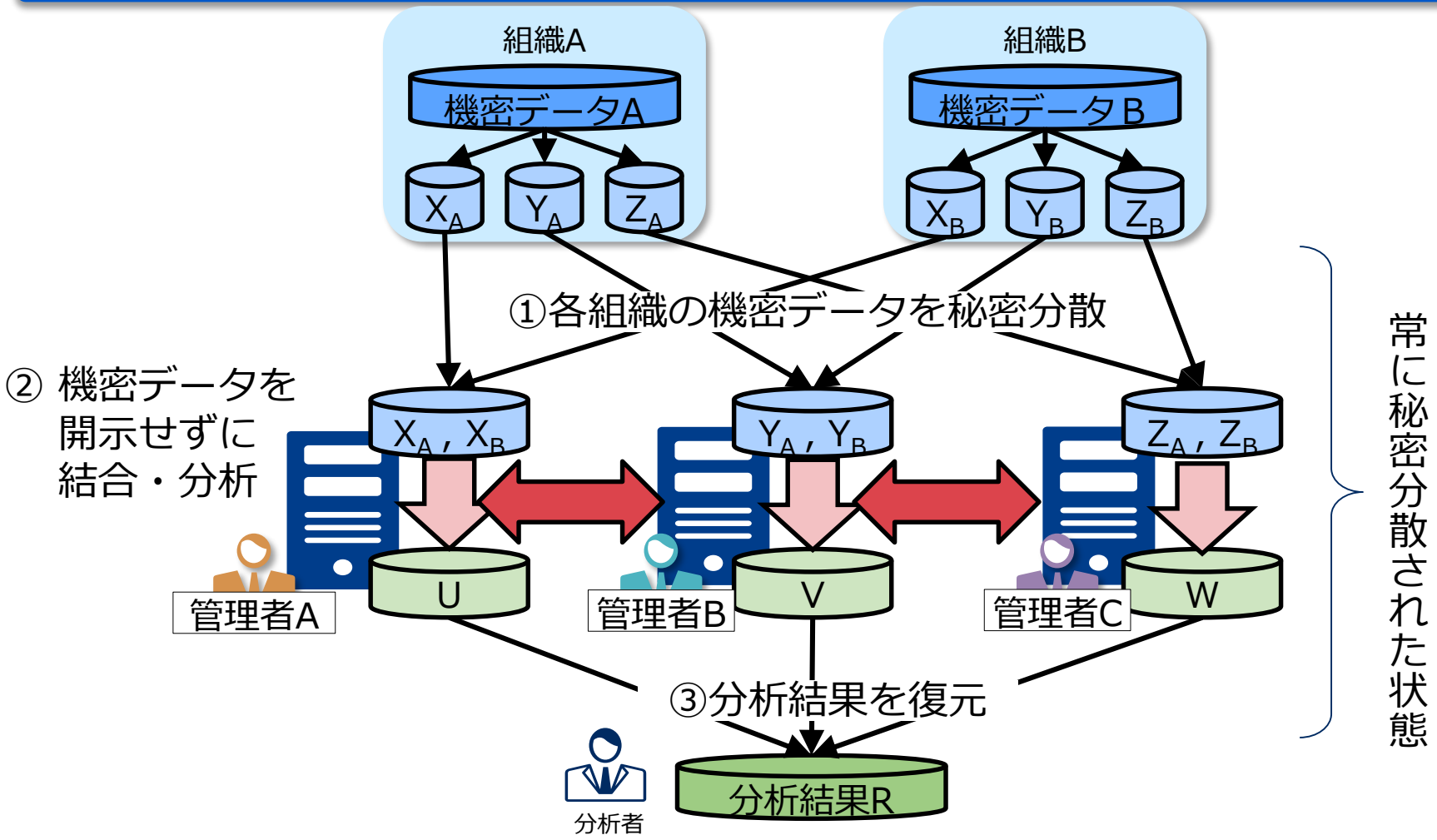
安全な領域に保持している鍵で、データを復号して処理する

・・・ その他方式も存在

© NEC Corporation 2019

秘密分散方式の秘密計算

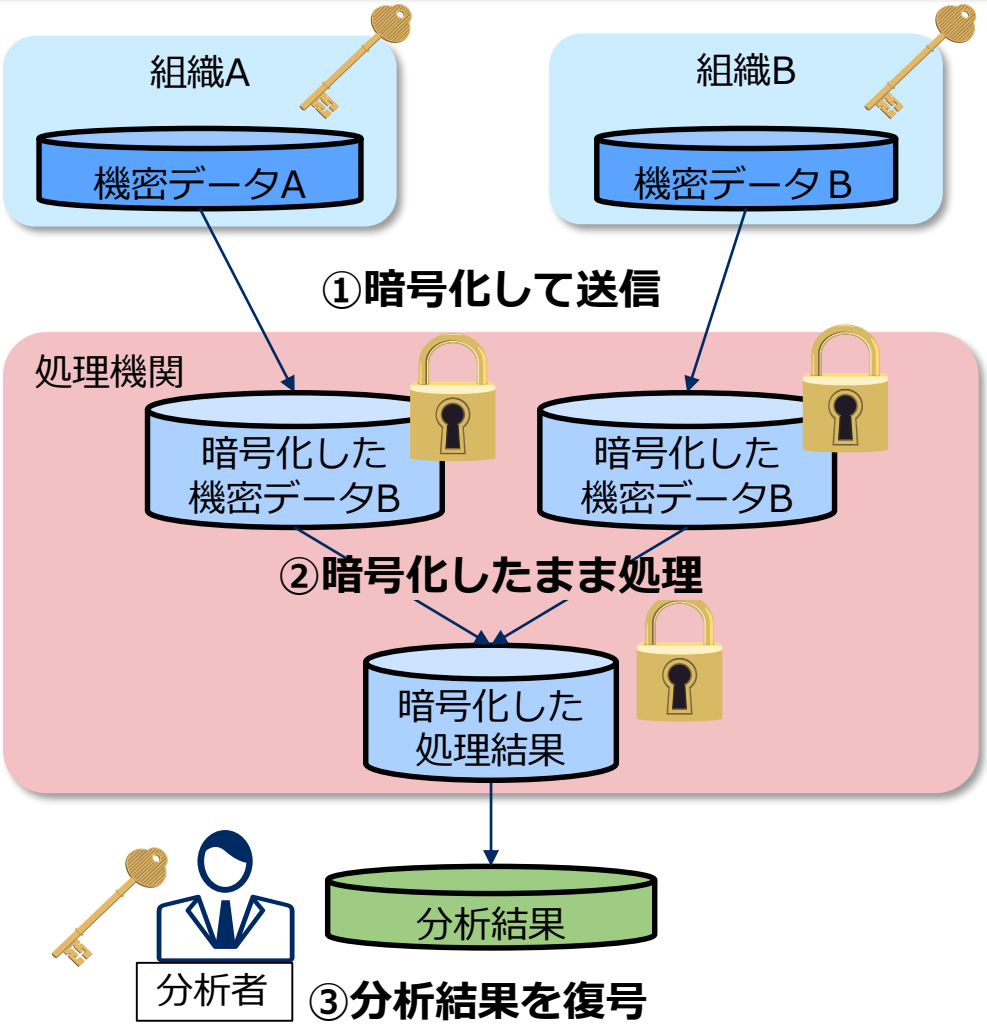
- 機密データを乱数に分割（秘密分散）し、秘密分散したまま処理
- 前提：結託等が無く、秘密分散された値が一定数集まらなければ安全



© NEC Corporation 2019

準同型暗号方式の秘密計算

- 準同型暗号を用いて、暗号化したまま復号せずに、結合して処理
- 前提：鍵が安全に管理されていれば、復号できないため安全



準同型暗号の例：
Enc(a) × Enc(b)
= Enc(a+b)

常に暗号化された状態

© NEC Corporation 2019

秘密計算方式の簡単なまとめ

各方式の簡単な整理

	方式	安全性の前提
秘密分散方式	**秘密分散**したまま処理	結託が無い （秘密分散した**データの分離**）
準同型暗号方式	**暗号化**したまま処理	鍵の安全管理 （暗号文と鍵の**分離**）

秘匿したまま処理

分離して管理

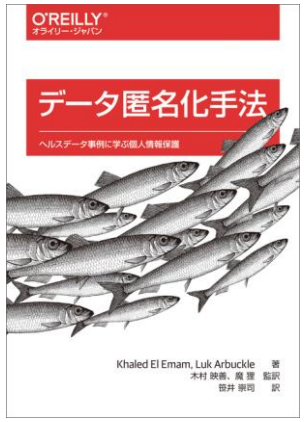
方式・安全の前提は異なるが、ある程度同様に扱えるのではないか

© NEC Corporation 2019

４．秘密計算を用いたデータ結合

参考資料：

“データ匿名化手法 ヘルスデータ事例に学ぶ個人情報保護”
著：Khaled El Emam, Luk Arbuckle,
監訳：木村映善, 魔狸
訳：笹井崇司.
12章「セキュアな連結」

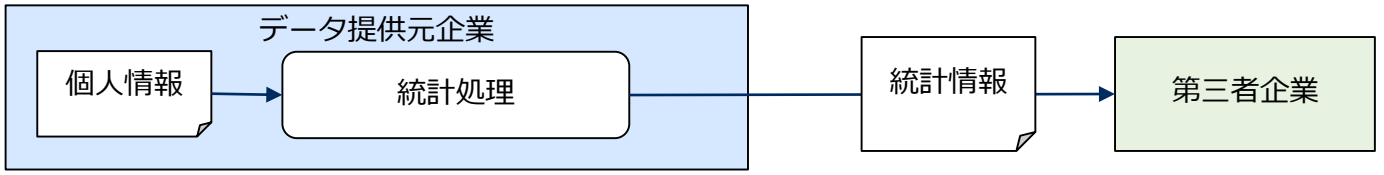


出典： オライリー社HP https://www.oreilly.co.jp/books/9784873117249/

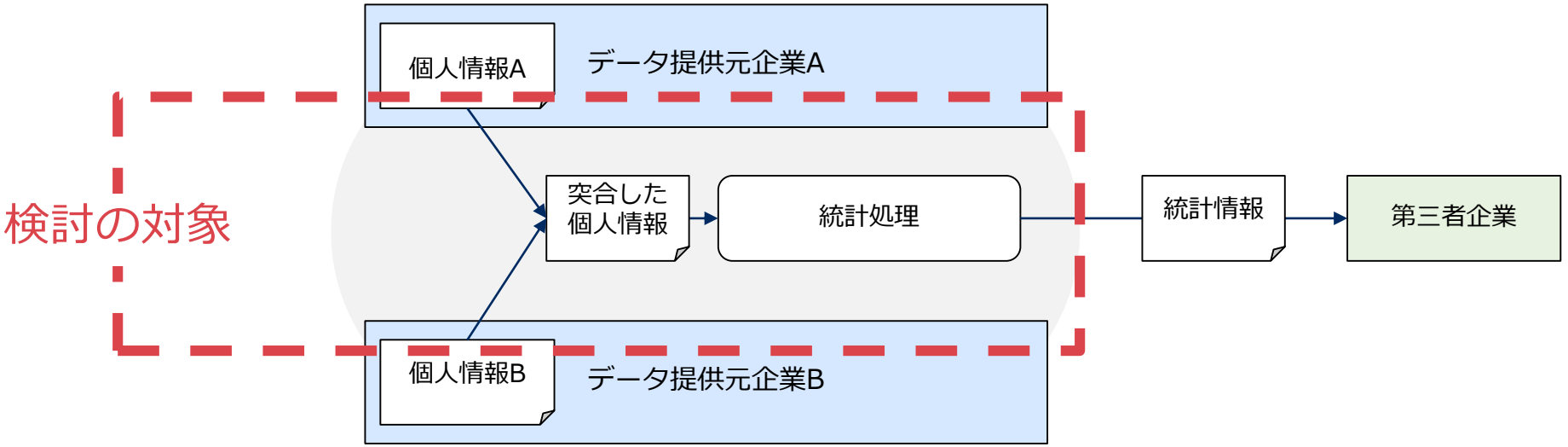
秘密計算技術による安全なデータ結合

データ提供元の複数企業が、秘密計算技術を用いることで、**責任をもって安全に個人情報を結合**して統計処理を行う

単一組織の処理



複数組織の処理

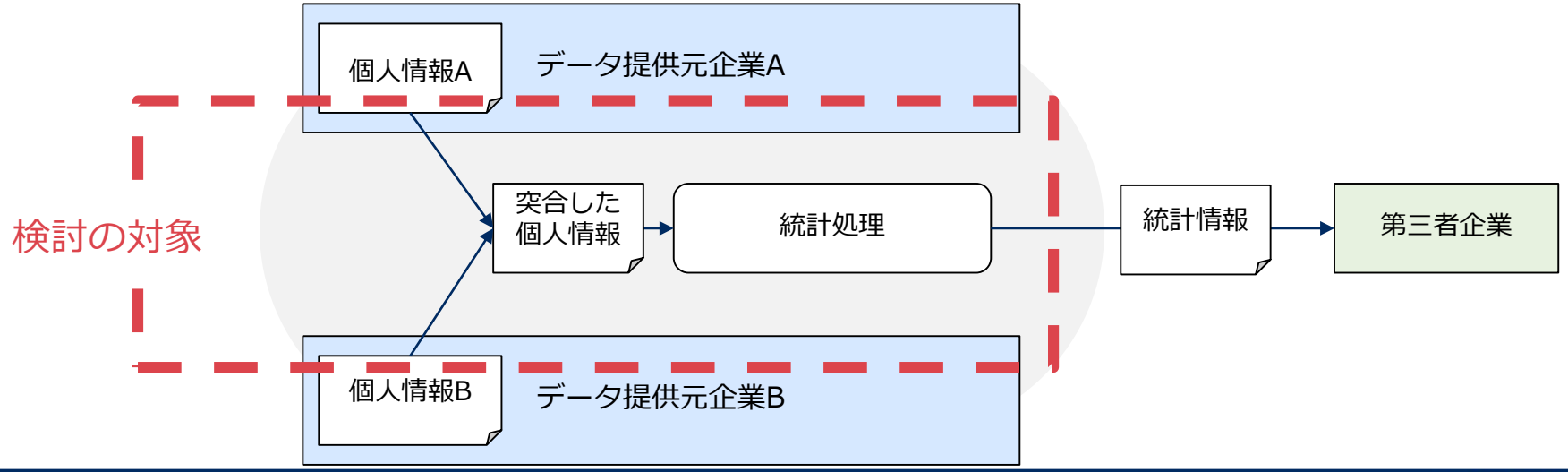


© NEC Corporation 2019

セキュアなデータ結合を実現する方式・技術を整理

実現方式の整理

秘密計算技術の利用	秘密計算技術の方式	実現方式
利用しない (完全に信頼できる機関を設置し、生データで処理)	ー	方式１
利用する	秘密分散ベースを利用	方式２
	準同型暗号を利用	方式３
	その他（本発表では割愛）	・・・

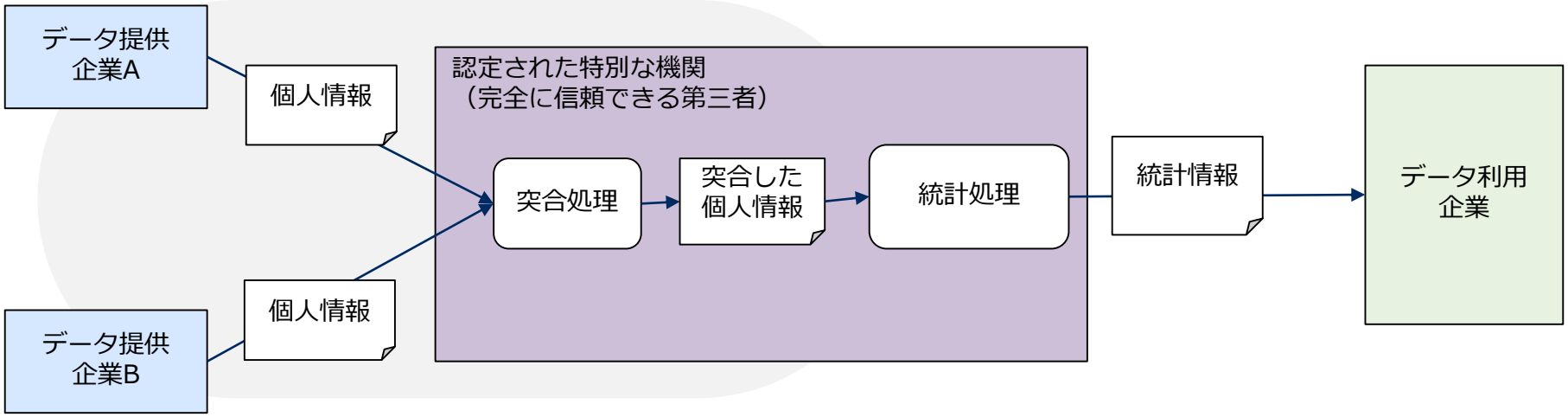


© NEC Corporation 2019

方式１：完全に信頼できる第三者を設置

認定された特別な機関にデータを送り、処理した結果を提供

- 次世代医療基盤法の”認定事業者”に近い考え

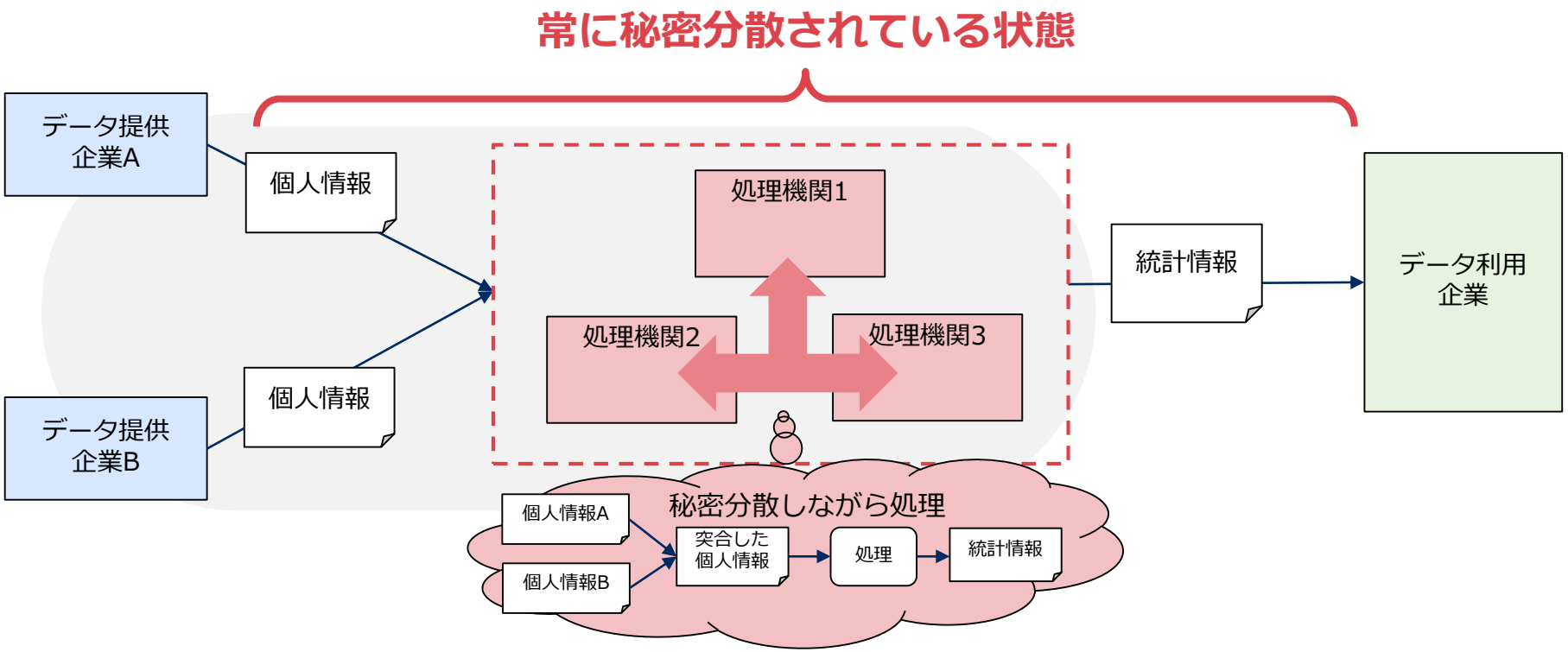


懸念点

- 「完全に信頼できる第三者」は生データを閲覧可能
- 「完全に信頼できる第三者」の認定・監査等のコストが大きい（「データ匿名化手法」本の主張）
- 一部の機関だけが認められると、処理内容（統計処理等）の多様化が望めない

© NEC Corporation 2019

方式２：秘密分散方式の例

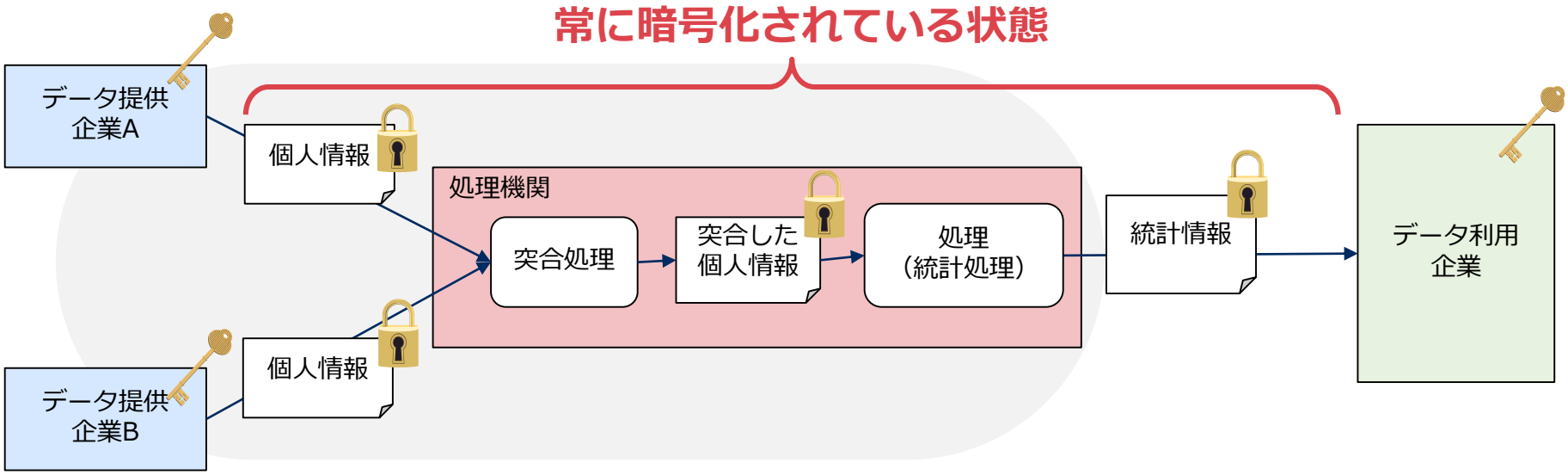


安全であるための条件：結託防止

（例：結託すれば処理途中のデータを取得可能）

© NEC Corporation 2019

方式３：準同型暗号方式の例



安全であるための条件：

- 鍵の適切な管理（例：不正入手した鍵によって処理途中での復号できてしまう）
- 結託防止（例：暗号化したデータを鍵を持つ他者へ提供できてしまう）

© NEC Corporation 2019

方式のまとめ

本発表で紹介した3方式の整理

	説明	仲介者による データ閲覧	安全性の前提
方式１	完全に信頼できる機関で実現	出来てしまう	仲介者が不正しない※1
方式２	秘密分散方式の秘密計算で実現	不可能(安全)	鍵の安全管理など
方式３	準同型暗号方式の秘密計算で実現	不可能(安全)	結託の防止など

- ※1 完全に信頼できる仲介者（第三者）の設置は、
  認定・内部外部監査等の運用コストが懸念(「データ匿名化手法」本の主張)

安全性の前提を明確化し、関連する制度等の整備が必要ではないか

© NEC Corporation 2019

５．制度議論や技術の動向

秘密計算への社会的な期待

経団連や自民党では、秘密計算の研究開発や社会実装の促進を提言

経団連「Society 5.0を実現するデータ活用推進戦略」

セキュリティ技術に関しては、データ流通および活用に対する過度な拒否反応を防ぎ、かつ国民の安全・安心を担保するためにも、**関連分野の技術をもつ企業が協力**し、**秘密計算**や高度な暗号化等の安全管理に関する技術を**データ活用におけるわが国の重要インフラのひとつ**ととらえ、開発・展開していくことも望まれる

出展：経団連, “Society 5.0を実現するデータ活用推進戦略”, 2017年12月12日.
「III. データ活用の推進に向けた鍵」「２．必要なデータを使える」「（６）技術開発」. p.15

自民党「経済構造改革戦略： Target 4」

個人情報保護の観点から開発を進めている**秘密計算技術**をはじめ、最新のセキュリティ技術の研究開発を推進する。また新たな技術の社会実装に向けて、**規制のサンドボックス制度の活用**を促していく。

出典：自由民主党 政務調査会,” 「経済構造改革戦略： Target 4」経済構造改革に関する特命委員会　最終報告”, 2018年4月27日.
https://www.jimin.jp/news/policy/137249.html,

© NEC Corporation 2019

情報法制研究所(JILIS)「秘密計算技術応用研究タスクフォース」

情報法制研究所にて、秘密計算に関する法制度について議論されている

■主幹理事： 高木理事

■関与理事等：鈴木理事長、板倉参与

■趣旨：

秘密計算技術を応用したプライバシー保護データマイニング（PPDM：Privacy Preserving Data Mining）の技術を利用するに際しても、形式上、暗号化した個人データを第三者に提供することになるので、個人情報保護法23条の規制が障害となって技術を利用できないのではないかとする課題があった。この問題を解決すべく、そもそもこれまで、どのような意味で「暗号化しても個人情報である」との説が唱えられてきたのかを整理した上で、**秘密計算技術**に基づくPPDMでの**データ交換の個人データ該当性について検討し提言**にとりまとめる。

■研究概要：

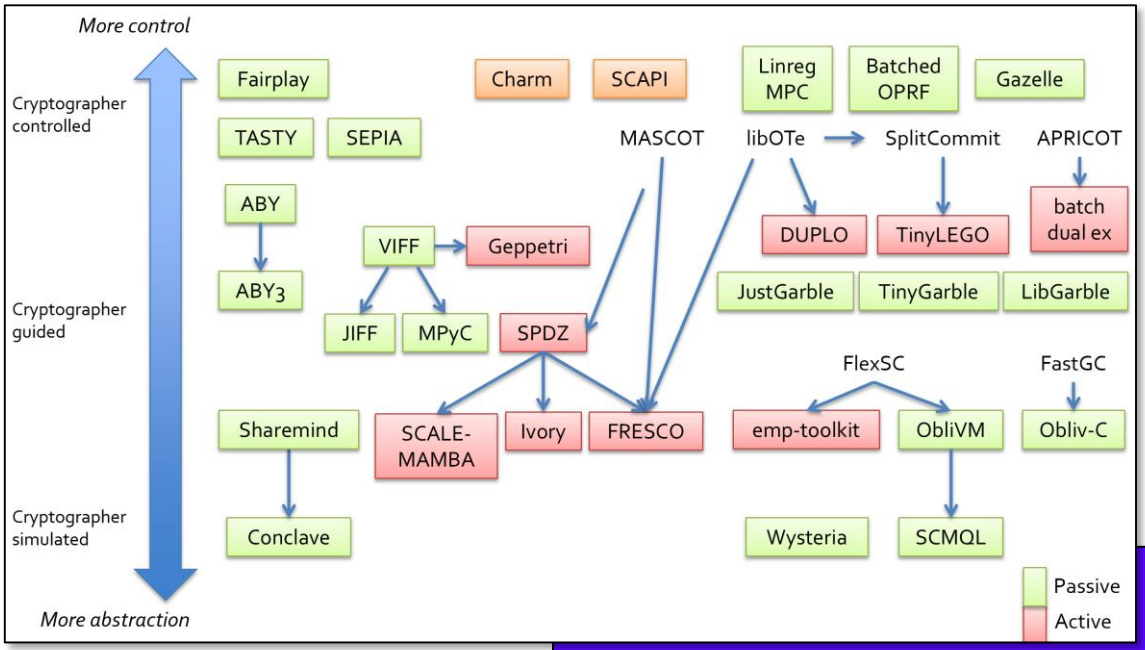
・秘密計算技術の仕組みを模式化し、複数の方式について分類し整理する。
・暗号化と個人情報該当性に係る論点を整理し、秘密計算技術がこの基準に適合する要件を示す。
・提言として取りまとめて公表する。

出典：情報法制研究所のホームページ記載内容からの抜粋
https://www.jilis.org/taskforce/

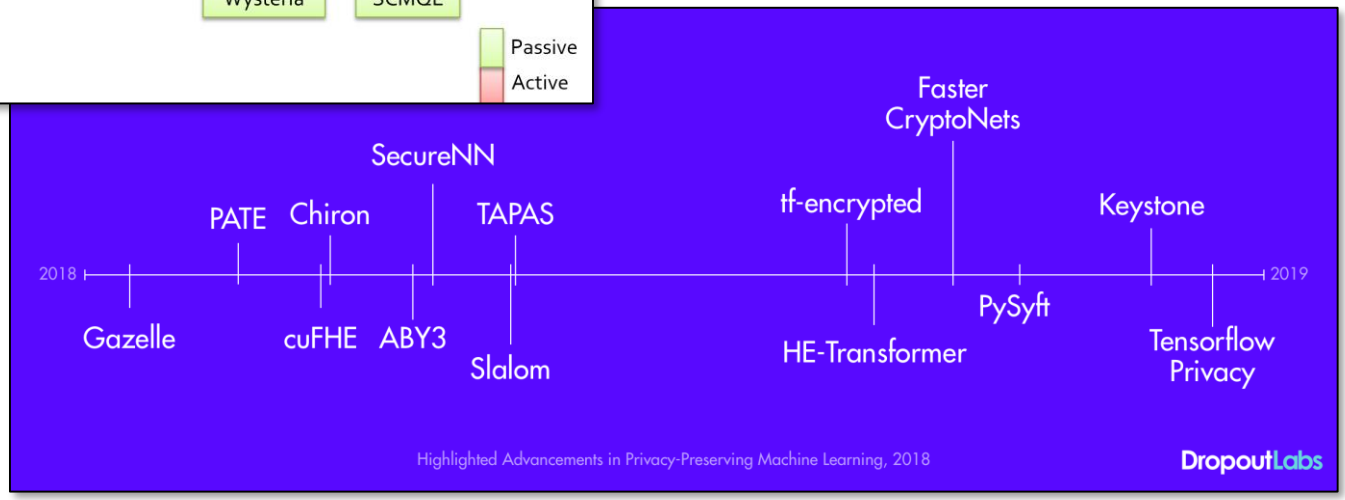
© NEC Corporation 2019

技術動向（ライブラリの実装動向）

秘密計算やプライバシ保護に関する様々なライブラリが公開されつつある



出典：Mayank Varia, “A Survey of MPC Offerings”, Presentation Slides, Differential Privacy Meets Multi-Party Computation (DPMPC) Workshop, 2018.
http://www.bu.edu/hic/dpmpc-2018/
http://www.bu.edu/hic/files/2018/06/2018-06-05-Mayank.Varia_-1.pptx

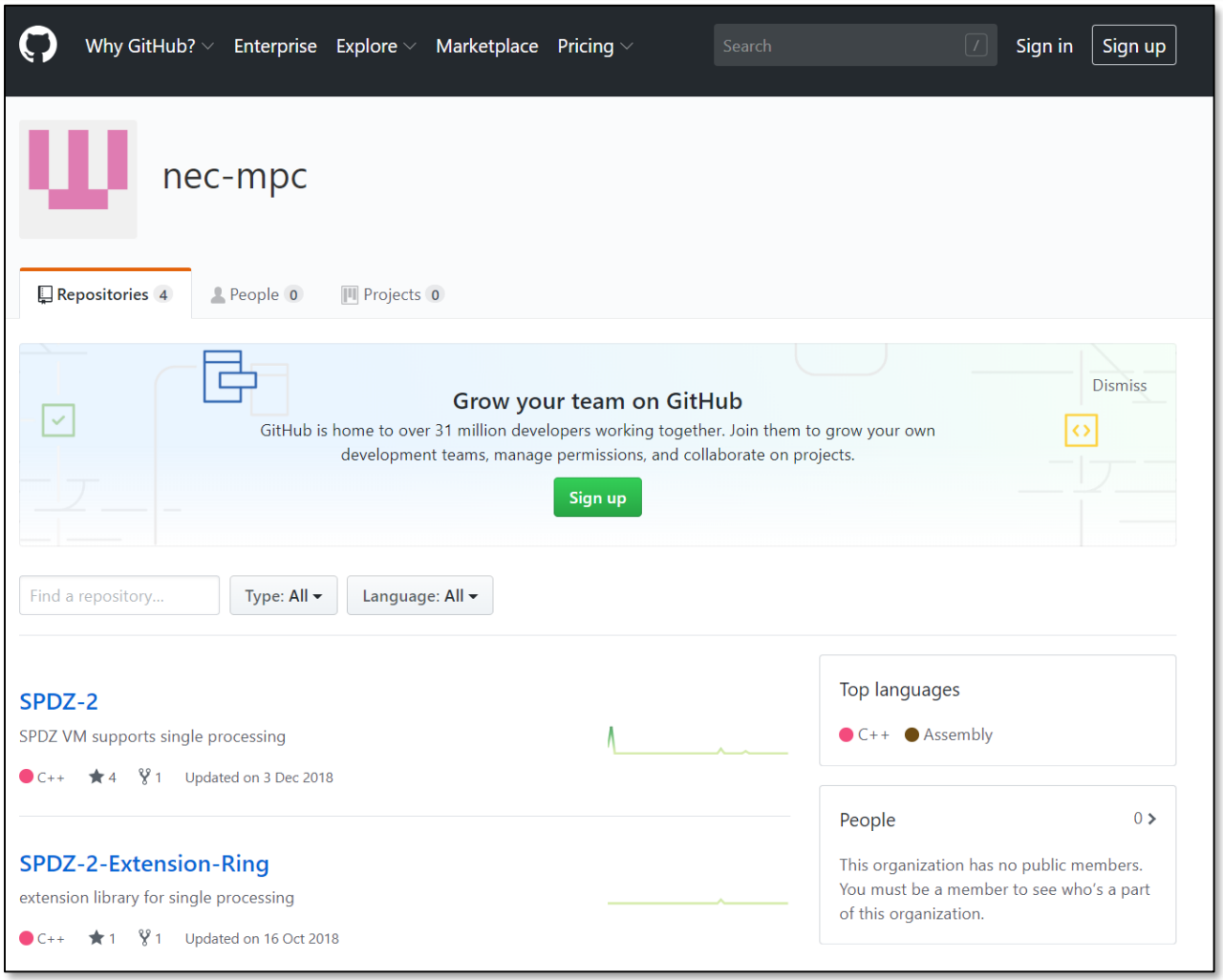


出展：Dropout Labs, *2018 was a breakout year for privacy-preserving machine learning*
https://medium.com/dropoutlabs/privacy-preserving-machine-learning-2018-a-year-in-review-b6345a95ae0f

© NEC Corporation 2019

おまけ：NECの秘密計算ソースコード公開

NECは安全性や性能検証のため、非商用目的の利用に限定してコード開示



出典： GitHub “nec-mpc”, https://github.com/nec-mpc

© NEC Corporation 2019

まとめ

- 組織間での個人データの結合分析は社会価値を生む
- データ結合を実現するモデル例：
  - 信頼のおける第3者を設置する方式
  - 秘密計算を用いた方式
    - 例：秘密分散方式、準同型暗号方式
- 秘密計算を用いると安全なデータ結合が可能ではないか？
- 社会実装には、安全の基準・制度などが必要ではないか？

技術や制度について
是非皆さんと議論をさせてください。

© NEC Corporation 2019