\Orchestrating a brighter world NEC

パネルディスカッション
「プライバシー保護データマイニング技術の実社会での活用について」資料

NECの秘密計算技術

日本電気株式会社 セキュリティ研究所
主任研究員 竹之内隆夫

2018年10月31日
プライバシ保護データマイニングシンポジウム
～フィンテックにおけるイノベーション創出を目指して～

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

安全なデータ結合・分析による社会価値創造

組織が保有する様々な機密データ(企業秘密、個人情報等)を、相互に開示せずに結合・分析し、組織間でのデータ活用による価値創出を促進

疾病と運動の相関分析による予防医療

政府･自治体

ゲノムと投薬の相関分析による個別化医療

医療研究機関

金融情報の結合分析による不正送金検知

金融機関

・・・・・

複数組織のデータを結合し
分析結果だけを提供

安全なデータ結合・分析
(秘密計算技術)

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	運動量情報 位置情報	銀行残高 送金情報など	位置情報 購買情報など	・・・・・
医療機関	ヘルスケア企業	金融機関	キャリア、ECサイトなど	

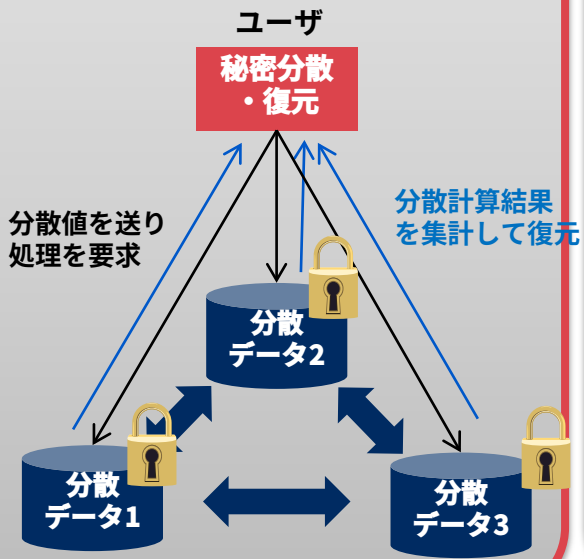
秘密計算技術の様々な方式

秘密計算

NEC注力方式

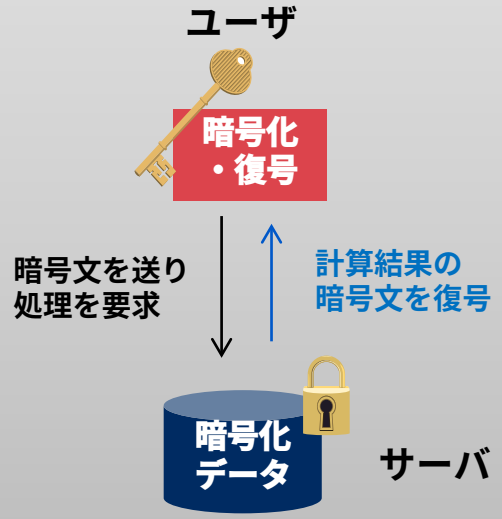
秘密分散を利用した方式

データを秘密分散したまま処理



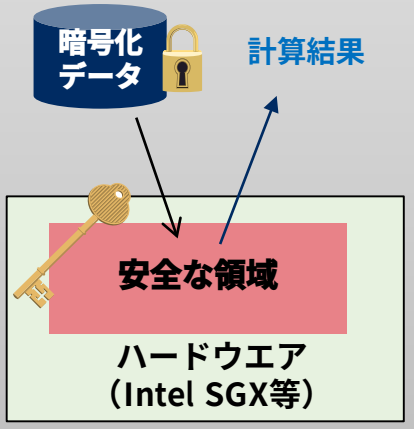
準同型暗号を利用した方式

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

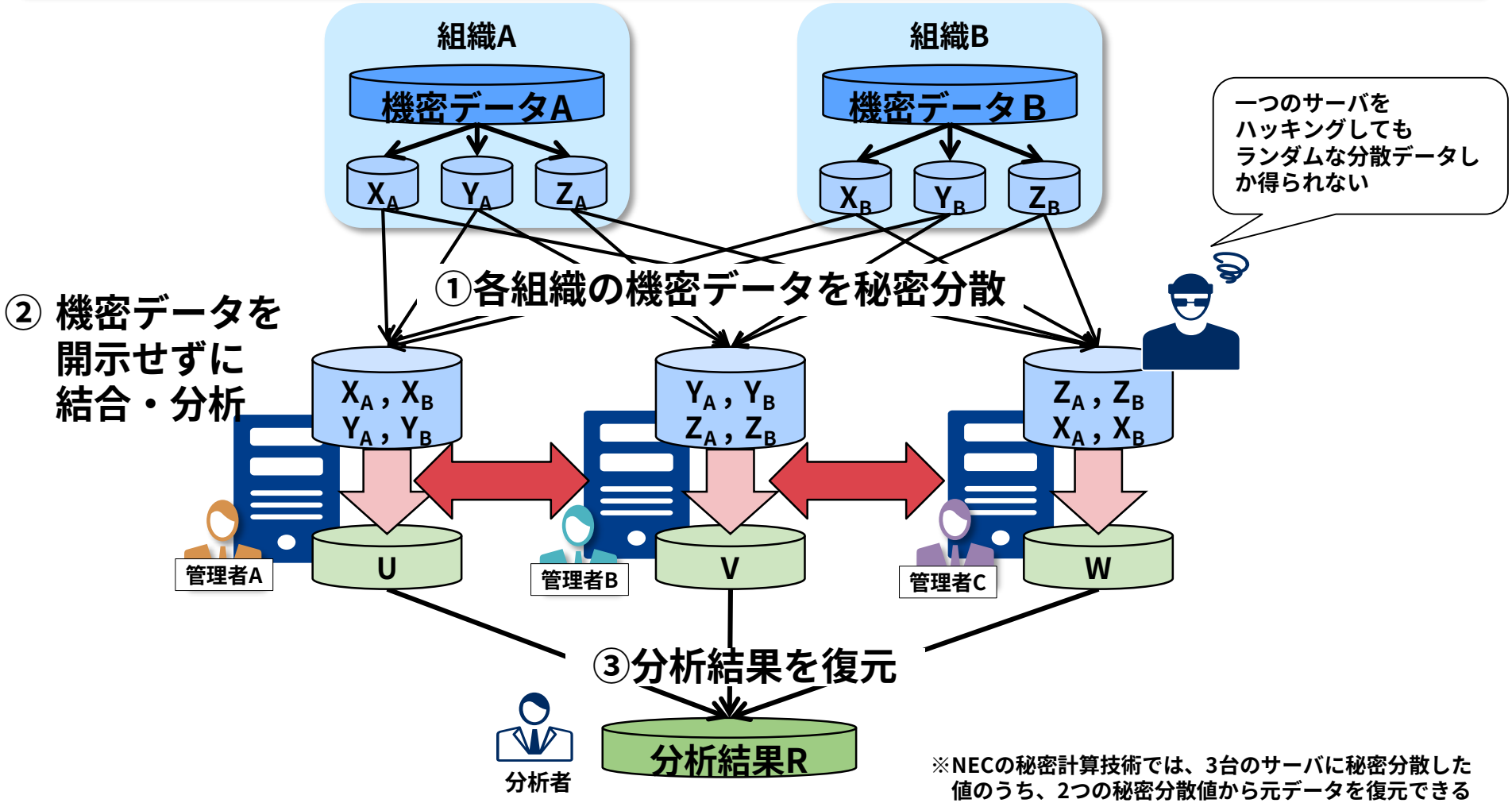


安全な領域に保持している鍵で、データを復号して処理する

● ● ●
その他方式も存在

NECの秘密計算技術の概要

- 複数サーバに秘匿したデータを分散保持し、秘匿したままの処理が可能
- 異なる組織のデータを、秘匿したまま結合・分析し、分析結果を開示

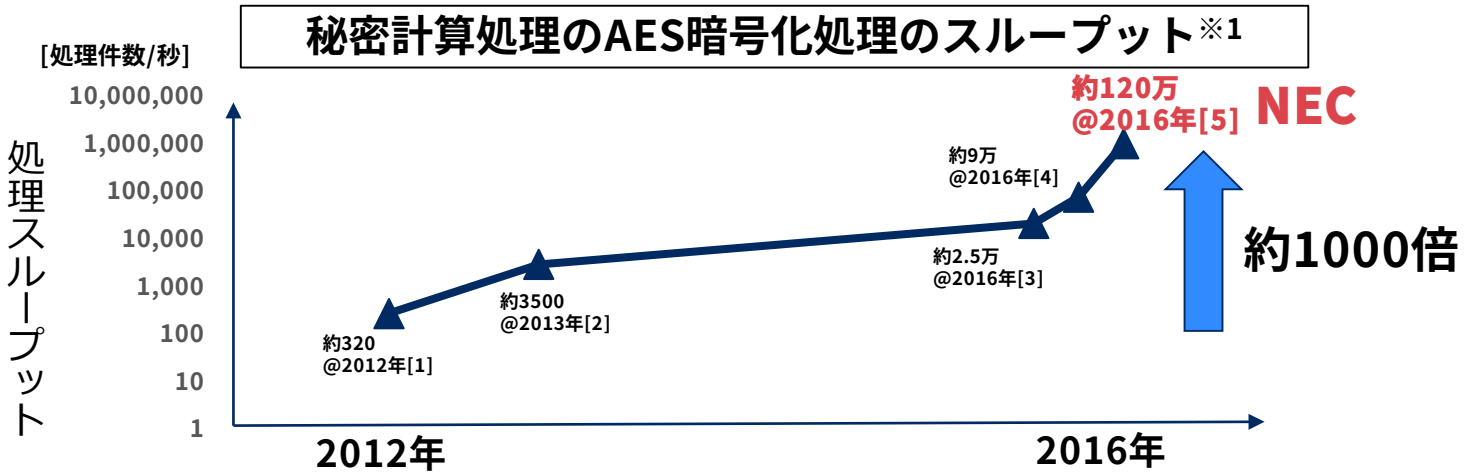


※NECの秘密計算技術では、3台のサーバに秘密分散した値のうち、2つの秘密分散値から元データを復元できる

NECの秘密計算技術の特長

NECは高速な秘密計算を実現し、一部処理で実用的な性能を達成

秘密計算は近年桁違いに高速化を実現（2012年以降で約1000倍）



例：顔特徴量の照合処理やDNA編集距離計算で、現実的な性能を達成※2

- 顔特徴量の照合処理： **1000次元の特徴量の照合が約45,000件/秒※3**
- **DNA編集距離の計算処理**： **長さ100のDNA**配列同士の距離計算：約**145/秒**

国際的に高い評価を得て、難関国際学会に採択。
CCS2016(Best Paper)、Eurocrypt2017、S&P2017、CCS2018

[1] J. Launchbury, I.S. Diatchki, T. DuBuisson and A. Adams-Moran. "Effcient lookup-table protocol in secure multiparty computation". ACM ICFP2012.
[2] S. Laur, R. Talviste and J. Willemson. "From Oblivious AES to Effcient and Secure Database Join in the Multiparty Setting", ACNS2013.
[3] R. Talviste. "Applying Secure Multi-Party Computation in Practice", Ph.D dissertation, Univ. of Tartu, 2016.
[4] J. Randmets. Personal comm. AES performance on the new Sharemind cluster. May, 2016.
[5] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, Kazuma Ohara,"High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority", ACM CCS2016.

※1 semi-honest安全な3パーティの秘密計算で比較。[5]論文のTable.1を参考にグラフ化
※2 詳細は「土田 他, “不正検知可能なマルチパーティー計算による生体情報と遺伝子情報の保護”, SCIS2018」を参照
※3 VISAのピーク時トランザクション数：秒間47,000件

付録：論文・プレスリリース

論文

- [1] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, Kazuma Ohara, "High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority", ACM CCS 2016. (Best Paper Award)
- [2] Jun Furukawa, Yehuda Lindell, Ariel Nof, Or Weinstein, "High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority", EUROCRYPT 2017.
- [3] Toshinori Araki, Assi Barak, Jun Furukawa, Yehuda Lindell, Ariel Nof, Kazuma Ohara, Adi Watzman, Or Weinstein. "Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier“, IEEE S&P 2017.
- [4] Toshinori Araki, Assi Barak, Jun Furukawa, Marcel Keller, Yehuda Lindell, Kazuma Ohara, Hikaru Tsuchida, “Generalizing the SPDZ Compiler For Other Protocols”, ACM CCS 2018.

プレスリリース

- "NEC、機密情報の漏えいを強固に防止する秘密計算の高速化手法を開発～大規模な認証システムで利用できる性能を実現～“, 2016年12月15日
  - http://jpn.nec.com/press/201612/20161215_02.html

付録：秘密計算の社会的な期待

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,

付録：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/


Orchestrating a brighter world
NEC