Orchestrating a brighter world

NEC

高速秘密計算説明資料

2016年12月 15日

NEC セキュリティ研究所

1．秘密計算 (Secure Computation)

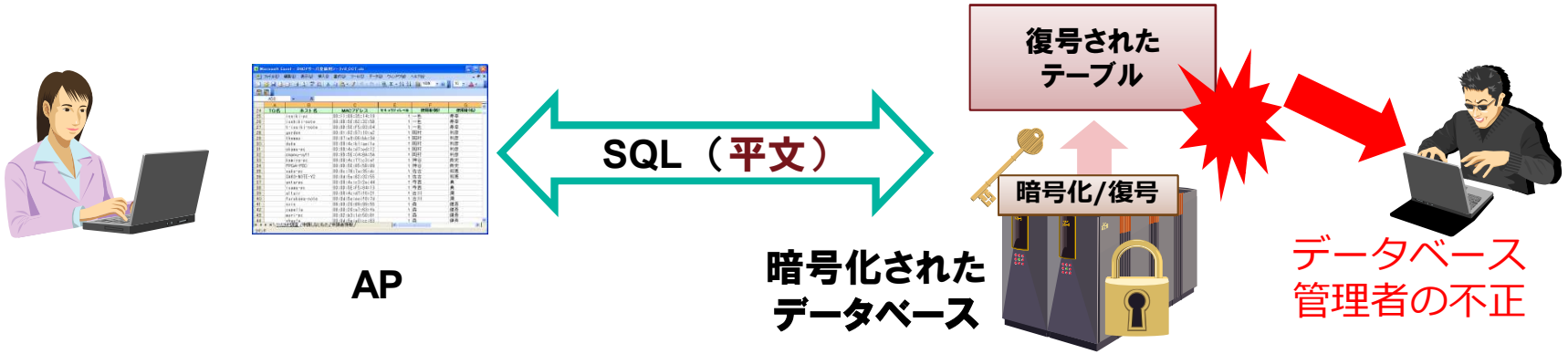
- 暗号化はデータが流出した際にも漏えいを防げる有効な手段だが、従来は、データを処理する際に元データに一旦戻す必要があり、管理者権限を悪用すると攻撃者は元データを復元して入手できる可能性があった。
- **秘密計算**は、暗号化したデータを元のデータに戻さずそのまま処理する技術。データが常に暗号化されているので、元データの漏えいを完全に防止できる。

1．従来の対策

データ処理を伴うと従来手法では抜本的な情報漏えい対策は難しい

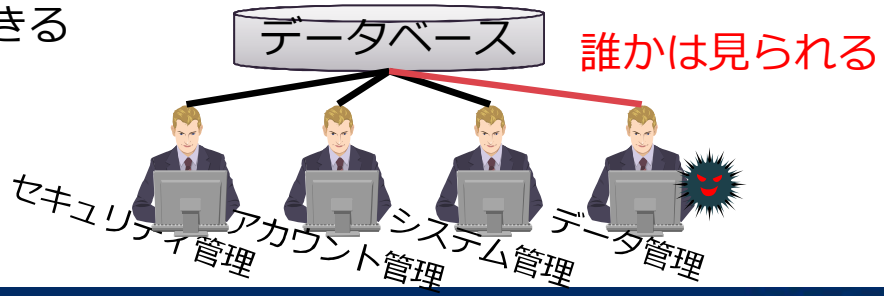
●データベースの従来の暗号化

- ストレージ上では暗号化、ディスクの盗難での情報漏えいの心配なし
- 鍵はデータベース側にあり、データ利用時には復元してアプリケーションはそのままに暗号化適用可能　⇒　データベース管理者はデータ入手可能



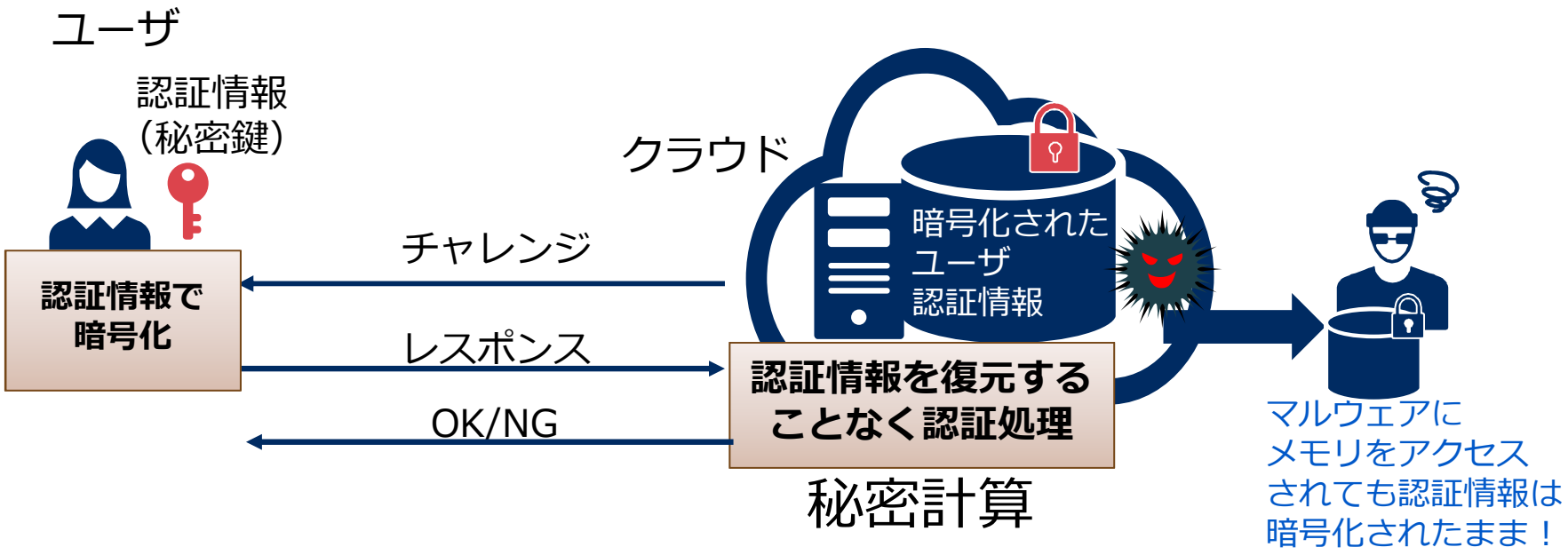
●管理権限の分掌

- 相互監視による不正の抑止、一人の管理者の不正の影響を限定
- 運用が煩雑、誰かはデータを見ることができる



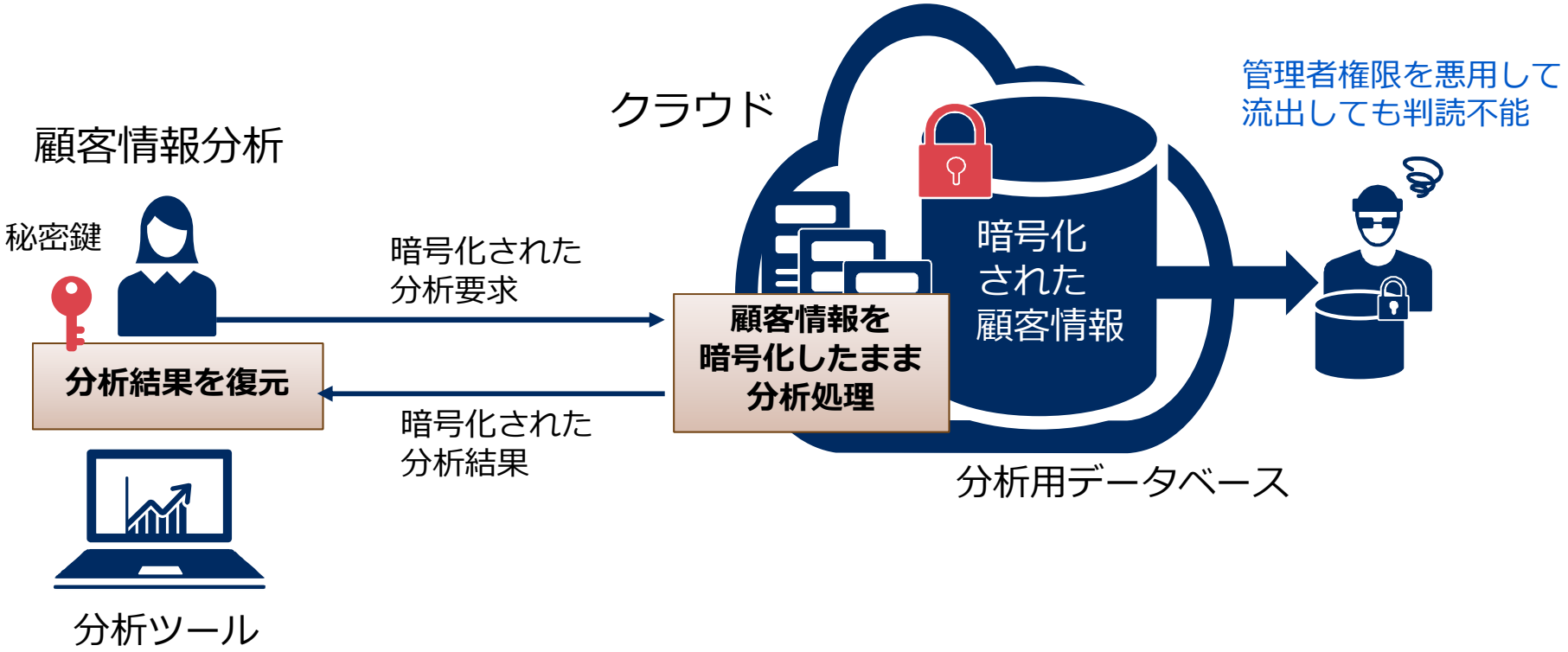
1．秘密計算の想定適用例：認証サーバ

- 秘密鍵やパスワード、生体認証の特徴量などの認証情報の漏えいは不正アクセスから大量の情報漏えいにつながる
- 秘密計算によって認証サーバが保有する大量のクライアントの認証情報の漏えいを強固に防ぎながら認証処理が可能になる



1．秘密計算の想定適用例：分析用データベース

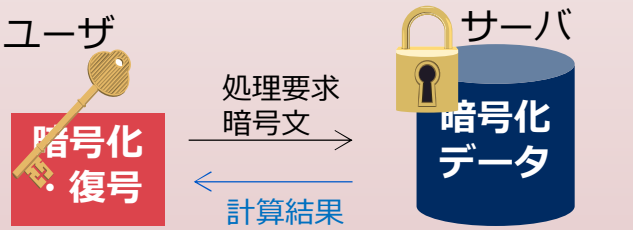
秘密計算によって情報漏えいのリスクを抑えることで、データベースに顧客情報や住民情報などの機密情報を大量に集積して活用することが可能になる



1．秘密計算の分類

秘密計算
Secure Computation

検索可能暗号・準同型暗号
Searchable Encryption,
Homomorphic Encryption



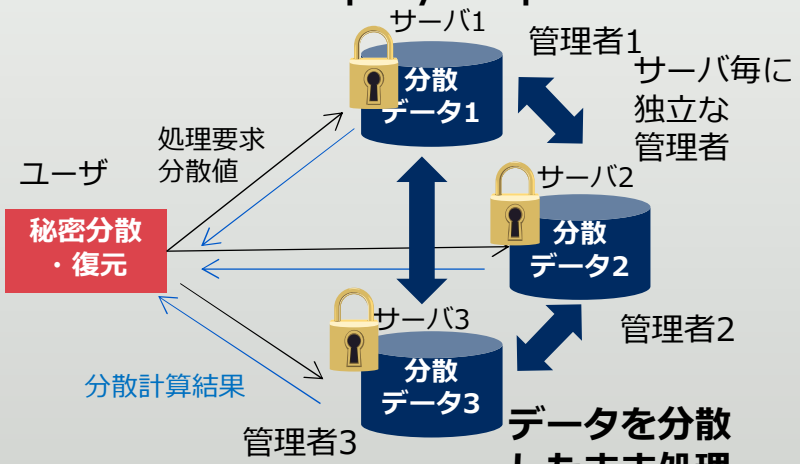
データ処理可能な特殊な暗号化

加法準同型暗号

$$E(a + b) = F(E(a), E(b))$$

a+b の暗号文がa, bそれぞれの暗号文から計算可能

マルチパーティ計算
Secure Multiparty Computation



データを分散したまま処理

和(a+b)のマルチパーティ計算

a=a1+a2+a3,
b=b1+b2+b3

c=c1+c2+c3
= a + b

分散　　復元

サーバ1	a1	b1
サーバ2	a2	b2
サーバ3	a3	b3

和

c1 =a1+b1
c2 =a2+b2
c3 =a3+b3

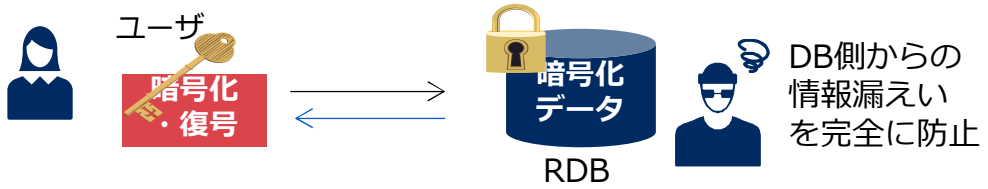
積は複雑（後述）

1．秘密計算方式の比較

検索可能暗号・準同型暗号

- **処理に応じて新たな暗号化（利用モード）の設計必要、複雑な処理は困難**
- 簡易な特定の処理に対しては非常に効率の良い暗号方式が存在
  - **定型業務の主な処理である、インデックスによる“参照・更新”の秘匿計算に対応する検索可能暗号を利用したRDBを開発**

2013年度　NEC
データベースの秘匿計算技術を発表

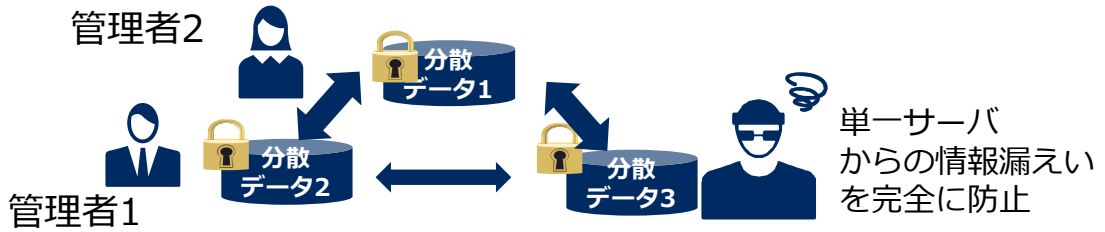


今回の発表②
分析用データベース

マルチパーティ計算

- **任意の処理に対応可能な方式**が30年前に開発されたが、大変遅かった
  - **NECはマルチパーティ計算の高速化研究で世界をリード、実用化が視野に入っている！**

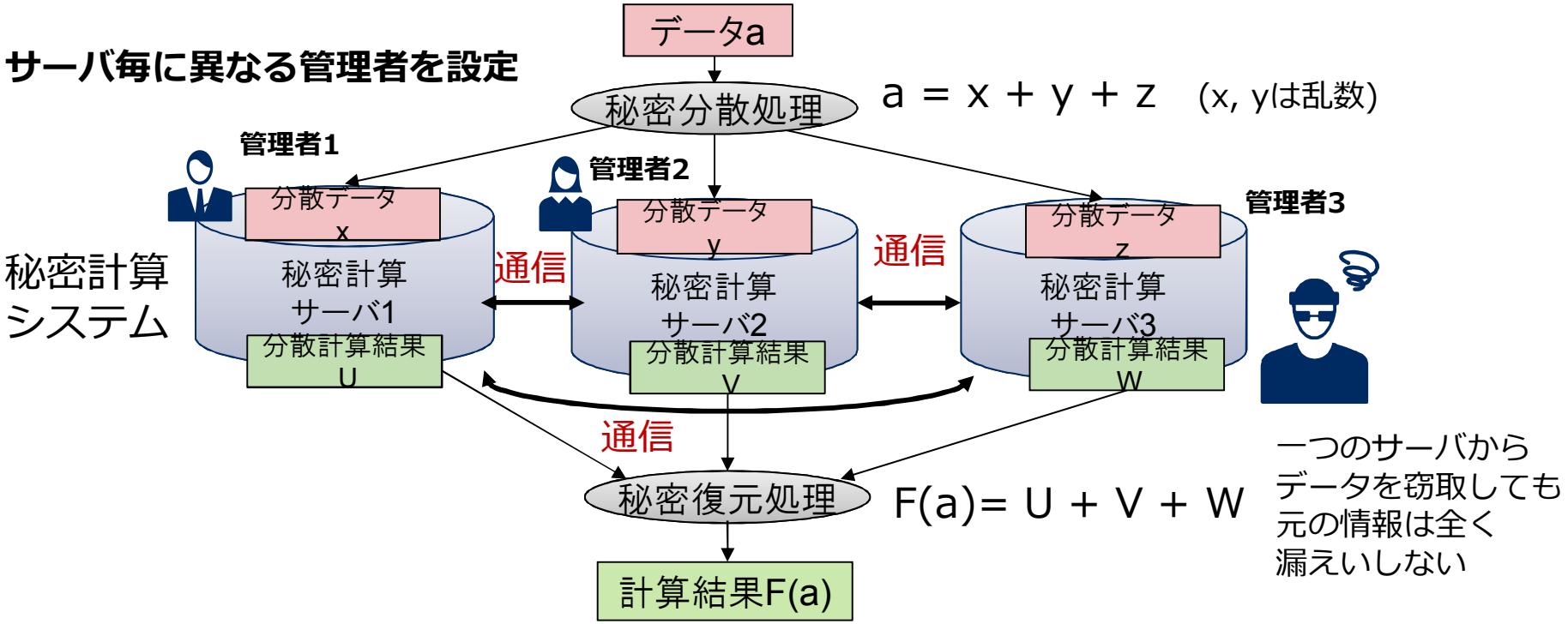
今回の発表①
高速な基本アルゴリズム



2．マルチパーティ計算

複数のサーバが協力して計算を行う技術であり，以下の特徴を持つ.

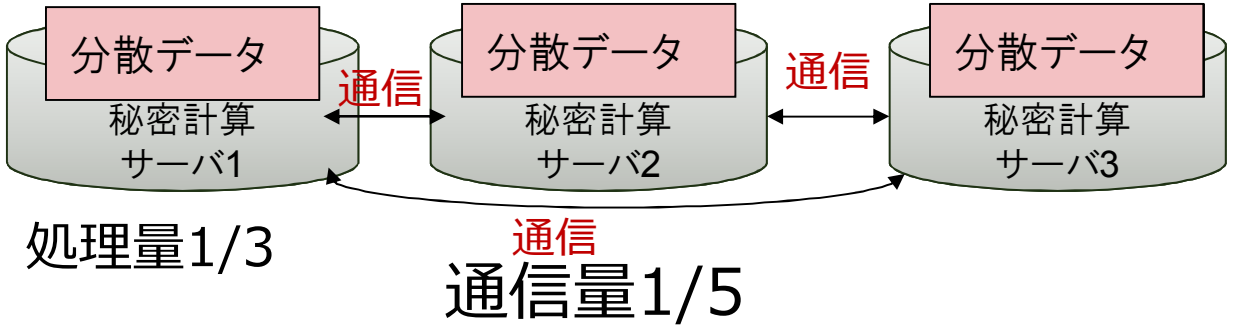
- **それぞれのサーバは，入力データ，途中の結果，計算結果を知ることができない.**
  - データは“**秘密分散**”されて入力される.
  - 計算は秘密計算サーバ間で通信しながら実行，**各サーバは秘密分散された結果を得る.**



2．マルチパーティ計算の基本演算高速化

- 秘密計算は基本演算に対するアルゴリズムを用意することで任意の処理への対応が可能
  - 論理和(xor)と論理積(and)
  - 算術和と算術乗算
- ‘和’は容易であるが、’積’はサーバ間通信が発生してとても重い処理
- NECは’積’のマルチパーティ計算でサーバ間通信量を競合比1/5, 計算量1/3にする新たなアルゴリズムの開発に成功
  - 論理積(and)に対して実装評価で性能実証

マルチパーティ計算高速化



分散データ量は従来方式に対して２倍

2．基本演算高速化：秘密鍵を分散した暗号化処理で実証

競合方式のスループットを大幅に上回る性能を実証

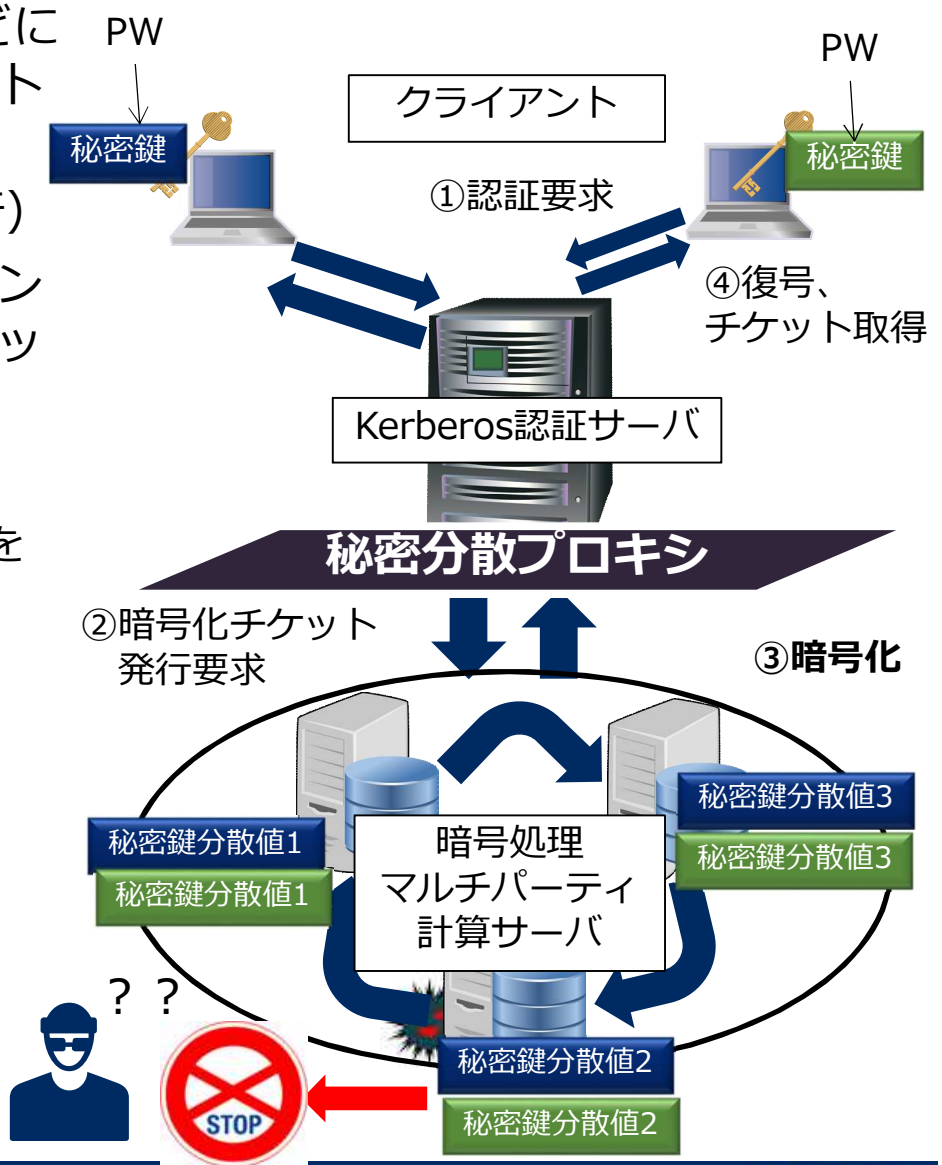
提案年	方式(フレームワーク)	スループット [AES/sec]
2013	[ACNS2013]	3450
2016	Cybernetica社 “Sharemind”	25,000
2016	Cybernetica社 “Sharemind”	90,000
2016	**本研究の提案**	**1,324,117**

- 標準暗号AESで秘密鍵を秘密分散したままの暗号化処理を実装評価
- 当初（2013年）の競合と比べて**383倍のスループット**
  （2016年と比べても**14倍**）

2．基本演算高速化：認証サーバで性能を実証

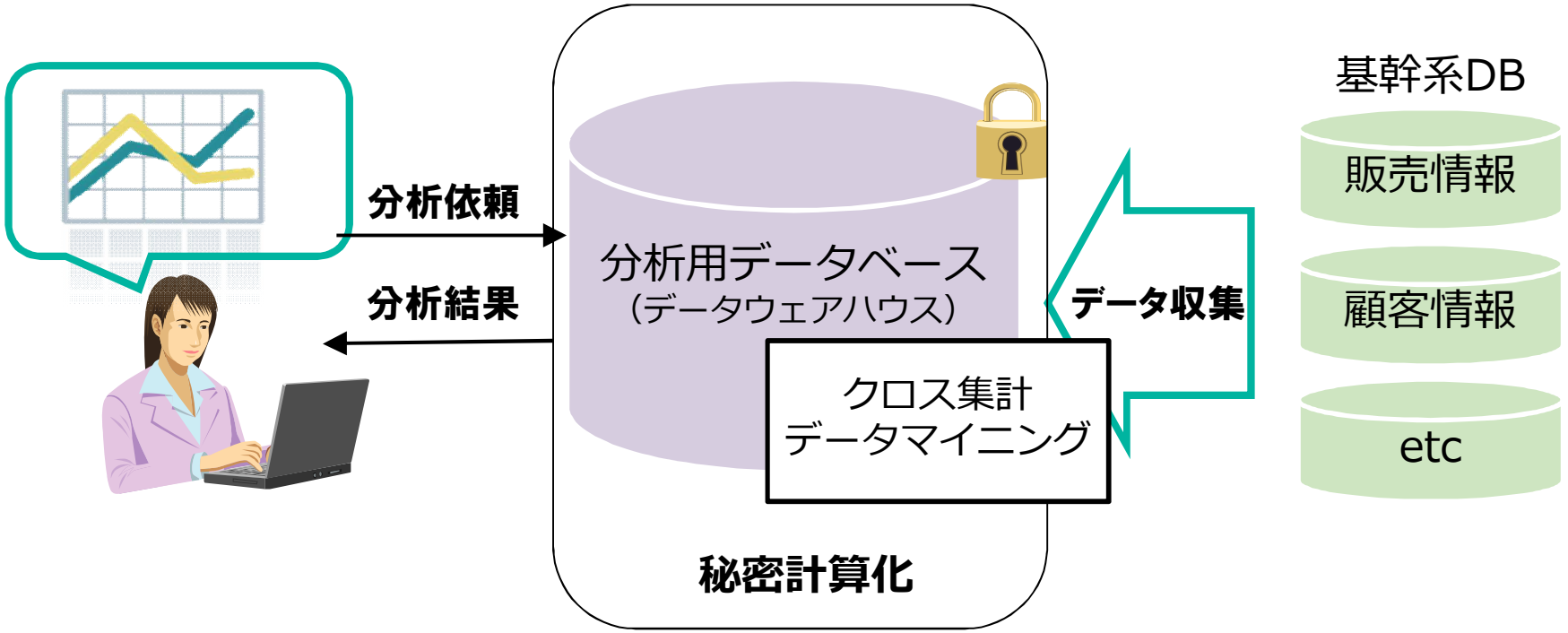
- Kerberos認証：シングルサインオンなどに利用される、共通鍵暗号を利用したネットワーク認証方式

  （サーバアクセスのためのチケットを発行）
- 秘密計算によって認証サーバがクライアントの秘密鍵を復元することなく認証チケット発行処理が可能
- 同時認証処理 **35,000件/sec** を達成
  - 大規模な組織で実用に耐えうる性能レベルを十分にクリア



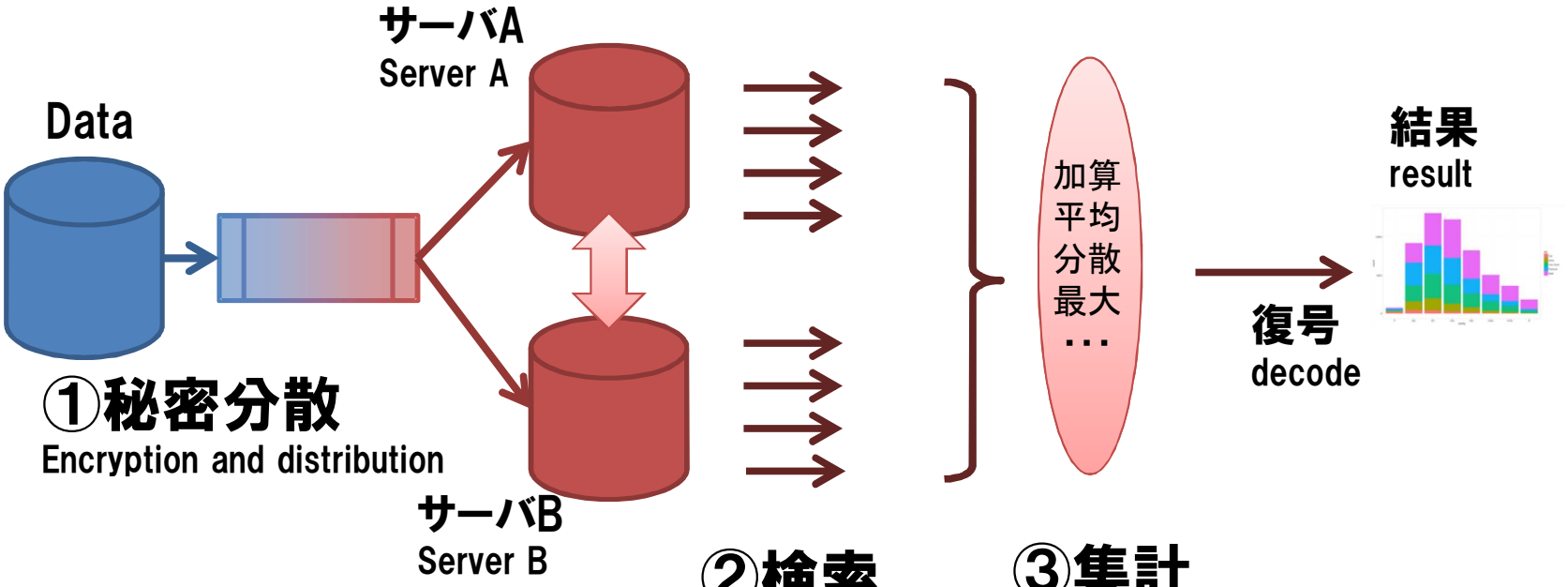
3．秘密計算による分析用データベースの実現

- データウェアハウスは、「過去」のデータを複数の基幹系システムから収集・蓄積・解析し，企業の意思決定のために活用される情報システム
- 秘密計算によって、従来は情報漏えいのリスクから集積することが困難であった機微な情報の活用も可能になることが期待される



３．検索処理の高速化

- マルチパーティ計算適用で課題となる、集計対象のデータを選別する検索処理について、検索可能暗号を利用する方式を開発
- 上記を用いて、秘密計算を適用した分析用データベースを世界で初めて実現
  - 暗号化なしと比較して6倍のサーバリソースで同程度の処理速度を達成
  - 1千万件のデータに対して、クロス集計を１分で実行（96コア利用時）

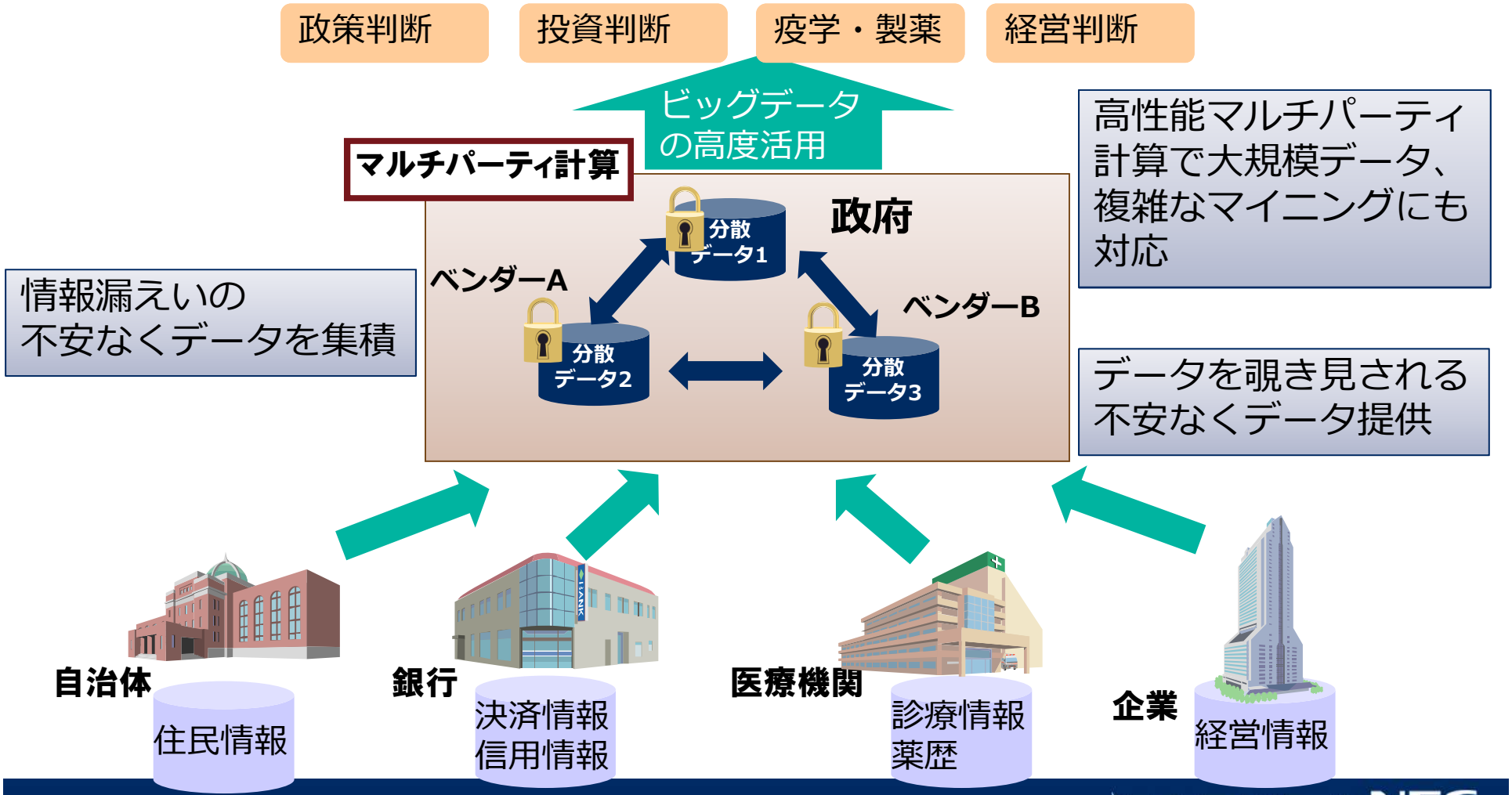


②検索可能暗号を用いて高速フィルタリング

③最新のマルチパーティ計算技術の適用

3．将来の活用想定例：ビッグデータ分析

- 行政、金融機関、医療機関、企業が保持する、様々なデータ活用のための
  セキュアな活用基盤



４．まとめ

秘密計算

- 検索可能暗号・準同型暗号
- **マルチパーティ計算（分散による秘匿）**

NECは世界をリードする、マルチパーティ計算の高速化に成功

- 基本アルゴリズムの改良により通信量と計算量の大幅な削減、秘密鍵を秘匿したままの暗号化処理、Kerberos認証で実用性実証（従来の14倍の高速化）
- 秘密計算による分析用データベースプロトタイプを開発、暗号化なしとの比較で6倍のサーバリソース量で同程度の処理速度を実現

今後一層の性能向上、汎用化の研究開発を進めて、マルチパーティ計算による強固な情報漏えい防止の実用化を図る

- 研究課題
  - 高速な基本アルゴリズムの拡充（算術演算、浮動小数点演算など）
  - “秘密計算コンパイラ”　（通常のプログラムの“マルチパーティ計算化”を自動化）


Orchestrating a brighter world
NEC