資料5

\Orchestrating a brighter world NEC

# NECの考える分散システムとセキュリティ

2016年05月19日　日本電気株式会社

# 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。

# 目次

1. NECの考える分散システム
2. 分散システムの課題とセキュリティ
3. 分散システムを支える技術
    3.1「通信仮想化」技術
    3.2「自己学習型システム異常検知」技術
    3.3「秘密計算」技術
    3.4「秘密分散」技術

# 1. NECの考える分散システム

# IoT時代の到来：進化したデバイスがインターネットに繋がる

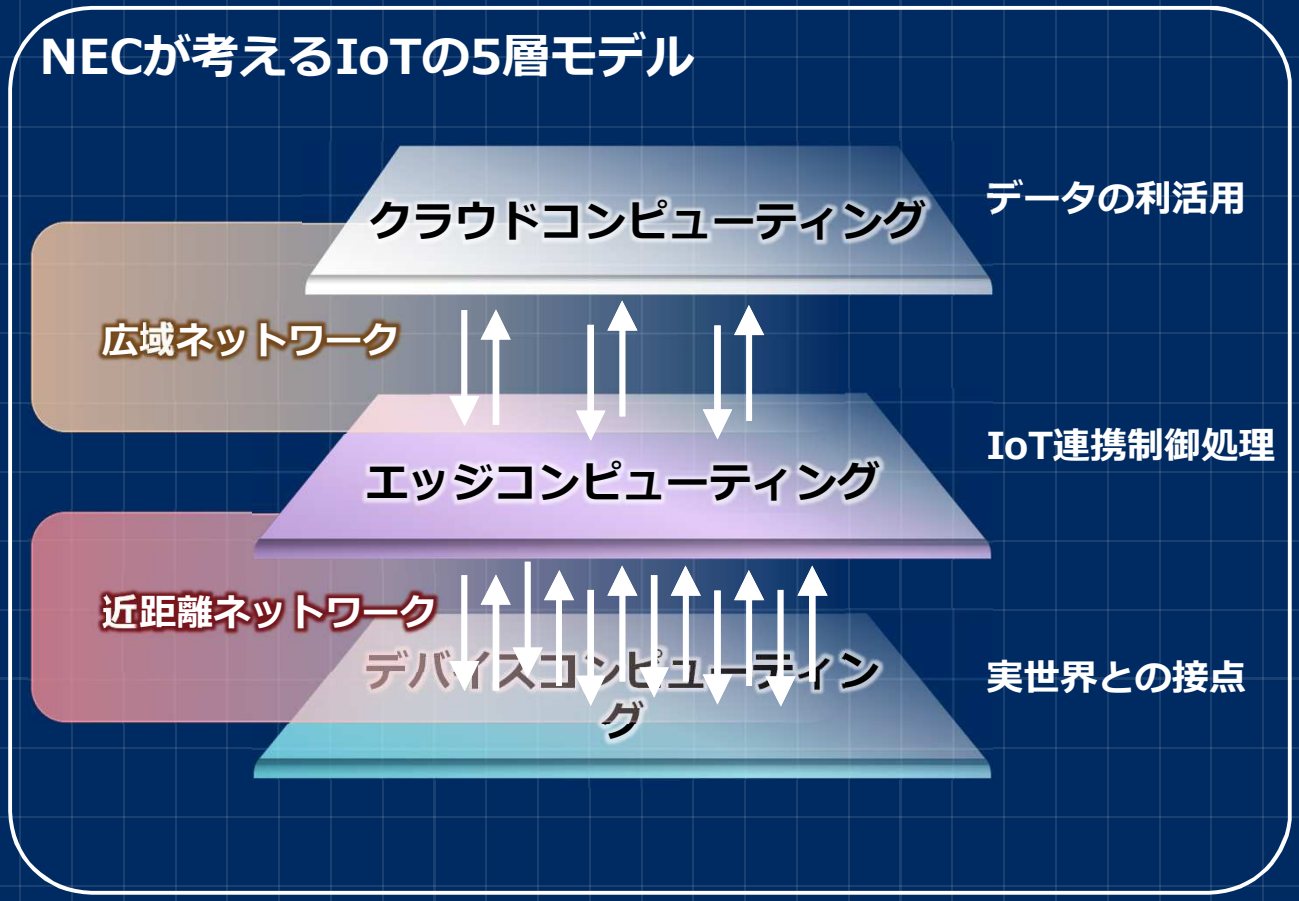

IoT：（Internet of things）の世界需要見通し308兆円

出典：JEITA：電子情報産業の世界生産見通し　（2020年）

# IoTで拡大する市場

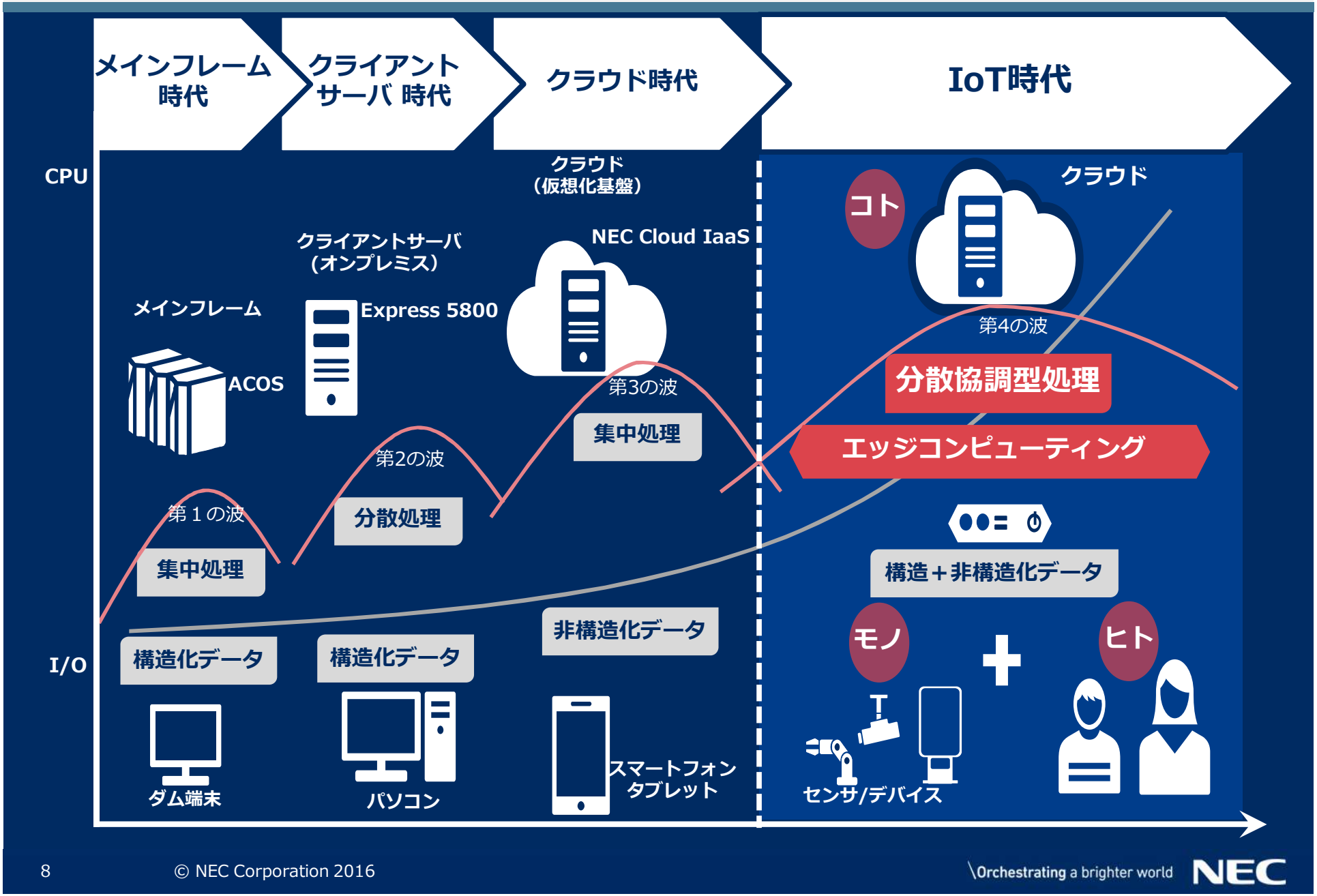
従来つながりが無かったモノ・コト同士が
容易につながり価値を生む時代へ

# ICTプラットフォームの強化ポイント



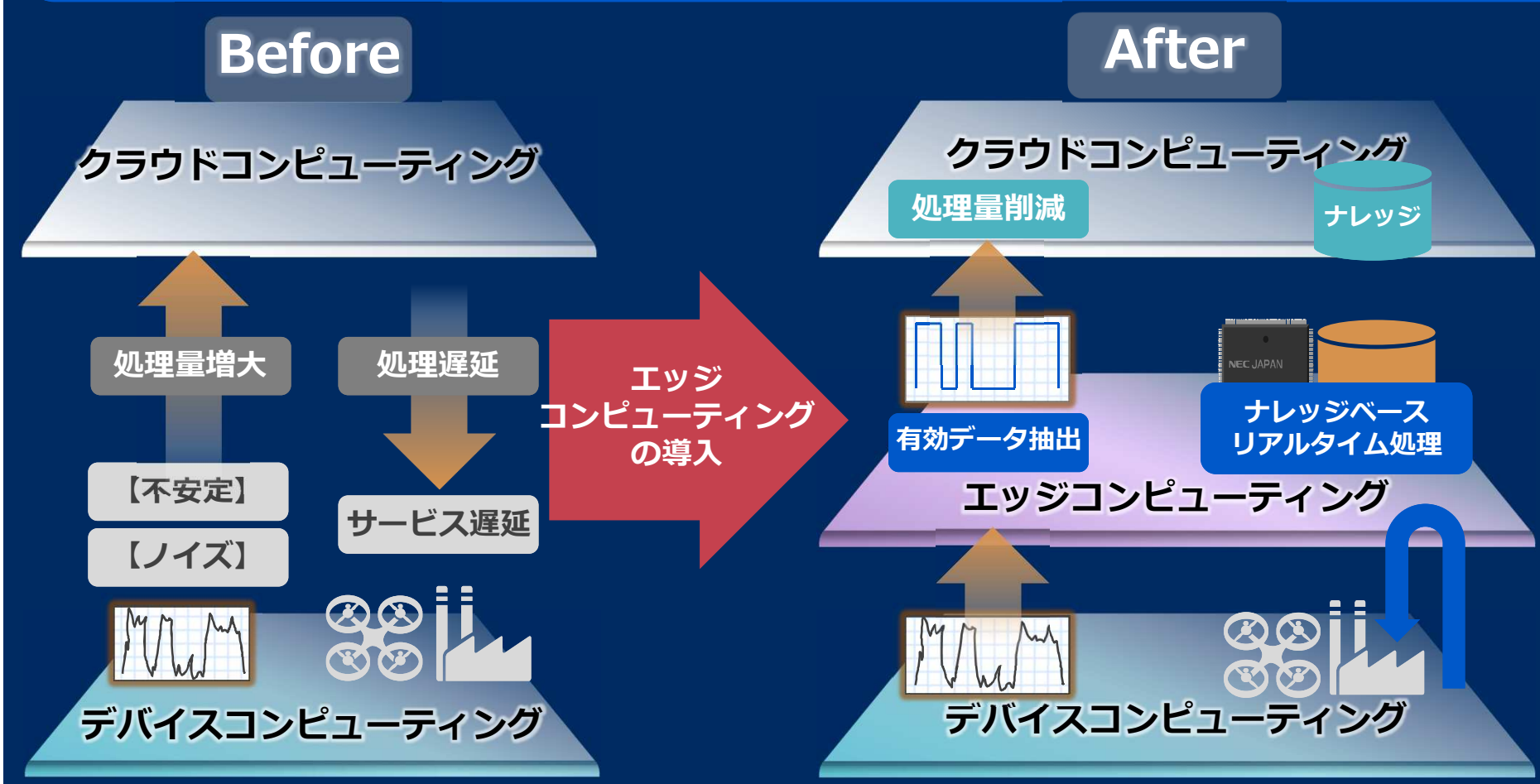

- 高速・高精度な分析処理
- 分散協調型処理
- デバイス仮想化
- セキュリティ
- 統合運用管理

# NECのICTプラットフォームの変遷



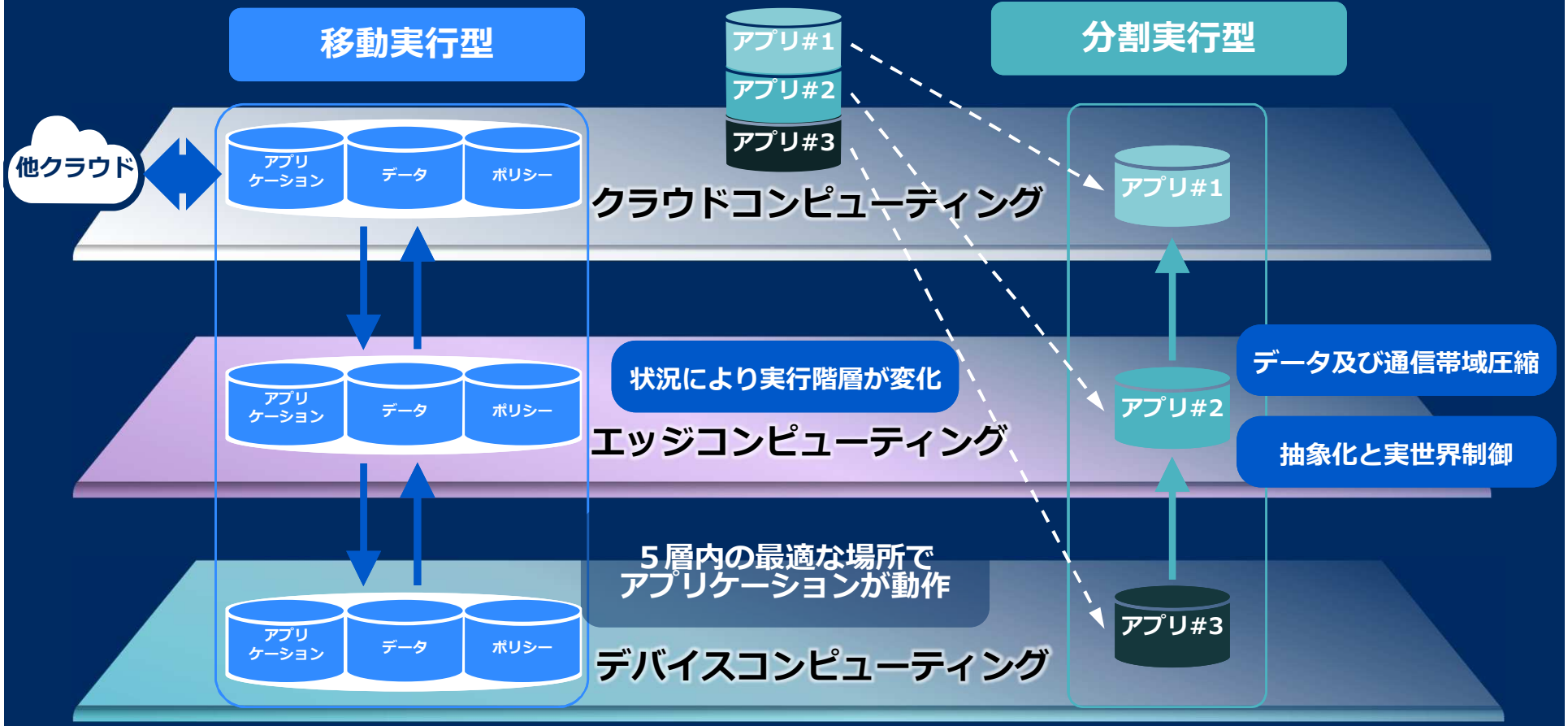
# エッジコンピューティングの必要性

●大量・不安定な実世界データが増大、一次処理でシステム負荷を削減
●ナレッジベースのリアルタイム処理を実現しシステム適応範囲を拡大



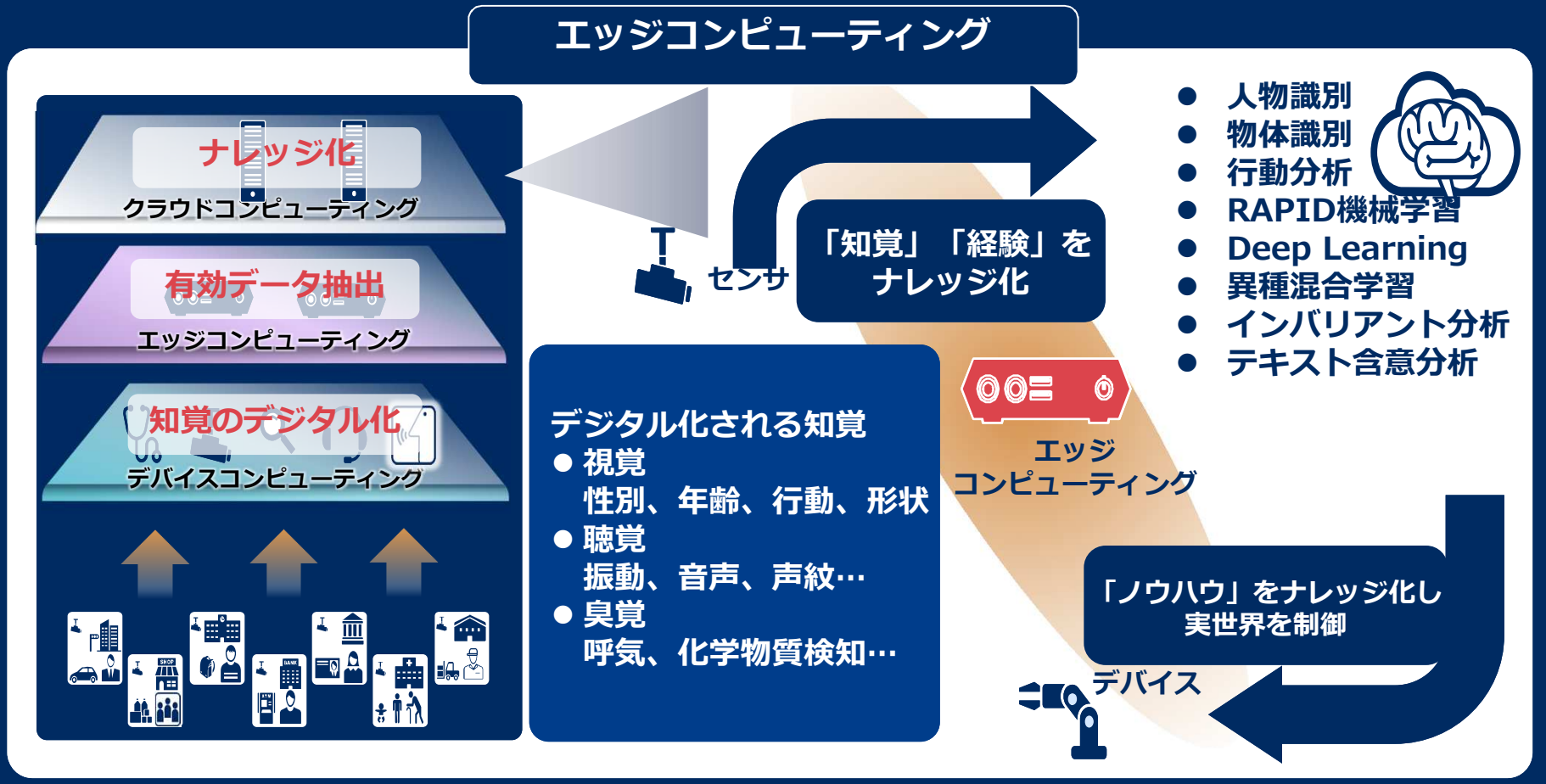
# 分散協調型処理の必要性

必要な場所に必要なサービスをリアルタイムに提供するには、データ特性やネットワーク状態に応じソフトウエアが最適動作する分散協調型処理が必要



# エッジコンピューティングの強化

●従来のM2Mに加えヒトの知覚や経験をデジタル化しナレッジへ
●モノとヒトのナレッジを融合し、新しい価値を提供



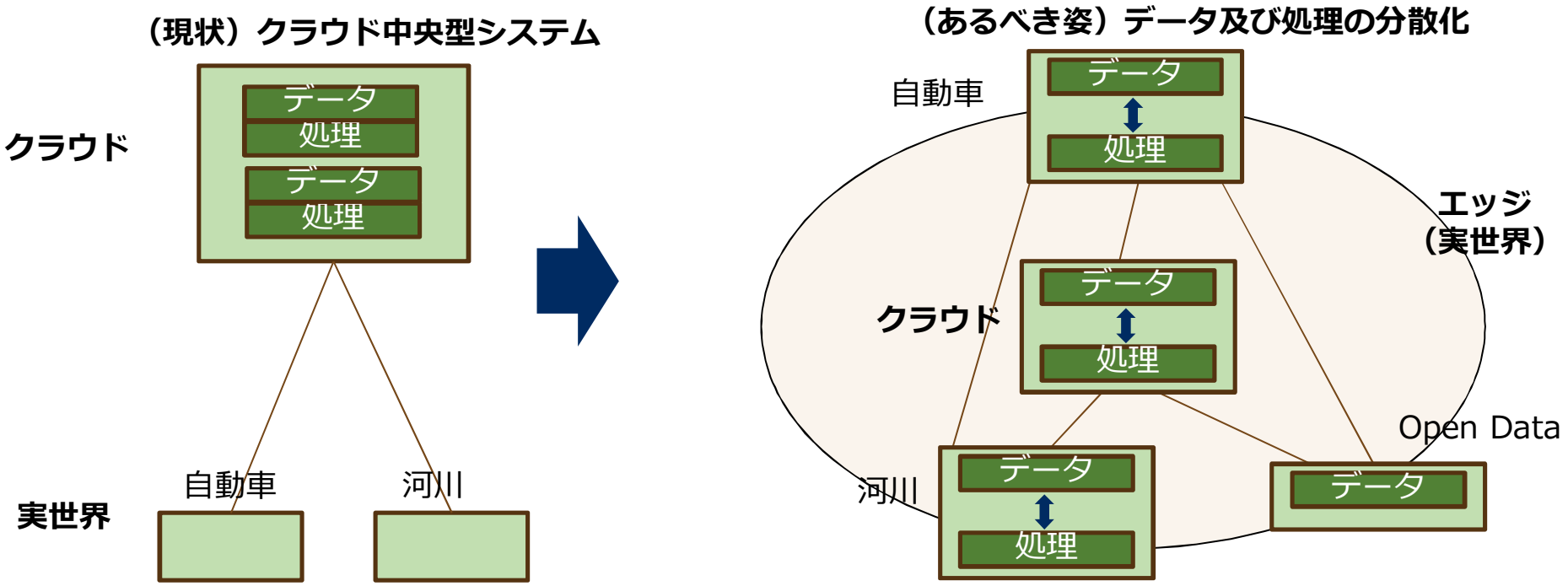
# 2. 分散システムの課題とセキュリティ

# 分散システムの必要性

IoTでは、従来のデータと処理のクラウド一極集中が成り立たない
結果、データも処理も分散化前提のシステムとなる

- IoTでは、扱う実世界や既存のデータ量が爆発的に増える
- 実世界でのリアルタイム性処理確保のため、データを実世界の近くに置かざるを得ない

（例）車両自動運転、局地災害時の避難指示など。




クラウドにデータ及び処理が集中

クラウドと実世界にデータ及び処理が分散

# データ及び処理の分散化によるメリット

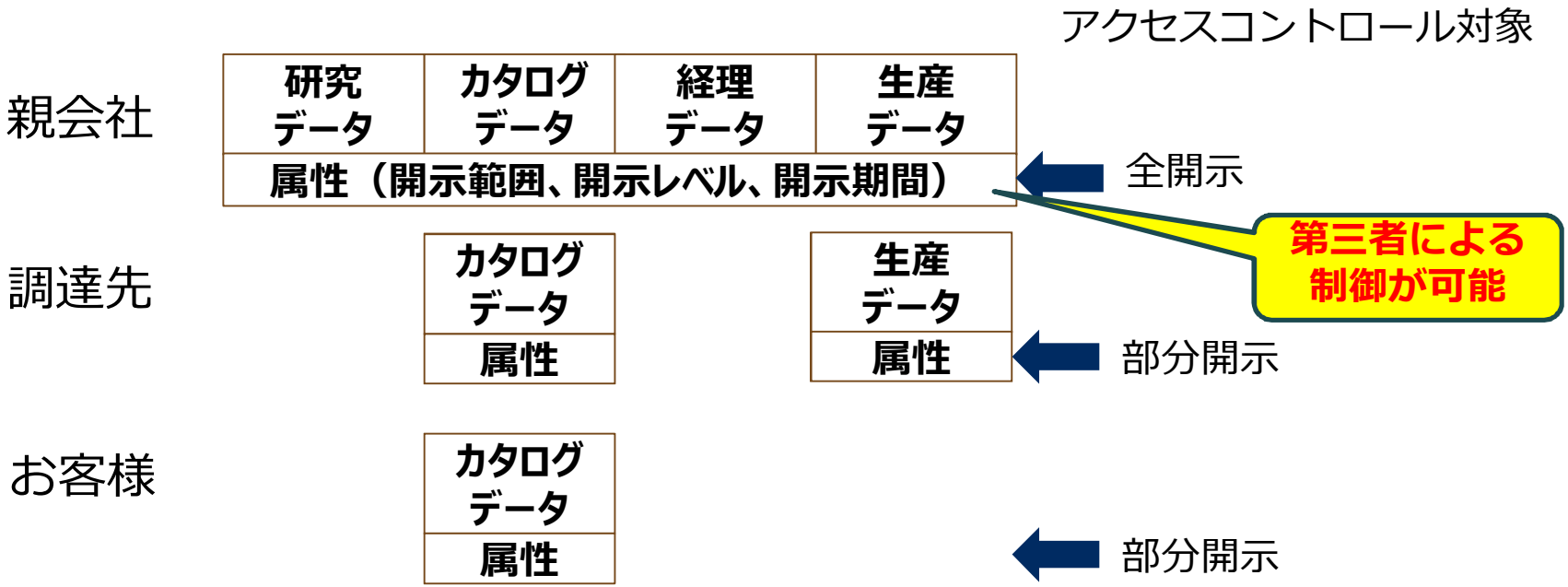
## 従来のシステムでは処理系とデータが一対一になっていた。

⇒データと処理が分散及び分離されることで、処理系とデータの一対一の関係がなくなる為、処理系に支配されないデータの利活用が可能となる。

（例）処理基盤を持つ勝者のベンダーがデータを寡占化

## データのオープンな利活用を促進できる可能性がある。

異業種間のデータの利活用が促進し、新しいサービスが生まれる可能性



# データ及び処理の分散化によるセキュリティリスクと対策

## セキュリティリスク

- 分散データ格納への要求に応えるには、分散システム一般の課題として、システムへの脅威増に対応が必要
- IoTインフラ上で分散サービスを構成した場合の主な脅威
  - 個別ノードへの攻撃・改ざん、乗っ取り
  - 悪意のあるサービス提供者
  - 悪意のあるサービスへの参加者
  - データの漏えい

## サービスでの対策１：システムの一部分への攻撃・改ざん対策

- 改ざんを受けた可能性のあるノードの自律閉塞
- 改ざん、乗っ取りのある可能性のあるノード・データの外部主導での排除

## サービスでの対策２：悪意のあるサービス提供者、参加者等の排除

- 悪意を持つ参加者等の数を圧倒的に上回る善意の参加者（ブロックチェーン）
- サービスのレベル、実装のセキュリティレベルなど信用度に関する認証局的役割を持つ新たなサービスの確立

**分散システムに具備すべき技術**

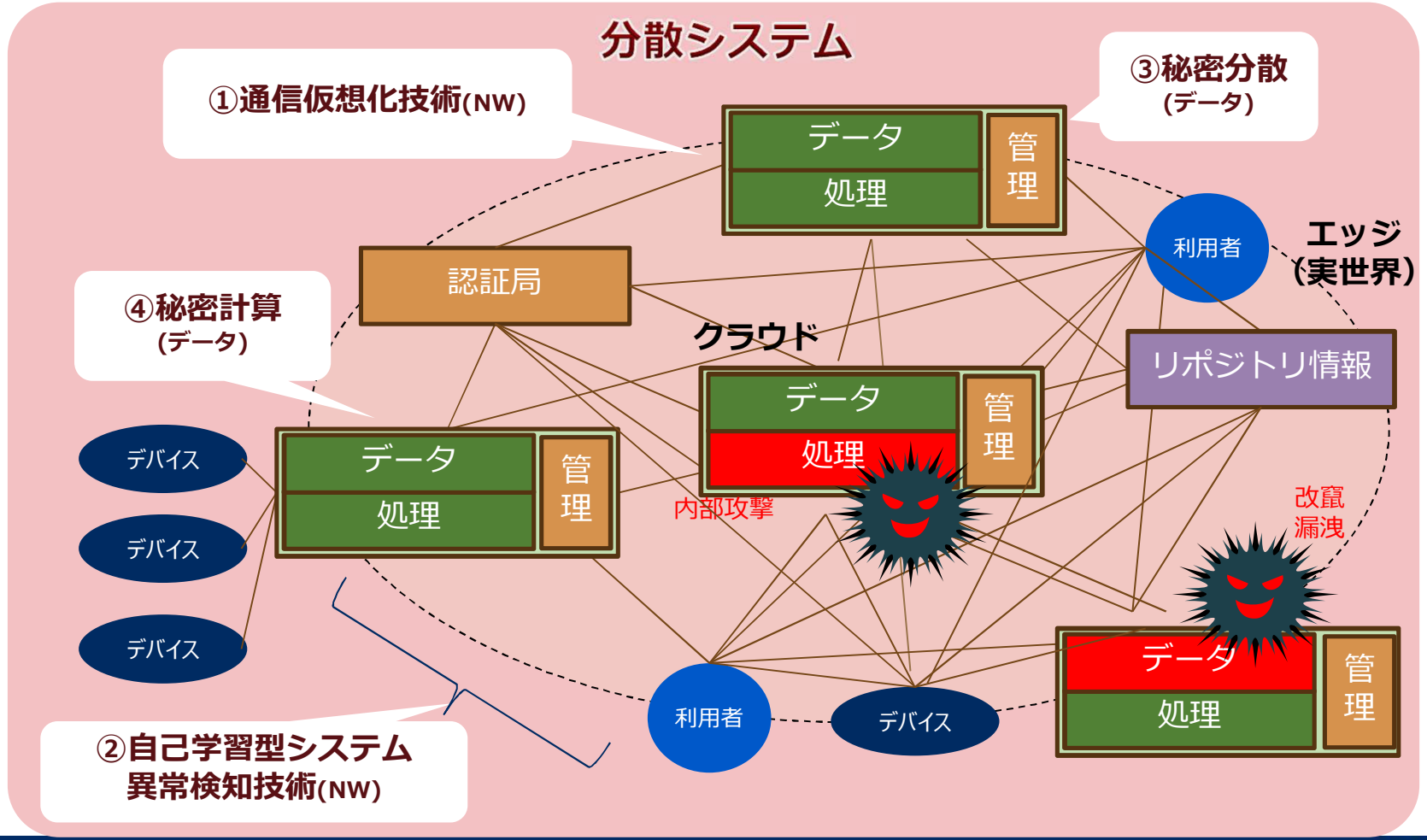
- **データ通信系と管理系を分離する技術**
- **システム全体の異常や攻撃を自律的に検知する技術**
- **セキュアにデータ及び処理を分散する技術**

# 分散システムの課題とセキュリティ

**①データ通信系と管理系を論理的に分離する通信仮想化技術**

**②システム全体の異常や攻撃を自律的に検知可能とする自己学習型システム異常検知技術**

**セキュアにデータ及び処理を分散する技術**
③データを分散する**秘密分散**
④集めないで計算する**秘密計算**

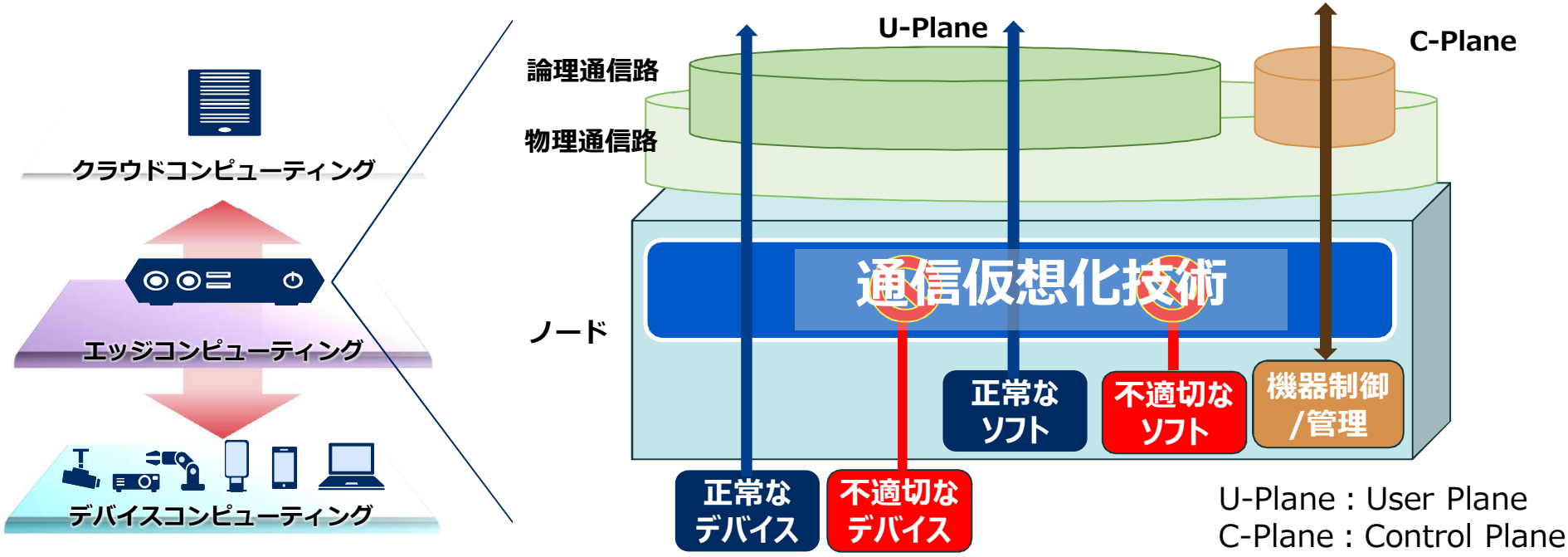


# 3. 分散システムを支える技術

# 3.1. 通信仮想化技術

**各ノードはデータ保存や分散処理（アプリ）など複数の役目を担う**
**悪意あるノードを完全に隔離すると、これらの正常な機能も停止する**

**C-Plane/U-Planeを分離、悪意あるデータ通信を隔離しながら**
**ノードを制御可能な通信仮想化技術の確立が重要**




U-Plane : User Plane
C-Plane : Control Plane

NWをソフト制御できるOpenFlow技術などの活用が必要
分散システムの制御には、認証局やリポジトリ情報の確立が合わせて必要

# 3.2.自己学習型システム異常検知技術

## 過去に発生した攻撃の経験を基とした「マルウェアの感染を防ぐ」アプローチは限界

（例）

- 「パターン・マッチ」による対策
- 「振る舞い検知」による対策
- 「サンドボックス」による対策

→ 攻撃者は常に新しい攻撃手法を開発。
常に後手に回った対策しか行えない。

## パラダイムシフトをもたらす新しいアプローチ

**●システムの通常の動作を完全に把握し、通常とは異なるシステム動作から攻撃を検知**

**従来のアプローチ**

過去に受けた攻撃の経験を
基にマルウェアの感染を防ぐ

→

**新しいアプローチ**

マルウェアに感染してしまうことを前提に
サイバー攻撃の知識を用いることなく、
未知攻撃を検知し被害発生前に対策

# 3.2.自己学習型システム異常検知技術

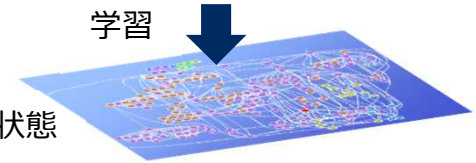
AI(人工知能)を活用して、
未知のサイバー攻撃を自動で検知・隔離する最新技術

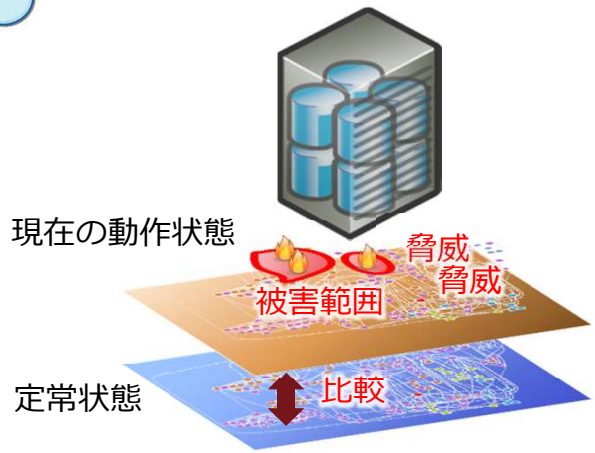
①システム全体の
動作状態から
**定常状態を学習**

②現在のシステム動作と
定常状態をリアルタイムで
比較・分析し、**異常を検知**

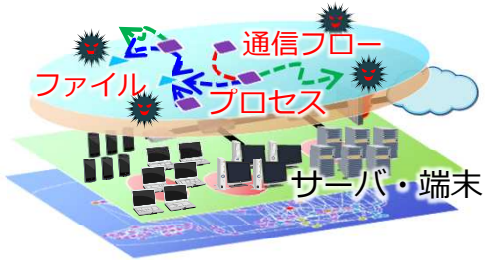
③被害範囲を特定、
ネットワーク
から**自動隔離**

プログラム起動やファイルアクセス
など軽量なログ収集




被害範囲の
自動特定・自動隔離




- **未知のサイバー攻撃**もリアルタイムに自動検知
- 従来の人手による分析の**1/10以下**の時間で被害範囲を特定

# （参考）3.2.自己学習型システム異常検知技術

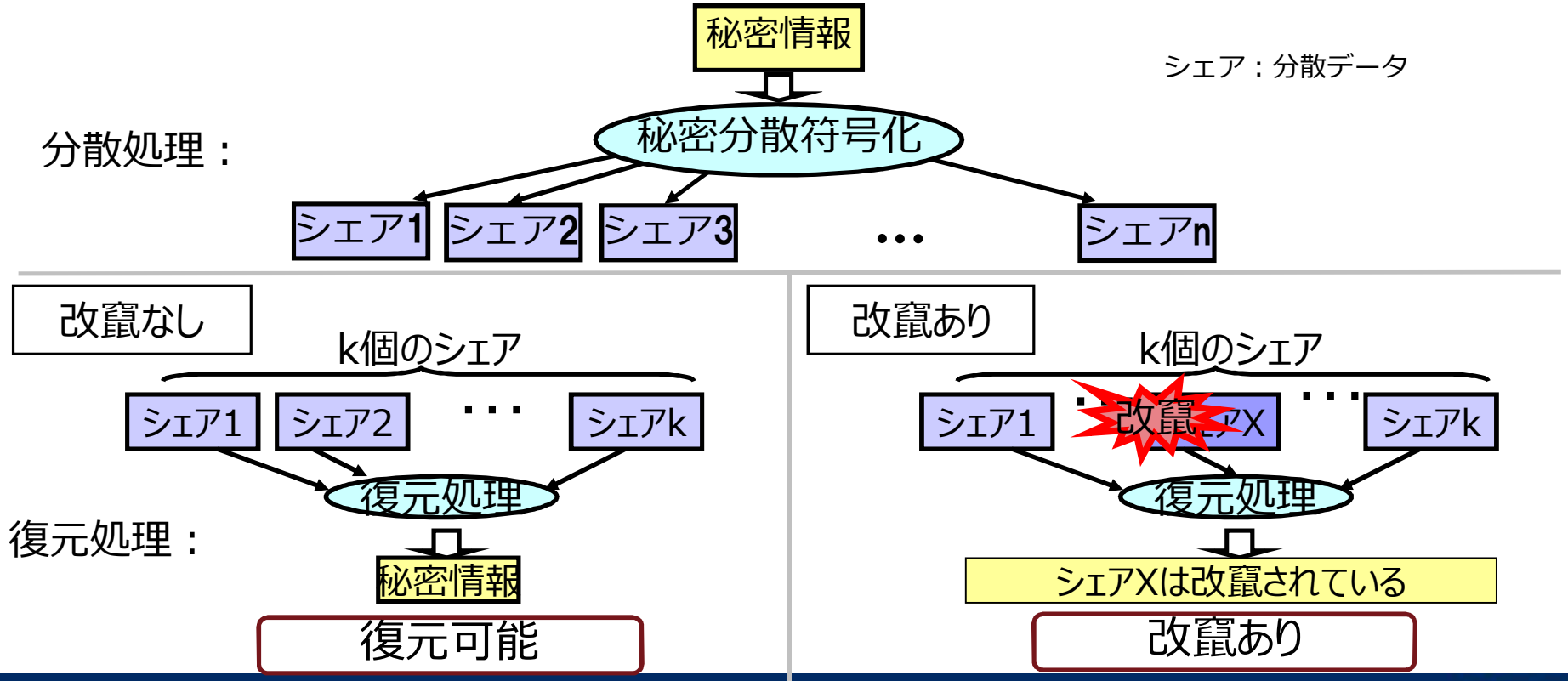
運用イメージ

## ホスト間のNWにおける定常動作と異常をリアルタイムに表示

# 3.3. 秘密分散技術：改竄検知機能付き秘密分散法

セキュアにデータを分散するための技術
データサイズ/処理能力と、ユースケースやサービスとの整合性の確認必要

- 機密性：一定数以下のシェアが漏洩したり盗難されても、元の情報の秘密は完全に保証
- 可用性：一定数以下のシェアが紛失したり破損しても、残りのシェアから秘密情報を復元
- **保全性：改竄されたシェアが含まれていても，その事実を検知できる**



# 3.4. 秘密計算（セキュアマルチパーティー計算）

分散システムへの適用には、処理分散量と実行処理時間の相関を取り、
サービス別のSLA(※)の達成検証が必要

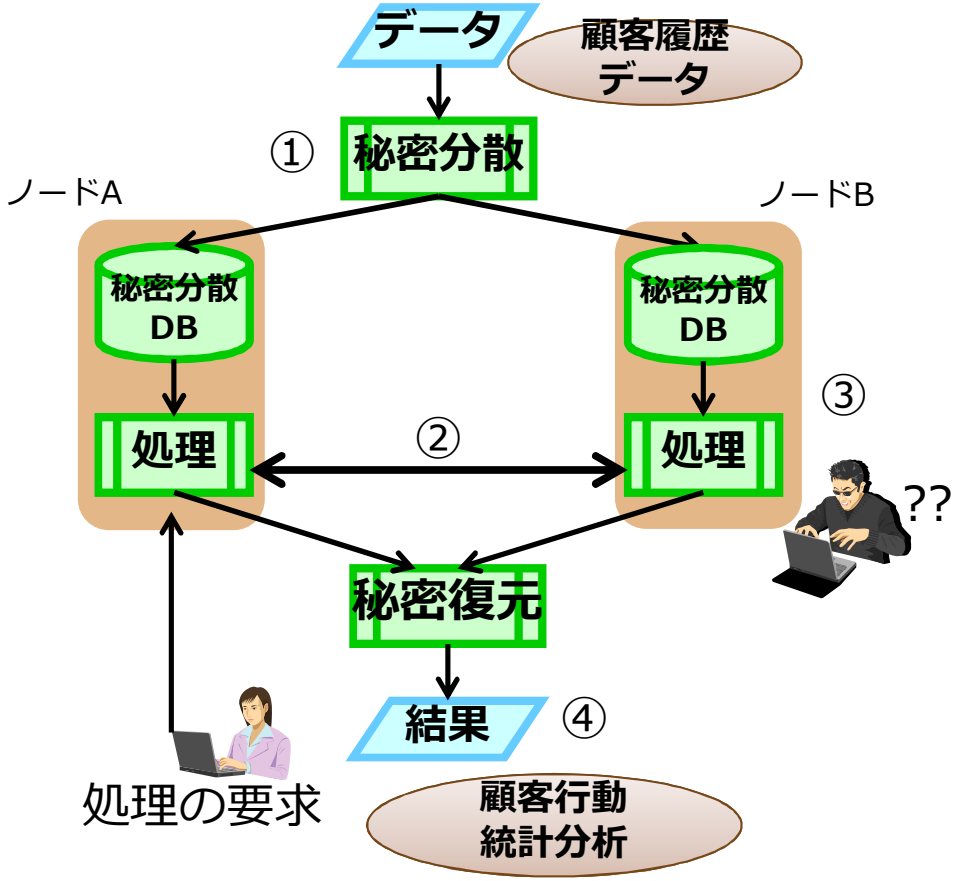
## データを暗号化したまま、ノードが共同で計算する方式

①秘密分散によりデータを秘匿

②互いに通信しながら、合意した任意の処理を分散実行

③処理中のデータからは元のデータも処理結果も完全に秘密

④秘匿された処理結果の復元により、処理結果のみを取得可能




※SLA：Service Level Agreement


Orchestrating a brighter world
NEC