資料2-3

NTTコミュニケーションズの スマートヘルスケアにおける プライバシー強化関連技術に関する取り組み

NTTコミュニケーションズ株式会社
ビジネスソリューション本部 スマートワールドビジネス部
櫻井 陽一

NTT Comが描く、Smart Healthcareのビジョン

日本の医療ヘルスケアを取り巻く社会的課題を解決することを目的として、予防・治療・ケアにいたる各ステージにおいてデータを収集・蓄積、さらに分析・活用することで新たなヘルスケアサービスを提供し医療プロセスの革新やデータ利活用による新たな付加価値を創造します。

プレシジョンヘルスケア
（予防）

プレシジョンメディスン
（治療）

プレシジョンケア
（高齢者ケア）

豊かな生活（= Smart Life）の実現

医療機関

▶治療歴の正確な把握・診療への活用
▶服薬歴の把握・重複処方の防止

健保組合・健康経営企業

▶疾病リスク予測
▶社員の健康増進

製薬会社・医療研究機関

▶創薬
▶医療技術革新

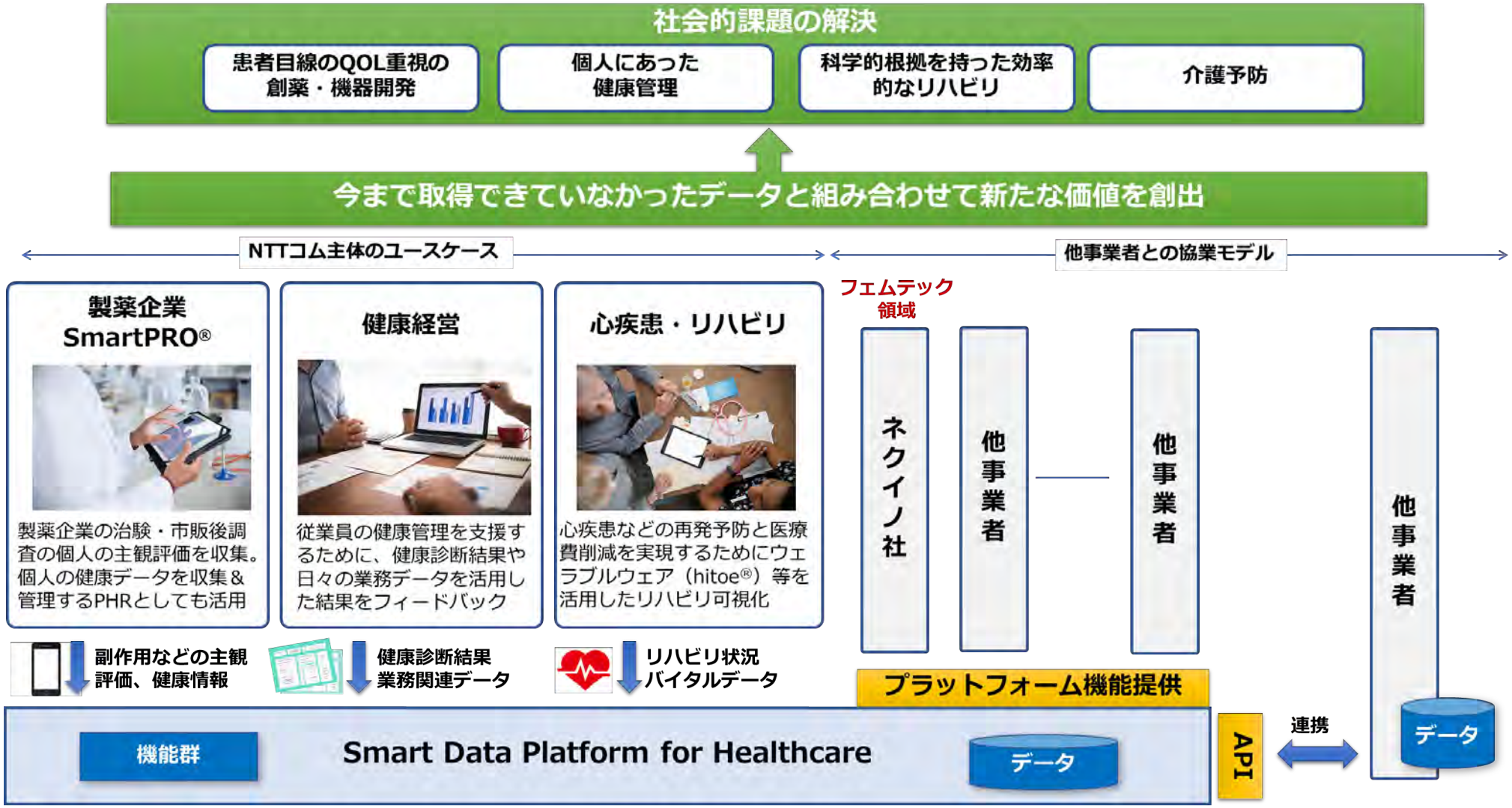
食品会社・保険会社

▶新たな健康サービスの開発

Smart Data Platform for Healthcare

妊娠期から高齢期までのライフコースデータ

NTT Comが描く、Smart Healthcareのビジョン



Smart Data Platform for Healthcareについて

データを安全に収集＆保管、本人の動的な同意取得管理、秘密計算・匿名加工などのデータ統計処理に必要な機能を具備しており、医療ヘルスケアデータなどの機微なデータを利活用したサービス提供が可能です。

医療サービス

ヘルスケアサービス

商品開発

生活習慣病リスク予測　/ゲノム×健診データ疾患リスク解明　/リハビリ活動量見える化　　等

NTTコム提供 サービス

他事業者様 サービス

Smart Data Platform for Healthcare

ストレージ　セキュリティ　分析　他事業者連携(認証連携、API)

同意取得　認証認可　ID連携　秘密分散 秘密計算　匿名加工　データ正規化

他データ
(医療情報等)

連携

活動量　食事　バイタルデータ　OTC・サプリ服用　健診データ

診察データ　服薬データ　xxx　xxx　xxx

活動量　食事　バイタルデータ　服薬データ　xxx

ライフコースデータ

予防　治療　ケア

漏えい事件と機微情報の重要度の高まり

近年、ストレージへの攻撃が世界各国で発生しており、またゲノム情報から顔を再現できる時代になりつつあることから、機微情報の重要度はさらに高まっています。

【近年発生したデータ漏えい事例】

- **Amazon Web Servicesへの攻撃**
  - 米大手金融某社が顧客の基本情報と、一部社会保障番号や銀行口座番号が、AWSへの攻撃から不正取得されたことを発表した

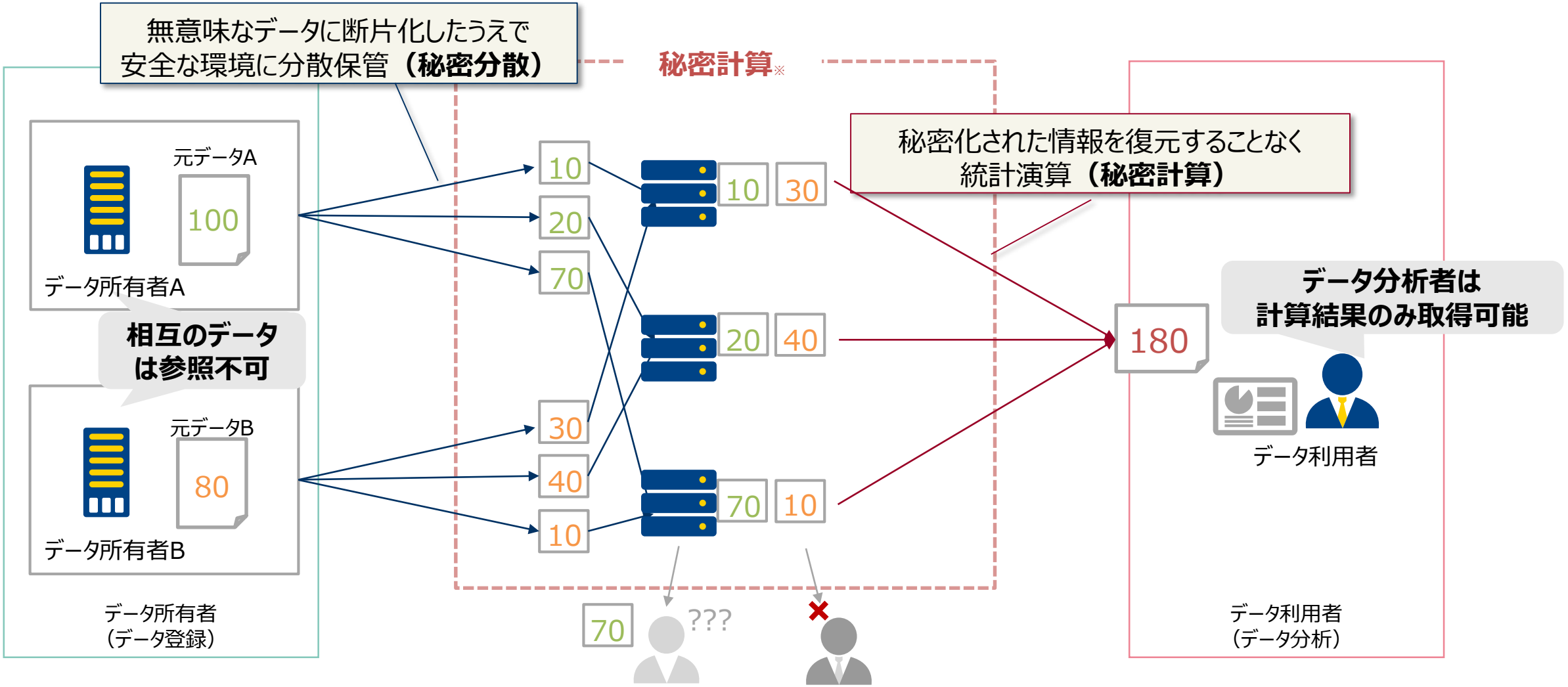
- **2800万人の生体認証情報が流出**
  - 韓国セキュリティサービス事業者が管理する指紋や顔写真を含む生体認証情報2780万件が流出した

- **ゲノム情報から顔の容貌を再現可能な時代**
  - バイオテクノロジー企業の某社が身元不明のゲノム情報から顔の容貌を再現可能なアルゴリズムを発表した

【上段】容疑者はAWS元従業員と現地報道、米金融大手で1億件超の個人情報漏洩（日経XTECH）
<https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05628/>
【中段】Report: Data Breach in Biometric Security Platform Affecting Millions of Users（vpnMentor）
<https://www.fintechnews.org/report-data-breach-in-biometric-security-platform-affecting-millions-of-users/>
【下段】Researchers produce images of people’s faces from their genomes（The Economist）
<https://www.economist.com/science-and-technology/2017/09/09/researchers-produce-images-of-peoples-faces-from-their-genomes>

秘密計算（MPC:Multi-Party Computation）の概要

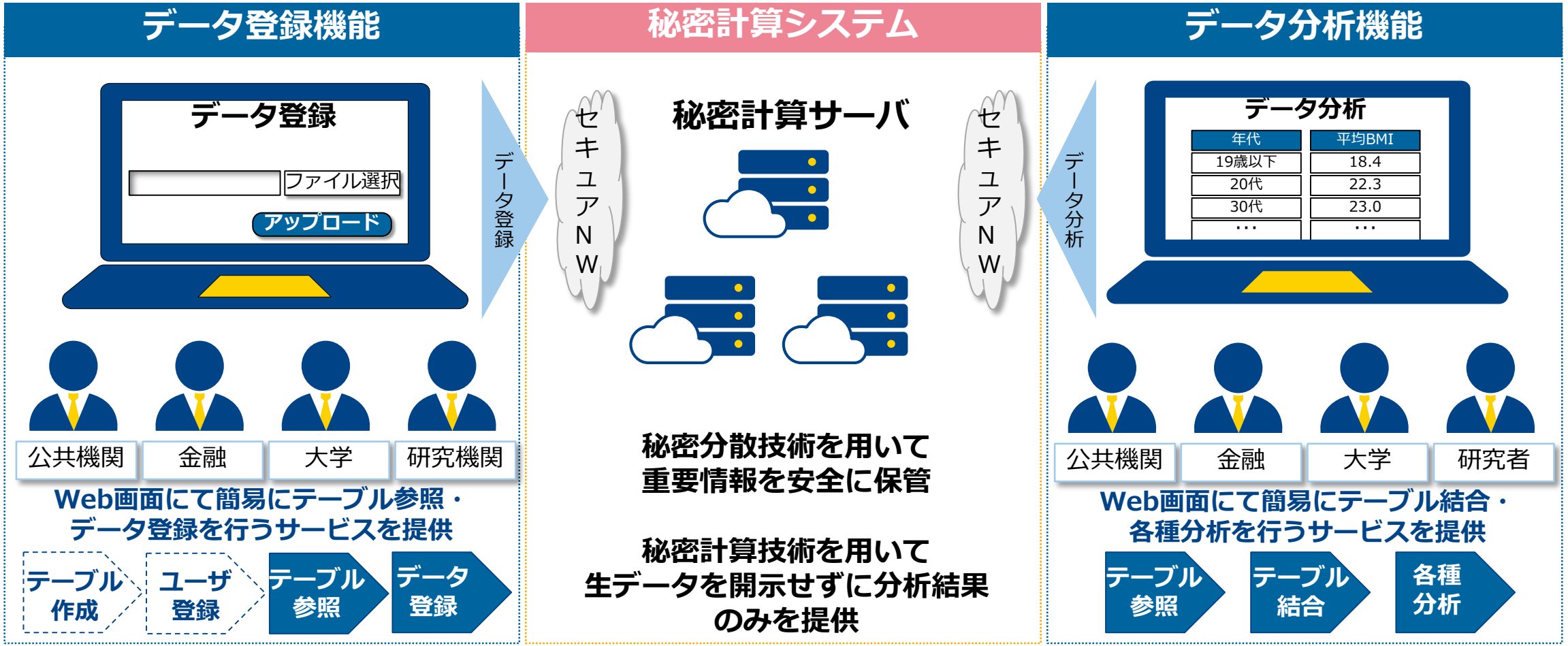
秘密分散技術とは、ある情報を意味のない複数の断片データに変換し分散保管する技術であり、
また、秘密計算（MPC）は秘密分散された情報を復元せずに演算処理可能な技術です。



秘密計算ソリューション「析秘」

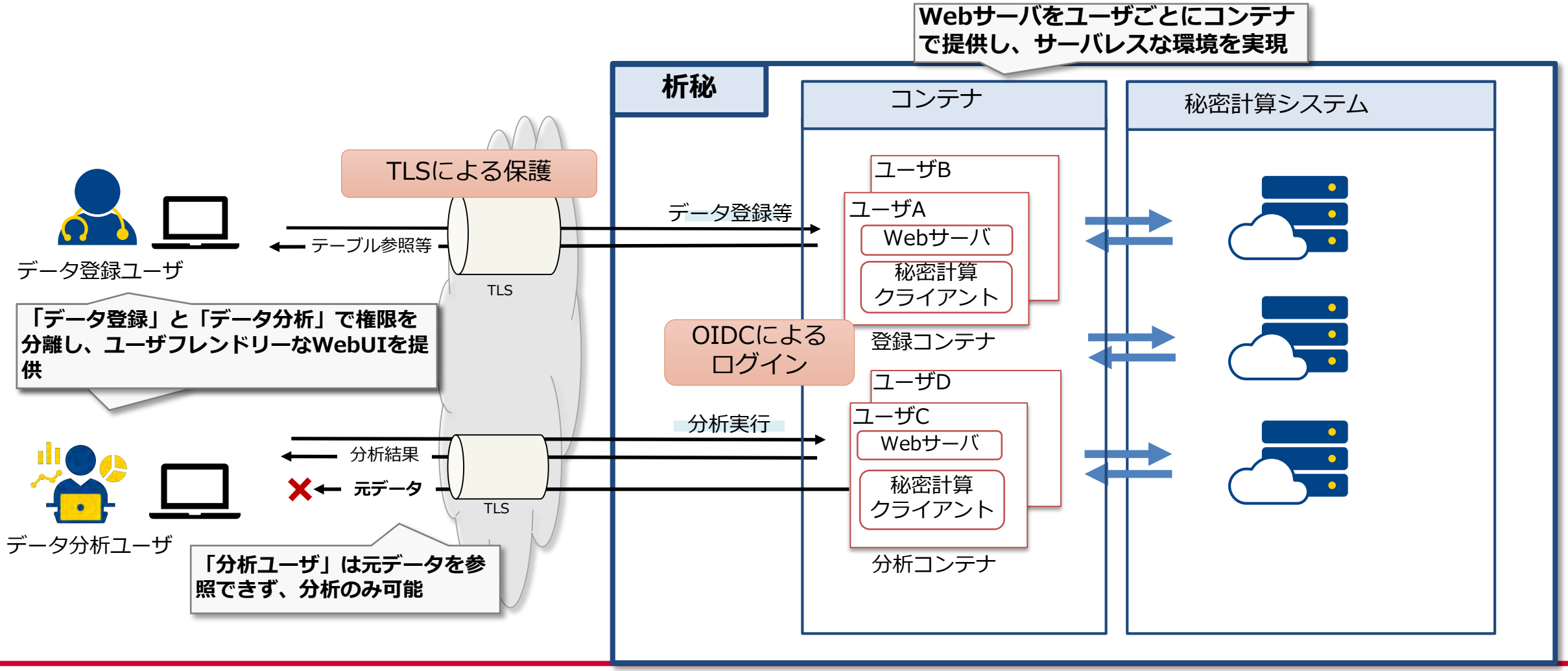
「析秘」は、重要情報を安全に分析できる秘密計算を、ブラウザを利用して操作することが可能なクラウドサービスです。

析秘サービス　全体イメージ



析秘の概要

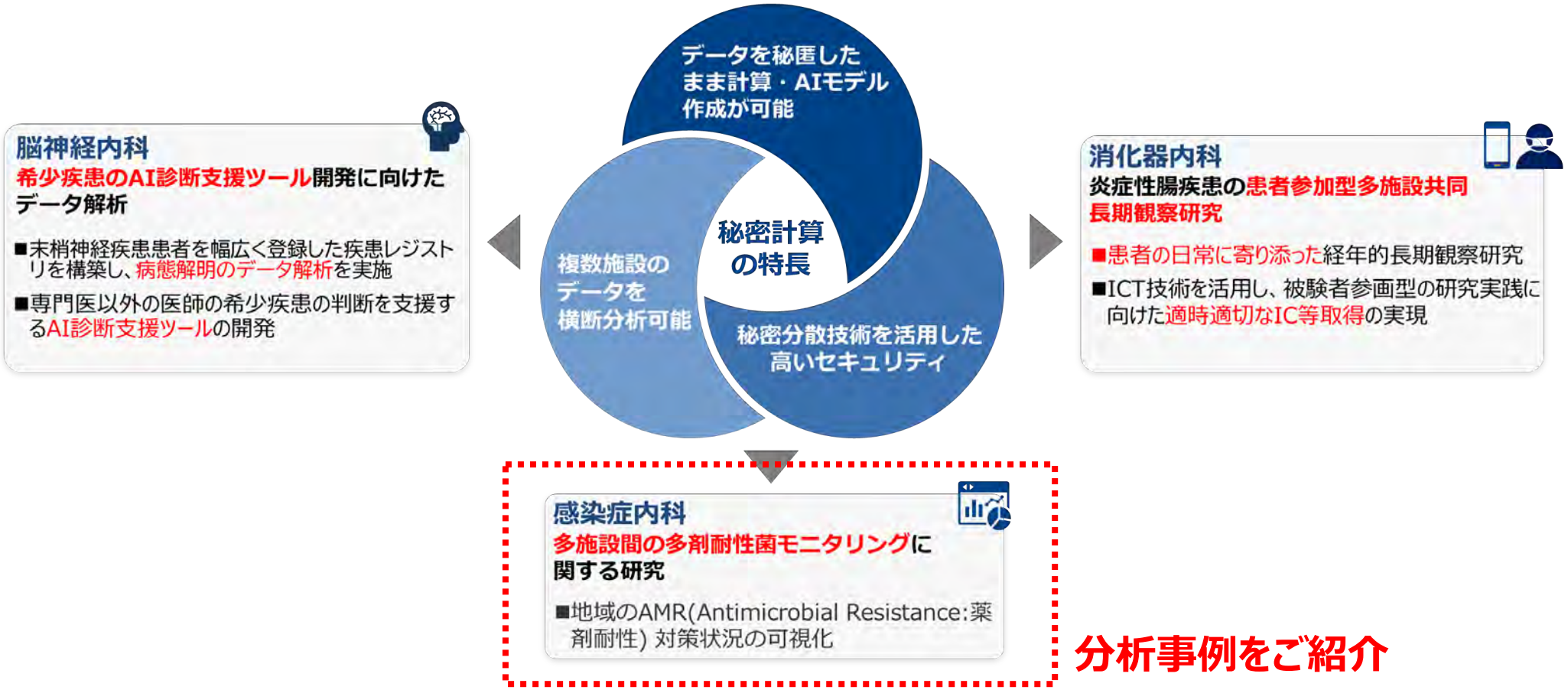
「析秘」ではデータ登録・データ分析をユーザフレンドリーに行えるWebUIを提供します。Webサーバはユーザ毎にコンテナで提供し、サーバレスのモダンアーキテクチャによるサービス化を実現しております。



医療業界における秘密計算技術の適用例

NTT Comは、高い機密性を有し、また情報を秘匿化したままで横断分析が可能な秘密計算技術を臨床研究等に活用する共同研究を千葉大学病院と進めています。

■ 2020年に共同研究に着手、現在**3診療科（消化器内科、脳神経内科、感染症内科）と研究**を実施



分析事例をご紹介

秘密計算の適用例：千葉大学病院との共同研究

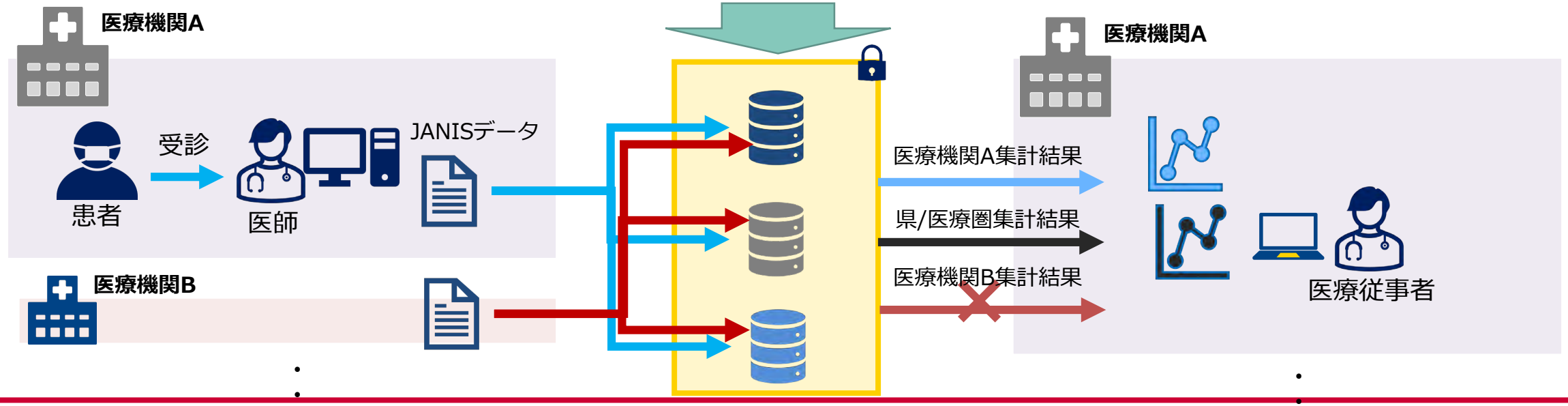
プライバシー保護
機密情報保護
横断分析

感染症内科：多施設間の多剤耐性菌モニタリングに関する研究
JANIS(院内感染対策サーベイランス)データを用いた2次医療圏ごとの薬剤耐性菌対策動向の可視化

薬剤耐性（AMR： Antimicrobial Resistance ）菌（耐性菌）における課題
- **耐性菌は、抗菌薬（抗生物質）に耐性を持つ菌**
- **耐性菌による2013年死亡者数は、世界規模で70万人**
- **何もしなければ2050年の死亡者数は、がんによる死亡数を超える**
- **必要のない抗菌薬の服用、自己判断による服用方法の変更が原因**
- **抗菌薬適正使用推進のための県全体、2次医療圏単位の耐性菌検出率等の資料がない**

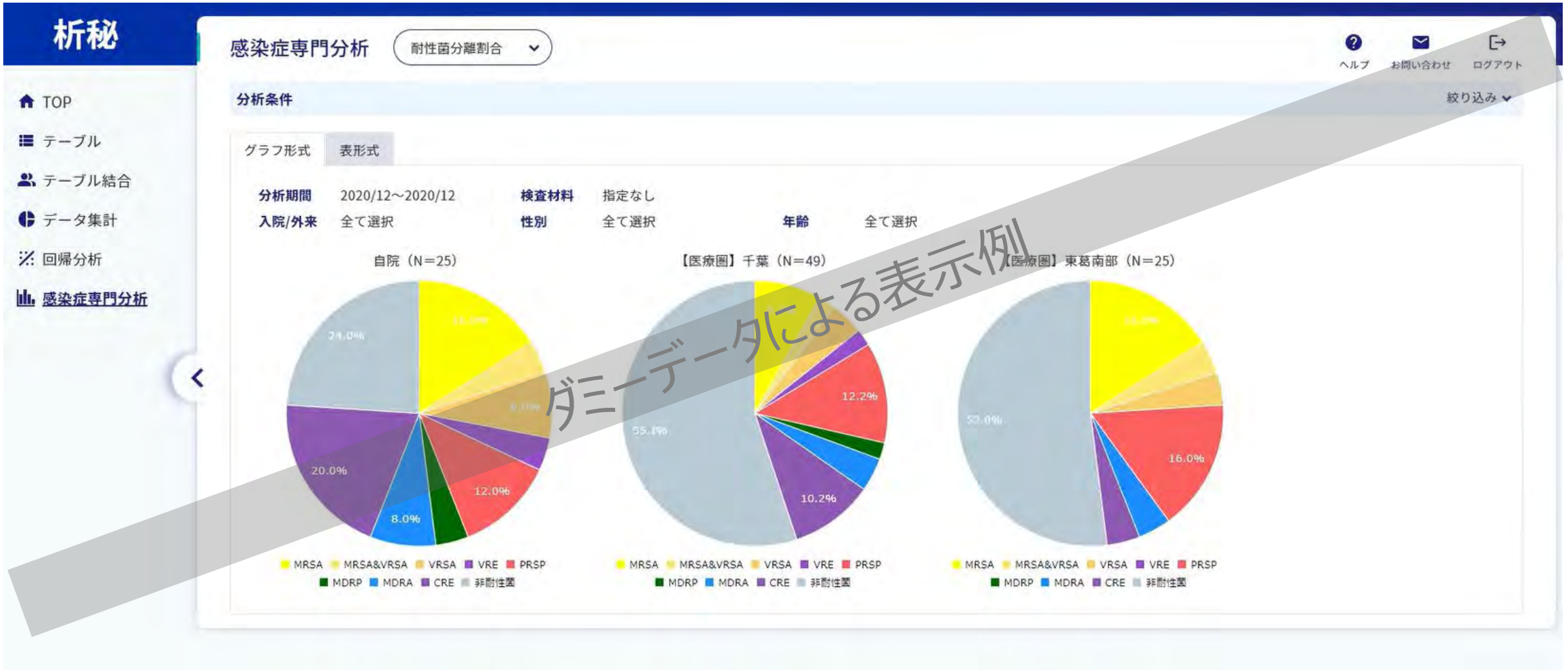
＋

各医療機関提出のJANISデータを使用するが、病院の詳細な発生状況を他医療機関に開示することは避けたい



秘密計算による分析事例（UIを用いた分析）

秘密計算技術を活用し、複数施設と連携して各医療機関のJANIS(院内感染対策サーベイランス)データを用いた
2次医療圏ごとの薬剤耐性菌分離割合の可視化を各医療機関のデータを秘匿化したまま実現しました。



今後のセキュリティ標準の動向

量子コンピュータの登場により暗号の標準は大きな変革期を迎えます。さらに、現在は解読できなくても
過去に遡って解読される脅威から、情報理論的に安全なセキュリティ技術への期待が高まっています。

- **量子コンピュータの登場に伴い、暗号の標準が変革期を迎える**
  - 米国立標準技術研究所（NIST）の暗号方式移行プラン

- **さらに、計算量的安全性によるセキュリティ技術への脅威も存在する**
  - 米某局のデータセンターでは世界の全人口分のデータを保存可能であり、
    今はデータを盗聴して保存し、将来高度な計算機を用いて過去の全データを解読する *“Store now, Read later”*

**どんな計算機を使っても解読不可能な情報理論的安全性を持った
セキュリティ技術への期待が高まる**

参考文献　：*NIST<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>*
CRYPTREC<https://www.cryptrec.go.jp/report/cryptrec-mt-1421-2019.pdf>

暗号の安全性の分類

量子暗号は、量子コンピュータに対する耐性だけでなく、今後いかなるコンピュータが登場したとしても
解読不可能な情報理論的安全性を有しています。

高

安全性

低*2

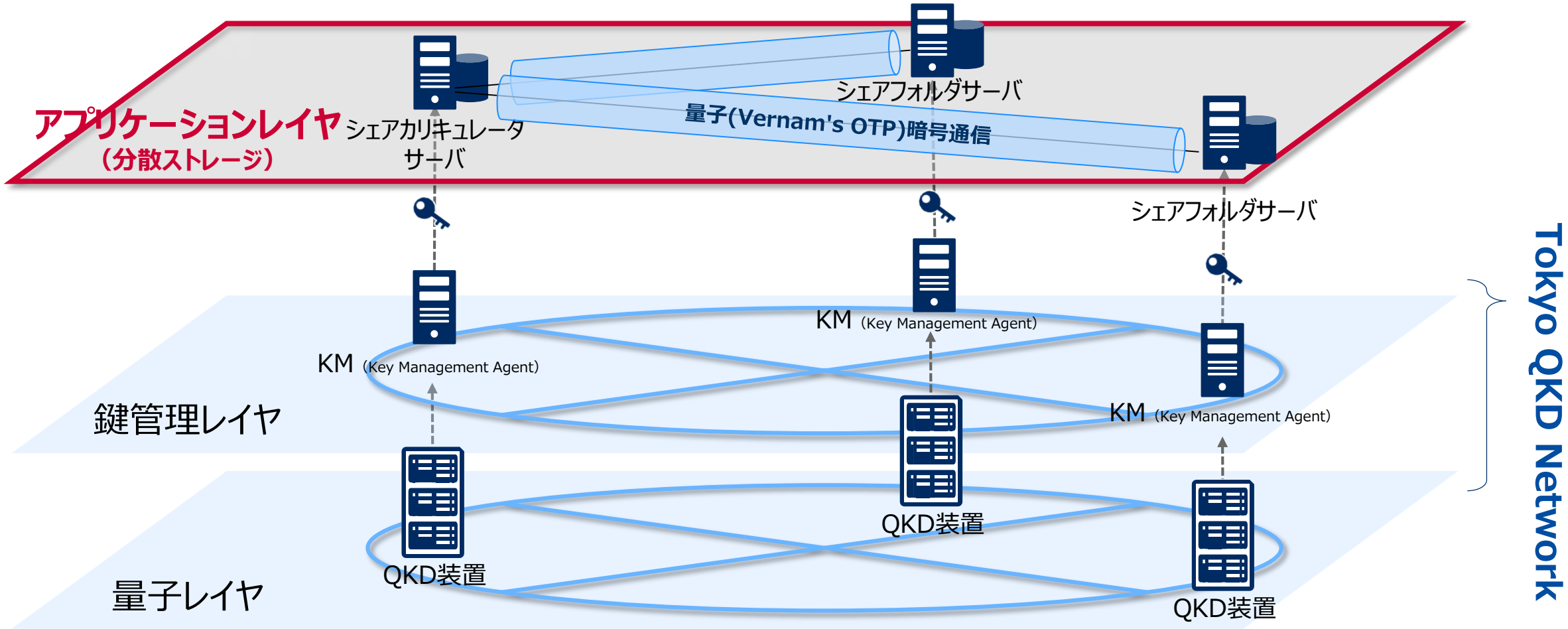
コンピュータの計算能力による分類	量子コンピュータへの耐性による分類	具体例
情報理論的安全 • いかなるコンピュータでも暗号を解けない - 無限に時間をかけても解けない • 危殆化しない		**量子暗号**、 秘密分散・計算*1
計算量的安全 • 現在のコンピュータでは暗号を解けない - 解読に3000年程度かかるので事実上解けない • 危殆化する - コンピュータの進化に合わせた定期的な暗号の更新が必須	**耐量子性を持つ** • 量子コンピュータでも効率的に解けない	共通鍵暗号、 格子暗号
	耐量子性を持たない • 現在のコンピュータでは効率的に解けないが量子コンピュータなら効率的に解ける	RSA、楕円曲線暗号、DSA

*1 乱数生成方法にも依存し、真性乱数を利用する場合
*2 便宜上低となっているが現状では十分に安全とされているレベル

NICT様との取り組み①

量子鍵配送ネットワークを活用した分散ストレージ

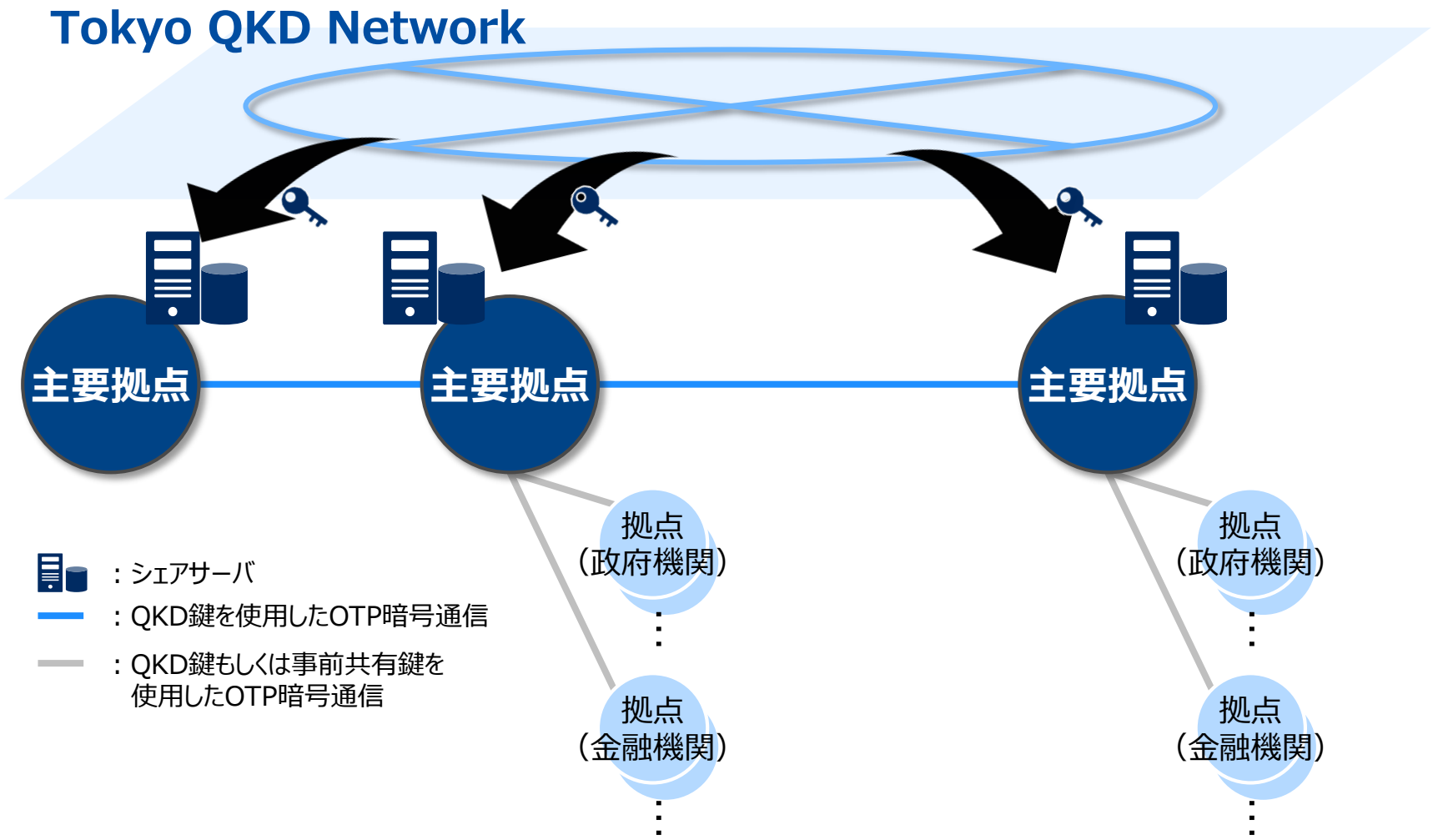
機微情報を保護可能な秘密分散技術に、Tokyo QKD Networkから供給される情報理論的に安全な鍵を用いた量子暗号通信(Vernam's OTP)を適用し、安全なストレージの実現に向けた実証実験を進めています。



NICT様との取り組み②

量子鍵配送網を活用した量子セキュアクラウド

量子鍵配送網上に構築した分散ストレージを活用し、官民を問わず多様な実証を可能とする量子セキュアクラウドの実現に向けてNICT様と取り組んでいます。量子セキュアクラウドへは政府機関、金融機関からの接続を想定しています。



量子暗号/量子セキュアクラウドの実用化に向けた期待

- 近年、ユーザの暗号化技術や暗号強度への意識が高まっており、クラウド化が進む中において
  国内企業が安心できる技術レイヤの必要性は高まっている。

- 様々なセキュリティ技術方式の中で、安全性、コスト、ユーザビリティのバランスが取れた実例や実績が
  実用化・導入の後押しとなる。

- 官民問わず利用可能な量子通信ネットワークのテストベッドである量子セキュアクラウドの実現によって、
  技術検証・実証が促進される。