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

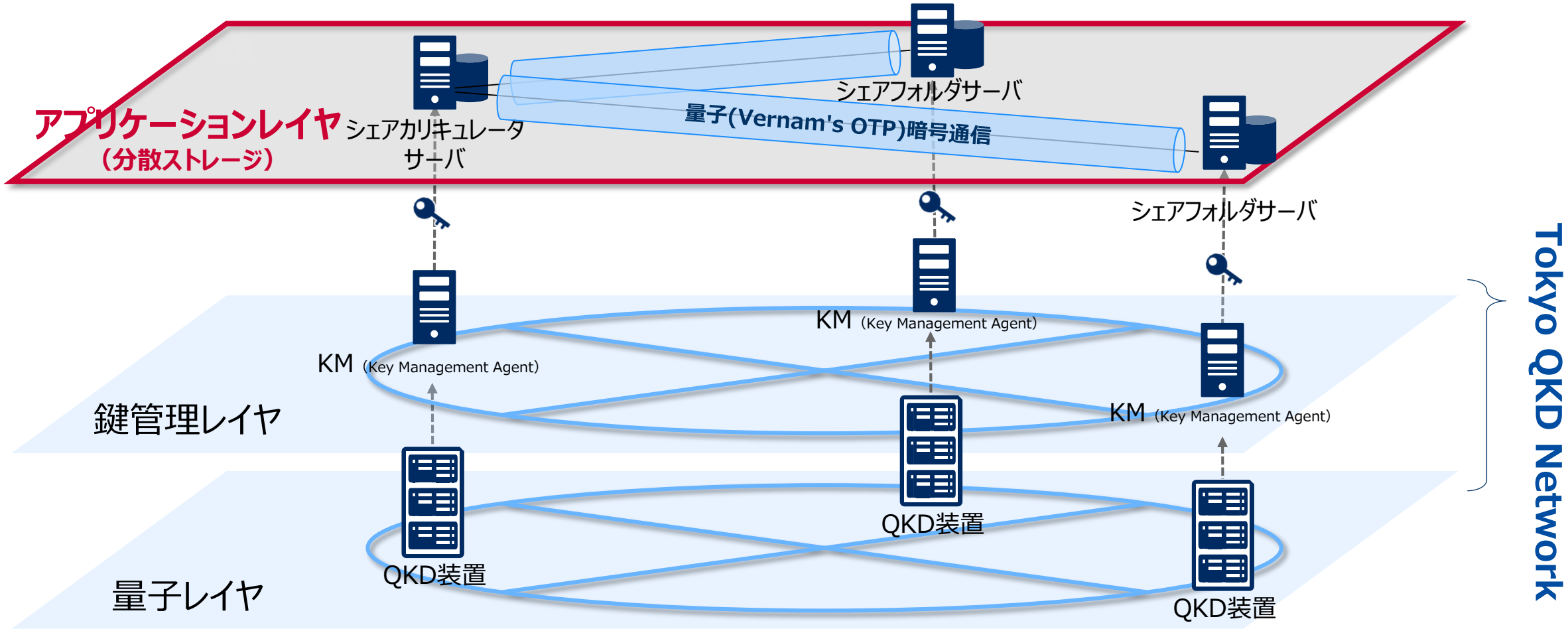
コンピュータの計算能力による分類	量子コンピュータへの耐性による分類	具体例
情報理論的安全 • いかなるコンピュータでも暗号を解けない - 無限に時間をかけても解けない • 危殆化しない		**量子暗号**、 秘密分散・計算*1
計算量的安全 • 現在のコンピュータでは暗号を解けない - 解読に3000年程度かかるので事実上解けない • 危殆化する - コンピュータの進化に合わせた定期的な暗号の更新が必須	**耐量子性を持つ** • 量子コンピュータでも効率的に解けない	共通鍵暗号、 格子暗号
	耐量子性を持たない • 現在のコンピュータでは効率的に解けないが量子コンピュータなら効率的に解け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

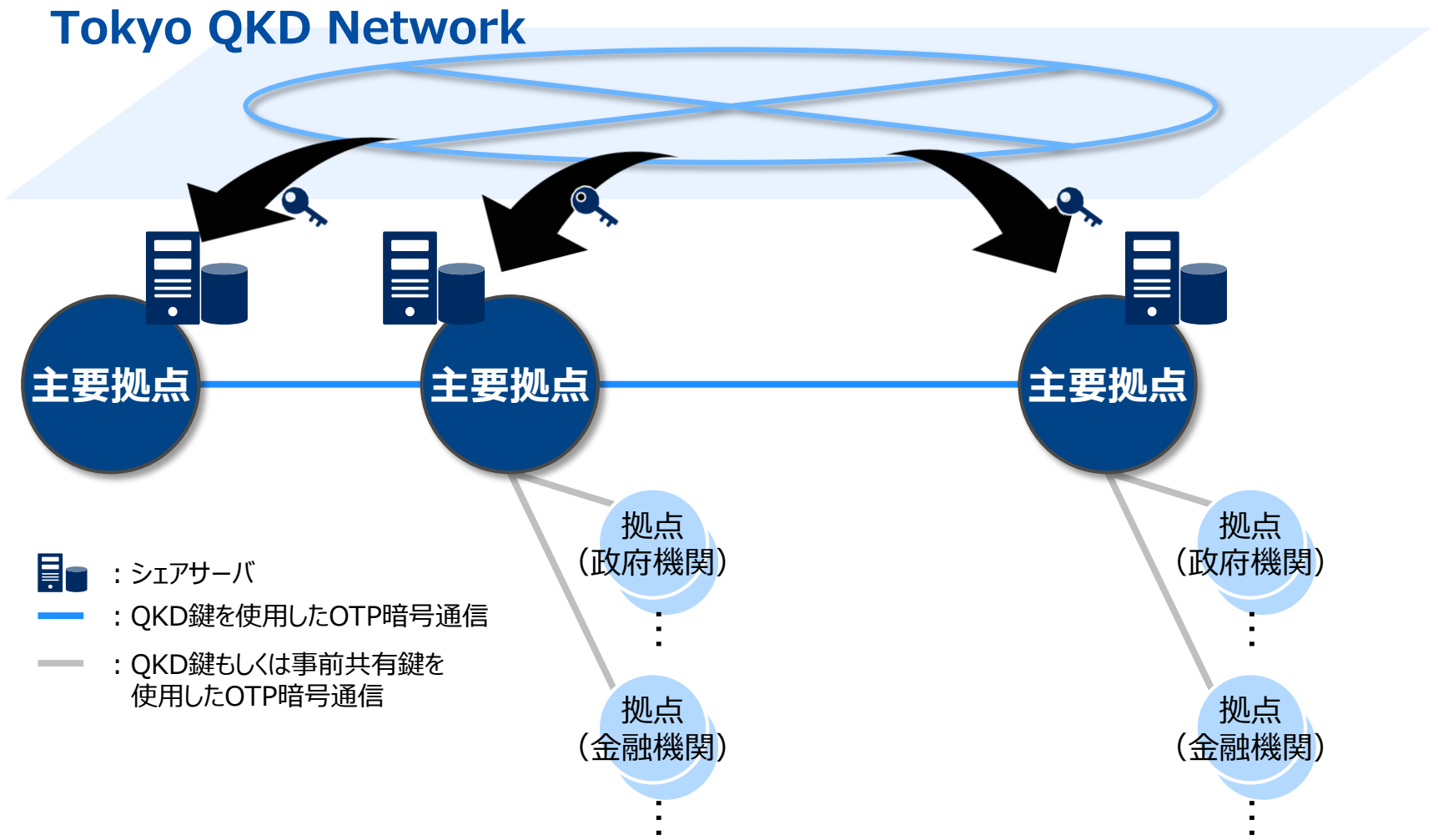
機微情報を保護可能な秘密分散技術に、Tokyo QKD Networkから供給される情報理論的に安全な鍵を用いた量子暗号通信(Vernam's OTP)を適用し、安全なストレージの実現に向けた実証実験を進めています。



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。