2015年4月16日、JST
第1回拡大運営会議

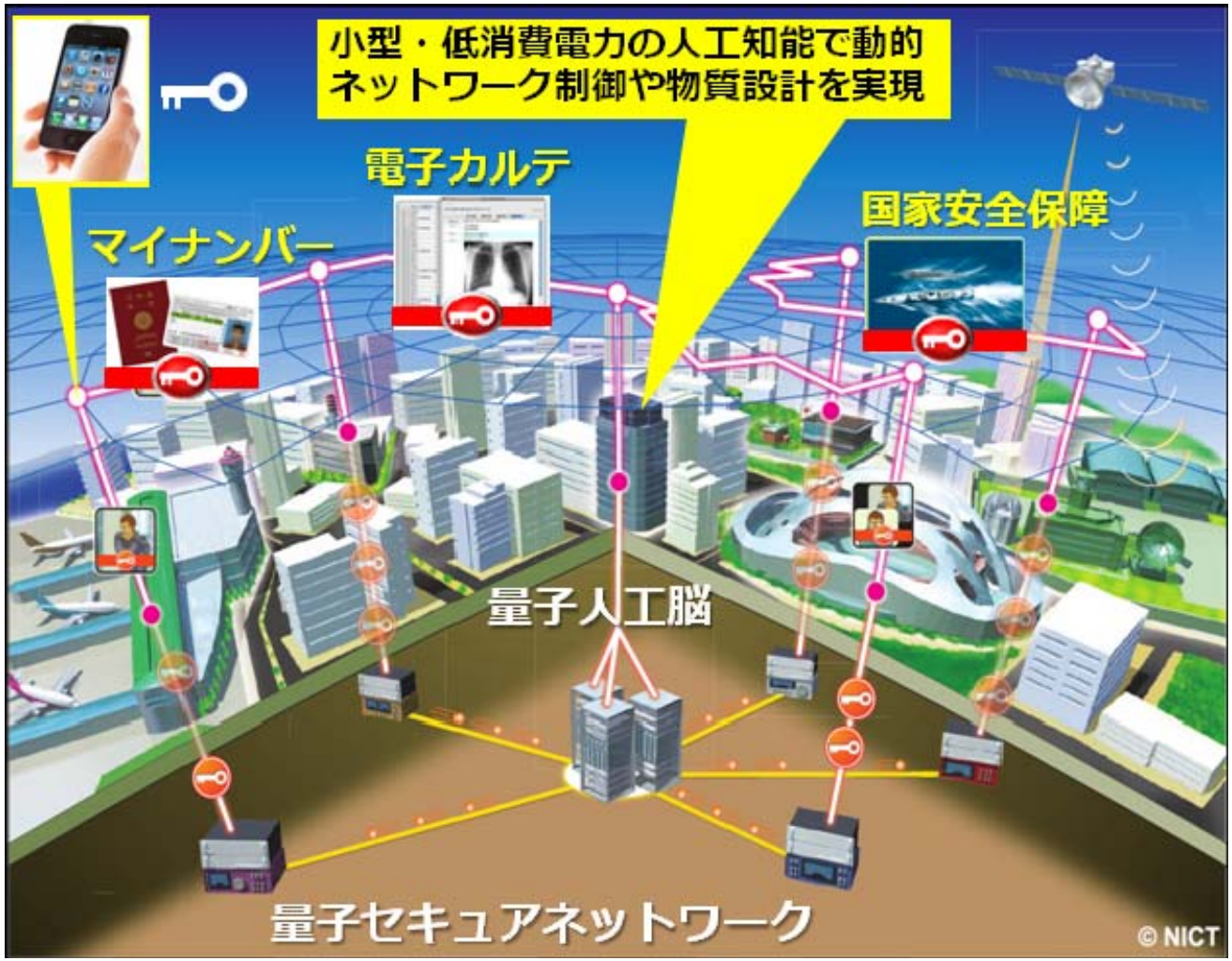
ImPACTプログラム
「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」

量子セキュアネットワーク

情報通信研究機構
量子ICT研究室
佐々木雅英

量子セキュアネットワーク

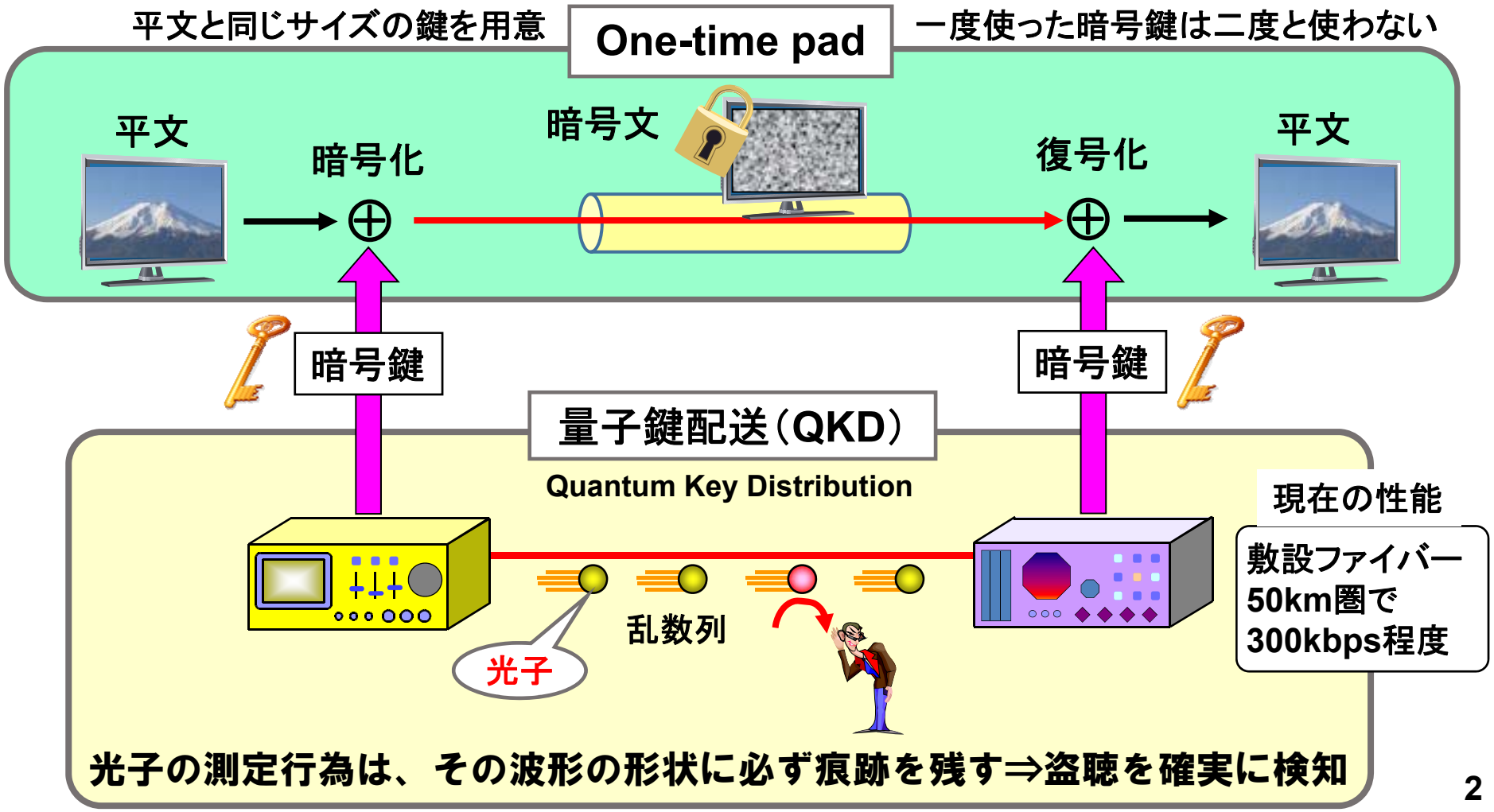
原理的に盗聴できない暗号鍵を様々な情報端末や制御機器に供給
⇒重要情報を安全に、遅延なく、組織を跨いでシームレスに伝送
① 第一世代を東京圏に構築し実用環境で稼働（QKDプラットフォーム）
② 新原理のQKDや物理レイヤ暗号など次世代技術の開発



NICT
NEC
東芝
三菱電機
NTT
東北大
学習院大
東大
北大
東工大

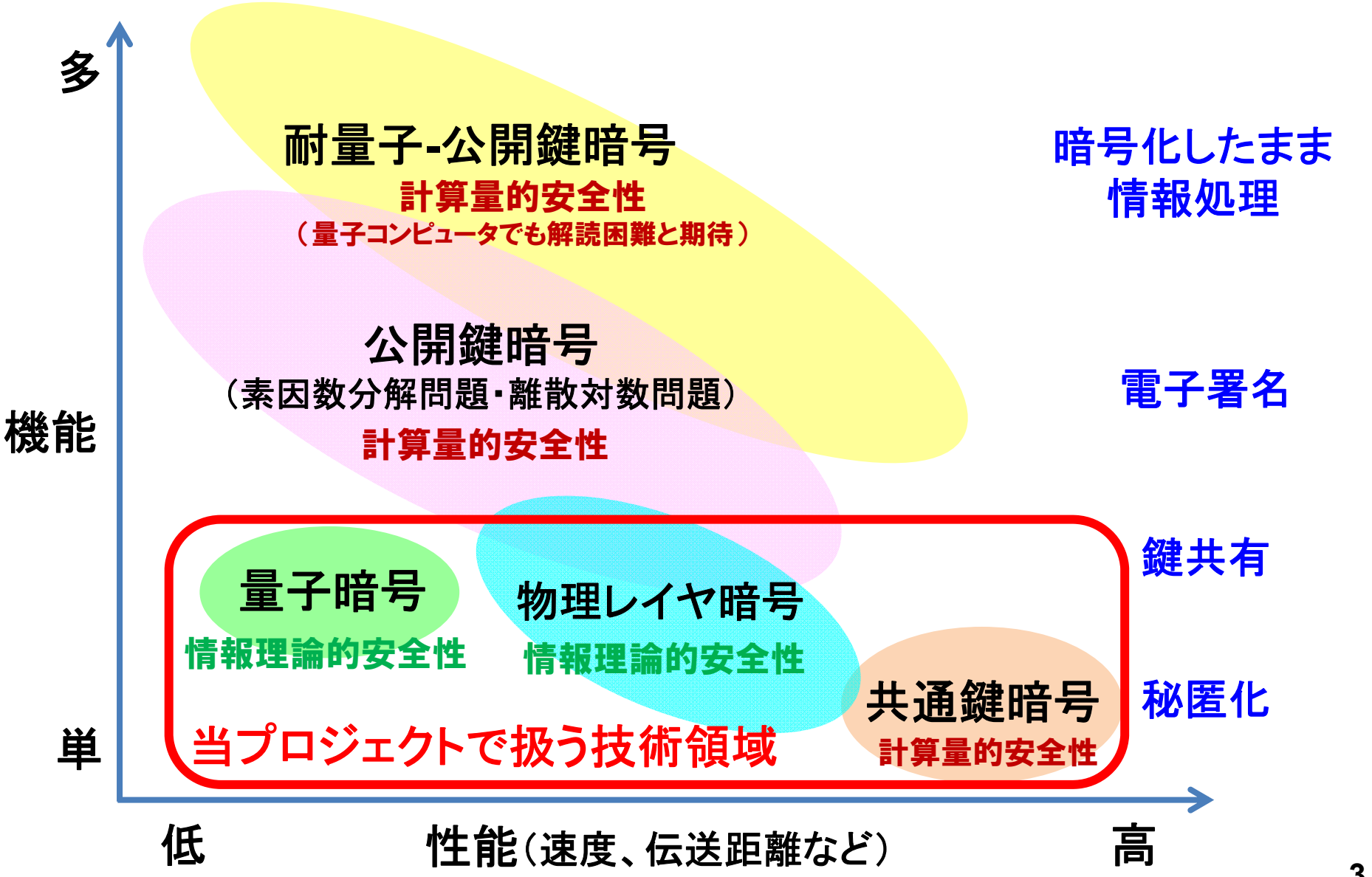
量子暗号とは

量子鍵配送とワンタイムパッド暗号化の組合せ
⇒ どんな（将来現れる）技術でも解読不可能

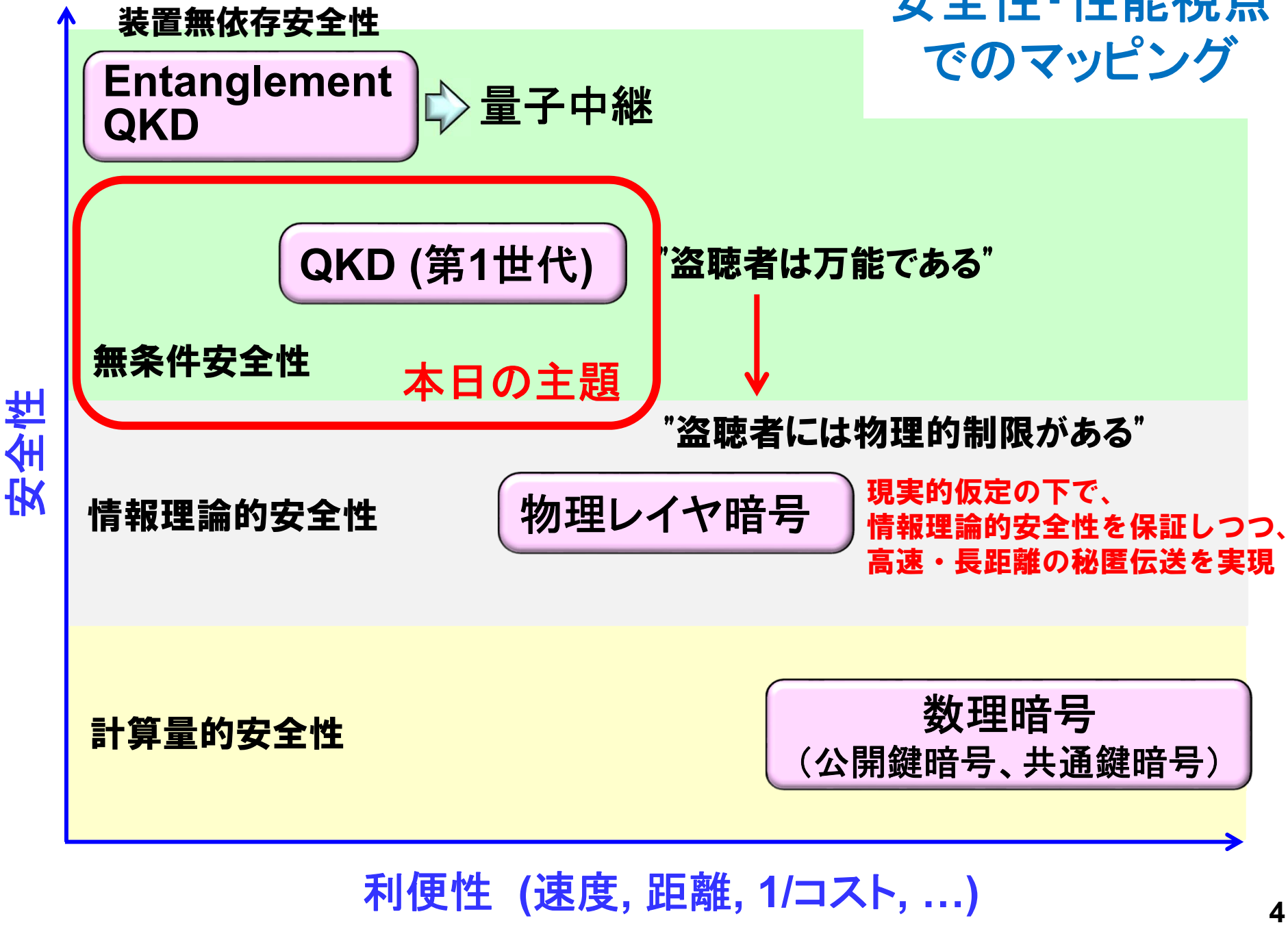


暗号技術の概要

機能・性能視点でのマッピング

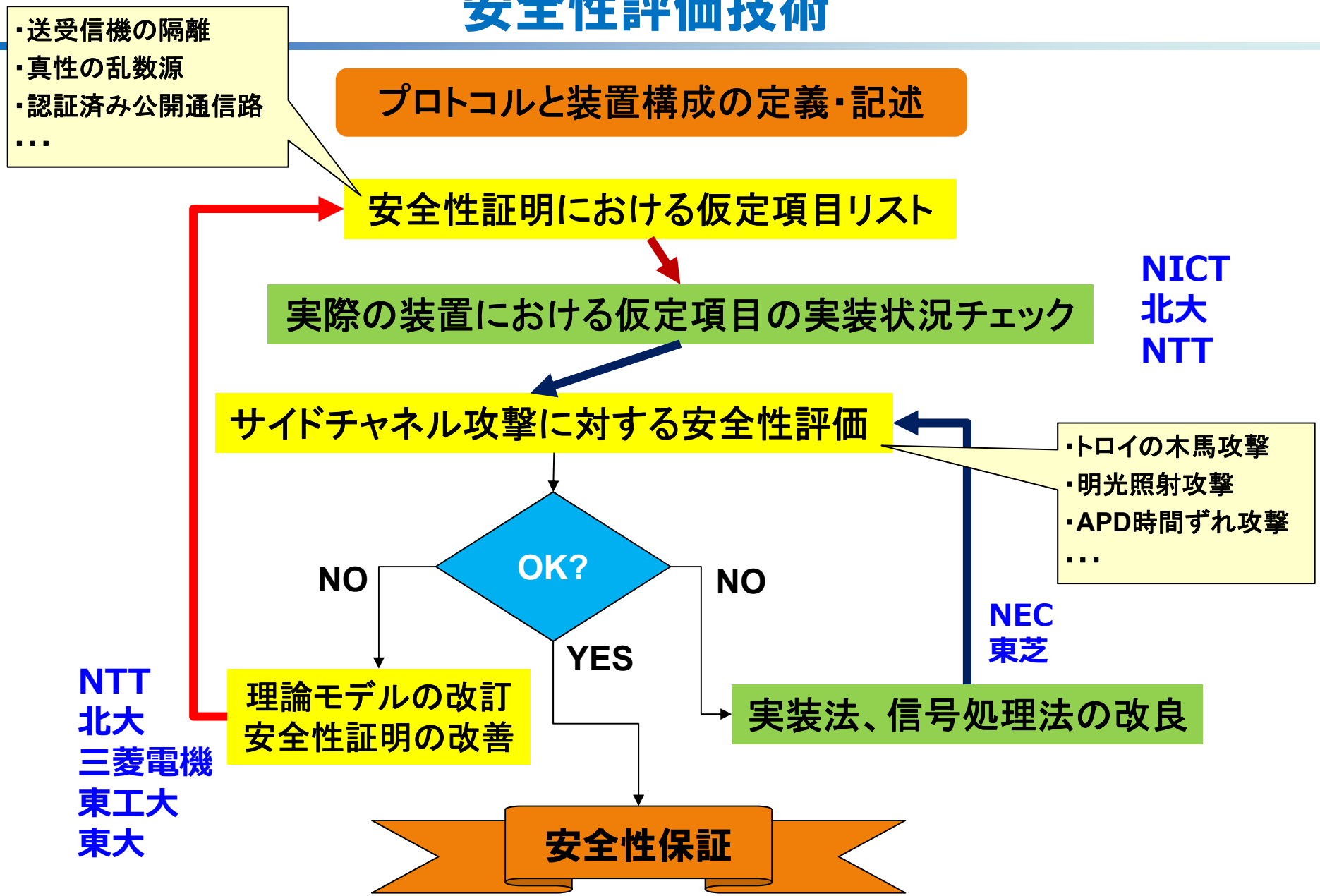


安全性・性能視点でのマッピング



安全性・性能視点でのマッピング

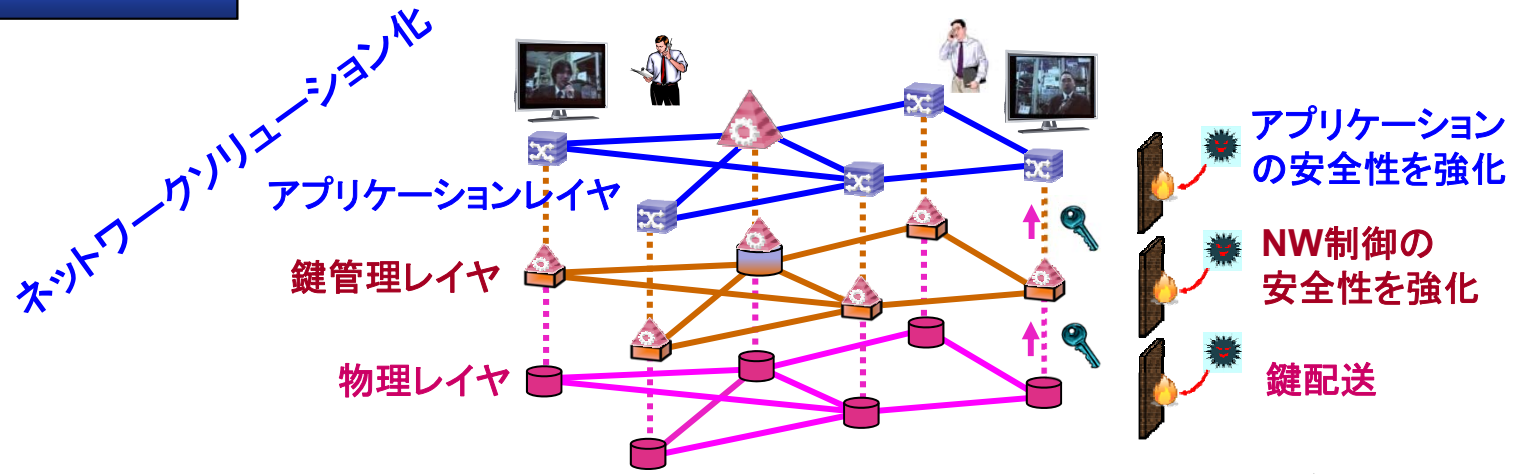
安全性評価技術



欧州ETSI（QKD-ISG）とも連携しながら、検証とドキュメント化を推進

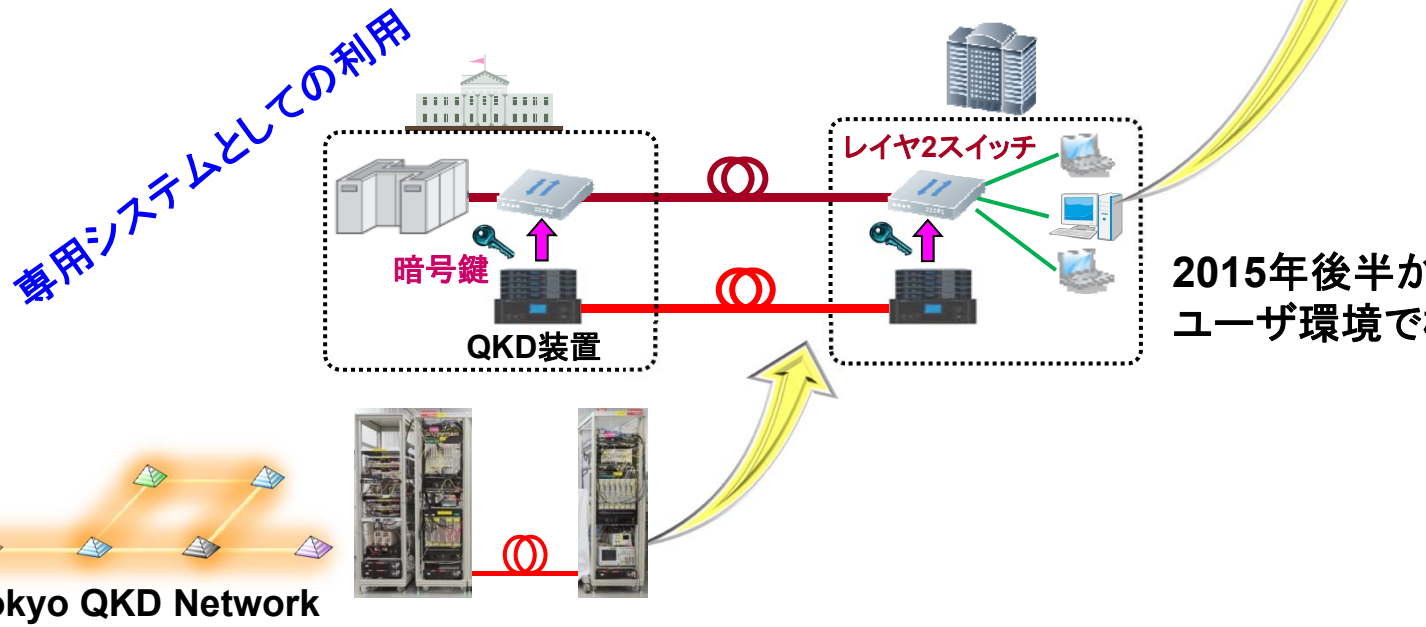
QKD実用化への道筋

第3層（ネットワークレイヤ）のIPルータで秘匿化と認証⇒民生用途へ



2020以降、実運用

第2層（データレイヤ）の専用回線の秘匿化⇒国家用途へ



2015年後半から
ユーザ環境で検証

2014年 ImPACT実施期間 2019年

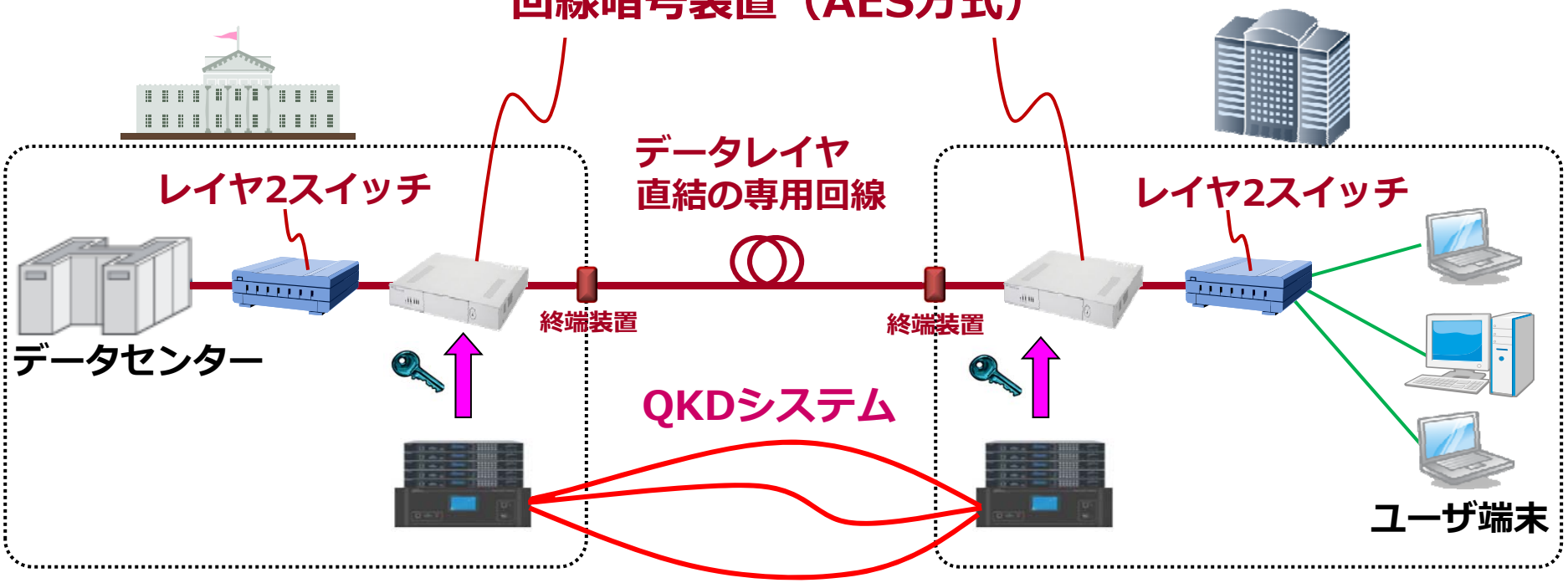
第１ステップ：データレイヤの秘匿化システム

製品例

・NEC社製 COMCIPHER
・ドイツSECUNET社製 SINA (NATO採用)

100Mbps～10Gbps
でリアルタイム暗号化

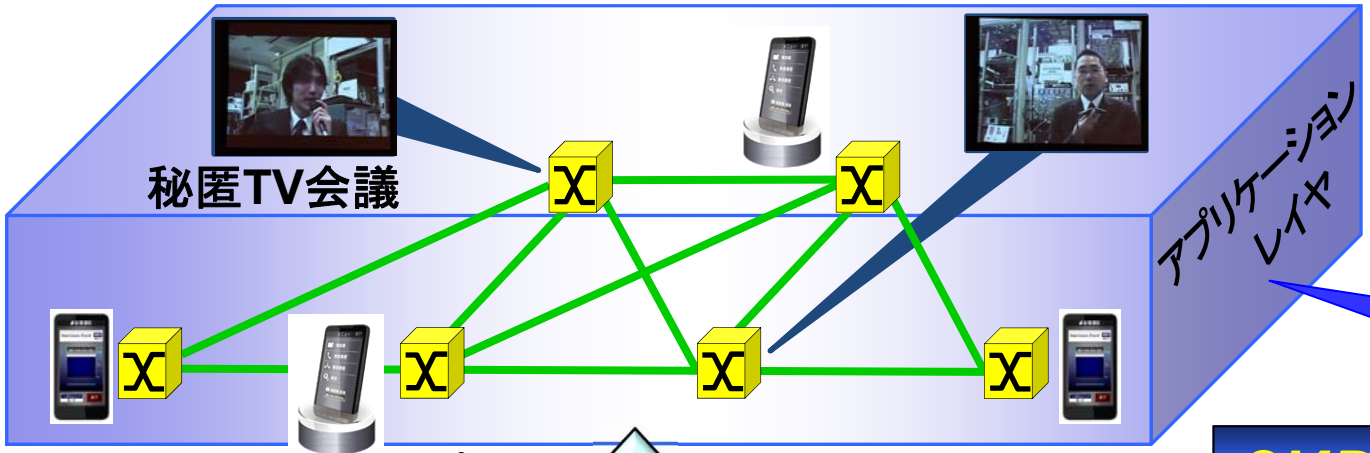
Advanced Encryption Standard
（代表的な共通鍵暗号方式）



① 回線暗号装置への鍵更新 ⇒ 安全性強化
② One-time padモードの追加 ⇒ 完全秘匿化
③ 盗聴検知　⇒ 通信路のモニタ

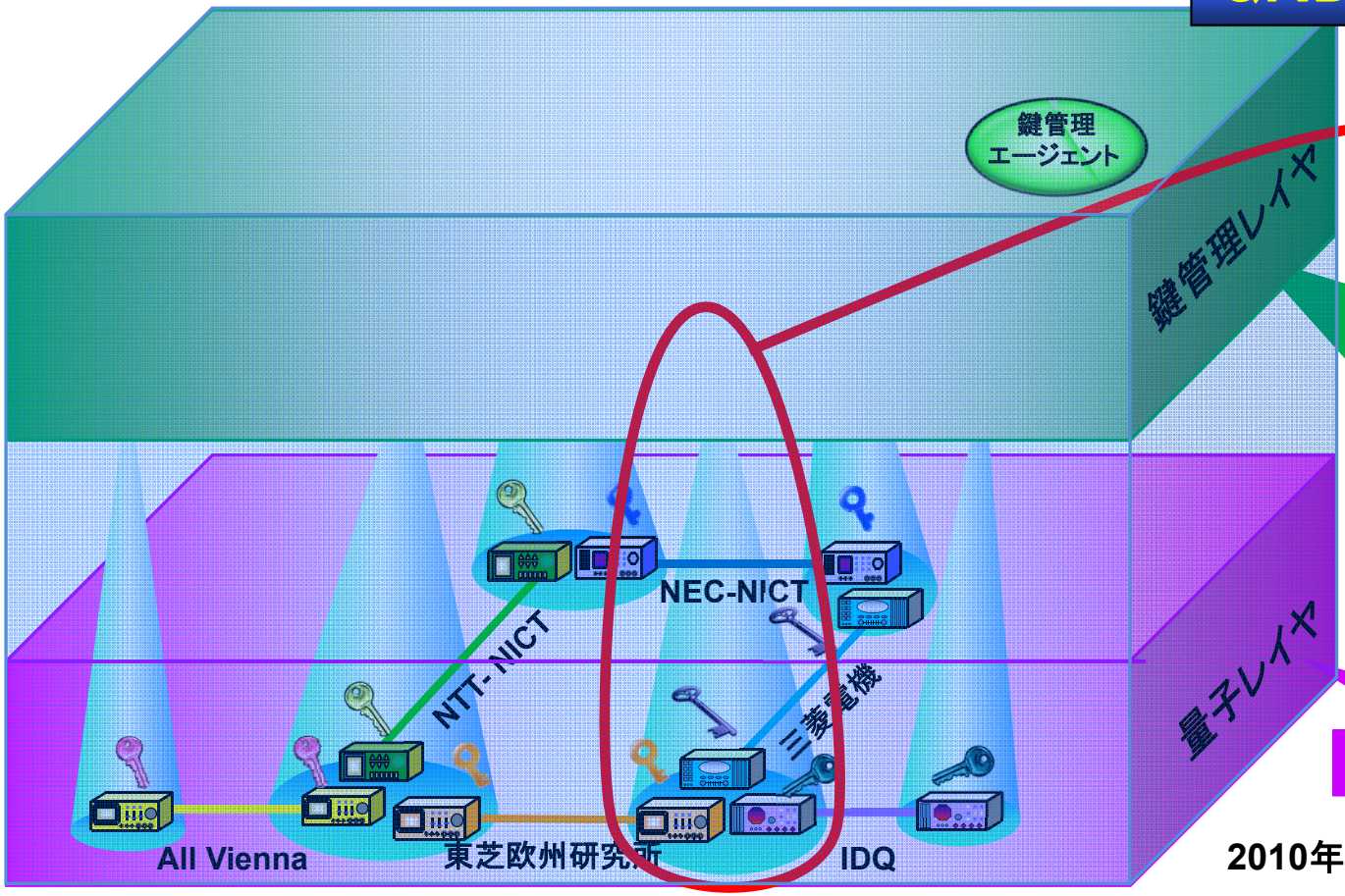
今後、位置情報取得機能も実装

第２ステップ：ネットワーク化



アプリケーションを実行

QKDプラットフォーム



信頼できるノード

・Wegman-Carter認証を行い正規ユーザ間で安全に暗号鍵をカプセルリレー
・盗聴検知、経路切替え

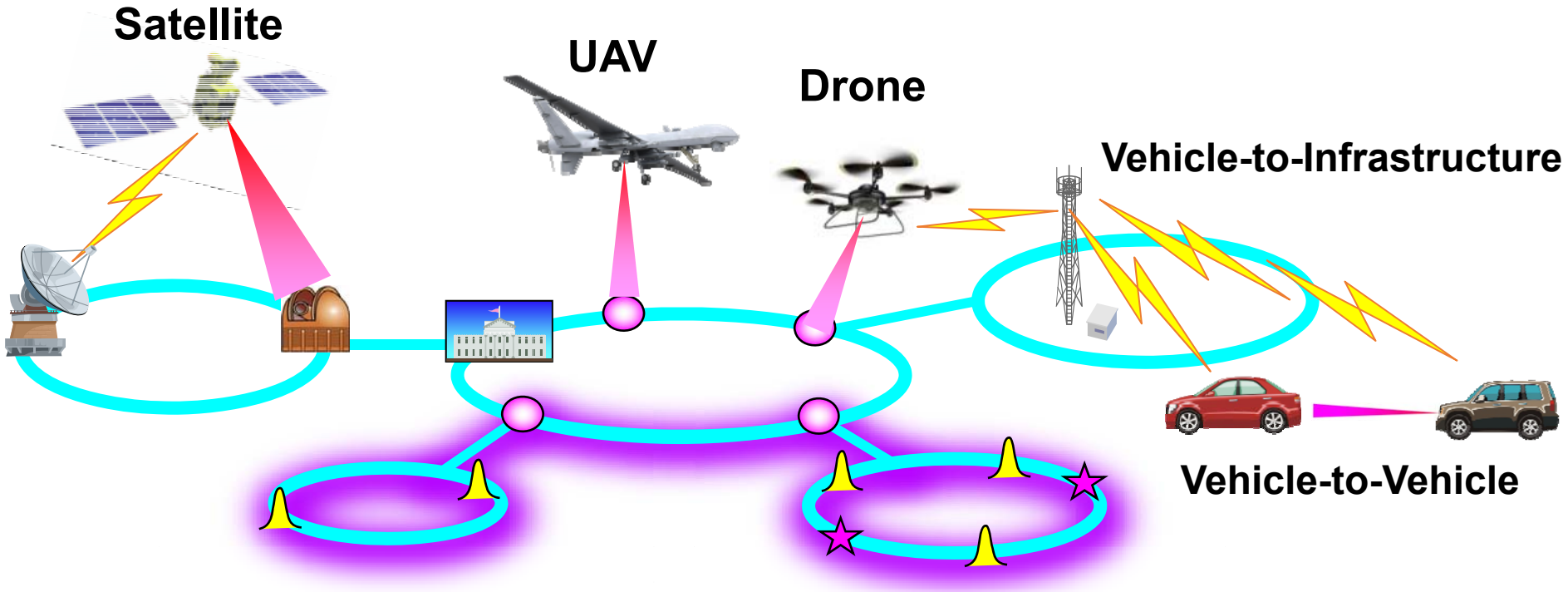
各QKDリンクで暗号鍵を生成

2010年時の接続形態

次世代技術の開発

物理レイヤ暗号

移動体や衛星からなるグローバルリンク上で、通信性能と安全性のバランスを自在に設計・制御できる新技術を開拓　NICT、東工大

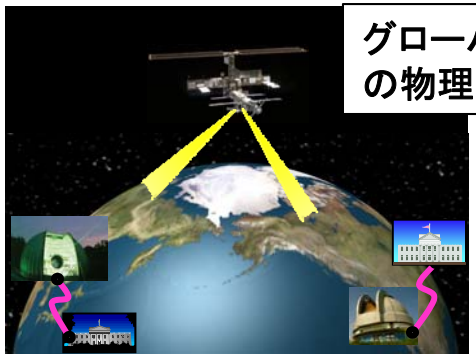


新原理、新方式の開拓、現代暗号との融合

- 雑音耐性の向上（総当たり差動位相-QKD）：東大、NTT
- 安価なフォトダイオードで動く低コストQKD：学習院大
- QKDの秘匿性増強をPUF技術に導入し、性能改善：三菱電機

PUF（Physically Unclonable Function）：物理的複製困難関数

推進体制



グローバル化のための物理レイヤ暗号

NICT、東工大

アプリケーション層

QKD装置とAPI
NEC、東芝、三菱電機

量子ストリーム暗号
東北大
低コストQKD
学習院大

鍵管理層

物理層

新原理、新方式開拓
東大、NTT

暗号鍵

既存のセキュリティ技術と統合運用

情報端末の安全性を強化

リレー配送による鍵交換

どんな盗聴も即座に検知

安全性評価技術
NICT、北大、NTTが主導し全機関で連携