安全・安心なグローバルネットワークに向けた物理レイヤ暗号

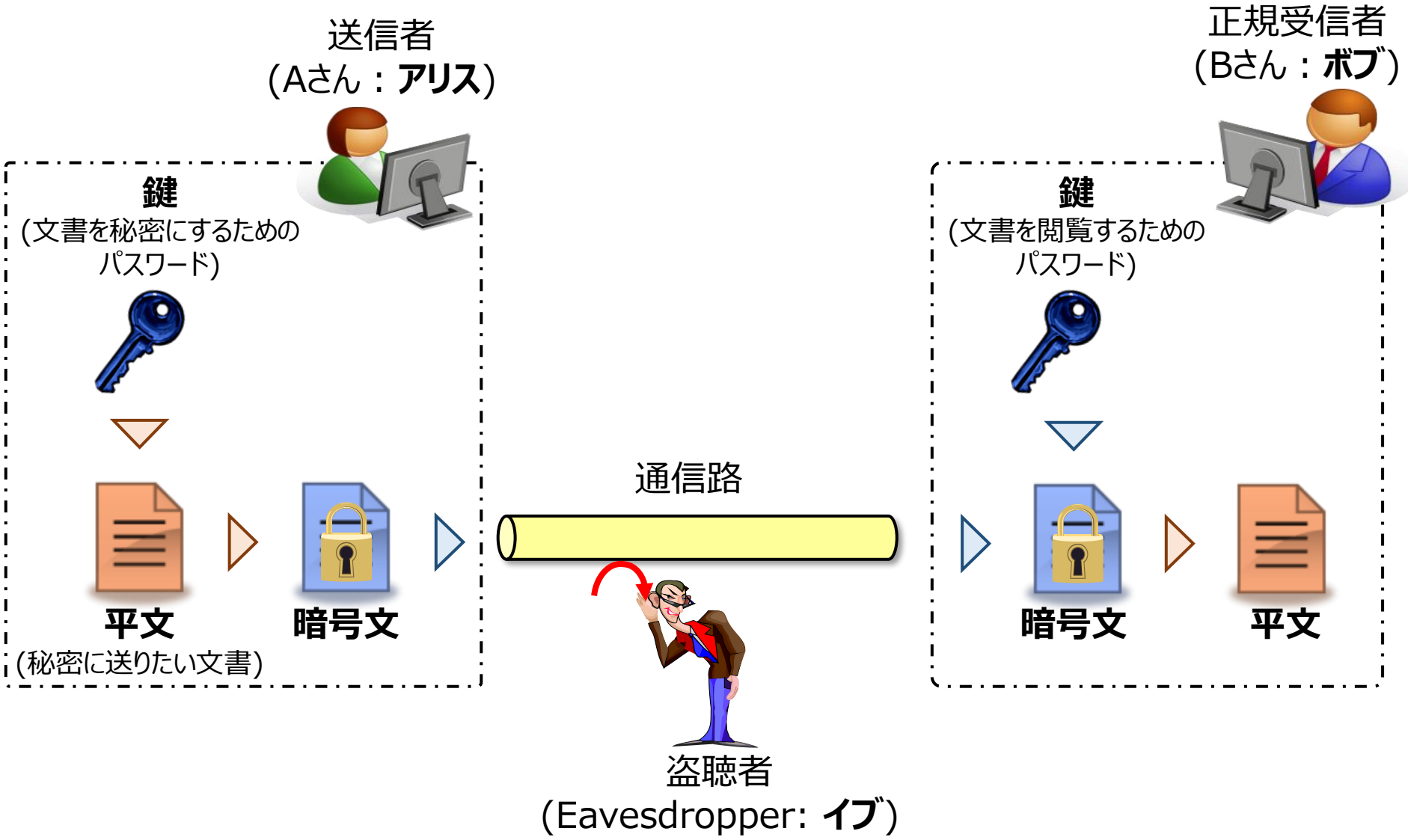
情報通信研究機構　量子ICT協創センター
研究マネージャー　遠藤 寛之

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

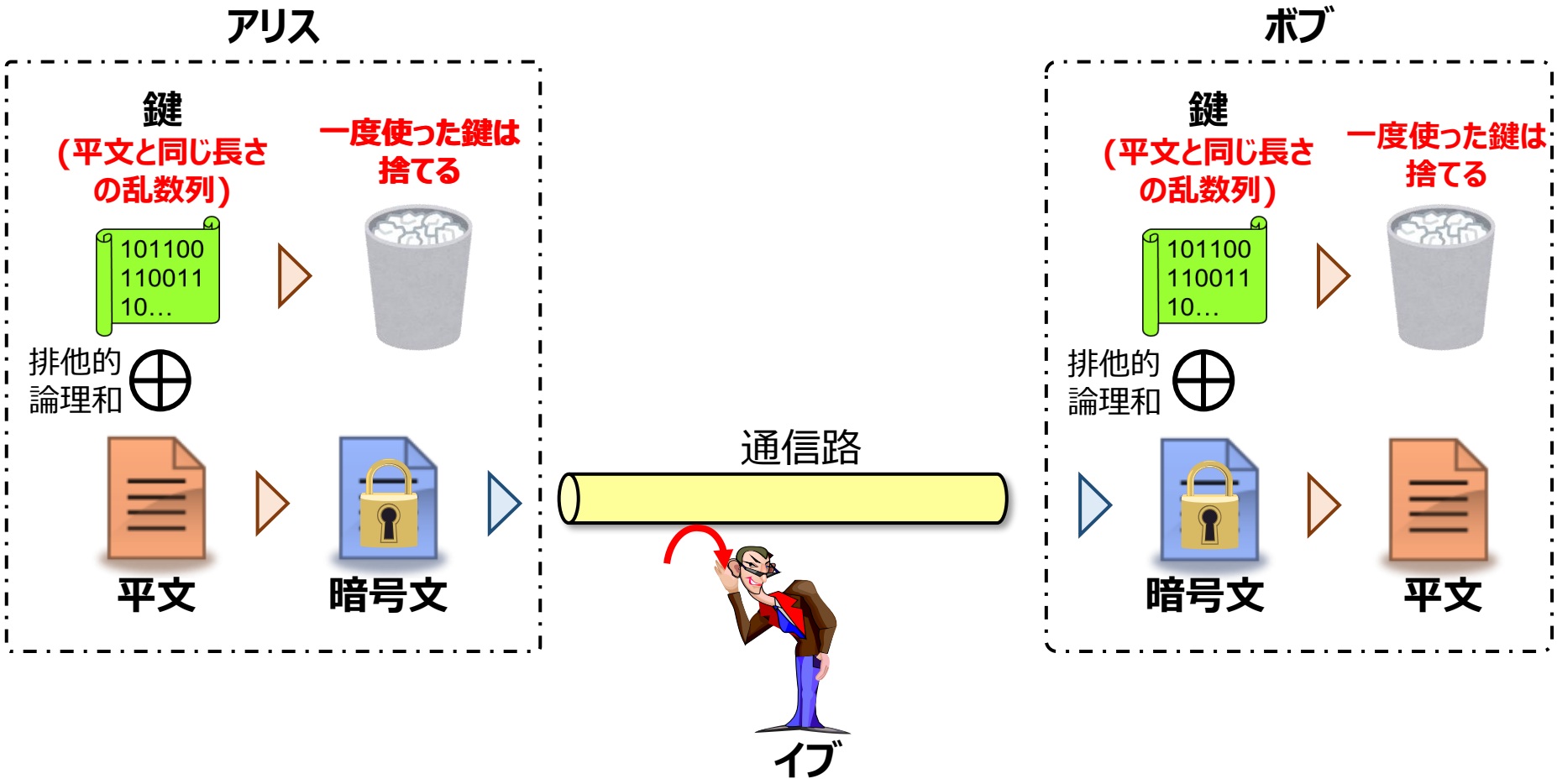
新技術説明会
New Technology Presentation Meetings!

はじめに：量子暗号について

暗号：秘密にしたい情報を安全に送る技術



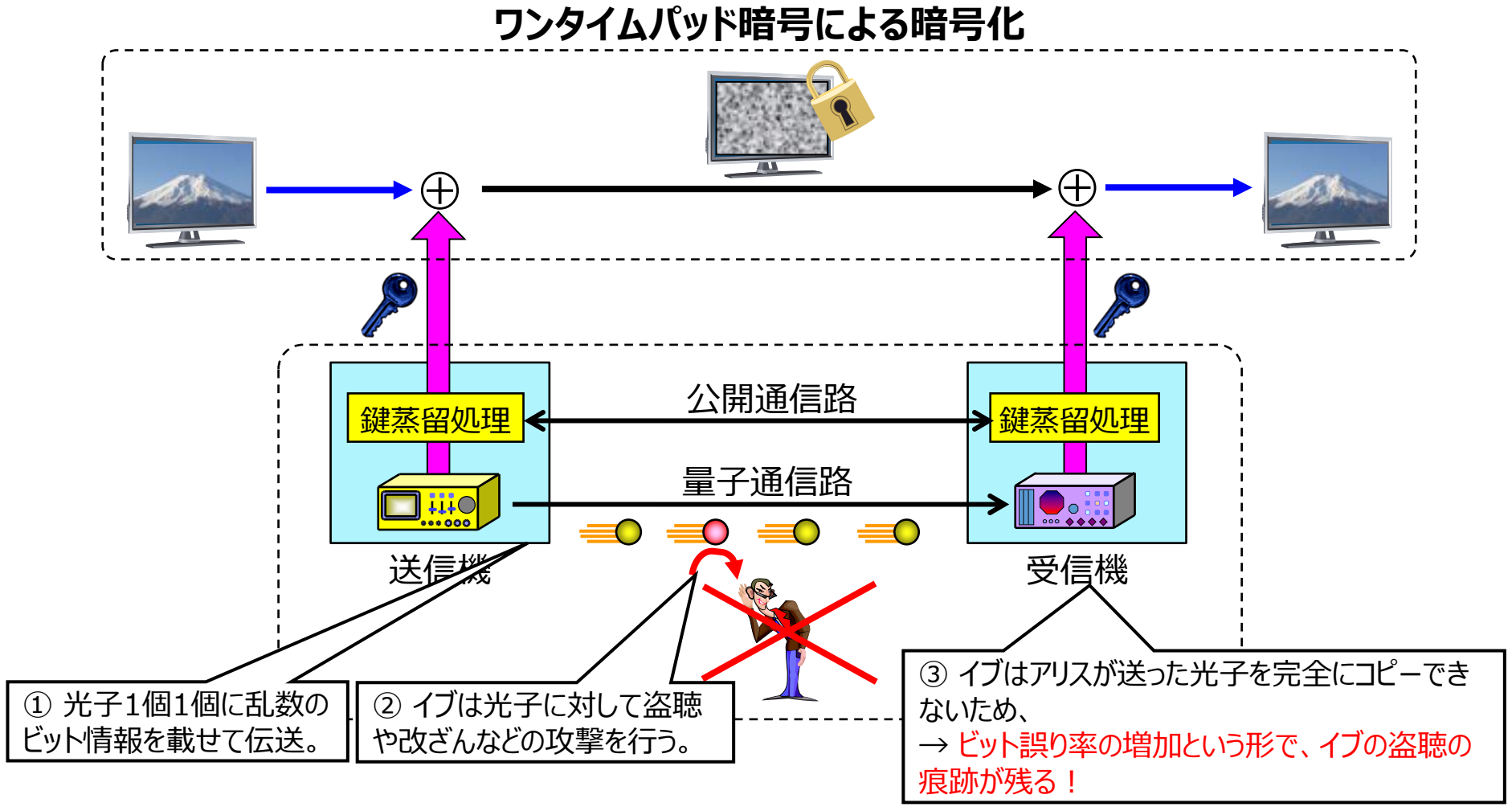
どんな計算機に対しても安全な暗号：バーナムのワンタイムパッド暗号



イブはどんな高性能な計算機を持っていたとしても、あてずっぽうに鍵を当てはめる以外に有効な解読手段が無いこと(＝情報理論的に安全)が数学的に証明されている。

→ 非常に長い鍵を安全に共有するための手段が必要！

量子暗号：「量子」の力で鍵共有の問題を解決



量子鍵配送(QKD)

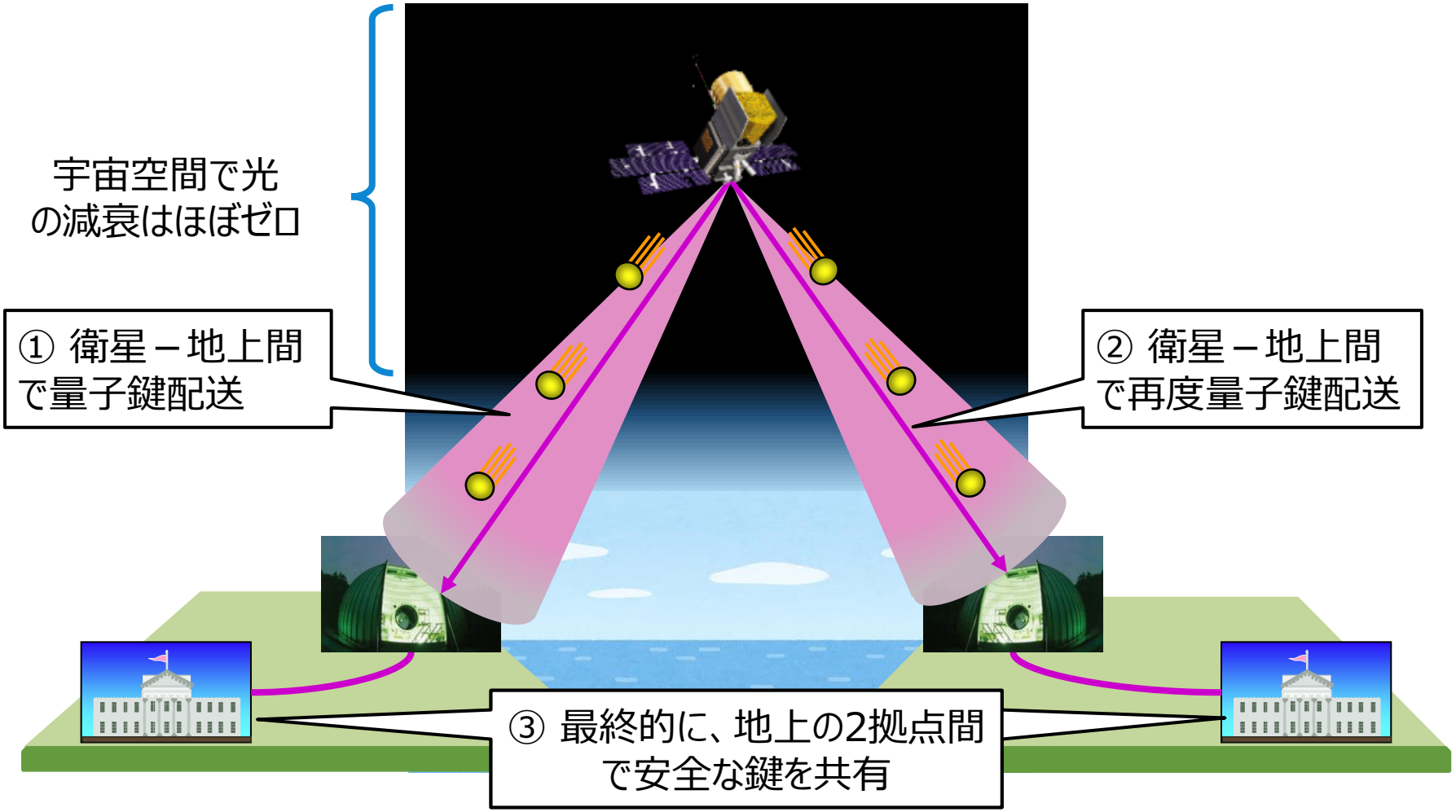
「量子」の力で物理学的に可能なあらゆる攻撃に対しても安全な鍵配送を実現

量子鍵配送のグローバル化に向けた課題

1. **伝送距離/鍵生成速度の制限**
   光子を光ファイバで伝送する場合、光ファイバ中の光子の損失(損失率=0.2dB/km)によって、伝送距離と鍵生成速度が制限される。
   - 50kmのファイバでは1Mbps
   - 100kmのファイバでは1kbps
     A. R. Dixon, *et al*. *Opt. Express*, **23**(6), 7583, (2015).

2. **カプセルリレーの限界**
   長距離化、多地点ネットワーク化は、『信頼できる局舎』による鍵のカプセルリレーで実現
   - カプセルリレーのみでは大陸間の鍵生成は難しい。

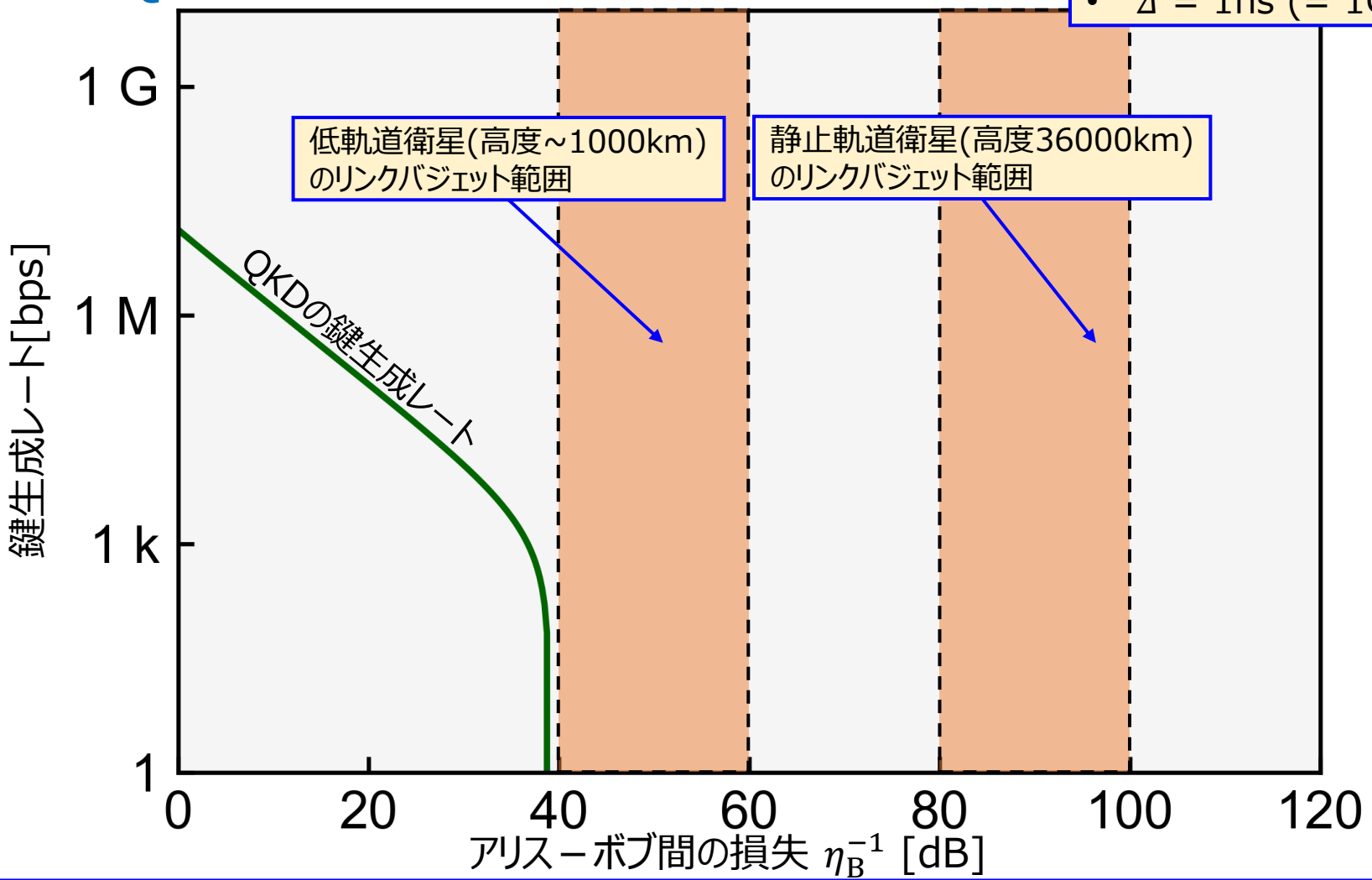
衛星による量子鍵配送



- 地上光ファイバ網では不可能な距離での鍵配送
- 衛星間での光回線によりネットワークの拡張（広域/ｸﾞﾛｰﾊﾞﾙ化）も可能。

衛星によるQKDの限界

- λ_B = 1kHz
- Δ = 1ns (= 1GHz)



現行のQKDでは静止軌道衛星―地上局間の鍵共有は非常に難しい
→ 安全・安心なネットワークのグローバル化にはこの限界を打破する新しい技術が必要！

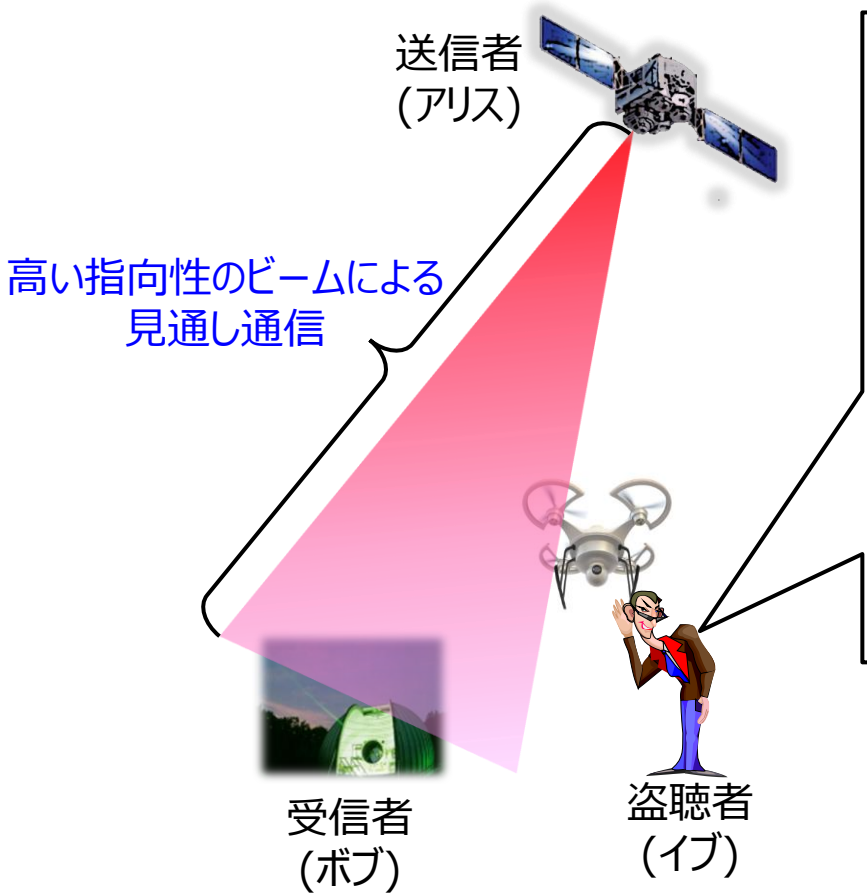
本日のメインテーマ
～物理レイヤ暗号について～

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

新技術説明会
New Technology Presentation Meetings!

物理レイヤ暗号

攻撃者の盗聴モデルへの仮定に基づいて伝送速度/伝送距離を適切に設定可能であり、
さらには情報理論的に安全な秘匿通信技術



量子暗号の盗聴者

盗聴者は世界中のあらゆるところから物理学的に許されるあらゆる攻撃を行える。

→ 鍵生成の性能に制限

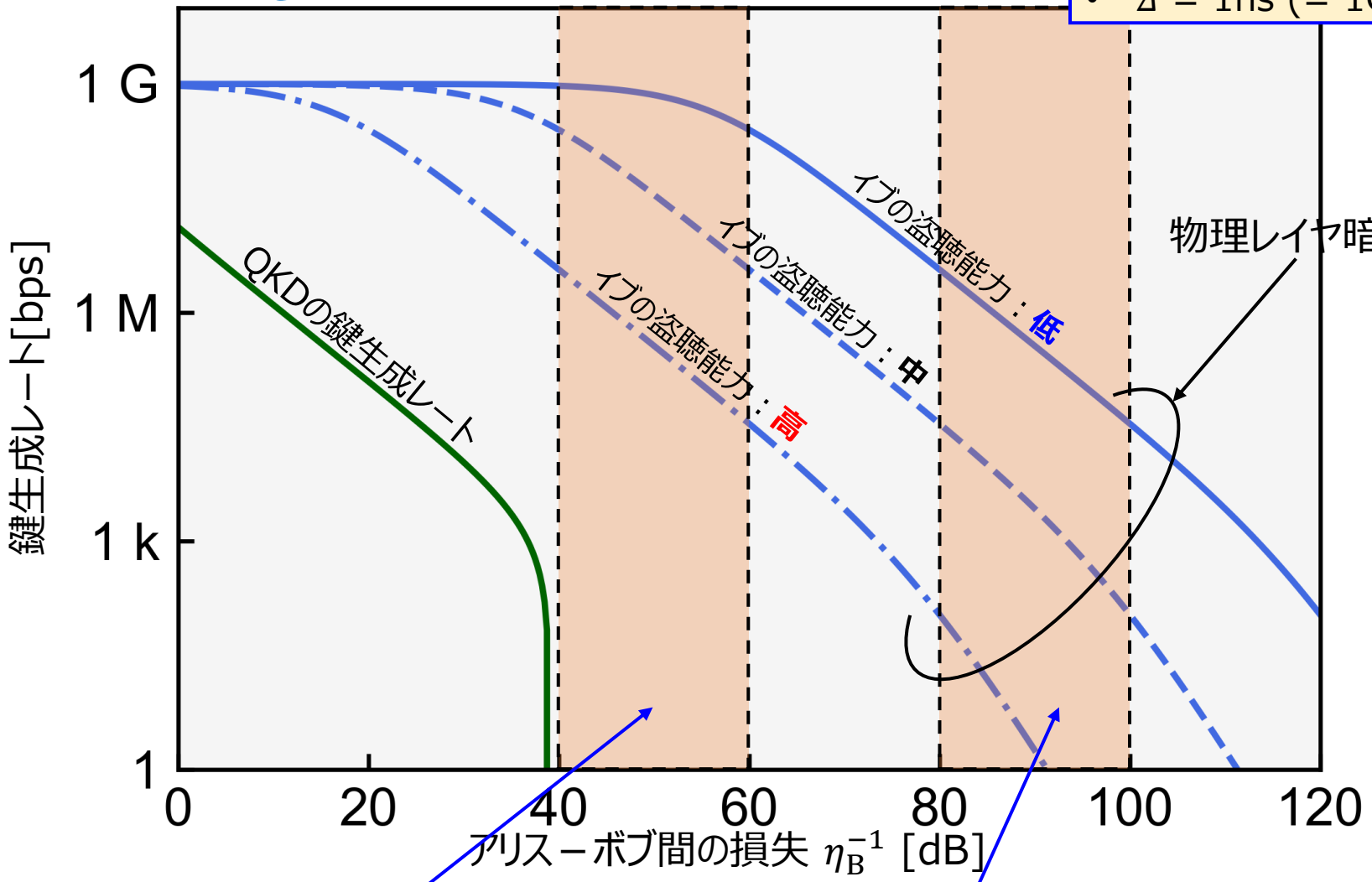
物理レイヤ暗号の盗聴者

盗聴者はビームの外側という限られた領域から光子を抜き取るようなパッシブな攻撃しか行えない。

→ **鍵生成の性能の向上が可能！**

物理レイヤ暗号とQKDの比較

- λ_B = 1kHz
- Δ = 1ns (= 1GHz)



Tokyo FSO Testbedによる物理レイヤ暗号の実証に向けた実験

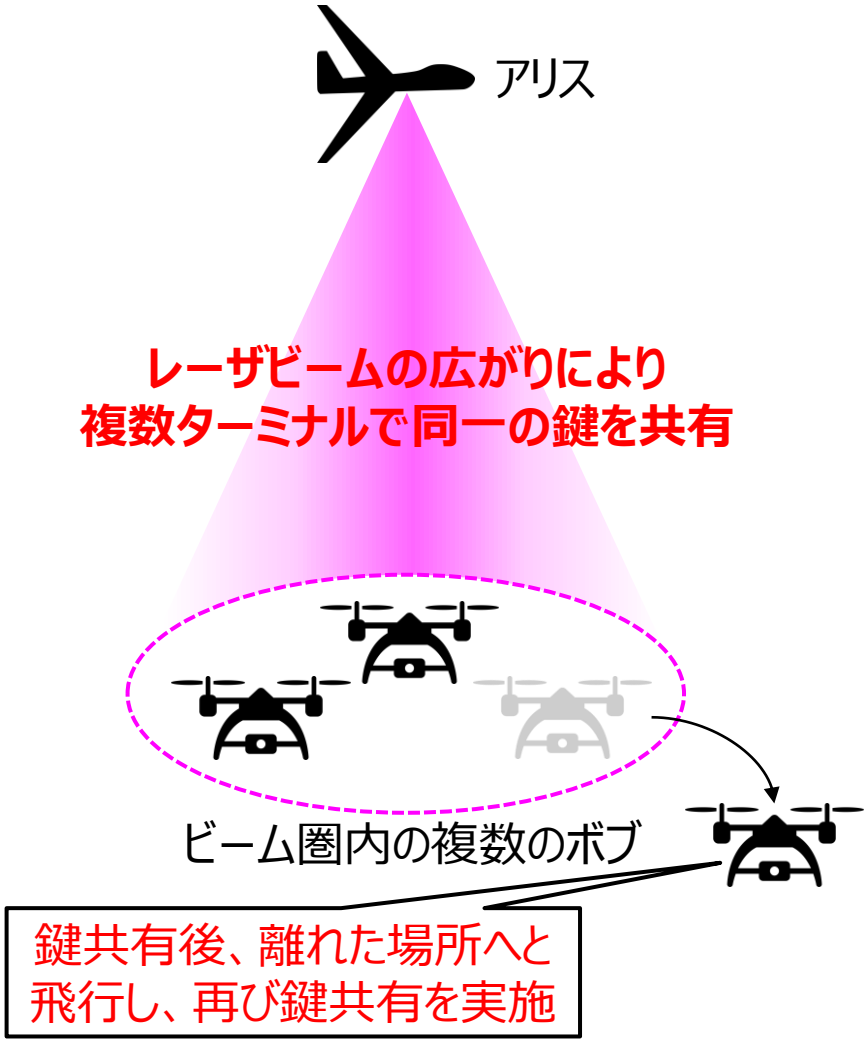
H. Endo *et al.*, *Opt. Express*, **24**(8), 8940 (2016).
M. Fujiwara *et al.*, *Opt. Express*, **26**(15), 19513 (2018).
H. Endo *et al.*, *Opt. Express*, **26**(18), 23305 (2018).

アリス
(全天候型レーザ送信ドーム)

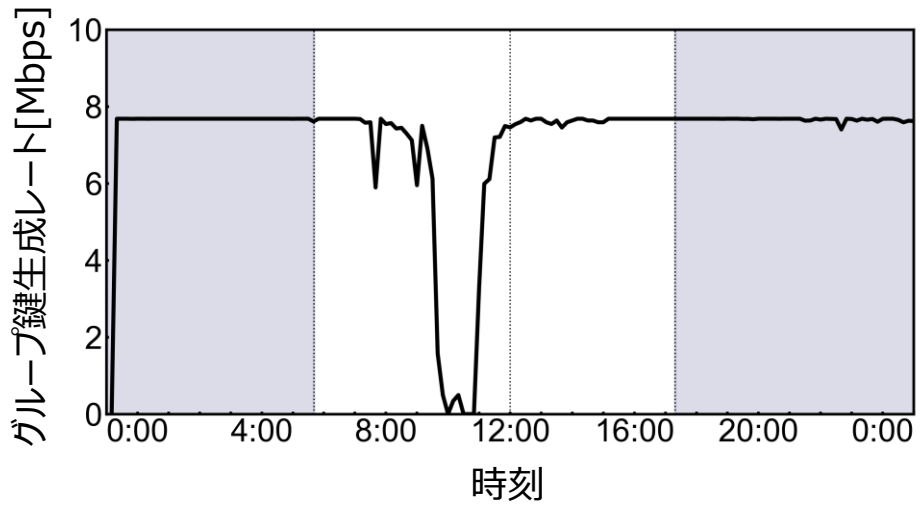
v-イブ
(漏えい情報量のモニター)

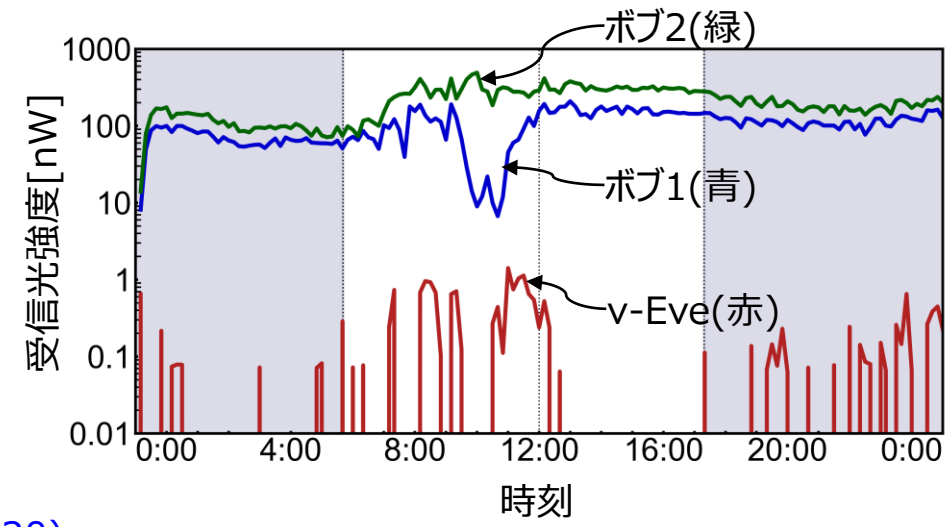
ボブ
(受信光学系)

グループ鍵共有の実証実験



Tokyo FSO Testbedでの実験(2018/10/6)





H. Endo *et al.*, *OSA. Continuum*, **3**(9), 2525 (2020).

物理レイヤ暗号に関する特許技術

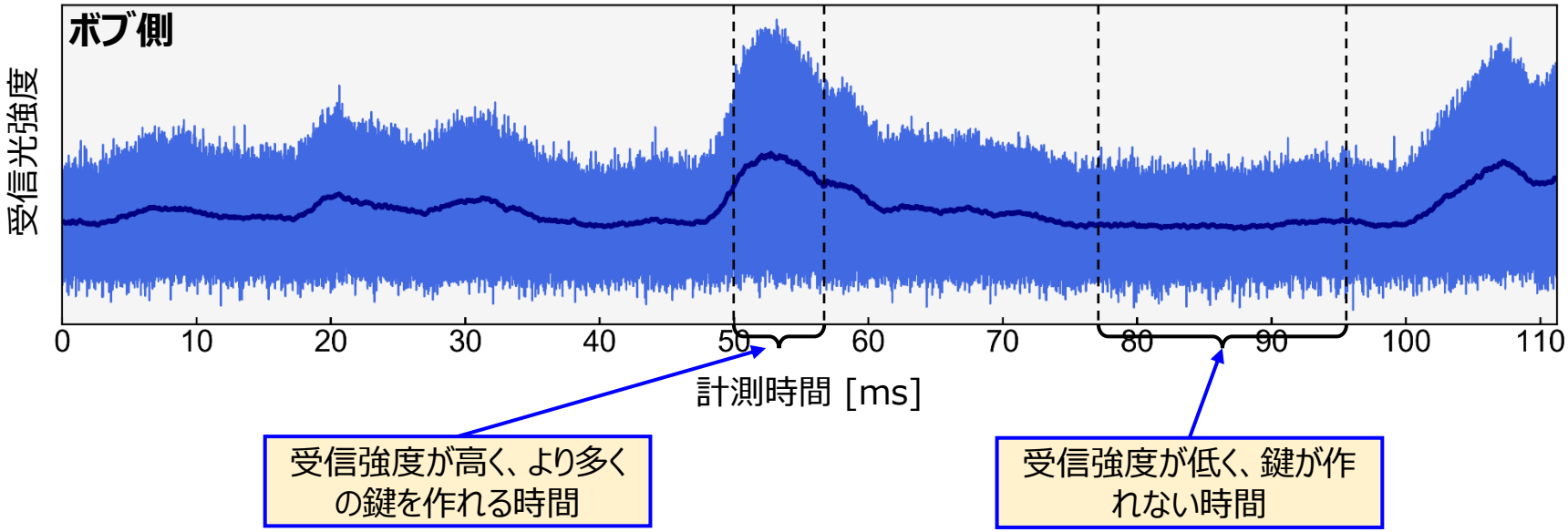
国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

新技術説明会
New Technology Presentation Meetings!

情報通信研究機構　新技術説明会
オンライン開催

Tokyo FSO Testbedによる実験から見えてきた問題点

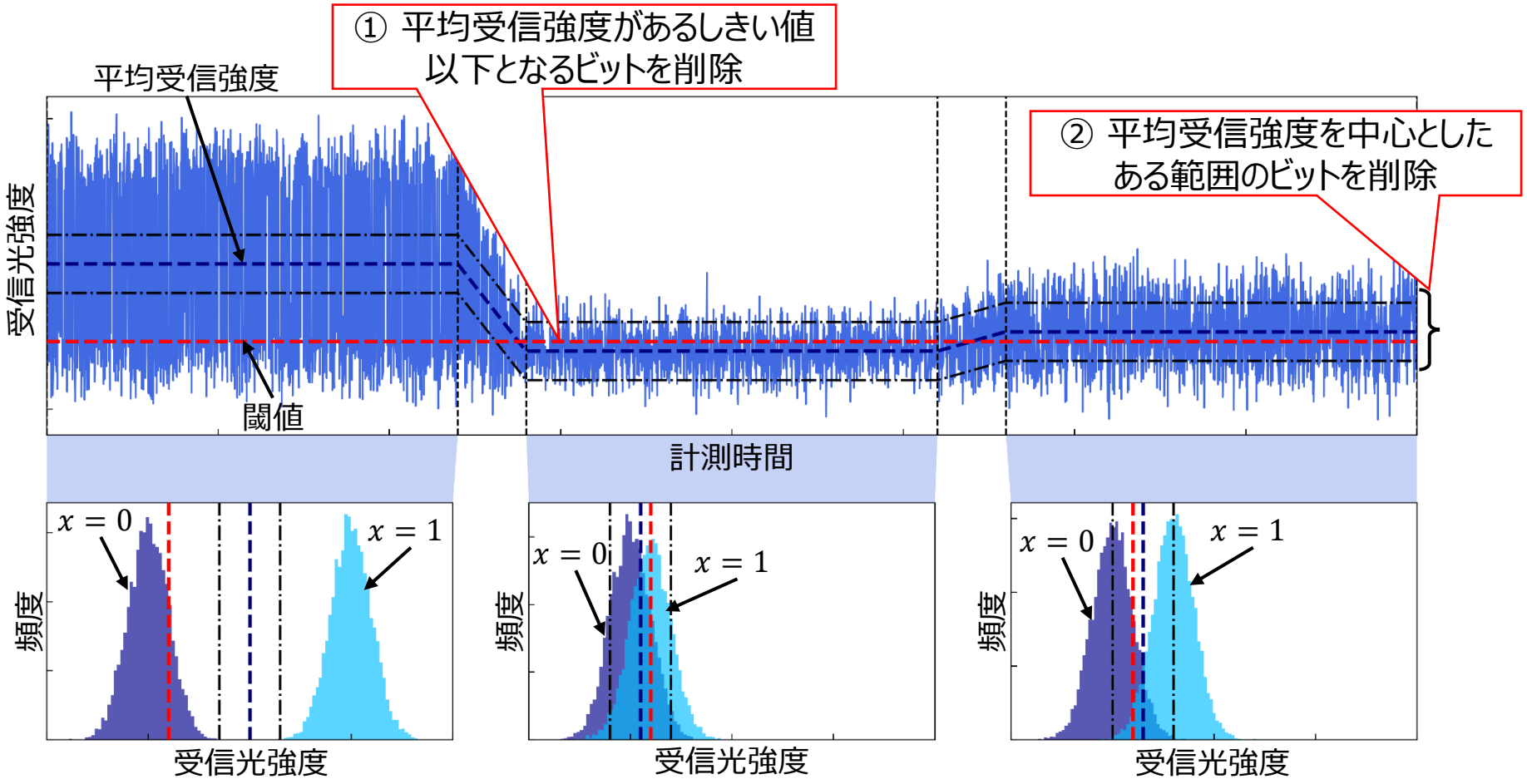
光空間通信では大気ゆらぎの影響を受けて、受信強度が経時変化する。



従来のファイバー系で用いられていた量子暗号で使われているような誤り訂正技術では、このような受信強度の経時変化を想定していないため、本来の性能を発揮できず、非効率的になる。

新技術の特徴

大気ゆらぎの状態を活用して、どの時刻のデータから鍵を作るかを選別する。

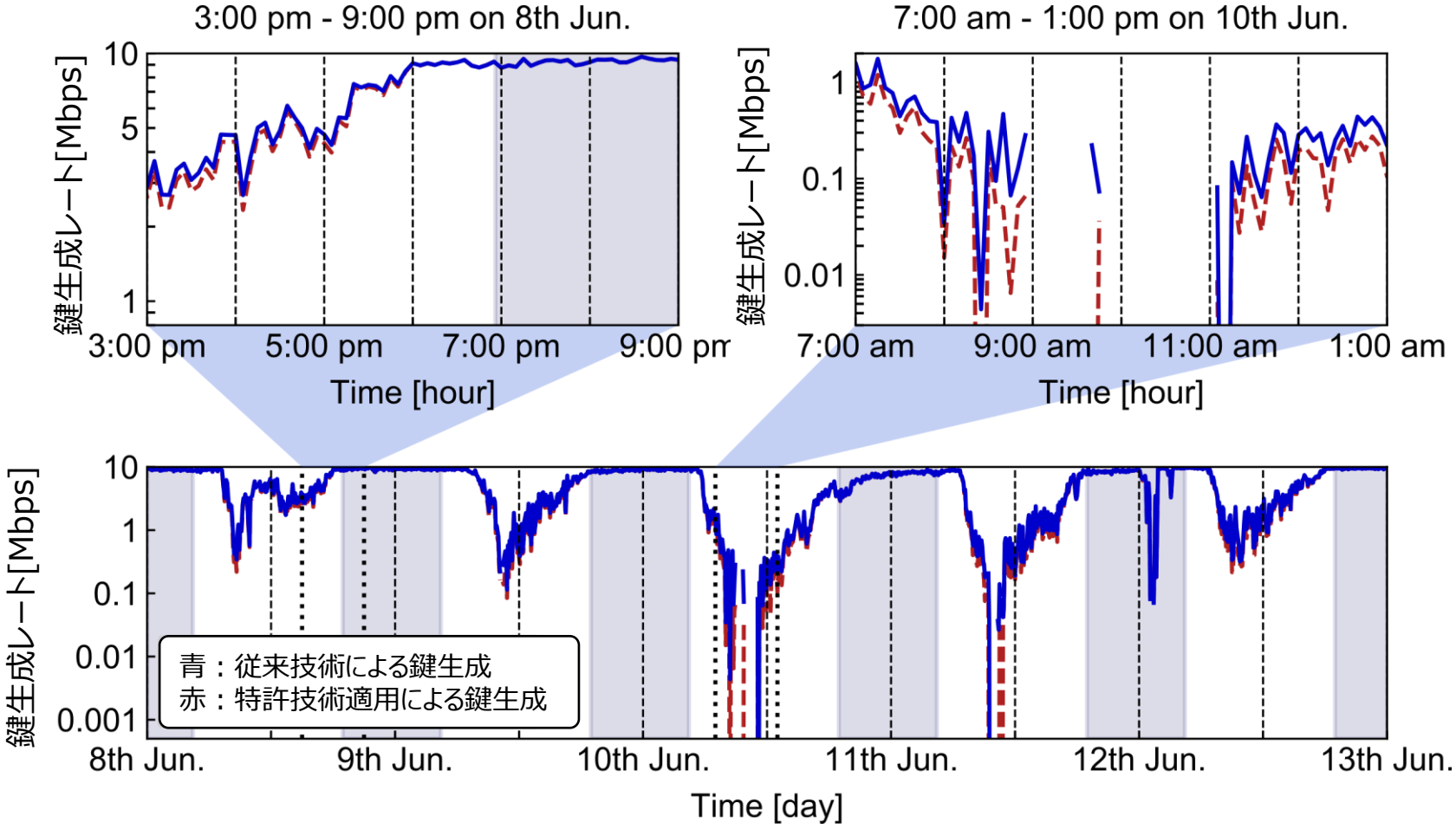


エラーフリーな領域
ほぼすべてのビットが
削除されない

アウテージしている領域
すべてのビットが削除される

エラーがある領域
エラーである確率の高いビット
が削除される

従来技術との比較



特許技術適用により：

- 日中において10 kbpsから60 kbpsの改善が見られる。
- 鍵生成ができなかった時刻でも鍵生成が可能になる。

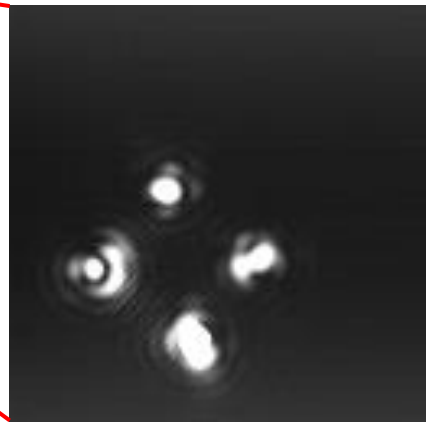
想定される用途

- 本技術によって、衛星通信を含めた、光空間通信による物理レイヤ暗号が被る大気ゆらぎの影響を緩和させ、この技術の鍵生成速度や鍵生成距離を大幅に高めることができる。
- 上記以外に、誤り訂正符号に要求される性能を下げることができ、ソフトウェアやハードウェアの簡略化に貢献する。
- また、適切な技術と組み合わせることで、1対1の光空間通信への応用に展開することも可能と思われる。

実用化に向けた課題

- 大気ゆらぎに関するデータをより簡便に取得するための装置や手法が必要となる。
- 現在、DIMM(Differential Image Motion Monitor)装置を用いて取得した大気ゆらぎデータを解析中。
- 物理レイヤ暗号一般にも当てはまるが、実用化に向けて、この大気ゆらぎデータと、見通しの状態、漏洩情報量などを結びつける手法を開発していく必要がある。

DIMM装置



カメラ画像の輝点の相対位置変化から大気ゆらぎの度合いを測定

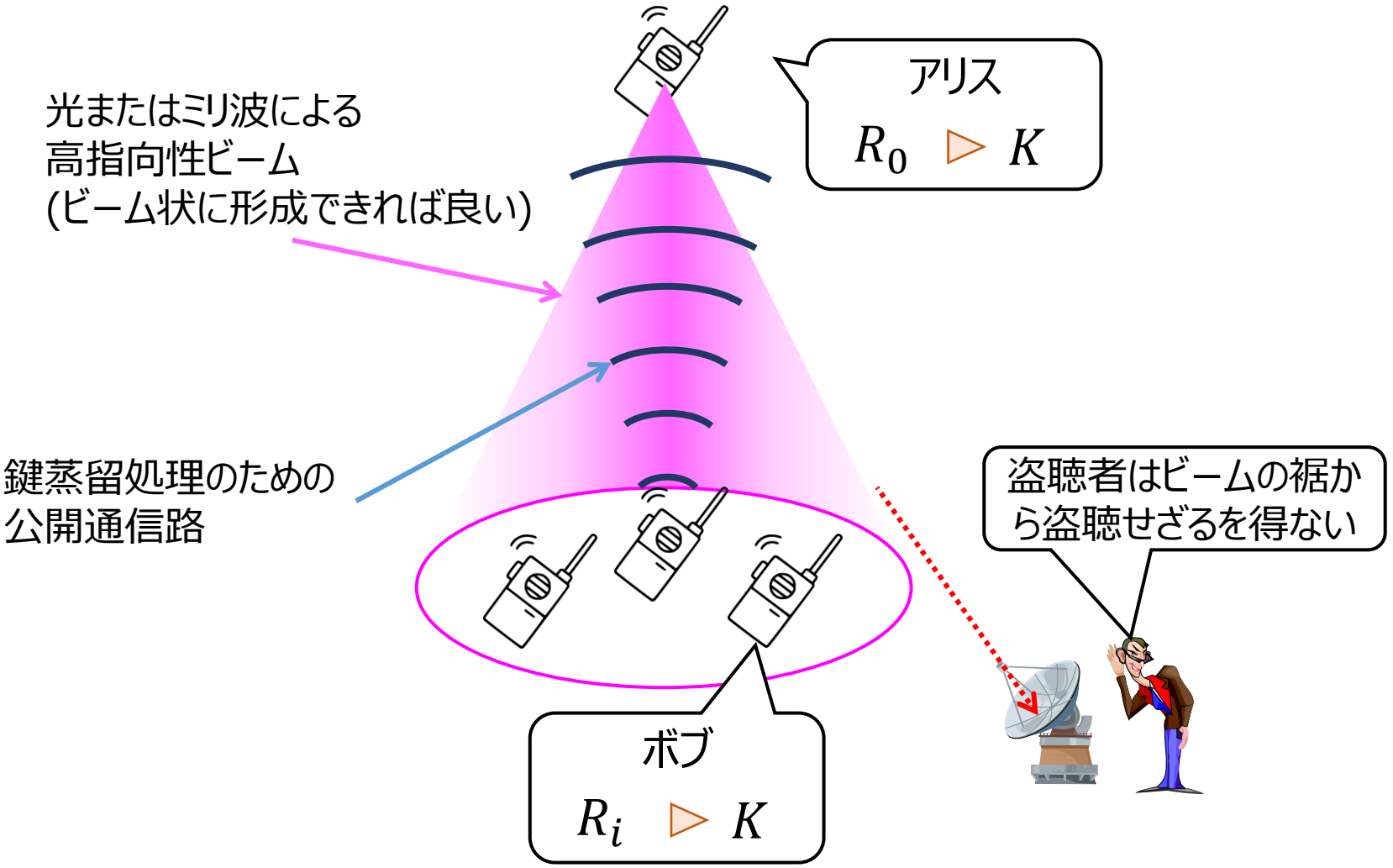
企業様への期待

- DIMMに限らず、大気ゆらぎに関する測定技術を持つ企業様との共同研究を希望する。
- また、DIMMに限らず、物理レイヤ暗号技術の実用化に向けて、以下の技術を持つ企業様との共同研究を希望する。
  - 誤り訂正技術
  - 光空間通信・可視光通信技術
  - ミリ波通信技術
  - モーター制御技術(装置の指向制御のため)
  - LIDAR技術(通信路の見通し確保のため)
  - AI技術(過去のデータを活用した予測を行うため)

本技術に関する知的財産権

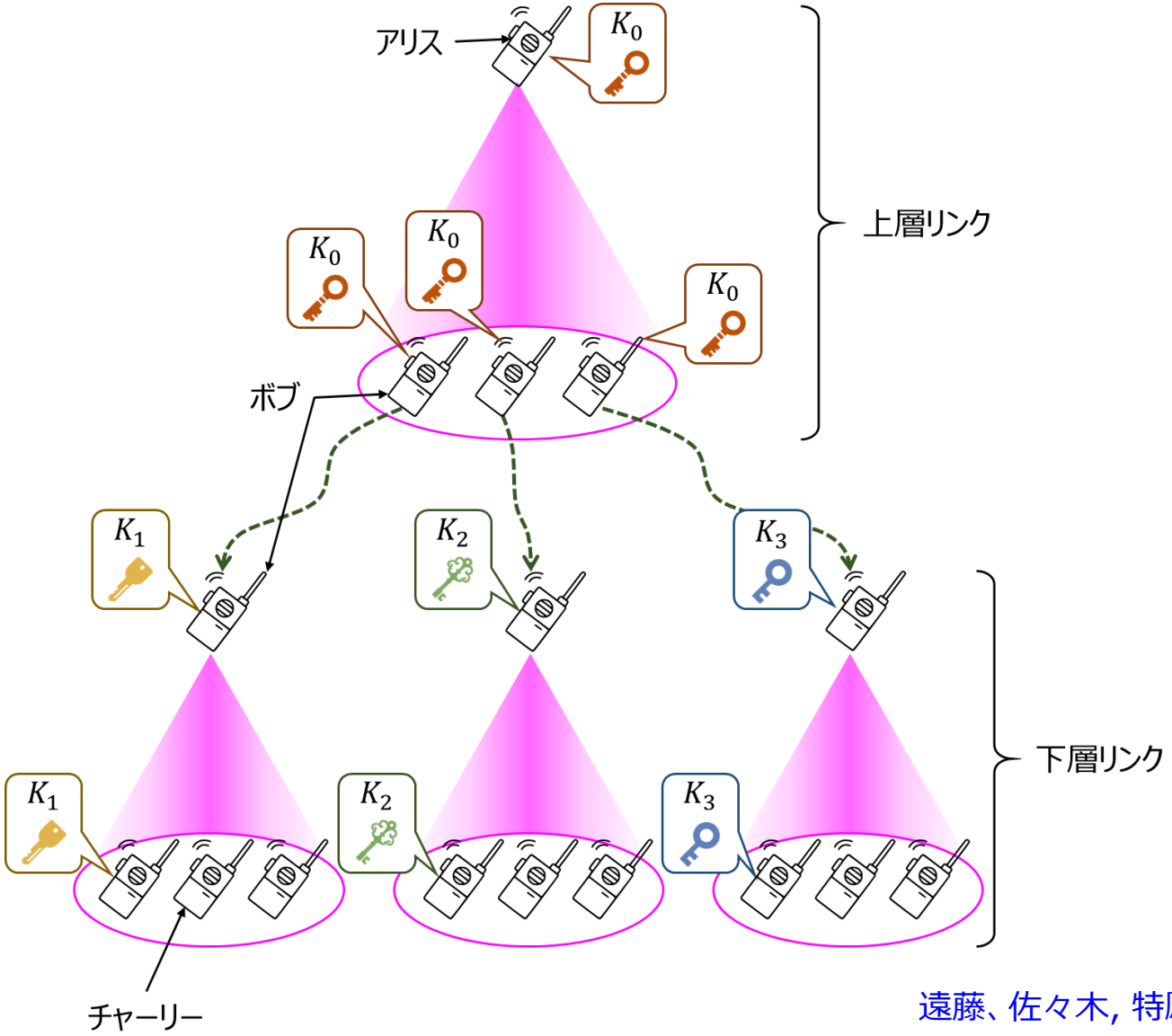
- 発明の名称　：秘密鍵共有方法及びシステム
- 出願番号　：特願2019-235286
- 出願人　：情報通信研究機構
- 発明者　：遠藤 寛之、佐々木 雅英

関連技術１：物理レイヤ暗号によるグループ鍵共有



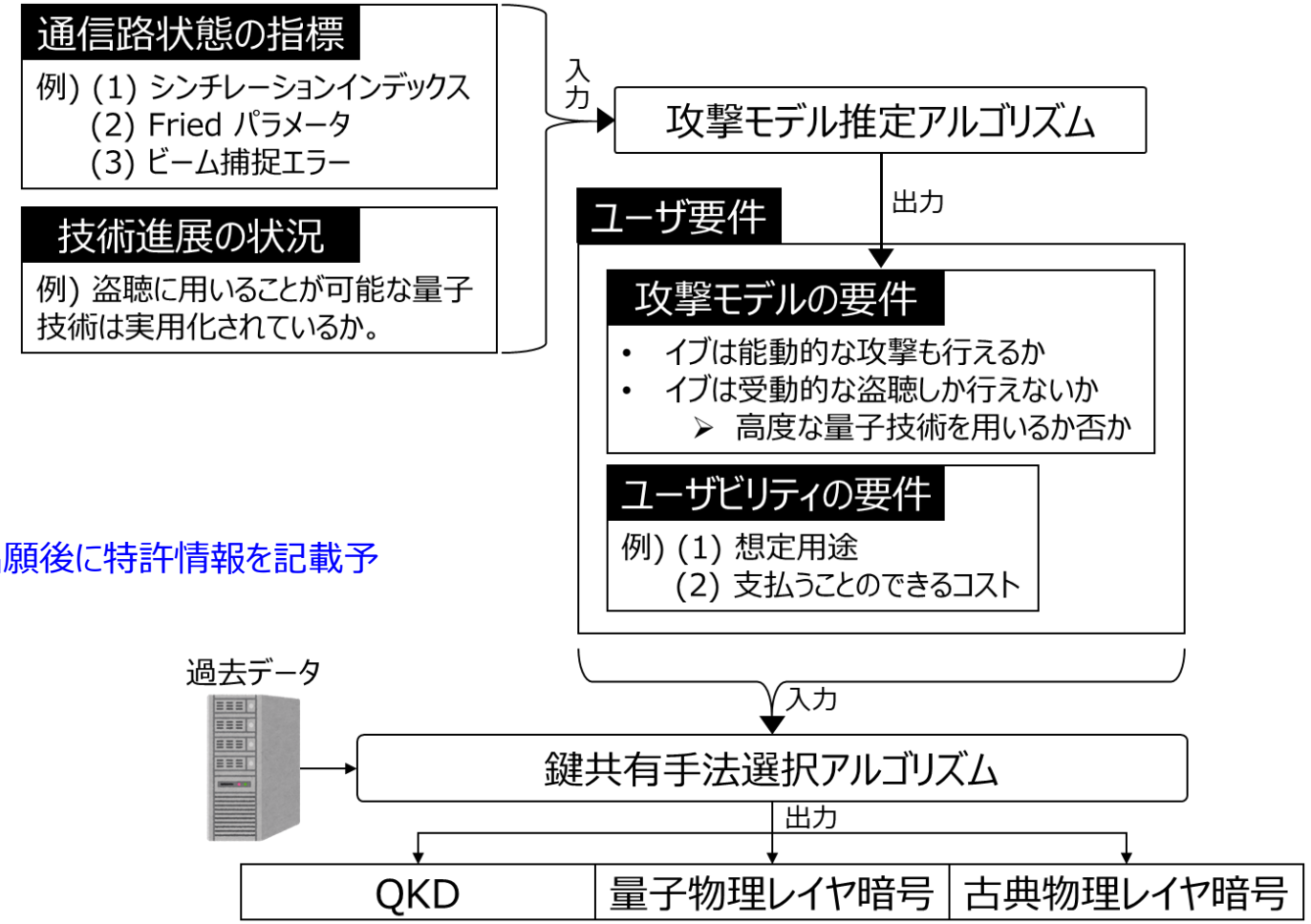
遠藤、佐々木, 特願2020-012325

関連技術１：物理レイヤ暗号によるグループ鍵共有



遠藤、佐々木, 特願2020-012325

関連技術２：見通し通信向けの適応的鍵共有技術



※10月4日の出願後に特許情報を記載予定

安全性の課題や性能が異なる3つの鍵共有技術を用途に応じて使い分けることがで、一つの技術だけではカバーしきれない、広大な利用シーンをカバーできる技術を生み出すことができる。

お問い合わせ先・謝辞

国立研究開発法人　情報通信研究機構
イノベーション推進部門
知財活用推進室

ＴＥＬ　０４２－３２７－６９５０
e-mail　ｉｐｐｏ@ｍｌ．ｎｉｃｔ．ｇｏ．ｊｐ

謝辞

- 本発表には、総務省「ICT重点技術の研究開発プロジェクト（JP MI00316）」のうち「衛星通信における量子暗号の研究開発（JPJ007462）」の一環として実施されたものを含む。
- 本発表には、科研費(17H01281、19K14992)の助成を受けて行われたものを含む。