Orchestrating a brighter world

NEC

IPSJ/TTC共催セミナー
「量子コンピュータ＆量子通信の最新動向と展望」

量子鍵配送ネットワークとアプリケーション

2019年４月11日

NECシステムプラットフォーム研究所　田島　章雄

本発表の一部は情報通信研究機構「セキュアフォトニックネットワーク技術の研究開発」、内閣府革新的研究開発推進プログラム「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」、戦略的イノベーション創造プログラム第2期「光・量子を活用したSociety 5.0実現化技術」の成果である。

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。

アウトライン

1. イントロダクション
2. 量子鍵配送 (QKD) ネットワーク
   - QKDネットワークへの要求
   - QKDネットワークアーキクチャ
3. QKDシステム
   - NECのQKDシステム
   - 紹介ビデオ(6 min.)

4. QKDネットワークのアプリケーション
   - 有線暗号通信(QKD-AESハイブリッドシステム)
   - 無線暗号通信(秘匿スマートフォンシステム)
5. 標準化動向
6. まとめ

Background

光ファイバ通信においても盗聴が行われている可能性

- 国家レベルの秘匿通信がタッピング＆解読されている危険性
- スノーデンファイル;

http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

- 近い将来、個人情報にも同様な危険がおよぶ可能性
  - 金融情報
  - ゲノム情報

暗号化通信を行うためには、離れた拠点間での暗号化鍵の共有が課題

- 現代暗号による共有(計算量による安全性保証)
  - 公開鍵暗号, 共通鍵暗号
- 人手による鍵共有 (人に対する信頼).

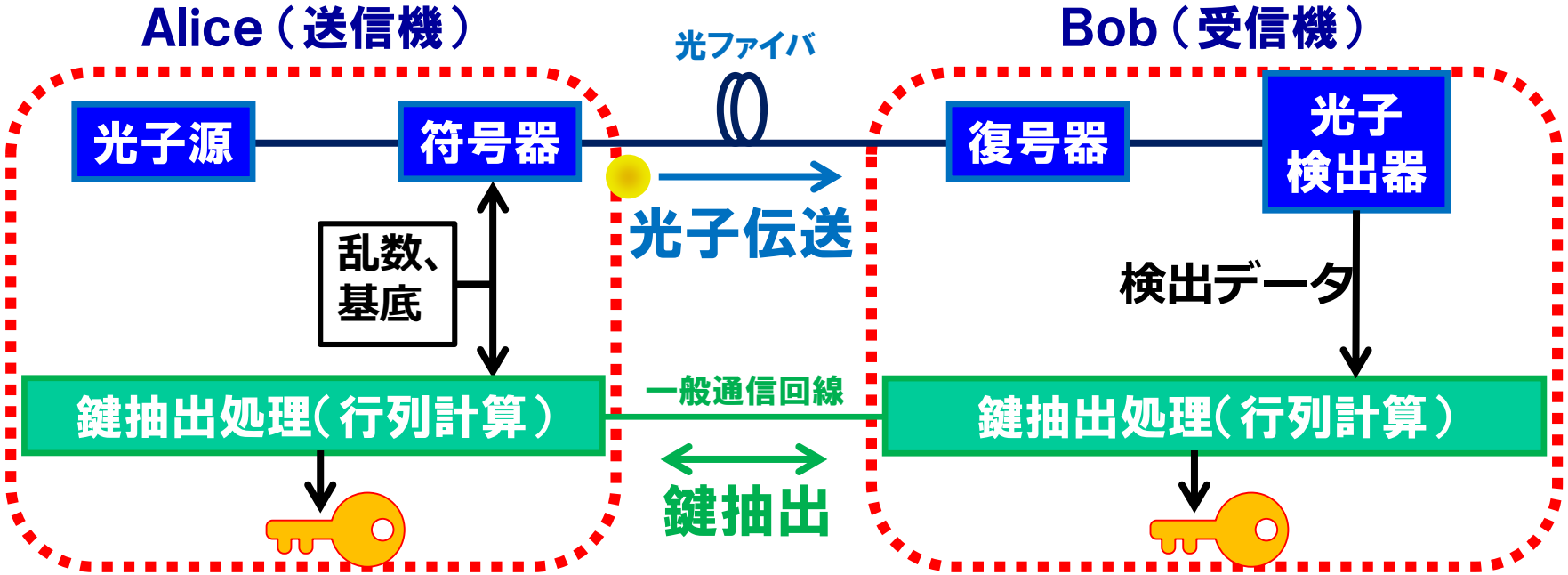
⇨量子鍵配送(Quantum Key Distribution)による安全な鍵共有

GCHQ: Government Communications Headquarters

量子鍵配送(ＱＫＤ)システム概要

光子一つ一つに情報を載せることで、盗聴不可能な暗号鍵共有技術

- 受信した情報のみを用いて鍵生成
- 量子力学による安全性保証



ワンタイムパッド(OTP)暗号の鍵として用いれば、解読不可能な暗号

- データと同じ長さの暗号鍵を一度限りで使い捨て
- 情報理論による保証

Point-to-pointのリンク

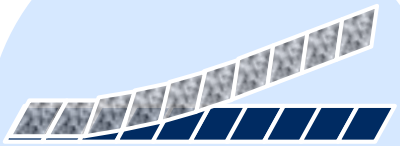
ワンタイムパッド

平文と同長の暗号鍵で暗号化し、使用した暗号鍵は破棄

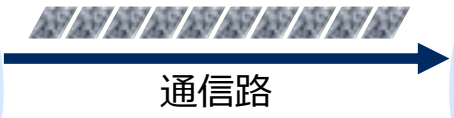
ワンタイムパッド = 送信者及び受信者が、送受信するメッセージと同じ長さの鍵を事前に共有しておき、その鍵を使用してメッセージの暗号化・復号を実施する暗号方式

ポイント ・**平文と同じ長さの暗号鍵によって暗号化して通信する**

暗号化

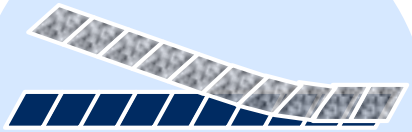


データの帯(平文)に目隠しシール(暗号鍵)を1bitずつ貼る



目隠しシールが貼られた(暗号化)状態で通信する

復号



目隠しシールをはがし、データの帯を確認する

暗号鍵は破棄

ポイント ・**使用済み暗号鍵は捨て、二度と使用しない**

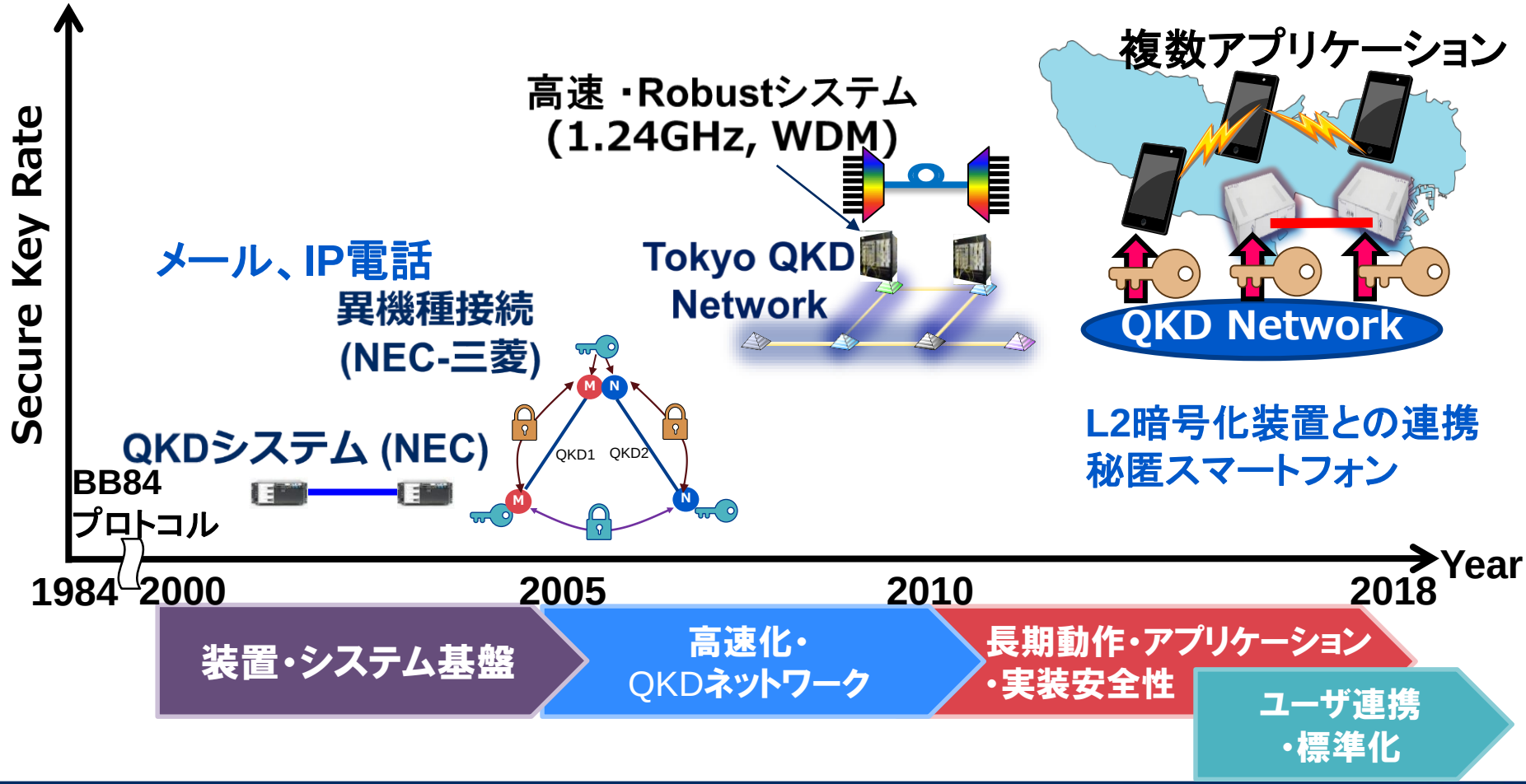
量子暗号技術の発展

1984	BB84 protocol	Bennett, Brassard
1989	First QKD experiment 32 cm free space transmission, polarization-based	Bennett
1993	10 km over optical fiber Phase-modulation-based QKD	 BT
1996	Plug & Play QKD Self-balanced interferometer, 23 km transmission	 ジュネーブ大
2000 **～**	Practical QKD experiments (including field trial) 96 km field trial Two-weeks continuous QKD	 三菱 NEC
2005 **～**	Quantum Key Distribution Network R&D Boston area QKD network QKD Network in Viena Tokyo QKD Network	 BBN, Bosto大, Harvard大 SECOQC Pj. Japan (NICT) team
2010	High-speed QKD System Sinusoidally gated APDs The self-differencing avalanche photodiode PLC based WDM QKD system	 日大, NTT 東芝 NEC
2015 **～**	Stable QKD system (30+ days) 小金井-大手町 小金井-府中, Cyber Security Factory	 東芝 NEC

研究開発トレンドとNECの主要成果

商用アクセスファイバ
2週間連続動作(世界初)
7.15kbps@10dB, QBER~7.5%

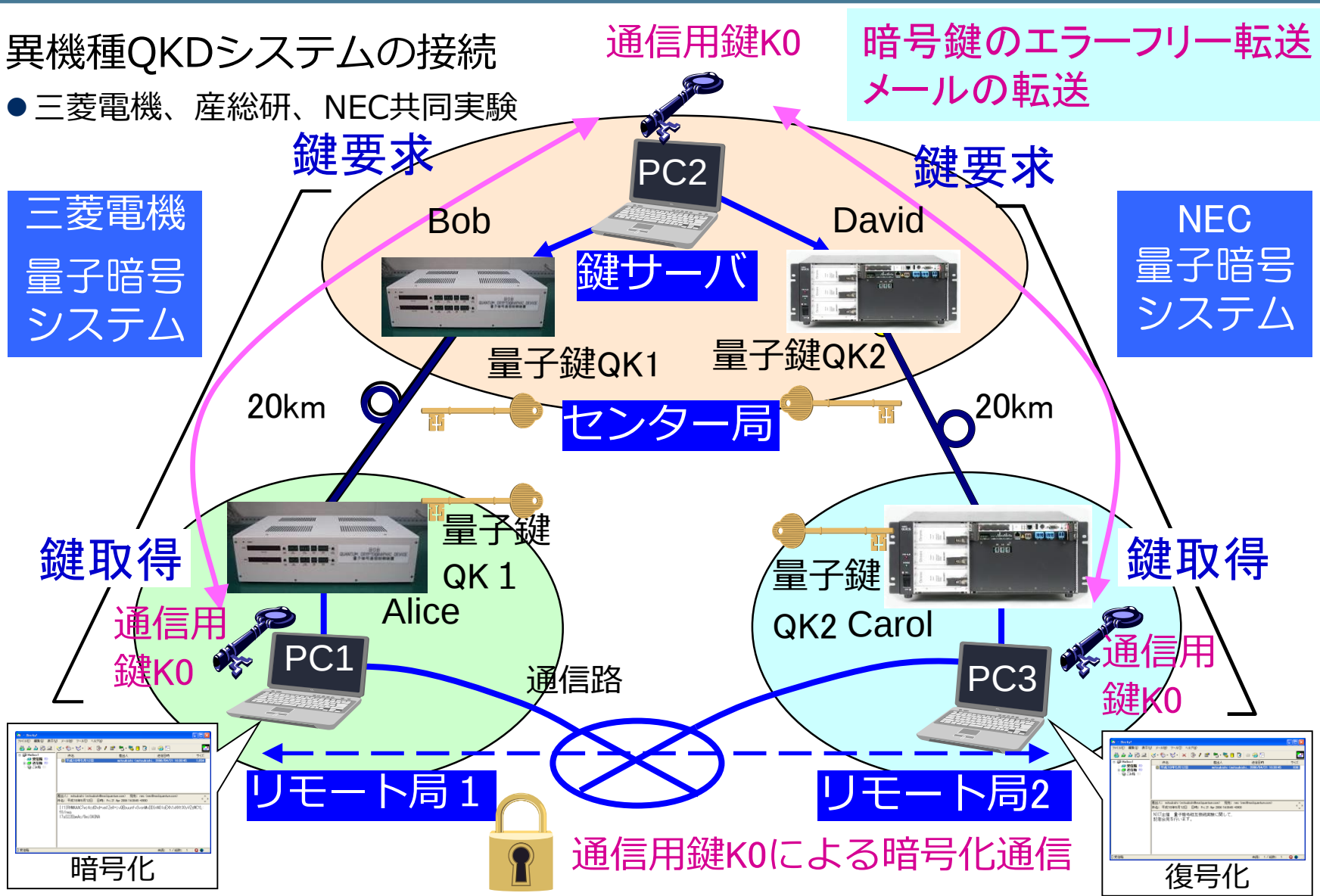
2波長 30日間連続動作(小金井-府中)
21週間連続動作(サーバルーム)
230kbps/λ@10dB, QBER<1.8%



QKDネットワークにむけた初期の実験　2006年

異機種QKDシステムの接続

- 三菱電機、産総研、NEC共同実験



田島ほか電子情報通信学会ソ大会B-10-21 (2006)

QKD技術に関する最近のニュース

QUANTUM XCHANGE(米国)ニュースリリース

- **June 26, 2018** – Quantum Xchange today launches the first quantum, fiber-optic network in the United States and commercial Quantum Key Distribution (QKD) service for quantum-safe data protection based on the laws of quantum physics.

https://quantumxc.com/quantum-xchange-launches-the-first-quantum-network-in-the-united-states-to-provide-quantum-safe-encryption-over-unlimited-distances/

QuantumCTek (中国)ニュースリリース

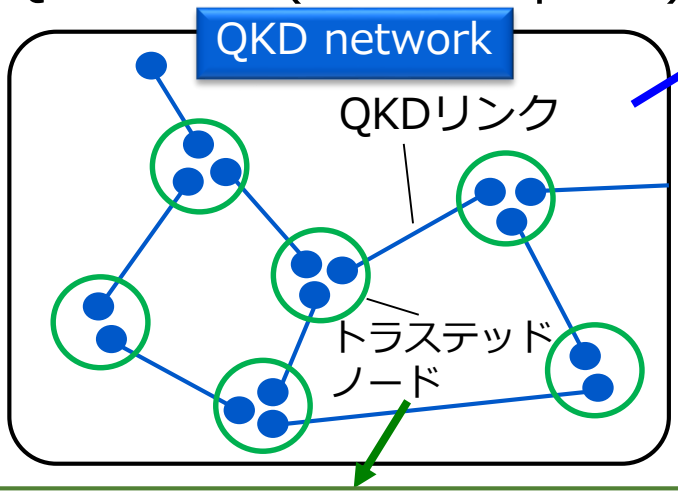
Following the Industrial and Commercial Bank of China and Bank of Communications, Bank of China Succeeds in Realizing 1000 Kilometers of Quantum Cryptography Application

- **January 19, 2018** - In the first half of 2017, the technologies and products for quantum secure communications of QuantumCTek have assisted many large state-owned commercial banks such as Industrial and Commercial Bank of China and Bank of Communications to realize quantum encrypted transmission of core business data.

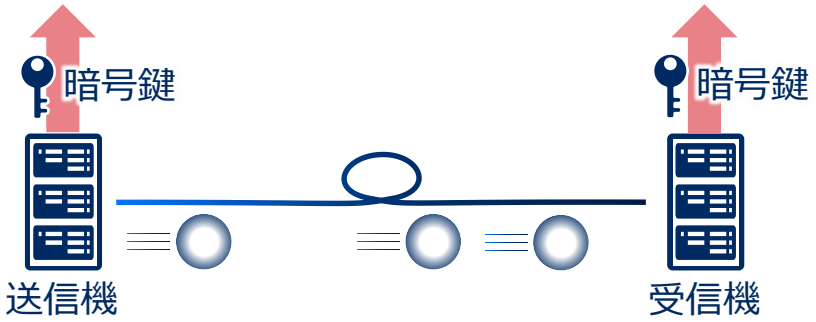
http://www.quantum-comm.com/English/News/2018/2018/0308/498.html

QKDネットワークとは

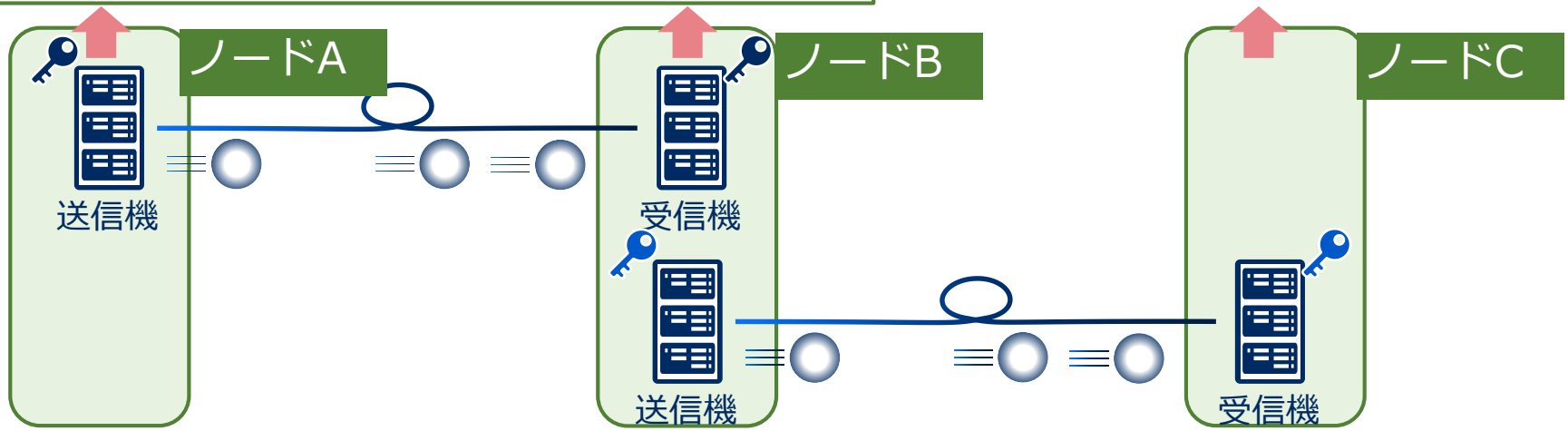
- 任意の2ノード間で情報理論的に安全な鍵共有を実現
- QKDリンク(Point-to-point)＋トラステッドノード



QKDリンク: p-to-pの鍵共有



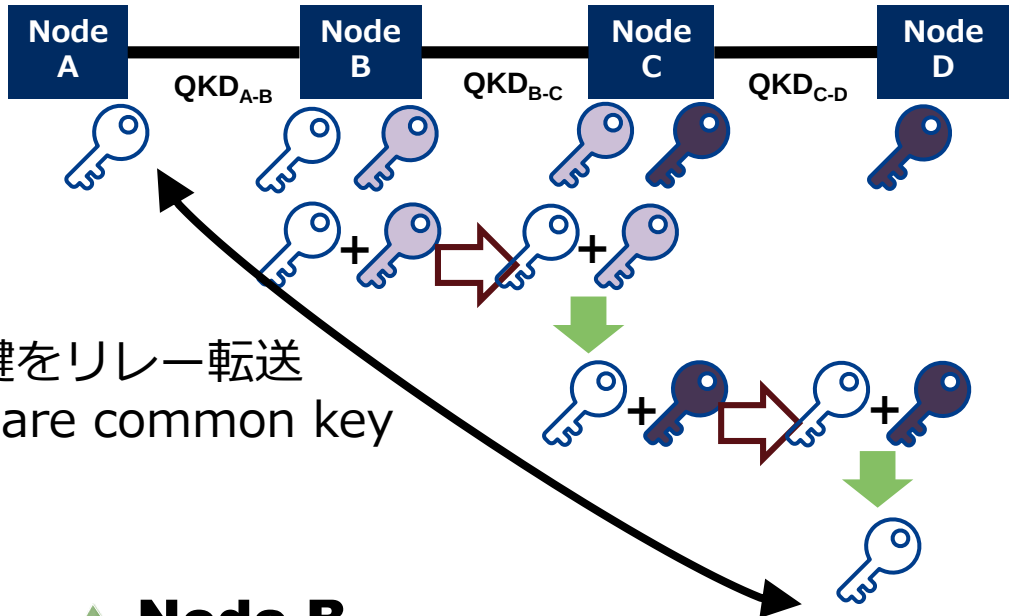
トラステッドノード：鍵のリレーと供給



鍵リレー技術

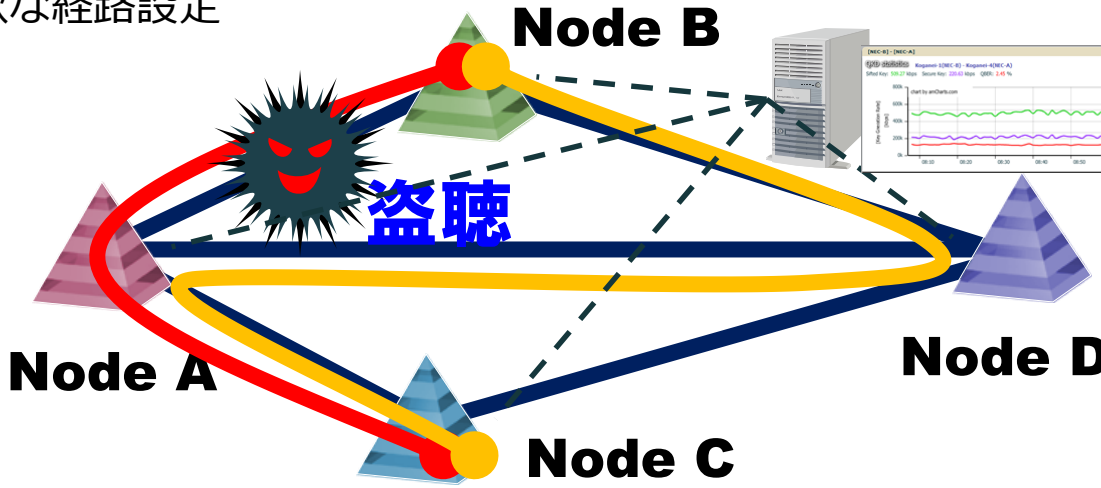
直接QKDリンクで接続されていないノード間で安全に鍵共有する技術

- 長距離対応



OTP暗号化により鍵をリレー転送
Nodes A and C share common key

- 柔軟な経路設定



リレー経路変更
B→A→C
B→D→C

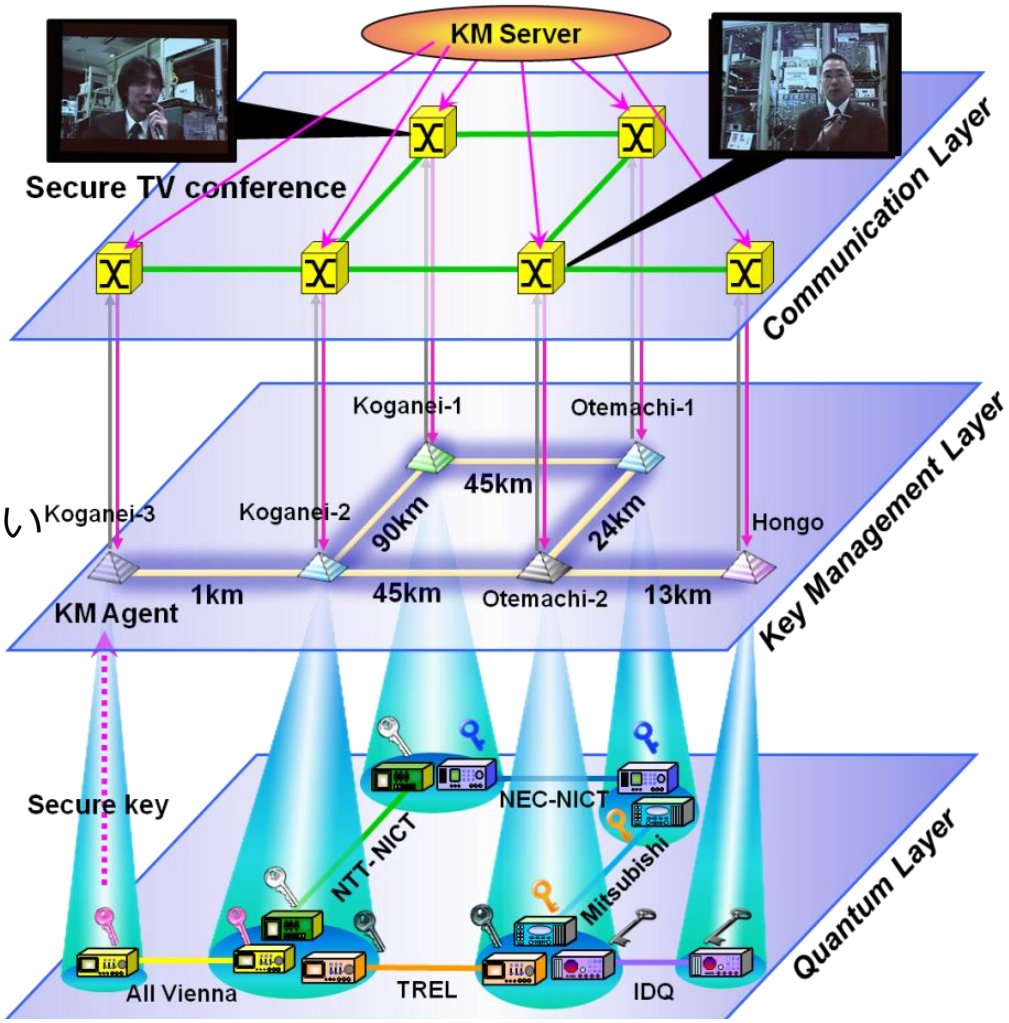
2010年　東京QKDネットワーク構築

都内にQKDネットワーク構築

- 大手町、小金井、本郷を拠点
- 6ノード構成のQKDネットワーク
- 複数機関開発のQKD装置
  - NEC, 東芝UK, NTT, All Viena, IDQ, 三菱

秘匿TV会議のデモ実施

- QKD装置によって生成した量子鍵を用いてビデオ信号をOTP暗号化
- 一対一(Point to point) 通信
- TV会議アプリケーションに特化



M. Sasaki et al., Opt. Express 19, 10387 (2011)

アプリケーション拡張
→新規ネットワークアーキテクチャ、機能、マネージメント

QKDネットワークへの要求

1. 多様なネットワークトポロジーへの対応
   1. Point-to-point
   2. リング、メッシュ他

2. 拡張性、可用性

3. アプリケーションに依存しない鍵供給
   1. 高速PTP 通信
      - 例：データセンタと遠隔バックアップセンタ
   2. Multipoint-to-multipoint (MPTMP)通信
      - 例：複数のスマートフォン間での秘匿通信

4. 多様なQKD装置、プロトコルへの対応
   1. BB84
      - NEC, 東芝
   2. CV-QKD
      - 学習院大
   3. RR-DPS QKD, Coherent one-way etc.

QKDネットワークアーキテクチャ (3レイヤ構成)

鍵供給レイヤ

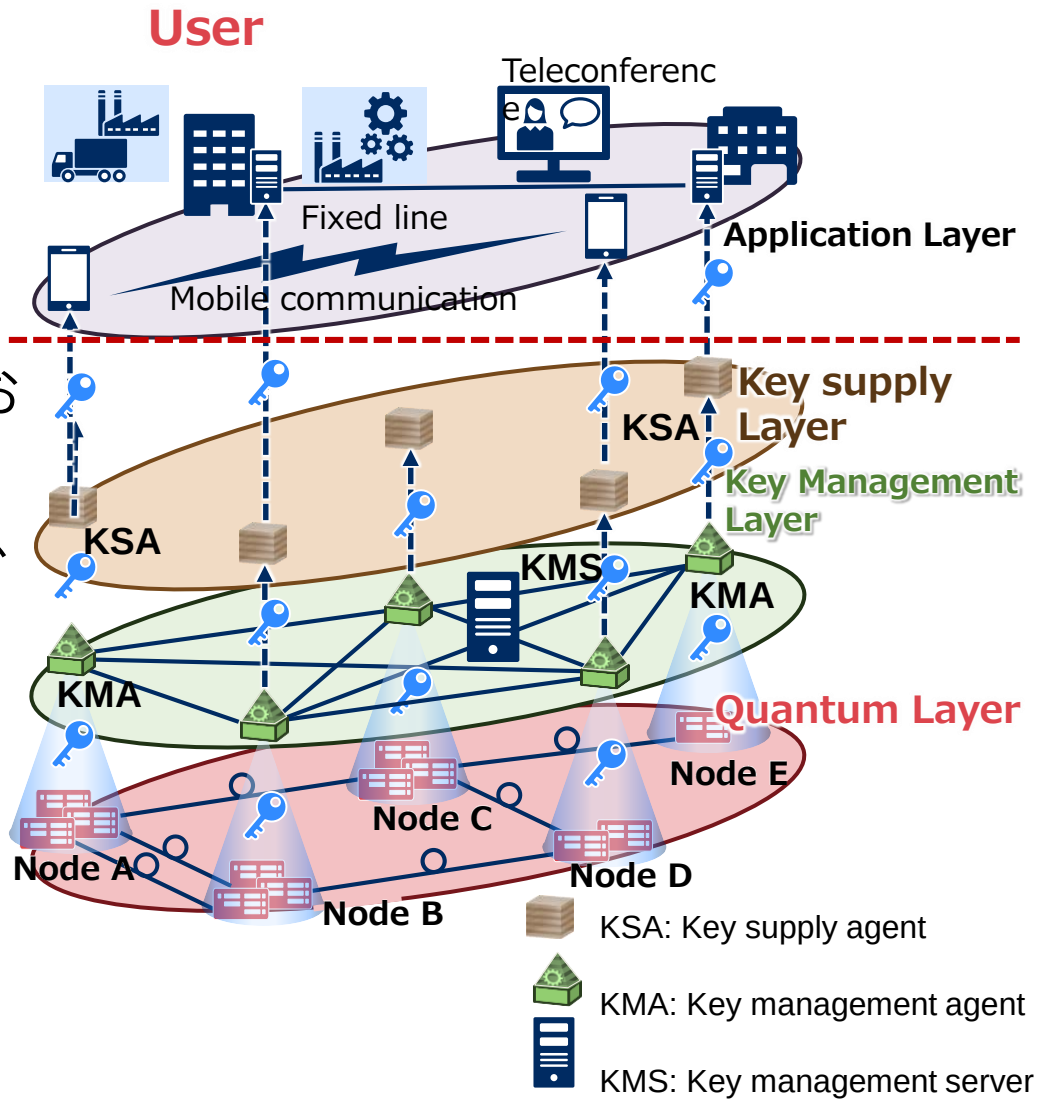
- アプリケーションへの鍵供給

鍵管理レイヤ

- 鍵蓄積、鍵リレー経路の管理および制御
- パフォーマンスモニタ(誤り率、鍵消費/蓄積量)
- 鍵供給レイヤへの鍵受け渡し

量子レイヤ

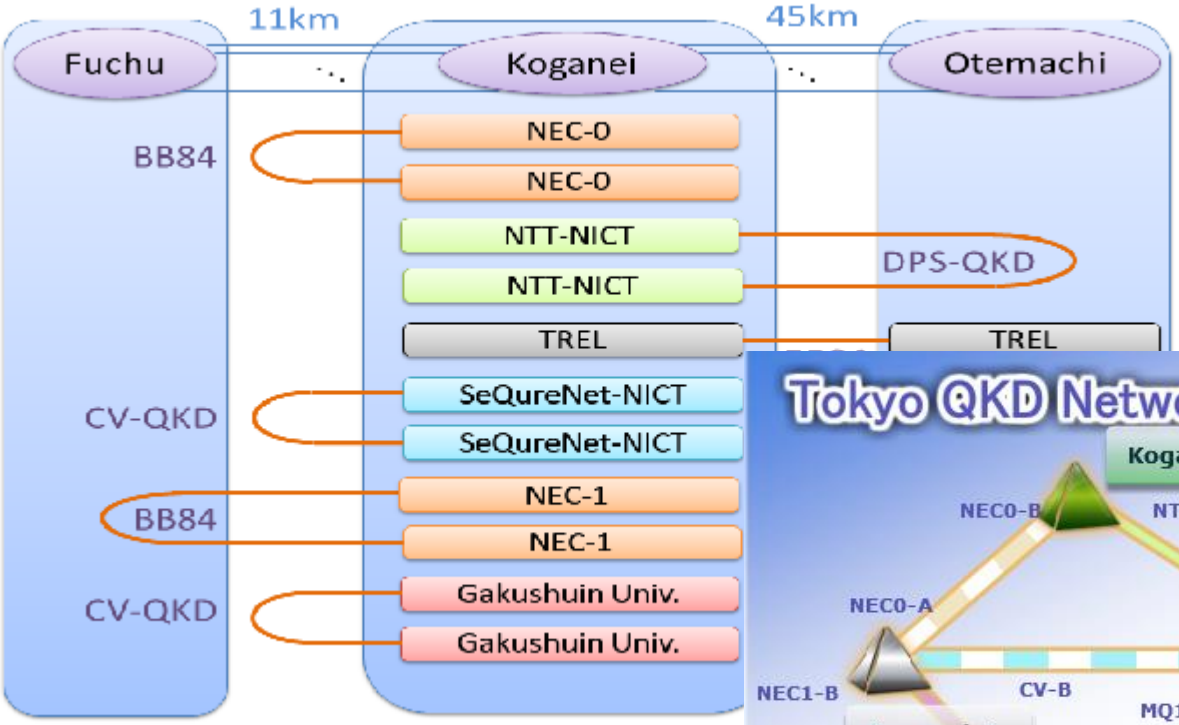
- QKDリンクによる鍵生成

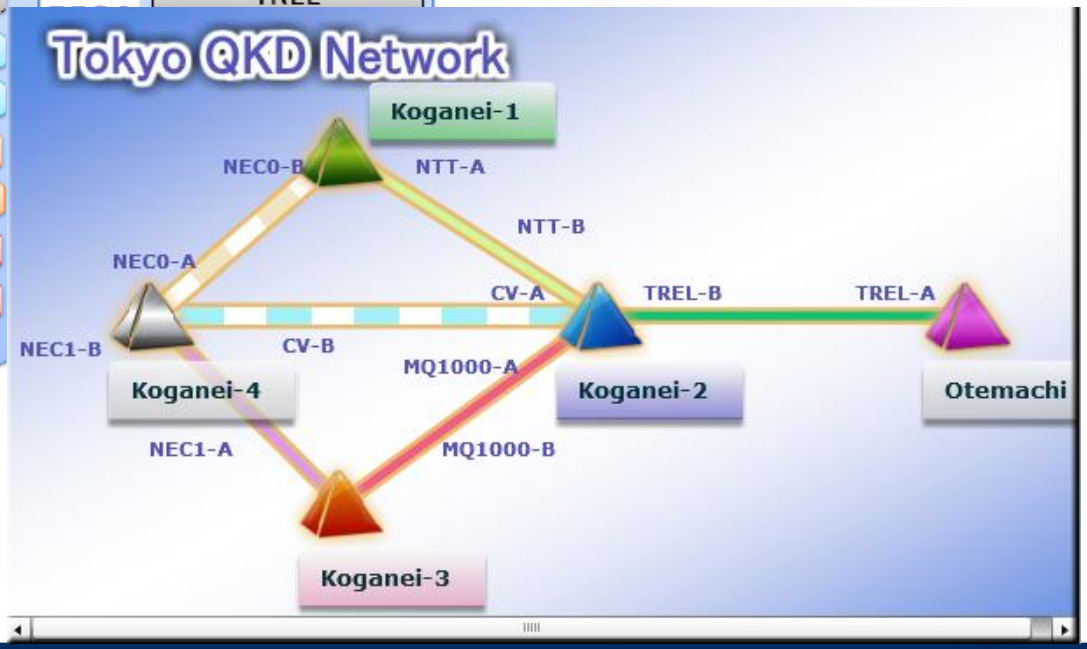


東京QKDネットワーク(アップデート)

2010年構築したものからアップデート

- 新ネットワークアーキテクチャ
- 拠点の変更：大手町、小金井、府中





URL: http://www.tokyoqkd.jp/

NECのQKD装置

・波長多重システムにより、暗号鍵の需要に対応した暗号鍵生成装置を実現

1波長システム(基本システム)

特徴

- **小型化/低コスト化**

用途

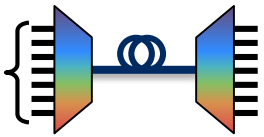
- 100kbps程度の通信用途 (例：VoIP)

送信機　受信機

波長多重システム(拡張システム)

特徴

- **暗号鍵生成の高速化**

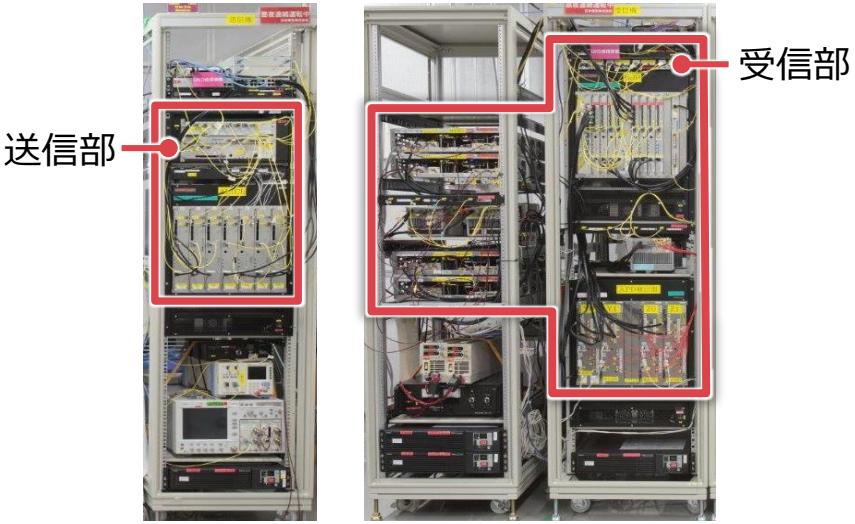


NECは8波長多重システムを検証

用途

- 1Mbps程度の通信用途 (例：TV電話)

送信機　受信機

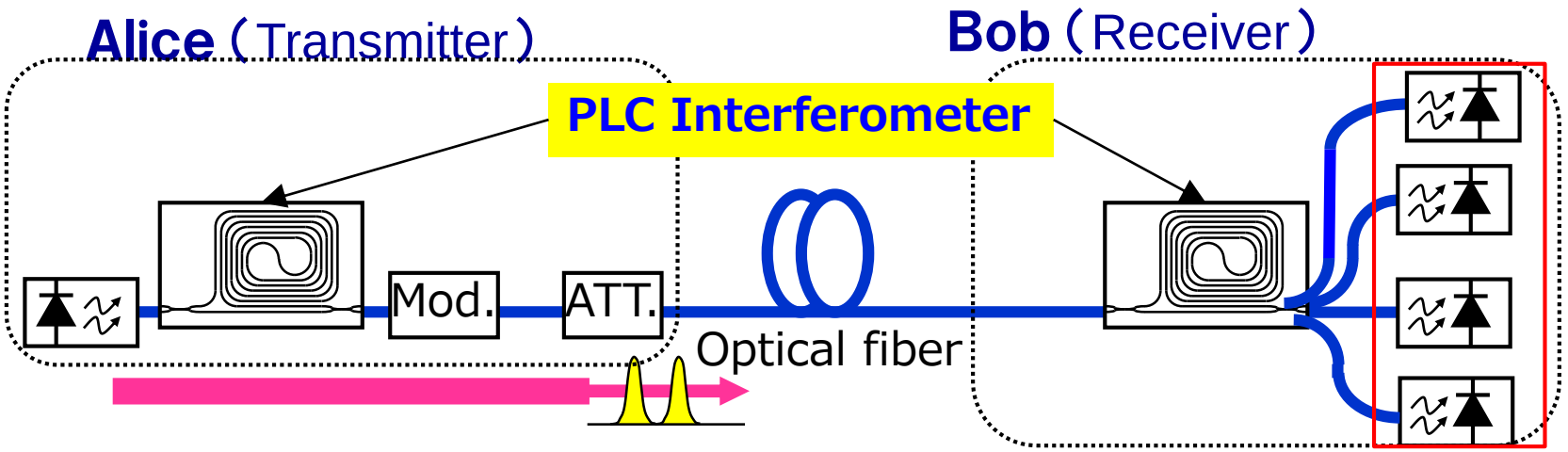


安定動作のための要素技術

PLC* 光干渉計

- 外部環境変動の影響を受けない光子伝送
  - 温度無依存
  - 偏波無依存
    - OPGW(光ファイバ複合架空地線)のような100 KHz以上の高速偏波変動があっても問題なし
- メカニカル部品不要
  - 偏波制御器やファイバ遅延制御器不要
  - 高信頼

＊PLC: Planar Lightwave Circuit



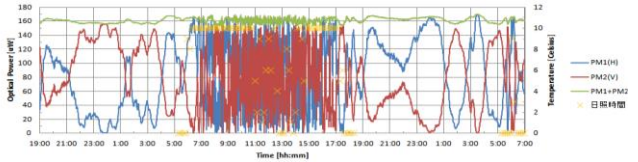
Stable photon transmission without mechanical device is achieved.

環境変動の影響を受けない鍵生成

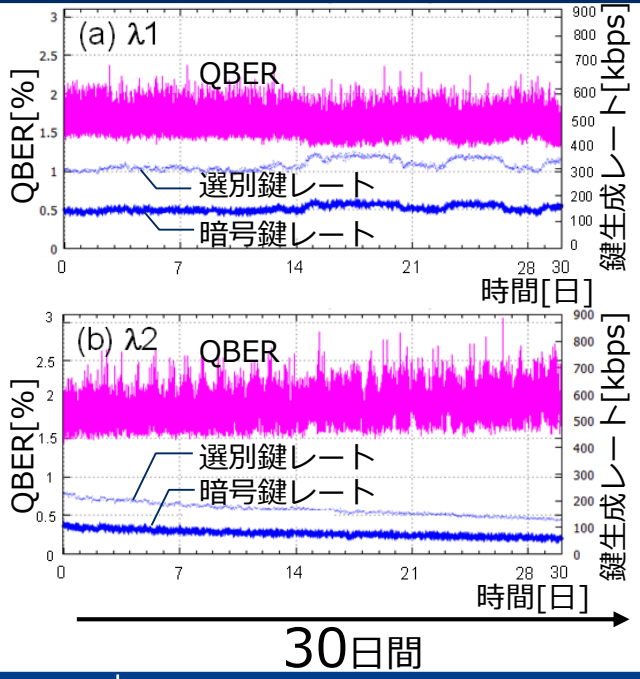
環境条件の厳しいフィールドファイバでの安定動作確認(技術実証)

実験の位置関係

偏波の時間変動

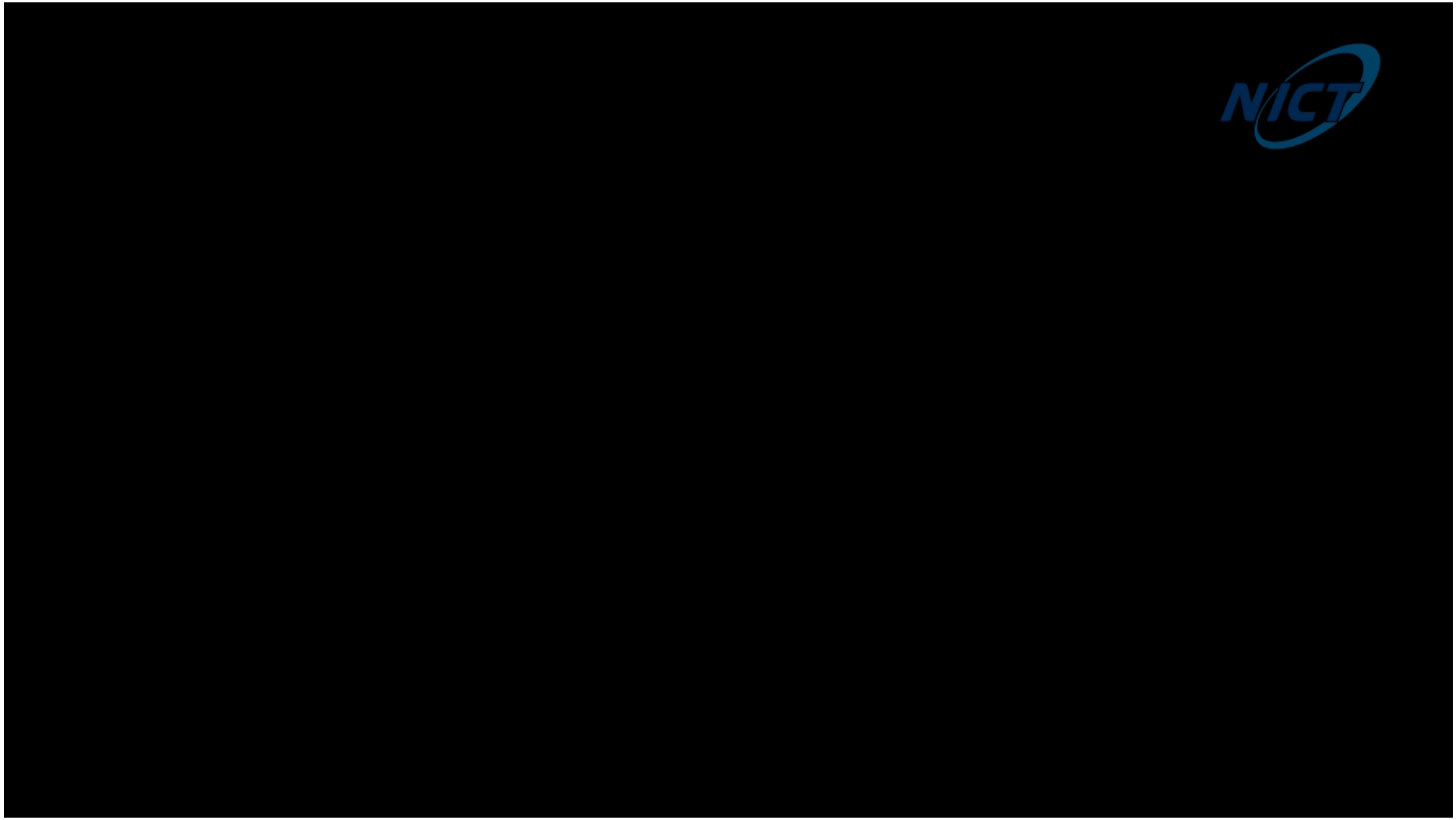


30日間連続稼働評価結果



	QBER [%]	選別鍵	暗号鍵
2λ Total	1.70	483.3 kbps	112.4 kbps

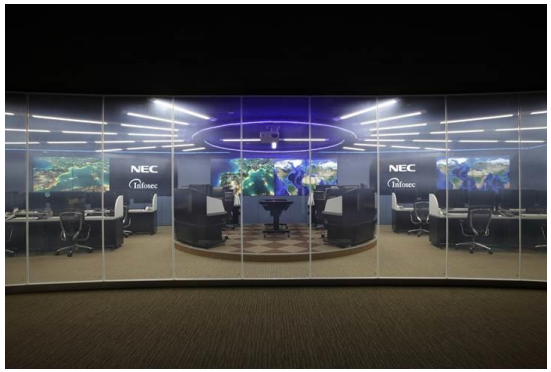
紹介ビデオ



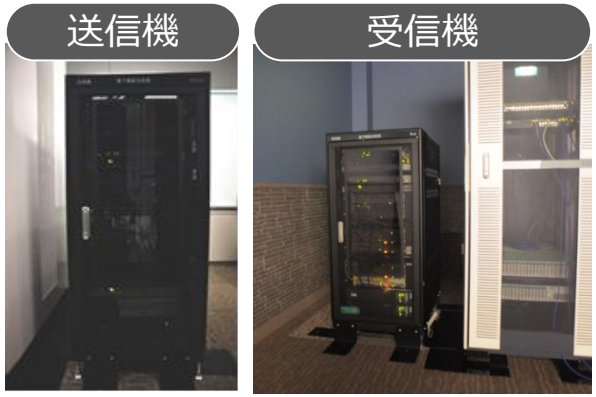
実環境における評価

**評価実験により、実用化に向けたノウハウを蓄積し、
暗号鍵の生成から活用までのトータルソリューションを提案**

- QKD実用化に向けた評価実験をサイバーセキュリティ・ファクトリーで開始
  (2015年9月プレスリリース：http://jpn.nec.com/press/201509/20150928_03.html)



サイバーセキュリティ・ファクトリー



サイバーセキュリティ・ファクトリーに設置したQKD装置

ポイント1

実用化に向けてのノウハウを蓄積

量子鍵配送装置を長期間**実環境で**評価し、**理論検証**及び安全性評価等を推進

ポイント2

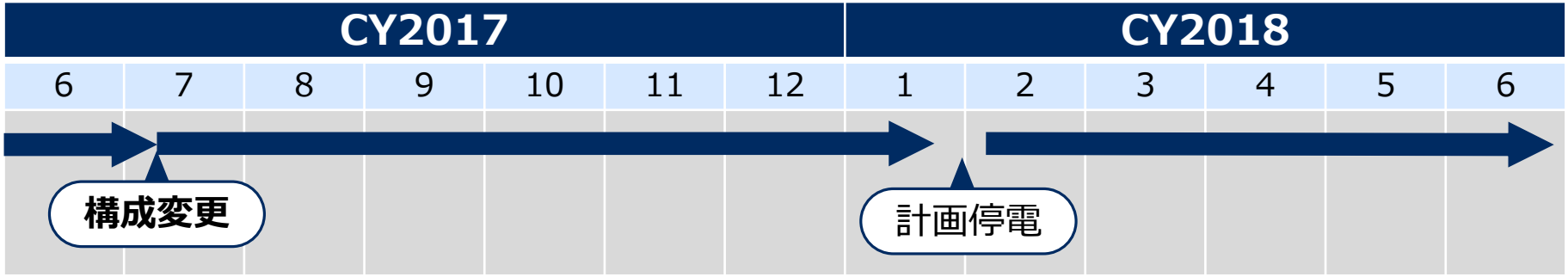
暗号鍵の生成から活用までのトータルソリューションを提案

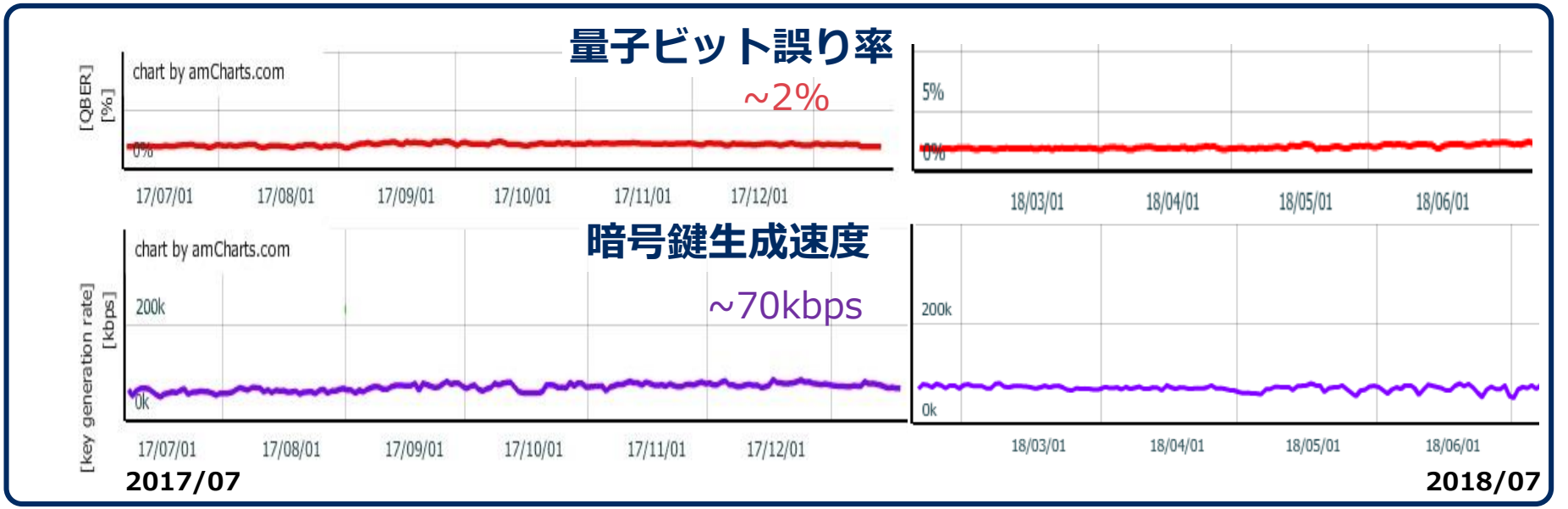
量子鍵配送に加え、暗号鍵を用いたアプリケーションとして、
NEC製品をカスタマイズした回線暗号装置(現代暗号)と暗号鍵のハイブリッド運用について
評価を行い、**ユーザの運用を考慮した適用方法**を検討

長期間動作試験状況(2017/7~2018/7)

■ **NECサイバーセキュリティファクトリーでの長期間動作試験継続(2017/7~)**
- **移設、ネットワーク構成変更、ビルの計画停電での停止以外、安定動作**

連続稼働評価結果





QKDネットワークのアプリケーション例

QKDの利用シーン

拠点間、建屋間

有線暗号通信への適用
(実用化に向けたQKDの基本構成)
▶ p.24

スマートフォン間

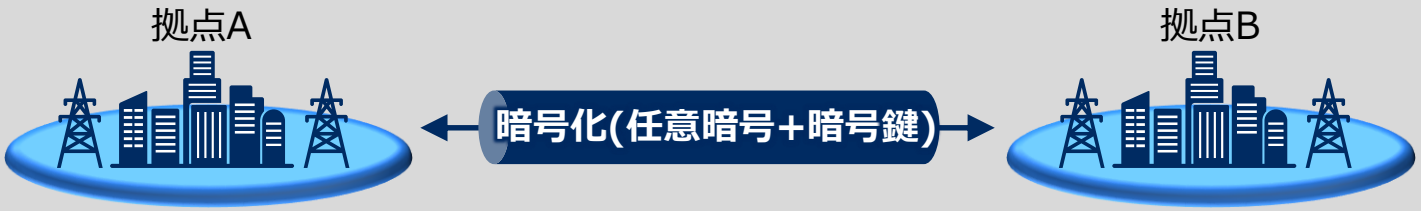
無線暗号通信への適用
(モバイル通信を想定)
▶ p.27

有線暗号通信への適用

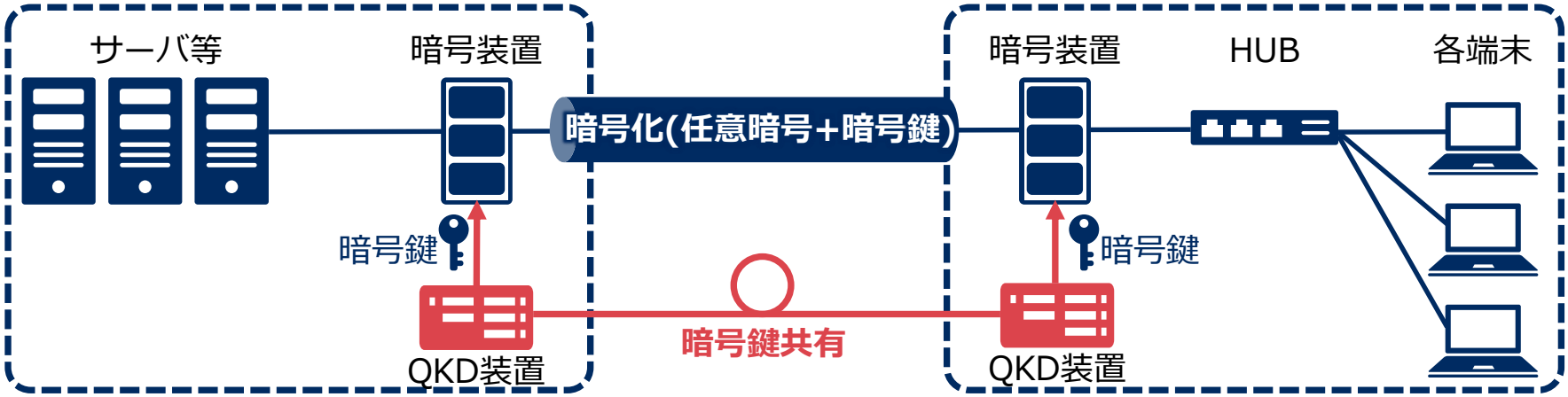
拠点間及び建屋間の通信情報保全に、量子鍵配送を活用

- 従来より運用する秘匿装置に対し、暗号鍵を任意の暗号の“Seed”として供給することで、**既存暗号方式を変更せずに、より安全な暗号運用が可能**
- 暗号鍵生成量の範囲で、**暗号鍵の更新頻度は自由に設定可能**(○日、△時間、□分等)

拠点間通信への適用例



建屋間通信への適用例

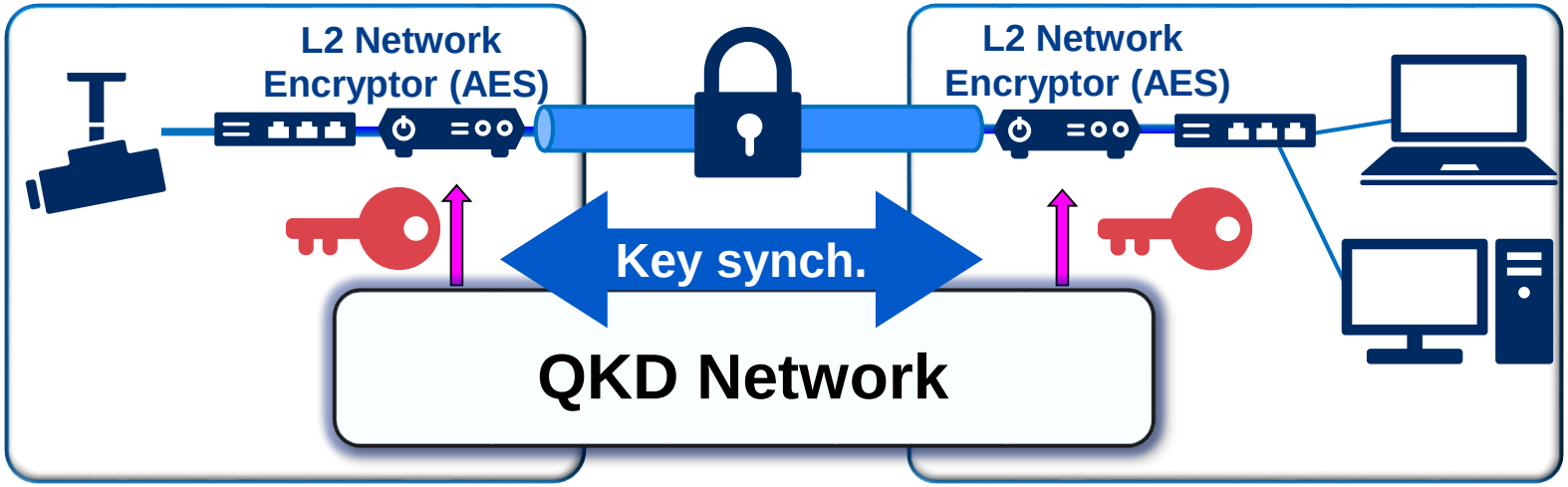


QKD-AESハイブリッドシステム

NECのレイヤ2回線暗号装置 “COMCIPHER(AES)”と統合

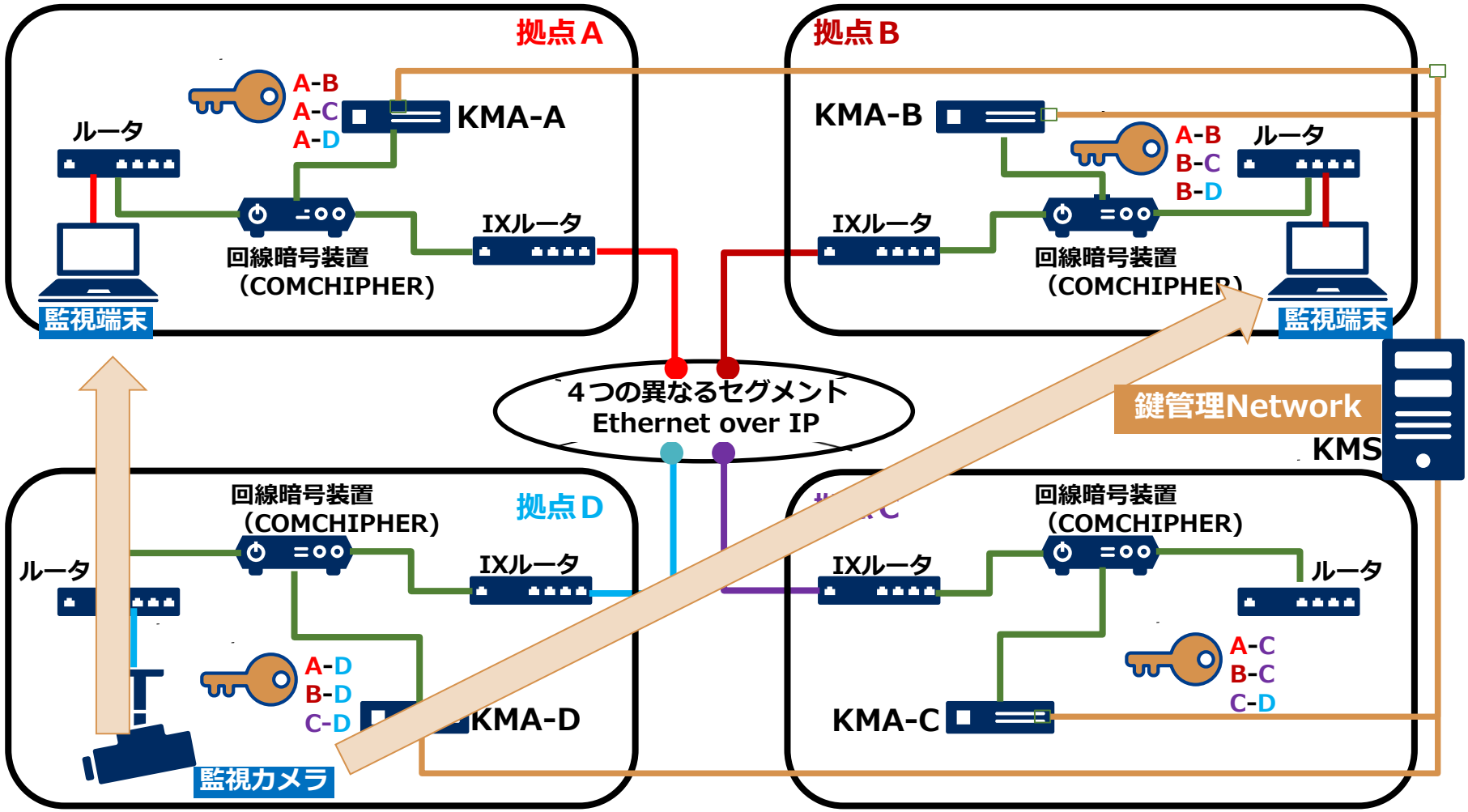
- 回線(Data over Ethernet)をAES暗号化
- QKDネットワークから供給 した量子鍵をAESの鍵として用い、周期的に更新
- 外部からの鍵供給と暗号装置間での鍵の同期機構を新たに開発。

Continuous operation in Cyber Security Factory was confirmed.



L2暗号化通信ネットワーク

- 複数拠点間で量子鍵をフルメッシュ共有、共有した鍵を回線暗号装置に供給
- 監視カメラ(拠点D)の映像を監視端末(拠点A、B)にL2暗号通信で送信

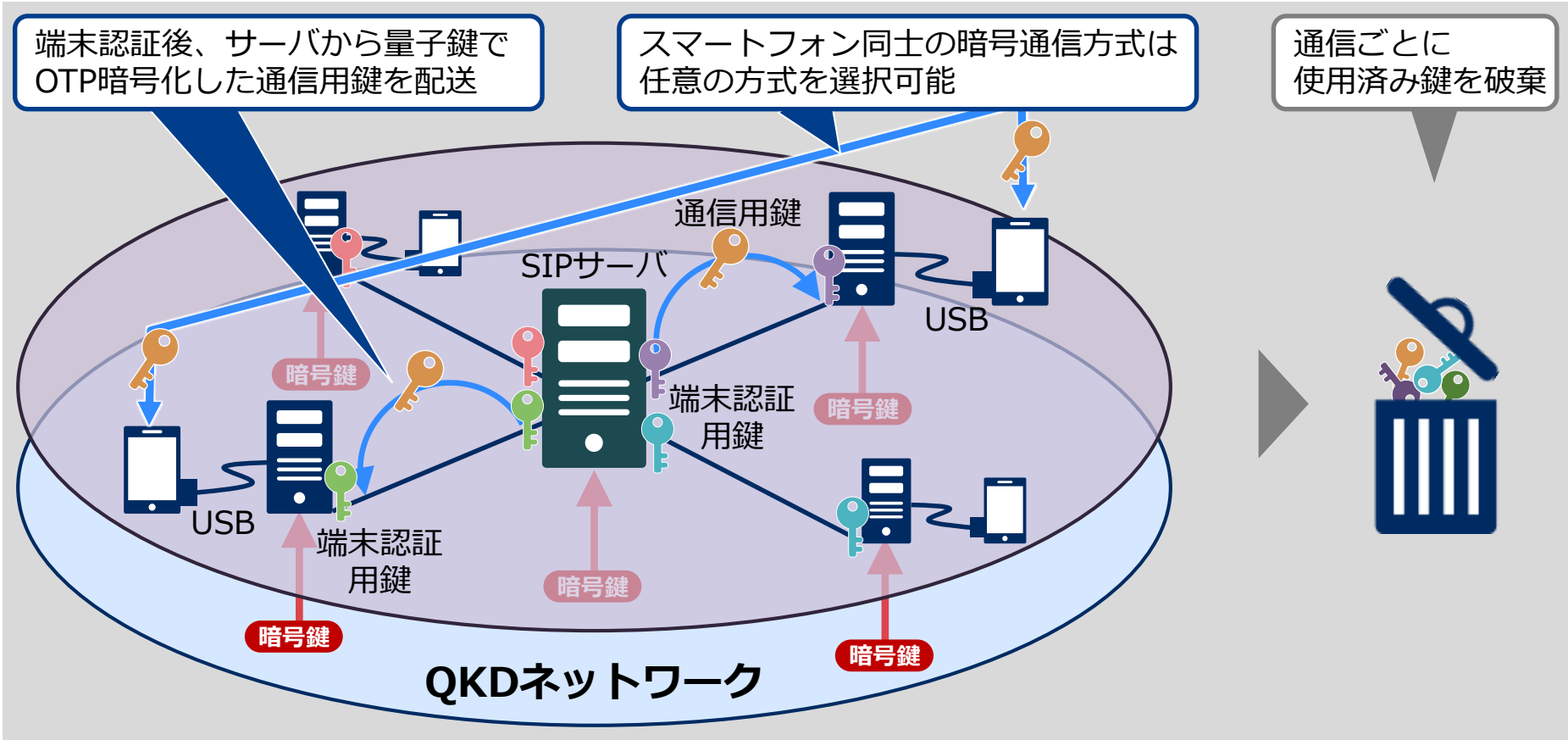


KMS: Key Management Server, KMA: Key management agent

無線暗号通信への適用(モバイル通信等)

スマートフォン同士の音声やデータ通信情報の保全に、量子鍵配送を活用

- **端末認証及びサーバ接続に、それぞれ量子鍵を活用**
- **通信用鍵の配送時に、量子鍵でOTP暗号化**することで、携帯網でも安全に鍵を配送
- **通信ごとに使用済み鍵を破棄**



量子鍵配送技術に関する標準化活動

量子鍵配送技術に関する標準化活動が活発化

- 韓国、中国からの国際標準化機関への提案

国際標準化団体および海外の地域・国内標準化団体のうち、以下をはじめとする団体において量子鍵配送に関連した提案および仕様作成が行われている。

- 国際標準化機関
  - ITU(International Telecommunication Union)
    - 1947年設立の国際標準機関
    - ITU-Tは通信分野の標準策定を担当する「電気通信標準化部門」
  - ISO/IEC(International Organization for Standardization/International Electrotechnical Committee)
    - ISO:1947年設立の国際標準機関
    - IEC:1906年設立の国際標準機関
    - ISOとIECが共同で合同委員会を組織し、電気・電子分野の標準化推進
- 地域・国内標準化機関
  - ETSI(European Telecommunications Standards Institute)
    - 1988年設立の欧州における電気通信産業に関する独立非営利標準化機関
  - CCSA(China Communications Standards Association)
    - 2002年設立の中国の通信産業規格を管轄する唯一の標準化機関

各標準化団体のアプローチ

ITU-T SG13/17

- QKDネットワークシステムとしてのアプローチ
  - QKDネットワークのフレームワーク (SG13)
    - Y.QKDN_FR “Framework for Networks to support Quantum Key Distribution”
  - QKDネットワークの機能アーキテクチャ(SG13)
    - Y.QKDN_Arch “Functional architecture of the Quantum Key Distribution network”
  - 鍵管理フレームワーク（SG13)
    - Y.QKDN_KM “Key management for Quantum Key Distribution network”
  - 鍵リレーや中継機能に関するセキュリティ(SG17)
    - X.sec_QKDN_km “Security Requirements for QKD Networks - Key Management”

日本チームとしても積極的に貢献

ISO/IEC JTC1/SC27 WG3

- QKDのセキュリティ要求や試験評価方法

ETSI ISG-QKD

- QKD装置・システムを起点とした仕様
  - コンポーネントやモジュール特性
  - 実装安全性
  - API

CCSA

- 装置、システム、ネットワーク全般

まとめ

QKDネットワークの機能とアーキテクチャ

- QKDリンク＋トラステッドノード
- 複数レイヤ構成ネットワーク

QKDネットワークを支えるQKDシステム

- Long-term and highly stable operation was achieved.

QKDネットワークのアプリケーション例

- 有線暗号通信(QKD-AESハイブリッドシステム)
- 無線暗号通信(秘匿スマートフォンシステム)

最新の標準化状況

- QKDに関する各標準化団体の動向とITU-Tにおける日本チームの寄与

近い将来、QKDシステム/ネットワーク技術によってセキュア通信インフラストラクチャが構築されることを期待。