量子暗号一問一答

初版

2020年5月26日

執筆者

小林 宏明	（主筆）	国立研究開発法人情報通信研究機構
遠山 裕之	（執筆）	日本電気株式会社
鯨岡 真美子	（執筆）	株式会社東芝
松尾 昌彦	（編集）	国立研究開発法人情報通信研究機構

本書は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society 5.0 実現化技術」（管理法人：量子科学技術研究開発機構）の光・量子通信出口戦略検討分科会 普及戦略タスクフォースによって編纂された。

目次

1.運用

目次

2.技術

3.ドキュメント

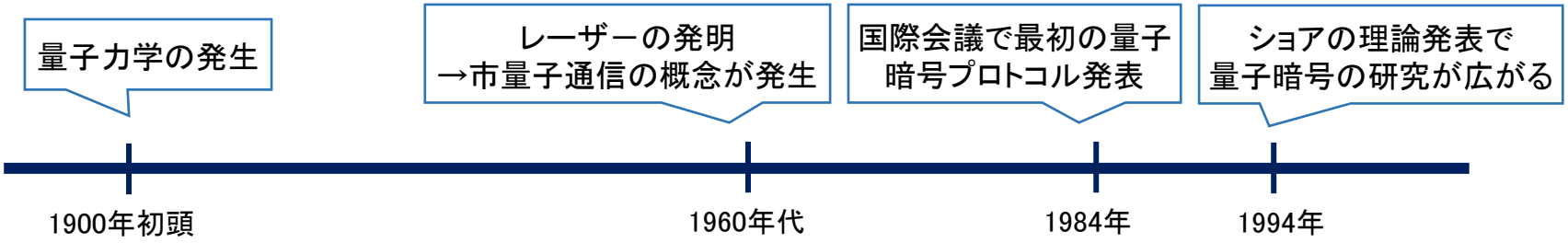
1.運用

Q1-1 量子暗号はどのようにして誕生したのですか？

A. 量子通信の利用技術が実現されて行くなか、偶然の出会いから量子暗号の理論が生まれました。

- 1900年初頭に量子力学が生まれ、それから半世紀ほど経って1960年代にレーザーが発明されるとほぼ同時に量子通信の概念も生まれました。それまで通信は電波を利用して行われてきましたが、実はレーザーに使う光の粒子のエネルギーは、温度に換算すると光子1つで1万度くらいに相当するのです。それだけのエネルギーを持っているレーザーを使えば、電波よりももっと情報量の大きな通信が出来るだろうというアイデアがあって、そこから少しずつ量子通信は発展して行きました。ただ、当時はまだ光ファイバが実用化の段階にはなく、物理学の理論的な学問でしかありませんでした。
- 1980年代に入って、量子通信は非常に大きな転換点を迎えます。量子通信が具体的な暗号に利用出来ることが分かったり、光子だけでなく原子や分子を操る技術が実現されたことで、量子計算などあらゆる情報通信に量子を利用するというアイデアがどんどん生まれるようになりました。量子暗号が具体化するきっかけは偶然だったそうです。1982年に当時IBMで量子力学を研究していた物理学者のチャールズ・ベネットとモントリオール大学の暗号学者ジル・ブラサールが休暇で来ていたプエルトリコのプールで偶然出会って、何気ない会話から量子暗号の理論が生まれたそうです。このエピソードにちなみ、1984年の国際会議で彼らが発表した最初の量子暗号プロトコルは、BB84と名付けられています。

出典:https://www.nict.go.jp/publication/NICT-News/1102/01.html



Q1-2 なぜ早急に量子暗号を導入しなければならないのか？

A. 量子コンピュータの出現により現代暗号の危殆化が見込まれます。
理論的安全性が証明されている量子暗号の早期導入により、現在流通するデータの将来的な危険性を下げる必要があります。

現代暗号で暗号化されたデータが、今後量子コンピュータの出現で解読される危険性があります。
また、耐量子-公開鍵暗号もコンピュータ性能の進展により、将来解読される危険性があります。

高

安全性

低(*1)

コンピュータの計算能力への耐性による分類	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 • どんな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(*3)**
保有期間が10年を超える場合、情報理論的安全性が必要になると想定	**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	
計算量的安全 • 今のコンピュータでは暗号を解けない - 解読に今のコンピュータで約3000年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	**2030年(*2)を目安に耐量子暗号への移行が必要となると想定**	• 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) 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
(*2) NIST SP800-57 Part1 Rev4, 5.6.2（https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf）にて「112bit security は2030年まで許容するが、それ以降の適用は禁止」と明言している
(*3) 乱数生成方法等にも依存し，プロトコルの検討が必要

Q1-3 量子コンピュータと量子暗号の違いは何ですか？

A. 両者は同じ「量子」を使っていますが、
量子コンピュータ は量子力学の重ね合わせの性質を計算処理に応用したものです。
量子暗号（量子鍵配送）は量子力学の不確定性の性質を鍵共有に応用したものです。

量子コンピューター

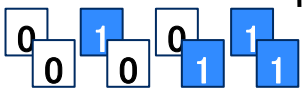
「0」か「1」に加え、「0でも1でもある状態」も表現可能（「0」と「1」の両方を同時に表現可能）

- 量子ビット(Quantum Bit：Qbit)は、量子力学を応用して、「0」と「1」を重ね合わせた状態も同時に表現できる
  →**多種類の情報を処理できる**
- 複数の情報を同時処理(並列処理)できる
  →素因数分解も**短時間で処理できる**

2量子ビットの場合

「00」「01」「10」「11」の**全てを同時に表現**

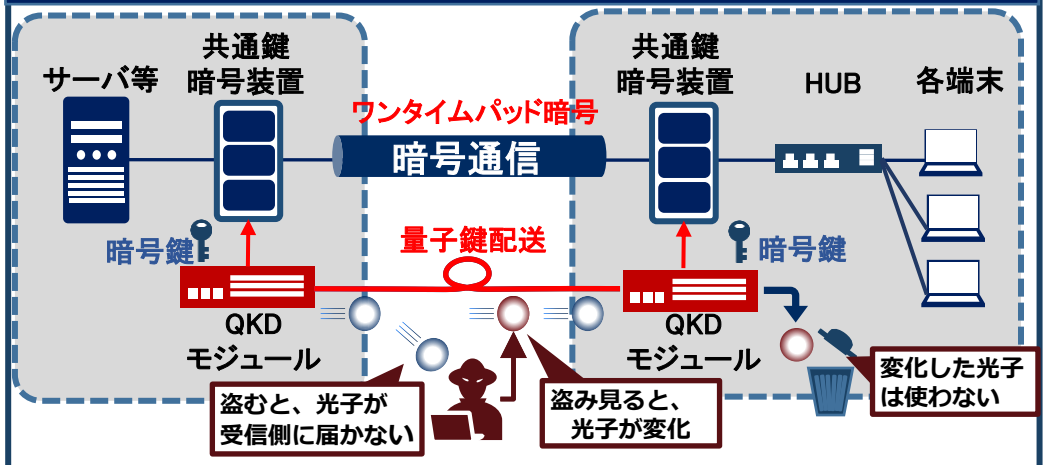
重ね合わせで同時に表現



量子ビットのイメージ

量子の重ね合わせの性質を利用した超並列処理を行う計算機

量子暗号



・**量子暗号**は**量子鍵配送**と**ワンタイムパッド暗号**からなる
・**量子鍵配送**は、光の量子力学的性質（**量子の不確定性**）により“盗み見ると光子の状態が変化“、”光子は盗むと受信側に届かない”といった性質を利用して**暗号鍵の安全性を保障**する
・**情報理論的に安全な**“ワンタイムパッド暗号”を利用することで、無限大の計算能力を持っても解読不能。

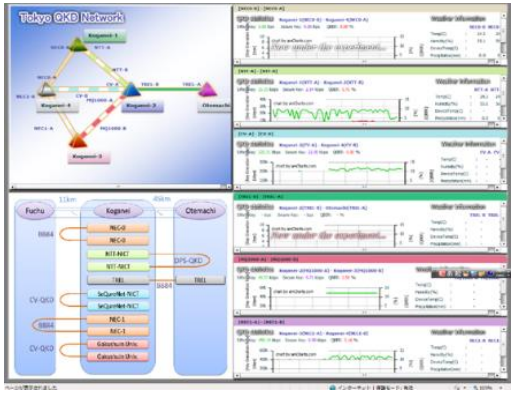
量子の不確定性という性質を利用した情報理論的に安全な暗号

Q1-4 諸外国の量子暗号の研究動向はどうなっていますか？

A. 日本、欧州、中国において 量子鍵配送ネットワークを試験運用中

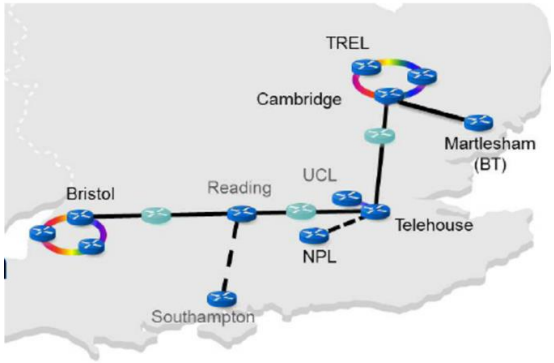
開発機関/企業 ／ 項　目	日本 (NICT/NEC/東芝/学習院大)	欧州(英国) (東芝欧州/BritishTelecom /ADVA)	中国 (中国科学技術大学 /QuantumCtek/QTEC/CAS /Quantumnet)
名称	Tokyo QKD Network (2010-)	Quantum Communication Hub (2018-)	Quantum Backbone (2017-)
ネットワークカバレージ範囲 鍵配送速度	100 km圏/6-8ノード 300 kbps/リンク	200 km圏/１０ノード 300 kbps/リンク	2,000 km圏/32ノード 100 km圏/50ノード 20 kbps
QKDプロトコル	Decoy-BB84、CV、DPS	Decoy-BB84、CV、MDI	Decoy-BB84、CV、E91
特徴	秘匿通信＋安全なデータ保存 ⇒安全性強化の為のデータ 分散バックアップ機能適用	秘匿通信 ⇒ネットワーク仮想化技術の適用	秘匿通信 ⇒世界最大規模の量子鍵配送ネットワーク
想定アプリケーション例	医療、製造、金融、官公庁等	テレコムキャリア等	金融、電力等

日本の動向



出典：http://www.tokyoqkd.jp/web_gui/crypt_gui

英国の動向



出典：https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/EXECUTIVE_TRACK/BT_BEESON_KEYNOTE.pdf

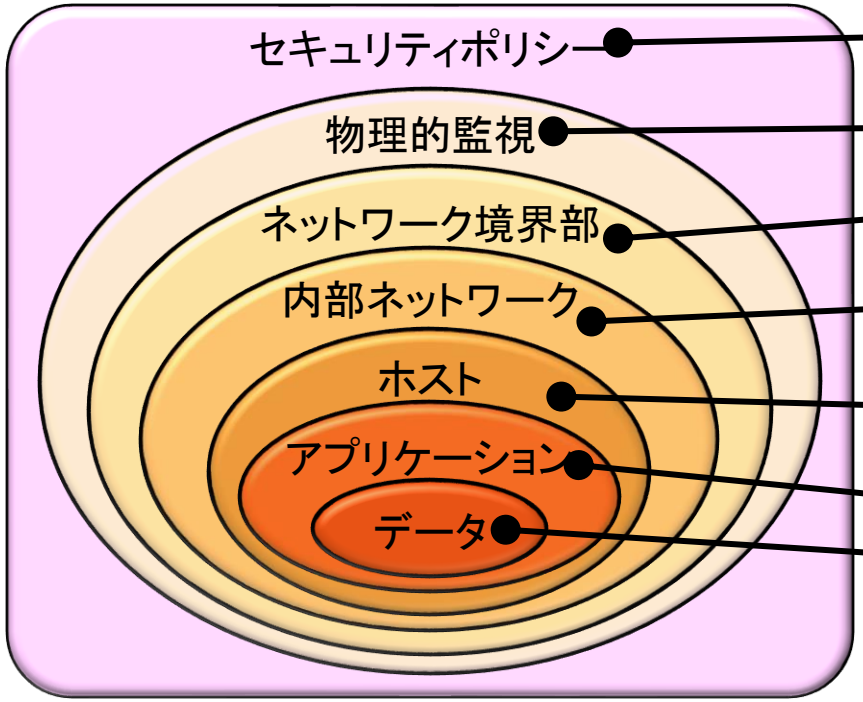
中国の動向

出典：https://docbox.etsi.org/Workshop/2015/201510_IQCWORKSHOP/UofChongqing_HongXiang.pdf

米国/EU/中国/日本などの各国で、国として量子技術（量子コンピュータ，量子暗号）研究開発の戦略を策定し、巨費を投じています。

Q1-6 量子暗号を導入することによって、これまでのサイバー攻撃への対処はどうなるのですか？

A. 量子暗号だけでは十分ではありません。従来のセキュリティ対策に加えて理論的に安全な量子暗号を適用することで、より強固なセキュリティを確保できます。



サイバーセキュリティシステムの防御層

法整備、運用基準、ユーザ教育

モニタ監視、警備員、
人手による管理・運用

ファイアウォール、侵入検知

アクセス管理、マルウェア監視、
トラフィック監視

OS、アプリ、パスワードの更新・管理

マルウェア対策、ユーザ認証

・公開鍵暗号、共通鍵暗号
・**量子暗号**

**量子暗号が強力な
トラストアンカーを務める**

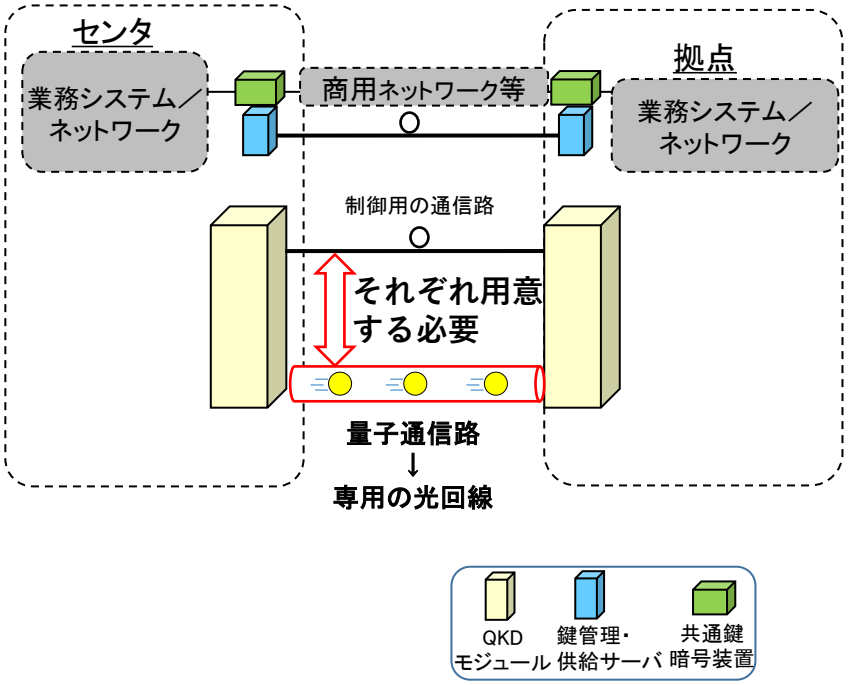
情報通信システムは多種多様なハードウェア、ミドルウェア、ソフトウェアからなっており、多層的なセキュリティ対策が必要とされます(**トラストチェーン**)。量子暗号は、安全に共有された鍵のみを用いて暗号通信を実現することで、暗号解読による情報の漏洩を防ぎます(**トラストアンカー**)。
また、解読不可能な量子暗号をセキュリティ対策に用いることで、攻撃者の攻撃意欲を低減・消失させる効果が期待できます。

Q1-7 量子暗号はこれまでよりネットワーク負荷を与えることにはならないですか？

A. 量子暗号による暗号化によりネットワーク負荷は高まりませんが、量子鍵配送には制御用の帯域と専用の光回線が必要になります。
一方CV-QKDでは他通信と混在が可能となります。

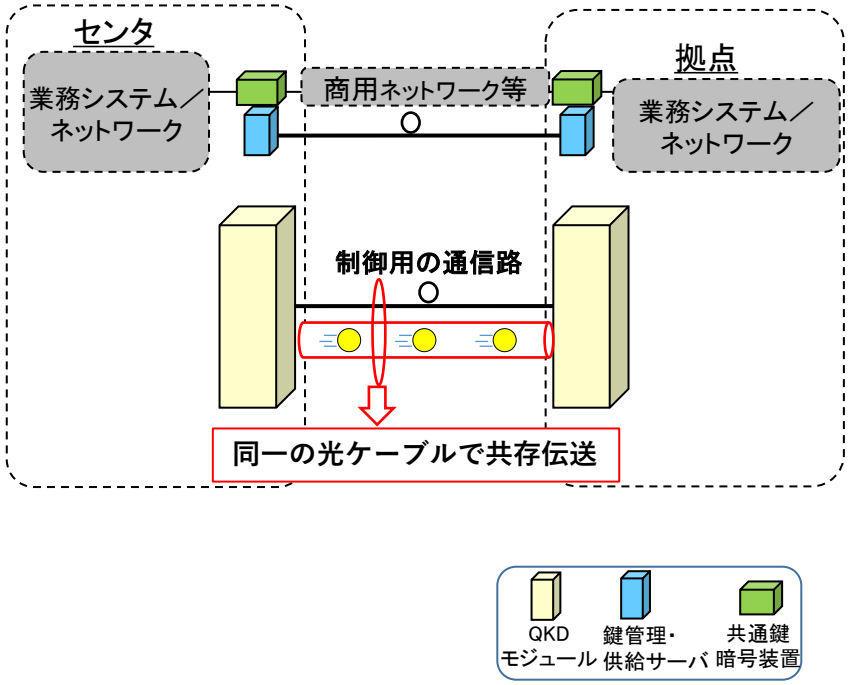
BB84方式

量子通信を他の通信との共存伝送が困難
→制御用の通信路と量子通信路の2本を用意する必要あり



CV-QKD

量子通信と他の通信との共存伝送が可能
→制御用の通信と量子通信を同一の光ケーブルで実装可能



Q1-8 量子暗号導入の必要性・有効性・その他費用対効果は何ですか？

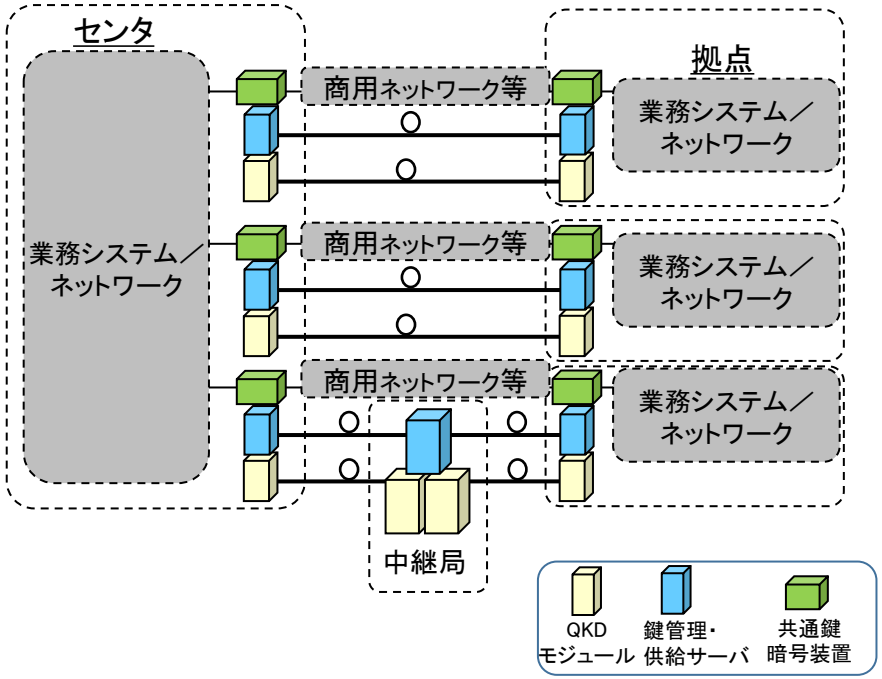
A. 既存の暗号技術の課題を解決し、長期間危殆化せず運用可能な暗号システムを構築できます。また、システム間での互換利用ができることより、基幹システムなどの大規模システムでの導入がしやすく、投資効果を上げやすいと考えます。

必要性

- 計算能力や解読アルゴリズムの進歩とともに暗号の危殆化の脅威
- 鍵共有の盗聴が検知できない危険性
- 高機密用途など暗号仕様が非公開の組織間通信ではシステム間での直接暗号通信が困難
- 鍵情報を運んでいる時に盗難されると、新たな鍵情報の共有の為、一時的に暗号システムが使えなくなる

有効性

- 計算能力や解読アルゴリズムの進歩があっても破られないため、長期的な保護が可能となる
- 量子通信路上の盗聴は検知可能であるため、安全な鍵のみ使うことで安全な通信が可能
- 鍵管理によりネットワークが異なるシステム間で暗号鍵をやり取りし、相互接続を確保できる
- 暗号化は鍵と平文の簡単な計算(排他的論理和)であるため処理遅延(レイテンシー)を解消

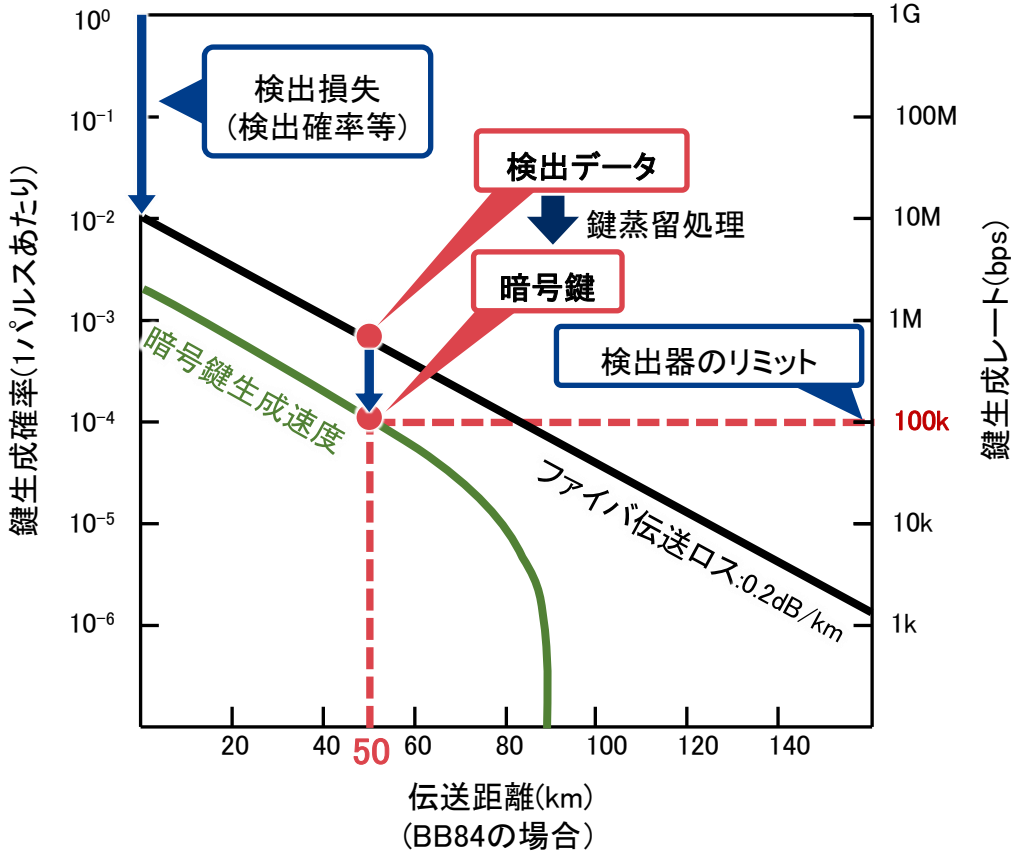


費用対効果

上記構成例の導入費用として数億円程度が見込まれる。対して、危殆化せず、長期に渡り鍵の配付にかかる人的リソースを削減し、盗難リスクを防ぐ

Q1-9 量子暗号を導入する上で考慮すべき事項・制約は何ですか？

A. 直接通信距離の制限があります。（中継局の設定が必要 Q1-10参照）
量子鍵配送の生成速度の制限があります。（暗号鍵のハイブリッド運用）



量子鍵生成速度の制限

- 光ファイバの伝送ロス
  （距離が伸びるほど検出できる光子が減少）
- 鍵蒸留処理での選別
  （安全性の高い暗号鍵を生成するため、
  暗号鍵の生成量は減少する）

直接通信距離の制限

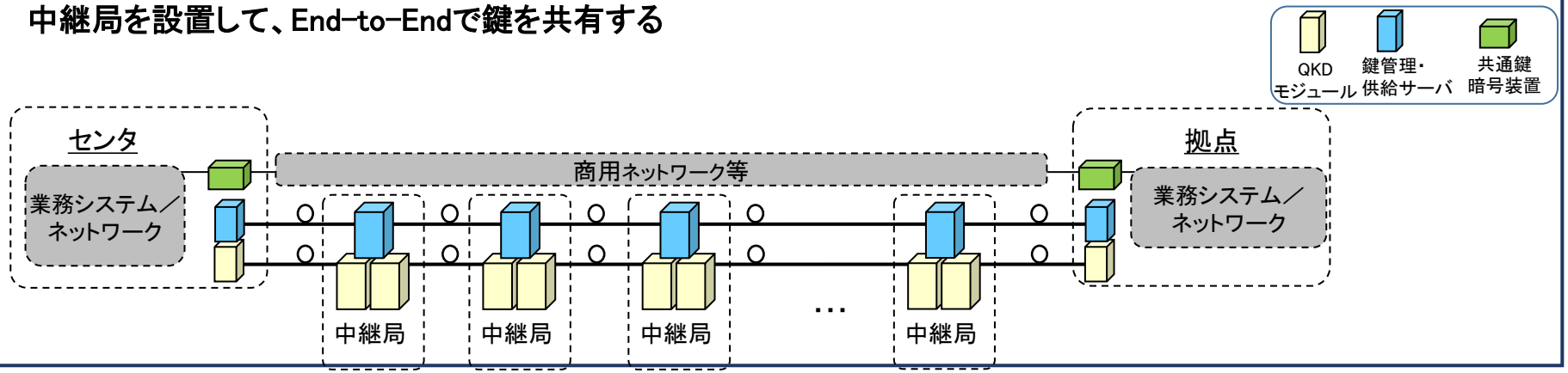
- 光ファイバの伝送ロス
  （距離が伸びるほど伝送できる光子が減少）
- 光子検出性能の限界

Q1-10 考慮すべき事項・制約の解決方法はありますか？

A. 長距離伝送の場合：中継局を設置して、End-to-Endで鍵を共有
大容量通信の場合：①重要なセッション用に暗号鍵を蓄積して利用
②量子鍵配送と既存の共通鍵暗号(AES等)を組み合わせて利用

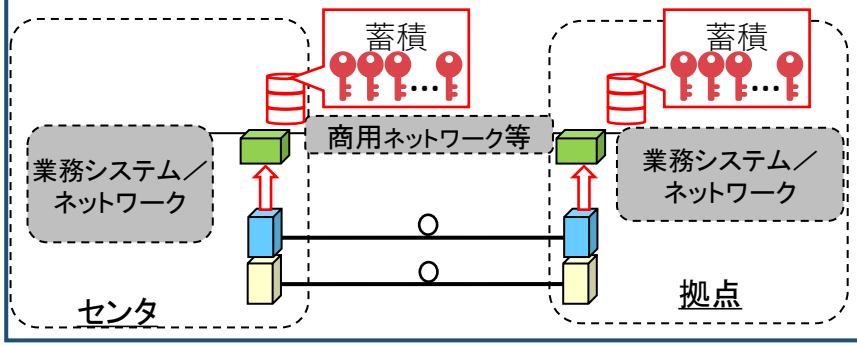
長距離伝送

中継局を設置して、End-to-Endで鍵を共有する

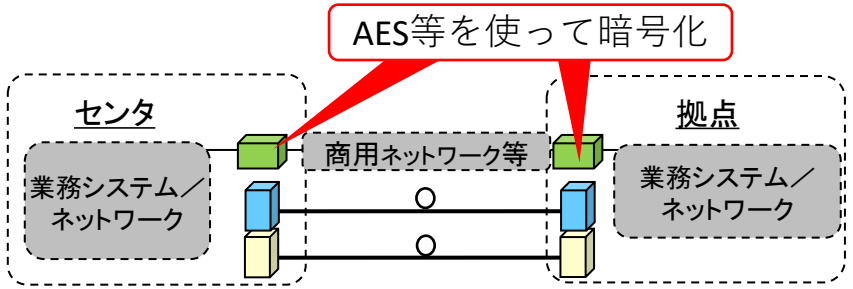


大容量通信

解決方法1：重要なセッション用に暗号鍵を蓄積



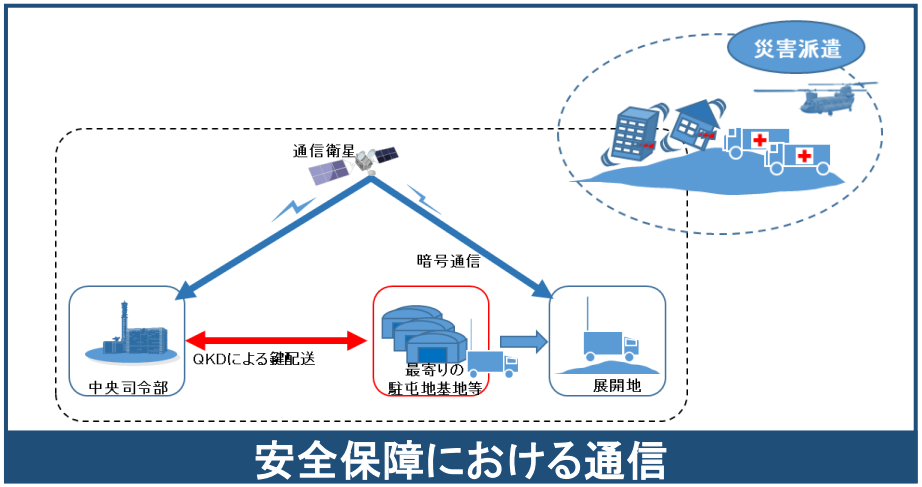
解決方法2：QKDと既存の共通鍵暗号(AES等)を組み合わせて利用



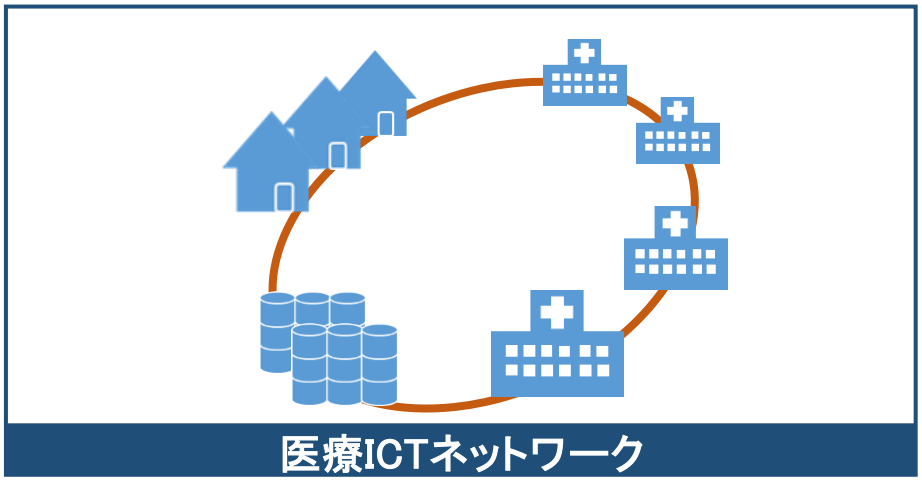
Q1-11 量子暗号はどんな分野に適用されるべきですか？

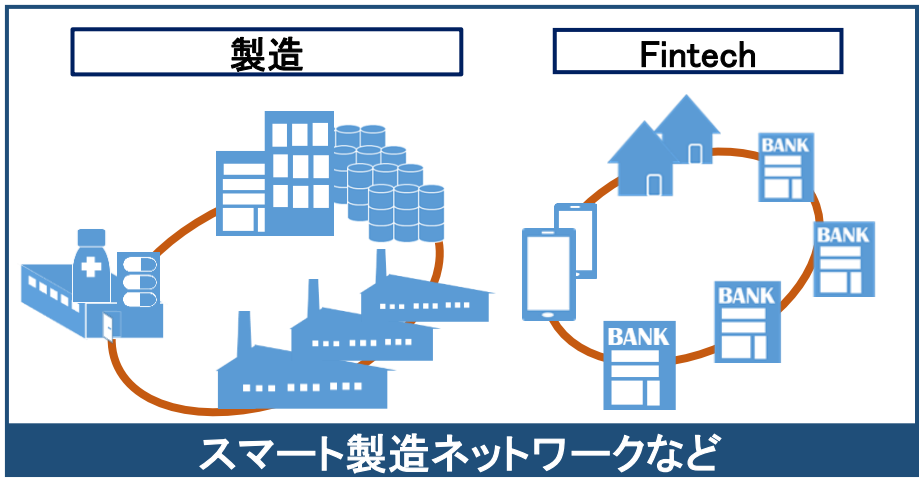
A. ●将来に渡って秘密保持が必要な安全保障などの分野
●遺伝子ゲノムなどの個人の秘密情報を扱い強固なプライバシー保護が必要な医療ICTなどの分野
●企業活動の維持に必要なスマート製造などの分野

量子暗号の利用例



安全保障における通信

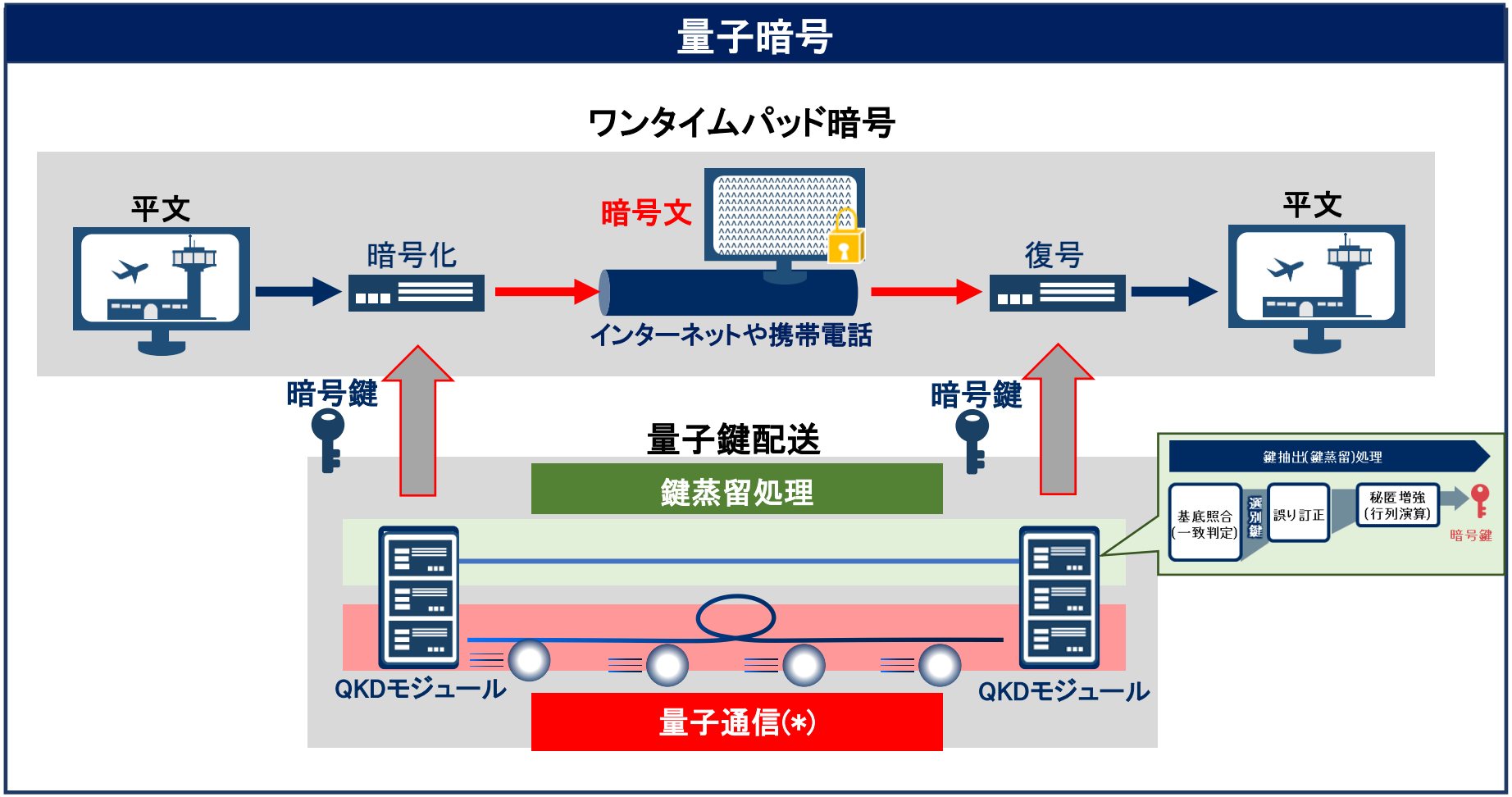

医療ICTネットワーク



スマート製造ネットワークなど

Q1-12 量子暗号と量子鍵配送、量子通信はどういう関係ですか？

A. **量子暗号**は**量子鍵配送**で共有した鍵を**ワンタイムパッド暗号**で利用する方式を指し、**量子鍵配送**は量子通信を用いて光子一個の偏光などの量子状態に情報を載せて伝送し鍵情報を共有しています。

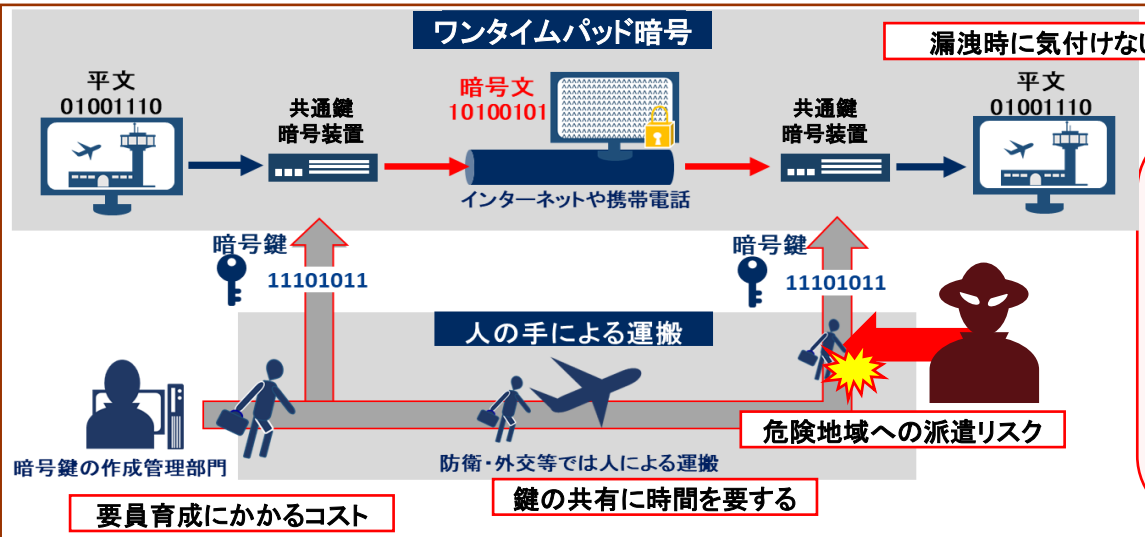


＊Q1-12：量子通信「その2」の方式

Q1-13 既存の暗号運用(人手による配送)と量子暗号(量子鍵配送)の違いは何か？

A. 量子暗号を導入することで、安全性を保ったまま利便性を確保可能となります。

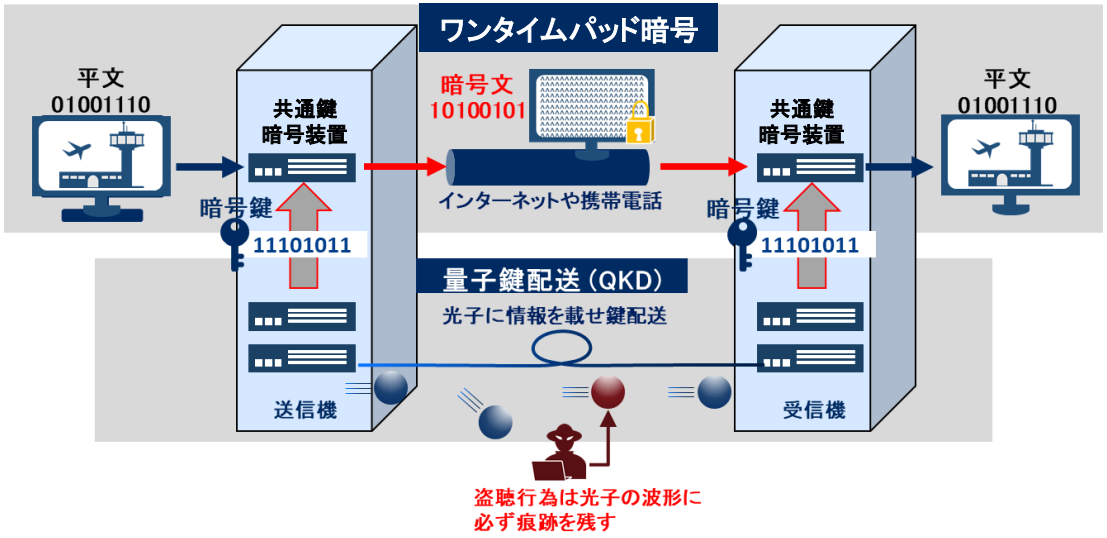
既存暗号①人手による配送



鍵の共有に人が介在

- 要員育成にかかるコスト
- 危険地域への派遣リスク
- 漏洩時に気付けない
- 鍵の共有に時間を要する

量子鍵配送



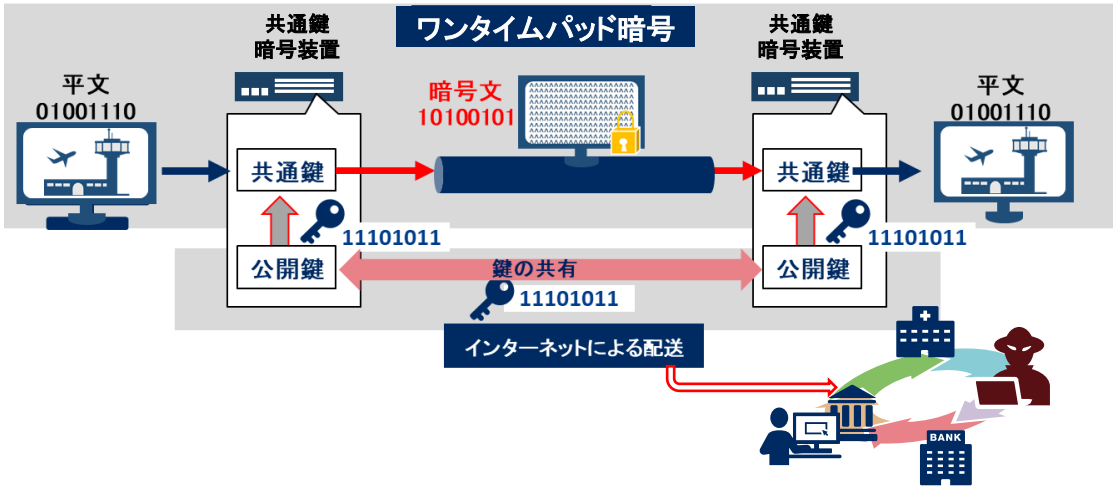
人手を介さない共有

- システム置き換えによる省人化
- 要員の生命リスク減
- 鍵の盗聴を検知可能
- リアルタイムな共有が可能

Q1-14 既存の暗号運用（公開鍵暗号）と量子暗号(量子鍵配送)の違いは何か？

A. 量子暗号を導入することで、利便性を保ったまま安全性を確保可能となります。

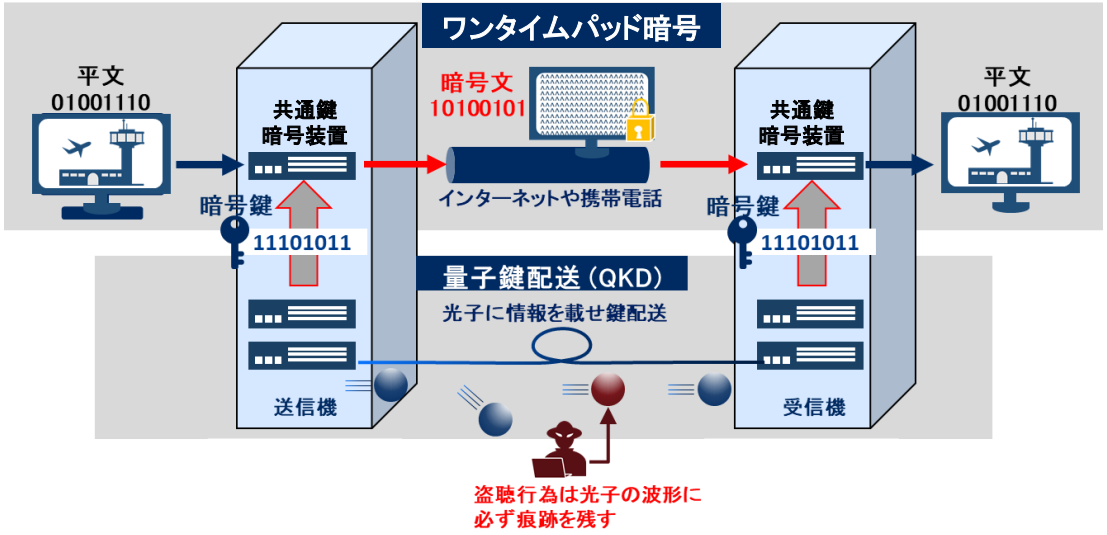
既存暗号②公開鍵暗号



計算量的安全性に依存

- システム更新によるコスト
- 漏洩時に気付けない
- インターネット上に流出した情報は永遠に残ってしまう

量子鍵配送



情報理論的安全性

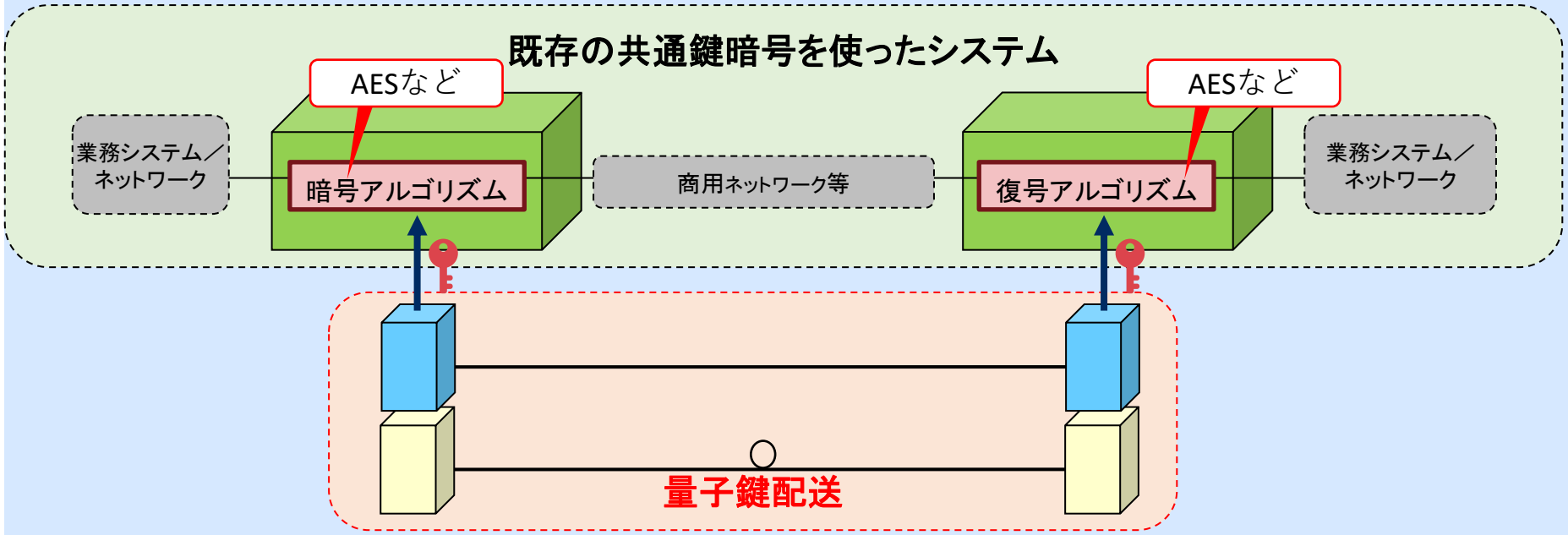
- 危殆化による更新不要
- 鍵の盗聴を検知可能
- 将来的にも解読不可能

Q1-15 量子鍵配送は、既存の暗号との共存はできるのですか？

A. 量子鍵配送を共通鍵暗号の鍵共有に活用することで共存は可能です。
暗号化にAES等の既存の共通鍵暗号方式を使うことで、鍵生成速度以上の大容量暗号通信が可能となります。

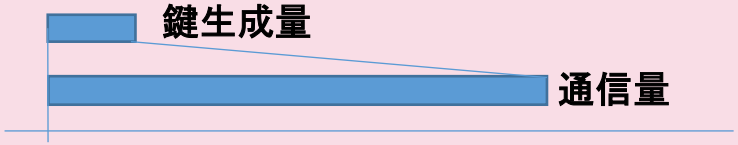
システムイメージ

QKDと既存の共通鍵暗号(AES等)を組み合わせて利用



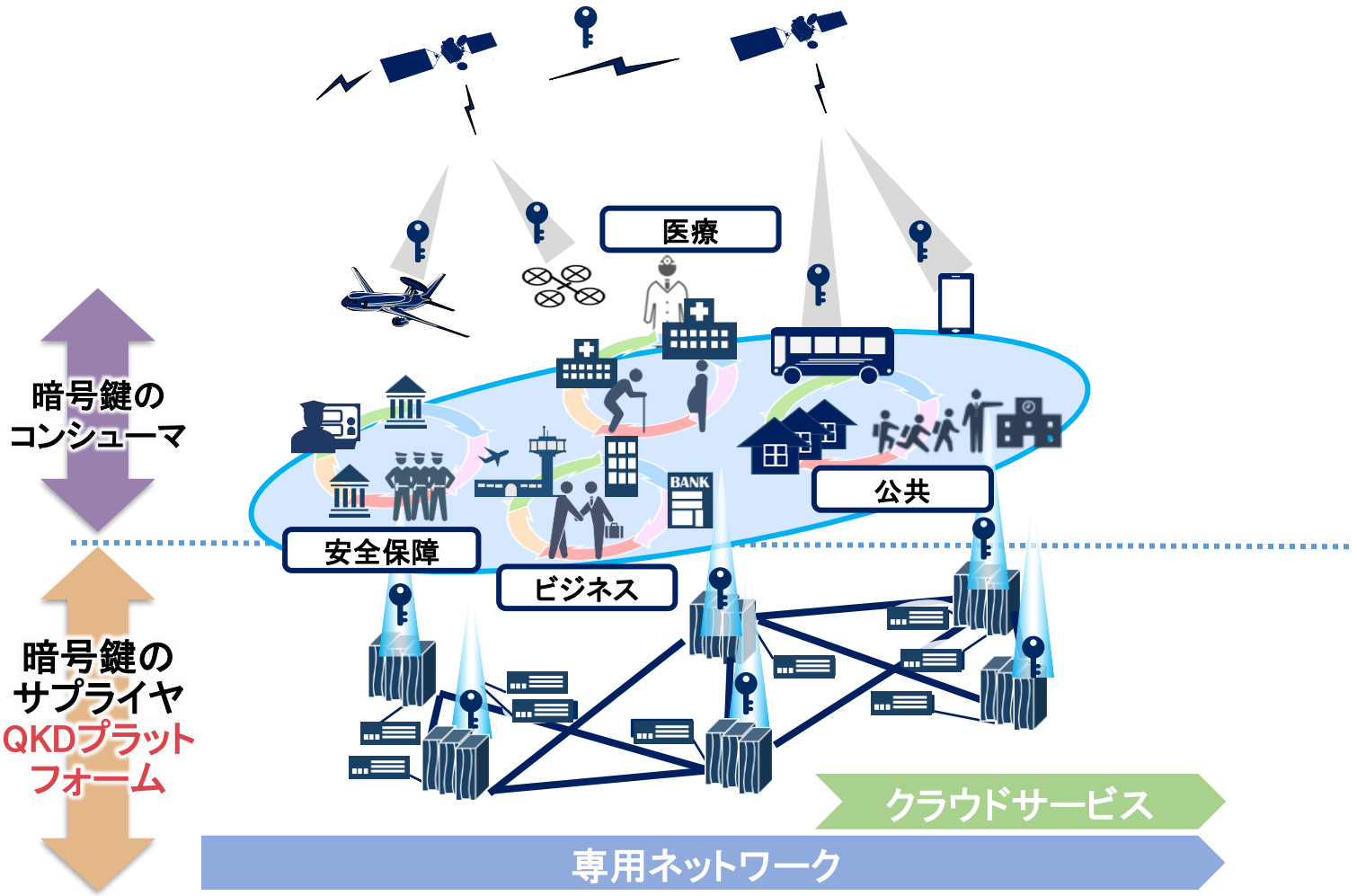
暗号鍵の更新頻度を可変すれば、安全性は更に高まる

大容量の暗号通信が可能



Q1-16 量子暗号はどんな人が利用できるのですか？

A. ICT社会に向けて 家庭のインターネットを含むあらゆる通信に対して利用できるようにすべきと考えています。
まずは安全保障や外交、医療など非常に高いセキュリティレベルを必要とされる分野を中心に 導入・普及を進めます。

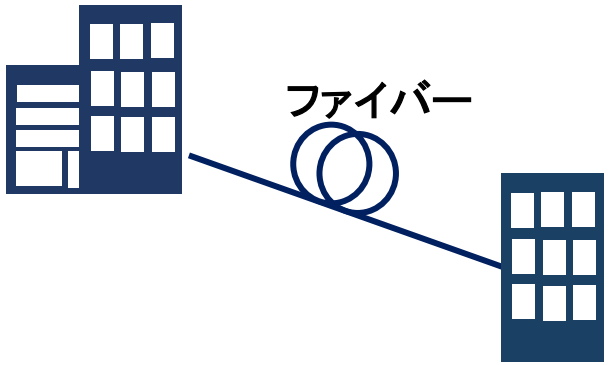


Q1-17 有線量子暗号と衛星量子暗号（無線量子暗号）は何が違うのですか？

A. 有線量子暗号では既存の光ファイバー通信技術を応用することにより、高速な量子暗号通信が可能です。一方、衛星量子暗号通信では人工衛星を経由することで、より長距離での量子暗号通信が可能となります。

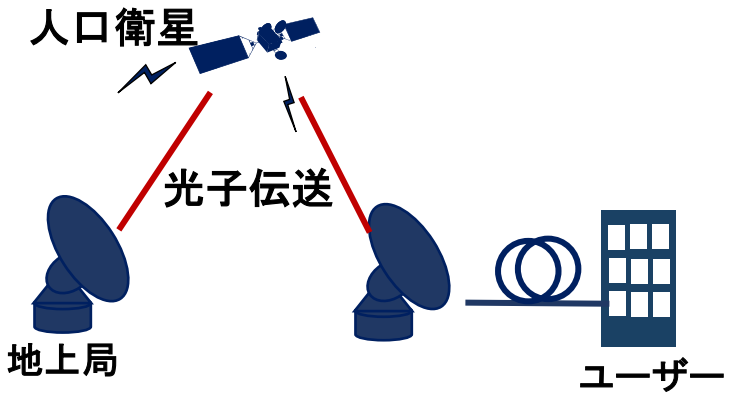
有線量子暗号

- **ファイバー伝送**が中心
- ファイバー中のロス、検出器のノイズにより伝送距離に限界 （～数百km）



無線量子暗号

- 空間伝送
- 人工衛星の利用
  - 同時見通し → ＞1000km
  - 衛星移動（古典中継） → 距離制限なし



将来的にファイバー伝送と空間伝送の融合で、ビル間・山頂など、グローバルでフレキシブルなQKDネットワークを構築します。

2.技術

Q2-1 量子鍵配送の仕組みや動作原理を簡単に教えてください。

A. 量子鍵配送は、量子通信（単一光子伝送）と鍵蒸留処理からなります。

量子通信

量子通信路を介した
光パルスの送受信操作

乱数列のビット情報0,1に基づき、適切な量子信号を次々と生成して量子通信路で送り、適切な測定法を用いてこれらを検出し、暗号鍵の元となるデータ**生鍵**を送受信者間で蓄積して行く。

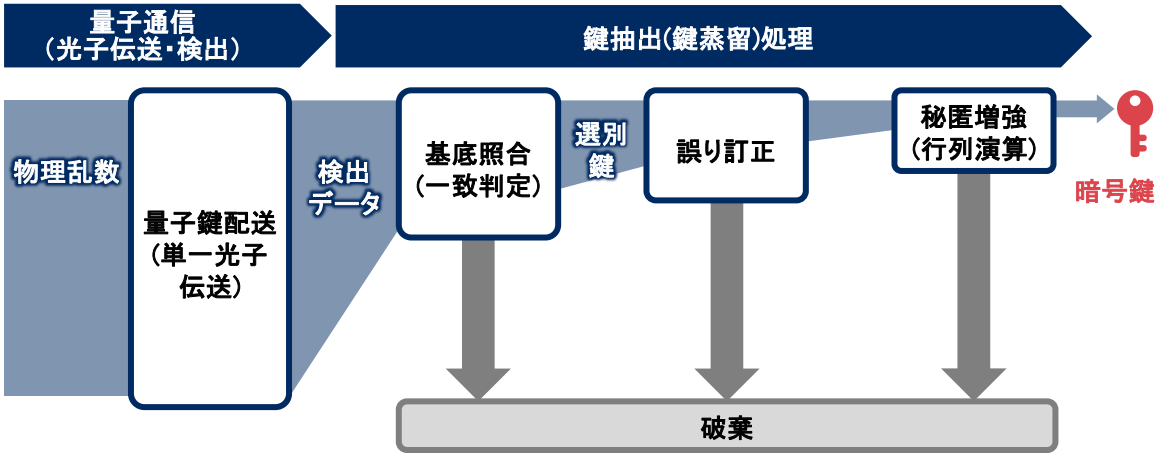
光の検出方式によりプロトコルが異なり、プロトコルは主に2つの方式があります。
- **BB84プロトコル**
- **CV-QKDプロトコル**

鍵蒸留処理

パラメータを推定し 生鍵から安全な暗号鍵を抽出する処理

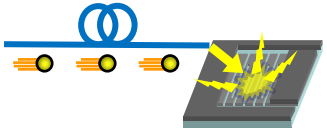
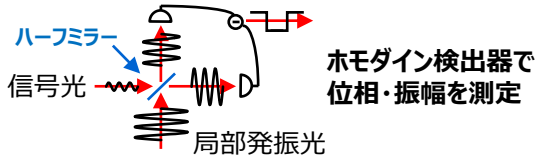
1) 基底照合
送受信者の基底が一致するスロットのみを選択する。この選別によって残るビット列のことをふるい鍵という。

2) 誤り訂正と秘匿性増強
ふるい鍵のビット誤りを誤り訂正し、さらに安全な暗号鍵を抽出し共有する。



Q2-2 BB84とCV-QKDは何が違うのか？それぞれの特徴は何か？

A. 光の検出方法が異なります。
そのため、以下の様な特徴の違いがあります。

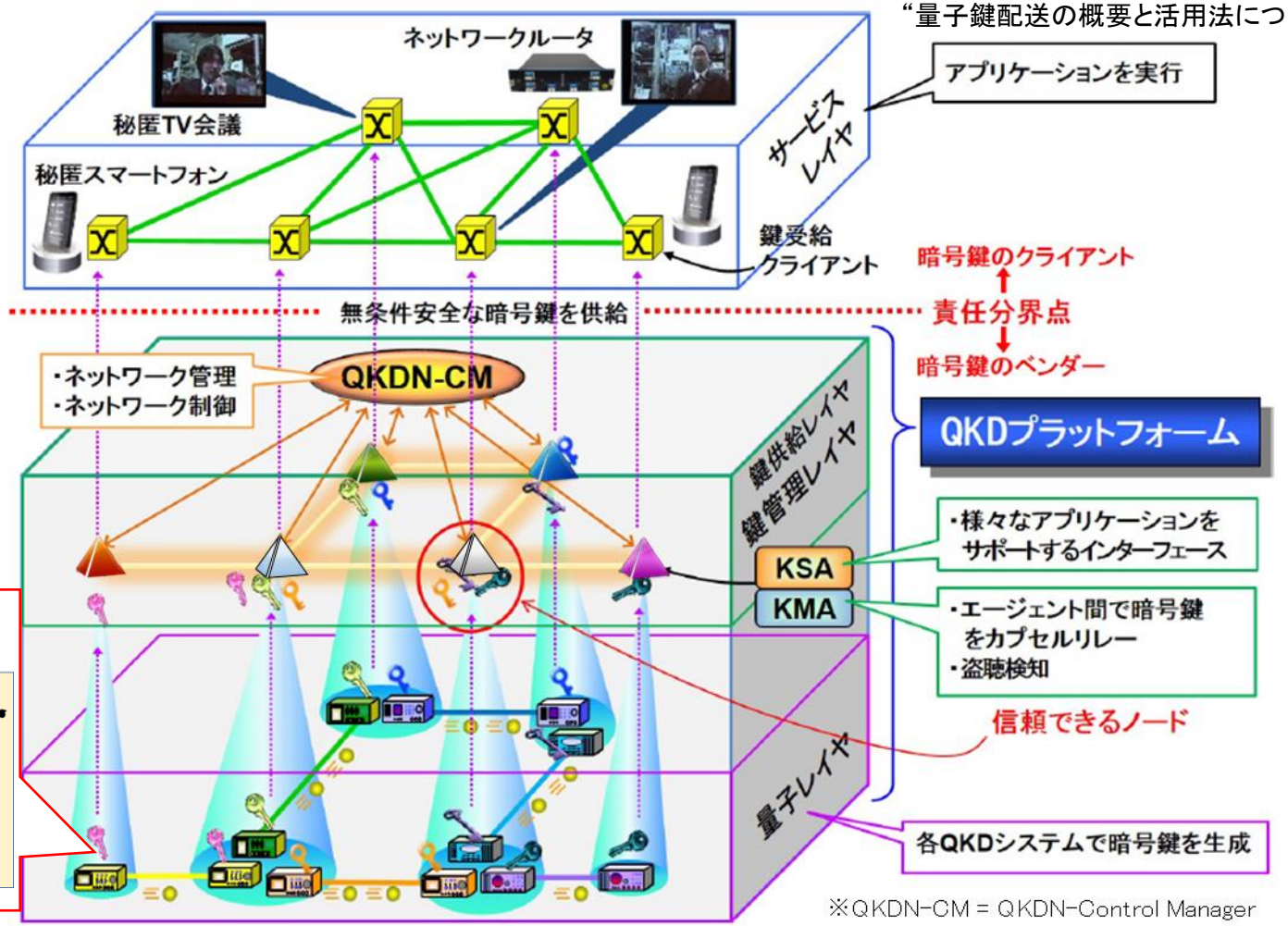
項目	BB84	CV-QKD
概要	鍵情報は光子の偏光や位相（離散量）にエンコードする	鍵情報は光の振幅や位相（連続量）にエンコードする
光検出	単一光子検出器を利用  	◎標準的なバランス型光検出器を利用 
鍵生成レート	◎13.72 Mbps @ 10 km ◎10 bps @ 240 km	1 Mbps @ 25 km 0.5 kbps @ 100 km
ファイバー内のデータ通信との共存可否	追加のフィルターが必要 データ通信の増幅不可 実験例:2波多重した計200Gbpsのデータと共存伝送	◎追加部品不要 ◎データ通信の増幅可能 実験例:100波多重・光増幅した計18.3Tbpsのデータと共存伝送
技術の成熟度	◎実装・評価実績多数	新技術のため実装評価が必要
安全性の証明	◎無条件安全性が証明済み	変調法に応じ，攻撃モデルに制限
用途	安全保障分野などのハイエンド向け	民生用途向け
装置サイズ	19インチラックマウント	
参考価格（1対向）	検出器・干渉計のため高額	◎汎用品で製造可能なため比較的低価格
メーカー	NEC, 東芝, IDQ, QuantumCTek	NEC, Huawei Research

安全性や性能、コストなどの差があり、適用するシステムに合わせて組み合わせることで最適な環境を構築できます。

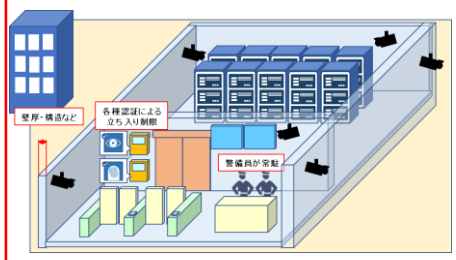
Q2-3 量子暗号のQKDアーキテクチャとはどういうものですか？

A. QKDプラットフォームは量子レイヤ、鍵管理レイヤ、鍵供給レイヤの3つのレイヤから構築されます。サービスレイヤはQKDプラットフォームから安全な暗号鍵を供給され、アプリケーションを実行します。

出典：一般社団法人量子ICTフォーラム
“量子鍵配送の概要と活用法について”

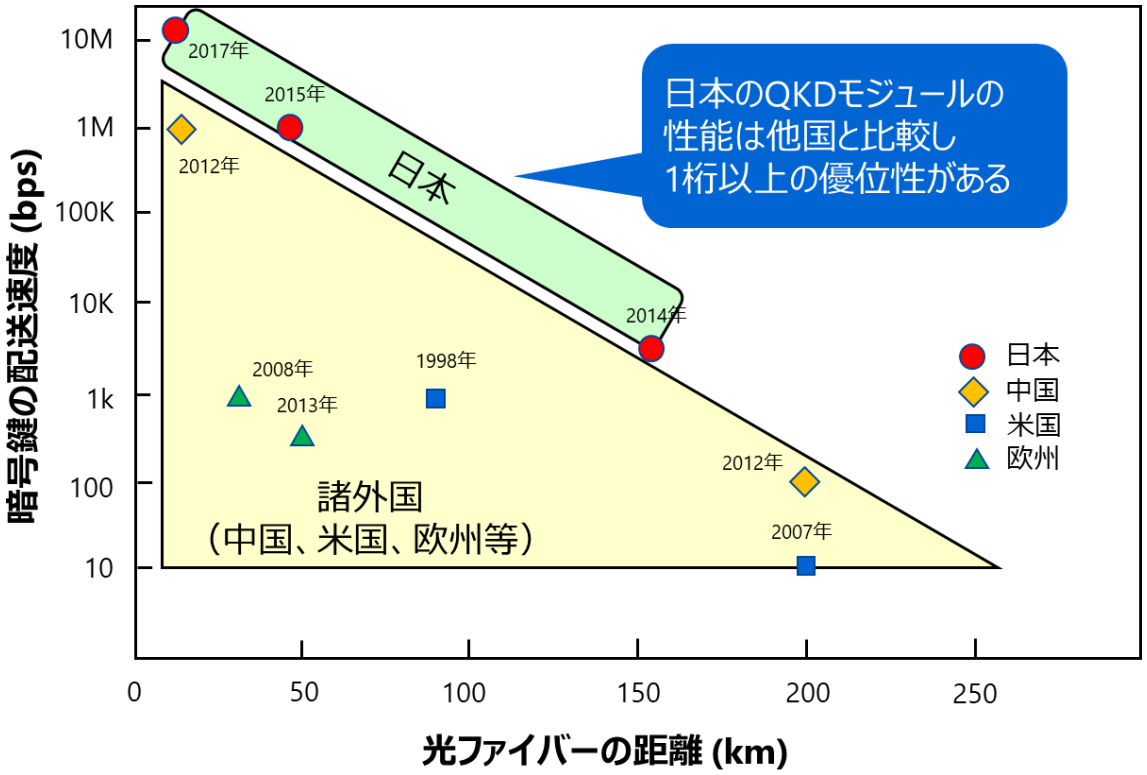


トラステッドノードのイメージ



Q2-4 量子鍵配送の伝送距離と鍵生成能力はどれくらいですか？

A. 伝送距離 50km　数100kbps（商用ファイバーでの実証結果）



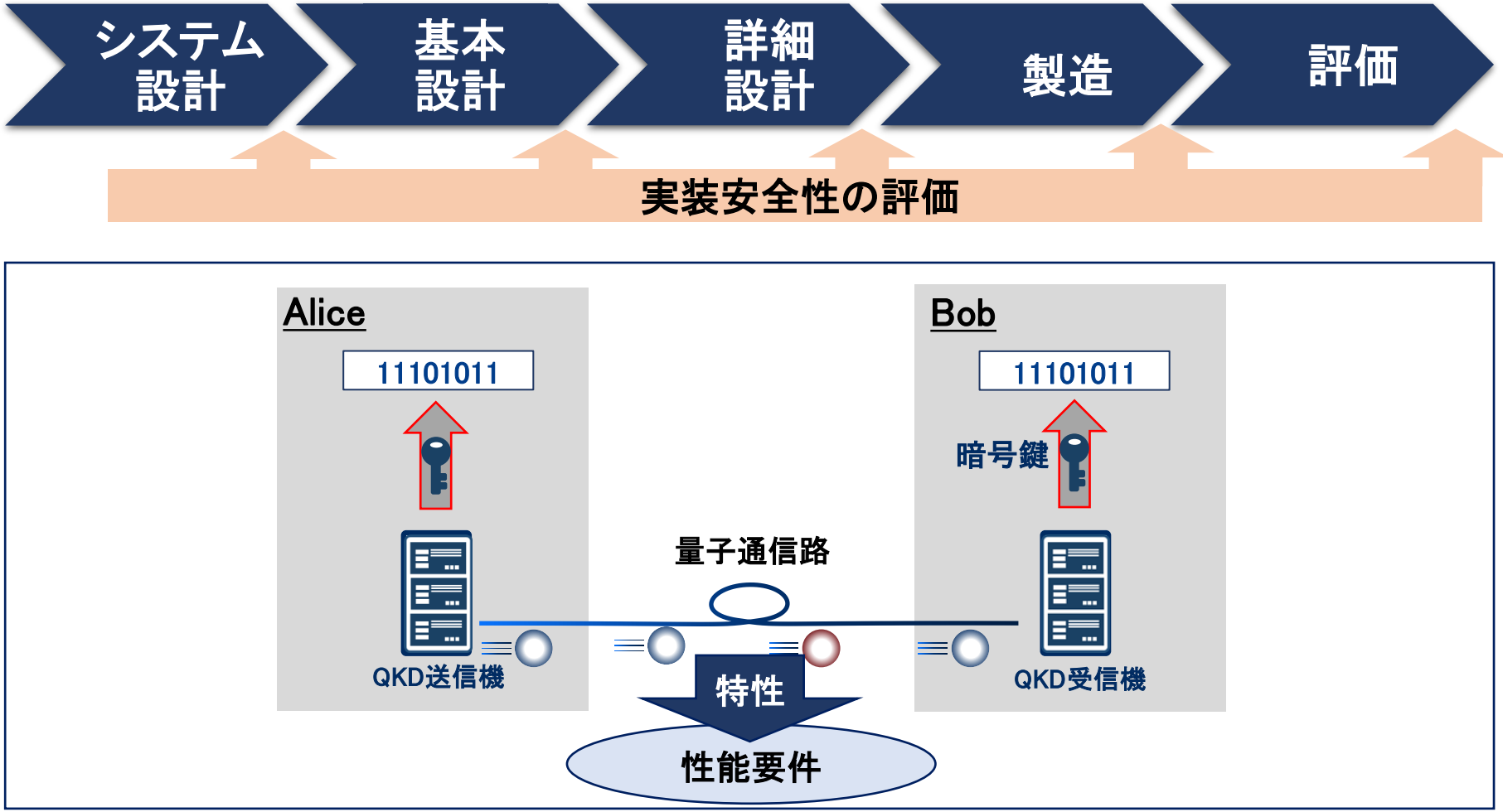
試験実績
現時点での性能(1波長あたり)

- 距離
  50kmの場合、鍵生成 100-300kbps

【距離制限の要因】
- **光ファイバの伝送ロス(距離が伸びるほど伝送できる光子が減少)**
- **光子検出性能の限界**

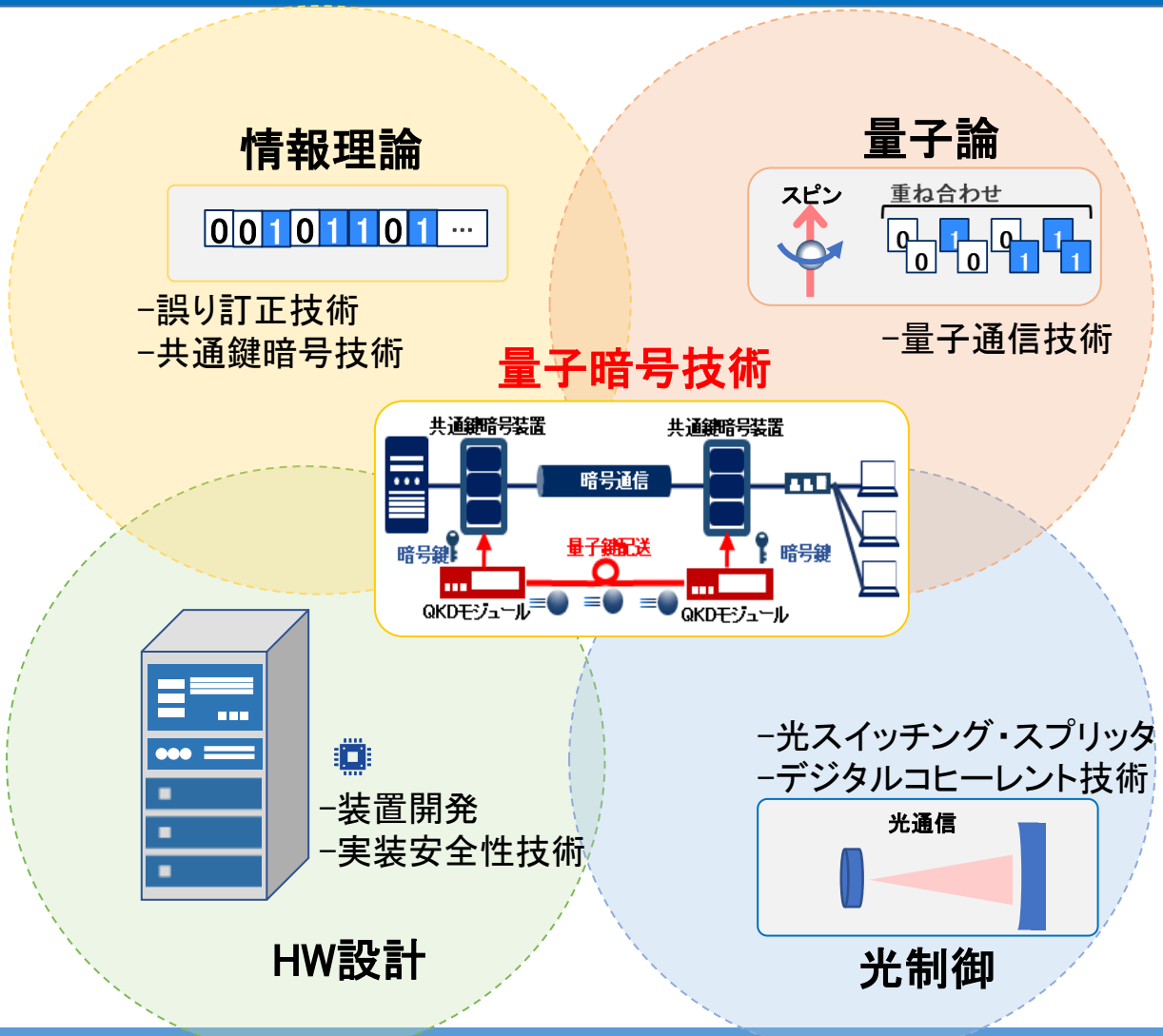
Q2-5 QKDシステム構築のための設計手法を教えてください

A. 通常のセキュリティシステムと変わりませんが、特有の性能要件として装置や回線などの特性を踏まえる必要があります。



Q2-6 量子暗号技術を支える技術要素は何ですか？

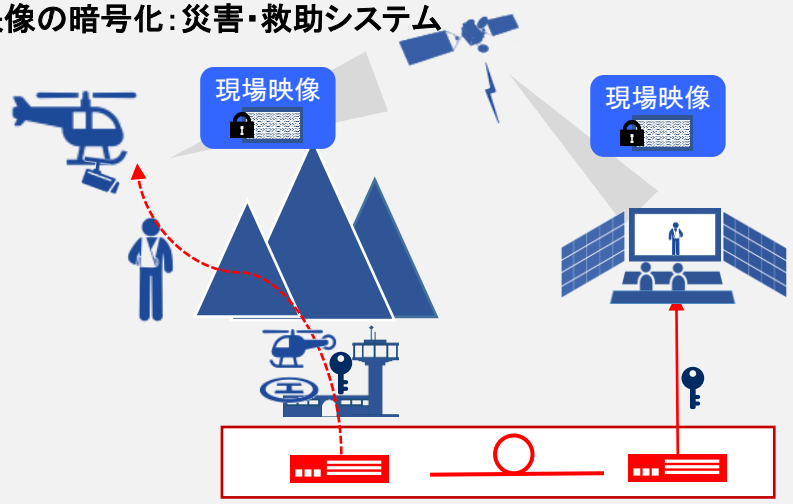
A. 光子検出技術、光子送信技術、鍵蒸留技術、情報理論、暗号理論があります。
アプリケーションとして実現するには、加えてネットワーク技術、セキュリティ技術も必要になります。



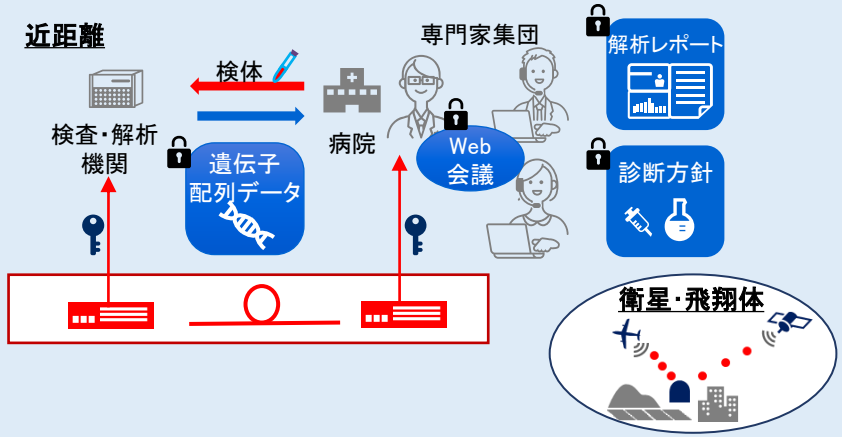
Q2-7 QKDのエンドユーザのアプリケーションにはどのようなものが考えられますか？

A. 移動体、スマホ、タブレットなどの端末や回線暗号、サーバで暗号化、秘密分散データベースなどの様々なシステムと連携したアプリケーションが考えられます。

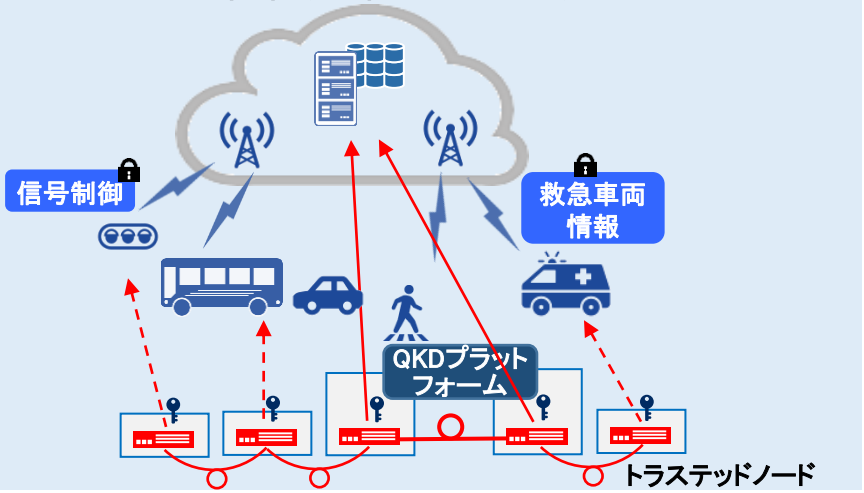
映像の暗号化：災害・救助システム



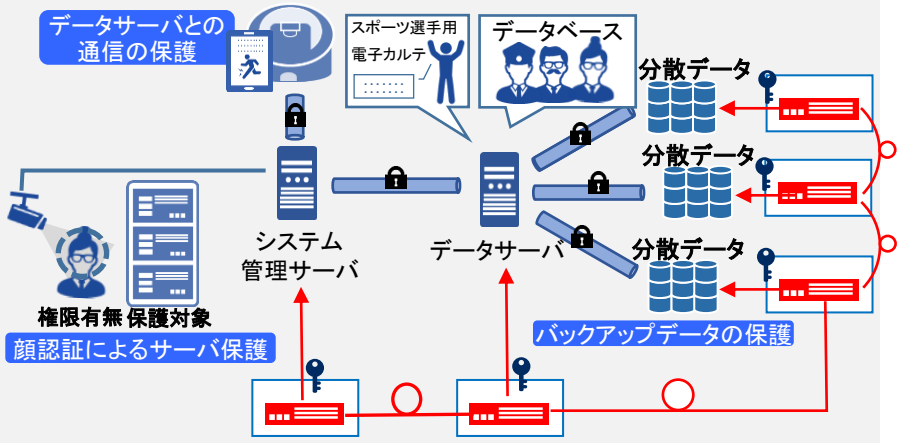
ゲノム情報の暗号化：クリニカルシーケンス



車両位置・信号制御情報の暗号化：都市交通システム



顔情報の暗号化、暗号化分散データベース：スポーツ選手用電子カルテ管理



Q2-8 量子暗号に対する脅威は何ですか？

A. 脅威の種類は、意図的な脅威／管理上の脅威／偶発的な脅威の3つに分けることができます。以下に想定される脅威と対策例を示します。

分類		脅威の種類	対策例
情報漏洩	意図的な脅威	通信路の盗聴	通信路暗号化、専用線
	管理上の脅威	装置からの情報漏洩	入退室管理。施錠管理
	管理上の脅威	装置の盗難・廃棄時の盗難	耐タンパ、難読化、セキュア消去
	意図的な脅威	サイドチャネル攻撃	脆弱性対策
	意図的な脅威	バックドア攻撃	組込みデバイスの精査、耐タンパ
なりすまし	意図的な脅威	なりすまし	認証
不正アクセス	意図的な脅威	物理侵入	入退室管理、施錠管理
	意図的な脅威	装置・サーバへの不正アクセス	脆弱性対策、認証
	意図的な脅威	不正操作	操作者認証
	管理上の脅威	不正媒体の接続	デバイス接続制限
	意図的な脅威	マルウェア感染	アンチウィルス
	意図的な脅威	アプリからの不正アクセス	アクセス制御、認証
情報改竄・消去	意図的な脅威	鍵情報、鍵管理情報の改ざん・消去	アクセス制御、権限管理、データ暗号化
否認	意図的な脅威	否認	デジタル署名
	意図的な脅威	偽造	データ署名
DoS攻撃	意図的な脅威	サーバへの高負荷攻撃	冗長化
	意図的な脅威	通信路遮断	冗長化
	管理上の脅威	通信輻輳・通信妨害(無線の場合)	冗長化
災害	偶発的な脅威	通信路障害	冗長化
	偶発的な脅威	インフラ障害	無停電電源装置
人的エラー	管理上の脅威	過失操作	フィルタリング、確認画面
管理上の脅威	偶発的な脅威	不具合・故障・バグ	定期メンテナンス

参考:制御システムのセキュリティリスク分析ガイド 第2版 https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

Q2-9 現在の量子暗号装置はどれくらいの大きさですか？

A. QKDモジュールは2-3Uサイズになる予定です。
QKDプラットフォームを構築するには送信側、受信側に各ラック1本を想定しています。

【QKDプラットフォーム】 ※東芝製品の場合

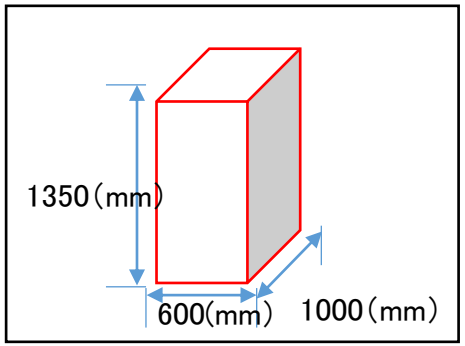
暗号化装置（製品化検討中） → 2U

鍵供給サーバ（汎用サーバ） → 1U

鍵管理サーバ（汎用サーバ） → 1U

【QKDモジュール】（製品化予定） → 2-3U

参考：25Uラックのサイズ



Q2-10 量子鍵配送のシーケンス・プロトコル・データフォーマットを教えてください。

A. 量子鍵配送のシーケンス及びデータの種類は、以下の通りです。①の量子状態の送受信方法（プロトコル）によって、その後のプロセスにも違いが現れます。

3.ドキュメント

Q3-1　量子暗号を学ぶために何から始めたらよいですか？

A.　まず「がんばって理解しようとする気持ちを持つこと」が大切です。
入門書として適する本を下記にご紹介します。

□「量子情報通信」基礎から最前線まで　　【参考書】
著者: 佐々木雅英、他35名
発行：オプトロニクス社（2006年）

□量子暗号　　【読み物】
著者：石井茂
発行：日経BP社（2007年）

□量子元年、進化する通信　　【読み物】
著者：佐々木雅英、根本香絵、池谷瑠絵
発行：丸善ライブラリー 新書（2014年）

□量子暗号と東京QKDネットワークの紹介【Webページ】
<http://www.nict.go.jp/quantum/>（一番下辺）

Q3-2 標準化団体はどのようなものがありますか？

A. 国際標準化機構（ISO）／国際電気標準会議(IEC) 、国際電気通信連合-電気通信標準化部門（ITU-T） などがあります。