メディア向け勉強会　2019年4月18日@丸の内オアゾ

～「量子コンピュータ」「量子通信」の次に来る、「量子中継ネットワーク」～

小坂英男

kosaka-hideo-yp@ynu.ac.jp
http://kosaka-lab.ynu.ac.jp

横浜国立大学・先端科学高等研究院

CREST　科研費 KAKENHI　京 K computer　SUMITOMO ELECTRIC Connect with Innovation　SII　AIST NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY (AIST)　NIMS　QST

小坂英男の経歴（量子情報関連のみ抜粋）

- 米UCLAにて　DARPAの量子情報Pj（Spins）参画
  半導体量子ドットを用いた「量子中継素子」の研究
- NECにて　総務省「量子暗号」委託研究に参画
  世界初の100km超量子暗号の実証
- 東北大にて
  CRESTチーム代表 「量子メディア変換」実証
  NICT委託研究チーム代表 「量子もつれ中継」
- 横浜国大において
  科研費基盤S代表 「ダイヤモンド量子メディア変換」
  CRESTチーム代表 「ダイヤモンド量子セキュリティ」
- その他、FIRST、ポスト「京」プロジェクトなどに参画

Newton
GRAPHIC SCIENCE MAGAZINE ニュートン
2018年6月号

協力
小坂英男
横浜国立大学大学院工学研究院教授

量子もつれの光子を宇宙から配送

人工衛星

量子衛星

量子もつれになった
光子のペア（EPRペア）

量子もつれ

量子もつれ

受信者

中継地点5

量子中継器

中継地点4

量子もつれになった
光子のペア（EPRペア）

中継地点1

中継地点2

中継地点3

量子もつれの光子を地上で中継

量子もつれ

送信者

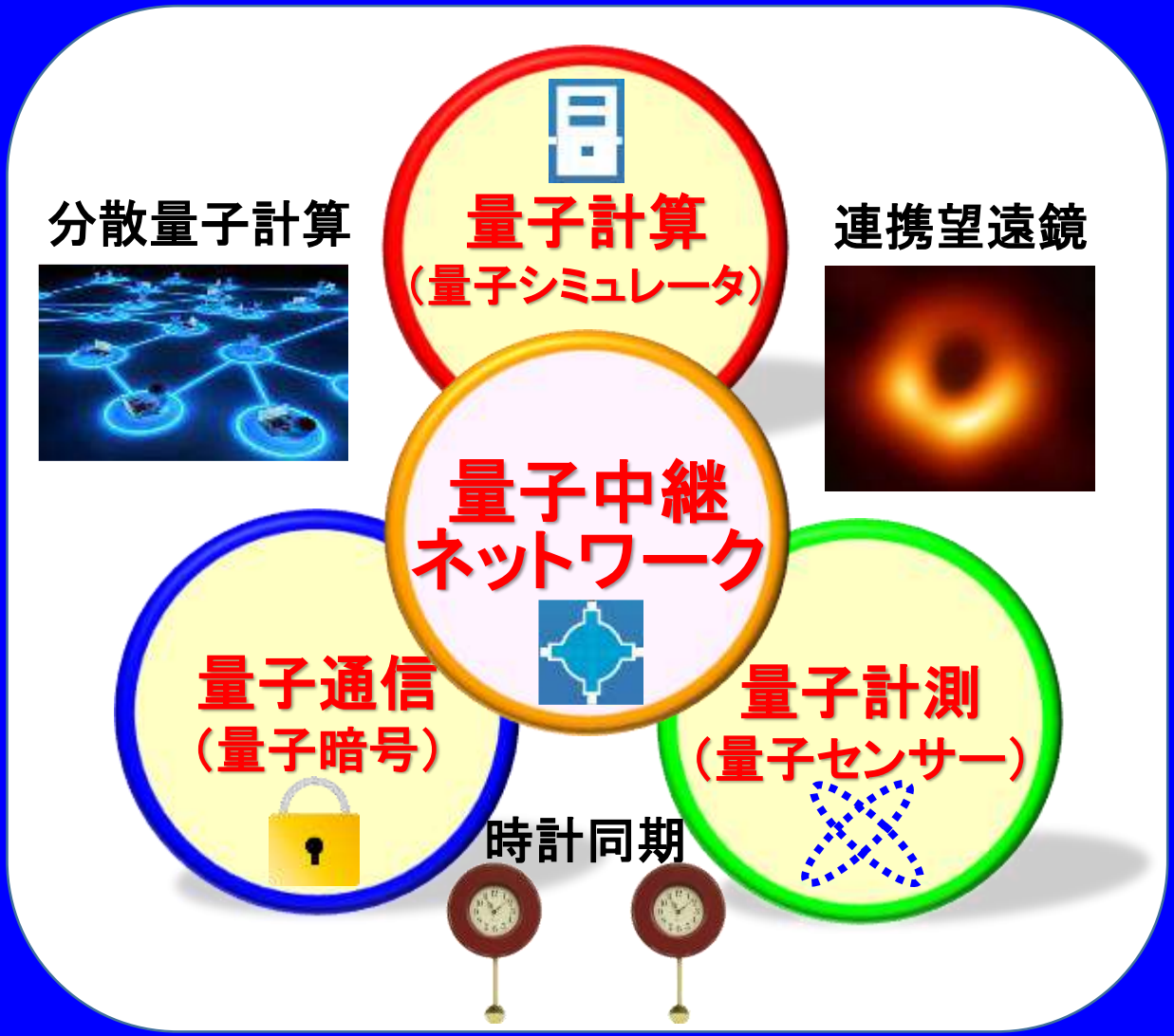
光子をもつれさせて、
中継地点間の短い量子
もつれをつなげる

量子中継ネットワークのイメージ

67

量子中継ネットワークは何に役立つの？

量子計算、量子通信、量子計測を接続する究極の技術！



本講演の内容

1．量子中継ネットワーク研究の世界動向

2．そもそも量子中継とは？

3．量子中継ネットワーク研究最前線

4．我々の取り組み

5．量子中継関連プロジェクトの最新情報

量子コンピュータ 9000兆倍の破壊力

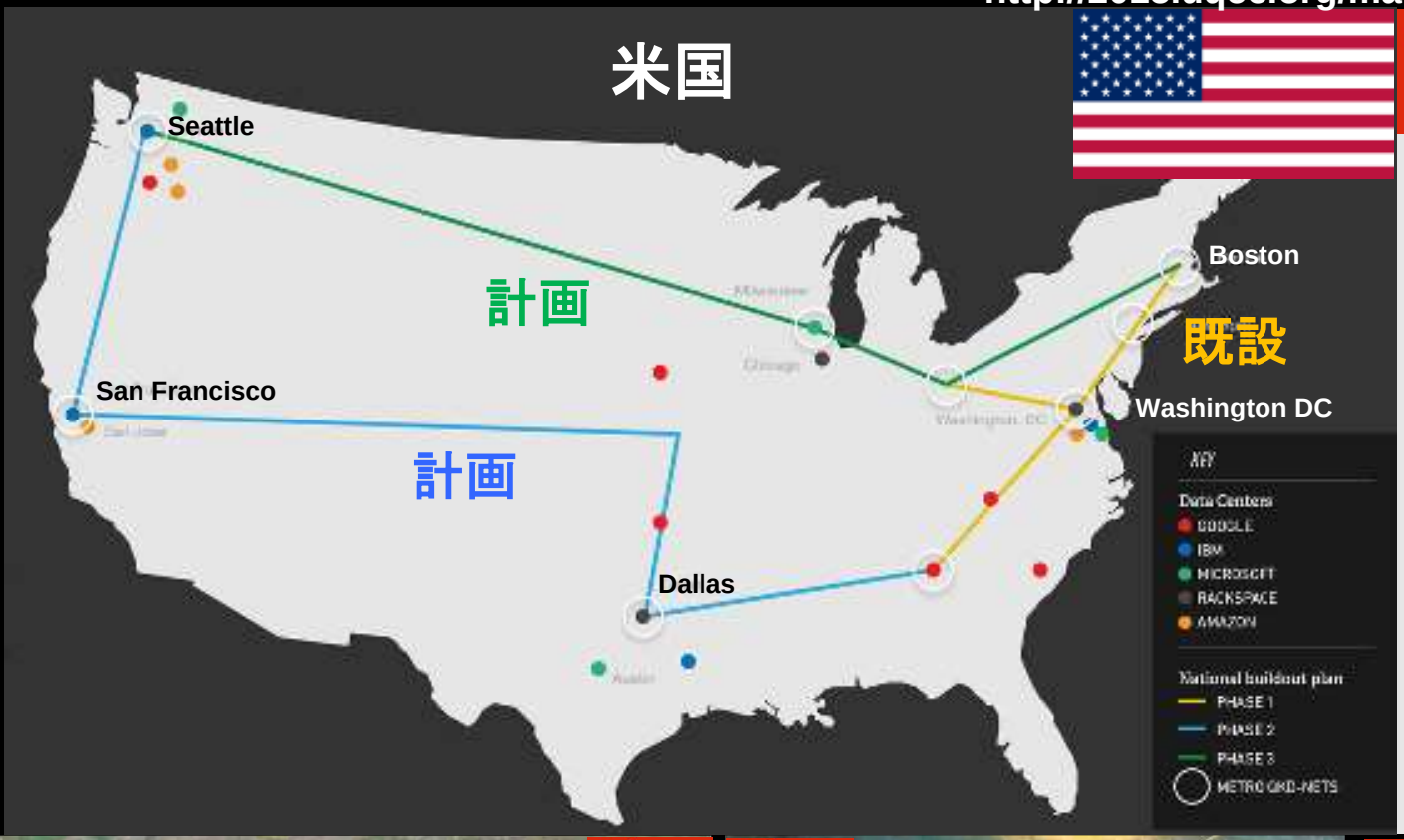
日経コンピュータ　2017.6.22

THE VERGE

2014年11月

米国・中国の量子暗号通信ネットワーク

http://2015.uqcc.org/materials/pdf/Part-V_Zhang.pdf

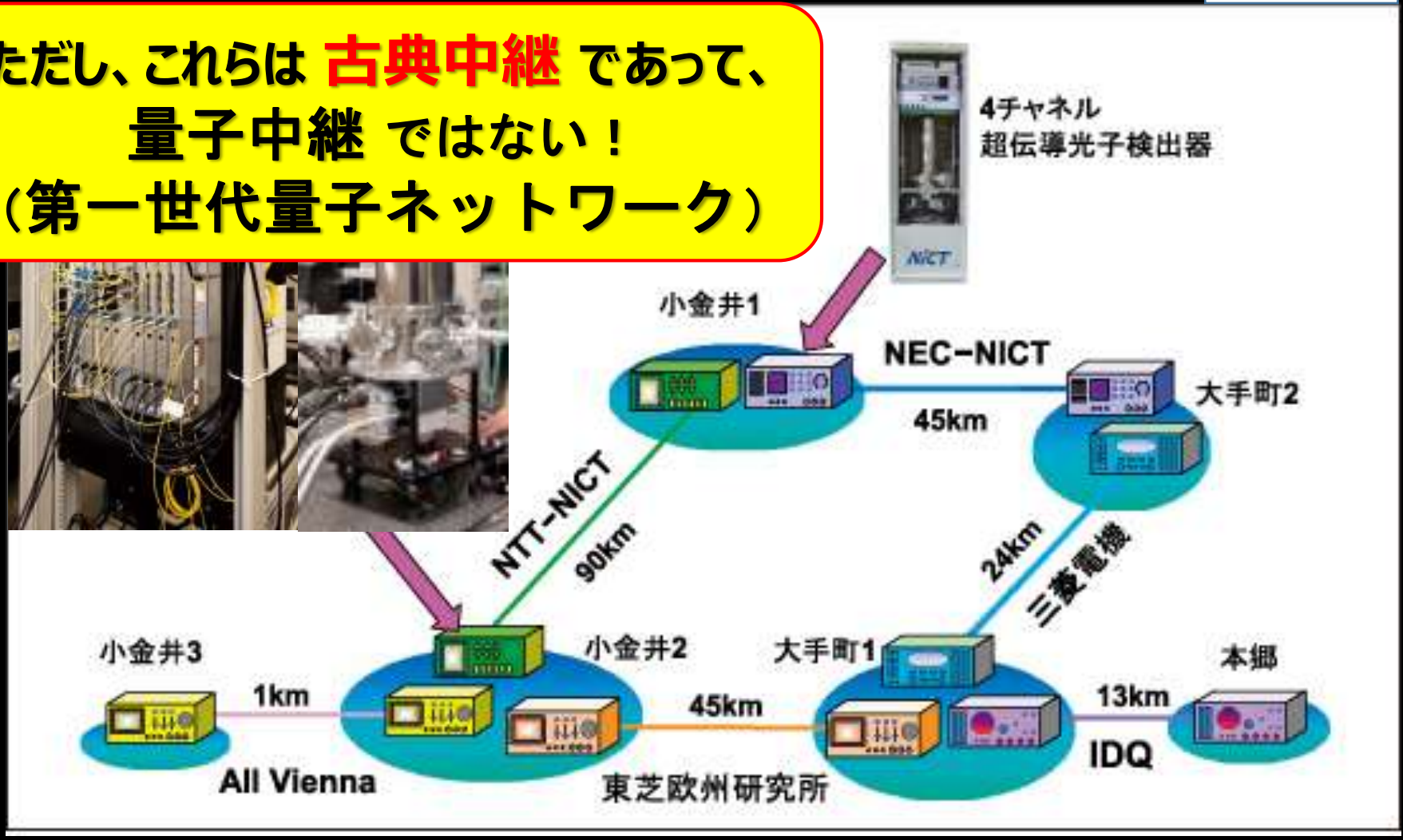


2010年10月

量子暗号ネットワーク（東京QKDネットワーク）

全長200km

ただし、これらは **古典中継** であって、
量子中継 ではない！
（第一世代量子ネットワーク）



中国、盗聴不可能な量子暗号衛星を打ち上げ

CNN.co.jp

2016年8月

Science AAAS

2017年7月

もつれ光子対1200 km送信

Pan Group, Science, July 2017

2018年1月　オーストリアとテレビ会議

中国、量子応用研究センター建設
1兆円規模、37ヘクタール

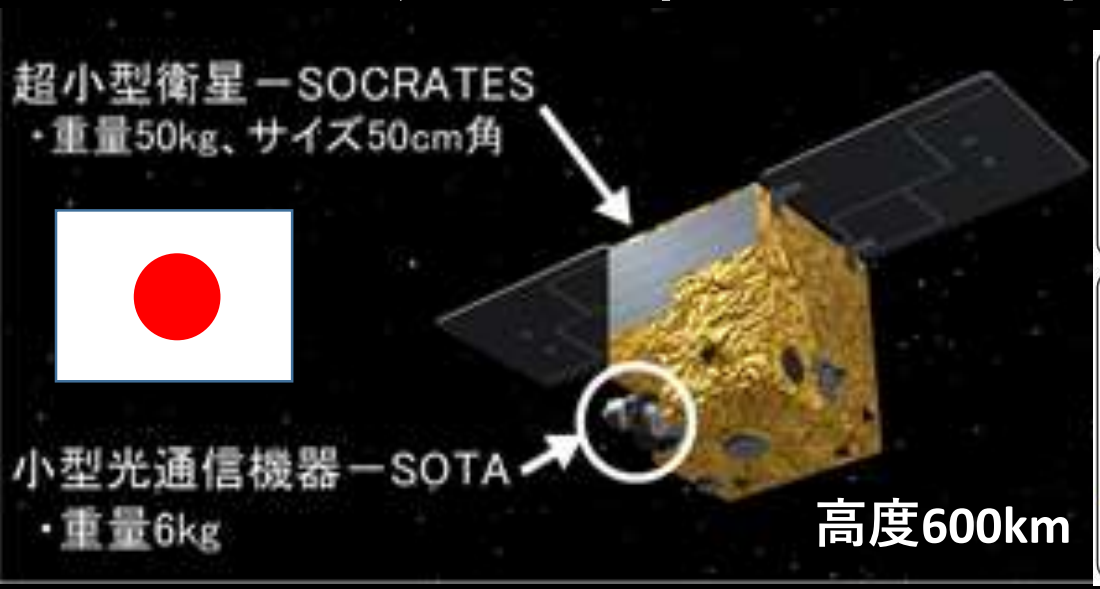
USTC(Shanghai)

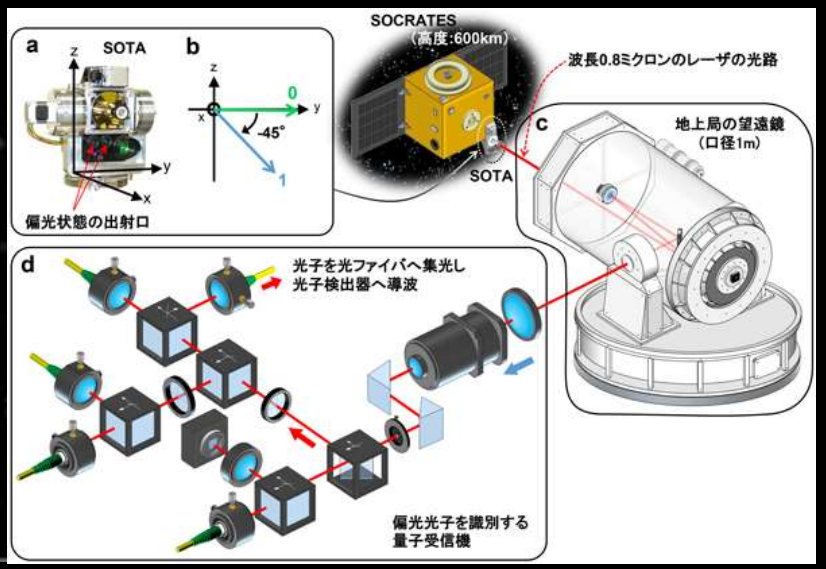
USTC(Hefei)

nature photonics

2017年7月

情報通信研究機構(NICT)
超小型衛星と地上間で量子暗号通信成功





2018年度
総務省
量子衛星通信
開発を本格化

nature photonics

2016年9月

中国･カナダの量子中継実験

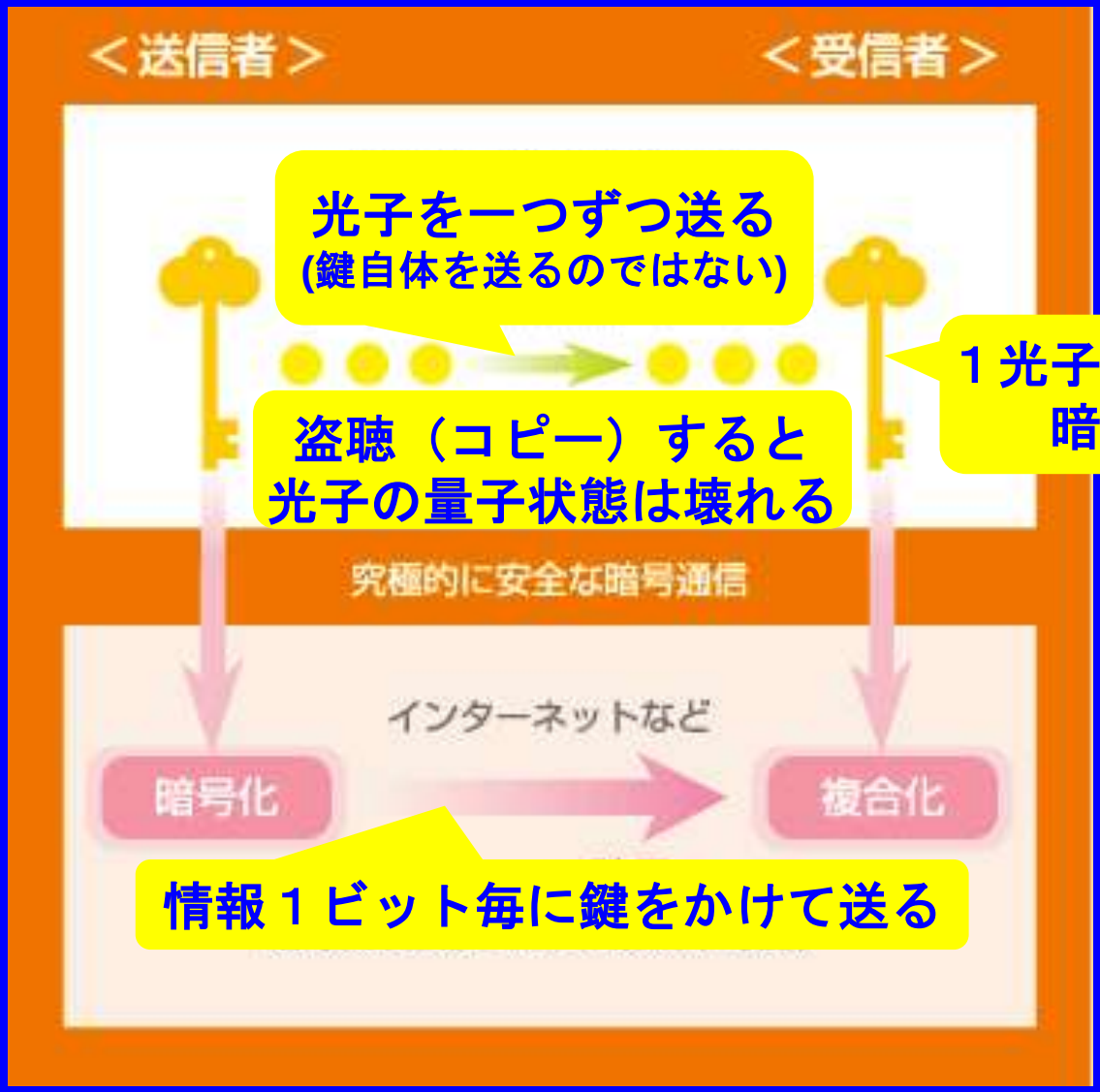
そもそも量子中継とは？

量子？	モノの名前ではない！性質！
量子メディア？	モノの名前 光子、原子（電子、核子）
量子暗号通信？	通信ではない！鍵！
量子もつれ？	双子ではない！一つ！
量子テレポーテーション？	必ずしも遠くに飛ばない！

量子暗号通信とは？

通信の鍵を光子で送ること！＝ 量子鍵配送（QKD）

Quantum Key Distribution



https://www.tdk.co.jp/techmag/knowledge/200706/index.htm

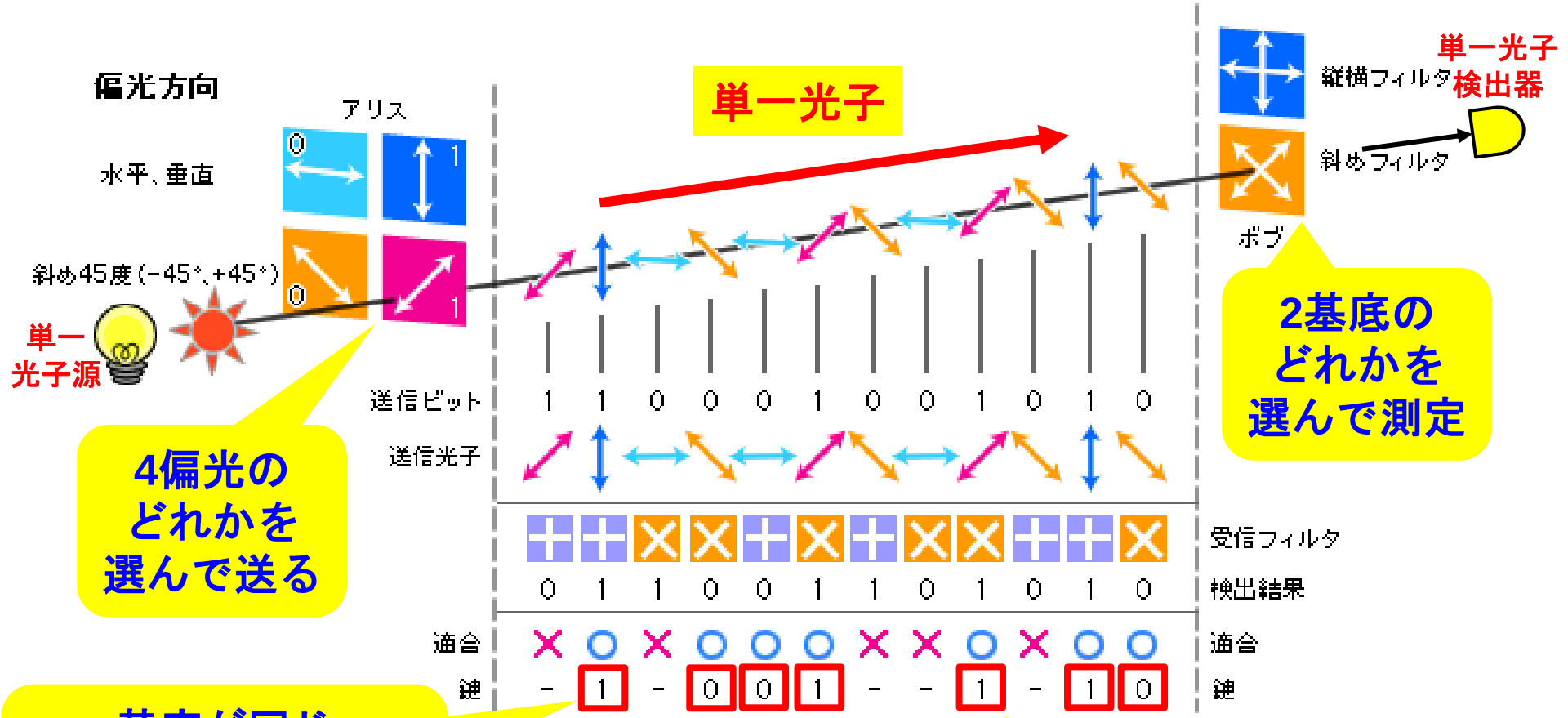
量子暗号通信の分類

	量子もつれ型		光子型	光波型
安全証明	装置モデルに対する仮定を緩和、あらゆる攻撃に対して安全	装置モデルに対する一定の仮定のもと、あらゆる攻撃に対して安全	装置モデルに対する一定の仮定のもと、あらゆる攻撃に対して安全	量子一括攻撃まで安全
安全性レベル	極めて高	高	高	中
プロトコル	Device-independent QKD, Measurement-device independent QKD (MDI)	E91 BBM92	BB84, DPS, Coherent-one way, RR-DPS	Continuous variable (CV)
実装形態	量もつれ光子源 ＋ 高感度単一光子検出	量もつれ光子源 ＋ 単一光子検出	コヒーレント光 / 単一光子源 ＋ 単一光子検出	コヒーレント光 ＋ ホモダイン検波
コスト	極めて高	高	中	低

2016年量子科学技術委員会佐々木雅英氏（NICT）資料

BB84の原理

“量子重ね合わせ”の原理を利用！



4偏光の
どれかを
選んで送る

2基底の
どれかを
選んで測定

基底が同じ
ときだけを
選びビット鍵を得る

ビット鍵 をもとに
暗号通信 を行う！

http://j-net21.smrj.go.jp/develop/digital/pic/001-20101222-01-03.gif

“量子重ね合わせ”とは？

E91(BBM92)の原理

“量子もつれ”の原理でより安全に！

2基底のどれかを選んで測定

もつれ光子対

縦横フィルタ

斜めフィルタ

ボブ

2基底のどれかを選んで測定

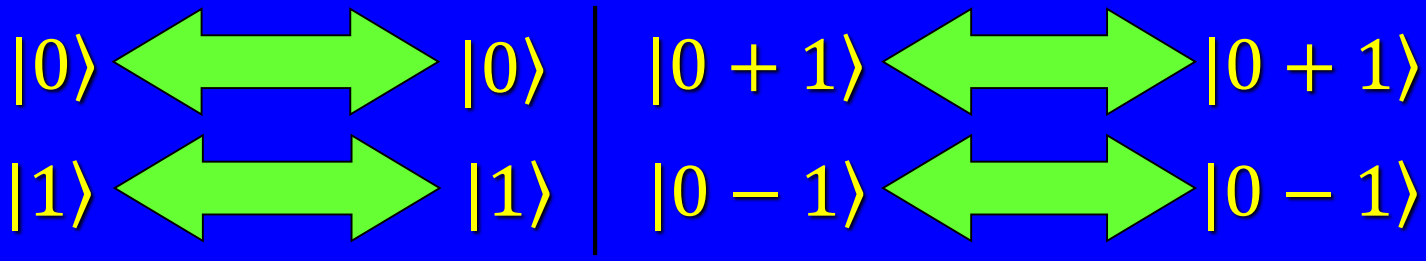
アリス

基底が同じときだけを選び鍵を得る

“量子もつれ”とは？

２つの量子が相関した状態

基底状態だけでなく重ね合わせ状態も相関！



二つの量子で“一つの状態”となっている

“ベル状態”と呼ぶ４種類がある

二つの量子の重ね合わせ状態

$$\begin{bmatrix} |0\,0\rangle + |1\,1\rangle \\ |0\,0\rangle - |1\,1\rangle \\ |0\,1\rangle + |1\,0\rangle \\ |0\,1\rangle - |1\,0\rangle \end{bmatrix}$$

どの種類かを測定 → ベル測定

どうして長距離量子暗号通信は難しいか？

量子はコピー（増幅）ができない！

コピーすると
量子状態は壊れる

光子を一つずつ送る必要がある！

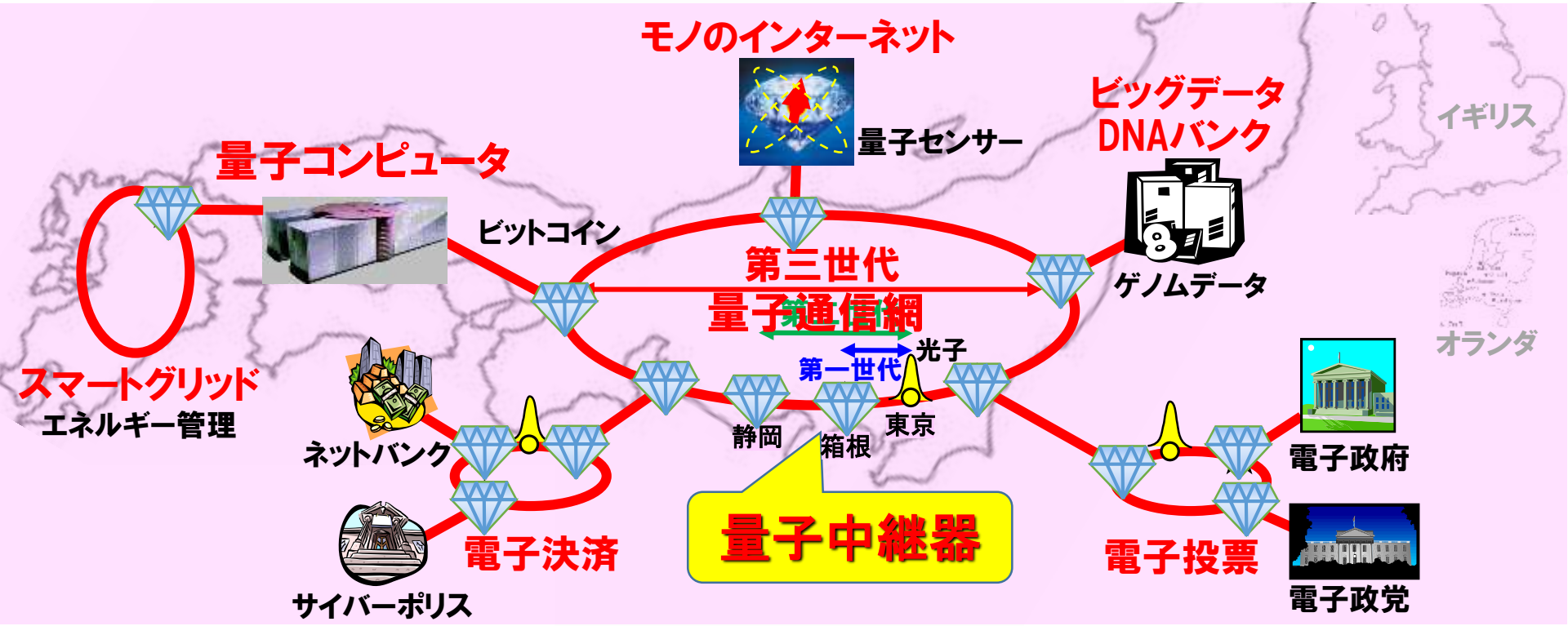
光ファイバー中では100km程度が限界

べき乗で減衰 ~ $(\text{単位損失})^{L}$

量子中継が不可欠

多項式で減衰 ~ $(\text{単位損失}) \times L$

量子暗号通信の世代



第一世代～100km　単一光子を直接伝送 ⇒ 中継が不要

これは簡単！

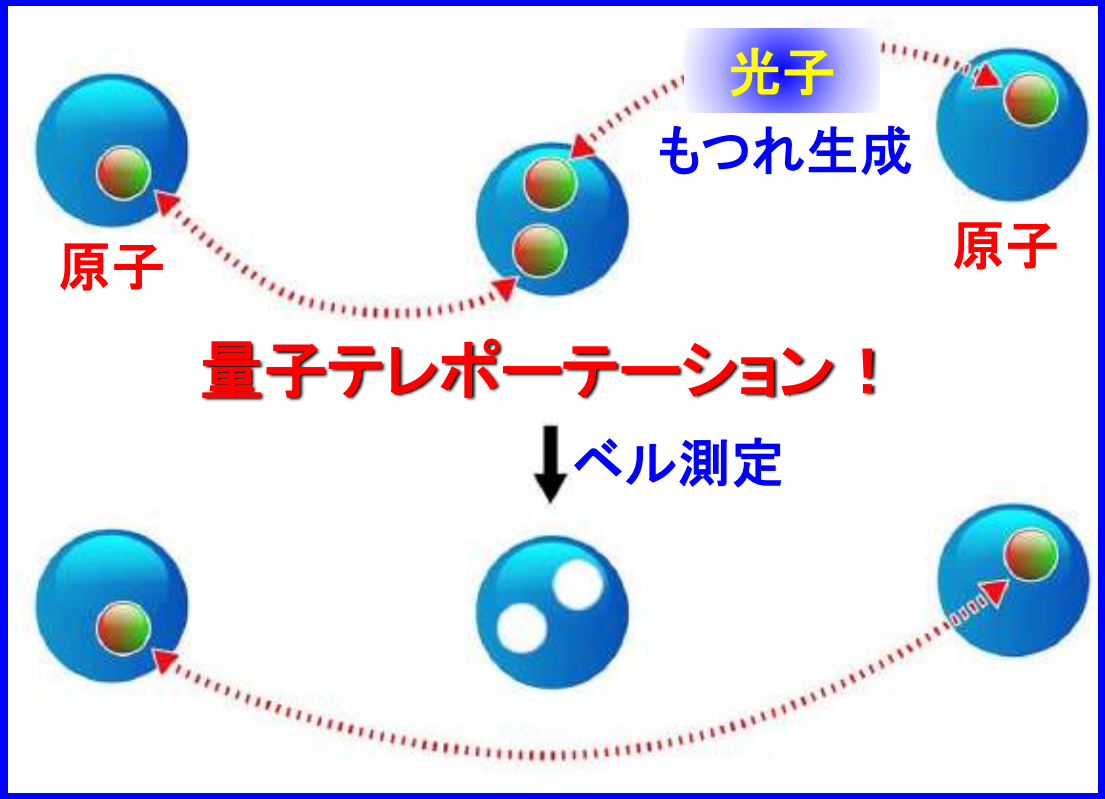
第二世代～200km　中継が一度だけ必要 ⇒ 確率的量子中継

第三世代＞1000km 中継が何度も必要 ⇒ 決定論的量子中継

これは大変！

量子中継の原理？

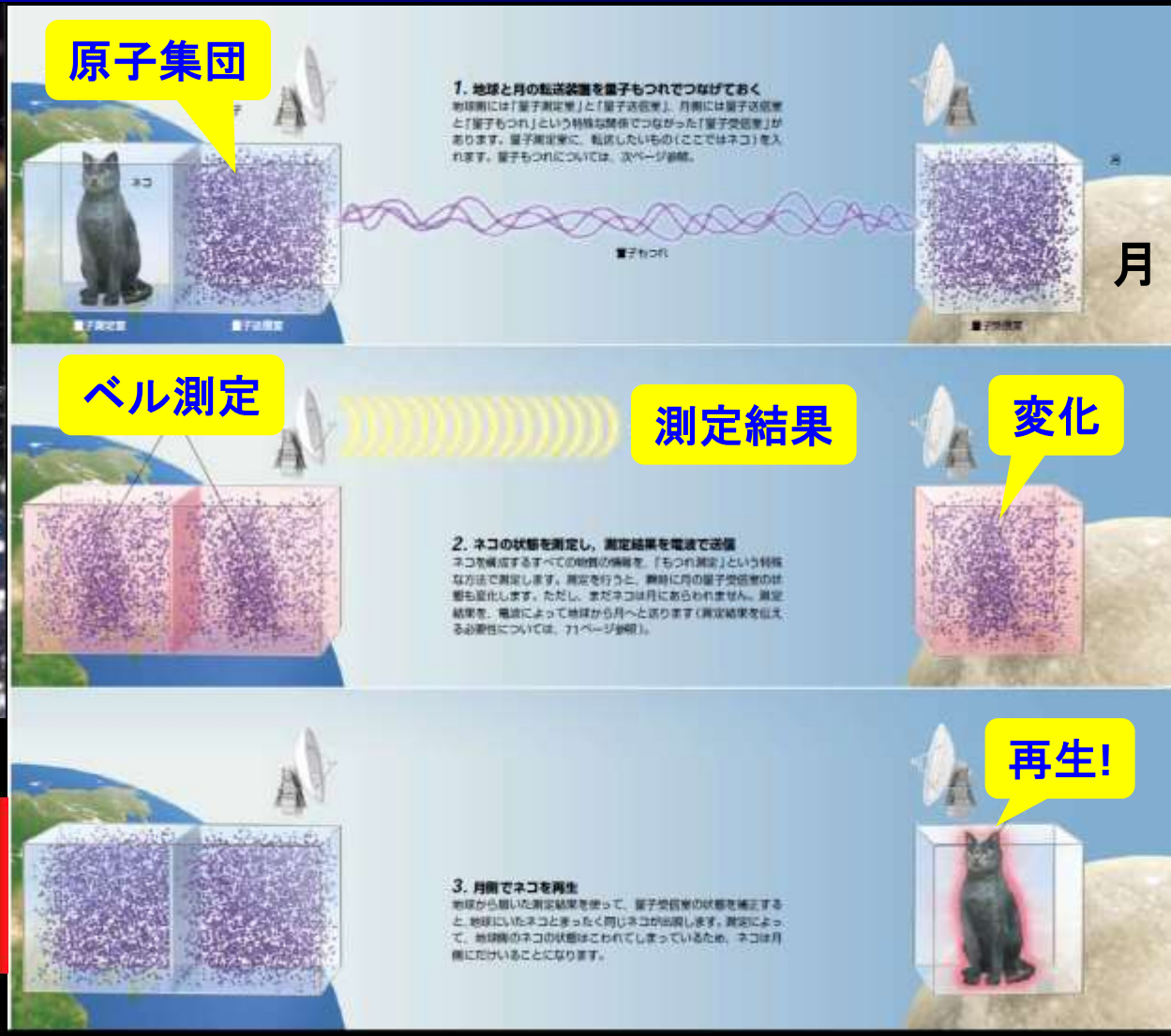
光子と同様に原子も量子！



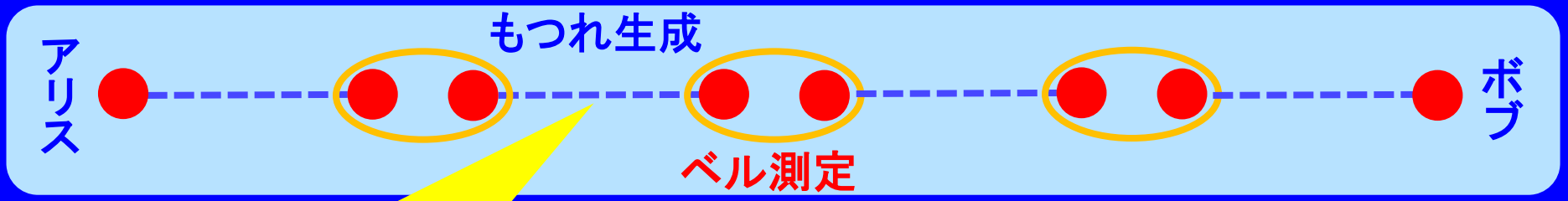
長距離もつれのできあがり！

量子テレポーテーション？

Newton
GRAPHIC SCIENCE MAGAZINE ニュートン
2018年6月号



量子中継ネットワークの原理



もつれ生成 と ベル測定 で
もつれ を拡張！

テレポーテーション

量子暗号

分散量子計算

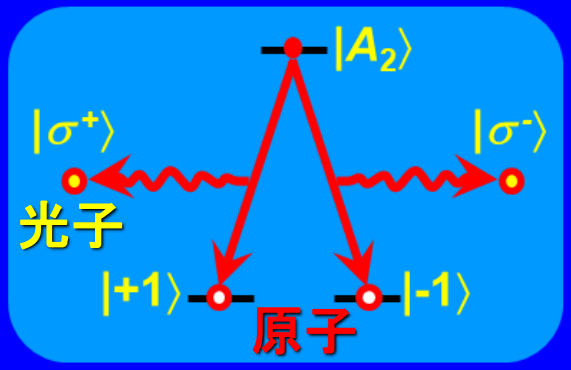
連携望遠鏡

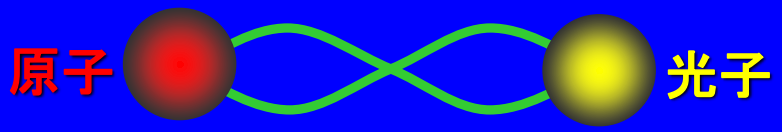
時計同期

“もつれ”の作り方

１.非線形結晶から“もつれ光子対”が発生

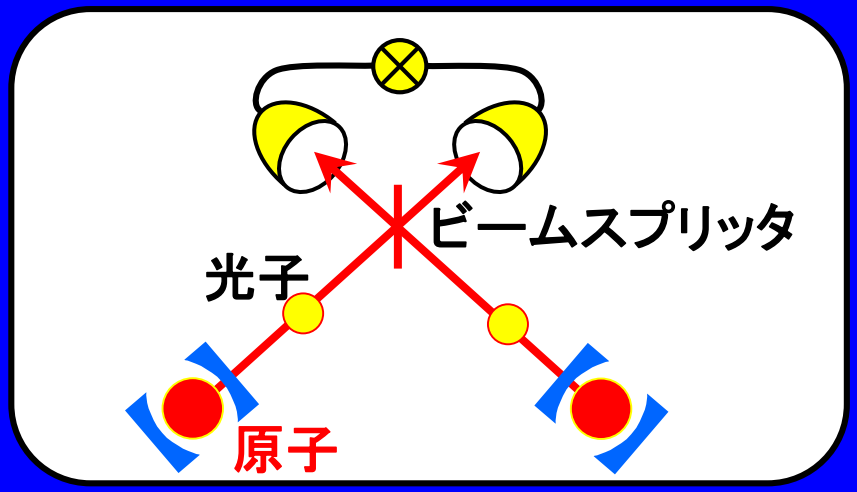
２.励起状態から“原子ともつれた光子”が発生





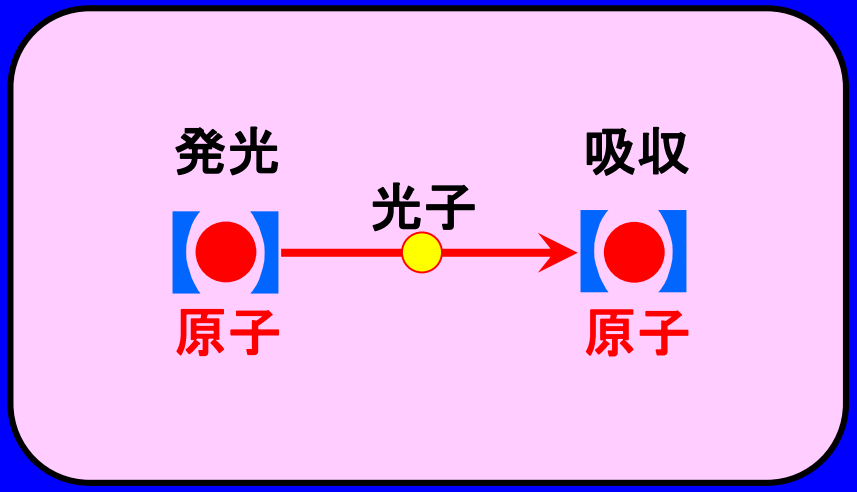
原子間もつれの作り方

発光 + ビームスプリッタ



正確な時間合わせが必要

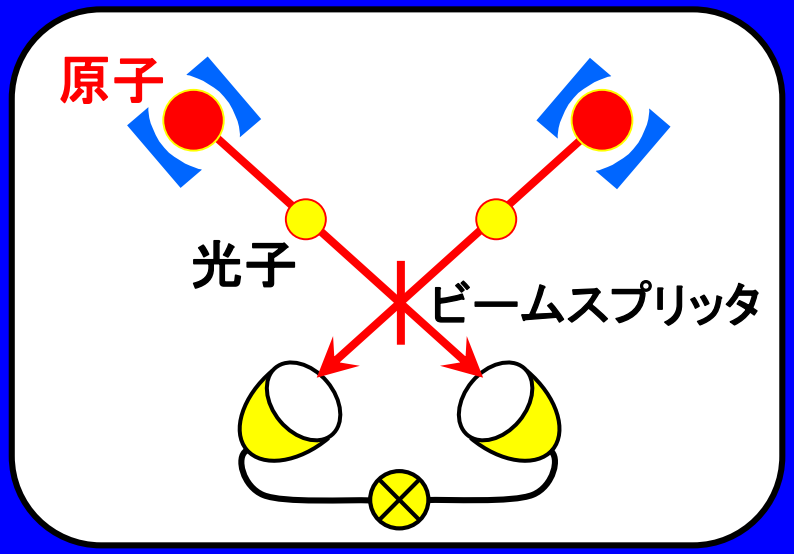
発光 + 吸収



正確な時間合わせが不要

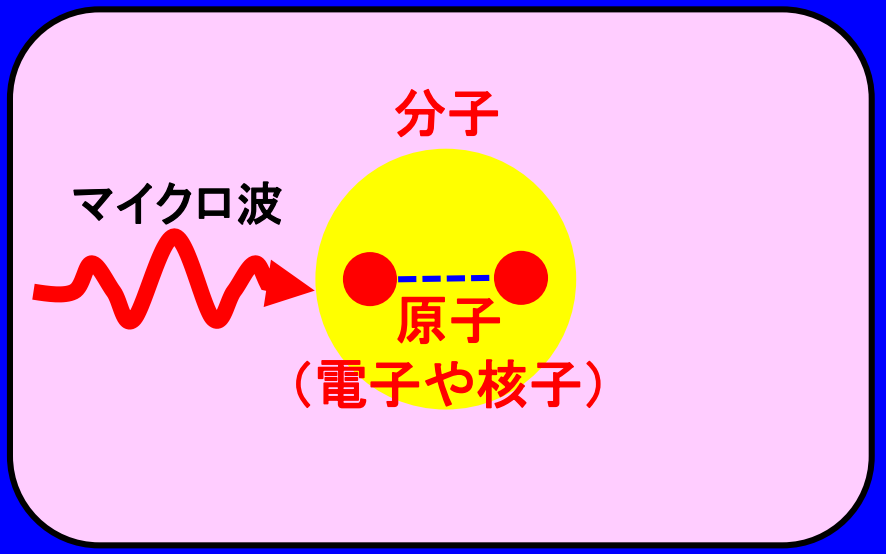
原子間もつれの測り方

発光 + ビームスプリッタ



確率的な中継

分子の中で測定

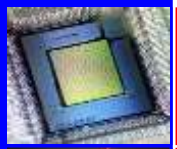


決定論的な中継

量子中継ネットワーク
研究最前線

量子ビットの代表例

量子計算に最適



	操作性	メモリ性	動作温度（実装性）	集積性
超電導量子回路	◎	× (<1ms)	× (<10mK)	◎
ダイヤモンドNV中心	○	◎ （>10s）	◎ (RT,<10K)	△
イオントラップ	○	◎ （>10s）	× (～μK?)	△
半導体量子ドット	○	× (<1ms)	△ (<1K)	○
希土類結晶	×	× (<1ms)	△ (<3K)	×

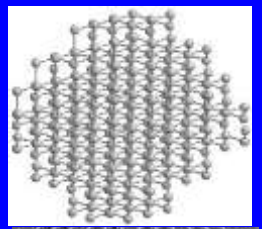
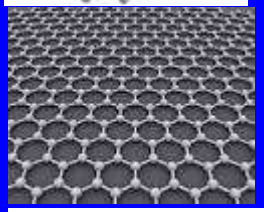
量子中継に最適

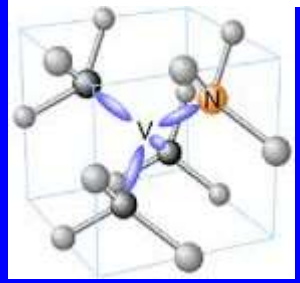
なぜダイヤモンドNV中心？

♦ 物理的・機械的に安定している！
♠ 量子状態を極めて長く保持できる！
♣ 発光や吸収といった光学過程が強く、きれい！

高次元
低次元

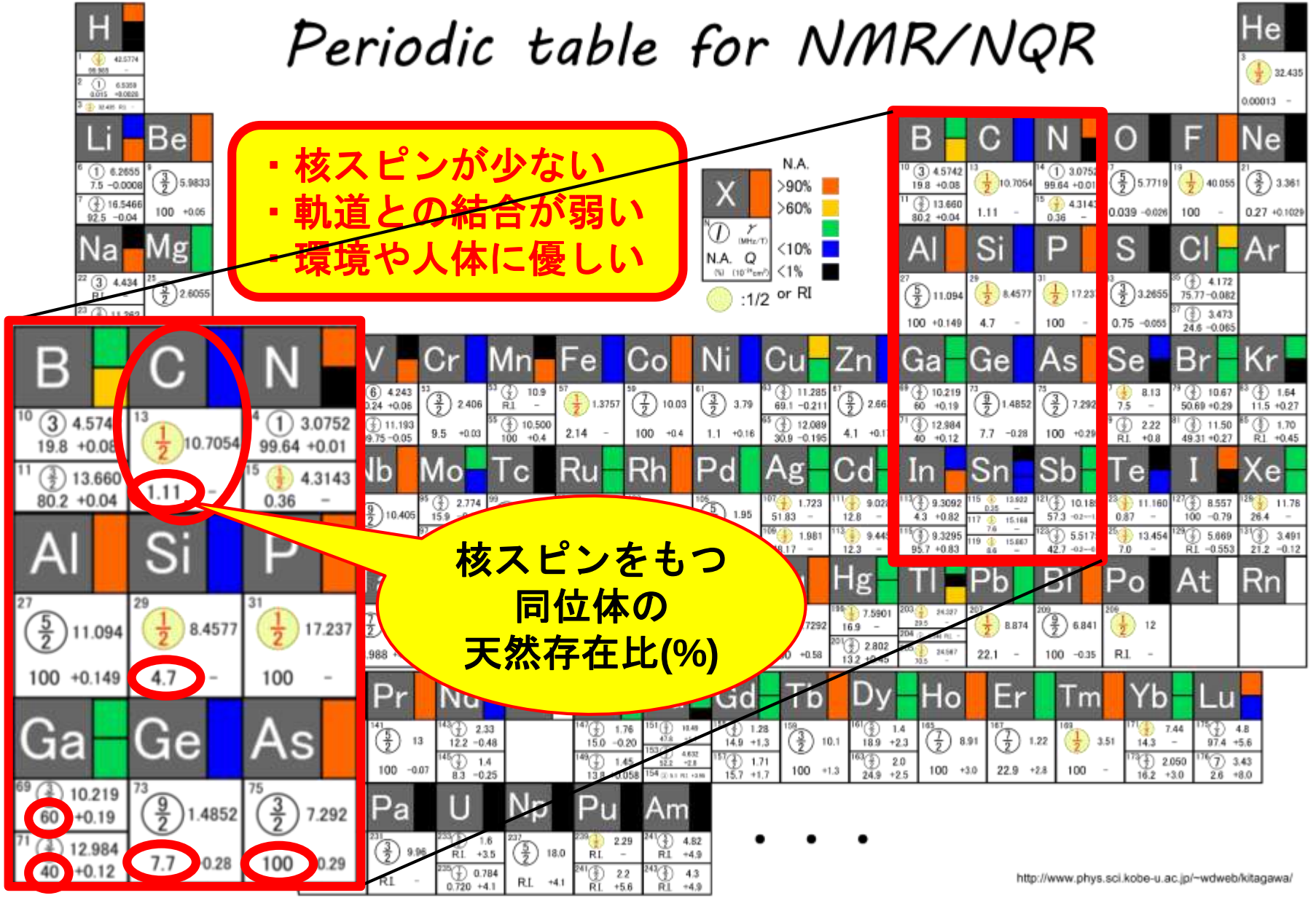
3D　ダイヤモンド
2D　グラフェン
1D　ナノチューブ
0D　ダイヤモンド欠陥

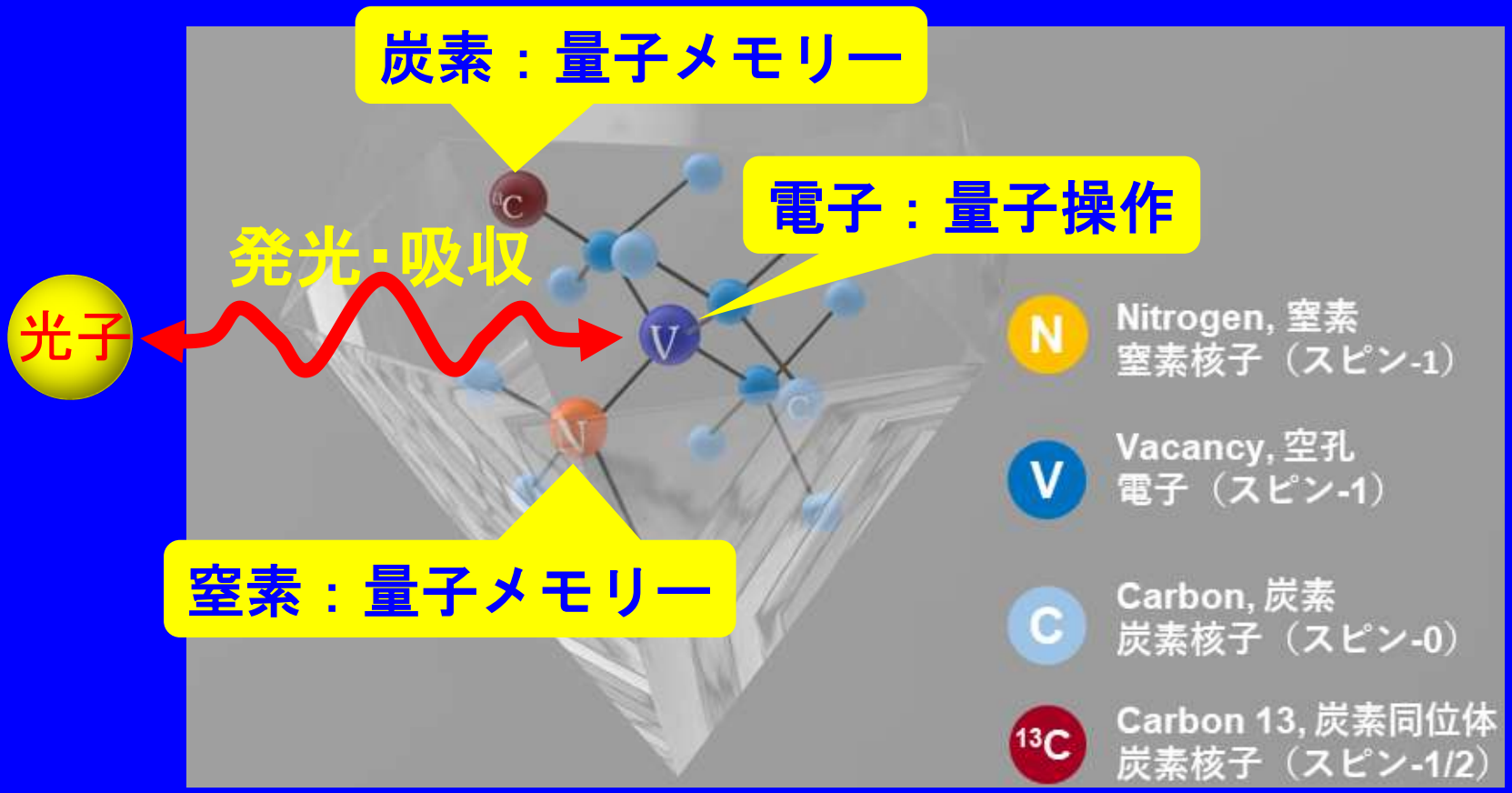


真空中の**孤立原子**に近く
結晶中に**固定**されている
表面からの**雑音**が少ない

なぜ炭素？


Periodic table for NMR/NQR
・核スピンが少ない
・軌道との結合が弱い
・環境や人体に優しい
核スピンをもつ
同位体の
天然存在比(%)
N.A.
>90%
>60%
<10%
<1%
:1/2 or RI
http://www.phys.sci.kobe-u.ac.jp/~wdweb/kitagawa/

ダイヤモンドNV中心



圧倒的に長い
量子メモリー時間
10秒以上(<10K)

光子とメモリーを変換する
小型の量子コンピュータ

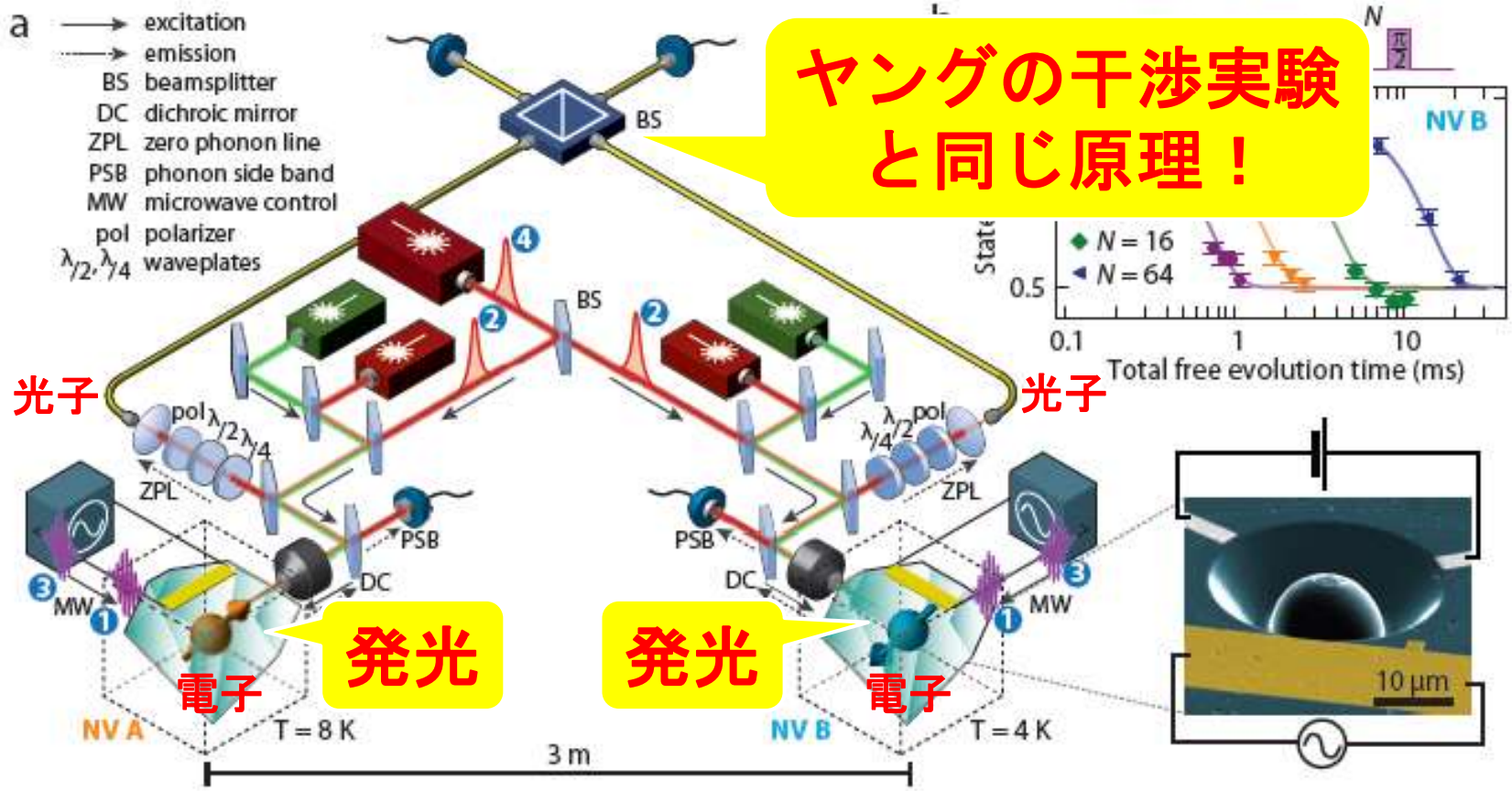
nature

ダイヤモンド間の量子もつれに成功

2013年

Heralded entanglement between solid-state qubits separated by 3 meters

H. Bernien,[1] B. Hensen,[1] W. Pfaff,[1] G. Koolstra,[1] M.S. Blok,[1] L. Robledo,[1]
T.H. Taminiau,[1] M. Markham,[2] D.J. Twitchen,[2] L. Childress,[3] and R. Hanson[1,*]



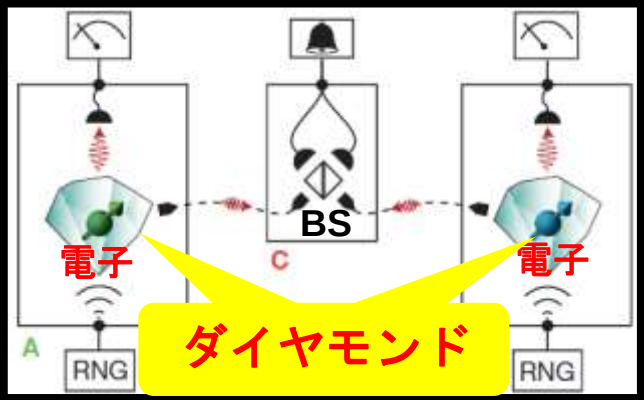
nature

遠距離（1.3km）量子もつれに成功

2015年

Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen[1,2], H. Bernien[1,2]†, A. E. Dréau[1,2], A. Reiserer[1,2], N. Kalb[1,2], M. S. Blok[1,2], J. Ruitenberg[1,2], R. F. L. Vermeulen[1,2], R. N. Schouten[1,2], C. Abellán[3], W. Amaya[3], V. Pruneri[3,4], M. W. Mitchell[3,4], M. Markham[5], D. J. Twitchen[5], D. Elkouss[1], S. Wehner[1], T. H. Taminiau[1,2] & R. Hanson[1,2]



1.3km

⇒ Requires perfect coherence

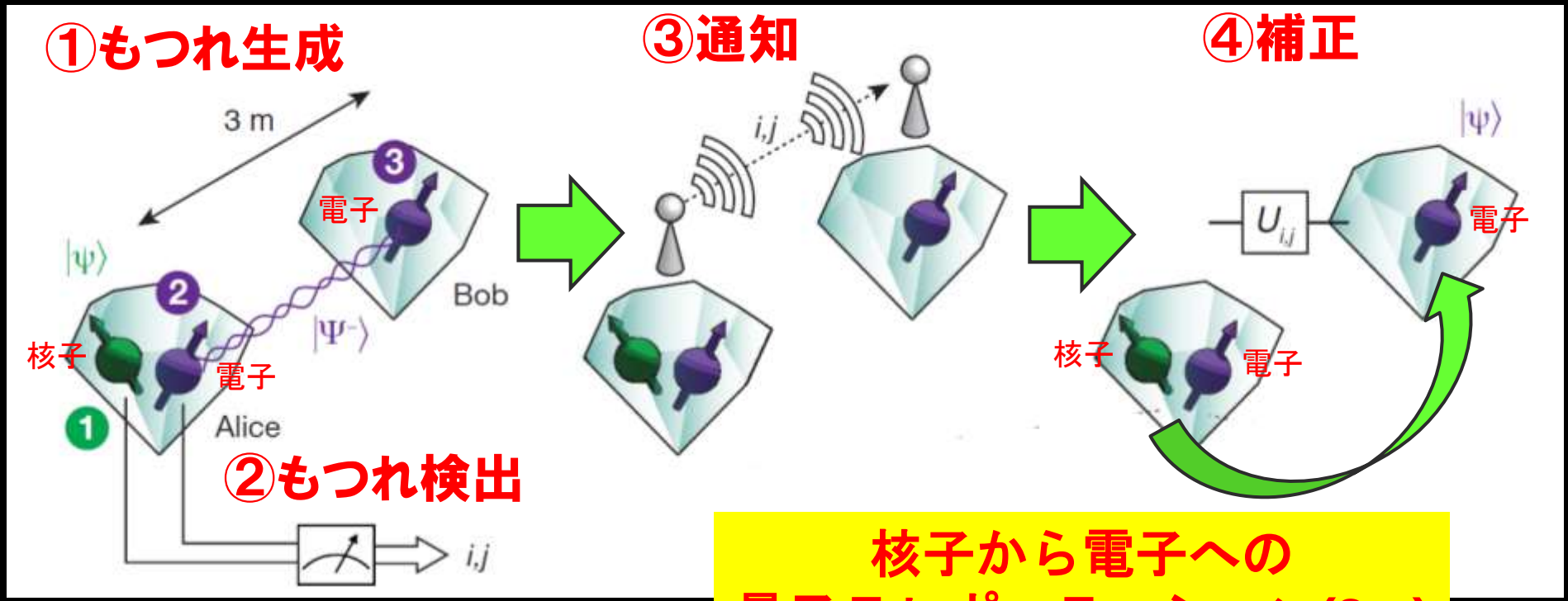
nature

2014年

ダイヤモンドを用いた量子テレポーテーションに成功

Unconditional quantum teleportation between distant solid-state qubits

Wolfgang Pfaff, Bas Hensen, Hannes Bernien, Suzanne B. van Dam, Machiel S. Blok,Tim H. Taminiau, Marijn J. Tiggelman,Raymond N. Schouten, Matthew Markham, Daniel J. Twitchen, and Ronald Hanson



核子から電子への
量子テレポーテーション(3m)

我々の取り組み

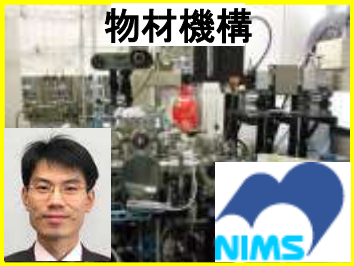
発光−吸収型量子中継

研究体制

横浜国大（小坂）
システム実証

＋

産総研（加藤） 微細加工
ドーピング制御
物材機構（寺地） 結晶成長
量研機構（小野田）イオン注入



京大化研（水落）
量子物性

NTT（松崎）
量子理論

シュトゥットガルト大
(Wrachtrup)

ウルム大
(Jelezko)

SUMITOMO ELECTRIC
Connect with Innovation

SII

材料・ナノ構造
素子

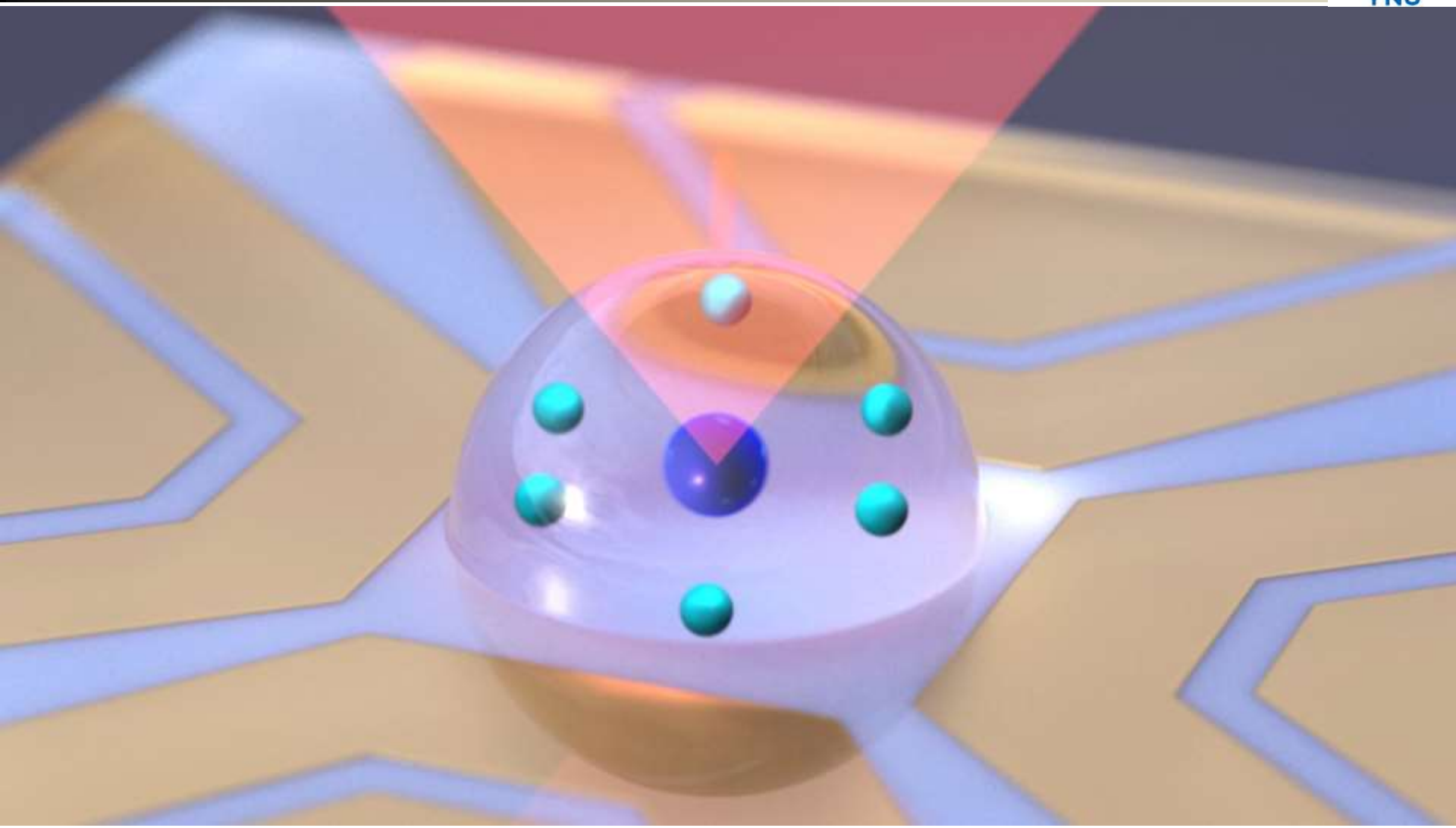
NTT AT & NTT EL

マイクロ波・光波
モジュール

NEC

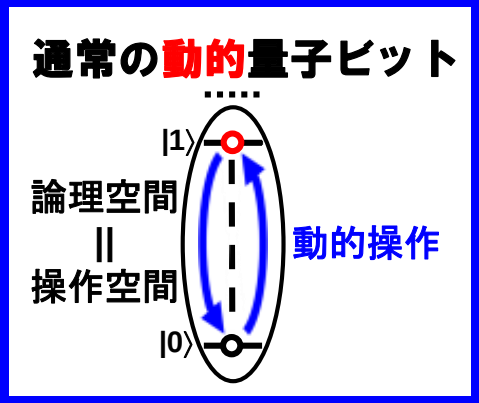
電子制御
システム

発光-吸収型ダイヤモンド量子中継素子

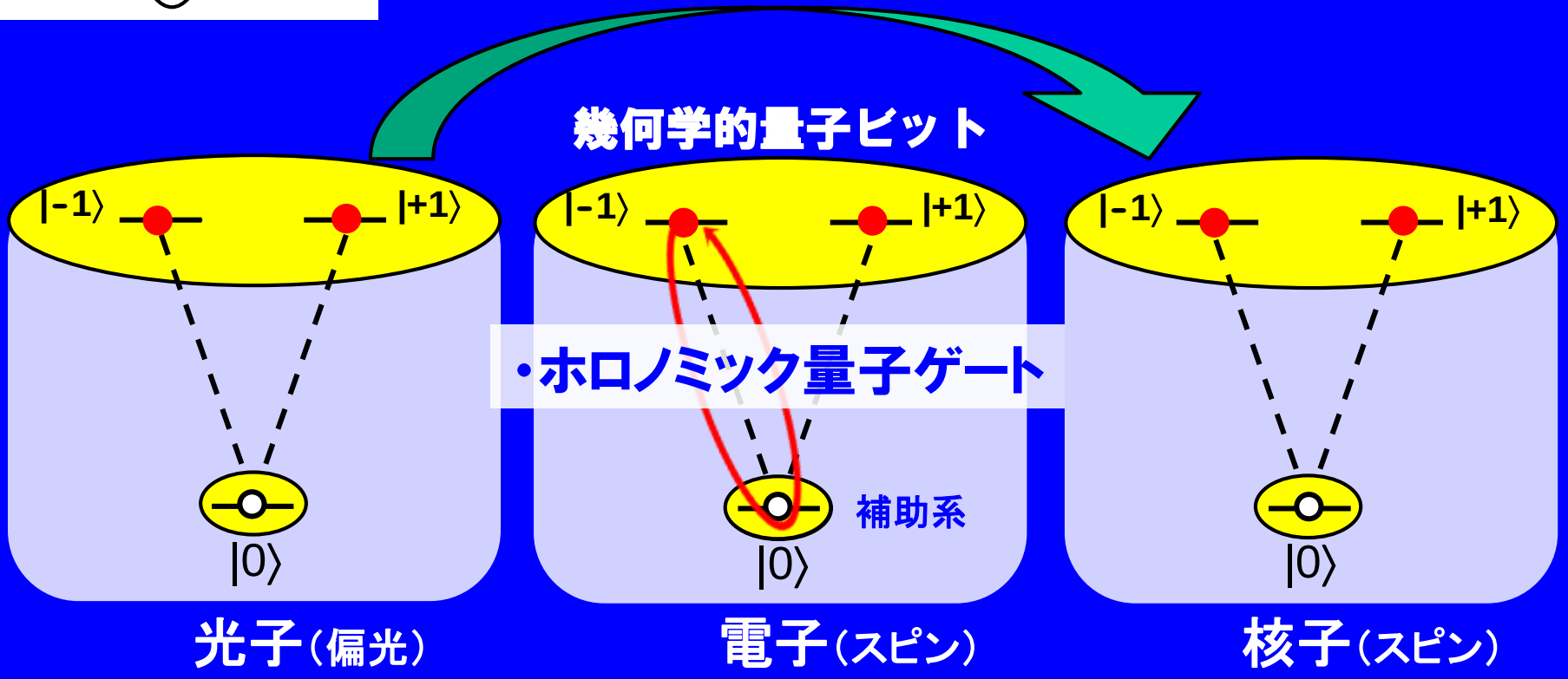


幾何学的量子ビット

エネルギー差のない
幾何学的な量子ビット



・量子テレポーテーション転写



補助系を介して量子操作

量子テレポーテーション転写

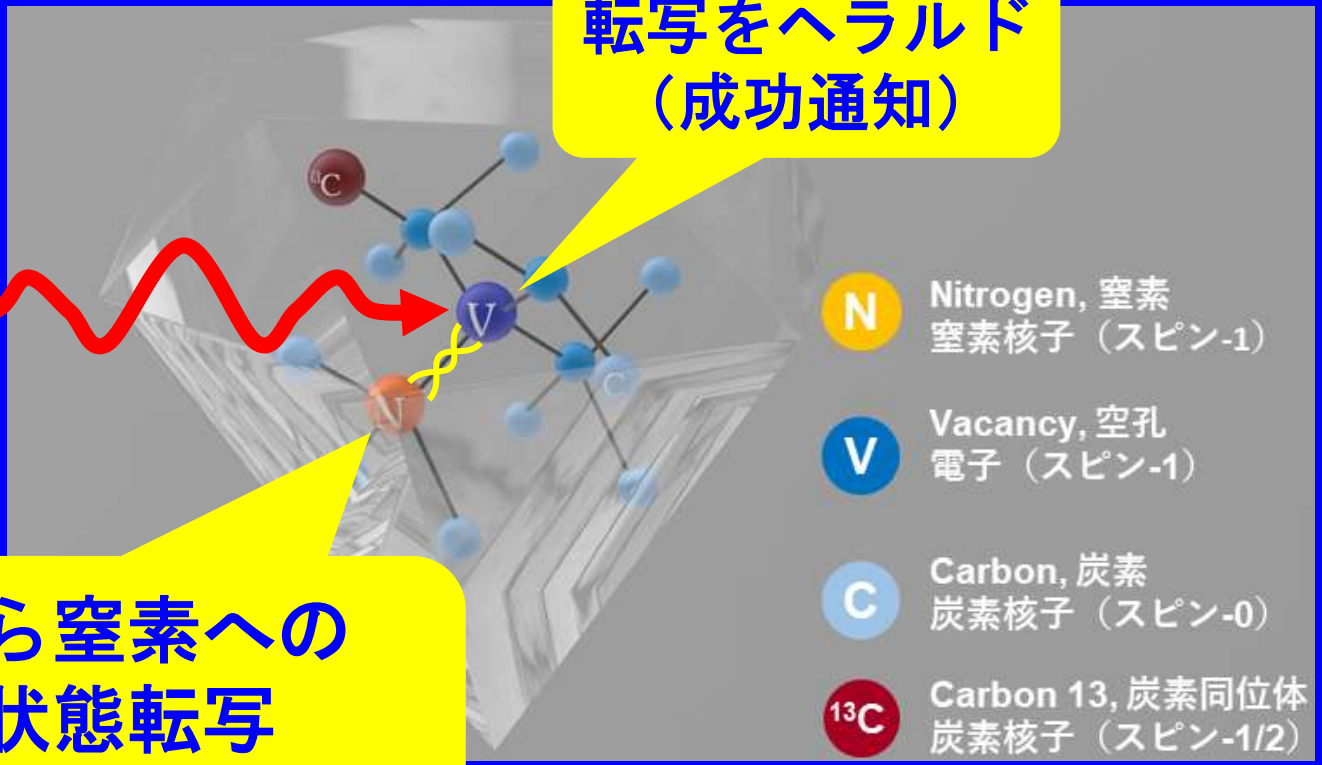
nature photonics 2016

S. Yan, H. Kosaka et al.

シュトゥットガルト大Wrachtrup教授との共同研究

転写をヘラルド
（成功通知）

光子

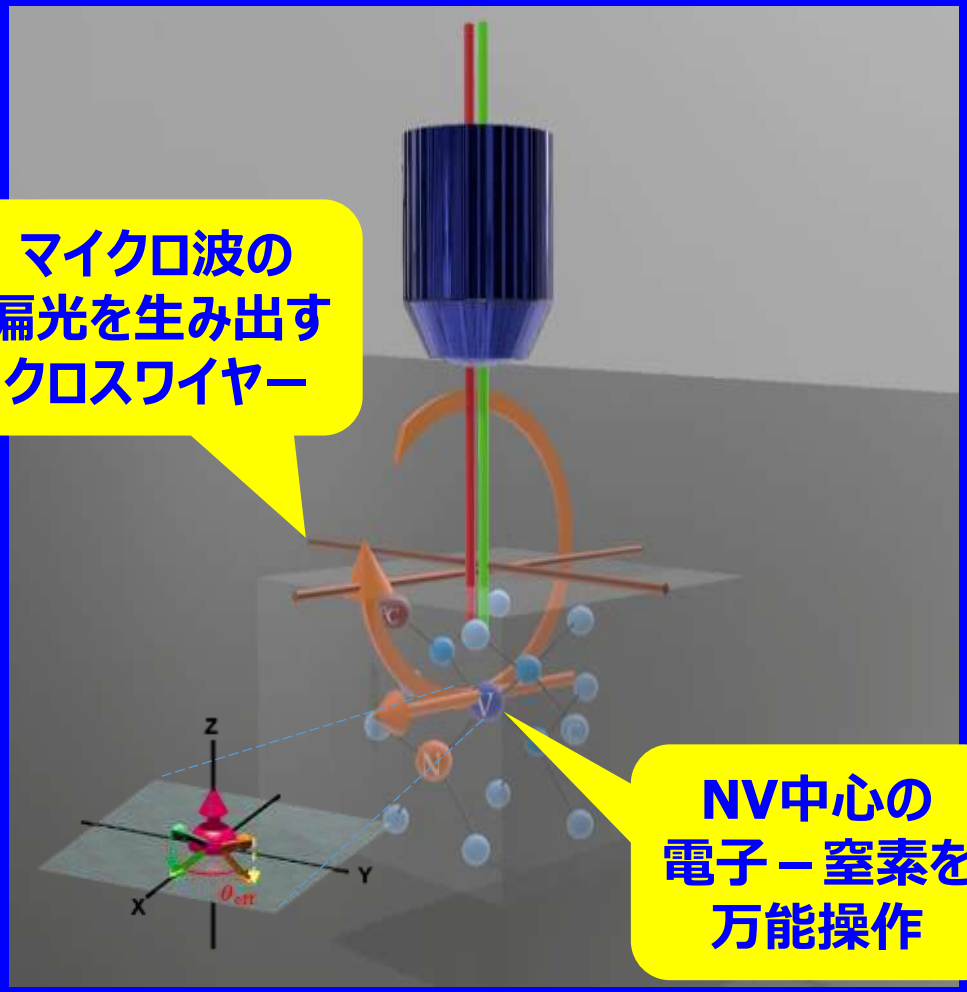


光子から窒素への
量子状態転写
（量子メディア変換）

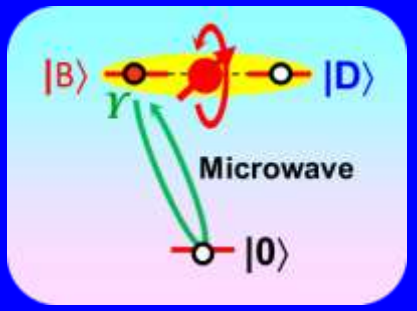
ホロノミック量子ゲート

nature COMMUNICATIONS 2018

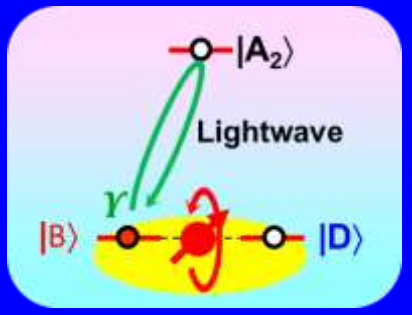
K. Nagata, K. Kuramitani, Y. Sekiguchi and H. Kosaka



マイクロ波の場合



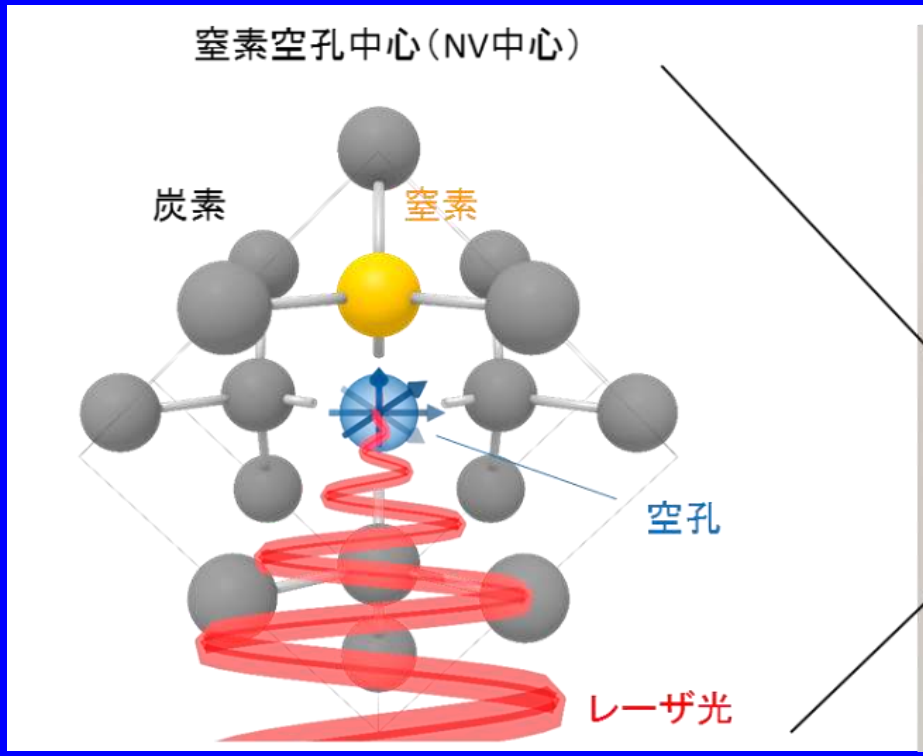
光波の場合

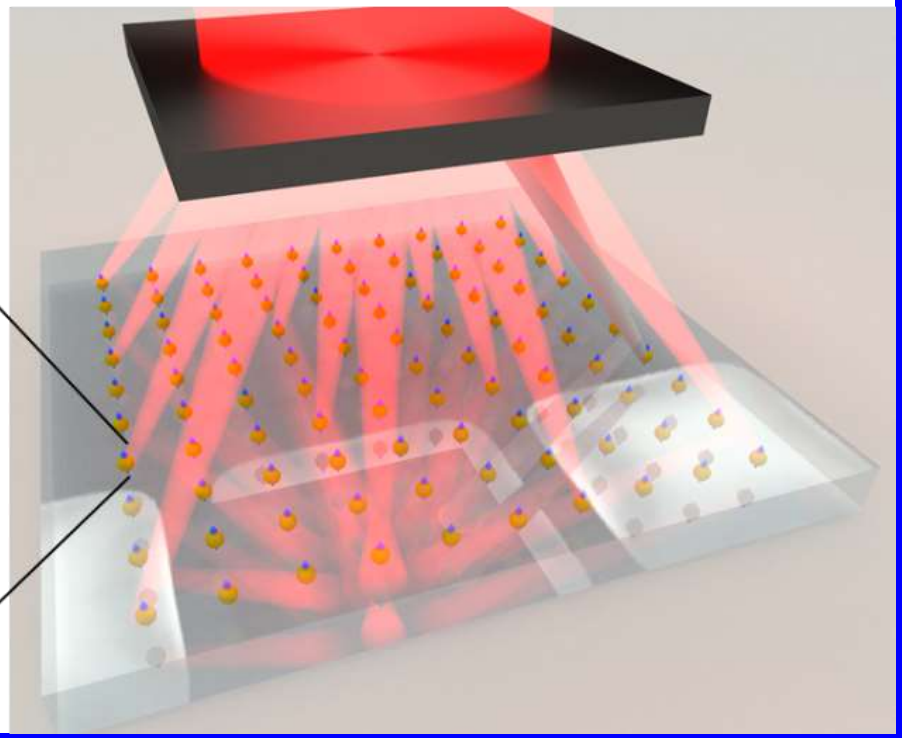


光波によるホロノミック量子ゲート

nature photonics 2017

Y. Sekiguchi, N. Niikura, R. Kuroiwa, H. Kano and H. Kosaka



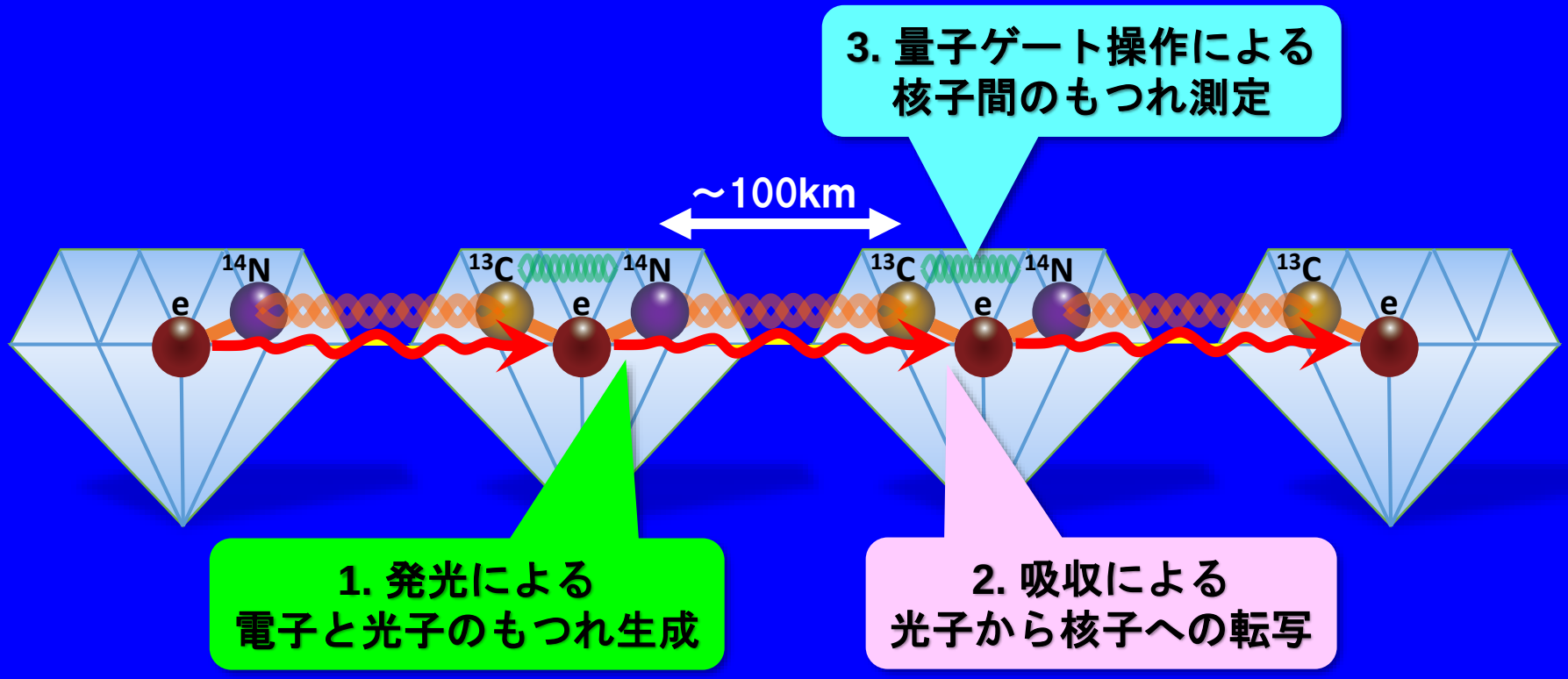


量子集積チップの光アクセスを可能に

マイクロワットで従来より100倍速く、
3倍高い精度で光スピン制御

発光-吸収型 量子中継ネットワーク

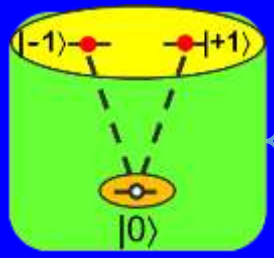
発光ー吸収だけでネットワークを形成！



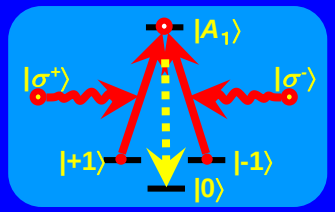
正確な時間合わせが不要！

YNUにおける成果発表リスト

量子ビット
判定条件



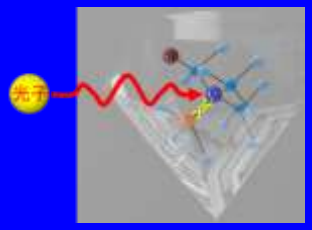
読み出し 電子–光子もつれ検出



Phys. Rev. Lett. 2015

Physical Review Letters, 114, 053603 (2015)

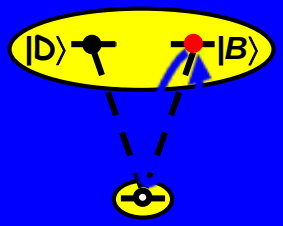
書き込み 量子テレポーテーション転写



Nature Photonics 2016

Nature Photonics, 10,507-511(2016)

保持 幾何学的スピンエコー



Nature Communication 2016

Nature Communications, 7, 11668 (2016)

制御 ホロノミック量子ゲート

Nature Photonics 2017

Nature Photonics, 11, 309-314 (2017)

Nature Communications 2018

Nature Communications, 9, 3227 (2018)

拡張性 ハミルトニアン機械学習

Optics Letters 2018

Optics Letters, 43, 2380-2383 (2018)

量子中継関連プロジェクト

最新情報

世界中で沸き立つ研究意欲　量子情報技術

表 各国の研究プロジェクトの概要

オランダ

2015年6月 10年で1億3500万ユーロ（約162億円）の研究資金を、量子ゲート方式を研究する「QuTech」に投資

2015年9月 米インテルが同じくQuTechに5000万ドル（約55億円）を出資

英国

2013年 5年で2億7000万ポンド（約378億円）の研究資金を英国工学・物理科学研究会議に量子情報分野向けとして出資

EU

2016年 10年で10億ユーロ（約1200億円）の研究資金を量子情報の研究向けに出資すると発表

欧州委員会

中国

2015年 重点科学研究分野4項目の一つに量子情報を認定し、中国科学院に量子計算実験室を設立

2016年 量子暗号通信衛星を打ち上げ

日本

2014年 革新的研究開発推進プログラム（ImPACT）に5年で30億円を出資

量子人工脳（レーザーネットワーク型）の開発を進める

2018年 文科省が量子化学技術委員会を発足し、量子情報分野の研究プロジェクトを開始予定

日経コンピュータ　2017.6.22

米国
Quantum Initiative
1000億円

➡ **QuTech 200億円**
量子計算、量子中継

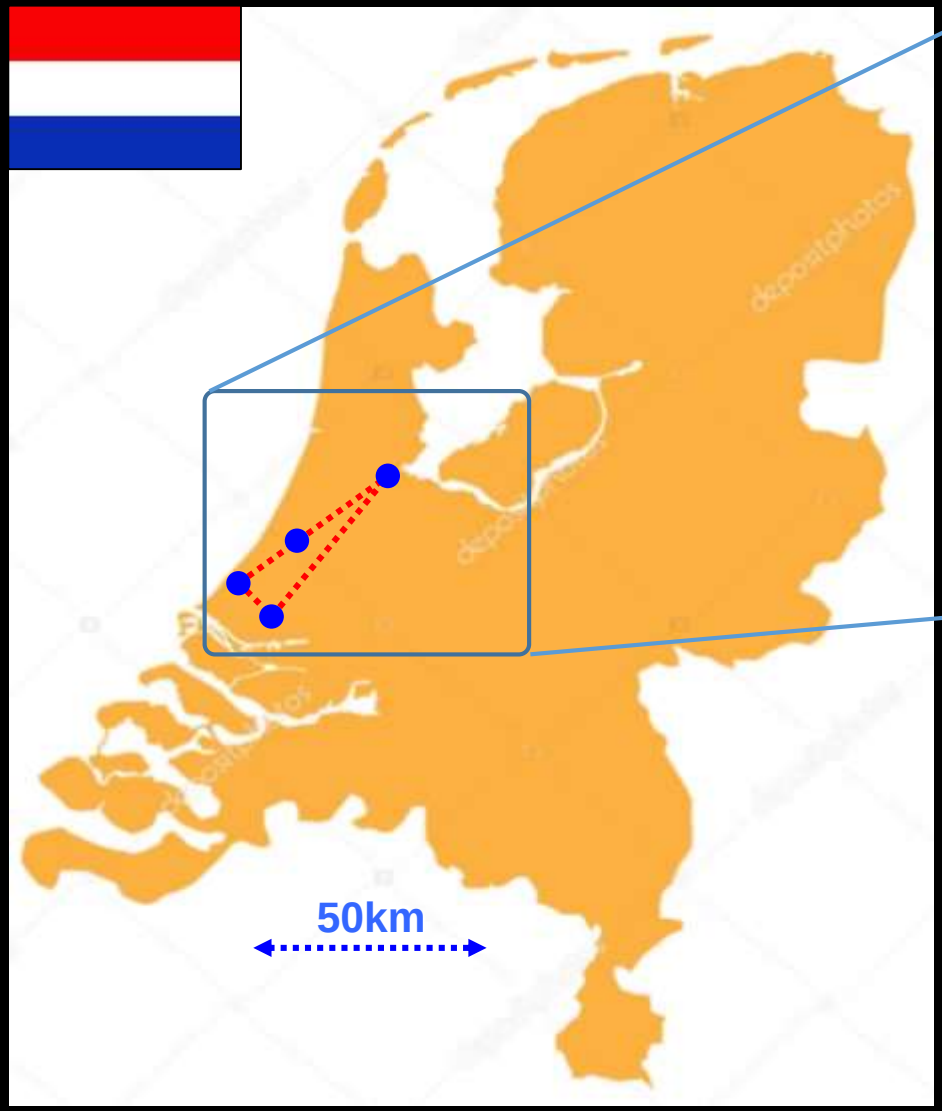
➡ **Quantum Tech. Hub**
400億円（5年）
量子分野全般

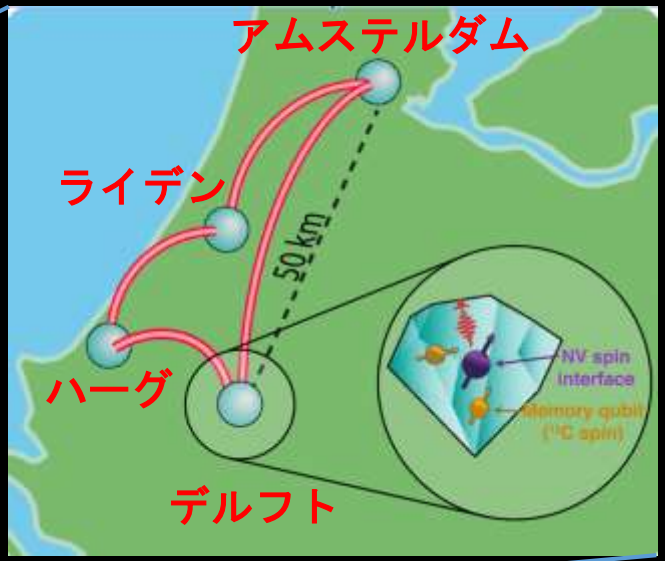
➡ **Quantum Flagship**
1300億円（10年）
量子インターネット
を含む量子分野全般

➡ **CAS, USTC(Hefei)**
1000億円越
量子NW（2000km）
量子衛星（1200km）

➡ **Q-Leap, SIP**

オランダの量子中継ネットワーク（2020完成）





4都市
量子中継
全長
100km

Quantum Sci. Technol. 2 (2017) 034002

https://labs.ripe.net/Members/becha/introduction-to-the-quantum-internet

ドイツの量子中継コンソーシアム（Q.Link.X）

2019年発足

ダイヤモンド、量子ドット、冷却原子

Partners

- **Technische Universität München**
- Technische Universität Dortmund
- **HighFinesse Laser and Electronic Systems GmbH,** Tübingen
- Fraunhofer Heinrich-Hertz-Institut, Berlin
- Technische Universität Berlin
- **Universität Stuttgart**
- Universität Paderborn
- **Universität des Saarlandes, Saarbrücken**
- Freie Universität Berlin
- Leibniz-Institut für Festkörper- und Werkstoffforschung Dresden
- Ruhr-Universität Bochum
- **Swabian Instruments GmbH**
- Leibniz Universität Hannover
- Max-Planck-Institut für Quantenoptik, Garching
- Julius-Maximilians-Universität Würzburg
- Universität Bremen
- Heinrich-Heine-Universität Düsseldorf
- **Universität Ulm**
- Humboldt-Universität zu Berlin
- **Universität Kassel**
- **Johannes Gutenberg-Universität Mainz**
- **Karlsruher Institut für Technologie**
- Ludwig-Maximilians-Universität München

https://qlinkx.de/

ドイツにおける量子中継ネットワーク関連プロジェクト

- Quantum Repeater consortium project
  - ~20 researchers collaborate for building QR
  - 15 M EUR for 3 years for ~20 groups
  - https://qlinkx.de/

- EU Quantum Technology Flagship
  - 1 Billion EUR for 10 yeas
  - Includes Quantum Repeater https://qt.eu/

- Quantera (←Qutega)
  - European initiative but funding comes from the individual country
  - 2017: 34 M EUR, 2019 20M EUR
  - https://www.quantera.eu/

- Federal German program on Quantum technologies
  - 650 M EUR for 4 years
  - https://www.quantentechnologien.de/

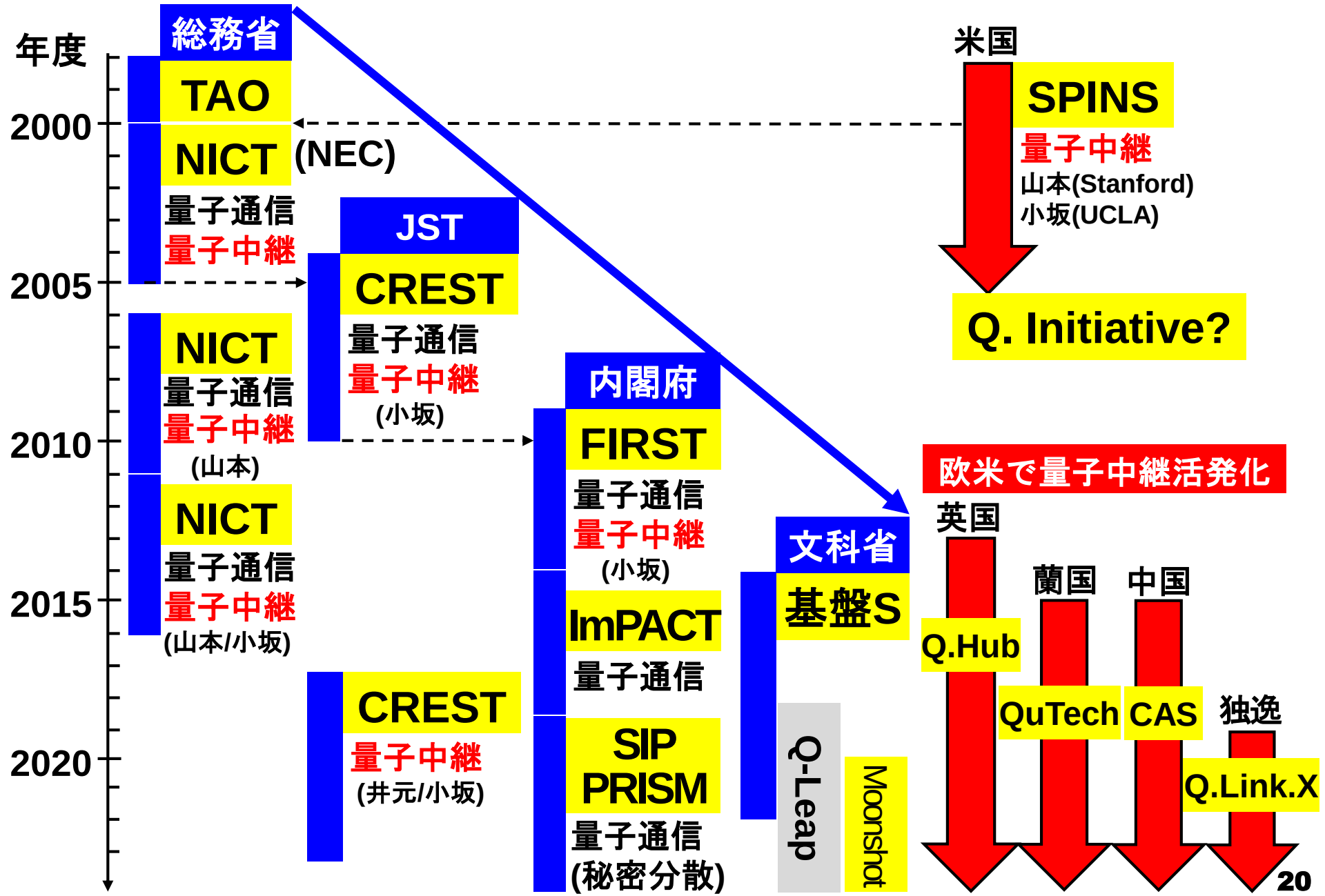
ドイツ版CREST？

- Junior research groups funded in the framework of the federal program
  - 10 Groups with funding 2.5 - 4.5 M EUR per project for 5 years

https://www.photonikforschung.de/projekte/quantentechnologien/foerdermassnahme/quantum-futur.html **ドイツ版さきがけ？**

Kai Mueller氏 (TU München)より

量子通信・量子中継 関連プロジェクトの推移



量子中継ネットワークのロードマップ

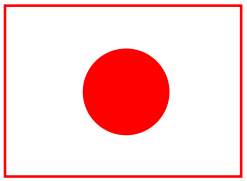
NICT（情報通信機構）ホームページより

量子暗号装置サプライヤー

米国調査会社インサイドクァンタムテクノロジー社報告書より

Approach to Profiling
ID Quantique
MagiQ Technologies
NTT
QuintessenceLabs
Nucrypt
Oki Electric
IBM
Raytheon
SK Telecom
Toshiba
Universal Quantum Devices
ZTE

ABB (Acquired Keymile)
Nokia
KPN
Qubitekk
Post Quantum
QuantumXchange
SeQureNet
Anhui Qasky
KETS quantum Security
Fujitsu
Mitsubishi
QinetiQ
NEC(本リストにはない？)



http://quantum-internet.team/

QUANTUM INTERNET ALLIANCE

The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth

LEARN MORE CONTACT

Leading actors from industry

CMS elementsix EXPERTS IN POSITIONING UQUANS MYCRYOFIRM Cryodevices & Consulting SAP

SURF SARA Swabian Instruments TNO innovation for life TOPTICA PHOTONICS VERIQLOUD

ABN-AMRO amsix le cnam i2cat IDQ

kpn QuantiCor RIPE NCC SURF NET TOSHIBA Leading Innovation TOYOTA

AUSTRIAN ACADEMY OF SCIENCES - IQOQI

CNRS

ICFO

INSTITUTO DE TELECOMUNICAÇÕES

MAX PLANCK INSTITUTE OF QUANTUM OPTICS

NIELS BOHR INSTITUTE – UNIVERSITY OF COPENHAGEN

QUTECH – TU DELFT

SORBONNE UNIVERSITY

UNIVERSITY OF BASEL

UNIVERSITY OF GENEVA

UNIVERSITY OF INNSBRUCK

UNIVERSITY OF STUTTGART

インターネットタスクフォースの動向

メルカリ R4D
永山翔太氏作成

- Internet Engineering Task Force (IETF)
  - 古典インターネットの標準化組織（年3回ミーティング）
  - 右図のレイヤーを取り扱う
  - セキュリティ部門が量子計算対策

  https://datatracker.ietf.org/meeting/102/materials/agenda-102-ipsecme-02
- Internet Research Task Force (IRTF)
  - 標準化にはまだ至らないレベルの技術を取り扱う
  - Quantum Internet Research Group (proposed)

  https://www.irtf.org/mailman/listinfo/qirg
- RIPE NCC（Réseaux IP Européens Network Coordination Centre）
  - インターネットレジストリ：欧州のIPアドレス管理
  - TU Delftと協力して量子インターネット
  - 2020年までに欧州4都市を量子インターネットで接続

  https://labs.ripe.net/Members/becha/introduction-to-the-quantum-internet
  - 量子インターネットの運用や使途までターゲット
  - 量子インターネットハッカソン

  https://labs.ripe.net/Members/becha/join-the-quantum-internet-hackathon-2018
- BBN Technologies
  - 古典インターネットのパケット通信開発に大きな貢献
  - 量子インターネットのネットワークレイヤーも数年前から

  https://arxiv.org/pdf/1708.07142.pdf

TCP/IP群

アプリケーション層

BGP - DHCP - DNS - FTP - HTTP - IMAP - IRC - LDAP - MGCP - NNTP - NTP - SNTP - TIME - POP - RIP - ONC RPC - RTP - SIP - SMTP - SNMP - SSH - Telnet - TFTP - TLS/SSL - XMPP
カテゴリ

トランスポート層

TCP - UDP - DCCP - SCTP - RSVP
カテゴリ

インターネット層

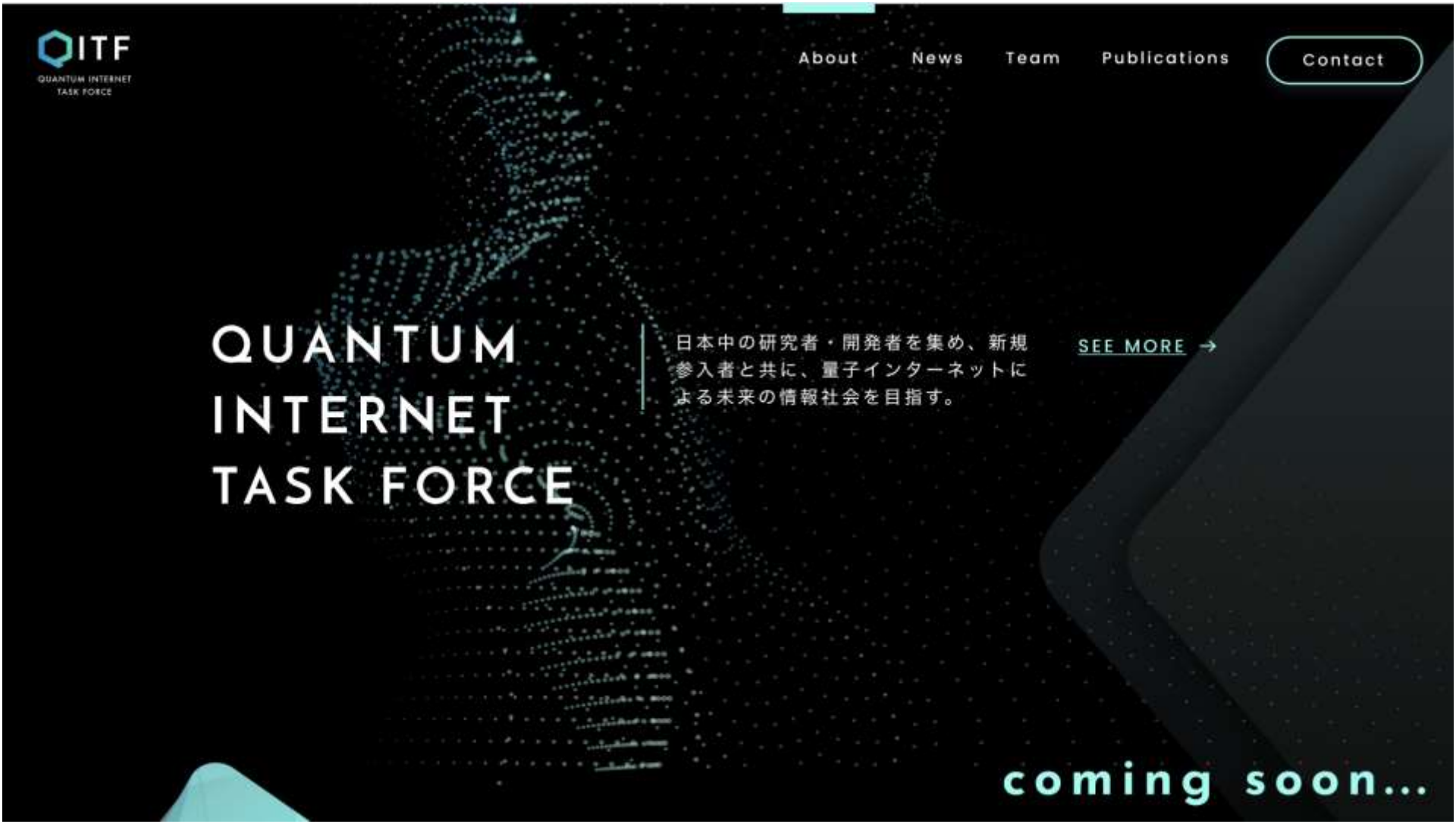
IP (IPv4、IPv6) - ICMP - ICMPv6 - NDP - IGMP - IPsec
カテゴリ

リンク層

ARP - OSPF - SPB - トンネリング (L2TP) - PPP - MAC （イーサネット、IEEE 802.11、DSL、ISDN）
カテゴリ

量子インターネットタスクフォース

メルカリ R4D
永山翔太氏作成



まとめ

- 現在研究されている量子通信ネットワーク（第一世代）は長距離の絶対安全性を保障しない。
- これを保障するためには、量子中継ネットワーク（第三世代）の開発が不可欠である。
- 量子中継器は光子と量子メモリーの間の量子メディア変換を行う小型の量子コンピュータである。
- 発光と吸収だけで量子中継ネットワークを形成。