4-6　衛星量子鍵配送に向けた地上-衛星間における偏光特性測定実験

4-6 Experimental Results of Polarization Characteristics Measurements through Satellite-to-Ground Propagation Paths toward Satellite Quantum Key Distribution

豊嶋守生　竹中秀樹　荘司洋三　高山佳久　小山善貞　國森裕生
TOYOSHIMA Morio, TAKENAKA Hideki, SHOJI Yozo, TAKAYAMA Yoshihisa, KOYAMA Yoshisada, and KUNIMORI Hiroo

要旨

宇宙空間からレーザ光源を用いた偏光特性の測定実験が、宇宙-地上間の大気伝搬路において行われた。衛星は日本製のレーザ通信機器を搭載した衛星と NICT の光地上局が用いられ、衛星から送信されたレーザビームのストークスパラメータと偏光度が測定された。結果として、宇宙-地上間の大気を通過したレーザ光の偏光は、rms 誤差で 1.6° 以下であり、偏光度は 99.4 ± 4.4%であった。本測定結果は、衛星を介した量子鍵配送の回線計算に貢献し、将来、量子暗号を広域展開するのに有益な結果である。

The polarization characteristics through space-to-ground atmospheric transmission paths were measured by using a laser source in orbit. An existing Japanese laser communication satellite and the NICT's optical ground station were used to measure Stokes parameters and the degree of polarization of the laser beam transmitted from the satellite. As a result, the polarization was preserved within an rms error of 1.6°, and the degree of polarization was 99.4±4.4% through the space-to-ground atmosphere. These results contribute to the link estimation for quantum key distribution via satellites and provide the potential for enhancements in quantum cryptography worldwide in the future.

[キーワード]
大気伝搬，レーザビーム伝送，偏光，空間光通信，量子鍵配送
Atmospheric propagation, Laser beam transmission, Polarization, Free-space optical communication, Quantum key distribution

1　まえがき

近年、大災害や事故の多発、世界的な感染症の流行、テロの頻発や国内の治安の悪化など、社会の安全・安心を脅かす危険や脅威が顕在化し始めている。科学技術は、社会的な価値を創出していく手段であり、知的な価値の創出、産業的な価値の創出と並んで、これらの危険や脅威に対処し社会の安全・安心を確保する要請に応えるもので、近年特に重要となっていきている [1]。情報通信技術では、情報漏えいや不正アクセスなどを防止する情報セキュリティ技術の要請が高まっており、盗聴技術が高度化する中で暗号技術は益々重要になってきている。

光や電子の量子効果を直接制御することで従来にはない革新的な性能を実現する量子情報通信技術が近年注目されている。盗聴を完全に見破る量子暗号や [2][3]、量子もつれ現象を使った遠距離での量子テレポーテーション [4]、従来の通信容量のシャノン限界を超える符号化技術等 [5]、新しい原理が実証され、実用化に向けた研究が加速している。既にファイバベースの商用では、実際

の量子暗号装置として、スイス Id Quantique 社製品の Cerberis、Vectis および Clavis、米国 MagiQ Technologies 社製品の MAGIQ QPN SECURITY GATEWAY 7505、フランス Smart Quantum 社製品の SQBox など、ベンチャー企業数社から販売されるに至っている [6]-[8]。スイスでは、2007 年 10 月に行われたジュネーブ市の選挙において、インターネット投票で既に量子鍵配送が採用されている [9]。これらは、量子鍵配送（QKD）技術が実用領域に入ってきたことを示している。

量子鍵配送は、現状、光ファイバでは 100 km 程度の距離の伝送が限界であり、それより遠距離になると、受信器の雑音やファイバ中の散乱光の雑音、また偏光を用いる場合には非線形性等の影響により、中継なしにそれ以上遠方へ送ることができない。しかし、自由空間においては空間的な損失はあるが、非線形要因がないため遠方への伝送には理想的な媒体である。これが宇宙において量子暗号が期待される所以である [10][11]。よって、将来の宇宙応用のため、衛星量子鍵配送の可能性を検証するのは重要である。低軌道周回衛星（LEO）は、通常時速 7 km/s の高速で軌道を周回しており、ドップラシフトの影響がある。これにより、衛星量子鍵配送には、ドップラシフトの存在下では、タイムビン方式よりも偏光を用いた伝送方式が最適な方法であると考えられるが、これまで宇宙-地上間で非偏光特性を精密に測定した例はなかった。

本稿では、衛星に搭載された偏光度（DOP）99.4％という高度に偏光したレーザ光源を用いて、世界で初めて宇宙-地上間における偏光特性を測定したので報告する。

2　光地上局を用いた地球規模のグローバル量子鍵配送

2.1　量子鍵配送の原理

量子鍵配送には、不確定性原理を利用した様々な量子状態を用いることが可能であるが、その中でも光の偏光を用いて行うことが利用しやすい。偏光を持った単一光子の検出について図 1 に示した。たとえば、図の左側で、縦偏光を持った単一光子が横偏光を通過させる偏光ビームスプリッタに入射した場合、“A”検出器ではいつも光ることになるが、“B”検出器では光らない。一方、図の右側で、斜め θ の角度で偏光した単一光子が、偏光ビームスプリッタを通過した場合、“A”検出器では $\sin^2\theta$ の確率で光り、“B”検出器では $\cos^2\theta$ の確率で光ることになる。ただし、単一光子なので両方同時には受からないことと、かつ、受信後にはどちらの偏光だったかは断定できない。つまり、以下のことが言える。

- 縦に直交した偏光は区別できる。
- 斜めに直交した偏光は区別できない（全くランダム）。
- 測定後、どちらの偏光だったかの情報は光子には残っていない。

量子鍵配送は、この全くランダムになる性質を利用して行っている。図 2 に BB84 方式での鍵交換の方法を示す。送信者（Alice）は、送りたい情報ビット（Original bits）を、縦と斜めの 2 つ

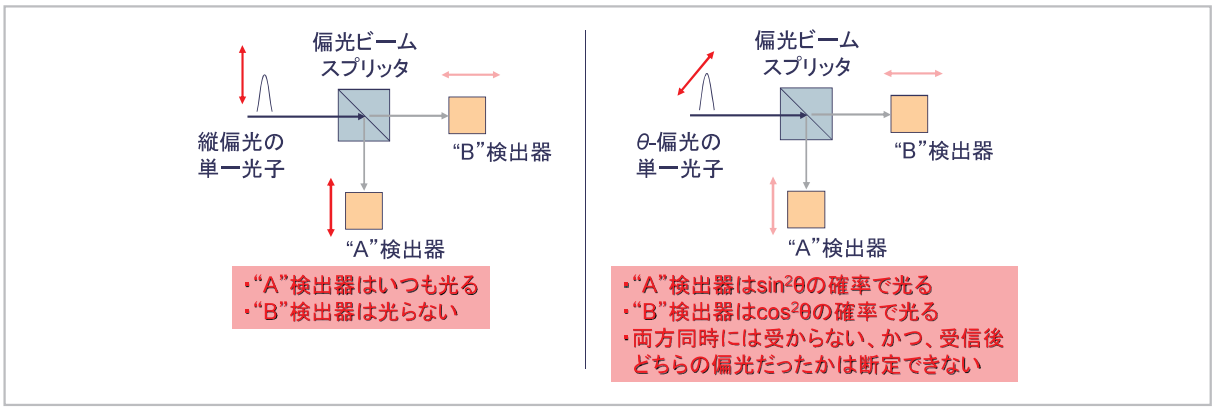

図 1　偏光を持った単一光子の検出

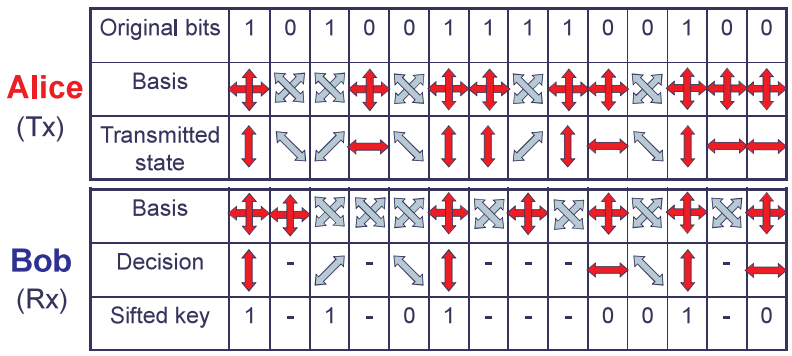

図２　BB84 方式による鍵の生成

の偏光基底（Basis）を選択して、情報（Transmitted state）を送信する。その際に、受信者（Bob）は、縦と斜めの２つの偏光基底（Basis）をランダムに選択して光検出器で受信し結果（Decision）を得る。一通り受信した後で、Alice と Bob で選んだ偏光基底をお互いに公衆回線で確認して同じものだけを選ぶ。この時、情報交換したのは縦か斜めの偏光基底の状態だけで、情報ビットそのものは情報交換していないため、偏光基底の情報だけでは盗聴できない。こうして得られた情報ビットを、ふるい鍵（Sifted key）と呼んでおり、Alice と Bob で鍵の共有ができる。もし、Bob が受け取る前に盗聴されたとしても、盗聴者 Eve が異なる偏光基底で読み取った値はランダムになってしまうため、Eve が信号をコピーして再送したとしても、Bob 側でのビット誤り率の増加によって盗聴が判明することになる。

2.2　任意の２つの地上局を用いた量子鍵配送

任意の２つの地上局を用いた量子鍵配送・共有実験は、地球規模で図３に示す手順で実現可能である。

1）衛星から量子鍵 α を量子もつれにより生成・配送し、地上局 A で量子鍵 α を保存する。
2）地上局 B の上空で、衛星から量子鍵 β を生成・配送し、地上局 B で量子鍵 β を保存する。
3）衛星では量子鍵 $\gamma = \alpha \mathrm{XOR} \beta$ を算出し通常の通信回線で両ユーザに配送する。（XOR は排他的論理和で、γ は盗聴されてもよい）

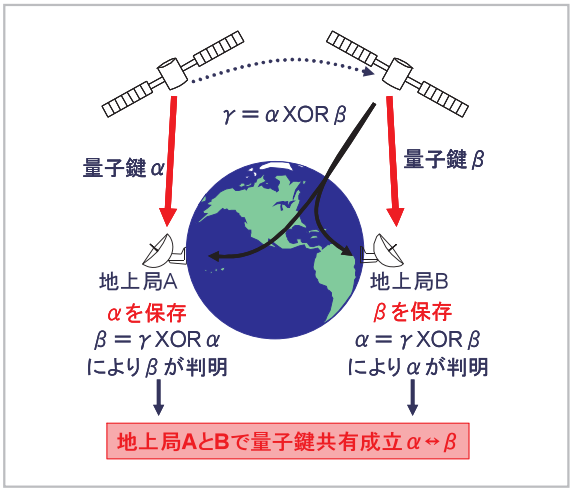

図３　任意の２つの地上局を用いた量子鍵配送

4）それぞれの地上局で自分の量子鍵と γ を XOR することで相手の量子鍵を共有できる。

任意の２つの地上局を用いた量子鍵配送・共有実験は、例えば、ヨーロッパで量子鍵を衛星に送信し、地球の反対側の日本で下ろすことによりグローバルな量子鍵配送が可能となる。ファイバでは現状実現できない長距離伝送が可能な宇宙量子暗号通信において、地球規模の量子鍵配送が可能であるということは、将来の応用に重要な意味を持つと考えられる。

3　地上–衛星間光地上局通信実験の構成

3.1　実験概要

情報通信研究機構（NICT）では、宇宙空間にある人工のレーザ光源を用いて、偏光特性を測定

した。偏光測定は、光衛星間通信実験衛星（OICETS、和名「きらり」）を用いて行われた[12]。「きらり」を用いたNICT光地上局通信実験（KODEN）は、2006年3、5、9月と、2008年10月から2009年2月にかけて、宇宙航空研究開発機構（JAXA）との共同研究により実施された。衛星はJAXAにより事前に送信されたストアコマンドにより自動制御される。東京都小金井市に設置された光地上局は、NICTにより運用された。衛星搭載の光通信機器は、26 cm直径のカセグレン型の望遠鏡を有している。1000 km離れた衛星からのレーザビームは、波長847 nmの波長をもち、ビーム広がり角は約6 μradであり、地上でのビームサイズが6 m程度にしかならない。

初期のフェーズ1–3の実験後、NICTでは将来の衛星量子鍵配送のためには、上層大気を通過する際、氷粒等が偏光に影響を与えることが懸念され[13][14]、その偏光特性を測定することが重要であると考えた。そこで、NICTではKODEN実験を再開し、宇宙–地上間大気伝搬路における偏光特性の確認をフェーズ4の実験として2008年10月から2009年2月まで実施した。

3.2 偏光測定システム

図4にNICT光地上局における偏光測定実験の構成を示す。ポラリメータは、1.5 mの主望遠鏡に平行に取り付けられた。受信電力、ストークスパラメータ、偏光度（DOP）等のデータが、1.5 cmの開口径を持つビームエキスパンダを通して測定され、10 Hzのサンプリングレートで記録される。用いたポラリメータの測定可能範囲は、受信電力範囲が－60 dBmから＋10 dBmであり、規格化したストークスパラメータの測定精度は0.005、DOPの測定精度は±0.5％以下であり、波長範囲は700～1000 nmである。後方散乱等の背景光の影響については、ポラリメータの開口がアップリンクビームとは別光学系であるため、影響は認められなかった。

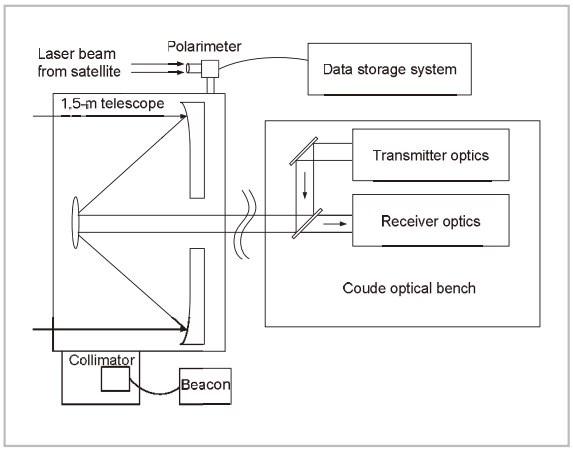

図4 NICT光地上局における偏光測定系の構成

3.3 衛星打ち上げ前の地上試験における偏光特性

「きらり」搭載の半導体レーザの偏光特性は、熱真空試験において測定されている[15]。レーザビームの偏光特性の測定結果は、光学分野の視点からは右旋偏波（$\mathrm{RHCP}|_{\mathrm{Optical}}$）であり、DOPは99.4％で、非偏光度は0.49％以下であった。偏光の定義として、ストークスパラメータが（S0, S1, S2, S3）=（1, 0, 0, 1）の時に右旋偏波$\mathrm{RHCP}|_{\mathrm{Optical}}$と定義されている[16]。空間レーザ通信においては、強い送信光から非常に弱い受信光をアイソレーションするために偏光分離が用いられ、通信機器の姿勢角度によらず1/4波長板1枚で直行する偏光に分離できるため、通信には通常円偏光が用いられる。IEEEによる定義を用いる場合、光学分野での円偏光の定義はIEEEの定義と正反対になる[17]。RF信号に対する左旋偏波（$\mathrm{LHCP}|_{\mathrm{RF}}$）は、固定した観測面を後方から見たときに、反時計回りの電磁界の回転方向と定義される。この定義はRFの衛星通信では共通であるが、光学分野における定義では、$\mathrm{LHCP}|_{\mathrm{RF}}$は$\mathrm{RHCP}|_{\mathrm{Optical}}$とみなされる。

4 衛星–地上大気伝搬路における偏光特性の測定結果

4.1 偏光度の測定結果

衛星を用いた偏光測定は、2008年10月から2009年2月にかけて実施された。そのうち、2008年12月23日の夜16:16:08–16:21:58（UTC）に行われた実験結果を示す。この実験における衛星–地上局間の最小距離は、最大仰角35.3°の時に959.8 kmであり、衛星仰角15°以上となる実験時間は350秒であった。天候は晴天で雲は無く、

測定されたシンチレーションインデックスは、衛星仰角により 0.05 から 0.4 まで変化が見られた。DOP とその rms 誤差は 99.4 ± 4.4％と測定された。測定誤差± 4.4％は、偏光測定器で測定した DOP 測定値の変動成分を表しており、信号変動による測定誤差が主要因であると考えられる。

4.2　ストークスパラメータの測定結果

図 5 に（S1, S2, S3）のストークスパラメータを、ポアンカレ球上にプロットした偏光特性を示す。測定された rms 誤差は 3.2° 以下であり、ポアンカレ球上での 1 周は、偏光の角度としては 180° に相当するため rms 誤差は半分の 1.6° となる。従って、直行する偏光成分によるクロストークの誤差としては、tan（1.6°）＝ 0.028 により 2.8％が影響することになり、これが量子ビット誤り率（QBER）へ寄与する上限と見なすことができる。量子分野でのビット誤り率は、しばしば QBER と呼ばれ、安全性証明においては、通常、ビット誤り率は全て盗聴者 Eve の盗聴に起因するとみなされており、攻撃者の能力を多めにみつもる「安全サイドに倒す」仮定で用いられている。過去のファイバによる伝送では 100 km 程度が限界であり [18]、144 km の自由空間の大気中水平伝搬でのフィールド実験では、光学系の不完全性等により QBER として 4.8 ± 1％が報告されており [19]、本測定結果は様々な大気層の伝搬路であるにもかかわらず、小さく抑えられている。QBER の値として 11％が量子鍵配送を行える理論的な上限となっている [20]。よって、本偏光特性の測定結果は、大気の影響として実測値の観点から上限値を与える貴重な結果であると共に、回線解析の観点から衛星量子鍵配送におけるシステム設計へ貢献するものである。

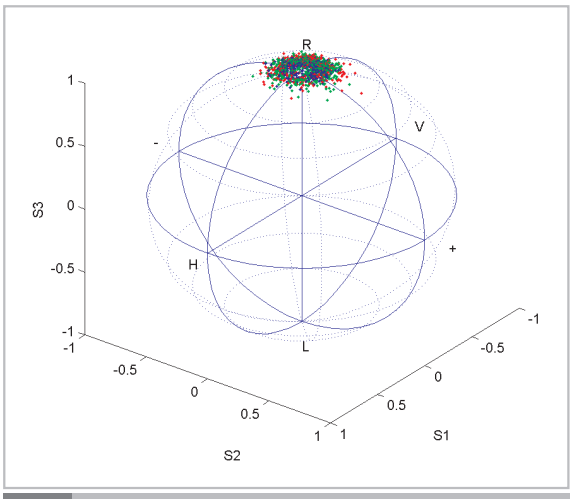

図 5　衛星からのダウンリンクレーザビームの偏光特性

青、緑、赤の点は、受信電力範囲が－ 39 dBm から－ 35 dBm、－ 41 dBm から－ 39 dBm、そして－ 43 dBm から－ 41 dBm をそれぞれ示している。

5　むすび

衛星搭載のレーザ光源により、宇宙–地上間の大気伝搬路における偏光特性の測定実験を行った。LEO 衛星と NICT 光地上局を用いて、衛星から送信されたレーザ光源の DOP とストークスパラメータの測定が行われた。結果として、宇宙–地上間の大気を通過したレーザ光の偏光は、rms 誤差で 1.6° 以下で保たれており、DOP は 99.4 ± 4.4％であった。これらの測定は、大気の影響として実測値の観点から上限値を与える貴重な結果であると共に、回線解析の観点から衛星量子鍵配送におけるシステム設計へ貢献し、将来、量子暗号を広域展開するのに有益な結果である。

謝辞

本実験を遂行するに当たりご協力いただいた、宇宙航空研究開発機構、NEC 東芝スペースシステム㈱、宇宙技術開発㈱の関係各位に深く感謝する次第である。

参考文献

1　Ministry of Education, Culture, Sports, Science and Technology (MEXT) “Report on science and technology policy on contributing the secure and safety society,” 2004. (in Japanese) http://www.mext.go.jp/a_menu/kagaku/anzen/houkoku/04042302/all.pdf

2 C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proc. International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984.

3 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, pp. 145–195, 2002.

4 D. Bouwmeester, A. Ekert, and A. Zeilinger, ed., "The Physics of Quantum Information," Springer, New York, 2000.

5 M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, "Exceeding classical capacity limit in quantum optical channel," Phys. Rev. Lett. 90, 16, 167906, 2003.

6 Specification sheet of Cerberis, http://www.idquantique.com/products/files/Cerberis-specs.pdf

7 Data sheet of MAGIQ QPN 8505, http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf

8 Data sheet of SQBox Defender, http://www.smartquantum.com/IMG/pdf/SQBox_Defender_Datasheet-3.pdf

9 M. E. Peck, "Geneva Vote Will Use Quantum Cryptography," http://spectrum.ieee.org/oct07/5634

10 R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. 4, pp. 43.1–43.14, 2002.

11 R. Hughes and J. Nordholt, "Refining Quantum Cryptography," Science 16, pp. 1584–1586, Sept. 2011. http://www.sciencemag.org/content/333/6049/1584.full.pdf

12 M. Toyoshima, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, W. Klaus, M. Toyoda, H. Kunimori, T. Jono, Y. Takayama, and K. Arai, "Ground-to-satellite laser communication experiments," IEEE AES Magazine 23, 8, pp. 10–18, 2008.

13 S. R. Pal and A. I. Carswell, "The Polarization Characteristics of Lidar Scattering from Snow and Ice Crystals in the Atmosphere," Journal of Applied Meteorology 16, pp. 70–80, 1977.

14 Y. A. Kravtsov, "New effects in wave propagation and scattering in random media (a mini review)," Applied Optics 32, 15, pp. 2681–2691, 1993.

15 M. Toyoshima, Yamakawa, T. Yamawaki, and K. Arai, "Reconfirmation of the optical performances of the laser communications terminal onboard the OICETS satellite," Acta Astronautica 55, 3-9, pp. 261–269, 2004.

16 M. Born and E. Wolf, "Principles of Optics-7th ed.," Cambridge University Press, London, 1999.

17 D. Roddy, "Satellite communications-2nd ed.," McGraw-Hill, New York, 1989.

18 N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys., 74, 145-195, 2002.

19 R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B.Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement based quantum communication over 144 km," Nature Physics 3, pp. 481–486, 2007.

20 N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems," Phys. Rev. Let. 88, 127902, pp. 1–4, 2002.

（平成 24 年 3 月 14 日 採録）

豊嶋守生（とよしまもりお）
ワイヤレスネットワーク研究所
宇宙通信システム研究室室長
博士（工学）
衛星通信、大気ゆらぎ、レーザ通信、量子暗号
morio@nict.go.jp

竹中秀樹（たけなかひでき）
ワイヤレスネットワーク研究所
宇宙通信システム研究室有期技術員
衛星通信、レーザ通信
take@nict.go.jp

荘司洋三（しょうじようぞう）
ネットワーク研究本部
ネットワークシステム総合研究室
プランニングマネージャー
博士（工学）
ミリ波通信システム、光電波融合通信システム、コヒーレント光通信システム、有無線仮想化
shoji@nict.go.jp

高山佳久（たかやまよしひさ）
ワイヤレスネットワーク研究所
宇宙通信システム研究室主任研究員
博士（工学）
非線形光学、位相共役光学、フォトニック結晶、電磁波解析、宇宙光通信
takayama@nict.go.jp

小山善貞（こやまよしさだ）
ワイヤレスネットワーク研究所
宇宙通信システム研究室専攻研究員
光通信、衛星搭載機器
koyama.yoshisada@nict.go.jp

國森裕生（くにもりひろお）
ワイヤレスネットワーク研究所
宇宙通信システム研究室主任研究員
衛星レーザ測距
kuni@nict.go.jp