様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １７ 日現在

機関番号：８２６３６
研究種目：若手研究
研究期間：2019～2020
課題番号：１９Ｋ１４９９２

研究課題名（和文）安全な光空間通信のための大気ゆらぎ情報を活用した漏えい情報量評価

研究課題名（英文）Leaked information estimation based on atmospheric turbulence toward secure free-space optical communications

研究代表者
遠藤　寛之（Endo, Hiroyuki）

国立研究開発法人情報通信研究機構・未来ICT研究所量子ICT先端開発センター・研究員

研究者番号：５０８０９７０４

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：　レーザ光やLEDによる光空間通信は、搬送波ビームの広がりが狭く、送受信者間の見通しを確保した上で行われるため、電波無線通信よりも高い安全性を持つとされている。しかし、大気ゆらぎの影響に引き起こされる、見通し外の盗聴者への情報漏えいが安全性の問題として上げられる。
　本研究開発では、そのような大気揺らぎによる情報漏えいを予測するための技術の開発を目指して、大気ゆらぎを測定するための装置を開発し、実フィールド環境において大気ゆらぎと漏えい情報量を定量的に関係付けるための実証実験を行った。併せて、大気ゆらぎの情報に応じて、秘匿通信におけるパラメータ最適化を行う技術の提案と実証を行った。

研究成果の学術的意義や社会的意義
大気ゆらぎが光空間通信における情報漏えいが起こることは、提案者らはフィールド実験により検証していたが、大気ゆらぎの強度との関係の定量化は、大気ゆらぎがランダムな現象であることから困難なものであった。本研究では大気揺らぎを測定する装置を用いることにより、この関係が定量化できる可能性を見出すことができた。これは、情報漏えいと大気ゆらぎの関係のメカニズムを理解する上で重要な知見を与えるものである。この研究が発展していくことにより、電波無線通信では賄いきれない通信の需要に応えるために研究されている光空間通信の安全性をより高めることが可能になる。

研究成果の概要（英文）：Free-space optical communications based on laser light or LED are considered to have higher security than radio-wave counterparts because the divergence of the carrier wave beam is narrower and thus the line-of-sight between the transmitter and the receiver should be secured. However, information leakage to the eavesdropper outside the line-of-sight caused by the influence of atmospheric fluctuation is an urgent security problem.
In this research and development, to develop a technology for predicting information leakage due to such atmospheric fluctuations, we developed a device for measuring atmospheric fluctuations, and demonstrated the real-field experiment to quantitatively relate the atmospheric fluctuations and the amount of information leakage. In addition, we propose and demonstrate a technology for parameter optimization in secure communication according to the information of atmospheric fluctuations.

研究分野：光空間通信

キーワード：光空間通信　物理レイヤ暗号　大気ゆらぎ　情報理論的安全性

１．研究開始当初の背景

近年における映像技術の飛躍的な向上やコンテンツサービスの拡大により、高速・大容量な通信への需要が高まっている。しかし、使用できる周波数が逼迫しつつある電波無線通信のみではその需要に応えることは難しいことから、より高周波帯にあるレーザ光や LED による光空間通信に注目が集まっている。

電波よりも高周波帯にあることから、レーザ光や LED は空間中を狭い広がりで伝搬する。そのため、送信者(アリス)と受信者(ボブ)は通信の際に互いの見通しをカメラなどの手段で確保する必要がある。このことは一方で、盗聴者(イブ)による通信路中の企ても発見しやすいことも意味している。すなわち、光空間通信路では、イブの盗聴能力や攻撃手段にリーズナブルな制限を与えることができ、安全性の高い通信を実現することができる。提案者はこれまで、以上の光空間通信の見通し通信という特徴を用いることで、どのような計算機でも解読できない秘密通信や暗号鍵の共有を可能にする、物理レイヤ暗号という手法を研究してきた。

しかし、大気中を伝搬するレーザ光は、風や気温変化によって生じる大気中の屈折率のゆらぎの影響により、その広がりや方向に経時変化が生じる。このようないわゆる大気ゆらぎの影響は、1 対 1 の光空間通信の性能を大きく劣化させることが知られているが、深刻な情報漏えいも引き起こすことも提案者らの過去の研究より明らかになっている【H. Endo et al. (2016)】。このような大気ゆらぎによる情報漏えいを防ぐには、ボブ側及びイブ側における大気ゆらぎに関する情報(通信路状態情報(CSI: Channel State Information))と漏えい情報を結びつけるための技術が必要となる。

２．研究の目的

本研究の目的を、図 1 に示すような衛星―地上間の光空間通信を例として説明する。人工衛星(アリス)はデータ送信のためのダウンリンク光を地上局(ボブ)に照射する。一方、ボブは位置補足のためのビーコン光をアリスへと照射する。このダウンリンク光とビーコン光は同一経路を伝搬するため、両者が経験する大気ゆらぎに相関が現れることが期待できる。そこで、衛星は搭載センサでビーコン光を測定し、そこからボブ側の CSI に関する情報を推定する。

さらに、地上局の周囲は十分な警備により安全性が保たれていると仮定し、その警備エリアの境界上にダウンリンク光から漏れるパワーを推定するためのプローブ系を配置する。このプローブ系の測定結果から、ビーム裾に潜んでいるイブに漏えいする情報量の上界を推定する。しかし、このようなプローブ系を用意できない状況も考えられる。そこで、アリスが推定した CSI から、この系に漏えいした情報量を予測する手法も開発する。以上の CSI の情報、そしてそこから推定される漏えい情報量を元に、アリスはビームの強度や角度を調整し、秘匿性を向上させることが可能になる。

以上のようなシステム実現に向けた要素技術を開発し、そのフィールド実証を申請者がこれまで物理レイヤ暗号の実証に用いてきた光空間通信テストベッドなどで行うことを本課題の目的とする。

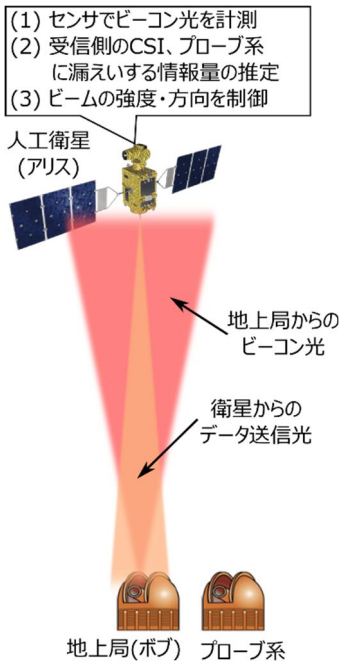

図１．本研究の概念図。

３．研究の方法

図１に示すようなシステム実現に向けた要素技術として、DIMM(Differential Image Motion Monitor)センサと呼ばれる装置を開発し、実フィールド環境において DIMM センサから得られた CSI に関する情報と漏えい情報量を関連付け、その情報に応じて秘匿通信におけるパラメータ最適化を行う技術を提案し、フィールド試験を実施する。

DIMM センサの概要図を図 2 に示す。この装置の特徴として、非常に簡素な装置構成で構築可能であり、様々なプラットフォームに実装可能であることが挙げられる。このセンサは、カメラ、レンズ、ウェッジプレート、複数の開口を持つマスクからなる。マスクの開口を通過した光が、ウェッジプレートにより屈折され、カメラの焦点面において複数のスポットを形成する。そのスポットの重心位置の分散から大気ゆらぎの強度を求めることができる。今回は、実験に用いる波長(1,550nm)に合わせて赤外線カメラを用意した。この赤外線カメラに口径 20cm のカ

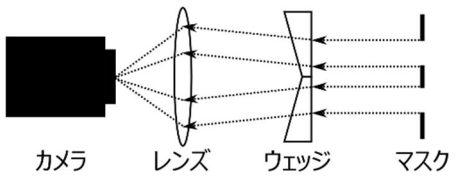

図 2.DIMM センサの概要図

セグレン式天体望遠鏡を取り付け、さらに望遠鏡の開口に図 3 に概要図を示すような、4 つの穴が十字型に配置されているマスクをはめ込む。本来、このマスクにはウェッジプレートを取り付ける必要があるが、今回用意した赤外線カメラの素子サイズが小さく(横 4.51㎜×縦 2.88㎜)、市販品のウェッジプレートの角度(0.5 度)では偏向された光が素子外にフォーカスされてしまうことが判明した。そこで、過去の文献でも行われている【M. Panahi et al. (2020)】ように望遠鏡のフォーカスをあえてずらす方法を採用した。なお、この手法ではスポットの象が大きく歪むことも明らかになったため、研究機関 2 年目の後半に、より素子数の大きい赤外線カメラ(横 6.4㎜×縦 5.12㎜)と、特注品のウェッジプレート(0.1 度)とを調達し、図 2 の概要図の DIMM 装置が実現可能になった。

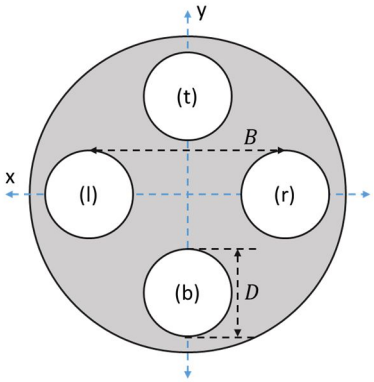

図 3.本研究開発で設計した DIMM マスクの概要図。

また、DIMM 装置で取得した動画を処理し、大気ゆらぎに関する情報を取得するためのソフトウェアも開発した。DIMM 装置からは、図 4 にスクリーンショットの一例を示すような動画を取得できる。開発したソフトウェアは、DIMM 装置が取得した動画を読み込み、マシンビジョンに特化した処理のライブラリである open CV を用いて各スポットの重心値(図 4 中の赤い点)を検出する。そして、縦及び横方向に相対するスポットの重心の分散値から、以下の数式により、大気の屈折率が均一である領域のスケールであるフリードパラメータrを算出する。

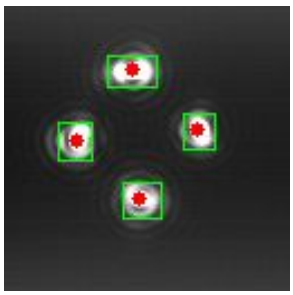
図 4.スポット動画のスクリーンショット。2020 年 7 月 8 日 13 時 10 分取得。

$$r = \frac{\frac{6}{\lambda^5}(\sigma_4^2)^{-\frac{3}{5}}}{B^{\frac{6}{5}}}\left[0.0424D^{-\frac{1}{3}} - 0.012B^{-\frac{1}{3}}\right]^{\frac{3}{5}}$$

ここで、λはレーザの波長、Dはマスク上の開口の直径、Bは縦及び横に相対する開口同士の距離である(図 3 参照)。また、σ_4^2は以下に定義する量の分散値である。

$$C_4 = -\frac{\left(t_x^{(r)} - t_x^{(l)}\right) + \left(t_y^{(t)} - t_y^{(b)}\right)}{4F_{\mathrm{tel}}B}$$

ここで、$t_x^{(r)}$、$t_x^{(l)}$、$t_x^{(t)}$、$t_x^{(b)}$は右、左、上、下のスポットの偏位、F_{tel}は望遠鏡の焦点距離である。

図 5．光空間通信テストベッドの鳥瞰図

以上の装置を、図 5 に示す、光空間通信テストベッドに実装した。この光空間通信テストベッドは、電気通信大学(東京都調布市)に設置された全天候型ドーム内のレーザ送信機(アリス)と、情報通信研究機構(東京都小金井市)に設置された 3 つの受信機からなっている。電気通信大学と情報通信研究機構は 7.8㎞ 離れており、これらの送受信機により 7.8㎞ の光空間通信リンクを形成している。この 7.8㎞ という距離は地球を取り巻く大気の厚さと同等であり、本研究課題で実証するシステムが将来的にその応用を目指す衛星―地上間の光空間通信路を模擬する上で適したものとなっている。

NICT が所有する 6 階建てビルの 6 階に、ボブ 1 とボブ 2 と呼ばれる 2 台の受信システムを

設置している。今回の実験ではこれらボブのすぐ後方に DIMM 装置を設置している。一方、同じビルの屋上には v-イブ(virtual-イブ)と呼ばれているコンテナ型の受信システムが設置されている。これは、図 1 に示したプローブ系の役割を担う。なお、v-イブとボブは直線距離にして約 12m 離れている。

アリスは中心波長 1550nm の CW レーザを光源として用いて、予め物理乱数源から生成しておいた物理乱数列を NRZ(Non-Return-to-Zero)のオンオフ強度変調で伝送する。シグナル光はシングルモードファイバ(SMF)により光増幅器に入力され、100mW に増幅された後に、ファイバーコリメータによって直径約 5.5mm のビームに拡大される。NICT 側の 3 つのターミナルはほぼ同一の構成である。これらのターミナルは、半値全幅約 7.8m に広がったビームの一部分をカセグレン式望遠鏡で集光する。なお、ボブの望遠鏡は口径Dが 111mm、焦点距離fが 800mm である一方、イブの望遠鏡は直径Dが 100mm、焦点距離fが 2000mm である。光信号は径 200um のマルチモードファイバ(MMF)にカップルされ、光検出器(ボブ側：PIN フォトダイオード(PIN PD)検出器、v-イブ側:アバランシェフォトダイオード(APD)検出器)で計測される。検出器からの信号は増幅された後、オシロスコープ(サンプリングレート 50MHz、ローパスフィルター(LPF) による 20MHz の帯域制限)により A/D 変換される。収録されたデータは PC に送られ、そこでカットオフ周波数 6MHz の LPF 処理後、クロック信号再生処理(CDR)、フレーム同期処理などのオフライン信号処理を実施し、乱数ビット列の復調を完了する。

4．研究成果

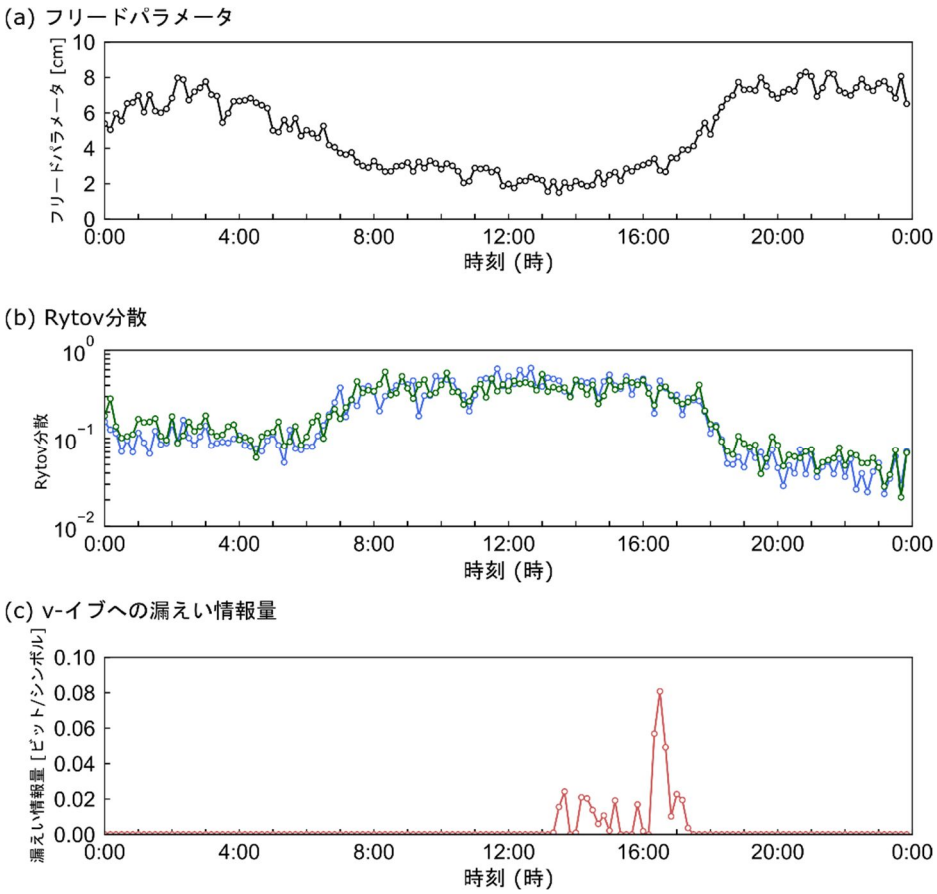

図 6．2020 年 8 月 23 日に実施した伝送実験結果。図(b)の Rytov 分散の曲線について、青色はボブ 1、緑色はボブ 2 で取得されたデータに基づいて計算されている。

2020 年度は新型コロナ禍の影響を受けながらも、8 月中に数週間の伝送実験を実施し、大量のデータ蓄積を行った。図 6 に 2020 年 8 月 23 日に取得した結果の一例を示す。この実験では、光空間通信テストベッドのアリスから乱数データを変調した光信号を 10Mbit 分伝送し、DIMM 装置によりフリードパラメータを測定し、ボブ 1 の受信強度のゆらぎから Rytov 分散と呼ばれる、やはり大気ゆらぎの指標として用いられる量を算出した。合わせて、v-イブが受信したデータから算出した漏えい情報量強度も示している。

図 6(a)にフリードパラメータ、(b)に Rytov 分散を示す。前者は大気の屈折率が均一な領域のスケールを表していることから、その値が大きいほど大気の状態は安定している。一方で後者はゆらぎのパラメータであるため小さいほど大気の状態は安定している。そのため、両者が反相関しているように見える今回の結果はリーズナブルな結果であると言える。両者のデータは、夜中

には大気の状態が安定している一方で、日中には大気の状態が不安定になっていることを示している。なお、7.8㎞という長距離のリンクに置いて、このようなデータを取得した例は少なく、貴重なデータであると言える。

また、図 6(c)漏えい情報量を示している。この結果からは 14 時頃から 18 時ごろにかけて、v-イブへの漏えい情報量が増加しており、情報漏えいが生じた可能性を示唆している。この時刻にはフリードパラメータや Rytov 分散が増加しているため、この情報漏えいが大気ゆらぎにより引き起こされている可能性は高い。一方で、14 時以前には、大気が不安定であるにも関わらず、漏えい情報量が 0 に近い。これは、熱によるビルや装置の伸縮や気象の変化など、複合的な理由が関与しているためと考えることができる。

大気ゆらぎと情報漏えいの関係は、大気ゆらぎが本質的にランダムな現象であることと、気象の変化などの様々な実環境データも関わってくることから、これまでは定量化が非常に困難であった。しかし、今回の結果は、それらの定量化の可能性を示すものであり、光空間通信の安全性の研究に重要な知見を与える。今後は、実証実験で取得した大量のデータを元に、情報漏えいが起こるメカニズムを明らかにしていくことが目標となる。

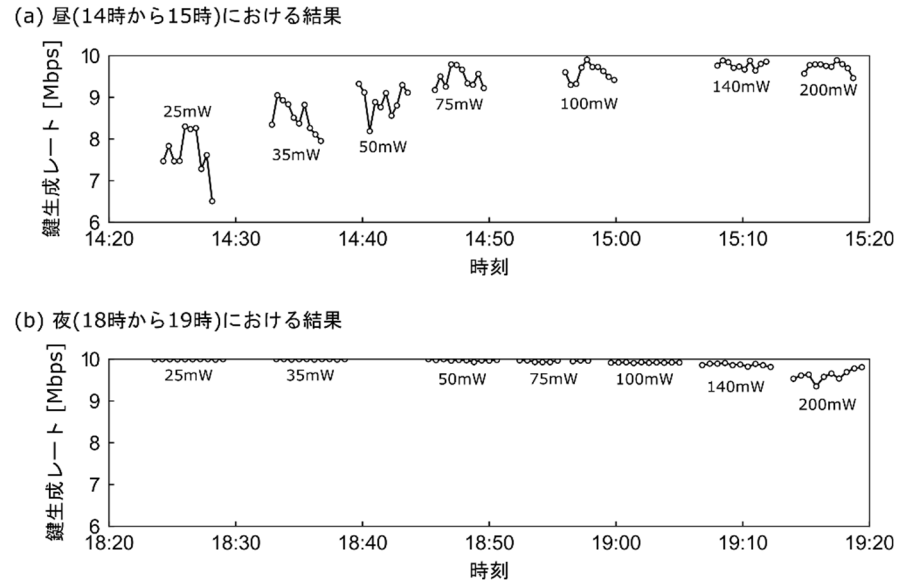

図 7．2020 年 9 月 11 日に実施した送信パワー変更実験の結果。

また、送信者が大気ゆらぎの状況を確認し、その状況に合わせてビームの強度などを最適化する機構の実証のために、アリスが照射するビームの強度を 25㎽から 200㎽の間で変化させた際の秘匿通信の性能変化を検証した。秘匿通信の性能は、物理レイヤ暗号による鍵生成レートにより測られる。この鍵生成レートは、アリス－ボブ間で誤りなしに受信可能な情報レートと、v-イブに漏えいしている情報量の差で定められる。今回の実験では送信レートが 10㎒z であるため、アリスとボブの間でほぼエラーフリーであり、情報漏えいが無視できる理想的な場合には、鍵生成レートは最大で 10㎅ps になる。

大気のゆらぎの影響を比較するため、大気が比較的に不安定になる 14 時から 15 時(図 7(a))と比較的に安定する 18 時から 19 時(図 7(b))における二つの時間帯で実験を実施した。昼の時間帯には、送信パワーを上げるほど鍵生成レートが向上していく。これは、大気の状態が不安定であることからボブと v-イブの両者ともポインティングエラーなどによる損失が大きく、アリスとボブの間の情報レートを向上させるために送信パワーを向上させても、致命的な情報漏えいが発生しないためであると考えられる。一方で、夜の時間帯ではこの傾向は逆転し、送信パワーを上げると鍵生成レートが減少していく。これは、大気の状態が安定になるため、ボブとイブの両者とも光が受信しやすい状況となるため、高い送信パワーが情報漏えいを引き起こすためであると考えられる。一方で、昼の時間帯よりも十分に低い送信パワーでもアリス－ボブ間で十分に高い情報レートでの通信が可能になるため、低い送信パワーでの通信が最適な結果となる。

以上の結果は、鍵生成レートを最大化するという意味での最適な送信パワーは大気ゆらぎの強度に依存していることを意味する。このことは、アリスは大気ゆらぎの情報から最適な送信パワーを推定し、適応的に変化させることで物理レイヤ暗号による秘匿通信を最適化する機構が構築可能であることを示唆している。この条件をより定量化し、AI のような予測手法と組み合わせることにより、新しい研究の展望が拓かれる。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Endo Hiroyuki、Fujiwara Mikio、Kitamura Mitsuo、Tsuzuki Orie、Shimizu Ryosuke、Takeoka Masahiro、Sasaki Masahide	４．巻 3
２．論文標題 Group key agreement over free-space optical links	５．発行年 2020年
３．雑誌名 OSA Continuum	６．最初と最後の頁 2525～2543
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OSAC.389853	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, and M Sasaki
２．発表標題 Free-space optical secret key agreement with post-selection based on channel state information
３．学会等名 Environmental Effects on Light Propagation and Adaptive Systems II（国際学会）
４．発表年 2019年

１．発表者名 H. Endo and M. Sasaki
２．発表標題 Secret Key Agreement for Satellite Laser Communications
３．学会等名 37th International Communications Satellite Systems Conference (ICSSC)（国際学会）
４．発表年 2019年

１．発表者名 遠藤寛之，佐々木雅英，
２．発表標題 衛星光通信に向けた物理レイヤ暗号
３．学会等名 第64回宇宙科学技術連合講演会
４．発表年 2020年

〔図書〕　計0件

〔出願〕　計3件

産業財産権の名称	発明者	権利者
秘密鍵共有方法及びシステム	遠藤 寛之，佐々木 雅英	情報通信研究機構
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2019-235286	2019年	国内

産業財産権の名称	発明者	権利者
秘密鍵共有システム及び秘密鍵共有方法	遠藤 寛之，佐々木 雅英	情報通信研究機構
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2020-012325	2020年	国内

産業財産権の名称	発明者	権利者
秘密鍵共有システム及び秘密鍵共有方法	遠藤 寛之，佐々木 雅英	情報通信研究機構
産業財産権の種類、番号	出願年	国内・外国の別
特許、PCT/JP2021/2129	2020年	外国

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関