PRODRONE®

SAN-ES

国立研究開発法人
情報通信研究機構

プレスリリース
平成 27 年 9 月 28 日

国立研究開発法人情報通信研究機構
株式会社プロドローン
株式会社サンエストレーディング

ドローンの通信の安全性を強化する技術を開発

～量子鍵配送ネットワークからドローンに暗号鍵を供給し、安全な飛行制御通信を実現～

【ポイント】

- ドローンと地上局間の制御通信をパケットごとに暗号化、情報漏えい等を完全防御
- 複数の地上局を量子鍵配送ネットワークで結び、ドローンを広域で飛行誘導する制御通信技術
- 複数地上局間での鍵配送を手渡しで行う飛行誘導システムを 2 年後に商品化する予定

国立研究開発法人情報通信研究機構（NICT、理事長: 坂内 正夫）は、株式会社プロドローン（プロドローン、代表取締役: 河野 雅一）及び株式会社サンエストレーディング（サンエストレーディング、代表取締役: 坂野 良行）と共同で、ドローン[*1] の飛行制御通信の安全性を強化する技術を開発しました。真性乱数[*2] を共通の暗号鍵としてドローンと地上局間で安全に共有し、制御通信をパケットごとに暗号化することで、制御の乗っ取りや情報漏えいを完全に防御します。さらに、複数の暗号鍵をドローンに搭載し、対となる暗号鍵を複数の地上局に量子鍵配送ネットワーク[*3] で配送することにより、複数の地上局間で安全に飛行制御を引き継ぎながら、ドローンを広域で飛行誘導するセキュア制御通信技術を開発し、その実証実験に成功しました。

上記技術の商品化については、乱数生成器を地上局に導入し、ユーザ・機器認証を経て暗号鍵をドローンに供給し、地上局間では手渡しで鍵配送を行う飛行誘導システムを 2 年後に予定しています。

本成果は、9 月 28 日（月）に一橋講堂にて開催される第 4 回 量子暗号・量子通信国際会議（UQCC 2015）にて発表します。

※ 本研究開発の一部は、総合科学技術会議・イノベーション会議により制度設計された革新的研究開発推進プログラム（ImPACT）の支援を受けています。

【背景】

回転翼を持つ小型無人航空機、いわゆるドローンの技術が急速に進歩し、空撮や測量、インフラ点検などの分野で利用が広がっています。一方で、飛行の安全性対策が喫緊の課題となっています。特に、ドローンの遠隔制御に使われる無線通信は、傍受や干渉、妨害の影響を受けやすく、通信の乗っ取りや情報漏えいなども懸念されています。しかし、現状、標準的な暗号化すら行われていないケースが多く、ドローンの制御通信における情報セキュリティ対策は十分ではありません。また、ドローンを無線通信で制御できるエリアにはまだ限界があるため、目視圏内で飛行させることが多く、広域での安全な飛行制御には、依然、多くの課題があります。特に、警備や国家安全保障関連分野では、ドローンと地上局間の制御通信の安全性とデータ通信の秘匿性を抜本的に高め、かつ、広域にわたって安全に飛行制御する技術が必須とされています。

【今回の成果】

ドローン制御通信において、制御の乗っ取りや情報漏えいを完全に防御するセキュア制御通信技術を開発しました。

ドローンの制御は、同装置の無線通信の代表的な方式の一つであるシリアル通信[*4] の制御信号（周波数 2.4GHz の電波信号）を、パケットごとに異なる真性乱数を用いて暗号化（ワンタイムパッド暗号化[*5]）して行いました（図 1 参照）。この暗号化は、真性乱数と制御信号パケットの単なる足し算で行い、従来の暗号化で用いていた複雑な関数や膨大な計算を必要としません。これにより、処理遅延のないセキュア制御通信を、低

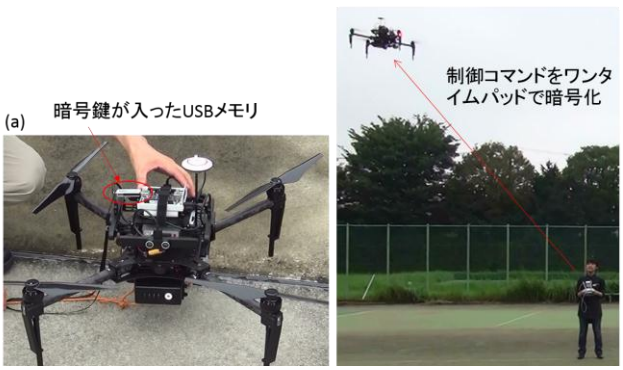


図 1 暗号鍵（真性乱数）の供給と
ワンタイムパッド暗号化による飛行制御

速処理でも小型かつ安価なデバイスで実現できます。

また、現在市販されている無線装置でのドローン制御距離は 1km 程度に制限されています。ドローンの運用範囲を拡大するためには、地上局間での制御の引継ぎが必要になります。今回開発したシステムでは、一度使った鍵は二度と使わないワンタイムパッド暗号化を用いていますので、複数の暗号鍵（真性乱数）をドローンに搭載し、対となる暗号鍵（真性乱数）をそれぞれの地上局に配送する必要があります。地上での暗号鍵の配送法には、(1)信頼できる宅配サービス等を利用した人手による配送（第一世代: 図 2a）、(2)量子鍵配送ネットワークによる自動配送（第二世代[*6]: 図 2b）があります。

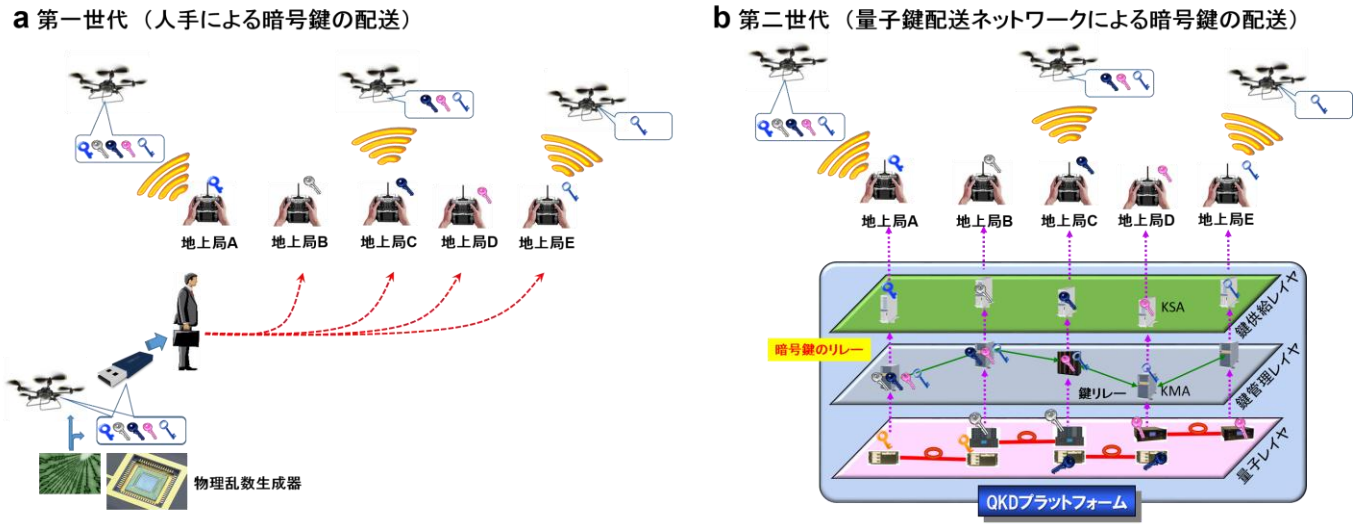


図 2 研究開発を進めているドローン広域セキュア制御通信システム

今回、2 つの飛行制御エリア A、B 間で安全に制御通信を引き継ぐ第一世代システムの実証実験に成功しました（図 3 参照）。さらに、NICT が管理運営する量子鍵配送（QKD）ネットワーク「東京 QKD ネットワーク」で配送された暗号鍵を 2 つの地上局に供給し、飛行制御を引き継ぐ第二世代の実証実験にも成功しました。今回の第二世代の実験では、ドローンの制御範囲を NICT 構内に限定していますが、将来の広域セキュア制御通信技術に必要な原理が実証されました。

図 3 異なる飛行制御エリア間での暗号化制御通信の引継ぎ

※ 今回の実験は、NICT 内において安全管理に関する審査を事前に経た上、NICT 敷地内テストフィールド及び研究棟屋上という場所に限定して、GPS 機能を用いた飛行区域制限やロープ締結などの手法によって運用の安全性を確保した状態で実施しました。

【今後の展望】

当開発チームは、地上での暗号鍵の配送に信頼できる宅配サービス等を利用し、通信を使わずに供給する第一世代システムを 2 年以内に商品化する予定です（図 2 参照）。

また、NICT 敷地内の東京量子鍵配送ネットワークにおいて第二世代システムの研究開発を継続していきます。

量子鍵配送ネットワークをドローンの運用に活用することで、実装上の制約が多いドローン上でも、簡易な方式によって極めて高い安全性を実現できるようになります。加えて、この広域セキュア制御通信技術を用いれば、複数の地上局とドローンから成るネットワークシステム上で、乗っ取りや情報漏えいを防ぎながら、動的に飛行エリアや経路の選択と制御を行うことも可能になります。

さらに、従来の電波による方式のほか、レーザー光を使った大容量かつ安全なデータ通信ネットワークを実現するための研究開発にも積極的に取り組んでいきます。

＜本件に関する発表学会＞

第 4 回 量子暗号・量子通信国際会議

The Fourth International Conference on Updating Quantum Cryptography and Communications (UQCC 2015)

会期: 2015 年 9 月 28 日（月） 9:30 - 12:30
会場: 一橋大学 一橋講堂（〒101-8439 東京都千代田区一ツ橋 2-1-2 学術総合センター内）
URL: http://2015.uqcc.org/

各機関の役割分担

- NICT: 基本方式を発案し、量子鍵配送ネットワークの技術とテストベッドを提供
- プロドローン: 鍵インターフェースと鍵管理システムをドローンに実装し、セキュア制御通信技術を開発
- サンエストレーディング: 応用市場を調査し、セキュア制御通信技術の仕様要件を抽出

実験の概要に関する動画

https://youtu.be/KqOW6hqF9qU

＜ 本件に関する問い合わせ先 ＞

NICT
未来 ICT 研究所 量子 ICT 研究室
佐々木 雅英
Tel: 042-327-6524
E-mail: psasaki@nict.go.jp

プロドローン
開発統括
市原 和雄
Tel: 03-5212-5132
Fax: 03-5212-5102
E-mail: info@prodrone.jp

サンエストレーディング
営業部
前原 光徳
Tel: 03-3795-8121
E-mail: mmaehara@sanes.co.jp

＜ 広報 ＞

NICT
広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

プロドローン
MK 統括
楠本 慎太郎
Tel: 052-954-0286
Fax: 052-954-0025
E-mail: kusumoto@prodrone.jp

サンエストレーディング
営業部
前原 光徳
Tel: 03-3795-8121
E-mail: mmaehara@sanes.co.jp

＜用語解説＞

***1 ドローン**

4 つ以上の複数の回転翼を持ち、垂直離着陸と高速な空中移動を可能とする小型無人航空機。ヘリコプターと異なり単純な機構であるため、廉価で製造可能であり、空撮や測量、農薬散布、橋梁や太陽光パネルなどの構造物の検査など、様々な分野での利用が進んでいる。現在、飛行禁止空域や飛行方法に関する航空法関連法規の改正が行われつつあるが、技術の進歩や利用の多様化の状況を踏まえ、無人航空機を使用する事業の健全な発展に資する方策や措置についても検討が行われている。

***2 真性乱数**

規則性も再現性もない完全にランダムな数字の系列。通常、ビット値 0,1 が等確率で互いに独立に、周期性がなく予測不可能にランダムに並んでいるビット列を指す。真性乱数を生成するデバイスとしては、熱雑音や量子力学的現象などの予測不可能な物理現象を利用する物理乱数生成器が代表的なものである。しかし、このような物理乱数生成器の速度には限界があるため、実際の多くの用途では、確定的な計算アルゴリズムによって生成された、いわゆる疑似乱数を用いる場合が多い。疑似乱数は、必ず周期性を持ち、高度な計算機で解読される危険が伴う。

***3 量子鍵配送ネットワーク**

量子鍵配送（Quantum Key Distribution: QKD）とは、微弱な光に乱数の情報を乗せて伝送し送受信者間で適切な信号処理を行うことで、2 地点間で原理的に盗聴されない暗号鍵（真性乱数）を共有する技術。現在、インターネット上の鍵交換では、計算アルゴリズムに基づいて安全性を保証する公開鍵暗号が使われているが、強力な計算機が登場すれば破られる危険性がある。これに対して、量子鍵配送は量子力学の法則に基づいて安全性を保証しており、どんな盗聴技術や解読技術でも破られないことが数学的に証明されている。

QKD は、光通信路で結ばれた 2 地点間の回線（リンク）上において 1 対 1 で鍵共有を行う。2 つの QKD リンクを、盗聴者が侵入できない物理的に防御された安全な局舎（セキュアノード）を介して接続し、セキュアノード内において、QKD による暗号鍵をもう一方の暗号鍵でカプセル化してリレー配送することで、複数の QKD リンクをネットワーク化し、長距離化、広域化することができる。これが量子鍵配送ネットワークである。2010 年以降、NICT が有する光テストベッド上に、都市圏の量子鍵配送ネットワーク、いわゆる Tokyo QKD Network が構築され、試験運用や次世代技術の研究開発が行われている。特に、ネットワークスイッチやスマートフォンなど様々な情報通信機器に暗号鍵を供給し安全なセキュリティサービスを提供するためのソフトウェア（アプリケーションインターフェース）を搭載したネットワークシステム、いわゆる QKD プラットフォームが開発され、現在、いくつかの重要通信サービスを提供する実用環境の下で、長期的な安全性や信頼性のテストが行われている。

***4 シリアル通信**

模型飛行機や模型自動車を無線で制御するためリモート制御のシリアル通信プロトコルは、デファクトスタンダードがあり、世界中で互換性のある装置が製造、販売されている。

***5 ワンタイムパッド暗号化**

送信する情報（平文）のデジタルデータと同じ長さの真性乱数[*2] を暗号鍵として用意し、はぎ取り式メモ（パッド）のように 1 回ごとに使い捨てる暗号化方式。異なる平文ごとに、異なる暗号鍵を使う。平文と暗号鍵のビット和によって暗号文を生成して伝送し、受信側で再び暗号文と暗号鍵のビット和によって平文を復号する。

ドローン制御通信のワンタイムパッド暗号化についての詳細

地上にある送信機と、ドローンに搭載される受信機は、近年 2.4GHz 帯の電波を用いて通信が行われている。通信データは制御に関するコマンド群で、シリアル通信に準拠し、スタートバイト、エンドバイトやステータス情報を含み、1 パケット 25 バイトの固定長で、18 種類の制御情報を表現し、短い時間間隔で繰り返し送出される。

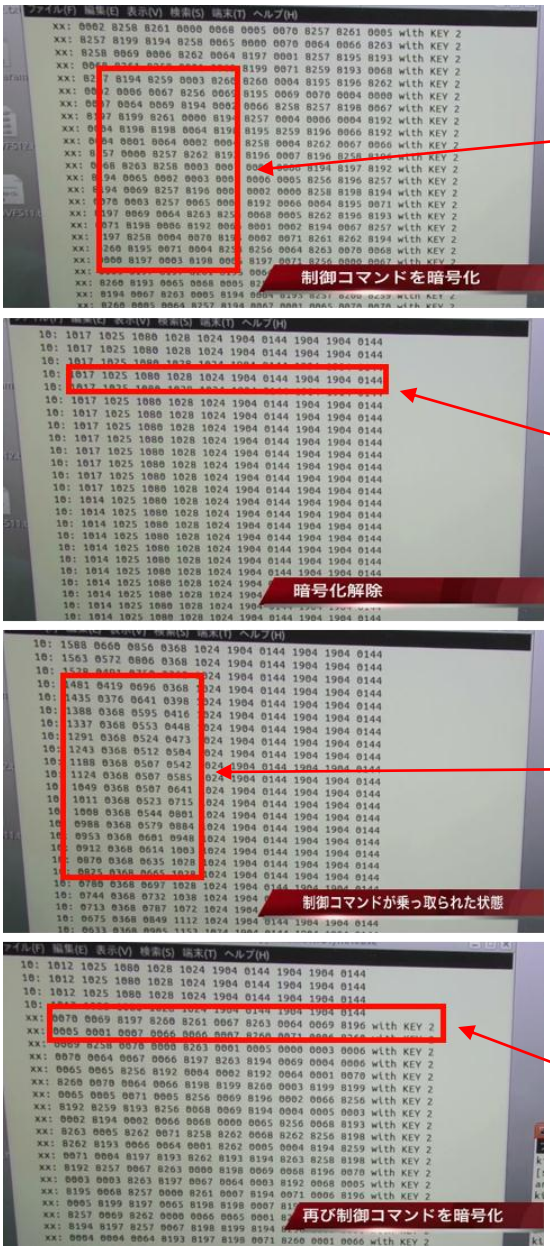
送信機が生成するこの 25 バイトのデータは、今回作製した地上局制御装置を経由する際、スタートバイトとエンドバイトを除き、さらに、末尾へ 2 バイトのチェックサムを追加した後、地上局制御装置内部に蓄積された真性乱数と論理和処理を施されて暗号化される。

暗号化されたデータは、先頭に 1 バイトのシーケンス番号をつけ、全長 26 バイトで送信される。ドローン上の受信装置は、繰り返し 26 バイトのデータを受信するが、最初の 1 バイトにより、パケットの一時的な欠落やドローン内部に保持する真性乱数の先頭アドレスを計算し、復号を試みる。復号した結果は、末尾 2 バイトのチェックサムを確認し、合致している場合に有効データとして、ドローンの制御装置に渡される。

制御通信に関してのみであれば、おおむね 30 分の飛行に 3M バイトのサイズの真性乱数で対応可能であり、本システムは、高度なセキュリティを実装して運用可能な形でユーザに提供することができる。

図 4 は、地上にいる盗聴者が、正規の地上局とドローン間の無線通信を傍受している様子（盗聴装置のモニタ画面）を示している。(a)は、制御コマンドの信号を暗号化している状態を傍受している様子で、制御コマンドは完全に暗号化されており、盗聴者にはランダムな数字の列にしか見えず、意味のある情報を与えない。(b)は、暗号化を解いた状態で、ドローンの制御に使われるコマンドの特定のコード（決まった数値の列）が見えるようになっている。(c)は、盗聴者が強

制的に制御コマンドを変更しており、ドローンの制御を乗っ取っている状態になっている。(d)は、再び制御コマンドを暗号化した場合の画面で、盗聴者には制御コマンドのコードの判別が付かない状態に戻る。



(a)制御コマンドを暗号化

制御データ内の可変量データを監視している。暗号化されているため、ランダムな値となっている。

(b)制御コマンド生データ

制御データ内には 0～2000 の値を持つ 16 種類の可変量データが含まれており、図では 16 種類のうち 10 種類を監視している。

(c) 制御コマンド強制変更

制御データのうち、最初の 1 つはモータの出力に関連し、次の 3 つは機体の姿勢に関するデータである。このデータをハッキングして異常な操作データを送っている(実際にドローンがこのデータを受けると異常な動作となる。)。

(d) 再暗号化

暗号化するとランダムな値となり、このデータを変更しようとしても意味のない値となってしまうため、ハッキングができない。また、すべてのタイミングで異なる乱数と組み合わされているため、偶然の一致が連続することはない。

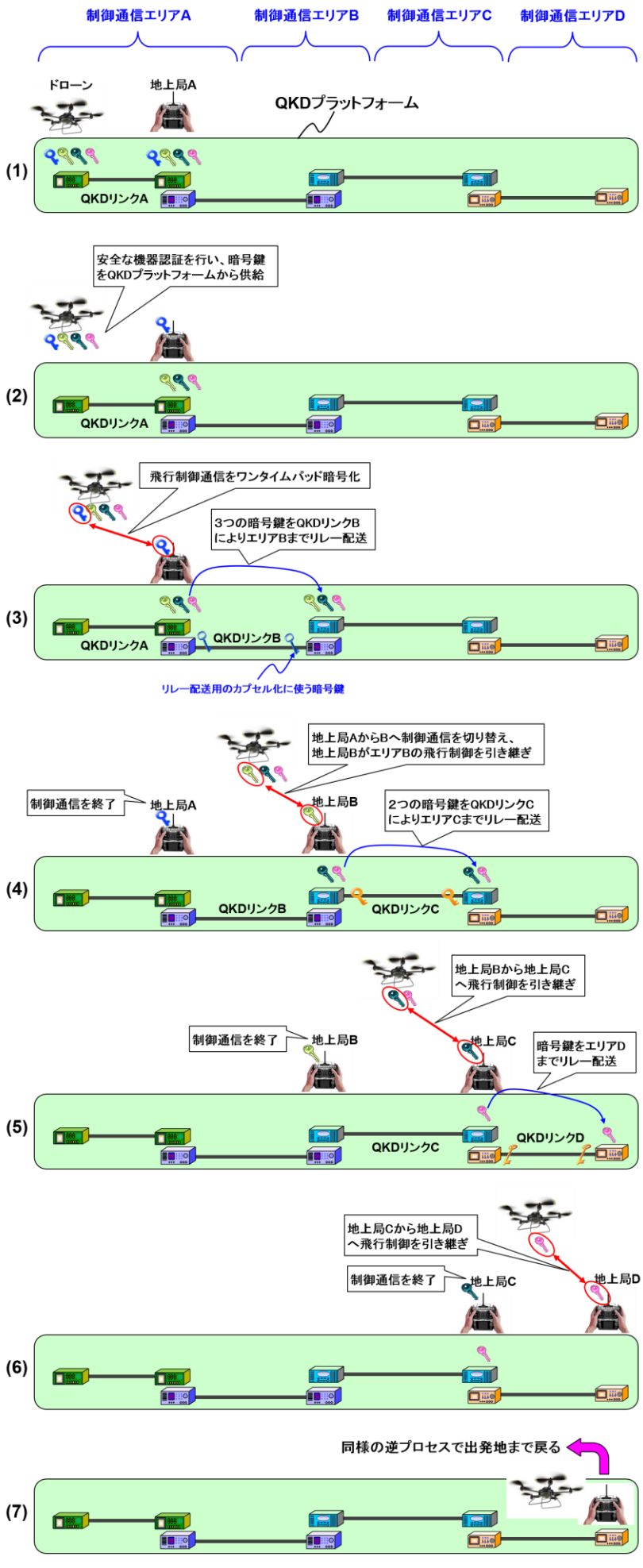
図 4 ドローン制御通信の暗号化の ON-OFF、及び盗聴者による制御コマンドの強制変更を模擬的に再現

*6 量子鍵配送ネットワークを用いたドローンの広域セキュア制御通信技術 (第二世代)について

ドローンと地上局間の通信では、通常、地上局そのものからドローンを飛ばすので、飛ばす前に操縦者自身が真性乱数の対を用意し、対の一方をドローンへ手渡しで供給することができる。ワンタイムパッドでの暗号化・復号化の処理は、単純なビット和なので、計算処理遅延はほとんど生じない。一方、真性乱数の対を用意して、正しい認証を行った上でドローンへ暗号鍵を手渡す必要がある。なお、ドローンの飛行時間がそれほど長くない場合には、市販のメモリによって必要な量の暗号鍵を十分格納できる。

ドローンをその無線通信制御エリアの圏内を超えて、広域へ安全に飛行させたい場合には、暗号鍵をほかの制御通信エリアへ配送しておかなければならない。この配送には、信頼できる宅配システム、あるいは QKD プラットフォーム(用語解説[*3]「量子鍵配送ネットワーク」を参照)を利用するという 2 つの方法がある。QKD プラットフォームでは、常時、QKD 装置によって暗号鍵を生成、配送し、利用に備えて蓄えておくことができる。また、ユーザからリクエストがあれば、必要なノード間で随時、暗号鍵を配送、共有することができる。

QKD プラットフォームを活用した広域セキュア制御通信方式の典型的な例として、4 つの制御通信エリア A、B、C、D にわたって制御を安全に引き継ぎ、広域で飛行させる場合の概要を図 5 に示す。



(1) QKD プラットフォーム上の QKD リンク A において、これから使う 4 種類の暗号鍵を生成した状態を示す。

(2) ドローンが 4 種類の暗号鍵を QKD 装置から供給されるとともに、地上局 A は、1 番目の暗号鍵を供給される。鍵供給は USB などを介して行う。その際には、情報理論的安全性を持つ認証方式（Wegman-Carter 方式など）により適切なユーザ・機器認証を行う。

(3) ドローンは、一つ目の暗号鍵で飛行制御通信をワンタイムパッド暗号化しながら、制御通信エリア A 内において、安全な飛行制御通信を行う【より正確には、最初、ドローンと地上局間でお互いにユーザ認証を行ってから、制御通信を開始する。そのため、厳密には、ユーザ認証用と制御通信用に 2 種類の暗号鍵が必要だが、ここでは 1 種類の鍵の図柄で代表させている。】。
その間、QKD プラットフォームでは、3 つの暗号鍵を QKD リンク B により、地上局 B までリレー配送しておく。

(4) 地上局 A から B へ制御通信を切り替え、地上局 B がエリア B の飛行制御を引き継ぐ。同時に、2 つの暗号鍵を QKD リンク C により、地上局 C までリレー配送する。

(5) (4) 同様の作業を行う。

(6) エリア D での制御通信を行い、最終的には地上局 D へドローンを着陸させる。

(7) 同様のプロセスを、新たに暗号鍵を生成しながら、逆向きに走らせることで、ドローンを再び出発地点に戻らせることができる。

図 5 量子鍵配送ネットワークを用いたドローン広域セキュア制御通信（第二世代）