マルチコプターを用いたサイバー攻撃に対する一検討

岡本 薫[†1] 樫原 茂[†1] 山口 英[†1]

本論文では、マルチコプターを用いたサイバー攻撃の検知方法について検討を行う。小型コンピュータを搭載したマルチコプターの登場により、これまでのサイバー攻撃のようにネットワーク経由ではなく、物理的に攻撃対象に接近し、建物外部から無線ネットワークを介してサイバー攻撃を行うことが可能となりつつある。本論文では、マルチコプターとして AR. Drone 2.0 を対象にサイバー攻撃の実行可能性の調査・分析を行った結果をもとに、対象ネットワークの有線・無線ネットワークトラフィック、電波、映像、音の複合情報を用いたマルチコプター用統合監視システムについて検討を行う。また、検知手法の一例として、無線ネットワーク上での AR. Drone 2.0 の通信パケットを取得、分析することで、AR. Drone 2.0 の接近及び手動操縦と自動操縦の判別が可能であることを示した。

1. はじめに

近年、小型コンピュータの進化、画像システムの高性能化、無線通信の発展等により、小型コンピュータと高性能カメラを搭載した容易な操作性の無人飛行機（Unmanned Aerial Vehicle: UAV）が登場し注目を集めている。なかでも、Parrot 社の AR.Drone 2.0 [1]をはじめとするマルチコプター[2,3]は空撮等の趣味の範囲だけではなく、実生活においても身近な存在になろうとしている。例えば、Amazon.com が提案しているマルチコプターを用いた 30 分以内の配送[4]や、セコム株式会社の小型監視飛行ロボット[5]などがあげられる。今後も、マルチコプターを用いた様々なサービスが登場すると考えられる。

このようなマルチコプターは様々なサービス提供の可能性を秘めている一方で、空中を飛行するため、安全性やプライバシーに対する問題を解決することが求められている[6][7]。安全性においては、各国において UAV に対する規制が異なり、UAV の飛行に対する法規制は成熟していない。また、プライバシーにおいては、明日にでも身近に発生しうる盗撮等の危険性についても防ぐ方法がないのが現状である。

さらに、マルチコプターはカメラだけでなく、小型コンピュータも搭載または可搬することが可能であるため、マルチコプターからのサイバー攻撃が起こりうる環境も十分に整ったといえる。これまでのサイバー攻撃と異なる点としては、ネットワーク越しではなく、攻撃対象に直接接近し、無線ネットワーク（特に Wi-Fi）を介したサービス妨害や不正アクセスが可能となる。システムに対する影響がある場合は、既存のセキュリティシステムにより検知／対策が可能であると考えられるが、それでも攻撃元を特定することは困難である。一方、無線通信のパケット傍受のように、システムに対する影響が無い場合は、攻撃対象となっていることにも気がつかないと考えられる。特に、マルチコプターは人のように入館管理等を必要としない上空から、建物内部に対してサイバー攻撃を行うため、これまでのサイバー攻撃対策だけでは不十分であるといえる。

これまで、このようなマルチコプターを用いた研究は数多く行われているが、サイバー攻撃に関する研究はほとんどない。文献[8]では、AR.Drone 2.0（以下、AR.Drone と呼ぶ）を用いたサイバー攻撃のモデルを示し、セキュリティの重要性を述べているが、具体的な方法については述べられていない。このような UAV によるサイバー攻撃に対する研究は我々の知る限り行われておらず、今後重要な研究分野になると予想される。特に、UAV によるサイバー攻撃において、攻撃元を特定することが重要であると考える。そこで、本論文では、最初のステップとして、マルチコプターの中でも低コストで入手可能かつサイバー攻撃を実行する能力があると考えられる AR.Drone を研究対象とし、マルチコプターによるサイバー攻撃を検知するためのシステムについて検討を行う。マルチコプターによるサイバー攻撃検知システムを検討する上で、AR.Drone の基本性能を実機により調査し、その結果から考えられる検知手法について検討を行う。また、ネットワークの観点から、検討した手法によりマルチコプターの検知が可能かどうかについても実際のデータを用いて分析する。

2. 関連研究

これまでマルチコプターの姿勢制御などを対象にした研究は数多く行われており、様々な応用に関する研究が徐々に増加しつつある。中でも AR.Drone は実機によ

†1 奈良先端科学技術大学院大学 情報科学研究科
〒630-0192 奈良県生駒市高山町 8916-5

る研究対象としてよく利用されている。しかし、AR.Drone は Wi-Fi を使ってコントロールを行うため、飛行範囲が狭いという問題点を持つ。そこで、文献[9]では、スマートフォンを AR.Drone に搭載することで飛行範囲を拡張している。実現方法としては、ユーザのスマートフォンから AR.Drone 上のスマートフォンに 3G ネットワーク経由でコントロール情報を送信し、AR.Drone 上のスマートフォンはその情報を Wi-Fi 経由で AR.Drone へ転送する。その結果、3G ネットワークが接続可能な範囲を AR.Drone は飛行することが可能となる。また、マルチコプターは飛行範囲に加えバッテリの制約もある。文献[10]では、飛行時に複数の AR.Drone を一列に並べ、それぞれを有線で結び電気を供給する。その結果、連続飛行が可能となり、複数の AR.Drone を用いることで、センシング範囲を拡張している。また、必要に応じて、AR.Drone は接続された環境から離れ飛行することも可能である。このように飛行範囲を広げることで、マルチコプターによる新たなサービス提供の可能性を引き出す研究が行われている。

一方で、マルチコプターの悪用に対する研究報告も行われている。前節でも述べたように、文献[8]では AR.Drone を用いたサイバー攻撃の例が示されている。例では、AR.Drone に Raspberry Pi を搭載し、搭載した Raspberry Pi の Wi-Fi を使ってデータ取得やネットワークへの不正アクセスを行うモデルや、複数の AR.Drone が連携するモデルについて示されている。このようにマルチコプターと小型コンピュータの組み合わせにより、UAV によるサイバー攻撃の可能性が高まりつつあるが、そのようなサイバー攻撃の検知・対策手法についての議論は少ないといえる。

3. AR.Drone 2.0 の基本性能の調査

本節では、マルチコプターとして AR Drone を対象に、空中からのサイバー攻撃の実行可能性について調査を行う。まず、3.1 節では AR.Drone 2.0 の技術仕様と操縦方法について概説する。3.2 節では AR.Drone に小型コピュータを搭載した際の飛行確認試験を行う。3.3 節では GPS 情報を用いた自律航行によるサイバー攻撃の実行可能性について調査を行う。

3.1 技術仕様と操縦方法

AR Drone 2.0 の技術仕様と操縦方法について簡単に述べる。Parrot 社の仕様書[11]によると、AR Drone 2.0 は屋外飛行時の大きさは 451 mm×451 mm であり、重量は 380 g である。また、搭載されている制御ボードの CPU は 1GHz 32 bit ARM Cortex A8 processor with 800MHz video DSP TMS320DMC64x であり、メモリは 1Gbit DDR2 RAM at 200MHz である。OS は Linux 2.6.32 が使用されており、通信メディアとしては IEEE 802.11b/g/n が使用可能である。このように、AR. Drone 2.0 はプログラミング可能な環境であることが分かる。

操縦方法においては、手動操縦と自動操縦の 2 種類が利用可能である。手動操縦では、スマートフォンまたはパソコン（以下、PC と呼ぶ）を Wi-Fi 経由で AR.Drone と接続し、AR.Freeflight アプリケーション[12]を用いることで手動操縦が可能である。一方、自動操縦においては、GPS ユニットを USB 接続で AR.Drone に搭載し、、QGroundControl アプリケーション[13]により飛行経路を設定し、設定情報を AR.Drone に転送することで自動操縦が可能である。このように AR.Drone は自由にプログラミングできる環境と容易な操縦性を提供している。

3.2 小型コンピュータ搭載時の飛行確認試験

AR.Drone は Linux OS 搭載であるため、搭載されている Linux 上でプログラムを実行することも可能であるが、処理負荷によっては飛行制御に影響を与えると考えられる。そこで、文献[8]においても示されていたように、サイバー攻撃用の小型コンピュータとして Raspberry Pi Model-B[14]を搭載した際の飛行性能について調査する。

飛行条件は、外的要因、特に風の影響を避けるため屋内で実施した。屋内飛行においては、屋内用ハルと呼ばれるローター保護カバーを使用し、バッテリは 1,000mA の標準タイプを用いた。また、操縦用アプリケーションは Windows 8.1 上に AR.Freeflight をインストールし、PC より AR.Drone をコントロールした。

実験では、PC より AR. Drone に離陸命令を出し、その場でホバリングをさせ、平衡状態を維持させ、壁等に衝突の恐れが生じた場合のみ PC より指令を出し、回避させた。飛行時間は、離陸してからバッテリ残量が 0%となり、AR.Drone が自動で着陸を開始し、接地するまでを計測した。小型コンピュータを搭載しない標準飛行形態と搭載した追加機器搭載飛行形態において、それぞれ 10 回ずつ実施した。

飛行実験の結果を表 1 に示す。表 1 より、Raspberry Pi を搭載した状態でも飛行可能であり、飛行時間については大きな変化は見られなかった。これは、搭載モーターの出力が高く、搭載機器の重量が与えた影響が軽微であったためと考えられる。また、飛行時間のばらつきは、バッテリの充電状況などのコンディションが影響したものと考えられる。この結果より、Raspberry Pi 程度の小型コンピュータは十分に搭載可能であることが明らかとなった。

表１　飛行時間の比較

項目	標準飛行形態	追加機器搭載飛行形態
飛行時間（平均）	7 分 21 秒	7 分 18 秒
（最大）	7 分 43 秒	7 分 49 秒
（最小）	6 分 50 秒	7 分 2 秒

3.3 自律航行によるサイバー攻撃の可能性

次に、自律航行によるサイバー攻撃の可能性を調査する。調査では、図 1 に示すような飛行経路を設定し、AR.Drone に経路情報を転送することで、AR.Drone は模擬攻撃対象に向かい、模擬攻撃対象空域において２分間のホバリングし、その後設定飛行経路に沿った帰投を行う。

実験では、AR.Drone は設定された飛行経路を順調に指定空域に進出し、ホバリングを実施後、飛行経路を経て着陸指定ポイントに着陸した。飛行経路には樹木等の障害物があったが、事前に障害物の高さなどを考慮し、経路だけでなく高度も設定することで、障害物に接触することなく飛行可能であった。表 2 にはこの調査の日時、天候、飛行時間の情報等をまとめている。本実験では安全性のため飛行スピードを小さく設定しているが、飛行スピードを上げることでより遠距離から短時間で攻撃対象へ接近、及び攻撃対象からの帰投が可能である。以上より、AR.Drone の飛行性能は高く、大きな改修をしない標準状態でもサイバー攻撃を実施することは可能であると考える。

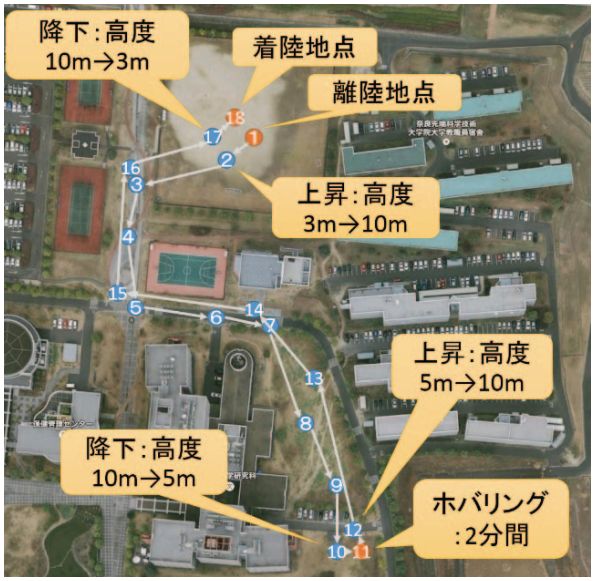

図１　飛行経路図

表２　飛行諸元

実施年月日	2014 年 5 月 14 日（水）
天候	曇り，微風
設定経由地点数	１８
離陸時刻	11 時 51 分
着陸時刻	11 時 58 分
飛行時間	7 分 24 秒
ホバリング時間	120 秒
バッテリ残量	48%

4. マルチコプターによるサイバー攻撃検知システムの検討

前節で述べたように、マルチコプターを用いたサイバー攻撃は可能であり、今後、このようなマルチコプターによるサイバー攻撃を検知・対策する手法が必要となる。以下、4.1 節では、このような悪意あるマルチコプターを検知するためのシステムについて検討し、4.2 節ではパケットキャプチャによる検知の可能性について調査する。

4.1 マルチコプター用統合監視システム

マルチコプターにおいて考えられるサイバー攻撃として、サービス妨害（Denial of Service (DoS) attack）、不正アクセス、パケット傍受、光学偵察（盗撮）等があげられる。これらは、標的のシステムに影響を与える攻撃と与えない攻撃に大きく分類できる。サービス妨害や不正アクセスなど標的のシステムに何らかの影響を与える場合は、これまで行われてきた研究成果[15][16][17]を活かすことで攻撃に対する検知は可能であると考える。しかし、パケット傍受や光学偵察のように、標的のシステムに影響を与えない攻撃の場合、攻撃を検知することはできない。そこで、本節では、これまでの調査により得られた知見をもとに、悪意あるマルチコプターを検知できるシステムアーキテクチャについて検討する。

図２に現在検討しているマルチコプター用統合監視システムの概念図を示す。これまでのサイバー攻撃とは異なり、ネットワークトラフィックやシステムの挙動等を分析するだけでは、マルチコプターによるサイバー攻撃を検知することは困難であるため、悪意あるマルチコプター自体を検知することが重要となる。そこで検討している監視システムでは、対象ネットワークの有線・無線ネットワークトラフィック、電波、映像、音の複合情報を用いることで、悪意あるマルチコプターの検知を試みる。まず、ネットワークトラフィックにおいては、これまでに開発されているツール等を用いることで、システムに影響を与える攻撃であれば検知可能である。しかし、ビルなどの建物外から攻撃の場合、攻撃元（マルチ

コプターの接近）を特定することは困難である。攻撃元の特定、およびシステムに影響を与えない攻撃を検知するためには、無線ネットワークトラフィックキャプチャー、電波、映像、音の要素を組み合わせた検知が必要であると考える。

以下、それぞれの要素における検知方法案について述べる。まず、マルチコプターの接近を検知するためには、マルチコプターが発する無線トラフィックを取得、分析することで接近を検知できると考えられる。AR.Drone では機体制御を行うために、Wi-Fi を使用しているため、機体から何らかの制御パケットが発信されている。そこで、これらの特徴ある制御パケットを検知することで、AR.Drone の接近を検知できると考えられる。しかし、マルチコプターの中には Wi-Fi 以外の無線通信メディアにより機体制御を行うものもあるため、無線ネットワークトラフィックだけの分析だけでは不十分である。次に、異なる無線通信メディアによる制御を検知するために、各周波数帯を定期的に自動的に調査し、新たに出現した電波を検知することが重要である。更に、実際の接近を検知するためには、映像・音による分析も重要となる。特に、マルチコプターによるサイバー攻撃は上空でホバリングすると想定できるため、カメラによる物体認識を行うことが可能であると考えられる。また、マルチコプターのモーター音も日常音と比較すると特異であるため、音分析により接近を検知できる可能性があると考えられる。しかし、これらの情報は環境や天候などの影響により、安定した検知を行うことが困難であり、これらの複合情報を分析することで悪意あるマルチコプターの検知を行うことが重要であると考える。

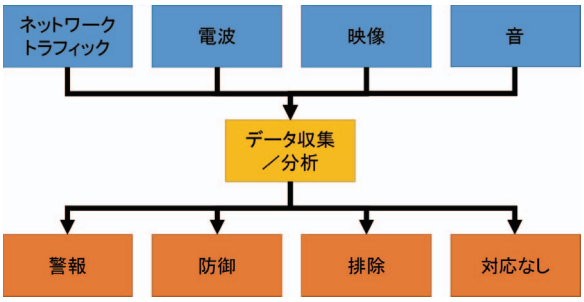

図２　マルチコプター用統合監視システム概念図

4.2 パケットキャプチャによる AR. Drone 2.0 の検知

本節では、AR.Drone 2.0 を対象に AR.Drone の送受信パケットを取得・分析することで、AR.Drone の接近を検知可能であるかについて調査する。3.1 節で述べたように、AR.Drone の操縦方法としては、手動操縦と自動操縦の２種類がある。これらの操縦方法の違いから、AR.Drone を制御するための情報は異なると考え、AR.Drone の送受信パケットを Wireshark により取得し分析する。

まず、自動操縦時における制御パケットについて調査する。調査では、3.2 節と同様に飛行経路を事前設定し、自動航法にて飛行させ、自動操縦用の PC 上で AR.Drone との通信パケットを Wireshark により取得した。調査時の飛行経路図と飛行時間を図 3 と表 3 にそれぞれ示す。図 3 に示すように、本調査ではグラウンド内で常に AR.Drone がパケットを送信した時に通信可能な範囲に自動操縦用の PC が存在する環境で通信パケットの取得を行った。

図３　飛行経路図

表３　飛行実験諸元

実施年月日	2014 年 5 月 14 日（水）
天候	曇り、微風
離陸時刻	11 時 30 分
着陸時刻	11 時 36 分
飛行時間	6 分

自動操縦においては、AR.Drone は操縦指令用の独自プロトコルの他に、Micro Air Vehicle Communication Protocol[18]（以下「MAVLink」と呼ぶ）を利用しており、MAVLink による操縦指令及び自機情報の送受信が可能である。Wireshark により取得できた結果の一部を図 4 に示す。図 4 の結果から、表 4 に示すように、姿勢情報、GPS 情報、機体情報が取得可能であることが分かる。このように、AR.Drone では自動操縦時においても機体から PC に対して機体情報に関するパケットを送信しており、これらのパケットを取得し分析することで、AR.Drone の接近およびホバリングで静止しているなどを判別可能である。

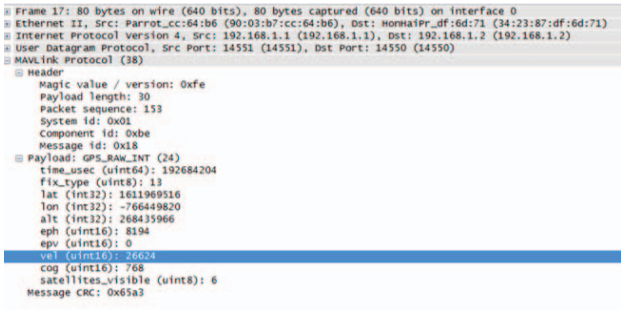

図４　自動操縦時において取得したパケット

表４　取得したパケットから機体の状態を判別可能な情報

姿勢情報	横方向傾き及びその速度、 縦方向傾き及びその速度、 機首方向及びその速度
GPS 情報	緯度、経度、高度、対地速度、進路、探知衛星数
機体情報	バッテリ電圧

次に、手動操縦時における制御パケットについて調査する。本調査では、PC 上で AR.Drone を手動操縦し、そのときに通信されたパケットを調査する。図５に手動操縦時に取得したパケットの例を示す。ここで取得したパケットは、自動操縦時には確認されなかった制御パケットであり、PC から AR.Drone に対して送信されている。このパケットに含まれる情報を表 5 に示す。表 5 に示すように、PC から AR.Drone に対して、機体の制御命令が送られていることが分かる。以上のように、使用されている通信プロトコルの違いによって、操縦方式が検知でき、AR.Drone の接近だけでなく、攻撃者本人が近くにいるかどうかの判断にもつながると考えられる。このようにマルチコプターから送受信されるパケットの特性を利用することは、マルチコプターによるサイバー攻撃を検知する上で重要な指標であると言える。

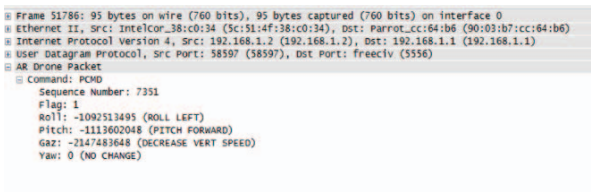

図５　手動操縦時において取得したパケット

表５　操縦指令用パケット主要情報

送信元	192.168.1.2（PC）
送信先	192.168.1.1（AR. Drone 2.0）
送信元ポート	58597
送信先ポート	5556
主要情報	横方向傾き指令 縦方向傾き指令 揚力変更指令 機首方向変更指令

5. おわりに

本論文では、マルチコプターによるサイバー攻撃に対する検知方法についての検討を行った。これまでのサイバー攻撃とは異なり、マルチコプターを用いたサイバー攻撃は攻撃対象に物理的に接近しサイバー攻撃を行うことが可能である。しかし、パケット傍受や光学偵察のように標的システムに対して影響を与えない場合、マルチコプターによるサイバー攻撃を検知することは困難である。そこで、マルチコプターとして AR.Drone を対象に、AR.Drone を実際に飛行させて得られた知見から、ネットワークトラフィック、電波、映像、音の複合情報の分析により、マルチコプターによるサイバー攻撃を検知するためのマルチコプター用統合監視システムを構築について検討した。また、検知情報の一つとして、マルチコプターが送受信するパケットに着目し、送受信される制御パケットを分析することで、マルチコプターが自動操縦または手動操縦であることが判別可能であることを示した。

今後の課題として、本論文ではマルチコプターによるサイバー攻撃を検知するためのアイデアを示したが、実際にマルチコプター用統合監視システムを実現する上では、各情報の取得方法および検知率、またそれらの複合情報からどのように分析・判断するかについて十分に調査する必要がある。

参考文献

[1] Parrot, http://ardrone2.parrot.com. (アクセス日:2014 年 5 月 15 日)
[2] DJI, http://www.dji.com. (アクセス日:2014 年 5 月 15 日)
[3] Phenox, http://phenoxlab.com/. (アクセス日:2014 年 5 月 15 日)
[4] Amazon Prime Air, http://www.amazon.com/b?node=8037720011. (アクセス日:2014 年 5 月 15 日)
[5] セコム株式会社, "世界初、民間防犯用の自律型の小型飛行監視ロボットを開発", http://www.secom.co.jp/corporate/release/2012/nr_20121226.html. (アクセス日:2014 年 5 月 15 日)
[6] Schneider, D., "Open season on drones?," Spectrum, IEEE , vol.51, no.1, pp.32,33, January 2014.
[7] Villasenor, J., ""Drones" and the future of domestic aviation [Point of View]," Proceedings of the IEEE , vol.102, no.3,

pp.235,238, March 2014.
[8] Evgeny Abramov, Maxim Kobilev, and Oleg Makarevich. 2013. Using quadrocopter as a pentest tool. In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 404-407.
[9] Dan He, Haoyi Ren, Weidong Hua, Gang Pan, Shijian Li, and Zhaohui Wu. 2011. FlyingBuddy: augment human mobility and perceptibility. In Proceedings of the 13th international conference on Ubiquitous computing (UbiComp '11). ACM, New York, NY, USA, 615-616.
[10] Yutaro Kyono, Takuro Yonezawa, Hiroki Nozaki, Masaki Ogawa, Tomotaka Ito, Jin Nakazawa, Kazunori Takashio, and Hideyuki Tokuda. 2013. EverCopter: continuous and adaptive over-the-air sensing with detachable wired flying objects. In Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication (UbiComp '13 Adjunct). ACM, New York, NY, USA, 299-302.
[11] Parrot, TECHNICAL SPECIFICATIONS, http://ardrone2.parrot.com/ardrone-2/specifications/. (アクセス日:2014 年 5 月 15 日)
[12] Parrot, AR.Freeflight, http://www.parrot.com/usa/apps/. (アクセス日:2014 年 5 月 15 日)
[13] QGroundControl, http://www.qgroundcontrol.org. (アクセス日:2014 年 5 月 15 日)
[14] Raspberry Pi, http://www.raspberrypi.org. (アクセス日:2014 年 5 月 15 日)
[15] N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, Network attacks: Taxonomy, tools and systems, Journal of Network and Computer Applications, Volume 40, April 2014, Pages 307-324.
[16] Igino Corona, Giorgio Giacinto, Fabio Roli, Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues, Information Sciences, Volume 239, 1 August 2013, Pages 201-225.
[17] Kemal Bicakci, Bulent Tavli, Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, Computer Standards & Interfaces, Volume 31, Issue 5, September 2009, Pages 931-941.
[18] MAVLink Micro Air Vehicle Communication Protocol, http://qgroundcontrol.org/mavlink/start. (アクセス日:2014 年 5 月 15 日)