SECURITY REPORT

2021 NOV

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

ドローン産業の発展とセキュリティ強化方法

01. 概要

第4次産業革命のセンシング技術、人工知能、5G、ロボット技術、自律飛行などの技術は、低電力、低コスト、高性能といった特性から広範囲で産業分野の重要技術としてドローンに活用されることになった。活用範囲として考えられていた偵察、監視などの国防業務を遂行するための技術は、発達と共に物流受送、交通、農業、人命救助、安全診断、放送などへの活用が進みだしている。狭い範囲では無人航行飛行体から、広い範囲では無人航空機や無人飛行装置などをドローンに準用することで急速に拡大している。

新たな市場であり、未来航空産業の重要技術としてドローンが目立つことでアメリカ、EU、中国、日本など世界の各国では我勝ちに有・無人航空機のロードマップを発表し、国家重点産業としてドローン産業育成と市場活性化に努力している。

ドローン産業の技術発展と市場可能性の展望とは異なり、2019年9月サウジアラビアの石油施設ではドローンから発生した火事事故や、登録義務のない重さ12kg以下の無登録ドローンによる、誤作動、爆発事故、セキュリティ事故など、単純な事故を超えて人命被害及び資産に関わる被害に繋がる可能性があるため体系的な対策が必要である。そこで今回は多様な産業分野で活用されているドローンのセキュリティインシデントや解決方法について確認したいと思う。

ドローン産業の発展とセキュリティ強化方法

02. ドローンの概念や主な特徴

1) ドローンの概念

ドローン(Drone)の辞書的な意味は「(蜂などの) ブンブンうなる」もしくは「単調な低い声で[ものうげに]語る」を意味するが、最近のドローン市場の観点からみるとパイロットが乗らずにプログラムかされた経路もしくは遠隔操縦を介して移動する飛行体を意味する。ドローンの最大離陸重量や目的などによってUAV(Unmanned Aerial Vehicle)やUSA(Unmanned Aircraft System)とも呼ばれる。

偵察及び監視などの軍事的な目的で開発されたドローンは先端技術と融合し低価で小型中心の単純な撮影目的から、物品受送・山林保護及び監視、施設物の安全診断、通信網活用、海洋管理、農業支援などの高価な中型中心に発展している。このような発展背景としては人工知能、IoT、センサー技術、3D/4Dプリンティング技術を利用した重要技術の発展、効率性向上、費用節減効果をもたらすことで新たなサービスの創出に寄与している。ドローンの活用範囲が拡張されることで「表1」のような主要役割と技術要素の分類ができる。

ドローン産業の発展とセキュリティ強化方法

年代	主要目的	主要役割	主要技術トレンド	主要Product
1960年代	初期無人飛行体	• ベトナム戦争戦場録画	• 無人飛行体技術戦場録画 • 初期航空電子技術実用化	• AQM-34
1970年代	改良型無人飛行体	• 中東戦争 欺瞞機、破壊用無人機投入 • 中東戦争戦場録画	• レーダー攪乱技術 • アナログデータリンク、 慣性航法 • リアルタイム映像送信技術	• Mastiff • Ryan 147 • Scout
1980年代	無人機システム	• 低高度及び近距離無人システム • 民需用(農業用)開発	• リアルタイム情報処理技術 • 昼・夜間観測映像技術	• CL-89 • Pioneer, Searcher • R50
1990年代	旧性能無人機システム	• 湾岸戦争戦術無人機 • 民需用無人機(農薬散布用)実用化	• デジタルマップ(Digital Map) • GPS航法及び誘導 • デジタル通信	• CL-289, Hunter • Predator • Rmax
2000年代	戦略無人機システム	• アフガン戦争迎撃機能保有無人機 • 民需用無人機産業化開発着手(通信中継など)	• 長期滞空/ステルス機能 • 人工知能イメージ認識(CNN, RNN)、 精密誘導制御技術 • 衛星通信	• Predator, Reaper • Global Hwak, Fire Scout • Smart UAV, Heliosなど
2010年代	自律化レベル向上及び産業化	• 広域偵察、長期滞空無人機 • 産業用無人機実用化 無人戦闘機(UCAV)	• 統合体系化技術 (合同戦術概念導入) • 自律化 • 群集化 (Swarming)	• X-45, X-47 • Zephyr • Solar Eagle
2020年代	先端技術融合産業	• 第4次産業革命重要技術のテストベッドとして活用 • 個人用自律飛行航空機(PAV)など未来重要航空産業	• 低価・小型中心の単純撮影から高価・中型への変化 • 大型無人航空機 • 自律飛行ドローン商用化	• Hermes 450, Heron, Sparrow, Trion

「表1」ドローンの時代別主要目的のトレンド分析
(参考：韓国産業技術評価管理院、無人航空機(ドローン)技術動向と産業展望、KEIT PD Issue Paper, Vol 15-7, 2015の中、一部再構成)

ドローン産業の発展とセキュリティ強化方法

03. ドローンの活用分野

ドローンは戦争のために開発されたのが始めで、軍事分野を中心に市場及び産業が形成されていた。しかしながら技術の発展でドローンのサイズ及び形、機能が多様になり多くの企業が民間ドローン市場を作り出した。

アメリカでは地域監視及び偵察のためにMQ-1プレデター、グローバルホークなど軍事用目的の高度無人偵察機を運用しており、民間産業分野ではアマゾン、ドミノピザなどの企業が物流サービスの目的としてドローンを活用している。実際に2021年5月アメリカのドローン専門業者の一つであるMissonGOはドローンを活用して人の臓器である膵臓を約16kmの距離まで運搬を成功した。

上記事例のようにドローン関連産業は次の「表2」のように農業、放送・撮影、物流・運送、測量・探査、建築・土木、環境監視、民生治安、教育など多様な分野でドローン活用産業として著しく発展し、実用化している。

ドローン産業の発展とセキュリティ強化方法

分類	特徴	必要技術	活用事例
農業	• 農地土壌状態、均平度など把握可能 • 作物の種、肥料など広範囲に水田と畑に散布可能	• 農地把握のためのRGB-Dのようなセンサー技術 • 地図及び地形を把握するためのマルチスペクトル(Multispectral)、ハイパースペクトル(hyperspectral)映像技術	• 2020年A国の政府機関でドローン湛水直播試験栽培を実施 • 2021年5月A国の政府機関ドローン活用した稲の中期除草剤散布デモンストレーションを実施
物流・運送	• 遠隔地物品もしくは衣料品の送達可能 • 長距離貨物を安全で早く送達可能	• ドローンを安全に操縦するための軽量化、小型化されたADS-B(Automatic Dependent Surveillance-Broadcast)のような航空監視技術 • 非可視圏領域で操縦するためのBVLOS (Beyond Visual Line Of Sight)技術	• 2021年2月24日、A国の政府機関でドローン物品配送のためのドローン専門業者に事業登録証を発行 • 2012年B国地震災害の際、ドローンを利用して救急薬品を運送
放送・撮影	• 映画、広告、ニュースなどメディア分野で活用 • 人が直接撮影しにくい郊外や広い地域の撮影可能	• 険地もしくは都心地の撮影のためのSLAM (Simultaneous Localization and Mapping)航法技術 • 長い時間撮影のためのバッテリーの軽量化、性能改善などの滞空時間向上技術	• C国の放送局、2014年ソチ冬季五輪の撮影 • 2014年ある放送局からライオン生態系撮影
建築	• 大型建築現場の工事進行度の確認が可能 • 土地の測量に活用可能	• 正確な建築現場の把握のためのToF Lidarなどを活用したセンサー技術 • レーダーもしくはLidar 技術を活用した衝突防止技術	• 2019年末、A国の建設会社から建設産業用のドローン監視システム構築

[表2]ドローンの産業別活用分野技術及び特徴

4. ドローンの構成要素分析

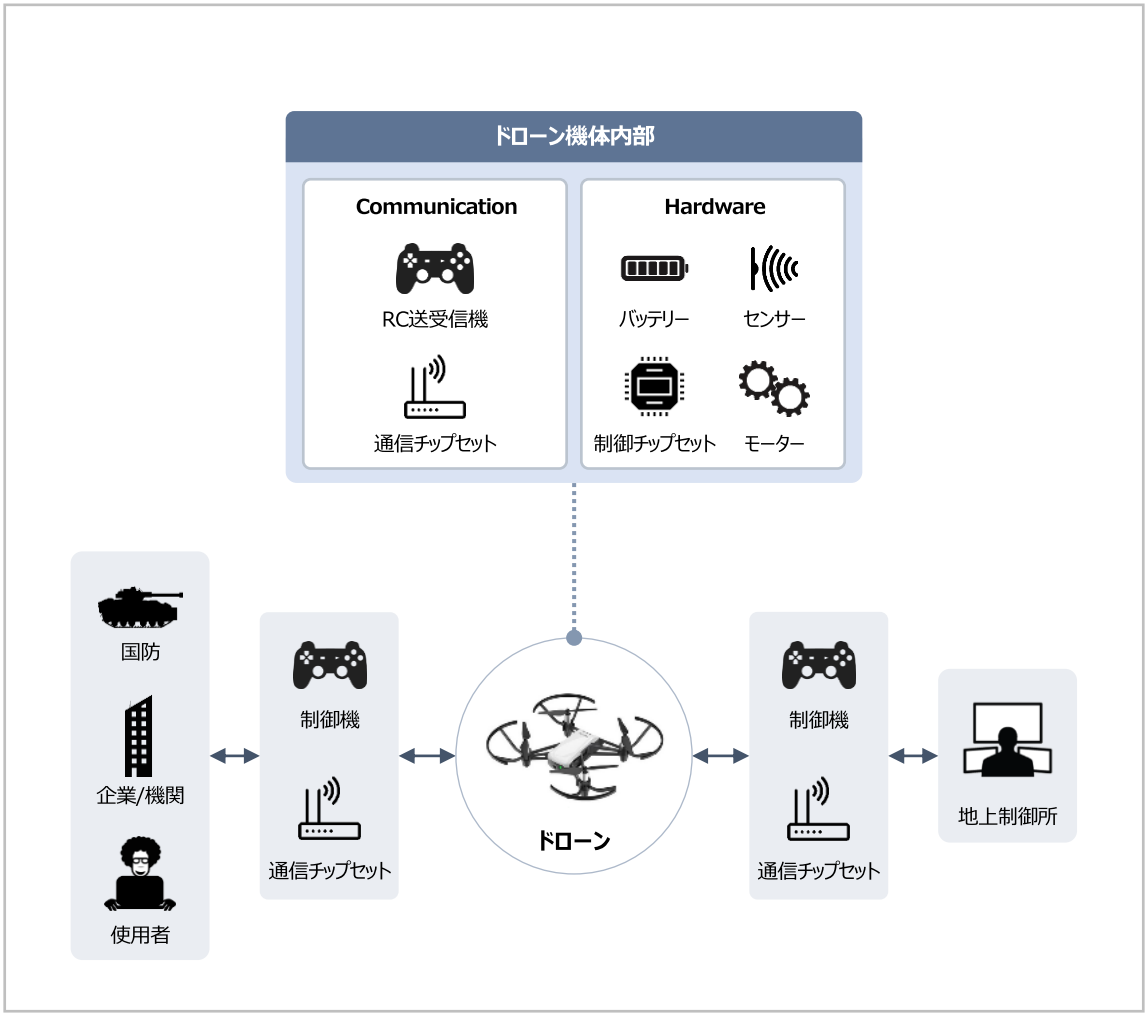
ドローンのセキュリティ脅威要素を確認するためにはドローンを起動するための全般的な構成要素に対しての理解が必要である。

ドローンはドローン産業の発展のための基盤インフラ構築及び主要施設保護に対しる飛行禁止領域の設定、不法飛行体の監視及び対応のための安全運航管理、ドローンによる不法侵入と攻撃を対応するためのセキュリティ技術などが基盤として構成される。

ドローン産業の発展とセキュリティ強化方法

ドローンの動かすには大きく△「ドローンシステム(UAC, Unmanned Aircraft System)のドローン」、△「ドローンを操縦し、状態のモニタリングができる地上制御装置」、△「ドローンを操縦する使用者(個人及び機関)」、△「ドローンと地上制御所を繋ぐ通信機器」、△「非免許無線通信・Cellular(セルラー)方式無線通信・専用免許帯域地上無線通信・衛星通信などで構成されたドローン無線通信技術」などで構成でいる。

ドローンを構成しているデバイスであるドローン機体はハードウェアとネットワーク通信のための通信機器領域で分類できる。通信機器はWi-Fi、Bluetooth、長距離通信カバレッジのためのCellular(LTE, 5Gなど)のモジュールが内蔵されていて、現在の位置情報が提供できるGPS、加速度センサー、 ジャイロセンサー、超音波センサー、カメラなどが存在する。外部環境情報を収集するためのカメラ、温度及び湿度を測定するためのセンサー、ToF, LiDARセンサーなども利用する。



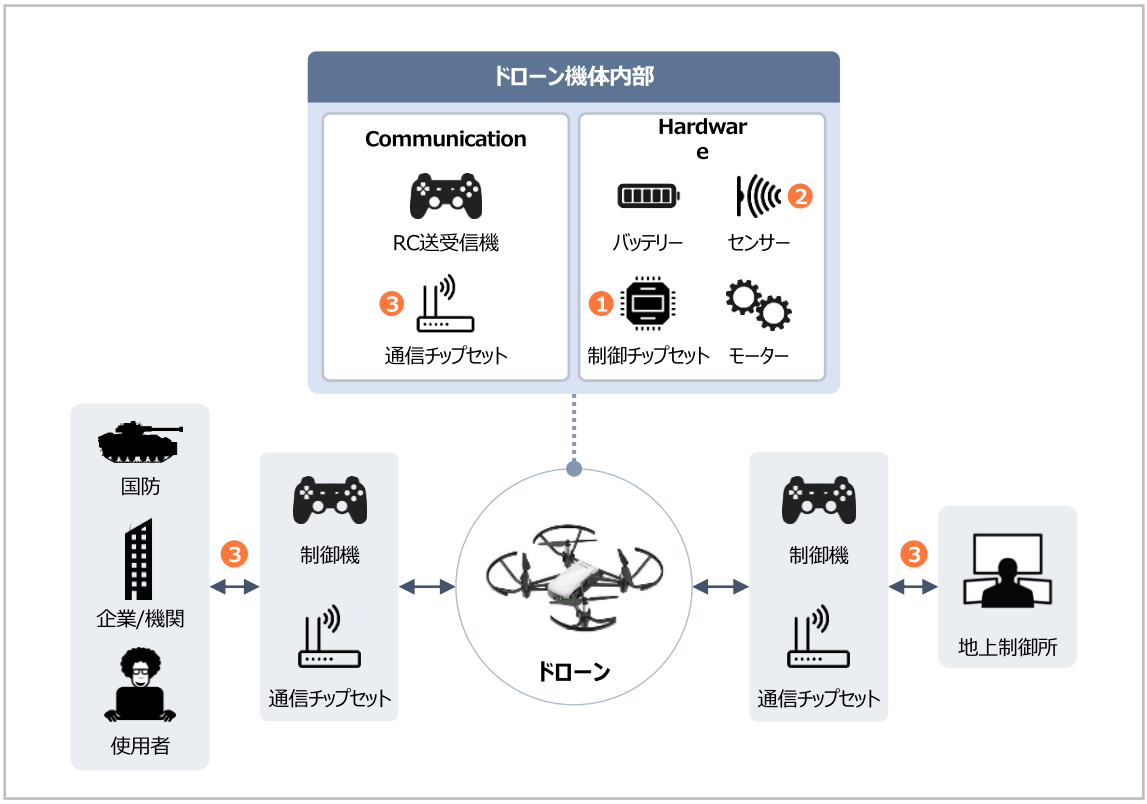
[図1]ドローン生態系構成要素

5.ドローンのセキュリティ脅威分析

ドローンは、GPS、Bluetooth 、5Gなどのネットワーク通信を介して送信された命令によって、リモート制御したり、事前にプログラム化された経路及び任務を遂行する。ドローンを構成している無線ネットワークを基盤として命令の制御及び遂行が行われるため、脆弱な無線ネットワーク通信及びインフラ構成によってサイバー攻撃対象にされる可能性が高い。

ドローンサービスから発生しうるセキュリティ脅威は△「ドローン・地上制御装置・情報提供装置別の資産要素で発生しうるセキュリティ脅威」と△「テロ・人命被害・犯罪のようなドローンによる直接的な被害」で区別できる。構成要素別のセキュリティ脅威を確認してみるとドローン環境では△GPS Spoofingと GPS Jamming、△制御信号電波妨害及び無力化、△センサー攪乱、△組込みシステムのファームウェア改ざんによるシステム権限奪取などが発生する可能性があり、地上制御装置からは△機密情報漏洩、△暗号化キーの漏えい及び脆弱なパスワードアルゴリズムによる制御権奪取、△間違った設計及び構成によるソフトウェアエラーなどが発生しうる。情報提供装置からも△センサーハイジャッキング、再送信攻撃、中間者攻撃のようなメッセージ改ざん攻撃、△データ改ざんなどが発生しうる。

ドローンシステムにて発生しうるセキュリティ脅威は多様のため、シナリオ基盤でセキュリティ脅威を構成し、これに対する対応方法の提示が必要である。「図2」ではドローンシステムから発生しうるセキュリティ脅威シナリオ3種(△GPSモジュールなどが存在する制御チップへの攻撃、△間違った設計によって発生される攻撃、△地上制御所及び使用者とドローンの通信の中で発生する攻撃)についてよる詳しく確認したいと思う。



[図2]ドローンセキュリティ脅威概念図

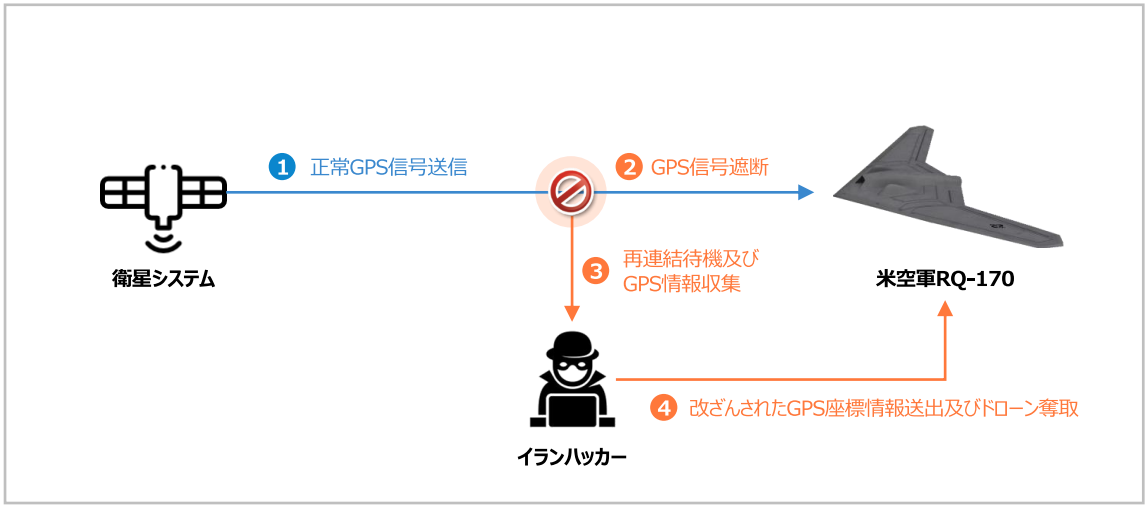
ドローン産業の発展とセキュリティ強化方法

1) 制御チップセットの攻撃

機体の中のGPS受信機、ジャイロセンサー、気圧センサーなどのセンサー信号処理、及びモーター制御用のコントローラチップはドローンの重要要素であるため、攻撃者の標的とされている。GPS受信機の場合、ドローンの位置情報を処理するために指定された経路で移動するための正確な位置情報を知る為の重要要素である。アメリカで使用される軍事用GPS信号の場合、暗号化されているが民間用のGPSの場合、暗号化されていない場合ことが多い。そのため、民間で使用されるドローンはほぼ暗号化されていないデータ及び、通信を利用しており中間者攻撃されやすい構造を持っている。

このような構造的な脆弱性を利用した代表的な攻撃がGPS SpoofingとGPS Jammingになる。GPS Spoofingは事前に衛星の位置と時間を計算して衛星から送信されたGPS信号の代わりに攻撃者が改ざんしたGPS信号を送信して位置と時間を操る攻撃方法である。最近はGPS Simulatorや無線通信の研究目的のUSRPなどを利用して攻撃がより容易である。GPS Jamming攻撃の場合、運事用中のドローンが使用する周波数の帯域より強い信号を送出して正常の周波数の受信を妨害する攻撃方法である。

[図3]のように実際2011年12月アメリカがイスラエルと共同で開発して無人ステルスドローンRQ-170がイランを偵察している途中、GPS Spoofing攻撃でドローンを奪取された事件があった。イランはドローンのGPSを強制的に遮断し、GPSが再連結した際に暗号化されていないGPS信号を探してイランの領土の座標を送信した。イラン領土内に着陸させてアメリカの最先端ドローンをリバースエンジニアリングドローンの技術習得及び複製に成功した。イランは2014年に複製したドローンの試験飛行に成功し、2016年にはステルス機能を搭載した長距離攻撃用のドローンを公開した。

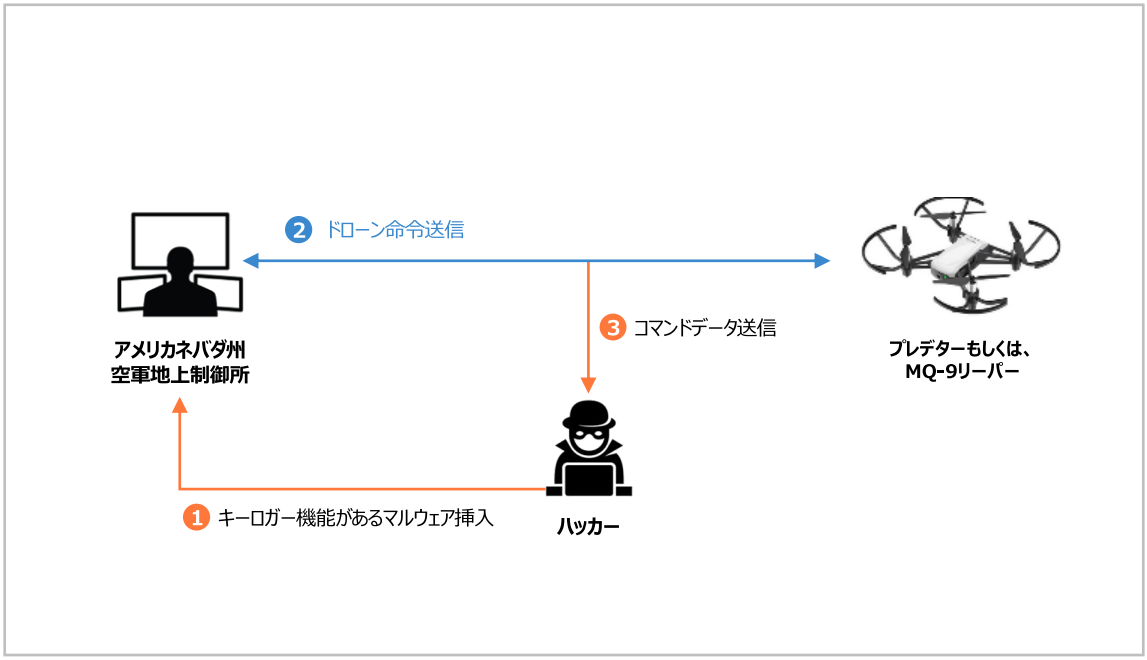


[図3] RQ-170ドローンGPS Spoofing攻撃概念図

2) 間違った設計によって発生する攻撃

ドローンには任務を遂行するためのイメージ処理センサー、高解像度カメラなどの様々なセンサーとこれを活用するため多様なハードウェアとソフトウェアが存在する。最近オープンソースの活用が多くなり、セキュリティが考慮されていない設計及び開発によるセキュリティ脅威は高くなっている。特に間違った設計は、ファームウェア脆弱性及び、アクセス制御の不備、悪意的な機能操作及びプログラム制御、ファームウェア改ざんによるシステム無力化などに活用できる。

ファームウェア脆弱性によるマルウェア挿入はドローンデバイス自体のセキュリティ脅威だけではなくドローンを制御する地上制御所まで影響を及ぼせる。「図4」のように2017年米軍が使用する高度偵察用監視ドローンであるプレデターとMQ-9リーパーを操縦するネバダ州の米空軍基地にキーロガーマルウェアが送信されて操縦者が入力したコマンドが漏洩された事例がある。



[図4]キーロガー挿入攻撃概念図

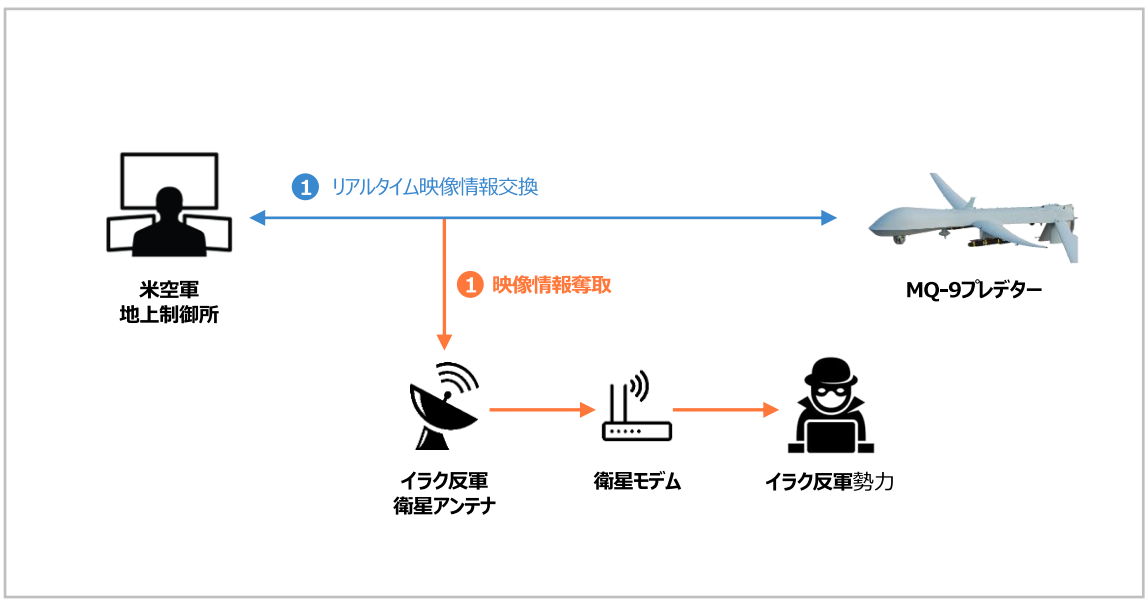
3) ドローン地上制御所もしくは、ドローン使用者の間からの攻撃

飛行過程で必要な重要要素で△4G、5Gなどを利用した超低遅延サービスを提供するCellular無線通信、△Wi-Fi、Private方法の非免許無線通信、△商用衛星通信技術、などで区分できる。ドローンの場合、上空で移動するため、無線通信の安全性は何よりも重要だが、一般的にWi-Fiを利用したデータの送受信が一般的である。特に公開型Wi-Fiを使用する場合、攻撃者による不法アクセス及びファームウェアの改ざんを誘発する可能性が高いため、使用に注意が必要である。

ドローンで最も使われている通信プロトコルであるMAVLink(Micro Air Vehicle Link)はドローン環境に最適化された軽量化プロトコルであるが、単純なパケット構造のためアルゴリズムの硬度が弱いという弱点を持っている。このようなプロトコルの弱点は通信課程でパケットを盗んだり、改ざんできる中間者攻撃(MITM, Man In The Middle Attack)が発生しうる。

「図5」のように権限がない使用者が途中でネットワーク通信を盗聴したり操作して他の使用者に送信する攻撃方法である。スニッフィング、セッションハイジャッキング、パケット挿入攻撃などを通してドローンと使用者もしくは、地上制御装置の間に送信されるデータを盗聴したり、改ざんしてファームウェアエラーを発生させる。

実際に2009年イラク反軍シーア派の武装勢力がロシアで開発された「Skygrabber」プラグラムを利用して米空軍のMQ-9プレデターが送信する作戦地域に対する映像情報を奪取し、当該の映像データは暗号化されていない送信であることが明らかになった。



[図5]イラク反軍映像奪取攻撃概念図

ドローン産業の発展とセキュリティ強化方法

06.ドローンセキュリティ脅威に対する対応方法

セキュリティ脅威に対応するためには次の「表3」のように△管理的な側面、△物理的な側面、△技術的な側面を考慮して対応戦略を立てる必要である。

まず、「管理的な側面」からの対応方法である。ドローンの場合、人が直接操縦する非自律飛行と、既に経路が入力されたプログラムで操縦される自律飛行が存在する。この二つの場合、全て人が介入して飛行する。従って、ドローンを操縦する使用者もしくは、ドローン地上制御の管理者に対してセキュリティ教育が絶対的に必要である。多様なセキュリティソリューションと多層セキュリティ体系が構築されていても、ソーシャルエンジニアリングなどを通じて内部の職員、及び協力業者の職員を狙う攻撃はセキュリティインシデントの原因として作用する可能性があるためである。

ドローンが飛行するためには多数の技術要素が有機的に連携されているため、一つのセキュリティ脅威は連鎖的に作用する。従って、攻撃を事前に予防するために周期的に脆弱性診断、ペネトレーションテストなどを行ってセキュリティレベルを診断し、ドローンの安全な飛行と飛行中発生しうる異常兆候を把握するためにログ記録の義務化及びドローン専用監視センターを構築して、法などの制度的にセキュリティ強化の義務化指定が必要である。

次は「物理的な側面」からの対応方法である。ドローンの場合、人が直接操縦せず、中長距離を移動する飛行体であるため、攻撃者に機体を奪取されたら内部に保存されている重要情報や技術などが漏えいする可能性が高い。従って、リバースエンジニアリング、重要保存情報奪取及び漏出を対応するためにはJTAGの無効化などのハードウェア観点からのセキュリティ処置が必要である。

ドローンには高性能カメラの設置が可能で、物流配送の機能を悪用して爆発物などを運搬したり、他のドローンの飛行を妨害するなどのテロや犯罪、私生活領域の進入、盗撮などを引き起こす可能性があるため、電磁場形成を用いてドローを墜落さえるドローンディフェンダー技術の適用が必要である。

最後に「技術的な側面」からの対応方法である。ドローンの内部には衛星、地上制御などと通信できる通信機器と多様な任務を遂行するための高性能カメラ、イメージセンサー、データ保存装置などの構成要素が存在する。このような構成要素はセキュリティ脅威が発生すると内部情報漏えい、ドローン奪取、テロもしくは、犯罪に悪用される可能性がある。従って、通信機器の場合、暗号化通信を適用したり、データを保護するために軽量化された暗号化アルゴリズムを使用するなど対策の準備が必要である。

ドローン産業の発展とセキュリティ強化方法

分類	細部項目	対応方法
管理的な側面	ログ記録の義務化	• 事後分析機能(フォレンジック、インシデント原因分析)強化のためのロギング義務化 • 使用者アクセス履歴、設定値変更履歴、機能遂行履歴など明示
	認証強化	• ドローンユニーク識別番号指定 • 収集したデータ照会、削除時の管理者認証手順樹立
	ドローン監視センター構築	• ドローン認証情報管理、ドローンID情報管理 • 飛行計画、飛行状態監視、飛行経路監視 • 飛行経路作成、経路閉鎖など管理
	セキュリティ診断	• ドローン生態系セキュリティ脅威事前セキュリティ強化方法 (周期的な脆弱性診断、ペネトレーションテスト)
	セキュリティ教育	• ドローン操縦資格評価の実効性をためるための現実反映 • ドローン操縦者及び性御センター管理者のセキュリティ認識教育強化
	法などの制度的サポート	• ネガティブ方法の規制最小化及びサンドボックスを通じた実用化促進 • ドローン活性化のための試験事業拡大 • ドローンインフラ拡張及び企業支援ハブモデル拡散 • 非事業用ドローン保険加入義務化検討 • ドローンによる私生活侵害の処罰規定を設ける
物理的な側面	物理的機器奪取対応	• リバースエンジニアリング、メモリ、サイドチャンネル攻撃, プライベートキー漏えいなど デバイスハッキング対応
	非認可不法機器搭載制限	• 生化学武器、爆弾テロによる社会的混乱対応体系樹立 • アンチドローン基盤の不法ドローン監視： 肉眼検知、検知、無線電波信号検知、レーダー検知
	物理的脅威緩和	• JTAG (Joint Test Action Group)無効化 • ドローンディフェンダー(電子機長形成によるドローン無力化)
技術的な側面	ソフトウェア改ざん対応	• MDC(Modification Detection Code)使用 • セキュア組込み、Secure Coding使用 • H.264基盤のリアルタイムストリーミング暗号化サポート DRM
	ドローン通信保護	• SSL, TLSなどの暗号化通信適用 • MAVSec (MAVLink + ChaCha20暗号化アルゴリズム)適用 • AES-CCMP認証、PRN除去及びRF相殺
	アクセス制御	• 無認証Wi-Fi基盤の不法的アクセス制限 • ドローンにアクセスする非認可ねっとぁーくの遮断
	データ保護	• 軽量化暗号アルゴリズム(HIGHLIGHT, LEAなど)適用

[表3]ドローンセキュリティ脅威に対する対応方法

07. 最後に

ここまでドローンを構成する構成要素及びセキュリティ脅威とこれに対応するための方法について調べてみた。最近第4次産業革命の重要技術が発展することによって超低遅延、超高速ネットワークの連携でドローン市場も急激な発展をしている。このような発展に反して連携性の強化で攻撃表面(Attack Surface)が増加することによってドローン環境のセキュリティ脅威も絶えずに増加している。

次世代融合技術の成長動力として注目されているドローン産業は未来物流と交通の重要要素でグローバル市場を先導するためには、総合的な観点とセキュリティを考慮したインフラ構築が必要である。特に製造及びサービス、コンテンツ融合でドローン市場の新しいビジネスモデルが創出され、モデル事業と規制サンドボックスを通じたネガティブ規制の緩和などで安全なインフラづくり及び技術底辺などの成長動力を図り、より安全な成長基盤を持っているドローン産業の活性化を期待する。

08. 参考資料

[1]
https://www.droneportal.or.kr/subList/20000000028
[2]
https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=118&ST=&SV=
[3]
https://ettrends.etri.re.kr/ettrends/138/0905001770/
[4]
https://www.korea.kr/archive/expDocView.do?docId=37916
[5]
https://biz.chosun.com/site/data/html_dir/2020/06/25/2020062503698.html
[6]
https://news.joins.com/article/21198765
[7]
https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EB%93%9C%EB%A1%A0%EB%B2%95