

民生ドローンのセキュリティリスクに関する研究

A study on security risks of consumer drones

惣島雅樹・法制倫理分科会・情報セキュリティ大学院大学

1. 背景

- 近年、無人航空機分野はその市場規模が著しく成長しており、2025年時点の日本国内の市場規模は5490億円に達すると見込まれている^[1]。
- その用途は、物流、防犯、農業、点検、土木・建設、空撮など幅広く、今後も市場規模は拡大していくことが予測される。
- このような状況の中で、日本国内では2022年に航空法が改正され、特に人命に影響を与えるような飛行を行う機体に対して、セキュリティを含む様々な要件を定めた機体認証等の制度が開始したが、2024年10月時点で認証済みの機体は6機種にとどまっている^[2]。

2. 先行研究等

- 民生のドローンには、GPS等を利用して事前に作成した飛行計画に従って自動飛行するもの、LTE通信等を利用して目視外から操縦を行うもの、Wi-FiやBluetoothなどを利用してスマートフォンから操縦を行うもの等があり、これまでの研究でGPSスプーフィング、ネットワークを経由した第三者の乗っ取り等の危険性が指摘されている。
- 例えば、VishalらはフランスParrot社のBepop2に対して、動作中に正規の操縦者のWi-Fi接続を排除し、第三者が制御を奪取することで、意図的に墜落させるなどの操作が可能であることを示した^[3]。
- さらに、Pixhawk/Ardupilotをはじめとして、ドローンに関するオープンソースのハードウェア/ソフトウェアのプロジェクトも発達しているが、これらについても十分なセキュリティ対策を実装することが求められる。

3. 今後の計画

- 民生ドローンのハードウェア構成、ソフトウェア構成を調査・整理し、セキュリティリスクの分析・課題の明確化を行う。
- 国内外のドローンのセキュリティに関する法律・規則を調査し、それらに準拠するようなセキュリティ対策を提案する。
- セキュリティ対策を実装したドローンを仮作し、セキュリティ性能を検証する。

[1] インプレス総合研究所 <https://research.impress.co.jp/topics/list/drone/685>

[2] 国土交通省 “型式認証を取得している無人航空機一覧(2024/10/22現在)” <https://www.mlit.go.jp/koku/content/001742208.pdf>

[3] Vishal Dey et al. "Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study." In Proceedings of the 31st International Conference on VLSI Design (VLSID), 2018, pp. 398–403.