【調査レポート】

ドローンの業務活用における セキュリティ対策の意識調査

一般社団法人セキュアドローン協議会

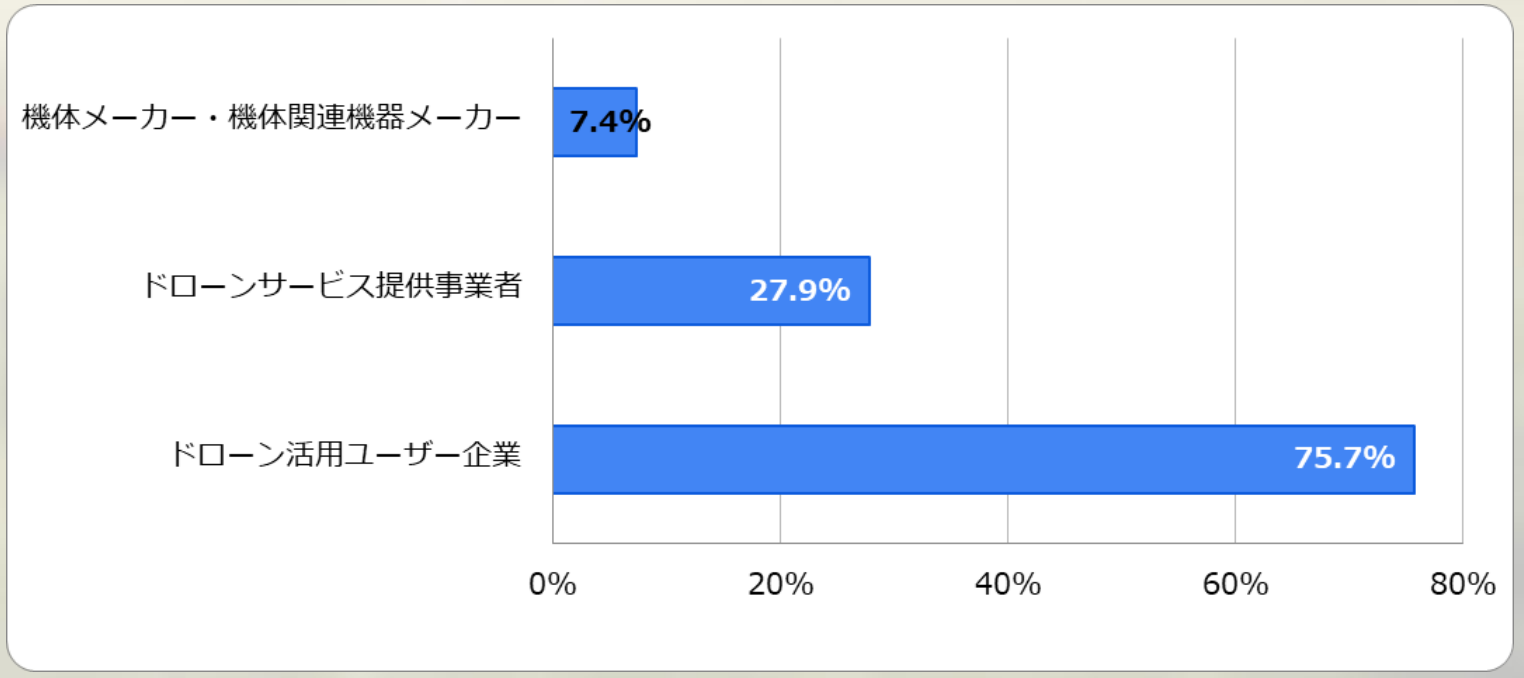
2023年12月6日

ドローンの業務活用におけるセキュリティ対策の意識調査

【実施期間】2023年11月1日(水)～11月17日(金)
【回答数】136件
【調査対象】

- 機体メーカー・機体関連機器メーカー
- ドローンサービス提供事業者
- ドローン活用ユーザー企業

【実施方法】インターネットによる調査



※複数回答

調査サマリーと考察

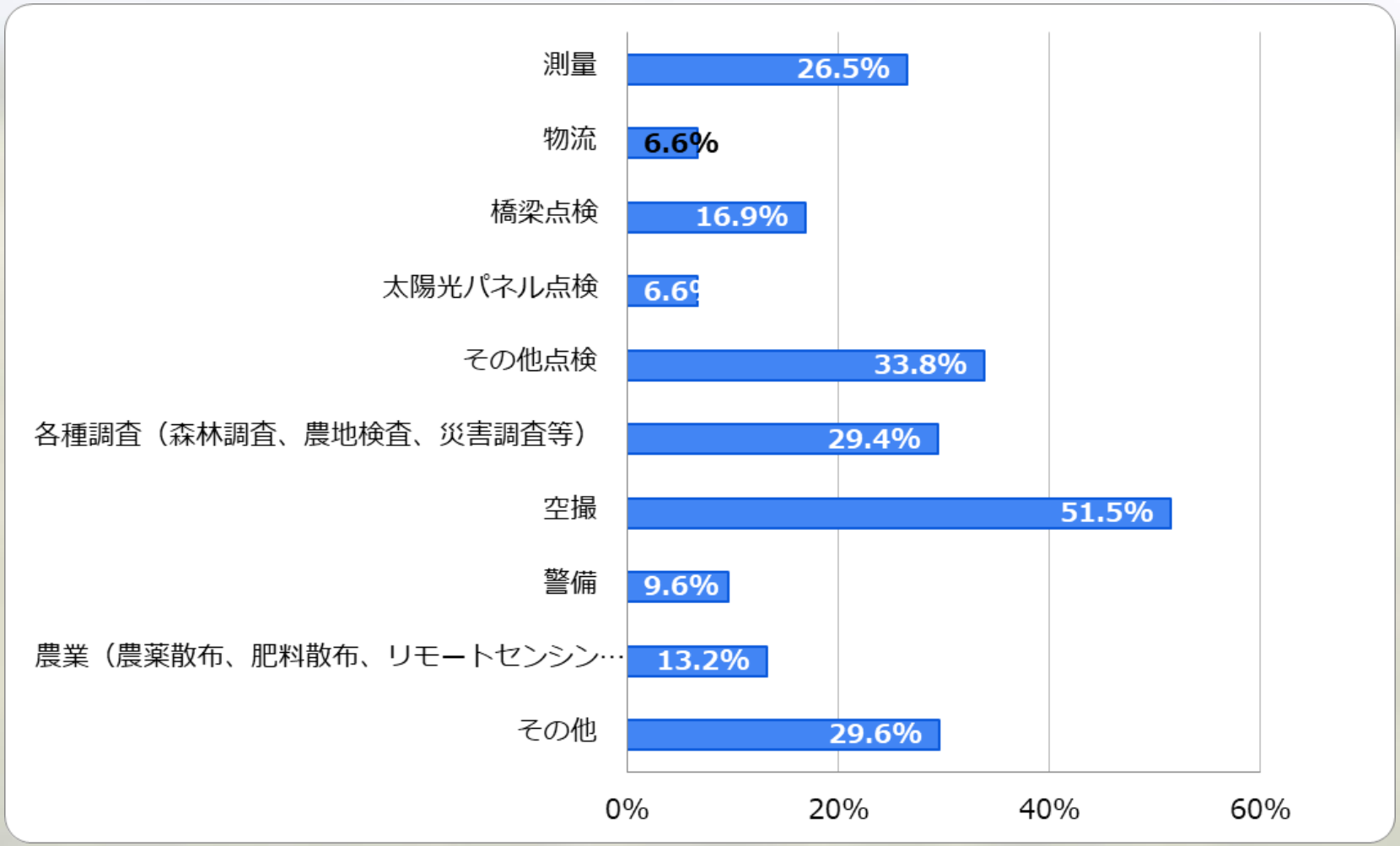
【調査サマリー】

- ドローンの業務活用において、セキュリティ対策は必要だと思うかの設問についての回答は、「とても必要だと思う：58.1%」「必要だと思う：39.7%」と大半の回答者が、ドローンのセキュリティ対策の必要性を認識している。
  しかし、ドローンのセキュリティ対策の実施については、「対策している：5.9%」「将来的な対策を検討している：16.2%」となり、ドローンのセキュリティ対策の必要性と実際の対策について大きなギャップがある結果となった。
- ドローンのセキュリティ対策における予算については、「予算をかけている：2.9%」「将来的に予算をかけることを検討している：27.9%」を、「予算をかけていない／予算がない：56.7%」が上回る結果となった。
- ドローンの業務活用において、「空撮：51.5%」が最も多く次いで「その他点検：33.8%」「測量：26.5%」となった。
- 携帯電話等の上空利用（LTE等）の回答では、「すでに使用している：7.4%」に留まり、「将来的な使用を検討している：43.4%」となった。「すでに使用している」と回答した方の内訳は、「遠隔操作：66.2%」「映像・画像送信：63.5%」が高い回答結果となっていた。
- その他の設問についての調査サマリーは、以下のような結果となった。
  - ドローンを業務活用するうえで、セキュリティ上の心配な点
    「電波障害・GPS障害：73.5%」「墜落：73.5%」「ドローンで取得した情報漏えい（各種ログや映像・画像データ等）：69.9%」「悪意ある第三者によるハッキング・乗っ取り：65.4%」「悪意ある第三者による脆弱性の悪用：45.6%」
  - ドローン機体本体、航行管理以外でサイバー攻撃の課題を意識して運用しているか
    「運用している：3.7%」「将来的な運用を検討している：16.9%」「運用していない：61.0%」「わからない：18.4%」
  - ドローンに実装するソフトウェアの脆弱性診断は実施しているか
    「実施している：2.2%」「将来的な実施を検討している：12.5%」「実施していない：51.5%」「独自のソフトウェア実装は行っていない：18.4%」「わからない：15.4%」
  - ドローンのファームウェアアップデート情報を定期的に確認しているか
    「確認している：62.5%」「確認していない：19.9%」「わからない：17.6%」

【考察】

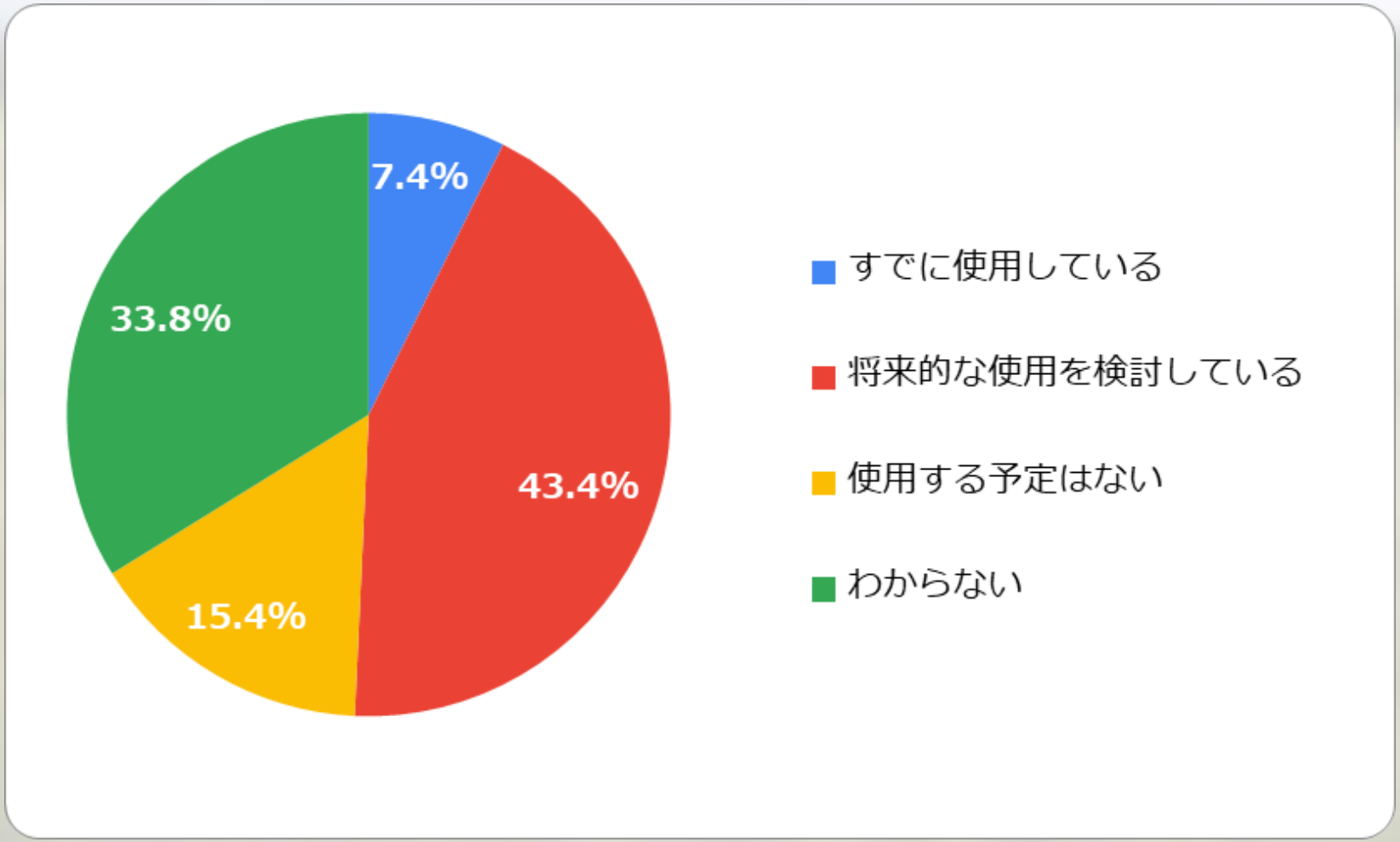
- 今回のアンケート調査では、「悪意ある第三者によるハッキング・乗っ取り」など、セキュリティ対策の必要性を認識する一方、実際の対策については、予算上の課題もあると見受けられ、経営層を含めたドローンのセキュリティ対策の重要性についての意識向上が必要ではないかと思われる。今後、セキュアドローン協議会では、このアンケートの結果内容を鑑みて、次版のドローンセキュリティガイドで、セキュリティ対策の具体的な内容や優先順位といった記載を掲載し、ドローンのセキュリティ対策が進んでいくことを支援していくことを考えている。

ドローンをどのような業務で活用していますか？

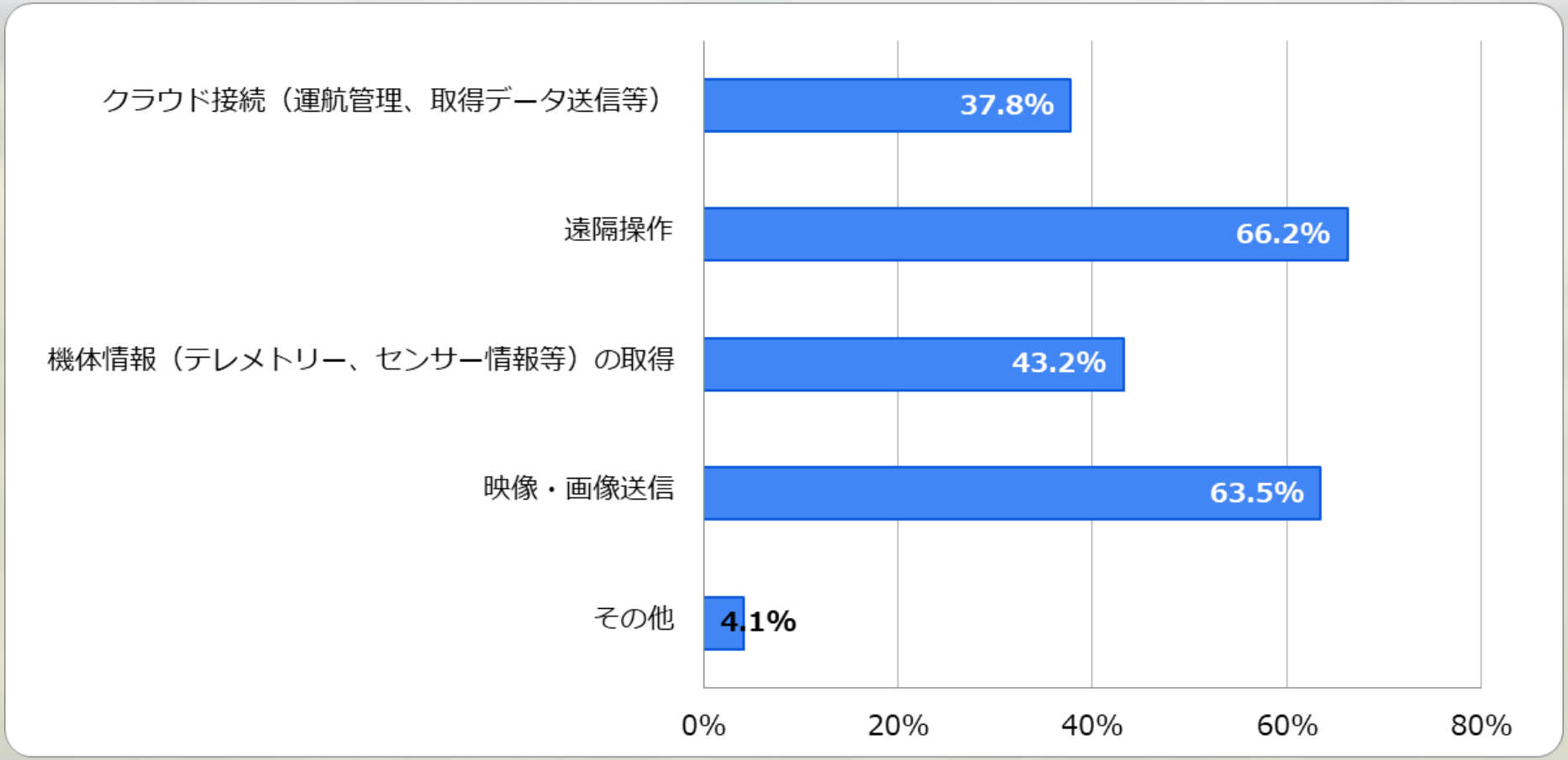


※複数回答

ドローンの業務活用において、携帯電話等の上空利用（LTE等）を使用していますか？もしくは、将来的な使用を検討していますか？

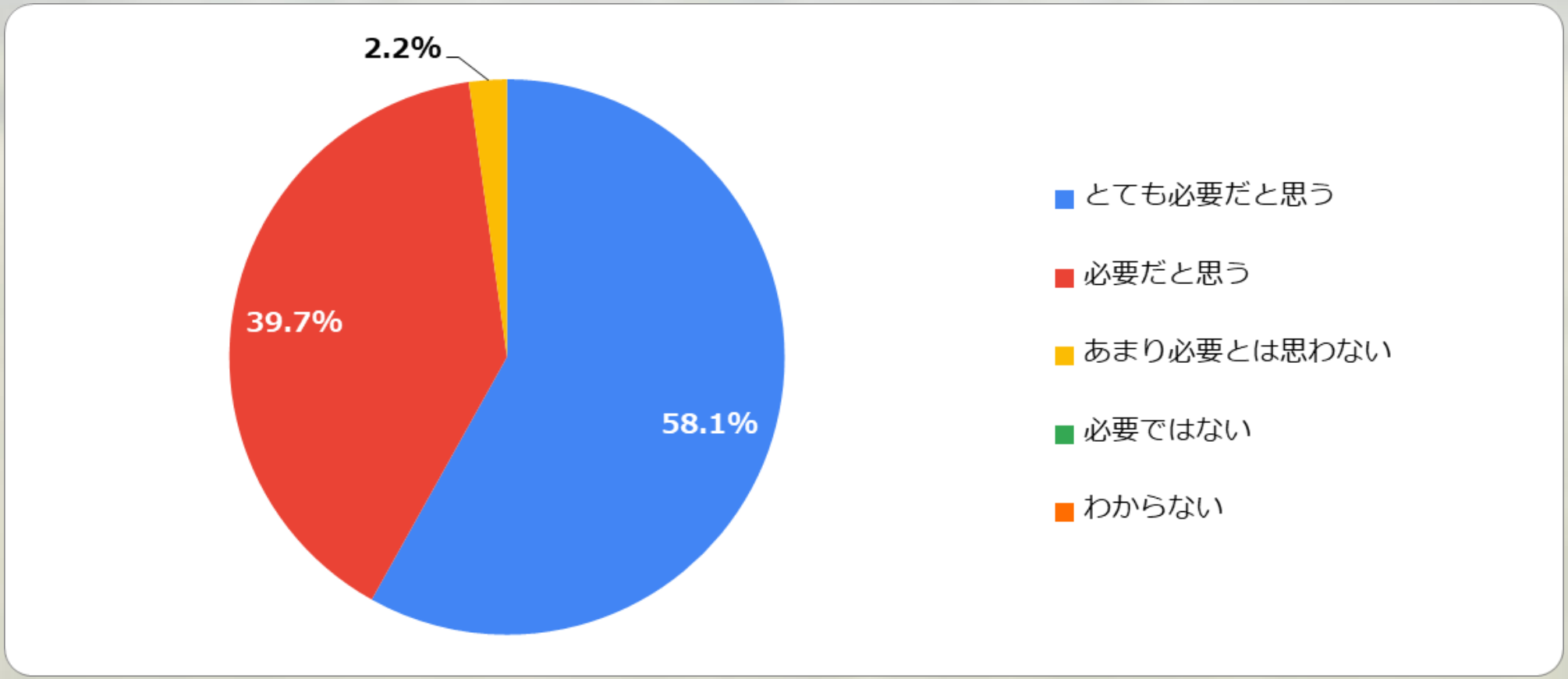


携帯電話等の上空利用（LTE等）を「すでに使用している」もしくは「将来的な使用を検討している」と回答された方は、どのような用途で使用していますか。もしくは使用する予定でしょうか？

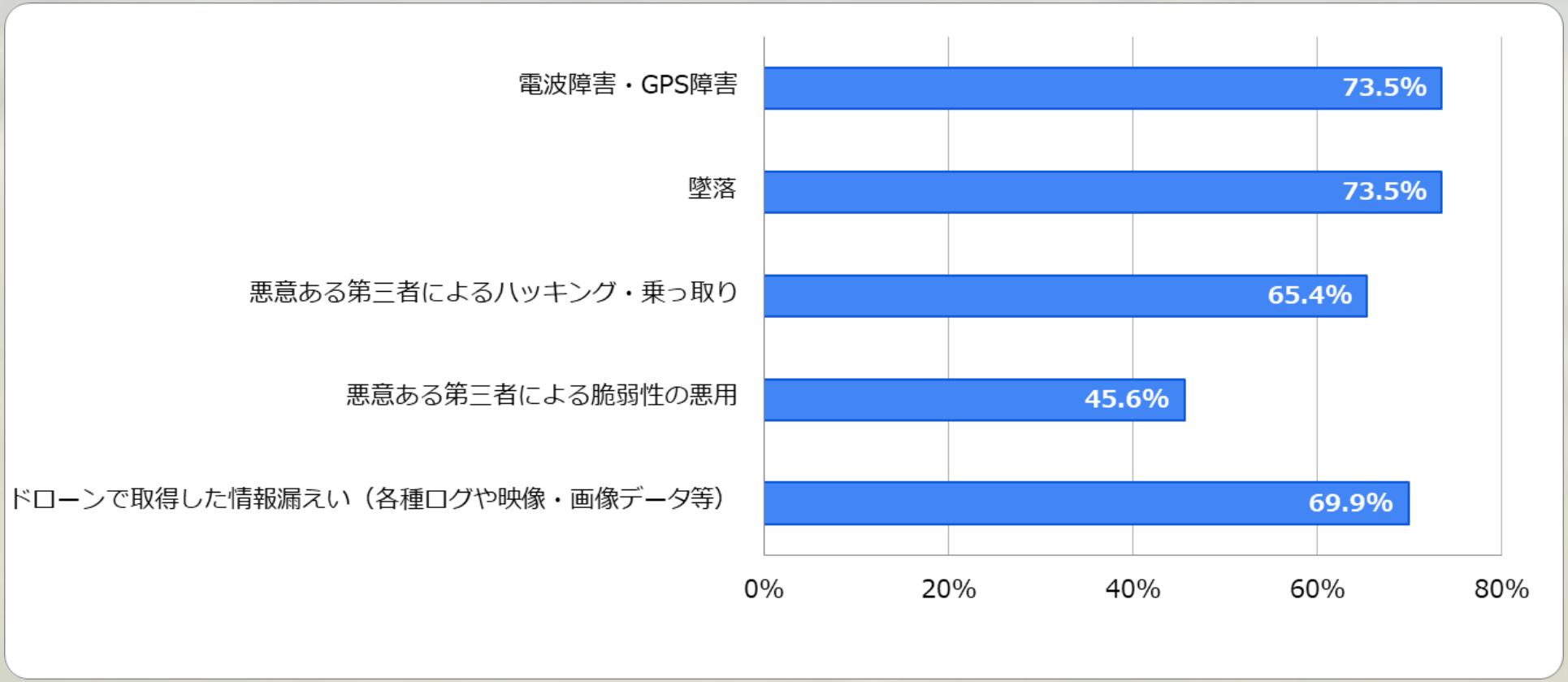


※複数回答

ドローンの業務活用において、セキュリティ対策は必要だと思いますか？

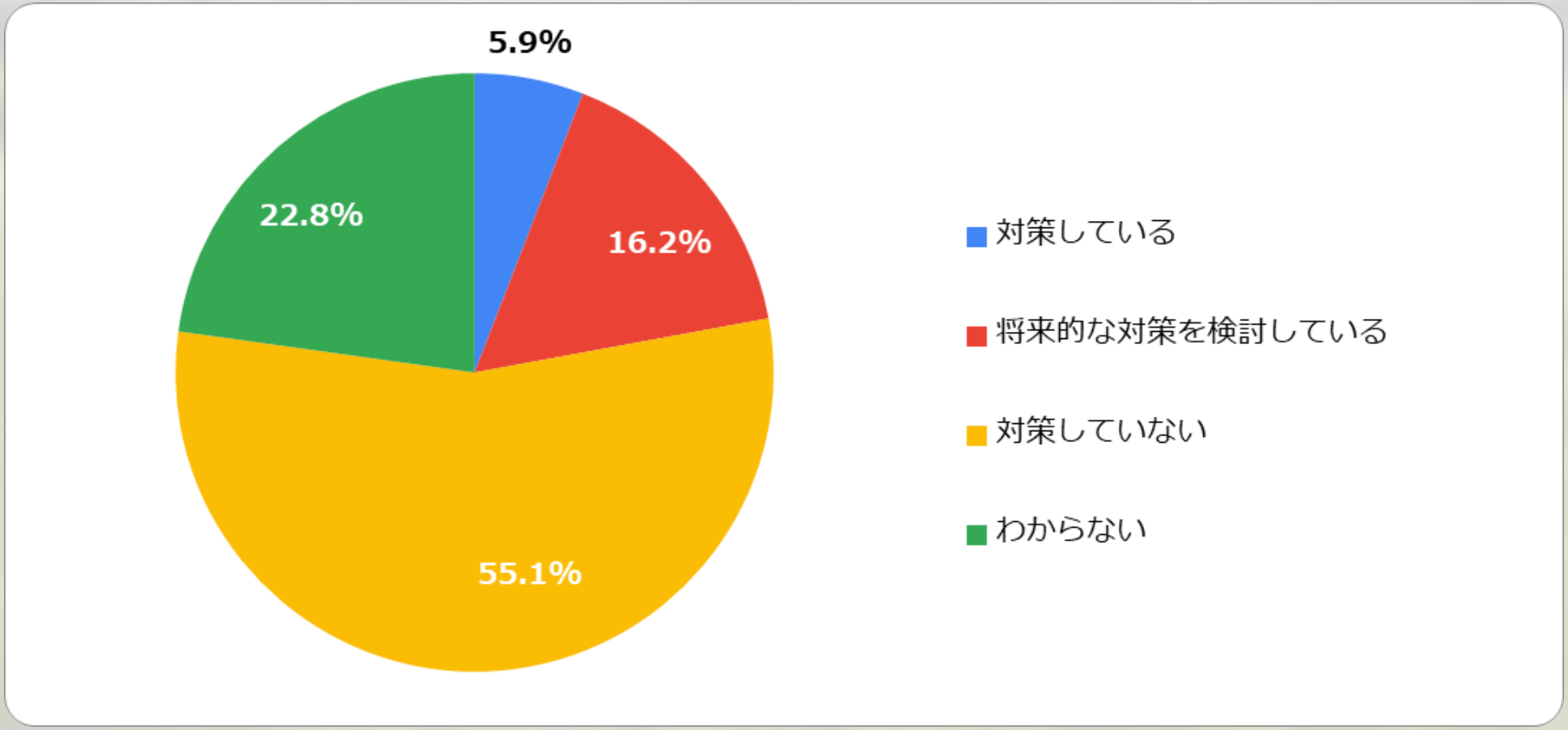


ドローンを業務活用するうえで、セキュリティ上で心配な点はありますでしょうか？



※複数回答

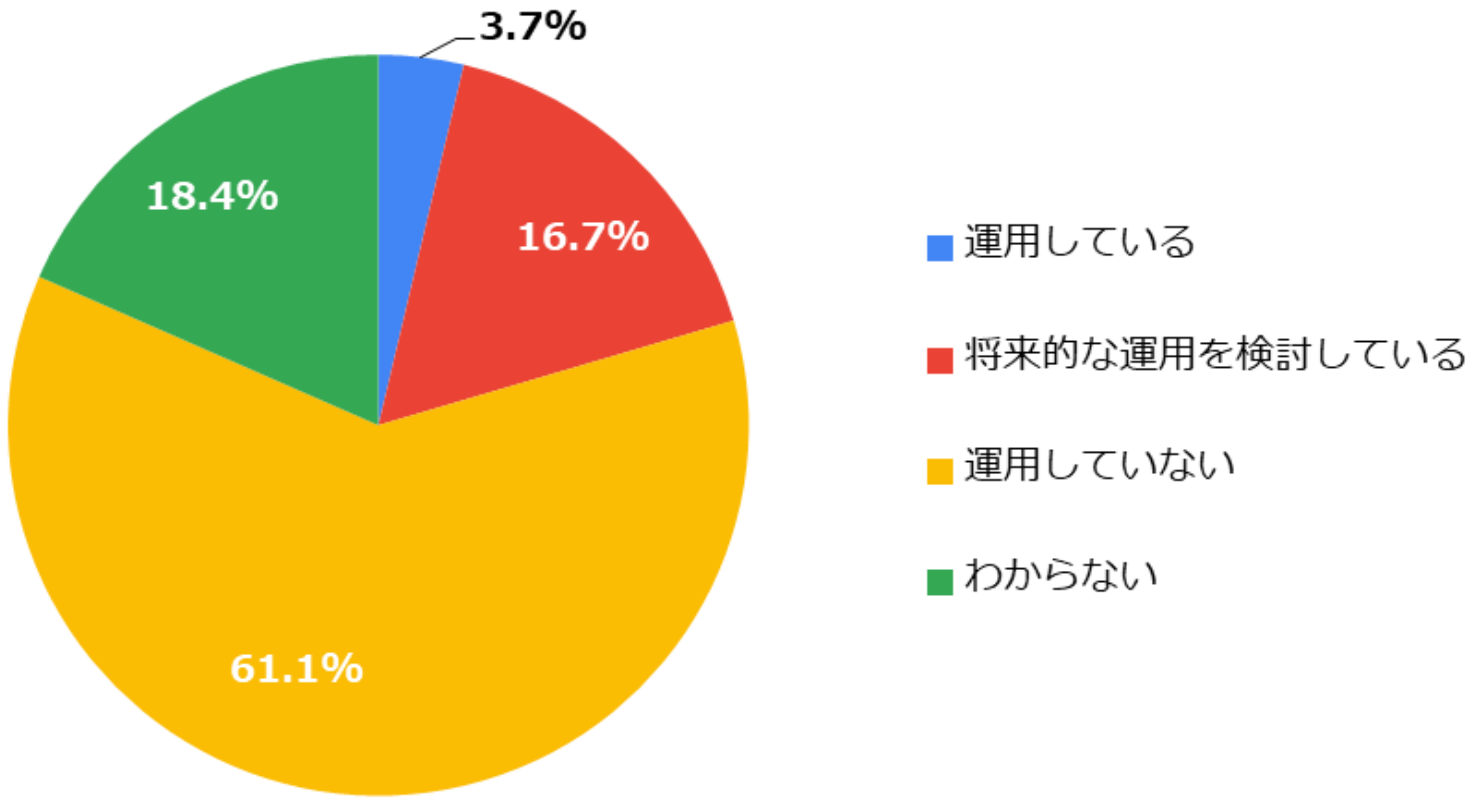
ドローンのセキュリティ対策は何か実施していますか？



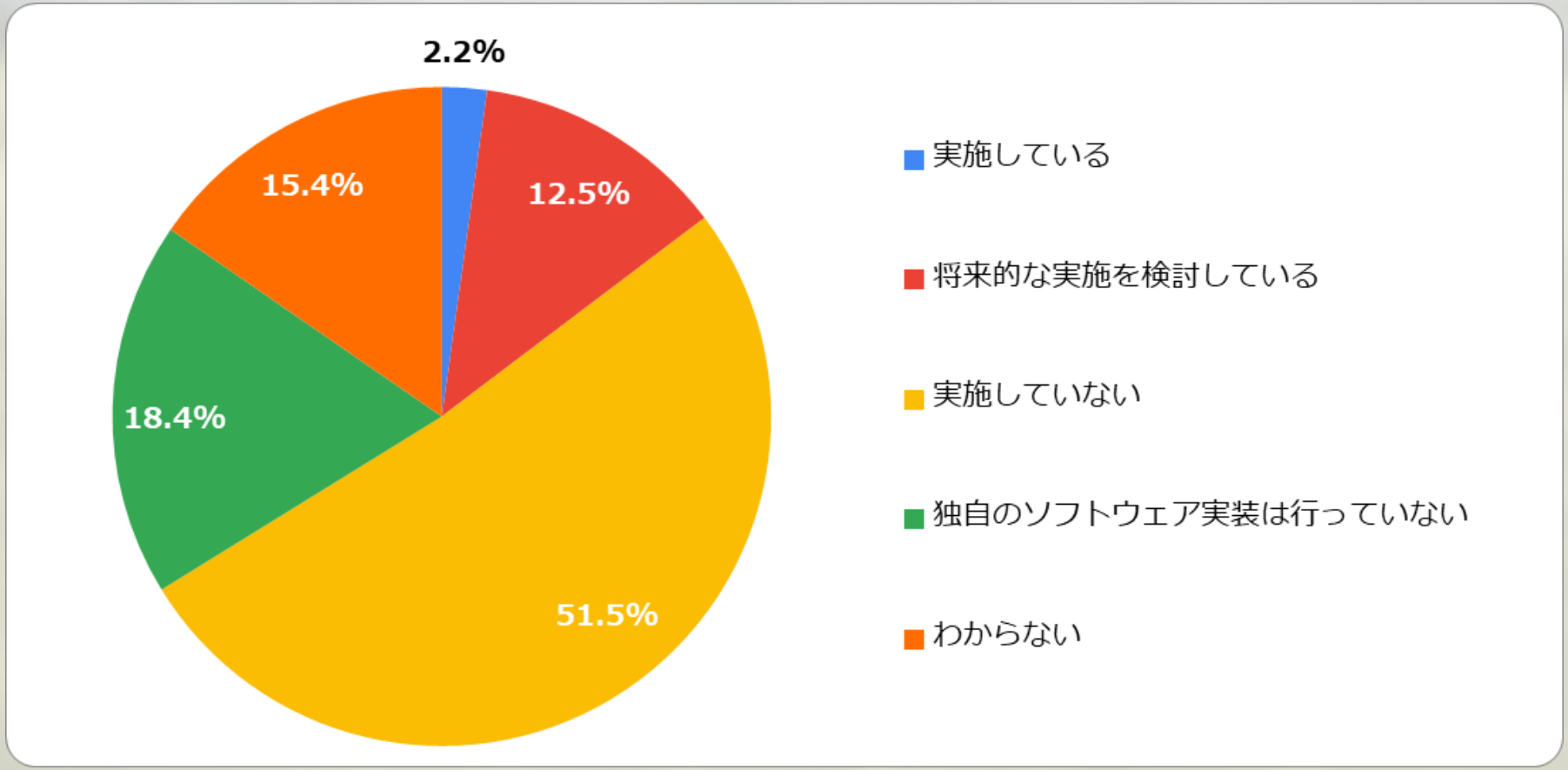
「対策している」もしくは「将来的な対策を検討している」と回答された方は、どのような対策を実施していますか？実施している対策の内容についてご記載ください。

撮影データを社内クラウドに保管し、SDカード等からは削除する
データの管理についてのセキュリティ方法についての情報取得
VPN接続を検討
国産のセキュリティ性の高い機体を採用している
ジャミングであったり、混信などによる操縦不能状態などについて出来る限りの対策を施したい。
暗号通信、ブロックチェーン技術の活用検討
事前調査し、安全と思われる会社にのみ発注する。
独自サーバーの設定
認証用サーバーの用意
セキュリティ、他社ドローン対策
補助者、立ち入り制限
フライトアプリのアカウントは共有しておらず、アカウントID、PASSは個人管理としてログは個人のみ確認出来る様にしている。
電波障害等はフライト時の送信機からの情報のみであるが、混線が多いようであれば飛行範囲の変更等で対応している。
係留方式にて飛行させている
データやログインにおける認証強化
データを機体SDカードに保存
国産などセキュアな機体への更新
セキュリティ対応のドローンを使用する
データ取得中は、ドローン企業サーバーに接続しない
通信の安定化を図るために、機器メーカー等と話を始めている
業界での一般的な対策
機体メーカー選定の検討
現在は出来ていないので、検討が必要と思っている
暗号化通信、機体認証
ガイドラインの作成
通信ポート制限、ファイアウォール、暗号化

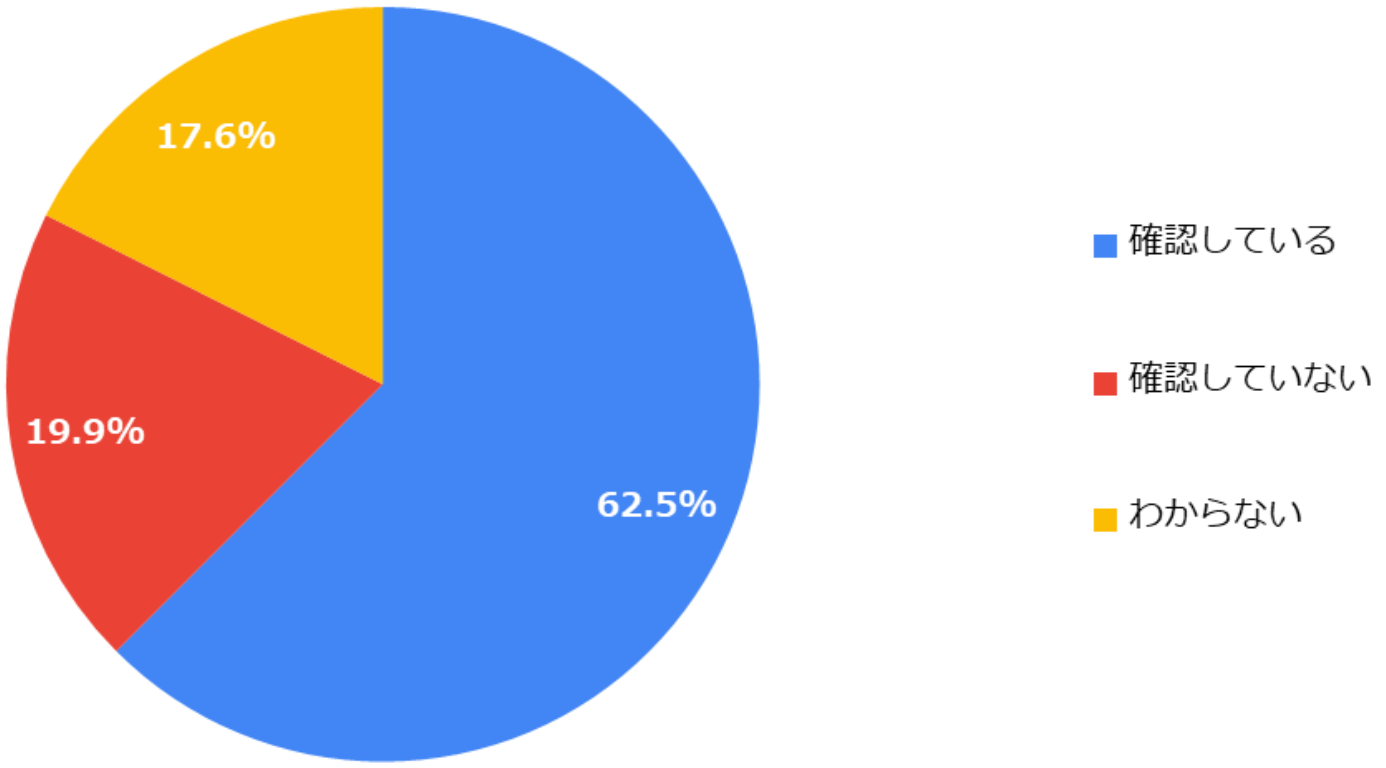
ドローンの業務活用において、ドローン機体本体、航行管理以外でサイバー攻撃の課題を意識して運用されていますか？



ドローンに実装するソフトウェアの脆弱性診断は実施していますか？



ドローンのファームウェアアップデート情報を定期的に確認していますか？



ドローンの業務活用において、セキュリティ対策のため予算をかけていますか？