米国の選挙に対する外国の悪質な影響力の脅威に関する情報共有を調整するための米国司法省の取り組みの評価

★ ★ ★

評価検査部

24-080

2024 年 7 月

エグゼクティブサマリー

米国の選挙に対する外国の悪質な影響力の脅威に関する情報共有を調整するための米国司法省の取り組みの評価

はじめに

米国の選挙の完全性を守ることは、法の支配を守り、国の安全を保ち、市民の権利を守るという米国司法省（DOJ）の全体的な使命の重要な要素である。 米連邦捜査局（FBI）は、「外国政府、非国家主体、またはその代理人による、破壊的、秘密（または宣言されていない）強制的、または犯罪的な活動であり、分断の種をまき、民主的なプロセスや制度を弱体化させ、外国人主体の戦略目標に有利なように政策や規制の決定を誘導するもの」と定義している。

2017 年 1 月、米国情報機関は、2016 年の米国大統領選挙に影響を及ぼそうとするロシアの努力は、"以前の作戦と比較して、直接的さ、活動のレベル、努力の範囲が著しくエスカレートしている "ことを示したとする評価を発表した。 同様に、2019 年の米上院情報特別委員会と 2018 年の米下院情報特別委員会は、ロシア政府が歴史的に米国の選挙への干渉を試みており、スピアフィッシング、ハッキング作戦、ソーシャルメディア・キャンペーンなどの戦術を用いて、各州の有権者登録データベースへの攻撃や政府や企業を標的としたサイバー作戦を通じて、2016 年の選挙への干渉を試みたことを一部認めている。 2017 年、FBI は、米国の選挙を標的にした作戦を含む、米国を標的にした「あらゆる悪質な外国の影響力作戦を特定し、これに対抗する」ために、外国影響力タスクフォース（FITF）を設立した。 司法省の国家安全保障局（NSD）と連邦検事局（USAO）は、FBI と協力して外国の悪質な影響力の脅威と戦っている。 さらに、司法省とその構成機関は、他の連邦政府パートナー、州、ソーシャルメディア企業と情報を共有し、米国の選挙に向けられた外国の悪意ある影響に対抗している。

司法省監察総監室（OIG）は、米国選挙に向けられた外国の悪意ある影響に関連する同省の情報共有システムの有効性を評価し、その対応に関する同省の監督と管理を評価し、この分野における同省の取り組みのギャップや重複を特定するために、本評価を実施した。 われわれは、2016 年の米国大統領選挙に向けられた外国の悪意ある影響力を受けて FITF が開発した同省の情報共有システムの側面を評価するため、ソーシャルメディア企業との同省の情報共有に焦点を当てた。

勧告

本報告書では、司法省が、米国の選挙に向けられた外国の悪意ある影響に対抗するために、憲法修正第 1 条の権利を保護する形でソーシャルメディア企業と情報を共有するための公的かつ戦略的なアプローチを取ることを確実にし、その結果、司法省に対する国民の信頼を強化するために、2 つの勧告を行う。

結果の概要

我々は、FBI が米国情報機関の他のメンバーとソーシャルメディア企業を巻き込んだ「情報共有モデル」を開発したが、司法省も FBI もソーシャルメディア企業との情報共有に適用される具体的なポリシーやガイダンスは持っていないことを明らかにした。　また、米国の選挙に向けられた外国の悪意ある影響に対抗することを任務とする司法省の各部門は、効果的に情報を共有していることもわかった。

同省は以前、ソーシャルメディア企業との特定のタイプの関わり方に関するガイダンスを欠いていた。

司法省も FBI も、2024 年 2 月まではソーシャルメディア企業との情報共有に適用される特定のポリシーやガイダンスは持っていないことがわかった。

われわれが現地調査を行った時点では、FBI は「情報共有モデル」によって、米国の選挙に向けられた外国の悪質な影響力に関する情報を共有していた。情報共有モデルとは、FBI が他の米国情報コミュニティ機関から外国の悪質な影響力行為者に関連する情報を入手し、その情報をソーシャルメディア企業と共有するものである。場合によっては、各社は自社のプラットフォームでのさらなる活動を調査することを選択したかもしれない。司法省が取得した裁判所命令を受け、各社は FBI に情報を提供することができた。　その結果、新たな手がかりが得られる可能性があり、FBI の作戦活動に役立ち、企業と共有できる追加情報を特定できる可能性がある。

FBI 職員によると、具体的な方針や指針がない場合、FBI の情報共有方法は「行為者主導かコンテンツ主導か」というアプローチに基づいているという。　司法省と FBI の関係者によると、FBI は外国の悪意ある影響力に関連するソーシャルメディアコンテンツを監視しておらず、オンライン上で拡散された特定のシナリオを調査することもないという。　FBI は、外国の悪質な影響活動を特定するためにオンラインコンテンツを利用するのではなく、進行中の捜査の中で開発された、または特定の外国人行為者の活動に関する他の連邦機関から受け取った情報に基づいて行動していると、私たちは述べた。　しかし、文書調査の結果、外国人行為者がソーシャルメディア活動で特定のテーマや物語を宣伝する予定であることを示す情報を FBI が得た場合、FBI は「コンテンツ」情報を共有していることも分かりました。　FBI は、FBI から提供された情報を評価し、顧客が各社の利用規約に違反したことに基づいて何らかの措置を講じるかどうかを判断するのは、ソーシャルメディア企業に依存していると述べている。

また、米国の選挙に向けられた外国の悪意ある影響に関するソーシャルメディア企業との関わり方について、同省には包括的な戦略がなく、その結果リスクに直面していることも分かった。　具体的には、FBI は多くのソー

シャルメディア企業が拠点を置くサンフランシスコ地域のソーシャルメディア企業とは関係を維持しているが、同地域以外のソーシャルメディア企業とは継続的な関係を築いていない。　さらに、外国資本のソーシャルメディア・プラットフォームの拡大や、米国の選挙に向けられた外国の悪意ある影響力キャンペーンを支援する可能性のある新技術の開発など、新たな脅威に直面していることが分かった。

FBI のモデルとアプローチはこの枠組みを整えたが、それにもかかわらず、ソーシャルメディア企業が言論の場を提供しているという事実から生じる固有のリスクがある。　FBI がソーシャルメディア企業と外国の悪意ある影響力の脅威に関する情報を共有するだけでは、憲法修正第 1 条への明白な影響はないが、その情報が、そのプラットフォームで参加する人々の言論を制限または排除するような方法で、共有された情報に基づいて行動するよう企業を説得することを目的とした強制または重大な奨励を構成すると合理的に認識され得るような方法で伝達された場合、懸念が生じる可能性がある。　司法省と FBI は 2024 年 2 月に新しい標準業務手順書（SOP）を発表し、このリスクを認め、軽減するための措置を講じた。　私たちは、この SOP とそれが憲法修正第 1 条の権利をどのように保護するのかを一般に知らせる方法を特定することが、司法省と FBI に対する国民の信頼を強化することになると考える。

NSD、USAO、FBI 各支部は、米国の選挙に対する脅威を伴う海外からの悪質な影響力案件に関する情報を効果的に共有している。

われわれは、米国の選挙に向けられた外国の悪意ある影響に関する情報を共有することを任務とする司法省の 3 部門内および部門間で、効果的な調整が行われていることを発見した。　司法省内では、米国の選挙に向けられた外国の悪質な影響力に関する調整は、外国の悪質な影響力と闘うための司法省の全体的なアプローチについて決定する戦略的な事件管理レベルと、FBI 捜査官、連邦検事補、NSD 弁護士が個々の事件の捜査と起訴について毎週調整する事件捜査レベルの両方で行われている。　われわれが話を聞いた司法省の 3 部局の職員は、米国の選挙に向けられた外国の悪質な影響力に関する司法省内の情報共有関係について、肯定的な見解を示した。

目次

エグゼクティブサマリー ii

目次 v

はじめに 1

背景 2

OIG 評価の目的と範囲 7

評価結果 9

同省は以前、ソーシャル メディア企業との特定のタイプの関わり方に関するガイダンスを欠いていた。 ... 9

NSD、USAO、FBI の各支部は、米国の選挙に対する脅威を伴う外国の悪質な インフルエンス事件に関する情報を効果的に共有している。 25

結論と勧告 29

結論 29

勧告 30

附属書 1：目的、範囲、方法論 31

規格 31

目的と範囲 31

方法論 32

附属書 2：対外影響タスクフォースの任務、構造、発展、および FBI サイバー課の役割 34

対外影響タスクフォースの使命と構造 34

FITF 設立の背景 34

FITF における FBI サイバー部門の役割 34

附属書 3：FBI が情報を共有するために利用できるデータベースとシステム 36

FBI 公式記録システム 36

連邦機関以外との情報共有方法 37

米国政府内の情報共有方法 38

一般からの情報受信方法 40

附属書 4：選挙犯罪に対抗する司法省の任務の概要 41

附属書 5：司法省による他の連邦政府機関および州政府関係者との選挙関連情報共有 42

国土安全保障省との調整 42

他の連邦政府機関との調整 43

州政府関係者との調整 43

附属書 6．外国の悪質な影響に対抗する司法省の使命に関連する法律と政策の説明 45

合衆国憲法修正第 1 条 45

法令 45

大統領令 46

司法省の方針 47

FBI の方針 48

附属書 7：報告書草案に対する同省の回答 51

附属書 8：同局の回答に対する OIG の分析 58

はじめに

米国の選挙の完全性を守ることは、法の支配を守り、国の安全を保ち、市民の権利を守るという米国司法省（DOJ、Department of Justice）の全体的な使命の重要な要素である。 さらに、司法省の戦略計画によれば、司法省は、外国の悪意ある影響力活動を含む、米国の国家安全保障に対する脅威を調査し、破壊し、訴追する責任を負っている。 選挙は州やその自治体によって管理されているが、司法省は選挙に向けられた外国の悪質な影響力活動を調査する第一の責任を負っている（本文欄参照）。

米国を標的にした外国の悪意ある影響力に関する懸念は、1796 年の有名な告別演説でジョージ・ワシントン大統領が "陰湿な...外国の影響力 "に警告を発した、我が国の建国にまで遡る。 外国諸国は何世紀にもわたって米国を標的とした悪質な影響力キャンペーンを行ってきたが、こうした取り組みは近年、特に 2016 年の大統領選挙中とそれ以降、斬新な形をとっている。 2017 年 1 月、米国情報機関は、ロシアの 2016 年大統領選挙への影響力行使は、"以前の作戦と比較して、その直接的さ、活動のレベル、努力の範囲が著しくエスカレートしている "とする評価を発表した。[1]

同様に、2019 年の米上院情報特別委員会と 2018 年の米下院情報常任特別委員会は、ロシア政府が歴史的に米国の選挙に干渉しようと試みており、スピアフィッシング、ハッキング作戦、ソーシャルメディア・キャンペーンなどの戦術を用いて、各州の有権者登録データベースへの攻撃や政府や企業を標的にしたサイバー作戦を通じて、2016 年の選挙に干渉しようとしたことを一部認定した。 2019 年、米国議会は国家情報長官室に対外悪質影響センターを設置した。 その 2 年前、米連邦捜査局（FBI）は、米国を標的にした作戦など、米国を標的にした「あらゆる悪質な外国影響工作を特定し、これに対抗する」ために、外国影響工作部隊（FITF）を設立していた。

外国の悪影響

FBI は、外国の悪意ある影響力を、「外国政府、非国家主体、またはその代理人による、破壊的、秘密（または宣言されていない）、強制的、または犯罪的な活動であり、分断の種をまき、民主的なプロセスや制度を弱体化させ、政策や規制の決定を外国主体の戦略目標に有利に、敵対国に不利になるように誘導するもの」と定義している。

出典 FBI 訓練資料

選挙 FBI、国家安全保障局（NSD）、連邦検事局（USAO）の 3 つの部局は、こうした外国の悪意ある影響力の脅威と闘うという司法省の使命を追求するために協力している。 さらに、同省とその構成機関は、米国情報

[1] 米国の情報コミュニティは、18 の行政機関（国家安全保障局、中央情報局、FBI など）と、外交関係の遂行と米国の国家安全保障の保護に必要な情報活動を個別に、あるいは協力して行う組織で構成されている。 詳細については、国家情報長官室（ODNI）, "Members of the IC", www.dni.gov/index.php/what-we-do/members-of-the-ic （2023 年 10 月 11 日アクセス）を参照のこと。

コミュニティ、米国国土安全保障省（DHS）、米国財務省、州・地方政府、民間企業（ソーシャルメディア企業など）など、司法省以外の組織と連携し、外国の悪質な影響力の脅威に関する情報を共有している。

監察総監室（OIG）は、米国の選挙に向けられた外国の悪意ある影響に関連する同省の情報共有システムの有効性と回復力を評価し、米国の選挙に向けられた外国の悪意ある影響への対応に関する同省の監督と管理を評価し、この分野における同省の取り組みにギャップや重複がないかを確認するために、この評価を実施した。

背景

外国の悪影響

外国の悪意ある影響力は、多くの形態や戦術をとり、外国人行為者や目的によって異なる場合がある。 FBI によると、外国の悪意ある影響とみなされるには、外国人行為者または代理人に関連した活動でなければならず、米国の利益を犠牲にして外国のアジェンダを計画、推進することも含まれる。 外国による悪質な影響活動は、戦略的な地政学的目標を達成するために、外国の権力者が米国の政策に影響を与えたり、政治的感情や言論を歪めたり、民主的プロセスや価値観に対する信頼を損なったりする行為である。 対外的な影響力活動には、さまざまな外国の活動が含まれるが、FBI が捜査の対象とするのは、こうした活動の破壊的、未申告、犯罪的、強制的な性質である。 このような活動の例としては、メディア記事の秘密裡の掲載、便宜を図るための経済的強制、贈収賄、脅迫、サイバー侵入、選挙資金違反、分裂団体へのあからさまな資金提供などがある。

誤情報

敵対者は虚偽または誤解を招く情報を使用する。 敵の意図によって、誤情報が偽情報に変わることがある。

偽情報

敵対者は、意図的に作成または拡散された虚偽または誤解を招く情報を利用し、特定のターゲットオーディエンスの態度や行動を変化させ、情報の作成者に利益をもたらす。

出典 国家情報会議

外国の悪意ある影響力は米国社会のあらゆる側面を標的にしているが、司法省は「選挙は、指導者を選ぶプロセスという民主主義の中核的要素に対する信頼を損なう機会を提供するため、外国の影響力キャンペーンにとって特に魅力的な標的である」と述べている。[2] 選挙に向けられた外国の悪意ある影響活動は、選挙インフラや政治キャンペーンを標的としたサイバー活動、政治団体やキャンペーンを支援したり害を及ぼすことを目的とした秘密影響活動、不和の種まきを目的とした誤報・偽情報キャンペーン、不正な選挙資金スキーム、外国代理人登録法（FARA）および関連法の違反など、さまざまな形態をとる可能性がある（政府の誤報・偽情報の定義についてはテキストボックスを参照）。

[2] DOJ, Report of Attorney General's Cyber Digital Task Force (July 2018), Chapter 1, page 2.

連邦捜査局

FBI は、対外的な悪意ある影響活動を調査する主導機関である。 FBI 本部では、FITF が米国を標的とする外国の悪意ある影響活動に関する調査を特定し、監督している。 このセクションでは、FITF の創設と現在の役割、および FBI のサイバー部門と現場事務所が果たす補完的役割について説明する。

海外影響力タスクフォース

2017 年、FBI は 2016 年の米大統領選におけるロシアの悪質な影響力を直接のきっかけとして、防諜部内に FITF を創設した。[3] 防諜部門の前課長補佐は、FITF には防諜、サイバー、犯罪捜査の経験を持つスタッフが集まり、外国の悪意ある影響による選挙の脅威に取り組んだと説明した。 2018 年の中間選挙後、FBI は FITF の有効性を見直し、タスクフォースをロシアを拠点とする外国の悪質な影響力のみに焦点を当てたものから、中国、イラン、その他の世界的な敵対国からの外国の悪質な影響力行為者を含むものへと拡大した。[4] この拡大以降、FITF は全般的に対外悪意影響に焦点を当て、対外悪意影響選挙業務は全体の業務量のごく一部を占めるにすぎない。

捜査の観点から、FITF プログラム・マネージャーは、米国の選挙に対する脅威を含む、外国の悪意ある影響力を扱う防諜事件を、FBI の 56 の現場事務所全体で監督している。 FITF プログラム・マネージャーは、他の FBI 本部の部署や支局の担当者と協力し、事件の対立を解消し、事件のすべての重要な出来事の調整と追跡を確実にし、外国の悪意ある影響力の脅威に関する情報を共有する。 これらのプログラム・マネージャーはまた、FBI のパートナーである米国情報機関のリエゾンとも連携している。

---

[3] 防諜部が管理する FBI の防諜任務は、米国における外国情報活動の摘発、防止、調査である。 この任務には、「わが国の国益に悪影響を及ぼす米国に関する情報を収集するため、人的手段（スパイなど）や技術的手段（ハッカーなど）を用いる外国の諜報機関や組織の行動を探知し、合法的に対抗すること」が含まれ、米国の選挙に向けられた外国の悪意ある影響に対抗することも含まれる。

[4] さらに最近、議会は 2019 年 12 月に ODNI 内に対外悪質影響センター（FMIC）を設立した。 その議会憲章によると、FMIC は "選挙の安全保障を含む、外国の悪意ある影響力に関連する、保有または取得したすべての情報およびその他の報告を分析し、統合するための米国政府の主要組織として機能する"。 ODNI のウェブサイトによれば、FMIC は FBI や他の連邦機関と提携し、外国の悪意ある影響力の脅威に対する認識を促進している。 FMIC は 2022 年 9 月に発足し、本報告書で後述する 2019 年に設立された ODNI 選挙脅威執行部の後継組織とされている。

FBI は FMIC の発足と同時に FMIC と関わりを持ち始め、以前は選挙脅威対策本部と関わっていた。 FBI は現在も FMIC のスタッフとの交流を続けているが、これらの交流は特定のガイダンスや法律の指示によるものではない。 今回の評価では、2022 年における FBI の活動を調査していないため、FBI と FMIC との交流は評価しなかった。 我々の評価範囲の詳細については、附属書 1 を参照されたい。

サイバー部門

サイバー課が管理する FBI のサイバー任務は、サイバー攻撃とサイバー侵入の捜査である。 選挙に特化すると、サイバー部門は、政治キャンペーン、州の選挙インフラ、選挙機器の民間ベンダーを標的にした攻撃など、米国のコンピュータネットワーク上でのサイバー攻撃や違法行為を調査する。 サイバー部門は、選挙を保護するために、調査、情報、インシデント対応のリソースを使用している。[5] サイバー課の任務と FITF との違いについての詳細は、附属書 2 を参照のこと。

現地事務所

FBI の捜査のほとんどは、全国にある 56 の FBI 支局で行われる。 FBI 支局には防諜班とサイバー班があり、FBI 本部の対応部署が管理する捜査を担当し、他の捜査や米国情報機関の優先事項との戦略的な監視と牽制を図っている。

方針に従い、FBI の各支部は、FBI の捜査上の必要性を促進するため、担当地域内での関係を維持している。これには、州および地方政府、選挙関係者、法執行機関、民間団体、一般市民との協力が含まれる。 選挙犯罪に対抗する司法省の任務の詳細については、附属書 4 を参照のこと。 州政府関係者との DOJ の選挙関連情報共有については、附属書 5 を参照のこと。

その他の司法省構成機関

国家安全保障部

司法省の NSD の使命は、法の支配に則り、あらゆる国家安全保障上の脅威から米国を守り抜くことである。NSD は、一方では連邦検察官と FBI、他方では他の米国情報コミュニティ機関の間で、より大きな連携を確保するように設計されている。 NSD の防諜・輸出管理部門は、FARA 違反を含む外国の影響・干渉事件の起訴において米国内務省を支援し、一方、法律・政策部門は、外国の悪意ある影響に対抗するための司法省の政策策定の主要な結節点として機能している。 本報告書の草稿のレビューに対し、同省は、NSD が 2023 年 6 月に国家安全保障サイバー課を設立したことを報告した。 このセクションは現在、主に、ソーシャルメディア・プラットフォームを含むオンライン・プラットフォームが犯罪の実行の中心となっている犯罪など、「サイバー対応」された外国の影響・干渉事件の捜査・起訴を担当している。

---

[5] サイバー部門はまた、Private Industry Notification (PIN)や FBI Liaison Alert System (FLASH)報告書を用いて、重要インフラ部門に対する脅威に関するサイバー脅威情報をタイムリーに民間部門パートナーに通知している。 サイバー部門は、連邦政府が民間企業と共有するサイバー脅威情報の量、質、適時性を高めることを義務付けた大統領令 13636 に対応して、PIN と FLASH レポートを作成した。 これらの報告書の詳細については、附属書 3 を参照のこと。

連邦検事事務所

USAO は、全国 94 の連邦司法地区で捜査と起訴を行い、連邦法を執行する。 NSD と連携して、USAO は以下に述べるように、法的手続きを開始する際に FBI 支部を支援する。 USAO は最終的に、NSD と協議の上、対外悪意影響事件で刑事告発を行うかどうかを決定する。

DOJ 以外のパートナー

FBI は、国家安全保障局（NSA）など米国情報機関のパートナーと協力し、米国の選挙に対する外国の悪質な影響力の脅威に関する情報を共有している。 米国情報コミュニティーのパートナーは、米国の選挙や利害関係者に向けられた外国からの悪質な影響に関する FBI の捜査に役立つ可能性のある情報を、現在行っている情報収集活動から開発したものを FBI に提供している。 一例として、FBI は、米国防総省のサイバー司令部から外国の悪質な影響力キャンペーンに関する情報を送受信し、米国財務省と協力して、そのようなキャンペーンに関与する外国行為者に対する制裁を求めている。 さらに FBI は、外国の悪質な影響力と闘うという任務において DHS と連絡を取り合っており、DHS のサイバーセキュリティ＆インフラセキュリティ局はその主要なパートナーである。

選挙は州によって管理されているため、FBI は、米国の選挙に対する外国の悪質な影響力の脅威に関する情報を州政府と共有する必要がある場合がある。 しかし、選挙セキュリティに関する連邦政府の主要パートナーは DHS であるため、外国の悪質な影響力対策に関する FBI と州政府との交流は限られている。 FBI が外国の悪質な影響力の脅威に関する情報を州と共有する場合、共有されるのは通常、州の選挙システムに対するサイバー脅威に関するものである。 司法省の他の連邦政府機関や州政府関係者との選挙関連の情報共有に関する詳細は、附属書 5 を参照のこと。

法的・政策的枠組み

以下では、米国の選挙に向けられた外国の悪質な影響力に関する情報を共有するための DOJ の取り組みの指針となる、いくつかの既存の方針について説明する。[6] また、DOJ が外国の悪質な影響力の捜査で使用できる、あらゆる種類の連邦刑事事件の捜査で使用されるいくつかの法的手段についても説明する。 これらの政策と手段、および DOJ の対外的な悪意ある影響に関する業務に関連するその他の法律と政策については、附属書 6 でさらに詳しく説明する。

---

[6] 本報告書の草稿を検討した際、FBI は機密扱いの別のポリシーの存在を指摘した。 この方針は FBI が所有するものではなく、情報機関のメンバーが憲法上の保護を遵守した方法でソーシャルメディア関連データを分析するための原則とガイドラインを確立するための省庁間プロセスを通じて策定されたものである。

大統領令 12333-米国の諜報活動

大統領令（E.O. ）12333 は、1981 年に発布され、その後数回の大統領令によって改正されたもので、米国情報共同体を設立し、FBI を含む米国情報共同体機関の目標、方向性、任務、責任を定めている。 これらの責務のひとつは、適用される法律と大統領の指針に基づき、完全かつ自由な情報交換を可能にする方法で、情報を準備し提供することである。

行政府の通知の枠組み

2019 年、連邦政府は、米国の国家安全保障と選挙の完全性を守るために必要な場合、米国の選挙に影響を与えようとする外国の秘密工作について、連邦議会議員、州・地方政府関係者、民間団体、一般市民への通知を確実に行うための枠組みを採択した。 この枠組みは、サイバー侵入やその他の犯罪行為を含む、外国による干渉の被害者に通知するための既存の法的・政策的要件を補完するものである。 この枠組みによると、選挙インフラを含む重要インフラに関する通知は DHS が、それ以外の通知は FBI が担当する。[7] 連邦政府機関が米国の選挙に向けられた外国の干渉キャンペーンを特定した場合、国家情報長官室（ODNI）が組織し、米国の選挙に影響を与えようとする外国の試みを評価する任務を負う省庁間グループに通知することが義務付けられている。[8]

司法省の方針

司法マニュアルは、外国影響活動の開示に関する司法省の方針を示している。 司法マニュアルは、適切かつ司法省の方針と慣行および米国の国家安全保障上の利益に合致する場合には、外国影響活動の被害者および無意識の標的に警告を発することが司法省の方針であると述べている。 捜査上または運用上の懸念から、すべての対外的影響活動を開示することが不可能な場合があることを認識した上で、司法マニュアルの第 9-90.730 節は、逮捕や告発を支援するため、被害者に警告するため、関連する議会委員会に通知するため、一般市民またはその他の影響を受ける個人に警告するためなど、そのような活動を開示する可能性のあるいくつかの理由を概説している。

---

[7] DHS は、16 の重要インフラ部門を特定した。その資産、システム、ネットワークは、物理的か仮想的かを問わず、米国にとって極めて重要であり、その機能停止や破壊は、国家安全保障、経済安全保障、公衆衛生もしくは安全、またはそれらの組み合わせに衰弱的な影響を及ぼすと考えられている。 これらのセクターのひとつである政府施設には、選挙を管理し結果を報告するために使用される物理的、電子的、技術的リソースが含まれる。

[8] FBI と NSD を含む ODNI によって組織された省庁間グループは、米国の選挙に影響を与えようとする外国の試みについて、利害関係者や国民に通知するかどうかを決定する際に、多くの要素を考慮する。 本報告書では、連邦政府がこの枠組みを用いて行った決定については評価していない。

米国の選挙に向けられた外国の悪意ある影響に関する捜査など、防諜捜査を含む捜査に関する FBI の主要な指針は、国内捜査活動ガイド（DIOG）である。 DIOG には、FBI が予備的な捜査を開始したり、本格的な捜査を開始したりするために必要な事実関係の種類、FBI が捜査のために情報を収集するために使用する手法、捜査中に FBI が情報を共有する可能性のある組織など、FBI 捜査官が取る可能性のあるさまざまな捜査手順が概説されている。

調査ツール

米国内のソーシャルメディアやテクノロジー・プラットフォームを利用した外国の悪質な影響力キャンペーンに関する情報を求める場合、FBI は現地の USAO や NSD と連携して、その活動に関する詳細な情報を得るための手段をいくつか用意している。 これらの手段を総称してリーガル・プロセスと呼ぶ。 法的手続きとは、FBI が USAO や NSD と連携して、第三者に証拠を提出させるために開始できる手続きを指す。 例えば、FBI はソーシャルメディアやテクノロジー企業に対し、現在の購読者情報を入手するための大陪審召喚を求めることができる。[9] FBI がより広範な情報を必要とする場合、電子通信プライバシー法に基づく進行中の犯罪捜査の一環として、合衆国法律集第 18 編第 2703 条(d)に基づき、米国連邦地裁に過去の加入者情報の提出命令を求めることができる。 メッセージの内容など、より詳細な情報を取得する必要がある場合、あるいはコンピュータやサーバーに保存されているデータなど、進行中の捜査のための証拠にアクセスする必要がある場合、FBI は連邦地裁の発行する捜査令状を求めることができる。

OIG 評価の目的と範囲

OIG は、2016 年、2018 年、2020 年の米国選挙サイクルにおいて、外国の悪質な選挙影響に関連する同省の情報共有システムの有効性と回復力を評価し、外国の悪質な選挙影響に対応するための同省の活動の監督、管理、協調を評価し、これらの取り組みの間のギャップや重複を特定するために、本評価を実施した。

2022 年の米国選挙サイクルでは、現地調査時に選挙サイクルが進行中であり、司法省の活動を妨害したくなかったため、これらの取り組みを調査しなかった。

われわれは、外国の悪意ある影響と闘うという DOJ の全体的な使命に関連する DOJ の政策と慣行、およびそれらの政策と慣行が、2016 年、2018 年、および 2020 年の選挙サイクルにおいて、米国の選挙に向けられた外国の悪意ある影響の脅威と具体的にどのように連動しているかを調査した。 また、選挙に対する外国の悪質

---

[9] 加入者情報には、利用者の名前、住所、電話接続記録またはセッション時間記録、サービス期間、電話番号または一時的に割り当てられたネットワークアドレスを含むその他の加入者番号または身元、およびクレジットカード番号または銀行口座番号などの当該サービスに対する支払手段および支払元が含まれる。 合衆国法律集第 18 編第 2703 条(c)(2)。 加入者情報には、送信された通信の内容は含まれない。

な影響力の脅威に関連する情報を送受信するために、同省が連邦、州、地方レベルのパートナー機関とどのように連携しているかも評価した。

FBI から入手できる証拠には限界があるため、選挙インフラを標的にしたサイバー作戦や、政治団体を支援したり危害を加えたりすることを目的とした秘密裏の影響力工作など、外国の悪意ある影響力が取り得るすべての形態に関する同省の情報共有については評価しなかった。　我々は、2016 年米国大統領選挙に向けられた外国の悪意ある影響力を受けて FITF が開発した同省の情報共有システムの側面を評価するため、ソーシャルメディア企業との情報共有に焦点を当てたが、これは多くの FBI 職員がこれらのやり取りについて我々に説明し、我々はこれらのやり取りが重要であると結論付けたためである。

OIG は、米国の選挙に向けられた外国の悪意ある影響力とは無関係の不正投票や選挙資金犯罪など、国内に起因する選挙犯罪に関連する情報の共有については評価しておらず、また、国内の行為者に関するソーシャルメディア企業との FBI の情報共有についても評価していない。[10] 。

評価の方法については、附属書 1 で述べている。

---

[10]OIG がこの評価を開始した後、FBI とソーシャルメディア企業との関係が民事訴訟の対象となった。　この訴訟で、連邦第 5 巡回区控訴裁判所は、原告側が求めた仮差し止め命令について、FBI 当局者が「(1) プラットフォームに対し、コンテンツの節度を保つよう強制し、(2) 節度に関するポリシーの変更により、節度を保つよう促した可能性が高く、いずれも憲法修正第 1 条に違反する」と判断した。　Missouri v. Biden, 83 F.4th 350, 388 (5th Cir. 2023)。　この報告書の草稿に対し、同省は第 5 巡回区の判示に同意できないと述べ、第 5 巡回区が FBI の通信が「口調や態様において明白に脅迫的であった」とは言えないと判断したことを指摘し、むしろ「FBI はプラットフォームに対して何らかの権限を行使していたため、FBI の削除要請は強制的な性質を持つものとして "合理的に解釈できる"」と結論づけたに過ぎないと指摘した。

2024 年 6 月 26 日、連邦最高裁判所は、原告には問題の仮差し止め命令を求める十分な資格がないとし、第 5 巡回区の判決を破棄した。　Murthy v. Missouri, 144 S. Ct. 1972 (2024). 最高裁は仮差し止め命令に関する判決を下し、下級裁判所に差し戻したが、仮差し止め命令の請求の原因となった根本的な訴訟は現在も進行中であり、そのため、米国選挙への外国からの影響に関する FBI に対する申し立てが訴訟に含まれている限り、OIG はそれらの申し立てを本評価の範囲に含めなかった。

われわれの評価と訴訟には重なる部分もあったが、訴訟はわれわれの範囲よりはるかに広範であった。　この訴訟では、司法省に加え、米国保健福祉省、国土安全保障省、国務省など、さまざまな連邦政府機関が被告となった。　われわれは、ソーシャルメディア企業を含む多くの異なる主体との DOJ の情報共有の有効性を調査したが、それは米国の選挙に向けられた外国の悪意ある影響力についてのみであった。

評価結果

同省は以前、ソーシャル メディア企業との特定のタイプの関わり方に関するガイダンスを欠いていた。

米国の選挙に対する外国の悪意ある影響力の脅威と闘うという司法省の使命を追求するため、FBI は米国情報コミュニティ（IC）の他のパートナー機関やソーシャルメディア企業を含む情報共有の方法を開発した。 我々の実地調査時点では、米情報機関にも FBI にも、ソーシャルメディア企業との情報共有に適用される特定のポリシーやガイダンスはなかった。[11] FBI がソーシャルメディア企業に対して行ったコミュニケーションは、外国人行為者のソーシャルメディアや電子メール・アカウントに関する情報共有が中心であったが、外国人行為者がソーシャルメディア活動で特定のテーマやシナリオの宣伝を計画していることを示す情報を FBI が入手した場合、FBI が「コンテンツ」情報を共有していることも判明した。[12] 私たちの実地調査終了後、司法省と FBI は共同で、特定の投稿や動画のアップロードなど、特定の外国の悪意ある影響活動やアカウントに関する情報を、FBI がソーシャルメディア企業と共有する際の手順を正式に定めた新しい標準業務手順書（SOP）を起草した。 この SOP は、われわれの実地調査時に存在した一般的なガイダンスよりは改善されているが、機密事項であるため、一般公開には適していない。 最後に、我々は、同省が外国の悪意ある影響力問題に関するソーシャルメディア企業との関与のための包括的な戦略を持っていないことを発見した。

ソーシャルメディア企業は、政府による侵害から憲法修正第 1 条の保護の対象となる言論の場を提供しているため、このような方針と戦略の欠如は潜在的なリスクを生み出した。 FBI が単に外国の悪意ある影響力の脅威に関する情報をソーシャルメディア企業と共有することによる憲法修正第 1 条への明白な影響はないが、その情報が、そのプラットフォームで参加する人々の言論を制限または排除するような方法で、共有された情報に基づいて行動するようそれらの企業を説得することを目的とした強制または重大な激励を構成すると合理的に受け取られるような方法で伝達された場合には、懸念が生じる可能性がある。

---

[11] FBI はまた、米国の選挙に向けられた外国の悪意ある影響力に関する情報を、DHS や州・地方政府と共有している。この情報共有は主にサイバー脅威に焦点を当てたもので、附属書 5 で説明している。

[12] 本報告書では、「行為者」という用語を、行為者の身元を確認する情報（アカウント・ハンドルや インターネット・プロトコル・アドレスなど）を指すものとして使用している。 また、「コンテンツ」という用語は、外国人行為者によって伝達された、または伝達される予定の情報に広く関連するあらゆる情報を指す。これには、外国人行為者が使用している、または使用する予定であると FBI が考えるテーマや、共有されている、または共有される可能性があると FBI が考える情報が含まれる。 例えば、FBI は、2020 年の大統領選挙で議論されている問題に関連する特定のハッシュタグやテーマを特定し、特定の外国人行為者が米国内の緊張や分裂を煽るためにソーシャルメディア活動で使用する予定であると考えた。

FBI は「情報共有モデル」を作成し、米国の選挙に対する外国の悪意ある影響力の脅威をソーシャルメディア企業と共有した。

FBI は、潜在的な手がかりを得やすくするために、外国の悪質な影響力を持つ行為者に関する情報をソーシャルメディア企業と共有する方法を開発した。　この手法の一環として、ソーシャルメディア企業も政府と情報を共有するが、これは通常、合衆国法典第 18 編第 2703 条(d)に基づいて取得される法的手続きによるものである。[13]

図 1 海外からの悪質な影響情報をソーシャルメディア企業と共有するための FBI の情報共有モデル

注：「サニタイゼーション」とは、情報源、方法、能力、分析手順を保護し、より広範な拡散を可能にするための情報編集のことである。

---

[13] FBI によると、ソーシャルメディア企業は、法的手続きによらず、自発的に FBI に情報を提供することもあるという。例えば FBI は、2023 年秋にあるソーシャルメディア企業が複数のウェブサイトやソーシャルメディアのアカウントを FBI に提供し、そのソーシャルメディア企業が外国の悪質な影響力活動に関連していると評価したと述べた。

出典　OIG による FBI および非 FBI のインタビュー対象者の証言の要約

私たちは、FBI がケース・レベルで IC パートナーと重要な情報共有関係を維持していることを知った。　情報共有を促進するため、特定の IC パートナーは、現場と本部の両方で、FBI にスタッフ（「エンベッド」と呼ばれる）を派遣している。　これらのエンベッドは、外国の悪質な影響主体に関する情報の「サニタイズ」要請を促進し、関連する米国情報機関の報告を FBI の同僚と共有する。　エンベッドは、米国情報コミュニティが提供できるインテリジェンスの種類を FBI 職員に教えるのに役立ち、他の方法では FBI が入手できない情報へのアクセスを容易にし、ソーシャルメディア企業などの外部団体との情報共有プロセスを迅速化する。　ある FBI 特別捜査官は、2020 年の選挙期間中、IC パートナー機関に情報を求めることができ、その情報をソーシャルメディア企業と共有することができたため、IC パートナー機関からの支援は彼の捜査にとって極めて重要であったと語った。　IC パートナー機関の関係者は、FBI との協力は重要だと我々に語った。なぜなら、彼らの機関とは異なり、FBI は米国の選挙に対する外国の干渉を防ぐために法執行措置を取ることができるからだ。　この思いは、Foreign Influence Task Force (FITF)の課長も同じで、FBI は、ソーシャルメディアのプラットフォームで外国人行為者が何をしているかについての情報を得るために、法的手続きを取ることによって、ソーシャルメディア企業をフォローアップできる唯一の米国情報コミュニティ機関であると述べている。

司法省によるイランのサイバー情報操作と脅迫キャンペーンの阻止

FBI は、2020 年の米国大統領選挙に影響を与えようとする 2 人のイラン人による企てに対抗するため、対外悪意影響情報共有モデルを利用した。　FBI は、米国で活動する極右過激派組織としてメディアに取り上げられた「プラウド・ボーイズ」が作成したとされる米国の有権者を脅迫するオンライン動画が、実際には米国の有権者に影響を与えようとするイラン人によって作成されたものであることに気づいた。このイラン人はまた、ある州の有権者向けウェブサイトをハッキングして得た情報を使って、アメリカの有権者に脅迫メッセージを送っていた。

米国憲法は米国外で活動する外国人行為者には適用されないため、動画とその内容は憲法修正第 1 条によって保護されなかった。　FBI は、ソーシャルメディア会社が動画を特定するのに役立つ動画に関する技術情報を入手した。　FBI はこの情報をソーシャルメディア会社に伝え、ソーシャルメディア会社はイランの動画を特定し、プラットフォームから削除した。

その後、FBI 長官と国家情報長官が記者会見を開き、イラン人による脅迫であったことを公表した。　その後、司法省は 2 人のイラン人をコンピューター詐欺と侵入、有権者脅迫、州をまたがる脅迫の送信に関する多数の犯罪で起訴した。　さらに、米国財務省は、起訴された個人とその関係者数名を制裁対象に指定し、イラン人行為者が米国内の財産にアクセスすることを阻止し、米国内の人々が彼らと取引することを禁止した。

出典　司法省、FBI、財務省

FBI 職員によると、2016 年の米国大統領選挙前および選挙期間中、FBI は主要なソーシャルメディア企業と効果的で確立された関係を築いていなかった。　その代わり、この時期、FBI とソーシャルメディア企業との交流は、主に詐欺、テロ対策、児童に対する犯罪に関するコミュニケーションに限られていた。　FBI 職員によると、ロシアによる 2016 年大統領選挙への干渉の試みが公になった後、ソーシャルメディア企業は、何が起きたのかもっと知りたいと FBI に連絡したという。　各社はまた、自社のプラットフォームにおける外国の悪意

ある影響力活動についてもっと知りたい、こうした脅威の範囲をよりよく理解するために FBI から情報を得たいと表明した。

FBI は、ソーシャルメディア企業が 2016 年の選挙干渉について知りたがっていることを、これらの企業と関係を構築する機会とみなし、改善の可能性がある分野を特定するために企業からのフィードバックを求めたと述べた。 例えば、この対話に関与した FBI の弁護士によると、ソーシャルメディア企業は、機密情報を提供するという FBI の当時の慣行について、機密保持資格を持つ従業員の数が限られているため現実的ではないと説明した。 FBI の弁護士はさらに、ソーシャルメディア企業は FBI を協力的ではなく敵対的に見ているようだと述べた。 FITF の監督官も、ソーシャルメディア企業は、FBI が企業に情報を求めるだけで、企業と情報を共有していないように見えると不満を述べた。

FBI 関係者によると、このフィードバックの結果、ソーシャルメディア企業に対し、海外の悪質な影響力の脅威に関する機密扱いのない情報を、互恵関係を期待せずに提供することにしたという。 FBI は 2018 年、この新たな情報共有アプローチを初めて実験的に導入し、プラットフォームの利用規約に違反した可能性のある外国の悪質行為者のアカウントについて、インターネットプロトコル（IP）アドレス、ソーシャルメディアハンドル、電子メールアドレス、ウェブサイトなどの識別情報をソーシャルメディア企業数社に提供した。[14] このような違反行為には、外国人行為者が偽のアカウントを開設することも含まれる。 FBI はさらに、この情報を「無条件」で企業に提供することを決定したため、企業には見返りを求めなかった。 2018 年から 2023 年 6 月までの間、FBI はこのやり方を継続し、外国の悪意ある行為者に属することが分かっている識別情報を提供する書面をソーシャルメディア企業に定期的に提供した。[151]

---

[14]この情報共有の方法は、前述したより発展した情報共有モデルの初期の例であった。 現在 FBI がソーシャルメディア企業との情報共有に用いている方法については、附属書 3 を参照のこと。

[15]OIG は、2020 年 8 月 1 日から 11 月 3 日の間に FBI がソーシャルメディア企業と開催した、外国の悪質な影響力に関するすべての会議（会議に先立って送付された資料や FBI がソーシャルメディア企業に提供したデータを含む）を示す文書を調査した。 さらに OIG は、この期間に FBI が暗号化されたファイル共有プラットフォームにアップロードし、1 社以上のソーシャルメディア企業と共有した、米国の選挙に向けられた外国の悪意ある影響に関するすべてのファイルであると FBI が我々に説明したものを確認した。

FBI は時には、行為者に関する情報に加えて、外国人行為者と結びついたテーマに関する情報を共有することもあった。 例えば、2020 年 10 月 13 日、FBI はソーシャルメディア企業 6 社と 10 件の文書を共有した。 10 文書のうち 7 文書は、イランの行為者に関する情報を提供するもので、ソーシャルメディアのハンドルネームや、これらの行為者がプロパガンダの発信に使用すると FBI が考えた一連のハッシュタグなどが含まれていた。 1 つの文書では、ロシアの関係者に関する情報と、書籍の出版に関連する予想される行動が提供されていた。 もうひとつは、選挙犯罪に関する FBI のプレスリリースへのリンクである。 最後の文書には、FBI サンフランシスコ支局の連絡先が記載されていた。 このような情報共有の影響については、以下のセクションで詳しく述べる。

ソーシャルメディア企業は、FBI が外国の悪意ある影響力関連の情報を共有したと公言している。 ある企業のウェブサイトでは、FBI が 2018 年の連邦議会選挙の前に、同社のプラットフォーム上での "オンライン活動 " について、FBI が "外国団体にリンクしている "と考える情報を送ってきたことを確認している。 同社は、これらの外国団体に関連するアカウントが「協調的な不正行為を行っている」と判断し、プラットフォーム上でのその種の活動を禁止しているため、プラットフォームから削除したと述べている。 もう 1 社は、FBI から提供された情報に基づき、「2020 年第 1 回米大統領選討論会の間、一般市民の会話を妨害しようとした」イラン人のアカウントを同社プラットフォームから削除したことを公に認めた。 FBI 関係者によると、ソーシャルメディア各社は FBI から提供された情報を評価し、FBI が法的手続きを取れば、アカウント接続に関する追加情報を共有できると FBI に伝えたこともあったという。[16] FBI はそれを実行し、ソーシャルメディア企業から収集した情報を他の連邦機関に提供した。 あるソーシャルメディア企業の代表は、この情報を共有するという FBI の決定を、「信頼構築の重要な瞬間」であったと述べている。なぜなら、その情報は「信頼でき、実行可能で、具体的」であり、その結果、プラットフォームは即座に行動を起こすことができたからだ。

FBI はまた、特定のソーシャルメディア企業と四半期ごとに定期的な会合を設け、各社のプラットフォームにおける外国の悪意ある影響力の脅威について議論している。[17] 2 社の関係者は 2018 年 9 月の議会公聴会で、特に FBI との会合に関する協力が、外国の影響工作に対抗するために増加したと証言した。 また別の企業の関係者は、2023 年 2 月の議会公聴会で、複数のテクノロジー企業が FBI とより緊密な情報共有関係の構築に取り組んできたと証言した。

2018 年の中間選挙後から 2023 年半ばにかけて行われたソーシャルメディア企業との四半期ごとのミーティングは、FBI サンフランシスコ支局の民間セクター・エンゲージメント班が、FBI と民間企業との公式なパイプ役として進行役を務めた。 会合の目的は、FITF とソーシャルメディア・プラットフォームが脅威指標情報を共有することと、双方が外国の悪意ある影響主体から見た傾向やテーマに関する戦略的脅威情報を共有するこ

OIG は、この 3 カ月を経過していない記録、FBI 以外の機関が主催した会議の結果得られた記録、または対外的な悪意ある影響に関する情報交換の範囲を超えている内容の記録は調査しなかった（附属書 1 の目的と範囲を参照）。 さらに OIG は、会議の文書に記載された内容や本評価の範囲に関連する内容以外の、会議中に共有された内容については評価しなかった。

[16] このような情報を入手するために FBI が利用できる法的手続きの種類については、附属書 6 を 参照のこと。

[17] 本報告書の草稿に対し、FBI は、特定の企業との定期的な面談の日程は、脅威の指標や、外国の悪意ある影響行為者がその企業のサービスを活用する可能性があるというその他の具体的な情報を FBI が把握した場合、または企業が外国の悪意ある影響に関して FBI との関与を求めた場合のいずれかであり、依然として運営上決定されていると述べた。 FBI は、前述のミズーリ州対バイデン訴訟のため、ソーシャルメディア企業との面会を中止したと述べた。

とだった。[18] FBI は、各企業が経験した課題や潜在的な脅威についてより気軽に話し合えるように、同業他社が同席するグループではなく、各企業と個別に面談した。 我々が確認した資料によると、2020 年 11 月の大統領選挙までの 3 ヶ月間に、FBI はこのような会合を 13 の異なる企業と 29 回開催した。

また、2018 年と 2020 年の選挙を前に、FBI が外国の悪意ある影響に対抗するために情報を共有していたソーシャルメディア企業 4 社の代表者にインタビューしたところ、4 社ともこの時期の FBI とのやりとりに概ね満足していることが分かった。 2 社は、FBI と企業の双方が外国の敵対勢力の手口を学ぶにつれて、情報共有プロセスは時間の経過とともに改善されたと報告した。2 社は、FITF の設立が情報共有プロセスの標準化に役立ったとの見解を示した。 ある企業は、このような定期的な交流を通じて最新の情報を共有できることは、事後的に政府の報告書を読むよりも、プラットフォームにとってはるかに有益であると述べた。 また別の企業は、四半期に一度のミーティングは、知識豊富な FBI 職員に質問する場を設けてくれるので助かると述べた。

国民の信頼を維持し、機密性の高い法執行権限を一貫性と客観性をもって行使することは、司法省の使命にとって重要であることから、私たちは FBI の担当者に、ソーシャルメディア企業との対外的な悪意ある影響に関する情報共有モデルが、FBI の他の業務を促進するために同じ企業と FBI がやりとりする際に、プラスまたはマイナスの影響を及ぼしたかどうかを尋ねた。 FBI 関係者は、（外国の悪意ある影響や選挙とは無関係の）他の FBI の任務分野に悪影響が及んだことは把握していないと述べた。 ある職員は、選挙関連の情報共有により、FBI が情報共有に関与する企業間の信頼関係が構築され、FBI の他の任務が強化されたと感じていると述べた。

同省は、政府機関やサイバー攻撃の被害者と外国の悪意ある影響情報を共有するためのガイダンスには従ったが、ソーシャルメディア企業と脅威情報を共有するためのガイダンスには欠けていた。

われわれは、司法省が、外国の悪意ある影響力が関与する状況での情報共有の指針となる政府全体の一般的な方針に従っていること、および FBI が、特定の状況で適用される追加的な方針を持っていることを明らかにした。 以下に説明するこれらの一般的な方針は、FBI が他の連邦政府機関、州政府、地方政府、およびコンピュータネットワークへの不法侵入などのサイバー攻撃の被害者となった場合の民間企業との情報共有について規定している。 しかし、私たちが現地調査を行った時点では、司法省にも FBI にも、米国の選挙に向けられた外国の悪意ある影響などのトピックに関する、ソーシャルメディア企業との FBI の情報共有をカバーするポリシーはなかった。

---

[18] このようなハイレベルな傾向やテーマの自発的な共有は、法的な手続きを経て行われるものではない。 FBI は、大統領令 12333 に基づき、民間団体からこのような情報を受け取る権限を与えられている。

連邦政府内の調整

FBI を含む IC パートナー間の情報共有は、大統領令（E.O.）12333 で定められており、広範な情報共有が認められている。 例えば、E.O.の 1.1(g)項では、「すべての省庁は、適用される法律とガイダンスに基づき、完全かつ自由な情報交換を可能にする方法で情報を準備し、提供する責任がある」とされている。[19] この情報共有の権限は 2016 年の選挙中もあったが、前国家情報長官室（ODNI）の選挙脅威担当幹部は、米国情報コミュニティは、外国の影響工作から米国の選挙をよりよく守るのに役立ったかもしれない情報を十分に共有していなかったことを認識していると我々に語った。

我々は、FBI が他の連邦政府機関と連携して、外国による悪質な影響力キャンペーンの被害者に対し、一貫した非政治的な通告を行うための指針として、行政府通告の枠組みを使用していることを知った。 この枠組みは、既存の法律や政策に基づいて通告が行われる場合を超えて、国家の安全保障と選挙の完全性を守るために必要な場合、連邦政府が外国の干渉に関する通告を行うタイミングを規定している。 しかし、この枠組みは、外国人行為者が偽情報を拡散する可能性のあるソーシャルメディア企業をプラットフォームとする FBI の通常の情報共有は対象としていない。 2019 年、司法省は他の IC パートナーおよび国家安全保障会議と協力して、米国の国家安全保障と選挙を保護するために通知が必要な場合に、米国の選挙に向けられた外国からの干渉について、適切な議員、州・地方政府当局者、候補者・選挙運動、民間団体、および一般市民が通知されるようにするため、この政府全体の枠組みを開発した。 さらに FBI は、選挙および選挙に関連しない影響活動を含む、外国による影響活動の個々の標的について、外国影響防御ブリーフィング委員会（Foreign Influence Defensive Briefing Board）を通じて通知することを定めた内部方針を策定した。[20]

州および地方政府との調整

我々はまた、州政府および地方政府を標的にした外国の悪意ある影響力キャンペーンを通知する際に適用される法律と政策についても学んだ。 大まかに言えば、E.O.12333 のセクション 1.6(e)は、FBI を含む米国情報コミュニティの全メンバー機関の長に対し、「法律または大統領の指示により、州、地方、部族、および民間セクターの団体に対し、適宜、情報またはインテリジェンスの共有を促進する」ことを求めている。[21] さらに、選挙インフラに特に影響を及ぼすサイバー侵入について、FBI が州や地方の当局者に通知するための方針を定めていることがわかった。[22] このポリシーによると、サイバー侵入が州内の地方選挙当局に影響を与えた場

---

[19] E.O. 12333 は E.O. 13284、E.O. 13355、E.O. 13470 によって修正された。

[20] FBI ポリシー・ノーティス 1166N、ディフェンシブ・ブリーフィング・ポリシー・ノーティス、2021 年 9 月 8 日。

[21] E.O.12333 である。

[22] 州および地方への通知方針は、FBI のサイバー課ポリシー・ガイドによって規定されている FBI の既存のサイバー被害者通知プロセスを補足するガイダンスであった。 州および地方への通知方針は、2022 年のサイバー課方針ガイドのその後の改訂によって取って代わられた。

合、FBI は影響を受けた地方当局と州の選挙責任者の両方に通知し、選挙セキュリティに関する FBI のやり取りが州および地方選挙当局の両方の役割を尊重するようにするという。 州政府当局との司法省の選挙関連情報共有に関する追加情報については、附属書 5 を参照のこと。

サイバー攻撃被害者との調整

また、民間企業がサイバー攻撃の被害を受けた場合の通知に関する法律や政策も見つかった。 具体的には、E.O.13636 は、連邦政府が民間部門とのサイバー脅威情報の共有を強化することを義務付けている。[23] この E.O. を実施するため、FBI は、サイバー脅威に関する一般的な認識を共有する民間企業向け通知（PIN）や、脅威の無力化に役立つ重要な技術情報を含む FBI 連絡警報システム（FLASH）レポートを提供している。FBI による PIN と FLASH レポートの使用に関する詳細は、附属書 3 を参照のこと。

ソーシャルメディア企業との調整

上記の情報共有方法とは対照的に、我々の実地調査時点では、FBI がソーシャルメディア企業との間で、そのプラットフォーム上での外国の悪意ある影響活動に関する脅威情報を共有することは、司法省や FBI の特定のポリシーやガイダンスによって規定されていないことがわかった。 E.O.12333 は、FBI が国家安全保障の任務の一環として、民間団体に情報を送信したり、民間団体から情報を受け取ったりすることを一般的に認めている。[24] さらに FBI 長官は、ソーシャルメディア企業を含む民間セクターと強固な関係を築くことが、外国の悪意ある影響に対抗する FBI のアプローチの柱であることを公に強調している。[25] また、議会証言の中で、FBI 長官は、通信技術の発達やインターネットの利用により変化する海外からの影響力の性質に対処するために、FBI はパートナーと協力しなければならないと述べている。[26] ある FBI 課長は、FBI 長官が、外国人行為者が自社のプラットフォームを悪用した場合、FBI には企業に通知する義務があると明言したと述べた。

FBI が民間団体、特にメディアや通信機関と関わることは、憲法修正第 1 条の観点から微妙な場合がある。情報共有それ自体から憲法修正第 1 条の懸念が生じることはないが、FBI は、情報共有から生じる直接的また

---

[23] E.O. 13636 である。

[24] E.O. 12333 の第 1.4 項(g)および第 1.6 項(e)。 E.O.12333 は、法的手続きによらない情報を民間団体から受け取ることを FBI に許可している。

[25] E.O.12333 は、FBI を含む米国情報コミュニティ機関の長に対し、「法律または大統領の指示により、州、地方、部族、および民間部門主体に対する情報またはインテリジェンスの共有を、必要に応じて促進する」ことを要求しており、米国情報コミュニティ機関に対し、米国を保護するための情報およびインテリジェンスの収集と発信を行う際、州、地方、部族政府、および必要に応じて民間部門主体の責任と要件を考慮するよう求めている。

[26] 連邦捜査局の監視」に関する米上院司法委員会でのクリストファー・A・レイ連邦捜査局長官の証言（2022 年 8 月 4 日）、www.judiciary.senate.gov/imo/media/ doc/Testimony%20-%20Wray%20-%2022-08-04.pdf (accessed October 12, 2023).

は間接的な要請を含め、このような団体との交流が、その正確な性質によっては、ソーシャルメディア企業に対し、その顧客が投稿する言論を制限または排除するよう説得することを目的とした強制または重大な奨励と合理的に受け取られ、憲法修正第 1 条の保護に関わる可能性があることに留意しなければならない。[27]

現地調査の際、FBI 職員に、米国の選挙に向けられた外国の悪意ある影響に対抗するため、ソーシャルメディア企業との情報共有をどの方針に基づいて行っているかを尋ねたところ、憲法修正第 1 条と FBI 国内捜査活動ガイド（DIOG）が、この分野における FBI の情報共有の根拠となっているが、外国の悪意ある影響に対する脅威情報をソーシャルメディア企業と共有することを特に規定した方針、ガイダンス、SOP はないと回答した。 DIOG は、修正第 1 条を FBI の活動に適用する際の指針を示し、法執行行為が違憲であるためには、修正第 1 条の権利行使を完全に損なう必要はないことを認めている。 むしろ、DIOG のもとで認可された捜査目的なしに、「個人がこれらの権利を行使する能力を著しく低下させたり、弱めたりする」活動も違憲となる。 DIOG はさらに、FBI はいかなる捜査活動も、憲法修正第 1 条で保護された活動のみを根拠とすることはできないと述べている（詳細は附属書 6 を参照）。

米国司法長官の国内 FBI 活動ガイドライン（司法長官ガイドライン）もまた、FBI が憲法修正第 1 条をどのように適用すべきかについて指針を示している。[28] 司法長官ガイドラインの制限は、捜査活動の唯一の目的が憲法修正第 1 条の権利の行使を「監視」することである場合、その捜査活動が憲法修正第 1 条の権利を直接侵害するか否かにかかわらず、FBI がそれを「監視」することを禁止することにより、憲法修正第 1 条の要件を超えるように見える。 私たちがインタビューした複数の FBI 職員は、ソーシャルメディア企業との情報共有に対する FBI のアプローチにおいて、憲法修正第 1 条が重要であることを確認している。 司法長官ガイドラインには、FBI 職員が従うべき基本原則が示されているが、ソーシャルメディア企業のような民間団体と情報を共有する際に、FBI 職員が憲法修正第 1 条の権利を確実に保護する方法については詳しく説明されていない。 むしろ、限られたガイダンスは、捜査対象者の会話を監視するといった捜査活動に焦点を当てている。

具体的なポリシーやガイダンスがない中で、どのようにソーシャルメディア企業と情報を共有しているのか、現地調査中に FBI 職員に尋ねたところ、FBI 職員は、FBI の情報共有方法は「行為者主導対コンテンツ主導」のアプローチに基づいていると明言した。 このアプローチについて、司法省と FBI の担当者は、憲法修正第 1 条の権利を保護するため、FBI はプラットフォーム上のソーシャルメディアコンテンツを外国の悪意ある影響

---

[27]例えば、Blum v. Yaretsky, 457 U.S. 991, 1004 (1982)を参照のこと： 「国家は通常、強制的な権力を行使したり、あからさまなものであれ隠微なものであれ、その選択が法律上国家の選択とみなされなければならないような重大な働きかけを行った場合にのみ、私的な決定に対して責任を負うことができる。

[28] 司法長官ガイドラインは、米国内における FBI の捜査活動を統制する省の方針を定めたものである。 同省は、国家安全保障上の脅威を含む脅威から米国を守るために FBI の権限と捜査方法を十分に活用する必要性と、プライバシーを尊重し、法を遵守する人々の生活への不必要な侵入を避ける必要性とのバランスを取るために、この方針を発表した。

に関連して監視することはなく、またオンラインで拡散されている外国の悪意ある影響に関連する特定のシナリオを調査することもないと述べた。 しかし次のセクションでは、FBI がソーシャルメディア企業とのコミュニケーションにおいて「コンテンツ」情報を共有した事例について説明する。 具体的には、外国人行為者が米国人に向けたソーシャルメディア活動で特定のテーマやナラティブの宣伝を計画していることを示す情報を得た場合に、FBI はこのような行動をとった。

ある FITF ユニットチーフによると、FBI は、外国の悪意ある影響活動を示す可能性のあるオンラインコンテンツを探すのではなく、進行中の捜査の中で開発された、あるいは他の連邦機関から受け取った、特定の外国行為者の活動に関するインテリジェンスに基づいて行動した。 FBI は、ソーシャルメディア・プラットフォーム上での外国の悪意ある影響活動に関する脅威情報を受け取った場合、そのプラットフォーム上での外国の悪意ある影響活動に関する関連情報の非機密版をソーシャルメディア企業と共有した可能性がある。 この説明は、FITF の任務に関する FBI のプレゼンテーションのレビューと一致した。このプレゼンテーションでは、「外国の悪意ある影響活動の破壊的、未申告、犯罪的、または強制的な性質」が FBI の捜査上の関心の根拠であると述べられている。 あるソーシャルメディア企業の代表は、FBI が共有した情報は、同社がすでに追跡しているものと一致しており、同社と FBI は同じ考え方に立っていると確信したと述べた。

FITF の 2 人のユニット長は、外国の悪意ある影響力キャンペーンは、憲法修正第 1 条で保護されている米国内の人々の言論を増幅させようとすることが多いと説明した。 これらの職員は、増幅のようなソーシャルメディア・プラットフォーム上での疑わしい活動が、外国人行為者と関連付けられるかどうかを FBI が判断しようとしたこと、FBI の焦点は外国人行為者が増幅しているコンテンツよりも疑わしい活動であったことを説明した。[29] FBI 防諜部門の元課長補佐によると、ソーシャルメディア企業はその後、自社のプラットフォームにおける外国の悪意ある影響活動を調査するためにこの情報を利用した可能性があり、企業が内部調査の結果を FBI と共有する前に、FBI が裁判所命令を企業に出すよう要請した可能性があるという。 FBI がソーシャルメディア企業から情報を入手するための法的手続きについては、附属書 6 を参照のこと。

FBI 職員によると、憲法修正第 1 条の懸念から、FBI は、ソーシャルメディア企業がその情報をどのように扱うべきかについて指示を与えることなく、外国の悪意ある影響力情報をソーシャルメディア企業と共有したという。 FBI と司法省の職員は、ソーシャルメディア企業が米国政府の代理人として行動するような状況を作りたくないため、具体的な行動を取るよう企業に指示しなかったと表明した。 しかし、FBI 職員はまた、FBI がソーシャルメディア企業の利用規約に違反する可能性があると考える方法で、ソーシャルメディア企業のプラットフォームを利用している外国の悪質な影響力のある行為者について、FBI がソーシャルメディア企業に情

[29] 本報告書の草稿に対し、FBI は、防諜部門の任務は、ソーシャルメディア・プラットフォーム上での不審な活動に関連する、外国の起因を特定することであると述べた。 外国人行為者に起因するソーシャルメディア活動の証拠がある場合、防諜部門は必要に応じて調査を行う。

報を提供していると述べた。[30] FBI 関係者によると、FBI は各社の利用規約を理解しようと努めたが、実際に違反があったかどうかの判断は各社が行ったという。[31]

ある FBI 弁護士は、FBI がソーシャルメディア企業と信頼関係を築き、FBI 職員と企業の双方が情報共有関係の自発的な性質を理解するようになるまでには長い時間がかかったと指摘した。 ある司法省国家安全保障局(NSD)の弁護士は、ソーシャルメディア企業は、FBI が行動を指示していないことを理解していると思うかとの質問に対し、自身の経験では、ソーシャルメディア企業は FBI の要求に反発し、対応する前に FBI に法的手続きを要求することを恐れていないと述べた。 OIG は、2020 年の米国大統領選挙前の 3 ヶ月間に FBI とソーシャルメディア企業との間で交わされた、外国の悪意ある影響に関する通信のサンプルを調査したところ、ソーシャルメディア企業の 1 社が、FBI が提供した情報に基づき、何も行動を起こさなかったと FBI に通知していたことが分かった。 OIG はまた、別の企業が FBI が提供した情報に基づいて自社のプラットフォームから一部のアカウントを削除したが、その他のアカウントは利用規約に違反していないと判断したため、削除しなかったという文書も確認した。

同省は、ソーシャルメディア企業との間で、外国人行為者に関連するテーマなどのコンテンツ情報を共有することに関する明確な方針を欠いていた。

前述のとおり、FBI がソーシャルメディア企業に行った連絡では、一般的に外国人行為者に焦点を当て、特に外国人行為者に起因するソーシャルメディアや電子メールアカウントに関する情報を共有する一方、その情報をどう扱うかについての指示は与えていないことが判明した。 しかし、文書レビューの中で、FBI が「コンテンツ」情報を共有したのは、外国人行為者が米国人に向けたソーシャルメディア活動で特定のテーマやナラティブの宣伝を計画していることを示す情報があった場合であることもわかった。[32]

---

[30] さらに、これらの関係者は、ソーシャルメディア企業は、自社のプラットフォームにおける潜在的な外国の悪意ある影響活動を調査し、自社のポリシーに基づいて適切な行動を決定するために使用できるツールを持っていると述べた。

[31] 複数の FBI 職員が同様に OIG にこのアプローチを説明したが、FBI の一般的な慣行に関する彼らの説明は、上記で言及した米国第 5 巡回区控訴裁判所の 2023 年 10 月の判決と矛盾している可能性がある。 Missouri v. Biden, 83 F.4th 350, 388 (5th Cir. 2023), rev rev'd sub nom.Murthy v. Missouri, 144 S. Ct. 1972 (2024). 本報告書の草稿に対し、FBI は第 5 巡回区の結論に同意しないことを明らかにした。

[32] 私たちが調査した文書では、FBI が複数のソーシャルメディア企業と同時に共有した外国の悪質な影響力者に関するコンテンツ情報は、特定の投稿を引用したものではなかった。 また、FBI が外国人行為者に関連する特定の投稿を単一のソーシャルメディア企業と共有した例も確認した。

われわれの評価は、米国の選挙に対する外国の悪意ある影響力の脅威に関する情報共有に重点を置いていたため、同省が国内の行為者に関する情報をソーシャルメディア企業とどの程度共有しているかは評価しなかった。

この見解に対し、FITF 課長は、FBI の「行為者主導型対コンテンツ主導型」モデルは、FBI がコンテンツに関する情報をソーシャルメディア・プラットフォームと決して共有しないという意味ではなく、むしろ、外国人行為者であることとその活動が、行為者がソーシャルメディア・プラットフォーム上でプッシュしようとしているメッセージやテーマを含め、共有する情報の性質を決定していると述べた。 FBI の担当特別捜査官補（ASAC）によると、ソーシャルメディア企業は、海外の行為者の活動から FBI が見たテーマについて FBI に質問してきたという。 ASAC は OIG に対し、この種の情報は FBI が定期的に各社と共有するものではないが、各社はソーシャルメディア企業が自社のプラットフォームで外国の悪意ある影響活動を監視できるよう、選挙に向けた外国人行為者の行動のテーマを知ることは有益だと FBI に語ったと述べた。 また ASAC は OIG に対し、外国人行為者がソーシャルメディア・プラットフォーム上で米国人に宣伝しようと計画している具体的なテーマについて議論していることについて、FBI が信頼できる情報を共有できた場合もあると述べた。

ソーシャルメディア・プラットフォームとコンテンツ情報を共有することは、対外的な影響力キャンペーンの複雑な性質や憲法修正第 1 条に影響を与える可能性があるため、この分野に内在するリスクを軽減する必要があると考える。 他の政府機関との共有とは異なり、民間企業、特にソーシャルメディア・プラットフォームとのコンテンツ共有は、上述の米国第 5 巡回区控訴裁判所の判決に示されるように、ユニークな一連の課題をもたらす。[33] さらに、国家情報会議（National Intelligence Council）が発表した外国の悪質な影響力対策に関するガイダンスでは、「（外国の悪質な）影響力キャンペーンは、一般的に言論を構成しうる方法で行われるため、各省庁は市民の自由の保護を確保するために、外国の悪質な影響力活動を具体的に定義するよう注意すべきである」と指摘している。[34]

私たちが話を聞いた司法省と FBI の職員は、ソーシャルメディア上の言論に関連する憲法修正第 1 条の微妙な懸念のため、米国の選挙に向けられた外国の悪意ある影響と闘うという司法省の使命には固有のリスクが伴うことに同意した。 NSD の元司法次官補は OIG に対し、外国の悪質な影響キャンペーンと闘う際、司法省は他者からどのように受け止められるかについて敏感でなければならず、慎重に情報を共有しなければならないと述べた。 また、司法省がソーシャルメディア・プラットフォームとどのように連携するかという枠組みは、一般にはよく理解されておらず、司法省の信頼性と評判に大きな損害を与える可能性があると付け加えた。 同氏は、外国の悪意ある影響力に関しては透明性が重要であると指摘し、FBI と司法省がソーシャルメディア企業と面会する際に何をするのか、一般市民がもっと明確に理解すればよいと思うと述べた。 同様に、FBI のある

---

[33]OIG は、最高裁判所が最近、ソーシャルメディア企業の行動を制限または管理しようとする政府関係者の憲法修正第 1 条のリスクについて、別の意見を発表したことを指摘している。 Moody v. NetChoice LLC, 144 S. Ct. 2383 (2024)を参照のこと。 これは連邦法学の活発かつ発展的な分野である。

[34]国家情報会議は、国家情報長官の米国情報共同体の長としての役割を支援し、米国情報共同体の長期戦略分析の中心である。

弁護士は、言論の自由という意味合いから、FBI は外国の偽情報キャンペーンに対抗する努力において「リスキーな法的空間」で活動していると認めた。 同弁護士は、党派的な政治的体裁や法的問題を避けるため、FBI がソーシャルメディア企業に提供するのは「外国人（行為者）のアカウント情報」に限られるようにしなければならないと述べた。

FBI は、外国の悪質な影響力との闘いに伴うリスクと課題を認識しており、FITF の任務について司法省の関係者に説明する際にも、そのことを認めている。 これらの資料では、海外からの悪質な影響と闘う FBI の取り組みの概要が広く紹介されているが、FBI は、このような捜査事項は政治的に微妙な場合が多く、影響活動は「白か黒か」ではなく、「グレーゾーン」で行われることを強調している。

われわれがインタビューした司法省と FBI の職員は、外国の脅威に対抗するために、FBI が外国の悪質な影響力を持つ選挙関連情報をソーシャルメディア・プラットフォームと共有し続けるべきだという意見で一致した。 彼らは、外国の悪質な影響力を持つ脅威行為者の情報をソーシャルメディア・プラットフォームと共有しないことに伴う国家安全保障上のリスクは、情報共有を継続することによる FBI の公共イメージへの潜在的な悪影響を上回ると考えていた。 彼らは、ソーシャルメディア企業と情報を共有するための FBI の使命、アプローチ、手順をより明確かつ透明性をもって定義したポリシーまたはガイダンスを支持することを表明した。 担当の FBI 情報アナリストは、米国の選挙に向けられた外国の悪意ある影響との戦いは流動的であるため、ポリシーの策定は難しいかもしれないと語ったが、ポリシーがあれば FBI を保護し、FBI の行動の境界を明確にすることができると認めた。 NSD の元司法次官補と FBI 防諜部門の元課長補佐は、ソーシャルメディア企業との情報共有プロセスに関するポリシーを持つことに価値があるとの意見で一致した。 重要な国家安全保障目標を推進するために、ソーシャルメディア企業と情報を共有する必要性についてのこの評価は、透明性と一貫性の重要性を強調している。

我々の実地調査終了後、司法省と FBI は共同で、FBI によるソーシャルメディア企業への対外悪意影響脅威情報の伝達を規定する新しい SOP を起草した。 FBI はこの SOP を 2024 年 2 月から実施し、本報告書の草案に対する OIG のレビューに応じて、SOP の写しを初めて OIG に提供した。[35] 機密扱いとなっている SOP は、特定の投稿や動画のアップロードなど、特定の海外悪質影響活動やアカウントに関する情報を、FBI がソーシャルメディア企業と共有する際の手順を正式に定めたものである。 これらの手順には以下が含まれる：

- その情報が外国の悪意ある影響であると判断するための基準、

[35] FBI はまた、2024 年 1 月の国家安全保障会議（National Security Council）の非機密文書 "Interim Guidance Regarding Certain Engagement with Tech Companies Regarding Online Content "のコピーも提供した。 司法省と FBI は、このガイダンスに概説されている原則を新しい SOP に取り入れた。

- 監督承認要件
- すべての情報開示に含まれる標準的な文言と、本報告書で上述した憲法修正第一条のリスクを具体的に認識し対処する、FBI とソーシャルメディア企業とのさらなる関わりを規定するガイダンス。

我々は、この SOP は、実地調査時に存在した一般的なガイダンスよりも改善されていると結論づけた。 例えば、監督の承認要件は適切なレベルに絞られており、実質的なレビューと法的なレビューの両方が確保されていると判断した。 また、SOP には、ソーシャルメディア企業との情報共有に適格であるための基準が記載されていると判断した。

このように、以前の一般的なガイダンスよりも改善されているにもかかわらず、我々は、SOP が、ソーシャルメディア企業に情報を開示する決定を FBI の記録に記録する際に、職員があらかじめ入力された基準や定型的な基準を使用することを禁止していないことに留意する。 我々は FBI に対し、現在の SOP がこの懸念に対応しているかどうかを検討するよう奨励する。 さらに、SOP には機微（センシティブ）マークが付されているため、SOP は一般公開には適さないと FBI は OIG に伝えた。 前述したように、NSD の元司法次官補は、司法省の活動が一般によく理解されない場合、司法省の信頼性と評判が危険にさらされると明言している。 そこで我々は、憲法修正第 1 条の権利も保護しつつ、外国の悪意ある影響力の脅威情報をソーシャルメディア企業に送信するために導入した手続きについて、司法省が国民に知らせることができる方法を特定することを勧告する。

米選挙に対する外国の悪質な影響力の脅威の状況に対処するための、ソーシャルメディア企業との関与に対する戦略的アプローチが欠如していた。

われわれがインタビューした FBI とソーシャルメディア企業の関係者は、2018 年と 2020 年の選挙期間中に外国の悪意ある影響力に関する情報を共有する関係に満足していると表明したが、われわれは、FBI が外国の悪意ある影響力問題に関するソーシャルメディア企業との関与に関する包括的な戦略を持っていないことを明らかにした。 FBI 当局者や報告書は、外国人所有のソーシャルメディア・プラットフォームの拡大や、外国の悪意ある影響力キャンペーンを支援する可能性のある新技術の開発など、新たな脅威が米国の選挙にリスクをもたらしていると記述している。 NSD の主導により、司法省は 2018 年の司法長官サイバー・デジタル・タスクフォース報告書において、外国の悪意ある影響力に対抗するための初の全体的戦略を策定した。この報告書は、外国の影響力の脅威を暴露し、これに対抗するための司法省の行動に関する一般的指針を示し、その後司法マニュアルに組み込まれた。[36] この報告書は、「司法省はソーシャルメディア・プロバイダーとの戦略的

[36] DOJ, Report of the Attorney General's Cyber Digital Task Force (July 2018). 司法省が情報開示の決定を下す際に重視する原則を含む、司法マニュアルの結果セクションの詳細については、附属書 6 を参照のこと。

パートナーシップを維持している」と大々的に述べているが、そのようなパートナーシップを確立・維持するためのアプローチは示していない。 サイバー・デジタル・タスクフォースの報告書に携わった NSD の元司法次官補によると、同省とソーシャルメディア企業との交流は流動的で、従来は FBI が主導していたという。 現地調査において、我々は、ソーシャルメディア企業との関係に対する戦略的アプローチの欠如に関連する 3 つのリスク領域を特定した。

第一に、FBI はサンフランシスコ支局の担当地域内のソーシャルメディア企業とは関係を維持しているが、サンフランシスコ湾岸地域外のソーシャルメディア企業とは継続的な関係がない。 FITF 課長は、サンフランシスコ支局の担当地域外に所在する 6 社未満の企業とは、特定の企業に関連すると思われるアカウント・ハンドルなどの具体的かつ個別的な情報を伝えるために、時折接触していると述べた。 サンフランシスコ・ベイエリア外に所在する企業に対して、FBI が特定の個別情報を伝達するために時折接触して情報共有することは、サンフランシスコ・ベイエリア内に所在する企業に対して用いられる、より定期的で信頼構築のためのアプローチとは異なるように見える。[37] このようなアプローチの違いは、外国の悪意ある影響力のある活動家がこれらのプラットフォームのアカウントを使い始めた場合にリスクを生じさせる可能性がある。 FITF の四半期ミーティングの記録（前述）をレビューしたところ、このようなリスクもあることがわかった。 そのような会議の記録には、ソーシャルメディア企業の代表が、自分の会社が調査を行い、外国人行為者が小規模のソーシャルメディア・プラットフォームで同調的な聴衆とコンタクトを構築していると判断したと述べたことが記録されている。[38] FBI 防諜部門の元課長補佐は、小規模なソーシャルメディア企業は、外国人行為者に狙われる可能性があり、特にそのプラットフォームのユーザーの特定の党派的傾向にアピールするメッセージを広めることができると述べた。 他の関係者は、小規模な会社も含め、国内の他の地域のソーシャルメディア会社と継続的な関係を築くことは、FBI にとって有益だと述べた。 一部の FBI 関係者やあるソーシャルメディア企業の代表者は、外国の悪意ある影響力の脅威に対処する専任のセキュリティ・オペレーション・スタッフを持たない可能性のある小規模企業との情報共有関係を確立することは、FBI にとってより困難かもしれないと指摘した。

---

[37] FBI サンフランシスコ支局の ASAC は、情報共有のための 3 つのアプローチについて、(1)定期的な会議や捜査協力の要請以外でも企業と接触し、信頼関係を構築するために、複数のコミュニケーション手段を活用する、(2)米国の選挙に向けられた外国の悪意ある影響に対抗するために、企業と協力関係を構築する、(3)テクノロジー企業特有の文化を理解する、と説明した。

例えば、テクノロジー業界における会議の服装は、他の業界や政府で適切とされる服装よりもカジュアルであることが分かった。 また、要請や問い合わせに対応する際の適時性についての考え方は、政府とテクノロジー業界とでは大きく異なることもわかった。

[38] 本報告書の草稿に対し、FBI は、標的となっている企業に関連する実用的で具体的な情報を共有することが、ソーシャルメディア企業との信頼構築に向けた FBI の取り組みにとって重要であると述べた。 さらに FBI は、こうした関係は自発的なものであり、その成功には不可欠であるため、企業に定期的な関与を強制することはできないと述べた。

第二に、外国資本のソーシャルメディア・プラットフォームの拡大が課題となっている。 FBI 職員は、これらの企業と情報共有関係を持つことは、国家安全保障上のリスクをもたらす可能性があると述べた。 外国のソーシャルメディア・プラットフォームで外国の悪意ある影響力キャンペーンが行われた場合、FBI の対応には、米国を拠点とするプラットフォームで行われる外国の悪意ある影響力キャンペーンとは異なるアプローチが必要になると、FBI 当局者は述べた。 FBI 職員は、そのような企業との情報共有は、情報が外国の敵の手に渡る可能性があるため、困難であると述べた。 その代わりに、FBI は外国のパートナー国からの支援に頼る必要があるかもしれない。

第三に、テクノロジーの発展が進むにつれて、外国人行為者は外国の影響力キャンペーンに高度なツールを使用する可能性がある。 われわれがインタビューした FBI 職員は、外国人行為者が米国の選挙をターゲットにした影響力キャンペーンを推進するために、人工知能技術を使用してコンテンツを操作または生成する「ディープフェイク」を使用する可能性があるとの懸念を表明した。[39] 2020 年 1 月、FBI の民間部門局は、民間部門全体に広く配布することを目的とした報告書を配布し、個人や敵対する政治団体が利用できる以上の技術的資源を持つ外国の悪意ある行為者が、自分たちの利益に有利だと考える候補者を支援したり、脅威だと考える候補者を弱体化させたりするために、ディープフェイクで生成したコンテンツをソーシャルメディアに投稿する可能性があると警告した。 報告書は、このようなコンテンツが拡散すれば、有権者の誤解を増幅させ、標的とされた候補者の米国有権者に対する信頼性を損なう可能性がある、と警告している。

司法省、特に FBI は、法執行機関であると同時に、ソーシャルメディア企業とのやり取りを主導する情報機関として、弾力性を向上させ、米国の選挙に向けられた進化する外国の悪意ある影響力の脅威の状況に関連するリスクに対処するために、もっとできることがあると考える。 同省は、サンフランシスコ・ベイエリア以外の企業との戦略的関与の欠如、外国人所有のソーシャルメディア・プラットフォームの台頭、外国人行為者が外国への悪意ある影響力キャンペーンで採用する可能性のあるテクノロジーの進化に対処すべきである。 外国の悪質な影響力に関するソーシャルメディア企業との情報共有を調整する包括的な省庁レベルの戦略が欠如していることは、司法省の使命がカバーする他の優先的脅威分野とは対照的である。 さらに、ソーシャルメディア企業は、政府による侵害から憲法修正第 1 条の保護の対象となる言論の場を提供しているため、（前述した）政策や戦略の欠如は潜在的なリスクを生む。

前述の通り、我々の実地調査終了後、同省と FBI は共同で、FBI によるソーシャルメディア企業への海外悪質影響脅威情報の伝達を規定する新 SOP を起草し、2024 年 2 月からその手順を実施した。 同省と FBI は、外国の悪意ある影響力の脅威に対処するための同省の広範な戦略は、司法マニュアルと DIOG で議論されており、新しい SOP は実質的にこのテーマに関するソーシャルメディア企業との関与の戦略として機能していると

---

[39] ディープフェイク」とは、リアルな写真、音声、映像、その他の偽造品のことで、人工知能技術によって作成されることがほとんどである。

の立場をとっている。 我々はこの立場を評価するために SOP を評価し、また新 SOP に引用されているが OIG にレビューのためにこれまで提供されていなかった「外国影響タスクフォースの使命と戦略」と題された 2018 年の文書も評価した。

我々は、この SOP は、FBI と対話する意思があり、FBI がコンタクトと関係を確立するための措置を講じているソーシャルメディア企業に FBI が情報を提供するための合理的なアプローチの概要を示していると結論づけた。 しかし、より広範な戦略を策定するためのさらなる作業が、FBI が直接連絡を取ることができず、連絡先や関係を構築していなかったソーシャルメディア・プラットフォーム上で外国人行為者が外国の悪意ある影響活動に関与することから生じる可能性のあるリスクに対処する上で、同省と FBI を支援することになると考えている。 海外影響対策本部の任務と戦略」文書を調査したところ、我々が指摘したのと同じリスクをいくつか想定していることがわかった。

したがって、我々は、米国の選挙に向けられた外国の悪意ある影響に対抗するためのソーシャルメディア企業との情報共有に対する司法省のアプローチが、憲法修正第 1 条の権利に関連するリスクにも対処しつつ、進化する脅威の状況に対応できるようにするための包括的な戦略を策定し、実施することを勧告する。

NSD、USAO、FBI の各支部は、米国の選挙に対する脅威を伴う外国の悪質な インフルエンス事件に関する情報を効果的に共有している。

われわれは、米国の選挙に向けられた外国の悪意ある影響に関する事件情報を共有することを任務とする司法省の 3 部門である NSD、USAO、FBI の内部で、またそれらの間で効果的な調整が行われていることを発見した。 DOJ 内では、米国の選挙に向けられた外国の悪質な影響力に関する調整が 2 つのレベルで行われている。(1)NSD が起訴を通じて外国の悪質な影響力の脅威と闘う DOJ の全体的なアプローチに関する決定を導く、戦略的な事件管理レベル、(2)FBI 捜査官、米国弁護士補（AUSA）、NSD の弁護士が個々の事件の捜査と起訴について毎週調整する、事件ごとの捜査レベル。 NSD、USAO、FBI の関係者は、定期的に連絡を取り合い、対外的な悪意ある影響力案件についてパートナーとして協力し合っていると語った。

NSD は、外国の悪意ある影響に関する情報と専門知識を共有する上で重要な役割を果たしている。

司法省の NSD は、司法省を代表し、IC 内の調整を含む省庁間調整において、米国の選挙に向けられた外国の悪意ある影響に関する戦略的情報を共有する主要な役割を果たしている。 戦略レベルでは、NSD は ODNI 主催の会議や国家安全保障会議を通じて、FBI や他の IC パートナーと交流している。 FBI と他の米国情報コミュニティ機関との関わりには、FITF が FBI の利益を代表する省庁間会議がある。 ODNI の選挙脅威担当役員だった人物によると、こうした省庁間会議では、2020 年の大統領選挙に向けた情報共有に関連する政策課題に関する作業も行われた。 NSD と FBI はまた、他の IC パートナーとともに、行政機関通報枠組みを通じて促

進される議論にも参加している。[40] このような話し合いに参加した元 NSD 司法次官補によると、この枠組みは、各省庁が米国の選挙に味方をするように見えることなく情報を共有する方法について話し合う機会を作っているという。

NSD はまた、政策を立案する上でも、訴追において主導的な役割を果たす上でも、外国の悪質な影響力に対抗するための法的専門知識を有する司法省の主要部門としての役割を果たしている。 NSD は、本部レベルでも現場レベルでも、捜査や事件レベルの情報共有の役割を担っている。 FBI の DIOG では、FBI と NSD が定期的に会合を開き、国家安全保障上の脅威とその脅威に対処するためのアプローチに関する情報を共有することが義務付けられている。 FITF は、外国の悪質な影響力の脅威に対応する FBI の主導的な部署であり、NSD の防諜・輸出管理課（CES）は、外国の悪質な影響力の脅威に対応する NSD の主導的な部署である。 FITF の課長と CES の副課長は、外国の悪意ある影響力のポートフォリオを担当し、関連するケースについて毎月会合を開いている。[41] また、FITF のスタッフは、NSD の弁護士とも効果的に連携しており、機密性の高い事案について頻繁に調整を行っていると報告している。 NSD の専門知識は、ハイレベルの省庁間会議、政策立案、対外的な悪意ある影響調査に関する省庁間の調整を含め、対外的な悪意ある影響に関する効果的な情報共有を促進している。

USAO、NSD、FBI の各支部は、米国の選挙に対する脅威を伴う海外からの悪質な影響力案件に関する情報共有のため、効果的に連携している。

司法マニュアルは、国家安全保障に影響、関与、または関連する犯罪規定を特定し、捜査の過程で捜査令状を要求する必要性など特定の事象が発生した場合、USAO に対し、これらの法令が関係する、または国家安全保障に影響、関与、または関連する事例について NSD の CES と協議するよう求めている。 これには、NSD 当局者が外国の悪意ある影響力の捜査や、米国の選挙に向けられた外国の悪意ある影響力に関する最近の起訴に関連していると語った法令も含まれる。[42] CES 課長代理によると、これらの協議要件は、FBI と USAO が NSD の弁護士と外国の悪質な影響力案件について協議することを保証するものだが、USAO との調整は司法マニュアルにある最低要件よりも頻繁に行われているという。 また、NSD はソーシャルメディア企業に対するすべての法的手続きにサインオフする必要はないが、法的手続きが行われていることは通常認識していると付け加えた。 彼女は、対外的な悪意ある影響力案件では、NSD、FBI、AUSA の間で共同して意思決定が行われることを強調した。

---

[40] 本報告書の「はじめに 」で、行政機関への通知の枠組みについて、さらに詳しく説明した。

[41] CES は、国家安全保障、外交関係、軍事・戦略物資や技術の輸出に影響する事件の捜査と起訴を監督する。

[42] 司法省は司法マニュアルの全文をウェブサイトで公開している。 例えば、DOJ, Justice Manual § 9-90.000-National Security, www.justice.gov/jm/jm-9-90000-national-security#9-90.020 (accessed July 26, 2023)を参照のこと。

全国選挙司令部

国政選挙日の直前と直後の数週間、連携した情報共有を促進するため、FBI 本部は、戦略情報調整センター（Strategic Information and Coordination Center）内に全国選挙司令部（National Election Command Post: NECP）を設置している。 NECP は、FBI の選挙関連業務全般の調整、情報の分析と発信、全国の FBI 案件に対する司法省の迅速な相談対応、他の政府機関とのリアルタイムの情報共有の促進、デコンフリクションを担当している。 2020 年 NECP には、FITF の職員を含む FBI 本部の職員、FBI 各支局に共有される情報を審査する司法省の弁護士、特にソーシャルメディア企業との情報共有のために FBI サンフランシスコ支局に出向く司法省の弁護士、司法省以外の 5 つのパートナー機関のリエゾンなどが参加した。 外国の悪意ある影響力に関する情報の共有に加え、NECP はサイバー侵入に関連する情報や、選挙法違反の犯罪に関連する情報も共有した。

FBI は NECP を補完するため、すべての現地事務所に、国内と国外両方の悪意ある影響力の脅威に対処できるスタッフを含む、現地選挙司令部の設置を義務付けた。 これらの現地司令部は、各現地事務所が受け取ったタレコミを NECP に提出し、評価を受けるとともに、NECP から現地事務所に転送されたタレコミに対処した。 また、サンフランシスコの FBI 支局は、海外の悪質な影響力の脅威に関する情報を共有するため、地域の選挙対策本部の一部として、地域のテクノロジー企業やソーシャルメディア企業と専用の通信チャネルを設置した。

NECP における FBI サイバー課の関与については、附属書 3 "ウォッチフロアと CyNERGY "を参照のこと。

出典 FBI

NSD の関係者は、NSD の裁判弁護士と AUSA は対等なパートナーとして対外悪意影響事件に取り組んでいると語った。 われわれがインタビューしたある AUSA は、USAO と NSD が協力して、各事件で NSD が果たす役割について共同決定を下すと述べている。 ある AUSA は、NSD が "全体像 "を把握し、関連する FBI 事務所と USAO の間の調整を促進するため、CES は対外悪意影響事件の "全体的な調整役 "であると述べた。 NSD は FBI のケースワークをより高度に戦略的にとらえ、DOJ の全コンポーネントが問題に関して同期していることを確認するためである。 例えば、ある AUSA は、NSD が対外的な悪意ある影響に関する新たな問題を認識できるよう、必要以上に早く NSD に問題を報告していると述べた。 また別の AUSA は、外国の悪意ある影響事件を含む、新たな防諜事件やサイバー国家安全保障事件の開廷を許可した場合、すぐに CES に通知していると語った。 さらに別の AUSA は、2016 年の大統領選挙期間中、毎週 CES との電話会議に参加し、事件情報を共有していたと語った。

USAO は個々の捜査に特化した情報共有に重点を置いている。 AUSA と FBI 捜査官は、現在進行中の対外的な悪意ある影響に関する事件を捜査するために、各事務所間で概して効果的な相互作用があると述べている。 私たちがインタビューした AUSA は、捜査の初期段階で FBI 職員が各事務所に関与し、事件の全体的なアプローチや初期の法的手続きの要請を支援できるようにすると、連携が最も効果的になると述べた。 ある FBI 特別捜査官は、外国の悪意ある影響力に対抗する最善の方法の 1 つは、外国人行為者の活動を効果的でなくするよう、公に暴露することで

あると述べた。　この暴露を達成する最善の方法は、FBI 特別捜査官と AUSA ができるだけ早く協力し、公開できる刑事告発を作成することであると説明した。[43]

米国の選挙に向けられた外国の悪質な影響力の脅威に関する捜査に携わったある AUSA は、地元の FBI 支局と USAO は「非常にオープンな対話」を行っていると述べた。　また別の AUSA によると、2020 年の大統領選挙に対する外国の悪質な影響力の脅威に関するある捜査では、USAO と FBI 特別捜査官との連携により、選挙が行われる前に、外国の悪質な行為者が管理するウェブサイトの集合に対して破壊的な行動を取るために必要な証拠を政府が作成することができたという。

[43] 米国内で身柄を拘束される可能性が低い外国人行為者を起訴することは、外国人行為者の悪質な影響力キャンペーンを世間に知らしめ、金融資産へのアクセス能力を制限し、訴追の脅威から米国または米国に友好的な国への渡航を制限することで、外国人行為者とその犯罪ネットワークを混乱させることを目的としている。

結論と勧告

結論

FBI は、米国の選挙に対する外国の悪意ある影響力の脅威に関連する情報を、米国の情報コミュニティの他のメンバーやソーシャルメディア企業と共有するための情報共有モデルを開発した。 しかし、われわれが現地調査を行った時点では、司法省はソーシャルメディア企業と共有する情報に関するガイダンスを持っていなかった。 このガイダンスの欠如は、ソーシャルメディアが米国の選挙に関連して保護された政治的言論の場としてしばしば使用されるという事実から生じる潜在的なリスクを FBI と司法省にもたらした。 司法省と FBI の関係者は、米国の選挙に向けられた外国の悪意ある影響と闘うという FBI の任務の繊細さを認め、FBI の情報共有方法は「行為者主導かコンテンツ主導か」というアプローチに基づいていると明言した。 この行為者主導のアプローチについて、米財務省と FBI の関係者は、FBI はプラットフォーム上のソーシャルメディアコンテンツを外国の悪質な影響力に関連して監視したり、特定のシナリオに基づいてソーシャルメディアの活動を調査したりはしておらず、むしろ外国人行為者の活動に関するインテリジェンスに基づいて行動していると述べた。 しかし、FBI がソーシャルメディア企業と共有する情報には、外国人行為者がソーシャルメディア活動で特定のテーマやナラティブの宣伝を計画していることを示すインテリジェンスがある場合、「コンテンツ」情報も記載されることがあった。

同省と FBI は共同で、FBI によるソーシャルメディア企業への海外悪質影響脅威情報の伝達を規定する新しい標準業務手順書（SOP）を起草し、2024 年 2 月に実施した。 これは以前の一般的なガイダンスよりは改善されたが、SOP は、ソーシャルメディア企業への情報開示を正当化する際に、従業員があらかじめ入力された基準や定型的な基準を使用することを禁止していないことに留意されたい。 我々は FBI に対し、現在書かれている SOP がこの懸念に対応しているかどうかを検討するよう奨励する。 さらに、FBI はその機密マークを考慮し、SOP は一般公開には適さないと OIG に伝えた。 司法省の活動が一般によく理解されない場合、司法省の信頼性と評判が損なわれる可能性があるため、我々は、憲法修正第 1 条の権利を保護する方法で、ソーシャルメディア企業に外国の悪意ある影響力の脅威情報を送信するために導入した手順について、司法省が一般に知らせることができる方法を特定することを勧告する。 また、司法省は、米国の選挙に向けられた外国の悪質な影響力に関するソーシャルメディア企業との関与へのアプローチを導く包括的な戦略を持っておらず、その結果、ソーシャルメディア企業との情報共有関係へのアプローチが、その企業の拠点によってまちまちであることが分かった。 包括的な戦略を確立することは、司法省が米国の選挙に向けられた外国の悪意ある影響という困難な脅威の状況に対処し、脅威と闘うために司法省がソーシャルメディア企業との関与に一貫したアプローチを取ることを確実にするのに役立つだろう。

従来、司法省とソーシャルメディア企業との交流は FBI が中心的な役割を果たしてきた が、外国の悪質な影響力との闘いに関する方針を策定する司法省の主要部門は国家安全保障局 （NSD）である。 したがって、外国

の悪質な影響力と闘うためにソーシャルメディア企業と情報を共有する FBI の取り組みが、このリスクを認識し、それを軽減する方法で実施されることを保証するために、司法省はこの方針またはガイダンスを策定すべきであると考える。　米国の選挙を守るという司法省の重要な使命に貢献するだけでなく、憲法修正第 1 条の潜在的な影響を認識する形でこれを推進する政策や指針は、司法省に対する国民の信頼を強化するだろう。

最後に、われわれは、FBI、NSD、連邦検事局が、米国の選挙に対する外国の悪質な影響力の脅威に関する事件情報の共有について、外国の悪質な影響力対策に関する司法省の全体的なアプローチを決定する戦略的な事件管理レベルと、FBI 捜査官、連邦検事補、NSD の弁護士が個々の事件の捜査と起訴について日々調整する事件レベルで、効果的に調整していることを明らかにした。　米国の選挙に向けられた外国の悪質な影響力に関する事件情報の共有を任務とする司法省の 3 部局の各担当者に話を聞いたところ、米国の選挙に向けられた外国の悪質な影響力に関する省内の情報共有関係について肯定的な見解を示し、部局間の情報共有が捜査の目的達成を促進することを強調した。

勧告

米国の選挙に向けられた外国の悪意ある影響と闘うという司法省の使命におけるリスクに対処するため、我々は司法省に以下を勧告する：

1. 憲法修正第 1 条の権利を保護し、ソーシャルメディア企業に外国の悪意ある影響脅威情報を送信するために同省が導入した手続きについて、国民に周知するためのアプローチを策定する。

2. 米国の選挙に向けられた外国の悪意ある影響に対抗するためのソーシャルメディア企業との情報共有に対する司法省のアプローチが、進化する脅威の状況に対応できるよう、包括的な戦略を策定し、実施する。

附属書 1：目的、範囲、方法論

規格

OIG は、誠実性と効率性に関する監察官総長会議の「監察と評価の質基準」（2012 年 1 月）に従い、本評価を実施した。

目的と範囲

OIG は、2016 年、2018 年、2020 年の米国選挙サイクルにおける、米国選挙に対する外国の悪意ある影響力の脅威と、そのような脅威に対応するための同省の活動の監督、管理、調整に関連する同省の情報共有システムの有効性と回復力を評価するとともに、これらの取り組みにおけるギャップや重複を特定するために、本評価を実施した。 2022 年の米国選挙サイクルでは、現地調査時に選挙サイクルが進行中であり、DOJ の活動を妨げたくなかったため、これらの取り組みを調査しなかった。 また、米国の選挙に向けられた外国の悪意ある影響力とは無関係の不正投票や選挙資金犯罪など、国内発の選挙犯罪に関連する情報の共有についても調査しておらず、国内行為者に関するソーシャルメディア企業との FBI の情報共有についても調査していない。

我々のフィールドワークは 2021 年 10 月から 2023 年 4 月にかけて行われた。

FBI から入手可能な証拠には限界があるため、選挙インフラを標的としたサイバー作戦や、政治団体を支援または害することを目的とした秘密裏の影響力作戦など、外国の悪意ある影響力が取り得るすべての形態に関する同省の情報共有については評価しなかった。 我々は、2016 年米国大統領選挙に向けられた外国の悪意ある影響に対応するため、外国影響タスクフォース（FITF）が開発した同省の情報共有システムの側面を評価するため、ソーシャルメディア企業との情報共有に焦点を当てたが、これは多くの FBI 職員がこれらのやり取りについて我々に説明し、我々はこれらのやり取りが重要であると結論付けたためである。

OIG がこの評価を開始した後、FBI とソーシャルメディア企業との関係が民事訴訟の対象となった。 この訴訟で、連邦第 5 巡回区控訴裁判所は、原告側が求めた仮差し止め命令について、FBI 当局者が「（1）プラットフォームに対し、コンテンツの節度を保つよう強制し、（2）節度に関するポリシーの変更により、節度を保つよう促した可能性が高く、いずれも憲法修正第 1 条に違反する」と判断した。 Missouri v. Biden, 83 F.4th 350, at 388 (5th Cir. 2023)。 この報告書の草稿に対し、同省は第 5 巡回区の判示に同意できないと述べ、第 5 巡回区が FBI の通信が「口調や態様において明白に脅迫的であった」とは言えないと判断したことを指摘し、むしろ「FBI はプラットフォームに対して何らかの権限を行使していたため、FBI の削除要請は強制的な性質を持つものとして "合理的に解釈できる"」と結論づけたに過ぎないと指摘した。 2024 年 6 月 26 日、最高裁判所は第 5 巡回控訴裁の判決を破棄し、原告には問題となった仮差し止め命令を求める十分な資格がないとした。 Murthy v. Missouri, 144 S. Ct. 1972 (2024). 最高裁は仮差し止め命令に関する判決を下し、下

級裁判所に差し戻したが、仮差し止め命令の請求の原因となった根本的な訴訟は現在も進行中であり、そのため、米国選挙への外国からの影響に関する FBI に対する申し立てが訴訟に含まれている限り、OIG はこれらの申し立てを本評価の範囲に含めなかった。

方法論

我々の調査方法は、司法省、他の連邦政府、州、および地方政府関係者へのインタビューであり、サンフランシスコ・ベイエリアへの訪問を含め、FBI、米国連邦検事局（USAO）、米国国土安全保障省（DHS）、州、および地方政府関係者、ならびにソーシャルメディア企業数社の代表者と面会した。　また、同省と FBI の方針を分析し、FBI の情報共有活動に関連する記録を調査した。

インタビューと観察

今回の評価では 93 件のインタビューを実施した。　面談の対象となった人物は、その期間中、特定された職務に就いていた。　フィールドワークの一環として、我々は FBI サンフランシスコ支局を訪問した。

司法省のインタビュー

FBI では、防諜部、法務部、特別捜査官と情報分析官を含む FITF、サイバー部、保安部の現職員と元職員にインタビューを行った。　我々は、FBI が情報共有のために使用できるデータベースのデモと、それらのデータベースを使用して共有された、米国の選挙に向けられた外国の悪意ある影響力に関する情報の例を要求した。　これらのシステムに関する追加情報を附属書 3 に示す。　また、スーパーバイザーや特別捜査官を含む FBI の現場部門スタッフにもインタビューを行った。

国家安全保障部では、現職および元職の監督弁護士と非監督弁護士にインタビューを行った。

USAO では、米国の選挙に向けられた外国の悪意ある影響に関わる調査や訴追に携わったことのある米国弁護士補にインタビューを行った。

DOJ 以外のインタビュー

我々は、国家情報長官室や DHS のサイバーセキュリティ＆インフラセキュリティ局など、他の連邦政府機関の関係者にインタビューを行った。

われわれは、5 つの州で選挙結果の認証を担当する機関の職員にインタビューを行った。

我々は、FBI が 2020 年の大統領選挙までの数ヶ月間、米国の選挙に向けられた外国の悪意ある影響に関する情報を定期的に共有していたソーシャルメディア企業 4 社の従業員にインタビューを行った。

方針と文書の見直し

米国の選挙に向けられた外国の悪意ある影響に関する情報を共有するための規則とパラメータを理解するため、我々は大統領令、省庁および FBI の方針、ならびに外国の悪意ある影響と選挙関連の脅威への対応という一般的なトピックに関連する省庁および FBI の研修資料（FBI の『国内捜査および作戦ガイド』2020 年 3 月版の関連箇所を含む）を検討した。

米国の選挙に向けた外国の悪意ある影響力をテーマに、ソーシャルメディア企業と四半期ごとに二者間会合を開くという FBI の慣行と、それらの企業とどのような情報交換が行われたかを理解するため、2020 年 8 月 1 日から 11 月 3 日の間に FBI がこの目的でソーシャルメディア企業と開いたすべての会合の記録を調査した。この期間を選んだのは、大統領選挙前の 90 日間を含んでおり、インタビューによると、選挙間近には FBI とソーシャルメディア企業とのコミュニケーションが頻繁に行われているという。　また、この 90 日間に、二者間会合に直接関連して、あるいは別個のコミュニケーションとして、ソーシャルメディア企業と共有された外国の悪意ある影響力に関するすべての情報のコピーも調査した。

附属書 2：対外影響タスクフォースの任務、構造、発展、および FBI サイバー課の役割

対外影響タスクフォースの使命と構造

対外影響タスクフォース（FITF）の任務と組織は、創設以来発展してきた。 我々の評価時点では、FITF の使命は、民主的制度と国民の信頼を守り、共通の活動イメージを構築し、敵対者のコストを引き上げ、世界中の敵対者が提示する脅威を軽減することである。 FITF には、FBI の防諜部門、サイバー部門、犯罪捜査部門、テロ対策部門の職員が、統一された指揮系統のもとに集まっている。

構造的には、FITF は防諜部門の課長とサイバー課の課長補佐によって率いられている。 FITF は 3 つのユニット（ロシア連邦に焦点を当てたユニット、中華人民共和国に焦点を当てたユニット、その他すべての外国に焦点を当てた第 3 のグローバル・ユニット）に分かれており、各ユニットは特別捜査官と情報分析官で構成されている。 ほとんどの特別捜査官は、FITF に配属されると、プログラム・マネージャーの役割を果たす。

FITF 設立の背景

FITF が創設される以前は、FBI は対外的な悪意ある影響力の脅威を調査していたが、これらに特化した単一の FBI 部隊やチームは存在しなかった。 その代わりに、サイバー、防諜、犯罪の脅威を担当する FBI 本部の部局と、それに関連する現場部局の分隊が、特定の焦点（行為者グループや地域など）に基づき、その種の捜査に関連する形で、対外悪意影響事件の捜査を行っていた。

FITF の指導部は、拡大期には FBI が臨時のチームを編成し、ロシア以外の敵対勢力に焦点を当てたと説明し、選挙後はチームを分散させ、次の選挙に向けて再編成するのではなく、選挙サイクルの間にも外国への影響力の脅威は存在するため、通年でチームを維持することにしたと述べた。 議会証言の中で、FBI 長官は、焦点の拡大と敵対勢力の拡大に対応するため、選挙と海外影響力の脅威に関する常設の「急増」能力を維持するためのリソースを追加したと述べた。 また FBI は、FITF の任務の拡大に伴い、FITF 課長を幹部の指導的立場にした。

FITF における FBI サイバー部門の役割

前述したように、FITF は防諜部門の中で運営されており、選挙に関連する外国の悪意ある影響力の脅威に取り組む防諜およびサイバーの経験を持つスタッフを含む 3 つのユニットで構成されている。 上級幹部を含む FBI 関係者は、このタスクフォース・モデルが、外国の悪質な影響力問題に関する情報共有を調整する効果的な手段であると評価している。

これとは別に、FBI サイバー課の任務は、国家的行為者によるコンピューター侵入などの捜査であり、2020 年の大統領選挙中にイラン人が米国のある州の有権者データベースをハッキングして侵入したような、選挙関連のコンピューター侵入が含まれることもある。 このようなケースを担当するサイバー課の職員は、FITF の職員と協働するが、FITF に配属されるわけではない。 さらに、FITF に代わって連絡を取るなど、ソーシャルメディア企業とのやり取りを担当する主な職員は、サイバー経験のある現場部門の職員である。

サイバー部門が関与した FITF ケースの例

外国の悪意ある影響に関する事件が FBI のサイバー部隊によって現場で行われる場合、現場の捜査官はサイバー課のプログラム・マネージャーと関わり、そのプログラム・マネージャーが FITF のプログラム・マネージャーと調整する。 例えば、政治キャンペーンへのハッキングがあった場合、FITF は迅速に FBI のサイバー課と連携する。 あるサイバー課の職員は、政治キャンペーンや電子メールアカウントがハッキングされた場合、サイバー課が侵入を調査すると説明した。しかし、盗まれた非公開情報が一般に流出した場合は、防諜部門が影響力工作の可能性を調査する。

出典 OIG による FBI 職員への聞き取り調査

米国の選挙に向けられた外国の悪意ある影響に関する FITF とサイバー課の役割は、影響と干渉のカテゴリーに分類される外国の活動に沿って大まかに分けられる。 国家情報会議は「選挙への影響力」を、候補者、政党、有権者やその嗜好、政治プロセスなど、米国の選挙に直接的または間接的に影響を与えることを意図した、あからさまおよび秘密裏の活動を含むと定義している。 国家情報会議は「選挙干渉」を、有権者登録、投開票、結果報告など、選挙の技術的側面を対象とした選挙影響活動のサブセットと定義している。 FITF の指導部によると、FBI もまた、影響と干渉に関するこれらの理解を採用しているという。 防諜経験のある FITF 職員は、影響力キャンペーンに焦点を当てている。 サイバー経験のある FITF 職員、および FITF に属さないサイバー課の職員は、米国の選挙に向けられた外国からの干渉活動を含む干渉に焦点を当てている。

防諜部門とサイバー課の FBI 職員は、FITF におけるそれぞれの任務は互いに異なるものであり、それぞれの役割を明確に定義することができると説明した。 具体的には、サイバー課の職員は、影響力のサブセットである悪意ある干渉は、コンピュータシステムへの侵入（またはハッキング）と考えることができると述べた。一方、防諜部門の職員は、悪意ある影響力は広範であり、スパイ活動、有権者の意見や信頼に影響を与えようとする試み、技術的干渉（ハッキング）などの秘密活動が含まれると説明した。

附属書 3：FBI が情報を共有するために利用できるデータベースとシステム

評価結果で取り上げたように、FBI は四半期ごとにソーシャルメディア・プラットフォームと二者間会合を開き、ソーシャルメディア・プラットフォームにおける外国の悪質な影響力の脅威に関する情報を共有することを主な目的としていた。 さらに、FBI 職員は、より広範な他の目的のために存在する、情報を受信または配信するシステムについて説明したが、これらのシステムは、そのような必要が生じた場合に、米国の選挙に向けられた外国の悪意ある影響力に関する情報を共有するためにも使用することができる。 以下に、これらの追加の方法について述べる。

FBI 公式記録システム

センチネル

2012 年から使用されているセンチネルは、FBI の第 3 世代のケース管理および公式記録管理システムである。[44] FBI の捜査・管理活動の記録をケースファイルとして管理し、各事件の開始から終結までを記録する。 米国の選挙に向けられた外国の悪意ある影響に関わる事件は、センチネルでは以下のように分類される：

- FBI の防諜部門が監督する、特定の国の対外的な悪意ある影響活動を標的にした防諜捜査、あるいは以下のようなものである。
- 選挙（選挙運動や候補者を含む）に関連する特定のサイバー侵入に焦点を当て、FBI のサイバー部門が監督する犯罪捜査。

FBI の職員によると、センチネルは外国の悪意ある影響と分類されたすべてのケースを特定できるが、米国の選挙に向けられた脅威を含むサブセットを特定するためには、これらのケースを手作業で確認する必要があるという。

2020 年、FBI は選挙日の前後約 1 週間、選挙関連の事件や情報情報が大量に報告されたため、Sentinel を使って管理した。 FBI は、これらの情報のうち外国の悪意ある影響に関わるものはほとんどなかったと報告した

---

[44] 2006 年から 2014 年にかけて、OIG は FBI のセンチネル計画と実施を評価する 10 件の監査を行った。 2014 年の監査には、一連の監査の全リストが含まれている。 DOJ OIG, Audit of the Status of the Federal Bureau of Investigation's Sentinel Program, Audit Report 14-31 (September 2014), oig.justice.gov/reports/auditstatus-federal-bureau-investigations-sentinel-program を参照のこと。

が、Sentinel はこのプロセスを通じてどれだけの外国の悪意ある影響関連の情報を受け取り、処理したかを定量化することはできなかったと述べた。

連邦機関以外との情報共有方法

Telporter

Teleporter は暗号化されたファイル共有システムで、連邦、州、地方、部族、外国の政府機関や民間セクターのパートナーなど、FBI が信頼関係を維持しているあらゆる組織と業務ファイルを共有することができる。[45] テレポーターは、法執行機関向けにウェブベースの捜査ツールや分析リソースを提供する安全なプラットフォームである、FBI の法執行機関エンタープライズポータルに含まれる機能の一つである。 テレポーターの FBI ユーザーは、共有するファイルをアップロードし、受信者を指定し、受信者がファイルにアクセスできる制限時間を設定し、受信者に共有ファイルをダウンロードするためのリンクを含む電子メールを送信する。 Teleporter の FBI ユーザーには、受信者にアップロードリンクを送信するオプションもあり、これにより受信者は限られた期間内にファイルを FBI に提供することができる。 受信者は、ファイルをダウンロードまたはアップロードするために、少なくとも Teleporter への一時的なアクセス権が付与されていなければならない。

我々の評価対象期間中、FBI は Teleporter を使用して、既知の外国人行為者に関連するインターネットプロトコルアドレス、ドメイン名、ソーシャルメディアハンドルなどの外国の悪意ある影響力情報をソーシャルメディアプラットフォームと共有した。 FBI はまた、Teleporter を使用して、ソーシャルメディアプラットフォームから自発的に提供された、そのプラットフォーム上での潜在的な外国の悪意ある影響活動に関連するヒントを受け入れた。

非政府系暗号化メッセージング・アプリケーション

2020 年秋、FBI は暗号化されたメッセージング・アプリケーション上にチャンネルを開設し、海外影響タスクフォース（FITF）、FBI サンフランシスコ支局、米国土安全保障省（DHS）、7 つのソーシャルメディア・プラットフォームの参加者とリアルタイムで通信を行った。 FBI はこのチャンネルを、FBI の全国選挙司令部

---

[45] FBI の刑事司法情報サービス部門は、法執行機関向けにさまざまな支援サービスを提供している。 Teleporter は、同部門の Law Enforcement Enterprise Portal でホストされているツールで、業務関連ファイルを法執行機関やパートナー・コミュニティ間で共有・移動することができ、FBI と信頼関係を維持している人なら誰でも利用できる。 ファイルのアップロードやダウンロードを行うため、テレポーターへの一時的なアクセスは、個人を問わず許可される。

（NECP）が活動している間、機密扱いでない外国の悪意ある影響脅威情報を共有するという限定的な目的のために開設した。[46] このチャンネルは 2020 年 10 月 27 日から 11 月 7 日まで使用された。

FBI はこのチャンネルを使って、外国人行為者が管理するソーシャルメディアのハンドルネーム、ドメイン名、ウェブサイト、外国人行為者が影響力活動を行うために使うテーマを共有した。 FBI は、これらの情報を Sentinel で事前に承認し、FBI 法律顧問室の弁護士と、記録保存の目的で作戦課長が承認することを義務付けていた。 さらに FBI は、このチャンネルを通じて米国人の特定情報を流すことを禁止した。

民間企業への通知／FBI リエゾンアラートシステム報告書

大統領令（E.O.）13636 は、連邦政府に対し、民間企業と共有するサイバー脅威情報の量、質、適時性を向上させることを要求した。 この目標を達成するため、FBI のサイバー部門は、民間部門パートナーに脅威情報を提供し、そのデータを使用して特定されたサイバー標的活動に関する情報を FBI に提供するようパートナーに要請するために、Private Industry Notification (PIN) と FBI Liaison Alert System (FLASH) レポートを作成している。 PIN と FLASH の両レポートには、未分類の実行可能な情報のみが含まれ、脅威の無力化を支援するように設計されている。 PIN は、進行中または出現しつつあるサイバー脅威に関する文脈情報を提供し、FLASH レポートは、捜査または諜報活動を通じて得られた技術的指標を提供する。 PIN と FLASH レポートは、共有される脅威情報の性質に応じて、特定の受信者に限定して配布されることもあれば、広く一般に配布されることもある。

PIN または FLASH 報告書の主執筆者は、FBI サイバー部門本部の情報部門のアナリストであり、報告書が国家的行為者を対象としている場合は、FBI 防諜部門と連携している。 FBI は、2020 年 8 月以降に発表した、米国の選挙に影響を及ぼす可能性のあるサイバー国家脅威に関する PIN や FLASH 報告書を含む 5 つの報告書を確認した。

米国政府内の情報共有方法

インテリジェンス情報レポート

FBI は、捜査や活動を通じて入手した未評価の生のインテリジェンス情報を、米国情報機関を含む他の連邦政府パートナーと共有するために、インテリジェンス情報報告書（IIR）を使用している。 IIR は、連邦政府機

---

[46] FBI の担当特別捜査官補の話によると、FBI は当初、2020 年の選挙に向けて、これらの参加者が同じ部屋にいるような合同司令塔を設置する予定だったが、コロナウイルス感染症 2019 年のパンデミックにより、FBI は代わりに仮想共有スペースを使用することを余儀なくされた。 FBI と他の参加団体は、この目的のために非政府機関の暗号化メッセージング・アプリケーションを使用することに同意した。

関が生の情報（FBI や他機関の分析評価や判断を含まない情報）を迅速に共有するために使用される。 IIR は、共有される情報を収集した FBI の現場事務所が起草、配布する。 FITF の監督情報分析官によると、FITF は 2020 年の選挙前に、外国の悪意ある影響に関連する情報を発見した場合、IIR を作成・配布するよう現地事務所にガイダンスを送ったという。

各 IIR には、その IIR に含まれる情報に関連する情報要件を特定するためのタグが付けられており、それによって、IIR がより広範に拡散されているにもかかわらず、特定の米情報コミュニティ要員の注意がその IIR に向けられるようになっている。[47] FBI 情報総局の担当者は、米国の選挙に向けられた外国の悪意ある影響に関する情報を共有するために、FBI がどの程度 IIR を利用しているかを定量化することはできない、と述べている。

Pulse

Pulse は、米国情報コミュニティーの各機関が管理するデータベースで、31 種類のインテリジェンス・プロダクトを保存している。 このデータベースには、各参加機関が情報製品を公表するための複数のチャンネルがあり、キーワード検索機能を提供している。 米国情報コミュニティ全体で働く個人がパルスにアクセスできるが、個々のユーザーが閲覧できる製品は、ユーザーのセキュリティ・クリアランスとアクセス・レベルによって異なる。

クロニクル

クロニクルは、米国の情報コミュニティ機関が利用できるリソースであり、FBI はこれらの機関と大量の生データを共有するために利用している。 具体的には、民間部門から自発的に提供された情報、あるいは法的手続きを経て民間部門から入手した情報など、実行可能な技術的詳細情報を、その情報に基づいて公表する前に共有するために、FBI はクロニクルを使用している。

ウォッチ・フロアとシナジー

FBI は、30 を超える連邦法執行機関、情報機関、防衛機関が連携し、サイバー脅威の捜査を支援するために情報を調整、統合、共有する、全米サイバー捜査合同タスクフォースに所属している。 タスクフォースでの役割の一環として、FBI は、サイバーインシデントの報告を省庁間で共有し、受け取った報告を関連する FBI の捜査部門に指示するために、ウォッチフロアと呼ばれる 24 時間 365 日のコマンドセンターを運営している。

---

[47] 情報要件とは、米情報コミュニティが情報収集を必要とし、そのためにリソースを投入する権限を与えられているトピックのことである。

ウォッチフロアは、報告書に選挙関連のタグを付けることができるが、このタグは、外国の悪意ある影響力に関する報告書だけでなく、他の種類の選挙関連の脅威に関する報告書も含んでいる。

重大なサイバー事件やイベントが発生した場合、FBI はサイバー部門イベント調整センター（Cyber Division Event Coordination Center）を稼動させ、特定のイベントに関連する専門家を配置し、ウォッチフロア（Watch Floor）が受け取ったイベント関連の報告を確認、処理する。 FBI は、2020 年の選挙日の前後 1 週間、サイバー課イベント調整センターを作動させ、選挙関連の専門家を配置した。 サイバー課イベント調整センターは、FBI の NECP へのサイバー課の参加を構成し、FBI の選挙関連業務全般の調整を担当した。 この同じ専門家グループは、2020 年のスーパーチューズデーと 2021 年の就任式の日にも待機していた。

CyNERGY は、連邦政府機関がサイバーインシデントを追跡し、選挙に関連するインシデントを含む可能性のあるサイバー侵入のターゲットへの通知を調整するための、FBI がホストする省庁間データベースである。 この追跡は E.O.13636 で義務付けられている。 我々の実地調査時点では、FBI は DHS のサイバーセキュリティ＆インフラセキュリティ局、国家安全保障局、米国財務省との間で、これらの機関がデータベースにアクセスし、貢献することを認める覚書を最終的に取り交わしていた。 その時点で FBI は、CyNERGY へのアクセスを他の連邦政府機関にも認めるための覚書を作成中であった。

一般からの情報受信方法

インターネット犯罪苦情センター

FBI サイバー課のインターネット犯罪苦情センター（IC3）ユニットは、FBI の IC3 データベースを管理している。 2000 年に創設された IC3 データベースは、サイバー犯罪を報告するための全米の中心的なハブとして機能している。 オンラインシステムを通じて、一般市民が苦情を提出することができ、FBI はそれを分析して、FBI がどのように対応すべきかを決定する。

IC3 ユニットのスタッフは、FITF および FBI の Election Fraud Working Group と協力して、IC3 データベースに提出された苦情を選挙関連と分類するために使用できるキーワードを開発した。 これらのキーワードは、米国の選挙に向けられた潜在的な外国の悪意ある影響と、外国の悪意ある影響とは関係のない選挙関連の脅威の両方をカバーしている。 FBI は、2020 年に IC3 データベースに提出された数千件の苦情のうち、外国の悪意ある影響に関連するものばかりではないが、63 件を選挙に関連するものとして分類したと述べている。

附属書 4：選挙犯罪に対抗する司法省の任務の概要

米国の選挙に向けられた外国の悪意ある影響に対抗することに加え、司法省には選挙犯罪と闘うという、より広範な使命がある。 連邦法は、選挙職員やスタッフに対する暴力の脅迫、有権者に対する脅迫や賄賂、票の売買、有権者へのなりすまし、有資格者の投票を妨げるために選挙の時間、場所、方法について意図的に嘘をつくこと、票の集計を改ざんすること、投票箱に詰め物をすること、有権者の意に反して、あるいは有権者の意見を無視して投票用紙に印をつけることを犯罪としている。 連邦法はまた、有権者の権利のための特別な保護を含んでおり、脅迫を含む干渉や、投票すること、あるいは自分の選んだ候補者に投票することを妨げたり、思いとどまらせたりすることを目的としたその他の行為から、有権者が自由に投票できることを定めている。このような選挙法の枠組みに対する違反の捜査は、FBI、連邦検事局（USAO）、刑事局、公民権局など、司法省の複数の部門が担当している。

- 同省は 2021 年、選挙作業員に対する暴力の脅威への対処に重点を置く「選挙脅威タスクフォース」を創設した。 このタスクフォースは、選挙作業員に対する脅迫の申し立てや報告を評価し、全米の USAO や FBI の現地事務所と協力して、これらの犯罪を捜査し、必要に応じて訴追する。 このタスクフォースには、司法省の刑事部、公民権部、国家安全保障部、FBI を含む複数の組織と、米国国土安全保障省などの主要な省庁間パートナーが参加している。

- 各 FBI 支部は、少なくとも特別捜査官 1 名と情報分析官 1 名を選挙犯罪コーディネーターに任命し、選挙犯罪の疑惑を評価し、脅威を調査し、情報を収集するための支部の取り組みを指揮している。 選挙犯罪コーディネーターはまた、各事務所が担当する地域の州・地方当局者との連絡窓口となり、アウトリーチ活動を行い、地域の法執行機関との関係を構築する。

- 各連邦選挙に先立ち、USAO は、刑事部や公民権部などの司法省本部部門と協議の上、選挙権に関する懸念、選挙職員やスタッフに対する暴力の脅威、選挙詐欺などに関する選挙当日の苦情の処理を監督する責任を負う地区選挙担当官を任命する。

- 公民権部門の投票部門と刑事部門は、選挙に関するさまざまな連邦法を執行している。 投票部門は選挙を監視し、連邦投票法違反に関する苦情を受理し、刑事部門は捜査を行い、FBI と連携して有権者の脅迫や弾圧などの犯罪違反を追及する。

- 刑事課の公共誠実部門は、いくつかの分野で選挙犯罪を扱っている。 このセクションでは、票の買収、多重投票、虚偽の登録や虚偽の投票用紙の提出、票の改ざん、贈収賄、投票の時間、場所、方法に関する偽情報など、選挙詐欺犯罪や不正投票を扱っている。 同セクションは、公民権法では保護されない政治団体を標的にするなど、公民権部が扱わない有権者脅迫や弾圧の事件を起訴する責任を負っている。 同課はまた、選挙資金法に違反した外国団体の訴追など、選挙資金犯罪も起訴する。

附属書 5：司法省による他の連邦政府機関および州政府関係者との選挙関連情報共有

報告書本文で取り上げた司法省、国家安全保障局、ソーシャルメディア企業間の関係に加え、司法省は米国の選挙に向けられた外国の悪意ある影響に対抗する取り組みにおいて、他の政府機関とも関係を維持している。連邦政府内では、司法省は米国土安全保障省（DHS）や米財務省とも関係を維持している。 DOJ はまた、州や地方政府とも限られた交流しかない。

国土安全保障省との調整

DHS における司法省の主要なパートナーは、サイバーセキュリティ＆インフラセキュリティ局（CISA）であることがわかった。 CISA と司法省は、サイバー事件対応、選挙の安全保障、外国の悪意ある影響活動への対処など、いくつかの共通の任務で協力している。 外国の悪意ある影響活動への対策に関して、CISA 関係者は、CISA は選挙に関する正確な情報を国民に提供することを通じて、回復力を促進することに重点を置いていると述べた。 回復力を促進する努力の中で、CISA は国務長官を含む州や地方の選挙当局者と交流している。CISA の職員は、CISA と司法省は、外国の悪意ある影響と闘うという使命が一致しているため、日々連携していると語った。

CISA の職員は、CISA と FBI はインシデント対応で連携しており、FBI が犯罪捜査を主導する一方で、CISA は修復とインシデント管理に注力していると述べた。 CISA 職員によると、FBI は、サイバー侵入インシデント発生時に CISA の役割を支援するために、他の連邦政府パートナーとの連携を図るのに効果的である。CISA 職員は、CISA は新しい機関であるため、FBI もその信頼性とリソースを提供しており、これは重要であると述べた。 例えば、CISA 職員は、インシデント対応中に CISA が疑わしいインターネット・プロトコル（IP）アドレスを特定した場合、FBI と連携し、FBI は Sentinel でその IP アドレスに関するあらゆる情報を検索できると話した。[48] FBI がすでにその IP アドレスに関する情報を持っている場合、それは新たなインシデントがより深刻である可能性を示している可能性がある。

国土安全保障情報ネットワーク

国土安全保障情報ネットワーク（Homeland Security Information Network）は、連邦、州、地方、地域、部族、国際、民間セクターのパートナー間で、機密だが未分類の情報を共有するための DHS 主催のシステムであ

[48] 情報共有のための FBI のセンチネル利用については、附属書 3 を参照のこと。

る。 2020 年のこのシステムの用途のひとつは、連邦、州、地方、地域機関が選挙関連の脅威や事件を監視、分析、対応できるようにすることだった。

他の連邦政府機関との調整

我々はまた、司法省が米国財務省と協力して、外国の悪質な影響力を持つ行為者に対する制裁を、緩和または混乱させる手法として求めることがあることを知ったが、この関係を詳細に調査したわけではない。 複数の司法省職員は、特に米国が外国の悪意ある影響行為者の身柄を確保できそうにない場合、制裁は外国の悪意ある影響に対抗する上で非常に効果的な手段になり得ると我々に語った。 このような省庁間の関係を促進するため、FBI は財務省の外国資産管理局（Office of Foreign Assets Control）に駐在官を置き、両省庁間の制裁問題の調整を行っている。 外国人影響力タスクフォース（FITF）のプログラム・マネージャーは、外国資産管理局の FBI デタイリーを通じて、外国の捜査対象に対する制裁を求めることができる。

OIG が詳しく調査しなかったもう一つの連邦政府機関との関係は、司法省および FBI と米国国防総省との関係である。 FBI 関係者によると、国防総省の米サイバー軍司令部は、FBI やその民間部門のパートナーにとって実用的な情報を FBI に提供することがあったという。 このような場合、FBI はソーシャルメディア企業に共有された関連情報のパイプ役となり、サイバー司令部が FITF に情報を提供し、FITF が関連情報を FBI サンフランシスコ支部に伝え、民間部門のパートナーに広めた。

州政府関係者との調整

我々は、州政府および地方政府が、米国の選挙に向けられた外国の悪意ある影響力に関して、FBI との交流が限られていることを明らかにした。 我々は、規模、地理的地域、2020 年米国大統領選挙における党派的嗜好の多様性を代表する 5 つの州の判断サンプルの関係者にインタビューを行った。 州レベルの政府と FBI との交流は、郡レベルの政府との交流よりも広範であったが、州と FBI との交流の大部分は、外国の悪意ある影響力とは関係がないようであった。 ほとんどの州は、選挙セキュリティに関する連邦政府の主要なパートナーは、FBI ではなく DHS/CISA であると表明した。

自国の選挙に向けられた外国の悪意ある影響への対策に関する FBI とのやりとりについて、州当局者は FBI と良好な関係を築いていると表明した。 私たちがインタビューした州当局者は、一般的な外国の悪意ある影響キャンペーンへの対応に重点を置くよりも、サイバー侵入や物理的インフラへのその他の攻撃から守ることに重点を置いていた。 さらに、州当局者は、自国の選挙に向けられた外国の悪意ある影響活動に関する FBI のインテリジェンスから特定の詳細を得る必要はないと話した。 例えば、州当局者は、どの外国人行為者が自国の選挙を攻撃しているかを詳細に示す帰属情報は、対応にとって重要ではないと語った。 むしろ州当局者が懸念していたのは、保護措置を講じるために必要な情報を得たり、選挙の継続的な完全性を確保したりすることだった。

各州の FBI との主な窓口は、選挙犯罪コーディネーター（Election Crimes Coordinators）と呼ばれる、国内発の選挙犯罪を扱う支局の FBI 捜査官であったが、前述のサイバーセキュリティ重視の観点から、各州は FBI のサイバー課とも接触していた（FITF とサイバー課の任務の違いについては、附属書 2 を参照）。 （FITF とサイバー課の任務の違いについては、附属書 2 を参照のこと）。 一部の州は、地元の連邦検事局（USAO）との接触も報告したが、ほとんどの州は、外国の悪意ある影響に関する USAO とのコミュニケーションは限られていた。

インタビューした州当局者の中には、FBI と連邦政府の他の部局、特に DHS との関係を十分に区別できない人もいた。 しかし、FBI との関係の深さにはばらつきがあるものの、州当局者は、必要であれば FBI に連絡を取ることができると確信しており、FBI との関係の重要な要素は、選挙システムの安全確保や有権者の安心に役立つ実用的な情報の提供であることを強調していた。

附属書 6．外国の悪質な影響に対抗する司法省の使命に関連する法律と政策の説明

我々の実地調査中、司法省と FBI の職員は、連邦法、大統領令、司法省と FBI の方針、捜査手段を確認した。これらは、司法省と FBI が、米国の選挙に向けられた脅威を含む外国の悪意ある影響力の脅威に関連する情報を収集する能力、およびこの任務に関連する情報を広める義務に関するパラメータを定めるものである。 以下に、これらの法律、命令、政策について説明する。

合衆国憲法修正第 1 条

"連邦議会は、宗教の確立、その自由な行使の禁止、言論・報道の自由、平和的に集会し、政府に苦情の救済を請願する人民の権利について、いかなる法律も制定してはならない。"

法令

以下の法令は、外国の悪意ある影響力の捜査に関連するものとして、インタビューに応じた人々によって特定されたか、米国の選挙に向けられた外国の悪意ある影響力に関する最近の起訴で起訴されたものである。

合衆国法典第 22 編第 611 条ほか-外国代理人登録法

外国代理人登録法(FARA)は、政治活動や同法に規定されたその他の活動に従事する外国元締めの特定の代理人に対し、外国元締めとの関係や、その活動を支援するための活動や出納を定期的に公開することを義務付けている。 必要な情報を開示することにより、政府および米国民は、外国代理人としての機能に照らして、そのような人物の活動を評価しやすくなる。 司法省国家安全保障局（NSD）の防諜・輸出管理課（CES）の FARA ユニットは、FARA の管理と執行を担当している。

合衆国法典第 18 編第 951 条-外国政府のエージェント

合衆国法律集第 18 編第 951 条は、外交官を除く、外国政府または外国高官の管理下で活動する斡 旋業者に対して、行動する前に米国司法長官に通知することを義務付けている。 FARA に基づく登録は、この法律の目的上、必要な通知として機能する。

合衆国法典第 18 編第 594 条-有権者の脅迫

合衆国法典第 18 編第 594 条は、連邦候補者を選出するためにのみ、あるいは部分的に行われる選挙において投票する、あるいは投票しない個人の権利を妨害する目的で、誰かを威嚇、脅迫、強制すること、あるいはそうしようとすることを禁止している。

合衆国法典第 18 編第 1030 条-コンピュータ詐欺・乱用法

コンピュータ詐欺・乱用法には、コンピュータに関する犯罪行為として、国家安全保障情報の入手、コンピュータにアクセスして情報を入手すること、政府のコンピュータに不法侵入すること、コンピュータにアクセスして詐欺を働き価値を得ること、故意に送信して損害を与えること、故意にアクセスして無謀にも損害を与えること、故意にアクセスして損害や損失を与えることに過失があること、パスワードを売買すること、コンピュータを使った恐喝の 7 種類が含まれている。

合衆国法律集第 18 編第 371 条-米国を欺く共謀罪

一般的な共謀罪である合衆国法典第 18 編第 371 条は、「二人以上の者が共謀して、合衆国に対して犯罪を犯すか、または合衆国もしくはその機関を、いかなる方法であれ、いかなる目的であれ、詐取する場合」を犯罪としている。　この法律の目的は、政府機能を欺瞞的行為による挫折や歪曲から守ることである。　ハス対ヘンケル事件（216 U.S. 462, 479 (1910)）における連邦最高裁判所によれば、第 371 条は「政府部門の合法的機能を損ない、妨害し、敗北させる目的のあらゆる共謀」に及び、これには連邦選挙も含まれる。

合衆国法典第 18 編第 875 条-州内通信

合衆国法典第 18 編第 875 条は、州をまたがる脅迫的通信の送信を禁止している。　他の条項の中でも、この法律は、州際通商または外国通商において、"人を誘拐するという脅迫、または他人の人を傷つけるという脅迫を含む通信 "を送信することを禁止している。

大統領令

大統領令 12333-米国の諜報活動

大統領令（E.O. ）12333 は、1981 年に発布され、その後数回の大統領令によって改正されたもので、米国情報機関を設立し、FBI を含む情報機関のさまざまな活動基準を定めている。　E.O.12333 は、国家安全保障に対する脅威を調査し、諜報活動を行う FBI の権限を定めている。　具体的には、国家情報長官と協議の上、司法長官が承認した手続きガイドラインに従い、国家および司法省の任務を支援するため、対外情報および防諜

情報を収集、分析、作成、発信することを FBI に求めている。 E.O.12333 はまた、対外諜報・防諜任務を遂行するために必要な対外諜報活動を行い、外国のパートナー機関との関係を構築するよう FBI に求めている。

司法省の方針

司法マニュアル§9-90.730-対外影響活動の開示

司法マニュアルには、公開されている司法省の方針と手順が記載されている。 9-90.730 項は、外国の影響力活動の開示に関するもので、被害者や一般市民に対して外国の悪意ある影響力活動を開示するかどうかを司法省が評価するための枠組みを提供している。 外国の悪質な影響力活動に関して同省が収集した情報は、連邦犯罪の逮捕および告発を支援するため、外国の影響力活動に起因する連邦犯罪の被害者に警告するため、脅威への対抗を支援するために必要な場合、外国政府が支援する秘密支援の無自覚な受領者に警告するために開示されることがある；テクノロジー企業やその他の民間団体に対し、そのサービスが秘密裏に外国政府のプロパガンダや偽情報を流布したり、政治組織や団体にその他の秘密裏の支援を提供するために使用されている場合、外国への影響力行使を警告する。

こうした通告を行うかどうか、またどのように行うかを決定する際、司法マニュアルは、いくつかの重要な原則と方針に留意するよう同省に指示している。 司法マニュアルは、米国に対する外国の影響力行使について、被害者、その他の影響を受ける個人、または米国民に注意を喚起する努力において、党派的な政治的配慮がいかなる役割も担ってはならないことを求めている。 そのような努力は、いかなる政治的、社会的集団、あるいはいかなる個人、組織に対しても、いかなる利益や不利益を与えることを目的とするものであってはならない。 外国の悪質な影響力活動を公表するかどうか、またどのように公表するかを検討するにあたり、司法マニュアルは、情報源や方法、捜査、その他の米国政府の活動を保護するよう求めている。 従って、外国政府による悪質な影響活動は、その活動が外国政府によるものであると高い信頼性をもって断定できる場合にのみ、米国司法省は公表する。 外国政府のために行動していない未知の情報源や国内情報源による偽情報やその他の支援、影響への対応は、外国による影響活動の公開に関する司法省の方針の範囲外である。 選挙期間中の犯罪捜査や国家安全保障に関する捜査が問題となる場合、司法マニュアルやその他の司法省の方針は、告発の時期や明白な捜査段階に関する長年の方針を守るよう、司法省とその構成機関に求めている。

司法長官による FBI 国内活動のガイドライン

司法長官の FBI 国内捜査ガイドライン（司法長官ガイドライン）は、米国内での FBI の捜査活動に関する司法省の方針を定めたものである。 司法長官ガイドラインは、FBI が入手または作成した情報を、FBI および司法省内だけでなく、他の連邦、州、地方、または部族の機関や米国情報コミュニティとも、その責務に関連する場合は「許容的共有」することを認めている。 司法長官ガイドラインによると、FBI は、情報共有に関する特定の制約によって制限されている場合を除き、米国とその国民をテロリズムや国家安全保障に対するその他の

脅威から守るため、関連する責任を持つ機関に、可能な限り一貫して完全に情報を提供する責任を負っている。

司法長官ガイドラインはまた、憲法修正第 1 条で保護された活動を監視する目的だけのために、米国人に関する情報を調査、収集、保持することを禁じている。

FBI の方針

国内調査および業務ガイド

国内捜査および活動ガイド（DIOG）は、米国内、米国領土内、またはすべての国の領土外で FBI が行うすべての捜査活動および情報収集活動に適用される。 DIOG は、外国内での FBI の捜査活動および情報収集活動には適用されない。

憲法修正第 1 条の FBI 活動への適用

DIOG は、憲法修正第 1 条の適用に基づき、FBI の捜査活動に制限を設けている。 DIOG によると、「FBI は、(i)その収集が許可された捜査目的と論理的に関連している、(ii)その収集が発言者のメッセージ伝達能力を実際に侵害しない、(iii)その収集方法が最小侵襲的方法ポリシーに準拠している限り、憲法で保護された言論の内容を合法的に収集、保持、検討することができる」という。 DIOG はさらに、保護された言論を伝える人の能力を低下させる法執行活動は、その人の憲法修正第 1 条の権利を妨害する可能性があり、したがって、その人の言論の自由を妨害する目的のみで FBI が行うことはできないと述べている。 このような制限があるにもかかわらず、DIOG は、「言論の自由を妨害したり、言論に従事する者を罰するための高い基準にもかかわらず、法律は、FBI 職員が、保護される言論の形態を観察し、収集し、その内容を検討することを妨げるものではない。

査定と調査

FBI は、捜査活動を査定、予備捜査、完全捜査に分類している。

捜査は、活動の根拠となる事実の確実性（述 定と呼ばれる）のレベルに応じて行われる。 査定は、連邦犯罪や国家安全保障への脅威を探知、情報を入手、防止、保護するため、あるいは対外情報を収集するために実施される。 査察を開始するために「特定の事実を前提とすること」は要求されないが、査察の根拠は恣意的または根拠のない憶測であってはならず、また憲法修正第 1 条で保護された活動の行使のみに基づいて査察を行うこともできない。 FBI は、犯罪または国家的脅威の活動の可能性について事実による推定を行った場合、予備調査または本調査を開始することができる。 予備捜査とは、犯罪行為または国家安全保障への脅威の可能性を示す申し立てまたは情報に基づく捜査活動である。 完全捜査とは、連邦犯罪または国家安全保障に対する脅威を構成する活動が発生した、または発生した可能性がある、発生中である、または発生する可能性がある、と

いう明確な事実的根拠がある場合の捜査活動である。 調査は、そのような活動、またはそのような活動への個人、グループ、組織の関与や役割に関連する情報を得ることができる。

FBI は、査定または正式な捜査を開始する前に、限定的な情報収集を行うことが許されているが、査定または捜査が開始されると、FBI 職員はさまざまな捜査手段を用いることができるようになる。 FBI 職員が利用できる捜査手段は、査定や捜査の種類によって異なる。

米国の選挙に向けられた外国の悪意ある影響に対抗するためによく使われる調査ツール

大陪審召喚状

刑事事件では、検察官が大陪審に証拠を提出し、大陪審は、個人が犯罪を犯し、裁判にかけられるべきと信じるに足る理由があるかどうかを判断する。 特定の FBI 査察において、FBI は現地の連邦検事局（USAO）および NSD と連携し、電子メール・プロバイダーやソーシャルメディア・プラットフォームなど、電子通信サービスやリモート・コンピューティング・サービスのプロバイダーから加入者や顧客情報を入手するための大陪審召喚状を発行することがある。 FBI はまた、USAO や NSD と協力して、捜査中に、加入者情報だけでなく、捜査に関連するその他の情報も含めて、大陪審の召喚状を取得することがある。 司法管轄区によっては、大陪審召喚状によって得られた情報の共有が裁判所の判決によって制限される場合があり、IC パートナーなどの他の連邦機関とそのような情報を共有する前に、NSD を含む USAO および司法省とさらに協議する必要がある。 連邦刑事訴訟規則 6(e)は、大陪審で発生するほとんどの情報に秘密保持の要件を課しているが、連邦検察官が外国情報、防諜、テロ関連の脅威情報を共有することを認めている。[49] このような情報は、法律で許される最大限の範囲内で、規則と矛盾しない方法で共有されなければならないというのが、司法省の方針である。 大陪審召喚状の発行に関する FBI の監督承認要件はないが、すべての大陪審召喚状は、評価または捜査を扱う USAO によって発行されなければならない。

2703(d)命令

電子通信プライバシー法（ECPA）第 2703 条は、政府が電子情報を入手するためのいくつかの仕組みを規定している。[50] その一つである 2703(d)命令は、米国の選挙に向けられた外国からの悪意ある影響に対抗するという FBI の任務において一般的に使用されている。 2703(d)命令を求める捜査官は上司の承認を必要とせず、連邦検事補と NSD と協力して裁判所命令を要請する。 このような命令を得るためには、FBI は、有線通信や電子通信の内容、あるいは求められている記録やその他の情報が、進行中の犯罪捜査に関連し、かつ重要であ

---

[49] 連邦刑事訴訟規則 6(e)。

[50] ECPA は、有線通信、口頭通信、電子的通信を、それらの通信が行われている間、それらが転送されている間、およびそれらがコンピュータに保存されている間に保護する。 同法は、電子メール、電話での会話、電子的に保存されたデータに適用される。

ると信じるに足る合理的な根拠があることを示す、具体的かつ明確な事実を提示しなければならない。 合衆国法典第 18 編第 2703 条(d)により許可された裁判所命令は、連邦判事、連邦地方裁判所、または同等の州裁判所判事により発行される。[51]

ECPA によると、裁判所が 2703(d)命令を出した場合、電子通信サービスまたはリモート・コンピューティング・サービスのプロバイダは、加入者の氏名、住所、市内および長距離電話の記録、またはセッションの時間および持続時間の記録、サービスの期間（開始日を含む）および利用したサービスの種類、電話番号または計器番号、または一時的に割り当てられたネットワーク・アドレスを含むその他の加入者番号または身元、およびサービスの支払手段または支払元（クレジットカード番号または銀行口座番号を含む）を開示しなければならない。[52] インタビュイーによれば、2703(d)命令の利点のひとつは、命令による返却が連邦刑事訴訟規則 6(e)の適用を受けないため、FBI が収集した情報を他者と共有することが容易になることである。 FBI 捜査官は、2703 条(d)命令を利用して、ソーシャルメディアやその他のオンライン・アカウントのアカウント・ログや過去の取引記録を入手することができ、これは、FBI が外国情報機関の諜報員が追加のアカウントを管理しているかどうかを判断するのに役立つ。[53] FBI は、2703(d)命令から得られた情報をもとに、捜査令状の正当な理由を作成する。

捜索令状

電子ストレージのコンテンツへのアクセスには、ECPA2703 条(a)に基づき、連邦裁判所が発行する捜査令状が必要である。 FBI は、捜査令状によってネットワーク・アカウントの全内容を入手することができ、これにより、召喚令状または 2703(d)命令によってまだ入手されていない可能性のあるアカウントに関するあらゆる情報を入手することができる。 電子記憶情報を取得するための捜査令状は、顧客や加入者に通知することなくプロバイダに発行することができる。 捜査令状を求める捜査官は、NSD の CES が監督する法令違反に関する捜査など、特定の場合には USAO または DOJ 本部と調整する。 この場合の捜査令状は、タイトル III の捜査令状とは異なる。 タイトル III の捜査令状は、アカウントからリアルタイムの情報を提供するために使用することができ、米国の選挙に向けられた外国の悪意ある影響に関わるケースでは頻繁に発行されるものではない。

---

[51] 合衆国法律集第 18 編第 2703 条(d)、第 2711 条(3)。

[52] 合衆国法典第 18 編第 2703 条(c)(2)。

[53] 連邦裁判所によって出された 2703 条(d)命令は、それを出した裁判所の管轄区域外でも効力を持つ。つまり、2703 条(d)命令は、たとえその情報が発行した裁判所の管轄区域外に保存されていたとしても、プロバイダに対して情報開示を強制することができる。

附属書 7：報告書草案に対する同省の回答

U.S. Department of Justice

Office of the Deputy Attorney General

Office of the Deputy Attorney General

950 Pennsylvania Ave., N.W.
RFK Main Justice Bldg.
Washington, D.C. 20530

MEMORANDUM

TO: Allison Russo
Assistant Inspector General
Evaluation and Inspections Division
Office of the Inspector General

FROM: George D. Turner
Associate Deputy Attorney General
Office of the Deputy Attorney General

DATE: July 12, 2024

SUBJECT: Department of Justice's Response to Formal Draft Report, "Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections"

The Department of Justice (DOJ) appreciates the opportunity to provide a response to the Formal Draft Report prepared by the Office of the Inspector General (OIG), transmitted to DOJ on May 30, 2024, entitled "Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections" (Formal Draft Report). This response reflects the consolidated input of relevant DOJ components, including the Federal Bureau of Investigation (FBI), National Security Division (NSD), Executive Office for United States Attorneys, and Civil Division.

Below, we address the two recommendations contained in the Formal Draft Report. The Department concurs with both recommendations, as explained more fully herein.

First Recommendation

The first recommendation calls for DOJ to "[d]evelop an approach for informing the public about the procedures the Department has put into place to transmit foreign malign influence threat information to social media companies that is protective of First Amendment rights." As reflected in the Formal Draft Report, following the district court's July 2023 decision in *Missouri v. Biden*, DOJ worked over several months to develop a standard operating procedure (SOP) for sharing foreign malign influence (FMI) information with social media companies that serves and promotes two fundamental DOJ priorities: combatting FMI operations

posing a threat to U.S. national security, and protecting the vital First Amendment rights of Americans. Recognizing that FMI threats are constantly evolving, the SOP is designed to be an adaptive document. The first iteration of the SOP was implemented in early February 2024, and DOJ—through FBI—has been actively sharing FMI threat information with social media companies pursuant to the SOP since then.

We concur with OIG's first recommendation, as we believe it will be beneficial to ensure that the public is aware that DOJ's sharing of information with social media companies about potential FMI threats to national security, including election interference, is undertaken pursuant to carefully calibrated protocols that protect First Amendment rights. We will address this recommendation by making publicly available a detailed summary version of the SOP and posting that summary on DOJ's website by July 31, 2024. We will also further inform the public about the SOP through DOJ's planned outward-facing actions responsive to OIG's second recommendation, as discussed below.

As background with respect to the SOP, in July 2023, a Louisiana district court issued an injunction in *Missouri* restricting FBI's engagement with social media companies based on the judge's view that such engagement was likely violative of the First Amendment because it involved allegedly coercive requests to remove content from the companies' platforms. In September 2023, the Fifth Circuit upheld a modified version of the injunction. *Missouri v. Biden*, 83 F.4th 350 (5th Cir. 2023). The Supreme Court subsequently stayed the injunction in October 2023. On June 26, 2024, the Supreme Court reversed the Fifth Circuit's judgment, holding that the plaintiffs lacked standing to seek such an injunction. *Murthy v. Missouri*, No. 23-411 (June 26, 2004).

Following the October 2023 stay, DOJ began developing a standardized approach for sharing FMI information with social media companies that continued to appropriately account for First Amendment considerations. Over several months, DOJ worked to formulate such guidance, which ultimately resulted in the SOP.

The SOP reflects the fundamental premise, rooted in longstanding Supreme Court precedent, *see, e.g.*, *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963); *Blum v. Yaretsky*, 457 U.S. 991 (1982), that it is permissible and appropriate for FBI to share FMI information with social media companies, as long as it is clear that ultimately it is up to the company whether to take any action, such as removing content or barring users, based on the shared information. The SOP includes, among other things, the following principles, guidance, and protocols:

- The SOP recognizes the critical importance both of DOJ being able to share FMI threat information with social media companies in order to carry out DOJ's national security mission, and of doing so in a manner that does not infringe upon on any applicable First Amendment protections.

- The SOP defines what constitutes FMI with reference to specific categories of FMI activity and information.

- The SOP requires that certain conditions must be met for FBI to share FMI information with a social media company, including that the FBI personnel has identified specific, credible, and articulable facts that provide high confidence for assessing that the information at issue relates to activity attributable to a foreign government, foreign non-state actor, or their proxy engaged in an FMI operation.[1]

- The SOP requires that communications with social media must include a standardized caveat explaining that FBI does not request or expect the receiving company to take any particular action based on the shared information.

- The SOP specifies procedures for how FBI personnel can appropriately respond to follow-up questions or requests from social media companies seeking additional information from FBI after receiving FMI information.

Since the SOP went into effect in early February 2024, FBI has been actively sharing FMI threat information with social media companies on a continuing basis pursuant to the SOP. We look forward to informing the public about the SOP by posting a summary version of the SOP on our website, and to further highlighting and explaining the SOP to the public as part of the planned actions discussed below in response to the second recommendation.

Second Recommendation

The second recommendation calls for DOJ to "[d]evelop and implement a comprehensive strategy to ensure that the Department of Justice's approach to information sharing with social media companies to combat foreign malign influence directed at U.S. elections can adapt to address the evolving threat landscape." While we concur with this recommendation, we note that, over the course of several years and as further outlined below, DOJ has already developed and is actively implementing a strategic approach (which includes the SOP) for sharing information with social media companies and combatting the inherently fluid threat of FMI directed at our elections. We plan to address this recommendation by taking a series of additional actions by August 31, 2024 to further refine and strengthen our strategy, including:

- **Development and Release of Strategic Principles.** DOJ will set forth in a public manner the principles reflecting DOJ's strategy for sharing FMI information with social media companies to combat the evolving threat landscape.

- **Resumption of FBI's Regular Meetings with Social Media Companies.** As part of that strategy, FBI will resume regular meetings in the coming weeks with social media companies to brief and discuss potential FMI threats involving the companies' platforms.

[1] The Formal Draft Report suggests that the SOP might permit FBI employees to use "pre-populated or boilerplate criteria when justifying a disclosure of information to a social media company." Formal Draft Rpt. at 27. To the contrary, and as set forth above, the SOP requires FBI employees to identify specific, credible, and articulable facts—which must be reflected in the report transmitted to the social media company—supporting a high-confidence FBI assessment that the shared information relates to an FMI threat.

FBI will conduct these meetings—as FBI did before pausing the meetings in summer 2023 due to the now-vacated *Missouri* injunction (*see infra* at 5)—in a manner that is entirely consistent with applicable First Amendment principles. As has been FBI's practice, FBI will conduct these engagements with social media companies located across the country, depending on the circumstances and nature of the potential threats.

- **Outreach by FBI Field Offices to Social Media Companies.** FBI will instruct FBI Field Offices in the coming weeks to conduct outreach—in coordination with the FBI's Foreign Influence Task Force (FITF)—to any identified social media companies located in their areas of responsibility, to develop contacts at those companies and ensure they are aware of the SOP and DOJ's overall approach for engaging with social media companies regarding FMI threat information.

- **Engagements by Senior Officials.** In the coming months, senior DOJ officials will highlight and explain, during public engagements with relevant stakeholders and the public, DOJ's strategy for information sharing with social media companies to combat FMI directed at our elections.

- **Launch of DOJ Website Page.** DOJ plans to launch a new section on its website dedicated to ensuring public awareness of DOJ's strategy for engaging with social media companies regarding FMI. The website page will collect and highlight in a single location relevant resources, guidance, and other materials, including the summary of the SOP discussed above.

As background, the U.S. Intelligence Community (USIC) has publicly described how the FMI operations of hostile state actors from China, Iran, and Russia directly threaten U.S. national security. *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024), at 12, 17, 20. Congress has specifically recognized that FMI poses a serious threat to national security, finding in 2019 that foreign actors have used social media platforms to engage in FMI activities that threaten U.S. national security, and likely will continue to do so. 50 U.S.C. § 3369. Congress found, among other things, that foreign adversaries were deploying "information warfare operations [involving] the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion." 50 U.S.C. § 3369(a)(2). Congress also found that "[b]ecause these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms." *Id.* § 3369(a)(7). The statute further states that "information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations." *Id.* § 3369(b)(2).

Since well before those Congressional findings, DOJ, acting through the FBI, has been working to combat FMI. In the fall of 2017, the FBI Director established FITF to combat the emerging FMI threat. As set forth in FITF's Mission and Strategy framework, referenced in the Formal Draft Report, FITF is a multi-division FBI section comprised of operational and

analytical personnel from the FBI's Counterintelligence, Cyber, and Criminal Investigative Divisions with the authority and mandate to identify, investigate, and combat FMI operations targeting U.S. democratic institutions, with specific focus on the U.S. electoral process. FITF serves as FBI's central coordination point for the USIC and international partners for engaging in a whole-of-government approach to combatting FMI threats. The FBI, principally through FITF, is the DOJ component responsible for engaging with social media companies—including through information sharing—regarding FMI threats.

FITF's formative Mission and Strategy document expressly includes the strategic priority of sharing FMI threat information with social media companies, while also highlighting the imperative of not infringing upon First Amendment rights. As set forth in that strategy framework, FITF's key lines of effort since its inception have included: (a) "Lead the engagement with social media and Internet technology providers to enable an effective dialogue focused on 1) understanding and leveraging the visibility and capabilities of these providers, and 2) providing actionable direction to enable self-monitoring and mitigation efforts of those organizations' platforms"; and (b) "Develop a clear strategic messaging framework to define USG's posture for specific key audiences [including] Internet technology and social media providers." The strategic framework further provides that, in carrying out its mission, FITF must "protect the rights embodied in the Constitution" and, in particular, avoid engaging in any investigative activities "based upon speech protected under the First Amendment."

As DOJ has developed and deployed its strategy for engaging with social media companies about FMI, we have also drawn on and implemented guidance from an array of other sources, including guidance specifically directed at ensuring that First Amendment rights are protected. For example, all of FBI's investigative activity, including information sharing with social media companies, must adhere to the Attorney General Guidelines on Domestic Investigations (AGG-DOM) and the FBI Domestic Investigations and Operations Guidance (DIOG). Both documents reinforce the core principle that FBI must protect the rights and liberties of all Americans. The AGG-DOM provides that all investigative activities "must be carried out in conformity with the Constitution and all applicable statutes," and specifically prohibits "investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment." AGG-DOM § I(C)(3). The DIOG expands on this principle and includes a section dedicated to requirements related to protecting First Amendment activity. The DIOG notes that "[n]o investigative activity . . . may be taken solely on the basis of activities that are protected by the First Amendment," and that "even 'monitoring' the exercise of First Amendment rights" is prohibited. DIOG §§ 5-2, 4-3. The DIOG also provides that "when First Amendment rights are at stake, the choice and use of investigative methods should be focused in a manner that minimizes potential infringement of those rights." *Id.* § 4-19.

Further, the Justice Manual (JM) sets forth DOJ policy principles regarding the disclosure of foreign influence operations. *See* JM § 9-90.730. As set forth in the JM, it is "the Department's policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with the Department's policies and practices, and with our national security interests." *Id.* Recognizing that it is often not possible or prudent to publicly disclose FMI operations because of investigative considerations, the JM provides a strategic

framework for DOJ to evaluate whether, when, and under what circumstances to disclose FMI operations. This strategic approach includes that DOJ may disclose FMI threat information "[t]o alert technology companies or other private sector entities to foreign influence operations where their services are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups." *Id.*[2]

As part of DOJ's strategy for engagement with social media companies, following the 2018 midterm elections, FBI established a practice of regularly meeting with social media companies to discuss potential FMI threats on the companies' platforms. FITF coordinated and led the meetings, which involved an array of social media companies located in the San Francisco area given the cluster of such companies based there, as well as other social media companies located in other regions. These meetings afforded a valuable opportunity for two-way discussion, enabling FBI and social media companies to share information that both sides were seeing on the companies' platforms relating to potential threat indicators and trends. FBI met with each company individually, rather than in a group setting with industry competitors present, to facilitate the most fulsome and productive engagement regarding potential threat information implicating the company's platform. FBI met with each company on a quarterly basis, and also met with companies more frequently depending on threat-specific factors—such as when a particular company requested to discuss potential FMI threats with FBI, and when FBI was aware of information indicating that an FMI actor was poised to leverage a company's platform in furtherance of FMI operations. However, in summer 2023, FBI suspended these regular meetings with social media companies following the issuance of the injunction in *Missouri*. As set forth above, and in light of the Supreme Court's recent decision, FBI will resume these meetings—which are both important to DOJ's national security mission and fully consistent with the First Amendment—on an expedited basis, and will conduct these meetings with social media companies located across the country.

As reflected in the Formal Draft Report, another key prong of DOJ's strategy for sharing FMI threat information with social media companies over the past several years has been, and remains, providing specific threat-related data to social media companies on a continuous basis. Specifically, FBI obtains information from the USIC relating to FMI actors leveraging particular online platforms, and FBI then promptly shares that information with the relevant social media company. This strategic approach combats FMI threats in multiple critical ways, including by enabling the company to remove or otherwise regulate the content on its platform, to the extent the company elects to do so, and by facilitating further investigation of the FMI actors involved—including through the company's gathering of additional relevant information pursuant to legal process served by FBI. As set forth above, in early February 2024, DOJ implemented the SOP, which established the existing framework for this prong of DOJ's information-sharing strategy, consistent with applicable First Amendment principles.

---

[2] Footnote 6 of the Formal Draft Report references a separate classified guidance document, which was formulated in 2019 through an interagency process and was not issued by DOJ. This guidance articulated principles for other government agencies' efforts to combat FMI operations, and has been provided to OIG.

As the foregoing reflects, DOJ has developed and is actively implementing an evolving, multi-faceted, strategic approach for sharing FMI threat information with social media companies that is creative, impactful, and protective of First Amendment rights. Nevertheless, we welcome OIG's recommendation, as we continuously strive to enhance our strategy and inform the public about our work, and we will address the recommendation through the planned series of actions outlined above.

附属書 8：同局の回答に対する OIG の分析

OIG は本報告書の草案を同省に提供し、コメントを求めた。　同省の回答は本報告書の附属書 7 に含まれている。　同局の回答に対する OIG の分析と、勧告を解決するために必要な措置については、後述する。

勧告 1

憲法修正第 1 条の権利を保護し、ソーシャルメディア企業に外国の悪意ある影響脅威情報を送信するために同省が導入した手続きについて、国民に周知するためのアプローチを策定する。

ステータス　解決済みである。

司法省の回答　同省は勧告に同意し、司法省が選挙妨害を含む国家安全保障に対する潜在的な外国の悪意ある影響力の脅威に関する情報をソーシャルメディア企業と共有することは、憲法修正第 1 条の権利を保護する慎重に調整されたプロトコルに従って実施されていることを国民に確実に認識させることが有益であると述べた。同省は、ソーシャルメディア企業と外国の悪質な影響力の脅威に関する情報を共有するための同省の手続きの概要を作成し、2024 年 7 月 31 日までにその概要を司法省のウェブサイトに掲載すると述べた。

OIG の分析　司法省の提案した措置は勧告に対応している。　2024 年 10 月 23 日までに、ソーシャルメディア企業と外国の悪質な影響力の脅威情報を共有するための同省の手順の公開要約のコピーと、要約が司法省のウェブサイトに掲載されたことを示す文書を提出すること。

勧告 2

米国の選挙に向けられた外国の悪意ある影響に対抗するためのソーシャルメディア企業との情報共有に対する司法省のアプローチが、進化する脅威の状況に対応できるよう、包括的な戦略を策定し、実施する。

ステータス　解決済みである。

同省の回答　同省は勧告に同意し、ソーシャルメディア企業と情報を共有し、米国の選挙に向けられた外国の悪意ある影響力という本質的に流動的な脅威に対抗するための戦略をさらに洗練・強化するため、2024 年 8 月 31 日までに一連の追加行動を取ると表明した。　同省が計画している行動には、ソーシャルメディア企業と外国の悪質な影響力に関する情報を共有するための戦略原則を策定し、公表すること、ソーシャルメディア企業と定期的な会合を再開し、ソーシャルメディア企業のプラットフォームに関わる外国の悪質な影響力の脅威の可能性について話し合うことなどが含まれる、FBI の現場事務所と FBI の対外影響タスクフォース（FITF）に対し、こうした関与に関する同省の全体的な戦略に従って、担当地域内のソーシャルメディア企業へのアウトリーチを実施するよう指示すること、関連する利害関係者との公開の場で同省の戦略を強調すること、同省の

戦略と指針を一般に周知させるため、司法省のウェブサイトに新しいセクションを設けることなどが含まれる。

OIG の分析　同局の提案した措置は勧告に対応している。　2024 年 10 月 23 日までに、以下の書類を提出すること：

- には、前述の通り、同省の戦略原則が盛り込まれている；
- この報告書の日付以降に、FBI がソーシャルメディア企業との間で、その企業のプラットフォームに関わる潜在的な外国の悪意ある影響力の脅威について話し合った会議；
- この報告書の日付以降、FBI の現場事務所と FITF がソーシャルメディア企業への働きかけを実施した努力は、外国の悪意ある影響情報をソーシャルメディア企業と共有するための FBI の戦略原則に沿ったものであった；
- 参加者、日時、場所、議論のテーマなど、司法省高官による関係者との関わり、およびこれらのイニシアチブを公表するために司法省が作成したウェブページ。