“あなたの家族は苦しむだろう”

中国が自由民主主義国のウイグル人をハッキング、監視、脅迫している方法

UHRP
UYGHUR HUMAN RIGHTS PROJECT
ئۇيغۇر كىشىلىك ھوقۇق قوغدۇلۇشى

THE OXUS SOCIETY
FOR CENTRAL ASIAN AFFAIRS

ウイグル人権プロジェクトについて

ウイグル人権プロジェクト（UHRP）は、研究に基づくアドボカシーを通じてウイグル人の権利を促進する。 我々は、国際人権基準に従ってウイグルの市民的、政治的、社会的、文化的、経済的権利を擁護するために、英語と中国語でレポートと分析を公開している。

中央アジア問題のためのオクサス協会（Oxus Society）について

中央アジア問題のためのオクサス協会は、中央アジアと世界の他の地域との間の学術交流を促進することを目的としたワシントンDCに本拠地を置く非営利団体。

著者

Natalie Hallは、中央アジア問題のためのオクサス協会の研究者であり、カーネギー国際平和基金の元プログラムコーディネーターである。
Bradley Jardineは、中国と米国のキッシンジャー研究所のウィルソン・センターのグローバルフェローおよび中央アジア問題のためのオクサス協会の研究ディレクターである。

謝辞

著者は、このレポートを専門的レビューとして編集して下さったUHRPの研究とアドボカシーのためのシニアプログラムオフィサーElise Anderson博士；UHRP開発、展開、およびリサーチオフィサーReece Thompson；UHRPリサーチディレクターHenryk Szadziewskiに感謝の意を表明します。また、このレポートのために国境を越えた弾圧の真実を共有することを申し出たすべてのウイグル人に心より感謝いたします。 最後に、著者は人権とデジタルセキュリティポリシーに関するアドバイスして下さったEliza Campbellに感謝したいと思います。
カバーはYetteSuによってデザインされた。

1602 L Street NW | Washington, DC 20036
www.uhrp.org | info@uhrp.org

www.oxussociety.org | info@oxussociety.com

目次

I. 要約

2002年以来、中華人民共和国（PRC）は、海外に住むウイグル人を統制する取り組みの一環として、前例のない国境を越えた抑圧活動に携わってきた。その結果、ウイグル人は、絶えることなくハラスメント、脅迫、弾圧という形で、中国の権威主義体制を長い間味わってきた。この恐怖の行動は、2017年から中国がウイグル地方で大規模な弾圧と抑留の政策の開始とともに劇的に拡大していった。

このレポートは、中国によるウイグル人への国境を越えた抑圧に関する以前の研究を拡張し、ウイグル人権プロジェクトおよび中央アジア問題のためのオクサス協会と協力して収集された、19年の間22カ国にわたるステージ1の国境を越えた抑圧の5,530例がデータセットに追加された。脅迫やハラスメントの事件は報告されないことが多く、この数はハラスメント事件とその影響を受けたウイグル人の数ははるかに多い可能性があることを示唆している。中国の第1段階のウイグル人の国境を越えた抑圧が、第2段階と第3段階の抑圧の事例と並行して広範囲に及んでいることは、中国政府が海外に住んでいるウイグル人をどのように追跡し、弾圧し、脅迫し、不安、恐怖、うつ病をもたらしたかを示している。

北米、アジア太平洋、ヨーロッパの自由民主主義の国々に住む72人のウイグル人に調査を行った。そのうち、95.8％が脅迫されていると報告し、73.5％がデジタルリスク、脅威、またはその他の形のオンラインハラスメントを経験したと述べた 。世界中のウイグル人は自分たちを守ることに関心があり、89.7％の回答者がセキュリティに関する知識を増やすことに関心を示している。しかし、多くの回答者は、この保護が必ず自国政府によるものであるとは感じてはいなかった。44.1％の回答者が、受け入れ国政府がこの脅迫を真剣に受け止めるべきだと感じており、たった20.5％だけが受け入れ国政府がこれらの問題を解決すべきだと感じている。

我々のレポートは、中国政府によって侵害された民主主義の世界に住んでいるウイグル人が、民主主義政府によって保証された権利をどのように持ち続けているか、そして国家の同調者がデータ収集、監視、脅迫、ハラスメントを通じて、ウイグル人、さらには他の多くの人の自由をどのように制限しているかに主に焦点を当てて調査データの分析をおこなったものである。中国の権威主義は国境をはるかに超えている。一党独裁の国が他の国とそれらの組織をウイグル人に対する暴力と脅迫の行動に引き入れ、国や他の関係者はまだウイグル人の保護に責任を負ってはいない。

さらに、我々の調査結果は、非ウイグル人が彼らの自由と個人の権利を脅かすこの活動の標的になっていることを示唆している。また、海外に住んでいるウイグル人の脅迫とハラスメントに関するオープンソースのニュース報道に総合的なレビューを行うことにより、中国のウイグル人の国境を越えた抑圧に関する既存のデータセットが拡張されていった。さらに、この公開されているデータが、世界中のウイグル人に行った10件のオリジナルのインタビューとして追加されている。これらの我々が収集して分析した情報は、これまでのウイグル人のデジタル不安の最も総合的な調査の1つであることを示唆している。

この世界的展開への対応もグローバルでなければならない。 オクサス協会とUHRPは、市民社会と民間部門、政府、および政府間組織に対する13の勧めによって、下記を含めて迅速な行動を促している：

- 政府は、難民の入国枠を増やし、官僚的障壁を合理化し、手続きを合理化し、デジタル衛生教育プログラムを含むデジタルハラスメントの影響を緩和するための支援などを提供することにより、ウイグル難民の第三国再定住プログラムのための安全な避難所を作るべき。
- 政府は、この国境を越えた弾圧に関与する中国の国家機関の代価を引き上げることにより、説明責任を強化するべき。
- すべての関係者は、人権のプライバシーに関する審議と個人情報の保護の中に、デジタル権利の実現化を組み込むべき。
- 民間部門は、ウイグル語、中国語、トルコ語など、関連するすべての言語でオンラインプラットフォーム上のデジタル脅威を監視し、国家主体のハラスメントを特定するツールを開発し、適切な言語で安全な通信プラットフォームを利用できるようにするべきだ。

II. 序論

2019年、オーストラリアに住むウイグル人のNurgul Sawutは、ボットネットのより自分のFacebookアカウントが標的にされていたことが分かった。 この偽のアカウントの集まりは、彼女の妹のプロフィールを模倣し、公的な非難の活動として彼女を攻撃し、彼女のパソコンをマルウェアに感染させた。 このマルウェア（対象者の電子デバイスへのアクセスと制御を提供するなど悪意のソフトウェア）は、Sawut氏の電話に2回侵入した。 一つのケースでは、彼女はデバイスをリセットすることができたが、もう一つのケースでは、彼女は自分の携帯を完全に破棄しなければならなくなった。 それ以来、彼女は暗号化された電子メールの使用を開始し、WeChatを携帯電話にダウンロードすることを避け、Facebookアカウントの外部アプリ連携を解除した。

彼女の反抗に対する報復として、Sawut氏は中国の治安機関が新疆ウイグル自治区（XUAR）1に住んでいる親戚たちを逮捕および拘留したと考えた。 その後、2021年に、彼女は自分の名前が中国の「テロ容疑者」リストに載っている10,000人の一人であることを知り、彼女は自分の行動主義に基づいて、驚いてはいないと発言した２。 しかし、多くのウイグル人にとって、そのような告発は警告としてもたらされ、たくさんのウイグル人が海外で中国の追加的な監視の対象となっていることを示唆している。 ウイグル人の多くの人々と同様に、Sawut氏は、主権の国境を越えた、中国の慣行である強制感を感じていた[3]。

---

[1] 我々はこの地域を「ウイグル地域」と「XUAR」（「新疆ウイグル自治区」の略）と呼びる。世界中のウイグル人は、中国の当局が好む「新疆ウイグル自治区」の短縮形である「新疆」を攻撃的な植民地用語と見なしている。 「ウイグル地域」に加えて、多くのウイグル人は彼らの故郷を「東トルキスタン」とも呼んでいる。

[2] Josh Taylor, “I Can't Be That Careless': Australian Uyghur Activist Targeted Online,” *Guardian,* May 15, 2021, https://www.theguardian.com/world/2021/ may/16/i-cant-be-that-careless- australian-uyghur-activist-targeted-online.

[3] “Repression across Borders: The CCP’s Illegal Harassment and Coercion of Uyghur Americans,” Uyghur Human Rights Project, August 28, 2019, https://docs.uhrp.org/pdf/UHRP_RepressionAcrossBorders.pdf.

現在、推定50万人のウイグル人が世界中に住んでおり、中央アジア、トルコ、ヨーロッパ、アジア太平洋、および北アメリカが主に人口集中地となっている。 我々の以前の報告によると、これらのコミュニティは、特に権威主義体制の国々のウイグル人、中国政府は、海外のウイグル人を追跡し、本国に送還を要求するよう各国の治安機関に圧力をかけており、協力を要求しているため、ますます頭を抱えている[4]。1997年以来、海外に住む1,149人のウイグル人が中国の治安機関の要請により受け入れ国政府によって拘留され、その中でも同じ期間に確認された427人のウイグル人が東南アジアと中東に集中しており、中国に移送または返還された5。合わせて、これらの個人は、国境を越えた抑圧の1,548の別々のケースで表されている[6]。

我々がステージ2とステージ3として分類したこれらの形態の抑圧は主にイスラム世界で起こっているが、西側の民主主義もまた、ステージ1の抑圧、つまり逮捕と送還のレベルに達していない脅迫の形態で包囲されている 7 。まとめて、我々のデータは、ウイグル人の国境を越えた抑圧の7,078件が世界中で発生したことを示唆している。ウイグル人が国家支援の脅迫の標的になることが多くなるにつれて、敵性外国勢力が民主主義国々のウイグル人住民の憲法上および政治上の権利を弱体化させる公民権の2層モデルが出てきた。政策立案者と観察者が同様に懸念しているのは、国家機関とその代理人たちは処罰されずマルウェア、ボットネット、さらには追跡デバイスを使用して監視、ハラスメント、脅迫に伴い、新興技術が北京の国境を越えた抑圧の能力をどのように加速させているかである。特にデジタル技術は、中国共産党に、ディアスポラウイグル人の活動を監視し、治外法権の政治的統制のコストを削減するための新しいツールを提供し、国境を越えた中国国家の範囲が拡大されていた。

ウイグル人が国家支援の脅迫の標的になることが多くなるにつれて、敵性外国勢力が民主主義国々のウイグル人住民の憲法上および政治上の権利を弱体化させる公民権の2層モデルが出てきた。

[4] Bradley Jardine, Edward Lemon, and Natalie Hall, “No Space Left to Run: China’s Transnational Repression of Uyghurs,” Oxus Society for Central Asian Affairs and the UyghurHuman Rights Project, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas- transnational-repression-of-uyghurs/.

[5] Bradley Jardine and Robert Evans, “Nets Cast From the Earth to the Sky: China’s Hunt for Pakistan’s Uyghurs,” Uyghur Human Rights Project and Oxus Society for Central Asian Affairs,August 18, 2021, https://oxussociety.org/nets-cast-from-the-earth-to-the-sky-chinas-hunt-for- pakistans-uyghurs/.

[6] “China's Transnational Repression of Uyghurs Dataset,” Oxus Society for Central Asian Affairs, accessed on August 8, 2021, https://oxussociety.org/viz/transnational-repression/.

[7] Bradley Jardine, Edward Lemon, and Natalie Hall, “No Space Left to Run: China’s Transnational Repression of Uyghurs,” Uyghur Human Rights Project and Oxus Society forCentral Asian Affairs, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas- transnational-repression-of-uyghurs/.

このレポートは、中国とその国際的代理がディアスポラウイグル人の監視とハラスメントの体系的な活動に携わっている方法と範囲を調査する。 我々の研究は主に民主主義に焦点を当てている。民主主義は、中国政府の手の届かない天国として見られてきた。しかし、このレポートが明らかにしているように、民主主義は、多くの観察者が考えている中国政府の脅迫やハラスメントに反する天国ではない。 中国のウイグル人を支配する努力は国境をはるかに超えている。 その行動は、民主的な受入国によって保証されている言論の自由、集会の自由、そして時には旅行や移動の自由さえも含むウイグルの権利を侵している[8]。

独裁政権が国境を越えてどのように政治抑圧するかを評価する「反亡命」研究とは異なり、我々の研究では、ほとんどの標的ウイグル人が対象になる前は政治的活躍をしていなかったことがわかった。 一部のウイグル人は国境を越えた弾圧を経験した後も非政治的であり続け、他のウイグル人は中国の脅迫とハラスメントに対して行動に駆り立てられた。 我々の分析では国境を越えた抑圧の前に、証言をすること、人権団体に積極的に関与すること、メディアに話しかけること、または公にすることを「政治的に活発」として定義する。 これらの基準を満たしていない人々、または中国政府がハラスメントや脅迫を行った後に政治的に活発になった人々は、そのように注視している。 我々のデータは、中国の国境を越えた抑圧が、ディアスポラウイグル人を政治的活動に向かわせる要因の1つであることを示している。

我々のデータは、中国の国境を越えた抑圧が、ディアスポラウイグル人を政治的活動に向かわせる要因の1つであることを示している。

民族性と文化に基づく大量ターゲティングは、中国のセキュリティサービスの基準となっている。 この行動の大規模な範囲は、海外に住む多くのディアスポラウイグル人に恐怖と不確実性を植え付け、政治的に活発な個人や不活発な個人の活動を効果的に混乱させた。 このレポートは、民主主義国家におけるディアスポラウイグル人の脆弱性を評価し、ウイグル人の市民と住民が他のディアスポラ社会と同じ権利と自由を保証するために、直面するリスクの軽減に役立つ政策オプションを提案することを目的としている。

[8] “China upset as Interpol removes wanted alert for exiled Uyghur leader,” *Reuters*, February 24,2018, https://www.reuters.com/article/us-china-xinjiang/china-upset-as-interpol-removes- wanted-alert-for-exiled-uighur-leader-idUSKCN1G80FK.

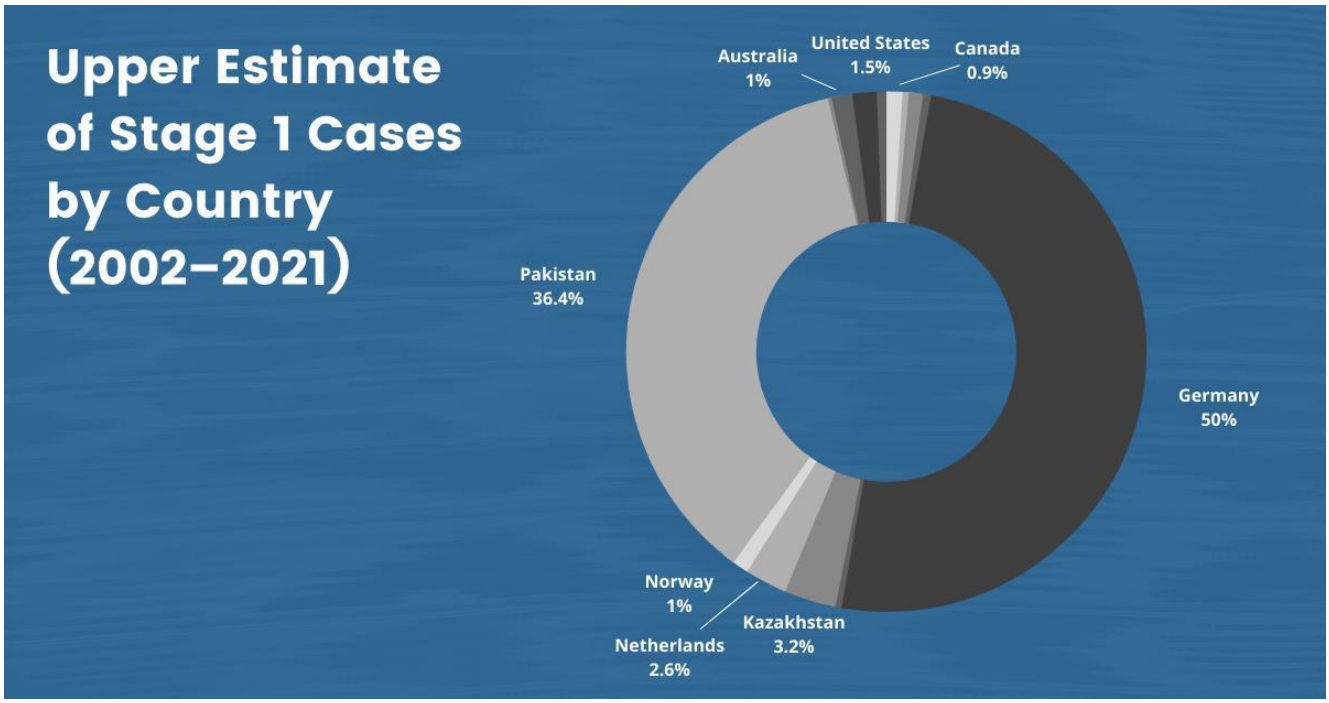

図１．この表は、我々が公開されているレポートと元のインタビューに基づいて記録したステージ1の国境を越えた抑圧の5,530件の地理的分布を示している。 これは、2001年から2021年にかけて世界中で収集されたすべてのケースを表している。世界ウイグル会議の所在地であるドイツでは、多数の事件が発生している。 資料提供：オクサス協会。

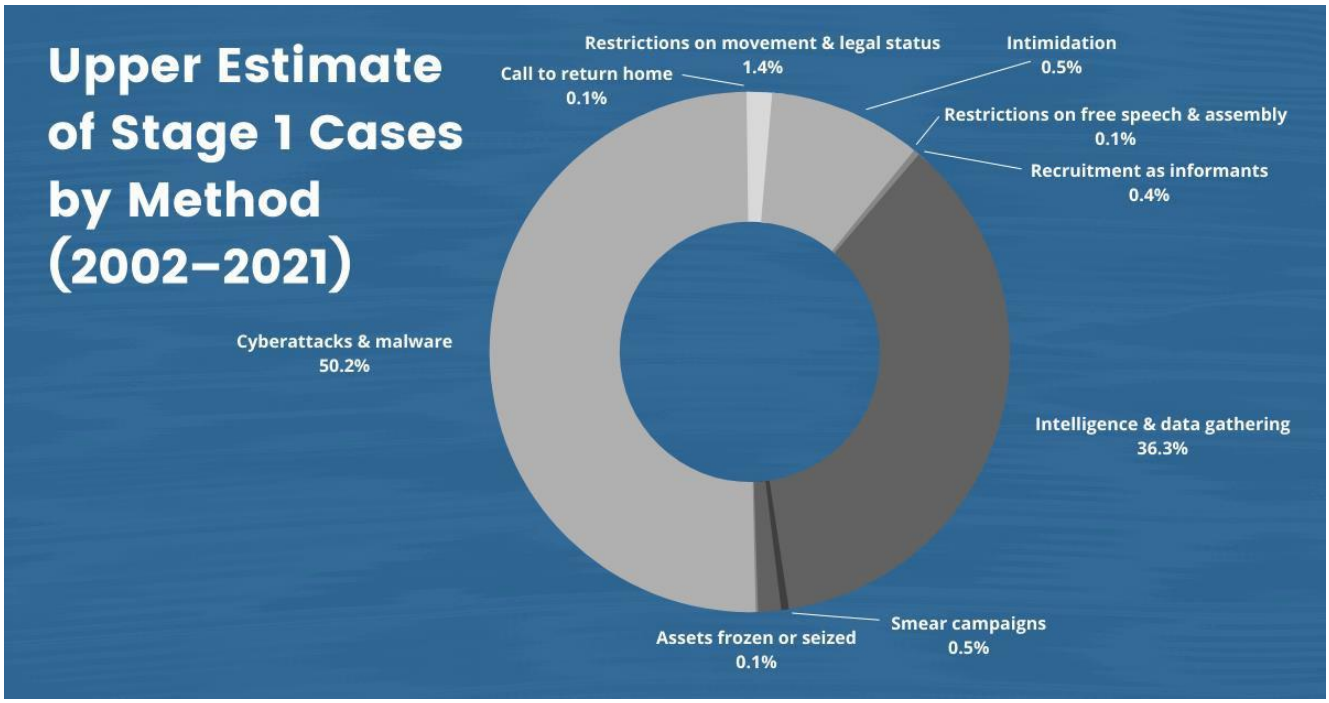

図２． この表は、我々がが記録したステージ1の国境を越えた抑圧の5,530件の方法的分布を示している。 これは、2001年から2021年にかけて世界中で収集されたすべてのケースを表している。 記録されたすべてのケースの50％以上がサイバー攻撃である。 資料提供：オクサス協会。

III. 方法論

中国の国境を越えた抑圧の戦略は、世界中のウイグル人に自己検閲をさせ、政治的活動と感じる行動をさらに慎重にやらせるのに非常に効果的であることが証明されている。 中国の監視捜査網が海外に拡大するにつれ、影響や報復を恐れて身元を明らかにせずに匿名でインタビューが行われている。 さらに、故郷の家族に対する具体的な脅威は、ディアスポラウイグル人の個人が公の証言などメディア発言を出す前に熟考しなければならないリスクの高い努力になっている。

このレポートは、ウイグル人権プロジェクトと協力して、中央アジア問題のためのオクサス協会の著者によって作成された中国によるウイグル人の国境を越えた抑圧のデータセットに基づいている。 中国によるウイグル人の国境を越えた抑圧のデータセットには、1997年に最初の拘留と判決言渡しの事例が記録されて以来、中華人民共和国が実施したXUARからのウイグル人市民を標的に国境を越えた抑圧の事件が含まれている[9]。完全なデータセットに記録されているさまざまなケースを評価するために、中央アジア政治亡命者（CAPE）データベースで採用されている国境を越えた抑圧の3段階モデルを使用する：

[9] The forms of transnational repression discussed in this report have largely targeted Uyghur former citizens of the XUAR. While we do not believe that only Uyghurs have been the targets ofthis repression, the cases in our dataset overwhelmingly show that Uyghurs living abroad are a special target of the Chinese state.

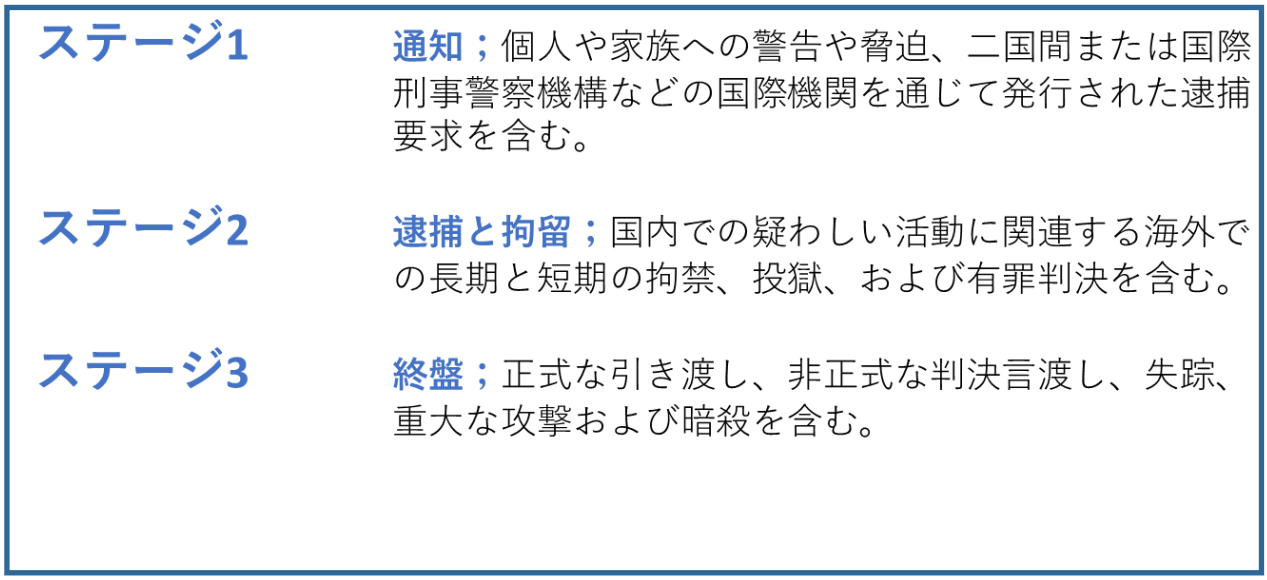

図３．Saipira Furstenberg、John Heathershaw、Edward Lemon、David Lewis、およびAlexanderCooleyによって概説された国境を越えた抑圧を評価するCAPE方法論。 資料提供：中央アジア政治亡命者のデータベース。

CAPEの通り、これらの3段階に従って、3ポイントの順序尺度で国境を越えた抑圧の程度を測定した。 次に、各ケースに1から3のスコアを付け、その内3は国境を越えた抑圧の最も深刻な形態である中国への強制送還を表している。我々の2021年6月のレポートでは、この順序尺度のステージ2と3に焦点を当てており[10]、多くの個別のケースには、さまざまなステージにわたる抑圧の形態が含まれていることが分かった。 したがって、現在のレポートでは、この現象の進行中の性質を完全に記録するために、ステージ1のみに焦点を当てている。

[10] Bradley Jardine, Edward Lemon, Natalie Hall, “No Space Left to Run: China's Transnational Repression of Uyghurs,” Oxus Society for Central Asian Affairs and Uyghur Human Rights Project, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas-transnational- repression-of-uyghurs/.

我々は攻撃の特定の類型に従い、各ケースをコーディングした（以下に概説する）。 次に、以前に標的にされた個人であっても、時間や地理で区切られた各例を個別に記録した。 たとえば、2019年、Mehmet Tohti氏は、家の外に未知の車両が駐車したり、ドアをノックして彼の活動について情報を求めたり、さまざまなハラスメントや脅迫を経験した。どちらも、以下に概説する脅迫のカテゴリに該当する11。 2016年、Mehmet氏は遠方の親戚に電話をかけ、その親戚は電話の直後に拘留された12。これらの事件と中国政府によって展開されたさまざまな戦略の分離時間により、データセットに2つの別個の例として入力された。

我々はデータセットを2つの大きなカテゴリに分けた。 1番目のカテゴリは完全な記入で構成され、既知の氏名と履歴を持つ個人のケースが記録された。 2番目のカテゴリが匿名ケースと呼ばれ、名前が公開されていないウイグルの個人またはグループを指す。匿名の事件は、ウイグル人に対する大規模な公的攻撃の一部であった可能性があり、影響を受けた個人の数が特定できるが、個人の特定または利用可能なレポート以外の背景を追加することはできない。 ケースの上限は、完全な記入と匿名のケースの組み合わせである。

我々の2020年7月のレポートのステージ2および3のデータと同様に、ステージ1のデータは世界中の事例を表している。 ただし、我々の現在のレポートでの分析は、ヨーロッパ、アジア太平洋地域、および北アメリカに焦点を当てている。 伝統的に、国際舞台で難民の避難所や自由な価値観の防壁として認識されてきたこれらの地域は、権威主義の手の届かない天国として見られてきた。

---

[11] Rachel Gilmore, “‘We’re coming to get you’: China’s critics facing threats, retaliation for activism in Canada,” *Global News*, April 2, 2021, https://globalnews.ca/news/7734158/china-pressure-activists-canada-uyghur-hong-kong-tibet-spying/.

[12] Tom Blackwell, “‘Don’t step out of line’: Confidential report reveals how Chinese officials harass activists in Canada,” *National Post*, January 5, 2018, https://nationalpost.com/news/world/confidential-report-reveals-how-chinese-officials-harass-activists-in-canada-there-is-a-consistent-pattern/wcm/2de0402f-5d1c-4a0a-b4bb-8dcfd56b3788.

しかし、私たちの調査結果は別のことを示唆し,世界のこれらの地域に住むウイグル人は、依然として中国の脅迫、強制、ハラスメントの行動の標的となっている。

我々は米国のワシントンD.C.、オーストラリアのアデレード、カナダのトロント、日本の東京、 ノルウェーのオスロ、 ドイツのミュンヘンではウイグル人に10回のインタビューを行い、ディアスポラの人口が多いこれらの主要な対象都市に住むウイグル人の特定の状況について、より多くの背景を知ることができた。 また、世界中のウイグルNGOと協力しているサイバーセキュリティの専門家とエンジニアに3回のインタビューを実施した。

さらに、サイバー攻撃に関するウイグル人の脆弱性の程度を評価するために2つの調査を行った。 私たちは一回目の調査を英語で北米のウイグルのディアスポラ社会に送った。 次に、2回目の調査をウイグル語に翻訳し、ウイグル人として特定された人だけが回答できるようにした。 この調査は、日本、オーストラリア、ヨーロッパのいくつかのウイグル社会に配った。 網羅的ではないが、これらの調査から収集したデータは、ウイグルのディアスポラ社会の脆弱性に対する重要な洞察を提供する。

IV. ディアスポラウイグル人における脅威の脆弱性の評価：調査結果

彼らの連絡先や通信を事実上守ることが困難な状況であるために、他からの侵入や監視のターゲットにされるという驚異が活動家に伸し掛かってくる。活動家は、急速に進化している攻撃と欺瞞の方法を常に把握する必要があるだけでなく、機知に富んだ国家の行動に対抗することも知り、毎日のセキュリティ上の決定を下す。 さらに、現在のデジタルツールとプラットフォームの複雑さは、活動家が直面する脅威の技術的基盤についての理解がさらに難しくなる。 その結果、活動家は適切な保護のツールとレベルの選択に不安を感じることがよくある。

これらのより重要な傾向のケース探究として、我々は米国、オーストラリア、ヨーロッパ、および日本のウイグル人ディアスポラ社会に、ウイグル人たちの脆弱性を評価するためのデジタルの

安全性とセキュリティの実践に焦点を当てた小規模な調査への参加を要請した。 調査した72人のうち：

- 回答者の95.8%が、独自のデジタル脅威を感じた。
- その内の73.5%が「デジタルリスク、脅威、または監視の形態」の経験を報告した。
- ディアスポラのウイグル人は、これらの脅威に対応して身を守ることを目指してきた：
- 回答者の51.5%は、適切なセキュリティ上の決定のためにインターネット資源にアクセスする方法を知っていると感じた。
- 回答者の73.2%は、情報セキュリティのための新しいツールや手法を生活に取り入れることができていると感じた。

ただし、回答者は、ウイグル人たちはデジタルセキュリティと衛生に関して準備がまだ整っていないと感じた：

- セキュリティの専門家にアドバイスを求めるときに誰に連絡すればよいかを知っているのはわずか33.8%だった。
- 50%は、デジタルセキュリティについて十分なトレーニングを受けていないと感じた。
- 89.7%が、セキュリティに関する知識と技術を向上させることに関心があった。

一部の政府は、国境内に住む人々がそのような事件を報告しやすくしている。たとえば、米国連邦捜査局の防諜速報は、ハラスメントに直面しているウイグル人がFBIのチップラインに電話し、何が起こったかについて報告することができると述べた13。ただし、まだやるべきことが明らかに残っている：

[13] “Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs’ Rights” (counterintelligence bulletin), U.S. Federal Bureau of Investigation, August 11, 2021, https://s.ipvm.com/uploads/embedded_file/07b033ce06e5a7a52f4591f49b3feb19be3a558d132df949f515d3107fa4da87/20bad084-f6b4-4d5f-980a-7e04ca90158c.pdf.

- 回答者の41.2%は、セキュリティ事件の報告方法がわからないと感じ、29.5%はわかると感じた（他の29.4%はどちらにも回答していなかった）。
- セキュリティの問題が不確かである時でさえ、30.9%は受け入れらない一方、39.7%は、報告を受け入れた。（回答者の追加の29.4%は、どちらにも回答していなかった）。
- 回答者の44.1%だけが、受入国政府または警察が自分たちの事件を真剣に受け止めると感じた。20.5%は、直面したセキュリティ問題が解決されると感じた。

水飲み場型攻撃：攻撃対象のユーザーが普段アクセスするWebサイトを改ざんし、マルウェアをダウンロードさせて感染させる標的型攻撃の手法。
フィッシング攻撃：信頼できるソースから送信されたように見える偽の通信（電子メール、SMS など）を送りつけ、個人または組織のアカウントや個人データアカウント情報（ユーザID、パスワードなど）といった重要な個人情報を盗み出し、またネットワークやシステムを侵害し、ネットワークの身代金（ランサムウェア）を要求するマルウェアの一種。フィッシング攻撃は、マルウェアをターゲットのデバイスにダウンロードさせるためにも使用できる。
スピアフィッシング攻撃：グループではなく特定の個人情報を収集する標的型フィッシング攻撃である。 攻撃者は、コンテンツと言語的手がかりを使用し、電子メールとメッセージを特定のターゲットに合わせて調整し、ユーザーのアカウントの侵害を促させたり、リンクをクリックさせたり、マルウェアを含むファイルをダウンロードさせることがよくある。

中国のハッカーは、組織レベルを超えて海外のウイグル人を標的にしている。個々のウイグル人は、政治的に活動しなくても、世界中でますます攻撃されている。 重要なことに、中国政府は、ソーシャルメディアやサイバー行動を通じてまたスマートフォンのマルウェアやバックドアを通じて、ウイグル人をオンラインでターゲットにし、データを収集し、スパイしている。 これらの努力は包括的な行動の一部である。 2017年以来、中国は、いわゆる対テロ戦争の一環として国内および海外の両方で監視と情報収集を拡大してきた。

「従来の」スパイや情報提供者ではなくハッカーを使うと、このデータ収集のコストが削減される。 中国がそのような攻撃に直接関与することを証明するのは難しいが、攻撃がウイグル人を標的にしているという事実から、ハッカーが少なくとも政府の利益に貢献していることを示唆する。

反対派や人権団体の通信を標的にすることは、中国にいる情報提供者を危険にさらす可能性がある。 2010年に多数のYahooアカウントがハッキングされた後、世界ウイグル会議の広報担当者Dilshat Raxitは、過去に電子メールで連絡した中国国内の連絡先の一部に連絡が取れなかったと報告した。 ある場合には、例えば、2015年にマイクロソフトの元従業員がマイクロソフトはハッカーの対象者に、その内多くのウイグル人、電子メールアカウントが侵入されたことを伝えなかったことを明らかにしたときのように、民間企業はユーザーに通知しないことも倍増している[14]。

2012年以降、中国政府は、隠れたマルウェアを介してAndroidシステムのバックドアへのアクセスを通じて、外部ユーザーが通話を録音したり、電話のマイクをオンにしたり、写真をダウンロードしたり、位置情報を共有したり、また会話履歴をチャットアプリからダウンロードするようになってきた。ウイグル人がよく使うWebサイトは、iPhoneからデータを吸い上げるマルウェアで破損された。上記のように、これらの努力は、国内外の市民に関するビッグデータを収集する中国のドラッグネットの一部となる。2015年、中国政府はXUARに住むウイグル人の携帯を押収し始め、スパイウェアをインストールした状態で返却あるいはまったく別の携帯を返却した。各携帯に特有なシリアル番号が記録され、ウイグル地域の路上でますます普及しているカメラやハードウェアとペアにされ、政府はほぼ一定の監視が保証されている。ウイグル人は、複数の携帯を持っていた、携帯を持っていなかった、携帯を処分した、または「古すぎる」携帯を持っていたという理由で逮捕され、拘留された[15]。

---

[14] Joseph Menn, “Microsoft failed to warn victims of Chinese email hack: former employees,”*Reuters,* December 30, 2015, https://www.reuters.com/article/us-microsoft-china- insight/microsoft-failed-to-warn-victims-of-chinese-email-hack-former-employees- idUSKBN0UE01Z20151231.

[15] Paul Mozur and Nicole Perlroth, “China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn,” *New York Times,* January 19, 2021, https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html.

2019年7月に、ガーディアンは、イルケシタム国境検問所の中国国境警備隊が旅行者の携帯にスパイウェアをダウンロードし、電子メール、SMS、連絡先、スマートフォン自体に関する情報などのデータを取得し、ラマダンの間の断食とダライラマに関する資料を含む禁止されたコンテンツをスキャンしていたことを明らかにした16 。外国人旅行者を含むXUARの人々を監視と追跡する中国政府の努力は、国籍に関係なく国境から始まる。 彼らが手に入れた情報は、警察が海外に住むウイグル人のデータベースを構築するための仕事に役立つ。

これらの取り組みは、2013年から共有コマンドとコントロール（C2）インフラストラクチャーやルートマルウェアを備えたアプリとニュースサイトを介して配布された4種類の監視ウェアと組み合わされ、共有の起源を示唆している。 Lookoutの分析者は、これらのツール間で共有されている命名規則、コーディング手法、インフラストラクチャー、および共有されているターゲットは、この監視ウェアが中国製であることを示していると述べた。例えば、DoubleAgentとGoldenEagleはチベット人をターゲットにするためにも使用され、マルウェアファミリーの少なくとも1つのログステートメントは中国語である。さらに、ハイテク企業Lookoutの研究者は、これらのコードを覗き込み、IPの発信元を分析し、発信元が北京であることが分かってきた。この一連の監視ウェアは、ウイグル人のユーザーに合わせた何百の偽のアプリで使用されていた。これらのアプリは、VPNやラジオフリーアジアを含む他のサイトを模倣し、ウイグル人やチベット人がよく使うサイトに導入された。分析者はマルウェアをSilkBean、Double Agent、CarbonSteal、GoldenEagleの4つの主要なグループに分類した。すべてのマルウェアがスマートフォンからデータを単一の外部コマンドとコントロールセンターに盗み出すように設計されている。ハッカーは、これらの4種類のマルウェアを使用し、ウイグル地域だけでなく、「統合ジョイント・オペレーション・プラットフォーム」（一体化統合作戦プラットフォーム、IJOP）リストにあるアフガニスタン、エジプト、フランス、インドネシア、イラン、カザフスタン、クウェート、マレーシア、パキスタン、サウジアラビア、シリア、トルコ、ウズベキスタンの国々のウイグル人を標的にした[17]。

[16] Hilary Osborne and Sam Cutler, “Chinese border guards put secret surveillance app on tourists' phones,” *Guardian*, July 2, 2019, https://www.theguardian.com/world/2019/jul/02/ chinese-border-guards-surveillance-app-tourists-phones.

[17] “Mobile APT Surveillance Campaigns Targeting Uyghurs,” *Lookout*, June 2020, https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf, 18.

マルウェアの名前	機能
SilkBean	多くの場合、サードパーティのAndroidアプリストアからアプリがダウンロードされると、外部の行動者が70以上のコマンドをリモートで実行できるようになる。 2つのアプリケーションパッケージ名（com.uyghur.hunter.islamapkとcom.islamapk.uy）は、このマルウェアがウイグル人を明示的に対象としていることを表している。
DoubleAgent	WhatsApp、Skype、Telegramなどのさまざまなアプリから暗号化されていないデータをコピーする。 さらに、DoubleAgentには、SilkBeanとの直接的なコマンドとコントロールセンターの重なりがある。
CarbonSteal	外部の行動者が、感染させたデバイスの通話や音声の録音；SMSおよびMMSメッセージ、通話記録、インストール済みアプリ、およびそれらのインストールに関するデータのコピー；位置追跡；デバイスの電源がオンまたはオフになったときのログ；追加のアプリと機能をアップロード；などができるようにさせる。分析者は、CarbonStealがまだ活発で進化していると信じる。
GoldenEagle	外部の行動者が連絡先情報、インストールされたアプリに関する情報、発信者の履歴、外部ストレージで見つかった資料、およびテキストメッセージをコピーできるようにさせる。 外部の行動者は、スクリーンショットや写真の撮影、通話の録音、電話の環境下で音声録音、電話の位置追跡、電話のソフトウェアのアクセス、さらにマルウェアのインストールなどができるようにさせる。

表1：ウイグル人に対するサイバー攻撃で使用されたマルウェアの種類。 ほとんどが中国のユーザー対象になる。　資料提供：Lookout。

中国政府に付属しているハッカーがウェブサイト経由でマルウェアをホストおよび配布したことには、他にも注目すべき事例が

あった。2019年、Lookoutは、中国のハッカーがシリアのウイグル人を標的とするシリアンニュースというサイトを作成したことを明らかにした。 また、彼らはアフガニスタン、クウェート、インドネシア、マレーシア、パキスタン、トルコに住むウイグル人を対象にし、データを収集する同様のアプリを作成した。 アプリは、ウイグル語、英語、アラビア語、中国語、トルコ語、パシュトゥー語、ペルシア語、マレー語、インドネシア語、ウズベク語、ウルドゥー語、ヒンドゥー語で利用できる[18]。

2018年、中国のハッカーグループが中国のTianfu CupでiPhoneへのバックドアハッキングを「発見」した。 「カオス」と呼ばれるこのハッキングにより、マルウェアが埋め込まれたWebページにアクセスした後、iPhoneをリモートで乗っ取ることができた。2019年1月に、Appleは修正を提供した。ただし、2019年後半のハッキングの調査では、このバックドアハッキングおよびAndroidシステムにも同様のハッキングが少なくとも2018年から使用されていることが明らかになり、つまり、ウイグル人の個人用iPhoneは1年以上政府による悪用に対して無防備だった19。 2019年8月に、GoogleはiPhoneの5つの「開発鎖」を公開した。そのうちの1つはカオスを複製し、政府に付属しているハッカーによって開始された20。2019年9月に、ロイターは、中国政府関連のハッカーがカザフスタン、トルコ、インド、タイ、マレーシアなど中央および南アジアの通信会社の弱点を悪用したと報告した20。これらのハッカーは収集したユーザーデータと通話記録を分析し、海外のウイグル人を含む「価値の高い個人」を検索した。これらのデータにより、ハッカーは海外に住むウイグル人が誰およびどこと連絡を取ったかについて情報を得ることができ、海外に住むウイグル人とその家族の両方にとって潜在的に危険な情報であった[21]。

---

[18] Mozur and Perlroth, “China's Software Stalked Uighurs Earlier and More Widely.”

[19] Ian Beer, “A very deep dive into iOS exploit chains found in the wild,” Project Zero (blog),August 29, 2019, https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios- exploit.html; Thomas Brewster, “iPhone Hackers Caught by Google Targeted Android and Microsoft Windows, Say Sources,” *Forbes*, September 1, 2019, https://www.forbes.com/sites/thomasbrewster/2019/09/01/iphone-hackers-caught-by-google-also-targeted-android-and- microsoft-windows-say-sources/.

[20] O’Neill, “How China turned a prize-winning iPhone hack against the Uyghurs.”

[21] Jack Stubbs, “China hacked Asian telecoms to spy on Uighur travelers: sources,” *Reuters*, September 5, 2019, https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5.

2019年に、サイバーセキュリティ会社Volexityは、ウイグル語でニュース、リソース、その他の内容を提供する11の侵害されたウェブサイトを発見した。 これらのウェブサイトはすべてグレート.ファイアウォールの後にあり、海外に住むウイグル人だけがアクセスするようになっていた。 これらのウェブサイトには、ウイグルアカデミー、トルキスタンタイムズ、ウイグルタイムズ（英語、中国語、ウイグル語）、東トルキスタン教育連帯協会などが含まれていた。 Volexityはまた、ハッカーが偽のGoogleアプリケーションとプラグインを使い、メールや連絡先情報を盗んだこと、またGoogleを含む実際のウェブサイトに一連の「ドッペルゲンガードメイン」を作成したことも明らかにした[22]。

2021年5月に、サイバーセキュリティの専門家がパキスタンのウイグル人を標的とした陰謀を暴いた。 この行動には、国連と国連難民高等弁務官の名前とロゴを使用し、悪意のある資料を電子メールで送信することが含まれていた。 彼らはまた、「トルコ文化遺産財団」と呼ばれる偽の人権財団のウェブサイトを立ち上げ、パソコンにWindowsソフトウェアへのバックドアをインストールさせ、ハッカーにデータへのアクセスを与えるようにした[23]。 ある証拠は、パキスタンとウイグル地方に住むウイグル人が主要な標的であったことを示唆し、またトルコとマレーシアに住むウイグル人にも同じ行動を示している。 研究者によると、これらのフィッシングの試みは報告の時点でも継続している[24]。

[22] Andrew Case, Matthew Meltzer, and Stephen Adair, “Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs,” *Volexity*, September 2, 2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of- uyghurs/.

[23] Shoshanna Solomon, “Israel-Based Cybersecurity Experts Expose Ongoing Hack Attack on Uyghurs,” *Times of Israel*, May 27, 2021, https://www.timesofisrael.com/israel-based- cybersecurity-experts-expose-ongoing-hack-attacks-on-uighurs/.

[24] Tim Starks, “Possible Chinese hackers pose as UN, human rights group to eavesdrop on beleaguered Uyghur population,” *CyberScoop*, May 27, 2021, https://www.cyberscoop. com/uighur-chinese-hackers-pakistan-check-point-kaspersky/; “Uyghurs, a Turkic ethnic minority in China, targeted via fake foundations,” CheckPoint Research, May 27, 2017, https://research.checkpoint.com/2021/uyghurs-a-Turkic-ethnic-minority-in-china-targeted-via- fake-foundations/.

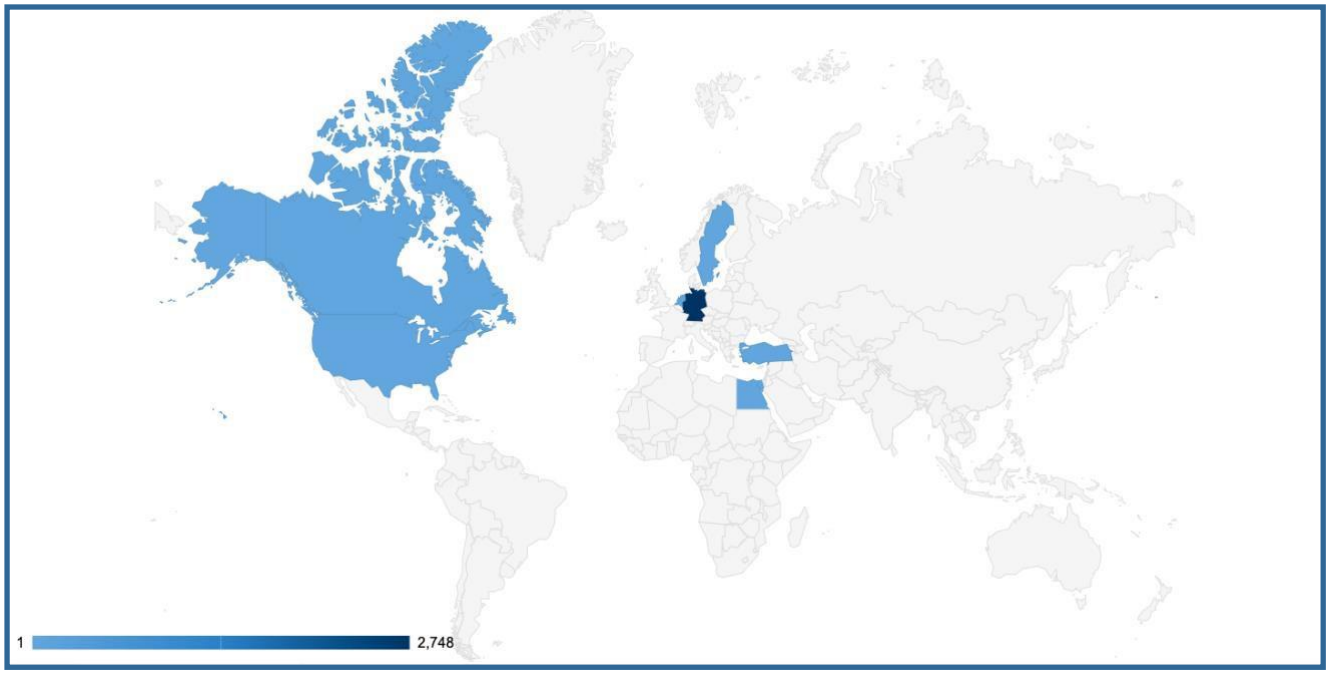

図4. 世界中のウイグル人に対するサイバー攻撃の地図（2002-2021）。 このマップは、データセット内の2,774件のサイバー攻撃の地理的分布を示しています。 カザフスタンとパキスタンでのテレコムハッキング事件は、国際メディアで報告された事件の詳細な数がなかったため、地図には含まれていなかった。 資料提供：中央アジア問題のためのオクサス協会。

V. 中国政府の第1段階「国境を越えた抑圧」の方法

中国政府は、様々な方法でウイグル人のディアスポラコミュニティーを強制的にコントロールしようと動いている。

我々は、中国によるディアスポラウイグル人に対する第1段階の弾圧の形態を合計10個確認した。

タイポロジー	定義
資産の凍結・差押	ウイグル地域または中国政府の代理として活動するホスト国において、中国政府により資産を差し押さえられた個人または集団の事例
帰国の呼び掛け	中国政府の代表者が直接呼び出した個人またはグループ、あるいは中国政府の代表者が強制的に帰国を要求している家族が呼び出した個人またはグループの例。
サイバー攻撃とマルウェア	ボットネット、マルウェア、スパイウェア、フィッシング詐欺、ダウンロード販売などのサイバー攻撃により、個人や集団がネット上で標的にされる事例。

情報・データ収集	個人または集団が中国政府に自分の個人情報を渡すように要求された例。
能動的な監視や脅迫を含む威嚇行為	個人または集団が、新疆ウイグル自治区である当局や現地の大使館・領事館、あるいは中国当局からWeChatを通じて強要された家族から繰り返し連絡を受けたり、ウイグル地域から受入国の自宅住所に迷惑な荷物が送られたり、受入国で知らない人物やノーマークの車両に尾行されたり、抗議行動で写真撮影されたり、などの事例がある。
インフォーマントとして採用	個人が他人の情報を長期間にわたって中国政府に渡すように要求された事例。
出入国管理による移動と在留資格の制限	個人または集団が、パスポートやその他の政府発行の書類を更新される代わりに、違法な片道旅行書類を与えられ、自由な移動の権利を制限されたり、パスポートの更新を拒否されたりする例[25]。

[25] “Weaponized Passports: the Crisis of Uyghur Statelessness,” Uyghur Human Rights Project, April 1, 2020, https://uhrp.org/report/weaponized-passports-the-crisis-of-uyghur-statelessness/.

ジャーナリストや公述人への攻撃を含む、言論・集会などの権利に対する制限	個人または集団が、言論の自由や集会の自由を行使できないような、ハラスメント、脅迫、監視にさらされている事例。
中傷行為	個人または集団が中国政府の中傷キャンペーンを受け、個人としての信用を失い、ウイグル地区での人権侵害の主張に疑いを持たれている事例。このような形態の攻撃は、国営メディアによる「生存証明」ビデオの制作・普及と重なることが多くなっている[26]。
プロキシの使用と脅威	個人の家族、友人、同僚など身近な人が、ウイグル地域で脅迫されたり、逮捕・拘束されたりしている事例。

表2: データセット内のケースで観測された10種類の攻撃の説明。資料提供：オクサス中央アジア協会。

VI.国境を越えた弾圧の地域的事例

権威主義的な支配者が情報空間を支配し、外部の活動家を黙らせるための戦略として、国境を越えた弾圧が世界的に増加している[27]。中国は、この慣行の世界で最も悪質な加害者として浮上している[28]。Oxus Society for Central Asian AffairsとUHRPが過去に作成したデータセットの第1段階、第2段階、第3段階のデータを統合すると、中国政府とそれに隣接する主体は、6地域46カ国において少なくとも7078件の国境を越えた弾圧を行っていることが分かる。民主主義国家もまた、国境を越えた抑圧と闘っている。ただし、我々が第1段階として特徴付けたような、それほど極端ではない形の抑圧である。

[26] "'The Government Never Oppresses Us': Proof-of-Life Videos as Intimidation and a Violationof Uyghur Family Unity," *UHRP*, February 2, 2021, https://uhrp.org/report/the-government- never-oppresses-us-chinas-proof-of-life-videos-as-intimidation-and-a-violation-of-uyghur- family-unity/.

[27] Alex Dukalskis, *Making the World Safe for Dictatorship*, (Oxford: Oxford University Press, 2021),5.

[28] "Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression,"Freedom House, January 2021, https://freedomhouse.org/sites/default/files/2021-01/FH_TransnationalRepressionReport2021_rev012521_web.pdf, 15.

中国政府の国境を越えた抑圧の方法は、法規範を侵食し、言論の自由と平和的抗議の権利を保障されている自由民主主義国に住む多くのウイグル人の憲法上の権利を無視するものである。ウイグル人は、自分たちを支配し黙らせようとする外国勢力の強権によって、それらの権利を抑圧されてきたのである。

ヨーロッパ

欧州は30年以上にわたってウイグルのディアスポラコミュニティの本拠地であり、XUAR（新疆ウイグル自治区）の弾圧から逃れたウイグル人の聖域である。2021年3月、EUは1989年の天安門事件以来、初めて中国共産党の幹部に対して制裁を行った[29]。しかし、こうした制裁にもかかわらず、ウイグル人を中国に送還しないと明言したのは、ドイツ（2018年）[30]とスウェーデン（2019年）のみである[31]。さらに、スウェーデンはウイグル人を「迫害される集団」の一部と宣言していることから、亡命資格の申請手続きはよりわかりやすくなっている[32]。ヨーロッパに逃れてきたウイグル難民の最も有力な避難所の一つであるドイツは、2020年に難民申請をする中国人の数が2倍になると報告している。これは過去3年間の増加傾向の中で最も新しいピークである[33]。各国政府は通常、民族別に移民データを集計していないため、ヨーロッパ全域のウイグル難民の正確な数についての詳細は不明である。

---

[29] Eyck Freymann and Elettra Ardissino, “China and Europe Are Breaking Over Human Rights,”*Foreign Policy*, March 29, 2021, https://foreignpolicy.com/2021/03/29/europe-cai-china-human- rights-uyghurs-sanctions/.

[30] In 2018, Germany deported a 23 year-old Uyghur student due to an administrative error. He disappeared in China, and has not been heard from since. After this incident, Germany halted the deportation of Uyghurs to China. For more information. see Adam Taylor, “Germany accidentally deported a Uyghur man to China. His lawyer hasn't heard from him since,” *Washington Post*, August 6, 2018, https://www.washingtonpost.com/world/2018/08/06/germany-accidentally-deported-uighur-man-china-his-lawyer-hasnt-heard-him-since/; “Germany halts Uighur deportations to China,” *Deutsche Welle*, August 23, 2018, https://www.dw.com/en/ germany-halts-uighur-deportations-to-china/a-45190309.

[31] Ellen Halliday, “Uighurs Can't Escape Chinese Repression, Even in Europe,” *Atlantic*, August20, 2019, https://www.theatlantic.com/international/archive/2019/08/china-threatens-uighurs- europe/596347/.

[32] Anna Hayes, “Sweden Leads the Way on Uyghur Rights,” *Fair Observer*, June 16, 2020, https://www.fairobserver.com/region/asia_pacific/anna-hayes-uighur-rights-china-persecution-surveillance-concentration-camps-asylum-news-18221/.

[33] “China Asylum Claims to Germany More Than Double,” *Deutsche Welle*, February 16, 2020, https://www.dw.com/en/china-asylum-claims-to-germany-more-than-double/a-52396720.

しかし、ヨーロッパに住むウイグル人は、今でも中国の国境を越えた弾圧の長い腕にさらされている。多くの人が、ハラスメントや 脅迫、スパイ活動の強要、ソーシャルメディア の監視キャンペーンに直面していると報告している。私たちのデータセットには、ハラスメントを受けたと名乗り出たウイグル人のケース50件と、国境を越えて強制し、黙らせようとする中国の取り組みに関するより高い推定値の3,040件が含まれている。

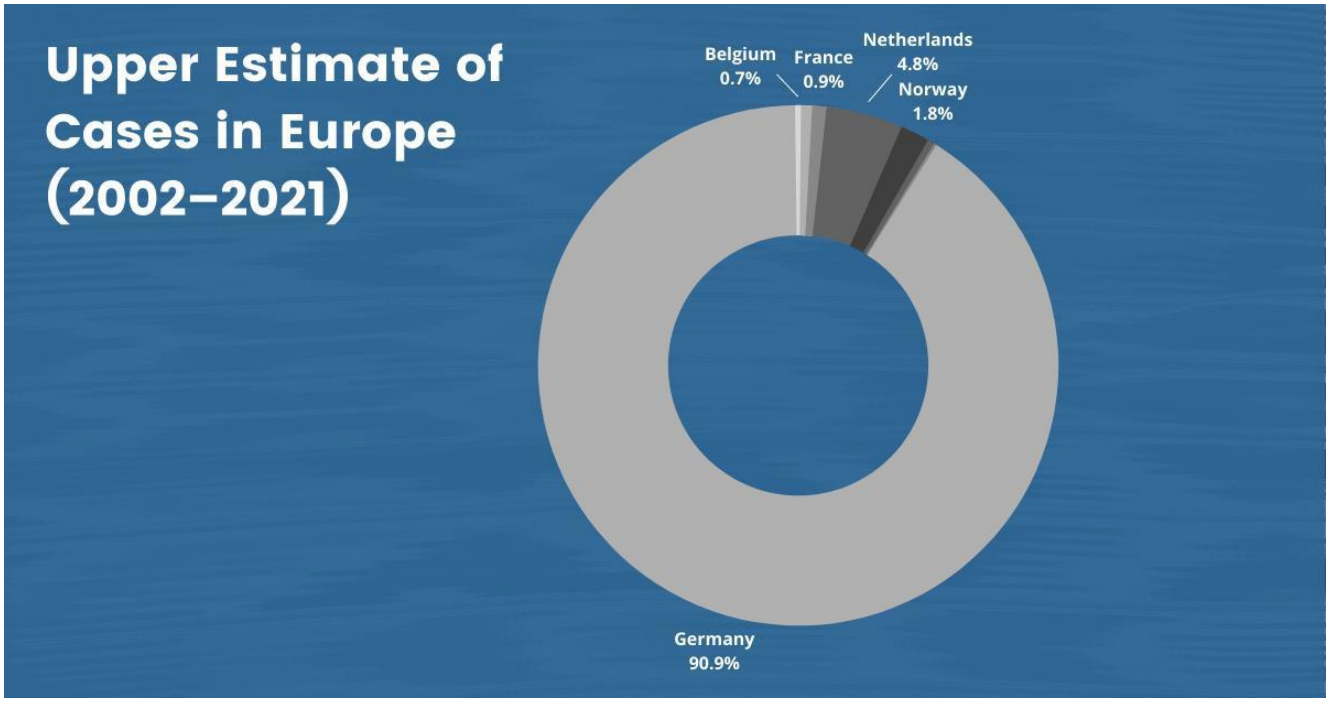

図5. ヨーロッパで記録された3,040件の第1段階の国家間を越えた弾圧の地理的分布を示したものです。前述の通り、世界ウイグル会議に対するサイバー攻撃が続いているため、ドイツで発生したケースが圧倒的に多数を占めた。資料提供：オクサス中央アジア協会（Oxus Society for Central Asian Affairs）

近年、欧州の国境内における中国国家の威嚇は増加しているが、それは2007年以降に発生したものである。公開された報告によると、ドイツの憲法保護局（BfV）は同年から、ドイツ国内でのウイグル人の活動を監視する中国の取り組みを確認していた。例えば、ミュンヘンの中国外交官、Ji Wumin氏は、同市のウイグルコミュニティに関する情報を渡す人物と何度も会っているところを目撃されたとされ、追放される前に出国している[34]。その後、2011年にドイツ連邦検察は、「L」とだけ名乗る64歳の人物に対するスパイ容疑も発表した（現地の個人情報保護法に基づく）[35]。連邦検察は、ウイグル出身の中国人を同様に告発していた。検察は、彼らが2008年4月から2009年10月の間に、ミュンヘンのウイグル人コミュニティに関する情報を中国情報機関に流したと主張している。ガーディアン紙の取材時に匿名を選んだ別のウイグル人は、ドイツでイードを祝うウイグル人の写真を撮ることと、最近来た人の名前を渡すよう要求された」と述べた[36]。

ドイツはウイグル人の移民が多いため、海外では中国の脅迫、情報収集、サイバー攻撃の標的となってきた。また、ドイツには「世界ウイグル会議」をはじめとするウイグル支援組織が存在する。世界ウイグル会議(WUC)は、現Rabiye kadeer元総裁と長く関わり、ウイグル地域の人々の権利と自由を擁護してきた。これに対し、北京は同NGOに「テロ組織」のレッテルを貼り、同組織のスタッフに対し、数十年にわたり国境を越えた弾圧行為を行ってきた[37]。

---

[34] “The Fifth Poison: The Harassment of Uyghurs Overseas,” Uyghur Human Rights Project, November 28, 2017, https://uhrp.org/docs/The-Fifth-Poison-The-Harrassment-of-Uyghurs-Overseas.pdf, 11.

[35] “German Man Charged With Spying on Exiles for China,” *Associated Press* via *Fox News*, April 8, 2011, https://www.foxnews.com/world/german-man-charged-with-spying-on-exiles-for-china.

[36] Benjamin Haas, “‘Think of Your Family’: China Threatens European Citizens over Xinjiang Protests,” *Guardian*, October 16, 2019, https://www.theguardian.com/world/2019/oct/17/think-of-your-family-china-threatens-european-citizens-over-xinjiang-protests.

[37] “China Smears Former Xinjiang Residents Who Testified About Abuses in the Region,” *Radio Free Asia*, April 13, 2021, https://www.rfa.org/english/news/uyghur/smear-04132021191322.html.

2009年、スウェーデンのウイグル人が巻き込まれた事件は、中国の党国家が海外における情報網の構築に自信を深めていることを示すものだった。スウェーデンに帰化したBarbur Mehsut氏は、「外国勢力の利益のために個人に関する情報を不法に取得・配布した」容疑で逮捕され、金銭報酬のほか、娘のビザや妻の就職先も獲得していた。最終的には、16カ月の禁固刑を言い渡された。Barbur被告は2009年5月に米国で開催された世界ウイグル会議の会合に出席していた。彼はスウェーデン、ノルウェー、ドイツ、米国におけるウイグル人活動家の活動、健康、財政に関する情報を、ストックホルムの中国大使館の報道官であるZhou Lulu氏と人民日報スウェーデン特派員のLei Da氏に伝えたという。中国の諜報員は、グアンタナモ湾で「非敵性戦闘員」として拘束され、38当時スウェーデンへの亡命を申請していたウイグル人「グアンタナモ22人」の一人、Adil Hakim氏の情報を収集したとしてバーブル・メスート氏を起訴した[39]。Barbur氏は警察に対し、中国国家は、これが承認されれば、アディル氏のケースが、より多くのウイグル人が亡命希望者としてスウェーデンに定住する前例となることを懸念していると述べた。ウイグルのスパイはAdil氏と連絡を取り、彼のケースの詳細を中国当局に伝え、アルバニアから到着したハキムを空港で出迎えたこともあったという。

中国が西南アジア地域や海外におけるウイグル人への監視をエスカレートさせる中、ヨーロッパでは国境を越えた弾圧の事例が増加している。ウイグル人活動家でフィンランド国籍のHalmurat Harri氏は、母親の2017年の逮捕に抗議し、ヨーロッパで活動を続けたことに対し、当局が2018年に父親を拘束したと述べている。その後、両親はともに釈放され、自宅軟禁となった[40]。フィンランドに住む他のウイグル人はさらに、抗議活動で監視や写真撮影を受け、

しかし、ヨーロッパに住むウイグル人は、今でも中国の国境を越えた弾圧の長い腕にさらされている。多くの人が、ハラスメントや脅迫、スパイ活動の強要、ソーシャルメディア の監視キャンペーンに直面していると報告している。

[38] His name also appears as “Adil Hakimjan” in some sources.

[39] Ritt Goldstein, “Is China spying on Uighurs abroad?” *Christian Science Monitor,* July 14, 2009, https://www.csmonitor.com/World/Asia-Pacific/2009/0714/p06s12-woap.html.

[40] Xinrou Shu, “Heretic, separatist, traitor: Uyghur Halmurat Harri's Inbetween Life,” *Supchina*,April 22, 2021, https://supchina.com/2021/04/22/heretic-separatist-traitor-uyghur-activist- halmurat-harris-in-between-life/.

中国政府がその情報を使って自国の親族をターゲットにしていると報告している[41]。フランスでも近年、ウイグル人コミュニティが標的にされ、脅かされている。中国四川省の警察官がフランスにいるウイグル人にWeChatで手紙を送り、自宅、学校、職場の住所、写真、身分証明書と配偶者の身分証明書のスキャン、フランスで結婚した場合は結婚証明書を要求している[42]。XUARの故郷の家族も強要の一手段として用いられ、2017年から2018年の間だけでもフランスで4件発生している。2019年、Gulnahar（仮名）とAdili（仮名）は、ウイグルディアスポラのメンバーに関する情報を求める中国政府当局から連絡を受けたと報告した[43]。その1年前の2018年には、他の2人のフランス人ウイグル人、Mariem（仮名）とNijat（仮名）が、同様のハラスメントを受けたと報告していた[44]。2019年以降、オランダ在住の活動家Abdurehim Gheni氏は、中国人と思われる正体不明の人物による監視と脅迫の常習的な標的になっている。彼はアムステルダムでの抗議活動中に写真を撮られ、脅迫され、彼を罵倒しようとする人々によって中傷され、信用を失墜させられた。また、ハラスメントに直面し、電話で殺すという脅迫を受けたこともある。ゲニさんはこのことをオランダ警察に報告し、警察はAbdurehim氏の抗議活動に警察を常駐させ、必要に応じて警察に連絡する直通電話を与えるなど、保護措置をより積極的にとるようになった[45]。

---

[41] Halliday, “Uighurs Can’t Escape Chinese Repression."

[42] Bethany Allen-Ebrahimian, “Chinese Police are Demanding Personal Information From Uyghurs in France,” *Foreign Policy*, March 2, 2018, https://foreignpolicy.com/2018/03/02/chinese-police-are-secretly-demanding-personal-information-from-french-citizens-uighurs-xinjiang/.

[43] Baptiste Fallevoz, Jonathan Walsh, and Georges Yazbeck, “How China Keeps a Close Eye onthe Uyghur Diaspora in France,” *France 24*, December 16, 2019, https://www.france24.com/en/asia-pacific/20191216-focus-how-china-keeps-a-grip-on-uighur- diaspora-in-france-surveillance-threats.

[44] Joëlle Garrus, “No Place to Hide: Exiled Chinese Uyghurs Feel State’s Long Reach,” *Agence France-Presse* via Hong Kong Free Press, August 17, 2018, https://hongkongfp.com/2018/08/19/no-place-hide-exiled-chinese-uighur-muslims-feel-states-long-reach/.

[45] “Nowhere Feels Safe,” *Amnesty International*, February 21, 2020, updated September 10, 2021, https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear/.

ベルギーに住むウイグル人は、家族や中国当局から自分やウイグルディアスポラ社会の情報を求める苦痛な電話を受けたり、抗議行動から窓を黒く塗った領事館の車に追いかけられたりしたと報じられている[46]。ベルギーの治安当局は、現地の中国大使館で書類や荷物を受け取る必要性について、その主張に従うのは危険であることをウイグル人に伝えるよう努めた。しかし、ベルギー政府は現地に住むウイグル人が嫌がらせを受けるのを防ぐことが、まだできていない。

ノルウェーでは、2,500 人という小さなウイグル・コミュニティの間でも恐怖心が高まっている。2019年10月、同国に住む少なくとも30人のウイグル人が、ノルウェー国籍であるにもかかわらず、中国大使館から自動発信の電話を受けたとウイグル擁護団体に警告を発した[47]。ノルウェー在住の活動家Abduweli Ayup氏は、私たちとのインタビューで、2019年にトルコから現地に移住して以来、中国の治安サービスの直接的なターゲットになっていると指摘し、（2020年1月に）Facebookのメッセンジャーで、流出したQaraqashリストについて話し合うのをやめるように警告する電話がかかってきた "と述べていた。彼はさらに続けてこう言った："その年の後半には、ベルゲンのウイグル人コミュニティに関する情報とともに、私の携帯電話番号を要求する電話をメッセンジャーで再び受けましたが、私はその提供を拒否した。" この活動家は、死の脅迫も受けたと話した[48]。

欧州における中国の国境を越えた弾圧は、少なくともいくつかのケースで自治体や 全国政府も標的にされている。2017年6月、ドイツのワイマール市は、毎年恒例の人権賞を、投獄中のウイグル人教授Ilham tohti氏に授与したと発表した。発表後、同市の賞のウェブページが繰り返し攻撃され、賞に関連するコンテンツが削除された。フランスもまた、ウイグル地域の人権侵害に関する物語をコントロールしようとする中国のキャンペーンの標的になっている。2019年2月、フランスのストラスブールで開かれたXUARに関する学術会議が、後に私服の中国領事館職員と判明した2人の人物によって中断された。

---

[46] Ellen Halliday, “Uighurs Can't Escape Chinese Repression, Even in Europe,” *Atlantic,* August20, 2019, https://www.theatlantic.com/international/archive/2019/08/china-threatens-uighurs- europe/596347/.

[47] Kiyya Baloch, “Norway: Automated Calls From Chinese Embassy Spook Uyghur Diaspora,”*Al Jazeera*, November 14, 2019, https://www.aljazeera.com/features/2019/11/14/norway- automated-calls-from-china-embassy-spook-uighur-diaspora.

[48] Abduweli Ayup (Uyghur diaspora member), online interview by Bradley Jardine, October 5,2021.

この職員は、パネリストの信用を失墜させ、主張の信憑性について疑念を広めるためのプロパガンダを流布しようとした[49]。

ドイツ在住のウイグル人活動家、世界ウイグル会議のボランティア、導師であるAbdujelil Emet氏は、中国当局からの嫌がらせに直に直面してきた。2019年、彼は連邦議会の人権に関する公聴会を傍聴した2日後に、ウイグル地方の妹から突然の電話を受けた。Abdujelil氏は警戒心から、ウイグル地区の家族にドイツの電話番号を教えたことはなかった。彼が電話に出ると、妹は共産党とXUARでの生活の質を褒め称えた。そして、弟が死んだという知らせを伝えた。その時、妹の背後から、ささやくような声が聞こえてきた。中国側の関係者が電話に出て、Abdujelil氏にドイツでの活動をやめるように要求した。そして、「家族のことを考えろ」とも付け加えた。これは明らかに脅迫である。Abdujelil氏はドイツでの活動を止めなければ、彼の家族はその結果に直面することになる。これに対して、Abdujelil氏は、「家族に何かあったら、自分はウイグル人の人権をもっと主張するようになり、中国政府にとってもっと大きな問題になるだけだ」と話した[50]。

2021年6月、ポリティコ・ヨーロッパは、リスボン市役所が "標準業務手順 "の一環として、反体制者や活動家の個人情報を世界中の弾圧政権と共有していたことを明らかにした。抗議活動を行うには、活動家や反体制派は市に登録し、個人情報を渡さなければならず、その情報を共有していた。アムネスティ・インターナショナルの現地支部によれば、2011年以降、この慣行にはウイグル人の情報を中国政府と共有することも含まれ、その結果、中国政府はリスボンでの抗議活動を手配した人々の家族を追いかけることができるようになったという。長い間、難民の天国と自負してきたこの国で、このニュースはその保護の実質に疑問を投げかけるものである。さらに、ポルトガルやEUの難民・市民として、ウイグル人が持つ言論や集会の自由、脅迫や嫌がらせからの保護といった権利も損なわれている[51]。

---

[49] Halliday, “Uighurs Can't Escape Chinese Repression, Even in Europe.”

[50] Haas, “Think of Your Family.’

[51] Aitor Hernández-Morales, “Lisbon Has Shared Dissident Info with Repressive Regimes for Years,” *Politico*, June 11, 2021 https://www.politico.eu/article/lisbon-portugal-dissidents- personal-data-repressive-regimes/.

アジア太平洋地域

オーストラリアとニュージーランドは、他の多くの自由民主主義国と同様、中国政府の嫌がらせや脅迫から逃れようとするウイグル人にとっての避難先となってきた。しかし、我々のデータは、オーストラリアとニュージーランドが提供する安全な避難所が脅威にさらされていることを明らかにしています。私たちのデータセットには、中国政府に狙われたオーストラリアとニュージーランド在住のウイグル人が18人確認され、上限は60人と見積もられている。同様に、日本も自国に住むウイグル人に対しては限られた安全しか保証できず、中には中国政府による継続的な嫌がらせに遭っている人もいる。我々のデータセットには、そのような4つの事例が記載されていて、合計で21の事例があると推定されている[51]。

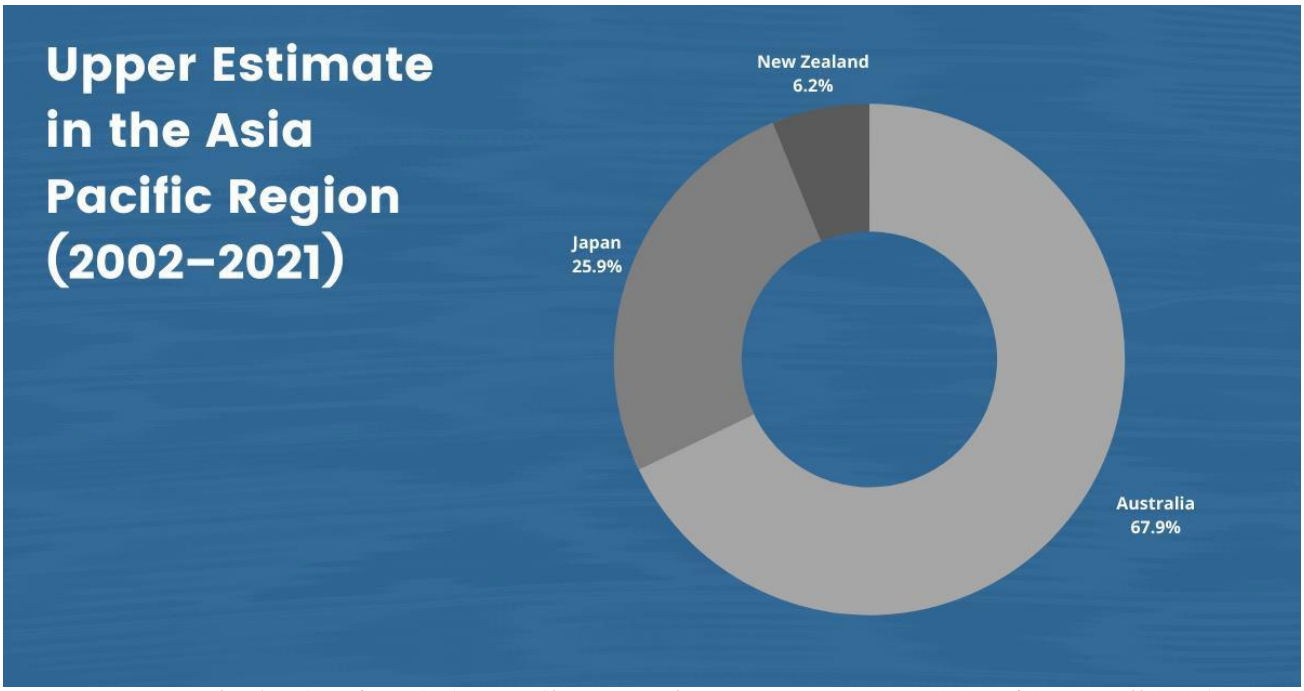

図6. この図は、アジア太平洋地域で記録された81件のステージ1のトランスナショナルな抑圧事例の地理的な分布を示したものである。資料提供：オクサス中央アジア協会

現在、オーストラリアには推定3,000人のウイグル人が居住している。オーストラリア政府は10年以上前から、中国によるオーストラリア国内のウイグル人の監視に懸念を示してきた。2006年、オーストラリア外務貿易省は次のように述べている。「中国当局はオーストラリア国内のウイグル人団体を監視し、そのメンバーや支持者に関する情報を得ようとしているようだ[...]。情報を追求する上で、中国当局は必ずしも政治的なプロフィールを持たない情報源を排除することはないだろう[52]。" オーストラリアのウイグル人の何人かは、議会の委員会で、自分たちが直面している脅迫や 嫌がらせについて語り、その多くは安全上の懸念を理由に挙げている[53]。コミュニティのメンバーは、政府関係者が同席するWeChatでの通話や、政治的な活動をしないよう促す家族からの電話といった形の圧力を報じている。また、オーストラリアにいるウイグル人は、自分の情報を渡すように要求されたと報告している。中には、母国の家族を守るために応じた人もいたが、最初の情報を提供した後、さらに情報を提供するように求められた[54]。

中国の国家安全保障当局は、2017年9月に初めてDawut（仮名）に接触し、彼が帰国するのか、あるいはまだ帰国していない理由を説明するよう要求した。Dawut氏は家族と定住しているオーストラリアでの雇用証明を送ったが、国家安全保障当局はさらに要求するためにメールを送り返した。家族の写真やパスポートなど、オーストラリアでの生活の写真が欲しかった[55]。オーストラリア在住のウイグル人活動家兼通訳のEldana Abbas氏は、キャンベラの中国大使館から電話を受け、活動中に個人やグループから写真を撮られたことを報告した[56]。

---

[52]Australia Refugee Review Tribunal - Country Research Section for China, CH31854 China, May29, 2007, https://www.refworld.org/pdfid/4b6fe1862.pdf, 5.

[53] Daniel Hurst, “Uyghurs Tell Australian Inquiry of ‘Intimidation and Harassment’ from Chinese Government,” *Guardian*, October 8, 2020, https://www.theguardian.com/australia-news/2020/oct/09/uighurs-to-tell-australian-inquiry-of-intimidation-and-harassment-from- chinese-government.

[54] Ibid.

[55] Joshua Boscaini, “Chinese Authorities Accused of Intimidating Uyghurs in Australia,” *ABC News* (Australia), March 30 2019, https://www.abc.net.au/news/2019-03-31/chinese-government-accused-of-intimidating-australian-uyghurs/10945090.

[56] “Nowhere Feels Safe,” Amnesty International.

陳永林というオーストラリアの中国大使館からの亡命者は2005年に、大使館がオーストラリアで1000人の情報提供者と工作員を育ててきたと主張した[57]。このような圧力は今でも日常的にかけられている。

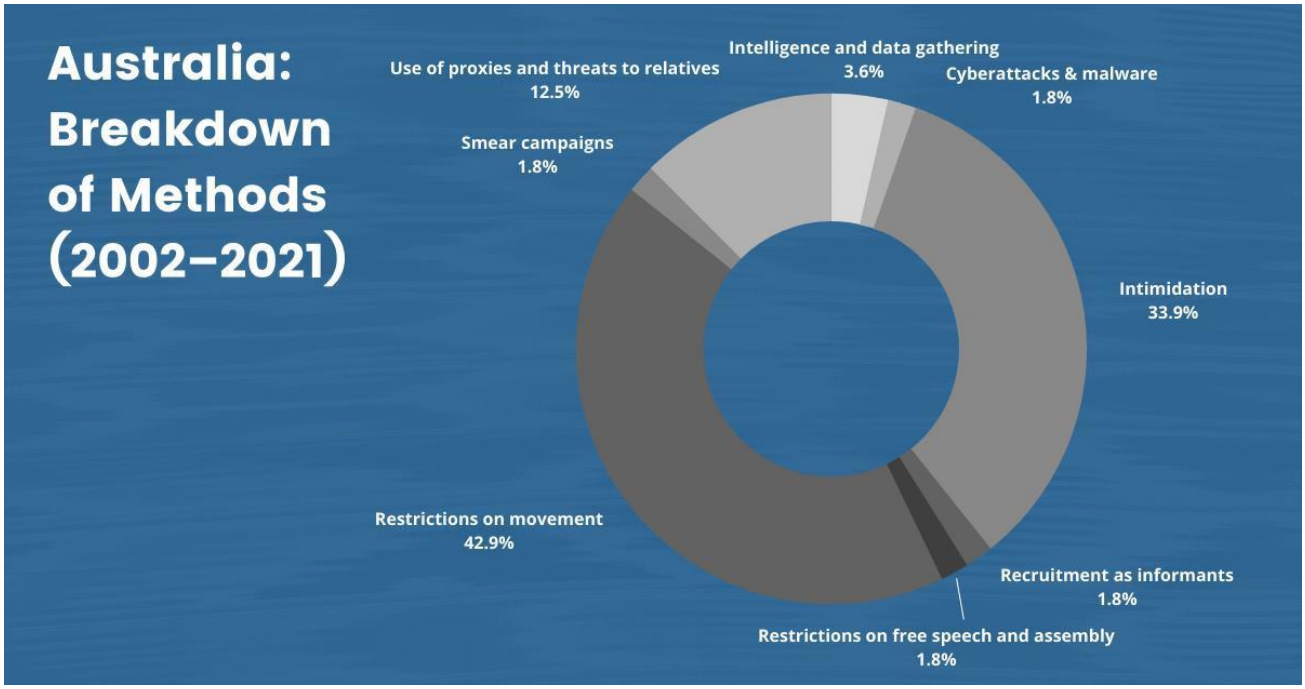

図7．この図は、中国政府がオーストラリア国内に住むウイグル人に対して展開した第1段階の国境を越えた弾圧の方法を示している。資料提供：オクサス中央アジア協会

ニュージーランドにいるウイグル人もまた、北京の監視下に置かれている。Shawdun Abul-Gopur氏は2010年、家族を残して西アジアを離れ、ニュージーランドへ渡った[58]。その年の後半、中国政府は彼の帰国を要求し、最終的に呼び出しは止まりましたが、それはわずかな時間でした。5 年後の 2016 年、彼の母親は彼に電話をかけ、ニュージーランドでの生活について情報を求めた。Shawdun氏はそれを拒否した。その後、中国大使館の代表から電話がかかってくるようになり、ウイグル地区の家族を脅し、大使館に荷物を受け取りに来るよう要求された。"私たちはあなたを見つけることができるよ、ニュージーランドにいるのだから」と念を押された[59]。

[57] "Second defector backs spy claims," *CNN*, June 7, 2005, http://www.cnn.com/2005/WORLD/asiapcf/06/07/australia.china.diplomat/; Andrew Greene, "Chinese spies in Australia on the rise, former diplomat Chen Yonglin says," *ABC News* (Australia), November 20, 2016, https://www.abc.net.au/news/2016-11-20/how-many-spies-does-china-have-in-australia/8041004.

[58] Also spelled as "Shawudun Abduguphur" in some sources.

[59] "Migrant receives chilling warning: We can find you. We are in New Zealand,'" *New Zealand Herald*, July 29, 2019, https://www.nzherald.co.nz/nz/migrant-receives-chilling-warning-we-can-find-you-we-are-in-new-zealand/GY4DPLW4EXXA35LRQYLT3YLXAY/.

その後、応答がないため、78歳の母親と3人の兄弟が拘束されたものと思われる。その後、釈放されたものの、2016年以降、連絡が取れなくなったそうだ[60]。

世界の他の地域と同様、アジア太平洋地域におけるウイグル人の標的が劇的に急増したのは、2017年にウイグル地方で大規模な抑留作戦が開始されたのと同時期であった。2018年には、日本にいるHalmat Rozi氏を訪ねるために海外渡航したXUARの家族が拘束された。大学院進学のために日本に移り住み、卒業後も日本に滞在していたHalmat氏は、家族に連絡を取ったところ、「二度と連絡を取るな」と言われたそうだ[61]。2020年5月、Halmat氏はお兄さんともう一人の身元不明者から電話を受け、抗議活動の詳細、Halmat氏がRebiya Kadeer氏と連絡を取っているか、Halmat氏が日本ウイグル協会について情報を提供できるか、などを尋ねられた[62]。お兄さんは、Halmat氏に協力するよう勧めた。数週間後、Halmat氏のもとに再び国家安全保障局から電話がかかってきて、日本での抗議行動について情報を要求された。Halmat氏は、今度は地元のテレビ局に連絡し、テレビ局はHalmat氏の話を報道することにした[63]。Halmat氏は、国家安全保障局との関係を断つため、彼らが使っていたアプリを削除し、家族との連絡も絶つなど、現実を重く受け止めている[64]。Halmat氏の物語は、XUARにおける人権侵害と中国政府の長いリーチに対する認識と政治的可視性を高める上で、重要な役割を果たした。

陳永林というオーストラリアの中国大使館からの亡命者は2005年に、大使館がオーストラリアで1000人の情報提供者と工作員を育ててきたと主張した

[60] Ashley Westerman, “New Zealand condemns China's treatment of Uyghurs but won't call it genocide,” *Public Radio International - The World*, May 11, 2021, https://www.pri.org/stories/2021-05-11/new-zealand-condemns-china-s-treatment-uyghurs-wont-call-it-genocide; Mike Wesley- Smith, “Kiwi Uyghur man claims harassment and threats by Chinese embassy,” Newshub, July 27, 2019, https://www.newshub.co.nz/home/shows/2019/07/kiwi-uyghur-man-claims- harassment-and-threats-by-chinese-embassy.html.

[61] Takamura Keiichi, “Backstories: Uighurs abroad still feel pressure,” *NHK*, July 28, 2020, https://www3.nhk.or.jp/nhkworld/en/news/backstories/1222/.

[62] Takao Harakawa and Sakei Shimbun, “Chinese Abuse of Uyghurs Reaches Japan, Blackmails Migrant into Spying on Tokyo,” *JapanForward*, October 1, 2020, https://japan-forward.com/chin ese-abuse-of-uyghur-reaches-japan-blackmails-migrant-into-spying-on-tokyo/.

[63] Takamura Keiichi, “Backstories: Uighurs abroad still feel pressure.”

[64] Harakawa and Shimbun, “Chinese Abuse of Uyghurs Reaches Japan.”

Halmat氏のケースは、決して特殊なものではない。身元を守るために匿名を希望した別の日本在住ウイグル人が、私たちとのインタビューで、中国の治安機関が情報提供者から情報を入手する方法の一部を明らかにした。2019年5月、Yusuf氏（仮名）は、新疆の親戚の一人を知っていると言い、日本への留学のアドバイスを探していると主張する男性からWeChatのメッセージを受け取るようになった。しかし、数週間もしないうちに、その男は新疆公防署の工作員であることが明らかになった。「ウイグル人活動家の情報を教えてくれれば、あなたの親戚を助けることができる」と書いてあった。ユスプ氏は、東京で毎年開かれるウイグル人の集会に出席し、その集会を訪れる予定のNASAのウイグル人技術者で国際活動家のErkin Sidick氏の写真を提供するように指示された。Yusuf氏が断ると、捜査官は口調を変えて「あなたの家族は苦しむだろう」と言った。私はあなたの友人であり、あなたとあなたの家族を助けたいのだということを忘れないでください" と言った[65]。

それからの数カ月は、Yusuf氏夫妻に大きな負担がかかった。「家族を苦しめたくないが、仲間を裏切りたくもない。妻は「家族を危険にさらしたのは私だ」と責めた。すべてが重くのしかかった。" 2020年を通じて、諜報員はYusuf氏に、日本のソーシャルメディアから東京のウイグル活動に関する投稿を書き写すよう依頼した。当初、依頼に応じたYusuf氏は、その仕事を断った。それでも捜査官は仕事を辞めずに指示し、"国家安全保障 "への貢献に対して月給を支払うと言った。Yusuf氏が原稿料を受け取るのを拒否すると、捜査官は代わりに家族に支払うよう主張した。Yusuf氏は再び拒否したが、後日WeChatで家族が中国のセキュリティ担当者から支払いを受けているというメッセージを受け取り、「私はあなたの友人であることとあなたの家族を守っていることを忘れないでくださいね」と言ったという。その後、その諜報員は、監視してほしい日本の専門家の情報をどんどん送ってくるようになった。ブログの翻訳、抗議活動への参加状況、活動資金の提供者などが主な内容だった。その中には、日本人が含まれていた。中国がこの日本人を監視し始めた後、Yusuf氏は、彼が罪を犯すように強要されているのではないかと恐れ、日本の情報機関に報告した。これに対し、Yusuf氏の親族の1人が彼を糾弾するメッセージを送ってきたが、これは治安部隊が実力行使で入手したものだとYusuf氏は考えている[66]。

[65] Yusup (Uyghur diaspora member), online interview by Bradley Jardine, September 15, 2021.

そしてついに、2年以上にわたって情報員と接触してきたユスプ氏は、2021年2月にWeChatのアカウントを削除し、二度と自分の家族に連絡を取らないという苦渋の決断をした[67]。

日本には約3000人のウイグル人居住者がいるが、日本の世論が反中国に傾いているにもかかわらず、日本政府は中国政府の行動に対する非難や、国内に住むウイグル人を保護するための具体的な行動をまだとってはいない。しかし、欧米諸国と同様の政治的・立法的措置を求めるHalmat氏の要望が聞き入れられないわけではない。2021年初頭の時点で、日本政府は世界マグニツキー法に類似した制裁措置の議論を始めている[68]。

また、過去にも中国政府は、ウイグル人活動家や同盟者が開催するイベントに抗議したり、ディアスポラのウイグル人に嫌がらせをしたりして、アジア太平洋地域のウイグル人の活動を封じようとしたことがある。2020年12月2日、オーストラリアでウイグルの権利と自由を断固として支持するオーストラリア・ユダヤ人協会が、オーストラリア・ウイグル・タングリタグ（Tangritagh）女性協会会長のRamila Chanishef氏を招いてイベントを開催した。このイベントの最中に、正体不明のハッカーが侵入し、画面上で「卑猥で罵倒的なメッセージ」を流布し、Ramila氏と彼女の発言の信用を失墜させようとする行為が行われた[69]。2018年3月、キャンベラで数千人のウイグル人が中国政府の差別に抗議するデモを行い、これはオーストラリアで過去最大のウイグル人主導のデモとなった。

---

[66] XUAR authorities have filmed and publicly released many such “denouncements,” all of which appear to be produced under coercion and duress. For more on the phenomenon, see“‘The Government Never Oppresses Us’: China’s Proof-of-Life Videos as Intimidation and aViolation of Uyghur Family Unity,” Uyghur Human Rights Project, February 2, 2021, https://uhrp.org/report/the-government-never-oppresses-us-chinas-proof-of-life-videos-as- intimidation-and-a-violation-of-uyghur-family-unity/.

[67] Yusup, interview by Bradley Jardine.

[68] Ben Dooley and Hisako Ueno, “Japan Is Finding It Harder to Stay Quiet on Abuse of China's Uyghurs,” *New York Times,* April 1, 2021, https://www.nytimes.com/2021/04/01/world/asia/ japan-uyghurs-xinjiang.html.

[69] David Adler, “CCP's persecution of the Uyghurs,” *Spectator*, January 16, 2021, https://www.spectator.com.au/2021/01/ccps-persecution-of-the-uyghurs/.

この集会は、シドニー、アデレード、ニューヨーク、イスタンブールなど、世界各地で連動して開催されました[70]。デモが終わった数時間後、オーストラリアで生まれた10代の若者たちを含むディアスポラのウイグル人たちは、嫌がらせの電話やビデオチャット、メッセージを受け取るようになった[71]。中国政府が彼らを脅して黙らせようとしたとされるにもかかわらず、オーストラリアのウイグル人は抗議を続けている。約170世帯のウイグル人コミュニティがあるアデレードでは、中国領事館が近所に建設されることに懸念を示している。中国領事館はこれまでもアデレードに存在していたが、この新しい建物は、地元コミュニティから監視拠点となる可能性があると見られ、より恒常的で実質的な存在であることを示唆している。この領事館は、中国政府が設置した5番目の領事館であり、オーストラリアでは4番目に大きい領事館である。

アデレードのウイグル人たちは、オーストラリアにある中国大使館や領事館から何度も電話を受け、自分たちのすぐ近くに新たな拠点が生まれることに懸念を抱いていると指摘している。その結果、中国政府の長い支配を肌で感じてきたウイグル人やチベット人などが、アデレード領事館の前で何度も抗議行動を起こしている[72]。ウイグル人のオーストラリア市民であるZulfiya Abdulla氏は、我々のインタビューの中で、アデレードのコミュニティの多くのメンバーが、ウイグル地域の親族から抗議をやめるようにと電話を受け、監視されていることを示唆したと述べた。"隣人から、（XUARの）家族が「（アデレードの）モスクに行くのをやめろ」と言ったと聞いた。"これは、私たちがここで監視されていることを示すものである。彼女は、オーストラリア国籍であるため、自分自身の心配はしていないが、家族のことは心配している。

---

[70] Gerry Shih, “Ethnic Uighurs Protest Chinese security crackdown,” *Associated Press*, March 15,2018, https://apnews.com/article/7817b44ef57641d8a36cd1fe17a1e379.

[71] Rick Noack, “Uighurs fled persecution in China. Now Beijing's harassment has followed them to Australia,” *Washington Post*, February 10, 2019, https://www.washingtonpost.com/world/2019/02/07/uighurs-australia/.

[72] Peta Doherty, “Adelaide's Uighur community fears new Chinese consulate building will leadto monitoring,” *SBS*, April 6, 2021, https://www.sbs.com.au/news/adelaide-s-uighur- community-fears-new-chinese-consulate-building-will-lead-to-monitoring; Rebecca Brice and Rhett Burnie, “New Adelaide Consulate attracts angry protest after complaints about size, human rights abuses,” *ABC News* (Australia), March 29, 2021, https://www.abc.net.au/news/ 2021-03-30/protest-at-opening-of-new-adelaide-chinese-consulate/100037766.

「娘が国会議員に立候補しているが、嫌がらせの標的にならないか心配だ」と、中国の国境を越えた弾圧が引き起こす政治活動への潜在的な危機感を示している[73]。

ニュージーランドは日本やオーストラリアと同様、「新疆ウイグル自治区における深刻な人権侵害」を糾弾するだけで、自国に住むウイグル人を保護する明確な行動をまだ取っていない[74]。また、同国の入国管理制度もウイグル人を危険にさらしている。米国と同様、ニュージーランドの亡命制度は3年周期で難民の枠が設定されている。亡命者は国際的に難民として認められ、「UNHCRからニュージーランド政府に照会された」者でなければならない。

さらに、これらの難民は「ニュージーランド移民局]政策、信頼性、定住、セキュリティ、移民のリスク、および健康」に基づいて審査される 。5週間後の "レセプションプログラム"、これらの難民は、ニュージーランドの永住者になる[75]。他の人は、ニュージーランドの亡命のために申請することができるプロセスは書き込みのように6ヶ月もかかる。ニュージーランドのこの移民プロセスは、亡命申請が処理されるまで、一時的なビザで国に居住する一部のウイグル人を残している-彼らは長期雇用や政府の書類を得ることができない法的宙ぶらりん状態だ[76]。

北アメリカ

2021年1月19日、米国はウイグル地方における人権侵害をジェノサイドと宣言した。

---

[73] Zulfiya Abdulla (Uyghur diaspora member), online interview by Bradley Jardine, October 1,2021.

[74] “New Zealand parliament says Uighur rights abuses taking place in China,” *Reuters*, May 4, 2021, https://www.reuters.com/world/asia-pacific/new-zealand-parliament-says-uyghur-rights- abuses-taking-place-china-2021-05-05/.

[75] New Zealand Refugee and Protection Office website, last updated 2021, accessed July 13, 2021, https://www.immigration.govt.nz/about-us/what-we-do/our-strategies-and-projects/supporting- refugees-and-asylum-seekers/refugee-and-protection-unit/new-zealand-refugee-quota- programme.

[76] Gill Bonnett, “Uighur refugee who fled China left jobless while awaiting NZ residence,” *RNZ*, January 30, 2020, https://www.rnz.co.nz/news/national/408464/uighur-refugee-who-fled-china- left-jobless-while-awaiting-nz-residence.

続いて2021年2月22日、 カナダも同様の宣言を発表した。これらの宣言は、この問題への関心を高め、オランダ（2021年3月1日宣言）、英国（2021年4月22日発表）など、追随した自由民主主義国の間でさらなる行動を呼び起こすきっかけとなった。しかし、カナダや米国に住むウイグル人は、主権国家の国境を越えて彼らを統制し黙らせようとする中国政府の努力に、今も日々立ち向かわなければならい。私たちのデータセットには、米国とカナダに住んでいる間に中国の国境を越えた抑圧を経験した個人に関する64の名前付きケースと上限推定値130のケースが含まれている。

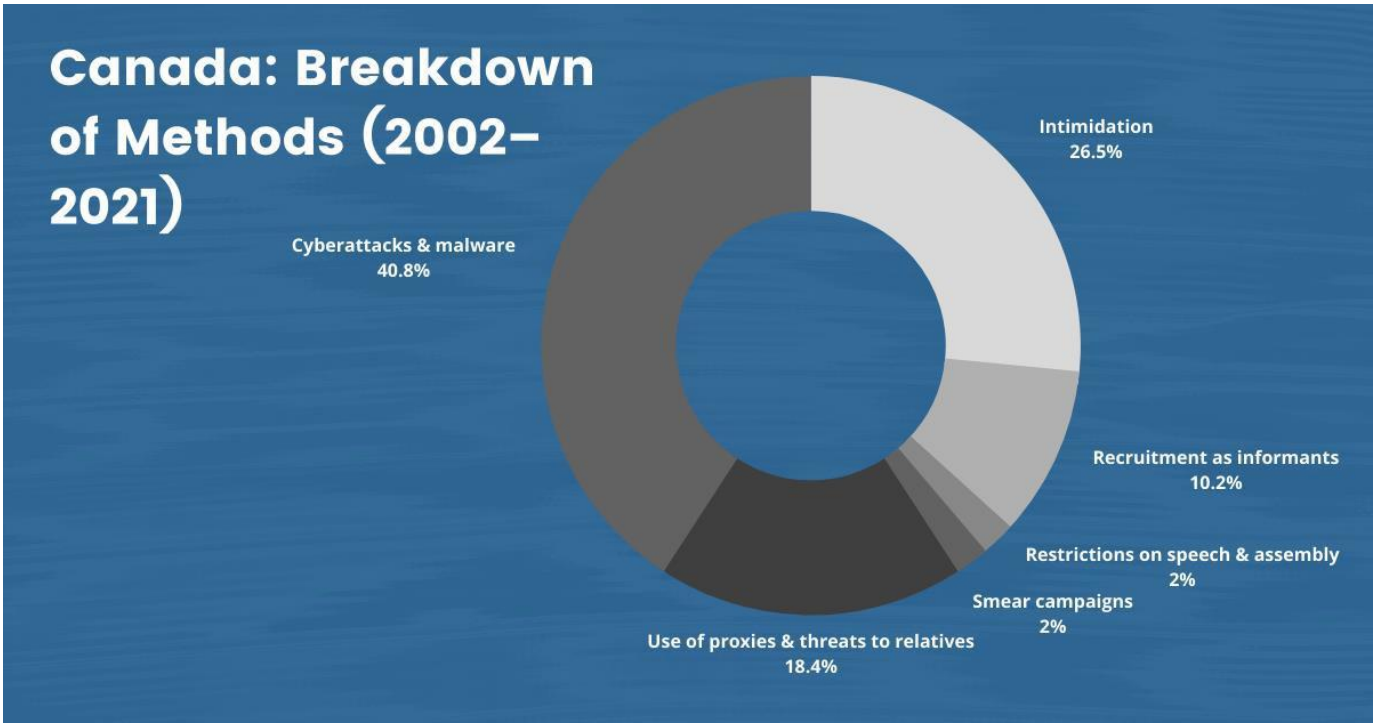

図8 この図は、中国政府がカナダ国内に住むウイグル人に対して展開した第1段階のトランスナショナルな弾圧の方法を示している。資料提供：オクサス中央アジア協会

2018 年にカナダ政府に提出された機密報告書によると、中国政府によるディアスポラ・コミュニティへの威嚇や嫌がらせが常態化している。この脅迫は奏功しているようで、多くの反体制派がカナダ国内での活動を停止し、カナダ政府に懸念されている[77]。Dilnur Enwer氏は2019年1月にカナダに到着し、亡命を申請した。

[77] Tom Blackwell, "'Don't Step Out of Line': Confidential report reveals how Chinese officials harass activists in China," *National Post*, January 5, 2018, https://nationalpost.com/news/world/ confidential-report-reveals-how-chinese-officials-harass-activists-in-canada-there-is-a-consistent-

モントリオール在住の彼女は、到着以来、正体不明の人物や中国大使館から何度も電話を受け、"重要な書類 "を受け取るために中国大使館に行くように要求されたと報告している。ウイグル地方の家族との連絡が途絶える前に、親族の一人が「大使館に捕まり、XUARに送り返される」と警告したそうだ[78]。

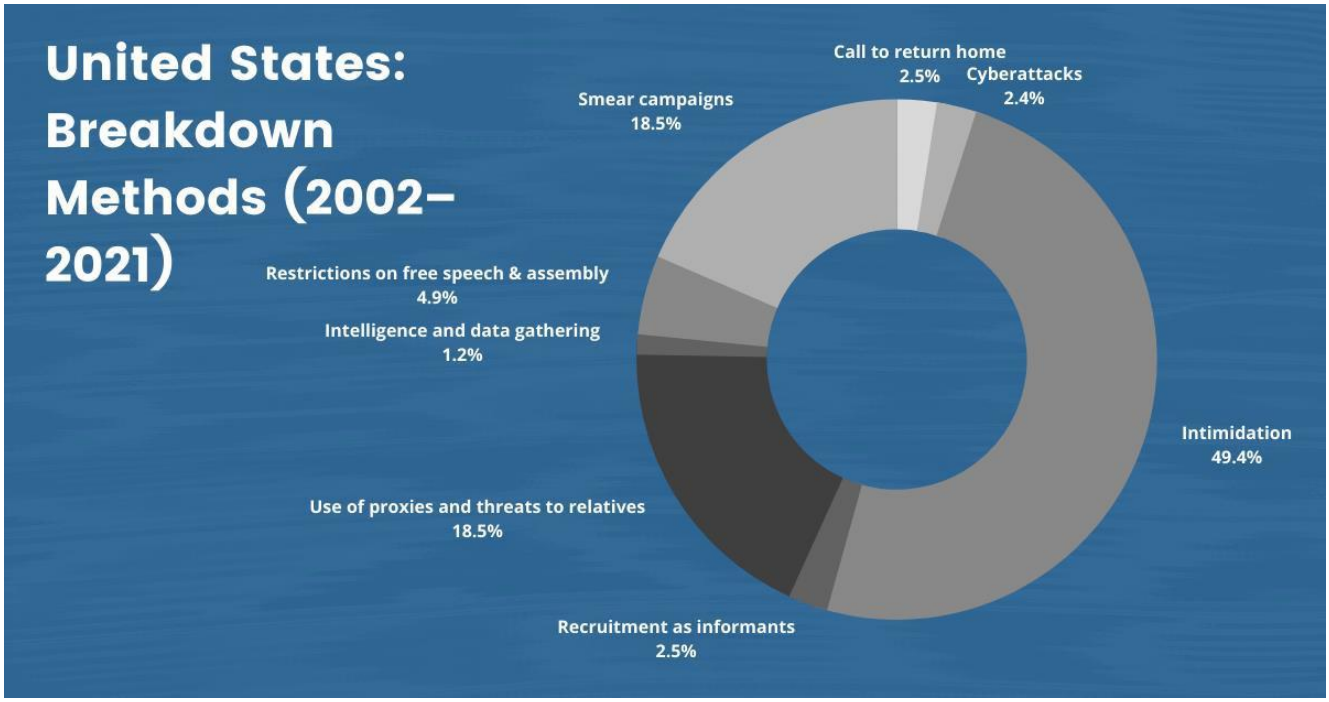

図9. この図は、中国政府が米国内に住むウイグル人に対して展開している第1段階のトランスナショナルな抑圧の方法を示している。資料提供：オクサス中央アジア協会

主にバージニア州北部のワシントンD.C.郊外を中心とするウイグル系アメリカ人コミュニティーは、合計で約10,000人にのぼる。D.C.地域の多くのウイグル人は、WeChatを含むチャットアプリ、ボイスメール、電話、電子メール、第三者のメッセージで脅迫を

pattern/wcm/2de0402f-5d1c-4a0a-b4bb-8dcfd56b3788/; Jeremy Nuttall, “Putting the Spotlight on Genocide; Canada’s Small Uyghur Community Struggles to Make People Understand,” *Toronto Star*, November 21, 2020, https://www.thestar.com/news/canada/2020/11/21/putting-the-spot light-on-a-genocide-canadas-small-uighur-community-struggles-to-make-people-understand. html.

[78] “Nowhere Feels Safe.”

受けるなど、日々嫌がらせや脅迫を受けていると述べている[79]。これらのやり取りの一部で、中国当局は、米国に住むウイグル人にパスポート情報やその他の詳細、および将来の抗議活動や組織活動に関する情報を要求したと伝えられている。 ワシントンD.C.とその周辺の多くのウイグル人コミュニティーのメンバーは、米国での抗議行動に参加するときに、顔を覆い隠し、写真を撮る人々から身元を隠すためにマスクやサングラスを着用することがよくある[80]。

米国の他の地域のウイグル人も同様に圧力に直面している。2018年に、Gulruy Asqar氏はヒューストンの中国領事館から電話を受け始めた。これらの電話は、彼女が領事館に提出する必要があると思われる重要な文書に関する録音されたメッセージから始まった。それから中国人が答えて彼女の詳細を尋ねる。Gulruy氏は、最後まで毎回拒否してきた。大使館のスタッフに、自分は米国市民であり、「彼らの文書を気にしなかった」と語った。通話が停止し、その後に中国の郵便配達会社からの電話が始まった。彼女は、自分の個人情報を収集する別の試みを行ったのではないかと疑っていた[81]。

中国の国家工作員は、ウイグル地域の家族を代理人として使い、ウイグル人コミュニティーに圧力をかけることが増えている。ウイグル・アメリカ協会会長のクKuzzat Altay氏は、2018年にバージニア州フェアファックスでウイグル人のディアスポラコミュニティのための起業家ネットワークを立ち上げた。しかし、25人のメンバーのほとんどが、ウイグル地域にいる家族から脱退を促す電話を受け、グループから脱退した[83]。政治活動に応じて抑圧が発生することもあった。

カナダや米国に住むウイグル人は、主権国家の国境を越えて彼らを統制し黙らせようとする中国政府の努力に、今も日々立ち向かわなければならないのである。

[79] Omer Kanat, “China’s Cross Border Campaign to Terrorize Uyghur Americans,” *The Diplomat*,August 29, 2019, https://thediplomat.com/2019/08/chinas-cross-border-campaign-to-terrorize- uyghur-americans/.

[80] Colm Quinn, “‘We’re a People That Are Grieving’: Local Uyghurs Have Escaped China, ButStill Fear Repression,” *DCist*, March 14, 2019, https://dcist.com/story/19/03/14/were-a-people- that-are-grieving-local-uighurs-have-escaped-china-but-still-fear-repression/.

[81] “Nowhere Feels Safe,” Amnesty International.

[82] “Kuzzat Altay” (bio), Uyghur American Association, June 10, 2021, accessed via archivedversion of the website on October 25, 2021, https://web.archive.org/web/20210610190710/ https://www.uyghuraa.org/kuzzat.

[83] “Targets of Crackdown in China Fear Government’s Reach in U.S.,” *Associated Press*, March 8, 2020, https://apnews.com/article/religion-immigration-ap-top-news-international-news-politics-7dc7c0df54fc0d270a15186ac9e5ba84.

2018年9月、Rushan Abbas氏はワシントンのシンクタンクのイベントで、ウイグル地域の人権侵害について講演した。その数日後、妹のGulshan氏は新疆ウイグル自治区で拘束された。Rushan Abbas氏は、これは自分を黙らせるための報復行為だと考えている[84]。その後、彼女はワシントンD.C.を拠点とするアドボカシー団体「Campaign for Uyghurs」を設立し、現在はエグゼクティブ・ディレクターを務めている。

新型コロナウイルスの流行により、ウイグルの危機に関するイベントの多くはオンライン形式に移行する必要があった。これらのイベントの中には、講演者の信用を失墜させ、さらに講演を阻止しようとすることでイベントを妨害しようとする未知の参入者によって「ズームボム」されたものがあった。2020年11月、ブランダイス大学の学生は、活動家のRayhan Asat氏と複数の学者を招いて、新疆ウイグル自治区におけるウイグル抑圧に関するイベントを開催した。Rayhan氏によると、イベントの前に大学の事務局が中国人学生・学者協会のメンバーから脅迫的なテンプレートメールを受け取ったそうである。イベント中に一部の参加者は習近平や他の著名な中国共産党指導者の写真を選び、ライブ映像の代わりに使用した。また、ある発言者の発言中に中国の国歌を流したユーザもいた。Rayhan氏の報告によると、彼女の発表中に参加者が画面共有を乗っ取り、彼女のスライドや投獄されている弟のEkpar Asat氏の画像に下品で嫌がらせのような言葉を書き込んでいた[85]。「私たちは非常に強力な政府に立ち向かっており、大学には私たちの味方になってもらう必要がある」と、彼女は私たちのインタビューに答えた。「これらのキャンパスは、私たちに残された最後のプラットフォームであり、中国はそれを閉ざすためにあらゆる手段を講じている。」と語った[86]。

カナダ在住のウイグル人も、中国政府からスパイ行為を強要されたことを報告している。 2015年に匿名を条件にグローブ・アンド・メールに語ったウイグル人は、中国の治安機関がさまざまな脅威を利用して、カナダでスパイ活動を行い、新疆ウイグル自治区への訪問中に中国政府に報告するように強制したと述べた。

[84] “Nowhere Feels Safe,” Amnesty International.

[85] Lin Yang, “China-Sensitive Topics at US Universities Draw More Online Harassment,” *Voice of America*, November 20, 2020, https://www.voanews.com/a/usa_china-sensitive-topics-us-univers ities-draw-more-online-harassment/6198648.html/;

[86] Rayhan Asat (Uyghur diaspora member), interview by Bradley Jardine, Washington, DC, July18, 2021.

別のカナダ国籍のウイグル人Quttapay（仮名）氏は、ウイグル地域の駅で2人の国家警備員から連絡を受け、彼を採用しようとした。彼らは失敗し、Quttapay氏は国を離れるために48時間を与えられた。カナダ在住のウイグル人のベクリ（Bekkr、仮名）氏とユスップ（Yusup、仮名）氏は、カナダのマスコミに、中国を離れるには文書の正しい組み合わせを確保する必要があったと語った。中国の警察は、彼らが海外でスパイ活動を行う意思がある場合にのみ、必要なパスポート（ウイグル人にとっては珍しい）を発行することを申し出た。ベクリ氏は、パスポートを確保する別の方法を見つけた。ユスップ氏は今のところスパイ活動から抜け出す方法を話したが、セキュリティサービスからの警告が残されました：「私たちは忍耐強いです[87]。」

世界中のウイグル人をターゲットにしたFacebookのフィッシング詐欺には、カナダとアメリカ国籍のウイグル人も含まれていた。Facebook Canadaは、標的となったカナダ国内の「20人未満」の人々に通知する予定だった。Facebookによると、この作戦では標的となった人々に到達するために様々なテクニックを使っていたとのことである。同社によると、ハッカーたちは、「ジャーナリスト、学生、人権擁護者、ウイグルコミュニティーのメンバーなどを装ったFacebookアカウントを開設し、標的となった人々と信頼関係を築き、悪意のあるリンクをクリックさせるよう仕向けた」のだという。Facebookによると、彼らはまた、ウイグルやトルコの人気ニュースサイトに見せかけた悪質なウェブサイトを立ち上げ、正規のウェブサイトへの訪問者を感染させる「水飲み場攻撃」を仕掛けていたという。Facebookは、ハッカーたちが、マルウェアを含むウイグル語をテーマにしたアプリが入った偽のサードパーティーストアを立ち上げたことも付け加えた。これらのストアには、キーボードアプリ、祈祷アプリ、辞書アプリなどのアプリケーションが含まれていた。

ウイグル人権擁護プロジェクトのエグゼクティブ・ディレクターであるMehmet Tohti氏は、中国当局は以前からカナダの2千人のウイグル人コミュニティーを標的にしてきたと述べている。カナダ議会のメンバーは、Justin Trudeau首相に対し、オンラインでカナダ人を保護する法律の導入を求めている[88]。

---

[87] Craig Offman, “Uyghur-Canadians Say Chinese Officials Detained, Blackmailed Them,” *Globe and Mail*, April 22, 2015, https://www.theglobeandmail.com/news/national/uyghur-canadians- say-chinese-officials-detained-blackmailed-them/article24056142/.

[88] Elizabeth Thompson, “Cyber Espionage Operation Targeted Canadia Uyghurs, Says Facebook,” *Canadian Broadcasting Corporation*, March 24, 2021, https://www.cbc.ca/news/politics/china-uyghur-canada-espionage-1.5962221.

カナダの公安大臣ビル・ブレア（Bill Blair）氏は議員への書簡で、「中国を含む外国は、様々な国家機関や非国家の代理人を通じて、カナダを含む世界中の個人を脅し、脅迫しようとする 」と述べている[89]。

2019年のウイグル法と2020年のウイグル人権政策法は、新疆ウイグル自治区での大虐殺（ジェノサイド）に責任のある中国共産党幹部を制裁するとともに、中国の脅迫と嫌がらせのキャンペーンからウイグル系米国人を保護しようとするものである[90]。前者については効果的であり、米国財務省はこれらの法律とグローバル・マグニツキー法を通じて、新疆ウイグル自治区の様々な中国共産党幹部に対して数回の制裁を加えているが、これらの法律が中国政府の悪意ある影響からウイグル人のディアスポラ社会を守るのに役立ったかどうかは不明である[91]。2020年ウイグル人権法は、米国政府の関連機関が米国内のウイグル人コミュニティーを保護するための努力について議会に報告することを求めている。2021年8月、FBIは米国在住のウイグル人に対する国境を越えた弾圧に関する未分類の防諜情報を発表し、中国政府の「異論を封じ込め、指示を出し、情報を収集し、遵守を強制する」意図を指摘し、海外からの嫌がらせや強制に直面している在米ウイグル人の具体的な事例について言及していた[92]。米国政府と対応機関は、サイバーセキュリティについて一般の人々を教育し、個人やグループがインシデントを報告するための手段を作成しようと努めてきたが、これらのリソースと脆弱なコミュニティの間のギャップを埋めるには多くの作業が必要である[93]。

---

[89] Bill Blair, “Response to the December 18, 2020 motion on Foreign Interference,” Public Safety Canada, August 20, 2021, https://www.passengerprotect-protectiondespassagers.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/27-en.aspx.

[90] US Congress, Senate, *UIGHUR Act of 2019*, S 178, 166th Congress, introduced in Senate January 17, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/178/text; US Congress, Senate, *Uyghur Human Rights Policy Act of 2020* S 3744, 116th Congress, introducedMay 14, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3744.

[91] John Ruwitch, “U.S. Sanctions Chinese Officials, Including Politburo Member, For Xinjiang Abuses,” *NPR*, July 9, 2020, https://www.npr.org/2020/07/09/889406296/u-s-sanctions-chinese-officials-including-politburo-member-for-xinjiang-abuses.

[92] “Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs’ Rights,” FBI.

[93] “Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs’ Rights, FBI. See also “Cyber Incident Reporting,” U.S. Federal Bureau of Investigation; “ReportIncidents, Phishing, Malware or Vulnerabilities,” Cybersecurity and Infrastructure Security Agency, accessed August 8, 2021, https://us-cert.cisa.gov/report; “What We Investigate: The Cyber Threat,” U.S. Federal Bureau of Investigation, accessed August 8, 2021, https://www.fbi.gov/investigate/cyber.

中国のハラスメントに立ち向かうには、まだもっと大きなギャップが残っている。

VII. マシーンへようこそ：ウイグル地域とその周辺におけるデジタル権威主義

2020年、中国の習近平国家主席兼党総書記は一連の演説で、10年後までにAI至上主義を実現する野望を表明した。国際メディアは「新たな宇宙開発競争」と報じているが、中国は研究先進国と競い合い、自らをAIイノベーションの世界的ハブとすることを目指した[94]。中国共産党は、民間企業や新興企業と多くの提携関係を結び、米国から優秀なコンピュータ科学者を採用するなどして、あらゆる手段でこの目標を達成しようとしている[95]。最近のアトランティックの記事で指摘されているように、これらの目標は、中国の安全保障サービスを強化し、反対意見を予測し、どこで抗議が起ころうともそれに対抗できるように設計されたAIを搭載したアルゴリズムで武装させることにもつながるかもしれない。この技術と、中国本土にすでに存在する数億台のカメラとを組み合わせれば、国家は個人を特定し、その情報を、生体情報、旅行記録、購入品、通話記録、家族、友人、仲間などを含むいくつかの警察のデータベースのうちの1つのデータと組み合わせることができるようになる可能性がある。人々とその忠誠心を評価し、脅威を探すために設計されたコンピューターアルゴリズムは、いずれ「リスク」評価を行い、それに応じて人にステータスを割り当て、必要であれば、犯罪が行われる前に逮捕の対象とすることができるようになる[96]。中国の人口を「予測的に取り締まる」ためのこの努力は、これらの方法が開拓されてきた新疆ウイグル自治区に住むウイグル人や他のチュルク系イスラム教徒の大多数の人々に深い影響を及ぼしている。

---

[94] Kai Strittmatter, *We Have Been Harmonized* (New York: Harper Collins, 2020), 176.

[95] Ibid., 167–213.

[96] Ross Andersen, “The Panopticon is already here,” *Atlantic*, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

2018年以降、中国政府が使用している3種類の顔認識ソフトウェアとA.I.アルゴリズムは、「ウイグル人」にコード化された身体的特徴を識別すると主張している。中国企業のYitu、Megvii、Sensetime、Cloud Walkは、ウイグルの特徴を認識するためのアルゴリズムの改良に取り組んでおり、2018年には、ハイテク大手のHikvisionが自社の顔認識カメラで、性別のほか、ターゲットがウイグル人かどうかを認識できるとウェブサイトに記載している[97]。一方、中国企業のiFlytekは、ウイグル語を「読み取る」ことができる音声認識技術を使って、新疆ウイグル自治区での「犯罪解決」に貢献したと自慢している。この会社は、中国政府の音声・音声パターンのデータベース構築に協力している[98]。これらの企業の中には、ハイテク大手のファーウェイとともに、ウイグル地域での監視国家の実施に一役買っているとして、米国の制裁対象になっているところもある[99]。これらの企業の中には、ハイテク企業のファーウェイとともに、ウイグル地域での監視状態を実施する役割を果たしているため、米国の制裁の対象となっている企業もある。

重要なのは、このような監視状態を作り上げるために使われる新技術の多くが、西側政府がその販売を抑制しようとしているにもかかわらず、西側企業から中国に販売されていることである。

BBCによる2021年の記事では、感情を読み取るように設計された顔認識技術が、ウイグル地域の拘置所でもテストされていたことが報じられている。これらのカメラは、「否定的な」「不安な」感情を読み取り、対象者を「予断」するためのものである[100]。この感情の読み取りは、「自動感情認識」とも呼ばれ、ほとんどの場合、正確とは言い難い。しかし、顔の表情や感情表現に影響を与える社会的、文化的、個人的な要素を考慮することなく、感情を分類することに依存している。2001年9月11日の事件後、米国運輸保安局が「テロを起こしそうな人」を見分けるために同様の技術に頼ったプログラムでは、何の成果も得られなかった[101]。疑似科学に基づくこの技術は、恣意的な理由でウイグル人を迫害するための新たなデータポイントとして機能しているのだ。これらの企業は、中央アジアやパキスタンなど、デジタル・シルクロードに沿って国際的なスマートシティプログラムを実施することが

[97] Strittmatter, *We Have Been Harmonized*, 200.

[98] Ibid., 202–203.

[99] Ibid., 203.

[100] Jane Wakefield, “AI emotion-detection software tested on Uyghurs,” *BBC*, May 26, 2021, https://www.bbc.com/news/technology-57101248.

[101] Kate Crawford, “Artificial Intelligence is Misreading Human Emotion,” *Atlantic*, April 27, 2021, https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading- human-emotion/618696/.

多くなっており、これらはウイグル人に対する国境を越えた弾圧の重要な拠点となっている[102]。

重要なことに、この監視状態を作成するために使用された新興技術の多くは、西側政府がそれらの販売を削減しようとしたにもかかわらず、西側の関係者によって中国に販売されている。2021年6月のニューヨークタイムズの報道によると、プロメガとサーモフィッシャーという2つの米国企業は、中国の企業にDNA機器を販売し続け、その企業がウイグル地域の警察に技術を転売している。DNA収集は中国では特定のグループ（たとえば、刑事事件、移民労働者など）の標準ですが、ウイグル地域では、このデータ収集ははるかに広範囲で、ほぼ全人口に及んでいる[103]。

これらの技術により、新疆ウイグル自治区の公安局（PSB）は、最終的に「万人のための健康診断」と呼ばれるプログラムの中で、住民が「健康診断」のために呼び出されたウイグル地域内の駅で地元警察が収集した数千の固有の血液サンプルとDNAサンプルの収集と配列決定を行うことができるようになった[104]。この情報は、身長、体重、指紋、顔や声の記録などと共に、ウイグル人の行動を監視、追跡、モデル化するためのデータベースに追加された。中国の報道機関によると、このプログラムでは、新疆ウイグル自治区全域で3600万人以上のデータが収集された[105]。この事件は、中国の国家がどのように西側の技術を適切に利用し、ウイグル人に対する人権侵害を犯すかを明らかにする一連の事件の中で、最新のものに過ぎない。

---

[102] Bradley Jardine, “China’s Surveillance State has Eyes on Central Asia,” *Foreign Policy*, November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan- uzbekistan-china-surveillance-state-eyes-central-asia/; Bradley Jardine and Robert Evans, “NetsCast from the Earth to the Sky.”

[103] “China: Police DNA Database Threatens Privacy,” Human Rights Watch, May 15, 2017, https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy.

[104] “China: Minority Region Collects DNA From Millions,” Human Rights Watch, December 13,2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions#.

[105] Geoffrey Cain, *The Perfect Police State* (New York: Hachette Book Group, 2021), 115–18; Sui- Lee Wee, “China Still Buys American DNA Equipment for Xinjiang Despite Blocks,” *New YorkTimes*, June 11, 2021, https://www.nytimes.com/2021/06/11/business/china-dna-xinjiang- american.html.

同じ技術が海外のウイグル人に対して使用されている。 2018年、ドバイに住むウイグル人のAhmad Talip氏は、恣意的な投獄中に血液サンプルの提供を強制されたと述べた[106] 。アフマド・タリプ氏の主張は、中国の情報機関が海外に住むウイグル人のデータを収集する大きなパターンに当てはまる。この新しい「IDカードシステム」は、ウイグル地域のものと同様、対象者のDNAを含む詳細な情報を要求し、その情報を使って海外のウイグル人コミュニティーを監視しているのである。

党幹部は、このデータセットにデータを入れるために、米国などに住むウイグル人の情報を明示的に要求している。2018年、Barna（仮名）氏は母親からメッセージを受け取り、車のナンバープレートのほか、銀行カード番号、写真付き身分証明書、電話番号の画像を送るよう要求された。これは、中国の国家IDカードの新しいシステムのデータベースに追加するためであると伝えられている。このデータベースとこれらのIDカードは、海外に住むウイグル人を含むことを目的としています。バルナ氏は、米国でカードまたは銀行口座を持っていることについて嘘をつき、どちらかを持っていることを否定したが、母親の安全を懸念して、写真付き身分証明書の画像を母親に送信した。メッセージの調子から、中国当局が母親に強要したことが分かった[107]。

トルコに留学するために新疆ウイグル自治区を離れたJevlan Shirmemmet氏は [108]、ウイグル地域での家族の逮捕についてソーシャルメディアに投稿した数週間後に受けた電話の録音をBBCに提供した。アンカラの中国大使館からだと言った発信者は、ジェヴラン氏に「新疆を離れてから連絡を取った人を全員書き留めて」、「あなたの活動を説明する」メールを送れば、「本土があなたの家族の状況を再考してくれるかもしれない」と言ったのである。以前はトルコに住んでいたが、現在は米国に住んでいるもう一人のウイグル人、Mustafa Aksu氏は、警察官になった昔の友人からのメッセージをBBCに見せ、Mustafa氏にトルコのウイグル

[106] “Uyghur Speaks Out About Husband's 'Deportation' From UAE,” *Middle East Eye*, February 8,2021, https://www.middleeasteye.net/news/uighur-speaks-out-against-husbands-deportation- uae.

[107] Bethany Allen-Ebrahimian, “Chinese Cops Now Spying on American Soil,” *DailyBeast*, August 14, 2018, https://www.thedailybeast.com/chinese-police-are-spying-on-uighurson-american-soil.

[108] His name is also spelled “Jewlan Shirmemet” in some sources.

人活動家の活動に関する情報を提供するよう圧力をかけようとした[109]。

このような政府による弾圧の国際化は、主にアルゴリズムによる監視によって、2017年以降、劇的に加速している。新疆ウイグル自治区では、警察署が「統合共同運営システム（IJOP）」[110]と呼ばれる強力なデータベースにデータを送り込んでいる。

IJOPでは、ブラックリストに登録された26カ国の人々と接触しているウイグル人を、その他の考えられる多くの理由とともに、疑わしい人物として分類している[111]。この26カ国に渡航した人、家族が住んでいる人、あるいはこの26カ国の人々と交流のある人は、尋問、拘束、または投獄されている。中国の高度な監視システムの境界はますます曖昧になり、情報収集と嫌がらせは世界中で増加している。

新しい情報ではさらに、自由民主主義が治安国家の目を引いていることを示唆している。2021年3月、地方警察署である上海公安局（PSB）がハッキングされ、110万件の監視記録が漏洩した。この大量の文書からの暴露の1つは、コードネーム「ウイグルテロリスト」の保護されていないデータベースであった。これは、世界中のセキュリティ機関がアクセスできるオープンソースデータベースの一部であった。このプラットフォームの存在は、中国によるウイグル人に対する国際的なキャンペーンの巨大な範囲のほんの一端を垣間見るに過ぎない。このデータベースには、PSBによって拘束、尋問、監視された数千人のウイグル人の「テロリスト容疑者」の記録が含まれている。このデータベースには、数千人のウイグル人の「テロリスト容疑者」の記録が含まれており、この「テロリスト容疑者」は、400人以上が未成年であり、その中には5歳の子供もいたことから、遠大な主張に基づいているように思われる[112]。このデータベースには、さらに監視するために、上海に旅行したという理由だけでフラグが立てられた5,000人以上の外国人の情報も含まれている。

---

[109] Joel Gunter, “The cost of speaking up against China,” *BBC*, March 31, 2021, https://www.bbc.com/news/world-asia-china-56563449.

[110] “China’s Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App,” Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas- algorithms-repression/reverse-engineering-xinjiang-police-mass.

[111] “‘Eradicating Ideological Viruses’: China’s Campaign of Mass Repression in Xinjiang,” Human Rights Watch September 9, 2018, https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

[112] Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs,” *ABC News* (Australia), April 1, 2021, https://www.abc.net.au/news/2021-04-01/shanghai-files-shed-light-on-china-surveillance-state/100040896.

このリストには、少なくとも3人のウイグル族のオーストラリア人が含まれている。そのうちの2人（Nurgul Sawut と Maimaitaji Kasimu[113] ）は市民権を持っており、もう一人は匿名の永住者で、彼が抗議活動に参加した後に母親が拘留されると脅かされたと伝えられている。また、オーストラリアに住むウイグル人コミュニティーのリーダー数人も、「テロリスト」としてブラックリストに載っている[114]。上海リストは、彼らが中国政府のターゲットであることのさらなる証拠である。

中国のウイグル人に対する脅迫、嫌がらせ、統制の意欲は、中国のウイグル地区での活動や海外在住のウイグル人の返還・逮捕の動きと相関して、この5年間で増加しています。特に中国政府が力を入れているのは、第1段階の国家を超えた抑圧であるサイバー攻撃で2,774件、電話や直接の脅迫、監視などの脅迫で526件が記録されています。また、第1段階の弾圧は主に自由民主主義国に住むウイグル人に集中しており、ヨーロッパで3,040件、アジア太平洋地域で81件、さらに北米で130件が記録されている。

VIII. サイバースペース：国境を越えた抑圧の次のフロンティア

現代の通信技術は、中国の治安機関の活動範囲を急速に拡大し、海外在住のウイグル人の情報を得るための新しい方法と戦術を生み出し、クラウドソーシングによる威嚇の機会を拡大した。ますます、中国政府は、ウイグル人の人々が直面している虐待について発言することの危険性を高めるために、ボットネットと標的偽情報キャンペーンの組み合わせを使用している。

---

[113] “Maimaitaji Kasimu” is a pinyin transliteration of the Chinese-language version of the name Memethaji Qasim.

[114] “Australian Uyghurs Say They’ve been Monitored and Threatened” (video), MSN, April 15, 2021, https://www.msn.com/en-au/lifestyle/lifestyleroyals/australian-uyghurs-say-theyve-been- monitored-and-threatened/vp-BB1fFzjr; “Australians Flagged in Shanghai Security Files,” *ABC News* (Australia).

コンピュータ技術者がインフラを保護するために高いコストが必要であるため、このような持続的な攻撃は、組織の活動能力を低下させ、悪意のある攻撃者が市民社会を効果的に「値下げ」することを可能にするのである。

中国のサイバー能力の高まりは、ここ数カ月、欧米の著名な政府高官や政治評論家の注目を集めている。2021年3月、マイクロソフトは、多数のハッカーがMicrosoftExchange電子メールプログラムを使用して世界中の組織に侵入する「フリー・フォー・オール」（free- for-all）を開始したことで中国を非難した 。2021年7月、米国政府は、中国国家安全保障省（MSS）とその関連ハッカーが、世界中で100,000を超えるMicrosoftExchangeサーバを攻撃および侵害したとして非難した 。アナリストはまた、過去10年間に行われたいくつかの有名なスパイウェア・キャンペーンは、人民解放軍（PLA）と関連があると分析されている 。中国のハッキング・エコシステムは、国家の関係者だけでなく、中国政府に代わってハッキングする民間の雇用関係者や民族主義者の個人を含むように、より広く拡大しているようである [118]。

2018年度のインターネット発展統計報告書によると、中国の地下のサイバー犯罪者は150億米ドル以上の規模であり、情報セキュリティ産業の約2倍の規模である。また、同じ中国語の資料によると、中国のサイバー犯罪は年間30％以上の割合で増加しており、地下のサイバー犯罪ネットワークで働く人は40万人と

ますます、中国政府は、ウイグル人の人々が直面している虐待について発言することの危険性を高めるために、ボットネットと標的偽情報キャンペーンの組み合わせを使用している。

[115] Kevin Collier, “China Behind Another Hack as U.S. Cybersecurity Issues Mount,” *NBC*, April21, 2021, https://www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues- mount-rcna744.

[116] John Hudson and Ellen Nakashima, “U.S., Allies Accuse China of hacking Microsoft and Condoning Other Cyberattacks,” *Washington Post*, July 19, 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

[117] “China Sharpens Hacking to Hound its Minorities, Far and Wide,” *New York Times*, October 22, 2019, https://www.nytimes.com/2019/10/22/technology/china-hackers-ethnic-minorities.html.

[118] Paul Mozur and Chris Buckley, “Spies for Hire: China’s New Breed of Hackers Blends Espionage and Entrepreneurship,” *New York Times*, August 26, 2021, https://www.nytimes.com/2021/08/26/technology/china-hackers.html; Patrick Howell O'Neill, “How China turned a prize- winning iPhone hack against the Uyghurs,” *MIT Technology Review*, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

推定されている[119]。これらのサイバー犯罪ネットワークは、しばしば国家権力に影響を与える。例えば、サイバーセキュリティ企業のFireEyeは、中国の国家に支援されたハッカー集団が、2012年以降、中国政府のために14カ国でスパイ活動を行っている間、個人的な利益のための活動を行ったと報告した。同社の2019年の報告書では、ハッキンググループ「APT41」は、セキュリティ企業が追跡している他の中国ベースのグループとは異なり、通常スパイ活動に使われる非公開のマルウェアを使って、ゲーム開発者への攻撃で利益を上げていたと述べている 。このようなネットワークは、人権団体やジャーナリストもターゲットにしている。中国のスパイウェアは、国境を越え、世界中のシンクタンク、政府機関、人権団体、法律事務所などにも広がっている 。中国政府によるハッキング活動の否定は、ターゲットとなった組織の多くが高度なネットワーク・セキュリティを持っていないことや、愛国心や単なる悪戯心が動機の個人ハッカーが国家の後押しを必要とせずに行動を起こすことができるため、しばしばもっともらしい空気を持っている。さらに、サイバーセキュリティの分野では、行為者がその身元、出所、コードを隠して帰属を回避したり、誤った方向に誘導したりすることができるため、帰属証明が長引く課題となっている[122]。ウイグルの擁護団体は特に露出されたままである。 特に、世界ウイグル会議（WUC）は、定期的なDDoS攻撃とフィッシング詐欺の対象となっている。以下の表は、WUCに対する攻撃や嫌がらせの概要を示している。

[119] Allen Bernard, “Chinese Cybersecurity Criminals are Getting More Organized and Dangerous,” *TechRepublic*, February 13, 2020, https://www.techrepublic.com/article/chinese-cyber-criminals-are-getting-more-organized-and-dangerous/.

[120] Josh Taylor, “Chinese Cyber hackers ‘Blurring Boundary Between State Power and Crime,” *Guardian*, August 7, 2019, https://www.theguardian.com/technology/2019/aug/08/chinese-cyberhackers-blurring-line-between-state-power-and.

[121] Andrea Peterson, “Chinese Cyberspies Have Hacked Middle East Experts at Major U.S. ThinkTanks,” *Washington Post*, July 7, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/07/07/chinese-cyberspies-have-hacked-middle-east-experts-at-major-u-s-think-tanks/.

[122] Myriam Dunn Cavelty, “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities,” *Science and Engineering Ethics*, vol. 20, no. 3 (2014): 709, https://www.researchgate.net/publication/261997877.

年度	概要
2011	2011年6月28日から、世界ウイグル会議は分散型サービス拒否（DDoS）攻撃を受け、2009年のウルムチ騒乱の2周年記念行事に支障をきたすようになった。 WUCのスタッフは、イベントを継続できるように代替のWordPressサイトを作成したが、このサイトもDDoS攻撃に遭い、閉鎖せざるを得なくなった。このDDoS攻撃により、WUCのウェブサイトは記念日の約1週間後である7月11日まで完全に閉鎖されたままであった。ウェブサイトへの攻撃に加えて、WUCの役員には、通信を妨害するスパムメールや正体不明の番号からの着信が殺到した[123]。
2012	2012年の執行委員会の前に、世界ウイグル会議は、ウイルスによってウェブサイトが機能不全に陥った10団体のうちの1つであった。また、WUCのサーバは「関連団体の活動家をターゲットにした偽メールの配信を強要された」[124]。
2013	少なくとも4年間（2009年～2013年）続いたフィッシング・キャンペーンにおいて、WUCの職員は、侵害されたメールアドレスや見覚えのあるアドレスから数千通のメールを受け取った。また、これらのメッセージは、WUCのデバイスにマルウェアをダウンロードさせるために、なじみのあるテーマ、言語、トピックを利用していた[125]。

[123] "World Uyghur Congress Facing DDoS Attacks, Electronic Spamming, Telephone Blockade Ahead of July 5, 2009 Anniversary," World Uyghur Congress, July 4, 2011, https://www.uyghurcongress.org/en/world-uyghur-congress-wuc-facing-ddos-cyber-attacks-electronic-spamming- and-telephone-blockade-ahead-of-5-july-2009-anniversary/.

[124] "Hackers Target Uyghur Groups," *Radio Free Asia*, September 6, 2012, https://www.rfa.org/english/news/uyghur/hackers-09062012153043.html.

[125] Engin Kirda, "A Look at Advanced Targeted Attacks Through the Lens of a Human-Rights NGO, World Uyghur Congress," *Lastline*, August 12, 2014, https://www.lastline.com/labsblog/a-look-at-advanced-targeted-attacks-through-the-lense-of-a-human-rights-ngo-world-uyghur- congress/.

2013	WUCの関係者を含め、中国政府に対するアドボカシー活動を行っているウイグル人が、ハッキングされたチベット人高官活動家のアカウントから送られたメールを受信し、アンドロイドにマルウェアをインストールするよう設計されたスピアフィッシングキャンペーンの犠牲者となった。このメールは、WUCの会議の詳細に関するもので、感染したデバイスから情報を盗み出し、外部のコマンド・コントロールにエクスポートするマルウェアを含むファイルが添付され、受信者の全連絡先リストに送信された。Kaspersky Labsの研究者は、北京にあるC2サーバへのエクスポートを追跡している[126]。
2019	世界ウイグル会議のFacebookページが、過去にも他のページを攻撃したことのある中国の民族主義団体「地巴中央軍」によって攻撃されたのである。WUCのページには、新疆の牧歌的な生活やウイグル人を「テロリスト」と断じる投稿など、地覇中央軍のロゴがウォーターマークされた数千枚の画像が殺到したのである[127]。

表3：2011年から2019年までの世界ウイグル会議へのサイバー攻撃の表。資料提供：オクサス中央アジア協会、世界ウイグル会議。

2016年からWUCのウェブ開発者であるMuhemmedeli Niyaz氏が、組織のウェブサイトを保護する彼の仕事について話してくれた。 彼は次のように述べている。

[126] “Chinese Hacking Impact on Human Rights and Commercial Rule of Law,” Hearing before the Congressional-Executive Commission on China, 113th Congress, First Session, Washington,D.C., June 25, 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG- 113hhrg81855.htm; “Researchers Identify Targeted Email Attack Distributing Android Trojan App: A Recent Attack Against Human Rights Activists That Used Android Malware Might be the First of Many,” *Network World* via The World Uyghur Congress, March 26, 2013, https://www.uyghurcongress.org/en/researchers-identify-targeted-email-attack-distributing- android-trojan-app-a-recent-targeted-attack-against-human-rights-activists-that-used-android- malware-might-be-the-first-of-many/; Kurt Baumgartner and Danie Maslennikov, “Android Trojan Found in Targeted Attack,” SecureList by Kaspersky, March 26, 2013, https://securelist. com/android-trojan-found-in-targeted-attack-58/35552/.

[127] Elizabeth Law, “China's social media ‘army’ wages war on Uighurs,” *Agence France-Presse* via *Hong Kong Free Press*, May 7, 2019, https://hongkongfp.com/2019/05/07/chinas-social-media-troll- army-wages-war-uighurs/.

> 主な攻撃はDDoSであり、これらは通常、重要なイベントを開催したり、レポートをリリースしたりするときに発生する。の日はウェブサイトが開かないので、24時間体制でオンラインを維持する必要がある。 最近では、コンテンツと組織のTwitterアカウントを削除するために、ウイグル語のYouTubeチャンネルがハッキングされています。近年では、ウイグル語のYouTubeチャンネルがハッキングされてコンテンツが削除されたり、当団体のTwitterアカウントが削除されたりしている。

また、WUCは、不正なリンクや添付ファイルを通じて送られるマルウェアを利用したフィッシング攻撃にも遭っている。Niyaz氏は、「これらの活動は、予算が限られているWUCに多大な財政的負担を強いている」と指摘している[128]。

2012年と2013年、カスペルスキーの研究者は、世界ウイグル会議に対する攻撃をさらに分析し、ウイグル人のMac OS Xユーザがマルウェアに感染する脆弱性があることを発見した。インストールされると、マルウェアはMac OS Xオペレーティングシステムのバックドアを悪用し、外部のコマンド&コントロール・センターがデバイスを制御することを可能にする。アナリストは、C2ロケーションを解読することに成功し、中国の蘭州であると指摘した[129]。彼らはさらに、この高度な持続的脅威（APT）が報告の時点で激化していることを指摘した[128] 。

2012年と2013年、カスペルスキーの研究者は、世界ウイグル会議に対する攻撃をさらに分析し、ウイグル人のMac OS Xユーザがマルウェアに感染する脆弱性があることを発見した。インストールされると、マルウェアはMac OS Xオペレーティングシステムのバックドアを悪用し、外部のコマンド&コントロール・センターがデバイスを制御することを可能にする。アナリストは、C2ロケーションを解読することに成功し、中国の蘭州であると指摘した[129]。彼らはさらに、この高度な持続的脅威（APT）が報告の時点で激化していることを指摘した[130] 。

[128] Muhammedeli Niyaz (web developer at WUC), online interview by Bradley Jardine, July 16,2021.

[129] Costin Rau, “New Mac OS X backdoor variant used in APT attacks,” Securelist (blog) by Kaspersky, June 29, 2012, https://securelist.com/new-macos-x-backdoor-variant-used-in-apt-attacks/33214/. A screengrab clearly notes the C2 location as Lanzhou.

[130] Kurt Baumgartner and Costin Rau, “Cyber Attacks Against Uyghur Mac OS X Users Intensify,” Securelist (blog) by Kaspersky, February 13, 2019, https://securelist.com/cyber- attacks-against-uyghur-mac-os-x-users-intensify/64259/. Costin Rau, “New Mac OS X backdoorvariant used in APT attacks.”

WUCのボランティア2名は、4年間で1,493通の不審な電子メールを受け取ったと報告している。そのうち、1,116通にマルウェアの添付ファイルが含まれていた。これらの電子メールは、2014年のUsenixシンポジウムレポート「NGOのレンズを介した標的型攻撃の調査」で分析され、特定の個人が使い慣れた名前（侵害された電子メールアカウントを含む）を使用してマルウェアをインストールするように誘導するようにソーシャル・エンジニアリングされていることがわかった。さらに、報告された84％の電子メールは偽装された送信者から送信された。まとめると、この電子メール・キャンペーンは、ウイグル人活動家を標的とするハッカーが、知らないうちに受信者が悪意のある添付ファイルを開いてダウンロードし、マルウェアをコンピュータにインストールできるように、メッセージを確実に受信できるようにソーシャル・エンジニアリングメッセージに焦点を当てることを示唆している[131]。

トロント大学を拠点とするCitizen Labが2014年のレポート「Communities @ Risk」では、中国のサイバースパイ活動は、持続的で適応力があり、技術的には単純だが、高度なソーシャル・エンジニアリングを駆使していると特徴づけている。これらのフィッシング詐欺とマルウェアパッケージは低品質である。それでも、攻撃者はその性質を隠すために多大かつ執拗な努力を払っていた。ハッカーは、組織内であっても、既知の連絡先から送信されたように見せかけるためにパッケージを電子メールに埋め込むことがよくあった。このマルウェアをダウンロードすると、第三者がキーストロークを読み取り、ファイルをダウンロードし、感染したデバイスのウェブカメラとマイクをオンにすることができるようになる。さらに報告書は、政府機関や民間企業に比べて自衛のためのリソースが少ない市民社会組織は、この種の攻撃に対して特に脆弱であることを強調している。報告書が指摘するように、このような取り組みは、「安全な場所」とされる場所にまで国家の手を伸ばすものである[132]。WUCのような組織は、中国のスパイ活動に対して脆弱なままである。

---

[131] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda, “A Look at Targeted Attacks through the Lense of an NGO,” 23rd USENIX SecuritySymposium, San Diego, CA, August 20–22, 2014, https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/le-blond. [132] “Communities @ Risk: Targeted Digital Threats Against Civil Society,” Citizen Lab, Munk School of Global Affairs, University of Toronto, November 11, 2014, https://targetedthreats.net/media/1-ExecutiveSummary.pdf, 5.

IX. ボットネットと連携したソーシャルメディアキャンペーン

ウイグル人活動家、人権団体職員、その他ウイグル地域での大量虐殺について発言している多くの人々が、中国政府のアカウント、中国のボット、中国の偽情報のターゲットになっており、この報告書を書いている時点でも、これらはすべてエスカレートし続けている[133]。このキャンペーンはTwitter、YouTube、Facebook、TikTokなどのソーシャルメディアアカウントで展開され、人権侵害から目をそらし、国際的な関心をポジティブなシナリオや明らかな偽情報に向けさせようとするものである。カンタベリー大学のAnne-Marie Brady教授によると、新疆に関するソーシャルメディアキャンペーンは、中国の研究者が過去25年間に見た単一のテーマに関する最も大規模な世界的プロパガンダキャンペーンであり、より「独断的で … 攻撃的」になってきている[134]。ASPIの研究者はこのキャンペーンを分析し、中国政府と「フリンジメディア」のコンテンツが、人権に関する統計と事実情報の信用を傷つけるために、TwitterとFacebookの数百のアカウントで何千回も配布、共有、再共有されていることを示した。新疆ウイグル自治区での虐待は、西側のメディアや人権団体の信用を傷つけ、中国政府の主張を主張する。

---

[133] Albert Zhang and Jacob Wallis, “Strange bedfellows on Xinjiang: The CCP, Fringe Media, and U.S. Social Media Platforms,” Australian Strategic Policy Institute, March 30, 2021, https://www.aspi.org.au/report/strange-bedfellows.

[134] “China Tries to Counter Xinjiang Backlash With… A Musical?” *New York Times*, April 5, 2021, https://www.nytimes.com/2021/04/05/world/asia/china-uyghurs-propaganda-musical.html.

中国共産党中央統一戦線部の新疆オーディオ・ビデオ出版社から資金提供を受けたいくつかの組織は、新疆ウイグル自治区の中国共産党の美点を讃える映像を含め、社会に「再教育」および「社会復帰」されたウイグル人のビデオを作成した[135]。

2019年、中国政府と連携したトロールが、Arslan Hidayat氏が運営するFacebookページ「Talk to East Turkestan」を攻撃した。 1時間以内に、Arslan Hidayat氏のページには、新疆ウイグル自治区の画像を宣伝し、すべてのウイグル人を「テロリスト」であり「ISISと変わらない」と非難する1,400を超えるコメントを受け取った。ハッカーグループであるディバ中央軍は、中国の五毛党のトロール軍の一部であると考えられている[136]。多くの観察者がさまざまな役職や部門の公務員であると疑っているこれらのトロールは、中国政府によって利用され、中国の国家の物語や宣伝を促進し、仲間のトロール、ボット、外交官、民族主義者の「ネットユーザー」を応援し、政府にとって危険となりうるストーリーから目をそらすために利用されている[137]。

ウイグル人活動家、人権団体、およびウイグル地域での大量虐殺について発言した他の多くの人々は、中国政府のアカウント、中国のボット、および中国の偽情報のターゲットとなった。これらはすべて、このレポートの執筆時点でエスカレートし続けている。

[135] Zhang and Wallis, “Strange Bedfellows,” 6–7. See also “‘The Happiest Muslims in the World’: Disinformation, Propaganda, and the Uyghur Crisis,” Uyghur Human Rights Project, July 28, 2020, https://uhrp.org/report/uhrp-report-happiest-muslims-world-disinformation-propaganda- and-uyghur-crisis-html/.

[136] Strittmatter, *We Have Been Harmonized,* 72.

[137] Elizabeth Law, “China's social media ‘army wages a war on Uighurs,” *Hong Kong Free Press,* May 7, 2019, https://hongkongfp.com/2019/05/07/chinas-social-media-troll-army-wages-war- uighurs/; Henry Farrell, “The Chinese government fakes nearly 450 million social media comments a year, this is why,” *Washington Post*, May 19, 2016, https://www.washingtonpost. com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social- media-comments-a-year-this-is-why/; Kaveh Wadell, “‘Look, a Bird!’ Trolling by Distraction,” *Atlantic,* January 27, 2017, https://www.theatlantic.com/technology/archive/2017/01/trolling-by- distraction/514589/.

2021年、ロイターは、中国のハッカーがフェイスブックを使って海外のウイグル人をターゲットにしていたことを明らかにした。ハッカー集団は偽のアカウントを使い、ネット上のウイグル人グループに潜入して信頼関係を築いた後、マルウェアが埋め込まれた偽の不正サイトへのリンクを共有した。グループの個人がこれらのリンクをクリックすると、リンクはその個人のプラットフォーム上にマルウェアをダウンロードした。「Evil Eye」と呼ばれるグループの一員であるこれらのハッカーは、ウイグル人向けに特別に作られたウェブサイトを、マルウェアが接続されたAndroidアプリのように見せかけることもしていた。このキャンペーンでは、トルコ、カザフスタン、米国、オーストラリア、カナダ、シリアの約500人のウイグル人が標的とされた。これを受けて、Facebookはハッカーグループをウェブサイトから削除し、破損したドメインや偽のドメインをすべてブロックした 。しかし、Facebookは、中国がウイグル地域の大量虐殺（ジェノサイド）を否定する広告をプラットフォーム上で掲載することを許可し続けた[139]。

Facebookは、中国政府が主導するプラットフォームでウイグル人をターゲットしていることを知っているようだ。2021年10月、Facebookの内部告発者であるFrances Haugen氏は、上院商業委員会の消費者保護・製品安全・データセキュリティ小委員会での証言で、中国政府が世界中のウイグル人を監視するツールとしてFacebookを定期的に使用していると指摘した。彼女は、Facebookがこのようなスパイ活動やその他の活動を認識しているにもかかわらず、対策チームが一貫して同社の人員不足であると述べた[140]。

[138] Elizabeth Culliford and Raphael Satter, “Chinese hackers used Facebook to target Uighurs abroad, company says,” *Reuters*, March 24, 2021, https://www.reuters.com/article/us-facebook-china-cyber/chinese-hackers-used-facebook-to-target-uighurs-abroad-company-says- idUSKBN2BG2UU.

[139] Isobel Asher Hamilton, “Facebook is letting China run state ads denying the abuse of UyghurMuslims in Xinjiang, and staffers are reportedly raising concerns internally,” *Business Insider*, April 6, 2021, https://www.businessinsider.com/facebook-internal-tension-china-xinjiang-ads- adverts-uyghurs-2021-4.

[140] Caitlin Hu, “‘Terrifying’: Facebook whistleblower cites violence in Myanmar and Ethiopia, spying by China and Iran,” *CNN*, October 6, 2021, https://amp.cnn.com/cnn/2021/10/05/world/ meanwhile-in-america-oct-6-intl/index.html; Sheera Frenkel, “Whistle-Blower Warns of Foreign Influence on Facebook” (video), *New York Times*, October 5, 2021, https://www.nytimes.com/2021/10/05/technology/what-happened-at-facebook-whistleblower-hearing.html.

Facebookとは対照的に、Twitterは中国が自社のプラットフォームを嫌がらせの道具として利用することに対して反撃を試みている。Twitterは一部のアカウントを外国の国家的行為者としてリストアップし、ウェブサイトから永久に追放した。2020年には、リツイートされるコンテンツを生成するコアアカウント2万3750個と、ボットやトロールが運営する追加アカウント15万個のプラットフォームが解除された[141]。

このセクションで説明した、嫌がらせ、脅迫、強制は、ウイグル人個人だけでなく、ディアスポラコミュニティにも壊滅的な影響を及ぼしている。しかし、我々が収集したデータによると、中国政府によるこのようなウイグル人への圧力が、ある反応を引き起こしていることがわかった。調査対象のウイグル人の34.4%、つまり回答者の過半数が、中国政府による強制や嫌がらせに直面した後、声を上げ始めているのだ。これは、中国の国境を越えた抑圧が、一部のウイグル人を沈黙に追い込むのではなく、政治活動へと駆り立てていることを示している。

海外にいるウイグル人は脆弱な集団であり、そのメンバーは海外で新しい生活を築こうとする一方で、故郷との連絡を維持するためにテクノロジーに依存してきている。しかし悲しいことに、故郷との連絡を維持したいという彼らの願いは、中国国家による脅迫、ハラスメント、強制にさらされる可能性を残している。

[141] Kate Conger, “Twitter Removes Chinese Disinformation Campaign,” *New York Times,* June 11,2020, https://www.nytimes.com/2020/06/11/technology/twitter-chinese-misinformation.html.

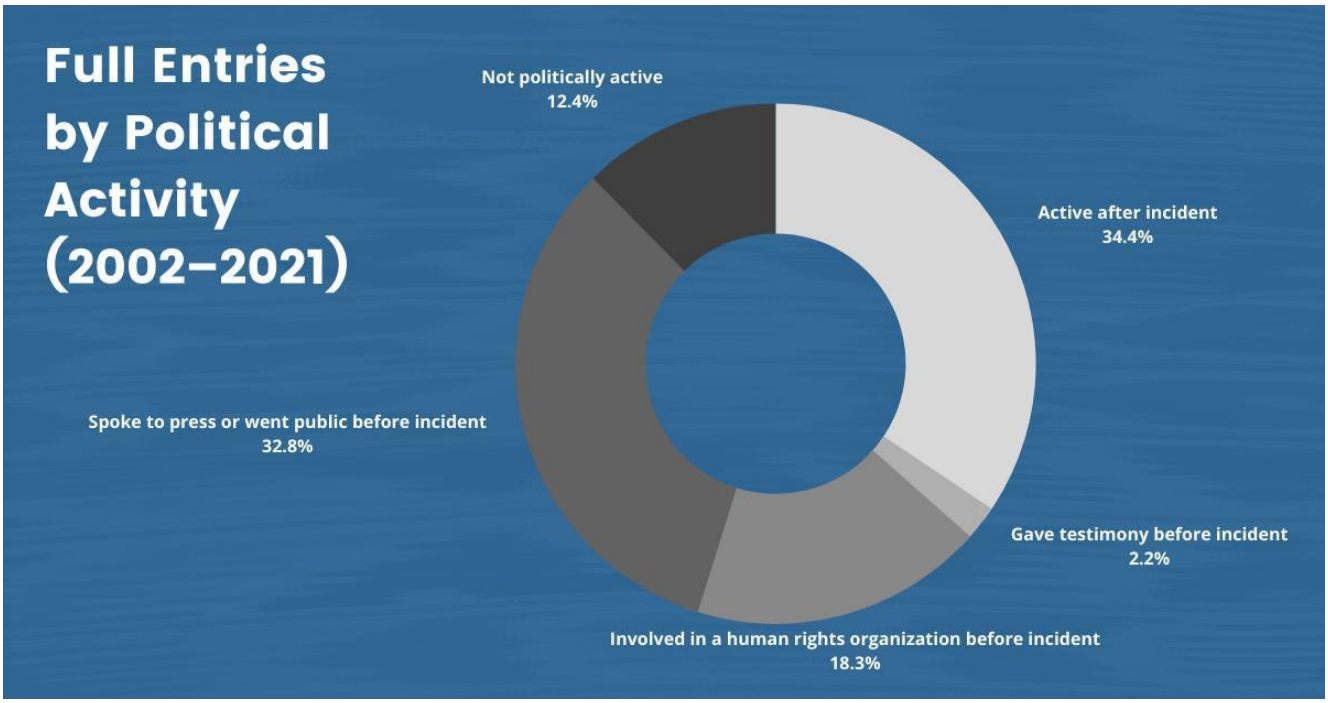

図10：政治活動別のフルエントリ（2002-2021年）。この図は、データセットに記録された186件のフルエントリ事件の政治活動を表している。当該事件のより詳細な情報により、ウイグル人がいつ、どのように政治活動（報道機関への発言を含む）を行うことになったかを明らかにすることができる。資料提供：オクサス・ソサエティ・フォー・セントラル・アジア・アフェア

X. 結論

海外にいるウイグル人は脆弱な集団であり、そのメンバーは海外で新しい生活を築こうとする一方で、故郷との連絡を維持するためにテクノロジーに依存してきている。しかし悲しいことに、故郷との連絡を維持したいという彼らの願いは、中国国家による脅迫、ハラスメント、強制にさらされる可能性を残している。私たちのデータセットには、中国政府が脅迫とハラスメントを用いて、海外のウイグル人を標的にし、監視し、黙らせるという、第1段階の国境を越えた抑圧のケースが5,530件記録されている。このような努力は、中国の監視・検閲体制をウイグル自治区内に拡大するものである。さらに、言論の自由と集会の権利という、自由民主主義憲法に謳われ、すべての人が共有すべき価値を否定することによって、海外在住のウイグル人の権利を直接侵害するものである。

本報告書で紹介した監視、データ収集、嫌がらせ、脅迫の体制は、恐怖を生む可能性があり、またしばしばそうなっている。インターネットはその創設当初から、自由、解放、交流の場となることを意図していたが、権威主義国家の道具にもなってしまった。インターネットはそのような国家が自らの勢力範囲を拡大し、主権国家の内外の行為者を監視し、オンライン・ハラスメントを行うことを可能にする。実際、デモ参加者や主催者がその活動をオンラインに移行するにつれ、彼らが反対しようとする政府もまたオンラインに移行している。この変化は、自己検閲、個人の直接検閲、そして国境を越えた抑圧の影響を受ける個人への多大な精神的負担という結果をもたらしている。秘密のデータ収集と監視の対象となる人々の自由は、表現の自由のための空間としてのインターネットの全体的な能力と同様に危険にさらされている。世界中の独裁者や非自由主義政権の指導者たちが互いに学び合い、個人を監視し、情報へのアクセスを制御し、自己表現能力を操作し、個人データの人々を分類しランク付けするシステムで彼らに不利になるように技術を獲得するにつれ、インターネットはますます制限された空間となる可能性がある。

さらに、ネット上での嫌がらせやその他のサイバー脅威は現実の世界にも影響を及ぼし、米国などでは反発を恐れて抗議活動への参加を拒否するウイグル人もいる。しかし、危険にさらされているのはウイグル人だけではない。我々の調査によれば、ウイグル人のために発言する他国の市民もまた、監視や嫌がらせを受けており、自己検閲や公的関与への恐怖のスパンを拡大させている可能性がある。このように、21世紀の国境を越えた抑圧の猛威がもたらす民主主義の後退に対抗するためには、政府は自国民や住民の権利を確保するために動かなければならない。

我々のこれまでの研究は、このような国境を越えた抑圧があまりにも一般的になりつつあることを示している。1997年以降、世界中で427人のウイグル人が、受入国から中国に強制送還され、超法規的に強制連行されており、このうち146人が2017年以降だけで強制送還された。さらに1,149人のウイグル人が受入国で拘束され、582人が2017年以降に拘束されている[142]。これらの数字は既知のケースを表しているだけで、報告されていないものはもっとたくさんあると思われる。この憂慮すべき事実は、世界における国境を越えた抑圧に対する保護の強化の必要性を明確にするものである。

[142] "China's Transnational Repression of Uyghurs Dataset," The Oxus Society for Central Asian Affairs, last accessed on August 8, 2021, https://oxussociety.org/viz/transnational-repression/; Lemon and Jardine, "No Space Left to Run."

XI. 政策的提言

本報告書の結果に基づき、我々は民主主義国家と国際組織が、中国が世界中で行っている国境を越えた弾圧に対抗するために、次のような措置を講じることを提言する：

市民社会と民間企業への提言

- **難民のケースマネージャーは、ウイグル人とともにデジタルの安全性を確保する必要がある。**ケースマネージャーは難民から信頼される存在であり、プライバシーに関する技術的な知識や支援のリソースとなり得る存在である。
- **民間のデジタル・プラットフォームは、**ウイグル語、中国語、トルコ語などを含むすべての関連言語での脅威を監視し、国家による嫌がらせを特定するツールを開発し、関連言語での安全なコミュニケーション・プラットフォームを利用できるようにすべきである。
- **開発者は、スパイウェアの市場に透明性と説明責任を持たせるために、厳格な規則と独立した監視を実施すべきである。**
  企業は、開発の全過程においてすべての法律と規制を完全に遵守することを保証し、販売および輸出ライセンスは独立した人権審査が条件とされるべきである。政府による監視技術の使用は、公開討論と批判的調査の対象とする必要があり、乱用の場合には国際的な制裁と救済のためのメカニズムが必要である。ウイグル人をターゲットにして監視するために使用され、したがって彼らの権利を侵害する監視ツールを提供する企業は、名指しで恥をかかされ、その欺瞞的行為は戦略的な訴訟の対象とされるべきである。

国家政策への提言

- **難民の受け入れ枠を増やすこと。** トルコ、パキスタン、中央アジアなどの第三国を経由するウイグル難民は、中国に送還される危険性があり、保護する必要がある。

- **ウイグル人のための専用の難民再定住プログラムを作る。** 各国政府は、中国国外のウイグル人がUNHCRの手続きを経ずに再定住を申請できる安全な経路を確立する必要がある。

- **ウイグル人のための書類の手続きを早めること。**多くのウイグル人は無国籍者として、仕事を得るため、子供を学校に通わせるための十分な書類を持たずに、窮地に立たされている。ウイグル人の亡命申請を迅速に行うことは、優先されるべきことである。

- **国境を越えた弾圧行為に責任を負う中国国民に標的を絞った制裁を課すこと。** 中国がウイグルのディアスポラに対して行っている重大な人権侵害に対して、グローバル・マグニツキー法のような国際的制裁メカニズムを発動させるべきである。これらの条項を発動することによって、これらの罪を犯している主要なグループや治安要員は、その資産を凍結され、渡航を制限されることができる。

- **国境を越えた抑圧について、同盟国とともに公の場で話し続けること。**国境を越えた抑圧が国家主権や標的とされた個人の人権にもたらす脅威に対する認識を高めることは、インターポールや国連のようなフォーラムで連合や首尾一貫した多国間対応を形成する上で極めて重要である

- **中国への技術輸出を選択的に禁止することを継続すること。**

  ウイグル人のDNAコーディング、ウイグル人の監視、その他ウイグル地域で起きている人権侵害に寄与するような技術について、民主主義政府がこれまで行ってきた取り組みは成功を収めてきました。しかし、より多くの技術が利用可能になるにつれ、これらの人権侵害への使用を防止することが最も重要である。

国際社会への提言

- **国連難民高等弁務官事務所（UNHCR）は、**難民と関わるINGOのデジタル・セキュリティを向上させるべきである。INGOは難民の個人情報を委託されている。この情報を保護し、機密を保持することは非常に重要である。残念ながら、現在の手続きや方針は必ずしもそのような保護を保証するものではない。
- **国際的な人権の議論にデジタルの権利を含める。** 難民や迫害されている少数民族の市民的自由と権利に関する議論には、監視、脅迫、嫌がらせからの自由、言論と表現の自由など彼らのデジタルな権利に関する議論も含まれるべきである。デジタルな権利に関する議論は、ウイグル人の声に焦点を当て、嫌がらせ、脅迫、強制が彼らの生活に与える損害を含むべきである。
- **同じ志を持つ国々は、民主的なデジタルガバナンスの統一的なビジョンを作成するために協力する必要がある。**このビジョンは、政策の文言や目標と連動して、グローバル・コミュニティだけでなく、脆弱な人々のデジタルな権利と人間の安全保障をよりよく保護するものである[143]。
- **脅迫や嫌がらせ、逮捕、強制送還など、**国境を越えたすべての抑圧行為の停止を求める国境を越えた抑圧に関する国際条約を締結すること。

[143] Adapted from Steven Feldstein's recommendations in *The Rise of Digital Repression* (NewYork: Oxford University Press, 2020)