2019.01

現代の選挙介入と日本での備え

サイバー攻撃とSNS上の影響工作が変える選挙介入

Contemporary Election Interference and Our Preparedness in Japan
The Impact of Cyber Attacks and Influence Operations on Social Networks

東京海上日動リスクコンサルティング

題名

現代の選挙介入と日本での備え：
サイバー攻撃と SNS 上の影響工作が変える選挙介入

Contemporary Election Interference and Our Preparedness in Japan:
The Impact of Cyber Attacks and Influence Operations on SNSs

発行月

2019 年 1 月

初版公開日： 2019 年 1 月 28 日
1.01 版公開日：2019 年 1 月 30 日

著者

川口 貴久（東京海上日動リスクコンサルティング株式会社
戦略・政治リスク研究所[注] 主任研究員）
土屋 大洋（慶應義塾大学大学院政策・メディア研究科 教授）

備考

- 本報告書中の評価、見通し、結論、その他一切の記述は執筆者個人に帰属し、いかなる組織・法人・グループとしての意見を代表するものではありません。
- 本報告書は執筆者が妥当であると認識する評価結果を記載していますが、報告書の記載内容（評価結果、事実関係を含む）に基づく意思決定とそれによって生じる損失等について、いかなる個人・法人（執筆者および執筆者の所属・関係する組織・機関を含む）も一切の責任を負いません。
- 本報告書は、政治的に中立的な立場で執筆されたもので、いかなる特定の政党・政策・政治主張等を支持または否定するものではありません。

[注] 戦略・政治リスク研究所（Research Institute for Strategic & Political Risks）は、東京海上日動リスクコンサルティング株式会社（Tokio Marine & Nichido Risk Consulting Co., Ltd 略称 TRC）内に設置されたバーチャルシンクタンクです。戦略・政治リスク研究所はグローバルな戦略問題・政治リスク・地政学リスクについて、個別企業・組織へのコンサルティングを超えた公益性の高い調査研究を行います。
https://tokiorisk.co.jp/service/politics/RISPR/

構成

情報源および出典・脚注について

本レポートの情報源は、日本語・英語による公的機関（行政府・立法府・司法府）の公開資料・声明、国内外の大学・シンクタンク・研究機関の研究者の分析・評価、セキュリティ会社の分析・評価、国内外の調査報道・記事、筆者らによる公式・非公式のインタビューである。本レポートで大きくとりあげるロシアによる 2016 年米大統領選挙介入は主として、以下の公開資料にもとづく。

1. 米連邦政府の公式声明・発表資料、閣僚・当局者の発言。特に米国家情報長官室（ODNI）・中央情報局（CIA）・連邦捜査局（FBI）・国家安全保障局（NSA）による評価報告書（2017 年 1 月 6 日）［Office of the Director of National Intelligence (ODNI), *Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution"* (January 6, 2017)］等
2. 米司法当局・連邦地方裁判所が公開した 3 つの起訴状［U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464 (September 28, 2018); U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018); U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018)］
3. 米連邦議会上下院による報告書および上下院に提出された報告書や公聴会証言等［例えば、U.S. House of Representatives Permanent Select Committee on Intelligence, Report on Russian Active Measures viii (March 2018); U.S. Senate the Committee on Foreign Relations, *Putin''s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,* A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (January 10, 2018)等］
4. セキュリティ大手 CrowdStrike 社等の評価、SNS 大手 Facebook 社や Twitter 社等の公開資料・米連邦議会証言等
5. 英仏政府機関等が公開した声明・報告書［例えば、Jean-Baptiste Jeangène Vilmer, et. al., *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris (August 2018) 等］
6. 政治家・政府当局者の回顧録等
7. その他の調査報道・新聞記事等

本レポートでは「ロシアによる 2016 年米大統領選挙への介入」旨の表現は上記出典にもとづくものであるが、本文中では重複を防ぐため、出典・脚注をつけない。ただし、介入の具体的な内容や固有名詞が登場する場合、その都度、出典・脚注を明示する。

なお「ロシアによる 2016 年米大統領選挙への介入」の詳細は、本レポート末尾の「別紙 1：ロシアによる 2016 年米大統領選挙介入」（全 16 頁）「別紙 2： 2016 年米大統領選挙に関する推移」（全 9 頁）に記載している。

また、要約は各章・節のまとめであるため、出典・脚注を明示していない。詳細や出典は対応する章・節を参照願う。

要約

公正な選挙の実現は民主主義の根幹である。ところが、2016 年の米大統領選挙は、我々の状況認識を大きく変えることになった。外国政府による選挙介入、それもインターネットを活用した選挙介入が明白になったからである。

現代の選挙介入は民主主義にとって差し迫った脅威である。この脅威に対抗するため、本レポートは、2016 年米大統領選挙やその他選挙介入の事例を検討し、行政府としての政府、立法府としての国会、政党・政治団体、メディア・SNS プラットフォーム、そして、有権者・国民がとるべき対策と対応について論じた。

1. 選挙介入

(1)「選挙介入」とは何か？

- 選挙介入（election interference）とは、選挙・国民投票等の政治「制度」や有権者の「意思決定」に対する影響工作（influence operation）である。影響工作とは、外国政府が対象社会を分断し、政治制度の信頼性を毀損させることを通じて、政治目標を達成するための活動であり、秘密工作、公然たる工作、サイバー攻撃等を組み合わせものである。
- 「制度」への攻撃とは、選挙関連インフラに対するサイバー攻撃や投票結果の改竄等が代表的であるが、選挙や民主主義の信頼性を失墜させることも「制度」への攻撃といえる。「意思決定」への攻撃は偽情報の流布、機密情報の暴露等を通じて、有権者の「頭の中」に働きかけ、認知・意思決定・投票行動を変えるものである。

(2) 現代の選挙介入：サイバー攻撃と SNS 上での影響工作

- 選挙介入や影響工作は新しい現象ではないが、現代の選挙介入は伝統的な秘密工作、公開工作に加えて、サイバー攻撃や SNS 上での活動を利用し、効果を最大化している。
- サイバー攻撃や SNS 上での活動の特徴として以下の点が指摘できる。
  - サイバー空間を通じた選挙介入は匿名性が高い。
  - サイバー空間を通じた選挙介入は、従来（オフライン）の選挙介入と比較して「より早く」「より大量に」「より安く」が可能である。
  - 個人データが蓄積されるインターネットや SNS は効果的な選挙介入を可能にする。

(3) 誰が介入するのか？

- 選挙介入は個人、犯罪集団、テロリスト、インターネット上のアナキスト集団等が実行できる。しかし、介入の「動機」と「能力」の双方で、国家が最大な脅威であることは疑いようがない。
- 国家は代理人（proxy）を用いることで、選挙介入に関与したことを否定する。

(4) どのように介入するのか？

- 「選挙介入」という言葉で人々がイメージするものは大きく異なる。ロシアによる 2016 年米大統領選挙介入やその他介入事例から、具体的な選挙介入行為として

次のものが考えられる。①候補者・政党等への攻撃・侵入、②機密情報の暴露、③選挙インフラへの攻撃・改竄、④フェイク・コンテンツ流布、⑤フェイク・コミュニケーション、⑥ホワイト・プロパガンダ等である。

2. 日本の文脈

(1) 日本国内での過去の選挙妨害

- 日本国内においても、過去、違法な選挙妨害が確認された（ただし、外国政府によるものではない）。日本の選挙においても、妨害・介入は珍しいものではない。
- 過去の選挙妨害は特定の選挙区における直接的な妨害、情報（言葉）による妨害であり、特定候補者の当落を狙ったものであった。

(2) 政治制度：多党制・議院内閣制下での選挙介入

- 選挙介入を行う攻撃者にとって、多党制よりも二大政党制、議会選挙よりも国家元首選挙の方が介入の「コストパフォーマンス」が高い。
- 日本の多党制・議院内閣制は介入の「コストパフォーマンス」が相対的に低いものの、同じく多党制・議院内閣制を採用するドイツでも 2017 年 9 月の議会選挙で介入が確認された。日本でも、議会選挙、特に単一の争点を中心に社会分断を狙った介入が行われる可能性がある。
- 通常の国政選挙とは異なり、憲法改正に関わる国民投票は、有権者の賛否を二分しやすく、政策への影響も大きいため、特別な注視が必要である。

(3) 選挙過程の電子化・インターネット利活用

- 日本の選挙過程では、電子化・インターネット利活用が検討されている。投開票については、一部自治体では電子投票が実施され、国政レベルにおいても在外邦人を念頭としたインターネット投票を導入予定である。
- 従来から指摘された投票・集計結果の改竄の可能性は高いとは言えないが、投票・集計結果への攻撃自体が（仮に攻撃・改竄が成功しなかったとしても）選挙の正統性や投開票の信頼性を揺るがしかねないリスクである。
- 投開票以外の選挙管理要素については、情報の改竄、窃取等のリスクが懸念される。

(4) SNS 等の利用状況とプラットフォーマーの対策

- 有権者の「意思決定」への攻撃としては、SNS やインターネット上での影響工作が懸念される。
- 日本国内のオンライン上のニュースサービスでは、ポータルサイトによるニュース配信（Yahoo!ニュース等）、ソーシャルメディア（LINE、Twitter、Facebook 等）によるニュース配信の利用率が高い。ソーシャルメディア系サービス・アプリの利用率も年代が若いほど上昇傾向にある。利用率が高いということは、SNS やインターネット上での影響工作を受ける曝露量（exposure）が高いということである。
- Facebook 社や Twitter 社は、2016 年米大統領選挙や 2018 年米中間選挙の経験を経て、選挙介入対策を講じており、日本国内で事業を展開するプラットフォーマーでも同程度かそれ以上の対策が期待される。

3. 提言

- 現代の選挙介入に対抗するためには、第一義的には政府による対策・対応の強化が不可欠である。また、政府に加えて、立法府である国会、政党・政治団体、メディアとプラットフォーマー、有権者である国民による準備と対策を進めていく必要がある。
- 対策・対応には、いくつかの側面がある。第一に、サイバー攻撃やSNS上の影響工作といった選挙介入自体を予防すること【予防】、である。しかし、こうした介入をゼロにすることは事実上不可能であるため、第二に、介入が生じた場合、その影響を極小化すること、影響が生じたとしても復旧力（レジリエンス）を高めること【極小化】である。第三に、介入に対して断固たる措置をとることで、現在進行形および将来の選挙介入を抑止すること【事後対応】である。

とるべき対策（現代の選挙介入に対する備え）

とるべき対策	予防	極小化	事後対応
政府がとるべき対策			
選挙インフラに関するリスク評価と対策	✓		
コンティンジェンシープラン（オフライン投開票）の策定・維持		✓	
選挙介入に関する規範形成・宣言政策	✓		✓
選挙介入の検知能力の向上、有権者および候補者等へのアラート	✓	✓	
アトリビューション能力の向上と制裁オプションの整備			✓
中学校・高校でのリテラシー教育	✓		
国会がとるべき対策			
選挙介入対策のための超党派委員会	✓		✓
公職選挙法改正等による選挙介入の規制	✓		✓
プラットフォーマーに対する規制	✓	✓	
政党・政治団体等がとるべき対策			
候補者のサイバーセキュリティ改善	✓		
政党・政治団体等のサイバーセキュリティ改善	✓		
メディア・SNSプラットフォーマー等がとるべき対策			
選挙介入・偽情報に関する明確な用語・用法の使用	✓		
偽情報の検証機能の確立	✓	✓	
インターネット上の選挙介入対策、オンライン上の透明性向上	✓		
有権者・国民がとるべき対策			
情報ソースの信頼性確認	✓		
個別の情報媒体やメディアについて知る	✓		
【非推奨】ファクトチェック機関への全面的信頼	✓		

※　法改正・立法を伴う対応は「政府」でも可能であるが、上記では便宜的に「国会」に分類した。

はじめに

公正な選挙の実現は民主主義の根幹である。しかし、歴史はその実現が難しいことを示している。近年の日本の選挙においても、例えば、一票の格差は常に問題となっている。また、買収等の公職選挙法違反による検挙も絶えることがない。公職選挙法は、候補者ができること、できないことを細かく規定しているが、2013 年 4 月までインターネットを使った選挙は実質的に行うことができなかった。遅れたのは選挙の公正性をいかに確保するかという点について合意がなかなか定まらなかったからである。

ところが、2016 年の米大統領選挙は、我々の状況認識を大きく変えることになった。外国政府による選挙介入、それもインターネットを活用した選挙介入が明白になったからである。それ以前にも他国への選挙介入の事例はあった。米国が秘密工作活動の一環として中南米諸国に介入したこともあったし、台湾の選挙に中国が露骨な介入を口にしたこともあった（詳細は本レポート 1.　　を参照）。しかし、2016 年の米大統領選挙においてロシア政府は、米国の SNS（Social Networking Service）のプラットフォームを活用し、米国民の頭の中に手を入れてかき回すかのようにフェイクニュースをばらまき、選挙の正統性そのものに米国民が疑いを抱くよう誘導しようとした。

それは、2001 年 9 月 11 日に起きた対米同時多発テロ（9.11 テロ）において、アルカイダが米国航空会社のジェット機というグローバリゼーションの象徴的な技術を使って米国経済の中心ニューヨークと政治の中心ワシントン DC を狙ったことと呼応している。ロシアの大統領選挙への介入は、人々を殺傷することはなかったが、米国の中心的価値への攻撃という点では、9.11 テロに匹敵する衝撃だった。

従来からのプロパガンダや世論誘導と比べ、インターネットはそのコストを劇的に下げ、実行主体を隠しやすくしている。例えば、戦時中に敵国にビラを撒くには大量にビラを作成・印刷し、撃墜されるリスクを背負いながら飛行機で敵国上空を飛ぶ必要があった。誰が撒いたかは自ずと明らかであっただろう。あるいは、ラジオ放送やテレビ放送を使って隣国にメッセージを流し続けるということも、ソフトパワー（強制力によらず、文化や政治的価値観、政策の魅力などに対する支持や理解、共感を得ることによる影響力）の一環として行われたが、電波が妨害されてしまえばそれまでであった。

しかし、インターネットでは広告を装ったり、一般人による投稿であることを見せかけたりしながら、メッセージを特定のターゲットに向けて送り届けることができるようになった。インターネットでは「サイバーカスケード[1]」や「エコーチェンバー」、「フィルターバブル[2]」と呼ばれるように、自分の好む情報にしか接しない環境を構築することができる。多様な意見に接する機会が減るため、目の前にある情報を信じ込む可能性が高くなる。こうした情報の環境変化はフェイクニュースの送り手には有利になる。

[1] キャス・サンスティーン（石川幸憲訳）『インターネットは民主主義の敵か』（毎日新聞社、2003 年）
[2] イーライ・パリサー（井口耕二訳）『閉じこもるインターネット：グーグル・パーソナライズ・民主主義』（早川書房、2012 年）

日本の選挙においては、米国大統領選挙ほど明白な事例は、今のところは起きていないだろう。しかし、これは宣戦布告を伴って行われる戦争とは全く異なる情報戦であり、時には物理的な戦争と組み合わせて行われるハイブリッド戦にもなるかもしれない。外国政府が日本の選挙に介入するとなれば、やみくもに行われるのではなく、何らかの具体的・抽象的な狙いを持って行われるだろう。それは特定候補を勝たせるためであったり、日本の政治制度そのものの信頼を損ねるためであったり、日本の経済システムを混乱させるためだったり、交渉を有利に進めるためだったりするかもしれない。その狙いが事前に分かっていれば対処はしやすいが、多くの場合は事前に分からず、密かに介入は行われ、事後にも気づかない場合があるかもしれない。

選挙介入は、多くの場合いつ来るか分からないとしても、天災ではなく人災であり、明白な脅威である。過去の事例を検証し、今後どのような可能性があるかを検討しておくことは、実際に事案が起きたときの初動体制に影響する（なお、日本および諸外国で予定されている選挙は表 1 を参照）。

本レポートはそうした問題意識から、選挙介入の事例を検討し、行政府としての政府、立法府としての国会、政党・政治団体、メディア・SNS プラットフォーム、そして、有権者・国民がとるべき対策と対応について論じた。

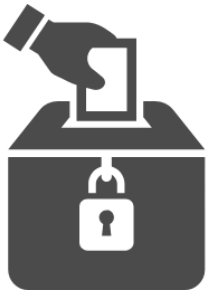
表 1：今後予定される日本および諸外国の主要な選挙

投票時期*	国・地域	選挙
2019 年　2 月 24 日	モルドバ	議会選挙
2 月 24 日	日本	普天間基地の辺野古移設に係る県民投票
3 月 3 日	エストニア	議会選挙
3 月 24 日	タイ	民政移管に向けた総選挙
3 月 31 日	ウクライナ	大統領選挙
4 月 7 日、21 日	日本	統一地方選挙
4 月 9 日	イスラエル	議会選挙
4 月 14 日	フィンランド	議会選挙
4 月 17 日	インドネシア	大統領選挙、国民議会選挙
5 月 12 日、26 日	リトアニア	大統領選挙
5 月 13 日	フィリピン	上下院中間選挙
5 月 23～26 日	欧州連合	欧州議会選挙
4～5 月	インド	下院選挙
7 月	日本	参議院議員選挙
7 月 20 日	アフガニスタン	大統領選挙
10 月	ウクライナ	議会選挙
	ラトビア	大統領選挙
	香港	地方選挙
2020 年　1 月	台湾	中華民国総統選挙、立法院選挙
7 月	日本	東京都知事選挙
11 月 3 日	米国	大統領選挙
未確定	香港	立法会選挙
2021 年　10 月頃	日本	衆議院議員選挙（満期解散の場合）

出典：筆者作成。
* 上記は 2019 年 1 月時点で判明している諸外国・日本の主要な選挙予定である。この他、特定争点に関する国民投票（例：2016 年 6 月 23 日の英国の EU 離脱を問う国民投票）、憲法改正に関わる国民投票（例：2017 年 4 月 16 日のトルコ憲法改正に関わる国民投票）等が開催される可能性がある。また議会の解散や首長の辞任、その他理由等により、選挙日程が前倒し・先送りされることもある。

1. 選挙介入

外国政府による選挙介入は新しい現象ではない。しかし、現代の選挙介入はサイバー攻撃や SNS 上での工作活動を組み合わせ、その影響力は甚大である。



（1）「選挙介入」とは何か？

- 選挙介入（election interference）とは、選挙・国民投票等の政治「制度」や有権者の「意思決定」に対する影響工作（influence operation）である。
- 影響工作とは、外国勢力が、対象社会の分断・政治制度の信頼性毀損させることを通じて、政治目標を達成するための活動であり、秘密工作、公然たる工作、サイバー攻撃等を組み合わせたものである。

「選挙介入」とは、政治制度と意思決定に対する影響工作

「選挙介入（election interference）」とは、選挙・国民投票等の政治「制度」や有権者の「意思決定」に対する影響工作（influence operation）を指す。

「影響工作」とは、外国政府が、対象社会の分断・政治制度の信頼性毀損させることを通じて、政治目標を達成するための活動であり、秘密工作、公然たる工作、サイバー攻撃等を組み合わせたものである[3]。類似の概念・用語として、「偽情報工作」「積極工作（active measures）」「情報操作（information manipulation）」「プロパガンダ工作」「フェイクニュース」「ハイブリッド戦争」があげられるが、ここでは包括的な概念として影響工作を用いる[4]。

前述のとおり、選挙介入は制度や意思決定に対する攻撃である。欧州委員会でセキュリティを担当するキング（Julian King）委員も選挙介入の 2 つの類型、つまり、選挙や民主主義といった「制度（systems）」に基づく介入、人々の「投票行動（voting behaviors）」基づく介入を指摘する[5]。前者は選挙関連インフラに対するサイバー攻撃や投票結果の改竄等が代表的であるが、選挙や民主主義の信頼性を失墜させることも「制度」への攻撃といえる。後者は偽情報の流布、機密情報の暴露等を通じて、有権者の「頭の中」に働きかけ、認知・意思決定・投票行動を変容させるものである。

---

[3] 米司法省が定義する「海外からの悪意ある影響工作（Malign Foreign Influence Operations）」も同様の定義である。Department of Justice, *Report of the Attorney General's Cyber-Digital Task Force* (July 19, 2018), pp.1-2.

[4] 米上院外交委員会はロシアに焦点を当てて、「現代のクレムリンの悪意ある影響工作（the Kremlin's malign influence operations）」を定義する。ジョンズホプキンズ大学のリッド（Thomas Rid）もロシアに焦点を当て「積極工作（active measures）」を定義する。フランス大統領選挙への介入を受けたフランス政府は、「情報操作（information manipulation）」として概念化している。 *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security, A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate*, One Hundred Fifteenth Congress, Second Session (January 10, 2018), p.37; Thomas Rid, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," Hearing before the Select Committee on Intelligence, U.S. Senate, One Hundred Fifteenth Congress, First Session (March 30, 2017); Vilmer, Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris (August 2018), pp.11-12.

[5] Julian King, "Commissioner King's speech to the Aspen Institute: Protecting Western democracies from manipulation and disinformation," European Commission (June 21, 2018). 詳細は、湯淺墾道「2019 年欧州議会選挙とインターネット・SNS（2）」『選挙』第 71 巻、9 号（2018 年 9 月）、1-2 頁。

選挙介入はどのような効果をもたらすのか

なぜ、外国の選挙に介入するのか。それは何らかの政治目標・戦略的目標を達成するためである。最も分かりやすいのは、**①外国勢力にとって有利な特定の候補者・政党・政策の実現可能性・当選可能性を高める**ことである。

しかし、影響工作は必ずしも、単一の候補者・政党・政策を支援するものではない。**②社会の分断・対立を深刻化・過激化させる**ことも選挙介入の狙いだ。影響工作は「社会の異なる政治グループ間での緊張を煽るため、SNS のプラットフォームを利用し、ユーザの政治的および人口動態上の分析結果に基づいて、異なるグループに同時にメッセージ（時には欺瞞情報）を発信する[6]」ことを含む。熟議の過程または結果として「国論を二分」することは健全な民主制であるが、選挙介入は「国論を二分」すること自体が目的である。

上記①②は有権者の意思決定・投票行動を意図的に誘導し、あるいは民意形成を妨害するものである。これらに加えて、選挙や民主主義といった制度の信頼性・正統性を損ねることも選挙介入の狙いである。

選挙介入は**③特定の選挙や投票の正統性、特定の選挙結果や投票結果にもとづく当選者・政策の信頼性を損ねる**ことで、選挙で民意を得たはずの政治家や政策を制約する効果がある。また特定の選挙・投票に留まらず、近代に発達した**④民主制や政治プロセス全般、メディアの信頼性を損ねる**、ものである[7]。

表 2：選挙介入の「対象」と「範囲」

対象＼範囲	特定の候補者・政策・選挙	社会全体・政治全体
有権者 （有権者の意思決定・投票行動、民意形成への攻撃）	• A 氏を当選させる。X 党を勝たせる。（B 氏を落選させる。Y 党を負けさせる） • 国民投票で法案を可決または否決させる。	• X 党支持者と Y 党支持者の対立を煽る、深刻化させる。 • 人種間、宗教間、その他の異なる社会集団間の対立を煽る、深刻化させる。
制度 （選挙や民主主義等の制度への攻撃）	• 特定の選挙・投票との結果の信頼性を損ねる。選挙結果に基づく政権や議員の信頼性を貶める。 • 「B 氏が当選した選挙はインチキだ！」等の声があがる。	• 民主主義、選挙制度への信頼性を貶める。 • 「民主主義には欠陥がある！」等の声があがる。

出典：筆者作成。

[6] *Report of the Attorney General's Cyber-Digital Task Force*, p.2.
[7] 民主主義が機能するためには、有権者が民主主義や投票等の「共通の政治知識（common political knowledge）」を持つことが不可欠である。したがって、民主国家はこうした「共通の政治知識」への攻撃に脆弱である。Henry Farrell & Bruce Schneier, *Common-Knowledge Attacks on Democracy*, Berkman Klein Center Research Publication No. 2018-7, Harvard University (October 2018).

（2）現代の選挙介入：サイバー攻撃と SNS 上での影響工作

- □ 選挙介入や影響工作は新しい現象ではないが、現代の選挙介入は伝統的な秘密工作、公開工作に加えて、サイバー攻撃や SNS 上での活動を利用し、効果を最大化している。
- □ サイバー攻撃や SNS 上での活動の特徴として以下の点が指摘できる。
  1. サイバー空間を通じた選挙介入は匿名性が高い。
  2. サイバー空間を通じた選挙介入は、従来（オフライン）の選挙介入と比較して「より早く」「より大量に」「より安く」が可能である。
  3. 個人データが蓄積されるインターネットや SNS は効果的な選挙介入を可能にする。

選挙介入の歴史は選挙自体の歴史同様に古い。18 世紀末に近代普通選挙が誕生するはるか以前から、古代ギリシアの投票制度（陶片追放制度）等でも、投票プロセスや結果に対する介入があったと推察される。冷戦時代では、米ソが友好勢力のために諸外国の選挙に介入・干渉した。

しかし、近年、選挙介入が注目されるようになったのは、サイバー空間や SNS の発達の結果、**選挙介入にサイバー攻撃や SNS 上の影響工作が用いられ、選挙介入の規模・影響が大きくなった**からである。その規模と影響を鑑みて、国際政治や安全保障分野を中心に、サイバー攻撃と影響工作から民主主義をどのように守るか、という観点での考察が行われている[8]。

攻撃者はサイバー攻撃を通じて政党や政治家事務所のネットワークに侵入し、機密情報を盗み、自らの政治目標に沿う形で機密情報を戦略的にリビール（暴露）する。あるいは情報インフラ化された選挙関連システムに侵入し、集計結果や選挙結果を改竄、または選挙関連システムを利用できないようにする。サイバー攻撃による改竄は成功せずとも、攻撃の事実自体が選挙の正統性を揺るがせる。攻撃者は Facebook、Twitter、YouTube 等の SNS 上で意図的な情報流布や偽情報を発信し、有権者の認知や投票行動に影響を及ぼそうとする[9]。

このように、現代の選挙介入は手法の面で新しさがある。サイバー攻撃や SNS 上の影響工作として、次の特徴が指摘できる。

---

[8] 例えば、Thomas Rid & Ben Buchanan, “Hacking Democracy,” *SAIS Review of International Affairs*, Vol.38, No.1 (Winter-Spring 2018), pp. 3-16; Joseph S. Nye, Jr., “Protecting Democracy in an Era of Cyber Information War,” Fall Series, Issue 318, Hoover Institution (November 13, 2018).

[9] オックスフォード大学のインターネット研究所（Oxford Internet Institute: OII）は SNS 上の影響工作を「コンピュータによるプロパガンダ（Computational Propaganda）」、「SNS 上で意図的な偽情報の散布するため、アルゴリズム、自動化、人的キュレーションを用いる」影響工作と定義する。OII の報告書によれば、2015-2017 年の米国、中国、ロシア、ポーランド、ブラジル、カナダ、ドイツ、ウクライナ、台湾ではコンピュータ・プロパガンダが確認された。Sam Woolley and Phil Howard, “Computational Propaganda Worldwide: Executive Summary,” Computational Propaganda Research Project, Working Paper No. 2017.11, Oxford Internet Institute, University of Oxford (June 19, 2017), p.3.
https://www.oii.ox.ac.uk/blog/computational-propaganda-worldwide-executive-summary/

特徴 1 サイバー空間を通じた選挙介入は匿名性が高い

サイバー攻撃や SNS 上の活動は、匿名性が高く、攻撃者をただちに断定することができない。これは「アトリビューション」問題と呼ばれる[10]。よく言われることだが、「ミサイルを撃てば、どこから発射されたかを直ちに特定できる」が、サイバー攻撃や SNS 上の影響工作の発信源を直ちに特定することは難しい。

ただし、匿名性が高いというのは「攻撃者を特定できない」ということではない。攻撃元の特定（アトリビューション）には時間がかかり、一定のリソースを必要とするが、不可能ではない。例えば、米国土安全保障省の政策担当次官補代理（2005－2009 年）を務めたローゼンツヴァイク（Paul Rosenzweig）は、条件付きでアトリビューションは実現可能だという。彼によれば、アトリビューションとは究極的に「リソース」と「許可」の問題である。十分な時間、資金、スキルと慎重さを備えた要員、場合によっては違法とみなされる行為（例えば、海外にあるサイバー攻撃の指揮・命令を行うサーバへの逆ハッキング（hack-back）等）に手をかけることによって、時間は要するがアトリビューションは実現可能である[11]。

とはいえ、選挙介入に関するアトリビューションは「時間との闘い」である。投票日よりも前に、攻撃者を特定し、耐え難い報復を与え、国民に警鐘を鳴らさなければならない。投票日以降のアトリビューションは、将来の選挙介入を抑止できるかもしれないが、その選挙については何ら意味をなさい。

特徴 2 サイバー空間を通じた選挙介入は「より早く」「より大量に」「より安く」

サイバー空間を通じた選挙介入は、遠隔地にいながら、「より早く」「より大量に」「より安く」を可能にする。例えば、2016 年米大統領選挙に関して、ロシア・サンクトペテルブルグに所在する Internet Research Agency（IRA）社は SNS 上で大規模な影響工作を展開した。表 3 に記載のとおり、IRA 社が購入した Facebook 上の政治広告は 3,393 点、IRA のコンテンツを視聴したであろう米国人は 1 億 2,600 万人に及ぶ（期間：2015 年 6 月から 2017 年 8 月）。Twitter 上でのボット（自動化されたプログラム）による投稿の視聴数は 2 億 8,800 万ビューに達する（期間：2016 年 9 月 1 日から 11 月 15 日）。

選挙介入の実行者は、これらを比較的短期間で実施し、低コストでこれを実現した。IRA の予算は、最も多い時（大統領選挙が佳境となる 2016 年 9 月）でさえ、月額予算は 7300 万ルーブル（約 1 億 3,000 万円）であった。オフラインで同様の効果を狙うとしたら、より多くのリソース（時間、要員、資金）を必要としたことは間違いない。これは選挙介入に限定されず、サイバー空間上の活動全般にいえることである。

---

[10] 詳細は土屋大洋『サイバーセキュリティと国際政治』（千倉書房、2015 年）、14-20 頁；Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *The Journal of Strategic Studies*, Vol.38, No.1-2, 2015, pp.4-37［トマス・リッド、ベン・ブキャナン（土屋大洋訳）「サイバー攻撃を行うのは誰か」『戦略研究』第 17 巻（2016 年 5 月）、59-98 頁］；川口貴久「サイバー攻撃は誰がやった？」、ChannelJ 運営情報サービス「安全保障用語」解説・コラム（2018 年 10 月 12 日）【http://dictionary.channelj.co.jp/2018/18101204/】を参照。

[11] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (New York: Praeger Security International, 2013), pp.78-79.

特徴 3 個人データが蓄積されるインターネットや SNS は効果的な選挙介入を可能にする

今日、人々は多くのニュースを SNS やインターネットから得ている。米国のデータであるが、2017 年 8 月時点で米国人の 67%は SNS からニュースを入手しており、これは増加傾向にある[12]。

そして、SNS をはじめとするインターネット空間は、ユーザにとって**「見たい」情報が目につきやすく、「見たくない」情報は目につきにくい状態**になりやすい。それは**「エコーチェンバー（Echo Chamber）」効果と「フィルターバブル（filter bubble）」効果**によるものである[13]。結果、ユーザが得る情報は偏りがちとなる。

「エコーチェンバー」効果とは、SNS 等で自分と同じような意見・情報ばかりが流通される閉じた環境が形成されることである。ここでは異なる意見や情報は「フェイク」として扱われやすい。

「フィルターバブル」効果とは、フィルターを通じて、自分に興味関心がある情報のみが選別され、そうした情報ばかりにアクセスすることである。この「フィルター」とは、検索エンジン、ブラウザ、SNS 等に埋め込まれたアルゴリズムである。

インターネットユーザや SNS 上のユーザ・有権者は、国籍・居住地、年齢、職業等の様々な情報をプラットフォーマーに提供している。こうした **SNS 上のユーザ・有権者に関するビッグデータを分析することで、より効果的な選挙介入が可能**である。SNS 上のユーザ情報・投票行動の分析は多くの政党やメディアが行っているように、攻撃者にもそれが可能である。

Facebook のユーザ情報約 8,700 万人を不正に入手していたケンブリッジ・アナリティカ（Cambridge Analytica）社の元従業員ワイリー（Christopher Wylie）によれば、SNS 上のグループの属性に合わせて、政治宣伝や情報を提供することで、ある特定の有権者グループの投票行動を自らにとって望ましいものにできる[14]。特定のグループの選好・嗜好に関するデータを分析することで、ターゲットに効果的なメッセージを発することができる。最も分かりやすい例は、Facebook 上でのターゲティング広告・政治広告だろう（表 3）。

特定グループを対象としたターゲティング広告だけではなく、原理的には個人にカスタマイズした「マイクロ・ターゲティング」広告も可能である。また、「検索エンジン最適化（Search Engine Optimization: SEO）」技術、すなわち、特定のサイト・情報が Google や Yahoo!等の検索エンジンで検索結果の上位にランクインされるような手法は特定ニュースや情報を多くの人に暴露させることができる「マス・ターゲティング」といえる。

---

[12] Elisa Shearer and Jeffrey Gottfried, News Use across Social Media Platforms 2017, Pew Research Center (September 6, 2017).

[13] パリサー、前掲書『閉じこもるインターネット』。こうした効果は、笹原和俊『フェイクニュースを科学する：拡散するデマ、陰謀論、プロパガンダのしくみ』（化学同人、2018 年）の「第 3 章　見たいものしか見えない情報環境」（81-115 頁）に詳しい。

[14] Carole Cadwalladr and Emma Graham-Harrison, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,” *The Guardian* (March 17, 2018).

表 3：IRA 社による Facebook 上の政治広告（ターゲティング広告）

No.	投稿イメージ	メタデータ
1		Ad ID 467 Ad Text America has always been hinged on hard-working people. If you remove jobs you'll remove our country from the world map. The state of Pennsylvania rose owing to multiple enterprises mining coal, producing steel, and creating the need for other jobs, groceries, doctors, dentists, insurance, gas, vehicles, mechanics and the list goes on. As far as Mr. Trump pursues the goal of creating more jobs and supports the working class. He said he would put miners back to work. We could help Mr. Trump win Pennsylvania which is a battleground state. We'd like to organize a rally "Miners for Trump" in Pennsylvania. Have something against coal industries? Please note then that burning coal is not more harmful than lumber. Alternative energy is only possible when subsidized by government for it is not lucrative. You cannot leave tens of thousands of people without a job just because of lobbyists' interests. The current list of locations is being elaborated. Suggested cities are Erie, Pittsburg, Scranton, Harrisburg, Allentown, and Philly Confirmed locations: Marconi Plaza, Philadelphia. Miners for Trump: Unity day in Pennsylvania Ad Landing Page https://www.facebook.com/events/312522819127036/ Ad Targeting Location - Living In: United States: New York (+50 mi) New York Age: 18 - 65+ Placements: News Feed on desktop computers or News Feed on mobile devices Ad Impressions 2 Ad Clicks 0 Ad Spend 2.96 RUB Ad Creation Date 09/22/16 05:01:05 AM PDT Ad End Date 10/01/16 01:00:00 PM PDT
2		Ad ID 1105 Ad Text On October 15, 1966, Bobby Seale and Huey P. Newton have founded BPP. Their idea was simple - we can't just talk to make the change, we must take action. They started to monitor the behavior of police officers and challenge police brutality in Oakland, California. And they succeeded. Unfortunately, the government and especially Federal Bureau of Investigation called the party "the greatest threat to the internal security of the country". They tried to close it, to incarcerate BPP's participants, and in 1982 the original party was dissolved. 50 years have passed since BBP's foundation, but the situation in the country stills the same. Cops are shooting Blacks. It spreads through all the country like the disease. Nowadays we need Black Panthers as never before. We need a strong hand that can protect us, that can keep our people safe, that can make Black Lives really matter. Let's get together and celebrate the 50th anniversary of the party that has made the change. Let's honor its founders and participants. Let's share their ideas and ideals! Black Panther Party 50th Anniversary Ad Landing Page https://www.facebook.com/events/1094784283992152/ Ad Targeting Location: United States: Cleveland (+34 mi) Ohio Age: 16 - 45 Language: English (UK) or English (US) Placements: News Feed on desktop computers or News Feed on mobile devices Ad Impressions 0 Ad Clicks 0 Ad Spend None Ad Creation Date 09/29/16 07:07:13 AM PDT Ad End Date 10/14/16 03:00:00 PM PDT

【説明】米下院情報問題常設特別調査委員会（HPSCI）は 2018 年 5 月 10 日、ロシア政府に関連する企業 IRA 社による政治公告約 3,500 点（2015 年第 2 四半期から、2017 年第 4 四半期までに確認されたもの）を公開した。全ての政治広告の実際の投稿イメージとメタデータ（作成・削除日時等）を掲載している。注目すべきは、こうした政治広告はターゲット層（上記の四角囲み）が絞り込まれている点である。上記のメタデータの No.1 はニューヨーク在住の 18 歳以上をターゲットにしているが、No.2 はオハイオ州クリーブランド（Cleveland）在住の 16-45 歳までをターゲットにしている。なお、こうした状況をふまえて、Facebook 社は 2018 年 5 月から政治広告をこれまで以上に規制している。

出典：以下で約 3,500 点の政治広告を確認できる。
The House Permanent Select Committee on Intelligence, Social Media Advertisements
https://democrats-intelligence.house.gov/social-media-content/social-media-advertisements.htm

（3）誰が介入するのか？

- □ 選挙介入は、個人、犯罪集団、テロリスト、インターネット上のアナキスト集団等が実行できる。しかし、介入の「動機」と「能力」の双方で、国家が最大な脅威であることは疑いようがない。
- □ 国家は代理人（proxy）を用いることで、選挙介入に関与したことを否定する。

選挙介入を行う最大の脅威は「動機」「能力」の面で国家である

選挙介入は、個人、犯罪集団、テロリスト、インターネット上のアナキスト集団等が実行できる。政策・政治に不満を持つ個人は「フェイクニュース」を作成できるし、インターネット上のアナキスト集団はより組織的・大規模にそれを実行可能である。

しかし、選挙介入を行う最大の脅威は国家である。国家には、他国の国政選挙に介入する政治的・戦略的「動機」がある。また選挙介入の「能力」面、すなわち資金、スキル、要員面でも優位性がある。選挙介入に限らず、サイバー攻撃や SNS 上の工作活動の中で、最も洗練された攻撃や破壊的活動は国家によるものである。

米セキュリティ会社マンディアント（Mandiant）の最高技術責任者を務めたベトリッチ（Richard Bejtlich）はサイバー攻撃について、**国家とその他のアクターを分かつのは、近接工作活動（close access operations）と電子信号諜報（Signal Intelligence: SIGINT）能力**だと論じる。国家はサイバー活動のため、必要であれば、諸外国に工作員を派遣する。逮捕・拘束の恐れがあるため、他のアクターはあまり行わない。また、インターネット上の大量の通信を傍受することのできる SIGINT 能力は国家のみが保有する資産である[15]。

国家は、「代理人」を使って選挙介入への関与を否定する

国家、具体的には軍、情報機関、治安機関は自ら選挙介入を行う。同時に、国家は選挙介入の際、「代理人」を使うことで、関与を否定することができる。こうした代理人は、国家から資金・技術・戦術的な支援を受けた偽造民間団体やペーパー企業等である。ただし、国家が選挙介入を行う場合の関与度は様々である。①最高指導者による承認と国家による直接指揮がある場合、②国家が「代理人」に支援を行い、介入を奨励する場合、③国家が「代理人」による介入を看過する場合（消極的関与）等である。

2016 年米大統領選挙においても、ロシア政府はその関与を否定するために、偽の攻撃者を仕立てあげた。ロシア連邦軍参謀本部情報総局（Glavnoye Razvedyvatelnoye Upravleniye: GRU, 英語表記では Main Intelligence Directorate of the General Staff）が、偽

[15] Richard Bejtlich (@taosecurity), tweets “Close access operations are one of the differentiators between nation state groups and other hacking units. Close access puts operators at risk of arrest. While some private org are willing to do this, it is not popular. National asset SIGINT is another differentiator.” at 00:50, October 5, 2018.

の攻撃者（「Guccifer 2.0」を自称するハッカー）をオンライン上に仕立てあげたことは有名である[16]。

国家による攻撃グループは洗練された活動を行うため、サイバーセキュリティ各社の関心度は高い。そのため、セキュリティ各社は詳細な調査を行い、攻撃者グループに独自の名称を与えている。ただし、セキュリティ各社が呼んでいる攻撃グループは完全に一致しているわけではなく、若干の差異もある[17]。

2016 年米大統領選挙介入では、ロシア GRU が大きな役割を担った。表 4 は、GRU または GRU と密接な関係にあるサイバー攻撃グループについて、セキュリティ各社がつけている名称、または攻撃グループが自称している名称である。これらは全て同じグループと考えて良い。

表 4：GRU または GRU と密接な関係にあるサイバー攻撃グループの名称

No.	名称	備考
1	APT 28	Fire Eye 社等による呼称。
2	Fancy Bear	CrowdStrike 社等による呼称。
3	Sofacy	Kaspersky 社、PaloAlto 社等による呼称。
4	Pawnstorm	Trend Micro 社等による呼称。
5	Sednit	ESET 社等による呼称。
6	CyberCaliphate	攻撃者がサイバー攻撃をイスラム過激派の仕業に見せかけるために用いる場合の自称。
7	Cyber Berkut	親露系の犯罪グループ。ウクライナ政府や NATO 関連サイトに DDoS 攻撃を行い、反ロシア系ウクライナ政治家の機密情報を暴露する。
8	Voodoo Bear	
9	BlackEnergy Actors	ウクライナで広域停電を引き起こすサイバー攻撃（2015 年 12 月）等を実行した攻撃グループの呼称。
10	STRONTIUM	Microsoft 社等による呼称。
11	Tsar Team	
12	Sandworm	

出典：“Reckless campaign of cyber attacks by Russian military intelligence service exposed,” National Cyber Security Centre (October 4, 2018)をもとに筆者作成。「備考」覧は筆者作成。なお、NCSC は英国の国営サイバーセキュリティ対策機関であり、同国で統一的な指針・助言の発出、サイバーセキュリティ・インシデントの対応・調整を行う。NCSC は、諜報機関である政府通信本部（Government Communications Headquarters: GCHQ）の一部であり、GCHQ のアセットや要員（特に SIGINT 能力）を利用していると考えられる。

[16] Office of the Director of National Intelligence (ODNI), *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (January 6, 2017), pp.2-3; U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018), pp.14-19.
[17] John S. Davis II, et.al., S*tateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica: RAND Corporation, 2017), pp.20-21.

（4）どのように介入するのか？

□ 「選挙介入」という言葉で人々がイメージするものは大きく異なる。ロシアによる 2016 年米大統領選挙介入やその他介入事例から、具体的な選挙介入行為として次のものが考えられる。
- 候補者・政党等への攻撃・侵入
- 機密情報の暴露
- 選挙インフラへの攻撃・改竄
- フェイク・コンテンツ流布
- フェイク・コミュニケーション
- ホワイト・プロパガンダ

2016 年米大統領選挙への介入

「選挙介入」という言葉で人々がイメージするものは大きく異なる。そして外国勢力による選挙介入の詳細が明らかになることは少ない。そのような中、2016 年米大統領選挙に対する選挙介入は規模と影響の観点で他を圧倒し、具体的な手法等を確認できる（詳細は巻末別紙を参照）。少なくとも米国が主張するロシアによる選挙介入は以下の要素を含む（表 5）。

表 5：2016 年米大統領選挙への介入の構成要素

No.	分類	概要
1	機密情報の窃取と暴露	・米民主党議会選挙委員会（DCCC）、米民主党全国委員会（DNC）、ヒラリー・クリントン候補選挙対策事務所等の民主党関係機関、共和党全国委員会（RNC）へのハッキングと情報窃取 ・収集した情報の暴露（自らが作り上げた架空のオンラインハッカーGuccifer 2.0 およびウェブサイト DCLeaks.com 経由した暴露、WikiLeaks 等への暴露）
2	各種メディアを用いた影響工作	・トロールやボットを用いたソーシャルメディア（Facebook, Twitter）上での世論誘導・分断、偽情報の投稿 ・ソーシャルメディア（Facebook, YouTube）を用いた政治広告・宣伝 ・ロシア系メディア（RT, sputnik）を用いた偽情報の拡散、プロパガンダ流布
3	選挙関連システムへの攻撃	・各州の選挙管理委員会ウェブサイトや関連システムへの攻撃、投票結果の改竄（未遂）、関連企業への攻撃

なお、ロシア政府とトランプ陣営の共謀が疑われている点については、本レポート執筆（2018 年 12 月）時点で明確な判断結果・評価結果が下されていないので割愛する。
出典：US District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018); *Indictment* ,Case 1:18-cr-00032-DLF (February 16, 2018); ONDI, *Op. Cit.*を基に筆者作成。

ロシアによる欧州各国の選挙への介入

ロシアによる選挙介入は米国だけにとどまらない。オランダ、フランス、ドイツでも国政選挙に介入が疑われており[18]、2016 年の英国の EU 離脱国民投票においても介入したとみられている[19]。大西洋評議会（Atlantic Council）の研究では、2016 年米大統領選挙介入を含む、複数のロシアによる選挙介入を分析し、選挙介入行為として以下を列挙する（表 6）[20]。

表 6：選挙介入行為の分類と概要（大西洋評議会）

分類	概要
インフラ侵入 （Infrastructure Exploitation）	偵察・情報収集活動を含む、ネットワークやシステムへの侵入と機密情報収集、脆弱性・機能情報の収集。
投票・集計結果の改竄 （Vote Manipulations）	投票結果、入力内容、伝送内容を改竄し、結果そのものや投票の信頼性に疑念を生じさせること。
戦略的情報開示・暴露 （Strategic Publication）	非合法に収集した情報、特に「インフラ侵入」で入手したものを暴露すること。
架空のコミュニケーション （False Front Engagement）	個人またはグループの虚偽の公的アイデンティティを作り、他者とコミュニケーション、刺激、組織化する。
感情の増幅 （Sentiment Amplification）	特定の視点を広く普及させ、突出させること。こうした感情の増幅は、国営メディア等を通じて明示的に遂行される場合もあれば、「架空のコミュニケーション」のように秘密裡に遂行される場合もある。
欺瞞情報の作成・流布 （Fabricated Content）	完全な虚偽または事実を歪曲したプロパガンダ。これは意図的に、有権者が候補者や選挙結果について誤解するように仕向けることを含む。

出典：Laura Galante & Shaun Ee, “Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents,” Issue Brief, Atlantic Council (September 2018).

大西洋評議会は上記の選挙介入行為について、欧米における 5 つの国政選挙を比較検討した（表 7）。

18 「ロシアが欧州各国で『選挙妨害』」『選択』（2017 年 3 月）、24-26 頁。
19 「ロシア、ツイッターで英政治介入か　EU 離脱巡り」『日本経済新聞』（2017 年 11 月 15 日）。
20 Laura Galante & Shaun Ee, “Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents,” Issue Brief, Atlantic Council (September 2018).　この他の分析として、スウェーデン国防大学非対称脅威研究センター（Center for Asymmetric Threat Studies : CATS）は、Hybrid COE（European Centre of Excellence for Countering Hybrid Threats）と共同で、「ハイブリッド脅威」を構成する 16 のツールを明示している。Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee & Madeline McCue, *Addressing Hybrid Threats* (Stockholm: Center for Asymmetric Threat Studies, Swedish Defence University, 2018).

表 7：ロシアによる最近の選挙介入の概要と比較（大西洋評議会）

選挙名（年）	ウクライナ 大統領選挙 （2014）	英国の EU 離脱 を問う国民投票 （2016）	米国 大統領選挙 （2016）	フランス 大統領選挙 （2017）	ドイツ連邦 議会選挙 （2017）
インフラ侵入	✓	※	✓	✓	✓
投票・集計結果 の改竄	✓				
戦略的 情報開示・暴露			✓	✓	
架空の ｺﾐｭﾆｹｰｼｮﾝ		✓	✓		
感情の増幅		✓	✓	✓	✓
欺瞞情報の 作成・流布	✓	✓	✓		✓

※一般的には、インフラ侵入があったと報じられているが、2018 年 9 月時点で明白な証拠はない。
出典：Galante & Ee, Op. Cit., p.7 より抜粋、作成。

アジア各国の選挙への介入：台湾、香港、アフガニスタン

2000 年に行われた台湾総統選挙では、台湾国防部のコンピュータ専門家と、中国の「愛国的」活動家との戦いが繰り広げられたといわれている。「紅客」と呼ばれる中国のハッカー・グループが台湾のコンピュータ・ネットワークを混乱させ、選挙を妨害するのではと懸念された。台湾政府は選挙結果の集計ネットワークを完全に閉じたものにするという対策を講じた。そして、安全対策が不十分な中央選挙委員会のサイトとの接続を完全に遮断した[21]。しかし、中国が実際にどれだけ介入を行ったのかは分からない。中国政府は選挙結果が出る直前まで、独立派の陳水扁が当選したら黙ってはいないと露骨な介入を口にしていたにも関わらず、陳水扁がこの選挙で勝利すると、「その言動を見守る」とトーンダウンした[22]。

2000 年の台湾総統選挙は、1997 年に中国へ返還されていた香港の政治にも影響を与えることになった。独立派の陳水扁が台湾で勝ったことで、中国政府はその動きが香港に及ぶことを警戒し、中国政府高官は香港のジャーナリストに対し、「国の主権と統一性を守ること」は報道機関の義務であるとして、独立支持に関する報道をしないように警告した[23]。

2003 年には、香港で反体制活動を規制する「国家安全法」の導入をめぐり、50 万人

[21] メリンダ・リウ「サイバー戦争の危うい影」『NEWSWEEK』（2000 年 3 月 22 日）、17-19 頁。
[22] 酒井亨「台湾選挙を左右した米国の“介入”：冷戦終わらない東アジアの問題」『東亜』第 540 号（2012 年 6 月）、32-38 頁。
[23] フランク・チン「中国の介入にも黙り込む香港」『NEWSWEEK』（2007 年 7 月 11 日）、13 頁。

を超える人々が抗議デモに参加した。しかし、2004 年 4 月、中国の全国人民代表大会常務委員会は、2007 から 08 年の香港の選挙で直接選挙を認めないと決定し、さらに、香港基本法の解釈権を行使し、香港が完全な民主的選挙を行う時期を独自に決めることはできないと発表した[24]。

その 10 年後、2017 年香港特別行政区行政長官選挙における中国全国人民代表大会常務委員会の決議が、被選挙（指名権）の開放や立法会構成の改革を否決すると、抗議デモが発生し、雨傘運動と呼ばれるようになった。

2012 年の台湾総統選挙においては、米国の意向と圧力が大きく作用したともいう。原発は米国にとって大きな利権の手段となっており、脱原発の流れを進めていた蔡英文総統候補は選挙中にトーンダウンを迫られた。台湾にとって米国との良好な関係は対中政策にとって重要な柱になる。選挙直前には事実上の駐台湾米国大使（米国在台湾協会（AIT）台北事務所元所長）を勤めたダグラス・パール（Douglas Paal）が台湾を訪問し、投票の 2 日前、地元テレビ局のインタビューで「現職の馬［英九］総統が再選されれば米国と中国大陸は安心し、米対関係も安定緊密になる」、対立候補の蔡英文候補が当選した場合、「米国政府は直ちに台湾に中台関係の現状維持を促す」と発言し、台湾の野党陣営からは「米国の選挙介入ではないか」との反発の声が上がった[25]。

2009 年 8 月 20 日に行われたアフガニスタンの大統領選挙では、イスラム原理主義組織タリバンが投票妨害を行ったと自ら宣言した。タリバンは、確認されただけで投票所などに 76 件のテロ攻撃を行い、30 人近い犠牲者を出した。それだけでなく、現職および対抗馬の両陣営が不正行為を行い、地元当局者職権を濫用して投票箱を運び出し、偽の投票用紙を詰めるといったことも行われたようである。一部の州では、有権者数どころか、人口をも上回る数の有権者登録カードが発行され、それが売買されている可能性も指摘された[26]。そして、現職のハミド・カルザイ（Hāmid Karzai）陣営の重大な不正行為が発覚し、得票数の約 3 分の 1 が無効になった[27]。

翌 2010 年に行われたアフガニスタンの総選挙では、投票日までに候補者 4 人をはじめ 20 人以上が殺害された。タリバンの司令官は、指先に投票したことを示すインクが付いていれば切り落とすと有権者を脅した。独立選挙委員会は当初約 7,000 箇所の投票所を設置する予定だったが、治安上の理由で 1,000 箇所近くが閉鎖された。この選挙では登録有権者 1,250 万人に対し、約 1,750 万枚の有権者カードが配布され、不正投票の可能性が強く疑われた[28]。

---

[24] 前掲注参照。
[25] 酒井、前掲論文、および以下を参照。澁谷司「2012 年台湾ダブル選挙と台湾の未来：米国の選挙介入で大敗した民主進歩党」『海外事情』（2012 年 3 月）、91-113 頁。
[26] ロン・モロー、サミ・ユサフザイ「アフガン真の勝者は誰？」『NEWSWEEK』（2009 年 9 月 2 日）、24 頁。
[27] ロン・モロー、サミ・ユサフザイ「アフガン総選挙『民意』は届くか」『NEWSWEEK』（2010 年 9 月 29 日）、24-25 頁。
[28] 前掲注参照。

想定すべき選挙介入の具体的行為

本レポートは、ロシアによる 2016 年米大統領選挙介入およびその他の介入事例から、選挙介入の具体的行為として次のものを想定する。

候補者・政党等への攻撃・侵入

- 候補者・政党、その関係者にサイバー攻撃を仕掛け、機密情報を窃取する。

＜直近の選挙介入から＞

- 攻撃者は 2015 年 5 月、ドイツ議会（Bundestag）へのサイバー攻撃を行い、16 ギガバイト（GB）のメールや情報を窃取した。攻撃を受けた 10 数件のメールアカウントは、メルケル（Angela D. Merkel）首相の議会用アカウントを含む（メルケル首相の執務用アカウントは被害を受けず）[29]。
- 攻撃者は 2016 年 3 月、（技術的には）高度ではない手法で米民主党全国委員会（DNC）等のネットワークに侵入、大量の機密情報を窃取した。具体的には、クラウド型メールサービス（Gmail 等）のセキュリティアラートを模したスピアフィッシングメールを大量に送り付け、関係者の ID とパスワードを入手した。

機密情報の暴露

- 候補者・政党等から盗みだした機密情報を暴露する。

＜直近の選挙介入から＞

- 2016 年米大統領選挙に関連して、攻撃者は、架空のペルソナ（偽のハッカー Guccifer 2.0）や暴露サイト（DCLeaks）を構築し、情報を流出させた。また既存の暴露サイト（WikiLeaks 等）を通じて情報を流出させた。情報暴露は①選挙期間を通じて小出しに、②重要な政治イベントのタイミングで行われた。
- 2017 年フランス大統領選挙の決選投票日（5 月 7 日）の直前、5 月 5 日、テキスト共有サイト Pastebin に大量のファイルがアップされた。これはマクロン（Emmanuel Macron）大統領候補の選挙事務所から盗み出されたメール情報等であり、Twitter 上では#MacronLeaks のハッシュタグとともに情報が拡散し、6 日には WikiLeaks が情報（マクロン陣営から漏洩した数万通のメール、写真、添付ファイル 9GB の情報）を暴露した。

選挙インフラへの攻撃・改竄

- 各自治体の選挙委員会等にサイバー攻撃を仕掛け、ウェブサイトを改竄する、有権者情報を盗む。
- 投票・集計に関するシステムに攻撃を仕掛け、集計結果を改竄する、投票・開票・集計を妨害する。攻撃の成否は別として、攻撃の事実は集計結果改竄の疑念を生む。
- 選挙インフラに関するベンダーや運営委託先に攻撃を仕掛ける。

[29] 「焦点：選挙控えたドイツ、サイバー攻撃や偽ニュースに戦々恐々」『Reuters』（2017 年 5 月 15 日）

フェイク・コンテンツ流布

- 特定政策の実現・妨害、特定候補者の当落、特定主張の普及を目的に、偽のコンテンツを作成し[30]、流布する。フェイク・コンテンツは一般的に「フェイクニュース」とも呼ばれる（ただし「フェイクニュース」との用語・表現は不適切な場合もある。詳細は後述）。ニュース形式ではなく、政治広告の場合もある。

フェイク・コミュニケーション

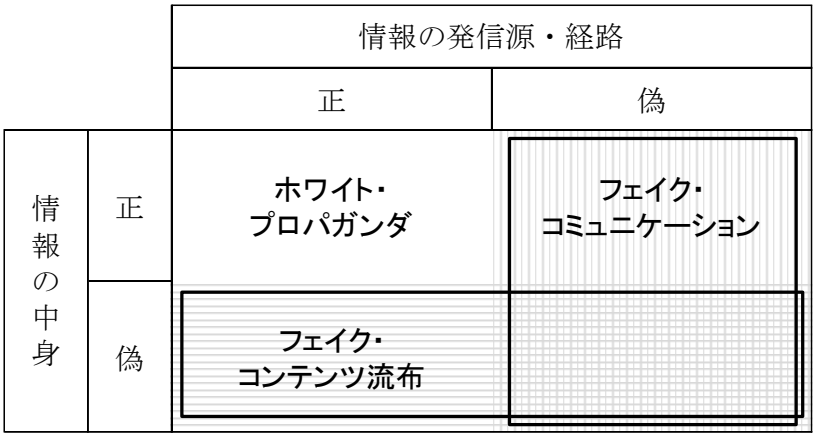
- 情報の発信源、経路、視聴者を偽装する。具体的には、
  - ✓ オンライン上で架空のアイデンティティの個人やグループの作成
  - ✓ 実際に存在する第三者（個人やグループ）のアインデンティティの偽装
  - ✓ 偽の SNS アカウントやウェブサイトの構築
  - ✓ トロールやボットを用いた SNS 上で架空の議論、架空のトレンド、架空のインフルエンサーの構築

ホワイト・プロパガンダ

- 情報発信源・媒体も事実関係も概ね妥当なものであるが、特定の政治目標のため、ある事実を強調・捨象したり、扇情的なヘッドラインやイメージを用いる。

なお「フェイク・コンテンツ流布」「フェイク・コミュニケーション」「ホワイト・プロパガンダ」の関係は、情報そのものと情報の発信源・経路の真贋で整理できる。これら媒体は、国営テレビ・ラジオ・通信社、機関紙、SNS 等多岐にわたる。

図１：情報の中身、発信源・経路の真偽性



出典：筆者作成。

[30] 機会学習等を利用した高性能の「ディープ・フェイク」も確認されている。Robert Chesney and Danielle K. Citron. “Disinformation on Steroids: The Thread if Deep Fakes,” Council on Foreign Relations (October 16, 2018).

情報セキュリティ、サイバーセキュリティとの関連

こうした選挙介入行為は、選挙や民主主義にとっての脅威であると同時に、情報セキュリティ、サイバーセキュリティ上での脅威でもある。情報セキュリティとは、「情報の C.I.A.を一定以上のレベルで維持すること」と定義される。

「C」とは Confidentiality（機密性）であり、機密情報等の漏洩がないことである。「I」とは Integrity（完全性）であり、情報やデータが正しい（間違っていない）ことである[31]。「A」とは Availability（可用性）であり、情報やシステムにアクセスできる（利用できる）ことを指す。サイバーセキュリティも同様の定義であり、サイバーセキュリティはサイバー空間上での情報の C.I.A.に焦点を当てている[32]。

前述の選挙介入行為を情報セキュリティ、サイバーセキュリティ上の位置づけを整理したのが表 8 である。「候補者・政党等への攻撃・侵入」「機密情報の暴露」は、対象から機密情報を窃取し、暴露するという意味では、機密性（C）に対する脅威といえる。

「選挙インフラへの攻撃・改竄」はあらゆる面で情報セキュリティ、サイバーセキュリティ上の脅威である。有権者登録情報を盗む攻撃は機密性（C）への脅威であるし、投票結果・集計結果や候補者ウェブサイトの改竄は完全性（I）への脅威であり、選挙関連システムを攻撃し投票妨害・集計妨害を行うことは可用性（A）への脅威である。「フェイク・コンテンツ流布」「フェイク・コミュニケーション」「ホワイト・プロパガンダ」はいずれも完全性（I）への脅威である。

表 8：想定すべき選挙介入行為と「情報の C.I.A.」との関連

選挙介入行為	脅かされる価値		
	機密性（C）	完全性（I）	可用性（A）
候補者・政党等への攻撃・侵入	✓		
機密情報の暴露	✓		
選挙インフラへの攻撃・改竄	✓	✓	✓
フェイク・コンテンツ流布		✓	
フェイク・コミュニケーション		✓	
ホワイト・プロパガンダ		✓	

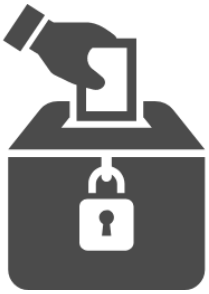
出典：筆者作成。

[31] ただし、米国の選挙法の「完全性」は、情報セキュリティでいう「完全性」とは若干異なる含意があるため、注意が必要である。湯浅墾道「選挙におけるインターネット利用：セキュリティに係る論点」総務省第 2 回　投票環境の向上方策等に関する研究会　資料 4（2018 年 1 月 23 日）［初出：湯淺墾道「アメリカにおける選挙権の観念の一断面：integrity を手がかりに」『青山法学論集』第 56 巻、第 4 号（2015 年 3 月）、71-99 頁］。

[32] 日本のサイバーセキュリティ基本法第 2 条が定義する「サイバーセキュリティ」の定義もほぼ同様である。詳細は筆者執筆の「サイバーセキュリティ」、ChannelJ 運営情報サービス「安全保障用語」解説・コラム（2018 年 10 月 12 日）【http://dictionary.channelj.co.jp/2018/18101201/】を参照。

2. 日本の文脈

過去、日本国内においても（外国政府によるものではないが）選挙妨害が確認された。今日、外国政府が日本の選挙に介入する際、攻撃者は日本固有の政治制度（多党制と議院内閣制）、日本で検討されている選挙過程の電子化・インターネット利活用、日本国内で利用されているニュースサービスや SNS を分析した上で、活動を行うだろう。



（1）日本国内での過去の選挙妨害

- 日本国内においても、過去、違法な選挙妨害が確認された（ただし、外国政府によるものではない）。日本の選挙においても、妨害・介入は珍しいものではない。
- 過去の選挙妨害は特定の選挙区における直接的な妨害、情報（言葉）による妨害であり、特定候補者の当落を狙ったものであった。

日本国内においても、過去、選挙妨害が確認された。ただし、外国政府によるものではない（それゆえ、本節では選挙「介入」ではなく、単に選挙「妨害」と表現する）。日本の選挙においても、妨害・介入は珍しいものではない。

日本における直接的な選挙妨害の事例

一般的に選挙不正という場合、投票箱のすり替え、集計操作、選挙人リストの改変、票の買収、選挙人登録の妨害、候補者登録の妨害、選挙人脅迫、候補者脅迫、複数回投票、幽霊投票などが考えられる[33]。

選挙介入・妨害の事例は、民主主義の歴史と同じくらい長い。日本においても様々な事件が起きている。1892（明治 25）年の第 2 回総選挙においては、死者 25 名、負傷者 388 名を出す大選挙干渉事件が起きた[34]。

第二次世界大戦後は死者が出るような事件は起きていないが、それでも数多くの選挙介入・妨害事件が起きた。1948 年、滋賀県の彦根市長選挙において、民主党の立候補者が、対立する自由党の立候補者の政見発表演説会に酒気を帯びたまま赴き、会場入り口の土間において大声で自由党候補者を罵り、制止しようとした者に対して暴力を振るい、演説を妨害した。この行為に対し、地方自治法附則第 12 条、市制第 73 条の 16、第 40 条により（衆議院議員の選挙に関する罰則が準用されるとの規定）衆議院議員選挙法第 115 条が適用され、有罪となった（公職選挙法の成立は 1950 年）[35]。

近年の選挙妨害の有名な事例としては、1992 年の奈良県下市町長選挙の事例がある。この選挙に際し、選挙長が立候補届出受理業務を開始したところ、届出に来たという人物が戸籍抄本等の確認作業を選挙長に断念させ、受付順位決定のためのくじの方法を執拗に要求した上になかなかくじを引こうとせず、怒号をあげるなどして業務を遅延させた。また同一人物が 1993 年の衆議院議員選挙における立候補と届出業務に際し、確認

---

33 大西裕編著『選挙ガバナンスの実態　世界編：その多様性と「民主主義の質」への影響』（ミネルヴァ書房、2017 年）、16 頁。
また、選挙が十分に機能しない場合、民主主義への影響としては以下の四つが考えられる。（1）有権者の代表の客観的な質の低下、（2）有権者の議会に対する信頼の喪失、（3）少数派による選挙以外の手段を通じての自身の利益実現、（4）暴動などを通じた民主主義体制への否定である。大西、前掲書、19 頁。
34 季武嘉也『選挙違反の歴史：ウラからみた日本の 100 年』（吉川弘文館、2007 年）、60-61 頁。
35 松本米治「衆議院議員選挙法第 115 条第 2 号にいわゆる『演説妨害』の意義」『法と経済』第 112 号、1950 年 8 月、42-47 頁。

作業を困難にし、怒号した上、所持していたボールペンを机上にたたきつけるなどして業務を遅延させた。選挙長の業務は公職選挙法上の業務と認定され、被告人は業務妨害罪（刑法第 233 条および 234 条）で有罪となった[36]。

2001 年の新潟県岩船郡粟島浦村長選挙においては、立候補予定者が選挙の告示日に、立候補届に必要な戸籍抄本の交付を村役場に申請したが、当日が休日であったため交付を受けられず、やむなく立候補を断念するという事例があった。これだけならば至極当然に思えるが、その背景として、村では戸籍抄本を交付する方向で検討する意見があったものの、現職の村長が戸籍抄本発行のために必要な村の公印を村長室に引き上げさせ、総務課長に対し「戸籍抄本を交付した場合には懲戒免職にする」という趣旨の発言をしたということがあった。その結果、現職の村長が無投票で再選を果たすことになった。裁判によって、他の立候補予定者の立候補を妨害して自ら無投票当選を果たした行為は公職選挙法第 205 条 1 項に違反するとされた[37]。

その他、主として野党の立場から、警察による選挙妨害が行われているという主張もある[38]。

こうした直接的な選挙妨害は物理的に可視化されているため、選挙妨害それ自体の事実と選挙妨害の実行者は直ちに周知されることが多い。しかし、現代の選挙妨害（有権者登録データベースを攻撃・改竄する、投票所での本人確認を妨害する、投開票・電子投開票を妨害する等）はインターネット経由であることから、攻撃者を直ちに特定できない。それればかりか、妨害の原因すら分からないかもしれない。

---

36 増田啓祐「実務刑事判例評釈（75）公職選挙法上の選挙長の立候補届出受理事務が業務妨害罪にいう「業務」に当たるとされた事例」『警察公論』第 55 巻 10 号、2000 年 10 月、89-95 頁。長谷川充弘「判例研究 公職選挙法上の選挙長の立候補届出受理事務が業務妨害罪の「業務」に当たるとされた事例」『研修』第 628 号、2000 年 10 月、11-32 頁。朝山芳史「公職選挙法上の選挙長の立候補届出受理事務と業務妨害罪にいう『業務』」『法曹時報』第 53 巻 11 号、2001 年 11 月、3314-3341 頁。林弘正「公職選挙法上の選挙長の立候補届出受理事務と業務妨害罪にいう『業務』」『現代刑事法』第 3 巻 5 号、2001 年 5 月、75-79 頁。

37 野中俊彦「村長選挙において現職の村長が他の立候補予定者の立候補を妨害して自ら無投票当選を果たした行為が公職選挙法 205 条 1 項にいう選挙の規定の違反に当たるとされた事例」『民商法雑誌』第 128 巻 2 号、2003 年 5 月、210-220 頁。東京大学判例研究会「最高裁判所民事判例研究（民集 56 巻 6 号）（26）村長選挙において現職の村長が他の立候補予定者の立候補を妨害して自ら無投票当選を果たした行為が公職選挙法にいう選挙の規定の違反に当たるとされた事例」『法学協会雑誌』第 122 巻 3 号、2005 年、397-415 頁。阪本勝「村長選挙において現職の村長が他の立候補予定者の立候補を妨害して自ら無投票当選を果たした行為が公職選挙法 205 条 1 項にいう選挙の規定の違反に当たるとされた事例」『法曹時報』第 56 巻 12 号、2004 年 12 月、2917-2935 頁。鶴恒介「村長選挙において現職の村長が他の立候補予定者の立候補を妨害して無投票当選を果たした行為が公職選挙法 205 条 1 項にいう選挙の規定の違反にあたるとされた事例」『自治研究』第 81 巻 2 号、2005 年 2 月、121-130 頁。

38 例えば、以下を参照。「日本共産党への不当な選挙干渉、妨害をただちに中止させよ」『前衛』第 497 号、1983 年 9 月、258-259 頁。岡田淳「住民の政治参加を攪乱・妨害：坂出市川津町選挙弾圧事件」『法と民主主義』第 221 号、1987 年 10 月、21-24 頁。服部融憲「公職選挙法による選挙過程妨害事件」『国際人権』第 15 号、2004 年、94-97 頁。「共謀罪の先取り、選挙妨害か 沖縄・多良間村議会選の候補者を県警が尾行」『週刊金曜日』第 25 巻 22 号、2017 年 6 月 9 日、16 頁。

日本における情報を使った選挙妨害の事例

情報による選挙妨害としては、東京都港区白金台にあった料亭・般若苑（はんにゃえん）をめぐって起きた騒動についての判決が 1969 年に出ている。訴えたのは元外務大臣の有田八郎とその妻である畔上（有田）輝井である。有田が 1959 年の東京都知事選挙に立候補した際、有田と、般若苑の経営者であり、有田と 1952 年に結婚（有田は再婚）した輝井との間の恋愛などについて記述した『般若苑マダム物語』と題する小冊子 10 万部が発売配布された[39]。著者は「和田ゆたか」となっていたが、逮捕された実際の著者は著述業の渡辺剛であった。出版元とされた太陽出版社も実在しない出版社であった（なお、有田と輝井は選挙後の 1960 年に離婚している）。

渡辺は、名誉毀損と選挙の自由妨害罪（公職選挙法第 225 条）に問われた。第一審判決では無罪になったが、1967 年の第二審では、「当該候補者を投票の対象として考慮する余地がないと判断させるおそれがあるものを、不特定多数の選挙人に対して大規模に頒布し、社会通念上、いわゆる『言葉の暴力』というべき行動が行なわれたとみられるような事態を発生させたと認められる場合には、これを質的にみれば、交通や集会の便を妨げたり、演説を妨害する行為に匹敵する程度の行為があったと解するのが相当である」として有罪となった[40]。

ところが、1969 年、最高裁は、名誉毀損だけを認定し、選挙の自由妨害については認定しなかった。裁判長は「公選法に規定された偽計詐術等による選挙の自由妨害というのは、これらを用いて選挙運動や投票を直接妨害する行為をいい、たんに候補者に対する有権者の判断の自由を妨げるような行為はこれに当らない」と述べた[41]。この最高裁の判決は、いわゆる怪文書の頒布だけをもって選挙の自由妨害には当たらないとした点で、それ以後の様々な事件の司法判断に影響を与えていくことになった。

この判決によって、選挙につきものの怪文書配布については、選挙の自由妨害（公職選挙法第 225 条）よりも当時の罰則としては軽かった「虚偽事項の公表」（公職選挙法第 235 条）が適用されるにとどまることになった[42]。

1960 年代後半の日本においては、一般の人々がインターネットを使える状況ではなく、この事件は小冊子による選挙の自由妨害が争われたが、二審において有罪とした理

---

39 和田ゆたか『割烹料亭般若苑マダム物語：元外務大臣有田八郎氏夫人』太陽出版社、1958 年。

40 出射義夫「誹謗文書の配布と選挙自由妨害罪の成否」『警察研究』第 44 巻第 4 号、1973 年 4 月、87-93 頁。福田平「選挙の自由妨害と名誉毀損：いわゆる盤若苑マダム物語事件をめぐって」『法律のひろば』第 22 巻 4 号、1969 年 4 月、34-38 頁。なお、この事件は、三島由紀夫の『宴のあと』（新潮社、1960 年）のモデルになっており、日本で最初のプライバシーの侵害についての裁判になっている。この事件以前に誹謗文書の配布に対して公職選挙法第 225 条が適用され、地裁レベルで有罪とされた事例もある。以下を参照。加賀収「誹謗文書の頒布と選挙の自由妨害罪：『般若苑マダム物語』事件控訴審判決を中心として」『警察学論集』第 21 巻 5 号、1968 年 5 月、36-46 頁。

41 「名誉毀損だけ有罪 『般若苑マダム物語』の渡辺　公選法違反成立せず」『朝日新聞』1969 年 2 月 6 日。

42 当時の罰則は、225 条が 4 年以下の懲役若しくは禁錮又は 7 万 5000 円以下の罰金で、235 条は 2 年以下の懲役若しくは禁錮又は 2 万 5000 円以下の罰金となっていた。「選挙“怪文書”に新判断　般若苑事件で最高裁　自由妨害にならぬ」『読売新聞』1969 年 2 月 6 日。ただし、現在では、225 条が 4 年以下の懲役若しくは禁錮又は 100 万円以下の罰金で、235 条も 4 年以下の懲役若しくは禁錮又は 100 万円以下の罰金となって、量刑は同じになっている。

由については、インターネット時代ではもっと容易に適用されるだろう。この事件当時からいわゆる「怪文書」が問題となっていたが、現在でもこうした文書は頻繁に頒布されている。しかし、最高裁が単に怪文書を頒布しただけでは選挙の自由妨害ならないとしたならば、現在のインターネット上にたくさん出ている誹謗中傷に近い怪文書やフェイクニュースも、それだけでは選挙の自由妨害としにくいということになる。

1972 年 10 月に最高裁は、1967 年の愛媛県知事選挙において配布された文書が、選挙管理委員会に届け出ていない文書（法定外文書）にあたると判断した。この選挙においては、保守系の候補と革新系の候補による一騎打ちの選挙戦が行われたが、保守系候補者の運動者が投票日の前日、「県民の皆様いよいよ明日は我々の手で県庁の日の丸をおろし高々と赤旗を立てる日です。また一日も早く愛媛の教育を改め、中国（紅衛兵）のような青少年をつくりましょう　一月二六日投票の日県民各位へ」と記載した文書を松山市内の該当数十カ所において配布した。この文書は、文字通りの内容を求めるものではなく、革新系の候補の当選妨害を狙ったものである。判決では、被告人らはこのような文書を頒布することによって直接的には革新系候補の人気を下落させ、その反面的効果として自分らの推薦する保守系候補の当選を得ようと企図したものとされた[43]。

この事件は、現在のフェイクニュースの頒布に相当する事案であるといえよう。革新系候補が、中国の文化大革命で悪名を馳せていた紅衛兵のような若者を育成しようと考えていたとは考えにくい。しかし、そうした印象を有権者に与えることで、反対候補を当選させようとしている。

般若苑の事件では、ペンネームによるものだとしても、一応は表現の自由で守られる著作物としての第三者執筆の書籍が使われた。無論、書籍の内容に明らかな誹謗中傷があれば名誉毀損の罪に問われることになる。しかし、愛媛県知事選挙における事件では、配布された文書が、第三者ではなく、選挙運動の運動員によって配布されたものであり、選挙管理委員会に届け出るべきものかどうかが問われた。この二つの事件の差を見れば、運動員によるものかどうかが重要な分かれ目となるといえるかもしれない。

現在のインターネットにおける怪文書や誹謗中傷文書、そして掲示板における書き込み、商品等のレビューにおいては、書き手の身分が明らかにされないことが多く、匿名性の影に隠れたままになっている。そうした情報が全く選挙結果に影響しないわけではないだろう。この問題は、インターネットが登場する前も後も共通してあるものだが、その深刻度はインターネットによって増したといえるだろう。

[43] 吉田淳一「選挙妨害的文書が法定外文書にあたるとされた事例」『警察学論集』第 26 巻 10 号、1973 年 10 月、190-194 頁。

(2) 政治制度：多党制・議院内閣制下の選挙介入

- □ 選挙介入を行う攻撃者にとって、多党制よりも二大政党制、議会選挙よりも国家元首選挙の方が介入の「コストパフォーマンス」が高い。
- □ 日本の多党制・議院内閣制は介入の「コストパフォーマンス」が相対的に低いものの、同じく多党制・議院内閣制を採用するドイツでも 2017 年 9 月の議会選挙で介入が確認された。日本でも、議会選挙、特に単一の争点を中心に社会分断を狙った介入が行われる可能性がある。
- □ 通常の国政選挙とは異なり、憲法改正に関わる国民投票は、有権者の賛否を二分しやすく、政策への影響も大きいため、特別な注視が必要である。

選挙制度と政党制度

選挙介入を行う攻撃者にとって、多党制よりも二大政党制、議会選挙よりも国家元首選挙の方が介入の「コストパフォーマンス」が高い。多党制よりも二大政党制の方が、政治争点が二極化しやすく、介入によって社会分断は生じやすい。また、議会選挙よりも国家元首を選出する選挙の方が選挙介入の影響・効果を最大化できる。

日本が採用する多党制・議院内閣制は、「選挙介入」のコストパフォーマンスが相対的に低いものの、同じく多党制・議院内閣制を採用するドイツでも 2017 年 9 月の連邦議会選挙で介入が確認された。日本でも、議会選挙、特に単一の争点を中心に社会分断を狙った介入が行われる可能性がある。2017 年ドイツ議会選挙への介入から、日本への示唆を考察する。

表 9：選挙制度と政党制度

選挙制度＼政党制	二大政党制	多党制
議会選挙	□ 2017 年米国中間選挙	□ 2017 年ドイツ連邦議会選挙 □ 日本の国政選挙
国家元首選挙	□ 2016 年米国大統領選挙	□ 2014 年ウクライナ大統領選挙[注1] □ 2017 年フランス大統領選挙[注2]
特定争点の国民投票	□ 2016 年英国の EU 離脱（BREXIT）を問う国民投票 □ 日本の憲法改正に関わる国民投票	

注 1　無所属のポロシェンコ（Petro Poroshenko）優位の中で、他 2 人の候補がポロシェンコを追う情勢。

注 2　第 1 回投票では、共和国前進のマクロン（Emmanuel Macron）、国民戦線のル・ペン（Marine Le Pen）、共和党のフィヨン（François Fillon）、不服従のフランスのメランション（Jean-Luc Mēlenchon）の 4 候補が拮抗。

出典：筆者作成。

2017 年ドイツ連邦議会選挙への介入

ドイツでは 2017 年 9 月 24 日、第 19 期連邦議会選挙が実施され、「ドイツのための選択肢（the Alternative für Deutschland: AfD）」が大きく躍進した[44]。こうした選挙結果と選挙介入の因果関係は明らかではないが、**ロシアによる選挙介入は AfD 躍進を狙ったもの**であると推察されている。

2017 年ドイツ連邦議会選挙に関連して、ロシアからのサイバー攻撃と影響工作として以下のものが確認された。

- 「APT28」「Fancy Bear」と呼ばれるサイバー攻撃グループが、2015 年 5 月、議会（Bundestag）へのサイバー攻撃を行い、16GB のメールや情報を窃取した。攻撃を受けた 10 数件のメールアカウントは、メルケル首相の議会用アカウントを含む（メルケル首相の執務用アカウントは被害を受けず）[45]。
- 「APT28」「Fancy Bear」と呼ばれるサイバー攻撃グループが 2016 年 4 月、キリスト教民主同盟（CDU）の幹部に対してフィッシング攻撃を行った。
- 選挙期間中、ドイツ語のロシア系メディアが反移民政策[46]の主張を展開した[47]。ドイツ語のロシア系メディアは、AfD に対してポジティブで、その他の政党・政治機構にはネガティブな傾向があった[48]。
- 選挙期間中、ドイツ語のロシア系メディアと AfD は「Our Lisa」物語を流布した[49]。「Our Lisa」物語とは、アラブ系イスラム教徒の移民らが、13 歳のロシア系ドイツ人の少女 Lisa を誘拐し、暴行したと報じられたもので、後に捏造された情報と判明した。メルケル首相の報道官がオバマ政権の報道官ローズ（Benjamin Rhodes）に対して語ったところによれば、ドイツ政府は調査の結果、この捏造された情報は最終的に「ロシア人」によるものとの判断を下した[50]。

2017 年の議会選挙に関する SNS 上での広範な活動については、ミュンヘン工科大学の研究者らが詳細を分析している。研究者らは、ドイツ連邦議会選挙に関する①約 3 億 5,300 万件のツイート、②約 3 万 7,000 件の Facebook 上のコンテンツ、③ツイッター上で言及された約 182 万の URL を分析した上で次の結論を下した。

---

44 AfD 躍進の背景には難民問題と欧州統合があったと指摘されている。この点については、中村登志哉「2017 年ドイツ連邦選挙における『ドイツのための選択肢』議会進出の分析：難民危機と欧州統合との関連を中心に」『グローバル・ガバナンス』第 4 号（2018 年 3 月）、42-54 頁。

45 「焦点：選挙控えたドイツ、サイバー攻撃や偽ニュースに戦々恐々」『Reuters』（2017 年 5 月 15 日）

46 メルケル首相が難民受入を表明していたことから、情報工作はメルケル首相以下の政権与党に対する反対キャンペーンと推察される。2017 年ドイツの総選挙前の政権与党はキリスト教民主・社会同盟（CDU/CSU）およびドイツ社会民主党（SPD）による大連立であり、介入は既存の大連立与党に対する反対キャンペーンともいえる。

47 Laura Galante & Shaun Ee, “Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents,” Issue Brief, Atlantic Council (September 2018), pp.12-13;

48 Juan Carlos Medina Serrano, et. al., *Social Media Report: The 2017 German Federal Elections*, Political Data Science (Technical University of Munich Press, 2018), pp.27.

49 Galante & Ee, *Op. Cit*.; Simon Shuster, “How Russian Voters Fueled the Rise of Germany's Far-Right,” *Time* (September 25, 2017).

50 Benjamin Rhodes, *The World as It Is: A Memoir of the Obama White House* (New York: Random House, 2018), p.606.

- Twitter および Facebook は、AfD 関連の情報であふれていた。これは、AfD の躍進に寄与した可能性がある。
- Twitter 上には、ドイツの選挙プロセスを狙ったオンラインでの改竄メカニズム（online manipulation mechanisms）が存在した。それにもかかわらず、観察された活動量は専門家が期待していたものよりも少なかった。検出されたボット、フェイクニュース、外国による介入技術がドイツ国民に与えた影響を測定することは難しい。しかし、ボットは AfD に好意的に振舞っていた。
- ドイツ国民は米国民よりも、オンライン上の改竄の影響を受けなかった。ドイツの左右両極のメディアは主流メディアに近く、異なる政党を支持する市民であっても、検証された情報を受け取った。また誤情報は選挙に関する議論で主要な役割を果たさなかった。Facebook と Twitter で最もシェアされたニュースは、誤解を招くようなストーリーは少なく、完全な偽情報はなかった。ただし移民に関するニュースはミスリードな事実を含んでいた。
- ドイツの政治機構は、ソーシャルメディアプラットフォーム上でも正しく表現されていた。またオンラインメディアのオーディエンスは（特定の支持政党を持つオーディエンスではなく）異なる政治的視点を持つオーディエンスであった[51]。

上記の結論は外国政府と関係のない SNS 上の活動を含んでいるが、ミュンヘン工科大の研究者らは Twitter 上での「オンライン改竄」と外国政府、つまりロシアとの関係についても検証した[52]。

- ロシアのトロールと思われるアカウントは、「RT（Russia Today）」や「スプートニク」ではなく、ドイツの一般的なメディアを引用し、メッセージを増幅していた。これは「ブライトバード（Breitbart）」や「ゲートウェイ・パンディット（The Gateway Pundit）」といった極右サイトを参照していた 2016 年米大統領選挙時のトロールの活動とは異なる[53]。
- ドイツ国内における主要なロシアのメディアである RT とスプートニクとドイツの主要なメディアである「ディ・ヴェルト（die Welt）」と「シュピーゲル（Spiegel）」の Twitter 上でのリツイート数を比較したところ、前者は後者の 3 分の 1 に達した。これは、ロシア系メディアが Twitter 上で大きな影響力を持つことを意味する。そして前述のとおり、ドイツ語のロシア系メディアは、AfD に対してポジティブで、その他の政党・政治機構にはネガティブな傾向があった。

[51] Serrano, *Op. Cit*., pp.53-54.
[52] Serrano, *Op. Cit*., pp.24-29.
[53] Serrano, *Op. Cit.*, pp.25.

日本への示唆

一般論として、多党制・議院内閣制は大統領制・二大政党制と比較して、選挙介入の効果を発揮しにくいと考えられるが、ドイツと同様に、日本でも議会選挙を狙った介入が行われる可能性がある。

2017 年ドイツ連邦議会選挙から、以下の点が示唆される。

1. 攻撃者は、ドイツ**政界に対する機密情報の窃取**（ただし、結果的に暴露されることはなかった）を行った。
   → 政治家・政党へのサイバー攻撃（機密情報の窃取とその暴露）は選挙制度・政党制度に関わらず有益な介入手法である可能性がある。

2. 首長選挙や二大政党制ではなくとも、**単一争点を切り口とした世論分断・影響工作**は効果を発揮する場合がある。ドイツでは移民問題が争点であり、反移民政策を掲げる AfD に対して好意的な影響工作が確認された。
   → 多党制であっても、与野党の対立が先鋭化する場合（自公の選挙協力、野党の統一候補化等）、争点領域は二極化されやすくなり、選挙介入の素地となるだろう。また通常の国政選挙とは異なり、憲法改正に関わる国民投票は、有権者の賛否を二分しやすく、政策への影響も大きいため、特別な注視が必要である。特に、憲法 9 条に係る改憲は、諸外国にとって高い関心があるテーマであるといえる。

3. 攻撃者は Twitter 上のトロールやロシア系メディアを通じて、**AfD に対して親和的なメッセージ**をオンライン上で発信した。ただし、その方法は 2016 年米大統領選挙とは異なり、**ドイツのメディア環境**に応じたものであった。ドイツ版「ブライトバード」「ゲートウェイ・パンディット」がなくとも、影響工作は可能である。
   → SNS 上の影響工作については、日本のメディア環境や攻撃者が支援するであろう政党・候補者を考察することが必要である。

（3）選挙過程の電子化・インターネット利活用

- □ 日本の選挙過程では、電子化・インターネット利活用が検討されている。投開票については、一部自治体では電子投票が実施され、国政レベルにおいても在外邦人を念頭としたインターネット投票を導入予定である。
- □ 従来から指摘された投票・集計結果の改竄の可能性は高いとは言えないが、投票・集計結果への攻撃自体が（仮に攻撃・改竄が成功しなかったとしても）選挙の正統性や投開票の信頼性を揺るがしかねないリスクである。
- □ 投開票以外の選挙管理要素については、情報の改竄、窃取等のリスクが懸念される。

日本の選挙過程の各要素においても、電子化・インターネット利活用が検討されているが、それぞれに一定のリスクが存在する（表 10 を参照）。

投開票については、一部の地方公共団体の議会・首長選挙で 2002 年より電磁的記録式投票（電子投票）が実施され、現在では 10 団体で 25 回実施されている[54]。また、国政レベルにおいても在外邦人を念頭としたインターネット投票を導入予定である[55]。最終的には、エストニアのように全国民に対してインターネット投票が開放されていく可能性もある。

投開票の電子化・インターネット利活用で懸念されるのが、投票・集計結果の改竄である。しかし、サイバー攻撃による**投票結果・集計結果の改竄の可能性は完全には排除されないものの、一般にその可能性は低い**と評価されている。

- 2016 年米大統領選挙期間中、選挙システムの脆弱性については、国土安全保障省のジョンソン（Jeh Johnson）長官が調査を行い、最終的には「不可能ではないが、可能性は低い」との結論に達した。ただし、投票システムへの攻撃はオバマ（Barack H. Obama）大統領の懸案事項であった[56]。
- ブルッキングス研究所のドイツ人研究者シュテルツミュラー（Constanze Stelzenmüller）は、米上院で「ドイツで用いられている投票技術へのハッキングの可能性は完全に排除できない。しかし、専門家らはまず成功しないと評価する。ターゲットしては有権者の頭の中の方がはるかに脆弱である」と証言する[57]。

---

[54] 総務省「電子投票の実施状況」（平成 28 年 1 月現在）
http://www.soumu.go.jp/senkyo/senkyo_s/news/touhyou/denjiteki/denjiteki03.html

[55] 総務省は、海外に在住する日本人向け在外投票を念頭に、インターネット投票導入に向けた実証実験（2019 年度）、公職選挙法改正を目指す（2020 年度以降）としている。なお、2016 年大統領選挙や 2018 年中間選挙で問題が指摘された米国では「インターネット投票」ではなく「電子投票」が主流である。これは、投票所における有権者の投票、投票所における開票、結果の送付、集計を電子化するものである。

[56] Michael Isikoff & David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump* (New York: Twelve, 2018) , pp.312-315; David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Scribe, 2018), pp.221-222

[57] Constanze Stelzenmüller, “The Impact of Russian Interference on Germany's Elections,” Testimony before the U.S. Senate Select Committee on Intelligence (June 28, 2017).

・ 選挙とセキュリティの専門家である情報セキュリティ大学院大学の湯淺墾道教授は、投票結果の改竄については従来から指摘されていたものの実現性は乏しい、と指摘する。湯淺教授によれば、改竄が行われ場合、集計結果で不整合が生じる等の問題が発生し、改竄が明らかになる可能性が高い[58]。

ただし、**投開票結果に対する攻撃・改竄は仮にそれが成功しないとしても、選挙の正統性・投開票の信頼性を揺るがしかねないリスク**である。2016 年米大統領選挙では、こうしたリスクがあったからこそ、オバマ政権はロシアに対する制裁措置を講じることができなかったとの見方がある（詳細は別紙 1 参照）。

投開票以外の選挙管理要素については、情報の改竄、窃取等のリスクが懸念される。選挙管理委員会が示す候補者ウェブサイトのリンクの改竄、候補者のウェブサイトの改竄といった比較的単純な攻撃から、電子的またはインターネットを通じた投票・集計作業の妨害といった攻撃が懸念される。

表 10：選挙管理の構成要素と電子化・インターネット利活用の動き

分類	電子化・インターネット利活用の動き	選挙介入のリスク
選挙運動	・ インターネットを利用した選挙運動（電子メール、ウェブページ、SNS 等）	・ 候補者や政党を語る偽の電子メール送信、ウェブサイトページでの宣伝、SNS 上での情報発信
選挙運動に係る選挙管理事務	・ 選挙管理委員会ウェブページ上での案内 ・ 選挙公報のインターネット上での提供	・ 選挙管理委員会ウェブページ上の情報の改竄
有権者登録	・ 選挙人名簿の電子ファイル化	・ 選挙人名簿の窃取、改竄、破壊による投票妨害
投票に係る諸選挙管理事務	・ 選挙人名簿との照合	・ 選挙人名簿の窃取、改竄、破壊による投票妨害
投票、投票記録の送付	・ 電子投票 ・ インターネット投票	・ 電子投票の記録・送付時の不正アクセス ・ 偽のインターネット投票用ページ（フィッシング等） ・ その他投票妨害
開票	・ 電子開票・集計 ・ 開票結果の選挙管理委員ウェブページでの公表	・ 開票結果・集計結果の改竄 ・ 公表結果の改竄

出典： 湯淺墾道「選挙とサイバーセキュリティ（2）」『月刊 選挙』第 71 巻、第 2 号（2018 年 2 月）、16 頁より作成（一部修正）。リスク欄は新たに追加。

[58] 情報セキュリティ大学院大学・湯淺墾道教授へのヒアリング（2018 年 12 月 4 日）より。

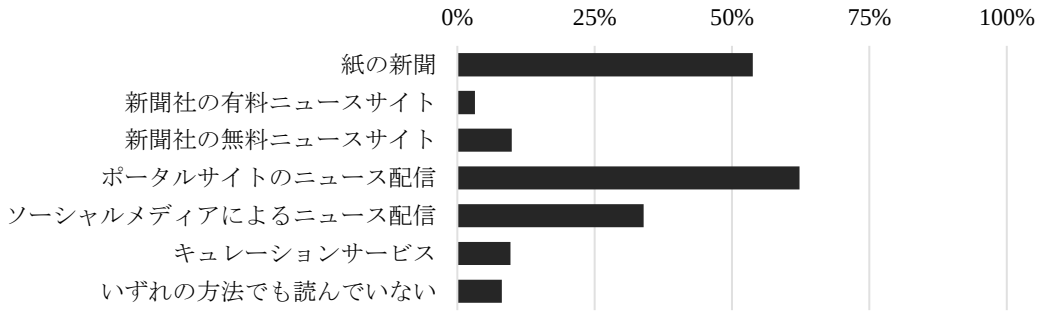
（4）SNS 等の利用状況とプラットフォーマーの対策

- 有権者の「意思決定」への攻撃としては、SNS やインターネット上での影響工作が懸念される。
- 日本国内のオンライン上のニュースサービスでは、ポータルサイトによるニュース配信（Yahoo!ニュース等）、ソーシャルメディアによるニュース配信の利用率が高い。ソーシャルメディア系サービス・アプリの利用率も年代が若いほど上昇傾向にある。利用率が高いということは、SNS やインターネット上での影響工作を受ける曝露量（exposure）が高いということである。
- Facebook 社や Twitter 社は、2016 年米大統領選挙や 2018 年米中間選挙の経験を経て、選挙介入対策を講じており、日本国内で事業を展開するプラットフォーマーでも同程度かそれ以上の対策が期待される。

日本国内のテキスト系ニュースサービスおよび SNS の利用状況

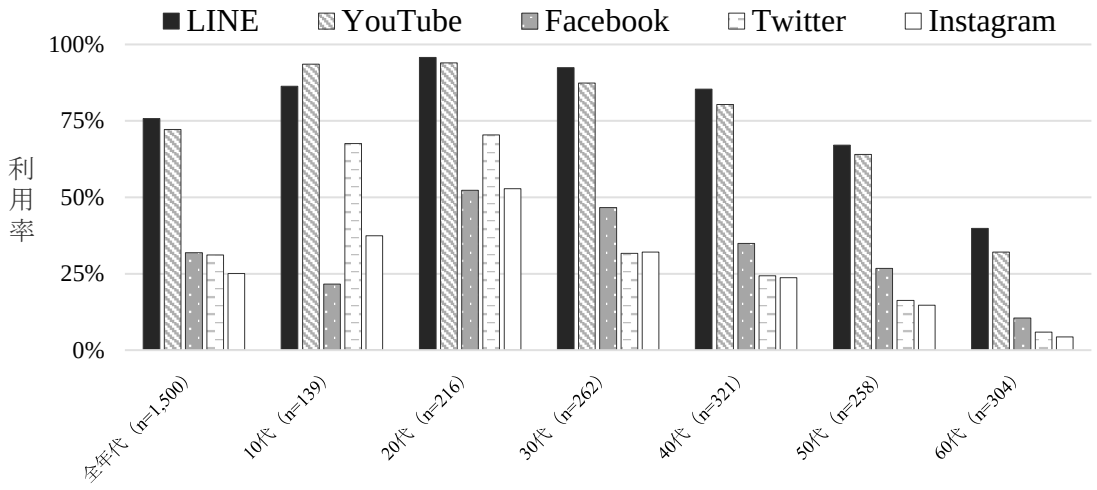
総務省の調査によれば、日本国内のテキスト系ニュースサービスの利用状況は、2017 年時点で、「Yahoo!ニュース」に代表される「ポータルサイトのニュース配信」の利用率（約 62%）が「紙の新聞」の利用率（約 54%）を上回った（図 2）。こうしたポータルサイトは新聞社・通信社・雑誌から配信されるニュースや情報を再配信するだけではなく、ポータルサイトのみに提供される情報も少なくない。ポータルサイトによっては、①ニュース記事に対するコメント機能、②ニュース記事に対する賛意・反意投稿機能、③コメント機能に対する賛意・反意投稿機能があることから、特定のニュース記事に対する注目が高まることもある。

図 2：利用しているテキスト系ニュースサービス



出典：総務省情報通信政策研究所「平成 29 年　情報通信メディアの利用時間と情報行動に関する調査」（2018 年 7 月）、71 頁。

図 3：主なソーシャルメディア系サービス・アプリの利用率



出典：総務省情報通信政策研究所「平成 29 年　情報通信メディアの利用時間と情報行動に関する調査」（2018 年年 7 月）、67 頁。

「ポータルサイトのニュース配信」に次いで、「ソーシャルメディアによるニュース配信」の利用率（約 34%）も高く、SNS もまた選挙介入の媒体として有益であることが示唆される。日本国内で用いられる SNS としては LINE、YouTube、Facebook、Twitter、Instagram の順で利用率が高い。SNS の利用率については年代別で顕著な違いが確認できる。諸外国とは異なり、LINE の利用率の高さは日本固有の事情ともいえる。なお、諸外国で利用率の高い WhatsApp、Telegram、WeChat については、SNS 上での偽情報活動が確認されている[59]。

オンライン上のテキスト系ニュースサービスや SNS の利用率が高いということは、それだけインターネット上での影響工作を受ける曝露量（exposure）が高いということである。改竄や偽情報流布のリスクは、公式ニュースサイト等を再配信するポータルサイトよりも、SNS の方が高いだろう。

Facebook 社や Twitter 社は、2016 年米大統領選挙や 2018 年米中間選挙の経験を経て、選挙介入対策を講じており、日本国内で事業を展開するプラットフォーマーでも同程度かそれ以上の対策が期待される（Facebook 社および Twitter 社による選挙介入対策は次頁以降のとおり）。

[59] 選挙に限定されないが、2017 年、全世界 48 か国で組織的なソーシャルメディア改竄活動（formally organized social media manipulation campaigns）が確認され、その内 5 か国では WhatsApp、Telegram、WeChat 等のアプリケーションでの偽情報活動が確認されている。Samantha Bradshaw & Philip N. Howard, “Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation” Computational Propaganda Research Project, Working Paper No. 2018.1, Oxford Internet Institute, University of Oxford (2018).

Facebook 社による取組

Facebook 社は 2016 年米大統領選挙に関するフェイクニュースや政治宣伝広告、ケンブリッジ・アナリティカ（Cambridge Analytica）経由でのユーザ情報約 8,700 万人の漏洩等を踏まえて、いくつかの対処策を打ち出している。

政治広告への規制

- Facebook 社は政治広告、正確には「政治または国家的に重要な問題に関連する広告」の透明性を高めるための取組を進めている。こうした政治広告は、米国を対象とする場合、「妊娠中絶」「予算」「市民権」「犯罪」「経済」「教育」「エネルギー」「環境」「外交政策」「政府改革」「銃火器」「健康」「移民」「インフラ」「軍事」「貧困」「社会保障」「税金」「テロ」「価値」が含まれ、相当に広範な定義である。
- Facebook 社は 2018 年 5 月 24 日、こうした政治広告のラベル表示「Promoted（political）」を開始した発表した。さらに「Paid for by」をクリックすると広告主だけではなく、広告料金やオーディエンスの内訳（年齢、性別、地域等）を確認できる。こうした政治広告を出す場合、事前に同社に対して政治信条・所在地等を申請しなければならない。現時点で、米国・英国・ブラジルで投稿され政治広告は以下のページから検索可能であり、個別の政治広告のパフォーマンスを確認できる。

  Facebook「政治または国家的に重要な問題に関連する広告を検索」
  https://www.facebook.com/ads/archive/?active_status=all&ad_type=political_and_issue_ads&country=ALL

外部アプリ開発者のデータアクセス制限、アプリの調査・監査

- Facebook 社は Facebook 上のデータにアクセス可能なアプリの調査・監査、外部開発者によるデータアクセスの制限等を発表した。

偽情報（疑いを含む）に関する注意喚起

- Facebook 社は、同サイト内で偽情報の可能性がある選挙関連投稿が掲載された場合、「誤った投票情報（incorrect voting info）」が表示されるような仕組みをつくった。しかし、Facebook で全ての投稿をチェックすることができないため、サードパーティに情報を送信し、ファクトチェックを行い、false 判定されたものはページランクが下がるようにしている[60]。

[60] “Expanding Our Policies on Voter Suppression,” Facebook Newsroom (October 15, 2018).

フェイクアカウントやスパム投稿の削除

- Facebook 社は 2018 年第 1 四半期の 3 か月で、8 億 3,700 万のスパム投稿を全て、ユーザが閲覧する前に削除した。こうしたスパム投稿を拡散する約 5 億 8,300 万のフェイクアカウントを削除している[61]。
- こうしたアカウントや投稿の削除は、次のような Facebook 社による「フェイクニュース」定義に基づいている。

表 11：Facebook 社による「フェイクニュース」の定義と構成

フェイク “アイデンティティ”	偽のアイデンティを用いたり、第三者のアイデンティティを悪用すること。
フェイク “オーディエンス”	人為的に視聴者を増やすため、あるいは特定のメッセージを普及支援のため、工作を行うこと。
フェイク“ファクト”	虚偽の情報を主張・拡散すること。
フェイク“ナラティブ”	不一致を利用し、紛争をつくるため、意図的に対立的なヘッドラインや言い回しをすること。事実関係に同意していたとしても、異なるメディアや視聴者は適切な物語が何であるかについて全く異なる見解を持っているため、最も対処が困難な領域。

出典：Guy Rosen, VP of Product Management, “Hard Questions: What is Facebook Doing to Protect Election Security?” Facebook News Room (March 29, 2018) より筆者作成。

- カリフォルニア州メンロパーク（Menlo Park）の本社に選挙対策室（Election War Room）を設置し、約 20 名のメンバーが SNS 上での不正な活動を監視することしている。直近では、ブラジル大統領選挙（2018 年 10 月）、米中間選挙（2018 年 11 月）に関する活動を監視し、2019 年に開催予定のインド総選挙にも対策を講じている[62]。

[61] Guy Rosen, VP of Product Management, “Facebook Publishes Enforcement Numbers for the First Time,” Facebook Newsroom (May 15, 2018).
[62] Aarti Betigeri, “Facebook deploys a “War Room” ahead of India’s elections,” *The Interpreter* (November 5, 2018).

Twitter 社による取組

Twitter 社も 2016 年米大統領選挙でのフェイクニュース流布を踏まえて、2018 年 10 月 1 日、11 月の米中間選挙に先立って 3 つの対策、「Twitter ルールの明確化」「検知と執行」「サービス・製品の改善」を発表した[63]。なお括弧内は筆者による補足である。

Twitter ルールの明確化（禁止行為の拡充）

- 最新のルールはフェイクアカウントの要素（他人のプロフィール画像・情報の利用、意図的な偽情報［位置情報を含む］の利用等）を明確に定義・禁止し、緊急かつ悪意ある行為を認めた場合はアカウントを削除する。
- フェイクアカウントの帰属を明らかにし、関連する他のアカウントにも対処する。
- Twitter 上で、ハッキングを通じて入手した情報の配布を禁じる。

検知と執行（フェイクアカウントの削除）

- Twitter 社は 2018 年 7 月、の一斉削除では、商業的に購入されたフォロワーやボット等数万件を削除した[64]。
- Twitter 社は 2018 年 8 月、米中間選挙に関する意図的な偽情報を配布する約 50 のアカウントを削除した。同じく 8 月には、イランに関連するとみられる 770 のアカウントを停止した。同社は RNC、DNC、各州の選挙機関と連携した取り組みを続けるとしている。また、潜在的にスパムや自動投稿アカウントを機械的に検知し、9 月初旬時点では毎週 940 万アカウントを検知している。
- Twitter 社は 2018 年 11 月 3 日、不正なアカウントを削除したと発表した。AFP の取材によれば、同社は「自動化された方法で虚偽の情報を拡散しようとした一連のアカウントについて、わが社のポリシーに違反しているため」としている[65]。同社は 9-10 月、民主党支持者に対して中間選挙投票のボイコットを呼びかけるアカウント 10,000 以上を削除したとしている[66]。

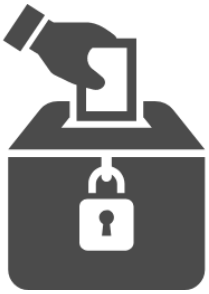
サービス・製品の改善（候補者に関するセキュリティ）

- Twitter 社は 2018 年 5 月、2018 年中間選挙候補者のアカウントに公式ラベル（election labels）を付与し、こうした候補者には二段階認証を有効化するようメッセージを送っている。

[63] Del Harvey and Yoel Roth, “An update on our elections integrity work,” Twitter Blog (October 1, 2018) https://blog.twitter.com/official/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html
[64] 詳細は、「Twitter は「健全なコミュニティ」になれるのか？ “偽アカウント”大量追放の余波」『Wired』（2018 年 8 月 25 日）
[65]「ツイッター、米選挙の偽情報拡散アカウントを削除」AFP BB News（2018 年 11 月 4 日）
[66] Christopher Bing, “Exclusive: Twitter deletes over 10,000 accounts that sought to discourage U.S. voting,” *Reuters* (November 3, 2018).

3. 提言

こうした現代の選挙介入に対抗するためには、第一義的には政府による対策・対応の強化が不可欠である。また、政府に加えて、立法府である国会、政党・政治団体、メディアとプラットフォーマー、有権者である国民による準備と対策を進めていく必要がある。



現代の選挙介入に対抗するためには、第一義的には政府による対策・対応の強化が不可欠である。政府に加えて、立法府である国会、政党・政治団体、メディアとプラットフォーマー、有権者である国民による準備と対策を進めていく必要がある。

対策・対応には、いくつかの側面がある。第一に、サイバー攻撃や SNS 上の影響工作といった選挙介入自体を予防すること【予防】、である。しかし、こうした介入をゼロにすることは事実上不可能であるため、第二に、介入が生じた場合、その影響を極小化すること、影響が生じたとしても復旧力（レジリエンス）を高めること【極小化】である。第三に、介入に対して断固たる措置をとることで、現在進行形および将来の選挙介入を抑止すること【事後対応】である。

表 12：とるべき対策（現代の選挙介入に対する備え）

とるべき対策		予防	極小化	事後対応
政府がとるべき対策				
	選挙インフラに関するリスク評価と対策	✓		
	コンティンジェンシープラン（オフライン投開票）の策定・維持		✓	
	選挙介入に関する規範形成・宣言政策	✓		✓
	選挙介入の検知能力の向上、有権者および候補者等へのアラート	✓	✓	
	アトリビューション能力の向上と制裁オプションの整備			✓
	中学校・高校でのリテラシー教育	✓		
国会がとるべき対策				
	選挙介入対策のための超党派委員会	✓		✓
	公職選挙法改正等による選挙介入の規制	✓		✓
	プラットフォーマーに対する規制	✓	✓	
政党・政治団体等がとるべき対策				
	候補者のサイバーセキュリティ改善	✓		
	政党・政治団体等のサイバーセキュリティ改善	✓		
メディア・SNS プラットフォーマー等がとるべき対策				
	選挙介入・偽情報に関する明確な用語・用法の使用	✓		
	偽情報の検証機能の確立	✓	✓	
	インターネット上の選挙介入対策、オンライン上の透明性向上	✓		
有権者・国民がとるべき対策				
	情報ソースの信頼性確認	✓		
	個別の情報媒体やメディアについて知る	✓		
	【非推奨】ファクトチェック機関への全面的信頼	✓		

※　法改正・立法を伴う対応は「政府」でも可能であるが、上記では便宜的に「国会」に分類した。

（1）政府がとるべき対策

1－1. 選挙インフラに関するリスク評価と対策

- 政府は、選挙管理や投開票で用いられるインフラや機器に関する技術的要件（基準や規格）や事務委託の要件を継続的に更新していくべきである。こうした要件に基づき、地方公共団体は選挙で用いるインフラや機器、委託事業者・サプライヤーのリスク評価を行い、調達先・契約先を選定すべきである。
- 前述の要件として、少なくとも、①選挙管理や投開票で用いるインフラの完成品および付属品・部品に、「日本の法律に違反し、外国政府の指示に従う可能性あるベンダー[67]」が関与しないこと、②選挙管理や投開票の記録は電磁的方式のみならず、印字形式でも記録されること等があげられる。

1－2. コンティンジェンシープラン（オフライン投開票）の策定・維持

- 現行の選挙プロセスにインターネットの活用拡大、電子化・自動化を行うことが検討されているが、外部からの介入・情報改竄リスクを考慮しなければならない。今後、選挙運動・投票のインターネット利用、投開票の電子化・自動化が進むと考えられるが、十分なサイバーセキュリティ上の対策を講じるとともに、**外部からの介入リスクが“僅かでも”懸念される場合、直ちに、手動による投開票（オフライン投開票）を可能とするコンティンジェンシープランを保有・維持すべきである**。
- 仮に投開票・集計システムへのサイバー攻撃が行われた場合、攻撃の成否に関わらず、投開票・選挙結果の信頼性は揺らぐ。こうした事態に備えるため、オフライン投開票を遂行するコンティンジェンシープランを策定・維持すべきである。実効的なコンティンジェンシープランは、選挙介入を行う国に対する拒否的抑止力になるだろう。
- 実際、2017 年 2 月 1 日、オランダ政府は翌 3 月の議会総選挙で、外部からのハッキングを考慮して、開票・集計を手動で行うことを決定した。また同年 3 月 6 日、フランス政府は大統領選挙に関する在外投票で、インターネット投票を一時停止することを発表した。

[67] この表現は、豪通信・芸術省の 5G 調達に関する決定（2018 年 8 月 23 日）を修正したもの。Ministers for Communications and the Arts, “Government Provides 5G Security Guidance To Australian Carriers” (August 23, 2018). 元々の表現は “the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law”である。

1－3. 選挙介入に関する規範形成・宣言政策

- 国際法における選挙介入行為の位置づけは明確ではない。政府は選挙介入を違法化するための国際規範を形成し、日本政府としての対外的な宣言政策を打ち出すべきである。
- 各国が任命した専門家で構成される多国間協議体「サイバースペースの安定性に関するグローバル委員会（Global Commission on the Stability of Cyberspace: GCSC）」[68]では、選挙インフラ防護のための以下の声明を採択した。こうした規範をその他の多国間合意でも確認していくべきである。

  国家および非国家主体は、選挙、国民投票に不可欠な技術インフラの妨害を意図したサイバー活動を追及したり、支援したり、許可すべきではない[69]。

- 政府は自由・民主制等の価値を共有する国々（米国、豪州、欧州各国等）と連携し、または独自で以下のような宣言政策を発出し、**外国勢力による選挙介入に対して自衛権行使を含めた断固たる姿勢**を内外に示すことが重要である。

  国家による選挙介入は国際違法行為[70]*、国際法が禁止する不介入原則違反に該当する*[71]*。*

  国家による選挙介入は、規模や影響によっては「政治的独立性を脅かす[72]*」可能性があり、国連憲章第 51 条下で認められる自衛権行使の要件となりうる*[73]*。*

---

[68] 日本からは JPCERT/CC の小宮山功一朗、筆者の土屋大洋が参加している。

[69] The Global Commission on the Stability of Cyberspace (GCSC), Call to Protect the Electoral Infrastructure (Bratislava, May 2018)

[70] サイバー攻撃・サイバー活動と国際法の専門家であり、タリン・マニュアルを編集したシュミット（Michael N. Schmitt）によれば、選挙介入は国際法における「グレーゾーン」、つまり戦争行為ではないにせよ、「国際違法行為（internationally wrongful acts）」に該当する場合があると指摘する。Ellen Nakashima, “Russia’s apparent meddling in U.S. election is not an act of war, cyber experts says,” *The Washington Post* (Feb. 7, 2017); Michael N. Schmitt, “‘Virtual’ Disenfranchisement: Cyber Election Meddling in the Gray Zones of International Law,” *Chicago Journal of International Law*, Vol.19, No1. (August 16, 2018), pp.30-67.

[71] 選挙介入は国際法の不介入原則に違反すると、例示的に宣言されている。2016 年米大統領選挙直後の 11 月 10 日、国務省法律顧問のイーガン（Brian Egan）は声明を発出した。彼によれば、国家によるサイバー活動は、他国による違法介入（unlawful intervention）を禁止する国際法と衝突する可能性がある。「例えば、国家によるサイバー活動、他国の選挙開催能力を妨害したり、他国の選挙結果を改竄するような活動は、明らかに不介入原則違反となるだろう」と述べた。Brian J. Egan, Legal Adviser, Department of State, Remarks on International Law and Stability in Cyberspace, Berkeley Law School (November 10, 2016) [Berkeley Journal of International Law, Vol.35, No.1, 169-180 に収録]

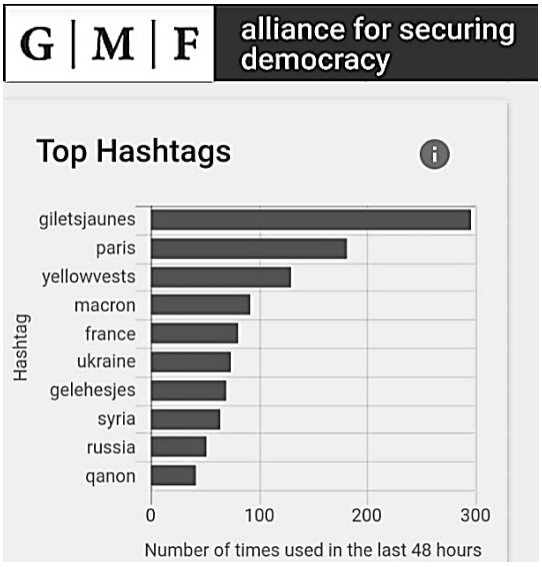
[72] 2011 年 9 月 15 日、米豪の外交・防衛閣僚会議（2 プラス 2）は「領土保全、**政治的独立性**、米豪の安全保障を脅かすようなサイバー攻撃」（下線強調は筆者）は太平洋安全保障条約（ANZUS）の集団的自衛権行使の対象である点を確認した。

[73] こうした宣言は実際に行われている。2016 年米大統領選挙投票日の直前の 2016 年 10 月 31 日、オバマ大統領はプーチン大統領に緊急回線で「国際法は、武力紛争法を含めて、サイバー空間での行為にも適用される」との言葉とともに警告したと報じられた。これが事実なら、ロシアによる選挙介入を「武力攻撃」と捉え、自衛権に基づく対応を示唆したことになる。William M. Arkin, Ken Dilanian and Cynthia McFadden, “What Obama Said to Putin on the Red Phone About the Election Hack,” *NBC News* (December 20.2016). またドイツのある専門家は「ロシアによる選挙介入があれば、欧州各国は北大西洋条約 5 条を発動すべきである」と主張する。Thorsten Benner & Mirko Hohmann, “Europe in Russia’s Digital Cross Hairs:

1－4. 選挙介入の検知能力の向上、有権者および候補者等へのアラート

- 政府は現在進行形の選挙介入、サイバー攻撃や SNS 上での影響工作が行われたことを検知（detect）する能力を向上させる必要がある。日本語でサービスを展開する主要な SNS プラットフォーマーに対しては、検知能力の向上と検知結果の通知義務を課すべきである。
- 政府は介入を検知した場合、**適切な方法と開示範囲にもとづき、有権者および候補者（政党を含む）、メディア、国会に事実関係の通知と注意喚起**を行うべきである。選挙介入に限らず、外国からのサイバー攻撃や SNS 上での影響工作が活発化している場合、国民に対して「天気予報」のような形式で注意喚起することも必要である。単に、サイバー攻撃や影響工作が展開されているという事実のみならず、米国ジャーマン・マーシャル財団が提供する「the Hamilton 68 dashboard」のように、**具体的なトピックスについても周知すべき**である。しかし、実際には政府がこうした「天気予報」を運営することは難しいため、大学やシンクタンク等の研究機関に助成・委託することが現実的であろう。

図 4：米国ジャーマン・マーシャル財団「the Hamilton 68 dashboard」



米国ジャーマン・マーシャル財団は the Hamilton 68 dashboard という Twitter 上の影響工作監視プロジェクトを実施してきた。左記はロシア政府と関係が深い 600 の Twitter アカウントの「つぶやき」、ハッシュタグの直近 48 時間のトレンドを分析したもの。左記ではフランス・マクロン政権への反対デモ、「黄色のベスト」運動についてのハッシュタグが増えていることを示している。これは、こうした Twitter アカウントが「黄色のベスト」運動に何らかの関心を持っていることを示唆する[74]。

出典：The German Marshall Fund of the United States, “Tracking Russian Influence Operations on Twitter,” （2018 年 12 月 9 日アクセス）
なお the Hamilton 68 dashboard は 12 月 21 日に終了し、2019 年春に Hamilton 68 Ver.2.0 を公開予定である。

What’s Next for France and Germany and How to Deal with It,” Snapshot on *Foreign Affairs*, 2016.

[74] フランス政府は、「黄色のベスト」運動に対するロシア政府の支援を調査すると発表した。Carol Matlack & Robert Williams, France to Probe Possible Russian Influence on Yellow Vest Riots, *Bloomberg* (December 7, 2018).

1－5. アトリビューション能力の向上と制裁オプションの整備

- 政府は選挙介入の発信源を特定する（アトリビューション）能力を向上させる必要がある。そのため、政府による電子信号諜報（Signal Intelligence: SIGINT）能力を強化し、通信傍受の要否・可能性についても検討を行うことが望ましい[75]。
- 政府は選挙介入に対する制裁オプションとして、①名指し批判（name & shame）、②経済制裁、③刑事訴追、④外交制裁、⑤サイバー攻撃、⑥キネティックな反撃等のあらゆる制裁オプションの整備することが重要である[76]。選挙介入、すなわち投票日までの限られた時間軸では、**即時性の高い制裁オプション（外交制裁とサイバー攻撃）を充実**させることが重要である[77]。

1－6. 中学校・高校でのリテラシー教育

- 政府は、中学校・高校で基本的な情報リテラシー教育・サイバーセキュリティ教育を拡充すべきである。情報リテラシー教育は選挙介入に限らず、SNS 上での偽情報の見分け方、情報の信頼性の確認方法等を盛り込むべきである。
- 米国の研究者シンガー（P. W. Singer）は、情報リテラシーは教育だけの問題ではなく、安全保障問題であるという[78]。スウェーデンや韓国の国民向け民間防衛マニュアル[79]は、戦時下に限定しているものの、交戦国によるデマ・プロパガンダへの備えが指摘されている。選挙介入が平時に行われていることを踏まえると、平時からの情報リテラシー強化が必要だろう。

---

75 宍戸常寿「現実空間と同じようにサイバー空間を守るために必要なこと」『Wedge』（2019 年 1 月号）、8-11 頁。

76 米国のアトリビューションと制裁・報復措置については、川口貴久「米国のサイバー抑止政策の刷新：アトリビューションとレジリエンス」『Keio SFC Journal』Vol.15、No.2（2016 年 3 月）、78-96 頁。

77 米サイバー軍はロシアによる 2018 年米中間選挙への介入を抑止するために対応したと報じられた。Ellen Nakashima, “Pentagon launches first cyber operation to deter Russian interference in midterm elections,” *The Washington Post* (October 23, 2018); Julian E. Barnes, “U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections,” *The New York Times* (October 23, 2018); Evan Perkoski, “U.S. Cyber Command Targeted Russian Operatives to Deter Election Meddling. Here’s Why,” *NetPolitics*, Council on Foreign Relations (October 31, 2018).

78 Singer, P. W., and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

79 Swedish Civil Contingencies Agency (MSB), If Crisis or War Comes, Important Information for the Population of Sweden (May 21, 2018); 韓国行政安全部「戦争・テロ等、非常時国民行動要領」（外務省 在大韓民国日本国大使館「在留邦人向け安全の手引き（安全マニュアル）」別添 4（2013 年 4 月 1 日））

（2）国会がとるべき対策

2－1. 選挙介入対策のための超党派委員会

- 衆参両院は選挙介入に関する超党派委員会を設置し、平時から、選挙介入対策に関する国会内での合意形成、政府への提言、国会としての対応を進めるべきである。有事においては、国会は政府と密接に連携し、超党派行動をとるべきである。
  - 2016 年米大統領選挙介入では、オバマ政権は自らの決定（対露制裁、国民への警鐘等）が共和党からの批判を巻き起こし、（当選が見込まれていた）クリントン候補の正統性を貶めると考え、十分な対応を講じることができなかった[80]。
  - オバマ政権とインテリジェンス・コミュニティは、民主党・共和党の代表達、通称「8 人衆（gang of eight）[81]」にブリーフィングを行った。彼らは一部、議会としての超党派の行動をとったが、結果的には党派性をもった行動に終始したといえる。
- 万が一、国政選挙で外国政府による選挙介入が行われた場合、介入が疑われる場合、委員会は選挙介入の事実関係・影響を調査する権限を付与されるべきである。
- ただし、この委員会の構成委員や出席可能な代議士は一定のセキュリティクリアランスを取得できる代議士に限定すべきである。

2－2. 公職選挙法改正等による選挙介入の規制

- 公職選挙法には「選挙活動」に関する定義がなく、外国人による選挙活動は規制されていない。政治資金規正法の外国人からの献金禁止（第二十二条の五）、放送法の外資資本規制のような規制が、公職選挙法にはない。そもそも選挙人資格がない外国人は公職選挙法の規制対象外である[82]。
- 国会（または政府）は公職選挙法改正や新たな立法・その他法改正を通じて、外国政府やその代理人による選挙活動、選挙介入を明示的に禁止し、取り締まるべきである。

[80] 例えば、下院特別情報委員会の報告書では、オバマ政権が大統領選挙投票日以前に対露対抗措置をとれなかった要因の一つとして、「行政府が選挙に近すぎるとの批判・警鐘を当然に懸念した」としている。U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI), *Report on Russian Active Measures*, Majority Report (March 22, 2018), p.38.

[81] 「8 人衆」とは、上下院の共和党・民主党それぞれの院内総務、院内幹事、上下院の情報委員会の委員長、副委員長の 8 人である。

[82] 情報セキュリティ大学院大学・湯淺墾道教授へのヒアリング（2018 年 12 月 4 日）結果より。

2−3. プラットフォーマーに対する規制

- 国会（または政府）は SNS やインターネット上の違法コンテンツに対する規制強化を検討する必要がある。具体的には、法整備を通じて、プラットフォーマーに対して、偽情報や違法コンテンツの迅速な削除を義務付けることについて検討すべきである。
  - 例えば、ドイツでは「ネットワーク執行法（ソーシャルネットワークにおける法執行の改善に関する法律）」が 2017 年 10 月 1 日から施行された。これは、ドイツ国内で 200 万人以上の登録者を抱える事業者に対して、違法コンテンツの削除・ブロック等の対応を課すものである。「違法コンテンツ」はフェイクニュースだけではなく、ポルノ、犯罪教唆等が含まれる。同法の下、事業者は窓口を設け、「明らかに違法なコンテンツ」は受付から 24 時間以内、「それ以外の違法コンテンツ」は受付から 7 日以内の対応が求められ、対応が十分ではない場合、最大 5,000 万ユーロの罰金が課せられる場合がある。
  - ネットワーク執行法については言論の自由に対する規制であるとの反対意見も根強い。他方、あるドイツ人研究者によれば、ネットワーク執行法制定の背景には、民主国家が民主主義を守るためには必要な措置であり、ドイツ憲法第 18 条下で保障された措置であるという[83]。いずれにせよ、法制化にあたっては丁寧な議論が必要だろう。
  - ただし、「フェイクニュース」は多義的な意味合いを持つ（例えば、Facebook 社の定義）ため、規制対象とする場合の定義は慎重であるべきである。規制対象とする「フェイクニュース」の定義は最小限なもの、すなわち「選挙、候補者に関する事実」に関する虚偽情報に限定すべきである。そうした意味で、多義的な意味合いを持つ「フェイクニュース」という用語は使用すべきでないかもしれない。

[83] Heidi Tworek, “How Germany Is Tackling Hate Speech: New Legislation Targets U.S. Social Media Companies,” Snapshot on *Foreign Affairs* (May 16, 2017).

（3）政党・政治団体等がとるべき対策

3－1. 候補者のサイバーセキュリティ改善

- 選挙候補者は自身のサイバーセキュリティを改善することが重要である。2016 年米大統領選挙介入では必ずしも技術的には高度ではない手法（人間の脆弱性に焦点を当てた攻撃）で、政党・関係機関・関係者が侵入・情報窃取を受けた。候補者は、①強固なパスワードの生成・管理、②利用するクラウド型フリーメール（Gmail, Yahoo!メール等）、SNS 等の二要素認証（Two Factors Authentication: 2FA）の有効化等の基本的な対策を実施することが重要である。

3－2. 政党・政治団体等のサイバーセキュリティ改善

- 政党・政治団体等は、脆弱性・侵害有無およびサイバーセキュリティ対策状況を定期的に評価・検証し、必要な措置を講じなければならならない。評価・検証は第三者機関が担うことが望ましい。
- 政党・政治団体等は、候補者・関係者（秘書や主要な支援者等）や職員に対して最低限のサイバーセキュリティ教育を実施すべきである。同様に、標的型メール攻撃やスピアフィッシング攻撃に関する訓練を通じて、候補者・関係者や職員のリテラシー向上に努めるべきである。

（4）メディア・SNS プラットフォーマー等がとるべき対策

4－1. 選挙介入・偽情報に関する明確な用語・用法の使用

- メディアは、選挙介入に関する特定行為について明確な用語・用法を用いるべきである。特に「フェイクニュース」は分かりやすい用語であるが、使用しないか、使用するにしても十分に注意することが必要である。実際、英国議会は「フェイクニュースの用語を使うべきではない」との勧告を発表している[84]。「フェイクニュース」という用語を避けるべき、または注意して使うべき理由は以下のとおりである。
  - 「フェイクニュース」の定義・対象範囲は用いる人・機関によって大きく異なるため。「匿名情報」や風刺画さえも、「フェイクニュース」と呼ばれるケースがある。
  - 問題の本質的な要素（外国勢力による内政干渉等）を過小評価してしまう可能性がある。
  - 権威主義国家では、「テロリズム」という用語と同様、「フェイクニュース」という用語は反政府勢力弾圧を正当化する目的で用いられるケースが散見される[85]。また、伝統的な大手メディアや自らに批判的なメディアのレッテル張りに用いられる。
- メディアは「フェイクニュース」に代わって、単に「虚偽情報」「偽情報」と呼ぶべきである。

4－2. 偽情報の検証機能の確立

- メディアはニュースおよび発信源の真偽を**技術的に検証できる専門的ジャーナリストを登用・育成、専門部署を設置すべき**である。具体的な検証方法の一部として、「フェイクニュースの調査ガイド（A Field Guide to “Fake News” and Other Information Disorders）」が公開されている[86]。
- メディアは既に報じたニュース・情報が偽情報にもとづくものであった場合、単一のプラットフォーム（ウェブサイト上の「誤報ページ」等）上で、偽情報・誤報の旨を公開すべきである。

[84] House of Commons (the U.K. Parliament), Digital Culture Media and Sport Committee, “Appendix: Government Response,” Disinformation and ‘fake news’: Interim Report: Government Response to the Committee’s Fifth Report of Session 2017–19 (October 23, 2018); Digital Culture Media and Sport Committee, Disinformation and ‘fake news’: Interim Report: Government Response to the Committee’s Fifth Report of Session 2017–19 (July 29, 2018)
[85] Freedom House, *Freedom in the Net 2018: The Rise of Digital Authoritarianism* (Washington, DC: Freedom House, October 2018), p.11.
[86] Liliana Bounegru, et al, *A Field Guide to “Fake News” and Other Information Disorders: A Collection of Recipes for Those who Love to Cook with Digital Methods and Other Information Disorders* (Public Data Lab., 2018)

4−3. インターネット上の選挙介入対策、オンライン上の透明性向上

- 一定規模以上の SNS プラットフォーマー等（例えば、日本国内の登録者 ID 数 500 万人を超える SNS プラットフォーマー等）は、次の対策を講じ、選挙介入を予防することに努めなければならない。
  - ☐ 偽情報への対処方針（偽情報の定義を含む）の明示
  - ☐ 偽情報に関する通報・受付窓口の設置
  - ☐ 偽のアカウントやボットの検知、削除
  - ☐ 偽の事実関係、犯罪・ヘイト情報の監視、削除
  - ☐ 政治関連広告のスポンサーやターゲット層の表示
  - ☐ リンク先のウェブサイトの概要（運営者、開設年月）の表示
  - ☐ 検索、広告、情報キュレーション等に関するアルゴリズムの公開
  - ☐ 外部アプリによる個人データへのアクセス制限、各種権限取得の制限
  - ☐ 国政選挙に関わる対応状況（政治関連広告、不正なアクティビティやアカウントの検知・対応状況等）に関する議会への報告
- 上記の対策の一部は、SNS プラットフォーマーに限定されず、スマートフォンやパソコン等の端末のブラウジングソフトベンダー、検索エンジン等にも適用されるべきである。

（5）有権者・国民がとるべき対策

5－1. 情報ソースの信頼性確認

- 煽動的な情報こそ、情報ソースを確認する。特に SNS は匿名性が高いため、感情的で煽動的な言葉が使われる。自分の投票行動を変えうるもの、確信させるような情報ほどソースを確認する必要がある。例えば、複数の情報ソースがないものは信頼性が低いと考えた方が良い。（「匿名の情報源」は直ちに偽情報とは断定できないものの、単一の「匿名の情報源」だけに頼った情報の信頼性は低くみるべきだろう）
- 新聞、テレビ、雑誌、ウェブサイト、SNS 等の各媒体はそれぞれの役割と特徴がある。「新聞しか読まない」「SNS しか見ない」よりも、複数の媒体に触れる方がよい。

5－2. 個別の情報媒体やメディアについて知る

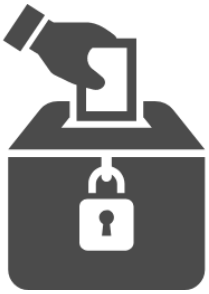
- 個別のテレビや新聞・通信社について知ることが望ましい。テレビ等は規制があるが、実際にはどのメディアにも政治スタンスがある。報道ではなく、評論は会社や執筆者個人の価値観が反映されやすい。
- 外国政府と密接な関係にあるメディア、特に日本語で情報提供しているメディアを知ることは重要である。一部のメディアは当該国の国益を反映し、政策誘導や選挙介入の悪意を持っているかもしれない。全てがフェイクということはないが、国益に照らし合わせ、事実の一部が強調されていたり、改変されている恐れがある。

5－3.【推奨しないこと】ファクトチェック機関への全面的信頼

- 情報の信頼性を評価する際、ファクトチェック機関を活用することは有益な場合がある。しかし、ファクトチェック機関の活用には大きな問題があり、ファクトチェック機関を全面的に信頼することは避けるべきである。
    1. ファクトチェック機関は政治的に偏向している場合がある（「誰が見張りを見張るのか」問題）。ファクトチェック機関を利用する場合、機関の出資団体や主要メンバーに政治的偏向、特定の政策・政党を支持していないかを確認することは不可欠である。しかし、そもそも、ファクトチェック機関の信頼性を検証できるリテラシーやスキルのある有権者は、ファクトチェック機関に頼らずとも自分自身でニュースや情報の信頼性を検証できるはずである。
    2. ファクトチェック機関は本質的に、量、速度、コストの面で偽情報に対抗できない。拡散される偽情報の速度と量に、人的な検証を必要するファクトチェックは対抗できない。また、一定の人的工数を要するファクトチェックは、コスト面でも偽情報に対抗できない。そもそも一度偽情報が拡散した場合、それが事実に反すると分かっていても更なる拡散を防ぐことは容易ではない。

4. 結論

現代の選挙介入は民主主義国家にとって差し迫った脅威である。この脅威に対抗するため、諸外国の選挙介入の実態を把握し、日本の文脈で再検討し、対策・対応を進めていく必要がある。



選挙介入とは

選挙介入、すなわち国政選挙・国民投票等の政治「制度」や有権者の「意思決定」に対する影響工作は民主主義国家にとって差し迫った脅威である。もちろん、外国勢力による選挙介入は新しい現象ではない。しかし、現代の選挙介入はサイバー攻撃やSNS上での工作活動を組み合わせ、その影響力は甚大である。

サイバー空間やSNS上では多様なアクターが存在するものの、選挙介入の主体として、最も懸念されるのは「国家」であり、その「代理人」である。これらをどのように抑止するかが喫緊の課題である。

日本の文脈

日本国内においても、過去、違法な選挙妨害が確認された（ただし、外国政府によるものではない）。日本の選挙も妨害・介入と無縁ではない。

確かに、選挙介入を行う側（攻撃者）にしてみれば、多党制・議院内閣制は介入の「コストパフォーマンス」が相対的に低い。しかし、2017年9月のドイツ議会選挙で介入が確認されたように、日本でも議会選挙、特に単一の争点を中心に社会分断を狙った介入が行われる可能性がある。また、通常の国政選挙とは異なり、憲法改正に関わる国民投票は、有権者の賛否を二分しやすく、政策への影響も大きいため、特別な注視が必要である。

日本では、選挙過程の電子化・インターネット利活用が検討・推進されている。従来から指摘された投票・集計結果の改竄の可能性は高いとは言えないが、投票・集計結果への攻撃自体が（仮に攻撃・改竄が成功しなかったとしても）選挙の正統性や投開票の信頼性を揺るがしかねないリスクである。投開票以外の選挙管理要素については、情報の改竄、窃取等のリスクが懸念される。

しかし、投票結果の改竄よりも、候補者の選挙運動や有権者の認知に対する攻撃の方が懸念すべきリスクである。日本国内のオンライン上のニュースサービスでは、ポータルサイトによるニュース配信（Yahoo!ニュース等）、ソーシャルメディア（LINE、Twitter、Facebook）によるニュース配信の利用率が高いということは、SNSやインターネット上で影響工作を受ける曝露量（exposure）が高いということである。Facebook社やTwitter社は2016年米大統領選挙や2018年米中間選挙の経験を経て、選挙介入対策を講じており、日本国内で事業を展開するプラットフォーマーでも同程度かそれ以上の対策が期待される。

提言

現代の選挙介入に対抗するためには、第一義的には政府による対策・対応の強化が不可欠である。また、政府に加えて、立法府である国会、政党・政治団体、メディアとプラットフォーマー、有権者である国民による準備と対策を進めていく必要がある。

求められる対策・対応として、第一に、サイバー攻撃やSNS上の影響工作といった選挙介入自体を予防すること【予防】、である。しかし、こうした介入をゼロにするこ

とは事実上不可能であるため、第二に、介入が生じた場合、その影響を極小化すること、影響が生じたとしても復旧力（レジリエンス）を高めること【極小化】である。第三に、介入に対して断固たる措置をとることで、現在進行形および将来の選挙介入を抑止すること【事後対応】である。

今後の課題

最後に、本レポートが十分に触れらなかった点、今後の課題について指摘する。

課題 1　様々な国の選挙介入手法について

本レポートは主に 2016 年米大統領選挙を事例に、すなわちロシアによる選挙介入を取り扱った。しかし、現在、選挙介入の担い手はロシアだけではない。

米国のインテリジェンス・コミュニティは米中間選挙（2018 年 11 月 6 日）への介入を調査[87]し、「投票妨害、集計結果の改竄、集計妨害等の米国の選挙インフラへの攻撃」は確認できなかったものの、「ロシアおよび中国、イランを含む諸外国による影響活動と情報キャンペーン（influence activities and messaging campaigns）」を確認した、と評価した[88]。こうした現状について、CIA 副長官を務めたモレル（Michael Morell）は「ロシアによる民主主義への干渉を抑止できなかったため、今や他の国々も干渉に参加している」と指摘している[89]。

ロシアによる選挙介入は、冷戦期における「積極工作（active measures）」に起源を持ち、直近では「ハイブリッド戦争（hybrid warfare）」の一部と位置付けられている。**中国には中国の、イランにはイランの影響工作の伝統と方法論がある**。こうした観点での分析と対策が必要であろう。

課題 2　分析・対応のための専門領域について

本レポートの執筆者 2 人の専門領域は国際政治、安全保障、サイバーセキュリティである。本レポートはあくまでも安全保障の観点で、民主主義に対する脅威として選挙介入を分析し、対策を検討した。しかし、選挙介入のテーマは広範で多様な専門領域に関わる。今後は様々な分野の専門性、少なくとも、**①日本の選挙制度（政治学、行政学、法学）、②介入国の外交・安全保障・情報工作、③SNS 上の情報伝播、④選挙インフラや SNS のサイバーセキュリティ等の観点での分析・対策検討**が必要であろう。

以上

---

87 大統領令 13848 号により、米インテリジェンス・コミュニティは選挙後 45 日以内に選挙介入の調査結果を報告しなければならない。

88 DNI Coats Statement on the Intelligence Community's Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, December 21, 2018

89 Michael Morell (@MichaelJMorell), tweets, "DNI Coats says “Russia, and other foreign countries, including China and Iran, conducted influence operations” in the mid terms.　B/c we have not deterred Russia from interfering in our democracy, others are now joining them. Significant failure of policy.” at 05:29, December 22, 2018.

主要な参考文献

Alperovitch, Dmitri, “Bears in the Midst: Intrusion into the Democratic National Committee,” CrowdStrike (June 15, 2016)

Blaze, Matt, Jake Braun, Harri Hursti, David Jefferson, Margaret MacAlpine, and Jeff Moss, *Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, DEF CON 26 Voting Village (September 2018)

Bounegru, Liliana, et al, *A Field Guide to “Fake News” and Other Information Disorders: A Collection of Recipes for Those who Love to Cook with Digital Methods and Other Information Disorders* (Public Data Lab., 2018)

Buchanan, Ben, and Michael Sulmeyer. “Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity.” Belfer Center for Science and International Affairs, Harvard Kennedy School (October 2016)

Cederberg, Gabriel, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections*, Belfer Center for Science and International Affairs, Harvard Kennedy School (September 7, 2018)

Clapper, James R., *Facts and Fears: Hard Truths from a Life in Intelligence* (New York: Random House, 2018)

Department of Justice, *Report of the Attorney General’s Cyber-Digital Task Force* (July 19, 2018)

DiResta, Renee, et.al., *The Tactics & Tropes of the Internet Research Agency* (New Knowledge, December 2018)

Galante, Laura, & Shaun Ee, “Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents,” Issue Brief, Atlantic Council (September 2018)

Harding, Luke, *Collusion: Secret Meetings, Dirty Money, and How Russia Helped Donald Trump Win* (New York: Vintage, 2017)

Howard, Philip N., et.al., *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (University of Oxford, December 2018)

Isikoff, Michael, & David Corn, *Russian Roulette: The Inside Story of Putin''s War on America and the Election of Donald Trump* (New York: Twelve, 2018)

Lewis, James Andrew, “Cognitive Effect and State Conflict in Cyberspace,” Center for Strategic & International Studies (September 26, 2018)

Mook, Robby, Matt Rhoades, & Eric Rosenbach, ""“Cybersecurity Campaign Playbook.” Belfer Center for Science and International Affairs, Harvard Kennedy School (November 2017)

Nye, Joseph S., “Protecting Democracy in an Era of Cyber Information War,” Fall Series, Issue 318, Hoover Institution (November 13, 2018)

Office of the Director of National Intelligence (ODNI), *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident*

Attribution (January 6, 2017)

Polyakova, Alina, and Spencer Phipps Boyer, “The future of political warfare: Russia, the West, and the coming age of global digital competition,” Brookings (March 2018)

Rid, Thomas, & Ben Buchanan, “Hacking Democracy,” *SAIS Review of International Affairs*, Vol.38, No.1 (Winter-Spring 2018), pp. 3-16.

Rid, Thomas, “Disinformation: A Primer in Russian Active Measures and Influence Campaigns,” Hearing before the Select Committee on Intelligence, U.S. Senate, One Hundred Fifteenth Congress, First Session (March 30, 2017)

Rid, Thomas, and Ben Buchanan, “Attributing Cyber Attacks,” *The Journal of Strategic Studies*, Vol.38, No.1-2 (2015), pp.4-37［トマス・リッド、ベン・ブキャナン（土屋大洋訳）「サイバー攻撃を行うのは誰か」『戦略研究』第 17 巻（2016 年 5 月）、59-98 頁］

Sanger, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Scribe, 2018)

Singer, P. W., and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018)

Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee & Madeline McCue, *Addressing Hybrid Threats* (Stockholm: Center for Asymmetric Threat Studies, Swedish Defence University, 2018)

U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464 (September 28, 2018)

U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018)

U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018)

U.S. House of Representatives Permanent Select Committee on Intelligence, Report on Russian Active Measures viii (March 2018)

U.S. Senate the Committee on Foreign Relations, *Putin''s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security,* A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations United States Senate, One Hundred Fifteenth Congress, Second Session (January 10, 2018)

Vilmer, Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies*, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris (August 2018)

Woolley, Sam, and Phil Howard, “Computational Propaganda Worldwide: Executive Summary,” Computational Propaganda Research Project, Working Paper, No. 2017.11, Oxford Internet Institute, University of Oxford (June 19, 2017)

ウッドワード，ボブ（伏見威蕃訳）『FEAR 恐怖の男：トランプ政権の真実』（日

本経済新聞社、2018 年）

川口貴久「サイバー攻撃は誰がやった？」、ChannelJ 運営情報サービス「安全保障用語」解説・コラム（2018 年 10 月 12 日）

川口貴久「米国のサイバー抑止政策の刷新：アトリビューションとレジリエンス」『Keio SFC Journal』特集：新しい安全保障論の展開、Vol.15、No.2（2016 年 3 月）、78-96 頁。

クリントン，ヒラリー・ロダム（髙山祥子訳）『WHAT HAPPENED：何が起きたのか？』（光文社、2018 年）

コミー，ジェームズ（藤田美菜子、江戸伸禎訳）『より高き忠誠：真実と嘘とリーダーシップ』（光文社、2018 年）

笹原和俊『フェイクニュースを科学する：拡散するデマ、陰謀論、プロパガンダのしくみ』（化学同人、2018 年）

土屋大洋『サイバーセキュリティと国際政治』（千倉書房、2015 年）

土屋大洋『暴露の世紀：国家を揺るがすサイバーテロリズム』（角川新書、2016 年）

ハーディング，ルーク（高取芳、米津篤八、井上大剛訳）『共謀：トランプとロシアをつなぐ黒い人脈とカネ』（集英社、2017 年）

ナイ，ジョセフ「露のサイバー攻撃　戦闘伴わぬ『新兵器』」『読売新聞』（2018 年 8 月 26 日）、1-2 面。

湯淺墾道「選挙とサイバーセキュリティ（2）」『月刊 選挙』第 71 巻、第 2 号（2018 年 2 月）、9-18 頁。

湯淺墾道「2019 年欧州議会選挙とインターネット・SNS（2）」『選挙』第 71 巻、9 号（2018 年 9 月）、1-5 頁。

執筆者略歴

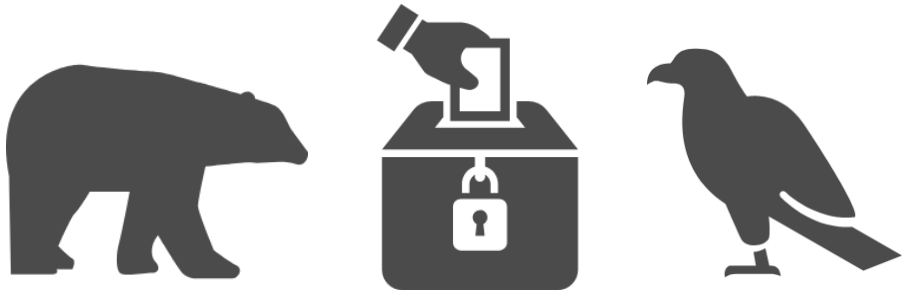
川口 貴久（Takahisa KAWAGUCHI），
東京海上日動リスクコンサルティング株式会社　主任研究員

【略歴】1985 年生まれ。慶應義塾大学大学院政策・メディア研究科修士課程修了（修士（政策・メディア））。東京海上日動リスクコンサルティング株式会社 戦略・政治リスク研究所 兼 ビジネスリスク本部 兼 ソリューション創造本部　主任研究員。プロジェクトマネージャとして、企業（自動車、製薬、金融等）・官公庁向けのリスクコンサルティングに多数従事する。特に、政治リスク・地政学リスクの調査分析・コンサルティング（朝鮮半島有事、トランプ政権の政策変更リスク対応等）、サイバー攻撃対応演習・サイバー攻撃発生時の予想損失額評価等に従事する。加えて、防衛大学校グローバルセキュリティセンター研究プロジェクト「危機管理制度の日米比較研究」共同研究者、日本再建イニシアティブ（RJIF）「21 世紀の地政学、地経学ダイナミクスと日本の戦略」研究会委員、日本国際問題研究所（JIIA）平成 25－26 年度外務省外交・安全保障調査研究事業「グローバル・コモンズ（サイバー、宇宙、北極海）における日米同盟の新しい課題」研究会委員、慶應義塾大学 SFC 研究所　上席所員、キヤノングローバル戦略研究所（CIGS）　外交・安全保障グループスタッフ等を歴任。この他、参議院　国際経済・外交に関する調査会における参考人意見陳述（2018 年 2 月 7 日）等。
【著作】共著『「技術」が変える戦争と平和』（道下徳成編著、芙蓉書房出版、2018 年）、共著『現代日本の地政学：13 のリスクと地経学の時代』（日本再建イニシアティブ著、中公新書、2017 年）、共著『仮想戦争の終わり：サイバー戦争とセキュリティ』（土屋大洋監修、KADOKAWA、2014 年）；川口貴久、土屋大洋「東京五輪をサイバーリスクから守る：官民連携で『許容できないサイバー攻撃』に対峙せよ」『リスクマネジメント TODAY』日本リスクマネジメント協会（2017 年 5 月）、5-9 頁；　川口貴久「米国のサイバー抑止政策の刷新：アトリビューションとレジリエンス」『Keio SFC Journal』特集：新しい安全保障論の展開, Vol.15, No.2（2016 年 3 月）；川口貴久「米国のサイバーセキュリティ政策：オバマ政権における進展と課題」『海外事情』第 64 巻、第 2 号（2016 年 2 月）、63-75 頁等多数。

土屋 大洋（Motohiro TSUCHIYA）
慶應義塾大学大学院政策・メディア研究科　教授

【略歴】1970 年生まれ。慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士（政策・メディア）。2011 年 4 月から慶應義塾大学大学院政策・メディア研究科教授（兼 総合政策学部教授）。これまでに、フルブライト研究員としてメリーランド大学国際開発・紛争管理センター客員研究員（2001 年 7 月－12 月）、安倍フェローとしてジョージ・ワシントン大学サイバースペース政策研究所（サイバー・セキュリティ＆プライバシー研究所に改名）客員研究員（2001 年 12 月－2002 年 6 月）、富士通総研経済研究所客員研究員（2004 年 1 月－2006 年 12 月）、国際大学グローバル・コミュニケーション・センター（GLOCOM）客員研究員（2004 年 4 月－2005 年 3 月、2009 年 4 月－2015 年 3 月）・フェロー（2005 年 4 月－2009 年 3 月）・上席客員研究員（2015 年 4 月－現在）、情報セキュリティ政策会議有識者構成員（2009 年 8 月－2013 年 10 月）、慶應義塾大学グローバルセキュリティ研究所（G-SEC）副所長（2009 年 9 月－2013 年 9 月）、総務省情報通信政策研究所（IICP）特別上級研究員（2010 年 7 月－2016 年 3 月）、イースト・ウエスト・センター客員研究員（2014 年 3 月－2015 年 3 月）、国際社会経済研究所客員研究員（2016 年 4 月－現職）、慶應義塾大学グローバルリサーチインスティテュート（KGRI）副所長兼上席研究員（2016 年 10 月－現在）、首相官邸「安全保障と防衛力に関する懇談会」有識者構成員（2018 年 8 月－12 月）等を兼任・歴任。
【著作】単著『暴露の世紀』（KADOKAWA、2016 年）、単著『サイバーセキュリティと国際政治』（千倉書房、2015 年）、単著『サイバー・テロ：日米 vs.中国』（文藝春秋、2012 年）、単著『ネットワーク・ヘゲモニー：「帝国」の情報戦略』（NTT 出版、2011 年）、単著『情報による安全保障：ネットワーク時代のインテリジェンス・コミュニティ』（慶應義塾大学出版会、2007 年）、単著『ネットワーク・パワー：情報時代の国際政治』（NTT 出版、2007 年）、単著『ネット・ポリティックス：9.11 以降の世界の情報戦略』（岩波書店、2003 年、第 19 回テレコム社会科学賞受賞）、『情報とグローバル・ガバナンス：インターネットから見た国家』（慶應義塾大学出版会、2001 年）；共著（持永大、村野正泰、土屋大洋）『サイバー空間を支配する者：21 世紀の国家、組織、個人の戦略』（日本経済新聞出版社、2018 年）等多数。

別紙:2016 年米大統領選挙



別紙 1：ロシアによる 2016 年米大統領選挙介入

米国家情報長官室（the Office of the Director of National Intelligence: ODNI）は 2017 年 1 月 6 日、オバマ（Barack H. Obama）大統領の指示にもとづき報告書「最近の米国選挙におけるロシアの活動と意図に関する評価」を公表する。ODNI 報告書（公開版）によれば、ロシアは「米国の民主的プロセスに関する国民の信頼を損ね、クリントン候補を非難し、彼女の当選可能性や大統領としての潜在性を害することを意図した」影響活動を展開し、この活動は「プーチン（Vladimir V. Putin）大統領の指示に基づく」ものであり、「プーチン大統領とロシア政府はトランプ候補に対して明らかに選好があった」とした。このような評価について、ODNI は機密情報・公開情報にもとづく「高い確信（high confidence）」をもつ、と明言した[90]。

米国が主張する「ロシアによる 2016 年の米国大統領選挙介入」は伝統的なメディア、サイバー攻撃、SNS 上での情報工作を組み合わせた活動であり、少なくとも以下の要素から構成される。下記 1 については、英国の国営サイバーセキュリティ組織「国家サイバーセキュリティセンター（NCSC）」もロシアの情報機関が実行したことに「高い確信」を与えている[91]。オーストラリア、オランダ、カナダ政府も同様の結論を下した。

表 1：2016 年米大統領選挙への介入の構成要素（再掲）

No.	分類	概要
1	機密情報の窃取と暴露	・米民主党議会選挙委員会（DCCC）、米民主党全国委員会（DNC）、ヒラリー・クリントン候補選挙対策事務所等の民主党関係機関、共和党全国委員会（RNC）へのハッキングと情報窃取 ・収集した情報の暴露（自らが作り上げた架空のオンラインハッカーGuccifer 2.0 およびウェブサイト DCLeaks.com 経由した暴露、WikiLeaks 等への暴露）
2	各種メディアを用いた影響工作	・トロールやボットを用いたソーシャルメディア（Facebook, Twitter）上での世論誘導・分断、偽情報の投稿 ・ソーシャルメディア（Facebook, YouTube）上での政治広告・宣伝 ・ロシア系メディア（RT, sputnik）を用いた偽情報の拡散、プロパガンダ流布
3	選挙関連システムへの攻撃	・各州の選挙管理委員会ウェブサイトや関連システムへの攻撃、投票結果の改竄（未遂）、関連企業への攻撃

なお、ロシア政府とトランプ陣営の共謀が疑われている点については、本レポート執筆（2018 年 12 月）時点で明確な判断結果・評価結果が下されていないので割愛する。

[90] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (January 6, 2017), i.
[91] National Cyber Security Center, Reckless campaign of cyber attacks by Russian military intelligence service exposed (October 4, 2018)

（1）DCCC、DNC、ヒラリー事務所へのサイバー攻撃と機密情報公開

2016 年選挙介入の 1 つは、米民主党関係機関へのサイバー攻撃と情報窃取、機密情報の暴露である。クリントン陣営の機密情報を入手した攻撃者は、大統領選挙期間を通じて、小出しに情報を暴露し続けた。

DNC 等へのサイバー攻撃を調査した米クラウドストライク（CrowdStrike）社は「2 つの独立した、ロシアの情報機関と関係のある敵対的存在が DNC ネットワーク上に存在」と指摘し、これらを「COZY BEAR」と「FANCY BEAR」と呼んだ[92]。前者はロシア連邦保安庁（FSB）、後者はロシア軍参謀本部情報総局（GRU）が関与するグループである。

COZY BEAR は、遅くとも 2015 年 9 月に標的型メール攻撃を端緒に DNC サーバへの侵入に成功していた[93]。他方、FANCY BEAR は 2016 年 4 月中旬に、DCCC を踏み台にし、DNC サーバに侵入した。FANCY BEAR については、26165 部隊が主に関係機関へのハッキング・情報窃取を担い、74455 部隊が機密情報の暴露を担ったと考えられる[94]。

GRU26165 部隊は 2016 年 3 月までに、クリントン選挙事務所、DCCC、DNC の関係者 300 名超にスピアフィッシングメールを送付した。このメールは、Google のセキュリティ注意喚起を模したものや「hillary-clinton-favorable-rating.xlsx」といった添付ファイルが用いられた[95]。3 月半ば、クリントン候補の選挙対策責任者のポデスタ（John Podesta）、選挙スタッフのラインハート（William Reinhart）等がスピアフィッシングメール中の偽の URL をクリックし、情報が漏えいする。

GRU は 4 月 6 日に DCCC 職員のアクセス ID とパスワードを入手し、4 月 12 日には DCCC のネットワークにマルウェア「X-Agent」を設置した。このマルウェアは、キーロガーとスクリーンショット転送機能があり、データを米アリゾナ州にある GRU が借りたサーバに転送していた。その際、GRU はマルウェア「X-Tunnel」を設置し、データを暗号化して外部に持ち出した[96]。

DCCC と DNC を兼務する職員の ID とパスワードを入手した GRU は、4 月 18 日までに DNC のネットワークに侵入し、6 月までに約 33 台のコンピュータ端末から情報を得た。DNC の端末にも DCCC と同様、「X-Agent」を設置し、DNC 内のデータを外部に転送した。GRU は DCCC と DNC のネットワーク上での情報収集にあたり、「hillary」「cruz」

---

92 Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” CrowdStrike (June 15, 2016). https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ 「FANCY BEAR」はクラウドストライク社の呼称であり、セキュリティ各社は COZY BEAR を「APT 29」（FireEye）、「CozyDuke」（Kaspersky）、FacyBear を「APT 28」（Fire Eye）、「Sofacy」（Kaspersky, paloalt）、「Threat Group-4127」（Secureworks）、「Pawn Storm」（Trend Micro）、「STRONTIUM」（Microsoft）等と呼んでいる。

93 2015 年 9 月時点で、FBI 特別捜査官 Adrian Hawkins は DNC に対して警鐘を鳴らしている。David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Scribe, 2018), pp.172-175.

94 *Indictment* (July 13, 2018), pp.1-5.

95 *Indictment* (July 13, 2018), p.7.

96 *Indictment* (July 13, 2018), p.10-11.

図１：フィッシングメールの例（ポデスタ氏に送付されたメール）

出典：Thomas Rid, “Disinformation: A Primer in Russian Active Measures and Influence Campaigns,” Hearing before the Select Committee on Intelligence, U.S. Senate, One Hundred Fifteenth Congress, First Session (March 30, 2017), p.8 より抜粋。

「trump」あるいは「Benghazi Investigation[97]」等のキーワードを検索していた。

DNC 首脳は 2016 年 4 月までに、サイバー攻撃を認識し、クラウドストライク社（起訴状では「Company 1」）に詳細調査を依頼した。この段階で、米政府は外国政府による選挙介入の「兆候」があると警鐘を鳴らしている。クラッパー（James R. Clapper）国家情報長官は 5 月 18 日、Bipartisan Policy Center での講演で、大統領選挙がサイバー攻撃を受けており、「（情報コミュニティは）いくつかの兆候を掴んでいる」と発言した[98]。

クリントンが大統領選挙における民主党候補指名を確実にした直後の 6 月 12 日、WikiLeaks 編集長のアサンジ（Julian Assange）が英国のテレビ番組で、近日中にクリントンのメールに関する公表を行うと発言した。6 月 14 日、DNC は自分達のサーバが不正侵入を受け、これは「ロシア政府によるインテリジェンス活動の一環」と発表した。同日付の『ワシントンポスト』紙が詳細を報じている[99]。

この時点でクリントンは「ニュースは不安なものだが、ショックではなかった」と振り返っている。2014 年には国務省の非機密ネットワークがロシアからの侵害にあい、被害はホワイトハウスやその他多くの議員や高官にも及び、DNC への攻撃も恒常的な攻撃の一部と考えていた[100]。

DNC 発表の翌日（6 月 15 日）、クラウドストライク社はブログ上で、前述のとおり、DNC ネットワーク上で「COZY BEAR」と「FANCY BEAR」が敵対行為をとっていると発表した。翌 16 日にはセキュアワークス（SecureWorks）社が、スピアフィッシング関連情報を分析した結果、Threat Group-4127（クラウドストライクがいう FANCY BEAR）はロシア国内で活動し、ロシア政府のために情報収集していることに「中程度の確信」とした。6 月 20 日、マンディアント社と Fidelis Cybersecurity System 社はそれぞれ、クラウドストライクの結論に同意すると発表した[101]。

---

97 2012 年、リビア東部の在ベンガジ米領事館襲撃事件に関する調査を指すと思われる。襲撃事件前より同領事館の警備強化が国務省に申請されており、襲撃事件の責任を当時のヒラリー・クリントン国務長官に問う声があった。

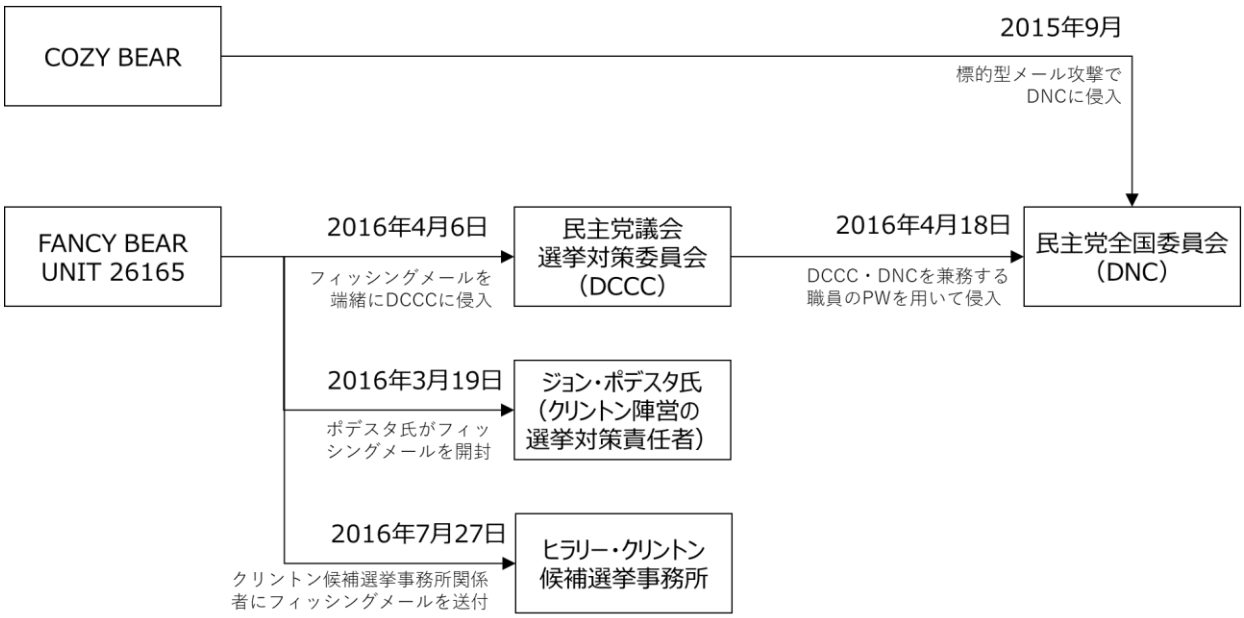
98 Nicole Gaouette, “Intel chief: Presidential campaigns under cyber attack,” *CNN* (May 18, 2016); James R. Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence* (New York: Random House, 2018), p.604.

99 Ellen Nakashima, “Russian government hackers penetrated DNC, stole opposition research on Trump,” *The Washington Post* (June 14, 2016).

100 ヒラリー・ロダム・クリントン（髙山祥子訳）『WHAT HAPPENED：何が起きたのか？』（2018 年、光文社）、374 頁。

101 “Threat Group-4127 Targets Hillary Clinton Presidential Campaign,” Secureworks (June 16, 2016); Ellen Nakashima, “Cyber researchers confirm Russian government hack of Democratic National Committee,” The Washington Post (June 20, 2016); “Findings from Analysis of DNC Intrusion Malware,” Fidelis Security Systems (June 20, 2016). マンディアント社の評価はワシントンポスト紙を参照。

図 2：FANCY BEAR と COZY BEAR による米民主党関係機関への攻撃経路



出典：U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018)で示された事実関係をもとに筆者作成。

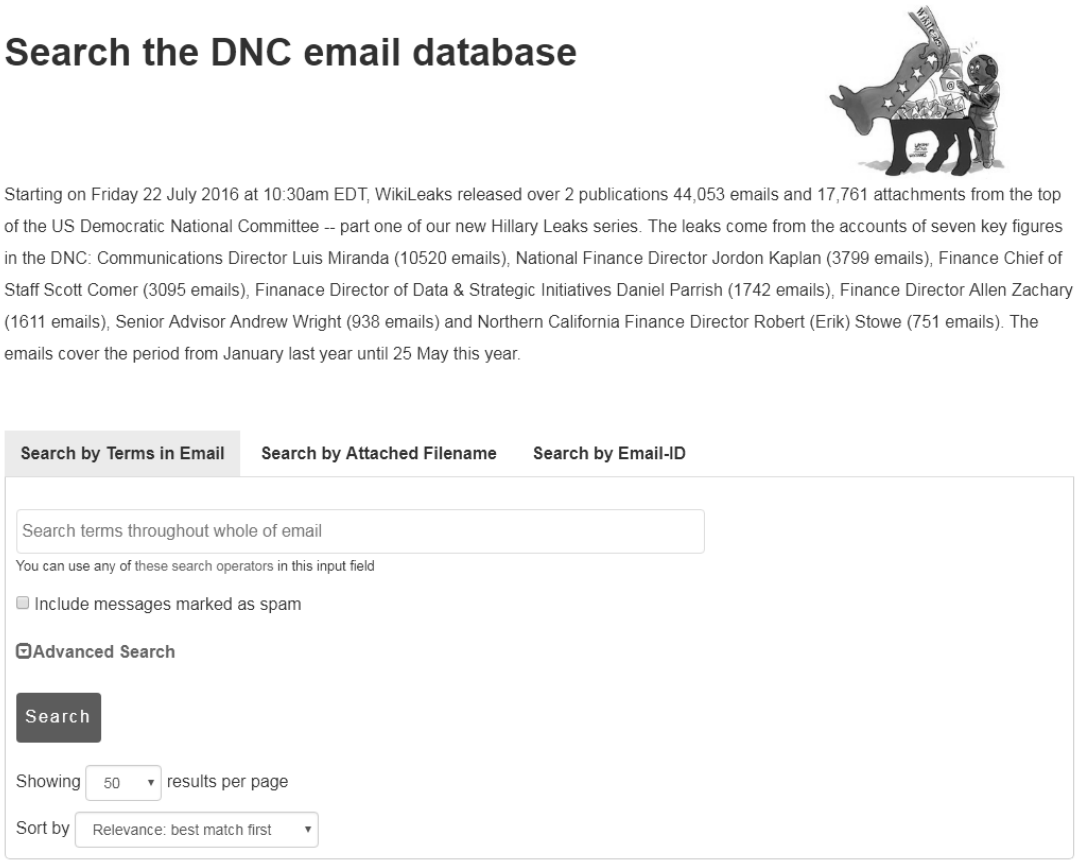
ところが、クラウドストライクの発表と同じ 6 月 15 日、「GUCCIFER 2.0」なるハッカーが自ら名乗り出て、DNC への攻撃は自分自身の単独犯行であり、DNC とクラウドストライク社の発表は嘘だと主張した。後の米国の評価では、GRU77455 部隊は「GUCCIFER 2.0」なる架空のペルソナを作り出し、サイバー攻撃で得られた機密情報を WikiLeaks に情報提供した。また GRU は「DC Leaks」というサイトを構築し、このサイト上でも選挙関連情報を暴露した[102]。

クリントンがケイン（Tim Kaine）上院議員を副大統領候補に指名すると発表した 7 月 22 日、WikiLeaks は DNC から流出したと思われるメール 20,000 点と添付ファイル 8,000 個を公開した。この情報公開によって、民主党幹部がサンダース（Bernie Sanders）候補潰しを企画し、クリントンに肩入れしたことが明らかになり、民主党内・支持者から民主党執行部への批判が高まった。結果、民主党全国大会前夜の 7 月 24 日、シュルツ（Debbie Wasserman Schultz）委員長は党大会閉幕時に同職を辞任することを発表した。

ロシアによる機密情報暴露は大統領選挙期間を通じて小出しに行われた。前述のように情報暴露は重要な政治イベントのタイミングで行われた。第 2 回大統領選挙討論会（10 月 9 日）の直前、10 月 7 日には、クリントン候補の選挙対策責任者のポデスタ（John Podesta）のメールが暴露され、投票日直前の 11 月 6 日にも新たな暴露が行われた。

[102] ODNI, *Op. Cit*., pp.2-3; *Indictment* (July 13, 2018), p.14-19.

図 3：米民主党全国委員会（DNC）の流出メールの検索画面



出典：WikiLeaks【https://wikileaks.org/dnc-emails/】より。

（2）メディアや SNS 等を通じた影響工作

さらに複雑であったのは、RT（Russia Today）やスプートニク等のメディアと SNS（Facebook, Twitter 等）上の活動を組み合わせた広範な影響工作である。ロシアは米国社会の分断と混乱、ヒラリー・クリントン候補の落選を狙って、SNS 上で政治広告を掲載し（無届での国外代理人よる米国内での政治活動）、「フェイクニュース」[103]を拡散し、国営メディアにこれを報じさせた。

IRA による影響工作

こうした活動を主に担ったのは、サンクトペテルブルクに所在する企業「インターネット・リサーチ・エージェンシー（Internet Research Agency: IRA）」である。IRA は 2013 年 7 月頃にロシアで法人登録され、現地では「Glavset」と呼ばれる。IRA は 2014 年 4 月頃までに「翻訳者プロジェクト（Project Lakhta）」と呼ばれる対米活動を企画し、Facebook や Twitter 等の SNS プラットフォームを活用し政治宣伝、政治集会の企画、特定候補の支援・中傷、世論分断を図った。米大統領選挙が佳境となる 2016 年 9 月の IRA の月額予算は 7,300 万ルーブル（約 1 億 3,000 万円）に達し、対米国担当部署では最大昼夜二交代の 80 名体制が敷かれた[104]。ただし、予算面についていえば、伝統的メディア（テレビ等）を用いるよりもはるかに安価であるといえる。

米インテリジェンス・コミュニティの報告書によれば、IRA 社の資金源は、ロシアの情報機関と密接な関係にあるプーチン大統領周辺である[105]。IRA 社は 2016 年米大統領選挙に関連し、米当局により起訴され[106]、経済制裁対象[107]となっている。

IRA の戦略を要約すれば、SNS 上の架空のペルソナがあたかも実在すると一般市民に

---

[103] *Indictment* (February 16, 2018), pp.12－23. ロシアの関与に係らず、2016 年米大統領選挙に関する広範なフェイクニュースは Liliana Bounegru, et al, *A Field Guide to "Fake News" and Other Information Disorders : A Collection of Recipes for Those who Love to Cook with Digital Methods and Other Information Disorders* (Public Data Lab., 2018), pp.24-25, 48-49,74-75, 118-119, 142-143.

[104] *Indictment* (February 16, 2018), pp.6-7.

[105] ODNI, *Op. Cit*., p.4.また IRA の概要については、次の報道を参照。「元工作員が語るロシア、デマ拡散サイバー部隊」『日本経済新聞』（2016 年 12 月 19 日）。

[106] 米司法省は 2018 年 2 月 16 日、2016 年の米国大統領選挙の介入に関する 8 件の罪で、ロシア企業 3 社とロシア人 13 名を起訴したと発表。被告らは「米国の政治システム全般と候補者への不信を拡大する」のが目標に、いわゆる「情報戦争」を遂行した。起訴された企業は、Internet Research Agency LLC (IRA)、Concord Management and Consulting LLC、Concord Catering の三社であり、起訴された人物はエフゲニー・プリゴジン（Yevgeniy Viktorovich Prigozhin）を含む。"Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," Department of Justice (February 16, 2018); U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018).
また、米司法省は 2018 年 10 月 19 日、IRA の選挙介入プロジェクト（Project Lakhta）の財政全般を統括した主任クシエノバ（Elena Alekseevna Khusyaynova）を起訴したと発表した。ただし、起訴状の日付は 9 月 28 日である。U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464 (September 28, 2018).

[107] 米財務省外国資産管理局（OFAC）は 2018 年 3 月 15 日、2016 年の米国大統領選挙の介入および別のサイバー攻撃事案（2018 年 2 月 15 日の NotPetya）に関して、ロシアの 5 団体とロシア人 19 名を制裁対象にしたと発表した。対象は、2018 年 2 月 16 日に刑事訴追された 3 団体・13 名（前掲脚注を参照）に加えて、GRU, FSB の二組織と FSB 職員 6 名である。 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," Department of the Treasury (March 15, 2018)

信じさせ、影響力を最大化すること、である。少なくともこの時点では、Facebook や Twitter がアカウントのボット判定をほとんど行っていなかったことは IRA にとって有利であった[108]。IRA は架空のペルソナを信じこませるため、選挙介入の証拠を消すため、米国市民による政治宣伝・SNS 投稿であるかのように隠ぺいを行った[109]。

IRA の（ニュースサイト等への）コメント部門で 1 日 12 時間・2 勤 2 休で約 3 か月間働いた元スタッフは、オフィスは「白を黒、黒を白と書かねばらならない場所」であり、「ある種の工場のようなもので、嘘をつき、不真実（untruths）を組み立てラインにのせていくようなもの」と語っている[110]。

写真 1：2016 年米国大統領選挙介入で SNS 上の影響工作を担った組織（Internet Research Agency: IRA）が入居していたと報道された建物

出典：筆者撮影（初出：土屋大洋「ロシアでサイバーセキュリティが議論されない理由」Newsweek 日本版（2017 年 12 月 25 日））。

[108] Sanger, *Op. Cit*., pp.184-185.
[109] IRA 他は、実在する米国人の氏名、顔写真、生年月日、社会保障番号を（一部は不正に）入手し、SNS 上で情報発信を行うことで、米国内から発信されたものであるかのように偽装した。また彼らは米国の祝日、東西海岸のタイムゾーンにあわせて、SNS への投稿日時・内容にも注意を払った。同時に、IRA 他は 2014 年までに米国を訪れ、SNS 投稿用と思われるカメラ、使い捨て携帯電話、SIM カード等の物資を調達した。*Indictment* (February 16, 2018), pp.12-19.
[110] Anton Troianovski, “A former Russian troll speaks: ‘It was like being in Orwell’s world’,” *The Washington Post* (February 17, 2018).

IRA は特定候補を支援・攻撃しただけではなく、様々な政治争点で社会・世論を分断しようと試みた。一般論として、影響工作は必ずしも、単一の候補者・政党・政策を支援するものではない。影響工作は「社会の異なる政治グループ間での緊張を煽るため、SNS のプラットフォームを利用し、ユーザの政治的および人口動態上の分析結果に基づいて、異なるグループに同時にメッセージ（時には欺瞞情報）を発信する」ことを含む。例えば、大統領選挙直後の 11 月 8 日、IRA は、Facebook 上でトランプ支持者と反トランプ支持者の集会を、同じ 11 月 12 日にニューヨークで開催することを企画した[111]。

分断の対象は共和党員・支持者と民主党員・支持者、トランプ支持者とクリントン支持者だけだはなく、所得階層、性別、民族・人種、銃規制、妊娠・中絶等の様々であった。実際、米上院情報特別委員会に提出された報告書によれば、IRA が投稿したポストのうち、直接「クリントン」「トランプ」といった言葉が使われたのは全体の約 10%以下である（表 2 を参照）。同報告書および別の報告書によれば、IRA は特にアフリカ系米国人やその他マイノリティグループ（ムスリム、LGBT）に焦点を当てていた[112]。

CSIS のスポルティング（Suzanne Spaulding）によれば、ロシアの狙いは、民主主義に透明性を与え、変革をもたらす「抗議行動（protest）」ではない。ロシアの戦略的目標はマイノリティグループに対して抗議行動を促すのではなく、社会に混乱を引き起こし、民主主義や制度の変化に対する失望をもたらすことである[113]。

表 2：IRA が投稿したポストと「クリントン」「トランプ」に関する言及

		Facebook	Instagram	Twitter
総ポスト数		61,483	116,205	10,401,029
「クリントン」に言及したポスト	ポスト数	1,777	7,915	198,123
	対全体比	2.9%	6.8%	1.9%
「トランプ」に言及したポスト	ポスト数	2,563	13,106	430,185
	対全体比	4.2%	11.3%	4.1%

出典：Renee DiResta, et.al., *The Tactics & Tropes of the Internet Research Agency* (New Knowledge, December 2018), p.76.

111 *Indictment* (February 16, 2018), p.23; *Report of the Attorney General's Cyber-Digital Task Force*, p.2.
112 Renee DiResta, et.al., *The Tactics & Tropes of the Internet Research Agency* (New Knowledge, December 2018); Philip N. Howard, et.al., *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (University of Oxford, December 2018)
113 Suzanne Spaulding, "Why Putin Targets Minorities," Center for Strategic and International Studies (December 21, 2018)

IRA は大量の政治広告を購入し、前述の特定の社会グループに対してメッセージを発信した。米下院情報問題常設特別調査委員会（HPSCI）は 2018 年 5 月 10 日、IRA による政治公告約 3,500 点（2015 年第 2 四半期から、2017 年第 4 四半期までに確認されたもの）を公開した。

表 3：Facebook 上の政治広告（ターゲティング広告）［再掲］

投稿イメージ	メタデータ
	Ad ID 467 Ad Text America has always been hinged on hard-working people. If you remove jobs you'll remove our country from the world map. The state of Pennsylvania rose owing to multiple enterprises mining coal, producing steel, and creating the need for other jobs, groceries, doctors, dentists, insurance, gas, vehicles, mechanics and the list goes on. As far as Mr. Trump pursues the goal of creating more jobs and supports the working class. He said he would put miners back to work. We could help Mr. Trump win Pennsylvania which is a battleground state. We'd like to organize a rally "Miners for Trump" in Pennsylvania. Have something against coal industries? Please note then that burning coal is not more harmful than lumber. Alternative energy is only possible when subsidized by government for it is not lucrative. You cannot leave tens of thousands of people without a job just because of lobbyists' interests. The current list of locations is being elaborated. Suggested cities are Erie, Pittsburg, Scranton, Harrisburg, Allentown, and Philly. Confirmed locations: Marconi Plaza, Philadelphia. Miners for Trump: Unity day in Pennsylvania Ad Landing Page https://www.facebook.com/events/312522819127036/ Ad Targeting Location - Living In: United States: New York (+50 mi) New York Age: 18 - 65+ Placements: News Feed on desktop computers or News Feed on mobile devices Ad Impressions 2 Ad Clicks 0 Ad Spend 2.96 RUB Ad Creation Date 09/22/16 05:01:05 AM PDT Ad End Date 10/01/16 01:00:00 PM PDT

出典：The House Permanent Select Committee on Intelligence, Social Media Advertisements

表 4：IRA が投稿したメッセージ

推定日時	宣伝内容の抜粋
4 月 6 日	多くの黒人が我々の#HillaryClintonIsNotMyPresident を支援してくれる。
4 月 7 日	私はヒラリー・クリントンに反対する。ごまかしに反対する。
4 月 19 日	我々の#HillaryClintonForPrison2016 に参加しよう
5 月 10 日	ドナルドはテロリストを打ち負かそうとしている…ヒラリーはテロリストを支援しようとしている。
5 月 19 日	共和党に投票しよう、トランプに投票しよう、銃器規制に反対しよう！
5 月 24 日	ヒラリー・クリントンは黒人が投票すべき候補者ではない。
6 月 7 日	トランプはより良い未来のため唯一の希望だ。
6 月 30 日	"#NeverHillary #HillaryForPrison #Hillary4Prison #HillaryForPrison2016 #Trump2016 #Trump #Trump4President"
7 月 20 日	オハイオ州は、ヒラリーを監獄に入れることを望む。
8 月 4 日	ヒラリー・クリントンは既にアイオワ州の民主党コーカスで有権者に詐欺を働いた。
8 月 10 日	ヒラリーは信用できない。我々退役軍人を無視するな！
10 月 14 日	あらゆる候補者の中で、ドナルド・トランプだけが唯一、テロリストから警察を守ることができる。
10 月 19 日	ヒラリーは悪魔（Satan）だ。彼女の罪と嘘はその邪悪さを証明している。

日時は全て 2016 年のもの。ハッシュタグ（#）以下は原語を記載した。

出典：U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018), p.20.

IRA による SNS 上での影響工作の正確な規模は分からない。しかし、2017 年 11 月 1 日に開催された下院情報委員会公開公聴会で、SNS 大手三社、すなわち Facebook 社（Instagram サービスを運営）、Twitter 社、Google 社（YouTube サービスを運営）は外国勢力による政治広告やプロパガンダの規模について指摘している。必ずしも大統領選挙期間とは一致しないが、おおよその規模は把握できる。米国の登録有権者が 2 億人、2016 年選挙で実際に投票に向かったのが 1 億 3,900 万名であることを踏まえると大きな数字である。全てのコンテンツが同様の拡散効果・曝露量をもったわけではないが、Facebook で最もシェアされたコンテンツは 640,390 のシェアを得た（図 3 を参照）。

Facebook ［期間：2015 年 6 月から 2017 年 8 月］

- IRA が購入した政治広告： 3,393 点
- IRA の政治広告を視聴した米国人： 1,140 万人
- IRA が関与した Facebook アカウント： 470
- IRA が作成したページ数： およそ 120
- IRA が作成したページ上のコンテンツ： 80,000 超
- IRA のコンテンツを視聴したであろう米国人： 1 億 2,600 万人

Twitter ［期間：2016 年 9 月 1 日から 11 月 15 日］

- 選挙について投稿したロシアに関連するボットアカウント： 36,746
- 左記期間における投稿数： 140 万件
- 左記期間においてボットの投稿の視聴数： 2 億 8,800 万ビュー
- 特定された IRA 職員が人力で操作したアカウント数： 2752 件
- 左記期間における IRA 関連アカウントの投稿数： およそ 131,000 件[114]

YouTube（Google）［期間：不明］

- ロシアが関与した投稿ビデオ数： 1,108 件
- ロシアが関与した投稿ビデオの視聴数： およそ 309,000 ビュー
- ロシアトゥデイ（RT）のチャンネル視聴数： 50 億ビュー超

出典：HPSCI Minority Staff, HPSCI Minority Exhibits During Open Hearing (November 1, 2017)
https://democrats-intelligence.house.gov/uploadedfiles/hpsci_minority_exhibits_memo_11.1.17.pdf
the House Permanent Select Committee on Intelligence, Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements (May 10, 2018)
https://democrats-intelligence.house.gov/social-media-content/default.aspx

[114] なお、Twitter 社による 2016 年米大統領選挙の振り返りは以下を参照。Twitter Public Policy, “Update on Twitter’s review of the 2016 US election,” Twitter Blog (Updated on January 31, 2018).
https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html

図 4：IRA が投稿し Facebook で最もシェアされたコンテンツ（2016 年 11 月 8 日以前）

2016 年 9 月 8 日に投稿され、640,390 のシェアを得た投稿。

テキスト：“At least 50,000 homeless veterans are starving dying in the streets, but liberals want to invite 620,000 refugees and settle them among us. We have to take care of our own citizens, and it must be the primary goal for our politicians!

テーマ：anti-immigrant, nationalist, frames, immigration as veterans versus immigrants

出典：Philip N. Howard, et.al., *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Appendix (University of Oxford, December 2018), p.5.

RT やスプートニクによる影響工作

IRA に加えて、RT（Russia Today）[115]やスプートニク（Sputnik）[116]も対米影響工作で大きな役割を担った[117]。第一に、SNS 上のプロパガンダと米大手メディアを繋ぐ「媒介」としての役割である。「ローマ教皇がトランプ候補を支持した」等の荒唐無稽なフェイクニュース（図 5 を参照）、RT やスプートニクがこうしたニュースを報じても選挙に大きな影響があった訳ではないが、米国のメディアが「RT やスプートニクが報じたニュース」を報じた際は影響があった。

クリントンは次のように振り返っている。

> *RT の影響力がどの程度なのかは分からない。…中略… RT の影響力は想像以上なのかもしれないが（たぶん数十万くらいか）、選挙結果そのものを左右するほどのものではないだろう。だが、RT の宣伝工作がアメリカの FOX ニュースやブライトバード、＜アレックス・ジョーンズのインフォウォーズ＞などのメディアにとりあげられ、フェイスブックにのったら、その影響力は格段に上がる。それが選挙運動中に頻繁に起きた。*[118]［傍点強調は筆者による］

---

[115] RT は 2005 年 12 月 10 日に開局したニュース専門の放送局である。ODNI 報告書によれば、RT 編集長のシモニャン（Margarita Simonyan）はロシア政府と密接なつながりがあり、コントロール下にあると指摘されている。ODNI, *Op. Cit.*, p.9.

[116] スプートニクは 2014 年 11 月 10 日設立に設立された通信社である。スプートニクが運営する「ラジオ・スプートニク」は、「ロシアの声（Voice of Russia）」を継承した。スプートニクは、ロシア政府が所有する国営通信社「ロシアの今日」の傘下企業である。なお、「ロシアの今日」は、テレビ放送ネットワーク「RT」とは異なる組織だが、2013 年 12 月 31 日以降、「ロシアの今日」および「RT」の編集長をシモニャンが兼務する。なお、スプートニクは 2015 年 3 月 20 日、日本語ニュースサイトを開設している。

[117] 正確にいえば、2017 年 1 月 6 日の ODNI 報告書は、IRA（2 段落分）よりも RT やスプートニク（8 頁分）に紙幅を割いている。ODNI, *Op. Cit.*, pp.3-4, 6-12. ただし、これは 2017 年 1 月時点で判明した事実関係に基づくものであり、その後、米当局や議会は IRA の活動に関する公式文書を数多く公開している。例えば、U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF (February 16, 2018).

[118] クリントン、前掲書『WHAT HAPPENED』、397 頁。

図 5：フェイクサイト「WTOE5News」が報じた「ローマ法王がトランプ候補を支持」

＜WTOE5News が報じた内容＞

News outlets around the world are reporting on the news that Pope Francis has made the unprecedented decision to endorse a US presidential candidate. His statement in support of Donald Trump was released from the Vatican this evening:

> I have been hesitant to offer any kind of support for either candidate in the US presidential election but I now feel that to not voice my concern would be a dereliction of my duty as the Holy See.

フェイクサイト「WTOE5News」は既に閉鎖されており、テキストの出典は Dan Evon, "Pope Francis Shocks World, Endorses Donald Trump for President," *Snopes* (July 10, 2016)
※Snopes はフェイクニュース検証サイト。

RT やスプートニクの第二の役割は、単独としての情報活動である[119]。遅くとも 2016 年 3 月以降、反クリントンキャンペーンを展開した。RT はニュース専門放送局であるが、SNS 上での情報発信に注力した。RT および RT America、その他の大手放送局 3 社（Al Jazera English、BBC World、CNN および CNN International）の SNS 上の視聴者を比較した結果、YouTube では RT および RT America の視聴者が、その他大手 3 社を上回った（Facebook や Twitter では、その他大手 3 社に大きく劣後）[120]。

例えば、RT は 2016 年 8 月 6 日、「アサンジ特集：ウィキリークスはクリントンを投獄できる E メールを持っているのか？」「クリントンとイスラム国の資金源は同一」と題された英語版動画を公開した。最も視聴された別の動画「クリントン財団への『慈善寄付』は全てクリントン夫妻の懐へ…（"How 100% of the Clintons' 'Charity' Went to…Themselves"）」（2016 年 8 月 16 日公開）は SNS 上で 900 万人が視聴した[121]。この動画には、次のような説明が付記されている。

> *2015 年、クリントンは慈善寄付金として 104 万 2,000 ドルを入手した。そのうち、100 万ドルはクリントン財団（the Clinton Family Foundation）に渡り、［クリントン夫妻は］資金の流れをコントロールできた。つまり、2015 年のクリントン慈善寄付金の 96%は自らの懐に入った。市民は 1%［の富裕層］が作り出す完全な富の循環、クリントン夫妻が支配する循環を打ち壊す*[122]。

[119] ODNI, *Op. Cit*., pp.3-4, 6-12.
[120] ODNI, *Op. Cit*., pp.10-11.
[121] ODNI, *Op. Cit*., p.4.
[122] RT America, "How 100% of Clintons' 2015 charity went to themselves," YouTube (August 16, 2016) https://www.youtube.com/watch?v=62uOVU6QXss

（3）選挙関連システムへのサイバー攻撃

以上は、有権者の投票行動を左右し、米国社会を分断するための介入といえる。これらに加えて、選挙関連システム自体への攻撃も確認された。

第一に、投票結果・集計結果の改竄や投開票の妨害である。これはオバマ政権、（オバマ大統領自身を含む）が最も懸念した攻撃である。結果として、投票集計（vote tallying）システムへのサイバー攻撃や改竄は成功しなかったと評価された[123]。

選挙期間中の 2016 年 8 月時点で、選挙システムの脆弱性については、国土安全保障省のジョンソン（Jeh Johnson）長官が調査を行い、最終的には「不可能ではないが、可能性は低い」との結論に達した。しかし、投票システムへの攻撃はオバマ大統領の懸案事項であった[124]。オバマ大統領の外交政策担当スピーチライターを勤めたローズ（Benjamin Rhodes）によれば、オバマ大統領が 11 月 8 日以前の対露制裁を決定しなかったのは「対露制裁は、大統領選挙当日、ロシアによる投票結果へのサイバー攻撃を招くと信じていたから」と指摘する[125]。また、クラッパー国家情報長官は、対露制裁が米国の電力インフラへの攻撃を招くのではないか、との懸念を表明したと報じられた。例え数時間・局所的であっても、投票日当日に停電が発生すれば、大統領選挙の信頼性が損ねられる[126]。

第二に、ウェブサイトの脆弱性を利用し、米国各州の選挙管理委員会ウェブサイト等への攻撃である。ロシアは 2014 年初期には米国の選挙プロセスと関連する技術インフラの調査を開始した[127]。国土安全保障省のサイバーセキュリティ・コミュニケーション担当次官補マンフラ（Jeanette Manfra）は、ほとんどの攻撃は成功しなかったが、21 の州のインターネット接続された選挙関連ネットワークが攻撃されたことを明らかにした[128]。

7 月 13 日起訴状によれば、GRU はある州（アリゾナ州またはイリノイ州と考えられる）の選挙管理委員会のウェブサイトを攻撃し、約 50 万名の有権者情報（氏名、社会保障番号、生年月日等）を窃取した[129]。有権者情報を窃取した目的は定かではないが、①有権者情報を分析し、属性に応じた SNS 上の影響工作に活用した、②有権者登録を改竄・抹消し、投票場での混乱を狙った等の可能性がある。

第三に、選挙インフラに関する企業への攻撃である。GRU は 2016 年 8 月、有権者登

---

123 ODNI, *Op. Cit*., p.3.　選挙インフラに対する攻撃の総括、対応については次のものを参照。Russian Targeting of Election Infrastructure During the 2016 Election:　Summary of Initial Findings and Recommendations (May 8, 2018)
https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf

124 Michael Isikoff & David Corn, *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump* (New York: Twelve, 2018), pp.312-315; Sanger, *Op. Cit*., pp.221-222

125 Peter Baker, “How Trump’s Election Shook Obama: ‘What if We Were Wrong?’,” *New York Times* (May 30, 2018).

126 Isikoff & Corn, *Op. Cit.*, pp.325-326; Sanger, *Op. Cit*., pp.225-226.

127 ODNI, *Op. Cit*., p.3.

128 “Written testimony of I&A Cyber Division Acting Director Dr. Samuel Liles, and NPPD Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra,” The Department of Homeland Security (June 21, 2017).

129 *Indictment* (July 13, 2018), pp.25-26.

録情報を検証するソフトウェアベンダーの端末にサインバー攻撃を仕掛けた。そして、2016 年 11 月頃あるいはそれ以前に、このベンダー企業のメールを模し、この企業のロゴを用いた WORD 文書を偽装し、選挙関係者 100 名以上にスピアフィッシングメールを送った[130]。後に NSA から機密文書が漏洩し、この企業はフロリダ州にある選挙システムベンダーVR System と報じられている[131]。

[130] *Indictment* (July 13, 2018), pp.25-26.
[131] Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept* (June 6, 2017).

別紙 2：2016 年米大統領選挙に関する推移

※ 当該機関による公式発表（ウェブサイト上でのプレスリリース等）がないもの、分かりにくいものについては出典を記載。出典詳細は表の末尾に記載。

表：ロシアによる 2016 年米国大統領選挙介入と米国の対応に関する推移

時期	概要	出典
2015 年 9 月頃	FBI が DNC テクニカルサポート部門に対して、ロシアからのサイバー攻撃に関する警鐘を鳴らす（ただし、これはロシア GRU ではなく、ロシア FSB と関係にある攻撃グループ Cozy Bear に関する警鐘。Cozy Bear は 6 月に DNC ネットワークに侵入）。	1
2016 年 3 月頃	DNC が、クリントン選挙事務所の弁護士マーク・エリアス（Marc Elias）にサイバー攻撃に関する警鐘を鳴らす。	2
3 月中旬	GRU が DNC、DCCC、ヒラリー・クリントン事務所関係者計 300 名超にスピアフィッシングメール（Gmail からの PW 変更要求を模したもの等）を送付。	3
3 月 19 日	クリントン候補の選挙対策責任者ポデスタ（John Podesta）がロシアからのスピアフィッシングメールを開封。メール受信時、懸念を感じたポデスタは IT 担当スタッフに確認したが、スタッフは「illegitimate（不正な）」と書くべきところを誤って「legitimate（本物の）」と書いた結果、ポデスタがメールを開封。結果的に約 50,000 通のメールが漏洩。	4
3 月 22 日	元 DNC 地方現地責任者（a former DNC regional field director）でクリントン選挙事務所選挙スタッフのラインハート（William Reinhart）がスピアフィッシングメールを開封する。	5
4 月 6 日	GRU が DCCC 職員のアクセス ID とパスワードを入手。	6
4 月 12 日	GRU が DCCC のネットワークにマルウェア「X-Agent」を設置。このマルウェアは、キーロガーとスクリーンショット転送機能があり、データを米アリゾナ州にある GRU が借りたサーバに転送。	7
4 月 18 日	GRU が DCCC と DNC を兼務する職員の ID とパスワードを入手し、4 月 18 日までに DNC のネットワークに侵入し、6 月までに約 33 台のコンピュータ端末から情報を得る。DNC の端末にも DCCC と同様、「X-Agent」を設置。	8
4 月中	DNC 幹部が、DNC ネットワークへの侵入を知る。その後、CrowdStrike に調査と対処を依頼。	9
5 月 4 日	共和党候補者のテッド・クルーズ（Ted Cruz）議員が共和党予備選挙からの撤退を表明したため、トランプが事実上の共和党指名を確実にする。	

時期	概要	出典
5 月 18 日	クラッパー（James Clapper）国家情報長官（DNI）が Bipartisan Policy Center での講演で、大統領選挙がサイバー攻撃を受けており、“We‘ve already had some indications of that” と発言。DNI 室の公共部門長 Brian P. Hale も Twitter 上で同主旨の声明を発表。	10
6 月 6 日	民主党予備選挙で、クリントン候補以外の主要候補が選挙戦から撤退したため、ヒラリー・クリントン候補の民主党候補指名が確実となる。	
6 月 12 日	WikiLeaks 編集長のアサンジ（Julian Assange）が英国の TV で、「近日中にクリントン候補のメールに関する公表を行う」と発言。	
6 月 14 日	DNC が、DNC サーバ不正侵入について、「ロシア政府によるインテリジェンス活動の一環」と発表。同日、WP 紙が詳細報道。	11
6 月 15 日	セキュリティ会社 CrowdStrike がブログ上で 2 つのハッキンググループ（Cozy Bear と Fancy Bear）について指摘。	12
6 月 15 日	GUCCIFER 2.0 を名乗るハッカーが名乗り出て、自分は単独犯であり、DNC と CrowdStrike の発表は嘘だと主張。　※後に米国は、GRU77455 部隊が、モスクワ時間の 6 月 15 日 16 時 19 分から 16 時 56 分に、実在するルーマニア人ハッカー「GUCCIFER」を模した「GUCCIFER 2.0」なるアカウントを作成したと断定。	13
6 月 16 日	Secureworks 社が、スピアフィッシング関連情報を分析した結果、Threat Group-4127（CrowdStrike がいう FANCY BEAR に相当）はロシア国内で活動し、ロシア政府のために情報収集していることに「中程度の確信」と発表。	14
6 月 20 日	Mandiant 社と Fidelis Cybersecurity System 社が、6 月 15 日に発表された CrowdStrike の結論に同意すると発表。	15
7 月 5 日	コミーFBI 長官がクリントン候補の E メール疑惑に関する捜査 (注) を終了すると発表。 (注) クリントン候補が、国務長官時代に私的メールサーバで機密情報を取り扱っていたことに関する件。FBI による捜査は 2015 年 7 月 10 日に開始された。	
7 月 12 日	バーニー・サンダース（Bernard Sanders）候補がヒラリー候補支持を明言するも、形式的には予備選挙からは撤退せず。	
7 月 18 日 ～7 月 21 日	共和党全国大会	
7 月 22 日	クリントン候補が、ケイン（Tim Kaine）上院議員を副大統領候補に指名（正式指名は 7 月 27 日の民主党全国大会）。	
7 月 22 日	WikiLeaks が DNC から流出したと思われるメール 20,000 点と添付ファイル 8,000 個を公開。	

時期	概要	出典
7 月 24 日	民主党全国大会前夜、シュルツ（Debbie Wasserman Schultz）委員長が党大会閉幕時に同職を辞任することを発表。理由は、WikiLeaks 上の公開メールにより、民主党幹部がサンダース（Bernie Sanders）を潰し、ヒラリー・クリントンに肩入れしたことが明らかになり、民主党内・支持者から批判が高まったため。	
7 月 25 日 ～7 月 28 日	民主党全国大会	
7 月 26 日	CIA が DNC への攻撃にロシア政府が関与していることについて、HUMINT も含めて「高い信頼性（high confidence）」と評価した、と報じられる。	16
7 月 26 日	NBC News のサバンナ・ガスリー（Savannah Guthrie）がオバマ大統領に「サイバー攻撃と暴露の背景にはロシアがいるのか？　彼らは大統領選挙を妨害しようとしているのか？」と質問し、オバマ大統領は、FBI が調査中であるとしながらも「専門家はこの件の実行者をロシア人と特定した（experts have attributed this to the Russians）」と回答。	17
7 月 27 日	クリントン個人事務所が利用するサードパーティメールが初めてフィッシングメールを受信。 同時期、クリントン候補の選挙キャンペーン関係者 76 のメールアドレスがフィッシングメールを受信。	18
7 月 31 日	クリントン候補が FOX ニュースによるインタビューで、DNC へのサイバー攻撃にロシアの情報機関が関与したと明言。	19
8 月 4 日	8 月 4 日のブレナン（John O. Brennan）CIA 長官が、ボルトニコフ（Alexander Bortnikov）FSB 長官との定例電話会談で「介入は確実に backrfire をもたらす」と警告（最初の米政府公式の警告）。	20
8 月半ば	ホワイトハウス国家安全保障会議（NSC）内でロシアへの複数の対抗措置が議論される。	
8 月末	クラッパー国家情報長官が米議会「8 人衆（gang of eight）」[注]にブリーフィングを行う。「8 人衆」が協議の結果、民主党ハリー・リード（Harry M. Reid）上院議員がコミーFBI 長官に書簡を送付。 [注] 上下院の共和党・民主党それぞれの院内総務、院内幹事、上下院の情報委員会の委員長、副委員長の 8 人。	21
9 月上旬	コミーFBI 長官が自身の署名入り原稿（ロシアによる干渉、国民向けの警鐘）を準備するも、公開されず（オバマ政権は公開決定を下さず。コミー長官によれば、オバマ大統領が非公開を決定したのは、各紙の世論調査がクリントン候補圧勝を報じていたため）。	22
9 月 5 日	中国・杭州で開催された G20 サミットで、オバマ大統領がプーチン大統領に「サイバー攻撃をやめろ。さもなければ大変な事態になる」と警告。記者会見でオバマ大統領は、米国が攻撃的なサイバー戦能力を保有していることを示唆。	23

時期	概要	出典
9 月 5 日	ワシントンポスト紙が「ロシアによる大規模サイバー攻撃が進行」と報道。	24
9 月 7 日	クラッパー国家情報長官が、オバマ大統領が"Experts have attributed this to the Russians"と言及したことを指摘した上で、「FBI が調査している間、私はオバマ大統領の指摘以上のことは言えない。しかし、別の点は繰り返し述べることができる。ロシアは常に、政府だけではなく、企業や個人のシステムにもハックしている」と述べる。	25
9 月 11 日	クリントン候補が「トランプ支持者は哀れ（basket of deplorables）」と発言。	
9 月 22 日	上下院の情報特別委員会所属の民主党議員ダイアン・ファインスタイン（Dianne Feistein）上院議員とアダム・シフ（Adam Sciff）下院議員（いずれもカリフォルニア州選出）は以下の声明を発表。 • 我々が受けたブリーフィングによれば、ロシアの情報機関が米国大統領選挙に対して、重大で組織的な介入を行っている。 • 我々は、ロシアの情報機関に対する指示は、ロシア政府の最高上位レベル（very senior levels of the Russian government）しか下せないと考えている。	26
9 月 26 日	大統領選挙第 1 回テレビ討論会	
10 月 7 日	午後 15 時、クラッパー国家情報長官とジェイ・ジョンソン（Jeh Johnson）国土安全保障長官が、共同会見を実施し、政府としては初めて公式的にロシアによる選挙介入に言及。要旨は以下のとおり。 • 米国情報コミュニティは、米国人や政治組織を含む米諸制度に対する最近の E メールの侵害はロシア政府が指示したと確信している。DCLeaks.com や WikiLeaks 上、または Guccifer2.0 による E メール暴露は、ロシアによる直接的努力の手法と動機と一致している。 • こうした情報窃取と暴露は、米国の選挙プロセスを妨害することを意図したものである。 • 米国情報コミュニティはこうした努力の規模と機微度をふまえて、こうした活動はロシアの最高指導部（Russia's senior-most officials）のみが許可できると考えている。 • いくつかの州では、選挙関連システムに対する侵入調査（scanning and probing）が確認されており、活動の多くはロシア企業が運営するサーバに起因する。しかし、現時点ではこうした活動がロシア政府によるものだとは考えていない。 • 米国情報コミュニティと国土安全保障省の評価によれば、（中略）投票数や選挙結果の改竄は極めて困難である。 ※ 共同会見は、ロシア系メディアや SNS 上の欺瞞情報流布には触れていない。なお、コミーFBI 長官は FBI の政治的中立性を主張し、参加せず。	27
	午後 16 時 5 分、ワシントンポスト紙が、トランプ候補の女性侮辱発言（音声）を公開（いわゆる「Access Hollywood」問題）。	

時期	概要	出典
	午後 16 時 30 分、WikiLeaks 上で、クリントン候補の選挙対策責任者ポデスタ氏のメールが暴露される。 ※3 月 19 日に侵入を受けていたもの。	
10 月 9 日	大統領選挙第 2 回テレビ討論会	
10 月 11 日	ジョシュ・アーネスト（Josh Earnest）報道官が、大統領専用機内で記者団に対して、「大統領はとりうるいくつかの対応を持っているし、相応の対応措置を検討している」「対抗措置を予め発表することはないだろう」「大統領は、決して我々が公表しない対応措置を選択することも可能だ」「大統領はこれまで、連邦政府は米国のシステムを防衛するだけではなく、海外において攻撃的作戦を遂行するための際立った能力も保有している、と語ってきた。とりうる対抗措置は様々なものがあり、何が適切かは大統領が決める」と述べる。翌 12 日のプレスブリーフィングでも同様の趣旨を述べ、「確実なことは、米国のシステムを守り、米国の政治システムや政治プロセスを損ねようとするロシアの試みを妨害するため、あらゆる資源を動員するという点だ」と述べる。	28
10 月 14 日	オバマ政権が情報機関に対してロシアへの報復オプション検討を指示したと報じられた。ジョー・バイデン（Joe Biden）副大統領が 10 月 14 日のテレビ番組 Meet the Press に出演し、「（プーチン大統領）にメッセージを送っている」「米国の選択の時であり、甚大な結果をもたらす状況」と発言。	29
10 月 19 日	大統領選挙第 3 回テレビ討論会	
10 月 28 日	コミーFBI 長官が議会に書簡を送付し、記者会見を実施。新たな証拠が発見されたため、クリントン候補の E メール問題に関する捜査を再開すると発表。	
10 月 30 日	民主党ハリー・リード（Harry M. Reid）上院議員がコミーFBI 長官に然るべく対処を求める書簡を送付。	
10 月 31 日	オバマ大統領がホットラインでプーチン大統領に電話をかけ、選挙介入を辞めなければ深刻な結果になると伝える。	30
	マザー・ジョーンズ誌が、ロシア政府によるトランプ陣営支援を扱った「スティール文書」[注]の内容を初めて報道。 [注] 元英国秘密情報部（Secret Intelligence Service: SIS）職員で英企業 Orbis Business Intelligence 所属のスティール（Christopher D. Steele）が 2016 年 6 月から 11 月までに作成した 16 本のメモ。	31
11 月 6 日	コミーFBI 長官が議会に書簡を送付し、記者会見を実施。新たな証拠を精査した結果、FBI は 7 月 5 日の結論を変えないと発表。	

時期	概要	出典
11 月 8 日	米大統領選挙投票日。トランプ候補が第 45 代合衆国大統領に選出される。獲得選挙人は、トランプ候補が 306 名、クリントン候補が 232 名（ただし、12 月 19 日の選挙人投票では、選挙人 7 名が誓約違反を行い、トランプ候補が 304 票、クリントン候補が 227 票を獲得）。	
12 月上旬	CIA が、ロシアによる選挙介入は単に「米国の選挙制度の信頼を貶める」事にとどまらず、「2016 年大統領選挙においてトランプを勝たせる」事を目的としていたと結論づけ、コミーFBI 長官とクラッパー国家情報長官は CIA の評価に同意した、と報じられる。	32
12 月 9 日	オバマ大統領は情報機関に対して、（オバマ自身が当選した）2008 年の大統領選挙まで遡って「外国勢力による選挙介入の有無」の調査を指示し、自身が退任する 1 月までに報告を求める。	
12 月 29 日	オバマ大統領が以下の対ロシア制裁を発表。 （1） ロシア軍参謀本部情報総局（GRU）、連邦保安庁（FSB）、GRU を支援した 3 つの企業、GRU 幹部 4 人の制裁対象指定（E.O.13964 で規定されていないサイバー攻撃。 E.O.13757 で新たに規定した「選挙プロセス・制度へのサイバー攻撃」） （2） ロシア人 2 名の制裁対象指定（E.O.13964 で規定されたサイバー攻撃） （3） ロシア諜報機関が利用していたメリーランド州とニューヨーク州の施設 2 カ所の閉鎖 （4） 米国駐在のロシア外交官 35 人の国外退去（persona non grata） （5） ロシアがサイバー活動で用いた技術情報の公開（DHS と FBI の共同発表）	33
2017 年 1 月 5 日	クラッパー国家情報長官、ブレナン CIA 長官、コミーFBI 長官、ロジャース NSA 長官が、ロシアによる選挙介入に関する調査結果をオバマ大統領に報告。	
1 月 6 日	クラッパー国家情報長官、ブレナン CIA 長官、コミーFBI 長官、ロジャース NSA 長官が、ロシアによる選挙介入に関する調査結果を議会「8 人衆」に報告。その後、ニューヨークに移動し、トランプ・タワーにて、トランプ次期大統領に同様の調査結果を報告。 その後、コミーFBI 長官が単独でトランプ次期大統領に対して、今後報道される予定のスティール文書の一部（2013 年、トランプがモスクワ市内のホテルでコールガールと興じている様子がロシア側に盗撮されたとの情報）についてブリーフィングを行う。	34
	国家情報長官室（ODNI）が米国の複数情報機関の評価結果として、報告書「最近の米国選挙におけるロシアの活動と意図に関する評価」を公表。	35
	米国土安全保障省が、選挙関連インフラを重要インフラ「行政」の下部インフラに指定。	

時期	概要	出典
1 月 10 日	バズフィードが「スティール文書」の原本とともに、トランプ陣営とロシア政府の共謀、ロシアがトランプ大統領の弱みを握っている疑惑（1 月 6 日にコミーFBI 長官がトランプ大統領にブリーフィングした内容）について報道。	36
5 月 17 日	米司法省が、ロシア政府とトランプ陣営の共謀に関する捜査のため、モラー（Robert Swan Mueller III）元 FBI 長官を特別検察官に任命。	
10 月 30 日	モラー特別検察官が、大統領選挙期間中のトランプ陣営選挙対策本部長だったマナフォート（Paul J. Manafort, Jr.）、その代理人だったゲーツ（Rick Gates）、外交顧問を務めたパパドプロス（George D. Papadopoulos）を起訴。	
12 月 1 日	モラー特別検察官が、フリン（Michael T. Flynn）前国家安全保障問題担当大統領補佐官を起訴。	
2018 年 2 月 16 日	米司法省は、米大陪審が 2016 年の米国大統領選挙の介入に関する 8 件の罪で、ロシア企業 3 社とロシア人 13 名を起訴したと発表。起訴内容は主に、SNS 上での偽情報流布に関するもの。	37
3 月 15 日	米財務省外国資産管理局（OFAC）は、2016 年の米国大統領選挙の介入および別のサイバー攻撃事案（2017 年に流行したマルウェア NotPetya）に関して、ロシアの 5 企業・組織とロシア人 19 名を制裁対象にしたと発表。	38
7 月 13 日	米司法省は、米大陪審が 2016 年の米国大統領選挙の介入に関する罪で、GRU 職員 12 名を起訴したと発表。起訴内容は主に、米 DNC 等へのサイバー攻撃と情報暴露、選挙インフラへのサイバー攻撃に関するもの。	39
10 月 4 日	米国、オーストラリア、カナダ、オランダ、英国が、ロシア GRU が広範なサイバー攻撃・活動に関与していると批判。この攻撃・活動の対象は米 DNC や世界反ドーピング機関を含む（オーストラリア、カナダ、オランダ、英国が米 DNC への攻撃をロシア GRU に帰した形）。	
10 月 19 日	米司法省は、IRA の選挙介入活動（Project Lakhta）の財政全般を統括したクシエノバ（Elena Alekseevna Khusyaynova）を起訴したと発表。ただし、起訴状の日付は 9 月 28 日。	40

出典：筆者作成。

「表：ロシアによる 2016 年米国大統領選挙介入と米国の対応に関する推移」出典一覧

[1] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Scribe, 2018), pp.172-174.
[2] ヒラリー・ロダム・クリントン（髙山祥子訳）『WHAT HAPPENED：何が起きたのか？』（2018 年、光文社）、373-374 頁。
[3] U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018), p.6.
[4] *Ibid.*
[5] 「米大統領選挙狙う「平凡なサイバー攻撃」のリスク」『ウォール・ストリート・ジャーナル日本版』（2016 年 11 月 2 日）
[6] *Indictment* (July 13, 2018), p.7.
[7] *Indictment* (July 13, 2018), pp.8-9.
[8] *Indictment* (July 13, 2018), p.10.
[9] クリントン、前掲書『WHAT HAPPENED』、374 頁。
[10] Nicole Gaouette, “Intel chief: Presidential campaigns under cyber attack,” *CNN* (May 18, 2016); James R. Clapper, *Facts and Fears: Hard Truths from a Life in Intelligence* (New York: Random House, 2018), p.604.
[11] Ellen Nakashima, “Russian government hackers penetrated DNC, stole opposition research on Trump,” *The Washington Post* (June 14, 2016).
[12] Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” CrowdStrike (June 15, 2016).
[13] *Indictment* (July 13, 2018), pp.14-17.
[14]“Threat Group-4127 Targets Hillary Clinton Presidential Campaign,” Secureworks (June 16, 2016).
[15] Ellen Nakashima, “Cyber researchers confirm Russian government hack of Democratic National Committee,” *The Washington Post* (June 20, 2016); “Findings from Analysis of DNC Intrusion Malware,” Fidelis Security Systems (June 20, 2016). Mandiant の評価はワシントンポスト紙を参照。
[16] Sanger, Op. Cit., p.214; David E. Sanger and Eric Schmitt, “Spy Agency Consensus Grows That Russia Hacked D.N.C.,” *New York Times* (July 26, 2016); 「米民主党のメール流出、ロシアの関与示す証拠＝米当局者ら」『REUTERS』（2016 年 7 月 26 日）。
[17] Nick Gass, “Obama on DNC hack: 'Experts attribute this to the Russians',” *POLITICO* (July 26, 2016).
[18] *Indictment* (July 13, 2018), pp.7-8.
[19] “Hillary Clinton on tight race, accusations against Trump,” *Fox News* (July 31, 2016).
[20] U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI), Report on Russian Active Measures, Majority Report (March 22, 2018), p.44；クリントン、前掲書『WHAT HAPPENED』、392 頁。
[21] ボブ・ウッドワード（伏見威蕃訳）『FEAR 恐怖の男：トランプ政権の真実』（日本経済新聞社、2018 年）、68 頁。
[22] ジェームズ・コミー（藤田美菜子、江戸伸禎訳）『より高き忠誠：真実と嘘とリーダーシップ』（光文社、2018 年）、302-303 頁。
[23] Press Conference by the President, at James S. Brady Press Briefing Room, The White House (December 16, 2016); Ben Rhodes, *The World As It Is: A Memoir of the Obama White House* (New York: Random House, 2018), pp.583-585.
[24] Dana Priest, Ellen Nakashima and Tom Hamburger, “U.S. investigating potential covert Russian plan to disrupt November elections,” *The Washinton Post* (September 5, 2016).
[25] James R. Clapper, Director of National Intelligence, “U.S. Intelligence as a Pillar of Stability during Transition,” INSA & AFCEA Intelligence & National Security Summit, Walter E. Washington Convention Center, Washington, DC (September 7, 2016).
https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2016/item/1627-dni-clapper-s-as-delivered-remarks-at-the-2016-insa-afcea-intelligence-national-security-summit
[26]「『ロシアがサイバー攻撃で大統領選挙をかく乱』米 2 議員が声明」『時事通信』（2016 年 9 月 23 日）；“Feinstein, Schiff Statement on Russian Hacking,” United States Senator for California: Dianne Feinstein (September 22, 2016).
[27] Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security (October 7, 2016); クリントン、前掲書『WHAT HAPPENED』、384、391-392 頁。
[28] Louis Nelson, “White House says U.S. will retaliate against Russia for hacking,” *POLITICO* (October 11, 2016); “Obama to consider 'proportional' response to Russia hacking,” *The Reuters* (October 12, 2016); Press Briefing by Press Secretary Josh Earnest, Office of the Press Secretary, The White House (October 12, 2016).
[29] William M. Arkin, Ken Dilanian and Robert Windrem, “CIA Prepping for Possible Cyber Strike Against Russia,” *NBC News* (October 15, 2016).
[30] William M. Arkin, Ken Dilanian and Cynthia McFadden, “What Obama Said to Putin on the Red Phone About the Election Hack,” *NBC News* (December 20.2016).
[31] David Corn, “A Veteran Spy Has Given the FBI Information Alleging a Russian Operation to Cultivate Donald Trump: Has the bureau investigated this material?” *Mother Jones* (October 31, 2016); Luke Harding, *Collusion: Secret Meetings, Dirty Money, and How Russia Helped Donald Trump Win* (New York: Vintage, 2017).

[32] Adam Entous, Ellen Nakashima and Greg Miller, “Secret CIA assessment says Russia was trying to help Trump win White House,” *The Washington Post* (December 9, 2016); Adam Entous and Ellen Nakashima, “FBI in agreement with CIA that Russia aimed to help Trump win White House,” *The Washington Post* (December 16, 2016).
[33] Office of the Press Secretary, The White House, “Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment” (December 29, 2016)；Office of the Press Secretary, The White House, “FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment” (December 29, 2016)；NCCIS, DHS & FBI, GRIZZLY STEPPE : Russian Malicious Cyber Activity, Reference Number: JAR-16-20296A (December 29, 2016).
[34] コミー、前掲『より高き忠誠』、342-355 頁。
[35] Office of the Director of National Intelligence, *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution* (January 6, 2017).
[36] 35 頁分のスティール文書の原文は以下で確認できる。Ken Bensinger, Miriam Elder & Mark Schoofs, “These Reports Allege Trump Has Deep Ties to Russia,” *BuzzFeed News* (January 10, 2017) https://www.buzzfeednews.com/article/kenbensinger/these-reports-allege-trump-has-deep-ties-to-russia
[37] U.S. District Court for the District of Columbia, *Indictment,* Case 1:18-cr-00032-DLF (February 16, 2018).
[38] “Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks,” Department of the Treasury (March 15, 2018).
[39] U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ (July 13, 2018).
[40] U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464 (September 28, 2018).

以上

東京海上日動リスクコンサルティング株式会社
戦略・政治リスク研究所
〒100-0004　東京都千代田区大手町1-5-1
大手町ファーストスクエア ウエストタワー 23階