Vol.2019-EIP-84 No.17
2019/6/4

デジタル・ゲリマンダーの事例研究と その法的課題への一考察

長迫智子[†1]

概要：近年，科学技術の発展により官民ともにサイバー空間の利活用が進んだことで，国家の安全保障体制にも変化が起こっている．国家規模でのサイバー攻撃が，単純に相手国のインフラや産業システムの攻撃に用いられるだけでなく，ＳＮＳやその他メディアでの情報戦の中に組み込まれ，各国の選挙結果に影響を及ぼすという事態に至り，民主主義に対する大きな脅威となっている．本研究では，そうしたデジタル・ゲリマンダーに関する事例研究を行い，各国の法制度上の対策や法的課題について考察する．

キーワード：デジタル・ゲリマンダー，選挙，インテリジェンス，投票行動，SNS，ハッキング

A Consideration on the Case Study of Digital Gerrymandering and its Legal Problems

TOMOKO NAGASAKO[†1]

Abstract: In recent years, security arrangements are changing, because technological developments promote the use and application of the cyber space by the public and private sectors. Some countries use global cyber attacks not just as the destructive attacks to the infrastructure systems or the industry systems, but also as the measure in the information warfare including SNS and other media which affects the election results, and it become the big threat to the democracy.
In this research, I study cases of the digital gerrymandering and consider countermeasures of legal systems and legal problems.

Keywords: Digital Gerrymandering, Election, Intelligence, Voting Behavior, SNS, Hacking

1. はじめに

近年，ICT 技術のめざましい進歩により，官民共々サイバー空間の利活用が進んでいる一方で，サイバー攻撃による脅威も同時に加速し，社会に対する危機は甚大化している現状がある．1990 年代以降のインターネットの普及，拡大により，テロリズムや国家間干渉，国際的紛争等の手法や対象が大きく様変わりしたことによって，国家の安全保障体制も対応を迫られ変容を遂げてきた．

こうした状況において，非伝統的安全保障の一形態としてサイバーセキュリティが注目を集め，各国も対応を迫られている．いわゆる「サイバー攻撃」の大半は，情報の改ざん，情報や知的財産の窃取，あるいは各種の妨害行為等である．しかし，コンピュータやインターネットを利用した攻撃により物理的な被害や人命に関わる事態も想定されるようになり，今後の安全保障に少なからぬ影響が出ると懸念されている．加えて，国家規模でのサイバー攻撃が，単純に相手国のインフラや産業システムの攻撃に用いられるだけでなく，ＳＮＳやその他メディアでの情報戦の中に組み込まれ，各国の世論に影響を与えることで民主主義に対する大きな脅威となっている．これらの危機に対応するかたちで，各国の安全保障に関与する諸機関や法制度の運用も，昨今の動向に独自の動きがみられるところであり，こうした情勢について注視していく必要があると筆者は考える．

2. 研究の背景と目的

当方の研究においては，サイバー攻撃を用いた選挙干渉，いわゆるデジタル・ゲリマンダーを主たる研究対象としている．サイバー攻撃とＳＮＳやその他メディアでの情報戦の融合により，その影響はサイバー空間にとどまらず，各国の選挙結果に影響を及ぼすという事態に至っている．こうしたデジタル・ゲリマンダーという脅威は，各国の主権を脅かし，民主主義体制を揺るがす，強大かつ複雑な新たな攻撃体系であると筆者は考える．各国内及び国際的な協力下での対策や規制の準備が喫緊の課題であり，これを克服することが出来なければ，民主主義的な既成の政治概念すらも崩れ去ることになろう．そうした危機意識が，研究の原動力としてある．

ついては，本研究報告においては，デジタル・ゲリマンダーが実際に行われたとされる米国選挙を代表的な事例研究としてとりあげ，それに対して，今現在どのような法制度上の対策が行われているか，また国際法及び各国国内法上でどのような課題があるのかを考察していく．その中で，デジタル・ゲリマンダーに対して特に各国のインテリジェンス機関が関与し，対抗しうるという，親和性をもつ構造についてもあわせて述べる．

†1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

3. デジタル・ゲリマンダーとは何か

3.1 デジタル・ゲリマンダーの類型

では，そもそもデジタル・ゲリマンダーとはどういったものであろうか．

本来のゲリマンダー（Gerrymandering）という語は，選挙において特定の政党や候補者に有利なように選挙区を区割りすることを指した[1].

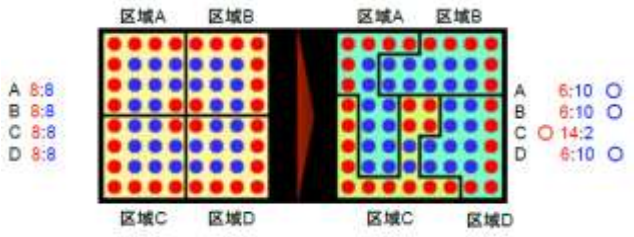

図 1　ゲリマンダーによる選挙区割りイメージ
（https://ja.wikipedia.org/wiki/ゲリマンダーの図を元に筆者加筆）

上図のように，区域 A―D では赤と青が同数だったところ，恣意的にその区割りを変更すると，区域 A，B，D では青が勝ち，区域 C では赤が勝ち，青が 3 区域を制したことで総合的には青が勝利する．このように，特定の候補者や勢力，政党等にとって有利なように区割りを変更することがゲリマンダーの原義である．

この語が発展し，デジタル・ゲリマンダー(Digital Gerrymandering)という語が，2014 年に Facebook 等の SNS による世論操作を通じた投票行動への影響力を論じた Zittrain によって初めて用いられたとされる[2]．しかし湯淺[3]によれば，SNS の利用だけでなく，インターネット上の様々な手段を用いた投票行動への影響力行使へとこの語の射程は広がっているとされ，デジタル・ゲリマンダーの現状の態様は以下のように類型化できるとされる．

① コンピュータ技術を使って恣意的な選挙区割りを行うこと（地理的ゲリマンダの高度化）
② 統計的データ分析(ビッグデータ分析)を用いて選挙区割以外の方法により投票結果にバイアスをかけること（たとえば，レンタルビデオ店の顧客にのみ投票を促すようなキャンペーンを行うことなど）
③ SNS などでメッセージの伝達にバイアスをかけることによって誘導を行うこと（感情伝染実験）
④ サーチエンジンの検索結果による世論操作
⑤ サイバー攻撃やフェイクニュースの流通等を通じた選挙全般への介入

そして，この⑤の類型に焦点が当たるようになったのは，２０１６年の米国大統領選挙において，ロシアの情報機関が候補者や政党関係者へのサイバー攻撃，SNS における広告利用，ボット的活動による特定意見の流通といった諸活動を通じて，選挙干渉を行った事案に注目が集まったことがきっかけとなっている．

デジタル・ゲリマンダーは，一見すると直接的には国家の安全保障には関わりがないように見えるが，その国の安全保障政策をはじめとする政策決定の根本にかかわる選挙に干渉するという点で，重大な主権侵害であり民主主義を脅かす絶大な脅威だと筆者は考える．

3.2 インテリジェンス機関との親和性

こうしたデジタル・ゲリマンダーについて，その実行行為や対応策において，各国のインテリジェンス機関が重要な役割を担っている．では，デジタル・ゲリマンダーとインテリジェンス機関の親和性はどういった点にあるのであろうか．インテリジェンスとは，「国家安全保障にとって重要な特定類型の情報が要求され，収集され，分析され，政策決定者に提供されるプロセスとその生産物のことで，それらを保護することや，そのために要請された合法的な権限に基づくオペレーションの実施も含む概念」([4]より筆者要約）であるが，こうしたオペレーションを実施する各国のインテリジェンス機関のどのような性質にデジタル・ゲリマンダーが結びつくのか．この点，先ずは，サイバーセキュリティそのものとインテリジェンス機関の親和性について述べたい．

近年のサイバー攻撃は，個人やハッカー集団だけでなく，国家間で攻撃や情報窃取，防衛，カウンターを行うサイバー戦の様相をも呈している．米国の国家情報長官室（Office of the Director of National Intelligence: ODNI）が２０１７年１月に発表した２０１６年大統領選挙に係る報告書では，選挙に対するサイバー攻撃についてロシア情報機関による国家的関与を指摘しており[5]，同年 7 月にドイツの連邦憲法擁護庁（Bundesamt für Verfassungsschutz: BfV）が発表した年次報告書の中でも，サイバー攻撃についてロシア，中国，イランの国家的関与があると指摘されている(BfV2017:31)．このように，国家的なサイバー戦という状況下では，各国のインテリジェンス機関が暗躍しているという事実がある．そうした攻撃に対する防御・対策という点で，各国のサイバーセキュリティ対策の中心となっているのもまた，多くの場合，インテリジェンス機関なのである．こうした情勢下では，日本も同様にサイバーセキュリティ戦略におけるインテリジェンス機関の活用を目指していく必要があるといえよう．

では，何故サイバーセキュリティにおいてインテリジェンス機関が中心的な役割を担っているのだろうか．インテリジェンス機関のどのような機能に，サイバーセキュリティとの親和性があるといえるのか．これに対する回答は，土屋[7]が述べている以下の見解が明瞭である．

「単純に答えれば，それは，アトリビューション問題に最も適切に対応できるのがインテリジェンス機関だからということになる．すでに行われた犯罪の実行者を逮捕し，訴追するのが法執行機関の役割になるが，サイバー攻撃が単なるサービス妨害や情報窃取にとどまらず，人的・物的被害が予想され，それが国境を越える安全保障問題となる可能性があることが理解されると，事前にサイバー攻撃を予期・防止し，潜在的な攻撃者を特定することが求められるようになる．それは従来，インテリジェンス機関が行ってきた『エスピオナージ』と呼ばれるスパイ活動に近くなる．エスピオナージとは，外国政府の軍事的・政治的な秘密について探ることを意味する．」

警察庁がまとめているサイバー攻撃の特徴には，①攻撃の実行者の特定が難しい，②攻撃の被害が潜在化する傾向がある，③国境を容易に越えて実行可能である，といった三点があげられており[8]，こうした特徴の問題から，サイバー攻撃の問題解決には上述のようにアトリビューション問題が密接に絡んでいる．同様に，

サイバーセキュリティにおけるアトリビューション問題の重要性を指摘している田川・林[9]は，サイバー攻撃の上述のような特徴から，従来は明確に区別されてきた，警察・防衛・インテリジェンスの機能をもつ各々の機関の協力と牽制関係に対する見直しの必要性を示唆している．そして，アトリビューション問題に関しては，それに伴うサイバー空間上の他国の機密情報の取得や監視行為が，国際法上の間諜行為に当てはまるのか否か，それによって当該行為が認められるのか否かという問題もある[10].

そして，デジタル・ゲリマンダーにおいては，サイバー攻撃によって窃取した情報の流通，SNS の活用によるフェイクニュースの流通等が組み合わされ，またインテリジェンス機関だけでなく，その機関が実行行為を委託している民間会社や個人ハッカー等，多種多様な手段・組織により干渉行為が行われる．そうした中で，行為者側の意図は旧来のプロパガンダと同様，特定の政治意見の広報・流布にあるため，それは依然情報戦の範疇としてインテリジェンス機関の所掌となる．一方でそうした多方向からの干渉に対抗する側は，行為者を調査するためにアトリビューション問題が極めて重要な意味を持ち，やはりインテリジェンス機関の実働が肝要となってくるのである．

デジタル・ゲリマンダーにおいて，いわゆる干渉国側とされる代表的な国家がロシア，中国であるが，下図のとおり，選挙干渉に係る実行行為を行っていると考えられている FSB（ロシア連邦保安庁）や GRU（ロシア連邦軍参謀本部情報総局），人民解放軍が，その国のインテリジェンス・コミュニティで重要な位置を占めていることがわかる．

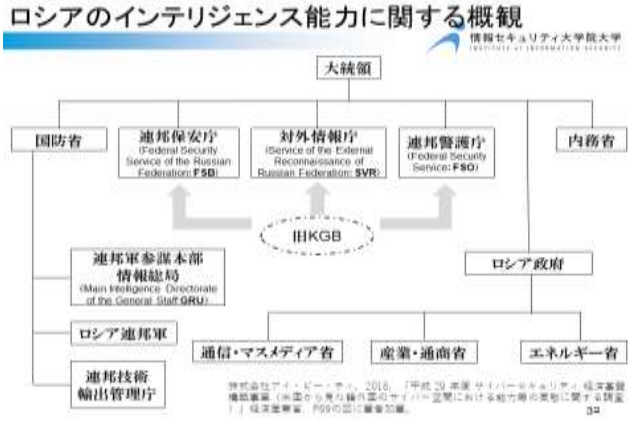

図 2　ロシアのインテリジェンス能力に関する概観
（[11]をもとに筆者加筆により再作成）

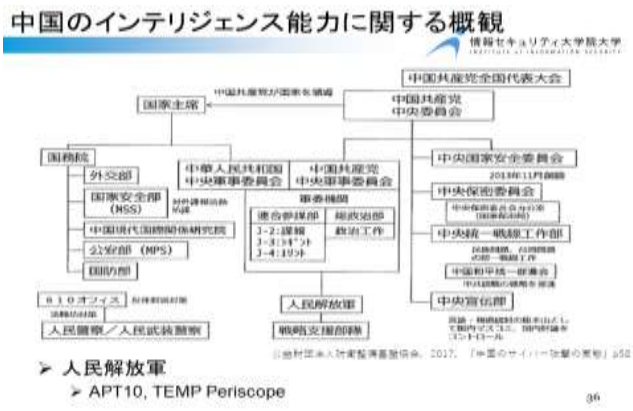

図 3　中国のインテリジェンス能力に関する概観[12]

そして以下では，実際のインテリジェンス機関によるデジタル・ゲリマンダーの事例をあげ，検討していく．

4. デジタル・ゲリマンダーの事例－2016 年米国大統領選挙－

2016 年 5 月，米国民主党全国委員会がサイバー攻撃を受け，委員会幹部の電子メール約 19,000 件以上がハッカーによって窃取された．そして，このメールは内部告発サイトである WikiLeaks や DC Leaks.com で公表されることとなり，その中で委員会幹部たちが，民主党の指名候補争いでヒラリー・クリントン前国務長官と競っていたバーニー・サンダース上院議員を意図的に落選させるような動きがあったことが暴露された．このリークにより民主党の全国委員長が全国大会前日に辞職する事態となり，クリントンをはじめとする民主党側の信頼は失墜した．

これら一連のハッキングにおいてはスフィアフィッシングや６種類のゼロデイ攻撃が用いられた[13]が，この点については，「組織のメンバーが，脆弱性を兵器化する高い技術力と多くの時間を持っているか，兵器化されたゼロデイ脆弱性を購入する予算を持っているかのどちらかである」として，国家またはそれ相応の組織でないと難しいという指摘が当初からあった．

選挙直後の NCCIC の報告書[14]では，ハッキングに関わった多くのハッカーのコードネームが列挙されているが，このうち Fancy Bear（別名 APT28）の背後には GRU（ロシア連邦軍参謀本部情報総局）が，Cozy Bear（別名 Office Monkeys, Cozy Car, Cozy Duke, または APT-29)の背後には FSB（ロシア連邦保安庁）の存在が示唆されている[15].

また同時に，この選挙においては Twitter や Facebook をはじめとする SNS においても，フェイクニュースの流通やトランプを支持しクリントンの評判を下げるような特定意見の発信，流布というかたちでロシアの関与があったことが報告されている．米国両院による情報委員会で明らかになった範囲では，2752 件の Twitter アカウント及び 3393 件の Facebook アカウントがロシア政府の工作に使われた[16]．Facebook に対しては，10 万ドル相当を費やしてロシア政府関係機関が 3000 以上の広告枠を購入していたことを Facebook が認めている[17]．こうした虚偽又はトランプ支持に偏向した情報の書き込みを組織的に行うトロール部隊を擁しており中心的に活動していたのが，サンクトペテルブルクにあった Internet Research Agency (IRA)である．表面的には新興財閥出資の民間会社を装っているが，その財閥が GRU やプーチン大統領とも密接な間柄にあることが ODNI の報告書では指摘されており[18]，これら IRA の活動は民間会社による自主的な愛国活動ではなく，国家的な工作活動であったと当該報告書は評価して以下のように述べている．

「我々はロシアのウラジミール・プーチン大統領が２０１６年，米国の大統領選を標的にした情報戦を指示したと強く確信している．その一貫した狙いは，米国における民主的手続きへの信頼を損ね，クリントン氏を中傷し，大統領への当選を妨害することだった．さらに，プーチン氏とロシア政府は，明らかに次期大統領トランプ氏への支持を強めていったと認定している．」[19]

こうしたロシアの関与が明らかになったことにより，対ロシアへの制裁として 2016 年 12 月には駐米ロシア外交官 35 人が国外追放されることとなった．

5. デジタル・ゲリマンダーへの各国の対策

5.1 事前的な対策：EU

EU もまたデジタル・ゲリマンダーを深刻な脅威と考えている．EU は，2015 年 3 月にロシアの選挙干渉活動（EU では選挙干渉以外のフェイクニュース流通等の活動も含めた総称として Disinformation という語を用いている）に対処する 11 人の作業部会「イースト・ストラトコム(The East StratCom Task Force)」を設立し，2016 年 1 月には更にその予算を拡大させた．「イースト・ストラトコム」は，ロシアの偽情報に対処し，情報の歪みを明確にすることを目指している．Disinformation に関する報告を毎週発行し，どのように虚偽の報道が蔓延するのか，そしてどのようにファクトチェックをきかせるか，といった内容をバイラルスタイルのメディアを活用して発信している．これらの情報は，一般の人々に広く行き渡るように，独自のウェブサイト(www.EUvsDisinfo.eu/)や Twitter (@EUvsDisinfo)，Facebook ("EU vs Disinformation")で遍く展開されている．

2016 年 11 月 23 日，欧州議会は，ロシアが仕掛ける「フェイクニュースとプロパガンダの闘い」に対抗手段を取るよう，EU と加盟諸国に要請する決議 を採択した[20]．その中で欧州議会は,「ロシアからのディスインフォメーション及びプロパガンダ戦線」が西側陣営の政治に対して影響力を及ぼす可能性について警告を発し，それが「時には非軍事作戦となって，大胆な手段を組み合わせている」と述べている．こうした強い表現から，欧州議会が選挙干渉に対して大きな危機感を抱いていることが窺える．

5.2 事後的な対策：米国

米国は，デジタル・ゲリマンダーに対して事後的な制裁を強める方策を打ち出している．2016 年の大統領選後，選挙干渉に関わったとされる関連団体や個人について，退去処分や資産凍結等の制裁，起訴等を個別に順次行ってきたが，去る 2018 年 9 月 12 日，トランプ大統領は，外国政府などによる米国の選挙介入に対して制裁を科すことを認める大統領令に署名した[21]．制裁の発動如何については，選挙結果が出てから 45 日以内に，介入があったかどうかを国家情報長官（Director of National Intelligence: DNI）が調査し，その後 45 日以内に司法長官と国土安全保障長官が制裁発動の是非を判断する．そして制裁対象者は米国内の資産が凍結され，米国人との取引が禁止されることとなる．先に述べたように，ODNI による報告書は，2016 年の大統領選にロシアが介入したと断定しており，2018 年 11 月の米国中間選挙を前に，選挙介入が想定されうる，ロシア，北朝鮮，イラン等への牽制措置を準備したといえるだろう．

ここで調査を担当する国家情報長官は，2004 年に情報改革とテロ予防法(The Intelligence Reform and Terrorism Prevention Act of 2004)により国家安全保障法が改正されたことにより設置されたポジションであり，米国のインテリジェンス・コミュニティを統括し，アメリカ連邦政府の 16 の情報機関の人事・予算を統括する権限を有する．つまり，米国における選挙介入においては，国家情報長官を通じて各インテリジェンス機関に調査の照会がなされることとなり，選挙介入対策としてインテリジェンス機関が重要な立ち位置を占めているといえよう．

また，在米ドイツ系財団 German Marshall Fund of the United States (GMF)が中心となって，2016 年には米国と EU が連携して，ロシアを主とした諸外国からの干渉行為を監視・調査する超党派の団体 Alliance for Securing Democracy (ASD)が発足した[22]．これにより，一国にとどまらない干渉行為への対抗が進んでいる．

5.3 包括的な対策：英国

英下院の文化・メディア・スポーツ委員会は，昨年 7 月，「偽情報と『フェイクニュース』についての調査報告書（中間報告）」を発表している[23]．ここにおいて提案された諸方策の中で，デジタル・ゲリマンダーへの対策となり得るものを検討する．

本報告書は，英米両国でメディア関係者，メディアの監督組織，テクノロジー企業の経営幹部など 61 人を召喚してヒアリングを行い，あわせて 150 を超える参考文書の提出を受けたことにより，フェイクニュースが社会に与える影響や，民主主義が今後どうなっていくかを調査した内容となっている．対象とした調査項目は「何がフェイクニュースか」，「フェイクニュースが国民の世界観にどのような影響を及ぼしているか」，「年齢，社会的背景，性別などの要素によってフェイクニュースの使い方や反応は異なるか」，「広告の販売方法の変化がフェイクニュースの成長を促したのか」といった点であり，その構成は，（1）序，これまでの背景（フェイクニュースとは何か），（2）テック企業の定義，役割，司法責任，（3）フェイスブック，GSR(グローバル・サイエンス・リサーチ）社及びケンブリッジ・ アナリティカ（CA）社事件におけるデータ利用，（4）政治運動，（5）政治運動におけるロシアの影響，（6）外国の選挙での SCL 社の影響，（7）デジタル・リテラシーといった 7 章から成る．

選挙対策の第一には，選挙管理委員会の意見を参考にし，ネットを使ったすべての選挙運動はどこの組織が誰の資金で行っているかを簡単に識別できるようにするべき，と述べている．政治資金関係による政治的・社会的アトリビューションを明らかにすることで，SNS 等に流入する外国国家資金を財源としたボットアカウントを排除することが出来る．

また，ミャンマーの少数民族ロヒンギャに対するヘイトスピーチがフェイスブックを通じて拡散され，これが民族浄化行為の発生につながった事例をあげ，SNS を主力とするプラットフォーマー大手には「グローバルな倫理規定」を設けるよう呼びかけ，もしこれが実現しない場合には，政府主導で倫理規定を強制的に順守させる規制を導入するべきとしている．

そして「デジタル・リテラシー」の項目で委員会は，政府が年内に発表するインターネットを安全に使うための白書に「リテラシー教育税」の導入を入れるよう提案した．慈善団体や非政府組織が開発するリテラシー教育をこの財源で実施に移すとしている．このようなリテラシー教育を推進することで，受け手のフェイクニュースに対する判断力が養われるとともに，フェイクニュース規制に対する法制度の整備を後押しする世論が涵養できると考えられる．

こうした英国の取組は，事前策または事後策として切り分けられるものではないが，中長期的にデジタル・ゲリマンダーのようなかたちで外国勢力が干渉しにくくなるようなサイバー空間の土

壌を醸成するための，包括的な対策であるといえるだろう．

6. 国家機関が関与するデジタル・ゲリマンダーの法的課題

6.1 国内法による規制：ドイツの SNS 法

以上のようなデジタル・ゲリマンダーの動向に対し，SNS の法規制というかたちで対応をとったのがドイツである．
2017 年 9 月に連邦議会選挙を控えていたドイツ政府は，同様のロシアの干渉を危惧し何らかの対応が急務だと考えていた．また，2015 年にシリア難民をはじめ大量の難民がドイツに押し寄せたことがきっかけとなり，国内で排外主義運動が高まりを見せたことで，SNS 上で難民及び難民を支援する人々に対するヘイトスピーチが急増していたということも背景に，SNS に対する何らかの規制を設ける動きが現実化した．

それにより 2017 年 6 月 30 日に成立したのが，「SNS における法執行を改善するための法律（Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken）」（通称，SNS 規制法，Facebook 法などとも呼ばれる）である．この法は SNS 事業者に，違法内容削除義務，その義務を果たすための苦情対応，手続整備義務，苦情対応状況の報告義務を課すとともに，これらの義務に対する違反に科される過料について定めた．また，SNS 規制法の制定に合わせてテレメディア法が改正され，匿名による違法な人格権侵害の場合の発信者情報開示制度が追加されることとなった．これにより，SNS 事業者は，警報に規定される「違法な内容」について「構成要件をみたし，かつ，正当化されない内容」の投稿に関し，基本的には通報から 24 時間以内の削除義務を有し，そうした苦情対応に関する報告書作成及び公開の義務を負うこととなったのである．

当該法律では第 1 条 3 項において「違法な内容」が列挙されているが，そのうち，いわゆるフェイクニュースに関連する規制内容は，100a 条の国家反逆的な事実の歪曲，126 条 2 項の，虚偽であると知りながら犯罪行為の実行が間近いと「偽装」することによって行われる脅迫，130 条 3 項の「アウシュヴィッツの嘘」（ナチスによるユダヤ人虐殺を否定したり，矮小化したりすること），187 条の虚偽であると知りながら，虚偽の事実を摘示してなされる名誉毀損といったものがあげられる．

しかし，この法については，SNS 事業者が高額の過料をおそれるあまりに，厳密な判断を放棄し，違法ではない内容の投稿まで安易に削除するようになることが懸念されており，表現の自由の萎縮効果という点からは批判もある[24].

また，本法は米国大統領選でみられた IRA によるトロール部隊やボットのような，特定の候補者への支持意見を大量に発信することへの対策とはなりえておらず，同年 9 月の連邦議会選挙で，親ロシア派である政党「ドイツのための選択肢(Alternative für Deutschland: AfD)」が大々的な SNS 発信により得票を伸ばしたことを鑑みると，この時点での実効性には疑義がある．しかし，世論の変化がデジタル・ゲリマンダーによるものなのか，社会的・経済的事象によるものなのかの峻別は難しく，この点，更なる検討が必要であろう．

6.2 国際法上の法的規制の可能性

本研究でとりあげるような，国家に帰属するインテリジェンス機関によるデジタル・ゲリマンダーに関わる諸活動に関しては，事前策としては SNS の監視や規制を行い，事後策としては実行関係者への制裁を行うというのが，現状行われている対策である．法的規制という点では，各国国内法の整備を待つほかないが，果たして上述のような対策でデジタル・ゲリマンダーを抑え込めるのであろうか．
デジタル・ゲリマンダーが国家間の問題である以上，国際法的な違法性を検討し規制を進めるべきではないかと筆者は考える．国家に帰属するインテリジェンス機関によるデジタル・ゲリマンダーに関わる諸活動は，サイバー空間上の他国の機密情報の窃取といった行動を含んでいるが，国際法上の間諜行為に当てはまるのか否か，それによって当該行為が認められるのか否かが問題となる．

この点，サイバー行動に適用される国際法の考え方をとりまとめた Tallinn Manual 2.0 を参照する[25]．同書はサイバー空間やサイバー行動に係る国際法を新たに作成するものではなく，慣習国際法が存在するという前提のもと，その内容を確認し記述したものである．

『Rule4. (主権の侵害)国家は他国の主権を侵害するサイバー行動を行ってはならない.』

これについては，ある国家機関が他国領域内で行うサイバー攻撃及び諜報は当然ながら主権の侵害となると解される．そして，遠隔のサイバー行動については，サイバー・インフラの物理的損害や機能喪失が生じた場合及び,「政府の機能の行使に必要なデータやサービスを妨げるサイバー行動（社会保障，選挙，徴税，外交，国防に関するデータの改変・削除など）」 は主権の侵害となるとされる．

選挙干渉という観点では，サイバー攻撃により選挙の投票データを操作したり，投票所の運営を妨害したり，といったレベルの妨害行動があってはじめて主権の侵害といえることとなり，デジタル・ゲリマンダーの事例では主権侵害とまではいえないだろう．

『Rule32. (平時のサイバー諜報)国家による平時のサイバー諜報はそれ自体は国際法に違反しないが，それを遂行する方法は国際法違反となりうる.』

この規則においては，本件のような選挙干渉が諜報にあたるかが問題となる．

こうした選挙干渉のような他国に対する能動的，積極的な働きかけは，インテリジェンス活動のうち秘密工作(covert action)にあたるとされる．秘密工作がインテリジェンス活動の範疇であるか否かは議論の余地があるところではあるが，前掲の定義に関連して Lowenthal は，「秘密工作は，他の手段では達成不可能な特定の政策目標を追求するために，正当な権限を持つ政策決定者が任務を与えた場合にのみ意味を持つし，またその場合に限って行われるべきである」[26]として，インテリジェンス活動の一つに含めている．

しかし，インテリジェンス活動のうち更に狭義の「諜報」にあたるかという点については，原文では「諜報」に” espionage”という語を用いていることから，情報収集に限定した行動と解することが妥当と考え，選挙干渉のような秘密工作は本規則の射程外であろう．

『Rule66.（国家による干渉）国家は，他国の国内または対外事項に，サイバー手段による場合を含め，干渉してはならない.』

中谷他[27]の解説によれば,「干渉(intervention)」は強制的要素をもたず,「介入(interference)」とは区別される概念とされる．意図的な介入であってもそれが強制を伴わない場合，又は，強制を伴う場合であってもそれが特定の国の国内又は対外事項に関するものでない場合，本規則の違反はないと解する．

すなわち，特定の国の選択の自由を奪うことを企図しないサイバー行動は，何ら強制的要素を有さない．他国によるプロパガンダの展開があっても，それにより選択の自由が奪われない限り，強制的な干渉になることはないだろう，と述べられている．よって，デジタル・ゲリマンダーについても，その選択の自由が完全に奪われない限りは選挙「干渉」とはいえないのである．

以上の検討から，デジタル・ゲリマンダーについて，現行の国際法上の違法性を認定するのは限界があると思われる．ついては，今後，国際法上でどのような規制の取り組みを進めていくことができるのか，また各国国内法で実効性のある法整備をどのように進めていけばよいのかが，今後の検討課題である．

7. おわりに

本報告では，デジタル・ゲリマンダーの特徴や事例を概観しつつ，その対策及び法的規制の可能性について検討を行った．現状では，事前的な対策，事後的な対策ともに有効な決定打とはいえない状況で，国際法的な違法性を問うことも難しいように考えられる．よって，今後各国が目指すべき方向性としては，デジタル・ゲリマンダーという新たなサイバー攻撃事象に対して，国際的に新たな法的規範を創りあげていき，また同時に，国内法において各国事情に沿った規制法を制定し政策に落とし込むことで対策をとっていくこととなろう．この点，当方の研究において，特に自国たる日本がどういった対策をとるべきかという点も含め，今後検討を進めていきたいと考えている．

謝辞　本研究についてご指導いただいた情報セキュリティ大学院大学の湯淺墾道先生，そして討論の際にご意見を頂戴した湯淺研究室の皆様に，謹んで感謝の意を表する．

参考文献

[1] 湯淺墾道. ディジタルゲリマンダの法規制の可能性. 情報処理, 1999, vol. 58, no. 12, 4p.
[2] Zittrain, Jonathan. Facebook Could Decide an Election Without Anyone Ever Finding Out. THE NEW REPUBLIC, 2014, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering
[3] 湯淺墾道. ディジタルゲリマンダの法規制の可能性. 情報処理, 1999, vol. 58, no. 12, 4p.
[4] Lowenthal, Mark M.. Intelligence: From Secrets to Policy. Washington D.C.: CQ press, 2008, 10p.
[5] Office of The Director of National Intelligence (ODNI). Assessing Russian Activities and Intentions in Recent US Elections. ICA, 2017.
[6] Bundesamt für Verfassungsschutz. Verfassungsschutzbericht 2016. Bundesministerium des Innern, für Bau und Heimat, 2017, 31p.
[7] 土屋大洋. サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト―. 国際政治, 2015, no. 179, 45p.
[8] 警察庁. 平成 24 年回顧と展望. 警察庁, 34p.
[9] 田川義博・林紘一郎. サイバーセキュリティのため情報共有と中核機関 サイバーセキュリティのため情報共有と中核機関 ―３つのモデルの相互比較とわが国への教訓―. 情報セキュリティ総合科学, 2016, no. 8, p. 37-39.
[10] 河野桂子. サイバー空間を通じた監視活動の法的評価―間諜行為，主権侵害と人権法（プライバシーの侵害）の観点から―. 防衛研究所紀要, 2017, vol. 19, no. 2, 50p.
[11] 株式会社アイ・ビー・ティ. 平成 29 年度 サイバーセキュリティ経済基盤構築事業（米国から見た諸外国のサイバー空間における能力等の実態に関する調査）. 経済産業省, 2018, 89p.
[12] 株式会社ラック. 中国のサイバー攻撃の実態. 公益財団法人防衛整備基盤協会, 2017, 58p.
[13] National Security Agency. Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, --- Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses. NSA, 2017, 1p.
[14] National Cybersecurity and Communications Integration Center (NCCIC). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Federal Bureau of Investigation, 2016, 4p.
[15] Office of The Director of National Intelligence (ODNI). Assessing Russian Activities and Intentions in Recent US Elections. ICA, 2017.
[16] “US Senate Select Committee on Intelligence – Hearing (2017.11.1)” https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections#.
[17] Harding, Luke. Collusion: Secret Meetings, Dirty Money, and How Russia Helped Donald Trump Win. New York: Vintage books, 2017, 111-112p
[18] Office of The Director of National Intelligence (ODNI). Assessing Russian Activities and Intentions in Recent US Elections. ICA, 2017, 4p
[19]. Office of The Director of National Intelligence (ODNI). Assessing Russian Activities and Intentions in Recent US Elections. ICA, 2017, (ii)p
[20] European Parliament , European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), 2016.
[21] THE WHITE HOUSE. Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, Federal Register 83 FR 46843. 2018.
[22] “Alliance For Securing Democracy – Putin Knocked. We Answered.” https://securingdemocracy.gmfus.org/
[23] House of Commons Digital, Culture, Media and Sport Committee. Disinformation and ‘fake news’: Interim Report Fifth Report of Session 2017–19. the House of Commons, 2018.
[24] 鈴木秀美. ドイツの SNS 対策法と表現の自由. メディア・コミュニケーション, 2018, no. 68, p8-9.
[25] Schmitt, Michael N. , Tallinn manual 2.0 on the international law applicable to cyber operations : prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. New York: Cambridge University Press, 2018.
[26] Lowenthal, Mark M.. Intelligence: From Secrets to Policy. Washington D.C.: CQ press, 2008, 250p.
[27] 中谷和弘・河野桂子・黒崎将広. サイバー攻撃の国際法－タリン・マニュアル 2.0 の解説－. 信山社, 2018.