総務省 学術雑誌『情報通信政策研究』 第2巻第1号
Journal of Information and Communications Policy Vol.2 No.1

寄稿論文

理念・原理・制度とサイバーセキュリティ法制
―選挙を中心に

湯淺　墾道[1]（情報セキュリティ大学院大学）

要　旨

個人情報やプライバシーのような個人の権利利益、企業の知的財産や営業秘密その他の経済的利益に係わる情報、地方公共団体や政府等の一般に情報公開することができない情報、安全保障や外交に関係する秘密情報その他、一般にサイバー攻撃によって窃取の対象となるとされる情報は、不正アクセス禁止法、個人情報保護法、プライバシー保護法制、営業秘密に関する法律その他によって保護されている。しかし民主主義の基礎となっている理念、原理、制度の存立がサイバー攻撃やサイバー空間の悪意をもった利活用によって脅かされる恐れがあり、それにどのように法的対処することが可能であるかという点の議論は、活発とは言い難い。さらに、人工知能（AI）に関する各種技術の急速な実用化によって、人工知能がインターネットを介して民主主義を支える各種の制度に「介入」する危険性も、現実化している。

そこで本稿では、特に民主主義を支える選挙に焦点を当て、選挙へのサイバー攻撃とサイバー空間の悪意をもった利活用の段階について先行研究の紹介と段階の整理を行う。次に、政府がどのように対応するべきかについて、アメリカとEUの例を参照する。

アメリカ政府は、外交的対抗、経済的対抗、技術的対抗という3つの対抗手段を講じている。もっとも、外交官追放等の外交的手段や口座凍結等による制裁では不十分であるとして、プロ・アクティブ、アクティブ・サイバー・ディフェンスのような積極的な技術的対抗手段の実行を主張する議論も存在する。また国土安全保障省は、選挙インフラを重要インフラの一つとして指定した。

EUは、選挙へのサイバー攻撃が2016年アメリカ大統領選挙において顕在化した後、選挙をサイバーセキュリティの重要な政策領域として位置づけるようになった。フェイクニュース対策は、デジタル単一市場創設という政策領域の一分野として位置づけられ、SNSを利用した世論誘導については表現の自由という基本的人権の侵害であると捉えられている。2018年1月にはフェイクニュース及び虚偽情報流布に関する有識者会合が設置され、4月に公表された最終報告書では「多元的な対応」が提案された。EUは特に世論を誘導する情報を媒介するプラットフォーマーに焦点を当てており、2018年7月までに共通の行動規範を策定して遵守することを求めた。

これらを参照して、日本において理念・原理・制度を守るためのサイバーセキュリティ法制のあり方とその限界についての検討を試みることにしたい。

キーワード：SNS　個人情報　選挙　世論　サイバーセキュリティ

[1] 情報セキュリティ大学院大学学長補佐・情報セキュリティ研究科教授

１．はじめに

本稿は、個人情報やプライバシーのような個人の権利利益、企業の知的財産や営業秘密その他の経済的利益に係わる情報、地方公共団体や政府等の一般に情報公開することができない情報、安全保障や外交に関係する秘密情報その他一般にサイバー攻撃によって窃取の対象となるとされる情報の流出や漏えいではなく、サイバー攻撃やサイバー空間の悪意をもった利活用によって民主主義の基礎となっている理念、原理、制度の存立が脅かされる恐れがあり、かつそれにどのように対処することが可能であるかという点を考察の対象とする。

というのも、民主主義の基礎となっている理念、原理、制度への各種のサイバー攻撃やサイバー空間を利用した容喙・干渉への対応の必要性は、必ずしも日本においては現実味を帯びて認識されているとはいえないように思われるからである。このことは、サイバー攻撃が高度化かつ多様化していることに対応して技術的・制度的な対策が立案され実施されつつあり、サイバー攻撃を通じたテロリズムや[2]武力行使が現実味を帯びると同時にそれに関する法的議論が活発になり、それに自衛権を行使して「反撃」する可能性についても検討の対象とされるようになってきたこととは対照的である[3]。もとより各種の重要インフラの防御や国それ自体の防衛の重要性は疑うべくもないが、さまざまな自由（特に精神的自由）や、選挙を通じて国民の民意を表出する国民代表の原理のような理念・原理・制度がサイバー攻撃やサイバー空間の悪意をもった利活用によって、直接・間接に脅かされていることの認識の重要性は、それに劣らないと思われる。さらに、人工知能（AI）に関する各種技術の急速な実用化によって、人工知能がインターネットを介して民主主義を支える各種の制度に「介入」する可能性も語られるようになってきた[4]。

このため本稿では、特に民主主義を支える根幹となっている選挙制度を中心として、サイバー攻撃やサイバー空間の悪意をもった利活用によって現実にそれが脅かされていることを取り上げ、それに政府がどのように対応するべきかについて、アメリカと EU の例も参照しながら検討を試みることにしたい。

２．選挙へのサイバー攻撃とサイバー空間の悪意をもった利活用

２．１．現状

選挙においては、デジタル・ゲリマンダー[5]と呼ばれるソーシャル・ネットワーク・サービス（SNS）自身による感情伝染実験、サイバー攻撃によって窃取した候補者・政党の内部情報の暴露、SNS を通じたフェイクニュースの流布とそれによる世論操作・誘導や投票

---

[2] 湯淺墾道「サイバー空間におけるテロ対策」大沢秀介・新井誠・横大道聡編『変容するテロリズムと法』（弘文堂、2017 年）60 頁以下を参照。
[3] 自由民主党サイバーセキュリティ対策本部「第 1 次提言～リスクの最小化に向けて。『コスト』から投資へ意識変革を～」（2018 年）77 頁。
[4] 山本龍彦編『AI と憲法』（日本経済新聞社、2018 年）、福田雅樹・林秀弥・成原慧編『AI がつなげる社会』（弘文堂、2017 年）などを参照。
[5] 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 58 巻 12 号（2017 年）1070 頁以下を参照。

行動への影響力行使など、サイバー攻撃とサイバー空間の悪意をもった利活用によって選挙に影響を与えようとする行為が広く見られるようになってきた。特にSNSは各国の選挙に大きな影響を与えており、フェイクニュースの伝播にも多用されるようになってきている。日本においては2013年に公職選挙法の改正によりインターネットを選挙運動に利用することが解禁され、当初は電子メールやウェブページの利用が想定されていたが、実際にはSNSのほうが積極的に選挙運動に利用されている[6]。インターネット選挙運動というよりもSNS選挙運動というほうが実態をよく表しているが、2018年9月に行われた沖縄県知事選挙では、SNS上でのフェイクニュース流布が連日のように報道されるに至った。

有権者の民意は、選挙における候補者や政党への投票を通じて有権者を代表する議員の議席に変換され、政治に反映される。SNSを介した選挙干渉は、有権者の民意の形成や候補者・政党への選択の過程に対して影響力を行使するものであり、SNSによって収集される有権者個人の社会経済的属性や政治的思想の傾向、行動範囲や交友範囲等に応じて、フェイクニュースや虚偽情報を含む特定の情報を意図的に流布したり特定の思想信条等に偏向した広告を表示させたりすることによって、有権者の民意の形成や候補者・政党への選択を特定の方向に誘導しようとする。

このようなSNSを通じた誘導は、幅広く多種多様な情報に基づいて有権者が自ら政治的争点について判断して自らの政治的意思を形成し、それに基づいて具体的な投票方向を決定して選挙において実際に投票するという民主主義の基盤としての選挙を危うくするものであることは疑いの余地がないであろう。

２．２．選挙へのサイバー攻撃とサイバー空間の悪意をもった利活用の段階

選挙のセキュリティについて検討する場合、以前は有権者のなりすまし、選挙人名簿の改ざん、投票結果の改ざん等、投票それ自体への影響を与える行為の発生を防止するために、投票と選挙管理に用いられる電子機器類のセキュリティに焦点を当てる、ということが多かった。しかし近年の選挙へのサイバー攻撃とサイバー空間の悪意をもった利活用による介入は、多段階にわたって行われるようになっており、次のように整理することができると思われる。

まず前段階として、民意形成（投票する意思の形成、または棄権意思の形成も含む）への介入がある。典型的にはSNSによる世論操作が想定されるが、特定の政治的傾向の有権者層の投票率を向上させることによって選挙結果に影響を与えることも考えられ、たとえばハーバード・ロースクールのジョナサン・ジットレイン教授は、SNSによる感情伝染実験を、選挙結果に影響を与える「デジタル・ゲリマンダー」であるとして批判した[7]。

ビクトリア大学のコリン・ベネット教授は、個人データを利用する世論誘導や選挙運動と

---

[6] インターネットの利用の経緯を概観するものとして、岡本哲和『日本のネット選挙　黎明期から18歳選挙権時代まで』（法律文化社、2017年）を参照。

[7] Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out,* NEW REPUBLIC, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

して、VRM (voter relations management)という概念を提唱している[8]。VRM は、 ビッグデータ、マイクロ・ターゲティング、モバイルデータという 3 種類のデータを活用するものであり、特定の傾向を有する有権者個人を特定して誘導を試みるマイクロ・ターゲティングに特色があるという。

ノースカロライナ大学のジーナップ・トゥフェックチー教授は、SNS やサーチエンジンの政治への影響の研究を通じて、ビッグデータ分析による世論操作の特色を指摘したが[9]、ビッグデータ分析による世論操作[10]の特色として次の 6 点を挙げている。

・きわめて厖大な量のデータの収集が可能となったこと。

・コンピューターによるプロファイリング技術や分析技術の進歩により政治的なターゲットをある特性を持つ集団から個人に特定することが可能になったこと。

・個人に対して直接アンケート調査等を実施して回答を得ることなしに特定の個人の思想や政治的傾向を知りうること。

・行動科学の深化によって「合理的人間」モデルをこえて人間の行動を予測することが可能となったこと。

・これらの理論に基づく実験をリアルタイムで容易に実施できること。

・大量のデータが必須であるがデータを操作するアルゴリズムは企業の営業秘密の壁の中にあり不透明であること。

また世論誘導を通じた選挙への介入という面では、サーチエンジンの検索結果の操作により世論を操作するというような行為も射程となる。このため筆者は、①コンピューター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、特定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等）、③SNS 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）、というような類型を考えることができよう。また、世論誘導を通じた選挙への介入という面では、④サーチエンジンの検索結果の操作による世論操作、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という整理を試みた[11]。

このような民意形成過程の次に、直接的に選挙結果を操作しようとする過程がある。アメリカのシンクタンクである新米国機構(New America)は 2018 年 4 月に選挙のサイバーセキュリティに関する政策提言を公表したが、その中では、選挙へのサイバー攻撃を次のように 3 段階に整理している[12]。

---

[8] Colin Bennett, *Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications*, 13 SURVEILLANCE & SOCIETY, 370-384 (2017).

[9] Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance and Computational Politics,* 19 FIRST MONDAY 1 (2014).

[10] もっとも、このようなビッグデータ分析が常に実際の選挙において奏功するとは限らないとも指摘される。2016 年大統領選挙では、ビッグデータ分析を過信して街頭演説の場所を絞り込んだりしたことがクリントン陣営の敗因の一つとなったとの分析がある。渡辺将人「2016 年アメリカ大統領選挙の選挙運動」選挙研究 33 巻 1 号（2017 年）24-25 頁。

[11] 湯淺、前注 5。

[12] NEW AMERICA, CYBERSECURITY INITIATIVE: HOW TO THINK ABOUT ELECTION CYBERSECURITY?, 6-7 (2018).

第 1 は有権者の民意形成への介入と世論誘導によって選挙結果に影響を与えようとする段階である。第 2 は選挙管理機関へのサイバー攻撃や電子投票機へのサイバー攻撃等によって有権者名簿や投票記録それ自体を改ざんする等、直接的に選挙結果を操作しようとする段階である。第 3 は、投票所を案内したり開票結果を公表したりする選挙管理機関のウェブサイトへの攻撃や選挙に関するニュースサイトへの攻撃等によって選挙に混乱をもたらそうとする段階である。

後述するように、EU も世論誘導から選挙管理機関へのサイバー攻撃等までの各段階を、選挙へのサイバー攻撃として広く捉え、対応を加盟国に促している。また 2017 年 11 月 27 日・28 日両日、ドイツのコンラート・アデナウアー財団(Konrad Adenauer Stiftung)主催による国際会議「乗っ取られる選挙(Hacked Election)」が東京で開催された[13]。ドイツ、アメリカ、インド、モンゴルその他各国のサイバーセキュリティ専門家、政党関係者、研究者による発表と討議が行われ、筆者も参加して報告を行ったが、ここでも「乗っ取られる選挙」として民意形成過程から選挙管理機関へのサイバー攻撃までの広範な含意を前提とした議論が行われた。

これらから考えると、選挙のサイバーセキュリティというとき、選挙管理機関へのサイバー攻撃や選挙に使用する電子機器類等へのサイバー攻撃だけを念頭に置くのは不十分であり、投票を通じた民意の表出という選挙の機能に着目して、その民意形成過程において外国政府等が背景となってサイバー攻撃とサイバー空間の悪意をもった利活用によって介入しようとすることも選挙のサイバーセキュリティ対策の射程に入れるべきであることが理解されよう。

２．３．SPE 事件

サイバー攻撃を、民主主義を支える理念・原理・制度への攻撃を見なして政府がこれに対処した初の例は、2014 年 11 月 24 日に発生したソニー・ピクチャーズ・エンタテインメント(SPE)社へのハッキング事件に対するアメリカ政府の対応であると思われる。

SPE 事件は、SPE がハッカーによるサイバー攻撃によってシステムをダウンさせられ、大量のデータが流出したと報道されたもので、流出したデータの中には、同社の映画に出演した俳優のパスポート番号や社会保障番号、同社の社員の給与などの個人情報のほか、未公開を含む 5 本の映画の映像データが含まれていた。さらに同社のホームページが改ざんされ、「要求が満たされるまで我々はハッキングを続ける」、「もし我々に従わない場合、以下に示すデータを全世界公開する」等というハッカーからの脅迫メッセージが掲載された。SPE は当時、北朝鮮（朝鮮民主主義人民共和国）の指導者である朝鮮労働党の金正恩第一書記を殺害することで北朝鮮は民主的な国家になるというストーリー「The Interview」という映画を公開する予定であり、ハッカーの要求はこの映画の公開中止であるとみられた。このため SPE は、公開を強行した場合には観客の安全に懸念が生じるとして、12 月 17 日に上映を中止すると決定した。

しかし 12 月 19 日、アメリカのオバマ大統領は記者会見を行い、「SPE の状況には同情するが、上演中止は誤っている」と批判した。さらに 2015 年 1 月 2 日、SPE に対するサ

[13] http://www.kas.de/politikdialog-asien/en/publications/50936/

イバー攻撃は「米国企業に破滅的な財務上の影響を与え、アーティストや他の市民の表現の自由を侵害することを画策した」ものであるとして、北朝鮮に対する追加制裁を行う大統領令を発出した。アメリカ政府は、私企業である SPE に対するサイバー攻撃に対して、外国政府が介入しているとして当該外国政府に対して外交上の制裁手段を発動したのである。外交上の制裁手段を発動した理由として、当該企業への財務上の影響という財産権もさることながら、「アーティストや他の市民の表現の自由を侵害」という国民の精神的な権利への侵害を挙げた。

アメリカ政府が SPE 事件を単なる私企業へのサイバー攻撃、サイバー犯罪とは捉えなかった理由として考えられるのは、かねてからアメリカはサイバー空間自体の保護やサイバー空間における自由なデータ流通や言論・経済活動の自由に対して強い関心を示してきたということである。

アメリカ政府は、2011 年 5 月にサイバー空間国際戦略(International Strategy for Cyberspace)を公表し、経済、ネットワークの防護、法執行（警察） 、国防、インターネット・ガバナンス、国際開発、インターネット上の自由の維持という 7 領域においてアメリカがめざす目標を提示している。SPE は一映画会社にすぎず、重要インフラ産業とは異なり、SPE の企業活動に支障が出たからといってただちにアメリカ市民の生活に重大な影響が出るというわけではないであろう。しかし、SPE に対するサイバー攻撃は、サイバー空間国際戦略が示すサイバー空間における経済とインターネット上の自由に対する重大な挑戦であると見ることは可能である。このような事件が続出すれば、アメリカの企業はサイバー攻撃によってその事業の推進に大きな支障を受けることになるばかりか、アメリカ国民が表現の自由や知る権利を享受することにも制約を受けることになる。このことは私企業に対するサイバー犯罪をこえるものであり、政府としてこれに外交政策によって対峙する必要があると判断したものと思われる。

SPE 事件では、アメリカ政府は、外交的対抗、経済的対抗、技術的対抗という 3 つの対抗手段を講じている。

外交的対抗手段として、ケリー国務長官が北朝鮮に影響力を有する中国の王毅外交部長に対して電話で北朝鮮のインターネット遮断に関する協力要請を行っている。これに対して 12 月 23 日に中国政府は記者会見を行い、華春蛍・報道官が「SPE に対するサイバー攻撃に北朝鮮政府に関与したという証拠はなく、北朝鮮政府とアメリカ政府は直接対話すべき」という趣旨の声明を発表したが、両国政府間で何らかの協議が行われた模様である。

より具体的な対抗手段となったのは、経済的対抗である。財務長官による追加制裁を実施し[14]、北朝鮮政府に関係する 3 機関と、それらの機関からイラン、ロシア、中国等に駐在する 10 名を制裁対象とした。

さらに、技術的対抗として、アトリビューション活動を行っている。2015 年 1 月 7 日、FBI のコミー長官がサイバーセキュリティの国際会議の席上で、事件の後に SPE から情報提供を受けて調査した結果、北朝鮮政府が責任を有していると結論を出すのに十分な証拠をつかんでいると述べた[15]。

---

[14] https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea

[15] FBI は、攻撃に用いられたマルウェア（コンピュータ・ウィルス）や攻撃経路が以前に

もっとも、外交官追放等の外交的手段や口座凍結等による制裁では不十分であるとして、プロ・アクティブ[16]、アクティブ・サイバー・ディフェンス[17]のような積極的な技術的対抗手段の実行を主張する議論も存在する。ただし積極的な技術的対抗手段には、国際法的評価[18]と国内法的評価[19]の乖離の恐れという問題が存在するほか、本当に実効性を有するか[20]という疑念も提示されている。

２．４．2016 年アメリカ大統領選挙とサイバー攻撃

2016 年に行われたアメリカ大統領選挙は、2 期 8 年の民主党オバマ政権の後の大統領選挙という点で注目されたが、選挙という民主主義を支える制度へのサイバー攻撃が行われ、

北朝鮮がアメリカ政府を攻撃した際に使われたものと類似していること、北朝鮮が関係しているとみられる IP アドレスが使われた痕跡があることが理由とする。FBI National Press Office, *Update on Sony Investigation*, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

16 2017 年 10 月には、民間事業者によるアクティブ・ディフェンスを合法化するアクティブ・ディフェンス確実化法案(Active Cyber Defense Certainty Act)が連邦議会に提出された。同法案はサイバー攻撃被害者に hack back（逆侵入）を許容するものであり、論議を呼んだものの、可決に至らなかった。H.R.4036 - 115th Congress (2017-2018). 同法案については、政府関係者からも反対、懸念が表明された。

17 アクティブ・ディフェンスによる積極的対抗を主張するものとして、SCOTT JASPER, STRATEGIC CYBER DETERRENCE: THE ACTIVE CYBER DEFENSE OPTION, 165-185 (2017)などを参照。

18 サイバーセキュリティ及び国際法の専門家がサイバー空間における武力行使該当性について検討したタリン・マニュアルにおいては、他の主権国家に対するサイバー攻撃に係る国家責任の可能性について指摘する。MICHAEL SCHMITT, ED., TALLYIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017). 河野桂子「サイバー・セキュリティに関する国際法の考察：タリン・マニュアルを中心に」戦略研究 15 巻（2015 年）25 頁以下、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 年）参照。また主権との関係については、中国が 2017 年に中華人民共和国サイバーセキュリティ法を制定し、第 1 条で「サイバー空間の主権及び国家の安全、社会公共の利益を維持」することを謳っていることが注目されるが、サイバー空間と国家主権との関係については塩原俊彦「サイバー空間と国家主権」境界研究 5 号（2015 年）29 頁以下参照。

19 ジョージ・ワシントン大学サイバー及び国土セキュリティセンターが 2016 年 10 月に発表した *Into the Grey Zone: The Private Sector and Active Defense against Cyber Threats* は民間事業者による積極的対応の可能性を示唆する。Center for Cyber & Homeland Security, George Washington University, *Into the Gray Zone: Active Defense by the Private Sector against Cyber Threats*, https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf. また州法レベルでは、2018 年にジョーシア州議会で hack back（逆侵入）を許容するコンピューター犯罪法改正案(SB 315)が賛成多数で成立したものの、マイクロソフト、Google 等のインターネット企業からも強い反対があり、ディール州知事は 5 月 8 日に法案への署名を拒否した。法案の審議経緯については州議会サイトを参照。http://www.legis.ga.gov/Legislation/en-US/display/20172018/SB/315

20 このような hack back の有用性と法的問題点、特に政府・安全保障機関と民間事業者との相違について検討するものとして、Alan Brill & Jason Smolanoff, *Hacking Back Against Cyberterrorists: Could You? Should You?*, 9 DEFENSE AGAINST TERRORISM REV. 35 (2017)参照。

ソーシャルネットワーキングサービス（SNS）から大量の個人情報を窃取して世論誘導等に利用したとみられる事例としても、歴史的なものになったといえる[21]。またアメリカ政府が、ロシア政府によるサイバー空間を利用した大統領選挙への介入を声明したという点でも、歴史上例を見ないものとなった。

この間のサイバー攻撃とアメリカ政府の対応に関する経緯は、表1の通りである。

表 1． 2016年アメリカ大統領選挙におけるサイバー攻撃の経緯

2016年5月18日	国家情報長官室のクラッパー(Clapper)報道官が、大統領選挙がハッカーの攻撃対象となっていると声明を発表
2016年7月	ウィキリークスが民主党の内部メール約2万通を公表、公表されたメールの中には民主党全国委員会のシュルツ(Schulz)委員長が民主党の大統領候補をクリントン(Clinton)候補と争ったバーニー・サンダース(Bernie Sanders)上院議員を否定的に述べたもの等が含まれていた
2016年7月24日	シュルツ委員長が民主党全国大会開幕前日に突然、委員長を辞任
2016年10月7日	国家安全保障省と国家情報長官室が、共同で「アメリカの情報機関のコミュニティは、政治団体を含むアメリカの市民や組織からの電子メールの近時の漏洩は、ロシア政府の指示によるものと確信する」と声明
2016年10月7日	共同声明の数時間後、ウィキリークスがクリントン候補のポデスタ選挙対策委員長のGmailからハッキングしたとみられる個人の電子メールを2000通以上暴露
2016年11月8日	大統領選投票日
2016年12月8日	オバマ(Obama)大統領が、情報機関に対してロシアからの大統領選に対するサイバー攻撃について詳細に調査するように指示
2016年12月29日	アメリカに駐在するロシアの外交官35名を国外追放する措置を講ずると発表
2017年1月6日	中央情報局（CIA）、連邦捜査局（FBI）、国家安全保障局（NSA） が「近時の米国選挙におけるロシアの活動と狙いに関する評価」を公表
2017年5月9日	トランプ大統領がコミー(Comey) FBI長官を解任
2017年5月17日	マラー(Mueller)元FBI長官が、ロシア介入疑惑を捜査する司法省特別検察官に任命される
2017年10月30日	マラー特別検察官がトランプ陣営関係者のポール・マナフォート、リック・ゲーツ両被告を起訴

[21] 湯淺墾道「選挙とサイバーセキュリティ（1)」選挙2018年1月号（2018年）10頁以下、「選挙とサイバーセキュリティ（2)」選挙2018年2月号（2018年）9頁以下参照。

2018 年 4 月 10 日	ケンブリッジ・アナリティカ社への個人情報不正流出問題で、Facebook 社ザッカーバーグ(Zuckerberg) CEO が連邦議会上院司法委員会及び商業科学運輸委員会との合同聴聞会で証言
2018 年 4 月 11 日	ザッカーバーグ CEO が連邦議会下院資源商業委員会の聴聞会に出席して証言
2018 年 5 月 22 日	ザッカーバーグ CEO が欧州議会で証言

本事件に際しては、Facebook から流出した大量のユーザーの個人情報が利用されたとみられている。流出は、アレクサンダー・コーガン氏というケンブリッジ大学の研究者が開発した「これがあなたのデジタルライフ(This is your digital life)」という Facebook 上で利用するアプリが発端となって発生し、Facebook は「これがあなたのデジタルライフ」に対して、アプリを利用したユーザーの個人データを受け取ることを認めた。Facebook 側の主張によれば、この個人データの第三者への提供などは契約で禁じていたが、コーガン氏が契約に違反して第三者に転売したという。その転売先はイギリスの政治コンサルティング会社であるケンブリッジ・アナリティカ社(Cambridge Analytica)であり、同社は 2016 年 6 月にイギリスで実施された EU 離脱国民投票では離脱側、2016 年のアメリカ大統領選挙ではトランプ陣営にコンサルティングを行ったことで知られる。またトランプ陣営の最高責任者としてトランプ候補を当選に導き、トランプ政権で 2017 年 8 月まで首席戦略官と上級顧問を努めていたスティーブ・バノン氏は、かつて同社の役員を務めていた。

本事件は、上記のような背景事情も含めて現在も特別検察官による捜査が継続中であり、事実関係が明らかになっていない部分が多い。しかし、2016 年アメリカ大統領選挙は、選挙管理機関・候補者や政党等へのサイバー攻撃を行い、それによって得られた情報も利用しつつ SNS を利用して世論誘導を試みたという点で、サイバー攻撃とサイバー空間の悪意をもった利活用とが連関した実例となっている。

この事件を受けて、2017 年 1 月 6 日、国土安全保障省は、選挙インフラを重要インフラ [22]の一つとして指定した。これによって、国土安全保障省は要請があった場合に選挙管理機関への支援を行うことができるようになったほか、他の情報機関との連携、インシデント情報の共有等も進められることになった。

ただし選挙インフラを重要インフラへの指定したことによる施策はフェイクニュース対策等を含めるものではなく、当初は州の選挙管理機関側が重要インフラ指定に反対していたこともあって [23]、必ずしも有効な対策とはならないという指摘 [24]もある。また、Facebook からの大量の個人情報流出という点に焦点が当たっているためか、有権者個人の投票権の侵害という観点からこの問題を取り扱おうとする議論は、現時点ではあまり見

[22] 42 U.S.C. §5195c(e).
[23] Eric Fischer, *The Designation of Election Systems as Critical Infrastructure*, 7-5700 IN FOCUS, https://fas.org/sgp/crs/misc/IF10677.pdf.
[24] David Fidler, "Transforming Election Cybersecurity" (2017). Articles by Maurer Faculty. 2547. https://www.repository.law.indiana.edu/facpub/2547

受けられない。

２．５．2019 年 EU 議会選挙

前述のようにサイバー攻撃とサイバー空間の悪意をもった利活用の脅威が 2016 年アメリカ大統領選挙において顕在化した後、EU は、選挙をサイバーセキュリティの重要な政策領域として位置づけるようになった。サイバーセキュリティ問題は、実際の選挙の執行にも影響を与えている。

選挙への影響としては、フランス在外投票におけるオンライン投票の中止が挙げられる。フランスでは2012年から国民議会選挙の在外投票にオンライン投票(インターネット投票)が導入され、多くの在外有権者に利用されてきた。2012 年選挙の場合、2012 年 5 月 23 日から 29 日までと、6 月 6 日から 12 日までの二回の投票期間（フランス国民議会の議員選挙は二回投票制となっているため）に、約 24 万票がオンラインによって投票された。2017 年大統領選挙からは、大統領選挙の在外投票についてもインターネット投票を導入することが計画されていた。しかし 2017 年 3 月 6 日、フランス外務省は在外投票におけるオンライン投票（インターネット投票）[25]の休止を発表した。これは、フランスの国家サイバーセキュリティ庁がフランスの選挙に関するサイバー攻撃の可能性がきわめて高いと警告したことに基づくとされるが、実際に 5 月の 2017 年フランス大統領選挙の際には、マクロン候補陣営の関係者の電子メールが 2000 通以上窃取されて公開されるという事案（「マクロン・リーク」と呼ばれる）が発生した [26]。この結果、2017 年 6 月 11 日及び 18 日に行われた国民議会選挙は、すべて紙の投票または代理投票によって実施された。

EU においては、フェイクニュース対策は、デジタル単一市場創設という政策領域の一分野として位置づけられ [27]、デジタル経済・社会担当としてマリヤ・ガブリエル委員（ブルガリア）[28]が所掌する。EU は近年、SNS を利用した世論誘導について disinfromation という語も用いており（本稿ではさしあたり「虚偽情報の流布」とする)、虚偽情報の流布は表現の自由という基本的人権の侵害であると捉えている。

2018 年 6 月 21 日にセキュリティを担当するジュリアン・キング委員が行ったスピーチは、EU の立場を端的に示している [29]。キング委員は、選挙に対する干渉としては 2 つのカテゴリーがあるとする。第 1 は制度に基づくものであり、第 2 は有権者の行動に基づくものである。

第 1 のカテゴリーには、有権者の数や票数を変えるために選挙管理や投票関係技術にサイバー攻撃を行って操作する行為が含まれる。たとえば選挙管理システムに侵入して有権

---

[25] https://www.diplomatie.gouv.fr/fr/services-aux-citoyens/actualites/article/francais-de-l-etranger-modalites-de-vote-aux-elections-legislatives-06-03-17

[26] 手法はアメリカ大統領選挙における活動と相似しており、マクロン候補陣営関係者の電子メールを窃取してリークすることにより、マクロン候補への評価を下げる狙いがあったとされている。また電子メールだけではなく、文書や写真も窃取されて公開された。

[27] https://ec.europa.eu/digital-single-market/en/fake-news

[28] 2009 年から 2017 年まで欧州議会議員をつとめ、Kristalina Georgieva 委員が 2017 年に世界銀行 CEO 就任のため委員を辞任した後任として就任した。

[29] https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-aspen-institute-protecting-western-democracies-manipulation-and_en

者登録ができないようにしたり、投票データを入手してデータを改ざんしたりすることがある。キング委員は、このような行為は選挙への信頼を喪失させるものであるが、実際に第2のカテゴリーのほうが深刻であるとする。

「私の見解では、これ（訳注：第2のカテゴリーのこと）には3つの形式があります。キャンペーン中の重要なポイントで情報を明らかにすることによって世論を変えるように設計されたハッキングとリーク。世論を動揺させ選挙結果に影響を与えるためのフェイクニュースの使用。そして、ユーザーの個人的な特性データから導き出された心理測定に基づいて特定ユーザーを標的としてメッセージを恣意的に送ること、ケンブリッジ・アナリティカのようなやり方です。これらの 3 つはサイバーを利用した選挙操作の別々の形式ですが、すべてが特定の方向に結果を歪めるように設計されています。」

「（有権者の）行動に基づく脅威に対抗するために、欧州委員会は4月に、ソーシャルメディアが民主主義に対する武器にならないようにするためインターネットプラットフォームに対して期待することを含めて、虚偽情報流布や行動の操作に対してさまざまな措置を提案しました。大規模な虚偽情報流布という武器は、現代の大量破壊兵器となりえます。」

スピーチの場ということもあるが、SNS を通じた虚偽情報流布による有権者の世論操作を「現代の大量破壊兵器」とまで呼んでいることが注目される。

EU におけるフェイクニュースへの取組みは、公的には 2017 年 5 月 16 日にジャン＝クロード・ユンケル委員長がガブリエル委員に対して書簡 [30]を発出したことにより開始された。

同書簡では、市民を保護するため、オンライン・プラットフォームによるフェイク情報の流布によって民主主義を脅かしている実態について EU レベルで調査する必要があると指摘している。このため、第一副委員長（より良い規制、組織間関係、法の支配と基本的人権、表現の自由、情報の自由、メディアの多様性と自由、インターネットの公開性、及び文化的・言語的多様性担当）と密接に連携して、調査を実施するように要請した。

2017 年 11 月 13 日から 2018 年 2 月 23 日にかけて、フェイクニュースとオンライン虚偽情報流布に関する意見聴取(Public consultation)が実施された [31]。意見聴取項目は、第 1 にフェイク情報とそのオンラインでの拡散の定義、第 2 にオンライン上でのフェイク情報の拡散に対してすでにプラットフォーム、ニュースメディア、市民組織等が実施している対策の調査、第 3 はフェイク情報のオンラインでの拡散を防止して情報の質を高める方策についての将来の行動の射程である。その結果は、ウェブサイト上で公開され [32]、同時期に実施された EU の公的な世論調査であるユーロバロメーターによる世論調査結果も公開され

30 https://ec.europa.eu/commission/commissioners/sites/cwt/files/commissioner_mission_letters/mission-letter-mariya-gabriel.pdf

31 https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_en#about-this-consultation

32 https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-online-disinformation

た [33]。また意見聴取の一環として、2017 年 11 月 13 日・14 日にマルチステークホルダーによる会議も開催された [34]。

2018 年 1 月 15 日にはフェイクニュース及び虚偽情報流布に関する有識者会合(High-Level Group on Fake News and online disinformation)が設置された [35]。この有識者会合には Facebook、Twitter、Google 代表も含まれ、SNS 事業者も加えたマルチステークホルダーによる協議の場となっている。2018 年 2 月 7 日には有識者会合の第 2 回会合が開催され、3 月 12 日に最終報告書が公表された [36]。

最終報告書は、公的にも私的にも検閲に該当するような対策は明確に排除されるべきであるとし、インターネットの分断や憎悪をもたらすような技術的方策も避けるべきであるとした。このことを前提として、報告書では「多元的な対応(multi-dimensional approach)」の必要性を指摘して、具体的には次の 5 点を勧告した。

・オンラインニュースの透明性を高めること。オンラインでの流通を可能にするシステムに関するデータの適切かつプライバシーに準拠した共有を含む。
・虚偽情報に対処するためメディアリテラシー及び情報リテラシーを促進し、ユーザーがデジタルメディア環境をナビゲートできるようにすること。
・ユーザーとジャーナリストが虚偽情報に対抗し、急速に進化する情報技術との積極的な取組を促進するためのツールを開発すること。
・欧州のニュースメディアのエコシステムの多様性と持続可能性を保護すること。
・異なるアクターによる措置を評価し、必要な対応を常に調整するため、欧州における虚偽情報の影響に関する継続的な調査を実施すること。

このような取組をへて、2018 年 4 月 26 日、虚偽情報に対する「多元的な対応」が正式に提案された [37]。

提案された多元的対応は、次の内容により構成されている。

・虚偽情報に関する行動規範
・各ファクトチェッカーの独立ネットワークの構築
・虚偽情報に対するセキュアなヨーロッパのオンライン・プラットフォーム
・メディアリテラシーの強化
・加盟国に対する選挙のレジリエンス強化支援

---

33 http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183

34 https://ec.europa.eu/digital-single-market/en/news/recordings-multi-stakeholder-conference-fake-news

35 https://ec.europa.eu/digital-single-market/en/news/experts-appointed-high-level-group-fake-news-and-online-disinformation

36 https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

37 http://europa.eu/rapid/press-release_IP-18-3370_en.htm

・質の高い多様な情報の支援
・戦略的なコミュニケーション政策の調整

プラットフォーマーに対しては 2018 年 7 月までに共通の行動規範(a common Code of Practice)を策定して遵守することを求めた。行動規範は、具体的には以下を目的とするとしている。

・スポンサーがついているコンテンツ、特に政治広告についての透明性を確保すること、また政治広告のターゲティングオプションを制限し、虚偽情報の提供者の利得を削減すること。
・アルゴリズムの機能と第三者による検証を可能にすることについて、明確に説明すること。
・他の視点を代表する異なるニュースソースをユーザーが発見してアクセスしやすいようにすること。
・フェイクアカウントの特定と閉鎖対策、自動ボットの問題への取組を開始すること。
・ファクトチェッカー、研究者、および公的機関がオンラインの虚偽情報を継続的に監視できるようにすること。

ガブリエル委員は、2018 年 9 月 26 日に Facebook、Google 等のプラットフォームと行動規範の遵守について合意したと公表し [38]、各プラットフォームのベストプラクティスも公表された。2018 年 12 月までに委員会は進捗状況を報告するとしており、今後はこれらの方策の有効性が検証されることになる予定である。

さらに、EU の専門機関でサイバーセキュリティを所掌する欧州ネットワーク情報セキュリティ機関（ENISA = European Network and Information Security Agency）[39]も、フェイクニュースや虚偽情報流布問題に関与している。ENISA の選挙のサイバーセキュリティ対策への参画は、直接的には、「ネットワーク及び情報システムの安全性に関する指令（EU）2016/1148」に基づく [40]。

ENISA は、2017 年 6 月に「サイバー空間における虚偽情報流布活動」[41]と題するレポートを公開した。

このレポートでは、「虚偽情報流布活動は、サイバー空間がネットワークとコンピューター機器とを統合するだけではなく、人的要素をも統合している」として、虚偽情報流布活動とその対策を概観し、サイバー攻撃によって窃取された情報を、場合によってはフェイクニュースも交えて暴露することを「汚染されたリーク(tainted leak)」と呼んでいる。

また ENISA は、2018 年 4 月に「ネットワーク及び情報セキュリティの強化並びにオン

[38] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454
[39] EU の専門機関の一つで、「EU 規則第 460/2004」に基づき 2004 年に設立された。
[40] 同指令の内容を解説するものとして、夏井高人「EU の行政機関に適用される個人データ保護規則における基本概念―個人データ保護条約及び EU 一般個人データ保護規則との関係を含めて―」法律論叢 89 巻 2・3 号（2017 年）205 頁以下参照。
[41] https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space

ライン虚偽情報流布（フェイクニュース）からの保護」[42]と題するオピニオン・ペーパーを公開した。その中では、ネットワーク及び情報セキュリティに関する一般的な対策として、選挙に関するシステムや機器類を重要インフラストラクチャの中に含めることを提案した。

また ENISA のオピニオン・ペーパーは人工知能についても言及し、「AI アルゴリズムの利用を、オンライン詐称キャンペーンやスクラップやスパムなどのオンライン・プラットフォームの誤用の検出を支援するために、導入するべきである。これらのアルゴリズムの出力は、何らかの措置を講じる前に、人間が確認する必要がある。」として、人工知能を虚偽情報流布の防止のため利用することを勧告すると共に、人間の関与が必要であることを指摘している。

ENISA の勧告をうけ、2018 年 2 月 14 日、欧州委員会は「欧州の特性強化と 2019 年欧州議会選挙の効果的な実施に関する委員会勧告」[43]を公表した。同勧告においては、欧州議会議員選挙に先立って欧州に関する議論に欧州市民を参画させること、欧州委員会委員長候補者の支援を行うこと、国内政党と欧州政党との関係について有権者に情報提供すること、国民と欧州の政党との関係についての有権者用の情報を整備することを勧告している。さらに、（選挙の）効率的な施行という項目も勧告として挙げている。その中では、サイバー攻撃と虚偽情報流布による選挙干渉のリスクを認識し、各国の選挙管理機関が実務的な対策等についての知見を共有してベスト・プラクティスを各国で実践するように求めた。

これをうけて、各国の政府代表、欧州委員会代表及び ENISA は、ネットワーク情報セキュリティ協力グループを組織して検討を進め、2018 年 7 月に「選挙技術のサイバーセキュリティに関する概要(Compendium on Cyber Security of Election Technology)」[44]と題するガイドラインが公表された[45]。ガイドラインはクラウス・ウェーレ(Klaus Welle)欧州議会事務総長の要請に基づき作成され、作業にあたってはエストニア及びチェコのサイバーセキュリティ機関が主導した[46]。このガイドラインは、主として各国の選挙管理機関における技術的対策を主な内容としているが[47]、フェイクニュースや虚偽情報流布への対策として、各国の経験を共有することの重要性を指摘している。またガイドラインには、これまでに選挙に関係して行われたサイバー攻撃の例が掲載された[48]。

３．対策の枠組み

前述したように、アメリカや EU では、選挙に対してサイバー攻撃やサイバー空間の悪意

---

[42] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news/
[43] https://ec.europa.eu/commission/sites/beta-political/files/recommendation-enhancing-european-nature-efficient-conduct-2019-elections_en.pdf
[44] NIS Cooperation Group, *Compendium on Cyber Security of Election Technology,* available at https://www.govcert.cz/download/akce-a-udalosti/Election_security_compendium_July_5_2018.pdf
[45] ガイドラインについては、湯淺墾道「2019 年欧州議会選挙とインターネット・SNS（3)」選挙 2018 年 10 月号（2018 年）1 頁以下参照。
[46] National Cyber and Information Security Agency, *Compendium on Cyber Security of Election Technology.* https://www.govcert.cz/en/info/events/2625-compendium-on-cyber-security-of-election-technology/
[47] *Supra* note 44, at 6.
[48] *Ibid,* at 49.

をもった利活用による介入・干渉の経験、またはその現実の危険性を背景として、重要インフラへの指定や、セキュリティ専門機関との連携によるガイドライン制定等が進んでおり、その成果が現れているかどうかは措くとしても、選挙という制度に対するサイバー攻撃に対して政府が対策を講じようとしている。

ただし両者のアプローチは異なり、アメリカの場合、ロシア政府が背景にあるとされることから、アメリカ連邦議会における議論はロシア政府や関係者がスポンサーになっていると見られる広告出稿やアカウントの開設問題、プライバシー保護問題が主な射程となっている。ケンブリッジ・アナリティカ社への大量の個人データの流出問題がその背景にあることは言うまでもないが、当初、連邦議会は SNS に対する法的規制を強めることには消極的であるとみられていた[49]。しかしその後、連邦法によるプライバシー保護規制強化の方向に動く可能性も出てきている。また州法による規制強化の可能性もある[50]。

他方で日本においては、冒頭で述べたように各種のサイバー攻撃やサイバー空間を利用した選挙への容喙・干渉への対応の必要性が必ずしも認識されているとはいえない。

しかし選挙への容喙・干渉への対応について考える際に選挙・民主主義に係わる制度、理念、原理の侵害を個人の権利の侵害として捉え、それを法的に救済することは、おそらく難しいであろう。個人の権利という観点から捉える場合、具体的に有権者の選挙権行使に制約を与えたり妨害したりするわけではなく、その前提となる政治的意思決定過程に対して影響力を行使し偏向・誘導しようとする行為が、どのような有権者個人の権利侵害に当たるのか、また権利侵害であるとすればどのように救済することができるのかという問題がある。

選挙権自体の侵害として捉えようとする場合、選挙に関する憲法上のさまざまな原則を選挙権それ自体の中に包含させ、サイバー攻撃や虚偽情報流布活動等を選挙に関する憲法上のさまざまな原則に内包される規範的要求の充足を妨害する選挙権の侵害、またはその行使の侵害と捉えることは、理論的には不可能ではないと思われる。したがって、その侵害に関して、選挙権保障という観点から、国家（政府）は侵害発生防止の責任（少なくとも努力義務）を負うと解することも可能ではあろう。特に、選挙権の中に一定の公務性を認める権利公務二元説の立場[51]からは、サイバー攻撃等や虚偽情報流布活動等を、公務と

---

[49] その背景には、このような個人に関するデータの自由な収集・集積・利活用によってインターネット企業の成長が誘引されてきたことがある。

[50] たとえば 2018 年 6 月 29 日、カリフォルニア州議会は「2018 年カリフォルニア州消費者プライバシー法」を制定する第 375 法案(Assembly Bill No. 375, AB375)を、下院で賛成 73、反対 0、棄権 7、上院で賛成 36、反対 0、棄権 3 という棄権者を除く全会一致で可決した。消費者プライバシー法は、もともとカリフォルニア州のイニシアティブ（州民発案）により制定が求められていたもので、州民投票運動の結果、2018 年 5 月に 629,000 通の州民発案署名が提出されてイニシアティブが受理され、6 月 28 日までに州議会が法案を成立させない場合には、2018 年 11 月に州民投票が実施され、法律として制定するかどうかが決定される予定となっていた。今回、Google 等のインターネット企業の反対にもかかわらず州議会側が消費者プライバシー法を可決し、州知事も署名した背景には、住民投票によってさらに厳格な内容の州法が成立することを回避するねらいがあったとみられている。

[51] 選挙権の法的性質については、これまでも憲法学界においてこれまで数度にわたる論争が繰り返され、特に 1970 年代から 80 年代にかけて選挙権論争とよばれる論争が展開され

しての自由な選挙権行使を妨げるものとして捉え、選挙権の侵害として把握することは不可能ではないと思われる。

ただし、選挙権は選挙制度という制度を通じなければ行使し得ないこと、選挙に関しては「理念」「権利」「原則」が交錯する部分が多いことから、権利に着目してその侵害の救済を図るというアプローチには限界もあろう。権利公務二元説からも「選挙に関する憲法上の原則にはさまざまな側面があるので、それらをすべて同じ選挙権の内容に含ませることは、選挙権をあまりにも包括的にとらえることになりはしないかとの懸念がある。選挙に関する憲法上の原則は人権ならびに国会の章に散在しているので、それらをまとめて整理したり、体系化したりするのはよい。しかしそれを選挙権の内容とする必要は少しもない。憲法上の明記された原則まで一つの権利のなかにすべて取り込むことが、解釈論として望ましい在り方なのか私には疑問である。」とする見方もある[52]。特に、有権者の民意形成の過程へのサイバー空間を通じた介入までを選挙権侵害と捉えることができるかどうかについては、表現の自由や知る権利の問題とも合わせて検討する必要があろう[53]。

サイバーセキュリティとの関係が大きな問題になりつつあるアメリカと EU の事例を参照すれば、インターネットを通じた攻撃・干渉に対して、有権者個人の権利侵害という観点ではなく、理念・原理・制度への攻撃という観点からどのように対応することが可能かを検討するほうが有益であるように思われる。その一つの方向性として、個人的権利利益の救済を図るのではなく、サイバー攻撃やサイバー空間の悪意をもった利活用による介入・干渉を「選挙の Integrity」[54]の侵害の一態様として捉え、制度としての選挙の保護を図るという施策のほうが、実際上は有効なのではないか。

情報セキュリティの領域では、Confidentiality、Integrity、Availability を一般に情報セキュリティの CIA といい、1992 年の OECD 情報セキュリティガイドライン[55]において示された概念である。このうち integrity は情報および処理方法が正確かつ完全であることの保護と定義され、具体的には情報の不正な改竄がないこと、情報処理結果の誤りがないこと、情報に欠損がないこととして一般に理解されている[56]。

1980 年代から情報の処理過程が人間の通常の知覚によっては可視的でないコンピューターが導入されるようになり、選挙管理に導入されるようになったコンピューターや情報システム、それらを相互に結合する情報ネットワークが正確かつ完全に動作することをどのように保証するかという問題が生じたことから、選挙における integrity が問われるようになった[57]。比較政治学や行政学においても、選挙の integrity が注目されており、比較政治

た。選挙権論争については、奥平康弘「参政権論」ジュリスト総合特集選挙（1986 年）6 頁以下、辻村みよ子『「権利」としての選挙権』（勁草書房、1989 年）などを参照。

52 野中俊彦『選挙法の研究』（信山社、2001 年）51 頁。

53 板倉、後注 61 も参照。

54 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 56 巻 4 号（2015 年）71-99 頁参照。

55 OECD, OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS (1992), http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

56 情報セキュリティの領域における integrity の定義の変遷については、岡村久道『情報セキュリティの法律（改訂版）』（商事法務、2011 年）2 頁以下を参照。

57 このような意味での integrity を問題とするものとして、たとえば Roy Saltman, *Accuracy,*

学者のピッパ・ノリスを中心とする The Electoral Integrity Project が発足し、世界各国の選挙の integrity を一定の指標[58]を用いて比較評価するという研究が進められ[59]、報告書も公開されている。選挙の民主化[60]、選挙のガバナンスという観点からみた場合、有権者の政治的意思を公正に選挙結果に反映することが必要であり、特定の勢力や集団が過大に政治的影響力を行使することを制限するため、選挙運動費用や政党の広告費用の高騰化等に歯止めをかけることも必要となる。選挙の integrity は、選挙を民主的に機能させるため一連の選挙のサイクル全体が適正に運用されることを要求するものであり、特定の勢力や集団が過大に政治的影響力を行使することの制限を要請する。このことから、サイバー攻撃やサイバー空間の悪意をもった利活用に対抗するための規制が正当化されるのではあるまいか。

ただ具体的な規制を仮に行おうとする場合、前述の有権者の民意形成への介入と世論誘導によって選挙結果に影響を与えようとする段階における規制を行おうとすると、現時点では有権者の世論プラットフォームとしての SNS に対する規制以外には効果的な方策は取りえないのではないかと考えられる。しかし SNS に対し、現在公職選挙法が定めているような選挙運動規制の対象としてフェイクニュースに関する実効的な法規制を及ぼすことは、副作用を生む可能性も高い。日本においてフェイクニュースを法的に規制することはきわめて困難であるとされており[61]、表現の自由の抑圧につながる恐れもある。このことから、EU が採用したような「共同規制」的手法から始めるのが現実的であるとは思われる。ただ EU においても、2017 年に SNS における法執行を改善するための法律[62]を制定してフェイクニュースについても規制対象に加えることとしたドイツのように、SNS に対して直接的な法規制の網を被せた国も存在する。どのような法規制が可能であり、また有効であるのかについては、EU による 2019 年欧州議会議員選挙に向けた取組の行方と効果を注視する必要がある。

またアメリカのように選挙管理に関係するシステムを重要インフラの一つとして指定するという方策は、日本においては「インフラ」という概念から逸脱するという拒否感・違

Integrity and Security in Computerized Vote- Tallying, 31 COMM. OF THE ACM, 1184 (1988).

58 指標については、Pippa Norris, Richard Frank, and Ferran Martínezi Coma, *Measuring Electoral Integrity Around the World: A New Dataset*, 47 PS: POLITICAL SCIENCE & POLITICS 789 (2014)を参照。

59 研究成果として、次のようなものがある。PIPPA NORRIS, RICHARD W. FRANK, AND FERRAN MARTÍNEZ I COMA, ADVANCING ELECTORAL INTEGRITY (2014), PIPPA NORRIS, WHY ELECTORAL INTEGRITY MATTERS (2014).

60 選挙の民主化については、さしあたり岩崎正洋「民主化とガバナンス」政経研究 49 巻 4 号（2013 年）25 頁以下参照。

61 フェイクニュースの法規制の困難性を指摘するものとして、たとえば板倉陽一郎「フェイクニュースへの法規制は劇薬か」を参照。
https://webronza.asahi.com/politics/articles/2017100100005.html

62 SNS における法執行を改善するための法律。SNS 事業者に違法内容削除義務、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している。鈴木秀美「ドイツの SNS 対策法と表現の自由」慶應義塾大学メディアコミュニケーション研究所紀要 68 号（2018 年）1 頁以下参照、實原隆志「ドイツの SNS 法―オーバーブロッキングの危険性について」情報法制研究 4 号（2018 年）46 頁以下参照。

和感があるかもしれない。しかし選挙は、それが紙の投票用紙を利用して行われているとしても、きわめて多くの電子機器によって支えられているのが現状である。にもかかわらず、実際に選挙管理のさまざまな場面で用いられている電子機器やアプリケーション・ソフトウェア類については統一的な規格や標準がない場合が多い。電子投票システムに関する技術的条件は平成 14 年に公表されているものの、それ以外は各地方公共団体のセキュリティ・ポリシー等に委ねられているというのが実態である。

地方公共団体の深刻な財政難から選挙管理に関する費用・人手も合理化の対象となっているのが実情であり、選挙のサイバーセキュリティを確保するには、費用・人手の確保が必要である。それを含めて選挙を管理する体制への負担増に有権者の同意を獲得することのほうが、先決かもしれない。

４．おわりに

近い将来、大量のデータと人工知能を利用した各種のサービスが選挙に関連して登場する可能性がある。

たとえば現在でも、有権者と立候補者、有権者と政党との考え方の一致度を測定することができるサービスとしてボートマッチ[63]が存在する。ボートマッチを利用すれば、有権者の投票方向の考慮・決定にあたって、有権者と立候補者・政党との考え方の一致度を測定することができるので、誰またはどの政党に投票すればよいかという点できわめて有益な情報を得ることができる。

有権者個人の行動履歴（GPS 情報）や、有権者自身が SNS において位置情報を公開したものを収集・分析することにより、有権者の行動履歴を復元・分析することは十二分に可能となっている。交友関係、趣味・嗜好等も、インターネット上の情報から大量に収集されつつあるので、近い将来には、これらの情報を人工知能関連技術によって詳細に分析することが可能となり、有権者の行動や意思、考え方と、立候補者・政党の考えとの一致を、きわめて精緻に測定するマッチングサービスを提供することも可能となろう[64]。このようなサービスが提供されたとき、中には、投票方向の決定をこの種のサービスに完全に委ねてしまう有権者が出現することも予想される。このような段階に至ったとき、サイバー攻撃やサイバー空間の悪意をもった利活用による選挙への攻撃、容喙、干渉と、それによる影響はさらに深刻なものになるであろう。選挙という民主主義の根幹をなす制度を、どのようにそれらから守るのかはきわめて大きな法的課題であり、本稿は到底、それに対する答えとはなり得ていない。人工知能に関する法制度や開発原則を検討する上で、選挙をはじめとする民主主義を支える理念・原理・制度への影響は看過できないということを指摘して、本稿をひとまず擱筆することにしたい。

---

63 上神貴佳、堤 英敬「投票支援のためのインターネット・ツール―日本版ボートマッチの作成プロセスについて」選挙学会紀要 10 号（2008 年）27 頁以下参照。
64 湯淺、前注 2、298 頁以下を参照。