講演録
Date: 2022.1.6
https://www.jilis.org/report/2021/jilisreport-vol4no1.pdf

ディープフェイクに関する各国の法規制の動向

一般財団法人 情報法制研究所 参与
明治大学 教授
湯淺 墾道

流布活動の蔓延をいかに規制すべきか

明治大学の湯淺でございます。今日は、ディープフェイクに関して、最近各国がどのような規制をしようとしているのかということについて、動向をご紹介させていただこうと思っております。

ディープフェイクに限らず、今日世論形成にSNSが非常に大きな影響を与えるようになってきております。それに伴って、フィルターバブルのような問題も生じておりますし、フェイクニュースやディスインフォメーション―ディスインフォメーションは流布活動そのものを指す場合が多いですが―、流布活動の蔓延をいかに規制すべきか。一方で、フェイクニュースやディスインフォメーションを止めるために、プラットフォーマーが特定のユーザーのアカウントを凍結して、表現内容を抑止するということも頻繁に行われております。私どもが存じ上げている弁護士の先生のアカウントが止められてしまったとか、そういう話はよく聞くわけでございます。

一方で、フェイクニュースやディスインフォメーションの背景にあるのは、従来の世論誘導、民意誘導が、ある程度、ターゲットをグループとして特定して、そのグループ向けの広告を打つというのが普通で、逆に言うと個人をターゲットとするのは難しかったわけですが、これが今日の技術進化によりまして、特定の個人を標的として民意の誘導を行うマイクロターゲティング技術が非常に進化してきているということでございます。実際に、アメリカ大統領選の際に、フェイスブックから違法に流出させた大量のデータを用いて、マイクロターゲティングを行っていた実態は、ケンブリッジアナリティカという、その種のデータ分析・データ誘導を専門に請け負う会社のスタッフであったブリタニー・カイザーという女性がいるんですけれども、ブリタニー・カイザーが回顧録というか暴露本を出しまして日本語にも翻訳されましたが、内幕を赤裸々に書いていらっしゃいます。

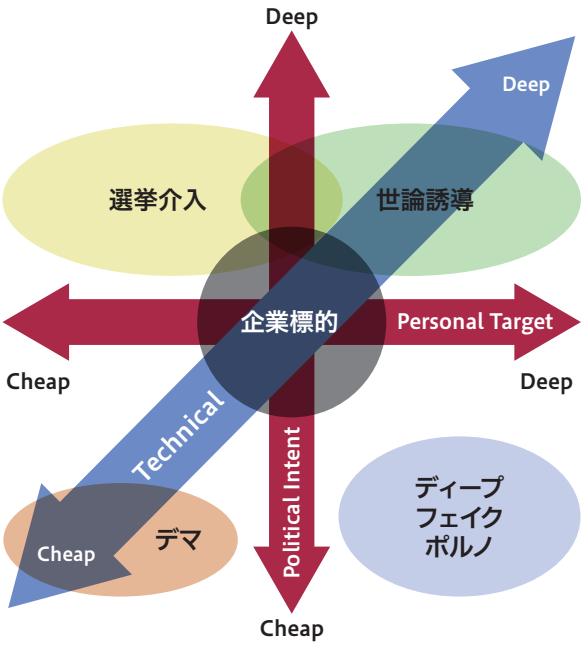
このマイクロターゲティングの基礎になっているのは、個人を特定して、個人の嗜好を測定し、そこに合わせた特定の広告を送り込むといういわゆるアドテクノロジーの高度化ということであって、このアドテクノロジー技術が民意誘導にも用いられているというのが現状であるということです。

フェイクニュース／ディスインフォメーションの分類

フェイクニュースとディスインフォメーションの類も分類するといろいろでありまして、個人をターゲットにしている度合いがチープなものもあれば、ディープなものもあります。政治的意図がディープなものもあれば逆にチープなものもあります。たとえば、熊本で発生した大地震のあとに、ライオンが動物園から逃げ出したというフェイクニュースを流したというのは、正直なところ個人をターゲットにしていない、また、政治的な意図もあまりない愉快犯的なものであった、ガセネタであったということでありますし、それから、政治的な意図はあまりない、低いんだけれども、特定の個人をターゲットにしていると、あるいは特定の性的な嗜好をターゲットにしてばら撒かれているということで問題になってきているのが、ディープフェイクを用いたポルノであります。

ヨーロッパの調査研究機関の調査によりますと、実態としてはディープフェイクのほとんどはポルノであるという指摘もあります。また、ディープフェイク技術を使ったチャイルドポルノも問題化しているところであります。一方で、政治的な意図が非常にディープであり、かつ、個人をターゲットとしている度合いも非常にディープであるというのが、今日問題になっている選挙介入あるいは世論誘導を目的としたフェイ

クニュースやディスインフォメーションであるといえます。なお、選挙介入それ自体には、必ずしも個人をターゲットとしないやり方も横行していますし、政治的な意図が深いという意味では同じですけれども、必ずしも個人をターゲットとしているものはディープではないケースもありますので、私の図では選挙介入はこのへんのところに置いておきました。



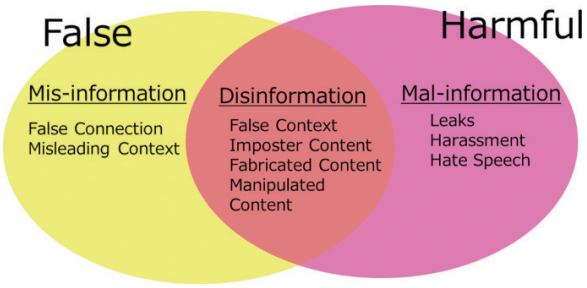
それから、技術的な深さの度合いというのも当然あるわけでして、個人をターゲットとする度合い、あるいは政治的な意図が深いものについては、技術的にもどんどん高度になってきているのが現実でございます。これは、ディープフェイクの語源になっているディープラーニングがどんどん高度化しているということもあるのでしょうけれども、それよりもむしろ、先ほど申し上げたアドネットワークがどんどん高度化しているという実態のほうが、影響ははるかに大きいのだろうと思います。

私の資料の最後にいくつか参考文献を載せてございますが、その中で昨年出ました長迫さんの論文を引用しております。

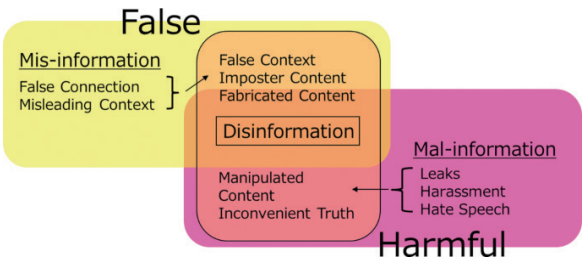
- Tomoko Nagasako, Global disinformation campaigns and legal challenges, Int. Cybersecur. Law Rev. (2020) 1:125–136.
  https://link.springer.com/article/10.1365%2Fs43439-020-00010-7

- 湯淺墾道「郵便・電子投票で民主主義のデジタル化は加速するか」外交66号

長迫さんの分類によりますと、ディスインフォメーションとは間違った情報（Mis-information）であり、かつ悪意を持った情報（Mal-information）が重なり合う象限がディスインフォメーションなのだ、と。ちなみに、悪意を持った情報の中には、それ自体誤っていないもの、リークだとかハラスメントだとかヘイトスピーチもありますので、これらはディスインフォメーションとは言い難い。ということで、長迫さんの分類によりますと、このような図になります。



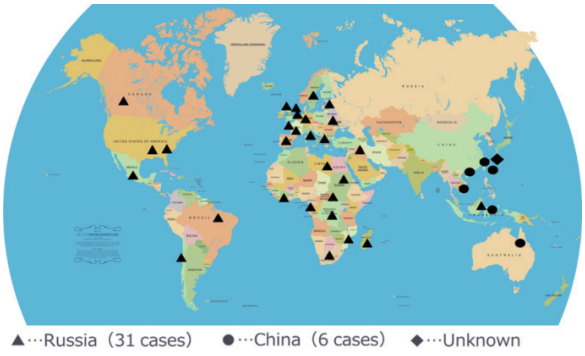
Source: Nagasako 2020



Source: Nagasako 2020

また、間違った情報と悪意のある情報をさらに細かく長迫さんが分類してみたのがこの図でございまして、これも論文から引用しておきましたが、ディスインフォメーションの中にはかなり階層があるということを、長迫さんの研究では示しております。

これも引用でございますけれども、長迫さんが調査をしてみて、ディスインフォメーションが観察された地域です。そのうち、ロシアがおそらく背景にあると思われるものが31事例、中国がおそらく背景にあ



Source: Nagasako 2020

ると思われるものは6事例であったというのが、この論文の中で示されている研究結果であります。

なお、現在ディスインフォメーションにも用いられており、また、プライバシー侵害の危険性が高いということで、サードパーティ Cookieを禁止しようとしている動きがあることは、ご存じの方も多いかと思います。これは、グーグルがGoogle Chromeにおけるサードパーティ Cookieのサポートを段階的に廃止するということを公にしたわけであります。その点についてはグーグルが、プライバシーサンドボックスというウェブサイトで説明しておりますが、さまざまな報道などを見ますと、サードパーティ Cookieの廃止には、広告業界、広告業界というよりは広告ネットワーク業界からの猛反発があったということのようでして、延期をせざるを得なくなったという話もあります。また、サードパーティ Cookieのサポートを止めたとしても、結局各種のフィンガープリント技術が使われるだけであると、ブラウザフィンガープリントだとか、デバイスフィンガープリントを使えば、結局サードパーティ Cookieを使わなくても、ネット上の行動は追跡できますし、9割以上の精度で特定できるというような研究もあるようですので、サードパーティ Cookieがサポートされなくなったからといってただちに問題が解決されるというわけではなさそうであります。

ディープフェイクの法規制

そういうような背景があることを前提としまして、ディープフェイクの法規制ということについて、本題のお話に入らせていただこうと思います。現時点で、選挙への介入目的や、あるいは世論誘導目的でのディープフェイクにフォーカスした規制を行っているのはEUとアメリカであると思います。その他の国でもフェイク規制を行っている国はかなり増えてまいりましたが、それは必ずしも選挙介入や世論誘導という文脈に限定されていなかったり、あるいは、むしろフェイクの取り締まりを口実として事実上の言論規制を敷くことに使われていたりするようなケースもあります。そういう意味でいいますと、選挙介入、世論誘導をターゲットにしたディープフェイクを排除しようとしているのは、特にEUとアメリカであるということができると思います。ただし、EUの対策は、ディスインフォメーション対策全般をフォーカスしていますので、ディープフェイクに特化したものでありません。これは、すでにEUはプラットフォーマーに対して、ディスインフォメーション全般の対策を取ることを求める自主的な規制、Code of Practiceを要求しているわけで、このような手法は生貝先生によれば共同規制であると名付けられておりますし、また共同規制という考え方は先般成立しました我が国の特定プラットフォーム規制法にも取り入れられているところであります。

これに対しまして、現時点でアメリカの州法と連邦法は、逆にディスインフォメーション全般をフォーカスするのではなくて、ディープフェイクの作成とディープフェイクの流布のところに焦点を当てているわけです。なぜディープフェイクだけなのかということについてはいろんな議論がありえますが、やはり表現活動全般に対する規制を敷くことには表現の自由との抵触の可能性が出てくること、あるいは、プラットフォーマーのほとんどはアメリカの企業ですから、やはりプラットフォーマーの成長によってアメリカ経済を牽引してきた実情等に鑑みると、本音としてプラットフォーマー規制はやりたくないというような問題など、様々な政治的な背景はあるんだろうと思います。

ちなみに、国際法上、ある国が、他国の政治や選挙に介入するために、ディープフェイクを作ってディープフェイクを組織的に流すディスインフォメーション活動をすることについてはどうなのかということです。サイバー空間を使った攻撃が果たして武力行使に該当するかということについては、タリン・マニュアル、今バージョン2でまもなくバージョン3.0が出るそうですけれども、タリン・マニュアルでずっと研究されてきたところですが、この選挙干渉については、政治的な言説としては「戦争」だという言い方がされます。アメリカの場合はディック・チェイニーや、国連大使のニッキー・ハーリーなどが公的に言いましたが、これは政治的な言説であって、法的にはこれは国際法上許容される諜報活動の一環に過ぎないので武力行使に当たらない、よって戦時国際法は適用されないという見方が今日の通説のようであります。

アメリカにおける規制の現況 ―選挙管理システム

さて、アメリカにおける規制をもう少し細かくて見てまいりますと、アメリカではそもそも、選挙管理システムは今から4年前に重要インフラとしての指定を受けました。指定の対象は有権者登録データベースと関連する情報通信システム、それから選挙管理に使用される情報インフラおよびシステム、投票結果の開票、集計および表示システムなどですね。それから、投票システムおよび関連インフラ、選挙管理

および投票システム用のストレージ、それから投票所それ自体です。これらは重要インフラ指定を受けていますので、もし、仮にこれらに直接サイバー攻撃が行われれば、重要インフラとして、アメリカの場合選挙は基本的に州政府によって執行されますけれども、州政府が要請した場合には国土安全保障省が連携して対処することができるという構造になっております。また、情報共有と分析を行ういわゆるISACの選挙版として、選挙インフラISAC（Elections Infrastructure ISAC）、いわゆるEI ISACが設置をされておりまして、連邦政府と州政府が情報共有をしております。で､資料の中には記載しておりませんが、注目するべき動きとしまして、最近ワシントン州が自前の選挙に対するサイバー攻撃を分析するための設備を整えて、かつ、州知事が分析を行うことが州法によって義務付けられたというケースがございましたので、これについても連邦政府と情報共有しながら行っていくのだろうと思います。ただし、選挙運動自体は重要インフラではありませんので、選挙運動自体の妨害、あるいは世論誘導のために大量の虚偽情報を組織的に流す、あるいはディープフェイクを作って流すということは、この重要インフラの指定の範囲の中には含まれないということになります。そのような制約をうけまして、全米でも最も多い人口を持っているカリフォルニア、それに次ぐテキサスの二つの州で、2020年の大統領選挙を前提にして、2020年の大統領選挙におけるディープフェイクを防止するためということで、ディープフェイクの規制法案が成立しております。

まず、カリフォルニアですけれども、投票日の60日前から、何人にも候補者に関するディープフェイクの発信を禁止するという法律ができました。ただし、これは2023年1月1日までのサンセットですので、そのあとどうなるかは現時点で未定でございます。規制対象は「実質的に虚偽の音声または視覚メディア(materially deceptive audio or visual media)」ということで、画像、音声または動画が虚偽であるものが規制対象ということになっております。フェイクの定義ですが、「候補者の外観、スピーチ、または行為に関する画像、音声または動画であって、当該の画像、音声または動画が誤って表示されるような方法で意図的に操作されたもの」、または「合理的な人物が、変更されていない元のバージョンを聞いたり、見たりした場合に、その人物が持っているものよりも、画像、音声または動画の表現内容について根本的に異なる理解または印象を持つようにしたもの」がフェイクであるという定義を置いております。

例外を除いて「いかなる人、協会、団体、企業、選挙運動委員会または選挙組織も、現実の悪意を持って、次の選挙運動用資料を製造、配布、公開または放送してはならない。」ということで、かなり細かく定義をしていまして、「公職の立候補者の画像または写真が重ねられているもの」とかですね、こういうものについて、要するにアイコラを作って配布、公開または放送してはならないというところも、規制対象に加えております。

他方で、そうしますと、こういうディープフェイクが出回っていますとか、こういうアイコラが出回っていますということを表現すること自体も禁じられてしまうことになるので、その場合は「この画像は事実を正確に表現するものではありません」という文言を表示しなければなりません。そうすると、これは作成、配布、公開または放送することができるという規定を置いております。

一方で、テキサス州のほうはディープフェイクという言葉をはっきり使って規制しているのが特色で、候補者を誹謗中傷したり選挙結果に影響を与えたりすることを目的としてディープフェイク・ビデオを作成してはならない、それから投票日の前30日間はフェイクと知りつつ流布させることもしてもならないということを決めておりまして、かつ、カリフォルニア州のほうと違うのは、刑事罰が科せられるということですね。これが文言でありますが、ディープフェイク・ビデオとは？という定義で、「欺くつもりで作成され、実際には発生しなかった行動を実行している実際の人物を描写しているかのように見えるビデオをさすものとする。」というような定義が置かれております。

アメリカにおける規制の現況 —IOGAN法と国防授権法

以上が州法レベルで、昨年2つの連邦法が制定されております。1つが、敵対的生成ネットワークの出力の識別に関する法律で、Identifying Outputs of Generative Adversarial Networks、頭文字を取って、IOGAN法と一般的に言っているようです。もう1つは国防授権法です。国防授権法というのは、アメリカでは国防に関する権限を連邦議会が大統領に授権するために、毎年予算だとかものすごい膨大な内容を組み込んだ法律を毎年制定するわけですが、昨年2021年度版の国防授権法で、国防授権法の中に「軍人とその家族を対象としたサイバー搾取とオンライン詐欺に関する研究」を国防長官は行わなければならないと、研究が義務付けられまして、その中にディープフェイクをやりなさいということも義務付けられたということです。

まずIOGAN法ですが、正式名称は非常に長いです。「全米科学財団理事長に、敵対的生成ネットワーク（ディープフェイクとも呼ばれる）、将来開発される可能性のあるその他の同等の技術、およびその他の目的で成される可能性のある出力に係る研究に対する支援を行うことを命ずる法律」ということで、全米科学財団（NSF）と米国国立標準技術研究所（NIST）に対し、敵対的生成ネットワークによって出力されたものを含む操作された、または合成されたメディアに関する研究を支援せよということを命じている法律です。具体的には、NSFはディープフェイクのコンテンツや情報の真正性に関する研究を支援しなさい、それから、NISTもディープフェイクの技術の機能や出力を調べるための技術ツールを開発するために、そのための研究を支援しなければならないと規定されています。また、NISTとNSFは、自分たちで研究するのではなくて、デジタルメディア企業を含む民間企業との研究機会の実現可能性に関して調査を行いなさい、民間企業に研究活動をさせるようにしなさいということで、それに対する報告書を連邦議会に共同で提出しなければいけないということが規定されています。ですから、このIOGAN法は、ディープフェイクを正面から規制するというよりは、ディープフェイクを識別し、ディープフェイクの対策を取るための技術開発をするということをNSFとNISTに命じている法律であると理解すれば分かりやすいのかもしれません。

一方で、国防授権法のほうは、589F条というところで、「軍人とその家族を対象としたサイバー搾取とオンライン詐欺に関する研究」という項目がございまして、「本法の制定日から150日以内に、国防長官は以下の調査を完了しなければいけない」。まずは「軍人とその家族を対象とした欺瞞的なオンライン・ターゲティングのリスク」すなわちマイクロターゲティングのリスクを調査しなければならない。その中には、「軍人とその家族を対象としたサイバー搾取を行う外国政府および非国家主体が現在もたらしている脅威についての次の情報評価」を行えということが書いてありまして、ここでディープフェイクを含むディスインフォメーション活動の調査を命じているということです。さらに、「外国の政府及び非国家主体が、隊員及びその家族を対象に、機械で操作されたメディア（一般に「ディープフェイク」と呼ばれる）を作成又は使用することによってもたらされる脅威についての情報評価」を行いなさいと、それに対する脆弱性を軽減するための提言を行いなさいということを指示していますので、国防長官に対してディープフェイクの脅威についての情報評価を行えという言い方をして、事実上ディープフェイクの特定、あるいはどの国から来ているのかとかですね、そういうことについての調査を命じるというような内容になっております。

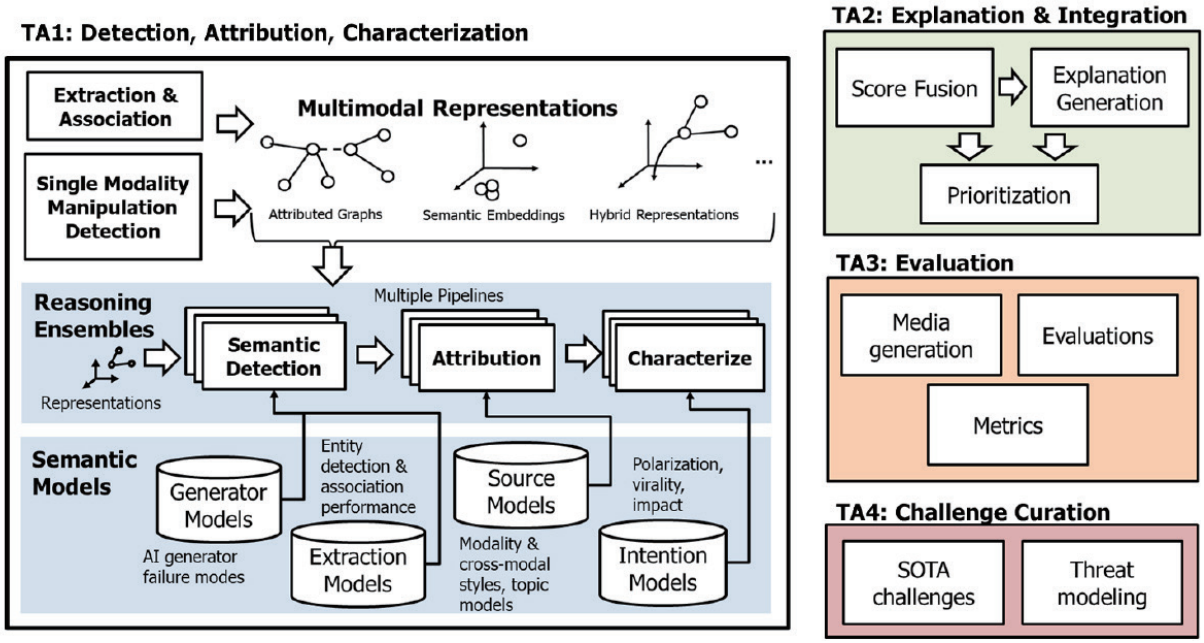
まあ結局その、こちらのほうは国防授権法ですから、基本的に軍人とその家族ということが念頭に置かれているわけですが、軍人とその家族に対するディープフェイクを含むディスインフォメーション活動それ自体が、information warfareのひとつなんだ、情報戦だというふうに評価をしているわけで、その文脈で、軍人とその家族に対するディープフェイクの情報評価を行いなさいという規定になっているわけですね。この調査結果は連邦議会の上下両院の軍事委員会に報告書として提出されることになっておりますが、機密情報を含んでよいということになっていますので、おそらく報告書は全部公開されるわけではないだろうと予想されます。

ディープフェイクを検知する技術

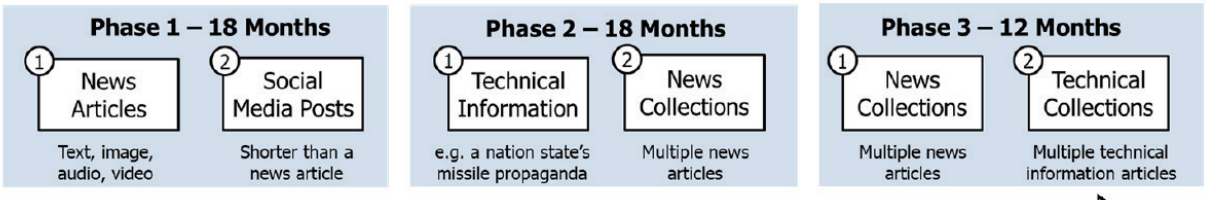
さて、そうしますと、ディープフェイクを検知することが重要になってくるわけですね。ただ単に、動画像に手が加えられているということを検知するだけでは十分とは言えなくて、要するに誰が、どのような意図のもとに、どういう手段でどういう人たちをターゲットにしてディープフェイクを作ってばら撒こうとしているのかを検知する必要が出てくるということになります。すでに、アメリカにおきましては、トランプ大統領のときに大統領令13848が出されておりまして、「アメリカ合衆国内の選挙への外国の干渉が発生した場合に一定の制裁を課す大統領令」ということで、連邦選挙終了後に選挙干渉がなかったかどうかを毎回調査しなければならない、もし海外からの干渉が明らかになかった場合には経済制裁措置を発動しますという内容になっているわけです。調査対象は一義的には連邦選挙、調査主体は国家情報長官で、45日以内に調査をやりなさいということを命じております。具体的には、選挙インフラに対する攻撃がなかったかということを主に調査しなさいということになっておりまして、これについては選挙が終わったあと、実際には45日以内を守れないことも出てきていますけれども、選挙が終わったあとには大統領令に基づく調査結果というのが公表されております。外国からの干渉とはこういう行為ですよという定義がありまして、「選挙に関し、外国政府又は外国政府の代理人若しくは代理として行動する者の隠ぺい的、詐欺的、欺瞞的若しくは不法な行為又は企て」というような規定を置いております。

それで、今具体的にディープフェイクを検出する技術として開発が進められているのがSemantic Forensicsという、通称Sema Forという技術です。Semantic Forensics自体は割と古くから提唱されている考え方ですが、今これをアメリカ政府はお金を付けて強力に研究開発を推進しようとしております。NSFとNISTは研究開発を民間事業者と共同でどうやって進めるかを報告せよと言われておりますが、実際にDARPAからSemantic Forensicsを具体的に進めるためにこういうプロジェクトを立ち上げますということの概要が公表されております。具体的には、ディープフェイクを含めたディスインフォメーション活動の検知、それからディスインフォメーション活動が誰によって行われているか、誰が支えているのかというようなAttributionを行う、そして、一体誰に対してどういう意図で行われているのかということを自動的に性格づける、この検知、Attribution、性格づけを、人手を使わずに自動的に行うツールを開発するというのが究極的な目的でありまして、先日、DARPAが民間事業者と連携して研究開発を行う際の研究開発の相手方として、Locked Martinが指名されています。

概念図を出しておりますが、これを少し省略して、DARPAのSemantic Forensicsで、まずdetectionのところでどうやって検知するのかということをDARPA自身の資料の中に書いてありますので、ちょっと引用してみると、今こういう映像が流れました、それから動画像と写真も出回りました、ニュースウェブサイトでこういうような文字が書いてありました、と。”April 1, 2019, Bob Smith On a rainy spring day, a vast, violent group gathered in front of the US Capitol to protest recent cuts in Social Security.”という、ボブ・スミスなるキャスターでしょうね、こういうことを言っている、と。その音声も流れているわけです。果たしてこれは真実なのか、フェイクなのか、あるいはディスインフォメーションなのか、ディープフェイクなのかということを自動的に検知する技術を作りたいということなんですね。で、まずprotestという言葉に注目して、テキストの中のprotest、そして実際の動画像や写真の中のイメージとを検証して、果たしてprotestを実際にしているのか。そうしますと、protestしている割には全然平和のうちに、子どももいたりしているわけなので、protestというテキストの部分は、これらのmodalitiesとは、“Conclusion: Media components consistent across modalities”で、protestしていることは間違いないけれども、じゃあviolent groupなのかということにしてみると、これらの動画像や静止画像や音声などから判断する限り、Media components not consistent across modalitiesということで、violent groupという表現はこれらとは合致しないということを具体的に突き止めるというわけですね。これはdetectionのところだけなので、具体的には、仮にこのviolent groupなる表現を使った情報を作ったのは誰なのか、そして一体誰がそれを広げようとしているのか、そこにお金を出しているのは一体いかなる団体なのか、場合によってはいかなる政府なのかということを、自動的に考察をする、それを一体何のためにやろうとしているのかという



https://www.fbo.gov/utils/view?id=614a021dc47a5466ce1747e3351113f4



Quantitative Assessment

Task	Metrics	Relevant Baselines	Program Goals P1	P2	P3
Manipulation detection	• Probability of Detection (Pd) • False Alarm Rate (FAR) • Equal Error Rate (EER)	• Human: 60% Pd [Deepfakes] • Image: 80% Pd at 10% FAR / 20% EER • Text entity recognition: 90% F1-score • Audio: 4% EER	80% Pd 10% FAR	85% Pd 8% FAR	90% Pd 5% FAR
Attribution	• Pd / FAR	• Image: 78% Pd at 10% FAR [camera id]	80% Pd 10% FAR	85% Pd 8% FAR	90% Pd 5% FAR
Prioritization for analyst	• Accuracy over degrees of malice	• Sentiment analysis: 70-80% F1-score	70% accuracy	80% accuracy	85% accuracy

https://www.fbo.gov/utils/view?id=614a021dc47a5466ce1747e3351113f4

ことを性格づけるところまで自動化するツールを、その分析を自動化するツールを、作ろうとしているのがDARPAのSemantic Forensicsの目的のようであります。

ディープフェイクに関する日本の法規制の現況

ディープフェイクに関しましては、このように広範に、アメリカでは規制の法制化が進んでおりますが、フェイクニュース・ディスインフォメーション全般ですね、日本の法規制の動きは正直言って鈍いです。まさに日本の公選法というのは、〇〇すべからずの「べからず選挙」と言われており、ものすごく規制をかけている割には、インターネット上のアクティビティには非常に緩いという矛盾があります。これもその一例ということができます。ただ、そもそも論として、非常に重い問いですが、ディープフェイクってそもそも規制すべきなのか、規制しても規制しなくてもいいのか、そもそもその種のものを規制すべきでないのかということを考えると、非常に、民主主義とは何かということを、根本的な問いにぶち当たってしまいます。たとえば、そういう虚偽、作られた情報というのは知る権利の対象にはそもそもならないのか、あるいは民意というのはそれぞれの有権者がまさに自律的かつ自由に形成すべきものであって、誘導されてはならないのか、誘導された民意というのは自由な民意ではないからそれは民意とは呼べないというものなのか。あるいは、表現の自由の保障との関係では、今後問題になってくるのはおそらく投げ銭モデルだと思いますし、現状では広告モデルなわけですが、これらは営利的な表現であって、純粋な政治的表現ではない。だから、ディープフェイクを含めたフェイク全般に、それが営利性をともっているのであれば表現の自由の保障は緩くても許されると考えるのかどうかですね。

まとめ

最後に、これはアメリカでも議論になっているところでありますが、アメリカの議論においては、海外発のものと、国内発のものは分けるべきだという考え方があります。つまり、freedom of speechというのは原則的には合衆国市民に対して保障されるものであって、外国政府や外国人に対して保障するものではないという理解のもとに、海外発のディープフェイクやディスインフォメーションは規制しても構わないのだという議論がアメリカにはあるわけです。じゃあ一体日本の場合はどうなのかと考えてみますと、日本の場合は外国人に選挙権を与えるべきかというところでは憲法の議論が非常に活発に行われてきまして、また最高裁判所が、地方選挙に限っては、定住している外国人に、地方の選挙権を与える・与えないというのは立法裁量の問題であるということをいって、かなり賛成側と反対側との間で一時論議になったことがありました。しかしながら、選挙運動を外国人がやっていいのかとかですね、そういうことについては、意外と実は議論が活発にはなされてこなかったと思います。うかつに議論すると政治的に利用されることを恐れたからかもしれませんが、ディープフェイクやディスインフォメーション全体を果たしてどう規制すべきかということを考えると、日

本の選挙法制、あるいは日本の選挙法制をめぐる議論全体の問題点にも実は行き当たるんだということを最後に指摘させていただきたいと思います。どうもご清聴ありがとうございました。

本稿は2021年7月11日(日) 〜 22日(木)に開催された第5回情報法制シンポジウムでの講演を元に作成したものです。

一般財団法人 情報法制研究所 参与
明治大学 教授

湯淺 墾道（ゆあさ　はるみち）

1970年生。青山学院大学法学部卒業。慶應義塾大学大学院法学研究科政治学専攻博士課程退学。2004年九州国際大学法学部専任講師。2005年同助教授。2008年同教授、九州国際大学副学長。2011年情報セキュリティ大学院大学情報セキュリティ研究科教授・九州国際大学客員教授。2012年情報セキュリティ大学院大学学長補佐。2020年情報セキュリティ大学院大学副学長。2021年明治大学公共政策大学院ガバナンス研究科教授。