［サイバー・ウォーズ］

⑥ 座談会：技術者とサイバー・ウォーズ

―アルゴリズムやフェイクニュースが“兵器”に―

栗原　聡（慶應義塾大学）　鳥海不二夫（東京大学）　平　和博（桜美林大学）　須川賢洋（新潟大学）
司会：長倉克枝（東京大学）　江間有沙（東京大学）

アルゴリズムやフェイクニュースが“兵器”として使われる事例が相次ぐ中，技術者は何に気をつけ，どうしていけばよいのか．さまざまな立場の専門家に語っていただいた．

“兵器”としてのフェイクニュース

長倉：中国やロシアの「ハイブリッド戦争」では，サイバー戦や情報戦が組み合わされ，アルゴリズムやフェイクニュースが“兵器”として使われることが指摘されています．平さんはご著書『悪のAI論　あなたはここまで支配されている』（朝日新書）などでも書かれていますが，最近の事例をご紹介いただけますか．

平：典型的なハイブリッド戦争は，2014年のロシアによるクリミア併合前後のウクライナ危機です．リアルの武力に加えて，サイバー攻撃とフェイクニュースの組合せの中でロシアが作戦を展開しました．

一方，フェイクニュースで皆さんが一番ご存知なのは2016年の米大統領選挙ですね．これはリアルの武力は入っていませんが，サイバー攻撃とフェイクニュースを組み合わせた，いわゆるハードパワーとソフトパワーの間のシャープパワーの典型例として挙げられています．たとえば，ロシア軍参謀本部情報総局（GRU）のハッカーの標的型フィッシング攻撃によって，ヒラリー・クリントン（Hillary Clinton）陣営の選挙対策本部長を務めたジョン・ポデスタ（John Podesta）氏のGmailのパスワードが奪われた事件があります．同氏の大量のメールが暴露サイト「ウィキリークス」で公表され，それを“証拠”として，「クリントン氏が児童虐待の地下組織に関与している」という「ピザゲート」と呼ばれる陰謀論が拡散する構図もありました．

このサイバー攻撃とフェイクニュースの組合せという構図は，2020年の米大統領選挙でもすでにその兆候が表れているという報道もあります．

長倉：サイバー攻撃やフェイクニュースの拡散をロ

左から，鳥海氏，栗原氏，平氏，須川氏

シアが行っているということですが，実際に手を動かしているのはどういった人たちですか？

平：米大統領選挙のフェイクニュースを作る部分は，インターネット･リサーチ･エージェンシー（IRA）という，サンクトペテルブルクの組織が主に担っているとされています．ここは民間企業ですが，実質的オーナは「プーチンの料理人」と言われる人物で，GRU の活動と連携していると見られています．

フェイクニュースの拡散は，Facebook や Twitter のようなプラットフォームが主な舞台となります．拡散には，ロシアとは直接の関係がない多様なプレーヤもかかわっています．米国内のトランプ（Trump）支持層や，米ロいずれとも関係のない，広告収入目当てで拡散したマケドニアの若者たち，さらには内容のインパクトから拡散に加担してしまった一般ユーザなどです．“兵器”としてフェイクニュースを仕込んでいる人たちの外縁で，その拡散を知らず知らずに担っている大勢の人たちがいるということになります．

そのベースとなっているのが，人々の関心・注目を集めることが経済的価値を持つという「アテンション・エコノミー」．そして，これに最適化しようとするアルゴリズムを担う IT 企業であり，それを実際に支えているのがソフトウェアエンジニアということですね．

鳥海：なぜフェイクニュースが“兵器”になるかというと，それを喜ぶ人たちがいるところをうまく突いているからです．フェイクニュースを作ったり流したりする技術はいくらでもできますが，それが拡散して人々の心に入っていくのは，技術にプラスして心理的な要素を活かさないといけない．そこには広報的に，人の心に刺さるものを作るという技術も必要ですね．そのフェイクニュースを流したことで喜ぶ人が一定数います．その人たちがフェイクニュースを“真実”に引き上げていくので，結果として無関係の人たちが信じてしまう．

ただ，平さんがおっしゃったサイバー攻撃とフェイクニュースは，分けて考えた方がいい．サイバー攻撃で（フェイクニュースの）ネタを持ってきて，フェイクニュースを作る．つまり，サイバー攻撃は製造側で，フェイクニュース拡散は流通側となります．こう分けて考えたときに，流通側については社会がそれを許容している状況があります．

平：2016 年の米大統領選では，拡散（流通側）についても，ロシアの IRA の関係者が 2014 年頃から米国内で現地調査をして，激戦州に焦点を絞った政治的マーケティング分析を行っています．民間企業がマーケティングをしてターゲティング広告を打つのと同じ手法で，“兵器”としてのフェイクニュースの拡散を行っていると言えます．

鳥海：（ネットで）フィルタバブルが現象として発生していて，そこでエコーチェンバーが起こることが分かっているので，こうしたマーケティングが有効になりました．

須川：従来，選挙や政治に対してこうしたマーケティングは行われてきませんでしたが，これが有効だということが分かってきたので使われるようになってきたということですね？

鳥海：そうですね．本来は候補者にとって有利な情報を流すという正当なやり方だったのが，対抗馬に対して不利な情報を流したりフェイクニュースを流したりする戦略も含めてマーケティングの手法が使われるようになりました．

須川：ディジタル・ゲリマンダの中にフェイクニュースも含まれるという捉え方は，ここ数年で政策科学の研究者の間でも共通認識になっています．そのディジタル・ゲリマンダはハイブリッド戦の 1 つのサブセットになっていますが，そこまではまだ多くの人に認識されていません．選挙や政治の側面でのみ捉えてしまう場合がほとんどで，フェイクニュースが“兵器”だとまで捉えられる人はまだまだ少ないのが現状です．

人間そのものが“兵器”

江間：アルゴリズムが“兵器”になる，というのが今回の対談のテーマですが，何が“兵器”なのかという概念を考え直していく時期にあるという気がしています．

栗原：今のインターネットにしても，SNSのような情報を伝搬させる仕組みにしても，まだまだ技術は未熟な状況です．そして，アルゴリズムが“兵器”という捉え方は否定しませんが，そもそも人間自体が“兵器”なのだと思います．公平な判断などできるわけがなく，自分の好みというフィルタと，自分でも気がつかない自分が持つバイアスを加味して，条件反射的に拡散する場合もあれば，意図的にフェイク情報を流したりもする．

たとえばミサイルのような複雑なシステムは，設計から製造まで入念な計画に従って作業が行われるわけですが，フェイクニュースの拡散による間違った世論形成やデマの拡散による社会混乱発生といった「攻撃」は不特定多数の人々の行為の創発現象により具現化します．フェイクニュースをミサイルに見立てた場合，いつどこで誰がミサイルを発射するのかをあらかじめ特定することはできず，防ぎようがありません．つまり，意図的に創発を制御できる人がいるとすれば，それは確実に成功することになります．

しかし，創発の怖さは作り出す側も完璧に制御できないところにあります．特に意図せず起こる創発が大きな混乱を招きます．そうした創発をどのように解明するのか，どう介入して制御していけるのか，そういった課題の解決こそ僕らがやる仕事であると考えています．僕ら人間はそう簡単に自分たちの行動を変えることはできませんが，テクノロジーが引き起こす現象であれば変えることができるはずです．我々研究に携わる者として一矢報いたい気持ちがあります．

須川：戦国時代でも日露戦争でも情報を“武器”にするということは行われてきましたが，今はネットワークの時代になり，拡散のスピードが速くなりました．もちろんそれは技術のおかげですが，一方でそれを制御するための技術もまた必要になります．

エンジニアと社会の位置関係

長倉：ケンブリッジ・アナリティカ（CA）の元エンジニアで内部告発を行ったクリストファー・ワイリー（Christopher Wylie）は著書で自身のCAでの仕事を振り返り「アルゴリズムは武器だ」と書いています．ただ彼は初めからそう知った上で仕事をしていたわけではありません．エンジニアとして気をつけることはできるのでしょうか？

須川：セキュリティはよく『スター・ウォーズ』のフォースに例えられます．ホワイトサイドorダークサイドという意味ですが，そうなれば当然にダークサイドに墜ちないようにしてほしいです．

鳥海：エンジニアに「あなたのフォースを正しく使いましょう」と言うわけですか．ジェダイはそんなに多くないので監視できていますが，エンジニアは世界に何百万人，何千万人といるので，その人たちに「あなたの作っているものは武器になり得る」と言っても……．よく考えると，ジェダイもちょいちょいダークサイドに落ちてますし．

平：ただ，エンジニアと社会の位置関係はイメー

ジしておいたほうがいいでしょう．国際政治から国内政治，軍事ビジネスに至る色々な場面で，今の社会はソフトウェアでできています．特にフェイクニュース絡みのアテンション・エコノミーで言うと，そこに最適化させたコードやソフトウェアは場合によっては民主主義に具体的なネガティブ・インパクトを与えています．その全体像の中で，エンジニアは，「私がやっていることは何か」というイメージを持つ必要があるのかもしれません．その“兵器”と自分が書いたコードがまったく遮断されたものではなくて，どこかでつながっている可能性があることは，意識しておいた方がいいのではないでしょうか．

まったくイメージしないところでつながってしまうというのは，まさにケンブリッジ･アナリティカの事例，さらにスノーデン事件で明らかになった，米国家安全保障局（NSA）による世界規模のネット監視もそうです．FacebookやGoogleといった民間企業が持っているデータを，テロ監視のような，民間企業の本来の目的や用途とはまったく違う形で使っていた．民間企業のデータが，知らぬ間に安全保障に流用されるという，思わぬ「底抜け」が起きている状況も，目の前の現実として理解しておくことが必要だと思います．

須川：データの収集と利活用は法律に触れる違法なやり方は論外で，ケンブリッジ・アナリティカによるFacebookのデータ利用も明らかな規約違反です．むしろ問題なのはグレーゾーンの場合で，そこに手を付けるかどうかは，エンジニアの倫理観が出てくるところではないでしょうか？．

鳥海：エンジニアとしてはグレーゾーンには手を付けると思うんですね，普通に．ただ，問題はエンジニアの行動原理がどこにあるかで，基本的に企業ならもっと上位で意思決定をしています．そこで意思決定されてエンジニアに指示された場合，それが黒ではなくてグレーで上が責任を持つのなら，エンジニアにはどうしようもないですよね．黒なら「倫理観」で止めることもできるでしょうけれど．そんな状態で「倫理観」と言われても，誰の倫理観かが問題です．それはエンジニアよりも意思決定者の問題になるのではないでしょうか．

栗原：映画『ダイ・ハード4.0』で悪役側がサイバーハッキング用のシステムを作るため，広くプログラマをバイトとして募集するのですが，開発を依頼されるプログラムはハッキングシステムを構成する個々のサブシスシムなので，それ自体では全体のシステム像が分からないような設定となっていましたね．バイトを引き受けたプログラマは，自分たちがまさか悪事の片棒を担いでいるなど思うわけもなかったのです．

最近ではディジタルツインなどと呼ばれますが，実世界を同じものをサイバー空間でも構築する動きもあります．サイバー空間では良いことも悪いことも物理空間と比べてより急速に強調されてしまいます．こうした状況で，何がホワイトでどこからがダークなのかの線引きが曖昧というのはきわめて厄介です．

鳥海：完全なホワイトからダークに落ちる可能性すらいくらでもあります．そこでエンジニアに「気をつけなさい」と言っても，ホワイトなことまでできなくなるだけな気がします．

平：“兵器化”するアルゴリズムの問題は，アルゴリズムとして優れているものが，社会の文脈に落とし込んだときに，相容れない結果を生み出してしまう可能性がある，という点です．たとえば，プ

ロダクトやサービスを作るプロセスのどこかで，エンジニア的ではない価値観を挟むことが必要ではないかな，と考えています．法律やガイドラインによって禁止されていなくても，社会の常識というか，世間知，世間相場のような価値観を入れるべきではないかと．メディアの感覚で言うと「編集」のようなプロセスです．そのプロダクトやサービスが，作り手の本来の意図を超えて，どんなインパクト及ぼす可能性があるのか，といった世間相場の“ものさし”を当ててみるということです．

ユーザ側も倫理観を

長倉：栗原さんは『AI 兵器と未来社会　キラーロボットの正体』（朝日新書）を昨年（2019 年）9 月に出されるなど，メディアでも安全保障と AI について積極的に発言されています．AI 研究者としては珍しいですが，なぜ安全保障と AI にかかわられるのでしょうか？

栗原：僕ら人類は，今のところ，地球における生存競争を生き抜いてきた頂点に君臨してますよね．そして，それをなし得た大きな要因が我々の持つ社会性です．しかし，人間が集団で社会生活を営む場合，実は 300 人くらいの集団が限界だとされていますが，今やそれを大幅に超える複雑な社会に人間は飲み込まれてしまっているのだと思います．もはや自分たちで制御できない状況です．ただ，これを招いたのはテクノロジーなのですから，逆にテクノロジーで解決しなければならない．

一方，進化の大原則は適者生存であり，そもそも生物は適応したものが生き残り，そうじゃないものは淘汰されます．その意味では我々ホモサピエンスなんて最悪ですからね（笑）．ホモサピエンスは同類であるネアンデルタール人を絶滅させ，これまでどれだけの種を絶滅させてきたのか．ホモサピエンスが誕生して数万年ですが，生物学的に，たとえば我々の闘争本能など何も変わっていないのです．それは，昨今の世界情勢を見るに自明かと思います．我々は何の解決もしてないし，進歩もしていない．

長倉：人間には闘争本能があり，そもそも争いは起こるものということですね．

須川：「衝突が起こり得る」という前提のもとで安全保障という概念があるわけですからね．

平：エンジニア，企業といったサービスの作り手だけでなく，受け手，ユーザのリテラシーを底上げしていく必要もあります．たとえば，ハイブリッド戦争の話で言えば，ネットのユーザ一人ひとりがすでに戦争に加担しているという現実がある．それを意識していくことも重要だと思っています．

鳥海：まさにユーザ側の倫理が重要になります．エンジニアが倫理観を持つのは，エンジニアが結果を予見できる状況です．でも，今の社会全体が複雑系になっている状態では，大体の場合予想外のことによって大きなダメージが生じます．そこでは倫理観はなんの役にも立ちません．

そこでは平さんがおっしゃる通り，エンジニアが作ったときには想定しなかった新たに生じた状況に対して，ユーザが何らかの倫理観を持って行動することによって良い方向に収束する可能性はあると思います．

意図的に作った結果なのか，意図せずにできてきた結果なのかによって話が変わってきますが，今は少なくともエンジニアとしては意図しなかったものが他者の手によって新たな方向に持ってい

かれることが非常に多いので，一人ひとりがそういうことが起き得るというふうに考えるしかないんじゃないかと思います．

正しく声を上げる

江間：では『情報処理』読者，特に若い人たちはどうしていけばいいでしょうか．

栗原：正しく声を上げるしかないんじゃないでしょうか．包丁職人は包丁を料理に使ってほしくて作っているし，人を刺すために使ってほしくない．僕らも同じで，悪いことには使ってほしくないですよね．それを言うしかないじゃないですか．

平：今の社会の骨格や基盤はソフトウェアからできていて，エンジニアは社会を支えるさまざまなパーツを作っている．その使命感と倫理観は，明確に持っていてほしいなと思います．

エンジニア一人ひとりの倫理観を表明することは可能だし，それによって倫理観に反する使われ方に歯止めをかける事例もあります．たとえばGoogleが米国防総省のAIプロジェクト「Project Maven」への参加を進めていた中で，現場のエンジニアを含む多くの社員が，それに対して「ノー」と言う声を上げた．結果としてGoogleはその計画をストップさせました．

フェイクニュースについては，アルゴリズムをアテンション・エコノミーに過剰に最適化させてきてしまったことが，今の問題の肝とも言えます．

現在は，このアテンション・エコノミーがすべて，と思ってしまいがちですが，特に若い人たちが，“そうではない枠組み”を発想することで，また違う世界を開いていってほしいと思っています．

鳥海：10年前の社会と今の社会では倫理観が違うんですよね．今，若い人たちに我々が倫理観を押し付けても，10年後，20年後には変わるものです．

須川：僕らは，権力に対して逆らうとか，軍事的な匂いのするものに対して抵抗することが正しい倫理観だとインプットされてきた世代なんですよね．でもこれからはこの考え方だけでは通じなくなるのは明白で，だからこそ技術や政治経済，安全保障までを俯瞰して考えることができるような技量が必要になるのではないでしょうか？

日時：2020年2月27日
場所：東京大学

栗原　聡（正会員） satoshi@keio.jp
慶應義塾大学理工学部教授／電気通信大学人工知能最先端研究センター特任教授．慶應義塾大学大学院卒業，NTT研究所，大阪大学，電気通信大学を経て現職．博士（工学）．群知能・汎用AI研究などに従事．近著は『AI兵器と未来社会 キラーロボットの正体（朝日新書）』．人工知能学会倫理委員会アドバイザー．

鳥海不二夫（正会員） tori@sys.t.u-tokyo.ac.jp
東京大学大学院工学系研究科准教授．計算社会科学，人工知能技術の社会応用などの研究に従事．情報法制研究所理事．人工知能学会，電子情報通信学会，日本社会情報学会，AAAI各会員．

平　和博 taira_k@obirin.ac.jp
ジャーナリスト，桜美林大学教授（リベラルアーツ学群メディア（ジャーナリズム）専攻）．早稲田大学卒業後，朝日新聞社入社．社会部，シリコンバレー駐在，科学グループデスク，編集委員，IT専門記者などを担当．2019年から現職．

須川賢洋（正会員） masahiro@jura.niigata-u.ac.jp
新潟大学法学部助教．修士（法学）．専門：サイバー法．コンピュータ犯罪，ディジタル知的財産，情報セキュリティ制度など先端技術と法律の関係を中心に研究．本会「電子化知的財産と社会基盤（EIP）研究会」幹事．

長倉克枝 katsue.nagakura@gmail.com
東京大学未来ビジョン研究センター客員研究員．

江間有沙 ema@ifi.u-tokyo.ac.jp
東京大学未来ビジョン研究センター特任講師．科学技術社会論．国立研究開発法人理化学研究所革新知能統合研究センター 客員研究員．人工知能学会倫理委員会副委員長．