国立情報学研究所ニュース　ISSN 1883-1966（Print）　ISSN 1884-0817（Online）

# NII Today

81
Sep. 2018
National Institute of Informatics News

NII Interview

## 機械学習の「不確かさ」にどう挑むか

石川冬樹［アーキテクチャ科学研究系 准教授／機械学習工学研究会 主査］

## 一本の論文で世界は変わる
## 国内外と連携し、課題に挑む

杉山 将氏［理化学研究所 革新知能統合研究センター長］

## 機械学習の本質を見極め、攻撃や不具合に備える

中島 震［情報社会相関研究系 教授］

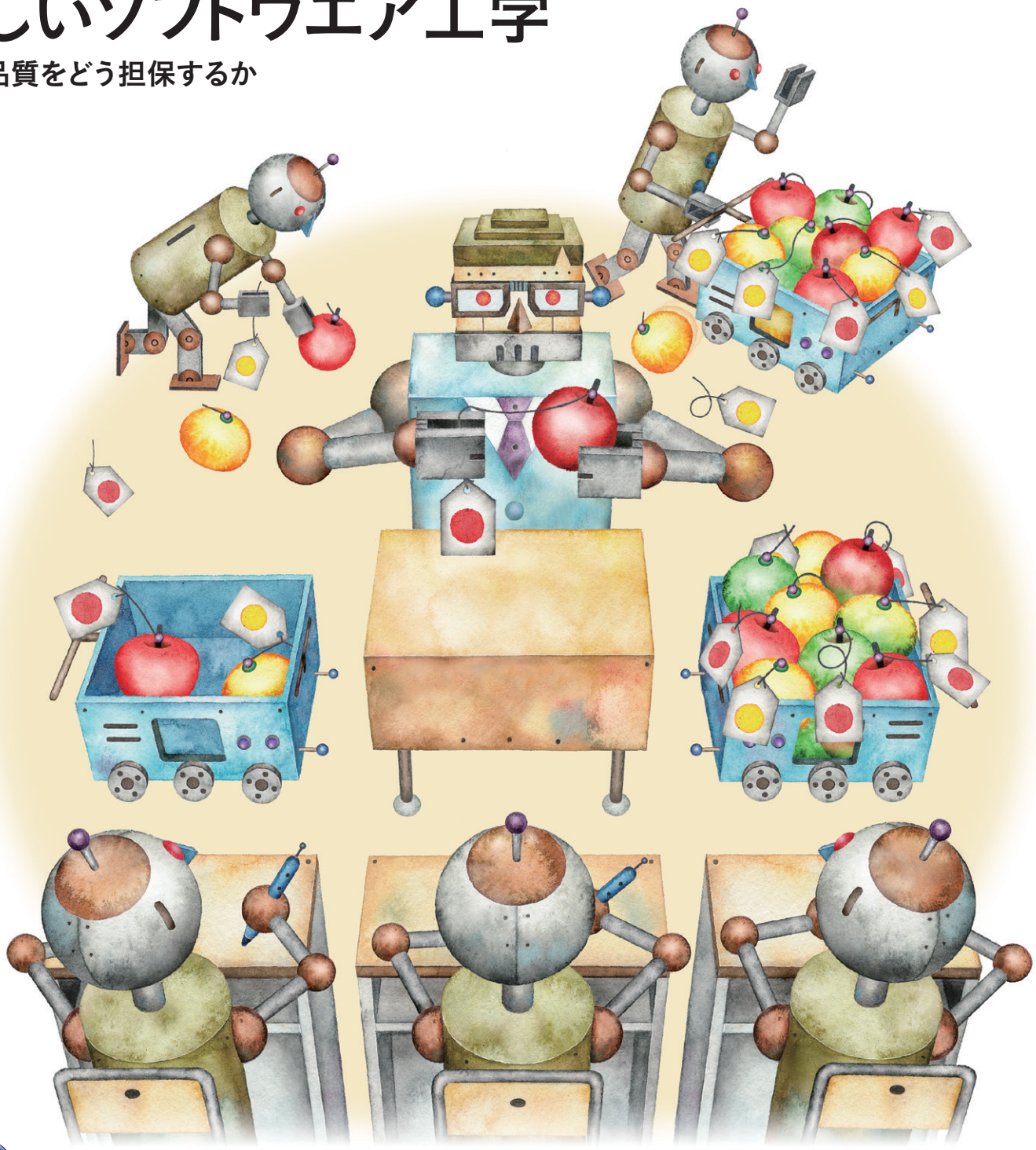
対談 **法的視点から機械学習の品質を考察する**

小塚荘一郎氏［学習院大学法学部 教授］
佐藤一郎［国立情報学研究所 副所長］

Feature

# 機械学習のための新しいソフトウエア工学

## AIの品質をどう担保するか



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

# 機械学習の「不確かさ」にどう挑むか

## 人工知能を活用した製品、サービスの社会における活用に向けて

石川冬樹　国立情報学研究所 アーキテクチャ科学研究系 准教授
電気通信大学 大学院情報理工学研究科 客員准教授
総合研究大学院大学 複合科学研究科 客員准教授

聞き手：村山恵一氏　日本経済新聞コメンテーター

**人工知能（AI）を活用した製品、サービスに対する関心が高まっている。機械学習（マシンラーニング）の技術が進化し、データが生み出す新たな価値への期待は大きい。ただ、機械学習が持つ「不確かさ」という特性ゆえに、企業においてシステム開発の最前線に立つエンジニアはかつてない課題に直面しているという。解決に向けた議論の場として、日本ソフトウェア科学会の研究会「機械学習工学研究会（MLSE）」が発足した。中心的な役割を担う国立情報学研究所の石川冬樹准教授にその背景を聞いた。**

**村山**　社会全体でAIの注目度が増し、産業界では新事業創出などへの期待が高まっています。

**石川**　機械学習ですごいことができる、いままでビジネスになっていなかったことが可能になるというのは指摘されている通りです。技術のライブラリーやフレームワークなどさまざまなツールが出てきました。選択肢が増え、それぞれの機能も豊富になっています。そうした技術を使うことで、機械学習を応用したシステムをつくることが容易になっています。それが今回のAIブームの背景でもあります。しかし、技術者の立場では、夢や魔法だとは考えていません。ふだん接する企業のエンジニアのなかには悩んでいる人が少なくないのです。

石川冬樹
Fuyuki Ishikawa

**村山**　それは一体どんな悩みなのですか。

**石川**　確かに何らかのシステムをつくることは簡単になりました。ただ、それを製品として世に送り出す、製造物責任をとるとなると話は別です。いままではソフトウエア開発にも慣習のようなものがあり、「ここまでやっておけば社会に受け入れられる」「自分たちはしっかりやったと胸を張れる」という基準がありましたが、そこがいま手探り状態になっています。

従来のソフトウエア開発は演繹的でした。システムの目的に応じて人がルールを書き出し、それをプログラム化するわけです。一方、訓練データからつくる機械学習のシステムは帰納型のソフトウエア構築といえます。人が決めたルールで動くわけではなく、データをたくさん与えてルールをつくらせるという間接的な手法です。直接の制御はできない、いわばブラックボックス。人の感覚が裏切られるかもしれません。エンジニアにとっては、自分がつくったものにもかかわらず、何ができ何ができないのか断言できない、やってみないとわからないという状況です。

税金の計算でもいいし、社員情報の登録でもいいのですが、これまでのシステム開発であれば、どのくらいの価値があるものなのかについて発注者である顧客と話し合い、それならばいくらで、という契約を結べます。ところが機械学習の場合、つ

くってみないと何％の精度が出せるのか判断できない。発注者と議論してつくるものを決める意思決定において、従来からある手法が通用しません。

そうした状況を何とかしたいと考えて立ち上げた研究会がMLSEです。ファシリテーターとして、勉強会を開くなど「場」を設けていきます。企業に勤めるエンジニアや研究者が参加者の中心になると想定しています。海外の研究を紹介したり、雑誌で特集記事を組んだりといったことにも取り組むつもりです。

**村山**　一方ですでにいろいろなシステムが機械学習を用いて開発されています。エンジニアはもやもやした気分で開発に取り組んでいるのですか。

**石川**　多いのは、まずはPoC（Proof of Concept：概念実証）でお試し版をつくり、うまくいったら本番のプロジェクトに移るというケースですが、これにも問題があります。それは「PoC貧乏」に陥る例があちこちで散見されることです。帰納型ソフトウエアの特徴として、100％の正解を保証できないという点が挙げられます。発注者が後から「精度が足りない」「能力が不十分」などと指摘できてしまうわけです。エンジニア側、受注企業側の悩みのタネになっています。

PoCでは実験に利用するデータもお試しで、できることに限りがあります。お試しデータではうまく動いたシステムも、本番データでうまくいくとは限りません。そこからエンジニアの苦労が始まることもあります。ですから発注者ときちんと議論するための道具づくりや、情報整理術の確立などが重要になります。

**村山**　「100％の精度は出せない」という機械学習の特質をわかったうえで使っていくという社会的なコンセンサスが必要になります。

**石川**　そうです。もちろんエンジニアは開発にベストを尽くし、技術的な穴をつぶすよう努力しています。それとは別に、システムの利用者や開発の資金を出す人が、機械学習とはそういうものであると理解する。それが大切です。それでも、たいへん役に立つ使い方がたくさんあります。リスクゼロのものはないという現実を突きつけられています。落ち着いて議論し、皆さんがそれを受け入れる必要があると思います。

例えば、自動運転車の実現に向けてカーメーカーが努力を尽くすのはすばらしいことですが、それには機械学習というものについての合意形成が欠かせません。それがないまま事故が起きると、過剰な拒否反応、規制につながりかねません。エンジニアが安心して開発に取り組めるように環境を整えることが重要です。

**村山**　リスクを踏まえたうえで、機械学習の恩恵を最大限に引き出す方向に世の中は進むべきですね。

**石川**　機械学習の一番すごいところは、「言葉にできない不確かなものもシステムにできる」という点です。いままでは要求を言葉にし、つくるものをルール化しなければならなかった。しかし、人が本当に実現したいことは、えてして漠然としているものです。そんなモヤッとしたものでも機械学習なら動くシステムにできるのです。

ですからエンジニアも、新たな課題に苦しみつつも、仕事を楽しんでいます。新しいものをつくる、試行錯誤して何かを生み出すというのは心躍るものです。技術開発の力や合意形成の力でなんとか課題を乗り越えたい。MLSEという研究会を通じ、問題意識を持ちながら楽しく盛り上げていければと思います。

**村山**　AI分野の研究開発を巡っては、有力なIT企業が多い米国が先行し、それを中国が国を挙げて追い上げています。米中二強の構図で日本が埋没すれば、国の競争力、安全保障の面から問題ではないですか。

**石川**　研究者としてやるべきことは、機械学習が入ったシステム全体をしっかりつくることです。帰納と演繹を融合し、すごく大事なところはルールベースで安全性を担保する。いいとこ取りで全体の完成度を高めるのが究極の目標です。機械学習が実用の段階になりましたが、いままでのつくり方との組み合わせを追求するのが次のステップになります。

モノや機械学習、従来型のシステム、ソフトウエアがかみ合っていいものができる。それが本来めざすところです。例えばパソコン用のOS（基本ソフト）は米国のものばかりですが、モノの部分は日本のものづくりに強みがあります。世界で戦える人がたくさんいます。そういう領域にAIが入り、さらに強くなるのが望ましい。製造業のなかには機械学習を試している企業がたくさんあります。総合力で日本の強みが発揮されればいいと思います。

（写真＝佐藤祐介）

**インタビュアーからのひとこと**

膨大なデータからマシン自身が学ぶ機械学習は、これまでなら困難だった領域にシステム化の可能性を広げたという意味で画期的だ。社会がAIに熱い視線を注ぐのも無理からぬ面がある。ただ、できあがるシステムは決して万能ではなく、間違うリスクが潜む。システムのつくり手と使い手が納得し信頼し合う関係を築く知恵がいま問われている。


**村山恵一** Keiichi Murayama

1992年東北大学法学部卒、日本経済新聞社入社。産業部でIT・電機、自動車、医療などを取材。ハーバード大学留学、シリコンバレー支局を経て2012年編集委員。15年論説委員兼務。17年から現職。担当はIT、スタートアップ。近著に『START UP 起業家のリアル』。


Interview

# 一本の論文で世界は変わる
# 国内外と連携し、課題に挑む

## 方法論を担う研究者として品質への責任を果たす

**杉山 将氏** 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（AIP センター）長
東京大学大学院 新領域創成科学研究科複雑理工学専攻 教授

聞き手：**谷島宣之** 日経 BP 社 日経 BP 総合研究所 上席研究員

**「一部の研究者が手がけてきた機械学習が注目を浴び、さまざまな領域での応用が期待されている。基礎を担ってきた我々研究者としてはたいへん嬉しい。安全性など課題が見え、プレッシャーも感じるが、ここでなら世界を変える研究がやり遂げられる」。機械学習研究の第一人者、杉山将東京大学大学院教授はこう語る。杉山氏がセンター長を務める理化学研究所 革新知能統合研究センターでは総勢 600 人ほどの研究者が国内外の組織と連携し、機械学習以外の方法論も含めて、応用や課題を意識した活動に取り組む。杉山氏に現状と課題、研究者の役割を尋ねた。**

### 世の中が一変した

「世の中、変わったよね」。機械学習の研究者が集まるコミュニティで時々こんな話になります。私は 20 年ほど機械学習の研究をしてきましたが、かつては時流に乗っていない分野でしたから、好きなことを好きなように研究できました。しかしディープモデルを使った機械学習、いわゆるディープラーニングが一大ブームになり、社会のあちこちで応用され、それが大きく報道され、多くの方から我々研究者に声をかけてもらえるようになりました。研究者が考案したアルゴリズムが社会で実際に使われる。責任重大です。「楽しかった昔に戻れないね」と言い合ったりしています。

世界の超大手企業が巨額の研究費を投入して研究する分野になりましたが、まだまだ解決できない問題は多い。機械学習やディープラーニングの拡張が必要ですし、まったく新しいやり方もありえるわけで、研究者のやりがいは変わりません。

私が取り組んでいるのは、集めたデータをコンピュータによって統計処理し、問題を解くアルゴリズムです。複数の問題に使える汎用性があるアルゴリズムや、不完全なデータからでも学習できるアルゴリズムなどを考案してきました。一方、アルゴリズムを裏付ける数学理論に取り組む研究者もいます。基礎となる方法論を両者で研究しているわけです。

方法論は研究者の発想しだいで優れたものをつくれますか

杉山 将

**Masashi Sugiyama**

2001 年に東京工業大学 情報理工学研究科にて博士（工学）の学位を取得。同年、同大学助手。2003 年同大学准教授。2014 年東京大学教授。2016 年より理化学研究所 革新知能統合研究センター（AIP センター）長を併任。機械学習とデータマイニングの理論研究とアルゴリズムの開発、および、その信号処理、画像処理、ロボット制御などへの応用研究に従事。

ら、「一本の論文で世界が変わる」研究成果を日本から出せると考えています。ディープラーニングも2006年に出た一本の論文がきっかけで、あれだけのブームになったわけですから。

## 誰もやらない問題に取り組む

私は革新知能統合研究センター（AIPセンター）のセンター長として、研究者を探したり、海外の大学と協力関係を結んだり、企業と提携して共同研究をする関係を築いたり、といった仕事をしています。

AIPセンターには今、フルタイムで120人、パートタイムで500人の研究者がいます。機械学習だけを研究しているわけではありませんし、方法論の研究に留まらず、応用に近い研究にも取り組んでもらっています。

AIPセンターでは10年間、じっくり研究ができます。これは世界でも例を見ない研究環境です。基礎に近い研究者の皆さんには「訳がわからないと言われてもかまわないから、解決できない問題を自分で見つけて挑戦し、10年後に一発当ててください」とお願いしています。画像処理や自動翻訳など、楽しそうな基礎研究の領域はあるのですが、世界の超大手企業が血眼で取り組んでいますから、そこはあえて避けています。

訳がわからなくてもよいというのは、「なぜそんな問題に取り組むのか」と周囲から言われるような問題を見つけることが大事だからです。どう解くのかまったくわからない問題と格闘するうちに、新しい方法論にたどりつくことを期待しています。

応用に近い研究者は他の科学分野、例えば医療や材料科学などを支援する研究と、防災や社会インフラ整備、高齢者のヘルスケアといった社会問題をにらんだ研究に、それぞれ取り組んでいます。応用といってもAIPセンターにいるのは情報系の研究者ですから、医療や材料の研究者の方や企業、社会問題に取り組んでいるパートナーの方と連携して研究を進めています。

## 課題はロバストネス

一人の研究者として研究に取り組み、AIPセンター長として数々の研究を見てくると課題がはっきりしてきます。研究者の間で今、最もホットなテーマは「ロバストネス」です。変化に強い方法論をどう用意するか。安全性あるいは品質への配慮ということです。

我々が研究する場合、ある問題をいったん抽象化してモデルにし、それを解くアルゴリズムを考えます。つまり綺麗な前提で綺麗な解き方を用意する。ところが応用の世界に入ると前提がすぐ変わる。そうなると前提が揺らぐことが前提となっているような、すべてを綺麗に決めておかない緩いモデルでも答えを出せるアルゴリズムが必要になってきます。

公平性や透明性という課題もあります。過去のデータに基づいてコンピュータに何かを判断させる場合、過去の人間の判断があまり公平でなかったとしたら、今後も公平でない判断をコンピュータが下しかねない。公平性については、日本ではあまり言及されていませんが、欧米は重要視しています。透明性とは、なぜそう判断をしたのか、はっきり示せるようにすることです。

いろいろな課題がありますが、方法論を担う研究者からすると、汎用性のあるコアの部分を押さえればよいはずだと考えます。実際、コアを押さえるやり方で、アルゴリズムの実装に苦労する、良いデータを集められない、といった課題に取り組んできました。安全性より前の実装段階でこうした課題があったのです。

実装について、私は「確率密度推定」という考え方を使って、ある程度まで汎用性があるアルゴリズムを複数集めたフレームワークを用意し、それを企業に使ってもらいました。特定の問題に特定のアルゴリズムを実装するやり方ですと、エンジニアの方がそのつどアルゴリズムを勉強しなければならず、時間とコストがかかっていました。

データ収集については、不完全なデータやスモールデータから判断できるアルゴリズムを研究しています。ビッグデータ時代と言われますが、それはインターネットサービスの分野くらいで、製造業や医療、社会インフラといった他分野では皆さんデータ収集に苦労されています。

ロバストネスを考えていくと方法論の研究だけでは足りません。AIPセンターに弁護士など法律の専門家に来ていただき、社会に応用した際の倫理あるいは法的な課題を研究しています。応用に近い側の研究者との協力関係をもっと密にする必要もあります。

先日、「機械学習工学研究会」（2～3頁参照）の会合に呼んでいただき、集まった方の熱意に衝撃を受けました。方法論は大事ですが、しょせんはアルゴリズムですから、実装するにはソフトウエアエンジニアの方が不可欠です。実装するといろいろな課題が見つかり、我々はアルゴリズムや理論を見直すわけです。

AIPセンターにはソフトウエア工学の研究者は少ないので、ソフトウエア工学側から我々を呼んでもらえるのはたいへんありがたいことです。我々からもソフトウエア工学側へ貢献していきたいと思っています。

（写真＝佐藤祐介）

### インタビュアーからのひとこと

研究者と組織の長を兼ねる。激務である。だが、杉山氏は研究を続けながら、その成果をまとめた書籍を英文で準備し、良い人材を求めて国内外を飛び回る。考案した方法論を企業に提案するなど、研究者の頃からコラボレーションに積極的だった。その姿勢があるから組織の長をこなせているのだろう。研究者あるいはセンター長として、ぜひ一発当ててほしい。

**谷島宣之** Nobuyuki Yajima

1960年生まれ。大学で数学を学び、コンピュータのエンジニアをめざしたが、1985年日経マグロウヒル社（現･日経BP社）に入社、『日経コンピュータ』誌の記者になる。2009年から『日経コンピュータ』編集長。2016年から現職。

Interview

# 機械学習の本質を見極め、攻撃や不具合に備える

## 「プロダクト品質」、「サービス品質」、「プラットフォーム品質」でのアプローチ

**中島 震** 国立情報学研究所 情報社会相関研究系 教授
総合研究大学院大学 複合科学研究科 教授

聞き手：**若江雅子氏** 読売新聞社 編集委員

**ここ数年、AI（人工知能）を欺く攻撃手法が次々と報告されている。パンダの画像にノイズを加えて見せたら、テナガザルと誤認識したり、道路標識の落書きで「一時停止」を「速度制限」と間違えたりと、AI は意外に騙されやすいようだ。今後、AI が私たちの生活に浸透すれば、その信頼性は命にもかかわる問題になる。だが、実は AI がなぜ間違えるのかはよくわからないという。どうしたらいいのだろう。AI の手法の一つである機械学習の品質問題を研究する中島震教授に聞いた。**

**若江**　最近、機械学習への攻撃手法の研究が次々と報告されていますね。

**中島**　2014 年にトロント大学の研究グループが「アドバーサリアル・エグザンプル」（Adversarial Examples、敵対標本）と呼ばれる攻撃手法を発表して以降、さまざまな研究が報告されるようになりました。これは、学習済みの画像認識モデルにデータを与えて推論を行わせる時に、特殊なノイズを加えることで、誤認識させる手法です。有名なのが、このトロント大学のグループが 2015 年に発表した事例で、パンダの画像にノイズを加えると、人間にはパンダにしか見えないのに、推論プログラムはテナガザルと判断してしまいます。2017 年にワシントン大学の研究者らが発表した交通標識のケースもよく知られています。「一時停止」の交通標識に黒い落書きをすると、「速度制限」の標識だと勘違いしてしまうのです。

中島 震
Shin Nakajima

**若江**　命にかかわる問題ですね。なぜそのようなことが起きるのでしょうか。

**中島**　この二つの研究は、機械学習の一つである深層ニューラルネットワークの学習アルゴリズムに問題があり、ある種のデータを与えた場合に誤認識が発生するものですが、実際には、誤認識の原因をうまく説明できないことが多いのです。

**若江**　なぜ分からないのですか。

**中島**　ものすごく簡単に言ってしまうと、機械学習の推論、つまり判断は、使っているアルゴリズムとデータに依存します。つまり、学習アルゴリズムが正しくても、おかしなデータで学習すれば、おかしな判断をするかもしれませんし、データが正しくても、アルゴリズムが間違っていておかしな判断をすることもあります。逆に、アルゴリズムが間違っていても、正しいと思われる結果が出ることさえあります。つまり、出てきた推論の判断結果だけみても、どこに問題があるか分からないことが多いのです。

**若江**　困りますね。どう対応したらいいのでしょうか。

**中島**　機械学習ソフトウエアの品質を考える上で、私は三つの視点からのアプローチが大切だと思っています。「プロダク

ト品質」、「サービス品質」、そして「プラットフォーム品質」です。プロダクト品質はバグのないプログラムをつくるなどの製造物の信頼性が、サービス品質は結果が期待を満たしているかという推論結果への信頼性が、それぞれ問われるものです。でも、機械学習の場合、さらにプラットフォーム品質が重要になると思うのです。

**若江**　プラットフォーム品質とは聞き慣れない言葉です。

**中島**　例えば、1から10までの手書きローマ数字を認識する学習プログラムをつくって、いろいろな数字を学ばせるとしましょう。きちんと学べば下手な手書きの字を入れても、正しい回答を出してくれそうなものですが、ここにローマ数字ではなく、漢数字を入れたら正しい結果は出てこないでしょう。そのとき、二つの考え方ができます。一つは、漢数字の認識を考えていなかったのが悪い、だから漢数字も対象に加えて学習しなおそうという考え方。もう一つは、ローマ数字を認識するプログラムに漢数字を入れたのだから、そんなデータを入れるのが悪い、だから使い方を制限しようという考え方です。機械学習では、このように実行結果から妥当性を判断し、学習の作業や学習に使用するデータを調整していく作業を継続していくことが必要で、この過程を支援するプラットフォームがきちんと機能するかどうかがプラットフォーム品質です。AIの信頼性を向上させるには、この三つの品質のうちどれが問題となっているのかを考えながらアプローチすることが大切です。

**若江**　それぞれの品質の信頼性を高めることで、AIの信頼性の問題は解決するのでしょうか。

**中島**　残念ながら、現状はそう簡単ではありません。機械学習の場合、使われながらデータが入力され、学んでいくわけですが、どんなデータが入力されるのか予測できないことも多いからです。

**若江**　あらかじめ利用可能な条件を設定しておけばいいのでは？

**中島**　機械学習の場合、利用可能な条件をなかなか明文化しにくいという問題があります。先ほどの道路標識の誤認識は、黒い落書きを入れると起きるものでしたが、落書きばかりではなく、雨水による汚れなど、いろいろなパターンがありそうですよね。だからといって、利用の条件として「道路標識のない場所で運転して」と言われたら使えないのと同じです。じゃあ、「道路標識に黒い落書きがある道では自動運転は使わない」という条件で使用し、雨水の汚れで誤認識が発生して事故になったら、誰の責任になるのでしょう。つくった人でしょうか、使用した人でしょうか。

**若江**　難しいですね。どうしたらいいのでしょうか。

**中島**　まずは使い方を分類しましょうというのが私の提案です。入ってくるデータが予測可能かどうか、推論結果の妥当性を人間でないと判断できないのか自動的な判断が可能なのか、不具合が起きた場合の深刻さはどのくらいか、という指標で三次元的に分類するのです。そして、ある程度、不具合が発生しても影響の小さい分野から使い始める。不具合が人間の命などに深刻な影響を与えるものは、あくまで人間の意思決定支援に使用をとどめるべきでしょう。例えば、レコメンデーションシステムは、広告に使うなら間違えても大きな問題はないかもしれませんが、医療に使う場合は命にかかわります。自動運転も完全にAIに任せるのはリスクが大き過ぎます。こうした分野でどのようにAIを使うのかは、テクノロジーの観点だけでは判断できません。社会受容性の視点から考えるべきで、それには、技術分野だけでなく社会科学の分野の人と一緒に考えていく必要があると思うのです。

**若江**　その結果、「便利でも使うべきではない」という判断もあり得るのでしょうか。

**中島**　アメリカの社会学者のチャールズ・ペローは『ノーマル・アクシデント～高危険度技術とともに生きる』という本の中で、1979年のスリーマイル島原子力発電所事故について、当たり前の些細な事象が積み重なった結果、破滅的な事故が起きたものだと分析し、適切にコントロールできない高度な技術は、たとえ技術的に可能だとしても、つくってはいけないと主張しました。AIにも同じことが言えるのではないかと思っています。そして、その可否は社会全体で考えるべきことです。

**若江**　最後に、先生が研究している第三者評価制度について教えて下さい。

**中島**　AIシステムを提供する人と使う人、双方の安心のために、第三者的な評価認証の機関が必要だと思っています。攻撃に対する耐性を確認したり、利用条件を明確化したり、不具合が起きた場合の責任を認定したりすることを想定しています。航空事故の情報を世界で共有していることに倣って、AIに関する事故情報の報告・共有の仕組みが技術発展に必要だと思っています。

（写真＝佐藤祐介）

## インタビュアーからのひとこと

一種のブームに沸く中で、AIが攻撃に弱く、品質保証も困難であるという点は見過ごされがちだ。人間の命にもかかわるAIの品質問題が未解決のままというのは怖い気がする。それだけに、「技術的につくることができても、つくってはいけない」ものがあり、その線引きに、テクノロジーと社会の対話が不可欠だという言葉が印象的だった。

**若江雅子** Masako Wakae

1988年 青山学院大学卒業、読売新聞社入社。社会部を経て2014年から編集委員。

# 法的視点から機械学習の品質を考察する

## 製造物責任（PL）法の専門家に聞く、AIの課題

小塚荘一郎氏
学習院大学法学部 教授

×

佐藤一郎
国立情報学研究所 副所長
情報社会相関研究系 教授
総合研究大学院大学 複合科学研究科 教授

**現在のAI（人工知能）システムは、開発に大量の学習データを用いることから、その判断基準も学習データに大きく依存する。しかし、学習データの品質の担保は技術的に難しい。また、学習データは、システムを運用しながらユーザーが新たに追加していく場合もあり、責任の所在を明らかにするのも困難だ。AIの品質保証について、宇宙ビジネスや自動運転、AIなど、先端技術と法の関わりに詳しい小塚荘一郎氏に法的観点から話を伺った。**

### Software-defined からData-defined へ

**佐藤**　なぜ、先端技術における法の問題に関心を持ってこられたのですか？

**小塚**　私が最初に研究したのはフランチャイズ契約で、法律的には、民法などに規定がない、「よくわからない」契約でした。それ以来ずっと、伝統的な考え方では容易に解決できないような取引形態の法的問題に興味を持ってきました。また、以前にITS（高度道路交通システム）に関する書籍（山下友信編『高度道路交通システム（ITS）と法』有斐閣、2005）を共同執筆した際に、「情報」をテーマに執筆する機会があり、以来、自動運転やAIについて考察するようになりました。

**佐藤**　本日は、まさにそのAIを支える技術基盤である機械学習および深層学習の品質保証に関して、法的観点からお尋ねします。というのも、これらの技術は従来のソフトウエア開発とは要件が大きく異なるためです。機械学習を一言で説明すると、大量のデータから学習して得られた「学習済みモデル」に入力を与えることで出力を得る仕組みと言えます。つまり、従来のソフトウエアのようにプログラムに明示的に分類基準（条件）を定めるのではなく、大量の学習用データから分類基準（学習済みモデル）を自動的に学習する。このようにSoftware-definedからData-definedへと移行したことで、得られる結果は統計に基づいたものになります。その際の品質保証を法的にどう捉えればいいのか、頭を悩ませています。

**小塚**　製造物責任（PL）法では、欠陥のある製品（製造物）を製造したメーカーなどが、製造物の欠陥から発生した損害を賠償する責任を負うとしています。この法は、「製造又は加工された動産（物）」を対象としているため、ソフトウエアそれ自体は直接の適用対象ではありませんが、物に組み込まれたソフトウエアは問題となります。そして、そのソフトウエアがデータに置き換えられたとしても、考え方は同じです。最終的に人が使う製品に欠陥があり、「通常有すべき安全性」がないのであれば、製造者に責任が生じます。したがって、AIが組み込まれたツールの「通常有すべき安全性」とは何かについて、まず議論する必要があるでしょう。

**佐藤**　機械学習が統計モデルに依拠している限り、原理的に安全性を100%担保することはできません。また、学習データは過去のものなので、過去に一度も起こったことのない未来

小塚荘一郎
Souichirou Kozuka

東京大学法学部卒業、同大学助手、上智大学法科大学院教授などを経て現職。総務省のAIネットワーク社会推進会議委員。著書に、『宇宙ビジネスのための宇宙法入門』、『支払決済法』（いずれも共著）などがあるほか、最近では『自動運転と法』（藤田友敬編）にも寄稿している。

の状況には適応できません。

**小塚**　もっとも、すでに世の中にある製造物でも、100% 安全性を備えているとは限りません。そのため、例えばロケットであれば、打ち上げの際の不測の事態に備えて、複数のラインで中止できるような冗長性を持たせています。つまり、人に危害を加えないようなセーフティガードがあればいい。ハサミも、使い方によっては凶器になりますが、世の中から放逐しないのと同じです。むしろ、ユーザーに対して注意喚起しながらうまく使っていくほうが、社会にとって望ましいのではないでしょうか。

**佐藤**　心強いお言葉をいただきました。

## ユーザーのリテラシー向上が不可欠

**佐藤**　もう一つ懸念しているのは、AI は例外的な状況にほとんど対応できない点です。学習データから外れた入力があった場合、一気に信頼性が落ちてしまう。そもそも、ユーザーはどういう学習データが与えられたのかを知りません。

**小塚**　まず、想定外の結果が出てしまったときに、ユーザーが容易にリアクションをとれるものなのかどうか。それが難しいのであれば、やはりなんらかの策を講じなければなりません。例えば、ユーザーをアシストするようなプロフェッショナル・ユーザーのような人が必要かもしれませんね。現状のままでは、技術の進歩にユーザーが追いついていけないのではないかという懸念があります。

**佐藤**　今は、BtoB が中心ですが、今後、一般消費者が AI を使うようになると、さまざまな問題が生じてくるように思います。

**小塚**　企業といえども、どれだけのリテラシーを有しているのでしょうか。例えば、スルガ銀行が勘定系システムの開発をめぐり IBM を訴えた裁判を見ても、双方に相当な認識のギャップがあったと感じます。ユーザーの AI リテラシーを高めるための取り組みが不可欠だと思います。

## 価値の源泉としてのデータをどう扱うか

**佐藤**　もう一つ、AI では、システムが稼働した後に、ユーザーやクライアントが新たに学習データを追加していくことがあります。当然、開発者側は追加データについて関知できません。場合によっては、攻撃データを追加することで、誤作動を起こさせることも可能です。しかも、機械学習の学習済みモデルは統計的な数値の塊なので、人が外から読んでも意味を理解できない。かといって、新たにデータを追加させないのでは AI の良さが発揮できないし、なんらかの約束事が必要だと思っています。

**小塚**　ただその場合は、どういう範囲のデータなら追加してもいいのかという条件を書き出す必要がありますが、それが技術的に可能なのかどうか。

**佐藤**　難しいですね。例えば自動運転向けの AI の場合、昼用のシステムなら、夜のデータは入れないでといった大雑把な制限しかできないでしょう。また、田舎道で学習した自動運転車は田舎道ではよくても、都会の道を走った場合は事故を起こしかねないという問題もあります。

**小塚**　そうなると、ますます開発者やユーザーの注意義務が重要になります。

**佐藤**　一方で、適切な学習データを蓄積したシステムほど価値が上がるということも考えられます。すなわち、中古品のほうが高く売れるわけです。また、学習済みモデルが流通した場合の知財も問題となります。

**小塚**　それは法律家としては考えさせられる課題です。リスクコントロールを、オリジナルの学習済みモデルを開発したメーカーではなく、中間の中古販売業者に委ねていいものかどうか。中古品の流通業者は、一般的にメーカーよりも規模、資力ともに小さいですから。もしかすると、骨董品販売の鑑定書に似た仕組みが必要かもしれません。ところで、学習済みモデル自体を流通させることは難しいのでしょうか。

**佐藤**　学習済みモデルの法的責任関係や権利関係が整理できないという問題があります。

**小塚**　利害関係者を集めて標準的な処理を決めるのも一つの手だと思います。ただ、そのようにしてしまうと競争がなくなりますから、そこで決めた標準が業界の慣行になるのがいいのかどうか悩ましいですね。いずれにしろ、リスクを放置したまま製品化すれば、注意義務を欠いたことになり、法的に追及されます。議論は不可欠です。

一方で、ドイツやアメリカでは、何かあれば損害賠償を負うことを前提に、新しい技術を普及させてきた歴史があります。日本では、誰もリスクをとりたがらないために、不幸にして事故が起きると、事故の当事者が必要以上に社会的に責められる傾向にあります。無過失責任という考え方も、技術の普及にあたって検討してもいいかもしれません。

**佐藤**　本日はたいへん貴重なご意見をありがとうございました。

（取材・文＝田井中麻都佳
写真＝佐藤祐介）

佐藤一郎
Ichiro Satoh

NEWS 1

# NIIウィークを開催、学術関連イベント目白押し

**NIIは6月18日（月）から23日（土）までの1週間を「NIIウィーク」と位置づけ、NIIのある学術総合センター（東京都千代田区）を会場にさまざまな学術関連イベントを開催しました。**

NIIの研究と取り組みをまとめて紹介

## Japan Open Science Summit 2018（JOSS2018）

JOSS2018で行われたパネルディスカッションの様子

第1弾として、NII、科学技術振興機構、物質・材料研究機構、科学技術・学術政策研究所、情報通信研究機構、学術資源リポジトリ協議会は共同で、日本や世界のオープンサイエンスの最新動向を発信する「Japan Open Science Summit 2018（JOSS2018）」を6月18日、19日に開催しました。JOSS2018は、オープンサイエンスを推進する研究者や市民科学団体、図書館やリサーチ・アドミニストレータなどの研究支援組織など、関係するすべてのステークホルダーが一堂に会する日本最大級のカンファレンスです。

初日は、基調講演にオーストラリア国立データサービス エグゼクティブディレクターのRoss Wilkinson氏をお招きし、「オープンデータとその質保証に関するオーストラリアおよび国際的な視点」と題してお話いただきました。第2日は、日本医療研究開発機構（AMED）の末松 誠理事長に「AMEDのミッション：データシェアリングはなぜ難しいか？」と題してご講演いただきました。また、主催6機関の代表が登壇し、「日本における研究データ利活用に関する活動の現状と展望」と題したパネルディスカッションを行いました。

## 学術情報基盤オープンフォーラム2018

6月20日、21日は、「学術情報基盤オープンフォーラム2018」を開催しました。本フォーラムは、NIIが構築・運用する学術情報ネットワーク「SINET5」によって実現する大学・研究機関における教育研究環境の具体的なイメージをいち早く関係者と共有し、利用者とともに発展させることが目的です。

2日間のプログラムでは、「コンテンツトラック」「クラウドトラック」「SINETトラック」「Open Scienceトラック」「ラーニング・アナリティクストラック」「セキュリティトラック」など9トラックでセッションを行い、講演や活発な議論を行いました。このうち、セキュリティトラックでは、2017年7月から本格スタートした大学間連携に基づく情報セキュリティ体制の基盤構築（NII-SOCS: NII Security Operation Collaboration Services）について、今後の在り方や方向性を話し合いました。

## オープンハウス2018

NIIウィークの最後は、NIIの研究成果や事業内容を広く一般の方々に知っていただくためのイベント「国立情報学研究所オープンハウス2018（研究成果発表・一般公開）」を6月22日、23日の2日間の日程で開催しました。

初日の基調講演には、国の成長戦略を話し合う政府の「未来投資会議」のキーパーソンである東京大学 五神（ごのかみ） 真（まこと） 総長をお招きし、「Society 5.0の実現に向けた国立情報学研究所への期待」と題してお話しいただきました。

第2日は、国際情報オリンピック向けの問題にチャレンジするプログラミングワークショップ「目指せ 未来の情報オリンピックメダリスト！」を開催しました。情報オリンピック日本委員会の筧（かけひ） 捷彦（かつひこ）理事長、国際情報オリンピックのメダリスト4人、国際プログラミング大会で入賞経験のあるNIIの吉田 悠一准教授、岩田 陽一助教が参加者をサポートしました。参加した高校1年生の男子生徒は、「自分が書いたプログラム通りに出力できるとすごくうれしい」、高校1年生の女子生徒は「難しいけれど、プログラミング言語の意味が分かると楽しくなる」と感想を話しました。

また、今年で4年目となるオープンハウスの人気企画「NII研究100連発」もたいへん盛り上がりを見せました。NIIの研究者10名が、一人7分間の持ち時間の中でそれぞれ10件、合計100件の研究成果を次々に発表すると、その迫力あるプレゼンに会場のお客様は圧倒された様子で見入っていました。

［上］基調講演を行う東京大学 五神 真 総長
［下］中高生が国際情報オリンピック向けの問題にチャレンジしたプログラミングのワークショップ

## 湘南会議100回記念シンポジウム

オープンハウスの開会式に先立ち、「湘南会議100回記念シンポジウム」を開催しました。NII湘南会議は、世界トップクラスの研究者を集めて合宿形式で情報学分野の課題を集中的に議論するセミナーで、開始から100回目を迎えたことを記念して今回のシンポジウムを開催しました。シンポジウムでは、計算幾何研究の大家であるザールラント大学のRaimund Seidel教授、四色定理の機械的な証明で有名なボルドー大学のPierre Casteran教授が基調講演を行いました。

## 総研大情報学専攻説明会

オープンハウスに合わせ、総合研究大学院大学（総研大）複合科学研究科 情報学専攻の説明会も開催しました。国立情報学研究所は総研大に参画し、複合科学研究科内に情報学専攻を設置。5年一貫制博士課程および3年次編入学博士課程の大学院教育を実施しています。

説明会では、情報学専攻の概要、出願方法などを説明したほか、情報学専攻に在籍している学生が、学生生活や自身の研究内容、情報学専攻の特徴などを話しました。

NEWS 2

# 日本代表は金1、銀1、銅2、全員がメダル獲得

## 日本初開催の国際情報オリンピック

第30回国際情報オリンピック（IOI 2018 JAPAN）が9月1日から8日まで、茨城県つくば市で開かれ、世界87カ国・地域、335人の高校生たちがプログラミングの腕を競いました。

日本代表は、井上航（いのうえわたる）さん（北九州工業高等専門学校3年）が総合6位タイで金メダル、細川寛晃（ほそかわひろあき）さん（灘高校3年）が銀メダル、清水郁実（しみずいくみ）さん（N高校3年）、行方光一（なめかたこういち）さん（筑波大学附属駒場高校2年）が銅メダルを獲得しました。また、開催国特別参加選手のため表彰対象にはならなかったものの、米田優峻（よねだまさたか）さん（筑波大学附属駒場高校1年）が金メダル相当、米田寛峻（よねだひろたか）さん（開成高校1年）、平木康傑（ひらきやすたか）さん（灘高校1年）が銀メダル相当、岸田陸玖（きしだりく）さん（京都市立堀川高校3年）が銅メダル相当のすばらしい成績を収めました。

国際情報オリンピックの競技の様子（写真提供：情報オリンピック日本委員会）

国際情報オリンピックは、高校生までの生徒を対象とする国際科学オリンピックの大会の一つ。競技は個人戦で、9月3日と5日の2日間、計10時間にわたり実施されました。今大会は、秘密のコマンドを探し出す「コンボ（combo）」や国際プログラミングコンテストの座席表の美しさを計算する「座席（seats）」、人形を動作させる回路を組んでいく「からくり人形（doll）」などの問題が出題されました。プログラムの実行時間や使用メモリに関して制限があり、正しいプログラムを書く能力だけでなく、アルゴリズムやデータ構造を考案する能力が求められます。採点の結果、上位約12分の1（今大会では29名）に金メダル、その次の上位約12分の2（今大会では55名）に銀メダル、次の上位約12分の3（今大会では83名）に銅メダルが授与されました。

競技のほか、数理情報科学の次世代を担う選手同士が交流を深めることを目的として、2日間のエクスカーション（体験型見学会）が行われました。選手たちは、つくば市の宇宙航空研究開発機構（JAXA）筑波宇宙センターや産業技術総合研究所サイエンス・スクエアつくばなどを訪れ、日本の最先端の科学技術に触れたほか、国営ひたち海浜公園やアクアワールド茨城県大洗水族館、大洗磯前神社などを訪れ、日本の自然や文化を満喫しました。

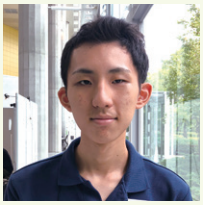
日本代表選手の（左から）井上さん、清水さん、行方さん、細川さん（写真提供：情報オリンピック日本委員会）

次回大会は、2019年夏、アゼルバイジャン共和国で開催される予定です。日本代表選手を選抜する国内予選（第18回日本情報オリンピック予選）は、10月9日より参加申込を受け付けます。詳細は、https://www.ioi-jp.org/joi/2018/index.html

### NIIは「SINET5」のネットワークを提供、ブースも出展

NIIは、特別協賛として日本大会をサポートしました。NIIが構築・運用する「SINET5」のネットワークの中に、専用の仮想プライベートネットワーク（L2VPN）を構築して、競技会場と、東京のサーバーをつなぎました。また、大会期間中、競技会場隣りのつくば国際会議場にブースを設置し、NIIの研究や事業を世界の選手にPRしました＝写真。


### メダリストの声



金メダル 井上航さん

金メダル Zi Song Yeoh さん（マレーシア代表）

パソコン甲子園をきっかけに本格的にプログラミングを始めました。1日目の「座席」の問題が難しく、大きな部分点がとれなかったことが反省点。でも、2日目は集中して良い結果を出すことができました。6位という結果は目標より上位だったので満足しています。これからは、他のプログラミングコンテストにも出場してみたい。将来は、プログラマーかエンジニアになりたいと思っています。

**外国人選手の声** 一緒に数学オリンピックに出場した友人にすすめられてプログラミングを始めました。3回目の出場で初めて金メダルを獲得することができてとても感激しています。普段は、いろいろなコンテストの過去問を解いて、腕を磨いています。日本大会は、競技だけでなくエクスカーションもとても楽しかった。サイエンス・スクエアが思い出に残りました。

SNS 「これいいね！」 Facebook、Twitterアカウントの最も注目を集めた記事（2018年6月~2018年8月）

**国立情報学研究所 NII（公式）** Facebook
www.facebook.com/jouhouken/

国立情報学研究所は、6月23日（土）に大学院説明会を開催します。ご関心をお持ちの方は、ぜひご参加ください。今回は、飯野さん（博士後期課程1年）からのメッセージをお届けします。「構造化知識を用いた楽器演奏の指導・学習支援に関する研究をしています。皆さまの参加をお待ちしております。」（2018/6/16）

**国立情報学研究所 NII（公式）** Twitter
@jouhouken

［NII研究100連発］
NIIで活躍する研究者10名が、1人10件、合計100件の研究を発表します。情報学の幅広い分野を俯瞰し、情報学の未来をともに考える75分の白熱プレゼンを見に来ませんか？MCは大向准教授（@i2k）と池澤あやかさん（@ikeay）です。（2018/6/5）

**つぶやくビット君** Twitter
@NII_Bit

NII研究100連発MCの池澤あやかさん（@ikeay）と大向一輝准教授（@i2k）、おつかれさまびっと！！！
#NIINow（2018/6/22）

＊記事の本文は一部編集・省略しています。

Essay

# 工学研究コミュニティの本来の姿

**吉岡 信和**
Nobukazu Yoshioka
国立情報学研究所
アーキテクチャ科学研究系
准教授

ソフトウエア工学とは、どのようにしたら、よりよいソフトウエアをつくることができるのかを研究する分野である。当たり前であるが、ソフトウエアをつくるための研究は、ソフトウエアをつくる人に使われないと意味がない。しかし、最近のソフトウエア工学コミュニティは、ソフトウエアをつくる人たちである企業からの参加者が少なくなっている。産学の交流が少なくなると、大学の研究者は、現実にありえない課題を想定してしまい、使われない解決法に労力をつぎ込んでしまう可能性が出てくる。

そうした中、本号で紹介した機械学習工学のコミュニティに参加している人の7割以上は企業の人である。今の活動は、コミュニティができたばかりということもあり、実際にソフトウエア開発の現場で体験している課題を共有し、整理することが中心となっている。つまり、研究者にとっては、ソフトウエアを開発する人の生の声を聞くことができ、解くべき課題が溢れている、またとない場になっている。

従来のソフトウエア工学は、人が知識を整理し、それを元にソフトウエアを論理的につくり上げる理論（演繹的なソフトウエア開発）を中心に発展してきた。この理論は、データ（事実）から規則を帰納的に導出する機械学習の理論（帰納的なソフトウエア構成）とは全く異なり、これまでのやり方では、機械学習を使って、品質の高い、適切なソフトウエアをつくることが難しい。そのため、機械学習を利用するさまざまなソフトウエア開発で課題に直面しているのである。

すなわち課題の本質は、統計処理を中心とした機械学習を、アルゴリズムやルール、推論などの、従来の論理的なソフトウエア記述と融合することに起因している。これを解決することは、学術的にも挑戦的で意義がある。

人間の脳が論理的思考と経験に基づく直感をうまく組み合わせて妥当な判断をするように、論理的に考える部分と、事実から帰納的に推測する部分をうまく組み合わせてソフトウエアをつくることができれば、さまざまな問題を妥当な判断で解決できるようになるだろう。

今は、この機械学習工学のコミュニティを運営する傍ら、現場の声に耳を傾けているが、これからが我々研究者が貢献できるかどうかの勝負どころである。さあ、研究者の叡智を結集し、課題に取り掛かろう。

## 今後の予定

**10月14日**｜大学共同利用機関シンポジウム2018（出展）
**10月16日～19日**｜CEATEC JAPAN 2018（出展）
**10月24日**｜市民講座「情報学最前線」第4回「将来の無線アクセスネットワーク ―今のままでは周波数が足りない！―」（講師：アーキテクチャ科学研究系 金子 めぐみ 准教授）＝詳細、お申し込みは https://www.nii.ac.jp/event/shimin/
**10月25日**｜第2回 SPARC Japan セミナー2018＝詳細は http://www.nii.ac.jp/sparc/
**10月30日～11月1日**｜第20回図書館総合展（出展）
**11月9日**｜第3回 SPARC Japan セミナー2018
**11月19日～21日**｜大学ICT推進協議会（AXIES）2018年度AXIES年次大会（出展）
**11月20日**｜市民講座「情報学最前線」第5回「リアルデータの『共同利用』 ―あなたの情報が学術研究に!? でも大丈夫―」（講師：コンテンツ科学研究系 大山 敬三 教授）
**11月30日**｜SINET特別セッション①「AIやICTを活用した牛の放牧による生産技術の開発」（講師：後藤 貴文 鹿児島大学 農水産獣医学域農学系 農学部農業生産科学科 教授）＝詳細、お申し込みは https://www.nii.ac.jp/event/shimin/
**12月11日**｜市民講座「情報学最前線」第6回「計算の理論と現実 ―難しいはずの計算がいとも？簡単に―」（講師：情報学プリンシプル研究系 岩田 陽一 助教）

**表紙の言葉** 機械学習にちなんで、「リンゴとオレンジの選別の仕方」を教える授業風景を描きました。教師ロボットが生徒ロボットに、赤いラベルが紐付けされたリンゴを見せています。よく見ると、ラベルが切れてしまった果物も混じっていますね。

情報から知を紡ぎだす。
NII
国立情報学研究所ニュース［NII Today］第81号 平成30年9月
発行｜大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
〒101-8430 東京都千代田区一ツ橋2丁目1番2号 学術総合センター
発行人｜喜連川 優　編集長｜佐藤一郎
表紙画｜城谷俊也　編集｜田井中麻都佳
制作｜株式会社マツダオフィス／サイテック・コミュニケーションズ
本誌についてのお問い合わせ｜総務部企画課 広報チーム
TEL｜03-4212-2028 FAX｜03-4212-2150 e-mail｜kouhou@nii.ac.jp


http://www.nii.ac.jp/about/publication/today/