蓮尾 一郎 Hasuo Ichiro

国立情報学研究所 アーキテクチャ科学研究系 教授
2016年よりERATO研究総括

特集1 OVERVIEW

自動運転車の安全性の数学的証明に挑戦
公道で通行可能な未来の実現に向けて

自動運転技術は、交通事故の防止につながる技術として高い注目を集めている。自動運転のレベルは0～5までの6段階に分けて定義されており、走行領域など決められた条件下で全ての運転操作を自動化する「レベル4」の実用化に向けた試みが着実に進んでいる。将来的に、自動運転車が公道で通行可能な未来を実現するためには、安全性を高めるだけでは不十分であり、住民への説明を重ねて安全性を保証する必要がある。自動運転車の安全性の数学的証明に取り組んでいる国立情報学研究所アーキテクチャ科学研究系の蓮尾一郎教授に信頼を高める道筋を聞いた。

生活に不可欠な最先端技術 無条件で信頼できない悩み

ITが各種の工業製品や公共システムに統合され、高性能・多機能なコンピューター搭載機器とネットワークインフラが私たちの仕事と生活に不可欠なものになってきた。これまで予想さえできなかったような新しい価値を生み出し続けている半面、私たちに最先端技術を無条件で信頼していいのかという悩みも引き起こした。その典型例が自動運転だ。自動車そのものだけでなく、道路整備や管制システム、通信システムなど周辺インフラを含めた対策が練られているところだが、万人が納得できる安全性保証の仕組みはいまだ確立できていない。

「安全性の保証は終わりのない取り組み。常に新しい技術が生まれ、社会も人も変わります。そこで誰もが現時点で納得できる安全性を論証できることが重要です」と国立情報学研究所アーキテクチャ科学研究系の蓮尾一郎教授は言う。数ある工業製品の中でも、自動車は自動制御の少しの間違いが極めて重大な事故を招きかねない。そのため、蓮尾さんは社会に信頼される安全性の論理的証明について研究を続けてきた。

この問題に取り組む蓮尾さんのグループのもともとの出発点は「圏論」という理論だ。これは、現代数学の抽象的議論を行うための言語に相当する。問題が自動的に解けていくように問題に正しい環境を設定するのが圏論の考え方だ。圏論の語彙（ごい）が限られているために、圏論を基に理論を確立できると本質を捉えた無駄のない理論が得られる。この圏論の威力を直接的・間接的にシステム設計に生かすのが、ERATO「メタ数理システムデザインプロジェクト」の目的であり、蓮尾さんたちの自動運転の研究では、圏論は直接使われていない一方で、圏論を専門にする多数の研究者が活躍している。

定義すべき要素は無数に 平易で論理的な証明が必要

自動運転の安全性はどのようにすれば証明できるのだろうか。数学では証明の基本前提として、証明する対象の定義が必要だ。ところが、自動運転システムでは膨大な部品やコンピューター、駆動系などの車本体に加えて、道路や他の走行車、人間の振る舞いなどのさまざまな要素も考慮しなければならない。定義すべき要素は無数にあり、仮に定義できたとしても巨大すぎる数値行列になり、解析するのは困難を極める。

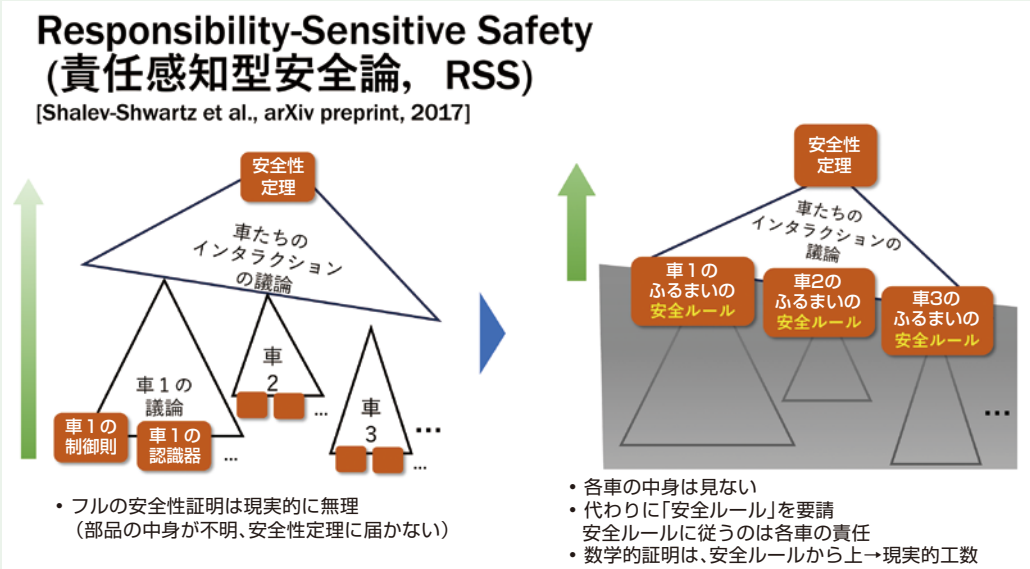
プログラムとして記述可能な部分は定義できるが、プログラムでは記述されない部品もあれば、人間の振る舞いなど数値化が困難な条件もある。定義できないものは、従来の方法による論理的証明が不可能になる。その場合は別の方法として、統計的な安全性証明を試みることになるが、あらゆる事態を想定した実車での検証はコストなどの理由から難しい。また、シミュレーションでもどれだけのシナリオを用意すれば十分なのか予見できず、現実的には困難だ。

つまり「100パーセントの安全は保証できないが、ここまで安全が保証できれば十分だ」という社会合意を得るための数学的根拠が必要である。一般的な工業製品では、国際安全規格の形で社会的合意を満たした基準ができているが、自動運転の場合は、まだそれがない。製造物責任を負うメーカーにとっては責任の限界が見えず、ビジネス上のリスクは莫大（ばくだい）だ。自動車保険などの周辺ビジネスにとっても、安全性証明は決定的な影響をもたらす。そのため、わかりやすく論理的な安全性証明が求められている。

企業が解決のヒントを提唱 適用範囲を広げた新手法確立

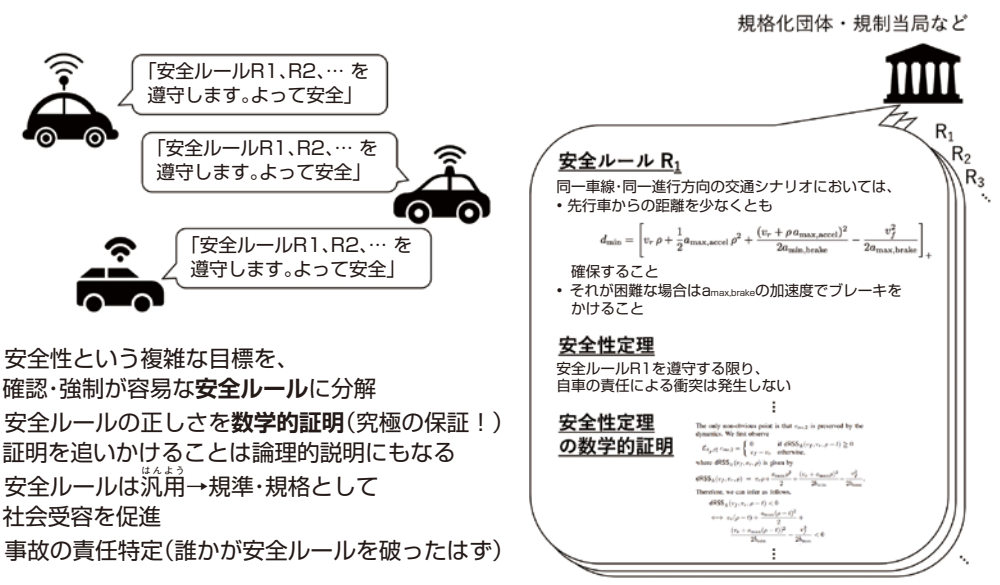
この問題を解決するヒントとなる方法論に、企業研究者のShalev-Shwartz（シャレフ シュワルツ）が提唱した「RSS（責任感知型安全論／Responsibility-Sensitive（レスポンシビリティー センシティブ）

図1 RSSの概念



多くの会社が自動運転車の開発に取り組んでいるが、各車種の制御則などを積み上げて一般的な安全性を議論していては、安全性定理に到達するのが難しい。一方で、各車の制御則などは無視して、その代わり安全に走行するためのルールを策定し、各車種にはそのルールに従うことを要請する。このルールをベースにすることで安全性を論理的に証明することが容易になる。

図2 RSSとGA-RSSの考え方



- 安全性という複雑な目標を、確認・強制が容易な**安全ルール**に分解
- 安全ルールの正しさを**数学的証明**（究極の保証！）証明を追いかけることは論理的説明にもなる
- 安全ルールは汎用（はんよう）→規準・規格として社会受容を促進
- 事故の責任特定（誰かが安全ルールを破ったはず）

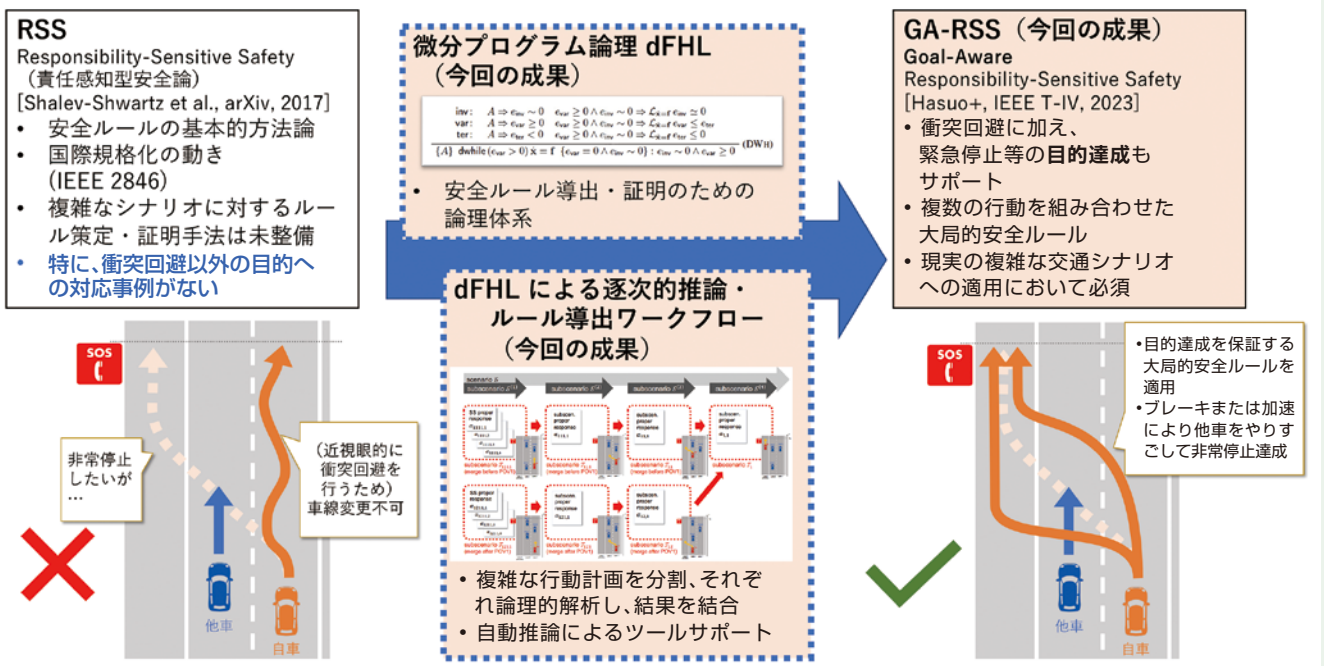
数学的に厳密な論理的安全ルールを提案し、さらに「この論理的安全ルールを順守する限り事故を起こさない」ことを「安全性定理」として数学的に証明した。

Safety（セイフティー）」がある**（図1）**。これは、多数のシミュレーションを基に安全性を証明する従来法とは異なり、まず自動運転車の交通安全のためのルールを策定し、そのルールの中で安全性を証明するアプローチをとる。この方法論ではルールを数式で表現し、数式の妥当性を論理的に証明することができる。数学的証明が可能なため、国際規格、業界標準、交通法規としての活用も盛んに議論されているところだ。

しかし問題は、どうやって安全ルールを策定すればよいのか、そのルールでの安全性をどう証明すればよいのかだ。その技術的基盤はまだ発達しておらず、例えば高速道路上で先行車に追突しないように追尾するといった限られた単純なシナリオであれば、車間距離を適正に保って衝突しないことが数式で簡単に証明できる。だが、そんなシンプルなシナリオだけでは、現実に起こりうるさまざまな交通事情に対応できるはずもない。

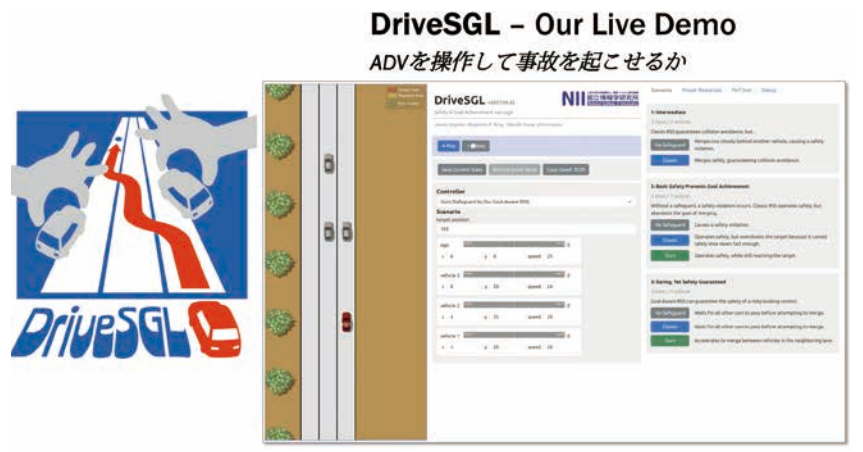
そこで、蓮尾さんはより複雑なシナリオとして、2車線を走行時に、車線変更をして左車線を走行する車列に割り込み、さらに減速して走行車線を抜け出し、緊急電話のある路肩の特定箇所に非常停車するというシナリオでの安全確保に取り組んだ。特定箇所に停車するためには、隣車線の車の速度に応じて加速したり減速したりする必要があるが、加速・減速しすぎると他車と衝突を起こし

図3 GA-RSSによる安全ルールの本格展開



RSS（左）にdFHL（中）を組み合わせることで GA-RSS（右）への拡張を実現し、多様な自動運転の状況へ適用できるようになった。この非常停止の例では、従来のRSS安全ルールは近視眼的な衝突回避行動の優先順位が高く、非常停止という目標を達成できなかった。一方、GA-RSS安全ルールは、加速やブレーキによって他車をやりすごす大局的な行動計画を安全ルールに組み込むことができ、非常停止という目標を達成できる。

図4 GA-RSSの効用を体験できるゲームソフトの開発



たり、オーバーランしたりしてしまう可能性がある。その複雑な意思決定を自動化するシミュレーション技術の開発に、蓮尾さんは成功した。

RSSの提唱者は証明の形式化までは行っていなかったため、蓮尾さんは「dFHL（differential Floyd-Hoare Logic、FloydとHoareはともに計算機科学者）」と名付けた形式論理の体系を考案した。これは、自動車制御のようにデジタル・アナログ両方にまたがるハイブリッドシステムの安全性証明を効率的に行うものだ。dFHLによって、自動運転車の複雑な行動計画を分割し、逐次的な解析が可能になり、蓮尾さんたちはRSSの適用範囲を拡張した新手法「GA-RSS（Goal-Aware RSS）」を確立した**（図2・3）**。「策定された安全ルールに則った自動運転車は事故を起こさない」という安全性定理の証明に成功したのだ。

ERATOで多くの成果を発表 一般製造業のDXにも貢献

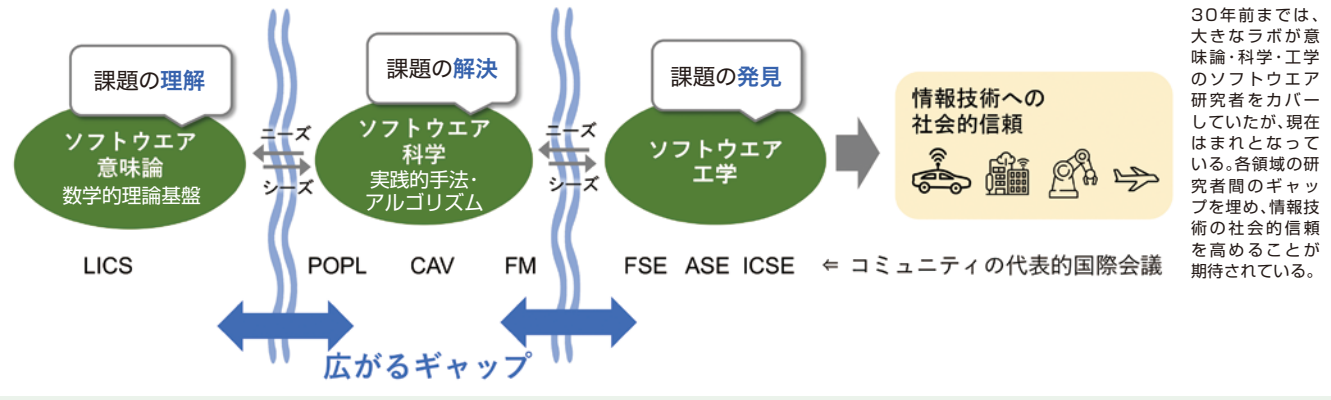
自動運転車の複雑な意思決定の安全性を数学的・論理的に証明可能にし、安全ルール策定をソフトウエアで支援するという革新的な技術を誕生させた蓮尾さん。この成果は、証明をするための論理体系を設計し、証明をする営みにソフトウエアによるサポートを与えるものだ。これまで証明作業は手書きだったのが、コンピューターで電子的に書けて効率化されたように、デジタルとアナログのハイブリッドシステムの安全性証明を効率よく実行できるという。「産業界での安全性保証の取り組みや国際規格策定に向けた動きに大きく貢献できると考えています」と笑顔で語る。

蓮尾さんはさらに、GA-RSSのゲーム形式のデモソフトも開発している。これは一般公開されていないが、自動走行しながら路肩の特定位置に非常停車しようとしている自動運転車を停車させないように、プレイヤーが他の車を使って邪魔をするゲームである**（図4）**。実際にプレイ動画を見ると、どのような邪魔をしても自動運転車は間違いなく安全に停車位置に停車できることが確認できた。

ERATOプロジェクトでは、自動運転に関してさまざまな成果を上げている。これまで「テストが難しいシミュレーション設定を自動で見つける技術の開発」や「自動車システム設計の安全性を自動分析する手法の開発」、「自動運転の経路計画プログラムから危険動作を自動検出する手法の開発」、「自動運転における重大な問題をシミュレーションで検出する技術の開発」といった一連の研究成果も発表している。これらは自動車業界のみならず、一般製造業のDXにも貢献する成果だ。

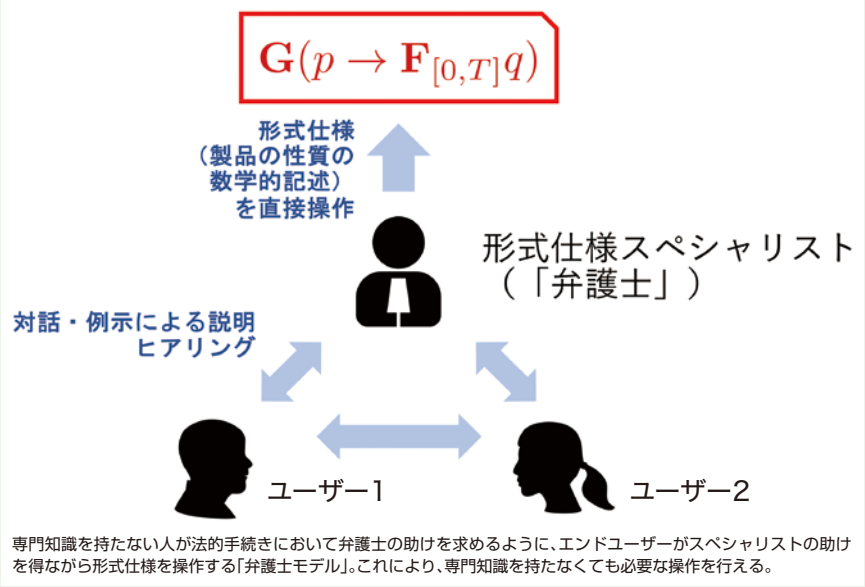
自動運転車以外でも、例えば「計測誤差があるセンサーを使っても安全に動くように制御ソフトウエアを自動変換する手法の開発」や「信頼性が高いガスタービンのシステム設計を自動で効率良く発見する技術の開発」、「意思決定支援システムが示す選択肢の正しさと計算スピードを両立する手法の開発」といった成果も上げている。「圏論を直接用いた理論的成果群はまた別にあるのですが、これらの実用的な成果群も、圏論で応用研究に挑もうというメンバーが

図5 ソフトウエア領域の研究者間のギャップ



30年前までは、大きなラボが意味論・科学・工学のソフトウエア研究者をカバーしていたが、現在はまれとなっている。各領域の研究者間のギャップを埋め、情報技術の社会的信頼を高めることが期待されている。

図6 弁護士モデル



専門知識を持たない人が法的手続きにおいて弁護士の助けを求めるように、エンドユーザーがスペシャリストの助けを得ながら形式仕様を操作する「弁護士モデル」。これにより、専門知識を持たなくても必要な操作を行える。

集まったからこそ、得られたものだと考えています」と蓮尾さんは総括する。

理論・応用研究者を再団結 研究をさらに国際的に展開

ERATOプロジェクトは、22年4月まではグループ0〜3の4グループで構成されていたが、現在はグループ0と追加で立ち上がったグループ4「高信頼ソフトウェアシステムグループ」と社会実装のための「ERATO MMSD 産業化チーム」から成り立っている。23年には、幕張メッセや独ミュンヘンで開催された自動車産業向け展示会へも出展し、国を超えた自動運転化社会の基盤作りに力を入れている。

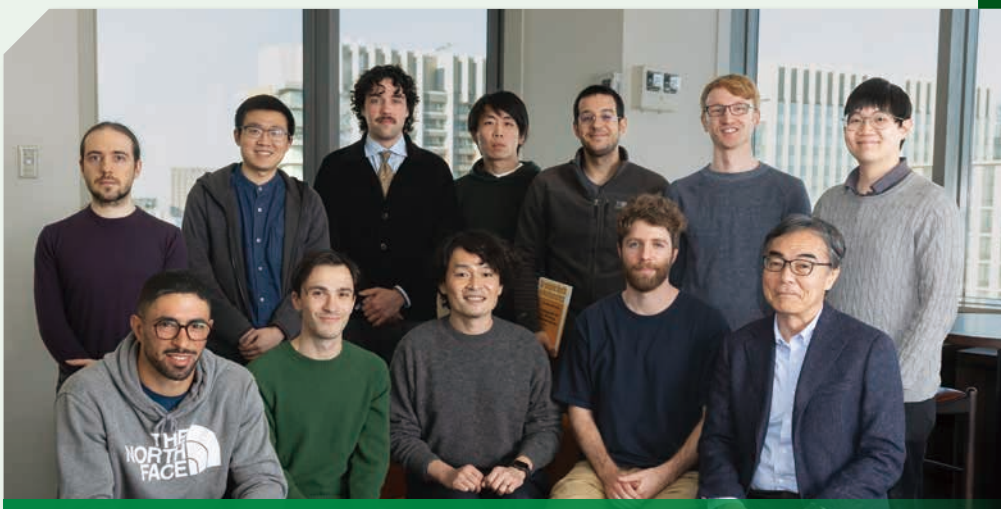
蓮尾さんは、ソフトウエア研究における理論・応用研究者間の溝が一昔前よりも深くなっていることに大きな危機感を抱いていたという。「そんな中、ERATOで応用研究に挑戦するきっかけをいただきました。学術面だけでなく、産業界にも貢献できたのは、チームメンバーや研究の種をくださった企業の皆さんのおかげです」と感謝の思いを語る。プロジェクトを通した人的交流で溝が狭まり、互いのニーズとシーズを理解して協働できるようになり、一気通貫に課題の理解・解決、そして新たな課題の発見が可能となった(図5)。

蓮尾さんの今後の目標は、研究者のさらなる再団結を図り、プロジェクトの研究を国際的なうねりにつなげていくことだ。すでにJSTのASPIRE（先端国際共同研究推進事業）で蘭・独・英との共同研究も始まっている。また、プロジェクトの成果を基に年内のスタートアップ企業設立に向けて準備を進めている。ソフトウエアの保守・改良を主事業とし、長期にわたって自動車メーカーなどに利用してもらえるようにすることが目的だ。

今後、安全性証明の対象は交通システムが未開発なドローンや、人間との関わりがセンシティブなホームロボットや介助ロボットにも発展していく可能性がある。蓮尾さんは、法律の専門家を信頼して法的な手続きを任せるように、さまざまな製品の安全性の条件を数学的に明示して、数学の専門家が正しいと判断すればユーザーが承認するモデルを検討している。蓮尾さんが「弁護士モデル」と呼ぶこのモデルにより、メーカーや規制団体、規格化団体が論理的な安全性証明を受け入れて認証し、エンドユーザーがそれを根拠に信頼するという仕組みが考えられる(図6)。

理論研究で得た知見を携えて応用研究に飛び込んだ蓮尾さん。数々の重要な研究成果を上げ、そこから派生して得られた成果はより一層広がりを見せることだろう。蓮尾さんの研究室は外国人研究者が多く、海外の大学とも協働してきた。今後も、国際的なネットワークをさらに拡張し、団結して研究を続ける蓮尾さんのプロジェクトからますます目が離せない。

（TEXT：土肥正弘、PHOTO：石原秀樹）



乖離（かいり）しがちであった理論と応用の研究者の再団結を図り、プロジェクトの研究を国際的なうねりにつなげていきたいです。国内外の研究者とともに、国際的に技術を産業界と社会につなぐ流れを作りたいと考えています。