ベリサーブ技術通信

Summer
2016

2016年6月発行

VERISERVE NAVIGATION
ベリサーブナビゲーション

Vol.6

システム品質向上と
人工知能の関係を考える
“数値化”と“データの蓄積”が
人工知能の可能性を広げていく

ロボット法と自動運転について

ソフトウェアやシステムの開発や
検証において品質向上や
効率化に貢献する
コンテキスト理解

他

Periodical Magazine

Presented by Veriserve.

VERISERVENAVIGATION | Vol. 6

ベリサーブナビゲーション

Summer 2016

Contents

インタビュー

電気通信大学 准教授 保木 邦仁 氏

システム品質向上と人工知能の関係を考える

“数値化”と“データの蓄積”が人工知能の可能性を広げていく

INTERVIEW

巻頭特集

インタビュー ｜ 電気通信大学 准教授　保木 邦仁 氏

システム品質向上と人工知能の関係を考える

“数値化”と“データの蓄積”が人工知能の可能性を広げていく

人工知能（AI）によるSNSアカウントや自動運転車が登場するなど、人工知能が一大ブームとなっています。将棋や囲碁においてトッププレイヤーにコンピュータが勝利したというニュースも話題となり、映画やアニメで描かれていた未来がすぐに現実になるのではないかと驚きとともに受け止められています。さまざまな領域で人工知能の活用が現実味を帯びてきた今、システム品質の向上における可能性はどの程度あるのでしょうか？ 将棋ソフト「Bonanza」の開発者であり、現在は人工知能の研究に携わる電気通信大学 准教授・保木 邦仁氏にお話を伺いました。

どこから人工知能と言えるのか、現時点で明確な定義はない

――最近「人工知能」に関するニュースを目にする機会が増え一大ブームの感もありますが、こうした動きを先生はどのように受け止めていらっしゃいますか？

保木 正直、驚いています。ここまで注目されるようになるとは思ってもいませんでした。人工知能というと、アニメや映画に登場するアンドロイドやロボットのようなものを思い浮かべる人も多いと思います。これらは人工知能の究極形のひとつですが、現状はまだそのレベルに到達しておらず、チェスや将棋、囲碁といった特定のゲームで人間を凌駕しうるようになったにすぎません。こういった最新の人工知能研究において中心を担っているのが「機械学習」です。理論自体は昔からあったのですが、それを実行する道具としてインターネットやコンピュータなどの高性能化が進み、ようやく現実的なものとなりました。10年ほど前から、桁違いな規模でデータを収集することが可能になり、こうした仕組みを使って収集・分析し続けた結果、今さまざまな成果が表れ始めたというわけです。

人工知能の定義は実は曖昧で、明確には定まっていません。例えば電卓を人工知能だというとあまり納得してもらえないかもしれません。確かに、単にインプットした数値列を演算処理して答えをアウトプットするような装置だと考えると、電卓は知能を持つとは言い難いです。しかし、囲碁や将棋ソフトが実際にすることも、このような単純な演算処理を大規模に行っているにすぎません。「ゲームソフトは人工知能だが電卓は人工知能ではない」という主張があるとして、その間のどこに人工知能とそれ以外の境界線（条件）があるのか明確ではなく、当事者である私にも分かりません。

緩やかに捉えれば、既に人工知能は身近なところに普及しています。迷惑メールのフィルタリング機能も、インターネット検索も人工知能と言えるでしょう。私は以前、季節の贈答用に味噌をかなりの数量、カード支払いで購入したのですが、クレジットカード会社に不正な買い物と判断され、カードを止められてしまった経験があります。カード会社のシステムが過去の購入履歴などから「この人はこんな買い物をする人じゃない」と判断したのでしょうか。これもひとつの人工知能ですが、その判断は間違っていたわけです。もしかすると、季節(お歳暮時期)的な情報が組み込まれていなかったのか……などと考えてしまいましたが、こうした点を改良することでより精度が高まっていくと思います。

精度の高い「数値」を与えることで大局観まで手に入れた人工知能

――先生の研究テーマは「思考型ゲームにおける高精度評価関数の設計及び人工知能の開発」ということですが、かみ砕いて教えていただけますか。

保木 邦仁 氏 ほき くにひと

2003 年　東北大学大学院 理科研究科 博士後期課程修了。
トロント大学の研究員時代にチェスのコンピュータソフトに関する論文を読み興味を持ち、趣味で将棋ソフトの開発を開始。
2005 年　将棋についてはまったくの素人ながら、チェスのソフトで採用されていた「力づく探索」に加え「機械学習」などを採用し、「Bonanza」を完成。
2006 年　「第 16 回世界コンピュータ将棋選手権」で初出場にして優勝。その実力はプロに迫ると評価を受ける。2009 年のオープンソース化後、Bonanza をベースとした将棋ソフトが続々と登場。
2010 年　8 月より電気通信大学 先端領域教育研究センター 特任助教。
2015 年　4 月より電気通信大学 情報理工学研究科 准教授。
現在の研究テーマは「思考型ゲームにおける高精度評価関数の設計及び人工知能の開発」。

保木　ゲームという枠組みの中で知能を人工的に作ることに挑戦しています。ゲームには、常に何らかのルールがあり、プレイヤーの選択肢も限定されていますし、なんと言っても明確な勝敗があります。「知能」というもの自体がそもそも曖昧でよく分かっていない中、精度の高い人工知能を作る研究としては、うってつけの題材と言えます。

その精度を左右するのが「評価関数」です。コンピュータで計算できるのは数字なので、とにかくあらゆるものを「数値化」するんですね。曖昧なものもどうにかして数値に置き換えていきます。例えば、将棋や囲碁の手でも「気持ちがいい」「バランスがいい」「上手にさばけている」など、手や局面を形容する表現がいろいろとあるのですが、こうした有利不利の感覚を数値化していきます。この精度が高ければ高いほど、コンピュータがあたかもプロ棋士のように判断できるようになります。感覚の数値化に成功した例として、囲碁のコンピュータソフトで次に打てる碁石の良し悪しを数値化したものがあり、この数値が囲碁の達人の評価（感覚）と極めて似ているそうです。先日プロ棋士に勝利し話題となった「アルファ碁」が、それまでの人

巻頭特集

インタビュー ｜ 電気通信大学 准教授　保木 邦仁 氏

工知能にはなかった“大局観”を有しているとされるのも、この数値の精度を追求したことで実現したと思われます。

――「人工知能」が、人間ならではとされてきた“大局観”のような高次の判断ができるようになり、人間の仕事が奪われてしまうのでは、という懸念もあるようですが……。

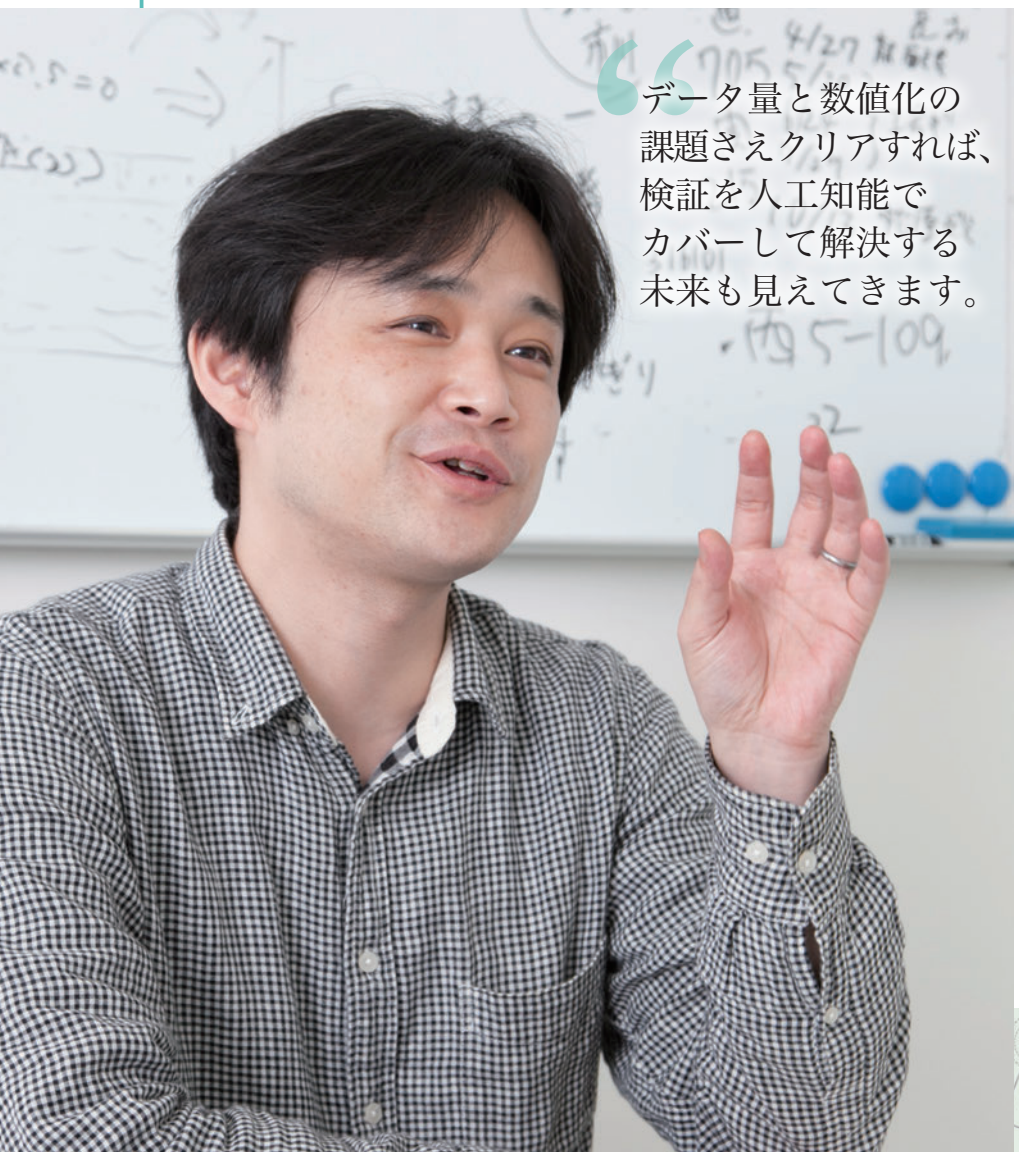
保木　最近の人工知能や機械学習の性能の高さは、やはり限定的な分野での成功と言えると思います。勝敗が明確ではない、例えばコメディアンのような曖昧なジャンルや、なんでも汎用的に対応できるもの、新しいものを生み出すといったことを人工知能に担わせるには、まだ相当時間がかかるのではないかというのが私の見解です。かなり遠い将来には、コンピュータでほとんどすべての仕事ができるようになってしまうかもしれませんが、一方で新しい仕事も生まれるでしょう。今まで以上に情報がスピード感をもって拡散していくので、仕事はもっと大変になるのではないでしょうか。人工知能をうまく利用しながら、ライバルと競うようになるのではと予測しています。

人工知能でヒューマンエラーを防ぐことは可能か

―― 人間ならではの弱み、マイナス面として「うっかりミスや見落とし」などのヒューマンエラーが挙げられます。現在のシステムでは「人間はミスをする」前提で設計（フールプルーフ）されているものの、トラブルはゼロになりません。ここを人工知能でカバーすることは可能でしょうか？

保木　以前、株式売買のシステムにおいて入力ミスによる誤発注の事件がありましたよね。このときは入力内容がおかしいという警告が画面に表示されていたにも関わらず、習慣から無視してしまった結果、大問題となりました。警告やアラート表示をよく見ずに「OK」「OK」と進んでしまうことは、私もよくあります。これを人工知能で検知して、本当に問題があるときにそれまで見たこともないような警告を出すことができたら、システムとしてより品質が高まったといえるでしょう。

ただ、機械学習は判断のベースとなるデータを以前よりも大量に扱えるようになってはきましたが、いまだレアケースに対応しづらいという課題が残っています。例えば、自動車の運転で「（高速道路などでの）逆走は危険」ということを学習させるのは大変難しいそうです。そもそも逆走しているケースのデータがほとんどないためです。システムの品質向上を図る上でも、極めてレアなケースのデータをどう集め、どう覚えさせていくかが鍵になると思います。



また、人工知能も判断ミスの可能性があることを忘れてはいけません。人工知能には２つのアプローチがあります。ひとつは数学的証明により段階を踏んで判断を下す方法、もうひとつは確率的に判断していく方法で、現在は後者のアプローチで大きな成果が出ています。しかし、確率をベースとした時点で、100%正しい答えを求めることを放棄していると言えます。つまり、「もっともらしければそれでいい」ということ。迷惑メールフィルタリングもそのメールが100%スパムメールだという確信はもてませんし、実際に大切なメールが迷惑メールフォルダに入っているケースもあります。こういったミス・間違いは、精度を高くすることで減っていくとは思いますが、確率的なアプローチをとる限り、絶対に間違えないシステムはあり得ません。そこで、ミスを減らす方法のひとつとして、複数の人工知能がそれぞれ別の視点でチェックするアプローチがあります。人間の作業でも複数人でチェックした方がミスを見つける確率が高くなるのと同じ考え方です。

データ蓄積、数値化の課題をクリアすれば、すでに実現の仕組みは揃っている

――システム検証における最近の傾向として、「大規模化／複雑化」「要件事項の曖昧さ（ユーザビリティなど）」「網羅性の難しさ」といったことが品質向上に向けたハードルとなっています。これらの課題を人工知能で解決し、システム検証をすべて行うことも現実的に可能でしょうか？

保木　システム検証を行う人工知能を作り出すとしても、現時点で成功している人工知能・機械学習のような、膨大なデータを処理するというアプローチは共通です。こういう場合は品質が悪い、良いというデータを数多く集めていくことで、いつの間にかできるようになっている可能性は十分にあると思います。システム規模が大きくなりすぎると全体を把握できなくなる、網羅的にチェックできなくなるという問題は、それこそ大規模なシステムの情報をひとつの人工知能にまとめてインプットすることで、全体の整合性をチェックすることは実現可能だと思います。

ユーザビリティや使い勝手は人によって捉え方が異なるもので、認識のズレが問題になるのも分かります。しかし、曖昧なものの数値化は機械学習・人工知能の基本です。将棋・囲碁の手の評価でも実現したように、ここを数値化してしまえば、ユーザビリティや使い勝手といった曖昧なものでも判定する仕組みは既に確立されています。

どちらにしても、判断の基準となるシステム検証／品質の“良し悪し”のデータを一定以上の規模で貯めることが必須です。判断の根拠となるデータ・事例が少なすぎると、今の枠組みではうまくいきません。仕組みや技術が揃った今こそ、データ処理の枠組みにどう乗せるのか、品質管理のためのデータをどうやって用意するのか、処理するのかを考えるタイミングなのではないでしょうか。データ量と数値化という２つの課題さえクリアできれば、システム検証やテストなどをひとつの人工知能でカバーして解決する未来も十分見えてきます。

問題はレアケースのデータをいかに短期間で貯めるかだと思います。この点については、人工知能がシステムを全体的にチェックし、人間がレアケースに注力して対応するという役割分担で、当面の品質向上につなげていけるのではないでしょうか。

――最後に、先生の今後の抱負についてぜひお聞かせください。

保木　僕自身としては、ビデオゲームやオンラインゲームなどより現実世界の競争に近いゲームをプレイする人工知能を作りたいと考えています。それが現実の経済や社会に大きな影響を与えられたらいいですね。

「コンピュータには無理」と思われていたことがここ数年で実際にできるようになり、新たな可能性が拡がっています。そんな時代にいるのは研究者としてとても幸運なこと。この幸運を活かし新しいことにどんどんチャレンジしていきたいと思います。

弁護士
波多江 崇 氏

ロボット法と自動運転について

今や、ロボットや AI に関するニュースに触れない日はありません。本稿では、今後ますます普及していくロボットに、どのような新しい問題が想定されるのかについて、主に自動運転を題材にしながら、現在の議論状況を紹介します。本稿中の意見や見解は筆者の私見です。予めご了承ください。

1. はじめに

2016 年 4 月 28 日、Google の CEO である Sundar Pichai は、「We will move from mobile first to an AI first world.」と述べ、今後、人工知能（AI）の重要性が高まることを踏まえ、Google としても AI に大きなウェイトを置いていくことを宣言した。

製造業においてはもちろん、医療や介護等の分野でもロボットが導入されて既に長いが、ここ 1–2 年のロボットや AI の浸透には目を見張るものがある。ある整理によれば、ロボットの普及ステージは、1960 年以降の産業用ロボット導入時期、1980 年以降の自動車業界への産業用ロボットの定着時期、1990 年代半ば以降の準備期（インターネットの時代）を経て、2010 年代以降の現在、爆発的普及期に入ったとされる。ロボットや AI の普及は、既に止められないところまで来ている。

現時点では一義的なロボットの定義は存在しない。したがって、例えばドローンと自動走行車がロボットと呼べるかについては賛否があり得る。しかし、ドローンと自動走行車、IoT（Internet of Things）や AI、あるいはこれらの組み合わせの延長線上のどこかに、ロボットであることにつき衆目の一致するテクノロジーを位置づけられることはかなり確かだろう。

波多江 崇 氏
はたえ　たかし

2003 年 京都大学法学部卒業。
2006 年 弁護士登録。
2014 年 ペンシルバニア大学ロースクール卒業（LL.M.）。
2015 年 CIPP/US（Certified Information Privacy Professional）登録。
2014 年 モルガン・ルイス&バッキアス法律事務所（米国）勤務
2015 年 TMI 総合法律事務所復帰。

2. ロボット法・総論

(1) これからのロボットの本質的要素

インターネットを定義づけるのが容易ではないように、ロボットを明確に定義づけるのは少なくとも現時点では難しい。従来は、センサー、知能・制御系、駆動系（Sense-Think-Act）の三要素を備えた機械と捉えられることが多かったが、これからのロボットは自律性を有しネットワーク化されていることが前提と理解されていることが多いようだ[1]。また、一般にロボットと関連する技術分野が多岐にわたることも整理を難しくしているといえる[2]。ここでは、インターネットを含むこれまでのテクノロジーと異なるロボットの本質を、3 点にまとめた Ryan Calo 教授の整理を紹介したい[3]（表1）。

Embodiment は、物理的な存在、フィジカルな存在、触れられるという意味であり、この点に関する異論はないだろう。法的な観点からは、ロボットにより身体や財産が物理的な損害を受ける可能性があるという点が重要ということになる。自動運転車も当然例外では

Embodiment	**身体性** （物理的存在、実在化）
Emergence	**創発性** （予測できないこと、不規則性）
Social Valence	**社会誘発性** （人間に感情を呼び起こすもの、社会的存在）

表 1：ロボットの本質（Ryan Calo 教授による整理）

ない。ロボットがネットワーク化していることを前提とすると、通信によってやりとりされる情報が物理的な損害を与え得る、あるいは、電気信号であるデータと物理的なアクションが非常に密接な関係を持つようになる、という点がこれからのロボットの特徴だといえるだろう。インターネットに避け難く伴う問題は、表現行為等による名誉棄損やプライバシー侵害、ヘイトスピーチ等、あるいは、著作権等の知的財産権の侵害だったが、ロボットに伴う問題としてまず挙げるべきは、事故や故障によるけがや財産権の物理的侵害といった安全面に関するものだというべきだろう。これは、インターネットが電気信号等を通じた情報の流通に過ぎず、基本的に物理的な存在ではなかったことと対照的である。

Emergenceは、和訳が難しいが、「予測できない」「創発的」という日本語をあてたい。[4]「予想外の成果もミスも伴う」と言ってもいいだろう。これは、法的な観点からは、今後のロボットを考えるうえで最も重要な特徴だといえる。なぜならば、生じた不幸な結果に対する責任の分配・帰属に関して、①誰が、②どのような根拠で責任を負うのかという問題に、根本的な変更をもたらしかねないからだ。これは、言い換えると、ロボットの Emergence は、人間の予見可能性、すなわち過失や故意の責任の認定あるいはその判断構造自体に大きな影響を与え得るということだ。

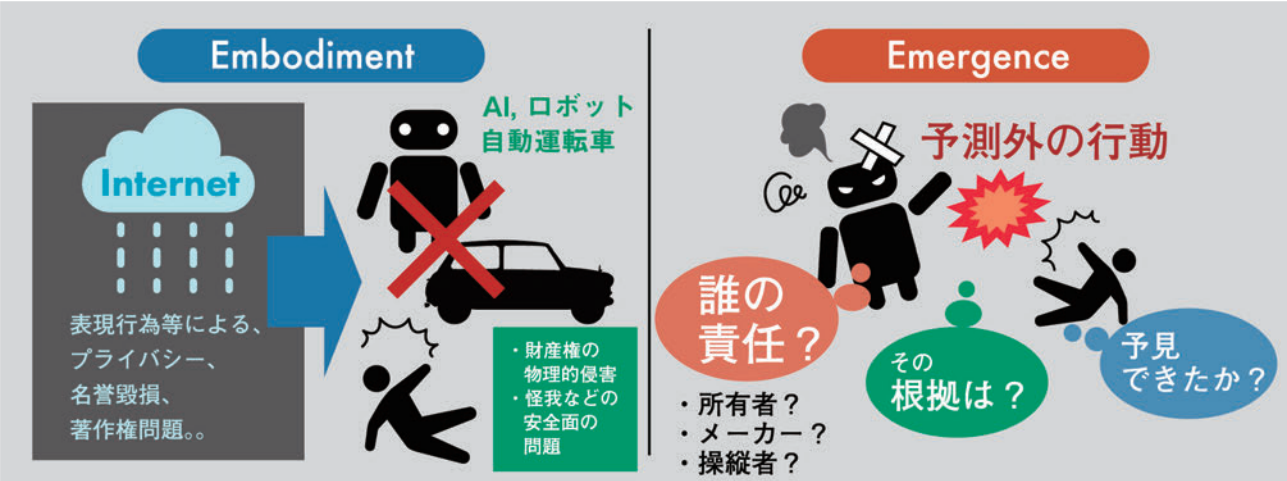
---

1. 経産省（ロボット革命実現会議）の取りまとめた、ロボット新戦略（2015年1月23日）においても、ロボットの「情報端末化」と「ネットワーク化」が指摘されている。（http://www.meti.go.jp/press/2014/01/20150123004/20150123004b.pdf）

2. 例えば、AI、ジェスチャー認識技術、感情認識技術、augmented reality（拡張現実）といった技術がロボットのコア技術として挙げられる。

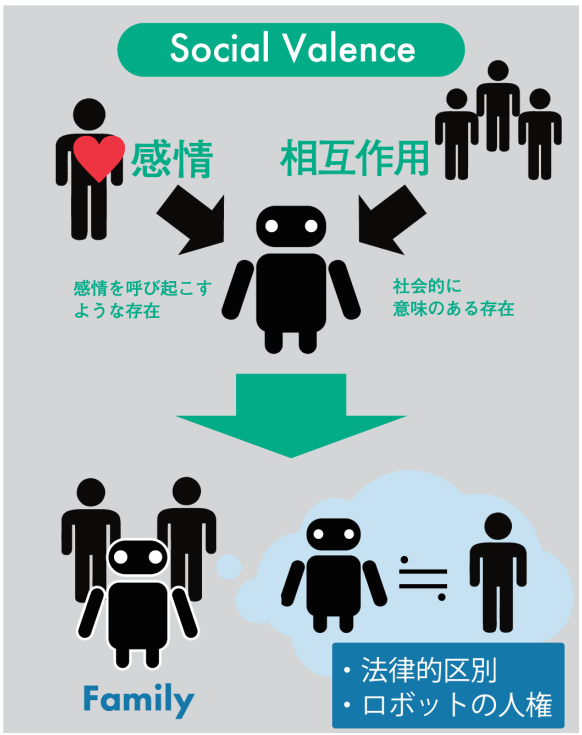
3. Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 CAL. L. REV. 513 (2015)

4. これは、内容的には、いわゆる「自律性を有する」に近いと思われるが、Calo 教授によれば、あえて自律的（autonomous）という語は用いなかったという。その理由は、自律的という語は、情緒的に過ぎ、ロボットが何らかの意図をもって意思決定するような、過度に人間味のある存在と捉えられてしまうためだとのことである。この背景には、自動学習や意思決定をつかさどるアルゴリズムは、その構造自体シンプルなものであって、ロボットの行う学習は、そのような比較的シンプルなアルゴリズムの適用を無数に繰り返すものだという理解があると思われる。Calo 教授のこの指摘は、「近い将来におけるロボット」を論じるうえで重要な視点を提供している。



ロボット法と自動運転について

弁護士　波多江 崇 氏



最後に、Social Valenceは、人間に何らかの感情を呼び起こすような性質、あるいは、社会的に意味のある存在といった意味である。恋愛対象とするための種々のロボットが生まれるのは間違いないだろうし、米国の研究論文では、Wingmanとしての機能を有するロボットとプライバシーの問題が論じられている[5]。特定の病気に罹患している子どもとロボットの相性が良いことも分かってきており、AIBOのような愛玩用のロボットのみならず、ドッグセラピーのような医療行為に近い働きをするロボットも多数生まれるだろう。要するに、ロボットは、EmbodimentやEmergenceという特質とあいまって、人の心や感情に深く触れるものになるのであり、その結果、私たちの日常生活や仕事、人間関係に大きな影響を与えていくことは間違いない。この点に関する法的な意味合いを分析することは難しいが、ロボット利用者の感情や心情に着目する必要性が高まってくる可能性、家族のあり方に大きな変更を強いる可能性、人とモノを厳然と区別する法律の考え方に揺らぎが出る可能性[6]や、さらにはロボットの人権（あるいはそれに対する人間の人権の再考）といった議論が生じる可能性がある。

（2）基本理念 ～ ロボットへの向き合い方

ロボットに関する基本理念としては、アイザック・アシモフのロボット工学三原則（1950年）[7]が引き合いに出されることが多い。これは、ロボットかくあるべしという基本的事項を宣言するもので、ロボットと法を論じるにあたっては、このような、人間がロボットにどのように向き合うべきかという基本理念の議論も必要だと思われる。

この点に関し、2015年10月11日のロボット法学会設立準備会において、新保史生教授が、ロボット法新8原則（試案）[8]を公表され、話題を呼んだ。また、総務省のAIネットワーク化検討会議は、AIに関する研究開発の原則として、類似の8原則を提示している[9][10]。

おそらく重要なことは、人間第一の原則はもちろんのこととして、多様な価値を生み出すロボットの発展と普及は避け難いという事実を前提に、①イノベーションを促進すべきこと、そして、②ロボットによる考え得る弊害を整理し、ルールを明確化していくことだと考える。①に関しては、関連技術分野の発展の支援のみならず、利用者・消費者が何を求めているかをよく知ること、あるいは、ロボットのアプリケーションすなわち活用法についてビジネス／研究サイドがリードしていくことが必要だ。これに際しては、意味のある失敗を成功と等しく歓迎する文化や、過度な政府の介入を避けることも必要だろう。②に関しては、既に述べた安全性に加え、プライバシー／サイバーセキュリティの2点が最も留意すべき重要な反対利益だと思わるが、3（3）で述べる責任の分配について明確なルールを策定することも重要だ。権利侵害を救済／未然に防止し、紛争に関するルール作りをするという意味で、ロボット法が必要なのは、一義的には①に関してだといえる。

（3）ロボットと倫理問題

多くの新しいテクノロジーがそうであるように、ロボットには倫理の問題が関わる。ロボットと倫理に関しては、議論がきわめて多岐にわたっており、筆者が認識する限りでも表2に記載したような議論がある。倫理の問題は、価値又は価値観の選択の問題であり、広く議論が必要な、困難な問題だといえる。本稿では、次項で自動運

自律型致死兵器システム（ロボットを含む）の軍事的使用の是非[11]
トロッコ問題／緊急避難プログラム（後述）
AIとシンギュラリティ
利用者のプライバシー
遠隔操作ロボットと不適切な「オズの魔法使い」的使用（あるいは「チューリング詐欺」）[12]
ロボットへの愛着又は依存（特に治療行為を行うロボットに関して）[13]
人型ロボットの外見とダイバーシティ（人種や性別、民族性等）
ロボットの性的な利用の是非
サイボーグ（人間と機械の融合）

表2：ロボットと倫理に関する議論

5. Wingmanとは、異性と親しくなりたいと考えている友人を助ける恋のキューピッドのような役割のことを指す俗語である。Jason Millar, Sketching an Ethics Evaluation Tool for Robot Design and Governance(draft; 2015)

6. いずれは、人間とロボットの融合体であるサイボーグが登場し、新しい問題を呈するだろう。コンピュータやRFIDによって構成される医療機器等の人体への組み込みや、義手や義足のIT化（例えば、パワードスーツのような製品）は既に始まっている。

7. アイザック・アシモフのロボット工学の三原則は、以下のとおり。
①ロボットは人間に危害を加えてはならない。また、その危険を看過することによって、人間に危害を及ぼしてはならない。
②ロボットは人間から与えられた命令に服従しなければならない。ただし、命令が第1条に反する場合は除く。
③ロボットは、第1条及び第2条に反するおそれのない限り、自己を守らなければならない。

8. ①人間第一の原則、②命令服従の原則、③秘密保持の原則、④利用制限の原則、⑤安全保護の原則、⑥公開・透明性の原則、⑦個人参加の原則、⑧責任の原則であり、参考になる。（http://robotlaw.jp/wp-content/uploads/2015/10/20151011robotlaw_shimpo.pdf）OECDのプライバシー8原則を参考にしているとのことであり、安全性よりもプライバシーの問題を重視しているとも読める。

9. ①透明性の原則、②利用者支援の原則、③制御可能性の原則、④セキュリティ確保の原則、⑤安全保護の原則、⑥プライバシー保護の原則、⑦倫理の原則⑧アカウンタビリティの原則である。①から⑧のそれぞれが非常に深い示唆を持つ（http://www.soumu.go.jp/main_content/000414975.pdf）。

10. 6月6日には、人工知能学会が、AI研究に関する倫理指針の素案をまとめた。基本的人権を守り、開発・運用の際には人類の安全に及ぼす脅威を排除すること、新たな不公平や格差をもたらす可能性を認識し、人類が公平、平等に人工知能を利用できるように最善を尽くすこと、可能性と限界について社会全般を啓蒙すること、他者に危害を加える意図で利用しないこと、他者のプライバシーを尊重し、取得した個人情報は内密に扱われなければならないこと等が盛り込まれており、参考になる。

11. 国連のCCW（Convention on Certain Conventional Weapons（特定通常兵器使用禁止制限条約））の枠組みの中では、LAWS(Lethal Autonomous Weapon Systems（自律型致死兵器システム））の使用に関する議論が活発に行われている。ロボットに関する議論は、兵器に関して最も進んでいるといえるだろう。Killer Robot（殺人ロボット）の完全廃止を求める声も日に日に強まっている。これらの議論は形式的には国際法（具体的には1949年ジュネーブ諸条約の国際的な武力紛争の犠牲者の保護に関する追加議定書（議定書）の第36条）の議論だが、基本は倫理的な問題だといえる。

12. オズの魔法使い的使用とは、人間がロボットを（遠隔）操作しているにもかかわらず、それを秘匿する方法で使用することをいう。チューリング詐欺も、同様の意味であり、機械が人間と同等に知的であるかどうかを判定するためのチューリングテストに由来する名称である。オズの魔法使い的な使用はどのような場合に許されるのか、どの時点でどのような情報をロボット利用者に通知すべきか、オプトアウトは可能か、といった議論が既に存在する。

13. ロボットを用いた治療又は準治療行為（主に精神疾患や発育障害等への対応）の終了に伴う、いわば「ロボットロス」による利用患者への悪影響の問題であり、まさに、Social Valenceの側面からくる問題だといえる。

ロボット法と自動運転について

弁護士　波多江 崇 氏

転に関係し得る点について述べ、その余の点は、簡潔な説明にとどめることとさせていただく。

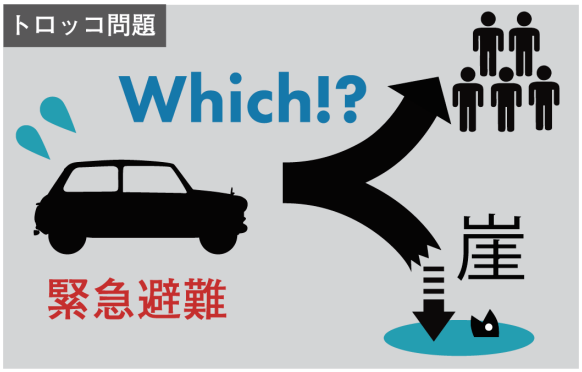
また、米国では、倫理的な面を重視して、人間とロボットの関係性や交流に関わる、エンジニア向け（すなわちロボットの設計に関する）基本倫理規範が提案されている。例えば、法的な観点からは、現行の関連法規の尊重、後の訴訟紛争における事後検証に備えてのロボットの意思決定プロセスの記録、利用者のインフォームドコンセントの最大限の実現等を含んでおり、示唆に富んでいる（表3）。

3. 自動運転を巡る議論状況

自動運転が提示する具体的な法律問題にはどのようなものがあるだろうか。以下では現在議論されている、あるいは想定され得る問題を簡単に取り上げる。ただし、本稿では、個別の問題点につき結論を追求するものではない。

(1) トロッコ問題

トロッコ問題とは、倫理学における思考実験の一つで、例えば、制御不能になったトロッコの先に、５人の人間がいて、このままではその５人が轢き殺されてしまう、ポイントを切り替えて別の線路に入れば、その５人は確実に助かるが、別の線路の先にいる1人が轢き殺されてしまう、という状況で、ポイントを切り替えるべきかどうか、といった内容のものだ。これを自動運転車にあてはめると、例えば、急に目の前の道路が陥没してしまったため、直進すると搭乗者が大けがをしてしまう、右にハンドルを切ると幼稚園児を轢いてしまう、左にハンドルを切ると80歳の老婦人を轢いてしまう、このとき自動運転をつかさどるプログラムはどのような判断をすべきか？という問題になる。急に目の前に小学生が飛び出してきたときはどうか？飛び出してきた小学生が３人だったらどうか？左は崖で左にハンドルを切ると搭乗者が確実に死亡してしまう場合はどうか？など、バリエーションは無限にある。



これはあくまで倫理学における思考実験であるため、このような場面が実際に起こる可能性は低いと思われる（特にエンジニアの方からはそのような発言がなされることが多いように思われる。）が、自動運転と法を論じる際には必ずといってよいほど取り上げられているし、自動運転の普及を前にして私たちが議論をしておく必要がある事柄の１つだといえる。

人間の尊厳に関するもの	ロボットにより感情をみたすことの必要性への尊重
	プライバシーの権利の尊重
	人間の心身の「弱さ」の尊重
設計に関するもの	プログラミング内容の透明性・公開
	ロボットの言動の予測可能性
	あらゆる面における信頼性の高い設計
	ロボットの現在の状態に関する情報のリアルタイムでの提供
	Kill Switch（人間がいつでも電源を切れる）
社会的な要素に関するもの	慎重な「オズの魔法使い」的使用（「チューリング詐欺」の防止）
	人型ロボットへの愛着が生じることへの配慮
	ロボットの形態と機能が目的達成のために必要範囲にとどまること
	人種、性別、健常者か否かによる差別の禁止

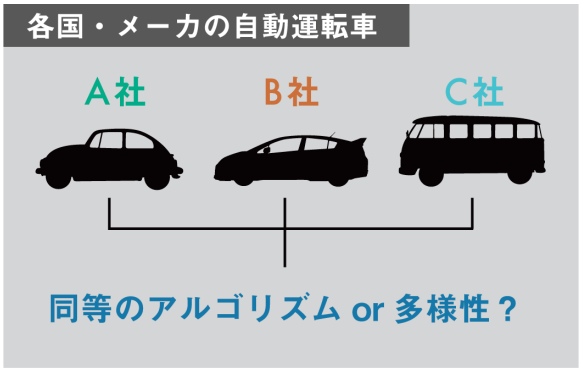
表3：Laurel D. Riek, Don Howard, A Code of Ethics for the Human-Robot Interaction Profession (2014)。
感情や愛着といった心の問題にも配慮している点で興味深いものになっている。

仮に人間が運転しているとした場合における上に述べたような「究極の選択」の場面は、刑法における緊急避難[14]と呼ばれるルールが適用される場面に非常に近い。現行の法律は、「これによって生じた害が避けようとした害の程度を超えなかった場合に限り」とされていることから、損害の大小によって人の行動を律しようとしていることが読み取れる。自動運転を支配するアルゴリズムは、このような損害の大小により自動車をコントロールするようにプログラムされるべきだろうか。またそもそもそのような損害の大小の予測や認知は技術的に可能だろうか。

思考の実験とそれにまつわる疑問には終わりがないが、自動運転の文脈でトロッコ問題を考えたときに、いくつかいえることはありそうだ。

まず、速度を落とすことの重要性である。自動運転車に関しては、法定速度を厳格に守り過ぎると追突事故が増えるなどしてかえって危険ではないか（つまり現実の世界では法定速度を守らなくてもよい実態がある）、自動運転車専用の道路又はレーンを作るべきではないか、などといった議論もなされているが、やはり確実に停止できるよう法定速度を保守的に設定することの重要性が感じられる。これは、速度を人間の対処できる範囲内にとどめることの重要性、という言い方もできるかもしれない。

次に、搭乗者の安全は優先せざるを得ないだろうということである。そうでなければ、消費者は、自動運転車に乗りたいと思わないし、そうなると自動運転車は普及しない。自動運転車には、一般論として「事故が起きにくくなる」「渋滞が減る」「燃費が良くなる」というメリットがあることは間違いないため、社会全体の厚生を考えたときに、自動運転車が普及できるような考え方やルールが必要だろう。



さらに、各社の自動運転車全てにおいて、ほぼ同等のプログラムがなされる必要があるかという問題がある。[15] メーカーや車種によって、あるいは自動車オーナーの設定によって、さらには国や地域によって、自動運転車の動きをつかさどるアルゴリズム（例えば上に述べたトロッコ問題の場面における一定の価値の選択）が大きく異なるというのは、予測可能性の観点から、ひいては自動運転車の普及の観点からも、望ましいことではないという立場もあるだろうし、製品としての多様性を認めた上で「価値の選択」は消費者に委ねるべきだとの立場もあるだろう。

（2）人間がコントロールする余地

2016 年 2 月 4 日、米国運輸省の国家道路交通安全局（National Highway Traffic Safety Administration; NHTSA）が、Google に対し、一般の自動車に必要な機能や仕様について定める安全規則の解釈上、一般論として、自動運転システムつまり AI がドライバーとみなすことができると公式に回答したことで話題になった。

この回答は、米国政府が、運転者を 1 人も乗せない「完全自動運転車」の公道走行を認めるか否かに関する規則の解釈を主題とするものに過ぎず、（3）で述べる事故等の際の法的な責任について何らの指針を示すものではない。また、結論として、完全自動運転車の公道走行は現行法令上まだ許されないことが確認されている。その意味では、このニュースのインパクトはさほど大きくならなかったこともうなずける。

しかし、Google と NHTSA の間のこのやり取りの中には、人間とテクノロジーの関係に関する興味深い議論が含まれている。[16] すなわち、Google が、自動車製造業者に適用される安全規則に関して、「ハンドルやブレー

14. 刑法 37 条 1 項「自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。」

15. この点は、小林正啓弁護士が提唱されている。(http://hanamizukilaw.cocolog-nifty.com/blog/2015/11/post-cfa8.html)

16. この点については、拙稿も参照。（https://wirelesswire.jp/2016/03/51254/、https://wirelesswire.jp/2016/03/51258/）

ロボット法と自動運転について

弁護士　波多江 崇 氏

キペダル（といった人間による操作器具）は必要ない」と主張していたのに対し、NHTSA は、「ブレーキペダル、ハンドル、その他の搭乗者による操作ツールが本当に不要か？これらを不要とした場合に本当に安全の面でリスクがないか？」につき、再検討するよう示唆した。この点に関し、Google と NHTSA の立場は大きく異なっていることが明らかになった。対照的に、TESLA は、現状のところ、ハンドルとブレーキペダルが設置され、そして運転者が運転席に座ることを想定した自動運転プログラムを進めているようだ。

完全自動運転車には、ブレーキペダルやハンドルの設置を義務づけるべきだろうか？例えば、ロボットに関する議論の中で、「Kill Switch」すなわち、いつでもロボットの電源を切れるような仕様を義務付けるべきではないかとの議論がある（表 3 を参照）。これは、予想外の動きまたは何らかのトラブルによってロボットが人間に対して害悪を行う万一の場合を想定してのことだと考えられる。自動運転車にブレーキペダルやハンドルを残すべきか否かは、これに似た問題だ。つまり、これは、人間が AI やロボットをどこまで信頼するか、あるいは、どの程度脅威とみるかという、人間とテクノロジーの基本的な関係性を論じる普遍的なものだといってよいだろう。この点については、個々人により、考え方が大きく違う可能性があり、議論を要する問題だといえる。上に述べた、命令服従の原則(脚注 8) 制御可能性の原則(脚注 9) も同じ問題意識に立つものだと考えられる。

(3) 法的な責任

2016 年 4 月 1 日に開催された We Robot2016[17] では、2013 年のアンケートの結果として、学会参加者の最も関心の高いロボットと法に関する問題が、ロボットによる問題行動があった場合の法的責任の所在と考え方であることが示された。[18] 最後に、自動運転に関する法的な責任について、みてみよう。

2016 年 4 月 7 日、警察庁は、自動走行の制度的課題等に関する調査研究報告書を公表した。[19] そこでは、今後の自動運転走行実験及び最終的な自動運転車の普及を見据え、法律上・運用上の課題が整理されているほか、公道実証事件のためのガイドライン案が示されている。これは、日本における自動運転車の普及の準備として重要な一つのステップだといえるが、法的な責任については、いわゆるレベル 3 までの自動運転では、民事・刑事上の責任に関しては、現状のとおり故意または過失が判断されることになることが説明されているほかは、被害者の立証の困難性・補償の遅れの危険に言及されている程度で、自動運転車によって生じる法的な責任に関する新たな問題については、具体的な方向性が示されていない。

このように、自動運転車が事故を起こした際の法的責任については、まだ大きな方向性すら定まっていない状況である。

例えば、ハンドルやブレーキペダルのない完全自動運転車が、停止した状態から、ウインカーを点滅させ、左車線に移動しようとした際、左後方から人間の運転によるバスが接近していたが、完全自動運転車の AI が、このバスの速度が若干落ちたために道を譲ってくれると誤って判断して左車線に入ったところ、後ろから直進してきたそのバスと接触してしまった、という事例を考える。[20]

---

17. 米国で 2012 年から開催されている、ロボットと法·政策、倫理、心理学、エンジニアリング等に関する学際的な学会。

18. http://robots.law.miami.edu/2016/wp-content/uploads/2015/07/Smart-robots-law.pdf

19. https://www.npa.go.jp/koutsuu/kikaku/jidosoko/kentoiinkai/report/honbun.pdf

20. これは、2016 年 2 月 14 日に、Google の自動運転車が関与した実際の事故の事例をもとにしている。

この事故が、人間の運転する自動車どうしの事故だった場合には、ケースにもよるが、直進していたバスよりも車線変更をした自動車の方に過失があると判断される可能性が高いだろう。それでは、このケースで、バスに生じた損害は、誰が賠償する責任を負うだろうか。ハンドルやブレーキペダルがない、つまり、自動車を停止させる手段を持たない自動運転車の搭乗者に責任を負わせることは難しいだろう。法は不可能を強いることはできないからだ。それでは自動車の所有者はどうか。この場合、現行法下では、「過失」原理に基づく損害賠償責任を導くことは非常に難しいと思われる。[21] AI の判断が結果的に誤りをおかし、それによって損害が生じることを予見したり、その結果を回避したりすることを所有者に求めることが難しいからだ。では自動車メーカーはどうか。また、自動車メーカーは、このケースで誤った判断をしたと思われる AI のプログラムの製造・供給者に対して責任を追及できるか。その場合、AI の欠陥や瑕疵の有無はどのように判断されるべきか。完全自動運転車の所有者は、自賠責保険が使えるか。[22] 完全自動運転車どうしの事故だった場合、過失相殺はどのように判断されるべきか。

これらは、上で述べた Embodiment と Emergence に関わる新しい問題だといえる。AI は、いかに精緻にプログラムしたとしても、予測し得ない判断や行動を行うことがどうしても避けられない。この点に関しては、そもそも現行の法体系内で対応すべきか、それとも新たな法令が必要か、といったそもそもの点から見解の相違がある。以上の議論状況から、AI プログラムの検証やアップデートの重要性が今後増すことは間違いないだろう。

(4)プライバシー/個人情報/サイバーセキュリティ

法的責任の分配のほかに自動運転に関して重要な分野としては、プライバシー又は個人情報の保護、そしてセキュリティの問題がある。自動運転車は、常に、膨大な量の情報を取得、処理する。これらの情報の中には、位置情報をはじめとして、特に他人には知られたくない情報が含まれるだろう。自動運転車の普及を妨げない方法で、どのように個人情報の取得につき同意を得たり、利用目的の通知をしたりできるか。ロボットやそのオペレーションシステムの開発事業者に対し、設計や表示に関し、どの程度のセキュリティ上の措置を義務づけられるか。この点については、基本的に現在の法規制の枠組みの延長線上で議論できそうだが、個別の問題への対処にはまだまだ議論が必要だ。

4. 最後に

ロボット法、あるいは自動運転と法を考えるということは、テクノロジーの活用に関する利用者のメリットや社会全体の福祉と、その他の反対利益・デメリットについて、適切なバランスを模索していくということだと考えることができる。このプロセスにおいて、極力、イノベーションを阻害してはならないというのが筆者の意見である。このことは、政府が過剰な介入をして、関連技術の開発者間の競争を不当に制限してはならないと言い換えることもできる。

また、冒頭の Pichai 氏の言葉に象徴されるとおり、ハードウェアに比べ、AI あるいはソフトウェアの重要性は、今後さらに増していくことが確実だ。そして、本稿で示した問題に対する答えあるいは答えに対するヒントは、ソフトウェア／アルゴリズム開発の現場、又は自動運転車等「実物」の運用の現場に最も多く存在すると考えられる。現在のようなロボット・AI の草創期においては、そのような現場の情報を踏まえた議論をすることが特に重要だと考える。

最後に、忘れてはならないことは、テクノロジーは常に変わり続けるということだ。世界を変えたインターネットも、今もなお変化を続けている。ロボットや自動運転技術に関しても、長い目で見て、変化を受け入れていくことが必要だと考える。

---

21. 過失に基づく損害賠償責任によっては責任を基礎づけられない場合、特殊な法理によって補償を導くことが考えられる。例えば、危険な動物によって生じた損害についてその管理の懈怠等をもとに飼主等の責任を認める民法 718 条を類推することが考えられるが、どのような場合に管理の懈怠等を認めるのかという問題が残る。また、危険な建物・工作物についてその設置又は保存の瑕疵に基づいて責任を負わせる民法 717 条の類推も考えられるが、やはり何をもって AI の設置又は保存の瑕疵といえるのかという問題は非常に難しい問題だ。

22. 自動運転車の事故に関して、保険が重要な役割を果たすことは多く指摘されている。この点に関しては、将来、抜本的な法改正が必要となる可能性がある。

特集2

ソフトウェアやシステムの開発や品質向上や効率化に貢献する

製品やサービスが高度化、複雑化する中で、ソフトウェアやシステムの品質向上や開発の効率化、さらにビジネスに結びつく付加価値への要求がますます高まっています。この要求に対して実証的ソフトウェア工学の観点から、ソフトウェアやシステムの開発において「コンテキスト」を理解することの重要性と有用性を説明します。

コンテキストとは

私は大学で実証的ソフトウェア工学 (Empirical Software Engineering) という研究分野を専門にしています。ソフトウェア工学と同様にソフトウェアの品質向上や開発の効率化を目指した技術や技法を構築したり、観察により現象の規則性や法則を解明したりすることを目的とした分野です。これに加えて実証的ソフトウェア工学では構築や解明の「コンテキスト (context)」を重視します。コンテキストは背景、環境、事情といった意味で使われます。コンテキストの辞書での定義は、文脈、前後関係です。実証的ソフトウェア工学では、技術や技法を実際の開発のコンテキストで利用したり、実際の開発を観察したりしてみて、技術や技法の効果や限界、規則性や法則を明らかにすることが推奨されています。その目的の一つは、コンテキストを含めて効果や限界を報告することにより、技術や技法が実務で利用されやすくすることにあります。

ソフトウェア開発の成功事例をそのまま別の場所でマネしてもうまくいかないときの理由の一つは、コンテキストが異なっているからです。本稿では、コンテキストを理解したり意識したりすることがソフトウェア開発一般においても有益であることを説明します[1]。普段から感じていらっしゃる方にはごく当たり前のことだと思いますが、意外と知られていません。研究を進める上で、ここ10年で400社を超える企業のソフトウェア技術者の方とお話をして私自身も感じています。

実証的ソフトウェア工学では、ソフトウェア開発の技術、技法とコンテキストの組み合わせを考慮しています。これにより、ある条件下ではうまくいくけれど、他の条件下ではうまくいかないことを客観的に説明できるようになります。技術や技法の知見を積上げるときに、単に「うまくいきました」ではなく「こういう条件下でうまくいきました」と表現できるようにすることで、より詳細な知見を積上げることができます。たとえば「状態遷移図に書く状態を網羅的に列挙できるような規模のソフトウェアではモデル検査が効果をもたらす」、「要素技術やビジネスが既知のものであり、開発中の要求の変更規模が小さい場合には PMBOK[2]

1　コンテキストを説明したご参考資料：「ソフトウェアテストシンポジウム北海道 2013」や「AgileTourOsaka2011」における講演資料。スライド公開サイト slideshare に掲載 (http://www.slideshare.net/smorisaki/)。

2　PMBOK「A Guide to the Project Management Body of Knowledge: プロジェクトマネジメント知識体系ガイド」で定義されている知識体系。ソフトウェア開発、建設をはじめとするプロジェクトを推進するプロジェクトマネジャ向けにプロジェクトマネジメントの基礎知識を体系化したもの。http://www.pmi.org/PMBOK-Guide-and-Standards.aspx。

森崎 修司 氏 もりさき　しゅうじ

2001年 奈良先端科学技術大学院大学 情報科学研究科博士後期課程修了
2001年より 通信事業者においてプロダクト企画、開発に責任者として従事
2005年より 文部科学省リーディングプロジェクト「e-society 基盤の統合開発」、経済産業省「先進社会基盤構築ソフトウェア開発事業」において、実証的ソフトウェア工学の研究に従事
2007年より 奈良先端科学技術大学院大学 情報科学研究科 助教、静岡大学 情報学部 助教、同学部 講師、同大学情報学研究科 准教授
2013年より 現職
ソフトウェア品質シンポジウム 2012～2016 企画委員会委員長をはじめ10 件の国内委員会の委員、及び、8 件の国際委員会の委員を務める。

検証においてコンテキスト理解

名古屋大学 情報科学研究科 准教授
森崎 修司 氏

に沿ったプロジェクトマネジメントが効果を発揮する」といった具合です。

ソフトウェアやシステムの役割もコンテキストの一つ

少し前のエンタープライズシステムにおけるITの役割は既存の手作業による事務処理をITで実現することでした。ITで実現すれば確実に低コストを実現できたからであり、そのときのソフトウェアやシステムの価値[3]は、既存の手続きや事務処理を忠実に実現することでした。しかし、そうした取り組みが一巡し、次の役割を担わなければならなくなりつつあります。組込みソフトウェアにおいても、メカ技術者、エレキ技術者から渡されたソフト仕様をそのとおりに実現していればよいという状況は変わりつつあります。

ソフトウェアやシステムがビジネスと密接に結びつき、新たなビジネス価値を生み出すことが求められつつあります。これまで取り組まれていた手続きや事務処理の忠実さや手作業の自動化といった正しさだけでなく、ソフトウェアやシステムの役割を見定めて、ビジネス価値を増すような提案をしていかなければならない時代になっています。ここでのソフトウェアやシステムの役割も先述のコンテキストに含まれています。つまり、あるコンテキストにおいてはソフトウェアやシステムのビジネス価値が高いが別のコンテキストではそうではなくなるということが起こる頻度も高まっています。

3　ここでの価値はプロジェクトや作業の出来高による進捗管理手法である EVM(Earned Value Management) で言及される価値ではなく、ソフトウェアやシステムがもたらすビジネス価値。

ソフトウェアやシステムのコンテキスト理解

コンテキストの理解が十分でないとソフトウェアやシステムをどのように作ればよいか、どういう点に注意して開発を進めればよいかといった点が不十分になる場合があります。理解が不十分な部分は、要求や検証のムラにつながります。たとえば、ソフトウェアやシステムから得られる価値によって、特に手厚く熟慮して要求を定義したり検証したりしないといけないユースケースとそうでないユースケースが生まれます。このように価値に応じて開発活動におけるコスト配分を変える考え方は Value-based Software Engineering[4] でも言及されています。

こうした価値が企画書、要求の背景、ソフトウェアやシステムの位置づけといった形で明示されていればわかりやすいのですが、多くのソフトウェアやシステムにおいては書かれていません。ただ単に、企画や要求を考える立場にある方が気づいているにも関わらず書いていないという場合もありますが、そもそも気づいてさえいないという場合もあります。つまり、価値は明示されておらず、要求定義書のテンプレートに「価値」の項目を加えるだけではコンテキストを明らかにすることは難しい場合もあるということです。

別の分野から新しい分野の職場へ異動、転職してきたばかりのときや新卒で初めてソフトウェアやシステムの開発に取り組んだときは、こうした明示されていない価値を感じる機会です。私はインターネットサー

4　Value-based Software Engineering：ソフトウェア工学が扱う対象に経済的価値を加味した考え方。Barry Boehm, Value-based Software Engineering. ACM SIGSOFT Software Engineering Notes, Vol.28, No.2 pp. 4(2003)

ソフトウェアやシステムの開発や検証において品質向上や効率化に貢献するコンテキスト理解

名古屋大学 情報科学研究科　准教授　森崎 修司 氏

ビスの開発にソフトウェア技術者として携わっていた時期があり、明示されていない価値を感じたことがあります。通信事業者としての責任や顧客からの期待といった暗黙的な要求があり、それにあわせて検証に濃淡があることを感じました。「この点が安心できるからこのサービスを買っていただけるので、その期待を裏切らないようにしてほしい」という当時の上司の言葉が頭に残っています。

レビューの効率化にもコンテキストがカギに

現在、私は要求、設計、コードレビューといったプロダクトレビューを研究対象の一つにしています。ここでも、ソフトウェアやシステムのコンテキストが明確でないと一定以上の効率化が難しいと感じています。これを効率化の段階を追いながら説明します。

レビューの安定実施をするための基礎段階では、次の３つが前提になります。①レビュー会議の際に話が横道に逸れたままにならない、②技術者同士で他の技術者に実力を認めさせるためのパフォーマンスの場にならない、③欠陥検出のペース配分のムラのせいで欠陥検出が途中で終わっていない、ことです。

次の段階としては、レビューの実施コストの配分の適正化が必要になり、次の２つが必要になります。①レビューアー全員が同じような着眼点で同じような箇所をチェックすることを避けている等、レビューアー間の重複が小さい、②テストで検出されると修正にかかるコストが大きくなる欠陥が優先的に検出できていて、テストでの修正コストが大きい欠陥から検出できている、ことです。

さらに高いレベルでの効率化を目指そうとすると全方位的な欠陥検出を諦めてソフトウェアやシステムのコンテキストを調べ、どのような価値があるかを明らかにして、価値の高い部分のレビューを優先して実施しなければなりません。

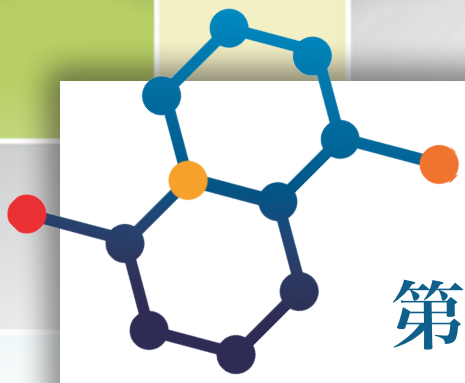
価値に応じてレビューのコスト配分ができている事例を調べたことがあります[5]ので、そのうちの一つを紹介します。自社とグループ会社向けにアカウント認証システムを開発、運用されているチームのレビューで特に重点化している部分をインタビューで伺いました。価値は三つあり、①正しいアカウント、パスワードで認証できること、②アカウント、パスワードの情報を漏洩しないこと、③認証リクエストが増える時期であってもスループットが極端に落ちないことです。これらの価値が提供できているかどうかをレビューで重点的に検証しているそうです。性能に関してはレビューだけでは確認が難しい部分もあるため、レビューとテストで役割分担をして、検証コストを適正配分しているそうです。簡単なように見えますが、価値を見極めなければ少数に絞り込むことができず、あれもこれもとなります。

価値やコンテキスト理解の重要性

ソフトウェアやシステムのコンテキストが明らかになっていないまま開発や検証が進められていることはまだまだたくさんあります。開発部門の管理職が部門間会議で聞いてきているにもかかわらず共有されていないといった初歩的なものもあります。その結果、開発部門の担当者、リーダー、管理職で考えが違うということも少なくありません。コンテキストを明らかにすることにより、こうした考えのズレを解消することにつながり、ソフトウェアやシステムのビジネス価値もさらに高まります。

実際には暗黙の価値を前提にしているにもかかわらず、「ウチの場合、ミッションクリティカルシステムだから濃淡はない。全網羅が前提である」「運用が始まっていないうちは何に価値があるかはわからない」といった考えで効率化ができていないことが多いのも事実です。改めて、コンテキストを理解することの重要性を、開発部門をはじめ多くの関係者に知っていただきたいと思います。

5　事例４件とコンテキストを考慮したレビューの手順を拙著「なぜ重大な問題を見逃すのか – 間違いだらけの設計レビュー 改訂版」（日経 BP 2015）で紹介しています。



「安全設計」を、原子力発電に例えて
分かりやすく解説するシリーズ

ベリサーブ
東 弘之

第５回：安全設計の概念

皆様こんにちは。安全設計の紹介の第５回になります。引き続き御付き合いいただければと思います。

◆コラムの流れ

前号のコラムでは、6. 原子力発電の安全設計についてお話ししました。今回は原子力発電から一旦離れ、7. 安全設計の概念を紹介します。

1. E=mc2（質量はエネルギーと等価）
2. 放射線と放射能
3. 核分裂反応
4. 核分裂の連鎖
5. 原子力発電の仕組み
6. 原子力発電の安全設計
7. **安全設計の概念**
8. 原子力事故は何故防げなかったのか
9. 安全なシステムを作るために

7. 安全設計の概念

安全な製品やシステムを作るためには、当然安全に着目してシステムや製品を設計せねばなりません。そもそも安全設計とは何をすることでしょうか。本章では、安全の定義、ハザードと危害の違いなどを示しながら、安全設計の流れについて簡単に説明したいと思います。また、ソフトウェアとハードウェアとでは、安全を脅かす原因の性質に違いがあります。ソフトウェアの安全確保はどのように考えるかについても述べたいと思います。

なお、本章は ISO/IEC Guide51:1999（JIS Z 8051:2004）をベースにお話しします。本規格は安全の基本概念を示しており、ISO および IEC 規格の安全側面における導入指針となっているものです。ISO や IEC の規格書は、安全の側面においては、本規格の指針に従って作成されています。また、ソフトウェアに関する安全性については、ISO/IEC Guide51 の下位規格である機能安全規格 IEC 61508（JIS C 0508）をベースに説明します。これは、電気・電子・プログラマブル電子安全関連系を対象とする機能安全に関する規格で、ソフトウェアに関する安全についても触れられています。

7–1. 安全の定義

ISO/IEC Guide51 では、**「安全」を「受容できないリスクがないこと」と定義**しています。**「リスク」は「危害の発生確率及びその危害の程度の組み合わせ」、「危害」は「人の受ける身体的障害若しくは健康障害、又は財産若しくは環境の受ける害」**です。すなわち「安全」は、リスクを許容可能なレベルまで低減させることで達成でき、また、**100% 危害がないという「絶対安全」を示していない**ということです。「安全」という用語はリスクがないことを保証していると誤解されやすいため、本規格では「安全ヘルメット」ではなく「保護ヘルメット」と呼ぶなど、「安全」という用語を避けることを推奨しています。

安全のイメージを掴んでいただくため、「何を」「何から」「何により」安全を確保するのかを**図 1** に示しました。これらは一例ですので、全てではありません。これを見ると、安全とは身体や命だけが保護対象でなく、財産やデータも保護対象ですし、安心も保護対象だったりします。

7–2. 安全性の高め方

本項では、システムや製品で安全性を高める設計方法を述べます。安全設計の流れを**図 2** に示しました。このように、**安全設計の基本は、リスクを明確にすること**にあります。

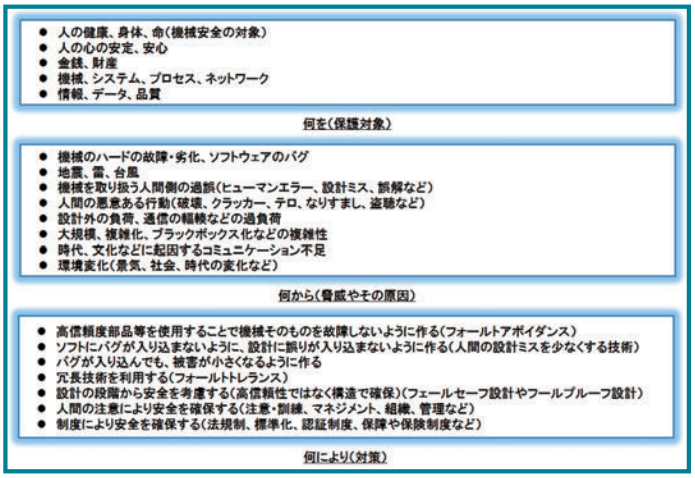


図 1 安全の確保にあたり
（参考文献：安全設計の基本概念，宮崎浩一，向殿政男，日本規格協会）

流れですが、まず、システムの目的や機能・構造、利用方法などを明確にし、想定使用者や接触者を特定し、想定される使用や誤使用を推定します**（図２の①）**。そして、潜在リスクを摘出し、ハザードを特定します**（図２の②）**。「ハザード」は「危険源」とも呼ばれ、「危害の潜在的な源」を指します。ハザードは、危害の発生源や性質を定義することが一般的で、例えば、感電や切断、火災などです。ハザードを特定したら、事故シナリオ分析などを行って、リスクの見積りを行います**（図２の③）**。その後、各リスクに対して発生頻度、危害の程度を予想し、リスクの程度を評価します**（図２の④）**。各リスクが許容可能かを判断し、許容可能でなければリスク低減方策を立案、実施します**（図２の⑤）**。これを許容可能なレベルになるまで繰り返します。

リスクアセスメントにおいては、What-if 分析や FMEA、 HAZOP、FTA などの技法を用いることになりますが、全てのリスクを抽出することは、とても難しいです。トラブル事例などの先例に倣うことがとても重要となります。

リスク低減方策における基本的な考え方は、**３ステップメソッド**と呼ばれるものです。**図２の左側**にあるように、「本質的安全設計方策」「安全防護及び付加保護方策」「使用上の情報」の順にリスク低減方策を講じます。ただ、それでも許容可能なリスクを達成できない場合は、使用段階でのリスク低減を検討します。

リスク評価では、安全機能ごとに達成すべき安全性度合いを、**安全度水準（SIL）**という尺度で割り当てます。その要求された SIL を実現するように安全設計を行います。

7–3. 本質安全（固有安全）と機能安全

安全の達成の考え方は、以下のような性質で成り立ちます。

- **ハザードの発生を抑制する性質**
- **ハザードが発生しても危害に至らない性質**
- **ハザードが発生しても危害を回避できる性質**

本質安全とは、ハザードの発生を抑制する性質を指します。一方、機能安全とは、ハザードが起こっても危害を回避できる性質や危害に至らない性質を指します。よくある鉄道踏切の例では、立体交差にすることで踏切内侵入の事故をなくし、本質安全を高めます。一方、信号や自動列車停止装置によって事故を低減し、機能安全を高めます。

製品やシステムの開発においては、安全性を確保するために、できるだけ本質的な安全を組み込むことを考えますが、全ての製品に対する本質安全設計は極めて困難です。ですので、利便性や経済性などを踏まえた上で、機能安全によっても安全を確保していきます。

7–4. ソフトウェアにおける安全性の評価

システムの安全性を評価するためには、ハードウェアやソフトウェアのみで完結するものではなく、**システムを利用する人間も含めたシステム全体で考慮せねばなりません。**そのため、ハードウェア、ソフトウェア両面で安全性を考慮するのですが、ハードウェアにおけるハザードとソフトウェアにおけるハザードは、異なる性質を持っているため、同じようにリスクアセスメントや低減方策を行えません。

ハードウェアにおけるハザードは、例えば劣化のように、確率論的に発生します。このような場合は、故障率という物理的特性で発生頻度を評価することができます。一方、**ソフトウェアにおけるハザードは、障害の有無が人間のエラーの有無で決まり、決定論的に発生します。**よって、確率論的に発生頻度を評価することが難しく、システムのアーキテクチャや開発プロセスの質によって評価せざるを得ません。ですので、IEC 61508

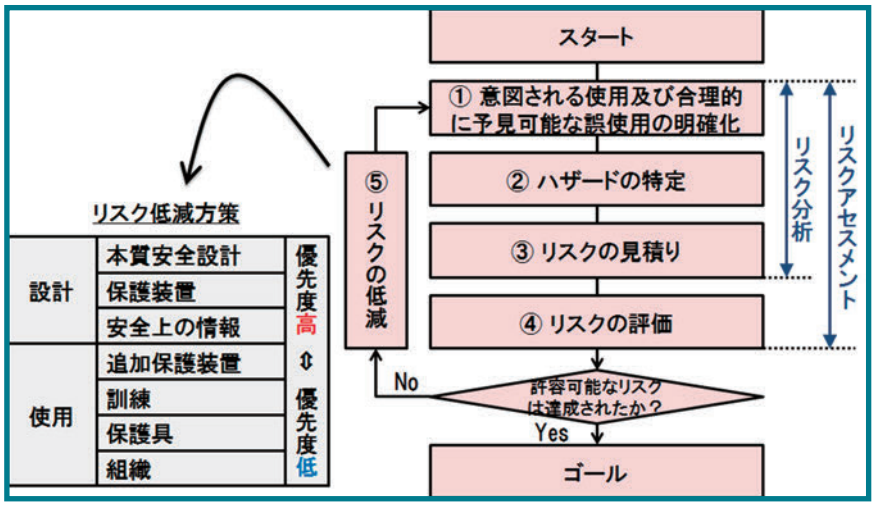


図２ リスク評価とリスク低減方策の流れ
（参考文献：安全設計の基本概念，宮崎浩一，向殿政男，日本規格協会）

ベリサーブ
東 弘之

では確率論的なハードウェア故障（ランダムハードウェア故障）と決定論的なソフトウェア故障（システマティック故障）を分類して、リスク分析や対策を行います。

ソフトウェアの故障は因果的に発生すると言われ、対処には原因を取り除く必要があります。この原因は様々なシステム開発工程で埋め込まれるため、IEC 61508 では**原因除去をシステム開発の全工程で行う必要がある**と規定しており、これを**全安全ライフサイクル**と呼んでいます。

ソフトウェアの安全性確保のポイントは、開発プロセスごとの検証結果や妥当性確認結果を明確にすることにあります。そのため IEC 61508 では、**V モデル開発が推奨**されています。ソフトウェア安全機能要求事項仕様書を作成し、定めた要求事項に従って開発しているかを、各開発プロセス検証することで、安全性が確保されていることを示します。

とはいえ、結局ソフトウェアの安全性確保は、決定論的な故障を引き起こすために定量評価が難しいという問題があり、ハードウェアのようにはいかないのが現状です。ソフトウェアの安全性を高めるための要件は色々な団体によって整理されていますので、これら情報を活用して最善の結果を出すことが、ソフトウェアの安全性を高める近道と言えると思います。例えば原子力の分野では、「ディジタル安全保護系規制要件調査等に関する報告書」（独立行政法人 原子力安全基盤機構（原子力規制庁に統合））があります。本報告書では、安全性ライフサイクルの各要求事項に沿って、安全性向上のための要件がまとめられています。また、開発プロセスごとに推奨される技法や方策、用いるべきでない技法や方策が紹介されています。例えば、ソフトウェア・アーキテクチャ設計プロセスにおいては、人工知能や動的再構成という技法・方策は用いるべきでないとなっています。

あとがき

今回は、安全設計の概念について述べました。**安全とは、受容できないリスクがないことを指し、絶対安全を指していない**ことを述べました。**安全性を高めるために、ハザードを特定し、リスクを分析、評価し、必要に応じてリスク低減方策を行う**ことも述べました。ハザードの特定やリスク分析、リスク評価をより正確に行い、適切なリスク低減方策を行うことが、安全性を高める設計に繋がります。

しかし、リスクが利用者の価値観や社会通念に照らして許容可能なレベルまで低減されたと判断、もしくは合意ができたときに、**「相対的に」安全である**としか言えず、曖昧です。価値観や社会通念は、国やその文化によって、また人によって異なりますし、時代によっても異なります。安全と一口に言っても捉え方は様々であり、安全性を知るにはどのようにリスクアセスメントしているのかを踏まえる必要があります。

次号は、本章を踏まえて、「8. 原子力事故は何故防げなかったのか」と「9. 安全なシステムを作るために」を説明したいと思います。

プチコラム 「３ステップメソッド」

本項ではリスク低減方策として３ステップメソッドを紹介しました。３つのステップについて、簡単に考え方と例を示します。

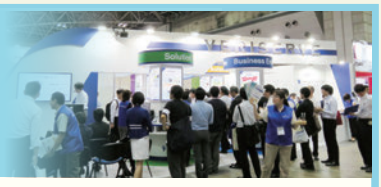
「本質的安全設計」では、危険源の除去や隔離によって安全性を確保します。フォールトアボイダンスを取り入れた設計などもありますが、ヒューマンエラーを減らすために人間工学を取り入れた設計も該当します。また、危険源の隔離は、そもそも人が危険源に近づく機会を減らすような設計を行います。壊れにくい部品を用いて修理の機会を減らす、機械化を進める、などの方法が挙げられます。

「安全防護」は、ガードや人感センサーを設けるような設計です。**「付加保護方策」**は、本質的安全設計や安全防護でもない方策です。代表的なものに非常停止機能があり、設計においては以下のようなことを踏まえます。（非常停止については、ISO13850（JIS B 9703）で設計原則が述べられています。）

- **非常停止機能は全ての運転モードよりも優先されること。**
- **リセットされるまで、他の全ての起動信号も有効にしないこと。**
- **本機能を他の安全機能の代替手段としないこと。**
- **本機能により、他の保護装置や安全機能の有効性が失われないこと。**

「使用上の情報」は、信号や警報などにより、使用上の正しい情報を使用者に伝える方策です。

ソフトウェア開発環境展（SODEC）で講演・出展しました



総称 Japan IT Week 春 第25回 ソフトウェア開発環境展 SODEC

ＩＴの最新事例や最先端技術情報の専門展として、12の展示会が同時開催されたJapan IT Week春において、当社は第25回ソフトウェア開発環境展（日程：2016年5月11日（水）～13日（金））、会場：東京国際展示場）で、講演とブース出展を行いました。

展示内容としては、当社のサービスやソリューションを4つに分類（Automotive、Solution、Business Enterprise、IoT）し、ＬＥＤパネルやサービスリーフレット、および詳細資料により来場者へ説明を行いました。ブース内プレゼンテーションでは、4つのテーマ（テストマネジメント、テストプロセス改善、静的テスト、品質技術外観）で、1日8講演を3日間通して実施しました。

また、別会場で開催された製品・技術ＰＲセミナーでは、当社も2日目のセミナーで講演しました。当社の松木を講演者として、「スペシャリストのテスト自動化実践ノウハウ」と題し、テストの実作業において有効なノウハウやポイントの説明を行いました。

河原田社員によるブースセミナーの様子

技術PRセミナーの様子（講師：松木社員）

2016年5月20日（金） JaSST'16 Tohoku 参加レポート

JaSST' 16 Tohoku : Japan Symposium on Software Testing in Tohoku 2016

2016年5月20日（金）、仙台市情報・産業プラザのセミナールームで開催されたソフトウェアテストシンポジウム（ＪａＳＳＴ'16 Ｔｏｈｏｋｕ）（主催：ソフトウェアテスト技術振興協会（ASTER）、ＪａＳＳＴ実行委員会）の参加報告をさせていただきます。

JaSST東北実行委員長の開催挨拶で始まったシンポジウムは、基調講演、ワーク、スポンサーライトニングトーク、情報交換会の4部構成で進行されました。

基調講演では、電気通信大学の西氏より「VSTePによるソフトウェアテストの開発」をテーマに、テストの全体像を捉えながらテストケースを具体化するためのテスト開発手法であるVSTePの概要、考え方、実施の流れ、導入のコツについて、重要なポイントにフォーカスした説明が行われました。

午後からのワークでは、参加者全員が1チーム6～7名のテストチームに分かれ、VSTePの考え方を利用して、同じソフトウェアのテスト開発（テスト要求分析、テスト観点図作成、テストコンテナ作成）を行いました。最後の情報交換会は、ワークでの実践を踏まえ、疑問点やより詳しい内容を確認するお悩み相談会となり、多数の質問に対して西氏からの回答・解説を受け理解を深める機会となりました。

当社は、スポンサー企業としてライトニングトークで会社とサービス概要をご紹介させていただき、当社のサービス提供について、参加者の方々にご協力とご支援をお願いしました。

ライトニングトークの様子（竹原社員の会社紹介）

読者アンケート

いつも『VERIserveNAVIgation』をお読みいただきましてありがとうございます。
今後さらに充実した内容をお届けできるように、記事に関するご意見・ご要望をお聞きする読者アンケートを実施いたします。
是非ともご協力いただきますよう、宜しくお願いいたします。
アンケートにご回答いただいた方にはもれなく
オフィスでも使えるオリジナル商品をプレゼントいたします。

応募方法は2通り

URLから応募
https://questant.jp/q/verinavi2016summer

QRコードを読み取って応募

ソフトウェアに
新たな価値を創造する

３０年以上にわたり、
ソフトウェア検証で品質向上に貢献しています。

仕様などの要求事項が満たされているかを評価する「Verification」と、
機能や性能が本来意図された用途や目的に合っているかを評価する「Validation」。
当社の社名にはこの2つの「V」を提供する（Service）という想いが
込められています。

VERISERVE

http://www.veriserve.co.jp/

VERISERVE NAVIGATION『ベリサーブナビゲーション』 2016年6月号

編集・発行：株式会社ベリサーブ
〒160-0023　東京都新宿区西新宿6-24-1 西新宿三井ﾋﾞﾙ14F
マーケティング部：03-5909-5700

本誌についてのお問い合わせ先：マーケティング部
発行責任者：西村憲一郎　編集責任者：竹原正人・豊本奈美江
verinavi@veriserve.co.jp