2016年7月1日発行
第12巻 第1号(通巻48号)
ISSN 1349-8622

SEC journal 45

巻頭言

栗島 聡 一般社団法人 日本データマネジメント・コンソーシアム[JDMC] 会長
株式会社NTTデータ 代表取締役副社長執行役員

所長対談

人工知能と人間の共進化

石山 洸 リクルートAI研究所 R.I.T (Recruit Institute of Technology) 推進室 室長

論文

ソフトウェア開発記録の多次元データ分析に向けた可視化方式 Treemap Forestの設計と実証的評価

中川 尊雄 奈良先端科学技術大学院大学／伊原 彰紀 奈良先端科学技術大学院大学
松本 健一 奈良先端科学技術大学院大学

特集

SEC 2015年度活動概要

＜システムグループ＞
情報処理システムの信頼性向上に向けて／重要インフラ等システム障害対策
システムの安全性・信頼性分析手法／定量的管理による信頼性・生産性向上
コーディング作法ガイド(ESCR)の整備について

＜ソフトウェアグループ＞
つながる世界(IoT時代)の高信頼化に向けて／「つながる世界の開発指針」の策定
「つながる世界の開発指針」に関する実証実験／システムズエンジニアリングの推進
先進設計・検証技術の適用事例紹介と分析

ソフトウェア工学分野の先導的研究支援事業について

報告

米国における有力組織との意見交換

解説

システム理論に基づくアクシデントモデルSTAMP

石井 正悟 SEC調査役

Column

半沢直樹が職を奪われないために

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

SEC journal No.45
Vol.12 No.1 Jul. 2016

巻頭言

企業・組織の競争力の源泉は「データ」にある

～あらゆる領域でビジネスとITをつなぐ　データの活用が問われる時代に～

栗島　聡

一般社団法人 日本データマネジメント・コンソーシアム［JDMC］会長
株式会社NTTデータ　代表取締役副社長執行役員

真にデータを活用し企業の競争力に貢献することを目指して、2011年４月に23社の会員で発足した日本データマネジメント・コンソーシアムは、５周年を迎え会員数200を超える団体となりました。

今なぜ“データマネジメント”が注目されているか

データをビジネスに活用することはこれまでも様々な形で行われてきましたが、活用のあり方がよりダイナミックになり、以前にも増して重要な活動となってきています。製造、流通、サービスなど事業活動のあらゆる場面で、データに基づく事業運営へのシフトが進みつつある今、IoT（Internet of Things）、人工知能（AI）といったテクノロジーの進化に対して忘れがちなのが、「データそのものが、目的に沿って活用できる状態になっているか」という観点です。

実際の現場では、企業内でのコード体系の不整合によってシステム間のデータ連携がスムーズにできない、オムニチャネルやカスタマー・ジャーニーといった新たなビジネスニーズにデータが活用できる状態になっていない、といったことが日常的に起きているのではないかと思います。どんなにコンピュータの能力が向上したにせよ、人間と同じように情報を渡せば（場合によっては人間よりも賢く）理解して答えを出してくれるという錯覚は危険です。間違ったデータを投入すれば、「正確に」間違ったアウトプットとなるのは当然のことであり、活用対象となるデータの意味や精度、粒度、鮮度などが適切にマネジメントされていなければ、事業目的に沿ったデータ活用はできません。

企業における業務や国民の生活の隅々までITが広く深く浸透した昨今、様々なヒトやモノの動きがデータとして蓄積され、分析できるような環境になっているにもかかわらず、いざ、その活用を試みようとしたときに「自社内のデータが活用に足る状態になっていないこと」に改めて気づかされる企業が増えてきました。この５年間でJDMCにこれだけの会員の参加をいただき、データマネジメントという概念に注目があつまっている背景には、このような現状があるからではないかと考えます。

今、正に“データマネジメント”を事業活動に取り入れる時期にある

JDMCでは、データマネジメントの定義として、『データをビジネスに活かすことができる状態で継続的に維持、更に進化させていくための組織的な営み』としております。データが利活用可能な状態になければ、どれだけ高価なシステムを導入しても価値を生み出すことはできません。一方で、データを整備し事業の武器として利活用することにより、従来できなかったようなマーケティングの高度化や自社商品・サービスの差異化、生産性の向上など、様々な分野で極めて大きな効果を創出することができます。

JDMCが去る３月に開催したカンファレンス「データマネジメント2016 ～データ駆動こそがビジネスを創る～（http://www.seminar-reg.jp/jdmc/dm2016）」では、こういったデータマネジメントによるビジネスへの効果について14社・団体のユーザー事例を発表していただきました。約1000名にも及ぶ参加者の方々には、正に「データからどれだけの価値を引き出せるか」が企業・組織の競争力の源泉となっていることを改めて実感していただけたのではないかと思います。

「共通語彙基盤」はデータマネジメントの重要な一要素

前述のカンファレンスにて、データマネジメントにおいて他の模範となる活動を実践している企業・機関などの中から優秀な事例を選定し、表彰させていただくデータマネジメント各賞の表彰式が行われました。その中で、独立行政法人情報処理推進機構（IPA）様の共通語彙基盤の取り組みを「特別賞」として表彰させていただきました（大賞は、セブン&アイ・ホールディングス）。

個々のデータを表す言葉（単語）に関して、その表記や意味・構造を統一し、共通的に意味が通じるようにすることは、多義的な言葉の意味変換といった余計な工数が生じたり、変換しても正確に意味が伝わらない、などといった活用上の問題を抑制する上で、非常に重要な役割があると認識しています。今後、IPA様とは共同適用研究や普及・啓発活動などでご一緒させていただき、更なるデータマネジメントの向上に寄与できれば幸甚と考えます。

一般社団法人 日本データマネジメント・コンソーシアム［JDMC］
Webサイト：http://japan-dmc.org/

人工知能と人間の共進化

リクルートAI研究所
R.I.T（Recruit Institute of Technology）
推進室 室長
石山 洸

SEC所長
松本 隆明

人工知能という言葉を聞かない日はない。2045年にはシンギュラリティを迎えるとの予測もある。そうした中、株式会社リクルートホールディングスは、「Recruit Institute of Technology」（R.I.T）を人工知能（AI）の研究所として再編、グローバル規模で研究を開始した。人工知能は今後どのような役割を果たすのか、人間とのかかわりはどうなっていくのかについて、R.I.T推進室長の石山氏に伺った。

人工知能の研究所を設立した二つの目的

松本　最近、IoTというキーワードの下、色々なものがつながって様々な新しいビジネスが生まれるという議論があります。それを実現していく上では人工知能が大きな役割を果たしていくのではないかと思いますが、まずリクルートさんが今人工知能の研究に力を入れられる理由から、お聞かせいただけますか。

石山 洸（いしやま こう）

Recruit Institute of Technology推進室室長。2006年、リクルート入社。雑誌・フリーペーパーのデジタル化を推進。新規事業提案制度を契機にビッグデータ関連の子会社設立。同社を成長させ、3年間でバイアウト。その後、メディアテクノロジーラボの責任者を経て現職。

石山　よくリクルートの仕事は、“おみくじビジネス”と言われています。進学や就職、結婚といった様々なライフイベントにかかわり、人生の節目に大切な情報をご提供させていただいているからです。情報提供の手段としては雑誌から始まり、それがフリーペーパーになり、フリーペーパーからパーソナルコンピューターでの情報提供になりました。更にフィーチャーフォンになり、スマートフォンになってきた。次の世代では、正にIoTや人工知能のようなものが情報提供あるいは情報を媒介する手段として非常に重要になってくると考えたことが、人工知能の研究所を設立した第一の目的です。

設立の目的はもう一つありました。実は、リクルートが目指すビジョンの一つに「2020年に人材ビジネスでグローバルNo.1になる」というものがあります。そのため、10年ほど前から、機械学習のエンジニアやデータサイエンティストが、リクルートに少しずつジョインしてくるようになっていて、現在、国内トップレベルのデータサイエンティストがリクルートの中で働いています。ビジネス上のゴールとして目指すグローバルNo.1という姿があったときに、テクノロジーの世界でも、グローバルのトップレベルになっていきたいという思いがあり、これまでは既存のビジネスモデルの中に機械学習を導入してきたのですが、もう一歩踏み込んで、人工知能あるいはIoTを含めて新しいビジネスモデルを作っていこうと考えました。これが二つ目の目的です。

新たなビジネスモデルの開発につなげる

松本　新しいビジネスとして具体的にイメージしているものはありますか？

石山　まだ研究段階なので、具体的なところに踏み込んでご紹介できないのですが、新しいビジネスにも２種類あると考えています。それは、本当に新しいビジネスドメインで新しいビジネスモデルを作るということと、既にリクルートがやっているビジネスドメインだけれども、ここに新しいビジネスモデルを開発していくということです。

例えば、人材のマッチングの世界やその他のライフイベントでの意思決定に役立つような情報提供の仕方も、定石的に分かっていたような情報と情報のマッチング、あるいは求職者と企業のマッチングというところは、これまでもかなりお手伝いできていたところがあるのですが、人間側にバイアスがあって、これまでは発見することができなかった新しい定石のようなものを、アルファ碁が新しい定石を見つけたように、人工知能が介在することで見えてくるものがあると思います。それを通じて、潜在ユーザ同士のマッチングができるような世界が作っていけるといいな、と感じています。

松本　人工知能の研究だけではなくて、新しいビジネスにつながるところを考えていく。いわゆるビジネスクリエーション

のようなところがポイントですね。そういったところも、リクルートさんの中で色々考えて、やられているのですか。

石山　はい。私自身がこの研究所にいるのもそうですし、Alon Halevy（アロン ハレヴィ）という52歳のイスラエル出身の者を当研究所のトップに据え、シリコンバレーのマウンテンビューに拠点を置いているというのも、それが理由です。研究ができる、同時にビジネス開発もできるという人材を、なるべく研究所に集めているわけです。

例えば、大学の先生を評価するh-indexという指標があります。引用されている論文を何本以上書いているかというものですが、アロンの場合、それが94と非常に高い。同時に、起業を２回経験していて、その２回とも自分の会社を売却している。実は２回目の売却先がグーグルで、彼はグーグルリサーチで10年間ビジネスのマネジメントを含めてやっていたんです。彼をトップに招聘した理由も、テクノロジーの開発もできるけれども、ビジネスの開発もできる、という正にその点です。そして今彼が、この二つを人材要件としながら、同じような人材を集めています。

テクノロジーとビジネスをつなぐハブになる

松本　でも、なかなかそういう人はいないのではないですか。私どもIPAも、IT人材をきちんと育てたいということで「未踏プロジェクト」に取り組み、非常に“尖がった”人材を発掘し、支援するということをやっていますが、そこから起業に至るところが、なかなかうまく行かないのですね。国民性の問題もあるのかもしれませんが、社会的な支援の仕組みも海外ほどうまくできていないため、人もなかなか育っていかない。そこは海外から招聘することを考えられているわけですね。

石山　国内の人材も海外の人材もいます。実は私自身のバックグラウンドも、大学院のときに、18本くらいの論文を２年間で書いていたんですが、リクルートに入った後も、リクルートとエンジェル投資家から出資を受けた資本金500万円の会社に一人で出向して、その会社を３年間で成長させてバイアウトした経験があります。

なるべく、テクノロジーとビジネスの経験値を両方持った人が集まって、そこから、言葉は悪いですけれども、同じ能力を持った人を再生産していくような、小さいシリコンバレーのようなエコシステムみたいなものを、私どもの研究所の中に作っていければいいなと考えています。あまり世の中では知られていないのですが、未踏クリエイター事業の中で未踏社団ができるときの、第１号法人会員が、実はリクルートなんです。

松本　当初からご協力いただきありがとうございます。

石山　IPAさんの側でもリクルートに対して、未踏の世界観の中にアントレプレナーシップを注入して欲しいという期待値があり、お声掛けいただいたようです。当時の手続きも私がお手伝いしていて、ですから実はIPAさんとはお付き合いが深いんです。未踏人材の方々とリクルートの人工知能研究所がコラボレーションする中で、彼らのテクノロジーと、リクルートのビジネスメイクのケイパビリティを融合させ、新しいビジネスを作っていければと思っています。

その際、ビジネスサイドが強い人だけが集まったり、テクノロジーサイドが強い人だけが集まると、なかなかマッチングしない。私たちの研究所がハブになって、もっとマッチングしやすいようにプロデュースさせていただくことができるといいのではないかと考えています。私たちが日本の中のイノベーションのハブのようなものになっていければいいですね。

松本　確かにそういう出会いの場そのものが少ないですね。せっかく未踏を卒業しても、なかなかチャンスがないし、人とのパスがない。どうやってビジネスにつなげられるかというところを少し埋めてあげられる人がいるだけで、スッと伸びるでしょう。それは非常にいいお話ですね。

まだデータが集まっていない産業セクターが重要に

松本　人工知能が新しいビジネスの創出につながるという意味で言うと、どういう業種あるいは分野が有望なのでしょうか？石山さんの目から見ていかがですか？

石山　大きく二つのチャンスがあると思っています。一つは、既にデータがたくさんある業界です。各セクターの中で、データがたくさん集まっているものと、そうでないものというのが、両方あると思っていて、既にデータが集まっているような領域は、正に人工知能が活躍できる余地がすごく大きい。すぐにビジネスが始められると思っています。

もう一つは、まだデータがたくさん集まっていないところです。これからデータが増えていくので、私自身は非常に大切だと思っています。そういった分野にいち早く参入して、人工知能の開発をしていくことが重要ではないでしょうか。

実は10年前に私がリクルートに入社したとき、まだ雑誌やフリーペーパーのメディアがメインビジネスで、デジタル化はそれほどされていませんでした。そこから10年かけてデジタル化をして、今正に人工知能が活かせるようなデータを作ることができたということ自体が、大きな価値ではないかと思っています。10年前のリクルートのような状態の産業セクターはまだたくさんあるので、そういったところにアントレプレナーシップがあって、テクノロジーに明るい人たちがどんどん入っていくことによって、その産業自体がデジタル化され、伸びていくのではないか。成長のポテンシャルがあるの

松本　隆明（まつもと　たかあき）

1978年東京工業大学大学院修士課程修了。同年日本電信電話公社（現NTT）に入社、オペレーティング・システムの研究開発、大規模公共システムへの導入SE、キャリア共通調達仕様の開発・標準化、情報セキュリティ技術の研究開発に従事。2002年に株式会社NTTデータに移り、2003年より技術開発本部本部長。2007年NTTデータ先端技術株式会社常務取締役。2012年７月より独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア高信頼化センター（SEC）所長。博士（工学）。

ではないかと思います。

松本　確かにその通りですね。ただ、データが幾らあっても、それをどう活用していくか、正にデータサイエンティストの役割になりますが、人工知能に全部やらせようと思ってもなかなか難しい。人間のスキルや能力をどう育てていくか、というところが難しい問題になるという気がします。

石山　おっしゃる通りです。私は二つあると思っていて、一つは、データサイエンティストの人たち自身が、いわゆる本当のエンドユーザの人たちとの定性的なコミュニケーションの量を増やすことが必要なのではないかと。実際、私自身の場合ですが、リクルートに入社したときに、まだIT人材採用のような仕組みがなかったので、最初の３カ月間は営業研修を受けていたんです。でも、このときの経験がすごく生きていて、いわゆるエンドユーザの方々とコミュニケーションをさせていただくことによって、実際のニーズがたくさん見つかって、機械学習のテクノロジーを使うと解決しそうだな、というインスピレーションを得たり、ヒントがたくさんありました。リクルートの中では営業研修という形だったわけですけれども、サンフランシスコでは、数年前からリーンスタートアップという言い方をしていて、プロブレムとソリューション、あるいはプロダクトとマーケットをどうフィッティングさせていくかということ自体が、科学的にメソドロジー化されていき、それがエコシステムの中で回っていくことによって、新しいビジネスモデルが生まれていく、という循環ができています。

そういう意味で期待したい部分は、テクノロジーを持っている人たち自身が、世の中、社会と直接接するような機会がもっともっと増えていったらいいなということです。そこからアントレプレナー型のデータサイエンティストが増えていくことによって、色々なアイデアが発現していくような社会になっていけばいいですね。

松本　なるほど。でも現場の情報を身をもって体験するというケースは、なかなかありませんね。そういう場をどうやって増やしていけばいいのか。とくに、単に特定の産業界だけではなくて、これからはますますオープンイノベーションになっていく。産業界を跨がって、こちらのデータを使うと別のドメインで新しいチャンスが生まれてくるといった橋渡し的なビジネスもこれから増えてくるでしょうし、つなぐ人も必要になりますね。とくに、IoTの時代は相互につながってきますから。

石山　おっしゃる通りですね。

データのアライアンスで競争力のあるビジネスを創出

松本　そういった人材はどうやって育てればいいと思われますか。

石山　意外に、最初は食べず嫌いで、どちらかというと、ラボの中に閉じ籠もりたいとか、研究室の中にいたいと言っている人も、実際に、プロダクトを作るフェーズになってくると、使ってみてどう思われたかということのフィードバックにはすごく関心があるのが分かりました。人工知能の手前でそのことをラーニングしていくというプロセス自体は、やってみると結構楽しい。これは私自身の経験からも分かっていて、思い切って最初の一歩を踏み出してみるところをサポートしてあげる、あるいは一度踏み込んだことがある人たちが引っ張っていく、そういった循環になっていくといいのではないかと思います。

松本　リクルートさんのそういう技術を持った人が、実際に違うドメインの業界や企業に入り込んで、一緒に何かをやっていくというケースも出てくるんでしょうか。

石山　リクルートの研究は三つの貢献というものを掲げていて、一つ目は、当たり前ですが、リクルートのビジネスへの貢献です。もう一つが科学への貢献で、積極的に論文を執筆していこうということがあります。そして三つ目が、社会への貢献で、例えば、オープンソースでテクノロジーを公開することによって、社会に貢献していきたいということです。汎用的なテクノロジーについては、リクルートの中のセクターだけでなく積極的にオープンソースにしていきたいという思いがあって、これから、そういうプロジェクトを始めていきたいと考えているところです。

松本　オープンソースにして技術を広げていくのもそうですが、本当にビジネスにつなげていくような、例えばリクルートさんが農業の分野に出ていって、現場で色々な情報を使って農業をスマート化するというようなことを始められるケースも考えられるんですか？

石山　農業であるかどうかは分かりませんが、ビジネスのバリューチェーンのようなものがあってリクルートと戦略的なパートナーシップを結べるような企業があったときに、それを例えばA社とすると、リクルートのデータを使うと、それがA社で人工知能を作るときの供試データとしてすごく役立つものになる。そうしたデータ上のシナジーがあって、一緒にビジネスができるような提携ができる。あるいは逆に、A社がリクルートのビジネスになるような供試データを持っていて、一緒にビジネスをするとリクルートもA社も売上を伸ばすことができる。こうしたスキームは機械学習の世界ではすごく考えやすいことです。そういったビジネススキームをどれだけたくさん考えられるかが、非常に重要だと思っています。そうしたデータのアライアンスを含めた競争戦略は今後大切になっていく可能性が高い。グローバルな競争環境の中でどう闘うかということの一つのヒントだと思います。例えば、よりリアル接点が多く、まだデジタル化されていない産業セクターの人たちといち早くアライアンスを組む。リアルなデータであればあるほど、本当にこの人たちを幸せにできる供試データになる可能性が高いと思うのです。既にオンライン上に載っているデータは、どちらかというと、本当の意味での供試データとしては不十分なものが多い。リアルなデータをいち早く取り込むことで、オンラインに強いプレーヤーとの競争戦略が作りやすくなるという構造があると思っています。

データの安全性をどう担保するのか

松本　話題が変わりますが私たちはソフトウェア高信頼化センターとして、ITシステムそのものの振興と、同時にその安全性の確保に力を入れています。これだけITが生活を支える時代になってくると、安全性をきちんと担保しなければ、社会生活が破綻してしまいます。人工知能の場合にデータがどこまで信じられるのか。確かにデータを分析してみて色々なことが分かるけれども、それが本当に正しいデータなのか、

誰かが保証しないと間違った方向にビジネスが展開されてしまう危険性があるのではないか。その点はどうお考えですか？

石山　データの質の問題については二つの観点があると思います。まずグローバルという観点があって、地域によってユーザが入力してできあがるデータのクオリティ、特性が違うと感じます。例えばある国ではあるデータが必ず入力されるが、ほかの国ではあまり入力されないということですね。こういう問題は機械学習を導入することで入力されない情報を補完していくということがあるのではないでしょうか。そこでは機械学習はかなり活躍できると思います。もう一つ、データが正しいか、あるいは妥当かというクオリティの問題があって、実は我々もその部分のリサーチはかねがねやっていきたいと考えているところです。当研究所でも自然理法解析のアドバイザーがたくさん入っていて、自然言語の非構造のデータ部分のクオリティ判定などに取り組んでいます。ただしこの分野は、コンピューターサイエンスの中でもまだまだ未発展の部分で、クオリティの高い低いということを決める評価関数をシャープに決めること自体が難しい。どういうメトリクスで評価してその供試データを作って学習させるのかということは非常に難しくて、一つの研究分野になるものだと感じています。

松本　そうですね。少し前に話題になりましたが、マイクロソフトの人工知能チャットボットがおかしな言動をするようになってしまった。あれも教育するための情報が少し偏ったものであったためといわれています。しかし、ではデータが間違っていたのかというとそれは誰も判断できない。とくに倫理にかかわる問題や精神論に類する話題などは誰も判定できないのではないでしょうか。サイエンスとしてその問題が解けるのかと心配にならないでもないですね。

石山　そうですね。サイエンスというよりは泥臭いエンジニアリングを含めたプロセスが必要なのかもしれないですね。企業側が機械学習のようなプロダクトを出す場合には、基本的にはリバースエンジニアリングされるリスクがあることを前提にしながらきちんと行うことが重要だと思います。例えば、グーグルの検索結果を人工知能と呼ぶかどうかは議論があるかもしれませんが、人工知能あるいは機械学習を使ったアルゴリズムでできているときに、当然SEOをかけてくるプレーヤーがいてリバースエンジニアリングされるということが分かりながら、ビジネス全体の設計をし、運営するという側面があると思います。マイクロソフトのチャットボットの場合も、そういうことを想定しながら作っていたら、また違うものになっていたのではないでしょうか。ですから、今回リバースエンジニアリングされたことを悲観するのではなくて、それを受け止めてもう一回サービスを作り直していく。新しい情報を得ることで人工知能自体がまた学習してより良いものになるという発展的なプロセスが生まれることを期待したいと思っています。

多くの人の協力関係の中で人工知能を育てる

松本　最近はレジリエンスエンジニアリングということが言われ始めています。がっちりしたエンジニアリングだけではなくて、ある程度柔軟性を持った許容性のあるエンジニアリングをしていかないといけないのではないか。環境はどんどん変わっていくので、それに対して画一的な方法論だけでやっていくと、間違った結果になってしまうこともある。そうしたことを考慮したエンジニアリングをやろうという方向になりつつあります。それと同じような考え方かもしれないですね。

石山　おっしゃる通りだと思います。そう考えていくと、アルゴリズムを作れる人だけで人工知能のサービス全体をマネジメントしていくことはできないので、色々なドメイン、あるいはスペシャリストの人たち、そしてユーザサイドの人たち、そういった人たちの協力の中で人工知能自体が育っていくことが必要だと思います。そういう世界観をどうディレクションしていけるかが大切ですね。

松本　安全性という意味で言うと、社会システムを安全なものにしていくために人工知能を活用していくということがあると思います。自動運転がそれに当たるかどうかは分かりませんが、自動運転も人工知能でなるべくやっていって、ドライバーのミスを減らし、交通事故を減らし、安全に寄与していこうという考え方だと思います。人工知能を使って安全性向上のために活用していくケースというのは、何か考えられますか。

石山　幾つかのパターンがあると思います。一つは顕在化しているリスク自体を減らしていくということです。自動車事故の件数がどれだけあって、そこに自動走行をいれることでどれくらい減っていくかということがまず一つ。もう一つは、今までどちらかというと人間自身がバイアスだと思っていて、リスクだと感じなかったけれども、実は機会損失がたくさんあった、というような問題もあると思う。人工知能を使うことによってそういった問題が改善できることが発見されていくことも、人工知能の持つポテンシャルの一つだと思います。

もう一つの軸がミクロとマクロということです。ある自動車があってそれが事故に遭わないということも大切ですが、マクロ経済全体のバランスのようなことを人工知能がどう支援してくれるのか。これは個人的にも興味がある分野です。例えばミクロ経済の世界の中で所得の分配が偏るときに、マクロ経済においてもその分配の問題自体を人工知能が支援してくれるとか、あるいはGDP自体も押し上げるけれども、所得分配もなだらかになるということを実現するためにはどうしたらいいのか、といった社会科学も人工知能によって進化し、社会システムの安定性がより担保されていく。こうした分野はまだまだ未開拓なので、そういったところにも転用されていくとうれしいですね。

松本　なるほど。それはスケールの大きな話ですね。

人工知能が新たな職業の可能性や就業機会を増やす

松本　逆にごく単純に、人間の作業を人工知能に置き換えていくことによってなるべくミスを減らしていくということも考えられると思いますが、最近、オックスフォード大学のマイケル・オズボーン博士が「人工知能によってなくなる職業」を示して話題になりました。単純作業に近いことはこれからどんどん人工知能に置き換えられていく分野なのか、あるいは知的なクリエイティブの部分もどんどん人工知能にやらせていくようになるのか、どちらの方向なのでしょうか。

石山　難しいのが、人間から見たときの単純･複雑という話と、人工知能やコンピューターから見たときの単純・複雑というのは異なっているケースもあるということです。一概に何が知的で何が非知的なものか、そもそもインテリジェンス自体の高さをどう測るか。人間が直感的にイメージする知的あるいは知的でない作業というような区分けは難しいと感じます。仕事に関する話でいうと、職業とは何だろうというのは、突き詰めるとこれも難しい。個々の職業の中には幾つかのタスク、やらなければならない仕事があって、幾つかに分解できるとしたときに、実は人工知能や機械学習によって置き換わっていく部分は、職業そのものではなくて、一部のタスクなんですね。今まではその職業を全うするために10のタスクをこなすスキルを持っていなくてはいけなかったのに、その中の２つのタスクがこなせれば、実はその職業に就けるということも考えられる。従って人工知能や機械学習が出てくることによって職業選択の機会自体が増えていく可能性が高いといえると思います。しかし、実際に世の中に出ているリサーチは「なくなる職業」についてのものが圧倒的に多くて、これ自体がある種の問題だといえるかもしれません。今後期待したいのは、機械学習について予測していく中で、生まれてくる職業を発見して、こうした新しく創発してくる職業に就けるようなケイパビリティを早期に発見して教育していくという社会システムだと思います。そうしたこと自体の発見も人口知能のテクノロジーを活用することで可能になるのではないか。そこのポイントが大切だと考えています。テクノロジーの問題はテクノロジーで解決するということができるような社会になっていけばいいなと思います。

松本　おっしゃる通りかもしれませんね。人工知能で職業がなくなるというのではなく、新たな職業が生まれる、あるいは今まではその職業に就けなかった人が人工知能の助けを借りることによって、その職業に就けるようになる。職業選択の機会が増えていく可能性があるわけですね。

石山　テクノロジーのプロバイダー側も、先ほどのリバースエンジニアリングの話と同じですが、社会的損失があるときにそれ以上の社会的価値をどう生み出していくかということをアルゴリズムの中である程度設計していく。一人ひとりがそういった人工知能をプロバイドしていくことによって、それ自体がビルトインスタビライザーのような機能になっていくのではないかと思います。

松本　もともと職業と人との出会いを事業のベースにされてきたリクルートさんが新しい職業を生み出し、雇用の機会を増やしていく、というようなケースも考えられるのですか？

石山　リクルートがどうかかわるかは色々考えていかなければならないのですが、実は世の中から自然に新しい職業はたくさん生まれているような気がしています。人工知能が成長していくシンギュラリティの仮説のベースになっているムーアの法則がありますが、ムーアの法則に引きずられて創発している職業がたくさんある。例えば、ソフトウェアエンジニアも、今までは受託するという仕事しかしていなかったと思いますが、クラウドのようなサービスが出てくることによって起業の参入障壁が低くなり、起業するエンジニアという職業が生まれています。起業するエンジニアが増えれば、競争環境上、例えばデザインで差別化しなければいけないということで、デザイナーの企業家が増え、そうすると今度はデザインだけでは差別化できなくなるので、もう少しユーザ心理を理解しながらマーケティングすることをやってみようという人が増え、そうすると今度は、そのインサイト自体をデータドリブンにきちんと捉えられないかということから、データサイエンティストという職業が生まれていくということが起こっていると思う。これは氷山の一角で、テクノロジーに引っ張られる形で生まれる新しい職業というのは今後もどんどん増えるのではないかと思います。

Data Robotの活用がコミュニケーションの機会を増やす

松本　プログラミングの経験もお持ちの石山さんはよくご存じだと思いますが、プログラムを作るということに関しても、これからは相当な部分を人工知能でできるようになる時代がくると思います。そうすると、どこを機械がやってどこを人間がやるのか、開発のライフサイクル全体の中の棲み分けが生まれてくる可能性が高いと思いますが､そのあたりはどうお考えですか？

石山　リクルートの事例で今の話に適合して面白いと思うのは、データサイエンティストの仕事自体を自動化する「Data Robot」という汎用機械学習プラットフォームサービスです。Data Robotを運営しているData Robot社にリクルートも出資をしています。一つの背景としては、データサイエンティストの供給自体が少ないということがあり、Data Robotのようなサービスを供給することでデータサイエンティストの不足を補っていくことができるということです。エクセルをドラッグアンドドロップして、予測したい項目を選んでボタンを押せばそれで予測できてしまう。しかも非常にたくさんのアルゴリズムを搭載していて、自動的に最適のアルゴリズムを選択してくれる。そのため、機械学習が全くできない、あるいはコードが書けないという人でも機械学習ができてしまうツールなのです。実際、データサイエンティストの人がそのツールを使い始めたら、今まではデータのクリーニングからアルゴリズムを作るということに80％のリソースを使っていて、解くべき問題を定式化するというところには20％のリソースしか使えていなかった。これがData Robotを使ったら、分析の作業自体が20％に減り、作れる予測モデルのところは５倍くらいに増えた。問題を定式化する時間が80％になり、この時間は実は人間とコミュニケーションしている時間になっているんです。もともと機械学習をやっているデータサイエンティストは、自分の中の仮説として「分析をしている時間が楽しい」というものを持っているのですが、よくよく彼を観察していると、人とのコミュニケーションが増えたほうが圧倒的に楽しそうになっているし、価値観自体も色々変わってきているような気がします。

松本　分かるような気がします。人と話をしながら「あっそれだ」と気づいたり発見したりすることも多いですからね。数字とにらめっこしているより、こうしたら面白いかもしれないというヒントを人から得るほうが楽しいでしょう。何を使って予

測するか、そこを決めることですよね。実際に決めてしまえばアルゴリズムで自動的に予測していける。そもそもどういう観点から分析をかけるか、ひらめきが重要であり、そこはおっしゃるようにコミュニケーションが大事でしょう。

石山　そうだと思います。コミュニケーションすることによって新しいニーズに気づくとか、新しい価値観に気づくことによって同じ問題を解くときの評価関数を変えるということがたくさん生まれる。コミュニケーションが非常に重要だということは間違いないと思います。私たちが共同研究をしているMITメディアラボのアレックス・サンディ・ペントランド先生のソーシャル物理学の理論の中でも、人と人とのコミュニケーション、とくにオフラインのコミュニケーションがあることによってイノベーションの高さが上がるとおっしゃっています。コミュニケーションが生まれることでイノベーションが生まれていくということはほぼ間違いないですね。

松本　ユーザの生の声を聞いてみないと新しいアイデアも浮かんでこないですからね。

石山　よりマクロで見てみると、先ほどのデータサイエンティストの供給不足というような雇用のミスマッチ自体は、まだマーケットベースでは起きています。供給が不足している領域に、人工知能の研究者がどれだけ人工知能を開発していって、その不足を補えるかということ自体も非常に大切で、社会的に期待されるところだと思います。

人工知能でどういう社会を作るのか、オープンで議論したい

松本　石山さんは「人と人工知能の共進化」ということをおっしゃっています。共進化というのはどういうイメージですか？

石山　例えば先ほどのいわゆるData Robotですが、Data Robotを使っていくとすごく簡単なので、データサイエンス自体が成長しないのではないかと思いがちですが、ベストプラクティスの手順を人工知能と一緒に分析していくので、彼等のデータサイエンス力自体も上がっていきます。Data Robotを使わなかったとしても、Data Robotを使い始める前と後の機械学習のベーススキルを比べてみると、後のほうが高くなっているということがあるのです。もう一つは当研究所の研究員が世界で２番目にData Robotを使っているんですが、その彼が色々なData Robotにもっとこういう企業があったらいいのにということをフィードバックしていて、それによってData Robot自体のロードマップも変わっていって、新しい機能が追加され、人工知能の側も進化するという循環が起こっています。こういうミクロのラーニングからマクロのラーニングに変わっていくと、世の中全体が共進化していくと考えているわけです。

松本　なるほど。お互いに学習していく世界が想定されているということですね。人工知能の将来を考えたときに、ある転換点があってぐっと変わっていくということがあるのでしょうか？

石山　「転換点」ということの解釈自体も、人によって違うところがあります。例えば日本ではよく「第一次人工知能ブーム」「第二次人工知能ブーム」といった言い方をしますが、世界も同じように区切るのかといえば必ずしもそうではない。日本で人工知能が冬の時代といわれていたときに、実はシリコンバレーでは機械学習を使った色々な成果が出ていました。一つの転換点のようなものがあったときに、それに対する解釈は人によってかなり違うと思います。そういう意味では「シンギュラリティ」よりも「マルチラリティ」という話をさせていただいています。

松本　ITの世界では、IoTの進展によって今は第三次から「第四次産業革命」への転換点だという言い方がありますが、急激に何かが明確に変わるということではなくて、徐々にある分野をベースにして変わっていって、全体としてみると結果としてこれは革命が起きているということですかね。

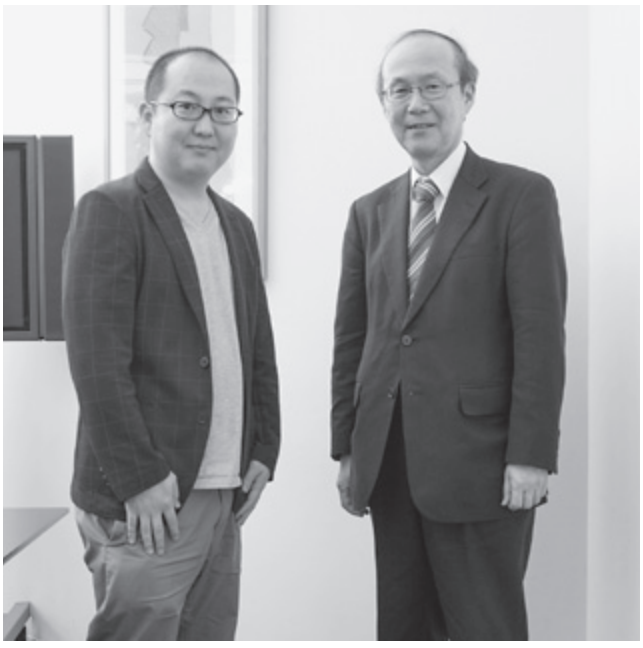
石山　そうだと思います。

松本　そのために一番大きなテクノロジーというのは何だと思われますか？

石山　テクノロジーもそうですが、スタンスというか、どういう社会になったら良いかという主観を色々な人たちが共有していくということが大切だと思います。先ほどの「第四次産業革命」のお話でいえば、普通にやっていったらたぶんこうなるよね、でももっと人間が意思を持って、こういう風に歩んでいったら第四次産業革命後の社会はこうできるんじゃないかということを、ターゲットを持って、かつそのターゲット自体もみんなが主観をボトムアップに合成しながらリッチな社会を作っていく。リッチな社会とは何かという価値観自体を作っていくことがすごく大切なのではないかと思っています。今、人工知能を社会にどう適用したらいいかということは、人工知能の研究者、あるいはコンピューターサイエンスの研究者という比較的狭いコミュニティの中でしか議論されていない。私はここにはリスクがあると思っています。これをどうオープン化し、人工知能にそれほど詳しくない人も、人工知能を通じてこういう社会ができればいいということを議論できるようなコミュニケーションにしていく必要があると思っています。

松本　それは大事な視点ですね。技術を超えた重要なポイントだと思います。社会が許容できるようになっていかなければ人工知能の活用も広がっていかないですからね。

本日は貴重なお話をありがとうございました。



ソフトウェア開発記録の多次元データ分析に向けた可視化方式 Treemap Forestの設計と実証的評価



中川 尊雄※　伊原 彰紀※　松本 健一※

ソフトウェア品質の第三者評価を行う分析者は，開発に従事していない者であることが妥当であり，客観的な視点から探索的解析を行うことが期待されている．しかし，ソフトウェア開発データに含まれる様々な要素（成果物，課題票，組織形態）の間にある関連性を考慮しながら解析を行うには工数を要する．本論文では，データ間の関連性に基づき，開発データの俯瞰を次々提示することで多次元データ分析を実現する新たな可視化方式Treemap Forestを提案する．Treemap Forestでは，データ間の関係性を明示化するため，開発データを関係データベース形式で表現し，開発データに対する探索的データ解析を実現する．有用性の評価実験を実施し，提案手法の利用は，従来よく用いられてきたExcelに比べ，約38%の時間でデータを解析できることを示した．

Treemap Forest: An Exploratory Data Visualization Approach for Software Development Project Datasets

Takao Nakagawa, Akinori Ihara, Kenichi Matsumoto

Software quality analysts in an independent evaluation organization should not be members of the software development team, because they are expected to perform evaluations from a neutral perspective. However exploratory data analysis targeting several kinds of software development datasets (e.g., products, issues, and members) is not easy to understand for analysts. In this study, we propose Treemap Forest, which is an exploratory data visualization approach for software development project datasets, and develop a prototype system with Treemap Forest. In order to evaluate the approach, we compare exploratory data analysis using Treemap Forest with traditional approaches. The Treemap approach can conduct tasks in 38% of the time taken by traditional approaches.

1　はじめに

ソフトウェア開発ベンダが製品・システムを提供する場合，利用者に対して安全性や信頼性をはじめとする品質についての説明を付することが求められる．しかし開発者が自ら評価することは妥当ではなく，「専門知識を有する中立的立場の第三者」が客観的に品質評価を行い，専門知識を持たない利用者にも理解できる説明を提示する仕組みが必要である［IPA］．

※奈良先端科学技術大学院大学, Nara Institute of Science and Technology

我々は，ソフトウェア品質の第三者評価の技術基盤の確立に向けて，ソフトウェアやその品質が実現される過程を解析・可視化するための概念「ソフトウェアプロジェクトトモグラフィ」を提唱・構築してきた[IPA2012][IPA2013]．ソフトウェアプロジェクトトモグラフィでは，ソフトウェア開発プロジェクトを，多様なプロジェクトデータとその解析結果から成るスナップショットの系列で表現する．スナップショットの系列から開発体制や開発速度などの俯瞰的な解析，また，特定のスナップショットから開発中に発生したイベントの解析を支援する．

本論文では，ソフトウェアプロジェクトトモグラフィを構成する要素技術である「ソフトウェア開発データの客観的な解析・可視化」を実現するための新たな可視化方式“Treemap Forest”を提案し，プロトタイプシステムを開発した．Treemap Forestの効果について被験者実験を行った．続く２節ではソフトウェア開発データに対する探索的データ解析の課題を，３節では課題を解決する可視化方式の設計を示す．４節でそのプロトタイプ実装について述べ，５節で実験設定を示し，その結果を６節に示す．

2　探索的データ解析

2.1　ソフトウェア品質評価のための探索的データ解析

昨今のソフトウェア開発では，版管理システム，課題管理システムなどを活用した開発データ（ソースコードの変更履歴，既知の欠陥情報など）が習慣的に記録されるようになりつつある．これらの開発データは膨大であり，その品質評価は第三者にとって工数のかかる作業である．従来研究では，膨大な開発データに対して，明確な分析目的を持たない状態で，データに潜むモデルや傾向を多角的に分析・評価する手法である探索的データ解析[Tukey]の有効性が評価されている．

ソフトウェア品質の第三者評価のために実施される探索的データ解析の主たる目的は，文献[IPA]における第三者評価のスコープのうち，①プロセス実施，②採用規格・技術の妥当性に対する検証的データ解析の前提となるモデルや基準の提供である．開発データは多変量データであることが多く，従来研究では，ソフトウェア開発データの多変量データから統計的に関連の強い変数を発見し，探索的データ解析を支援するツールHCE（Hierarchical Clustering Explorer）[Seo]の有効性が明らかにされている[大平]．

2.2　ソフトウェア開発の多次元データ解析

ソフトウェア開発データを解析する場合，課題，作業，成果物，人員など，異なる視点を同時に調査することが多い．具体的には図１のように成果物に関する「ソースコードの解析結果」や課題に関する「課題の優先順位や担当者」など，複数の二次元表で表される多変量データが解析対象となる．従って，開発データは関係データベース（RDB）のように，複数の表が共通に保持する要素（キー）で紐づけて取り扱うことが望ましい．しかし，多くの分析ツールや検証環境では複数の表を人手によって紐づけ，要素間の関係に潜む課題や特徴を解析しており，その分布や関係性の俯瞰的な把握は容易ではない．

本論文では，多変量データを俯瞰的に解析し，複数の多変量データの関係を探索的に解析する可視化方式を提案する．

ファイル名	行数	複雑度
Foo.java	241	31
Bar.java	122	15
Fizz.java	31	2
⋮	⋮	⋮

(a)成果物の表

課題ID	担当者	優先度
#1	Alice	高い
#2	Bob	低い
#3	Carol	高い
⋮	⋮	⋮

(b)課題の表

図１　課題と成果物に関する二次元表の例

3　可視化方式の設計

3.1　概要

本研究では，ソフトウェアトモグラフィが取り扱う多変量データについて，互いに関連する複数の多変量データを同時に可視化することで俯瞰的な可視化を実現する可視化方式を検討する．これは情報可視化における従来の原則“Overview first, zoom and filter, then details on demand”を実現する可視化方式であり，分析者がソフトウェア開発データを多角的な視点から効率的に解析を行う助けとなる．

本研究では，Treemap［Jenifer］と呼ばれる多次元データに対する可視化手法が持つ機能を，ソフトウェア開発データが持つ多変量・多次元データに合わせて拡張する可視化方式Treemap Forestを提案する．具体的には，以下の要件に基づいて，ソフトウェア開発データに対する新たな可視化方式の設計を行う．

(1)要素に含まれる特徴量の俯瞰的な提示

(2)要素間関係に基づく探索的データ解析の支援

3.2　要素に含まれる特徴量の俯瞰

二次元表で表されるソフトウェア開発データにおいて，特定の要素を構成する個々の項目が全体に占める割合や偏

りを解析することで，当該要素の特異点が発見される．

提案手法で利用するTreemapは，数値の比を面積の比として可視化する手法である．例えば図２は，Eclipseプロジェクトを対象に，モジュール別の課題数の比を可視化したもので，個々の矩形は各モジュールを，その面積は課題数を表している．以降，個々の矩形を「項目」，面積を決める量的属性を「尺」と呼ぶ．加えて，項目のソフトウェア開発データにおける分類（モジュールならば，成果物）を「要素」と呼ぶ．この表記に従うと図２は，「要素：成果物，項目：モジュール，尺：課題数」についてのTreemap可視化図である．

Treemapでは，同じ「成果物」の要素であっても異なる項目（例えば，ファイル，クラス），異なる尺（複雑度，コード行数）を指定できる．

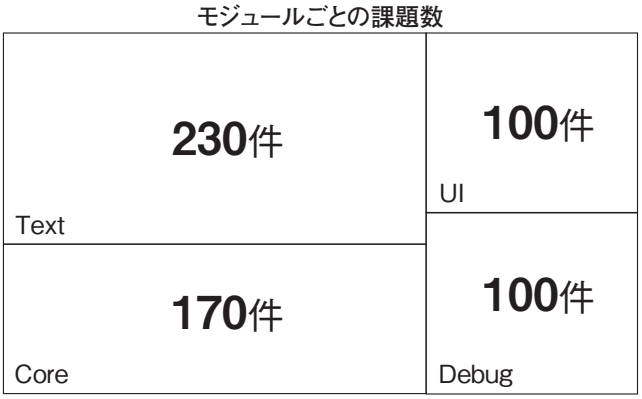


図２　Treemapの概略図

3.3　要素間関係に基づいた探索的データ解析

ソフトウェア開発データ中に出現する要素は，ほかの要素と関係している．例えば「開発者」は「課題を担当する」と「成果物を編集する」といったように，ほかの要素（課題，成果物）と関係する．従来，このような関連づけの作業は人手で複数の表を参照して行われてきたが，表の数が増えるにつれ現実的な方法ではなくなる．

Treemap Forestでは，RDBにおけるキーの機能を用いてこれらの関係を表現し，関係性に基づいて画面上に複数のTreemapを展開することで，作業の負担を軽減する．複数のTreemapを，データの関係に基づいて同時に展開する実際のイメージを，図３に示す．

図３上図は，各開発者が担当したプロジェクトの数についてのTreemapである（要素：組織，項目：開発者，尺：担当プロジェクト数）．

ここで，例えば分析者が開発者Aに注目して分析を行いたい場合，Treemap Forestでは開発者Aを表す矩形の内部に，開発者Aに関する新たなTreemapを入れ子状に展開できる．

図３下の各図は，それぞれ，開発者Aと関連する各要素について新たなTreemapを展開した際の図である．図中の赤枠部分の内側に新たなTreemapが展開されており，注目されていない開発者B・Cについては以前のままの要素・項目・尺度の組が選択されている．

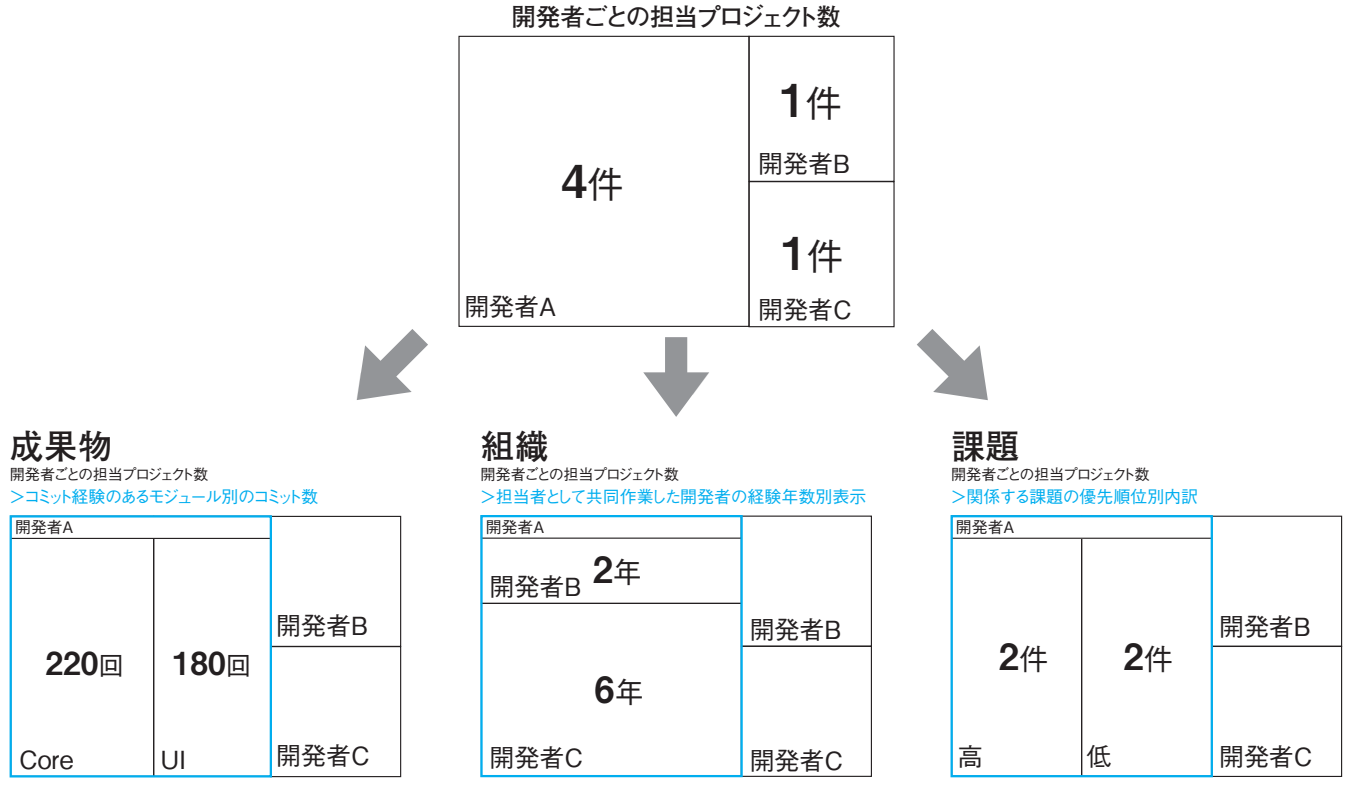


図３　外部キーを利用したTreemapの入れ子

図３下の各図で展開された新たなTreemapを構成する要素，項目，尺の組を次に示す．

- 左　：要素（成果物），項目（モジュール），尺（コミット数）の場合
- 中央：要素（組織），項目（共同作業を行った開発者），尺（経験年数）
- 右　：要素（課題），項目（優先順位），尺（課題数）

入れ子にしたTreemapを更に展開していくと，際限なく要素間の関係を可視化できるが，一方でひとつのTreemapの面積は小さくなり，視認性が下がると考えられる．そこで，Treemap Forestでは，ひとつのTreemapを選択して，画面全体へ拡大する機能（ズームアップ機能）を提供することで，この影響を排除する．

4　プロトタイプシステムの実装

我々は，設計した方式の有効性を評価するため，提案するソフトウェア開発データ可視化方式Treemap Forestのプロトタイプシステムを開発し，その有用性を確認した．本節では，Treemap Forestのプロトタイプシステムの概要を述べる．

4.1　システムの構成要素

本プロトタイプシステムは，可視化方式Treemap Forestを実装したものであり，ソフトウェア開発中に記録される要素（成果物，組織，課題，作業）に関する二次元表データの特徴を俯瞰的に提示し，更に，おのおのの二次元表データ間に紐づけられた情報を用いて，ほかの要素との関係，分布を提示する．分析者は，容易に複数の要素間の関係や特徴を俯瞰的に把握し，探索的データ解析を実現する．

4.2　システムの構成要素

プロトタイプの構成要素を図４に示す．それぞれの構成要素を述べる．

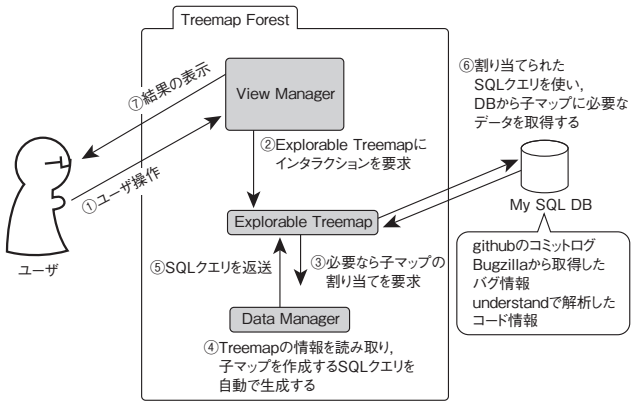


図４　Treemap Forestの構成

ViewManager：分析者の入力(要素,項目)を受け付け，ExplorableTreemapによって生成されたTreemapを提示する．

ExplorableTreemap：分析者の入力をDataManagerに受け渡して得たSQLクエリを用いてDBに問い合わせ，返却された値によってTreemapを構成する．

Treemapの構成には，Ben Fryが開発したTreemapライブラリを用いている．同ライブラリは，Martin Wattenberg，Ben Bedersonらが開発したJava用のライブラリをProcessing用に改造したもので，MPLライセンスの下配布されている．

DataManager：ExplorableTreemapから受け付けた入力情報をもとにSQLクエリを生成する．

DB：ソフトウェア開発データを関係データベース管理システムMySQLで一元管理する．

4.3　システムの操作と特徴

可視化方式Treemap Forest，及び，開発したプロトタイプの操作と特徴を述べる．

分析者は，評価対象プロジェクトの詳細，また，プロジェクトから収集された開発データの詳細を把握しておらず，品質評価において調査すべき事柄を知る手がかりがない．従って，Treemap Forestのプロトタイプでは，起動後に要素選択を行うと，項目，尺はランダムに決定され可視化結果が出力される．もちろん可視化後に，手動で項目，尺を変更することが可能である．図5は起動後に項目（課題）を選択後の出力結果で，優先順位別の課題数が表示されている．ここで，P１からP５は課題の優先順位のレベルを示す（P１が最も高くP５が最も低い）．

分析者がある項目とほかの要素の関係を解析する場合，新たに展開するTreemapの要素を選択する必要がある．プロトタイプシステムでは，項目をクリックすることで，各要素を表す扇形のボタン（上：組織，右：課題，左：成果物）を組み合わせた円形の要素セレクタを用意した．要素が選択されると，項目内に新たな Treemapが展開される．例えば図７は，図６に示されるセレクタで要素（成果物）を選択し，項目としてモジュール，尺として課題数が選ばれた場合に得られた出力であり，優先順位３の課題すべてについて，その課題数をモジュール別に表示したものと解釈できる．

プロジェクトの内容について俯瞰的な解析を繰り返した後も，ランダム性の機能は偶発的発見のために役立つ．もし分析者が望まない項目，尺を選択した場合は，項目，尺を選択しなおすための機能を用いて解決することができる．

最終的に，評価者は複数の要素間に見られる関係性を次々と可視化していく過程で，「最も複雑度の高いソースコードを担当した開発者」のような多要素にまたがる探索的データ解析を，従来手法（Excelなど）に比べて短時間で実現できる．

図5　優先順位別の課題数

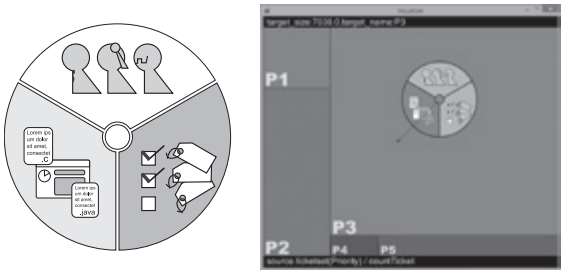


図6　要素セレクタ（左）と表示例（右）

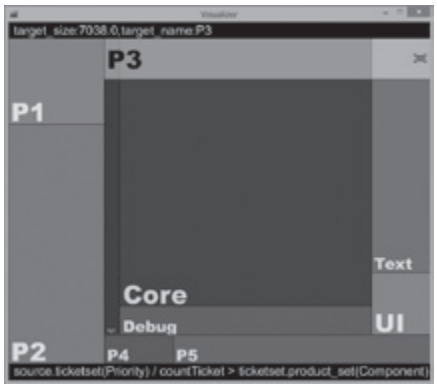


図7　優先順位３の課題のモジュール別課題数

5　被験者実験

5.1　概要と目的

ソフトウェアトモグラフィ可視化方式Treemap Forestを利用することで，ソフトウェア品質第三者評価の初期段階における，効率的な探索的データ解析の実現を評価するために被験者実験を行った．

実験では，分析対象のプロジェクトに対する深い知識を持たず，Treemap Forest，及び，そのプロトタイプの操作を初めて行う被験者が，(1) Treemap Forest，及び，プロトタイプを利用することで，プロジェクトデータの概要を短時間で探索できるか，(2) Treemap Forestを利用することで，プロジェクトの特徴，複数の要素に関係する知見を得ることができるか，を調べるため，二種類の実験を行った．

被験者を二群に分け，ある群ではTreemap Forestを，もう一方の群ではExcel 2013を用いて同内容の実験を行う．

実験１では，「最も関連チケット数の多いコンポーネント名を答えよ」のような，プロジェクトデータについての質問に回答するタスクを計６個用意し，それぞれのタスクにかかる時間を計測する．

実験２では，分析対象のソフトウェア開発に直接精通していない，ソフトウェア工学研究者が解析することを想定してプロジェクトデータを自由に探索してもらい，有用と思われる知見を発見してもらう．

実験結果の分析は，タスク完了時間，発見した知見の数・性質を比較する．

表１　実験に用いたプロジェクトデータ
（主キー，外部キーは他表との関係を表す）

要素	表	項目	尺
課　題	課題表	課題ID（主キー）	ー
		担当開発者名（外部キー）	関係チケット数
		報告開発者名（外部キー）	関係チケット数
		モジュールID（外部キー）	関係チケット数
		進捗状態	チケット数
		解決状態	チケット数
		チケット種別	チケット数
		優先順位	チケット数
組　織	開発者表	開発者名（主キー）	被割当てチケット数
成果物	ファイル表	ファイルID（主キー）	行数
			合計複雑度
			最大複雑度
			平均複雑度
			コメント割合
		モジュールID（外部キー）	所属ファイル数
	モジュール表	モジュールID（主キー）	総行数
			平均複雑度
			最大複雑度
			コメント割合
			継承ツリーの深さ
作　業	コミット表	コミットID（主キー）	ー
		モジュールID（外部キー）	コミット数
		開発者名（外部キー）	コミット数

5.2　対象データ

可視化対象の開発データはオープンソースソフトウェアであるEclipse JDTプロジェクトから収集した．各データは課題追跡システム，版追跡システム，そしてテクマトリックス社のソースコード解析ツール「Understand Ver.2.6※」から別々に得られた計５つの表から成る．表１に，対象データの構成を表す．本実験データでは，要素（作業）に紐づく項目・尺が存在しないため，これを可視化の対象としない．ただし，作業に関する表は利用される．

※Understand：http://www.techmatrix.co.jp/quality/understand/

表２　実験１における質問の一覧

Q１	チケットのPriorityについて，最もありふれたものはどれか
Q２	UIコンポーネントで最も複雑度の高いファイルの複雑度は幾つか
Q３	Enhancementチケットは全部でいくつあるか
Q４	Debugコンポーネントに多くコミットした主要な開発者の名前を５名挙げよ
Q５	UIコンポーネントに多くコミットした５人の開発者の中に，ひとり，ほとんどのチケットが解決できていない開発者が居る．特定せよ
Q６	最もチケット数の多い３つのコンポーネントについて，チケットの進捗状況に違いがあればそれを述べよ

5.3　被験者

被験者は，ソフトウェア工学，データマイニングに関連する研究に取り組む大学院生８名（修士課程７名，博士課程１名）である．それぞれの被験者は，プロジェクトに含まれるデータに対して，個人差はあるものの一定以上の知識を持つものである．また，被験者はいずれもExcelを用いたデータ分析，関数などの利用経験がある．一方で，本実験以前にTreemap Forestの使用経験は一度もない．

5.4　実験１

実験１では，5.1節で述べた(1)並びに(2)の一部を検証するため，プロジェクトデータに関する質問（計６個）を与え，解答までにかかった時間を測定する．Excelを利用する被験者は実験中にヘルプを参照することができ，Treemap Forestを利用する被験者は操作法に関するガイドを読むことができる．実験で用いた質問を表２に示す．なお，一問に15分以上かかった場合は解決不能とみなし，次のタスクに進んでもらう．

６つの質問のうち，Q１～Q３はTreemap Forestでは単一のツリーマップを見るだけで答えられる．Excelにおいても，一つの表を操作して答えられる．Q４～Q６は，Treemap Forestではツリーマップを何段か入れ子にする必要があり，Excelにおいては，複数の表を操作して答える必要がある．

5.5　実験２

実験２は5.1節で述べた目的(2)を検証するために，対象プロジェクトの開発データを自由に探索してもらい，有用と思われる知見を発見してもらうものである．本実験における知見は，研究者による第三者評価を想定しているため，プロジェクトの成功・失敗に関する状態や特徴的な要素について述べるものである．知見の例として実験開始前に被験者に提示したものを次に挙げる．

- UIコンポーネントに属するファイル群は，全体的に複雑度が均質であり，ファイルの切り分けがうまく行われたのではないか
- APTコンポーネントにおいて，優先順位の高いチケットはほとんど解決済みであり，優先順位づけがうまく働いているようだ

探索を行う時間は15分とし，Treemap Forestを用いる被験者は生成した知見をスクリーンショットと共に，Excelを用いる被験者は表から取得したデータと共に，記録してもらう．

5.6　実験手順

被験者は順に部屋に呼ばれ，Treemap Forest若しくはExcelについて20分程度の解説を受ける．次に，対象データに含まれるデータ数や，どのような表・要素が用意されているかの解説を受ける．Excelを用いる被験者には，操作法に関する知識の多寡が実験結果に影響を与えないよう，フィルタ機能の利用方法について教えた上で，ヘルプの使用が認められていることを伝えた．

その後，実験１，実験２の順番で実験を行う．

6　結果と考察

6.1　実験１の結果

実験１の質問／ツール別の解答時間を図８に示す．図中の各点は，質問ごとの被験者の解答時間（縦軸）を表す．また，制限時間を超えた場合，15分としてプロットしている．各被験者の詳細な解答時間と回答失敗数は，表４，５に示す．

表３，４から，Treemap Forestを使ったプロトタイプを利用した被験者群は，Excelを利用した被験者群の38%程度の時間で解答できており，Treemap Forestによって短時間でソフトウェア開発データを参照できることが分かる．

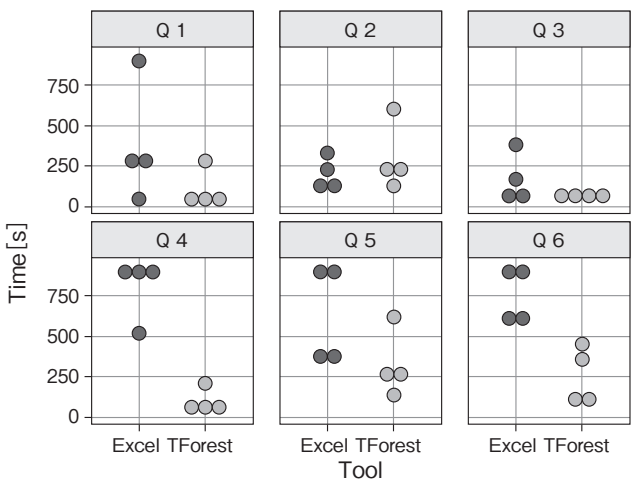


図８　各質問のツール別解答時間

表3　Treemap Forestによる解答時間（分：秒）

	A	B	C	D	平均
Q 1	05 : 21	00 : 43	00 : 28	00 : 46	01 : 49
Q 2	10 : 02	04 : 11	02 : 12	03 : 14	04 : 55
Q 3	01 : 34	00 : 27	00 : 27	00 : 48	00 : 49
Q 4	03 : 29	01 : 00	00 : 59	01 : 04	01 : 38
Q 5	04 : 14	10 : 21	04 : 38	02 : 18	05 : 23
Q 6	05 : 58	01 : 43	01 : 59	07 : 33	04 : 18
合計	30 : 38	18 : 25	10 : 43	15 : 43	18 : 52
回答失敗	0	0	0	0	0

※背景青は最小，グレーは最大.

表4　Excelによる解答時間（分：秒）

	E	F	G	H	平均
Q 1	–	01 : 03	04 : 03	04 : 36	>06 : 10
Q 2	05 : 32	04 : 24	01 : 35	02 : 39	03 : 33
Q 3	06 : 21	01 : 43	00 : 42	02 : 48	02 : 53
Q 4	–	08 : 39	–	–	>13 : 25
Q 5	–	06 : 13	–	06 : 20	>10 : 38
Q 6	–	–	10 : 39	09 : 46	>12 : 36
合計	71 : 53	37 : 02	46 : 59	41 : 09	49 : 16
回答失敗	4	1	2	1	2.25

※背景青は最小，グレーは最大.

表5　Treemap可視化図のみによる解答時間（分：秒）

	E	F	G	H	平均
Q 1	01 : 58	02 : 11	01 : 53	00 : 29	1 : 38
Q 3	03 : 23	01 : 35	01 : 48	01 : 39	1 : 57

※背景青は最小，グレーは最大.

正答数に着目すると，Treemap Forestを利用した全被験者は，すべての質問を時間内に正答していた．一方で，Excelを利用した被験者は全問正解者が居なかった．とくに，単一の表を見れば答えが分かるQ 1からQ 3においては被験者Eの一問不正解を除いて正答であったが，複数の表を閲覧しなくてはならないQ 4からQ 6では全体で7件失敗していた．このことから，Excelの場合，開発データの俯瞰や調査に時間がかかり，場合によっては正しい情報を得られないことが明らかになった．

6.2　実験2の結果

実験2において報告された知見はTreemap Forestで平均2.5件，Excelで2件と，大きな差が見られなかった．生成された知見と，知見を発見するために参照された要素を表6及び7に示す．

システムによって生成される知見の質や，言及される領域が異なるかに着目すると，Treemap Forestでは同一の被験者でも知見2や3のように課題や開発者，コンポーネントといった多様な要素に言及している一方，Excelを利用している被験者は知見2や7など，すべての被験者が単一の要素（課題表）から得られる知見のみを報告していた．

課題表は，実験データ中で最も属性の数が多い表であるため，Excelを利用した群はこの表から有用な知見を得られると感じた可能性がある．こうした分析は，要素間の紐づけにかかる手間を省き，仮説の生成数を上昇させる反面，Excelを利用した被験者にとって，成果物や作業といった要素に紐づいた量的属性，あるいは要素間の関係は見落としやすい部分であることを示唆している．

6.3　考察

実験1の解答時間・正答について質問別に見ると，ほぼすべての質問でExcelよりTreemap Forestの最小・最大・平均

表6　Treemap Forestで生成された知見（項目・表は関連する要素・表の頭文字, 例：モジュール表なら「モ」）

	生成された知見	要素	表
1	10人程度の比較的積極的な開発者によって運営されている	組/作	コ
2	各開発者が特定のモジュールに集中して，役割分担が行われている	組/成/作	コ/モ
3	コミット数が多いが，課題の割り当て数が少ない開発者が居る	組/課/作	課/コ
4	複雑なモジュールには未解決の課題が多い	成/課	モ/課
5	課題の割当が特定の開発者に集中しており，割り当てに問題がある	組/課	課
6	課題数最大のUIモジュール以外では，未解決課題が多い	成/課	モ/課
7	高優先順位な課題は解決済であり，品質が高い	課	課
8	多くの課題を割り当てられ，ほとんど解決済の，熟練した開発者が居る	組/課	課
9	機能拡張に関する課題は優先順位が低い	課	課

表7　Excelで生成された知見（項目・表は関連する要素・表の頭文字, 例：モジュール表なら「モ」）

	生成された知見	要素	表
1	Major課題の半分弱は優先順位が3以下であり，優先順位の割当てに問題がある	課	課
2	不具合修正課題の半分以上が解決済であり，品質向上意識が高い	課	課
3	機能拡張課題は全体の20%しか解決しておらず，やや消極的である	課	課
4	1832件も課題を抱えている開発者がおり，負担がかかっている	課/組	課
5	Coreに関する優先順位3以上の課題は解決済であり，優先順位が上手に働いている	課/成	課
6	特定の3人の開発者は600以上の課題を割り当てられているが，報告課題数が0であり，活動的ではない	課/組	課
7	UIモジュールは課題報告の重複が多い	課	課
8	UIを除くモジュールでは，課題修正が滞っており，開発者が足りていない	課/組	課

解答時間が短いが，唯一Q２においてはExcelのほうが短時間で解答できている．原因として，Q２の解答には各領域のサイズを把握し，最大の要素を見つける必要があるにもかかわらず，解答候補となるファイルが複数あり，Treemap表現による視覚的な比較がうまく働かなかった可能性が考えられる．

このことはTreemapが，全体に対する構成要素の中で，とくに大きな割合を占める特異的な構成要素を発見することに向いている反面，値のよく似た複数の構成要素の厳密な比較に不向きであることに由来する．ただし，本手法は厳密な検証を実施する前に簡易なモデルや仮説を生成することを目的とした探索的データ解析であり，意図的に捨象している部分であるとも言える．

また，本手法の有効性が，Treemapによる表現と，データ間の関連づけやユーザ操作のどちらに由来するかを調査するため，単一の表から生成可能な（データ間の関係を考慮しない）可視化図のみを用いた追加実験を実施した．結果を表５に示す．

実験の結果，Q １では平均１分38秒と，提案手法より素早く解答できることがわかった．また，解答時間の最小値には１秒しか差がない一方，最大値には３分以上の差が見られた．一方，Q ３では平均・最小・最大解答時間共にTreemap Forestのほうが短かった．これらの結果は，Treemap Forestは提示できるデータや可能な操作が多く，ユーザによっては習熟に時間がかかることや，操作に慣れるにつれて素早く情報を提示できる可能性を示唆する．

実験２で生成された知見に注目すると，Treemap Forestを利用した開発者に比べて，Excelを利用した開発者は特定の項目（例えば，UIモジュール）に注目した分析を行い，その厳密な数値について述べる傾向があることが分かった．

また，Treemap Forestで生成された仮説と関係する最大要素数は３，表数は２であった．本制約には，実験の時間的制約や，被験者の習熟度，システムの見やすさなどが影響すると考えられる．

ただし，本実験で用いたデータセットは開発記録のごく一部であり，実環境においては要素数や表数が変動する可能性があり，結果の一般化は難しい．そのため，ツールの可用範囲や，生成される仮説にかかる制約を明確化することは，今後の検討課題となる．

7　おわりに

本論文では，「ソフトウェアプロジェクトトモグラフィ」を構成する要素技術である「ソフトウェア開発データの量的属性の探索的可視化」を実現するため，新たな可視化方式であるTreemap Forestを提案し，その効果についての被験者実験を行った．

オープンソース開発データ（Eclipse JDT）についての質問に解答する実験１の結果，提案手法はExcelと比較して38%程度の時間で質問に解答できることがわかった．一方，Excelでは，制限時間内に解答できないケースも多く，ソフトウェア開発データの探索的データ解析におけるTreemap Forestの有用性が示された．

データを自由に探索し得られた知見を報告する実験２の結果，Treemap Forestでは複数の表が参照された反面，Excelでは課題表のデータしか参照されておらず，Treemap Forestによって広範なデータから知見を集められることが示された．

本研究の制約として，実験の可視化対象データにオープンソースプロジェクトから取得したものを使っていることや，厳密な値の比較に不向きということがある．また，HCEなどほかの探索的データ解析ツールには，データに対して統計処理を行うものが存在するが，Treemap Forestは値の分布を示すのみで，高度な統計解析が行えないことにも留意する必要がある．

ただし，これらの点を考慮したとしても，多面的なデータに対する俯瞰を短時間で実施でき，また要素間の関係に基づく知見を得ることができるTreemap Forestには有用性があると考えられる．

今後の課題として，前述した制約の解決に加え，オープンソースプロジェクト以外の開発データを対象としたTreemap Forestの適用や，学生以外の被験者による評価について検討する余地がある．

謝辞

本研究の一部は，独立行政法人情報処理推進機構（IPA）「2013 年度ソフトウェア工学分野の先導的研究支援事業」の委託に基づいて行われた．

【参考文献】

[IPA] 情報処理推進機構, “製品・システムにおけるソフトウェアの信頼性・安全性等に関する品質説明力強化のための制度構築ガイドライン”（平25-6）.
[IPA2012] 2012 年度ソフトウェア工学分野の先導的研究支援事業「ソフトウェア品質の第三者評価のための基盤技術－ソフトウェアプロジェクトトモグラフィの開発－」成果報告書, http://www.ipa.go.jp/files/000026806.pdf
[IPA2013] 2013 年度ソフトウェア工学分野の先導的研究支援事業「ソフトウェア品質の第三者評価のための基盤技術－ソフトウェアプロジェクトトモグラフィ技術の高度化－」成果報告書, http://www.ipa.go.jp/files/000045268.pdf
[Tukey] J.W.Tukey, “Exploratory Data Analysis,” Addison-Wesley, 1977.
[大平] 大平雅雄, 伊原彰紀, 中野大輔, 松本健一, “ソフトウェア品質の第三者評価における探索的データ解析ツールの利用とその効果：OSSデータを対象とした検証実験”, SEC journal, Vol.9, No.4, 2014.
[Jenifer] Jenifer Tidwell, “Designing Interfaces,” O’Reilly Media, 2011.
[Seo] J. Seo, B. Shneiderman, “Interactively Exploring Hierarchical Clustering Results,” IEEE Computer, Volume 35, Number 7, pp. 80-86, 2002.

SEC 2015年度活動概要

SEC副所長 和田 恭　SEC次長 日下 保裕　SEC企画グループリーダー 千脇 誠司
SEC企画グループ主任 川原 翔

2015年度は、IPA第三期中期計画（2013年度～2017年度）の中間である3年度目として、IoT※1時代の動きを見据えた活動に一定の成果が表れてくるなど、中期計画で掲げた事業目標の達成に向けた活動が着実に実を結びつつある。本稿では、2015年度の主な成果概要を紹介し、本稿以降で詳しい事業内容を紹介する。

1 重要インフラ分野の情報処理システムに係るソフトウェア障害情報の収集・分析及び対策

(1) 重要インフラの障害情報共有体制に新たに3産業分野が加わり、共有体制は6産業分野に拡大

① 民間では収集が困難な障害事例情報を収集・分析し、普遍性・一般性のある教訓事例を導き出し、「情報処理システム高信頼化教訓集2015年度版」として公開した。

② 重要インフラ分野などにおける情報処理システムの類似障害の再発防止や影響範囲縮小につなげるため、航空分野（航空運航）、金融分野（生命保険）及び情報通信分野（ケーブルテレビ）の3産業分野で障害情報共有体制を構築し、共有体制は合計6産業分野に拡大した。

(2)「組込みソフトウェア開発データ白書2015」の発行及び「ソフトウェア開発データ白書」最新版の発行決定

① 組込みソフトウェア分野におけるプロジェクトデータ（174件）を取りまとめた「組込みソフトウェア開発データ白書2015」を発行した。

②「ソフトウェア開発データ白書」の最新版発行を目指し、新たに262プロジェクトの開発データを収集し、分析及び原稿案の作成が完了した。2016年度中に最新版を発行する予定である。

2 利用者視点でのソフトウェア信頼性の見える化の促進

(1) IoT製品の開発者が開発時に考慮すべきリスクと対策を公表

IoT製品の開発者が開発時に考慮すべきリスクと対策を取りまとめ、「つながる世界の開発指針」を策定し、一般公開した。また、上記開発指針の策定に向けて、IPA、一般社団法人日本ロボット工業会ORiN※2協議会及び一般財団法人機械振興協会の三者共同により、ORiN上で実証実験を実施し、その有効性を検証した。

(2) 設計の重要性や経営層の関与のあり方などを解説したガイドブックを発行

セーフティ・セキュリティ設計の重要性やリスク分析手法、見える化手法、経営層の関与のあり方などを解説したガイドブック「つながる世界のセーフティ＆セキュリティ設計入門」を取りまとめ、同書は有償販売、ダイジェスト版は無償でWeb公開した。

(3) 先進的な設計手法・信頼性検証手法・技術等の取り組み事例を公開

ソフトウェアの信頼性確保を実現するための先進的な技術・手法について、製造業、流通業、商社、情報通信業などの取り組み事例34件を収集した「先進的な設計・検証技術の適用事例報告書2015年度版」を公開した。

3 海外有力機関との更なる関係強化

これまで連携をしている海外代表的機関の米国NIST※3、米国SEI※4、米国MIT※5、独国IESE※6、英国MISRA※7との関係を更に強化した。

① NISTとは、2016年1月に定期協議をワシントンで開催し、CPS-WG関連活動の情報を収集した。

② SEIとは、2016年1月にピッツバーグの研究所内で、ソフトウェア開発データの共同分析にかかわる意見交換を実施した。

③ MITとは、2015年6月にNancy Leveson教授を講演者として招聘したSEC特別セミナー「システムベースのエンジニアリング最新動向」を開催し、講演「Engineering a Safer and More Secure World」及びパネルディスカッション「日本におけるSTAMP※8活用の仕方について」を実施した。

④ IESEとは、2015年9月にIPA側がドイツを訪問し、Industrie4.0※9の全体像及びIESEが分担する事業の状況について情報収集を行った。更に、2016年3月にもIPA側がドイツを訪問し、新規事業として準備を進めているシステムズエンジニアリング分野の調査や、「つながる世界の開発指針」策定を受けた国際相互運用性確認プロジェクト（実証実験）等に関する実務レベルでの最終調整を実施した。

⑤ MISRAとは、2015年10月に開催したセミナー「ソフトウェア品質向上のためのコーディング技法と標準」において、主要メンバであるAndrew Banks氏及びChris Tapp氏を講演者として招聘し、コーディング技法とその標準化に向けた活動を紹介した。

4 SEC成果の普及展開

(1) SECセミナーなどを通じたSEC成果の普及展開

業界団体などと連携し、SECセミナーを計68回開催した。また、地域・団体などからの要請に応じた講師派遣も継続し、きめ細かい支援を実施した。

(2) 外部イベント出展などを通じたSEC成果の普及展開

① ソフトウェア開発技術関連の技術展示会（ETWest 2015※10、ET2015※11など）に出展し、SEC成果や取り組みの紹介を行うなど、積極的に普及活動を実施した。また、本年度は、アジア最大級のIT／エレクトロニクス産業の国際展示会であるCEATEC JAPAN 2015※12に初出展し、SECのみならず、IPAの事業全般を広く紹介した。

② JAXA※13と共催で、第13回クリティカルソフトウェアワークショップ（13thWOCS^2※14）を開催した（2016年1月19日～21日）。今回は、「つながるクリティカルシステム」をテーマに掲げて、セミナー、講演及びコンテストを開催した。

【脚注】

※1 IoT（Internet of Things）：モノのインターネット

※2 ORiN（Open Resource interface for the Network）：製造現場の各種装置に対して、メーカや製品の違いを越えて統一的なアクセス手段を提供するソフトウェア

※3 NIST（National Institute of Standards and Technology）：米国商務省国立標準技術研究所

※4 SEI（Software Engineering Institute）：米国カーネギーメロン大学ソフトウェア・エンジニアリング研究所

※5 MIT（Massachusetts Institute of Technology）：米国マサチューセッツ工科大学

※6 IESE（Institute for Experimental Software Engineering）：独国フラウンホーファー研究機構実験的ソフトウェア・エンジニアリング研究所

※7 MISRA（The Motor Industry Software Reliability Association）：自動車メーカ、部品メーカ、研究者から成る欧州の自動車業界団体

※8 STAMP（Systems-Theoretic Accident Model and Processes）：システム理論に基づく事故モデル

※9 Industrie4.0：ドイツ連邦政府が実施しているイノベーション推進政策の一部である産学官プロジェクト。本プロジェクトは、1970年代の「第3次産業革命」（エレクトロニクス・自動生産化）に続く、「第4次産業革命」と位置付けられている。

※10 ETWest2015（Embedded Technology West 2015）：組込み総合技術展　関西

※11 ET2015（Embedded Technology 2015）：組込み総合技術展

※12 CEATEC JAPAN 2015（Combined Exhibition of Advanced Technologies）

※13 JAXA（Japan Aerospace eXploration Agency）：国立研究開発法人宇宙航空研究開発機構

※14 WOCS^2（Workshop on Critical Software Systems）：クリティカルソフトウェアワークショップ

情報処理システムの信頼性向上に向けて

SECシステムグループリーダー　山下 博之

1 2015年度の活動概要

サイバー攻撃をはじめとするセキュリティの脅威の増大に対する施策が進められる中で、情報処理システムの障害もまた増加傾向にあることから、その信頼性向上に向けた取り組みを引き続き推進した。その主なものは、表１に整理する、データに基づく管理である。具体的には、同表に黒字で示す、システム障害事例を収集・分析し、その結果得られた再発防止策等を「教訓」として幅広く共有すること、及びソフトウェア開発データを収集し、その分析結果をプロジェクト管理やプロセス改善に役立てることである。また、システム構築の上流工程におけるプロセスを強化するための新たな取り組みを開始した。これらの取り組みは、図１に示す部会/WG体制の下で実施した。

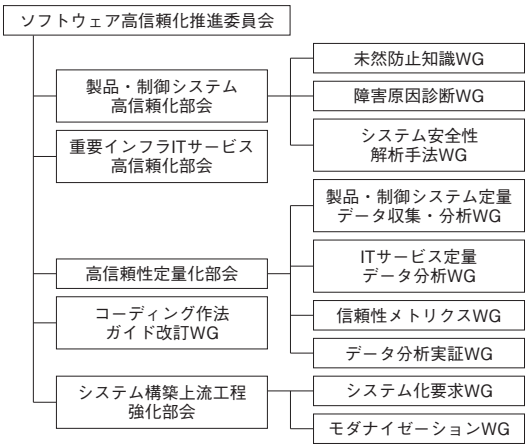
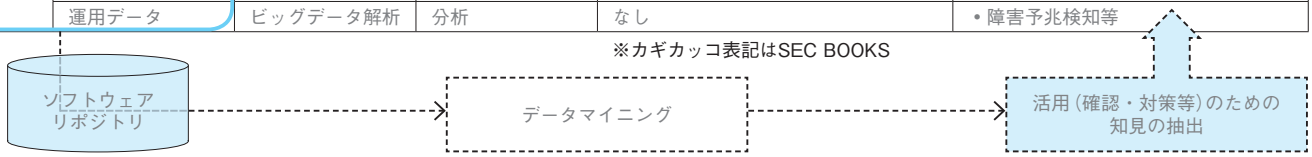


図１　システムグループの部会/WG体制

表１　データに基づく管理の分類

データ		手　法		見える化ツール（IPA成果）	主な活用方法
定　性	作業日報等	ビッグデータ解析	分析	なし	• 因果関係確認等
定　性	失敗/成功事例		分析	• チェックリスト（「ITプロジェクトの見える化」，信頼性自己診断ツール） • 情報処理システム高信頼化教訓集	• 妥当性確認（問題点抽出） • 障害再発防止策
定　性	障害事例		分析		
定　量	開発データ	インプロセス計測	品質管理	• 「定量的品質予測のススメ」 • 定量的プロジェクト管理ツール	• 異常の予兆検知
定　量	開発データ	インプロセス計測	プロジェクト管理		• 比較による計画策定・妥当性確認 • 因果関係明確化によるプロセスや組織等の改善
定　量	開発データ	ベンチマーキング	分析	• 「ソフトウェア開発データ白書」 • 開発データが語るメッセージ	
定　量	運用データ	ビッグデータ解析	分析	なし	• 障害予兆検知等

※カギカッコ表記はSEC BOOKS



2 ソフトウェア障害事例の収集・分析と再発防止策の導出・活用

ITサービスシステム及び組込みシステムの障害事例を収集・分析し、随時公開すると共に、最終的に計16件を２種の教訓集に追加して公開した。また、これまでの活動を整理し、障害事例から教訓を作成するため、及び教訓集を障害の未然防止に役立てるためのガイドを計４編公開した。さらに、多数のコンポーネントから成る複雑なシステムを対象とする事前のハザード分析や、事後の障害原因診断のための手法などについて検討し、それぞれガイドに取りまとめて公開した。

3 定量的プロジェクト管理

ソフトウェア開発データの統計分析に基づく傾向を示す従来のデータ白書に対し、新たに、信頼性向上に向けた開発プロセスや組織の改善のための分析結果を取りまとめたメッセージ集を公開した。また、有用な分析手法の発見と共有を目的に、開発データ提供企業が自らIPA/SECに蓄積されたデータを分析する活動を開始した。更に、組込みソフトウェアを対象とするデータ白書を初めて公開した。

4 システム構築上流工程のプロセス強化

情報処理システムに求められる要求の不確実さが増大するIoT時代を見据え、その構築の上流工程のプロセス等を強化する取り組みを開始した。ビジネス環境の変化が大きく予測しにくい状況においても、プロジェクトの失敗を減らし、サービスの信頼性を損なうことなくそのシステムに新たな要求を取り込みやすくするために、受発注者間で再構築リスクを共有すると共に、要求分析・要件定義を着実に行うことなどを主目的とする。

重要インフラ等システム障害対策

SEC調査役 三縄 俊信　SEC研究員 加藤 均　SEC研究員 目黒 達生
SEC主任 八嶋 俊介　SEC調査役 三原 幸博　SEC調査役 石田 茂
SEC調査役 十山 圭介　SEC調査役 石井 正悟　SEC研究員 松田 充弘
SECシステムグループリーダー 山下 博之

前年度に引き続き、重要インフラ分野等のシステム障害事例からヒアリングなどにより障害事例情報を収集し、その分析と対策の検討を行った。その結果、ITサービスシステム分野からは９件、機器の制御を行う組込みシステム分野からは７件の産業分野横断で活用可能な普遍的な教訓を導出し、前年度までの教訓と併せて分類整理した上で教訓集として公開した。また、教訓集等を自社内で活用するため、及び障害の未然防止に役立つ教訓を自ら作成し継続的に運用していくためのガイドブックを作成し公開した。更に、ITサービスシステムの障害事例情報を共有する仕組みの構築に向けた支援活動を行い、新たに３つの産業分野で情報共有の仕組みを構築し運用を開始した。

ITサービスシステム

1 背景

情報処理システムは、銀行や証券などの金融サービス、各種手続きのための行政サービス、ソーシャルネットワーク等の情報通信サービス、交通機関の運行制御など、私たちの生活や社会・経済基盤を支える重要インフラ分野等のITサービスに深く浸透し、ひとたび障害が発生するとその影響は非常に大きい。私たちが安全で安心な生活や社会・経済活動を続けるためには、重要インフラなどを支えるITサービスの一層の信頼性向上が求められている。

報道されたITサービス障害の発生件数は、図１に示すように、2009年から2015年にかけて増加傾向にあり、特に2015年度は、マイナンバー関連等のシステム稼働直後の初期障害が多く発生した。

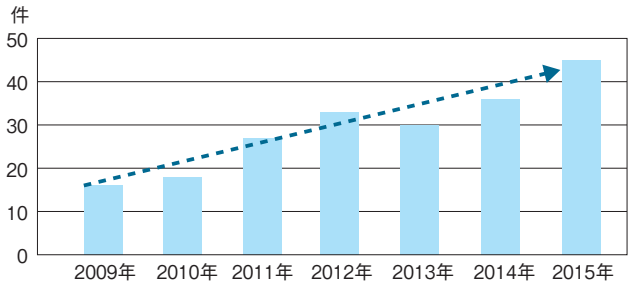


図１　報道されたITサービス障害の発生件数の推移

従来、情報処理システムの障害に対する原因分析と再発防止対策の実施は、多くの場合、当事者においてのみ行われ、その情報は公開されてこなかった。そのため、他業界・分野のシステムなど、当事者以外のシステムにおいて、類似の障害が発生することがあった。

情報処理システムの構築・運用やその管理は、社会や技術の進展につれて複雑化・多様化しており、一個人や一企業のカバーできる範囲には限界がある。そして、その複雑性・多様性は今後ますます拡大していくことは明らかである。従って、情報処理システムの構築・運用及びその管理にかかわる信頼性面での課題を解決するために、より多くの人たち・企業の経験を社会全体で共有・伝承することが求められている。

そこでIPA/SECでは、システムの障害事例情報の分析や対策手法の整理・体系化を通して得られる「教訓」を業界・分野を超えて幅広く共有し、類似障害の再発防止や影響範囲縮小につなげる仕組みの構築に向けた活動を2013年度から実施している。

2 障害事例の収集と教訓化

2015年度も継続して重要インフラITサービス高信頼化部会※1の活動を通じ、ITサービスシステム分野における障害事例を収集し、障害原因の分析を行い普遍化した上で９件の教訓を導出した（表１、表２）。これらを2014年度に取りまとめた教訓27件に追加して、計36件の教訓を収録した「情報処理システム高信頼化教訓集（ITサービス編）2015年度版」（以下、教訓集2015）を公開※2した。

表１　2015年度に導出した教訓の分野別件数

産業等分野	教訓数
情報通信分野	１件
金融分野	４件
行政・自治体分野	３件
その他	１件
計	９件

【脚注】
※1　重要インフラITサービス高信頼化部会：銀行、保険、証券、電力、鉄道、情報通信、政府・行政などの情報処理システムの有識者・専門家で構成する委員会
※2　URL: http://www.ipa.go.jp/sec/reports/20160331_1.html

表2　2015年度追加教訓（ITサービス編）

ID	教訓概要
ガバナンス／マネジメント領域	
G10	関係者からの疑義問合せは自社システムに問題が発生していることを前提に対処すべし！
G11	システムの重要度に応じて運用・保守の体制・作業に濃淡をつけるべし
G12	キャパシティ管理は、業務部門とIT部門のパートナーシップを強化すると共に、管理項目と閾値を設定してPDCAサイクルを回すべし
G13	キャパシティ管理は関連システムとの整合性の確保が大切
G14	設計時に定めたキャパシティ管理項目は、環境の変化に合わせて見直すべし
技術領域	
T19	リレーショナルデータベース（RDBMS）のクエリ自動最適化機能の適用は慎重に！
T20	パッケージ製品の機能カスタマイズはリスクを認識しとくに必要十分なチェック体制やチェック手順を整備して進めること
T21	作業ミスを減らすためには、作業指示者と作業者の連携で漏れのない対策を！
T22	隠れたバッファの存在を把握し、目的別の閾値設定と超過アラート監視でオーバフローを未然に防止すること

教訓作成に当たり、2015年度に報道されたシステム障害事例について当事者にヒアリングし、教訓化の了解を得た事例について匿名化・一般化を行った。ヒアリングを行ったシステム障害事例は下記。

- 電気通信事業者の通信システム障害
- 自治体コールセンタのシステム障害
- 金融機関のオンラインシステム障害
- 地方公共団体のICカード管理システム障害

更に、導出した教訓について、ITIL※3をベースとした国際規格JIS Q20000-1:2012※4によるサービスマネジメント分類との対応付けを実施した（表3）。

表3　追加教訓とITサービスマネジメントの対応

No.	JIS Q20000-1：2012より（●主な問題個所、△関連する問題個所）												
	5．新規またはサービス変更の設計及び移行	6．サービス提供プロセス					7．関係プロセス		8．解決プロセス		9．統合的制御プロセス		
		サービスレベル管理	サービス継続・可用性管理	サービス報告	容量・能力管理	情報セキュリティ管理	事業関係管理	供給者管理	インシデント管理	問題管理	構成管理	変更管理	リリース管理
G10							△		●				
G11			△								●		
G12			△		●								
G13			△		●							△	
G14			△		●								
T19	●				△								
T20	△							●					
T21	△										△	●	
T22			●		△						△		

これと同様に、教訓集2015に収録した教訓を分類したところ、統合的制御プロセスの構成管理、変更管理、サービス継続・可用性管理、容量・能力管理のプロセスに問題が多いことが分かった。

また、障害分析手法については、ヒューマンエラーに起因するシステム障害の分析手法としてImSAFER※5を調査し詳細な解説を追加した。このほか、STAMP※6に関する分析手法（STPA※7、CAST※8）を調査し、より具体的に活用できるよう解説を追加した。障害対策手法については、新たに3件を追加（表4）し、計23件とした。

表4　新たに追加した障害対策手法

追加した対策手法
障害再発防止のための組織的マネジメント
RDBシステム管理
ヒューマンファクターズ

3　システム障害情報共有の仕組み構築

各業界団体等にシステム障害情報の共有の仕組み構築を働きかけ、2015年度に新たに3つの情報共有グループを構築し、その運営を開始した。

（情報通信分野）

一般社団法人日本ケーブルテレビ連盟（正会員オペレータ370社）が連盟内に構築する運用情報共有システムを利用した障害情報共有の仕組みの活性化に向けて、IPA/SECが事例情報提供などの支援を行う活動を開始した。

（航空分野）

航空運航システム研究会（TFOS.SG※9（航空に関心のある学識経験者や技術者、パイロットなどで組織する民間研究団体））が「航空システム障害事例の分析に基づく教訓作成」を行うことを決定し、配下の航空システム部会とIPA/SECの協業により、航空システム障害事例を教訓化し情報共有すべく活動を開始した。

（金融分野）

一般社団法人生命保険協会の協力のもと、障害情報共有の取り組みに賛同する生命保険会社16社で構成するメーリングリストを使用した情報共有を行うこととし、その運用を開始した。

また、2014年度に運用を開始した3つの情報共有グループ（行政・電力・情報通信分野）についても、IPA/SECによる支援活動・意見交換を継続して実施した。

【脚注】

※3　ITIL：Information Technology Infrastructure Library、ITサービスマネジメントのベストプラクティス集で、ITサービスを提供するためのガイドライン
※4　JIS Q20000-1:2012：ITサービスを提供している組織が、サービスの内容やリスクを明確にすることで、ITサービスの継続的な管理、高い効率性、継続的改善を実現するための国際規格、ISO/IEC20000-1:2011対応
※5　Improvement for medical System by Analyzing Fault root in human Error incident
※6　Systems-Theoretic Accident Model and Processes（システム理論に基づく事故モデル）
※7　System Theoretic Process Analysis
※8　Causal Analysis using System Theory
※9　TFOS.SG：Total Flight Operation System Study Groupの略称

4 ガイドブックの作成

自社内で発生したシステム障害事例の原因分析を行い再発防止策などを「教訓」として作成するための手法をまとめた「情報処理システム高信頼化教訓作成ガイドブック（ITサービス編）」（以下、教訓作成ガイドブック）、及び自社で作成した教訓のほか、IPA/SECや他社などの第三者が提供する教訓を自社内で活用するための手法をまとめた「情報処理システム高信頼化教訓活用ガイドブック（ITサービス編）」（以下、教訓活用ガイドブック）を公開※10した。

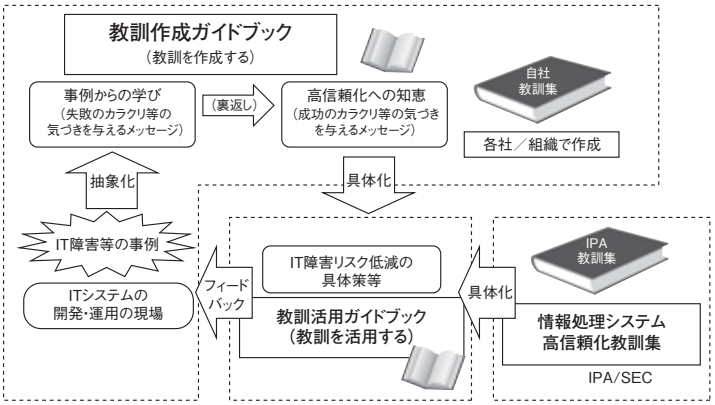


図2　教訓集2015とガイドブック2編

5 普及展開活動

① 新着教訓の逐次公開

教訓集に収録されている各教訓をインデックスからタイムリーに参照・利用可能となるようにIPA/SECのWebページ上に教訓リンク集を構築した。また、2015年度に作成した新しい教訓９件を前述の教訓集公開に先駆けてこの教訓リンク集に新着情報として逐次公開した。

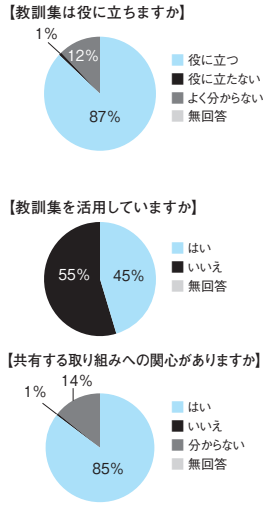
② 教訓集などのダウンロード状況

2014年度末に公開した教訓集などのダウンロード件数を調査した。

教訓集2014年度版　：　1,480回（2015年４月～ 2016年３月）
個別教訓リンク集　：　10,426回（2015年12月～ 2016年３月）

教訓集をダウンロードした方に活用状況アンケートを実施した。（アンケート発送先：916名、回答：115名）

その結果、教訓集は役に立つと回答した割合が87%であるが、活用している割合は45%となっており、活用を促進するための取り組みと内容の充実が課題とわかった。なお、このような産業分野横断的な共有への取り組みに対する関心があるかという質問に対しては、「はい」が85%と高いことが分かった。



- 他企業の事例を確認することで、他社と共通の事柄、相違している事柄が把握可能
- 経験には限りがあり、それ以外の教訓を享受できる
- アウトソーシング等のサービス業務における品質向上のための改善ポイントを考えるとき、ヒントとして有効
- 監査すべき着眼点の参考になる
- 実際に発生した障害及び、その対処法・防止策が記載されているため

- 社内教育として事例を説明
- 機能面に目が行きがちなところに対し、留意すべき考え方をチーム内に展開
- 事業部生産性品質向上施策の一環として教訓集を紹介、事業部内に展開
- 障害原因究明時に必要な基礎知識として、社内教育でケーススタディとして使用
- 担当チーム内での振り返りや意識付けの向上のケーススタディ材料として有益
- ITSMSの認証取得を受け経営者も参加するフォーラムを開催、その中で根本原因の対策、レビュー、運用手順の整備を行う上で参考として利用

図3　ダウンロードした方へのアンケート結果の例

③ 業界団体等への普及推進

各業界団体（14団体）に「情報処理システム高信頼化教訓集（ITサービス編）」を紹介し、活用についての説明と意見交換、必要に応じて講演会を実施した。また、講演実施後のIPA/SECの取り組みに関するアンケートを実施した。

結果は②のアンケート結果と同様の傾向であることが確認できた。

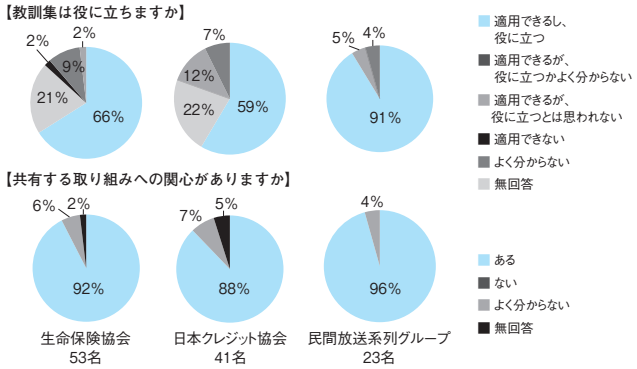


図4　IPA/SECの取り組みへの関心度アンケート結果の例

6 今後の予定

2016年に入っても航空システムや自治体のICカード発行システムなどの社会的影響が大きなシステム障害が発生している。

引き続き障害事例を収集しその普遍化を行い教訓として整理する活動を継続し、教訓集として更なる充実を図っていくと共に、情報処理システムの高信頼化に向けて有益な情報発信を強化していく予定である。

また、社会インフラ情報システムの一層の信頼性向上を目指し、活動を開始したシステム障害情報の共有の仕組みの運営を支援すると共に、新たな産業分野にも普及を働きかけ、自律的な活動を促しつつ、システム障害情報共有の裾野を拡大していきたい。

【脚注】

※10　URL: http://www.ipa.go.jp/sec/reports/20160229.html

組込みシステム

1 背景

近年、機器や製品（以下、組込みシステム）の機能の大半がコンピュータを利用してソフトウェアで実現されるようになってきている。それらには社会インフラとして重要な役割を担うものも多いが、実現する機能規模が肥大化すると共に複雑化する傾向にあり、IoTが進展する今日ではシステム全体として信頼性を確保するための更なる技術面での工夫や運用管理での工夫が求められている。

一方、企業間競争の激化により、差分開発といった短納期の製品開発が主流となり、システム高信頼化のための技術やノウハウがうまく伝承されていないといった問題も顕在化している。

このような組込みシステムの現状に鑑み、産業界におけるシステム高信頼の知見を集積し、将来に向けたシステム信頼性向上のための技術的な布石を打ち、その結果としてシステム信頼性に関する社会的な認識レベルを上げていくことを目的に、2013年度より「製品・制御システム高信頼化部会」とその傘下の一つである未然防止知識WGにて活動を進めてきた。

2015年度は「情報処理システム高信頼化教訓集（組込みシステム編）2015年度版」（以下、教訓集2015）[※11]の作成に加え、この教訓集などを自社内で活用し未然防止に役立つ教訓を自ら作成し継続的に運用していくための「障害未然防止のための教訓化ガイドブック（組込みシステム編）」（以下、教訓化ガイドブック）」「現場で役立つ教訓活用のための実践ガイドブック（組込みシステム編）」（以下、活用ガイドブック）を新たに作成した。[※12]

2 障害事例の収集と教訓化

2014年度に引き続き、産業界で実践されているシステムの品質上の問題を未然に防ぐための知識をもとに、組込みシステムの障害を一般化した。更に、組込みシステム開発企業において幅広く利活用できるようにするための対策の事例を新たに加え、新規７件の事例を公開した。（表５）

3 ガイドブックの作成

3.1 障害未然防止のための教訓化ガイドブック

3.1.1 背景と狙い

自社内で起きた障害の再発防止策の知見を他製品・技術に適用し、同じような障害の発生を未然に防ぐ手立てを講じるためには、ノウハウの一般化をいかに行うかが重要となる。しかしながら、異なる製品領域にまたがった知見の一般化は難しい。これは、

- 使用している動作原理、技術
- 商流・ビジネスモデル
- 開発プロセス
- 組織風土・不文律

が組織ごとに異なるためであり、同一企業であっても部門や事業場ごとにこうした要素が大きく異なっているためである。そこで、様々な製品・システム・組織の観点から障害を分析し、知見の一般化を行ううえで分野を問わず、共通的に活用できるポイントをまとめた教訓化ガイドブックを作成した。

表５　教訓一覧と対策が必要な工程との対応例

教訓番号	教訓タイトル	システム要求定義	システムアーキテクチャ設計	ソフトウェアアーキテクチャ設計	ソフトウェアアーキテクチャ設計（変更設計）	実装（コーディング）	レビュー	システムテスト	教育	プロジェクトマネジメント	運用
29	複数の事業体にまたがる重要システムでは関係者の立場・ニーズの視点から、想定しうる障害発生リスクを同定し効果的な危機管理体制を構築する	○	○						○	○	○
30	過去のハードウェア、ソフトウェア資産を使用する場合は、その内容や当時の方法について考慮する				○	○		○			
31	ミッションクリティカルシステムではリスク管理やV&Vを確実に実施する						○		○	○	
32	不測事態においても適切に動作するかの検証を十分に行い、条件変更時には潜在的なリスク許容度合いの変化を見逃さない		○		○		○	○		○	
33	不十分な設計となっている回避策は根本的に見直す		○	○							
34	重要なソフトウェアを変更する際は、変更管理を確実に実施する		○						○	○	
35	リスク分析によるハザード識別を行い、非常時には関係者が即応できる体制を構築する		○						○		○

目次

1．はじめに
2．教訓化のための概念モデル
3．教訓化の定着に向けたプロセスと組織活動
4．実践的アプローチ
5．未然防止に向けた企業内事例

図5　障害未然防止のための教訓化ガイドブック

3.1.2　ガイドブックの特徴

本ガイドブック作成に当たり、様々な分野の開発実務者にケーススタディを用いた体験型ワークショップに参加いただき、そこでの経験をもとに

- グループワーク用のケースの提示
- 教訓を抽出する観点（例えば、製品・技術、マネジメントなどの職種・分野を指定する観点）の設定
- 教訓の受け手に応じた気づきの与え方、伝え方の工夫

などのポイントを分野横断的に適用できるノウハウを取りまとめた。図6はワークショップで使用したケース資料を例示したものである。

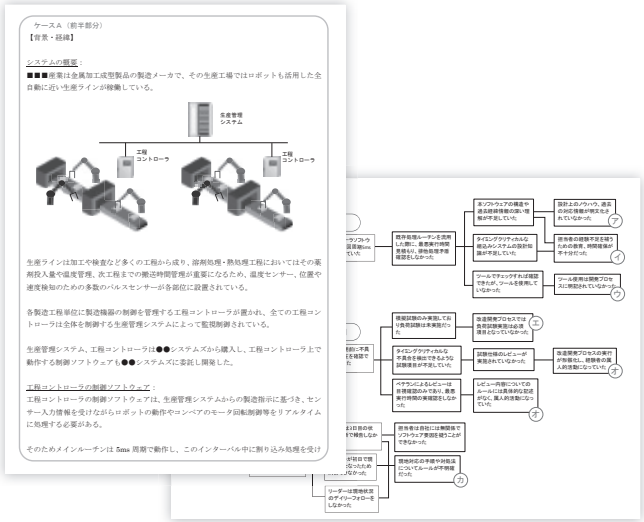


図6　抽出観点例

また、ワークショップ参加者からは「実例を想定した演習内容であり、ディスカッションを行うことができ有意義」、「演習の中でサンプルケースを見て作業を行うことにより、自社に置き換えて考えることができた」、「再発防止策から未然防止策を導き、他者へ伝えるのは工夫が必要と感じた」などのご評価をいただくことができた。

3.2　現場で役立つ教訓活用のためのガイドブック

3.2.1　背景と狙い

多くのものづくり企業で行われている実際の開発プロセスや社内教育などにおいて、前掲の教訓集を含め自社内で蓄積されている教訓情報をどのように活用することができるか、その実践的な活用法を解説するための活用ガイドブックを作成した。この際、企業内で実際に取り組まれている品質マネジメント、再発防止の活動事例も併せて掲載した。

目次

1．はじめに
2．教訓集の構成と特徴
3．組織学習のための基礎
4．基本的な活用方法
5．企業内での活動事例

図7　現場で役立つ教訓活用のための実践ガイドブック

3.2.2　ガイドブックの特徴

社内外からもたらされた教訓を自組織ですぐに活用できるよう、「社内教育・研修」、「開発プロセス」、「設計品質向上活動」の活用シーン別に分け、それぞれの応用例は、

- 想定される状況・課題
- 活用の狙い
- 活用方法
- 期待効果
- 留意事項

をポイントとし、図表なども含めて記述した。図8にこのイメージを例示する。

図8　ガイドブックのポイント

4　今後の予定

今後は、各企業が自ら高信頼なものづくりを継続的に取り組んでいくための教材作成や教育の普及に向け、セミナー等の開催と、それらの活用を意識した質・量両面からのブラッシュアップを進めていく。

また、教訓化及び知識整理方法のまとめ方に関しても、収集済み事例から要素知識を抽出・体系化を行うなど更なる内容の充実化に向けた取り組みを進めていく。

【脚注】

※11　URL:http://www.ipa.go.jp/sec/reports/20160331_2.html
※12　URL:http://www.ipa.go.jp/sec/reports/20160331_3.html

システムの安全性・信頼性分析手法

SEC調査役　三原　幸博　SEC調査役　十山　圭介　SEC調査役　石井　正悟
SEC研究員　松田　充弘　SEC調査役　三縄　俊信　SEC主任　八嶋　俊介

システムの安全性・信頼性の分析をテーマとして、障害原因診断WGにおいてシステムズエンジニアリング手法に基づく障害診断のための「大規模・複雑化した組込みシステムのための障害診断手法～モデルベースアプローチによる事後V&V※1の提案～ Ver. 2.0」(事後V&V)と、この手法を利用する際のシミュレーション環境のための事後検証用サンプルシステムを報告書※2にまとめて公開すると共に、システム安全性解析手法WGを設置してマサチューセッツ工科大学(MIT)で提唱されている安全性分析手法STAMP/STPA※3について調査/試行し、入門書※4にまとめて公開した。

1　障害原因診断手法

1.1　背景と狙い

ハードウェアの性能向上とネットワーク化の進展により、組込みシステムは従来の単一装置による単独システムから複数の機器やソフトウェアが協調する複合システムになっている。複合システムでは必然的にシステム間インターフェースが必要となり、このシステム間インターフェースの増加が今日の組込みシステムをより複雑なものにしている。そのため、組込みシステムに事故が生じた場合、その原因調査は容易ではない。

大規模・複雑化した組込みシステムに発生する障害の原因を体系的に究明するには、設計段階における検証と妥当性確認(V&V)で用いられる方法論の考え方を用いることが重要である。

また、障害原因の究明を目指すだけでなく、社会的な責任の遂行のため、根拠に基づいて広く社会に合意されるような説明となる調査・分析が求められている。重要な制御ロジックとしてソフトウェアが含まれる複雑な組込みシステムでは、製造者だけによる原因調査では不十分であるという点も問題意識として持っている。

2015年度の活動では主に、要求仕様のモデル化による理解と障害原因の診断手法の検討や、2節でも説明するSTAMP/STPA手法の適用、Simulinkを用いた新たな事後検証用のサンプルシステムの開発について取り組み、それらの結果を事後V&V報告書の改訂版として取りまとめた。

1.2　事後V&Vの特徴

V&Vは設計段階での考え落としや実装ミスを防ぐ方法であるが、障害発生時の原因究明では、正に、これと同じことを行う必要がある。更に、抽出した原因仮説により、発生した障害から観測される事象すべてを再現できるという証明まで必要とされるため、設計段階でのV&Vよりも具体的できめ細かい方法論を確立しておく必要がある。図1は事後V&Vの体系をまとめたもので、各要素技術の概要は以下の通りである。

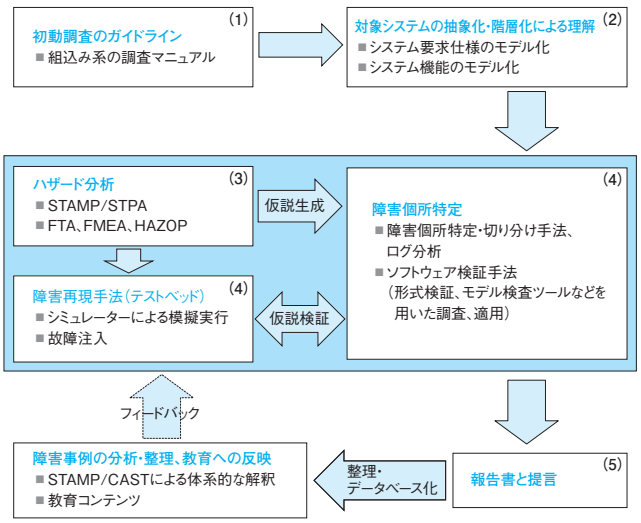


図1　事後V&Vの全体像

(1)初動調査としての分析に必要な情報の収集
(2)要求仕様障害発生に関連する部分の第三者による理解のための抽象化と階層化
(3)ハザード要因の体系的分析による障害原因仮説のリストアップ
(4)障害を引き起こすサブシステムの絞り込みと抽出した原因仮説の検証
(5)報告書へのまとめと本質的な改善に向けた提言

【脚注】
※1　Verification and Validation
※2　http://www.ipa.go.jp/sec/reports/20150331_4.html
※3　Systems-Theoretic Accident Model and Processes / System Theoretic Process Analysis
※4　http://www.ipa.go.jp/sec/reports/20160428.html

以下、今年度重点的に検討したシステム要求仕様のモデル化とSysML記述ツールを用いたSTPA分析、STAMPによる障害原因仮説の生成について概要を述べる。

1.3 システム要求仕様のモデル化

2014年度に事例とした化学プラントシミュレーターに関する要求をSysMLで記述し、STPAを適用して分析した。作業の手順と項目、SysML図との関連を表1に示す。

表1　システム記述に用いた作業の流れと内容

手順	作業項目	使用するSysML図
要求分析	要求を獲得する	要求図
	システムとその境界を決める	ブロック定義図
	システムの使われ方(機能)を定める	ユースケース図
	ユースケースの動作を表現する	シーケンス図 アクティビティ図 状態機械図
アーキテクチャー設計	システムを構成要素に分解する	ブロック定義図
	部品の相互作用を定義する	シーケンス図 アクティビティ図
	部品の相互接続を定義する	内部ブロック図
制約評価	システムの安全制約を獲得する	構造に関する図 動作に関する図
	ハザード分析し、設計を修正する(繰り返す)	
要求割当て	構成要素の要求仕様を定める	ブロック定義図
	要求の追跡性を確立する	要求図

STPAは、基本的にはシステム開発の初期の段階で、ハザードを引き起こす要因を識別することを可能にする。この手法が、既に開発を終えて稼働しているシステムに潜在する障害原因を識別することができるかを考察するために、SysMLで作成したシステム記述を参照し、以下のようにSTPA分析を進めた。

(1)コントロールストラクチャー図の作成
(2)非安全なコントロールアクションの識別
(3)ハザード誘発要因の識別
(4)安全制約の追加

このような分析により、診断対象とするシステムが得られた安全制約を守っているか、守っていないとすればその侵害によって障害現象が発生するか、といった仮説生成に活用できるものと考えられる。

1.4 SysMLとSTAMPによるシステム統合モデル化

前節ではSysMLの図を参照してSTPAを実施しているが、通常の開発工程とSTAMPに基づく分析工程の統合を図ることを目的に、SysMLの要求図を用いた安全制約の記述やSysMLのブロック定義図と内部ブロック図を用いたコントロールストラクチャーの記述を行った。

STPAの準備作業ではアクシデント・ハザード・安全制約の識別が行われ、図2に示すようにSysMLの要求図を用いてこれらの識別を実施している。(事例は前節と同様、化学プラントシミュレーターである。)

コントロールストラクチャーの記述においては、SysMLの内部ブロック図を用い、以下の手順で行った。

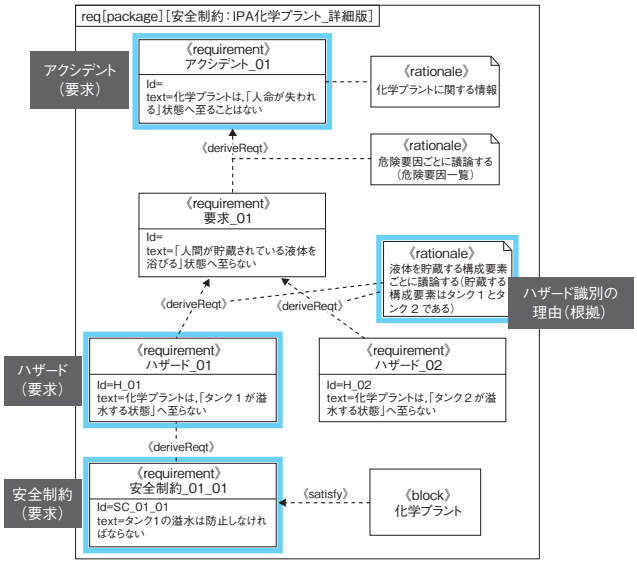


図2　要求図を用いたアクシデント、ハザード、安全制約の識別

(1)ブロック定義図(BBD)によってシステム構成要素を階層的に整理する
(2) BBD内でコントロールストラクチャー記述対象のブロックのレベルにそろえた内部ブロックを抽象コントロールストラクチャー(抽象CS)とする
(3)抽象CS内のブロックに対して内部ブロック図を記述し、そのレベルで得られたものを詳細コントロールストラクチャー(詳細CS)とする
(4)分析の観点に基づいて詳細CSのモデル要素を整理し、最終コントロールストラクチャーを構築する

両者の工程を統合することで、高機能なSysML記述ツールをSTAMPの構成要素の記述に利用でき、人手による作業と比較して作業効率が向上する。しかし、SysML記述のツールはSTAMPの構成要素記述やSTPA支援を目的としては作られていないため、今回記述したよりも抽象度の高いコントロールストラクチャーの記述法、記述した安全制約やコントロールストラクチャーに基づくSTPA支援の方法には更に検討が必要である。

1.5 STAMPによる障害原因仮説の生成

化学プラントシミュレーターに対してSTPAを適用して詳細な分析を行い、ハザードを誘発するシナリオを一般化し、運転員とコンピューターの間、並びに運転員とプラントの間のシナリオとしてまとめたものが図3である。

これらの誘発要因は応用領域によって異なるとはいえ、過去の事故原因を考えてみると一般的に成り立ち得る要因でもある。近年の組込みシステムではコンピューターを介した制御が一般的になっているが、このような制御では状態表示画面がコンピューターの不具合でフリーズした際に、それに気づかないこともあり得る。

安全が最重要視されるシステムでは、コンピューターが

ダウンした際の対処方法も設計に組み入れておくべきである。ここで示したようなハザード誘発要因をまとめておくことで、設計の際の気づきとして用いることもできる。

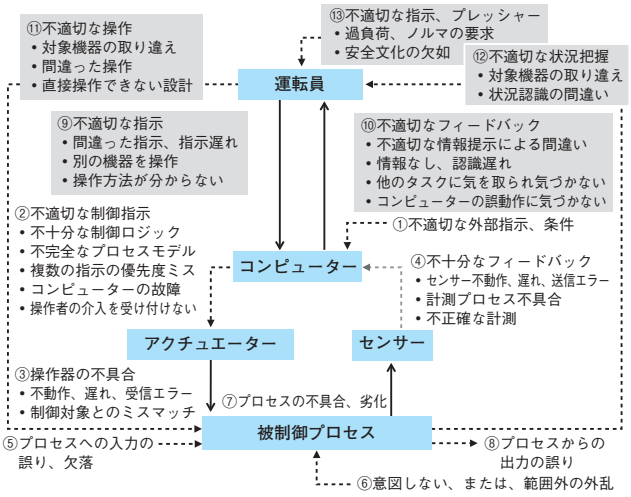


図3　人間系も含めたハザード誘発要因のまとめ

1.6　まとめと今後の取り組み

大規模・複雑化する組込みシステムが増えていく中で、その安全設計やトラブル対応には既存の技術では対応しきれなくなってきている。このようなシステムにおいて障害原因究明が必要とされた場合には、その障害の状況に応じて既存の技術だけでなく、STAMPのような最新の技術を迅速かつ適切に組み合わせて解決していくことが必要になる。

2015年度は化学プラントシミュレーターを仮想の対象として、様々な障害原因究明にかかわる要素技術の適用方法を検討した。要求仕様や機能仕様のSysMLを用いた記述法、SysMLとSTAMPを組み合わせた複雑なシステムのハザード分析、機械学習・人工知能技術を用いた障害診断法、形式手法（モデル検査）を用いた人間・機械の協調制御アルゴリズムの検証、などである。このように具体例でその使い方をショーケースのように可視化しておくことは、いざというときのための準備として必要不可欠なことであろう。

また、要素技術の検証のためのサンプルシステムとして、化学プラントシミュレーターに加えて倒立二輪車の自立制御と人間との協調制御システムを作成した。現実の世界の障害を直接扱うことは必ずしも容易ではないことから、今後も、これらのサンプルシステムを用いて、障害原因究明のためのツールの準備とその利用方法の蓄積を行っていく予定である。これは、障害診断にかかわるエンジニアの育成にも大きく寄与できると考えられる。

2　システム安全分析手法（STAMP/STPA）

近年、システムが大規模・複雑になり、更にネットワークによって相互に接続されて、システム障害もその構成要素に起因するのみならず、構成要素同士の間、更には、システムと人間との間の複雑な相互作用に起因するものがしばしば発生している。

このような状況において、SECではシステムの安全性に関して世界的に著名なMITのNancy Leveson教授が提唱しているSTAMP/STPAに着目し、前節の障害原因分析において適用を始めた。更に、この手法のより深い理解と有効性の確認、適用事例研究の実践などを当面の主な目的とするシステム安全性解析手法WGを設置し、活動を開始した。

STAMP/STPAは、FMEAやFTAをはじめとする従来の技術では全く達成不可能だった「ソフトウェアの仕様書なしにソフトウェアの安全解析を行うこと」、「故障にかかわらないハザード発生シナリオを識別すること」で、従来不可能と考えられてきた、「ソフトウェアの要求・設計ミスによるハザード誘発要因を識別する方法」と言われている。

2015年6月にはSEC特別セミナー「システムベースのエンジニアリング最新動向：複雑化するシステムの安全性とセキュリティを確保するためにすべきこと!」を開催し、Leveson教授に講演いただくと共に、STAMPの実経験者、研究者とWG委員を交えて「日本におけるSTAMP活用の仕方について」と題してパネルディスカッションを行った。併せてWG委員や関係者とLeveson教授との意見交換会を行い、STAMPの理解を深めることができた。

当WGの活動では、この手法に先進的に取り組んでいる委員の協力を受け、手法を理解する目的で委員から提供された具体的な事例（単線踏切制御システム）について、専門領域の知識の提供も受けながら、STAMP/STPAの適用研究を進めた。2016年1月に、国立研究開発法人宇宙航空研究開発機構（JAXA）とIPAとの共催で開催した第13回クリティカルソフトウェアワークショップ（13thWOCS[2]）においてもLeveson教授に特別基調講演をお願いし、それに引き続いてLeveson教授並びにJohn Thomas博士とWG委員及び関係者との意見交換会を開催した。

意見交換会において、Leveson教授より、上記踏切システムの事例が、初歩的な例ではあるが、対象システムのモデル化並びに安全性分析方法として良好であるとの評価を受けたこともあり、入門書「はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～」として小冊子にまとめて公開している。冊子の詳細な内容については本誌52ページの「システム理論に基づくアクシデントモデルSTAMP」を参照されたい。

引き続き人と機械が相互に関係するシステム、人と組織を中心とするプロセス、ITサービスなどの事例を分析しSTAMP/STPAの有用性を示すと共にHow toを事例と併せて示すことにより活用を促進していく。今年12月にはSTAMPワークショップinジャパンも計画しておりコミュニティ形成にも貢献していくことを目指している。

「はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～」

定量的管理による信頼性・生産性向上

SEC調査役 三原 幸博　SEC研究員 松田 充弘　SEC研究員 田代 宣子
SEC研究員 塚元 郁児　SEC専門委員 佐伯 正夫　SEC研究員 峯尾 正美　SEC専門委員 森下 哲成

SEC設立以来、定量的に管理されたソフトウェア開発データを業界から広く収集・分析し、ソフトウェアの信頼性・生産性向上のための統計データを「ソフトウェア開発データ白書」として公開している。2015年度は、従来からのエンタプライズシステムの白書に加え、新たに組込みシステムにフォーカスした「組込みソフトウェア開発データ白書2015」を発行した。一方エンタプライズシステムでは、従来の分析とは別の新たな視点での分析と提言を掲載した「ソフトウェア開発データが語るメッセージ2015」をWEB公開した。図１は、定量的管理の活動体制を示すもので、高信頼性定量化部会の配下に具体作業を目的とした４つのWGを設けている。「組込み」と「エンタプライズ」は、開発対象の分類や分析の観点などが異なるためWG活動を分けている。

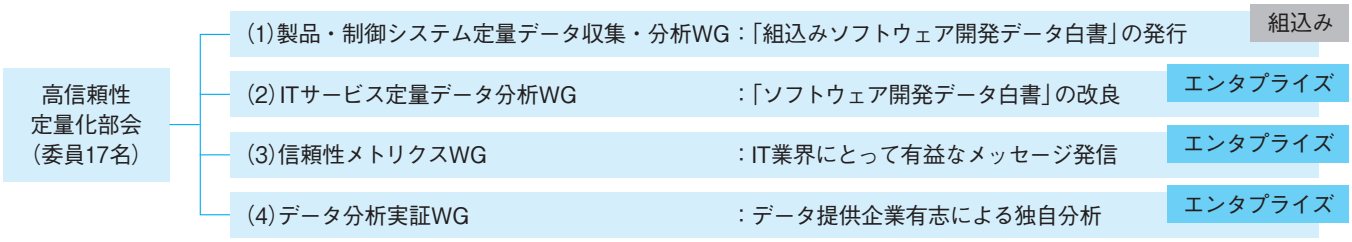


図１　定量的管理の活動体制

組込みシステム分野の活動

1 「組込みソフトウェア開発データ白書」の発行

図２　組込みソフトウェア開発データ白書2015

2015年11月、組込み業界向けに初めて「組込みソフトウェア開発データ白書2015」を発行した※1（図２）。これは、組込みシステムベンダ企業10社から提供していただいたプロジェクトデータ174件を分析したものであり、組込みソフトウェア開発で使用される言語の傾向や生産性や信頼性の指標を将来的に業界で共有することを目的としている。

現行のエンタプライズ向けのデータ白書には収集データの件数では及ばないものの、生産性や信頼性の定量的な指標となり得るものや、定性的な傾向が見えているので、いくつか紹介する。

1.1 収集データの分布と分析対象

プロジェクトデータ174件のプロファイルの分布状況を分析した結果、生産性や信頼性の分析対象を、次のものにフォーカスした。

(1) 改良（派生）開発

収集データは、新規開発５%、改良（派生）開発95%のため、2015年度版では改良（派生）開発を分析対象とした。

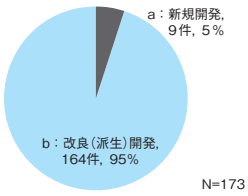


図３　開発プロジェクトの種別

(2) 開発言語

収集データでは開発言語は圧倒的にC言語が使われており、次にC++言語が多く使われている。C++言語は、C言語の代用を目的にするケースが大半であったため、2015年度は、それぞれを区別せず、C++言語またはC言語で開発したデータを分析対象とした（図４）。

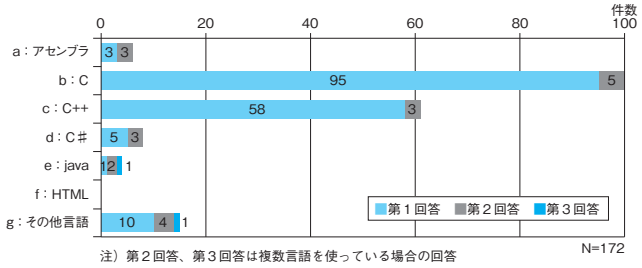


図４　開発言語

【脚注】

※1　http://www.ipa.go.jp/sec/reports/20151116.html

(3) SLOC規模

分析対象の規模感を掴むために、2015年度版の収集データの開発規模の分布を表１に示す。

表１　SLOCK規模　[単位：KSLOC]

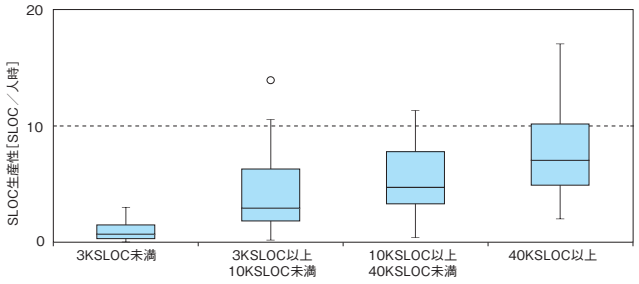
	N	P25	中央値	P75
SLOC規模	173	2.4	6.1	24
SLOC規模（母体含む）	173	61	249	511

1.2　分析結果

分析の結果、生産性や信頼性について以下のような組込みソフトウェア開発の側面が見えた。

(1) 規模別SLOC生産性

定量データ管理の中で最も関心の高い指標は生産性であるが、開発の現場に生産性指標の適用を検討する場合の留意事項として、ざっくりではあるが規模と生産性の傾向を明らかにした。生産性はエンジニア１人が単位時間（または期間）当たりにどれだけの行数のプログラムを開発できるのかを表す指標であるが、作業の対象は組織により異なる。ここでは、アーキテクチャ設計、詳細設計、実装・単体テスト、結合テスト、総合テストのソフトウェア開発５工程を対象にしている。図５に示す通り、生産性は、開発規模の大きさで違いが見られるため、組織の指標を定める際には、開発規模の小さいもの、大きいものを区別して行う必要がある。



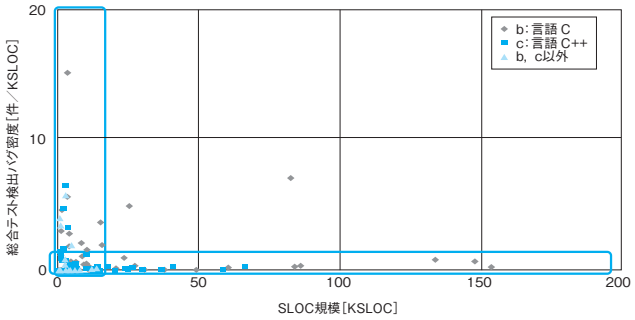
基本統計量　[SLOC／人時]

	N	P25	中央値	P75
3KSLOC未満	20	0.31	0.68	1.48
3KSLOC以上10KSLOC未満	18	1.81	2.92	6.29
10KSLOC以上40KSLOC未満	18	3.30	4.72	7.77
40KSLOC以上	6	4.90	7.03	10.16

図５　SLOC規模別SLOC生産性

(2) 信頼性

生産性の次に関心の高い指標は信頼性で、組込み製品の多くは市場に出す前のソフトウェア総合テストをどこまで網羅性を上げて実施すべきかの判断が難しい。その判断の１つとして、単位規模当たりどれだけのテストケースを実施するかの指標「テストケース密度」の設定と、総合テスト開始前の時点で単位規模当たり何件のバグが潜在しているかの予測のもとに、単位規模当たりに検出すべきバグ現象件数を設定できれば、市場に出すレベルの品質を判断することができる。図６は、総合テストで検出したバグ現象の件数を開発SLOC規模（母体規模は含まない）で正規化した「総合テスト検出バグ現象密度」の散布図である。SLOC規模がある程度大きい場合には、一定の範囲に収まっているが、規模の小さいところでは指標のバラつきが大きい。「指標を定める際には、ある程度の開発規模があるものを対象に定めるべき」といった推奨事項を明らかにした。



基本統計量　[件／KSLOC]

	N	P25	中央値	P75
b：言語C	47	0.01	0.44	1.70
c：言語C++	44	0.00	0.09	0.50
b，c 以外	16	0.00	0.04	1.10

図６　SLOC規模と総合テスト検出バグ現象密度

1.3　組込み分野とエンタプライズ分野の比較

ソフトウェアベンダ業界では、エンタプライズ分野を主要マーケットにしている企業が組込み分野に参入する場合や、組込みシステムを専門にしているベンダが、装置管理システムの開発などエンタプライズ分野のソフトウェア開発に事業領域を拡張する場合がある。そのようなケースでは、プロジェクト計画策定にあたり、組込み分野、エンタプライズ分野の特徴を把握しておく必要がある。2015年度版の組込みデータ白書に掲載した分析結果の中から、エンタプライズ分野の「ソフトウェア開発データ白書2014-2015」分析結果と比較して特徴の違いが見えたものを、幾つか紹介する。

(1) 工程別　工数・工期の比率

図７は、ソフトウェア開発のアーキテクチャ設計～総合テストまでの開発５工程の各工程に配分する工数と工期の比率を組込み分野とエンタプライズ分野で比較したものである。

左上の「組込み」の工数比率と左下の「エンタプライズ」の工数比率を比べてみると、「エンタプライズ」は、製作工程（組込みの実装・単体テスト工程）に突出して工数をかける傾向が読み取れる。一方、「組込み」では、実装・単体テスト工程に最も工数をかけるという点では、「エンタプライズ」と同じであるが、アーキテクチャ設計工程やテスト工程にも「エンタプライズ」よりも工数をかける傾向が見える。

次に右側の工期について、「組込み」と「エンタプライズ」を比べると、「エンタプライズ」では、工数と同様に製作工程に最も長い期間をかけるのに対して、「組込み」では、実装・単体テスト工程の期間は、リソースを増やすなどして、期間を圧縮している傾向が見える。

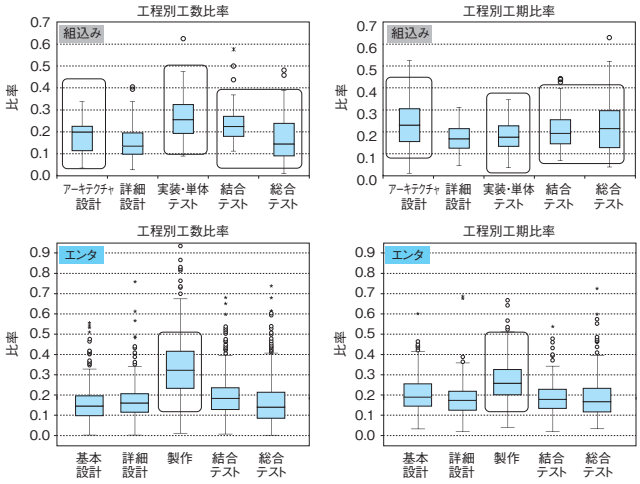


図7　工程別　工数・工期の比率

(2) 規模当たりのテストケース数、検出バグ数

図8は、結合テスト及び総合テストにおけるテストケース密度（KSLOC規模（母体規模は含まない）当たりのテストケース数）とテスト実施により検出するバグ密度（KSLOC規模当たりの検出バグ件数）を「組込み」と「エンタプライズ」で比較したものである。テストケース密度を「組込み」と「エンタプライズ」で比べてみると、中央値にて、結合テストで156：53、総合テスト83：17で、「組込み」は「エンタプライズ」の約3倍～5倍のテストケースを実施している。

一方で、検出バグ密度（図の右上：「組込み」、右下：「エンタプライズ」）では、結合テスト、総合テスト共に、「組込み」「エンタプライズ」両分野の差異が見られない。

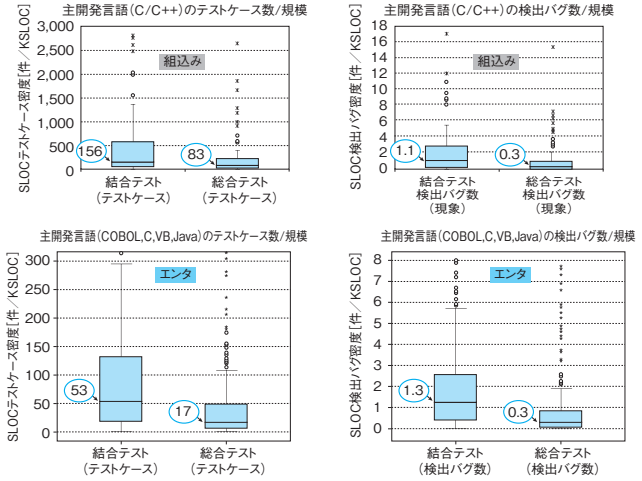


図8　規模当たりのテストケース数、検出バグ数

2 「組込みソフトウェア向けプロジェクトマネジメントガイド［定量データ活用編］」の発行

前節で紹介した「組込みソフトウェア開発データ白書2015」の発行に合わせて、「組込みソフトウェア向けプロジェクトマネジメントガイド［定量データ活用編］」を発行した（図9）。組込みソフトウェア開発の現場に、新たに信頼性や生産性の定量的指標による管理を導入しようとするには、経営者の理解を得ることが前提であり、本書は経営者にとっての恩恵や利点を伝えている。また、定量データを収集、管理することは、手間と労力がかかるという先入観を持たれる傾向がある。本書は、コストのかからない定量データ収集の仕組みや、定量データを活用したプロジェクトマネジメントのやり方、終了したプロジェクトの管理データから組織の弱点を見つけて組織を強化するために知見やノウハウも紹介している。

図9　組込みソフトウェア向けプロジェクトマネジメントガイド［定量データ活用編］

エンタプライズシステム分野の活動

3 「ソフトウェア開発データが語るメッセージ2015」の公開

これまで公開してきた統計データでは示されていなかった「ベスト・プラクティスをヒントに改善を図る」という点に着目し、IPAが保有する3,541件のプロジェクトデータの分析を行った。

分析の結果得られたベスト・プラクティスの傾向やソフトウェア開発における品質マネジメントの指針を取りまとめ「ソフトウェア開発データが語るメッセージ2015」[※2]として公開した。

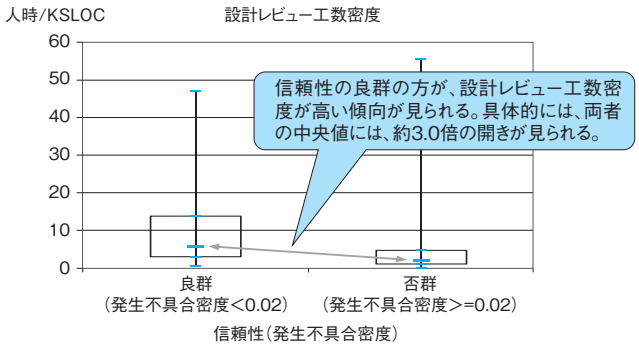
【ベスト・プラクティス抽出の観点】

- 「設計の文書化・レビュー・テストなどの品質保証プロセスや組織体制にどんな傾向が見られるか」
- 「信頼性を確保するためには、どの程度まで品質保証プロセスを実施すれば良いか」

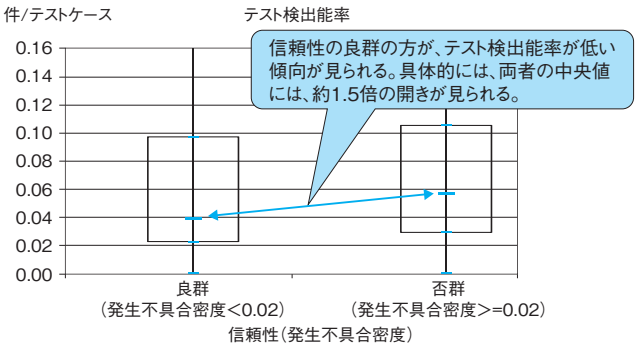
【本書掲載指針例】

- ベスト・プラクティスは「上流工程」に注力。テスト時の不具合が少ない傾向に（補足1、2）
- 設計レビューの効果を勘案した「設計レビュー工数」のコントロールを（補足3）

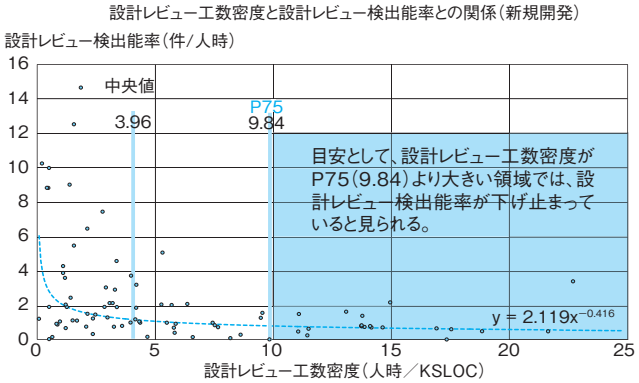
補足1：ベスト・プラクティスは、設計レビュー工数密度が高く上流工程に注力している。（中央値で約3.0倍）



補足２：良群はテスト検出能率も低いことから、テスト時における潜在的な不具合が少ない。（中央値で1.5倍）



補足３：設計レビュー工数密度の75パーセンタイル値以降では検出能率が下げ止まっている傾向にあるため、自社プロジェクトの設計レビュー工数密度の75パーセンタイル値までを目安にレビュー実施を。



●顧客が要求仕様に関与しているほど、生産性と信頼性が向上する傾向に。

本内容は、「日経SYSTEMS2015年10月号」にTRENDとして紹介された。

4　エンタプライズ分野の定量的管理の推進

4.1　ソフトウェア開発データ白書の原稿案の作成

「ソフトウェア開発データ白書2016-2017」の原稿案を作成し、ITサービス定量データ分析WGにて内容のレビューを行った。

【新たな記載内容】

●新たに分析項目を８項目追加すると共に、信頼性／生産性に関する変動要因分析を実施。

●ニーズが高かった業種編（金融保険業、情報通信業、製造業の３業種）の作成。

なお、本データ白書は、2016年秋に発行予定である。

4.2　ベンチマーキングガイド原稿案の検討

ベンチマーキングを「単に自プロジェクトの信頼性、生産性などを計測したデータと外部（公開）で蓄積されたベンチマークや自社の内部ベンチマークと対比して差異を把握するだけでなく、その差異要因となっている開発プロセスやマネジメントを改善する」と定義した。

そのベンチマーキングの具体的な実施方法や白書／ユーザでの実施例を取りまとめた「統計指標に基づく品質マネジメント実践集（仮称）」を作成し、ITサービス定量データ分析WGにて内容のレビューを行った。

同実践集は、2016年度早々の公開を予定している。

4.3　新たな開発スタイルに対応する取り組み

信頼性メトリクスWGでは、クラウドやPKG／サービス利用など新たな開発スタイルにおいてプロジェクト開始時点での見積もりが大きく乖離する事例を各社から出してもらい、分類整理した。

2016年度は、更にその内容をもとに開発スタイルごとに見積もりが大きく乖離する変動要因の主なものを抽出し、その計測方法や対処方法などをまとめたノウハウ集を作成予定である。

4.4　定量的管理の普及促進

定量的管理の普及促進のため、下記の活動を実施した。

●「ソフトウェア開発データ白書2014-2015」の普及活動の一環として、ETWest2015、ET2015、CEATEC JAPAN 2015にて、パネル展示やセミナーを実施。

●「ソフトウェア開発データ白書2014-2015」の概要及び追加分析について紹介するために、「ソフトウェア開発データ白書2014-2015」の関連セミナーを４回開催。

●オープンソースとして公開中の定量的プロジェクト管理ツール（EPM-X）に関するセミナーについて、PPMA※3との共催セミナー（東京計６回）を実施。

5　蓄積ソフトウェア開発データの活用促進

5.1　メトリクス分析に関する研究への活用

蓄積されているソフトウェア開発データをより一層活用し、ソフトウェアの信頼性・生産性向上に繋がる新たな分析手法の発見などを目指し、所定の守秘義務の下で蓄積データを大学などに貸与し、分析方法の研究に活用いただいている。

東海大学、法政大学及び同志社大学に加え、2015年度は新規に大阪大学、静岡大学、米国カーネギーメロン大学SEI（ソフトウェア工学研究所）にも貸与し、各大学の研究に貢献した。

5.2　データ提供企業間での独自分析目的データ活用

データ提供企業および高信頼性定量化部会の委員の中から有志を募り、各社独自の切り口での分析を行うデータ分析実証WGの活動を２月10日より開始した。

実施内容は、３ヶ月に１回の分析結果などの共有を中心としたＷＧと、適宜実施する各社個別のデータ分析作業である。本活動により有用な知見が得られれば、関係者の承諾を得て公開することとしている。

【脚注】

※2　http://www.ipa.go.jp/about/press/20150925.html

※3　一般社団法人実践的プロジェクトマネジメント推進協会（Practical Project Management Association）

コーディング作法ガイド(ESCR※1)の整備について

SEC調査役 三原 幸博　SEC調査役 十山 圭介

1 コーディング作法ガイド(ESCR C++)の改訂状況

IPA/SECでは組込みソフトウェアのソースコード品質をより良いものとすることを目的に、コーディングの際に注意すべき事柄やノウハウを作法ガイド：ESCRとして公開している。

ESCRは、コーディングにおける基本的な考え方(作法)と、作法を対象の言語に合わせて具体化した個々のルールとをソフトウェア品質特性の観点で整理したものである。組織やプロジェクトでコーディングルールを決める際や実際のコーディング時の参考のため、また個々人のプログラミング学習のためとして、書籍やPDFなどこれまで3万部を超えて多くの方々に利用いただいている。

ESCRはC言語とC++言語に対応しており、近年広く使用されるようになってきているC++言語向けでは2003年版の言語規格(C++03)に準拠したESCR［C++言語版］Ver. 1.0を2010年に発行している。

今回、この［C++言語版］について、言語の新しい標準規格C++11及びC++14に準拠し、また2013年度に改訂したESCR［C言語版］との整合性を確保するべく改訂作業を進めている。改訂作業は、コード記述のレベルを基本にライブラリ関数やテンプレートに関しては含めないというVer. 1.0と同じ方針で、2014年度からコーディング作法ガイド改訂WGにおいて開始しており、2015年度は、C++11及びC++14での改訂項目に対応した変更点とESCR［C言語版］の改訂に関連する変更点を整理しつつ、原稿作成を行った。改訂版は、2016年10月発行の予定である。

2 コーディング作法ガイドにおける海外連携

MISRA CとMISRA C++は英国MISRA※2が策定しているコーディングガイドラインであり、安全で信頼性の高いソフトウェアの開発のため自動車業界を中心に広範に運用され、標準技法としての地位を築いている。IPA/SECでは設立時から、ESCRとMISRA Cとで相互に記述の引用や、改訂時のレビューを行うなど、MISRAと連携して活動を実施している。

2015年10月14日に、MISRAからCとC++ WGの議長であるA. Banks氏とC. Tapp氏を招聘し、「ソフトウェア品質向上のためのコーディング技法と標準」と題するセミナー※3を、名古屋国際会議場においてIPA主催、ASIF・JASA・SESSAME共催で開催した。

本セミナーでは日本における安全で高信頼なソフトウェア開発の実践を目的に、ガイド適用時の効果や制限まで含めてMISRA C及びC++とESCR、セキュアコーディングのためのCERT C※4を関連付けると共に、これら技法の標準化に向けた日欧での活動についての紹介と議論を行った。MISRA側からはC、C++のガイドライン策定活動やスケジュール、安全性とセキュリティに関する活動を、日本側からはESCRの状況とSESSAME※5を中心とする日本での有志によるMISRA C適用に向けた活動を、それぞれ紹介した。

また、2014年よりESCRのセキュリティ対応に関してSECで作成しているESCRのルールとCWE※6の対応付けについて、米国NIST※7と意見交換を行っている。昨年度は、3月にNISTを訪問し、対応表の現状を説明した。

【脚注】

※1 ESCR：Embedded System development Coding Reference
※2 MISRA：The Motor Industry Software Reliability Association（欧州の自動車業界団体）
※3 http://sec.ipa.go.jp/seminar/20151014.html
※4 CERT C：C言語を使ってセキュアコーディングを行うためのルール等をまとめたコーディング規約
※5 SESSAME：NPO法人組込みソフトウェア管理者・技術者育成研究会
※6 CWE：Common Weakness Enumeration（ソフトウェアの脆弱性の種類や関連する情報について列挙したもの）
※7 NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

つながる世界（IoT時代）の高信頼化に向けて

～2015年度の取り組み結果～

SECソフトウェアグループリーダー　中尾 昌善

1 はじめに

IoT時代の到来を迎え、製品・システムがつながって、新しいサービスを創出したり、色々なデータを用いて製品・システムを制御する世の中へと変遷しつつある。このIoT時代のことを、別名で「つながる世界」と呼んでいる。そこでは、色々な品質の製品が氾濫し、それを利用者が勝手に選択してつなぐと、安全上あるいはセキュリティ上の問題を引き起こす危険がある。

この利用者リスクの増大を防止する取り組みが必要と考え、2013年度から開始した第三期中期計画の「ソフトウェアの利用者視点での信頼性の見える化」という取り組みの一環で、2015年度は、ソフトウェアやそれを含む製品・システムの信頼性向上に関する以下の活動を行ってきた。

2 「つながる世界の開発指針」の策定

つながる世界を実現するには、セーフティ・セキュリティ・リライアビリティなどの確保が必要である。これらの基盤的要件を満たした上での新しい製品・システムやサービスの創出が望ましい。一方で、開発事業者は、これらの基盤的要件の重要性を認識しつつも、つながる世界の製品開発において、それらの要件を具体化できずに手探り状態となっていた。安全基準などが存在する分野もあるが、それらは当該分野内の製品に適用されるものであり、分野をまたがってつながることを想定したものにはなっていなかった。そこで、つながる世界における製品開発を推進する方々を主なターゲットとして、開発時に考慮すべき着眼点を17個の指針に取りまとめた。これが、国内初の「つながる世界の開発指針」である。

3 「つながる世界の開発指針」に関する実証実験

上述の開発指針のリスク対応策として考えられる技術項目のうち、技術的に未確立な事項について、その実装可能性を実証した。実験はFA（Factory Automation）分野、すなわち工場における産業ロボットを対象とした。実験内容は、次の２つである。

(1) 障害の波及防止策（製造ラインにおける異常検出とその後の波及防止）

(2) 相互接続時の信用確認（製造ラインに装置を組み込む際の信用確認）

これらの実証実験は、FA機器をつなぐための基盤ソフトであるORiN（Open Resource interface for the Network）を利用しており、一般社団法人日本ロボット工業会ORiN協議会、一般財団法人機械振興協会、及びIPA/SECの３者協力により実施した。

4 システムズエンジニアリングの推進

IoT時代のシステム開発では、考慮すべき外部要因の拡大や未知のリスクへの対応が必要となってきている。これに対応するためには、広範な要件を考慮した安全・安心な開発方法や新規サービス創出のための方法論を確立していく必要がある。これに寄与すると考えられるのが、システムズエンジニアリングである。システムズエンジニアリングは、欧米では適用が進んでいるが、我が国では認知度も含めて定着していないのが実態である。まずは、各方面の識者の方々に、システム開発における課題認識を述べていただき、その解決にシステムズエンジニアリングが有用となるかを探るための議論を行った。この結果を次年度活動に活かしていくことにした。

5 先進設計・検証技術の適用事例紹介と分析

ソフトウェア開発における品質、コスト、手間などの改善に、多くの企業がチャレンジしてきている。それらの実践事例を広く紹介することにより、我が国のソフトウェア開発力の向上に貢献したいと考え、2015年11月に「先進的な設計・検証技術の適用事例報告書」を、IPAのWebページに公開した。まだ、IoT関連の事例は少ないが、今後の事例収集ではそれらが増えていくものと想定される。

更に、過去３年間に収集した58事例を分析することにより、取り組みの意義や手法の有効性などを示唆する結果が得られた。これを、2016年５月に「事例に見る先進的な設計・検証技術の適用分析」という書籍として取りまとめ、発行した。

6 おわりに

つながる世界でのソフトウェアの信頼性の確保に向けた課題は多岐にわたり、今後もそこに焦点を当てた取り組みを実施していく。

「つながる世界の開発指針」の策定

SEC研究員 宮原 真次　SEC研究員 小崎 光義　SEC研究員 遠山 真
SEC研究員 西尾 桂子　SEC研究員 丸山 秀史

1 はじめに

IoT（Internet of Things）では自動車や家電、ウエアラブル機器など様々な「モノ（Things）」がネットワークに接続されるが、このような「つながる世界」においては利便性は高いものの、遠隔から攻撃されたり故障の影響が他のモノに波及したりするなどのリスクも高い。そこでIPA/SECはIoTならではのリスクに着目し、開発者向けにリスク対策に資する開発指針をとりまとめることとした。

2 つながる世界とは

2.1 System of SystemsとしてのIoT

IoTでは、迅速かつ正確にデータを収集・分析し、ビッグデータとして新しい知見を得たり、リアルタイムに機器やシステムを制御したりすることが可能となる。また、自動車や家電、ヘルスケアなど異なる分野の機器やシステムが相互に連携して新しいサービスを実現することが可能である。

IoTには、複数のシステムが連携することでより大規模なシステムとなり、かつ新たな価値を創造する「System of Systems（SoS）」の考え方が当てはまる。本開発指針の「つながる世界」も単に「モノ」同士がつながるだけではなく、単体でも価値を持つIoTが他のIoTとつながることにより、新たな価値を提供するSoSの世界をイメージしている（図１）。

一方で、異なるIoTがつながることにより、今までにないセーフティやセキュリティ上の問題が発生する可能性もあり、リスクの特定と対策が必要となる。

2.2 IoTのリスクとは

IoTにおいては、IoT同士がつながることにより、故障の影響が広範囲に波及したり、接続点から第三者に侵入されて攻撃されたりするなどのリスクが想定される。それ以外にも、以下の特徴的なリスクが挙げられる。

(1) 想定しないつながりが発生する

IoTを構成する機器やシステムは相互につながりやすく、IoTサービス事業者はもちろん、ユーザが興味本位でつなげてしまうケースもある。その結果、メーカが想定しないつながりにより不具合が発生する危険性がある。

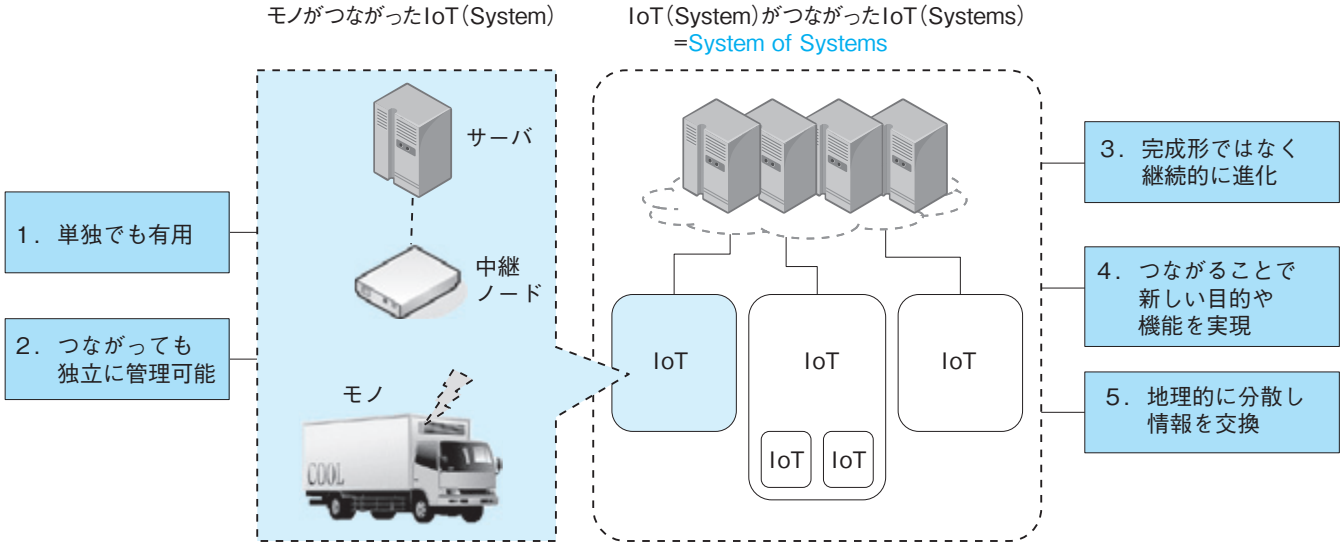


図1　System of SystemsとしてのIoT

(2) 管理されていないモノもつながる

IoTにつながる自動車や家電などは管理されていないものも多く、第三者が隙を見て不正なソフトウェアを埋め込むことも可能である。

(3) 身体や財産への危害がつながりにより波及する

生活に利用する機器は不具合によりユーザの身体や生命、財産に危害を及ぼす可能性がある。つながることで誤動作が引き起こされたり、被害が他の機器やシステムに波及したりすることが懸念される。

図2　つながりにより波及する危害

(4) 問題が発生してもユーザには分かりにくい

故障や破損など物理的な異常は分かりやすいが、ウイルス感染や無線経由での不正アクセスなどつながりに起因する問題は目に見えないため、問題が発生してもユーザが気づかない可能性が高い。

以上のように、IoTは社会全体に広がる重要なインフラであり、ユーザの身体や財産に危害を与える危険性もある。しかし、IoTは日々拡大し、変化するため、リスクの特定が難しいという問題がある。

3 欧米におけるIoT関連規格と本開発指針の位置付け

3.1 海外のIoT関連規格

IoTについては様々な団体で規格化が進められており、大まかには業界・分野に共通的な「共通・汎用規格」と特定の業界や分野に依存する「業界別・特定規格」とに分類できる。前者としてはIEEE、ISO/IEC、NIST、oneM2Mなどがあり、後者としてIndustrie 4.0やIICがある。Industrie 4.0とはドイツ政府が推進する製造業の高度化を目指すプロジェクトであり、第４次産業革命と称されている。その特徴はCyber Physical System (CPS)をベースとした製造業の高度化である。

IICは、米国企業中心に産業市場におけるIoTの推進を目指して設立された団体である。IICはエネルギー、医療、製造、運輸、行政などの領域を対象としている。IICではIoT向け規格の標準化団体に会員企業の要望を伝えることにより、相互運用性を実現し、テストベッドによる検証環境構築の推進を行っている。

Industrie 4.0はドイツの機械産業の国際市場拡大、IICは参加企業によるIoTプラットフォームビジネスの市場創生が主要な目的と想定される。

主要な関連規格の動向を表１に示す。

3.2 開発指針の位置付け

表１の「業界別・特定規格」については、前述のIndustrie 4.0やIICのように各国産業の活性化やIoTビジネス創造を狙いとしたものが多く、開発者が参考とするには具体化されていない。表１の「共通･汎用規格」についても、安全･安心に関する事項は分野共通・汎用的な内容となっており、個別の産業の開発者が参照するには実践的な内容にはなっていない。

そこでIPAでは、我が国の産業の安全・安心への取り組みの現状や各企業が抱える課題を踏まえて実用的な対策を整理する必要があると判断した。それに基づき、本開発指針では、各業界別の実際のリスク例をベースに安全・安心に関して実践的なレベルにまで踏み込みつつ、各業界で利用できるよう共通的・業界横断的なものとしてまとめることを目指した。

表１　海外におけるIoT関連規格の動向

	規格/団体	概要	主要参加メンバー等
共通・汎用規格	IEEE　P2413	IoTにおいてドメイン横断のプラットフォームを検討	－
	ISO/IEC 30141	JTC1 SWG5の後を受けてWG10でリファレンスアーキテクチャを検討	－
	NIST CPS PWG	CPSのFramework検討のためのPublic WG	－
	oneM2M	世界の主要７標準化団体の共同プロジェクト。 従来の垂直統合型M2Mサービスを共通PFで水平統合型に展開	Continua、HGI、OMA等業界団体等、約200社
代表的な業界別・特定規格	Industrie 4.0	ドイツ政府が製造業のイノベーション政策として主導	Siemens、Bosch、SAP等
	IIC	エネルギー、医療、製造、運輸、行政に焦点	GE、AT&T、IBM、Cisco、Intel等、約150社
	AllSeen Alliance	家電製品、モバイル端末向け規格	Qualcomm、LG、MS等、約50社
	OCF	家庭、企業における多様なデバイス間の相互運用のための規格	Intel、サムスン電子、Cisco、MS等
	HomeKit	iOSと機器をつなぐ規格	Apple等、約20社

4 開発指針の策定プロセス

開発指針の策定においては、学術研究者及び自動車、住宅、ATM、産業機械など多様な産業の識者から成る「つながる世界の開発指針検討WG」を立ち上げ、WGメンバのコンセンサスを取りながら検討を進めた。また、過去に発行した「つながる世界のソフトウェア品質ガイド」、「つながる世界のセーフティ &セキュリティ設計入門」などの作成において得られたセキュリティとセーフティの関係の整理などの知見も活用した。

その上で、以下のプロセスにて策定した。

(1)「IoTコンポーネント」に重点を置いた検討

IoTは２節で示したように異なる分野のIoT同士がつながって拡大していくため、新たなリスクの発生やリスクの影響範囲の変化によりリスク分析が難しい。そこで本開発指針では、２節で示したSoSの最小単位、すなわちIoTを構成する機器やシステムのうち単独で目的や機能を果たすものを「IoTコンポーネント」と呼び、IoTは「IoTコンポーネント」と「つながり（ネットワークや情報通信など）」から構成されるものと想定した。その上で、「IoTコンポーネント」のリスクを想定し、対策を検討することで、IoTの安全・安心を実現する指針を策定した。単体でも、つながっても安全・安心なIoTコンポーネントを実現できれば、日々、拡大・変化するIoTにおいても安全・安心を維持することが期待される。

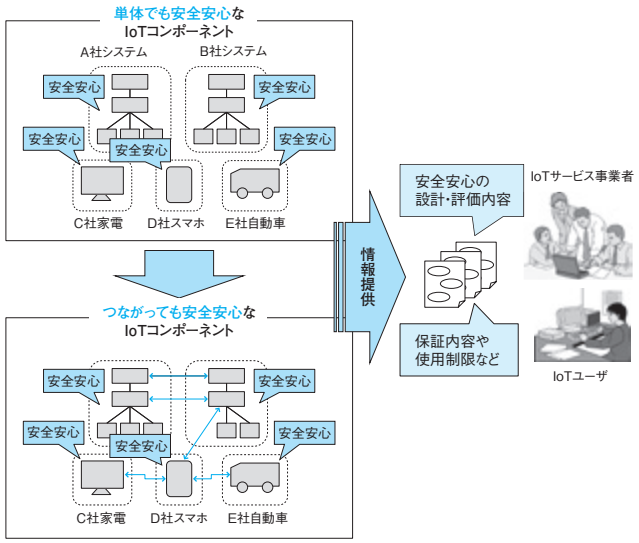


図３　単体でもつながっても安全・安心な「IoTコンポーネント」

(2)「IoTコンポーネント」のリスク分析

次にIoTコンポーネントを、「モノ本来の機能」や「情報」に「IoT機能（通信機能など）」を付加したモデルとして想定し、「守るべきもの」を整理した。また、IoTコンポーネントのつながり方のパターン、つなげた者、攻撃の発生個所などを整理し、これらを横軸、リスク事例を縦軸としてリスク分析表を作成した（詳細は本開発指針を参照いただきたい）。IoTのリスク事例はまだ少ないため、リスクの想定例を追加した。最後に、このリスク分析表を基に、開発指針を導出した。フローを図４に示す。

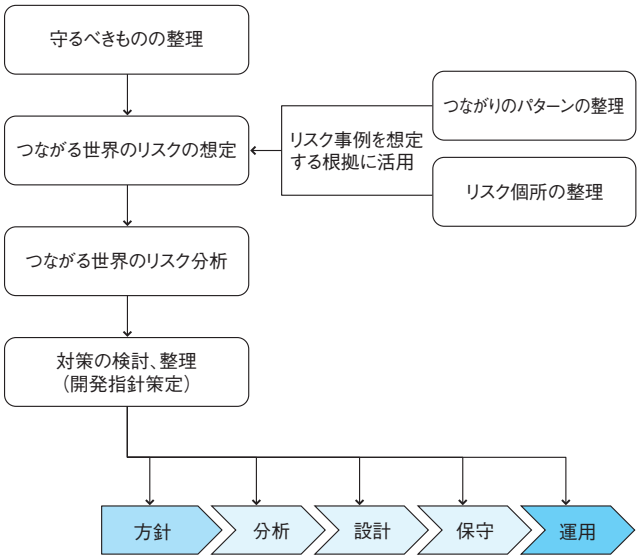


図４　開発指針の策定フロー

5 つながる世界の開発指針

(1) 開発指針の概要

図４の通り、「方針」「分析」「設計」「保守」及び「運用」のライフサイクルに合わせて17の開発指針を策定した。実情としてはハードウェアの性能、開発コストなどの制約などにより各指針で例示した対策を実装できないケースも想定されるが、少なくとも各指針の着眼点での検討は必ず実施いただきたいと考えている。開発指針の一覧を表２に示す。

ライフサイクルに合わせた理由は、自動車や家電などの機器は10年以上も利用されることがあるため、廃棄の段階まで安全・安心の対策が必要なためである。

本開発指針は開発者を主たる対象としているが、「方針」に含まれる３つの指針はメーカなどの経営者にIoTのリスクに気づいていただくために有用であると考えている。また、「保守」「運用」に含まれる５つの指針は開発者と保守者が連携してIoTコンポーネントの安全・安心を実現するために活用いただきたいと考えている。

表2　検討してほしい開発指針一覧

大項目	指　針	ポイント
方針	指針1　安全安心の基本方針を策定する	① 経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知すると共に、継続的に実現状況を把握し、見直していく。
	指針2　安全安心のための体制・人材を見直す	① つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。 ② そのための人材（開発担当者や保守担当者など）を確保・育成する。
	指針3　内部不正やミスに備える	① つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。 ② 関係者のミスを防ぐと共に、ミスがあっても安全安心を守る対策を検討する。
分析	指針4　守るべきものを特定する	① つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。 ② つなげるための機能（IoT機能）についても、本来機能や情報の安全安心のために、守るべきものとして特定する。
	指針5　つながることによるリスクを想定する	①クローズドなネットワーク向けの機器やシステムであっても、IoTコンポーネントとして使われる前提でリスクを想定する。 ② 保守時のリスク、保守用ツールの悪用によるリスクも想定する。
	指針6　つながりで波及するリスクを想定する	①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。 ② とくに、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。
	指針7　物理的なリスクを認識する	① 盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。 ② 中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。
設計	指針8　個々でも全体でも守れる設計をする	① 外部インターフェース経由／内包／物理的接触によるリスクに対して個々のIoTコンポーネントで対策を検討する。 ② 個々のIoTコンポーネントで対応しきれない場合は、それらを含む上位のIoTコンポーネントで対策を検討する。
	指針9　つながる相手に迷惑をかけない設計をする	① IoTコンポーネントの異常を検知できる設計を検討する。 ② 異常を検知したときの適切な振る舞いを検討する。
	指針10　安全安心を実現する設計の整合性を取る	① 安全安心を実現するための設計を見える化する。 ② 安全安心を実現するための設計の相互の影響を確認する。
	指針11　不特定の相手とつなげられても安全安心を確保できる設計をする	① IoTコンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。
	指針12　安全安心を実現する設計の検証・評価を行う	① つながる機器やシステムは、IoTならではのリスクも考慮して安全安心の設計の検証・評価を行う。
保守	指針13　自身がどのような状態かを把握し、記録する機能を設ける	① 自身の状態や他機器との通信状況を把握して記録する機能を検討する。 ② 記録を不正に消去・改ざんされないようにする機能を検討する。
	指針14　時間が経っても安全安心を維持する機能を設ける	① 経年で増大するリスクに対し、アップデートなどで安全安心を維持する機能を検討する。
運用	指針15　出荷後もIoTリスクを把握し、情報発信する	① 欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。 ② 必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。
	指針16　出荷後の関係事業者に守ってもらいたいことを伝える	① 導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務にかかわっている担当者や外部の事業者に伝える。
	指針17　つながることによるリスクを一般利用者に知ってもらう	① 不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクがあることを一般利用者に伝える。 ② 安全安心を維持していくために一般利用者に守ってもらいたいことを伝える。

(2) 指針の例

各指針は、指針／ポイント／解説／対策例により構成されている。言葉ではイメージが掴みにくい場合にはイラストや表も活用している。以下に特徴的な２つの指針について、意図を説明する。

［指針６］つながりで波及するリスクを想定する

つながる世界では、機器やシステムに故障が発生したり、ウイルスに感染したりした場合に、つながりを通じて影響が伝播する危険性がある。そこで本指針では、このようなつながりによるリスクの想定を推奨している。

具体例としては、つながりを介して他の機器やシステムの異常やウイルスの影響を受けるケースだけでなく、自分の異常やウイルス感染により加害者となるケースも挙げている。また、安全・安心のための対策レベルが異なるIoTコンポーネントがつながることで、対策レベルが低いIoTコンポーネントが攻撃の入口になるリスクも例として挙げている。

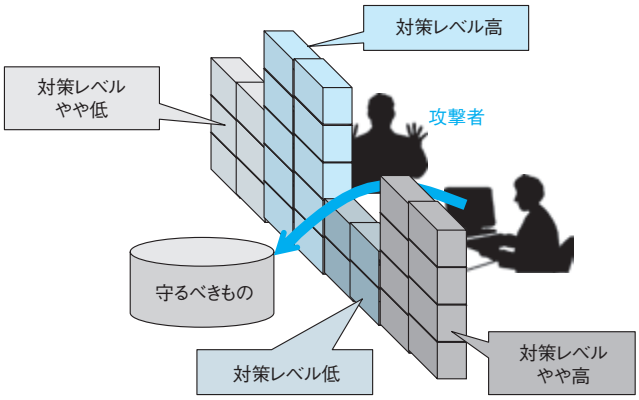


図５　弱い部分からリスクが発生するイメージ

IoTは前述の通りSystem of Systemsであるため、IoT同士が接続してより大きなIoTとなる中で、個々のIoTコンポーネントのリスクがIoT全体に波及する可能性を想定する必要がある。

［指針８］個々でも全体でも守れる設計をする

前述の指針６では、つながることによるリスクの想定を推奨しているが、本指針ではつながりをリスク対策に活用する設計を対象としている。まず、IoTコンポーネントの外部インターフェース、内包する要因、物理的接触によるリスクに対して対策を検討すると共に、IoTコンポーネントのリソース（CPUやメモリなどの能力）が不足している場合には、それらを含む上位のIoTコンポーネントで対策を検討することを推奨している。

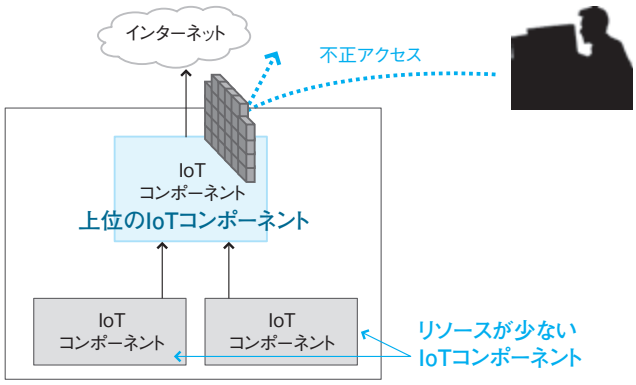


図６　上位のIoTコンポーネントで守るイメージ

更に、このIoTコンポーネントのつながりを利用して遠隔から監視し、異常検知や原因推定を行うことも例として挙げている。このようにリスクの要因となり得るつながりをリスク対策に活用することで安全・安心なつながる世界の実現が期待される。

(3) 指針の活用

開発指針については、IoTを構成する機器やシステムの安全･安心の実現に向けた検討に活用いただきたい。また、業界の実情に合わせて内容を整理することでリスク対策の実施状況のチェックリストとしても活用いただきたいと考えている。

6 おわりに

IPAは現在、多数のIoT関連の民間事業者が参画する「IoT推進コンソーシアム」が策定している「IoTセキュリティガイドライン」に対し、本開発指針の内容を反映させるべく提案を行っているところである。本ガイドラインは国のサイバーセキュリティ戦略で要求されているものであり、本開発指針を反映することによりIoTの安全・安心に寄与できると考えている。また、IoTに関連する各企業、業界団体、業界横断的団体に対して、開発指針の普及展開を依頼しているところである。具体的な現場での活用状況や課題を踏まえ、開発指針を適宜見直していくと共に、将来的には国際標準化や海外の関連団体との協調も視野に入れて進めていく予定である。

本開発指針は以下のWebサイトで公開しているので、積極的に活用いただきたい。

http://www.ipa.go.jp/sec/reports/20160324.html

「つながる世界の開発指針」に関する実証実験

SEC研究員　丸山 秀史　SEC研究員　小崎 光義　SEC研究員　宮原 真次

1 はじめに

IPA/SECでは、IoT時代を踏まえ、安全・安心な製品を開発するための「つながる世界の開発指針」を策定した。開発指針では、つながることによる事故やインシデントを未然に防ぐことを主眼に、指針ごとにポイント、解説、対策例について記載している。開発指針策定において、対策例の中には、既に確立して広く普及している技術と、まだ確立しておらずあまり普及していない技術があることが見えてきた。そのような未確立の技術の一部について、その実現性や有効性に関して実験システムを構築し、検証・評価を行った。

2 実証実験の方針

開発指針は分野共通のものであり分野間連携まで適用可能であるが、2015年度では、まずは単一の分野でその実証をする方針とした。また、対策については、なるべく特定の分野や特定の機器には依存せず、様々な分野の機器やソフトウェア製品の開発に参考となるような内容とすることを方針とした。

3 実証実験の体制

IoTにおける代表的な活動としてIndustrie 4.0がある。それと親和性の高いFA分野を実証実験の対象とした。実証実験環境には機器を連携させる基盤（ソフトウェア）が必要であり、FA分野における国内の整備状況を調査した結果、一般社団法人日本ロボット工業会ORiN[※1]協議会が開発した基盤製品ORiNがあることが分かった。また、機器や設置する場所について、一般財団法人機械振興協会が保有していることが分かった。体制としては、ORiN協議会、機械振興協会にご協力いただき、IPA/SECを含め３者で実証実験を行うことにした[※2]。

4 実験環境

実証実験環境としては、工場内のセル生産環境を想定して整備した。図１に示す通り、SCADA[※3] PC、セルコントロールPC、産業用ロボット（単軸）、産業用ロボット（６軸）、NC装置で構成した。

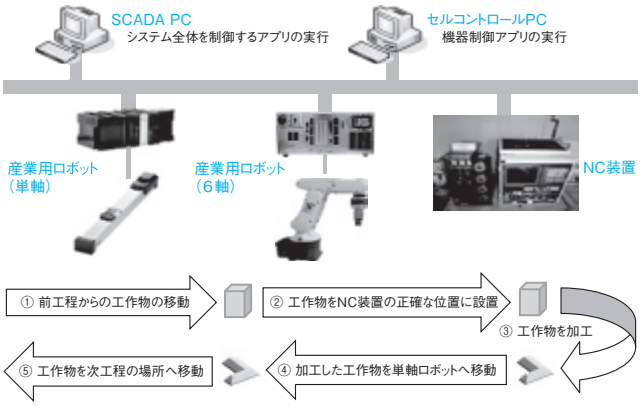


図１　セル生産環境を想定した実証実験環境

5 実証実験のテーマ選定

実証実験のテーマは、開発指針の【指針９ つながる相手に迷惑をかけない設計をする】及び【指針11 不特定の相手とつなげられても安全安心を確保できる設計をする】の２つを選定した。

(1) 障害の波及防止策（製造ライン稼働時の異常検出と対策）【指針９に対応】

工場の生産環境において、ロボットなどに障害が発生すると生産全体に影響を与える。ロボットに渡す制御データの内容や処理が複雑化しており、プログラムミスや運用ミスによる異常発生のリスクがある。更に、これらの機器がネットワークにつながるようになるとウイルス感染などにより異常動作を起こすリスクが増加する。障害の波及防止策として、工場内の装置から動作ログなどを収集し、異常を検知した場合に速やかに装置を安全に停止する仕組みについて検証することとした。

(2) 相互接続時の信用確認（要求品質が異なる装置を接続するときの対策）【指針11に対応】

ORiNなどの基盤製品が普及すると、連携可能な機器が増加する。それにより、実績がなく低品質の機器が接続される可能性が増加すると見込まれるが、そのような機器を接続すると精度の低い動作となったり、ウイルス感染のリスクなどが高まる。工場内に新規に装置を組み込む場合、その装置が信頼できる装置であることを確認するために、「品質情報」をやり取りする仕組みを検証することとした。

6 対策技術

(1)障害の波及防止策

本セル生産環境ではセルコントロールPCからロボットに動作指示が行われる。ロボットに障害が発生するとセル生産全体に影響を与えるため、ロボットの障害につながる動作指示パラメーター値の異常をいち早く検知し、障害発生前の対応を可能にする方法を検討した。そのための対策としては、ロボットが一定周期で繰り返し動作することに着目し、以下の3つの機能を導入した。

① 前準備で各機器の動作指示パラメーター値を採取して正常値として記録する機能。
② 動作指示パラメーター値を適切な時間幅で監視し、①で採取したデータと比較する機能。
③ 記録した正常値に含まれない場合は異常と判断してロボットを停止する機能。

(2)相互接続時の信用確認

相互接続時の問題に対して、以下の機能を組み込んだ。

① ロボットの信頼性を示す「品質情報」をアプリケーションから参照可能なロボットの固有情報の中に埋め込む機能。
② セルコントロールPC上のアプリケーションからコネクション確立前にその「品質情報」を確認し、接続可否を判定する機能。
③ 接続してよい信頼性であることが確認できた場合にコネクションを確立する機能。

図2　波及防止策未実施の場合

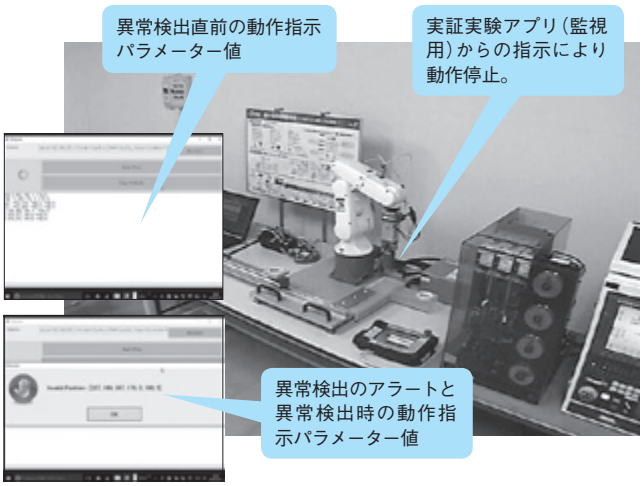


図3　波及防止策を実施している場合

7 対策技術の評価

(1)障害波及防止策の評価

図2は対策未実施の場合であり、図3は対策実施後の場合である。対策の実施により、ロボットの異常が工作物や他の機器に影響を与える前に検知できることを確認した。すなわち、ロボットの移動速度に対して十分に速い速度で異常を検知でき、結果としてロボットの障害による影響の波及抑止につながることを確認できた。また、ロボットとセルコントロールPCに対して制御に影響を与えない程度の負荷で異常を検知可能であることも確認できた。

(2)相互接続時の信用確認の評価

今回の実証実験では、ロボットとのコネクション確立前に「品質情報」を確認することで、要求品質の低い機器の接続を防止することが可能であることが確認できた。なお、今回の実証実験での「品質情報」は、実験用の品質識別子を使ったが、実際のシステムにこの対策を適用するに当たっては、「品質情報」の具体化と「品質情報」自体の信頼性を保証するための仕組みが必要である。

8 おわりに

今回は、工場内の製造機器が外部とつながったときに起こり得る異常動作のリスクや新規に機器を増設する場合の導入リスクを想定して実証実験を行った。今回、実証した異常検出及び波及防止手法や「品質情報」による信頼性確認手法は、他のIoTシステムでも参考となる対策技術であると考えている。本実験で得られた結果は、開発指針にも反映している。更に、ORiN協議会におけるORiNの次期バージョン仕様への提案や、FA以外の分野の基盤となるソフトウェアへの実装も提案していく予定である。IPAは、これらの取り組みを通じて、今後、IoT機器の安全・安心を確保する対策技術の普及に貢献していく。

本実証実験の報告書は以下のWebサイトで公開しており、詳細についてはそちらを参照していただきたい。

http://www.ipa.go.jp/sec/reports/20160511_3.html

【脚注】

※1　Open Resource interface for the Network
※2　http://www.ipa.go.jp/about/press/20151202.html
※3　Supervisory Control And Data Acquisition：産業用制御システムの一種

システムズエンジニアリングの推進

SEC調査役　室　修治

1　はじめに

近年、複数の独立したシステムが互いに関係し合って価値を提供しているような複雑なシステムが急増しており、その開発のためにシステム全体として捉えることの重要性が高まっている。欧米では、従来のシステム開発手法に加え、軍事・航空宇宙分野にリードされる形で、システムズエンジニアリングをベースとした複雑なシステムへの総合的なアプローチが取られるシステム開発事例が出てきており、標準化や方法論の知識化も進んでいる。

システムズエンジニアリングとは「システムを成功裏に実現するための複数の分野にまたがるアプローチ及び手段（INCOSE[※1]による定義）」とされており、システム開発にかかる課題解決のための有望な手法・技法と考えられるが、我が国においては適用場面や具体的技術、効果などについて認知も理解も進んでいない状況である。

これらを受け、IPA/SECでは、第４次産業革命をもたらすと言われているIoTの進展により、ITサービスの構造転換期になっていると考えられるこの機を捉え、あらためてシステム開発における課題を明らかにし、その解決策をシステムズエンジニアリングの理解を進めながら見出し、産業界に普及、展開することを目的とする活動に着手することとした。

2　事前ヒアリングの実施

活動を開始するにあたり、システム開発の現状及び課題の把握、課題解決のための取り組み状況などについて複数の企業や有識者にヒアリング調査を実施した。そこで得られたコメントのうち、下記に主要なものを載せる。

- 日本ではシステムズエンジニアリングの適用事例が航空・自動車分野などに限定されており、一般産業分野での関心が薄い。ユースケースも少なく、成功体験が普及しにくい。
- ノウハウの定式化、ツール化されていない部分が多いため、少人数のノウハウ保持者による有償コンサルサービスに限定されている。産業界で共有するためには知識体系の整備が必要である。（国際的には、システムズエンジニアリングについて、ISO/IEC/IEEE 15288:2015[※2]（システムライフサイクルプロセス）、SEBoK[※3]（システムエンジニアリング知識体系）、INCOSE システムズエンジニアリングハンドブックなど一定の標準、知識体系が整備されているが、国内の産業界には普及しておらず具体的な事例やツールの整備と共に普及のための施策が必要。）
- モデリングやシステムズエンジニアリング人材の育成が必要である。
- システムズエンジニアリングを教える大学が極めて少なく、学会もない。

3　課題の整理と取り組み項目の検討

事前ヒアリングの結果を踏まえ、更に課題の整理と取り組みテーマを検討するため、産・学より有識者にお集まりいただき、システム開発全般における課題認識の掘り起こしまでさかのぼり、そこで抽出した課題をシステムズエンジニアリングでどこまで解決できるかというアプローチで検討を進めた。

【課題の整理】

事前ヒアリングの結果に加え、参加メンバーよりそれぞれの立場で課題を提示いただき分類項目ごとに整理した。分類項目はおおよそ下記の５分類となる。

① 文化、制度、組織
② 社会環境
③ 技術、技術体系
④ 実践方法、適用方法、推進方法
⑤ 人材

議論の結果　③技術、技術体系、及び④実践方法、適用方法、推進方法について具体的に取り組む方向とし、⑤人材については育成教材の充実、上流設計に求められる人材像の明確化を当初の取り組みとし、具体的な育成については以降の検討とすることにした。また①文化、制度、組織と②社会環境の課題については上記取り組みを行う中での背景・参考として考慮していくこととした。（図１参照）

【取り組み項目の検討】

前述のように課題を整理した後、それらの解決策について検討し、2016年度以降の取り組み項目としてまとめた。第一のポイントはシステムの複雑化、システムとシステムがつながる状況での課題を解くためには、全体を的確に捉えた上で、それを適正に分解できることであり、その考え方を示すことが重要とされた。第二にそれらを実現する方法論を適用類型、効果と共に示し、理解を促進する。更に実際に方法論を現場に展開できるようノウハウや従事者の人材像を明らかにしていくこととした。（図１参照）

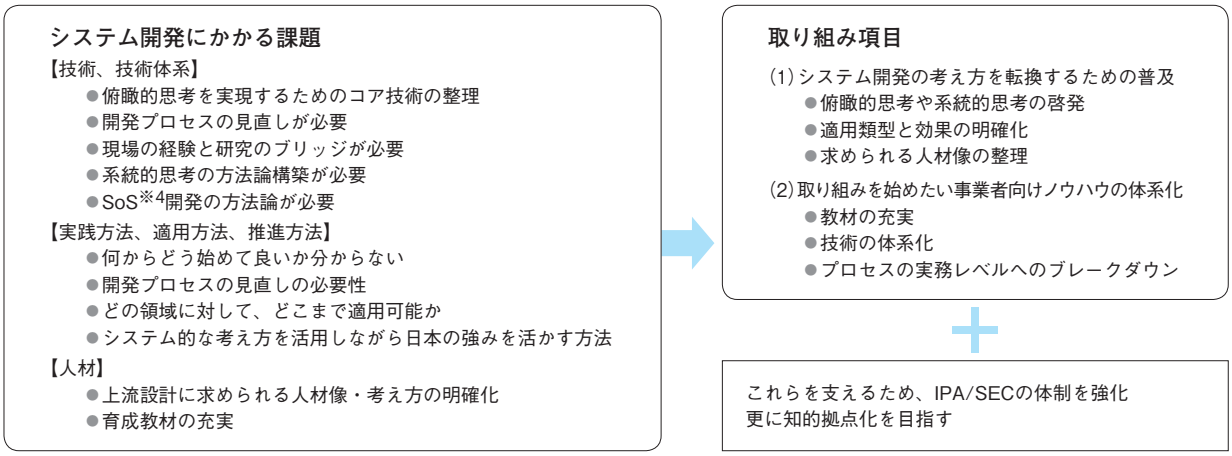


図1　「システム開発にかかる課題」と「取り組み項目」

4 課題解決とシステムズエンジニアリング

課題解決の方法論としてシステムズエンジニアリングを位置づける。上記取り組み項目におけるシステム開発の考え方の説明については、図２に示すように一般的な言葉で理解できるよう配慮し、更にシステムズエンジニアリングとは何か、どのような効果が得られるかを説明していくことを想定している。

5 今後の活動予定

2016年度については取り組み項目のうちシステム開発における課題を解決する新たな手法・技法であるシステムズエンジニアリングの有効領域について、事例に基づき効果と共に説明する啓発・入門書をまとめていくことを計画している。

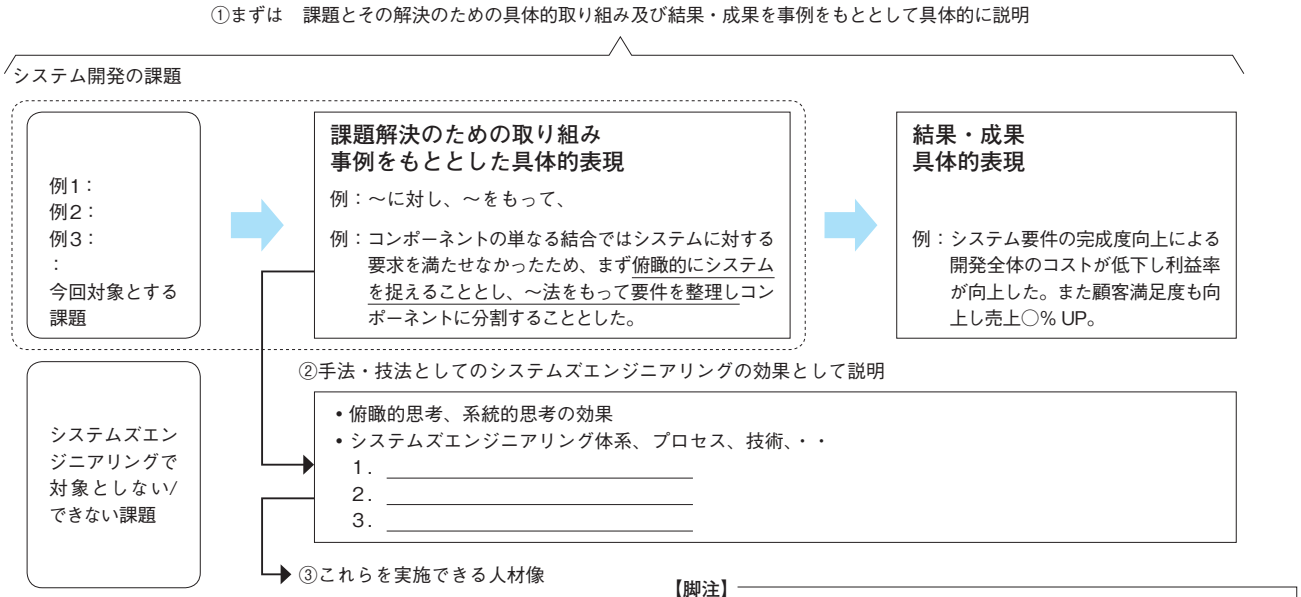


図2　課題解決アプローチとシステムズエンジニアリング

【脚注】
※1　The International Council on Systems Engineering
※2　Systems and software engineering - System life cycle processes
※3　The Guide to the Systems Engineering Body of Knowledge
※4　System of systems

先進設計・検証技術の適用事例紹介と分析

SEC調査役　室　修治
SEC研究員　藤原　由起子
SEC研究員　春山　浩行
SEC研究員　佐々木　方規

1　はじめに

システム及びソフトウェアの開発現場では、「品質確保」、「生産性向上」、「安心・安全な運用」など様々な課題を解決すべく先進的な開発技術の適用に積極的に取り組んでいるプロジェクトがある。それらのプロジェクトの事例から、ほかでは知ることのできない課題解決のための独自の工夫など、実践的な取り組み内容を紹介することにより、我が国のシステム及びソフトウェア開発の高信頼化に寄与したいと考える。

IPA/SECでは2013年度より事例収集活動を開始、最初の１年は技術、分野を限定せずに事例収集していたが、IoT[※1]などソフトウェア及びシステム開発を取り巻く状況の変化に伴い、より複雑・多様化してきた課題を解決できる技術・手法の適用事例に対象を絞り、活動を継続している。

2015年11月に「先進的な設計・検証技術の適用事例報告書 2015年度版」を公開し、2013年度版から延べ58件の事例を紹介した[※2]。更に、この公開事例58件を後述する様々な観点で分析・整理することにより得られた知見を書籍にまとめ、SEC BOOKS「事例に見る先進的な設計・検証技術の適用分析」として、2016年５月に刊行した[※3]。

目次

2　事例の収集

2015年度に収集した事例を設計系と検証系に大別し、表１に示す。設計系が10件、検証系が６件である。一部はすでに「先進的な設計・検証技術の適用事例報告書 2015年度版」として公開している。

2015年度の事例の収集は以下の方針で行った。

① 超上流及び保守・運用工程まで適用の範囲を広げて収集（表１　事例番号２、３、５、６、７）
② 開発者視点だけではなく、利用者（顧客企業）視点で課題に取り組んだ事例を収集（表１　事例番号５、13）
③ 最近注目を集めている、IoT、システムズエンジニアリング、派生開発に関わる適用事例を収集（表１　事例番号３、６、７、８、12）

3　収集した事例の分析

3.1　分析観点

2015年度上半期までの収集事例数は58件となった。これらを、「実施目的」、「適用技術」、「工程と技術の関連」、「実施時期と適用技術の傾向」、「適用技術と同時に実施した取

【脚注】

※1　Internet of Things
※2　先進的な設計・検証技術の適用事例報告書2013年度版
http://www.ipa.go.jp/sec/reports/20140530.html
先進的な設計・検証技術の適用事例報告書2015年度版
http://www.ipa.go.jp/sec/reports/20151118.html
※3　http://www.ipa.go.jp/sec/reports/20160511_1.html
※4　2015年度収集分の多くは「先進的な設計・検証技術の適用事例報告書2015年度版」で公開済みだが、一部事例（※7）は2016年度に公開予定
※5　Business Process Management
※6　Systems Modeling Language
※7　2016年度公開予定の事例

表1　先進的な設計・検証技術の適用事例一覧（2015年度収集※4）

	事例番号	標題	事例提供元
設計系	1	業務生産性向上や市場環境の変化に対応できる経営・業務を実現するために活用されるBPM※5の紹介	一般社団法人　コラボネット事業推進協会/株式会社BPM実践企画
	2	受注業務にビジネスアナリシス方法論を適用した業務システムの構築 ～中小企業の特注品業務プロセス改革の提案～	株式会社プロセスデザインエンジニアリング
	3	ビジネスへの貢献が求められる時代のソフトウェア開発の考え方 ～超高速開発ツールがもたらす方法論のイノベーション～	一般社団法人　ICT経営パートナーズ協会/MBC（Method Based Consulting）
	4	「フィーチャー」の概念を取り入れたモデルベース開発	三菱スペース・ソフトウエア株式会社
	5	大規模システム開発プロジェクトにおけるユーザーエクスペリエンス品質設計プロセスの適用とその効果	NECソリューションイノベータ株式会社
	6	モデルベース開発への移行に向けたC言語ソースコードに対する状態遷移抽出技術の適用	株式会社東芝
	7	製品開発におけるSysML※6適用の取り組み ～要求の可視化～	株式会社リコー
	8	組込みソフトウェアのアーキテクチャ設計の可視化	ビースラッシュ株式会社
	9	セイフティ＆セキュリティ設計のための準形式手法とモジュラーアプローチの設計現場への導入 ～ソフトウェアの５S三定で欠陥の少ないソフトウェアを作る～※7	セイコーエプソン株式会社
	10	短納期開発の要求を実現するWモデルの適用事例※7	株式会社リンクレア
検証系	11	まぜるな危険！プロダクトラインエンジニアリング ～バリアント管理の海外事例～※7	PureSystems, Inc、富士設備工業株式会社
	12	国際スタンダード認証に求められる「要件から検証結果までのトレーサビリティ管理」の効率化の取り組み	富士設備工業株式会社
	13	「コストモデル」を使った開発品質・生産性向上の取り組み ～バグ対応コストの見える化と最適化～	株式会社HS情報システムズ
	14	組込みシステムのユニットテストにおけるスタブ自動生成と仕様検証技術※7	ヤマハ株式会社
	15	ネットワーク型データモデルを用いた問題点の可視化と問題分析への応用例※7	株式会社日立ソリューション
	16	「SQA監査」と「確証レビュー（ISO 26262対応）」の融合 ～ SQAの更なる役立ちに向けて～※7	パナソニック株式会社

※7の事例は公開までにタイトルが変更になる可能性があります。

り組み」、「想定効果と結果の関連」、「効果の傾向」などの観点で分析し、実務適用の実態を浮き彫りにした。

3.2　主な分析結果

(1)ねらいに対する効果を表す「課題克服の割合」は97%と高く、成功事例として有益な情報であることを示している。

(2)取り組み目的のトップは品質である。

(3)品質課題の中でも、最も多い品質改善の目的は機能適合性※8（59%：34件/58件）と保守性※9（47%：27件/58件）が中心（トップ２）。保守性に注目した案件が多いことから、近年比率が高まっている派生開発案件の品質改善が重視されている傾向がうかがえる。

(4)品質改善の目的で件数が多い第三位は以下の通り。エンタプライズ系では満足性※10（33%：７件/22件）が第三位であり、利用者の満足度重視と推察される。Web・フロント系はセキュリティ※11（33%：４件/12件）であり、インターネット接続に伴う課題として重視していると考えられる。組込み・制御系は信頼性※12（21%：７件/33件）であり、製品・システムの可用性重視と思われる。

(5)半数以上の55%（32件/58件中）の事例で副次的な効果を発揮していたことから、先進的な開発技術を導入することは想定以上に様々な改善につながるものであると言える。より詳細に分析すると、品質改善は「生産性」・「コスト」・「人材育成」にも副次効果を発揮している。

(6)全数の４割を超える適用事例において、事業売上に貢献したとのアンケート回答があった。

(7)新しい取り組みをするときに気になることの一つである「先進的な開発技術の導入時に懐疑的な人、及びその理由」についてもアンケート調査を行った。結果は、「担当者」や「ベテラン技術者」が懐疑的な人の上位を占め、理由は「余計な手間がかかること」や「必要性のコンセンサスが得られない」ことが主であった。このことから、「担当者」と「ベテラン技術者」に対する合意形成活動（例えば、パイロットプロジェクトなどにより、新規技法などの遂行可能性やQCD改善効果などを実例として示す）が重要だと考えられる。

3.3　課題と適用事例・技術との紐付け

課題と適用技術の対応関係を分析し、ソフトウェア開発上の各課題について、どのような先進技術が有効であるかを明らかにした。一例を挙げると、満足性改善に効果的な主要技術は、UX（ユーザーエクスペリエンス）、HCD※13（人間中心設計）、RAD※14（高速開発）を活用したプロトタイピングなどであった。対応関係の明確化に加えて、「事例

表２　適用事例分類表（一部抜粋）：事例と適用工程や適用技術等の対応関係を示す※15

事例参照番号	適用領域①		適用領域②			適用工程共通フレーム2013										技法・手法																											
	設計系	検証系	エンタプライズ系	Web・フロント系	組込み・制御系	企画フェーズ	要件定義フェーズ	システム・ソフトウェア要件定義	基本設計	詳細設計	製作・ユニットテスト	ソフトウェア結合・総合テスト	システム結合・総合テスト	移行・運用準備フェーズ	運用・保守フェーズ	アジャイルソフトウェア開発モデル	ソフトウェアプロトタイプ開発モデル	イテレーション開発モデル【反復型開発モデル】	W(開発)モデル	BPM【ビジネスプロセスマネジメント】	MBSE【モデルベースシステムズエンジニアリング】	形式仕様記述	HCD【人間中心設計】	UX【ユーザーエクスペリエンス】	MBD【モデルベース開発】	MDD【モデル駆動開発】	保守・更改・派生開発（XDDP）	MILS/HILS/SILS	RAD【高速開発】	CASE	IDE【統合開発環境】	SPLE【ソフトウェアプロダクトライン開発】	ソフトウェアフレームワーク	テスト自動化	バグ分析（ODC分析）	形式検証	モデル検査	IV&V	耐故障性検証（運用時）	アシュアランスケース（D-Case）	セキュリティ	リスクアセスメント	独自開発・検証ツール
	7	1	2	0	6	0	3	7	6	6	3	3	3	3	2	0	1	1	0	0	8	3	0	0	5	1	2	2	1	1	1	0	0	0	0	0	0	0	2	1	0	0	1
A-10	■				■				■	■	■										■				■															■			
A-12	■				■			■	■	■	■	■	■								■				■			■															
15-A-5	■		■					■	■	■	■	■	■	■	■		■	■			■	■				■	■		■	■	■												
15-A-13	■				■			■	■	■											■				■			■															
15-A-14	■				■		■	■													■				■																		
15-A-15	■				■		■	■	■	■				■	■						■	■			■														■				
15-A-20	■				■			■	■	■											■						■												■				■
15-B-1		■	■				■	■				■	■	■							■	■																					

に見る先進的な設計・検証技術の適用分析」の適用事例分類表をもとに、Webサイトに掲載されている58件の事例から読者に最適な事例を簡単に見つけ出せるよう配慮した。求める事例の抽出条件は、下記に示す５つの軸（詳細項目数は約70）から複合的に選べる。

(1)適用領域①：　設計系、検証系

(2)適用領域②：　エンタプライズ系、Web/フロント系、組込み/制御系

(3)適用工程：　企画、要件定義、開発（システム/ソフトウェア要件定義、基本設計、詳細設計、製造、テスト）、移行/運用準備、運用/保守

(4)技術・手法：　アジャイルソフトウェア開発モデル、ソフトウェアプロトタイプ開発モデルなど28項目

(5)「課題」「効果」「今後の取り組み」の分類項目：　ソフトウェア高信頼化に影響を及ぼすと言われている主な項目、具体的には品質、生産性、コストなど

例えば、期待する効果を選択することで、適用すべき先進的な開発技術を容易に見つけ出すことができ、さらに該当する事例にたどり着くことができる。関心のある技術を選択することで、期待される効果や適用している事例を抽出することができる（表２）。

4 おわりに

2016年度についても事例収集を継続し、分析・整理を含め知見を拡充していく。収集分野は、昨年度と同様にシステムズエンジニアリングやモデルベース開発、高セキュリティ化、派生開発などに力点を置く。また、例年通り、事例を提供していただいた企業から講師を招き、現場の生の声を聞ける事例紹介セミナーなどを企画する。

【脚注】

※8　使用するときに、明示的及び暗黙のニーズを満足させる機能を提供する度合い。
※9　保守者によって修正できる有効性や効率性の度合い。
※10　製品またはシステムが明示された利用状況において使用されるとき、利用者ニーズが満足される度合い。
※11　人間または他の製品若しくはシステムが、認められた権限の種類及び水準に応じたデータアクセスの度合いを持てるように、製品またはシステムが情報及びデータを保護する度合い。
※12　明示された時間帯で、明示された条件下に、システム、製品または構成要素が明示された機能を実行する度合い。
※8～12　【参考】システム及びソフトウェアの品質モデル JIS X 25010：2013（ISO/IEC 25010：2011）製品品質モデル ８特性
※13　Human Centered Design
※14　Rapid Application Development
※15　付録（Excel形式）として右記webページよりダウンロード可能：　http://www.ipa.go.jp/sec/publish/tn16-001.html

表2　（前ページから続く）

事例参照番号	効果項目																								適用度合							
	品質														その他										レベル	1	2	3	4	5	6	7
	機能適合性	性能効率性	互換性	使用性	信頼性	セキュリティ	保守性	移植性	有効性	効率性	満足性	リスク回避性	利用状況網羅性	アシュアランス（保証）	障害原因の分析	コスト	納期	生産性（対応時間短縮）	人材育成意識改革	プロジェクトマネジメント	見積支援	普及促進	体制（強化・再構築）	グローバル展開		プロトタイプ	1プロジェクト	2～4プロジェクト	5～10プロジェクト	11以上 プロジェクト（他プロジェクト適用）	100以上 プロジェクト（部内適用）（製品適用）	1000以上 プロジェクト（全社適用）
	6	1	1	1	2	0	7	2	1	1	1	0	2	1	1	6	3	6	4	3	0	0	1	0		1	0	1	2	0	4	0
A-10	■						■	■											■	■					レベル１	■						
A-12	■						■									■	■	■	■						レベル３			■				
15-A-5	■		■	■			■	■	■	■	■		■			■	■	■	■	■			■		レベル４				■			
15-A-13		■					■									■		■							レベル６						■	
15-A-14	■						■						■			■	■		■	■					レベル６						■	
15-A-15	■														■			■							レベル６						■	
15-A-20					■		■									■		■							レベル６						■	
15-B-1	■				■		■							■		■		■							レベル４				■			

ソフトウェア工学分野の先導的研究支援事業について

SEC　調査役　小沢　理康

IPA/SECでは我が国におけるソフトウェア工学・システム工学分野の研究の促進及びその成果の産業化への展開を図る目的で、「ソフトウェア工学分野の先導的研究支援事業」を2012年度より実施している。2015年度は大学・公的研究機関からの研究提案６件を採択し、2012年度の開始から数えると20件の研究を支援している。このうち、2015年度に完了した研究６件の成果について、新たにIPAのWebページで公開した。本稿では2015年度に完了した研究成果と、2016年度事業の公募実施状況について報告する。なお、本事業は2016年度で終了し、事業の見直しを実施する。

1　研究支援事業の概要

ソフトウェアは、あらゆる産業や市民生活を支える基盤として不可欠な存在となってきており、複雑化・大規模化するソフトウェアの高信頼化や開発プロセスの高度化、それらの運用や保守についても様々な課題が存在している。また、システム同士を組み合わせて新しいシステムやサービスを開発し提供する場面が増えてきているが、ここでも開発のためのアプローチやシステムの信頼性確保のための課題が存在している。

このような課題に対して工学的なアプローチで解決策を提供しようとするソフトウェア工学や複雑な統合システム（System of Systems）へのシステム工学の適用にかかわる研究、及びソフトウェアの経済的効果に関する研究についての一層の振興をねらいとして本事業を実施してきた。

本事業では、研究内容の新規性・独自性だけでなく、研究成果の産業界への展開も重視している。IPA/SECでは産業界をはじめとする有識者から成る「ソフトウェア工学研究推進委員会」を設置し、研究区分の設定、採択テーマの選考、研究に対する助言などを実施している。

2　2015年度に完了した研究の成果

2015年度に完了した研究は、2014年度に採択した研究期間が２年度の研究が２件と、2015年度に採択した研究期間が単年度の研究が４件の計６件である（表１参照）。

表１　2015年度に完了した研究

区分※	期間	研究テーマ名	提案者名
A	２年	システムモデルと繰り返し型モデル検査による次世代自動運転車を取り巻くSystem of Systemsのアーキテクチャ設計	慶應義塾大学
B	２年	オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク	神奈川大学
B	１年	保証ケース作成支援方式の研究	名古屋大学
C	１年	携帯端末用アプリケーションソフトウェアが地方経済に与える効果の実証実験評価に関する研究	福井大学
D-2	１年	要求定義の高品質化のための要求仕様の整合性の検証知識の形式知化と一貫性検証支援ツールの開発	工学院大学
D-4	１年	データマイニング手法を応用した定性的信頼性／安全性解析支援ツールの開発	広島大学

※公募した研究区分～ A区分：「ソフトウェア工学分野の先導的な研究」、B区分：「ソフトウェア開発現場へのソフトウェア工学の適用に関する研究」、C区分：「ソフトウェアが経済社会にもたらす革新的効果に関する実証研究」、D-2区分:「ソフトウェアエンジニアリングの実践事例研究」、D-4区分:「モデルベースによるリスク評価を活用したシステムの安全性や品質の向上に関する研究」

それぞれの研究成果の概要を以下に示す。

◎システムモデルと繰り返し型モデル検査による次世代自動運転車を取り巻くSystem of Systemsのアーキテクチャ設計（慶應義塾大学）

次世代自動運転車の導入に向け、それを取り巻く交通インフラ、各種情報システムを含む周辺環境、ドライバなどをSystem of Systems（SoS）として捉えた上で、安全性を考慮したアーキテクチャを構築する。このため、安全性を脅かす状態に遷移しないよう、FDIR（Fault Detection, Isolation and Recovery）の概念を取り入れたシステムモデリングと繰り返し型モデル検査を用いることにより、安全性を確保するSoSアーキテクチャの構築方法を確立する。アーキテクチャを示すことにより、企業において次世代自動運転車を中心としたSoSを明確に捉えられるようになり、次世代自動運転車用のソフトウェア開発・設計、周辺情報システムなどの開発・設計を行うことが可能となる。

◎オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク（神奈川大学）

オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク（FFO：Formal assurance case Framework for Open systems dependability）を開発し、形式言語Agdaによる開発フレームワークとして提供する。FFO

は、アシュランス議論の記述に必要な用語定義を与える概念体系と、議論の部品や組み合わせ方のテンプレートライブラリから成る。FFOの標準的利用により、「最初にケース内容を思い付くのが困難」、「議論の仕方、品質が人によりけり」などのアシュランスケース導入時の問題を解決する。また、アシュランスケースの品質評価基準としての国際標準化活動につなげ、第三者認証の基盤を提供する。

◎保証ケース作成支援方式の研究（名古屋大学）

① 多様なモデルに対する統一的な保証ケース作成手法の研究

システムの安全性を保証するためには、システムの利用モデルや構造モデルを明らかにし、これら様々あるモデルの安全性を保証ケースで確認する必要がある。産業界における保証ケースの適用を進展させるため、多様なモデルに対する統一的な保証ケースの作成手法を研究する。

② 既存コンポーネントに対する保証ケース作成手法の研究

ソフトウェアコンポーネントを再利用することで、開発されたソフトウェアの品質を向上できる可能性がある。再利用対象コンポーネントの安全性を保証するためには、コンポーネントのモデルに対する保証ケースだけでなく、コンポーネントのコードに対する保証ケースが必要であることから、コードに対する保証ケース作成手法を研究する。

③ 保証ケースの客観的なレビュー手法の研究

作成された保証ケースの妥当性を確認するためには、保証ケースを適切にレビューする必要がある。保証ケースを構成する主張を記述する用語の適切性や一貫性、主張を下位の主張に分解する際の網羅性、主張に対する証拠の十分性などの観点から、保証ケースの妥当性を内容に踏み込んで客観的に確認するためのレビュー手法を研究する。

◎携帯端末用アプリケーションソフトウェアが地方経済に与える効果の実証実験評価に関する研究（福井大学）

本研究では、地域の商店街に活力を与える携帯端末用アプリケーションソフトウェアを開発する。開発するソフトウェアはすれ違い通信機能を利用したキャラクター育成ゲームであり、すれ違い通信を利用しているため、参加ユーザは外出して移動しないとゲームに参加することができない。従って、参加ユーザの街歩きが期待でき、商店街の活性化につながると考えられる。本ソフトウェアを利用した実証実験を実施し、参加ユーザが積極的に商店街に足を運び、各商店の来客数や売上高が増加するかを確認し、本ソフトウェアが地方の商店街に与える経済効果を明らかにする。

◎要求定義の高品質化のための要求仕様の整合性の検証知識の形式知化と一貫性検証支援ツールの開発（工学院大学）

本研究では、要求仕様の構成要素であるシナリオを取り上げ、要求仕様の品質特性である「一貫性」に着目し、ベテラン技術者が経験的に得たシナリオの整合性の検証知識を形式知化し、それら知識に基づくシナリオの一貫性検証支援ツールを実現する。開発するシナリオの一貫性検証支援ツールは、シナリオ内で言及されている、「アクター」「データ」「画面」「振る舞い」の記述が要求仕様書中の記述と整合していることを検証する。本研究の具体的な成果として、シナリオの整合性の検証知識とシナリオの一貫性検証支援ツールを提供する。

◎データマイニング手法を応用した定性的信頼性／安全性解析支援ツールの開発（広島大学）

本研究では、FTA（Fault Tree Analysis）、FMEA（Failure Mode and Effect Analysis）、HAZOP（Hazard and Operability Studies）などの定性的信頼性／安全性分析手法を支援するためのツール開発を行う。具体的には、設計や障害事例などの過去の情報を非構造型データベースとして蓄積し、FTAなどに現れる故障モードやガイドワードなどのキーワードと、対象とするシステムの設計情報（UML / SysML）を手がかりに、蓄積したデータベースから関連する過去の障害シナリオを抽出できるようにする。更に重要度に従ってランキングするシステム、ランキングを効率的に行うための学習アルゴリズムを開発する。このツールにより、経験豊富な分析者の知見を効率よく設計現場にフィードバックすることが可能となる。

3 2016年度公募の状況と採択結果

2016年度の公募に際しては、研究成果の実用化をより加速させるため、研究成果を企業が実用化する具体的な計画を研究提案の必須項目にすると共に、研究区分を２区分に絞り分かりやすくした（表２参照）。

表２　公募した研究区分

区分※	区分名	概要
A	ソフトウェア工学分野の実用化を目指した研究	ソフトウェア開発・システム開発において共通して適用可能な、要求工学、プロセス改善、高信頼性、アジャイル開発、形式手法、モデルベース開発などのソフトウェア工学分野の実用化を目指した研究。
B	ソフトウェア工学・システム工学の実践的な適用に関する研究	特定領域に対するソフトウェア開発現場への適用を目的としたソフトウェア工学の成果・手法を実用化する研究。またはスマートコミュニティ、ヘルスケア、ロボット、次世代自動車と交通システムなどの複雑な統合システム（System of Systems）の研究開発において、ソフトウェア工学・システム工学の成果・手法を適用する研究。ソフトウェアメトリクス、企業事例研究の発展、マイグレーション、モデルベース開発、ソフトウェア品質評価、システムの安全性、社会に対するサービスイメージを伴ったシステムに関する実用化に関する研究。

2016年度の公募には10件の応募があった。これらの提案については、ソフトウェア工学研究推進委員会において厳正な審査を行ったところ、採択すべき提案はなしとの結果になった。

米国における有力組織との意見交換

SEC　システムグループ　主任　八嶋　俊介
SEC　システムグループ　研究員　峯尾　正美
SEC　ソフトウェアグループ　研究員　小崎　光義

1 はじめに

IPA/SECでは、国際連携活動の一貫として、米国の有力なソフトウェア技術拠点であるNIST（米国商務省国立標準技術研究所※1）、SEI（カーネギーメロン大学ソフトウェア工学研究所※2）と定期協議を行っている。今回もこの２組織を訪問し、最新の取り組み事項について意見交換を行った。また、IV&Vの専門家として以前からIPA/SECの活動にご協力いただいているCukic博士（昨年ウェストバージニア大学からUNC（ノースカロライナ大学※3）に移籍）を訪問し、最近の取り組み内容について意見交換を行うと共に、米国の業界団体等を訪問し、IPA/SEC活動成果の普及を図った。本稿では2016年１月４日から１月10日にかけての上記米国出張について、その内容を報告する。

2 NISTとの意見交換

(1) CPS PWG※4の活動状況について

CPS PWGの関連活動として、スマートグリッド、CPS Framework概要、及びCPS PWGの５つのサブグループ（SG）のうち３つ（リファレンスアーキテクチャSG、ユースケースSG、タイミングSG）に関する情報を収集した。

本WGの取り組みとして、コモンランゲージ（共通の用語）、クロスドメインのテストベッド、ビジネスモデルを重視しているという説明があった。従来はドメイン内のデバイス間通信であったが、今後はドメイン間のインターオペラビリティが重要と考えられており、そのためにFrameworkが必要であるということであった。CPS Frameworkでは、OSIの７層モデルのようなものを目指すという説明もあった。また、具体的な事例をユースケースとして収集し議論しているということであった。

CPS FrameworkとIIC※5のリファレンスアーキテクチャとの関係について質問したところ、CPS Frameworkは実行可能なアクティビティから成る構造であるのに対し、IICのリファレンスアーキテクチャは、実際の使い方までは明確になっていないとのことであった。

また、ほかの標準類とCPS Frameworkとの関係については、標準類は指示的なものであるのに対し、CPS Frameworkは枠組みであることから、相互のギャップを埋めるため、NISTとしてもIoTの標準であるIEEE P2413やISO/IEC 30141の策定に参加し、密接に活動しているということであった。

写真１　NIST SSD（Software and Systems Division）チーフのRam D. Sriram氏と

(2) つながる世界の開発指針検討WGの活動状況について

IPA/SECが策定に取り組んでいる、「つながる世界の開発指針」について説明した。本開発指針では、つながる世界における安全安心（セキュリティ、セーフティ、リライアビリティ）について検討しており、NIST CPS FrameworkのTrustworthiness（セキュリティ、セーフティ、リライアビリティ、プライバシー、レジリエンス）と関連性が高いこと

を双方で共有した。

(3) ESCR※6とCWE※7の対応について

前回訪問時(2014年12月)、IPA/SEC内に設置されたWGで検討中のESCRとCWEの対応表を説明し、コメントをいただいた。今回の訪問では、協力に感謝すると共に、いただいたコメントをWGで議論し、対応表を公開した旨を報告した。また、引き続きESCR C++版についても同様の議論を進めていく予定であることを報告した。

3 AHAM(米国家電製品協会※8)との意見交換

AHAMは、DoE(エネルギー省※9)に対するロビー活動や、家電製品の性能に関する標準化や認証を行っている団体である。ここでは、IPA/SECの事業概要と、組込み分野への取り組みとして、ESCRの紹介を行った。

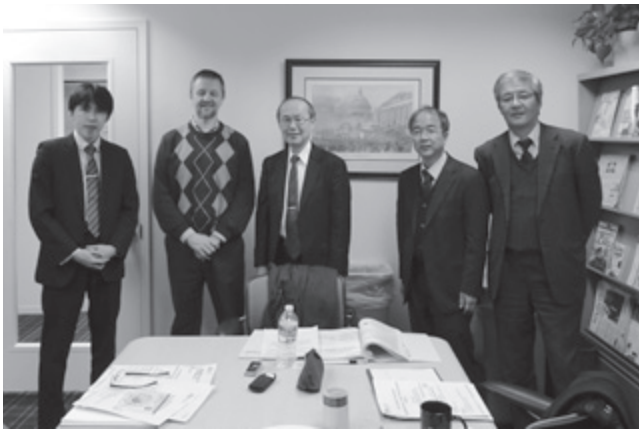


写真2　AHAM 標準化担当部長のMatthew B. Williams氏と

家電同士がつながるスマートハウスに関連して、日本においては、家電同士をつなげる標準プロトコルとして、ECHONET Liteが挙げられるが、米国ではSEPプロトコルが最も使われているとのことである。ただし、IoTへの対応はこれからという印象で、IICの動きもとくに気にしていない様子であった。

家電同士の相互接続性に関しては、5年前にAHAMからホワイトペーパーが発行されている。その中で、各プロトコルの比較表を作って評価しているとのことであった。また、標準化に関しては、家電制御の共通コマンド標準を作成しており、現在はユースケースの標準化に取り組んでいるとのことである。

IPA/SECの提供資料(ESCRの紹介など)は、約150社の会員企業に展開していただけることになった。

4 SAE International※10との意見交換

SAE Internationalの、主に自動車向け組込みソフトウェアの標準化を行っている委員会の担当者と電話会議を行った。当方からは、IPA/SECの事業概要と、組込み分野への取り組みとして、ESCRの紹介を行った。

先方の組込みソフトウェアの標準化活動は、現在活動休止中の状態とのことであるが、クライスラーのハッキング事例をはじめとした、セキュリティ対策については重要視しているようで、2016年1月末に、セキュリティに関する標準を出版する予定とのことであった。(後に、「SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems」が発行された。)

IPA/SECの提供資料(ESCRの紹介など)は、関係者に展開していただけることになった。

【脚注】

※1　NIST：国立標準技術研究所(National Institute of Standards and Technology)は、アメリカ合衆国商務省の技術部門であり、計量、標準化、基礎技術研究などを主な任務としている。

※2　SEI：カーネギーメロン大学ソフトウェア工学研究所(Carnegie Mellon University, Software Engineering Institute)は、アメリカ合衆国ペンシルベニア州に本部を置くカーネギーメロン大学に設置されているソフトウェア開発、ITセキュリティなどの研究機関である。

※3　UNC：ノースカロライナ大学(University of North Carolina)は、アメリカ合衆国ノースカロライナ州内16個所に大学を設置する州立大学の総称である。訪問したシャーロット校は、とくに工学、情報技術などの産学協同研究が盛んな大学である。

※4　CPS PWG：Cyber-Physical Systems Public Working Group

※5　IIC：Industrial Internet Consortiumは、インダストリアル・インターネットやIoTの標準化や普及推進を行う国際規模の団体である。

※6　ESCR：Embedded System development Coding Referenceは、組込みソフトウェアを作成するにあたって、ソフトウェアのソースコードの品質をより良いものとするために、コーディングの際に注意すべきことやノウハウを体系的に整理したものである。

※7　CWE：Common Weakness Enumerationは、ソフトウェアにおけるセキュリティ上の弱点(脆弱性)の種類を識別するために用いられる、共通の脆弱性タイプ一覧である。

※8　AHAM：米国家電製品協会(Association of Home Appliance Manufacturers)は、家庭用電化製品の性能や特性について、一定の基準で測定できるようにその基準を定めているアメリカの団体である。

※9　DoE：アメリカ合衆国エネルギー省(United States Department of Energy)は、アメリカ合衆国のエネルギー保障と核安全保障を担当する官庁であり、主な任務は、核兵器の製造・管理、原子力技術の開発、エネルギー源の安定確保、関連技術の開発である。

※10　SAE International：モビリティの専門家を会員とするアメリカの非営利団体である。“Society of Automotive Engineers, Inc.”が正式名称だが、“SAE International”と呼称している。

5 SEIとの意見交換

(1) ソフトウェア開発データ分析にかかわる意見交換

前回訪問時（2014年12月）の決定事項としてNDAを締結し送付した、IPA/SEC「ソフトウェア開発データ白書」のデータに基づいた共同でのデータ分析に関して、意見交換を行った。

当方からは、当該データの分析から得られた新たな知見の例を紹介し、先方からは、TSP（Team Software Process）での開発データを収集したSEMPR（Software Engineering Measured Performance Repository）の紹介があった。

双方のデータには共通項目も多いことから、まずは、共通項目が何であるかをお互いに認識し、その上で、何を分析するかをすり合わせることで合意した。双方のデータにて、同じ知見が得られるかなど、今後具体的なテーマに関して検討を進めたい。

写真３　SEIメンバと

(2) つながる世界の開発指針検討WGの活動状況について

IPA/SECが取り組んでいる、「つながる世界の開発指針」について、日本の動向を含めて説明した。日本では産官学が連携したIoT推進コンソーシアムが立ち上がり、今後取り組まれていくことについて、SEIのCTOに伝えていただけることになった。日本のIoTへの取り組みについて、深く興味を持っていただけることが期待される。

また、2016年１月開催予定のSCC（Software Certification Consortium）の会合で、セーフティ設計をテーマに各組織の取り組みが報告されることになっており、その情報を送付していただけることになった（発行日時点で開催済み）。

(3) SEIの研究 “Extending AADL for Security Design Assurance of the Internet of Things” について

アーキテクチャモデルを用いた分析／検証への取り組みとして、２つの取り組みの紹介があった。

① アーキテクチャ記述言語として活用されているAADLに、セキュリティに関する記述を拡張し、モデルを作成して形式的な検証を可能とするための研究の紹介があった。セキュリティの脅威については、STRIDE（なりすまし、改ざん、否認、暴露、サービス不能、権限の昇格）のモデルが利用されている。

本研究は、現段階では記述できる範囲はセキュリティに限られているが、今後はセーフティに関する適用も見込まれる。なお、AADLで脆弱性や安全性を分類するモデルは、MIT[※11]のNancy Leveson教授が提唱しているSTAMP[※12]に似ているのではないかと質問したところ、相互に補完しあうものであるということであった。この点について、関連資料をSEIから受領したので、今後検証したい。

② 上記と併せてDRS（Design Rule Space）を用いることで、ソフトウェアのバグの元となるアーキテクチャの問題点の検証を行う研究についての紹介があった。

(4) IPA/SECの組込み分野への取り組みについて

IPA/SECの組込み分野への取り組みとして、ESCRの紹介を行った。ここでは、関連する規格が常に更新されることなどからくる、コーディングガイドの更新の難しさに関する議論が行われた。（実際にESCRは、ver.1.0（2006年６月公開）、Ver1.1（2007年７月公開）から2.0（2014年３月公開）まで、約８年かかっている。）

また、ESCRの海外展開先としては、ベトナム、シンガポールなどのアジア諸国でも使われている旨を伝えた。

(5) SEIの研究 “Increasing Adoption of Secure Coding” について

複数の静的コードアナライザの結果をマージするツールを作成して、コーディングが終わってからではなく、コーディングをしながらセキュアコーディングに関する的確な診断を実施することで、生産性の向上を図った事例の紹介があった。

また、NISTに紹介したESCRとCWEの対応表については、SEIでもレビューいただけることになった。

6 ノースカロライナ大学（UNC）との意見交換

（1）組織の概要について

College of Computing and Informaticsの学部長から、組織の概要について説明を受けた。

- データサイエンス、データ分析、バイオマティクス（DNAなど）、ヘルスインフォマティクスなどに関連した８つのセンター及び研究所を持ち、約3,400万ドルの予算で運営されている。
- 約28,000人の学生を抱えており（当該学部は約2,000人）、シャーロット地域において最大の研究機関である。
- 情報科学からインフォマティクスへの拡張、T型人材の育成、産業と経済発展のニーズへの適用など、21世紀が必要とするリーダー人材の育成に力を入れている。

写真４　UNCメンバと

（2）最近の研究内容紹介（デモンストレーション含む）

ビッグデータ解析の例として２つの事例紹介（以下①、②）と、企業から実データを収集して行う研究（③）の紹介があった。

① ツイッターの文章を解析し、トピックごとのデータ量の変動をビジュアル化して観測し、更に位置情報と併せて表示することで、その時点でどのような事象がどこで発生しているかを解析するシステム。

② 競合しているチェーン店などに対して、顧客アンケートを実施し、改善点と対策費用などを評価することで対策すべき項目を決定し、顧客満足度を向上させる提案を行うもの。

③ 電力業界や金融業界などのシステムをモデル化してシミュレーションを行うことによって、セキュリティやレジリエンス（復旧性）に関する分析を行う研究。各企業から約10年にわたってデータを収集し、重要インフラ間の相互依存性と時間的波及を精緻にシミュレートすることが可能になっている。UNC及びGeorge Mason大学がハブとなり、NSA※13、Bank of America、MITRE※14などが参画（年間予算50万ドル）。

7 おわりに

NISTに関しては、今回、CPSやIoTに関する取り組みについての相互の活動に理解が深まり有意義であったと考えている。今後はTrustworthinessを中心に協調して活動できるスキームを作っていきたい。

SEIに関しては、ソフトウェア開発データの分析に関する共同研究について、相互のデータベース項目が開示された。窓口担当者の明確化を含め、より具体的なテーマの検討に着手できる状態となり、有意義な訪問であったと考える。

ノースカロライナ大学との議論では、産業界と密に連携して研究を進めている点が非常に印象的であった。研究項目の90％は企業のニーズに基づく研究であり、ベンチャーの支援まで行っている。日本でも産学連携が叫ばれているが、具体的な取り組みにつなげていかなければなかなか“死の谷”は越えられないと感じた。

また、新規開拓として米国の家電の業界団体と、主に自動車を中心とした組込みソフトウェア標準化委員会の担当者とコンタクトを取ることができ、双方ともESCRを広く展開いただけることとなった。このように、各業界のユーザに広く影響を与えることができる方々への紹介活動を通して普及展開を行い、現在はアジア内に閉じているESCRを、米国にも広く展開していきたい。

【脚注】

※11 MIT：マサチューセッツ工科大学（Massachusetts Institute of Technology）は、アメリカ合衆国マサチューセッツ州に本部を置く私立大学であり、５つのスクールと１つのカレッジ、51の研究機関が設置されている。

※12 STAMP：Systems-Theoretic Accident Model and Processesは、複雑なシステムに対する安全性解析の手法であり、人とシステムの間、システムとシステムの間の相互作用に着目して安全評価をするという特徴がある。この手法により、従来では対応が難しかった“システム全体”の安全評価が可能となる。

※13 NSA：国家安全保障局（National Security Agency）は、アメリカ合衆国国防総省（United States Department of Defense, DoD）の内部部局であり、電子機器を使った情報収集、暗号解読、政府情報通信システムの防護、情報分析などを担当する。

※14 MITRE：MITRE Corporationは、アメリカ合衆国政府の支援を受けて、政府向けの技術支援や研究開発を行っている非営利組織である。

システム理論に基づくアクシデントモデルSTAMP

SEC調査役 石井 正悟

IoT（Internet of Things）の普及に見られるように、コンピューターで制御されたシステムは、日常生活のあらゆる場面において密接に関与するようになってきて、システムの安全性向上が大きな課題になっている。一方で、システムの高機能化に伴い個々のシステム自体が大規模・複雑になり、更に様々なシステムがネットワークによって相互に接続されてシステムの大規模・複雑化に拍車がかかっているため、システム全体の安全性確保がますます難しくなってきている。実際に近年は、システム障害（アクシデント）もシステム構成要素に起因するのみならず、構成要素同士の間、ないし、システムと人間との間の複雑な相互作用によるものがしばしば発生している。その背景には、従来の安全性の考え方及びシステム開発手法は「アクシデントはシステム構成要素の故障に起因する」と仮定しており、システム構成要素の故障以外の事故原因（ハザード要因）をカバーしきれていないことが挙げられる。このような状況においてIPA/SECでは、システムの安全性に関して世界的に著名な米国マサチューセッツ工科大学（MIT）のNancy Leveson教授が提唱しているSTAMP（Systems-Theoretic Accident Model and Processes）に注目しつつ、コンピューターシステムの安全性向上に資する新たな手法について調査・研究・普及の活動を行っている。

1 STAMPとは

20世紀に開発されたシステムの多くは、構成要素が少なく、それらの役割も明確であり、それゆえアクシデントが起きた場合は、構成要素のどれが根本原因でアクシデントに至ったのかを分析することは容易であった。従来アクシデントは、根本原因となる機器の故障や人間のオペレーションミスがまず発生し、それがシステム内のほかの機器や人間に伝搬し、システム内で悪影響を食い止めることができずに、最終的に起こってしまうという、チェーンオブイベントの形のモデルとして捉えられていた。

しかし、21世紀になると、開発されるシステムの規模は非常に大きくなり、構成要素も爆発的に増大すると共に、要素間の相互作用も複雑になり、個々の要素の役割を理解しただけでは、もはやシステムを理解できなくなった。そのような相互作用が複雑なシステムにおけるアクシデントの原因は、一つの構成要素に限定できる要因だけではなく、複数の要素間の相互作用による要因も考える必要があった。

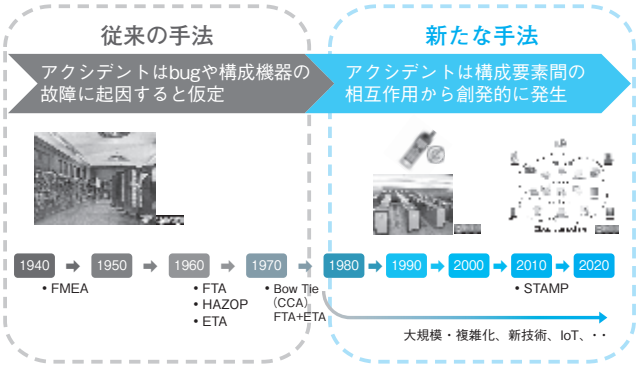


図1 コンピューターシステムと安全分析手法の変遷

MITのLeveson教授は、著書「Engineering a Safer World※1」の中で、システムの安全性は構成要素の相互作用から創発される（局所的な相互作用に隠れていたものが表面化して全体に影響を与える）ものであり、個々の要素を分割して分析するべきではないと述べた。そして、現代のシステムのアクシデントの多くは、システム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素（コントローラー：Controller）と制御される要素（被コントロールプロセス：Controlled Process）の相互作用が働かないことによって起きるというアクシデントモデルを提唱した。このモデルを「STAMP（Systems-Theoretic Accident Model and Processes）：システム理論に基づくアクシデントモデル」と呼ぶ。

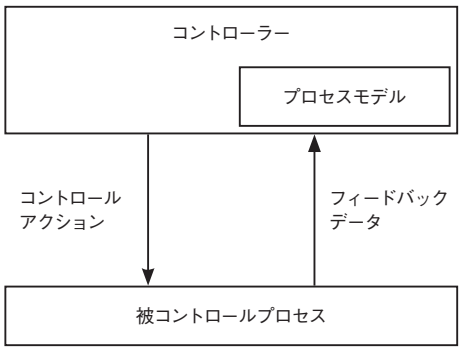


図2 STAMPにおける相互作用のモデル

STAMPモデルでは、システムの様々な階層でコントローラーと被コントロールプロセスに該当する要素が存在しており、それらの相互作用が適切に働くことによりシステムの安全が実現されるとする。STAMPモデルにおいて、アクシデントは相互作用が適切に働かないことによって起こり、具体的にはコントローラーから被コントロールプロセスへの必要な制御指示（コントロールアクション：Control Action）が適切に与えられないために起こるとしている。そして、不適切なコントロールアクションが与えられる要因として、コントローラー自身が想定する被コントロールプロセスの状態（プロセスモデル：Process Model）が、実際の被コントロールプロセスの状態を正しく反映できていないことが主要な要因であるとしている。たとえコントローラーも被コントロールプロセスも故障せずに、仕様通りに正しく動作していても、このような認識の不整合により不適切なコントロールアクションが与えられ、最終的にアクシデントにつながるというアクシデントモデルである。

2 安全性解析手法STPA

STAMP自身は分析手法ではなく、アクシデントを説明するモデルである。STAMPをベースとする、解析の道具立てやプロセスが幾つか提案されており、STPAはその一つでシステム開発を行う際などに用いるハザード分析手法である。

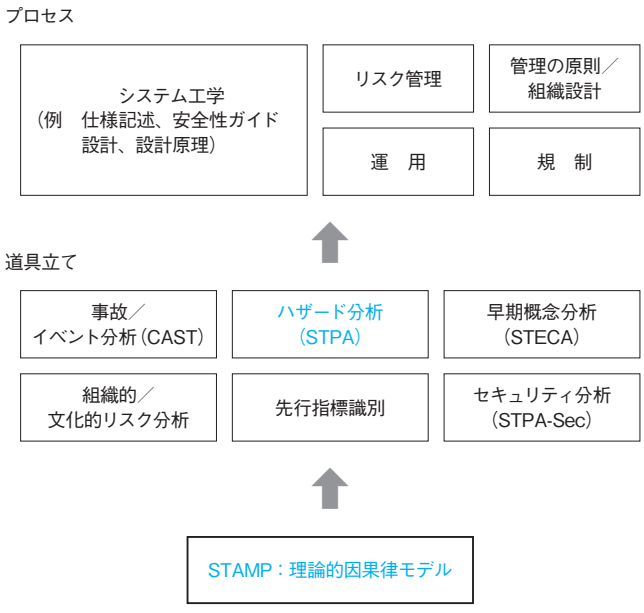


図3　STAMPに基づく分析の道具立てとプロセス※2

従来からハザード分析手法としては、強力でデファクトスタンダードとも言える手法のFTA（Fault Tree Analysis）、FMEA（Failure Mode and Effect Analysis）、HAZOP（HAZard and OPerability study）がある。それら従来手法とSTPAを比較すると表1のようになる。STPAは、複雑なシステムの「ソフトウェアの要求・設計ミス」を識別するのに適したものとされている。

表1　従来手法との比較

手法名	分析方法	特徴
従来手法（FTA、FMEA）	●フォールトツリー図や影響分析表を用いてハザード要因を分析する ●システムの構成要素と故障モードが決まるアーキテクチャー設計の段階から適用できる	●機器や組織の単一故障をハザード要因として識別する ●分岐条件を論理的に組むことで網羅的に分析できる ●深く分析できる反面、全体的な視野での分析が難しい
STAMP/STPA	●コントロールストラクチャーとコントロールループ図を用いてハザード要因を分析する ●システムの大まかな構成要素が決まる概念設計の段階から適用できる	●複数の機器や組織（人間）が、相互作用を行う複雑なシステムにおいて、相互作用のハザード要因を識別する ●過去のアクシデント事例データに基づくガイドワードにより網羅的に分析できる ●システム全体の振る舞いを確認しながら分析ができる

3 STPAの手順

STPAでは、Step 0（前準備）でシステムが安全を実現する大まかな構造を分析した後、Step 1でハザードに至るシナリオを、Step 2でハザードの詳細要因を分析する。

Step 0：（準備1）アクシデント、ハザード、安全制約の識別

対象システムにおいて分析対象となる、アクシデント、ハザード（アクシデントが潜在している具体的な状態）を定義し、ハザードを制御するためのシステム上の安全制約を識別する。

Step 0：（準備2）コントロールストラクチャーの構築

システムにおいて、安全制約の実現に関係するコンポーネント（サブシステム、機器、組織等）、及び、コンポーネント間の相互作用（コントロールアクション、フィードバックデータ）を分析し、制御構造図（コントロールストラクチャー図：Control Structure Diagram。以下、コントロールストラクチャー）を構築する。

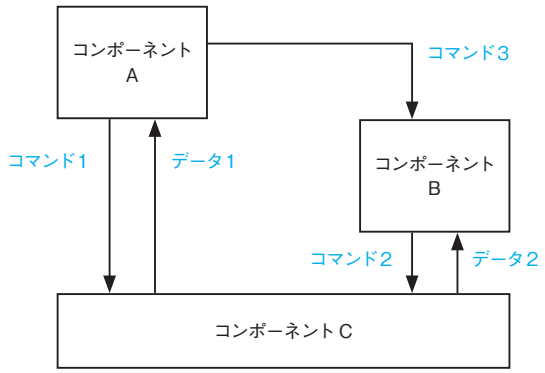


図4　コントロールストラクチャーの例

【脚注】

※1　Nancy G. Leveson：Engineering a Safer World: Systems Thinking Applied to Safety（Engineering Systems）, The MIT Press, 2012.

※2　An STPA Primer, http://psas.scripts.mit.edu/home/wp-content/uploads/2015/06/STPA-Primer-v1.pdf

Step 1：非安全なコントロールアクション（UCA）の抽出

コントロールストラクチャーから、安全制約の実行に必要なコントローラーによる指示すなわちコントロールアクションを識別し、4種類のガイドワードを適用して、ハザードにつながる非安全なコントロールアクション（Unsafe Control Action：UCA）を抽出する。

表2　非安全なコントロールアクションの抽出例

コントロールアクション	非安全なコントロールアクション			
	与えられないとハザード	与えられるとハザード	早過ぎ、遅過ぎ、誤順序でハザード	早過ぎる停止、長過ぎる適用でハザード
コマンド1	XX条件下で、コマンド1が提供されない場合、ハザードに至る（UCA1）	コマンド1の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド1の提供が、コマンド2よりも遅れた場合、指示が上書きされ、ハザードに至る（UCA2）	コマンド1が途中で停止した場合、ハザードには至らない
コマンド2	コマンド2が提供されない場合、処理が開始しないが、ハザードには至らない	コマンド2の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド2の提供が、連続した場合、指示が累積され、ハザードに至る（UCA3）	コマンド2が途中で停止した場合、ハザードには至らない
コマンド3	コマンド3が提供されない場合、処理が開始しないが、ハザードには至らない	コマンド3の内容が誤っていた場合、処理は停止するが、ハザードには至らない	コマンド3の提供が、遅い／早い場合、処理開始がずれるが、ハザードには至らない	コマンド3が途中で停止した場合、ハザードには至らない

Step 2：ハザード要因（HCF）の特定

Step 1で抽出した非安全なコントロールアクションごとに、関係するコントローラーと被コントロールプロセスを識別して、コントロールループ図を作成し、ガイドワードを適用してハザード要因（Hazard Causal Factor：HCF）を特定する。とくに、ソフトウェアや人間に起因する要因として、コントローラーの想定するプロセスモデルが、実際のプロセスの状態と矛盾することで起きる要因を特定する。

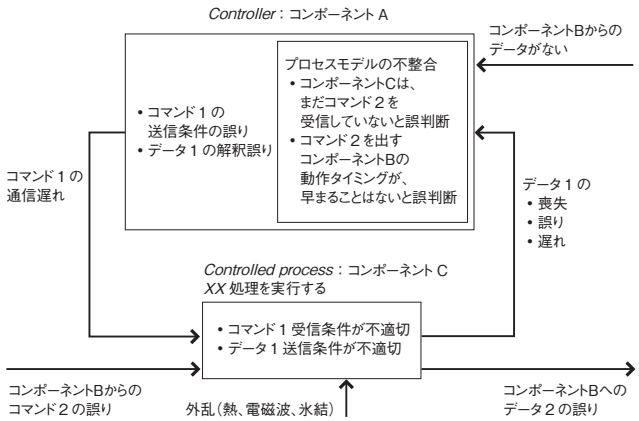


図5　ハザード要因（HCF）の抽出例

Step 1のUCA抽出において、想定外を排除するためのヒントとなるガイドワードが与えられている。

1. （**与えられないとハザード：Not Providing**）安全のために必要とされるコントロールアクションが与えられないことがハザードにつながる。
2. （**与えられるとハザード：Providing causes hazard**）ハザードにつながる非安全なコントロールアクションが与えられる。
3. （**早過ぎ、遅過ぎ、誤順序でハザード：Too early/too late, wrong order causes hazard**）安全のためのものであり得るコントロールアクションが、早過ぎて、遅過ぎて、または順序通りに与えられないことでハザードにつながる。
4. （**早過ぎる停止、長過ぎる適用でハザード：Stopping too soon/applying too long causes hazard**）（連続的、または非離散的なコントロールアクションにおいて）安全のためのコントロールアクションの停止が早過ぎる、若しくは適用が長過ぎることがハザードにつながる。

4 「はじめてのSTAMP/STPA」を公開※3

STAMP及びSTPAは非常に有効であると期待できるものの、既存の教科書は考え方を解説するものであるため、STAMP初心者にとっては理解が容易ではない。しかも、最新版を日本語に翻訳したものが公開されていない。更に、手法の実施手順についても前節のような概念的な説明であり、分析実施事例紹介でも分析実施結果のみの提示がほとんどである。そのため、いざ実際のシステムに対して分析しようとすると、どの開発ドキュメントの何と何を参照して、どのように作業すれば良いのか分からず、悩むことになる。あるいは、分かったつもりになって、誤った分析をしてしまい時間を無駄に経過させることになってしまいがちである。実際、IPA/SECがSTPAトライアルを実施したときにも上記の状況に陥った。

そこで、IPA/SECではSTAMP導入者向けに簡潔かつ具体的に手順を示す解説書を発行することとし、この度発行したのが「はじめてのSTAMP/STPA」という小冊子である。

IPA/SECでは、2015年度にシステム安全性解析手法WGを設置した。当WGでは、2015年6月にSEC特別セミナーに招聘したLeveson教授と意見交換会を実施し、それを受け我が国で実際に運用されている鉄道の踏切制御システムを対象に、STAMP有識者及び鉄道有識者を交えて、安全分析を実施した。その後2016年1月の13thWOCS[2]にLeveson教授を招聘した際にも意見交換会を実施し、上記分析結果を紹介したところ、Leveson教授から良好な評価を受けた。

本小冊子には、上記の分析結果を用いてSTPAの手順を具体的に解説している。

4.1 手順解説書の構成

本小冊子の構成は次のようになっている。

表3 「はじめてのSTAMP/STPA」の目次

はじめに
1． STAMP解説
2． STPAの手順（全体説明）
3． 対象システム概要
4． STPA分析実施例の説明
5． Advanced Technic
6． エンタープライズ系システムでのSTAMP適用
7． まとめ
おわりに

第１節と第２節には、我が国におけるSTAMP/STPAのエキスパートによる解説をつけた。STAMP/STPAの初学者にとって分かりやすい入門解説として有用であろう。当WGで分析対象とした鉄道の踏切制御システムについて第３節で述べ、分析の結果を第４節に示した。第５節には、支援ツールの活用、並びに、従来のシステム記述や分析によるシステムの振る舞いや特性の理解に基づいてSTPAを適用する試みについて述べた。第６節では、エンタープライズ系のシステムに対するSTAMP適用についての検討結果を示した。

4.2 手順解説書の特徴

以下に、本小冊子の特徴を記す。

分析作業の各Stepで、【Input/Process/Output】を整理して説明している。

表4 Input/Process/Outputの例

作業名称	UCA（Unsafe Control Action：非安全制御動作）の抽出
目的	ハザードにつながり得る制御動作の不具合を識別する（発想する）
入力	①UCAを導き出すための４つのガイドワード（４分類） ②アクシデント、ハザード、安全制約の一覧表 ③制御構造図
処理	①UCA識別の表を準備する ②最上列に４つのガイドワードを記す ③最左行に制御構造図中にある制御をすべて記す ④各マスごとに、当該（最左行の）制御動作が当該（最上列）状況になった場合、いずれかの安全制約違反に成り得るかを考える。 ⑤安全制約違反に成り得るならば、UCAであると判断する
出力	①縦軸：制御行動、横軸：ガイドワードとしたUCA一覧表。
	想定外を排除することを忘れないように。

実施例では、分析結果だけではなく、分析の際に作成した中間情報も含めて記載した。

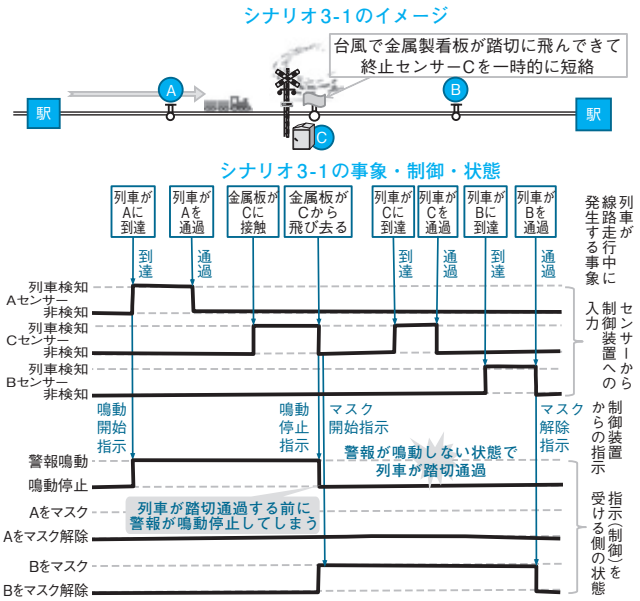


図６ 分析時に作成した中間情報の例

当WGが実際に具体的なシステムのSTPAによる分析を行い、分析結果について、STAMPの専門家、鉄道分野の専門家と議論して得た知見を整理し、勘所として解説している。

【勘所】
登場人物を整理する際には、要求仕様書に記載された登場人物のみをリストアップして、実装依存の登場人物が現れないようにする。
：
●制御とデータは区別しやすいようにする。制御は青、データは赤のように色分けしたり、制御は下向き矢印、データは上向き矢印に統一したり、など
：
コントロールストラクチャーにおけるブロック（コンポーネント）の数は4つ程度にするのが良いと言われている。

5 おわりに

IPA/SECが発行した「はじめてのSTAMP/STPA」が、システムの安全性に関するモデル化及び分析方法に関して、いくばくなりとも有用な情報を提供するものとなれば幸いである。

2015年度は主に、単線踏切制御という比較的にシンプルなシステムを取り上げて安全分析の検証を行ってきた。今後は、コンピューターシステムに人・組織が絡む複雑なシステムや、人と組織、組織と組織のプロセスに関する安全分析へのSTAMP適用可能性についても検証を行い、そこから得られた知見を公開していきたい。

2016年12月５、６日に九州大学にて、日本ではじめてのSTAMPワークショップが計画されているが、多くの産業界からの参加を期待したい。

URL：https://sites.google.com/site/stampwsj/

【脚注】
※3 http://www.ipa.go.jp/sec/reports/20160428.html

Column

半沢直樹が職を奪われないために

IPA顧問 松田 晃一

アルファ碁の衝撃

人工知能に関する話題がメディアに盛んに登場するようになった。専門誌ならばともかく、一般向けメディアでも解説や特集が組まれようになったのは、AIソフトのアルファ碁がトッププロの棋士に圧勝したインパクトが大きかったためだろう。

AIは人智を超えるのか？ AIの暴走は大丈夫なのか？人間の仕事が奪われるのではないか？などなどと話題は尽きない。AIが小説を書く、AIが作曲をする、AIが絵を描く… など、人間固有と思われている創造的な活動にまでAIがトライする世の中になってくると、本当に人智を超えてしまうのか、と考えてしまう。しかし、その可能性があるとしても大分先のことだろうから気楽だが、人間の仕事を奪うとなると、急に現実味を帯びた身近な話題となる。

AIは仕事を奪うか？

英国オックスフォード大学の研究者が発表した「雇用の未来：私たちの仕事はどこまでコンピュータに奪われるか？」という論文では、今後10年～20年の間に米国の雇用の47%が、コンピュータやロボットに職を奪われる可能性が高いとの研究結果を示し話題になっている。日本でも、野村総合研究所が同じ英国の研究者と共同で、日本を対象にした同様の研究を行い、それによれば日本の労働人口の約49%が就いている職業が代替可能との結果が得られたことを発表している。

通信販売受付係、データ入力オペレーター、金融機関窓口係、小売店のレジ係などが仕事を奪われそうな職種として並んでいる。これらは既にコンピュータに代替される兆しが見えていてあまり違和感はない。しかし、前述のオックスフォード大学の論文では、銀行の融資係、ローンオフィサーがAIに職を奪われる上位5位以内に挙がっている。

半沢直樹は仕事を失うか？

池井戸潤の人気小説の主人公、半沢直樹は融資課長ローンオフィサーだが、彼は仕事を失うのだろうか？銀行の融資係、なかでも地域に密着した金融機関の銀行マンは、融資先の経営者の会社経営に対する熱い想いと志に共感して、共に会社を育てるつもりで融資を決めるのだということを聞いたことがある。単に会社の経営指標の数字データだけからは会社の将来は見えてこない、経営者の人となりに投資をするのだ、と。このような仕事のあり方であれば、たぶんAIにとって替わられることはない人間にしかできない仕事であろう。

そういえば、近頃の医師の中には、患者の顔を全く見ずに、パソコンだけに向かって診察する医師が増えていると聞く。もし、そうだとすればこのような医師はAIにとって替わられてしまうのかも知れない。先ほどの論文では、医師は奪われる確率の最も低い職種の一つとされてはいるのだが…。

働き方への問い掛け

このように考えてくると、我々はAIに仕事を奪われることを心配してあたふたするのではなく、本当に人間にしかできない仕事のやり方をしているのか、といった仕事に対する向き合い方を問い掛けてみることが必要なように思う。AIにできることはAIに任せ、その力を借りながら本当に人間にしかできないこと、人間がやるべきことを人間がやる、という本来の働き方を取り戻していくべきだろう。

「ロボットは東大に入れるか」プロジェクトが進められている。AI技術の限界を見極め、それを克服し発展させるためのチャレンジであるが、もしプロジェクトが成功してロボットが東大に入学できたとしたら、そのときはAI技術の成果の達成を喜ぶというよりも、むしろ大学入試のあり方に対して大きな課題が突き付けられたと考えるべきだと思う。AIが合格してしまうような大学入試は、学生の資質や将来の可能性を見極める方法として果たして相応しいのかが問われるべきだと思うが如何だろうか？

書籍紹介

つながる世界の開発指針

～安全安心なIoTの実現に向けて 開発者に認識してほしい重要ポイント～

本書はIoT製品があらゆるモノとつながることを想定し、IoT製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化したものです。

自動車や家電などのあらゆる製品がインターネットに接続し、製品同士が相互に接続する「IoT社会」の到来により、利便性が高まることが期待される一方、想定外のつながりにより、IoT製品の利用者や製品の安全性・セキュリティを脅かすリスクの発生が懸念されています。このため、本書はIoT製品の安全性・セキュリティに関するリスクとその対策に着眼し、分野横断的に活用できる開発指針としています。機器やシステムの開発にかかわる企業の経営者、開発者及び保守者の方々に本書を手にしていただき、本開発指針を理解、実践していただきたいと思います。

独立行政法人情報処理推進機構
(IPA)技術本部
ソフトウェア高信頼化センター
(SEC)編集・発行

ISBN：978-4-905318-40-8
A5判・101頁
定価463円(税抜)
2016年５月11日刊

事例に見る先進的な設計・検証技術の適用分析

～高信頼化のための開発技術導入に向けて～

IPAが過去３年間で収集した58件の開発事例を分析し、先進的な開発技術を導入するメリットやその効果、開発技術のトレンドをまとめた書籍です。

IPAでは、2013年から自動車、流通、通信、医療など、様々な業種・分野における先進的な設計方法や検証技術を活用した成功事例(ベストプラクティス)を収集し、報告書として公開してきました。今回発行した本書は、これまで収集してきた事例を５つの軸で整理・分類し、想定される読者の視点で分析した結果や、先進的な技術を導入するためのポイントなどを解説した手引です。本書を活用することで、自社の事業領域と開発課題などをもとに解決策となる先進的な技術と、その技術を活用した成功事例を把握し、導入の参考とすることが可能です。

これまで、教科書的な技術や手法を解説した書籍は存在しましたが、実際の適用事例をもとに技術や手法を分析している解説書は本書が初めてとなります。

独立行政法人情報処理推進機構
(IPA)技術本部
ソフトウェア高信頼化センター
(SEC)編集・発行

ISBN：978-4-905318-39-2
A4変型判・189頁
定価926円(税抜)
2016年５月11日刊

▶上記書籍は、以下の方法で購入いただけます。　※その他、お近くの書店でお取り寄せが可能な場合があります。詳しくは各書店にお問い合わせください。
1 IPA直販　2 Amazon　3 書店(お取り扱い店舗：書泉ブックタワー(東京 秋葉原))
▶詳細はWeb サイトにてご確認ください。**SEC BOOKS：http://www.ipa.go.jp/sec/publish/index.html**

編集後記

今回発行のSEC journalは2015年度のSEC成果報告を特集しています。IoT時代を見据えた各種取り組み、詳細については本誌特集記事をご覧ください。私たちの活動から生まれる成果の特徴の一つは、理論をまとめた教科書ではなく、事例を基に分析した結果を解説している点です。これは、IPAの中立的な立場を活かし、民間では収集が困難な障害事例情報や各種開発データを収集・分析し、企業や業界を越えた取り組みとしてフィードバックすることで可能になっています。是非ご活用いただきたく、IPA/SECのWebページにお越しください。

さて、IPAオフィスのご近所には六義園(「りくぎえん」と読みます)という大変大きな庭園があり、お昼休みに散策することも可能な近さです。しだれ桜の開花時期や紅葉の季節は特に有名でテレビ中継も頻繁にあるのでご存知の方も多いと思います。周囲はビルに囲まれていますが、一歩門を入ると別世界というか非日常が待ち受けているので脳がついていけないほどです。夏のおすすめは「滝見の茶屋」、あずまやの横を渓流が走り、岩の間から落ちて水しぶきをあげています。都会の中でマイナスイオンを思い切り浴びる経験はいかがでしょうか。　（編集長）

編集部より

次世代のソフトウェア・エンジニアリングに関して等、忌憚のないご意見をお待ちしております。下記のFAXまたはメールにてお気軽にお寄せください。

SEC journal 編集部　FAX：03-5978-7517
e-mail：sec-journal_customer@ipa.go.jp

SEC journal 編集委員会

ペンギン（旭山動物園）　撮影：K.Hasegawa

SEC journal 第12巻 第1号（通巻48号） 2016年7月1日発行

編集兼発行人　独立行政法人情報処理推進機構
技術本部　ソフトウェア高信頼化センター
所長　松本 隆明
〒113-6591　東京都文京区本駒込2-28-8　文京グリーンコート センターオフィス16階
Tel：03-5978-7543　Fax：03-5978-7517
URL：http://www.ipa.go.jp/sec/　e-mail：sec-journal_customer@ipa.go.jp

SEC journal 論文募集

独立行政法人情報処理推進機構（IPA） 技術本部 ソフトウェア高信頼化センターでは、下記の内容で論文を募集しています。

論文テーマ

・ソフトウェア開発現場のソフトウェア・エンジニアリングをメインテーマとした実証論文または先導的な論文
・ソフトウェアが経済社会にもたらす革新的効果に関する実証論文

論文分野

品質向上・高品質化技術、レビュー・インスペクション手法、コーディング手法、テスト／検証技術、要求獲得・分析技術、ユーザビリティ技術、プロジェクト・マネジメント技術、設計手法・設計言語、支援ツール・開発環境、技術者スキル標準、キャリア開発、技術者教育、人材育成、組織経営、イノベーション

応募要項

締切り　：1 月・4 月・7 月・11 月　各月末日
査読結果：締切り後、約 1 カ月で通知。「採録」と判定された論文は SEC journal に掲載されます。
応募方法：投稿は随時受付けております。応募様式など詳しくは HP をご覧ください。
http://www.ipa.go.jp/sec/secjournal/papers.html

SEC journal 論文賞

毎年「採録」された論文を対象に審査し、優秀論文には SECjournal 論文賞として最優秀賞、優秀賞、所長賞を副賞と併せて贈呈します。

IoT 時代に活躍する**【組込みシステムの腕利きエンジニア】**を目指す！

国家試験 エンベデッドシステムスペシャリスト試験

高度な実践能力の証明に！

▶ 身近な場面を想定した出題を通して、最適な組込みシステム実現のために必要となる高度な実践能力（レベル 4）を問います。
（レベル 4 の定義）：専門分野において、自らのスキルの活用によって、独力で業務上の課題の発見と解決をリードするレベル。

技術要素	開発技術	管理技術
プロセッサ、メモリ、バス、計測・制御、リアルタイム OS、プラットフォーム、電気・電子回路、ネットワーク、セキュリティ	・要求分析の実行とレビュー ・設計の実行とレビュー ・テストの実行とレビュー	・開発環境マネジメント ・知財マネジメント ・構成管理、変更管理

▶ 近年の試験では、「無線通信ネットワークを使用した安全運転支援システム」、「3 次元複写機」、「通信機能をもつ電子血圧計を用いた健康管理システム」、「非接触型 IC カードを使用した入退場ゲートシステム」などのテーマを出題しました。

▶ 自動車、家電、モバイル機器などに搭載する組込みシステムや重要インフラの制御システムを、ハードウェアとソフトウェアを適切に組み合わせて構築し、求められる機能・性能・品質・セキュリティなどを実現できる組込みエンジニアを目指す方に最適です。

試験概要

【試験区分】エンベデッドシステムスペシャリスト試験（情報処理技術者試験 高度試験の 1 区分として実施）
【日　　時】年 1 回の実施（毎年 4 月第 3 日曜日）
【申込受付】毎年 1 月中旬から 2 月下旬（予定）まで WEB・郵送で申込み受付

詳しくは、Web ページをご覧ください。http://www.jitec.ipa.go.jp/index.html
試験概要の最新情報、過去問題、活用事例などをご紹介しています。

IPA Better Life with IT

SEC journal No.45
第12巻第１号（通巻48号）
2016年７月１日発行

ISSN 1349-8622