ベリサーブ技術通信

Spring 2016
Periodical Magazine
Presented by Veriserve.

2016年3月発行

VERISERVE NAVIGATION
ベリサーブナビゲーション

Vol. 5

情報セキュリティの脅威に常に
さらされる時代。
安心・安全なシステム運用のカギは
「定期的な検証」と「人の管理」

品質の真実　他

VERISERVENAVIGATION | Vol. 5

ベリサーブナビゲーション

Spring 2016

Contents

インタビュー

筑波大学 図書館情報メディア系 准教授 石井 夏生利 氏

情報セキュリティの脅威に常にさらされる時代。安心・安全なシステム運用のカギは「定期的な検証」と「人の管理」

INTERVIEW

巻頭特集

インタビュー ｜ 筑波大学 図書館情報メディア系 准教授　石井 夏生利 氏

情報セキュリティの脅威に常にさらされる時代。安心・安全なシステム運用のカギは「定期的な検証」と「人の管理」

あらゆる情報がネットワーク化している現代社会では、増え続ける個人情報や企業の機密情報に対するセキュリティリスクの問題が常につきまといます。全国民にかかわるマイナンバー制度もスタートした今、より安心・安全で高品質なシステムを運用するために企業が取り組むべきことについて、情報セキュリティ関連の法律を専門とする筑波大学 准教授・石井 夏生利氏にお話を伺いました。

情報セキュリティ、プライバシー侵害のリスクが高まっている

――「情報化社会」の最新トレンドについて、注目すべき動きやポイントについてお聞かせください。

石井 個人の情報としては、2008 年ごろからライフログ（注1）が注目を集めています。その後、ビッグデータ分析がトレンドとなり、こういった情報をマーケティングに活用する企業が現れました。さらにIoT（注2）が登場し、通信機器でないものまでネットワークにつながるようになり、センサーで個人が追跡され得る世の中になってきました。仕事柄、若い世代と接することが多いのですが、知らないうちに個人情報が集められ分析される“プライバシー侵害”の危険性はメディアなどでたくさんとりあげられているのに、位置情報の制限を付けずにSNS をやっている人などを見ると、自分の情報を外に出すことへの抵抗感が薄いと感じます。バイトテロ（注3）がなくならないのも、危機意識が低いことの表れでしょう。残念ながら即効薬はありませんが、自分の個人情報を不用意に公開したり、他人のことを勝手にネット上に書いたりする場合のリスクを授業で繰り返し話し、注意を促しています。

社会やIT 技術が大きく変化する中、個人情報保護法が改正されました。改正法では、機微な個人情報を取得する際には同意を取らなければならないなど新たな規制も入っていますから、企業は改正内容に配慮しなければなりません。同時に、「匿名加工情報」といってデータを匿名加工することで同意を得ずに第三者提供できるようにするための内容が盛り込まれ、匿名加工の方法が検討されています。

ですが、ある事業者にとっては匿名であっても、ほかの事業者が違ったデータと組み合わせると個人を特定できるかもしれないなど課題が多く、どう頑張っても完全な匿名化は難しいと、技術の専門家の中でも言われています。匿名化した情報をビッグデータとして販売／活用するなどビジネスチャンスとして考える企業もあると思いますが、コンプライアンス上のリスクも考慮し、より慎重になるべきと考えています。ちなみに、アメリカには情報を匿名化することで義務を軽くする法律（HIPAA プライバシールール）があります。EU も匿名化された情報にはデータ保護法を適用しないというルールはありますが、具体的な方法等は定められていません。

企業にとって「自社の営業秘密をどう守るか」は今も昔も変わらない課題です。それに対する国の動きとしては、経済産業省から出ている営業秘密管理指針（注4）や、不正競争防止法（注5）の改正が大きなトピックと言えるでしょう。まず営業秘密管理指針ですが、改正により解釈を緩やかにすること

石井 夏生利 氏

いしい かおり／1996 年司法試験合格。弁護士業務、企業法務部での勤務を経て、2004 年より情報セキュリティ大学院、2010 年 4 月より筑波大学 図書館情報メディア系 准教授。専門はプライバシー権や個人情報保護法、情報セキュリティ法など。

で、これまで要件を満たせなかった中小企業なども不正競争防止法の保護を受けられるようにしています。不正競争防止法については、大企業の基幹産業が危なくなるような機密情報が外国に漏れていたという事件を受け、情報保護を強化するための改正がなされました。

このように法規制も進んではいますが、システムやネットワーク、サービスが急速にグローバル化する今、企業も個人も自分自身でどうやって情報やプライバシーを守るかを意識することが求められると思います。

注 1：個人の日々の生活や体験などを記録したデータ。体調や食事、位置情報などの記録のほか、広義には SNS やブログへの投稿を含めることもある

注 2：Internet of Things。モノのインターネット。コンピュータやスマートフォンなどの情報・通信機器に限らず、さまざまなモノに通信機能を持たせることで、インターネット／クラウドサービスと情報交換・制御などを行う仕組み

注 3：アルバイト店員が勤務中に店の商品や什器を使って悪ふざけをし、その様子を撮影して SNS などに投稿すること。投稿された画像が Web 上で広く拡散されることで店舗や企業は深刻なダメージを被り、臨時休業や閉店・廃業に追い込まれることもある。「アルバイトによるテロ行為」を略した和製英語

注 4：企業の機密情報（営業秘密）が不正競争防止法で保護を受けるために必要とされる最低限の水準の対策を示すもの。平成 27 年に全面改訂された

注 5：営業秘密の侵害やコピー商品の販売などを規制し、公正な市場を確保するための法律。平成 27 年に改正が行われ、外国企業への情報漏えいなどが厳罰化された

巻頭特集

インタビュー ｜ 筑波大学 図書館情報メディア系 准教授　石井 夏生利 氏

情報保護と情報活用の「せめぎあい」を解決するには

―― ここからは特に企業において「どう情報を守ればよいか」についてお聞かせください。この1月よりマイナンバー制度が始まりましたが、企業がとるべき対策に変化はあるのでしょうか。

石井 先ほどお話した企業の営業秘密保持とは異なり、マイナンバーの安全管理は義務であり、違反すれば罰則もありますから、まずはその意識をしっかり持っていただく必要があります。ここまで厳しく法で定められているのは、マイナンバーにより個人のさまざまな情報が紐づけしやすくなるためです。とはいえ、多くの企業は「個人番号関係事務実施者」（注 6）であり、基本的には従業員の情報を集めて税務署などに提出するのみですから、個人情報と大きく違った管理をしなければならないということはありません。マイナンバーが記載された書類や記録媒体はキャビネットに保管する、データにはアクセス制御をかけるなど、定められた管理措置に沿って扱えば問題ないでしょう。

例えば、中小企業など今まであまり厳格な管理をしていなかったケースもあるかと思いますが、最低限の対策だけでも早急に整える必要があります。またどの企業であっても、外部の人間が PC などに触るときには特に注意しなければなりません。きちんと対策できているかどうか今一度確認していただきたいと思います。

――マイナンバーをはじめ個人情報保護の強化が求められる中、ビジネスにおける情報活用のニーズとせめぎあう状況があると思います。両立させることはできるのでしょうか。

石井　難しいテーマではありますが、避けては通れない問題ですね。解決の一つの方向性として、個人情報（プライバシー）保護の観点から、私が注目しているものに「プライバシー・バイ・デザイン」という考え方があります。カナダのプライバシー・コミッショナー（監督機関）が提唱し、世界的にも浸透しつつあるもので、システムの運用・設計の初期段階からプライバシー保護を組み込んでいこうという考え方です。

個人情報保護法は義務として企業に課せられるものであり、プライバシーも、侵害されたら事後的に損害賠償請求の対象になるという、いわば後ろ向きな発想でした。一方、「プライバシー・バイ・デザイン」は“ゼロサム”ではなく“ポジティブサム”で機能させるという、前向きな発想です。初期設定でプライバシーを事業運営やシステム設計に組み込み、相互でプラスの効果を図っていこうという点において、上手い取り組みであると注目しています。

また、「プライバシー・バイ・デザイン」を具体化させたものが「プライバシー・インパクト・アセスメント」といって、情報漏えいや目的外利用などのリスクがないかなど、あらかじめ用意したリストに沿ってチェックする仕組みです。アメリカ、カナダやオーストラリアに続き EU が今度の改正で採用する方向で動いています。日本でも、先般のマイナンバー法の特定個人情報保護評価において「プライバシー・インパクト・アセスメント」に基づく手法が導入されました。

この特定個人情報保護評価の対象は行政機関です。

注 6：行政機関がマイナンバーを業務利用する際に補助的に扱う立場にある事業者（主に民間企業）。自らの業務でマイナンバーを利用するものは「個人番号利用事務実施者」と呼び、税務署や年金事務所、保険組合など主に行政機関がこれに当たる

民間企業が対応する義務はないのですが、企業システムにこの仕組みを入れておくことで、プライバシー保護を担保したうえで情報活用を図る道筋が見えてくるのではないでしょうか。そもそも大規模システムを導入する際などには、自主的な取り組みとしてなんらかのチェックリストをベースにセキュリティを検証する仕組みを入れておくことが望ましいと考えています。今後はソフトウェアだけで対処するのではなく、このように“仕組み”として制度を設計し、リスクを下げる手法が主流になるのではないかと思います。

第三者機関によるセキュリティ検証がますます重要に

―― 企業の負担が重くなるばかりに思えますが、どう対応していけばよいのでしょうか。

石井　これらの取り組みを自社だけで行うのでなく、認証制度や第三者機関を活用することで、負担を軽くすることはできるはずです。客観的な立場・基準での検証があるかないかでは信頼性にも大きな差が出てきますし、このような第三者機関によるセキュリティ検証の必要性・重要性はますます高まっていくと考えています。

セキュリティに関して国内で幅広く使われている認証制度としては「ISMS」や「P マーク」がありますが、必ずしもこれらだけに限定する必要はありません。認証機関とは別のセキュリティ専門事業者などによるサポートを受け、セキュリティ基準を作成し定期的に検証する運用体制を整える……といった取り組みでも十分だと思います。

システム検証については、標的型攻撃の増加などの背景もあり、システムにバグや脆弱性が残ったまま使うのはあまりに危険です。ウイルス対策の更新や、事前の検証でシステムのバグをなくしておくことの重要性は言うまでもありません。こういった場面でも多くのノウハウを持った第三者機関による検証は有効でしょう。

また、ユーザビリティ（使いやすさ）とセキュリティは両立しないとも言われていますが、使いにくいシステムでは、使用者の都合で勝手に使い方を変えたり、ルールに沿わない使い方をしたりする恐れが生じ、情報漏えいのリスクが高くなってしまいます。そのような事態を防ぐためにも、ユーザビリティとセキュリティのバランスまで考慮した検証をしておきたいですね。

―― 最後に、セキュリティのあり方について企業の経営者が意識すべきポイントを教えてください。

石井　システムの整備やチェックはベストエフォートとしてやらなければならないものです。先に触れたとおり、第三者によるウイルスやバグの検証は欠かせませんが、さらに重要なのは一度チェックして終わりではなく、定期的な検証を続けることです。コスト削減や効率化だけにとらわれず、こういった取り組みこそがシステム品質の基本となることを理解していただけたらと思います。

また、情報を触るのは人ですから「システムの定期的なチェック」に加えて「人の管理」も重要です。自社の社員だけでなく、派遣社員も適切に管理しなければなりませんし、委託先の監督も必要になります。例えばクラウドサービスで、海外事業者は使わないという方針を採ったとしても、国内事業者であればどこでもよいわけではありません。セキュリティレベルも事業者によって差がありますから、情報管理の体制や情報開示の姿勢などを考慮したうえで委託先を選定することをお勧めします。

もう一つ、経営者として早い段階で行ってほしいのが、システム構築における「経営判断」です。企業としてなんとしても守りたい情報はどれなのか、また従業員のマイナンバーといった他者が関わる情報の取り扱いなど、情報によってどの程度のセキュリティで守るのかを経営視点で見極め、自社に必要なシステムを構築することがスタートとなります。そのシステムが正しく稼働しているかを定期的に検証し、人の管理を行うことで、何が問題なのかがはっきりと見えるようになり、明らかになった問題点を次へと活かしていく……、それが「安心・安全なシステム運用」の実現につながるのです。

―― 高度情報化社会においては常に情報漏えいのリスクを前提に高品質なシステムの運用に努めなければいけないということですね。関連する法整備や新たな仕組みに目を向け、また第三者によるシステムの検証やそこに携わる“人”の定期的な管理を継続的に行うことが必要であるということが分かりました。

本日はお忙しいところ貴重なお話をありがとうございました。

オープンソースソフトウェアの課題と

昨今、ソフトウェアの開発にオープンソースソフトウェア（OSS）は必要不可欠な存在となっています。本稿ではOSSの最新トレンド、OSSを利用する際の課題と対策、有効活用するためのベストプラクティスを説明いたします。

はじめに

まず、OSSを使わずにソフトウェアを開発する状況を想像してみて下さい。FacebookやGoogle、PayPal、Twitter等の巨大ITビジネスは生まれていたでしょうか。AppleはiPhoneを予定通りにリリースできたでしょうか。また、クラウドやコンテナ、IoT等の急速な事業発展は可能だったでしょうか。

答えは「NO」のはずです。では、なぜOSSがそのような加速的なソフトウェア開発を可能にしたのでしょうか。

それは、ずばり「品質」です。OSSはソースコードが無償で公開されているため、コストやスピード面でのメリットがあり、高い品質があるからこそ、企業のミッションクリティカルなシステムで積極的に利用されています。

ではなぜ、OSSの品質は高いのでしょうか。OSSは限られた技術者が開発するクローズドソースに比べて、コミュニティの「多くの目」がソースコードを精査します。そして、その数が多ければ多いほど、レビューの精度は高くなり、バグ修正や新機能の追加も迅速に行われます。まさにOSSの品質の高さはコミュニティ型ソフトウェア開発によってもたらされた、「オープンイノベーション」の賜物であると言えるでしょう。

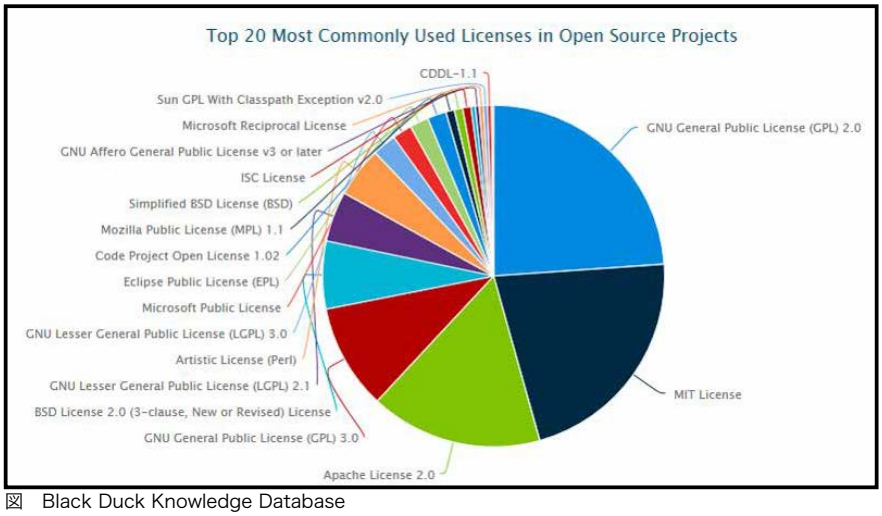


図　Black Duck Knowledge Database

それならば、OSSを利用すれば無条件に優れたソフトウェアを生産してくれるのかと聞かれると、残念ながらそうではありません。ではOSSを活用する上で留意すべき課題とは何でしょうか。ここでは3つの課題を考察し、その課題を克服しながらOSSを最大限に活用する、ベストプラクティスについて提示いたします。

課題と対策

最初に挙げる最大の課題は「OSSライセンスのコンプライアンス準拠」です。特にOSSを製品に組み込み、販売をする場合、利用したOSSのライセンス条件を理解する必要があります。代表的な例で言えば、GPL（＊1）等のコピーレフト（＊2）ライセンスは再頒布する際、ソースコードの開示が必須であり、海外のOSSライセンス係争事例のほとんどがGPL絡みです。実にGPLとその派生ライセンスの占める割合は47%（＊3）です。多くの優れたOSSのライセンスがGPLである現状を鑑みますと、GPLとうまく付き合うことがOSS活用のキーとなると言っても過言ではないでしょう。

ライセンス違反の多くが予期しないOSSの混入によって引き起こされていることから、オフショア開発ベンダーから納品されたコードや購入した第三者コードを水際で検証するプロセスは必須です。ソフトウェアサプライチェーンからのOSS混入を含むコンプライアンスポリシーの策定と運用は避けて通れないプロセスですが、OSSの規模（＊4）と複雑さ（＊5）を考慮すると、エクセル等を利用したマニュアル運用は不十分です。何故なら、Ｅｘｃｅｌでの管理はマニュアルでの更新が必要であり、OSSの規模と複雑さに対応できないためです。その結果、自動化ツールによるソースコード内

有効活用のヒント

ブラック・ダック・ソフトウェア株式会社
代表取締役
金　承顕 氏

の OSS の検知を開発プロセスの一部として運用することが求められます。

2つ目に重要な課題とされているのがセキュリティ脆弱性のリスク管理です。年間 4,000 件以上の脆弱性が報告されており、2014 年はまさにこの問題が顕在化された年でした。Open SSL の Heartbleed（＊ 6）を代表とする主要な OSS プロジェクトで脆弱性が発見され、多くの企業がどのアプリケーションで OSS が利用されているかを調査・確認するために多大な時間と労力を費やしました。

OSS セキュリティ脆弱性の特徴は、市販されている様々なコード解析ツールではほぼ検知されないことです。またソースコードが公開されている OSS は脆弱性の対象になり易く、YouTube でその手口が公開されていることもあります。これらの発見や対策はコミュニティや研究者によって行われ、NIST（＊ 7）が運営する National Vulnerability Database で公開されていますので、企業では利用している OSS の脆弱性情報をいち早入手し、被害を最小限に抑えることが重要となります。

最後の課題として、「OSS 運用リスク」が存在します。先に考察した 2 つの課題のような対外的リスクは

（＊ 1）GNU General Public License のこと。1983 年に MIT のリチャード・ストールマンによって発表された GNU プロジェクト内のソフトウェアの利用許諾条件などを定めたライセンスの一つ。主にフリーソフトウェアの開発、配布のために用いられるもので、FSF (Free Software Foundation) が公開している。

（＊ 2）コピーライトに対する考え方で、著作権は保持しつつプログラムを利用、改変、再頒布できる権利。

（＊ 3）ソース : Black Duck KnowledgeBase　（ 前ページ下図参照 ）

（＊ 4）Black Duck KnowledgeBase の最新データでは OSS プロジェクト数は 1,200,000、ライセンスの種類は 2,400、脆弱性データは 130,000 を超える。

（＊ 5）ライセンス A の OSS プロジェクトに含まれるファイルではライセンス B を有したり、ライセンスが宣言されていない OSS も存在する。また、バージョンによってライセンスが変更されたり、複数ライセンスを持つ特殊な OSS もある。

（＊ 6）2014 年に発覚したオープンソース暗号化ライブラリ「Open SSL」の脆弱性。

（＊ 7）National Institute of Standards and Technology（アメリカ国立標準技術研究所）

金　承顕 氏

（きむ　しょうけん）
ブラック・ダック・ソフトウェア株式会社
代表取締役
1985 年カリフォルニア大学バークレー校卒業、
同年リクルート入社、情報通信事業に従事。
2009 年 1 月に米 Black Duck Software, Inc. の
日本法人を設立し、代表に就任。

オープンソースソフトウェアの課題と有効活用のヒント

ブラック・ダック・ソフトウェア株式会社
金　承顕 氏

ありませんが、OSS を戦略的に利用する組織にとっては避けて通れない課題です。主な問題としてバージョンの氾濫が挙げられます。同一 OSS プロジェクトが複数アプリケーションで利用されて、しかも必要以上のバージョン数があり、バージョン間で大きな乖離がある場合、OSS 導入時の事前検証コストや OSS に脆弱性・不具合が見つかった場合の調査コストが会社内で重複するため、全体のサポートコストは跳ね上がります。また、古いバージョンに対してはコミュニティからのサポートが無くなることもあります。

有効活用のために

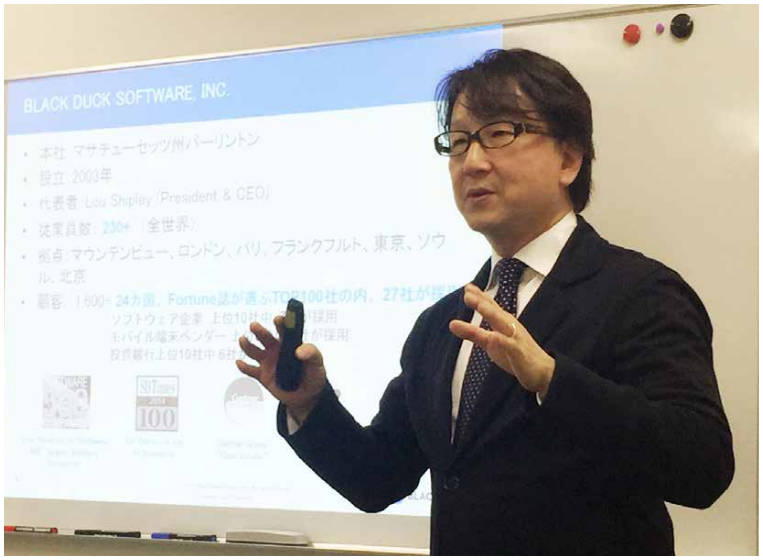
運用リスクを軽減するには社内で利用されている OSS とそのバージョンを可視化し、バージョンの統一を目指すことが求められます。同様に OSS コミュニティの動向や方針、次期バージョンについて理解し、自社の開発サイクルに適応することにより最適な OSS プロジェクトの利用が可能となります。

3 つの課題を克服し、OSS をソフトウェア開発で最大限活用するためのキーポイントは、以下の 6 つのテーマにまとめることができます。

1. 検索と選択：自社アプリケーションに最適な OSS プロジェクトを検索、評価、選択する
2. 社内利用の承認：開発部門だけでなく、利用目的に応じて法務・知財、セキュリティ、品質担当等からの承認を得る
3. カタログ管理：承認された OSS プロジェクト情報を一元管理し、バージョンやライセンスなどのメタデータ、また利用されているアプリケーションを把握する
4. コードの検証：開発プロセスにてコードの検証を行い、ライセンスに準拠しているか、影響度の高い脆弱性について対策を採っているかを確認する
5. モニタリング：アプリケーションのリリース後でも、脆弱性等の最新情報を迅速に入手する
6. 開発プロセスへの組込み：既存のソフトウェア開発サイクル・ツール群に組込み、自動化することで OSS 管理の効率化をアップする

上記のテーマに対して、OSS ツールベンダーが提供する OSS 管理プロセスを実現するプラットフォームを利用することが、ソフトウェア開発における OSS 活用に大変有効です。お客様が開発・運用しているアプリケーション内の全ての OSS を可視化し、ライセンス、セキュリティ脆弱性、運用リスクを明確にします。さらに、社内で実績を積んだ OSS は他アプリケーションでも再利用することが可能となり、開発のスピードアップ、コストダウンが実現され、自社の開発リソースを付加価値の高い分野につぎ込むことが可能となります。

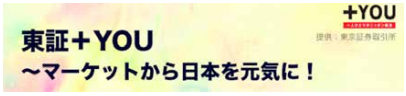
品質の高い OSS が溢れている昨今、これらを利用しない手はありません。その上でソースコードが公開されている OSS を安易に使うのではなく、課題やリスクを把握・克服した上で OSS の持つ強みを最大限活かせる開発手法をきちんと保持することが、品質向上の非常に重要なポイントとなるでしょう。



ラジオ NIKKEI に当社の新堀社長が出演しました

インタビュー内容を大公開

◆放送日時　：　2015 年 12 月 16 日（水）　11 時 10 分　～　11 時 25 分
◆番組コーナー：　マーケットプレス内　「東証+YOU ～マーケットから日本を元気に」
◆提供：東京証券取引所
◆司会進行：和島英樹、内田まさみ



2015 年12月16日（水）、東京証券取引所が提供するマーケットプレイス内「東証＋ YOU ～マーケットから日本を元気に」の番組に、当社の新堀社長が出演いたしました。実際のラジオは「東証＋ YOU」から聴くことができます。（2016 年 3 月 17 日現在）
当社の歴史やサービスを分かりやすくお伝えする内容となっておりますので、是非お聞きください。

まず番組の冒頭にて、司会進行の和島英樹さん、内田まさみさんのお二人より、ベリサーブの証券コード（3724）、創業、歴史について簡単なご紹介がありました。その後、新堀社長へのインタビューが始まりました。

1．事業内容

和島さん：まず、御社の事業内容をお伺いしたいのですが。
新堀社長：はい。ソフトウェアそのもの、あるいはソフトウェアが組み込まれている製品の動作検証を主な業務として行っております。

和島さん：上場会社で専門的におやりになっている会社って、そんなに多くは無いですよね？

新堀社長：多くはないですね。特に専業となるとかなり絞られてくるのではないかと思います。

和島さん：そうした中でも、御社の強みはどういうところでしょうか？

新堀社長：当社が創業したのが 2001 年になりますが、当時、正にこういったことを専業にしている会社が無かったと思います。そこからテスト、検証といったものをどういう風にやっていけば良いのか？という事を標準化したり、理論化したりしてきまして、当社は草分け的な存在だと思います。そういった意味では、非常に高い技術力を持っていることが強みになると思っております。

和島さん：ソフトウェアの検証といっても、扱う業種や機器など、凄く広そうな感じがしますが、そのあたりはいかがでしょうか？

新堀社長：非常に幅広くやっています。家電から産業機器、最近では自動車とか、かなりソフトウェアが入ってきていますので、検証の必要性が増えてきています。また、ソフトウェアの検証だけでなく、そこで培ってきたノウハウや経験を、製品の品質向上であるとか、あるいは開発のプロセスを組み替えて行って、より効率的な開発をするとか、効率的にしながらも、製品の質を高めて行くといった、プロセス改善のような業務が増えてきていて、業務の幅は広がってきています。

和島さん：取引されている会社数はどれくらいですか？

新堀社長：累計になると思いますが、大体 700 社位になります。

和島さん：700 社！？社数で 700 だと、製品数はもっと多くなりますね！

新堀社長：そうですね。製品自体も色々派生開発のような形でバージョンが変わっていったり機能が付加されたりということがずっとありましたので、そういった意味では、2001 年からやってきてかなり幅広いお客様とお取引させて頂いていますし、色々な経験を積ませて頂いていると思います。

和島さん：普通に考えてもスマートフォンとかデジカメだとかパッケージソフトは当然そうなのでしょうけれど、凄く色々な製品がありますよね。

新堀社長：そうですね。今や、ソフトウェアが入っていないものはたぶん無いというぐらい、広がってきていると思います。もちろんウェブももの凄く進歩してきていますし、使われ方も非常に多岐に及んできていて、且つそのソフトウェアで製品の良し悪しが決まるという時代になってきていると思うので、これからますます業務的には広がってくると思います。

内田さん：アナログからデジタルに変われば、御社の活躍の場がさらに拡大して行くということになるわけですよね。

新堀社長：そうですね。実際メーカーさんも、これまではあまりソフトウェアが入っていなかったのですが、これからは入れていかなければいけない。あるいは、ソフトウェアで制御する･コントロールする領域が凄く広がって、複雑化してきているので、これまでのやりかたでは通用しないということでお話を頂く、という機会も増えてきていると感じています。

2．事業環境の変化と対応

2-1 事業環境の変化

和島さん：関係としては良好な感じがしますが、事業環境について社長はどのようにご覧になっておられますか?

新堀社長：昨年から業績も良くなってきて、今期も好調になってきています。先ほども申し上げましたが、やはりソフトウェアの量・複雑さというのが高まってきています。それから製品開発のスピードも、国内外の競争に勝つという意味では、非常に早くなってきていると思います。ですから、今非常に環境自体は追い風なのだろうなと思います。

和島さん：お客様からすると、スマートフォンでもデジカメでもそうですが、凄く競争が激化している中で、やはり良い製品をちゃんと出す、ということが必要になってきていますよね。

新堀社長：そうですね。そこには早さということが求められますし、効率的に業務をこなし、且つ品質を高めて行くということも常に求められているのだろうと思います。

2-2 品質向上への対応

内田さん：顧客企業様にとっては、御社に色々な作業をやってもらうことで、会社にとってコスト削減になる、ということにつながるわけですか?

新堀社長：トータル的にはそういうところまで行けると思いますし、逆に我々としては、そういうところまで訴求していくべきだと思います。特に、ただ単にテストをするのではなくて、プロセスの見直しをご提案します。例えばお客様が、あるプロセスを順に追ってやっているところの無駄とか、あるいは抜けとかをチェックしながら、「そうであればこういうプロセスで開発されたほうが、あるいはテストを同時に組み込んでいったほうが良いのではないでしょうか」とかです。一般的には、テストは製品が出来上がってからやるものだと思います。ただ我々の強みのもう一つは、製品を作る段階、つまり設計の段階から、この製品の仕様だったらどういうチェッ

クをしなければいけないだろうか?ということを、開発の上流工程から設計していって、ちゃんと出来ているかということを開発の進捗と同時に行っていることです。上流工程からプロセスに組み込んでしまうことで、手戻りが少なくなる。例えば、仕様書の曖昧さだとか、仕様書にここまで盛り込まなくてはいけないですよ、ということが抜けていたりすると、実際のプログラマーが、システムを組むときに、勝手な思い込み、あるいは誤解をしてプログラムを組んでしまう。そうすると、出来上がったものが、当初想定していたものとちょっと違った形になってきます。それがバグとして出てきたりしますけども、この時点で対処しても、バグは減ってこないですよね。バグの数が増えてしまう。で、手戻りをするのでもう一回ここから作り直そう、となります。ところが、上流から、あるべき品質を固めて行くと、プログラミングがすごく効率的に行えるということがあって、結果として手戻りが発生しません。ここで何が良いかというと、同じ製品を作るにしても、2、3 回往復して作るところを、1 回で済むとなると、人件費・開発のコストがかなり減ってきます。そのようなことを、我々のサービスとしてご提供させて頂いています。

内田さん：なるほど。コスト削減にもなるし、高品質で確かなものを、スピード感をもって作れるようになるということなのですね。

2-3 環境変化への対応

和島さん：今 IoT とかモノのインターネットだとか、インダストリアル 4.0[1] とかって、私共も取材に行っていて凄い事になりそうな感じがするのですけど、やっぱりこれも今お話されたように、ちゃんときっちりやっていかないという話ですよね。

新堀社長：そうですね。それもありますし、アジャイル開発という言葉があったりしますけども、いわゆるウォーターフォール型で開発して行って、これを同時進行していくときに、どういった形で品質を高めて行くのかという取り組みも、これからはもっと必要になってくると思います。

和島さん：もう一点、自動車ですね。これは、ソフトの塊みたいになっていると思うのですけど、このことについていかがでしょうか?

新堀社長：まさにここは我々としても注力している分野です。おっしゃるとおり、自動車そのものがソフトウェアの塊みたいになっています。ソフトウェアが乗っている量もそうですけど、自動車の動作も複雑なセンサーを組み合わせながら作っていったり、制御していったりということが行われていますし、もちろん安全とか安心とかが求められています。且つ、燃費ですとか、いくつも超えなければいけないハードルがあって、そこをソフトウェアでやっていくようになってきています。これは今も注力していますけれど、これからも非常に注意深く見ていきたいですし、我々の出来ることはどんどん出していきたいと思っています。

和島さん：機械だったら壊れる、で済みますけど、自動車の場合安全・人命に関わってきますね。

内田さん：実際に業績の中身を見ると、自動車関連やエンタープライズ向けのところが、非常に伸びているのですね。案件が増えていますね。

和島さん：あと身近なところだと、電力の自由化とかマイナンバーとか話題になっていますけど、これもやっぱり同じ感じですよね。

新堀社長：そうですね。国の制度が変わったり仕組みが変わったり、規制が入ってきたり、あるいは取れたりといったときに必ず何かの変更が発生します。その時はもちろん製品も変わったりするでしょうけれども、その変更にどう対応するかは、やっぱりシステムが重要だと

1 ドイツ政府が主導し、産官学共同で進めている国家プロジェクト
http://www.sbbit.jp/article/cont1/29936

思います。なので、何かイベントがあるときは、非常に大きな需要が出てくると思います。

3. 研究活動

内田さん：御社の場合はホームページを拝見しても産学連携していろいろな研究を既にスタートさせているようですね。

新堀社長：そうですね。もともと創業の前から検証というものをどういう風にやっていくか?とか、経験と勘だけではなく、そこに理論化とか、標準化みたいなことを取り入れていって、効率よく質の高いサービスを提供して行くという観点で、勉強会のようなものを大学の先生方にお力添えを頂きまして行ってきています。

内田さん：宇宙関連のところも研究されているような感じですが、いかがですか?

新堀社長：はじめに「宇宙」と聞いたときに、「そこまではなぁ」と思ってはいたのですが、ただ、最近の開発スピードは速まっていることとか、どんどん民間に事業が移って行くんだろうと見ていると、そこを視野に入れてやるというのは面白いと思います。JAXA 様の中では IV&V という、独立的な立場で Verification と Validation という、検証と妥当性をチェックするという手法で、宇宙開発の機器の検証をやっています。宇宙はこれから可能性が広がってくると思いますので、いつぐらいかとか、どれくらいの規模かとかいうことはまだありませんが、夢を見るという意味では非常に夢のたくさん詰まった分野なのだろうと見ています。

4. 将来像

内田さん：そうすると、10 年後、御社はどんな姿になっていそうですか?

新堀社長：テストとか検証というところで我々は事業をスタートしていますけれども、そこから派生していって、世の中のシステムとか製品などの品質をどう高めるか?といったところに、一つのツールとしてテストが使えればと思います。あるいは、これまでやってきた中から、品質を高める為のサービスが生まれてくればいいと思っています。特に、日本の製品が世界で売られていったり、あるいはグローバルな企業が日本に入ってきたりというのを考えると、その中できちんと結果を出して行ける、世界にも通用する技術やサービスを出して行けるような会社になれたらいいと思っています。

和田さん、内田さん：今日はありがとうございました。

新堀社長：ありがとうございました。

収録後記：

定刻 5 分前に東京虎ノ門の株式会社日経ラジオ社受付に着くと、笑顔で編成製作局 / 情報製作局 / 解説委員の和島英樹さん、アナウンサーの内田まさみさんに出迎えていただきました。
(ちなみに、和島さんは直前に開催した、東大シンポジウムに来て頂きました。)
挨拶もそこそこに、何部屋もある他のスタジオをぬって奥へ行き、目指すスタジオへ入りました。そして世間話をしながら緊張をほぐして頂き、音取 (社長の声量と録音機のレベルあわせ) をしたあと、自然な流れで話しが始まりました。事前収録ということもありラジオに出演しているというよりは、通常の会議室で話をしているという雰囲気であっという間に収録が終了しました。

「安全設計」を、原子力発電に例えて
分かりやすく解説するシリーズ

第４回：原子力発電の安全設計

皆様こんにちは。東第三の東（弘）です。安全設計の紹介の第四回になります。引き続き御付き合いいただければと思います。

■コラムの流れ

前回のコラムでは、4．核分裂の連鎖と 5．原子力発電の仕組みについてお話ししました。今回は 6．原子力発電の安全設計を紹介します。

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

6．原子力発電の安全設計

日本の原子力施設は（日本以外もですが）、安全性確保のための基本的な考え方を持っています。それは何重にも安全対策を行う考え方で、多重防護（もしくは深層防護）と呼ばれており、以下のとおり 3 つのレベルで防護策をとり、事故を防止しようという考え方です。

第1のレベル）異常発生防止対策:異常の発生を防止する。
第2のレベル）異常拡大防止対策：異常が発生した場合には早期に検知し、事故に至らないよう異常の拡大を防止する。
第3のレベル）事故影響緩和対策：事故が発生した場合にも、その拡大を防止し影響を軽減する。

図 1 はこの多重防護の考え方を図にして示したものです。第 1 のレベルで異常の発生を防止するのですが、「人間はミスを犯す」「機械は故障する」ことを前提に、もし異常が発生しても第 2 のレベルで食い止め、それでも駄目なら第 3 のレベルで影響を抑えようというものです。

このような多重の防護設計によって、どんなことが起こっても大きな事故には繋がらないように思えます。本稿では、この中の「第 1 のレベル）異常発生防止対策」に関する幾つかの安全設計の事例を紹介したいと思います。これまでに紹介してきた 1 章から 5 章までは、本章の事例説明にあたって必要となる情報でした。しかし覚えている方はいらっしゃらないと思いますので、以下、簡単に箇条書きでおさらいを行います。

a) 核燃料（ウラン 235）に中性子がぶつかると、2 個の原子核と平均 2.4 個の中性子に分裂する。
b) これを核分裂反応と呼ぶ。原子核内の結合エネルギーが解放され、大エネルギーを放出する。
c) 核分裂反応によって産まれた中性子を、別のウラン 235 にぶつけることを繰り返すことで、核分裂が連鎖し、まとまった大きなエネルギーを得ることができる。
d) 核分裂反応は熱中性子（エネルギーの低い中性子、すなわち速度の遅い中性子）で起こる。
e) しかし核分裂反応で産まれた中性子は、エネルギーが高い（高速である）。
f) 次々と核反応を連鎖させるために、中性子の速度を減速させるための減速材が必要である。
g) 中性子は（弾性散乱する物体は）、自身と似た重さの原子にぶつかるほど速度が落ちやすい。
h) 日本の商業用原発の減速材には、中性子とほぼ同じ重さの水素原子を含む「水」を用いている。

6-1. フェールセーフの事例（制御棒駆動電源喪失への対応）

最初に、フェールセーフの事例を紹介します。フェールセーフは、**「アイテムが故障したとき、あらかじめ定められた一つの安全な状態をとるような設計上の性質」**（JIS Z 8115:2000 デイペンダビリティ（信頼性）用語）のことです。フェールセーフ設計では、装置やシステムは必

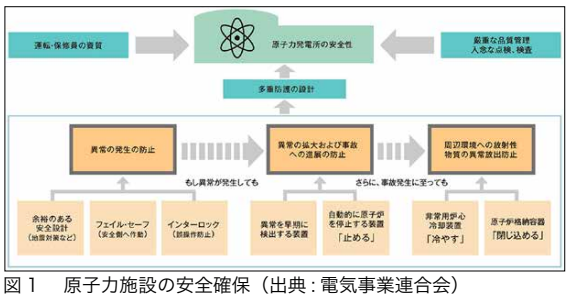


図 1　原子力施設の安全確保（出典：電気事業連合会）

ず故障するということを前提にし、故障した場合でも常に安全側に制御するように設計します。この**フェールセーフ設計の一つが、制御棒の駆動機構に取り入れられています。**

制御棒とは原子炉の出力制御に用いられる棒で、ホウ素やカドミウムといった中性子を吸収する材料でできています。この制御棒は**原子炉の出力を抑えたいときに使用**します。出力を抑えたいときには、制御棒を炉心にグッと挿入し、炉内の中性子を制御棒に吸収させます。そうすると、炉内の中性子が減るため、核分裂反応の量が減少します。逆に、起動時など原子炉の出力を上げたいときには、制御棒を炉心から抜き、炉内の中性子を増加させます。

制御棒は、地震発生時などの緊急時には特に重要となってきます。**緊急時には制御棒を炉心に一斉挿入して原子炉を即時停止（原子炉スクラムと呼びます）させなければなりません。**原子炉を安全に運転するためには、制御棒をいかなるときでも炉心に挿入できるよう、常に制御棒を制御できる状態でなければなりません。**図２**に原子炉の断面図を示します。制御棒は、原子炉の型によって挿入方向に違いがあります。BWR の場合（図２の左側）は原子炉下方から、PWR の場合(図２の右側）は原子炉上方から、電動駆動で挿入します。

制御棒制御に対する安全への脅威の一つに、**駆動用電源の喪失**が挙げられます。もし駆動用電源が喪失すると、いざというとき制御棒を炉心に挿入することができなくなるかもしれません。こうならぬよう、駆動用電源が喪失した場合でも制御棒を炉内に挿入できるよう、**制御棒駆動機構は電源装置が故障することを前提に設計されています。**例えば、PWR の場合、電磁石で制御棒を吊り上げる設計になっています。もし電源が喪失しても、電磁石の電源が切れて制御棒が重力で落下、炉内に挿入されます。重力を利用できない BWR の場合でも、ガス圧やバネを利用して、押し上がるように設計することで、電源喪失時に対応します。このように、制御棒の駆動は、駆動用電源の喪失という脅威に対しても安全側に制御するような設計、すなわちフェールセーフ設計を行っています。

6-2. フォールトトレランスの事例（電源設備の冗長化）

次に、フォールトトレランスの事例を紹介します。フォールトトレランスは、**「放置しておけば故障に至るようなフォールトや誤りが存在しても、要求機能の遂行を可能にするアイテムの属性」**(JIS Z 8115:2000 デイペンダビリティ（信頼性）用語）のことです。フォールトトレランスは、冗長技術の利用などで達成できます。冗長系（多重系）のシステムを組んでおき、一系が故障しても他の系で機能を補うことができるように設計しておくということです。

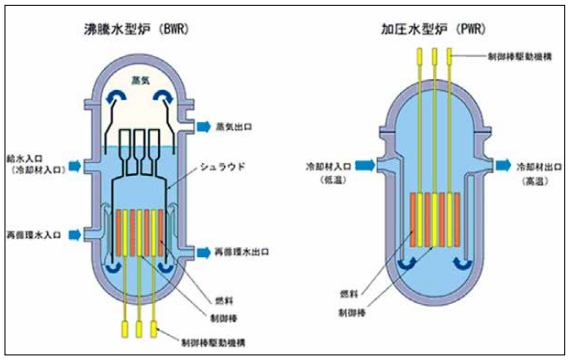


図２ 原子炉圧力容器断面図（出典：資源エネルギー庁）

原子炉には緊急時に炉心を冷やす装置が設置されています。この装置をいかなるときでも動作させるため、常に装置の電源が確保されていなければなりません。そのため、電源確保のために、複数の非常用電源（複数の発電機やバッテリー等）の備えや、複数の外部電源供給ルートの確保を行っています。このように、**電源設備の故障という脅威に対しても、電源供給に関する冗長系のシステムを組んでおき、機能を維持するような設計、すなわちフォールトトレラント設計を行っています。**なお、ここでは電源に関する冗長系について説明しましたが、**炉心冷却のための注水系システムなどにも冗長系システムが組まれています。**

6－3. 原子炉の本質安全設計の事例（自己制御性による安定化）

最後に、本質安全設計の事例を紹介します。日本の商業用原子力発電所の原子炉は、減速材に水を用いていると述べました。実は、**減速材に水を用いることは、原子炉の異常の発生を防止する方策の一つであり、本質安全設計にあたります。**

安全防護や安全装置などの他の力を借りず、システム自体で安全を確保する設計を本質安全設計と呼びます。固有安全設計や受動安全設計と呼ぶこともあります。本質安全設計の基本的考え方は、**危険源の除去（もしくは影響や発生確率の低減）と危険源の隔離**です。先に紹介した２つの事例も本質安全の方策の１つと考えて良いですが、脅威自体を完全に取り除いている訳ではありません。本項では、自然法則を利用し脅威自体が起こらないような設計を紹介します。

原子力発電における通常運転時は、原子炉内の**核分裂の量が時間と共に変化しないように（すなわち一定を保つように）制御**されています。１つの核分裂で産まれ

東日本第三事業部
東 弘之

る中性子は 2.4 個程度と述べましたが、そのうち 1.4 個は、制御棒で吸収させるなどして核分裂で用いられないようにしています。そうすることで、核分裂の量を一定に保つことができます。この状態を**臨界状態**と呼びます。

しかし、もし何らかの事故が発生し、制御棒が引き抜かれたまま操作できなくなったら、どうなってしまうでしょう。核分裂で産まれた中性子を満足に吸収することができず、産まれた中性子のうち平均 1 個以上の中性子が次の核分裂に使われるような状況に陥るかもしれません。こうなると、時間と共に核分裂の連鎖が増え始めます。このような、**連鎖が増える方向にある状態を臨界超過（もしくは超臨界）状態**と呼びます。原子炉起動時など、制御下におかれた臨界超過状態は問題ないのですが、制御不能な状態での臨界超過状態は、核分裂反応の暴走に繋がる恐れがあり、非常に危険です。が、**減速材に水を用いていると、このような状況に陥ったとしても、核分裂反応は暴走しない**のです。その理由を説明します。

核分裂反応が増加すると、応じて発熱量が増加します。すると、炉内の減速材（水）の温度が上がります。BWR の場合は、水の沸騰が激しくなりますので、**蒸気の泡（ボイド）が多くなります。**PWR の場合は、水が沸騰しないように圧力を掛けていますが、温度上昇と共に水が膨張するため、結果として水の密度が下がります。いずれにしても減速材の密度が下がるのですが、そのとき中性子はなかなか減速しなくなります。**図 3** をご覧ください。**沸騰すればする程、中性子が減速しなくなる**イメージを表してみました。このようにして中性子がなかなか減速しなくなると、核分裂反応は抑制されます。なぜなら、以前「4－2．核分裂連鎖の条件」項で説明したとおり、**核分裂反応は熱中性子で起こりやすく、高速中性子では殆ど起こらない**からです。このように、核分裂反応が増加すると、回り回って核分裂反応が抑制される結果となります。**図 4** にこれら現象を纏めました。これら効果をボイド効果や密度効果と呼びます。

減速材に水を用いた原子炉は、核分裂の暴走を防ぐ方向に反応が抑えられる特性、すなわち自己制御性を持っています。現在の日本の商用原子力発電所は冷却材・減速材に水を用いています。水を用いることで、原子炉が暴走し出力が上がったときでも、**図 5** のように自己制御が働きます。冷却材・減速材に水を選択することは、本質安全設計にあたります。他の国では、減速材に黒鉛を使った炉も稼働しています。例えば、ロシアで稼動している黒鉛減速沸騰軽水圧力管型原子炉と呼ばれる炉は減速材が黒鉛です。この型の炉には、特定の条件下で正の反応度フィードバック、すなわち核分裂が暴走するリスクを持ったものもあります。

あとがき

連載第四回目は、原子力発電所における安全設計の事例を紹介しました。まず、日本の原子力施設は安全性確保のため、多重防護の考えで作られていることを述べました。そして安全設計の事例を 3 つ紹介しました。**フェールセーフ設計とフォールトトレラント設計、本質安全設計**です。

勿論これら安全設計は一例にすぎず、他にも至る所に安全設計や安全対策が行われています。例えば、高性能高品質の機器や材料の使用、異常な温度や圧力にも余裕を持って対応できるスペックなどは、フォールトアボイダンス（「製造、設計などにおいて、アイテム及び構成要素にフォールトが発生しないようにする方法又は技術」（JIS Z 8115:2000 デイペンダビリティ（信頼性）用語）の思想に基づいた設計と言えます。

次号は、安全設計の概念について述べたいと思います。

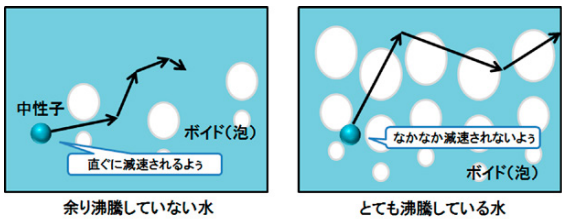


図 3　中性子の減速イメージ

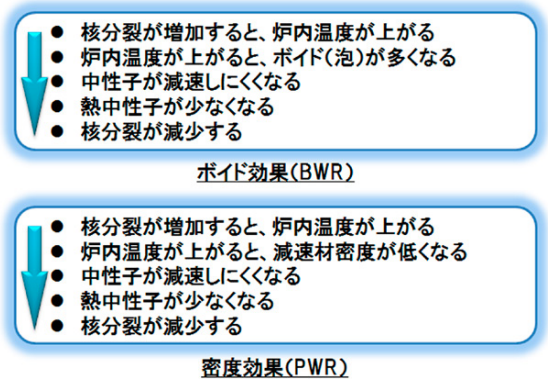


図 4　ボイド効果と密度効果

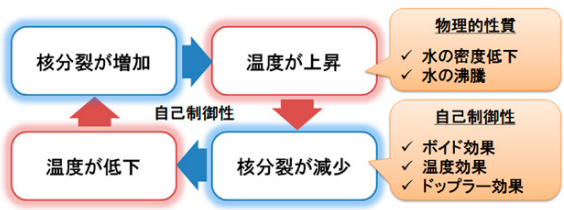


図 5　原子炉の核反応自己制御性

第3回 自動車機能安全カンファレンス

- Third Automotive Functional Safety Conference -

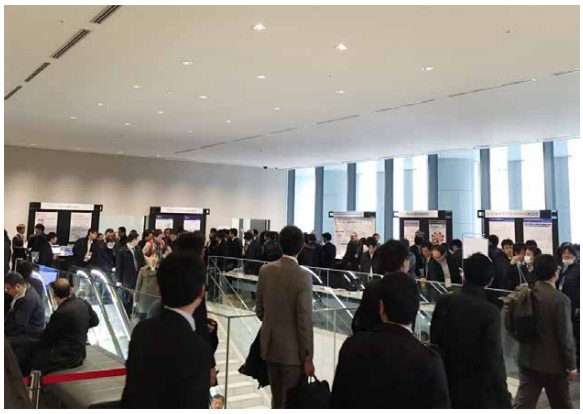
『自動運転に向けた機能安全』と『実例を含めた機能安全の実際』 2015/12/15 ～ 16

参加報告

マーケティング部
竹原　正人

当社がスポンサーとして協賛した第3回自動車機能安全カンファレンス（主催：株式会社インプレス、共催：一般財団法人日本自動車研究所（ＪＡＲＩ））が、去る2015年12月15日(火)、16日(水)にソラシティカンファレンスセンター（東京・御茶ノ水）にて開催されました。

当社はスポンサーの１社としてカンファレンスにて講演を行いましたので、参加報告をさせていただきます。



受付ロビーの様子

自動車機能安全カンファレンスは、自動車の機能安全関連のベストプラクティスや共通課題とその取組みに関する情報共有や、新たな潮流として話題の自動運転制御システムの発展に関して意見交換を行う場として開催されており、関連企業や団体及び学術会から自動車の機能安全及び自動運転技術開発について様々な視点から講演と発表が行われています。

初日に参加した講演の一部をご紹介します。

基調講演では、富士通テン株式会社の重松崇氏より「人間中心の自動運転を実現する安全設計と開発課題」をテーマとして、自動運転システムの一部の機能がヒトとシステムの相互連携により安全性を確保することが前提となっている中で、今後の技術開発の方向性について講演されました。また自動運転の将来については、

①国民の意識の問題
②法整備と法的責任
③コストと技術の問題
④信頼性の問題
⑤自動車産業の変革

というクリアすべき５つの問題があることを説明されました。漠然と認識はしていましたが、問題を詳細に聞いて、自動運転の実用化のためには、技術面以外にも超えるべきハードルがかなり高いことがわかりました。特別講演では、ＳＧＳジャパン株式会社の青木友保氏より「自動運転時代を見据えて現実的な機能安全規格対応」をテーマとして、機能安全規格が発行後５年を迎え、黎明期の厳格に規格に則した対応から、現実的な対応へとシフトした本格的な普及期に入り、さらに自動運転を見据えた次の機能安全規格対応の方針や事例が紹介されました。講演の中で、特に機能安全規格において、

①マネジメント
②プロセス

開演前の会場風景

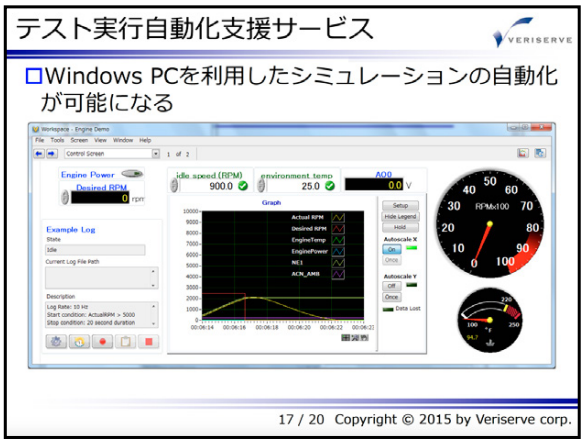
③要求記載

において、各々どこまで何を行うかを明確にし、目的と手段を取り違えないことが重要と指摘された点は、日々の業務にもつながる内容として印象強く残りました。

当社からは、オートモーティブ検証サービス開発部長の鈴木利彦が「ＥＣＵ開発におけるソフトウェア検証企業の役割」と題して、当社の概要紹介の後、機能安全に対応した当社サービスとその活用方法を説明しました。

当社　鈴木利彦の講演風景

講演内容としては、初めにＩＳＯ 26262 と当社の各サービスの関係、標準テストプロセス（ＶＳＭ）、システムテストカテゴリについて概要を紹介しました。次に具体的な活用方法として、当社サービスであるプロセス改善、ＰＭＯ



ＥＣＵ開発におけるソフトウェア検証企業の役割」講演資料

サービスおよびテスト実行自動化支援サービスを紹介し、お客様と当社の役割を明確にしつつ、各サービスを用いた活用方法を説明しました。最後に当社が開発おいて検証に参加したＳＣＳＫの車載ベーシックソフトウェアであるＱＩＮｅＳ－ＢＳＷを利用したＥＣＵ開発の効率化について提案しました。

最後に、カンファレンスでは３０以上のセッションが行われましたが、自動車関連は、今まさに旬な分野であり、２つの大会場はどのセッションも盛況でした。

講演内容に関する問い合わせ先：

以下のURLよりお問い合わせ下さい。

https://www.veriserve.co.jp/contact/

2016年3月8日（火）ー3月9日（水）

JaSST'16 Tokyo

JaSST' 16 Tokyo : Japan Symposium on Software Testing in Tokyko 2016

参加レポート

当社がプレミアムスポンサーとして協賛したソフトウェアテストシンポジウム（JaSST、運営：ソフトウェアテスト技術振興協会（ASTER））が開催されましたので、ご報告させていただきます。
JaSST は、ソフトウェア業界全体のテスト技術力の向上と普及を目指して ソフトウェアテスト分野の最新の研究発表や実践事例、テスト技法やツールの活用事例など、ソフトウェアテストやソフトウェア品質マネジメントに関する幅広い情報が得られる場として、2015 年 10 月からの1年間で全国8都市で開催されます。

日本大学理工学部　駿河台校舎1号館

JaSST 2016 年度最初にして最大集客数を誇る JaSST' Tokyo 2016（主催：JaSST'16 Tokyo 実行委員会）が、2016 年 3 月 8 日（火）～3 月 9 日（水）に、日本大学理工学部校舎にて開催されました。多くのセッションが実施された中で、当社では4人の社員が登壇し、ソフトウェアテストに関して様々な立場から発表を行いました。
主催された主なセッションと、当社社員の発表内容をご紹介します。

1日目の基調講演では、Grand Software Testing の John Hager 氏により、「Software Test Challenges in IoT devices IoT デバイスにおけるソフトウェアテストの課題」のテーマで講演がありました。モデルベーステストや IEEE、ISO 29119 (testing) など数多くの国際標準を世に送り出した John 氏による発表は大変説得力のあるもので、IoT 分野におけるテストの様々な課題点と、先進的なテスト技術 (SODA) やクラウドリソースを用いたテストアプローチなど、次世代におけるテスト戦略を提案しました。

8日、9日両日の昼下がりに行われた「ネットワークランチサービス & 展示ブースツアー」では、ランチを食べながらの参加者同士のコミュニケーションやスポンサー企業のサービス紹介が行われた後、複数のチームに分かれ、展示ブース見学が行われました。ランチは終始和やかな雰囲気で、見学では当社ブースに多くの参加者が訪れ、サービスについての質疑応答が交わされました。

当社の展示ブース

1日目のテクノロジーセッションでは、当社の蛭田恭章が「テストと仕様書 ～「仕様書は一側面である」という前提に立ったテスト活動～」のテーマで登壇しました。仕様書の過不足をテストの立場で是正する仕様レビュー活動と、仕様書をベースとしないテスト設計の2つについて、その考え方や課題などを解説しました。ソフトウェアの品質確保を「バグの作り込み防止」と「利用時の期待に答える」の2つの視点で考え、開発の工程では仕様書レビュー、テスト工程では「仕様書をベースとしないテスト」が必要とし、バグ情報や利用者情報をテストベースとしたテスト方法などを提示しました。

会場：日本大学理工学部　駿河台校舎１号館　ベリサーブはＪａＳＳＴに協賛しています。

ソフトウェアテストシンポジウム2016 東京

マーケティング部
豊本　奈美江

当社　蛭田恭章による講演

２日目はあいにくの雨模様でしたが、前日と同様多くの参加者が来場されました。この日はパネルディスカッションが多く開催されましたが、その中で当社社員が２名パネリストとして登壇しました。

「テスト自動化～自動丸になるためのルーティンとは？～」をテーマとしたディスカッションに、当社の後藤香織が、３人のパネリストの１人として参加しました。異なる業界のパネリストがテスト自動化エンジニアの人物像やそのキャリアパスについて、自らの経験から意見を交わしました。その中で、後藤の「前を進んでいる人が、良い背中を見せる」ということについて、他のパネリストからも共感を得ていました。

同時刻に開催された「テストのマネジメント」をテーマとしたパネルディスカッションに、当社の東弘之が３人のパネリストの１人として参加しました。テストチームやテストプロジェクトをうまくマネジメントするという難しい役割に、経験からくる生きたコメントや議論が展開されました。３人のコメントに共通していたのは、お客様が何を考えているかを知ること、テストの目的、ゴールを明確にすることで、プロジェクトをまとめることができるというものでした。その中で、東のお客様と「にぎる」というコメントについては、他のお二人もうなづきながらも「にぎる」とはどういうことかで、三者三様の解釈があり議論が盛り上がりました。

当社　後藤香織、東弘之（パネルディスカッション）

２日目のテクノロジーセッションでは、ベリサーブの須原秀敏が「AUTOSAR Acceptance Test の自動化の取り組み」のテーマで、車載組込ソフトウェア開発で話題となっている Autosar（AUTomotiveOpen System Architecture）がどういったものなのかの定義から、Autosar Acceptance Test のメリットを説明しました。テスト実施の苦労とコストを削減するためには Autosar Acceptance Test が有効であることを示し、実例を幾つか紹介しました。専門的な内容でしたが、講演後の質疑応答により、参加者の関心の高さが伺えました。

講演内容に関する問い合わせ先：
以下のURLよりお問い合わせ下さい。
https://www.veriserve.co.jp/contact/

当社　須原秀敏による講演

品質の真実

技術統括　佐々木 方規

国際規格 "SQuaRE" をアーキテクチャ設計に適用するための概念モデルについて

システムやソフトウェアの開発には、多くのステークホルダーが存在します。それらのステークホルダーがばらばらのメジャーで品質を評価すると、混乱することは容易に想像できます。そこで国際規格である SQuaRE が登場します。SQuaRE は、複数の国際規格で構成され、ISO/IEC25000 シリーズとして整備されています。しかし、国際規格として整備されても、正しく適用（評価）を行なわなければ結果を得られません。ソフトウェアを含むシステムのテスト（以後、ソフトウェアテストとします。）へ適用するポイントを説明します。

まずはソフトウェアテストの構造を考えてみましょう。ソフトウェアテストは、システム開発に対して従属的な支援プロセスとして考えることができます。どんなテストが求められているのかなど、テストへの要求（以後、テスト要求とします。）はシステム開発から発生します。これらのテスト要求は、具体的なものだけでなくイメージや暗黙的なものも含みます。これらを可視化するために、いきなり詳細にテスト要求を分析するのでなく、テスト要求の概念モデルを設計します。この概念モデルは、SQuaRE の各々の品質モデルをメタとして、適用が必要な品質のメタを構成するモデルを概念モデル（品質のメタモデル）と呼ぶことにします。ソフトウェアテストに長けた技術者であれば、直感的に概念モデルを考えてしまいます。このような技術者でなくても SQuaRE の製品品質モデルや利用時の品質モデルを利用すれば、概念モデルを設計するときに非常に有効です。ではなぜモデル化が必要であるのかも説明しておきます。SQuaRE には、システム／ソフトウェアの品質特性が詳細に定義されています。これらに従えば、テスト対象の品質構造を示すことができます。しかし、モデルを利用しないで具体的に詳細化してしまうと、品質構造を定義した背景などを示すコンテクストの追跡性が低くなってしまいます。経済産業省の報告書から引用した図 . 品質モデルのサイクルでは、各々の品質モデルの関係が理解できます。例えば、「利用時の品質要求」は、「利用者ニーズ」を入力とし「システムの品質要求」への出力とされ、また「利用時の品質」をメトリクスの評価を通じて測定されます。このように概念モデルでは、リレーションを意識した構造を持つことが望ましいと考えます。

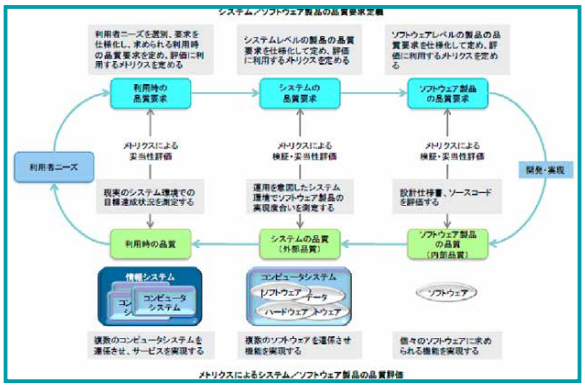


図 . 品質モデルのサイクル
（引用元）
経済産業省（以降は METI とする） ソフトウェアメトリクス高度化プロジェクト　プロダクト品質メトリクス WG
システム／ソフトウェア製品の品質要求定義と品質評価のためのメトリクスに関する調査報告　　発行：2011 年 3 月
http://www.meti.go.jp/policy/it_policy/softseibi/metrics/20110324product_metrics2010.pdf

SQuaRE をテスト観点としてテスト設計の導出に利用した事例を見てきましたが、その多くは概念モデルの構造を持たないため、テスト設計が固定化されていました。仕様ベースのテスト設計ではありがちですが、テスト対象の期待値が固定化されてしまい、「OK/NG」を評価するテスト仕様になります。品質モデルでは、ベンチマークによる測定値を評価することもあるので、期待値を品質モデルのサイクルの上位の要求と関連付けして評価するようにテスト設計できることが理想的です。これらの概念モデルを利用するメリットは、派生モデルの評価など同一概念モデルのテスト設計に流用できることです。これらを応用することで、高級モデルや量産モデルの差異を閾値の違いとして吸収させることで、同一の概念モデルを適用することで評価の品質を変化させずにテスト設計に展開することも可能になります。これらによりテストのリポジトリとして資産登録し、再利用性をあげることが期待できます。

今回は、SQuaRE をアーキテクチャ設計に適用するための概念モデルの説明をしましたが、次回はメタモデルを図解して説明します。

品質のスペシャリスト集団

３０年以上にわたり、
ソフトウェア検証で品質向上に貢献しています。

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

VERISERVE

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

VERISERVE NAVIGATION『ベリサーブナビゲーション』 2016年3月号

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

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