

VERISERVE NAVIGATION

ベリサーブナビゲーション

Periodical Magazine Presented by Veriserve.
Published in October 2016



Vol. 7



ベリサーブ技術通信

Autumn
2016

クリティカルシステムにおける安全・安心のための
ソフトウェア開発モデル

宇宙標準のソフトウェア
安全とIV&V

ドローンに関わる
法律問題と展望

他

ベリサーブナビゲーション

Autumn 2016

Contents

- 3 **Feature1**
国立研究開発法人 宇宙航空研究開発機構 (JAXA)
研究開発部門 研究領域上席
片平 真史 氏
クリティカルシステムにおける安全・安心のためのソフトウェア開発モデル
～ 宇宙標準のソフトウェア安全とIV&V ～
- 8 **Feature2**
弁護士：波多江 崇 氏、田中 健太郎 氏、木宮 瑞雄 氏
ドローンに関わる法律問題と展望
- 16 **Series**
「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
最終回：原子力事故は何故防げなかったのか
- 20 **Seminar**
ベリサーブ アカデミック イニシアティブ
『ソフトウェアと品質を考える』開催報告
- 22 **Event**
JaSST' 16 Kansai
IoT Japan 名古屋 2016
ETWest 2016



特集①

国立研究開発法人 宇宙航空研究開発機構 (JAXA)
研究開発部門 研究領域上席

片平 真史 氏

クリティカルシステムにおける安全・安心のための
ソフトウェア開発モデル

～宇宙標準のソフトウェア安全とIV&V～

Feature 1

特集1 | 国立研究開発法人 宇宙航空研究開発機構 (JAXA)

クリティカルシステムにおける安全・安心のためのソフトウェア開発モデル — 宇宙標準のソフトウェア安全とIV&V —

自動車・家電などの一般市販製品においても安全が盛んに議論されるようになり、その製品開発において安全規格に準拠した開発モデルの適用が進んでいます。しかし、自動車の自動運転などのコンピュータによる自動化が急速に進む現状では、製品の信頼性や故障のみに囚われることなく、利用ユーザの多様性・環境の変化を意識し、安全を確保する活動が必要となります。ここでは、安全なシステムを作り上げるための宇宙標準で採用されている活動を紹介し、要求定義・設計に立ち戻って、真の安全・安心とは何かを考える糸口となれと思います。

宇宙標準の第三者組織による ソフトウェア安全の向上

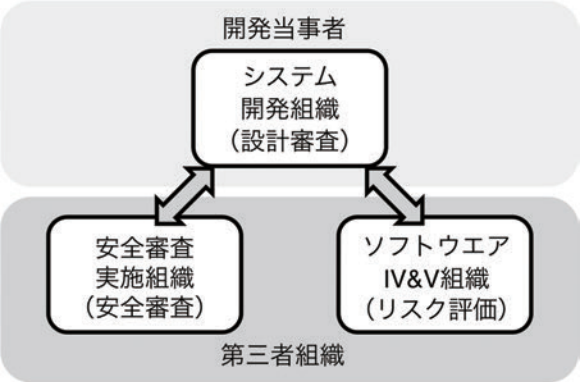
はじめは、1980年代に本格化した、アメリカ宇宙航空局(NASA)²との国際共同プロジェクト宇宙ステーション計画³における開発モデルなどの国際標準の調整の場でした。そのころの国立研究開発法人 宇宙航空研究開発機構(JAXA)⁴(旧 NASDA)⁵では、日本の宇宙輸送機(ロケット)や人工衛星などの宇宙開発がようやく本格化したところです。ソフトウェア開発についても、JIS規格に先立ち品質、信頼性に関する開発ルールが準備・適用され、人工衛星やロケットなどの製品開発が、それらのルールに従って進められていました。しかし、NASAとの宇宙ステーション計画に関する国際開発ルールの調整の場で新たに直面したことは、日本にはそれまで経験のない、宇宙飛行士が搭乗するような有人システムに対する**システム安全**の考え方、及びその安全達成のための**ソフトウェア独立検証及び妥当性確認(IV&V)**の必要性です。

最も特徴的なことは、安全を確保するため活動が**第三者組織**によっても実施され、客観的に専門家によって確認されることです。システム設計の安全確保のために第三者組織が安全設計要求を設定し、ハザード7解析の結果に基づき、その適合状況を確認しています。この確認は、開発工程に沿って、第三者の安全の専門家によって構成される安全審査会において確認を行っ

ています。また、システムの一部をなすソフトウェアは、同様に安全審査会において確認を行いつつ、かつ第三者組織によるソフトウェアIV&Vによりそのリスク評価を行っています(図①)。

安全設計要求をシステム設計へ確実に開発当事者が反映することになります。安全管理の手段として、安全審査会において、設計情報及び安全解析(ハザード解析)結果に基づき、客観的な観点で設計結果の安全性を確認し、安全を達成しています。

安全に関わるソフトウェアの確実な開発・運用を実現するためには、通常の品質保証活動に加え、開発組織とは異なる第三者組織がそのソフトウェア製品を客観的に評価することが必要となります。特に宇宙システム搭載ソフトウェアの場合、他の信頼性が求められる社会インフラにも増して、その使用環境が複雑であ



図①：安全確保のための第三者組織の活動

研究開発部門 研究領域上席 片平 真史 氏

片平 真史 氏 かたひら まさふみ

1988年 宇宙開発事業団 (NASDA) 入社
(現 国立研究開発法人 宇宙航空研究開発機構 (JAXA))
人工衛星運用・追跡管制、宇宙ステーション計画のソフトウェア安全・
ミッション保証要求調整、ソフトウェア安全設計・審査、などに従事

1995年 フロリダ工科大学 Computer Information Systems 修了

2000年 マサチューセッツ工科大学 (MIT) 航空宇宙工学部
Complex Systems Research Lab (Leveson 教授) 客員研究員
ロケット搭載装置開発、ソフトウェア IV&V 等の
ソフトウェアエンジニアリング研究業務に従事

2015年から 研究開発部門 研究領域上席、
奈良先端科学技術大学院大学 客員教授

り、想定しきれない事象も多く発生するために、この客観的な評価は、重要な役割を担っています。

このような第三者組織による安全向上の活動は、開発ルールに従うだけでは十分な効果は期待できず、**経営トップ**のその必要性の**理解**と活動を推進するための**コミットメント**が必ず必要となります。

設計解は安全の視点で決まる

宇宙分野では安全を確保するアプローチは**システム安全**を基礎としています。現在、他の分野で導入が進む機能安全を基礎とする考え方とは少し異なっています。**機能安全**では、製品の特徴、ハザードを考えるシステム分析を行わず、故障の少ない信頼度の高い装置を組み上げて安全を実現するということになります。製品を安全になるように設計した上で、改めて、システム全体でどのようなハザードがあり、そのハザード

1. : ハザードが事故等に至らないように、除去、最小化又は制御されている状態、即ち、リスクが許容できるレベルまで低い状態

2: NASA : National Aeronautics and Space Administration

3: ISS : International Space Station Program

4: JAXA : Japan Aerospace Exploration Agency

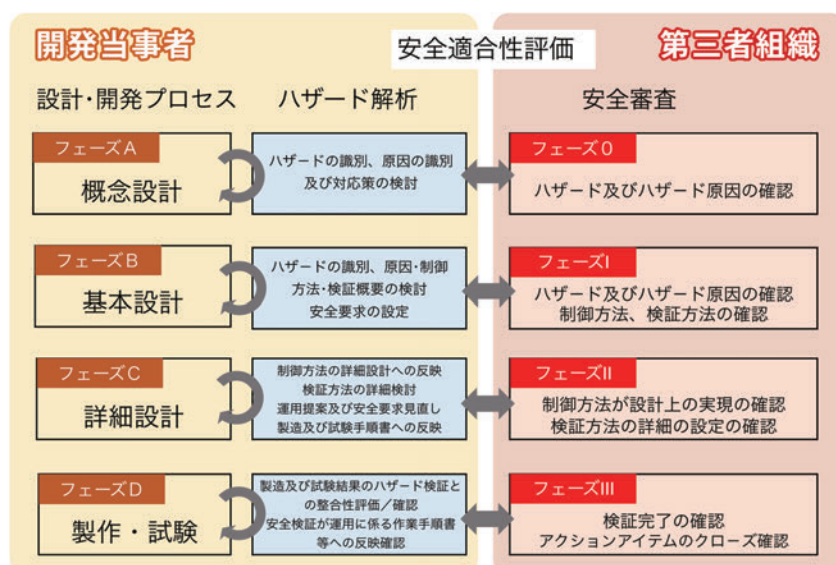
5: NASDA : National Space Development Agency of Japan(宇宙開発事業団)

6: IV&V : Independent Verification and Validation

7: 事故をもたらす要因が顕在又は潜在する状態

IV&Vの実施は製品の信頼性を向上させ、さらにステークホルダーに『安心』を与えることになります。

を制御しリスクを許容できるレベルまで抑制できたか解析し、不足があれば設計を見直すといった、システム安全の考えを取り入れています。「安全」を設計段階から組み入れる作業は図②に示すプロセスに沿って行われます。



図②：開発プロセスと安全適合性評価プロセスの関係

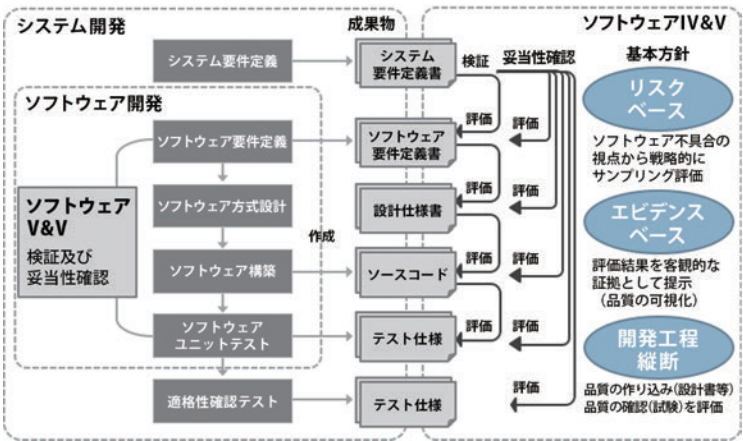
特集1 | 国立研究開発法人 宇宙航空研究開発機構 (JAXA)

開発当事者は、常に自身によるハザード解析や第三者組織による安全審査会を通じて、安全適合性を意識し、安全なシステムの設計を深めていきます。これを段階的に実施しながら、「安全」を熟考しシステムの中に組み込んでいくことになります。機能性・利便性のみを優先し、利用時に安全上の問題を起こすようなシステム設計は、リスクとして許容されず、再設計を行うことになり、かえってコスト面でも不利になります。これらの活動を通じて、まさしく、「設計解は安全の視点から決まる」、という**安全文化**が身につくことになります。このプロセスでは、基本設計段階において、対象システムに対する安全要求を抽出・設定し、安全設計として設計に反映していきます。過去の安全審査などの経験智から、設計へ反映すべき共有事項については、安全要求として蓄積され、これが資産となつて、さらに活用されていきます。

システムで利用されるソフトウェアに関しても、この安全審査プロセスにおいて、安全要求への適合性が評価されています。システム全体と同様に過去の経験智から導出された共通のソフトウェアの安全要求が適用され、ソフトウェアの必要時の不動作、意図しない不意の動作という点から、ハザードの原因となる事象が識別されています。また、ソフトウェアの場合、その特徴からそのロジックの設計・実装内容（完全性、一貫性など）が他のハードウェアよりも可視性が低いため、安全要求に適合しているかなどを、ソフトウェアの開発プロセスに沿って、第三者組織によるIV&Vとしても確認する必要があります。

第三者組織IV&Vによるソフトウェアの安全・安心の確保

宇宙分野におけるソフトウェアIV&Vの概念は、米国のアポロ計画の時代から適用が始まったと言われています。特に、NASAのスペースシャトル『チャレンジャー』の事故後、米国NRC(National Research Council)が行ったスペースシャトルフライトソフトウェア開発プロセスに対する勧告において、ソフトウェアIV&Vの強化が提言され、NASAでは1993年にNASA



図③：ソフトウェアの開発プロセスとIV&V プロセス

全体で行うIV&Vプログラムが設置されました。同時期から、JAXAにおいてもソフトウェアIV&Vを導入しています。ソフトウェアIV&Vとは、開発当事者から独立した組織が、開発当事者と異なる検証技術を用い、開発資金からの影響を受けない資金によって、ソフトウェアの課題や問題を洗い出し、潜在するリスクを軽減するためのライフサイクルを通して行うシステムエンジニアリングプロセスです（図③）。

ただし、開発当事者が行うV&V活動とは異なり、網羅的な確認ではなく、安全等に関わる重要なシナリオに関する視点で行うサンプルチェックです。従って、基本的にV&V活動の負担軽減に直結するものではありませんが、発見された課題や問題を氷山の一角と考え、類似箇所の確認などを行うことで、将来の不具合削減など開発の効率化に寄与できると思われます。

IV&Vという言葉は、日本メーカー製自動車の米国における意図しない急加速に関する審議の中で、米国議会などからの要請を受け、NASAがIV&Vを実施し“ソフトウェアに安全上の問題がない”という調査報告が出たことで、その有効性を含め脚光を浴びたことで知られています。日本国内においても、2014年6月に独立行政法人 情報処理推進機構（IPA）から「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（通称：ソフトウェア品質説明のための制度ガイドライン）」が発行され、宇宙分野以外の産業でも第三者による検証の重要性が認識され始めています。

研究開発部門 研究領域上席 片平 真史 氏

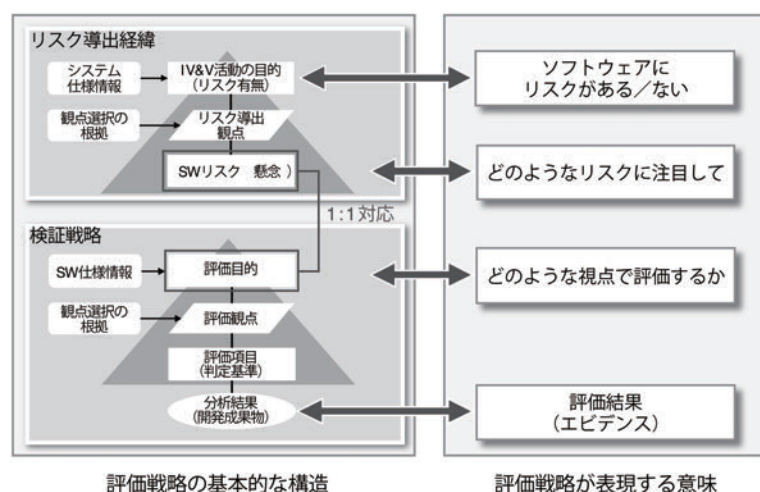
安全性の視点に戻って考えてみると、ソフトウェア開発において、仕様通り動作することの保証は、従来の品質工学、信頼性工学に基づく手法により強化が可能であるが、要求仕様等の上流工程における仕様定義時の正確性の欠如、不完全性の残留、想定不足、などがシステムの安全性に脅威をもたらすことが多いものです。

このため、IV&Vでは、開発の初期段階において、活動の重点を置くことが理想的とされています。要求初期段階に混入した仕様等の問題は、従来のソフトウェア試験などで発見できず、打上げ後（出荷・利用開始後）の致命的な不具合となり、安全上重大な問題を引き起こします。このような開発当事者が気づきにくい、要求そのものの矛盾や欠落などの問題点を、IV&Vなどにより客観的な視点で抽出できます。開発者の思い込みで発生するような、機能・性能が満足されない状態がないかを未然に確認することができます。

このソフトウェアのリスク低減のため、IV&Vでは、安全の視点で、以下の命題を解決することを主眼としています。

- ・ソフトウェアは、意図どおりに正しく振る舞うか？
Will the system software do what it is supposed to do?
- ・ソフトウェアは、意図しない振る舞いをしないか？
Will the system software do what it is not supposed to do?
- ・ソフトウェアは、不都合な事態に期待どおり振る舞うか？
Will the system software respond as expected under adverse conditions?

これらを達成するためのIV&V作業は多岐にわたります。作業の詳細はJAXAが発行しているガイドブックを参照いただくとして、ここでは、作業の具体化（検証戦略の導き方）及び命題の立証方法を説明します。図④に示す通り、対象システム（製品）がどのようなリスクを持つのか、そしてリスクをどのように低減したいのか、さらにリスク低減のためにどのような視点で評価するのか、最後に評価結果に基づきリスク低減を立証するという流れになります。



図④：IV&V 評価戦略の構成

このIV&Vは、網羅的なものではありませんが、客観的に第三者が確認することで、安全上致命的な思い込みや過誤などを排除するきっかけとなり、製品の信頼性を向上させることができます。さらに、セカンドオピニオンとしてステークホルダーに『安心』を与えることになります。

今後の取り組み

重要なことは、安全規格を満たすことやIV&Vを行うことではなく、自身の開発する製品のハザード（リスク）を見つめ、戦略的にコントロールすること、そのための能力のある人材育成や仕組みを構築すること、また、そのための優秀な資質を持ったエンジニアの発掘にあると考えます。

JAXAでは、IV&V技術を、安心・安全な日本のものづくりにおいて、強みとして活用できるように、そのノウハウを「IV&Vガイドブック【導入編】【実践編】」としてまとめ提供しています。ここでまとめられたIV&V技術は、開発当事者におけるV&V作業にも応用できますが、新規企業及びエンジニアの**独立検証産業への新たな参画**に活用されるものと期待しています。



IV&Vガイドブック【導入編】(88頁)
IV&Vガイドブック【実践編】(727頁)

8. 問い合わせ先 IVV_INFO@jaxa.jp



弁護士

波多江 崇 氏、田中 健太郎 氏、

1. はじめに

— ドローンの現状 —

ドローンが急速に普及している。ドローンは、私たちの生活や、仕事をどのように変えるだろうか。

ドローンとは、一般に、ある程度小型の無人航空機をいい、UAS (Unmanned Aircraft System) や UAV (Unmanned Aerial Vehicle) などとも呼ばれる。

最も早くドローンの商業利用に着目したアマゾン、ドローンを用いて、30分以内の配達を目指しているだけでなく、「ドローンハイウェイ」を提案するなど、ドローンを社会的なインフラとして活用する構想を早くから打ち出している。楽天も追随しているようだ。建設業界での普及も進んでおり、カメラを用いた橋梁やパイプライン等のインフラ・巨大施設の検査のみならず、建設現場の進捗管理（測量、土量測定、出来高確認等）に既にドローンが活用されている。最近では、建築物に直接接触（ノック）して、搭載した打音検査機により橋梁やトンネルの耐久性を診断できるドローンも登場した。農業分野でもドローンは活躍し始めている。米国等では、ドローンによる農薬散布のみならず、赤外線等を利用したセンサーによるマッピングや種まき、作物のモニタリング等による生産管理・効率化が始まっている。広大な農地や牧場は、ドローンが活躍できる分野であるのは間違いない。もちろん、映画や映像制作、地図作成等の測量の分野も有望だし、不審者を捕捉・追跡・撮影等するドローンによる警備サービスも登場している。警察による捜査、被災地や過疎地での物資の輸送、広告、さらには光と音楽を用いたドローンエンターテインメントショーへの活用も日々実

用化が進んでいる。また、海外では、さまざまな新しいサービスを提供する多数のドローン関連のスタートアップ企業が多額の資金調達を行っている。このように、ドローンは商用化のフェーズに入ったといえる。ハードウェアとしてのドローンの開発とともに、「どのようにドローンを活用するか」という勝負が始まっているというわけだ。

これは、ドローン又はドローンに搭載したデバイス等をコントロールするソフトウェアの重要性が今後いっそう高まってくることも意味していると思われる。正確な経路生成や、用途に応じたセンサーやカメラの機能の最大化はもちろん、強風の吹く橋梁近辺で上昇気流に弱いドローンをコントロールするのも、バランスを崩すことなく建築物に直接ノッキングするのも、高度なソフトウェアがあつてこそだからである。

本稿では、以上のようなソフトウェアの果たす役割の重要性に留意しつつ、ドローンを規制する法令を紹介した後、ドローンの提示する新しい安全、プライバシー等に関わる問題を、法的な観点から見ていきたい。

2. 規制法

ドローンに関する規制法令として、主に、①航空法、②無人機規制法、③電波法及び④条例に留意する必要がある。

(1) 航空法

改正前航空法においては、ドローンは、基本的に「航空機」に該当しないものとされていたことから、表①の限度で規制されるに過ぎなかった。

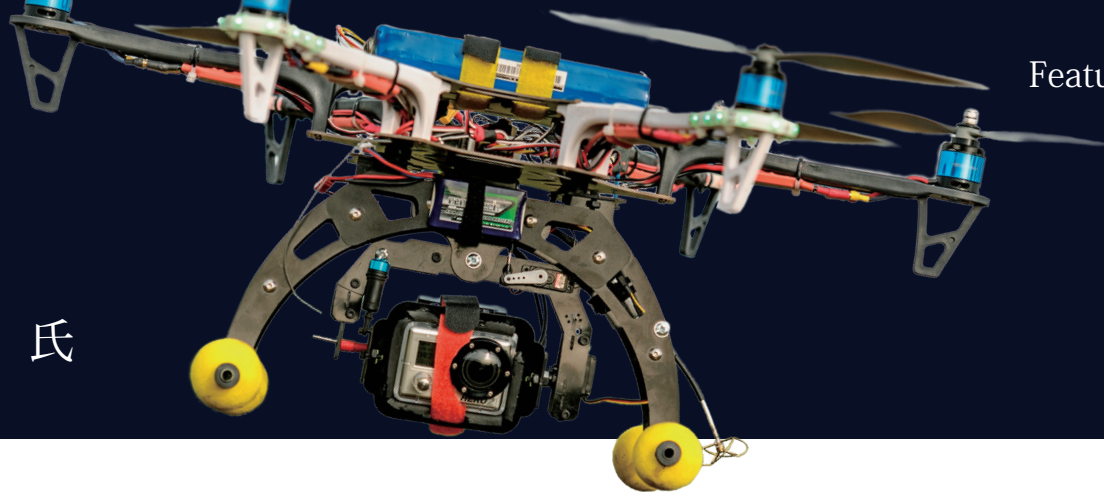
しかしながら、ドローンによる新たなサービス提供等が開始される中で、首相官邸への落下事件をはじめとする事故等も発生し、安全面の懸念が高まったため、小型無人機の運行方法等に関する規制を導入すべきと

左から、田中 健太郎氏、波多江 崇氏、木宮 瑞雄氏



展望

木宮 瑞雄 氏



の判断に基づき、緊急的な措置として、平成27年改正航空法では以下の規制内容が追加された。一言で言うと、安全確保の観点から、一定の空域での200g以

上のドローンの飛行を許可制とし、飛行方法にも具体的なルールを設けたものだ。(図①、表②)

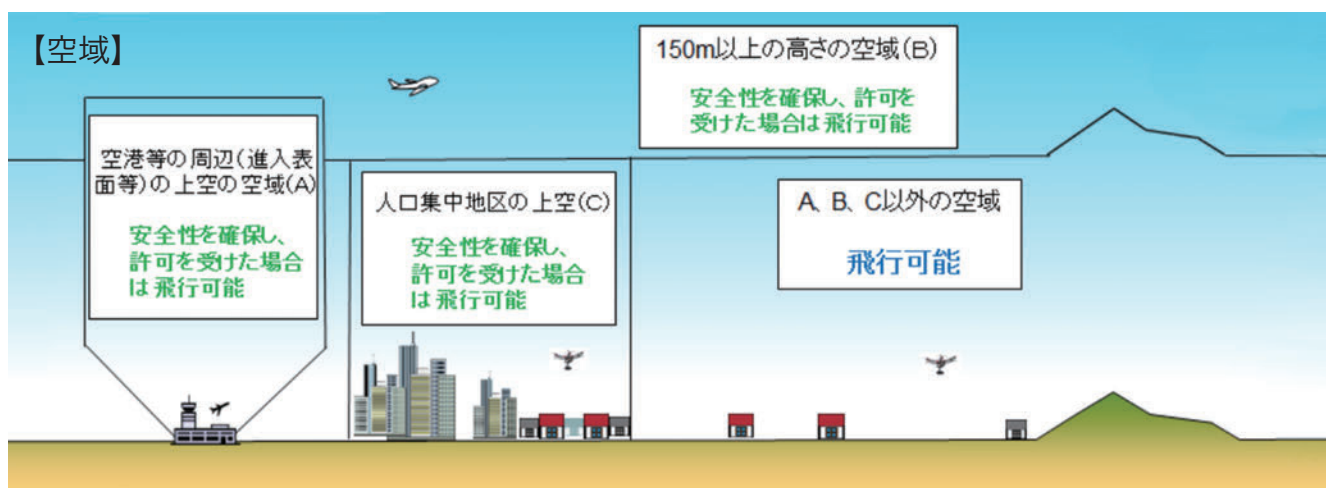
空域	規制概要
上空 250 m未満	航空路でない限り、自由に飛行可能。空港等の周辺等の飛行については、国土交通大臣の許可等が必要な場合あり。
上空 250 m以上	航空法 99 条の 2 第 2 項による事前の通報をすることで、自由に飛行可能。なお、重量 150kgを越えるものについては、航空機製造事業法上の「航空機」に該当し、製造の許可が必要。

表①：改正前航空法における規制概要

項目	規制概要
無人航空機の定義の新設（※） （航空法2条22項）	①航空の用に供することができる飛行機、回転翼航空機、滑空機、飛行船であり、かつ ②構造上人が乗ることができないもののうち、遠隔操作又は自動操縦により飛行させることができるもの （重量が 200 g 未満のものを除く。）
許可を必要とする空域（※） （航空法132条等） （図参照）	①航空機の航行の安全に影響を及ぼすおそれがある空域 (i) 進入表面、転移表面若しくは水面表面又は延長進入表面等の上空の空域 (ii) (i) 以外の空域であって、地表又は水面から 150 m 以上の高さの空域 ②人又は家屋の密集している地域の上空（①を除く。） (i) 人口密度の高い基本単位区（原則として人口密度が 1 平方キロメートル当たり 4,000 人以上）が隣接し、かつ、 (ii) その隣接した基本単位区内の人口が 5,000 人以上となる地域
承認を必要としない飛行方法 （航空法 132 条の 2 等）	①日出から日没までの間における飛行 ②当該無人航空機及びその周囲の状況を目視により常時監視して飛行 ③当該無人航空機と地上又は水上の人又は物件との間に 30 mを保つ飛行 ④祭礼、縁日、展示会その他の多数の者の集合する催しが行われている場所の上空以外の空域における飛行 ⑤当該無人航空機により爆発性又は易燃性を有する物件その他人に危害を与え、又は他の物件を損傷するおそれがある物件で火薬類等を輸送するものでないこと ⑥当該無人航空機から物件を投下しないこと。
罰則(157 条、159 条)	50 万円以下の罰金。両罰規定あり。

表②：平成27年改正航空法の規制概要

※事故や災害時の公共機関等による捜索・救助等の場合は例外あり。



図①：国土交通省「航空法の一部を開設する法律の概要」より引用

(空域の形状はイメージ)

弁護士： 波多江 崇 氏、田中 健太郎 氏、木宮 瑞雄 氏

許可は、1日だけでなく、1年等の一定期間での取得も可能である。例えば、損保ジャパン日本興亜は、大規模自然災害等の保険金の迅速な支払いにつなげるために、平成28年7月25日付けで、保険業界で初めて国土交通省から日本全国でのドローンの飛行に関する包括許可（飛行許可期間1年（毎年更新））を取得したと発表している。

ドローンに係る事故等のうち国土交通省に報告のあったものについては、国土交通省のHPに一覧がまとめられており、参考になる¹。また、花火大会にて無許可でドローンを飛行させ逮捕された事例等も散見されるため²、航空法の規制内容をより世間一般に周知させる必要があるだろう。

国土交通省は、平成28年7月29日に、東京都内で開催したドローンの環境整備に関する官民協議会で、ドローンの更なる安全確保に向けた制度設計の方向性を示し、急速に進展する新技術に対応するため、柔軟性を確保しつつ、迅速・段階的にルールを整備するとともに、有人機と無人機、無人機同士の衝突回避ルールについて平成28年度内を目途に整備する旨発表している。また、ドローン操縦者の免許制については現時点では困難との見解が示されており³、当面の間は操縦資格については民間に任せつつ、改正航空法を通じた安全確保を目指すものとされている。

今後は、海外で採用されている重さによってドローンを3つ又はそれ以上のクラスに分ける規制の細分化や、自律飛行（自動飛行）を見据えた航空管制等に関する議論も起こる可能性がある。ドローンの進化と普及に伴う、今後の航空法の再改正に向けた動きに注意すべきである⁴。

（2）無人機規制法

安全規制上の観点から、議員立法の形式で国会議事堂等の国の重要な施設等の上空における、小型無人機等の飛行を禁止した、いわゆる無人機規制法⁵も制定されている。なお、当該法令に違反した場合には、航空法と異なり、罰金（50万円以下）だけでなく懲役刑（1年以下の懲役）も科されている点に留意が必要である。

（3）電波法

平成26年11月に、空撮業務の実施のために、空中撮影用の小型無人機に取り付けたカメラの画像を上空から地上に無線で伝送するための不法無線局を開設した空撮会社及び同社社長が、電波法第4条の違反容疑で逮捕された（小型無人機で使用された不法無線局では全国で初めての事案である。）⁶。その後、横浜地検小田原支部は当該事案を平成27年6月23日付けで不起訴処分にしたが、処分の理由は明らかにされていない⁷。

その後も、平成28年3月14日付けで兵庫県内においてドローンの飛行が航空法及び電波法に違反するとして書類送検される事件等が起きている⁸。

電波を送受信する電気的設備を操作する場合、原則として総務大臣の免許を受けなければならない、免許を受けることなく電気的設備を操作したときは、1年以下の懲役又は100万円以下の罰金に処せられる可能性がある。

もともと、(i)発射する電波が著しく微弱な電気的設備で電波法施行規則第6条第1項で定められたもの、(ii)特定の用途及び目的の電波を送受信する電気的設備であり、技術基準適合証明を受けるなどの条件を満たすものを操作する場合には、例外的に免許は不要であるとされており、正規輸入品や大手量販店から購入したドローンはこれに該当するケースがほとんどであることから、免許の要否が問題になることは少ない。

1. 平成28年度 無人航空機に係る事故等の一覧(国土交通省に報告のあったもの) (<http://www.mlit.go.jp/common/001132992.pdf>) 及び平成27年度 無人航空機に係る事故等の一覧(国土交通省に報告のあったもの) (<http://www.mlit.go.jp/common/001125882.pdf>)。

2. 平成28年7月25日付け東京読売新聞夕刊10頁等。

3. 平成28年7月18日付け日本経済新聞朝刊15頁

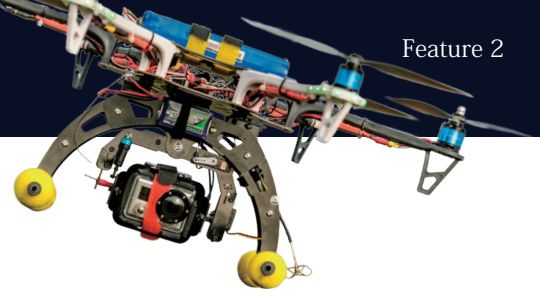
4. 米国政府の動きは昨年まで鈍かったが、米国連邦航空局は、平成28年6月、企業側からの要請を受けて、一定の場合に航空免許や飛行許可を不要とするなど規制を緩和する規則を決定した。さらに、今後は、超小型ドローンが人の頭上を飛行できる規則が発表されることが見込まれている。

5. 内閣総理大臣官邸その他の国の重要な施設等及び外国公館等の周辺地域の上空における小型無人機の飛行の禁止に関する法律

6. <http://www.soumu.go.jp/soutsu/kanto/press/27/0520k1.html>

7. 平成27年6月27日付け朝日新聞朝刊29頁。

8. 平成28年3月14日付け日本経済新聞大阪夕刊19頁。



しかしながら、並行輸入品や海外サイトから直接購入したドローンは、免許が必要なものがあるため、注意が必要である。

この点、現在行われているドローン専用の電波帯域ではドローンの商業利用に不十分であるとして、これまでも総務省において検討が進められてきたが、今夏を目途に無線設備規則等の省令を改正する予定とされている。また、携帯電話のようにドローンと基地局との間の直接通信を行いたいというニーズがある一方で、上空で利用される携帯電話の台数が増加した場合は、地上の携帯電話等の利用へ影響を与えるおそれがあるといった状況を踏まえ、携帯電話等を無人航空機に搭載して使用することについて、既設の無線局等の運用等に支障を与えない範囲で試験的な導入がなされることになった⁹。具体的には、実用化試験局の免許を受けることで、既設の無線局等の運用等に支障を与えないことを条件に、免許申請の際に提出する試験計画の範囲内で、携帯電話等を無人航空機に搭載した実用化試験を行うことができることとなった。この点については解決すべき課題が複数存在することから引き続き検証を行うことが必要であるため、今後の動向が注目される。

(4) 条例

ドローンの飛行が、都市公園の管理に支障がある行為にあたる旨を表明している自治体も多く、また、G7等の国際的な会合が開かれる場合に、一定期間に限り、小型無人機の飛行を禁止する旨を定めた条例が制定されるケースもあるため、法律だけでなく条例の調査も怠らないよう留意すべきである。

3. ドローン事故と 損害賠償等の法的責任

(1) 損害賠償責任の負担者

民法は、過失なければ責任なしという過失責任の原則をとっている。過失とは、一般に、結果発生の予見可能性がありながら、結果の発生を回避するために必要な行為をしなかったことを意味する。ドローンの墜落等により、けがや財産の損壊等をした場合、基本的

には、操縦者が民法上の不法行為に基づく損害賠償責任を負うことになる。裁判になれば、操縦者の過失が争点になるだろう。

例えば、強風によりラジコン飛行機の操作を誤り、見物人に衝突させ、側頭部骨折等の傷害を与えた事例で、操縦者の過失を認め、約200万円の損害賠償請求を認めた裁判例がある¹⁰。判決によれば、操縦者には、他人の全くいない場所を選択するか、又は人に衝突することがないように飛行進路をとるか、模型飛行機が人に向かうときには墜落させるような操縦方法を選択すべき注意義務があるにもかかわらず、これらの義務を怠った過失があると認定されている。今後、ドローンに関しても、同様の注意義務が認められる可能性があるだろう。

以上に対し、例えば、必要なメンテナンスを怠っていたなどの事情がない限り、ドローンの単なる所有者で操縦に関与していなかった者に対しては、損害賠償責任を問うのは難しい¹¹。

9. 総務省「無人航空機における携帯電話等の利用の試験的導入」<http://www.tele.soumu.go.jp/j/sys/others/uav/>。なお、同HPには、FAQ等も記載されており、参考になる点も多い。

10. 東京地判昭和50年1月28日判例タイムズ323号198頁。被告は、被害者である原告が存在することを認識していなかったことや、突風による不可抗力を主張し、過失を争っていたようである。

11. 自動車事故においては、人身事故の場合に限り、運行供用者の責任(自賠法3条)が認められ、被害者救済に寄与している。すなわち、運行供用者(自己のために自動車を運行の用に供する者。典型的には所有者)には、事実上無過失責任が負われる。ただし、賠償金は、強制保険である自賠責保険によりカバーされる。

波多江 崇氏

はたえ たかし

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

弁護士： 波多江 崇 氏、田中 健太郎 氏、木宮 瑞雄 氏

(2) ソフトウェアの瑕疵と製造物責任

操縦者の過失を問い難い事例もあり得る。例えば、GPS通信を行うソフトウェアの不具合により、巡航経路を誤った自動巡航型ドローンが、建設現場の障害物に激突して落下し、その下にいた作業員にけがをさせたという事例を考える。事実関係によっては、操縦者（使用者）の過失が認められない事例もあるだろう。操縦者には資力がなく、損害賠償請求をする実益がないケースも考えられる。このような場合には、ドローンのメーカーに対して、製造物責任法に基づく損害賠償をすることが考えられる。

製造物責任法は、平成6年に成立した法律で、製造業者等に故意や過失があったこと要件とせず、製造業者等が引渡した「製造物」に「欠陥」があることと、「欠陥」と損害との間の因果関係を立証すれば、製造業者等に損害賠償責任が生じることを定めている。被害者の立証の困難を軽減する趣旨である。製造物責任法にいう「製造物」には、ソフトウェアそのものは含まれないが、ソフトウェアを組み込んだ製品は「製造物」に含まれ、ソフトウェアの不具合は製造物の欠陥となり得る。また、ソフトウェアの仕様、性状等が原因でソフトウェアを組み込んだ製造物に起因する事故が発生した場合には、ソフトウェア部分の仕様や性状等が製造物全体の欠陥となり得る。上の事例で言えば、仮にドローンに搭載されたGPS通信を行うソフトウェアに欠陥が認められた場合には、ドローンのメーカーは、被害者に対して損害賠償責任を負う可能性がある。なお、ソフトウェアのベンダーが責任を免れるわけではなく、ソフトウェアの欠陥に基づき、ドローンのメー

カーからソフトウェアのベンダーに対して損害賠償請求（求償）がなされる可能性がある。

ソフトウェアが製造物責任法の適用される製造物に該当しないこととされた背景の1つには、立法当時、一般的にソフトウェアが人の生命・身体に対する危険性を有するものではないという前提があった。しかし、ソフトウェアは、今や様々な製品に組み込まれており、その不具合が人の生命・身体等に対して損害を及ぼす危険は高まっている。ドローンはその好例だといえるだろう。ドローンは、新しい被害者救済の枠組みの検討のきっかけとなる可能性がある。

(3) 正当防衛、妨害排除請求、保険等その他の問題

以上のほか、墜落してきたドローン、あるいは自宅敷地内に侵入してきた（侵入してきそうな）ドローンに対して、どのような対処ができるかという問題もある（本項では民事上の問題に限定して述べる。¹²）。

例えば、墜落してきたドローンを破壊して身を守る行為は、ドローンの墜落について(i)操縦者等の故意又は過失が認められる場合には正当防衛（民法720条1項）が、(ii)誰の故意又は過失も認められない場合には緊急避難（民法720条2項）が成立し、正当化され得る。

また、土地の所有権は、法令の制限がない限り、土地の上下に（無限定に）及ぶと定められているため（民法206条）、理論的には、所有地上空に侵入してきたドローンに対し、妨害排除請求権を行使できるとも思えるが、一定の高度以上の上空については土地の所有権の行使を認めない見解も有力であるし、そもそも裁判に要する時間を考えると実際に提訴して妨害排除請求を認める判決・決定をもらうことは現実的ではなく、どのような法的な（又はそれ以外の）対処法が可能か、あるいは航空法とは別の観点から私有地上空のドロー

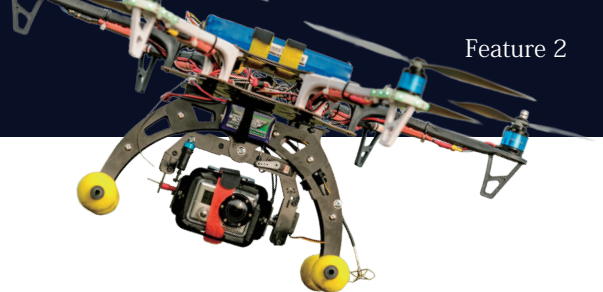


田中 健太郎 氏

たなか けんたろう

2007年 司法試験合格後、
法職多摩研究室専任講師。
2009年 中央大学法学部法律学科卒業。
2010年 弁護士登録。
2010年 TMI 総合法律事務所勤務。

12. 刑法上は、操縦者の過失により自身に墜落してきたドローンを、身を守るために破壊する行為には正当防衛が成立し得る。ドローンの墜落につき、刑法上誰の故意又は過失も認められないような場合には、正当防衛を認める見解と、緊急避難を認める見解がある。



ンの飛行を規制すべきではないか、今後議論が始まる可能性があるように思われる。

事故等への対策に関しては、既にドローンによる事故に対応する保険が販売されているし、販売時に保険が「付いてくる」ドローンも販売されているが、ドローンが今後いっそう普及すれば、保険のあり方も変わるだろう。自動車のように強制保険制度も検討されるかもしれない。

4. ドローンの利用と プライバシー・肖像権等

ドローンを利用して空からの映像撮影を行う場合、当該撮影がプライバシーや肖像権の侵害に該当する場合には、民事上、撮影者は不法行為に基づく損害賠償責任を負うこととなる。また、ドローンが撮影等した情報に個人情報が含まれている場合には、個人情報の保護に関する法律（個人情報保護法）による規制も問題となり得る。

(1) ドローンとプライバシー

一般に、他者にみだりに知られたくない情報をみだりに公表されない権利又は利益は「プライバシー権」として構成され、法的保護が与えられている。プライバシー侵害の有無は、公表されない法的利益と、公表する理由とを比較衡量することによって判断するものとされている。¹³

具体的にどのような場合にプライバシー侵害となるかはケースバイケースであるものの、ドローンによって空撮を行う場合を想定すると、一般的に、地上からの撮影と比べて高い上空からの映像が撮影されることになるため、それによって住居の塀の中や建物の内部などが撮影される場合には、他者に知られたくない情報や映像が含まれる可能性が高く、プライバシー侵害の危険性は高くなるといえるだろう。

また、従来判例は、他者にみだりに知られたくない

い情報を「公表」又は「開示」された場合にはじめてプライバシーが侵害されるとの考え方を採用しているとみられたが、Google ストリートビュー事件において福岡高等裁判所は「社会に生起するプライバシー侵害の態様は多様であって、出版物等の公表行為のみならず、私生活の平穩に対する侵入行為として、のぞき見、盗聴、写真撮影、私生活への干渉行為なども問題となり得る。写真ないし画像の撮影行為については、……その撮影行為により私生活上の平穩の利益が侵され、違法と評価されるものであれば、プライバシー侵害として不法行為を構成し、法的な救済の対象とされる」と判示し、公表行為のみならず撮影行為もプライバシー侵害の対象となると述べている。¹⁴ すなわち、ドローンによる空撮を行う場合であっても、撮影した写真や映像をインターネット等で公表するか否かにかかわらず、撮影行為自体がプライバシー侵害として違法となる可能性もあることに留意する必要がある。

(2) ドローンと肖像権

ドローンによって空撮を行う場合には、プライバシー権以外に肖像権にも配慮する必要がある。肖像権とは「みだりに自己の容ぼう等を撮影されない」という権利ないし法的利益である。¹⁵

そして、他者の容ぼう等の撮影行為が肖像権侵害として違法となるか否かは、判例上、「被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して、被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべき」とされている。¹⁶

具体的には、プライバシー権の場合と同じくケースバイケースの判断になるものの、公道等の公共の場で機械的に撮影をしているうちに人の容ぼう等が偶然に入り込んでしまった場合には、社会生活上の受忍限度

13. 最判平成 15 年 3 月 14 日民集 57 巻 3 号 229 頁

14. 福岡高判平成 24 年 7 月 13 日判例時報 2234 号 44 頁

15. 最判平成 17 年 11 月 10 日民集 59 巻 9 号 2428 頁

16. 最判平成 17 年 11 月 10 日民集 59 巻 9 号 2428 頁

弁護士： 波多江 崇 氏、田中 健太郎 氏、木宮 瑞雄 氏

を超えると判断される可能性は高くない。これに対して、公共の場であっても特定の個人に焦点を当ててその容ぼうを意図的に大写しにして撮影したり、公開されることを通常許容しないと考えられる状況や場面を撮影したりする場合や、住居の内部等にいる人の容ぼうを撮影する場合には、社会生活上の受忍限度を超え、肖像権を侵害するものと判断される可能性が高くなると考えられる。

(3) ドローンと個人情報保護法

個人情報保護法は、個人情報を「生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」と定義づけた上で、個人情報取扱事業者は、偽りその他不正な手段により個人情報を取得してはならないものとされている（個人情報保護法17条）。

したがって、個人情報取扱事業者が不正の意図をもって隠し撮りを行い、その結果、写真・映像等に、特定の個人を識別することができる情報が含まれることとなる場合には、個人情報保護法違反となる可能性がある。

(4) プライバシー等を侵害しないための工夫

総務省は、平成27年9月に『「ドローン」による撮影映像等のインターネット上での取扱いに係るガイドライン¹⁷』を公表し、プライバシー等を侵害しないために、図②のような取組を行うよう提言している。実際にドローンによる空撮を行うにあたって、第三者のプライバシー等を侵害しないようにするために参考となるので、一部抜粋して紹介する。

なお、本ガイドラインに関するパブリックコメント¹⁸では、「ドローンのみ禁止するのはおかしい」「通常の写真や映像の撮影と同じではないか」といった趣旨の意見が寄せられているが、総務省が回答しているとおり、「ドローンについては、これまでより安価で簡便な方法により、通常予期しない視点から戸建て住宅やマンションの部屋の中などを居住者の同意なしに撮影することが可能という特性があり」、かつ、「当該映像等にプライバシーや肖像権などの権利を侵害する情報が含まれていたときは、インターネットによる情報の拡散により、権利を侵害された者への影響が極めて大きい」ことから、「ドローンによる撮影映像等をインターネット上で閲覧可能とする行為について注意すべき事項を取りまとめたもの」にすぎず、新たな規制を課すものではない。言い換えれば、ドローンによるか否かを問わず、映像撮影等に不法行為が成立するか否かは、上記ガイドラインの内容にかかわらず、これまでの裁判例等の基準に基づいて個別具体的に判断されることとなる。

5. ドローンの利用と刑事罰等

ドローンの利用にあたっては、前述した航空法等の規制を遵守する必要があるほか、刑法や条例等に基づく刑事罰を受けないよう留意する必要がある。すなわち、以下に述べるとおり、ドローンの利用によって他人の生命、身体又は財産等を侵害したような場合に、刑法等の刑罰規定が適用されることとなる。

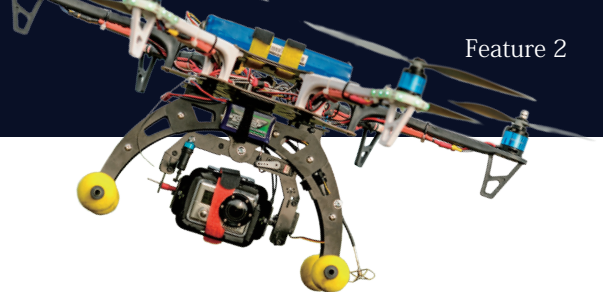
17. http://www.soumu.go.jp/main_content/000376723.pdf

18. http://www.soumu.go.jp/main_content/000376722.pdf

具体的に注意すべき事項

1. 住宅地にカメラを向けないようにするなど撮影態様に配慮すること
 2. プライバシー侵害の可能性がある撮影映像等にぼかしを入れるなどの配慮をすること
 3. 撮影映像等をインターネット上で公開するサービスを提供する電気通信事業者においては、削除依頼への対応を適切に行うこと
- （総務省『「ドローン」による撮影映像等のインターネット上での取扱いに係るガイドライン』8ページより引用）

図②：プライバシー侵害を事前防止するための取組み（一部抜粋、参考）



(1) 人に怪我をさせた場合

具体的には、ドローンを故意に人に当てたような場合には暴行罪（刑法208条）が成立し、それによって人に怪我をさせた場合には傷害罪（刑法204条）が成立する。

ドローンが当たった人が怪我をした場合には、故意がなくとも、過失傷害罪（刑法209条1項）が成立する可能性がある。さらに、ドローンの飛行が「業務上」行われたものである場合、例えばドローン飛行を反復継続しているテレビ局や撮影業者による空撮のための飛行であったような場合には、業務上過失傷害罪（刑法211条）が成立する可能性もある。過失の有無については、ドローンの整備がきちんに行われていたか、ドローンをどのくらいの高度で飛ばしていたか、周囲にどの程度人がいたか等の具体的な事実関係を考慮し、ドローンを飛行させた者がその注意義務を果たしていたか否かを判断することになるだろう。

(2) 物を壊した場合

建造物若しくは艦船を壊した場合には、建造物損壊罪（刑法260条）が成立し得る。また、建造物以外の物を壊したり、動物に怪我をさせた場合には器物損壊罪（刑法261条）が成立し得る。さらに、損壊した物が重要文化財であった場合には、文化財保護法違反の罪が成立することにも留意する必要がある（文化財保護法195条1項）。

実際に、平成27年9月19日にドローンを飛ばして姫路城の大手守最上層に衝突させ、銅製の窓枠を約5センチにわたり傷つけた男が、文化財保護法違反で書類送検されている¹⁹。

(3) 業務や公務を妨害した場合

また、ドローンの飛行によって人の業務を妨害した場合には威力業務妨害罪（刑法234条）が、公務員が職務を執行するに当たりこれに対して暴行又は脅迫を加えた場合には公務執行妨害罪（刑法95条1項）が、それぞれ成立し得る。

平成27年4月9日に放射性物質を含む土砂を入れた容器や発煙筒を載せたドローンを遠隔操作で永田町の

首相官邸の屋上に落下させた男が、同月22日にそれを発見した官邸職員らの業務を妨害したものとして、東京地裁から懲役2年執行猶予4年、ドローンの没収の判決を言い渡されている²⁰。

(4) その他

紙幅の都合上詳述はできないが、上記の他、軽犯罪法、各自治体の制定する迷惑防止条例その他の条例にも違反しないよう留意する必要がある。

6. 終わりに

ドローンという新しいテクノロジーは、多くの新しいサービスやビジネスを生み、私たちの生活や仕事を大きく変える可能性がある。また、上に述べたとおり、ドローンは、新しい法律問題を提示し、既にいくつかの法令やルールを変え、さらに今後も、事故に関わる補償やプライバシーの保護等の観点から、既存の法律の考え方に再考を迫るだろう。そして、今後の方向性として、法規制やルールは、厳しくなっていくことが予測される。このような流れの中で、ドローンのメーカー、あるいは、ドローンに関わるソフトウェアのベンダーは、法的な観点からも、競争力の観点からも、より高度な品質の製品を提供することが求められることになるだろう。筆者らも、安全やプライバシーといった利益を守りながら、ドローンという新しく夢のある技術の発展に微力ながら貢献したいと考えている。

19. 平成 27 年 12 月 10 日付け朝日新聞朝刊 29 面

20. 平成 28 年 2 月 17 日付け朝日新聞朝刊 38 面

木宮 瑞雄 氏

きみや みずお

2009 年 早稲田大学法学部卒業。

2012 年 早稲田大学大学院法務研究科修了。

2013 年 弁護士登録。

2014 年 TMI 総合法律事務所勤務。



「安全設計」を、原子力発電に例えて 分かりやすく解説するシリーズ

ベリサーブ 東日本第三事業部
東 弘之

最終回

原子力事故は何故防げなかったのか

皆様こんにちは。東第三の東(弘)です。
安全設計の紹介の第六回(最終回)に
なります。引き続き、最後まで御付き
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、7. 安全設計の概
念についてお話ししました。今回は「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」を紹
介します。8章では、幾つかの原子力
事故の原因を私なりに纏めます。
9章では、これらの原因を踏まえ、安
全なシステムを作るために必要なもの
を挙げてみます。

1. $E=mc^2$ (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

■ 8. 原子力事故は何故防げなかったのか

放射性物質や放射線が外部に漏れるよ
うな原子力関連施設の事故を、原子力
事故と呼びます。この原子力事故の大
きさを示す指標として、国際原子力事
象評価尺度 (INES) というものが広く

使われています。この指標は、国によ
って事故の大きさをまちまちに評価しな
いよう、原子炉の損傷度合いや外部へ
の放射性物質の拡散量などを基にして、
国際的に統一された尺度です。評価は
7段階で行われ、レベル4以上のもの
を原子力事故と呼んでいます(図1)。

本章では、原子力発電所の大きな事故
を3つ紹介し、それぞれの事故原因を
簡単に纏めます。そして、何故、事故
を防ぐことができなかったのか考えて
みたいと思います。紹介する事故は、ス
リーマイル島原子力発電所事故 (INES
レベル5) とチェルノブイリ原子力発
電所事故 (INES レベル7)、福島第一
原子力発電所事故 (INES レベル7) で
す。事故の真相は、未だに明らかにな
っていないものも多くあります。事故原
因が明確になるということは、責任の
所在が明らかになることを意味します。
組織間で事故原因元の擦り付け合いが
行われるケースが多く、証言と記録が
異なったり、記録の解釈が分かれたり

と、なかなか原因が解明しません。こ
のような未確定な説についても、代表
的な(一番確からしそうな?) 説をペー
スに記載しております。ご了承ください。

■ 8-1. スリーマイル島原子力発電所 事故

スリーマイル島原子力発電所(図2)は、
米国ペンシルベニア州を流れるサスケ
ハナ川の中州にあり、ワシントン D.C. と
ニューヨークの中間地点にあります。炉
型は加圧水型軽水炉 (PWR) で、その
2号炉が1979年に INES レベル5の
事故(所外へのリスクを伴う事故)を
起こしました。INES レベル5は、放
射性物質の限られた外部流出があった
場合や原子炉炉心に重大な損傷があっ
た場合に定められます。

この事故では、原子炉冷却材の流失に
より、炉心の約半分が溶融(メルトダ
ウン)しました。その結果、9万3千
テラベクレルの放射性物質が外部へ流



図1. 国際原子力事象評価尺度
(文部科学省)



図2. スリーマイル島原子力発電所

出しました。多くの周辺住民に避難や屋内退避の勧告が出され、パニックになったそうです。人体への影響はごく軽微で、事故の影響による死者は、公式には確認されていません。余談ですが、原発事故を扱った映画「チャイナ・シンドローム」が公開された直後にこの事故が発生したため、この映画は話題になったそうです。(DVD 持っていますので観たい方は是非)

事故の原因ですが、**些細な問題が起こった(弁の緩みから空気系配管に水が流入した)ことが始まりです**。この異常を検知し、二次系主給水ポンプやタービンが自動停止しました。「何故か開いているはずの補助給水系の弁が閉じたままになっていた」「加圧逃し弁が閉じない故障」「水位計の表示誤り」「表示誤りによる操作ミス」などが相まって、炉心の溶融にまで至りました。事故の主な原因を私なりに纏め、**図 3** に示します。

■ 8-2. チェルノブイリ原子力発電所事故

チェルノブイリ原子力発電所 (**図 4**) は、旧ソビエト連邦 (現ウクライナ) キエフ州にある、黒鉛減速沸騰軽水圧力管型原子炉 (RBMK) です。その 4 号炉が 1986 年に INES レベル 7 の事故 (深刻な事故) を起こしました。**INES レベル 7 は最も高いレベルの事故**であり、放射性物質の重大な外部流



図 4. チェルノブイリ原子力発電所

出があった場合や原子炉の壊滅・再建不能の場合に定められます。

この事故では、炉心溶融 (メルトダウン) を起こした上に、核反応が暴走して爆発し、広い範囲に影響を及ぼしました。事故によって **520 万テラベクレルの放射性物質が流出した**と言われていいます。**事故の公表を遅らせたこともあり、多くの人々が被爆しました**。急性放射線障害で死亡した作業員は 30 人程度とされていますが、事故の影響によって癌などで亡くなった人は多数いると思われます。IAEA や WHO の試算では、数千人規模ではないかと推測していますが、実態は明らかではありません。

事故は、試験運転 (非常用発電系統の

実験) 中に起こりました。実験開始の延期命令などもあり、低出力運転を維持していた炉自体が、不安定な状態になっていました。想定より出力が下がり過ぎたため、出力を上昇させようと次々と制御棒を引き抜き、また**実験に支障が出ないよう安全装置を解除**しました。実験中、急激に出力が上昇したため (この部分は文献により解釈が分かれています)、今度は一斉に制御棒を挿入しました。当時の RBMK 炉は、低出力時に暴走する恐れのある設計で、さらには制御棒の一斉挿入によって出力が一時的に上がる設計になっていました。この一斉制御棒挿入が引き金になって、核反応が暴走し爆発に至りました。事故の主な原因を**図 5** に示します。

1. 故障情報システムの不備 (による運転員の誤判断)

- 異常を示すランプの色が不統一であった。(赤と緑、赤が安全側というランプもあった。)
- 表示ランプ、警告音の数が多すぎた。(事故時、85 の警告音、100 以上の警報ランプが点灯し、訳が分からない状態だった。)
- 注意札で、肝心の異常を示すランプが隠されていた。
- 開閉ランプは状態を示さず、指令情報を示していた。(弁を閉じるように指令したが、実際には故障で開いたままだった。しかしランプは「閉」(指令情報) を示していた。)
- 状態を適切に示さない計器があった。(水位計が水位を示していないケース)
- 警報情報のプリントアウトが遅く、事態の変化についていけなかった。

2. (想定外を想定しない上層部の過信からの) 運転員の教育・訓練不足

- 原子炉や熱現象に対する十分な知識がなく、訓練も乏しい状態だった。
- 安全面ではなく、運転の効率化を中心とした指導を行ってきた。
- 想定された事象でなく対処方法を考慮できなかった。(他計器から誤りを推量できるはず)
- 運転員に全体を見る俯瞰的な視点が欠如し、問題箇所に意識集中してしまった。
- 過去の他の炉で発生した失敗を教訓とせず軽視したため、誰も問題に気付かなかった。

3. 経営悪化、建設コストの引き下げに伴う品質保証の不備

- 故障を繰り返していた機器を、対策することなく用いていた。

図 3. スリーマイル島原子力発電所事故の主な原因

1. 本質安全でない原子炉の設計

- 原子炉が不安定になる特性を持っていた。
(低出力領域では極めて大きい正の反応度フィードバック (暴走する恐れ) 特性を持つ炉)
- 制御棒設計にミスがあった。(ポジティブ・スクラム特性 (制御棒を一斉挿入すると、出力が一時的に上昇する特性) を持った設計)
- 圧力容器や格納容器がなく、事故に耐える構造でなかった。

2. 運転員の知識不足・教育不足

- 危険な状態や危険性のある操作を、運転員に教育していなかった
▶キセノン・オーバーライド特性の理解不足によって、実験開始の延期を受け入れた。
▶炉の反応度操作余裕 (制御棒の効きが悪くなる条件) の理解が不足していた。
▶誰一人、炉が危険な状態にあることに気付かなかった。
- 安全系を切り離して実験するという手順に、疑問を抱かなかった。

図 5. チェルノブイリ原子力発電所事故の主な原因

■ 8-3. 福島第一原子力発電所事故

福島第一原子力発電所(図6)は、福島県双葉町にある沸騰水型軽水炉(BWR)です。2011年の東日本大震災と津波を引き金に事故が発生し、1～4号機から多くの放射性物質が漏えいしました。チェルノブイリ原発事故と同じ、最も高いINESレベル7と評価されています。

この事故では、原子炉の炉心は熔融を起こし、原子炉建屋は水素爆発を起こしました。これらによって被害は拡大しました。旧原子力安全・保安院によると、事故後1ヶ月で77万テラベクレルの放射性物質が流出したということです。



図6. 福島第一原子力発電所

地震によって原子炉は緊急停止しましたが、その後の津波により電源を喪失しました。原子炉心は停止後も冷却を続けないと、燃料が発する熱で燃料自体が溶融します。しかし、非常用のバッテリー電源は余り持続せず、また電源復旧にかなり手間取ったため、炉心溶融(メルトダウン)を起こしてしまいました。また、炉心溶融によって大量に

発生した水素が、ベント(圧力容器の空気を外に抜くこと)により原子炉建屋内に充満し、水素爆発を引き起こしました。現場作業員が復水器を手動停止したり、水素発生を想定せずにベントしたりと、事故時の対応も十分ではありませんでした。事故の主な原因を図7に示します。

1. いざというときの準備不足(事故後の対応不備)
 - a. 長時間の電源喪失を想定した対応マニュアルが無く、事故対応中に手順を作成した。
 - b. 必要機材の連絡に不備があり、調達後の機器選別に時間を要した。誤配も発生した。
2. 運転員の知識不足・教育不足
 - a. 水素爆発を誰も予見できなかった。予見していれば、適切な対応を行えたはずである。
 - b. 他の冷却系で何とかするという甘い認識を持っていた。
 - c. 電源喪失時に自動で復水器弁が閉じるという仕組みを誰も知らなかった。
 - d. 破損するはずのない復水器を、破損する可能性を考慮して手動停止した。
3. 数々の提言・指摘を軽視し続けたこと(参考: Wikipedia)
 - a. 格納容器・建屋の強化、電源・水源の多重化し、水素爆発の防止装置をつけるべきなど、専門家からの提言が東京電力にあった(1992)。しかし、GE社から対策の話が来ないので不要と考え、対策を行わなかった。
 - b. 想定する津波の高さを15.7mに引き上げられていた(2008)。しかし、速やかな改修を保安院から指示されていなかったという理由で、津波対策を実施していなかった。
 - c. 電源喪失や大津波による冷却水喪失によって炉心溶融になる可能性についての指摘を国会等で質問された(2006/2010)。しかし、事例が無い(首相)、多重防護でしっかり事故を防げる(経済産業大臣)などとした。
 - d. 福島県内の原発は地震や津波対策が不十分だとIAEAから指摘された(2007)。これに対し、対策を強化すると言ったが、津波対策は行われなかった。
 - e. 大地震や津波を考慮しない理由を審議会で東京電力に問い質したが(2009)、情報が不十分で検討は続けるという回答だった。

図7. 福島第一原子力発電所事故の主な原因

安全なシステムを作るために

8章では、3つの大きな原子力事故について、何事故に至ったのか、何事故が拡大したのか、その主な原因を述べました。これらの原因を見て頂けると、何だかどの事故にも共通した原因があるように見えないでしょうか。基本的には、「安全設計の不備(故障情報システムの不備、本質安全でない設計、品質保証の不備)」「運転員の知識・教育不足」、そして「教訓や提言の軽視」あたりが原因になっていますでしょうか。

これら原因の裏には、共通した背景が見受けられます。それは「正常を逸した経済性の優先」と、「リスクに対する考え方の甘さ」です。スリーマイル島原発の品質保証の不備やチェルノブイリ原発の安全設計の不備は、いずれも安全性よりも経済性を優先させたことによります。福島第一原発における様々な提言や指摘を軽視した背景には、コストカットの強い圧力があったという話もあります。運転員への教育内容についても、原子炉の仕組みや特性、問題発生時の対処法よりも、経済的・効率

的な運転方法が中心となっていたそうです。このような教育では、いざ事故という時に、正しい判断や操作を行えません。

7章(前回のペリナビ)で述べたとおり、ISO/IEC Guide51では、「安全」を「受容できないリスクがないこと」と定義しています。この「リスク」は不確実な事項を扱うだけあって厄介です。同規格では、安全という概念について説明を行っています。そこでは、許容可能なリスクは、利便性や費用対効果、慣習

などの諸要因によって満たされるべき要件とのバランスで決定されるとあります。このバランス感覚は、どうしても利益を追求する運営会社側の都合（すなわち経済性）を優先しがちになります。映画「チャイナ・シンドローム」でも同様の筋書きでした。これだと、いくら安全設計技法を適用しようと、リスクの評価が正しく行われず、システムの安全性が高くなることはありません。（安全性に限らず、この話は利益率を優先する開発プロジェクトいずれにも当てはまりがちなと思います。）

纏めると、**安全性と経済性のバランスを正しく取ることこそが、安全なシステムを作るための最も重要な事柄**ではないでしょうか。そのためには、これらバ

ランスを正しく取れるような仕組みを作ることや、**経済性に傾かないほどの仕事への誇りや責任感を持った人材の**

創出こそが、その近道であると感じます。安全なシステムを作るために必要と思われる事柄を図8に示します。

1. **安全性に十分考慮する（当たり前？）。**
 - ▶ 安全性の高いシステムを目指し、適切な手法で安全性を高めると同時に、設計者や運用者に安全を優先した教育を施すことや、予算割り当てが安全面を十分に考慮したものであることが大切です。
2. **設計者や運用者への教育は、とても重要である。**
 - ▶ 「何故この手順なのか」「何故この規則があるのか」を理解しない担当者は、面倒だからと勝手に規則を変更したり、適当に作業したりします。また、理由を理解していないと、問題発生時に適切な対処を行えません。さらには、見張られていないと、面倒な規則や手順は破られます。規則を順守していることのチェック体制も必要です。
3. **経済性・生産性とは切り離れた組織が、安全性についてしっかりと判断する。**
 - ▶ 経済性を優先するのは、収益団体が事業主である限り仕方のないことなのかもしれません。事業主に対して、安全性に対する理解、安全性の重要性を啓蒙するだけでなく、経済と完全に分離した組織が、安全性と経済性について、バランスに偏りがちなことをチェックする体制を作り、かつそれを維持する必要があると感じます。
4. **安全対策は、纏めて一気にすり抜けるものである。多重防護を過信しないこと。**
 - ▶ 多重に対策していても、数々の安全対策を纏めて吹き飛ばします。1つ1つの対策に、心を込める必要があります。
5. **仕事への誇り、責任感を持つ / 持たせる。**

図8. 安全なシステムを作るためには案

あとがき

原子力施設は安全を高く意識して作られているはずですが、大きな事故が度々起こっています。本コラムではその根本原因を、「**正常を逸した経済性の優先**」と「**リスクに対する考え方の甘さ**」といたしました。安易に経済性に偏る考え方から目を背けないと安全性を保てず、結局は重大事故に繋がってしまいます。人類が原子の力を扱うには時期尚早なのかもしれません。

故・吉田昌郎元福島第一原発所長は、前例も無く唯一の冷却手段だった海水注入を、迅速で的確に決断し、実行しました。その後、上層部からの海水注入中止の命を受けた時も、拒否して注入を続行しました。上層部は、海水注入による原子炉腐食による廃炉や、海水注入による再臨界の可能性（結局危険無しという結論に至りました）、官邸からの了承が無い状況などを恐れ、注入中止を指示しました。最後の最後まで、上層部は迅速な判断を行わず、バランス感覚は経済性に偏ったものでした。この海水注入の続行がなければ、東京や東北地方は住めない地域になっていたかもしれないとも言われています。**吉田所長は、経験の無い状況でも的確に状況を把握、判断し、最後まで安全と経済のバランスを崩すことなく、誇りを持って処理にあたっていたのだと思います。**爆発を避けるための決死のベント作業を行った吉田所長の部下たちは、このような思いを持っていた吉田所長の命令だからこそ、死を覚悟しながらも指示に従ったと言っています。このような人材を育てることこそが、安全なシステムを作るため、維持するために必要なのではないのでしょうか。

ベリナビ執筆依頼を受けた際、たまたまシステムの安全性について興味を持っていたため、原子力発電所の安全性と結び付けて何か書けなかなと思い、本コラムを書くことにしました。色々と調べながら書いていましたので、話の流れを整えるのに苦労しました。8章（原子力事故の説明）の説明のために5章まで（核分裂反応や原子力発電の仕組み）の説明をしたのですが、仕組みの話を8章で活かせなかったことが、執筆にあたっての反省点です。

全6回に渡り、読み辛く未熟な文面に最後まで御付き合いいただきました読者の皆様に感謝いたします。最後まで御付き合いいただき、ありがとうございました。

東 弘之

「ソフトウェアと品質を考える」

日時

2016年9月8日(木)

場所

FUKURACIA
東京ステーション

開催報告

ベリサーブ マーケティング部

豊本 奈美江

去る2016年9月8日(木) FUKURACIA東京ステーションにて、ベリサーブ主催「アカデミックイニシアティブ『ソフトウェアと品質を考える』」を開催いたしました。当セミナーではソフトウェアの役割とその重要性が益々増大する中でIoTや自動車、自動化などの様々な切り口から、ソフトウェアの構築や品質向上へのヒントをご紹介します。

セミナーは冒頭の主催者による開催ご挨拶に続いて、2つの基調講演が行われました。

基調講演1 清水 吉男 氏



派生開発推進協議会代表
株式会社システムクリエイツ 代表取締役 清水吉男 氏

1つ目の基調講演では、派生開発推進協議会代表株式会社システムクリエイツ 代表取締役 清水吉男氏により、『IoT時代の派生開発とテスト』～変更情報が見えることでアジャイルへの対応も～と題してご講演いただきました。

「IoTは救世主か?」「開発現場の問題」「XDDPをアジャイルに対応するには」の3つの切り口から、“Software defined XXX”をキーワードとし、「**価値を継続的に、機敏に提供し続ける**」ことが強力な競争力となり、派生開発においてアジャイルな対応が求められることが説明されました。XDDP (eXtreme Derivative Development Process - 派生開発に特化したプロセスモデル) により、ソースコードの「変更」にアジャイルな対応が可能であるとし、その方法論を説明した上で、ソースコードの劣化や変更に対応できるスキルが必要であることも付け加えました。

わかりやすい資料と軽快な説明で参加者の好評をいただく内容となりました。

基調講演2 木下 佳樹 氏

2つ目の基調講演では、神奈川大学 理学部情報科学科 教授 木下 佳樹氏により、『オープンシステム・ディペンダビリティのアシュランス議論とディペンダビリティケース』～IEC62853のアプローチ～のテーマでお話いただきました。刻々と変化するオープンシステムについて、想定外の事態が発生しても期待され

るサービスを継続させる「ディペンダビリティ」の達成方法について、IEC62853の考えを交えながら説明されました。オープンシステム・ディペンダビリティを実現させるために、IEC62853の草稿で規定されている4つのプロセス「合意形成」「説明責任遂行」「障害対応」「変化対応」が必要であることと、それらを議論するために **GSN (Goal Structuring Notation)** の記述が有効であることが説明され、IEC62853規定の国際標準化に期待を寄せられました。

ディペンダビリティの用語を初めて聞く参加者も多く、新しい視点を得られた内容となりました。



神奈川大学 理学部情報科学科 教授 木下 佳樹 氏

当社社員による講演

基調講演の後、当社社員3名より講演を行いました。最初に谷崎 浩一から「効果的なテストを効率的に設計するための世界初のブレイクスルー ～テスト設計の方法論・支援ツールを活用～」のテーマで、効果的なテスト設計の方法論とテスト設計支援ツールについてご紹介しました。展示コーナーでのご説明では多数の参加者を集っていただき内容に対する関心の高さが伺えました。

次に後藤 香織により「事例から見るテスト自動化導入のいろは ～保守運用で泣かないための効果的なテスト自動化導入アプローチ～」と題し、



左から、当社 山崎 崇、谷崎 浩一、後藤 香織



セミナー会場の様子

テスト自動化導入の失敗事例と解決のためのポイントを、導入時・構築時・運用時・人が去る時の4つの時系列で解説しました。即時的な効果を期待されがちな自動化について、中長期的に成功を出すことを想定しておき、繰り返しテストをすることでコストメリットが期待できることを説明しました。説明資料は文字が大きく挿絵も多く、わかりやすいと好評を得ました。

最後に、山崎 崇より「テストからはじめるプロセス改善 ～テストプロセスアセスメントを利用した段階的な継続的改善活動のすすめ～」のテーマで登壇し、テスト改善活動としてテストプロセスアセスメント改善方法の概要とポイントについて、テストプロセスアセスメントを行うメリットと、実践する上でのポイントを解説しました。説明ポイントが明確で、実践的な内容に参加者の皆様に満足いただける内容となりました。

セミナーの締めくくりとして、閉会のご挨拶の後、展示ブースにおいてお集まりいただいた参加者の皆様へ当社サービスのご案内を行うとともに、講演者より講演内容についてのご質問に対して説明を行いました。

ベリサーブ アカデミックイニシアティブは名古屋、大阪でも開催予定です。是非ふるってご参加ください。

VERISERVE NAVIGATION

読者アンケート

ベリサーブオリジナル商品プレゼント!

いつも『VERISERVE NAVIGATION』をお読みいただきましてありがとうございます。

今後さらに充実した内容をお届けできるように、記事に関するご意見・ご要望をお聞きする読者アンケートを実施いたします。是非ともご協力いただきますよう、宜しくお願いいたします。

アンケートにご回答いただいた方にはオフィスで使えるオリジナル商品をプレゼントいたします。

応募方法は以下の2通りです。

1

QRコードを読み取って応募



2

URLから応募

<https://questant.jp/q/LNQU0GUG>

ペンやスマートフォンを立てられます。

※ペン・スマートフォンは付属しません。

木製デスクスタンド



2016年6月17日(金) いたみホール JaSST'16 Kansai

ソフトウェアテスト技術振興協会 (ASTER)、JaSST' 16 Kansai 実行委員会主催



基調講演会場風景

基調講演で日新システムズの前川氏より、「未来を共有することから部門の壁を越えて価値を描く組織になる」をテーマに、営業・企画・技術・テスト・品質保証など関連部門の役割を最大限に活かせるソフトウェア開発について講

演がありました。また個別／企画セッションとして、派生開発、テスト自動化、ユーザビリティなどを切り口として5セッションが開催されました。当社は、スポンサーセッションにおいて品質向上支援企業ベリサーブを紹介しました。



当社 山口 信太郎によるスポンサーセッションの様子

Cloud Days 2016 主催 日経BP社 IoT Japan 名古屋 2016 2016年6月16日(木)～17日(金) 名古屋国際会議場

本年3月に開催した東京と大阪に続き名古屋でもブース出展を行いました。「テスト自動化ソリューション」と「多端末接続性検証サービス」のパネル展示を行い、約110名の当社ブース来場者にサービス説明を行いました。



当社ブース



“ものづくり”がわかる、 “IoT”がわかる ETWest2016

2016年7月7日(木)～8日(金)
グランフロント大阪
一般社団法人組込みシステム技術協会
(JASA) 主催

昨年と同様ブース出展を行い、「テスト自動化支援サービス」、「ドキュメント検証サービス」および「沖縄テストセンター」をパネル展示、当社ブースへの来場者にサービス説明を行いました。



当社ブース



ソフトウェア品質向上で社会を支える

30年以上にわたり、
ソフトウェア検証で品質向上に貢献しています。

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





VERISERVE NAVIGATION 『ベリサーブナビゲーション』 2016 年 10 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 西新宿三井ビル 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

※本ベリナビの記事中に掲載する社名または製品名は、各社の商標または登録商標です。