第11回クリティカルソフトウェアワークショップ（11thWOCS^2）開催報告

独立行政法人宇宙航空研究開発機構（JAXA）
情報・計算工学センター ソフトウェアエンジニアリングチーム
大久保　梨思子　　氏家　亮
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）企画グループ
荒川　明夫

1. 開催概要

クリティカルソフトウェアワークショップ（WOCS^2）は、独立行政法人宇宙航空研究開発機構（JAXA）と独立行政法人情報処理推進機構（IPA）が共催する、宇宙・航空、自動車などのミッションクリティカルなソフトウェアの開発・運用・保守に関する技術やプロセスに焦点を当てたワークショップである。WOCS^{2}は2002年から開催しており、2009年からはIPAとの共催で産、学、官の枠をも超え、ソフトウェアシステムの安全についての議論の場を提供している。

第11回を迎えた今回のWOCS^{2}では、「SecurityとSafetyを融合させたシステムを考える」を主テーマとして掲げ、2014年1月15日（水）から1月17日（金）の3日間、御茶ノ水ソラシティカンファレンスセンターにて開催した。

2. 専門セミナー

1/15には専門セミナーとして、ソフトウェアの安全性と信頼性を確保するための技術に関するセミナーを開催した。このような専門セミナーの開催はWOCS^{2}において初めてである。今回はJAXAが実施するソフトウェアIV&V（独立検証及び有効性確認）の基礎について講義を行った。

ソフトウェアIV&Vとは、ソフトウェアのVerification（検証）とValidation（妥当性確認）をIndependent（独立）に実施することであり、JAXAでは1990年代から実施してきた。平成25年にはIPAにより「通称：ソフトウェア品質説明のための制度ガイドライン」が整備され、製品やシステムの品質説明力強化のために、供給者から独立性を確保した第三者による認証活動が注目されている。

セミナーではまず、IPA鈴木基司、JAXA片平真史からIV&Vを導入することの意義や効果について講義が行われた。IV&Vは決して網羅的なバグだしではなく、重大な技術的欠陥を早期に抽出することを目的としており、適切な評価観点／手法／範囲を選択することの重要性について説明を行った。

次に、前述の評価観点／手法の具体例について、JAXA梅田浩貴と川口真司から「IV&Vガイドブック【虎の巻】」（JAXA発行）を用いた講義が行われた。演習ではセンサー付き宇宙用便座のシステム仕様を題材とし、評価観点の詳細やV&VとIV&Vの違いについて説明が行われた。

（http://www.ipa.go.jp/sec/events/20140115.html で講義資料を公開中。また、JAXA講義資料及びIV&Vガイドブックの入手については IVV_INFO@jaxa.jp まで。）

3. 基調講演・招待講演

1/16にはソフトウェアの安全性、信頼性、セキュリティに関する基調講演、招待講演が計6件行われ、約150名が聴講した（表1）。

【基調講演】では、三菱航空機株式会社の篠田 和英氏、技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）／電気通信大学の新 誠一氏、株式会社ソニーコンピュータサイエンス研究所の所 眞理雄氏にご登壇いただいた。

篠田氏からは、高い安全性が要求される民間航空機において、発生確率が算出できる物理的な故障だけでなく、発生確率が定義できないソフトウェア開発中のエラーなどへの対策が重要視される現状についてご説明いただいた。更に、その様な対策を実現し、安全性を担保するためには安全・開発保証プロセスが重要であり、Mitsubishi Regional Jet（MRJ）の開発で如何に安全・開発保証プロセスに取り組んでいるかを型式証明の話を交えてご講演いただいた。

表１：基調講演／招待講演のプログラム

10：00 〜 10：10	開会挨拶 独立行政法人 宇宙航空研究開発機構 執行役　井澤一郎
10：10 〜 10：40	**オープニング講演** 独立行政法人 情報処理推進機構 ソフトウェア高信頼化センター　所長　松本隆明
10：40 〜 11：30	**民間航空機の安全・開発保証プロセスについて** **〜 MRJ 開発における取り組み〜** 三菱航空機株式会社 技術本部　開発保証部　部長　篠田和英
11：30 〜 12：20	**Safety Assessment Method for Flight Operation System.** **〜 Lessons from "RNP AR approaches" to Haneda Airport.** DNV ビジネス・アシュアランス・ジャパン株式会社 代表取締役社長　前田直樹
13：40 〜 14：30	**制御系セキュリティの国内での取り組み** 技術研究組合制御システムセキュリティセンター 理事長　新誠一
14：30 〜 15：20	**組込みシステムのセキュリティ対策 〜繋がる車でのケーススタディ〜** 独立行政法人 情報処理推進機構 技術本部 セキュリティーセンター 情報セキュリティ技術ラボラトリー主任 中野学
15：40 〜 16：30	**ハイブリッド認証に向けての工学的アプローチ** **〜機能安全とセキュリティの同時認証のための方法論〜** 独立行政法人 産業技術総合研究所 セキュアシステム研究部門システムライフサイクル研究グループ招聘研究員 田口研治
16：30 〜 17：20	**DEOS：巨大・複雑で変化し続けるシステムのディペンダビリティーを達成する** 株式会社ソニーコンピュータサイエンス研究所 エグゼクティブアドバイザー / ファウンダー　所眞理雄

（篠田和英氏）


（新誠一氏）

（所眞理雄氏）

新氏からは、近年制御系システムでセキュリティ対策が何故重要視されているか、対策の実現が何故難しいかについて、社会インフラなどでのセキリティ攻撃実例を交えてご説明いただいた。更に、制御系システムのセキュリティ問題への対策を検討するために CSSC が開発した様々な模擬システムのご紹介、CSSC が展開する評価認証・標準化活動のご紹介、今後の制御系システムのセキュリティ対策の展望についてご講演いただいた。

所氏からは、現代のコンピュータシステムは、機能、構造、システム境界が時間的に変化しつづけるシステム（オープンシステム）であり、その変化への対応、潜在的な障害の除去、説明責任の達成が非常に困難である現状についてご説明いただいた。更に、現状を打破するために検討された知識・技術体系である「オープンシステムのためのディペンダビリティ工学（DEOS：Dependability Engineering for Open Systems）」の検討過程、各検討段階で議論された課題、手法やツールを含む具体的な課題解決方法について、応用事例を交えてご講演いただいた。

【招待講演】では、DNV ビジネス・アシュアランス・ジャパン株式会社の前田 直樹氏、情報処理推進機構の中野 学、株式会社シーエーブイテクノロジーズ／独立行政法人産業技術総合研究所の田口 研治氏にご登壇いただいた。

前田氏からは、セーフティクリティカルなシステム開発で重要な役割を果たす安全性評価について、羽田空港 D 滑走路でのセーフティアセスメントの経験を基に、効果的な安全性評価の実現についてご講演いただいた。中野からは、組込み機器におけるセキュリティの現状とセキュリティ分析手法について、自動車を例としたご講演をいただいた。田口氏からは、現在の製品・プロセス認証の問題点を踏まえ、安全性とセキュリティの規格の同時認証の重要性とその実現方法についてご講演いただいた。

（基調講演、招待講演ともに、http://www.ipa.go.jp/sec/events/20140115.html で講演資料を公開中）

4. 一般講演

1/17 には一般講演として、様々な産業分野の企業、大学、研究所から全 18 件の安全及びセキュリティに関するご講演をいただき、約 130 名が聴講した。

（http://www.ipa.go.jp/sec/events/20140115.html で講演資料を公開中）

■ 11thWOCS^2 一般講演受賞者

安全に関するセッション（Safety セッション）での優秀賞の受賞者を表 2 に、セキュリティに関するセッション（Security セッション）の受賞者を表 3 に示す。

表 2：Safety セッション受賞者

Safety セッション	
最優秀賞	**「CARDION: 概念段階におけるハザード・脅威の抽出手法」**伊藤　昌夫（株式会社ニルソフトウェア）
優秀賞	**「イプシロンロケット搭載ソフトウェアによる安全設計の実装について」**井上　知也（株式会社 IHI エアロスペース）
	「JAXA-PAM と CMMI の補完的活用によるプロセス評価の効率化」込山　博（日本電気株式会社）

表 3：Secuity セッション受賞者

Security セッション	
最優秀賞	**「組込み開発におけるセキュリティ対策及び試験手法に関する一考察」**平井　康雅（株式会社 NTT データ）
優秀賞	**「著作権保護システムの車載セキュリティ応用と Safety への展開について」**倉内　伸和（パナソニックアドバンストテクノロジー株式会社）
	「形式手法を用いた安全・セキュリティ分析手順と要件の抽出方法の提唱」和田　学（株式会社ヴィッツ）

Safety セッションでは、宇宙機をはじめとした、高い信頼性が必要なシステム・ソフトウェアの開発や、安全性・信頼性向上のための取り組みについて講演があった。最優秀賞の伊藤氏は、開発の初期段階（概念段階）でハザード・脅威を抽出する手法について、車載ソフトウェアを例に講演された。

Security セッションでは、安全性とセキュリティを同時に確保することの難しさや相互の依存関係について多くの講演があった。最優秀賞の平井氏は、セキュリティが安全を脅かす 1 要素であると捉え、新たな枠組みを持つセキュリティ試験手法への取り組みについて講演された。従来、安全とセキュリティは別分野として発展してきたが、平井氏の講演は今回の WOCS^2 で掲げた「Security と Safety を 融合させたシステムを考える」というテーマに合致した講演であった。

5. SEC journal 論文書表彰式

1/17 の一般講演の後、WOCS^2 会場内にて平成 25 年 SEC journal 論文賞の受賞論文の発表を行った。最優秀賞を受賞した酒井氏の「アプリケーション保守サービスの定量化手法」についての論文は、従来見積もることが難しかった保守サービス量のコストや工数を独自の手法を用いて数値化し、これを可能にした点が高く評価された。

表 4：受賞者 3 編

SECjournal 論文賞	
最優秀賞	**「アプリケーション保守サービスの定量化手法」**酒井　大（日本アイ・ビー・エム株式会社グローバルビジネスサービス）
優秀賞	**「システム価値向上を目的とした Scrum の試行・評価」**中村　伸裕（住友電気工業株式会社 / 大阪大学）
所長賞	**「若年技術者向けソフトウェア開発研修プログラムの開発と評価」**大森　久美子（NTT　サービスイノベーション総合研究所　ソフトウェアイノベーションセンタ）

（SEC journal については、下記 WEB ページをご覧ください。

http://www.ipa.go.jp/sec/secjournal/index.html）

6. 今後の WOCS^2 について

今回の WOCS^2 では、昨年のアンケートを踏まえ、過去の WOCS^2 で扱っていない航空機分野の基調・招待講演を行い好評であった。今回もアンケートを通して多くのご意見をいただいたので、次回 WOCS^2 の基調・招待講演を含む全体運営に反映していく予定である。また、IV&V 専門セミナーについては、同内容の開催やより詳しい研修の要望が多く、新たなセミナーを企画していきたい。

次回 WOCS^2 については、2014 年 6 月以降に開催告知を行う予定である。

7. 謝辞

WOCS^2 プログラム委員の皆様、後援団体の皆様にはワークショップ成功のためにご支援いただきました。ここに深謝いたします。