「実用化を目指した組込みシステム用
ディペンダブル・オペレーティングシステム」
平成20 年度採択研究代表者

H24 年度
実績報告

倉光君郎

横浜国立大学大学院工学研究院･准教授

Security Weaver とＰスクリプトによる実行中の継続的な安全確保に関する研究

§１. 研究実施体制

(1)「倉光」グループ

①研究代表者:倉光君郎 （横浜国立大学大学院工学研究院、准教授）

②研究項目

・D-Script オープンソース開発と実証実験

(2)「山本」グループ

①主たる共同研究者:山本修一郎 （名古屋大学情報連携統括本部、教授）

②研究項目

・発展型 DEOS プロセス・アーキテクチャの研究

(3)「永山」グループ

①主たる共同研究者:永山 辰巳 （株式会社 Symphony 代表取締役）

②研究項目

・継続的 OSD 改善のための Agreement Description Database の研究開発

(4)「恩田」グループ

①主たる共同研究者:恩田 昌徳 （富士ゼロックス株式会社 研究技術開発本部コミュニケーション技術研究所）

② 研究項目

・D-Case 構成要素としての関連文書の管理機能の開発

・実証実験・ヒアリング等による有効性の検証

§2. 研究実施内容

(文中に番号がある場合は(3－1)に対応する)

(1) 全体: DEOS プロセス/アーキテクチャの実現にむけて

平成 24 年度は、本研究領域が目指すDEOSプロセスの実用化を一段と進めるため、産業界からの共同研究者を増やし、永山グループと恩田グループを追加した研究体制を構築した。これにより、研究代表者らが中心となって進めてきた D-Script、 平成 23年度より参画した山本グループによる D-Case 研究を結び、DEOS プロセスを実現する要となる D-ADD の研究開発と産業界を含めた実証実験が行えるようになった。

以下、研究グループごとに、研究実施内容を報告する。(A,B,C,D は、3-1 に対応)

(A) D-Script と実証実験 (主に倉光グループが担当)

D-Script は、変化するユーザの要求や環境変化にたいして、ステークホルダー合意を迅速的にシステムに反映させ、障害対応から変化対応まで実現するオープンシステムディペンダビリティを担うスクリプト技術である。倉光グループらが中心となって、DEOS プロセス/アーキテクチャの中核的な位置づけとして、企業ユーザと「スクリプトによる高信頼サービスの実現」ワークショップを開催しながら議論を深め、同時にオープンソースによる参照実装の開発を行ってきた。

今年度は、障害対応の D-Script の実証実験として、オンライン教育プログラミングシステム ASPEN の開発を行い、実際に横浜国立大学と早稲田大学の2つの演習科目において運用を行った。[A-8] その結果、予想外のサーバ負荷による障害対応、合意形成の難しさ、ログデータの消失などいくつかの重大な障害事例に直面し、スクリプトによる障害対応における実データを得ることができた。本実証実験は、サーバ環境を学内サーバから Amazon AWS クラウド環境に移行し、より企業ベースの運用体制で実証実験の規模と質を拡充した。

D-Script の記述実験では、D-Case によるスクリプトの記述手法の検討と、運用システムとの統合を検証した。特に着目したのは、障害診断スクリプトであり、D-Case モニターノードから障害回復の間をつなぐ重要な過程となる。図 1 は、D-Case でネットワークの正しさを議論しながら、個別のエビデンスとしてスクリプトの実行結果を配置したものである。D-Case を用いて議論することで、より網羅性の高いスクリプトが開発できた。このために D-Script と D-Case の統合開発環境としてツールの開発を行った。本手法を FX10 スパコンシステムの障害診断に適用すべく、東京大学情報基盤センターとの議論を開始している。

また、障害スクリプト作成の過程で、スクリプトの安全性が新たな課題となった。本来ならソフトウェアのリスク抽出は要求定義の過程で十分に行われるべきであるが、スクリプトの記述のときになってそれが不十分であることがわかることが多い、という実態に基づく。例えば、RAM ディスクにデータを一旦保存するというスクリプトは、プログラム的には何ら問題はないが、停電によるデータ損失のようなリスクが内在し、これらが2次災害を招く危険性が大きい。我々は、スクリプトのリスク抽出を半自動的に行うため、リスクボキャブラリの整備を行い、リスクボキャブラリと D-Case の議論を統合した

障害対応スクリプトの設計理論の検討を進めている。

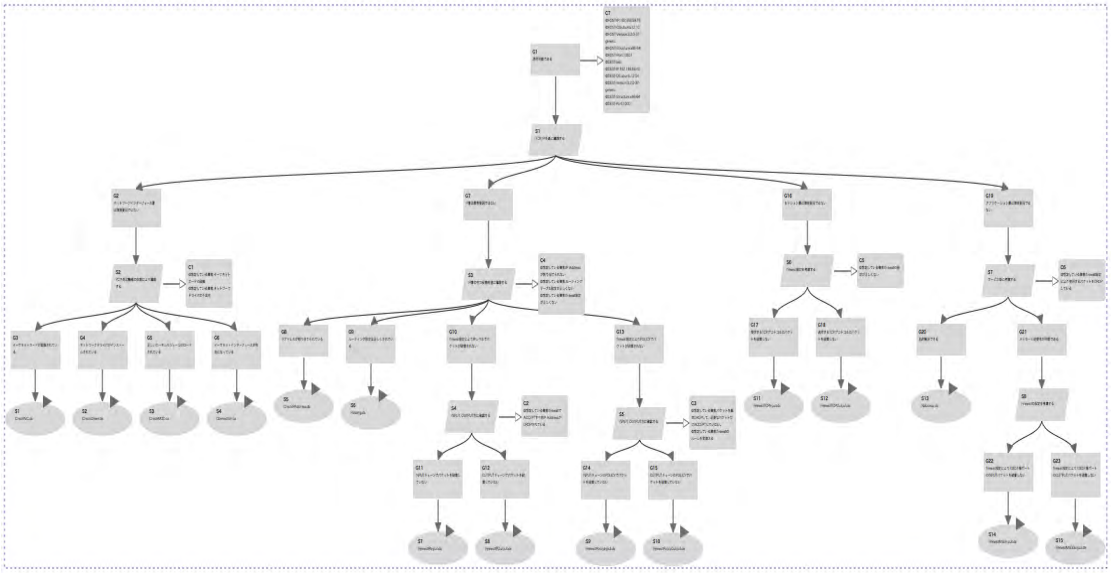

図1　D-Case の議論による D-Script の開発

D-Script のオープンソースソフトウエアとしての実装に関しては、従来の Konoha を最小限の機能に絞込み、約6分の1の大きさにコンパクト化を行い、ソフトウェアとしての堅牢さを高めた。これにより、大規模サーバシステムだけでなく、省メモリの組込みシステム環境(64kb 程度)まで、広範囲な実行環境で安定してスクリプト処理が可能になった。[A-9] 今後は、クラウド環境におけるデファクトである Amazon Web Service において、障害対応（モニタリング、診断、バックアップ、可用性向上など）サンプル記述を行い、記述性の評価を行なっていく予定である。

(B) D-Case 実証実験（主に山本グループが担当）

＜研究のねらい＞DEOS プロセス・アーキテクチャにおけるシステムのディペンダビリティ情報を担う D-Case は、これまで DEOS D-Case チームを中心に、基礎研究およびいくつかの実証実験を、ツール開発、標準化と並行して行なってきた。平成24年度は基礎研究・実装と並行しながら、特に企業の方が実際の業務において用いることを目指した。さらに DEOS, D-Case の国際標準化をねらった。

＜これまでの研究の概要＞ 山本グループでは平成23年度では、DEOS プロセスにおける要求マネージメントの基礎設計を行った。また一期生の石川研究チームおよび D-Case チームでは D-Case の記述法、ツール開発、システムモニタリング機能との連携の基礎開発を行った。

これらの研究成果を元に、企業の方々を対象として、D-Case 記述法、パターンに関する、パワーポイントスライドを基にした D-Case 入門本を出版した。これを用いて、企業、大学院生などを対象とした D-Case 講習会を 4 回開催した。企業の方々との交流の場として D-Case 実証評価研究会を 2 回開催した。企業の実際の製品を対象とした D-Case 記述実験を 3 回行った。また学生とともにスーパーコンピュータ運用手順、TOGAF などへの適用実験、さらに D-Case と用語辞書の相互変換

の検討などを行った。これらにより得られた知見をもとに、D-Case の実践に関する本を出版した。富士ゼロックスで開発されてきた D-Case の拡張を行い、GSN Community Standard への準拠、モジュール、さらには、ネットワーク間の D-Case の関係をモデル化する d*フレームワークの基礎実装を行った(図2)。

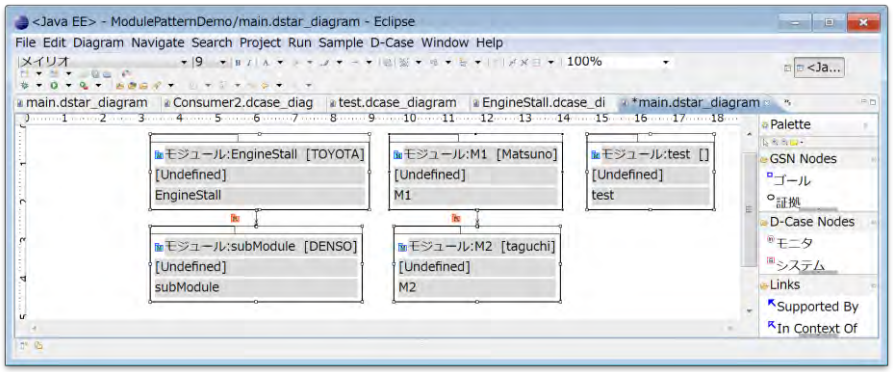

図2 d*フレームワークのための D-Case Editor における基礎実装

またオープングループ、OMG などの標準化会議で DEOS, D-Case の標準化を進めた。D-Case の情報提供の場として D-Case ホームページを開設した(http://www.dcase.jp)。ホームページには企業との共同実証実験の報告などがある。DEOS プロセスにおける D-RE, D-Script との連携基礎実験なども ET2012、オープングループなどをターゲットに引き続き行った。

＜研究成果＞ 研究成果として、国際論文誌 2 本、国際会議論文、その他研究会論文、口頭発表など45件が得られた。D-Case 実証評価研究会は 2 回とも 30 名以上の企業の方々が参加され、我々の研究報告に加え、企業の方からの発表を多く含み、活発な議論が行われた。図 3 は 2 月 20 日に名古屋のデンソークリエイト社で行われた第1回 D-Case 実証評価研究会の様子である。

図 3 第1回 D-Case 実証評価研究会の様子

D-Case 実証評価研究会は 2013 年度も開催される予定であり、DEOS 実用化のための集まりの一つになることが期待される。D-Case 講習会は試行を重ね、一日コースとして形が整ってきた。

D-Case Editor の機能拡張は[B-4]において発表予定である。オープングループでの標準化は Real Time Embedded Forum において、D-Case を中心とした提案内容の Company Review が行われる予定である。また、OMG においてトヨタ大畠氏を中心とした消費者機械規格の提案に協力し、2013 年 3 月に RFP(Request for Proposal) (http://www.omg.org/cgi-bin/doc?sysa/2013-3-20) が発行された。RFP には、DEOS ホワイトペーパーが参照されている。

＜今後の見通し＞ D-Case 入門、D-Case 実践本、D-Case ウエブページ、実証評価研究会、講習会など、企業への情報発信、コミュニケーションが軌道に乗りつつある。基礎研究成果の D-Case Editor への実装により、D-Script, D-RE との連携による DEOS プロセスの実証も視野に入りつつある。平成25年度はIPAなどの団体や企業の協業を通して、D-Case 実用化のためのまとめの研究開発が行える見通しである。

(C) D-ADD の開発（主に永山グループが担当）

＜研究のねらい＞ これまでの領域の研究にて、D-Case を格納するデータベースとして定義されてきた ADD（Agreement Description Database）について、DEOS プロセスを実行するための機能要件を明らかにして、領域の他の研究（D-Case、D-Script など）を統合することを実現する。DEOS プロセスを一巡させるための機能を持った ADD を、H24 年度より D-ADD と再命名した。

D-ADD は、単に D-Case の格納データベースだけにとどまらず、DEOS プロセスの各状態に依存した情報間の連携、運用する人間の操作、そして、D-ADD に格納される D-Case、各種文書の修正によるアシュアランスケースの更新、システム状態の変化に対応しなければならない。本研究は、それらを実現する D-ADD の諸性能を定義しなければならない。それらの機能を詳細化する中で、定型データ処理において実績のあるリレーショナルデータベースでは時間と共に情報の構造が変化する対象について効率よく表現することは難しいと考え、リレーショナルデータベース以外のデータベース技術を導入して D-ADD の設計を行う。

＜研究概要＞ D-ADD に格納される対象システムの情報（契約書、設計書、仕様書他、D-Case）は、正規化されたテーブル型のリレーショナルデータベースに格納するよりも、全体として不定形なデータ構造を意味的に関係づけてグラフデータベースに格納することで、D-ADD の実現性が高まると仮定した。特に D-Case そのもののデータ構造はグラフであり、主たる格納データである D-Case の更新は、グラフ構造の更新により計算することで、全体の構成管理を実現しようとするものである。そのため、各種文書も構造化された構成を持たせることで、D-Case、文書間の関連づけが容易になる。

D-ADD の主たる機能である合意記述であるが、ステークホルダーによる合意は、対象システムのライフサイクルの至る所で行われる。そのため、合意記述のデータ構造が時間的に変更され複雑化することが想定される。上記で説明した D-ADD に格納する対象システムの情報と同様に、合意記述のデータ構造もグラフ構造で保持することで、構造の時間変化に対応可能であると仮定した。合意記述と合意の対象となる各種データも、双方をグラフ構造で保持することで、たとえば、問題となる箇所の整合をデータ構造全体から発見するなどのグラフデータベースが得意とする能力を生

かしたD-ADDの機能設計が可能である。
<研究進捗状況> D-ADD の研究は、四半期毎の目標設定とその成果の確認から、段階的に進めた。四半期毎の結果を簡潔にまとめる。
1Q:「営業放送システム」(以下「営放システム」:放送局の基幹システム)のユースケースを考案し、D-ADD の対象システム監視機能を実現することで、D-ADD 全体のアーキテクチャの概要を掴んだ。1Q では、放送事故を防ぐというアシュアランスケースをD-Case で記述して、業務進行のチェックを対象データベースのログから判定するという機能を設計した。この設計により、領域のこれまでの研究であるモニターノード、D-Script などとの関連を、D-ADD 内部では D-ADD エンジンとして設計することで解決するのではないかとの感触を得ることが出来た。1Q の D-ADD エンジンは、D-ADD に格納済みのデータ群とモニターノードによって取り込まれた対象システムの状態データを照合させ、アシュアランスケースから導かれるルール(障害回避等)により処理し、D-Script に結果を返す機能として設計した。
2Q:D-ADDの主たる性能、格納情報である合意記述について設計を行い、試験的にではあるが、複数のステークホルダーで利用できる合意形成支援環境を構築した。我々はまずツゥールミンの論証分析を採用して、主張・反論を構成する情報を保持しつつ、ステークホルダー同士が議論し合意に至る機能を実装した。この結果、1Qの D-ADD エンジンと合意形成支援を考慮した D-ADD 全体の構成を見いだすことが出来た。
3Q:1Q、2Q の結果を考慮して、D-ADD と、主たる格納情報である D-Case との接続、またはD-Case ツールとの接続を検討した。研究の概要に述べたように、D-Case で記述されるアシュアランスケースは、対象システムに関する様々なデータ群と相互に関係を持っている。最低でも、D-Case エビデンスノードにはエビデンスとなる文書や合意記述などがリンクされていなければならない。各種文書と D-Case の相互関係を実現するために、各種文書から D-Case の部分木が作られる方式を考案した。この方式では、文書は文書リポジトリに構造的に格納され、D-Case情報は領域の研究成果である D-Case Weaver を改造して文書リポジトリに格納された文書情報との関連性を保持しつつ格納されるというプロトタイプシステムを開発した。
4Q:3Q の結果は、継続して検証する必要があるが、3Q にて、おおよそ研究の概要に掲げたテーマへの道筋が出来たと考え、それを検証するために、1Q+2Q+3Q を併せ持った H24 年度のD-ADD を 4Q プロトタイプシステムとして実現した。この 4Q プロトタイプシステムは、開発時のユースケースとして、1Q で用いた営放システムの放送事故を防ぐアシュアランスケースを発展させ、放送事故が起こってしまった場合を想定した。説明責任を果たすという DEOS プロセスにおける重要な機能の設計を行った。

＜研究成果＞
1. D-ADD の主たる機能である合意記述を合意形成支援環境として設計しプロトタイプシステムとして実現した。
2. D-ADDの主たる格納情報であるD-Caseを、関連する合意記述、各種文書と共にD-ADDに格

納する方式およびそのためのデータ構造を設計しプロトタイプシステムとして実現した。
3. DEOS プロセスを一巡させるために、1Q の D-ADD エンジンを拡張し、ルール設定、権限設定を機能追加して再設計した。1. 2. のプロトタイプシステムを結合した今年度の最終成果である D-ADD システムをプロトタイプとして実現した。

上記成果から当初の研究目標である、DEOS プロセスを実行するための機能要件が明らかになり、D-ADD の諸性能要件を明確にすると共に、時間と共に変化する情報を扱える D-ADD 実現に目処を付けた。D-ADD によって DEOS プロセスの重要な機能である説明責任を遂行する方法を研究開発仕様としてまとめ、来年度の目標が明確になった。

＜今後の見通し＞ 実用化を目指した D-ADD の研究開発は、11 月領域での最終報告時期と、最終翌年 3 月末までの時期と二段階に分けて目標策定ならびにスケジューリングを行う予定である。11 月の領域での最終報告時には、D-ADD によって DEOS プロセスを担当する他の研究チームの機能や研究成果を統合することが可能となり、DEOS プロセスそのものの設計や運用が柔軟になるように D-ADD が機能することを提示する。(DEOS プロセス自身のディペンダビリティも提示できなければならない)3 月末では、DEOS プロジェクトの出口戦略(e.g. コンソーシアム設立)に従って、一般企業が D-ADD、DEOS プロセスの利用価値として少なくともトライアルできる性能(安定性や、ユーザビリティを有していること)を実現出来ている必要がある。

(D) D-Case エビデンス管理機能の開発と実証実験 (主に恩田グループが担当)

＜D-Case 構成要素としての関連文書の管理機能の開発＞

D-Case で保証議論を構築しステークホルダー間でディペンダビリティについての合意を形成するためには、Evidence や Context となる文書を D-Case 内で適切に参照することが求められる。これらの文書は多数のステークホルダーが作成に関与し、ライフサイクルに合わせて頻繁に更新されるため、適切な管理、具体的には複数のステークホルダーがアクセスできる文書リポジトリへの登録や版管理などが必要となる。恩田グループでは、H23 年までに開発した D-Case 作成ツール「D-Case Editor」を拡張し、D-Case と文書リポジトリに登録され版管理されている文書との関連付けをおこなう機能を開発した。具体的には、D-Case 中の Evidence や Context に文書リポジトリ中の文書のある版への関連付けを作成する機能や、現在参照中の D-Case に関連付けられている文書が最新版かどうかを判別する機能、関連付けられている文書を参照する他の D-Case を列挙する機能などを開発した。これらの成果は DEOS プロジェクトメンバー内に公開され、プロジェクトメンバー内で有効性の検証をおこなっている。今後は、検証結果を元に改善をおこない、プロジェクト外への公開を目指す。

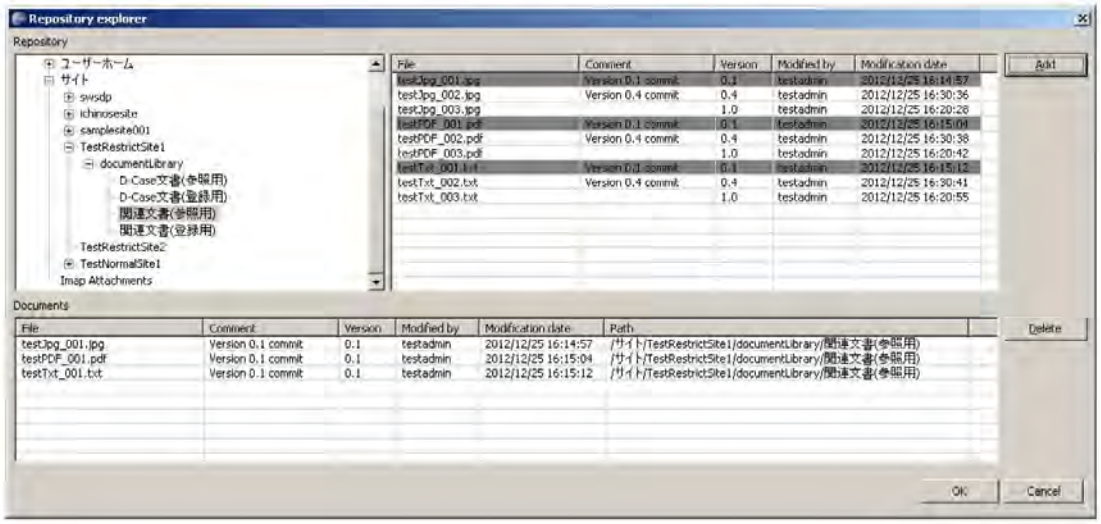

図4文書管理機能スナップショット

〈実証実験・ヒアリング等による有効性の検証＞

富士ゼロックスでは、若手技術者教育の一環として一般社団法人組込みシステム技術協会の主催する ET ロボコンに参加している。今年度開催された ET ロボコン 2012 に恩田グループの研究メンバーが参加し、コンテスト審査資料として D-Case を活用したモデルを提出した。本活動によって、D-Case を活用するためのノウハウを蓄積でき、研究メンバー以外のロボコン参加者に D-Case の利用方法を伝達することができた。また、プロジェクト外の第三者からの評価を受け、D-Case の記述粒度やその内容に関して適切かつ理解を促進するというコメントを得られた。さらに、本モデルが ET ロボコン 2012 における南関東地区大会・全国大会（チャンピョンシップ大会）において、最優秀モデル賞（エクセレント・モデル）を獲得し、D-Case の効果をプロジェクト外へアピールすることができた。今後は、富士ゼロックス社内で D-Case 活用に関する教育講座等を設置するなど、有効性を幅広く検証する機会を検討する。

§3. 成果発表等

(3－1) 原著論文発表

・論文詳細情報

A-1) Midori Sugaya, Hiroki Takamura, Youichi Ishiwata, Satoshi Kagami, Kimio Kuramitsu, Online Kernel Log Analysis for Robotics Application. Journal of Information Processing, 2012

A-2) Ide Masahiro, Kimio Kuramitsu. Just-in-time compiler for KonohaScript using LLVM. Journal of Information Processing Vol.20 No.4 1-8 (Oct. 2012) [DOI: 10.2197/ipsjjip.20.1]

B-1) Yutaka Matsuno, Shuichiro Yamamoto: A Framework for Dependability Consensus Building and In-Operation Assurance, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 4, Number 1 (2013) (ISSN: 2093-5382)

B-2) Yutaka Matsuno, Shuichiro Yamamoto: A New Method for Writing Assurance Cases. International Journal of Secure Software Engineering (IJSSE), Special Issue on Cybersecurity Scientific Validation (2013) (In press)

B-3) 中澤仁, 松野裕, 徳田英幸: D-Caseを用いたユビキタス・センサネットワーク管理ツール. 電子情報通信学会論文誌(和文 B) ユビキタス・センサネットワークを支えるシステム開発論文特集, J95-B No.11 pp. 1446-1460 (2012)

A-3) Takuma Wakamori. Masahiro Ide, Midori Sugaya, Kimio Kuramitsu. Reconfigurable Scripting Language with Programming Risk. Workshop on Open System Dependability 2012, in conjunction with ISSRE2012, 2012.

A-4) Motoki Yoan, Midori Sugaya, Kimio Kuramitsu. Converting Risk to Assurance Case, Workshop on Open System Dependability 2012, in conjunction with ISSRE2012, 2012.

A-5) 菅谷 みどり, 高村 博紀, 横手 靖彦, 倉光 君郎. DRE: フォルトモデルを考慮した障害回避の支援基盤の提案. 先進的計算基盤システムシンポジウム SACSIS 2012

A-6) 小野田 武朗, 菅谷 みどり, 倉光 君郎. Web技術文書からのFFI自動生成に関する実践. 情報処理学会ソフトウェア工学シンポジウム2012, 2012

A-7) 井出 真広, 志田 駿介, 倉光 君郎. LLVM を用いた静的型付きスクリプト言語 KonohaScript の Just-in-time コンパイラの設計と実装. 先進的計算基盤システムシンポジウム SACSIS 2012

A-8) 菅谷 みどり, 若森 拓馬, 倉光 君郎. 自動データ収集機能を備えたWeb ベースプログラミング学習システム情報処理学会 情報教育シンポジウム.Summer Symposium in Shizuoka 2012

A-9) 志田駿介, 菅谷 みどり, 倉光 君郎. 省メモリ環境におけるスクリプト処理系の開発. 情報処理学会組み込みシステムシンポジウム2012, 2012

A-10) Shinpei Nakata, Midori Sugaya, Kimio Kuramitsu. Fault Model of Foreign Function Interface across Different Domains. Fast Abstract, IEEE/IFIP Dependable System and Network 2012.

B-4) Yutaka Matsuno, Shuichiro Yamamoto: An Implementation of GSN Community Standard, ASSURE2013, in conjunction with ICSE 2013, San Francisco, May 2013 (accepted)

B-5) Shuichiro Yamamoto, Yutaka Matsuno: An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case, ASSURE2013, in conjunction with ICSE 2013, San Francisco, May 2013 (accepted)

B-6) Shota Takama, Vaise Patu, Yutaka Matsuno, Shuichiro Yamamoto: A Proposal on a Method for Reviewing Operation Manuals of Supercomputer (Short Paper), Proceedings of 2nd International Workshop on Open Systems Dependability, co-located with IEEE ISSRE 2012, Dallas (2012.11)

B-7) Vaise Patu, Yutaka Matsuno, Shuichiro Yamamoto. Application of D-Case to the data-upload flow diagram scenario of the Distributed E-Learning System called KISSEL(Short Paper), Proceedings of 2nd International Workshop on Open Systems Dependability, co-located with IEEE ISSRE 2012, Dallas (2012.11)

B-8) Kohei Tanaka, Yutaka Matsuno, Yoshihiro Nakabo, Seiko Shirasaka: Toward strategic development

of Hodoyoshi microsatellite using assurance cases, Proceedings of International Astronautical Federation (IAC 2012) (2012.9)

B-9) Yutaka Matsuno, Shuichiro Yamamoto: Toward Dynamic Assurance Cases, Proceedings of Tenth Conference on Knowledge-Based Software Engineering (JCKBSE 2012), pp.154-160 (2012.8)

B-10)田中康平、松野裕、中坊嘉宏、白坂成功、中須賀真一: アシュアランスケースにおける品質到達性とトレーサビリティを考慮した記述ルール提案と超小型衛星開発への適用評価、第 10 回クリティカルソフトウェアワークショップ (2012.9)

B-11) Shuichiro Yamamoto, Yutaka Matsuno: A review method based on a matrix interpretation of GSN, Proceedings of Tenth Conference on Knowledge-Based Software Engineering (JCKBSE 2012), pp.36-42 (2012.8)

B-12) Takuya Saruwatari, Takashi Hoshino, Shuichiro Yamamoto: Evaluation of an Assurance Case development method (d*). JCKBSE 2012: 72-80

B-13)Yutaka Matsuno, Shuichiro Yamamoto: Consensus Building and In-operation Assurance for Service Dependability, Proceedings of IFIP WG 8.4, 8.9/TC 5 International Cross-Domain Conference and Workshop on Availability, Reliability, and Security (CD-ARES), LNCS 7465, pp.639-653 (2012.8)

B-14)Shuichiro Yamamoto, Yutaka Matsuno: d* framework: Inter-Dependency Model for Dependability (Fast Abstract), Proceedings of IEEE Dependable Systems Network (DSN), 2 pages (2012.6)

B-15) Yutaka Matsuno, Kenji Taguchi, Yoshihiro Nakabo, Akira Ohata: Iterative and Simultaneous Development of Embedded Control Software and Dependability Cases for Consumer Devices, Proceedings of SICE Annual Conference 2012, Akita University (2012.8)

B-16) 伊東敦、松野裕: ET ロボコンを対象としたドメインからの D-Case による保証議論の構築, ソフトウエアシンポジウム、福井 (2012.6)

B-17) 山本修一郎、松野裕: システム継続性を保証するためのリスク分析手法の構築経験、ソフトウエアシンポジウム、福井 (2012.6)

(3－2) 知財出願

① 平成 24 年度特許出願件数(国内 1 件)

② CREST 研究期間累積件数(国内 4 件)