安全なシステム記述言語および高信頼 OS 記述言語

東京大学大学院情報理工学系研究科コンピュータ科学専攻 米澤　明憲
http://www.yl.is.s.u-tokyo.ac.jp/e-society

■ 研究発表

- 関口 龍郎. “C 言語のメモリモデルの安全な実装手法”, 日本ソフトウェア科学会第 7 回プログラミングおよび応用のシステムに関するワークショップ (SPA 2004) 論文集, 2004 年月 3 月 1 日～3 日, pp.113-127.
- 関口 龍郎. “C 言語のための現実的なポインタ解析”, 日本ソフトウェア科学会第 6 回プログラミングおよびプログラミング言語ワークショップ (PPL 2004) 論文集, 2004 年 3 月 11 日～13 日, pp. 52-63.
- Kohei Suenaga, Yutaka Oiwa, Eijiro Sumii and Akinori Yonezawa. The Interface Definition Language for Fail-Safe C. In Proceedings of the 2nd Mext-NSF-JSPS International Symposium on Software Security (ISSS 2003), June 2004. Lecture Notes in Computer Science, Volume 3233, pp.192-208, Springer-Verlag.
- Reynald Affeldt and Naoki Kobayashi. A Coq Library for Verification of Concurrent Programs, In Proceedings of the 4th International Workshop on Logical Frameworks and Meta-Languages (LFM 2004), Cork, Ireland, July 5 2004., pp.66-83, Electronic Notes in Theoretical Computer Science, Elsevier.
- Reynald Affeldt, Naoki Kobayashi, Akinori Yonezawa, Verification of Concurrent Programs using the Coq Proof Assistant: a Case Study, 2004 年並列／分散／協調処理に関する『青森』サマー・ワークショップ (SWoPP 青森 2004) , 11 pages, 2004, 青森市青森県, 2004 年 7 月 30 日～8 月 1 日.
- Reynald Affeldt and Naoki Kobayashi. Partial Order Reduction for Verification of Spatial Properties of Pi-Calculus Processes, In Proceedings of the 11th International Workshop on Expressiveness in Concurrency (EXPRESS 2004), London, UK, August 30, 2004, pp.113 - 127, 2004. Electronic Notes in Theoretical Computer Science, Elsevier.
- 古瀬 淳. フローグラフを使った extensional polymorphism のコンパイル, 日本ソフトウェア科学会第 21 回大会論文集, pp.286-290. 2004 年 9 月.
- Reynald Affeldt, Naoki Kobayashi and Akinori Yonezawa. Verification of Concurrent Programs using the Coq Proof Assistant: a Case Study, IPSJ Transactions on Programming, 2005, Vol. 46. No. SIG 1 (PRO 24) , pp.110-120 .
- 大岩 寛. Fail-Safe C の safe pointer 実装のオブジェクト指向言語のための拡張. 日本ソフトウェア科学会 第 7 回プログラミングおよびプログラミング言語ワークショップ (PPL 2005) 論文集, pp.246-260. 2005 年 3 月.
- Ste'phane Demri, Ranko Lazic' and David Nowak. On the freeze quantifier in Constraint LTL: decidability and complexity. In Proceedings of the 12th International Symposium on Temporal Representation and Reasoning (TIME 2005), 23-25 June 2005, Burlington, Vermont, USA. IEEE Computer Society, pp.113-121.
- Reynald Affeldt and Marti Nicolas. Encoding Separation Logic in Coq and Its Application. French/Japanese Joint Symposium on Computer Security. September 5 - 7, 2005. Keio University. 口頭発表.

- Jun Furuse. Information Flow Analysis and Type Systems for Secure C Language(VITC Project). French/Japanese Joint Symposium on Computer Security. September 5 - 7, 2005. Keio University. 口頭発表.
- Toshiyuki Maeda. A Type System for Memory-Secure Operating System Kernels. French/Japanese Joint Symposium on Computer Security. September 5 - 7, 2005. Keio University. 口頭発表.
- 古瀬 淳, 米澤 明憲. VITC: 対攻撃耐性コード生成コンパイラ. 日本ソフトウェア科学会第 22 回大会論文集, 5 pages. 2005 年 9 月.
- 前田俊行, 米澤明憲. 強く型付けされたオペレーティングシステム. 日本ソフトウェア科学会第 22 回大会論文集, 17 pages. 2005 年 9 月.
- Nicolas Marti, Reynald Affeldt and Akinori Yonezawa. Towards Formal Verification of Memory Properties using Separation Logic. 日本ソフトウェア科学会第 22 回大会論文集, 6 pages. 2005 年 9 月. 高橋奨励賞受賞.
- Ste'phane Demri and David Nowak. Reasoning about transfinite sequences (extended abstract). In Proceedings of the 3rd International Symposium on Automated Technology for Verification and Analysis (ATVA 2005), Taipei, Taiwan, October 4-7, 2005. Lecture Notes in Computer Science, Volume 3707, pp.248-262, Springer-Verlag.
- Toshiyuki Maeda and Akinori Yonezawa. Writing Practical Memory Management Code with a Strictly Typed Assembly Language. In Proceedings of the 3rd workshop on Semantics, Program Analysis, and Computing Environments for Memory Management (SPACE 2006). 2006, 14 pages.
- Nicolas Marti, Reynald Affeldt and Akinori Yonezawa. Verification of the Heap Manager of an Operating System using Separation Logic. In Proceedings of the 3rd workshop on Semantics, Program Analysis, and Computing Environments for Memory Management (SPACE 2006). 2006, pp.61-72.
- Nicolas Marti, Reynald Affeldt and Akinori Yonezawa. Tools and Experiments for Formal Verification of Operating Systems. 日本ソフトウェア科学会第 8 回プログラミングおよびプログラミング言語ワークショップ (PPL 2006) . ショートプレゼンテーション, 2006.
- Hiroshi Unno, Naoki Kobayashi. Combining Type-Based Analysis and Model Checking for Finding Counterexamples against Non-Interference. In Proceedings of the 1st ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS 2006), pp.17-26, 2006
- Nicolas Marti, Reynald Affeldt, Akinori Yonezawa. Model-checking of a Multi-threaded Operating System. 日本ソフトウェア科学会第 23 回大会論文集, 6 pages. 2006 年 9 月.
- Nicolas Marti, Reynald Affeldt, Akinori Yonezawa. Formal Verification of the Heap Manager of an Operating System using Separation Logic. In Proceedings of the 8th International Conference on Formal Engineering Methods (ICFEM 2006), 2006. Lecture Notes in Computer Science, Volume 4260, pp.400-419, Springer-Verlag.
- 古瀬 淳. VITC: 対攻撃耐性コード生成コンパイラ. 日本ソフトウェア科学会第 4 回ディペンダブルソフトウェアワークショップ (DSW06-2) , 10 pages, 2006 . Available from http://www.yl.is.s.u-tokyo.ac.jp/~furuse/vitc/papers/vitc-dsw062.pdf
- Jun Furuse, Dzung Dinh-Khac, Viet Ha Nguyen. Flow Sensitive Information Flow Analysis for C Programs. In Proceedings of Japan-Vietnam Workshop on Software Engineering (JVSE 2007), Vietnum, 2007. 7 pages. Available from http://www.yl.is.s.u-tokyo.ac.jp/~furuse/vitc/papers/vitc-jvse.pdf

- 古瀬 淳, 米澤 明憲. VITC: 対攻撃耐性コード生成コンパイラ. コンピュータソフトウェア vol. 25 no. 1 pp.180-185, 2008.
- Hiroshi Unno and Naoki Kobayashi. On-Demand Refinement of Dependent Types. To appear in Proceedings of the 9th International Symposium on Functional and Logic Programming (FLOPS 2008). April, 2008.
- 古瀬 淳. VITC: 情報流解析による高安全 C コンパイラ. 情報処理学会第 70 回全国大会論文集, 2008. 掲載予定
- 古瀬 淳, 米澤 明憲. 安全なシステム記述言語および高信頼 OS 記述言語～ VITC: 情報流解析による高安全 C コンパイラ. 情報処理学会誌『学と産の連携による基盤ソフトウエアの先進的開発』, 2008. 掲載予定
- Jun Furuse, Dzung Dinh-Khac, Viet Ha Nguyen. Information Flow Analysis for C-style Pointers and Casts. 投稿予定
- Jun Furuse and Ryozo Yamashita. Secure Information Flow for Resources. 投稿予定

■ 公開ソフトウェア

- 前田俊行: Kernel Mode Linux, 2003.
  URL: http://web.yl.is.s.u-tokyo.ac.jp/~tosh/kml/
  ユーザプログラムをカーネルモードで安全に実行させるための、型システムと OS 機構.
- Reynald Affeldt: applpi, 2004
  URL: http://www.yl.is.s.u-tokyo.ac.jp/~affeldt/applpi/
  並行プログラムを検証するための Coq ライブラリ
- 古瀬 淳: G'Caml version 3.09, 2004
  URL: http://www.yl.is.s.u-tokyo.ac.jp/~furuse/gcaml/
  実行時型情報を利用した多重定義が可能な関数型言語 O'Caml の拡張
- Toshiyuki Maeda: TALK: Typed Assembly Language for Kernel, 2005.
  URL: http://www.yl.is.s.u-tokyo.ac.jp/~tosh/talk
  型付アセンブリ言語の実装
- Toshiyuki Maeda: TOS: Typed Operating System, 2005.
  URL: http://www.yl.is.s.u-tokyo.ac.jp/~tosh/tos
  型付アセンブリ言語で書かれた OS カーネル
- Nicolas Marti and Reynald Affeldt: Seplog: Separation Logic in Coq, 2005.
  URL: http://savannah.nongnu.org/projects/seplog
  定理証明器 Coq 用 Separation logic ライブラリ
- 大岩 寛: Fail-Safe C [1], 2007.
  URL: https://staff.aist.go.jp/y.oiwa/FailSafeC/
  ANSI-C 規格完全準拠のメモリ安全 C 言語コンパイラ
- Jun Furuse: VITC, 2007.
  URL: http://www.yl.is.s.u-tokyo.ac.jp/e-society/vitc
  情報流解析による高安全 C コンパイラ

[1] 産業技術総合研究所情報セキュリティ研究センターが公開

■ 報道

- 攻撃されてもシステムを止めない C コンパイラの新たなアイデア. 日経バイト 2005 年 6 月号.
- 攻撃に耐えて動き続けるコードを生成するコンパイラー. 東大情報理工 ARA プログラム メールマガジン 第 53 号. 2005 年 6 月 22 日
- 「組み込みの安全性. 日経バイト 2005 年 7 月号 特集. (OS 用型付きアセンブリ言語 TALK に関する研究開発について掲載)

■ 受賞

- 関口 龍郎. 日本ソフトウェア科学会 第 10 回論文賞 2005 年度 (http://www.jssst.or.jp/admin/awards.html)
- Nicolas Marti. 日本ソフトウェア科学会 第 22 回大会 高橋奨励賞 2005 年度 (http://www.jssst.or.jp/admin/awards.html)

■ 人材養成

- 博士 4 名, 修士 3 名

■ 学位論文

- 大岩 寛, 安全な ANSI C コンパイラの実装手法. 博士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2004.
- Reynald Affeldt, Verification of Concurrent Programs using Proof Assistants. 博士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2004.
- Toshiyuki Maeda. Writing an Operating System with a Strictly Typed Assembly Language. 博士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2005.
- Hiroshi Unno. Combining Type-Based Analysis and Model Checking for Finding Counterexamples against Non-Interference. 修士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2005.
- Toshihiro Yoshino. A Framework Using a Common Language to Build Program Verifiers for Low-Level Language. 修士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2005.
- Nicolas Marti. Formal Verification of Low-Level Software. 博士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2007.
- Ryozo Yamashita. Information Flow Analysis for Resources. 修士論文, 東京大学大学院情報理工学系研究科コンピュータ科学専攻, 2007.