第1回セキュアシステムシンポジウム

2012年9月10日（月） 10:00～16:55
みらいCANホール（日本未来科学館 7F）

独立行政法人
産業技術総合研究所

第1回セキュアシステムシンポジウム

2012年9月10日（月）10:00～16:55
みらいCANホール（日本未来科学館7F）

9:30～	開場
10:00～10:20	開会挨拶 研究部門長　松井　俊浩
10:20～11:10	招待講演「情報セキュリティ技術開発の現状と産総研への期待」 三菱電機株式会社　松井　充
11:10～11:40	「制御システムセキュリティ研究グループの紹介」 制御システムセキュリティ研究グループ長　古原　和邦
11:40～13:20	ポスターセッション＆休憩
13:30～14:00	「スマホアプリのプライバシー問題の解決に向けて」 セキュアサービス研究グループ　高木　浩光
14:00～14:30	「ソフトウェア信頼性向上のための形式技法・開発支援ツールの研究」 高信頼ソフトウェア研究グループ長　大岩　寛
14:30～15:00	「FOTによるモデルベーステストと品質コントロール」 システムライフサイクル研究グループ　北村　崇師
15:15～15:45	「RISEC次世代セキュリティ研究グループにおける暗号技術の証明可能安全性への取り組み」 次世代セキュリティ研究グループ長　花岡　悟一郎
15:45～16:35	招待講演「Securing Google Chrome」 Google Inc. Ian Fette
16:35～16:50	セキュアシステム研究への期待 顧問　今井　秀樹
16:50～16:55	閉会の辞 副研究部門長　寶木　和夫

招待講演者紹介

三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部長　松井 充 氏

1987年　京都大学理学研究科修士課程数学専攻卒業, 三菱電機株式会社入社, 以降暗号技術・誤り訂正技術の研究開発に従事。
1993年　新暗号解読法「線形解読法」発表, 1994年 米国標準暗号（当時）DESの解読実験に成功。
1995年　ブロック暗号アルゴリズムMISTY発表。
1999年　欧州にて第三世代携帯電話(W-CDMA)標準暗号設計に従事。
2003年　市村産業賞本賞受賞。
2004年　全国発明表彰恩賜発明賞受賞。
現在　　三菱電機情報技術総合研究所情報セキュリティ技術部長, IACR理事, 情報処理学会理事, 情報処理学会フェロー

Google Inc. Google Chrome Team　Ian Fette　氏

Ian Fette is a senior product manager on the Google Chrome team. He joined the team in 2007, focused on security, browser infrastructure, and the team's implementation and development of new web standards. Currently, he focuses on performance, security, and networking. Prior to joining Google, Ian worked for the U.S. Government. Ian has degrees in Computer Science from the University of Michigan and Carnegie Mellon University.

セキュアシステムの研究

セキュアシステムシンポジウム開催にあたって

■ セキュアシステム研究部門長　松井俊浩　t.matsui@aist.go.jp

RISEC

講演のポイント

- **情報セキュリティとシステム検証の2研究センターの研究資産を承継して、新しくセキュアシステム研究部門が発足、つくばと関西で研究を実施**
- **サイバーセキュリティにシステムの信頼性やヒューマンファクタを加えた本格研究を推進**

講演の概要

ITの普及に伴い、コンピュータやネットワークから、クラウド、スマートフォン、組み込み機器、そしてそこにある大量の個人情報やビジネス機密がサイバーセキュリティや信頼性の脅威にさらされています。日々開発されるソフトウェアとその脆弱性を突く大量のマルウェアに対抗するには、個別の問題に対する具体的対処法や対策技術の研究開発にとどまらず、すべてのセキュリティの基盤となる強力な暗号技術やヒューマンファクタを織り込んだシステム設計/運用の方法、自律的にセキュリティ機能を増していくシステムなど、ゲームチェンジを促す基盤的な研究開発が必要です。システム検証やヒューマンファクタの研究者も得て、新技術の開発と同時に、政府のセキュリティ政策への貢献、セキュリティ評価技術の国際標準化作業への貢献などをも通じて、オールジャパンでのIT安全の確保と産業化に取り組みます。

大きく、４つの方向で研究を進めます。

1.ITサービスセキュリティ： スマフォやクラウドに潜む脆弱性や危険性への対策とともに制度やガイドによる防備

2.制御システムセキュリティ： 可用性を重要視される重要インフラの制御システムを守る(CSSC組合と協働)

3.安全なシステム開発： 形式検証やモデル検査によって、仕様から実装、運用までを系統的に扱う技術

4.次世代セキュリティ： 何が起こるかわからないセキュリティへの脅威に、特に暗号の側面で強化を図る

下図に示す実験装置を公開しています。また、これまでに開発してきた以下の技術：安全なCコンパイラ、HTTP相互認証、鍵の漏洩に強い認証法・鍵管理法、コンテンツ配信における著作権保護、ユーザの属性に応じて鍵が変化する関数暗号、仮想化技術を用いたマルウェア解析ツール、暗号デバイスの安全性評価、ヒューマンエラー抑止技術、抜けのないテストを生成するテスト設計支援ツール、長寿命製品の品質維持のための仕様書のリファクタリング、などの産業展開を図っていきます

RISEC関西

【公開実験装置】

↑ICチップセキュリティ解析装置

←組み込みシステムのモデル検査のための巨大状態数計算向き大容量メモリ計算機(関西)

RISECつくば

Securing Google Chrome

■ Invited Speaker : **Ian Fette**
ifette@google.com

■ Affiliation : Google Inc. Google Chrome Team

Point

- **Browsers are more complex, now exposing GPU and running native code.**
- **Attackers have increasingly more resources, including government support.**
- **We need new security mechanisms to make more possible while keeping users safe.**

Abstract

In this talk, I will discuss various mechanisms in place to protect Google Chrome users, from low-level techniques like sandboxing and process isolation, to higher level mitigations such as SSL certificate pinning, blacklist approaches, and in-browser detection of phishing attacks. Our users are the target of attacks every day, from wide-reaching malware campaigns to targeted attacks by nation states, all of which affect the design of the Chrome security model.

制御システムセキュリティ研究グループの紹介

■ 講演者： 古原 和邦
kobara_conf@m.aist.go.jp
■ 所属： セキュアシステム研究部門 制御システムセキュリティ研究グループ

RISEC

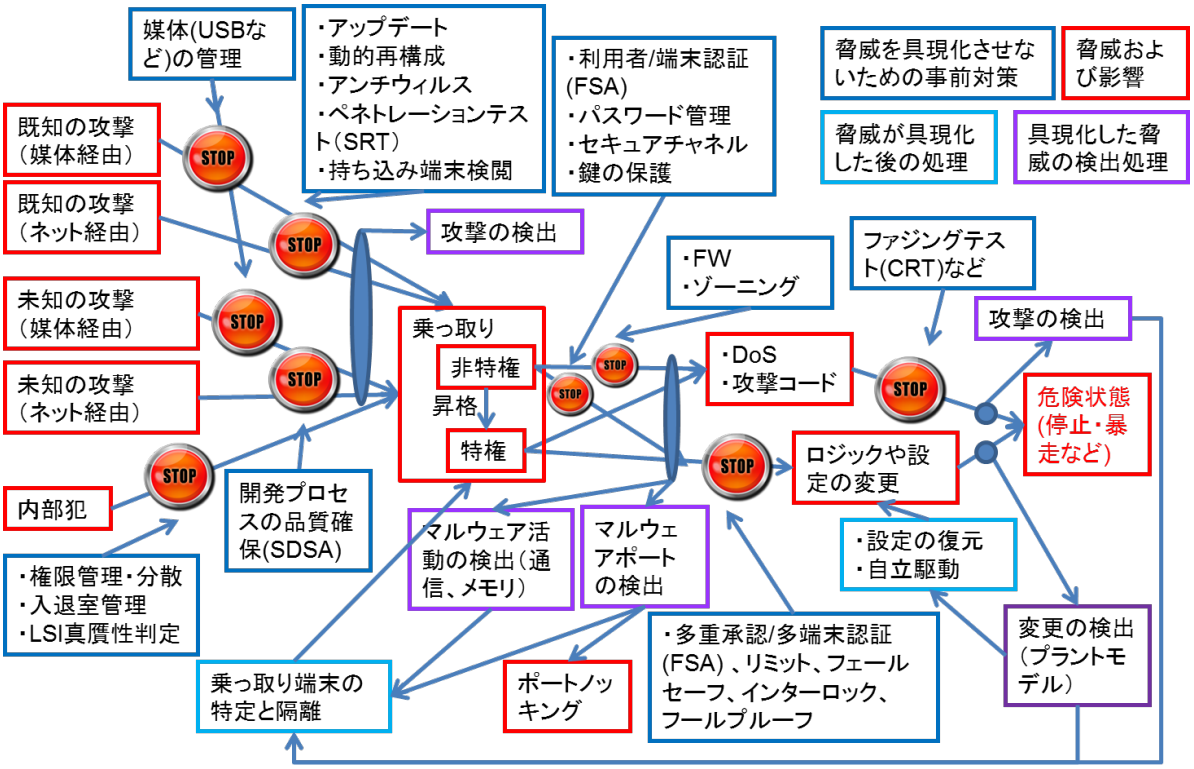
講演のポイント

- 制御システムとはどのような世界なのか
- どのような脅威があるのか
- どのような対策が可能なのか

講演の概要

制御システムは各種センサー、アクチュエーターおよびそれらのコントローラより構成され、また、それらの管理のために情報系ネットワークと疎あるいは蜜に接続される場合が多いです。装置の運用期間が長い上に、Windows OS やイーサーネットの導入など汎用化が進んでおり、従来インターネット上で問題となっていた攻撃を受けやすくなってきています。加えて、サイバー攻撃は不特定多数を狙った一般的なものから、特定の環境に特化した標的型へ変わってきており、隔離環境にある制御システムでさえその標的となり始めています。制御システムは、社会を支える重要インフラの構成要素であり、その防護が課題となっています。

セキュアシステム研究部門の制御システムセキュリティ研究グループでは、有効な対応策や評価手法に対する研究を行うため各種攻撃手法についてのノウハウを蓄積すると共に、脅威と対応策を網羅的に把握することで現場での状況や制約条件などに応じて最適な対応策を導出するための研究を行っています。また、現在欠けている技術や将来必要となる技術を実用化するための先進的な研究開発も行っています。本講演では、これらについてその背景や取り組みについて紹介します。



現在検討中の制御システムにおける脅威と対応策の関係図

スマホアプリのプライバシー問題の解決に向けて

■ 講演者： 高木 浩光
takagi.hiromitsu@aist.go.jp

■ 所属： セキュアシステム研究部門 セキュアサービス研究グループ

RISEC

講演のポイント

- **多様なスマートフォン用アプリの普及がもたらしたプライバシー上のリスクと社会不安の現状**
- **技術的手段のみによる解決の困難性と問題解決に向けての考え方を整理**
- **コンピュータ・プログラムに対する社会の信頼を確保するための制度上の解決策を提案**

講演の概要

昨年からのスマートフォン（スマホ）の急速な普及により、多様なスマホ用アプリが登場して利用が活発になりましたが、それに伴って、電話帳（連絡先）データやGPS位置情報など、利用者のプライバシーに関わる情報が、利用者の意図に反してサーバにアップロードされてしまうアプリの存在が次々と発覚するようになり、利用者の間に不安が広がっています。

この問題の解決が難しいのは、問題となるアプリが必ずしも悪意ある者によって作られているとは限らないところにあります。例えば、広告ビジネスのために利用者の嗜好を分析する目的であったり、利用者に便利なサービスを提供する目的で、それらの情報収集が行われる場合があります。そのような情報が送信されることを困ると感じるか否かは、個々の利用者の価値観によって異なると考えられます。そのため、一律に各アプリについて問題ある・ないの判別ができるわけではないところに難しさがあります。

セキュアサービス研究グループでは、総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」の「スマートフォンを経由した利用者情報の取扱いに関するWG」に対して、現状分析と問題解決に向けての意見を提出してきました。8月にはこの研究会の最終提言である「スマートフォン プライバシー イニシアティブ －利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－」が公表されており、当グループもこの提言を支持するところです。

この講演では、総務省研究会の提言を紹介しながら、当グループがこの課題についてどのように考えるか、スマホアプリの普及がもたらしたプライバシー上のリスクと社会不安の現状を外観した後、技術的手段のみによる解決の困難性と問題解決に向けての考え方を整理します。具体的には、歴史的経緯を振り返りながらWebとスマホアプリの違いについて比較し、「Permission確認方式」の限界について論じ、オプトイン方式による同意確認が必要であることを示します。

総務省研究会の提言は、各アプリ毎にプライバシーポリシーを掲げることを推奨し、アプリの処理内容の透明性を高めるべきとするものですが、これは法律に基づいたガイドラインではなく、その実効性をどう確保するかが課題となります。様々な施策が考えられるところですが、当グループは、平成16年経済産業省告示第235号「ソフトウエア等脆弱性関連情報取扱基準」に基づいた「情報セキュリティ早期警戒パートナーシップガイドライン」の運用を参考に、掲げるポリシーと実際の動作に齟齬があるアプリ等について、技術者からの通報を受け付け、当該アプリの作成・提供者と協議して、結果を公表する制度を提案します。

スマホ用のアプリに限らず、一般のコンピュータ・プログラムも対象にこのような仕組みを確立することで、コンピュータ・プログラムに対する社会の信頼を確保するのと同時に、自由なソフトウェア開発を促進し、業界の健全で持続可能な発展を促すことができるのではないかと考えています。

ソフトウェア信頼性向上のための形式技法・開発支援ツールの研究

■ 講演者： 大岩 寛
y.oiwa@aist.go.jp
■ 所属： セキュアシステム研究部門 高信頼ソフトウェア研究グループ

講演のポイント

- **高信頼ソフトウェアを、正確に、かつなるべく経済的に実現する技術を目指す**
- **得られたソフトウェア信頼性を他人に提示して「納得」して貰う技術も重要**
- **要求される信頼性レベルとコストに見合った技術を選択可能に**

講演の概要

ソフトウェアが制御機器の制御の重要な役割を占めることになってきており、ソフトウェアの信頼性はこれまで以上に強く求められる様になってきています。とくに、自動車や航空機など、「消費者機械」と呼ばれる消費者に直接の影響を与える機器の信頼性は、時に人命に直結するため極めて重要です。しかし、現在のソフトウェア実装では、時に様々な問題を引き起こしていることも事実です。たとえば、

- 2008年10月の Qantus 航空 72 便の急降下事故（負傷者115名）
- 2008年2月の湘南モノレールの停止不良・暴走事故（信号冒進・幸い死傷者なし）
- 1985年の医療機器の放射線過照射事故（最低5名死亡）と、繰り返される同様の事例（少なくとも9名死亡）

は、ソフトウェアの設計または実装の誤りが原因の一部であることが特定されています。また、2009年から2011年にアメリカにおいて問題となったプリウスのエンジン制御ソフトウェアの事象は、「ソフトウェアが安全であること、信頼できること」を他人に説明し、納得してもらうことの難しさを浮き彫りにしています。

一方で、現在のソフトウェア開発の現場では、要件分析からソフトウェアの最終テスト・出荷に至るまでの各段階において、「信頼性」の観点から見たときに、プロセス間の統合・連携が取れているとは必ずしも言えない状況があります。自然言語で書かれた仕様書は、たとえその仕様書を元に検査を行ったとしても、検査自体の信頼性を担保し、人に納得してもらうためには多くの追加コストが必要になります。

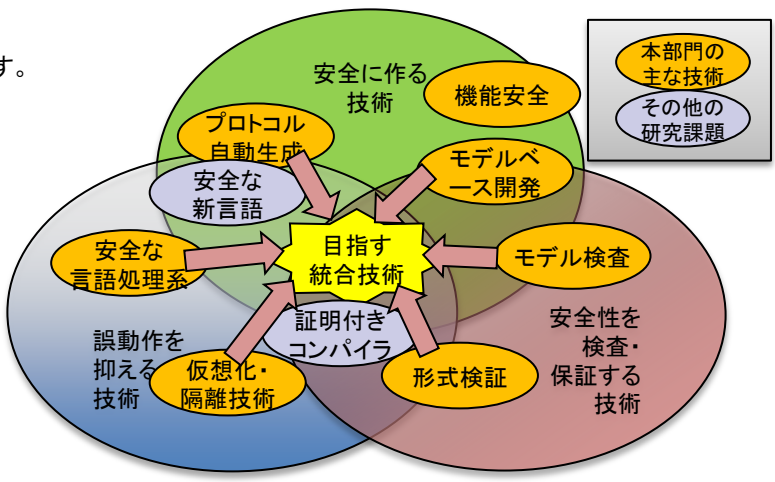
我々の研究グループでは、主に

- 高信頼ソフトウェアを確実に設計し作るための支援技術
- ソフトウェアが信頼できることを検査・保証し、本人及び他人に提示するための技術
- 完成したソフトウェアの誤動作を抑止し影響を低減する技術

の3つの観点から、高信頼ソフトウェアを、正確に、かつなるべく経済的に実現する技術の確立を目指しています。

とくに、現状のツールでしばしばありがちな、「ツールに手法が束縛される」状況をなるべく解消し、開発対象のシステムの信頼性要求やコスト要求に応じて適切な技術を取捨選択できる環境を、統合プロセスとして実現することを目指します。

講演では、これまで我々が開発した技術の概要や、これから目指す研究の方向性についてお話しします。技術の詳細については、各技術のポスター発表も合わせてお聞き頂けると幸いです。



RISEC次世代セキュリティ研究グループにおける暗号技術の証明可能安全性への取り組み

■ 講演者： 花岡 悟一郎
hanaoka-goichiro@aist.go.jp

■ 所属： 次世代セキュリティ研究グループ

講演のポイント

- **安全な情報システムを構築における、証明可能安全な暗号技術の必要性。証明可能安全でない技術を利用する場合の具体的な危険性**
- **証明可能安全な暗号技術の設計やその基盤理論に関する本グループの取り組み**

講演の概要

暗号理論分野における証明可能安全性とは、安全性評価の対象となる暗号時術の安全性を、なんらかの妥当な仮定の下、数学的に保証する安全性の概念である。そのような安全性を持つ暗号技術は、安全性の根拠となる仮定が崩れない限り、絶対に安全性が損なわれることがないため、非常に有用である。実際、十分に安全であるものと信頼される情報システムを構築するためには、そこで利用される暗号技術が証明可能安全であることが必須となっている。また、過去において、証明可能安全な暗号技術を利用しなかったために、後に深刻な脆弱性を指摘された情報システムも多数存在している。しかしながら、証明可能安全性をもつ暗号技術の設計や利用においては、極めて深い専門的知見が必要となるため取り扱いは必ずしも容易ではない。

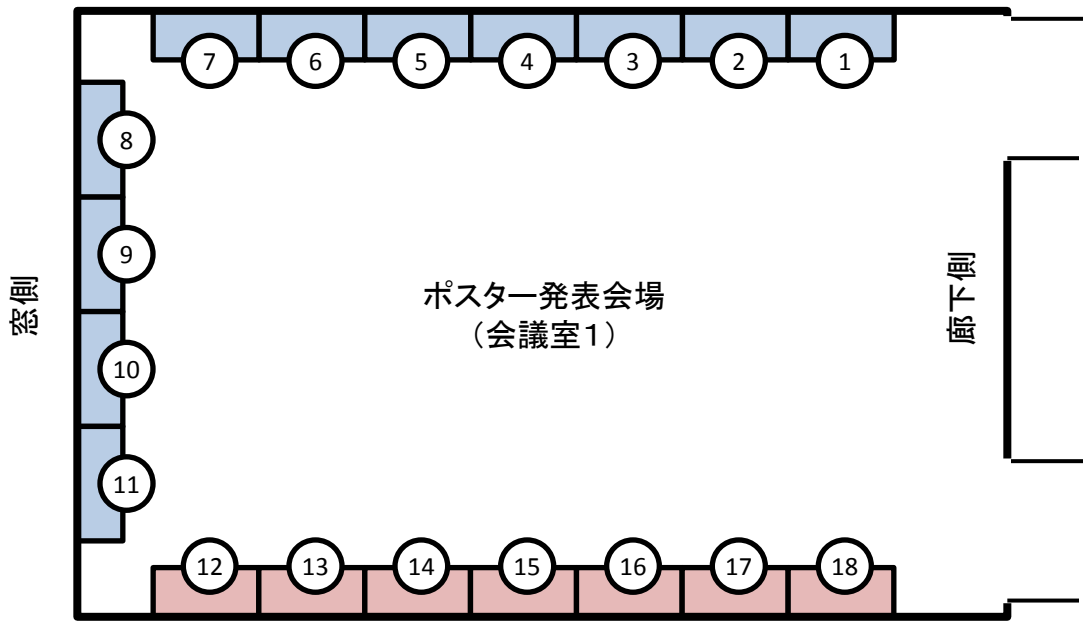
そこで、本研究グループにおいては、証明可能安全な暗号技術についての理論研究を集中的に行い、それらに関する最先端の知見を蓄積し、また、産総研内外の機関と連携することでそのような知見を実際のシステム開発に入力することで産業界への展開を図っている。そのための取り組みとして、公開鍵暗号、電子署名、関数暗号、放送暗号、時限暗号、準同型暗号、IDベース暗号、属性ベース暗号、代理人再暗号化暗号、フォワード安全暗号、鍵隔離暗号、量子暗号、耐量子計算機暗号、ゼロ知識証明、秘匿計算、否認可能認証、匿名認証、グループ署名、…などといった幅広い暗号技術に対して、証明可能安全性に関する理論的研究を行い、また、それらの成果を著名な国際会議や英文査読誌などを通じて発表していくことで、それらに関する知見を蓄積していること、さらに、そのような知見を高いレベルで活用できることを広く発信していく方針をとっている。

特に、本年度においては、現時点ですでに、暗号理論分野で最も権威ある学術組織である国際暗号研究学会（IACR）主催の国際会議であるCRYPTO 2012, ASIACRYPT 2012, PKC 2012をはじめ、その他にもSCN 2012, Pairing 2012といった著名な国際会議や、情報理論分野において最も権威ある英文査読誌であるIEEE Trans. on Information Theoryなどに、本研究グループからの成果が採録されている。なお、PKC 2012においては本研究グループから5件の論文が採録されているが、同会議全体の採録件数が41件（全投稿数は188件・採録率21．8%）、国内からは8件となっている。

上記のような活動により蓄積された知見は、産総研生命情報工学研究センターとの連携によるプライバシ保護化合物データ検索技術の開発や、NHK放送技術研究所との連携による不特定多数受信者向けコンテンツ配信技術の開発に活用されている。また、それらの知見に基づき、電子政府推奨暗号の安全性評価・監視を行うCRYPTRECプロジェクトや内閣官房情報セキュリティ研究センター（NISC）などにも貢献がなされている。

ポスターセッション

2012年9月10日（月）11:40～13:20
みらいCANホール（日本未来科学館7F 会議室1）



信頼性、安全性

① テスト指向仕様記述言語 SENS とテスト自動生成ツール
西原、崔、Nguyen、安藤

② 「Feature指向テスト（FOT）」による品質コントロール
北村、大崎、Artho

③ 止まらないマイコン FUJIMI
山形、早水

④ 安全設計の方法論
ー機能安全規格とトレーサビリティと安全分析
秋葉、シング、相馬、田口、竹内、矢田部

⑤ Open Systems Dependability
木下、武山、湯浅、木藤、平井

⑥ 形式仕様に基づくプロトコル実装の自動テスト
大岩、須崎、田中（哲）、飯島、八木

⑦ ソフトウェアのソースコードの形式検証
Affeldt、Marti

⑧ 並行システムの解析ツール ～複雑な並行処理の可視化～
磯部、大岩、高橋、田中（純）

⑨ セキュアなサービスに向けて
～バランスのとれた安全性・信頼性の実現～
渡辺、田沼、高木、中田、萩原、辛、山口

⑩ ヒューマンエラー対策技術
中田

⑪ 誤り訂正符号
～情報の信頼性向上を目指す数理科学的取り組み～
萩原

セキュリティ

⑫ HTTP 相互認証プロトコルとその標準化
大岩、高木、渡辺

⑬ ハードウェアの安全性評価技術と偽造防止技術
川村、片下、堀、坂根、姜

⑭ 制御システム高セキュア化の取り組み
高橋、古原、戸田、瀬河、海老原、須崎、渡辺、高木、山口

⑮ 破られる暗号
花岡、Schuldt、Mihaljevic、縫田、松田、今福

⑯ 破られない暗号
松田、Schuldt、花岡、縫田、Mihaljevic、今福

⑰ 不特定多数受信者向け暗号技術
縫田、花岡、Attrapadung、伍

⑱ 検索内容とデータベースの情報を相互に秘匿するデータ検索技術
縫田、花岡、Schuldt、松田

テスト指向仕様記述言語 SENS と テスト自動生成ツール

■ 研究担当者: 西原秀明 /崔　銀惠 / NGUYEN Tang / 安藤崇央
h.nishihara@aist.go.jp
■ 所属: 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

RISEC

研究のポイント

- **Formal Model Based Test－属人性を下げて工程全体の質を上げる、体系的なテスト設計**
- **システムのモデルを制約で記述するテスト指向仕様記述言語 SENS**
- **SAT ソルバを用いて制約をみたすモデルの振る舞いを高速に探索**

研究のねらい

組込みシステム開発のテスト工程では、技術者が経験を基に個々のテストケースを作成し、実機での振る舞いを確認する、というスタイルが多くとられています。しかし近年組込みシステムが複雑化し、属人性の強い従来の手法では十分にテストを行うことができません。本研究では、形式モデルを扱うことで個々の技術者に依存しないテストケースの生成を目指します。形式的に記述された仕様からモデルの可能な振る舞い全てを計算し、仕様の解釈のブレや振る舞いの見落としを防ぎます。

研究内容

組込みシステムの仕様を形式的に記述する言語 SENS を設計しました。SENS は制約として仕様を記述する独特な記述体系を持ち、システムの機能の詳細が決まっていない開発初期でも形式仕様として完結した記述を得ることができます。またテスト生成の際に採用する値を変数ごとに指定でき、特にテストしたい振る舞いなどテスト仕様の意図を SENS 記述に反映することができます。

SENS 処理系は SENS で記述された仕様を満たす状態遷移の全てを SAT ソルバ(制約解消ツール)を用いて高速に求めます。更に到達可能状態の確認、遷移シーケンスの生成など、仕様の改良や振る舞いの確認に有用な情報を生成する機能を備えています。

連携可能な技術・知財

- 制約を用いた形式仕様記述、モデリング
- SAT ソルバを用いた形式モデルの解析
- 特許出願情報:テスト仕様生成装置、テスト仕様生成方法、およびプログラム(特願2011-060199)

本研究はダイキン工業、京都工芸繊維大学との共同研究として実施されています。

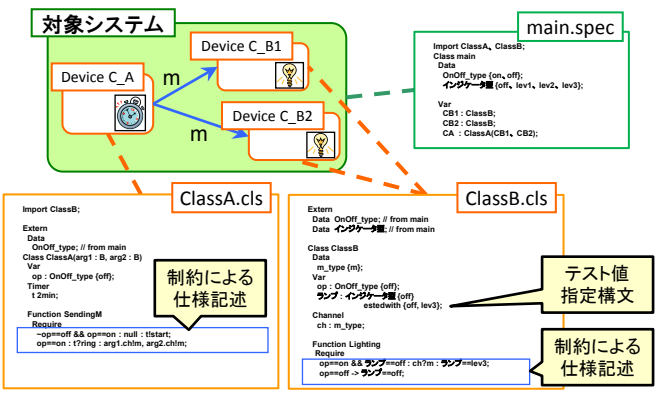


図1:SENS による仕様記述

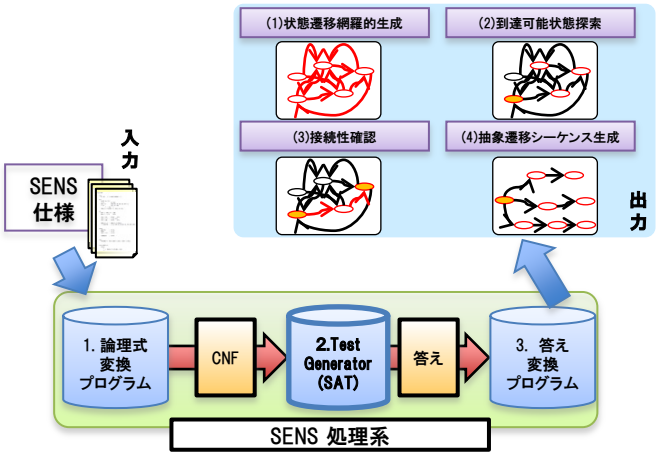


図2:SENS 処理系の機能

「Feature 指向テスト」による品質コントロール

Feature Oriented Testing (FOT)

■ 研究担当者：北村崇師、大崎人士、Cyrille Artho
t.kitamura@aist.go.jp

■ 所属：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

RISEC

研究のポイント

- **モデルによるテスト設計・保守、自動テスト**
- **「費用 v.s. 効果」平衡機能による、動的な品質コントロールの実現**
- **ISO26262 等、安全規格対応サポート**

研究のねらい

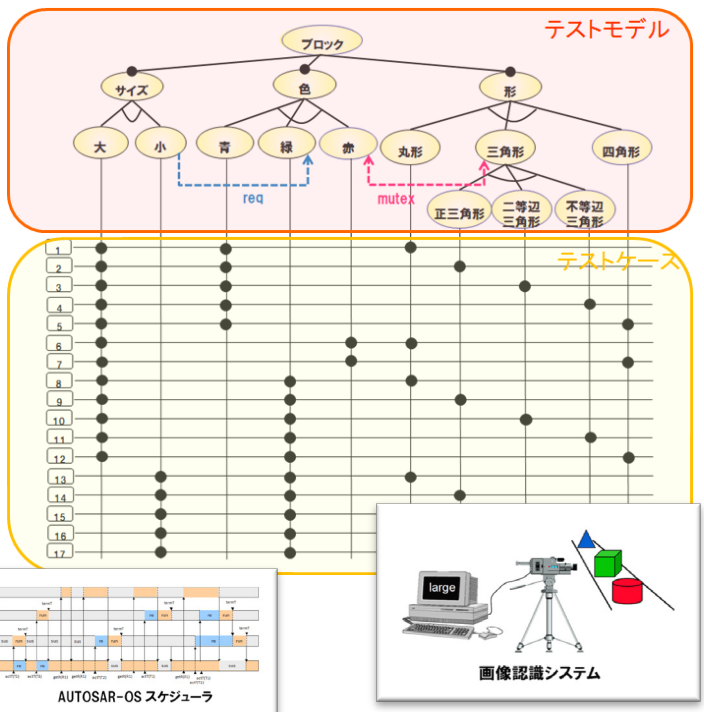
ソフトウェアが社会の基盤になるにつれ、その品質確保のための検証をいかに実施するは社会的な課題となっています。ソフトウェア検証に唯一の万能な方法はありません。また、数ある検証の科学的手法は、その技術の難易度や導入にかかるコスト等のため、産業界での普及は限定的です。我々は FOT（Feature Oriented Testing）と呼ぶテスト技法を研究開発しています。FOT では、ロジックツリーを用いてテスト設計を行い、そこからテストケース生成を自動化します。ロジックツリーの図式モデルは、システムのトップダウンな分析を通じたテスト設計を支援します。さらにそのモデルを操作し、コストに応じてテストケース量を動的に調整する、「費用 v.s. 効果」平衡機能による、品質コントロールを実現します。

研究内容

FOTとは？（画像認識システムのテストを事例に）

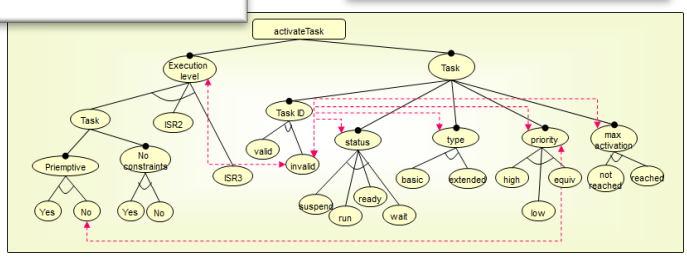
ベルトコンベア上を流れる様々なブロックの大きさを判定する画像認識システムのテストケースを作成せよ！

- 独自拡張した論理木を用いてテストケース設計
- 設計よりテストケースを自動生成
- コストに応じたテストケース量の調整



連携可能な技術・知財

- ソフトウェア品質の評価
- 学会発表：5th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation: ISoLA2012
- FOTツールの開発



止まらないマイコン
FUJIMI

■ 研究担当者：山形賴之/早水公二
yoriyuki.yamagata@aist.go.jp
■ 所属： 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

RISEC

研究のポイント

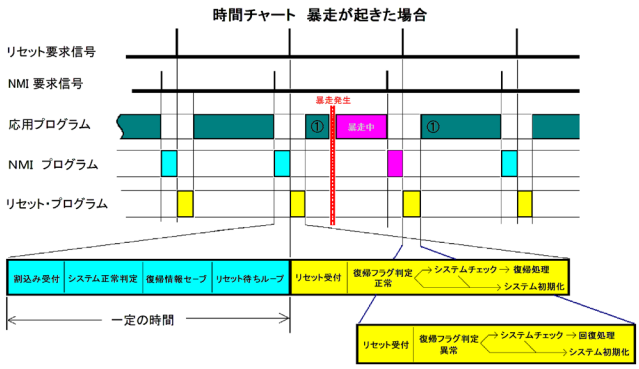
- 電気ノイズ等で誤動作しやすい組み込み機器や遠隔に設置されメンテの困難な機器の信頼性向上
- 定期的なシステムの内部状態保存動作とCPUリセットにより、誤動作直前の状態に瞬時に復帰
- アルゴリズムの網羅検証により信頼性を担保

研究のねらい

主に電気的ノイズの多い環境で作動する機器、遠隔地に設置される機器を対象に、障害耐性マイコンを導入し、機器の信頼性向上、メンテナンスコストの低減を目指す。これまで障害耐性マイコンは障害耐性をコアの多重化により実現してきた。しかし、マルチコアはコストの増加につながる他、多重化では繰り返し起きる障害には対処できない。本研究では、定期的にCPUの状態を保存した上、CPUコアをリセットすることにより、CPUを異常から瞬時に復帰させるシングルコア障害耐性マイコンFujimiを対象に、モデル検査技術を適応する。これにより、Fujimi自体の信頼性の確保とともに、動作要件を明確化しFujimiの導入を促進する。

研究内容

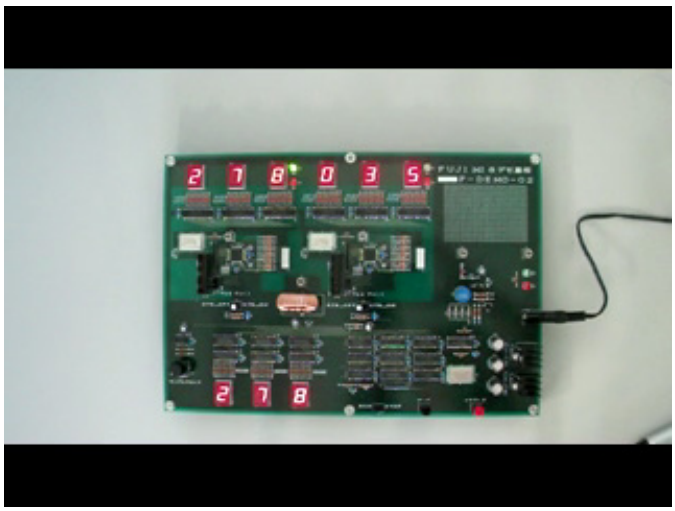
Fujimiはタイマーにより定期的に割り込みとリセットを生成するハードウェア部分と、割り込みおよびリセットを処理するソフトウェア部分が協調して動作する。本研究では、システム全体の仕様書をSMVによりモデル化し、暴走からの復帰可能性等を検証している。これまでの検証の結果、動作条件を満たしているにも関わらず、再起動してしまう例を見出した。今後、Fujimi上で動作するOSの部分検証や、Fujimi上でのプログラミング規約の検討などを行う予定である。



連携可能な技術・知財

- 仕様書からのモデル抽出技術
- モデルを用いたシミュレーション技術
- モデルにたいする網羅的検査技術
- 発見した不具合の解析技術

謝辞：本研究は、株式会社エルイーテックおよびシステム・コンサルタンツ株式会社との共同で実施されている。



安全設計の方法論
ー機能安全規格とトレーサビリティと安全分析

■ 研究担当者： 秋葉 澄孝 、シング クムドビラハム、相馬 大輔、田口 研治、竹内 泉、矢田部 俊介

■ 所属： 高信頼ソフトウェア研究グループ 、システムライフサイクル研究グループ

研究のポイント

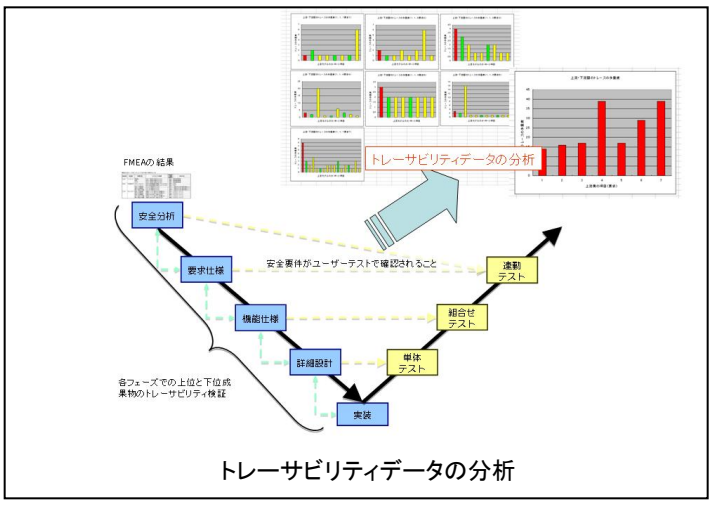
- 鉄道などの高信頼性を求められるシステムの開発において、設計品質を保証するためのシステム開発技術方法論を確立する
- 機能安全性に関する国際規格の認証プロセスを分析し、製品認証作業をやりやすくする

研究のねらい

- 公共交通会社との新システム導入に関する共同研究において、記述すべきシステムの抽象度等に応じた適切な設計方法論を助言し、仕様案の作成支援と内容確認を行い、また安全基準の策定の助言を行う。また、そのプロセスの分析を通じ、安全性を保障するシステム技術開発方法論を確立する。
- 安全性を漏れなく分析するための手法を調査・選択し、それを用いて実際のテスト工程を分析する。また、その実例の分析を通じ、製品の安全性を保障する手法を確立する。
- 安全分析などから得られた要件が過不足なく実装、テストされていることを確認するトレーサビリティ確保と、そのトレーサビリティデータを用いた品質向上のためのメトリクスの作成。

研究内容

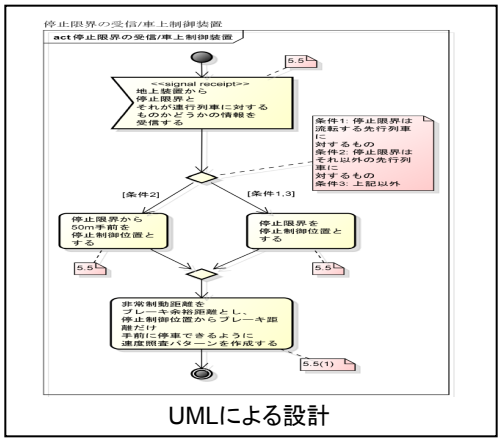
- 前年度は、適切な設計方法論としてUMLを選択し、仕様書について合計30枚のUML図を作成し、46カ所の問題点を指摘した。また仕様書中24カ所の暗黙知に関連する部分のリストアップなどを通じ、仕様案作成作業を支援した。今年度は、製品の安全基準の確立と国際規格認証プロセスの分析を行う。また、SafeMLなどの設計ツールの適応性実証実験を行う。
- 実際の開発で作成されたドキュメントに対しツールを用いトレーサビリティを確保し、漏れぬけなど使用の不備を指摘した。
- ひとつのトレーサビリティ対象要素に対する関連がいくつあるか（多重度）というメトリクスを作成しツールとして実装した。これにより品質が問題となりえる箇所を指摘した。今後は、新しいメトリクスを検討しそのツール化を行う。



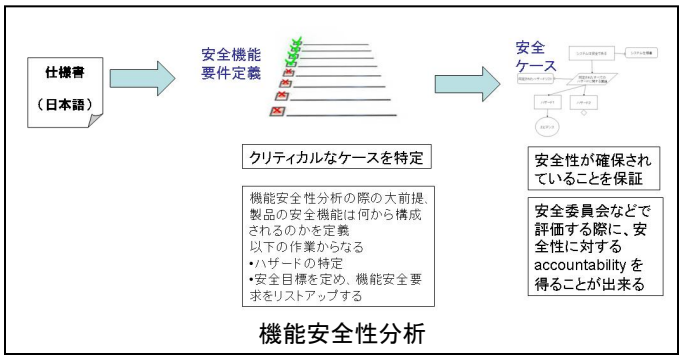
トレーサビリティデータの分析

連携可能な技術・知財

- 国際規格認証のモデル化
- 要求管理ツール
- プロダクトライン（派生）開発



UMLによる設計



機能安全性分析

Open Systems Dependability

■ 研究担当者: 木下　佳樹、武山　誠、湯浅　能史、木藤　浩之、平井　誠
kinoshita.yoshiki@aist.go.jp
■ 所属: セキュアシステム研究部門

RISEC

研究のポイント

- **変化し続けるシステムのサービスレベルやセキュリティを継続的に確保するプロセス**
- **上記を規定し、評価するための国際標準化および規格化活動**
- **上記システムやプロセスの妥当性論証を支援するツールおよびガイドラインの実証実験**

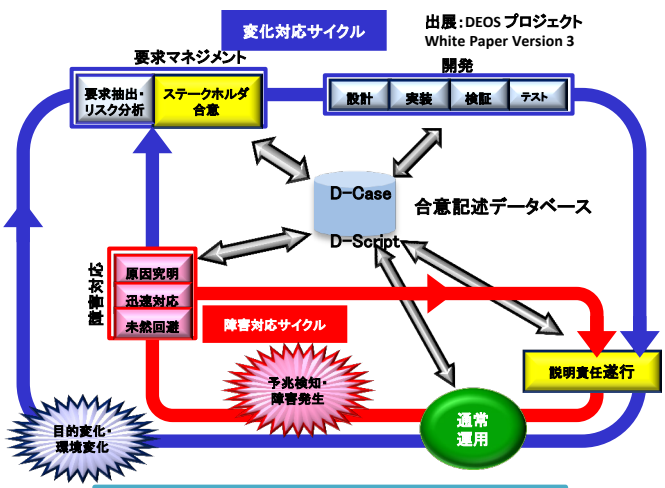
研究のねらい

現代のシステムは、環境に応じて変化し続けなければならない・複雑すぎて誰も全容を掴みきれないといった“オープンさ”をもちます。オープンさを無くそうとする従来型の努力だけでは、コスト相応の安全性や信頼性、「想定外」が起きた時のサービス継続性を確保できません。これらを、オープンシステムディペンダビリティ(OSD)という新たな統一的視点でとらえ、システムライフサイクル全体を継続的にマネジメントするプロセスで確保することをねらいます。軸となる関係者間合意の形成・妥当性確認の支援技術開発、ガイドラインの実証実験、OSDの概念・手段を産業界の「当たり前」にする国際標準化活動等を行っています。

研究内容

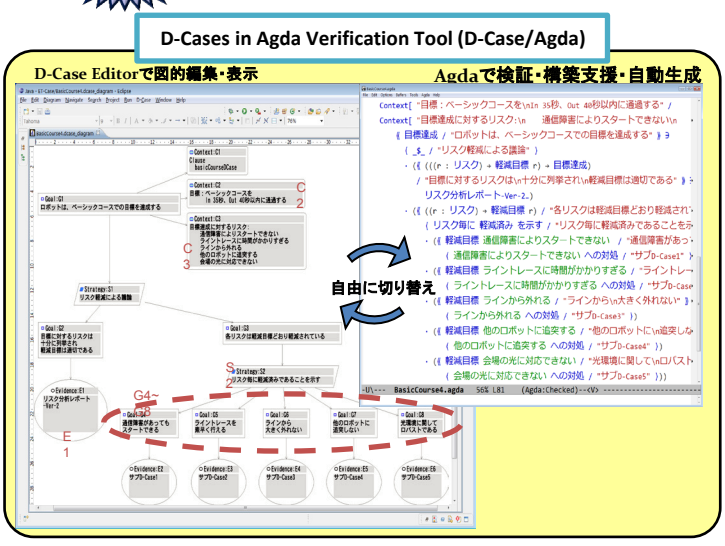
システム・ライフサイクルにおいて、各アクティビティが妥当になされたかを分析・論証し、D-Case(アシュランスケース)に記述します。Agda言語を用いて記述することにより、論理的に一貫した記述作業を支援し、機械的な確認が可能になります。また、図的表現との相互変換で、ステークホルダ間の合意形成を支援します。

OSDの効果的実現には、多くの関係者が概念と手段を共有し協力することが必要で、ISO, IEC, OMG 等の国際標準化団体において、共有の核となる新規格策定(OSDに必要なシステム・ライフサイクルに対する要求、アシュランスケース記述言語)と、OSDの視点を既存関連規格に導入する改定に向けて活動中です。



連携可能な技術・知財

- 本手法を用いた実証実験、ツールの提供
- 関連規格:SO/IEC 15026 Systems and software engineering - Systems and software assurance
  IEC 60300-1 DEPENDABILITY MANAGEMENT ? Part 1: Guidance for management and application
  OMG Structured Assurance Case Metamodel (SACM)
- 特許:特願2011-193452、「整合性検査装置、整合性検査方法、及びプログラム」(H23/9/6出願)
- 知財管理番号H24PRO-1369(H24/03/19)　D-Cases in Agda Verification Tool (D-Case/Agda)
- 本研究は、JST CREST研究領域DEOS受託研究「利用者指向ディペンダビリティの研究」の一環です。



形式仕様に基づくプロトコル実装の自動テスト

■ 研究担当者：大岩寛、須崎有康、田中哲、飯島賢吾、八木豊志樹
y.oiwa@aist.go.jp
■ 所属： セキュアシステム研究部門高信頼ソフトウェア研究グループ

研究のポイント

- **プロトコル実装の正当性検査の信頼性を向上**
- **形式化（機械化）した仕様書により検査ソフトを全自動で生成**
- **仮想マシンのスナップショット/ロールバック機能によるブラックボックステストの自動化**

研究のねらい

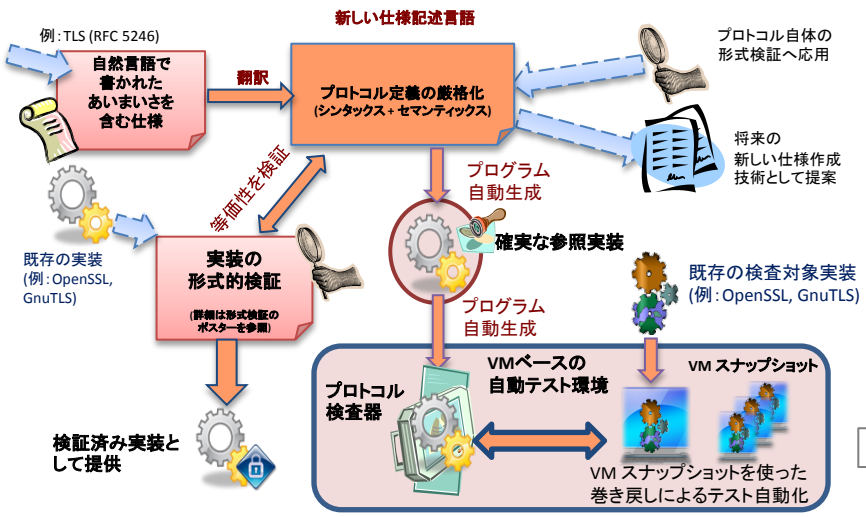
Webで暗号化通信に使われているTLS（SSL）など、インターネット標準のプロトコルは現実の実装において必ずしも仕様通りに反映されていない場合が多く、その実装の誤りが安全性の脆弱性に繋がるケースが複数見受けられています。また、仕様書自体にも曖昧さがある場合も多く、このような脆弱性は特定や修正が困難です。本プロジェクトではこの問題に対して、形式的手法による通信プロトコルの規格の記述を元に、その実装の様々な安全性評価・検証を統一的に扱うことのできる手法と、それに基づいた網羅的なブラックボックステストを実現し、実装の安全性と、安全性検査自体の信頼性を担保します。

研究内容

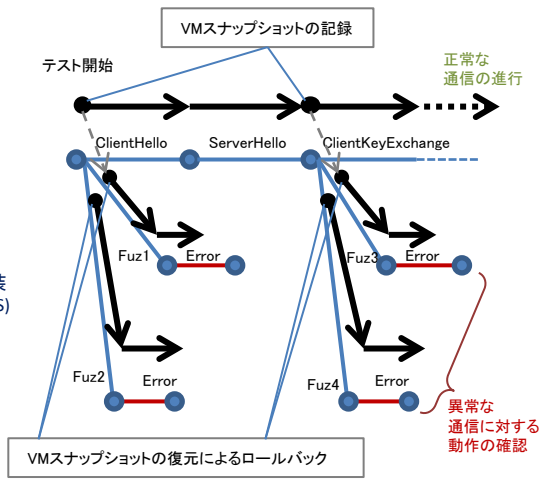
- 仕様記述の見直し（具体化）による仕様の曖昧さの排除
- 仕様記述からの自動生成により、原理的に「誤り」を含まない参照実装を提供
- 更に、プロトコル検査器も自動生成することで、安全性検査の信頼性も担保
- 仮想マシン (VM) およびスナップショットとの組み合わせで、既存の実装に対して網羅的なブラックボックステストを実現

連携可能な技術・知財

- 厳密性と理解の容易さを両立した新たなプロトコル仕様記述言語
- 仕様書に基づく厳密な動作確認用の参照実装
- Nested VM (KVM+QEMU) を使ったVMスナップショット・自在なロールバック制御技術



プロジェクト全体図



TLSプロトコルに対するVMスナップショットを用いた効率的なファジングテスト

独立行政法人 産業技術総合研究所

ソフトウェアのソースコードの形式検証

■ 研究担当者： AFFELDT Reynald (アフェルト・レナルド), MARTI Nicolas (マーティ・ニコラ)
reynald.affeldt@aist.go.jp

■ 所属： セキュアシステム研究部門・高信頼ソフトウェア研究グループ

RISEC

研究のポイント

- **ソフトウェアの安全性を機械的かつ厳密に検証**
- **検証結果として、第三者により確認可能な安全性証明を出力可能**
- **国際規格における最も厳密な評価保証レベルへの対応を目指す**

研究のねらい

組込みソフトウェアなどのクリティカルな部分

ソースコードレベル　　安全性, 性能

検証例
- ICカード向けの暗号プログラムの安全性の証明 [1]
- 符号付き多倍長整数処理の関数のライブラリの形式検証 [2]
- 通信プロトコルの実装 図3

研究内容

証明理論に基づく検証基盤の構築: 図2

現実的なプログラミング言語の厳密なモデル
(ICカード用のアセンブリ言語,
C言語のサブセット—アラインメントやパディングなどを含む)

論理的推論のための形式的ツール
(ポインター操作のための定理群, 詳細化のための疑似コード,
自動検証ツール, 検証済みコンパイラ)

Coq　代表的な定理証明支援系 Coq を使用
(フランス INRIA により 1985 年より開発, `http://coq.inria.fr`)

定理証明支援系
- 数学的なプログラミング言語(型付き) 図1
- 機械的理論的な推論(帰納法など)
- 具体的な証明オブジェクトの発行(型付きプログラム)

連携可能な技術・知財

- 組込みソフトウェアへの応用
- Seplog: A Library for Formal Verification of Low-level Programs
(産総研知財管理番号H22PRO-1175)
`http://staff.aist.go.jp/reynald.affeldt/coqdev`
- 参考文献:

[1] R. Affeldt, D. Nowak, K. Yamada. Certifying Assembly with Formal Cryptographic Proofs: the Case of BBS. *Science of Computer Programming*, 77(10-11):1058-1074, 2012. Elsevier

[2] R. Affeldt. On Construction of a Library of Formally Verified Low-level Arithmetic Functions. 27th ACM SIGAPP Symposium On Applied Computing, (2):1326-1331, 2012.

図1 定理証明支援系によるワークフロー

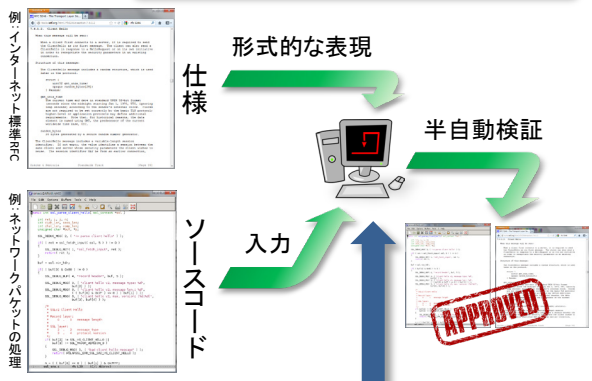
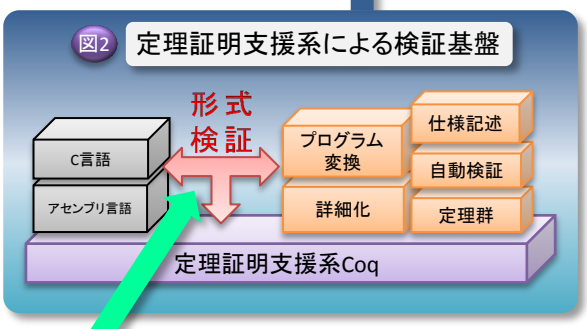


図2 定理証明支援系による検証基盤



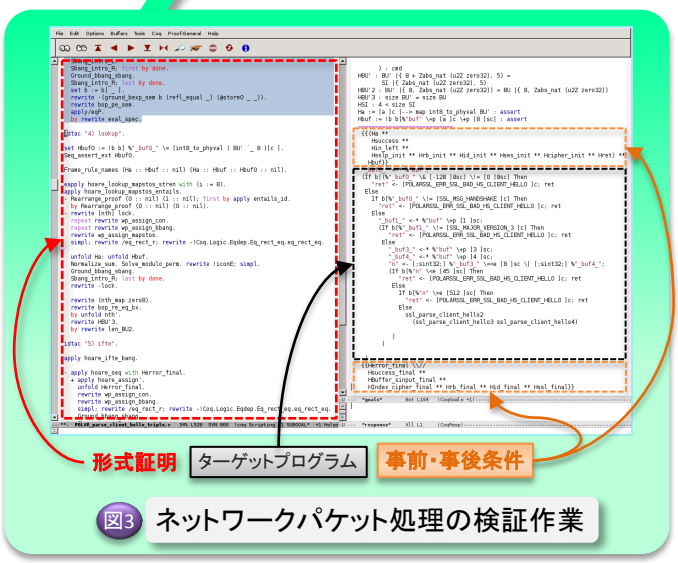


図3 ネットワークパケット処理の検証作業

並行システムの解析ツール
～複雑な並行処理の可視化～

■ 研究担当者：磯部祥尚*1／大岩寛*1／高橋孝一*2／田中純*3
y-isobe@aist.go.jp

■ 所属：セキュアシステム研究部門 *1 高信頼ソフトウェア研究グループ／*2 制御システムセキュリティ研究グループ／*3 イノベーション推進本部 ベンチャー開発部

RISEC

研究のポイント

- **ネットワークやマルチコアの普及によって、並行処理（協調する複数の処理）が身近に**
- **複雑な並行処理の全体像を理論的に解析して、簡潔に可視化するツールCONPASUを開発**
- **UMLなどの従来の設計モデル／ツールとも連携可能で、既存の開発工程への導入が容易**

研究のねらい

近年、様々な機械制御や情報処理に並行システムが使われています。並行システムでは、複数のプロセスが協調して複数のタスクを同時に処理（並行処理）するため、応答性や高速性を向上できます。しかし、並行処理を的確に把握することは容易ではないため、潜在化した欠陥がリリース後に発見されることもあります。本研究では、並行システムの設計支援を目的として、設計モデルからその並行処理を自動解析するツールCONPASUを開発しています。設計の欠陥を実装前に検出できるため、信頼性の向上だけでなく、開発工程における手戻りコストの削減も期待できます。すなわち、企業が蓄積した開発スキルやツールなどの貴重な資産をさらに活かす形で、QCD（品質、コスト、開発期間）を総合的に改善することができます。

研究内容

並行システムの設計モデル（各プロセスの振舞いと接続関係）から、並行システム全体の並行処理を解析（並行合成と状態数削減）する方法を研究し、その方法を基にツールCONPASUを開発しています。例えば図1は、3個のプロセスから構成される並行システムの設計モデル（図1左）をCONPASUで解析し、その全体の並行処理を表示した結果（図1右）を表しています。また、図2に示すように、CONPASUは入力言語にCSP_Mという形式言語を採用しており、このCSP_Mを通して既存ツール（FDRなど）と連携しながら、UMLなどの従来のモデルを解析することもできます。

連携可能な技術・知財

- モデルベース開発（例：UML）の設計・解析支援
- CONPASU：並行プロセス解析支援ツール
  （産総研知財管理番号H24PRO-1409）
- URL: http://staff.aist.go.jp/y-isobe/conpasu/
- 参考文献：Yoshinao Isobe, CONPASU-tool: A Concurrent Process Analysis Support Tool based on Symbolic Computation, CPA2011, WoTUG-33, IOS Press, pp.341-362, 2011.

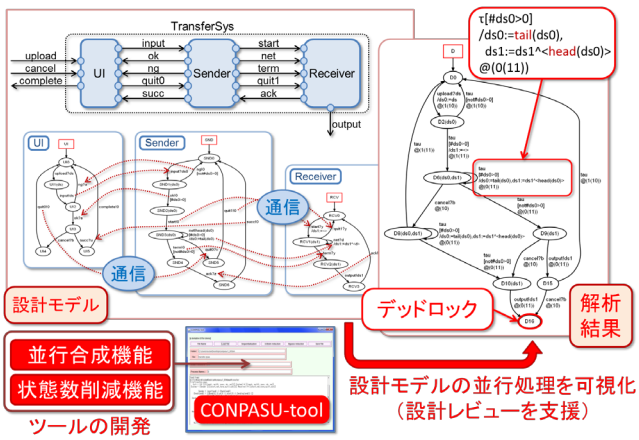


図1 CONPASUツールによる並行処理の可視化の例

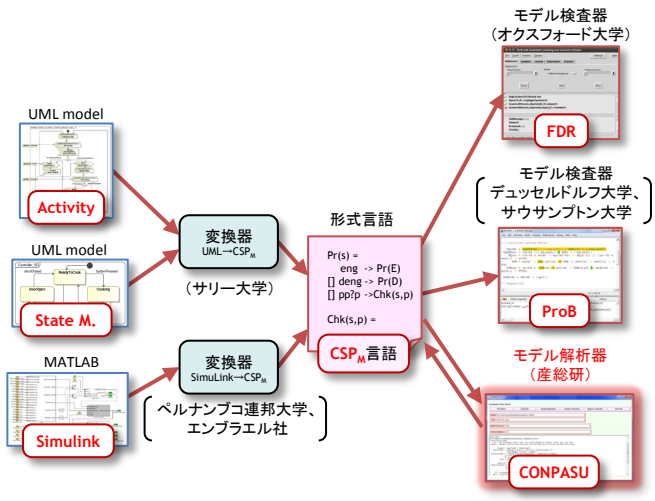


図2 CONPASUと既存モデル／ツールとの連携

セキュアなサービスに向けて
～バランスのとれた安全性・信頼性の実現～

■ 研究担当者：渡辺　創、田沼　均、高木　浩光、、中田　亨、萩原　学、辛　星漢、山口　利恵
h-watanabe@aist.go.jp
■ 所属：　セキュアサービス研究グループ

RISEC

研究のポイント

- **セキュア技術をもっと使いやすくする** ～安全なセキュア技術の研究開発
- **セキュア技術が本当にセキュアか検証する**～セキュアサービスに関する技術文書の公開
- **セキュア技術がどうあるべきか国内外に提言しリードする**～政策や標準化活動への貢献

研究のねらい

ますます大規模化するITサービスで、セキュリティやプライバシー侵害、使いやすさ、信頼性は大丈夫なのか？ プライバシー情報を貪欲に収集する携帯アプリの出現や、ネット銀行での詐欺事件の増加に対抗するための技術基準や標準的手法、ガイドラインを提案し、社会をリードする。

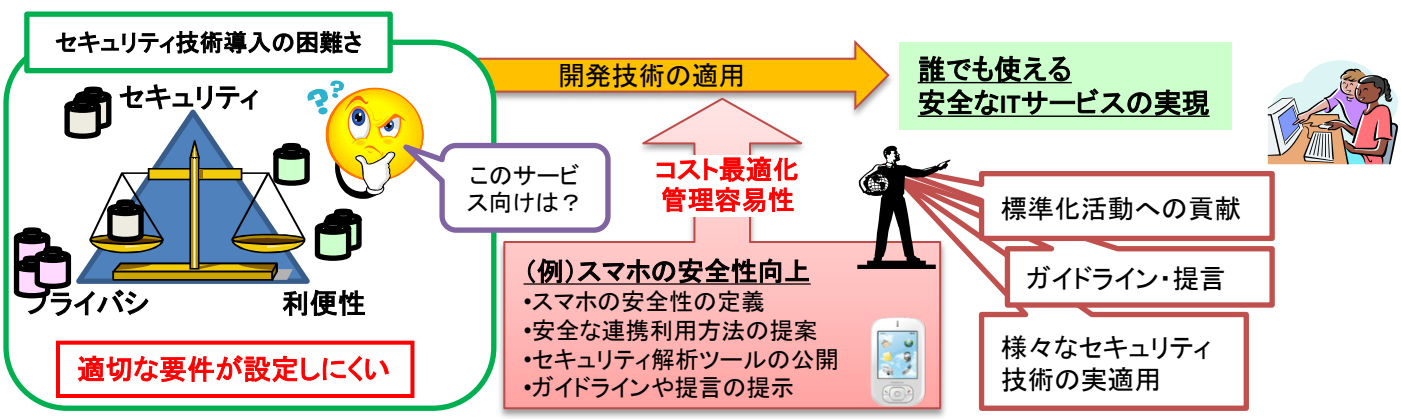
研究内容

➢フィッシング詐欺対策技術（Mutual）
・ネット上のフィッシング詐欺を防止できる新しい認証方式
➢最新の技術動向とサービス利用法の分析と提言
・スマートフォンのプライバシ
➢情報の誤りを自動的に訂正する技術，通信・記録情報の信頼性を向上する技術の研究開発
➢ヒューマンエラー防止技術
・ソーシャルエンジニアリング対策
・まちがえにくい手順の設計理論
➢標準策定への参画
・ISO/IEC JTC1 SC27: セキュリティ技術
・IEC TC65A/AHG16 機能安全とヒューマンファクター
・IETF (Internet Engineering Task Force)
・CRYPTREC:電子政府推奨暗号策定プロジェクト、等

連携可能な技術・知財

特許（出願中含）：
- 特許第4122434号 (US 7,284,154)「仮想ユーザを用いた操作性評価処理システム」
- 特許第4517072号 (US 6,879,877)「ヒューマン・インタフェース自由度効率評価装置」
- 特許第4863283号「軽量の認証プロトコルによる認証システム」
- 特許第4941912号「符号データ特定装置及びそのプログラム、並びに、フィンガープリント検出装置及びそのプログラム」
- 特許第5044784号「ユーザを認証する方法及びサーバ」
- 特願2003-100271 特許3896486「ウェブサイトの検査装置」
- 特願2005-271715 特許4738951「中継装置および中継装置を含む通信システム」
- 特願2007-019615 特許5044784「ユーザを認証する方法及びサーバ」
- 特願2008-299216「二次元コード生成装置」
- PCT/JP2011/050386, WO2011/087030「二次元コード、コード生成システム、プログラム、印刷物」

ソフトウェア知財：
- H21PRO-1048「二次元コードの生成ソフト(JAVAバイナリ版）」
- H23PRO-1271「QR-JAM ライブラリ for Linux 静的ライブラリおよび動的ライブラリ ver.1.0」



ヒューマンエラー対策技術

■ 研究担当者：中田亨
toru-nakata@aist.go.jp
■ 所属： セキュアシステム研究部門セキュアサービス研究グループ

研究のポイント

- **人間が安全へのリスク： 人為ミス、ソーシャルエンジニアリング**
- **人間のまちがい方の探求：人間的推論モデル、人の認識特性にあったインタフェース**
- **作業手順のロバスト化：まちがい耐性強化、リスクセンシティビティの増強戦略**

研究のねらい

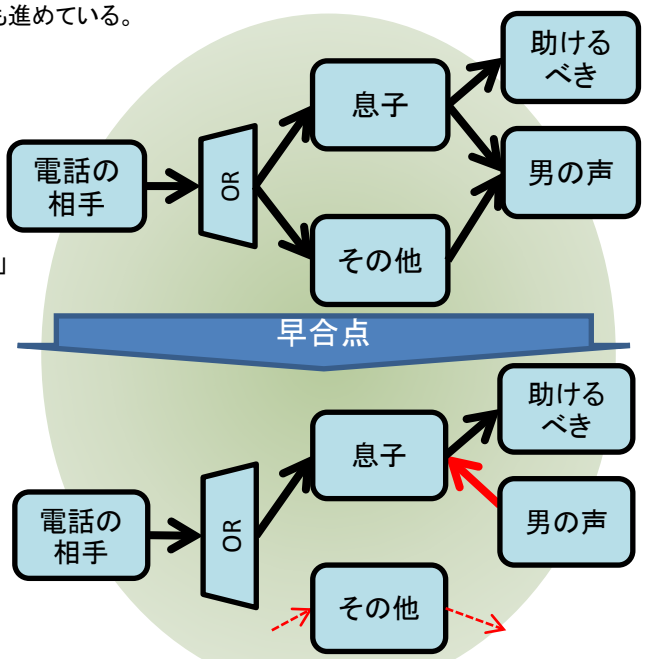
情報漏洩の90%は（敵対者による不正アクセスではなく）内部者の過失がもと。産業事故も8～9割が人為ミス。

人間は誰でも、ある種のトリックを使えば、コロリとだまされる。ソーシャルエンジニアリング（振り込め詐欺やウィルス入りメール）では、人間をだまして攻撃してくる。攻撃と防御の方法を設計するために、人間的推論モデルを開発した。

ミスをしても、攻撃を受けていても、それに早く気付けば問題がない。作業手順の中で適切なタイミングで検査を挿入することが、作業の安全化の本質であり、手順設計理論の研究も進めている。

研究内容

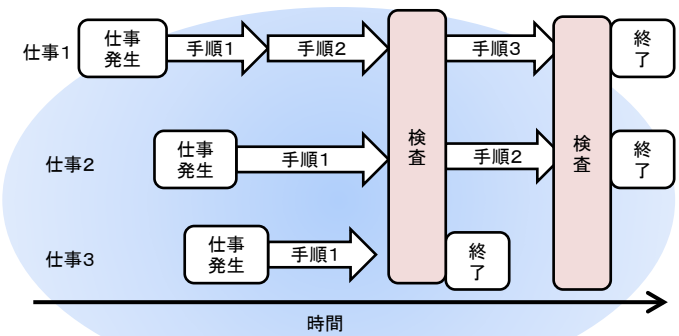
- 人間的推論モデルの特徴
  - •人間のミスパターンを模擬
    - •逆の混同：「AならばB」と「BならばA」
    - •否定の混同「AならばBでない」と「AでないならBでない」
    - •「かつ」「ならば」の混同
    - •多値論理：確信度、例示典型度に依存。
    - •具体性の影響：「板橋ならば東京」と「東京なら板橋」
  - •推論の図解：攻撃ルートや事故過程を検討
- 作業手順のロバスト化
  - •チェックの一斉挿入
  - •チェックの費用対効果の検証



オレオレ詐欺の人間的推論

連携可能な技術・知財

- ヒューマンエラー対策の共同研究実績
  - •金融機関、建設会社
- 国際標準委員会への参画
  - •IEC TC65A/AHG16 機能安全とヒューマンファクター
- 特許第4122434号 (US 7,284,154)「仮想ユーザを用いた操作性評価処理システム」
- 特許第4517072号 (US 6,879,877)「ヒューマン・インタフェース自由度効率評価装置」



手順設計： Control Point(横断的検査時刻)の設定

誤り訂正符号

～情報の信頼性向上を目指す数理科学的取り組み～

■ 研究担当者：萩原学
hagiwara.hagiwara@aist.go.jp
■ 所属：セキュアシステム研究部門　セキュアサービス研究グループ

RISEC

研究のポイント

- **全ての通信機器（携帯電話）・情報端末（パソコン）・記録媒体（USB）に必要不可欠な技術。**
- **デバイスや記録媒体のナノスケール化によるエラー率の上昇を抑えこむ誤り訂正技術。**
- **信頼性の向上はもちろん、セキュアサービスなどへ幅広く応用。**

研究のねらい

携帯電話を用いた音声・メール・画像の通信、パソコン・タブレット端末内の情報処理、ハードディスク・USBメモリ・microSDカードの情報記録。あまり意識されていませんが、これらの機器が扱う情報には、情報の誤り（欠損・消失・変化・環境による影響など）が常につきまとっています。

誤りを意識せず情報機器を利用できる背景には、「誤り訂正符号」と呼ばれる技術が活躍しています。より良い誤り訂正符号を発見することで、情報機器の性能向上だけでなく、機器開発の低コスト化、などなど意外な応用が広がっています。

研究内容

情報機器に最適な誤り訂正符号をつくるため、誤り訂正符号にまつわる理論を多角的に研究しています。具体的には、「誤りの種類や頻度の考察」、「誤り訂正可能な理論限界の導出」、「情報数学に基づいた誤り訂正符号空間の構築、および、誤り訂正のアルゴリズムの構成」、「理論や計算機実験による訂正性能評価」などが挙げられます。

さらに、誤り訂正符号の知識とアイデアを利用し、「暗号プロトコルの開発」、「二次元コードの開発」、「技術の解説（講演、連載、出版など）」、「ワークショップ・シンポジウムの運営」といった活動を行っています。

NO誤り訂正符号　NO情報社会

連携可能な技術・知財

- 特許第4941912号「符号データ特定装置及びそのプログラム、並びに、フィンガープリント検出装置及びそのプログラム」
- PCT/JP2011/050386、WO2011/087030「二次元コード、コード生成システム、プログラム、印刷物」
- 特願2008-299216「二次元コード生成装置」
- H21PRO-1048「二次元コードの生成ソフト(JAVAバイナリ版)」
- H23PRO-1271「QR-JAM ライブラリ for Linux 静的ライブラリおよび動的ライブラリ　ver。1。0」
- 書籍「符号理論　デジタルコミュニケーションにおける数学」、日本評論社、２０１２年８月

フリーソフト・博物館展示・雑誌連載・書籍

HTTP 相互認証プロトコルとその標準化

■ 研究担当者: 大岩 寛、高木 浩光、渡辺 創
h-watanabe@aist.go.jp
■ 所属: セキュアシステム研究部門セキュアサービス研究グループ、高信頼ソフトウェア研究グループ

研究のポイント

- **パスワードが意図したサーバに送られたかをユーザーが検証できるプロトコルを開発**
- **偽サーバへの接続をユーザにわかり易く提示するユーザインターフェイス**
- **ブラウザに標準搭載されることを目指し IETFに 国際標準提案中**

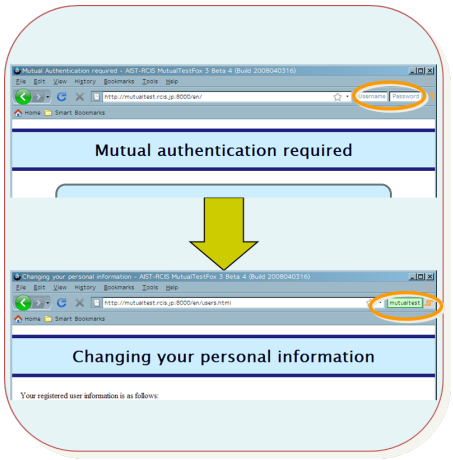
研究のねらい

ユーザを偽サーバに誘導しパスワード情報やカード情報などを詐取する、フィッシング詐欺が大きな社会問題になっています。しかし現状、相手が正規のサーバであることを確認できる標準技術が存在しません。我々は、ユーザがサーバにパスワード認証される際、同時にその情報を利用してユーザもサーバを認証可能とする認証方式を開発し、この問題への解答を与えました。現在、本技術がウェブサーバやブラウザに搭載され、ネットサービスで採用されることを目指し、インターネットの標準個人認証技術としてIETFに提案しています。

研究内容

フォーム認証ページは、フィッシングサイトが容易に模倣できます。インターネット標準のHTTP認証法は、ログアウト等の認証管理機能が欠如している、パスワードを毎回そのまま送信する等の問題があります。

我々は、パスワードを用いた強力な認証法(PAKE)を用い、相手の認証情報保持を相互に確認できる手法を開発しました。これにより、ユーザが正規サーバかを確認可能となり、通信データからのパスワード解析も不可能としました。また認証管理機能も設計し、ログアウトやゲストページ等の制御も可能としました。

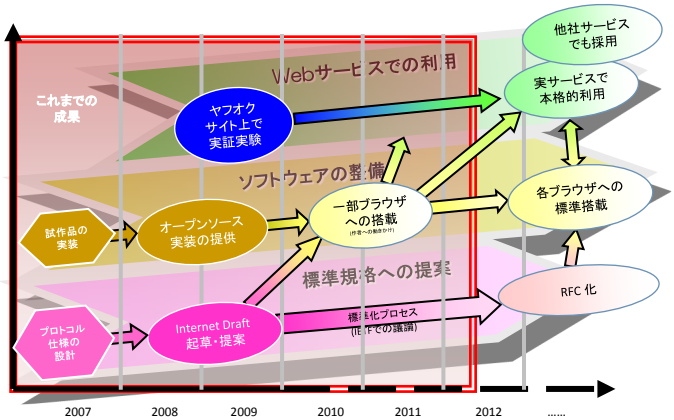


安全な入力欄を用いたユーザ認証の動作画面

連携可能な技術・知財

- 本手法を用いた認証サービス
- 本手法を利用したサービス連携
- Mutual Authentication Protocol for HTTP
  draft-oiwa-httpbis-mutualauth-00, IETF
- 特許第5044784号「ユーザを認証する方法及びサーバ」

謝辞:本内容は、ヤフー株式会社との共同研究成果です。



これまでの活動と今後の展開

ハードウェアの安全性評価技術と偽造防止技術

■ 研究担当者：川村、片下、堀、坂根、姜
risec-iccs-ml@aist.go.jp
■ 所属： ICチップセキュリティ研究班

RISEC

研究のポイント

- **暗号デバイスの電力や電磁波から秘密情報を解析するサイドチャネル攻撃**
- **攻撃への対策や評価手法を検証するための標準プラットフォームを構築**
- **LSIの物理的な「指紋」情報を利用することでデバイスの偽造を防止**

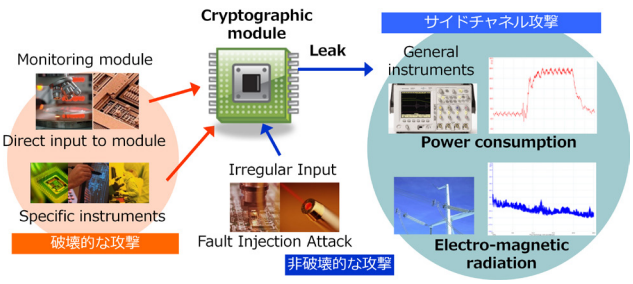
研究のねらい

標準化されている暗号アルゴリズムは理論的な安全性の検証がなされていますが，これを実装する際に不備があると安全性が損なわれてしまいます．そのため，暗号モジュール認証では，アルゴリズムが正しく実装されているか検証がなされています．しかし，暗号デバイスから発生する消費電力や電磁波などを解析して内部の秘密情報を盗み出す攻撃が可能であることが発見されており，サイドチャネル攻撃と呼ばれています．この脅威に対し，対策手法の開発や安全性評価手法の標準化が急務となっています．

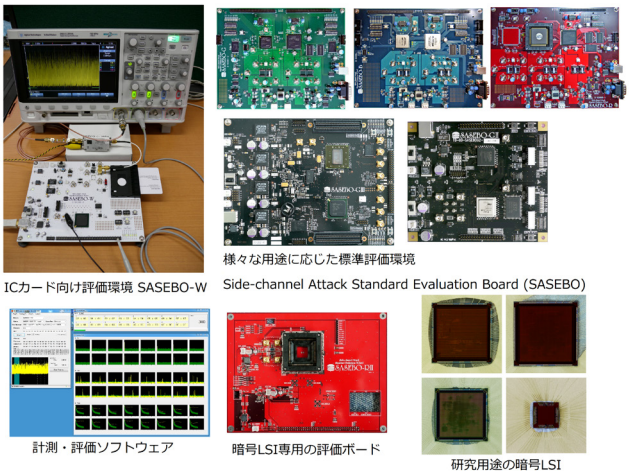
研究内容

ハードウェアの物理的な安全性評価技術の研究促進を目的に，サイドチャネル攻撃の標準評価ボードや専用暗号LSIを開発しました．本評価環境は国内外の100を超える研究機関で広く活用され，これらの研究を通じて数多くの論文も執筆されるようになっています．また，産総研で得られた知識や技術はWebサイトより積極的に公開しており，デバイスの安全性の向上に取り組んでいます．

このほか，評価技術を応用してデバイスの物理的な違いを抽出する手法の研究を進めており，人間の指紋のような情報を利用してLSIの偽造防止を目指しています．



サイドチャネル攻撃とは



物理的な安全性評価の標準プラットフォーム

連携可能な技術・知財

- 標準評価ボードSASEBOの設計知財
- サイドチャネル攻撃に適切な環境構築，計測手法，各種評価方法のノウハウ
- デバイスの偽造防止技術PUF(Physical Unclonable Function)の構成手法
- PUFデバイスの有効性評価

謝辞：
本研究の一部は、JST CRESTならびにJST SPACESの支援を受けて実施されました．

制御システム高セキュア化の取り組み

■ 研究担当者: 高橋、古原、戸田、瀬河、海老原、須崎、渡辺、高木、山口
k.takahashi@aist.go.jp
■ 所属: 制御システムセキュリティ研究グループ

RISEC

研究のポイント

- **隔離された制御システムをも標的とし始めたサイバー攻撃への対応**
- **電気ガス水道などの各種重要インフラを支える制御システムの防護**
- **制約条件を満たしつつ最大の効果を上げるためのアセスメント**

研究のねらい

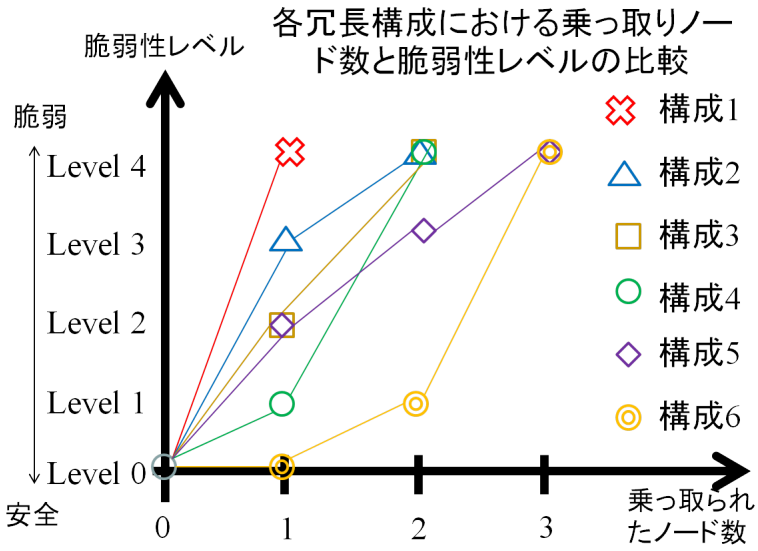
重要インフラを支える制御システムは、機器やネットワークが特殊である他、インターネットからも隔離されているためサイバー攻撃を受けることはないと考えられていました。一方、サイバー攻撃は、不特定多数を狙った愉快犯による攻撃から、反社会的な意図を持って特定の組織やシステムを標的とする高度な攻撃へと変わりつつあります。実際、海外では隔離環境にある制御システムが攻撃された例もあり、また、制御システム自体の汎用化も進んでいます。標準や可用性などの要件を満たしつつ、適切な対策を講じることが求められています。

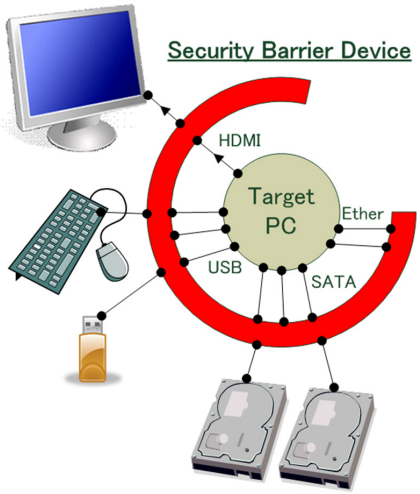
研究内容

制御システムには、止めてはならない、機器の更新期間が長い、既存システムとの互換性、運用体制、標準への準拠、コストなど、現場に応じて各種の制約条件が存在します。これらの制約条件を満たしつつ、最大の効果を上げるためのアセスメント技術を確立させると共に、日々進化するサイバー攻撃やマルウェアの将来を見越して、将来それらを封じ込めるための高度な検知・防止技術についても研究開発を行っています。また、技術研究組合制御システムセキュリティセンター(CSSC)の活動にも協力しています。

連携可能な技術・知財

- 制御システム向けセキュリティアセスメント
- マルウェアに気づかれることなく端末上からその挙動を検知・防止する技術
- 制御機器の設定値、プログラム、ファームウェアなどの安全なアップデート技術
- 特許出願情報2008-230969「複数の端末を用いた改ざん命令実行防止技術」





破られる暗号

■ 研究担当者：花岡悟一郎/SCHULDT Jacob/MIHALJEVIC Miodrag/縫田光司/松田隆宏/
今福健太郎
hanaoka-goichiro@aist.go.jp
■ 所属： セキュアシステム研究部門次世代セキュリティ研究グループ

RISEC

研究のポイント

- **暗号・認証技術が安全とはどういうことか？何を示せば安全と言えるか？**
- **どうすれば多数の暗号・認証技術の安全性を比較/評価できるのか？**
- **暗号・認証技術を部品として用いる情報システムの数学的証明技法に基づく安全性評価**

研究のねらい

ネットワーク社会を安全に機能させるため今や必須の基礎技術である暗号・認証技術には、将来にわたる長期的な安全性が要求されます。強固で客観的な安全性の根拠を与えるため、一般に暗号・認証技術を含む暗号技術には、実運用におけるあらゆる脅威を捉えた安全性要件と、その安全性要件を満足することを厳密な数学的な証明によって示されることが望まれます。本研究では、実社会で既に運用されているものを含む既存の暗号・認証技術やそれを部品として用いるシステム、さらに場合によってはその暗号技術の安全性の定義自体に対して、「安全性を破る」という攻撃者の観点から分析を行い、そこから得られる知見・知識・技術によって、真に安全な暗号・認証技術の構成や、それらの安全性評価の手法の確立を目指します。

研究内容

今日実運用されている暗号・認証技術には、「数学的に証明できる安全性」を持たないものが多数あります。また、次世代の様々な情報システム・サービス実現のために、「グループ署名」、「関数型暗号」など、従来よりも高度な機能を持つ暗号・認証技術が多数提案されていますが、安全性定義が実運用におけるあらゆる脅威を捉えているかの議論が不十分な場合が多いのが現状です。本研究では、既存暗号技術の安全性の不備の指摘、もしくは安全性証明などを行うことで、様々な角度から暗号・認証技術やそれらの拡張についての安全性評価を行っています。また、特定の安全性を持つ暗号技術の効率の限界を追求する研究なども行っています。

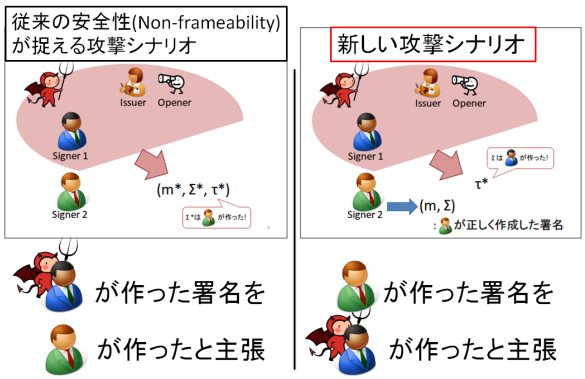


図1 高機能電子署名の一種「グループ署名」において従来の安全性定義の不足を指摘した例

連携可能な技術・知財

- 高機能な暗号要素技術の構成・安全性評価 (図1)
- ストリーム暗号の構成・安全性評価
- ペアリング暗号の基礎となる計算問題の困難性の評価
- 公開鍵暗号の暗号文サイズに関する効率限界の追求(図2)
- その他さまざまな情報システムの設計において必要とされる暗号・認証技術の安全性評価とその手法

謝辞：本研究の一部は、Indian Institute of Technology、富士通研究所、情報通信研究機構、中央大学、電気通信大学、東京大学と共同で実施しています。

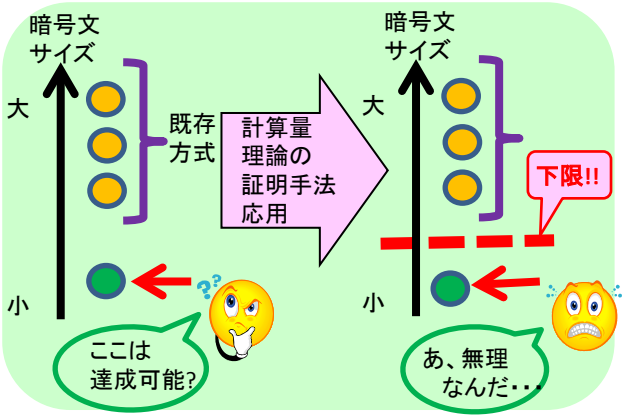


図2 ある種の公開鍵暗号の暗号文サイズの下限導出

破られない暗号

■ 研究担当者：松田隆宏/SCHULDT Jacob/花岡悟一郎/縫田光司/MIHALJEVIC Miodrag/
今福健太郎
t-matsuda@aist.go.jp
■ 所属： セキュアシステム研究部門次世代セキュリティ研究グループ

研究のポイント

- **暗号・認証技術が安全とはどういうことか？何を示せば安全と言えるか？**
- **どうすれば多数の暗号・認証技術の安全性を比較/評価できるのか？**
- **強固な安全性を数学的に証明可能な暗号・認証技術の設計、数学的証明技法の確立**

研究のねらい

ネットワーク社会を安全に機能させるための基礎的な要素技術として、暗号・認証技術は今や必要不可欠です。これらの技術は、将来にわたり長期的に解読・偽造が不可能であることが求められます。しかし、計算技術の今後の進歩の度合いなど予想がつかない部分もあり、高い安全性を確実に保証する普遍的な手立ては知られていません。だからといって、安全性を十分吟味せずに暗号技術を利用することは非常に危険であり、可能な範囲で最大限の安全性の根拠づけが必要です。本研究では、暗号理論・情報理論・計算量理論・量子論などの様々な技術・知見を駆使し、そのような安全性評価技術の確立を目指します。

研究内容

私たちの研究では、暗号・認証技術の安全性を数学的に証明するための手法の確立について取り組み、また、それらの手法を用いて、さまざまな暗号・認証技術が安全であるとは、どのような状態を指すのかを数学的に定義し、その上で、その様な安全性を証明可能とするための条件などを明らかにしています。さらに、さまざまな暗号・認証技術に関し、安全性上の問題点の指摘、もしくは、安全性の証明などを行うことで、利用者が安心してこれらの技術を利用できるようにします。また、これらの研究を通じ、社会における暗号技術についての様々な要求・問題解決に即座に答えられるように、暗号理論に関する知見を日々蓄えています。

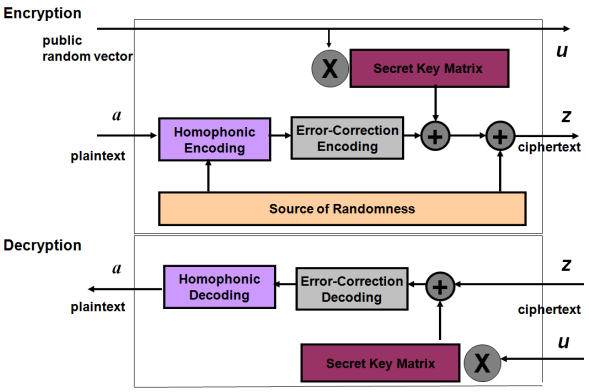


図1 量子コンピュータに耐性を持つ共通鍵暗号の一構成

連携可能な技術・知財

- 暗号技術を用いるシステムの数学的安全性評価手法
- 公開鍵暗号・電子署名の安全な設計手法・高効率化
- 量子コンピュータに耐性を持つ暗号・認証技術 (図1)
- 量子暗号についての知見
- その他様々な情報システムの設計における適切な暗号・認証技術の選定方法、及び、個別システム向けの最適な暗号・認証技術の設計 (図2)

謝辞：本研究の一部は、株式会社東芝、NHK、中央大学、東京大学、電気通信大学、筑波大学と共同で実施しています。

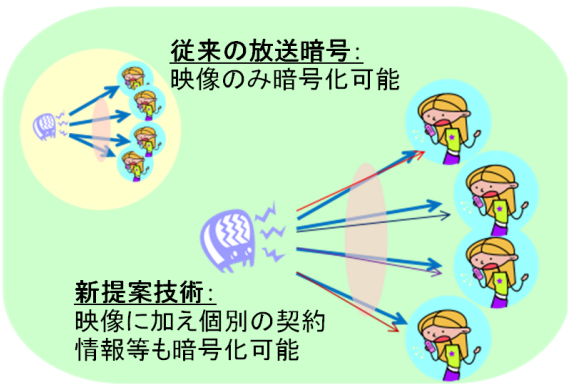


図2 個別システム向けの暗号技術の例

不特定多数受信者向け暗号技術

■ 研究担当者：縫田光司/花岡悟一郎/ATTRAPADUNG Nuttapong/伍軍
k.nuida@aist.go.jp
■ 所属：セキュアシステム研究部門次世代セキュリティ研究グループ

研究のポイント

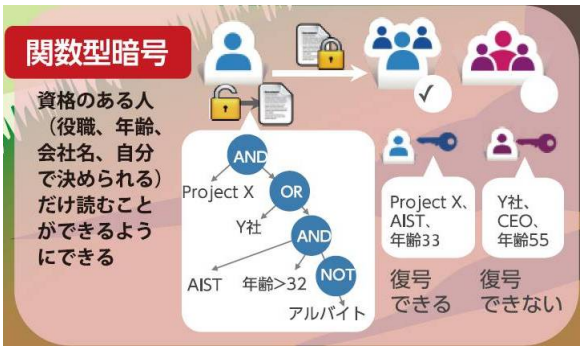
- **放送などの不特定多数へのコンテンツ配信で、権限のない者による盗み見を防止**
- **データの一斉送信と受信者制限機能の両立など柔軟なアクセス制御**
- **不正受信者間の結託や正規受信データの不正アップロードにも対応**

研究のねらい

放送をはじめとする不特定多数向けのコンテンツ配信においては、正規の契約済みユーザにのみコンテンツの視聴を許可することでコンテンツ制作者の権利保護に繋がりますし、また年齢などユーザの属性に応じた視聴制御の仕組みはユーザ側の安心にも繋がります。私たちは、このような厳格さと柔軟さを兼ね備えたコンテンツへのアクセス制御技術について、暗号技術の観点から研究に取り組んでいます。この研究によりコンテンツ産業の振興に貢献するとともに、研究で得た知見をNHKの次世代放送など近未来の新たな技術にも応用することを目指しています。

研究内容

私たちの研究の中心テーマは、不特定多数へのデーター斉送信に特化した暗号技術である「放送暗号」と、ユーザの属性に応じた暗号文の復号許可が可能な暗号技術である「関数型暗号」です。特に後者の技術については、コンテンツ配信に留まらず、多数のユーザが同時にデータへアクセス可能なクラウドサービス上でのアクセス制御技術への応用も見込まれています。また、正規受信者が復号後のコンテンツを不正に横流しする行為について、横流しされたコンテンツに不正者の「目印」が残るようにして、横流し行為を抑制するユーザ識別符号の研究も行っています。

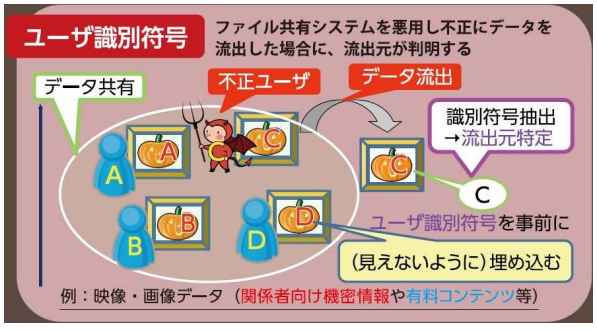


ユーザ属性に応じて復号許可する関数型暗号

連携可能な技術・知財

- 放送暗号の構成・安全性評価
- 関数型暗号の構成・安全性評価
- 電子指紋符号の構成・安全性評価
- 特許第4941912号(2012/03/09)「符号データ特定装置及びそのプログラム、並びに、フィンガープリント検出装置及びそのプログラム」

謝辞：本研究の一部は、財団法人国際科学技術財団平成19年度研究助成の助成を受けたものです。



コンテンツ流出元の目印を残す電子指紋符号

検索内容とデータベースの情報を相互に秘匿するデータ検索技術

■ 研究担当者：縫田光司/花岡悟一郎/SCHULDT Jacob/松田隆宏
k.nuida@aist.go.jp
■ 所属： セキュアシステム研究部門次世代セキュリティ研究グループ

研究のポイント

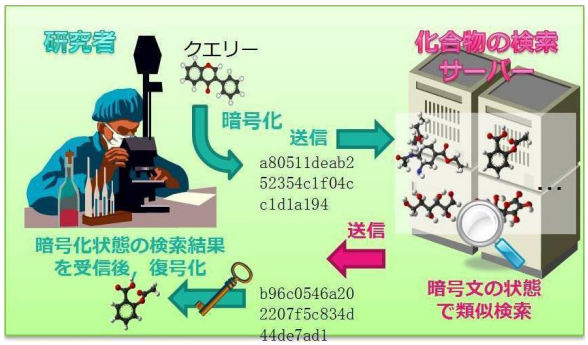
- 何を検索したいかをデータベース側に明かさずにデータ検索を実行できる技術
- しかも、検索対象の有無以外の余分なデータベース情報を検索者に対して秘匿可能
- 既存の手法と比較し、計算コストと通信コストのバランス良い削減を実現

研究のねらい

医療情報などのプライバシーに関わる情報や、研究開発に関わる機密性の高い情報についてデータベース検索サービスを利用する際には、データベース側に検索内容の情報を悪用される心配をすることになります。一方、検索サービス側でも、苦心して構築したデータベースの内容をできる限り公開したくないという状況が考えられます。そこで本研究では、検索者側の検索内容をデータベース側に公開することなく、またデータベース側から「検索と合致するデータの有無」以外の余分な情報を検索者側に公開することなく検索を実現するデータベース検索方式の設計とその安全性評価についての研究を行っています。

研究内容

本研究では、産総研生命情報工学研究センター（CBRC）などと連携し、データベース側と検索者側双方の情報を秘匿する化合物データベース検索プロトコルを研究しています。従来の方式では、検索内容の秘匿のみ実現され、データベース側の情報秘匿は考慮されていませんでした。一方、一般論によって双方の情報を秘匿する検索プロトコルを理論的には設計可能ですが、計算コストや通信コストが大きすぎる問題があります。本研究では、CBRCなどの提案方式をベースに、データベース側を含めた双方の情報秘匿と計算・通信コストのバランス良い削減を目指してプロトコルの設計改良と安全性の理論的評価を進めています。



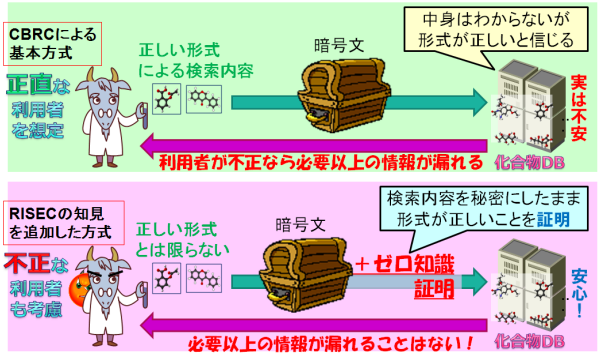
化合物のデータベース秘匿検索技術の概要

連携可能な技術・知財

- 準同型暗号の構成法と安全性証明に関する知見
- 加法準同型暗号を用いたデータ類似度判定プロトコル
- 暗号化状態のまま、平文のデータ形式の正当性を担保するゼロ知識証明プロトコル

謝辞：本研究は、産総研生命情報工学研究センター（CBRC）、東京大学、筑波大学と共同で実施しています。

高安全プライバシ保護データ検索



検索内容の正当性担保（当グループの知見）

お問合せ先

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
セキュアシステムシンポジウム実行委員会
TEL: 029-861-5284 FAX: 029-861-5285
E-MAIL: kickoff-sympo-ml@aist.go.jp
URL: http://www.risec.aist.go.jp/events/2012/0910-ja.html

本掲載記事の一部またはすべての内容について、無断転載を禁じます。
Reproduction in whole or in part without written permission is prohibited.

Copyright © 2012 AIST, All Rights Reserved.