研究課題名：　　暗号通信手順の安全性自動検証に関する研究
所属研究機関名：独立行政法人　産業技術総合研究所
研究者氏名：　　大崎　人士

Ⅰ．研究成果の概要

■　研究の趣旨･目的

高度情報化社会の基盤となる通信システムが安全かつ確実に動作することは、ますます重要になっている。銀行システム、電子商取引などの経済活動にとどまらず、市民生活、さらには国防にいたるまであらゆる場面においてインターネットの障害は社会生活に深刻な影響を及ぼす。インターネットにおける通信においては、特に、データの暗号化による通信の秘密の保護が必要であるが、そこでは破られにくい暗号法の技術と共に、暗号化法を通信網の中で正しく生かして使う技術が必要である。例えば、正規のデータ受取人に「なりすまして」暗号を解く鍵を不正に入手してプライベートなデータを入手するなどという攻撃を避けるための技術が要請される。これは解読が困難な暗号化法を考案する技術とは独立のものである。どのようにかたい暗号も復号法が必ずあり（さもないと受信者はデータを読み取れない）それを受信者に伝えなければならないが、そのときに横取りされないような通信手順が必要なのである。ここで問題となるのは、「なりすまし」などの悪意の第三者からの攻撃が決して成功しないことをどのようにして確かめるのかである。

そこで本研究では、情報科学における基礎技術を通信工学に応用し、情報システムの安全性を検証する技術について研究する。具体的には、書換系およびツリー・オートマトンの理論による数理的基礎を発展させ、暗号通信手順（暗号プロトコル）の安全性自動検証のための技術を開発し、暗号通信手順の安全性を自動的に検証するソフトウエア（「検証システム」と呼ぶ）を作成することを目的とする。

■　研究計画の概要

本研究の目的は「暗号をもちいた通信プロトコルで、意図する相手にのみ秘密情報を伝達することができるか（秘密保持性があるか）を自動検証する手法の開発」である。自動化の利点を失わずに、より広いクラスの通信プロトコルを検査の対象とするため、従来のツリー・オートマトンの定義を拡張する。そして、新しい数理的なモデルについての、閉包演算および決定問題の解決する。さらに、新しい数理的なモデルをもちいたリアクティブ・システムのための自動検証方法を考案し、現実的な時間で安全性を検証するためのアルゴリズムの開発や、近似計算アルゴリズムの開発などの研究する。

II．研究計画の詳細報告

（単位：百万円）

研究項目	所要経費			
	12 年度	13 年度	14 年度	合計
1．書換系に関する基礎研究	3.5	4.5	5	13
(1)調査研究 a. 海外研究所訪問等 b. 専門家の招聘	(3.5)			(3.5)
(2)プロトコル文法の制約条件に関する研究（書換閉包の研究）		(4.5)	(5)	(9.5)
2．等式付ツリーオートマンに関する基礎研究	3	4	3	10
(1)調査研究（専門家の招聘等）		(1)		(1)
(2)等式付ツリーオートマン理論の構築	(3)	(3)	(3)	(9)
3．検証自動化に向けた要素技術に関する研究	4.5	9.5	10	24
(1)通信プロトコルに関する調査研究（他分野専門家とのセミナー実施）		(5)		(5)
(2)自動検証ソフトウエアの構築 a. ソフトウエアの作成と実験 b. 実験計算機の管理と保守	(4.5)	(9)	(7)	(20.5)
(3)成果報告書及び CD-ROM 作成			(3)	(3)
所要経費（合計） （管理費を含む）	11	18	18	47

III. 研究成果の概要

■ 研究成果の概要

従来のツリー・オートマトン理論を拡張して、等式付ツリー・オートマトンという理論概念を導出し、

1. 線形等式付正規ツリー・オートマトンの空(くう)判定問題が決定可能であること
2. 結合則付ツリー・オートマトンの空判定問題が決定不可能であること
3. 結合則・交換則付ツリー・オートマトンと結合則付ツリー・オートマトンが受理言語上の合併集合および共通集合について閉じていること

などを示した（国外誌[6]）。

さらに、等式付ツリー・オートマトンによる自動検証の可能性を，理論的に裏付けるため、空判定問題が決定可能になるための十分条件を調べ、

4. 結合則・交換則付ツリー・オートマトンの空判定問題が決定可能であること

を示した（国外誌[5]）。これにより、結合則と交換則をうまく扱うことのできなかった従来の理論では、秘密保持性の自動検証がきわめて難しいとされていた「Diffie-Hellman の鍵交換プロトコル」や「Shamir のスリーパス・プロトコル」を使う暗号通信手順が、等式付ツリー・オートマトンによる自動検証の対象に含められることを示した（応募・主催講演等[9]）。いっぽう、結合則付正規ツリー・オートマトンと文脈自由文法との相互類似性を示すことにより、受理言語上の集合演算について閉じていないことも示した。この結果は、受理言語どうしの合併演算などを必要とする自動検証では、結合則付ツリー・オートマトンが正規であるというのは、強すぎる条件であることを表している。さらに、以下の事柄についても示した。

5. 結合則付ツリー・オートマトンの受理言語が補集合について閉じていること
6. 結合則付ツリー・オートマトンの受理言語が、変換を含まない書換系については、（あらかじめ自然数nを定めた場合の）n-ステップの書換関係について閉じていること

5や6の性質が、結合則・交換則付ツリー・オートマトンでも成り立つかについての調査は、今後の研究課題である。こうした理論的基礎をもとに、暗号通信手順の安全性自動検証システムを構築した。

■ 波及効果、発展方向、改善点等

本研究中に開発した暗号通信手順の安全性自動検証法は、原理的には、リアクティブ・システムと呼ばれる「動作中に外界からの多様な刺激を受けて、その刺激と内部状態から応答を決定する」装置全般に適用可能である。このタイプのシステムは、銀行のオンラインシステムや携帯電話等の通信システムなど、いちど稼働させてしまうと容易に停止することが出来ないことが、特徴である。安全で安定した情報システムの整備が、社会的な急務となっている現在、稼働前に十分な安全性の検証をおこなうことは、社会的ニーズでもある。また、大規模システムやマスプロダクトに対しては、検証で発見された誤りにより設計変更を余儀なくされた場合に、損失を極力小さく抑える必要があるため、設計の初期段階で検証できなければならないという要求もある。これは、携帯電話などの組込みプログラムが問題を含んでいる場合、その問題発見が遅れると莫大な製品回収コストを要することが一因している。しかし、リアクティブ・システムを単純に遷移系としてモデル化すると、しばしば状態空間が無限となり、従来のモデル検査法は無力である。このため、本研究で開発した「リアクティブ・システムの安全性検証法」（特許申請中）は、今後、暗号通信手順の安全性検証にとどまらず、例えば、携帯電話のようなライフスパンが短いマスプロダクトに対して、予想外の製造コスト（欠陥製品の回収コストなど）が発生する割合を減らし、製品の製造コストを削減することに、役立たせることが可能になると考えられる。

Ⅳ. 研究成果の公表等の状況

(1) 研究発表件数

	原著論文の発表	左記以外の誌上発表	口頭発表	合　計
国 内	3 件	0 件	12 件	15 件
国 際	4 件	0 件	6 件	10 件
合 計	7 件	0 件	18 件	25 件

(2) 特許等出願件数

1 件 (うち国内1件、国外 0 件)

(3) 受賞等

0 件 (うち国内 0 件、国外 0 件)

(4) 主な原著論文による発表の内訳

原著論文の発表 ＊発表者氏名:,「発表題目」,文献名,巻(号),頁, (掲載年) の順

国内誌 (国内英文誌を含む)

[1] Toshinori Takai, Hiroyuki Seki, Youhei Fujinaka and Yuichi Kaji: Layered transducing term rewriting system and its recognizability preserving property, IEICE Transactions on Information and Systems, vol. E86-D(2), pp. 285-295, 2003.

[2] Toshinori Takai, Yuichi Kaji, and Hiroyuki Seki: Right-linear finite-path overlapping term rewriting systems effectively preserve recognizability, Scienticae Mathematicae Japonicae. To appear.

[3] Toshinori Takai, Yuichi Kaji, and Hiroyuki Seki: Termination property of inverse finite path overlapping term rewriting system is decidable, IEICE Transactions on Information.

国外誌

[4] Hitoshi Ohsaki and Aart Middeldorp: Type introduction for equational rewriting」Acta Informatica, vol. 36(12), pp. 1007-1029, (2000)

[5] Hitoshi Ohsaki and Toshinori Takai: Decidability and closure properties of equational tree languages」 the 13th International Conference on Rewriting Techniques and Applications (RTA2002), Copenhagen (Denmark), 2002. Springer-Verlag, Lecture Notes in Computer Science 2378, pp. 114-128.

[6] Hitoshi Ohsaki: Beyond regularity: equational tree automata for associative and commutative theories」 the 15th International Conference of the European Association for Computer Science Logic (CSL2001),(2001). Springer-Verlag, Lecture Notes in Computer Science 2142, pp. 539-553.

[7] Hitoshi Ohsaki, Aart Middeldorp, and Jurgen Giesl:「Equational termination by semantic labelling」 the 14th International Conference of the European Association for Computer Science Logic (CSL2000),(2000). Springer-Verlag, Lecture Notes in Computer Science 1862, pp. 457-471.

⑸ 主要雑誌への研究成果発表

Journal	Impact Factor
Acta Informatica	0.604
Lecture Notes in Computer Science	0.515

暗号通信手順の安全性自動検証に関する研究