整理番号	１４大－３

育成試験の名称	新しい情報セキュリティ技術－カオス暗号システム
実施機関及び担当者	大阪府立大学 大学院 工学研究科 教授 川本　俊治

育成試験の目的

カオス写像をコンピュータで繰り返し計算すると丸め誤差が集積し、正確なカオス時系列を再現することはできないと言われてきた。この問題を解決し、カオスの工学的実用化を目的として、本課題では暗号システムへの応用を目標に、まず丸め誤差が集積しないカオス時系列計算アルゴリズムを提案し、PC 用のソフトウェアおよび暗号システム回路などのハードウェアを試作する。そして新しい情報セキュリティ技術として、インターネット上でのデータ・音声・画像の送受信により、ストリーム型・ブロック型カオス暗号システムの安全性および高速性を検証し、事業化を目指した試験を実施する。

試験方法

試　験　項　目	内　　容
ストリーム型・ブロック型カオス暗号システムの安全性・高速性に関するコンピュータシミュレーション	正確なカオス時系列を繰り返し計算できるアルゴリズムを提案し、暗号システムへ応用するシステム設計を行う。次にその安全性を理論的に保障できることを証明し、シミュレーションで提案アルゴリズムを用いた計算処理時間による高速性を比較検討する。
インターネット上におけるデータ・音声・画像の送受信による安全性・高速性の試験検証	カオス暗号システムのソフト･ハードの製作と調整および動作確認を行い、データ・音声・画像をインターネット上で送受信することにより、ストリーム型･ブロック型カオス暗号システムの安全性・高速性を検証する。
予　算　額	２００万円

試験結果

本課題の育成試験で得られた結果は以下の通り要約できる。

（１）暗号システムの提案アルゴリズムを設計することができた。

（２）暗号システム回路を製作し、コンピュータに組み込むソフトウェアを試作した後、ネットワーク上の PC 間でシステム動作を確認できた。

（３）ストリーム型・ブロック型のどちらにおいても理論的に安全性を確保できることが分かり、研究期間中に新たに得られたカオス的初期値依存関数による暗号システム（特許出願の申請中）は特に高速性（提案法の約５倍）に優れ、携帯電話・PDA などに適していることが分かった。

（４）本試験検証により、カオス暗号システムの事業化は可能と評価できる。

現在の状況及び今後の展開方策

平成１４年度 RSP 事業育成試験に採択され、従来システムに比べ５倍以上高速で安全なカオス暗号システムを試作した。（特許出願済）
本カオス暗号システムにより、海外と安全･高速に動画像の送受信をネットワーク上で検証し、本格的な商品化を目指して企業化し、引き合い企業が多数でてきている。
しかし、商品を売るためには米国、日本での政府の認証を取り、信用度を増す必要がある。