

# 暗号アルゴリズム

最近の話題から

ソフトウェア コンサルタント

鈴木裕信

Hironobu@h2np.Suginami.Tokyo.JP

# なぜ今暗号なのか

- 情報自体 (コンテンツ)を守る方法
  - 守るべきコンテンツが増えた
- オープンネットワークの時代
  - インフラを整備するより安くなった
- 必要な計算パワーが使える時代
  - 守る側に有利に働く

# コンピューター時代における暗号

## ■ 情報理論の成立とともに

– <http://cm.bell-labs.com/cm/ms/what/shannonday/>

## ■ シャノン (C. E. Shannon) が書いた2つの論文

– A Mathematical Theory of Communication (1948)

– Theory of Security System (1949)

## ■ 符号化3兄弟

– データ圧縮符号化、誤り訂正符号化、暗号

# 現代暗号

---

- 1970年代のDES以降
  - 情報理論にもとづいて安全性を証明
  - アルゴリズムを公開

# 暗号の分類

- 対称暗号 (symmetric cryptography)
  - 共通鍵暗号、秘密鍵暗号、慣用暗号
- 公開鍵暗号 (public key cryptography)
  - 非対称暗号

# 対称暗号

- 暗号化するプロセスと復号化するプロセスがシメトリックである
- 同じ鍵を使う



# 対称暗号の分類

---

- ストリーム暗号
  - ビット毎単位で暗号化・復号
- ブロック暗号
  - ブロック単位で暗号化・復号

# ブロック暗号

---

- 一定期間同一の鍵が使用される
  - 理論的完全秘匿性を達成できない

# 暗号の安全性とは何か

- 解読するためには膨大な計算量が必要となる
  - 世界中のコンピュータを利用できても計算に10万年かかるならば実質的に安全である
- 既存の暗号分析理論に対処している
  - 安全性評価をきちんと行っていること

# 向上する暗号分析理論

- NSAの作ったSKIPJACKはすでに安全ではない
- MAGENDAは発表し終わったと同時に安全性が崩壊した
- 分析されていない! = 安全
  - 複数により分析が行われ、それが十分に認められるときに安全といえる

# AESとは何か

- 米国商務省による次期標準暗号規格
- DESの後釜として公募
- 連邦規格 (FIPS) 実質上の世界標準
- 主催はNIST、技術コンサルタントにNSA
  - [http://csrc.nist.gov/encryption/aes/aes\\_home.htm](http://csrc.nist.gov/encryption/aes/aes_home.htm)

# AES以前の流れ

- 1970年代
  - 米国の標準暗号を公募・1977年にDESが標準暗号となる
- 1980年代後半から1990年代前半
  - 米国政府による暗号規制の強化・国家によるブラックボックス化した暗号
- 1990年代後半
  - 寿命が付きかけているDESに替わる新しい暗号の必要性・公開された規格

# AESの公募開始

- 1998年 6月公募締め切り
  - Symmetric, Block, 128-128/192-128/256-128
  - Windows 95 / Pentium Pro 200MHz
  - ANSI C / Borland C++ 5.0
  - Java / JDK 1.1
  - 各種ドキュメント

# 評価スケジュール

## ■ ラウンド1

- 1998年 8月 :1stカンファレンス
- 1999年 3月 :2ndカンファレンス
- 1999年 4月 :ラウンド1パブリックコメント締め切り

## ■ ラウンド2

- 1998年 5月 (? ):5つ程度の暗号がラウンド2へ進む

# ASEに応募してきた暗号

- 全部で15の暗号が受理された
- 暗号の評価は一切行わず公募要綱さえ正しければ受け付けた
- 書類の不備や提出したコードが動かないなどでいくつかの暗号は受理されなかった

# リスト

---

CAST-256

CRYPTON

DEAL

DFC

E2

FROG

HPC

LOKI97

MAGENTA

MARS

RC6

RIJNDAEL

SAFER+

SERPENT

TWOFISH

# 大きく4つに分類

- 評価の高いもの
  - RC6, MARS, TWOFISH, E2, SERPENT
- 人気がないもの
  - DFC, CAST-256, DEAL, CRYPTON, RIJNDAEL
- 安全性評価で問題が発見されたもの
  - MAGENTA, SAFER+, LOKI97
- 評価不可能なもの
  - FROG, HPC

# 評価の高い暗号について

---

- E2
- MARS
- RC6
- SERPENT
- TWOFISH

# E2

---

- 日本電信電話株式会社
  - 青木、植田、大久保、大田、神田、高嶋、盛合 (NTT)、松本 (横浜国大)
- 保守的なデザインと処理効率のバランスの良さ

# MARS

---

- IBM
  - 老舗中の老舗
- 今日的プロセッサをターゲット
- Type-3 Feistelと呼ぶ新しい構造

# RC6

---

- MIT, RSA
  - Ronald Rivest(MIT), Lisa Yin et al. (RSA)
- 新しい方式であるRC5の発展型
- Pentium Proをターゲット

# SERPENT

---

- アカデミック

- Ross Anderson(Univ. of Cambridge UK), Eli Biham(Technion, ISRAEL), Lars Knudsen(Univ of Bergen, Norway)

- 超保守的デザインと高い安全性マージン

# TWOFISH

---

- Counterpane Systems, Hi/fn, UCB
  - Bruce Schneier(counterpane), Doug Whiting(Hi/fn), David Wagner(UCB)
- 既存の良い構造を取り入れつつチューン

# NISTは何を基準に選ぶのか？

---

- 基準となるメジャーはあるのか？
  - NISTの速度計測表

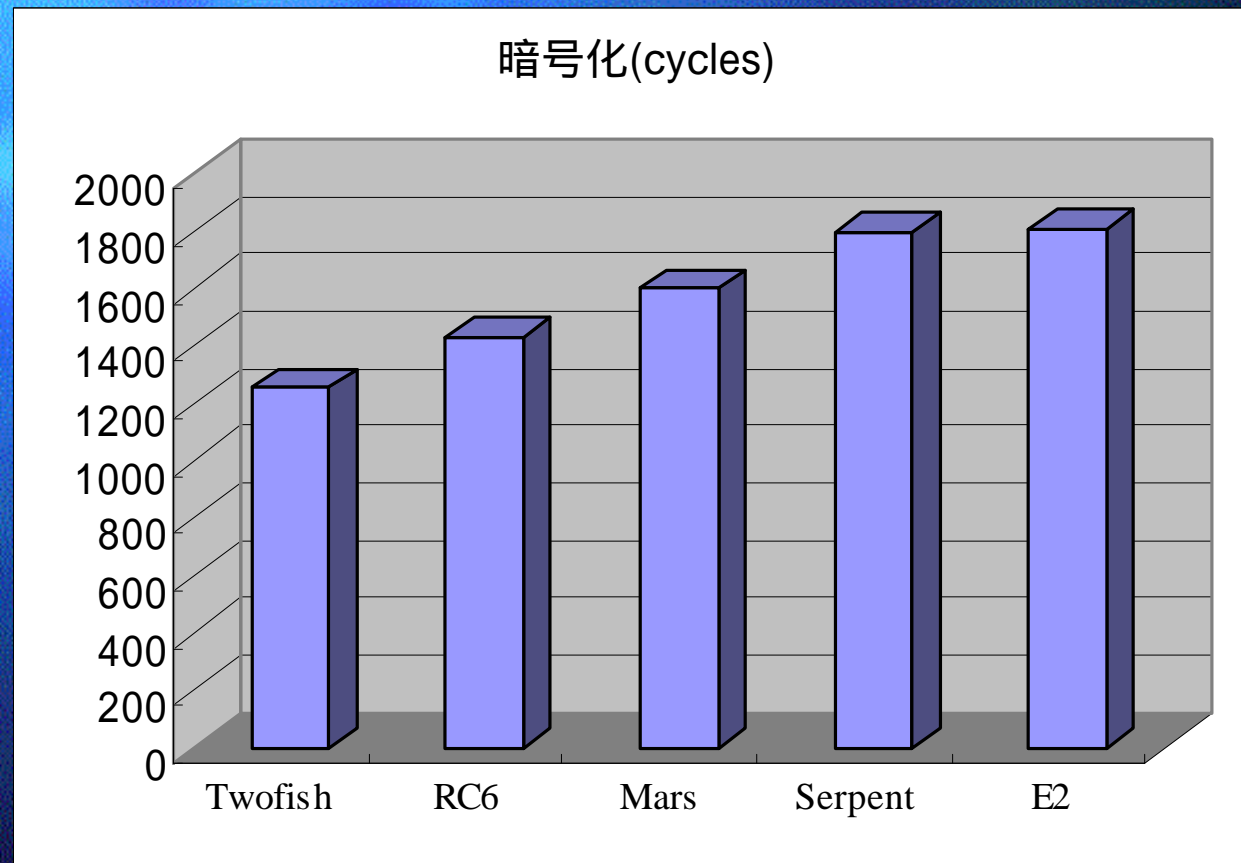
# 何をターゲットにするのか

---

- Pentium Pro, II, III ?
- 8, 16, 32, 64bit cpu?
- Java?
- Smartcard?
- Hardware?

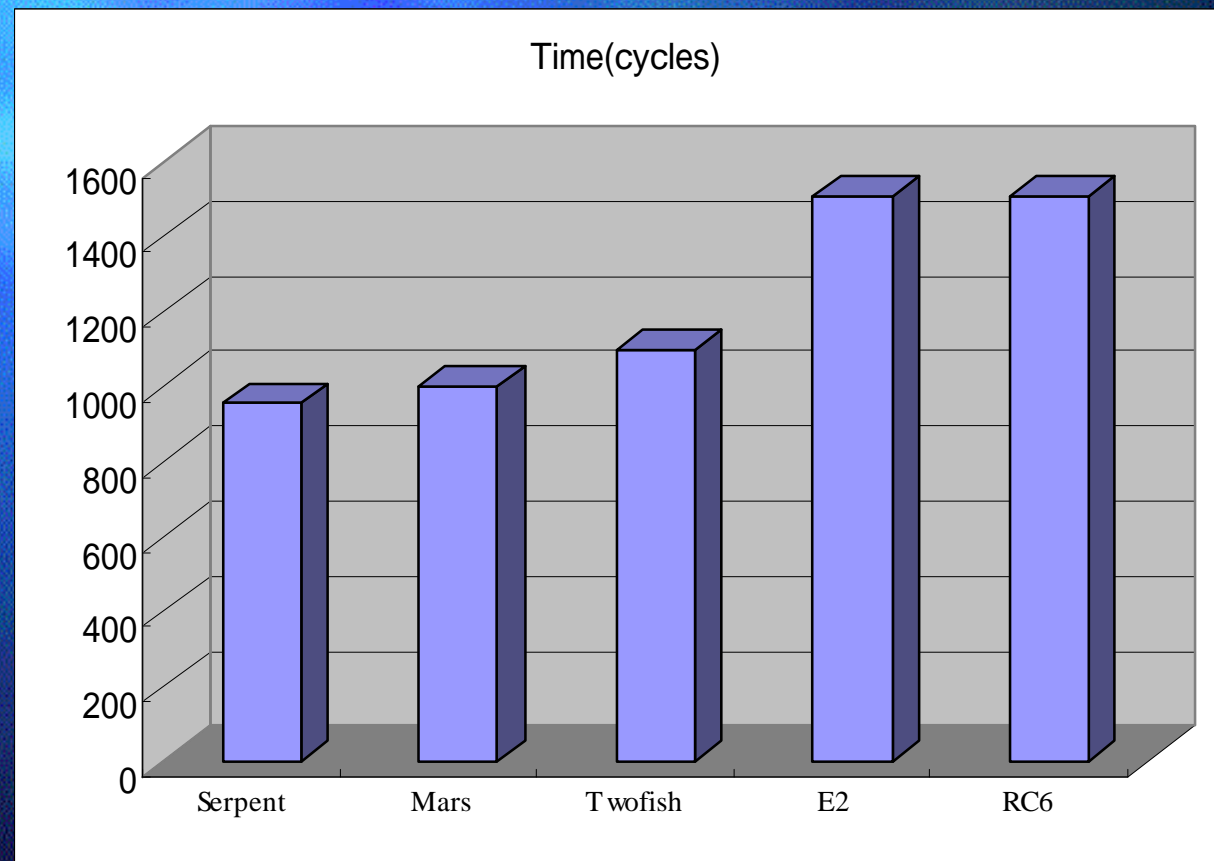
# プラットフォームによる違い

- Linux/GCC-2.7.2/Pentium 133MHz  
MMX



# 速度と安全性のバランス

## ■ 最小ラウンドでの速度比較



AESはこれだ！大胆予想

---

# 出走馬

---

- E2
- MARS
- RC6
- SERPENT
- TWOFISH

# 単勝

- 3番 (RC6 )に 5000円
- 2番 (MARS)に 3000円
- 5番 (TWOOFISH)に 1000円
- 4番 (SERPENT)に 800円
- 1番 (E2 )に 200円

# 安全性マージンで考える

---

- SERPENT
- MARS
- E2
- TWOFISH
- RC6

# 好き嫌いで考える

- SERPENT
- MARS
- RC6
- TWOFISH
- E2

# 複数採用するケースもありえる？

## ■ 複数を採用する

- すべての状況で有利な暗号などない
- すべての卵を1つのバスケットに入れない

## ■ AES 3兄弟

- イチロー、ジロー、サブロー

## ■ Round2に進んだすべてを採用する

# 結論

- 現代の暗号は多様な用途に使われ、そのすべてに有利な暗号は存在しない
- ソフトウェア実装はCPU、コンパイラなどに非常に左右される
- どこまで安全であるべきかの客観的基準をつくるのはむずかしい
- 将来新しく開発される暗号分析理論にどこまで耐えられるか予想はむずかしい