セキュリティ・キャンプ フォーラム 2017
2017年 3月 17日(金)

セキュリティ
技術者・研究者への期待
～ プラス増強のセキュリティ？ ～

首藤 一幸

東京工業大学

IPA 未踏 プロジェクトマネージャー

首藤 一幸 (43)

しゅどう　かずゆき

低レイヤーマン

1996　早稲田大学 修士課程

1998　早稲田大学 博士課程

2001　産総研　**国研**

2006　ウタゴエ(株)　**スタートアップ**

2008/12 東工大　**大学**

2009/ 5 未踏 PM

Java スレッド移送システム MOBA

Java Just-in-Time コンパイラ shuJIT

17,000ダウンロード, 商用実績

P2P の基盤ソフト Overlay Weaver

26,000ダウンロード, 15ヶ国

41ヶ国 673台以上で動作 (データベース)

P2P ライブ配信ソフト UG Live

未踏スパクリ × 2人, 商用化, 1万数千人に同時配信

書籍 Binary Hacks

著者5人, 1万数千部

P2P のアルゴリズム, 2009 ～

構造化オーバレイ / DHT の統一フレームワーク

分散データベース, 2009 ～

読み書き性能両立, Causal consistency, NVRAM / SCM

分散システムのシミュレーション, 2011 ～

1億ノード / 10台, 既存手法の20倍の性能, Apache Spark 上

魔法のようなソフト

大規模分散システム

セキュリティ関連の取り組み

- 早大 学生 ～ 助手，～ 2001 年
  - 管理面
    - サーバ・ネットワーク管理
    - 新入生への講義
    - サーバ管理者に対する啓蒙
  - 技術面
    - **DES の強度解析**，1996年 3月
    - **AES 応募のお手伝い**, 1998 ～ 1999年
- 産業技術総合研究所
- ウタゴエ (株) 取締役 CTO，2006 ～ 2008 年
  - **セキュリティコンサルとの攻防**
- 東京工業大学

root パスワード忘れた…
よし、exploit だ！

John the Ripper ラヴ

電子メールに
カード番号書いちゃダメ

パッチ当てようね

DES の強度解析

1996年 3月

- NTT 研究所でインターンシップ → 研究会で発表
- 線形解読法に対する強度、言われてるより低いよ。

社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

隣接S-boxの影響を一部考慮したDESの経路探索

青木和麻呂　首藤一幸 *

maro@isl.ntt.jp　shudoh@muraoka.info.waseda.ac.jp

NTT 情報通信研究所
〒238–03 神奈川県 横須賀市 武 1–2356

*早稲田大学理工学部情報学科
〒169 東京都 新宿区 大久保 3–4–1

あらまし　差分解読法や線形解読法に対する安全性を表す指標に最大差分特性確率、最大線形特性確率がある。松井が提案した探索アルゴリズムにより DES に対する最大差分特性確率や最大線形特性確率はすでに求められている。このアルゴリズムは DES の最小構造である S-box の差分特性確率や線形特性確率を求め、それから F関数の差分特性確率や線形特性確率を導き、最終的にアルゴリズム全体の差分特性確率や線形特性確率に拡張している。しかし実際には、計算量の問題から 1 つの F関数内の 8 つの S-box の差分特性確率や線形特性確率が独立に求められると仮定して差分特性確率や線形特性確率が求められていた。

今回の報告では DES の S-box の差分特性確率や線形特性確率が独立であるとの仮定を一部外して行なった最良経路探索法と探索結果を報告する。

和文キーワード　最大差分特性確率, 最大線形特性確率, 探索アルゴリズム, DES

*首藤は平成 8 年 3 月 NTT 情報通信研究所で本研究に参加

Characteristic Search for DES Considering Effect of Adjacent S-boxes

Kazumaro AOKI　Kazuyuki SHUDOH *

maro@isl.ntt.jp　shudoh@muraoka.info.waseda.ac.jp

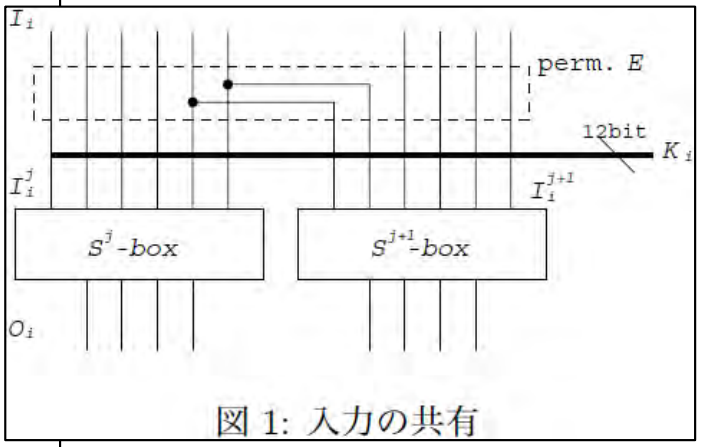


図 1: 入力の共有

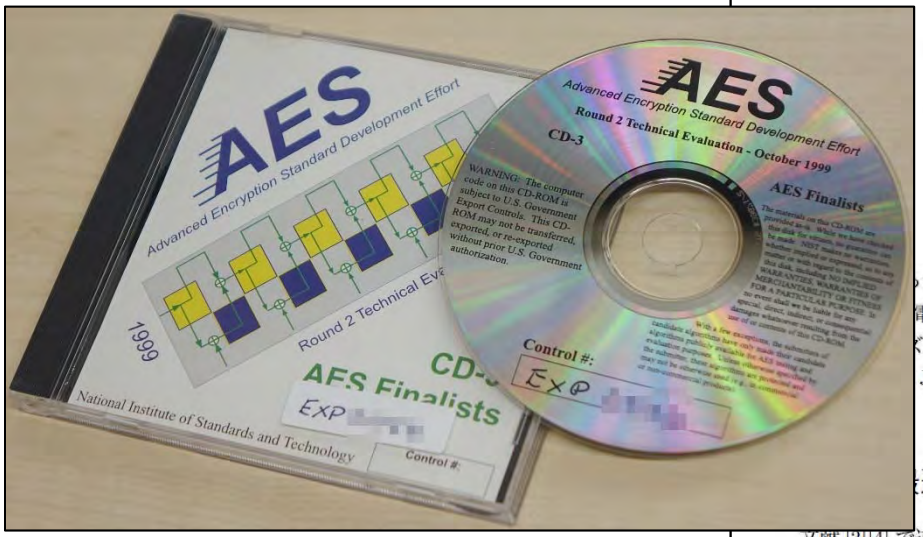
論文

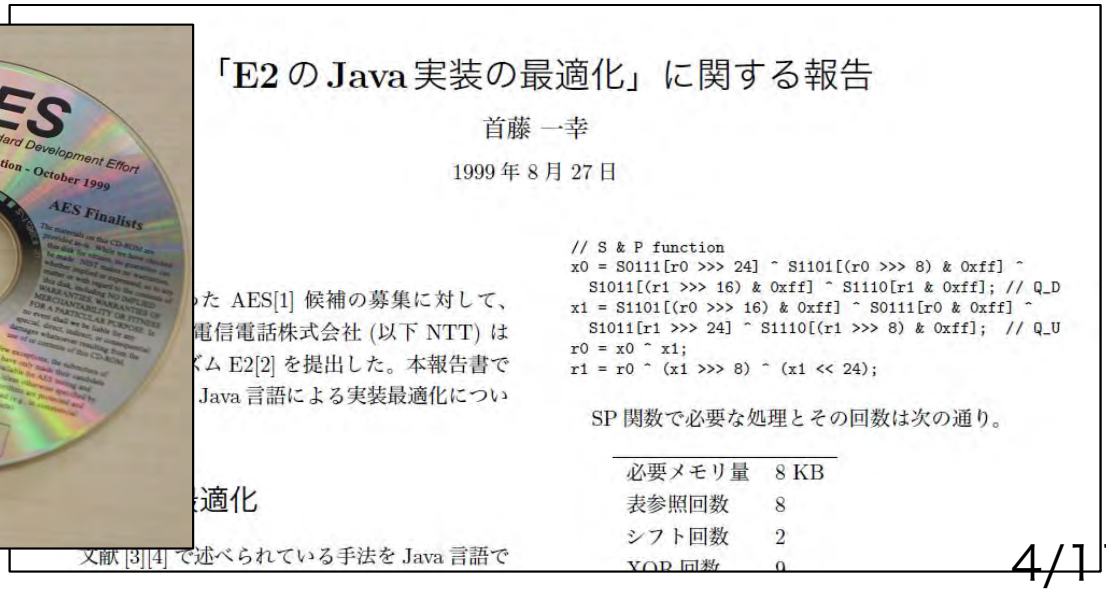
AES 応募のお手伝い　1998 ～ 1999年

- AES competition
  - DES の強度やばいから次を決めよう by NIST
- NTT の応募をお手伝い
  1. Java 言語版の高速実装
  2. 応募アルゴリズムの性能評価

共通鍵暗号方式 設計者が考えることを垣間見た

企業の本気を見た：
例: ASIC 実装のゲート数,
　　8 bit 実装の効率





「E2 の Java 実装の最適化」に関する報告

首藤 一幸

1999 年 8 月 27 日

た AES[1] 候補の募集に対して、
電信電話株式会社 (以下 NTT) は
ズム E2[2] を提出した。本報告書で
Java 言語による実装最適化につい

適化

文献 [3][4] で述べられている手法を Java 言語で

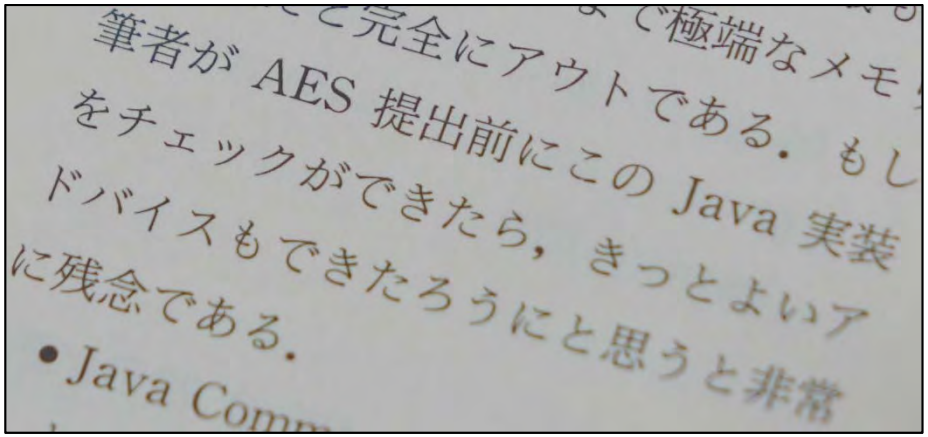
```
// S & P function
x0 = S0111[r0 >>> 24] ^ S1101[(r0 >>> 8) & 0xff] ^
  S1011[(r1 >>> 16) & 0xff] ^ S1110[r1 & 0xff]; // Q_D
x1 = S1101[(r0 >>> 16) & 0xff] ^ S0111[r0 & 0xff] ^
  S1011[r1 >>> 24] ^ S1110[(r1 >>> 8) & 0xff];  // Q_U
r0 = x0 ^ x1;
r1 = r0 ^ (x1 >>> 8) ^ (x1 << 24);
```

SP 関数で必要な処理とその回数は次の通り。

必要メモリ量	8 KB
表参照回数	8
シフト回数	2
XOR 回数	9

AES 応募のお手伝い　1998 ～ 1999年

- Finalists 5 候補に残れず！
  - 応募 21 → 受付 15 → Finalists 5 → AES 1 ＝ Rijndael (ラインデール, レインダール, …)
- メモリ消費量が理由？ 俺のせい？
-



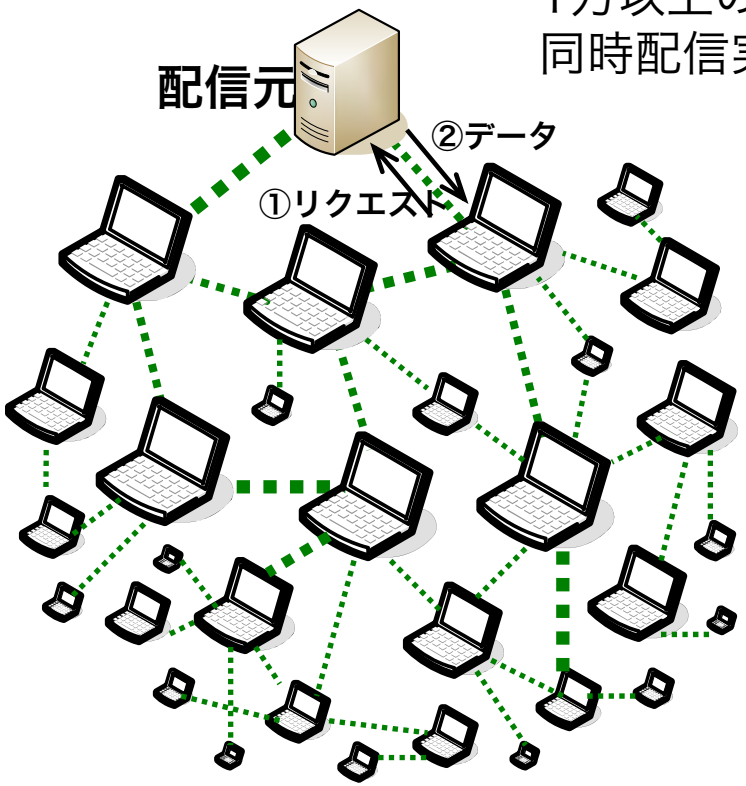
bit 誌 2000年 4月号

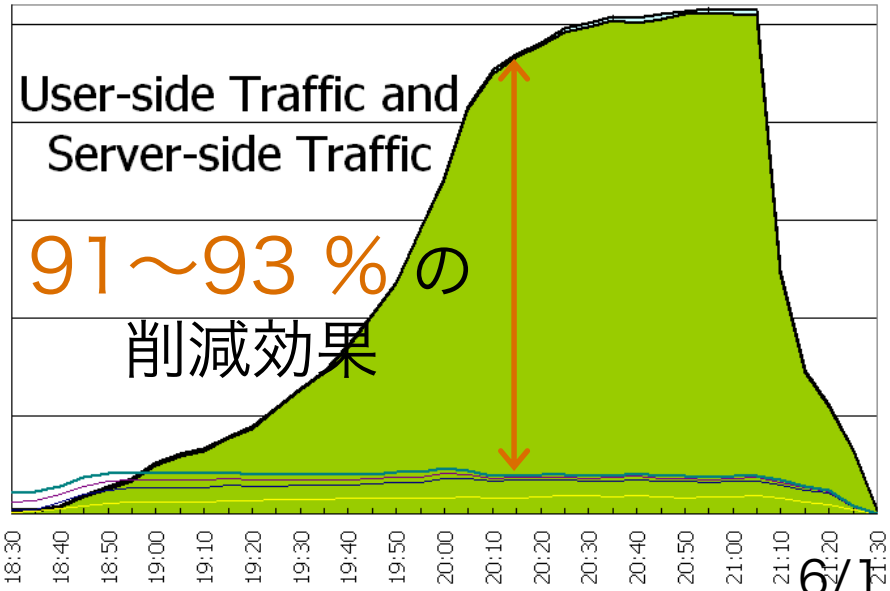
セキュリティコンサルとの攻防

2006年 7月

- ウタゴエ(株) の当時の事業：
  peer-to-peer ライブ配信

1万以上の視聴者への
同時配信実績





UTA GOE UNIVERSAL GRID

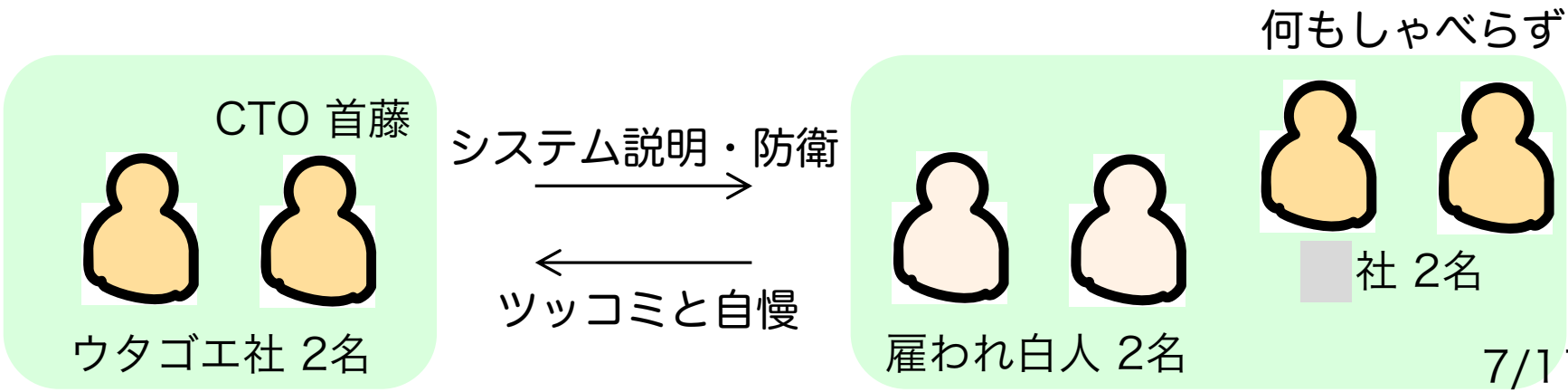
セキュリティコンサルとの攻防

2006年 7月

- 　社のアドバイスで、　社の子会社である
  セキュリティコンサル　社と打ち合わせ
  - 　社が連れてきた白人 2名 vs. 首藤
  - 白人「俺らがいじったら、銀行中のドアが一斉に開いたぜ。ハハ！」

- 　社自身の技術は？
- リスクをとって新しいものを世に問おうとしている自分達が、
  なんで、**あら捜し屋** にイジめられる？

→ **セキュリティコンサルへの嫌悪感**



マイナスの抑制とプラスの増強

- 目の前の課題や機会を分類：$2^3 = 8$ 象限
  - 重要性　高 𝕀 ～ 低 𝕚
  - 緊急性　高 𝔼 ～ 低 𝕖
  - 機会 ＋ ～ リスク －
    - 例：お金がなくて会社潰れる！ たぶん 𝕀𝔼 －

- どこに力を注ぐべきか？
  - 重要性 高・緊急性 高・リスク 𝕀𝔼 － ？
  - 経営者は？

マイナスの抑制とプラスの増強

- 経営者の本分は
  重要性 高・緊急性 低・機会 Ⅰe＋
  - ⅠE－ ではなく Ⅰe＋

- 根拠
  - 緊急性の高いリスク E－
    すでに明確な形をとっている & 対応は限られる。
    方法論の蓄積がある。ある程度の頭脳があれば対処できる。選択肢少なめ。⇒ 人材やサービスを買える。
    - 例：数カ月後に資金がショートする。

    問題 **解決**

  - 緊急性の低い機会 e＋
    不確実性 が高く、何をするかの選択が恣意的。

    問題 **設定**

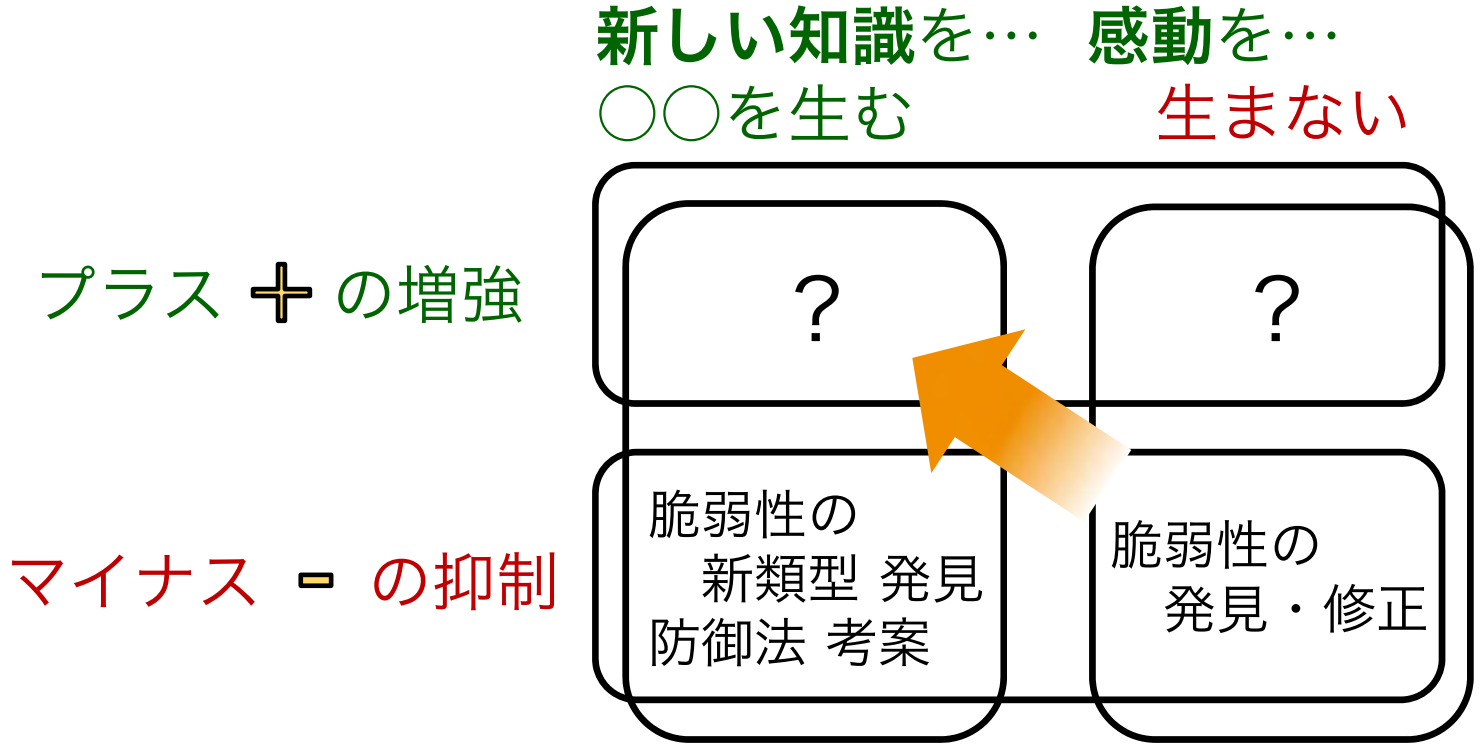
マイナスの抑制とプラスの増強

- ヒトはもともと、
  機会 ＋ よりリスク － に敏感
  - 我々は、死なずに生き残った祖先たちの子孫。
    脳はきっと、機会よりもリスクに敏感にできてる。

- リスク － には、自然に、簡単に、目が向く。
  だから、機会＋の方に注意を向けることに
  価値がある。
  - IPA ：セキュリティ施策 ⇔ マイナス抑制 = 規制行政 ？
    未踏 ⇔ プラス増強 = 振興行政 ？
  - マイナス抑制は、粛々と。内部統制とかセキュリティとか…

プラス増強のセキュリティ？

- セキュリティって、
  たいがい、マイナスの抑制じゃね？



- トップ人材なら右下にとどまるな！