

MWS企画セッション

**3F2-4 :**  
**暗号分野から学ぶ**  
**攻撃という名の安全性評価**

2018年1月25日(木)

○伊豆 哲也 (富士通研究所)

- 暗号分野では破ったことを暗号発明者に事前に報告するなどの紳士協定がある。
- 本発表では、暗号理論の研究における攻撃(解読)の研究の位置づけやより実用面での研究について、暗号研究から学ぶべき点を共有する機会とする。

## 27<sup>TH</sup> USENIX SECURITY SYMPOSIUM

AUGUST 15-17, 2018  
BALTIMORE, MD, USA



### Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (e.g., an IRB).
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The same applies if the submission deals with personally identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns. Contact the program co-chairs at [sec18chairs@usenix.org](mailto:sec18chairs@usenix.org) if you have any questions.

対応する記述なし

仮説：暗号が破れても  
世の中に与える影響は小さい

## ■ 暗号が破れるのは突然ではなく、過去の知見の蓄積の結果

■ 例：ハッシュ関数 MD5 (ハッシュ関数の以前のデファクトスタンダード)

- 1991年：アルゴリズム提案
- 1993年5月：別々のIVに対するコリジョン攻撃 (den Boer, Bosselaers)  
 $MD5(IV; X) = MD5(IV'; X')$
- 1996年5月：仕様とは異なるIVに対するコリジョン攻撃 (Dobbertin)  
 $MD5(IV; X) = MD5(IV; X')$
- 2004年8月：差分解読法によるコリジョン攻撃 (Wang, Feng, Lai, Yu)  
 $MD5(IV; X) = MD5(IV; X')$

## ■ 暗号が理論的に破れるのと、実際に破れる間には時間的なギャップがあることが多い

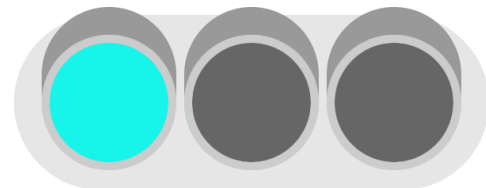
■ 例：SHA-1 (米国の旧ハッシュ関数標準)

- 2005年2月：SHA-1 のコリジョンの計算方法の発表      理論的な攻撃成功
- 2008年4月：CRYPTREC における SHA-1 の危殆化
- 2017年2月：SHA-1 のコリジョンが発見される      実際の攻撃成功

## ■ 安全：回避できない攻撃よりも効果的な攻撃が存在しない

■ 例：128ビット鍵の共通鍵暗号

- $2^{128}$  回よりも少ない計算量の攻撃が存在しないこと

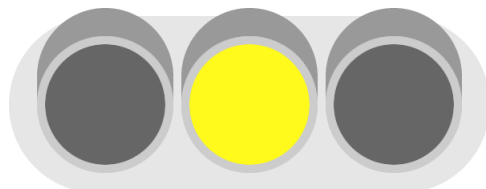


## ■ 要注意：回避できない攻撃よりも効果的な攻撃が理論的には存在するが、実際には攻撃できていない

■ 例：DESに対する差分解読攻撃が見つかった頃

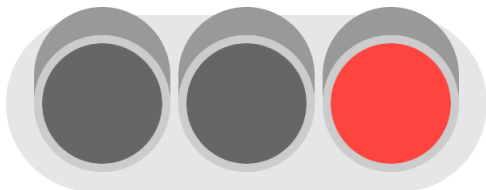
- 全数検索に必要な計算量は  $2^{56}$  回
- 差分解読攻撃に必要な計算量は  $2^{47}$  回
- しかし実際には解読に至らなかった

■ 暗号研究者はこの時点で「破られた」と言うことが多い



## ■ 危険：回避できない攻撃よりも効果的な攻撃が存在し、実際にも攻撃に成功した

■ 誰もが「破られた」と考える段階



# 根拠②：暗号が破れてもその暗号は使用されていない

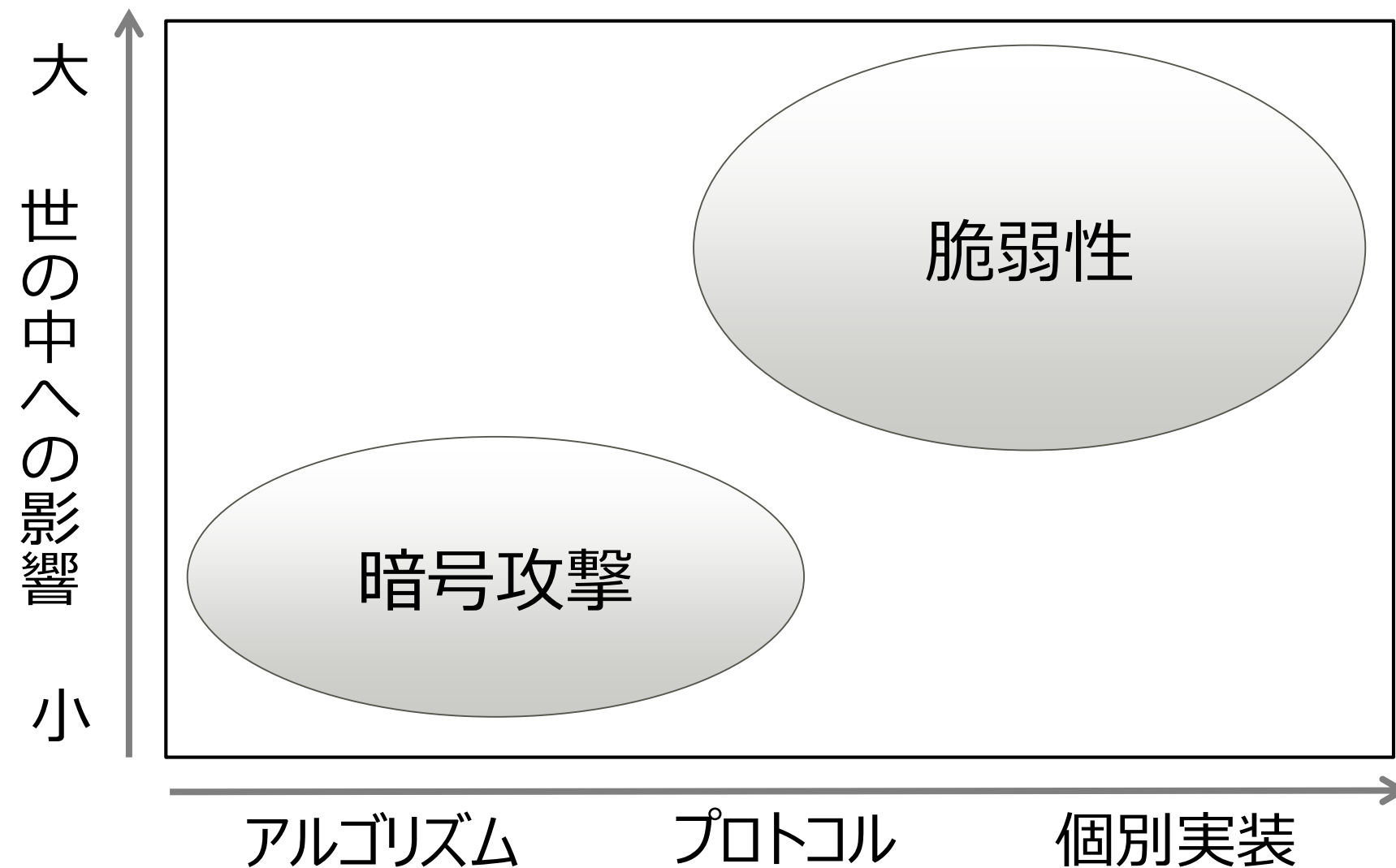
## ■ 破れることが予測されているアルゴリズムを危殆化し、新しい暗号に移行する

### ■ 例：SHA-3 (米国の次世代ハッシュ関数標準)

- 2005年2月：SHA-1 のコリジョンの計算方法の発表
- 2005年2月：NISTは SHA-2 への移行を推奨をアナウンス
- 2013年12月：NIST による SHA-1 の利用停止の期限
- 2012年12月：SHA-3 選定プロセスにおいて Keccak を選出
- 2017年2月：SHA-1 のコリジョンが発見される

### ■ 例：耐量子暗号

- 1994年：量子計算機における Shor アルゴリズムの発明
  - RSA, Diffie-Hellman, ECC が多項式時間で解読可能
- 2017年11月：量子計算機に耐性のある公開鍵暗号の標準化コンペティションを実施
  - 今後、数年をかけて標準耐量子公開鍵暗号アルゴリズムを制定



## ■ 2007年2月：APOP の脆弱性

- セキュアPOPプロトコルであるAPOPにおいて、パスワードのMD5ハッシュからパスワードが特定できる、という問題 → APOP は使用停止に
  - APOP の仕様上、MD5 以外のハッシュ関数を使用できる仕組みになっていなかった
- FSE 2007 において Leurent 等が論文発表
- NTT・電通大も同時期にほぼ同じ結果を得ていたが、IPAに脆弱性を届け出たため、FSE 2007 には論文投稿できなかった
  - ランプセッションで発表
  - IPA は脆弱性報告を受理、発表 (2017年4月)



## ■ プレプリントを公開する

- その成果のタイムスタンプを取得するため
  - 誰かが思いついたことは、他の誰かも思いつく
- その攻撃の有効性は論文ベースで議論される
  - 暗号理論分野は数学・情報科学などの分野が中心となって発展したため
  - 主張の検証可能性が確保される（「剽窃」騒ぎになりにくい）
  - 論文が評価の対象

## ■ 暗号作成者に連絡する


- 攻撃手法の正当性を確認する
  - そのプレプリントの査読者になる可能性が高い？

## ■ 暗号攻撃は世の中に影響を与えない

- 攻撃の可能性を事前に予測
- 予測した攻撃が成功する頃には社会に影響を与えないよう移行させている

## ■ 課題：予測できないような新攻撃への対応

- 過去の良い事例が思いつきませんでした
- 広く使われている暗号に対する新しい攻撃は発見されない？



**FUJITSU**

shaping tomorrow with you