IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

暗号アルゴリズム移行問題
- 暗号研究者の立場から -

IPA セキュリティセンター
暗号グループ　山岸　篤弘

問題意識の背景

- RSA暗号
  - 鍵の長さを変更する必要がある
    - モジュラスの変更
  - 1024bitでは、そろそろ危ないかなぁ。
- ハッシュ関数
  - SHA-1もそろそろ寿命かなぁ。
  - まだ、MD5も使われているし・・・。

暗号の安全性

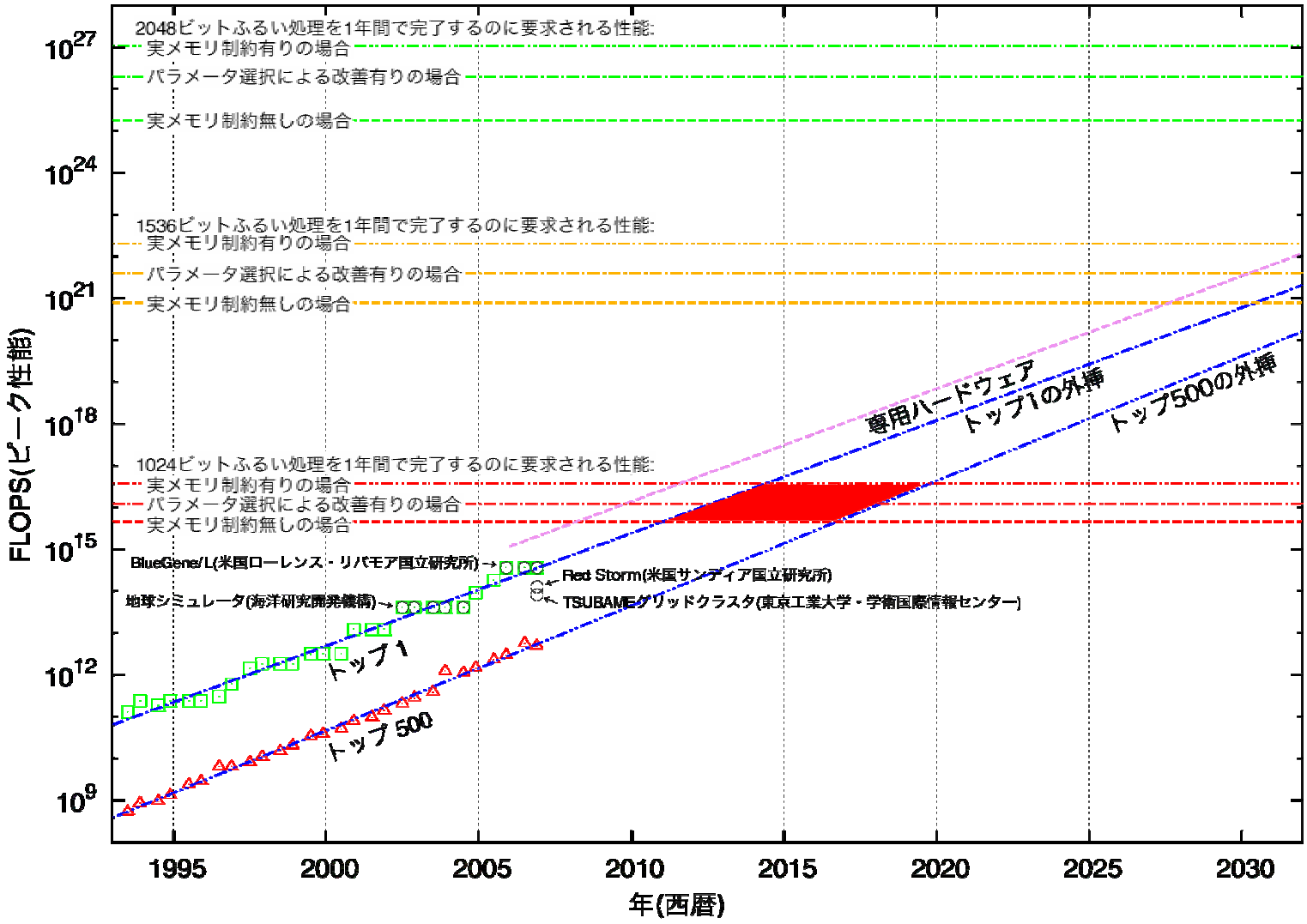
- 暗号の安全性への脅威
  - 解読法の進歩
  - 計算能力の向上
- 共通鍵暗号/ハッシュ関数
  - 解読法の進歩＞計算機能力の向上
- 公開鍵暗号
  - 素因数分解 (IFC)
    - 解読法の進歩＜計算機能力の向上
      - 素因数分解問題は劇的な変化は考えにくい
  - 離散対数問題
    - 解読法の進歩＞計算機能力の向上

地震型(予測が難しい)

火山型（予測可能？）

火山/地震

RSA暗号の安全性


2048ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
1536ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
1024ビットふるい処理を1年間で完了するのに要求される性能:
実メモリ制約有りの場合
パラメータ選択による改善有りの場合
実メモリ制約無しの場合
専用ハードウェア
トップ1の外挿
トップ500の外挿
BlueGene/L(米国ローレンス・リバモア国立研究所)
地球シミュレータ(海洋研究開発機構)
Red Storm(米国サンディア国立研究所)
TSUBAMEグリッドクラスタ(東京工業大学・学術国際情報センター)
トップ1
トップ500
FLOPS(ピーク性能)
年(西暦)
10^27
10^24
10^21
10^18
10^15
10^12
10^9
1995
2000
2005
2010
2015
2020
2025
2030

ハッシュ関数に求められる安全性(1)

~原像計算困難性 (Preimage Resistance)~

入力メッセージ M
(長さ任意のビット列)

ハッシュ関数
h

ハッシュ値(n ビットのビット列)
H = h(M)

たとえば
19A5 628F 6725 C360 2846 D682
7659 B396 F926 684D (16進数表示)

要件:
ハッシュ関数 h において、
与えられたどのハッシュ値 H に対しても、対応する入力メッセージ (原像) 、すなわち、H = h(M) を満たす M を、一つでも求めることが、十分に計算量を要し、困難であること。

補足:ハッシュ値の原像は一般に沢山あるが、それらのうちの一つすら具体的に求めることが困難であることを要求している。

事実:
与えられたハッシュ値に対応する入力を求めるために必要な計算量は、
ハッシュ値が n ビットであるとき、ハッシュ関数の計算を 2^n 回行うための計算量を超えない。

ハッシュ関数に求められる安全性(2)

~衝突困難性 (Collision Resistance)~

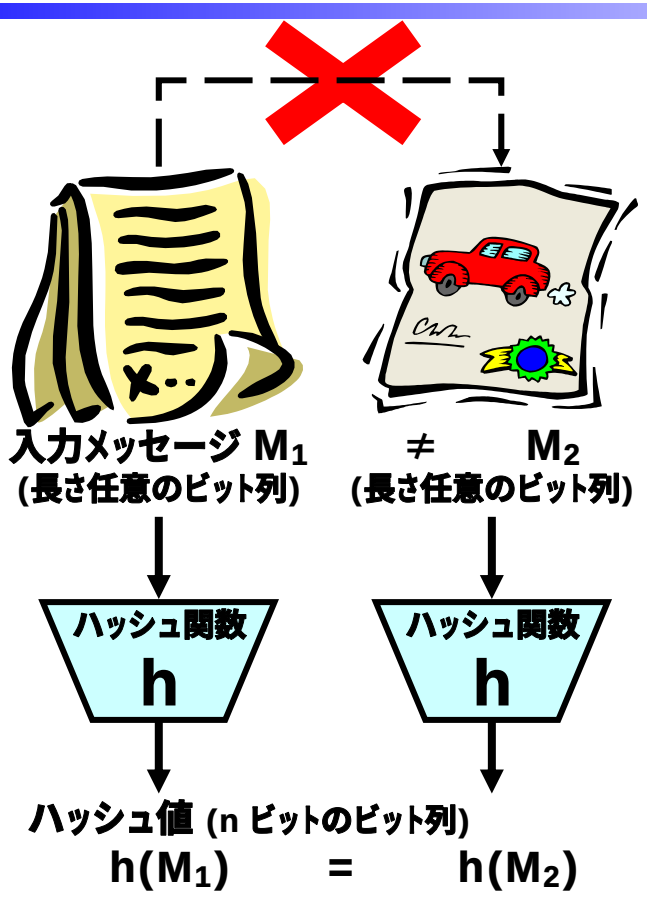
要件:
ハッシュ関数 h において、
異なる入力 メッセージの組で等しいハッシュ値を有する (衝突する) もの (衝突、あるいは、衝突ペアという) 、すなわち、
$h(M_1) = h(M_2)$ かつ $M_1 \neq M_2$ を満たす組 (M_1, M_2) を一つでも求めることが、
十分に計算量を要し、困難であること。

事実:
衝突をみつけるために必要な計算量は、
ハッシュ値が n ビットであるとき、
ハッシュ関数の計算を $2^{n/2}$ 回行うための計算量を超えない。($2^{n/2} \ll 2^n$ に注意)

補足: 両方の入力メッセージを選べるところが、第2原像計算困難性とは異なる。
ハッシュ関数が衝突困難性を有するならば、第2原像計算困難性も有する。

ハッシュ関数に求められる安全性(3)

~第2原像計算困難性(Second Preimage Resistance)~

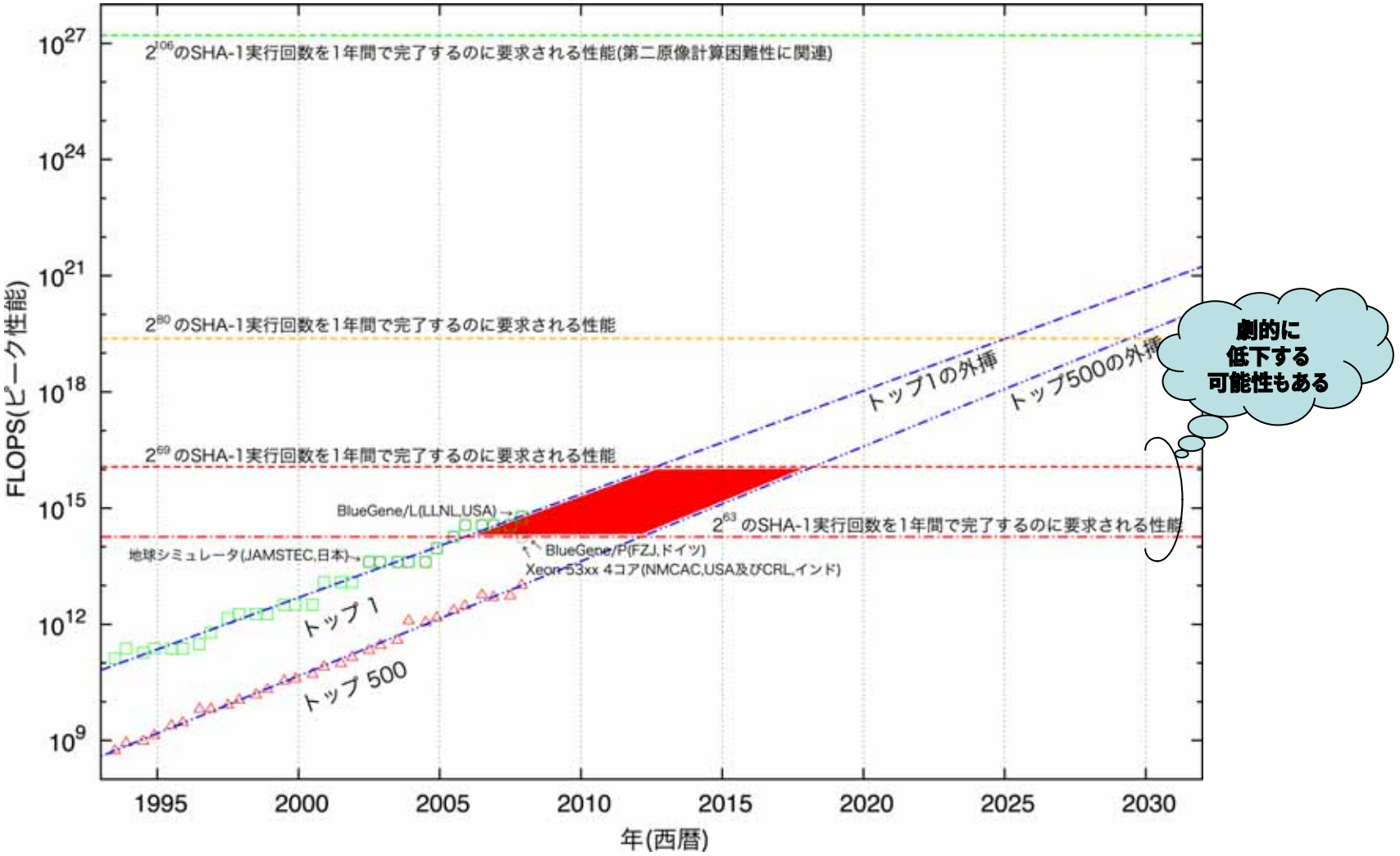


要件:
ハッシュ関数 h **において、**
与えられたどの入力メッセージ M_1 **に対しても、**$h(M_1)$ **と等しいハッシュ値を有する(衝突する)** M_1 **とは異なる入力メッセージ(第2原像という)、すなわち、**
$h(M_1) = h(M_2)$ **かつ** $M_1 \neq M_2$ **を満たす** M_2 **を、一つでも求めることが、十分に計算量を要し、困難であること。**

補足:第2原像は、一般にいくらでもあるが、それを具体的に求められるかどうかを問題としている。

事実:
第2原像をみつけるために必要な計算量は、ハッシュ値が n **ビットであるとき、ハッシュ関数の計算を** 2^n **回行うための計算量を超えない。**

SHA-1の安全性
- 衝突発見に必要な計算量 -



ハッシュ関数危殆化の影響

- 衝突発見
  - 電子文書の偽造が可能
    - 電子文書には、細工できる場所が多い
    - 細工されていても、気がつかない。
    - 必要な計算量が著しく低下すると、証明書も偽造される
      - MD5を用いた証明書の偽造例
        - » http://eprint.iacr.org/2006/360.pdf
        - » http://www.win.tue.nl/hashclash/TargetCollidingCertificates/TargetCollidingCertificatesAnnouncementv1.1.pdf
- 第2原像攻撃
  - 証明書の偽造が可能
  - 公開鍵基盤の危機

暗号屋としてのリコメンド

- **公開鍵暗号系**
  - **移行方針**：RSA1024→RSA**2048**
    - **課題**：RSA2048**の次をどうしましょう？**
- **ハッシュ関数**
  - ASH (**現在は、**SHA-3**と呼称**)
  - 2012**年を目標に**SHA-3**を開発**
    - **「『予定』は『未定』」**
  - **移行方針**：SHA-1→SHA256
    - SHA-3**実使用可能時期は、2～3年後？**
    - IETF**の動向は？**
    - SHA-3**実用化前に、**SHA-1**が危機的状況を迎えることは？**
      - **現実的な計算量での第2原像攻撃が出現した場合**
      - **衝突発見に必要な計算量が著しく低下したとき**
    - **「衝突発見」に伴う「風評被害」の予防**