報道発表
2012年6月18日

次世代暗号の解読で世界記録を達成

ペアリング暗号の安全性を確立し次世代暗号の標準化に貢献

九州大学
富士通研究所
情報通信研究機構

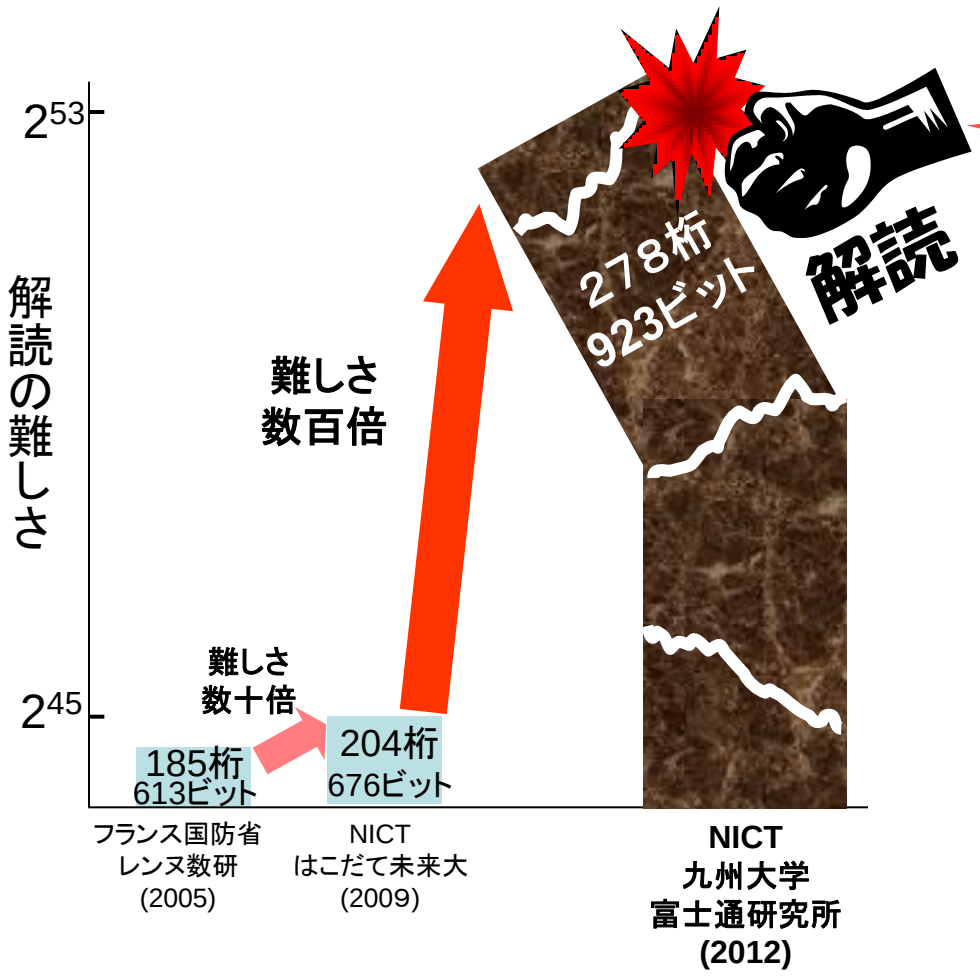
九州大学

FUJITSU

NICT 独立行政法人 情報通信研究機構

報道発表

278桁のペアリング暗号解読成功・世界記録達成



923ビット以下は
危険だ！！

目次

- 全体（高木，九州大学）
  - 研究の背景・課題・結果
- 技術（下山，富士通研）
  - 暗号技術の紹介
- 成果（篠原，NICT）
  - 今回の成果と今後

現代社会と暗号技術

昔の暗号

限られた人だけが使う特殊技術

現代の暗号

身近なもの

http://www.e-gov.go.jp/

暗号は現代社会に無くてはならない技術

暗号技術の進歩と広がり

	暗号の主な目的
計算機以前 古代・中世・近代	機密文書の秘匿
インターネットの普及 1990年代～	電子商取引・ネットワークセキュリティ
携帯端末の発展 2000年代～	著作権保護・ユビキタス端末認証
クラウドの登場 2010年代～	プライバシ保護・暗号データ検索

新しい暗号技術が登場し、応用先が拡大

暗号の歴史は解読技術の歴史

暗号の安全性検証サイクル

暗号の安全性検証サイクル

公開の場で議論・検証する

提案フェーズ

暗号のストレステスト

この攻撃はどうだ？

新しい解読
アルゴリズム

安全性検証フェーズ

何ビットの鍵長が安全？

10年程度の
サイクル

実用化フェーズ

鍵長の寿命

計算機スピードの向上
暗号解読技術の進歩

実用化されている公開鍵暗号の歴史

1980年　1990年　2000年　2010年

n=pq

第一世代
RSA暗号

安全性検証
512ビット

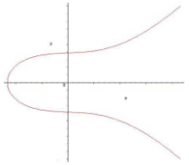
標準化
実用化

安全性検証
1024ビット

バージョン
アップ

安全性検証
2048ビット

バージョン
アップ



第二世代
楕円暗号

安全性検証
160ビット

標準化
実用化

安全性検証
192ビット

バージョン
アップ

第三世代
ペアリング暗号

安全性検証
???ビット

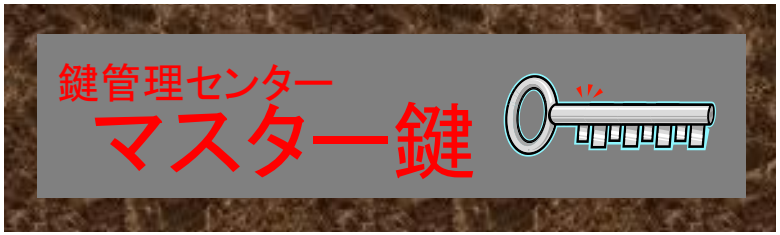
標準化
実用化

今回の成果

旧世代では実現できない高機能な暗号応用を達成
IDベース暗号、検索可能暗号、関数型暗号など

今回の成果概要

ペアリング暗号の安全性 ⟺ 鍵管理センター マスター鍵

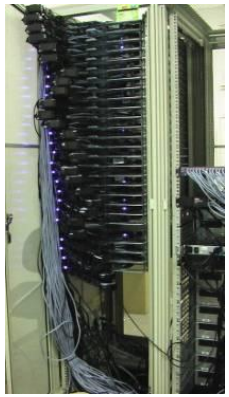


解読不可能と考えられていた鍵長の解読に成功

解読したマスター鍵 (公開鍵が278桁923 ビットに相当する)

d = 175279958485066813773020730619813142455096730 0

暗号解読世界記録達成！



解読実験データ

- 延べ計算日数: 148.2日
- 汎用コンピュータ: 21台（252コア）
- Intel Xeon 1コアで102年分の計算時間に相当

解読に用いた計算機

構成メンバ、役割分担、成果

産

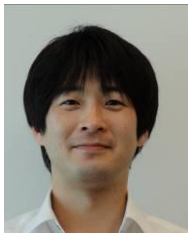
下山武司　富士通研究所　主任研究員

暗号解析・情報セキュリティの研究に従事
2008年情報処理学会喜安記念業績賞、IWSEC2009最優秀論文賞

解読アルゴリズム設計･プログラム並列化･解読実験進捗管理

➡ (産) 顧客に対して安全で便利な情報セキュリティサービスの提供可能

官



篠原直行　情報通信研究機構　研究員

数式処理・暗号理論の研究に従事
2008年度日本数式処理学会奨励賞

理論検討･パラメータの最適化･計算機導入

➡ (官) 電子政府向け暗号の安全な鍵長の設定や将来の危殆化予想に貢献

学

高木剛　九州大学マス･フォア･インダストリ研究所　教授

暗号理論・計算整数論の研究に従事
2009年船井情報科学振興賞、国際暗号学会CHES2011プログラム委員長

林卓也　九州大学大学院数理学府　博士後期課程3年生

暗号解析の研究に従事（富士通とNICTでインターンシップ）
情報処理学会CSS2009学生論文賞、電子情報通信学会SCIS2010論文賞

プロジェクト推進管理･プログラミング･計算機管理･実験実施

➡ (学) 離散対数問題など数学や情報科学の未解決問題へ挑戦

本成果はバランスのとれた産官学共同研究の成果

暗号技術について

～暗号解読までの道のり～

暗号の歴史は、解読の歴史

- **シーザー暗号**　紀元前

  古代ローマの皇帝
  ジュリアス・シーザーが使用

  弱点：単純、暗号文字に偏り

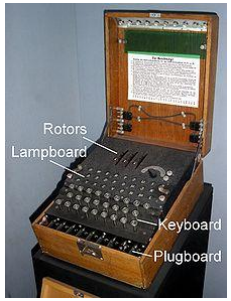
例：　I　LOVE　YOU
　　↓　13文字ずらす
　　V　YBIR　LBH

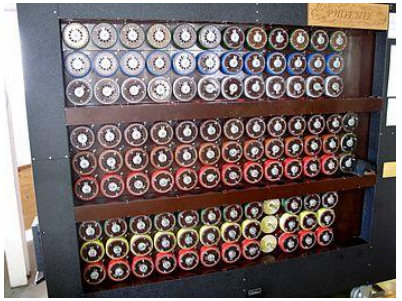
アメリカ南北戦争時に
使用された暗号円盤(*)

- **ENIGMA**　第二次大戦中

  ナチスドイツが使用した機械式暗号

  弱点：運用ミス＋解読計算機の登場



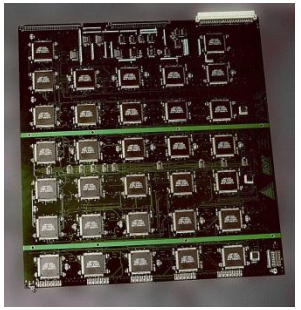


Enigma暗号装置(*)　イギリスが作った解読装置(Bombe) (*)

- **DES**　20世紀末(1970～1997)

  米国標準暗号、0と1の数列を計算機で暗号化

  弱点：秘密鍵の短さ＋計算機の進歩



「DES Cracker」
解読専用LSI(米国EFF) (*)

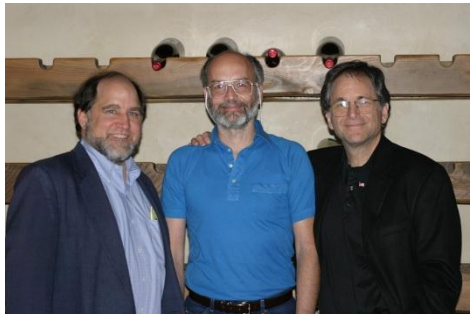
(*)出典 wikipedia

現代の暗号は、数学そのもの

- **RSA暗号**

  1977 年に発明された暗号
  インターネットの本格的な普及に貢献

  解読には 素因数分解



RSA暗号を開発した
Rivest, Shamir, Adleman(*1)

- **ペアリング暗号**

  2001年ごろ開発された新しい暗号
  今までの暗号では出来なかった応用が可能

  解読には ？？？

ペアリング暗号研究集会
のシンボルマーク(*2)

*1: 出典 USC http://www.usc.edu/dept/molecular-science/RSA-2003.htm
*2: 出典 International Conference Paring 2012

ペアリングってどういう意味?

「ペアリング(Pairing)」とは

数字の組(pair)を、うまく1個にする(～ing)数式。
これを暗号に応用したのが「ペアリング暗号」。

$$b = a^x$$

(簡略版)

ペアリングの数式

$$\eta_T(Q_\pi, Q_\pi) = \eta_T(Q_\pi, Q_e)^x$$

ペアリング暗号の解読

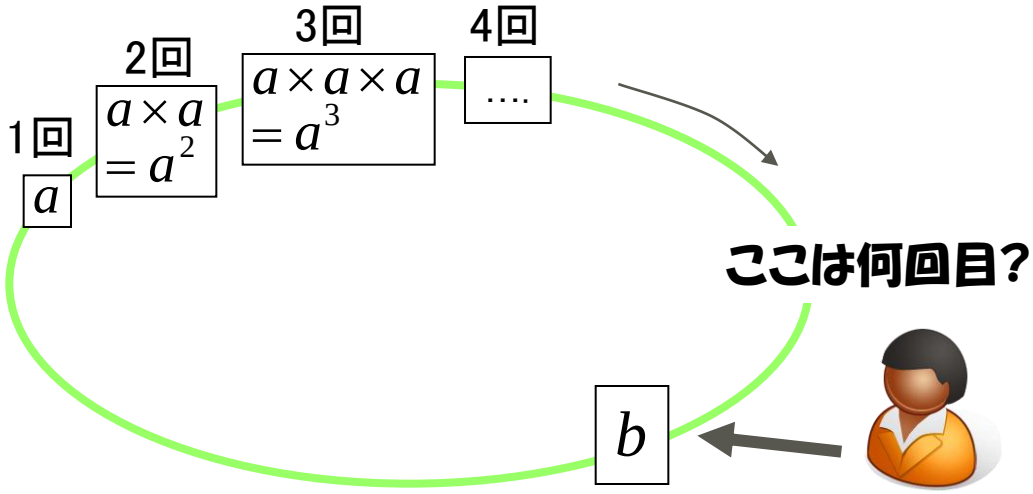
ペアリング暗号を解読するには、

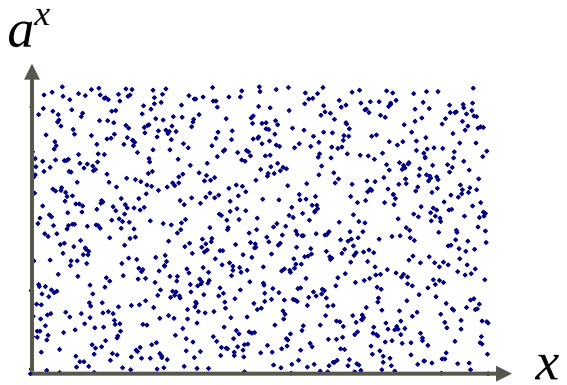
- **数式から 解 を求める**

$$b=a^{x}$$

ペアリング暗号の数式
（簡略版）

つまり、同じ数を繰り返し掛け算した「回数」を求める





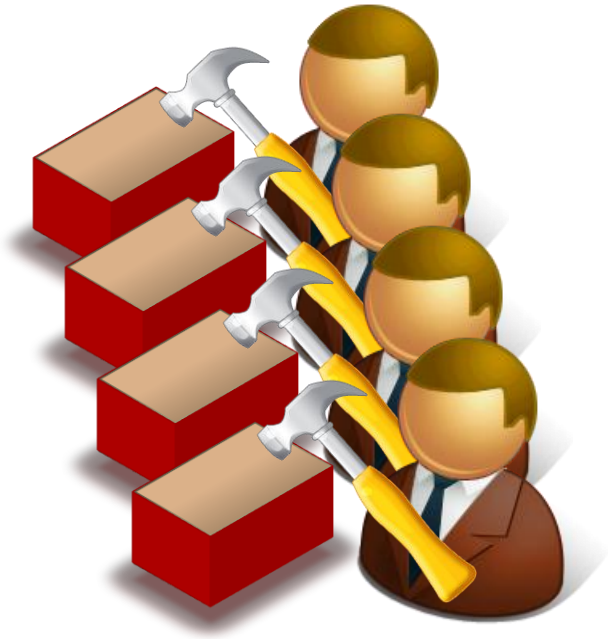
※ 数式のグラフ

暗号解読の基本アイデア

大きな1個の数式を解く → 変換 → **大量の小さい式を解く**

暗号の解読

計算しやすい



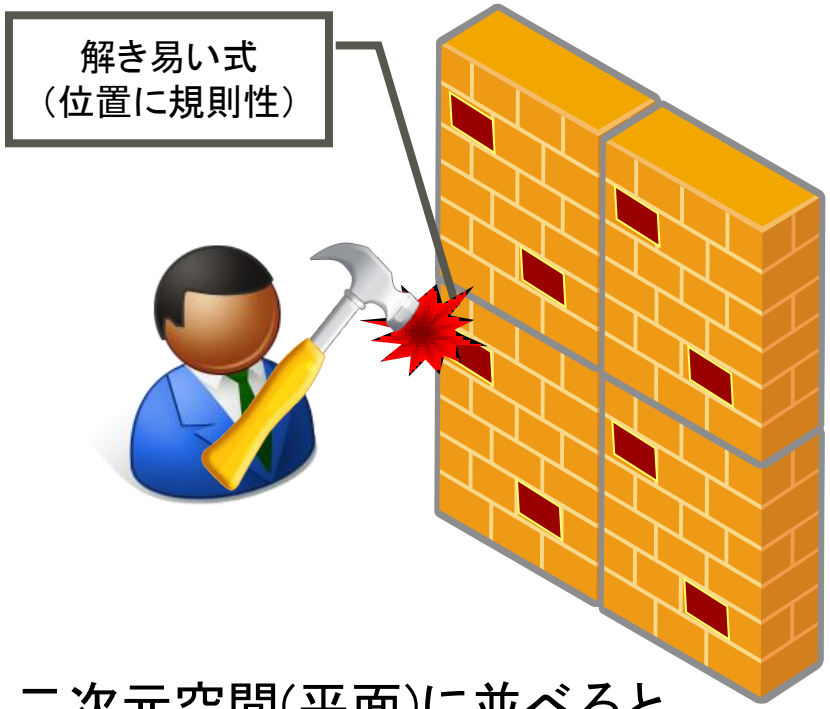
新しい解読法

「データ探索を二次元空間に拡張」

従来

解き易さに関係なく
1個ずつ順に解く

新しい解読法



二次元空間(平面)に並べると、
解き易い式に規則性があることに着目。
ポイントを絞って解く。

数十倍の効率化

ペアリング暗号解読までの紆余曲折

2010.4 ～2011.3	1年目：新理論と新攻撃法
	•データ探索を二次元空間に拡張 •数式を使って初期値を最適化
2011.3.11	**東日本大震災** **その後の節電や人手不足等、様々な影響で、約3ヶ月間遅延**
2011.4 ~2012.4	2年目:プログラミングと計算機実験
	•膨大な数値データから方程式の解を高速に計算 •計算機のパワーを限界まで引き出す並列プログラミング **「計算機パワーが足りない!」⇒新たに計算機増強。** **「あれ？計算に2万年かかる!」 ⇒プログラムミス発見。解決。** **「最後の計算が合わない!」⇒データのコピーミス！再計算…** **等々ありましたが、ついに…**

解読成功！

From: Shimoyama Takeshi
Subject: [dlp-tech 609] Re: ind log
Date: Tue, 24 Apr 2012 14:57:49 +0900

下山です。

> log_eta(pi, e) eta(pi, pi) = 1752799584850668137730207306198131424550967300

ECDLP でチェックし、合っていることを確認しました。

世界記録達成です！

On Tue, 24 Apr 2012 14:42:30 +0900
Takuya Hayashi wrote:
>
> 林です。
>
> log_eta(pi, e) eta(pi, pi) = 1752799584850668137730207306198131424550967300
>
> でチェックが取れました。
>

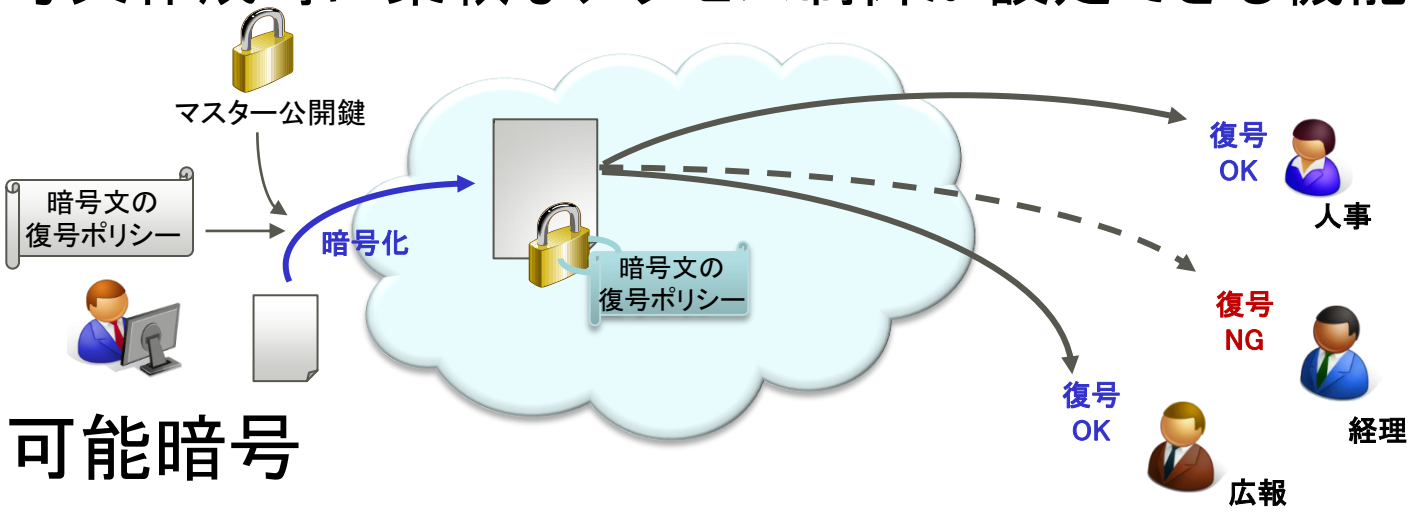
今回の成果と今後について

～ペアリング暗号の利用・普及に向けて～

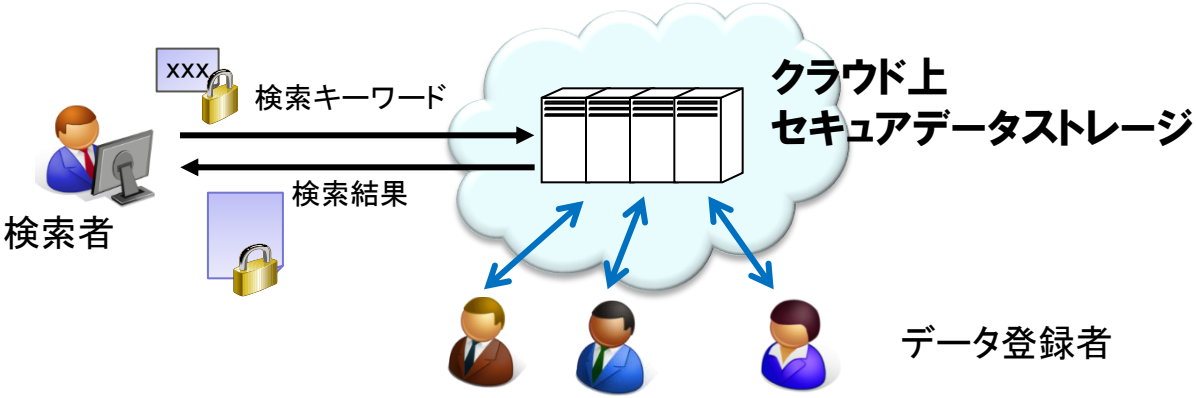
ペアリング暗号への期待：クラウドへの応用

今までの暗号では
実現不可能な機能

- 関数型暗号
  - 暗号文作成時に柔軟なアクセス制御が設定できる機能



- 検索可能暗号
  - 暗号化したままキーワード検索ができる機能

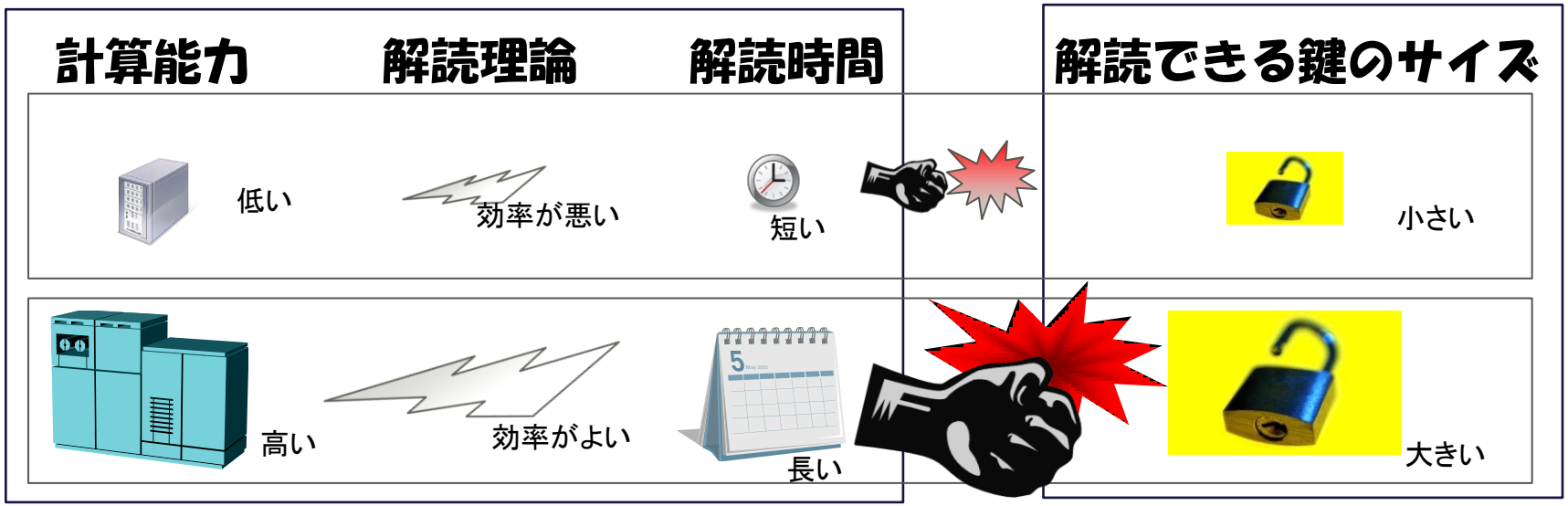


ペアリング暗号の安全性評価

ペアリング暗号の実用化
- 暗号応用
- 高速処理
- 安全性

検証が十分になされていない！

・暗号の安全性にからむ要素



ペアリング暗号の安全性評価

・安全性の目安

スーパーコンピューター
（世界一）

最新の理論とプログラム

1年

解読できる
最大の鍵長は？

知りたい！

現実的な計算能力

最新の理論とプログラム
（最良な計算方法は同じく利用）

？日

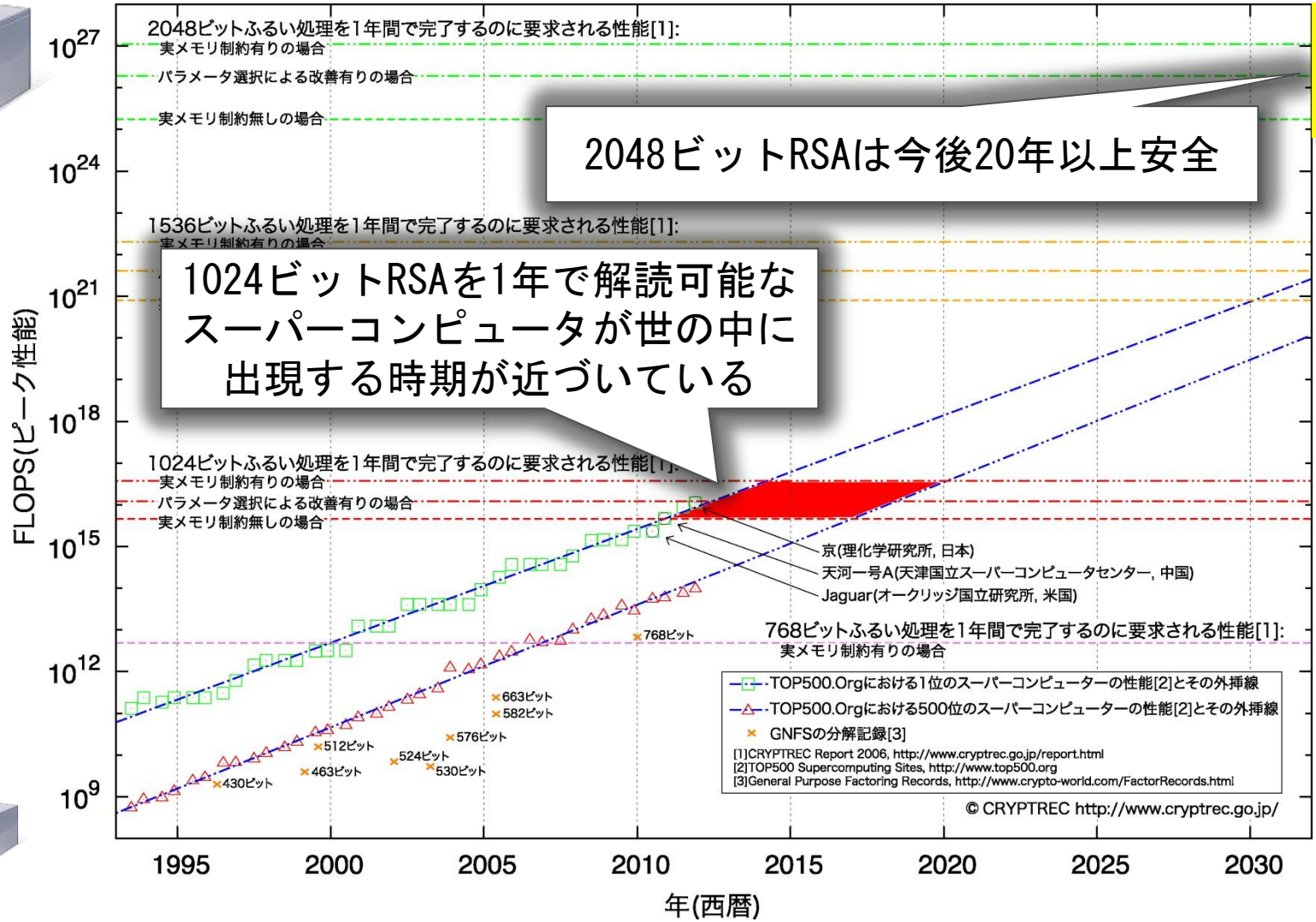
923ビット
（誤差が小さくなるように、**可能な限り大きく**）

世界記録

（例）RSA暗号の安全性予測

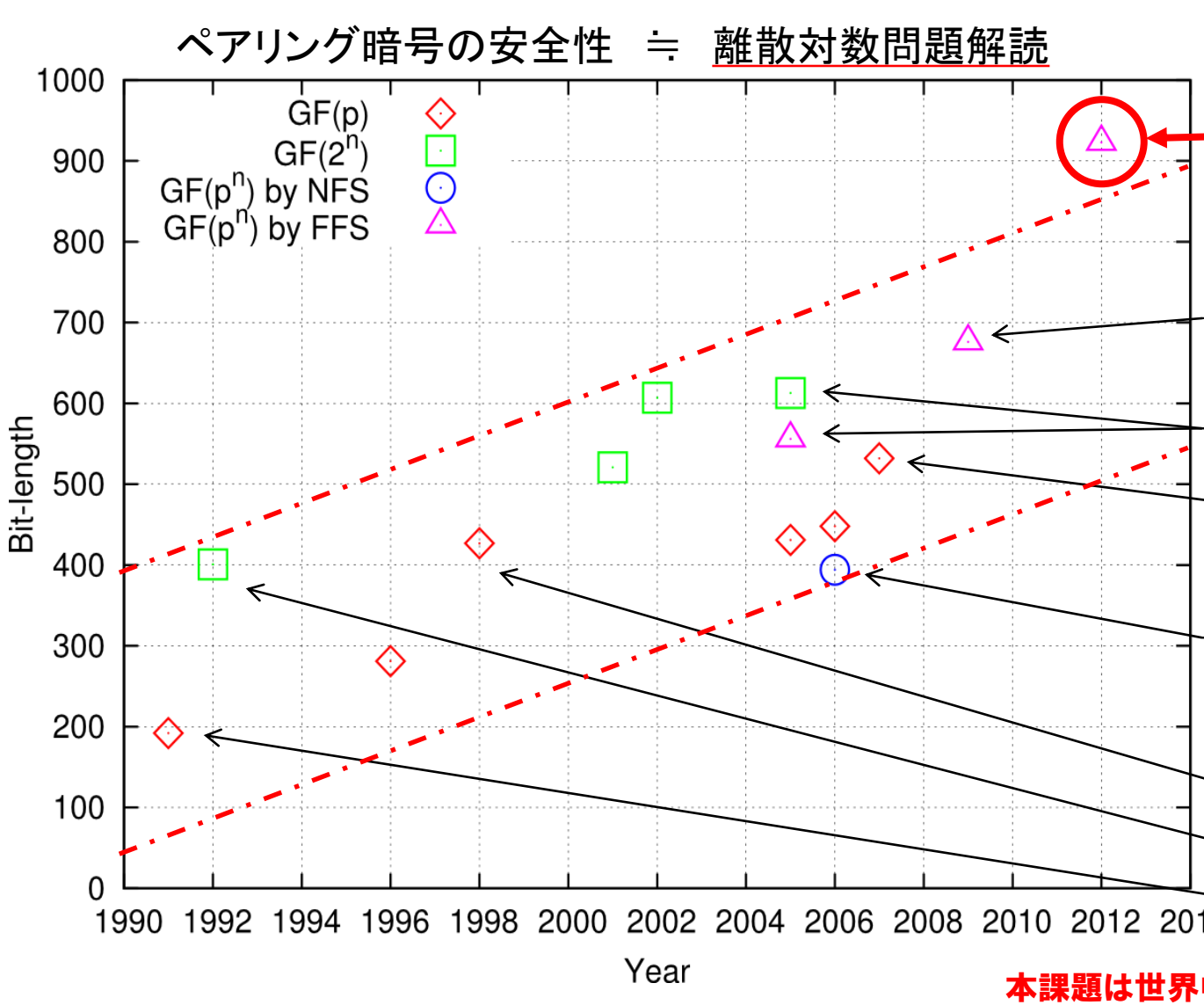
2048ビット
RSA

1024ビット
RSA



出典：暗号技術検討会 2011年度報告書

離散対数問題の解読世界記録の推移



今回の記録

NICT
九州大学
富士通研究所

はこだて未来大学
NICT

フランス・レンヌ大学
フランス国防省
ドイツ・ボン大学

フランス・レンヌ大学
フランス国防省
英・ブリストル大学
ベルギー・ルーベン大学

ドイツ・ザールランド大学

米・サンディア国立研究所

米・AT&T

本課題は世界中で活発に研究されてきた。

スーパーコンピュータを使った場合

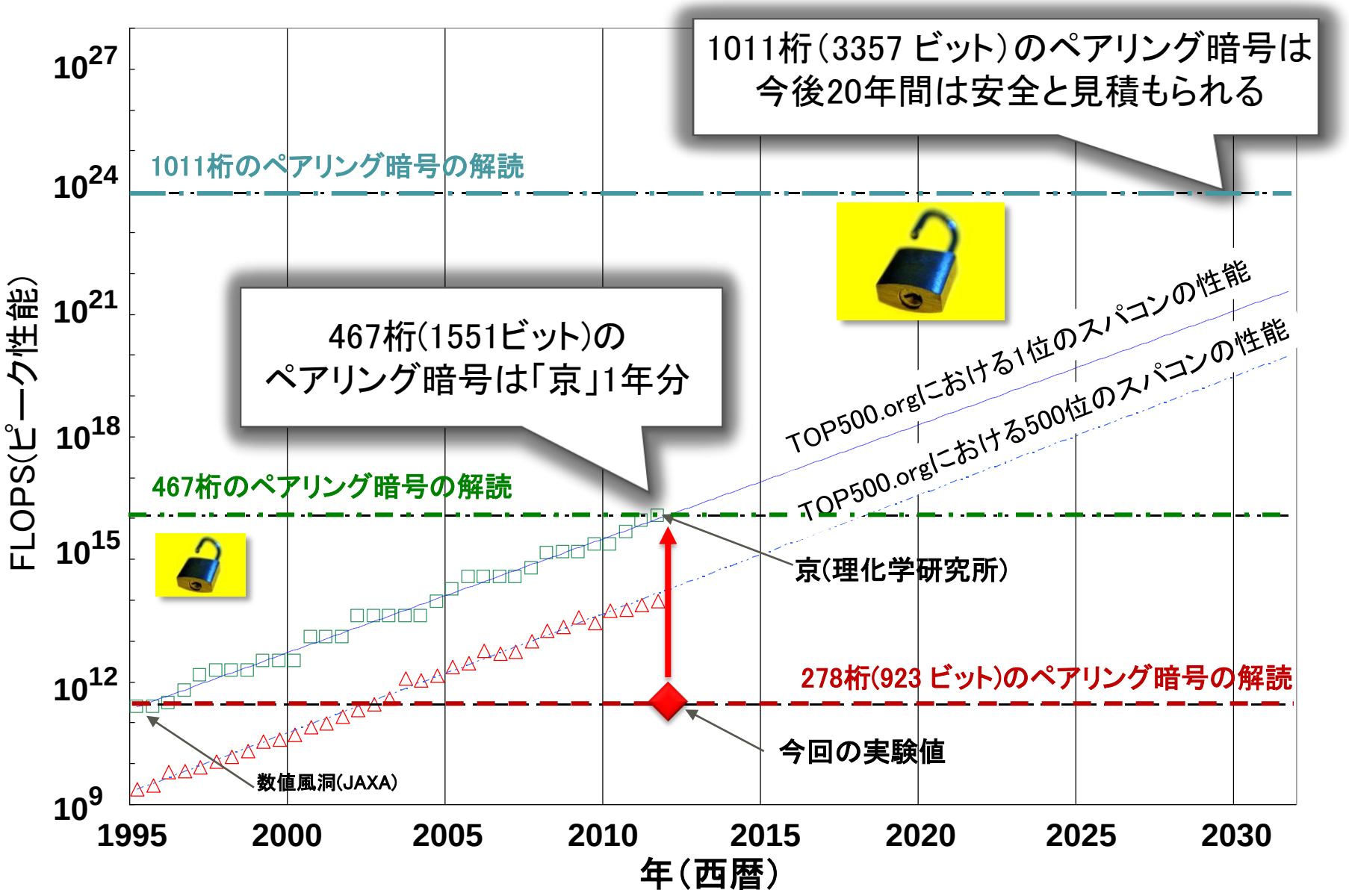
- 「京」(理化学研究所)
  - 1秒間に1京510兆回の浮動小数点演算ができるスパコン、富士通が開発
  - 2011年11月のスパコンランキング(TOP500)で、二期連続世界一

出典:理化学研究所

「京」の場合、今回の解読は当初**7.84年**相当の計算量

⇒解読方法の改良により**13.6分**に短縮！

安全なペアリング暗号は？



おわりに

- 多様な機能を実現する次世代公開鍵暗号として期待されている**ペアリング暗号**の安全性を評価した.
  - 安全性の根拠となっている**離散対数問題**の解読に挑戦.
  - **923ビット(278桁)の世界記録**を達成.
- ペアリング暗号の利用・普及に向けた第一歩
- 次世代暗号の標準化に貢献

(参考)ペアリング暗号の標準化動向

- IETF (Internet Engineering Task Force)
  - インターネットで利用される技術の標準化が進められている.
    - RFC5091 (2008): Identity-Based Cryptography Standard #1
    - RFC6508 (2012): Sakai-Kasahara Key Encryption

- IEEE (Institute of Electrical and Electronics Engineers)
  - IEEE P1363で公開鍵暗号全般の規格化が進められている.
    - IEEE P1363.3: Identity-Based Public Key Cryptography

- ISO/IEC JTC 1/SC27
  - 情報セキュリティ技術全般の国際標準化が進められている.
    - ISO/IEC 15946-5:2009, 情報技術 – セキュリティ技術 – 楕円曲線に基づく暗号技術 – 第5部: 楕円曲線生成

（参考）暗号解読の詳細（1）

解読した278桁の問題

$$\eta_T(Q_\pi, Q_e)^d = \eta_T(Q_\pi, Q_\pi)$$

$\eta_T(Q_\pi, Q_e) =$ 38800433495886595565794915117804301791956216126496
33753505427783629422269455264138068189689559795615
25344816410211431123312860924749088840134929946466
03722768262812502860133243856659609561406642571204
16986352367189380157271639015105245955171916153471
46090159708100336066775046 62（278桁）

$\eta_T(Q_\pi, Q_\pi) =$ 46734287517443010590455305354067475501311488858023
81578307764073517759202353742150374302890696257225
81076700842040576294159856312834601074257816660641
32894617609106484411671094954678248957612636298995
16934064158793581339938909792543958763103189737927
56292385366006478348254765 38（278桁）

解読結果

d = 175279958485066813773020730619813142455096730 0

（参考）暗号解読の詳細（2）

問題設定

有限体 $GF(3^{97}) = GF(3)[X]/(X^{97} + X^{16} + 2)$ 上の超特異楕円曲線

$$E(GF(3^{97})) : Y^2 = X^3 - X + 1$$

上の２点 $Q_\pi = (Int(\pi) + 4, Y_\pi), Q_e = (Int(e) + 15, Y_e)$ を定め、

楕円曲線から η_T ペアリングを用いて有限体 $GF(3^{582})$上の離散対数問題に変換

$$\eta_T(Q_\pi, Q_e)^d = \eta_T(Q_\pi, Q_\pi)$$

ただし、$Int(\pi), Int(e)$ は、円周率 $\pi = 3.14159...$ と自然対数の底 $e = 2.71828...$ をそれぞれ97桁の3進数に変換した値（問題の恣意性を排除）

（参考）ペアリング暗号の解読はどれぐらい難しい？

我々以前の結果

問題の桁数	解読の難しさ
204桁（676ビット）	解読可能
278桁（923ビット）	解読に数十万年

従来の世界記録

実質的に解読不可能

先行適用として、
既に多くの利用あり。

新攻撃法を使うと

問題の桁数	解読の難しさ
204桁（676ビット）	$2^{45.30}$
278桁（923ビット）	$2^{52.79}$

従来の世界記録から
数百倍難しい難問

手が届くかどうか？！

2^{40}	個人レベル
2^{50}	組織レベル
2^{60}	国家レベル

※計算の難しさのレベル