資料3

SHA-1及びRSA1024の安全性評価について

【暗号技術検討会事務局】
【暗号技術監視委員会事務局】

１．暗号技術検討会の概要

【暗号技術検討会事務局】

暗号技術検討会の概要

目的

客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化して、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられた、国民が安心して利用できる電子政府の構築に貢献する。

これまでの経緯

① 平成13年度から総務省大臣官房総括審議官及び経済産業省商務情報政策局長の研究会として本検討会を開催

② 平成13年10月、情報セキュリティ対策推進会議（事務局：内閣官房内閣安全保障・危機管理室（現：NISC））において本検討会の結果等を踏まえて、総務省及び経済産業省が「電子政府」における調達のための推奨すべき暗号のリストを作成する旨の「電子政府の情報セキュリティ確保のためのアクションプラン」が了承

③ 平成15年2月、「電子政府」における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表

④ 同月、行政情報システム関係課長連絡会議において（事務局：総務省行政管理局）、電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の「各府省の情報システム調達における暗号の利用方針」が了承

⑤ 平成18年6月、現行の主要な暗号技術の一つであるSHA-1の安全性についての見解を公表

今年度の主な検討課題

① 電子政府推奨暗号リストの見直しのための新たな暗号技術の公募方法の検討

② 電子政府推奨暗号の安全性及び信頼性確保のための調査・検討

③ 電子政府推奨暗号リストに関する調査・検討

④ 暗号モジュールセキュリティ要件及び試験要件の作成

⑤ 暗号技術の危殆化が想定より急速に進んだ場合の緊急事態対応策の検討　等

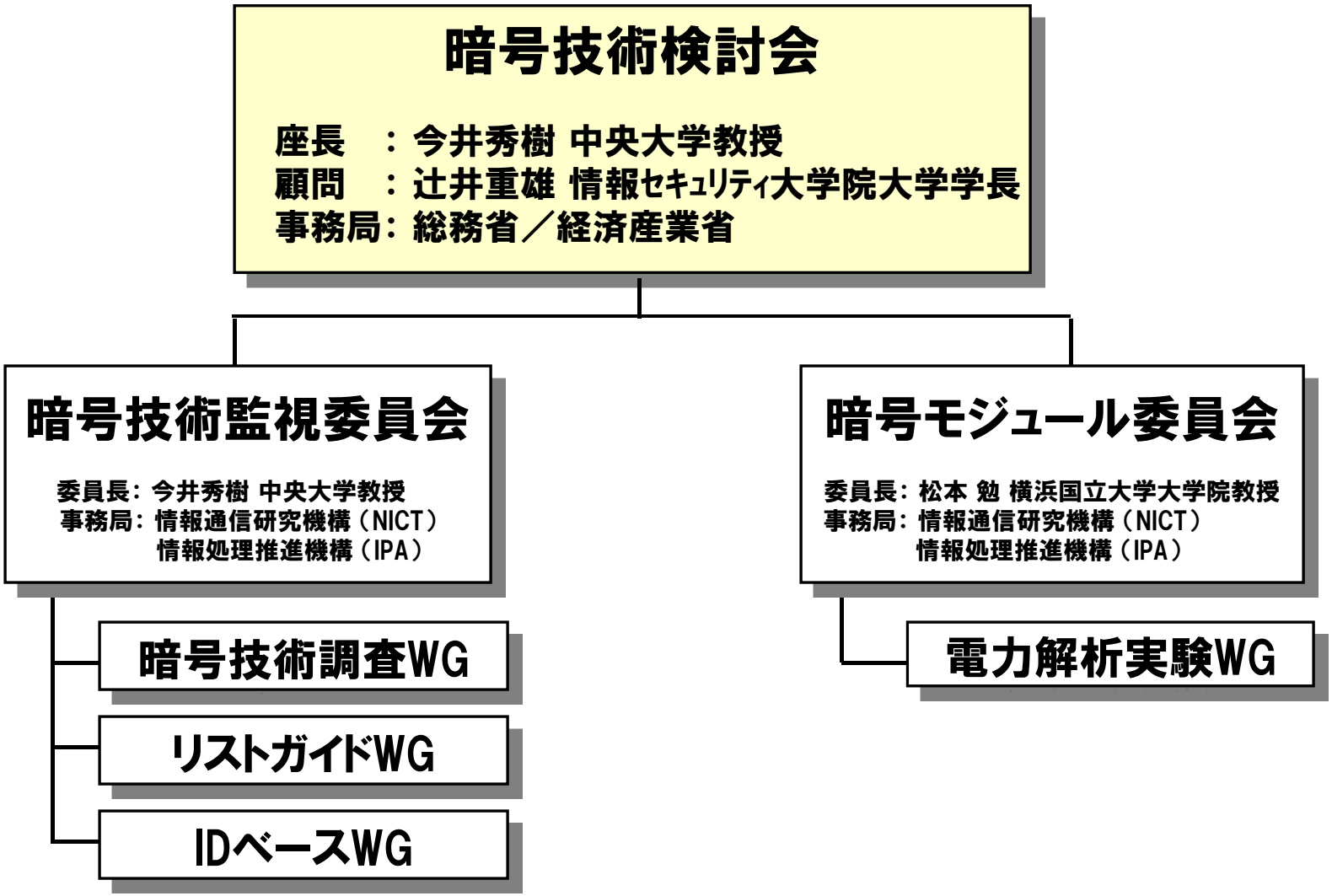
今後の予定

① 平成21年度から新しい暗号技術の公募を開始予定

② 平成24年度末までに新たな電子政府推奨暗号リストを公表予定

CRYPTRECの構成

※ CRYPTREC：Cryptography Research and Evaluation Committees



（検討会及び各委員会の役割）

暗号技術検討会：　暗号技術に関する総合的観点からの検討、政府内のセキュリティ関係機関との連携等

暗号技術監視委員会：　電子政府推奨暗号の安全性に関する日常的な監視、暗号アルゴリズムを対象とする調査等

暗号モジュール委員会：　暗号モジュールセキュリティ要件及び試験要件を作成、暗号実装関連技術を対象とする調査等

暗号技術検討会の構成員

（平成20年8月末現在、敬称略）

座長	今井　秀樹	中央大学理工学部電気電子情報通信工学科教授
顧問	辻井　重男	情報セキュリティ大学院大学学長
	岩下　直行	日本銀行金融研究所情報技術研究センター長
	太田　和夫	電気通信大学電気通信学部情報通信工学科教授
	武市　博明	情報通信ネットワーク産業協会常務理事
	岡本　栄司	筑波大学大学院システム情報工学研究科教授
	岡本　龍明	日本電信電話株式会社情報流通プラットフォーム研究所 主席研究員（（社）電気通信事業者協会代表兼務）
	加藤　義文	（社）テレコムサービス協会技術委員会委員長
	金子　敏信	東京理科大学理工学部電気電子情報工学科教授
	国分　明男	（財）ニューメディア開発協会常任理事・開発グループ長
	櫻井　幸一	九州大学大学院システム情報科学研究院教授
	佐々木　良一	東京電機大学未来科学部情報メディア学科教授
	宝木　和夫	（社）電子情報技術産業協会 情報セキュリティ委員会委員
	苗村　憲司	情報セキュリティ大学院大学教授
	松井　充	三菱電機株式会社情報技術総合研究所 情報セキュリティ技術部長
	松本　勉	横浜国立大学大学院環境情報研究院教授
	松本　泰	次世代電子商取引推進協議会 電子署名認証サブワーキンググループリーダ

電子政府推奨暗号リスト

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈:

（注 1）　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

（注 2）　KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

（注 3）　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注 4）　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1）　FIPS46-3 として規定されていること

2）　デファクトスタンダードとしての位置を保っていること

（注 5）　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

（注6）　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

（注7）　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

電子政府推奨暗号リストに関する修正情報

修正日付	修正箇所	修正前	修正後	修正理由
平成１７年１０月１２日	注釈の注4）の1）	FIPS46-3として規定されていること	SP800-67として規定されていること	仕様変更を伴わない、仕様書の指定先の変更

SHA-1の安全性に関する見解

SHA-1の安全性に関する見解

平成18年6月28日
暗号技術監視委員会

電子政府における情報セキュリティ確保のために、各府省の情報システム構築において暗号を利用する場合には、「各府省の情報システム調達における暗号の利用方針」（平成15年2月28日　行政情報システム関係課長連絡会議了承）において、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされている。
また、情報セキュリティ政策会議から出された「政府機関の情報セキュリティ対策のための統一基準（2005年12月版（全体版初版））」（平成17年12月13日）においても、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択することが基本遵守事項として明記されている。
電子政府推奨暗号リストでは、ハッシュ関数のSHA-1は注釈において、『（注6）新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。』と規定している。
SHA-1については、最近の研究動向によれば、Wangらにより2^{69}回以下のSHA-1の実行回数で同じハッシュ値を持つ2つのメッセージが発見できる衝突探索攻撃アルゴリズムが発表され、CRYPTRECで検証した結果、2^{69}回のSHA-1の実行回数で衝突発見できることの妥当性は検証された。また、近い将来に2^{63}回以下のSHA-1の実行回数で衝突発見できることも妥当性があるとの結論を得た。このことは、SHA-1を長期間にわたって利用する電子署名やタイムスタンプなどは、近い将来にSHA-1の衝突発見が現実的な問題に発展する可能性を示唆している。
　このようなことから、電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、SHA-256ビット以上のハッシュ関数の使用を薦める。

＊参照：CRYPTREC Report 2005「暗号技術監視委員会報告」
http://cryptrec.jp/

（参考）

　各種文献等を踏まえ、以下の参考情報を提供する。ただし、CRYPTRECとして、ここで引用した文献等の内容の正確性、信頼性、妥当性を保証するものではない。
　ハッシュ関数のSHA-1を利用している電子署名システムにおいて、仮に2^{63}回のSHA-1の実行回数で衝突が起こるということになれば、例えば、一般に用いられているCPUで構成される「PCクラスタ型」[i]のスーパーコンピュータのうち2006年4月現在で国内最高速のもの[ii]を使用して約7年間計算すると、同じハッシュ値を生成する異なる文書などが作成できる可能性がある。
　具体的には、電子署名された原文と同一の電子署名を生成できる別の文書が作成（偽造）され得るということであり、電子署名された文書（原文）の真がんの判断ができなくなるおそれがある。
　現時点では、電子署名された文書の有効性に疑問は生じていないが、SHA-1の衝突に関する最近の研究結果は、今後、暗号研究の進歩やコンピュータ処理能力の向上[iii]などによって、文書の有効期間が本来よりも著しく短縮され、電子署名された文書であっても、否認、なりすまし又は改ざんといった脅威にさらされる危険性があることを示唆している。

衝突発見に要する時間の目安（推定）

SHA-1の実行回数	2006年4月現在
2^{69}回	・国内最高速のスパコンで約462年以下
2^{63}回	・国内最高速のスパコンで約7年以下

処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得るため、この年数はあくまで推定である。なお、今後の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステム[iv]によっても、本推定以上の衝突発見能力を実現できる可能性がある。

注：現在のURLはhttp://www.cryptrec.go.jp/

２．SHA-1及びRSA1024の安全性評価

【暗号技術監視委員会事務局】
情報通信研究機構(NICT)
情報通信セキュリティ研究センター
セキュリティ基盤グループ

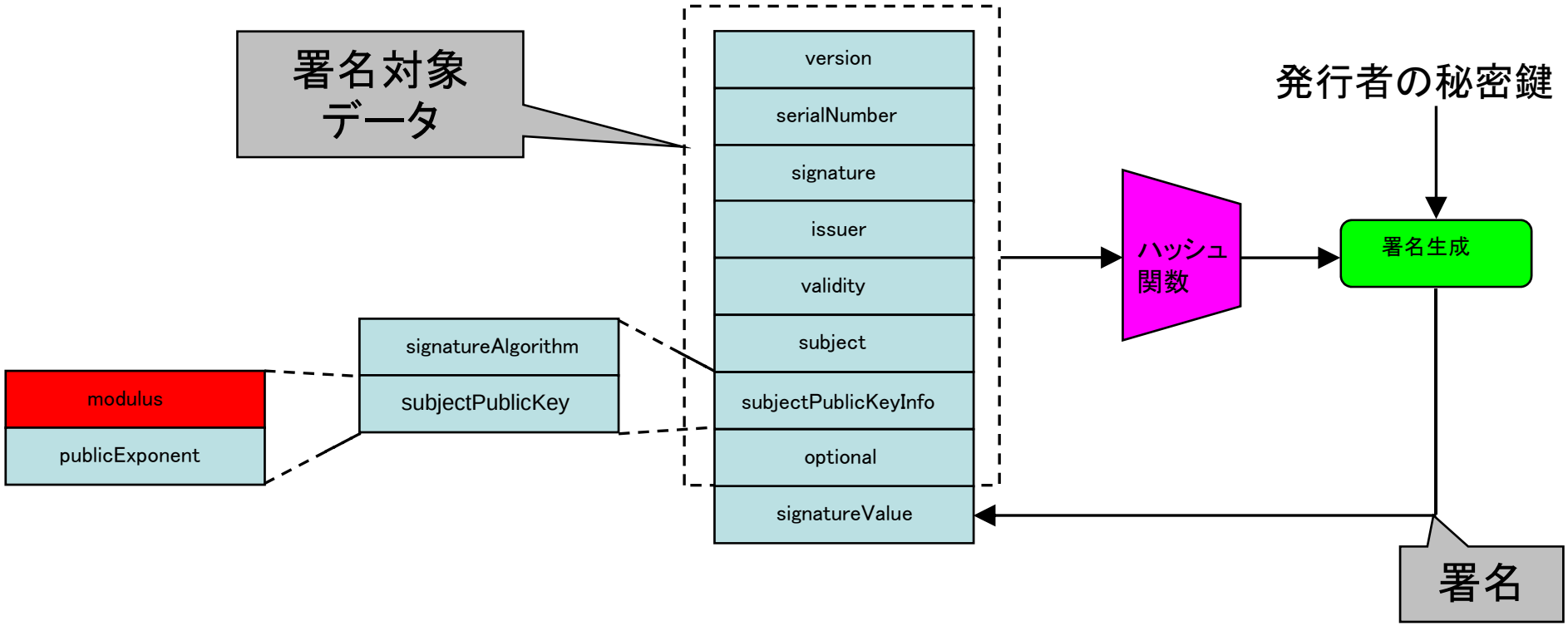
目次

２．１　はじめに

公開鍵暗号によるディジタル署名

- 添付型(with appendix)…署名対象の文書と署名が別々になっているもの。
  - 決定的(deterministic)…同一の文書に対する署名が常に同一なもの。
    - 例:RSASSA-PKCS1-v1_5(PKCS #1 v1.5)
  - 確率的(probabilistic)…同一の文書に対する署名が常に異なる。
    - 例: RSASSA-PSS(PKCS #1 v2.1)
- メッセージ回復型(with giving message recovery)…署名から元の文書を復元できるもの。
  - 決定的(deterministic)
    - 例: ISO/IEC 9796-2
  - 確率的(probabilistic)
    - 例: PSS-R(Bellare-Rogaway Eurocrypt'96)

例：X.509証明書



例： sha1withRSAEncryption（RSASSA-PKCS1-v1_5を利用）

- ●モジュラス（相異なる2つの素数の積で、サイズは1024ビット等）
- ●公開指数(65537等)
- ●ハッシュ関数（SHA-1）

ディジタル署名のセキュリティ要件

- データの作成者の特定（ユーザー認証）
- データにおける改ざんの検出（メッセージ認証）
- 署名を生成した事実の否認の防止（否認防止）

RSA署名への攻撃のタイプ

- 受動的攻撃
  - 署名検証用の鍵のみを用いて署名を偽造されるタイプ。
    - 同程度の大きさの相異なる2つの素数（pとq）の積（N=p・q）は、公開されているので、合成数Nを分解することにより、pとqを求められないよう、Nは十分大きな数でなければならない。
      - 素因数分解問題の困難性
        - ≫ この部分に問題があると、署名アルゴリズム部分に脆弱性がなくても、すべてのセキュリティ要件が無効となってしまう可能性がある。
- 能動的攻撃
  - 入手した署名等を用いて別の文書を偽造されるタイプ。
    - 署名アルゴリズム部分の暗号学的な強度
      - ハッシュ関数の暗号学的な強度（ユーザー認証以外のセキュリティ要件が無効となってしまう可能性がある。）
        - ≫ 衝突発見困難性
        - ≫ 第2原像計算困難性
        - ≫ 原像計算困難性
      - その他

２．２　RSA１０２４の安全性について

素因数分解問題とは

- 同程度の大きさの2つの相異なる素数p,qの積である合成数Nが与えられたときに、その素因数p,qを求める問題。
  - Nに含まれる最小素因数の大きさに依存して計算量が決まるもの。
    - 楕円曲線法（The Elliptic Curve Factorization Method）が現在、最速のアルゴリズム
  - Nの大きさに依存して計算量が決まるもの。
    - 一般数体ふるい法（The General Number Field Sieve）が現在、最速のアルゴリズム

一般数体ふるい法の計算量

- 合成数Nの場合、

$$L_N[\frac{1}{3}, \left(\frac{64}{9}\right)^{\frac{1}{3}} + o(1)], \quad \left(\frac{64}{9}\right)^{\frac{1}{3}} = 1.9229994\cdots$$

- と漸近的な評価がされている。ただし、

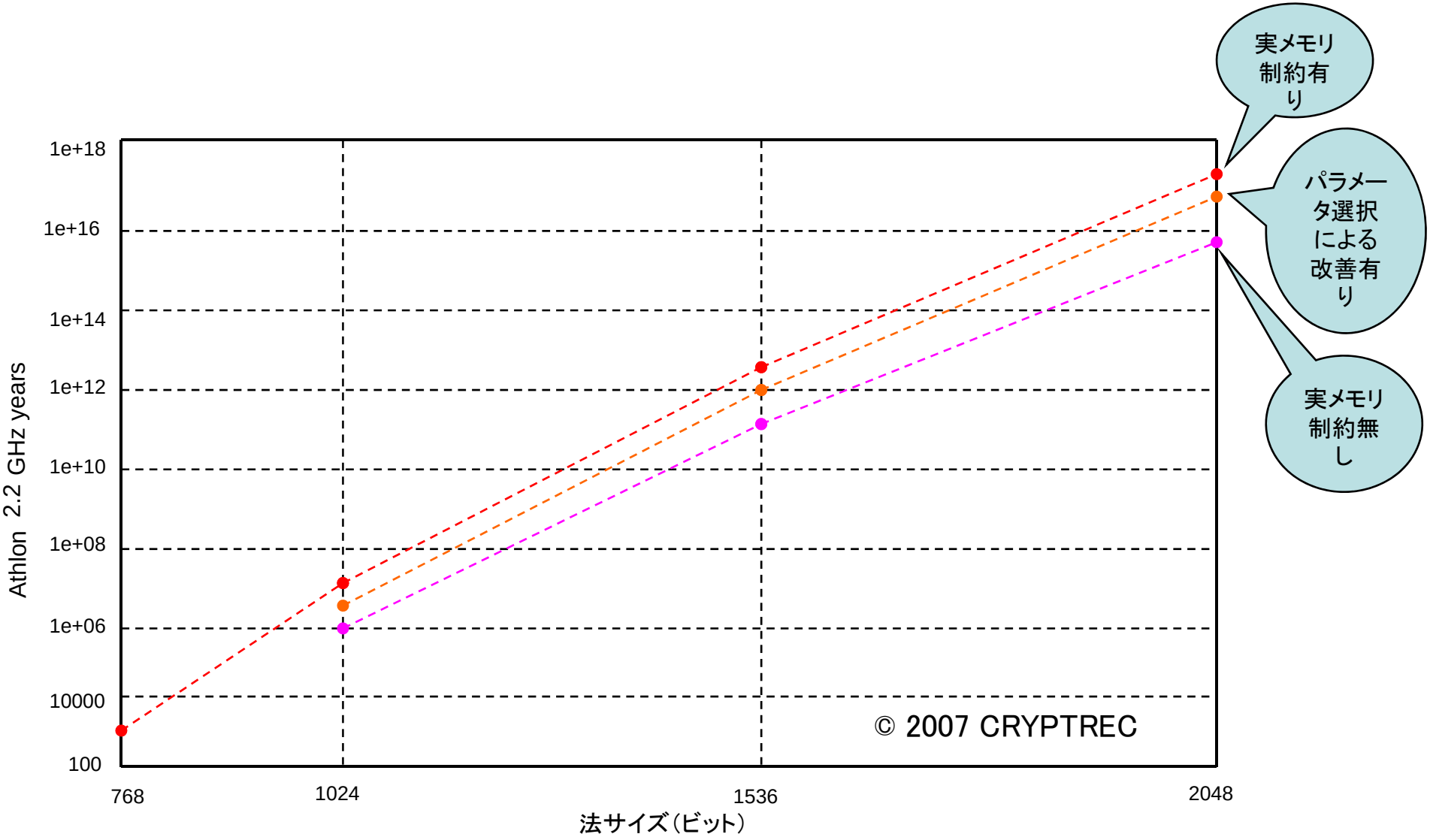
$$L_N[s, c] = \exp\left(c(\log N)^s (\log\log N)^{1-s}\right)$$

- o(1)はN->∞のとき0に近づく関数である。
  - 見積の際、注意して扱わないと誤差が大きくなる。

今回の評価方法

- 漸近的な評価式であるL_Nは利用せず、部分的に実験を行い、「ふるい処理」の計算量を推定した。
  - Dickman関数という特殊な関数を利用して、“ smooth ”（滑らか）な数の出現確率を評価している。
    - 用語説明：“smooth”であるとは、ある上界B以下の素数の集合F（factor baseと呼ばれる）の元で完全に素因数分解できることをいう。

今回の評価結果


実メモリ制約有り
パラメータ選択による改善有り
実メモリ制約無し
1e+18
1e+16
1e+14
1e+12
1e+10
1e+08
1e+06
10000
100
Athlon 2.2 GHz years
768
1024
1536
2048
法サイズ（ビット）
© 2007 CRYPTREC

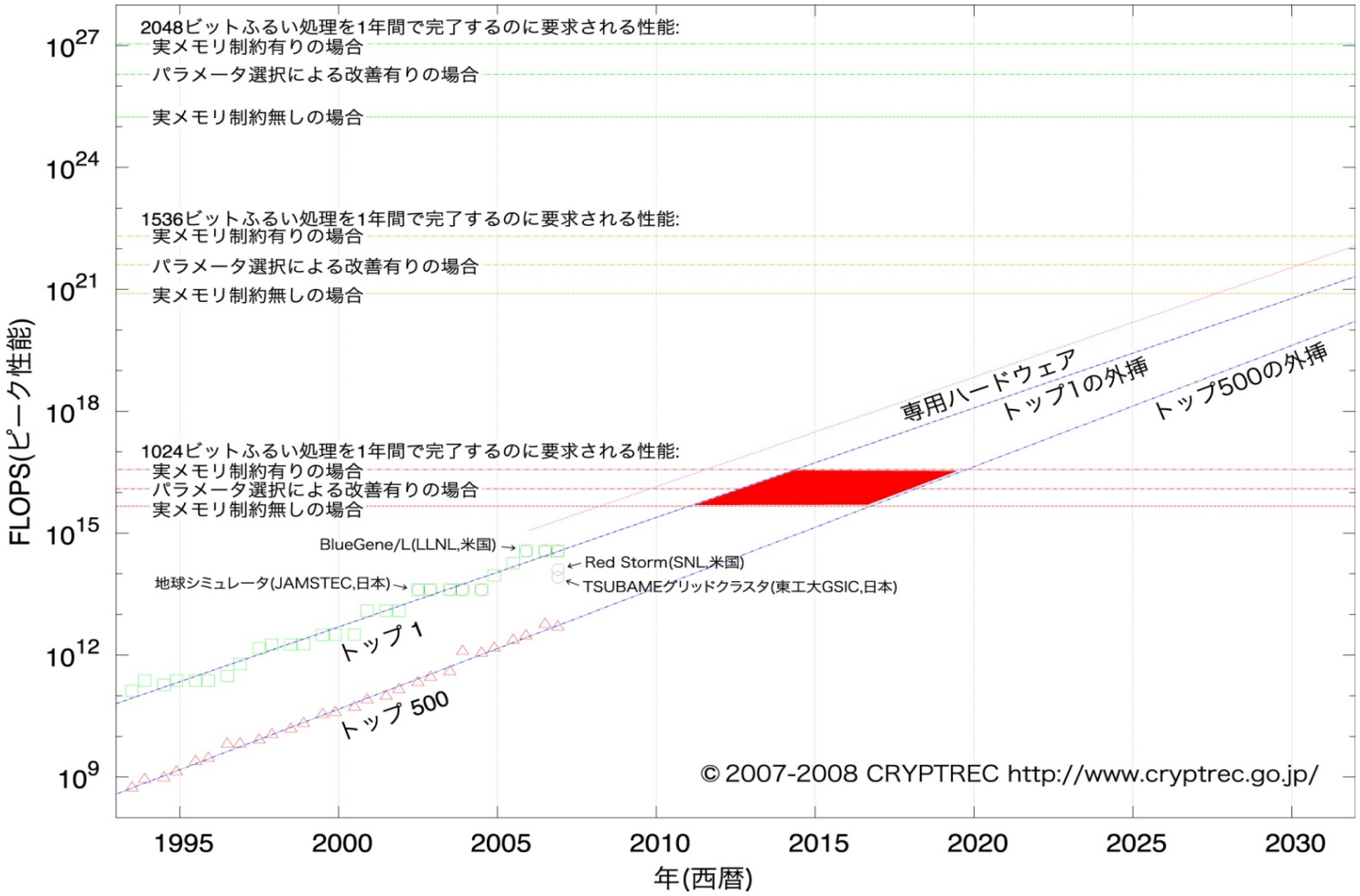
「計算量」と「年」の間の換算の難しさ

- 計算機の種類や能力にさまざまな違いがあるので、非常に難しい。
  - Blazeら論文（1996年）によるコストの区分は以下の通り。
    - Pedestrian Hacker: tiny ～ $400
    - Small Business: $10,000
    - Corporate Department: $300K
    - Big Company: $10M
    - Intelligence Agency: $300M
      - DES解読の際に威力を発揮したFPGA(Field Programmable Gate Array)やASIC(Application Specific Integrated Circuit)で代表させている。
  - CRYPTRECでは、分かり易さから、スーパーコンピュータ（スパコン）で代表させた。TOP500.Orgにおけるデータを利用している。
    - トップ1辺りのスパコンの価格は、$100M程度のコストと報道されている。

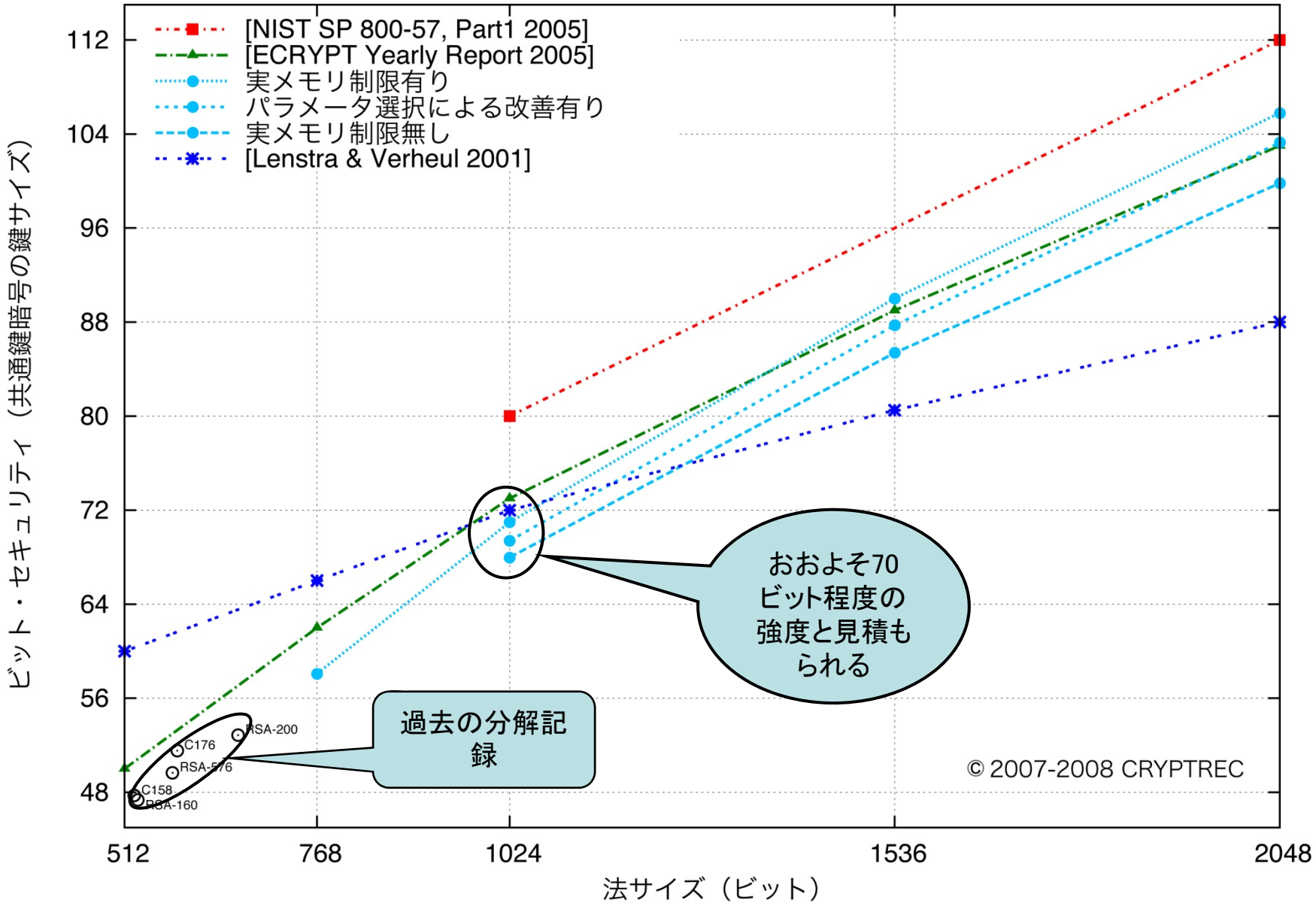
換算における注意事項

- 計算量に関する前提
  - これから30年間はブレークスルーがなく、一般数体ふるい法が最も効率の良いアルゴリズムである。
  - 漸近的な評価において、ふるい処理と線形代数処理は同じオーダーであること、一般数体ふるい法の世界記録においてこれまでのところふるい処理の方が多くの時間を要していることから、ふるい処理時間の方を重視した。
- 計算機に関する前提
  - 高性能な計算機としてスパコンを代表させた。
  - 整数演算性能と浮動小数点演算性能を、ほぼ同等（1：1）とした。
- 換算に関する前提
  - 暗号解読アルゴリズムの処理は、通常、整数演算を用いるので、整数演算性能で比較するのが妥当であるが、上述の前提により、浮動小数点演算性能への換算をおこなった。

1年間でふるい処理を完了するのに要求される処理性能の予測（CRYPTREC Report 2006）



ビット・セキュリティに関する比較



２．３　SHA-1の安全性について

ハッシュ関数に求められるセキュリティ要件

- 衝突発見困難性
  - $H(M_1) = H(M_2)$を満たす文書M_1、M_2を計算することが計算量的に難しいこと。（注：あらかじめハッシュ値は分かっていない。）
- ターゲット型衝突発見困難性
  - 与えられた文書P_1、P_2に対して、$H(P_1 \| S_1) = H(P_2 \| S_2)$を満たす文書$S_1$、$S_2$を計算することが計算量的に難しいこと。なお、ここで、$X \| Y$は文書XとYの連結を意味する。
- 第2原像計算困難性
  - あらかじめ与えられている文書M_1に対して、$H(M_1) = H(M_2)$を満たす文書M_2を計算することが計算量的に難しいこと。
- 原像計算困難性
  - ハッシュ値Hに対して、$H(M) = H$を満たす文書Mを計算することが計算量的に難しいこと。

Wang教授による衝突発見攻撃

- MD5やSHA-1等のハッシュ関数では、入力文書をある固定長のブロック毎に分割してから、逐次処理するような仕様になっている。
- Wang教授は、1つ目のブロックと2つ目のブロックのそれぞれに差分を加え、かつ、それぞれのブロック及びハッシュ関数の内部変数に条件を与えることで、衝突発見の効率を高めることに成功した。（国際暗号学会IACR：Eurocrypt 2005 & Crypto 2005）
- 現在のところ、計算の結果発見される文書は、ランダムなデータなので、それ自体で意味をなすような文書になる確率は非常に低いが、バイナリなデータを適当に文書中に埋め込むことにより、文書の偽造が可能になる場合がある。

Lenstra教授らのMD5への攻撃研究

- On the possibility of constructing meaningful hash collisions for public keys (ACISP 2005)
  - Colliding X.509 Certificates – MD5の攻撃手法を使って、電子証明書に関する衝突を作成した。公開鍵を格納するフィールド等を調節することにより作成可能。
- Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities (EUROCRYPT 2007)
  - ターゲット型衝突発見攻撃の研究。
    - 計算量は、約2^{50}回(MD5計算)と見積もられている。

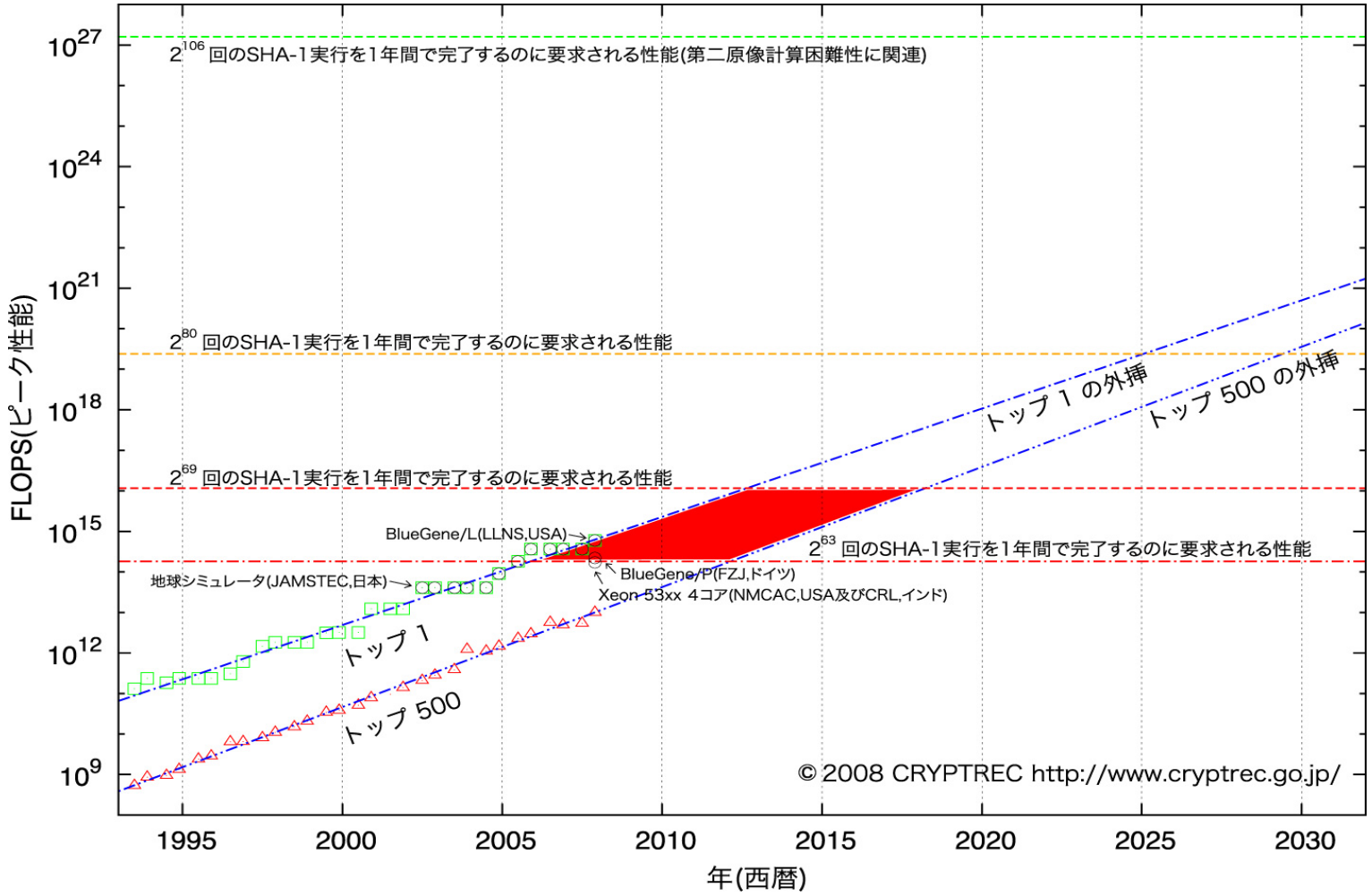
SHA-1の安全性評価について

◆SHA-1に対する攻撃については、Wangの2^{69}回のSHA-1実行回数の計算量による攻撃アルゴリズムの概略がCRYPTO 2005に先駆けてEurocrypt 2005のランプセッションとECRYPT on Hash Functionにおいて発表された。これ以外にもBiham,、Jouxなども SHA-1の攻撃結果を発表している。CRYPTO 2005では、Wangの攻撃アルゴリズムが正式に発表されたが、同時にランプセッションで計算量が2^{63}まで削減できるという発表があった。

◆2005年度のCRYPTRECでの評価結果

安全性評価
衝突発見困難性に対して、2^{69}回以下のSHA-1の実行回数で攻撃できる手法が発見された。ただし、公開された攻撃アルゴリズムには一部不明な点があり、第三者によって実装して検証されたわけではない。しかし、この攻撃アルゴリズムの不明な点は近い将来に明らかになり第三者による実装が可能になると予想されるので、本攻撃アルゴリズムは極めて大きな脅威になると考えられる。 第二原像計算困難性に対しては、2^{60}バイトのメッセージに対して2^{106}のSHA-1の実行回数で攻撃される手法が公開されたが、平成18年2月の時点で脅威とは言えない。

1年間で衝突を計算するのに要求される処理性能の予測（電子署名法検討会報告書 2008.05.30）



２．４　おわりに

- SHA-1の安全性
  - 衝突発見困難性のレベルは、現時点で63ビット以下。
    - スーパーコンピュータ・レベルのテクノロジとの比較では、2015 年前後には脅威となることが想定される。
  - ターゲット型衝突発見困難性のレベルは、まだ不確定である。
  - 第2原像計算困難性のレベルは、現時点で106ビット以下。
- RSA1024の安全性
  - 素因数分解問題の困難性のレベルは、現時点で70ビット以下。
    - スーパーコンピュータ・レベルのテクノロジとの比較では、概ね2015 年以降に脅威となることが想定される。