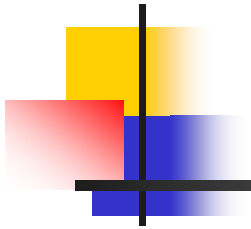
Internet Week 2009
H9: 3時間でわかるこれからの電子認証
～ (2) 暗号アルゴリズムの動向 ～

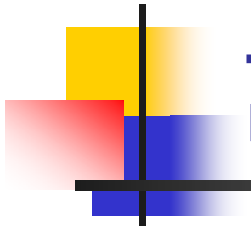
2009年11月25日

(独)情報通信研究機構
セキュリティ基盤グループ
黒川　貴司



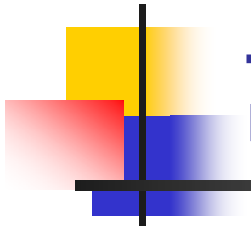
目次

- 認証
- 暗号アルゴリズム
- CRYPTREC活動
- 暗号アルゴリズムの動向



認証とは

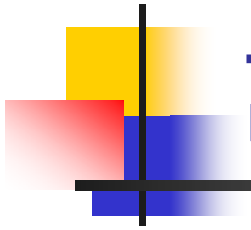
- コンピューター・システムで、対象の信頼性・正当性を確認すること。ユーザーの利用資格を確認することなど。暗号技術を用いて実現される。（広辞苑第６版より）
- （１）ネットワークを介した情報通信において、通信相手が、発信者が期待した正しい相手であること、あるいは通信内容が正当であることの保証。(2)ネットワークへアクセスする際の利用者や端末がそのネットワークの正当な利用者や端末であることの保証。（改訂 電子情報通信用語辞典、電子情報通信学会編、コロナ社）



認証とは（つづき）

- Entity authentication or identification
  - corroboration of the identity of an entity (e.g. a person, a computer terminal, a credit card, etc.)
- Message authentication
  - corroborating the source of information
- Certification
  - endorsement of information by a trusted entity

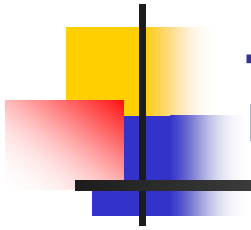
(Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, CRC Pressより)



認証システムの構成要素

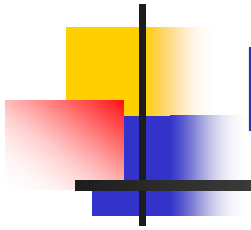
- 認証対象
- 識別特性
- 所有者
- 認証メカニズム
- アクセス制御メカニズム

（認証技術 パスワードから公開鍵まで、Richard E. Smith著／稲村雄監訳、オーム社より）



認証対象と識別特性

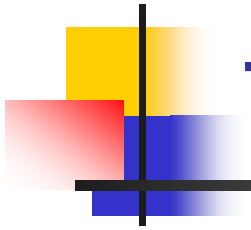
- システムへのログイン
  - 正規ユーザー／パスワード
- 銀行ATM
  - 口座の所有者／キャッシュカードと暗号番号
  - 口座の所有者／バイオメトリック（人の個人的特徴）
- Webサイト
  - Webサイトの所有者／SSLサーバー証明書



Entity Authenticationの分類

- ISO/IEC 9798-2
  - 対称暗号化アルゴリズムを使用するメカニズム
- ISO/IEC 9798-3
  - デジタル署名技術を使用するメカニズム
- ISO/IEC 9798-4
  - 暗号検査機能を使用するメカニズム
- ISO/IEC 9798-5
  - ゼロ知識証明技術を使用するメカニズム
- ISO/IEC 9798-6
  - 手動データ転送を使用するメカニズム

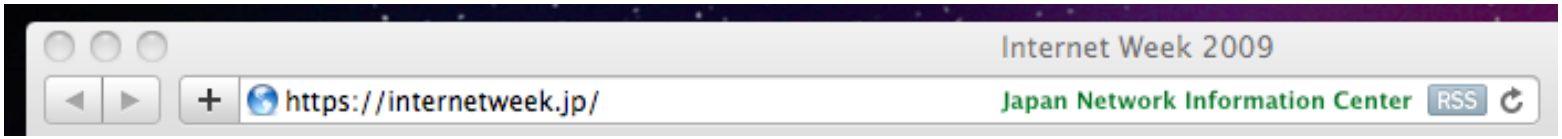
Challenge-and-Response プロトコル



- 秘密情報を開示することなく、秘密情報を知っていることを、検証可能な方法で示す。
  - 共通鍵暗号、公開鍵暗号を用いる方法
    - サーバーSが乱数rを生成し、rをユーザーUに渡す。
    - ユーザーUはrを暗号化し、その暗号文cをサーバーSに渡す。
    - サーバーSは渡されたcを検証する。
  - ゼロ知識証明を用いる方法
    - Schnorr方式
    - Fiat-Shamir方式

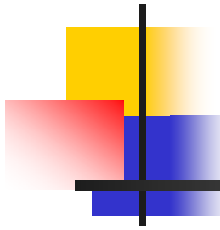
かくして暗号アルゴリズムは日常的に使われるようになった…

- インターネット上では
  - 例：SSL/TLSプロトコルの中で



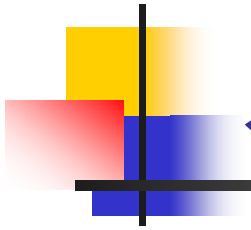
- 日常では
  - 例：無線LANのセキュリティプロトコルの中で
  - 例：ICカードの中で

よく使われている暗号アルゴリズムの代表選手

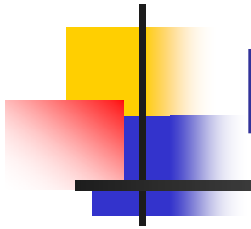


- ブロック暗号
  - DES
  - T-DES
- ストリーム暗号
  - RC4(Arcfour)

よく使われている暗号アルゴリズムの代表選手(つづき)



- ハッシュ関数
  - MD5
  - SHA-1
- 公開鍵暗号
  - RSA暗号



暗号アルゴリズムの危殆化

- ハッシュ関数MD5、SHA-1
- 素因数分解問題（1024ビットRSA型）

ハッシュ関数の安全性

- 衝突発見困難性
- Chosen-Prefix衝突発見困難性
  - 与えられた文書P_1、P_2に対して、ハッシュ値が等しくなるよう、

    $H(P_1 \| S_1) = H(P_2 \| S_2)$

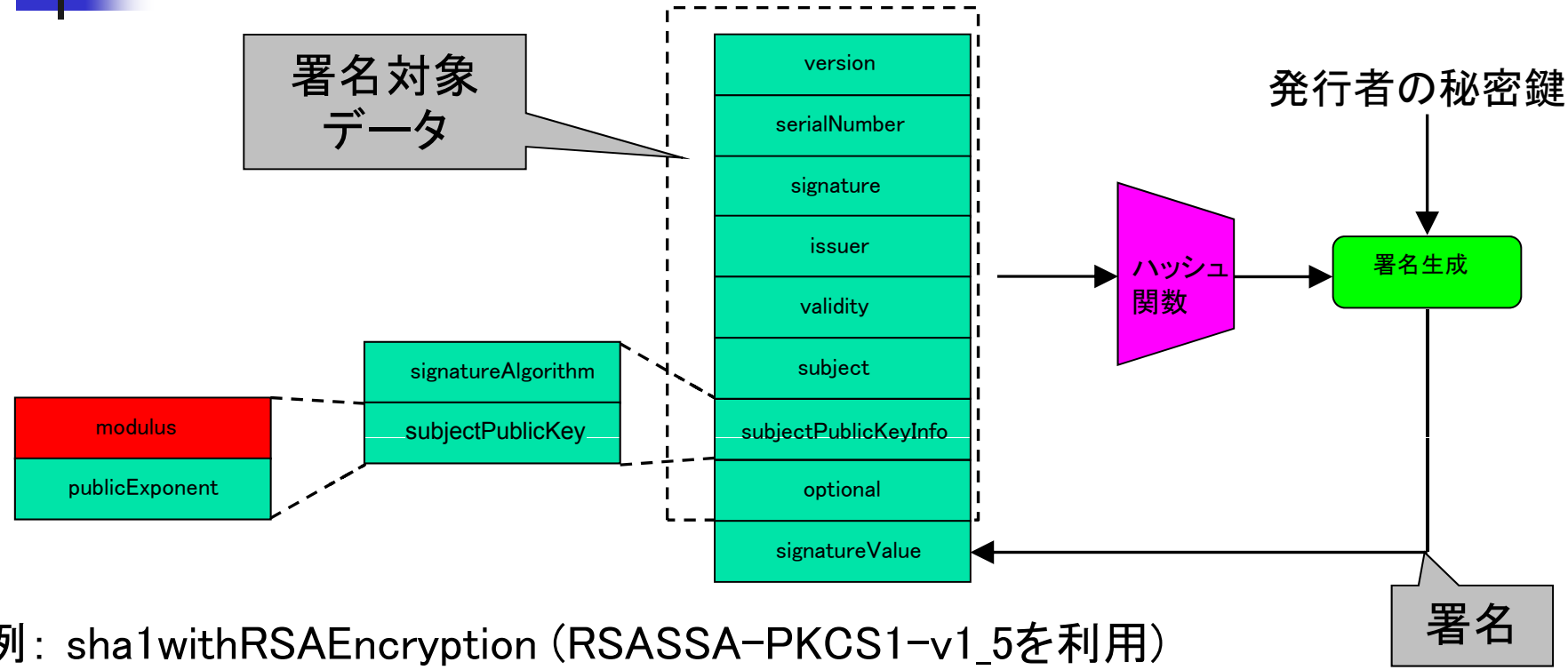
    を満たす文書S_1、S_2を計算することが計算量的に難しいこと。なお、ここで、$\|$は文書の連結を意味する。
- 第2原像計算困難性
- 原像計算困難性

MD5とSHA-1の衝突困難性

year	MD5		SHA-1	
	identical-prefix	chosen-prefix	identical-prefix	chosen-prefix
pre-2004	2^{64}(trivial)	2^{64}(trivial)		2^{80}(trivial)
2004	2^{40}			
2005	2^{37}		2^{69} 2^{63}	
2006	2^{32}	2^{49}		$2^{80-\varepsilon}$
2007	2^{25}	2^{42}	2^{61}	
2008	2^{21}			
2009	2^{16}	2^{39}	2^{52}	

“Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate,” Stevens,Sotirov,Appelbaum,Lenstra,Molnar,Osvik,Wegner, CRYPTO 2009, LNCS5677, pp.55-69, Springer, 2009 より

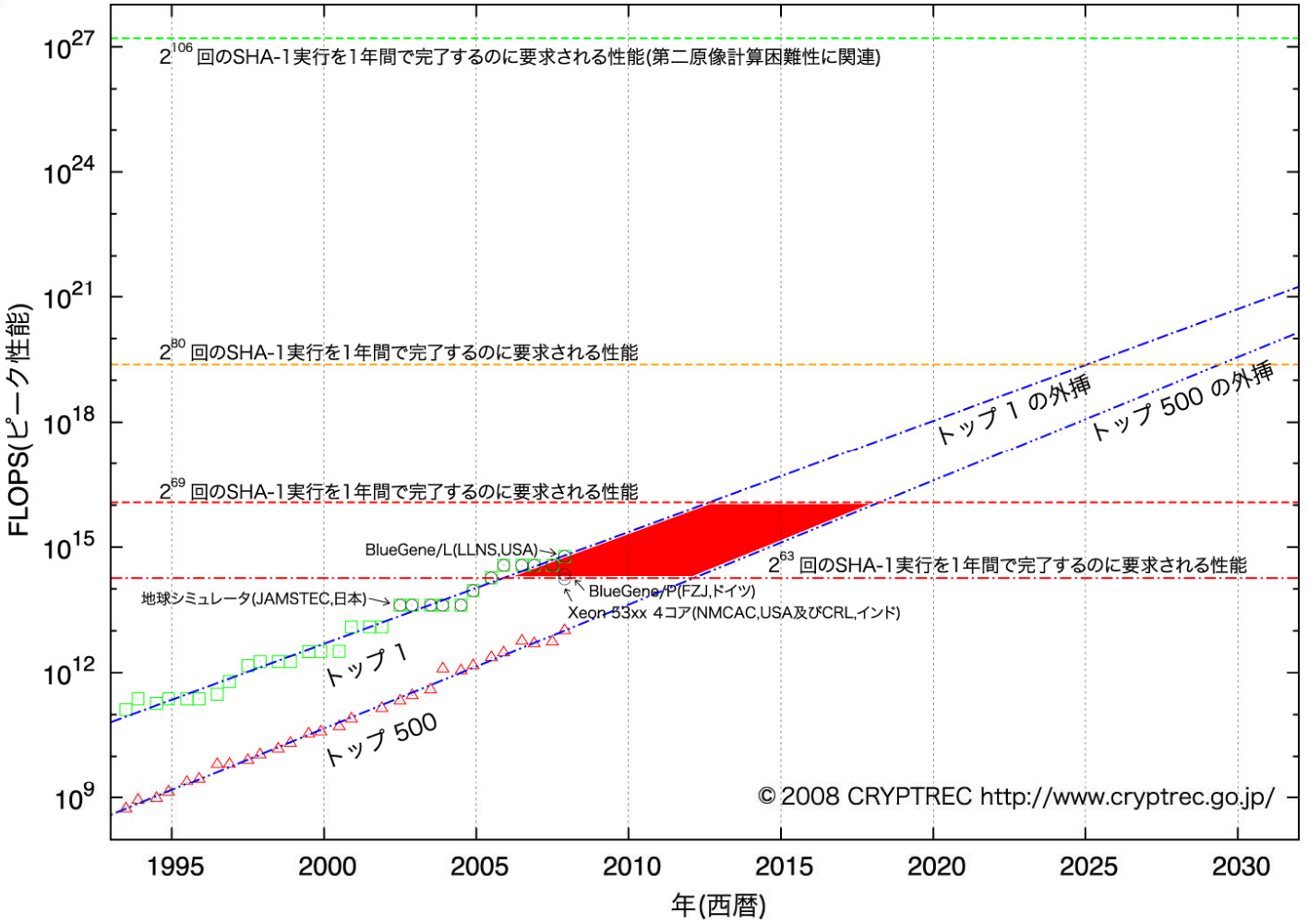
X.509証明書の構造

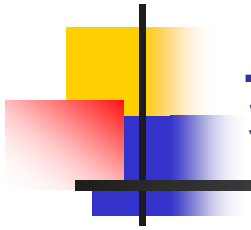


例： sha1withRSAEncryption (RSASSA-PKCS1-v1_5を利用)

- ●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）

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）





素因数分解問題

- 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、

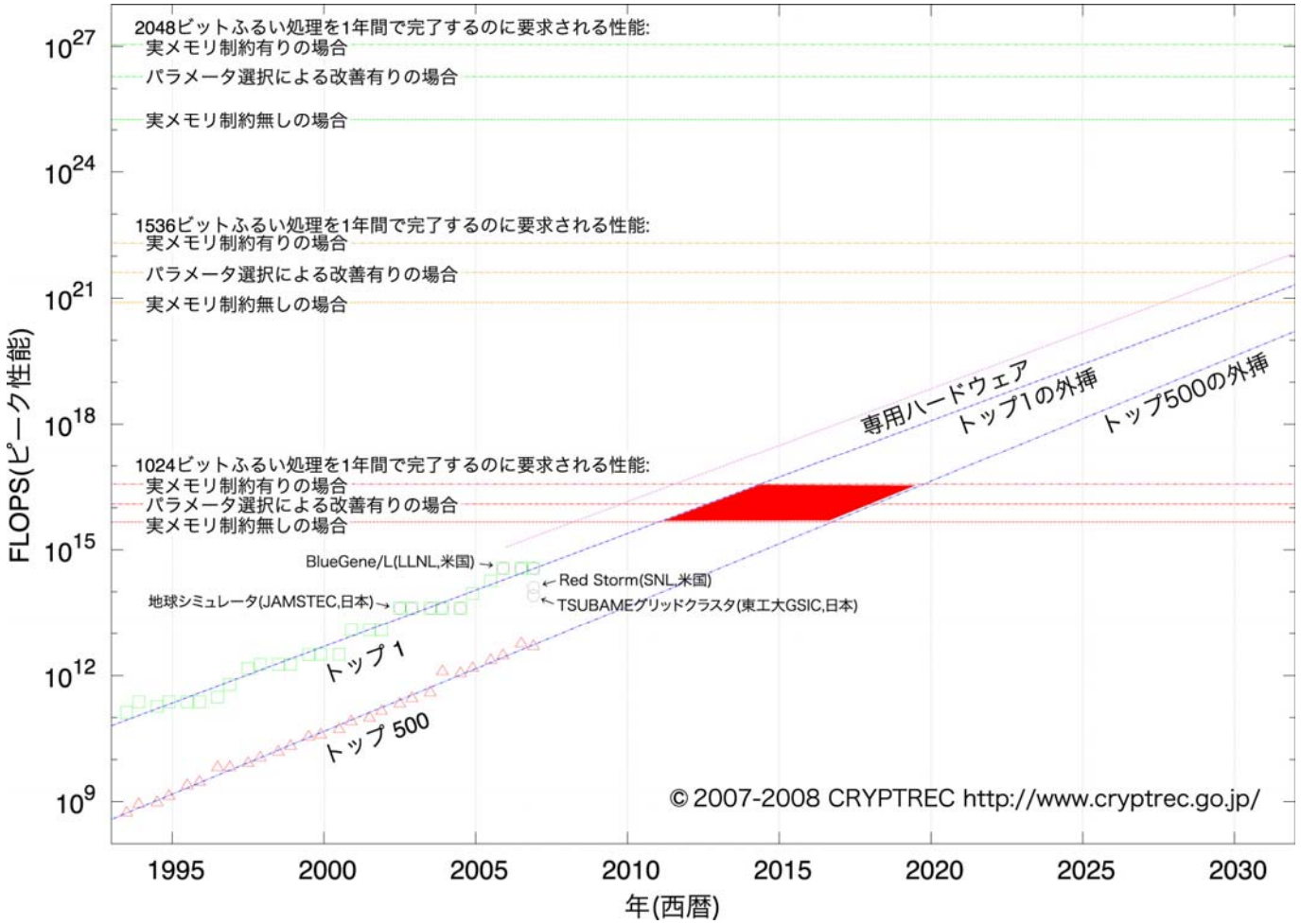
$$L_N[s,c] = \exp\left(c(\log N)^s(\log\log N)^{1-s}\right)$$

- 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。

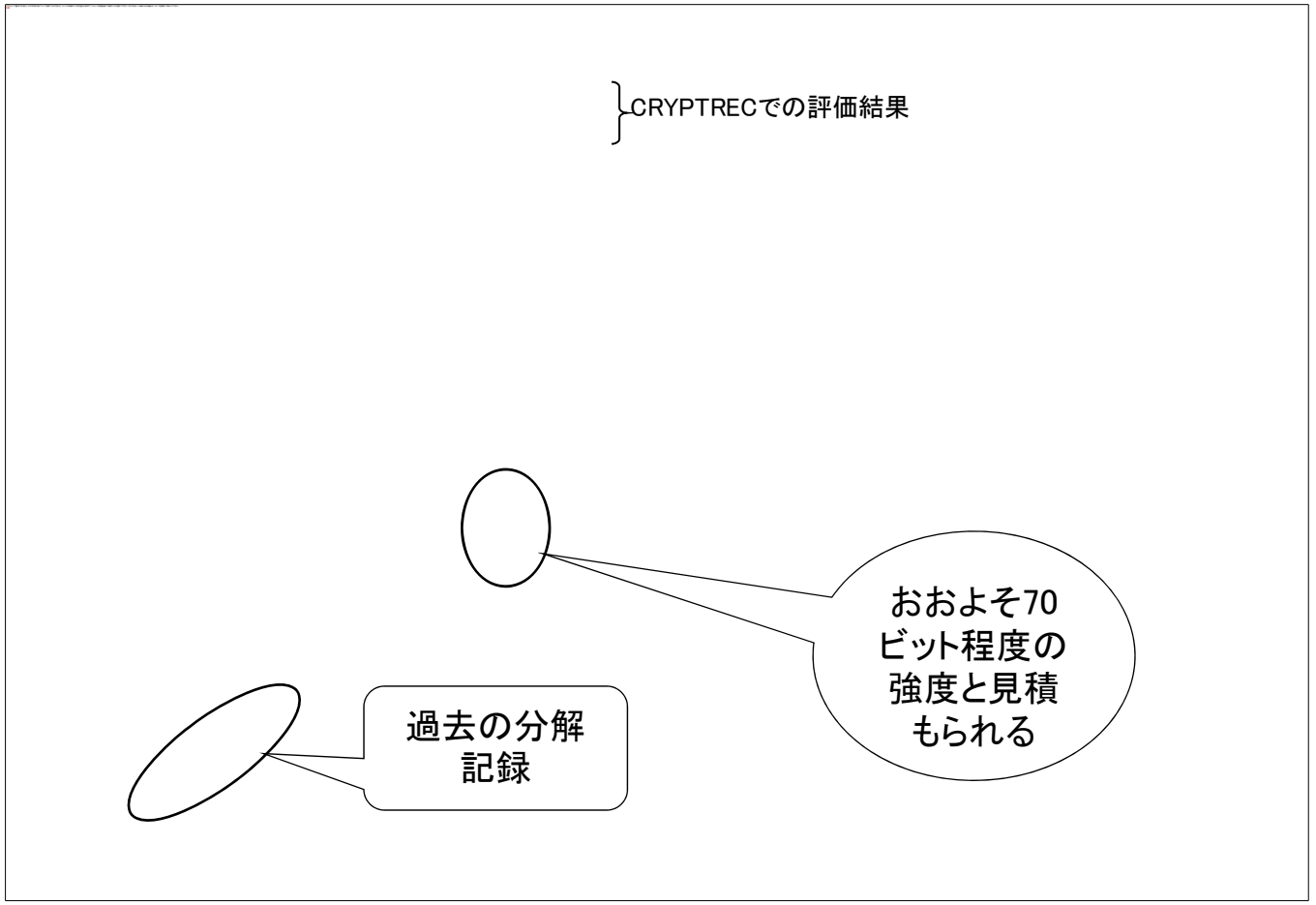
計算量と年の換算の複雑さ

- 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、TOP500.Orgにおけるデータを利用し、歴代のスーパーコンピューターと比較させている。
    - トップ1辺りのスパコンの価格は、$1M程度のコストと報道されている。

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)

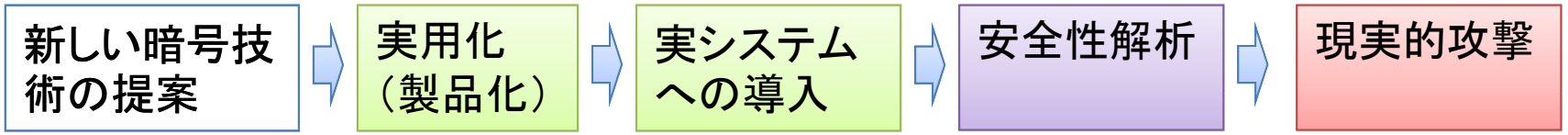


ビット・セキュリティの比較

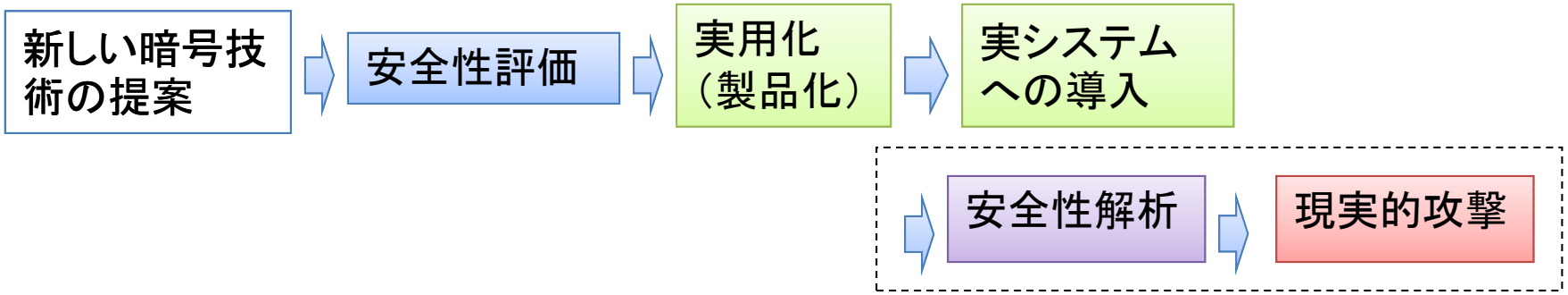


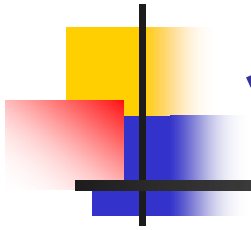
暗号アルゴリズムのライフサイクル

- 実システム導入後に、安全性解析がなされるケース
  - デファクト暗号に多いケース



- 安全性評価がなされた後に、実用化されるケース
  - 事前に安全性が評価されていることが望ましい

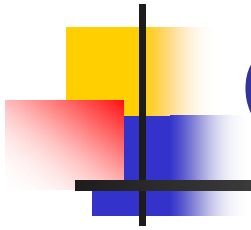




今後の課題

- コンピューター及びネットワークの性能向上により、素因数分解問題や離散対数問題に安全性を依存している公開鍵暗号の鍵サイズは、徐々に大きくしていく必要性がある。それに伴い、暗号化及び復号のために要求されるリソースが増大していく。
- リソースに限りがあるような、ICカードや携帯端末などとの間でインターオペラビリティーを取ることを重視するならば、要求されるリソースが低いアルゴリズムを選択することが望まれる。
- 新しいアルゴリズムを選択する場合には、暗号プロトコルへの影響や、どのようなパラメータを選択するのが適切なのかという問題とは別に、知財権に絡む問題なども新たに生じる。

CRYPTREC活動の背景



- 電子政府の基盤構築へ
  - 1990年代後半：行政の情報化推進
  - 1999年：ミレニアムプロジェクト
    - 2003年までに電子政府の基盤構築
  - 2000年以降：IT基本法，e-Japan戦略など
- 情報セキュリティの重要性の認識
  - 2000年省庁のホームページ改ざん事件
  - 2001年以降：IT戦略本部e-Japan重点計画など
    - 高度情報通信ネットワークの安全性・信頼性の確保
- 情報セキュリティの基盤としての暗号
  - 暗号の政府調達基準の不在
  - 暗号は電子政府の安全性の基盤

CRYPTREC活動の目的

- 電子政府に利用可能な暗号技術を提示
  - 電子政府システムに適用可能な暗号技術を公募
  - 応募暗号技術および事務局提案暗号技術を技術的・専門的見地から評価
  - 安全性，実装性等の特徴を分析・整理したリスト（電子政府推奨暗号リスト）を作成
- 暗号技術標準化へ貢献
- 暗号技術に対する信頼感醸成
  - 活動の公平性・透明性を確保

CRYPTRECの体制

(1)電子政府推奨暗号の監視
(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改訂に関する安全性評価

(1)暗号の実装に係る技術及び暗号を実装した暗号モジュールに体する攻撃手法に関する調査・検討
(2)電子政府推奨暗号リスト改訂に伴う実装性評価に関する調査・検討

(1)電子政府推奨暗号の適切な運用法をシステム設計者・運用者の観点から調査・検討

http://www.cryptrec.go.jp/system.html

電子政府推奨暗号リスト

- 総務省と経済産業省は2003年2月20日に、電子政府における調達のための推奨すべき暗号（電子政府推奨暗号）のリスト（電子政府推奨暗号リスト）を決定、公表しました。
- 同月28日に、行政情報システム関係課長連絡会議において、各府省は情報システムの構築に当たり暗号を利用する場合は、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旨が明記された「各府省の情報システム調達における暗号の利用方針」が了承されています。
- http://www.cryptrec.go.jp/list.html

別紙２

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。

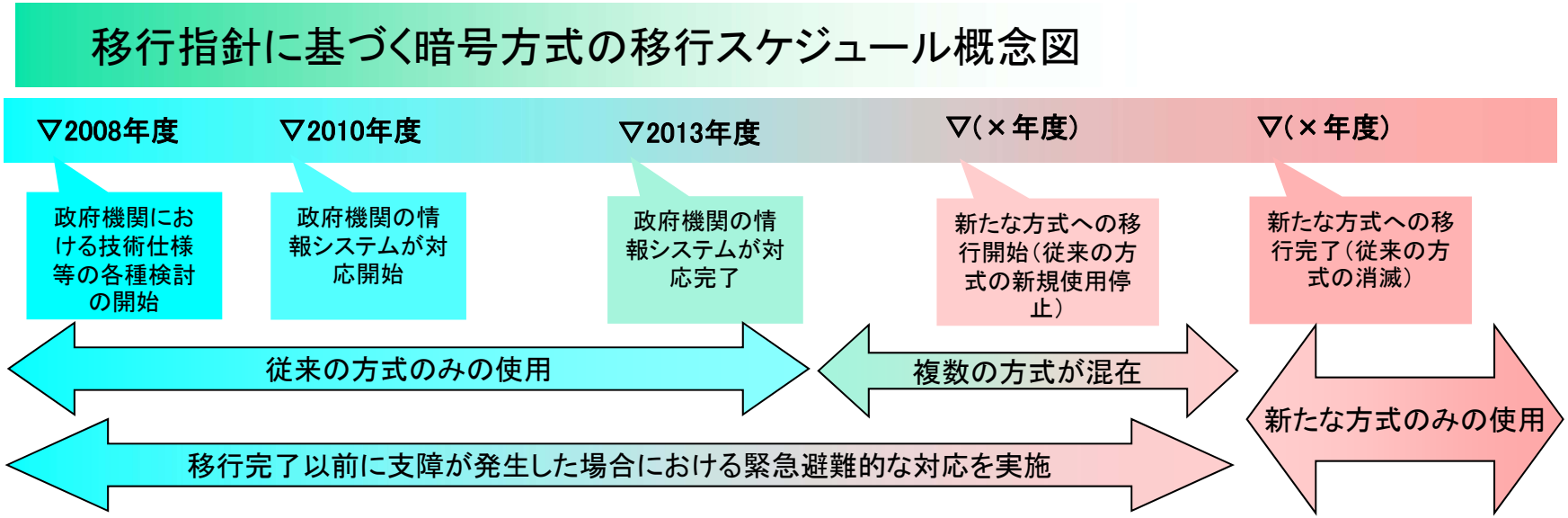
(注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(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。

CRYPTRECからの情報提供

- ハッシュ関数SHA-1及び公開鍵暗号方式RSA1024の安全性低下への対応
  - 内閣官房、総務省及び各府省庁は、「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」に従った取組みを推進する。
  - 総務省及び経済産業省は、現在使用されているSHA-1及びRSA1024並びに新たに使用するSHA-256及びRSA2048の安全性について引き続き監視し、必要な情報を速やかに各府省庁に提供する。

http://www.nisc.go.jp/active/general/res_niscrypt.html



リスト改訂の背景

現在の電子政府推奨暗号リスト（現リスト）
電子政府で利用可能な”安全な”暗号アルゴリズムを推奨

環境の変化・現リストの課題

- 暗号技術危殆化への対応
- 新しい技術への対応
- ISOにおける暗号技術標準化の進展
- 安全なシステム構築とリストの間のギャップ

新しい電子政府推奨暗号リスト（新リスト）
電子政府における安全な暗号技術の利用の促進する標準の提供

リスト改訂への要望

技術の経年劣化と新しい技術への対応

- 現リストの策定から5年経ち、暗号技術も大きく変化している
- 新しい技術にも目を向けることの必要性

安定した技術、市場で十分な利用実績がある技術

- 安全性に加えて、競争力（信頼性、商品の供給、価格）のあるもの
- 調達者、開発者、利用者にとってのわかりやすさ

リストの目的の明確化と情報提供や啓発

- 関連活動との協力による電子政府のセキュリティ確保
- 暗号技術を利用した調達者、開発者、利用者への情報提供を強化

新リストにおける基本方針

暗号技術のライフサイクルへの対応

- 暗号技術の経年劣化にも柔軟に対応できる
- 公募機会の拡大

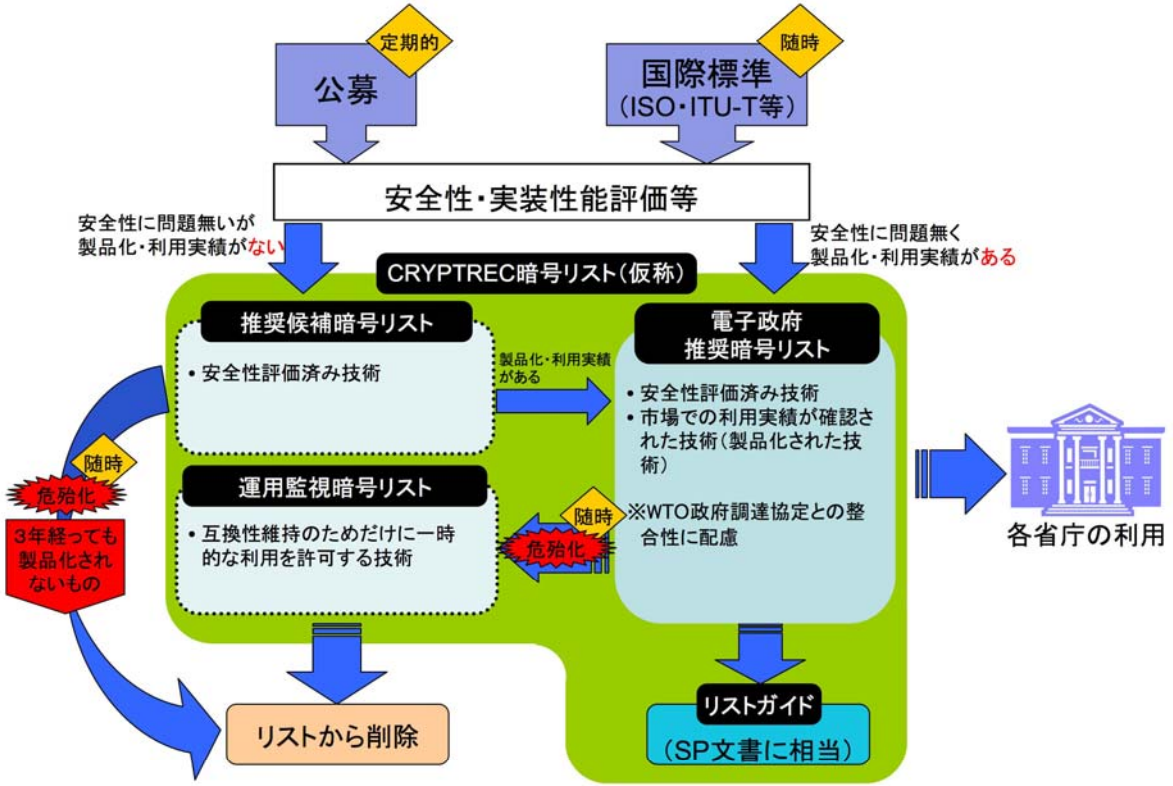
安定している技術の採用と国際動向への注意

- 電子政府における調達にあたり、製品化、利用実績を重視
- 国際標準との整合性を配慮

十分な情報発信

- リストの利活用に必要な技術情報の提供

新リストのイメージ図


定期的
公募
随時
国際標準
(ISO・ITU-T等)
安全性・実装性能評価等
安全性に問題無いが
製品化・利用実績がない
安全性に問題無く
製品化・利用実績がある
CRYPTREC暗号リスト(仮称)
推奨候補暗号リスト
• 安全性評価済み技術
製品化・利用実績
がある
電子政府
推奨暗号リスト
• 安全性評価済み技術
• 市場での利用実績が確認された技術(製品化された技術)
※WTO政府調達協定との整合性に配慮
随時
危殆化
運用監視暗号リスト
• 互換性維持のためだけに一時的な利用を許可する技術
随時
危殆化
3年経っても
製品化され
ないもの
各省庁の利用
リストから削除
リストガイド
(SP文書に相当)

公募実施の考え方

公募対象となる技術カテゴリ

以下のいずれかの条件を満たす技術カテゴリについて、定期的に公募を行う。

- 電子政府で利用されており標準化の必要性があるが、リストに掲載されていない
- すでにリストに掲載されている技術に比べ優位性のある新技術が存在し、電子政府での利用が見込まれる
- 実用化技術が確立されており、近い将来において電子政府で利用される見込みがある

2009年度における公募対象カテゴリ

- すでに電子政府で利用されているがリストにないカテゴリ
  - ✓メッセージ認証コード
  - ✓暗号利用モード
  - ✓エンティティ認証
- 既存技術に比べ優位性のある新技術が登場しているカテゴリ
  - ✓128bitブロック暗号
  - ✓ストリーム暗号

2009年度公募カテゴリ

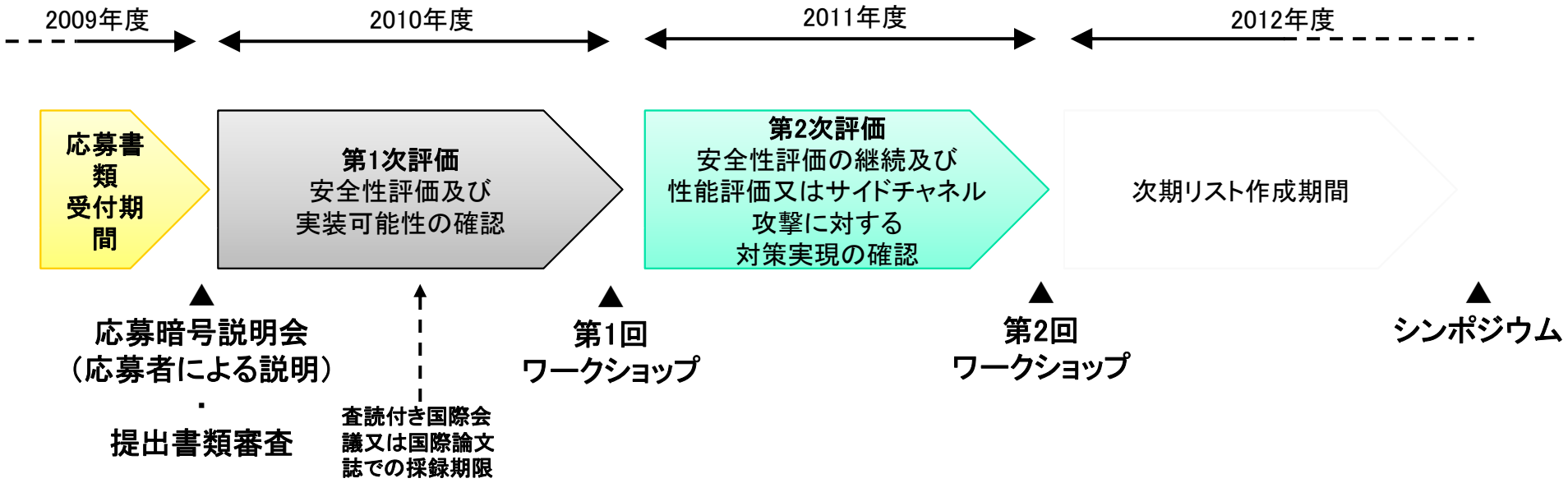
カテゴリ	仕様の概要
ブロック暗号	128bitブロック暗号（鍵長128bit/192bit/256bit）
ストリーム暗号	鍵長128bit以上
メッセージ認証コード	鍵長が128bitである128bitブロック暗号、および64bitブロック暗号を利用したメッセージ認証コード
暗号利用モード	秘匿に関する128bitブロック暗号、および64bitブロック暗号を対象とした暗号利用モード
エンティティ認証	電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、電子署名、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証技術、あるいは安全性を計算量的な困難さに帰着できるエンティティ認証技術

評価項目

カテゴリ	安全性評価	実装性評価
ブロック暗号	■差分攻撃、線形攻撃などの一般的攻撃 ■応募暗号に特化した攻撃、ヒューリスティックな安全性 ■サイドチャネル攻撃に耐性の強い実装の作りやすさ	ソフトウエア実装 ■処理速度、メモリ使用状況 ■鍵スケジュールなど個別の処理速度 ハードウエア実装 ■処理速度 ■リソース使用数量
ストリーム暗号	■Time/memory/data-tradeoff、分割統治攻撃、代数攻撃などの一般的攻撃 ■応募暗号に特化した攻撃、ヒューリスティックな安全性 ■サイドチャネル攻撃に耐性の強い実装の作りやすさ	
メッセージ認証コード	■証明可能安全性（適応的選択文書攻撃に対する識別不可能性） ■利用ブロック暗号に対する仮定の強さ ■利用ブロック暗号に特定に方式を適用した場合の安全性	
暗号利用モード	■証明可能安全性（適応的選択平文・暗号文攻撃に対する識別不可能性） ■利用ブロック暗号に対する仮定の強さ ■利用ブロック暗号に特定に方式を適用した場合の安全性	
エンティティ認証	■現リスト掲載暗号、あるいは新リストへの応募暗号のみを利用される暗号アルゴリズムは理想的に安全とする ■なりすましの成功、セッションの取り替えなどの認証への攻撃への安全性を形式化手法などを用いて検証	ソフトウエア実装 ■処理速度 ■メモリ使用量

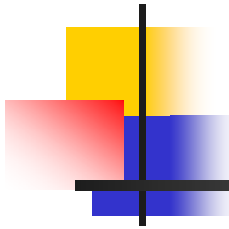
注意：これ以外を評価しないわけではない。

今後のスケジュール



応募書類受付期間：2009年10月1日～2010年2月4日17時必着
送付先：　情報通信研究機構 情報通信セキュリティ研究センター内
CRYPTREC事務局

http://cryptrec.go.jp/topics/cryptrec_20091001_application_open.html



IDベース暗号の歴史

1984: 岡本(龍), Shamir, IDベース暗号の概念

1985〜: KPS, ID-NKS, 合成数の離散対数問題など

2001: 境-大岸-笠原, Boneh-Franklin
ペアリングを利用した効率的な方式

2004: Boneh-Boyen1,2,3

2005: Waters 方式

2006: Gentry 方式

ペアリング暗号

- 鍵隔離暗号 (Key-Insulated Encryption)
- 代理再暗号化 (Proxy Re-encryption)
- キーワード検索暗号 (Keyword Searchable Encryption)
- 放送暗号 (Broadcast Encryption)
- グループ署名 (Group Signature)
- 属性暗号 (Attribute-based Encryption)
- ・・・

IDベース暗号の検討課題

運用

ID信頼性　PKG信頼性　ユーザ鍵管理　共通パラメータ管理　・・・

プロトコル

(階層的)IDベース暗号　鍵隔離暗号　代理再暗号化　放送暗号　・・・

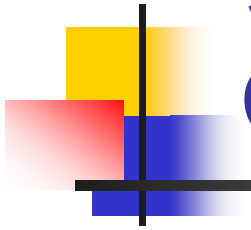
基盤アルゴリズム

Tate Pairing　Ate Pairing　ηT Pairing　MapToPoint　・・・

安全性評価

新しい数学的仮定　帰着効率　ハッシュ関数の理想化　・・・

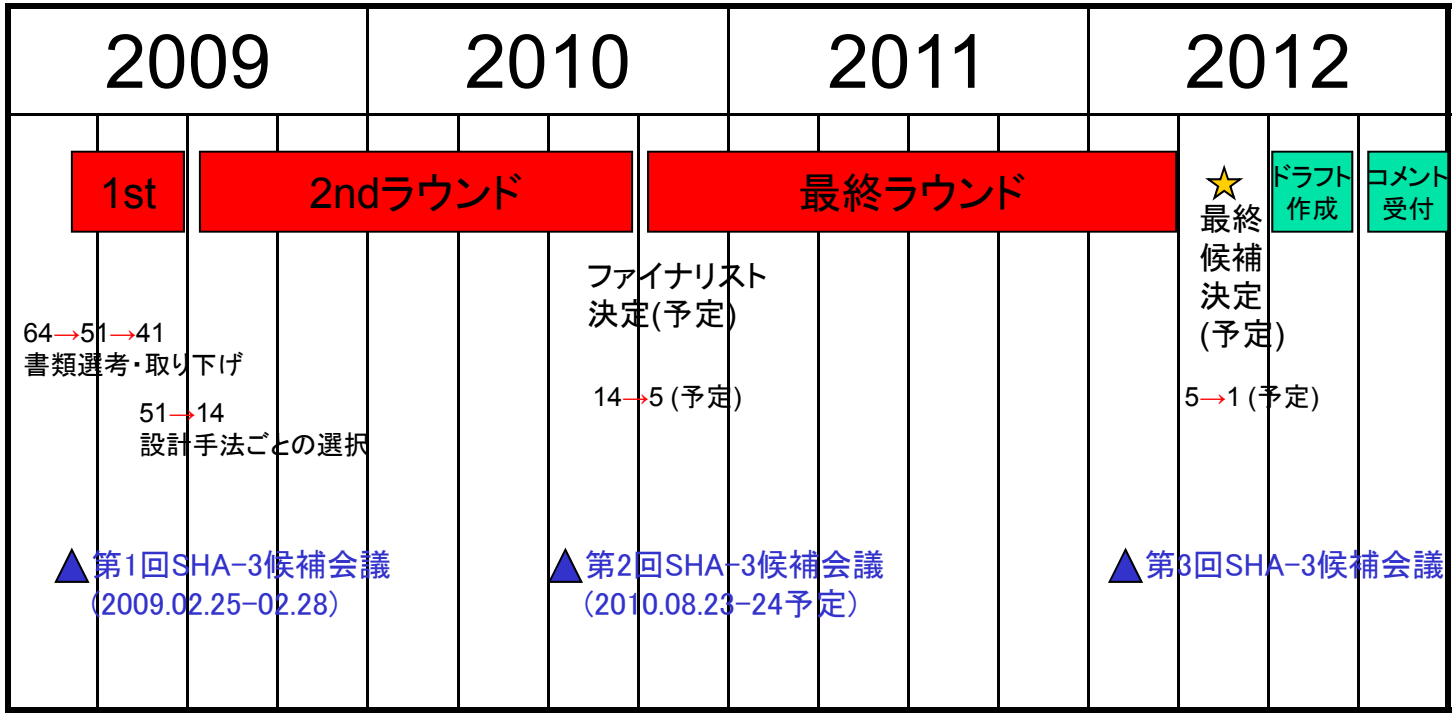
米国NISTのCryptographic Hash Competition



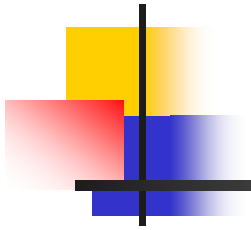
- 2004年に発表されたWangらによる衝突発見手法によって、MD5の衝突発見困難性は急速に失われた。
- SHA-1もMD5と似たような構造を有するため、SHA-2ファミリの次の世代を担うハッシュ関数が必要になった。
- 新しいハッシュ関数SHA-3を決定するためのコンペティション。
- NIST FIPS 180-2にSHA-3を追加する計画

http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Jan07.pdf

NISTのSHA-3選定スケジュール

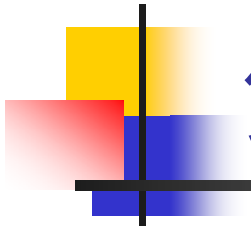


http://csrc.nist.gov/groups/ST/hash/timeline.html



国内から応募アルゴリズム

- AURORA
  - ソニー・名古屋大学
- Lesamnta
  - 日立製作所
- Luffa
  - 日立製作所・ルーヴァン・カトリック大学



第2ラウンドの候補アルゴリズムたち

- BLAKE
- Gr|stl
- Shabal
- BLUE MIDNIGHT WISH
- Hamsi
- SHAvite-3
- CubeHash
- JH
- SIMD
- ECHO
- Keccak
- Skein
- Fugue
- Luffa

http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html

ご清聴ありがとうございました。