（2009年度）
CRYPTREC 活動の概要と今後について

2010年3月2日

暗号技術検討会座長
暗号方式委員会委員長
今井秀樹(中央大学)

CRYPTREC 活動の概要

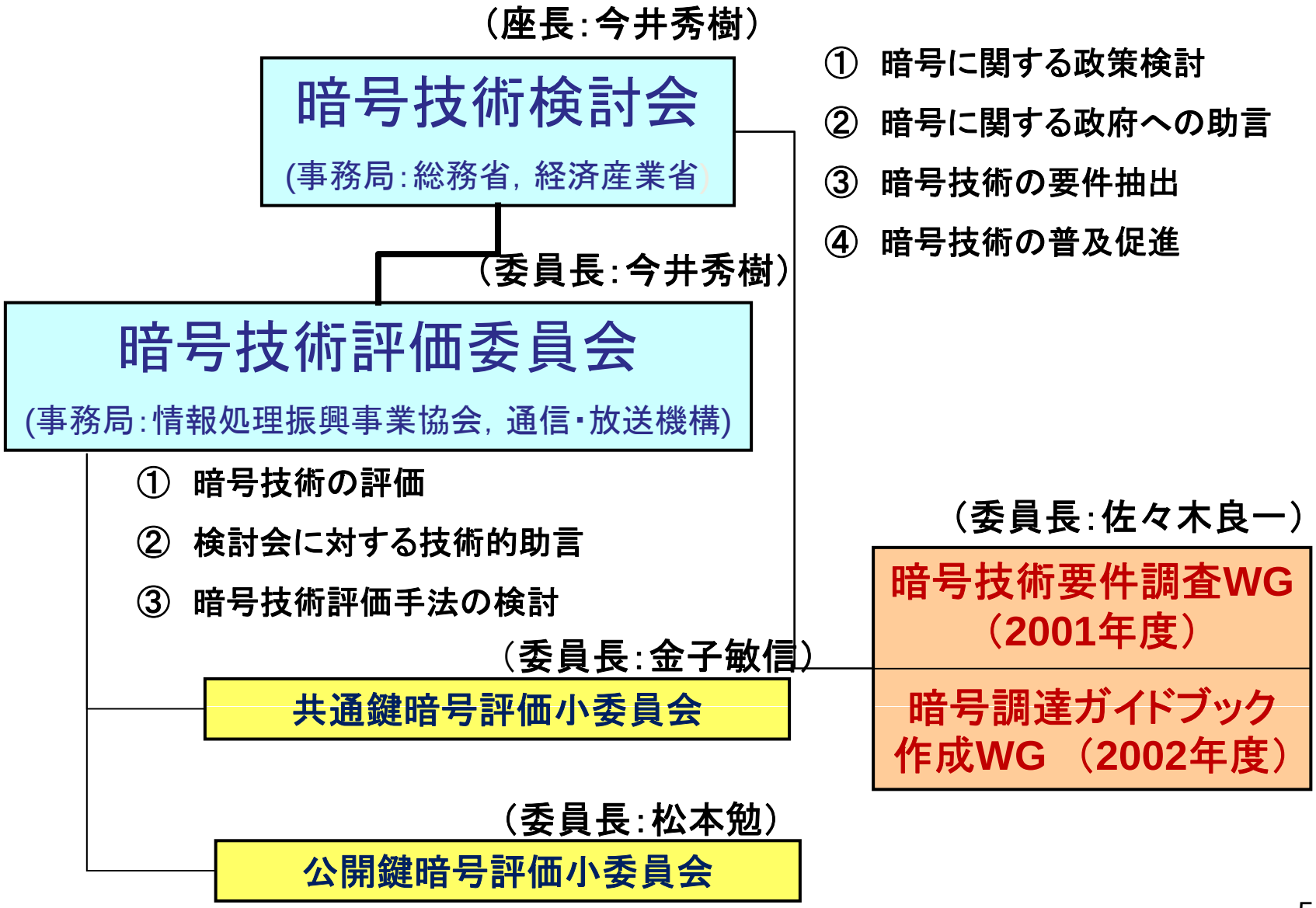
暗号評価 ―CRYPTREC―

- Cryptography Research and Evaluation Committees（暗号技術検討会，暗号技術評価委員会等）の略．しかし，その後，プロジェクト名としても使われる
- 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
- 現在は電子政府推奨暗号の安全性等の監視，暗号モジュールの評価基準等を検討
- **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**

電子政府推奨暗号

- 電子政府システムを対象
  - 国民との行政サービスに関連するシステムを対象（政府内で合意）
  - 地方公共団体についても考慮
  - 民間への浸透も視野に入れる
- 適用期間10年程度（2013年に改訂予定）
- CRYPTRECで安全性監視・維持
- 国際標準との整合性
  - ISO/IEC,NESSIE,NIST(AES)などとの協力
- 使いやすい暗号
  - システム調達のためのガイドブック
  - 広報・啓発
- 実装も考慮⇒JCMVP

2002年度のCRYPTREC体制



リスト策定までの活動

- 2000年6-7月　暗号技術公募
- 2000年8-01年3月　暗号技術評価（2段階）
- 2000年10月　暗号技術シンポジウム
- 2001年4月　　暗号技術評価報告会(2000年度)
- 2001年8-9月　暗号技術公募
- 2001年8-02年3月　　暗号技術評価（2段階）
- 2002年1月　　暗号技術評価ワークショップ
- 2002年4月　　暗号技術評価報告会(2001年度)
- 2002年4-11月　　詳細評価
- 2002年10月 - 03年1月　　リスト作成
- 2003年2月　　電子政府推奨暗号リスト公表
- 2003年5月　　暗号技術評価報告会(2002年度)

電子政府推奨暗号リスト

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

電子政府推奨暗号リスト注

(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。

2003～2008年度CRYPTREC体制

（座長：今井秀樹）

暗号技術検討会

(事務局：総務省，経済産業省)

（委員長：今井秀樹）

暗号技術監視委員会

(事務局：NICT，IPA)

（１） 電子政府推奨暗号の監視

（２） 暗号アルゴリズム等を主な対象とする調査・検討

（３） 電子政府推奨暗号リストの改訂に関する調査・検討

- IDベース暗号WG
- リストガイドWG

（委員長：松本勉）

暗号モジュール委員会

(事務局：IPA，NICT)

（１） 暗号モジュール評価基準及び試験基準の作成

（２） 暗号実装関連技術を主な対象とする調査・検討

- 電力解析実験WG

IPA:独立行政法人情報処理推進機構　NICT:独立行政法人情報通信研究機構

電子政府におけるリストの位置

- 2003年2月　行政情報システム関係課長連絡会議において可能な限り電子政府推奨暗号リストの暗号を利用することに合意(「各府省の情報システム調達における暗号の利用方針」).
- 2003年4月　CRYPTREC新体制発足（暗号技術監視委員会，暗号モジュール委員会の設置）
- 2005年12月　情報セキュリティ統一基準(政府機関の情報セキュリティ対策のための統一基準)において可能な限り電子推奨暗号リストの暗号を使用することが基本遵守事項(保護すべき情報・情報システムにおいて必須として実施すべき対策事項)に.

その後の活動

- 監視活動
  - RSA1024の安全性の検討
  - ハッシュ関数の脆弱性の調査・警告
    - MD5に関する警告
    - SHA-1に関する脆弱性情報の周知
  - 暗号の世代交代の指針の提示
- 暗号実装の評価
  - JCMVP構築
- リスト改訂

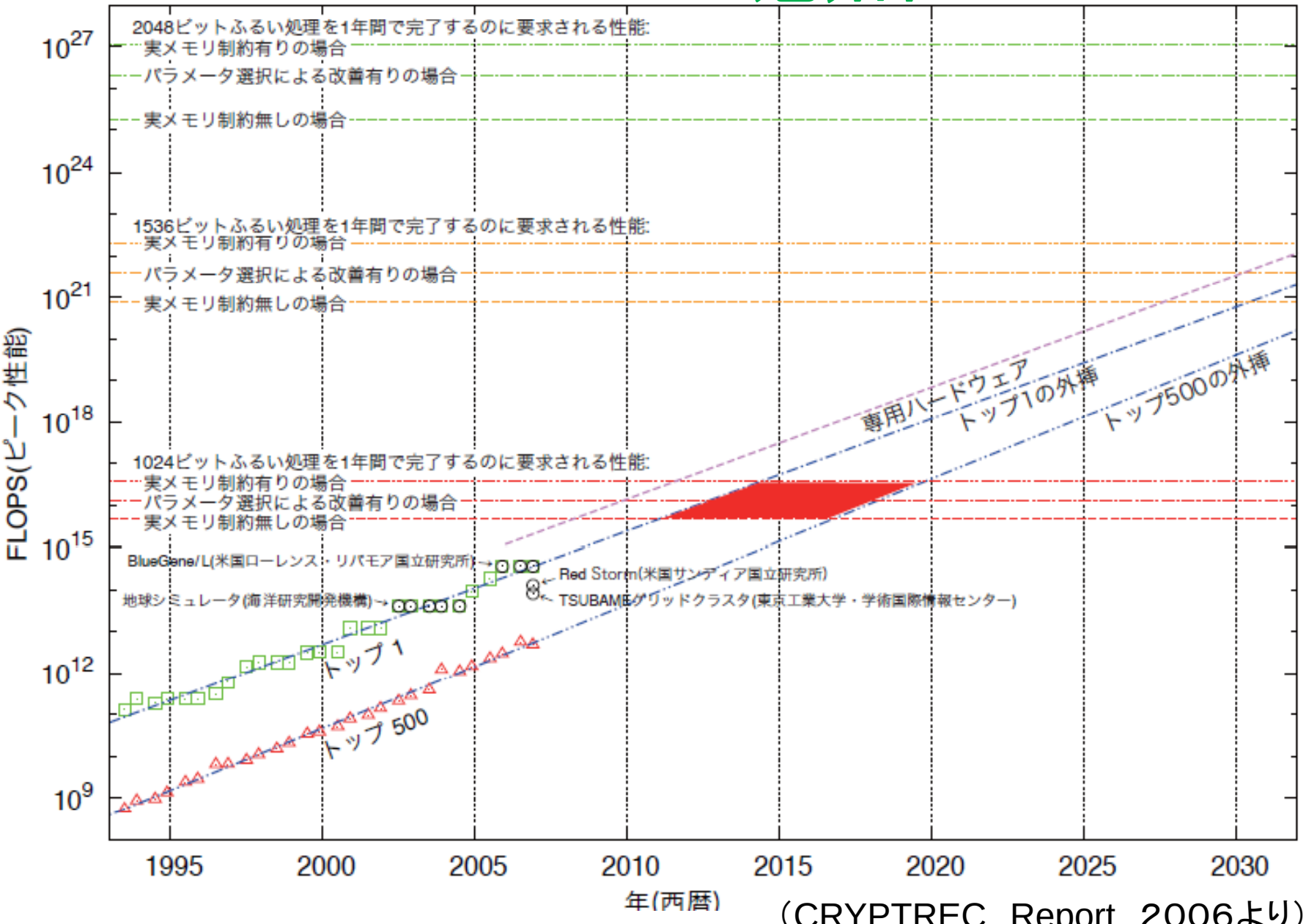
SHA-1とRSA1024の危殆化対策

- CRYPTRECは，SHA-1について，リストでは条件付きで使用を認めているが，*2004*年以降のハッシュ関数に対する攻撃法の進展により，*2005*年からSHA-1の危殆化の警告を発している.
- CRYPTRECは，*2006*年にRSA1024が*2010*年から*2020*年の間に解読される可能性を示し，*2007*年のCRYPTRECガイドブックでは2048ビット以上の鍵を用いることを推奨している.

ハッシュ関数の危殆化

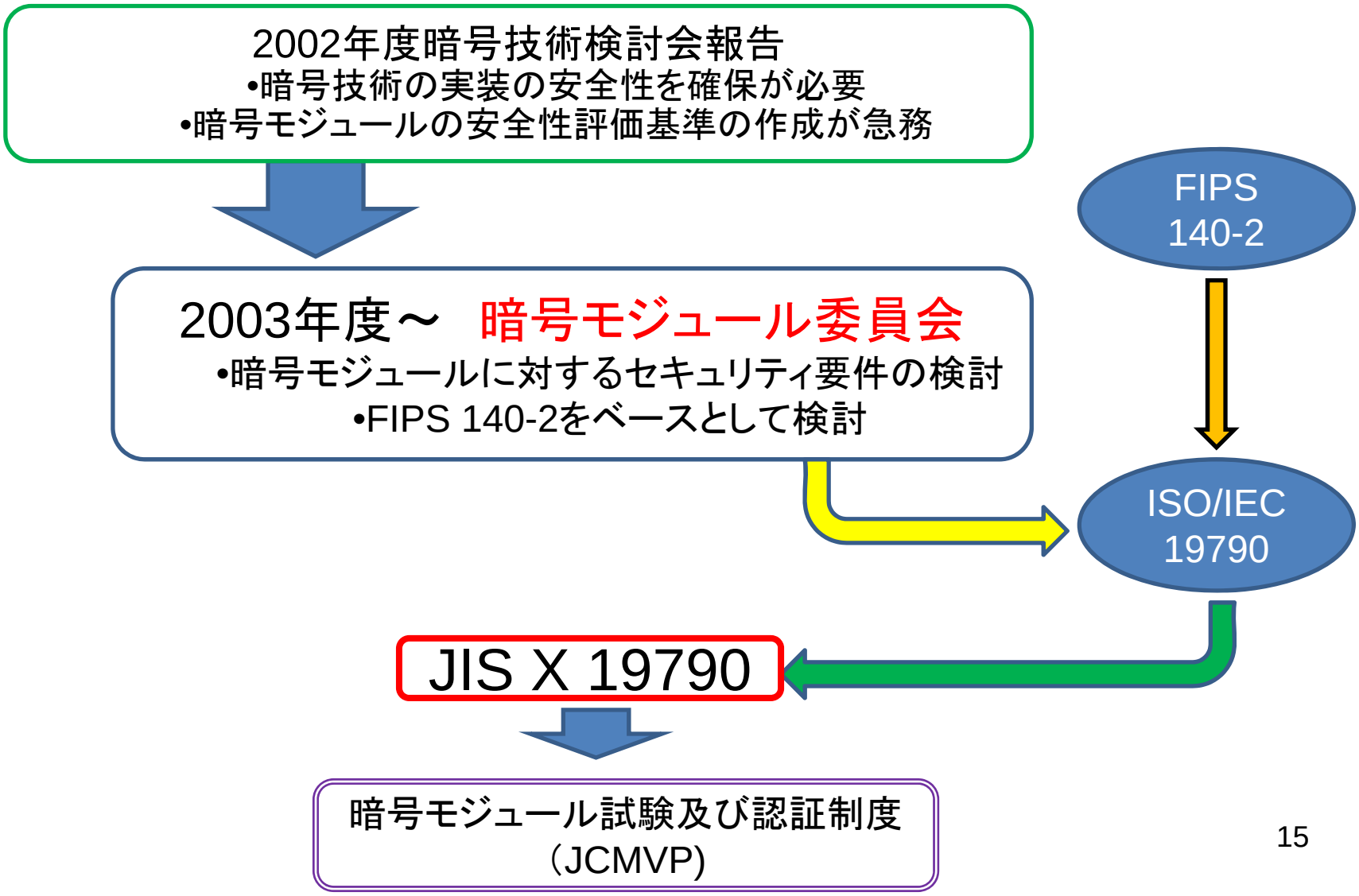
- ハッシュ関数への攻撃の進歩
  - 2004年8月，X. Wangらにより MD4, MD5, HAVAL-128, RIPEMD，SHA-0に対し，衝突を実際的な時間で求め得ることが示された（中国内では1997年に発表）
  - 2005年2月，SHA-1の衝突も数年程度の計算で求め得るとの報告があった。
    - まだ衝突は見つかっていない。
  - その後も攻撃法は進歩し，MD5を用いるシステムは現実的脅威にさらされている.
    - SHA-1についても、注意深く監視する必要がある。
  - これに対し，NISTは早期にSHA-2（SHA-224, 256, 384, 512)への移行を勧めている

RSA1024の危殆化



（CRYPTREC Report 2006より）

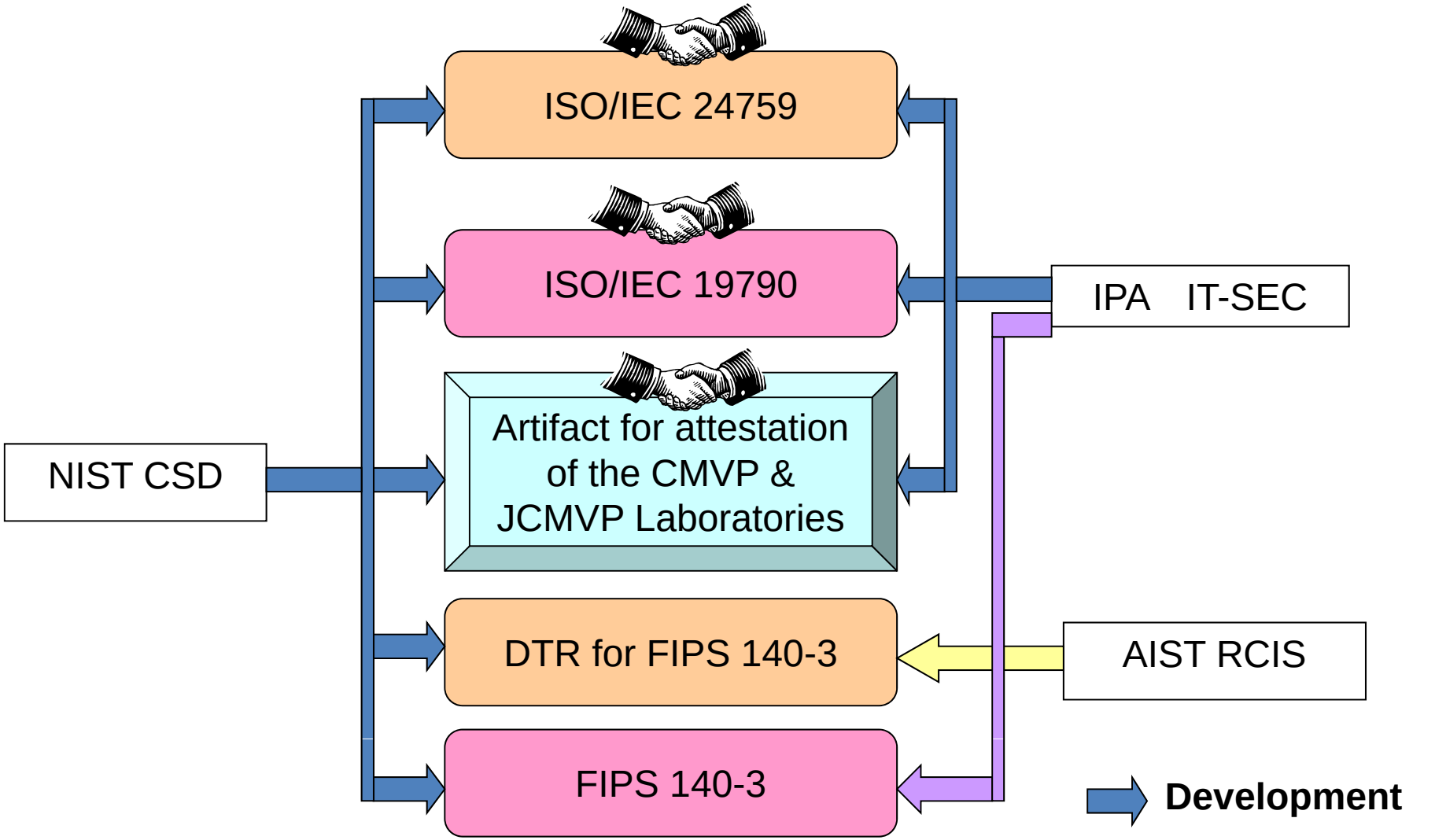
CRYPTRECの波及効果
- JCMVPの設立 -



日本版 CMVP（JCMVP）

- CMVP: Cryptographic Module Validation Program（暗号モジュール試験及び認証制度）
- 暗号アルゴリズムはCRYPTRECリスト等による
- FIPS140-2，ISO/IEC 19790 に基づく適合試験
- 2007年4月に開始
  - 認証機関はIPA
  - 試験機関はIPA，（株）電子商取引安全研究所評価センター，（財）日本品質保証機構関西試験センター
  - 認定機関は（独）製品評価技術基盤機構（NITE）
- FIPS140-3制定中
  - CRYPTREC等の研究成果も反映

CMVP & JCMVP



IPA：IPA:INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
IT-SEC：IT SEcurity Center
AIST: National Institute of Advanced Industrial Science and Technology
RCIS：Research Center for Information Security

CRYPTRECの波及効果
- 暗号の世代交代 -

暗号技術の監視活動

- ハッシュ関数SHA-1の安全性の低下
- RSA暗号の鍵長に関する安全性予測

↓

内閣官房情報セキュリティセンター等への情報提供

↓

- 「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」
- 「電子署名及び認証業務に関する法律」の告示の見直し

電子政府推奨暗号リストの改訂

リストの改訂の必要性

- 暗号技術の機能（特に安全性）の経年劣化は避け難い
- 当初から5年後（2008年）見直し，10年後(2013年）改訂を想定
- 前回には公募できなかったカテゴリの暗号技術で現時点で公募すべきものの存在
- CRYPTRECに対する社会的要請の拡大（利用実績，実装性などより実際的な面からの評価の必要性）

リストの改訂の目的と方法

- 電子政府において暗号技術を利用する際に安全で適切な暗号技術を選択するための指針を与える
- 暗号を利用した技術をシステムのセキュリティ要件に合わせて正しく組み込むための指針を与える
- 国際標準等との関係をより明確にする
- 今後の改訂の姿を示す
- 新たな暗号技術を公募し，安全性，実装性，利用実績等を評価する
- 現リストに掲載されている暗号技術の見直しを行い，現リスト全体の構成を改める
- 暗号技術のライフサイクルに対応したものとする

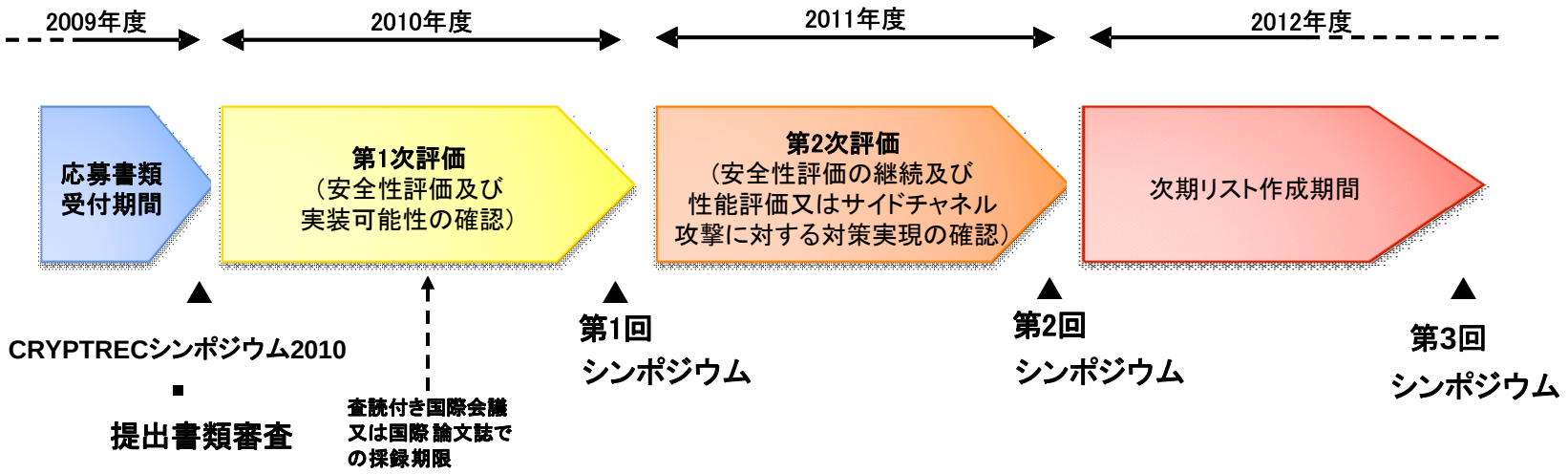
公募対象の暗号技術カテゴリの要件

- 現リストに含まれていないが、電子政府システムの構築において安全性及び実装性の高い技術仕様の推奨が必要とされている暗号技術カテゴリであること
- 安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち国際学会で注目されている新技術が提案されている暗号技術カテゴリであること
- 普及・標準化が見込まれる暗号技術カテゴリであること

暗号技術カテゴリ

	電子政府推奨暗号リスト（現リスト）	CRYPTREC 暗号リスト（仮称）（次期リスト）
公開鍵暗号	署名	署名
	守秘	守秘
	鍵共有	鍵共有
共通鍵暗号	64 ビットブロック暗号	ブロック暗号
	128 ビットブロック暗号	今回の公募
	ストリーム暗号	ストリーム暗号 今回の公募
		メッセージ認証コード 今回の公募
		暗号利用モード 今回の公募
	ハッシュ関数	ハッシュ関数
	疑似乱数生成系	
		エンティティ認証 今回の公募

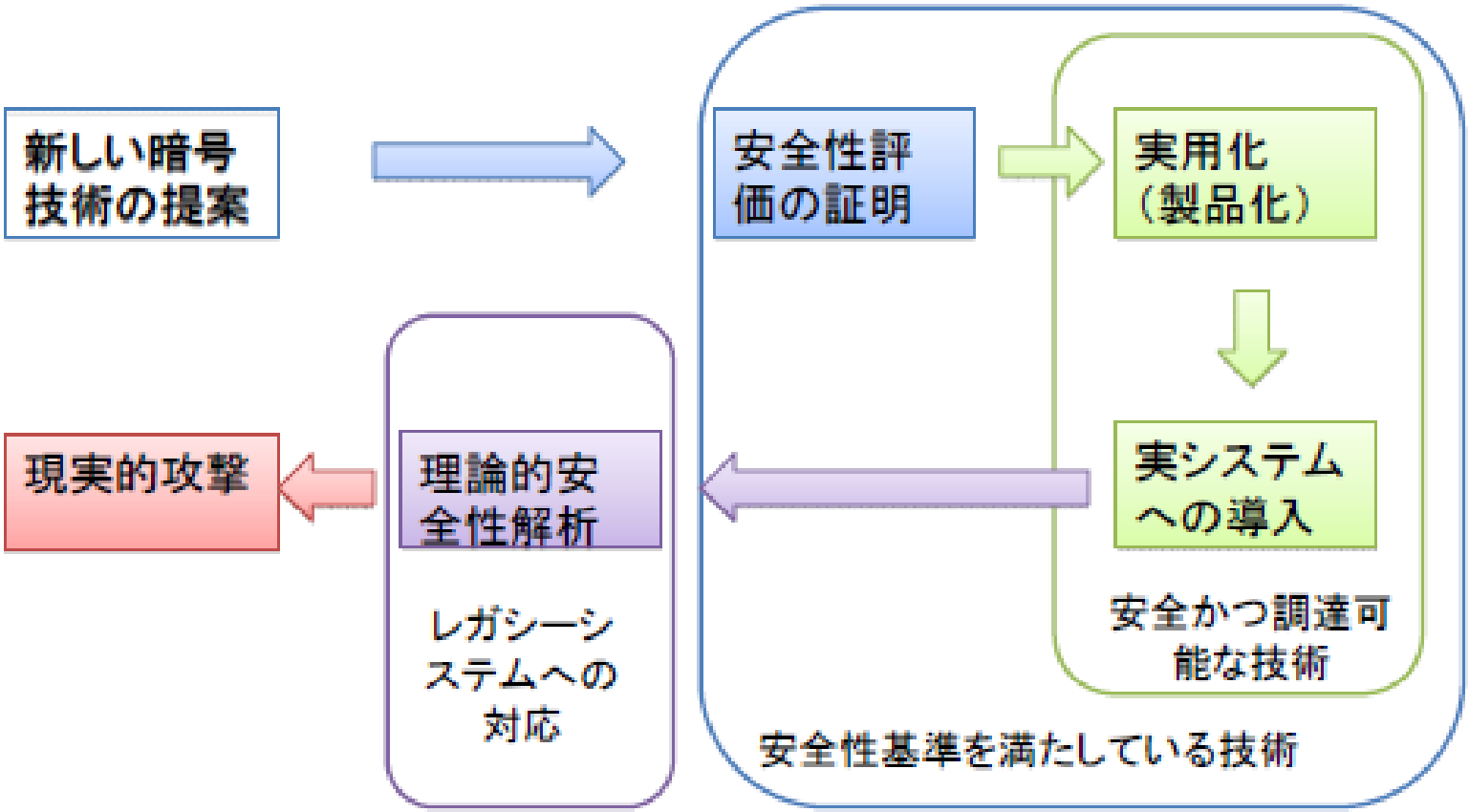
公募スケジュール



「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」より

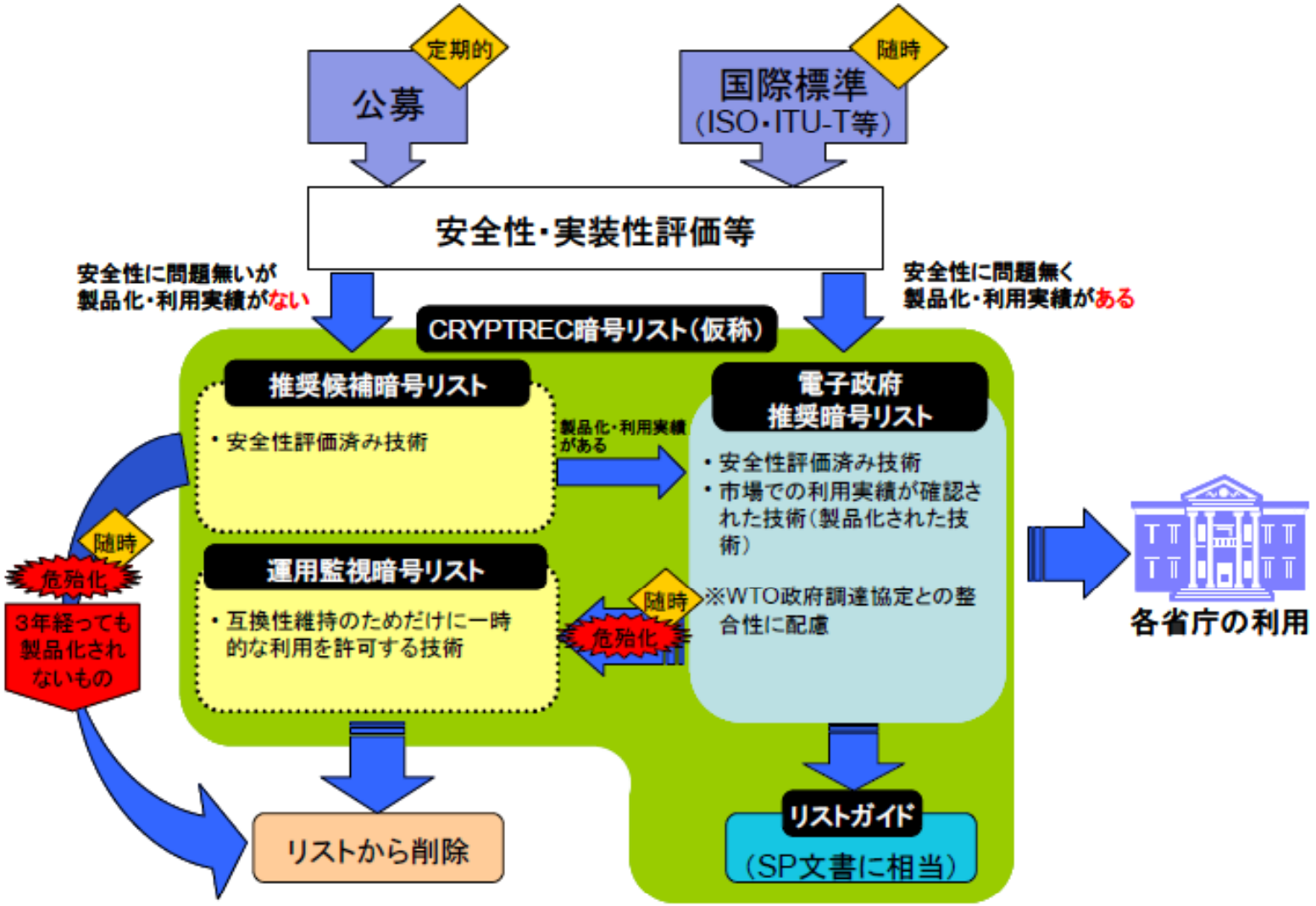
暗号技術のライフサイクルへの対応

暗号アルゴリズムのライフサイクル



リストに3つのカテゴリを設け、ライフサイクルに応じて柔軟に変動

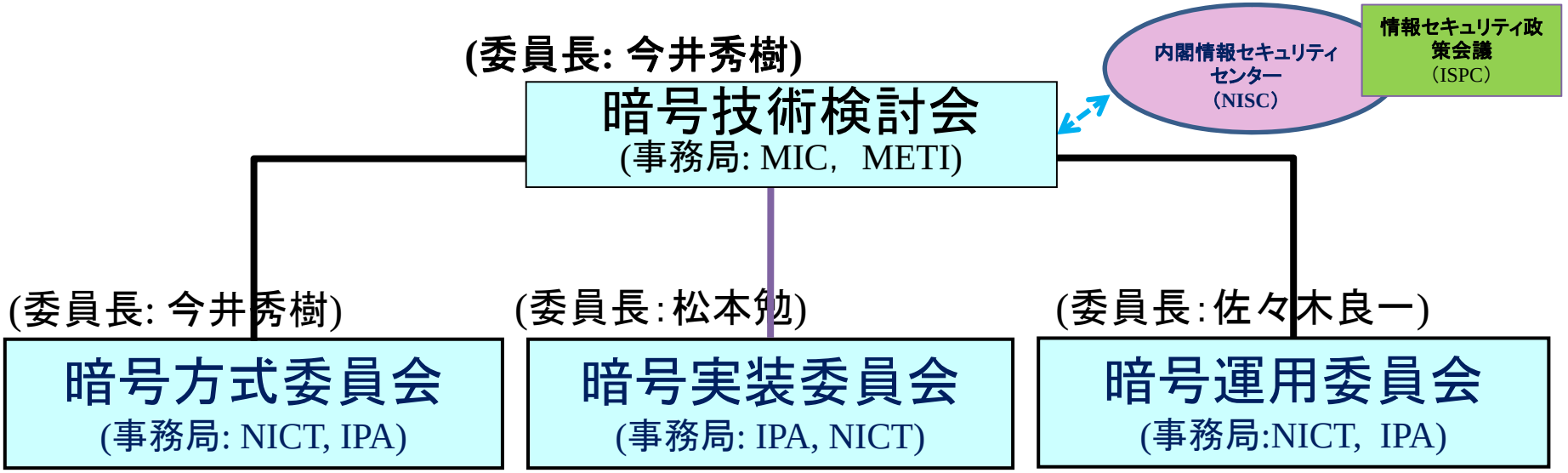
CRYPTREC公募・運用スキーム



「電子政府推奨暗号リスト改訂のための暗号技術公募要項(2009 年度)」より

2009年度の活動と今後

2009年度以降のCRYPTREC体制



1. 応募暗号の安全性評価基準に関する検討
2. 動向調査・監視活動
3. 電子政府推奨暗号リストの改訂に関する調査・検討

1. 実装性評価に関する検討
2. サイドチャネル攻撃耐性の評価
3. サイドチャネル攻撃検証に関する情報収集

1. 暗号技術の製品化・利用実績等の評価
2. 運用監視暗号の危殆化対策の検討
3. 次世代暗号技術等の調査・検討

2009年度のCRYPTREC活動の概要

新しい電子政府推奨暗号リスト策定作業の開始

公募の開始

実装評価の範囲と方法に関する検討

新しいリストの運用に関する検討

リストガイド作成と継続的な監視活動

リストガイド作成

学会等での安全性の知見の調査

国際標準との連携

ハッシュ関数評価における連携

ISOモジュール評価に対するコメント

暗号方式委員会　　暗号実装委員会　　暗号運用委員会

2009年度暗号方式委員会活動の概要
-暗号公募の開始-

- 2009年10月1日に、五つの技術カテゴリで公募を開始
  - 128ビットブロック暗号
  - ストリーム暗号
  - 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
- 2010年2月4日に応募締め切り
  - 6件の応募（詳細はこの後のプレゼンテーション参照）
- このCRYPTRECシンポジウムで、提案技術のプレゼンテーションと質疑応答を実施し、2010年度の評価実施に向けた意見収集を実施する。
- 次年度の暗号方式委員会で、安全性評価を実施する。

2009年度暗号方式委員会活動の概要
-リストガイド作成と継続的な監視活動-

監視活動

- 国内外の学会における、暗号の安全性に関する研究成果の取りまとめ
- 今年度は暗号の基礎となる数学的問題の評価、関連鍵攻撃に関する報告など
- 監視結果は、CRYPTRECレポートで公開予定

リストガイド

リストガイドWG（高木剛主査）

- IDベース暗号に関する継続検討
  - PKIが提供する信頼との比較による、IDベース暗号の利点と課題の抽出
  - 電子政府において利用した場合の推奨と課題の取りまとめ
    - 電子メールシステム
    - Webによる情報提供システム
- 現リストで「例示」となっている疑似乱数生成に関する実装仕様の提示
  - JCMVP Approvalとなっているアルゴリズムを対象

2009年度暗号方式委員会活動の概要
-ハッシュ関数評価における連携-

- 現在、米国のNISTが、次期ハッシュ関数SHA-3の選考を実施中
- CRYPTRECでは、同時期に重複した評価を実施するのではなく、SHA-3の選考過程と結果を参照し、日本の電子政府で利用されるハッシュ関数の評価を実施する
- CRYPTRECで必要とされる評価と、NISTで実施する評価を近づけるために、NISTの評価活動への貢献を行う
  - 電子政府での適用に必要とされる以下の項目
    - 安全性評価の基準
    - 実装評価の基準
- 今後も継続的にCRYPTRECとNISTの連携、国際間連携を実施予定

2009年度暗号実装委員会活動の概要

- 実装性能評価に関する検討
  - 実装性能評価ツールの検討（2009年度）
    - ソフトウェア及びハードウェア
    - 実装用インタフェース仕様
  - 実装性能評価の評価項目、評価手法、評価結果の判断基準（2010年度の課題）
- サイドチャネル攻撃耐性の評価に関する検討
  - 確認方法の検討
  - サイドチャネル攻撃検証に関する情報収集
- 国際貢献
  - ISO/IEC 19790の早期改訂案の検討

2009年度暗号運用委員会の活動概要

- 暗号技術の運用を主な対象とする調査・検討
- 暗号技術に対する製品化・利用実績等の評価
  - 以下の観点から、論点の整理中
    - 利用実績
    - 国際標準技術
- 利用実績の論点の例
  - 利用実績の定義
  - 利用実績の判断方法
- 国際標準技術に関する論点の例
  - 国際標準化機関とはどの範囲か
  - 標準化の対象は
    - アルゴリズムのみ
    - プロトコルまで含めるか

今後に向けて

- 組織／体制の強化
- NISCとの関係の強化
- 研究機関との連携の強化
- NIST等との国際連携の強化
- 国際標準への貢献
- リストの柔軟な見直し
- 対象分野の整理／拡大