CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術の公募について

CRYPTREC事務局

CRYPTREC
Cryptography Research and Evaluation Committees

公募対象のカテゴリ --- 公募開始ルールの明確化

(1) 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

(2)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。

(3)普及・標準化が見込まれる暗号技術カテゴリであること。

以上の観点から随時公募について検討を行える。
(「電子政府推奨暗号リストの改訂に関する骨子」より)

CRYPTREC
Cryptography Research and Evaluation Committees

リスト記載の暗号技術カテゴリの見直し --- リストガイドとの併用

相互接続性が必要ない要素技術や例示のみのカテゴリ、利用されなくなったカテゴリは削除してリストガイドで補足する

→ 擬似乱数生成系をカテゴリからの削除

擬似乱数生成系については、公開鍵暗号技術等で利用される要素技術であり、相互接続性に影響を与えないこと、安全性要件として満たすべき乱数検定法が示されていることから、リストガイドにて参照することが適当であると考えられる。
よって、電子政府推奨暗号リスト（仮称）及び推奨暗号候補リスト（仮称）から外し、2009年度公募カテゴリには入れないこととする。

(「電子政府推奨暗号リストの改訂に関する骨子」より)

CRYPTREC
Cryptography Research and Evaluation Committees

応募可能な暗号技術

(1)十分な安全性を有する暗号技術であること。ただし、現リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であること。

(2)個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。

(3)当該技術を利用した製品が販売済みであるか又は、販売の予定があること。

(4)安全性評価及び、実装性能評価に足る技術仕様が公表されていること。

(5)暗号技術に関する基本特許については、製造、販売、使用に対して、無償(Royalty Free)又は、妥当かつ非差別的（Reasonable And Non-Discriminatory）な条件で、暗号技術の実施許諾権が与えられること。

(「電子政府推奨暗号リストの改訂に関する骨子」より)

CRYPTREC
Cryptography Research and Evaluation Committees

リストへの要望・目的
- ・電子政府推奨暗号リストの有用性を高めたい
- ・国際標準化となり得るものを選択したい
- ・優れた暗号技術は高い学術成果に裏付けられている

2.2.応募暗号に関する留意事項

(3)応募される暗号技術は、2010年9月末までに、査読付きの国際会議、又は、査読付きの国際論文誌で発表されているか、あるいは、採録が決定されているものに限ります。

(「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)」P.2より)

CRYPTREC
Cryptography Research and Evaluation Committees

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

(公募要項 p.1)

CRYPTREC
Cryptography Research and Evaluation Committees

今回の公募に対する代表的な質問

Q1.ハッシュ関数や公開鍵暗号の公募を実施しないのは何故か？

ハッシュ関数 → NISTのSHA-3選定(2012年決定)と同時期
公開鍵暗号 → 公募開始ルール(2枚目)による判断

2009年度の公募対象カテゴリではないのであって、
今後も公募しないという意味ではない。

Q2.国際標準技術はどのように扱うのか？

「講演2:リスト改訂スキーム」参照
公募カテゴリによらず、委員会審議に基づき対象となった技術は安全性及び
実装性能評価などを実施する。その結果に従ってリストの登録を検討する。

CRYPTREC
Cryptography Research and Evaluation Committees

Q3.現リストにおける公募対象外のカテゴリの扱いについて

公開鍵暗号(署名、守秘、鍵共有)、64ビットブロック暗号、ハッシュ関数については
カテゴリと登録されている技術はそのまま継続される。
ただしリスト改訂のための第2次評価において安全性の再確認及び実装性能について
調査を予定している。
公募対象カテゴリに登録されている技術もそのまま継続し、第2次評価において
安全性の再確認及び実装性能について調査を予定している。
全技術の状況を整理した上でリストの構築を行う。
(11枚目及び13枚目に関連説明)

CRYPTREC
Cryptography Research and Evaluation Committees

評価項目

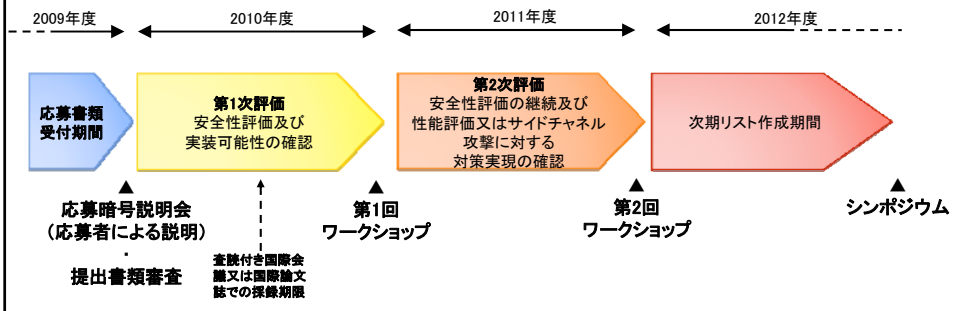
カテゴリ	安全性評価	実装性評価
ブロック暗号	•差分攻撃、線形攻撃などの一般的攻撃 •応募暗号に特化した攻撃、ヒューリスティックな安全性 •サイドチャネル攻撃に耐性の強い実装の作りやすさ	ソフトウエア実装 •処理速度、メモリ使用状況 •鍵スケジュールなど個別の処理速度 ハードウエア実装 •処理速度 •リソース使用数量
ストリーム暗号	•Time/memory/data-tradeoff、分割統治攻撃、代数攻撃などの一般的攻撃 •応募暗号に特化した攻撃、ヒューリスティックな安全性 •サイドチャネル攻撃に耐性の強い実装の作りやすさ	
メッセージ認証コード	•証明可能安全性（適応的選択文書攻撃に対する識別不可能性） •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

(公募要項 p.15)

CRYPTREC
Cryptography Research and Evaluation Committees

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



(公募要項 p.15)

CRYPTREC
Cryptography Research and Evaluation Committees

評価の基本的な考え方
既存のリストに掲載されている暗号よりも、安全性・実装性において優位にあること

2010年度

第1次評価
（応募技術の評価）

1. アルゴリズムの安全性評価
・前回同様に学術的視点から評価

2. 実現可能性の確認
・参照ソースコード
・参照ハードウェア設計記述

2011年度

第2次評価
（応募技術の継続評価、**現リスト再評価**）

3. SW/HW性能評価
・評価環境は2010年10月頃公開予定

4. サイドチャネル攻撃に対する対策実現の確認
・対策を実装で実現できることの確認
・実施詳細は検討中

11

CRYPTREC
Cryptography Research and Evaluation Committees

評価結果は原則公開

「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)」

1.公募の概要
(2)暗号技術評価の実施にあたっては、暗号技術評価に実績のある国内及び国外の専門家に委託した評価や学会及び論文誌等で発表された評価を踏まえ、各暗号技術の安全性及び実装性等の特徴を整理します。その結果は、事務局が開催するワークショップや報告書等を通じて、一般に公表することを予定しています。応募者にとって不利益と解される情報を含むこともあり得ます。

2010年3月頃　応募暗号説明会

2011年2月頃　第1回ワークショップ

2012年2月頃　第2回ワークショップ

2013年2月頃　CRYPTRECシンポジウム2013

CRYPTREC
Cryptography Research and Evaluation Committees

2012年度　次期リスト作成作業(予定)

1) 評価項目にパスした全ての技術は**「推奨暗号候補リスト(仮称)」**に登録
(*「リスト改訂概念図」は2013年以降の運用イメージを記載)

2) 製品化、利用実績、国際標準化などの状況を調査
(評価の詳細は2009年度から審議開始)

3) 製品化・利用実績がある(安定した調達が可能)と判断された技術で
「電子政府推奨暗号リスト(仮称)」を構成

4) リストの正式名称の決定(2012年度以前に決定の見込み)

5) CRYPTRECシンポジウム2013で公開予定

CRYPTREC
Cryptography Research and Evaluation Committees

たくさんのご応募お待ちしております