CRYPTREC

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）

CRYPTREC 事務局

2009 年 3 月 27 日
2009 年 7 月 10 日改訂
2009 年 10 月 1 日改訂

目次

＜添付資料＞

別紙 1 暗号技術応募書（提出資料 1）
別紙 2 誓約書（提出資料 6）
別紙 3 公開の状況等に関する情報（提出資料 7）
別紙 4 自己チェックリスト（提出資料 9）

1．　公募の概要

総務省及び経済産業省が開催している暗号技術検討会（座長：今井秀樹中央大学教授）では、電子政府利用等に資する暗号技術の評価等を行っており、2003年2月に発表した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（以下、「電子政府推奨暗号リスト」又は「現リスト」という。）の改訂を行うことを目的として、「電子政府推奨暗号リストの改訂に関する骨子(案)」（以下、「骨子案」という。）を作成し、2008年8月6日から2008年9月5日までの間、当該骨子案について意見募集[1]を行いました。

意見募集の結果[2]を踏まえ、CRYPTRECでは、「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）」を策定しましたので、公表いたします。

（1）これを受けて、CRYPTREC は評価対象暗号技術を公募し、CRYPTREC 事務局の情報通信研究機構及び情報処理推進機構（以下、「事務局」という。）は、暗号技術評価を実施します。
（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（「9．ワークショップ」を参照のこと。）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。
（3）2009 年度から 2010 年度にかけては、主に応募された暗号技術の評価を実施します。また、2011 年度には、応募された暗号技術の評価を継続するほか、現リストに登録されている暗号技術の再評価も行います。
（4）CRYPTREC 内に設置された暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申します。答申された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定されます。決定については、2012 年度実施を予定しています。なお、仮称付きの語句に関しては、「5．公募の目的」又は骨子案をご覧下さい。

2．　公募の対象

2.1．暗号技術の種別

（1）共通鍵暗号技術

共通鍵暗号技術に関しては、以下の暗号技術の種別に属する方式を公募します。

a)　128bit ブロック暗号　（鍵長 128bit/192bit/256bit）
b)　ストリーム暗号　　（鍵長 128bit 以上）

[1] http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=145207347
[2] http://search.e-gov.go.jp/servlet/Public?ANKEN_TYPE=3&CLASSNAME=Pcm1090&KID=145207347

（2）メッセージ認証コード
鍵長が128bitである128bitブロック暗号及び64bitブロック暗号を利用したメッセージ認証コードを公募します。

（3）暗号利用モード
秘匿に関する128bitブロック暗号及び64bitブロック暗号を対象とした利用モードを公募します。

（4）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、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、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を公募します。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とします。要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能です。

2.2. 応募暗号に関する留意事項

（1） ブロック暗号及びストリーム暗号については、現リストに掲載されている暗号技術と同等以上の特長（安全性又は実装性）を持つ技術に限ります。
（2） 同一の技術的根拠を有する方式に関しては、最善な方式を選択して、1つの暗号技術の種別のみに応募して下さい。
（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。
（4） 国内及び国外において評価が可能であり、かつ、第三者が全ての機能を実装可能となる情報を開示してあるものに限ります。評価を依頼する際に必須なものです。したがって、応募書類受付締切までに公知であることを明確にして下さい。なお、万一応募書類締切時点までに公知にできない理由がある場合には、2009年9月末までに事務局へ相談して下さい。
（5） 評価する際に知的財産の利用が無償で行えるものに限ります。
（6） 公募する暗号技術、又はそれを実装した製品が、電子政府等の利用に際し、次期リスト策定後3年以内までに調達可能なものであることを条件とします。

3. 応募方法

（1）提出期限
2009年10月1日から2010年2月4日17時（必着）までに情報通信研究機構・情報通信セキュリティ研究センター内 CRYPTREC事務局宛てに郵送又は宅配便にて提出

して下さい。また、書類提出は、郵送又は宅配便でのみ受付け、応募者持参による受付は行いません。なお、送料は発信元払いでお願いします。

（2）提出物

提出書類（文書及び電子媒体）（「6．提出書類」を参照のこと。）を 1 つの封筒に入れ、「暗号技術応募」と表に朱記の上、提出して下さい。1 応募暗号技術につき 1 封筒での提出として下さい。

電子媒体については、全ての電子データを CD-R（ISO 9660 Level 1 又は Joliet 形式）にまとめて入れ、暗号技術名と応募者名を記入して下さい。なお、提出物については返却致しませんのでご了承下さい。

（3）応募に関する問い合わせ及び提出先

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 事務局宛
〒184-8795　東京都小金井市貫井北町四丁目 2 番 1 号
e-mail：　info@cryptrec.go.jp
FAX：　042-327-5609
問い合わせの受付は e-mail 又は FAX のみとします（電話での問い合わせは、ご遠慮下さい）。

4．　応募に際しての留意事項

（1）応募に際しては、提出書類（「6．提出書類」を参照のこと。）に漏れが無いことを確認の上、応募者側で自己チェックリストを記入し、提出書類に添えて提出して下さい。
（2）別紙 2（p.22 参照）の誓約書を提出して下さい。
（3）本公募の実施に際し、事務局と応募者との間での金銭の授受は行いません。暗号技術の開発、書類の作成、自己評価その他の応募に際して応募者側で発生する費用、及び追加資料等の作成及び提出、実装性評価時の立会い等に際して応募者側で発生する費用は、応募者が負担して下さい。評価の委託その他の事務局側で発生する費用は事務局が負担します。
（4）評価者（外部評価者を含む）については、審査の公平性の観点から、応募者に対して開示しません。
（5）応募担当者は、適時連絡が取れ、日本語が話せる方として下さい。特に、応募書類受付締切から応募暗号説明会までの期間は、常時連絡が取れるようにお願いします。また、応募担当者の連絡先等に変更が生じる場合は、速やかに事務局へ暗号技術応募書（電子データ含む）の更新版を送付願います。
（6）提出資料の不備、暗号技術に関連する知的財産の実施・利用やライセンス上に問題がある等、評価の実施が困難であると事務局が判断した場合には、応募資格を喪失する場合がありますのでご了承下さい。

5. 公募の目的

5.1. 背景

CRYPTREC は、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アップすることを目的に、2000 年度に暗号技術の公募・評価活動を開始し、2002 年度末に電子政府推奨暗号リスト（以下、「現リスト」という。）を発表しました。

その後、各府省に対してその利用を推奨することにより、電子政府の高度な安全性と信頼性を確保することを目指して、2003 年度から監視活動及び安全性評価を継続して行ってきました。これにより、現リストの信頼性は高められ、また、それらの活動に基づいた暗号の危殆化への対応・提言は電子政府において広く認知されてきました。

現リストには、策定時点において、今後 10 年間は安心して利用できるという観点で選定された暗号が掲載されています。しかし、策定から 5 年余りが経過し、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にあります。

また、今日では CRYPTREC への要望が、暗号技術に対する安全性評価とその周知のみならず、安心・安全な情報通信システムを構築する上で、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するものへと変化しつつあります。

さらに、暗号技術の評価の面において、政府調達等における入手しやすさや導入コスト、相互運用性、普及度合い等の観点も取り入れる必要性が指摘されているところです。

これらの状況を踏まえ、2013 年度以降の電子政府における暗号技術の利用に当たり、信頼性のある暗号技術のリストとして、現リストの改訂を行います。この結果は、電子政府において暗号技術を利用する際の参考として様々な形で利用されることが期待されます。

5.2. 新しい CRYPTREC 暗号リストの構成と本公募の位置づけ

先に述べた背景に従い、2013 年度から、推奨する暗号のリストのみから構成される現リストから、新たな推奨暗号の体系に移行する予定です。

今回の見直しに合わせて、下記の（1）～（3）の各リスト及び(4)リストガイドをまとめて「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）として公開します。

(1) 電子政府推奨暗号リスト
(2) 推奨候補暗号リスト
(3) 運用監視暗号リスト
(4) リストガイド

CRYPTREC により安全性が確認された暗号技術は、（1）～（3）の 3 つのリストのいずれかに登録されます。各リストへの登録は、WTO 政府調達協定との整合性に配慮し

つつ、安全性や市場動向により決定されます。登録の見直しは一定の間隔で行います。
　現リストに掲載されている暗号技術については、安全性の再評価を行った上で次期リスト運用開始前に推奨候補暗号リストへ登録されていたものとして扱います。次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況等により電子政府推奨暗号リストへ登録するか否かの決定を行います。

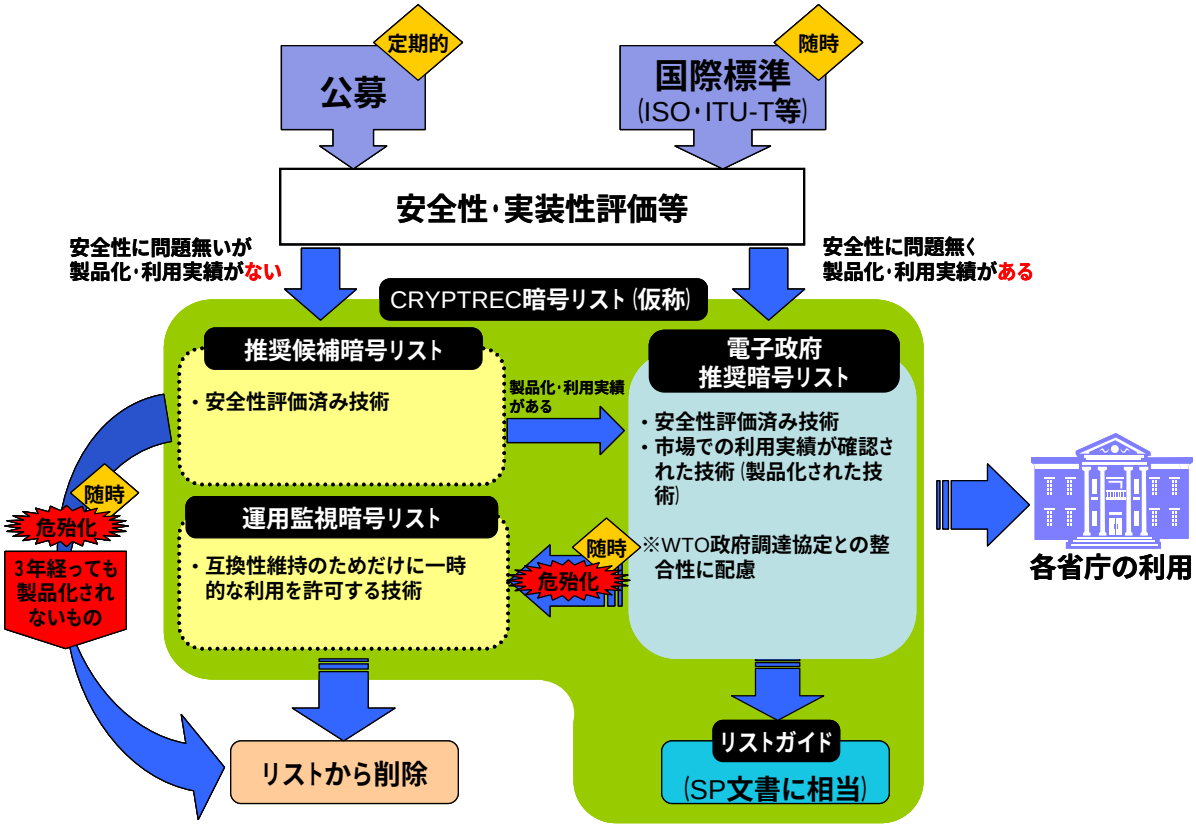

図１．リスト改訂概念（案）

次期リストにおけるそれぞれのリストの役割は以下のとおりです。

(1) 電子政府推奨暗号リスト
　CRYPTREC により安全性が確認され、かつ市場において利用実績が十分である暗号技術リスト。電子政府構築（政府調達）の際には当該技術の利用を推奨します（現リストと同等の位置づけ）。ここに登録される技術は国際標準化機関等により、標準化されていることが望まれます。

(2) 推奨候補暗号リスト
　CRYPTREC により安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類されます。電子政府構築（政府調達）の際には当該技術も利用することができます。

本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リストに登録されます。また、利用実績が十分であると認められなかった場合にはここから削除されます。危殆化が生じた暗号技術については、随時ここから削除されます。

(3) 運用監視暗号リスト

電子政府推奨暗号リストに登録されていたが、実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったもののうち、互換性維持のために継続利用を容認するもののリスト。暗号解読のリスクと、電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断します。CRYPTRECとして互換性維持以外の目的では利用を推奨しません。

(4) リストガイド

電子政府で利用されている、あるいは利用する可能性のある暗号技術について、その技術概要と、推奨する利用方法を記述します。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行います。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載します。リストガイドは、システム運用者及び設計者の利用や、システム利用者への啓発を目的とします。

今回の暗号技術の公募は、現リストにおいて早期にリストの改訂が必要である技術カテゴリを対象として、推奨候補暗号リスト、あるいは電子政府推奨暗号リストへ登録するための、安全性及び実装性の評価を行うことを目的に行います。

6. 提出書類

今回の応募に際して必要な提出書類は以下のとおりです。なお、提出された情報については、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）にて公開する予定です。

項番	提出書類	1.記述言語 2.提出形式	作成要領の書式	電子データのファイル名	参照ページ
6.1	暗号技術応募書	1.和文及び英文 2.文書及び電子データ	別紙 1	和文:09appl_j.pdf 英文:09appl_e.pdf	9
6.2	暗号技術仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09spec_j.pdf 英文:09spec_e.pdf	9
6.3	自己評価書	1.和文及び英文 2.文書及び電子データ	なし	和文:09eval_j.pdf 英文:09eval_e.pdf	10
6.4	テストベクトル	2.電子データのみ	なし	半角英数で、任意	11
6.5	参照ソースコード	1.英文 2.電子データのみ	なし	半角英数で、任意	12
	参照ソースコード仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09sref_j.pdf 英文:09sref_e.pdf	
	参照ハードウェア設計記述	1.英文 2.電子データのみ	なし	半角英数で、任意	
	参照ハードウェア設計記述仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09href_j.pdf 英文:09href_e.pdf	
	テストベクトル生成ソースコード	1.英文 2.電子データのみ	なし	半角英数で、任意	
	テストベクトル生成ソースコード仕様書	1.和文及び英文 2.文書及び電子データ	なし	和文:09tvec_j.pdf 英文:09tvec_e.pdf	
6.6	誓約書	1.和文 2.文書の原本	別紙 2	なし	13
6.7	公開の状況等に関する情報	1.和文 2.文書及び電子データ	別紙 3	和文:09publ_j.pdf	13
6.8	応募暗号説明会発表資料	1.和文及び英文 2.文書及び電子データ	なし	和文:09brfg_j.pdf 英文:09brfg_e.pdf	14
6.9	自己チェックリスト	1.和文 2.文書の写し	別紙 4	なし	14

表 1．提出書類一覧

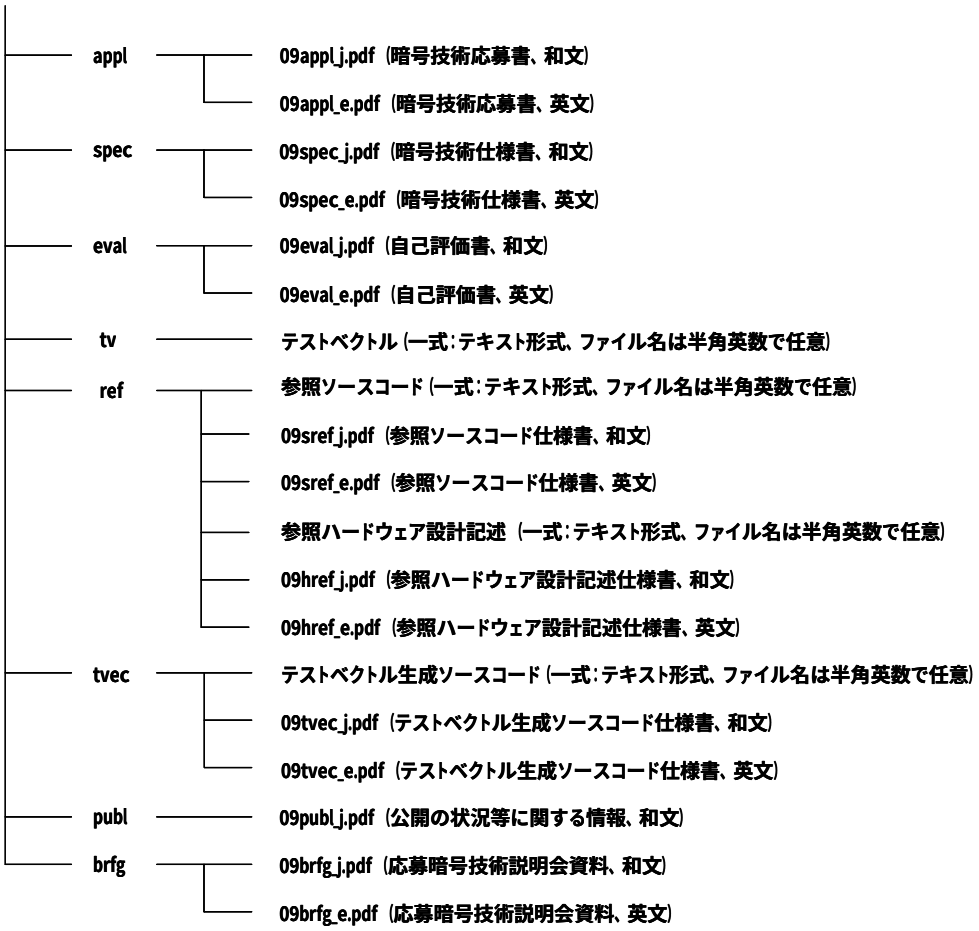

図 2．提出書類（電子データ）の構成図

ⅰ）提出書類となる各種電子ファイルは、上に示すようなファイル名（半角英数）をつけて下さい。

ⅱ）電子ファイルは、それぞれ上に示すようなディレクトリを作成し、対応するディレクトリ直下に保存して下さい。（ディレクトリ名は半角英数）

注）

○文書については、全て日本工業規格 A4 判として下さい。

○6.1～6.3、6.5 及び 6.8 は、和文・英文両方の提出が必要です。和文を正文とし、両者の内容に齟齬があった場合は和文を優先しますが、可能な限り同一の内容として下さい。評価の実施に関して支障が出る場合には応募資格を喪失することもあり得ます。

○6.1～6.3、6.5、6.7 及び 6.8 のファイル形式については、以下のものとし、表 2 に示したファイル名を使用して下さい。

・Adobe PDF 形式

日本語版：Adobe Acrobat 日本語フォントで読めるもの

英語版：Adobe Acrobat で読めるもの

○6.4 及び 6.5 のプログラムの電子データについては、テキスト形式として下さい。

○評価においては国外における評価も想定していますので、提出書類のうち 6.1～6.3、6.5 及び 6.8 の電子媒体については、全ての電子データを CD-R(ISO 9660 Level 1 又

は Joliet 形式)にまとめて入れ、暗号技術名と応募者名を記入して下さい。

それぞれの提出書類について、以下に説明します。

6.1. 暗号技術応募書（別紙 1 の書式）

ⅰ）応募日
・応募書提出日を記入して下さい。

ⅱ）暗号技術名
・正式名称を読み方も含めて記述して下さい。また、正式名称が長い場合は、略称名を 5 文字程度のアルファベット表記で記述して下さい。

ⅲ）応募暗号技術公開ホームページ URL
・国内外の暗号技術者が、評価を行う際に必要となるデータを参照できるホームページ URL を記入して下さい（和文及び英文）。

ⅳ）応募暗号種別
・該当する項目を 1 つだけ選択して下さい。

ⅴ）応募責任者
・今回の応募に関する一切の責任を負う方とします。
・本応募に関する責任者の企業・団体名、所属・役職及び氏名を記入して下さい。

ⅵ）応募担当者
・今回の応募に関し、事務局との問い合わせ・連絡窓口となる方とします。
・本応募担当者は、日本語が話せる方として下さい。
・応募担当者の氏名、企業・団体名、所属・役職、所在地、電話番号（代表、直通を明記）、FAX 番号及び e-mail アドレスを記入して下さい。

ⅶ）開発者
・開発者の氏名及び企業・団体名を記入して下さい。

ⅷ)応募暗号調達窓口
・次期リスト策定後 3 年以内までに調達可能であることが応募条件であることから、応募暗号技術を調達する場合の窓口（連絡先）を記述して下さい。
・応募時点で正式な調達窓口が設置されていない場合においても、調達に関する問い合わせに答えられる仮窓口を記述して下さい。

ⅳ)応募暗号説明会
・応募暗号説明会における発表予定者名、参加人数を記述して下さい。

6.2. 暗号技術仕様書

ア　設計方針、設計基準
ⅰ)応募暗号技術についての設計方針及び設計基準を記述して下さい。
ⅱ)共通鍵暗号の場合は、現リストに記載された暗号技術と同等以上の特長（安全性又は実装性等）についても記述して下さい。

イ　暗号アルゴリズム（実装に必要な全情報）
第三者が評価・実装するために十分な仕様が完全に記述されていることが必

要です。記述が十分でない場合、応募資格を喪失することがあります。具体的には以下に従って下さい。

ⅰ）暗号アルゴリズムの完全な仕様を記述して下さい。アルゴリズムの実装に必要なすべての情報（数式、テーブル、アルゴリズム、図及びパラメータ）を記述して下さい。

ⅱ）暗号鍵等のパラメータの設定に条件がある場合には、パラメータの設定基準、推奨値も記述して下さい。

ⅲ）共通鍵暗号で複数の鍵長をサポートする場合には、互換性の有無に関しても明記して下さい。

ⅳ）応募技術の入出力は、ビット列レベルで記述して下さい。

ⅴ）入力が Z/nZ（Z は有理整数環）の元等、実装する上で実現法が一意に定まらない場合は、ビット列への変換法の推奨方式も同時に提示して下さい。

ⅵ）endian の種類を記述して下さい。

ⅶ）高速実装やコンパクト実装に関する方法等があれば記述して下さい。

ⅷ）実装方法についての説明

本応募暗号技術を実装するために必要な実装手順等の情報を記述して下さい。

情報が不十分であるために実装ができない場合には、応募資格を喪失することがあります。

また、評価に必要な情報の追加提出を求めることがあります。

ウ　バージョン情報

今回の応募以外に、同一若しくは類似した名称で他に発表又は応募した暗号技術、同一仕様で名称が異なった暗号技術等があれば列挙して下さい。

また、それぞれの相違点を明記して下さい。また、バージョン更新時に推奨パラメータが変更された場合には、変更した理由を明記して下さい。

バージョンの更新について、設計思想、安全性及び実装性の違いを明確に記述して下さい。また、バージョン更新をした理由についても明記して下さい。

異なるバージョン間における互換性の有無を完全に記述して下さい。バージョンが異なる場合に想定されるユーザー側のメリット及びデメリットについても記述して下さい。

エ　利用実績・推奨用途等

応募暗号技術に係る利用実績や推奨用途について記述して下さい。

6.3. 自己評価書

応募される暗号技術に対する応募者自身による自己評価情報を記述して下さい。自己評価が十分でないと判断される場合には、応募資格を喪失することがあります。

また、ウ・エ・オ・カの項目については詳細に記述して下さい。

ア　設計思想

他の著名な暗号技術との差別化、優位性等も含め記述して下さい（既存の技術と比べて優位性がある部分、提案技術が電子政府で使用するものとして妥当であると考えられる部分等）。

イ　ベースとして用いる理論（数学的仮定）・技術

応募される暗号に、ベースとして用いられている理論（数学的仮定）や技術について記述して下さい。

ウ　安全性に対する評価

応募される暗号の安全性に関する根拠及び通常想定される汎用的な攻撃法に対する対抗策を具体的に示して下さい。

想定する攻撃法に関しては、「7．評価項目」を参考にして下さい。なお、評価項目に例示されている攻撃法が適用できない場合には、評価は必要ありませんが、その攻撃法が適用できないと判断した理由を明示して下さい。但し、全く自己評価がなされていない場合は、応募資格を喪失する場合があります。

応募暗号に固有の特殊な攻撃法が想定される場合には、その攻撃法に対し施した対抗策についても具体的に提出して下さい。

提案方式に対する既知の攻撃論文の有無や学会(ASIACRYPT、CRYPTO、EUROCRYPT、FSE、ISEC、PKC、SCIS 等)等で攻撃や問題点が指摘されている場合には、その攻撃論文を引用し、これに対する技術的コメントを記述して下さい。

証明可能安全性を主張する場合にはそのレベルを記述し、その論証を行うか、学会等で発表されているならその論文等について記述して下さい。

エ　ソフトウェアの実装性評価

速度評価、リソース使用量（コード量・ワークエリア）、記述言語、評価プラットホーム等を記述して下さい。また、実際に速度計測を行った場合には、計測法を詳細に記述して下さい。

※ブロック暗号に関しては、鍵スケジュール部単独の速度評価結果も記述して下さい。

オ　ハードウェアの実装性評価

使用したプロセス（Field Programmable Gate-Array、Gate-Array 等）、速度評価、設計環境、リソース使用量（Field Programmable Gate-Array の場合は使用セル量、Gate-Array 等の場合はゲート数）等を記述して下さい。

※ エンティティ認証は対象外です。

カ　サイドチャネル攻撃に対する評価

本項目は、自己評価書の提出に当たっては必須ではありませんが、サイドチャネル攻撃に対する耐性を主張する場合には、攻撃法、施した対抗策及び動作環境等についてできるだけ詳しく記述して下さい。学会等で発表されているならその論文等について記述して下さい。

キ　第三者評価実績

既に第三者評価を受けた実績がある場合には、評価者名及び評価結果を記述して下さい。開示可能であれば、報告書のコピーもあわせて（できるだけ電子データで）添付して下さい。

6.4. テストベクトル

実装性確認のために十分な量のテストベクトルを記述して下さい。十分な量のテストベクトルが提出されないときには応募資格を喪失することがあります。テストベクトルは暗号処理途中の中間結果と、暗号全体をブラックボックスと見な

したときの入出力対の 2 種類を提出して下さい。どちらのファイルもテキスト形式で生成し、キャラクタセットとしては ASCII のみを使って下さい。改行コードは MS-DOS 形式(CR+LF)とします。

暗号処理途中の中間結果については、応募暗号技術を第三者が実装する上でデバッグの役に立つ情報について、少なくとも入出力 1 対に対応するデータをなるべく詳しく記述して下さい。例えば、共通鍵暗号については繰り返し処理ごとの入出力等を記述して下さい。

暗号全体をブラックボックスと見たときの入出力対については、以下に示す応募する暗号技術ごとの方針に従って下さい。どの暗号技術についても、テストベクトルには endian の間違い等ビット列表記が反転した場合等を検出できるデータを含む等、テストベクトルとして相応しい入出力を選んで下さい。

乱数を用いる場合は、再度検証可能なように、擬似乱数生成系を用い、種(Seed)を明示して下さい。

ア　共通鍵暗号技術

ⅰ)ストリーム暗号

10 例以上の鍵に対し、8192bit 以上の処理例

ⅱ)ブロック暗号

10 例以上の鍵に対し、128 ブロック以上の処理例

イ　メッセージ認証コード

3 例以上の鍵に対し、3 例以上の処理例

ウ　暗号利用モード

3 例以上の鍵に対し、3 例以上の処理例

エ　エンティティ認証

共通鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。

公開鍵暗号を利用する場合には、3 例以上の鍵に対し、3 例以上の処理例。テストベクトルには、ランダムに生成されたデータを含んで下さい。また、ベキ乗剰余等の数学的構造を含む場合は、境界条件となるデータを含んで下さい。

なお、再度検証可能なように、擬似乱数生成系を用い、種（Seed）を明示して下さい。

6.5. 参照ソースコード

ⅰ） 応募暗号技術の実装が実際に可能であることを確認するため、また応募暗号技術に関連する各種データの正当性の効率的な検証を可能とするために参照ソースコードとその仕様書を提出して下さい。

参照ソースコードは、ソフトウェアの実装性評価向けには ANSI C で、ハードウェアの実装性評価向けには Verilog-HDL で記述して下さい。なお、この目的を達成するため、参照ソースコードを見難くするような、処理中の機微データをゼロクリアする等の安全性を高めるような部分を記述する必要はありません。

ⅱ） 参照ソースコードでは、推奨パラメータを含む応募暗号技術の全ての機能を

実現して下さい。さらに、参照ソースコードの可読性を落とさない範囲で移植性の高いものとして下さい。例えば、ソフトウェア評価の場合には、endian 非依存とし、最低限 int、long、pointer の長さが 32bit の処理系で動くように作成して下さい。多倍長整数を利用する場合は GNU MP ライブラリなどの利用を推奨します。

iii) テストベクトル生成ソースコードとその仕様書も提出して下さい。テストベクトル生成プログラムは参照ソースコード中の関数を呼び出すものとします。

6.6. 誓約書（別紙 2 の書式）

本項目に関しては、別紙 2 の書式に従って記述して下さい。提出がない場合には、応募資格を喪失しますのでご留意下さい。

6.7. 公開の状況等に関する情報（別紙 3 の書式）

本項目に関しては、別紙 3 の書式に従い下記ア～ウの内容について記述して下さい。

ア　応募暗号技術の公開時期とその学会名

本公募では、仕様等が公開されている暗号技術を評価対象としていますので、仕様等の公開の状況を確認するために必要な情報（応募暗号技術が公開された時期、学会名、あるいは掲載文献名等）を提出して下さい。なお、応募時点で仕様等の公開がなされていない場合には、その時点での状況とともに、2010 年 9 月末までの公開スケジュールを提出し、応募暗号技術に関する論文発表や仕様書等の公開された際には、その状況を確認するために必要な情報を提出して下さい。

イ　輸出規制問題を解決していることの宣誓書とその証拠

応募された暗号技術の評価については、事務局より評価の一部を海外を含めた評価者に外部委託することを予定しており、提出された情報を我が国の非居住者である委託者に提供すること等も予想されます。このため、「6．提出書類」の 6.1～6.5 及び 6.7 の情報のそれぞれについて、非居住者への提供等に際して輸出管理上許可が不要であると考える場合には、その根拠及び確認のための文書を提出して下さい（例えば、学会誌、雑誌、論文集等で既に公開されており不特定多数の方が自由に入手できる情報であるため許可不要と考える場合には、当該学会誌、雑誌、論文誌等の関連部分等を提出するとともに、公開形態についての説明を加えて下さい）。

ウ　知的財産権とライセンス

応募された暗号技術に関して取得あるいは出願中の特許、著作権、ライセンス方針等の知的財産に関する状況を応募書類の「自社特許とその扱い」の中で記述して下さい。

応募された暗号技術に関連し、他社が特許権、著作権等の知的財産を保有する場合、それらの権利関係についても、応募書類の「関連する他社の特許」の

中で可能な範囲で記述して下さい。

事務局及び評価者が評価の実施に際して必要となる知的財産の利用（特許法上の発明の実施、著作権法上の著作物（全ての応募書類）の複製・領布等、事務局が評価を委託する第三者による利用を含む）を無償で行えることを明記して下さい。知的財産上の制限により評価の実施が妨げられる場合は、応募資格を喪失することがあります。

また、政府機関で使用する場合のライセンス方針を記述して下さい（無償又は、妥当かつ非差別的な条件に限ります）。

なお、評価のために、事務局及び評価者が応募者と、秘密保持契約等の特別な契約を結ぶことはいたしません。

6.8. 応募暗号説明会発表資料

応募される暗号技術についての説明資料を作成し、Adobe PDF 形式にて提出して下さい。資料構成としては、以下を参考にし、説明内容は 15 分程度のもので作成して下さい。なお、白黒のハードコピーが配布資料となることにご留意下さい。

<資料構成>

１．表紙（応募暗号名、発表者名を記載）
２．技術仕様について
３．安全性に関する自己評価について
４．実装性に関する自己評価について
５．公開状況、ライセンス等について

6.9. 自己チェックリスト（別紙 4 の書式）

「自己チェックリスト」に従って内容を確認して下さい。このチェック結果を記入した「自己チェックリスト」の写しを、提出物と同じく封筒に入れて提出して下さい。

7.　評価項目

7.1.　評価スケジュール（予定）

CRYPTREC シンポジウム 2010(応募暗号説明会併催)：　2010 年 3 月 2 日・3 日
第 1 次評価実施：　2010 年 4 月～2011 年 3 月
第 1 回ワークショップ開催：　2011 年 2 月頃
第 2 次評価実施：　2011 年 4 月～2012 年 3 月
第 2 回ワークショップ開催：　2012 年 2 月頃
2012 年度シンポジウム：　2013 年 2 月頃

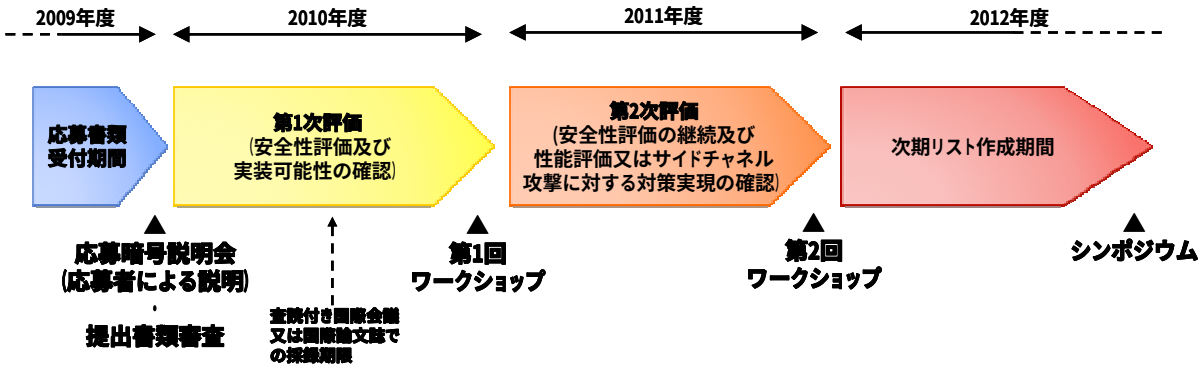

図 3．評価スケジュール（予定）

7.2.　共通鍵暗号技術

共通鍵暗号については、現リストに掲載されている暗号技術と比較して安全性又は実装性において優れた暗号技術を公募します。そのため、評価においても現リストに掲載された暗号に対する優位点の評価を行います。

（１）安全性評価項目

暗号は守秘目的以外にも利用されるので、いわゆる暗号文単独攻撃以外の既知平文攻撃、(適応的)選択平文・暗号文攻撃、関連鍵攻撃、選択IV攻撃等、攻撃者にとって非常に都合のよい環境での耐性も評価します。

ア　ブロック暗号に関する評価項目

差分攻撃法や線形攻撃法等の既知の一般的な攻撃法に対する耐性を評価します。また、応募暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがあります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

イ　ストリーム暗号に関する評価項目

time/memory/data-tradeoffや分割統治攻撃、相関攻撃、またGroebner基底計算アルゴリズムを元にした代数攻撃等の既知の攻撃法に対する耐性を評価しま

す。また、応募暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがあります。その他、サイドチャネル攻撃等に対する耐性についても評価します。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用量（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソースの使用状況（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.3. メッセージ認証コード

（1）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択文書攻撃や、検証オラクルを多数回呼び出したときの識別不能性について評価します。また、nonce や乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher modelや関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.4. 暗号利用モード

（1）安全性評価項目

利用ブロック暗号をもとにした証明可能安全性、特に適応的選択平文・暗号文攻撃に対する識別不能性について評価します。また、nonceや乱数要素の有無についても評価します。さらに利用ブロック暗号に対する仮定の強さ(ideal cipher modelや関連鍵攻撃耐性)についても評価します。さらに、利用ブロック暗号に特定の方式を適用した場合の安全性についても評価の対象とすることがあります。

（2）実装性評価項目

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

イ　ソフトウェア実装による評価項目

ソフトウェア実装に関しては、次の項目について評価します。

ⅰ）標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。

ⅱ）鍵スケジュール個別の処理速度も評価します。

ウ　ハードウェア実装による評価項目

使用するプロセス（Field Programmable Gate-Array、Gate-Array 等）別に、処理速度評価及びリソース使用量（Field Programmable Gate-Array の場合には使用セル数、Gate-Array 等の場合には使用ゲート数等）を評価します。

7.5. エンティティ認証

（1）安全性評価項目

安全性の評価は、エンティティ認証としてのセキュリティに問題が生じないことを、形式的な手法を用いて行います。安全性を脅かす状態としては、なりすましの成功、セッションの取り換え等を想定します。

暗号プリミティブとして、電子政府推奨暗号リストに掲載されている、あるいは応募中の共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードのみを利用している場合には、暗号プリミティブを理想的に安全なものとして安全性の評価を行います。その他の暗号プリミティブを用いる場合には、暗号プリミティブを理想化せずに安全性の検証を行います。

上記のいずれの場合も、提案者はプロトコルの安全性を示す情報を提出し、本公募における安全性評価では、これらの正当性を検証します。

（2）実装性評価項目

エンティティ認証プロトコルの実装性能評価として、ソフトウェアによる実装性評価を行います。標準的なプラットホーム上での処理速度、リソースの使用状況（コード量、作業領域等）等を評価します。通信時間は考慮しません。

ア　共通条件

「7.6 実装性評価について」を参照して下さい。

7.6. 実装性評価について

実装性評価について共通的な条件を記述します。実装性評価を行う目的は、

- 実現可能性の確認、
- 性能の評価
- サイドチャネル攻撃に対する対策実現の確認

の 3 つです。

（1）実現可能性の確認

- 提案された暗号アルゴリズムが、事務局が指定した動作環境において実装可能であり、かつ、動作可能であることを確認することが目的です。応募時に提出されたテストベクトルを処理できることを確認します。第 1 次評価期間内に実施します。
- 実現可能性の確認で用いた参照ソースコード及び参照ハードウェア設計記述は、性能の評価には利用しませんが、第三者が実装する場合の参考として公開する予定です。想定している動作環境は、以下のとおりです。
- 暗号利用モード及びメッセージ認証コードの実装性評価では、128bit ブロック暗号及び 64bit ブロック暗号を使用するものとします。ここで用いるブロック暗号は、事務局から提供します。

（i） ソフトウェアでの実現可能性の確認のための動作環境

- CPU: Intel x86 アーキテクチャ互換のプロセッサ
- Memory: 2GB 以上
- OS: Microsoft Windows のいずれかのエディション

（ii）ハードウェアでの実現可能性の確認のための動作環境

- FPGA： Xilinx FPGA XC5VLX30、もしくは、XC5VLX50

また、設計環境としては以下のとおりです。

（i） ソフトウェアでの実現可能性の確認のための設計環境

- 記述言語： ANSI-C 言語
- Compiler: Microsoft Visual Studio

（ii）ハードウェアでの実現可能性の確認のための動作環境

- 設計記述言語： Verilog-HDL
- 論理合成： Xilinx ISE Foundation
- 配置配線： Xilinx ISE Foundation
- 論理シミュレーション： Mentor Graphics ModelSim

（2）性能の評価

- 性能の評価は、安全性評価及び実現可能性の確認を通過し、次期リストへの掲載が可能と判断された暗号技術に対して第 2 次評価期間内に実施します。
- 性能の評価を行う動作環境については、実現可能性の確認で使用する動作環境に準じるものを想定していますが、性能の評価を実施する上で必要となる情報は、安全性評価及び実現可能性の確認の段階（2010 年 10 月頃）で、公開する予定です。
- 性能の評価で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことを想定しています。詳細については、2010 年度末までに CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。
- ソフトウェアの性能の評価に関しては、通常の PC 環境における性能を測定します。各暗号技術の種別毎の評価項目については、7.2 から 7.5 の該当する評価項目を参照して下さい。処理速度のほか、リソース使用量（静的メモリ量、動的メモリ量）の評価を想定しています。
- ハードウェアの性能の評価に関しては、FPGA 環境における性能をシミュレーションにより測定します。回路規模、クリティカルパス遅延及びスループットの測定を想定しています。

（3）サイドチャネル攻撃に対する対策実現の確認

- サイドチャネル攻撃に対する対策を実装アルゴリズムで実現できることを確認することが目的です。ソフトウェア実装及びハードウェア実装の両方を対象とします。第 2 次評価期間内に実施します。
- 原則として、提出された自己評価書に記述された対策技術を確認の対象としますが、応募書類提出後に学会又は論文誌に採録された応募暗号に関する対策についても、脅威の重要度・実現性等を考慮して、暗号実装委員会が別途認めたものを確認の対象とすることがあります。
- サイドチャネル攻撃に対する対策実現の確認で使用する実装については、事務局からソースコードの提出を要求しませんが、事務局が指定する動作環境にて実行可能なロードモジュールを応募者側で実装して頂き、事務局立会いにて実地で測定を行うことも想定しています。詳細については、2010 年度末までに CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

8. 応募暗号説明会について

応募された暗号技術の評価を開始するにあたり、応募者自ら公の場で、応募暗号技術の技術仕様、安全性、実装性、公開状況、及びライセンス等について説明する機会を設けます。本説明会は一般公開とし、全応募者が説明することを原則とします。

説明時間を 15 分程度、質疑応答時間を 10 分程度取ることを予定していますが、応募者数が多い場合には短くなることがあります。

応募暗号説明会は、2010 年 3 月 2 日・3 日に開催する予定の「CRYPTREC シンポジウム 2010」と併催されます。プログラムなどの詳細については、確定し次第、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

応募者数の事前把握のため、応募を予定されている方は CRYPTREC 事務局まで事前に連絡くださるようお願い致します。締め切りは 2009 年 11 月 30 日(月)とします。なお、この事前連絡は任意であって、書類等の提出の必要はありません。

9. ワークショップについて

ワークショップ（「7.1 評価スケジュール（予定）」を参照のこと。）は、開催時点までの暗号方式委員会及び暗号実装委員会における最新の評価結果を公表し、それらを検討する場を設けるために開催されます。この機会を利用して、応募者が自らの意見を述べることもできます。

第 1 次評価実施期間（2010 年 4 月～2011 年 3 月）の後に開催予定の第 1 回ワークショップでは、応募暗号技術の安全性評価及び実現可能性の確認結果を公表する予定です。

第 2 次評価実施期間（2011 年 4 月～2012 年 3 月）の後に開催予定の第 2 回ワークショップでは、第 1 次評価実施期間後に継続して実施された安全性評価、性能の評価及びサイドチャネル攻撃に対する対策実現の確認結果を公表する予定です。また、現リストに掲載されている暗号技術に関する再評価の結果も公表する予定です。

詳細については、各年度の 10 月頃に正式日程を CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

10. シンポジウムについて

シンポジウム（「7.1 評価スケジュール（予定）」を参照のこと。）は、それまでに実施されてきた電子政府推奨暗号リストの改訂、暗号技術公募と評価活動及び次期リスト策定に関して、広く一般に報告するために開催することを想定しています。詳細については、確定し次第、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定です。

以　上

（別紙 1）

受付番号	

応募日　20　　年　　月　　日

CRYPTREC 事務局　御中

暗号技術応募書（提出資料 1）

<table>
<tr><td colspan="4">暗号技術名：</td><td colspan="2">略称名：</td></tr>
<tr><td colspan="6">応募暗号技術公開ホームページURL：</td></tr>
<tr><td colspan="6">応募暗号種別</td></tr>
<tr><td colspan="2">１．共通暗号技術</td><td colspan="4">a)128bitブロック暗号　b)ストリーム暗号</td></tr>
<tr><td colspan="6">２．メッセージ認証コード</td></tr>
<tr><td colspan="6">３．暗号利用モード</td></tr>
<tr><td colspan="6">４．エンティティ認証</td></tr>
<tr><td colspan="6">応募責任者</td></tr>
<tr><td colspan="6">企業・団体名：</td></tr>
<tr><td colspan="2">責任者氏名：</td><td>印</td><td colspan="3">所属・役職：</td></tr>
<tr><td colspan="6">応募担当者</td></tr>
<tr><td colspan="6">企業・団体名：</td></tr>
<tr><td colspan="3">担当者氏名：</td><td colspan="3">所属・役職：</td></tr>
<tr><td colspan="6">所在地：〒</td></tr>
<tr><td colspan="3">TEL：（代表）</td><td colspan="3">（直通）</td></tr>
<tr><td colspan="3">FAX:</td><td colspan="3">e-mail:</td></tr>
<tr><td colspan="6">開発者</td></tr>
<tr><td colspan="3">開発者名：</td><td colspan="3">企業・団体名：</td></tr>
<tr><td colspan="6">応募暗号調達窓口</td></tr>
<tr><td colspan="3">担当者氏名：</td><td colspan="3">所属・役職：</td></tr>
<tr><td colspan="3">企業・団体名：</td><td colspan="3">所在地：〒</td></tr>
<tr><td colspan="2">TEL:</td><td colspan="2">FAX:</td><td colspan="2">e-mail:</td></tr>
<tr><td colspan="6">応募暗号説明会</td></tr>
<tr><td colspan="4">発表者氏名：</td><td colspan="2">参加人数：</td></tr>
<tr><td colspan="2">TEL:</td><td colspan="2">FAX:</td><td colspan="2">e-mail:</td></tr>
</table>

（別紙 2）

CRYPTREC 事務局宛

誓約書（提出資料 6）

このたび、「電子政府推奨暗号リスト改訂のための暗号技術公募」への応募にあたり、以下の事項について、ここに誓います。

記

1. 応募暗号技術○○○○○○○○に関するすべての技術は公知であり、提出書類を国外の評価者等に提供することは輸出管理上の許可が不要であること
2. 応募暗号技術○○○○○○○○の評価において、事務局との間において金銭等の授受を行わないこと
3. 応募暗号技術○○○○○○○○に係る評価を行う際に、当該暗号技術に関連する特許権、著作権等の知的財産の実施・利用について、CRYPTREC 検討会事務局（外部評価者を含む）に対して、無償で通常実施権や利用許諾等を与えること。
4. 応募暗号技術○○○○○○○○に関する特許権、著作権等の知的財産については、それを利用する製品等に対して、無償又は妥当かつ非差別的な条件で、通常実施権、利用許諾等を与えること
5. 応募暗号技術○○○○○○○○の評価において、不利益と解される情報を含むことがあっても異議を申し立てないこと
6. 応募暗号技術○○○○○○○○が、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ない場合には、応募資格を喪失することに異議を申し立てないこと
7. 応募暗号技術○○○○○○○○を使用する製品は、｛既に製品化され調達可能になっている／CRYPTREC 暗号リスト（仮称）策定後 3 年以内に製品化がなされるよう鋭意努力する｝こと
8. 応募暗号技術○○○○○○○○の評価結果の如何に関わらず、CRYPTREC 暗号リスト（仮称）に掲載されなくても異議を申し立てないこと

20○○年○月○日

応募暗号責任者
会社名・部署名　○○○○○○○○
住　所　○○○○○○○○丁目○番○号
氏　名　○○○○○○　　印

以　上

（別紙 3）

各項目の記入スペースの配分は応募者の任意とします。1 ページに収める必要はありません。

公開の状況等に関する情報（提出資料 7）

暗号技術名：
応募責任者名： 印
ⅰ)応募暗号技術を発表した国際会議又は国際論文誌に関する情報を列挙して下さい： 発表期日： 発表者： 会議名又は論文誌名：
ⅱ)輸出管理 輸出管理上の許可が不要であることを示す根拠に関する情報を列挙して下さい：
ⅲ) 知的財産とライセンス方針： 応募暗号技術に関連する知財権などに関する情報を明記して下さい。また、電子政府で使用する際のライセンス方針を明記して下さい：
ⅳ)調達可能性について 応募暗号技術が既に製品等で利用されている場合には、その製品名に関する情報を列挙して下さい：
その他関連事項等あれば記載して下さい。

（別紙 4）

自己チェックリスト （提出書類 9）

暗号技術名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本チェックリストは、あくまでも事務手続き上のチェックリストです。
下記内容が確認できたら、□部分を黒く(■)塗りつぶして使用します。

＜チェック項目＞

□ 1.応募暗号技術は、次期リスト策定後、3 年以内に製品化がなされ、調達可能ですか？
□ 2.応募暗号技術は、応募書類受付締切までに公知となっていますか？
□ 3.応募暗号技術は、査読付きの国際会議、国際論文誌に採録されていますか？
□ 4.一つの暗号技術の種別のみに応募していますか？
□ 5.応募暗号技術は、今回公募する暗号技術の種別に該当しますか？
□ 6.応募に必要な以下の提出物（文書・電子データ）が揃っていますか？
［暗号技術応募書、暗号技術仕様書、自己評価書、テストベクトル、参照ソースコード、誓約書、公開状況等に関する情報、応募暗号説明会資料、自己チェックリスト］
□ 7.以下の内容が網羅されていますか？

●暗号技術応募書（P．9)
□ 8.応募暗号技術公開ホームページ URL が記載されていますか？
□ 9.応募担当者は、適時連絡が取れ、日本語が話せる方ですか？
□10.応募担当者の電話番号（代表、直通を明記)、FAX 番号、e-mail アドレスをもれなく記入していますか？

●暗号技術仕様書（P．9)
□11.応募暗号が現リストに掲載されている暗号技術と同等以上の特長を持つ点について記述していますか？
□12.実装に必要な全情報を記載していますか？
□13.応募暗号技術は第三者が全ての機能を実装可能ですか？
□14.今回の応募以外に、同じような名称で他に発表又は応募した暗号技術があれば列挙していますか？

●自己評価書（P．10)
□15.十分な自己評価が記載されていますか？

●テストベクトル（P．11)
□16.公募要項に示された要求件数以上のテストベクトルが提出されていますか？

●参照ソースコード（P．12)
□17.実装動作確認済ですか？
□18.テストベクトル生成ソースコードは添付されていますか？

●誓約書(P．13)
□19．提出資料に誓約書は含まれていますか？

●公開の状況等に関する情報（P．13)
□20.応募暗号技術の公開時期とその学会名は記述されていますか？
□21.輸出規制問題を解決していることの証拠について記載及び資料添付されていますか？
□22.知財権とライセンスについて記載されていますか？
□23.ライセンス方針は、電子政府における利用において無償か、あるいは、妥当かつ非差別的な条件となっていますか？

●応募暗号説明会発表資料（P．14)
□24.提出資料に応募暗号説明会発表資料は含まれていますか？