暗号技術
公募要領

情報処理振興事業協会
セキュリティセンター

平成１２年７月５日
確定版

暗号技術　公募要領

情報処理振興事業協会
平成１２年6月１３日
確定版　平成１２年7月5日

１．事業の目的

政府は､平成１５年度（２００３年度）までに行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指しています。

電子政府の構築は、デジタル経済・社会の一つのモデルであり、その中で実施される情報セキュリティ確保のための対策もまた、広く民間の範となり、それによって、我が国のネットワーク全体の安全性・信頼性を高めることが期待されます。

本事業の目的は、電子政府における情報セキュリティの基盤技術である各種暗号技術を公募し、応募された暗号技術について、専門的・客観的見地から評価・調査を実施し、電子政府のシステム構築において利用可能な技術につき、安全性、実装性等の特徴をリストとして政府に提出することです。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政府部内で様々な形で利用されることが期待されます。

２．事業の概要及びスケジュール

本事業は、通商産業省の電子政府情報セキュリティ技術開発事業の一環として同省からの委託を受けて、情報処理振興事業協会が行う調査事業であり、暗号技術の専門的知見を有する方々から構成される「暗号技術評価委員会」を組織してこの事業を実施します。具体的には、以下を行います。

（１）電子政府のシステム構築において利用可能な暗号技術について公募します。
（２）暗号技術のカテゴリー毎に、評価基準を定めます。
（３）評価基準に従って、応募された暗号技術、その他評価が必要と判断される暗号技術について評価を行います。評価はスクリーニング評価と詳細評価の２段階で行い、詳細評価はスクリーニング評価を通過したもののみを対象とします。具体的な評価の実施は、暗号技術評価に実績のある国内外の評価者に外

部委託することがあります。
（４）外部委託による評価や学会等で発表された評価等も踏まえ、各暗号技術の安全性、実装性等の特徴を整理します。その結果は、政府部内での利用に供するほか、公表が適当と判断される部分につい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）。

暗号評価スケジュール

評価基準の公開（済）：	平成１２年７月５日
応募の締め切り：	平成１２年７月１４日
スクリーニング評価の実施：	平成１２年８月～９月
スクリーニング評価結果の公表：	平成１２年１０月初旬
詳細評価の実施：	平成１２年１０月～１２月
詳細評価結果の公表：	平成１３年２月以降

３．公募の対象

以下の分類（１）・（２）・（３）・（４）の暗号技術について、電子政府のシステム構築に当たって利用可能な技術を評価対象として公募します。多くの評価者に評価いただくため、及び、多くの実装者（ベンダー）に様々な用途で活用していただくために、仕様等が公開された暗号技術を公募の対象としています。

（１） 公開鍵暗号

公開鍵暗号については、守秘・認証・署名・鍵共有いずれかの一つの機能を実現する実現例付きの暗号方式を公募します。複数の機能を同時に実現できる場合には、主要な機能を一つ指定して下さい。主要な機能を指定する仕方が複数ある場合は、別の暗号方式として応募して下さい。

ここで、暗号方式（暗号スキーム）とは、基本暗号（暗号プリミティブ）と補助関数（暗号補助関数）とを用いて機能を発揮させるアルゴリズムを指し、基本暗号の要件と、補助関数の要件と、アルゴリズムの記述とからなります。

基本暗号とは、素因数分解問題、離散対数問題、楕円曲線上の離散対数問題、その他の安全性根拠に基づく安全性を有する要素暗号アルゴリズムです。

補助関数とは、ハッシュ関数や乱数（疑似乱数）等、暗号方式が機能を発揮する上で、基本暗号の外に必要となる要素を指します。

暗号方式の実現例とは、暗号方式において以下の手順により定まる具体的暗号で、それをソフトウェアまたはハードウェアで実装できるものを指します。

まず、暗号方式を定めて下さい．次に、基本暗号および補助関数を具体的に定めてください。新規の補助関数については、本公募のそれぞれのカテゴリーにも応募して下さい。さらに、基本暗号や補助関数に与えるパラメータの選択基準や推奨例を具体的に示して下さい。最後に、実現例を実装する場合に使用する多倍長演算ルーチンや補助プロセッサ等に関しても明示して下さい。

（２） 共通鍵暗号

共通鍵暗号については、以下の詳細分類に属する方式を公募します。

① ストリーム暗号（初期値空間：128bit 以上、状態数：128bit 以上）

② 64bit ブロック暗号（鍵長：128bit 以上）

③ 128bit ブロック暗号（鍵長：128bit 以上）

（３） ハッシュ関数

128bit 以上のハッシュ値を発生する方式を公募します。主用途は、公開鍵暗号の基本暗号と組み合わせて使用することを想定しています。

（４） 疑似乱数生成

暗号の鍵または鍵の種等を生成する疑似乱数生成アルゴリズムを公募します。

４．応募に際して必要となる事項

暗号技術の応募に際しては以下が必要となります。

４．１ 「公募対象の暗号技術」の条件

応募される暗号技術が「３．公募の対象」を満たしていることが必要です。

特に、仕様等が公開された暗号技術であることが必要であり、この判断には、以下の（条件１）及び（条件２）を基準として用います（外為法等法令・権利等の関係も含め、必要な手続は応募者側で行って下さい)。ただし、応募時点でこのような状況におかれていない場合、詳細評価開始予定の平成１２年１０月以前（平成１２年９月末まで）にこのような状況におかれることが予定されていれば応募を認めることとします（９月末の段階で仕様等の公開を情報処理振興事業協会が確認できない場合は原則として評価を中止します)。

（条件１）「４．２評価応募のために必要な情報の提出」の（２）～（４）（暗号技術概要説明書、暗号技術仕様書、自己評価書）の情報（和文、英文とも）

（以下、本公募要領において、「仕様等」とは、これらを指すこととします。）が、公知の技術その他不特定多数の方が自由に入手できる情報であり、かつ以下のいずれかであること。

①新聞、書籍、雑誌、カタログ等により、既に不特定多数の方に対して公開されている技術データ（取扱説明書、保守マニュアル等特定の物品の購入に際して添付されている情報はこれに該当しません。）

②学会誌、公開特許情報、公開シンポジウムの議事録等不特定多数の方が入手可能な技術データ

③図書館、工場の見学コース、講演会、展示会その他で不特定多数の方が閲覧又は聴講可能な技術データ

（条件２）応募者側で開設したウェブ・ページ上において、仕様等、または不特定多数の方が仕様等を自由かつ困難なく入手するための具体的方法が公開されていること。

なお、スクリーニング評価を通過した暗号技術については、ウェブ上に掲載された上記情報に情報処理振興事業協会よりリンクを設定することを予定しています。

４．２　評価応募のために必要な情報の提出

暗号技術の評価のために、応募段階（平成１２年７月１４日）に必要な提出物(1)～(9)を一覧表として示します。なお、提出いただいた情報に関しては、応募時点より、情報処理振興事業協会から第三者に開示することがあります。

項番	提出物	提出文書記述言語、媒体	応募書類等作成要領の書式
(1)	暗号技術応募書	和文 文書及び電子媒体	「暗号技術応募書」
(2)	暗号技術概要説明書	和文および英文 文書及び電子媒体	「暗号技術概要説明書」
(3)	暗号技術仕様書	和文および英文 文書及び電子媒体	定型書式なし
(4)	自己評価書	和文および英文 文書及び電子媒体	定型書式なし
(5)	テストベクタ	電子媒体のみ（テキスト形式）	定型書式なし

(6)	サンプルコード	電子媒体のみ（テキスト形式）	定型書式なし
(7)	公開の状況等に関する情報	和文 文書及び電子媒体	定型書式なし
(8)	知的所有権に関する情報	和文 文書及び電子媒体	定型書式なし
(9)	会社概要表	和文 文書及び電子媒体	「会社概要表」

（2）～（4）は、和文・英文両方の提出が必要ですが、応募段階（平成１２年７月１４日）では、和文、英文のどちらか一方のみの提出でも応募受付を行います。ただし、その場合でも、平成１２年９月末（必着）までに残る一方の提出が必要となります。

なお、本評価時に用いる正式言語は日本語とし、英語を補助的に用います。

詳細評価においては海外評価も想定していますので、提出物のうち(2)～(4)は和文と英文の両方で提出書類を作成して下さい（和文を正文とし、英文を仮訳として扱い、両者の内容に齟齬があった場合は和文を優先しますが、可能な限り同一内容として下さい。評価の実施に障害を生じる場合には評価対象外とすることもあり得ます)。

以下に、それぞれの提出物につき説明を加えます。

（１） 暗号技術応募書

「暗号技術応募書」に従い、暗号名、応募者、開発者等を記述して下さい。

① 応募日

応募書提出日を記入して下さい。

② 暗号名

暗号名を記入して下さい。

③ 分類

公開鍵暗号、共通鍵暗号、ハッシュ関数、疑似乱数生成の分類のうちから１つ選択して下さい。

④ 応募者

応募者は技術内容について十分把握している人として下さい。

氏名、企業・団体名、所属（部署名、学部名)、役職、所在地、電話番号（代表、直通を明記)、ＦＡＸ番号、Ｅ－ｍａｉｌアドレス、ウェブアドレスを記入して下さい。

⑤ 開発者

開発者と応募者が異なる場合に記入して下さい。

開発者の氏名、企業・団体名を記入して下さい。

（２）暗号技術概要説明書

「暗号技術概要説明書」に従い、以下を記述して下さい。

① 暗号名

暗号名を記入して下さい。

② 分類

公開鍵暗号、共通鍵暗号、ハッシュ関数、疑似乱数生成の分類のうちから１つ選択して下さい。

③ 詳細分類

公開鍵暗号の場合には、守秘、認証、署名、鍵共有のうちから１つ選択して下さい。

共通鍵暗号の場合には、ストリーム暗号、６４ｂｉｔブロック暗号、１２８ｂｉｔブロック暗号のうちから１つ選択して下さい。

④ 設計方針

設計の透明性、構造の簡明性・柔軟性等に関する主張を記述して下さい。

⑤ 想定するアプリケーション

想定するアプリケーションの範囲を記述して下さい。

⑥ ベースとして用いる理論・技術

ベースとして用いる理論、技術について記述して下さい。

⑦ 利用実績・参考文献等

利用実績、関連する主要な参考文献（論文名、著者名、掲載雑誌名、発表年等）を記述して下さい。

（３）暗号技術仕様書

① 設計方針、設計基準

② 暗号アルゴリズム（実装に必要な全情報）

第三者が実装・評価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、評価対象外とすることがあります。具体的には以下に従って下さい。

ａ）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（数学的な方程式、テーブル、アルゴリズム、図とパラメータ）を記述して下さい。

ｂ）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。

ｃ）公開鍵暗号については、ベースとなる群・環・体等も記述して下さ

い。

ｄ）公開鍵暗号を利用する機能を実現する上で、必要となる補助関数に関しても記述して下さい。補助関数に、新規のハッシュ関数、乱数（疑似乱数）が含まれる場合には、本公募のそれぞれのカテゴリーにも応募して下さい。

ｅ）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。

（注）一般的でない特殊な装置が必要である場合や非公開の部分がある場合は評価対象外とします。

情報が不十分であるために実装ができない場合には、原則として、評価対象外とします。

評価に必要な情報の追加提出を求めることがあります。

（４）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。

特に、①・②の項目については必ず記述して下さい。自己評価が十分でないと判断される場合には、評価対象外とすることがあります。

①　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、「５．評価基準」を参考にして下さい。

「５．評価基準」で想定したすべての攻撃法に対する評価は必要ありません。特に評価基準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、評価対象外とします。

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(ISEC・SCIS・CRYPTO・EUROCRYPT・ASISACRYPT・FSE・PKC 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。

② ソフトウェアでの実装評価

速度評価・メモリ使用量（コード量・ワークエリア）・最適化の有無・記述言語・評価プラットホーム等を記述して下さい。

（注）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。
公開鍵暗号の場合で、コプロセッサを使用して、高速化をはかる場合には、コプロセッサを制御するＲＡＭサイズやＲＯＭサイズ、および、コプロセッサを使用した場合のソフトウェア、ハードウェア全体を通しての処理速度評価も別に記述して下さい。

③ ハードウェアでの実装評価
使用したプロセス（Field Programmable Gate-Array、ゲートアレイ）・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、ゲートアレイ等の場合はゲート数）等を記述して下さい。
なお、処理速度やリソース使用量は、シミュレーション評価結果でもかまいません。
（注）公開鍵暗号の実装評価に関しては、コプロセッサを利用して高速化することが可能であれば、使用したコプロセッサの機能、ゲート規模と処理性能を記述して下さい。

④ 第三者評価実績
すでに第三者評価を受けた実績がある場合には、その評価結果を記述して下さい。報告書があれば添付して下さい。

（５）テストベクタ
実装確認のために十分な量のテストベクタを記述して下さい。十分な量のテストベクタが提出されないときには評価対象外とすることがあります。最低条件は以下の通りです。
① 公開鍵暗号
鍵対：１０対
各鍵対に対する処理例：２０例
② 共通鍵暗号
ａ)ストリーム暗号
鍵：１０
各鍵の例に対するデータサイズ
512bit×１６（各初期値を変化させること）
1,024bit×８（各初期値を変化させること）
2,048bit×４（各初期値を変化させること）
4,096bit×２（各初期値を変化させること）
8,192bit×１

ｂ)ブロック暗号

１ブロック分の処理例及びその中間処理結果データ

１０例の鍵で、各鍵毎の ECB モードでの処理例：4,096block

③ ハッシュ関数

元のデータサイズ：512bit、1,024bit、2,048bit、4,096bit、16,384bit、65,536bit

データサイズ毎の処理例：１０例

但し、繰り返し型のハッシュ関数の場合は、元のデータサイズが 512bit の場合の中間処理結果を含んだ例を１例つけること。

④ 疑似乱数生成

初期値１０個、各初期値に対して 32,768bit 毎の発生例

（６）サンプルコード

サンプルコードを ANSI-C で記述して下さい。

サンプルコードの提出がないことのみをもって評価対象外とすることはありませんが、実装チェックの手間を軽減するため可能な限り提出して下さい。

（７）公開の状況等に関する情報

本事業では、仕様等が公開されている（「４．１」参照）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を提出して下さい（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、９月末までの予定を提出し、仕様書等の公開がなされ次第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)。

また、本事業では、情報処理振興事業協会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、「４．２　評価応募のために必要な情報」の（２）～（６）の情報のそれぞれについて、輸出管理上下記の①～③のいずれの状態にあると考えられるかを明示の上、この点につき情報処理振興事業協会が確認するために必要な情報を提出して下さい。提出された情報が不十分であり、十分な評価の迅速な実施が困難であると情報処理振興事業協会が判断する場合、評価対象外とすることがあります。

① 提出情報の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のコピー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)。
② 提出情報の非居住者への提供等に際して応募時点では輸出管理上許可を要するが９月末までに許可不要の状態におかれると考える場合には、その根拠（予定の具体的内容等）につき文書で提出して下さい（許可不要の状態におかれた際には速やかにその根拠、及び確認のための文書を提出して下さい)。
③ 提出情報の非居住者への提供等に際して輸出管理上許可が必要であると考える場合には、その旨記述して下さい。

（８）知的所有権に関する情報

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所有権に関する状況を応募書類の「自社特許とその扱い」の中で説明して下さい。

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権を保有する場合、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説明して下さい。

情報処理振興事業協会が評価の実施に際して必要となる知的所有権の利用（特許法上の発明の実施、著作権法上の著作物の複製・頒布等、情報処理振興事業協会が評価を委託する第三者による利用を含む）が無償で行えることを確認できる情報を提出して下さい。知的所有権上の制限により評価の実施が妨げられる場合は、情報処理振興事業協会の判断により評価対象外とすることがあります。

通常に利用する場合の知的所有権の扱いを理由に応募された暗号技術を評価対象外とすることは原則とありませんが、電子政府における利用において甚だしい障害となることが予想される場合には評価対象外とする場合もあります。

（９）会社概要表

応募者が企業の場合は「会社概要表」も提出して下さい。

４．３　評価への対応

応募受付後、評価の過程において、情報処理振興事業協会より不明な点につき照会したり、必要な情報の追加を求めたりする可能性が考えられますので、日本語での対応が可能な方を応募者として指定ください。

評価のために必要な対応が迅速になされない場合には情報処理振興事業協会の判断で評価を中止することがあります。

５.評価基準

応募された暗号技術は、安全性と実装性の両面から評価します。

５．１ 公開鍵暗号

（１）安全性評価基準

応募された守秘、認証、署名、鍵共有いずれかの機能を実現する暗号方式（暗号スキーム）に関して、その暗号方式（暗号スキーム）で要求された要件を満たす基本暗号、補助関数を仮定して、暗号方式（暗号スキーム）としての安全性を評価します。また、応募された実現例で使用した基本暗号（暗号プリミティブ）や補助関数を、提案された暗号方式における基本暗号（暗号プリミティブ）や補助関数の満たすべき要件との適合性、妥当性の観点からを評価します。

また、提案されたパラメータとプリミティブは、最も影響があると思われる攻撃法によって、評価します。

(a)暗号方式（暗号スキーム）に関する安全性評価項目

攻撃の方法と目標に応じた暗号方式の振舞いを評価します。攻撃方法と攻撃の目標の組み合わせ毎に、応募方式が、安全性の証明を有するか、あるいは、ヒューリスティックな根拠を有するか等の観点で評価します。

攻撃の方法：受動的攻撃、能動的攻撃、その他の攻撃

攻撃の目標：実現すべき機能（守秘、認証、署名、鍵共有）の欠損状況

(b)基本暗号（暗号プリミティブ）に関する安全性評価項目

ｉ）整数の素因数分解問題に基づく基本暗号

既知の攻撃法に対する計算量的耐性（例えば、rho 法、ｐ－１法、ｐ＋１法、Fermat 法、２次ふるい法、楕円曲線法、数体ふるい法等)、および、基本暗号に固有なその他の方法について評価します。

ii）有限体上の離散対数問題に基づく基本暗号

既知の攻撃法に対する計算量的耐性（例えば、Pohlig-Hellman のアルゴリズム、平方剰余法、指数計算法、数体ふるい法等)、および、基本暗号に固有なその他の方法について評価します。

iii)楕円曲線上の離散対数問題に基づく基本暗号

既知の攻撃法に対する計算量的耐性（例えば、Pohlig-Hellman のアルゴリズム、平方剰余法、Frey-Rück 帰着、Semaev-Smart-Satoh-Araki アルゴリズム、Weil Descent を用いたアルゴリズム等)、および、基本暗号に固有なその他の方法について評価します。

iv）その他の安全性根拠に基づく基本暗号

既知の攻撃法、基本暗号に固有の攻撃法等に対して評価します。

（２）暗号方式の実現例に関する実装性評価

実装の見地からの評価は次の項目に基づいて行います。

i) 提出された暗号技術仕様書には、実装に十分な情報が記載されているかを評価します。

ii) 応募された暗号方式が、標準的なプラットホームで実行可能か、また、 実装する際に、非常に特殊なハードウェアや巨大な量の記憶装置が仮定されていないことも評価します。

iii) 応募された暗号方式（暗号スキーム）を標準的なプラットホーム上で、ソフトウェアで実現した場合の処理速度、メモリ等のリソース使用量を評価します。

iv) 応募された暗号方式（暗号スキーム）を、実システムあるいはアプリケーションに適用する場合の特別な留意事項、例えば、特権を与えられた認証機関などを必要とする等の留意事項が存在する場合には、この留意事項も評価します。

v) 応募された暗号方式（暗号スキーム）あるいは基本関数（暗号プリミティブ）が処理するデータブロックの大きさを評価します。 また、もし応募された暗号方式（暗号スキーム）が２以上のエンティティの間で、インタラクション（データ交換）を必要とする場合、その際のインタラクション数も評価します。

vi) もし応募された暗号方式（暗号スキーム）の使用実績がある場合には、その実績も考慮します。

５．２ 共通鍵暗号

(1)安全性評価基準

(a)ストリーム暗号に関する評価項目

応募されたストリーム暗号は、線形複雑度、線形解読法、divide-and-conquer 攻撃等（文献[S1]等を参照してください）等のよく知られている攻撃に対する耐性を評価します。また、その他の攻撃に対する耐性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。その他のストリーム暗号に対する攻撃に関しては、文献[S1]-[S18]を参照して下さい。

(b)ブロック暗号に関する評価項目

線形攻撃法、差分攻撃法など汎用的な攻撃法（文献[B3],[B7]を参照して下さい）に関する耐性を評価します。

その他の攻撃法（例えば、高階差分、補間、Impossible Differential、Truncated Differential、Boomerang、Non-surjective、Mod n、χ^2、Related Key、Slide 攻撃等）に対する耐性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。その他のブロック暗号への攻撃に関しては、文献[B1]-[B18]を参照して下さい。

さらに、統計量情報による評価（例えば、無相関性、アバランシェ性等）や実装に関係した攻撃（例えば、Timing、Power Analysis、Differential Power Analysis 等）等のサイドチャネル攻撃に対して耐性を評価します。

（サイドチャネル攻撃に関しては、文献[B18],[B19]を参照して下さい。）

（２）実装性評価基準

(a)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、メモリ等の使用状況（コード量、作業領域など）などを評価します。

ii）鍵スケジューラ個別の処理速度も評価します。

(b)ハードウェア実装による評価項目

使用するプロセス（フィールドプログラマブルゲートアレイ、ゲートアレイ）別に、処理速度評価、リソース使用数量（フィールドプログラマブルゲートアレイの場合には、使用セル数、ゲートアレイ等の場合に、使用ゲート数等）を評価します。

注意：シミュレーション評価結果をもって、処理速度、リソース消費量の評価とすることがあります。

５．３ ハッシュ関数

（１）安全性評価基準

安全性の評価は次の項目に基づいて行います。

i）衝突一致困難性に関する項目。

ii）統計量情報（例えば、無相関性、アバランシェ性、一様性等）による項目。

さらに、また、ヒューリスティックな安全性の根拠や文献[H1]-[H8]に示すような攻撃に対しての安全性も評価することがあります。

（２）実装性評価基準

(a)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。

標準的なプラットホーム上での処理速度、メモリ等の使用状況（コード量、作業領域など）などを評価します。

(b)ハードウェア実装による評価項目

使用するプロセス（フィールドプログラマブルゲートアレイ、ゲートアレイ）別に、処理速度評価、リソース使用数量（フィールドプログラマブルゲートアレイの場合には、使用セル数、ゲートアレイ等の場合に、使用ゲート数等）を評価します。

注意：シミュレーション評価結果をもって、処理速度、リソース消費量の評価とすることがあります。

５．４ 疑似乱数生成

（１）安全性評価基準

評価の観点は、統計量的な性質の評価と乱数性（例えば、FIPS140-1 に示される、 Monobit テスト、ポーカーテスト、ランテスト（０-１の balancedness 、頻度テスト）と Long Run Test のような）のテストで示される統計上の性質です。また、文献[R1]-[R24]に示すような他の攻撃への耐性やヒューリスティックな安全性の根拠についても評価することがあります。

（２）ソフトウェアでの実装評価基準

ソフトウェア実装に関しては、標準的なプラットホーム上での処理速度、メモリ等の使用状況（コード量、作業領域など）などを評価します。

「５.評価基準」における実装性評価の目的は、処理性能や、リソースの使用状況に関する評価です。具体的には、処理速度や使用するリソースの量を相対的に比較します。安全性が高くても超大型の計算機でしか実現できない方式や高価な専用環境を必要とする方式は相対的に不利となります。

６．応募に際しての留意事項

（１）本事業の実施に際し、情報処理振興事業協会から応募者へ、あるいは応募者から情報処理振興事業協会への費用等の支払いは、いずれも行いません。

（２）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、及び評価期間中の対応に係る費用は応募者側で負担して下さい。外部委託評価その他の情報処理振興事業協会側で発生する費用は協会が負担します。

（３）評価の実施が困難であると情報処理振興事業協会が判断した場合には、評価対象外とする場合がありますので、応募に際しては「４．応募に際して必要となる事項」を参照の上漏れの無いようご注意願います。

７．応募方法

（１）提出期限

平成１２年７月１４日（必着）までに情報処理振興事業協会セキュリティセンター暗号技術調査室宛てに郵送にて提出して下さい。

（２） 提出物

４．２の「評価応募のために必要な情報」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。電子媒体については、全ての電子データを CD-R、CD-RW、光磁気ディスクのいずれかにまとめて入れ、暗号名と応募社名を記入したラベルを添付して下さい。

(3) 応募に関する問い合わせ及び提出先

情報処理振興事業協会　セキュリティセンター　暗号技術調査

〒113-6591　東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス 16 階

FAX　　03-5978-7518

E-mail　crypto-kobo@ipa.go.jp

問い合わせの受付は E-mail あるいは FAX のみとします（電話での問い合わせは、ご遠慮下さい）。

以上