別紙２

「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（案）に対する意見並びにこれに対する総務省及び経済産業省の考え方

平成２５年３月１日

「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（案）に対する意見の募集で寄せられたご意見について

○ 意見募集期間：平成24年12月12日～平成25年1月10日

○ 提出意見総数： 6件

（１） 個人 ４件
（２） 法人・団体 ２件

項目	頂いたご意見	ご意見に対する考え方
【意見1】AES の解釈について		
電子政府推奨暗号リスト	選定内容については専門家の判断に従います。運用面のコメントです。情報セキュリティにおいて、電子政府推奨暗号の利用が義務付けられる場合があります（省庁関係との契約など）。ところが、「AES-256 は推奨暗号ではない」と言われました（推奨は AES-128）。異なるビット長が利用できる暗号方式においては、利用して良いビット長の全てをリストアップしていただきたいです。 【個人1－1】	電子政府推奨暗号の仕様書は、CRYPTREC ウェブサイト（http://www.cryptrec.go.jp/method.html）に掲載されているとおりであり、特に CRYPTREC 暗号リストにおいて利用上の注釈が明記されていない限り、仕様書に記載された鍵長は全て利用できます。例えば、ご意見にありました AES は鍵長 128 ビット、192 ビット、256 ビットが利用できることが記載されています。なお、AES の技術分類である「共通鍵暗号・128ビットブロック暗号」は、ブロック長が 128 ビットであることを意味しております。
【意見2】電子政府推奨暗号リスト、推奨候補暗号リスト及び運用監視暗号リストの位置付け		
全体	提案の「電子政府参照暗号」は「電子政府推奨暗号」を改定した物ですが、言葉の意味は「推奨」の方が強く、優先して選択すべきは「推奨暗号」と捉えられます。ここで、KCipher-2 を選定した場合「電子政府推奨暗号を利用する」という要件を満たすのか否か。使用するのは「推奨暗号」でも「参照暗号」でも良いのか。「推奨暗号」は最新の解析に耐えないものもあるので「参照暗号」から選定すべきなのか。「参照暗号」は推奨候補であるため「推奨暗号」から選定すべきなのか。「推奨暗号」と「参照暗号」の位置付けを明確に打ち出していただきたいです。 【個人1－2】	CRYPTREC としては「CRYPTREC 暗号リスト」中の電子政府推奨暗号リストに掲載する暗号技術の利用を推奨いたします。したがって、KCipher-2 は推奨する暗号技術となります。なお、電子政府推奨暗号リストと推奨候補暗号リストの位置づけの違いを明確にするため、両リストの説明文を修正しました。同様に、CRYPTREC 暗号リスト全体の位置づけを明確にするため、注釈についても併せて見直しました。 また、電子政府推奨暗号リストに記載された暗号技術の運用に関しては政府機関の情報セキュリティ対策のための統一基準群（平成 24 年度版）において定められており、各リストに掲載された暗号技術の政府調達での利用について、適切に定められるよう関係省庁と調整してまいります。

【意見3】ストリーム暗号を電子政府推奨暗号リストに掲載してほしい。		
電子政府推奨暗号リスト	スマートフォンやタブレットを端末としたモバイルシステム開発をする企業としてコメントさせて頂きます。アプリ／システム開発をする際のセキュリティ強化への要求は、モバイル環境の場合特に強く、スマートフォンにおいては社会的な要求にまで発展している状況だと感じています。さて、私どもはモバイルのセキュリティをテーマとする事が多いのですが、解決策として「暗号化」を中心に検討をしています。その際にケアすべきが、1．大容量化への対応、2．伝送路の秘匿性確保、となる事が多く、大容量データの暗号化やその伝送路の秘匿性確保において、従来よりも高速に暗号処理されないと、利用に堪えない程のストレスを生み出す事を体感しております。（スマホで動画ファイルを復号化、など。）そのような観点から、「高速」に暗号化できるストリーム暗号を利用できるように、電子政府推奨暗号リストに掲載して頂きたいと願っています。どうぞ宜しくお願い致します。 【法人・団体1】	電子政府推奨暗号リストには、ご指摘のストリーム暗号も選定されておりますので、本案に賛成のご意見として承ります。
【意見4】電子政府推奨暗号リストの共通鍵暗号方式にブロック暗号とストリーム暗号の両方を選定すべき。		
電子政府推奨暗号リスト	（ICT関連企業の広告・宣伝に関してコンサルティングしている企業の立場から） ・ISO などの国際標準と同様に、共通鍵暗号方式は、ブロック暗号、ストリーム暗号の両方を選定すべきであり、電子政府推奨暗号リストに両カテゴリがリストに掲載されているのは望ましい状況である。 【法人・団体2】	本案に賛成のご意見として承ります。

【意見5】電子政府推奨暗号リストの選定基準決定の経緯を明らかにすべき。		
全体	公募要項において、推奨リストは「利用実績が十分なもの」とされておりましたが、本案では「利用実績が十分か今後の普及が見込まれる」と変更されております。公募要項からの変更ですので、本来は再びパブリックコメントを募集すべき大きな方針転換であるように思います。また、何を根拠に今後の普及が見込まれると判断されたのでしょうか？その判断基準や使用したデータを教えてください。私見ではSSL や携帯電話などで普及が進むと判断したのでは？と思いますが、そうであればリスト名に冠する「電子政府」用途の意味が分かりません。 【個人2－1】	電子政府推奨暗号リストの説明文は、その選定基準を反映した結果表現が変わっておりますが、リスト改定にかかる方針は、暗号技術公募要項5.1 節の背景に記載がありますように、「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、・・・（中略）・・・現リストの改訂を行います」に沿ったものであり、当初より変更されておりません。また、普及が見込まれる根拠に関しては民間での利用が進むことにより、政府における調達容易性が上昇することを考慮しております。 今回のリスト改定においては、安全性の評価に加え、現状の調達容易性や将来的な調達容易性などの観点も考慮し、CRYPTREC Report2011 及びCRYPTRECシンポジウム2012で発表したとおり、「電子政府推奨暗号リストの掲載個数を限定したうえで、国産暗号の普及展開をどのようにすすめるべきか等を最大限加味」するという方針に基づいて選定基準を定めました。 なお、本選定基準決定の詳しい経緯につきましては、CRYPTREC ウェブサイトのトピックスに掲載している『「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（案）に係る意見募集について』、CRYPTREC Report、暗号技術検討会報告書等をご参照ください。

【意見6】推奨候補暗号リストの意義について。		
推奨候補暗号リスト	候補リストは、既に電子政府で利用中であるが他の電子政府システムで利用される見込みがないということでしょうか？システム更改においては、委員会は当然ながら推奨暗号を使用せよ、ということになると思います。すると、候補暗号が採用さることは委員会の方針ではあり得ないように思えます。このリストは廃止し監視リストと合わせるか、互換性維持リストなど名称を変更した方が適切に思えます。 候補リストも利用実績があれば推奨リストに登録されると公募要項のリスト改定概念図にありますが、この条件や判断基準は何でしょうか？また、推奨暗号を使用せよ、と指示しておきながら候補暗号の利用が電子政府内で進むという状況が想像できません。どのような状況を想定されているのか、ご教示ください。 【個人２－２】	推奨候補暗号リストは、あくまで「CRYPTREC により安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト」であって、政府機関の情報システムにおいて使用すべきでないと判断したものではありません。 今回の改定では、民間等での利用が進むことにより、政府における調達容易性が上昇することを考慮して、民間での利用実績等を調査しており、今後、民間での利用が高まる等によって、推奨候補暗号リストに掲載されている暗号技術が電子政府推奨暗号リストに掲載される可能性があります。
【意見7】耐量子計算機暗号の公募について。		
全体	公開鍵暗号、特に耐量子計算機暗号が盛んに議論されていますが、公募の予定はないのでしょうか？ 【個人２－３】	現時点では公募の予定はありませんが、今後検討させていただく予定です。
【意見8】脳通信に関するセキュリティについて。		
全体	脳通信に関する、セキュリティについて意見を述べさせていただきます。 今後機械から人、人から人、人から機械での通信において、その通信にセキュリティをかけることによって、外部からのアクセスを遮断させる技術開発や、ブレインネットの規制など倫理的に許されない問題を判断する機関、そのための立法を早急に作成するべき時期に来ていると考えます。 そのための予算が拡充されますように願っています。 これからも日本や世界のために頑張ってください。今年一年皆さまが良い年になりますように。 【個人3】	ご意見については今後の参考とさせていただきます。

【意見９】メッセージ認証コード及びハッシュ関数の利用方法について。		
電子政府推奨暗号リスト及び運用監視暗号リスト	メッセージ認証コードにHMACが記載されているがHMAC利用時には特定のハッシュ関数の利用を必須としている．既に危殆化されたと認識されているMD5との併用，つまりHMAC-MD5はどのように扱うべきなのか，また運用監視暗号リストに掲載され「推奨すべき状態ではなくなった」SHA1との併用，つまりHMAC-SHA1はどのように扱うべきなのか不明瞭である． HMACとして利用する場合のハッシュ関数は電子政府推奨暗号リストに掲載しているアルゴリズムであれば利用を推奨され，運用監視暗号リストに掲載しているアルゴリズムであれば互換性維持のために継続利用を容認するものであると，考えればよいのか？また，CMACについても選択するブロック暗号の種類に応じてどのように考えればよいか不明瞭である． ハッシュ関数 RIPEMD-160, SHA-1において，現リストの以下の注釈に呼応する説明を入れるべきではないか？ 「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利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。」 上記注釈の「この限りではない」という制限を全面的に排除するのであれば，「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当該公開鍵暗号アルゴリズムは利用しない。」などと記載すべきではないか？ 【個人４－１】	メッセージ認証コードのHMAC及びCMACに関しては、併用するハッシュ関数やブロック暗号が電子政府推奨暗号、推奨候補暗号および運用監視暗号のいずれであっても安全性上の問題は見つかっておらず、HMAC-SHA1を含めて電子政府推奨暗号リストに含まれます。ただし、リストに掲載されていないMD5等の暗号技術の安全性はCRYPTRECにおいて確認されておらず、例えばHMAC-MD5は電子政府推奨暗号リストに含まれません。 また、同様にメッセージ認証コードの他、暗号利用モード及びエンティティ認証でも他の技術分類の暗号技術と組み合わせて利用することとされていますが、その場合CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせることで安全性が確保されるため、リスト説明への注釈を追加いたします。これに合わせて、（注2）及び（注6）の注釈は暗号技術欄から技術分類欄に移動します。 なお、現リストのハッシュ関数 RIPEMD-160, SHA-1に付与されている注釈については、これらのハッシュ関数が、「互換性維持のために継続利用を容認する」と明記している運用監視暗号リストに移り、この説明と注釈が重複することから削除しております。

【意見10】「当面の利用」の記述について。		
電子政府推奨暗号リスト及び運用監視暗号リスト	注釈（注3）（注9）における「当面の利用」を明確にすべきである. SHA-1 および RSA-1024 についてのみ（注1）（注8）に記載されているように外部文書にて「移行指針」で定められている不均衡を無くし, 3-key Triple DES および RSAES-PKCS1-v1_5 についても移行指針を定めるべきである. 特に後者の RSAES-PKCS1-v1_5 においては運用監視暗号リストに掲載されていることからも速やかに新しい方式への移行が行われるべきであるのみ関わらず「当面の利用」を許可するという“逃げの姿勢”のようにも見受けられる. 【個人4－2】	注3(Triple DES)で「当面の利用」を許可している理由といたしまして、注2に記載のようにそもそも 128 ビットブロック暗号を推奨しているということと、高い利用実績があることがあげられます。また、調査の結果から 64 ビットブロック暗号が満たすべき安全性を十分に達成していると判断致しました。 注9(RSAES-PKCS1-v1_5)で「当面の利用」を許可している理由といたしまして、調査の結果、高い利用実績があり、互換性維持のため利用が必要になることがあげられます。 なお、運用監視暗号リストに掲載された暗号技術の移行指針については、今後関係省庁と調整させていただきます。
【意見11】CBC-MAC の取扱いについて。		
運用監視暗号リスト	注釈（注11）の表現を改めるべきである. 現案では「メッセージ長を固定して利用」すれば OK という意味ではなくメッセージ長を固定していない場合には利用してはいけない, という意味合いにすべきである. 【個人4－3】	メッセージ認証コードのビット長の切り詰めを適切に行うことにより、メッセージ長を固定しないでも安全に使える場合があります。今回の注釈では、このような利用方法の可能性も考慮に入れているため、現在の注釈のままとさせて頂きます。

【意見12】セキュリティパラメータの記述について。		
運用監視暗号リスト	（関連資料）安全性評価結果 page.10 判定理由および次期リストにおける注釈： ハッシュ関数・MAC によると， ハッシュ関数 RIPEMD-160, SHA-1 が「推奨すべき状態ではなくなった」と判断された基準は「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」という注釈に依るものであり 80 ビット安全性では不十分で 128 ビット安全性が必要であるという主張をしているものと考えられる. 一方で公開鍵暗号については，このような考え方はなく，具体的には鍵長に関する制限が本リストには設けられていないことに違和感がある．それぞれのアルゴリズムに対して推奨される鍵長やセキュリティパラメータについても併記すべきではないか？ もしこれらに関して他のドキュメント（利用ガイドラインなど）で補足されている場合には「電子政府における調達のために参照すべき暗号のリスト」における（注1）（注8）などのように当該ドキュメントを注釈に含めるべきである. 【個人４－４】	改定前の電子政府推奨暗号に記載された暗号の運用に関してはこれまで CRYPTREC リストガイドにおいて指針を示しております。今回のリスト改定を踏まえ、対応する文書の整備が行われる予定です。ご指摘の注釈における表現に関しては、これらの文書の改定をどのように適時反映させるかを含め、今後の検討課題とさせて頂きます。

【意見13】擬似乱数生成系のアルゴリズムについて。		
全体	前回のリストに掲載されていた擬似乱数生成系のアルゴリズムは「例示」という注釈付きであったものも必要であったと認識している. 昨年公開された下記の論文では, RSA 公開鍵生成時や DSA 署名において用いられる一時鍵の生成時に十分なエントロピーを保持しない乱数生成モジュールを用いたことにより秘密鍵が意図せず漏えいする問題を示しており, 電子調達される製品群においても「暗号学的に安全な」モジュールを用いられるべきであるという立場に立つと, 今回のリストで擬似乱数生成系のアルゴリズムが除外されたことに疑問を覚える. [1] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter, ″Ron was wrong, Whit is right″ http://eprint.iacr.org/2012/064 [2] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter ″Public Keys″ http://www.iacr.org/conferences/crypto2012/abstracts/session11-2.html [3] Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman, ″Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices″ https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices 【個人4－5】	擬似乱数生成系は相互運用性が不要であることや、アルゴリズム自体よりも実装面やシード値の与え方など運用面が重要であることから、今回の CRYPTREC 暗号リストでは対象技術から除外いたしました。なお、擬似乱数生成系については 2009 年版リストガイドにおいて評価しております。実装についても、暗号モジュール試験及び認証制度（JCMVP）において認証された擬似乱数生成系モジュールが複数あるなど、調達における判断が可能な環境にあります。

【意見14】アルゴリズムのみでの利用可否の判定について。		
全体	アルゴリズムのみの利用可否判定は既に破たんしている．Proprietary なシステムではなく標準プロトコルを利用したシステムにおいては，それぞれのプロトコルに応じた利用推奨方式を定めるべきである． 例えば SSL/TLS においては設定が推奨される CipherSuites のリストが選定されている方が，発注者・受注者ともに発注・受注内容および指示が明確となり，お互いがハッピーな状況になると思われる．現在のリストだと RC4 を利用した CipherSuites は（互換性確保のため）設定してよいのか，（危険なため）設定していけないのかよく分からないという状況になっている． 暗号アルゴリズム単体の安全性で評価を閉じるのではなく，それを利用することを想定したトータルな視点での安全性評価を次回以降の評価方法・結果開示方法に取り入れて頂きたい． 【個人４－６】	暗号アルゴリズムの安全性等を確認し、政府調達において利用を推奨する暗号アルゴリズムを選定しリスト化することは、安全な政府の情報システムを構築するために必要な活動です。 また、各暗号技術の推奨設定については、SSL/TLS における暗号スイートに関しては 2011 年度版リストガイド(SSL/TLS)においてすでに推奨される設定を示しておりますが、今後もこのようなガイドライン等を通じて CRYPTREC 暗号に記載された暗号技術の利用方法の推奨について示してまいります。

【意見15】選定基準の根拠を明確にしてほしい（1）。		
全体	（関連資料）評価 A 判定結果 Page3. 評価 A の各評価項目における選定基準および（関連資料）評価 B 判定結果 Page3. 評価 B の各評価項目における選定基準（1） ----- 「3項目以上」や「2件以上」，「50%以上」「10%以上」という数値の根拠が明瞭ではない. 【個人4－7】	今回のリスト改定は、安全性の評価に加え、現状の調達容易性や将来的な調達容易性などの観点も考慮し、2011 年度暗号技術検討会で決定された「国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用する」ことを目的として、「電子政府推奨暗号リストの掲載個数を限定したうえで、国産暗号の普及展開をどのようにすすめるべきか等を最大限加味」するという方針に基づいて選定を実施したものです。同方針を具体化する基準として、2 つの観点（「すでに十分な利用実績がある」と「国際標準化・製品化促進の進展が期待できる根拠がある」）から、利用実績が十分であるかを判断する評価 A では市販製品の採用実績など 4 項目、今後の普及が見込まれるかを判断する評価 B では今後の進展が期待できる根拠としてのアピールポイントなど 8 項目で評価する選定基準を決定しました。 各選定基準の閾値については、過去の利用実績調査結果や国際的に広く利用されている代表的な暗号アルゴリズムの普及状況等を参考にして、「50%」は過半数の製品での採用実績があり広く普及しているといえる基準として、「10%」は暗号の提案会社・グループ会社等以外の他社製品においても一定程度の採用実績が見込める基準として取り入れました。 また、「3 項目以上」の閾値は、①できるだけ多くの評価項目を満たすほうが望ましいが、暗号の提案会社の経営戦略の自由度を著しく損なう必須的条件として課すのは適当ではない、②評価 A と評価 B が実質的に同じ選定基準となることは避けるべき、との観点を考慮して決定しました。なお、「2 件以上」との条件を付加したのは、実際には利用実績が少ないにもかかわらず、たまたま一つの調査対象に含まれただけで利用実績ありと判断される偶然性を極力排除すべきとの考えからです。

【意見16】選定基準の根拠を明確にしてほしい（2）。		
全体	（関連資料）評価 A 判定結果 ----- 「採用実績」と“利用実績”は異なると考える．搭載されているか，ではなく実際に利用されているかどうかで「実績」を測るべきではなかったか？ また，システム，製品，オープンソースにおいてその採用実績のパーセンテージが製品種類数によって算出されている点もおかしい． あまり利用されていない製品でも，とても利用されている製品でも，同じ傾斜であるのは普及率として測る場合に妥当であるとはいえない． 【個人4－8】	評価における客観性を確保する観点から、現状で入手可能な利用実績データのうち、公平かつ検証可能なデータのみを用いて評価しております。 製品の利用度（シェア、販売数など）等についての検証可能なデータの入手方法やそれらのデータが入手できた際の評価方法の見直しについては、今後の検討課題とさせていただきます。