「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）に対する意見募集に寄せられたご意見並びにそれらに対するデジタル庁、総務省及び経済産業省の考え方

令和５年３月３０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：令和5年3月9日～令和5年3月23日

○ 提出意見総数： 4件

（1） 個人 4件

（2） 法人・団体 0件

項目	頂いたご意見	ご意見に対する考え方
【意見1】入力データについて		
全般	（意見）アルファベットの大文字と小文字を区別して認識するタイプの暗号を導入するのは、どうでしょうか。 （理由）より、セキュリティレベルが上ると思うから、です。 【個人1－1】	CRYPTREC 暗号リストに掲載している暗号技術では、入力データや鍵等はビット列として取り扱います。
【意見2】表の体裁について		
電子政府推奨暗号リスト	（意見）表の左上の枠を加えるのは、どうでしょうか。 （理由）枠が抜けているため、です。 【個人1－2】	ご指摘を踏まえ、表の改ページ箇所を修正いたしました。

項目	頂いたご意見	ご意見に対する考え方
【意見3】DSA について		
電子政府推奨暗号リスト	（意見）DSA に関しては「電子政府推奨暗号リスト」ではなく「運用監視暗号リスト」にリストするべきではないか？ （理由）NIST FIPS186-5（ドラフト）では以下の扱いとなっているため。 デジタル署名アルゴリズム (DSA) この標準の以前のバージョンでは、DSA が指定されていました。この規格は、DSA を承認しなくなりました。 デジタル署名の生成。 DSA は、事前に生成された署名を検証するために使用できます。 この規格の実装日。 DSA の仕様については、FIPS 186-4 [20] を参照してください。 ―― 4 The Digital Signature Algorithm (DSA) Prior versions of this standard specified the DSA. This standard no longer approves DSA for digital signature generation. DSA may be used to verify signatures generated prior to the implementation date of this standard. See FIPS 186-4 [20] for the specifications for DSA. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5-draft.pdf 【個人2】	頂きました御意見は、今後の検討課題とさせて頂きます。

項目	頂いたご意見	ご意見に対する考え方
【意見４】SHA-1 について		
運用監視暗号リスト	SHA-2 への移行が十分進んだことを考慮し、SHA-1 は廃止してよいと思う。 【個人３－１】	頂きました御意見は、今後の検討課題とさせて頂きます。
【意見５】3-key Triple DES について		
運用監視暗号リスト	AES への移行が十分に進んだ点や、現在脆弱性が指摘されている点も加味すると、3DES は廃止するべきだと思う。 【個人３－２】	頂きました御意見は、今後の検討課題とさせて頂きます。
【意見６】CBC について		
電子政府推奨暗号リスト	以下、「「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）」の改定案」に意見を行う。 ＞1 頁 ＞電子政府推奨暗号リスト 「暗号利用モード」の「秘匿モード」に「CBC」が含まれているが、CBC は、かなりの数、かなり多くの場合（TLS1.2 を含んでいる場合も多い）で危険という報告が行われているので、電子政府推奨暗号リストへの掲載は停止すべきと考える。 （条件によっては脆弱性が発揮されない場合もあると思われるが、そもそも CBC を利用しない方が安全と思われる。TLS などにおいては（TLS1.2 以降において）基本として全く CBC を利用しない方が望ましいと思われる。CBC の掲載は問題あるものと思われる。） 意見は以上である。 【個人４】	暗号利用モード（秘匿モード）CBC の暗号技術自体の安全性は CRYPTREC により確認されており、電子政府推奨暗号リストへの掲載を維持することが適当と考えます。 なお、暗号技術の利用時に安全性を確保する方法については、CRYPTREC で作成している「TLS 暗号設定ガイドライン」等において示しています。