

各府省の情報システム調達における暗号の利用方針

平成15年2月28日
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、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（「電子政府推奨暗号リスト」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

電子政府推奨暗号リスト

平成15年2月20日

総務省
経済産業省

| 技術分類 | | 名称 |
|-------|------------------------------|--|
| 公開鍵暗号 | 署名 | DSA |
| | | ECDSA |
| | | RSASSA-PKCS1-v1_5 |
| | | RSA-PSS |
| | 守秘 | RSA-OAEP |
| | | RSAES-PKCS1-v1_5 ^(注1) |
| | 鍵共有 | DH |
| | | ECDH |
| | | PSEC-KEM ^(注2) |
| 共通鍵暗号 | 64 ビットブロック暗号 ^(注3) | CIPHERUNICORN-E |
| | | Hierocrypt-L1 |
| | | MISTY1 |
| | | 3-key Triple DES ^(注4) |
| | 128 ビットブロック暗号 | AES |
| | | Camellia |
| | | CIPHERUNICORN-A |
| | | Hierocrypt-3 |
| | | SC2000 |
| | ストリーム暗号 | MUGI |
| | | MULTI-S01 |
| | | 128-bit RC4 ^(注5) |
| | | |
| その他 | ハッシュ関数 | RIPEMD-160 ^(注6) |
| | | SHA-1 ^(注6) |
| | | SHA-256 |
| | | SHA-384 |
| | | SHA-512 |
| | 擬似乱数生成系 ^(注7) | PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1 |
| | | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1 |
| | | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 |
| | | |
| | | |

注釈:

(注1) SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注2) KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

- (注3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128ビットブロック暗号を選択することが望ましい。
- (注4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
- 1) FIPS46-3として規定されていること
 - 2) デファクトスタンダードとしての位置を保っていること
- (注5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
- (注6) 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使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。
- (注7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。