

| 大分類                      | 暗号アルゴリズム                         | 機能又はモード                              | アルゴリズム仕様書<br>「, 」の後は章・節番号                              | 下位アルゴリズム   | 試験仕様書            |
|--------------------------|----------------------------------|--------------------------------------|--|------------|------------------|
| 公開鍵<br>(FIPS<br>186-4 系) | DSA2                             | ドメインパラメータ生成                          | FIPS 186-4, 4.3.1                                      | SHA        | DSA2VS           |
|                          |                                  | ドメインパラメータ検証                          | FIPS 186-4   |            |                  |
|                          |                                  | 鍵ペア生成                                | FIPS 186-4, 4.4.1                                      | DRBG       |                  |
|                          |                                  | 署名生成                                 | FIPS 186-4, 4.6  | SHA / DRBG |                  |
|                          |                                  | 署名検証                                 | FIPS 186-4, 4.7  | SHA        |                  |
|                          | RSA2                             | ANS 9.31 鍵生成                         | ANSI X9.31, 4.1  | SHA / DRBG | RSA2VS           |
|                          |                                  | ANS 9.31 署名生成                        | ANSI X9.31, 4.2  | SHA        |                  |
|                          |                                  | ANS 9.31 署名検証                        | ANSI X9.31, 4.3  |            |                  |
|                          |                                  | RSASSA-PKCS1-v1_5 署名生成               | PKCS#1 v2.1, 8.2.1                                     |            |                  |
|                          |                                  | RSASSA-PKCS1-v1_5 署名検証               | PKCS#1 v2.1, 8.2.2                                     |            |                  |
|                          |                                  | RSASSA-PSS 署名生成                      | PKCS#1 v2.1, 8.2                                       |            |                  |
|                          |                                  | RSASSA-PSS 署名検証                      | PKCS#1 v2.1, 8.2                                       |            |                  |
|                          |                                  | 署名生成 Primitive RSASP1 for Mod2048    | PKCS#1 v2.1, 5.2                                       |            |                  |
|                          |                                  | 186-2 旧試験, ANS 9.31 署名検証             | ANSI X9.31, 4.3  |            |                  |
|                          |                                  | 186-2 旧試験,<br>RSASSA-PKCS1-v1_5 署名検証 | PKCS#1 v2.1, 8.2.2                                     |            |                  |
|                          |                                  | 186-2 旧試験,<br>RSASSA-PSS 署名検証        | PKCS#1 v2.1, 8.2                                       |            |                  |
|                          | ECDSA2                           | 鍵ペア生成                                | ANSI X9.62, 5.2.1                                      | DRBG       | ECDSA2VS         |
|                          |                                  | 公開鍵検証                                | ANSI X9.62, 5.2.2                                      | none       |                  |
|                          |                                  | 署名生成                                 | ANSI X9.62, 5.3  | SHA / DRBG |                  |
| 署名検証                     |                                  | ANSI X9.62, 5.4                      | SHA  |            |                  |
| 共通鍵                      | AES                              | ECB モード                              | ● FIPS 197<br>● SP 800-38A, 6.1                        |            | AESVS            |
|                          |                                  | CBC モード                              | ● FIPS 197<br>● SP 800-38A, 6.2                        |            |                  |
|                          |                                  | OFB モード                              | ● FIPS 197<br>● SP 800-38A, 6.4                        |            |                  |
|                          |                                  | CFB 1 モード                            | ● FIPS 197<br>● SP 800-38A, 6.3                        |            |                  |
|                          |                                  | AES, CFB 8 モード                       | ● FIPS 197<br>● SP 800-38A, 6.3                        |            |                  |
|                          |                                  | AES, CFB 128 モード                     | ● FIPS 197<br>● SP 800-38A, 6.3                        |            |                  |
|                          |                                  | AES, CTR モード                         | ● FIPS 197<br>● SP 800-38A, 6.5                        |            |                  |
|                          | XTS-AES                          | -                                    | SP 800-38E   | AES        | XTSVS            |
|                          | Triple-DES                       | ECB モード                              | ● SP 800-67<br>● ANSI X9.52, 7.1 or<br>SP 800-38A, 6.1 | none       | SP 800-20<br>MMT |
|                          |                                  | CBC モード                              | ● SP 800-67<br>● ANSI X9.52, 7.2 or<br>SP 800-38A, 6.2 |            |                  |
|                          |                                  | CBC-Interleaved モード                  | ● SP 800-67<br>● ANSI X9.52, 7.3                       |            |                  |
|                          |                                  | CFB モード                              | ● SP 800-67<br>● ANSI X9.52, 7.4 or<br>SP 800-38A, 6.3 |            |                  |
|                          |                                  | CFB-Pipelined モード                    | ● SP 800-67<br>● ANSI X9.52, 7.5                       |            |                  |
|                          |                                  | OFB モード                              | ● SP 800-67<br>● ANSI X9.52, 7.6 or<br>SP 800-38A, 6.4 |            |                  |
|                          |                                  | OFB-Interleaved モード                  | ● SP 800-67<br>● ANSI X9.52, 7.7                       |            |                  |
| CTR モード                  | ● SP 800-67<br>● SP 800-38A, 6.5 |                                      |  |            |                  |
| ハッシュ                     | SHA-1                            | -                                    | FIPS 180-4, 6.1  | none       | SHAVS            |
|                          | SHA-224                          | -                                    | FIPS 180-4, 6.3  |            |                  |

|                         |                         |                   |                     |  |        |  |
|-------------------------|-------------------------|-------------------|---------------------|--|--------|--|
| (SHS)                   | SHA-256                 | -                 | FIPS 180-4, 6.2     |  |        |  |
|                         | SHA-384                 | -                 | FIPS 180-4, 6.5     |  |        |  |
|                         | SHA-512                 | -                 | FIPS 180-4, 6.4     |  |        |  |
|                         | SHA-512/224             | -                 | FIPS 180-4, 6.6     |  |        |  |
|                         | SHA-512/256             | -                 | FIPS 180-4, 6.7     |  |        |  |
| ハッシュ<br>(SHA-3)         | SHA3-224                | -                 | FIPS 202, 6.1       | none   | SHA3VS |  |
|                         | SHA3-256                | -                 |                     |  |        |  |
|                         | SHA3-384                | -                 |                     |  |        |  |
|                         | SHA3-512                | -                 |                     |  |        |  |
|                         | SHAKE128                | -                 | FIPS 202, 6.2       |  |        |  |
|                         | SHAKE256                | -                 |                     |  |        |  |
| メッセージ認証<br>(MAC)        | CMAC                    | 生成 w/ AES         | SP 800-38B, 6.2     | none   | CMACVS |  |
|                         |                         | 検証 w/ AES         | SP 800-38B, 6.3     | AES  |        |  |
|                         |                         | 生成 w/ TDES        | SP 800-38B, 6.2     | TDES   |        |  |
|                         |                         | 検証 w/ TDES        | SP 800-38B, 6.3     | TDES   |        |  |
|                         | CCM(AES CCM)            | -                 | SP 800-38C, 6       | AES  | CCMVS  |  |
|                         | GCM(AES GCM)            | -                 | SP 800-38D, 7       | AES<br>DRBG *Required only if IVs generated internally using method in Section 8.2.2 | GCMVS  |  |
|                         | * GMAC を含む              |                   |                     |  |        |  |
|                         | HMAC w/ SHA1            | -                 | FIPS 198, 4         | SHA  | HMACVS |  |
|                         | HMAC w/ SHA224          | -                 |                     |  |        |  |
|                         | HMAC w/ SHA256          | -                 |                     |  |        |  |
|                         | HMAC w/ SHA384          | -                 |                     |  |        |  |
|                         | HMAC w/ SHA512          | -                 |                     |  |        |  |
|                         | HMAC w/ SHA512/224      | -                 |                     |  |        |  |
|                         | HMAC w/ SHA512/256      | -                 |                     |  |        |  |
|                         |                         |                   |                     |  |        |  |
| 疑似乱数<br>ビット生成器          | Hash_DRBG               | -                 | SP 800-90A, 10.1.1  | SHA  | DRBGVS |  |
|                         | HMAC_DRBG               | -                 | SP 800-90A, 10.1.2  | HMAC   |        |  |
|                         | CTR_DRBG                | -                 | SP 800-90A, 10.2.1  | TDES or AES  |        |  |
| 鍵確立<br>(鍵合意システム<br>FFC) | dhHybrid1               | -                 | SP 800-56A, 6.1.1.1 | SHA / DRBG   | KASVS  |  |
|                         | MQV2                    | -                 | SP 800-56A, 6.1.1.3 |  |        |  |
|                         |                         |                   |                     |  |        | *Optional-Required only if KC supported<br>CCM / CMAC / HMAC |
|                         | dhEphem                 | -                 | SP 800-56A, 6.1.2.1 | SHA / DRBG   |        |  |
|                         | dhHybridOneFlow         | -                 | SP 800-56A, 6.2.1.1 | SHA / DRBG   |        |  |
|                         | MQV1                    | -                 | SP 800-56A, 6.2.1.3 |  |        |  |
|                         | dhOneFlow               | -                 | SP 800-56A, 6.2.2.1 |  |        |  |
| dhStatic                | -                       | SP 800-56A, 6.3.1 |                     | *Optional-Required only if KC supported<br>CCM / CMAC / HMAC                         |        |  |
| 鍵確立<br>(鍵合意システム<br>ECC) | Full Unified Model      | -                 | SP 800-56A, 6.1.1.2 | ECDSA / SHA / DRBG<br>*If KC is supported<br>CCM / CMAC / HMAC                       | KASVS  |  |
|                         | Full MQV                | -                 | SP 800-56A, 6.1.1.4 | SHA / DRBG   |        |  |
|                         | Ephemeral Unified Model | -                 | SP 800-56A, 6.1.2.2 | *If KC is supported<br>CCM / CMAC / HMAC   |        |  |
|                         | One Pass Unified Model  | -                 | SP 800-56A, 6.2.1.2 |  |        |  |
|                         | One Pass MQV            | -                 | SP 800-56A, 6.2.1.4 |  |        |  |
|                         | One-Pass Diffie-Hellman | -                 | SP 800-56A, 6.2.2.2 |  |        |  |
|                         | Static Unified Model    | -                 | SP 800-56A, 6.3.2   |  |        |  |

|                                 |  |                  |                     |  |         |
|---------------------------------|--|------------------|---------------------|--|---------|
|                                 | ECC CDH Component Test                           | -                | SP 800-56A, 5.7.1.2 | ECDSA (Key Pair)<br>*If Key Pair Generation or Key Pair Regeneration is contained.<br>*If KC is supported<br>CCM / CMAC / HMAC |         |
| 鍵導出関数(KDF)                      | SP 800-108 KDF in Counter Mode                   | -                | SP 800-108, 5.1     | SP800-56A KAS, SP 800-90 DRBG  | KBKDFVS |
|                                 | SP 800-108 KDF in Feedback Mode                  | -                | SP 800-108, 5.2     | CMAC or HMAC used in generating KDF  |         |
|                                 | SP 800-108 KDF in Double-Pipeline Iteration Mode | -                | SP 800-108, 5.3     |  |         |
|                                 | IKE version 1 KDF                                | -                | SP 800-135, 4.1.1   | SHA / HMAC   |         |
|                                 | IKE version 2 KDF                                | -                | SP 800-135, 4.1.2   | SHA / HMAC   |         |
|                                 | Key Derivation in TLS 1.0/1.1                    | -                | SP 800-135, 4.2.1   | SHA / HMAC   |         |
|                                 | Key Derivation in TLS 1.2                        | -                | SP 800-135, 4.2.2   |  |         |
|                                 | KDF in ANS X9.63-2001                            | -                | SP 800-135, 5.1     | SHA  |         |
|                                 | SSH KDF  | -                | SP 800-135, 5.2     | SHA  |         |
|                                 | SRTP KDF   | -                | SP 800-135, 5.3     | AES  |         |
|                                 | SNMP KDF   | -                | SP 800-135, 5.4     | SHA  |         |
| TPM KDF                         | -  | SP 800-135, 5.5  | SHA / HMAC          |  |         |
| RSADP Component                 | -  | SP800-56B, 7.1.2 | none                |  |         |
| 鍵包み並びに認証暗号化及び復号(KW, KWP 及び TKW) | AES Key Wrap (KW)                                | -                | SP 800-38F, 6.2     | AES  | KWVS    |
|                                 | AES Key Wrap with Padding (KWP)                  | -                | SP 800-38F, 6.3     | AES  |         |
|                                 | Triple DEA Key Wrap (TKW)                        | -                | SP 800-38F, 7.2     | TDES   |         |

| 文書名略称                     | 文書名称   |
|---------------------------|--|
| ANSI X9.31                | ANS X9.31-1998, 1998 September 9                                 |
| ANSI X9.52                | ANS X9.52-1998, 1998 July 29                                     |
| ANSI X9.62                | ANS X9.62-1998, Jan 7 1999                                       |
| FIPS 180-4                | FIPS 180-4, March 2012   |
| FIPS 186-2                | FIPS PUB 186-2, 2000 January 27                                  |
| FIPS 186-2+ Change Notice | FIPS PUB 186-2, 2000 January 27 + Change Notice, 2001 October 5  |
| FIPS 186-4                | FIPS PUB 186-4, July 2013  |
| FIPS 197                  | FIPS 197, 2001 November 26                                       |
| FIPS 198                  | FIPS PUB 198-1, July 2008  |
| FIPS 202                  | FIPS PUB 202, August 2015  |
| PKCS#1 v2.1               | PKCS #1 v2.1: RSA Cryptography Standard, 2002 June 14            |
| SP 800-38A                | NIST Special Publication 800-38A, 2001 Edition                   |
| SP 800-38B                | NIST Special Publication 800-38B, May 2005                       |
| SP 800-38C                | NIST Special Publication 800-38C, May 2004                       |
| SP 800-38D                | NIST Special Publication 800-38D, November 2007                  |
| SP 800-38E                | NIST Special Publication 800-38E, January 2010                   |
| SP 800-38F                | NIST Special Publication 800-38F, December 2012                  |
| SP 800-56A                | NIST Special Publication 800-56A, March 2007                     |
| SP 800-56B                | NIST Special Publication 800-56B, August 2009                    |
| SP 800-67                 | NIST Special Publication 800-67 Revision 1, Revised January 2012 |
| SP 800-90A                | NIST Special Publication 800-90A, January 2012                   |
| SP 800-108                | NIST Special Publication 800-108, October 2009                   |
| SP 800-135                | NIST Special Publication 800-135, Revision 1, December 2011      |