2011年度版リストガイド(SSL/TLS)

平成24年3月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

目 次

1　本書の位置づけ

1.1　本書の目的

リストガイドは、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、電子政府推奨暗号を利用する際に必要となる情報並びに推奨を示すものである。

本書では、電子政府をはじめとして、よく利用されている SSL/TLS について、その利用方法並びに選択すべき暗号アルゴリズムについて情報提供を行うものである。

1.2　本書の構成

本書では、2 章で SSL/TLS に関する情報提供ならびに推奨事項を示す。

1.3　本書の利用範囲

本書の内容は 2012 年 3 月 31 日時点の情報に基づき構成されている。従って、今後、電子政府推奨暗号の改訂や電子政府推奨暗号に係る攻撃方法の研究動向、Internet Engineering Task Force (以下、「IETF」という。) における各種 Request For Comments(以下、「RFC」という。) やその他標準規格の策定状況及び NIST の Special Publicaion(以下、「SP」という。) をはじめとする推奨文書等の改訂状況等によって、本書に掲載される内容がそぐわないくなるケースが発生する可能性がある。

本書を利用する際には、関連する標準規格並びに各種推奨文書等も同時に参照し、適切に判断を行うことを勧める。

1.3.1　登録商標について

本書では、原則的に商品名及びサービス名の標記については、登録商標に従った。本書で用いる図表等に記載する会社名、商品名、サービス名は一般に各社の商標、又は、登録商標である。

表 1: 本書に登場する登録商標

商標名	権利者
Windows	マイクロソフト　コーポレイション
Internet Explorer	マイクロソフト　コーポレイション
FireFox	モジラ　ファウンデーション
Safari	Apple Inc.
Google Chrome	Google Inc.

2　SSL/TLS に関する推奨

2.1　TLS の実行環境

2012 年 3 月現在、Windows 環境下での最新のブラウザにおける SSL/TLS の実装状況を表 2 に示す (詳細を 2.2 に示す)。

表 2: 各種ブラウザの SSL/TLS の実装状況

ブラウザ	SSL2.0	SSL3.0/TLS 1.0	TLS 1.1/1.2
Internet Explorer 9	デフォルト OFF (ON/OFF 選択可)	デフォルト ON (ON/OFF 選択可)	デフォルト OFF (ON/OFF 選択可)
FireFox 9	無効化	デフォルト ON	未実装
Google Chrome 15	無効化	設定項目なし (実装上は ON)	未実装
Safari 5	無効化	設定項目なし (実装上は ON)	未実装

推奨する暗号スイート (2.2 節参照) を適切に利用する場合、TLS 1.1/1.2 の利用が望ましい。一方で、現状では TLS 1.1/1.2 の利用環境が限られているが、今後各種ブラウザにおいて TLS 1.1/1.2 の実装が進むことが想定されている。このため、最新の OS の導入を進め、各種ブラウザの TLS 1.1/1.2 への対応にあわせて、適切にバージョンアップを行える OS 環境に移行しておくことが望ましい。

2.2　推奨暗号スイート

SSL/TLS において利用可能な暗号スイートの中から、電子政府において利用可能な暗号スイート（推奨暗号スイート）を選定するための判断フローを図 1 に示す。

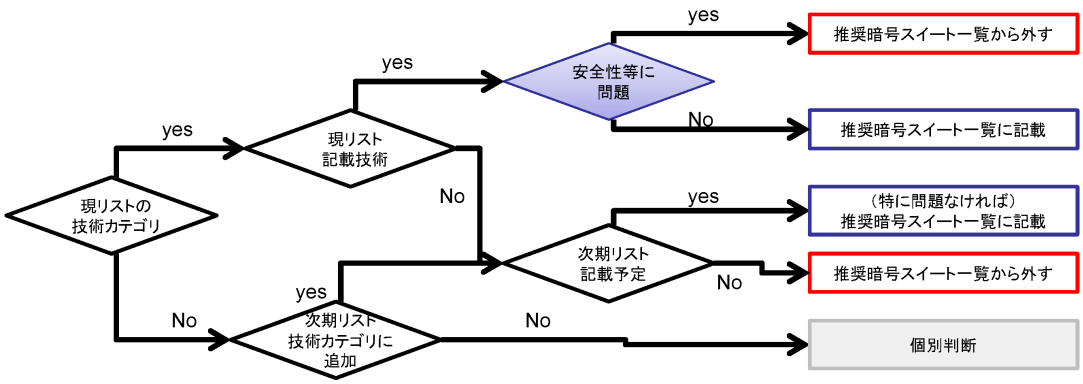

図 1: 推奨暗号スイートの判断フロー

電子政府において利用を推奨する暗号スイートの一覧を表 3 に示す。表中灰色で色抜きされた暗号スイートは、利用を推奨できない暗号スイートであり、以下のいずれかの条件を満たす暗号スイートである。

- 電子政府推奨暗号として指定された暗号プリミティブを用いているが、鍵長等について安全性上問題がある場合
- 電子政府推奨暗号として指定された技術カテゴリだが、記載されていない暗号プリミティブを用いている場合
- 電子政府推奨暗号として指定されない技術カテゴリを用いており、かつ、推奨できない場合

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0x00,0x00	TLS_NULL_WITH_NULL_NULL	5246
0x00,0x01	TLS_RSA_WITH_NULL_MD5	5246
0x00,0x02	TLS_RSA_WITH_NULL_SHA	5246
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5	4346
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5	5246
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA	5246
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	4346
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA	5469
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA	5469
0x00,0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x0B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x0C	TLS_DH_DSS_WITH_DES_CBC_SHA	5469
0x00,0x0D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x0E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x0F	TLS_DH_RSA_WITH_DES_CBC_SHA	5469
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA	5469
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA	5469
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	4346
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5	5246
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	4346
0x00,0x1A	TLS_DH_anon_WITH_DES_CBC_SHA	5469
0x00,0x1B	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	5246
0x00,0x2C	TLS_PSK_WITH_NULL_SHA	4785
0x00,0x2D	TLS_DHE_PSK_WITH_NULL_SHA	4785

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0x00,0x2E	TLS_RSA_PSK_WITH_NULL_SHA	4785
0x00,0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	5246
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA	5246
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA	5246
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	5246
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	5246
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA	5246
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA	5246
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA	5246
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA	5246
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	5246
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	5246
0x00,0x3A	TLS_DH_anon_WITH_AES_256_CBC_SHA	5246
0x00,0x3B	TLS_RSA_WITH_NULL_SHA256	5246
0x00,0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	5246
0x00,0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	5246
0x00,0x3E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	5246
0x00,0x3F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	5246
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	5246
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	5932
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	5246
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	5246
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	5246
0x00,0x6A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	5246
0x00,0x6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	5246
0x00,0x6C	TLS_DH_anon_WITH_AES_128_CBC_SHA256	5246
0x00,0x6D	TLS_DH_anon_WITH_AES_256_CBC_SHA256	5246
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	5932
0x00,0x8A	TLS_PSK_WITH_RC4_128_SHA	4279
0x00,0x8B	TLS_PSK_WITH_3DES_EDE_CBC_SHA	4279
0x00,0x8C	TLS_PSK_WITH_AES_128_CBC_SHA	4279
0x00,0x8D	TLS_PSK_WITH_AES_256_CBC_SHA	4279
0x00,0x8E	TLS_DHE_PSK_WITH_RC4_128_SHA	4279
0x00,0x8F	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA	4279

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA	4279
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA	4279
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA	4279
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA	4279
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA	4279
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA	4279
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA	4162
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA	4162
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA	4162
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA	4162
0x00,0x9A	TLS_DHE_RSA_WITH_SEED_CBC_SHA	4162
0x00,0x9B	TLS_DH_anon_WITH_SEED_CBC_SHA	4162
0x00,0x9C	TLS_RSA_WITH_AES_128_GCM_SHA256	5288
0x00,0x9D	TLS_RSA_WITH_AES_256_GCM_SHA384	5288
0x00,0x9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	5288
0x00,0x9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	5288
0x00,0xA0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	5288
0x00,0xA1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	5288
0x00,0xA2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	5288
0x00,0xA3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	5288
0x00,0xA4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	5288
0x00,0xA5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	5288
0x00,0xA6	TLS_DH_anon_WITH_AES_128_GCM_SHA256	5288
0x00,0xA7	TLS_DH_anon_WITH_AES_256_GCM_SHA384	5288
0x00,0xA8	TLS_PSK_WITH_AES_128_GCM_SHA256	5487
0x00,0xA9	TLS_PSK_WITH_AES_256_GCM_SHA384	5487
0x00,0xAA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	5487
0x00,0xAB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	5487
0x00,0xAC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	5487
0x00,0xAD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	5487
0x00,0xAE	TLS_PSK_WITH_AES_128_CBC_SHA256	5487
0x00,0xAF	TLS_PSK_WITH_AES_256_CBC_SHA384	5487
0x00,0xB0	TLS_PSK_WITH_NULL_SHA256	5487
0x00,0xB1	TLS_PSK_WITH_NULL_SHA384	5487
0x00,0xB2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	5487
0x00,0xB3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	5487
0x00,0xB4	TLS_DHE_PSK_WITH_NULL_SHA256	5487
0x00,0xB5	TLS_DHE_PSK_WITH_NULL_SHA384	5487
0x00,0xB6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	5487
0x00,0xB7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	5487
0x00,0xB8	TLS_RSA_PSK_WITH_NULL_SHA256	5487
0x00,0xB9	TLS_RSA_PSK_WITH_NULL_SHA384	5487
0x00,0xBA	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	5932
0x00,0xBB	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256	5932

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0x00,0xBC	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	5932
0x00,0xBD	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	5932
0x00,0xBE	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	5932
0x00,0xBF	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	5932
0x00,0xC0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	5932
0x00,0xC1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256	5932
0x00,0xC2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256	5932
0x00,0xC3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	5932
0x00,0xC4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	5932
0x00,0xC5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	5932
0xC0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA	4492
0xC0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	4492
0xC0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	4492
0xC0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	4492
0xC0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	4492
0x0xC0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA	4492
0xC0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	4492
0xC0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	4492
0xC0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	4492
0xC0,0x0A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	4492
0xC0,0x0B	TLS_ECDH_RSA_WITH_NULL_SHA	4492
0xC0,0x0C	TLS_ECDH_RSA_WITH_RC4_128_SHA	4492
0xC0,0x0D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	4492
0xC0,0x0E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	4492
0xC0,0x0F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	4492
0xC0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA	4492
0xC0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA	4492
0xC0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	4492
0xC0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	4492
0xC0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	4492
0xC0,0x15	TLS_ECDH_anon_WITH_NULL_SHA	4492
0xC0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA	4492
0xC0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	4492
0xC0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	4492
0xC0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	4492
0xC0,0x1A	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	5054
0xC0,0x1B	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA	5054
0xC0,0x1C	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA	5054
0xC0,0x1D	TLS_SRP_SHA_WITH_AES_128_CBC_SHA	5054
0xC0,0x1E	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA	5054
0xC0,0x1F	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA	5054
0xC0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA	5054
0xC0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA	5054
0xC0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA	5054

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0xC0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	5289
0xC0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	5289
0xC0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	5289
0xC0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	5289
0xC0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	5289
0xC0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	5289
0xC0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	5289
0xC0,0x2A	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	5289
0xC0,0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	5289
0xC0,0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	5289
0xC0,0x2D	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	5289
0xC0,0x2E	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	5289
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	5289
0xC0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	5289
0xC0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	5289
0xC0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	5289
0xC0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA	5489
0xC0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA	5489
0xC0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	5489
0xC0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	5489
0xC0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	5489
0xC0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	5489
0xC0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA	5489
0xC0,0x3A	TLS_ECDHE_PSK_WITH_NULL_SHA256	5489
0xC0,0x3B	TLS_ECDHE_PSK_WITH_NULL_SHA384	5489
0xC0,0x3C	TLS_RSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x3D	TLS_RSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x3E	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x3F	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x4A	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x4B	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x4C	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x4D	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x4E	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256	6209

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0xC0,0x4F	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x5A	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x5B	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x5C	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x5D	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x5E	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x5F	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x6A	TLS_PSK_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x6B	TLS_PSK_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x6C	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x6D	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x6E	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256	6209
0xC0,0x6F	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384	6209
0xC0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256	6209
0xC0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384	6209
0xC0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x7A	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	6367

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

表 3: 推奨暗号スイート一覧

番号	暗号スイート	RFC
0xC0,0x7B	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x7C	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x7D	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x7E	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x7F	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x8A	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x8B	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x8C	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x8D	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x8E	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x8F	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256	6367
0xC0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384	6367
0xC0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384	6367
0xC0,0x9A	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256	6367
0xC0,0x9B	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384	6367

灰色で色抜きされた部分は電子政府において利用を推奨しない暗号スイートである

付録 A SSL/TLS の実行環境ごとの利用可能性

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
Windows 95	Internet Explorer 3★	◯	◯	×	×	×
	Internet Explorer 5	◯	◯	×	×	×
	Internet Explorer 6	×	×	×	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3	×	×	×	×	×
	FireFox 4	×	×	×	×	×
	FireFox 5	×	×	×	×	×
	FireFox 6	×	×	×	×	×
	FireFox 7	×	×	×	×	×
	FireFox 8	×	×	×	×	×
	Safari 3	×	×	×	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	Google Chrome 15.0	×	×	×	×	×
Windows 98	Internet Explorer 4★	◯	◯	×	×	×
	Internet Explorer 5	◯	◯	×	×	×
	Internet Explorer 6	◯	◯	×	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3	×	×	×	×	×
	FireFox 4	×	×	×	×	×
	FireFox 5	×	×	×	×	×
	FireFox 6	×	×	×	×	×
	FireFox 7	×	×	×	×	×
	FireFox 8	×	×	×	×	×
	Safari 3	×	×	×	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×
	Google Chrome 15.0	×	×	×	×	×
Windows Me	Internet Explorer 5	×	×	×	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	Internet Explorer 5★	◯	◯	△	×	×
	Internet Explorer 6	◯	◯	△	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3	×	×	×	×	×
	FireFox 4	×	×	×	×	×
	FireFox 5	×	×	×	×	×
	FireFox 6	×	×	×	×	×
	FireFox 7	×	×	×	×	×
	FireFox 8	×	×	×	×	×
	Safari 3	×	×	×	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×
	Google Chrome 15.0	×	×	×	×	×
Windows NT 4.0	Internet Explorer 3★	◯	◯	×	×	×
	Internet Explorer 5	×	×	×	×	×
	Internet Explorer 6	×	×	×	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3.6	×	×	×	×	×
	FireFox 4	×	×	×	×	×
	FireFox 5	×	×	×	×	×
	FireFox 6	×	×	×	×	×
	FireFox 7	×	×	×	×	×
	FireFox 8	×	×	×	×	×
	Safari 3	×	×	×	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×
	Google Chrome 15.0	×	×	×	×	×
Windows 2000	Internet Explorer 5★	◯	◯	△	×	×
	Internet Explorer 6	◯	◯	△	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	FireFox 3.6	×	◯	◯	×	×
	FireFox 4	×	◯	◯	×	×
	FireFox 5	×	◯	◯	×	×
	FireFox 6	×	◯	◯	×	×
	FireFox 7	×	◯	◯	×	×
	FireFox 8	×	◯	◯	×	×
	Safari 3	×	×	×	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×
	Google Chrome 15.0	×	×	×	×	×
Windows XP	Internet Explorer 5	×	×	×	×	×
	Internet Explorer 6★	◯	◯	△	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3.6	×	◯	◯	×	×
	FireFox 4	×	◯	◯	×	×
	FireFox 5	×	◯	◯	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	FireFox 6	×	◯	◯	×	×
	FireFox 7	×	◯	◯	×	×
	FireFox 8	×	◯	◯	×	×
	Safari 3	◯	◯	◯	×	×
	Safari 4	×	×	×	×	×
	Safari 5	×	×	×	×	×
	Google Chrome 1.0	×	×	×	×	×
	Google Chrome 2.0	×	×	×	×	×
	Google Chrome 3.0	×	×	×	×	×
	Google Chrome 4.0	×	×	×	×	×
	Google Chrome 4.1	×	×	×	×	×
	Google Chrome 5.0	×	×	×	×	×
	Google Chrome 6.0	×	×	×	×	×
	Google Chrome 7.0	×	×	×	×	×
	Google Chrome 8.0	×	×	×	×	×
	Google Chrome 9.0	×	×	×	×	×
	Google Chrome 10.0	×	×	×	×	×
	Google Chrome 11.0	×	×	×	×	×
	Google Chrome 12.0	×	×	×	×	×
	Google Chrome 13.0	×	×	×	×	×
	Google Chrome 14.0	×	×	×	×	×
	Google Chrome 15.0	×	×	×	×	×
Windows XP + SP3	Internet Explorer 5	×	×	×	×	×
	Internet Explorer 6★	◯	◯	△	×	×
	Internet Explorer 7	△	◯	◯	×	×
	Internet Explorer 8	△	◯	◯	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3.6	×	◯	◯	×	×
	FireFox 4	×	◯	◯	×	×
	FireFox 5	×	◯	◯	×	×
	FireFox 6	×	◯	◯	×	×
	FireFox 7	×	◯	◯	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	FireFox 8	×	◯	◯	×	×
	Firefox 9	×	◯	◯	×	×
	Safari 3	◯	◯	◯	×	×
	Safari 4	×	◯	◯	×	×
	Safari 5	×	◯	◯	×	×
	Google Chrome 1.0	△	◯	◯	×	×
	Google Chrome 2.0	△	◯	◯	×	×
	Google Chrome 3.0	△	◯	◯	×	×
	Google Chrome 4.0	△	◯	◯	×	×
	Google Chrome 4.1	△	◯	◯	×	×
	Google Chrome 5.0	△	◯	◯	×	×
	Google Chrome 6.0	△	◯	◯	×	×
	Google Chrome 7.0	△	◯	◯	×	×
	Google Chrome 8.0	△	◯	◯	×	×
	Google Chrome 9.0	△	◯	◯	×	×
	Google Chrome 10.0	×	◯	◯	×	×
	Google Chrome 11.0	×	◯	◯	×	×
	Google Chrome 12.0	×	◯	◯	×	×
	Google Chrome 13.0	×	◯	◯	×	×
	Google Chrome 14.0	×	◯	◯	×	×
	Google Chrome 15.0	×	◯	◯	×	×
Windows Vista	Internet Explorer 5	×	×	×	×	×
	Internet Explorer 6	×	×	×	×	×
	Internet Explorer 7★	△	◯	◯	×	×
	Internet Explorer 8	×	×	×	×	×
	Internet Explorer 9	×	×	×	×	×
	FireFox 3.6	×	◯	◯	×	×
	FireFox 4	×	◯	◯	×	×
	FireFox 5	×	◯	◯	×	×
	FireFox 6	×	◯	◯	×	×
	FireFox 7	×	◯	◯	×	×
	FireFox 8	×	◯	◯	×	×
	Safari 3	×	◯	◯	×	×

★:デフォルトブラウザ

◯:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	Safari 4	×	○	○	×	×
	Safari 5	×	○	○	×	×
	Google Chrome 1.0	△	○	○	×	×
	Google Chrome 2.0	△	○	○	×	×
	Google Chrome 3.0	△	○	○	×	×
	Google Chrome 4.0	△	○	○	×	×
	Google Chrome 4.1	△	○	○	×	×
	Google Chrome 5.0	△	○	○	×	×
	Google Chrome 6.0	△	○	○	×	×
	Google Chrome 7.0	△	○	○	×	×
	Google Chrome 8.0	△	○	○	×	×
	Google Chrome 9.0	△	○	○	×	×
	Google Chrome 10.0	×	○	○	×	×
	Google Chrome 11.0	×	○	○	×	×
	Google Chrome 12.0	×	○	○	×	×
	Google Chrome 13.0	×	○	○	×	×
	Google Chrome 14.0	×	○	○	×	×
	Google Chrome 15.0	×	○	○	×	×
Windows 7 + SP1	Internet Explorer 5	×	×	×	×	×
	Internet Explorer 6	×	×	×	×	×
	Internet Explorer 7	×	×	×	×	×
	Internet Explorer 8★	△	○	○	△	△
	Internet Explorer 9	△	○	○	△	△
	FireFox 3.6	△	○	○	×	×
	FireFox 4	×	○	○	×	×
	FireFox 5	×	○	○	×	×
	FireFox 6	×	○	○	×	×
	FireFox 7	×	○	○	×	×
	FireFox 8	×	○	○	×	×
	FireFox 9	×	○	○	×	×
	Safari 3	×	○	○	×	×
	Safari 4	×	○	○	×	×

★:デフォルトブラウザ

○:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

表 4: SSL/TLS の実行環境ごとの利用可能性

OS	ブラウザ	SSL		TLS		
		v2.0	v3.0	v1.0	v1.1	v1.2
	Safari 5	×	○	○	×	×
	Google Chrome 1.0	△	○	○	×	×
	Google Chrome 2.0	△	○	○	×	×
	Google Chrome 3.0	△	○	○	×	×
	Google Chrome 4.0	△	○	○	×	×
	Google Chrome 4.1	△	○	○	×	×
	Google Chrome 5.0	△	○	○	×	×
	Google Chrome 6.0	△	○	○	×	×
	Google Chrome 7.0	△	○	○	×	×
	Google Chrome 8.0	△	○	○	×	×
	Google Chrome 9.0	△	○	○	×	×
	Google Chrome 10.0	×	○	○	×	×
	Google Chrome 11.0	×	○	○	×	×
	Google Chrome 12.0	×	○	○	×	×
	Google Chrome 13.0	×	○	○	×	×
	Google Chrome 14.0	×	○	○	×	×
	Google Chrome 15.0	×	○	○	×	×

★:デフォルトブラウザ

○:ブラウザのインストール時にデフォルトで利用可能

△:利用するためにはオプションの変更等，設定することで利用可能

×:設定項目自体がなく利用することができない，または，インストールできない

参考文献

[推奨暗号] 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）
http://www.cryptrec.go.jp/images/cryptrec_01.pdf

[統一基準] 内閣官房情報セキュリティセンター、“政府機関の情報セキュリティ対策のための統一基準（第４版）”.
http://www.nisc.go.jp/active/general/pdf/K303-081.pdf

[IANA] Internet Assigned Number Authority, “Transport Layer Security (TLS) Parameters ”, Last Updated 2011-12-10.
http://www.iana.org/assignments/tls-parameters/tls-parameters.xml

[SP800-113] Sheila Frankel, Paul Hoffman Angela Orebaugh, Richard Park, “Special Publication 800-113 Guide to SSL VPNs ”National Institute os Standards and Technology, Jul 2008.
http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

発行日　2012 年 9 月 30 日第 1 版 第 1 刷
発行者
・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室、
セキュリティ基盤研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN