項番	ページ	引用文献			版数	変更要否	最新化日付 2015/5 以降は黄	タイトル タイトルではないものは水色	対象サイト等
		文献名	記載場所等	記載行等					
1	8	RFC 4346				×	2006年4月	The Transport Layer Security (TLS) Protocol Version 1.1	https://www.ipa.go.jp/security/rfc/RFC4346EN.html
2	8	RFC 6101				×	2011年8月	The Secure Sockets Layer (SSL) Protocol Version 3.0	https://tools.ietf.org/html/rfc6101
3	8	RFC 2246				×	1999年1月	The TLS Protocol Version 1.0	https://www.ipa.go.jp/security/rfc/RFC2246-00JA.html
4	8	RFC 5246				×	2008年8月	The Transport Layer Security (TLS) Protocol Version 1.2	https://www.ipa.go.jp/security/rfc/RFC5246-00JA.html
5	8	CRYPTREC暗号技術ガイドライン（SSL/TLSにおける近年の攻撃への対応状況）	脚注	6		×	2014/3/25	CRYPTREC暗号技術ガイドライン(SSL/TLS における近年の攻撃への対応)	http://www.cryptrec.go.jp/report/c13_kentou_gijiO2_r2.pdf
6	9	SSL3.0 の脆弱性対策について	脚注	8		×	2014/10/30	SSL 3.0 の脆弱性対策について(CVE-2014-3566)	http://www.ipa.go.jp/security/announce/20141017-ssl.html
7	11	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)	脚注	10		×	2013/3/1	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）	http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
8	11	政府機関の情報セキュリティ対策のための統一基準（平成26年度版）	本文 2.2.1項	7		①	2016/8/31	政府機関の情報セキュリティ対策のための統一基準（平成28年度版）	https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
9	12	NIST SP800-57 Part 1 Revision 3	本文	9	Revision 4	②	2016/1/28	Recommendation for Key Management, Part 1: General	https://csrc.nist.gov/csrc/media/publications/sp/800-57-part-1/rev-4/final/documents/sp800-57p1r4_draft.pdf#search=%27NIST+SP80057+Part+1+Revision+4%27
10	22	The POODLE bites again	脚注	14		×	2014/12/8	The POODLE bites again (08 Dec 2014)	https://www.imperialviolet.org/2014/12/08/poodleagain.html
10-1	22	Apache Http Server における SSL 3.0 の無効化	本文内の図			×	2016/1/6	httpd における POODLE SSLv3.0 脆弱性問題の解決方法	https://access.redhat.com/ja/solutions/1232613
10-2	22	Windows における SSL 3.0 の無効化	本文内の図			×	2015/4/15	SSL 3.0 の脆弱性により、情報漏えいが起こる	https://technet.microsoft.com/ja-jp/library/security/3009008.aspx
11	22	CVE-2014-8730	脚注	15		×	2014/11/10	CVE-2014-8730	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8730
12	23	SECG Consortium	脚注	16		×	2005/2/10	SECG Consortium	http://www.secg.org/certicom_patent_letter_SECG.pdf
13	30	CRYPTREC Report 2013	脚注	19		③	2017年3月	CRYPTREC Report 2016	http://www.cryptrec.go.jp/report/cryptrec-rp-0002-2016.pdf#search=%27CRYPTREC+Report+2016%27
14	30	政府機関の情報ｼｽﾃﾑにおいて使用されている暗号ｱﾙｺﾞﾘｽﾞﾑSHA-1及びRSA1024に係る移行指針	脚注	20		×	2012/10/26	政府機関の情報ｼｽﾃﾑにおいて使用されている暗号ｱﾙｺﾞﾘｽﾞﾑSHA-1及びRSA1024に係る移行指針	http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
15	31	コラム	本文			×		~~誤記（正：heatbleed、誤：Heartbeat）？~~	
16	〃	〃	脚注	21		×	2014/5/9	Keys left unchanged in many Heartbleed replacement certificates!	http://news.netcraft.com/archives/2014/05/09/keys-left-unchanged-in-many-heartbleed-replacement-certificates.html
17	35	NIST SP800-52 revision 1 (draft)	脚注	23		④	2014年4月	NIST SP800-52 revision 1	https://csrc.nist.gov/csrc/media/publications/sp/800-52/rev-1/final/documents/draft_sp800_52_r1.pdf#search=%27NIST+SP80052+revision+1%27
18	35	Algorithms, Key Sizes and Parameters Report – 2013 recommendations	脚注	24		×	2014/11/21	Algorithms, key size and parameters report 2014	https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
19	37	(2015年1月のAlexaの調査結果)	脚注	25		×	2015年1月	January 2015 scan results	https://securitypitfalls.wordpress.com/2015/02/01/january-2015-scan-results/
20	45	既知の解読可能な鍵ペアでないことを確認するサービス	脚注	29		⑤	2017/11/1 現在	(The keycheck service is no longer available.) 利用不可になったらしい	https://factorable.net/keycheck.html
21	49	RFC 6797				×	2012年11月	HTTP Strict Transport Security (HSTS)	https://tools.ietf.org/html/rfc6797
22	51	RFC 5746				×	2010年2月	Transport Layer Security (TLS) Renegotiation Indication Extension	https://tools.ietf.org/html/rfc5746
23	52	RFC 6066				×	2011年1月	Transport Layer Security (TLS) Extensions: Extension Definitions	https://tools.ietf.org/html/rfc6066
24	53	EMET	脚注	33		⑥		サポート終了日は 2018年7月31日。Windows 10 最新バージョンへの移行をお勧め。	http://technet.microsoft.com/ja-jp/security/jj653751
25	55	Microsoft Internet Explorer サポートライフサイクルポリシーに関するFAQ	本文 8.1.2項	23		×	2016/3/31	サポート ライフサイクル ポリシーに関する FAQ - Internet Explorer	http://support2.microsoft.com/gp/microsoft-internet-explorer
25-1	55	デスクトップ向けOS	本文 8.1.1項	7～11		⑦			
26	57	バージョン別IEのセキュリティ機能	本文 8.2.2項	12		⑧	2013/2/15	バージョン別セキュリティ既定値一覧表	http://msdn.microsoft.com/ja-jp/ie/cc844005.aspx
27	58	Firefox	本文 8.2.2項	1		⑨		(最新の 56.0.2 では「ﾂｰﾙ」「ｵﾌﾟｼｮﾝ」の証明書項目で一択（オンかオフ）に変更されている)	
28	59	Microsoft Internet Explorer	脚注	34		○	2015/10/19	SHA1 Deprecation Policy	http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
29	59	Google Chrome	脚注	35		⑩	2014/9/5	Gradually Sunsetting SHA-1	https://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
30	〃	〃	脚注	36		〃	2015/3/12	Towards the sunset of SHA-1	https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/QNVVo4_dyQE
31	59	Mozilla Firefox	脚注	37		⑪	2010/12/31	Dates for Phasing out MD5-based signatures and 1024-bit moduli	https://wiki.mozilla.org/CA:MD5and1024
32	59	SHA-1で署名されたサーバ証明書	脚注	38		⑫	2017/11/1 現在	(Not Found) 記事が削除されたらしい	https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signaturealgorithms/
33	60	マイクロソフトセキュリティアドバイザリ3009008	本文 8.3.2項	10		⑬	2015/4/15	SSL 3.0 の脆弱性により、情報漏えいが起こる	https://technet.microsoft.com/ja-jp/library/security/3009008.aspx
34	76	特定の暗号化アルゴリズムおよびSchannel.dll のプロトコルの使用を制限する方法	本文 B.2.4	5		⑭		How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll	https://support.microsoft.com/en-us/kb/245030
35	82	Public-Key-Pinsヘッダを自動作成するサイト	脚注	40		×	2016/1/2	JavaScript Public-Key-Pins (HPKP) calculator v1.0.3	https://projects.dm.id.lv/s/pkp-online/calculator.html
36	83	Microsoft IISの場合	本文 B.6.4			×		(IIS 10.0でも操作は同じ（実機確認))	
37	84	Windowsでの設定例	本文 C.1	2		⑮		(Windows Server 2016 では「SSL暗号の順序」ではなく「SSL暗号の順位」と表示（実機確認)	
38	〃	フリーウェア	脚注	42		○		(Windows Server 2008、2008 R2、2012、2012 R2、2016 に拡大されている)	https://www.nartac.com/Products/IISCrypto/

39	全般	本ガイドラインの公開	全般			○		（日付けきで至る所に記載されているが改訂後は日付の変更が必要）	
40		以下、下に記載の ⑮ 以降も改訂が必要	各項参照	←		←			

① P.11 の「政府機関の情報セキュリティ対策のための統一基準（抄）」を「統一基準」シート［C18-P28］の記載に全面変更
② P.12 の本文 9 行目に記載の文献名を Revision 4 に変更
③ P.30 の本文 9 行目に記載の文献名を「CRYPTREC Report 2016」に変更
P.30 の本文 9 行目に記載の「図3.1、図3.2」を「図3.3、図3.4」に変更
④ P.35 の脚注 23 の記載から「(draft)」を削除
⑤ P.45 の脚注 29 記載のサービスが無くなったのでこの記載を削除（または、他に代わるものがあれば記載）
併せて、脚注に該当する本文で記載の「提供されている」に該当するサービスがないなら「また」以降を削除することが望ましい。
⑥ EMET は 2018/7/31 までサポート延長されたものの Windows 10 への乗り換えが推奨されているので括弧内を修正することが望ましい
「EMET バージョン4.0 以降よりサポート」 → 「EMET は 2018/7/31 までサポートが受けられるが Windows 10 への移行が推奨されている」
⑦ サポートが有効な OS はすべて IE11 が最新であり、最新の IE のみサポートされることから、以下の記載に変更
Windows 7 SP1 ： 2020年1月14日
Windows 8.1 ： 2023年1月10日
Windows 10 ： 2025年10月14日
併せて、表 16 も以下のように変更（もしくは削除）
Internet Explorer 11 Windows 7 SP1 → 2020/1/14
Internet Explorer 11 Windows 8.1 → 2023/1/10
Internet Explorer 11 Windows 10 → 2025/10/14
Microsoft Edge Windows 10 → 2025/10/14

⑧ このサイトに掲載されている設定は IE10 までであり項番 25 のライフサイクルポリシーと矛盾するので、P.57 の 10 ～13 行目は削除することが望ましい
P.57 20 ～ 25 行目、および表は削除（IE11しかサポートしていないため）もしくは IE11 のみ残して Edge を加える
Edge は「コントロールパネル」「インターネットオプション」「詳細設定」で設定する（メニューからの設定は不可）
P.58 最上部の図がどのバージョンのものなのか不明なため判断できないが、我が Windows7 とは画面が異なる

⑨ 最新の 56.0.2 では「ﾂｰﾙ」「ｵﾌﾟｼｮﾝ」の証明書項目で一択（オンかオフ）に変更されている
併せて、画面キャプチャの差し替えが必要
（特に Firefox は頻繁に更新されるので画面キャプチャが必要かどうかの議論も必要…）
よって、以下のような修正が必要

「Firefox では、証明書マネージャが証明書の有効性をオンラインチェックできるようにする設定が提供されている。
デフォルトではチェックされた状態であり、特段の理由がない場合に変更することは推奨しない。」
Windows 版（56.0.2）
「ﾂｰﾙ」「ｵﾌﾟｼｮﾝ」→【ﾌﾟﾗｲﾊﾞｼｰとｾｷｭﾘﾃｨ】カテゴリ→「ｾｷｭﾘﾃｨ」ｸﾞﾙｰﾌﾟの『証明書』に
「OCSP レスポンダーサーバーに問い合わせて証明書の現在の正当性を確認する」
Linux 版（52.4.0）
「編集」「設定」→【詳細】カテゴリ→「証明書」タブ
「OCSP レスポンダに問い合わせてデジタル証明書の有効性をリアルタイムに確認する」

⑩ 8.1.2 で、対象を最新版のブラウザに限定しているので、本項目は v62 のみでよい
「Chrome 56 で、SHA-1を使った証明書のサポートを完全に打ち切った」
「Chrome 54 以降では、EnableSha1ForLocalAnchors ポリシーを設定できます。
これは、Chrome でサポートが廃止された後でも、ローカルにインストールされたトラスト アンカーに
チェーンされた証明書の使用を許可するためのものです。位置情報などのセキュアオリジンが必要な機能は、
動作は続けるものの、ページに "neutral, lacking security" である旨が表示されます。
2017 年 3 月に安定版チャンネルにリリースされる予定の Chrome 57 以降では、このポリシーが設定されていない場合、
ローカルにインストールされたルートへのチェーンを使用する SHA-1 証明書は信頼されなくなります。
なお、このポリシーが設定されていなくても、クライアントの認証をリクエストするウェブサイトには、SHA-1 クライアント証明書が提示されます。
このポリシーは、SHA-1 からの移行が間に合わない場合に猶予期間を与えることだけを意図したものです。
そのため、2019 年 1 月 1 日以降の最初の Chrome のリリースで削除される予定です。」
https://developers-jp.googleblog.com/2016/11/sha-1-certificates-in-chrome.html

⑪ 8.1.2 で、対象を最新版のブラウザに限定しているので、本項目は不要
また、以下のように順次、予定が前倒し実施されたので、過去の経過を記載することはあまり意味を持たない。
計画↓
「Firefox 36 以降廃止予定
Firefox 48 以降では、2016 年 1 月以降に発行された SHA-1 証明書は、手作業でインポートされたルート証明書を除き 受け入れられません
Firefox 53（2017 年 4 月公開）でこの期間条件がなくなり、公的認証局によって発行された SHA-1 証明書はすべて信頼できない接続エラー表示になる」
計画の変更↓
「2017 年 3 月公開の Firefox 52 で この変更を前倒しで行う」
計画の変更の変更↓
「2017 年 3 月 7 日の Firefox 52 最終リリースを待つことなく、2 月 24 日にリモートですべての Firefox ユーザーの SHA-1 対応を無効化しました。」
https://www.fxsitecompat.com/ja/docs/2016/sha-1-certificates-issued-by-public-ca-will-no-longer-be-accepted/

⑫ ここで引用するセキュリティアドバイザリは現存するものの、Windows 10、Windows Server 2016 が未記載。
この中の「推奨するアクション」に「Windows で SSL 3.0 を無効にする」という項目があるが、Windows Server 2016 実機を確認すると
このアクションを取らなければ SSL 3.0 は有効になっているようだが、このセキュリティアドバイザリには Windows Server 2016 が対象として
含まれていない以上、お墨付きの文書をポイントすることができない。
⑬ 文書の対象 OS はすべてサポートが終了したもの。
現存する OS の設定ではないので、記載自体が無意味。
「高セキュリティ型」「推奨セキュリティ型」…のレジストリ設定をそのまま適用しても問題が発生しないかの裏付けがとれない。
以下に、Windows 10（Windows Server 2016）の設定を発見したが、趣旨が合致しているか不明確。
How to deploy custom cipher suite ordering in Windows Se https://support.microsoft.com/en-us/help/4032720/how-to-deploy-custom-cipher-suite-ordering-in-windows-server-2016
以下の文書には Windows Server 2016 と明記されているので、これをネタに見直して記述（**背景色が黒のセルをクリック！**）
① AD FS の SSL または TLS プロトコルおよび暗号スイートを管 https://docs.microsoft.com/ja-jp/windows-server/identity/ad-fs/operations/manage-ssl-protocols-in-ad-fs
② TLS/SSL の設定（Vista、7、8、8.1、Server 2008、Server 20 https://msdn.microsoft.com/ja-jp/library/dn786418(v=ws.11).aspx

③　同上（英語版）　https://technet.microsoft.com/en-us/library/dn786418(v=ws.11).aspx
④　同上（英語版）に Windows Server 2016 が加わった記事（英語　https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings
④の情報とガイドを突き合わせた修正見直し案はこちらのリンクをクリック！？

⑭　Windows Server 2016 の画面の出方は微妙に違うので、必要に応じて画面キャプチャの差し替えが必要
また、暗号リストは見直しする必要があるだろう…
以下、Windows Server 2016 のグループポリシー内に定義されている Cipher Suite
(1) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
(2) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
(3) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
(4) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
(5) TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
(6) TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
(7) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
(8) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
(9) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
(10) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
(11) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
(12) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
(13) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
(14) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
(15) TLS_DHE_RSA_WITH_AES_256_CBC_SHA
(16) TLS_DHE_RSA_WITH_AES_128_CBC_SHA
(17) TLS_RSA_WITH_AES_256_GCM_SHA384
(18) TLS_RSA_WITH_AES_128_GCM_SHA256
(19) TLS_RSA_WITH_AES_256_CBC_SHA256
(20) TLS_RSA_WITH_AES_128_CBC_SHA256
(21) TLS_RSA_WITH_AES_256_CBC_SHA
(22) TLS_RSA_WITH_AES_128_CBC_SHA
(23) TLS_RSA_WITH_3DES_EDE_CBC_SHA
(24) TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
(25) TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
(26) TLS_DHE_DSS_WITH_AES_256_CBC_SHA
(27) TLS_DHE_DSS_WITH_AES_128_CBC_SHA
(28) TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
(29) TLS_RSA_WITH_RC4_128_SHA
(30) TLS_RSA_WITH_RC4_128_MD5
(31) TLS_RSA_WITH_NULL_SHA256
(32) TLS_RSA_WITH_NULL_SHA
(33) TLS_PSK_WITH_AES_256_GCM_SHA384
(34) TLS_PSK_WITH_AES_128_GCM_SHA256
(35) TLS_PSK_WITH_AES_256_CBC_SHA384
(36) TLS_PSK_WITH_AES_128_CBC_SHA256
(37) TLS_PSK_WITH_NULL_SHA384
(38) TLS_PSK_WITH_NULL_SHA256
以下、PDF 文書に記載されている内容（番号は、上記一覧の番号に対応）
●　高セキュリティ型の設定例（楕円曲線暗号あり）
(1) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
(2) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
●　推奨セキュリティ型の設定例（楕円曲線暗号あり）
(2) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
(8) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
(10) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
(12) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
(14) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
(20) TLS_RSA_WITH_AES_128_CBC_SHA256
(22) TLS_RSA_WITH_AES_128_CBC_SHA
(1) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
(7) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
(9) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
(11) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
(13) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
(19) TLS_RSA_WITH_AES_256_CBC_SHA256
(21) TLS_RSA_WITH_AES_256_CBC_SHA
●　セキュリティ例外型の設定例（楕円曲線暗号あり）
(2) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
(8) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
(10) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
(12) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
(14) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
(20) TLS_RSA_WITH_AES_128_CBC_SHA256
(22) TLS_RSA_WITH_AES_128_CBC_SHA
(1) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
(7) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
(9) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
(11) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
(13) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
(19) TLS_RSA_WITH_AES_256_CBC_SHA256
(21) TLS_RSA_WITH_AES_256_CBC_SHA

(29) TLS_RSA_WITH_RC4_128_SHA
(23) TLS_RSA_WITH_3DES_EDE_CBC_SHA

⑮ P.85 Appendix C 暗号スイート設定例
Apache の場合…　の記載に関して実機にて確認の結果、
「…VirtualHost中のSSLCipherSuiteの設定を以下のように追記…」
と書かれているものの実機（Ubuntu 16.04 32bit）では「VirtualHost の中」という文言が相応しくない。
/etc/apache2/mods-available/ssl.conf の <IfMidule mod_ssl.c> の中が正解。

⑯ Windows 10 Enterprise マシンを構築して確認すると、標準で Edge 実装であり IE は未実装
なので、IE の記述は Appendix に移行したほうが望ましい。
同時に、Firefox や Chrome の旧バージョンに関する記述も Appendix への移行が望ましい。

⑰ 7.2.5 Public Key Pinningの設定有効化の項目に、以下を追記

HPKP は Google のエンジニアがインターネット標準化団体の Internet Engineering Task Force（IETF）を通じて発表した標準規格だが、
今では悪影響もあると考えられており、Google Chrome 67 で HPKP のサポートを廃止する計画を明らかにした。
Chrome 67 の安定版がリリースされるのは、2018 年 5 月 29 日頃の見込み。
https://japan.cnet.com/article/35109624/

【参考】HPKP の仕組みについては以下
http://blog.livedoor.jp/k_urushima/archives/1811745.html

⑱ Appendix B ー B.2.4. Microsoft IISの場合　項の「各OSにおけるプロトコルバージョンのサポート状況」の表は修正する必要あり
見直し修正案はこちらのリンクをクリック！？