まとめ

暗号通信設定に関してSSL/TLS暗号設定ガイドラインと同様の目的を持つ以下の国内外の他機関が発行するSSL/TLSに関する文献を調査した。

- エストニア（ESTONIA）…4文書
- ドイツ（GERMANY）…1文書
- 韓国（大韓民国）…6文書
- イギリス（英）…6文書
- フランス（仏）…5文書
- カナダ（加）…5文書
- オーストラリア（豪）…3文書
- アメリカ（米）…2文書

同様に、以下の業界団体が発行するSSL/TLSに関する文献について調査した。

- ETSI…1文書
- CABF…1文書
- PCI…1文書
- OWASP…2文書
- OASIS…1文書
- HIPPA…4文書
- Mozilla…1文書

エストニア共和国

文書名	分類	セクション	規定内容		
			規定	差分	
ISKE カタログ Ver 8.03 発行者　Riigi infosüsteemi Amet（国家情報システム局） 発効日　2017年6月 対象者　電子政府に関連する政府組織	プロトコル	HT.72	SSL/TLS		TLS / SSL使用のパラメータ化
	暗号化ツール	HT.52	暗号装置の追加要件		MD2、MD4、MD5 の禁止 RIPEMD-160、SHA-1 の禁止 SHA-2ファミリ、RIPEMDより長いハッシュを推奨 10年以上使用　RSA：1536ビット以上 15年以上使用　RSA：4096ビット以上

参考文献等

ISKE kataloogid v8.03	https://iske.ria.ee/8_03/ISKE_kataloogid/8_Kataloog_H
Three-level IT baseline security system ISKE	https://www.ria.ee/en/iske-en.html
The system of security measures for information systems （2007年12月20日共和国政府規則252）	https://www.ria.ee/public/ISKE/Regulation-the-system-of-security-measures-for-information-systems-2007-12-20.pdf
IT-turbejuhend （2009年7月）	https://www.ria.ee/public/ISKE/Infoturbe_soovituste_juhend_v1.pdf

ドイツ連邦共和国

文書名	分類	セクション	規定内容		
			規定	差分	
IT Baseline Protection Manual 発行者　BSI（英語名：Federal Office for Information Security） 発効日　2013年9月 対象者　電子政府に関連する政府組織 企業に対しても適用が推奨	プロトコル	S 5.66	SSL		TLS 1.0以上またはSSL 3.0以上を使用する必要があり SSL 2.xは、中間者攻撃に対する保護機能を提供していないため、使用しない
			鍵長	すべき	少なくとも100ビット長
				それ以外	ECBモードで暗号化すべきではない。CBCまたはCFBモードを使用する必要あり。
		S 5.45	ブラウザ		HTTPS プロトコルを使用して暗号化された接続が使用されていることを確認する必要がある。
	暗号アルゴリズム	S 5.36	暗号アルゴリズム		S 3.23 参照 AES-128、AES-192、AES-256、SERPENTが含まれ、キー長は少なくとも128ビット RSA または楕円曲線に基づく暗号化手順

参考文献等

IT Baseline Protection Manual（2013年版）	https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html;jsessionid=CA82EA536006D8A1E57F900F1CAC18AF.2_cid369

大韓民国

文書名	分類	セクション	規定内容		
			規定	差分	
ICT Practices in korea 発行者　Ministry of Science and ICT（科学技術情報通信部） 発効日　2014/12/4 対象者　不明（国民向けらしい）		9	電子政府標準フレームワーク		公共部門に適用される開発枠組みの基準

暗号関連の技術情報は非公開

参考文献

ICT Practices in korea	http://www.msip.go.kr/dynamic/file/afieldfile/msse59/1325559/2014/12/18/ICT_English.pdf
eGovernment Standard Framework	https://www.egovframe.go.kr/uss/eng/index.do
ガイド類	http://www.kisa.or.kr/public/laws/laws3.jsp
国家と暗号の関わり方に関する海外調査報告書	https://www.ipa.go.jp/files/000013768.pdf#search=%27%E6%9A%97%E5%8F%B7+%E9%9F%93%E5%9B%BD+%E9%9D%9E%E5%85%AC%E9%96%8B%27
各国政府の暗号政策動向	http://c-faculty.chuo-u.ac.jp/~tsujii/pdf/150620kanda.pdf#search=%27%E6%9A%97%E5%8F%B7+%E9%9F%93%E5%9B%BD+%E9%9D%9E%E5%85%AC%E9%96%8B%27
各国における情報セキュリティに対する取り組みに関する調査（2009年3月 株式会社三菱総合研究所）	https://www.nisc.go.jp/inquiry/pdf/product_service.pdf

グレートブリテン及び北アイルランド連合王国

文書名	分類	セクション	規定内容	
			規定	差分
Using TLS to protect data 発行者　NCSC 発効日　2016/10/7 対象者　英国政府 地方自治体 国家インフラ（クラウドサービスベンダーを指していると思われる） サプライヤー	プロトコル 暗号アルゴリズム ↑ 鍵 証明書	Deploying TLS for ↑ └ 章のタイトル	鍵長	2048ビット
			署名アルゴリズム	SHA256
			SSL	SSLv3 の禁止
			TLS	TLS 1.0 の非推奨 TLS 1.1、1.2 の推奨（1.1 は必要最低限に限る）
			暗号スイート	以下の暗号スイートは非推奨
				AEAD の推奨
				ADH は認証を未提供
				NULL 暗号は暗号化を未提供
				Export 暗号スイートは安全ではない
				40、56ビットの暗号スイートは簡単に破られる
				RC4 は安全ではない
				3DES は弱い
				以下の暗号スイートを推奨
				TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
				TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
				TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
				TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
				TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
				TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
				TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
				TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
				TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
				TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
				TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
				TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
				TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
				TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
				TLS_DHE_RSA_WITH_AES_128_CBC_SHA
				TLS_DHE_RSA_WITH_AES_256_CBC_SHA
				TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
				TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
		Recommended crypt ↑ └ 章のタイトル	TLS 暗号化プロファイル （推奨値）	TLSのスイートBプロファイルの要約

Protocol	TLS v1.2
Encryption	AES with 128-bit key in GCM mode
Pseudo-random function	TLS PRF (with SHA-256)
Authentication	ECDSA-256 with SHA-256 on P-256 curve
Key exchange	ECDH using P-256 curve
Algorithm type	Description

TLS の基礎プロファイル

Protocol	TLS v1.2
Encryption	AES with 128-bit key in CBC mode
Pseudo-random function	TLS PRF (with SHA-256)
Authentication	X.509 certificates with RSA signatures (2048 bits) and SHA-256
Key exchange	DH Group 14 (2048-bit MODP Group)
Integrity	SHA-256
Algorithm type	Description

参考文献

Using TLS to protect data	https://www.ncsc.gov.uk/guidance/tls-external-facing-services
Secure configuration recommendations でリンクするサイト	https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices
〃	https://support.google.com/webmasters/answer/6073543
〃	https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility
NSCS ガイダンス	https://www.ncsc.gov.uk/guidance
End User Devices Security and Configuration Guidance	https://www.ncsc.gov.uk/guidance/end-user-device-security

フランス共和国

文書名	分類	セクション	規定内容		
			規定	差分	
Security Recommendations for TLS	プロトコル	2.1	SSL/TLS	R3	TLS 1.2のみを使用してください
				R4	SSL v2 の使用禁止
発行者 ANSSI （国家情報通信システムセキュリティ庁）				R3-	TLS 1.2を優先し、TLS 1.1とTLS 1.0は容認
発効日 FR Version 1.1: 2016/8/19				R4	SSL v2 の使用禁止
EN Version 1.1: 2017/1/24				R3--	TLS 1.2を優先し、TLS 1.1、TLS 1.0、およびSSLv3は容認
対象者 あらゆる規模の組織の管理者				R4	SSL v2 の使用禁止
ソリューションの開発者		2.2	鍵交換	R5	鍵交換中にサーバーを認証します。
関連するすべてのユーザ				R6	常にPFS対応の鍵交換を行います。
				R6-	PFS対応鍵交換を優先します。
				R7	ECDHE鍵交換を実行します。
				R7-	DHE鍵交換を実行します。
			アルゴリズム	R8	AES暗号化を使用します。
				R8-	CamelliaまたはARIA暗号化を使用します。
				R8--	AESを賞賛し、リフレッシュメントで3DESに耐えます。
			認証コード	R9	SHA-2でHMACを構築する
				R9-	SHA-2でHMACを優先し、SHA-1でHMAC を容認
			暗号化モード	R10	強力な暗号化モードを使用する
				R10-	encrypt_then_macなしでCBCモードを使用する
		Appendix A		推奨	以下、推奨する暗号化スイート

TLS 1.2 suites recommended for servers with an ECDSA key

Value	Cipher suite
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC0AD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM
0xC0AC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS 1.2 suites recommended for servers with an RSA key

Value	Cipher suite
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Table A.3: Recommended suites for use with Camellia

Value	Cipher suite
0xC087	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
0xC086	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
0xC073	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
0xC072	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
0xC08B	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
0xC08A	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
0xC077	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
0xC076	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256

Table A.4: Recommended suites for use with ARIA

Value	Cipher suite
0xC05D	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
0xC05C	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
0xC061	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
0xC060	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
0xC049	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384
0xC048	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256
0xC04D	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384
0xC04C	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256

Finally, for deployments with pre-shared keys, the recommended suites are mentioned in table A.5.
Table A.5: Recommended suites for use with a PSK

Value	Cipher suite
0xC038	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
0xC037	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

<table>
<tr><td></td><td></td><td></td><td></td><td>緩和</td><td>Relaxed Suites for TLS 1.2

TLS 1.2 suites tolerated in the absence of ECC support
<table><tr><th>Value</th><th>Cipher suite</th></tr><tr><td>0x009F</td><td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td></tr><tr><td>0x009E</td><td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td></tr><tr><td>0xC09F</td><td>TLS_DHE_RSA_WITH_AES_256_CCM</td></tr><tr><td>0xC09E</td><td>TLS_DHE_RSA_WITH_AES_128_CCM</td></tr><tr><td>0x006B</td><td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td></tr><tr><td>0x0067</td><td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</td></tr></table>
TLS 1.2 suites tolerated in the absence of DH support
<table><tr><th>Value</th><th>Cipher suite</th></tr><tr><td>0x009D</td><td>TLS_RSA_WITH_AES_256_GCM_SHA384</td></tr><tr><td>0x009C</td><td>TLS_RSA_WITH_AES_128_GCM_SHA256</td></tr><tr><td>0xC09D</td><td>TLS_RSA_WITH_AES_256_CCM</td></tr><tr><td>0xC09C</td><td>TLS_RSA_WITH_AES_128_CCM</td></tr><tr><td>0x003D</td><td>TLS_RSA_WITH_AES_256_CBC_SHA256</td></tr><tr><td>0x003C</td><td>TLS_RSA_WITH_AES_128_CBC_SHA256</td></tr></table>
TLS suites tolerated for password authentication
<table><tr><th>Value</th><th>Cipher suite</th></tr><tr><td>0xC021</td><td>TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>0xC01E</td><td>TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA</td></tr></table>
Relaxed Suites for TLS 1.0

Suites tolerated for TLS 1.0
<table><tr><th>Value</th><th>Cipher suite</th></tr><tr><td>0xC00A</td><td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>0xC009</td><td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>0xC014</td><td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>0xC013</td><td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td></tr></table>
Suites barely tolerated for TLS 1.0
<table><tr><th>Value</th><th>Cipher suite</th></tr><tr><td>0x0039</td><td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>0x0033</td><td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>0xC008</td><td>TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA</td></tr><tr><td>0xC012</td><td>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA</td></tr><tr><td>0x0016</td><td>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</td></tr><tr><td>0x0035</td><td>TLS_RSA_WITH_AES_256_CBC_SHA</td></tr><tr><td>0x002F</td><td>TLS_RSA_WITH_AES_128_CBC_SHA</td></tr><tr><td>0x000A</td><td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td></tr></table></td></tr>
<tr><td></td><td>証明書</td><td>3</td><td>Basic Fields</td><td>R21</td><td>SHA-2で署名</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R22</td><td>3年の期間有効な証明書を所持</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R23</td><td>十分な大きさのキーを使用</td></tr>
<tr><td></td><td></td><td></td><td>Extensions</td><td>R24</td><td>適切な KeyUsage</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R25</td><td>適切な ExtendedKeyUsage</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R26</td><td>適切な（サーバー側の）SubjectAlternativeName を指定</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R27</td><td>各証明書を1つの TLS 終端ポイントだけ保持</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R28</td><td>CAによって定義されたSKIに対応するAKIを負担</td></tr>
<tr><td></td><td></td><td></td><td></td><td>R29</td><td>失効情報を提供</td></tr>
</table>

【注意】 Rx, Rx-, Rx-- 標記：「Rx：推奨事項（x は番号）」、「Rx-：推奨事項が不可能な場合」、「Rx--：最低の信頼レベル」

参考文献

Security Recommendations for TLS				https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf
RÉFÉRENTIEL GÉNÉRAL DE SÉCURITÉ	version 2.0			https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf
Référentiel Général de Sécurité	version 2.0	Annexe B1	Mécanismes cryptographiques	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
Référentiel Général de Sécurité	version 2.0	Annexe B2	Gestion des clés cryptographiques	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf
Référentiel Général de Sécurité	version 1.0	Annexe B3	Authentification	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf

カナダ

文書名	分類	セクション	規定内容		
			規定	差分	
Guidance on Securely Configuring Network Protocols 発行者　CSE（カナダ政府の通信セキュリティ機関） 発効日　2016/8/2 対象者　不明（政府およびベンダ）	公開鍵	2	Public Key Infrastructure		SHA-1を公開鍵証明書の電子署名の生成または検証に使用すべきではない NIST SP 800-57パート3 Rev1 Section 2 にしたがうことを推奨
	プロトコル	3	SSL/TLS		TLS 1.2 の使用を推奨 （他のバージョンの TLS と全ての SSL の使用は非推奨） NIST SP 800-52 Rev1の section 3.9 および 4.9 にしたがうことを推奨
		3.1	TLS Cipher Suites		次の TLS 暗号スイートは、ITSP.40.111 で提供される暗号ガイダンスを満たす TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_CCM TLS_DHE_RSA_WITH_AES_256_CCM TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CCM TLS_RSA_WITH_AES_256_CCM TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	暗号アルゴリズム	5.1.1	SSH		CBCモードはSSHで使用しない 以下の暗号アルゴリズムを推奨 aes128-ctr (RFC 4344 [34]) aes192-ctr (RFC 4344 [34]) aes256-ctr (RFC 4344 [34]) 3des-ctr (RFC 4344 [34]) cast128-ctr (RFC 4344 [34]) AEAD_AES_128_GCM (RFC 5647 [35]) AEAD_AES_256_GCM (RFC 5647 [35])

参考文献

Guidance on Securely Configuring Network Protocols	https://www.cse-cst.gc.ca/en/node/1830/html/26507
Cryptography	https://www.cse-cst.gc.ca/en/publication/list/Cryptography
Government of Canada Information Technology Strategic Plan 2016-2020	https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/information-technology-strategy/strategic-plan-2016-2020.html#toc8
CMVP	https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program
CMVP Standards	https://www.cse-cst.gc.ca/en/page/standards

オーストラリア連邦

文書名	分類	セクション	規定内容		
			規定	差分	
2017 Australian Government Information Security 発行者　ASD（オーストラリア信号局） 発効日　2017/11/23 更新 対象者　不明（政府およびベンダ）	暗号アルゴリズム	P.242 以降	暗号アルゴリズム		承認された非対称/公開鍵アルゴリズムは
				高優先度	ECDH ECDSA
				低優先度	DH DSA
					RSA 承認されたハッシュアルゴリズム SHA-224 SHA-256 SHA-384 SHA-512 承認された対称暗号化アルゴリズム AES 128 AES 192 AES 256 3DES
			デジタル署名	すべき	DSA 2048ビット以上
				必須	DSA 1024ビット以上
			スイートB	機密	AES 256 SHA-384 NIST P-384 NIST P-384
				機密 （やや下）	AES 128 SHA-256 NIST P-256 NIST P-256
				または 高機密	CNSSAM recommendation AES 256 bit key CNSSAM recommendation SHA-384 CNSSAM recommendation NIST P-384 or RSA 3072-bit or larger CNSSAM recommendation DH 3072-bit or larger or NIST P-384 or RSA 3072-bit or larger.

参考文献

Australian Government Information Security Manual	https://www.asd.gov.au/infosec/ism/
2017 Australian Government Information Security Manual (Controls)	https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf#search=%27Australian++Government++Information++and++Commu+nications++Technology+Security++Manual%27
Protective Security Policy Framework Document Map - Version 1.4 - amended June 2016	https://www.protectivesecurity.gov.au/resources/Documents/Protective-Security-Policy-Framework-Map.pdf

アメリカ合衆国

文書名	分類	セクション	規定内容	
			規定	差分
SP 800-52 Rev.1 発行者　NIST 発効日　2014年4月 対象者　不明（政府およびベンダ）	プロトコル	4.1	プロトコルバージョン	TLS 1.1 をサポートするよう構成し、TLS 1.2 をサポートするよう構成すべき 政府機関は、2015年1月1日までにTLS 1.2をサポートする移行計画を策定する予定です。
		付録C	TLS Cipher Suite	Table C-1: Pre-shared Key Cipher Suites

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_PSK_WITH_3DES_EDE_CBC_SHA	PSK	3DES_EDE_CBC	SHA-1	Per RFC
TLS_PSK_WITH_AES_128_CBC_SHA	PSK	AES_128_CBC	SHA-1	Per RFC
TLS_PSK_WITH_AES_256_CBC_SHA	PSK	AES_256_CBC	SHA-1	Per RFC
TLS_PSK_WITH_AES_128_GCM_SHA256	PSK	AES_128_GCM	N/A	SHA-256
TLS_PSK_WITH_AES_256_GCM_SHA384	PSK	AES_256_GCM	N/A	SHA-384
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA	DHE_PSK	3DES_EDE_CBC	SHA-1	Per RFC
TLS_DHE_PSK_WITH_AES_128_CBC_SHA	DHE_PSK	AES_128_CBC	SHA-1	Per RFC
TLS_DHE_PSK_WITH_AES_256_CBC_SHA	DHE_PSK	AES_256_CBC	SHA-1	Per RFC
TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	DHE_PSK	AES_128_GCM	N/A	SHA-256
TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	DHE_PSK	AES_256_GCM	N/A	SHA-384
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA	RSA_PSK	3DES_EDE_CBC	SHA-1	Per RFC
TLS_RSA_PSK_WITH_AES_128_CBC_SHA	RSA_PSK	AES_128_CBC	SHA-1	Per RFC
TLS_RSA_PSK_WITH_AES_256_CBC_SHA	RSA_PSK	AES_256_CBC	SHA-1	Per RFC
TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	RSA_PSK	AES_128_GCM	N/A	SHA-256
TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	RSA_PSK	AES_256_GCM	N/A	SHA-384
TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA	ECDHE_PSK	3DES_EDE_CBC	SHA-1	Per RFC
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	ECDHE_PSK	AES_128_CBC	SHA-1	Per RFC
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	ECDHE_PSK	AES_256_CBC	SHA-1	Per RFC
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	ECDHE_PSK	AES_128_CBC	SHA-256	SHA-256
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	ECDHE_PSK	AES_256_CBC	SHA-384	SHA-384

3.3.1

Table 3-2: Cipher Suites for RSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES_EDE_CBC	SHA-1	Per RFC
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	AES_128_CBC	SHA-1	Per RFC
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	AES_256_CBC	SHA-1	Per RFC
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE	3DES_EDE_CBC	SHA-1	Per RFC
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE	AES_128_CBC	SHA-1	Per RFC
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE	AES_256_CBC	SHA-1	Per RFC

Table 3-4: Cipher Suites for ECDSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE	3DES_EDE_CBC	SHA-1	Per RFC
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE	AES_128_CBC	SHA-1	Per RFC
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE	AES_256_CBC	SHA-1	Per RFC

Table 3-6: Cipher Suites for DSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE	3DES_EDE_CBC	SHA-1	Per RFC
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE	AES_128_CBC	SHA-1	Per RFC
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE	AES_256_CBC	SHA-1	Per RFC

Table 3-8: Cipher Suites for DH Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	DH	3DES_EDE_CBC	SHA-1	Per RFC
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH	AES_128_CBC	SHA-1	Per RFC
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH	AES_256_CBC	SHA-1	Per RFC

Table 3-10: Cipher Suites for ECDH Server Certificate

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH	3DES_EDE_CBC	SHA-1	Per RFC
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH	AES_128_CBC	SHA-1	Per RFC
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH	AES_256_CBC	SHA-1	Per RFC

Table 3-3: Additional TLS 1.2 Cipher Suites for RSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	AES_128_GCM	N/A	SHA-256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	AES_256_GCM	N/A	SHA-384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	AES_128_CBC	N/A	SHA-256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	AES_128_GCM	N/A	SHA-256
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	AES_128_CBC	SHA-256	SHA-256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	AES_256_CBC	SHA-256	SHA-256
TLS_RSA_WITH_AES_128_CCM	RSA	AES_128_CCM	N/A	SHA-256
TLS_RSA_WITH_AES_256_CCM	RSA	AES_256_CCM	N/A	SHA-256

Table 3-5: Additional TLS 1.2 Cipher Suites for ECDSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	AES_128_CBC	SHA-256	SHA-256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	AES_128_GCM	N/A	SHA-256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE	AES_256_GCM	N/A	SHA-384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	AES_256_CBC	SHA-384	SHA-384

Table 3-7: Additional TLS 1.2 Cipher Suites for DSA Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE	AES_128_CBC	SHA-256	SHA-256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE	AES_256_CBC	SHA-256	SHA-256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE	AES_128_GCM	N/A	SHA-256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE	AES_256_GCM	N/A	SHA-384

Table 3-9: Additional TLS 1.2 Cipher Suites for DH Server Certificates

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	DH	AES_128_CBC	SHA-256	SHA-256
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	DH	AES_256_CBC	SHA-256	SHA-256
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	DH	AES_128_GCM	N/A	SHA-256
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	DH	AES_256_GCM	N/A	SHA-384

Table 3-11: Additional TLS 1.2 Cipher Suites for ECDH Server Certificate

Cipher Suite Name	Key Exchange	Encryption	Hash function for HMAC	Hash Function for PRF
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH	AES_128_CBC	SHA-256	SHA-256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH	AES_256_CBC	SHA-384	SHA-384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH	AES_128_GCM	N/A	SHA-256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH	AES_256_GCM	N/A	SHA-384

SP 800-131A Rev. 1 発行者　NIST 発効日　2015年11月 対象者　不明（政府およびベンダ）	証明書	3	デジタル署名	Table 2: Approval Status of Algorithms Used for Digital Signature Generation and Verification **Digital Signature Process** / **Use** Digital Signature Generation: < 112 bits of security strength: DSA: len(p) < 2048 OR len(q) < 224; RSA: len(n) < 2048; ECDSA: len(n) < 224 — Disallowed Digital Signature Generation: ≥ 112 bits of security strength: DSA: len(p) ≥ 2048 AND len(q) ≥ 224; RSA: len(n) ≥ 2048; ECDSA: len(n) ≥ 224 — Acceptable Digital Signature Verification: < 112 bits of security strength: DSA [*3]: ((512 ≤ len(p) < 2048) OR (160 ≤ len(q) < 224)); RSA: 1024 ≤ len(n) < 2048; ECDSA: 160 ≤ len(n) < 224 — Legacy-use Digital Signature Verification: ≥ 112 bits of security strength: DSA: len(p) ≥ 2048 AND len(q) ≥ 224; RSA: len(n) ≥ 2048; ECDSA: len(n) ≥ 224 — Acceptable [*3]：The lower bounds for len(p) and len(q) are those that were specified in [FIPS 186-2]. len（p）とlen（q）の下限は、[FIPS 186-2]で指定されたものです。
	暗号アルゴリズム	9	ハッシュ関数	Table 9: Approval Status of Hash Functions **Hash Function** / **Use** SHA-1: Digital signature generation — Disallowed except where specifically allowed by NIST protocol-specific guidance. SHA-1: Digital signature verification — Legacy-use SHA-1: Non-digital signature applications — Acceptable SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256): Acceptable for all hash function applications SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512): Acceptable for all hash function applications

参考文献

SP 800-131A　https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final

SP 800-52 Rev.1　https://csrc.nist.gov/publications/detail/sp/800-52/rev-1/final

以下、業界団体等

ETSI 欧州電気通信標準化協会

文書名	分類	セクション	規定内容	
			規定	差分
ETSI TS 118 103 V2.4.1 (2016-09) oneM2M; Security solutions (oneM2M TS-0003 ver 発行者　ETSI 発効日　2016年9月 対象者　不明（運用者、開発者）	プロトコル	10.2.1	TLS	TLS v1.2 を使用しなければならない
	暗号スイート	10.2.2	暗号スイート	TLS-PSK-Based Security Frameworks TLS 実装　TLS_PSK_WITH_AES_128_CBC_SHA256 DTLS実装　TLS_PSK_WITH_AES_128_CCM_8
		10.2.3		Certificate-Based Security Frameworks TLS 実装　TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 DTLS実装　TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
				【参考】：赤字は、全ての国に記載なし 青字は、米（P451）、英（P87）、仏（R157）、加（Q273）に記載あり。
ETSI TS 133 320 V9.7.0 (2013-02) Universal Mobile Telecommunications System (UMT 発行者　ETSI 発効日　2013年2月 対象者　不明（運用者、開発者）	プロトコル	8.3.4	TLS	SSL 3.0 は使用しないでください TLS 1.1 はサポートされなければならない TLS 1.2 はサポートする必要あり
	暗号スイート		暗号スイート	RSA_WITH_AES_128_CBC_SHA のサポートは必須 TLS 1.2 に列挙されたTLS暗号スイートのみが使用される RC4 の暗号スイートは使用してはならない RSA_WITH_RC4_128_SHA のサポートは必須ではない

ここで出版される文書は「ガイドライン」ではなく「標準」

参考文献

文献の検索サイト　http://www.etsi.org/standards

CABF CA/Browser Forum

文書名	分類	セクション	規定内容	
			規定	差分
この団体は、証明書の管理、各種手続き、監査、云々、技術面ではないことを規定しているようであり、暗号スイートのガイドライン的な記述の文書は見つからない、				

PCI DSS （PCI Security Standards Council）

文書名	分類	セクション	規定内容	
			規定	差分
SSL および初期の TLS はセキュリティ制御としてこれらの要件を満たすために使用すべきではありません。				

Mozilla

文書名	分類	セクション	規定内容			
			規定	差分		
Security/Server Side TLS 発行日　2018年1月17（最終更新日） 対象者　サーバでTLSを構築する運用者	暗号スイート	3.6.3	暗号スイート	推奨	0xC0, 0x2C	ECDHE-ECDSA-AES256-GCM-SHA384
					0xC0, 0x30	ECDHE-RSA-AES256-GCM-SHA384
					0xCC, 0x14	ECDHE-ECDSA-CHACHA20-POLY1305
					0xCC, 0x13	ECDHE-RSA-CHACHA20-POLY1305
					0xC0, 0x2B	ECDHE-ECDSA-AES128-GCM-SHA256
					0xC0, 0x2F	ECDHE-RSA-AES128-GCM-SHA256
					0xC0, 0x24	ECDHE-ECDSA-AES256-SHA384
					0xC0, 0x28	ECDHE-RSA-AES256-SHA384
					0xC0, 0x23	ECDHE-ECDSA-AES128-SHA256
					0xC0, 0x27	ECDHE-RSA-AES128-SHA256
				互換性維持（デフォルト）	0xCC, 0x14	ECDHE-ECDSA-CHACHA20-POLY1305
					0xCC, 0x13	ECDHE-RSA-CHACHA20-POLY1305
					0xC0, 0x2B	ECDHE-ECDSA-AES128-GCM-SHA256
					0xC0, 0x2F	ECDHE-RSA-AES128-GCM-SHA256
					0xC0, 0x2C	ECDHE-ECDSA-AES256-GCM-SHA384
					0xC0, 0x30	ECDHE-RSA-AES256-GCM-SHA384
					0x00, 0x9E	DHE-RSA-AES128-GCM-SHA256
					0x00, 0x9F	DHE-RSA-AES256-GCM-SHA384
					0xC0, 0x23	ECDHE-ECDSA-AES128-SHA256
					0xC0, 0x27	ECDHE-RSA-AES128-SHA256
					0xC0, 0x09	ECDHE-ECDSA-AES128-SHA
					0xC0, 0x28	ECDHE-RSA-AES256-SHA384
					0xC0, 0x13	ECDHE-RSA-AES128-SHA
					0xC0, 0x24	ECDHE-ECDSA-AES256-SHA384
					0xC0, 0x0A	ECDHE-ECDSA-AES256-SHA
					0xC0, 0x14	ECDHE-RSA-AES256-SHA
					0x00, 0x67	DHE-RSA-AES128-SHA256
					0x00, 0x33	DHE-RSA-AES128-SHA
					0x00, 0x6B	DHE-RSA-AES256-SHA256
					0x00, 0x39	DHE-RSA-AES256-SHA
					0xC0, 0x08	ECDHE-ECDSA-DES-CBC3-SHA
					0xC0, 0x12	ECDHE-RSA-DES-CBC3-SHA
					0x00, 0x16	EDH-RSA-DES-CBC3-SHA
					0x00, 0x9C	AES128-GCM-SHA256
					0x00, 0x9D	AES256-GCM-SHA384
					0x00, 0x3C	AES128-SHA256
					0x00, 0x3D	AES256-SHA256
					0x00, 0x2F	AES128-SHA
					0x00, 0x35	AES256-SHA
					0x00, 0x0A	DES-CBC3-SHA

				下位互換性	0xCC,0x14　ECDHE-ECDSA-CHACHA20-POLY1305 0xCC,0x13　ECDHE-RSA-CHACHA20-POLY1305 0xC0,0x2F　ECDHE-RSA-AES128-GCM-SHA256 0xC0,0x2B　ECDHE-ECDSA-AES128-GCM-SHA256 0xC0,0x30　ECDHE-RSA-AES256-GCM-SHA384 0xC0,0x2C　ECDHE-ECDSA-AES256-GCM-SHA384 0x00,0x9E　DHE-RSA-AES128-GCM-SHA256 0x00,0xA2　DHE-DSS-AES128-GCM-SHA256 0x00,0xA3　DHE-DSS-AES256-GCM-SHA384 0x00,0x9F　DHE-RSA-AES256-GCM-SHA384 0xC0,0x27　ECDHE-RSA-AES128-SHA256 0xC0,0x23　ECDHE-ECDSA-AES128-SHA256 0xC0,0x13　ECDHE-RSA-AES128-SHA 0xC0,0x09　ECDHE-ECDSA-AES128-SHA 0xC0,0x28　ECDHE-RSA-AES256-SHA384 0xC0,0x24　ECDHE-ECDSA-AES256-SHA384 0xC0,0x14　ECDHE-RSA-AES256-SHA 0xC0,0x0A　ECDHE-ECDSA-AES256-SHA 0x00,0x67　DHE-RSA-AES128-SHA256 0x00,0x33　DHE-RSA-AES128-SHA 0x00,0x40　DHE-DSS-AES128-SHA256 0x00,0x6B　DHE-RSA-AES256-SHA256 0x00,0x38　DHE-DSS-AES256-SHA 0x00,0x39　DHE-RSA-AES256-SHA 0xC0,0x12　ECDHE-RSA-DES-CBC3-SHA 0xC0,0x08　ECDHE-ECDSA-DES-CBC3-SHA 0x00,0x16　EDH-RSA-DES-CBC3-SHA 0x00,0x9C　AES128-GCM-SHA256 0x00,0x9D　AES256-GCM-SHA384 0x00,0x3C　AES128-SHA256 0x00,0x3D　AES256-SHA256 0x00,0x2F　AES128-SHA 0x00,0x35　AES256-SHA 0x00,0x6A　DHE-DSS-AES256-SHA256 0x00,0x32　DHE-DSS-AES128-SHA 0x00,0x0A　DES-CBC3-SHA 0x00,0x9A　DHE-RSA-SEED-SHA 0x00,0x99　DHE-DSS-SEED-SHA 0xCC,0x15　DHE-RSA-CHACHA20-POLY1305 0xC0,0x77　ECDHE-RSA-CAMELLIA256-SHA384 0xC0,0x73　ECDHE-ECDSA-CAMELLIA256-SHA384 0x00,0xC4　DHE-RSA-CAMELLIA256-SHA256 0x00,0xC3　DHE-DSS-CAMELLIA256-SHA256 0x00,0x88　DHE-RSA-CAMELLIA256-SHA 0x00,0x87　DHE-DSS-CAMELLIA256-SHA 0x00,0xC0　CAMELLIA256-SHA256 0x00,0x84　CAMELLIA256-SHA 0xC0,0x76　ECDHE-RSA-CAMELLIA128-SHA256 0xC0,0x72　ECDHE-ECDSA-CAMELLIA128-SHA256 0x00,0xBE　DHE-RSA-CAMELLIA128-SHA256 0x00,0xBD　DHE-DSS-CAMELLIA128-SHA256 0x00,0x45　DHE-RSA-CAMELLIA128-SHA 0x00,0x44　DHE-DSS-CAMELLIA128-SHA 0x00,0xBA　CAMELLIA128-SHA256 0x00,0x41　CAMELLIA128-SHA 0x00,0x96　SEED-SHA
			プロトコルバージョン	推奨	TLSv1.2
				互換性維持（デフォルト）	TLSv1.2, TLSv1.1, TLSv1
				下位互換性	TLSv1.2, TLSv1.1, TLSv1, SSLv3
			楕円曲線	推奨	prime256v1, secp384r1, secp521r1
				互換性維持（デフォルト）	prime256v1, secp384r1, secp521r1
				下位互換性	prime256v1, secp384r1, secp521r1
			証明書の種類	推奨	ECDSA
				互換性維持（デフォルト）	RSA
				下位互換性	RSA
			証明書の楕円曲線	推奨	prime256v1, secp384r1, secp521r1
				互換性維持（デフォルト）	'None
				下位互換性	'None
			証明書の署名	推奨	sha256WithRSAEncryption, ecdsa-with-SHA256, ecdsa-with-SHA384, ecdsa-with-SHA512
				互換性維持（デフォルト）	sha256WithRSAEncryption
				下位互換性	sha256WithRSAEncryption
			RSAの鍵長	推奨	2048 (if not ecdsa)
				互換性維持（デフォルト）	2048
				下位互換性	2048
			DHの鍵長	推奨	2048 (if not ecdsa)
				互換性維持（デフォルト）	2048
				下位互換性	1024
			ECDHの鍵長	推奨	256
				互換性維持（デフォルト）	256
				下位互換性	256

参考文献

Security/Server Side TLS　https://wiki.mozilla.org/Security/Server_Side_TLS