TLS暗号設定ガイドラインチェックリスト

2020.07.07版

【チェックリストの使い方】
本チェックリストは、選択した設定基準に対応した要求設定を実施したことを確認するためのチェックリストである

○ 選択した設定基準に応じたチェックリストのチェックシートを下部の「タグ」から選択する
○ 当該チェックシートに記載のチェック項目全てについて参照章の記載を参考に設定内容を確認する
○ 「要求設定確認」は選択したチェックシートを利用してよいかの確認項目であり、「該当」にチェックが入る場合に限り、当該チェックシートを利用してよい
○ 「遵守項目」については要求設定に合致していることを確認して「済」にチェックが入ることが必要である
○ 「遵守項目」以外については記載内容を確認し、設定の実態に即して適切なほうのチェックボックスにチェックを入れる

＜チェックリストの例＞

【高セキュリティ型チェックリスト】

選択した設定基準に対応したチェックリストのチェックシートを用いる

要求設定が満たされていることを確認したら「済」にチェックを入れる

要求設定の詳細な内容が記載されている章番号

選択したチェックシートを利用してよいかの確認項目であり、「該当」にチェックが入る場合に限り利用してよい

「遵守項目」は要求設定に合致していることを確認して「済」にチェックが入ることが必要である

「遵守項目」以外については記載内容を確認し、設定の実態に即して適切なほうのチェックボックスにチェックを入れる

	チェック項目	参照章		
①要求設定確認	①-1)【遵守項目】高セキュリティ型の設定基準の環境であるか	3.1節	□該	
②プロトコルバージョン設定	[illegible]たか	5.1節	□済	
	[illegible]たか。ただし、TLS1.2を明確に利用[illegible]をチェックする	5.1節	□済	□設定せず
	②-3)【遵守項目】SSL2.0からTLS1.1までを設定無効（利用不可）にしたか	5.1節	□済	
③サーバ証明書設定	③-1)【遵守項目】サーバの公開鍵情報（Subject Public Key Info）のSubject Public Key [illegible]orithmと鍵長の組合せが以下のいずれかを満たしているか ・ RSAで鍵長は ・ 楕円曲線暗号	5.2節	□済	
	③-2)【遵守項[illegible]Signature Algorithm）と鍵長の組合せが以下のいずれかを満たしているか ・ RSA署名とSHA-256以上の組合せで鍵長2048ビット以上 ・ ECDSAとSHA-256以上の組合せで鍵長256ビット（NIST P-256）以上	5.2節	□済	
	③-3)【遵守項目】サーバ証明書の発行・更新を行う際に、自ら公開鍵と秘密鍵の鍵ペアを生成する場合には、新たな公開鍵と秘密鍵の鍵ペアを生成しているか	5.2節	□済	
	③-4)【遵守項目】上記③-3)についての指示を仕様書や運用手順書等に明記したか	5.2節	□済	
	③-5)【遵守項目】 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	5.2節	□済	
④暗号スイート設定	④-1)【遵守項目】表21記載の暗号アルゴリズムを全てを設定無効（利用不可）にしたか	5.3節	□済	
	④-2) ECDHEを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-2-1のチェック不要）		□設定する	□設定せず
	④-2-1)【遵守項目】ECDHEの鍵長を256ビ[illegible]		□済	
	④-3) DHEを利用する暗号スイートを設定す[illegible] 設定しない場合は「設定せず」をチェックす		設定する	□設定せず
	④-3-1)【遵守項目】DHEの鍵長を2048ビット以上に設定したか	[illegible]節	□済	
	④-4)【推奨項目】表22記載の暗号アルゴリズムを組み合わせた暗号スイートのみで設定しているか。 設定しない／できない場合は「設定せず」をチェックする	5.3節	□済	□設定せず
	④-5) 暗号スイートの優先順位が設定できるか。 設定できない場合は「設定不可」をチェックする（④-5-1のチェック不要）		□設定可	□設定不可
	④-5-1)【推奨項目】表24記載の暗号スイートの優先順位で設定したか。優先順位どおりに設定できない／しない場合は「設定せず」をチェックする	5.3節	□済	□設定せず
⑤附録	⑤) Appendix C：暗号スイートの設定例の最新版のドキュメントを参照して設定したか。参照していない場合には「参照せず」をチェックする	Appendix C	□参照済	□参照せず

【推奨セキュリティ型チェックリスト】　　2020.07.07版

チェック項目		参照章		
①要求設定確認	チェック項目なし			
②プロトコルバージョン設定	②-1）【遵守項目】TLS1.2を設定有効としたか	4.1節	□済	
	②-2）【遵守項目】SSL2.0からTLS1.1までを設定無効（利用不可）にしたか	4.1節	□済	
	②-3）TLS1.3が実装されているか。 実装されていない場合は「未実装」をチェックする（②-3-1のチェック不要）		□実装済	□未実装
	②-3-1）【推奨項目】TLS1.3について設定を有効にしたか。ただし、 TLS1.3を明確に利用しない場合は「設定せず」をチェックする	4.1節	□済	□設定せず
③サーバ証明書設定	③-1）【遵守項目】サーバの公開鍵情報（Subject Public Key Info）の Subject Public Key Algorithmと鍵長の組合せが以下のいずれかを満たしているか □ RSAで鍵長は2048ビット以上 □ 楕円曲線暗号で鍵長256ビット以上	4.2節	□済	
	③-2）【遵守項目】認証局の署名アルゴリズム（Certificate Signature Algorithm）と鍵長の組合せが以下のいずれかを満たしているか □ RSA署名とSHA-256の組合せで鍵長2048ビット以上 □ ECDSAとSHA-256の組合せで鍵長256ビット（NIST P-256）以上	4.2節	□済	
	③-3）【遵守項目】サーバ証明書の発行・更新を行う際に、自ら公開鍵と秘密鍵の鍵ペアを生成する場合には、新たな公開鍵と秘密鍵の鍵ペアを生成しているか	4.2節	□済	
	③-4）【遵守項目】上記③-3)についての指示を仕様書や運用手順書等に明記したか	4.2節	□済	
	③-5）【遵守項目】 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	4.2節	□済	
④暗号スイート設定	④-1）【遵守項目】表15記載の暗号アルゴリズムを全てを設定無効（利用不可）にしたか	4.3節	□済	
	④-2）ECDHEを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-2-1のチェック不要）		□設定する	□設定せず
	④-2-1）【遵守項目】ECDHEの鍵長を256ビット以上に設定したか	4.3節	□済	
	④-3）DHEを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-3-1のチェック不要）		□設定する	□設定せず
	④-3-1）【遵守項目】DHEの鍵長を2048ビット以上に設定したか	4.3節	□済	
	④-4）【推奨項目】表16記載の暗号アルゴリズムを組み合わせた暗号スイートのみで設定しているか。 設定しない／できない場合は「設定せず」をチェックする	4.3節	□済	□設定せず
	④-5）暗号スイートの優先順位が設定できるか。 設定できない場合は「設定不可」をチェックする（④-5-1のチェック不要）		□設定可	□設定不可
	④-5-1）【推奨項目】表18記載の暗号スイートの優先順位で設定したか。 優先順位どおりに設定できない／しない場合は「設定せず」をチェックする	4.3節	□済	□設定せず
⑤附録	⑤）Appendix C：暗号スイートの設定例の最新版のドキュメントを参照して設定したか。参照していない場合には「参照せず」をチェックする	Appendix C	□参照済	□参照せず

【表15】（TLS暗号設定ガイドライン 4.3節）
※下記の暗号アルゴリズムのいずれかを含む暗号スイートは
「全種類」設定無効化（利用不可）とすること

【遵守項目】利用禁止暗号アルゴリズム一覧（2020年1月7日時点）		
鍵交換		DH
		ECDH
署名		GOST R 34.10-2012
暗号化	ブロック暗号	RC2
		EXPORT-RC2
		IDEA
		DES
		EXPORT-DES
		GOST 28147-89
		Magma
		3-key Triple DES
		Kuznyechik
		ARIA
		SEED
	暗号利用モード	CTR_OMAC
	ストリーム暗号	RC4
		EXPORT-RC4
ハッシュ関数		MD5
		GOST R 34.11-2012

【表16】（TLS暗号設定ガイドライン 4.3節）
※下記の暗号アルゴリズムだけを組み合わせた暗号スイートのみで
設定（利用可）されている

【推奨項目】利用推奨暗号アルゴリズム一覧		
鍵交換		ECDHE
		DHE
署名		ECDSA
		RSASSA PKCS#1 v1.5 (RSA)
		RSASSA-PSS（TLS1.3のみ）
暗号化	ブロック暗号	AES
		Camellia（TLS1.2のみ）
	暗号利用モード	GCM
		CCM
		CCM_8
		CBC
	ストリーム暗号	ChaCha20-Poly1305
ハッシュ関数		SHA-256
		SHA-384
		SHA-1

【表18】（TLS暗号設定ガイドライン 4.3節）

【推奨項目】TLS1.2を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループＡ	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2B)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2F)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x86)
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	(0xC0,0xAC)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	(0xC0,0xAE)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2C)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x30)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x87)
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8B)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	(0xC0,0xAD)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	(0xC0,0xAF)
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA9)
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA8)
グループＢ	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9E)
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7C)
	TLS_DHE_RSA_WITH_AES_128_CCM	(0xC0,0x9E)
	TLS_DHE_RSA_WITH_AES_128_CCM_8	(0xC0,0xA2)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9F)
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7D)
	TLS_DHE_RSA_WITH_AES_256_CCM	(0xC0,0x9F)
	TLS_DHE_RSA_WITH_AES_256_CCM_8	(0xC0,0xA3)
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xAA)
グループＣ	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	(0xC0,0x23)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	(0xC0,0x27)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x72)
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x76)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	(0xC0,0x24)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	(0xC0,0x28)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x73)
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x77)
グループＤ	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	(0xC0,0x09)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	(0xC0,0x13)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	(0xC0,0x0A)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	(0xC0,0x14)
グループＥ	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x67)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBE)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x6B)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC4)
グループＦ	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	(0x00,0x33)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x45)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	(0x00,0x39)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x88)

【推奨項目】TLS1.3を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループＡ	TLS_AES_128_GCM_SHA256	(0x13,0x01)
	TLS_AES_128_CCM_SHA256	(0x13,0x04)
	TLS_AES_128_CCM_8_SHA256	(0x13,0x05)
	TLS_AES_256_GCM_SHA384	(0x13,0x02)
	TLS_CHACHA20_POLY1305_SHA256	(0x13,0x03)
鍵交換	ECDHE（優先）	RFC8446に規定
	DHE	RFC8446に規定
署名	ECDSA	RFC8446に規定
	RSA-PSS	RFC8446に規定
	RSASSA-PKCS1-v1_5	RFC8446に規定

【高セキュリティ型チェックリスト】　　2020.07.07版

チェック項目		参照章		
①要求設定確認	①-1)【遵守項目】高セキュリティ型の設定基準を満たすことが必要な利用環境であるか	3.1節	□該当	
②プロトコルバージョン設定	②-1)【遵守項目】TLS1.3を設定有効としたか	5.1節	□済	
	②-2)【遵守項目】TLS1.2を設定有効としたか。ただし、TLS1.2を明確に利用しないと判明している場合は「設定せず」をチェックする	5.1節	□済	□設定せず
	②-3)【遵守項目】SSL2.0からTLS1.1までを設定無効（利用不可）にしたか	5.1節	□済	
③サーバ証明書設定	③-1)【遵守項目】サーバの公開鍵情報（Subject Public Key Info）のSubject Public Key Algorithmと鍵長の組合せが以下のいずれかを満たしているか □ RSAで鍵長は2048ビット以上 □ 楕円曲線暗号で鍵長256ビット以上	5.2節	□済	
	③-2)【遵守項目】認証局の署名アルゴリズム（Certificate Signature Algorithm）と鍵長の組合せが以下のいずれかを満たしているか □ RSA署名とSHA-256以上の組合せで鍵長2048ビット以上 □ ECDSAとSHA-256以上の組合せで鍵長256ビット（NIST P-256）以上	5.2節	□済	
	③-3)【遵守項目】サーバ証明書の発行・更新を行う際に、自ら公開鍵と秘密鍵の鍵ペアを生成する場合には、新たな公開鍵と秘密鍵の鍵ペアを生成しているか	5.2節	□済	
	③-4)【遵守項目】上記③-3)についての指示を仕様書や運用手順書等に明記したか	5.2節	□済	
	③-5)【遵守項目】 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	5.2節	□済	
④暗号スイート設定	④-1)【遵守項目】表21記載の暗号アルゴリズムを全てを設定無効（利用不可）にしたか	5.3節	□済	
	④-2) ECDHEを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-2-1のチェック不要）		□設定する	□設定せず
	④-2-1)【遵守項目】ECDHEの鍵長を256ビット以上に設定したか	5.3節	□済	
	④-3) DHEを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-3-1のチェック不要）		□設定する	□設定せず
	④-3-1)【遵守項目】DHEの鍵長を2048ビット以上に設定したか	5.3節	□済	
	④-4)【推奨項目】表22記載の暗号アルゴリズムを組み合わせた暗号スイートのみで設定しているか。 設定しない／できない場合は「設定せず」をチェックする	5.3節	□済	□設定せず
	④-5) 暗号スイートの優先順位が設定できるか。 設定できない場合は「設定不可」をチェックする（④-5-1のチェック不要）		□設定可	□設定不可
	④-5-1) 【推奨項目】表24記載の暗号スイートの優先順位で設定したか。 優先順位どおりに設定できない／しない場合は「設定せず」をチェックする	5.3節	□済	□設定せず
⑤附録	⑤) Appendix C：暗号スイートの設定例の最新版のドキュメントを参照して設定したか。参照していない場合には「参照せず」をチェックする	Appendix C	□参照済	□参照せず

【表21】（TLS暗号設定ガイドライン 5.3節）
※下記の暗号アルゴリズムのいずれかを含む暗号スイートは
「全種類」設定無効化（利用不可）とすること

【遵守項目】利用禁止暗号アルゴリズム一覧（2020年1月7日時点）		
鍵交換		DH
		ECDH
		RSAES PKCS#1 v1.5 (RSA)
署名		GOST R 34.10-2012
暗号化	ブロック暗号	RC2
		EXPORT-RC2
		IDEA
		DES
		EXPORT-DES
		GOST 28147-89
		Magma
		3-key Triple DES
		Kuznyechik
		ARIA
		SEED
	暗号利用モード	CBC
		CTR_OMAC
	ストリーム暗号	RC4
		EXPORT-RC4
ハッシュ関数		MD5
		SHA-1
		GOST R 34.11-2012

【表22】（TLS暗号設定ガイドライン 5.3節）
※下記の暗号アルゴリズムだけを組み合わせた暗号スイートのみで
設定（利用可）されている

【推奨項目】利用推奨暗号アルゴリズム一覧		
鍵交換		ECDHE
		DHE
署名		ECDSA
		RSASSA PKCS#1 v1.5 (RSA)
		RSASSA-PSS（TLS1.3のみ）
暗号化	ブロック暗号	AES
		Camellia（TLS1.2のみ）
	暗号利用モード	GCM
		CCM
		CCM_8
	ストリーム暗号	ChaCha20-Poly1305
ハッシュ関数		SHA-256
		SHA-384

【表24】（TLS暗号設定ガイドライン 5.3節）

【推奨項目】TLS1.3を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループA	TLS_AES_256_GCM_SHA384	(0x13,0x02)
	TLS_CHACHA20_POLY1305_SHA256	(0x13,0x03)
	TLS_AES_128_GCM_SHA256	(0x13,0x01)
	TLS_AES_128_CCM_SHA256	(0x13,0x04)
	TLS_AES_128_CCM_8_SHA256	(0x13,0x05)
鍵交換	ECDHE（優先）	RFC8446に規定
	DHE	RFC8446に規定
署名	ECDSA	RFC8446に規定
	RSA-PSS	RFC8446に規定
	RSASSA-PKCS1-v1_5	RFC8446に規定

【推奨項目】TLS1.2を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループA	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2C)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x30)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x87)
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8B)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	(0xC0,0xAD)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	(0xC0,0xAF)
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA9)
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA8)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2B)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2F)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x86)
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	(0xC0,0xAC)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	(0xC0,0xAE)
グループB	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9F)
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7D)
	TLS_DHE_RSA_WITH_AES_256_CCM	(0xC0,0x9F)
	TLS_DHE_RSA_WITH_AES_256_CCM_8	(0xC0,0xA3)
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xAA)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9E)
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7C)
	TLS_DHE_RSA_WITH_AES_128_CCM	(0xC0,0x9E)
	TLS_DHE_RSA_WITH_AES_128_CCM_8	(0xC0,0xA2)

【セキュリティ例外型チェックリスト】　2020.07.07版

チェック項目		参照章		
①要求設定確認	①-1）【遵守項目】推奨セキュリティ型以上の設定が現実的ではない等の特殊事情があるケースに該当するか	3.1節	□該当	
	①-2）【遵守項目】推奨セキュリティ型への移行完了までの短期暫定運用を前提とし、早期の利用終了期限を含む移行計画を策定するなど、今後の対処方針を具体的に策定しているか	3.1節	□済	
②プロトコルバージョン設定	②-1）【遵守項目】SSL3.0及びSSL2.0を設定無効（利用不可）にしたか	6.1節	□済	
	②-2）TLS1.2が実装されているか。 実装されていない場合は「未実装」をチェックする（②-2-1のチェック不要）		□実装済	□未実装
	②-2-1）【遵守項目】TLS1.2について設定を有効にしたか	6.1節	□済	
	②-3）TLS1.1とTLS1.0のいずれか、または両方の設定を有効にするか。 両方とも有効にしない場合は「設定せず」をチェックする（②-3-1のチェック不要）		□設定する	□設定せず
	②-3-1）【遵守項目】TLS1.1とTLS1.0のいずれか、または両方を設定有効とする必要性を確認したか	6.1節	□済	
	②-4）TLS1.3が実装されているか。 実装されていない場合は未実装にチェックする（②-4-1のチェック不要）		□実装済	□未実装
	②-4-1）【推奨項目】TLS1.3について設定を有効にしたか。 ただし、TLS1.3を明確に利用しないと判断している場合には「設定せず」をチェックする	6.1節	□済	□設定せず
	②-5）プロトコルバージョンの優先順位が設定できるか。 設定できない場合は「設定不可」にチェックする（②-5-1のチェック不要）		□設定可	□設定不可
	②-5-1）【推奨項目】最も新しいバージョンによる接続を最優先とし、接続できない場合に順番に一つずつ前のバージョンで接続するように設定したか。設定しない場合は「設定せず」をチェックする	6.1節	□済	□設定せず
③サーバ証明書設定	③-1）【遵守項目】サーバの公開鍵情報（Subject Public Key Info）のSubject Public Key Algorithmと鍵長の組合せが以下のいずれかを満たしているか □ RSAで鍵長は2048ビット以上	6.2節	□済	
	③-2）【遵守項目】認証局の署名アルゴリズム（Certificate Signature Algorithm）と鍵長の組合せが以下のいずれかを満たしているか □ RSA署名とSHA-256の組合せで鍵長2048ビット以上	6.2節	□済	
	③-3）【遵守項目】サーバ証明書の発行・更新を行う際に、自ら公開鍵と秘密鍵の鍵ペアを生成する場合には、新たな公開鍵と秘密鍵の鍵ペアを生成しているか	6.2節	□済	
	③-4）【遵守項目】上記③-3)についての指示を仕様書や運用手順書等に明記したか	6.2節	□済	
	③-5）【遵守項目】 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	6.2節	□済	
④暗号スイート設定	④-1）【遵守項目】表27記載の暗号アルゴリズムを全てを設定無効（利用不可）にしたか	6.3節	□済	
	④-2）ECDHE／ECDHを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-2-1のチェック不要）		□設定する	□設定せず
	④-2-1）【遵守項目】ECDHE/ECDHの鍵長を256ビット以上に設定したか	6.3節	□済	
	④-3）DHE/DHを利用する暗号スイートを設定するか。 設定しない場合は「設定せず」をチェックする（④-3-1のチェック不要）		□設定する	□設定せず
	④-3-1）【遵守項目】DHE/DHの鍵長を1024ビット以上に設定したか	6.3節	□済	
	④-4）【推奨項目】表28記載の暗号アルゴリズムを組み合わせた暗号スイートのみで設定しているか。 設定しない／できない場合には「設定せず」をチェックする	6.3節	□済	□設定せず
	④-5）暗号スイートの優先順位が設定できるか。 設定できない場合は「設定不可」をチェックする（④-5-1のチェック不要）		□設定可	□設定不可
	④-5-1）【推奨項目】表30記載の暗号スイートの優先順位で設定したか。 優先順位どおりに設定できない／しない場合には「設定せず」をチェックする	6.3節	□済	□設定せず
⑤附録	⑤）Appendix C：暗号スイートの設定例の最新版のドキュメントを参照して設定したか。参照していない場合には「参照せず」をチェックする	Appendix C	□参照済	□参照せず

【表27】（TLS暗号設定ガイドライン 6.3節）
※下記の暗号アルゴリズムのいずれかを含む暗号スイートは
「全種類」設定無効化（利用不可）とすること

【遵守項目】利用禁止暗号アルゴリズム一覧（2020年1月7日時点）		
署名		GOST R 34.10-2012
暗号化	ブロック暗号	RC2
		EXPORT-RC2
		IDEA
		DES
		EXPORT-DES
		GOST 28147-89
		Magma
		3-key Triple DES
		Kuznyechik
		ARIA
		SEED
	暗号利用モード	CTR_OMAC
	ストリーム暗号	RC4
		EXPORT-RC4
ハッシュ関数		MD5
		GOST R 34.11-2012

【表28】（TLS暗号設定ガイドライン 6.3節）
※下記の暗号アルゴリズムだけを組み合わせた暗号スイートのみで
設定（利用可）されている

【推奨項目】利用推奨暗号アルゴリズム一覧		
鍵交換		DHE
		ECDHE
		RSAES PKCS#1 v1.5 (RSA)
		DH
		ECDH
署名		RSASSA PKCS#1 v1.5 (RSA)
		ECDSA
		RSASSA-PSS（TLS1.3のみ）
暗号化	ブロック暗号	AES
		Camellia（TLS1.2まで）
	暗号利用モード	GCM
		CCM
		CCM_8
		CBC
	ストリーム暗号	ChaCha20-Poly1305
ハッシュ関数		SHA-256
		SHA-384
		SHA-1

【表30】（TLS暗号設定ガイドライン 6.3節）

【推奨項目】TLS1.2を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループX	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9E)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2B)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2F)
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7C)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x86)
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8A)
	TLS_DHE_RSA_WITH_AES_128_CCM	(0xC0,0x9E)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	(0xC0,0xAC)
	TLS_DHE_RSA_WITH_AES_128_CCM_8	(0xC0,0xA2)
	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	(0xC0,0xAE)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9F)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2C)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x30)
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7D)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x87)
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8B)
	TLS_DHE_RSA_WITH_AES_256_CCM	(0xC0,0x9F)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	(0xC0,0xAD)
	TLS_DHE_RSA_WITH_AES_256_CCM_8	(0xC0,0xA3)
	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	(0xC0,0xAF)
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xAA)
	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA9)
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	(0xCC,0xA8)
グループY	TLS_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9C)
	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	(0x00,0xA0)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2D)
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x31)
	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7A)
	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7E)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x88)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8C)
	TLS_RSA_WITH_AES_128_CCM	(0xC0,0x9C)
	TLS_RSA_WITH_AES_128_CCM_8	(0xC0,0xA0)
	TLS_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9D)
	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	(0x00,0xA1)
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2E)
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x32)
	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7B)
	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7F)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x89)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8D)
	TLS_RSA_WITH_AES_256_CCM	(0xC0,0x9D)
	TLS_RSA_WITH_AES_256_CCM_8	(0xC0,0xA1)

（グループZに続く）

【表30（続）】（TLS暗号設定ガイドライン 6.3節）

【推奨項目】TLS1.2を利用する場合の優先順位（続）		
優先順位グループ	暗号スイート名	スイート番号
グループZ	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x67)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBE)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	(0x00,0x33)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x45)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	(0xC0,0x23)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	(0xC0,0x27)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x72)
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x76)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	(0xC0,0x09)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	(0xC0,0x13)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x6B)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC4)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	(0x00,0x39)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x88)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	(0xC0,0x24)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	(0xC0,0x28)
	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x73)
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x77)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	(0xC0,0x0A)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	(0xC0,0x14)
	TLS_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x3C)
	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x3F)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	(0xC0,0x25)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	(0xC0,0x29)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBA)
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBC)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x74)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x78)
	TLS_RSA_WITH_AES_128_CBC_SHA	(0x00,0x2F)
	TLS_DH_RSA_WITH_AES_128_CBC_SHA	(0x00,0x31)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	(0xC0,0x04)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	(0xC0,0x0E)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x41)
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x43)
	TLS_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x3D)
	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x69)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	(0xC0,0x26)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	(0xC0,0x2A)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC0)
	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC2)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x75)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x79)
	TLS_RSA_WITH_AES_256_CBC_SHA	(0x00,0x35)
	TLS_DH_RSA_WITH_AES_256_CBC_SHA	(0x00,0x37)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	(0xC0,0x05)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	(0xC0,0x0F)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x84)
	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x86)
【推奨項目】TLS1.3を利用する場合の優先順位		
優先順位グループ	暗号スイート名	スイート番号
グループA	TLS_AES_128_GCM_SHA256	(0x13,0x01)
	TLS_AES_128_CCM_SHA256	(0x13,0x04)
	TLS_AES_128_CCM_8_SHA256	(0x13,0x05)
	TLS_AES_256_GCM_SHA384	(0x13,0x02)
	TLS_CHACHA20_POLY1305_SHA256	(0x13,0x03)
鍵交換	ECDHE（優先）	RFC8446に規定
	DHE	RFC8446に規定
署名	ECDSA	RFC8446に規定
	RSA-PSS	RFC8446に規定
	RSASSA-PKCS1-v1_5	RFC8446に規定