SSL/TLS暗号設定ガイドラインチェックリスト

【チェックリストの使い方】
本チェックリストは、以下の項目について、選択した設定基準に対応した要求設定をもれなく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を下部の「タグ」から選択し、当該シートにおいて条件該当するチェック項目全てについて、該当章に記載の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求められる。なお、チェック項目の条件該非については次ページ以降も併せて参照のこと。

◇ プロトコルバージョンの設定（ガイドライン第4章）
◇ サーバ証明書の設定（ガイドライン第5章）
◇ 暗号スイートの設定（ガイドライン第6章）

＜チェックリストの例＞
【高セキュリティ型のチェックリスト】

選択したセキュリティ水準に対応したチェックリストを用いる

チェック		参照章	済
①要求設定確認	①-1）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	□
②プロトコルバージョン設定	②-1）TLS1.2を設定有効にしたか	4.1節	□
	②-2）TLS1.1以前を設定無効（利用不可）にしたか	4.1節	□
③サーバ証明書設定	③-1）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		□
	③-2）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2048ビット以上 ・ 楕円曲線で鍵長256ビット以上	5.1節	□
	③-3）[illegible]行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	□
	③-4）[illegible]行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	□
	③-5）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暗号スイート設定	□ ④-i）楕円曲線暗号を利用しない場合は左の□と以下の項目を[illegible]		
	④-i-1）表1記載の暗号スイート（網掛けを除く）の全部または[illegible]たか		□
	④-i-[illegible]（網掛けを除く）から少なくとも一[illegible]	6.1節／6.5.1節	□
	④-i-[illegible]番（グループαの暗号スイートの次に[illegible]っているか	6.1節／6.5.1節	□
	④-i-[illegible]て利用不可の設定をしたか	6.1節／6.5.1節	□
	④-i-5）DHE[illegible]2048ビット以上に設定したか	6.1節／6.5.1節	□
	□ ④-ii）楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1）表1記載の暗号スイート（網掛けを含む）の全部または一部を設定[illegible]	6.1節／6.5.1節	□
	[illegible]表1記載のグループαの暗号スイート（網掛けを含む）から少なく	6.1節／6.5.1節	□
	[illegible]のグループ順番（グループαの暗号スイートが並ぶ）を守っているか	6.1節／6.5.1節	□
	[illegible]以外は、すべて利用不可の設定をしたか	6.1節／6.5.1節	□
	[illegible]以上に設定したか	6.1節／6.5.1節	□
	□ ④-ii-6）DHEの暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-ii-7）DHEの鍵長を2048ビット以上に設定したか	6.1節／6.5.1節	□

要求設定の詳細な内容が記載されている章番号

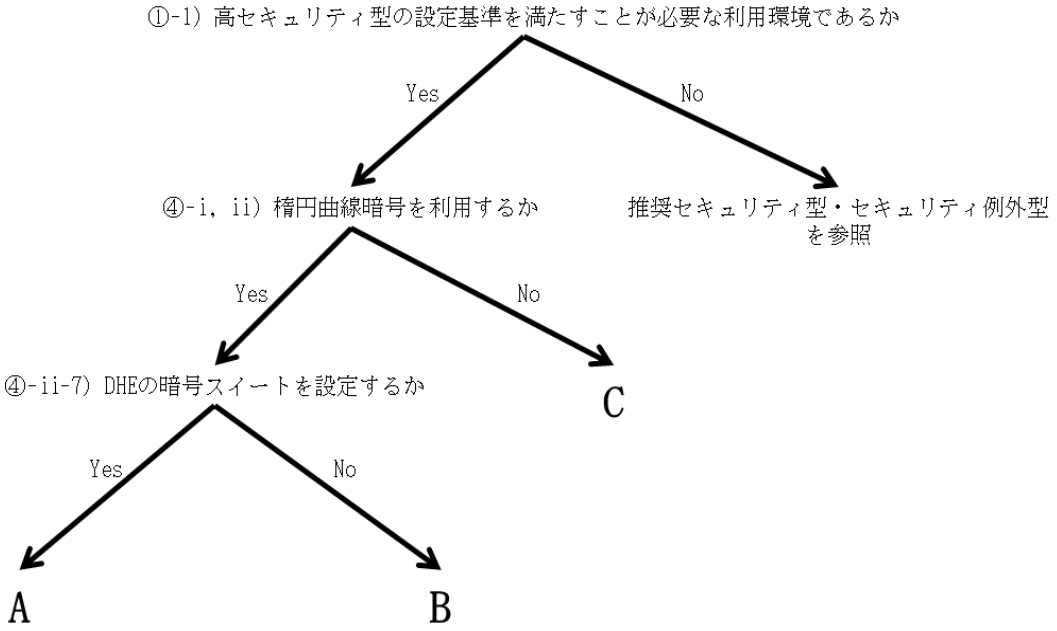
確認すべき要求事項の概要が記載されている

要求設定が満たされていることを確認したらチェックを入れる

この色がついているチェック項目は該当する場合のみ確認する
この例では「楕円曲線暗号を利用する場合」の確認対象となる

この色がついているチェック項目を利用する場合にチェックを入れる
この例では「楕円曲線暗号を利用する場合」 にチェックを入れる

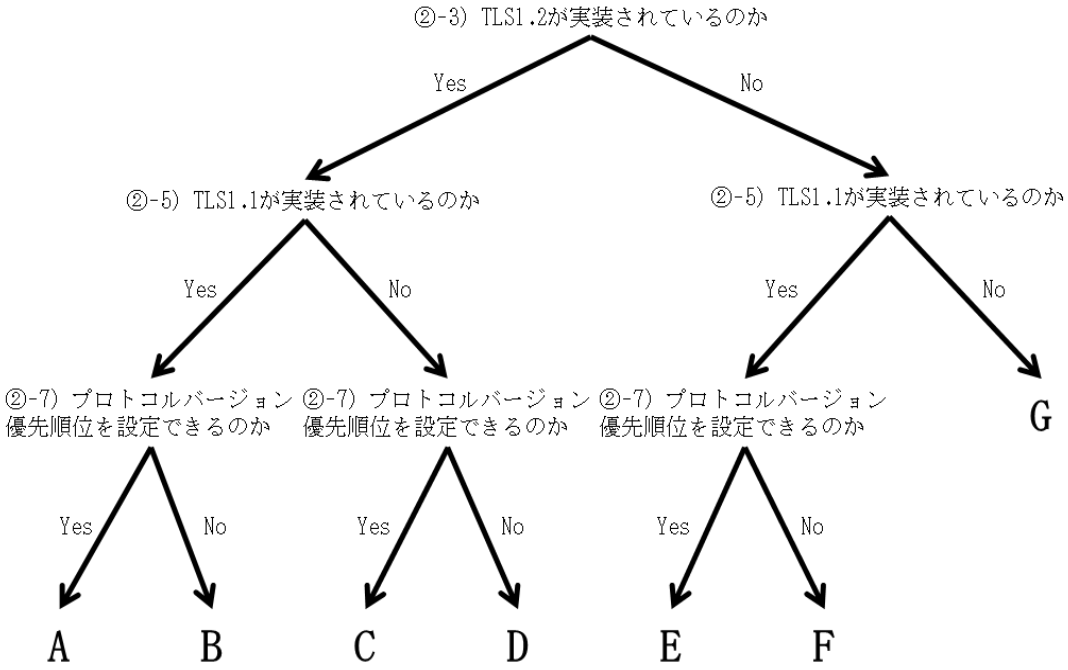
高セキュリティ型



対象外 ・・・ 対象外のチェック項目

チェック項目		A	B	C
①要求設定確認	①-1)			
②プロトコルバージョン設定	②-1)			
	②-2)			
③サーバ証明書設定	③-1)			
	③-2)			
	③-3)			
	③-4)			
	③-5)			
④暗号スイート設定	④-i)	対象外	対象外	
	④-i-1)	対象外	対象外	
	④-i-2)	対象外	対象外	
	④-i-3)	対象外	対象外	
	④-i-4)	対象外	対象外	
	④-i-5)	対象外	対象外	
	④-ii)			対象外
	④-ii-1)			対象外
	④-ii-2)			対象外
	④-ii-3)			対象外
	④-ii-4)			対象外
	④-ii-5)			対象外
	④-ii-6)		対象外	対象外
	④-ii-7)		対象外	対象外

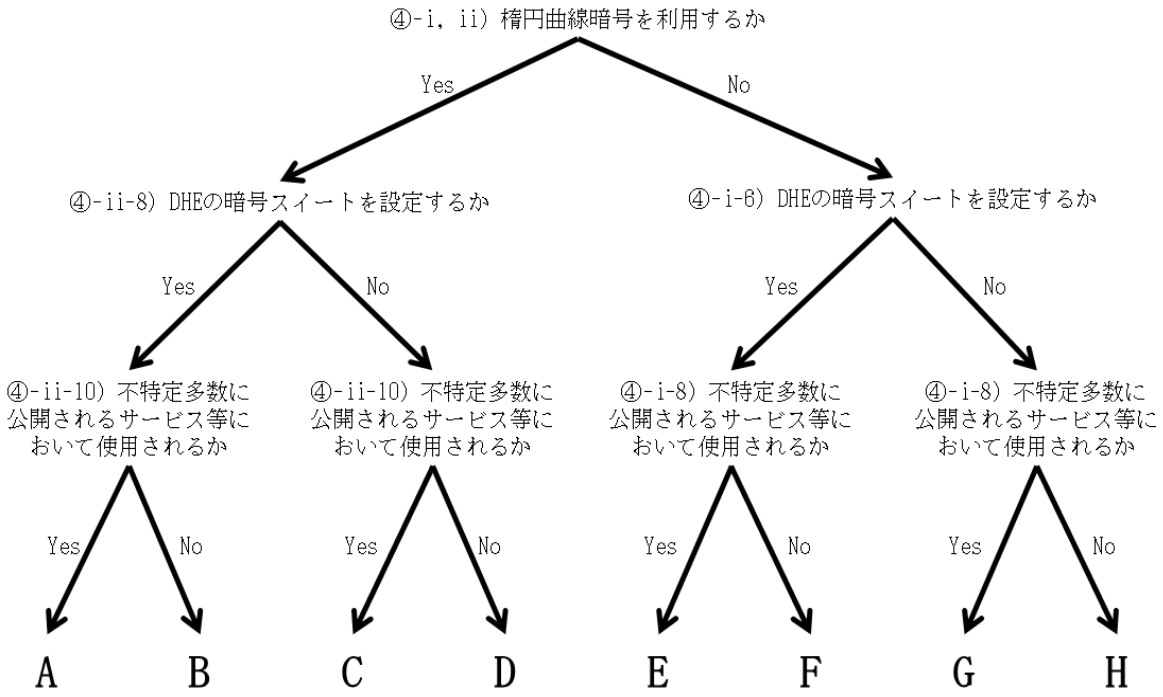
推奨セキュリティ型（1／2）



対象外 ・・・ 対象外のチェック項目

チェック項目		A	B	C	D	E	F	G
①要求設定確認	①-1)							
②プロトコルバージョン設定	②-1)							
	②-2)							
	②-3)					対象外	対象外	対象外
	②-4)					対象外	対象外	対象外
	②-5)			対象外	対象外			対象外
	②-6)			対象外	対象外			対象外
	②-7)		対象外		対象外		対象外	対象外
	②-8)		対象外		対象外		対象外	対象外
③サーバ証明書設定	③-1)							
	③-2)							
	③-3)							
	③-4)							
	③-5)							

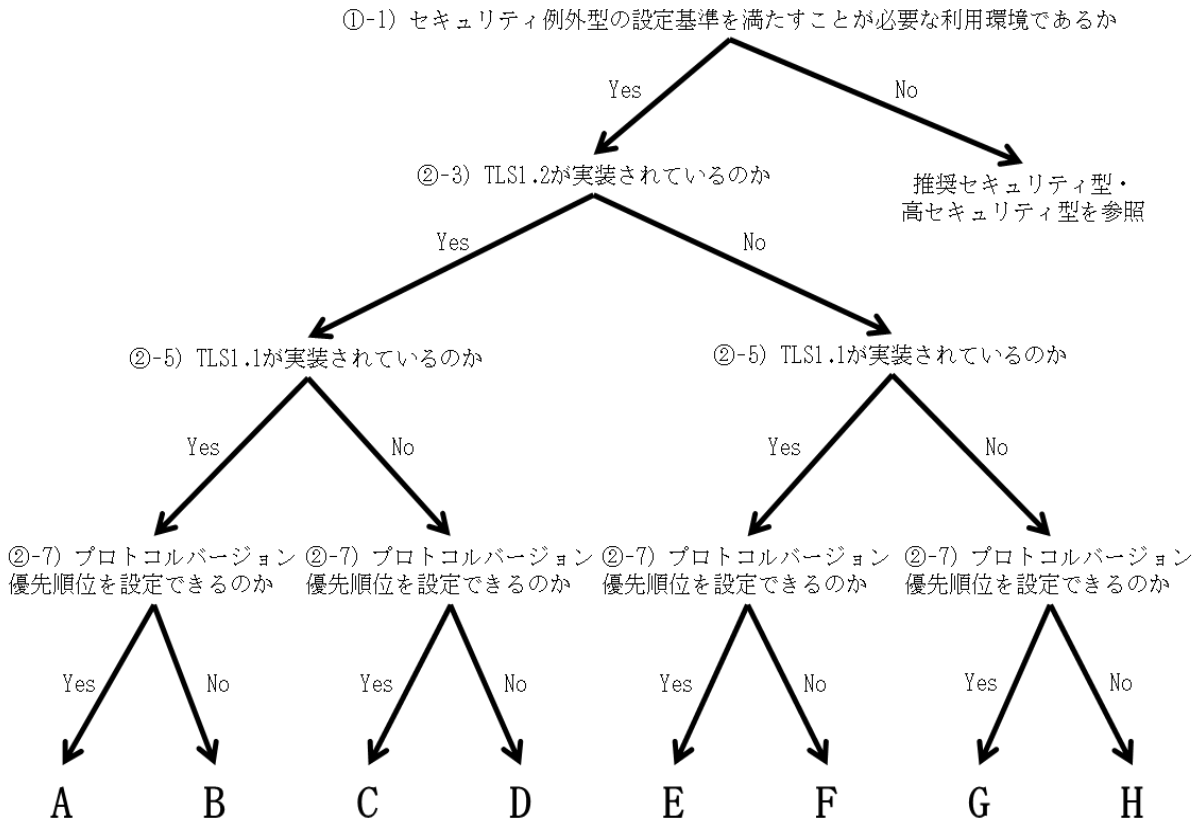
推奨セキュリティ型（２／2）



対象外 ・・・ 対象外のチェック項目

チェック項目		A	B	C	D	E	F	G	H
④暗号スイート設定	④-i)	対象外	対象外	対象外	対象外				
	④-i-1)	対象外	対象外	対象外	対象外				
	④-i-2)	対象外	対象外	対象外	対象外				
	④-i-3)	対象外	対象外	対象外	対象外				
	④-i-4)	対象外	対象外	対象外	対象外				
	④-i-5)	対象外	対象外	対象外	対象外				
	④-i-6)	対象外	対象外	対象外	対象外			対象外	対象外
	④-i-7)	対象外	対象外	対象外	対象外			対象外	対象外
	④-i-8)	対象外	対象外	対象外	対象外		対象外		対象外
	④-i-9)	対象外	対象外	対象外	対象外		対象外		対象外
	④-ii)					対象外	対象外	対象外	対象外
	④-ii-1)					対象外	対象外	対象外	対象外
	④-ii-2)					対象外	対象外	対象外	対象外
	④-ii-3)					対象外	対象外	対象外	対象外
	④-ii-4)					対象外	対象外	対象外	対象外
	④-ii-5)					対象外	対象外	対象外	対象外
	④-ii-6)					対象外	対象外	対象外	対象外
	④-ii-7)			対象外	対象外	対象外	対象外	対象外	対象外
	④-ii-8)			対象外	対象外	対象外	対象外	対象外	対象外
	④-ii-9)		対象外		対象外	対象外	対象外	対象外	対象外
	④-ii-10)		対象外		対象外	対象外	対象外	対象外	対象外

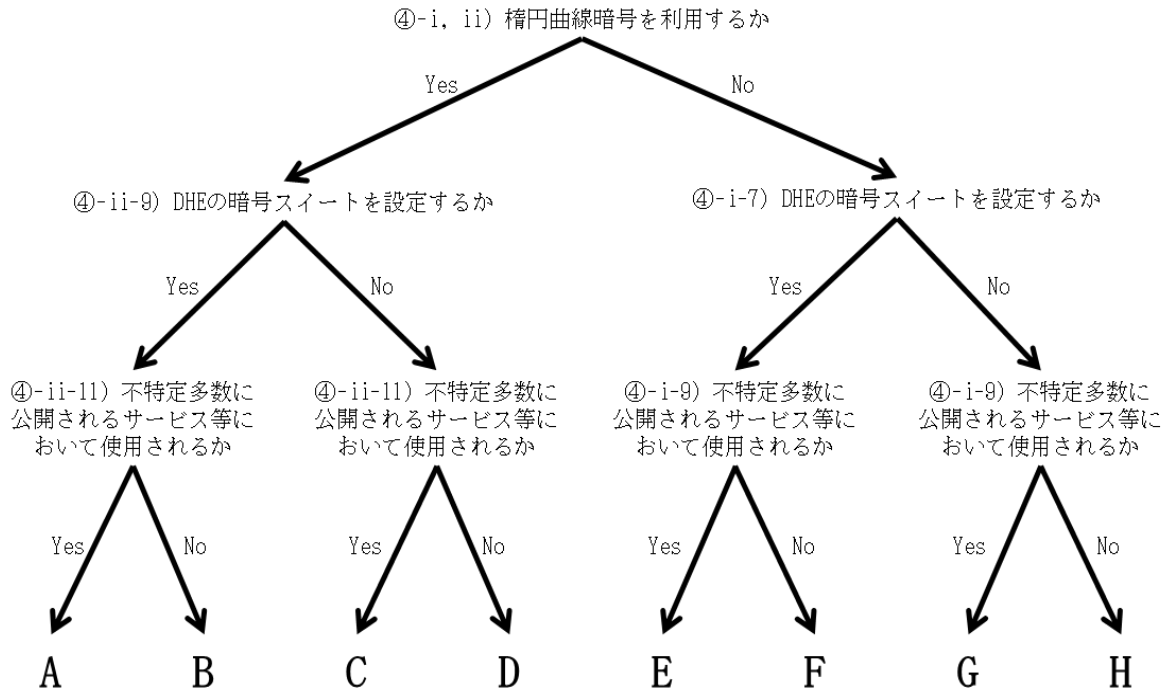
セキュリティ例外型（1／2）



対象外 ・・・ 対象外のチェック項目

チェック項目		A	B	C	D	E	F	G	H
①要求設定確認	①-1）								
	①-2）								
②プロトコルバージョン設定	②-1）								
	②-2）								
	②-3）					対象外	対象外	対象外	対象外
	②-4）					対象外	対象外	対象外	対象外
	②-5）			対象外	対象外			対象外	対象外
	②-6）			対象外	対象外			対象外	対象外
	②-7）		対象外		対象外		対象外		対象外
	②-8）		対象外		対象外		対象外		対象外
③サーバ証明書設定	③-1）								
	③-2）								
	③-3）								
	③-4）								
	③-5）								

セキュリティ例外型（２／２）



対象外 ・・・ 対象外のチェック項目

チェック項目		A	B	C	D	E	F	G	H
④暗号スイート設定	④-i)	対象外	対象外	対象外	対象外				
	④-i-1)	対象外	対象外	対象外	対象外				
	④-i-2)	対象外	対象外	対象外	対象外				
	④-i-3)	対象外	対象外	対象外	対象外				
	④-i-4)	対象外	対象外	対象外	対象外				
	④-i-5)	対象外	対象外	対象外	対象外				
	④-i-6)	対象外	対象外	対象外	対象外				
	④-i-7)	対象外	対象外	対象外	対象外			対象外	対象外
	④-i-8)	対象外	対象外	対象外	対象外			対象外	対象外
	④-i-9)	対象外	対象外	対象外	対象外		対象外		対象外
	④-i-10)	対象外	対象外	対象外	対象外		対象外		対象外
	④-i-11)	対象外	対象外	対象外	対象外		対象外		対象外
	④-ii)					対象外	対象外	対象外	対象外
	④-ii-1)					対象外	対象外	対象外	対象外
	④-ii-2)					対象外	対象外	対象外	対象外
	④-ii-3)					対象外	対象外	対象外	対象外
	④-ii-4)					対象外	対象外	対象外	対象外
	④-ii-5)					対象外	対象外	対象外	対象外
	④-ii-6)					対象外	対象外	対象外	対象外
	④-ii-7)					対象外	対象外	対象外	対象外
	④-ii-8)			対象外	対象外	対象外	対象外	対象外	対象外
	④-ii-9)			対象外	対象外	対象外	対象外	対象外	対象外
	④-ii-10)		対象外		対象外	対象外	対象外	対象外	対象外
	④-ii-11)		対象外		対象外	対象外	対象外	対象外	対象外
	④-ii-12)		対象外		対象外	対象外	対象外	対象外	対象外

【高セキュリティ型のチェックリスト】

チェック項目		参照章	済
①要求設定確認	①-1）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	☐
②プロトコルバージョン設定	②-1）TLS1.2を設定有効にしたか	4.1節	☐
	②-2）TLS1.1以前を設定無効（利用不可）にしたか	4.1節	☐
③サーバ証明書設定	③-1）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	5.1節	☐
	③-2）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	5.1節	☐
	③-3）サーバ証明書の発行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	☐
	③-4）サーバ証明書の発行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	☐
	③-5）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	5.1節	☐
④暗号スイート設定	☐ ④-i）楕円曲線暗号を利用しない場合は左の□と以下の項目をチェック		
	④-i-1）表1記載の暗号スイート（網掛けを除く）の全部または一部を設定したか	6.1節／6.5.1節	☐
	④-i-2）表1記載のグループαの暗号スイート（網掛けを除く）から少なくとも一つは設定したか	6.1節／6.5.1節	☐
	④-i-3）表1記載の暗号スイートのグループ順番（グループαの暗号スイートの次にグループβの暗号スイートが並ぶ）を守っているか	6.1節／6.5.1節	☐
	④-i-4）表1記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.1節	☐
	④-i-5）DHEの鍵長を2048ビット以上に設定したか	6.1節／6.5.1節	☐
	☐ ④-ii）楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1）表1記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1節／6.5.1節	☐
	④-ii-2）表1記載のグループαの暗号スイート（網掛けを含む）から少なくとも一つは設定したか	6.1節／6.5.1節	☐
	④-ii-3）表1記載の暗号スイートのグループ順番（グループαの暗号スイートの次にグループβの暗号スイートが並ぶ）を守っているか	6.1節／6.5.1節	☐
	④-ii-4）表1記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.1節	☐
	④-ii-5）ECDHEの鍵長を256ビット以上に設定したか	6.1節／6.5.1節	☐
	☐ ④-ii-6）DHEの暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-ii-7）DHEの鍵長を2048ビット以上に設定したか	6.1節／6.5.1節	☐

【表1】

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 α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9F)
	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7D)
	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)
グループ β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9E)
	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7C)
	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)

【推奨セキュリティ型のチェックリスト（1/2）】

チェック項目		参照章	済
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）TLS1.0を設定有効にしたか	4.1節	□
	②-2）SSL2.0及びSSL3.0を設定無効（利用不可）にしたか	4.1節	□
	□ ②-3）TLS1.2が実装されている場合には左の□と以下の項目をチェック		
	②-4）TLS1.2について設定を有効にしたか	4.1節	□
	□ ②-5）TLS1.1が実装されている場合には左の□と以下の項目をチェック		
	②-6）TLS1.1について設定を有効にしたか	4.1節	□
	□ ②-7）プロトコルバージョン優先順位を設定できる場合には左の□と以下の項目をチェック		
	②-8）設定有効になっているプロトコルバージョンのうち、もっとも新しいバージョンによる接続を最優先にしたか。接続できない場合に、順番に一つずつ前のプロトコルバージョンでの接続するようにしたか	4.1節	□
③サーバ証明書設定	③-1）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	5.1節	□
	③-2）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	5.1節	□
	③-3）サーバ証明書の発行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	□
	③-4）サーバ証明書の発行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	□
	③-5）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	5.1節	□

（続く）

【推奨セキュリティ型のチェックリスト（2/2）】

チェック項目		参照章	済
④暗号スイート設定	□ ④-i）楕円曲線暗号を利用しない場合は左の□と以下の項目をチェック		
	④-i-1）表2記載の暗号スイート（網掛けを除く）の全部または一部を設定したか	6.1節／6.5.2節	□
	④-i-2）表2記載のグループA及びグループBの暗号スイート（網掛けを除く）から少なくとも一つは設定したか	6.1節／6.5.2節	□
	④-i-3）表2記載の暗号スイートのグループ順番の制限[注]を守っているか	6.1節／6.5.2節	□
	④-i-4）表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□
	④-i-5）RSAの鍵長を2048ビット以上に設定したか	6.1節／6.5.2節	□
	□ ④-i-6）DHEを利用する暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-i-7）DHEの鍵長を1024ビット以上に設定したか	6.1節／6.5.2節	□
	□ ④-i-8）不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-i-9）AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□
	□ ④-ii）楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1）表2記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1節／6.5.2節	□
	④-ii-2）表2記載のグループA及びグループBの暗号スイート（網掛けを含む）から少なくとも一つは設定したか	6.1節／6.5.2節	□
	④-ii-3）表2記載の暗号スイートのグループ順番の制限[注]を守っているか	6.1節／6.5.2節	□
	④-ii-4）表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□
	④-ii-5）ECDHE/ECDHの鍵長を256ビット以上に設定したか	6.1節／6.5.2節	□
	④-ii-6）RSAの鍵長を2048ビット以上に設定したか	6.1節／6.5.2節	□
	□ ④-ii-7）DHEを利用する暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-ii-8）DHEの鍵長を1024ビット以上に設定したか	6.1節／6.5.2節	□
	□ ④-ii-9）不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-ii-10）AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□

［注］　許容される暗号スイートのグループ順番は以下のとおり
(128ビット安全性優先の場合)
・グループA→グループB→グループC→グループD→グループE→グループF
(256ビット安全性優先の場合)
・グループD→グループA→グループE→グループB→グループF→グループC

【表2】

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_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_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_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_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)
グループB	TLS_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9C)
	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7A)
	TLS_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x3C)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBA)
	TLS_RSA_WITH_AES_128_CBC_SHA	(0x00,0x2F)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x41)
グループC	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2D)
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x31)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x88)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8C)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	(0xC0,0x25)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	(0xC0,0x29)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x74)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x78)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	(0xC0,0x04)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	(0xC0,0x0E)
グループD	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_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_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_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)
グループE	TLS_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9D)
	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7B)
	TLS_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x3D)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC0)
	TLS_RSA_WITH_AES_256_CBC_SHA	(0x00,0x35)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x84)
グループF	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2E)
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x32)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x89)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8D)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	(0xC0,0x26)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	(0xC0,0x2A)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x75)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x79)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	(0xC0,0x05)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	(0xC0,0x0F)

【セキュリティ例外型のチェックリスト（1/2）】

チェック項目		参照章	済
①要求設定確認	①-1）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	□
	①-2）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	□
②プロトコルバージョン設定	②-1）TLS1.0及びSSL3.0を設定有効にしたか	4.1節	□
	②-2）SSL2.0を設定無効（利用不可）にしたか	4.1節	□
	□ ②-3）TLS1.2が実装されている場合には左の□と以下の項目をチェック		
	②-4）TLS1.2について設定を有効にしたか	4.1節	□
	□ ②-5）TLS1.1が実装されている場合には左の□と以下の項目をチェック		
	②-6）TLS1.1について設定を有効にしたか	4.1節	□
	□ ②-7）プロトコルバージョン優先順位を設定できる場合には左の□と以下の項目をチェック		
	②-8）設定有効になっているプロトコルバージョンのうち、もっとも新しいバージョンによる接続を最優先にしたか。接続できない場合に、順番に一つずつ前のプロトコルバージョンでの接続するようにしたか	4.1節	□
③サーバ証明書設定	③-1）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 ・ RSA署名とSHA-1の組合せで鍵長2048ビット以上	5.1節	□
	③-2）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を満たしているか ・ RSAで鍵長は2048ビット以上	5.1節	□
	③-3）サーバ証明書の発行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	□
	③-4）サーバ証明書の発行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	□
	③-5）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	5.1節	□

（続く）

【セキュリティ例外型のチェックリスト（2/2）】

チェック項目		参照章	済
④暗号スイート設定	□ ④-i）楕円曲線暗号を利用しない場合は左の□と以下の項目をチェック		
	④-i-1）表3記載の暗号スイート（網掛けを除く）の全部または一部を設定したか	6.1節／6.5.3節	□
	④-i-2）表3記載のグループA及びグループBの暗号スイート（網掛けを除く）から少なくとも一つは設定したか	6.1節／6.5.3節	□
	④-i-3）表3記載のグループGの暗号スイートを設定したか	6.1節／6.5.3節	□
	④-i-4）表3記載の暗号スイートのグループ順番の制限[注]を守っているか	6.1節／6.5.3節	□
	④-i-5）表3記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.3節	□
	④-i-6）RSAの鍵長を2048ビット以上に設定したか	6.1節／6.5.3節	□
	□ ④-i-7）DHEを利用する暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-i-8）DHEの鍵長を1024ビット以上に設定したか	6.1節／6.5.3節	□
	□ ④-i-9）不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-i-10）AES128-SHAの暗号スイートを設定したか	6.1節／6.5.3節	□
	④-i-11）DHE-DSS-DES-CBC3-SHAとDES-CBC3-SHAの少なくとも一方は設定したか	6.1節／6.5.3節	□
	□ ④-ii）楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1）表3記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1節／6.5.3節	□
	④-ii-2）表3記載のグループA及びグループBの暗号スイート（網掛けを含む）から少なくとも一つは設定したか	6.1節／6.5.3節	□
	④-ii-3）表3記載のグループGの暗号スイートを設定したか	6.1節／6.5.3節	□
	④-ii-4）表3記載の暗号スイートのグループ順番の制限[注]を守っているか	6.1節／6.5.3節	□
	④-ii-5）表3記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.3節	□
	④-ii-6）ECDHE/ECDHの鍵長を256ビット以上に設定したか	6.1節／6.5.2節	□
	④-ii-7）RSAの鍵長を2048ビット以上に設定したか	6.1節／6.5.3節	□
	□ ④-ii-8）DHEを利用する暗号スイートを設定する場合は左の□と以下の項目をチェック		
	④-ii-9）DHEの鍵長を1024ビット以上に設定したか	6.1節／6.5.3節	□
	□ ④-ii-10）不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-ii-11）AES128-SHAの暗号スイートを設定したか	6.1節／6.5.3節	□
	④-ii-12）DES-CBC3-SHAの暗号スイートを設定したか	6.1節／6.5.3節	□

［注］　許容される暗号スイートのグループ順番は以下のとおり
（128ビット安全性優先の場合）
・グループA→グループB→グループC→グループD
→グループE→グループF→グループG→グループH

（256ビット安全性優先の場合）
・グループD→グループA→グループE→グループB
→グループF→グループC→グループG→グループH

【表3】

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_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_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_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_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)
グループB	TLS_RSA_WITH_AES_128_GCM_SHA256	(0x00,0x9C)
	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x7A)
	TLS_RSA_WITH_AES_128_CBC_SHA256	(0x00,0x3C)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0x00,0xBA)
	TLS_RSA_WITH_AES_128_CBC_SHA	(0x00,0x2F)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	(0x00,0x41)
グループC	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	(0xC0,0x2D)
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	(0xC0,0x31)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x88)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	(0xC0,0x8C)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	(0xC0,0x25)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	(0xC0,0x29)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x74)
	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	(0xC0,0x78)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	(0xC0,0x04)
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	(0xC0,0x0E)
グループD	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_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_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_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)
グループE	TLS_RSA_WITH_AES_256_GCM_SHA384	(0x00,0x9D)
	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x7B)
	TLS_RSA_WITH_AES_256_CBC_SHA256	(0x00,0x3D)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	(0x00,0xC0)
	TLS_RSA_WITH_AES_256_CBC_SHA	(0x00,0x35)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	(0x00,0x84)
グループF	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	(0xC0,0x2E)
	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	(0xC0,0x32)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x89)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	(0xC0,0x8D)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	(0xC0,0x26)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	(0xC0,0x2A)
	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x75)
	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	(0xC0,0x79)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	(0xC0,0x05)
	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	(0xC0,0x0F)

【表3（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G	TLS_RSA_WITH_RC4_128_SHA	(0x00,0x05)
グループH	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	(0x00,0x16)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA	(0x00,0x0A)