# TLS 暗号設定

# サーバ設定編 & 暗号スイートの設定例

# （Windows IIS 用 ver1.1）

令和 2 年 10 月

独立行政法人 情報処理推進機構

# 目次

本書では、Windows IIS でのサーバ設定及び暗号スイートの設定を行う上での参考情報として、設定方法例を記載する。正式な取扱説明書やマニュアルを参照するとともに、一参考資料として利用されたい。

# 1. サーバ設定方法のまとめ

## 1.1. プロトコルバージョンの設定方法

各 OS におけるプロトコルバージョンのサポート状況は以下の通りである。

| | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 | SSL 3.0 | SSL 2.0 |
|---|---|---|---|---|---|---|
| Windows Server（1903以降） | △ | ○ | ○ | ○ | ▼ | × |
| Windows Server（1809以前）<br>Windows Server 2019以前 | △ | ○ | ○ | ○ | ▼ | × |
| Windows 10（1903以降） | △ | ○ | ○ | ○ | ○ | ▼ |
| Windows 10（1809以前） | △ | ○ | ○ | ○ | ○ | ▼ |

凡例：○：サポートあり　　△：サポートしているがテスト環境向けの試験提供
×：サポートなし　　▼：サポートしているが既定で無効化

サポートされているプロトコルバージョンの利用可否については、以下の設定例に従い、レジストリを設定する。なお、現在、TLS 1.3 については、テスト環境向けの試験提供であるため、本ドキュメントでは取り扱っていない。設定方法は、マイクロソフト社の最新のドキュメントを参照すること。

**参考情報：**

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
https://support.microsoft.com/en-us/kb/245030

- 推奨セキュリティ型
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 2.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 3.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥TLS 1.0¥Server
  "DisabledByDefault"=dword:00000001

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥TLS 1.1¥Server
"DisabledByDefault"=dword:00000001

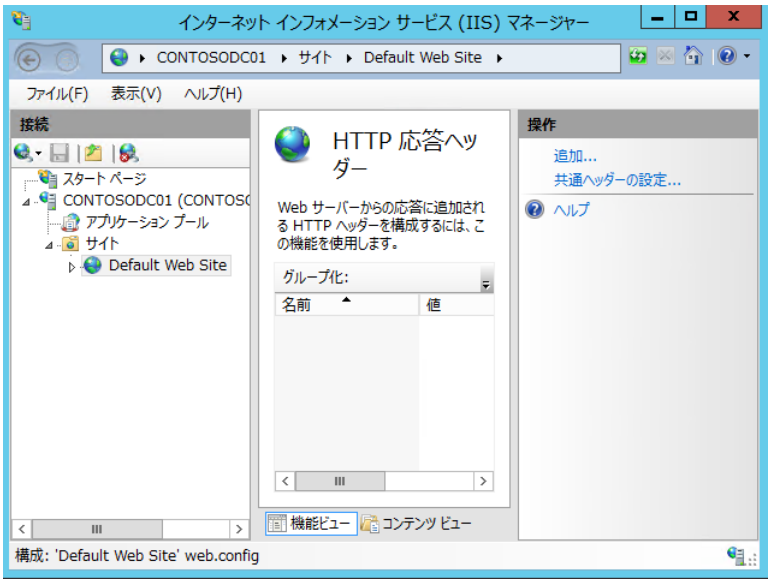
- 高セキュリティ型
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 2.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 3.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥TLS 1.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥TLS 1.1¥Server
  "DisabledByDefault"=dword:00000001

- セキュリティ例外型
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 3.0¥Server
  "DisabledByDefault"=dword:00000001
  HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 2.0¥Server
  "DisabledByDefault"=dword:00000001

### 1.2. HTTP Strict Transport Security（HSTS）の設定方法

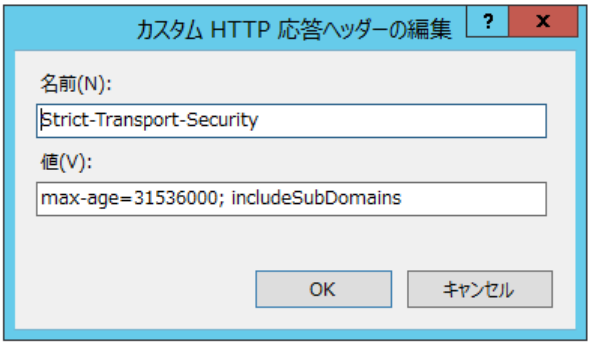
HTTP ヘッダに HSTS の情報を追加するために、以下の手順により設定する。

1）「IIS マネージャー」を開く
2）「機能ビュー」を開く
3）「HTTP 応答ヘッダ」をダブルクリックする
4）「操作」のペインで「追加」をクリックする




5） 「名前」「値」の箇所を以下のように設定する。なお、max-age は有効期間を表し、この例では 365 日（31,536,000 秒）の有効期間を設定することを意味している。また、includeSubDomains がある場合、サブドメインにも適用される

名前：Strict-Transport-Security
値　：max-age=31536000; includeSubDomains




6） 「OK」をクリックする。

### 1.3. OCSP stapling の設定方法

Windows Server 2008 以降の Windows では、デフォルトで OCSP Stapling が設定されている。

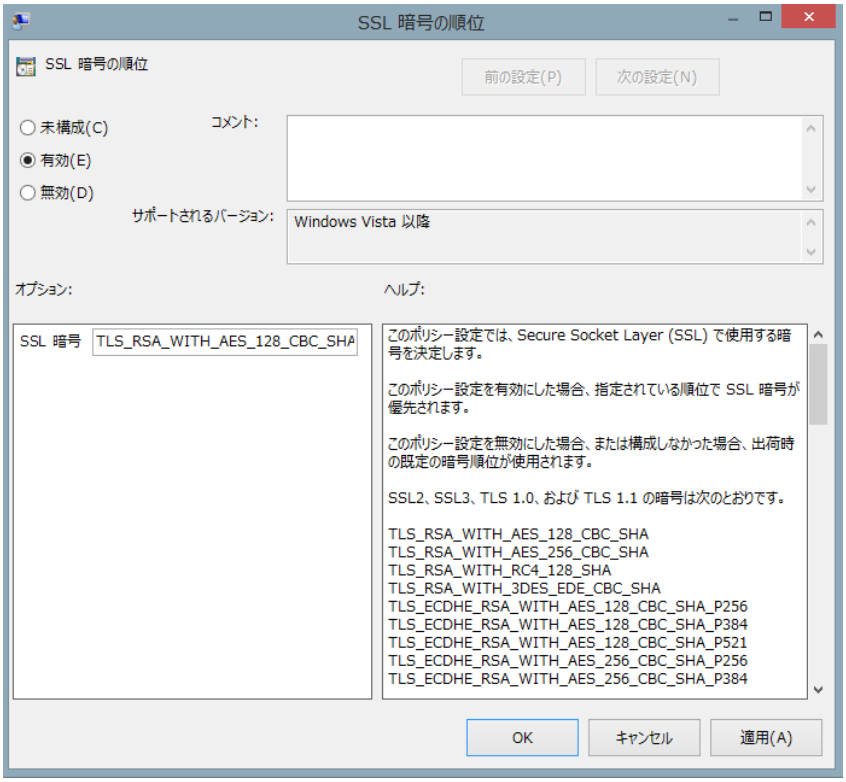
## 2. 暗号スイート設定例のまとめ

本設定例は、Windows 10 v1903、v1909、及び v2004 における TLS 1.2 対応暗号スイートの設定を示している。その他の Windows バージョンの暗号スイートの設定は、以下の参考情報を参考にして設定すること[1]。

Cipher Suites in TLS/SSL (Schannel SSP)
https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

なお、現在、TLS 1.3 については、テスト環境向けの試験提供であるため、本ドキュメントでは取り扱っていない。設定方法は、マイクロソフト社の最新のドキュメントを参照すること。

1) コマンドプロンプトで gpedit.msc と入力し、Enter を押してグループポリシーオブジェクトエディタを起動する。
2) ［コンピューターの構成］＞［管理用テンプレート］＞［ネットワーク］＞［SSL 構成設定］の順に展開する。
3) ［SSL 構成設定］で［SSL 暗号（「SSL 暗号化スイート」と表記される場合もある）の順序］をダブルクリックする。
4) ［SSL 暗号の順序］ウィンドウで、［有効］をクリックする。
5) ウィンドウで、[SSL 暗号]フィールドの内容を設定したい暗号リストの内容と置き換える。




[1] Windows Server 2012, 2016 及び 2019 については、GUI で暗号スイートやプロトコルバージョンを設定できるフリーウェアを NARTAC IIS Crypto が公開している
https://www.nartac.com/Products/IISCrypto/

なお、暗号リストは「,」で暗号スイートを連結して 1 行で記述し、空白や改行を含めない。
優先順位は記述した順番で設定される。

- 推奨セキュリティ型の設定例
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- 高セキュリティ型の設定例
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- セキュリティ例外型の設定例
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA

6）［適用（A)］＞［OK］をクリックする。
7）グループポリシーオブジェクトエディタを閉じ、システムを再起動する。

## 3. 設定内容の確認方法

TLS 暗号設定 サーバ設定編の「7. 設定内容の確認方法」を参照されたい。
https://www.ipa.go.jp/security/ipg/documents/tls_server_config_20200707.pdf

## 4. 修正履歴

- 2020.10.20 (ver 1.1)
  「1.1. プロトコルバージョンの設定方法」の推奨セキュリティ型の誤植修正