

# **TLS 暗号設定**

**サーバ設定編 & 暗号スイートの設定例**

**(Windows IIS 用 ver2.0)**

令和 6 年 3 月

独立行政法人 情報処理推進機構

## 目次

1.	サーバ設定方法のまとめ .....	2
1.1.	プロトコルバージョンの設定方法 .....	2
1.2.	HTTP Strict Transport Security (HSTS) の設定方法 .....	2
1.3.	OCSP stapling の設定方法 .....	4
2.	暗号スイート設定例のまとめ .....	4
3.	設定内容の確認方法 .....	6
4.	修正履歴 .....	6

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

現在サポートされている OS バージョンにおける、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
2023 年 9 月の Windows 11 Insider Preview 以降	○	○	▼	▼	▼	×
Windows Server, Windows Server 2022 以降, 2023 年 9 月の Windows 11 Insider Preview よりも前の Windows 11	○	○	○	○	▼	×
Windows Server 2019 以前, Windows 10	×	○	○	○	▼	×

凡例：○：サポートあり ×：サポートなし ▼：サポートしているが既定で無効

詳細なサポート状況および最新の状況については、マイクロソフトの公式情報 [TLS/SSL のプロトコル \(Schannel SSP\) - Win32 apps | Microsoft Learn](https://learn.microsoft.com/ja-jp/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp) を参照すること。

[https://learn.microsoft.com/ja-jp/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-](https://learn.microsoft.com/ja-jp/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp)

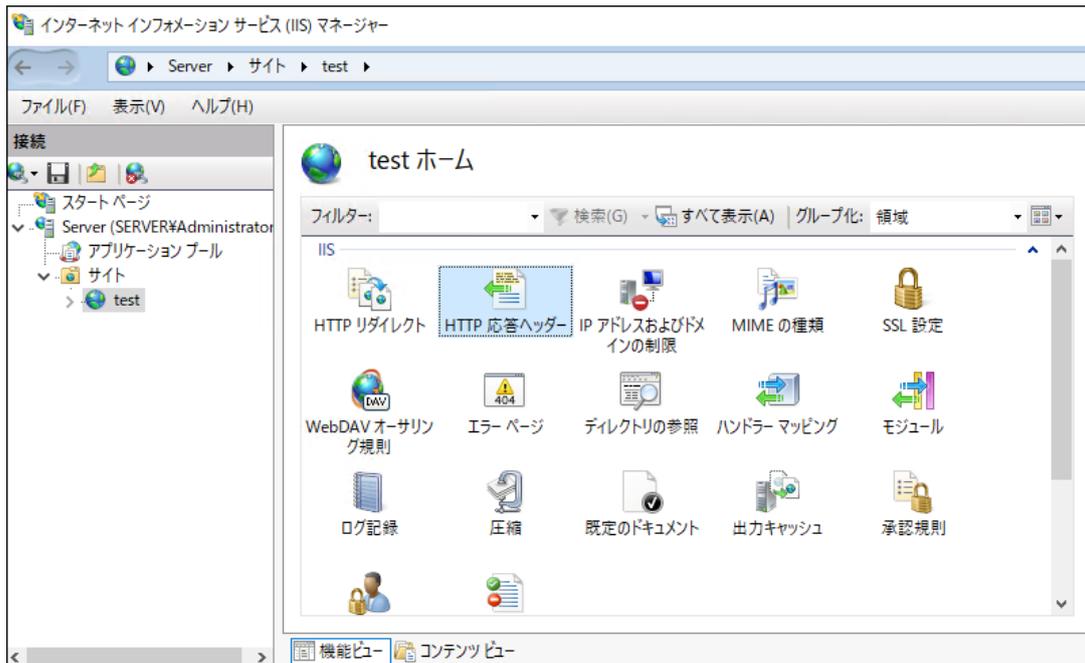
また、暗号化アルゴリズムとプロトコルを制限する方法については、[暗号化アルゴリズムとプロトコルを制限する - Windows Server | Microsoft Learn](https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/restrict-cryptographic-algorithms-protocols-schannel) を参照すること。

<https://learn.microsoft.com/ja-jp/troubleshoot/windows-server/certificates-and-public-key-infrastructure-pki/restrict-cryptographic-algorithms-protocols-schannel>

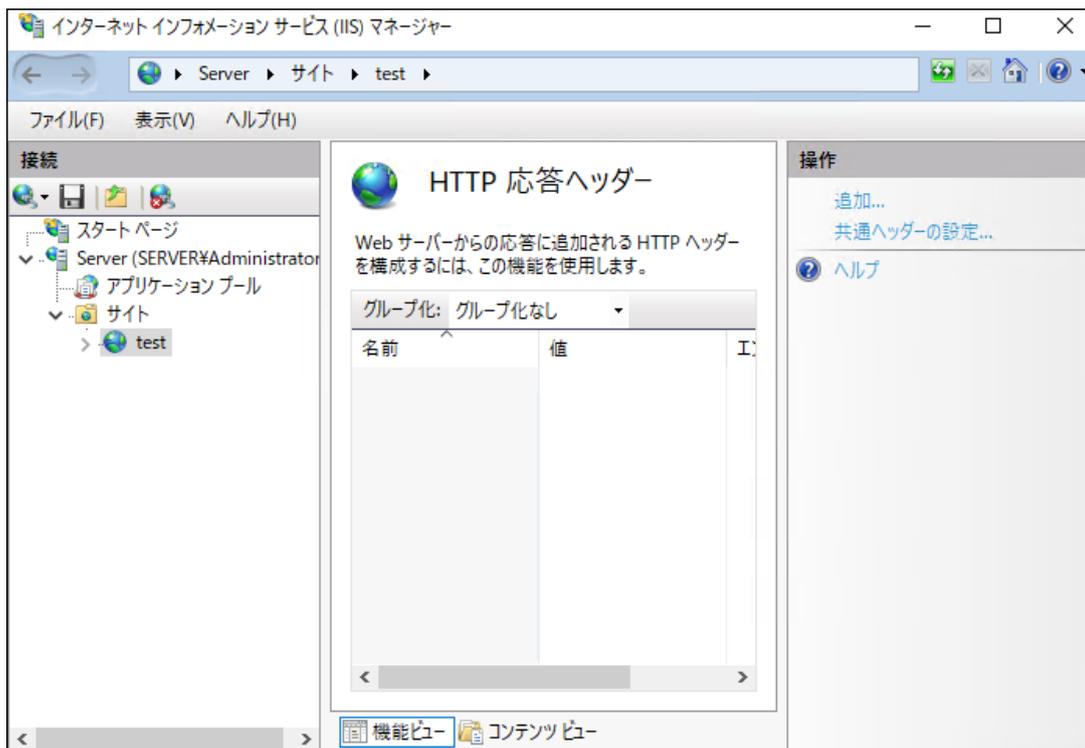
### 1.2. HTTP Strict Transport Security (HSTS) の設定方法

HTTP ヘッダーに HSTS の情報を追加するために、以下の手順により設定する。本設定例では、Windows Server 2022 で GUI を利用した設定を示している。

- 1) 「IIS マネージャー」を開く。
- 2) 左側のペインで、HSTS を有効にするサイトをクリックして選択する。
- 3) 右側のペインで、「機能ビュー」のカテゴリから「HTTP 応答ヘッダー」をダブルクリックする。



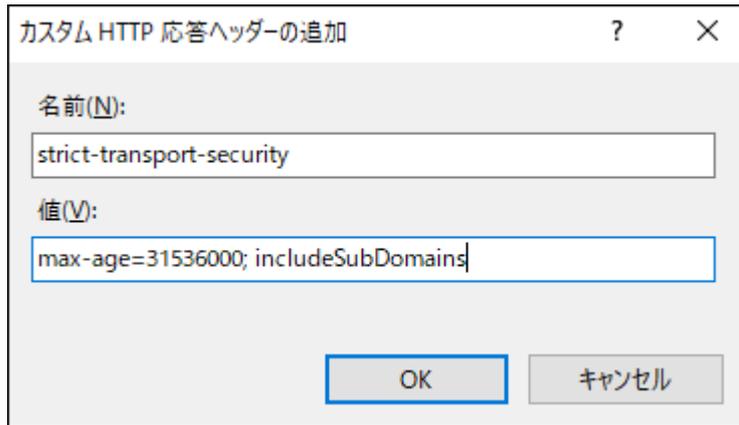
4) 「操作」のペインで「追加」をクリックする。



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

現在サポートされている Windows では、既定で 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 11 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<sup>[1]</sup>。

TLS/SSL (Schannel SSP) の暗号スイート

<https://learn.microsoft.com/ja-jp/windows/win32/secauthn/cipher-suites-in-schannel>

- 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。

---

<sup>[1]</sup> Windows Server 2012, 2016, 2019 及び 2022 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。

PowerShell を使用して構成する場合は、マイクロソフトの公式ドキュメント、[TLS/SSL \(Schannel SSP\) の暗号スイート - Win32 apps | Microsoft Learn](#) から、設定する対象の OS の

ページを参照し、リンクされている「コマンドレット」のページを確認すること。

<https://learn.microsoft.com/ja-jp/windows/win32/secauthn/cipher-suites-in-schannel>

### 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\\_20240617.pdf](https://www.ipa.go.jp/security/ipg/documents/tls_server_config_20240617.pdf)

### 4. 修正履歴

修正日	修正内容
2020.7.17 (Ver.1.0)	初版発行
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
2024.3.31 (Ver.2.0)	● Windows OS における TLS プロトコルバージョンのサポート状況および OCSP stapling の設定状況を更新 ● 「暗号化アルゴリズムと TLS プロトコルバージョンの制限方法」および「暗号スイートの設定」に関するマイクロソフトの公式情報へのリンクを更新