SSL/TLS 暗号設定 暗号スイートの設定例

平成 27 年 8 月

独立行政法人 情報処理推進機構
国立研究開発法人 情報通信研究機構

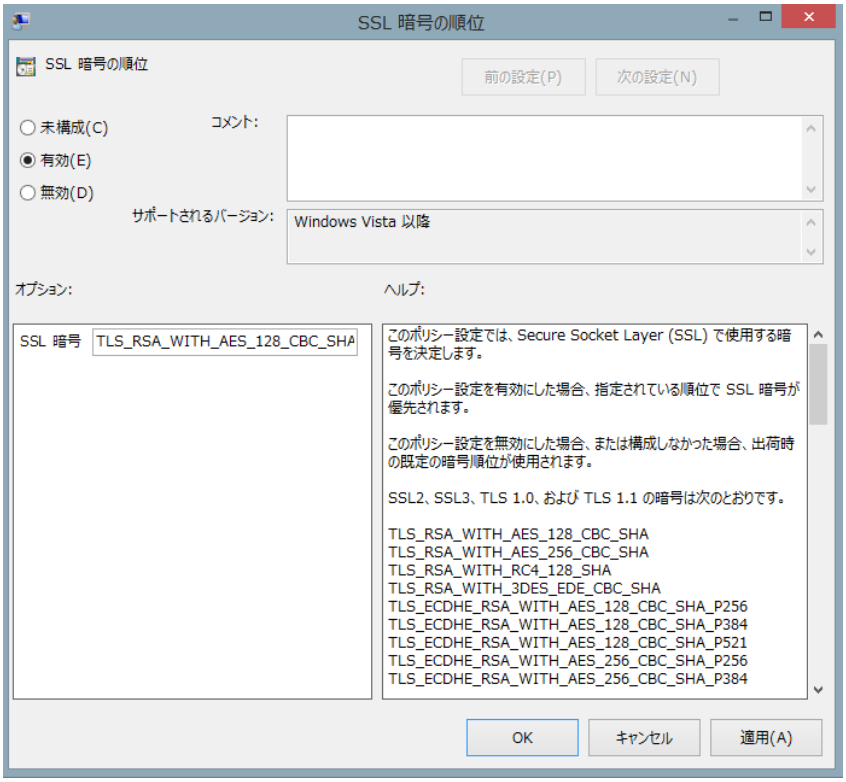
目次

本書では、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。

なお、利用するバージョンやディストリビューションの違いにより、実装されている暗号スイートの種類や設定方法が異なる場合があることに留意すること。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. Windows での設定例[1]

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。



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。

[1] Windows Server 2008, 2008 R2, 2012, 2012 R2 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/

- 高セキュリティ型の設定例（楕円曲線暗号あり）
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256

- 推奨セキュリティ型の設定例（楕円曲線暗号あり）
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA

- セキュリティ例外型の設定例（楕円曲線暗号あり）
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_3DES_EDE_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。

2. OpenSSL 系での設定例

2.1. Apache, lighttpd, nginx の場合

Apache、lighttpd、nginx での暗号スイートの設定においては、2.2 節の OpenSSL での暗号スイート設定例に従った設定を行う。

- Apache の場合の記述
  2.2 節に従い、VirtualHost 中の SSLCipherSuite の設定を以下のように追記する。
  SSLCipherSuite "暗号スイート設定例"
- lighttpd の場合の記述
  2.2 節に従い、$SERVER 中の ssl.cipher-list の設定を以下のように追記する。

ssl.cipher-list = "暗号スイート設定例"

- nginx
  2.2 節に従い、server 中の ssl_ciphers の設定を以下のように追記する。
  ssl_ciphers "暗号スイート設定例";

2.2. OpenSSL 系での暗号スイートの設定例

OpenSSL 系では、ガイドライン 6.5 節に記載する暗号スイート名に対応する独自の表記を利用する（表 1 参照）。

〔SSLCipherSuite "暗号スイート設定例"の表記方法〕
例えば、高セキュリティ型の設定例（基本）なら
SSLCipherSuite "DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256"
と表記する。

なお、OpenSSL では暗号スイートの設定をパターンによる表記[2]で簡略化して記載することができる。ただし、パターンによる設定は、ガイドライン 6.5 節に記載する詳細要求設定に従った設定を行うことが難しいため、本ガイドラインでは取り上げない。

- 高セキュリティ型の設定例（基本[3]）
  DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256

- 高セキュリティ型の設定例（楕円曲線暗号あり[4]）
  ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256

- 推奨セキュリティ型の設定例（基本[5]）
  DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:CAMELLIA128-SHA:AES128-SHA:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA

[2] 「ECDHE+AESGCM:DHE+CAMELLIA:DHE+AES:!DSS:!DH:!PSK:!SRP」のような表記をパターンによる表記という
[3] 「DHE+AESGCM:!DSS:!PSK:!SRP」での設定パターンによる暗号スイートをガイドライン 6.5.1 節の優先順位に合わせたもの
[4] 「ECDHE+AESGCM:EDH+AESGCM:!DSS:!PSK:!SRP」での設定パターンによる暗号スイートをガイドライン 6.5.1 節の優先順位に合わせたもの
[5] 「DHE+AESGCM:RSA+AESGCM:DHE+CAMELLIA:DHE+AES:RSA+CAMELLIA:RSA+AES:!DSS:!PSK:!SRP」での設定パターンによる暗号スイートをガイドライン 6.5.2 節の優先順位に合わせたもの

256-SHA:DHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA:AES256-SHA

- 推奨セキュリティ型の設定例（楕円曲線暗号あり[6]）
  ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:CAMELLIA128-SHA:AES128-SHA:ECDH-ECDSA-AES128-GCM-SHA256:ECDH-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA:DHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA:AES256-SHA:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384

- セキュリティ例外型の設定例（基本[7]）
  DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:CAMELLIA128-SHA:AES128-SHA:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA:DHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:CAMELLIA256-SHA:AES256-SHA:RC4-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA

[6]
「ECDHE+AESGCM:DHE+AESGCM:RSA+AESGCM:DHE+CAMELLIA:DHE+AES:RSA+CAMELLIA:RSA+AES:ECDH+AESGCM:!DSS:!PSK:!SRP」での設定パターンによる暗号スイートをガイドライン 6.5.2 節の優先順位に合わせたもの

[7]
「DHE+AESGCM:RSA+AESGCM:DHE+CAMELLIA:DHE+AES:RSA+CAMELLIA:RSA+AES:RC4-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:!DSS:!PSK:!SRP」での設定パターンによる暗号スイートをガイドライン 6.5.3 節の優先順位に合わせたもの

表 1　代表的な暗号スイートの対比表

ガイドライン 6.5 節に記載する暗号スイート名	OpenSSL での暗号スイート名表記
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_CAMELLIA_256_SHA	CAMELLIA256-SHA
TLS_RSA_WITH_CAMELLIA_128_SHA	CAMELLIA128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA