

TLS 暗号設定 暗号スイートの設定例

Ver 2.0

令和 6 年 6 月

独立行政法人 情報処理推進機構

目次

1.	OpenSSL 系での設定例.....	2
1.1.	OpenSSL の設定.....	2
1.1.1.	OpenSSL 系での暗号スイートの設定例.....	2
1.1.2.	一般的な名称と OpenSSL での名称の対応表.....	5
1.2.	アプリケーションの設定	7
1.2.1.	Apache+mod_ssl の設定.....	7
1.2.2.	lighttpd の設定	7
1.2.3.	nginx の設定	8
2.	GnuTLS 系での設定例について	8
3.	修正履歴	9

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。

本書は以下のソフトウェアバージョンを対象として作成された。採用したバージョンについて、OpenSSL は 2024 年 4 月 1 日時点で最新の LongTermSupport 版¹とし、それ以外のソフトウェアは同時点の最新安定版とした。

OpenSSL 3.0.13

Apache httpd 2.4.58

lighttpd 1.4.75

nginx 1.24.0

なお、mod_gnutls は 2023 年 10 月にリリースされた Apache 2.4.58 ではサポートが廃止されているため、本書では GnuTLS、及び mod_gnutls での設定例の説明を削除した。GnuTLS での設定例を確認する場合はアーカイブの Ver.1.0 を参考にされたい。

1. OpenSSL 系での設定例

1.1. OpenSSL の設定

nginx が TLS1.3 暗号スイートの設定に対応したことを受け、本書が対象とする上記のソフトウェアでは旧 1.1.2 節で記載されていた方法を使用する必要がなくなったため、Ver.1.0 での 1.1.2 節「設定ファイルを用いた TLS1.3 暗号スイートの設定」を削除した。

1.1.1. OpenSSL 系での暗号スイートの設定例

本節では、Ver.1.0 で記載されていた TLS1.2 以前でのパターン名による設定例のままでは TLS 暗号設定ガイドライン Ver 3.1 での CCM、CCM_8 の優先順位の扱いに準拠しない部分が生じるため、Ver.1.0 から該当の設定例を変更した。

[TLS1.3 用暗号スイート設定文字列]

TLS1.3 でサポートする暗号スイートは、コロン(:)で区切られた暗号スイート名を並べた文字列によって指定する。このとき、先頭に記載されたものがより高い優先順位を持つ。

以下にガイドラインに適合する TLS1.3 用の暗号スイートの設定例を示す。これはガイドラインに記載されたもののうち極力多くをサポートする設定例であるため、必要に応じて一部を削除することも可能である。

¹ サポート期限が 2026 年 9 月 7 日までと安定版の中で最も長い。

- 推奨セキュリティ型、セキュリティ例外型の設定例

TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_SHA256:TLS_AES_128_CCM_8_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256

- 高セキュリティ型の設定例

TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_SHA256:TLS_AES_128_CCM_8_SHA256

[TLS1.2 以前用暗号スイート設定文字列]

TLS1.2 以前でサポートする暗号スイートは、コロン(:)で区切られた以下の要素を並べた文字列によって暗号スイートのリストを設定する。この文字列は左から順に処理され、最終的にリストの先頭に存在する暗号スイートがより高い優先順位を持つ。

- OpenSSL 独自の暗号スイート名（1.1.2 節参照）による指定

- 暗号スイートのリストに、順に特定の暗号スイートが追加される

- 個別の暗号スイート名に代えた「ECDHE」「ECDHE+AESGCM」といったパターン

- 暗号スイートのリストに該当する暗号スイートがすべて追加される

- 「+」によって複数のパターン名が連結された場合、それらの共通部分が対象となる

- パターン名のうち、特に混同に注意が必要なものを以下に示す

- ✧ kRSA RSA 鍵交換を使用する暗号スイート
(TLS_RSA_WITH_AES_128_CBC_SHA など)

- ✧ aRSA RSA 認証を使用する暗号スイート
(kRSA のものに加えて TLS_DHE_RSA_WITH_AES_128_CBC_SHA など)

- 前述の 2 つの記法に「+」「-」「!」を前置した暗号スイートのリストの操作

- 「+」を前置した場合、リスト中の該当する暗号スイートがその時点での優先順位最下位に移動する

- 「-」を前置した場合、リスト中の該当する暗号スイートがリストから削除される

- 「!」を前置した場合、リスト中の該当する暗号スイートがリストから削除され、該当する暗号スイートはリストに追加することが不可能になる

以下にガイドラインの各型に適合する TLS1.2 以前用の暗号スイートの設定例を示す。これらはガイドラインに記載されたもののうち極力多くをサポートする設定例であるため、必要に応じて一部を削除することも可能である。

なお、パターン名での設定例で、Ver.1.0 では CCM と CCM8 間で優先順位の指定が行われていなかったため、デフォルトの優先順位により CCM よりも CCM8 が優先されていた。そこで TLS 暗号設定ガイドライン Ver 3.1 で指定されている優先順位に合わせて CCM8 よりも CCM を優先させるため、要所に「+AESCCM8」を挟むように変更した。

また、CCM8 の設定が不要な場合の設定例も（AESCCM8 無効）として以下に示した。

- パターン名による推奨セキュリティ型の設定例

ECDHE+AESGCM:DHE+aRSA+AESGCM:ECHE+AESCCM:DHE+aRSA+AESCCM:+AESCCM8:+AES256:ECHE+CHACHA20:DHE+aRSA+CHACHA20:+DHE:ECHE+AES128:ECHE+CAMELLIA128:ECHE+AES:ECHE+CAMELLIA:+ECHE+SHA:DHE+aRSA+AES128:DHE+aRSA+CAMELLIA128:DHE+aRSA+AES:DH
E+aRSA+CAMELLIA:+DHE+aRSA+SHA

- パターン名による推奨セキュリティ型の設定例（AESCCM8 無効）

ECHE+AESGCM:DHE+aRSA+AESGCM:ECHE+AESCCM:DHE+aRSA+AESCCM:+AES256:ECHE+CHACHA20:DHE+aRSA+CHACHA20:+DHE:ECHE+AES128:ECHE+CAMELLIA128:ECHE+AES:ECHE+CAMELLIA:+ECHE+SHA:DHE+aRSA+AES128:DHE+aRSA+CAMELLIA128:DHE+aRSA+AES:DHE+aRSA+CAMELLIA:+DHE+aRSA+SHA:-AESCCM8

- パターン名による高セキュリティ型の設定例

ECHE+AESGCM:DHE+aRSA+AESGCM:ECHE+AESCCM:DHE+aRSA+AESCCM:+AESCCM8:ECHE+CHACHA20:DHE+aRSA+CHACHA20:+AES128:+DHE

- パターン名による高セキュリティ型の設定例（AESCCM8 無効）

ECHE+AESGCM:DHE+aRSA+AESGCM:ECHE+AESCCM:DHE+aRSA+AESCCM:ECHE+CHACHA20:DHE+aRSA+CHACHA20:+AES128:+DHE:-AESCCM8

- パターン名によるセキュリティ例外型の設定例

DHE+aRSA+AESGCM:ECHE+AESGCM:DHE+aRSA+AESCCM:ECHE+AESCCM:+AESCCM8:+AES256:DHE+aRSA+CHACHA20:ECHE+CHACHA20:kRSA+AESGCM:kRSA+AESCCM:+kRSA+AESCCM8:+kRSA+AES256:DHE+aRSA+AES128:DHE+aRSA+CAMELLIA128:+DHE+aRSA+SHA:ECHE+AES128:ECHE+CAMELLIA128:+ECHE+SHA:DHE+aRSA+AES256:DHE+aRSA+CAMELLIA256:+DHE+aRSA+AES256+SHA:+DHE+aRSA+CAMELLIA256+SHA:ECHE+AES256:ECHE+CAMELLIA256:+ECHE+AES256+SHA:kRSA+AES128:kRSA+CAMELLIA128:+kRSA+SHA:kRSA+AES:kRSA+CAMELLIA:+kRSA+AES256+SHA:+kRSA+CAMELLIA256+SHA

- パターン名によるセキュリティ例外型の設定例（AESCCM8 無効）

DHE+aRSA+AESGCM:ECHE+AESGCM:DHE+aRSA+AESCCM:ECHE+AESCCM:+AES256:DHE+aRSA+CHACHA20:ECHE+CHACHA20:kRSA+AESGCM:kRSA+AESCCM:+kRSA+AES256:DHE+aRSA+AES128:DHE+aRSA+CAMELLIA128:+DHE+aRSA+SHA:ECHE+AES128:ECHE+CAMELLIA128:+ECHE+SHA:DHE+aRSA+AES256:DHE+aRSA+CAMELLIA256:+DHE+aRSA+AES256+SHA:+DHE+aRSA+CAMELLIA256+SHA:ECHE+AES256:ECHE+CAMELLIA256:+ECHE+AES256+SHA:kRSA+AES128:kRSA+CAMELLIA128:+kRSA+SHA:kRSA+AES:kRSA+CAMELLIA:+kRSA+AES256+SHA:+kRSA+CAMELLIA256+SHA:-AESCCM8

- 暗号スイート名による推奨セキュリティ型の設定例

ECHE-ECDSA-AES128-GCM-SHA256:ECHE-RSA-AES128-GCM-SHA256:ECHE-ECDSA-AES128-CCM:ECHE-ECDSA-AES128-CCM8:ECHE-ECDSA-AES256-GCM-SHA384:ECHE-RSA-AES256-GCM-SHA384:ECHE-ECDSA-AES256-CCM:ECHE-ECDSA-AES256-CCM8:ECHE-ECDSA-CHACHA20-POLY1305:ECHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-CCM:DHE-RSA-AE

S128-CCM8:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-CCM:DHE-RSA-AES256-CCM8:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA256-SHA

- 暗号スイート名による高セキュリティ型の設定例

ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES256-CCM8:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-CCM:ECDHE-ECDSA-AES128-CCM8:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-CCM:DHE-RSA-AES256-CCM8:DHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-CCM:DHE-RSA-AES128-CCM8

- 暗号スイート名によるセキュリティ例外型の設定例

DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-CCM:ECDHE-ECDSA-AES128-CCM:DHE-RSA-AES128-CCM8:ECDHE-ECDSA-AES128-CCM8:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-CCM:ECDHE-ECDSA-AES256-CCM:DHE-RSA-AES256-CCM8:ECDHE-ECDSA-AES256-CCM8:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:AES128-GCM-SHA256:AES128-CCM:AES128-CCM8:AES256-GCM-SHA384:AES256-CCM:AES256-CCM8:DHE-RSA-AES128-SHA256:DHE-RSA-CAMELLIA128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-CAMELLIA128-SHA256:ECDHE-RSA-CAMELLIA128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-CAMELLIA256-SHA384:ECDHE-RSA-CAMELLIA256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:AES128-SHA256:CAMELLIA128-SHA256:AES128-SHA:CAMELLIA128-SHA:AES256-SHA256:CAMELLIA256-SHA256:AES256-SHA:CAMELLIA256-SHA

1.1.2. 一般的な名称と OpenSSL での名称の対応表

本節は Ver.1.0 からの変更はない。

ガイドラインでの暗号スイート名表記	OpenSSL での暗号スイート名表記
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_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_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	ECDHE-ECDSA-AES128-CCM
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	ECDHE-ECDSA-AES256-CCM
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	ECDHE-ECDSA-AES128-CCM8
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	ECDHE-ECDSA-AES256-CCM8
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	非対応
TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	非対応
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	非対応
TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	非対応
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305
TLS_DHE_RSA_WITH_AES_128_CCM	DHE-RSA-AES128-CCM
TLS_DHE_RSA_WITH_AES_256_CCM	DHE-RSA-AES256-CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8	DHE-RSA-AES128-CCM8
TLS_DHE_RSA_WITH_AES_256_CCM_8	DHE-RSA-AES256-CCM8
TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	非対応
TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	非対応
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	非対応
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	非対応
TLS_RSA_WITH_AES_128_CCM	AES128-CCM
TLS_RSA_WITH_AES_256_CCM	AES256-CCM
TLS_RSA_WITH_AES_128_CCM_8	AES128-CCM8
TLS_RSA_WITH_AES_256_CCM_8	AES256-CCM8
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	ECDHE-ECDSA-CAMELLIA128-SHA256
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	ECDHE-RSA-CAMELLIA128-SHA256
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	ECDHE-ECDSA-CAMELLIA256-SHA384
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	ECDHE-RSA-CAMELLIA256-SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	DHE-RSA-CAMELLIA128-SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	DHE-RSA-CAMELLIA256-SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	CAMELLIA128-SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	CAMELLIA256-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA

1.2. アプリケーションの設定

1.2.1. Apache+mod_ssl の設定

1.1.1 節に従い、各<VirtualHost>中の SSLCipherSuite を以下のように設定する。本節は Ver.1.0 からの変更はない。

SSLCipherSuite "TLS1.2 以前用暗号スイート設定文字列"

SSLCipherSuite TLSv1.3 "TLS1.3 用暗号スイート設定文字列"

1.2.2. lighttpd の設定

1.1.1 節に従い、各\$SERVER["socket"]によるポート設定中の ssl.cipher-list および ssl.openssl.ssl-conf-cmd を以下のように設定する。公式で推奨されている設定方法が変更されたため、本節では Ver.1.0 から TLS1.2, TLS1.3 それぞれでの設定方法を修正した。

ssl.openssl.ssl-conf-cmd += ("CipherString" => "TLS1.2 以前用暗号スイート設定文字列")

ssl.openssl.ssl-conf-cmd += ("Ciphersuites" => "TLS1.3 用暗号スイート設定文字列")

1.2.3. nginx の設定

1.1.1 節に従い、各 server 中の `ssl_ciphers` を以下のように設定する。nginx が TLS1.3 暗号スイートに対応したため、本節では Ver.1.0 から TLS1.3 での設定方法を追記した。

```
ssl_ciphers "TLS1.2 以前用暗号スイート設定文字列";  
ssl_conf_command Ciphersuites "TLS1.3 暗号スイート用文字列";
```

2. GnuTLS 系での設定例について

前書きに記載した通り、`mod_gnutls` は Apache 2.4.58 では公式にサポートが行われていないため、本書では GnuTLS 及び `mod_gnutls` での設定例の記載を削除した。該当ソフトウェアの設定例についてはアーカイブの Ver.1.0 を参照されたい。

3. 修正履歴

修正日	修正内容
2020.7.7 (Ver.1.0)	初版発行
2024.6.17 (Ver.2.0)	<ul style="list-style-type: none">● 最新安定版のバージョンのライブラリ、ソフトウェアを利用した内容に更新● mod_gnutls の公式メンテナンスが廃止されたため、対象ソフトウェアから mod_gnutls 及び GnuTLS を削除。それに従って関連する節を削除● 「1.1.1 OpenSSL 系での暗号スイートの設定例」にて、TLS1.2 以前での各パターン名による設定例を TLS 暗号設定ガイドライン Ver.3.1 に記載されている優先順に準拠するよう修正