SSLの暗号スイート

SSL HTTPS

この記事は最終更新日から3年以上が経過しています。

はじめに

最近ではGoogle及び各ブラウザがHTTPSを推奨しています。WebサイトをHTTPSで運用している場合、SSLの暗号スイートの設定が欠かせません。しかし、下手に設定するとせっかくHTTPSを利用したのに肝心の安全性が台無しになります。ここでは、そのSSLの暗号スイートの指定方法についてまとめます。

基本的な書き方

暗号スイートは `A:B:C:・・・` のように、各スイートをコロンで区切って書きます。 `A`，`B`，`C`，・・・はそれぞれ次のようにして指定します。

暗号名単体(例: AES・AESGCM・ECDSA・ECDHE・RSAなど)

その暗号を使用する**全ての**暗号スイートをリストの**末尾に**追加します。強固なものから脆弱なものまで、該当するなら全て追加されます。

例: AESを使用する暗号スイートの末尾に3DESを使用する暗号スイートを追加

```
$ openssl ciphers -v 'AESGCM:3DES'
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
DH-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH/DSS   Au=DH   Enc=AESGC
DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=DSS  Enc=AESG
DH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH/RSA   Au=DH   Enc=AESGC
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=RSA  Enc=AESG
ADH-AES256-GCM-SHA384   TLSv1.2 Kx=DH       Au=None Enc=AESGCM
ECDH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AES
ECDH-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc
AES256-GCM-SHA384       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
DH-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH/DSS   Au=DH   Enc=AESGC
DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=DSS  Enc=AESG
```

```
DH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH/RSA   Au=DH   Enc=AESGCM
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM
ADH-AES128-GCM-SHA256   TLSv1.2 Kx=DH       Au=None Enc=AESGCM
ECDH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/RSA Au=ECDH Enc=AESGCM
ECDH-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH/ECDSA Au=ECDH Enc=
AES128-GCM-SHA256       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM
ECDHE-RSA-DES-CBC3-SHA  SSLv3 Kx=ECDH     Au=RSA  Enc=3DES(168
ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH     Au=ECDSA Enc=3DES(1
SRP-DSS-3DES-EDE-CBC-SHA SSLv3 Kx=SRP      Au=DSS  Enc=3DES(16
SRP-RSA-3DES-EDE-CBC-SHA SSLv3 Kx=SRP      Au=RSA  Enc=3DES(16
SRP-3DES-EDE-CBC-SHA    SSLv3 Kx=SRP      Au=SRP  Enc=3DES(168
EDH-RSA-DES-CBC3-SHA    SSLv3 Kx=DH       Au=RSA  Enc=3DES(168
EDH-DSS-DES-CBC3-SHA    SSLv3 Kx=DH       Au=DSS  Enc=3DES(168
DH-RSA-DES-CBC3-SHA     SSLv3 Kx=DH/RSA   Au=DH   Enc=3DES(168
DH-DSS-DES-CBC3-SHA     SSLv3 Kx=DH/DSS   Au=DH   Enc=3DES(168
AECDH-DES-CBC3-SHA      SSLv3 Kx=ECDH     Au=None Enc=3DES(168
ADH-DES-CBC3-SHA        SSLv3 Kx=DH       Au=None Enc=3DES(168
ECDH-RSA-DES-CBC3-SHA   SSLv3 Kx=ECDH/RSA Au=ECDH Enc=3DES(168
ECDH-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=3DES(1
DES-CBC3-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168
PSK-3DES-EDE-CBC-SHA    SSLv3 Kx=PSK      Au=PSK  Enc=3DES(168
```

よく使うものを次の表に記載します。

文字列	意味
AES	AESで本文の暗号化を行う暗号化スイート(AESGCMも含む)
AES128	128bitのAESで本文の暗号化を行う暗号化スイート(AESGCMも含む)

文字列	意味
AES256	256bitのAESで本文の暗号化を行う暗号化スイート(AESGCMも含む)
AESGCM	AES(GCMモード)で本文を暗号化する暗号化スイート(普通のAESよりも安全なので最優先推奨)
3DES	3DES(AESより前時代の暗号であるDESで3回暗号化する)で本文を暗号化する暗号化スイート(AESより遅い&強度が落ちるためXP以前のIE対策限定)
kRSA	RSAで鍵交換を行う暗号化スイート(優先度は最低)
ECDHE	楕円曲線ディフィー・ヘルマン鍵共有で鍵交換を行う暗号化スイート(鍵交換は原則これを第一優先とすべき)
DHE	ディフィー・ヘルマン鍵共有で鍵交換を行う暗号化スイート(優先度はECDHEkとRSAの中間)
aRSA	RSAで認証を行う暗号化スイート(SSLの証明書がRSAの場合に指定)
RSA	kRSA と aRSA のいずれかに該当する暗号化スイート
ECDSA	ECDSAで認証を行う暗号化スイート(SSLの証明書がECDSAの場合に指定)
SSLv3	SSL3.0以降で使用できる暗号スイート(MAC(メッセージ認証符号)にSHA1を使用しているため**優先度は最低**)
TLSv1.2	TLS1.2以降で使用できる暗号スイート(MACにSHA2を使用しているためこちらを優先)

複数の暗号を+ではさむ(例: AES+ECDHE)

該当するすべての暗号を使用する暗号スイートを全てリストの末尾に追加します。

```
$ openssl ciphers -v 'AESGCM+DH'
DH-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH/DSS   Au=DH   Enc=AESGCM
DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=DSS  Enc=AESGCM
DH-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH/RSA   Au=DH   Enc=AESGCM
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM
ADH-AES256-GCM-SHA384   TLSv1.2 Kx=DH       Au=None Enc=AESGCM
DH-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH/DSS   Au=DH   Enc=AESGCM
DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=DSS  Enc=AESGCM
DH-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH/RSA   Au=DH   Enc=AESGCM
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=RSA  Enc=AESGCM
ADH-AES128-GCM-SHA256   TLSv1.2 Kx=DH       Au=None Enc=AESGCM
```

特定の暗号スイートの優先度を最低にする

次のリストからAES256bitを使用している暗号スイートをリストの末尾に移動したいとします。

```
$ openssl ciphers -v 'AES+ECDHE'
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=
```

```
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(25
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-RSA-AES256-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(256)
ECDHE-ECDSA-AES256-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(256
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(12
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-RSA-AES128-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(128)
ECDHE-ECDSA-AES128-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(128
```

その場合、末尾に +AES256 を追加します。 + の後に暗号名を書くと、リストに入っていてその暗号を使用している暗号スイートがリストの末尾に移動します。

```
$ openssl ciphers -v 'AES+ECDHE:+AES256'
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(12
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-RSA-AES128-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(128)
ECDHE-ECDSA-AES128-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(128
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(25
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
```

```
ECDHE-RSA-AES256-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(256)
ECDHE-ECDSA-AES256-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(256
```

さらに、SHA1をMACに使用している暗号化スイートもリストの末尾に移動します。

```
$ openssl ciphers -v 'AES+ECDHE:+AES256:+SSLv3'
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(12
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(25
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-RSA-AES128-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(128)
ECDHE-ECDSA-AES128-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(128
ECDHE-RSA-AES256-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(256)
ECDHE-ECDSA-AES256-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(256
```

この場合、優先度はAES256bit > SHA1となります。

特定の暗号スイートをリストから外す

次のリストからRC4を外すことを考えてみます。

```
$ openssl ciphers -v 'MEDIUM'
DHE-RSA-SEED-SHA        SSLv3 Kx=DH       Au=RSA  Enc=SEED(128
DHE-DSS-SEED-SHA        SSLv3 Kx=DH       Au=DSS  Enc=SEED(128
DH-RSA-SEED-SHA         SSLv3 Kx=DH/RSA   Au=DH   Enc=SEED(128
DH-DSS-SEED-SHA         SSLv3 Kx=DH/DSS   Au=DH   Enc=SEED(128
ADH-SEED-SHA            SSLv3 Kx=DH       Au=None Enc=SEED(128
SEED-SHA                SSLv3 Kx=RSA      Au=RSA  Enc=SEED(128
IDEA-CBC-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=IDEA(128
ECDHE-RSA-RC4-SHA       SSLv3 Kx=ECDH     Au=RSA  Enc=RC4(128)
ECDHE-ECDSA-RC4-SHA     SSLv3 Kx=ECDH     Au=ECDSA Enc=RC4(128
AECDH-RC4-SHA           SSLv3 Kx=ECDH     Au=None Enc=RC4(128)
ADH-RC4-MD5             SSLv3 Kx=DH       Au=None Enc=RC4(128)
ECDH-RSA-RC4-SHA        SSLv3 Kx=ECDH/RSA Au=ECDH Enc=RC4(128)
ECDH-ECDSA-RC4-SHA      SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=RC4(12
RC4-SHA                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)
RC4-MD5                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)
PSK-RC4-SHA             SSLv3 Kx=PSK      Au=PSK  Enc=RC4(128)
```

現在のリストから一時的に外す場合には -RC4 を追加します。

```
$ openssl ciphers -v 'MEDIUM:-RC4'
DHE-RSA-SEED-SHA        SSLv3 Kx=DH       Au=RSA  Enc=SEED(128
DHE-DSS-SEED-SHA        SSLv3 Kx=DH       Au=DSS  Enc=SEED(128
DH-RSA-SEED-SHA         SSLv3 Kx=DH/RSA   Au=DH   Enc=SEED(128
DH-DSS-SEED-SHA         SSLv3 Kx=DH/DSS   Au=DH   Enc=SEED(128
ADH-SEED-SHA            SSLv3 Kx=DH       Au=None Enc=SEED(128
SEED-SHA                SSLv3 Kx=RSA      Au=RSA  Enc=SEED(128
IDEA-CBC-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=IDEA(128
```

しかし、 - で除外すると、再びリストに追加されてしまうことがありえます。

```
$ openssl ciphers -v 'MEDIUM:-RC4:MEDIUM'
DHE-RSA-SEED-SHA        SSLv3 Kx=DH       Au=RSA  Enc=SEED(128
DHE-DSS-SEED-SHA        SSLv3 Kx=DH       Au=DSS  Enc=SEED(128
DH-RSA-SEED-SHA         SSLv3 Kx=DH/RSA   Au=DH   Enc=SEED(128
DH-DSS-SEED-SHA         SSLv3 Kx=DH/DSS   Au=DH   Enc=SEED(128
ADH-SEED-SHA            SSLv3 Kx=DH       Au=None Enc=SEED(128
SEED-SHA                SSLv3 Kx=RSA      Au=RSA  Enc=SEED(128
IDEA-CBC-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=IDEA(128
ECDHE-RSA-RC4-SHA       SSLv3 Kx=ECDH     Au=RSA  Enc=RC4(128)
ECDHE-ECDSA-RC4-SHA     SSLv3 Kx=ECDH     Au=ECDSA Enc=RC4(128
```

```
AECDH-RC4-SHA           SSLv3 Kx=ECDH     Au=None Enc=RC4(128)
ADH-RC4-MD5             SSLv3 Kx=DH       Au=None Enc=RC4(128)
ECDH-RSA-RC4-SHA        SSLv3 Kx=ECDH/RSA Au=ECDH Enc=RC4(128)
ECDH-ECDSA-RC4-SHA      SSLv3 Kx=ECDH/ECDSA Au=ECDH Enc=RC4(12
RC4-SHA                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)
RC4-MD5                 SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)
PSK-RC4-SHA             SSLv3 Kx=PSK      Au=PSK  Enc=RC4(128)
```

末尾にRC4が再び追加されています。RC4には二度とリストに追加されてほしくないという場合には、 - の代わりに ! を使用します。

```
$ openssl ciphers -v 'MEDIUM:!RC4:MEDIUM'
DHE-RSA-SEED-SHA        SSLv3 Kx=DH       Au=RSA  Enc=SEED(128
DHE-DSS-SEED-SHA        SSLv3 Kx=DH       Au=DSS  Enc=SEED(128
DH-RSA-SEED-SHA         SSLv3 Kx=DH/RSA   Au=DH   Enc=SEED(128
DH-DSS-SEED-SHA         SSLv3 Kx=DH/DSS   Au=DH   Enc=SEED(128
ADH-SEED-SHA            SSLv3 Kx=DH       Au=None Enc=SEED(128
SEED-SHA                SSLv3 Kx=RSA      Au=RSA  Enc=SEED(128
IDEA-CBC-SHA            SSLv3 Kx=RSA      Au=RSA  Enc=IDEA(128
```

今度はRC4がリストにないことがわかります。

一般サイト用個人的おすすめ設定

設定方針

- 暗号化はAESのみ(PCでハードウェアアクセラレーションが効くため)
- AESGCMが使える場合は最優先
- 鍵交換はECDHE・DHE・RSAのみとし、優先順位はECDHE > DHE > RSA
- 鍵長は128bit優先、256bitは後回し
- TLS1.2で追加された暗号化スイートを優先

以下のコマンドの実行環境

Windows10 + Git Bash + OpenSSL 1.0.2

証明書がRSAで署名されている場合

AESGCM+aRSA:AES+ECDHE+aRSA:AES+DHE+aRSA:AES+kRSA+aRSA:+AES256:+SSLv3 を指定します。

```
$ openssl ciphers -v 'AESGCM+aRSA:AES+ECDHE+aRSA:AES+DHE+aRSA:A
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH       Au=RSA  Enc=AESG
AES128-GCM-SHA256       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(12
DHE-RSA-AES128-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(12
AES128-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(12
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AE
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH       Au=RSA  Enc=AESG
AES256-GCM-SHA384       TLSv1.2 Kx=RSA      Au=RSA  Enc=AESGCM
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=RSA  Enc=AES(25
DHE-RSA-AES256-SHA256   TLSv1.2 Kx=DH       Au=RSA  Enc=AES(25
AES256-SHA256           TLSv1.2 Kx=RSA      Au=RSA  Enc=AES(25
ECDHE-RSA-AES128-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(128)
DHE-RSA-AES128-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(128)
AES128-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)
ECDHE-RSA-AES256-SHA    SSLv3 Kx=ECDH     Au=RSA  Enc=AES(256)
DHE-RSA-AES256-SHA      SSLv3 Kx=DH       Au=RSA  Enc=AES(256)
AES256-SHA              SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)
```

なお、XP版IE用対策のために3DESのサポートを加えたい場合は、末尾に :3DES+aRSA+kRSA を加えます。

証明書がECDSAで署名されている場合

AES+ECDSA:+AES256:+SSLv3 を指定します。ECDSAの証明書を使用する場合、ECDHE以外の鍵交換アルゴリズムは使用できないようです。

```
$ openssl ciphers -v 'AES+ECDSA:+AES256:+SSLv3'
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH     Au=ECDSA Enc=AES
ECDHE-ECDSA-AES128-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(128
ECDHE-ECDSA-AES256-SHA  SSLv3 Kx=ECDH     Au=ECDSA Enc=AES(256
```