SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討

― 調査報告書 別紙 2 ―

付録 B および付録 C に係る改訂案

2018 年 6 月

IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

目次

SSL/TLS 暗号設定ガイドライン付録改訂案

付録 B（Appendix B）および付録 C（Appendix C）に係る記述の改訂案を改訂前後の記載で示す。

記載例は、以下のとおりである。

- 改訂前

  改訂前の SSL/TLS ガイドライン v1.1 の記述である。

  改訂する箇所を黄色いマーカーで示す。

- 改訂後

  SSL/TLS 暗号設定ガイドライン改訂及び鍵管理ガイドライン作成のための調査・検討報告書（以下、報告書）の調査結果を受けて作成した改訂案である。

  改訂した箇所を水色のマーカーで示す。

Appendix B：サーバ設定編

- B.1.1. Apache の場合
  - 改訂前

    Apache HTTP Server の設定ファイル（デフォルトの場合、httpd-ssl.conf）での設定例を以下に示す。

    <VirtualHost *:443>

    （中略）

    SSLEngine on

    証明書と鍵の設定 [1]

    SSLCertificateFile /etc/ssl/chain.crt

    SSLCertificateKeyFile /etc/ssl/server.key

    暗号スイート設定。Appendix C.2 も参照のこと

    SSLCipherSuite "暗号スイート設定"

    プロトコルバージョン設定。Appendix B.2.1 も参照のこと

    SSLProtocol バージョン設定

    暗号スイート順序サーバ優先設定

    SSLHonorCipherOrder On

[1] 設定する内容は以下のとおり。
/etc/ssl/chain.crt：サーバ証明書および中間証明書、/etc/ssl/server.key：サーバ証明書に対応する秘密鍵

HTTP Strict Transport Security、OCSP Stapling、Public Key Pinning の設定をする場合には、ここに追記する。7.2 節及び Appendix B.4 以降も参照のこと

</VirtualHost>

➢ 改訂後

Apache HTTP Server の設定ファイル（デフォルトの場合、httpd-ssl.conf）での設定例を以下に示す。

暗号スイート設定。Appendix C.2 も参照のこと

SSLCipherSuite "暗号スイート設定"

暗号スイート順序サーバ優先設定

SSLHonorCipherOrder On

プロトコルバージョン設定。Appendix B.2.1 も参照のこと

SSLProtocol バージョン設定

<VirtualHost _default_:443>

（中略）

SSLEngine on

（中略）

証明書と鍵の設定 [2]

SSLCertificateFile /etc/ssl/chain.crt

SSLCertificateKeyFile /etc/ssl/server.key

HTTP Strict Transport Security、OCSP Stapling、Public Key Pinning の設定をする場合には、ここに追記する。7.2 節及び Appendix B.4 以降も参照のこと

</VirtualHost>

- B.2.1. Apache の場合
  - ➢ 改訂前
    - セキュリティ例外型

      SSLProtocol All -SSLv2
  - ➢ 改訂後

[2] 設定する内容は以下のとおり。
/etc/ssl/chain.crt：サーバ証明書および中間証明書、/etc/ssl/server.key：サーバ証明書に対応する秘密鍵

- セキュリティ例外型

  SSLProtocol All -SSLv2 +SSLv3

- B.2.2. lighttpd の場合
  - 改訂前

    lighttpd での設定例を以下に示す。

    - 高セキュリティ型

      ssl.use-tlsv1.1 = "disable"

      ssl.use-tlsv1 = "disable"

      ssl.use-sslv3 = "disable"

      ssl.use-sslv2 = "disable"

  - 改訂後

    lighttpd での設定例を以下に示す。

    - 高セキュリティ型

      ssl.openssl.ssl-conf-cmd = ("Protocol" => "-ALL, TLSv1.2")

- B.2.4. Microsoft IIS の場合
  - 改訂前

    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。

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
Windows Server 2008	×	×	○	○	○
Windows Vista	×	×	○	○	○
Windows Server 2008 R2（以降）	○	○	○	○	○
Windows 7 以降の Windows	○	○	○	○	○

    凡例：○ サポートあり　　× サポートなし

    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。

    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

    - 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

- 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

- セキュリティ例外型

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥Schannel¥Protocols¥SSL 2.0¥Server
"DisabledByDefault"=dword:00000001

➢ 改訂後

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。

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
Windows 7	△	△	○	○	○
Windows 8	○	○	○	○	△
Windows 8.1	○	○	○	○	△
Windows 10	○	○	○	▲	△
Windows Server 2008	●	△	○	○	○
Windows Server 2008 R2	△	△	○	○	○
Windows Server 2012	○	○	○	○	△
Windows Server 2012 R2	○	○	○	○	△
Windows Server 2016	○	○	○	△	×

凡例：○ サポートあり
× サポートなし
△ サポートしているが、デフォルトで無効になっているもの
▲ バージョン 1607 以降はデフォルトで無効になったもの
● サポートするアップデート（KB4019276）が適用された場合

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。

参考情報：

Transport Layer Security (TLS) registry settings

https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#ssl-20

						セキュリティ型		
プロトコル	レジストリキー（HKLM¥SYSTEM¥）	名前	型	値	効果	高	推奨	例外
SSL 2.0	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 2.0¥Server	DisabledByDefault	DWORD	00000001	無効化	○	○	○
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 2.0¥Server	Enabled	DWORD	00000000		○	○	○
SSL 3.0	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 3.0¥Server	DisabledByDefault	DWORD	00000001	無効化	○	○	
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 3.0¥Server	Enabled	DWORD	00000000		○	○	
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 3.0¥Server	DisabledByDefault	DWORD	00000000	有効化			○
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 3.0¥Server	Enabled	DWORD	00000001				○
TLS 1.0	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.0¥Server	DisabledByDefault	DWORD	00000001	無効化	○		
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.0¥Server	Enabled	DWORD	00000000		○		
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.0¥Server	DisabledByDefault	DWORD	00000000	有効化		○	○
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.0¥Server	Enabled	DWORD	00000001			○	○
TLS 1.1	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.1¥Server	DisabledByDefault	DWORD	00000001	無効化	○		
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.1¥Server	Enabled	DWORD	00000000		○		
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.1¥Server	DisabledByDefault	DWORD	00000000	有効化			
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.1¥Server	Enabled	DWORD	00000001				
TLS 1.2	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.2¥Server	DisabledByDefault	DWORD	00000000	有効化	○		
	CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥TLS 1.2¥Server	Enabled	DWORD	00000001		○		

凡例　○：設定が必要な項目

補足：

SSL 2.0	Windows 10 バージョン 1607 および Windows Server 2016 以降、SSL 2.0 は削除されサポートされなくなりました。
SSL 3.0	Windows 10 バージョン 1607 および Windows Server 2016 以降、SSL 3.0 はデフォルトで無効になっています。

TLS 1.1	Windows Server 2008 R2 を実行するサーバで TLS 1.1 を有効にしてネゴシエートするには、適切なサブキー（クライアント、サーバ）に DisabledByDefault エントリを作成し、それを "00000000"に設定する必要があります。 エントリはレジストリには表示されず、デフォルトで "00000001" に設定されています。
TLS 1.2	Windows Server 2008 R2 を実行するサーバで TLS 1.2 を有効にしてネゴシエートするには、適切なサブキー（クライアント、サーバ）に DisabledByDefault エントリを作成し、それを "00000000"に設定する必要があります。 エントリはレジストリには表示されず、デフォルトで "00000001" に設定されています。

- B.4.1. Apache の場合
  - 改訂前

    なお、HTTP の場合に強制的に HTTPS にリダイレクトするためには、<VirtualHost *:80>中の RewriteRule、RewriteEngine の設定を以下のように追記する。

    <VirtualHost *:80>

    （中略）

    ServerAlias *

    RewriteEngine On

    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]

    </VirtualHost>
  - 改訂後

    なお、HTTP の場合に強制的に HTTPS にリダイレクトするためには、<VirtualHost *:80>中の RewriteRule、RewriteEngine、RewriteCond の設定を以下のように追記する。

    <VirtualHost *:80>

    （中略）

    ServerAlias *

    RewriteEngine On

    RewriteCond %{HTTPS} off

    RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R,L]

    </VirtualHost>
- B.4.2. lighttpd の場合
  - 改訂前

    setenv.add-response-header = (

    "Strict-Transport-Security" => "max-age=31536000; includeSubDomains"

)
  - 改訂後

    setenv.add-response-header = (

    "Strict-Transport-Security" => "max-age=31536000; includeSubdomains"

)
- B.5.1. Apache の場合
  - 改訂前

    SSLStaplingCache shmcb:/tmp/stapling_cache(128000)

    <VirtualHost *:443>

    （中略）

    SSLCACertificateFile /etc/ssl/ca-certs.pem

SSLUseStapling on

</VirtualHost>

- 改訂後

SSLUseStapling On

SSLStaplingCache shmcb:/tmp/stapling_cache(128000)

SSLStaplingStandardCacheTimeout 3600

SSLStaplingErrorCacheTimeout 600

<VirtualHost *:443>

（中略）

SSLCACertificateFile /etc/ssl/ca-certs.pem

</VirtualHost>

- B.6.1. Apache の場合
  - 改訂前

B.6 の表記に従い、mod_headers モジュールを有効にし、以下の設定を追加する。

Header always set Public-Key-Pins 'pin-sha256="証明書の公開鍵情報の SHA-256 ハッシュ値（pinned　fingerprint）の Base64 値"; pin-sha256="バックアップのための公開鍵情報の SHA-256 ハッシュ値（backup pinned fingerprint）の Base64 値"; max-age=有効期間'

ちなみに、mod_headers モジュールを有効にするためには、httpd.conf において

LoadModule headers_module modules/mod_headers.so

を設定する。

  - 改訂後

Apache 2.4 未満の場合は、

B.6 の表記に従い、mod_headers モジュールを有効にし、以下の設定を追加する。

Header always set Public-Key-Pins 'pin-sha256="証明書の公開鍵情報の SHA-256 ハッシュ値（pinned　fingerprint）の Base64 値"; pin-sha256="バックアップのための公開鍵情報の SHA-256 ハッシュ値（backup pinned fingerprint）の Base64 値"; max-age=有効期間'

ちなみに、mod_headers モジュールを有効にするためには、httpd.conf において

LoadModule headers_module modules/mod_headers.so

を設定する。

Apache 2.4 以降はすでに導入・有効化されているので、/etc/httpd/conf.modules.d/00-base.conf に

LoadModule headers_module modules/mod_headers.so

が記述されていることを確認する。

Appendix C：暗号スイートの設定例

- C.2.1. Apache, lighttpd, nginx の場合
  - 改訂前
    - Apache の場合の記述

    C.2.2 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"
  - 改訂後
    - Apache の場合の記述

    C.2.2 に従い、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"
- C.2.2. OpenSSL 系での暗号スイートの設定例
  - 改訂前（誤記）

    表 1　代表的な暗号スイートの対比表中

    TLS_RSA_WITH_CAMELLIA_256_SHA

    TLS_RSA_WITH_CAMELLIA_128_SHA
  - 改訂後

    TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

    TLS_RSA_WITH_CAMELLIA_128_CBC_SHA