# SSL 3.0 の脆弱性に関する注意喚起

rev1.0

平成 26 年 10 月 15 日

株式会社ファイブドライブ
〒100-0011 東京都千代田区内幸町 1-1-7
TEL:03-5511-5875/FAX:03-5512-5505

**注意事項**

本文書は2014年10月15日時点で公開されている脆弱性情報にもとづいて作成されています。脆弱性の影響を受ける条件、改善策及び回避策等は公開情報をもとに記載しており、今後新たに公開される情報により変更される可能性がありますのでご注意ください。

# 目　次

## 1. 脆弱性の概要

暗号化通信で利用されているSSLプロトコルのバージョン3.0において、通信内容の盗聴が可能な脆弱性が報告されました。

| | |
|---|---|
| CVE | CVE-2014-3566 (CVSS基本値未評価) |
| リモートからの攻撃の可否 | 可 |
| 攻撃コード（攻撃手法）の公開 | 特定の攻撃コードで攻撃が可能となるタイプの脆弱性ではありません。 |

## 2. 影響するソフトウェア・バージョン

本脆弱性はSSL 3.0のプロトコル自体に存在する脆弱性です。従って、使用しているSSLソフトウェアの種類にかかわらずCBCモードがサポートされているSSL 3.0が利用可能なソフトウェアすべてが影響を受けます。

※ 以下のSSLプロトコルは、本脆弱性の影響を受けません。

- CBCモードを利用していないSSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2
- CBCモードを利用しない暗号スイート

## 3. 想定されるリスク

暗号化通信の通信内容が盗聴される危険性があります。

## 4. 攻撃が成立する環境

本脆弱性を利用した攻撃を成立させるためには、攻撃者が中間者攻撃を行うことができる状況にあることが前提となります。同一 LAN 環境に攻撃者と被害者が存在する場合は、現実的なリスクとして中間者攻撃が行われる可能性がありますが、インターネット経由で攻撃者が他のユーザに対して中間者攻撃を成立させるのは一般的に困難です。ただし、暗号化が行われていない（または脆弱な暗号化方式を利用している）公衆無線 LAN 環境などを利用している場合には、同一のアクセスポイントを利用している攻撃者により中間者攻撃が行われる可能性があります。

中間者攻撃を行うことが可能な環境において、攻撃者は被害者と被害者が通信しようとしているサーバとの間に割り込み、暗号化通信プロトコルとして SSL 3.0 を利用させるように仕向けます。そのため、通信内容の盗聴の対象となる被害者の環境においても CBC モードがサポートされている SSL 3.0 が利用可能なソフトウェア（ブラウザ）が利用されている必要があります。このような環境において、攻撃者は被害者のブラウザと通信先のサーバの中間で、SSL 3.0 の脆弱性を利用した通信内容の一部を盗み見ることが可能となります。

## 5. 脆弱性の有無の確認方法

確認を実施したいサーバで以下のコマンドを実行してください。($はコマンドプロンプト)

※Linux 系サーバで OpenSSL を利用している場合の確認方法です。

```
$ openssl ciphers -v | grep SSLv3 | grep CBC
```

以下のような出力となった場合（サポートしている暗号スイートが出力された場合）には**脆弱性が存在します。**

```
KRB5-DES-CBC-MD5        SSLv3 Kx=KRB5     Au=KRB5 Enc=DES(56)   Mac=MD5
KRB5-DES-CBC-SHA        SSLv3 Kx=KRB5     Au=KRB5 Enc=DES(56)   Mac=SHA1
EDH-RSA-DES-CBC-SHA     SSLv3 Kx=DH       Au=RSA  Enc=DES(56)   Mac=SHA1
EDH-DSS-DES-CBC-SHA     SSLv3 Kx=DH       Au=DSS  Enc=DES(56)   Mac=SHA1
DES-CBC-SHA           SSLv3 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=SHA1
```

※出力される暗号スイートはバージョンや設定により異なります。

出力が無かった場合には**脆弱性は存在しません。**

上記はサーバにインストールされている OpenSSL がサポートしている暗号スイートの確認方法ですが、Apache mod_ssl 等を利用している場合には、Web サーバの設定で暗号スイートを個別に無効化することも可能です。リモートから Web サーバにおいて SSL 3.0 が利用可能な設定となっているか確認する方法は以下の通りです。(openssl コマンドを利用します)

[コマンド書式]

$ openssl s_client -connect [対象サーバの IP アドレス]:[ポート番号] -[SSL/TLS バージョン]

[実行例]

以下の例では、サーバ IP 192.168.0.1 のポート 443/tcp で確認する場合となります。

・SSLv3 の場合の例

# openssl s_client -connect 192.168.0.1:443 -ssl3

・TLSv1 の場合の例

# openssl s_client -connect 192.168.0.1:443 -tls1

上記コマンドを実行し、SSL/TLS セッションが確立できる場合には、指定した暗号化スイートはサポートされていると判断されます。コマンド実行後、エラーが発生して SSL/TLS セッションが確立できない場合には、指定した暗号化スイートはサポートされていないと判断されます。

[エラー発生時の例]

$ openssl s_client -connect 127.0.0.1:443 -ssl3

CONNECTED(00000003)

2839:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1102:SSL alert number 40

2839:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:539:

## 6. 改善策

SSL 3.0 のプロトコル自体に脆弱性があるため、サーバ側で SSL 3.0 をサポートしないことが改善策となります。

- SSL 3.0 を無効にし、TLS 1.0、TLS 1.1、TLS 1.2 を有効にする。
- SSL 3.0 における CBC モードを無効化する。

OpenSSLを利用したApache mod_sslおよびnginx、IISにおける暗号スイートの設定変更例を示します。

■OpenSSLを利用したApache mod_ssl暗号スイートの設定
SSLProtocolディレクティブによりSSLv3を削除してサービスを再起動してください。

［設定例］

```
SSLProtocol all -SSLv2 -SSLv3
```

■nginxの設定
設定ファイルのssl_protocolsディレクティブの設定からSSLv3を削除しサービスを再起動してください。

［設定例］

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

■IISの暗号スイート設定
『注意』
設定の変更にあたり、レジストリを誤って変更すると、深刻な問題が発生することがあります。レジストリを変更する際には十分に注意してください。

＜プロトコルの制限＞
●SSLv3の無効化（IIS6.0以降の場合）
IIS6.0以降においてSSLv3を無効化する方法は、以下の通りです。
以下のレジストリのサブキー内にDWORD値を次の内容で作成しサーバを再起動することによりSSLv3を利用停止にすることが可能です。

・レジストリ：
HKey_Local_Machine¥System¥CurrentControlSet¥Control¥SecurityProviders¥SCHANNEL¥Protocols¥SSL 3.0¥Server
・作成するDWORD　名前：Enabled　値：0

設定変更にあたっては下記参考情報を参考にしてください。

- インターネット インフォメーション サービスで PCT 1.0、SSL 2.0、SSL 3.0、または TLS 1.0 を無効にする方法
  http://support.microsoft.com/kb/187498/ja

ただし、SSL 3.0 を無効にした場合、TLS 1.0 以上をサポートしていないブラウザを利用しているユーザ（極めて古い携帯端末やブラウザを利用している場合など）は、サーバに SSL 接続できなくなります。

現在は一般的なブラウザ(Internet Explorer、Google Chrome、Firefox)において SSL 3.0 がサポートされていますが、Google Chrome や Firefox は今後 SSL 3.0 をサポートしない（デフォルトで無効化する）方針を打ち出しています。

## 7. 回避策

改善策の実施が困難な場合は、一時的な回避策として以下の方法を実施することが挙げられます。

- SSLサーバ側でTLS_FALLBACK_SCSVオプション（プロトコルダウングレードを抑止するオプション）を有効にする。

※ 回避策は一時的に脆弱性の影響を回避することを目的としたものであり、本脆弱性によるすべての攻撃を防御できることを保証するものではありません。回避策の実施と同時に改善策の実施を進めることを推奨いたします。

# 8. 参考情報


- 「This POODLE Bites: Exploiting The SSL 3.0 Fallback」
  https://www.openssl.org/~bodo/ssl-poodle.pdf
- Microsoft「セキュリティアドバイザリ3009008「SSL 3.0の脆弱性により、情報漏えいが起こる」を公開」
  http://blogs.technet.com/b/jpsecurity/archive/2014/10/15/3009008-ssl3.aspx

本文書の記載内容についてご不明な点がございましたら、下記のお問い合わせ先までお問い合わせください。

株式会社ファイブドライブ
TEL：03-5511-5875（受付時間：平日 10 時～18 時）
FAX：03-5512-5505
MAIL：secinfo@fivedrive.jp
担当：脆弱性情報担当

以上