お客様各位

2014 年 10 月 15 日
ジェイサート株式会社

SSL v3.0 に関する脆弱性 POODLE につきまして
(Padding Oracle On Downgraded Legacy Encryption)

米国時間 2014 年 10 月 14 日(火)、SSL 3.0 に関わる脆弱性 (CVE-2014-3566、この脆弱性を Padding Oracle On Downgraded Legacy Encryption) 略して「POODLE」と呼称) を中間者攻撃され、SSL 通信が解読され、個人情報、パスワード、Cookie などが盗まれるリスクがある、とのアナウンスがございました。

その影響範囲につきましては、

1. サーバ側だけではなく、SSLv3 を使用するクライアント側(IE や Chome 等ブラウザや HTTPS 通信をつかうアプリケーションなど)にも影響あり
2. SSLv3.0 と後方互換性をもつ TLSv1.0 および TLSv1.1 以降には影響なし
3. なお、スターフィールド SSL 含む SSL サーバ証明書に関わる脆弱性ではありません

その他詳細情報につきましては、以下サイトをご参照ください。
http://jvn.jp/vu/JVNVU98283300/ (JPCert コーディネーションセンター提供)

お客様におかれましては、サーバ・クライアントの製造元や提供元がウェブ上等で公開している本脆弱性対処法に関する情報を参照され、「SSL v3.0 の無効化」を早期に実施されることをお奨め致します。

なお、本脆弱性に関し、お客様サーバ環境に設定済のスターフィールド SSL のリキー再発行や再設定の必要はありません。

また、弊社ウェブサイトは SSL v3.0 無効化を実施済です。

以上

【参考情報】

先ずは、サーバ製造元あるいは提供元にお問い合わせください。

以下は、飽く迄もウェブ上関連情報を弊社にてピックアップしたものに過ぎません。

0.　お客様サイトの SSL v3.0 の設定状況確認：

https://www.ssllabs.com/ssltest/index.html

1. apache での SSL v3.0 無効化：

https://scottlinux.com/2013/06/18/disable-sslv2-and-sslv3-in-apache/

http://qiita.com/watarin/items/2b0d91f797ca70a1171b

http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslprotocol

2. nginx での SSL v3.0 無効化：

http://nginx.com/blog/nginx-poodle-ssl/

3. Windows Server/IIS での SSL v3.0 無効化：

https://technet.microsoft.com/library/security/3009008.aspx

http://dev.classmethod.jp/cloud/aws/disalbe-sslv3-use-iis-crypto/

【注】 無効化処理により、IIS6 on Windows XP 以前のレガシーサーバ での SSL 接続に不具合が生じるとの情報がございます。製造元あるいは提供元にご確認ください。

4. AWS 環境各種サーバでの SSL v3.0 無効化：

http://dev.classmethod.jp/cloud/aws/cve-2014-3566-poodle-issue/

5. F5/Big IP での SSL v3.0 無効化：

https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip

6. Tomcat での SSL v3.0 の無効化：

https://access.redhat.com/ja/node/1232723