お客様各位

2016 年 3 月 2 日
ジェイサート株式会社

SSL v2 に関する脆弱性 (DROWN) につきまして

米国時間 2016 年 3 月 1 日(火)、SSL v2 に関わる脆弱性 (CVE-2016-0800、この脆弱性を Decrypting RSA with Obsolete and Weakened eNcryption) 略して「DROWN」と呼称) を SSL v2 におけるハンドシェイク時のデータを解析することで、暗号化されたネットワークトラフィックの解読が可能となるリスクがある、とのアナウンスがございました。

https://drownattack.com/
お客様サイトの SSL v2 の設定状況確認:
https://www.ssllabs.com/ssltest/index.html

その対処法ですが、

1. SSL/TLS 接続する全てのサーバが 「SSL v2 無効化」 されていることを確認してください。(TLS1.1 以上への Upgrade を推奨します)
2. その対象は Web サーバ/HTTP のみならず、SMTP, POP, IMAP 等、SSL/TLS をサポートする一切サーバを含みます。
3. 特に、異なるサーバ間で秘密鍵(および証明書)を共有して利用されているお客様は、いずれか 1 台でも SSL v2 の無効化漏れがあった場合、秘密鍵を奪取され SSL v2 無効化済のその他サーバがハッキングされるリスクがございますので、ご注意ください!
4. 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ので、証明書の再発行や新規取直しの必要はありません。

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/JVNVU90617353/ (JPCert コーディネーションセンター提供)
https://drownattack.com/#check (サーバソフトウェア別対処法)

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 v2 の無効化」を早期に実施されることをお奨め致します。

以上