お客様各位

2015 年 3 月 6 日
ジェイサート株式会社

輸出グレード RSA 暗号サポートに起因する脆弱性 FREAK につきまして
(Factoring attack on RSA-EXPORT Keys)

米国時間 3 月 5 日(木)、米国マイクロソフトが、Windows への TLS/SSL 実装に使われている「セキュアチャネル」(Schannel)にインターネットの通信の暗号化に使われる TLS/SSL プロトコルに 1990 年代の米暗号輸出規制に起因する脆弱性が存在していることを確認した、と発表しました。

この脆弱性は、中間者攻撃により強度の弱い (<=512bit) RSA 輸出暗号を強制利用させる (Factoring attack on RSA-EXPORT Kyes : FREAK) ことで、暗号化された SSL/TLS セッションの暗号化通信を盗み見できる可能性がある、とのことです。

その影響範囲につきましては、マイクロソフト商品のみならず、当該輸出グレード RSA 暗号を使用あるいはサポートするサーバやクライアント(各種ブラウザ)にも影響がありますので、今後サーバ・クライアントの製造元や提供元により逐次公開される本脆弱性対処法に関する情報を参照され、**「輸出グレード RSA 暗号の無効化」を早期に実施されることをお奨め致します。**

- http://jvn.jp/vu/JVNVU99125992/
- http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-001009.html
- https://jvn.jp/vu/JVNVU98974537/index.html
- http://blog.trendmicro.com/trendlabs-security-intelligence/freak-vulnerability-forces-weaker-encryption/

なお、本脆弱性は、スターフィールド SSL 含む SSL サーバ証明書に関わるものではありません。従いまして、サーバ側での本脆弱性の排除作業に関連し、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本脆弱性に該当するサーバソフトウェアを使用しておりません。

- https://www.jcert.co.jp/index.html
- https://jstore.jcert.co.jp/sslsales/ControlDSF0101ServiceMenu

以上