No. E15001

GAKUEN ユーザ様　各位

日本システム技術株式会社

SSL/TLS実装の脆弱性に関するお知らせ

平素は弊社製品「GAKUEN シリーズ」をご愛顧いただきありがとうございます。

この度、IPA（独立行政法人　情報処理推進機構）および各種報道によって注意喚起が行われております SSL/TLS 実装の脆弱性問題について、ご案内申し上げます。

SSL/TLS 実装の脆弱性（CVE-2015-0204 通称「FREAK 攻撃」）につきまして、
GAKUEN/UNIVERSAL PASSPORT EX の以下のバージョンにおいて、SSL 通信をご利用いただいているお客様については影響を受ける可能性があります。

※詳細は下記サイトをご確認ください。
SSL/TLS の実装が輸出グレードの RSA 鍵を受け入れる問題（FREAK 攻撃）
http://jvn.jp/vu/JVNVU99125992/index.html

＜対象となるバージョン＞
GAKUEN/UNIVERSAL PASSPORT EX V1.0 をご利用のお客様
GAKUEN/UNIVERSAL PASSPORT EX V1.1 をご利用のお客様
GAKUEN/UNIVERSAL PASSPORT EX V1.2 をご利用のお客様
GAKUEN/UNIVERSAL PASSPORT EX V1.3 をご利用のお客様(※)
※V1.3 については最新のミドルウェア Fixpack（Fixpack 37）を適用されているお客様は本脆弱性の影響を受けません。

輸出グレード暗号(RSA Export)と呼ばれる暗号方式が使用可能となっている環境において、中間者攻撃が可能となり、サーバ～クライアント間の暗号化通信が盗聴・改ざんされる可能性がございます。従いまして弊社では下記の通り、サーバ設定による輸出グレード暗号の無効化を推奨いたします。

GAKUEN/UNIVERSAL PASSPORT EXV1.0～V1.3 にて SSL 通信をご利用のお客様は、別紙「輸出グレード暗号の無効化手順」をご確認の上、輸出グレード暗号を無効にしていただきますようお願いいたします。

回避策等、本問題に関する情報については今後追加・更新される可能性があります。定期的に情報収集を行い、適切な対応をお願いいたします。

ご不明な点がございましたら、GAKUEN サポートセンターまでご連絡ください。

以上

No. E15001

別紙「輸出グレード暗号の無効化手順」

以下の作業は GAKUEN/UNIVERSAL PASSPORT EX の Web サーバにて実施してください。

※ 手順3の IBM HTTP Server（以下、IHS と表記）のサービス再起動時に、GAKUEN/UNIVERSAL PASSPORT EX のサービスが一時的に停止しますので、運用時間外での設定をお願いいたします。

手順1. 「{IHS インストールディレクトリ}¥conf¥httpd.conf」のバックアップを取得します。
httpd.conf を任意の場所にコピーしてください。
※IHS インストールディレクトリ … 通常は"D(C):¥IBM¥HTTPServer"

手順2. 「{ IHS インストールディレクトリ}¥conf¥httpd.conf」をテキストエディタで開き、最下行付近にある<VirtualHost>で囲まれた部分に以下の通り追記します。

＜変更前＞

```
==========================================
 <VirtualHost *:443>
 SSLEnable
 SSLProtocolDisable SSLv2 SSLv3
  …
    ～中略～
 </VirtualHost>
==========================================
```

＜変更後＞

```
==========================================
 <VirtualHost *:443>
 SSLEnable
 SSLProtocolDisable SSLv2 SSLv3                  ←※
 SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA      ←左記の記述を追加
 SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA      ←左記の記述を追加
 SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA     ←左記の記述を追加
  …
    ～中略～
 </VirtualHost>
==========================================
```

※の記述についても記載がない場合は併せて追記をお願い致します。

手順3. IHS サービスを再起動します。
（Windows の管理ツール-[サービス]から「IBM HTTP Server」で始まるサービスを再起動）

※注意事項※

古いブラウザを利用している場合や、意図的に TLS を無効化している場合など、ブラウザのバージョン・設定によっては上記設定を行うと GAKUEN/UNIVERSAL PASSPORT EX へ接続できなくなる場合があります。セキュリティの観点より、ブラウザのアップデート、またはブラウザ設定による TLS の有効化を実施していただきますようお願いいたします。