平成 22 年 2 月 12 日

ジェイサート株式会社

「ネット暗号の 2010 年問題」対応方針のこと

昨年末、弊社 Starfield SSL 証明書の提供元である米国 Go Daddy Group, Inc.が、米国マイクロソフト本社と協議、所謂国内における「ネット暗号の 2010 年問題」に相当する次世代暗号への対応につき、下記の通り合意しましたので、お知らせいたします。

記

１．　ルート証明書の Upgrade について

(ア) 公開鍵暗号強度

① 2003 年来、他社に先んじて 2048bit に対応済であり、**今回特段の対応の必要なし**。

1. あらゆる PC クライアントや iPhone 等のスマートフォンに**搭載済み**。
2. 国内仕様携帯端末には 2010 年春モデルから順次搭載。

(イ) ハッシュ関数および共通鍵暗号強度

① SHA1 の脆弱性が明確になり次第、即時 SHA256 に変更すべく**準備完了済み**。

② 共通鍵暗号はハッシュ関数 Upgrade 時に同時に AES 方式に変更。

２．　エンド証明書（お客様のサーバに搭載する証明書）の Upgrade について

(ア) 公開鍵暗号強度（CSR 生成時に証明書利用者によりサーバ上で指定）

① **2010 年 7 月より移行予定**。

(イ) ハッシュ関数および共通鍵暗号

① SHA1 の脆弱性が明確になるか、あるいは**遅くとも 2012 年 1 月 1 日より SHA256 へ移行予定**。

② 共通鍵暗号はハッシュ関数 Upgrade 時に同時に AES 方式に変更。

なお、国内仕様携帯端末（i mode, ez-web, Y!ケイタイ）については、証明書のブランドに関わらず上記「次世代 SSL」仕様について対応し切れていない、との理解ですので、当面は「旧世代（1024bit x SHA1）」の SSL 証明書の継続利用が無難であろうと想定しております。

また、本合意内容につきましては、他社認証局においても「おおよそ同一内容」であろうと想定されますが、その詳細に付きましてはそれぞれの認証局に確認頂きますよう、お願い致します。

以上

（参考）「ネット暗号の 2010 年問題」とは：
http://itpro.nikkeibp.co.jp/article/Keyword/20090119/323069/