報道関係者各位

プレスリリース

2009 年 10 月 9 日

ジェイサート株式会社

スターフィールド SSL の「ネット暗号の 2010 年問題」への対応状況について

ジェイサート株式会社(本社：東京都千代田区、代表取締役：石原 章年)は、世界の SSL サーバ証明書市場で第 2 位の発行規模を誇る米国 Go Daddy 社の「スターフィールド SSL」の「ネット暗号の 2010 年問題（*）」に関する対応状況について発表致します。

（*）「ネット暗号の 2010 年問題」とは

インターネット上で、個人情報など機密性高い情報を安全に送受信するために使用されて来た現行世代の暗号技術に脆弱性ありとして、米国政府および企業は 2010 年末までに次世代技術への移行を決定しているが、その一方で国内においては、国内仕様で運用されている機器やシステムの置き換えなどコスト面での負担も大きく、その対応が遅れ気味である状況を言う。 詳しくは、日経 10 月 5 日朝刊 http://www.shopbiz.jp/ss/news/43446.html

1） Go Daddy 社は、2005 年に米国国立標準技術研究所（NIST）が米国政府に対し本問題を提起して以降、「2010 年」に向けて抜かりなく対応を進めてきており、**予定通り「2010 年末までに」以下のすべての要件につき実施完了する予定です**。

	暗号技術	効用	現行	2010年以降
1	公開鍵暗号	送受信者のなりすまし防止	RSA1024bit	RSA2048bit
2	共通鍵暗号	通信データの盗聴防止	2TDES	AES
3	ハッシュ関数	通信データの改ざん防止	SHA1	SHA256

2） スターフィールド SSL においては、上記**「公開鍵暗号強度」の変更（RSA2048bit）に限り**、2009 年 1 月に米国マイクロソフト社が同社製品に搭載する SSL ルート証明書の要件を上記の NIST 勧告に則し変更する決定をしたことに伴い、**すべての「証明のパス」（ルート証明書、中間証明書、エンド加入者証明書）において、先行して実施済です**。

- 米国マイクロソフト社告知内容：
http://technet.microsoft.com/en-us/library/cc751157.aspx

3） スターフィールド SSL においては、残りの要件を満足する、**新世代 SHA2 ルート証明書（SHA256 with AES）についても既に生成済**であり、2010 年末までに確実に市場投入すべく準備が完了しております。

４）　本問題は国内においても、昨年より専門家によって突っ込んだ議論が展開されて来ております。

http://itpro.nikkeibp.co.jp/article/NEWS/20080424/299972/

http://www.atmarkit.co.jp/ad/sflash/0810encryption/encryption01.html

http://www.atmarkit.co.jp/fsecurity/rensai/crypt01/crypt01.html

http://www.atmarkit.co.jp/fsecurity/rensai/crypt01/crypt02.html

【Go Daddy Group, Inc.　会社概要】

代表　：CEO ＆ Founder　Bob Parsons

本社　：米国アリゾナ州スコッツデール

年商　：700 億円(2008 年実績)

URL　：http://www.godaddy.com

事業概要：

1.ドメインレジストラ事業(世界最大 3,300 万ドメイン)

2.ホスティング事業(北米最大 320 万アカウント)

3.SSL 証明書事業(世界第 2 位 シェア 27%)

【ジェイサート株式会社　会社概要】

代表　：代表取締役　石原 章年

本社　：〒102-0082 東京都千代田区一番町 3 番 8 号 大宮ビル 2 階

資本金：7,600 万円

URL　：http://www.jcert.co.jp