お客様各位

2017 年 10 月 23 日
ジェイサート株式会社

Infineon 製 RSA ライブラリが RSA 鍵ペアを適切に生成しない問題につきまして

米国時間 2017 年 10 月 16 日(月)に CERT/CC により公表された脆弱性(CVE-2017-15361)については、Infineon 製 RSA ライブラリが RSA 鍵ペアを適切に生成しないという問題(ROCA: Return of Coppersmith's Attack)に関するものです。

当該ライブラリを使って RSA 鍵ペアを生成している場合、鍵の全数探索よりも効率的な探索手法が適用可能で、2048 ビット以下の鍵長においては、悪意ある第三者が RSA 公開鍵を取得するだけで、相対の秘密鍵を奪取・盗取できる可能性がある、とのことです。

なお、本件は当該ライブラリにおける RSA の鍵生成に関する問題であり、ECC (楕円曲線暗号)は影響を受けず、また、他社デバイスやライブラリで生成した RSA 鍵も当該ライブラリで安全に使用できる、とのことです。

詳しくは、以下サイト情報をご参照ください。
http://www.kb.cert.org/vuls/id/307015
https://jvn.jp/vu/JVNVU95530052/
https://www.venafi.com/blog/roca-risks-are-your-keys-safe

他方、弊社提携先米国 Go Daddy 社からは、
1. 本件が公表されるまでに弊社を介して発行された証明書には、当該 RSA ライブラリで生成された公開鍵(CSR)を含むものは一切存在していないこと、および
2. 今後の発行処理においては、お客様から提示されるすべての公開鍵(CSR)をスクリーニングしてから発行処理を受理する機能を米国認証局内システムに実装済であること

との報告を受けておりますので、本問題による脆弱性のリスクなく、スターフィールド SSL を安心して継続利用頂けます。

以上