2016 年 12 月

お客様各位

セイコーソリューションズ株式会社

TSA 公開鍵証明書の OCSP 対応について

弊社サービスで利用しております電子証明書の発行局 GMO グローバルサイン株式会社より以下の連絡を受けました。

つきましては、2017 年 2 月 1 日以降、新しい TSA 公開鍵証明書に変更するまでの期間、当社の発行するタイムスタンプは Code signing 用途でのご利用はできませんのでご注意ください。

新しい TSA 公開鍵証明書への変更は 2017 年 5 月 1 日より順次対応する予定です。

マイクロソフト社からの要求により、世界的な脅威となっているマルウエア対策として、2017 年 2 月 1 日より、Code signing で利用される電子証明書と TSA 公開鍵証明書の失効情報の提供方法に OCSP が必須となりました。
これまでの CRL に加えて、新たに OCSP での情報提供を開始いたします。
本対応に伴い、OCSP の URL を記載した TSA 公開鍵証明書に変更いたします。

参考)
◇Microsoft：Trusted Root Program Requirements
http://social.technet.microsoft.com/wiki/contents/articles/31633.microsoft-trusted-root-program-requirements.aspx
◇The CA/Browser Forum Code Signing Working Group：Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
https://casecurity.org/wp-content/uploads/2016/09/Minimum-requirements-for-the-Issuance-and-Management-of-code-signing.pdf

本件に関するお問い合わせは、下記までお願いいたします。
chrono_contact@seiko-sol.co.jp

※Code signing：ソフトウエアにデジタル署名を行う電子署名
※CRL：（Certificate Revocation List）定期的に生成され公開される失効した公開鍵証明書のリスト
※OCSP：（Online Certificate Status Protocol）公開鍵証明書の失効状態を取得するための通信プロトコル

以上