2011 年 7 月 8 日

ベリサイン個人電子証明書ご利用者 各位

株式会社 ドゥイット
ベリサイン電子証明書担当

ベリサイン 個人用電子証明書 Class1 ライト CA証明書の鍵長変更のお知らせ

平素より大変お世話になっております。弊社からベリサイン個人電子証明書のご購入、ご利用をいただき、誠にありがとうございます。

さてこの度、2011年 7月 16日発行分より個人用電子証明書 Class1ライトおよび、その上位階層に当たる CA に含まれる公開鍵について、1024bit鍵長での発行を終了とし、2048bit鍵長での発行へ切換えをおこないます。お手数ではございますが、以下の内容をご参照いただき、ご対応をお願いいたします。（電子証明書をクライアント認証でご利用いただいていますお客様は、システムご担当者様へご確認をお願いいたします。）

何卒よろしくお願い申し上げます。

記

1. 背景： NIST（米国標準技術局）の勧告

   NIST（米国標準技術局）では、米国連邦政府機関の情報システムについて、計算機性能の向上や、暗号アルゴリズムの脆弱性の問題などを考慮し、安全性確保の観点から 2010 年末を期限に 1024bit 鍵長の利用を終了する方針を示しました。これらを踏まえ、ベリサイン社では個人用電子証明書 Class1 ライトの証明書を 1024bit 鍵長での発行は 2011 年 7 月 15 日をもって終了し、2048bit 鍵長での発行へ切換えをおこなう方針で対応することになりました。

2. 鍵長変更による影響範囲に関して

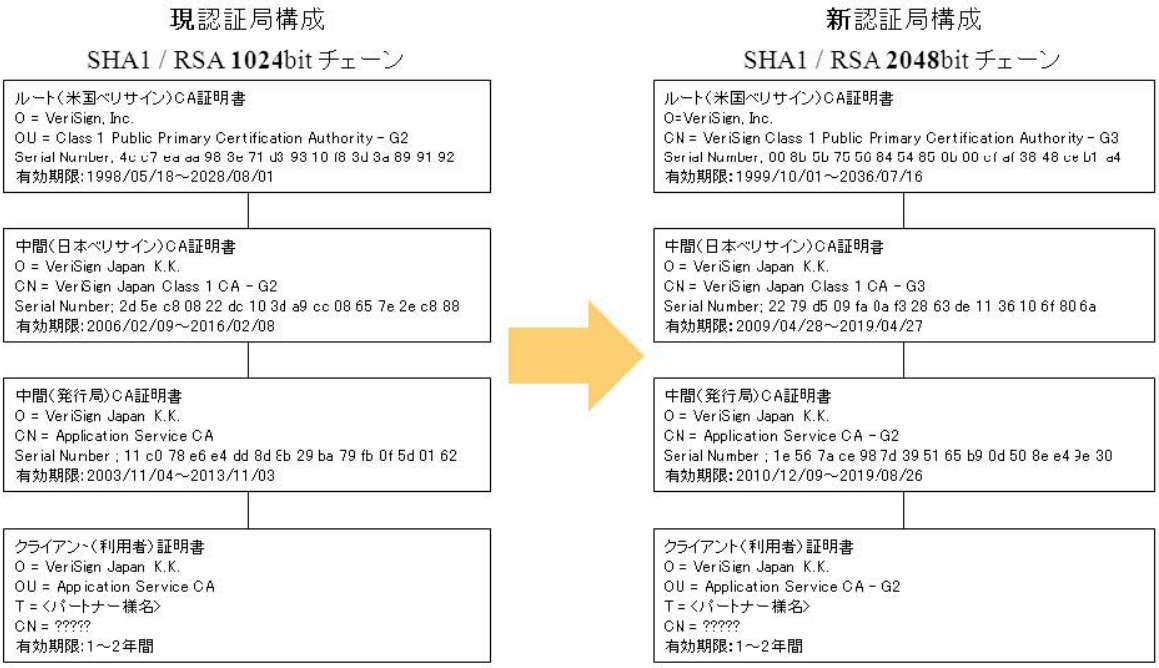
   ・Class1ライトにて SSLクライアント認証でのアクセスコントロールをご利用のお客様におかれましては、アクセスコントロール設定の追加が必要となります。

   ・また、お客様がご利用中のアプリケーションやICカード等によっては、鍵長変更によって何らかの影響が発生する可能性がございます。当該影響についてご不明な点がございましたら、各開発元へ事前にご確認いただけますよう、お願いいたします。

   ・S/MIME用（電子メールにて署名、暗号化をご利用）でご利用のお客様におかれましては、設定変更は不要です。

3. 認証局階層構造の変更

   2011年 7月16日以降に発行される利用者証明書は下図の右側にあります「新認証局構成」（SHA1/RSA 2048bitチェーン）での発行となります。SSLクライアント認証などのアクセスコントロールの設定をおこなわれている場合には、新認証局構成をアクセスコントロールの設定に追加頂く必要がありますのでご注意ください。



4. 新認証局証明書の取得について

2011/7/16 日以降に発行される証明書ファイル（p12 ファイル）には新認証局証明書がパッキング（含まれて）おります。また、他の方法として以下のウェブサイトより入手可能となっております。

日本ベリサイン Class 1中間CA-G3 証明書

Common Name = VeriSign Japan Class 1 CA - G3

Serial Number: 22 79 d5 09 fa 0a f3 28 63 de 11 36 10 6f 80 6a

Operational Period: 4/28/2009 to 4/27/2019

https://www.verisign.co.jp/repository/intermediate/vsj_c1ca_g3.html

日本ベリサイン Application Service Class 1中間CA-G2証明書

Common Name = Application Service CA -G2

Serial Number: 1e 56 7a ce 98 7d 39 51 65 b9 0d 50 8e e4 9e 30

Operational Period: 12/09/2010 to 4/26/2019

https://www.verisign.co.jp/repository/intermediate/Application_Service_CA-G2.html

以上

株式会社ドゥイット　ベリサイン電子証明書担当
TEL：03-5367-3777／FAX：03-6368-4300／E-Mail：info@interfax.jp
http://www.do-it.co.jp/did/