

シマンテック電子証明書ご利用者 各位

株式会社 ドウイット
電子証明書担当

Symantec PKI Class1 Certificate
署名アルゴリズムのSHA-2移行につきまして（第一報）

拝啓 お客様におかれましては、ますますご清栄のこととお慶び申し上げます。弊社からシマンテック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。

早速ではございますが、この度、Symantec PKI Class1 Certificateにおきまして、署名アルゴリズムをSHA-1から SHA-256WithRSAEncryption（以下、SHA-2）へ移行いたします。つきましては下記のとおり、今後の対応予定をご案内いたします。

本対応に伴い、お手数ではございますが、以下の内容（下記項番3）をご参照いただき、ご対応をお願いいたします。

何卒よろしくお願い申し上げます。

敬 具

記

1. 実施内容

Symantec PKI Class1 Certificate のルートおよび中間認証局を、SHA-2 の新しい認証局へ移行いたします。また、Symantec PKI Class1 Certificate 認証局から発行されるエンドエンティティ証明書および CRL のプロファイル変更を実施し、署名アルゴリズムを SHA-2 に変更いたします。

2. 実施スケジュール（予定）

2015年9月までの変更実施を予定しております。
具体的な日程は、決定次第、改めてご連絡いたします。

3. お客様への影響およびご確認事項

当変更の実施までに、お客様の証明書のご利用環境（メーラー、ブラウザ等）における、SHA-2 証明書の対応状況をご確認いただきますようお願いいたします。現在各ベンダーにてサポートされている一般的なメーラーおよびブラウザ等は、SHA-2に対応しております。
証明書を、お客様で独自に作成されたアプリケーションにてご利用の場合は、事前に対象アプリケーションのSHA-2対応状況をご確認いただきますようお願いいたします。

なお、証明書をSSLクライアント認証でご利用の場合は、アプリケーションやウェブサーバーに、新しいSHA-2の上位認証局の追加等を実施いただく必要がございます。

当変更に伴う、**発行済みの電子証明書への影響はございません。発行済みの電子証明書は、現在の有効期間満了まで、問題なくご利用いただけます。**

<SHA-2移行に関する参考情報>

<http://www.symantec.com/ja/jp/page.jsp?id=ssl-sha2-transition>

以 上