日経テレコン　ＳＳＬ証明書の「ＳＨＡ－２」方式への変更について

2015 年 11 月 10 日

日本経済新聞社デジタルメディア局

平素より格別のご高配を賜り誠にありがとうございます。

このたび、日経テレコンでは、2015 年 11 月 30 日（月）未明に SSL 証明書を現在の「SHA-1」方式から「SHA-2」方式へ変更する予定です。

変更後は、「SHA-2」方式に対応していないお客様のご利用環境からは、日経テレコンがご利用いただけなくなります。お客さまのご利用環境が、「SHA-2」に対応していない場合は、ブラウザや接続用ライブラリのバージョンアップなど、事前にご対応が必要になります。

お手数をおかけしますが、ご理解、ご協力を賜りますようお願い申し上げます。

◇ＳＳＬ証明書の「ＳＨＡ－２」方式について

「SHA-2」方式は、インターネット通信で使用される暗号化方式のひとつで、SSL 証明書が偽造・改ざんされたものでないことを示すために利用されています。従来の「SHA-1」方式に比べてより安全性が向上します。

※「SHA-2」方式に対応している利用環境の例

ブラウザ	Microsoft Internet Explorer 6 (Windows XP SP3) 以降 Google Chrome 1.0 以降 Mozilla Firefox 3.02 以降　など
OS	Microsoft Windows XP SP3 以降 Microsoft Windows Server 2003 (SP2 + Hotfix KB2868626) 以降　など
ライブラリ	OpenSSL Project OpenSSL 0.9.8o 以降※ GnuTLS 1.7.4 以降 Oracle JRE 1.7.0 以降、1.6.0_17 以降、1.5.0_22 以降、1.4.2_19 以降 Mozilla NSS 3.11.10 以降 Microsoft .NET 3.5 SP1 以降　など ※ハッシュアルゴリズムの SHA256 は、OpenSSL 0.9.8 より搭載されておりますが、標準で有効になったのは 0.9.8o からです。

◇ご利用環境が「ＳＨＡ－２」方式に対応しているかの事前確認について

（１）　ブラウザからのご利用の場合

シマンテック社が提供している下記のサイトにて、お客さまのご利用環境が「SHA-2」方式に対応しているかを確認することができます。

https://ssltest-sha2int.jp.websecurity.symantec.com/

（２）　OpenSSL などライブラリ経由で接続している場合

日経テレコンを「SHA-2」方式に移行した事前確認用のサイトを用意しました。

ただし、サイトの URL と ID・パスワードが通常のものと異なりますので、接続テストを実施される場合は、必要な情報をご案内いたします。

なお、接続テスト用のサイトは 11 月 25 日（水）まで稼動する予定です。

以　上