サイトのセキュリティ強化について

2016.03.31

いつもご利用いただき、誠にありがとうございます。

経緯

本サイトでは、お客様の個人情報を守るためにSSL(Secure Sockets Layer：暗号化）という暗号通信技術を使用していますが、お客さまにより安全にご利用いただくため、セキュリティの強化を行ってまいります。
本対応に伴い、お客様がお使いのブラウザ及びそのバージョンにより、弊社のサイトがご利用いただけなくなることがございます。以下、詳細をご確認くださいますようお願いいたします。

対応内容

(1)SSLサーバー証明書を現在使用している「SHA-1」から安全性の高い「SHA-2」へ移行
■SHA-2方式について
「SHA-2」とは、インターネットを安全にご利用いただくために、通信を暗号化させる方式のサーバー証明書の種類です。高度な暗号化方式を採用しているので、安全性が向上します。

(2)SSL通信のひとつ「SSL3.0」遮断し、安全性の高い「TLS」に切り換え
■SSL3.0の脆弱性について
暗号化通信技術のSSL3.0に重大な脆弱性があることが、先日アメリカgoogle社より発表されました。この脆弱性により、クッキーの内容を読み取られる危険性があり、お客様のパスワードが盗まれる可能性があるため、本サイトではSSL3.0脆弱性への対応を実施しております。

セキュリティ強化対応予定日

(1)「SHA-2」への対応：2016年6月1日
(2)TSL1.1及びTLS1.2による通信は2016年4月1日よりご利用可能となります。

ご利用いただけなくなる主な環境

ブラウザ：InternetExplorer6.0 SP2以下の環境
　OS　：Windows XP SP2以前のOS
携帯電話：主に発売開始が2009年以前の端末（フィーチャーフォン）

ブラウザの設定について

(1)ウィンドウズでInternetExplorerをお使いのお客様で
ログインができないなどの事象がある場合には、下記の設定をご確認ください。

(ｱ).「ツール」→「インターネット オプション」→「詳細設定」の順にクリックします。
(ｲ).「SSL 2.0を使用する」「SSL 3.0を使用する」のチェックを外します。
(ｳ).「TLS1.0を使用する」「TLS1.1を使用する」「TLS1.2を使用する」にチェックを入れます。
(ｴ).「OK」をクリックし、ブラウザを再起動します。

(2)ウィンドウズでFirefox及び、Google Chromeをお使いのお客様

SSL3.0の脆弱性に対応したバージョンのリリースがMozillaおよびグーグル社から予定されております。対応バージョンがリリースされましたら、ブラウザのバージョンアップをお願いいたします。

(3)マックをお使いのお客様

SSL3.0の脆弱性に対応したソフトウェアアップデートがアップル社から提供されております。
ソフトウェアをアップデートしていただきますよう、お願いいたします。

対応可否確認について

大変お手数をおかけいたしますが、お客さまのインターネットセキュリティ設定（TLS通信）をご確認いただくと共に、お使いいただいている環境が「SHA-2」方式に対応されているかご確認お願いいたします。

==========

シマンテック社「ハッシュアルゴリズムのSHA-1からSHA-2への移行に関して」
https://www.symantec.com/ja/jp/page.jsp?id=ssl-information-center
表示された画面上の「詳しくはこちら」をクリック願います。

シマンテック社のブラウザ・端末用 SHA-2対応確認用テストページ
https://ssltest-sha2int.jp.websecurity.symantec.com/

This page is for TEST SHA256 SSL Certificate.
と記載されたページが表示されましたら、ご利用可能機器です。

==========

※セキュリティのバージョンアップ後に「SHA-2」に対応していない環境から当サイトにアクセスいただいた場合、「SSLエラー」となり『ページを表示できません』等のメッセージが表示されます。
（表示内容は、ご利用の環境によって異なります）

※「SHA-2」に対応していない環境は、既にメーカーサポートも終了しておりますので、製品メーカーや携帯電話会社等へお問い合わせの上、インターネットご利用環境のバージョンアップ等をお願いいたします。

お客様にはご迷惑をおかけいたしますが、何卒ご理解くださいますようお願いいたします。

不二商事株式会社
ライフデザイン事業部