2016 年 12 月 吉日

お客様各位

株式会社ＫＤＳ

「サーバー証明書」の新しい仕様への切替のお知らせ

SaaS 型 WEB 給与明細配付システムでは、通信内容を暗号化して第三者から盗み見られないようにすることで安全性を高めています。この通信内容の暗号化にあたっては「サーバー証明書」を使用していますが、このサーバー証明書について、セキュリティをより高めるため、新しい仕様への切替を実施しましたのでお知らせします。

暗号化通信（SSL／TLS）を使用する際に用いるサーバー証明書について、これまで広く使用されてきた暗号アルゴリズム SHA-1 から、より安全性の高い暗号アルゴリズム SHA-2 に移行することが世界的な取組として進められており、2016 年 1 月 1 日以降は SHA-1 を用いた新規のサーバー証明書が発行されなくなりました。

（総務省：国民のための情報セキュリティサイト「引用」）

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/12.html

今日使用されているＰＣ・スマートフォンの端末の多くは、既に新しい仕様のサーバー証明書（SHA-2）に対応しているため従来通り暗号化通信が可能ですが、フィーチャーフォン（ガラケー）の一部機種や旧ＰＣ等においては、SaaS 型 WEB 給与明細配付システムの Web サイトが表示できなくなる可能性がございます。

SHA-2 に対応していないフィーチャーフォン（ガラケー）の情報につきましては、各携帯電話会社のホームページをご確認ください。

NTT ドコモ：https://www.nttdocomo.co.jp/info/notice/pages/150715_00.html

KDDI（au）：http://www.kddi.com/important-news/20150715/

SoftBank：http://www.softbank.jp/mobile/info/personal/news/support/20150715a/

以上