2018 年 6 月 27 日

お客さま各位

ハンドレッドステイ東京新宿

サーバーへの不正アクセスにより、当ホテルのウェブサイトからご予約いただいたお客さまの個人情報流出に関するお詫びとお知らせ

平素より「ハンドレッドステイ東京新宿」をご利用いただき誠にありがとうございます。

このたび、当ホテルが導入していた宿泊予約システムのサーバーに対して（＊）、悪意ある第三者が不正にアクセスし、お客さまの個人情報の一部が外部流出した可能性があることが判明しました。当社の宿泊予約システムは、ファストブッキングジャパン株式会社から提供を受けており、同社の親会社にあたるフランス法人のファストブッキングが所有するサーバーに対して不正アクセスがあったものです。お客さまには多大なご心配とご迷惑をお掛けしましたことを深くお詫び申し上げます。
下記のとおり、判明した内容やご注意事項、再発防止策についてご案内申し上げます。

なお、情報が流出したお客さまのうち、当ホテルで連絡先情報を把握できているお客さまについては、順次、同内容についてご連絡を差し上げております。また、個人情報保護委員会には速やかに当該事案を届け出ております。

＊当該宿泊予約システムは、本日までに利用を停止し、新システムへの移行を完了しております。

記

発生事案：2018 年 6 月 15 日に、ファストブッキングが所有するサーバーに悪意ある第三者から不正アクセスがあり、複数の国内宿泊施設の暗号化されていない個人情報が流出。その中にハンドレッドステイ東京新宿が含まれていることが判明しました。
次に、6 月 17 日にも同サーバーに対して不正アクセスがあり、暗号化されていない個人情報が流出しましたが、当ホテルに関連する情報の流出がないことを確認しています。
＊詳細はファストブッキングジャパンの発表資料をご覧ください。

対象範囲：2017 年 5 月 1 日～2018 年 6 月 15 日の期間に「ハンドレッドステイ東京新宿」公式ウェブサイト（http://www.hundredstay.jp/ja-jp ）より直接ご予約いただいたお客さま（予約成立後にキャンセルされたお客さま情報も含まれます）

流出件数：全 124 件

流出情報：お客さまの氏名、国籍、メールアドレス、電話番号、予約金額、予約番号、予約ホテル名、チェックイン日、チェックアウト日
なお、クレジットカード情報は含まれていないことを確認しています。

注意事項：流出したメールアドレスに対して、振込督促や外部サイトへのアクセスを促すフィッシング詐欺に誘引するメールが届く可能性がございますのでご注意下さい。
なお、ハンドレッドステイ東京新宿から振込督促や当ホテルと関係のない他サイトへのアクセスを促すメールを送ることはありません。

再発防止策： 今後、以下の再発防止策を講じてまいります。

① 外部システムを利用する際のセキュリティレベルの確認および定期的なモニタリング、第三者による評価の実施を徹底する。
② 社内関連規則について、再度社員への周知徹底を図る。

以　上

＜本件に関するお客さまからのお問い合わせ先＞

ハンドレッドステイ東京新宿　お客さま相談受付窓口
Email：hundred_stay@hundredstay.jp