2023年10月17日
株式会社 ホテル京阪
（ホテル京阪 淀屋橋）

# 【重要なお知らせ】
# （続報）不正アクセスによるお客様の個人情報流出の可能性および フィッシングサイトに誘導するメッセージ配信についてのお詫びとお知らせ

ホテル京阪 淀屋橋（大阪市中央区）におきまして、当ホテルで利用するBooking.com社（本社：オランダ、アムステルダム）の管理画面が不正アクセスを受け、同社経由で当ホテルをご予約いただきました一部のお客様に対し、フィッシングサイト（不正な手法を用いて個人情報や経済的価値のある情報を搾取する偽のＷＥＢサイト）へ誘導するメッセージが配信された件につきましては、お客様には多大なるご迷惑とご心配をおかけしておりますこと、改めて深くお詫びを申し上げます。

2023年8月10日に【重要なお知らせ】にて本件事案を公表いたしましたが、その後の調査により判明いたしました事実につきまして、以下の通りご報告を申し上げます。

## １．原　因

Booking.com社、関係機関および専門調査会社と連携し、原因の究明や被害の内容等について調査を進めてまいりました。その結果、当ホテルにおいてシステムを管理する弊社端末のうち１台がマルウェア(※)に感染し、攻撃者によって窃取された認証情報が使用され、同店で利用するBooking.com社の管理画面に不正アクセスされたと判断しております。

※マルウェア：悪意のあるソフトウェアの総称で、コンピュータウィルスもマルウェアの一種となります。

## ２．被害状況

(1)第三者による個人情報の閲覧

①個人情報を閲覧された可能性がある期間

・2023年8月1日～8月7日

②個人情報を閲覧された可能性があるお客様

・Booking.com経由で、当ホテルを上記の期間に2023年8月7日～2024年2月27日を宿泊日としてご予約いただいておりましたお客様。

③閲覧された可能性があるお客様の情報

・Booking.com経由でご予約の際に登録された情報のうち、お名前、国、希望言語、電話番号、メールアドレス(※1)、メッセージの送受信内容(※2)、その他ご宿泊日等の情報。

※1　Booking.comでのご予約の際にメッセージ送受信用に自動で割り振られるメールアドレスであり、Booking.comにお客様が登録されたご自身のメールアドレスではございません。

※2　上記②に該当するご予約に関するメッセージの送受信内容のみとなります。

・なお、Booking.com 社より、クレジットカード情報を閲覧された形跡はなかったとの報告を受けております。

④その他

・淀屋橋店以外の弊社ホテルにおきましては、同様の事象がなかったことを確認しております。

⑵第三者によるフィッシングサイトに誘導するメッセージの配信

◇第三者からフィッシングメッセージが送信されたお客様には、事案発生確認後直ちに状況をご説明のうえ貼付されたＵＲＬリンクへのアクセスをされないようご案内いたしました。

◇万一、フィッシングメッセージのリンク先にアクセスされ、クレジットカード情報の入力や支払いを行ってしまった場合は、直ちに Booking.com 社へのご連絡をお願いいたします。

◇お客様におかれましては、引き続き不審なメッセージにご注意いただき、同種のメッセージの配信を受けた場合は、貼付されたＵＲＬリンクへのアクセスをされないようお願い申し上げます。

３．今後の対応と再発防止策

調査結果および関係機関、専門調査会社からの指摘を踏まえ、セキュリティ対策ツールの追加導入を図るとともに不正アクセスへの監視を強化いたします。また、従業員に対する徹底した教育と適宜情報の共有を図って不正アクセスへの意識を高め、再発の防止に努めてまいります。

以　上