

2026 年 10 月 21 日

お客様各位

東京建物リゾート株式会社

不正アクセスによるお客様情報の第三者閲覧の可能性に関するお知らせ（最終報）

2026 年 5 月 29 日に当社ホームページにてお知らせいたしました、当社が運営する「ホテルレジーナ河口湖」において、当施設が利用している宿泊予約サイト Booking.com を通して予約された一部のお客様に対し、WhatsApp 等を通じてフィッシングサイトへ誘導するメッセージが配信された事象につきまして、お客様ならびに関係者の皆様に多大なるご心配とご迷惑をおかけしておりますことを、改めて深くお詫び申し上げます。

本事案の発覚以降、外部専門家の協力を得て原因の究明および影響範囲の特定を進めてまいりましたが、このたび調査が完了いたしましたので、その調査結果および今後の対応について、下記のとおりご報告いたします。

1. 経緯

2026 年 5 月 28 日以降、Booking.com 経由で「ホテルレジーナ河口湖」をご予約された一部のお客様より、WhatsApp 等のメッセージアプリを通じて、当施設からの案内を装った不審なメッセージが送信されているとのご連絡をいただきました。当該事象の確認後、直ちに関連するシステムおよびホテル内端末の利用状況を確認するとともに、外部専門家の協力のもと詳細な事実関係の調査および影響範囲の特定を開始いたしました。

2. 調査結果について

外部専門家による詳細な調査の結果、当施設にて業務に使用していた PC1 台が、マルウェア(※)に感染していたことが確認されました。

※マルウェアとは、コンピューターやシステムに不正な動作をさせ、情報の窃取やデータの破壊などを引き起こす悪意のあるソフトウェアの総称です。

当該 PC 内を調査した結果、同 PC に保存されていた一部のお客様の個人情報について、第三者による閲覧または取得が行われた可能性を否定できないと判断しております。なお、本件は当該 PC 内に保存されていた情報に関するものであり、当施設をご利用されたすべてのお客様が一律に対象となるものではありません。

これらの調査結果を踏まえ、個人情報保護法の趣旨に基づき、情報漏えいのおそれがある対象者様につきまして、下記のとおりご案内申し上げます。

なお、現時点において外部への情報公開や二次被害の報告は確認されていません。

記

【対象となる可能性のあるお客様】

外部専門家の調査により、当該 PC 内に保存されていたことが確認されたファイル等に個人情報が含まれていた一部のお客様が対象となる可能性があります。当施設をご利用されたすべてのお客様が対象となるものではありません。

【漏えいのおそれがある項目】

- ・ご予約者様情報（氏名、住所、国籍、電話番号、メールアドレス）
- ・ご予約内容（宿泊日、プラン、料金など）

【対象となるお客様へのご連絡】

今回の調査結果を踏まえ、個人情報第三者に閲覧または取得された可能性を否定できないと判断したお客様には、個別にご連絡を差し上げております。また、個別のご連絡が困難な方につきましては、本公表をもってご案内に代えさせていただきます。

なお、当社が運営する他の施設においては、同様の事象は確認されておりません。

【対象のお客様へのお願い】

本事案に関連し、「ご登録いただいたメールアドレス」や「Booking.com のメッセージ機能」、「その他 SNS」宛に当社を装った不審な連絡が届く可能性がございます。

万が一、内容に心当たりのない連絡が届いた場合は、開封や記載された URL へのアクセス等を行わず、削除いただきますようお願いいたします。また、クレジットカード情報等の入力を求められた場合も絶対に入力を行わないようお願い申し上げます。

3. 原因について

当該 PC において、不審なメールを起点として外部サイトへ誘導された後、マルウェアに感染していたことが判明しております。

4. 今後の対応について

当社は、このたびの事態を厳粛に受け止め、調査結果を踏まえたうえでシステムのセキュリティ対策および監視態勢の強化を行い、再発防止を図ってまいります。

お客様ならびに関係者の皆様には、多大なるご迷惑とご心配をおかけしましたことを重ねて深くお詫び申し上げます。

今後も、再発防止と信頼回復に努めてまいりますので、何卒ご理解とご協力を賜りますようお願い申し上げます。

【本件に関するお問い合わせ先】

東京建物リゾート株式会社 ホテル事業部

mail : ttr_contact@tt-resort.co.jp

※お問い合わせについては順次回答致しますが、お問い合わせ多数の場合、
回答にお時間をいただく場合がありますのでご了承下さい。

以上