

2023年7月19日

(株) ホテルグランヴィア大阪

## 【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と、フィッシングサイトに誘導するメッセージの配信について

当社において利用している Booking.com 社が提供する宿泊予約情報管理システム（以下、管理システム）が不正アクセスを受けたこと、また一部のお客様に対し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件につきまして、お客様・関係者の皆様にご心配をおかけしており深くお詫び申し上げます。

前回（2023年6月1日）のお知らせ以降、調査により判明しました事実につきまして、以下のとおりご報告いたします。

### 1. 調査結果（原因について）

当社は、関係機関及び専門会社と連携して、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、今回管理システムへの不正アクセスを受けた原因は、システムの管理を行う当社の端末1台がマルウェア感染したことにありと判断しております。

### 2. 調査結果（被害状況について）

#### 事象①

管理システム内の宿泊予約情報（宿泊日を2022年5月1日から2024年3月31日とするもの）に含まれるお客様の個人情報（クレジットカード情報含む）が流出した可能性につきましては、システム提供元の Booking.com 社へ確認を依頼した結果、そのような形跡はないと報告を受けております。

#### 事象②

一部のお客様に、フィッシングサイトへ誘導する URL リンクが付されたメッセージが配信された件につきましては、配信されたお客様には注意喚起の連絡を行いましたが、現時点で被害のご報告はございません。

お客様におかれましては、引き続きご注意いただき、そのような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

調査結果及び関係機関等からの指摘を踏まえ、セキュリティツールの導入や従業員に対する教育等を実施しました。今後も引き続き、更なる対策の強化を行ってまいります。

今後万が一、個人情報流出やフィッシングによるお客様の被害が確認された場合には、関係先に速やかに連絡し、必要な対応をいたします。

### 4. お客様のお問い合わせ窓口

ご質問等のお問い合わせは、以下の窓口からお願いいたします。

フリーダイヤル：0120-94-1374 メールアドレス：[granvia@hgo.co.jp](mailto:granvia@hgo.co.jp)

受付期間：2023年7月19日(水) 9:00～17:00 ～ 7月31日(月) 9:00～17:00