

[Important] Apology and Notice Regarding Unauthorized Access to Reservation Information

As of October 15, 2026

Dear Valued Guests,

Thank you for your continued patronage of our hotels.

We regret to inform you that it has come to our attention that an unauthorized third party gained access to an external system used by our hotels for reservation management, and that information relating to guest reservations may have been viewed or obtained. We sincerely apologize for the considerable concern and inconvenience this matter may cause you.

1. Summary of the Incident

On September 21, 2026, an unauthorized third party accessed “TEMAIRAZU,” the reservation management system used by our hotels and provided by Temairazu Co., Ltd. We are unable to rule out the possibility that some of the reservation information stored in the system was viewed or obtained externally.

Reservations that may be affected: Reservations made on or before September 21, 2026, with a stay date on or after September 21, 2026.

2. Information That May Have Been Viewed or Obtained

Reservation information, including your name, address, telephone number, email address, stay dates, reservation number, accommodation charges, and payment method.

Please note that credit card information is not handled by this system and is therefore not included.

3. Cause

The incident was caused by a security vulnerability in a function of a service previously provided by Temairazu Co., Ltd. The company completed corrective measures for the affected component on September 26, 2026, and is continuing its investigation in cooperation with external specialist organizations.

4. Suspicious Messages Reported

In connection with this incident, we have confirmed instances of suspicious messages (sent via WhatsApp, email, SMS, and other channels) that impersonate our hotels or booking sites and request that recipients enter credit card information or make payments. Recently, we have also identified emails purporting to relate to “online check-in” or an “accommodation itinerary.”

5. Our Requests to Guests

We respectfully ask that you:

- Refrain from opening any URLs or links contained in suspicious messages impersonating our hotels or booking sites.
- Refrain from entering credit card information or personal information in response to such messages.
- Refrain from replying to such messages.
- Refrain from making any payment or money transfer as instructed in such messages.

Should you have entered your card information on a suspicious website, please contact your credit card company and financial institution.

6. Actions Taken

- We have requested that Temairazu Co., Ltd. and the other related reservation system providers identify the cause and investigate measures to prevent recurrence.
- We have issued cautionary notices on the website of each hotel.

7. Inquiries

※Please be aware that, even where the sender's email address appears to belong to one of our hotels, it may have been spoofed.

The official email addresses of our properties are as follows.

- THE AOYAMA GRAND HOTEL: reception@aoyamagrand.com
- THE ORIENT: oriental-rsv@plandosee.co.jp
- WITH THE STYLE FUKUOKA: style@plandosee.co.jp
- THE LUIGANS Spa & Resort: luigans@plandosee.co.jp
- OCHIAIRO: info@ochiairo.co.jp
- MARUFUKURO: reservation-mfr@plandosee.co.jp
- THE ALPS HOTEL HAKUBA: info@thealpshotelhakuba.com
- Southwest Grand Hotel: reception@southwestgrand.com
- South Gate Hotel Okinawa: reception@southgatehotel.jp
- THE UBUFURU ISHIGAKI: ishigaki-reception@plandosee.co.jp

[Inquiries Regarding the System Involved in This Incident]

Temairazu Co., Ltd. Emergency Help Desk

helpdesk@temairazu.com

Once again, we extend our deepest apologies for the considerable concern and inconvenience this matter has caused.

Sincerely,

Plan・Do・See Inc.

【重要】ご予約情報への不正アクセスに関するお詫びとお知らせ

2026年10月15日

お客様各位

いつも当社が運営するホテルをご利用いただき、誠にありがとうございます。

このたび、当社運営ホテルが予約管理に利用している外部のシステムに第三者による不正アクセスがあり、お客様のご予約に関する情報が閲覧・取得された可能性があることが判明いたしました。多大なるご心配とご迷惑をおかけしますことを、心よりお詫び申し上げます。

1. 概要

2026年9月21日、当社運営ホテルが予約管理に利用しているシステム「TEMAIRAZU」（提供元：手間いらず株式会社）に対し、第三者による不正アクセスが行われました。同システムに保存されていたご予約情報の一部が、外部から閲覧・取得された可能性を否定できない状況です。

対象となる可能性があるご予約：予約日が2026年9月21日まで、かつ宿泊日が2026年9月21日以降

2. 閲覧・取得された可能性がある情報

氏名・住所・電話番号・メールアドレス・宿泊日程・予約番号・宿泊料金・支払方法等を含む予約情報

クレジットカード情報は同システムで取り扱っておらず、含まれておりません。

3. 原因

手間いらず株式会社が過去に提供していたサービスの機能の一部に、セキュリティ上の問題があったことが原因です。同社は2026年9月26日に、原因箇所への対策を完了しており、引き続き外部の専門機関と連携して、調査を進めております。

4. 二次被害について

本件に関連し、当社運営ホテルや予約サイトを装った不審なメッセージ（WhatsApp、メール、SMS等）が送信され、クレジットカード情報の入力やお支払いを求められる事例が確認されております。最近では「オンラインチェックイン」「宿泊予定表」などを名乗る文面のメールも確認されています。

5. お客様へのお願い

- ・当社運営ホテルや予約サイトを装った不審なメッセージのURLやリンクを開かないください
- ・当社運営ホテルや予約サイトを装った不審なメッセージへクレジットカード情報や個人情報を入力しないでください
- ・当社運営ホテルや予約サイトを装った不審なメッセージには返信しないでください
- ・当該メッセージの指示による支払いや送金を行わないでください

万が一、不審なサイトにカード情報を入力された場合は、速やかにご利用のカード会社及び金融機関へご連絡ください。

6. 当社の対応

- ・手間いらず社及び関係する予約システム各社への再発防止調査依頼と原因の特定
- ・各ホテルWebサイトでの注意喚起

7. お問い合わせ

※送信元メールアドレスが当社運営ホテルのものであるように表示されている場合でも、送信元が偽造されている可能性がありますので、不審なメールに記載されたURLやリンクは開かないようお願いいたします。

当社運営ホテルの公式メールアドレスは以下のとおりです。

- ・THE AOYAMA GRAND HOTEL：reception@aoyamagrand.com
- ・THE ORIENT：oriental-rsv@plandosee.co.jp
- ・WITH THE STYLE FUKUOKA：style@plandosee.co.jp
- ・THE LUIGANS Spa & Resort：luigans@plandosee.co.jp
- ・おちあいろう：info@ochiairo.co.jp
- ・丸福樓：reservation-mfr@plandosee.co.jp
- ・THE ALPS HOTEL HAKUBA：info@thealpshotelhakuba.com
- ・Southwest Grand Hotel：reception@southwestgrand.com
- ・South Gate Hotel Okinawa：reception@southgatehotel.jp
- ・THE UBUFURU ISHIGAKI：ishigaki-reception@plandosee.co.jp

【本件の原因となったシステムに関するお問い合わせ】

手間いらず株式会社 緊急ヘルプデスク
helpdesk@temairazu.com

あらためて、多大なるご心配とご迷惑をおかけしておりますことを、深くお詫び申し上げます。

株式会社Plan・Do・See