

## 弊社業務委託先における不正アクセス被害に伴う情報漏えいのおそれについて

弊社が点検サポート業務の一部を委託している委託先（日本テレネット株式会社（以下「日本テレネット社」といいます。))のサーバにおいて不正アクセス被害が発生し、弊社のお客さま情報の漏えいのおそれがあることが、2026年4月8日に日本テレネット社からの報告により判明いたしました。

お客さまおよび関係者の皆様にご心配、ご迷惑をおかけすることとなり深くお詫び申し上げます。

以下、本日時点で判明している状況について、お知らせいたします。

### <情報漏えいのおそれがある弊社お客さま情報>

弊社の点検サポート業務（以下「本業務」といいます。）のうち、コールセンター業務の一部に係る発注者様・住宅事業者様のお名前、電話番号、住所、会社名、メールアドレス等合計43,362件です（なお、病歴などの要配慮個人情報やクレジットカード番号など直接的に財産的被害が発生するおそれがある個人情報は含まれておりません。）。

詳細はこちらをご覧ください。

[サイバー攻撃によるシステム障害発生について - 日本テレネット株式会社 -  
https://www.nippon-tele.net/](https://www.nippon-tele.net/)

### <委託先からの報告>

現時点で日本テレネット社からは以下の報告を受けております。

#### 1 判明の経緯及び対象となった情報

日本テレネット社は、当初、今回のサイバー攻撃の対象となったサーバ（以下「対象サーバ」といいます。）は、本業務のサービスサーバとは別環境での運用になっており、攻撃対象範囲外である旨判断しておりました。

その後、日本テレネット社において、弊社の情報が対象サーバに保存されていた可能性はないか詳細に調査したところ、本業務に利用していたデータ（以下「対象データ」といいます。）が、対象サーバに保存されていることが判明いたしました。

対象データは、弊社と日本テレネット社との間で定めた業務要件に基づいて、本業務のうち架電業務を実施する際の元データとして使用するために、対象サーバに保存していたものです。対象データには43,362件の個人情報が含まれており、具体的には発注者様・住宅事業者様のお名前、電話番号、住所、会社名、メールアドレス等が含まれております。

## 2 情報漏えいの調査状況

現時点において、対象データが外部へ流出した事実は確認されておりません。加えて、日本テレネット社のコンタクトセンターに対して、これらに関連する被害のお申し出も確認されておりません。引き続き、日本テレネット社において外部専門業者に依頼し、ダークウェブモニタリングを実施することを予定しております。

この過程において対象データが漏えいした事実が確認された場合には、速やかにお知らせいたします。

### < 弊社の対応 >

本件については日本テレネット社とともに調査を継続中ではあるものの、本件判明後、現時点において対象データの外部流出や第三者による二次利用その他不正利用等の事実は確認されておりません。

しかしながら、弊社としても本件を厳粛に受け止め、委託先の管理を含め、より一層の管理体制の強化に努めるとともに、不正アクセスなどの犯罪行為には厳正に対処してまいります。

今後、万が一にも情報流出や不正利用などを確認いたしましたら個別にご連絡させていただきます。

本件に関連しまして、ご心配やご不明な点がございましたら、以下のお問い合わせ窓口までご連絡いただきますようお願い申し上げます。

< 本業務に関するお問い合わせ窓口（ハウスプラス住宅保証株式会社） >

WEB : [https://www.houseplus.co.jp/hpj/contact/contactform\\_hc.html](https://www.houseplus.co.jp/hpj/contact/contactform_hc.html)

< 情報漏えいに関するお問い合わせ窓口（日本テレネット株式会社） >

電話番号：050-3207-1513

受付時間：平日 9：00～17:00

（土日・祝日を除く）

※本窓口は、日本テレネット株式会社によって運営されています。

以上