当社システムへの不正アクセスに関するご案内

2026/9/10更新

このたびは、お客さま、お取引先、パートナー企業その他関係者の皆さまに、多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。

2026年9月10日に公表いたしました「当社システムへの不正アクセスに関する調査結果および再発防止策について（第三報）」に関し、本ページではお客さま向けの情報をまとめてご案内しております。
最新のニュースリリース、よくあるご質問（FAQ）のほか、必要なお知らせを随時掲載いたします。

目次

- 最新のニュースリリース
- よくあるご質問
- 不正アクセスに関するお問い合わせ窓口

最新のニュースリリース

- 当社システムへの不正アクセスに関する調査結果および再発防止策について（第三報）（2026/9/10）

よくあるご質問

すべてのFAQを開く　すべてのFAQを閉じる

お知らせ・対象範囲について

今回の第三報は何ですか。第一報、第二報と何が変わったのですか。

開く

第一報では「さくらのレンタルサーバ」の一部環境に対する不正アクセス、一部サーバーへのマルウェア設置、および一部のお客さま情報が閲覧または取得された可能性についてお知らせしました。

第二報では、調査の過程で新たに当社の販売管理システムに対する不正アクセスの可能性を確認し、会員情報等への影響の可能性についてお知らせしました。

第三報では、一連の調査結果を踏まえ、不正アクセスの影響範囲、対象となる可能性のある情報、実施した対応および再発防止策についてご報告しています。

調査の結果、データが外部へ持ち出されたことを裏付ける明確な事実や、本件に起因する情報の不正利用・その他の二次被害は現時点で確認されておりません。

自分が1,360,563アカウントの対象かどうか、どうすれば確認できますか。

開く

調査の結果、当社システムに保存されていた会員情報について、影響を受けた可能性のある対象は1,360,563アカウントであることが判明しております。

対象となるお客さまには個別にご案内しております。

今後、新たにお客さまへのご案内が必要と判断した場合は、対象となるお客さまへ個別にご案内するとともに、当社ウェブサイトでもお知らせいたします。

なお、登録情報の不備等により個別のご案内が困難なお客さまについては、第三報の公表をもってお知らせに代えさせていただいております。

ご不安な場合は、予防的措置としてパスワードのご変更をお勧めしております。

1,360,563アカウントとは何ですか。

開く

当社サービスをご利用いただいているお客さまの契約情報等を管理する販売管理システムに保存されていた会員情報のうち、第三者による閲覧または取得の可能性がある対象件数です。

1,360,563アカウントは対象となる可能性がある会員情報の総数を示しており、お客さまごとの情報について実際に閲覧または取得されたかを確認できた件数ではありません。

1,360,563アカウントすべてが漏えいしたのですか。

開く

調査の結果、販売管理システムに保存されていた会員情報等について、第三者による閲覧または取得の可能性があることを確認しております。

ただし、1,360,563アカウントすべてについて実際に閲覧または取得されたことを確認したものではありません。

951アカウントと1,360,563アカウントは重複していますか。

開く

はい、重複しています。

サービスは解約済みで、退会したはずなのにメールが届きました。なぜですか。

開く

サービスの解約と退会は異なるお手続きであり、お客さまご自身では退会された認識であっても、実際には退会手続きが完了していない場合がございます。

当社では、サービス（さくらのレンタルサーバ、さくらのクラウド等）をご解約いただいた後も、会員を退会されない限り、会員情報としてお客さまにご登録いただいた情報を保持しています。
今回不正アクセスを確認した販売管理システムには、これらの会員情報が保存されていたため、現在サービスをご利用いただいていないお客さまにも、ご登録のメールアドレス宛にご案内をお送りしております。

解約	ご利用中のサービス契約を終了するお手続き
退会	会員情報の削除を申請し、会員登録を終了するお手続き

会員の退会をご希望の場合は、以下をご確認ください。

› 会員の退会をしたい

今回の対象はレンタルサーバー利用者だけですか。

開く

販売管理システムへの不正アクセスにより、「さくらのレンタルサーバ」の利用者に限らず、当社に会員登録いただいているお客さまの会員情報について、第三者による閲覧または取得の可能性があることを確認しております。
なお、「さくらのレンタルサーバ」を除くサービス提供環境について、不正アクセスを示す兆候は確認されませんでした。

対象と連絡を受けていない場合、対応は不要ですか。

開く

現時点で対象のご案内を受けていない場合でも、予防措置としてパスワードの使い回しがないかご確認いただくことを推奨します。
また、本件に便乗したフィッシングメールや不審な電話等には十分ご注意ください。
今後、新たに公表すべき事実が判明した場合は、当社Webサイト等でお知らせいたします。

メールが本当にさくらインターネットから送られたものか確認したい。

開く

当社からのご案内は、差出人アドレス「support@sakura.ad.jp」よりお送りしております。メールの差出人アドレスをご確認ください。
メールの内容に不安がある場合は、メール内のリンクを利用せず、本ページのご案内をご確認ください。
なお、当社がメールや電話等でお客さまのパスワードや認証情報をお伺いすることはありません。

続報はいつありますか。

開く

今後、新たに公表すべき事実が判明した場合には速やかにお知らせします。
当社からのご連絡は、ご登録のメールアドレス宛および当社公式サイトのお知らせに限られます。

影響範囲について

どのような情報が漏えいした可能性がありますか。

開く

調査の結果、第三者による閲覧または取得の可能性がある情報として、以下を確認しております。

「さくらのレンタルサーバ」の一部のお客さま（951アカウント）	● メールデータ ● Webサイトデータ ● ログ情報 ● その他お客さまの利用領域内に保存されたファイル等
販売管理システムに保存されていた会員情報等（1,360,563アカウント）	● 会員ID ● 会社名 ● 部署名 ● 住所 ● 氏名 ● 電話番号 ● メールアドレス ● 生年月日 ● 性別 ● FAX番号 ● 契約サービス ● 契約期間 ● 請求金額等

なお、当社ではクレジットカード情報を保持していないため、**クレジットカード情報の漏えいはございません。**
また、上記は対象となる可能性のある情報項目を示すものであり、すべての情報が実際に閲覧または取得されたことを示すものではありません

クレジットカード情報は含まれていますか。

開く

当社ではクレジットカード情報を保持していないため、**クレジットカード情報の漏えいはございません。**

データは外部に持ち出されたのですか。

開く

データが外部へ持ち出されたことを裏付ける明確な事実は確認されておりません。
あわせて、本件に起因する情報の不正利用、その他の二次被害についても、現時点において確認されておりません。

自分の情報が実際に閲覧または取得されたか知りたい。

開く

調査の結果、販売管理システムに保存されていた会員情報等について、第三者による閲覧または取得の可能性があることを確認しておりますが、実際にどのお客さまのどの情報が閲覧または取得されたかについては特定できません。
なお、現時点でデータが外部へ持ち出されたことを裏付ける明確な事実は確認されておらず、本件に起因する情報の不正利用やその他の二次被害も確認されておりません。

今後、新たにお客さまへのご案内が必要と判断した場合は、対象となるお客さまへ個別にご案内するとともに、当社ウェブサイトでもお知らせいたします。

メールの内容や受信メールも閲覧されたのですか。

開く

第三報で公表しているとおり、「さくらのレンタルサーバ」の一部のお客さま（951アカウント）について、お客さま利用領域に保存されていたメールデータ、Webサイトデータ、ログ情報その他のファイル等が第三者により閲覧または取得された可能性があることを確認しております。

お客さまごとの情報について、どのデータが実際に閲覧または取得されたかを個別に特定することはできません。

なお、調査の結果、データが外部へ持ち出されたことを裏付ける明確な事実は確認されておらず、本件に起因する情報の不正利用やその他の二次被害も現時点では確認されておりません。

WordPressのデータやWebサイトのデータ、お問い合わせフォームの内容も閲覧された可能性がありますか。

開く

第三報で公表しているとおり、「さくらのレンタルサーバ」の一部のお客さま（951アカウント）について、お客さま利用領域に保存されていたメールデータ、Webサイトデータ、ログ情報その他のファイル等が第三者により閲覧または取得された可能性があることを確認しております。

お客さまごとの情報について、どのデータが実際に閲覧または取得されたかを個別に特定することはできません。

なお、調査の結果、データが外部へ持ち出されたことを裏付ける明確な事実は確認されておらず、本件に起因する情報の不正利用やその他の二次被害も現時点では確認されておりません。

ドメイン・DNS設定に影響はありますか。

開く

ドメイン設定やDNS設定が不正に変更された事実は確認されておりません。

ご心配な場合は、会員メニューやドメインコントロールパネルにて設定内容をご確認ください。

二次被害は確認されていますか。

開く

現時点で、本件に起因する情報の不正利用やその他の二次被害は確認されておりません。

また、本件の対象となった情報がインターネットやダークウェブ上で公開された事実も確認されておりません。

ただし、本件に便乗したフィッシングメールや不審な電話には十分ご注意ください。

※ダークウェブ：一般的な検索エンジンでは見つけることができないインターネット上の領域で、情報の売買などに悪用されることがあります。

パスワード・認証について

パスワード情報も漏えいしたのですか。

開く

一部のお客さまについて、ハッシュ化された会員IDのパスワード情報30アカウントが第三者に閲覧された可能性があることを確認しております。
※ハッシュ化されたパスワード情報：元のパスワードには復元が困難な状態にしたデータ。

さくらのレンタルサーバをご利用のお客さま

販売管理システムに保存されていた情報には、「さくらのレンタルサーバ」の一部の初期サーバーパスワードが含まれます。
「さくらのレンタルサーバ」においては、影響を受けた可能性のあるサーバーパスワードが現在も利用されていることが確認できた契約について、お客さまのアカウント保護および第三者による不正利用防止のため、当社にてサーバーパスワードを変更させていただきました。
対象となるお客さまに対しては個別にご案内しておりますので、会員メニューへログインしていただき、お客さまご自身の任意のパスワードに変更いただくようお願いしております。

さくらのVPSをご利用のお客さま

販売管理システムに保存されていた情報には、「さくらのVPS」の一部における管理者初期パスワードが含まれます。
当該情報が保存されていた「さくらのVPS」を契約のお客さまに対しては個別にご案内し、現在も契約時に発行された初期パスワードをご利用の場合には、パスワードを変更いただくようお願いしております。

パスワードは変更した方がいいですか。

開く

サーバーパスワード、メールパスワード

さくらのレンタルサーバ・さくらのメールボックスのサーバーパスワード、メールパスワードの変更について、対象となるお客さまへ個別にご案内しております。

会員メニューパスワード

当社の会員メニューでは、ログイン時に2要素認証（ご登録メールアドレスへの認証コード送信、SMS認証、または認証アプリ）を必須としております。
パスワードのみではログインできない仕組みとなっているため、会員メニューのパスワードを直ちに変更いただく必要性は高くありません。
詳細は本ページ内「会員メニューのパスワードは変更する必要がありますか。」をご確認ください。

会員メニューのパスワードは変更する必要がありますか。

開く

当社の会員メニューでは、ログイン時に2要素認証（ご登録メールアドレスへの認証コード送信、SMS認証、または認証アプリ）を必須としております。
パスワードのみではログインできない仕組みとなっているため、会員メニューのパスワードを直ちに変更いただく必要性は高くありません。
ただし、より安全にご利用いただくための予防的措置として、以下のご確認をお勧めいたします。

- 他サービスで使い回しているパスワードの変更
  当社と同じパスワードを他のWebサービスでもご利用の場合は、不正ログインの被害を防ぐため、他サービス側のパスワードを変更いただくことを強くお勧めいたします。
- 会員メニューパスワードの変更
  念のため変更をご希望される場合は、以下よりお手続きいただけます。
  › 会員メニューパスワードを変更したい

- 2要素認証設定の確認
  より強固な認証方式（SMSや認証アプリ等）への変更・設定確認は以下をご確認ください。
  - 会員メニューの2要素認証のログイン方法・設定変更

セキュリティ対策・その他

今、自分は何をすればいいですか。

開く

当社では、本件に関する公表および FAQ の公開を行うとともに、お問い合わせ窓口を設置し対応を継続しております。
また、以下のお客さまに対して、電子メール等により個別にご案内しております。

- 「さくらのレンタルサーバ」について影響を受けた可能性があるお客さま（サーバーパスワードおよびメールパスワードの変更が必要と判断したお客さまを含む）
- 管理者用の初期パスワードの確認および変更が必要と判断した「さくらの VPS」のお客さま
- 販売管理システムに保存されていた会員情報について影響を受けた可能性があるお客さま

個別のご案内を受け取られたお客さまにおかれましては、ご案内内容をご確認のうえ、必要な対応をお願いいたします。
また、本件に便乗したフィッシングメールや不審な電話、SMS等には十分ご注意ください。

今後、お客さまご自身による新たな対応が必要であることが判明した場合には、対象となるお客さまへ個別にご案内するとともに、当社ウェブサイトでもお知らせいたします。

この機会に見直しておくべきセキュリティ対策はありますか。

開く

本件に関わらず、安全に各種サービスをご利用いただくため、以下のセキュリティ対策の見直しをお勧めいたします。

- パスワードの使い回しの解消
  複数のサービスで同一のパスワードを使い回さないよう、サービスごとに異なるパスワードを設定してください。
- 登録情報の最新化
  当社からの重要なお知らせや2要素認証コードを確実に受信できるよう、登録されているメールアドレスや電話番号が現在利用可能なものであるかをご確認ください。
- 不要なアカウントの整理
  長期間ご利用になっていないWebサービスのアカウントやメールアドレス等がある場合は、アカウント削除や登録情報の見直しをご検討ください。
  - 登録情報の確認・変更をしたい
  - 会員メニューの2要素認証のログイン方法・設定変更
- 不審な連絡への警戒
  お心当たりのないログイン通知やメールを受信した場合は、送信元や内容をご確認いただき、不審な点がある場合は記載されたリンクのクリックや添付ファイルの開封はお控えください。
  なお、**当社からパスワードや認証コード、クレジットカード情報等をメールや電話でお伺いすることはありません。**

不審なメールが届きました。今回の件と関係ありますか。

開く

個別のメールと本件との関連性は判断できません。
また、本件に起因する情報の不正利用やその他の二次被害は現時点で確認されておりません。

不審なメールを受信した場合は、リンクや添付ファイルを開かず削除してください。
当社がメールや電話等でパスワードや認証情報をお伺いすることはありません。

不正アクセスに関するお問い合わせ窓口

お客さまからのお問い合わせ先

メール	support@sakura.ad.jp
電話（本件専用）	0120-378-719 受付時間：10:00〜18:00（土日祝を除く）

※お問い合わせの際は、会員IDをお知らせください。
※電話は本件専用の窓口です。本件以外のサービスに関するお問い合わせは、カスタマーセンターをご利用ください。
※ **当社からお電話にてパスワードやクレジットカード情報をお伺いすることはありません。不審な電話にご注意ください。**

© SAKURA internet Inc.