

2026 年 10 月 21 日

お客様各位

株式会社ネットアシスト

【重要】セキュリティ関連のお問い合わせ増加に伴う

対応についてのご案内

平素より弊社サービスをご利用いただき、誠にありがとうございます。

現在、さくらのクラウドにおける脆弱性対応に伴うメンテナンスへの対応に加え、PHP の脆弱性に関する情報の公表を受け、弊社へのお問い合わせおよび対応のご依頼が増加しております。

また、昨今のセキュリティに関するお問い合わせや緊急対応の増加も重なり、対象環境の確認、お問い合わせへの回答、作業日程の調整および作業の実施までに、通常よりお時間をいただいております。

お客様にはご不便、ご心配をおかけいたしますが、現在の状況と弊社の対応方針について、以下のとおりご案内申し上げます。

1. 現在の対応状況について

今回の一連の脆弱性対応では、多数のサーバー・システムについて、影響の有無や対策の必要性を確認する必要があります。

弊社では、公開情報やサービス提供元からの案内を確認するとともに、お客様のご契約内容や対象環境に応じて、必要な調査および対応の検討を順次進めております。

脆弱性への対応は、対象環境や稼働中のサービスによって作業内容・影響が異なるため、事前の確認を行ったうえで進める必要があります。

また、詳細情報や修正プログラムの公開状況によっては、対応方法や実施時期を直ちにご案内できない場合がございます。

2. 弊社の運用体制と現在の対応状況について

弊社では、多数のサーバー環境について、24 時間 365 日の監視・運用保守サービスを提供しております。

そのうえで、一連のセキュリティ対応およびお客様からのご依頼対応を進めております。

弊社が管理する非常に多くのサーバーが対応対象となっており、通常の運用保守業務に加えて、多数の対応が発生しております。

また、昨今のサイバー攻撃の増加や攻撃手法の高度化に伴い、弊社においてもセキュリティ関連のお問い合わせや緊急対応のご依頼が非常に増加しております。

特に夜間帯や休日は、通常の監視業務に加え、突発的な障害やセキュリティインシデントに迅速に対応できる体制を確保する必要があるとございます。

個別の作業を過度に集中させることは、通常の監視・障害対応体制に影響を及ぼすだけでなく、作業品質の低下や新たな障害リスクにつながるおそれがございます。

こうした状況下において、至急の対応やお客様のご希望日時（夜間・休日）に合わせた対応をご希望されることは、弊社としても十分に理解しております。

そのため、弊社としては、すべてのお客様のシステムの安全性と安定稼働を守るという観点から、対応リソースの適切な配分と運用品質の維持を最優先に判断する必要があるとございます。

3. 一連のご依頼に関する弊社の対応方針

- ・ご契約内容、対象環境、緊急性およびシステムへの影響等を順次確認してまいります。
- ・お問い合わせへの回答や作業の実施までに、お時間をいただく場合がございます。
- ・ご希望の作業日時や回答期限に沿えない場合がございます。
- ・さくらのクラウドのメンテナンスに伴う事前再起動については、別途ご案内のとおり、お客様ごとの個別のご希望日時に合わせた作業は、原則としてお受けいたしかねます。

なお、業務上の重大な影響が想定されるなど、特別な事情がある場合には個別にご相談を承りますが、作業日時や対応の可否につきましては、弊社の運用体制および全体の対応状況を踏まえて判断させていただきます。

4. お客様へのお願い

弊社は、24 時間 365 日の監視・運用保守サービスを提供する MSP 事業者として、お客様のシステムの安定稼働を支える責任を担っております。

今回のような広範囲に及ぶ緊急のセキュリティ対応においては、個別のご要望に可能な限りお応えすることも重要である一方、すべてのお客様に対する監視・障害対応体制を維持し、全体の安全性と運用品質を確保することが、弊社の最も重要な責務であると考えております。

お客様にはご不便、ご心配をおかけすることもあるかと存じますが、今回の対応方針は、限られた運用リソースの中で、すべてのお客様のシステムを安全かつ安定的に運用するための判断となります。

何卒、事情をご賢察のうえ、ご理解とご協力を賜りますようお願い申し上げます。
弊社といたしましても、関連情報を注視し、お客様への影響を可能な限り抑えながら、適切な対応に努めてまいります。

以上

参考情報

さくらインターネット株式会社

<https://www.sakura.ad.jp/corporate/information/announcements/2026/10/16/1968226051/>

さくらのクラウド 脆弱性対応状況

<https://cloud.sakura.ad.jp/news/2026/10/16/cve-2026-99999/>

PHP 公式告知

<https://www.php.net/archive/2026.php#2026-10-20-1>

脆弱性の概要と対応指針（GMO Flatt Security）

<https://blog.flatt.tech/entry/php2shell>