平素は当サービスをご利用いただき誠にありがとうございます。
エックスサーバーサポートでございます。

```
XServerアカウントID：[アカウントID]
サーバーID　　：[サーバーID]（[サーバーホスト名]）
ドメイン名　　：[ドメイン1]
　　[ドメイン2]
　　[ドメイン3]
...

お問合せ番号：[お問合せ番号]
```

お客様のサーバーアカウントにおいて、サーバーに対する負荷が著しく高い状況を確認いたしました。
この度の負荷上昇に際してプロセスの稼働状況を確認しましたところ、以下の不正なプロセスが多数稼働しておりました。

▼稼働していた不正なプロセス

```
Sat Sep 20 18:07:57 2025 /opt/php-7.4.33-2/bin/php /home/[サーバーID]/[ドメイン名]/public_html/l.php
```

…

これを受け、当サポートにてセキュリティ調査を行いましたところ、
お客様がご利用のプログラムにセキュリティ上致命的なバグ（脆弱性）が存在し、
当該脆弱性を第三者に悪用されてしまった可能性が非常に高い状況でございました。

そのため、事後のご案内となり大変恐縮でございますが、緊急措置として下記制限を実施しております。

▼サポートにて実施した制限内容

```
・複数ドメインにおいて「WordPressセキュリティ設定」の全機能を有効化
 ▼マニュアル > WordPressセキュリティ設定
 https://www.xserver.ne.jp/manual/man_server_wpsecurity.php

 https://support.xserver.ne.jp/manual/man_server_wpsecurity.php

・複数ドメインにおいて「WAF設定」の全機能を有効化
 ▼マニュアル > WAF設定
 https://www.xserver.ne.jp/manual/man_server_waf.php

 https://support.xserver.ne.jp/manual/man_server_waf.php

・設置されていた不正プログラムファイルについて、パーミッションを「000」へ変更し、機能を無効化
```

[不正プログラムと思われるファイル一覧]
…

この度のような不正アクセスの被害に遭われた場合、検出された不正なファイル以外にも、
他の不正なファイルやバックドア（不正アクセスを容易とする仕組み）などが設置されている可能性が考えられます。

不正アクセスによる被害の発生を防ぐため、下記内容をご確認いただき、ご対応下さいますよう、よろしくお願いいたします。

…

【1】サポートにて実施したセキュリティ調査について

お客様のサーバーアカウントにおいて
前述の不正なファイル（ウイルス、マルウェアなど）が検出されるとともに、

日本国外からの不審なアクセスを確認いたしました。

[不審なアクセスログの一部]

```
[ドメイン名] [IPアドレス] - - [20/Sep/2025:18:07:45 +0900] "POST /about.php?520 HTTP/1.1" 200 1750 "-" "Mozilla/5.0 (Wi
[ドメイン名] [IPアドレス] - - [20/Sep/2025:18:07:46 +0900] "POST /about.php?520 HTTP/1.1" 200 1787 "-" "Mozilla/5.0 (Wi
```

上記ログに記載されているファイルにつきましては、
不正に設置または改ざんされている可能性が高くございます。

なお、不正アクセスの根本原因は下記パターンに大別されます。

▼不正アクセスの根本原因

```
(1)お客様が運用中のプログラム(WordPress等)において
  [1]プログラム(WordPress等)の管理パスワードが流出し、第三者に不正ログインされた。
  [2]セキュリティ上問題のある致命的なバグ（脆弱性）が存在し、第三者に脆弱性を利用された。

  不正ログインされる、もしくは脆弱性が存在する場合、WordPressに限らず
  下記のような操作をプログラム経由で実施されてしまう可能性がございます。

  （一例）
  ・WordPressやFTP、メール等のアカウントのID、パスワードの奪取
  ・不正なアカウント、不正なファイルの設置
  ・既存ファイルの改ざん
  ・他者への攻撃の実行
  ・不正なコンテンツ、フィッシングサイトの公開・開設


(2)お客様のサーバーアカウントに関するFTP情報が流出し、
  第三者に不正にFTP接続をされた。

  →FTP操作自体によるファイル改ざんはもとより、
    任意のプログラムを設置することでどんな操作でも実行できてしまいます。
```

お客様のサーバーアカウントにおいては不審なFTPアクセスが見られないことから、
消去法的なご案内となりますが、
プログラム(WordPress等)の管理パスワードが流出しプログラムを悪用されたか
お客様が運用中のプログラムの脆弱性を悪用されてしまった可能性が高いものと思われます。

【2】お客様に行っていただきたい対応内容について

お客様のPCや運用中のサイトのセキュリティ対策は
お客様ご自身にて管理を行っていただく責任がございます。

この度の不正アクセスについて、原因を根絶し、不正に設置されたファイルや
改ざんされたファイルをサーバーアカウント上から完全に駆逐するため、
大変お手数ですが、下記作業をなさいますようお願いいたします。

1. **ご利用のPCにてセキュリティチェックを行ってください。**

お客様のご利用PC端末にてセキュリティソフトを最新版に更新していただき、
ウイルスチェックと駆除をおこなってください。

また、Windows UpdateやAdobe Reader、Flash Playerなどの
ご利用PC端末にインストールされているソフトウェアにつきましても、
最新版へ更新してください。

※本件はプログラムの脆弱性に起因する不正アクセスの可能性が高い状況では
ございますが、念のため上記ご確認をお願いいたします。

2. **検出されているすべてのファイルの完全削除　または、該当ドメイン名を「初期化」してください。**

下記、ケース1、ケース2のうち【いずれか一方のみ】を実施してください。
※いずれの対応を行った場合でも、後続[3] 〜 [5]の作業は必須となります。

※バックアップ機能からデータ復元をご検討のお客様へ
ドメインの「初期化」をご対応前に、サーバーパネル「バックアップ機能」画面より
バックアップデータが取得できることを必ずご確認いただいた上で
作業を進めていただくようお願いいたします。

※一部のお客様環境では、ファイル数過多等による負荷が原因となり、
自動バックアップ機能の対象から除外されております。

ケース1■検出されているすべてのファイルの完全削除する場合　（※推奨）

前述「サポートにて実施した制限内容」にリストアップされている
[不正プログラムと思われるファイル一覧]に記載されている【すべてのファイル】について
ファイルの削除を実施してください。

※ファイルを別の場所に移動させる、ファイル名を変更するといった対応は効果がございません。

※パーミッションが000となっているものを削除せず、他者が実行できる状態にすると
不正な攻撃が再発し、サポートにおいてより強い制限を実施する可能性がございます。

※バックアップや作業用端末に保存されているファイルもすでに汚染されている可能性がございます。
再発防止のため、セキュリティ上問題のない、改ざんされていないクリーンな
データをアップロードなさいますようお願いいたいます。

ケース2■該当ドメイン名を「初期化」する場合　※該当ドメイン名のウェブ領域に設置されたすべてのファイルが削除されます

「サーバーパネル」→「ドメイン設定」→該当ドメインの「初期化」とアクセスしていただき、「ウェブ領域・設定の初期化」をご選択のうえ、該当ドメイン名を初期化してください。

※複数のドメインが汚染されている場合は、不正プログラムが1つ以上設置されていたドメインについてドメイン名を初期化することを推奨いたします。

※上記作業により、該当ドメイン名のウェブ領域に設置されたすべてのファイルが削除されます。

画像、プログラム、設定ファイルなどの必要なデータは事前にバックアップを取った上でドメイン名を初期化してください。

※上記作業による、データベースの初期化・削除はございません。

[3] FTPソフトによるデータアップロードなど、ホームページ再開のための作業を行ってください。

制限時点のデータは不正に改ざんされているデータを含む可能性や
セキュリティ上問題がある可能性がございます。

再発防止のため、セキュリティ上問題のない、改ざんされていないクリーンな
　データをアップロードなさいますようお願いいたいます。

※CGIプログラムをご利用の場合はパーミッションの変更にご注意ください。

[4] 該当ドメインにて設置されていたプログラムにおいて、脆弱性の調査を必ず行ってください。

不正アクセスの原因を明確にした上で、
　ホームページの運用を再開なさいますようお願いいたします。

※不正アクセスの原因を特定しないままホームページを再開した場合、
　　再度同様の被害に遭う可能性が非常に高くなってしまいます。

◆「WordPress」や「Joomla!」などのCMSツールをご利用の場合、
　　脆弱性が発表されていない最新バージョンを必ずご利用ください。
　　旧バージョンのCMSツールには、脆弱性が報告されているケースが
　　非常に多くございます。

また、プラグインやテーマファイルにつきましても、
　　最新のものを新規にインストールしていただくことを推奨いたします。

[5] 設置されているWordPress等の設置プログラムについて管理パスワードを変更してください。

WordPress等の設置プログラムにて、管理画面より管理パスワードの変更をお願いいたします。

既に【パスワードが攻撃者によって特定】されており
　悪用されている可能性が非常に高い状況です。

　【重要】管理パスワードの変更をお願いいたします

　パスワード総当り(ブルートフォースアタック)による攻撃や、
　お客様が運用中のプログラムに脆弱性が存在し、
　該当脆弱性を悪用され、不正にアクセスの被害にあわれた可能性が高いものと思われます。

　※これまでと同じパスワードは絶対に設定しないでください。
　　また、アルファベット・数字を絡めた、第三者に推測されづらい
　　パスワードをご設定ください。

　※念のため、今回不正アクセスが発生しておりましたドメイン以外の
　　WordPress・その他設置プログラムでも、同様に管理パスワードの変更をご検討お願いいたします。

【3】推奨される設定について

お客様のウェブサイトにてPHPプログラムをご利用の場合、
サーバーパネルの「php.ini設定」にて
「allow_url_fopen」および「allow_url_include」をいずれも
「無効（Off）」にすることを強くお勧めいたします。

◇マニュアル：php.ini設定
　https://www.xserver.ne.jp/manual/man_server_phpini_edit.php

※上記設定項目は「外部ファイルを読み込む/実行する」操作に対する可否設定です。

ご利用のプログラムにより、上記それぞれの設定を「On」にする
　必要がある場合もございますが、外部からのデータ読み込み等が必要ない場合、

これら設定は無効にしたうえでプログラムをご運用ください。

【4】自動バックアップ機能について

サーバーパネル内の『自動バックアップ』機能により、
過去のデータはバックアップされており
無償でバックアップデータの取得が可能です。

バックアップデータを公開領域に設置する際には、
特に【1】でご案内した不正ファイルが含まれていないかどうか、
十分ご確認いただいた上でご利用ください。

◇自動バックアップとは？
https://www.xserver.ne.jp/functions/service_backup.php
https://business.xserver.ne.jp/service/detail_backup.php

◇自動バックアップからのデータ取得
https://www.xserver.ne.jp/manual/man_server_download.php
https://support.xserver.ne.jp/manual/man_server_download.php

なお、今後、同様の状況が再度確認された場合、
さらなる制限を実施する可能性がございます。

不正アクセスによる被害の発生・再発を防ぐための措置でございます。
何卒ご理解くださいますようお願いいたします。

以上、何卒よろしくお願い申し上げます。
ご不明な点などございましたら、お気軽にお問い合わせください。

◆本内容と関連するお問い合わせの際は..