

## 必要な対応措置①

### セキュリティチェックと不正ファイルの削除

#### PCのセキュリティチェック

ご利用のPC端末のセキュリティソフトを最新版に更新し、ウイルスチェックと駆除を行ってください。Windows UpdateやAdobe Readerなどのソフトウェアも最新版に更新することをお勧めします。

#### 不正ファイルの完全削除


添付ファイル「20250614\_infectedfiles\_XXXXXXXXXX.txt」に記載されているすべての不正ファイルを削除してください。ファイルを別の場所に移動したり、名前を変更したりする対応では効果がありません。

#### ドメインの初期化(代替手段)

不正ファイルの削除が難しい場合は、サーバーパネルの「ドメイン設定」から該当ドメインを初期化することも可能です。この場合、そのドメインのウェブ領域のすべてのファイルが削除されますので、必要なデータは事前にバックアップを取ってください。

汚染されたファイルとは、サーバー内の他のPHPファイルを不正に書き換え、ウェブサイトにアクセスできない状態にしたり、不審なフィッシングサイトにリダイレクトするものです。完全に削除することが重要です。





# サイバーセキュリティ 脅威への対応ガイド

エックスサーバーをご利用のお客様へ、サーバーセキュリティに関する重要なお案内をいたします。お客様のウェブサイトにおいて不正アクセスが検出され、緊急措置が必要な状況です。このプレゼンテーションでは、発生した問題と対応方法について詳細にご説明いたします。

セキュリティ対策は、お客様のデータとウェブサイトを守るために不可欠です。適切な対応と予防策を講じることで、今後の被害を防ぐことができます。

**Yukiko Hamabe**

# 不正アクセスの概要と緊急措置

お客様のサーバーアカウントにおいて不審なファイルの設置が確認され、日本国外からの不審なアクセスも検出されました。これらは、ウイルスやマルウェアといった不正プログラムである可能性が高いです。

## 脆弱性の発見

お客様が運用中のプログラム (WordPress など) にセキュリティ上致命的なバグ (脆弱性) が存在していました。

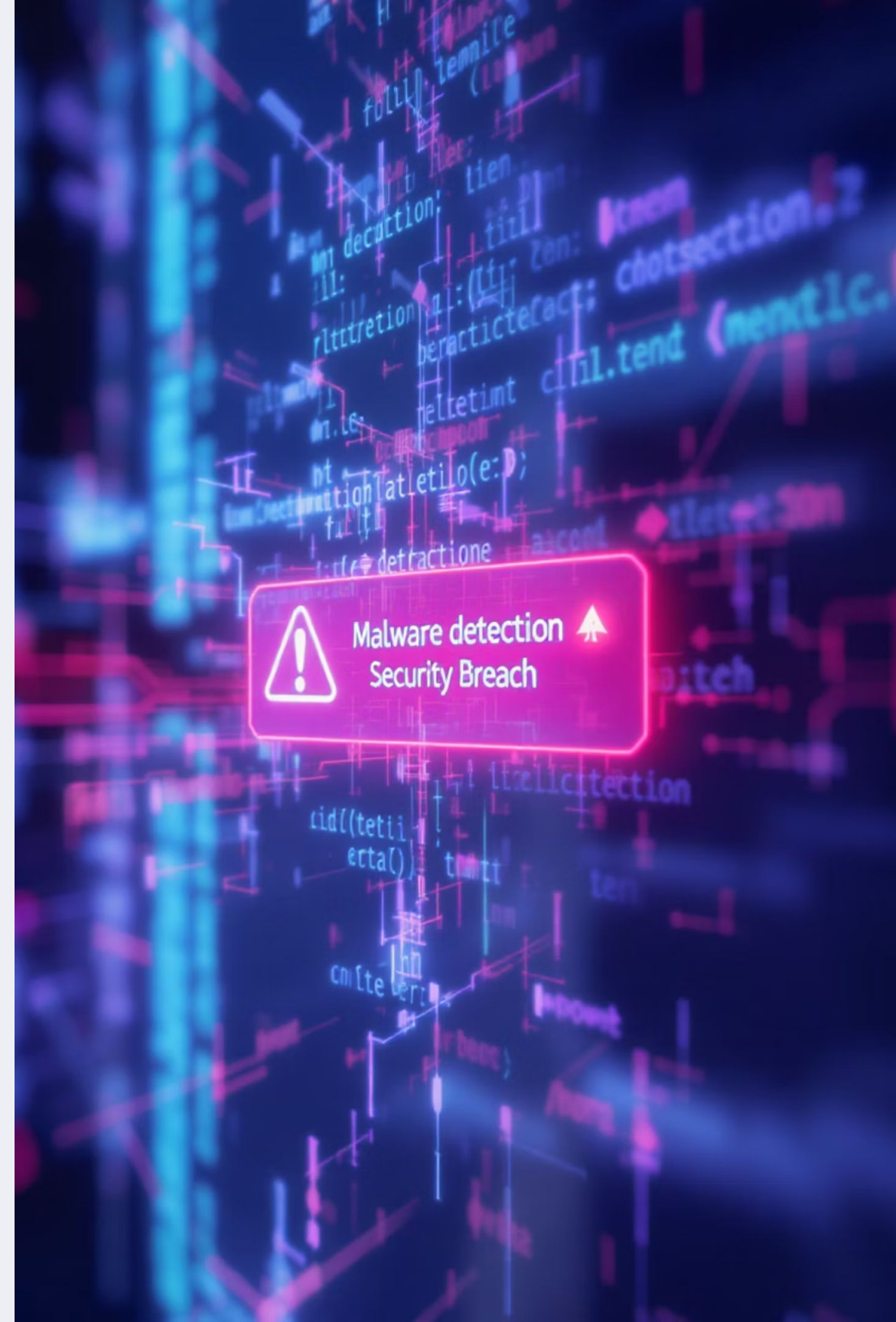
## 不正アクセスの発生

第三者によってその脆弱性が悪用され、サーバーに不正アクセスが行われました。

## 緊急保護措置

エックスサーバーサポートにて、WordPress セキュリティ設定と WAF 設定の全機能を有効化しました。

また、不正プログラムファイルについては、パーミッションを「000」へ変更し、機能を無効化する措置を取らせていただきました。



# 不正アクセスの原因分析

## 考えられる主な原因

お客様のサーバーアカウントでは不審なFTPアクセスが見られないことから、次の2つの可能性が高いと考えられます：

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. ご利用のプログラムに脆弱性が存在し、それが悪用された

検出された不正ファイル以外にも、バックドア (不正アクセスを容易にする仕組み) が設置されている可能性があります。  
サイト全体の安全性を確保するため、早急な対応が必要です。

## 不正アクセスによる影響

不正アクセスにより、以下のような操作が行われる可能性があります：

- ・ アカウント情報 (ID・パスワード) の奪取
- ・ 不正なファイルの設置
- ・ 既存ファイルの改ざん
- ・ フィッシングサイトの公開
- ・ 他サイトへの攻撃の踏み台として利用

## 必要な対応措置②

# 安全なサイト復旧と再発防止

### 1 クリーンなデータのアップロード

FTPソフトを使用して、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してください。バックアップデータを使用する場合も、不正ファイルが含まれていないか十分確認してください。

### 2 脆弱性の調査と修正

設置されていたプログラム（WordPressなど）の脆弱性を調査し、最新バージョンにアップデートしてください。プラグインやテーマファイルも最新のものを新規にインストールすることをお勧めします。

### 3 管理パスワードの変更

WordPress等の管理画面より、管理パスワードを必ず変更してください。これまでと同じパスワードは絶対に設定せず、アルファベット・数字を組み合わせた、第三者に推測されにくいパスワードを設定してください。

不正アクセスの原因を特定せずにホームページを再開すると、再度同様の被害に遭う可能性が非常に高くなります。セキュリティ対策を徹底した上で、サイトの復旧を行ってください。

# 推奨されるセキュリティ設定

## php.ini設定の最適化

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」において、以下の設定を「無効(Off)」にすることを強くお勧めします:

- allow\_url\_fopen
- allow\_url\_include

これらは「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。外部からのデータ読み込みが必要ない場合は、無効にすることでセキュリティが向上します。

## WordPressセキュリティ機能の活用

今回、サポートにて以下の設定を有効化しました:

- WordPressセキュリティ設定の全機能
- WAF設定の全機能

特に「**WAF設定**」については、コンテンツに支障がない限り、有効のままとすることを強くお勧めします。これにより、多くの不正アクセス試行をブロックすることができます。

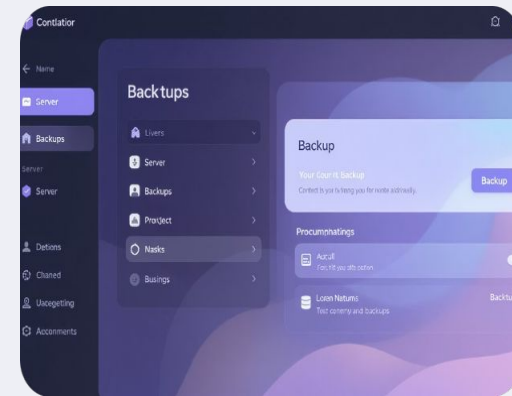
WordPressセキュリティ設定マニュアル

WAF設定マニュアル

# 自動バックアップ機能の活用方法

## バックアップの確認と取得

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。サーバーパネルにログインし、「バックアップ」メニューからデータを確認できます。



## バックアップからの復元

バックアップデータを公開領域に設置する際には、前述の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。クリーンな状態のバックアップを選択することが重要です。



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いる場合があります。ドメインの「初期化」を行う前に、サーバーパネルでバックアップデータが取得できることを必ず確認してください。

[自動バックアップについて詳細](#)

[バックアップデータ取得マニュアル](#)

# セキュリティ対策のまとめと次のステップ

## 不正ファイルの削除

添付ファイルに記載されているすべての不正ファイルを完全に削除するか、該当ドメインを初期化してください。



## セキュリティ設定の維持

WAF設定などのセキュリティ機能を有効にしたままにし、定期的にセキュリティチェックを行ってください。



## プログラムの更新

WordPressなどのCMSツール、プラグイン、テーマをすべて最新バージョンに更新してください。

## パスワード変更

管理パスワードを強固なものに変更し、定期的に更新する習慣をつけてください。

今後も同様の状況が確認された場合、さらなる制限を実施する可能性があります。セキュリティ対策は継続的に行うことが重要です。ご不明な点がございましたら、お問い合わせ番号を記載の上、エックスサーバーサポートまでお問い合わせください。

原因をつきとめることがまずは一番！

同じことの繰り返しが起こる場合、パスワードの漏洩ではない

ハッカーがウェブサーバーで操作できる状態になっている

その場合、  
Apache or NGINX ? はオープンソースなので、  
Webサーバーを停止しないことには、延々と戻らない