LAC SECURITY INSIGHT

第 18 号



JSOC JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

DiaForce

2026 年 11 月

株式会社ラック

LAC SECURITY INSIGHT

第 18 号／2026 秋

目　　次

03 はじめに

04 サイバー119 で出動したインシデント傾向

09 JSOC で観測したサイバー攻撃傾向

13 特集：wp2shell 攻撃の実態

LAC SECURITY INSIGHT（以下、本文書）は、情報提供を目的としており、記述を利用した結果生じるいかなる損失についても、株式会社ラックは責任を負いかねます。
本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。
LAC、ラック、JSOC、JSIG、サイバー救急センター、サイバー119 は、株式会社ラックの商標または登録商標です。
この他、本文書に記載した会社名・製品名は各社の商標または登録商標です。
表紙の写真は、フリー素材ぱくたそ（www.pakutaso.com）の写真を利用しています。
本文書を引用する際は出典元を必ず明記してください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

© 2026 LAC Co., Ltd. All Rights Reserved.

はじめに

本レポートは、ラックの中でもサイバー攻撃の脅威に対して最前線で対応している JSOC およびサイバー救急センター、そして攻撃者が利用するサイバー攻撃手法も活用してお客様のシステムへ侵入テストを行うデジタルペンテスト部において、分析・調査・侵入テストを実施する中で得た、最近の脅威の傾向や特徴を、セキュリティ専門家が「洞察」としてまとめたものです。

昨今、日本国内でもサイバー攻撃による深刻な被害が相次いでいます。攻撃による影響は一つの組織にとどまらず、取引先やサプライチェーンを含めて事業活動に影響が及ぶケースもあり、サイバー攻撃への備えはこれまで以上に重要になっています。

本レポートは、日々発生している実際の攻撃やインシデントに根ざし、日本の企業や団体を狙った脅威を中心にまとめています。単に個々の脅威や攻撃手法を紹介するだけではなく、実際の現場で観測された攻撃やインシデントを振り返り、その変化や特徴から何が読み取れるのかという視点を大切にしています。

サイバー攻撃を取り巻く環境は絶えず変化しており、セキュリティ対策についても、実際の脅威の変化を捉えながら継続的に見直していくことが重要です。

本レポートが、皆さまにとって自組織を取り巻く脅威を知るだけでなく、「自分たちの環境ではどうだろうか」と考え、次の対策につなげるきっかけとなれば幸いです。

株式会社ラック
MSS マネージドサービス部 JSOC アナリスト&サポート第二 G グループマネージャー
芹澤 宗寛

サイバー119で出動したインシデント傾向

2026年7月～9月の出動傾向

当該期間では、マルウェアによる被害の相談が23%、サーバ不正侵入による被害の相談が52%であり、両者で全体の75%を占めています。この割合は、前四半期（2026年4月から6月）の59%および前年同期（2025年7月から9月）の68%と比較して増加しています。特に、サーバ不正侵入による被害の相談は、前四半期（31%）および前年同期（39%）から増加し、当該期間の相談全体の半数を超えています。

マルウェア関連の被害では、ランサムウェアによる被害が全体の11%を占めています。前四半期（15%）および前年同期（16%）と比較して割合は低下していますが、ランサムウェアに関する相談件数自体は減少していません。当該期間では、サーバ不正侵入を中心に相談件数が増加したため、相談全体に占めるランサムウェアの割合が相対的に低下したものです。ランサムウェアによる被害は、当該期間においてもマルウェア関連被害の中で最も高い割合を占めています。

サーバ不正侵入の被害では、Webアプリケーションの脆弱性に起因する被害が全体の16%を占め、前四半期（8%）および前年同期（6%）と比較して増加しています。特に、WordPressの脆弱性を悪用した侵害に関する相談が複数寄せられました。脆弱性に関する注意喚起が公表された後も、自組織への影響や侵害の有無が確認されないまま、侵害を受けてから発見までに期間を要した事例も確認されています。製品やソフトウェアの脆弱性情報が公開された際には、影響を受ける製品の有無やバージョンを確認し、修正版を適用するだけでなく、既に侵害されていないかを確認することが重要です。

また、ID不正利用による被害は全体の19%を占め、前四半期（17%）から増加した一方、前年同期（24%）からは減少しています。ID不正利用とWebアプリケーションの脆弱性悪用を合わせると全体の35%となり、サーバ不正侵入による被害の約7割を占めています。脆弱性への対応に加えて、共用アカウントや外部組織に提供しているアカウント、利用終了後も有効なまま残されているアカウントなど、正規アカウントの管理状況を見直すことも重要です。

当該期間では、サポート詐欺による被害の相談が全体の10%を占めています。前四半期（23%）から減少した一方、前年同期（6%）を上回っています。また、内部犯行による被害の相談は8%となり、前四半期（11%）および前年同期（10%）から減少しています。

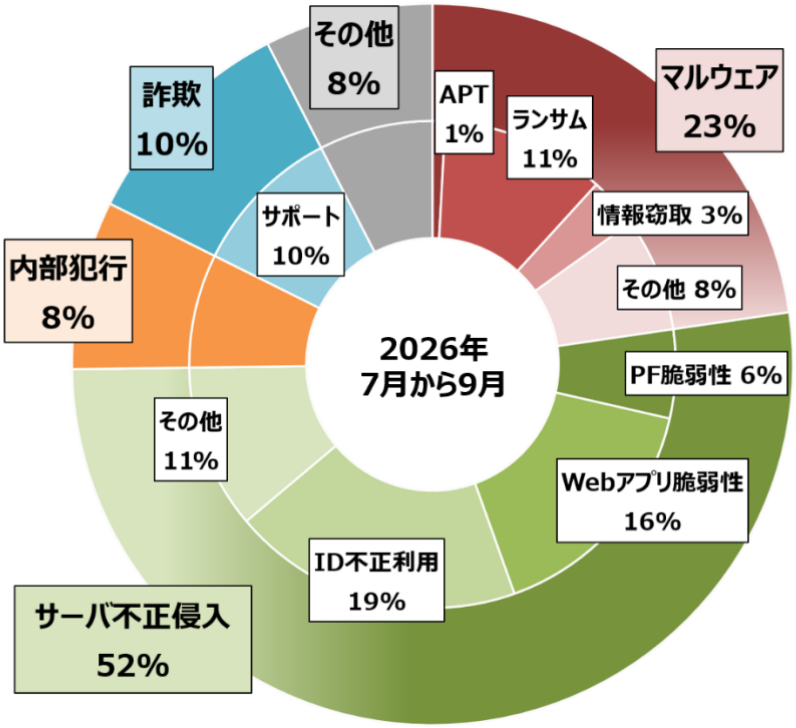


図 1 2026 年 7 月から 9 月の出動インシデントの内訳

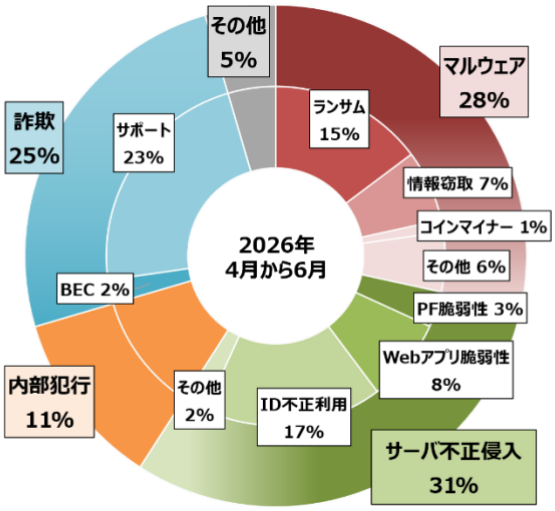


図 2 前四半期（2026 年 4 月から 6 月）

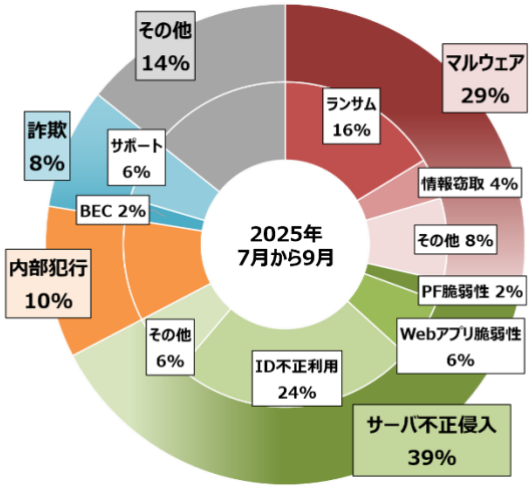


図 3 前年同期（2025 年 7 月から 9 月）

下表は、当該期間（2026 年 7 月～9 月）、前四半期（2026 年 4 月～6 月）および前年同期（2025 年 7 月～9 月）の各期間における相談件数の割合を業種別に集計し、上位 5 業種の推移を示したものです。

情報通信業は当該期間において 33%となり、前四半期（33%）および前年同期（33%）と同じ割合であり、引き続き最も高い割合を占めています。

卸売業，小売業は 11%となり、前四半期（7%）および前年同期（8%）と比較して増加しています。卸売業，小売業の増加には、一般利用者向けの Web サイトや Web サービスを運営する組織からの相談が寄せられたことが影響しています。組織の規模や業種にかかわらず、インターネットに公開されているサービスは攻撃対象になり得るため、継続的な脆弱性管理等の対応が必要です。

順位	当該期間（2026 年 7 月から 9 月）		前四半期（2026 年 4 月から 6 月）		前年同期（2025 年 7 月から 9 月）	
1	情報通信業	33%	情報通信業	33%	情報通信業	33%
2	卸売業，小売業	11%	製造業	21%	製造業	15%
3	製造業	9%	卸売業，小売業	7%	学術研究，専門・技術サービス業	13%
4	サービス業（他に分類されないもの）	7%	サービス業（他に分類されないもの）	7%	金融業，保険業	12%
5	学術研究，専門・技術サービス業	7%	学術研究，専門・技術サービス業	7%	卸売業，小売業	8%

表 1 上位 5 業種の相談件数割合

Web サイトへの侵害事例

2026 年 7 月から 9 月にかけて、Web アプリケーションの脆弱性を悪用した侵害に関する割合が急増しました。特に多く寄せられたのが、7 月に公表された WordPress の二つの脆弱性、CVE-2026-60137 および CVE-2026-63030 を組み合わせた攻撃手法「wp2shell」に関する相談です。

wp2shell は、WordPress の二つの脆弱性を組み合わせることで、管理者権限などを必要とせずに、遠隔から任意のコードを実行する攻撃手法です。観測された攻撃の技術的な詳細は本誌の特集記事で紹介しています。

wp2shell については、2026 年 7 月 22 日に IPA から注意喚起が公表され、影響を受ける WordPress の速やかな更新が呼びかけられていました。一方で、7 月下旬に侵害を受けたものの、その事実に 9 月まで気付かなかった事例が複数確認されています。侵害の発見や対策が遅れた場合、その間も攻撃者による不正な活動が継続し、被害や影響が拡大するおそれがあります。注意喚起が公表された際には、対象となる WordPress の有無やバージョンを速やかに確認し、修正版を適用することが重要です。また、脆弱性が悪用されていた可能性も考慮し、既に侵害を受けていないかについても併せて点検する必要があります。

インターネットに公開された Web サイトは、組織の規模や業種にかかわらず攻撃対象となる可能性があります。そのため、脆弱性に関する注意喚起が公表された際には、自組織への影響の有無を速やかに確認し、必要な対応につなげることが重要です。日頃から自組織で利用しているソフトウェアやそのバージョンを把握するとともに、関連する脆弱性情報を継続的に収集し、影響有無を判断できる体制を整備しておくことが望まれます。また、影響を受けるバージョンを使用していた場合は、修正版を適用するとともに、既に侵害されている可能性も考慮し、不正アカウント、不審なプラグインやファイルの有無、アクセスログ上の不審な記録などを点検することが重要です。

また、レンタルサーバやホスティングサービスを利用している場合は、サービスや契約プランによって、取得できるログやバックアップ、サービス事業者から提供を受けられる情報が異なります。平時から、利用者とサービス事業者の責任分界を確認し、利用者側で確認・保全できる情報の範囲、ログの保存期間と取得方法、インシデント発生時にサービス事業者へ依頼できる対応を整理しておくことも重要です。

管理が不十分な正規アカウントの不正利用

サーバやクラウドサービスへの不正侵入では、脆弱性の悪用だけでなく、正規の認証情報を使用した不正アクセスも引き続き確認されています。正規アカウントによるログインは、システム上では通常の認証成功として記録されます。そのため、アカウントの利用者や利用状況が適切に管理されていなければ、不正利用を通常の業務上のアクセスと区別しにくくなり、発見が遅れる可能性があります。

特に注意が必要なのが、共用アカウント、外部組織に提供しているアカウント、本来は利用を終了しているにもかかわらず有効なまま残されているアカウントです。

共用アカウントや外部組織に提供しているアカウントには、複数人で使用する共用アカウントや、業務委託先・運用保守業者に発行したアカウントなどが該当します。これらのアカウントは、実際の利用者や利用状況を自組織で把握しにくく、担当者の変更後も以前の利用者が認証情報を保持し続けるなど、意図しない範囲に認証情報が残存し、漏えい・不正利用のリスクが高まります。

また、本来は利用を終了しているにもかかわらず有効なまま残されているアカウントには、構築や検証のために作成したテスト用アカウント、異動により不要となったアカウント、退職者のアカウント、契約終了後も残存している委託先のアカウントなどが該当します。このようなアカウントは、管理や監視の対象から外れやすく、脆弱なパスワードや必要以上の権限が残ったままになることがあります。その結果、攻撃者に侵入や被害拡大の足掛かりとして悪用される可能性があります。

対策として、まず、現在有効になっているアカウントを棚卸しし、利用者、管理責任者、利用目的、付与されている権限、有効期間および最終利用日時を確認することが重要です。利用者や利用目的を確認できないアカウント、業務や契約が終了したアカウント、長期間利用されていないアカウントについては、必要性を確認した上で無効化または削除してください。

共用アカウントや外部組織に提供しているアカウントについては、管理責任者、利用者、利用目的を明確にし、必要な範囲に権限を制限してください。また、利用者や管理責任者の変更や異動・退職、委託契約・保守作業の終了などを契機として、認証情報の更新、権限の見直し、アカウントの無効化または削除を行う管理ルールを定めることが重要です。利用期間があらかじめ決まっているアカウントには有効期限を設定するなど、アカウントの発行から利用終了時の失効までを一連の管理として整備してください。

JSOC で観測したサイバー攻撃傾向

重要インシデントのトピックス

2026 年 7 月から 9 月に発生した重要インシデント（検知件数の多寡を問わず攻撃の成功を確認もしくは被害が発生している可能性が高いと判断されるセキュリティインシデント）の合計件数は 178 件でした。内訳はインターネットからの攻撃によるインシデントが 22 件（12.4%）、ネットワーク内部からの通信によるインシデントが 156 件（87.6%）であり、インターネットからの攻撃によるインシデントは前四半期と比較して増加しました。

1）インターネットからの攻撃により発生した重要インシデント

WordPress Core に存在する未認証の任意コード実行につながる脆弱性チェーン（CVE-2026-63030 および CVE-2026-60137）を狙った攻撃によるインシデントが発生しました。そのほかにはファイルアップロードを悪用した攻撃によるインシデントが発生しました。これらのインシデントの多くは、WordPress や Joomla!などの CMS のプラグインに存在する脆弱性を狙ったものでした。図 4 に 2026 年 7 月から 9 月の重要インシデントの内訳を示します。

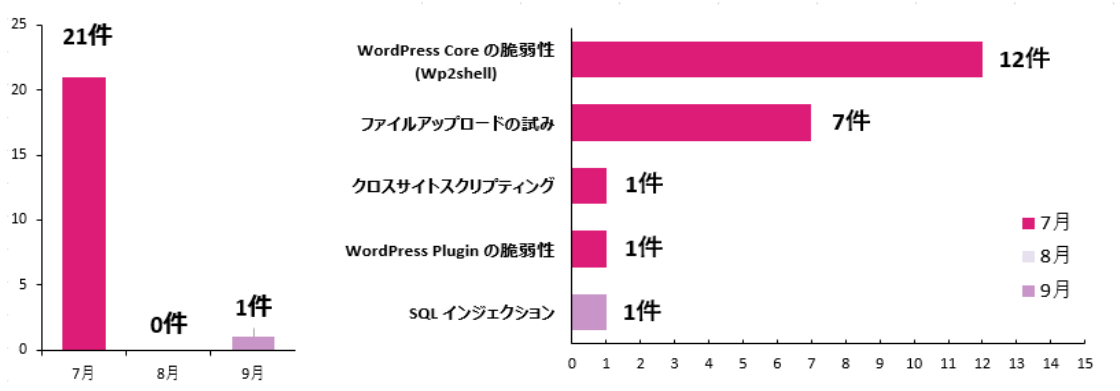


図 4 [外部から] 2026 年 7 月から 9 月の重要インシデントの内訳（月別・種類別）

2) ネットワーク内部から発生した重要インシデント

マルウェア感染に起因する重要インシデントが多数発生しました。これらのインシデントでは、前四半期に引き続き、macOS を標的とする情報窃取マルウェアの一種である AMOS Stealer、ブラウザに保存された機微情報の窃取を行う Arechclient2 に感染したことに起因する通信を検知しました。加えて、Clickfix の手口により悪性スクリプトを取得する通信や、ユーザの端末資源を無断で使用し、暗号資産を採掘するマイニングマルウェアに感染したことに起因する通信を検知しました。マルウェア以外に分類している重要インシデントについては、監視対象ホストから外部に対する不審な通信や不審なドメイン名の名前解決の通信を検知したことによるインシデントが発生しました。図 5 に 2026 年 7 月から 9 月の重要インシデントの内訳を示します。

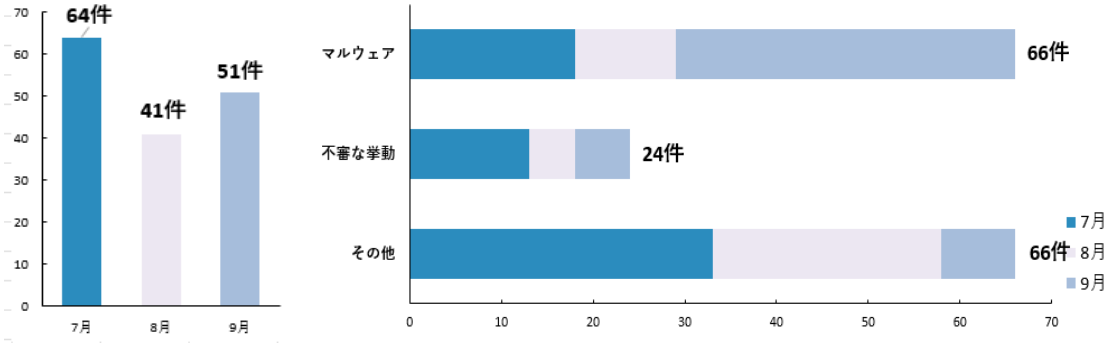


図 5 [内部から] 2026 年 7 月から 9 月の重要インシデントの内訳（月別･種類別）

EDR 製品の検知による重要インシデントは 29 件発生しました。マルウェア感染につながる挙動を検知したことによるインシデントが 5 件、攻撃者によって行われた可能性のある不審な挙動を検知したことによるインシデントが 24 件でした。前四半期に引き続き、USB メモリを介したマルウェア感染の通信を検知したことによるインシデントが発生しました。そのほかにも、インストーラーに偽装した不審なファイルの実行や、不審なソフトウェアによる認証情報の窃取等のインシデントも発生しました。図 6 に NW 監視（IPS/IDS 他）、端末監視それぞれで検知したインシデント種別の内訳を示します。

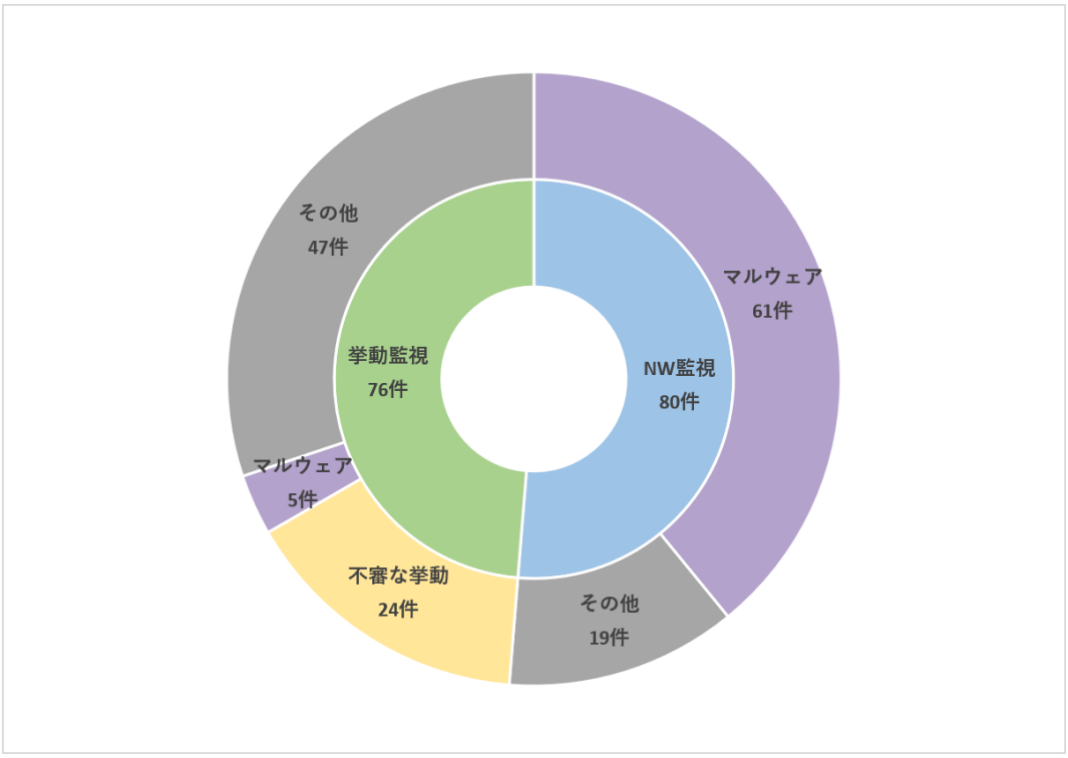


図 6 [内部から] 監視形態ごとのインシデント種類別内訳

注意が必要な通信

注意が必要な通信や、大きな被害には発展していないものの検知件数が多い攻撃通信を、下表で紹介します。

表 2 注意が必要な通信について

概要	JSOC の検知内容	検知時期
Ivanti Sentry の脆弱性（CVE-2026-10520）を狙った攻撃	脆弱性を悪用し、コード実行を試みる通信を多数検知しました。	6 月 29 日～
FortiAuthenticator の脆弱性（CVE-2026-44277）を狙った攻撃	脆弱性を悪用し、管理インタフェースへのアクセスを試みる通信を多数検知しました。	7 月 3 日～
82.39.115.22（英国）からの攻撃通信	Apache や WordPress Core および各種プラグインの脆弱性を狙った攻撃を多数検知しました。	6 月 21 日～
Citrix NetScaler ADC および NetScaler Gateway の脆弱性（CVE-2026-88771）を狙った攻撃通信	脆弱性を悪用し、コード実行を試みる通信を検知しました。	9 月 29 日～

特集：wp2shell 攻撃の実態

サイバー119 では、日々、サイバー攻撃の被害に遭われた方々からの相談や、端末の調査依頼を受け付けています。その中で、WordPress を狙う「wp2shell」と呼ばれる攻撃手法による侵害事例が継続的に観測されています。wp2shell による侵害は、単なるコンテンツの改ざんにとどまらず、サーバ侵害の起点となり得るなど、重大な影響を及ぼす可能性があります。

本特集では、サイバー119 で実際に観測した wp2shell の攻撃手法と、それによって生じた影響について、検知傾向とあわせて紹介します。

「wp2shell」の攻撃手法について

wp2shell は、WordPress 本体に存在する二つの脆弱性「CVE-2026-63030」および「CVE-2026-60137」を悪用する攻撃手法の通称です。wp2shell は、特定の脆弱なプラグインやテーマを必要とせず、影響を受けるバージョン（6.9.0～6.9.4、7.0.0～7.0.1）の標準的な WordPress 環境でも成立する可能性があります。また、WordPress は企業の Web サイトで広く利用されていることから、サイバー119 にも本攻撃に関する相談が多く寄せられています。

CVE-2026-63030 は REST API のバッチ処理に関する脆弱性で、CVE-2026-60137 は WordPress 6.8 系から存在していた SQL インジェクションの脆弱性です。標準的な WordPress 構成では、CVE-2026-60137 単体での悪用は不可能と考えられていました。wp2shell では CVE-2026-63030 と組み合わせることで、CVE-2026-60137 による SQL インジェクションが可能となり、認証を必要とせず任意のコード実行に至る可能性があります。

サイバー119 で実施したフォレンジック調査では、wp2shell の被害に遭ったサーバのアクセスログから、図 7 および図 8（それぞれ異なる環境）に示す、REST API のバッチエンドポイントに対する POST リクエストを 2 パターン確認しました。POST リクエストの通信内容はアクセスログに記録されないため、このログだけで攻撃かどうかを判定することは困難です。しかし、直後にサーバ上に残された侵害痕跡などから、図 7 および図 8 の POST リクエストでは、CVE-2026-60137 のペイロードを含む不正な JSON データが送信されたものと判断しています。

```
***.***.***[.]***[1] - - [19/Jul/2026:15:03:56 +0900] "POST /wp-json/batch/v1 HTTP/1.1" 207 8717 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1 31.0.0.0 Safari/537.36"
```

図 7 REST API エンドポイントへの不審な POST リクエスト（パターン 1）

```
***.***.***[.]***[1] - - [19/Jul/2026:16:07:50 +0900] "POST /?rest_route=/batch/v1 HTTP/1.1" 207 10 29 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36"
```

図 8 REST API エンドポイントへの不審な POST リクエスト（パターン 2）

wp2shell の攻撃傾向

wp2shell が成功した場合、攻撃者は被害サーバ上で任意のコードを実行する可能性があります。サイバー119 が実施したフォレンジック調査では、wp2shell の悪用後に WordPress 上で不正なユーザが作成され、そのアカウントを足掛かりとして、不正なプラグインや WebShell が設置された事例を確認しています。さらに、不正ユーザによって設置された WebShell（任意のコード実行など遠隔操作機能を持つマルウェア）を起点として第二、第三の攻撃へ発展する可能性があるため、wp2shell の侵害を契機に、多様な攻撃手法が実行されるおそれがあります。

同じ調査では、被害サーバに残された不審ファイル、ファイルの操作痕跡、アクセスログなどから、以下の攻撃手法が併用されていたことを確認しました。

（1） WordPress 管理機能への不正アクセス

WordPress 管理機能に対する、以下の不正アクセス手法を確認しました。

- wp2shell による認証回避
- wp2shell によって作成されたマルウェアによる認証回避
- wp2shell によって作成された不正ユーザによるログイン

攻撃者は、継続的な不正アクセスを可能にするため、これらの手法を併用することがあります。例えば、wp2shell による認証回避は、WordPress がアップデートされると再侵入できなくなる可能性がありますが、マルウェアによる認証回避であれば、アップデート後もアクセスを継続できる場

[1] IP アドレスはマスクしています。

合があります。同様に、WAF の導入などによってマルウェアを利用した認証回避が困難になった場合でも、不正ユーザでのログインが引き続き可能な場合があります。

（2） 不正な WordPress ユーザの作成・削除

攻撃者によって作成された不正ユーザは、主に WordPress 管理機能への不正アクセスに用いられます。調査において観測した、攻撃者が作成したとみられる不審 WordPress ユーザの例を、表 3 に示します。

表 3 攻撃者によって作成されたとみられる不審 WordPress ユーザの例

display_name	user_email
attacker	attacker[@]wp2shell[.]invalid
wordpress	info[@]wordpress[.]com
wp2_60ede8f72abf	wp2_60ede8f72abf[@]wp2shell[.]invalid
Nx_748e6543f7ed	Nx_748e6543f7ed[@]nx[.]invalid
wordpress_ae99c2edd0c9	wordpress_ae99c2edd0c9[@]wordpress [.]com

不審 WordPress ユーザには、以下の特徴を確認しました。

- display_name がランダムな文字列を含んでいる
- display_name に「wordpress」などのアプリケーション名が使用されている
- user_email が実在しないとみられるメールアドレスで登録されている

（3） 不審ファイルの作成

wp2shell のように、外部公開された Web サイトを介して行われる攻撃では、攻撃者が最初に掌握するのは、apache ユーザなどのサービスアカウントの権限である傾向があります。そのため、侵害直後に作成される不審ファイルは、Web ルート配下に作成される傾向があります。

wp2shell が侵害のきっかけとなったサーバの調査において確認された不審ファイルについて、一部の例を表 4 に示します。

表 4 攻撃者によって作成されたとみられる不審ファイルの例

ファイルパス	不審ファイルの種別
/var/www/html/wp-content/plugins/wpcontent-optimizer_96e754/wp-contentoptimizer_96e754.php	WebShell
/var/www/html/wp-content/plugins/wp2shell_b03f9ca1/wp2shell_b03f9ca1.php	WordPress の認証回避を行う不正プラグイン
/var/www/html/wp-content/mu-plugins/galex_patch.php	wp2shell の使用を制限する不審ファイル
（復元したファイルのため正確なファイルパス不明）/plugins/wp-crontrol/.pkexec/gconv-modules	CVE-2021-4034[2]を悪用して権限昇格を行うマルウェア

「/var/www/html/wp-content/mu-plugins/galex_patch.php」について補足します。このファイルは、特定の TOKEN を含む Web アクセスの場合に限って wp2shell を悪用できるよう制御する（TOKEN が設定されていない場合は 403 を返す）PHP ファイルです。攻撃者がこの PHP ファイルを作成した目的は不明ですが、wp2shell を使用した侵害経路を独占しようとしたものと推測しています。作成後の期間には、wp2shellを試行したとみられる通信に対して403を返した痕跡を確認しました。

```
***.***.***[.]***[1] - - [21/Jul/2026:02:55:55 +0900] "GET /?rest_route=/batch/v1 HTTP/1.1" 403 74 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

図 9 galex_patch.php の制御により、wp2shell を試行した通信に 403 が返された痕跡

[2] TRENDMICRO,「メモリ破損の脆弱性「PwnKit」（CVE-2021-4034）をトレンドマイクロの技術で検出する方法」
https://www.trendmicro.com/ja_jp/research/22/c/how-to-detect-PwnKit.html

攻撃者は何を狙うのか

攻撃者は、wp2shell による侵害を足掛かりとして、Web サーバ上に存在するさまざまな資産の窃取を試みます。wp2shell の被害に遭ったサーバのフォレンジック調査では、以下の攻撃活動やその影響を確認しました。

（1） 環境情報の外部送信

wp2shell によって作成された不審ファイルが実行され、以下に示す Web サーバの環境情報が外部へ送信された痕跡を確認しました。

- OS 情報
- ドキュメントルート
- サイト URL
- メモリ容量
- プロセッサ数
- ソフトウェアのバージョン
- ディスク容量

攻撃者は、サーバへの攻撃に先立ち、対象サーバの環境情報を収集する傾向があります。例えば、脆弱性が残るソフトウェアがサーバにインストールされていることが判明した場合、権限昇格などの攻撃に悪用される危険性があります。

（2） メール送信環境の調査

wp2shell によって作成された WebShell によって、以下に示すメール送信環境情報の調査を行うコマンドが実行されていた痕跡を確認しました。

- sendmail コマンドの有無
- PHP の mail()関数、proc_open()関数の実行可否
- PHP でサーバを操作可能な関数が無効化されていないか
- サーバの 25 番ポートの応答状態
- 名前解決の可否

侵害されたサーバが悪用されて外部へ不審メールを送信されることで、侵害されたサーバが攻撃の起点となるといった二次的な被害が発生する危険性があります。

（3） 機微情報の窃取

攻撃者は、wp2shell によって作成した WebShell などのマルウェアを通じて、Web サーバ上の機微情報を探索し、窃取を試みます。調査では、Web サーバの設定ファイルや、WordPress で使用されるデータベースの漏えいを確認しました。

（4） 痕跡の消去

攻撃者は、攻撃対象のサーバ上で自身の活動痕跡を削除し、検知の回避や事後調査の妨害を図ることがあります。調査では、攻撃者の活動によって生成されたとみられるログファイルが削除されていたことを確認しました。

さいごに

wp2shell は、認証を回避して任意のコードを実行できるため、深刻な影響をもたらす可能性があります。

未侵害の環境では、wp2shell の脆弱性を修正したバージョンに WordPress を更新することが、基本的な対策となります。一方、更新前に侵害を受けていた場合、不正ユーザや WebShell などが残存している可能性があるため、更新だけでなく、侵害痕跡の確認と除去も必要です。なお、現在も JSOC の監視では、wp2shell を狙った攻撃が継続して観測されています（図 10）。また、今後、流通している脆弱性スキャナに攻撃用ペイロードが組み込まれる可能性もあるため、検知件数のピークを過ぎた後も予断を許さない状況です。

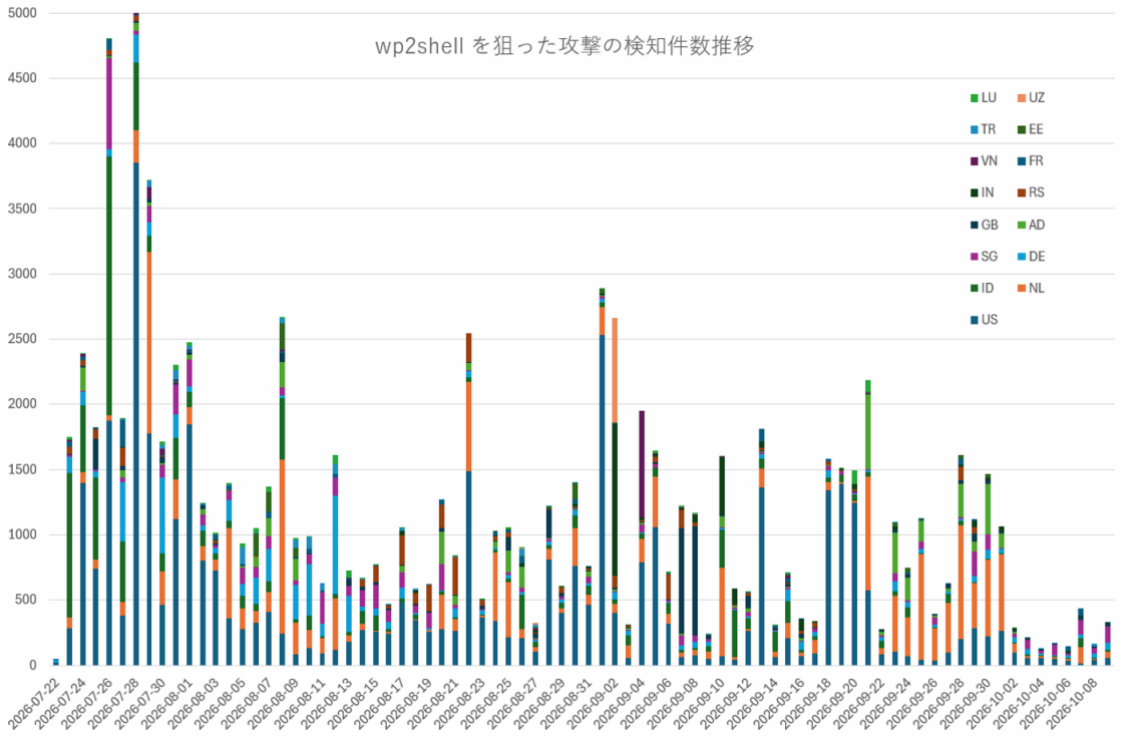


図 10 JSOC における wp2shell を狙った攻撃の検知件数推移

WordPress を使用した Web サーバを運用している場合は、特に以下の対策に取り組むことを推奨します。

対策	対策する理由
継続的な WordPress のバージョンアップ	wp2shell に限らず、脆弱性が発見された場合は、修正版へ更新することで対策できます。
WordPress 管理機能へのアクセス制御	WordPress の管理画面や API へのアクセスを必要最小限に制限することで、攻撃の対象範囲を限定し、脆弱性を悪用した攻撃がもたらすリスクを低減できます。

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/5TVC3RG

【memo】

【memo】

株式会社ラック
〒102-0093
東京都千代田区平河町 2-16-1
平河町森タワー
https://www.lac.co.jp/

