2026.07.06 | 17:05 重要 その他

+4

【重要】開発環境への不正アクセスによるセキュリティインシデントに関するご報告とお詫び

2026年7月23日（木）11:20更新

平素は格別のご高配を賜り、厚く御礼申し上げます。

この度、弊社の開発環境端末におきまして、外部からの不正アクセスによるセキュリティインシデ

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

が発生いたしました。お客様には多大なるご心配とご迷惑をおかけしておりますこと、深くお詫び申し上げます。

なお、詳細な調査の結果、実在するお客様の個人情報および機密情報の漏えいは一切ないことが確認されております。

なお、本件に関する最新の状況、および今後の各モール再認証スケジュール等につきましては、新たな進捗があり次第、本ページを随時更新してご報告申し上げてまいります。
上の「最終更新日時」をご確認のうえ、最新の情報をご参照いただけますようお願い申し上げます。

本件に関する経緯、原因、影響範囲、および今後の再発防止策につきまして、下記の通りご報告申し上げます。

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

インシデントの概要

2026年7月4日（土）、弊社の開発環境端末上のデータベース（MySQL）およびキャッシュサーバ（Redis）に対して外部からの不正アクセスが発生いたしました。

データベース内の情報が外部へ送信され、その後データが削除される被害を確認しております。

影響範囲と被害状況について

① お客様の個人情報・機密情報について

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

ーデータ）であり、**実在するお客様の個人情報は一切含まれておりません。**

② 窃取された情報について

一部のAPIキー、アプリケーションID、テストデータ、および「ワサビ管理者アカウント」の情報が窃取されました。

管理者アカウントのパスワードは強固な暗号化（ソルト付きSHA-256でハッシュ化）が施されており、平文ではございませんが、二次被害防止のため、速やかに全てのアカウントを停止し、パスワードの変更を実施いたしました。

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

③本番環境への影響について

窃取された情報の中に、一部本番環境でも使用されているAPIキーとアプリケーションIDが含まれておりました。

APIキー： 速やかに再発行および旧キーの無効化を完了しており、不正利用は確認されておりません。

アプリケーションID： OAuth認証が必要な仕様のため、機密情報が直接漏えいすることはございませんが、念のため現在再発行の手続きを進めております。

- 対象となるAPI：**Luxclusif、ヤフーショッピング、併売ヤフオク、競りナビ、UPS、Shopify、Walmart**
- 不明なサイト等で上記のOAuth認証（連携許可）を行わない限り、これによって注文情報や

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

2026年7月23日（木）11:20　追記

【Luxclusifの対応について】

本件につきましては弊社にて対応を完了しております。店舗様での作業やご対応は一切不要でございますので、ご安心ください。

④ キャッシュサーバ（Redis）について

暗号資産マイニングを目的とした不正な設定の書き込みを確認しましたが、コンテナ内に隔離された環境であり、実行プログラムが存在しなかったため、システムへの被害は発生しておりません。

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

前述の通り、現在アプリケーションIDの再発行手続きを行っております。

再発行が完了した折には、誠にお手数ではございますが、**各モールの設定画面にて再認証を行っていただく必要がございます。**

具体的な手順や実施時期につきましては、確定次第、改めてご案内申し上げます。

発生原因

以下の要因が重なり、開発用データベースがインターネットから直接接続可能な状態になっていたことが原因です。

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

部からも接続可能（0.0.0.0）な設定になっていたこと。

2. 当該端末を接続していた自宅ルーターの設定およびファームウェアの不具合により、該当ポートが外部へ転送（パブリックに公開）される状態になっていたこと。

これにより、探索ボットが公開ポートを発見し、侵入に至りました。

発生から対応までの経緯

2026年7月4日（土）

- **08:56**：開発環境端末へ不正アクセスが発生

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

- **11:52**：攻撃元の特定、被害状況の確認を開始。
- **14:52**：二次被害防止のため、全WASABISWITCHのワサビ管理者アカウントを全停止し、セッションを強制削除。
- **17:13**：根本原因を確定。
- **18:28**：該当社員から社内へインシデント発生を報告。
- **19:47**：情報の流出状況を改めて詳細に確認。
- **20:35**：緊急性の高いクレデンシャル情報（APIキー等）を再発行し、全WASABI SWITCHへ反映の上、流出した情報を無効化。
- **22:42**：恒久対策としてソースコードを修正

2026年7月5日（日）

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

- 10:00：クレデンシャル情報（アプリケーションID）の再発行手続きを開始。

2026年7月6日（月）

- **11:00**：全WASABISWITCHのワサビ管理者アカウントのパスワードを変更した上で、アカウントの稼働を再開。

再発防止策

弊社では本事態を重く受け止め、以下の対策を講じ、セキュリティ体制の強化を徹底いたします。

1. **アクセス制御の徹底：** Dockerの公開ポートを「127.0.0.1（ローカル）」に限定し、外部からの直接接続を遮断（MySQL・Redis等すべての公開ポートに適用）。

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

2. **認証情報の強化：** MySQL、Redis等すべてのシステムにおけるパスワードおよび認証情報の定期的なローテーション（変更）を実施。
3. **開発データの無害化（サニタイズ）：** 開発環境で使用するデータに含まれるパスワードハッシュや認証情報をダミー値へ置き換え、本番データへの紐付きを完全に排除。
4. **アカウントの保護：** 影響を受けた全スタッフのパスワード再設定。
5. **ネットワーク設定の是正：** 対象ルーターのUPnP機能の無効化およびポート転送設定の削除。
6. **社内セキュリティ診断の実施：** 開発担当者全員の端末・環境に対するペネトレーションテスト（侵入テスト）を実施し、脆弱性がないことを確認。
7. **第三者機関による監査：** 外部のセキュリティ専門企業へコンサルティングを依頼し、総合的な

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

いましたら、弊社担当者またはサポート窓口までお問い合わせくださいますようお願い申し上げます。

改めまして、この度は多大なるご迷惑とご心配をおかけいたしましたこと、重ねて深くお詫び申し上げます。

2026年7月6日

株式会社ワサビ

以上



関連記事

2018.06.09 その他

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら

2024.06.14 その他

【楽天市場】あす楽廃止に伴う対応についてのお知らせ

2025.12.04 その他 メルカリShops

【メルカリ】メルカリメンテナンスについて

2026.05.13 その他 楽天市場

【楽天市場】店舗種別「楽天市場」について

2025.01.28 その他

【利益率】仕様変更のお知らせ

ライト版を使い始めた方向け
動画でサポート！
詳しくはこちら

導入ご検討企業様はメールもしく
はWEBサイトのフォームからでお
問い合わせ下さい。

info@wasabi-inc.biz

お問い合わせフォームはこちら

COPYRIGHT© WASABI INC. ALL RIGHTS RESERVED.

ライト版を
使い始めた方向け
動画でサポート！
詳しくはこちら