2025 年 6 月 26 日

「PR TIMES」ご利用ユーザー各位

株式会社 PR TIMES

PR TIMES 不正アクセス(5 月 7 日発表)の再発防止策の追加と実施予定について

平素より「PR TIMES」をご利用いただきまして、誠にありがとうございます。

当社は、2025 年 5 月 7 日発表の「PR TIMES、不正アクセスによる情報漏えいの可能性に関するお詫びとご報告」において、2025 年 4 月 24 日より第三者によるサーバー内部への不正アクセスとサイバー攻撃が行われたことを受け、個人情報と発表前プレスリリース情報を中心とする保有情報が漏えいした可能性があることを公表し、再発防止策を示しておりましたが、その後に検討を重ねて再発防止策を追加することを決定いたしましたので、お知らせいたします。

本件不正アクセスの発覚以降、今日に至るまでも、お客様情報の不正利用などの事実は確認されておりませんが、お客様にはご心配をお掛けする事態となりましたことを、改めて深くお詫び申し上げます。

当社は、より一層のセキュリティ対策と監視体制の強化を実現し、より安心してサービスをご利用いただける環境をご提供するため、追加の対策を含め、「PR TIMES」において下記の再発防止策およびセキュリティ強化策を講じてまいります。

記

1. 実施済みの措置

- 管理者画面のアクセス許可 IP アドレスを、社内からの接続と VPN(仮想の専用回線)からの接続のみに制限
- 今回バックドアファイルが配置された箇所で、不正なファイルを実行できないようにする設定の追加を完了
- 管理者画面にアクセスできる全アカウントのログインパスワードを変更
- 不要な共有アカウントの削除

2. 実施予定の措置 (5 月 7 日発表)

- 現在導入している WAF(Web Application Firewall)の設定の見直し (2025 年 10 月末の完了を予定)
- 2022 年より進めているセキュリティをより担保しやすい新管理者画面への移行 (2025 年 12 月中旬を予定)

3. 新たに決定した実施予定の措置 (新規追加)※実装予定順

- 【全ユーザー向け】ログイン二段階認証と ON/OFF 設定
  (企業ユーザー:2025 年 8 月上旬、メディアユーザー:同年 9 月上旬、個人ユーザー:同年 10 月上旬の実装予定)

  二段階認証はインターネットサービスへのログイン時に ID とパスワードによる認証に加え、「もう一つの確認要素」を必須とするセキュリティシステムです。この認証を導入した後にログインを試みるユーザーは、ID(メールアドレス)とパスワードを入力したのち、ID 宛に送られるコードを認証画面

に入力しなければ、ログインできません。仮に第三者が ID とパスワードを不正に入手した場合でも、パスワード単体ではログインが完了しないため、なりすまし対策として効果が見込めると考えております。なお、この認証はご利用アカウントごとに利用有無を設定できる仕様といたします（企業ユーザーの場合、同アカウント内すべてのユーザーに適用されるため、利用有無を設定できる権限はメインユーザーのみに付与いたします）。

・ 【企業ユーザー向け】IP アドレス制限と ON/OFF 設定
（2025 年 9 月上旬の実装予定）

IP アドレスによるアクセス制限は、特定のシステムへのアクセスを、事前に許可された特定の IP アドレスからのみに限定するセキュリティ対策です。この仕組みを、プレスリリース発表を管理する企業アカウントのログインに適用することで、許可されていない IP アドレスからの接続試行は、ログイン時点で遮断されます。たとえ第三者が ID（メールアドレス）とパスワードを不正に入手したとしても、許可されていない IP アドレスからの不正なログインを遮断することで、なりすまし配信を防止いたします。

不正ログイン対策として有効な一方、設定を誤ると正規のユーザー様ご自身がログインできなくなる可能性があります。プレスリリース配信などの重要な業務に支障をきたす事態を防ぐため、設定ミスが起こりにくい画面設計や、万が一の際すぐにご相談いただけるお問い合わせ窓口への導線の整備を含めて、実装いたします。

なお、このアクセス制限は企業アカウントごとに利用有無を設定できる仕様といたします（企業ユーザーの場合、同アカウント内すべてのユーザーに適用されるため、利用有無を設定できる権限はメインユーザーのみに付与いたします）。

・ 【全ユーザー向け】パスワードのセキュリティ向上
（企業ユーザー・メディアユーザー・個人ユーザーともに、2025 年 11 月下旬の実装予定）

文字数と入力規則、それぞれ複雑性を十分に担保できるルールへと変更し、セキュリティを強化いたします。既にご利用いただいているユーザーの皆様には事前にお伝えしたうえで、変更後のルールを満たしたパスワードを作成いただくようご案内いたします。

現在ご利用中のお客様、そして新たに登録されるお客様の双方が円滑にサービスをご利用いただける状態を両立させるとともに、ご利用中のパスワードでお客様がログインできなくなる事態を起こさないよう慎重に進めてまいります。先行して 2025 年 8 月上旬から実装を開始する「ログイン二段階認証」の開発を進める期間に、現在ご利用いただいている皆様への影響を詳細に調査し、ご不便をお掛けすることなく移行できるよう進行してまいります。

・ 【運営側】削除データの保持期間 30 日間
（2025 年 12 月中旬の実装予定）

お客様の画面上から削除されたデータ（登録情報、下書きコンテンツ、リスト情報、等）は、削除後 30 日間は運営側で復旧可能な状態で保持し、その後はデータベース上から完全に削除される仕様にいたします。不必要なデータ残存を防ぎます。

お客様からお預かりした大切なデータを、万が一のシステム欠陥や誤削除で失われることのないよう、影響範囲の詳細な調査から着手いたします。さらに、テスト工程におきましても、通常の操作確認に加え、削除されるデータの種類や保存場所など、あらゆる条件を想定した網羅的な検証を行った後に、実装いたします。

・ 【全ユーザー向け】ログイン通知及びログイン履歴の強化
（企業ユーザー・メディアユーザー・個人ユーザーともに、2026 年 3 月下旬の実装予定）

管理画面へログインされた場所（国や都道府県）やご利用のデバイスといった情報を、新たに履歴表示や通知メールに加えます。現在、企業アカウントのログイン履歴はユーザー名・IP アドレス・日付を表示しておりますが、デバイス・場所（国内であれば都道府県名、海外であれば国名）を追加で表示いたします。また、不審なログインがあった場合は強制ログアウトさせられる仕組みも導入いたします。

まずは履歴情報を安全に取得・保存する仕組みの構築から着手し、先行して 2025 年 12 月に導入する「削除データの保持期間」の仕組みとの間でデータの不整合が生じないよう、「削除データの保持期間」の開発後に本機能の開発に着手し、データの取得から画面（UI）の開発までを慎重に進めてまいります。

以上の措置を講じて、発表前の重要情報をお預かりするプラットフォーム運営企業として、より一層のセキュリティ対策と監視体制の強化を実現し、信用回復に努めてまいります。

なお、上記機能の実装にあたりましては、システムの停止が必要なメンテナンスは予定しておらず、出来る限りサービスを継続的にご利用いただける環境を維持しながら、機能強化を実現してまいります。
（2026 年 3 月下旬実装予定の「ログイン通知及びログイン履歴の強化」のみ、実装後に再度ログインし直していただく必要が想定されておりますが、その際は改めて事前にご案内いたします。）

【お問い合わせ窓口】
本件不正アクセスに関するお問い合わせは、こちらの窓口で引き続き受け付けております。
お電話：03-6625-4684（平日 9:00～19:00、土日祝 10:00～17:00）、03-6625-4876
フォーム：https://tayori.com/f/prtimes-unauthorized-access/

なお、当社から個人情報保護委員会への確報を提出完了しており、必要な場合には連携させていただきますので、ご入用の際はお申し付けください。

皆様には、多大なるご心配をお掛けしておりますことを、改めてお詫び申し上げます。
今後とも「PR TIMES」をご愛顧いただきますよう、何卒宜しくお願い申し上げます。

PR TIMES：https://prtimes.jp/

以上