（別表）NewsPicks サービス本体のセキュリティ対策（2026年10月20日時点）

| 分類 | 対策内容 |
|---|---|
| **第三者認証** | ISO/IEC 27001（ISMS）認証を取得しております。 |
| **組織体制** | 最高情報セキュリティ責任者（CISO）を置き、全社横断の情報セキュリティ専任チームと、インシデント対応組織（CSIRT）を設置しております。内部監査部門による監査を年1回実施しております。 |
| **脆弱性診断** | 外部の専門機関による脆弱性診断を年1回実施しております。<br>（Webアプリケーション、スマートフォンアプリケーション、AWS基盤） |
| **不正アクセス・DDoS対策** | AWS WAF で不正な通信を遮断しております。シグネチャは自動で更新しております。DDoS 攻撃には AWS Shield と AWS WAF のレート制御で対処しております。 |
| **侵入検知** | Amazon GuardDuty（侵入検知システム〈IDS〉に相当するサービス）で、不正な通信や悪意ある操作を継続的に監視しております。 |
| **監視体制** | AWS CloudWatch と New Relic でシステムの稼働・性能・障害を監視しております。セキュリティログは AWS CloudTrail に集約し、常時監視しております。 |
| **ネットワーク構成** | ロードバランサー等を除き、インターネットから直接アクセスできるサーバー・データベースは設けておりません。通信は AWS のセキュリティグループで、必要最小限のポート・プロトコルに限って許可しております。 |
| **通信の暗号化** | 全てのサービスを HTTPS（TLS 1.2 以上）で提供しております。HTTP でアクセスされた場合も HTTPS へ転送します。TLS 1.1 以下は無効にしております。 |
| **保存データの暗号化** | データベース（Amazon Aurora）、ファイルストレージ（Amazon S3）、バックアップは、いずれも AES-256 で暗号化して保存しております。暗号鍵は AWS KMS で管理しております。 |
| **パスワードの保護** | お客様のパスワードは bcrypt でハッシュ化して保存しており、平文では保存しておりません。パスワードは12文字以上かつ英数字混在を必須としております。6回続けてログインに失敗するとアカウントを30分間ロックします。 |
| **社内からのアクセス管理** | 本番環境には、シングルサインオンと多要素認証を経由し、AWS IAM で必要最小限の権限を与えて接続しております。アカウントは四半期ごとに棚卸しし、退職者のアカウントは最終稼働日に削除しております。 |
| **AWS環境の操作ログ** | AWS CloudTrail で操作の記録を残し、1年以上保管しております。ログファイルの検証機能を有効にし、改ざんを検知できるようにしております。 |
| **利用ライブラリの脆弱性管理** | 利用しているライブラリは、ツールで継続的に自動スキャンしております。深刻度の高い脆弱性から優先して対応しております。基盤のセキュリティパッチは影響を分析したうえで、緊急性の高いものからすぐに適用しております。 |
| **不正プログラム対策** | サーバーは読み取り専用のコンテナで動かしており、不正なプログラムを置けない構成にしております。 |

株式会社ユーザベース