

# スクリレの安全性について

## 個人情報を持たない「端末認証」だから、漏洩リスクがありません

### 🔒 漏洩リスクなし

氏名・メールアドレス・電話番号をサーバーに保存しないため、漏洩するデータ自体が存在しません。

### 🛡️ 変更等の対処不要

保護者側でID・パスワードを使っていないため、変更や再設定の手間は一切発生しません。

### 🏢 強固なインフラ保護

基盤はMicrosoft Azure国内データセンター。特定IP制限とWAF監視で不正侵入を厳格に防御しています。

## 従来の連絡システムと「スクリレ」の根本的な違い

| 比較項目   | 一般的なシステム（個人情報を蓄積）           | スクリレ（個人情報ゼロ設計）                          |
|--------|-----------------------------|-----------------------------------------|
| 保持する情報 | 氏名・メールアドレス・電話番号・パスワード等      | <b>個人情報は非保持</b><br>（クラス共通QRコードと出席番号で接続） |
| 攻撃リスク  | 不正アクセス時に大量の連絡先や個人情報が流出する恐れ  | <b>重要個人情報を持たないため、抜き取られる心配が皆無</b>        |
| ユーザー負担 | パスワード管理の手間や、漏洩時の変更・再設定対応が必須 | <b>ID/PW記憶不要。毎朝アプリを開くだけで安心・安全に利用可能</b>  |

## スクリレ独自の「端末認証」の仕組み

### 1 案内書QRコード読取

学校から配布された登録案内書のQRコードをアプリで読み取ります。



### 2 端末固有IDで紐づけ

出席番号とスマートフォン現物の識別子のみでセキュアに接続します。



### 3 不正アクセス遮断

スマホ現物がないと操作不能。遠隔からの不正侵入を物理的に排除します。



### スマホ現物認証による「なりすまし・乗っ取り」の排除

お使いのスマートフォン端末そのものを認証キーとして使用するため、確実に「保護者様ご本人のスマートフォン」からの操作に限定されます。スマホ現物が手元にない限り第三者がアクセスすることは不可能なため、遠隔からの乗っ取りや不正ログインを遮断します。

## クラウド基盤とコンプライアンス（Microsoft Azureの厳格な防御）

### ✓ 国内データセンター限定

ISMAP準拠の国内Azure（東日本/西日本）を採用。データは日本国内法のもとで安全に管理。

### ✓ アクセス制限&IP遮断

サーバー管理は特定IP端末に限定。開発部門も直接アクセスできない権限分離を実施。

### ✓ 通信&データの完全暗号化

通信はTLS2.0（HTTPS）、DB保存データは透過的データ暗号化（TDE）により強固に保護。

### ✓ 第三者認証・24時間365日監視

ISO 27001（ISMS）・Pマーク取得済み。24時間WAF監視と年1回の外部脆弱性診断を実施。