🔒 セキュリティポリシー

VRCSでは、お客様の重要なデータとプライバシーを保護するため、最新のセキュリティ技術とベストプラクティスを採用し、継続的なセキュリティ強化を行っております。

🛡️ セキュリティ対策

1. CSRF(クロスサイトリクエストフォージェリ)対策
   対策内容： すべての重要な操作にCSRFトークンによる検証機能を実装
   保護対象： ログイン、データ送信、設定変更、ファイルダウンロード、全APIエンドポイント
   お客様への効果： 悪意のある不正な操作を自動的にブロックし、アカウントの安全性を向上

2. 認証・セッション管理の強化
   対策内容： パスワードは暗号化して保存(管理者による復号は不可)
   セッション情報の暗号化 ／不正アクセスの自動検出
   セッションタイムアウトの最適化 ／未認証ユーザーの適切なリダイレクト
   お客様への効果： アカウントの不正使用を防止し、安全なログイン環境を提供

3. アクセス制御の実装
   対策内容： ページと機能に応じた適切なアクセス制御
   制御対象： ログイン必須ページ:ジョブ管理、ダウンロード機能
   公開ページ:ロボットライブラリ閲覧、利用規約、プライバシーポリシー
   管理者専用機能:ユーザー管理、システム設定
   お客様への効果： 権限に応じた適切なアクセス制御により、データの機密性を保護

4. データ保護の強化
   保存データの暗号化
   Microsoft Azure標準機能によるAES-256暗号化
   データライフサイクル管理
   機能分離によるデータアクセス制御と適切なデータ管理
   ダウンロード機能:ログインユーザーのみがアクセス可能
   計算JOBデータ:最大5日間保存後、自動的に完全削除(データの復元は不可能)
   データセンター
   日本国内(Microsoft Azure 東日本リージョン)
   ISO 27001、SOC 2 認証取得済み
   お客様への効果: データの暗号化保存により、情報漏洩リスクを最小化

5. 通信の暗号化
   実装内容： TLS 1.3による通信の暗号化
   HSTS適用によるHTTPS通信の強制
   SSL Server TestでA評価(2025年12月1日)を取得し、
   接続の暗号化品質を第三者評価で確認済み
   お客様への効果: 通信データの盗聴や改ざんを防止し、安全なデータ送受信を実現

🛠️ 継続的なセキュリティ監視

定期的な監査
セキュリティ脆弱性の定期的な監視
最新のセキュリティ脅威への対応
システムの継続的な改善

対応体制
セキュリティインシデント発生時の迅速な対応
お客様への適切な情報提供
必要に応じたシステムの緊急停止

📞 セキュリティに関するお問い合わせ

セキュリティインシデントの報告
セキュリティ上の問題を発見された場合や、不正アクセスの疑いがある場合は、
上記お問合せフォームよりご連絡ください。

🔄 セキュリティポリシーの更新

当社では、セキュリティ技術の進歩と脅威の変化に応じて、本セキュリティポリシーを定期的に更新いたします。重要な変更がある場合は、サービス内でお知らせいたします。

制定日:2025年10月1日
最終更新日:2026年1月6日
https://vrcsmanager.tpec.co.jp/security