



セキュリティホワイトペーパー

Ver1.0

2022年3月

株式会社プロレド・パートナーズ

- はじめに
- 利用者との責任分界点
- データ保管場所
- データの削除
- 利用者登録、招待
- アクセス権の管理
- パスワードの配布
- アカウント保護
- 暗号化の状況
- 変更管理
- 手順書の提供
- ログの提供
- ログのクロックに関する情報
- 脆弱性管理に関する状況
- 開発におけるセキュリティ情報
- インシデント発生時の対応
- 改訂履歴

はじめに

- 本セキュリティホワイトペーパーは、Pro-SignおよびPro-Leadのセキュリティに関して、利用規約を補足する文書です。利用者は、利用規約とあわせて本文書に従いサービスを利用する必要があります。利用規約またはプライバシーポリシーの内容と本文書内容との間に相違がある場合は、本文書の内容が優先するものとします。なお、とくに記載がない場合はPro-SignおよびPro-Lead共通の記述となります。

利用者との責任分界点

- 株式会社プロレド・パートナーズ（以下「当社」と表記）の責任
 - 当社は、以下のセキュリティ対策を実施します。
 - 当社が提供するサービスのセキュリティ対策
 - 上記サービスの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策
- 利用者の責任
 - 利用者は、以下のセキュリティおよびプライバシー保護の対策を実施する必要があります。
 - 各利用者に付与されたパスワードの適切な管理
 - アカウントの適切な管理（登録、削除、権限設定、組織管理者設定など）
 - 登録された情報の適切な管理

データ保管場所

- 当社は日本の法人であり、本社所在地は東京都です。サービスの開発、運用はすべて日本国内で行っています。
- 当社のサービスは、AmazonWebServices(AWS)を利用して構築しており、システムが保管するデータおよびそのバックアップデータは、いずれもAWSの管理するデータセンターに保管されています。
- メール送信など一部の処理に海外のリージョンを利用することはありますが、利用者からお預かりしたデータは、AWS東京リージョンに保管されます。また、AWSとの契約においては準拠法を日本法とする契約を結んでいます。

データの削除

- 現状で利用者のサービス利用終了後にデータの削除は行っておりませんが、2022年9月までに下記の通り対応予定です。
 - 利用者のデータについては、契約終了後の1ヶ月以内に削除
 - ただし契約書や見積書等の電子帳簿保存法の対象となるデータについては、当社が定める期間、当社が定める方法により参照可能

利用者登録、招待

- 利用者は、新規登録もしくは招待（Pro-Signのみ）を受けた際に、アカウントを作成できます。
- 企業担当者等の招待権限を持つ利用者は、新たな利用者を招待できます（Pro-Signのみ）。

アクセス権の管理

- 企業担当者等は自社内の一般ユーザーの権限を設定できます（Pro-Signのみ）。

パスワードの配布

- 利用者がアカウントを登録する際に自身のパスワードを設定できます。

アカウント保護

- パスワード設定時に短いパスワードや推測されやすいパスワードが登録できないようパスワード強度のチェックを行っております。

暗号化の状況

- データベースに保管される利用者の各種情報は、暗号化され適切なアクセス権のもとで保管されます。

変更管理

- 利用者への影響があるサービスの変更や、サービス停止を伴うメンテナンスについての情報は、下記のリンク先から参照できます。
- [Pro-Sign](#)
- [Pro-Lead](#)

手順書の提供

- サービス利用開始後に各種マニュアルを利用できます。

ログの提供

- 個別の利用者に対してのログ提供は行っておりません。

ログのクロックに関する情報

- ログの時間は、AWSが提供するNTPサービスと同期しています。

脆弱性管理に関する状況

- 当社が提供するサービスの開発チームは、利用するOS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。

- 当社が提供するサービスで利用しているライブラリ、コンポーネントに対する脆弱性パッチが公開された場合は、速やかに適用します。
- 半年に1回程度の間隔で外部機関による脆弱性診断を利用しております。

開発におけるセキュリティ情報

- コードレビュー実施などにより、基本的な脆弱性への対応ができているかなどの確認を行っています。
- サーバーにインストールされているライブラリ群について、バージョンが古い、脆弱性が発見されたなどのチェックを行っています。

インシデント発生時の対応

- お客様に大きな影響を与えるセキュリティインシデント（データの消失、長時間のシステム停止等）が発生した場合は、インシデント発生から2営業日以内を目標に、下記のリンク先Webページに情報を掲載します。また対象利用者への説明、4営業日以内の対処およびサービス安定化を行います。
- [Pro-Sign](#)
- [Pro-Lead](#)

改訂履歴

- 2022年3月Ver1.0作成