セキュリティホワイトペーパー（krewData）

メシウス株式会社

2023 年 11 月 1 日　Ver 1.1

用語の定義

このホワイトペーパーで使用する用語の定義を以下に示します。

用語	定義
krewData API	krewData の機能を外部から実行するための下記ヘルプドキュメントに記載されている API (Application Programming Interface) https://docs.krew.mescius.jp/krewdata/#api.html
外部連携するクラウドサービス	krewData が接続、およびデータ入出力を行う kintone 以外の外部クラウドサービス
サードパーティ	サイボウズ社、および krewData が接続、およびデータ入出力を行う外部クラウドサービスのプロバイダー
サードパーティ API	kintone、または外部連携するクラウドサービスの機能を外部から実行するための API
実行ユーザー	krewData が kintone アプリの情報、およびレコードデータを取得／更新する際の認証情報として使用する kintone アカウント
スケジュール	krewData がデータの集計・加工処理を自動実行する日時
設定情報	お客様が krewData の各機能を利用するために設定／保存した各種情報（データ編集フロー、スケジュール、アカウント情報、その他各機能で利用するデータなど）
データ編集フロー	krewData のコマンドを組み合わせ、データの入力から出力までの一連の集計・加工手順を定義した情報
プラグイン	kintone アプリに追加して使用するアプリの機能を拡張するプログラム

はじめに

1.1　ホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、メシウス株式会社（以下、当社）が提供する「krewData」におけるセキュリティの取り組みを、サービス利用者の方に向けてご確認いただくことを目的としております。

1.2　責任分界点

「krewData」は、Amazon Web Services（以下、AWS）を基盤にシステムを構築しています。また、kintone および外部連携するクラウドサービスが提供している API を使用して各サービスとのデータ入出力を行います。krewData に関する責任分界点は以下の通りとなります。

2　セキュリティへの取り組み

2.1　ISO/IEC27001、JIP-ISMS517-1.0（ISO/IEC27017）

当社は、2022 年 7 月に情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC 27001:2013（JIS Q 27001:2014）、および ISO/IEC 27017:2015（JIS Q 27017:2016）を取得しております。「krewData」が保有する情報資産を機密性、完全性、可用性の観点から維持・改善するために、事業内におけるセキュリティルールを確立し、継続的に運用、監視、改善を行っております。

2.2　クラウドコンピューティング環境

「krewData」は、クラウドコンピューティング環境として AWS を採用しています。AWS は、クラウドシステム運用の多くの実績があり、そのノウハウやサービスの継続的な改善や機能追加にも力を入れています。また、ISO/IEC27001:2013、ISO/IEC27017:2015 の認定を受けており、AWS が「krewData」の基盤として適切であると判断し、利用しております。

AWS のセキュリティ対策については、下記 URL をご参照ください。

AWS クラウドセキュリティ：https://aws.amazon.com/jp/security/

2.3　アカウント管理

「krewData」を利用するためのサービス固有のアカウントはありません。サービス利用者は、「krewData」の機能を利用して kintone、または外部連携するクラウドサービスにアクセスするために、kintone、または外部連携するクラウドサービスで作成したアカウントを「krewData」に登録して使用します。

2.4　サービス内におけるアクセス制限

「krewData」は kintone アプリのプラグインとして動作し、プラグインを追加した kintone アプリのアプリ管理権限を持つユーザーのみが利用できます。

kintone、または外部連携するクラウドサービスへのアクセスは「krewData」に登録した kintone、または外部連携するクラウドサービスのアカウントを使用して行います。アクセス制御はこのアカウントのアクセス権により kintone、または外部連携するクラウドサービス側で実施されます。

2.5　特権的なユーティリティプログラムの使用

「krewData」を利用するためのサービス固有のアカウントはなく、特権ユーザーは存在しません。このため、特権を使用してユーティリティプログラムや API を操作することはありません。

2.6　データの保管場所

お客様のデータ並びにバックアップは、AWS の日本国内リージョンに保管されます。

2.7　データの利用

法律上必要な場合を除き、保存されているお客様のデータを当社が利用することはございません。

2.8　データの削除

契約が終了した場合、お客様が「krewData」に保存した設定情報は契約終了から 30 日後に消去されます。さらに、その 7 日後にバックアップデータが消去され、以降、お客様の設定情報を復元することができないようになっております。尚、データ削除の証明書に類する書類は発行しておりません。

「krewData」に保存されるデータの詳細は、下記 URL をご参照ください。

https://docs.krew.mescius.jp/krewdata/#data_to_handle.html

2.9 アクセスコントロール

「krewData」は、当社内外問わず悪意のあるユーザーからの攻撃を防ぐために、必要最小限のポート開放を行っており、故意・過失による不正アクセスの可能性を抑制しています。また、「krewData」の機能を利用する際には kintone アカウントによる認証を行っています。

2.10 暗号化の状況

「krewData」のデータは、データベースに AES-256 により暗号化され保存されています。また、一般に公開される利用サービスの通信は TLS 1.2 方式により暗号化されます。

2.11 バックアップの状況

データベースに保管されるお客様の設定情報は、日次でバックアップを取得しています。バックアップは、7 世代分保管されます。

バックアップの対象となる「krewData」に保存されるデータの詳細は、下記 URL をご参照ください。

https://docs.krew.mescius.jp/krewdata/#data_to_handle.html

2.12 クロック

システムで使用しているクラウドサービスのクロックは NTP（Network Time Protocol）サーバを使用して時刻同期を行っており、タイムゾーンは UTC となっています。

2.13 ログに関する情報

「krewData」は、情報セキュリティポリシーに従い、最低 12 か月間のシステムログを保存し、監視を行っています。収集したログは、サービス利用状況の把握、障害発生時の原因調査などの目的で使用します。

2.14 情報のラベル付け

「krewData」は、保存されたデータに対してラベル付けを行う機能は提供しておりません。

2.15 ネットワークの分離

「krewData」は、マルチテナント方式でサービスを提供しています。各テナントのネットワークは VPC（Virtual Private Cloud）を用いて他の仮想ネットワークから論理的に切り離すよう構築しており、テナント間のアクセスができない構成になっています。

2.16 サービスのバージョンアップ

サービスのバージョンアップは、実施前に「krewData」利用契約時にご登録頂いた担当者のメールアドレスに対して、メールにてご連絡いたします。

2.17 開発におけるセキュリティ情報

「krewData」のシステム開発は、脆弱性を作りこまないよう、 OWASP Application Security Verification Standard などの一般的なセキュリティ対策基準に従って実施されます。

2.18 インシデント発生時の対応

当社 Web サイトのお知らせページ（https://krew.mescius.jp/news/）や「障害/メンテナンス情報」（https://krew.statuspal.io/）にて通知いたします。また、影響度に応じてご契約者様・追加連絡先へのメール配信も行います。

なお、お客様からの情報セキュリティインシデントに関する問合せは、メールで es.security@mescius.com までお知らせください。

2.19 適用法令

お客様と当社との間の契約は、日本法に基づいて解釈されるものとします。AWS に適用される法域については、準拠法は日本法で、裁判所は東京地裁になります。

【改訂履歴】

本書の改訂履歴は以下のとおりです。

Ver.	発行日	改訂内容
1.0	2023/07/04	制定
1.1	2023/11/01	・当社社名を変更 ・当社サイトの URL を変更