krewセキュリティチェックシート (経産省版)

バージョン：1.2

◆本チェックシートはメシウス株式会社が提供するクラウドサービス krewSheet、krewData、krewDashboard (以下「krewシリーズ」)について安全・信頼性に係る情報を記載したものです。
◆本チェックシートの項目は、経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版
（https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）を基に、任意で項目の追加削除、及び主客体の解釈を加えて作成したものです。
◆本チェックシートは、改善のために予告なく変更することがあります。
◆ISO27001の認証について
メシウス株式会社は、情報セキュリティに対する国際水準の第三者適合性評価制度である「情報セキュリティマネジメントシステム」の認証基準を取得しています。
認証番号：JQA-IM1900、認証規格：ISO／IEC27001：2013／JIS Q 27001：2014
認証機関：一般社団法人 日本品質保証機構、初回認証登録日：2022年7月1日
登録活動範囲：
・業務アプリ開発支援ツールの開発／販売／サポート
・システム開発支援ツールの開発／販売／サポート／サービス提供
・学校法人向け会計／給与／資産／学費／人事システムおよび関連サービスの開発／販売／サポート／サービス提供
◆ISMSクラウドセキュリティ認証について
メシウス株式会社は、クラウドサービスに特化した情報セキュリティの認証である「ISMSクラウドセキュリティ認証」を取得しています。
認証番号：JQA-IC0075、認証規格：JIP-ISMS517-1.0
認証機関：一般社団法人 日本品質保証機構、初回認証登録日：2022年7月1日
登録活動範囲：
・学校法人向け業務システムサービス（LeySer System、LeySer Web出願、LeySerKids）
・業務アプリケーション機能拡張サービス（krew、RayKit）

項番	確認事項	実施有無	備考
1 情報セキュリティのための方針群			
1-1	経営陣によって承認された情報セキュリティに関する基本方 針を定めた文書があること。また、該当文書を全従業員及びクラウドサービス利用者に明示すること。	○	当社代表取締役によって承認された情報セキュリティ基本方針を定めております。当社情報セキュリティ基本方針は、全従業員に社内規定として周知し、クラウドサービス利用者には当社ホームページに公開しております。 ・情報セキュリティ基本方針：https://www.mescius.com/security.html
1-2	情報セキュリティに関する基本方針を定めた文書は、定期的 またはクラウドサービス提供に関係する重大な変更が生じた場合に、レビューすること。	○	当社は情報セキュリティマネジメントシステム（以下、ISMS）を構築し、情報セキュリティ保全活動を効果的に推進するために、情報セキュリティ基本方針を定め、実施運用し、監査及び見直しを行う仕組みを確立しております。また、当社代表取締役によって承認された情報セキュリティ方針は、ISMSに基づき、経営者によって毎年及び重大な変化が発生した場合に見直しております。
2 情報セキュリティのための組織			
2-1 内部組織			
2-1-1	経営陣は、情報セキュリティに関する取り組みについての責 任及び関与を明示し、組織内におけるセキュリティを積極的に支持・支援を行うこと。	○	情報セキュリティ基本方針は業務に関わる役員、社員が継続的に情報セキュリティ対策を推進することを宣言しております。また、ISMSの整備・運用方法を明記した文書（以下、情報セキュリティ管理策運用規定）にて、各項目に責任と権限を明記し、実施しております。

2-1-2	情報セキュリティ責任者とその役割を明確に定めること。ま たクラウドサービスの情報セキュリティに関する窓口を明確にし、外部に公開すること。	○	情報セキュリティ管理策運用規定にて、管理責任者の責任と権限を定めております。また同マニュアルにて、情報セキュリティの方針、目標の設定、承認、マネジメントレビュー、関係当局との連絡体制構築の実施など、全社のセキュリティ活動の推進を行うことが役割であることを明記しております。krewシリーズの情報セキュリティに関する窓口は、メールでお問い合わせいただく窓口を公開しております。 ・電子メール：es.security@mescius.com
2-1-3	情報セキュリティ対策、設備の認可に対する手順等を明確にし、文書化すること。	○	情報セキュリティ管理策運用規定にて、情報セキュリティ対策（日々の活動、緊急対応、役割、承認等）を明記しております。
2-1-4	クラウドサービス利用者がクラウドサービスの受け入れを行うために必要な資料を作成し、提供すること。また、提供するクラウドサービスSLA などサービス開始前の合意事項をクラウドサービスの利用を検討する者に明示すること。	○	本チェックシートにて、クラウドサービス利用者に対し、提供するクラウドサービスに関するセキュリティ対策を記載し、提供しております。また、krewシリーズはSLAを規定しておりませんが、サービス開始前の合意は、クラウドサービス利用者に対し、当社ホームページ（https://krew.mescius.jp/slo/）に提供するサービスレベル目標（SLO）を公開しております。
2-1-5	クラウドサービスのサポート窓口、苦情窓口を明確にし、外部に公開すること。	○	メール、Webフォーム、電話でお問い合わせいただく窓口を公開しております。 ・電子メール：es.sales@mescius.com ・Webフォーム（技術サポート）：https://krew.zendesk.com/hc/ja/requests/new ・電話：050-5490-4660 営業時間、電話の受付時間は、当社営業日の10:00～12:00、13:30～17:00とさせていただいております。電子メール、Webフォームは24時間365日受け付けております。 技術サポートの内容は、krew技術サポートサービス説明書（https://download.krew.mescius.jp/license/krew_support_service.pdf）にて規定しております。
3 人的資産のセキュリティ			
3-1 雇用前			
3-1-1	従業員のセキュリティの役割及び責任は、情報セキュリティ基本方針に従って定め、文書化すること。また該当文書を雇用予定の従業員に対して説明し、この文書に対する明確な同意をもって雇用契約を結ぶこと。	○	情報セキュリティ基本方針（https://www.mescius.com/security.html）及び社内セキュリティに関する従業員が遵守すべき社内規程（情報セキュリティ管理規定）を定めております。また、雇用する従業員とは、雇用契約書を締結し、その中で就業規則及び社内規程の遵守について署名、押印をもって明確に同意を確認しております。
3-2 雇用期間中			
3-2-1	すべての従業員に対して、情報セキュリティに関する意識向上のための教育・訓練を実施すること。	○	すべての従業員は情報セキュリティに関する意識向上のための教育及び訓練を受けなければならない旨、情報セキュリティ管理策運用規程に明記されております。また、情報セキュリティ管理策運用規定に則り、教育及び訓練を実施しております。
3-2-2	セキュリティ違反を犯した従業員に対する対応手続きを備えること。	○	ISMSの規程で定められた内容に違反（情報セキュリティ違反）する行為を行った従業者については、「就業規則」に従い、懲戒手続きを行うことが情報セキュリティ管理策運用規定に明記されております。
3-3 雇用の終了または変更			
3-3-1	従業員の雇用の終了または変更となった場合に、情報資産、アクセス権等の返却・削除・変更の手続きについて明確にすること。	○	情報セキュリティ管理策運用規程にて、従業員の雇用の終了または変更となった場合の手続きが明記されております。 - 秘密保持契約書に署名しなければならない。 - 退職時は、保有していた全ての当社資産を返却しなくてはならない。 - アクセス権等の削除または使用停止、変更を行う。
4 資産の管理			
4-1	情報資産について明確にし、重要な情報資産の目録及び各情報資産の利用の許容範囲に関する文書を作成し、維持すること。また情報資産について管理責任者を指定すること。	○	情報資産台帳にて、各資産名、管理責任者、C.I.Aレベル、利用許可範囲、保存期間ごとに分類し、記載しており、当台帳は、ISMSにおいて、定期的に見直し、更新しております。
4-2	組織に対しての価値、法的要求事項、取り扱いに慎重を要する度合い及び重要性の観点から情報資産を分類すること。	○	

5 物理的及び環境的セキュリティ			
5-1	重要な情報資産がある領域を保護するために、物理的セキュリティ境界(例えば、有人受付、カード制御による入口)を用いること。	○	情報資産がある領域（セキュリティエリアは、執務スペース）は、セキュリティカード制御を用いて、フリースペースとの物理的な境界を設けております。重要な情報資産がある領域である入室制限スペースは、施錠したドアと閉鎖された空間により境界を設けております。重要な情報資産のある重要書類スペースは、施錠したキャビネットにより物理的な境界を設けております。
5-2	重要な情報資産がある領域へ許可された者のみがアクセスできるように入退室等を管理するための手順、管理方法を文書化すること。	○	重要な情報資産がある領域は、情報セキュリティ管理策運用規程に明記されており、許可された者のみがアクセスできるようにセキュリティカード制御及び専用鍵を有しております。
5-3	サーバーが設置されているデータセンターは耐震構造となっていること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
5-4	データセンターの落雷対策を確認すること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
5-5	データセンターの水害対策を確認すること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
5-6	データセンターの静電気対策を確認すること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6 運用のセキュリティ・アクセス制御			
6-1	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の運用管理の手順について文書化し、維持していくこと。	○	アプリケーションの運用管理手順については文書を作成しています。こちらの文書については操作方法の変更や機材追加・変更が発生する毎に更新しております。 krewDataはAWSにてサーバーレスで構築／運用されており、OS、サーバー、ネットワーク機器の運用管理はAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-2	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の変更について管理すること。またクラウドサービス利用者に影響を及ぼすものは事前に通知すること。	○	krewシリーズ各製品のアップデートなど、通常、メンテナンス実施日の1週間前までに告知します。 ※緊急でメンテナンスを行う場合はその限りではありません。 通知方法は、弊社Webサイトでの掲載及び、ご契約者様・追加連絡先へのメール連絡となります。
6-3	クラウドサービスを利用できるオペレーティングシステムやウェブブラウザの種類とバージョンを明示すること。利用できるOSとブラウザに変更が生じる場合は事前に通知すること。	○	krewシリーズ各製品はkintone上で提供しているサービスであり、クライアント環境要件はkintoneに準じます。 ※kintoneモバイル版では動作しません。
6-4	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	脆弱性情報について適宜収集し、影響について確認をしております。なお、krewDataはAWSにてサーバーレスで構築／運用されており、オペレーティングシステム、サーバー、ネットワーク機器についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-5	クラウドサービスの資源の利用状況について監視・調整をし、利用状況の予測に基づいて設計した容量・性能等の要求事項について文書化し、維持していくこと。	○	クラウドサービスの利用状況については監視を実施しております。krewDataはAWSにてサーバーレスで構築／運用されており、リソースの増強・増設は自動で行われます。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-6	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器について脆弱性診断を行うこと。また、その結果を基に対策を行うこと。	○	OWASP アプリケーションセキュリティ検証標準に従ってサービスリリース前にレビューを行い、問題が発見された場合は対処を行っております。

6-7	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また、認可されていないモバイルコードを実行できないようにすることが望ましい。	○	kintone連携製品で使用できるモバイルコード（JavaScript）は、cybozu.com上で動作します。cybozu.comを提供するサイボウズ社では、安全なJavaScriptコードを作成することを支援する目的として「セキュアコーディングガイドライン」を公開しており、弊社では本ガイドラインに従ったアプリケーション開発を行っております。 https://cybozudev.zendesk.com/hc/ja/articles/201919400-%E3%82%BB%E3%82%AD%E3%83%A5%E3%82%A2%E3%82%B3%E3%83%BC%E3%83%87%E3%82%A3%E3%83%B3%E3%82%B0-%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3
6-8	クラウドサービス利用者の情報、ソフトウェア及びソフトウェアの設定について定期的にバックアップを取得し、検査すること。	○	krewDataにおいて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、オンラインヘルプ「krewDataで取り扱うデータ」（https://docs.krew.mescius.jp/krewdata/#data_to_handle.html）をご参照ください。※krewSheet、krewDashboardはkintone上で動作します。当社サーバー側でkintoneアプリデータの取得／保存は一切行いません。
6-9	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネット ワーク機器の稼働監視をすること。サービスの停止を検知した場合は、利用者に対して通知すること。	○	クラウドサービスの提供に用いるアプリケーションの監視を実施しております。なお、krewDataはAWSにてサーバーレスで構築／運用されており、オペレーティングシステム、サーバー、ネットワーク機器についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です サービスの停止を検知した場合は、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。
6-10	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器の障害監視をすること。障害を検知した場合は、利用者に対して通知すること。	○	クラウドサービスの提供に用いるアプリケーションの監視を実施しております。なお、krewDataはAWSにてサーバーレスで構築／運用されており、オペレーティングシステム、サーバー、ネットワーク機器についてはAWSの管理範囲となっております。※krewSheet/krewDashboardはkintone上で動作するため、対象外です 障害を検知した場合は、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。
6-11	システムの運用担当者(開発・インフラ)の作業については記録すること。	○	作業を実施する際には変更管理に則り、相互確認を行いながら複数人で実施しております。作業は手順書に基づいて実施しております。
6-12	例外処理及びセキュリティ事象を記録した監査ログを取得すること。また該当のログのアラートについては定期確認し、改竄、許可されていないアクセスがないように保護する。	○	例外処理、およびセキュリティ事象を記録した監査ログを取得しております。該当のログについては運用管理者及びアクセスが許可されたもののみがアクセスできる場所に保管しております。
6-13	クラウドサービス上で取得する利用者の活動、例外処理及びセキュリティ事象を記録した監査ログについて明示すること。また監査ログの保持する期間、提供方法、提供のタイミングについて明示すること。	○	情報セキュリティ管理策運用規定に従い 、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。お客様へのログの提供サービスは行っておりません。
6-14	クラウドサービスの提供に用いるアプリケーション、オペレーティングシステム、サーバー、ネットワーク機器については正確な時刻源と同期させること。	○	krewDataはAWSにて構築／運用されており、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。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-15	クラウド基盤システムへのアクセスについては、各個人に一意な識別子にし、セキュリティに配慮したログオン手順、認証技術によって制御すること。またアクセス制御方針について文書化すること。	○	システムのアカウントについては当社規定に則り、各個人に一意の識別子を付与しております。アクセスが許可されていない者がアクセスできないように制御しております。

6-16	クラウド基盤システムへのアクセス権限の追加・削除・変更について手順を備えること。また特権の割り当て及び利用は制限し、管理すること。	△	クラウド基盤システムへのアクセス権限の追加・削除・変更に関する手順の文書化は行っておりません。特権の割り当て及び利用は制限し、管理しております。
6-17	システムの運用担当者が利用するパスワードについては管理し、また良質なパスワードにすること。	○	パスワードについては情報セキュリティ管理策運用規程に則り、管理しております。
6-18	クラウド事業者は、クラウド利用者がネットワークサービスの利用に関する方針を策定できるよう、クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	○	krewシリーズ各製品は、cybozu.comをプラットフォーム（アプリケーションを動作する、データを保存するなどの基盤製品）としています。cybozu.comを運営するサイボウズ社では、cybozu.com サービスを利用する際の認証方法、アクセス制限の設定について（https://www.cybozu.com/jp/security/illegal_access/）明記しております。 krewDataはAWSにて構築／運用されております。krewDataを利用するにあたり、AWSに関して特段の制限はありません。
6-19	提供するクラウドサービスにおいてアクセス制御機能を提供すること。	-	krewシリーズ各製品はkintone上で提供しているものであり、アクセス制御はkintoneに準じます。krewシリーズ各製品を利用する際にはライセンス認証を行います。
6-20	クラウド事業者は、各クラウド利用者に割り当てたコンピューティング資源に、他のクラウド利用者や許可されていないユーザがアクセスできないように管理し、物理的な設定や移行にかかわらず、仮想環境の分離を確実にすることが望ましい。 ネットワーク若しくはインタフェースの分離がなされていない場合、クラウド事業者は、アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。 クラウド事業者は、クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために、クラウド環境における情報セキュリティについて評価を実施することが望ましい。	○	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。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-21	提供するクラウドサービスにおいて利用者のID登録・削除機能を提供すること。	-	krewシリーズ各製品へはkintoneを通じて行われ、本事項はkintoneに準じます。
6-22	提供するクラウドサービスにおいて特権の割り当て及び利用制限し、管理する機能を提供すること。	○	krewシリーズ各製品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。
6-23	提供するクラウドサービスにてパスワード管理ができるような機能を提供すること。また良質なパスワードを確実にする機能があること。	-	krewシリーズ各製品へはkintoneを通じて行われ、本事項はkintoneに準じます。
6-24	提供するクラウドサービスで提供している情報セキュリティ対策及び機能を列記し、明示すること。	○	ISMS文書（情報セキュリティ管理規定）に沿った開発を実施しております。 ・DBデータ搾取の保護に対応しています。 ・DBデータを定期バックアップし、データ消失に対応しています。 ・システムを不正に操作できないよう保護に対応しています。 ・データセンターにAWSを使用し、高度なセキュリティに対応しています。
6-25	一定の使用中断時間が経過したときには、使用が中断しているセッションを遮断すること。またリスクの高い業務用ソフトウェアについては、接続時間の制限を利用すること。	-	krewシリーズ各製品へはkintoneを通じて行われ、本事項はkintoneに準じます。
6-26	ネットワークを脅威から保護、またネットワークのセキュリティを維持するためにネットワークを適切に管理し、アクセス制御をすること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-27	ネットワーク管理者の権限割り当て及び利用は制限し、管理すること。またネットワーク管理者もアクセスを管理するためにセキュリティに配慮したログオン手順、認証技術によって制御すること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
6-28	外部及び内部からの不正なアクセスを防止する装置(ファイアウォール等)を導入すること。また利用することを許可したサービスへのアクセスだけを提供すること。	○	krewDataはAWSにて構築／運用されており、マルチテナントの公開システムとして運用しております。サービスへのアクセスについてはサービス利用のための特定のポートのみを公開しております。また、ウェブアプリケーションファイアウォール（WAF）を設置し、外部及び内部からの不正アクセスを防止しております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です

6-29	クラウドサービスへの接続方法に応じた認証方法を提供すること。クラウドサービスへの接続方法に応じた認証方法を、クラウドサービスの利用を検討するものに明示すること。	-	krewシリーズ各製品はkintone上で提供しているものであり、アクセス制御はkintoneに準じます。krewシリーズ各製品を利用する際にはライセンス認証を行います。
6-30	クラウドサービスの契約が終了した場合にデータが消去されること。消去されるなら、その時期や削除される範囲について確認すること。	○	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。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、オンラインヘルプ「krewDataで取り扱うデータ」（https://docs.krew.mescius.jp/krewdata/#data_to_handle.html）をご参照ください。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。 ※krewSheet、krewDashboardはkintone上で動作します。当社サーバー側でkintoneアプリデータの取得／保存は一切行いません。
6-31	クラウドサービスを利用するネットワーク経路が暗号化されていることを確認すること。クラウドサービスで利用する情報がシステム上で暗号化されていること。	○	krewDataではサービスを利用するお客様端末と当社サーバー間の通信はkintone経由で行われます。当社サーバーとkintone間の通信はすべてkintone APIにより行われ、通信プロトコルはHTTPS（TLS 1.2）を使用しております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
7 供給者関係			
7-1	外部組織がかかわる業務プロセスから、情報資産に対するリスクを識別し、適切な対策を実施すること。	○	krewDataにお客様が登録した情報については、その情報の内容を問わず、最善の注意を持って管理し、別段の定めがある場合を除き（krewサービス利用規約のデータの入力・管理、個人情報の取扱いに記載）、お客様の書面による承諾を得ることなく、本サービス以外の目的のために利用あるいは複製し、または第三者に利用させ、もしくは開示、漏洩いたしません。 また、krewDataではAWSを利用しておりますが、AWSではSOCレポート（https://aws.amazon.com/jp/compliance/soc-faqs/）において重要なコンプライアンス管理および目標を AWSがどのように達成したかを実証する、独立したサードパーティーによる審査報告書を公開しております。 ※krewSheet、krewDashboardはkintone上で動作します。当社サーバー側でkintoneアプリデータの取得／保存は一切行いません。
8 情報セキュリティ事象・情報セキュリティインシデント			
8-1	すべての従業員は、システムまたはサービスの中で発見したまたは疑いをもったセキュリティ弱点はどのようなものでも記録し、報告するようにすること。	○	情報セキュリティ管理策運用規程にて、セキュリティ事故の定義、発生時の報告について定めており、またウィルス感染の疑いや利用しているサービスから情報漏えい等の事故があった場合の報告連絡手段、対応手続を定めております。
8-2	情報セキュリティインシデントに対する迅速、効果的で毅然とした対応をするために責任体制及び手順書を確立すること。	○	情報セキュリティ管理策運用規程にて、情報セキュリティインシデントに対応するため、責任体制、報告連絡手段、対応手順を定めております。
8-3	情報セキュリティインシデントの報告をまとめ、定期的にクラウド利用者に明示すること。	○	定期的な明示はしておりませんが、当社およびkrewシリーズ各製品における情報セキュリティインシデントは、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/）にて公開いたします。
9 事業継続マネジメントにおける情報セキュリティの側面			
9-1	業務プロセスの中断を引き起こし得る事象は、中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに特定すること。	○	情報セキュリティ管理策運用規程に従い、事業継続リスク分析及びビジネスインパクト分析をおこなっております。その中で各業務プロセスの中断発生確率、復旧許容時間から優先度を定め、要求されたレベルで時間で復旧できるように事業継続計画を作成しております。
9-2	クラウド事業者は，クラウドサービスを提供するシステムの冗長化を図るとともに、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	○	krewDataはAWSにてサーバーレスで構築／運用されており、本事項はAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
9-3	事業継続計画については定期的に試験・更新すること。	○	情報セキュリティ管理策運用規程に従い、事業継続計画の有効性の評価を毎年1回行い、有効性に問題があると判断された場合には見直しを行っています。
9-4	クラウドサービス提供に用いる機材は、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です

9-5	クラウドサービス提供に用いる機材を設置する部屋には、火災検知・通報システム及び消火設備を用意すること。	○	krewDataはAWSにて構築／運用されており、本事項についてはAWSの管理範囲となっております。 ※krewSheet/krewDashboardはkintone上で動作するため、対象外です
10 遵守			
10-1	関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取り組み方を明確に定め、文書化し、維持すること。また重要な記録については消失、破壊及び改ざんから保護し、適切に管理すること。	○	ISMSに影響を及ぼす可能性のある変更(関連する法令、国の定める指針その他の規と改正状況を反映した資源、組織、規定、規格の変更)は、ISMSの中で、確認されることになっております。ISMSに作成・利用される文書・記録は、文書ごとに、管理者、承認者、保管期間を定め、適切に管理しております。
10-2	クラウド事業者は，クラウド事業を営む地域（国，州など），データセンターの所在する地域（国，州など）及びクラウド事業者自らが適用を受ける法令，規制及び契約上の要求事項を明示することが望ましい。	○	krewSheet、krewDashboardはkintone上で動作します。krewDataはAWSの東京リージョンで構築／運用しております。 また、krewサービス利用規約（準拠法および裁判管轄）において、準拠法および裁判管轄について定めております。 ・krewサービス利用規約：https://download.krew.mescius.jp/license/krew_license.pdf
10-3	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい	○	krewサービス利用規約（知的財産権等）において、知的財産権について利用を許諾する範囲を定めております。
10-4	認可されていない目的のための情報処理施設の利用は阻止すること。	○	情報セキュリティ管理策運用規程にて、物理的境界及びその他の各境界へのアクセスが許可される者について定めており、アクセス許可がされていない者はアクセスできないように制限をかけております。またアクセス許可判断方針についても定めております。
10-5	個人データ及び個人情報は、関連する法令、規制、及び適用がある場合には、契約事項の中の要求にしたがって確実に保護すること。	○	当社のプライバシーポリシーに従って適切に取り扱っております。 ・プライバシーポリシー（メシウスの個人情報保護方針）：https://www.mescius.com/policy/privacy/
10-6	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、脆弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。また、クラウド事業者は、クラウド利用者の個別の監査要求に応える代わりに、クラウド利用者との合意に基づき、独立したレビュー及び評価の結果を提供することが望ましい。	○	krewシリーズの各製品は、OWASP アプリケーションセキュリティ検証標準に従ってサービスリリース前にレビューを行い、問題が発見された場合は対処を行っております。レビュー結果は非公開とさせていただいております。 また、クラウド利用者による脆弱性診断は非対応とさせていただいております。
11 その他			
11-1	記録媒体(書類、記録メディア)の保管管理については適切に行うこと。また廃棄する際には記録された情報を復元できないように安全に処分すること。また再利用の際には機密情報の漏えい等につながらないように対処すること。	○	情報セキュリティ管理策運用規程にて、記録媒体の情報取扱方法（保管、廃棄）を定め、適切に取り扱っております。
11-2	重要な情報資産については、机の上に放置せず安全な場所に保管すること（クリアデスク）。また離席時には情報を盗み見られないように情報端末の画面をロックすること(クリアスクリーン)。	○	情報セキュリティ管理策運用規程にて、クリアデスク（重要な情報資産は、作業終了時には、施錠されたキャビネット、引出しに保管）と離席する場合は、第三者が容易に操作及び閲覧ができないようスクリーンロック等の対策を講じるよう定め、実施しております。
11-3	従業員のパソコンにウィルス対策を行うこと。また技術的脆弱性に関する情報は、定期的に収集し、適切にパッチの適用を行うこと。	○	情報セキュリティ管理策運用規程にて、クライアントPCに関する利用者の遵守事項（ウィルス対策等）を定め、遵守しております。技術的脆弱性に関する情報は、ウィルス、スパイウエア、技術的脆弱性等への対策について、情報収集と情報周知を実施しております。
11-4	サービス提供を終了する場合は、利用者に対して事前に通知を行うこと。	○	krewシリーズ各製品の提供終了およびサービス廃止する場合、3ヶ月以上前に通知いたします。詳細はkrewサービス利用規約（本サービスの廃止）にて定めております。
11-5	サービス提供にあたって役割分担および責任範囲を明示していること。	○	責任分界点はkrewシリーズ各製品のセキュリティホワイトペーパーを参照してください。
11-6	情報のラベル付けをする機能が提供されていること。	×	krewシリーズ各製品では情報のラベル付けをする機能を提供しておりません。