クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）（https://www.soumu.go.jp/main_content/000771515.pdf）を基に任意で項目の追加削除を行い作成したものです。

ANNEX2 対策一覧

ISMS 管理策	項番	対策項目	対策内容	区分	公開回答
A.5	Ⅱ．1．情報セキュリティへの組織的取組の基本方針				
A.5.1	Ⅱ．１．１．組織の基本的な方針を定めた文書				
A.5.1.1	Ⅱ．１．１．１	方針の作成・承認・配布	クラウドサービス事業者は、組織全体での情報セキュリティに関する取組についての基本的な方針、役割、責任等を定めた文書を作成し、経営陣の承認及び署名等を経て、組織内及び関係する組織に配布すること。	基本	当社ISMSに基づき、実施しています。
A.5.1.2	Ⅱ．１．１．２	方針の変更	情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更や不適合が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。事業者は、経営陣の承認の下で方針の改定等を実施し、組織内及び関係する組織に通知すること。	基本	当社ISMSに基づき、実施しています。
A.5.1.1	Ⅱ．１．１．３	文書保護	事業者は、情報セキュリティに関する基本的な方針を定めた文書を、不正な開示や変更から保護すること。	推奨	当社ISMSに基づき、実施しています。
A.6	Ⅱ．２．情報セキュリティのための組織				
A.6.1	Ⅱ．２．１．内部組織				
A.6.1.1	Ⅱ．２．１．１	情報セキュリティ責任者	経営陣は、情報セキュリティに関する取組についての責任と関与を明示する。更に、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命し、人員・資産・予算等のリソース面で積極的な支援・支持を行うこと。	基本	当社ISMSに基づき、実施しています。
A.6.1.1	Ⅱ．２．１．２	システム一覧	情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定めるとともに、個々の組織の職務記述書にセキュリティとプライバシーに関する役割と責任を記載すること。	基本	当社ISMSに基づき、実施しています。
A.6.1.2	Ⅱ．２．１．３	相反する職務と責任の分離	組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、相反する職務及び責任範囲は、分離すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．２．１．４	リスク管理戦略	情報セキュリティへの侵害が、業務、資産、個人、他の組織及びサプライチェーンへもたらす脅威に対するリスクを管理するために、組織全体の包括的なリスク管理戦略を策定する。リスク管理戦略は、定期的又はクラウドサービスの提供に係る変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．２．１．５	テスト、トレーニング及び監視	組織全体にわたって実施されるセキュリティテスト、プライバシーテスト、トレーニングを監視すること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．２．１．６	組織内苦情管理	組織のセキュリティ施策とプライバシーの取組に対する従業員からの苦情、懸念又は質問を受け取り、対応するための仕組みを構築すること。	推奨	当社ISMSに基づき、実施しています。
A.6.2	Ⅱ．２．２．モバイル機器及びテレワーキング				
A.6.2.1	Ⅱ．２．２．１	モバイル機器の利用方針	モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じること。	基本	当社ISMSに基づき、実施しています。
A.6.2.2	Ⅱ．２．２．２	テレワーキングでの情報保護	テレワーキングでアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施すること。	基本	当社ISMSに基づき、実施しています。
A.15.1.3	Ⅱ．３．サプライチェーンに関する管理				
A.15.1.3	Ⅱ．３．１．サプライチェーン事業者間の合意				
	Ⅱ．３．１．１	リスク対策と文書化	サプライチェーン事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティリスク対策及びサービスレベルを文書化するとともに、サプライチェーン事業者によって確実に実施されることを担保すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．３．１．２	サービスの監視	サプライチェーン事業者が提供するクラウドサービスを定常的に監視・レビューし、運用に関する記録及び報告を常に実施すること。また、定期的に監査を実施することについて、サプライチェーン事業者と合意し文書化すること。	基本	当社ISMSに基づき、文書化および合意しています。

クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

	Ⅱ．3．1．3	リスク評価とレビュー	サプライチェーン事業者が提供するシステム、システムコンポーネント、クラウドサービスに関連するサプライチェーン関連のリスクを評価及びレビューすることについて、サプライチェーン事業者と合意し文書化すること。	基本	合意内容に含んでおりません。
	Ⅱ．3．1．4	関連情報の保護	システム、システムコンポーネント、クラウドサービスに関するサプライチェーン関連情報を保護することについて、サプライチェーン事業者と合意し文書化すること。	基本	当社ISMSに基づき、文書化および合意しています。
	Ⅱ．3．1．5	侵害通知	サプライチェーンのセキュリティ侵害に関する通知について手順を確立し、サプライチェーン事業者と合意し文書化する。	基本	当社ISMSに基づき、文書化および合意しています。
	Ⅱ．3．1．6	変更管理	関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価に伴う、サプライチェーン事業者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び対応策の保守及び改善を含む）を管理することについて、サプライチェーン事業者と合意し文書化すること。	基本	当社ISMSに基づき、文書化および合意しています。
	Ⅱ．3．1．7	耐タンパー性と検出	システム、システムコンポーネント、クラウドサービスの改ざん防止プログラムを実装することについて、サプライチェーン事業者と合意し文書化すること。	推奨	サプライヤーとの合意内容に含んでおりません。
	Ⅱ．3．1．8	システム又はシステムコンポーネントの検査	改ざんを検出するために、システム、システムコンポーネント又はクラウドサービスをランダムに検査することについて、サプライチェーン事業者と合意し文書化すること。	推奨	サプライヤーとの合意内容に含んでおりません。
	Ⅱ．3．1．9	システムコンポーネントの信頼性	偽造システムコンポーネントがシステムやクラウドサービスに侵入することを検出及び防止する手段を実装することについて、サプライチェーン事業者と合意し文書化すること。	推奨	サプライヤーとの合意内容に含んでおりません。
	Ⅱ．3．1．10	システムコンポーネントの廃棄	データ、ドキュメント、ツール、又はシステムコンポーネントを破棄する方法を確立するとともに、廃棄方法についてサプライチェーン事業者と合意し文書化すること。	基本	サプライヤーとの合意内容に含んでおりません。
A.15.1.3	Ⅱ．3．2．サプライチェーン事業者の選定				
	Ⅱ．3．2．1．	選定・契約	サプライチェーン事業者のリスクからクラウドサービスを保護するために、状況に応じて最も適した取得・調達・契約方法を採用すること。	基本	当社ISMSに基づき、実施しています。
A.8	Ⅱ．4．情報資産の管理				
A.8.1	Ⅱ．4．1．情報資産に対する責任				
	Ⅱ．4．1．1．	管理責任者	取り扱う各情報資産について管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にした上で管理するとともに、文書化すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．4．1．2．	事業者間の引継ぎ	クラウドサービス利用者がクラウドサービスの利用を終了するにあたり、他のクラウドサービスへの乗換を行うことが想定される。クラウドサービス利用者によるクラウドサービス選定の自由を守るため、事業者は預託された情報を他のクラウドサービスに引き継ぐか否かに関して、予め利用者と合意し、文書化すること。	基本	データエクスポート機能について、マニュアルに記載し、利用者に提供しています。
	Ⅱ．4．1．3．	バックアップ	情報、ソフトウェア及びシステムのバックアップは、利用者と合意されたバックアップ方針に従って、事業者が定期的に実施し、バックアップ内容を検査すること。また、事業者は、利用者にバックアップ機能の仕様を提供すること。	基本	当社ISMSに基づき、バックアップを実施しています。利用者が実施するバックアップについては、データエクスポート機能について、マニュアルに記載し、利用者に提供しています。
	Ⅱ．4．1．4．	当初目的との一致	時間の経過とともに、当初の目的や提供機能の範囲外のサービス及び機能をサポートする場合があるが、情報資産が当初の目的と一致して使用されていることを確認すること。	推奨	当社ISMSに基づき、実施しています。収集した個人情報については、「KING OF TIME」使用規約　第６条に記載しています。
A.8.2	Ⅱ．4．2．情報の分類				
	Ⅱ．4．2．1．	資産目録	組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、機密性や重要性の観点から情報資産を分類した上で、資産目録を作成し、維持すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．4．2．2．	データ識別	事業者は、利用者のデータ及びクラウドサービスから派生したデータを明確に識別すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．4．2．3．	情報資産の取扱い	情報資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施すること。	基本	当社ISMSに基づき、実施しています。

クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

A.18.2.2	**Ⅱ．４．３．情報セキュリティポリシーの遵守、点検及び監査**				
	Ⅱ．４．３．１．	**レビュー**	各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行うこと。また、組織の情報セキュリティのための方針群及び標準に関し、システムや提供するクラウドサービスが、定めに従って技術的に順守されていることをレビューすること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．４．３．２．	**点検・監査**	クラウドサービスの提供に用いるシステムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に検証・監査すること。システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、実施すること。	基本	当社ISMSに基づき、実施しています。
A.9.1	**Ⅱ．４．４．アクセス管理**				
A.9.1.1	**Ⅱ．４．４．１．**	**アクセス制御方針**	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすること。また、情報及びシステム機能へのアクセスは、アクセス制御方針に従って、制限すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．４．４．２．	**アクセス制御**	事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを、利用者が制限できるようにアクセス制御を提供すること。	基本	IPアドレスによる管理者のアクセス制限などの機能を提供しています。 https://support.ta.kingoftime.jp/hc/ja/articles/360038257234
A.9.4.4	**Ⅱ．４．４．３．**	**ユーティリティプログラムの使用**	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラム(データベースの中身を強制的に書き換えることが出来る機能や一時的にポートを開放する機能等)の使用は、制限し、厳しく管理すること。また、事業者は、クラウドサービス内で利用される全てのユーティリティプログラムのための要求事項を特定すること。	基本	当社ISMSに基づき、実施しています。また、KOTサービス内で利用できるユーティリプログラムはありません。
A.9.4.5	**Ⅱ．４．４．４．**	**プログラムソースコードへのアクセス**	プログラムソースコードへのアクセスは、制限すること。	基本	当社ISMSに基づき、制限しています。
	Ⅱ．４．４．５．	**アクセス制御となりすまし対策**	利用者及びシステム管理者等のアクセスを管理するために、適切な認証方法、特定の場所や装置からの接続を認証する方法等によって、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法とパスワードの有効期限を規定に含めること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．４．５．構成管理				
	Ⅱ．４．５．１．	**構成管理のポリシーと手順**	目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンス を取り扱う構成管理ポリシー及び構成管理ポリシーと関連する対応策の実施手順を策定・文書化すること。	基本	当社ISMSに基づき、文書化しています。
	Ⅱ．４．５．２．	**ベースライン構成**	システムの最新のベースライン構成、システムコンポーネント一覧を把握・文書化すること。	推奨	当社ISMSに基づき、文書化しています。
	Ⅱ．４．５．３．	**構成変更管理**	構成管理の対象となるシステムに対する変更について定めるとともに、変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可すること。また、変更に関する関連の活動を監査し、レビューすること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．４．５．４．	**変更に対するアクセス制限**	システムに対する変更に関して、物理的／論理的なアクセス制限を定義・文書化・承認のうえ実施すること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．４．５．５．	**設定項目**	運用上の要求事項に適合し、最も制限された運用を実現するためのセキュリティ設定に関するチェックリストを使用して、システムに導入されている製品の設定項目を把握し文書化すること。	推奨	当社ISMSに基づき、文書化しています。
	Ⅱ．４．５．６．	**ソフトウェアの使用制限**	契約上の取り決めと著作権法に従ってソフトウェアと関連ドキュメントを使用するとともに、ライセンスの数によって保護されるソフトウェアと関連ドキュメントの使用をモニタリングし、それらが複製されないようにすること	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．４．５．７．	**クラウドサービス利用者によるソフトウェアのインストール**	利用者によるソフトウェアのインストールを管理するためのポリシーを確立するとともにポリシーが遵守されていることをモニタリングすること。	推奨	KOTサービス内でソフトウェアのインストールはできません。
	Ⅱ．４．５．８．	**情報の場所**	情報の場所と、情報が処理及び保存されるシステムコンポーネントを特定して文書化すること。また、個人を特定できる情報がどのように処理されているかについて文書化すること。	推奨	当社ISMSに基づき、文書化しています。
A.7	**Ⅱ．５．従業員に係る情報セキュリティ**				

クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

A.7.1	Ⅱ．５．１．雇用前				
A.7.1.1	Ⅱ．５．１．１．	雇用契約	雇用予定の従業員(就業形態に関わらず)に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。	基本	当社ISMSに基づき、実施しています。
A.7.2	Ⅱ．５．２．雇用期間中				
	Ⅱ．５．２．１．	教育・訓練	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．５．２．２．	教育のフィードバック	組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．５．２．３．	契約違反	従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えること。	基本	当社ISMSに基づき、実施しています。
A.7.3	Ⅱ．５．３．雇用の終了又は変更				
	Ⅱ．５．３．１．	アクセス権・資産の取扱い	従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。	基本	当社ISMSに基づき、実施しています。
A.16	Ⅱ．６．情報セキュリティインシデントの管理				
A.16.1	Ⅱ．６．１．情報セキュリティインシデント及びぜい弱性の報告				
	Ⅱ．６．１．１．	組織内報告	全ての従業員に対し、業務において発見あるいは疑いをもったシステムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求すること。報告を受けた後に、迅速に効果的な対応ができるよう、責任体制及び手順を確立すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．６．１．２．	クラウドサービス事業者とクラウドサービス利用者間の報告	事業者は、利用者が情報セキュリティ事象を事業者に報告する仕組み、事業者が情報セキュリティ事象を利用者に報告する仕組み及び利用者が報告を受けた情報セキュリティ事象の状況を追跡する仕組みを提供すること。	基本	お客様の個人情報について、漏洩、滅失、毀損が発生した場合、速やかにその時点で把握している事項を速報としてメールおよび当社HPで通知します。 また、調査終了後、速やかに調査結果を確報としてメールおよび当社HPで報告します。
	Ⅱ．６．１．３．	インシデントの評価と分類	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．６．１．４．	フィードバック	情報セキュリティインシデントの分析及び解決から得られた知識は、情報セキュリティインシデントが将来起こる可能性又はその影響を低減するために用いること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．６．１．５．	証拠の収集・取得	証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．７．コンプライアンス				
	Ⅱ．７．１．法令と規則の遵守				
	Ⅱ．７．１．１．	関連法規と記録	個人情報、要配慮個人情報、プライバシー情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。また、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）について、法令、契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理するとともに、利用者から求められたときには提供すること。	基本	当社ISMSに基づき、実施しています。また、法令に基づいた要求を受けた際には、提供しています。
	Ⅱ．７．１．２．	利用可否	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のためにシステム及び情報処理施設を利用させないこと。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．７．１．３．	ソフトウェア製品	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施すること。	基本	当社ISMSに基づき、実施しています。

	Ⅱ．7．1．4．	不正アクセス・流出からの保護	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護すること。また、事業者は、利用者によるクラウドサービスの利用に関連して、事業者が収集し、保存する記録の保護に関する情報を、利用者に提供すること。	基本	当社ISMSに基づき、実施しています。また、利用者に関する情報の開示要求を受けた際には、提供しています。
	Ⅱ．7．1．5．	暗号化	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いるとともに、利用者が法令及び規制の順守をレビューできるようにするために、事業者は実施している暗号による対応策を記載すること。	基本	利用者から情報の開示要求を受けた際には、提供しています。
	Ⅱ．8．ユーザサポートの責任				
	Ⅱ．8．1．利用者への責任				
	Ⅱ．8．1．1．	責任	クラウドサービスの提供に支障が生じた場合には、その原因がサプライチェーンの事業者に起因するものであったとしても、利用者と直接契約を結ぶ事業者が、その責任において一元的にユーザサポートを実施すること。	基本	「KING OF TIME」使用規約　第５条に基づき、実施しています。
	Ⅱ．8．1．2．	SLA	事業者自身の責任範囲を SLA 等により文書化し、クラウド利用者に明確に示すこと。	基本	SLAを公開しています。 https://www.kingoftime.jp/faq/sla
	Ⅱ．8．1．3．	情報提供	クラウドサービスの新規利用/変更を計画しているクラウド利用者への情報提供にあたっては、組織のガバナンス規定を順守した上で、クラウド利用者が、必要な統制機能及び能力を有しているクラウドサービス及びこれを提供する事業者を選定できるようにすること。	基本	無償トライアル期間で一定期間ご利用のうえで、ご検討いただいています。
	Ⅱ．8．1．4．	クラウドサービス利用者からの苦情対応	提供しているクラウドサービスに対し、利用者からの苦情、懸念又は質問を受け取り、対応するためのプロセスを構築すること。	基本	ユーザーサポートの窓口を用意しています。
	Ⅱ．8．2．保守				
	Ⅱ．8．2．1．	システム保守ポリシーと手順	システム保守の目的、適用範囲、役割、責任、経営コミットメント、組織間の調整及び保守ポリシーを策定、文書化し、関係する組織に配布すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．2．	保守管理	保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録をレビューすること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．3．	保守ツール	システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューすること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．4．	リモート保守	リモート保守及び診断を承認のうえモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可すること。また、リモート保守及び診断のためのセッションを確立する際には、厳格な認証機能を使用するのに加え、リモート保守及び診断の記録を保管すること。リモート保守が完了したら、セッションとネットワーク接続を終了すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．5．	保守要員	保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．6．	保守要員による保守	保守要員が付添いなしで保守を行う場合、その要員が必要なアクセス権限を有することを確認すること。また、必要なアクセス権限を持たない要員による保守活動を監督するために、必要なアクセス権限と技術的能力を有する職員を指定すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．8．2．7．	タイムリーな保守	システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行うこと。	基本	当社ISMSに基づき、実施しています。
A.17	Ⅱ．9．事業継続マネジメントにおける情報セキュリティ				
A.17.1	Ⅱ．9．1．情報セキュリティの継続				
A.17.1.2	Ⅱ．9．1．1．	情報セキュリティ継続計画の策定と実施	組織は、大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持すること。	基本	当社ISMSに基づき、実施しています。
A.17.1.3	Ⅱ．9．1．2．	情報セキュリティ継続の検証、レビュー及び評価	情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、組織は、定められた間隔でこれらの対策を検証すること。	基本	当社ISMSに基づき、検証しています。
	Ⅱ．9．2．緊急時対応計画				

	Ⅱ．９．２．１．	緊急時対応計画の策定と手順	目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．９．２．２．	緊急時対応トレーニング	利用者に対して、役割と責任に応じた緊急時対応トレーニングを実施すること。	推奨	利用者に対する緊急時対応トレーニングは実施しておりません。
	Ⅱ．９．２．３．	緊急時対応計画のテスト	緊急時対応計画の有効性を判断して計画の欠陥を特定するために、緊急時対応計画のテストを実施すること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．９．２．４．	代替処理サイト	利用者とシステムバックアップ情報の保存と取得を許可するための契約を締結するとともに、代替処理サイトを確立すること。また、代替処理サイトがプライマリサイトと同等の管理機能を提供することを確認すること。	推奨	代替用サイト（DRサイト）を利用しています。
	Ⅱ．９．２．５．	代替処理サイトで再開	代替処理サイトを定め、利用者と合意した目標復旧時間内に、システムオペレーションを移転・再開して、極めて重要なミッション／業務機能を遂行できるようにすること。	推奨	代替用サイト（DRサイト）の要件に基づき、利用しています。
	Ⅱ．９．２．６．	通信サービス	一次処理サイトや代替処理サイトのいずれかにおいて一次通信サービスが利用できない場合に、極めて重要なミッションや業務機能を支援する代替通信サービスを確立すること。	推奨	ネットワークインフラ環境が利用できない状況でのKOTサービスは提供していません。
	Ⅱ．９．２．７．	システムの復旧と再構成	システムの途絶、侵害、又は不具合が発生した場合に、システムを従前の状態に復旧し、再構成できるようにすること。	推奨	当社ISMSに基づき、実施しています。
	Ⅱ．９．２．８．	代替通信プロトコル	利用者が、業務の継続性を維持するために組織が定めた代替通信プロトコルを使用できるようにすること。	推奨	代替通信プロトコルの利用は想定していません。
	Ⅱ．９．２．９．	代替のセキュリティ対策	組織が定めたセキュリティ機能を実施するための主な手段が利用できない場合、又は侵害された場合に、それらのセキュリティ機能を満たすための代替の、又は補助的なセキュリティ対策を実装すること。	推奨	対策の代替手段は想定していません。
A.10	Ⅱ．１０．その他				
A.10.1	Ⅱ．１０．１．暗号と認証				
A.10.1.1	Ⅱ．１０．１．１．	方針	情報を保護するための暗号利用に関する方針を、策定し、実施すること。	基本	当社ISMSに基づき、実施しています。
	Ⅱ．１０．１．２．	情報提供	事業者は、利用者に、事業者が処理する情報を保護するために、暗号を利用する環境に関する情報を提供すること。また、事業者は、利用者自らの暗号による保護を適用することを支援するために、事業者が提供する能力についても利用者に情報を提供すること。	基本	暗号を利用する環境に関する情報は、当社ISMSに基づいた範囲で、利用者から情報の開示要求を受けた際に提供しています。
A.10.1.2	Ⅱ．１０．１．３．	暗号鍵の作成と管理	組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄すること。	基本	当社ISMSに基づき、実施しています。
A.6.1.5	Ⅱ．１０．２．開発プロセスにおけるセキュリティ				
A.6.1.5	Ⅱ．１０．２．１．	開発プロセスにおける情報セキュリティへの取組	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。	基本	当社ISMSに基づき、実施しています。
A.12	Ⅲ．１．運用における情報セキュリティ【SaaS】				
A.12.1	Ⅲ．１．１．運用管理				
	Ⅲ．１．１．１．	情報セキュリティ監視手順の策定	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。また、クラウドサービスの提供に用いるアプリケーションの運用・管理に関する手順書を作成すること。	基本	当社ISMSに基づき、定めています。
	Ⅲ．１．１．２．	運用管理端末	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。 従業員等が用いる運用管理端末の全ファイルのウイルスチェックを行うこと。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．１．１．３．	稼働・障害監視	クラウドサービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行うこと。稼働停止や異常を検知した場合は、クラウドサービス利用者に速報すること。また、結果を評価・総括して、管理責任者に報告すること。	基本	当社ISMSに基づき、実施しています。また、利用者に影響のある事象および対応については、情報提供をしています。
	Ⅲ．１．１．４．	追加報告	クラウドサービスの提供に用いるアプリケーションに係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告をクラウドサービス利用者に対して行うこと。	基本	当社ISMSに基づき、実施しています。また、利用者に影響のある事象および対応については、情報提供をしています。

クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

Ⅲ．1．1．5．	定期報告	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結果、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。	基本	KOTサービス内のステータスサイトにて、サービス提供におけるステータス情報を公開しています。
Ⅲ．1．1．6．	時刻同期	クラウドサービスの提供に用いるアプリケーションの時刻同期の方法を規定し、実施すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．7．	パスワード管理	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にすること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．8．	クラウドサービスの変更管理	情報セキュリティに影響を与える組織、業務プロセス及びシステムの変更を管理すること。また、事業者は、クラウドサービスに影響を与える可能性のあるクラウドサービスの変更について、利用者に情報を提供すること。	基本	当社ISMSに基づき、実施しています。また、利用者に影響のある変更については、情報提供をしています。
Ⅲ．1．1．9．	リソース監視	要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測すること。また、事業者は、資源不足による情報セキュリティインシデントの発生を防ぐため、資源全体の容量・能力を監視すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．10．	環境分離	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために分離すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．11．	マルウェア対策	マルウェアから保護するために、検出、予防及び回復のための対策を実施すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．12．	イベントログの取得	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューすること。また、事業者は、利用者に、ログ取得機能を提供すること。	基本	当社ISMSに基づき、実施しています。また、管理画面にて、ログイン履歴および従業員情報の編集履歴を確認することができます。
Ⅲ．1．1．13．	ログの保護	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護すること。	基本	当社ISMSに基づき、保護しています。
Ⅲ．1．1．14．	作業記録	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューすること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．15．	ソフトウェア導入	運用システムに関わるソフトウェアの導入を管理するための手順を実施すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．1．16．	技術的ぜい弱性	利用中のシステムの技術的ぜい弱性に関する情報は、時機を失せずに獲得すること。.また、そのようなぜい弱性に組織がさらされている状況を評価すること。さらに、それらと関連するリスクに対処するために、適切な手段をとること。また、事業者は、提供するクラウドサービスに影響し得る技術的ぜい弱性の管理に関する情報を利用者が利用できるようにすること。	基本	当社ISMSに基づき、実施しています。また、利用者に影響のある脆弱性情報については、情報提供をしています。
Ⅲ．1．2．システム及び情報の完全性				
Ⅲ．1．2．1．	原本性確保	電子データの原本性確保を行うこと。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．2．2．	メモリ保護	許可されていない不正なコード実行からシステムメモリを保護するために、セキュリティ対策を実施すること。	推奨	当社ISMSに基づき、実施しています。
Ⅲ．1．2．3．	セキュリティ侵害の検知	システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知すること。	基本	当社ISMSに基づき、検知しています。
Ⅲ．1．2．4．	情報の更新	不要になった情報は削除すること。	推奨	当社ISMSに基づき、削除しています。
Ⅲ．1．2．5．	代替情報源	主要な情報源が破損しているか利用できない場合、システム又はシステムコンポーネントが重要な機能又はサービスを実行するための代替情報源を使用すること。	推奨	データの冗長化をしています。
Ⅲ．1．2．6．	情報の断片化	一度システムに侵入されると、失われた情報を回復する方法は、通常は存在しない。組織は、情報を異なる要素に分割し、それらの要素を複数のシステム又はシステムコンポーネントと場所に分散すること。	推奨	当社ISMSに基づき、実施しています。
Ⅲ．1．3．媒体の保管と廃棄				
Ⅲ．1．3．1．	媒体保管	紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．3．2．	廃棄	機器及び媒体を正式な手順に基づいて廃棄すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．1．3．3．	輸送	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護すること。	基本	当社ISMSに基づき、実施しています。
Ⅲ．2．アプリケーション				

	Ⅲ．２．１．アプリケーションの情報セキュリティ対策				
	Ⅲ．２．１．１．	**ウイルス対策**	クラウドサービスの提供に用いるアプリケーション（データ・プログラム等）についてウイルス等に対する対策を講じること。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．２．１．２．	**公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮**	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護すること。	基本	当社ISMSに基づき、保護しています。
	Ⅲ．２．１．３．	**アプリケーションサービスのトランザクションの保護**	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、 保護すること。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生	基本	当社ISMSに基づき、保護しています。
	Ⅲ．２．１．４．	**プラットフォーム変更後のアプリケーションの技術的レビュー**	プラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験すること。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．２．１．５．	**パッケージソフトウェアの変更に対する制限**	パッケージソフトウェアの変更は、必要な変更だけに限ることが望ましい。また、全ての変更を厳重に管理すること。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．２．２．データの保護				
	Ⅲ．２．２．１．	**バックアップ**	利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを実施すること。	基本	当社ISMSに基づき、実施しています。 また、バックアップについては、SLAに記載しております。 https://www.kingoftime.jp/faq/sla
	Ⅲ．２．２．２．	**バックアップ情報の完全性**	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．２．３．セッション管理				
	Ⅲ．２．３．１．	**セッションのライフサイクル管理**	セッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行うこと。	基本	当社ISMSに基づき、実施しています。
	Ⅲ．２．３．２．	**セッションの真正性**	通信セッションの真正性を保護すること。	基本	当社ISMSに基づき、保護しています。
	Ⅲ．２．３．３．	**同時セッションの制御**	同時処理されるアカウントの割り当て数、又はアカウントタイプの割り当て数は、システムが定めた各セッションの割り当て数まで制限すること。	基本	制御しておりません。
	Ⅲ．２．３．４．	**セッションのロック**	定められたアイドル時間を経過した場合、又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断すること。	基本	30分無操作で当該セッションが切断されます。