

SkymatiX

クラウドセキュリティホワイトペーパー

2023年8月7日(1.3版)

株式会社スカイマティクス

目次

1. はじめに	4
1.1. 本書の目的	4
1.2. 適用範囲	4
2. セキュリティ方針	5
2.1. 情報セキュリティ方針	5
2.2. 責任分界点	6
2.3. ICTサプライチェーン	6
2.4. 個人情報保護	6
3. 利用者へのセキュリティ機能の提供	7
3.1. 情報資産の管理	7
3.1.1. 情報資産のラベル付け	7
3.2. アクセス制御	7
3.2.1. 利用者登録及び登録削除	7
3.2.2. アカウント管理及びアクセス権の管理	7
4. 利用者へのセキュリティ情報の提供	9
4.1. 当社の開発や運用における共通方針	9
4.1.1. 技術的脆弱性の管理	9
4.1.2. 特権的なユーティリティプログラムの使用	9
4.1.3. クロックの同期	9
4.2. 当社の開発方針	9
4.2.1. 通信の暗号化	9
4.2.2. データの暗号化	9
4.2.3. ネットワーク及び仮想コンピューティング環境における分離	10
4.2.4. 仮想マシンの要塞化	10
4.2.5. 情報のバックアップ	10
4.3. 当社の運用方針	10
4.3.1. アプリケーションのサービスレベル	10
4.3.2. 変更管理	11
4.3.3. ネットワークセキュリティ管理の整合	11
4.3.4. 情報機器の処分または再利用	11
4.3.5. クラウドサービスカスタマの資産の除去	11
4.3.6. 容量・能力の提供	11
4.3.7. 障害対応と復旧までの目標時間	12
4.4. 情報セキュリティインシデントの取り扱い	12
4.4.1. 報告するインシデントの範囲	12
4.4.2. インシデントの通知手順と通知までの目標時間	12
4.5. コンプライアンス	12
4.5.1. 所在地及び利用者データの保存場所	12

4.5.2. 適用法令	12
4.5.3. 証拠の収集	13
4.5.4. 記録の保護	13
4.5.5. 情報セキュリティの独立したレビュー	13
5. 改訂履歴	14

1. はじめに

1.1. 本書の目的

本書は、株式会社スカイマティクス(以下、当社と呼びます)のクラウド製品の利用を検討されている方、または、既にご利用頂いている方に向けて、当社クラウド製品のセキュリティへの取り組みをご確認いただくとともに、当社クラウド製品を安全にご利用いただくための留意事項をご確認いただくことを目的としています。

1.2. 適用範囲

本書の適用範囲となる製品は以下の通りです。

- KUMIKI

2. セキュリティ方針

2.1. 情報セキュリティ方針

当社は情報セキュリティ方針を定め、クラウドサービスカスタマが安心して当社のクラウド製品をご利用いただけるように取り組んでおります。

また、この情報セキュリティ方針及び関連する社内規則等は、毎年のISMS活動の中で、年に1回、見直しております。

情報セキュリティ方針

倫理・法を厳格に遵守する独立した企業の社会的責任のひとつとして、また社会から深く信頼される企業となるため、当社は情報セキュリティを重視してまいります。そのため、以下の事項を確実に実行してゆく決意をここに表明するものです。

1. 当社は情報セキュリティポリシーを策定し、それを基盤に社会的に高度と認められる水準以上の情報セキュリティマネジメントシステムを確立し、その運用、徹底、及びその有効性の継続的改善に、積極性をもって取り組みます。
2. 当社は情報セキュリティを具体的に確保するために、情報セキュリティ責任者及び情報セキュリティ委員会を設置し、情報セキュリティ確保のための社内の組織体制を構築・運営していきます。
3. 情報セキュリティ維持への参画は全社員の基本的責任であるものとし、その方針を全社員に徹底し、その理解・協力のもと、具体的に実行してゆくための啓発活動と教育を積極的に実施していきます。また、情報セキュリティポリシーの不遵守行動に対しては、組織として厳格な態度と、然るべき罰則をもって臨みます。
4. 情報セキュリティマネジメントシステムの基盤として、当社は別途定めるように情報を区分し、自社情報資産はもとより顧客情報資産や個人情報、社員の個人情報等をも含め、その重要性に従った適正な管理を行います。
5. 情報セキュリティポリシーの遵守及び情報セキュリティマネジメントシステムの継続的改善のため、定期的なマネジメントレビューの一環として情報セキュリティポリシーの認識度、運用状況の確認を含む情報セキュリティマネジメントシステムのレビューを継続して実施していきます。

2.2. 責任分界点

当社は、利用者と当社の情報セキュリティの責任範囲について下記のとおり定義しております。

区分

責任範囲

利用者の責任	<ul style="list-style-type: none"> ● ユーザー管理のデータ <ul style="list-style-type: none"> ○ ログインID及びパスワード ○ 当社サービスにアップロードするデータ ○ 当社サービスからダウンロードしたデータ ● サービスの設定内容 ● インターネット環境 ● ユーザー端末
当社の責任	<ul style="list-style-type: none"> ● Webアプリケーション ● スマホ向けアプリケーション ● 保存データ(顧客情報、設定情報、各種ログデータ) ● クラウドサービスプラットフォーム/OS/ミドルウェア

2.3. ICTサプライチェーン

当社は、クラウドサービスプラットフォーム(Aamazon Web Services)を利用して環境を構築しています。

また、当社の開発業務の委託先については、契約の定めにしたがって管理を行っており、当社と同等の情報セキュリティ水準を要求するように定めています。

2.4. 個人情報保護

当社は、プライバシーポリシー及び利用約款に記載の通り、個人情報を保護しております。

<https://skymatix.co.jp/privacy/>

3. 利用者へのセキュリティ機能の提供

3.1. 情報資産の管理

3.1.1. 情報資産のラベル付け

当社は、利用者が情報を分類し、ラベル付けをするための機能を提供しております。具体的な操作手順はマニュアルをご覧ください。

3.2. アクセス制御

3.2.1. 利用者登録及び登録削除

契約管理者のアカウントは当社が発行します。

当社は、契約管理者がユーザーアカウントを登録および削除する機能を提供しております。具体的な操作手順はマニュアルをご覧ください。

3.2.2. アカウント管理及びアクセス権の管理

当社はアカウントのアクセス保護のための仕組みとしてIDとパスワードによる認証を提供しています。KUMIKIのパスワードポリシーは半角英数字をそれぞれ含む6文字以上となっています。

また、多要素認証の提供を希望されるお客様については、別途有償で提供致します。

なお、標準サービスとしては利用者側のアクセス制御機能は提供しておりません。IPアドレスや証明書などによるアクセス制御の導入をご要望される場合は、サービス窓口まで個別にご相談下さい。

アクセス権の管理利用者は、以下の権限管理機能により、アカウントのアクセス制御を実施頂けます。

製品	権限
KUMIKI	<ul style="list-style-type: none">● 契約管理者 全ての閲覧・操作が可能 契約に関する事項の手続きが可能● 管理者 指定されたフォルダ・プロジェクトにおいて、全ての閲覧・操作が可能● 一般ユーザー 指定されたフォルダ・プロジェクトにおいて、全ての閲覧及び指定された操作が可能● ゲスト

	<p>指定されたフォルダ・プロジェクトにおいて、閲覧のみ可能</p> <ul style="list-style-type: none"> ● ドローンオペレータ 指定されたフォルダ・プロジェクトの閲覧と指定されたフォルダ内でのプロジェクト作成が可能
--	--

3.3. 運用

3.3.1. アクセスログ取得

当社は、利用者のアカウントに対して、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどのアクセスログを取得していますが、閲覧する機能は提供していません。アクセスログの提供を希望されるお客様については、別途有償で提供致します。アクセスログの提供をご希望される場合は、サービス窓口にお知らせ下さい。

なお、アクセスログの保存期間は90日となります。

3.3.2. 操作ログ取得

当社は、利用者のアカウントに対して、アプリケーションの操作ログを取得していますが、閲覧する機能は提供していません。操作ログの提供を希望されるお客様については、別途有償で提供致します。操作ログの提供をご希望される場合は、サービス窓口にお知らせ下さい。

なお、操作ログの保存期間は90日となります。

3.3.3. 利用状況の確認

当社は、ログイン回数・プロジェクト総数・アップロード回数・ファイル総数・ダウンロード回数などクラウドサービスの利用状況を確認するためのダッシュボード機能を提供しております。

4. 利用者へのセキュリティ情報の提供

4.1. 当社の開発や運用における共通方針

4.1.1. 技術的脆弱性の管理

当社は、クラウド製品を開発、運用する際に、当社のセキュリティポリシーに従って定期的に脆弱性評価(プラットフォーム診断)を実施しています。

また、脆弱性情報を収集するとともに、脆弱性対策を実施しています。

4.1.2. 特権的なユーティリティプログラムの使用

当社は、製品の開発や運用において、特権的ユーティリティプログラム及び特権的ユーティリティプログラムを利用する従業員を制限し、定期的にレビューしています。

また、当社製品の利用者には、当社製品の特権的なユーティリティプログラムは提供しておりません。

4.1.3. クロックの同期

当社が提供するクラウドサービス内で提供する時刻情報は、タイムゾーンJST(UTC+9)で取得されます。ログの時間は、クラウドサービスプラットフォーム(AWS)が提供するNTPサービスに同期されています。

4.2. 当社の開発方針

当社は、社内で定めた開発規定にしたがってクラウド製品を開発しています。この規定に従い、開発時にはソースコードレビューを実施し、レビューを実施したソースコードしか本番環境に反映できない仕組みとすることで、開発したソースコードが開発規定に従っていることを確認しています。

また開発規定はセキュリティ上の注意点も含んでおり、必要に応じてクラウドサービスプラットフォーム(AWS)が提供する脆弱性診断ツールなどを用いて、脆弱性を診断することで、安全性を確認しています。

4.2.1. 通信の暗号化

当社は、通信内容を暗号化することで、データ漏洩や改ざんを防止しています。利用者の端末と、クラウドサービスプラットフォーム間のインターネット通信をHTTPS(TLS1.2)により暗号化しています。

4.2.2. データの暗号化

当社は、利用者データをサーバー上に保存する際も暗号化を行い、データ漏洩や内部不正による持ち出しを防止しています。当社のセキュリティポリシーにしたがって、データベース及びクラウドストレージに保存されるデータを暗号化しています。

4.2.3. ネットワーク及び仮想コンピューティング環境における分離

当社は、利用者が別の利用者のデータを閲覧することができないよう、また当社の従業員が利用者のデータを必要以上に閲覧することができないように、適切に分離しております。

4.2.4. 仮想マシンの要塞化

当社は、クラウドサービスの提供に必要なポート、プロトコル及びサービスのみを提供しております。

また、アンチウイルスソフトによりウイルス対策を実施するとともに、WAF・DDoS保護サービスにより不正アクセスを含むサイバー攻撃対策を実施しています。

4.2.5. 情報のバックアップ

当社は、以下に従い利用者データのバックアップを取得しております。

なお、バックアップデータからの復旧機能はユーザーに提供しておらず、当社がクラウドサービスを運用する中で必要と判断した場合にのみ、バックアップデータから復元を実施します。

製品	バックアップ方針
KUMIKI	<ul style="list-style-type: none">● データベース<ul style="list-style-type: none">○ バックアップサイクル: 1日1回○ 保管期間: 7日間○ バックアップデータ保管場所: 日本国内

4.3. 当社の運用方針

4.3.1. アプリケーションのサービスレベル

当社は、クラウドサービスのサービスレベルとして以下の指標として定めています。

項目	設定
サービス時間	<ul style="list-style-type: none">● Web上で提供するサービス: 24時間365日● サポートサービス: 9:00~17:30(土日祝日、年末年始、当社所定の休暇を除く)
計画停止	メンテナンスやバージョンアップ等の為、計画停止を行います。計画停止は年間60時間以内とし、可能な限り夜間に行います。但し、合理的な理由から早朝、日中帯で行う可能性もございます。
計画停止予告案内	5営業日前までに電子メール、書面、本サービス内のお知らせ又は当社のホームページに掲示し、案内致します。
緊急停止	セキュリティ危殆化等のやむを得ない場合は計画停止とは別途の緊急停止がありえます。また、当社は合理的な努力をもって管理を行い欠陥や障害に備えますが、本サービス用設備に

	やむを得ない故障や欠陥が認められた場合、サービスを停止する場合がございます。
サービス稼働率	99.0%以上 ※上述の計画停止時間を含みます。
アップデート	アップデートは都度当社が必要と判断した場合、実施します。また、ネットワーク環境によってアップデートに時間を要する場合があります。

4.3.2. 変更管理

機能の変更や廃止、一時的なメンテナンスなど、利用者に影響を与える可能性が生じる場合は、メールやクラウドサービス内の通知機能により利用者に通知します。

4.3.3. ネットワークセキュリティ管理の整合

物理ネットワークと仮想ネットワークの間で整合がとれなくなるような変更作業が行えないように、ネットワークセキュリティを管理しています。

4.3.4. 情報機器の処分または再利用

当社は、利用していた情報機器を廃棄及び再利用する際は、当社と機器ベンダーの契約に基づき適切に処理を行っています。

4.3.5. クラウドサービスカスタマの資産の除去

契約管理者が当社のクラウドサービスを解約された場合、解約後はクラウドサービス上の各種データをダウンロードできなくなります。必要に応じて、解約前にダウンロードして下さい。

なお、当社は、利用者がサービスの利用を終了した場合、当社所定の期間を経過後、アップロードデータ、生成データを削除します。消去したデータはいかなる場合でも復旧することはできません。

4.3.6. 容量・能力の提供

当社は、サービス提供のために利用している各種リソースについて容量・負荷を常に監視し、必要に応じてリソースを増強します。

4.3.7. 障害対応と復旧までの目標時間

何らかの理由でクラウドサービスが停止した場合、当社は復旧計画に従ってサービスの普及を試みます。単一障害が発生した場合の目標復旧時間は1時間としています。複合障害が発生した場合の目標復旧時間は24時間としています。

4.4. 情報セキュリティインシデントの取り扱い

4.4.1. 報告するインシデントの範囲

情報インシデントのうち、利用者に明確な被害が及ぶ場合又はクラウドサービスの継続に影響を及ぼすと判断された場合を重大インシデントと定義して、利用者への報告対象とします。以下に示すようなものが重大インシデントに該当します。

- クラウドサービスへの不正アクセスにより、サーバーに保存された情報が外部に流出した。
- サーバーのウイルス感染により、サーバーに保存された情報が外部に流出した。
- 外部からの攻撃により、クラウドサービスが利用できない状態となり、その状態が一定時間以上継続した。
- なりすましサイトにより、クラウドサービスの利用者に被害が発生した。

4.4.2. インシデントの通知手順と通知までの目標時間

利用者に大きな影響を与える情報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、当社が情報セキュリティインシデントを発見してから1営業日以内を目標に、メールやクラウドサービス内の通知機能により利用者に通知します。

なお、情報セキュリティインシデントに関する問合せは、サービス窓口より受け付けています。

4.5. コンプライアンス

4.5.1. 所在地及び利用者データの保存場所

当社は、日本の法人であり、本店所在地は東京都です。クラウドサービスの開発、運営は全て日本国内で行っております。

クラウドサービスは、Amazon Web Services(AWS)を利用して構築しており、システムが保管するデータ及びそのバックアップデータは、AWSが管理する日本国内のデータセンターに保管されています。

4.5.2. 適用法令

当社と利用者との間の契約における適用法令は利用約款に記載の通り、日本国法を適用しています。

4.5.3. 証拠の収集

当社は、サービス内で収集されるデジタル証拠となりうるデータ(ログや利用者コンテンツなど)を第三者(警察や裁判所など)に提出する条件について利用約款に記載しています。

4.5.4. 記録の保護

利用者データは、不正なアクセスや改ざんを防ぐため、許可された従業員しかアクセスできない、適切に管理されたアクセス権のもとで保管されます。

4.5.5. 情報セキュリティの独立したレビュー

当社は、JIS Q27001 (ISO/IEC27001) 及び JIS 27017 (ISO/IEC27017) について第三者による審査を受け、それぞれの認証を取得しております。

5. 改訂履歴

版数	日付	主な変更内容
1.0	2022年10月26日	初版作成
1.1	2022年10月31日	2022年10月27日にISO27001及びISO27017の認証が取得できたことを踏まえて、「4.5.5 情報セキュリティの独立したレビュー」の記載内容を見直した。!
1.2	2023年5月23日	3.2.2 アクセス管理及びアクセス権の管理に関する情報を追記した。 4.2.4 仮想マシンの要塞化に関する情報を追加した。
1.3	2023年8月7日	3.2.2 アカウント管理及びアクセス権の管理に関する情報を更新した。

■お問い合わせ(ご購入前)

ご購入前のお客様からの、資料請求、お見積もり、ご購入、ご導入などについてのお問い合わせは下記にて承っております。

<https://skymatix.co.jp/contact/>

■お問い合わせ(ご購入後)

当社製品をご利用中のお客様からのお問い合わせは、サービス窓口から承っております。

製品	サービス窓口
KUMKI	kumiki-support@skymatix.co.jp