Mass

media assets on the cloud

Mass セキュリティ・ホワイトペーパー

ISO/IEC 27017

第 1.2 版

ビジュアル・グラフィックス株式会社

2025/10/08

1 本書の目的

当ホワイトペーパーは、ビジュアル・グラフィックス株式会社（以下「当社」）が提供するクラウドサービスである Mass（以下「本サービス」）に関する情報セキュリティへの取り組みを記載したものです。

記載内容については、クラウドサービスに関する情報セキュリティの国際規格である ISO/IEC 27017:2015 において、クラウドサービス事業者が、クラウドサービス利用者に対して、開示もしくは公開を求めている事項に基づき、構成されています。

なお、各項目の末尾に記載されているカッコ【】は、ISO/IEC 27017:2015 の該当する項番を表しています。

2 情報セキュリティの取り組み

2.1 情報セキュリティのための方針群【5.1.1】

本サービスは、当社の定めた情報セキュリティ基本方針（https://www.vgi.co.jp/about/privacy_policy.html）に従い、サービス運営を行います。この方針には、クラウドサービスに関する情報セキュリティの管理事項が含まれます。

2.2 情報セキュリティの役割及び責任（クラウドコンピューティング環境における役割及び責任の共有及び分担）【6.1.1】

本サービスでは、利用規約（https://www.mass-cloud.io/mass-terms-and-conditions/）にて契約やサービス内容を定義し、サービス提供を実施しております。お客様は、本サービスのアプリケーション内でのユーザー管理、アクセス権限設定、および入力されるデータの正確性・適切性について責任を負います。当社は、本サービスの基盤となるインフラストラクチャ、プラットフォーム、および本サービスのアプリケーション自体のセキュリティと可用性について責任を負います。これらについては、本サービスの利用開始時に利用規約として同意いただく事項となります。

また、サービスの利用契約が終了した場合、本サービス内に保管されているデータは、速やかに物理的に削除します。

2.3 関係当局との連絡【6.1.3】

サービス内のデータは、ピアクラウドサービスプロバイダの国内リージョンに保管しています。

2.4 クラウドコンピューティング環境における役割及び責任の責任分担【CLD.6.3.1】

本サービスは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供します。

保存されたデータ （ユーザー情報、コンテンツ、付加情報）	お客様の責任範囲
アプリケーション	ビジュアル・グラフィックスの責任範囲
ミドルウェア	
OS	
仮想ホスト	
仮想化層（ハイパーバイザー）	他事業者様の管理範囲
物理設備 （サーバー・ストレージ・ネットワーク）	
土地・建物	

2.5 情報セキュリティの意識向上、教育及び訓練【7.2.2】

本サービスでは、サービス運営担当者に対し、当社が定めたセキュリティ教育に加え、情報セキュリティ基本方針に定めた管理事項の運営に必要な教育を実施しています。

2.6 資産目録【8.1.1】

本サービスでは、お客様の情報資産（お客様が保存されるデータ）と、当社が本サービスを運営するための情報を、明確に分離しています。なお、お客様の情報資産（お客様が保存されるデータ）に関しては、お客様の管理範囲です。

2.7 クラウドサービスカスタマの資産の除去【CLD.8.1.5】

サービスの利用契約が終了した場合、サービス内に保管されているデータは、速やかに物理的に削除します。バックアップについても同様に削除します。

2.8 情報のラベル付け【8.2.2】

本サービスでは、BROWSE 機能内に以下の機能を提供し、ユーザー様のデータ分類をサポートします。

- 技術メタデータ
- ユーザメタデータ
- タグ

使用方法の詳細はサービス内のマニュアルサイト（https://visual-graphics-inc.slite.page/p/oVSC7soOsZSAg2/mass-cloud-io-on-the-cloud-platform-SaaS）をご参照ください。

2.9 利用者登録及び登録削除【9.2.1】

本サービスでは、テナント管理者、プロジェクト管理者、一般ユーザー、参照ユーザーといった標準権限に加え、お客様の必要に応じて独自の権限を定義し、利用者 ID の登録及び削除機能を提供しております。登録や削除の手順は、サービスドキュメントに記載しております。

2.10 利用者アクセスの提供【9.2.2】

本サービスの初期アカウントの発行は、申込書へ記載されたメールアドレスを ID としてテナント管理者を登録します。本サービスは、テナント管理者、プロジェクト管理者、一般ユーザー、参照ユーザー、およびお客様が定義したカスタム権限といった利用者ごとの権限設定によるアクセス制御機能について、利用者登録、変更の機能を提供しております。

2.11 特権的アクセス権の管理【9.2.3】

本サービスでは、二要素認証をはじめとした、お客様のセキュリティに配慮した認証技術を提供しています。

2.12 利用者の秘密認証情報の管理【9.2.4】

本サービスは、管理者 ID、利用者 ID の登録やパスワード変更、再発行方法につきましては、サービスドキュメントに記載しております。

2.13 情報へのアクセス制限【9.4.1】

本サービスは、テナント管理者、プロジェクト管理者、一般ユーザー、参照ユーザー、およびお客様が定義したカスタム権限といった各権限を有する利用者によって、機能制限を行うことができます。

2.14特権的なユーティリティプログラムの使用【9.4.4】

本サービスの運用に必要な内部ユーティリティプログラムを使用しています。これらのプログラムは、厳格な認証とアクセス制御の下で管理されており、セキュリティ手順を回避する機能は提供しておりません。ユーティリティプログラムのアクセス権限は定期的に点検しています。

2.15仮想コンピューティング環境における分離【CLD.9.5.1】

本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、コンピューティングリソースは共有リソース方式で提供されますが、ストレージはお客様ごとに論理的に分離しています。

2.16仮想マシンの要塞化 【CLD.9.5.2】

お客様が利用するサービスの提供に用いる仮想環境は、IP/プロトコル/ポートへのアクセス制限などを実施しています。

2.17暗号による管理策の利用方針 【10.1.1】

本サービスのご利用においてデータのやりとりする通信は、SSL/TLS による通信の暗号化を使用しています。

2.18装置のセキュリティを保った処分又は再利用 【11.2.7】

本サービスは、サービスの提供に関連する機材の故障などにより交換した記憶媒体の再利用、廃棄に際し、適切なプロセスでデータの削除や設備の破壊を行います。

2.19変更管理【12.1.2】

本サービスは、サービスの仕様変更について利用規約に定め、サービスを提供します。

2.20容量・能力の管理【12.1.3】

本サービスでは、安定的にサービスを提供するため、日々の稼働監視を実施しています。 監視・分析の結果、必要と判断された場合、適切なタイミングにてシステムメンテナンスを実施します。

2.21実務管理者の運用のセキュリティ【CLD.12.1.5】

本サービスでは、サービスの利用に必要な操作手順を、マニュアルなどのドキュメントとして提供しています。

2.22 情報のバックアップ【12.3.1】

本サービスでは、サービスの提供に用いるデータベースのバックアップを、日次で二世代を取得/保持しています。
必要に応じて、エンドユーザーによる Mass Desktop アプリを利用したバックアップの取得を可能としています。

2.23 イベントログ取得【12.4.1】

本サービスでは、サービスの維持管理に必要となる適切なログを取得しています。
また、管理権限を有している利用者へエンドユーザーのサービス利用に関わるログの確認機能を提供しています。

2.24 クロックの同期【12.4.4】

本サービスでは、サービス提供に必要なシステムのクロック同期を、Amazon Time Sync Service の技術を用いて実施しています。

2.25 クラウドサービスの監視【CLD.12.4.5】

本サービスでは、サービスの提供に必要なシステムおよびログの監視を行っています。また、エンドユーザーの利用できるサービスを確認する機能を提供しています。

2.26 技術的ぜい弱性の管理【12.6.1】

本サービスでは、ぜい弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、当社の責任範囲において影響が ある場合には、速やかに対応します。

2.27 ネットワークの分離【13.1.3】

本サービスのストレージでは、お客様ごとに論理的にネットワークを分離し、サービス運営で必要となる管理ネットワークに関しても、お客様のネットワークと分離しています。

2.28 仮想及び物理ネットワークのセキュリティ管理の整合【CLD.13.1.4】

本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、サーバーやネットワークは共有リソースとして提供されますが、ストレージはお客様ごとに論理的に分離されています。

2.29 情報セキュリティ要求事項の分析及び仕様化【14.1.1】

本サービスでは、お客様のストレージ利用状況に関する監視機能を提供しています。詳細はサービスドキュメントにおいて定義します。

2.30 セキュリティに配慮した開発のための方針【14.2.1】

本サービスは、IPA の開発ガイドラインに基づき、セキュリティに配慮した開発を行っています。開発を外部に委託する際は、業務委託契約においてセキュリティに関する合意を定め、これに基づき開発が行われます。また、第三者による定期的なセキュリティ診断を実施しています。

2.31 供給者との合意におけるセキュリティの取扱い【15.1.2】

本サービスは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供します。 本サービスの責任分界点については、「情報セキュリティの役割及び責任」をご確認ください。

2.32 ICT サプライチェーン【15.1.3】

本サービスでは、ピアクラウドサービスプロバイダに対して当社の情報セキュリティ方針を示し、それを達成するためのリスクマネジメント活動の実施を要求するよう定めています。

2.33 責任及び手順【16.1.1】

本サービスは、当社が確認したセキュリティインシデントがお客様に重大な影響を及ぼす場合、確認より 4 時間以内を目標にお客様管理者様へメールまたはサービス画面のメッセージ機能にて通知を行います。情報セキュリティインシデントに関するお問い合わせは、サポートセンターで承ります。

2.34 情報セキュリティ事象の報告【16.1.2】

情報セキュリティ事故が発生した場合には、メールなどにて速やかに報告いたします。また、お客様からの事象報告はお問い合わせ窓口にて受け付けております。

2.35 証拠の収集【16.1.7】

本サービスのご利用に関して、お客様責任範囲における情報セキュリティインシデントに関するログなどの証拠の収集はお客様にてご実施いただく範囲となります。弊社責任範囲でのログなどの証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。
また、法令に基づき権限を有する公的機関から適法な手続により、開示または提供の要請があった場合は、クラウドサービスカスタマへの通知および同意を経ることなく、当該機関に情報を開示することについて合意いただく必要があります。

2.36 適用法令及び契約上の要求事項の特定【18.1.1】

本サービスのご利用に関して、適用される準拠法は日本国の法令です。

2.37 知的財産権【18.1.2】

本サービスをご利用いただく上での知的財産権に関わるご相談は、当社までお問い合わせください。

2.38 記録の保護【18.1.3】

本サービスは、クラウドサービスカスタマの契約情報の保護や廃棄については、重要な記録の区分をするとともに、管理基準を定め、適切に管理しております。加えて、サービス運営のために取得するイベントログ、アクセスログ、および管理者操作ログなどの監査証跡は、重要な記録として扱い保護します。

2.39 暗号化機能に対する規制【18.1.5】

本サービスは SSL/TLS の暗号化を使用しております。なお、輸出規制の対象となる暗号化の利用はありません。

2.40 情報セキュリティの独立したレビュー【18.2.1】

当社は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受け、認証の取得状況を当社ウェブサイトで公開する。認証取得前にサービス利用が見込まれる潜在的なカスタマから審査状況の開示を求められた場合、求めに応じて監査結果を開示する。

3 更新履歴

版数	日付	更新内容
第 1.0 版	2025 年 7 月 8 日	初版発行
第 1.1 版	2025 年 9 月 26 日	項 2.22、2.40 更新
第 1.2 版	2025 年 10 月 8 日	項 2.30、2.38 更新