and.T®
JMC教育専用クラウド

情報セキュリティホワイトペーパー

Ver. 1.3

JMC

目次

このホワイトペーパーについて

このホワイトペーパー（以下、本書）は、株式会社 JMC（以下、当社）が提供するクラウドサービスにおける、セキュリティへの取り組みについて理解を深めていただくためのものです。クラウドセキュリティの国際規格 ISO/IEC 27017 の中で、特に利用者に向けて情報開示が求められる事項について、セキュリティの取り組みをご確認いただくことができます。

本書の適用範囲について

JMC 教育専用クラウドサービス and.T（以下、本サービス）が、本書の適用範囲です。

サービス概要

教育クラウド上のポータルサイトを中心とした、教育の情報化支援サービス。

and.T（アンドティ）は、教育の情報化をトータルで支援する「教育情報化基盤サービス」。教育クラウド上のポータルサイトをベースに、Web アプリケーションを安全に利用できる環境を提供します。

ISO/IEC 27017 について

ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、情報セキュリティ全般に関するマネジメントシステム規格 ISO/IEC 27001 の取り組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

クラウドサービスの管理策

本項では、ISO/IEC 27017 管理策の実践の規範の項番に沿って本サービスの管理策を記載します。
本サービスにおける ISO/IEC 27017 の定める管理項目への管理策は、以下のとおりです。

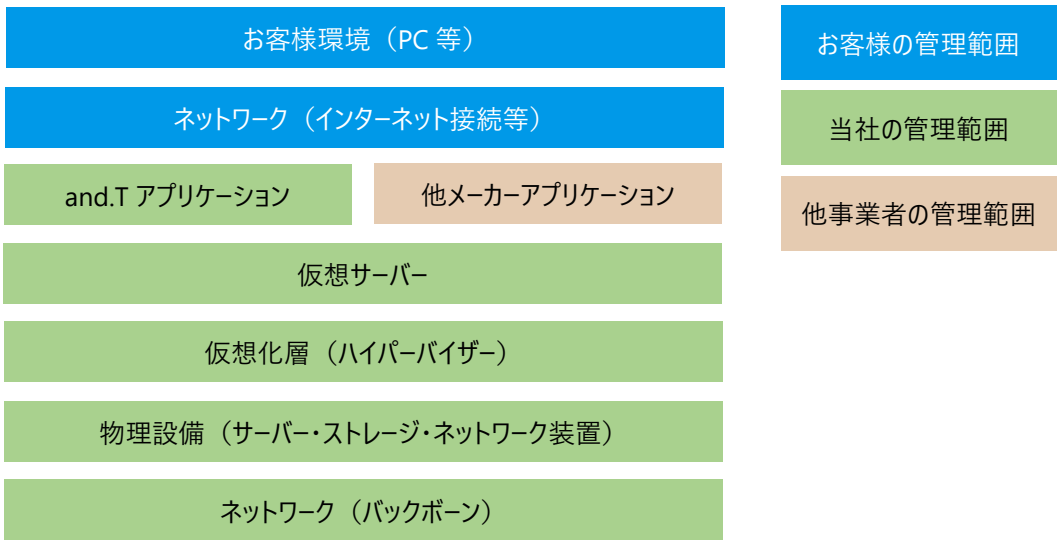
A.5.1.1 情報セキュリティのための方針群

・ 本サービスは、当社の定めた情報セキュリティ基本方針、並びにクラウドサービス情報セキュリティポリシーに従い、サービス運営を行います。『https://www.jmc.ne.jp/security/』

A.6.1.1 情報セキュリティの役割及び責任

・ 本サービスは、図 1 の管理範囲における情報セキュリティの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 （図 1）



A.6.1.3 関係当局との連絡

・ 当社の所在地は、当社ウェブサイトでご確認ください。 『https://www.jmc.ne.jp/』
・ 本サービスにて保存されるデータの所在は、日本国内のデータセンターです。

CLD.6.3.1 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

・ 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、「A.6.1.1 情報セキュリティの役割及び責任」をご確認ください。

A.7.2.2 情報セキュリティの意識向上、教育及び訓練

・ 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、クラウドサービス情報セキュリティポリシー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。

A.8.1.1 資産目録

・ 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。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

・ お客様の情報資産（お客様が保存されるデータ）は、ご利用終了後、利用規約の定める期間内に破棄します。
・ ただし、お客様の情報資産を含まない、ログ等の当社がサービスを運営するための情報は対象外とします。

A.8.2.2 情報のラベル付け

・ 本サービスでは、お客様ごとに個別の識別および利用サービスを分類しています。
・ ご契約のサービスごとに、お客様の情報資産（お客様が保存されるデータ）を分類しています。

A.9.1.2 ネットワーク及びネットワークサービスへのアクセス

・ 本サービスは、当社の定める経路以外からのアクセスの禁止について利用規約に定め、サービスを提供します。

A.9.2.1 利用者登録及び登録削除

・ 本サービスは、利用者の登録・変更、および利用者に対する機能・アクセス制限を、定められた登録依頼書・変更依頼書を用い、管理権限を有する利用者から申請された内容に基づき実施します。

A.9.2.2 利用者アクセスの提供

・ 本サービスは、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、及び仕様を当社の定める依頼書として定め、サービスを提供します。

A.9.2.3 特権的アクセス権の管理

・ 本サービスでは、専用 USB キーによる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。

A.9.2.4 利用者の秘密認証情報の管理

・ 本サービスは、お客様が利用できる認証機能について利用手順を製品マニュアルなどに定め、サービスを提供します。

A.9.4.1 情報へのアクセス制限

・ 本サービスは、管理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。

A.9.4.4 特権的なユーティリティプログラムの使用

・ 本サービスでは、サービスの利用において認証が必要です。
・ セキュリティ手順を回避し、各種サービス機能の利用を可能とするユーティリティプログラムは、提供していません。

CLD.9.5.1 仮想コンピューティング環境における分離

・ 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、ストレージをお客様ごとに論理的に分離しています。

CLD.9.5.2 仮想マシンの要塞化

・ 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。

A.10.1.1 暗号による管理策の利用方針

・本サービスのご利用において保存されるデータは、「AES-256-XTS」で暗号化され保管されます。
・お客様の利用するサイトでは SSL/TLS による通信の暗号化を使用しています。

A.11.2.7 装置のセキュリティを保った処分又は再利用

・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。

A.12.1.2 変更管理

・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。

A.12.1.3 容量・能力の管理

・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。

CLD.12.1.5 実務管理者の運用のセキュリティ

・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。

A.12.3.1 情報のバックアップ

・本サービスでは、サービスの提供に用いる仮想マシンのバックアップを、日次で 7 世代を取得/保持しています。

A.12.4.1 イベントログ取得

・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。

A.12.4.3 実務管理者及び運用担当者の作業ログ

・本サービスでは、サービスの提供に関わる作業及び結果を記録し、レビューを実施しています。

A.12.4.4 クロックの同期

・ 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、NTP などの技術を用いて実施しています。

CLD.12.4.5 クラウドサービスの監視

・ 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。

A.12.6.1 技術的ぜい弱性の管理

・ 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。

A.13.1.3 ネットワークの分離

・ 本サービスでは、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。

CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合

・ 本サービスでは、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。

A.14.1.1 情報セキュリティ要求事項の分析及び仕様化

以下、主なセキュリティ機能です。

・専用 USB キーでの認証によるチャレンジレスポンス認証
・アンチウイルス
・アンチスパム
・IDS/IPS（不正侵入防止システム）
・WAF（Web アプリケーションファイアウォール）

A.14.2.1 セキュリティに配慮した開発のための方針

・本サービスは、当社にて定めた規約に則ったセキュリティに配慮した開発を行っています。
・また、開発を外部に委託する際も、これに準じた契約のもと開発が行われます。

A.15.1.2 供給者との合意におけるセキュリティの取扱い

・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、「A.6.1.1 情報セキュリティの役割及び責任」をご確認ください。

A.15.1.3 ICT サプライチェーン

・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。

A.16.1.1 責任及び手順

・ 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 56 時間以内を目標にお客様管理者様へメール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問合せは、and.T サポートセンターでお受けいたします。

A.16.1.2 情報セキュリティ事象の報告

・ 本サービスでは、and.T サポートセンターへのお問い合わせで、相互に情報のやりとりができる仕組みを提供しています。

A.16.1.7 証拠の収集

・ 本サービスのご利用に関して、法令または裁判所の命令に基づき開示が義務付けられた情報は、利用者の同意なく開示することがあります。

A.18.1.1 適用法令及び契約上の要求事項の特定

・ 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。

A.18.1.2 知的財産権

・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。

A.18.1.3 記録の保護

・本サービスは、情報保護ポリシーについて利用規約に定め、サービスを提供します。

A.18.1.5 暗号化機能に対する規制

・輸出規制の対象となる暗号化の利用はありません。

A.18.2.1 情報セキュリティの独立したレビュー

・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しています。

改版履歴

・ Ver. 1.0 : 2020/12/22 初版作成
・ Ver. 1.1 : 2021/02/12 P5 「本サービスの責任分界点（図 1）」を修正
・ Ver. 1.2 : 2021/02/19 P10「責任及び手順」の条文を変更
・ Ver. 1.3 : 2021/07/28 P5 「情報セキュリティのための方針群」の掲載 URL を追加
P8 通信の暗号化情報（SSL/TLS）を A.18.1.5 から A.10.1.1 に移動