TICクラウドサービス
ISO/IEC 27017 ホワイトペーパー

株式会社鳥取県情報センター
TOTTORI PREFECTURE INFORMATION-CENTER

株式会社鳥取県情報センター

2020 年 3 月 31 日（第 1.1 版）

目次

1. はじめに

1.1 ホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、ISMS クラウドセキュリティ認証である、「JIP-ISMS517-1.0（ISO/IEC 27017:2015）」で求められている要求事項の中で、特に利用者に向けての情報開示が求められている事項について、TIC クラウドサービスにおけるセキュリティの取り組みを確認いただくことを目的としています。

また、TIC クラウドサービスを利用して、独自のクラウドサービスを展開されているご利用者様（以下、クラウドサービスカスタマ）において、『ISMS クラウドセキュリティ認証（JIP-ISMS517-1.0）』もしくは、『ISO/IEC 27017 の適合審査』の認証取得を検討されている場合に必要となる情報をご確認いただくことができます。

これらは、ISO/IEC 27017:2015 「箇条 4.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係」に定められている『クラウドサービスプロバイダは，クラウドサービスカスタマがその情報セキュリティ要求事項を満たすために必要な情報及び技術支援を提供することが望ましい。』への対応となります。

なお、TIC クラウドサービスは、常に進化を続けていますので、最新の情報については、弊社営業までご相談いただくか、弊社 Web サイトをご確認ください。

1.2 本書の適用範囲について

TIC クラウドサービスが本書の適用範囲となります。

1.3 本書で使用する用語について

本書は、JIP-ISMS517-1.0、ISO/IEC 27017:2015 および JIS Q 27017:2016 で記されている用語については、改変せずに使用しております。

2. ISMS クラウドセキュリティ認証について

2.1 ISO/IEC 27017:2015 とは

ISO/IEC 27017 とは、国際標準化機構（ISO）と国際電気標準会議（IEC）が定める、情報セキュリティマネジメントに関する国際規格である ISO/IEC 27000 シリーズの一つであり、クラウドサービスのための情報セキュリティ管理策の実践の規範をまとめた文書です。

ISO/IEC 27017:2015 は、ISMS（ISO/IEC 27001:2013）に関する情報セキュリティ管理策の実践の規範である ISO/IEC 27002:2013 をベースにクラウドに特化した管理策が記載された文書で、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指針が示されています。

また、日本規格協会、情報処理学会によって申出があり、JIS Q 27017:2016 として、JIS 化されています。

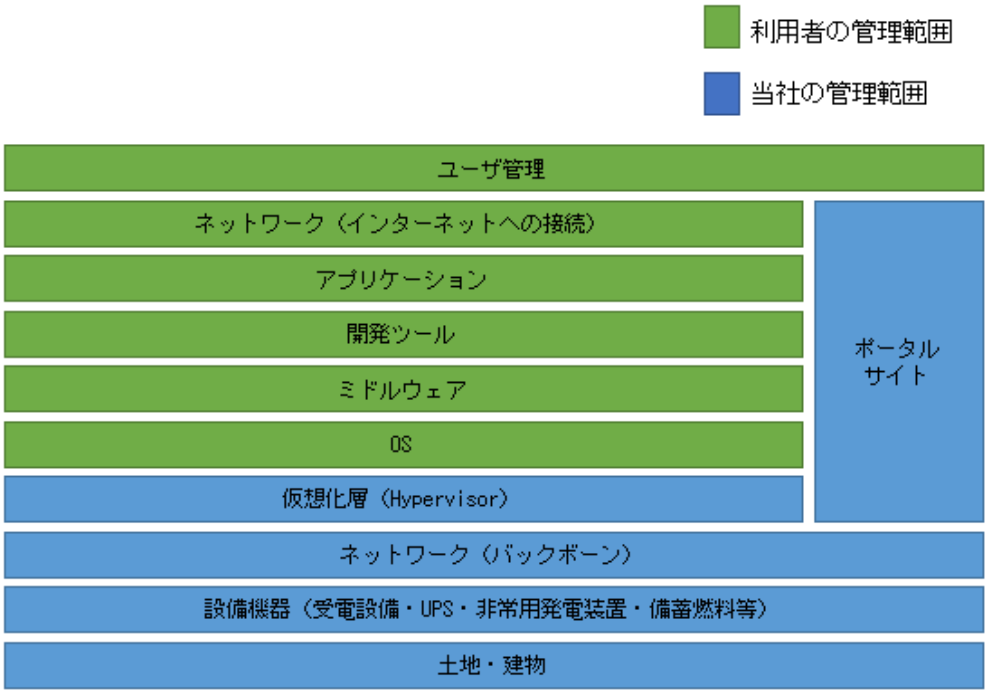
3. TIC クラウドサービスについて

3.1 TIC クラウドサービスについて

TIC クラウドサービスは、パブリッククラウドに分類される IaaS（Infrastructure as a Service）のサービスです。TIC クラウドサービスにはさまざまな機能が備わっていますが、TIC クラウドサービスを利用するうえで最も基本的な仮想マシンの利用に必要となる機能を『TIC クラウサービス』として提供しています。

3.2 責任分界点について

TIC クラウドサービスに関する責任分界点は、以下のようになります。



図：責任分界点

なお、弊社が WindowsOS の SPLA ライセンスを提供する仮想マシンについては、弊社が OS を導入した状態で提供しますが、利用開始後の OS はクラウドサービスカスタマの管理範囲となります。

SPLA でご契約頂いた Microsoft SQL については、インストーラーをデスクトップに置いた状態でご提供します。インストールおよび管理につきましてはクラウドサービスカスタマの管理範囲となります。

4. JIP-ISMS517-10、ISO/IEC 27017:2015 への対応

4.1 クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001 の 4.3】

認証審査を受けるにあたって、組織は、クラウドサービスを含めた ISMS の適用範囲の決定を行い文書化することが求められています。弊社においては、スコープを『TIC クラウドサービス』と定めています。

なお、TIC クラウドサービスにおいては、サプライチェーンにほかのクラウドサービスプロバイダは存在していないことから、弊社はクラウドサービスプロバイダであり、クラウドサービスカスタマではありません。また、ピアクラウドサービスプロバイダも存在しておりません。

＜認証取得を検討されているクラウドサービスカスタマに向けて＞

TIC クラウドサービス上でクラウドサービスを提供している事業者様が、ISMS クラウド認証の取得を行う場合は、「クラウドサービスプロバイダ」と「クラウドサービスカスタマ」の両方をスコープとする必要があります。

4.2 ISO/IEC 27017:2015（JIS Q 27017:2016） への対応

ISO/IEC 27017 は、ISO/IEC 27002 と共通する管理策については、同じ項番が付与されていますので、ISO/IEC 27001 附属書 A の項番ともーいたします。

また、既存の ISO/IEC 27001 附属書 A および ISO/IEC 27002 で想定されていないクラウド特有の拡張された管理策については、「附属書 A（規定）クラウドサービス拡張管理策集」として、頭に『CLD』がつく項番が付与されています。また、頭に『CLD』がつく管理策についても、そのあとに続く番号は、ISO/IEC 27001 附属書 A および ISO/IEC 27002 で定められた番号とも整合がとられています。

本書においては、閲覧時の利便性を考慮し、項番の順番に沿って、クラウドサービスプロバイダとしての取り組みについて解説を行います。

5.1.1 情報セキュリティのための方針群

TIC クラウドサービスでは、以下の方針を定めております。

弊社の情報セキュリティ基本方針に従い、自治体向けのサービス運営を行います。セキュリティに関して、極めて重要な事項として取り扱います。

TIC クラウドサービスでは、弊社運用担当者がクラウドサービスカスタマの情報資産(クラウドサービスカスタマにて保存されるデータ)にはアクセスできない仕組みとなっております。

なお、マルチテナント形式のサービス品目に関しては仮想化技術やネットワークセキュリティ技術を採用し、お客様システムごとに論理的にセキュアな環境で、リソースを提供しています。

また、物理的にセキュアな環境のサービスもご提供し、クラウドサービスカスタマの要件にあ

った環境を選択することが可能となっています。
自治体向けと民間向けのクラウド環境は物理的に隔離して運用を行っています。

6.1.1　情報セキュリティの役割及び責任

TIC クラウドサービスでは、「IaaS 型クラウドサービス利用契約書」や「IaaS 型クラウドサービス仕様書」にて契約やサービス内容（SLA など）を定義し、サービス提供を実施しております。
基本的には OS の管理者権限をお渡しするサービスに関しては OS 以上のレイヤーがクラウドサービスカスタマ（お客様）の責任範囲となり、ハイパーバイザの管理者権限をお渡しするサービスに関してはハイパーバイザ以上のレイヤーがクラウドサービスカスタマの責任範囲となります。
これらについては、TIC クラウド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。

6.1.3　関係当局との連絡

TIC クラウドサービスでは、クラウドサービスカスタマデータを保存する可能性のある国は、日本国となります。

CLD6.3.1　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

TIC クラウドサービスでは、「IaaS 型クラウドサービス利用契約書」や「IaaS 型クラウドサービス仕様書」（SLA）においてサービス内容及び役割・権限を定義し、サービス提供を実施しております。
また、お問い合わせ窓口はポータルサイトに掲載しております。

7.2.2　情報セキュリティの自覚、教育及び訓練

弊社では社員及び関係する外部社員に対して教育・訓練の計画を策定し実施しております。
また、実施結果に基づき理解度を評価し再教育・訓練を行い、セキュリティに関する事項を順守しております。

8.1.1　資産目録

TIC クラウドサービスでは、クラウドサービスカスタマの情報資産(クラウドサービスカスタマにて保存されるデータ)と弊社がサービスを運営するための情報は、明確に分離しております。
なお、クラウドサービスカスタマの情報資産(お客様にて保存されるデータ)に関しては、クラウドサービスカスタマに OS やハイパーバイザの管理者権限をお渡しするため、クラウドサービスカスタマの管理範囲となります。

8.2.2　情報のラベル付け

TIC クラウドサービスでは、ご契約頂きました仮想マシンごとのサービスコードにて、クラウドサービスカスタマごとの識別および利用サービスを分類しています。
クラウドサービスカスタマは、ご契約頂きましたサービス品目ごとにクラウドサービスカスタマの情報資産(お客様にて保存されるデータ)を分類することが可能となっています。

CLD8.1.5　クラウドサービスカスタマの資産の除去

TIC クラウドサービスでは、仮想マシンの管理については、クラウドサービスカスタマで実施いただく必要があることから、利用終了時には、必要に応じてデータのエクスポートなどを実施いただくとともに、クラウドサービスカスタマにおいてデータの削除を実施いただくこととなります。
また、クラウドサービスカスタマが仮想マシンの削除を行わずに利用を終了された場合は、契約終了後 10 日後に自動的に仮想マシンの削除が行われます。

9.2.1　利用者登録及び登録抹消

TIC クラウドサービスでは、クラウドサービスカスタマ専用のポータルサイトを利用できるユーザの追加・削除については、ポータルサイトの問い合わせフォームから申請をして頂くことで弊社にてご対応いたします。
仮想マシンにアクセスするためのユーティリティプログラム（vSpehre Web Client）のユーザの登録及び削除についても、ポータルサイトの問い合わせフォームから申請をして頂くことで弊社にてご対応いたします。
仮想マシンの OS 上のユーザについては、管理者権限（root、Administrator など）を含めクラウドサービスカスタマの管理となっていますので、クラウドサービスカスタマの定める規定に従い運用いただくことができます。

9.2.2　利用者アクセスの提供（プロビジョニング）

TIC クラウドサービスでは、クラウドサービスカスタマ専用のポータルサイトへのアクセス権については、契約時に作成したアカウントの管理者がマスターユーザとなり、ポータルサイトにログインして頂くことで障害・メンテナンス情報などをご覧頂くことができます。
なお、クラウドサービスカスタマの作成された仮想マシンへのアクセス権については、クラウドサービスカスタマの定めた規定により運用いただくこととなります。

9.2.3　特権的なアクセス権の管理

仮想マシンに対する特権的なアクセス件については弊社が保有し、申請に基づいてユーザには必要な権限を付与しています。

9.2.4　利用者の秘密認証情報の管理

TIC クラウドサービスでは、ポータルサイトのアカウント情報は TIC クラウドサービスご契約時に発行いたします。初回ご利用時にクラウドサービスカスタマによる変更をして頂き、適切なパスワード管理をお願いいたします。
ユーティリティプログラム（vSphere Web Client）のアカウント情報もご契約時に発行いたします。パスワード変更をご希望される場合は、弊社にご連絡ください。
また、マルチユーザ機能を使用し、利用者の追加を行う場合は、マスターユーザによる操作が必要となります。

9.4.1　情報へのアクセス制限

TIC クラウドサービスでは、ポータルサイトへのアクセスについて、弊社にご依頼頂くことで利用の制限を行うことができます。
また、仮想マシンの管理者権限（root、Administrator など）はクラウドサービスカスタマが保有していますので、クラウドサービスカスタマの定めた規定に従い運用いただくことができます。
閉域網及び限られたエリアからのみのアクセスに限定しており、アクセス制限を制御しています。

9.4.4　特権的なユーティリティプログラムの使用

TIC クラウドサービスでは、TIC クラウドサービスの利用を支援する使用者の特権的なユーティリティプログラムは vSphere Web Client としています。
利用においては認証が必要となっており、セキュリティ手順を回避することのできるユーティリティプログラムは提供しておりません。
ユーティリティプログラム（vSphere Web Client）の機能はユーザごとに制限されており、コンソールアクセスのみの利用となっています。
ユーティリティプログラムのアクセス権限を定期的に点検しています。

CLD9.5.1　仮想コンピューティング環境における分離

TIC クラウドサービスでは、仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージをクラウドサービスカスタマごとに論理的に分離しています。

CLD9.5.2　仮想マシンの要塞化

外部から仮想マシンへの通信を行う場合は FW の設定が必要です。OS 上の FW 設定は、クラウドサービスカスタマ自身で設定いただく必要があります。また、弊社のインターネット環境を利用したアクセスについては弊社側の FW 設定変更も必要となり、こちらはご依頼頂くことで弊社にて設定いたします。

あわせて、仮想マシンの管理者権限（root、Administrator など）は、クラウドサービスカスタマが保有していますので、クラウドサービスカスタマ自身で必要なサービスの選定やログの取得など実施いただくことができます。
なお、ご契約頂きましたサービスの初期状態に関しては、サービス仕様書（SLA）およびご利用の手引きにて開示しております。
仮想マシンが利用するネットワークは、利用者単位でVLANを用いて分割されているため、利用者をまたいだアクセスは不可能です。
仮想マシン上で稼働するOSレベルで必要な要塞化については、クラウドサービスカスタマ自身で必要なサービスの選定やログの取得など実施いただくことができます。

10.1.1 暗号による管理策の利用方針

TIC クラウドサービスでは、基本的にクラウドサービスカスタマの情報資産(クラウドサービスカスタマにて保存されるデータ)に関して、弊社にて暗号化を実施することはございません。
クラウドサービスカスタマに OS やハイパーバイザの管理者権限をお渡しするサービスであるため、データの暗号化はクラウドサービスカスタマの実施範囲となりますので、クラウドサービスカスタマのセキュリティポリシーに合わせたセキュリティ保護を実施して頂くことが可能となっています。

11.2.7 装置のセキュリティを保った処分又は再利用

TIC クラウドサービスでは、使用している記憶媒体については、RAID により冗長化された領域に、仮想のストレージ領域を保持しているため、ストレージを構成する HDD を一つだけ取得しても、中の情報が取り出せない状態になっています。
なお、故障などにより交換した記憶媒体の処理については、弊社と機器ベンダーとの契約に基づき適切に処理を行っています。
TIC クラウドサービスの設備を再利用、廃棄する際には適切なプロセスで、データの削除や設備の破壊を実施しております。

12.1.2 変更管理

TIC クラウドサービスでは、サービス内容を変更する場合、影響のあるクラウドサービスカスタマに対し変更内容をメールにてご連絡いたします。また、メンテナンスを実施する際、クラウドサービスカスタマに影響のある場合もご連絡しております。

12.1.3 容量・能力の管理

TIC クラウドサービスでは、サービススペックを明確にするとともに、各種リソースについて常に監視を行っており、リソースの増強などを進めています。仮想マシンのCPU、メモリ、ネットワークの利用量に関しては、ユーティリティプログラム（vSphere Web Client）の機能を用いて

確認することが可能です。詳しい手順については、ご利用の手引きにて説明します。

12.3.1 情報のバックアップ

TIC クラウドサービスでは、仮想マシンイメージの snapshot を取得しています。日次(23 時スタート)で Disk To Disk によるバックアップを取得しており、7 世代以上を保持しています。
バックアップ結果についてはネットワークオペレーションセンターにて毎日目視で確認する運用を行っています。異常が検知された際はクラウド業務担当者へ連絡し、対応を行います。
また、バックアップ検証用サーバにて年一回バックアップデータのリストア試験を行います。
また、仮想マシン内の個別データのバックアップについては、クラウドサービスカスタマの範疇とします。

12.4.1 イベントログ取得

TIC クラウドサービスでは、ユーティリティプログラム（vSphere Web Client）の機能を用いてログを確認することが可能です。詳しい手順については、ご利用の手引きに記載しています。
仮想マシンについては、クラウドサービスカスタマに管理者権限（root、Administrator 等）が付与されていますので、クラウドサービスカスタマのポリシーに従い取得いただくことができます。
また、クラウドサービスカスタマの責任の範囲においては、OS の管理者権限をお渡しするサービスであるため、それらの範囲においてクラウドサービスカスタマ自身でログを取得することが可能となっています。

12.4.4 クロックの同期

TIC クラウドサービスでは、物理ホストの NTP サーバの同期は弊社で実施しており、VMware Tools を導入した仮想マシンは、自動的に物理ホストと NTP 同期を行います。お客様の個別ネットワークで NTP 同期をとる際は、お客様で作業をお願いします。
クロックの同期方法の例はご利用の手引きを参照ください。

12.6.1 技術的な脆弱性の管理

TIC クラウドサービスでは、脆弱性情報を常時収集しております。収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合については、速やかに対応しております。
また、クラウドサービスカスタマに影響しうるインシデントについても、クラウドサービスカスタマへメールにてお伝えしております。

CLD12.1.5 実務管理者の運用のセキュリティ

TIC クラウドサービスでは、TIC クラウドサービスをご利用いただくにあたり、必要な操作手順

についてはご利用の手引きにて文書化し提供しております。
ご利用の手引きにおいては、特定の作業エリアのみで参照可能です。

CLD12.4.5　クラウドサービスの監視

TIC クラウドサービスでは、ユーティリティプログラム(vSphere Web Client)を用いて、特定のエリアから仮想マシンのCPU、メモリ、ネットワークの利用量等を参照いただくことができます。
クラウドサービスカスタマの責任範囲の監視につきましては、クラウドサービスカスタマにて実施頂く必要があります。
クラウドサービス管理機能の確認方法はご利用の手引きを参照ください。

13.1.3　ネットワークの領域分割

TIC クラウドサービスでは、ネットワークの仮想化技術（VLAN 等）の使用により、他のクラウドサービスカスタマと論理的にネットワークを分離し、高い機密性を確保しています。
また、サービス運営で必要となる弊社管理ネットワークに関しても、クラウドサービスカスタマのネットワークと分離しております。

CLD13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

TIC クラウドサービスでは、お客様ごとに個別のネットワーク(VLAN)を提供します。そのため、物理ネットワーク、仮想ネットワークにかかわらず、統一的なポリシーに基づいて情報セキュリティを担保します。

14.1.1　情報セキュリティ要求事項の分析及び仕様化

TIC クラウドサービスでは、UTM 機能、監視機能、SOC サービス等提供しています。詳しくはお客様ごとのサービス仕様書において定義します。

14.2.1　セキュリティに配慮した開発のための方針

TIC クラウドサービスでは、IPA から提供される脆弱性情報等を提供することが可能です。また、OracleDB を用いた開発を行うための、専用の仮想基盤を用意しています。

15.1.2　供給者との合意に含まれるセキュリティの取り組み

TIC クラウドサービスでは、TIC とクラウドサービスカスタマの責任分界点は、サービス利用契約書で示しています。なお、サービス提供内容はサービス仕様書に記載しております。

15.1.3　ICT サプライチェーン

TIC クラウドサービスでは、弊社のデータセンター内に環境を構築しています。弊社からの委託先については、契約の定めにしたがい管理を行っています。また、現時点においてピアク

ラウドサービスプロバイダは存在しません。今後利用する場合には、同等の情報セキュリティ水準を要求するよう定めています。
合わせて、サプライチェーンでクラウドサービスを提供する場合は、供給者に対して弊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。

16.1.1 責任及び手順

TIC クラウドサービスでは、契約者情報やクラウドサービスカスタマに影響のあるインシデントが発生した場合には、弊社の規定に基づき通知を行います。なお、責任範囲、通知目標時間、通知手順については、契約書をご参照ください。

16.1.2 情報セキュリティ事象の報告

お客様の責任の範囲で発生したインシデントについてはメールにて報告を頂き、弊社のインシデント対応フローに従って対応を行います。
当社原因のインシデントについての報告はポータルサイト内で掲載します。
TIC クラウドサービスではポータルサイトにて、お客様がインシデントを追跡するための仕組みを提供します。

16.1.7 証拠の収集

TIC クラウドサービスでは、仮想マシンの管理者権限（root、Administrator 等）は、クラウドサービスカスタマが保有しているため、デジタル証拠となり得る情報については、ご契約者様に管理いただく必要があります。
なお、捜査機関または監督官庁より指導、摘発、注意もしくは照会を受けた場合は、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。

18.1.1 適用法令及び契約上の要求事項の特定

TIC クラウドサービスでは、準拠法を日本法と定めています。
お客様から関連法規の提示を求められた場合には、関連法規一覧を提供します。法令の遵守状況においては、定期的な内部監査を実施しています。

18.1.2 知的財産権

TIC クラウドサービス上で知的財産権及び権利関係のあるソフトウェアをご利用頂く場合、必要な情報がありましたらお問い合わせください。
TIC クラウドサービスでは、苦情相談窓口をホームページ上に公開しています。

18.1.3 記録の保護

TIC クラウドサービスでは、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。

18.1.5 暗号化機能に対する規制

ユーティリティプログラム(vSphere Web Client)での仮想マシンへのアクセスにおいては、SSL/TLS による通信の暗号化を行っています。
その他、リモートアクセス機能（VPN）など提供しております。
なお、輸出規制の対象となる暗号化の利用はありません。

18.2.1 情報セキュリティの独立したレビュー

TIC クラウドサービスでは、以下の各事項を実施しています。
・ISO/IEC 27001 および JIP-ISMS517-1.0（ISO/IEC 27017）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いることで、情報セキュリティに対する取り組みの証憑としています。
・TIC クラウドの利用を検討している事業者およびクラウドサービスカスタマの定めるチェックシート等について回答を行っています。（なお、回答までに 1 週間程度のお時間を頂戴しています。）
・使用しているデータセンターについては、監査の受け入れを行っており、建物設備について見学いただくことができます。
・「ホワイトペーパー」により情報の開示を行っています。

改訂履歴

版数	日付	主な変更内容
初版	2019/9/30	初版発行
1.1	2020/3/31	15.1.2、16.1.2 の内容修正