IDCF クラウド

ISO/IEC 27017 ホワイトペーパー

株式会社 IDC フロンティア

2021 年 1 月 18 日（第 4.1 版）

もくじ

はじめに 4
ホワイトペーパーの目的 4
本書の適用範囲について 4
本書で使用する用語について 4
ISMS クラウドセキュリティ認証について 5
ISO/IEC 27017:2015 とは 5
JIP-ISMS517-1.0 と ISO/IEC 27017:2015 の関係性 5
認証審査について 6
IDCF クラウド コンピューティングサービスについて 7
IDCF クラウド コンピューティングサービスについて 7
責任分界点について 7
JIP-ISMS517-1.0、ISO/IEC 27017:2015 への対応 8
1. JIP-ISMS517-1.0 への対応 8
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】 8
2. ISO/IEC 27017:2015（JIS Q 27017:2016） への対応 8
5.1.1 情報セキュリティのための方針群 9
6.1.1 情報セキュリティの役割及び責任 9
6.1.3 関係当局との連絡 9
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分担 9
CLD.8.1.5 クラウドサービスカスタマの資産の除去 9
8.2.2 情報のラベル付け 10
9.2.1 利用者登録及び登録削除 10
9.2.2 利用者アクセスの提供(provisioning) 10
9.2.3 特権的アクセス権の管理 10
9.2.4 利用者の秘密認証情報の管理 10
9.4.1 情報へのアクセス制限 11
9.4.4 特権的なユーティリティプログラムの使用 11
CLD.9.5.1 仮想コンピューティング環境における分離 11
CLD.9.5.2 仮想マシンの要塞化 11
10.1.1 暗号による管理策の利用方針 12
11.2.7 装置のセキュリティを保った処分又は再利用 12
12.1.2 変更管理 12
12.1.3 容量・能力の管理 12

CLD.12.1.5　実務管理者の運用のセキュリティ 12
12.3.1　情報のバックアップ 13
12.4.1　イベントログ取得 13
12.4.4　クロックの同期 13
CLD.12.4.5　クラウドサービスの監視 14
12.6.1　技術的ぜい弱性の管理 14
13.1.3　ネットワークの分離 14
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 14
14.1.1　情報セキュリティ要求事項の分析及び仕様化 14
14.2.1　セキュリティに配慮した開発のための方針 15
15.1.2　供給者との合意におけるセキュリティの取扱い 15
15.1.3　ICT サプライチェーン 15
16.1.1　責任及び手順 15
16.1.2　情報セキュリティ事象の報告 15
16.1.7　証拠の収集 16
18.1.1　適用法令及び契約上の要求事項の特定 16
18.1.2　知的財産権 16
18.1.3　記録の保護 16
18.1.5　暗号化機能に対する規制 16
18.2.1　情報セキュリティの独立したレビュー 16
改訂履歴 18

はじめに

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、IDCF クラウド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、IDCF クラウドを利用して、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、IDCF クラウドは、常に進化を続けていますので、最新の情報については、当社営業までご相談いただくか、当社 Web サイトをご確認ください。
【当社 Web サイト】
https://www.idcf.jp/

本書の適用範囲について

IDCF クラウド　コンピューティングサービスが本書の適用範囲となります。

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。

ISMS クラウドセキュリティ認証について

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。

JIP-ISMS517-1.0 と ISO/IEC 27017:2015 の関係性

ISO/IEC 27017:2015 は、クラウドサービス固有の情報セキュリティ管理策および実施の手引きを追加するガイドライン規格であり、ISO/IEC 27002:2013 と同様に要求事項（認証基準）ではありません。
また、ISO/IEC 27000 シリーズでは、ISO/IEC 27017:2015 についての要求事項（認証基準）となる文書は発行されておりません。

要求事項 （認証基準）	実践のための規範 （ガイドライン）
ISO/IEC 27001	ISO/IEC 27002
未発行	ISO/IEC 27017

そのため、一般財団法人日本情報経済社会推進協会（JIPDEC）は、ISMS クラウドセキュリティ認証のための新たな認証基準として「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項 JIP-ISMS517-1.0」を 2016 年 8 月 1 日に施行し、以下の関係となりました。

要求事項 （認証基準）	実践のための規範 （ガイドライン）
ISO/IEC 27001	ISO/IEC 27002
JIP-ISMS517-1.0	ISO/IEC 27017

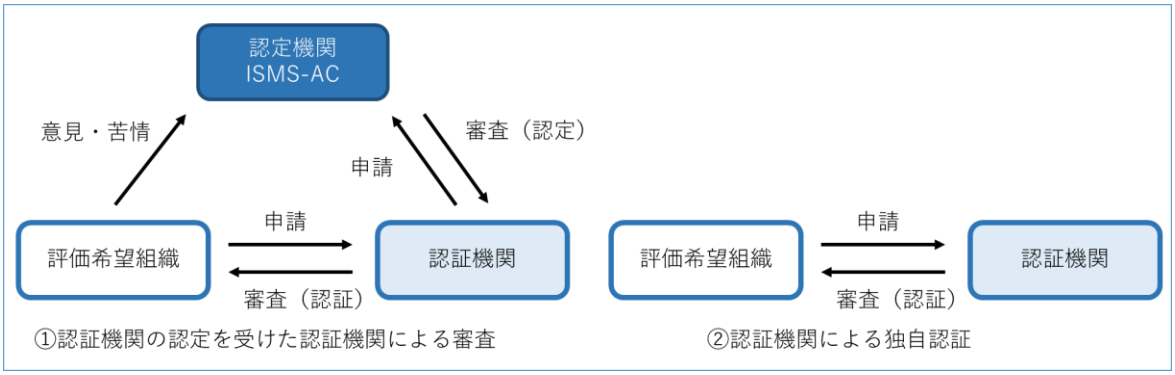
認証審査について

ISO/IEC 27017:2015 への適合審査については、現状 2 種類の方法があります。

① **認証機関の認定を受けた認証機関による審査**
※『ISO/IEC 27017:2015』の認証基準となる『JIP-ISMS517-1.0』への適合が認められた場合、認証機関および認定機関のマークが付与された証書が発行されます

② **認証機関による独自認定**
※『ISO/IEC 27017:2015』に対する認証機関の定めた適合基準への適合が認められた場合、認証機関のマークの付与された証書が発行されます

それぞれの方法について、図示した場合以下のようになります。



この 2 種類の審査方法の一番の違いは、認証機関が正しく審査を行える能力を認定機関である一般社団法人情報マネジメントシステム認定センター（ISMS-AC）が認定しているか否かということです。

なお、ISMS-AC による認定を受けた認証機関については、こちらのサイトから最新の情報を参照することができます。
【ISMS クラウドセキュリティ認証機関一覧】
https://isms.jp/lst/isr/index-ismscls.html

IDC フロンティアの提供する IDCF クラウド　コンピューティングサービスは、①の方式での審査を受けています。

【補足】
ISMS（ISO/IEC 27001）の審査を日本企業が日本の認定機関に審査を依頼する場合、一般的には、①の方式で審査が実施されています。

IDCF クラウド　コンピューティングサービスについて

IDCF クラウド　コンピューティングサービスについて

IDCF クラウドは、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。IDCF クラウドにはさまざまな機能が備わっていますが、IDCF クラウド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『IDCF クラウド　コンピューティングサービス』として提供しています。

責任分界点について

IDCF クラウド　コンピューティングサービスに関する責任分界点は、以下のようになります。

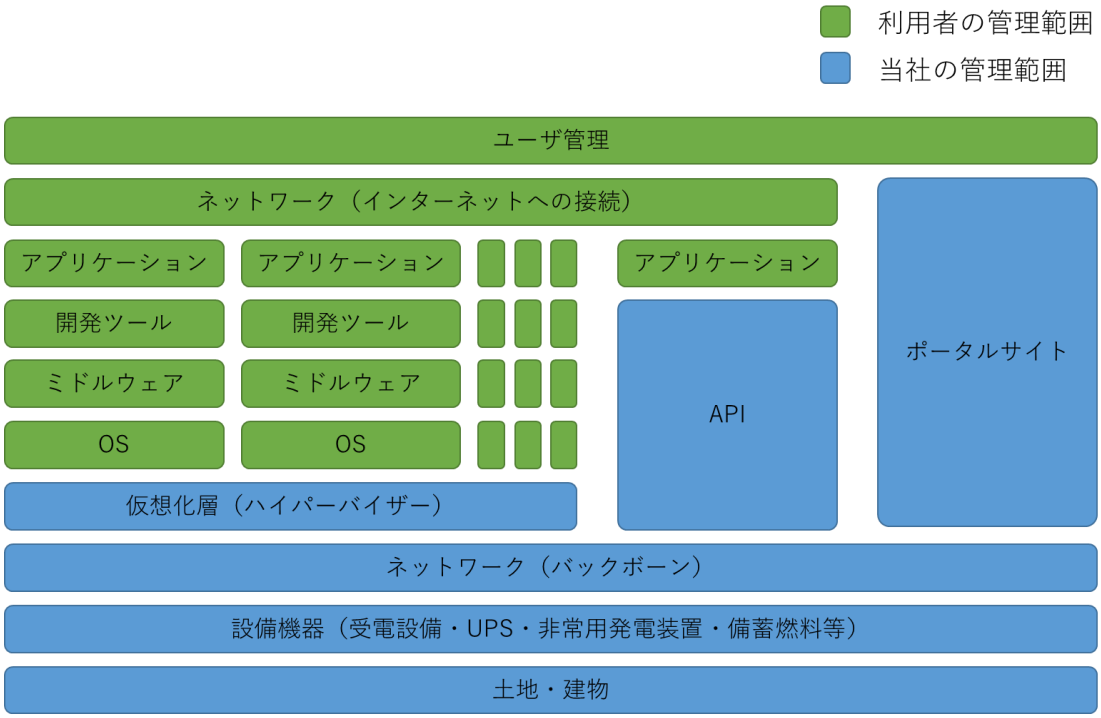


図　責任分界点

なお、仮想マシンを作成するために OS のテンプレートを提供していますが、テンプレートの利用開始後の OS の管理については、クラウドサービスカスタマの管理範囲となります。また、テンプレートについては、作成時点での最新版となっていますので、利用開始時にパッチを適用させるなど、クラウドサービスカスタマにおいて、セキュリティ対策を実施いただきますようお願いします。

JIP-ISMS517-1.0、ISO/IEC 27017:2015 への対応

1. JIP-ISMS517-1.0　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。当社においては、スコープを『IDCF クラウド　コンピューティングサービスの提供に係るクラウドサービスプロバイダとしてのシステム運用・保守』と定めています。

なお、IDCF クラウドにおいては、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、当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＞

IDCF クラウド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。

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 の項番とも一致します。

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

クラウドサービスプロバイダは、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ方針の拡充が求められています。これらについては、当社のセキュリティポリシーの見直しを行い、クラウドサービスカスタマが安心して利用できるよう取り組みを行っています。

6.1.1　情報セキュリティの役割及び責任

「クラウドサービスに関する契約約款　第 6 条、文書 A　第 6 条、文書 B　第 6 条ほか」で役割及び責任について明記しており、これらについては、IDCF クラウド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

地理的所在地は「クラウドサービスに関する契約約款　第 33 条、第 34 条」で定めています。また、現時点において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。

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分担

サービスに関する事項は「クラウドサービスに関する契約約款　文書 B　第 7 条ほか」、「クラウドサービスに関する重要事項等説明書」に示している通りです。また、責任分界点については、前出の「責任分界点について」の項を参照ください。

CLD.8.1.5　クラウドサービスカスタマの資産の除去

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等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仮想マシン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、当社側で削除を行わせていただくことを「クラウドサービスに関する契約約款　文書 B　第 12 条」で定めています。

なお、仮想マシン上に保存しているデータや、クラウドコンソールより仮想マシンを削除した場合、仮想マシンが使用していた領域も消去されます。この際にストレージ内のメタデータも削除される

ため、一度削除を実施されると、仮想マシンの復元ができないようになっています。仮想マシンの削除を実施される際にはご注意ください。

8.2.2　情報のラベル付け

仮想マシン上に保存されたデータに対してラベル付けを行う機能は提供しておりません。
ポータルサイト上においては、「仮想マシン名」、「IP アドレス名」、「ボリューム名」などのラベル付け機能を提供しています。

9.2.1　利用者登録及び登録削除

ポータルサイトを利用できるユーザーを管理する機能を提供しており、クラウドサービスカスタマでユーザー管理が行えるようになっています。また、仮想マシンについては、管理者権限（root、Administrator 等）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(provisioning)

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ーとなり、マスターユーザー、パワーユーザー、一般ユーザー、ビリングユーザーの 4 種のユーザータイプから、IDCF クラウドのポータルサイト上で行える機能の制限を行うことができます。
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　特権的アクセス権の管理

ポータルサイトにおいては、ID/パスワードによる認証だけでなく、Google Authenticator を利用した 2 段階認証の利用ができます。マスターユーザーは、管理するマルチユーザーに対して、2 段階認証の強制適用を行うこともできます。
また、ポータルサイトへの接続元 IP アドレス制限についても設定いただくことができます。

9.2.4　利用者の秘密認証情報の管理

初期のアカウント登録手順については、「めちゃ楽ガイド（https://www.idcf.jp/help/cloud/guide/pdf/IDCFCloud_installation_guide.pdf）」に詳細な手順を記

載しています。また、マルチユーザー機能を使用し、利用者の追加を行う場合は、マスターユーザーによる操作が必要となります。専用画面から利用者のメールアドレスを含めた情報の登録を行っていただきます。マスターユーザーによる登録が完了すると、登録いただいたメールアドレスに対し、パスワード設定用 URL が記載されたメールが届きますので、画面の指示に従っていただき、パスワードの設定を行っていただくこととなります。なお、パスワード設定用 URL については、一定時間のみ有効なものとなりますので、ご注意ください。

9.4.1　情報へのアクセス制限

ポータルサイトへのアクセスについては、クラウドサービスカスタマの管理権限を保有している方によって、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 等）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。

9.4.4　特権的なユーティリティプログラムの使用

IDCF クラウド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、「ポータルサイト上での機能」および「API」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。

CLD.9.5.1　仮想コンピューティング環境における分離

クラウドサービスカスタマの利用する仮想マシンやネットワークは、VLAN によって論理的に分離されています。

CLD.9.5.2　仮想マシンの要塞化

アカウント作成時に提供される仮想ルータに FW 機能を備えており、利用開始時点においては、すべてのポートが閉じた状況としています。また、外部から仮想マシンへの通信を行う場合は、ポートフォワードの設定が必要です。これらの仮想ルータの設定は、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。あわせて、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。

10.1.1　暗号による管理策の利用方針

仮想マシンについては、標準で暗号化の処理を提供しておりません。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ますので、クラウドサービスカスタマの定めるポリシーに基づき運用いただくことができます。

11.2.7　装置のセキュリティを保った処分又は再利用

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、故障等により交換した記憶媒体の処理については、当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。

12.1.2　変更管理

クラウドサービスカスタマに何らかの影響が発生する可能性のある変更及びメンテナンスについては、事前に通知を行っています。通知方法については、「クラウドサービスに関する契約約款第 31 条」で定めています。

12.1.3　容量・能力の管理

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、ゾーンの増強などを進めています。また、ポータルサイトを通じて、サービス全体のレスポンス等の情報についてもクラウドサービスカスタマに公開しています。

CLD.12.1.5　実務管理者の運用のセキュリティ

「仕様書（https://www.idcf.jp/cloud/pdf/IDCFCloud_spec.pdf）」、「めちゃ楽ガイド（https://www.idcf.jp/help/cloud/guide/pdf/IDCFCloud_installation_guide.pdf）」および「ご利用ガイド（https://www.idcf.jp/help/cloud/guide/）」等を提供しています。また、操作手順や活用方法についてまとめた書籍「シンプル・パワフル IDCF クラウド攻略（ISBN：978-4-87783-405-0）」も出版しています。

12.3.1　情報のバックアップ

スナップショットの機能を備えており、クラウドサービスカスタマが自由に取得（スケジュール設定を含む）することができます。この機能を使用した場合、取得したスナップショットの保管場所は論理的に分離されているため、他のクラウドサービスカスタマがアクセスすることはできません。
なお、スナップショット作成や、スナップショットから仮想マシンを戻すために必要となる時間については、利用状況によって異なりますので、定期的に確認いただくことをおすすめします。

12.4.1　イベントログ取得

ポータルサイトへのログインのログは、ポータルサイトから閲覧できます。また、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。
なお、標準で提供している仮想ルータについては、ログの取得機能がありません。必要に応じて、仮想マシン側で取得いただくか、もしくは、VyOS などのネットワーク・オペレーティング・システムを使用するなど、ほかの手段で取得いただく必要があります。

12.4.4　クロックの同期

当社が用意している仮想マシンのテンプレートは、当社が管理する NTP サーバーを参照するよう設定しています。
なお、ISO/IEC 27001 の同項目では、「単一の参照時刻源と同期させなければならない」と定められています。そのため、クラウドサービスカスタマの組織が ISO 27001 を取得されている場合、以下の対応を行うことで、規格要求事項に準拠することができます。

＜方法 1：クラウドサービスカスタマの時刻源に合わせる＞
クラウドサービスカスタマの使用している時刻源に同期させます。

＜方法 2：クラウドサービス側に合わせる＞
仮想マシンを NTP サーバーとし、すべての時刻を同期させます。
（なお、当社の用意しているNTP サーバーは、当社のテンプレートを使用した仮想マシン以外の利用は、ご遠慮ください）

＜方法 3：複数の NTP サーバーの集合を一つの時刻源として扱う＞
NTP は万が一参照先の時刻が何らかの原因で時刻がずれた場合に、その影響を受けることを回避するため、その時刻の信頼性を低いとみなして、同期候補から外す仕組みを備えています。たとえば、当社のテンプレートを使用した仮想マシンを NTP サーバーの 1 台とし、クラウドサービスカ

スタマの管理するそのほかの 2 台以上の NTP サーバーで信頼性を担保した時刻を一つの時刻源とみなすことができます。

CLD.12.4.5　クラウドサービスの監視

ネットワークの利用量等をコントロールパネルから参照いただくことができます。また、トラヒックの総量については、常時監視を行っており、DDoS に対する防御機能を標準機能として提供しています。
あわせて、仮想マシンについては、CPU やメモリの急激な高騰を検知できるよう、エコアライアンスパートナーの提供する監視ツールを活用いただくことができます。

12.6.1　技術的ぜい弱性の管理

当社の管理するポータルサイト等については、リリース前および、定期的な脆弱性診断の実施や、定期的なネットワーク診断を行っています。
また、ぜい弱性情報の収集を行い、対策を行うとともに、必要に応じてポータルサイト等で対応の呼びかけなどを実施しています。

13.1.3　ネットワークの分離

VLAN により、契約アカウントごとにネットワークの分離をしています。

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

当社の内部規定を策定し、文書化しています。また、変更管理プロセスにより、物理と仮想での整合が取れなくなるような変更作業を行えないようコントロールを実施しています。

14.1.1　情報セキュリティ要求事項の分析及び仕様化

IDCF クラウドにおいては、「仕様書（https://www.idcf.jp/cloud/pdf/IDCFCloud_spec.pdf）」、「めちゃ楽ガイド（https://www.idcf.jp/help/cloud/guide/pdf/IDCFCloud_installation_guide.pdf）」および「ご利用ガイド（https://www.idcf.jp/help/cloud/guide/）」等を提供しています。また、操作手順や活用方法についてまとめた書籍「シンプル・パワフル IDCF クラウド攻略（ISBN：978-4-87783-405-0）」も出版しています。

14.2.1　セキュリティに配慮した開発のための方針

当社の管理するポータルサイト等については、リリース前および、定期的な脆弱性診断の実施や、定期的なネットワーク診断を行うことを方針として定めています。

15.1.2　供給者との合意におけるセキュリティの取扱い

当社とクラウドサービスカスタマの責任分界点は、契約約款で示しています。IDCF クラウドのアカウント作成時に契約約款に同意いただきますと、IDCF クラウドの利用ができるようになります。
なお、責任分界点についての解説は、前出の「責任分界点について」の項を参照ください。

15.1.3　ICT サプライチェーン

IDCF クラウドは、当社のデータセンターに当社で環境を構築しています。当社からの委託先については、契約約款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、供給者に対して情報セキュリティ目的を示し、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

当社で確認したインシデントについては、当社内の通知規定に基づき、通知を行います。なお、通知は、「クラウドサービスに関する契約約款」で定めた方法で行います。

16.1.2　情報セキュリティ事象の報告

クラウドサービスカスタマからの問い合わせや報告は、ポータルサイト上で、チケットの起票が行えるようにしており、カスタマが発見した情報セキュリティ事象の報告を行うことができます。
チケットとなっていますので、問い合わせの履歴の追跡ができます。

16.1.7　証拠の収集

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、ディ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、「クラウドサービスに関する契約約款」で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

「クラウドサービスに関する契約約款　第 34 条」で準拠法を日本法と定めています。

18.1.2　知的財産権

クラウドサービスカスタマからの問い合わせは、ポータルサイト上からチケットの起票によって行うことができます。

18.1.3　記録の保護

「クラウドサービスに関する契約約款　第 24 条、第 25 条、第 26 条、第 27 条」で定めています。

18.1.5　暗号化機能に対する規制

仮想マシン上で利用できる暗号化機能は、提供しておりません。クラウドサービスカスタマの定める規定に基づき運用いただくことができます。
クラウドポータルサイトへの Web アクセスにおいては、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。詳細は仕様書をご確認ください。

18.2.1　情報セキュリティの独立したレビュー

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。
- FISC や J-Tier について、セルフチェックを実施し、クラウドサービスカスタマの求めに応じてチェック結果の開示を行っています。

- IDCF 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、サイトツアー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。
- 「セキュリティホワイトペーパー」および本書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	2017/7/10	初版発行
第 2 版	2018/5/1	・ISMS-AC 設立に伴う変更 ・契約約款改定に伴う変更 ・15.1.3　の更新
第 3 版	2018/6/5	・8.2.2　の更新 ・18.1.5　の更新
第 4 版	2020/2/18	・契約約款改定に伴う変更
第 4.1 版	2021/1/18	・JIP-ISMS517-1.0(ISO/IEC 27017:2015) のスコープの変更