

## IBM Cloud Identity

本「サービス記述書」は「クラウド・サービス」について規定するものです。該当する注文関連文書には、お客様の発注に関する価格の詳細情報および追加の詳細情報が記載されています。

### 1. クラウド・サービス

IBM Cloud Identity は、内部ユーザー（従業員）および外部ユーザーのためのシングル・サインオン (SSO)、多要素認証および ID ライフサイクル管理を提供します。

#### 1.1 オファリング

お客様は、以下の利用可能なオファリングから選択することができます。これらはすべて、1 秒につき 400 イベントの「イベント」キャパシティを備えています。

##### 1.1.1 IBM Cloud Identity Connect

本「クラウド・サービス」は、シングル・サインオン (SSO) および Open ID Connect (OIDC)、クラウド・ベースの API 権限のための Authentication as a Service、アプリケーション・ランチパッド、管理者報告および解析ダッシュボードを提供します。本「クラウド・サービス」は、最新の標準に基づく認証とフェデレーション・プロトコルを使用して (共通アプリケーションに対する数百ものコネクタを含む。)、ユーザーをアプリケーションに接続します。本「クラウド・サービス」は、イネープリング・ソフトウェアとして含まれるオンプレミスの IBM Security Access Management (ISAM) ソフトウェア・プログラムと密に連携して、お客様が、オンプレミス・アプリケーションとクラウド・アプリケーションの両方に及ぶアクセス管理についてそれぞれの基幹業務の要求をサポートするためのソリューションを提供します。

##### 1.1.2 IBM Cloud Identity Connect for ISAM

本「クラウド・サービス」は、オンプレミスの IBM Security Access Management (ISAM) ソフトウェア・プログラムと密に連携して、お客様が、オンプレミス・アプリケーションとクラウド・アプリケーションの両方に及ぶアクセス管理についてそれぞれの基幹業務の要求をサポートするためのソリューションを提供します。本「クラウド・サービス」では、お客様が IBM Security Access Management (ISAM) プログラムのソフトウェア・サブスクリプション & サポート (S&S) の有効な使用許諾を取得している必要があります。当該 S&S はお客様の「クラウド・サービス」のサブスクリプション期間中、有効でなければなりません。本「クラウド・サービス」に対するお客様の使用許諾は、お客様のオンプレミス ISAM ライセンスの使用許諾と同等でなければなりません。お客様の S&S が継続されない場合は、本「クラウド・サービス」も終了します。第 5.2 項に定めるイネープリング・ソフトウェアに対するアクセスは、本「クラウド・サービス」には含まれていません。

##### 1.1.3 IBM Cloud Identity Essentials

本「クラウド・サービス」は、お客様が使用しているさまざまな IBM クラウド・アプリケーションおよびパブリック・クラウド・アプリケーションに対するシングル・サインオン (SSO) 機能をお客様に提供します。本「クラウド・サービス」を IBM の MaaS360 と連動させて、条件付きアクセスなどの追加レベルのセキュリティ管理を提供することができます。

##### 1.1.4 IBM Cloud Identity Verify

本「クラウド・サービス」は、デジタル・サービスにアクセスする時に ID を確認するために、Cloud Identity Connect によって (または直接 API 呼び出しによって) 保護されているアプリケーションおよび他の実施ポイント (RADIUS クライアント、Unix/Linux PAM サーバーおよび Windows サーバーを含む。) に多要素認証を提供します。これには、電子メール、SMS およびタイム・ベース (ソフトウェア・トークン) のワンタイム・パスワード、ならびに IBM Verify を備えたプッシュ・ベースのモバイル生体認証などの仕組みが含まれます。本「クラウド・サービス」は、オンプレミスの IBM Security Access Management (ISAM) ソフトウェア・プログラムと連携して、お客様が、オンプレミス・アプリケーションとクラウド・アプリケーションの両方に及ぶアクセス管理についてそれぞれの基幹業務の要求をサ

ポートするためのソリューションを提供します。これは、単独で、または Cloud Identity Connect、Cloud Identity Connect for ISAM および Cloud Identity Essentials を補足するために利用することができます。

### 1.1.5 IBM Cloud Identity Govern

本「クラウド・サービス」は、イネーブリング・ソフトウェアとして含まれるオンプレミスの IBM Governance and Intelligence (IGI) ソフトウェア・プログラムと密に連携して、お客様が、オンプレミス・アプリケーションとクラウド・アプリケーションの両方に及ぶアクセス管理についてそれぞれの基幹業務の要求をサポートするためのソリューションを提供します。本「クラウド・サービス」は、クラウド内で拡張された ID ライフサイクル管理機能を組織に提供するもので、アプリケーション・アクセス要求ワークフローが含まれます。

### 1.1.6 IBM Cloud Identity Connect and Verify

本「クラウド・サービス」は、単一のオフオファリングとして IBM Cloud Identity Connect および IBM Cloud Identity Verify の機能をお客様に提供します。

### 1.1.7 IBM Cloud Identity Analyze

本「クラウド・サービス」は、IBM Security Identity Governance and Intelligence (IGI) および IBM Security Identity Manager (ISIM) など、既存の IBM ソリューションを拡張して管理対象ユーザーの全体的なリスク・プロファイルを提供します。本「クラウド・サービス」には、さまざまなソースからのアクティビティ・データや使用許諾データを処理する、オンプレミスの多目的アナリティクス・エンジンが含まれており、これによりアクセス・リスクに関する洞察に基づいて対策を講じるための機能と共に、かかるリスクの 360 度のビューを提供します。

### 1.1.8 IBM Cloud Identity Adaptive Access

本「クラウド・サービス」では、ユーザーやユーザーのデバイス、および行動パターンに関して「人工知能」(AI) 採用のコンテキストに応じた洞察を使用して、組織が正しい認証ポリシーを適用できるようにします。

### 1.1.9 IBM Cloud Identity Connect Verify and Govern

本「クラウド・サービス」は、単一のオフオファリングとして IBM Cloud Identity Connect、IBM Cloud Identity Verify および IBM Cloud Identity Govern の機能をお客様に提供します。

## 1.2 オプション・サービス

### 1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud は、お客様が社内の非実稼働活動のためにのみ使用できる IBM Cloud Identity プラットフォームの別個のインスタンスです。これには、テスト、パフォーマンス調整、障害診断、社内ベンチマーク、段階的な品質保証活動、および公開されたアプリケーション・プログラミング・インターフェースを使用した、「クラウド・サービス」に対する社内用の追加機能または拡張機能の開発が含まれますが、これらに限定されません。本「クラウド・サービス」には、第 3 条「サービス・レベルおよびテクニカル・サポート」の条件に従って、可用性のサービス・レベル・アグリーメント (SLA) を含めるオプションがあります。本「クラウド・サービス」は、100 イベント/秒のキャパシティを備えています。

### 1.2.2 IBM Cloud Identity Vanity Domain

お客様は、バニティー・ドメイン (1 つのドメイン) により、プラットフォームから提供されるすぐに使用できるデフォルトのテナント・ドメインを使用するのではなく、お客様の組織が所有し、お客様の組織への関連性が高いドメインを使用できます。このドメインの SSL 証明書は、IBM によって保持され、1 年ごとに更新されます。

### 1.2.3 IBM Cloud Identity Application Gateway Hosted

このアプリケーション・ゲートウェイは、非標準 (または既存) ベースの認証メカニズムのサポートを求めているお客様に対して、IBM が管理およびホストする軽量アプライアンスを提供します。これらのメカニズムには、LTPA および HTTP ヘッダー・ベースの認証が含まれます。継続モニタリングおよび保守は IBM が管理します。

## 1.3 アクセラレーション・サービス

### 1.3.1 IBM Cloud Identity Connect Solution Planning

このサービスでは、1 週間のプロフェッショナル・サービスを提供します。このサービスの間、IBM は以下の一部または全部のサービスを実行します。

- クラウド・ベースの SaaS アプリケーションのシングル・サインオンを確立する。
- アプリケーションを簡単に見つけられるランチパッドを構成する。
- 既製のコネクタを使用してアプリケーションを接続する。
- ソリューションの計画立案、アーキテクチャーおよびガイダンス。
- IBM が推奨するアプローチおよび手法。

### 1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

このサービスでは、多要素認証の課題、および IBM Cloud Identity Verify を使用したお客様のアプリケーションの保護に重点を置いた 3 日間のプロフェッショナル・サービス・ワークショップを提供します。このワークショップは、以下の一部または全部を対象とします。

- 認証が必要なすべてのデジタルおよび人による対話に使い慣れた認証機能を組み込む。
- 開発者が使いやすい REST API を使用した強力な認証をアプリケーションで実行できるようにする。
- ID セキュリティーに関して業界のベスト・プラクティスを推奨する。
- 携帯電話、タブレット、およびラップトップを含むすべての物理的な仕様や規格で、ユーザー・エクスペリエンスおよび採用を効率化する。

### 1.3.3 IBM Cloud Security Strategy and Planning

このサービスでは、インフラストラクチャーおよびアプリケーションのセキュリティに重点を置いた、クラウド・セキュリティのベスト・プラクティスの適用方法に関する 3 週間のプロフェッショナル・サービス・ワークショップを提供します。このワークショップは、以下の一部または全部を対象とします。

- クラウド・ベースの SaaS アプリケーションのシングル・サインオンを確立する。
- アプリケーションを簡単に見つけられるランチパッドを構成する。
- 既製のコネクタを使用してアプリケーションを接続する。
- ソリューションの計画立案、アーキテクチャーおよびガイダンス。
- サイバー・セキュリティの最新動向に関する洞察。
- IBM が推奨するアプローチおよび手法。

### 1.3.4 IBM Cloud Identity Expert On Demand

このサービスでは、開始後 30 日以内に 2 時間単位のセッションで 20 時間のプロフェッショナル・サービスが提供されます。このサービスでは、クラウド ID アーキテクトが疑問に回答し、ガイダンスおよび推奨を提供します。以下が含まれますが、これらに限定されません。

- お客様のクラウド ID ソリューションの実装を強化するためのテクニカル・スキル。
- お客様のクラウド ID ソリューションに関する設計上および実装上の疑問。
- お客様のクラウド ID のソリューション/戦略に関するガイダンス。

## 2. データ処理およびデータ保護に関するデータ・シート

IBM のデータ処理補足契約書 (<http://ibm.com/dpa> に公開。「DPA」)のほか、以下のリンクの「データ処理およびデータ保護に関するデータ・シート」(データ・シートまたは「DPA 別表」)にも、「クラウド・サービス」およびそのオプション(処理対象の「コンテンツ」の種類、対象となる処理活動、データ保護機能、および「コンテンツ」の保存および返却についての仕様に関連)に関する追加的なデータ保護情報が記載されています。DPA は、i) EU 一般データ保護規則 (EU/2016/679) (GDPR)、または ii)

<http://ibm.com/dpa/dpl>に記載されているその他のデータ保護法が適用される場合に、その適用範囲に限り、「コンテンツ」に含まれる個人データに適用されます。

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D>

### 3. サービス・レベルおよびテクニカル・サポート

#### 3.1 サービス・レベル・アグリーメント

IBM は、以下の可用性のサービス・レベル・アグリーメント (以下「SLA」といいます。) をお客様に提供します。IBM は、下表のとおり、「クラウド・サービス」の累積的な可用性に基づき、適用しうる最大の補償を適用します。「可用性」は、契約月における分単位の総時間数から、契約月における「サービス・ダウン」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。「サービス・ダウン」の定義、請求のプロセス、サービスの可用性の問題に関して IBM に連絡する方法については、IBM の SaaS サポートの概要 ([https://www.ibm.com/software/support/saas\\_support\\_overview.html](https://www.ibm.com/software/support/saas_support_overview.html)) に掲載されています。

可用性	クレジット (月額サブスクリプション料金のパーセント*)
99.9% 未満	10%

\*サブスクリプション料金は、請求対象月に関して約定した料金です。

##### 3.1.1 本「SLA」に関するその他の情報

お客様の期間の最初の 60 日の間 (以下「バーンイン期間」といいます。) は、本契約に基づく最低 99.9% の「実行可能時間パーセンテージ」を達成するために、お客様は IBM Cloud Identity 環境の障害によるクレジットの資格を与えられないものとします。バーンイン期間の前またはその期間中に、IBM Cloud Identity Service への移行が予定される既存のお客様構成、ポリシー、データまたはコード (以下「既存コンポーネント」といいます。) のうち、IBM Cloud Identity Service で本契約に含まれた「実行可能時間パーセンテージ」を順調に達成することを妨げるものを IBM が特定した場合、IBM は、お客様に対し、当該の「既存コンポーネント」について通知し、IBM の独自判断で SLA の条件からそれらを除外する権利を留保します。IBM がお客様に対し、除外された「既存コンポーネント」について通知した場合、IBM は可能な限り、除外された当該コンポーネントが本契約の「実行可能時間パーセンテージ」を満たすことができるように、お客様に改善計画を提示する責任を負うものとします。両当事者が別途合意した場合を除いて、お客様は当該改善の費用に対して全責任を負うものとします。

#### 3.2 テクニカル・サポート

「クラウド・サービス」のテクニカル・サポート (サポート窓口の連絡先情報、重大度レベル、サポート利用可能時間、応答時間、その他のサポート情報およびサポート・プロセスなど) を参照するには、IBM サポート・ガイド (<https://www.ibm.com/support/home/pages/support-guide/>) の「クラウド・サービス」を選択します。

### 4. 料金

#### 4.1 課金単位

「クラウド・サービス」の課金単位は、「個別契約書」に記載されます。

以下の課金単位が本「クラウド・サービス」に適用されます。

- 「許可ユーザー」とは、直接または間接のいかなる方法においても (例えば、多重化プログラム、デバイスまたはアプリケーション・サーバーを通じて) 「クラウド・サービス」へのアクセス権限を付与されている特定のユーザーを指します。
- 「従業員」とは、「クラウド・サービス」へのアクセスが与えられているか否かを問わず、お客様の「エンタープライズ」で雇用されている、またはお客様の「エンタープライズ」から支払いを受けている、もしくはお客様の「エンタープライズ」の代理を務める特定の個人です。

- 「適格参加者」とは、「クラウド・サービス」が管理または追跡するサービス提供プログラムに参加できる個人または法人です。
- 「インスタンス」は、「クラウド・サービス」の特定の構成への各アクセスを意味します。
- 「エンゲージメント」とは、「クラウド・サービス」に関するプロフェッショナル・サービスまたはトレーニング・サービスです。
- 「イベント」は、「クラウド・サービス」が処理する、または「クラウド・サービス」の利用に関連する、特定のイベントが1回発生することをいいます。
  - Cloud Identity Connect では、「イベント」は、「クラウド・サービス」に対する http リクエストです。
  - Cloud Identity Verify では、「イベント」は、「クラウド・サービス」によって呼び出される多要素方式です。

## 5. 追加条件

2019年1月1日より前に締結されるクラウド・サービス契約書(または同等のクラウド基本契約)については、<https://www.ibm.com/acs> に掲載されている条件を適用します。

### 5.1 お客様事例

お客様は、IBM が広報活動またはマーケティングのコミュニケーションにおいて、お客様を「クラウド・サービス」の利用者として公に言及できることに同意します。

### 5.2 イネープリング・ソフトウェア

「クラウド・サービス」には以下の「イネープリング・ソフトウェア」が含まれます。

以下のイネープリング・ソフトウェアは、IBM Cloud Identity Connect、IBM Cloud Identity Connect and Verify、および IBM Cloud Identity Connect Verify and Govern の「クラウド・サービス」とのみ併用できます。

- IBM Security Access Manager Virtual Enterprise Edition

以下のイネープリング・ソフトウェアは、IBM Cloud Identity Govern および IBM Cloud Identity Connect Verify and Govern の「クラウド・サービス」とのみ併用できます。

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

以下のイネープリング・ソフトウェアは、IBM Cloud Identity Analyze の「サービス」とのみ併用できません。

- IBM Cloud Identity Analyze のオンプレミス・アナリティクス・エンジン

### 5.3 確認

お客様は、i) IBM およびその独立監査人がお客様の本契約の遵守状況を確認するために合理的に必要な記録、システム・ツールの出力を保管し、要求に応じて提供するものとします。また、ii) かかる確認の結果必要と判断された使用許諾を、IBM のその時点における最新の料金ですみやかに注文して支払うほか、その他の料金および債務を、IBM の請求書の記載に従い支払うものとします。これらの遵守状況の確認義務は、該当する「クラウド・サービス」の有効期間中および期間後の2年間有効に存続します。