クラウドサービス

セキュリティホワイトペーパー

ＣＳアカウンティング株式会社

2024 年 12 月 1 日　第 4 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」といいます）は、ＣＳアカウンティング株式会社（以下「ＣＳアカウンティング」または「当社」といいます）のクラウドサービス（以下「ＣＳクラウド」といいます）を既にご利用中の方およびご利用を検討される方に向けて、ＣＳクラウドのセキュリティへの取り組み、または実装されているセキュリティ対策についてご理解頂くことを目的としています。

1.2. セキュリティへの取り組み

ＣＳアカウンティングでは、経理・人事のアウトソーシング事業者としてお客様が大切な情報を安心してお取り扱いして頂けるよう、情報セキュリティ対策に積極的に取り組んでおります。当社では「情報セキュリティ基本方針」や「プライバシーポリシー」を定め、すべての従業員に対して定期的にセキュリティ教育・訓練を実施しております。
また、情報セキュリティマネジメントシステム（ISMS）の国際規格である ISO/IEC27001:2022(JIS Q 27001:2023)を取得しております。
情報セキュリティに対する取り組みは、当社ホームページ上でも紹介しております。

- ＣＳアカウンティング株式会社｜情報セキュリティへの取り組み
  https://www.cs-acctg.com/isms/

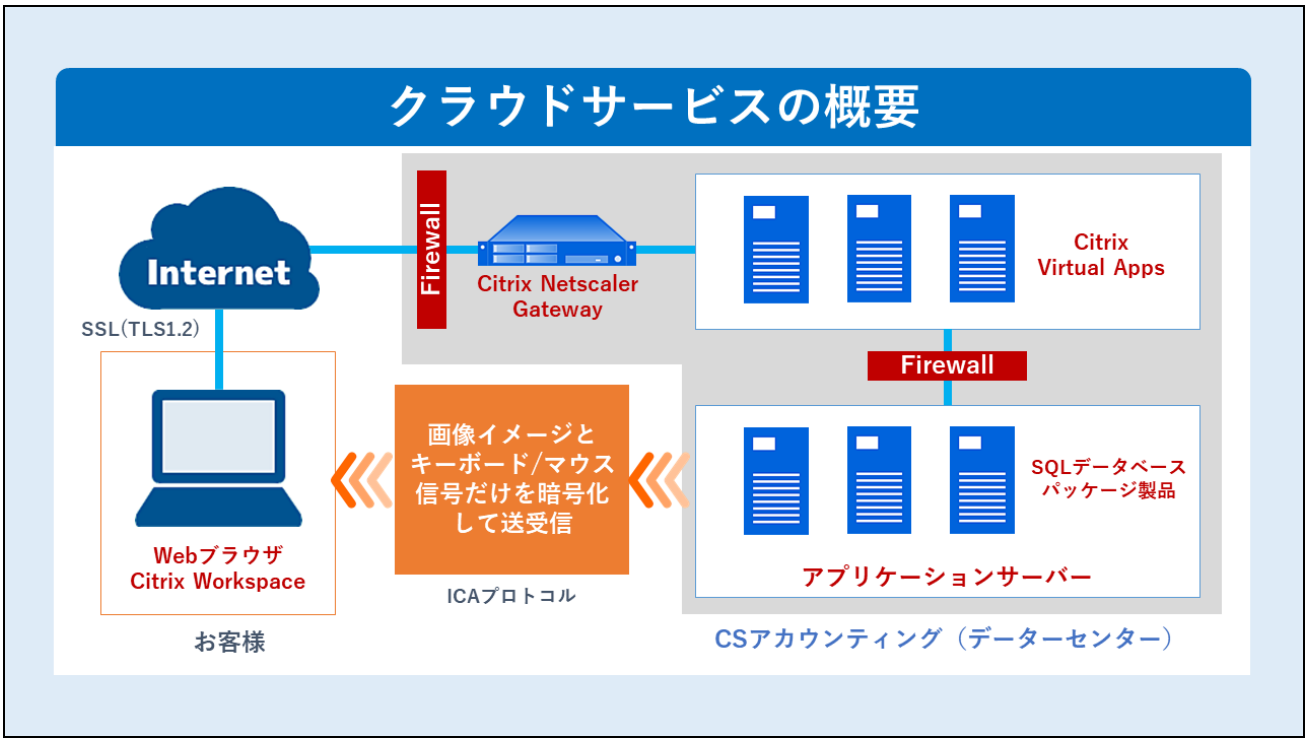
1.3. 本書の適用範囲

本書の適用範囲はＣＳクラウドに限定しています。本書はＣＳクラウドの構成、設備、アプリケーション、運用、セキュリティ対策について説明しています。

2. ＣＳクラウドの概要

2.1. ＣＳクラウドの構成

ＣＳクラウドを構成するシステムは東京に位置し、日本国内向けにサービス提供しています。また、カスタマデータは後述する東京都内のデータセンターに保管されます。
ＣＳクラウドの構成概要は下図の通りです。



（図 1：ＣＳクラウド概要図）

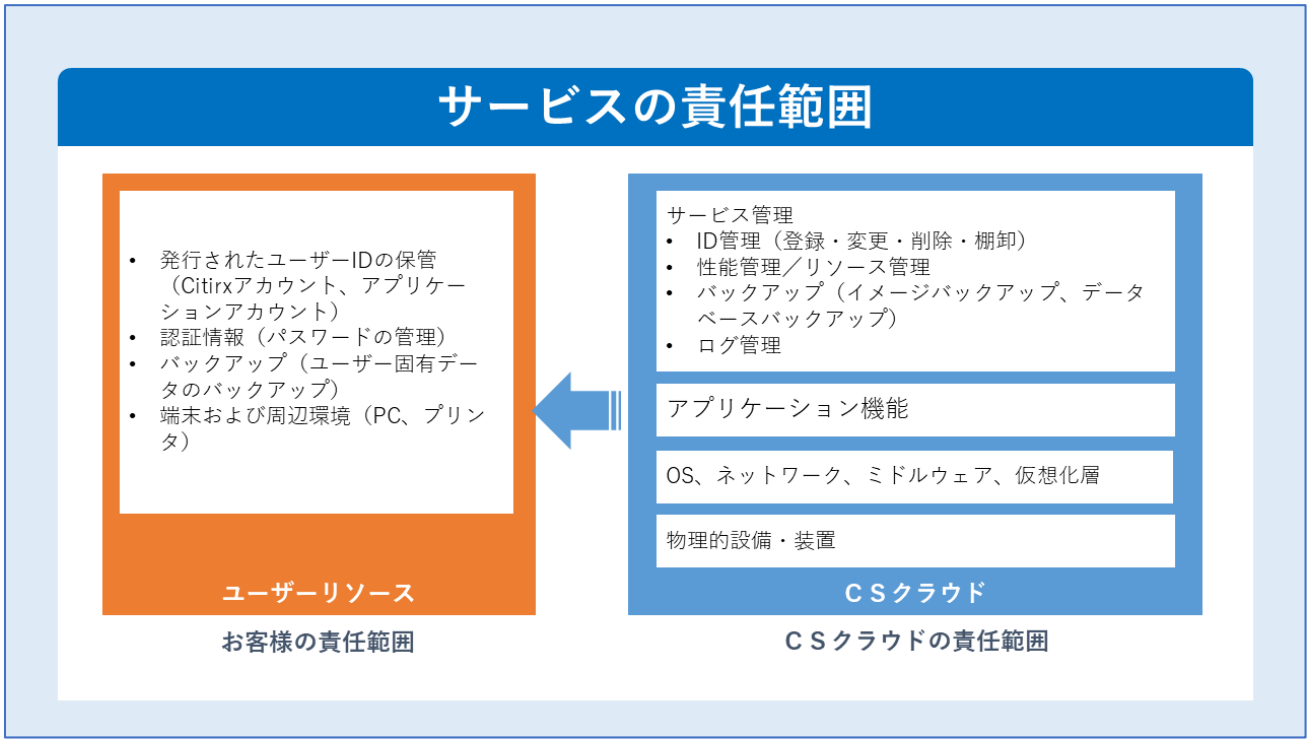
2.2. ＣＳクラウドの特徴

- ＣＳクラウドは米シトリックス社の製品(※)を採用した SaaS 型の安全なサービスを提供しています。シトリックス社の独自プロトコルである ICA プロトコルを使用することで、サーバ側で動作する画面のイメージとキーボード／マウス信号のみを通信するため、クライアント側の PC に不要なデータが残りません。
- 通信経路上は TLS プロトコルによって暗号化されます。暗号化プロトコルは TLS1.2 のみを採用し、脆弱性のある SSL2.0、SSL3.0 および TLS1.0、TLS1.1 は対応していません。

※ シトリックス社正式名称「Citirix Systems,Inc.」。Citrix Workspace および Citrix Virtual Apps は Citrix Systemx,Inc.の登録商標または商標です。

2.3.　ＣＳクラウドの責任範囲

下図にＣＳクラウドの責任範囲とお客様（以下「ユーザー」といいます）の責任範囲の概要を記します。



（図 2：ＣＳクラウド責任範囲）

ＣＳクラウドは SaaS 型のクラウドサービスです。ＣＳクラウドは、物理的設備から OS およびネットワーク層、アプリケーション機能、サービス管理までを責任範囲として提供します。
ユーザーは利用者の ID 管理、パスワード等の管理、ユーザー固有のデータバックアップなどが責任範囲となります。
なお、上記のネットワークはＣＳクラウド内部のネットワークに限定され、ユーザーリソースとＣＳクラウド間の外部ネットワークについては責任の範囲ではありません。
また、「2.4　ＣＳクラウドが提供するパッケージ製品」に該当するソフトウェアの瑕疵・バグに関しても責任の範囲ではありません。

2.4.　ＣＳクラウドが提供するパッケージ製品

ＣＳクラウドが提供するパッケージ製品は以下になります。

- メーカー：株式会社オービックビジネスコンサルタント（以下、OBC）
  製品：奉行 V ERP11 シリーズ

3. ＣＳクラウドにおける物理的セキュリティ対策

3.1. データセンターについて

CS クラウドはセコムトラストシステムズ株式会社の「セキュアデータセンター」（以下、「データセンター」といいます）の設備を使用しています。以下、セコムトラストシステムズ株式会社様ご協力により、データセンターの設備・環境を記載いたします。

3.1.1 ロケーション

東京都内にあるデータセンターは、都心からのアクセスが 30 分圏内の立地であり、地震による被害や液状化のリスクが低いエリアに位置し、海抜 50m以上で水害や津波の恐れが極めて低い安定した地盤に立地しています。また、東京都が公表している「地域危険度測定調査」でも安全性が最も高い「ランク 1」とされています。

3.1.2 地震対策

データセンターは免震構造の建物であり、震度 7 の地震に対してデータセンター機能を維持する構造となっています。また、架台はスラブにアンカー固定し、サーバラックは架台にボルトによる耐震固定を行っています。

3.1.3 水害・防水対策

データセンターは海抜 50m 以上および海岸からの直線距離約 18km に位置し、水害や津波の恐れが極めて低い地域となります。また、建物内は床防水塗装や漏水センサーなど必要な対策が行われています。

3.1.4 火災対策

データセンター内は自動火災報知設備、サーバ室・電気室には超高感度煙感知器が設置されております。サーバ室・電気室は窒素ガス消火により、サーバおよびその他機器類に損傷を与えない設備となっています。

3.1.5 落雷・電磁波対策

データセンターは直撃雷および側雷の対策をしています。また、特高受電設備には特高最大耐電圧 72KVA の誘導雷対策をしています。また、電磁波を発生させる電力設備（送電線等）からも離れており、サーバ室内の壁内には銅箔による電磁波シールドを施しています。

3.1.6 電源設備

データセンターは異なる 2 カ所の変電所からの給電ルートを確保しており、建物内は完全二重化されています。また、UPS および非常用発電機を N＋1 の冗長構成で設置しており、停電時においても継続的な電力供給を行うことを可能としています。

3.1.7 空調設備・防塵対策

データセンターの空調設備は空冷方式を採用し、水配管はありません。床吹き上げ式のサーバ室専用空調としており、N+1 の冗長構成により機器のメンテナンスや故障時にも継続して適切な温度・湿度の提供が可能な設計となっています。
また、サーバ室内のスラブ床に防塵塗装を施し、粉塵の発生を抑制しています。

3.1.8 防犯設備

データセンターはビル全体の防犯設備、監視体制および中央監視室を有した建物となっています。監視カメラは各室出入口およびサーバ室までの入館者の動線に添って設置しており、録画データは 1.5 年間保存しています。監視カメラ記録は週次にてチェックを行っています。
また、セコムの常駐警備員を配置し、24 時間 365 日体制で手荷物検査、X 線検査、金属探知機検査による入館チェックを行っています。
サーバ室内のラックは、電子錠、扉センサー、IC カードリーダーによりこじ開けや解放放置を検知する設備となっています。

3.1.9 入退館管理

データセンターの入退館は、入退受付管理システムによって事前申請を必要としています。データセンターへの入館においては、IC カード認証、生体認証（静脈認証、ウォークスルー顔認証)、ローターゲート（共連れ防止）にて不正な侵入を防御、X 線検査機、金属探知機を設置し、持ち込み、持ち出しチェックを有人にて実施しています。なお、入退館の記録は 1.5 年間保管しています。

3.2. 物理的装置について

CS クラウドを構成するサーバ、ストレージ、ネットワーク機器、回線等の機器・設備は、障害や事故、災害に備えてサービスを維持継続するために適切に管理されています。

3.3.1 サーバ・ストレージ

CS クラウドを構成するサーバは、ハイパー・コンバージド・インフラストラクチャ（以下「HCI」といいます）による複数ノードから構築されており、機器の一部または 1 台の機器全体の障害に対して影響なくサービスを継続可能となっています。
ストレージは RAID5 または RAID6 相当の冗長化を行って耐障害性を高めています。
物理的なサーバ・ストレージは適切に構成管理され、必要に応じた保守を実施しています。

3.3.2 ネットワーク機器・回線

CS クラウドを構成するネットワーク機器および回線は、二重化または予備機・予備回線により冗長構成となっています。CS クラウドのサービスを提供するメインのサイト以外に、非常用サイトを準備し、障害時のサービス継続を維持しています。

4. ＣＳクラウドのサービス構成

4.1. 概要

ＣＳクラウドはユーザーリソースの機密性、完全性、可用性を意識した設計およびサービス提供を行っています。

4.1.1 機密性

ＣＳクラウドは単一の仮想マシン上に複数のユーザー領域を含むマルチテナント方式となっていますが、ユーザー領域は厳格に分離されており、権限の無いユーザーがアクセスすることはできません。また、ユーザーとの契約に関する情報など特に重要なデータについては、ＣＳクラウドを構成するシステム内には保持していません。なお、ユーザー側に割り当てられた権限に関する機密性については、ユーザーにより適切な対策を行ってください。
ＣＳクラウドはユーザーリソースのデータ漏えいが生じないように防止策を施しています。

4.1.2 完全性

ＣＳクラウドはユーザーリソースについてデータ保護を実施し、厳重な管理を行っています。コンピューターウイルス等の不正プログラムによる被害を防ぐため、サービス管理で使用する機器について、ウイルスチェック・脆弱性チェックなどのセキュリティ対策を実施しています。インシデントが発生した場合は、定められた手順に従い、報告・調査・駆除・再発防止を実施しています。なお、ユーザー側に割り当てられたユーザーリソースへの完全性については、ユーザーにより適切な対策を行ってください。

4.1.3 可用性

ＣＳクラウドではそれぞれのユーザーリソースは分離しており、また、ユーザーリソースとサービス管理のための領域を、ネットワークを含め分離することで障害時の影響範囲を限定しています。
ＣＳクラウドでは障害が発生した場合に備え、機器および回線の冗長化、バックアップおよびシステム監視などの対策を施しています。また、障害発生時の回復についても手順を定めています。なお、ユーザーに割り当てられたユーザーリソースへの可用性については、ユーザーにより適切な対策を行ってください。

4.2. サービス管理

4.2.1 運用体制

ＣＳクラウドでは、サービス提供に携わる要員に対して、能力と責任に応じた教育・育成を実施しています。要員はそれぞれ、アカウント管理（発行、変更、削除、権限設定、棚卸など）、インフラ保守（機器、ネットワーク、仮想マシン、ＯＳ，端末、パッケージ製品、バックアップなど）、セキュリティ対応（ウイルス対策ソフト、ファイアウォール、不正アクセス対策など）、サービス監視（死活監視、パフォーマンス監視、リソース監視、ログ監視など）、問合せ対応などの役割を担っています。また、システムの運用に対して必要な権限のみを各担当の要員に割り当てています。
ＣＳクラウドの運用管理は、ＣＳアカウンティングのシステム部門が担当し、VPN 接続による機密性を保持した通信によって実施しています。

4.2.2 システムライフサイクル

ＣＳクラウドではシステムの導入に際して、機能および性能に関する評価を行った上で計画的に実施しています。システムは継続的な保守サポートが存在する条件で利用し、保守切れの際にリプレイスを行います。
システムの廃棄の際は、機密保護対策を含めた手順に則り実施しています。

4.2.3 システム保守

ＣＳクラウドのシステムを構成する機器、ネットワーク、ＯＳ、ミドルウェア、パッケージ製品、および運用管理のための端末などは、適切な保守を行っています。それぞれサポート契約、ベンダーとのリレーションシップ、バージョン管理を含むシステム管理を実施しています。

4.2.4 アカウント管理

ＣＳクラウドのアカウントは、別紙「ＣＳクラウドサービス利用申込書」（以下、「利用申込書」の情報に従って登録、変更、削除を行っています。

- 登録・発行

「利用申込書」の情報に従ってアカウントを登録し、ユーザーID と初期パスワードを発行いたします。契約期間内のユーザーID 追加の際も同様に「利用申込書」を提出する必要があります。
ユーザーID は「Citrix ログイン ID」および「パッケージ製品（奉行）用ログイン ID」の 2 種類があり、それぞれ初期パスワードを通知いたします。パスワードは初回ログイン時にユーザーによって変更する必要があります。

- 削除

契約期間内の一部のユーザーID の削除、および契約終了時のすべてのユーザーID の削除は、「利用申込書」の「解約」欄を選択し、提出して頂くことによって実施されます。

- 権限変更

アカウントの権限変更は、お問合せ窓口宛にメールにてご相談を承ります。

- 棚卸

ＣＳクラウドのアカウントは、定期的に棚卸を実施し、不要なアカウントおよび権限付与の防止を行っています。

4.2.5 サービス監視

ＣＳクラウドは、サービス提供を維持するための各機器（物理ホスト、ネットワーク、ストレージ等）およびプログラムが稼働する仮想マシンに対して、監視を実施しています。

- 死活監視

各機器および仮想マシンに対して一定間隔の ping チェックを自動的に行い、障害時に運用担当者にアラート通知します。

- パフォーマンス監視

各機器および仮想マシンの CPU 稼動状況を計測し、一定時間しきい値を超過した場合、運用担当者にアラート通知します。この場合、原因を調査し、要因の除去あるいはシステムの拡張を含む対策を行います。また、物理ホストに付随する管理ツールによって、物理的な環境変化やパーツの故障・劣化等に関する情報を運用担当者に通知することで、性能の低下を防止しています。

- リソース監視

各機器および仮想マシンのメモリ使用率、ディスク使用率を計測し、しきい値を超過した場合、運用担当者にアラート通知をします。この場合、原因を調査し、要因の除去あるいは静的または動的にリソースの拡張を行います。

- ログ監視

サービス提供に関連するログは、運用担当者によって定期的にチェックしています。

4.2.6 バックアップ

ＣＳクラウドのサービス提供に必要なシステムのバックアップは、定期的かつ厳重に実施されています。バックアップデータは、システム管理者のみに権限が割り当てられた領域に保存されます。ＣＳクラウドのバックアップデータは、不測のインシデント発生時に対し、可用性を維持するためにシステム管理が利用するものであり、ユーザーは直接バックアップデータを利用することは出来ません。ユーザー固有の領域におけるバックアップは、ユーザーにて取得してください。

なお、一部のバックアップデータは、致命的な障害に備え、別サイトにコピーを保存しています。

また、プログラム変更時等は臨時のバックアップを取得しています。

バックアップの種別は下記の通りです。

種別	サイクル	保管期限
仮想マシン	日次	7 日間
データベース（通常）	日次	7 日間
データベース（災害用）※1	月次	2 か月

※１：データベース（災害用）は別サイトにバックアップを取得しています。
※ユーザー個別領域のバックアップからのデータリストアをご要望される場合は、別途ご相談となります。

4.2.7 セキュリティ対応

ＣＳクラウドは、サービス提供を構成するシステムに対し、適切なセキュリティ対応を実施しています。

- ＯＳ・ミドルウェアのパッチ対応

ＯＳ、ミドルウェアの脆弱性に関する修正プログラム（パッチ）は、影響範囲を検証し、適時適用しています。

- ウイルス対策

仮想マシンおよび運用担当の端末は、ウイルス対策ソフトを導入し、最新状態を保つよう実施しています。

- ファイアウォール

ネットワーク機器、仮想マシン、端末は、それぞれ不要なプロトコルおよび通信ポートを解放しないファイアウォールを設定しています。

- 不正侵入・出口対策・サイバー攻撃

ＣＳクラウドのネットワークは、アプリケーション識別、UTM 機能、未知のマルウェア検知など多層防御が可能なファイアウォール機器を設置することで、不正侵入、出口対策およびサイバー攻撃に備えています。

- 暗号化

ＣＳクラウドの通信経路上のデータは TLS1.2 プロトコルによって暗号化され、保護されます。
ユーザーはこの暗号化方式が自社のルールや法令規制に則しているかご確認ください。

- 第三者機関によるセキュリティ診断

ＣＳクラウドは、第三者機関によって定期的にセキュリティ診断を実施しています。診断結果によって脆弱性が報告された際は、サービスに影響がない範囲で対策を実施しています。

- セキュリティ教育

ＣＳアカウンティングでは、全従業員に対し定期的に情報セキュリティ教育を実施しています。さらに、ＣＳクラウドの運用担当者は、外部機関（JPCERT 等）やメーカーからの最新のセキュリティ情報を共有し、迅速な対応が可能な体制を整えています。

4.2.8 ログの管理

ＣＳクラウドの各種ログは、インシデント発生時や問合せ時などトレーサビリティ向上のため、運用担当者またはユーザーが利用可能なよう、適切に取得し、一定期間保存しています。
また、運用担当者の端末には不正操作防止の目的のため、画面録画による記録も保存しています。

種別	閲覧可能	保管期限
イベントログ	担当者（※1）	6 か月（機器によって異なる）
操作ログ（奉行）	担当者およびユーザー	1 年
SYSLOG（ネットワーク機器など）	運用管理者（※2）	6 か月（機器によって異なる）

※１：CS クラウドのサポート担当者
※２：CS アカウンティングシステム部の運用管理者

4.2.9 時刻同期

ＣＳクラウドのシステムは、下記の NTP サーバに時刻同期を行っています。
ntp1.jst.mfeed.ad.jp / ntp.nict.jp

4.2.10 開発環境

ＣＳクラウドは、ミドルウェアとパッケージ製品の組み合わせによって提供されるサービスであり、ＣＳアカウンティングではプログラムの開発は行っていません。
しかし、ユーザーから提供される初期導入時のデータコンバート処理はご相談により対応しております。
コンバート対応やパッケージ製品のアップデート検証に利用する開発環境は、本番環境とネットワークを分離し、影響を及ぼさない対策を実施しています。

4.2.11 問合せ対応

ＣＳクラウドの問合せ対応は、メールもしくは電話にて承っています。問合せ対応の範囲は、契約・解約に関する事項、アカウントに関するお問合せ、不具合・障害に関するお問合せとしています。
パッケージ製品（奉行）の利用方法に関するお問合せは、メーカー窓口をご案内しています。
当社ウェブサイト（https://www.cs-acctg.com/cloud/）の「ご質問・お問い合わせ」をご参照ください。

4.2.12 インシデント管理

ＣＳクラウドにおけるインシデント発生には、手順に基づき関係者への情報伝達を行い、調査・対応を行っています。インシデント情報をユーザーに提供する手順および基準は次の通りです。
・ 開示レベル：ユーザーリソースに影響を及ぼす可能性のあるインシデント、またはデータ侵害の可能

性のあるインシデント発生時。機密情報に抵触しないレベルの開示
・ 通知手段：当社ウェブサイトまたはメール
・ 通知までの目標時間：4 時間
・ ユーザーがインシデントを検知した際の報告先：当社問合せ窓口（「4.2.11 問合せ対応」参照）

なお、ユーザーが情報セキュリティ事象の状況を追跡する目的のため、お客様のご協力が必要な場合があります。その場合は別途方法・手段等をお知らせいたします。
また、サービスに影響しない軽微なインシデント（機器パーツの故障および予防交換など）を含め、インシデント発生の情報を社内データベースに記録・蓄積し、障害の再発防止に努めています。

4.2.13 サービス利用制限

ＣＳクラウドは、SaaS 型マルチテナント方式サービスのため、パッケージ製品が有する機能の一部を提供できない場合があります。また、ユーザーの端末環境によって、利用が限定される場合があります。
詳細は「附属Ａ：サービス利用制限事項」をご参照ください。

4.2.14 利用契約終了後の措置

解約その他の事由によりＣＳクラウドの利用契約が終了した後、本サービスにより当該ユーザーによってサーバに格納されたデータは原則としてすべて消去いたします。
ただし、他の業務委託契約等が継続する場合や、法令に基づいた保存管理を要望される場合は、別途ご相談となります。
なお、以下のＣＳクラウド派生データについては、個別のユーザー情報を分離することができないため、保管期限まで情報が保有されます。
・ システムバックアップ（仮想マシン、データベース）
・ ログ（イベントログ、操作ログ）
・ インデックス情報

4.2.15 供給者関係／ICT サプライチェーン

ＣＳクラウドを構成する設備・製品の選定は、客観的に評価し、セキュリティ面の水準を満たした ICT サプライチェーンを選定しています。ICT サプライチェーンとはパートナー契約を結び、契約範囲内で製品を利用したサービスをＣＳクラウドに適用しています。
また、システムの運用等を外部委託する場合は、事前に目的や範囲などを明らかにし、安全性保護のため、機密保護を盛り込んだ委託契約を締結しています。

4.2.16 規約・SLA

ＣＳクラウドを利用するためには、「クラウドサービス利用規約」への同意が必要となります。
また、ＣＳクラウドは「クラウドサービス利用規約」第 10 条に記載された内容の品質保証制度（SLA）を提供しています。SLA の目安として、月間稼働率を当社ウェブサイトに掲載しております。SLA の詳細は「クラウドサービス利用規約」をご参照ください。

4.2.17 法制度

ＣＳクラウドは「クラウドサービス利用規約」において、準拠法を日本法とし（第 22 条)、専属的合意管轄裁判所を東京地方裁判所（第 21 条）としています。電気通信事業法、個人情報保護法、不正アクセス禁止法などの情報セキュリティに関する法令、規範およびガイドラインを順守して運営しています。

4.2.18 メンテナンスおよび通知

ＣＳクラウドでは、ユーザー向けの情報としてメンテナンス・障害情報などの情報、および変更管理に関する通知を当社ウェブサイトおよびメールにてお送りいたします。メンテナンスのお知らせは、1 か月前を目安としています。ただしパッケージ製品のアップデートに伴う「臨時メンテナンス」や、障害発生時の「緊急メンテナンス」はこの限りではありません。また、定期メンテナンス（日次 0:00〜6:00）についてはアナウンスいたしません。

5. ユーザーに提供されるセキュリティ機能

5.1. ログイン ID およびパスワード

ＣＳクラウドを利用するためには、ユーザー1 名に対し、2 つのログイン ID とパスワードが発行されます。発行された ID およびパスワードは、不正利用を防止するためにも大切に保管してください。
パスワードは以下の条件にて変更が可能です。

5.1.1 パスワードポリシー

- ログイン ID：Citrix ログイン ID

パスワードの文字数：8 文字以上
パスワードの複雑さ：英語大文字、英語小文字、数字、記号のうち 3 種類以上
パスワードの有効期限：90 日（機能上の制限により設けていない場合があります）
パスワード履歴：過去 2 回まで利用したパスワードは設定不可

- ログイン ID：奉行ログイン ID

パスワードの文字数：8 文字以上
パスワードの複雑さ：英語大文字、英語小文字、数字、記号のうち 3 種類以上
パスワードの有効期限：90 日
パスワード履歴：過去 3 回まで利用したパスワードは設定不可

- アカウントロック

Citrix ログイン ID：5 回
奉行ログイン ID：5 回
アカウントロックの解除はＣＳクラウドお問合せ窓口にメールにてご依頼ください

- パスワード初期化

パスワードを忘れてしまった、あるいは利用者変更による ID 再利用時等の場合には、パスワード初期化のご依頼をＣＳクラウドお問合せ窓口にメールにてご依頼ください。

※アカウントロック解除およびパスワード初期化のご依頼に対して、サポート窓口担当者は顧客情報を元にご本人確認を行った上で対応いたします。

5.2. 操作ログ表示

ＣＳクラウドでは、奉行シリーズ製品に付属する「操作ログ表示」機能をご利用可能です。

- 奉行シリーズ

メインメニューから「管理ツール」→「操作ログ表示」にて操作ログを閲覧可能です。

5.3. メニュー権限

ＣＳクラウドでは、奉行シリーズのメニュー権限を変更することができます。メニュー権限の変更はサポート窓口までご相談ください。

5.4. バックアップ

ＣＳクラウドではお客様固有のデータ領域を、適時バックアップすることが可能です。
奉行シリーズの場合はメニューの「随時処理」－「バックアップ」を選択してください。
（ただし、ユーザーID が「参照権限」のみのご契約の場合は、バックアップ機能をご利用出来ません。）

5.5. ラベル付け

ＣＳクラウドの奉行シリーズにおいて、データ領域のラベル機能として以下の変更が可能です。

・ メインメニューから「導入処理」－「会社情報登録」
・ 「会社名」「会社コード」の編集が可能
※ 変更される場合は、サポート窓口までご連絡ください。

6. 附属 A ：サービス利用制限事項

6.1. OBC 奉行シリーズで利用できない機能

- 奉行M y スペースおよび関連機能
- コミュニケーションツール「LinkIT」および関連機能
- メール送受信機能
- 領域の新規作成
- バックアップ復元
- サードパーティ製アドイン製品

6.2. Citrix ユーザー環境における不具合

- デュアルモニター環境（サブ画面に不具合が生じる場合があります）

7. 改訂履歴

版数	日付	変更内容
初版	2019/04/01	初版作成
第 2 版	2019/06/25	・「2.ＣＳクラウドの構成」にカスタマデータの保存場所を追記 ・「4.2.12 インシデント管理」にインシデント発生時の開示レベルを追記 ・「4.2.14 利用契約終了後の措置」にクラウド派生データに関する内容を追加 ・「4.2.18 メンテナンスおよび通知」に変更管理に関する情報の通知を追記 ・「5.5 ラベル付け」追加
第 3 版	2022/11/1	・「2.4. ＣＳクラウドが提供するパッケージ製品」について VERP11 へのバージョンアップに伴い、名称変更 ・「4.2.6 バックアップ」のデータベース（通常）の保管期限を修正 ・「4.2.8 ログの管理」イベントログの保管期限を修正
第 4 版	2024/12/1	・「1.2 セキュリティへの取り組み」 JISQ27001:2014/ISO/IEC27001:2013 を JISQ27001:2023/ISO/IEC27001:2022 に変更 ・「4.2.8 ログの管理」イベントログの保管期限を修正