ISM CloudOne
セキュリティ運用方針（4版）

2024年5月22日

クオリティソフト株式会社
http://www.qualitysoft.com/

目次

1. 概要

1.1. はじめに

本書は、ISM　CloudOne再販版サービス（以下本サービス）のセキュリティ運用方針について記しています。

2. セキュリティ運用方針

2.1. 利用者との責任分界点

本サービスのセキュリティは、当社と利用者様の責任範囲を定め、それぞれの役割を分担し対策する考え方（共同責任モデル）にて実施いたします。

2.1.1. クオリティソフト（以下当社）の責任

当社は本サービスにおいて、以下のセキュリティ対策を実施します。

・本サービスを提供するプログラムおよびミドルウェアの脆弱性対応
・本サービスユーザーコンソールのセキュリティ対策
・クライアントプログラムからのデータ通信処理についてのセキュリティ対策

2.1.2. 利用者様の責任

利用者様は、本サービスユーザーコンソールにログインするための管理者アカウントにおいて、以下のセキュリティ対策を実施する必要があります。

・管理者アカウントの適切な管理（登録、削除、各種権限の設定）
・パスワードの適切な管理

2.2. データの保管場所

お客様にご利用いただくにあたり、本サービスにて収集するデータは下記クラウドベンダーのデータセンターに保管しています。

データ保管場所：Amazon Web Services（以下、AWS）　日本国　東京リージョン

2.3. データの削除

本サービスの解約手続きなどをおこなった場合、本サービスにて収集したお客様のデータ（カスタマデータ）を削除いたします。削除したカスタマデータにつきましては復旧できません。
削除する条件、タイミングおよび対象となるデータは次項とします。

データを保存している物理装置の再利用、処分については、AWSのポリシーに準拠しています。
（https://aws.amazon.com/jp/compliance/data-center/controls/　デバイスの管理を参照）

2.3.1. 削除する条件

本サービスの解約処理を実施済みであること

2.3.2. 削除するタイミング

本サービス解約日より60日経過後即時

2.3.3. 削除対象

本サービスをご利用時にお伝えする企業コードに紐づくすべてのカスタマデータ

2.4. ラベル付け

本サービスにてグルーピングができる項目を記します。

2.4.1. 組織

「組織」として、「グループ」と「ユーザー」を設定できます。
登録したクライアントを、グループ毎またはユーザー毎にグルーピングが可能です。

2.4.2. 個別ポリシー

登録したクライアントに適用したいポリシーを個別に追加し、グルーピングが可能です。

2.5. 管理者登録、削除および権限の管理

2.5.1. 管理者登録

本サービス開始時にお伝えする初期設定アカウントにて、以降のサービスを利用する際に使用する管理者の登録が行なえます。

2.5.2. 管理者削除

登録した管理者情報は、いつでも削除が可能です。ただし、削除にあたっては削除したい管理者以外の管理者にてユーザーコンソールにログインする必要があります。

2.5.3. 管理者権限の管理

管理者の権限を、設定し管理することができます。権限の詳細はマニュアルを参照ください（複数選択が可能です）。

また、作成したグループを選択することで、選択したグループに対してのみの権限を設定することができます。

2.6. パスワードの管理

管理者のパスワードは、管理者登録時に設定できます。パスワードの変更は、ユーザーコンソールにログインした際、または、別の管理者にてログインした際に変更できます。

2.7. 暗号化の対象

本サービスで暗号化の対象は下記です。
・ユーザーコンソールへの接続にあたっては、SSL通信によって暗号化されます。
・ISMクライアントとISMサーバー間の通信は、SSL通信にて暗号化 または、データを暗号化した上でhttp通信にて送信しています。

・ユーザーコンソールにログインする管理者アカウントのパスワードは、暗号化されて保存しています。

2.8. サービス稼働状況の管理

本サービスの稼働状況は、下記URLのメンテナンス情報サイトに公開しています。
・「https://www.qualitysoft.com/product/supports/notice/」

2.9. 変更の管理

本サービスの停止をともなうメンテナンス作業については、下記にてお知らせしています。
緊急時を除き、原則作業の2週間前にお知らせいたします。
・ユーザーコンソールのおしらせ
・登録いただいているお客様情報にたいしてのメール告知
・「https://www.qualitysoft.com/product/supports/notice/」　のメンテナンス情報サイト

2.10. マニュアルのご提供

本サービスの各機能をご利用にあたってのマニュアルは、ユーザーコンソールよりご利用可能です。
マニュアルは、ユーザーコンソール上で利用できるオンラインマニュアルとダウンロードしてご利用いただくPDF形式の2種類がございます。
また、ユーザーコンソールから本サービスにおいての制限事項（PDF形式）もダウンロードしてご利用いただけます。

2.11. 本サービスのバックアップについて

本サービスのバックアップは、AWSが提供するスナップショット機能にて取得しています。
取得したバックアップデータは、AWSの高可用、高耐久性ストレージのS3サービスにて保管します。
バックアップは、本サービス全体の復旧を目的として取得しています。このため、個々のお客様のデータを個別に復旧することはできません。
バックアップは仮想マシンのOS部分とデータ部分でそれぞれ下記ポリシーで取得、保持します。

OS部分	：	毎日6時に取得	7世代保持
データ部分	：	2時間おきに取得	36世代保持
		毎日6時に取得	15世代保持

またこれに加え、メンテナンス作業時の開始前、開始後に取得します。

2.12. サービスのクロック同期について

本サービスはAWSが提供するNTPサービスと同期しています。

2.13. 脆弱性管理について

当社は、本サービスを稼働させるにあたって利用しているOS、ミドルウェア等に関する脆弱性情報を、定期的に収集しています。
本サービスに利用しているOS、ミドルウェア等の脆弱性に対するパッチが公開された場合は、当社内で十分な検証をおこなった後、速やかに適用します。

2.14. 運用環境のセキュリティについて

本サービスはAWSのサービスをもちいてセキュリティ対策を実施しています。

2.15. サービス開発におけるセキュリティについて

サービス開発段階のプログラムに対して、第三者機関による脆弱性検証を実施しています。

2.16. セキュリティインシデント発生時の対応

セキュリティインシデントが発生した場合は、当社Webサイトのメンテナンス情報ページへ掲載いたします。あわせて、ご契約時に登録いただいたメールアドレス宛にメールでもご報告します。

セキュリティインシデントに対してのお問い合わせは、下記リンク先よりご連絡ください。
https://www.qualitysoft.com/contact/

2.17. カスタマデータの保護および第三者提供について

カスタマデータについては、本サービスのデータベースサーバー内にて保管しています。
このサーバーに対してのアクセスは、当社内においてもサービス運用に携わる一部の者しかアクセスできないよう権限を設定しています。
ログデータについては、AWSの高可用、高耐久性ストレージのS3サービスにて保管しています。
こちらも同様にサービス運用に携わる一部の者しかアクセスできないよう権限を設定しています。
ただし、法令に基づき裁判所もしくは政府機関の命令等により開示が求められた場合には、カスタマデータを第三者へ開示することができるものとします。
カスタマデータの保護は利用者様の責任範囲においてデータのバックアップを行い実施するものとします。

2.18. 適用法令

利用者様と当社との契約に関する解釈は日本法に準拠いたします。

2.19. 認証

当社は、情報セキュリティマネジメントシステムの国際規格である「ISO/IEC27001:2013 / JIS Q 27001:2014」（https://isms.jp/lst/ind/CR_JQA-IM1459.html）および「ISO/IEC 27017:2015」（https://isms.jp/isms-cls/lst/ind/CR_JQA-IC0048.html）の認証を取得しています。

情報セキュリティマネジメントシステム認証登録範囲
　情報セキュリティパッケージソフトウェアの開発
　自社パッケージソフトウェアによるクラウドセキュリティサービスの提供
　自社パッケージソフトウェアによるクラウドセキュリティサービスの販売及びサポート
　ドローンの販売及び操作方法のトレーニング

ISMSクラウドセキュリティ認証登録範囲
　クラウドサービスプロバイダとして以下のサービスを提供
　　・ＩＴ資産管理
　　・エンドポイントセキュリティ管理ツール
　クラウドサービスカスタマとして以下のサービスを利用
　　・ＩａａＳ型システム開発運用環境

2.20. セキュリティに関する独立したレビュー

年一回、情報セキュリティマネジメントシステムおよび、情報セキュリティマネジメントシステムクラウドについてレビューを行ない、必要に応じて見直しを行っています。

レビューは弊社内担当部門に対して、内部監査をを実施し、予防や是正を行っています。
内部監査員は、ISO/IEC27001:2013内部監査員セミナー受講者、ISMSクラウドセキュリティ関連セミ

ナー受講者で構成されています。

2.21. 免責

当社が提供する本サービスは、外部のクラウドサービス（AWS／運営会社Amazon Web Service,Inc.）を利用しています。本書に記載したセキュリティ運用方針は、AWSのサービスに対して及ぶものではありません。また、AWSサービスに対して、本書の遵守を保証するものではありません。

改訂履歴

版数	改定日	改定内容
1.0	2020年5月11日	初版
2.0	2020年9月1日	「2.11本サービスのバックアップについて」の内容更新
3.0	2020年11月5日	「2.7暗号化の対象」の内容修正 「2.19認証」の内容追加
4.0	2024年5月22日	「2.20セキュリティに関する独立したレビュー」の内容更新

以上