

QUALITY SUITE
セキュリティ運用方針(1版)

2022年1月7日

クオリティソフト株式会社

<http://www.qualitysoft.com/>

目次

概要	2
はじめに	2
セキュリティ運用方針	2
利用者との責任分界点	2
クオリティソフト(以下当社)の責任	2
利用者様の責任	2
データの保管場所	2
データの削除	2
削除する条件	2
削除するタイミング	3
削除対象	3
ラベル付け	3
有償サービスにおけるグルーピング	3
無償サービスにおけるグルーピング	3
管理者アカウントの権限、登録および削除	3
管理者アカウントの権限	3
管理者アカウントの登録	3
管理者アカウントの削除	3
パスワードの管理	4
暗号化の対象	4
サービス稼働状況の管理	4
変更の管理	4
マニュアルのご提供	4
本サービスのバックアップについて	4
サービスのクロック同期について	5
脆弱性管理について	5
運用環境のセキュリティについて	5
サービス開発におけるセキュリティについて	5
セキュリティインシデント発生時の対応	5
カスタマデータの保護および第三者提供について	5
適用法令	5
認証	6
セキュリティに関する独立したレビュー	6
免責	6
改訂履歴	6

1. 概要

1.1. はじめに

本書は、QUALITY SUITEサービス(以下本サービス)のセキュリティ運用方針を記しています。

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クラウド基盤のセキュリティ対策
- ・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に保管しています。

データ保管場所: 日本国 東京都内および大阪府内データセンター

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、ISO27001に適合した当社の情報セキュリティマネジメントシステムの情報取扱規程に準拠しています。

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

2.3.3. 削除対象

本サービスをご利用時にお伝えするID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(有償・無償サービス)にてグルーピングができる項目を記します。

2.4.1. 有償サービスにおけるグルーピング

クライアントを分類する為、「組織」「グループ」「ユーザー」を設定し、クライアントを割り当てることで、組織・グループ・ユーザー毎にグルーピングをすることが可能です。

また、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、グルーピングをすることも可能です。

2.4.2. 無償サービスにおけるグルーピング

クライアントを分類する為、「組織」「グループ」を設定し、クライアントを割り当てることで、組織・グループ毎にグルーピングをすることが可能です。

2.5. 管理者アカウントの権限、登録および削除

2.5.1. 管理者アカウントの権限

管理者アカウントはシステム管理者と、それ以外の管理者に区別されます。

- ・システム管理者:すべての情報閲覧と運用設定が可能
- ・システム管理者以外の管理者:アカウントの管理対象組織の設定のみ可能

権限の詳細は本サービスのマニュアルをご参照ください。

2.5.2. 管理者アカウントの登録

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

2.5.3. 管理者アカウントの削除

登録した管理者アカウント情報は、いつでも削除が可能です。ただし、削除にあたってはシステム管理者のアカウント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。

2.6. パスワードの管理

管理者のパスワードは、管理者作成時に初回ログイン用パスワードを設定した後、ユーザーコンソールに初めてログインした際に更新する必要があります。また、ユーザーコンソールにログインした際、共通メニューからパスワードを変更できます。

2.7. 暗号化の対象

本サービスで暗号化の対象は下記の通りです。

- ・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。
- ・クライアントとサーバー間の通信は、SSL通信にて暗号化しています。
- ・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、暗号化されて保存されています。

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/QUALiTY_SUITE/support/maintenance/」

2.9. 変更の管理

本サービスの停止をとま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1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
- ・「https://www.qualitysoft.com/QUALiTY_SUITE/support/maintenance/」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、オンラインまたはユーザーコンソールにてご利用可能です。また、当社Webサイト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。

- ・マニュアル: <https://manual.qualitysuite.net/QSE/v1/>
- ・制限事項(PDF): https://www.qualitysoft.com/QUALiTY_SUITE/support/restrictions/

2.11. 本サービスのバックアップについて

本サービスは、スナップショットにてシステム全体のバックアップを取得しています。取得したバックアップデータは、バックアップ用ストレージに保管します。

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。

バックアップは下記ポリシーに沿って取得、保持します。

- | | | | |
|---------------|---|--------------|-------|
| OS部分 | : | メンテナンス時の実施前後 | 7世代保持 |
| 認証情報部分 | : | 1日毎に1回 | 7世代保持 |
| データ部分(認証情報以外) | : | 1日毎に1回 | 1世代保持 |

2.12. サービスのクロック同期について

本サービスはNICT(独立行政法人 情報通信研究機構)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

本サービスは社内の運用規程に従い、FWを用いたネットワークへの不正侵入の防止とDDoS保護、 サービスのパフォーマンス及びアラート監視等の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、当社にて運用するストレージ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/1st/ind/CR_JQA-IM1459.html) および「ISO/IEC 27017:2015」(https://isms.jp/isms-cl/1st/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

本サービスの認証は登録予定です。

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審査員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、国内業者のファシリティサービスを利用しています。本書に記載したセキュリティ運用方針は、該当のファシリティサービスに対して及ぶものではありません。また、該当のファシリティサービスに対して、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	2022年1月7日	初版
以下余白		

以上