ホワイトペーパー

tracpath

1.2 版

2025 年 2 月 26 日

株式会社オープングルーヴ

目次

1. はじめに 1
   1.1 ホワイトペーパーの目的 1
   1.2 ホワイトペーパーの対象 1
2. 第三者認証 1
3. 組織的管理策 2
   3.1 責任範囲（共有 Model） 2
   3.2 地理的所在地 2
4. 資産の管理 3
   4.1 情報のラベル付け 3
   4.2 サービス利用停止後のデータの扱い 3
5. アクセス制御 3
   5.1 利用者アクセスの管理 3
   5.2 認証情報の管理 3
   5.3 ユーティリティプログラム 4
6. 暗号 4
   6.1 暗号化 4
7. 運用のセキュリティ 4
   7.1 変更 4
   7.2 バックアップ 4
   7.3 ログ 4
   7.4 技術的脆弱性の管理 5
   7.5 管理者用手順 5
   7.6 クラウドサービスの監視 5
   7.7 容量・能力の管理 5
   7.8 装置のセキュリティを保った処分又は再利用 6
8. 通信のセキュリティ 6
   8.1 ネットワーク 6
9. システムの取得、開発及び保守 6
   9.1 情報セキュリティ機能 6
   9.2 開発プロセス 7
   9.3 サプライチェーン 7
10. 情報セキュリティインシデントの管理 7
   10.1 インシデント対応プロセス 7

10.2 インシデント対応 7
11. 順守 8
11.1 適用法令及び契約上の要求事項 8
11.2 証拠の収集 8
11.3 知的財産権 8
11.4 記録の保護 8
11.5 暗号化機能に対する規制 9
11.6 内部教育の実施 9
11.7 情報セキュリティのパフォーマンス評価 9
12. tracpath に関するお問い合わせ 9

1. はじめに

1.1 ホワイトペーパーの目的

tracpath は、エンジニアがソフトウェア開発に全力を注ぐための環境を整えるための当社のクラウドサービスです。ソースコードのバージョン管理やシステム開発に必要なナレッジを統合的に管理し、効率的なソフトウェア開発プロセスを実現します。

本ドキュメントは、tracpath の提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

1.2 ホワイトペーパーの対象

tracpath の導入を検討中の方
tracpath を利用中の方

2. 第三者認証

ISO/IEC27001
当社は、2024 年 4 月 16 日に ISMS（Information Security Management System）の国際規格である ISO/IEC27001・27017 を取得しています。

ICMS-SR0650 / JIS Q 27001

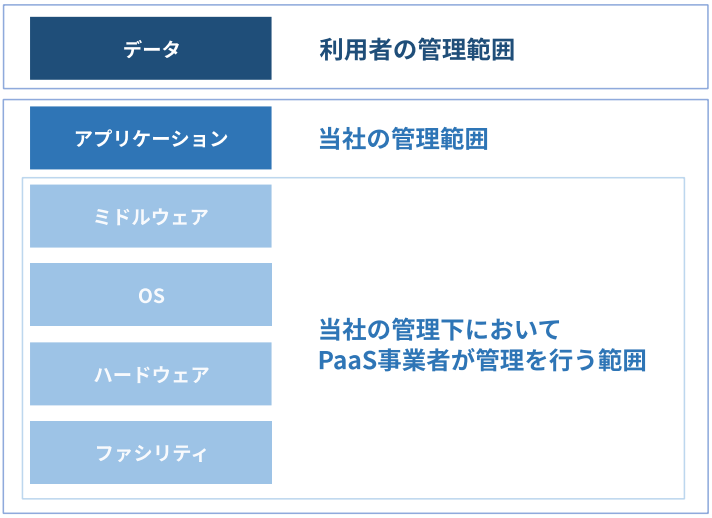
Cloud-SR0650 / JIP-ISMS517

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://www.opengroove.com/security

3. 組織的管理策

3.1 責任範囲（共有 Model）

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。
また、当社は、基盤上に構築したアプリケーションに対して責任を負います。
アプリケーション上のデータについては、ユーザ様の責任において保護していただく必要があります。



当社の責任
・tracpath のセキュリティ対策
・tracpath に保管されたユーザ様情報の保護
ユーザ様の責任
・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）
・パスワード等の利用者の秘密認証情報の管理
・ユーザ様が取扱うデータに対してのバックアップ

3.2 地理的所在地

当社の所在地、並びに当社がお客様のデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

4. 資産の管理

4.1 情報のラベル付け

tracpath は、ディレクトリによるファイル管理機能を提供し、ユーザ様のデータ分類をサポートします。使用方法の詳細は「ユーザマニュアル」をご参照ください。

4.2 サービス利用停止後のデータの扱い

tracpath で利用者様が作成・保存した利用者様のデータの除去に関しては、利用停止の 30 日経過後からの 30 日以内で完全に消去いたします。ただし、利用者様のデータを含まないサービス共通のログデータはこれに含まれません。

5. アクセス制御

5.1 利用者アクセスの管理

tracpath は、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。お客さまは管理者画面から簡単な操作によりアカウント登録・削除を行い、またユーザに対する権限の割り当てを行うことが出来ます。使用方法の詳細は「ユーザマニュアル」をご参照ください。

5.2 認証情報の管理

初期のアカウント登録手順は「ユーザマニュアル」をご参照ください。アカウントの登録が完了すると、登録したメールアドレスに対し、一定時間のみ有効なパスワード設定用 URL が記載されたメールが届きますので、画面の指示に従いパスワードの設定を行っていただきます。

パスワードの設定はユーザ様のセキュリティポリシーにもとづいて実施してください。また、tracpath のユーザアカウントは 2 段階認証が可能です。

管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

5.3　ユーティリティプログラム

ユーティリティプログラムは管理者権限に限定して利用可能です。管理者権限を厳重に管理することによりユーティリティプログラムの使用制限につながります。

6.　暗号

6.1　暗号化

ユーザ様のバージョン管理システムリポジトリや Wiki、チケットなどを保存しているデータベースは ASE-256 データ暗号化で暗号化されたストレージ上に格納しています。また、ストレージのスナップショットも同様に暗号化されています。

ユーザ様のパスワードは、ハッシュ化を施した上で保存しています。

tracpath とユーザ様間での HTTPS 通信は TLS 1.2 で、SSH 通信は AES-CTR で暗号化し、情報の盗聴等のリスクに対処しています。
SSH アクセスに使用する秘密鍵はユーザ様の責任にて厳重に管理してください。

7.　運用のセキュリティ

7.1　変更

ユーザ様に影響を与える tracpath の変更は、ご登録頂いたメールアドレス宛に事前通知します。また、各種の変更管理に関する情報は管理者画面より、確認することができます。

7.2　バックアップ

システム及びユーザ様データのバックアップは、1 時間ごと 24 世代・日次 7 世代・週次 4 世代分のデータを保持します。ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応していません。

7.3　ログ

tracpath の維持管理に必要となる適切なログを取得しています。
ユーザ様が tracpath へのアクセスログを必要とされる場合には、当社までご相談ください。

tracpath は基盤として利用するクラウドサービス事業者が提供する時刻同期サービスを利用し時刻同期を行っています。ログは日本標準時（UTC+9:00）で提供されます。

7.4　技術的脆弱性の管理

tracpath を構成するソフトウェアに脆弱性が発見された場合、速やかに影響調査を行い、必要な対策を講じます。発見された脆弱性がリモートから攻撃可能のような影響度の高いものである場合には tracpath のブログやトップ画面等で告知し、その状況を随時公表します。

脆弱性情報の収集は以下の手段により行います。
・使用するディストリビューション開発元から公開される脆弱性情報
・Common Vulnerabilities and Exposures（CVE）から公開される脆弱性情報
・Japan Vulnerability Notes（JVN）から公開される脆弱性情報
・使用するソフトウェア開発元から公開される脆弱性情報

7.5　管理者用手順

「ユーザマニュアル」等の各種マニュアルの提供に加え、管理者画面より QA サポートを提供しています。

7.6　クラウドサービスの監視

当社は tracpath が正常にサービスを提供していること、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していなか等の監視を行っています。
監視状況や結果をユーザ様が参照する機能は提供していません。監視結果が必要な場合は、当社までご相談ください。

7.7　容量・能力の管理

当社はサーバリソース及びネットワークリソースを監視しています。サーバリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。

7.8　装置のセキュリティを保った処分又は再利用

当社は、管理部に装置の処分又は再利用に関する役割を集中し、従業員による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

8.　通信のセキュリティ

8.1　ネットワーク

tracpath 専用の仮想ネットワークを構築し、サービス提供・運用に必要なポートのみのアクセスを許可し、各サーバを IDS/ IPS により監視することによりセキュリティを確保しています。

tracpath はネットワークの仮想化技術を利用し tracpath とそれ以外とのネットワークの分離を適切に行っています。また、ユーザ様に提供するクラウドコンピューティング環境と、当社の管理用環境を別セグメントとして分離しています。

9.　システムの取得、開発及び保守

9.1　情報セキュリティ機能

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 の管理策）	本ホワイトペーパーの記述
5.16　識別情報の管理	利用者アクセスの管理
5.17　認証情報	認証情報の管理
5.18　アクセス権	利用者アクセスの管理
8.2　特権的アクセス権	認証情報の管理
8.3　情報へのアクセス制限	利用者アクセスの管理
8.13　情報のバックアップ	バックアップ
8.15　ログ取得	ログ
8.24　暗号の使用	暗号化
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

9.2　開発プロセス

当社のクラウドサービスの開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。

9.3　サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

10. 情報セキュリティインシデントの管理

10.1 インシデント対応プロセス

当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

10.2 インシデント対応

tracpath に関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

項目	内容
報告する範囲	データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキィリティインシデント

項目	内容
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 72 時間以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛、管理者画面 （必用に応じて電話等の手段を使用する場合もあります。）
問合せ窓口	お問い合せフォーム
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、tracpath 内のお問合せページよりご連絡ください。

11. 順守

11.1 適用法令及び契約上の要求事項

利用契約に関する準拠法は、日本法とします。別途、「利用規約」をご参照ください。

11.2 証拠の収集

法令また権限のある官公庁からの要求により tracpath 上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。合意について別途、「利用規約」をご参照ください。

11.3 知的財産権

本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。別途、「利用規約」をご参照ください。

11.4 記録の保護

アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログを一定期間保存します。

11.5 暗号化機能に対する規制

tracpath において暗号化の規制対象になる地域にはサービスを提供していません。

11.6 内部教育の実施

当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。
また、クラウドコンピューティングに関する契約相手に対しても、同等レベルの教育を求めています。

11.7 情報セキュリティのパフォーマンス評価

当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

12. tracpath に関するお問い合わせ

株式会社オープングルーヴ　トラックパスサポート
TEL：03-6803-1647
メール：support@tracpath.com