CONFIDENTIAL

セキュリティ行動規範

セキュリティ行動規範は「tracpath」を運営している株式会社オープングルーヴが 社内のセキュリティ管理のために利用する文書です。
当サービスにおける情報セキュリティの取り組み状況について現状を通知するために公開しております。

第1.0版：2012年7月1日

管理

項番	方針
1	利用者データの管理方針、情報セキュリティに関してトップマネジメントによる組織的継続的な取り組みを実施しています。
2	当サービスの運用手順は文書化され、従業員に周知しています。
3	従業員のPCおよびサーバはウィルス対策ソフトウェアが導入されており、常に最新の状態で維持されています。
4	従業員のPCおよびサーバはOSのセキュリティアップデートを自動実施する設定になっており、常に最新の状態で維持されています。
5	従業員のPCおよびサーバにはWinnyなどのP2Pソフトウェアはインストールされておらず、使用も認めていません。
6	従業員の業務に関するメールやファイル転送ソフトなどによる自宅PCへ転送することは禁止しています。
7	従業員の個人PCの使用は禁止しています。
8	当サービスの開発・運用はすべて当社にて行っております。
9	サービス利用者の情報を保管するサーバにログインするためには、認証鍵による証明が必要です。認証鍵は当社従業員の限られた者のみが厳密に管理しております。
10	サービス利用者の情報を保管するサーバはAmazonEC2クラウドにあり、物理的な記憶媒体の接続（USBメモリなど）によるアクセスはできません。

従業員

項番	方針
1	従業員は業務上知り得た情報の機密保持に関する誓約書に署名しています。
2	誓約書には従業員の不正行為に対する法的な責任を負担する旨の内容に署名しています。
3	従業員に対して情報セキュリティ、顧客データの取り扱いルール、個人情報保護の教育、説明を実施しています。
4	従業員が当サービスのセキュリティ上の問題発見時の対応フローと連絡先が明示されています。
5	サービス利用者のデータへのアクセス権は限られた管理者に限定され、許可された人のみアクセスすることができます。ただし、問題発生以外に利用者のデータにアクセスすることはありません。
6	サービス利用者のデータをCDや紙媒体で受領した場合のデータ管理フローと破棄方法がルール化されています。
7	サービス利用者のデータを当サービス外に持ち出すことはありません。特別に必要性が求められている場合は管理者の承認のもとに作業を行います。

トラブル対応

項番	方針
1	サービス利用者の情報が漏洩した場合、漏洩範囲・漏洩経路を調査するためのサーバログ、アクセスログ等の各種ログを常に取得しています。
2	万一、セキュリティホールが見つかった場合や利用者情報の漏洩が判明した場合は当サービスへ外部から接続することができないように制限します。これは問題が解決するまで継続します。
3	情報の漏洩が判明した場合の運用手順は文書化されています。