tracpathのセキュリティについて

tracpathのクラウドサービスは、エンタープライズ環境において求められる高いレベルの安全対策が施されたサービスとして設計されています。お客様の大切なソースコードや設計情報を守るために実施しているtracpathクラウドサービスのセキュリティ対策とセキュリティ管理についてご説明します。

第1.0版：2012年7月1日

共通セキュリティ仕様

tracpathでは有料プラン、無料プランに関係なく高いセキュリティ対策済みのサービスを提供しています。

項番	方針
1	tracpathのサービス提供サーバ、管理している全てのサーバに対して、ウィルスソフトウェアによる全体スキャンを実施(約3ヶ月毎)。
2	暗号化されたサーバアクセス、データ伝送方式。(256ビットSSL証明書)
3	オンラインバックアップ(Online Backup)は1日に3回実施され、約30日間のバックアップ履歴データを保持しています。
4	バックアップ(Cold Backup)データは地理的に異なるクラウド(AmazonEC2 Tokyo/US)に退避されています。
5	HTTPSプロトコル(SSL)によりWebのデータ転送(通信)を暗号化しています。
6	すべてのサーバ・ソフトウェアは最新のセキュリティ・パッチが適用されています。

物理的なセキュリティ(Amazon EC2)

tracpathはクラウドにてサービスを提供しているため、tracpathとして物理的なリソースを持っていません。
tracpathは Amazon EC3 サービスを利用しています。以下は Amazon Web Service についての情報となります。

項番	方針
1	SOC 1/SSAE 16/ISAE 3402
2	FISMA Moderate
3	PCI DSS レベル 1
4	ISO 27001
5	武器規制国際交渉規則へのコンプライアンス
6	FIPS 140-2
7	HIPAA

セキュリティ管理

tracpathを開発・運営している株式会社オープングルーヴは独自にセキュリティに対する行動規範を設けています。

項番	方針
1	株式会社オープングルーヴのセキュリティ行動規範。（別紙参照：http://ciklone.com/security_rule.html）
2	セキュリティポリシーを1年おきにチェックし、厳格に運用しています。
3	ユーザデータ・サーバへのアクセスは標準で制限されています。当社内のLANにアクセスするためにはユーザ認証機能により特定ユーザのみ許可されており、セキュリティ教育を受けた従業員だけが社内サーバにアクセスすることが可能です。
4	許可された従業員のアクセスや操作はすべて監査ログとして3ヶ月保存されています。
5	tracpathのプログラムはすべてソースコードレビューが実施されています。
6	利用者のデータは、当社の秘密保持契約によって保護します。サービスに関わる従業員はすべて秘密保持契約の上で開発を行っています。

冗長性

tracpathのサービスはクラウドサービスを利用しています。

項番	方針
1	tracpathは物理的に異なる複数の Availability Zone(データセンター)を利用しています。現在は東京(tokyo region)とアメリカ(US region)にある Availability Zoneを利用しています。
2	暗号化されたサーバアクセス、データ伝送方式。(256ビットSSL証明書)
3	ユーザのプロジェクトデータはオンラインバックアップにより、サービスを提供しながらバックアップされています。バックアップされたファイルは存在期間の異なるディスクスペースにコールドバックアップされる仕組みになっています。Amazon Elastic Block Store（EBS）サービスレベルは99.999%の可用性です。
4	バックアップデータは最大で約30日間保存されます。
5	tracpathのデータベースサーバ(DB)、DNSサーバ、Proxyサーバ、監視サーバは冗長化された状態で運用されています。

ネットワークセキュリティ

項番	方針
1	HTTPS(256bit SSL GlobalSigh証明書)による暗号化されたデータ転送を提供しています。
2	IP制限、特定のIPアドレスとIPアドレス範囲を指定することで、ユーザに対するアクセス制限機能が利用可能です。
3	公開されている全てのサイトはファイアウォール(Firewall)によりアクセス可能なポートが制限しています。

アカウント管理

tracpathは以下の機能を提供しています。

項番	方針
1	アカウントのロックアウト機能。(セキュリティ施策)
2	利用者は柔軟なグループ管理・アカウント管理、ロール管理が可能です。
3	グループ、アカウントをロールによる権限管理が可能です。
4	プロジェクト管理ツールとSubversion等のリポジトリ管理の権限を統合管理することができます。
5	管理アカウントはアカウントロック、パスワードの強制変更がブラウザから操作することができます。

外部からの攻撃に対する対策

tracpathでは外部からの攻撃に対する対策として一般的な対策は当然ですが、下記のような対策をサービスレベルで提供しています。

項番	方針
1	DoS等の不正なIPアドレスを接続不可にします。
2	サーバアクセスとデータ転送はすべて暗号化しています。
3	サーバ管理者のアクセスログ、操作ログはすべて保存しています。
4	公開サーバ以外(HTTPS)のサーバ群は限られたIPのみアクセスすることが可能です。外部からインターネット経由の直接アクセスすることができません。

契約終了後のデータ管理

tracpathでは有料プラン、無料プランに関係なく高いセキュリティ対策済みのサービスを提供しています。

項番	方針
1	利用者にてアカウントの解除をブラウザ画面から実行して頂きます。アカウントを解除した時点で、すべてのプロジェクトとリポジトリを完全に削除します。この操作は元に戻すことが出来ません。
2	フリーアカウントを利用しているとき、継続して180日間ログインがない場合、アカウントは削除される場合があります。削除されたデータは、復元できない可能性があります。
3	削除は物理削除のため、間違って削除したとき復元できない場合があります。

セキュリティに対するお願い

利用者のプロジェクトチームや会社で徹底することを期待しています。

項番	方針
1	プロジェクトに必要なくなったユーザアカウントが残っている場合、ロックするか削除してください。
2	チームメンバーに定期的にパスワードを更新するように注意喚起してください。(1～3ヶ月毎の更新がおすすめです)
3	管理アカウントを利用すれば、すべてのアカウントをロックしたり、パスワードを強制的に変更することができます。厳密な管理をおすすめします。
4	パスワードの有効期限機能を活用してください。
5	強いパスワードを作成するようにしてください。Microsoftが推奨する強いパスワードのページを参照してください。