自動翻訳サービス（T-4OO）の機密保持体制について

株式会社ロゼッタ
執行役員　MT事業部長
渡邊　麻呂

発行日：2020年12月1日

① 公的認証・認定

プライバシーマーク:取得済

登録番号：第 17001847（04）号
登録日　：西暦 2014年 3月 17日
有効期間：西暦 2020年 3月 17日 ～ 西暦 2022年 3月16日

② 弊社情報管理体制

情報を取り扱う従業員は弊社開発部内の必要最小限の者に限定し、 当該従業員に対しては、適宜セキュリティ管理に 関する教育・指導を実施するなど、特に注意・意識向上を図っております。 また、本サービスの開発・運用は全て弊社社員によって行われ、外部への作業委託などは行っていません。

- **全社セキュリティポリシーの運用**
  情報システム本部 本部長（ＣＩＯ）が責任者となり、情報システム部門が中心となって、情報管理の適切な運用を 行っています。
- **開発・運用部門のセキュリティポリシー運用**
  開発本部 本部長が責任者となり、ソフトウェアのライフサイクルに応じたセキュリティ管理を行っています。
- **ＣＳＭ部門のセキュリティ運用**
  ＣＳＭ部門長が責任者となり、お客様の個人情報の取り扱い、及び本サービスの管理システム上のセキュリティ 管理を行っています。

③ お客様ごとのデータ分離

- **データベースへのデータ保管**
  お客様（ご契約企業ＩＤ）ごとに異なるデータベースが作成され、他のお客様と物理的・論理的に区別して管理されます。

④ 情報漏洩への対策

- **インターネット上でのデータ暗号化対策**
  お客様パソコン上で動作するウェブブラウザと弊社T-4OOサービス間は、ｈｔｔｐｓ（ＴＬＳ１．２／１．３対応）で暗号化通信が行われますので、第三者によってデータを覗かれる心配はありません。

- **サービスインフラの環境**
  本サービスの構成機器（サーバー機器、ネットワーク機器、ストレージ機器等）は、各種認証（ＩＳＭＳ、ＰＣＩＤＳＳなど）を取得済みの都内データセンターに設置されています。データセンターでは、２４時間・３６５日有人体制で、外部からの人的・物理的・ 技術的不正アクセスから保護されています。

⑤ システム上での翻訳データ保管

- **翻訳内容の保管期間**
  - ログインしたユーザIDで、過去２週間に行った翻訳結果を閲覧することができます。
  - ２週間経過後に、自動的にサーバ上から削除されます。
  - ウェブ画面上の翻訳結果を「削除する」というボタンから、任意のタイミングで翻訳結果を削除可能です。

- **ご解約後のお客様データ削除**
  - １か月経過後に、自動的にサーバ上から削除されます。
  - 即時の削除をご希望される場合は、個別に削除対応可能です。
  - お客様データ削除後は、一切のデータ復旧ができません。

- **データのバックアップ**
  日次でバックアップが取得されます。バックアップデータは、常時３世代保管されます。

- **データの複製、再利用**
  バックアップを目的とした複製のみが実施されます。
  本サービスでは、独自に収集した学習データをもとに機械学習を行いますので、お客様の翻訳データの再利用や二次利用は行われません。

⑥ 脆弱性対策

- 脆弱性が認知され次第、検証環境での動作確認を経て、随時本番環境への適用が行われます。
  - ファイアウォール、ＩＰＳ、ＷＡＦ
  - ＯＳ、ミドルウェア（ウェブサーバ、ＤＢサーバ、他）、アプリケーション

⑦ 外部パブリッククラウドの利用

- **ロゼッタ内製エンジンで翻訳する言語**
  日英・英日翻訳、日中・中日翻訳の一部(※)

  その他の言語

  - 韓国語、 タイ語、 ベトナム語、 タガログ語、 インドネシア語、 ヒンディー語、 マレー語
  - ロシア語、 アラビア語、 ベンガル語、 ペルシア語、 トルコ語
  - フランス語、 ドイツ語、 イタリア語、 ポルトガル語、 スペイン語、 ギリシア語、 フィンランド語、 ポーランド語、 スウェーデン語

  弊社が調達したハードウェア、ソフトウェア上で動作し、全てのデータは国内で管理されます。

  ※「日英・英日翻訳、日中・中日翻訳の一部」以外の言語は、下記『パブリッククラウドサービス』を利用する場合があります。
  ※外部パブリッククラウドサービスを利用せず、内製エンジンのみで上記言語を翻訳する設定も可能です。

- **一部、パブリッククラウドを活用する言語**
  日中・中日、日韓、韓日翻訳の一部
  内製エンジンを、パブリッククラウド（AWS）環境で運用しています。
  全てのデータは国内で管理されます。社外とのデータ受け渡しはありません。

  ※パブリッククラウド（AWS）の詳細なセキュリティポリシーの開示をご要望の場合、別途お問い合わせいただきます様お願い申し上げます。
  ※このサービスを利用しない設定にすることもできます。

- **外部パブリッククラウド(外部API)を活用する言語**
  上記の言語以外
  本サービスから、外部パブリッククラウドサービスの提供する翻訳APIを利用します。
  外部パブリッククラウドサービスでのデータ取り扱いについては、外部パブリッククラウドサービスのプライバシーポリシーに依存します。

  ※外部パブリッククラウドサービスを利用しない設定にすることもできます。

⑧ 秘密保持契約書の締結

- 個別に秘密保持契約書を締結することも可能です。

情報セキュリティ対策チェックリスト

「中小企業の情報セキュリティ対策ガイドライン」－「組織的な情報セキュリティ対策ガイドライン」より

1．情報セキュリティに対する組織的な取り組み状況

#	内容	チェック	補足
1	情報セキュリティに関する経営者の意図が従業員に明確に示されていますか？	Yes	いずれの下記社内規定によって定義されており、各組織単位に情報管理責任者を任命し、情報システム本部長が統括します。 ・社内情報セキュリティポリシー ・個人情報保護規定 ・就業規定 なお、T-4OOは開発・環境構築・運用管理の全てを弊社社員によって行っていますので、外部への業務委託などは発生しておりません。
2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	Yes	
3	管理すべき重要な情報資産を区分していますか？	Yes	
4	重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めていますか？	Yes	
5	外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取っていますか？	Yes	
6	従業者（派遣を含む）に対してセキュリティに関して就業上何をしなければいけないかを明確にしていますか？	Yes	
7	情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与えていますか？	Yes	

2．物理的セキュリティ

#	内容	チェック	補足
1	重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行っていますか？	Yes	
2	重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害に配慮し適切に配置・設置していますか？	Yes	
3	重要な書類、モバイルPC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行っていますか？	Yes	

3．情報システム及び通信ネットワークの運用管理状況

#	内容	チェック	補足
1	情報システムの運用に関して運用ルールを策定していますか？	Yes	
2	ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか？	Yes	
3	導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行っていますか？	Yes	
4	通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施していますか？	Yes	ウェブシステムとの通信は、httpsプロトコルによる暗号化が行われています。また、開発、及び運用でサーバなどへアクセスする際には、特定のネットワークセグメントからのssh公開鍵認証でのみ接続を許可し、アクセスは全てログに保存される仕組みを採っています。
5	モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施していますか？	Yes	特にUSBなどの外部記憶媒体の利用は、ハードウェアおよびソフトウェアの機能で無効となっています。例外として、社内決裁を経ての利用は可能と規定されていますが、これまでに許可された事例はありません。

4．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況

#	内容	チェック	補足
1	情報（データ）や情報システムへのアクセスを制限するために、利用者IDの管理（パスワードの管理など）を行っていますか？	Yes	個人ごとのIDを付与し、人事異動または従業員の退職等が発生した場合には、即日アカウント・権限の変更・削除を実施しています。また、定期的に権限付与の見直しを行います。
2	重要な情報に対するアクセス権限の設定を行っていますか？	Yes	管理IDまたは特権IDに関しては、各組織の部門長が任命した担当者へ付与される運用となっています。
3	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISPサービス 等）を行っていますか？	Yes	ファイアーウォール、ＩＰＳ、ＷＡＦが導入されています。
4	無線LANのセキュリティ対策（WPA2の導入等）を行っていますか？	Yes	
5	ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか？	Yes	

5．情報セキュリティ上の事故対応状況

#	内容	チェック	補足
1	情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか？	Yes	
2	情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握していますか？	Yes	

用語

- T-4OO : Translation for Onsha Only
- HTTPS : Hypertext Transfer Protocol Secure
- TLS : Transport Layer Security
- ISMS : Information Security Management System
- PCIDSS: Payment Card Industry Data Security Standard
- IPS : Intrusion prevention system
- WAF : Web Application Firewall
- SLA : Service Level Agreement
- CSM : Customer Success Manager

以上