TANOMUセキュリティ関連資料

TANOMU

この資料は、株式会社タノム（以下、当社）のセキュリティ対策への取り組みについて、お客様、お取引先様、およびその他ステークホルダーの皆様に分かりやすく説明することを目的とした、以下の3つの資料をまとめたものになります。

- セキュリティホワイトペーパー
- SLO
- セキュリティチェックシート

各資料は、必要に応じて改定いたします。
改訂履歴は末尾のページをご覧ください。

セキュリティホワイトペーパー

はじめに

このセキュリティホワイトペーパーは、当社のセキュリティ対策への取り組みについて、お客様、お取引先様、およびその他ステークホルダーの皆様に分かりやすく説明することを目的としています。

このホワイトペーパーを通じて、当社のセキュリティ対策への理解を深めていただき、皆様との信頼関係をより強固なものにしたいと考えております。

対象となる当社のサービスは「TANOMU」になります。

1. セキュリティポリシー

当社は、情報セキュリティの重要性を認識し、お客様からお預かりする情報資産および当社の事業活動に関連する情報資産を、不正アクセス、漏えい、改ざん、紛失、破壊などの脅威から保護するため、以下にセキュリティポリシーを定めます。

1.1 基本方針

1.1.1 機密性

情報資産へのアクセスは、業務上必要な範囲に限定し、許可された従業員のみがアクセスできるようにします。

1.1.2 完全性

情報資産の正確性および信頼性を維持し、不正な改ざんや破壊から保護します。

1.1.3 可用性

許可された従業員が、必要なときに情報資産にアクセスできるようにします。

1.1.4 法令遵守

情報セキュリティに関する法令、規制、およびその他の規範を遵守します。

1.1.5 継続的改善

セキュリティ対策を定期的に見直し、継続的に改善します。

1.2 適用範囲

このセキュリティポリシーは、当社の業務に従事するすべての人に適用されます。

1.3 情報資産の定義

情報資産とは、当社が保有する、事業活動に関連するあらゆる情報のことを指します。

1.3.1 顧客情報

氏名、住所、電話番号、メールアドレスなどの個人情報、取引履歴、契約内容など

1.3.2 社内情報

財務情報、人事情報、技術情報、営業情報、機密情報など

1.3.3 システム情報

サーバ、ネットワーク機器、ソフトウェア、データベースなど

1.4 個人情報保護

当社の事業運営における個人情報の重要性に鑑み、以下のWebサイトに掲載しているプライバシーポリシーを定め、個人情報保護のための社内組織体制を確立し、実施し、維持し、改善の取り組みを実施します。

https://lp.tano.mu/security/privacy/

1.5 セキュリティ対策

当社は、情報資産を保護するため、以下のようなセキュリティ対策を実施します。

1.5.1 技術的対策

ファイアウォール、Webアプリケーションファイアウォール(WAF)などのセキュリティ対策、暗号化、アクセス制御、認証システムなどの対策を実施いたします。

1.5.2 管理的対策

リスクアセスメント、セキュリティ教育、内部監査、インシデント対応など

1.6 継続的改善

当社は、セキュリティポリシーおよびセキュリティ対策を定期的に見直し、継続的に改善します。

2. 技術的対策

当社は、情報資産を保護するため、多岐にわたる技術的対策を講じています。

2.1 ネットワークセキュリティ

2.1.1 Webアプリケーションファイアウォール (WAF)

Webアプリケーションへの攻撃を防御するため、Webアプリケーションファイアウォール (WAF) を導入しています。WAFは、Webアプリケーションへのトラフィックを監視し、SQLインジェクション、クロスサイトスクリプティング (XSS) などの攻撃を検知し、遮断します。

2.1.4 ネットワークセグメント化

ネットワークを複数のセグメントに分割し、セグメントごとにアクセス制御を行うことで、セキュリティリスクを分散させています。万が一、一つのセグメントが侵害された場合でも、他のセグメントへの影響を最小限に抑えることができます。

2.2 アプリケーションセキュリティ

2.2.1 セキュアコーディング

Webアプリケーション開発においては、セキュアコーディングを徹底し、セキュリティ脆弱性を作り込まないようにしています。サニタイジングやバリデーションなど脆弱性を産まない開発を行っています。

2.2.2 脆弱性診断

定期的に脆弱性診断を実施し、セキュリティ上の問題がないことを確認しています。脆弱性診断は外部の診断サービスを利用し、高い頻度で実施しています。

2.3 データセキュリティ

2.3.1 暗号化

重要なデータは、暗号化して保存および通信することで、機密性を確保しています。

2.3.2 アクセス制御

情報資産へのアクセスは、業務上必要な範囲に限定し、許可された従業員のみがアクセスできるように、アクセス制御を実施しています。アクセス制御は、役割に基づいて設定し、必要最低限の権限のみを付与しています。

2.3.3 認証システム

従業員の本人確認を厳密に行うため、強固な認証システムを導入しています。パスワード認証に加え、多要素認証を導入することで、セキュリティ強度を高めています。

2.4 インフラストラクチャの監視

2.4.1 監視項目

クラウドサービスの監視機能を活用し、インフラストラクチャを 24 時間 365 日体制で監視しています。監視項目は、CPU 使用率、メモリ使用率、ディスク使用量、ネットワークトラフィックなど多岐にわたります。

2.4.2 異常の検知

異常を検知した場合は、自動的にアラートが通知され、速やかに対応します。

2.5 インフラストラクチャの拡張

クラウドサービスの機能を利用し、トラフィックや負荷の増大に応じて、インフラストラクチャを自動で拡張します。これにより、サービスの可用性を維持し、お客様に安定的にサービスを提供いたします。

2.6 その他の対策

2.6.1 多要素認証

重要なシステムへのアクセスには、多要素認証を導入し、セキュリティを強化しています。

2.6.2 シングルサインオン (SSO)

複数のシステムを利用する際に、一度の認証で全てのシステムにアクセスできるように、シングルサインオン (SSO) を導入しています。SSOは、ユーザの利便性を向上させるとともに、パスワード管理の手間を削減することで、セキュリティリスクを低減します。

3. 管理的対策

当社は、技術的な対策に加えて、組織的・人的な側面から情報セキュリティを強化するための管理的対策を徹底しています。

3.1 インシデント対応

インシデント発生時に備え、対応体制を整備しています。定期的にトレーニングを実施することで、迅速な対応を可能としています。

3.2 脆弱性管理

システムの脆弱性を定期的に診断し、発見された脆弱性に対しては、速やかに対策を講じています。

3.3 アクセス管理

情報資産へのアクセスは、業務上必要な範囲に限定し、許可された従業員のみがアクセスできるように、アクセス制御を実施しています。

3.4 従業員への教育

当社の全従業員にむけてセキュリティ講習を定期的に実施しております。セキュリティ対策やインシデント対応など多面的な教育を継続的に実施しています。

4. バックアップ

当社では、災害や障害に備え、お客様のデータと当社のシステムを保護するため、以下のバックアップ対策を実施しています。

4.1 データのバックアップ

お客様からお預かりしたデータは、以下の方法でバックアップを取得しています。

4.1.1 データベース

クラウドサービスが提供する自動バックアップ機能を利用し、データベースのバックアップを毎日取得しています。

4.1.2 ファイルストレージ

クラウドストレージに保存されているデータは、クラウドサービスが提供するバージョン管理機能を利用し、過去のバージョンを保持しています。

4.2 システムのバックアップ

当社のシステム構成をコードとして管理したうえでインフラストラクチャを構築しています。 これにより、必要に応じてシステム全体を迅速に再構築することができます。

4.3 バックアップの保存

バックアップデータは、クラウドサービスが提供する強力な保護機能を使うことで、災害発生時や不正アクセスによる侵入時のデータ損失リスクを低減しています。

4.4 お客様によるバックアップ

お客様ご自身でデータをバックアップしたい場合は、一部のデータについては当社が提供するアプリケーションの管理画面からCSVでデータを出力することができます。

4.5 BCP

当社は事業継続計画 (BCP) を策定し事業を継続できる体制を構築しています。RTO (Recovery Time Objective: 復旧目標時間) は 12時間、RPO (Recovery Point Objective: 目標復旧時点) は 1時間としています。つまり、災害や障害発生から 12時間以内にサービスを復旧し、最大 1時間前のデータまで復元することを目標としています。

5. コンプライアンス

当社は、情報セキュリティに関する法令、規制、およびその他の規範を遵守し、お客様に安心してサービスをご利用いただけるよう、コンプライアンスを重視した事業活動を行っています。

5.1 認証取得状況

当社は、情報セキュリティマネジメントシステム (ISMS) の ISO/IEC 27001 の認証を取得しています。当社がセキュリティ基準を満たしていることを証明しています。

5.2 法令遵守

当社は、個人情報保護法、不正アクセス禁止法、電気通信事業法など、情報セキュリティに関する法令を遵守しています。 また、業界のガイドラインやベストプラクティスも積極的に取り入れ、セキュリティレベルの向上に努めています。

5.3 継続的改善

当社は、情報セキュリティに関するコンプライアンス体制を継続的に改善しています。 最新のセキュリティ脅威や法規制の変更などを常に把握し、セキュリティ対策を強化することで、お客様に安心してサービスをご利用いただけるよう努めています。

6. インシデント対応

当社は、インシデント発生時に迅速かつ適切に対応するため、以下の体制を整備しています。

6.1 インシデント対応体制

インシデント発生時は、責任者が中心となり、インシデント対応を統括します。インシデントの内容に応じて各部門が連携して対応します。また必要に応じて、外部の専門機関や関係当局に協力を要請します。

6.2 インシデント対応手順

6.2.1 インシデントの検知

システムの監視、ログの分析、従業員からの報告などにより、インシデントを検知します。インシデントの発生を疑う場合は、速やかに社内の関係部署に情報を展開します。

6.2.2 インシデントの初動対応

責任者はインシデントの状況を把握し、被害拡大の防止を最優先に行動します。必要に応じて、システムの停止、ネットワークの遮断、データのバックアップなどの措置を講じます。

6.2.3 インシデントの調査

インシデントの原因、影響範囲、被害状況などを調査します。調査には、ログ分析、マルウェア解析、脆弱性診断などの手法を用います。

6.2.4 インシデントの復旧

インシデントの影響を受けたシステムやデータを復旧します。復旧には、データのバックアップからのリストア、システムの再構築などの作業を行います。

6.2.5 インシデントの報告

インシデントの状況、原因、影響範囲、対応内容などを、関係部署、経営層、必要に応じて外部機関や関係当局に報告します。

6.2.6 再発防止

インシデントの原因を分析し、再発防止策を検討・実施します。再発防止策には、システムのセキュリティ強化、従業員教育、セキュリティポリシーの見直しなどが含まれます。

7. お客様への注意喚起

当社は、お客様に安全にサービスをご利用いただくために、以下の点にご注意いただくようお願いいたします。

7.1 当社とお客様との責任分界点

7.1.1 当社の責任

当社は、TANOMUのセキュリティ対策を実施いたします。ネットワークやデータの保護、サーバーのセキュリティ対策など実施いたします。

7.1.2 お客様の責任

お客様は、パスワードやアカウントの適切な管理を実施いただく必要がございます。

当社では、以下のパスワードポリシーを定めています。

- 8文字以上、英大文字・小文字・数字・記号を組み合わせたパスワード
- 辞書に載っている単語や個人情報を含むパスワードは使用しない
- 他のサービスで利用しているパスワードと同じパスワードは使用しない

パスワードを他人に教えない、メモに書き残さない、共有しないなど、厳重に管理してください。

また、OSやソフトウェアのセキュリティアップデートを定期的に実施し、OSやソフトウェアの脆弱性を解消してください。

7.2 セキュリティを向上するオプション機能について

当社は、セキュリティを向上するためのオプション機能を提供しています。

7.2.1 多要素認証の強制

多要素認証を強制することで、不正アクセスのリスクを減らすことができます。
TANOMUでは多要素認証の設定は任意ですが、多要素認証を強制するオプションをご用意しています。多要素認証の導入を希望されるお客様は、当社までご連絡ください。

サービスレベル目標(SLO)

概要

このドキュメントは、お客様に提供するサービスの品質を明確にするためのサービスレベル目標（以下SLO）を定めたものです。

SLOとは、サービスの可用性、性能、障害対応など、お客様にとって重要なサービスレベル指標について、目標値を設定したものです。

このSLOを通じて、お客様にサービスの品質に対する透明性と信頼性を提供し、安心してサービスをご利用いただけるよう努めます。

サービスレベル目標

1. 可用性

1.1 稼働率

99.9%を目標とします。

※ 計画停止／メンテナンス時間を除きます。
※ 稼働率計算は分単位で行います。

1.2 サービス復旧時間（RTO）

障害発生時のサービス復旧時間は、12時間以内を目標とします。

1.3 目標復旧時点（RPO）

障害発生時に許容できるデータ損失の範囲は、1時間以内とします。

1.4 データの耐久性

データの耐久性について、99.999%を目標とします。

2. メンテナンス

2.1 定期メンテナンス

毎週水曜日 14時 〜 14時15分（日本標準時）の15分間です。

※実施しない場合もございます。

2.2 計画停止

定期メンテナンス以外のサーバーメンテナンスなどによる計画停止が行われる場合、事前にWeb掲載・メールにて通知します。

2.3 臨時メンテナンス

サービスの安定稼働のため、定期メンテナンス以外にやむを得ず緊急メンテナンスを実施させていただく場合がございます。

2.4 アップデート内容の事前通知

計画停止やアップデートにより著しく操作性が変わる場合、7日前までにWeb掲載・メールにて通知します。

3. 性能

3.1 APIレスポンスタイム

APIレスポンスタイムについて平均 300ms以内を目標とします。

3.2 エラー率

予期せぬエラーレスポンスの割合について、0.01%以下を目標とします。

3.3 スループット

1分あたり5,000リクエストのスループットを目標とします。

4. 障害対応

4.1 障害の検知

監視システムによるサービス監視を常時実施します。

4.2 障害対応の体制

モニタリングシステムから異常が検知された場合、運用ドキュメントに沿って対応します。

サービス稼働に影響が出ていると判断した場合には、利用ユーザへ速やかに告知します。

4.3 障害の通知

障害は迅速にWeb掲載または該当するお客様へメール、個別に合意した連絡手段にて通知します。

5. サポート

5.1 メール受付

365日24時間受付いたします。 2営業日以内の回答を目標とします。

※年末年始・夏季休暇・社員研修期間を除きます。
※重大な障害発生の場合、営業時間外に連絡をさせていただくことがあります。

SLO適用範囲

本SLOの適用範囲は、本システム（TANOMU）、及び関連するオプションサービスとします。

また、本SLOの不達成が、以下の要因によって生じた場合、本SLOは適用されません。

- 日本国外での利用
- 当社の合理的な管理・統制の及ばない現象（天変地異、不可抗力、通信遮断等のインフラ障害、ハードウェア・ミドルウェアにおける不可避の障害を含む）
- 本システムではなく、個々のPC、又は他社提供のサービス（回線など）に依存する問題に起因する現象
- 事前通知済の計画停止実施時間帯での利用（お客様の事情により、登録されたお客様の連絡先が更新されていなかったことに起因する通知未達を含む）
- お客様の作為に起因する場合（又は、お客様が承諾しプラットフォームID・PWを割り当てた第三者の作為に起因する場合）

TANOMUセキュリティチェックシート

本チェックシートは、株式会社タノムが提供する TANOMU について、そのセキュリティに関わる対策を記載した資料です。

株式会社タノムは、法令及びその他の規範を遵守し、セキュリティに関する取り組みを実施しています。

株式会社タノムは ISO/IEC27001:2013／JIS Q 27001:2014 に基づくISMS認証を取得しています。（認証登録範囲：WEBサービスの運営・開発事業）

本チェックシートは、以下の資料を元に、独自の項目の追加削除などを行ったものになっております。

●IPA - 安全なウェブサイトの作り方 (第7版)
https://www.ipa.go.jp/security/vuln/websecurity/about.html

●経済産業省 - クラウドサービスレベルのチェックリスト
https://warp.da.ndl.go.jp/info:ndljp/pid/8658576/www.meti.go.jp/press/20100816001/20100816001-4.pdf

IPA - 安全なウェブサイトの作り方 (第7版)

No	カテゴリ	項目	回答
1-(i)-a	SQLインジェクション	SQL文の組み立ては全てプレースホルダで実装する	対応済
1-(i)-b	SQLインジェクション	SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する	対応済
1-(ii)	SQLインジェクション	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない	対応済
1-(iii)	SQLインジェクション	エラーメッセージをそのままブラウザに表示しない	対応済
1-(iv)	SQLインジェクション	データベースアカウントに適切な権限を与える	対応済
2-(i)	OSコマンド・インジェクション	シェルを起動できる言語機能の利用を避ける	対応済
2-(ii)	OSコマンド・インジェクション	シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する	対応済
3-(i)-a	パス名パラメータの未チェック／ディレクトリ・トラバーサル	外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける	対応済
3-(i)-b	パス名パラメータの未チェック／ディレクトリ・トラバーサル	ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする	対応済
3-(ii)	パス名パラメータの未チェック／ディレクトリ・トラバーサル	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する	対応済
3-(iii)	パス名パラメータの未チェック／ディレクトリ・トラバーサル	ファイル名のチェックを行う	対応済
4-(i)	セッション管理の不備	セッションIDを推測が困難なものにする	対応済
4-(ii)	セッション管理の不備	セッションIDをURLパラメータに格納しない	対応済
4-(iii)	セッション管理の不備	HTTPS通信で利用するCookieにはsecure属性を加える	対応済
4-(iv)-a	セッション管理の不備	ログイン成功後に、新しくセッションを開始する	対応済
4-(iv)-b	セッション管理の不備	ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する	対応済
4-(v)	セッション管理の不備	セッションIDを固定値にしない	対応済
4-(vi)	セッション管理の不備	セッションIDをCookieにセットする場合、有効期限の設定に注意する	対応済

No	カテゴリ	項目	回答
5-(i)	クロスサイト・スクリプティング	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	対応済
5-(ii)	クロスサイト・スクリプティング	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	対応済
5-(iii)	クロスサイト・スクリプティング	<script>...</script> 要素の内容を動的に生成しない。	対応済
5-(iv)	クロスサイト・スクリプティング	スタイルシートを任意のサイトから取り込めるようにしない。	対応済
5-(v)	クロスサイト・スクリプティング	入力値の内容チェックを行う。	対応済
5-(vi)	クロスサイト・スクリプティング	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	対応不要 HTMLテキストの入力を許可する場合の対策だが、許可しないため
5-(vii)	クロスサイト・スクリプティング	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	対応不要 HTMLテキストの入力を許可する場合の対策だが、許可しないため
5-(viii)	クロスサイト・スクリプティング	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。	対応済
5-(ix)	クロスサイト・スクリプティング	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	対応済
5-(x)	クロスサイト・スクリプティング	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	対応中
6-(i)-a	CSRF	処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	対応済 hiddenではありませんが、適切な方法で対応済みです
6-(i)-b	CSRF	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	対応済 一部の重要な処理においてのみパスワードの再入力を求めています

No	カテゴリ	項目	回答
6-(i)-c	CSRF	Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	対応不要 トークンによるチェックを実施しているためリファラーによるチェックは実施していません
6-(ii)	CSRF	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	対応済 一部の重要な処理においてのみ送信しています
7-(i)-a	HTTPヘッダ・インジェクション	ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	対応済
7-(i)-b	HTTPヘッダ・インジェクション	改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	対応済
7-(ii)	HTTPヘッダ・インジェクション	外部からの入力の全てについて、改行コードを削除する。	対応済
8-(i)-a	メールヘッダ・インジェクション	メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。	対応済
8-(i)-b	メールヘッダ・インジェクション	ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する（8-(i) を採用できない場合）。	対応済
8-(ii)	メールヘッダ・インジェクション	HTMLで宛先を指定しない。	対応済
8-(iii)	メールヘッダ・インジェクション	外部からの入力の全てについて、改行コードを削除する。	対応済
9-(i)-a	クリックジャッキング	HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。	対応不要 非推奨の対応のため対応しておりません
9-(i)-b	クリックジャッキング	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	対応済 一部の重要な処理においてのみパスワードの再入力を求めています
9-(ii)	クリックジャッキング	重要な処理は、一連の操作をマウスのみで実行できないようにする。	対応済
10-(i)-a	バッファオーバーフロー	直接メモリにアクセスできない言語で記述する。	対応済
10-(i)-b	バッファオーバーフロー	直接メモリにアクセスできる言語で記述する部分を最小限にする。	対応済

No	カテゴリ	項目	回答
10-(ii)	バッファオーバーフロー	脆弱性が修正されたバージョンのライブラリを使用する。	対応済
11-(i)	アクセス制御や認可制御の欠落	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。	対応済
11-(ii)	アクセス制御や認可制御の欠落	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。	対応済

経済産業省 - クラウドサービスレベルのチェックリスト

No	カテゴリ	項目	補足	回答
1	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	24時間365日（計画停止／定期保守を除く）
2	可用性	計画停止予定通知	定期的な保守停止に関する事前連絡確認（事前通知のタイミング／方法の記述を含む）	ログイン後のトップページにて通知いたします
3	可用性	サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	現状定義しておりません サービス終了が判明次第、WEBサイトおよびメールで通知します
4	可用性	突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	現状定義しておりません
5	可用性	サービス稼働率	サービスを利用できる確率（（計画サービス時間ー停止時間）÷計画サービス時間）	99.9%を目標値として定めておりますが、実測値は公開しておりません
6	可用性	ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	複数のデータセンターで冗長化しています
7	可用性	重大障害時の代替手段	早期復旧が不可能な場合の代替措置	代替手段はございません万が一に備えてお客様が事前にマスタデータをCSV形式でダウンロードいただくことができるようになっています
8	可用性	代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	CSV
9	可用性	アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	随時更新しております
10	信頼性	平均復旧時間(MTTR)	障害発生から修理完了までの平均時間（修理時間の和÷故障回数）	公開しておりません
11	信頼性	目標復旧時間(RTO)	障害発生後のサービス提供の再開に関して設定された目標時間	12時間以内を目標としています

No	カテゴリ	項目	補足	回答
12	信頼性	障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	公開しておりません
13	信頼性	システム監視基準	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視	死活監視、パフォーマンス監視（アプリケーション、サーバー、ネットワークなど）、エラー監視を実施しています
14	信頼性	障害通知プロセス	障害発生時の連絡プロセス（通知先／方法／経路）	チャットツールにて社内に通知され、対応いたします お客様へのご連絡は必要に応じてサービス内告知・Webサイト・メール・電話などを通じてご連絡いたします
15	信頼性	障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	社内への通知は数分以内に実施されます お客様へのご連絡は可能な限り迅速に実施いたします
16	信頼性	障害監視間隔	障害インシデントを収集／集計する時間間隔	1分間隔です
17	信頼性	サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	ございません 必要に応じてサービス内告知・Webサイト・メール・電話などを通じてご連絡いたします
18	信頼性	ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	ございません
19	性能	応答時間	処理の応答時間	公開しておりません 通常の利用に問題のない範囲で応答しております
20	性能	遅延	処理の応答時間の遅延継続時間	公開しておりません 通常の利用に問題のない範囲で応答しております
21	性能	バッチ処理時間	バッチ処理（一括処理）の応答時間	公開しておりません 通常の利用に問題のない範囲で処理しております
22	拡張性	カスタマイズ性	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	カスタマイズの内容については契約書およびマニュアルに記載がございます 機能追加を伴うカスタマイズにつきましては、都度対応可否を判断しております

No	カテゴリ	項目	補足	回答
23	拡張性	外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外 部のシステムとの接続仕様（API、開発言語等）	別途ご契約いただくことでFTP連携が利用可能です
24	拡張性	同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	制限はございません
25	拡張性	提供リソースの上限	ディスク容量の上限／ページビューの上限	制限はございません
26	サポート	サービス提供時間帯（障害対応）	障害対応時の問合せ受付業務を実施する時間帯	以下のとおり受付を行っております 電話：平日10:00 ~ 17:00メール：24時間365日
27	サポート	サービス提供時間帯（一般問合せ）	一般問合せ時の問合せ受付業務を実施する時間帯	以下のとおり受付を行っております 電話：平日10:00 ~ 17:00メール：24時間365日
28	データ管理	バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	日次でバックアップを取得しております バックアップは有効期間内は削除できないようになっています
29	データ管理	バックアップデータを取得するタイミング(RPO)	バックアップデータをとり、データを保証する時点	1時間を目標としております
30	データ管理	バックアップデータの保存期間	データをバックアップした媒体を保管する期限	30日間保持しています
31	データ管理	データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	サービス解約時に、必要に応じてデータを削除する場合がございます
32	データ管理	バックアップ世代数	保証する世代数	30日間保持しています
33	データ管理	データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	暗号化して保存されています
34	データ管理	マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	ストレージは分離しておりません テナントIDをもとに論理的に分離して管理しています

No	カテゴリ	項目	補足	回答
35	データ管理	データ漏えい・破壊時の補償／保険	データ漏えい・破壊時の補償／保険の有無	利用規約の範囲内で保証いたします
36	データ管理	解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏えいの懸念のない状態が構築できていること	必要に応じてデータを削除する場合がございます お客様がCSVデータをダウンロードできるようになっておりますので、解約前のダウンロードをお願いいたします
37	データ管理	預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	ございません ただし、通信経路はTLSで暗号化されています
38	データ管理	入力データ形式の制限機能	入力データ形式の制限機能の有無	データ入力時および送受信時に必要に応じて検証を実施しています
39	セキュリティ	公的認証取得の要件	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていること	ISO 27001の認定を取得しており、以下からご確認いただけます https://lp.tano.mu/security
40	セキュリティ	アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	週次で機械診断を実施しています
41	セキュリティ	情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること	データへのアクセスは業務上必要な従業員に制限しています
42	セキュリティ	通信の暗号化レベル	システムとやりとりされる通信の暗号化強度	TLS1.2以上を強制しています
43	セキュリティ	会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	ございません
44	セキュリティ	マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	テナントIDを識別子とし、論理的に分離しています

No	カテゴリ	項目	補足	回答
45	セキュリティ	情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	データへのアクセスは業務上必要な従業員に制限しています
46	セキュリティ	セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	個人別にIDを付与し、操作ログを追跡可能にしています
47	セキュリティ	ウイルススキャン	ウイルススキャンの頻度	従業員の端末はリアルタイムスキャンを有効化しています
48	セキュリティ	二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	バックアップはクラウド上に保持し、持ち出し可能な外部媒体への保管は禁止しています
49	セキュリティ	データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しています

TANOMU独自の項目

No	カテゴリ	項目	回答
1	セキュリティ	ログインパスワードが保存される際のパスワードの暗号化方式	ソルト付きハッシュ化され保存されています
2	セキュリティ	WAFを導入しているかどうか	WAFを導入し、監視体制を構築しております
3	セキュリティ	WAFの設定内容について	WAFの設定内容の詳細については公開しておりません
4	セキュリティ	管理者アカウントのログイン時に多要素認証を実施しているか	実施しています
5	セキュリティ	IPSやIDSを導入しているかどうか	IDSを導入しています
6	セキュリティ	利用することができる国を制限しているかどうか	制限ございません
7	セキュリティ	パスワードの文字列に対してルールがあるかどうか	以下の制限がございます 最低8文字/IDやメールアドレスと同一の文字列は禁止/数字のみのパスワードを禁止/リストに含まれる推測されやすいパスワードを禁止
8	セキュリティ	利用者が多要素認証を設定することができるかどうか	可能です
9	セキュリティ	Single Sign On に対応しているかどうか	LINEでのログインが可能です
10	セキュリティ	クレジットカード情報は取り扱っていますか	取り扱いはございますが、情報は外部の決済サービスプロバイダー側に保存されます
11	セキュリティ	ログやシステムが出力するファイルに、個人情報・決済情報・ユーザーIDやパスワードといった機密情報を保存していませんか	機密情報はログデータなどに出力していません
12	ネットワーク	利用時に消費されるデータ容量	ご利用いただく内容によって変動するため定めがございません
13	ネットワーク	利用時に必要なネットワーク帯域幅	ご利用いただく内容によって変動するため定めがございませんが、最低限1Mbps程度は必要になると思われます
14	その他	利用規約はどこで確認できますか	以下のサイト上でご確認いただけます https://lp.tano.mu/terms
15	その他	プライバシーポリシーはどこで確認できますか	以下のサイト上でご確認いただけます https://lp.tano.mu/security
16	その他	サーバーの所在地	日本国内です
17	その他	開発や運用を第三者に委託しているかどうか	ございません
18	その他	サービスの利用にあたり推奨環境はありますか	以下のサイト上でご確認いただけます https://lp.tano.mu/environment

改定履歴

セキュリティホワイトペーパー

版	改定日	改定内容
1.0	2025/02/13	初版発行

SLO

版	改定日	改定内容
1.0	2025/02/13	初版発行

セキュリティチェックシート

版	改定日	改定内容
1.0	2025/02/13	初版発行