

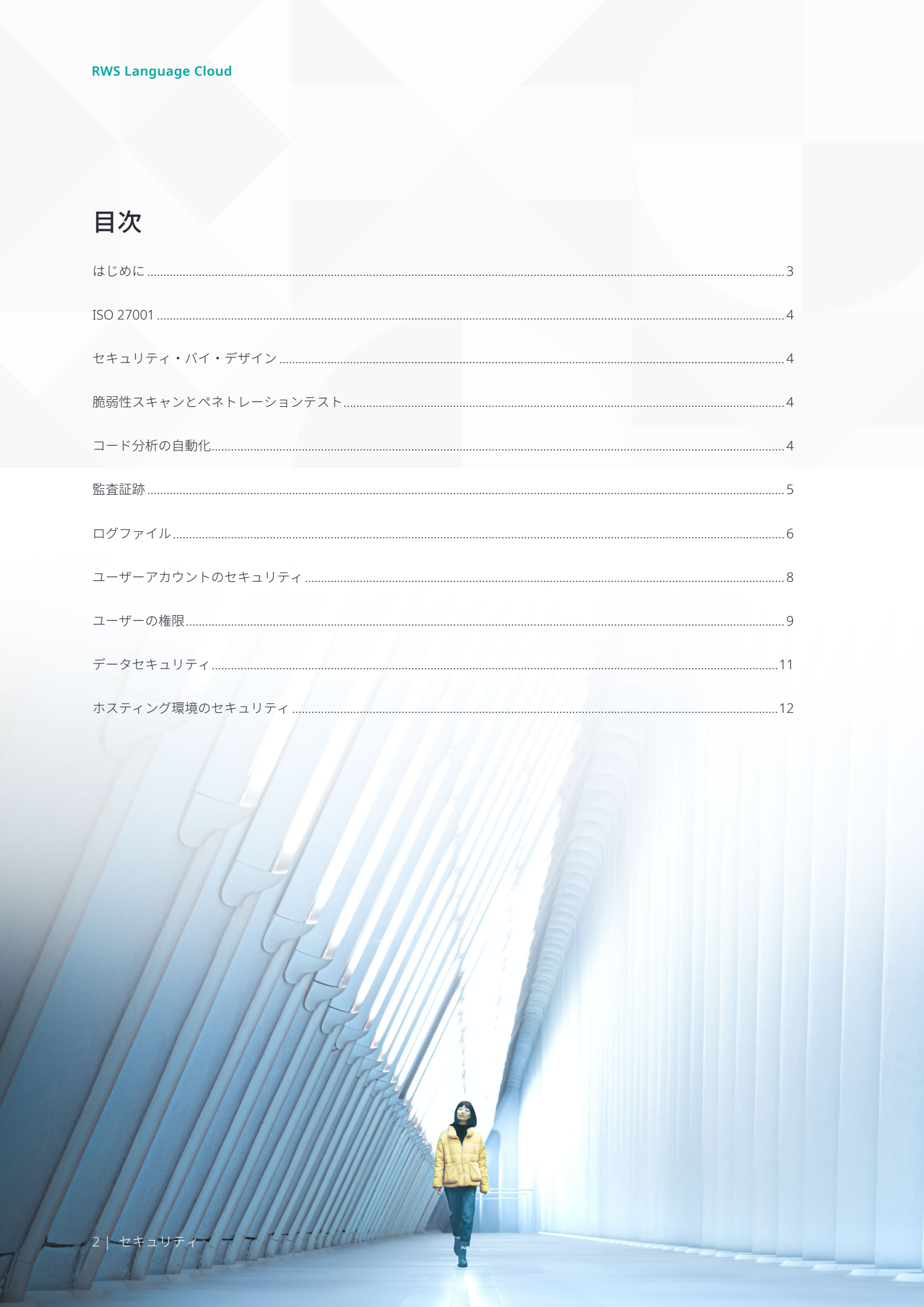


RWS Language Cloud

セキュリティ

目次

はじめに	3
ISO 27001	4
セキュリティ・バイ・デザイン	4
脆弱性スキャンとペネトレーションテスト	4
コード分析の自動化	4
監査証跡	5
ログファイル	6
ユーザーアカウントのセキュリティ	8
ユーザーの権限	9
データセキュリティ	11
ホスティング環境のセキュリティ	12



はじめに

お客様の情報のセキュリティは当社の最優先事項です。当社の人材、ポリシー、手順に支えられる最先端のテクノロジーを使用して、お客様のビジネスとデータを確実に保護します。

このホワイトペーパーでは、お客様がコンテンツを安心して処理および管理できる環境を実現するために、RWS® Language Cloud の開発やホストをどのように行っているのかを詳しくご説明します。こうした対策は、Trados® Enterprise、Trados® Accelerate、Trados® Team、Trados Studio® で提供されるクラウド機能など、Language Cloud でホストされている全製品に適用されます。

ISO 27001

RWS Language Cloud の開発組織は ISO 27001 認定を取得しています。つまり、使用している設備、チーム、ポリシー、手順が、独立した外部査定人による定期的な監査を受けているということです。



セキュリティ・バイ・デザイン

製品の新機能を開発する際に、当社はセキュアなソフトウェア開発ライフサイクルに従い、「セキュリティ第一」のアプローチを取っています。RWS Language Cloud では開発プロセスの一環として徹底したテストを行い、翻訳対象コンテンツやアプリケーションのユーザーに関するデータなど、処理対象となるデータにとって安全な環境を継続的に提供しています。

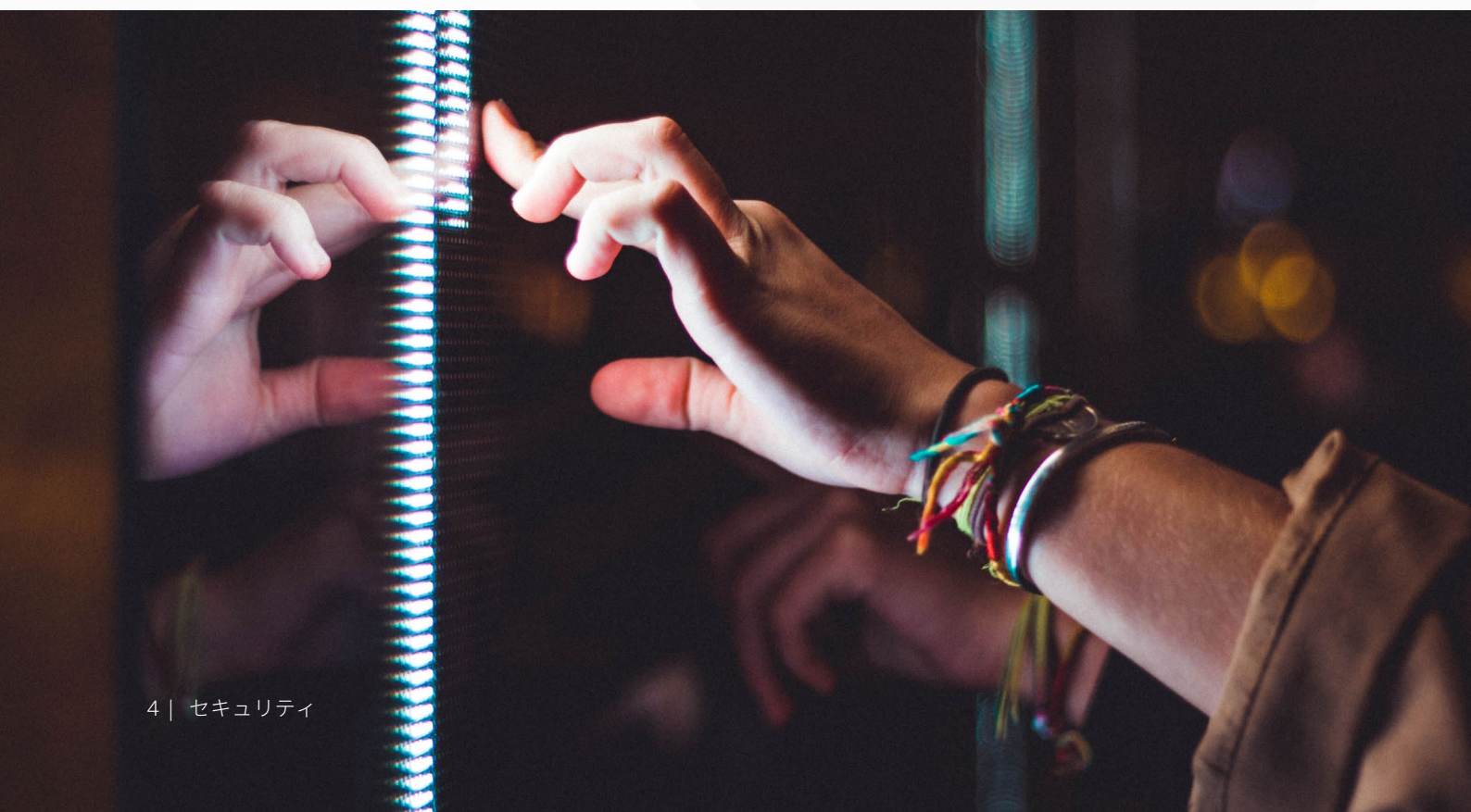
脆弱性スキャンとペネトレーションテスト

当社は、アプリケーションに対して厳格な脆弱性診断とペネトレーションテストを定期的に行っています。これには、ウェブアプリケーションセキュリティリスクの OWASP Top 10 に対するテストが必ず含まれています。毎年、第三者機関と協力して、外部の脆弱性テストとペネトレーションテストを実行しています。高レベルおよびクリティカルレベルの脆弱性は、できる限り早急に修正されます。中、低レベルの脆弱性は、リスクを考慮するか、問題が発生しない期間内に修復します。



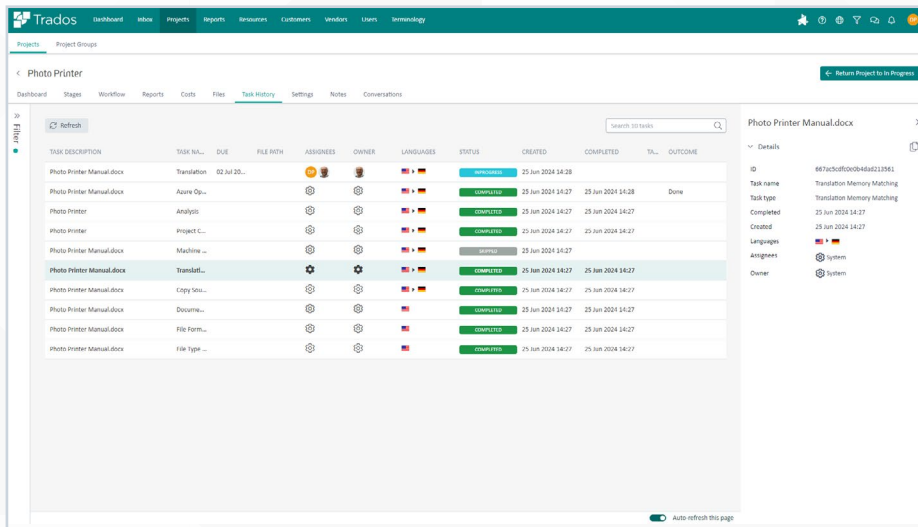
コード分析の自動化

ペネトレーションテストと脆弱性テストに加え、すべてのアプリケーションのソースコードに対して、静的アプリケーションセキュリティテスト (SAST) と動的アプリケーションセキュリティテスト (DAST) が実施されます。品質のしきい値を満たしていない場合は、ビルドに失敗するゲートがあります。こうした障害は自動的に発生するため、脆弱性が見つかった場合は、一連の監査可能なテストと再テストが実施されます。



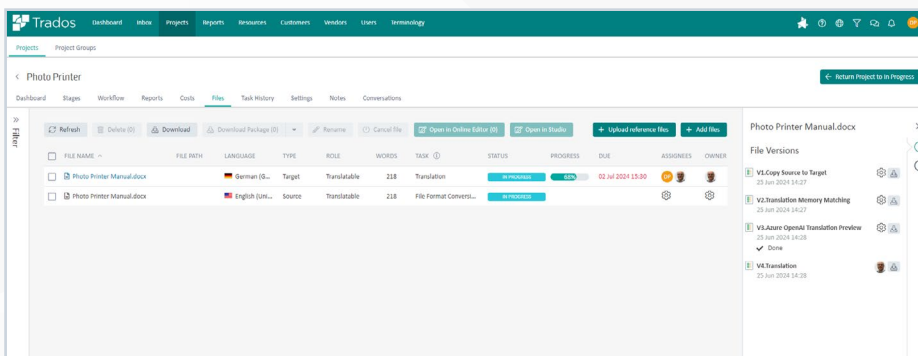
監査証跡

RWS Language Cloud では、アプリケーションで処理されたすべてのファイルについて完全な監査証跡が保持されます。予期しないセキュリティインシデントや潜在的なデータ漏えいが発生した場合、十分な権限を持つユーザー（通常は管理者）がワークフローの進行中にファイルの履歴を照会し、そのファイルで実行されたワークフロータスクとそのファイルにアクセスしたユーザーを特定することができます。



プロジェクトのファイルの監査証跡。

RWS Language Cloud では、ワークフローライフサイクル全体を通じて、ファイルの全バージョンの履歴も保持されます。以下のスクリーンショットは、さまざまなワークフロータスク（自動タスクとヒューマンタスク）を経たファイルのバージョン履歴を示しています。



ワークフローを進行中のファイルのバージョン履歴が表示される。

ログファイル

RWS Language Cloud には、セキュリティインシデントが発生した場合に使用できるさまざまなログファイルが用意されています。

UI のログファイル

RWS Language Cloud アプリケーションのユーザーインターフェイス（UI）にアクセスするユーザーを対象としたログファイルが作成され、標準の NCSA 複合ログ形式で保存されます。ログエントリの例：

```
10.228.144.254 - - [30/Aug/2024:03:08:14 +0000] "GET /lc/t/483384/dashboard HTTP/1.1" 200 14196 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36" 761 14548 581839
```

ログファイルには次の情報が含まれています。

- **[host]** - リクエストを行うクライアントの IP アドレスまたはホスト/サブドメイン名
- **[rfc931]** - リクエストを行うクライアントの識別子
- **[username]** - クライアントが認証に使用したユーザー名
- **[date:time timezone]** - リクエストのタイムスタンプ
- **[request]** - リクエストされたリソース、メソッド、プロトコルバージョン
- **[statuscode]** - リクエストの結果
- **[bytes]** - 転送されたデータのバイト数
- **[referrer]** - サイトに訪問したユーザーがクリックしたリンク元の URL
- **[user_agent]** - 訪問者が使用しているウェブブラウザとプラットフォーム
- **[cookies]** - ブラウザから渡された 1 つ以上の Cookie



マイクロサービスのログファイル

RWS Language Cloud プラットフォームはマイクロサービスアーキテクチャです。つまり、プラットフォームに多数のコンポーネント（またはサービス）が存在するという事です。サービスごとに1つのタスクがあり、ログファイルが作成されます。API リクエストは、プラットフォームインバウンドエンドポイント（API ゲートウェイ）と各内部コンポーネント（サービス）の両方でログに記録されます。デバッグ情報もログに記録され、特定の行動の追跡に役立ちます。以下に例を示します。

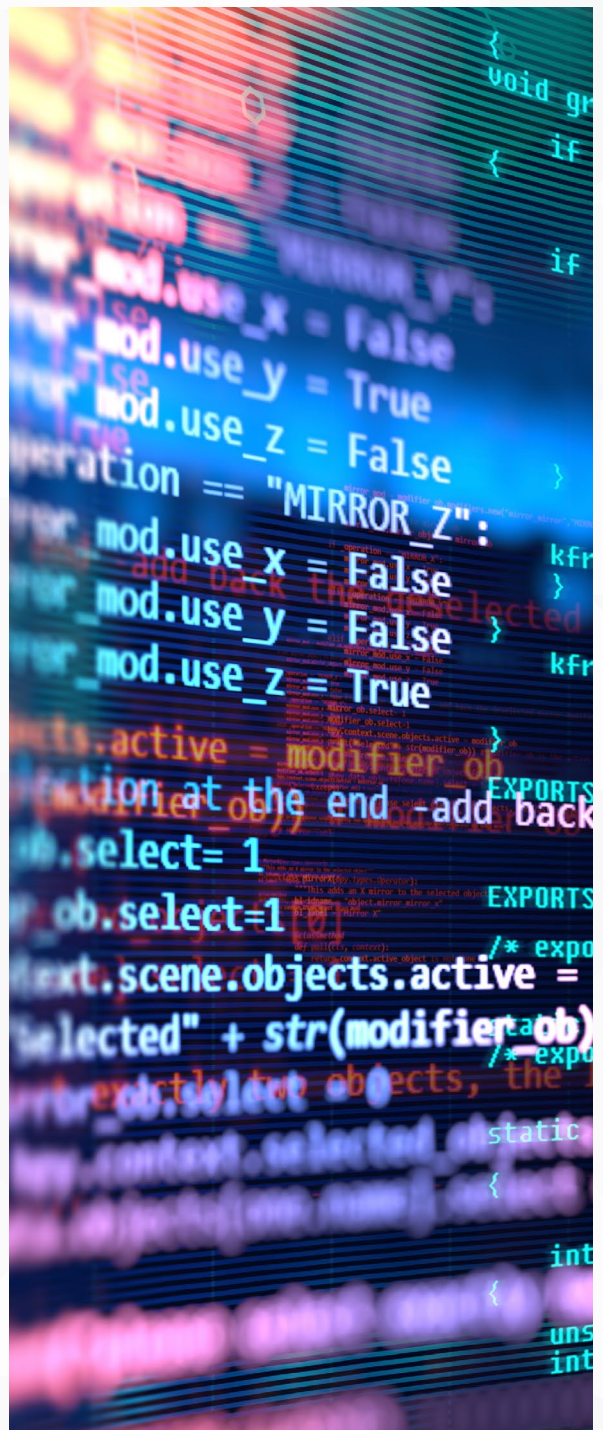
```
2024-09-01 07:45:31,880 INFO [http-nio-8765-exec-5179]
[e76eafec-506f-4645-b6b2-d163ba173379] [lc.api.gateway]
[guest] c.s.l.l.a.g.w.RequestLoggingConfiguration$1
[RequestLoggingConfiguration.java:35] Incoming request
[GET /gw-account-web/accounts/5ee8b4e27b56b01e50b71a82/settings?tenant=461371, client=10.228.60.25,
headers=[host:"de1-lc-apigw.sdlproducts.com",
accept:"*/*", authorization:"masked", x-lc-caller-app:"LCUI/2.2.9", x-lc-appsid:"masked"]]
```

```
2024-09-01 07:45:32,004 INFO [http-nio-8080-exec-74]
[e76eafec-506f-4645-b6b2-d163ba173379] [lc.account.
service] [5ee8b4e27b56b01e50b71a82]
c.s.l.g.a.s.a.AccountServiceImpl [AccountServiceImpl.
java:1484] getAccountSettings >>
5ee8b4e27b56b01e50b71a82
```

```
2024-09-01 07:45:32,011 DEBUG [http-nio-8080-exec-74]
[e76eafec-506f-4645-b6b2-d163ba173379] [lc.account.
service] [5ee8b4e27b56b01e50b71a82]
c.s.l.g.a.s.r.SubscriptionRepositoryImpl
[SubscriptionRepositoryImpl.java:191] There is no
subscription in cache for accountId=5ee8b4e27b56b01e50b71a82 sandbox=true
```

ログの監視と保存

デフォルトで、ログは一元管理されたロギングサーバーに90日間保持されます。基本的なログ監視を実施しており、内部APIエラーは自動的に監視され、エラー数が事前設定したしきい値を超えると、内部の連携ツールにアラートが発信されます。



ユーザーアカウントのセキュリティ

RWS Language Cloud には、ユーザーセキュリティをサポートするさまざまな機能が組み込まれています。

RWS ID

RWS Language Cloud のすべてのユーザーは、RWS ID を使用してプラットフォームにアクセスする必要があります。RWS ID はシングルサインオン (SSO) ソリューションで、Auth0 が提供するサードパーティ製 ID プラットフォームがベースになっています。Auth0 は、最高レベルのセキュリティ資格情報を提供するプロバイダとして高く評価されています。Auth0 のセキュリティについて詳しくは、auth0.com/security をご覧ください。

フェデレーション

RWS ID は、お客様の ID プロバイダにフェデレーションできます。これにより、お客様自身の環境と同じレベルのセキュリティを確保できます。フェデレーションのオプションには、LDAP、ADFS、Azure Active Directory、OpenID Connect、SAML などがあります。

多要素認証

RWS ID をお客様の ID プロバイダとフェデレーションしない場合は、多要素認証 (MFA) をドメイン単位で実装可能です。MFA は認証方式の 1 つで、認証メカニズムに対して次の証拠 (要素) を複数提示できなければ、ユーザーにアクセス権が付与されません。

- 知識要素 (パスワードなど、そのユーザーが知っていること)
- 所有要素 (モバイルデバイスなど、そのユーザーが持っているもの)
- 生体要素 (指紋など、そのユーザーを示すもの)

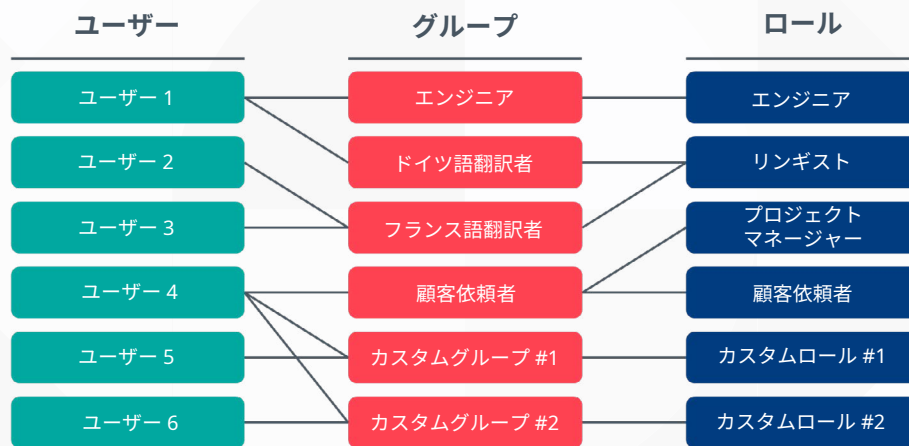
セッションタイムアウト

RWS Language Cloud でセッションが非アクティブのままになっていると、自動的にタイムアウトします。ユーザーがアプリケーションで作業を続行するには、再認証が必要になります。



ユーザーの権限

RWS Language Cloud では、各ユーザーが1つ以上のユーザーグループに属し、各グループに1つ以上のロールが割り当てられます。ロール（一連の権限）によって、グループのメンバーがどの組織構造レベルで、どの処理を実行できるのかが決まります。複数のグループに属するユーザーのロールを決める場合、各グループのロールをすべてまとめたスーパーセットを作成します。



ユーザーとグループはアカウント管理者によって管理されます。マネージドサービスについては、RWSの担当者がアカウント管理者になり、ユーザーやグループを設定しますが、設定後、RWSの担当者がお客様のデータにアクセスすることはできません。また、RWSが一切関与せず、各自でユーザーとグループを管理することもできます。

Jane Smith

<p>First name *</p> <input type="text" value="Jane"/>	<p>Groups *</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; gap: 5px;"> PM Project Managers x A Administrators x E Engineers x T Terminologists x </div>
<p>Last name *</p> <input type="text" value="Smith"/>	<p>Domains</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; gap: 5px;"> M Manufacturing x IT IT x </div>
<p>Email *</p> <input type="text" value="jsmith@translationsrus.com"/>	
<p>Location *</p> <input type="text" value="/Root"/>	

プラットフォームでユーザーを追加し、グループに割り当てる。

独自のロール

RWS Language Cloud では、既定のロールのほかに、独自のロールを作成してグループに割り当てることができます。カスタムロールには複数の権限を付与することができ、グループのメンバーが実行できる処理を柔軟に決めることができます。

新しいカスタムロールを作成する。

プロジェクトの設定

追加のプロジェクト設定も構成できます。[ファイルのダウンロードを制限する]チェックボックスをオンにすると、ユーザーはオフラインで翻訳するためにファイルをダウンロードできなくなります。その代わりに、ファイルをダウンロードせずに、Online Editor で作業を完了させる必要があります。指定した日数が経過した後、プロジェクトを自動的に完了させてアーカイブすることもできます。これにより、プロジェクトが意図せずアクティブなままになっていた場合に、データにアクセスされないように防止できます。

プロジェクト設定を編集して、プロジェクトデータへのアクセスを制限する。

データセキュリティ

RWS は、データを運用しホストしている国で適用されるデータプライバシーとセキュリティに関するすべての法律を遵守するよう取り組んでいます。

アカウントの作成時に使用される PII

PII（個人を特定できる情報）とは、個人の身元を明らかにするために使用される可能性のある、個人に関連付けられたあらゆる情報を指します。RWS ID にはユーザーに関する最小限の情報（名前や E メールアドレスなど）が保存されており、こうしたデータを他のシステムで使用できないようになっています。ユーザーに関連付けられた PII は、リクエストに基づいて編集、エクスポート、削除できます。

翻訳用に送信されるコンテンツ内の PII

現時点で、RWS Language Cloud には、自動匿名化や仮匿名化に関する規定はありません。翻訳対象のデータを RWS Language Cloud に送信する前に、必要に応じて、ユーザーが匿名化または仮匿名化を指定できます。

保存中の暗号化

アプリケーション内にあるすべてのデータが、保存時に暗号化されます。データ転送にはセキュアなプロトコルも使用します。ユーザーのローカルシステムにダウンロードされたデータが暗号化される保証はありませんが、セキュアなプロジェクト機能を使用してこうしたリスクを軽減できます。

データの分離

各顧客のデータは他のすべての顧客のデータから論理的に分離されているため、顧客は互いのデータを「見る」ことができません。RWS Language Cloud は、テナントレベルの分離にメタデータを使用します。実行時のテナント分離は、ベストプラクティスに従って動的に生成された ID とアクセス管理ポリシーを使用して実行されます。

データのテスト

また、開発環境とテスト環境は本番環境から切り離されており、共通のデータは存在しません。特に許可が与えられていない限り、当社がテスト環境や開発環境で顧客データを使用することはありません。

データの保管場所

RWS Language Cloud は、AWS Frankfurt と AWS Montreal でホストされています。お客様は、データを保存するロケーションを選択できます。選択すると、リクエストしたロケーションにすべての顧客データが保存されます。AWS Frankfurt のバックアップは、AWS Ireland に保存されます。AWS Montreal のバックアップは、AWS Calgary に保存されます。

AI 機能使用時のデータのセキュリティ

RWS Language Cloud で利用できる AI 機能は、他のアプリケーション機能と同じセキュリティ対策に従って設計、開発、導入、運用、保守されています。RWS は、お客様のデータはお客様のものであり、データを使用する場所はお客様が指定する必要があると認識しています。当社の AI 機能は、顧客データを大規模言語モデル (LLM) のトレーニングや微調整に使用していません。当社が AI を活用した機能を使用する場合、次の 2 つのカテゴリのいずれかに該当する AI モデルを使用します。

- **RWS が制御**
RWS が制御する AI モデルは AWS のインフラストラクチャでホストされているため、顧客データがコアホスティング環境から離れることはありません。
- **顧客が制御**
お客様が外部の AI モデルを使用している場合、このモデルとの間でデータがセキュアに転送されます。モデル内のデータのセキュリティは、お客様の責任です。

ホスティング環境のセキュリティ

ホスティング環境のセキュリティ

RWS Language Cloud は、RWS Cloud Operations によって SaaS アプリケーションとしてホストされています。この部門はすべてのホスト型製品で ISO 27001 認定を取得しており、SOC 2 Type 2 認証の統制と方針に完全準拠しています。

さらに RWS Cloud Operations は、さまざまなセキュリティツールや機能も利用してお客様のデータのセキュリティを確保しています。たとえば、次のような機能があります。

- ・ 異常検出機能を備えたイベント管理監視ツール
- ・ 境界ファイアウォール、ウイルス対策付きの統合型ネットワーク脅威防御 (NTP)
- ・ リアルタイムのイベント管理アクティビティをサポートする 24 時間年中無休の運用体制
- ・ 脅威を可視化する業界推奨ツール
- ・ 最先端の脆弱性 & ペネトレーションセキュリティテストスキャナー
- ・ IT Infrastructure Library (ITIL) に準拠したインシデント管理用チケットツール

ホスティングプロバイダのセキュリティ

当社は、Amazon Web Services (AWS) と当社製品のホストに関する契約を締結しています。AWS は、ISO 27001、SSAE 16、SOC 1、SOC 2、SOC 3 を始めとした複数のセキュリティ認定を取得しています。ホスティングパートナーが採用しているセキュリティ対策に加え、RWS では次に関するポリシーや手順も定めています。



アクセス制御



データセキュリティ



物理的な保護



可用性と積極的な監視



論理的な保護



リスク評価



データバックアップ

ウイルス対策

RWS Language Cloud にアップロードされたすべてのファイルは、ウイルス対策ソフトウェアによって自動的にスキャンされます。悪意のあるコンテンツが存在するとフラグが付けられたファイルは、ダウンロードがブロックされ、隔離されます。RWS Language Cloud は、こうしたファイルを感染していないバージョンに置き換える機能を備えています。

セキュリティに対する当社のアプローチについて詳しくは、こちらをご覧ください
rws.com/jp/legal/security

当社のプライバシーポリシーについては、こちらをご覧ください
rws.com/jp/legal/privacy

RWS について

RWS Holdings plc は、テクノロジーを駆使した言語サービス、コンテンツサービス、知的財産サービスを提供する、唯一無二のリーディングプロバイダです。当社はコンテンツの変革と多言語データ分析を通じて、AI を活用したテクノロジーと人間の専門知識を組み合わせ、お客様がどこでも、あらゆる言語で理解されるようにすることでビジネスの成長をサポートします。

当社が目指しているのは、グローバルな理解の実現です。文化の理解、企業の理解、技術の理解を組み合わせることにより、当社のサービスとテクノロジーが、顧客の獲得と維持、魅力的なユーザー体験の提供、コンプライアンスの維持、データやコンテンツにおける実用的なインサイトの獲得など、お客様をさまざまな面でサポートします。

過去 20 年間にわたり、当社は独自の AI ソリューションを進化させるとともに、お客様による多言語 AI アプリケーションの探求、構築、使用を支援してきました。また、45 件以上の AI 関連特許と 100 件以上の査読論文を保有し、お客様の AI 導入をサポートしてきた経験と専門知識があります。

世界のトップブランド 100 社の 80% 以上、フォーチュン誌の「最も賞賛される企業」20 社の 4 分の 3 以上、さらに大手製薬会社、投資銀行、法律事務所、特許事務所のほぼすべてが当社を利用しています。クライアントベースは、ヨーロッパ、アジア太平洋、アフリカ、北南米に広がっています。5 つの大陸に展開した 65 を超えるグローバル拠点から、自動車、化学、金融、法律、医療、製薬、テクノロジー、電気通信の各分野のお客様にサービスを提供しています。

1958 年に設立された RWS は、英国に本社を置き、AIM、ロンドン証券取引所規制市場に上場されています (RWS.L)。

詳細については、www.rws.com/jp をご覧ください。

© 2024 All rights reserved. ここに記載されている情報は、RWS Group* の機密情報および専有情報とみなされます。

* RWS Group とは、RWS Holdings plc およびその関連会社および子会社の代表を意味します。