ホワイトペーパー

Asana のセキュリティとプライバシー

Asana によるデータ保護

asana

目次

はじめに 4
インフラストラクチャ 5
- ウェブサーバー 6
- データベース 6
  - マスター 6
  - 顧客データ 6
  - ユーザーデータ 6
- ファイルストレージ 6
- ヨーロッパのインフラストラクチャ 6
- データセキュリティ 7
  - 転送時の暗号化 7
  - 保存時の暗号化 7
- マルチテナンシー 8
- スケーラビリティおよび信頼性 8
  - システム可用性のレベル 8
  - 稼働状況確認ページ 8
- バックアップ 8

製品セキュリティ機能 9
- 管理者 9
- ユーザープロビジョニング機能 9
- ログインセキュリティ 9
  - パスワードの安全措置 9
  - Google SSO 10
  - SAML を使用したシングルサインオン 10
- アクセス権限 10
  - Asana オブジェクト 10
    - タスク 10
    - プロジェクト 11
    - チーム 11
    - 組織 11
    - ユーザー 11
- ゲスト管理 12
- アプリのホワイトリスト 12
- データコントロール 13

アプリケーションのセキュリティ 14

Asana プラットフォーム 15
連携 15
サービスアカウント 15
サードパーティアプリケーション 16
運用上のセキュリティ 17
Asana の情報セキュリティ 17
機密情報 17
人事管理 17
ユーザーアクセスのレビューとポリシー 17
物理的セキュリティ 17
Asana の拠点 17
データセンターセキュリティ 18
ネットワークセキュリティ 18
IT セキュリティ 18
リスクと脆弱性の管理 18
侵入テスト 18
バグバウンティ 18
ソフトウェア開発ライフサイクル 19
インシデントレスポンス 19
災害復旧と事業継続 19
データ保持とデータ廃棄 20
データ保持 20
データ廃棄 20
監視 20
サブプロセッサーとベンダー管理 20
プライバシー、証明書、コンプライアンス 21
プライバシーポリシー 21
証明書と法令順守 21
プライバシーシールドフレームワーク 21
サービスと組織の統制 (SOC 2) 21
GDPR 22
DPA 22
法の執行 22
おわりに 23

最終更新: 2020年 2月[1]

[1] 本ホワイトペーパーは Asana のセキュリティの現状を説明していますが、将来、機能 / 製品がリリースされた時点で変更される場合があります。

はじめに

現在、世界中の企業が、日常業務から戦略的イニシアチブまで、より協働的かつフレキシブルに仕事を管理、整理するために、新しいツールを導入しています。これらのツールは仕事管理ソリューションと呼ばれる新しいソフトウェアのカテゴリに属し、Asana はその代表的存在です。

Asana はチームがより迅速にビジネスの結果を出せるよう、仕事の計画、整理、実行を支援します。195 か国で 75,000 社以上が有料サービス会員で、数百万人が利用する Asana は、チームの全員が何を、誰が、いつまでにやるべきか、確実に把握できるようにすることで、透明性 (クラリティ) の向上を進め、仕事に対するメンバーの足並みを揃えることに役立っています。Asana で作成されたタスクは、なんと 10 億以上に上ります。

お客様は安心して Asana にデータを預けられるため、ビジネスにとって最も重要な仕事に集中できます。だからこそ、当社では使いやすくコラボレーションに適したワークマネジメントソリューションを作ることだけでなく、お客様のデータを安全に守ることに力を入れています。

Asana では、企業文化を通じて、全従業員のセキュリティ意識を高めています。この信用と透明性を重んじる企業文化こそが、お客様の情報資産の保護に対する全体的な考え方、自覚、重視の姿勢を方向付けています。当社の経営陣は、ポリシー声明、行動規範、共通のミッションや価値観に関する表明を通じて、こうした意識を当社の価値観や行動基準の中で強化し、また「全部任せ、全責任を負う」姿勢を推奨する環境作りのために、さまざまなアクションを起こしています。

Asana はセキュリティプログラムとセキュリティ慣行の設計および実装に当たり、以下の原則を重視します。

- 不正アクセスから当社のウェブアプリおよびモバイルアプリを保護するための、物理的および環境的セキュリティ
- アプリケーションの可用性の維持
- 顧客データを保護するための機密性
- ライフサイクルを通してデータの正確性と一貫性を保持するための整合性

本ホワイトペーパーでは、インフラストラクチャ、製品、運用、コンプライアンス、認証の観点からセキュリティとプライバシーについて説明します。

本ホワイトペーパーの大部分はすべての Asana プランに当てはまりますが、Premium、Business、Enterprise の有料プランを念頭に置いて作成されています。[2] 機能が一部のプランで利用できない場合は、その旨明記されています。

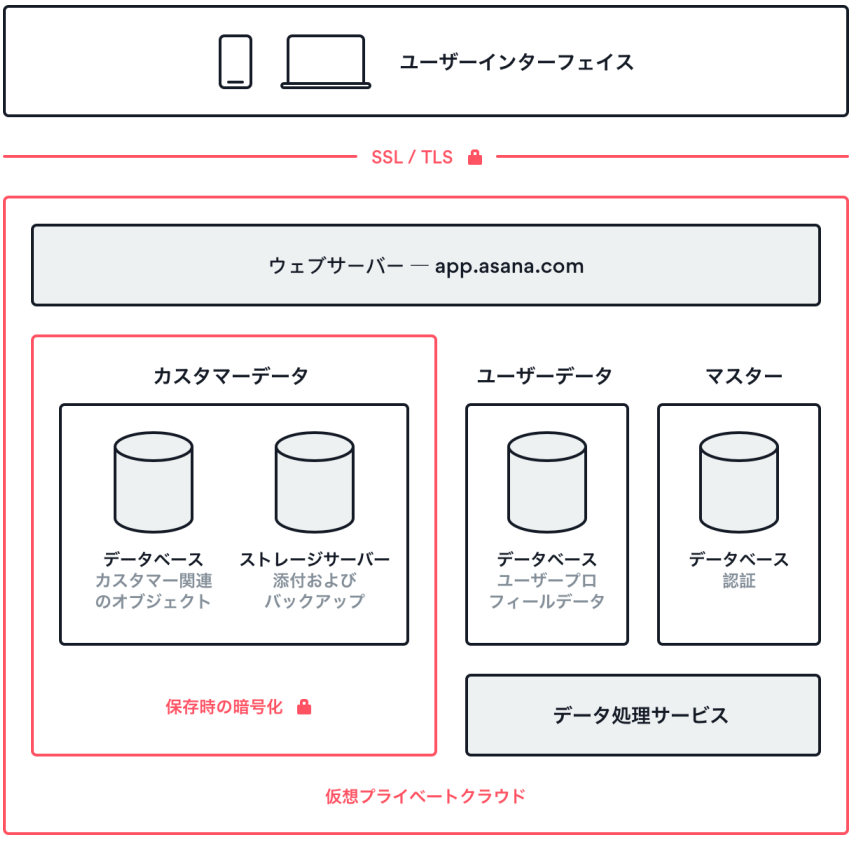
[2] Asana の各プランについて詳しくは、 asana.com/pricing をご参照ください。

インフラストラクチャ

Asana は、主に Amazon Web Services (AWS) のクラウドコンピューティングサービス製品を、Asana プラットフォームの土台となる構成要素として活用しています。

AWS はクラウドコンピューティングインフラストラクチャのセキュリティとコンプライアンスを管理し、Asana はクラウドコンピューティングインフラストラクチャ上のソフトウェアと機密データのセキュリティとコンプライアンスを管理します。AWS の責任共有モデルをご参照ください。[3]

Asana は Amazon の仮想プライベートクラウドを使用し、AWS が提供するネットワーキングサービスと構成要素を使用してセキュアでスケーラブル、管理が簡単なネットワークアーキテクチャを設計しました。Amazon の Elastic Compute Cloud (EC2) サービスが Asana プラットフォームの大部分を実行し、信頼性が高く、スケーラブルでセキュアな方法で、お客様のデータを処理します。下に Asana のインフラストラクチャを簡単に図示します。



[3] http://aws.amazon.com/compliance/shared-responsibility-model
* 暗号化は Enterprise のお客様のみに適用されます。

当社の本番環境のインフラストラクチャはロックダウンされており、当社の負荷分散装置のみが、外部からのウェブトラフィックを受信できます。各ホストには役割が割り当てられています。セキュリティグループを使用して、これらの役割の間で予測されるトラフィックを定義しています。

ウェブサーバー

Amazon の CloudFront コンテンツ配信ネットワーク (CDN) を使用して、Asana の静的アセットをスケーラブルな方法で低遅延かつ高速に転送します。

データベース

データベースは Amazon のリレーショナルデータベースサービス (RDS) で、マネージド MySQL データベースを運用します。

マスター

それぞれのユーザーの、暗号化されたパスワード (ハッシュ化およびソルト化された bcrypt) と認証情報を保管します。

顧客データ

チーム、プロジェクト、タスクなど、お客様が Asana にアップロードしたすべての情報を保管します。

ユーザーデータ

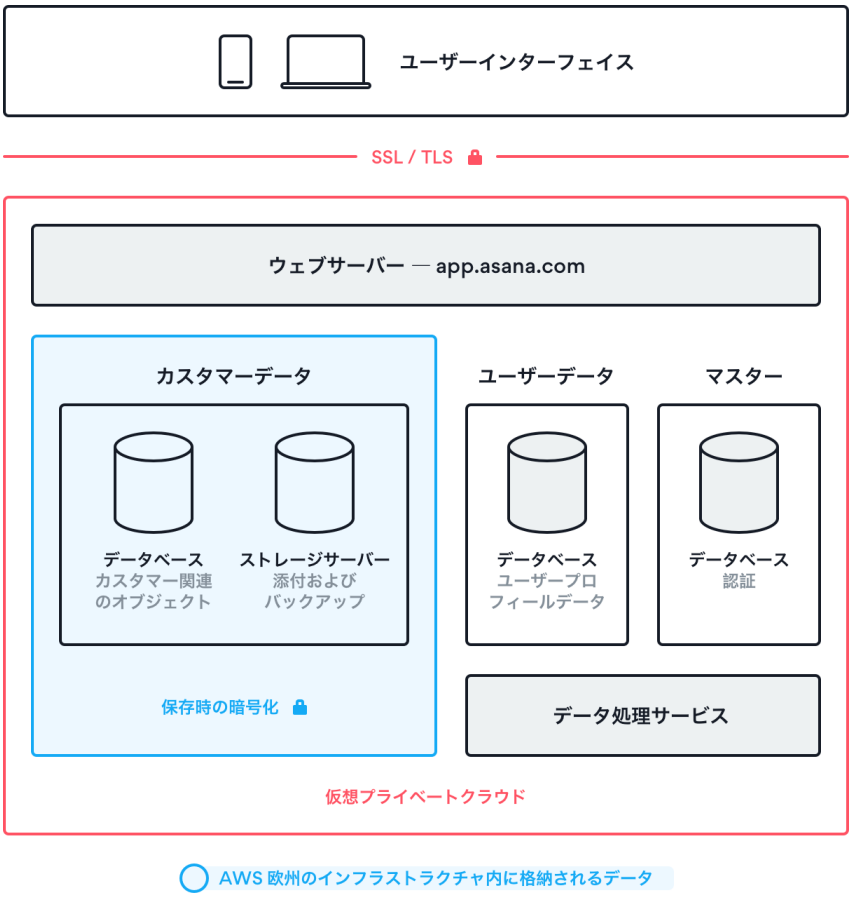
ユーザー名やメールアドレスなど、ユーザープロフィールに関連した情報を保管します。

ファイルストレージ

ストレージサーバーは Amazon の Simple Storage Service (S3) です。ここには添付ファイルやデータベースのバックアップが保管されます。添付ファイルは、コンピューターから Asana タスクに直接アップロードされたあらゆるファイルを指します。クラウドホストのコンテンツコラボレーションプラットフォームからの添付ファイルは、これらのプラットフォームへのリンクとして作成され、Asana のストレージサーバーには保管されません。

ヨーロッパのインフラストラクチャ

Asana はデータをヨーロッパ内に置く必要のある Enterprise のお客様に対して、ヨーロッパのデータセンターを提供します。顧客データはフランクフルト (ドイツ) の AWS 欧州リージョンに保管され、バックアップがダブリン (アイルランド) の AWS リージョンに保管されます。米国とヨーロッパのインフラストラクチャについて、いずれも AWS データセンターを使用します。組織全体の顧客データは、お客様の要望に応じて米国または EU 内に保管されます。下図は、お客様がヨーロッパのインフラストラクチャを利用する場合の、Asana のインフラストラクチャを簡易的に表したものです。



データセキュリティ

転送時の暗号化

app.asana.com への接続は 128 ビット暗号で暗号化され、TLS 1.2 以上のバージョンをサポートします。接続の暗号化と認証には AES_128_GCM、鍵交換方式には ECDHE_RSA が使用されます。Asana は Forward Secrecy と AES-GCM をサポートし、RC4 または SSL 3.0 以下のバージョンを使用した安全でない接続を禁止します。グインと機密データの転送は TLS/SSL のみで実行されます。

保存時の暗号化

Enterprise のお客様向けに、Asana は顧客データが保管時に AES 256 ビット秘密鍵を使用して暗号化されることを保証します。

マルチテナンシー

インフラストラクチャは複数の顧客インスタンス間で共有されます。したがって Asana はマルチテナントのウェブアプリケーションです。アカウントの認証、論理的なデータベースフィールドの分離、セッション管理コントロールを実装して、お客様のアクセスを、それぞれの組織に関連したデータのみに制限しています。

スケーラビリティおよび信頼性

Asana はサービスのスケーラビリティを保証する Amazon Web Services を使用しています。データベースは同期して複製されるので、データベースの障害が発生してもすばやく復元できます。また、万一に備えてデータベースのスナップショットを定期的に作成し、離れた場所にあるデータセンターで安全に保管することにより、たとえ Amazon のリージョン全体で障害が起きたとしても、必要に応じて別の場所で復元できるようにしています。

システム可用性のレベル

Enterprise のお客様には 99.9% のサービス稼働時間を保証しています。

稼働状況確認ページ

信頼とは努力によって得るものであり、私たちは、システムのステータスとパフォーマンスについて透明性を提供することがそのはじめの一歩だと信じています。Asana の稼働状況確認ページでは、過去 12 時間、7 日間、30 日間、1 年間のウェブアプリ、モバイルアプリ、API の可用性を公開しています。 trust.asana.com をご確認ください。

バックアップ

データベースのスナップショットは毎日作成されます。バックアップは本番環境のデータベースと同じ方法で保護されています。Enterprise のお客様には、バックアップのクロスリージョンコピーを行うことを保証します。

製品セキュリティ機能

Asana はユーザーや管理者がデータを保護するために必要な機能を備えています。これらの機能はお客様のデータの包括的な管理コントロールと可視性を提供します。下記の機能の一部は Asana のプランによってはご利用になれない場合があります。Asana のプランについては、 asana.com/pricing をご覧ください。

管理者

管理者は、ユーザーが組織やワークフローに参加、離脱するのに合わせて、チームを管理して、メンバーやゲストの追加や、プロビジョニングの解除を行えます。また、管理者は管理 API を使用してドメインのエクスポート、構成、権限、サードパーティアプリ、チーム設定、ユーザー設定を管理することもできます。

ユーザープロビジョニング機能

Asana では、ユーザーや管理者が、自身のデータにアクセスできるメンバーを管理できます。

- ユーザーや管理者は、メンバーやゲスト (外部メンバー) を組織やチームに招待できます。
- 管理者は管理者コンソールから任意のメンバーやゲストを削除できます。

さらに、Enterprise のお客様は SCIM (クロスドメインアイデンティティ管理システム) 標準を使って、Asana と自社のクラウドアイデンティティプロバイダーを連携することで、その他の SaaS ソリューションと同時にユーザーのプロビジョニングやプロビジョニングの解除を実行できます。

ログインセキュリティ

Asana の管理者は、ユーザーが Asana のアカウントにログインする際の認証方法を決定できます。これには、Asana 認証情報、Google SSO、SAML 2.0 を使ったシングルサインオンの 3 つのオプションがあります。

パスワードの安全措置

ユーザーが Asana 認証情報でアカウントにログインすることを許可されている場合、管理者はパスワードの強度要件を指定できます。「強力な」パスワードを必要条件にすると、ユーザーは小文字、大文字、数字、特殊文字のうち 3 つを含む 8 文字以上のパスワードを使用する必要があります。

また、管理者は、組織のすべてのユーザーのパスワードを強制的にリセットすることもできます。

Google SSO

管理者は組織のユーザーに、Asana へのログインに Google GSuite アカウントを使用することを指定できます。

SAML を使用したシングルサインオン

Enterprise の管理者はアイデンティティプロバイダー (IdP) を構成し、ユーザーに対し、クラウド IdP アカウント認証情報を使用して Asana にログインすることをリクエストできます。これは SAML 認証標準に基づいて構成されます。

アクセス権限

管理者およびユーザーは他のユーザーを招待して自身のデータへのアクセスを許可することができます。ユーザーを組織に招待する際には、さまざまな権限設定が可能です。招待されるユーザーのアクセス権は、オブジェクトレベル (タスク、プロジェクト、チーム、組織) で、いくつかの種類から選んで設定できます。アクセス権はユーザーレベルでなくオブジェクトレベルで定義されます。つまり、1 人の同じユーザーでも、コンテンツに応じてコメント限定でアクセスできたり、完全に非表示となったり、リクエストによる「承認制」でアクセスできたり、完全な利用権限が付与されたり、といったことがあり得ます。各オブジェクトや権限の種類についての詳細は Asana ガイド、asana.com/guide でご確認ください。

Asana オブジェクト

タスク

Asana のタスクの公開設定は、非公開、公開、非公開プロジェクトに含まれる、または公開プロジェクトに含まれる、のいずれかになります。

タスク:	**アクセスできるユーザー:**
非公開タスク	タスクのコラボレーターのみ
公開タスク	組織メンバー全員
非公開プロジェクト内のタスク	タスクのコラボレーターとプロジェクトメンバー
公開プロジェクト内のタスク	タスクのコラボレーター、プロジェクトメンバー、チームメンバー
サブタスク	タスクのコラボレーターと親タスクにアクセスできるメンバー

プロジェクト

Asana のプロジェクトは非公開にすることも公開することもできます。プロジェクトへのアクセス権を持つユーザーは、そのプロジェクト内のすべてのタスクや会話にアクセスできます。プロジェクトにユーザーを追加するとき、編集可能またはコメント限定のいずれかのアクセス設定をすることができます。

プロジェクト:	**アクセスできるユーザー:**
非公開プロジェクト	プロジェクトメンバー
公開プロジェクト	チームメンバーとプロジェクトメンバー
公開チーム内の公開プロジェクト	組織メンバー、チームメンバー、プロジェクトメンバー

チーム

Asana のチームは非公開、公開、または承認制にすることができます。チームに所属するメンバーは、そのチームのすべての会話と公開プロジェクトにアクセスできます。

チーム:	**アクセスできるユーザー:**	**参加の可否:**
非公開	チームメンバー	不可
組織に公開	チームメンバーと組織メンバー	可
承認制チーム	承認制チーム	要承認

組織

Asana の組織はチーム、プロジェクト、タスクを含む最上位のオブジェクトです。

ユーザー

Asana のユーザーは、使用するメールアドレスに関連付けられた個人のアカウントを取得します。そのアカウントには上述のさまざまなデータオブジェクトへのアクセス権が付与されます。さらに、デフォルトでは、ユーザーアカウントは使用するメールドメインに基づき、1 つの組織に自動的にアクセスできます。

フルメンバー

組織のメンバーシップは、使用するメールアドレスに関連付けられているドメインを基にしています。組織のメンバーになるには、組織が承認しているメールドメインのいずれかを持つメールアドレスを使用する必要があります。

組織のメンバーができることは以下のとおりです。

- 新しいチームの作成
- 組織内で参加リクエストが可能な全チームのリストの表示
- 組織内の他のメンバーやゲストの名前とメールアドレスの表示
- 組織で公開されているプロジェクトやタスクへのアクセス

ゲスト

組織で承認されたメールドメインのメールアドレスを持たないクライアント、請負業者、お客様などの外部メンバーは、組織のゲストとしてコラボレーションできます。ゲストには組織内で限定的なアクセス権が与えられ、本人に明示的に共有されたもののみ閲覧できます。

組織のゲストは、招待されない限りチームに参加することはできません。また、他のチームを作成、表示したり、チームへの参加をリクエストしたりすることはできません。

限定アクセスメンバー

チームにはそれぞれ独自のメンバーが所属し、固有のプロジェクトがあります。チーム内の一部のプロジェクトにアクセス権がない人は、チーム設定のメンバータブに限定アクセスメンバーであることが表示されます。

限定アクセスメンバーは、自分が追加されたプロジェクトとタスクは見ることができますが、チームの会話や他のプロジェクトは見ることができません。

ゲスト管理

Enterprise の管理者は、外部メンバー (ゲスト) を招待できるユーザーを指定できます。管理者は以下の 3 つのオプションのいずれかを選択して、組織ゲストを招待する権限を持つユーザーを決めることができます。

- 管理者のみ
- 管理者と組織メンバー
- 全員 (組織メンバーとゲストの両方が含まれます)

アプリのホワイトリスト

Asana Enterprise の管理者は、Asana のアカウントを持つユーザーが使用できるサードパーティ連携を決めたり、好ましくない連携をブロックしたりできます。 asana.com/apps を参照して、利用可能なサードパーティアプリケーションをご確認ください。

データコントロール

お客様は簡単に Asana のデータを選択してエクスポートしたり削除したりできます。また、Asana API を使用してドメイン全体のデータを自動的にエクスポートすることもできます。

アプリケーションのセキュリティ

Asana のサービスは、ウェブベースの SaaS (サービスとしてのソフトウェア) アプリケーションです。ユーザーは、ウェブブラウザー、モバイルアプリケーション (Android と iOS)、アプリケーションプログラミングインターフェイス (API) を使用して自身のデータにアクセスできます。

Asana を構成するサービスとコンポーネントは、React アプリケーションフレームワークに基づいて、主に JavaScript、TypeScript、Python、Scala で書かれています。Asana は OWASP Foundation が定義するセキュリティベストプラクティスに従い、常にセキュリティバイデザインというアプローチに基づいて開発されています。このように、当社は包括的な措置を講じて、以下のトピックを含む (ただし、これに限定されない) セキュリティリスクを回避しています。

- インジェクション
- 認証の不備
- 機密データの露出
- XML 外部実体攻撃 (XXE)
- アクセス制御の不備
- セキュリティ設定のミス
- クロスサイトスクリプティング (XSS)
- 安全でないデシリアライゼーション
- 既知の脆弱性を持つコンポーネントの使用
- 不十分なロギングと監視
- クロスサイトリクエストフォージェリ (CSRF)
- 未検証のリダイレクトと転送

Asana は OWASP Top 10 のすべてのリスクに対する監査を毎年受けています。

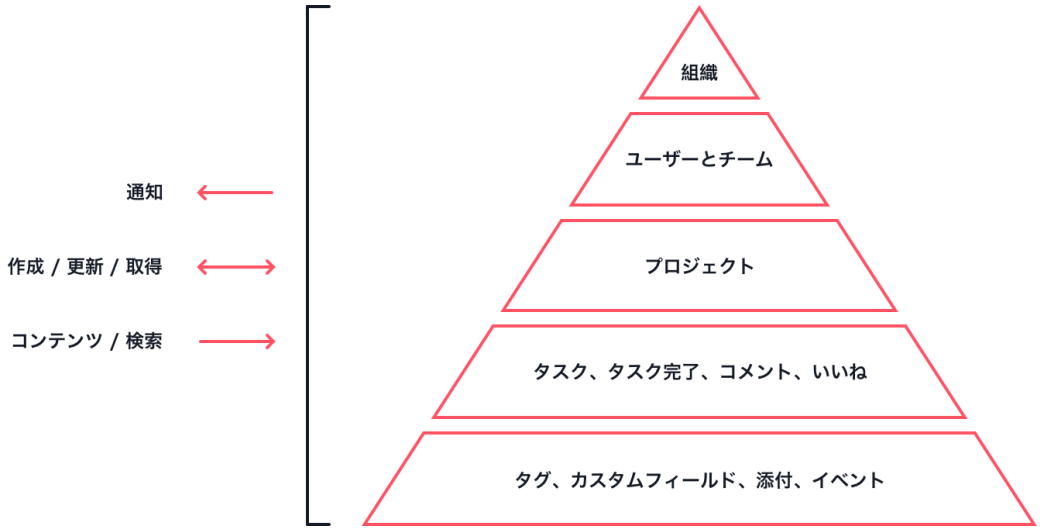
Asana プラットフォーム

連携

Asana ではユーザーがアプリケーションプログラミングインターフェイス (API) を使用して、アカウントにアクセスできます。Asana API は RESTful インターフェイスです。プラットフォーム上のデータの大部分についてプログラムでの更新、アクセスが可能なほか、変更が起きると自動的に反応することもできます。リソースにアクセスするための予測可能な URL が提供され、コマンドの受信と応答のために組み込みの HTTP 機能が使用されます。これにより、コマンドラインユーティリティ、ブラウザープラグイン、ネイティブアプリケーションなど、さまざまな環境から Asana と容易に通信できます。お客様はこれらの API を使用してカスタムソリューションの作成や、その他のソフトウェアとの連携が可能です。Asana は OAuth 2.0 または個人アクセストークンを API の認証方法としてサポートしています。

Asana API について詳しくは、 asana.com/developers をご覧ください。

下の図は実行可能なアクションと操作に関連するオブジェクトの概要を表しています。



デフォルトでは、すべてのソフトウェアやスクリプトの権限は、実行するユーザーの権限に従います。つまり、使用できるデータはユーザーがアクセス権を持つデータに限定されます。追加のアクセス権が必要な場合、Enterprise のお客様は「サービスアカウント」をご利用いただけます。詳細は下記をご覧ください。

サービスアカウント

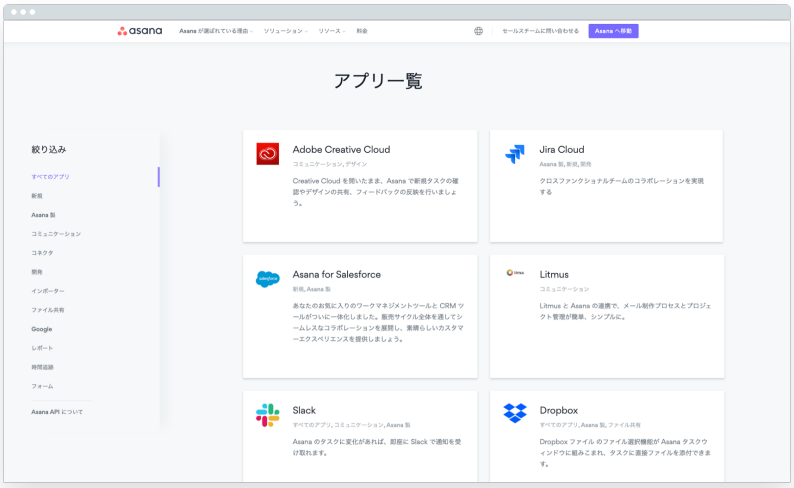
Asana Enterprise のお客様は、サービスアカウントを使用して、すべてのコンテンツにアクセスできます。たとえば、サービスアカウントにより、組織全体のデータのエクスポートやチームアクティビティの監視などが可能です。

サードパーティアプリケーション

Asana の API では何百ものソフトウェアと簡単に連携でき、お客様はそれを利用して Asana の使用体験を向上かつ補完できます。Asana は Google や Microsoft の多様なツールと連携して、お客様のワークフローを合理化し、生産性を高めます。その他のベンダーのサードパーティツールとも連携でき、以下のような機能を利用できます。

- アプリ間のメッセージの同期
- ワークフローの自動化
- プラットフォームの拡張
- ソフトウェア開発
- データインポート
- ファイル共有
- レポート
- 時間追跡
- データの受け付け

サードパーティアプリケーションの一覧は asana.com/apps でご確認いただけます。



運用上のセキュリティ

Asana の情報セキュリティ

Asana は正式な情報セキュリティマネジメントプログラムを運用しており、Asana の最高情報セキュリティ責任者 (CISO) の管轄下のセキュリティ専門スタッフが担当しています。この組織はセキュリティコントロールの実装と Asana における悪意ある行為の監視を行っています。

機密情報

Asana は、すべてのお客様のデータを分類に関わらず機密情報として扱います。本ポリシーにより、機密情報へのアクセスを、業務の一環としてそうした機密情報へのアクセスを必要とする従業員に制限し、かつ、お客様に特定のサービスを提供する上で当該情報へのアクセスを必要とする状況のみに限定します。そのような場合、従業員は担当の業務を実施する上で必要な、最小限の機密情報のみにアクセスするよう指示を受けます。

人事管理

Asana のすべての従業員と請負業者は、守秘義務契約と職務発明契約に署名し、雇用時と、その後は年 1 回、正式なセキュリティ意識向上トレーニングに参加することを義務付けられています。

すべての技術者はデータアクセスポリシー契約に署名し、Asana 採用前に身元調査を受けます。さらに、顧客データのすべてのエントリーポイントにセキュリティゲートウェイを設置し、すべてのデータアクセスはログに記録され無期限で保管されます。

Asana ではポリシーへの違反者に対する懲戒処分の指針を設けています。

ユーザーアクセスのレビューとポリシー

四半期ごとに、経営陣は管理対象システムへのユーザーアクセスのレビューを行い、アクセスが引き続き適切であることを確認し、必要のなくなったアクセス権を削除します。退職した社員のアクセス権も削除されます。

物理的セキュリティ

Asana の拠点

Asana のオフィスへの入退室のセキュリティ管理にはキーカードを使用し、アクセスがログに記録されます。すべてのオフィスには侵入警報システムが設置されています。訪問者は受付にて記録されます。すべての従業員には、不審な行為、施設への無断侵入、物品の盗難 / 紛失が起きた場合の報告義務があります。

データセンターセキュリティ

Asana は AWS による世界クラスの物理的および環境的セキュリティ管理を利用しています。[4]

ネットワークセキュリティ

当社では、オフィスのネットワークとネットワーク上のデバイスの可用性を常に監視しています。ファイアウォール、DNS サーバー、DHCP サーバー、ルーターなどのネットワークデバイスによって記録されたログを 1 か所で収集し、セキュリティ装置 (ファイアウォール)、ワイヤレスアクセスポイント、スイッチのネットワークログを保存しています。

IT セキュリティ

すべてのノートパソコンとワークステーションは、ディスク全体を暗号化し、一元管理されたイメージによりプロビジョニングしています。従業員のマシンには必ずアップデートを適用し、ワークステーションにマルウェアが侵入していないか念入りに監視しています。また、デバイスマネージャーを使用して重要なパッチを適用したり、マシンを遠隔消去したりすることもできます。当社は可能な限り二要素認証を使用し、企業インフラストラクチャに対するアクセスのセキュリティをいっそう強化しています。Asana は定期的にセキュリティスキャンを実行しています。

リスクと脆弱性の管理

Asana は、システム内の脆弱性を積極的に特定する継続的なリスク管理プロセスを実施し、会社の運営に対して新しく発生する脅威のアセスメントを実行しています。

Asana は本番環境における内部システムと外部システムの両方の脆弱性スキャンを実行しています。Asana のセキュリティチームは年 4 回以上スキャンを実行し、その評価に基づき脆弱性を修正しています。また、セキュリティ責任者が本番環境に大きな変化が起こったと判断した場合にも、脆弱性スキャンが実行されます。

侵入テスト

当社は外部のセキュリティ専門会社と提携して、コードに対する一般的なエクスプロイトをテストし、本番サーバーに対してネットワークスキャニングツールを使用しています。侵入テストは年 1 回実行されています。脆弱性が確認された場合は修正し、再テストします。

バグバウンティ

当社では、外部のバグバウンティプログラム[5] を利用し、脆弱性を発見したセキュリティリサーチャーに報酬を支払っています。

---

[4] http://aws.amazon.com/compliance/data-center/controls

[5] http://asana.com/bounty

ソフトウェア開発ライフサイクル

Asana は Git バージョン管理システムを使用しています。Asana のコードベースが変更されると、自動化された一連のテストとレビューが実施された後に、人の手によるレビューも行われます。自動化システムによるテストに合格すると、その変更はまずステージングサーバーにプッシュされ、そこで Asana の社員がテストを行ってから、最終的に本番環境のサーバーと Asana の顧客ベースへとプッシュされます。また、機密性が特に高い変更や機能に対しては、特別なセキュリティレビューも追加で行われます。さらに、Asana のエンジニアが特に重要な更新のみを選別 (チェリーピック) し、本番環境のサーバーに速やかにプッシュすることもできるようにしています。

アクセス制御を変更した場合は、それがパブリッシュされた場所をすべてリストに記録しています。また、アクセス制御のルールが正しく作成され、ルールに従って正しく機能していることをチェックする一連のユニットテストも自動で実施しています。

インシデントレスポンス

当社は、Asana により転送、保管、その他処理される機密データまたは個人データの、偶然または不法な破壊、損失、盗難、変更、無断の開示、またはアクセスに関連するセキュリティインシデントやセキュリティインシデントと疑われる事象に対して合理的で一貫性のある対応を確立するため、インシデントレスポンスプランを策定し、実施しています。このインシデントレスポンスプランには、セキュリティインシデントに対する Asana のセキュリティトリアージ、調査、修正、報告方法の詳細が決められています。Asana はデータ漏洩時に備え、サードパーティのデジタルフォレンジックサービスおよびインシデント対応企業と提携しています。

災害復旧と事業継続

Asana は予期せぬ不可避の災害の発生により長期的なサービス停止が起こった場合、妥当な期間内に可能な限り広範囲のサービスを復旧するための事業継続計画を用意しています。災害後、最重要の技術インフラストラクチャとシステムを復旧または持続させるための一連の災害復旧ポリシーと手順が文書化されています。

Asana の主要なデータセンターは、米国内に置かれるデータについてはバージニア州、ヨーロッパに置かれるデータについてはフランクフルト (ドイツ) の AWS でホストされ、同じ AWS リージョンに冗長性があります。1 つの AWS データセンターに障害が発生しても、復旧手順により別のデータセンターからノードが復元されます。大災害の発生を考慮して、災害復旧 (DR) サイトは、米国内のデータについてはオハイオ州、ヨーロッパ内のデータについてはダブリン (アイルランド) の AWS データセンターにホストされています。[6]

[6] RDS マルチ AZ 展開による複数のアベイラビリティゾーン

データ保持とデータ廃棄

データ保持

当社はお客様の情報を、当社のプライバシーポリシーで説明されている目的を果たすために必要な期間保持します。Enterprise のお客様のドメインデータはリクエストにより削除します。

データ廃棄

お客様の組織の正式な代表者から要求していただくことにより、お客様は顧客データのエクスポートまたはドメイン削除をリクエストできます。ただし、適用される法律に準拠するため、Asana は保持されたいかなる顧客データの機密性をも維持することに同意した上で、リクエストの日付を過ぎてから該当の顧客データを実際に処理する場合があります。

監視

Asana は、Amazon CloudWatch と、重要なデータをログから抽出し監視サービスにプッシュするカスタムスクリプトとを組み合わせて使用しています。Asana は社内とお客様向けの両方の物理的なインフラストラクチャとコンピューティングインフラストラクチャのキャパシティ使用率を監視し、提供されるサービスが同意されたサービス品質保証 (SLA) と一致しているかを確認しています。当社ではネットワークとアプリケーションのセキュリティスキャンを自動的に実行しています。監視スクリプトを週 1 回実行し、コードの変更が適切にレビューされていることを確認しています。

特定のアプリケーションとマシンログは無期限で保持され、一般的に S3 の長期ストレージに保管されます。より詳細なマシンログはログを生成するマシンのみに保管され、通常 2 週間保持されます。

サブプロセッサーとベンダー管理

Asana は合理的な手段を講じて、当社のポリシーに沿ったセキュリティ対策を実装しそれを維持するサードパーティサービスプロバイダーのみを選択し採用します。Asana でソフトウェアが実装される前、またはソフトウェアベンダーを使用する前に、Asana の IT チームはベンダーのセキュリティプロトコル、データ保持ポリシー、プライバシーポリシー、セキュリティ追跡記録を慎重に審査します。ソフトウェアまたはソフトウェアベンダーが、Asana のデータとエンドユーザーを十分に保護する能力を証明できない場合、当社の IT チームはそれらの使用を拒否する場合があります。ベンダーの再審査は年 1 回行われます。

当社の現在のサブプロセッサーは、「規約」ページで確認できます。[7]

[7] http://asana.com/terms#subprocessors

プライバシー、証明書、コンプライアンス

プライバシーポリシー

Asana のプライバシーポリシーは、「規約」ページで確認できます。[8] ここには以下の内容が記載されています。

- ユーザーの種類と該当するプライバシーポリシー
- 加入者向けのプライバシー規約
- 無料ユーザー向けのプライバシー規約
- サイト訪問者向けのプライバシー規約
- すべてのユーザー向けの追加プライバシー規約
- Asana 連絡先情報

証明書と法令順守

Asana は複数のプライバシーとセキュリティに関する標準の適格性審査を受け、以下の証明書を取得しています。

プライバシーシールドフレームワーク

Asana は、EU 加盟国とスイス内の個人情報の収集、使用、保管に関して、それぞれ EU-米国間とスイス-米国間のプライバシーシールドフレームワークの認定を受けています。[9]

サービスと組織の統制 (SOC 2)

Asana はセキュリティ、可用性、機密性に関連する内部統制に対して SOC 2 (タイプ II) の認定を受けています。SOC 2 (タイプ II) の認定の取得は、当社によるこれらの 3 つの原則に関する統制の業務プロセスと実施状況が独立したサードパーティ機関に認証されたことを意味します。

[8] http://asana.com/terms#privacy-policy

[9] https://www.privacyshield.gov/participant?id=a2zt0000000TNLRAA4&contact=true

GDPR

EU 一般データ保護規則（「GDPR」）は EU 諸国居住者の個人データの保護を定めるヨーロッパの法律で、2018年5月 25日に施行されました。GDPR の下で、EU 内居住者の個人データの収集、保持、使用、その他処理を行う組織は、(組織の所在地に関わらず) そのデータに対して決められたプライバシーとセキュリティ対策を講じる必要があります。Asana は包括的な GDPR コンプライアンスプログラムを確立し、お客様およびベンダーと協力して GDPR コンプライアンスに取り組んでいます。GDPR に準拠するために Asana が実践する重要な手順の一部を以下に示します。

- 当社のパートナー、ベンダー、ユーザーに関するポリシーと契約の改定
- セキュリティ対策と手順の充実
- 当社が収集、使用、共有するデータの綿密なレビューとマッピング
- より堅牢な社内のプライバシーとセキュリティ文書の作成
- GDPR 要件とプライバシー / セキュリティベストプラクティス全般に関する従業員の教育
- データ主体の権利のポリシーと応答プロセスの慎重な評価と構築
- 以下に、Asana の GDPR コンプライアンスプログラムの重要なポイントについて詳述します。また、お客様が自社の GDPR コンプライアンスイニシアチブに Asana を活用する方法を説明します。

DPA

EU 一般データ保護規則 (GDPR) に従い、「データ管理者」(データ処理の目的と手段を判断する組織) は、「データプロセッサー」(データを代わりに処理するその他の組織) と契約を締結する必要があります。EU の個人データを管理するお客様は、Asana が GDPR の要件に従って個人データを処理、保護する堅牢なデータ処理契約を Asana と締結できます。この契約には、データ管理者の指示に従って個人データを処理する Asana の義務が含まれます。データ処理補遺条項は「規約」ページに掲載されています。[10]

法の執行

Asana は「規約」ページに定める「法執行機関向けデータリクエストガイドライン」に従います。[11]

[10] http://asana.com/terms#data-processing

[11] http://asana.com/terms#law-enforcement-guidelines

おわりに

当社では、チームの連携を促し、仕事を整理して成果を出すことに集中するために Asana を毎日活用しています。Asana のプラットフォームのセキュリティを維持することは、お客様の情報はもちろん、私たち自身のデータを保護するためにも不可欠であり、データ保護は私たちの最優先事項です。

私たちはデータセキュリティを常に念頭に置きながら、Asana の使用性をさらに向上させることで、協働ワークマネジメント分野のトップ企業となることを目指し、努力しています。Asana の有料プランについての詳細は、当社のセールスチーム（sales@asana.com）までメールでお問い合わせください。

セキュリティに関する疑問などは、security@asana.com までメールでお問い合わせください。