monday.com
セキュリティおよびプライバシーに関するホワイトペーパー

日付	バージョン	変更内容
2021年11月	1.0	最終版

本ホワイトペーパーは、公開日時点におけるmonday.comのセキュリティおよびプライバシーに対する取り組みについて概要を説明するものであり、その内容は予告なく変更される場合があります。将来的な計画についての説明は、monday.comの独自の判断により、変更または延期される場合があります。本ホワイトペーパーは情報提供のみを目的としており、法的助言を構成するものではなく、またいずれかの契約書の条件を補足したり、そこに組み込まれたりするものと理解されるべきものではありません。

目次

1. はじめに

monday.comワークOSは、世界中の12万7000社以上の企業のデータを管理しており、このような責任を負う立場から、お客様に最高水準のセキュリティとデータ保護を提供できるよう全力で取り組んでいます。当社は、データセキュリティを最優先事項とすることで、お客様の信頼を獲得します。

当社のミッションステートメント
当社がmonday.comワークOS上でデータを管理するお客様に安心感を提供する。

社内体制
monday.comの情報セキュリティに関する取り組みは、CISO、セキュリティ部門、そしてインフラ・R&D・運用・ITの各部門の代表者で構成されるセキュリティフォーラムによって指導・監視されています。
monday.comのプライバシーに関する取り組みは、法務・プライバシー・セキュリティの各部門の代表者で構成されるプライバシーフォーラムによって指導・監視されています。

関連リンク
monday.comトラストセンター
monday.comリーガルポータル
monday.comのステータスページ
復処理者、子会社、サポート
monday.comにおけるセキュリティとプライバシー - よくある質問
脆弱性の報告
サポートとナレッジベース
料金とプラン
monday.Engineeringブログ

---

2. インフラのセキュリティ

ホスティング業者

当社のサービスは、高い可用性とレジリエンスを実現するため、Amazon Web Services（AWS）のインフラを利用し、バージニア州北部（米国）およびフランクフルト（ドイツ）をメインに複数のリージョンにホストされています。[1]アベイラビリティゾーンも複数のゾーンに分散され、さまざまなリージョンに専用の災害復旧（DR）用のデプロイメントを構築しています。お客様のアカウントは、単一のリージョンに紐づけられます。

AWSの責任共有モデルの下、AWSはクラウドコンピューティングインフラのセキュリティを管理し、monday.comはクラウドコンピューティングインフラ上にあるソフトウェアとデータのセキュリティを管理します。

当社のアクティビティログ機能（詳細は後述）では、米国にあるGoogle Cloud Platform（GCP）にデータがバックアップされます。

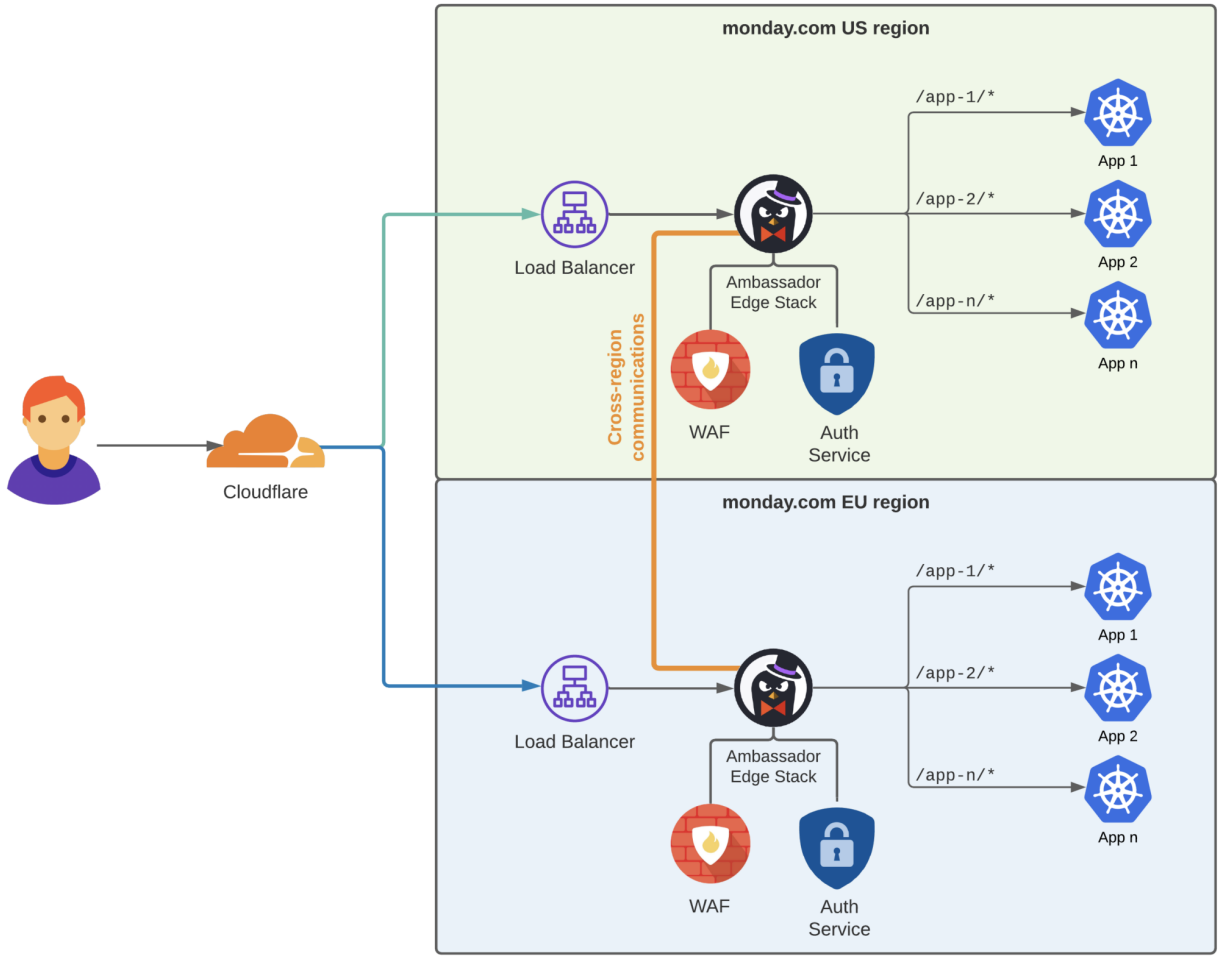
ネットワークアーキテクチャ

- monday.comのネットワークアーキテクチャは、パブリックサブネットとプライベートサブネットの分離を含め、AWSのベストプラクティスに従って構築されています。
- monday.comでは、DDoS攻撃や総当たり攻撃を防ぐため、CloudflareやFastlyをはじめとする複数のCDNプロバイダーを利用しています。レート制限は、エッジおよびアプリケーションレベルの両方で設定されています。
- ロードバランサーはパブリックサブネット上に設置されていますが、Webアプリケーションサーバーやデータベースなどの内部ネットワークコンポーネントはプライベートサブネット上に設置され、パブリックIPアドレスは割り当てられていません。
- コンテンツベースで動的に攻撃をブロックするため、Webアプリケーションファイアウォール（WAF）が設置されています。
- 特定のIPアドレスのみを許可（ホワイトリスト登録）し、許可されたポートのみを通じてネットワークリソースにアクセスできるようにするため、ネットワーク全体でファイアウォールが使用されています。セキュリティグループのルールは、必要なポートからのアクセスのみを許可するよう設定されています。
- 全ての本番環境資産に対して有効となるネイティブのAWSセキュリティサービスと並行して、ネットワーク侵入検知システム（NIDS）センサーを利用しています。

次の図は、米国データリージョンとEUデータリージョンにおけるmonday.comのネットワーク構成図です。[2]

[1]エンタープライズプランのお客様は、自社データのホスト先として、ドイツのフランクフルトにあるEUデータセンターを選択することができます。

[2] グリッドネットワークの概要図は、ご要望があれば、MNDA（相互秘密保持契約）に署名することを条件に提供されます。



構成の変更を確実に追跡・監査できるよう、Infrastructure-as-Codeを幅広く利用しています。monday.comのインフラ部門は、四半期ごとに非武装（境界）ネットワークの構成を見直し、セキュリティの維持・向上に必要と思われる変更を実施します。

AWSアドバンストテクノロジーパートナー

monday.comは、AWSアドバンストテクノロジーパートナーでもあります。これは、当社組織がインフラ、情報セキュリティ、ベストプラクティスに基づく設計等に関して、AWS自体による厳格な審査を受けたことを証明するものです。

ネットワークのセキュリティ

純粋なクラウドベースのソリューションであるmonday.comには、ネットワーク境界部を正確に把握するために、最新のクラウド指向の管理手法を利用できるという優位性があります。当

社は、NIDSおよびエッジロケーションからのトラフィックログを利用してネットワークログの収集・監視を行うほか、セキュリティ情報・イベント管理（SIEM）システムを通じて関連アラームの確認を行っています。また、セキュリティ監視ツールも利用し、クラウドプロバイダーから頻繁にセキュリティグループおよびネットワークACL（アクセスコントロールリスト）の構成を取得し、当社ネットワークの全体像を把握しています。

monday.comのインフラ部門は、四半期ごとに非武装（境界）ネットワークの構成を見直し、セキュリティの維持・向上に必要と思われる変更を実施します。さらに年1回、外部の監査人に依頼し、ネットワーク構成の見直しを行っています。

本番環境へのアクセス

本番環境資産へのアクセス権は、ロールに基づき、知る必要（need-to-know）および最小権限（least privileges）の原則に従い付与されます。管理権限は、当社インフラ部門の人員（少数の熟達したエンジニアに限定）にのみ付与されます。monday.comのサーバーへのアクセスには、必ず当社のVPNを利用する必要があります。VPNは、当社のエンタープライズ・アイデンティティプロバイダー（IdP）を使って認証が行われ、完全な監査が実施され、強力なパスワードと多段階認証（MFA）が求められます。
当社エンジニアによる本番環境資産へのアクセスは、Kubernetesのポートフォワードを使って行われ、同様に当社のIdPを使って認証が行われます。

ハードニング

サーバーでは最新のUbuntu LTS版（20.04）が使用され、CIS（Center for Internet Security）の規格に沿ってハードニング（堅牢化）が行われています。

データベース

monday.comでは、MySQL、Elasticsearch、Redisなどのデータベースが使用されています。当社の連携機能で使用される外部システムへのAPIキーは、セルフレプリケーション機能をもつ専用のHashiCorp Vaultクラスタに保管されます。

ファイルストレージ

ファイルストレージは、AWSのStorage Service（S3）上にホストされ、ここに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。添付ファイルには、お客様がmonday.comサービスにアップロードした全てのファイルが含まれます。
monday.comは、ユーザーがサービスにアップロードするファイルを対象にマルウェア自動検出サービスを提供しており、感染したファイルが外部からサービスにアップロードされないよう万全を期しています。また、アップロードが禁止されているファイルの拡張子をリスト化したブラックリストも用意されています。ファイル拡張子のブラックリストには、実行可能ファイルやHTMLなど、危険と考えられる可能性のあるファイルの種類が登録されています。当社では、これらのファイルの種類をブロックすることで、マルウェアへの感染リスクを大幅に軽減しています。

マルチリージョン

2021年1月、monday.comはデータリージョンを拡大し、ドイツのフランクフルトを欧州初のデータリージョンとして採用しました（現在はエンタープライズプランの顧客のみ利用可能）。

米国リージョンと同一のインフラ原則が採用されているため、同等レベルのセキュリティ対策と制御が実施され、EU内のお客様はCIAトライアド（機密性、完全性、可用性）の原則が順守されるという安心感をもってmonday.comを利用することができます。
monday.comネットワーク構成図の要点は、上図に示したとおりです。
将来的には、他のリージョンにもデータセンターを開設する予定です。

暗号化と鍵管理

転送中の暗号化

オープンネットワーク上で転送されるデータは、TLS 1.3（最低でもTLS 1.2）を使って暗号化されます。

保管中の暗号化

保管中のデータは、AES-256を使って暗号化されます。暗号鍵の保管には、AWS Key Management Service（KMS）を利用しています。現在、monday.comサービスに送信され、当社がお客様に代わって処理する顧客データの暗号化には全て、カスタマーマスターキー（CMK）が使用されています。CMKは、毎年ローテーションが行われます。

テナントの分離

当社の環境はマルチテナント方式で、顧客同士が論理的に分離されています。顧客データは、複数のパラメータを組み合わせて生成される一意のIDを使って、アプリケーションレベルで分離されています。

当社は現在、お客様向けに、テナントレベルの暗号化（TLE）を可能にするための作業を進めています。TLEは、保管中のデータをアカウント単位の専用鍵で暗号化するためのレイヤーで、権限のないシステムやユーザーがデータを見られないように保護機能を提供します。

TLEは、主に2つのシナリオに対して保護機能を提供します。

1. **攻撃者：**データベースのフィールド内のデータが暗号化されるため、攻撃者がデータベースにアクセスしてデータを抽出しても、暗号化されたデータしか取得できなくなります。
2. **偶発的な共有：**データがアカウント単位の専用鍵で暗号化されるため、誤ってデータがアカウント間で共有された場合も、平文として共有されることがなくなります。

近い将来、エンタープライズプランのお客様には、独自の暗号鍵を持ち込む（BYOK: Bring Your Own Key）機能を提供する予定です。

バックアップ

monday.comは、monday.comサービスに送信され、当社がお客様に代わって処理する顧客データのバックアップを行います。当社は、常に5分ごとにユーザーデータをバックアップし、暗号化されたバックアップをAWSの複数のアベイラビリティゾーンに分散させます。また、冗長性を確保するため、AWSのそれぞれ異なるリージョンに複数のDRサイトを構築しています。アクティビティログのデータは、GCPにバックアップされます。

スケーラビリティと信頼性

1つまたは複数のコンポーネントに不具合が発生した場合に、システムの正常性に与える影響を最小化するため、マイクロサービスアーキテクチャを採用しています。monday.comのサー

ビスは完全にコンテナ化されており、オーケストレーションにKubernetesを使用しています。これにより、インフラのスケーラビリティが高まり、エンドユーザーに質の高い体験を提供しつつ、増大する顧客の需要に対応できる適切な構成になっています。

インフラリソースの可監査性と保守性を確保するため、Terraformを使ったInfrastructure-as-codeを広く利用しています。

monday.comでは、全てのインフラコンポーネントのパフォーマンス指標を継続的にモニタリングし、スケーラビリティに優れたインフラを構築しています。また、四半期ごとにインフラエンジニアとインフラ管理チームによるスケーラビリティレビューを実施し、顧客数と製品機能数が増大する中で質の高いサービスを提供するためのロードマップを整備しています。

サービス品質保証（SLA）

当社サービスの可用性は、ステータスページを通じて監視することができます。メンテナンスのためにシステムのダウンタイムが必要になることは稀であり、システムの停止が必要かつ実行可能な場合は、週末の利用の少ない時間帯にスケジュールが設定されます。

ダウンタイムに関する通知は、ステータスページを通じてすぐに確認できます。可用性や当社チームによる問題対応に関する通知をメールまたはテキストメッセージで受信したい場合は、ステータスページで設定できます。

エンタープライズプランのお客様には、99.9%のアップタイム保証が提供されます。

3. セキュリティ関連の特徴と機能

認証

monday.comは、次の認証手段に対応しています。

資格情報

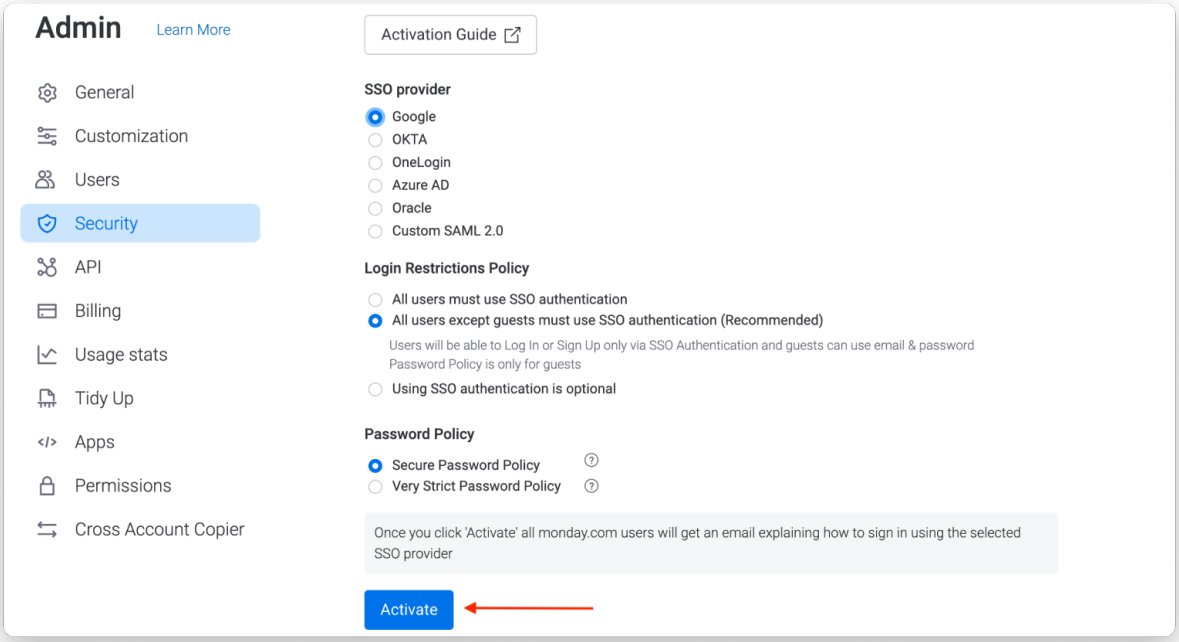
資格情報を使ってアカウント認証を行う場合は、アカウントパスワードの強度設定に関して2つの選択肢が管理者に提示されます。

1. 8文字以上で、同じ文字の反復または連続使用は禁止。
2. 8文字以上で、同じ文字の反復または連続使用は禁止。また、数字（1，2，3）、小文字（a, b, c）、大文字（A, B, C）がそれぞれ1つ以上含まれること。

Googleシングルサインオン（SSO）

Google SSOはセキュアな認証システムで、ユーザーはGoogleアカウントを使ってmonday.comのサービスにログインすることができ、複数のパスワードを覚えるという負担が軽減されます。

この機能は、プロプランおよびエンタープライズプランでのみ利用できます。



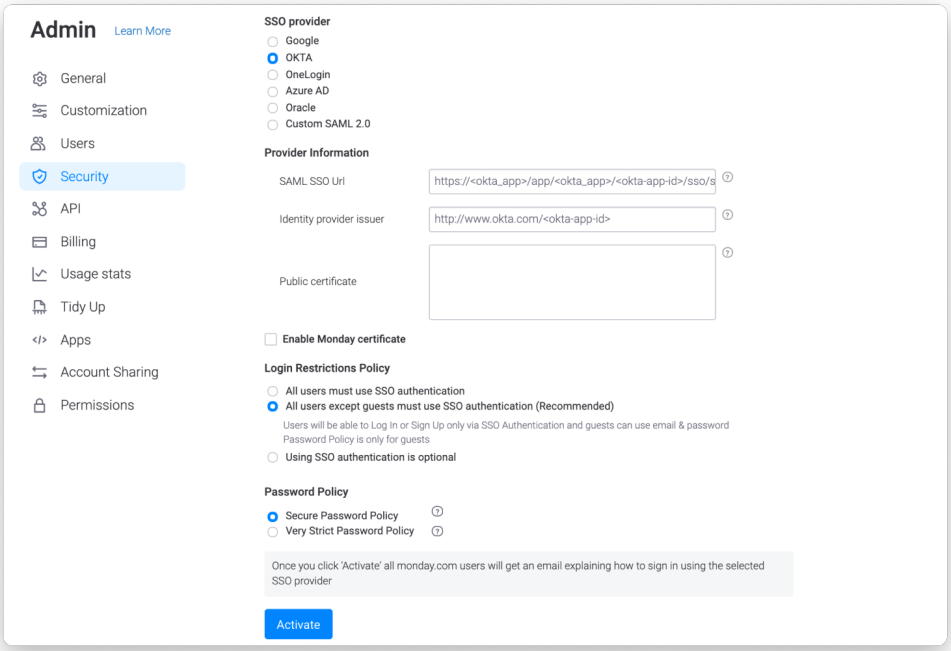
アイデンティティプロバイダー（IdP）

monday.comは現在、3つの主要なアイデンティティプロバイダーに対応しています。

1. OKTA
2. Azure AD
3. OneLogin

さらに、お客様はカスタムSAML　2.0を使って、独自のプロバイダーを利用することもできます。

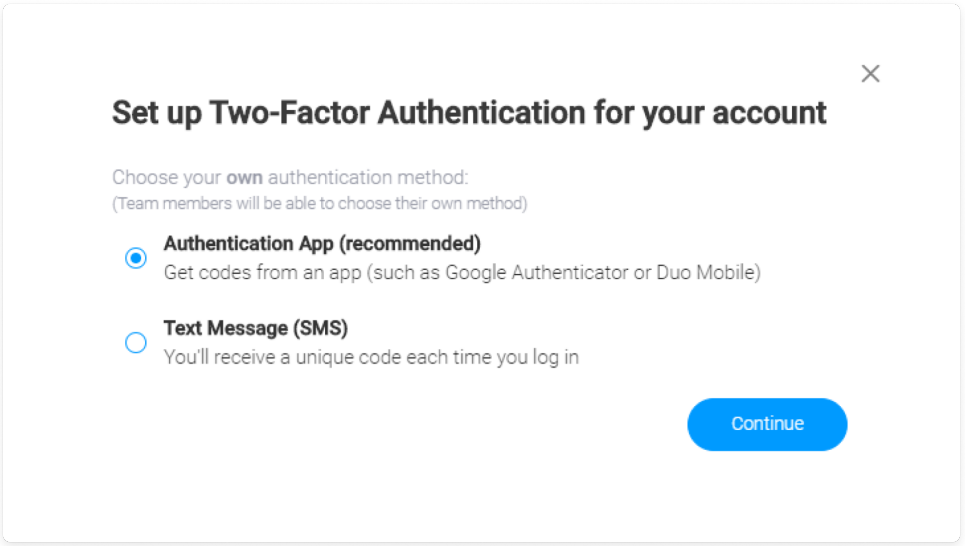
この機能は、エンタープライズプランのお客様のみ利用できます。



2段階認証（2FA）

上記の認証手段に加え、管理者は追加のセキュリティレイヤーを構成し、テキストメッセージ（SMS）または認証アプリを使った2FAを有効にすることができます。

ご利用のIdPを連携させる場合は、お客様側で2FAを有効にする必要があるのでご注意ください。



権限付与

SCIMによるプロビジョニング

クロスドメインID管理システム（SCIM）は、複数のアプリケーション間でユーザー管理を行うためのプロトコルで、複数のアプリケーションを対象に同時にかつ簡単にユーザーデータとチームデータのプロビジョニング（追加）、デプロビジョニング（無効化）、更新を行うことができます。monday.comでは、SCIMによるプロビジョニングを3つの方法でセットアップできます。

1. monday.comの既存のSCIMアプリケーション
    a. OKTA
    b. Azure AD
    c. OneLogin
2. 顧客が指定するアイデンティティプロバイダーとのカスタムSCIM連携
3. APIを使ったSCIMによるプロビジョニング

次の表は、monday.comのSCIM連携でサポートされている**ユーザー**属性の一覧です。

monday.comの属性	SCIM APIの属性	説明
Name（必須）	name, displayName	ユーザーの表示名
Email Address（必須）	userName, email	ユーザーがmonday.comサービスへのログインに使用するメールアドレス
Active（必須）	active	ユーザーを作成する際は、このフィールドを「true」に設定する必要があります。ユーザーの「active」値を「false」に変更すると、monday.comのサービスでユーザーが無効になります。
Position	title	ユーザーの組織内での職位
Timezone	timezone	ユーザーのタイムゾーン（プラットフォーム内の全ての日付がこのタイムゾーンで設定されます）
Locale	locale	monday.comでは、各ロケールに対応したローカライズ版が表示されます。
Phone Number	phoneNumbers	ユーザーの電話番号（「primary」に指定した番号のみが表示されます）
Home Address	addresses	ユーザーの住所（「primary」に指定した番号のみが表示されます）
User Type	userType	アカウント内の各ユーザーのレベル。設定できる値：admin、member、viewer、guest（既定値は「member」）。

次の表は、monday.comのSCIM連携でサポートされている**チーム**属性の一覧です。

monday.comの属性	SCIM APIの属性	説明
Name（必須）	displayName	チームの表示名
Users	members	チームに割り当てられたユーザーのリスト

この機能は、エンタープライズプランのお客様のみ利用できます。

アクセス権

monday.comでは、アカウント上で誰がどのような操作を行えるかを管理できます。データの閲覧や編集を制限できるよう、カスタマイズ可能なさまざまなタイプのアクセス権が用意されています。具体的には以下のとおりです。

1. **ボードのアクセス権**
    a. ボードの種類：「メイン」「共有」「プライベート」
    b. 制限：「すべて編集」「コンテンツの編集」「担当者による編集」「閲覧のみ」
2. **カラムのアクセス権**：「カラムの編集を制限」「カラムの閲覧を制限」
3. **ダッシュボードのアクセス権**
    a. ダッシュボードの種類：「メイン」「プライベート」
    b. 制限：ダッシュボードの所有者のみが、ダッシュボードやダッシュボード内のアプリやウィジェットを編集できます。
4. **ワークスペースのアクセス権**
    a. ワークスペースの種類：「公開」「非公開」
    b. 制限：「立入禁止」「管理者のみ」「ワークスペースの所有者」「全員」
5. **アカウントのアクセス権：**管理者は、次の機能に関して制限（「立入禁止」「管理者のみ」「全員」）を設けることができます。
    a. ファイルのアップロード
    b. ボードのブロードキャスト
    c. メインボードの作成
    d. プライベートボードの作成
    e. 共有ボードの作成
    f. 連携の作成
    g. 自動化の作成
    h. ワークスペースの作成
    i. アカウントの全ユーザーをアップデートまたはボードに@メンションまたは登録
    j. ボード、アクティビティログ、検索結果、アップデートをExcelにエクスポート

プランによっては上記機能の一部が利用できない可能性があるのでご注意ください。

monday.com内のロール

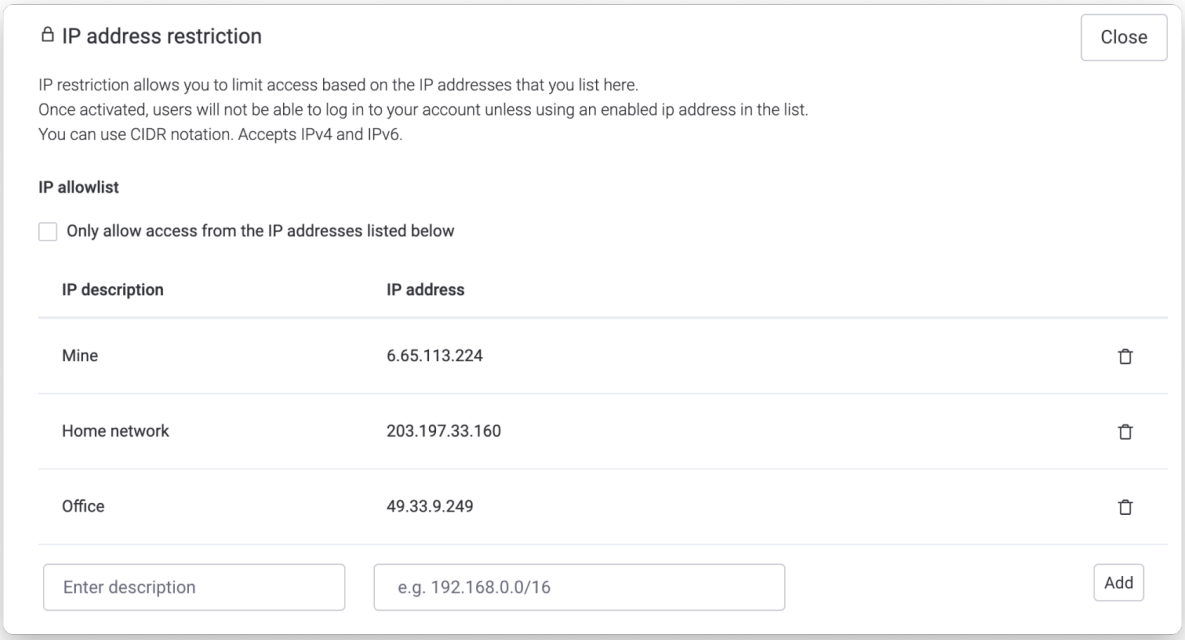
monday.com内のロール

ロール	説明	できること	できないこと
管理者	自分のチームの管理をするチームメンバー（複数選択可）	• アカウント全体の統括 • ユーザー、ボード、セキュリティ、請求など全てを管理（下記の「管理者パネル」の項で説明）	
メンバー	編集権をもつ （招待できるメンバー数はプランによって異なります）	• ボード、アイテム、フォルダーの作成・編集 • ボードやアイテム内で他のメンバーを招待 • 全てのメインボードの閲覧	

		• 共有ボードやプライベートボードへの招待を受ける • 自身のプロフィールの編集 • コミュニケーションと添付ファイルの追加	
閲覧者	ボードの閲覧のみ可能で、編集権は一切なし （購入したプランの種類にかかわらず、招待できる閲覧者数に制限はありません）	• アカウントのメインワークスペースの全てのボードの閲覧 • アイテムの表示、アップデートの確認 • ボード内の検索・絞り込み • 共有ボードやプライベートボードへの招待を受ける • 自身のプロフィールの編集 • 新規閲覧者の招待 • ボードビューの表示 • アイテムへの割り当てを受ける • チームに追加してもらう • ボードをExcelにエクスポート	• 新規ボードの作成・削除 • ボードの内容、構造、設定の変更 • アイテムへのアップデートの追加、他のユーザーが投稿したアップデートへのいいね • アイテムやボードに自分自身や他のユーザーを登録 • ボードの所有者に指定される • ゲストを共有ボードに招待 • チームの作成
ゲスト	ベンダー、クライアント、フリーランサー、外部コンサルタントなど組織外のユーザー	• 共有ボードへの招待を受ける • メンバーとしての機能	• メインボードやプライベートボードの情報の閲覧

IPアドレスの制限

管理者は、アカウントにアクセスできる許可IPアドレス群を予め設定することができます。これにより、アカウントへのアクセスを、特定の場所（オフィス）から参加している、あるいは特定のVPNを使用しているなど、一定の条件を満たすユーザーに限定することができます。ユーザーが許可リストに登録されていないIPアドレスからログインを試みた場合、エラーメッセージが表示され、それ以上先に進むことはできません。
この機能は、エンタープライズプランのお客様のみ利用できます。

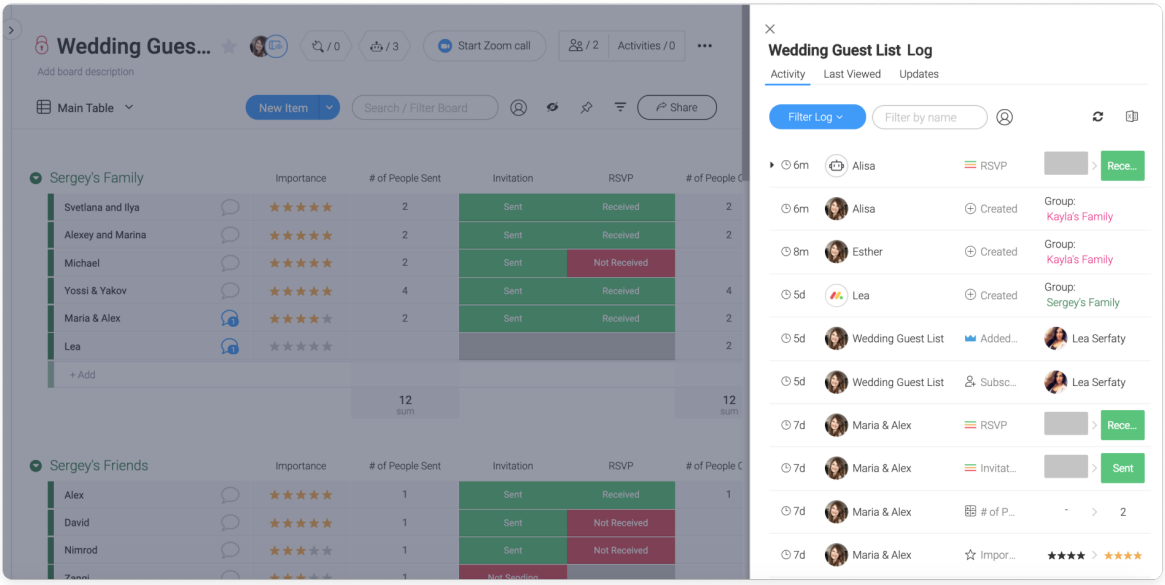


ログ

アクティビティログ

アクティビティログには2種類あります。

1. **ボードアクティビティログ**には、日付、ステータス、グループ間の移動、自動化、権限の変更など、ボードの過去のアクティビティが全て一覧で表示されます。ボードアクティビティログに表示される情報は、顧客の階層（ティア）によって変わります。ベーシックプランの場合は過去1週間分のアクティビティのみ、スタンダードプランの場合は6か月分のアクティビティデータ、プロおよびエンタープライズプランの場合は最大1年分のデータが記録されています。

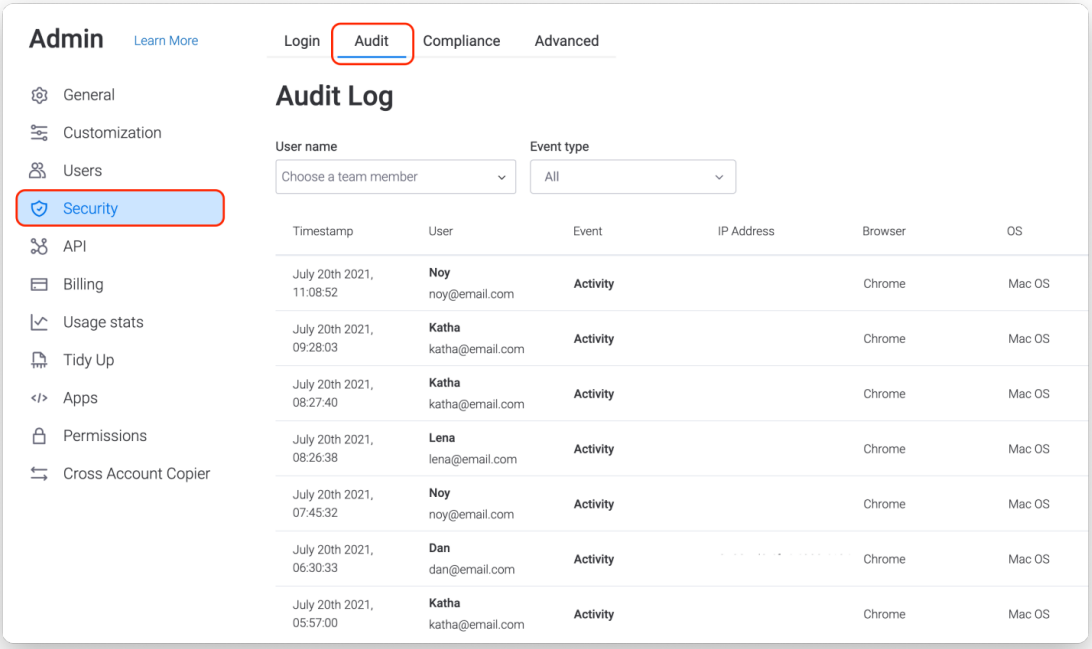


2. **アイテムアクティビティログ**には、個別のアイテムに対する全てのアップデートが記録されます。アイテムアクティビティログでは、当該アイテムのアップデートの完全な履歴とその正確な日時を確認できます。アップデートは全て新しい順に表示されます。任意のアップデートに関して、アラートリマインダーを設定することができます。

アイテムアクティビティログおよびボードアクティビティログは、ボタンをクリックするだけで簡単にExcelにエクスポートできます。

監査ログ

監査ログは、アカウントのセキュリティに関する全てのアクティビティについて詳細なレポートをアカウント管理者に提供します。このセクションでは、ユーザーが最後にアカウントにログインし、ログアウトした日時、ログインに使用したデバイス、当該セッションで使用されたIPアドレスを確認できます。これにより、アカウント管理者は疑わしいアクティビティを全て監視し、必要に応じてパニックモードを有効にすることができます。
また、監査ログには、ログインの失敗、添付ファイルのダウンロード、ボードデータのエクスポートなど、潜在的な脆弱性イベントも表示されます。この機能は、エンタープライズプランのお客様のみ利用できます。



相互運用性とポータビリティ

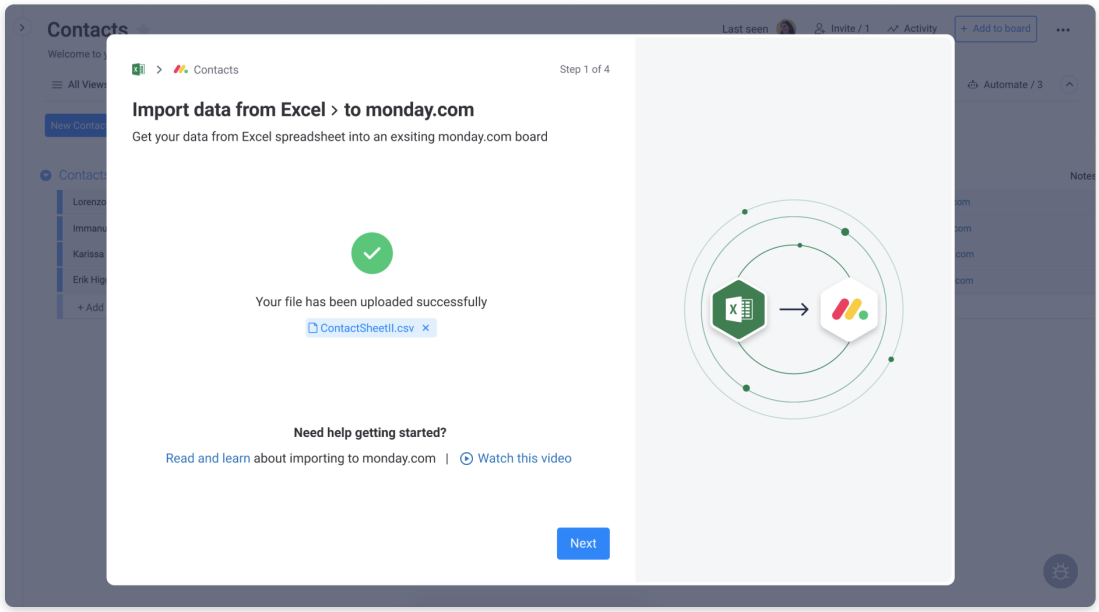
連携

monday.comは、カスタマイズされたワークフローを作成するため、他のさまざまなソフトウェアソリューションとの連携をサポートしています。既に利用しているツールにmonday.comを接続して、チームの作業を一元管理することができます。
連携機能はオプションで、管理者パネルから無効にできます。

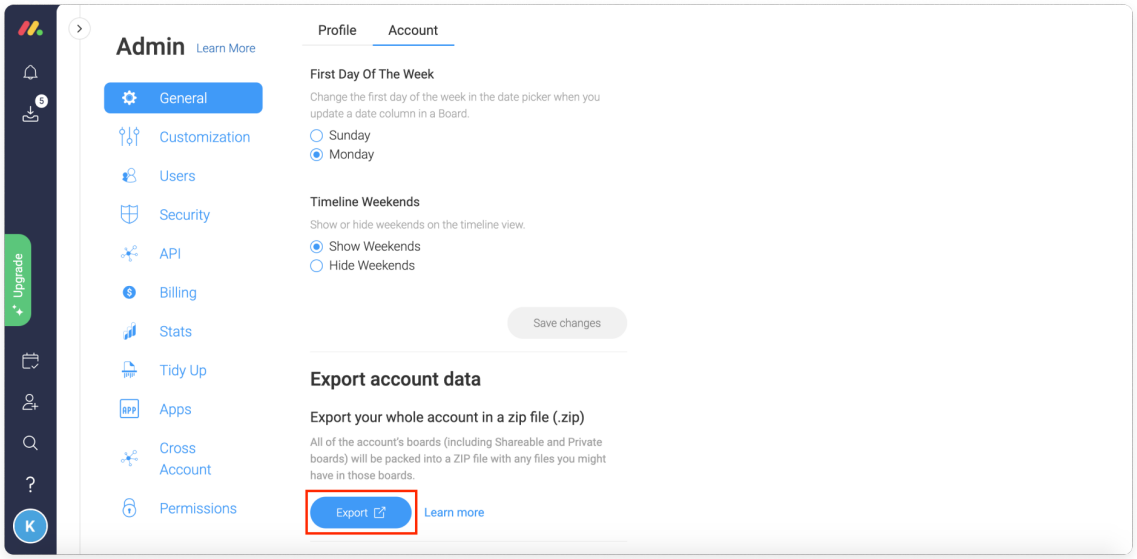
Excelのインポートと エクスポート

monday.comは、顧客に2種類のデータ管理機能を提供します。

1. Excelスプレッドシートのデータを（新規または既存の）monday.comのボードに変換



2. monday.comからデータのエクスポート
    a. ボードをExcelにエクスポート
    b. 管理者パネルを通じて、アカウント全体のデータをエクスポート。zipファイルとしてエクスポートされ、これにはExcelのシートとアカウントにアップロードされたファイルが含まれます。

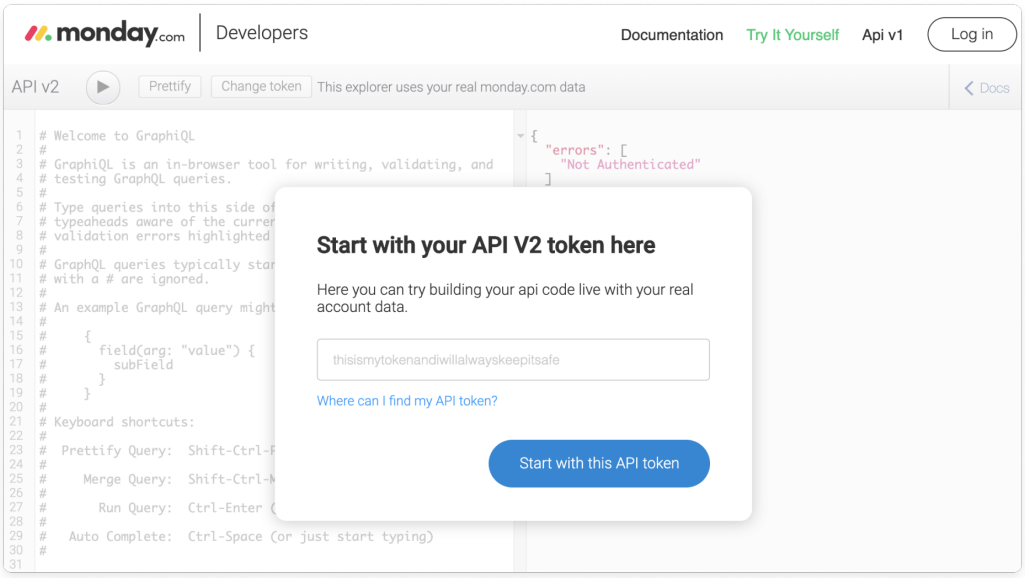


API

monday.comでは、GraphQL　APIを提供しています。これはmondayアプリフレームワークの一部で、開発者は、monday.comアカウント内のデータにアクセスしたり、更新したりするプログラムを組むことができます。

以下は、APIのユースケースの一例です。

- ボードデータにアクセスして、monday.comダッシュボード内にカスタムレポートを生成する。
- 別のシステム上にレコードが作成された際に、ボード上に新規アイテムを作成する。
- プログラミングにより、別のソースからデータをインポートする



管理者パネル

管理者は、管理者パネル上で、セキュリティ設定、アカウントのユーザー、アカウントのカスタマイズ、請求など、あらゆる管理作業を行うことができます。

承認済みドメイン

管理者は次の2つの設定から選ぶことができます。

1. 管理者のみが、任意のメールドメインからメンバーおよび閲覧者をアカウントに招待できる。
2. 管理者が、ユーザーがアカウントの登録に使用できるメールドメインを1つ決定する。

メールドメインのブロック

管理者は、ユーザーが特定のメールドメインからmonday.comの新規アカウントを作成できないようにすることができます。この機能は、同一組織内で余分なmonday.comアカウントが作成されるのを防ぐのに便利です。複数の法人ドメインを持つ組織の場合は、会社のデータガバナンスに関するルールを順守する上で問題になる可能性があるため、特に有用です。

新規アカウントの作成をブロックするには、メールドメインをmonday.comサービスに提出して審査を受け、所有権の認定を受けます。ブロック対象ドメインに該当する場合は、主たる組織のアカウントへのオンボーディングのためアカウントの管理者に転送されます。
この機能は、エンタープライズプランのお客様のみ利用できます。

パニックモード
パニックモードを有効にすると、アカウントを一時的にブロックすることができます。アカウントの管理者が当社のカスタマーサクセスチームにリクエストを送信するまで、誰もアカウントにアクセスできない状態になります。チームメンバーの資格情報が漏洩した場合は、この機能が極めて重要になります。
この機能は、エンタープライズプランのお客様のみ利用できます。

セッション管理
管理者は、管理者パネルのセキュリティセクションでセッションタブをクリックすることで、全てのユーザーのセッションデータの確認や、セッションの制御およびリセットを行うことができます。
この機能は、エンタープライズプランのお客様のみ利用できます。

APIトークンの生成
アカウントでパーソナルGraphQL　APIトークンを生成する権限を付与できるのは、管理者のみです（対象は全員、管理者のみ、または対象者なし）。これにより、ユーザーがAPIトークンを生成し、誤ってサードパーティツールと共有したり、パブリックリポジトリに送信してトークンを公開し、アカウントの機微なデータを外部に漏洩させるのを防ぐことができます。トークンを生成できないユーザーには警告が表示されます。
この機能は、エンタープライズプランのお客様のみ利用できます。

コンテンツディレクトリ
コンテンツディレクトリでは、アカウント内にある全てのワークスペース、ボード、ダッシュボード、ワークドックの概要を確認することができます。また、これらの各機能について、その所有者、登録者、作成日、最終更新日、アカウントの残りのメンバーに対する公開・非公開の別を確認することもできます。

*　本ホワイトペーパーは、管理者パネルから管理できる全ての機能を網羅しているわけではないのでご注意ください。その他の情報については、当社のサポート記事をご覧ください。
アカウントの管理者が管理するその他の機能については、ログイン、2段階認証、SCIMによるプロビジョニング、アクセス権、IPアドレスの制限、mondayアプリ、監査ログ、APIトークン、HIPAA準拠の構成など、本文書のさまざまな章で論じられている可能性があります。

---

4. アプリケーションのセキュリティ

セキュアソフトウェア開発ライフサイクル（S-SDLC）

- monday.comでは、セキュアソフトウェア開発ライフサイクル（S-SDLC）におけるセキュリティを実現するため、OWASP Top 10の方法論を採用しています。
- コードは全て、本番環境へのデプロイ前にコードの品質を確保するため、CI/CD（継続的インテグレーション/継続的デリバリー）プロセスの一環として静的解析（SAST）とピアレビューが行われます。
- 動的アプリケーションセキュリティテスト（DAST）は、少なくとも週1回実施されます。
- 当社では、リリースする新機能について専用のテストを書くことを特に重視する一方、旧来の機能については数年にわたり実際の現場で信頼性が証明されています。
- アプリケーションの脆弱性については、デプロイ中およびデプロイ後に継続的な評価と監視を行っています。
- サーバーサイドのサードパーティライブラリは全て、ソフトウェア構成分析（SCA）ツールを用いて、公開済みの脆弱性に関するチェックが自動的に行われます。

Webアプリケーションファイアウォール（WAF）

未知の攻撃に対する防御のため、アプリケーションレベルのトラフィックのフィルタリング、監視、ブロックを行うWebアプリケーションファイアウォール（WAF）が設置されています。

脆弱性管理

脆弱性は開発バックログで集中管理され、サービスおよび顧客データの機密性、完全性、可用性に対する影響度の評価結果に基づき分類されます。脆弱性の深刻度の点数は、共通脆弱性評価システム（CVSS）により判断されます。その後、深刻度に応じて予め定められた期間内に、当社のR&D部門がパッチ管理ポリシーに従い修復を実行します。

セキュリティチャンピオン

社内のセキュリティチャンピオンコミュニティは、全てのR&Dチームから集まった開発者で構成されています。セキュリティチャンピオンはセキュリティに関する高度なトレーニングを受け、セキュリティに関するガイダンスを提供し、必要に応じてセキュリティコードレビューを実施する資格を有します。

ペネトレーションテスト

独立した第三者により、年1回、手動および自動のテスト手法を用いたアプリケーションのペネトレーションテストが実施されます。実施業者は毎年変わります。
これに加え、社内のアプリケーションセキュリティチームが、社内のセキュリティメカニズムとアーキテクチャに関する深い理解が求められる各種機能について、定期的にセキュリティ監査とペネトレーションテストを実施します。
外部および内部のペネトレーションテストの一環として、当社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が使用されます。

脆弱性報奨金制度

monday.comでは、HackerOne上で内部管理型の脆弱性報奨金制度を運用しており、世界中のセキュリティ研究者が倫理的に責任感を持ってセキュリティに関する脆弱性を調査し、当社セキュリティチームに開示できる体制を整えています。一部の機能については、セキュリティコミュニティによる調査と取り組みをその領域に集中させるため、HackerOne上で特別プロモーションの対象となります。

同プログラムの一環として、当社ではハッカー向けのホールオブフェイム・スコアボードを運用しています。

5. ITセキュリティ

エンドポイントセキュリティ
従業員の作業用端末は全て、マルウェアの検出と検疫を行う集中管理型のEDRソリューションで保護されています。EDRソリューションは、マネージド型SOCチームにより24時間365日、継続的にモニタリングされています。
作業用端末は全てFileVault/BitLockerを使って暗号化され、パスワードで保護されており、画面のタイムアウトは10分間に設定されています。
また、デバイスマネージャーを介してパッチを適用したり、リモートで端末のデータを消去することも可能です。

パスワードポリシー
当社の社内ポリシーでは、パスワードは12文字以上で、次の文字を含むという条件が定められています。

1. 大文字
2. 小文字
3. 数字
4. 記号

企業向けパスワード管理ソリューションが利用されており、デフォルトのパスワードは定期的に変更されます。また、パスワードの再利用や共通パスワードの利用は技術的に不可能となっており、120日経過するとパスワードが有効期限切れになります。

ID・アクセス管理
システムへのアクセス権は、当社のエンタープライズ・アイデンティティプロバイダー（IdP）ソリューションを通じて、人事部門の要求と知る必要（need-to-know）および最小権限（least privilege）の原則に従い、ロールに基づいて、ITチームにより付与されます。
ユーザーのアクセス権は、雇用条件の変更後または雇用の終了後24時間以内に変更されます。また、アクセス権が適切であることを確認するために、四半期ごとにユーザーのアクセス権のレビューが実施されます。既に必要なくなったアクセス権は削除され、文書に記録されます。

メールの保護
monday.comでは、メールプロバイダーとしてGoogle Workspaceを利用しており、サードパーティのメールリレーを利用して保護されています。DMARCおよびSPFが採用されています。従業員に対しては、フィッシング回避のベストプラクティスに関して継続的に教育が行われ、定期的にテストが実施されます。

無線アクセスポイント
monday.comでは、本社の無線通信のセキュリティを確保するため、業界標準のテクノロジーを利用しています。ネットワーク全体で速やかなデプロビジョニングと否認防止を実現し、不正アクセスポイントを監視するため、さまざまなツール、特にWPA2エンタープライズを利用しています。

6. 運用のセキュリティ

顧客データへのアクセス
monday.comは、お客様がmonday.comサービスに送信する全てのデータを取り扱います。当社は、お客様のためにのみ、「ブラックボックス」としてデータを処理します。「ブラックボックス」とは、monday.comのサービス実行のために通常は顧客データへのアクセスは行われず、当社が送信された全ての顧客データを最高レベルの注意と機密度をもって取り扱うことを意味します。
monday.comによる顧客データへのアクセスは、事例ごとに、当社の利用規約またはお客様との各契約に従い制限されます。

人的資源
採用調査
当社が本社を置くイスラエルでは、採用調査を行うという慣習がなく、法律で制限されています。当社が実施する調査には、職歴の確認と前職の直属の上司に対する電話確認が含まれます。

雇用契約
monday.comの雇用契約には、守秘義務に関する規定と、特定の義務および責任に違反した場合に直ちに契約の終了を可能にする規定が必ず含まれています。
また、monday.comでは、人的資源のセキュリティに関するポリシーを策定しており、採用から退職まで、雇用期間中に求められるセキュリティ関連の活動および責任について定めています。

利用規定
monday.comでは、利用規定が定められており、セキュリティチームとより参加部署の多いセキュリティフォーラムにより年1回レビューが実施されます。当社の従業員は、採用時またはポリシーに重大な変更があった場合、ポリシーへの署名を求められます。

トレーニングと意識啓発
monday.comの従業員は、採用時のオンボーディングプロセスの一環として、またその後少なくとも年1回、情報セキュリティおよび順守すべきプライバシー関連の義務についてトレーニングを受けます。トレーニングには、記述式の課題だけでなく個別指導も含まれ、セキュリティチームによるモニタリングの対象となります。
従業員の意識をさらに高めるため、四半期ごとに「セキュリティ＆プライバシーウィーク」が実施されます。
また、必要に応じて、専門に特化したトレーニングセッションが実施されます（例：開発者に対するセキュアコーディングに関するトレーニング）。

雇用の終了
ユーザーのアクセス権は、雇用条件の変更後または雇用の終了後24時間以内に変更され、会社の機器が返却されます。アクセス権が適切であることを確認するために、四半期ごとにユーザーのアクセス権のレビューが実施されます。

レッドチーム演習
当社では年2回、当社の防御体制に対するレッドチーム演習を実施しています。これには、内部ペネトレーションテストやインフラ攻撃が含まれ、仮想的な攻撃のシミュレーションが行われます。レッドチーム演習は、攻撃・防御に通じた一流のサードパーティ・セキュリティコンサルティング企業により行われ、ハイエンドの洗練された攻撃手法が用いられ、潜在的なセキュリティリスクと脆弱性が独自の視点で明らかになります。

カバナンスとリスク管理
monday.comでは、monday.comのシステムに内在する脆弱性を積極的に特定し、当社のオペレーションに対する新たな脅威を評価するために、継続的なリスク管理プロセスを整備しています。monday.comは、ISO 27001認証の一環として、毎年リスク評価を受けています。

インシデント対応・管理
monday.comのインシデント対応計画（IRP）では、セキュリティインシデントやプライバシーインシデントの検知、担当者へのエスカレーション、コミュニケーション（社内・社外）、軽減、事後分析に関するガイドラインが定められています。
monday.comのインデント対応チーム（IRT）は、セキュリティ・R&D・法務の各部門の代表者、事例に応じてその他の部署の代表者、そして必要に応じてサードパーティのインシデント対応業者により構成されます。

通知
monday.comは、データインシデントを把握した場合、データ処理補足契約書第7条（「データインシデントの管理および通知」）の規定に従い、影響を受けるお客様に遅滞なく通知を行います。
影響を受けるお客様に対しては、データ漏洩の性質、monday.comが把握している負の影響、monday.comが講じた措置、通知時点におけるインシデントの修復または軽減プランが通知されます。

災害復旧と事業継続
monday.comは、当社の物理的なオフィス（本番用のインフラは一切設置されていません）に影響を及ぼす災害に対処するため、ISO 27001に沿った事業継続計画を整備しています。
また、当社の本番環境に影響を及ぼす災害に対処するための災害復旧計画（DRP）も策定されており、サービスの中核機能を専用のDRロケーションから復元するプロセスが定められています。テストは、少なくとも年2回実施されます。monday.comのDRテストは、ウォークスルー、模擬災害またはコンポーネントテストの形で行われます。

データの保持・破棄
データの保持
monday.comは、プライバシーポリシーに記載された目的を達成するのに必要な期間、monday.comの管理下にある情報を保持します。monday.comがお客様に代わって処理するデータは、利用規約、データ処理補足契約書、その他当該お客様との間の商業上の取り決めに従って保持されます。

データの削除
monday.comのお客様は、送信したデータを完全にコントロールする権利を有し、サービスのユーザーインターフェースを通じて利用可能な手段を用いて、いつでもデータを修正、エクスポートまたは削除することができます。
サブスクリプションが終了または満了した場合、お客様は、アカウント閉鎖手続きの一環として、自らのデータの削除を要請することができます。お客様のデータは要請から90日以内に削除されます。これには、ロールバックが認められる30日間と、削除手続きを進めるための追加の60日間が含まれます。
また、お客様はプラットフォーム内にアカウントのデータを残すという選択をすることもでき、その場合、当社は引き続きデータを保持しますが、当社の裁量によりいつでも削除することができます。

データの破壊
当社のサービスはAWS上にホストされ、特定のデータはGCPにバックアップされます。どちらのクラウドコンピューティングプロバイダーも、マルチテナント環境で機微データを安全に保管できるよう、データの分散と削除に関する独自の戦略を導入しています。ストレージメディアの撤去は、NIST 800-88で詳細に定められた手法を用いて、上記プロバイダーにより実施されます。

監視・ログ
monday.comは、ネットワーク侵入検知システム（NIDS）によるネットワークログ、エッジロケーションからのトラフィックログ、イベントの追跡・監査用のアプリケーションレベルのログ、アクセスの監査および高い権限が必要なオペレーションの監査用のシステムレベルのログを収集し、監視を行います。ログは、セキュリティ情報イベント管理（SIEM）ソリューションに転送され、マネージド型SOCチームにより継続的に（24時間365日）監視されます。

サプライチェーン管理
復処理者
monday.comは、復処理者　（グローバルデータリージョンおよびEUデータリージョンの両方）がデータセキュリティおよびプライバシー分野の業界標準を順守するよう徹底し、復処理者の選定プロセスにおいてこれらの分野を特に重視しています。当社は、全ての復処理者に関して、特にデータ処理補足契約書その他の関連文書や保護措置が整備されていることを確認しています。また、プライバシー、法的側面、情報セキュリティに関する評価ならびに質問票ベースの監査を、全て業界標準および法規制上の要件に従って実施しています。復処理者の評価は、少なくとも年1回実施されます。

ベンダー管理
monday.comでは、当社が利用するサービスおよびソフトウェアの両方について、セントラルリポジトリ型の資産管理プログラムを導入しています。リポジトリの資産は、セキュリティ・法務・プライバシー・調達の各部門により継続的に整備され、承認プロセスは全従業員に伝えられます。
サービスまたはソフトウェアの利用開始時および更新時には、最高でどの機密レベルのデータにアクセスするかに応じて、各部門が取引先のベンダーを分類します。この分類は、適切なリスクレベルを判断し、業界標準および法規制上の要件に従ってベンダーを審査するために必要となります。

物理的なセキュリティ

monday.comのオフィス

monday.comのオフィス内の物理的なIT資産は、ノートパソコンとオフィスネットワーク用デバイスに限定されます。オフィスネットワーク用デバイスは、24時間365日運用の環境制御されたサーバールーム内で保護されており、サーバールームはパスワードで施錠され、CCTVカメラで監視されています。オフィスへの物理的なアクセスは、生体認証を通じて制御されています。来訪者は、オフィスへの入室時に記録され、オフィス滞在中は、常にmonday.comの従業員の付き添いが求められます。従業員は全員、疑わしい行動、施設への不正アクセス、盗難や紛失物のインシデントを報告する必要があります。

データセンターのセキュリティ

monday.comは、AWSおよびGCPのワールドクラスの物理的・環境的セキュリティ対策を利用しており、その結果、レジリエンスの高いインフラが構築されています。これらのセキュリティ対策の詳細については、次のリンク先をご覧ください。
https://aws.amazon.com/security/、https://cloud.google.com/security/

7. コンプライアンス、プライバシー、認証

監査の保証と順守

monday.comでは、業界標準となっている複数のコンプライアンスプログラムや、当社サービス提供地域の主要なプライバシーおよびデータ保護法制に従い、セキュリティおよびプライバシーに関するプログラムを構築しています。

ISO 27001、27017、27018、27032、27701

monday.comは、ISO（国際標準化機構）の国際標準に従い、これに沿って情報セキュリティ、クラウドサービス、プライバシーを管理しています。当社は毎年、独立した第三者の監査を受けており、5つのISO認証を取得しています。

- **ISO/IEC 27001:2013**は、情報セキュリティ管理システム（ISMS）に関する最も厳格なグローバルセキュリティ規格です。
- **ISO/IEC 27018:2014**は、パブリッククラウドコンピューティング環境において、ISO/IEC 29100が定めるプライバシー原則に沿った個人情報（PII）保護策を導入する上で一般的に認められる管理目的、管理策、ガイドラインを定めています。
- **ISO/IEC 27017:2015**は、クラウドサービスのプロバイダーおよび顧客の双方を対象に、管理策とその導入に関するガイダンスを定めています。クラウドサービスの提供と利用に関する情報セキュリティ管理策のガイドラインが提供されており、関連する管理策について詳細な導入のガイダンスが定められています。
- **ISO/IEC 27032:2012**は、サイバーセキュリティの状態を改善するためのガイダンスを定めており、サイバーセキュリティ固有の事項と他のセキュリティ分野、特に情報セキュリティ、ネットワークセキュリティ、インターネットセキュリティ、重要情報インフラ防護（CIIP）に対する依存関係を明らかにしています。
- **ISO/IEC 27701:2019**は、プライバシー情報管理システム（PIMS）の確立、導入、維持、継続的改善に関する要件とガイダンスを定めています。

当社が取得している認証は、こちらで全て確認できます。

SOC 1、SOC 2、SOC 3

monday.comは、SOC（Service and Organization Controls）報告書を取得しました。

- **SOC 1 Type II監査**は、顧客の財務報告に係る内部統制を調査するものです。
- **SOC 2 Type II監査**は、セキュリティ、可用性、機密性に関して業界内で最も厳格な基準を満たすという当社の姿勢を証明するものです。同監査により、monday.comのセキュリティ統制がAICPA（米国公認会計士協会）のTrustサービス原則および基準、そしてHIPAAのセキュリティ要件に準拠していることが証明されています。
- **SOC 3報告書**は、SOC 2 Type II報告書の簡易版であり、公開されています。

監査は、独立した第三者により毎年実施され、4月～3月を対象とした報告書が年1回発行されます。

monday.comのSOC報告書は、次のリンク先で確認できます：SOC 1、SOC 2、SOC 3

クラウドセキュリティアライアンス（CSA）

クラウドセキュリティアライアンス（CSA）は非営利団体で、「クラウド コンピューティング内のセキュリティを保証するためのベストプラクティスの使用を推進し、その他あらゆる形式のコンピューティングのセキュリティ確保に役立つよう、クラウドコンピューティングの利用に関する教育を提供する」ことを使命としています。monday.comは、自由参加型のCSA「Security, Trust, Assurance, and Risk Registry（STAR）」自己評価に参加し、CSAが公表しているベストプラクティスに関する当社の順守状況を文書にまとめています。当社が作成した「CSA Consensus Assessments Initiative Questionnaire（CAIQ）」は、CSAのWebサイトで無料公開されています。

医療保険の携行性と責任に関する法律（HIPAA）

医療保険の携行性と責任に関する法律（HIPAA）は、医療データの保護を推進することを目的としています。病院、診療所、健康・医療保険、保護対象保険情報（PHI）の取扱い企業などの組織は、HIPAAの順守が求められています。この義務の適用範囲は、上記組織と取引する企業や、上記組織に代わってPHIに接する企業にも拡大される場合があります。

monday.comでは、お客様が機微な医療情報を送信できるように、エンタープライズプランのお客様に対し、HIPAA準拠のアカウント構成を提供しています。HIPAAの対象となるお客様は、PHIの保護と適切な処理を受けられるよう、HIPAAデータを送信する前に当社と事業提携契約（BAA）を締結する必要があります。

monday.comとGDPR

当社のグローバルプライバシープログラムは、世界で最も包括的で先進的なデータ保護規制に基づいており、EUおよび英国の一般データ保護規則（GDPR）が基準となっています。

とりわけ、monday.comのプライバシーフォーラムは、組織全体の製品・プロセス開発や、個人データの使用を伴うさまざまな活動を継続的に監視し、プライバシーバイデザイン、データ最小化とストレージ制限、処理の合法性と公正性、当社の活動および目的の透明性といったGDPRの各原則が順守されるよう徹底しています。

プライバシーポリシー

monday.comのプライバシーポリシーは、当社がデータ管理者として独自の目的で処理する個人データに関してプライバシーおよびデータ保護の取り組みを定めたもので、次のリンク先で確認できます。

データ処理補足契約書（DPA）

monday.comの利用規約およびお客様との契約書には全て、お客様のために個人データが確実に保護され、適切に処理されるよう、データ処理補足契約書が含まれています。 当社のデータ処理補足契約書は、オンラインで確認し、署名することができます。

個人データの越境移転

monday.comの本社はイスラエルにあり、米国、英国、オーストラリア、ブラジルに子会社、ウクライナとグアテマラにサポートチームが置かれています。復処理者もさまざまな国で登録されており、詳細は復処理者のページで確認できます。
当社は、EEA（欧州経済領域）および英国から他の国に個人データを移転する際、GDPRの下で提供されている合法的な移転メカニズムを利用します。具体的には、欧州委員会による「十分性認定（adequacy decisions）」（例：英国およびイスラエルが、EU起源の個人データの保護に関して十分な水準の保護を提供しているとみなす認定）やEU標準契約条項などで、こちらとこちらで確認できます。

管理者と処理者

GDPRは、個人データの収集および処理に関して、データ管理者とデータ処理者という2つの主要な役割を定義し、区別しています。データ管理者は個人データを処理する手段と目的を決定し、データ処理者は管理者に代わってデータを処理します。

- monday.comは、お客様、ユーザーおよびWebサイト訪問者に関する個人データのデータ管理者です。詳細は、プライバシーポリシーに記載されています。
- monday.comは、お客様およびユーザーがプラットフォーム（それぞれのmonday.comアカウント内のボードおよびアイテム）に送信する個人データのデータ処理者で、お客様に代わってこのデータを処理します。当社はこれを、お客様と締結するデータ処理補足契約書に従って行います。このデータの処理に関して支援を受けるために当社が利用するサードパーティサービスプロバイダーは、当社の「復処理者」になります。

monday.comとCCPA

monday.comは、「サービスプロバイダー」として、お客様がmonday.comを中断なく使用できるよう、また当社がCCPAに従ってカリフォルニア州のお客様の個人情報を処理できるよう、世界中の類似の規制（GDPRなど）および進化する業界標準に配慮しつつ、当社に適用される2018年のカリフォルニア州消費者プライバシー法（CCPA）およびカリフォルニア州司法長官が定める規制の要件を順守します。
詳細は、こちらで確認できます。

オーストラリアのプライバシー法（APA）とプライバシー原則（APP）

オーストラリアのプライバシー法（APA）およびプライバシー原則（APP）は、個人情報の収集、処理、利用および共有に関する構造的な枠組みを定めており、自らの情報の取扱いについて消費者により大きなコントロール権限を与えています。monday.comは、APAおよびAPPの要件を順守します。
詳細は、こちらで確認できます。

内部監査

当社のセキュリティ・プライバシー・インフラ・R&D・IT・運用・法務の各部門は、四半期ごとにセキュリティ＆プライバシーウィークを実施しています。具体的には、ユーザーアクセスレビュー、ファイアウォール構成レビュー、クリアデスクの点検、意識啓発のためのトレーニングや活動をはじめ、さまざまな監査活動が実施されます。

政府当局への開示

monday.comは、政府当局が当社の保持する顧客データに正当な理由なくアクセスすることを認めていません。当社が（米国その他の）当局から顧客データの開示要請を受けることは稀です。過去、そうした要請を受けた事例は数少なく、対象範囲は限定されており、当該データを要請する理由も非常に正当なものでした（例：特定のアカウントに関連する不法行為の疑い）。

要請が有効かつ正当なものであることを確認するため、当社の法務部門およびプライバシー部門により要請内容の確認が行われ、法律上厳密に必要なデータに限り開示が行われます。当社は、それが禁止されている場合や潜在的なリスクによりそれが不可能な場合を除き、かかる開示を実施する前に、商業上合理的な範囲で顧客に通知する努力を行います。[3]当社はまた、適用法に従い、FISA（外国情報監視法）第702条を含め、GDPRまたは英国のGDPRで保護されている個人データに関する一括監視の要請を拒否するよう、商業上合理的な努力を行います。

PrivacyTeamとDPO

monday.comは、イスラエルを代表するプライバシーコンサルタント企業であるPrivacyTeamにより保護されており、PrivacyTeamと協力して顧客データとプライバシーの保護のために鋭意努力しています。詳細は、こちらで確認できます。

monday.comは、データ保護責任者として、プライバシー問題に長年取り組むPrivacyTeamのAner　Rabinovitz氏を任命しました。データ保護責任者は、monday.comのプライバシー面での継続的なコンプライアンスについて監視・助言を行い、プライバシーの問題に関してデータ主体および監督機関との連絡窓口となります。

---

[3]詳細は、プライバシーポリシー第4条（「データ共有」）で確認できます。

8. エピローグ

本ホワイトペーパーは、セキュリティおよびプライバシーに対するmonday.comの取り組みについて、概要を幅広く説明するものです。当然、複雑なテーマであるため、さまざまな疑問をお持ちかもしれません。
より詳しい情報については、セキュリティトラストセンターおよびリーガルポータルをご覧ください。
情報セキュリティおよびプライバシーに関するmonday.comの体制についてご不明な点がある場合は、security@monday.comまたはdpo@monday.com宛に担当者にお問い合わせいただくこともできます。一般的なサポートについては、support@monday.comで24時間365日受け付けております。
セキュリティに関する懸念事項や脆弱性について報告したい場合は、security@monday.com宛にメールを送信するか、https://monday.com/security/form/のHackerOneフォームを通じてご報告ください。

免責条項： このバージョンは、英語の原文を翻訳したものであり、便宜上の目的でのみ提供されています。この英語の原文は、正式な法的拘束力のあるバージョンであり、矛盾が生じた場合には英語の原文が優先されるものとします。