miro

Miro のセキュリティーとコンプライアンス

信頼のエンタープライズ グレード保護機能

miro

目次

miro

概要

いまや企業にとって、イノベーションは事業の存続に必要不可欠となりました。Miro は、時代を見据えたイノベーションのためのビジュアル ワークスペースとして、企業の革新的な取り組みをサポートし、Google、Nike、Ikea、Deloitte、Cisco などの Fortune 100 社の 99% を含め、革新的な戦略で成功を納めた 18 万を超える組織に選ばれる、信頼のサービスを提供しています。

Miro は、戦略立案やプラン、顧客のニーズにフォーカスした製品やサービスの設計など、さまざまな用途に活用されています。しかし、分散したグローバルなチーム連携では、機密情報を扱うための安全で信頼性の高いプラットフォームが必要となります。また、組織内のすべての関係者が必要なときに適切なアクセス権を確保している必要もあります。

この白書では、**エンタープライズ グレードのインフラのセキュリティー、コンプライアンス、製品セキュリティー制御、プライバシー**を最も重視しつつ、Miro がどのようにイノベーションを支えているのかを概説します

責任の共有

本書の目的は、当社の役割を説明し、御社が Miro でセキュリティーへの取り組みを一層強化する際に有効なすべてのオプションをお伝えすることにあります。

この図は、セキュリティーに対する当社の施策の概要を示しています。下の 2 つの層は、情報セキュリティーを確保してコンプライアンスを支援するために Miro が管理するものです。上の 2 つの層は、各社のセキュリティーとコンプライアンスの要件に基づいてお客様が構成できるよう当社で構築した機能を表しています。

本書では、これらの機能について詳しく説明していきます。

Miro のセキュリティーとコンプライアンスのアーキテクチャー

インフラストラクチャーのセキュリティー

Miro は、エンタープライズ グレードの SaaS（Software-as-a-Service：サービスとしてのソフトウェア）プラットフォームとして、情報の保護がセキュリティー管理の取り組みで大きな部分を占めます。これには、クラウドリソースに加え、コンピューターやネットワークシステムなど物理的なテクノロジー資産も考慮されます。これらの資産を安全に保つことで、従来のサイバー セキュリティー攻撃だけではなく、直接的な盗難や自然災害などの物理的な脅威からの保護にも役立ち、結果として、お客様の情報を保護することができるのです。

データセンター

Miro は、主としてクラウド コンピューティング インフラストラクチャーに Amazon Web Services（AWS）を使用し、AWS のセキュリティー機能を活用してホストされたデータと作業負荷を保護しています。クラウド コンピューティングは、共通のアカウンタビリティー モデルに基づいて構築されています。

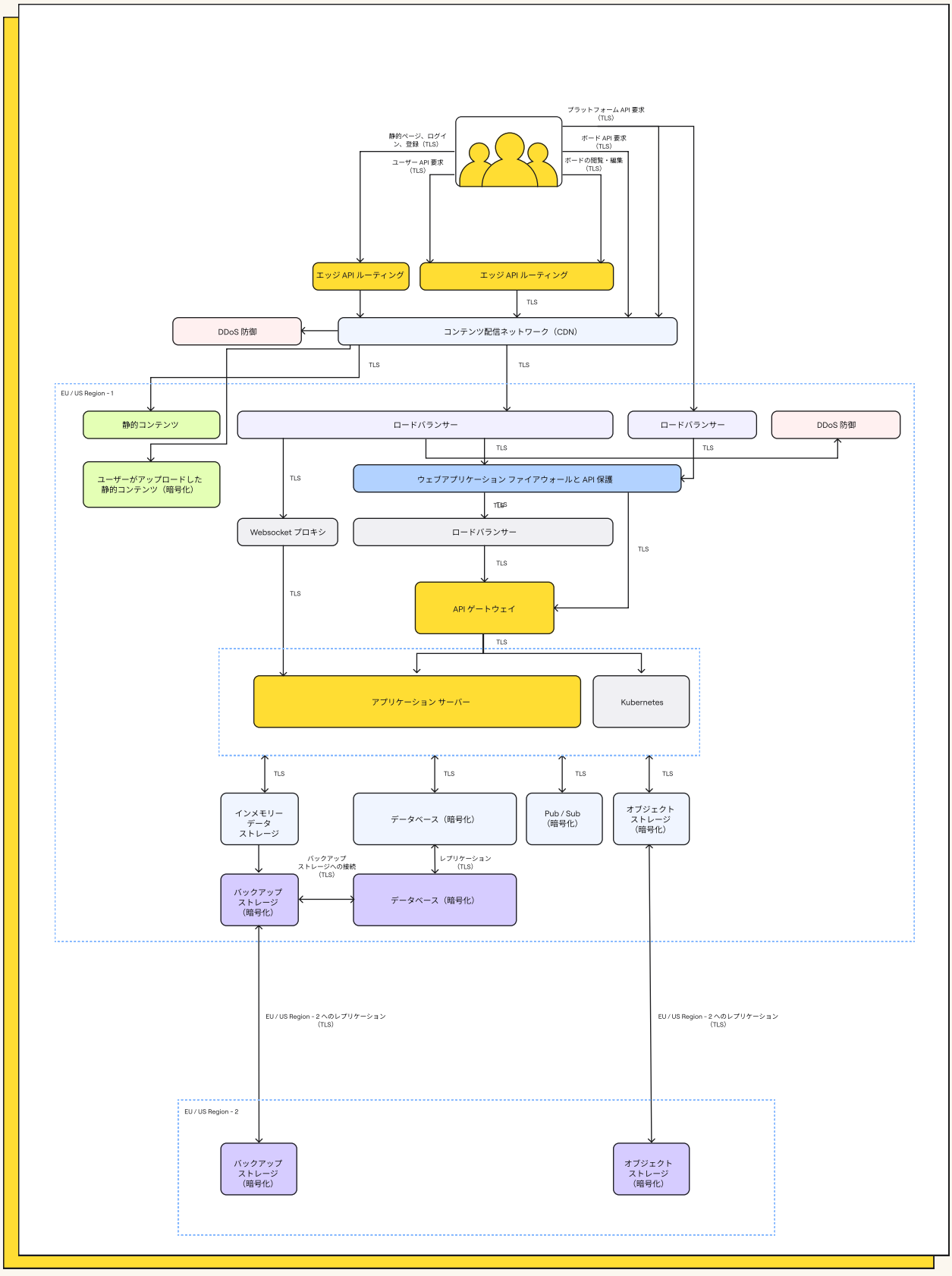
AWS は、データセンターの物質的な制御、データプライバシーの保障、サービスに対する厳重な管理といった、堅固なセキュリティー対策を実装しています。AWS コンピューティング環境は、SOC 1/SSAE 16/ISAE 3402（旧 SAS 70）、SOC 2、ISO 9001 / ISO 27001、FedRAMP、DoD SRG、PCI DSS Level 1 などの、さまざまな地域や業種の公認機関による認定のもと、継続的に監査されています。

Miro の主要なプロダクション システムは、EU（アイルランド）と米国（オハイオ）にある AWS データセンターに置かれています。また、EU（フランクフルト）および米国（バージニア）にある AWS データセンターは、通常時バックアップデータを保存する目的で使用されており、万一の場合には災害復旧プランに沿って稼働させることもできます。

AWS クラウド インフラストラクチャー内で Miro は、業界のベストプラクティスと AWS の Well-Architected フレームワークに準じ、クラウド インフラストラクチャーの論理、ネットワーク、アプリケーション セキュリティーを設定します。保護対策は、明示的に許可されていない限り、最小権限の原則（PoLP）と拒否の原則（deny by default）により、階層的に実装されます。管理とアクセスの権限は特定の従業員に対して厳密に制限されており、多要素認証（MFA）と仮想プライベート ネットワーク（VPN）を介したマネージド デバイスからのアクセスが必要となります。

詳しくは、AWS の責任共有モデルを参照してください。

EU と米国でのデータフロー



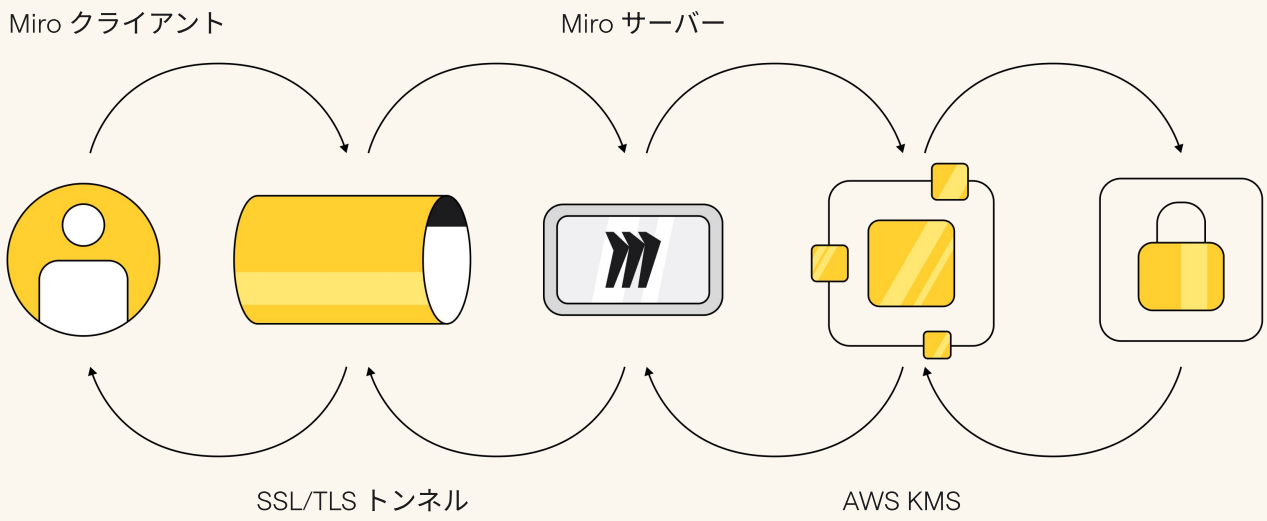
miro

データの暗号化

Miro は、ユーザーデータを保護するために様々な暗号化方式を採用し、データセキュリティーと法人のお客様が要する技術的要件との均衡をとっています。

Miro は保存中と転送中いずれのデータ保護についても、最新の暗号化標準に準拠しています。つまり、保存時は**AES 256 ビット（高度暗号化標準）**暗号化、転送時は TLS 1.2 に加えて **TLS 1.3（トランスポート層セキュリティー）**をサポートしています。この仕組みにより、データのライフサイクル全体を通じて、エンドツーエンドの暗号化を確保できます。

Miro の暗号化の仕組み



詳しくは、暗号化に関するホワイトペーパーをダウンロードの上ご確認ください。

暗号鍵の管理

Miro の鍵管理インフラストラクチャーは運用上、技術上、手続き上のセキュリティー管理を念頭に置いて設計されており、暗号鍵への直接アクセスを極めて厳しく制限しています。暗号鍵の生成、交換、保管は、ばらばらに分散処理されます。Miro では、AWS Key Management System（KMS）を介して、ユーザー自身の AWS アカウントで発行された鍵を使った鍵管理システムを使用しています。

- **ファイル暗号鍵：**ファイル暗号鍵の生成、保管、保護は、生産システム インフラストラクチャーのセキュリティー制御とセキュリティー ポリシーに沿って実行されます。
- **内部の SSH 鍵：**生産システムへのアクセスは独自の SSH 鍵の組み合わせにより制限され、内部システムにより公開鍵への切り替えプロセスを保護した上で管理し、プライベート鍵を安全に保存します。
- **鍵の配布：**Miro は、機密性の高い暗号鍵を運用に必要なシステムに限定して自動的に配布し、管理します。暗号鍵配布システムは AWS KMS を基盤とするものです。

シークレット管理

パスワード、API キー、データベース認証情報、証明書などの機密データは、当社のシークレット管理システムで安全に保存されます。当社のシークレット管理システムへのアクセスは、秘密データを必要とするサービスに限定して許可され、当社の少数の運用エンジニアにのみ限定されています。

アクセス制御および認証

Miro の技術的アクセス制御と社内規定では、ユーザーのボードやその他のユーザーのアカウントに関する情報に、従業員が恣意的にアクセスすることを禁じています。Miro の中核サービスの開発を担当する少数のエンジニアのみが、問題解決の必要がある場合にのみ、かつユーザーの明示的な同意がある場合に限り、アクセスできます。Miro のサポート担当者であっても、お客様から明示的に招待されない限り、ボードのコンテンツを利用することはできません。従業員のアクセス権は、退職時に即時失効します。

ネットワーク セキュリティー

Miro は、セキュリティー グループ、プロキシ、ネットワーク セキュリティーの監視とテスト、侵入検知システム、監査など、多層にわたる保護と防御を使い、バックエンド ネットワークのセキュリティーを維持しています。

本番環境における内部ネットワークへのアクセスは、シングルサインオン（SSO）および MFA を使用して、VPN 経由で許可されたユーザーグループのみに制限され、すべてのシステムで鍵認証を必須としています。

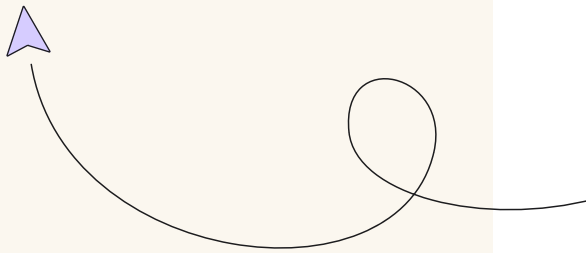
脆弱性に関する取扱い

Miro のセキュリティー担当部門は、自動および手動で定期的にアプリケーションとインフラストラクチャー セキュリティーのテストを定期的に実施し、脆弱性リスクを特定、対処します。また、毎年、独立したサービスプロバイダーによる外部ペネトレーションテストを実施し、検出された問題は 速やかに処理されます。また、当社製品やサービスで見つかった脆弱性を提起する公開バグ報奨金プログラムでは、セキュリティー研究者に報奨金も提供しています。

チェンジマネジメント

Miro には、正式な変更管理ポリシーが備わっており、本番環境に実装する前にすべてのアプリケーションの変更内容をチェックし、セキュリティー要件が満たされている状態であることを確認しています。Miro では、本番環境における変更権限は許可された担当者のみに制限されています。また、セキュリティーチームが、サーバー、ファイアウォール、その他のセキュリティー関連の構成を、業界標準に沿った最新の状態に維持します。

クラウド セキュリティー ポスチャー管理（CSPM）を利用することで、クラウド環境において最も重要な脅威の状況を常に把握し、クラウド インフラストラクチャーで必要とされる脆弱性や更新に関する警告を受け取ることができます。



セキュリティー ポリシー

> Miro では、リスクを評価し、サービスのセキュリティー、機密性、完全性、可用性を継続的に改善しています。当社では、セキュリティー ポリシー（情報セキュリティー、安全なソフトウェア開発ライフサイクル、インシデント対応、論理アクセス、変更管理）を、少なくとも年に一度は見直し、承認を行っています。また、上記のポリシーのコンプライアンスを監視し、アプリケーションとネットワーク セキュリティーのテスト、社内外でのリスク評価を実施しています。

社内規定とアクセス権

現地の法令で許可されている場合において、Miro の従業員は過去の犯罪歴の調査を受け、セキュリティー規定の確認書への署名、守秘義務厳守への同意、必須のセキュリティー トレーニングの完了が必要とされており、最善の慣行に従い顧客データを確実に保護できるよう対処しています。

ネットワーク間のアクセス許可は、最小限の従業員とサービスに厳しく制限しています。また、ファイアウォールの構成を厳密に制御し、これも少数の管理者に制限しています。他のリソースへのアクセス許可は、適切な個人による明示的な承認によって許可されており、アクセス要求と正当な理由の記録は管理者によって記録されています

フィジカル セキュリティー

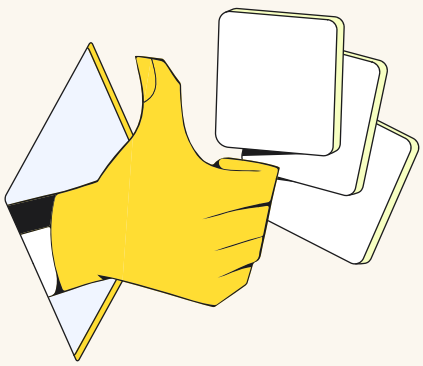
Miro はサードパーティーの専門プロバイダーによる物理的なセキュリティー ポリシーを実施し、企業オフィス内のセキュリティーを管理しています。コーポレート施設への物理的なアクセス許可は、バッジアクセスシステムを介して許可を受けた Miro の担当者のみに制限されています。ビジター バッジシステムを使用し、許可された個人のみが設備内にアクセスできるよう徹底しています。コーポレートサーバーが位置するエリアへのアクセス許可は、バッジアクセス システムによりその任務を認められた個人にのみ限定されます。コーポレート環境および本番環境への物理的なアクセスが承認された個人のリストは、四半期に最低一度は見直しを行います。

信頼性

Miro のサーバーインフラは、安全なデータ保管環境と高い可用性を提供します。すべてのアプリケーション サービスは、冗長性を高めるため、負荷分散と耐障害システムを備えた複数のサーバー上で実行されています。またクラスタートポロジーは、N+1 レベルの高い可用性で分類されます。ユーザーデータは、保護のために複数の可用性リージョンに複製され、暗号化されて定期的にバックアップされます。さらに日々のデータベースのバックアップは、メインのデータセンターとは別の場所に保存されます。

インシデント対応

Miro のインシデント対応チームは、365 日 24 時間、年中無休であらゆるインシデントに対応可能な体制を整えています。インシデント処理規定は、サービスの可用性、整合性、セキュリティー、プライバシー、機密性の問題に対処します。この手順とは、インシデントへの迅速な対応、緊急度の評価、封じ込め措置、関係者とのやり取り、status.miro.com 内でのステータス更新などを指します。



ディザスター リカバリー

Miro のビジネス運営に影響を及ぼす危機や災害が発生した場合、当社のインフラストラクチャー部門は、災害復旧プラン（DRP）に準じて情報セキュリティー要件に対応します。調査結果は文書化され、解決されるまで追跡調査を行います。当該部門は、実際の回復時間（RTA）の測定等を含む本プランの審査とテストを、毎年 1 回以上実施します。

DRP は、耐久性と可用性の両方の障害に対処します。耐久性に関する被害とは、プライマリー データセンターがすべてまたは永久に消失した場合、あるいはデータセンターからの通信が不可能になった場合、データを提供できなくなった状況を意味します。

目標復旧時間（RTO）は、災害発生後にビジネスプロセスまたはサービスの復元までに許容できる時間とサービスレベルを意味します。目標復旧時点（RPO）は、サービスの中断によって失われる可能性があるデータの最大許容期間を意味します。

Miro のインシデント対応とディザスターリカバリー プランは、計画された間隔で、または組織内もしくは環境に大きな変化が発生した場合にテストを実施することになっています。

コンプライアンス、監査、認証

Ponemon Institute の『Cost of a Data Breach Report 2023（データ漏えいのコストに関する報告書 2023 年）』によると、データ侵害の最大要因のひとつに、セキュリティー規制を順守していないことがあげられています。Miro がコンプライアンス順守を重要視しているのは、そのためです。Miro には、最高情報セキュリティー責任者が率いる専任のセキュリティー部門があり、この部門はコンプライアンスとガバナンスを専門とする複数のセキュリティー チームで構成されています。Miro のデータプライバシー責任者は、プライバシー規制を確実に順守できるよう、データプライバシーを管理、監督します。社内の独立した 監査機能が、ガバナンスの客観的な保証と審査を確保するために設けられています。

Miro の準拠状況

Miro は、ビジネス展開する特定地域の法的要件を順守しています。また、不正なデータアクセス、侵害、脅威から顧客データを保護するためのデータセキュリティーやプライバシーの基準についても、透明性を確保しています。

これらの認証と、確立された基準の監査・認証により、当社は、SOC 2 Type II の独立保証報告などの、監査期間中の統制のコンプライアンスと運用の有効性を評価することができます。

この評価には以下のようなものがあります：

- SOC 2 Type II や ISO/IEC 27001 などの**情報セキュリティー標準**
- 業界をリードする EU データレジデンシー ソリューションと標準契約条項の使用による**データ転送標準**を通じて、一般データ保護規則（GDPR）順守に対応する EU と英国外で、適切なレベルのデータ保護を提供しています。
- Cloud Security Alliance、Cyber Essentials、TISAX などの、**地域およびセクター固有の認定**
- 英国規格協会（BSI）のような優良機関による**定期的な第三者監査**
- **アクセシビリティー ガイドラインと** VPAT に基づくアクセシビリティー適合性レポート（ACR）

Miro のユーザー個人データ保護

欧州の GDPR など個人情報保護法やデータ保護法規は厳格化しており、企業がユーザーデータを収集、処理、転送、保存する方法に関して、厳しい義務を課しています。これらの規制に従わない場合は、多額の罰金が課されて規制当局の監視下に置かれるのに加え、顧客からの信頼喪失にもつながり、SaaS ビジネスに打撃を与えかねません。

Miro は、従業員の行動と製品設計を通じて、顧客の個人データを保護することに重点を置き、確立された業界慣行に基づいて、プライバシーとデータ保護プログラムを実施しています。従業員にはデータ保護基準の順守と守秘義務が課され、また、技術的制限の対象となります（従業員規定およびアクセスを参照）。Miro の製品設計プロセスには、規制の点検項目と法的審査が含まれ、製品および技術部門には、設計基準に関する定期的な研修を実施しています。

Miro のプライバシーポリシーは、Miro がデータ管理者として処理する個人データ種別を、確立された業務目的とともに、明示的かつ透過性をもって定めています。また、Miro が個人データの処理を目的として関与するサードパーティー種別の概要、データ保護法に基づく個人の権利の行使の方法、Miro が EU 地域外に個人データを転送することに依拠したデータ転送の仕組みについても概説しています。

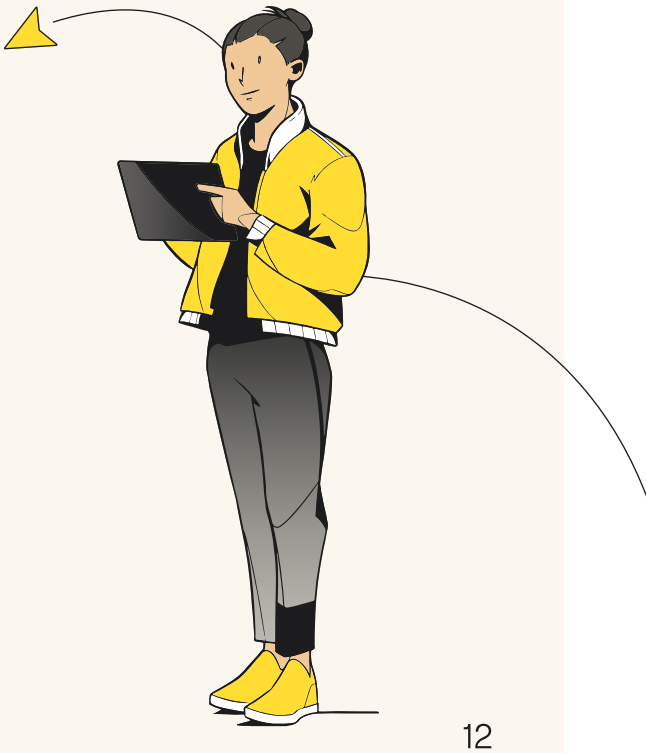
Miro がお客様に代わって個人データを処理する場合、またはお客様の個人データを EU 外に転送する場合、当社は、GDPR、カリフォルニア州消費者プライバシー法（およびカリフォルニア州プライバシー権法による修正内容）、およびその他の米国および世界のプライバシーおよびデータ保護法で義務付けられている契約上の確約を含む、データ処理補遺条項（DPA）などを通じて、適切な条件を締結することに同意します。

第三者によるデータ処理

Miro は、お客様の個人情報を処理するサードパーティーと契約する場合、法的審査やセキュリティー審査、適切なデータ処理・転送条件への同意など、厳格な調達プロセスを要求しています。Miro は、当該サードパーティーが記載されたリストを DPA 内のリンクからオンラインで入手できるようにし、関連するサードパーティーを当該リストで変更または追加する場合は、DPA に示されたプロセスに従って、その意図をお客様に通知します。

製品セキュリティー

クラウドベースのプラットフォームである Miro は、デスクトップとモバイル端末の両方のウェブサイトのブラウザーから、または両プラットフォームの専用アプリから利用できます。これらのサービス提供方法と、Miro のようなプラットホームを介したリモートでの分散コラボレーションの性質により、当社では、お客様がゼロトラスト アーキテクチャー（ZTA）を実現できるよう支援することが必要です。これは、お客様が適切なセキュリティー ソリューションを利用できるようにするだけでなく、正しく導入されるよう支援することも意味します。



ゼロトラスト アーキテクチャー

ユーザーの位置情報またはネットワーク エントリー ポイントに基づいて幅広いアクセスを許可する従来のセキュリティーモデルとは異なり、ZTA では、脅威は社内外を問わず、どこからでも発生する可能性があることを前提としています。これは、従業員があらゆる場所やデバイスから企業リソースを利用するという現代的な働き方において、ますます重要になっています。ZTA では、ユーザーのデータやリソースでのあらゆる作業において、ID、デバイスのセキュリティー、セキュリティー ポリシーの順守を継続的に検証することを提唱しています。

Miro は、コラボレーション機能を損なうことなく、管理者がきめ細かい権限設定と制御を用いて適切なポリシーを設定できるようにすることで、**企業の ZTA への取り組みを支援**します。これらのセキュリティー制御には、次のような項目があります。

- **SSO：**SAML ベースの SSO を使用することで、Okta、Azure AD、AuthO、Google SSO などのユーザーが選択した ID プロバイダー（IdP）経由で Miro にアクセスできます。これにより、ユーザーが各アプリケーションの認証情報を繰り返し入力する必要がなくなるため、時間を節約できると同時に、攻撃対象の数も削減します。

- **2FA：**Miro では、SSO なしで 2 要素認証（2FA）を利用できるため、ユーザーが会社の Miro サブスクリプションにアクセスする際の保護を追加できます。2FA は、メールアドレスとパスワードでログインするすべてのユーザー（SSO を使用する企業の外部コラボレーターや、SSO を設定していない組織の全ユーザー）に適用されます。ユーザーは、これを自分のプロフィール画面で設定するか、または、会社の管理者が組織全体で 2FA を有効化することができます。Miro は、Microsoft Authenticator、Google Authenticator、Authy などの時間ベースのワンタイムパスワード（TOTP）アプリケーションを使用して 2FA を適用します。

- **アイドルセッションのタイムアウト：**ユーザーが非アクティブでいられる時間の長さに制限を設け、自動的にログアウトするよう設定できます。この制限により、既存のユーザーセッションデータを盗用しようと試みる攻撃者（リモート、または無人ワークステーション経由）がアクセスできる時間枠が最小限に抑えられます。

- **管理者向けのロールベースアクセス：**各種ワークフローを実行するためにユーザーに割り当てることができる複数の管理者ロール（会社の管理者、ユーザー管理者、コンテンツ管理者など）があり、それぞれに特定のレベルのアクセス権限、設定、構成が設けられます。これにより、管理者の負荷がセキュアに分散され、管理者による不要な権限の保持や機密情報へのアクセスを防ぎます。

- **共有ポリシー：**組織のコンテンツにアクセスするタイミングと方法を決定し、ポリシーを次のように設定できます。
  - 許可されたドメイン外での共有を制限する
  - 公開リンクによる共有を制限する
  - 公開ボードのパスワードを要求する（組織レベル）
  - チーム全体および会社全体での共有を制限する（チームレベル）
  - ボードの他のチームへの移行を制限する（チームレベル）
  - 顧客テンプレートの全社的な共有を制限する

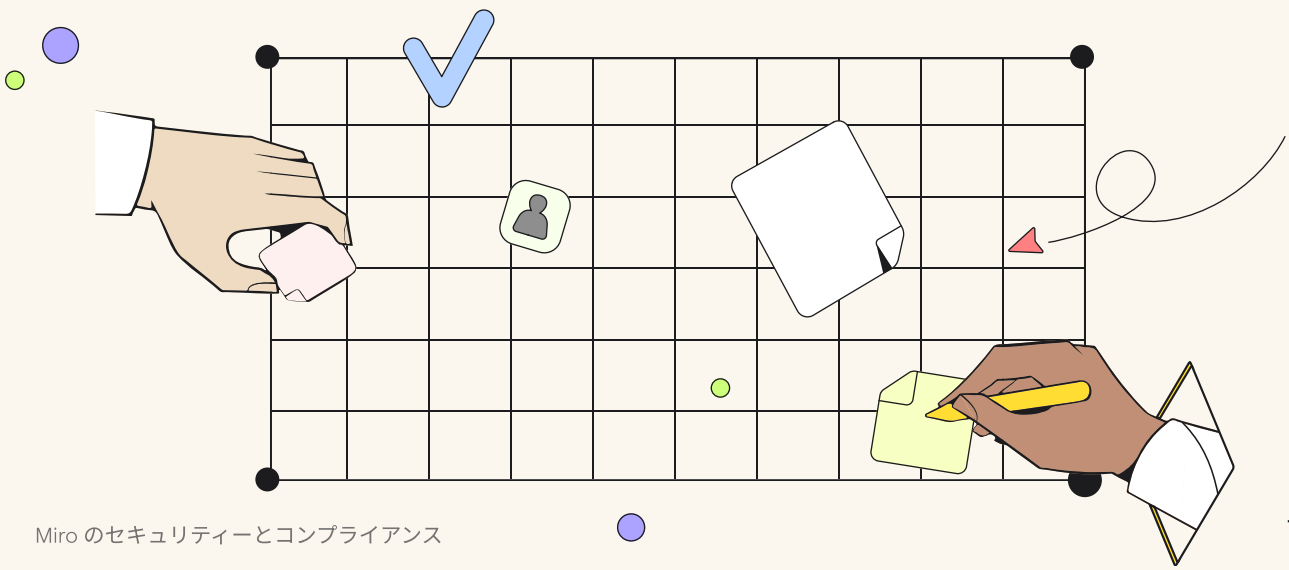
- **Enterprise モビリティ マネジメント：**Microsoft Intune や VMware Workspace ONE などのエンタープライズ モビリティ管理（EMM）ツールのインテグレーションにより、企業または個人のデバイスから Miro へのアクセスを安全に管理、Android と iOS の両方に対応します。

- **監査ログ：**会社の管理者は、組織内のすべてのアクティビティーを表示できます。監査ログは、トラブルシューティングやグローバルなセキュリティー設定の変更、新しいユーザーの招待、新しいボードの作成など、重要なイベントの詳細なレポートが必要な場合に 役立ちます。

- **機密分類：**Enterprise プランのユーザーは、ボードのコンテンツに機密分類ラベルを割り当てて、機密性レベルを示すことができます。既定のラベルを会社レベルまたはチームレベルで構成できる他、ユーザーはダッシュボードからラベルによるボードの絞り込み検索ができます。

- **コンテンツのライフサイクル管理：**Miro を使用すれば、会社別に絞り込み、企業レベルでボードのライフサイクルを効率的に管理することができます。また、ごみ箱のグローバルメニューに簡単にアクセスでき、ボードの復元や完全な削除ができます。

- **管理：**自動化は、何十万ものボードやユーザーを管理する際の時間を節約し、また、エラーを防止する上で重要な役割を果たします。SCIM または JIT プロビジョニングを活用することで、ユーザーのアクセスの自動化と、ライフサイクル管理の合理化が可能になります。



人工知能

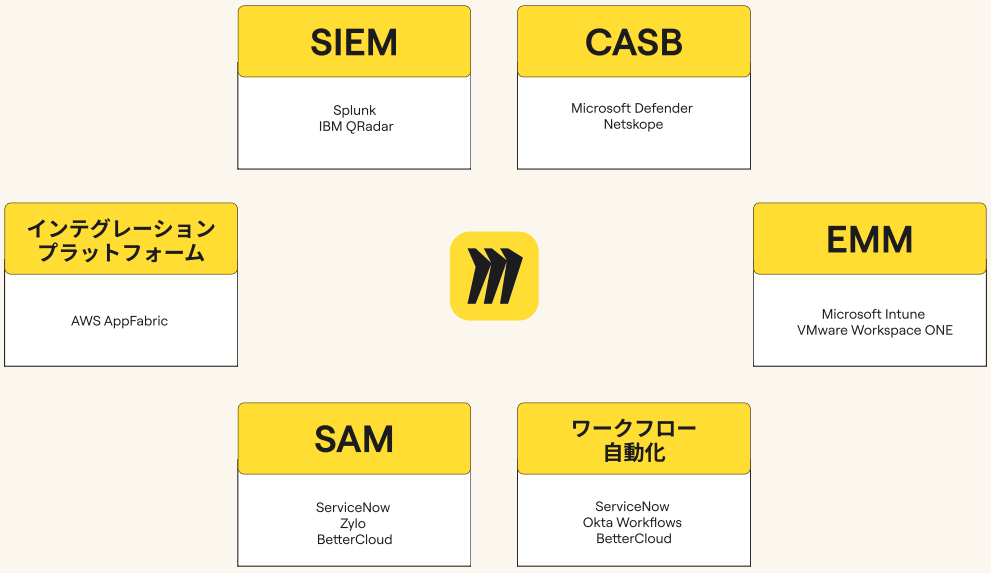
Miro の AI は、セキュリティーに関してその他の製品と同じ配慮と注意を払って扱われています。AI に関する当社の指針と原則に関するガイドでは、倫理的で責任ある AI 開発へのコミットメントを示しており、これは、お客様、ユーザー、パートナー各社との信頼を維持するためのものです。

またこれには、透明性の高い AI モデルによる説明責任も伴います。当社はデータを、当社のプライバシーポリシーに概説した方法、または Miro とお客様の間で明示的に合意された方法でのみ使用し、お客様がそのコンテンツを完全に制御しています。また、お客様はオプトインまたはオプトアウトによる AI サービスの制御もできます。詳しくはホワイトペーパーを参照してください

Enterprise エコシステムのインテグレーション

Enterprise プランのお客様は、SIEM ソリューション、CASB（クラウドアクセス セキュリティー ブローカー）、EMM、インテグレーション プラットフォーム、SAM（ソフトウェア資産管理）ツール、ワークフローの自動化など、様々なセキュリティーおよびコンプライアンス関連のインテグレーションを使用できます。企業が独自のカスタム インテグレーションを開発することも可能です

エンタープライズグレードの各種インテグレーション



miro | ENTERPRISE GUARD

Miro Enterprise Guard：高度なデータセキュリティーおよびガバナンスのアドオン

Miro での作業は戦略的な内容を含むことが多く、ガバナンスが必要となります。Miroを使用して機密データや専有データを作成、保存するお客様が増えており、機密データは会社のポリシーとは関係なしに予期せぬ場所で共有される可能性があります。これに加え、Miro のボードのコンテンツ量は、最大手のお客様において年間 2.5 倍の割合で増加しており、データセキュリティーとガバナンス関連のリスクはさらに高まっています。

認証や SSO など、SaaS アプリケーションに対する中核となるエンタープライズ グレードのセキュリティー機能や、きめ細かなアクセス制御など、データを保護するタイミングや方法についてほとんどのお客様に充分な制御を提供しています。しかし中には、Miro の自社事業にとっての戦略性と、業界の規制コンプライアンス要件、またはその両方のために、標準のセキュリティー対策に加えて追加の保護を求める企業もあります。

そこでご紹介したいのが、高度なデータセキュリティーとガバナンスのアドオンである Miro Enterprise Guard です。

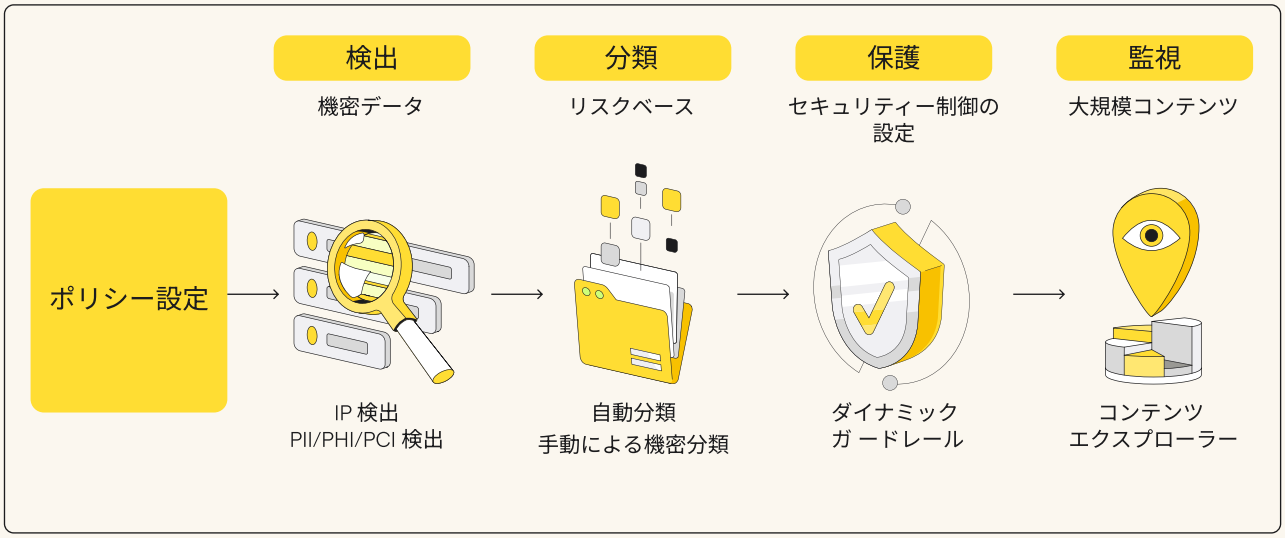
[1] 2017 年から 2023 年までの従業員数 1,000 人以上の法人企業におけるボードの累積成長率

機密性の高いデータの検出、分類、保護

Enterprise Guard は、Miro 全体で機密データの識別と分類のプロセスを自動化し、データセキュリティー制御を支えます。Miro Enterprise Guard では次のことが可能です。

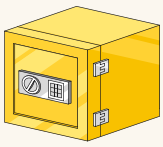
- Miro のボードをスキャンし、PII、PCI、PHI、ビジネスクリティカルな情報などの機密データを特定して分類し、保持、削除、修復の判断をサポートします。
- Miro または他のデータセキュリティー ツールのインテグレーションにより設定できる、事前に定義された条件に基づいて、検知されたデータに**分類ラベルを自動的に**適用します。
- ボードの機密分類ラベルに基づいて**インテリジェント ガードレール**を適用します。インテリジェント ガードレールは、ポリシーに従って設定する動的制御であり、コピー、貼り付け、公開共有、ボードのエクスポートなどのユーザーによる特定の操作を防止できます。
- **コンテンツ エクスプローラー**では、機密性の高いコンテンツを含むすべての Miro ボードおよび各ボードの分類ラベルを、一か所で表示することもできます。組織全体のコラボレーションを支えつつ、保護する必要があるデータに対して可視性を高めることで、その正確な制御が可能になります。

セキュリティーをリスクに適応させる

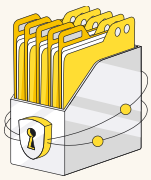


コンテンツのライフサイクルを大規模に管理

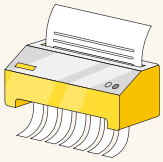
Enterprise Guard は、ボードのライフサイクル管理プロセスを自動化し、コンプライアンスまたは会社の規定要件への準拠を支えます。
この機能を使用すると、以下の項目が可能になります。



完全な監査証跡が付随した、ポリシーに従ったボードの保持



完全な監査証跡が付随した、ポリシーに従ったボードの削除



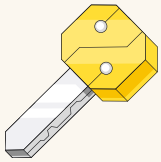
組織レベルで廃棄ポリシーを定義し、Miro ボードの防御的な永久削除および保持について制御を強化

鍵管理

また、Enterprise Guard アドオンバンドルの一環として、暗号鍵管理（EKM）を有効にすることができ、AWS KMS を利用して暗号化キーを完全かつ独立して制御できます。

さらに、監査の可視性が向上し、アカウント名、プロジェクト名、ユーザー生成コンテンツ（ウィジェット、コメント、アップロードされたファイルなど）といったデータに対するアクセス制御が強化されます。

さらに、ユーザーが独自の鍵を持ち込む（BYOK）際に、すべての API コールのログにアクセスして鍵の使用履歴を確認することができ、コンプライアンスや規制条件への準拠を支えます。



暗号鍵管理（EKM）

まとめ

多くの経営幹部は、会社のイノベーションと競争力が不十分であると感じており、実際のところ 82% のビジネスリーダーが、革新的な事業への早期取り組み無しでは、企業は 5 年以内に衰退するだろうと予想しています。イノベーションを阻む最大の要因の一つは、時代遅れになった旧式のツールなどといった、技術的な課題です。経営層も一般社員も、旧型のテクノロジーが創造性を抑圧し、生産性を阻害すると感じています。多くの組織が、セキュリティーへの影響を十分に考慮せずに、共同作業ツールの実装を急いでいるのはそのためです。

Miro のようなビジュアル コラボレーション ワークスペースを使えば、イノベーションを簡単かつ安全に行うことができます。当社は、情報という最も価値のある資産を託してくださっているユーザーの皆様のセキュリティー確保に真摯に取り組んでおり、Fortune 100 社の 99% を含め、世界で 6,000 万以上のユーザーにご利用いただいています。著名企業も導入済みの、共同作業とイノベーションを可能にするワークスペースをご利用ください。当社の信頼のシステムで、データの安全性の確かさを実感いただけると思います。

詳しくは、営業担当者までお問い合わせください。

参考リソース

Miro トラストセンター
暗号化に関するホワイトペーパー
Miro のデータレジデンシー
セキュリティーとコンプライアンスに関するよくある質問（ヘルプセンター）
透明性に関する年次報告書
プライバシーポリシー
サービス利用規約
Miro Enterprise
アクセシビリティー ガイドライン

Miro はイノベーションのためのビジュアルワークスペースとして、物理的に異なる場所で作業する分散型チームの未来に、大きな飛躍のチャンスをもたらします。参加者の心を惹きつけるワークショップや会議の企画実行、製品のデザイン、さまざまなアイデアのブレインストーミング他、Miro の無限大のキャンバスがあらゆるタスクをサポートします。サンフランシスコとアムステルダムの 2 都市に共同本社を置き、Fortune 誌が選ぶ 100 企業の 99% を含め、世界中 6 千万人以上のユーザーに愛用されています。Miro は 2011 年に創業し、現在世界各国に 12 拠点、1,800 人以上の従業員を抱えるグローバル企業です。

miro

さらに詳しい情報は miro.com をご覧ください。

Miro Enterprise プラン
https://miro.com/ja/enterprise/

Miroブログ
https://miro.com/ja/blog/articles/

LinkedIn
https://www.linkedin.com/company/mirohq/

X（旧 Twitter）
https://twitter.com/MiroHQ