



Google Workspace

組織を保護する Google Workspace の仕組み

新しい働き方で情報を保護しながら安全
につながり、つくり、協力しましょう。



目次

概要	3
働き方の根本的な変化	4
従来型のツールがセキュリティリスクを高める理由	5
最新の脅威の状況に対応するよう設計された Workspace	6
Google AI を活用してスパム、フィッシング、マルウェアを検出、防止	8
場所を問わず、より安全な働き方を実現	9
コンプライアンスの遵守とデジタル主権の確立	13
生成 AI 時代におけるデータのプライバシー保護	16
Gemini for Workspace で導入されているプライバシーとセキュリティの 管理機能	17
Workspace のセキュリティと主権に関するお客様の声	20
働き方を改革して、安全に従業員の潜在能力をすべて引き出す	21



概要

Google Workspace は昨今の脅威の状況を念頭に置いて設計された、世界中で利用されている最も安全なクラウドネイティブのコミュニケーションおよびコラボレーション スイートです。Workspace を使用すると、組織はシック デスクトップ アプリにパッチを適用することも、エンドユーザーのデバイスに保存されたローカル ファイルの損失を心配することも、インフラストラクチャを安全かつ最新の状態に保つ必要もなくなります。このことは、IT およびセキュリティ チームのセキュリティ リスク、コスト、ワークロードの軽減につながります。

主なポイント:

 **従来型のツールでは、組織がセキュリティ上の脅威に対して脆弱なままである:** 従来型のコラボレーション ツールはオンプレミスのインフラストラクチャとソフトウェアのパッチ適用に依存しているため、ハッカーの標的になることが増えています。

 **Google Workspace は構造的により安全:** Google Workspace はクラウドベースで、あらゆるブラウザおよびモバイルアプリで動作し、自動的に更新されるため、脆弱性やデータ侵害の影響を受けにくくなっています。また、AI による脅威の検出、ゼロトラストのアクセス制御、強力なアカウント保護などの高度なセキュリティ機能も提供しています。

 **Google Workspace は、厳格度の高い基準の認定を受けている:** FedRAMP High、DoD IL4、HIPAA、GDPR をはじめとしたさまざまなコンプライアンス要件に対応し、デジタル主権に関しては追加の管理機能を利用できます。

 **Gemini for Workspace を使えば、データのプライバシーを保護しながら生産性を向上させることが可能:** Gemini for Workspace を使用してメールを要約する際も、会議でメモをとったり、ブログ投稿を作成したり、スライドに独自の画像を追加したりする際も、データはお客様のものであり、お客様の管理下にあります。つまり Gemini for Workspace では、お客様のコンテンツはお客様からのプロンプトに対してより有用な回答を提供するためにのみ使用され、Gemini for Workspace などの生成 AI モデルのトレーニングまたは改善のためには使用されません。

主なメリット:

- ✓ 脅威を未然に防止できる
- ✓ 場所やデバイスを問わず、組織でより安全に業務を行える
- ✓ 規制を遵守し、データ主権を維持できる
- ✓ データのプライバシーを守り、自分の管理下に置きながら、時間を節約し、創造性を高めることができる

働き方の根本的な変化

生成 AI を使うことで効率よく仕事を進められます。組織とユーザーは、これまで以上に機密性の高いデータや情報にアクセスしたり、作成、共有したりするようになりました。そうしたデータの多くは現在、世界中のどこからでも簡単にアクセスできるようにクラウドに保存されており、社内、社外はもちろん、現在では Gemini for Google Workspace などの生成 AI コラボレーターとも頻繁に共有されています。現代のこのような働き方と職場における生成 AI の急速な進歩には、メリットも多い反面、従来型のコラボレーションツールでは対処しきれない新たなセキュリティ上の課題も生じています。



従来型のツールがセキュリティリスクを高める理由

従来型のツールに対する攻撃の成功件数の増加

277
日

データ侵害を特定して封じ込めるまでに要する平均時間¹

948
万ドル

米国におけるデータ侵害の平均コスト。445 万ドルが世界平均¹

73
日

サードパーティ製ソフトウェアにパッチが適用されるまでの平均時間¹

従来型のツールは単純に現代のコラボレーションを想定した設計になっていません。ローカルのデスクトップソフトウェア、ローカル ファイル、オンプレミスのアイデンティティ ディレクトリを使い続けると、セキュリティリスクが高まります。それと同時に、IT チームは急速に量と巧妙さを増し続ける最新のサイバー攻撃への対応に苦慮しており、従業員の分散化、臨時従業員、ハイブリッドな勤務形態がそれをさらに困難にしています。

このような古いアプローチと脆弱性により、セキュリティリスクが増大し、顧客のコストが増加します。サイバー保険会社の Coalition は、40,000 人の顧客に基づいて独自の分析を実施し、Microsoft 365 でも Exchange でもなく Workspace を選択することで、以下のメリットが得られることを明らかにしました。

- Microsoft 365 でセキュリティに関する申し立てが発生する確率は、Google Workspace の **2 倍超**²
- Microsoft Exchange でセキュリティに関する申し立てが発生する確率は、Google Workspace の **約 3 倍**²
- Microsoft 365 または Exchange で振り込め詐欺 (FTF) もしくはビジネスメール詐欺 (BEC) に関する申し立てが発生する確率は、Google Workspace の **2.33 倍**²

最新の脅威の状況に対応するよう設計された Workspace

Workspace の設計は他と異なります。そして、その違いが重要です。Workspace は Google AI を活用した自動脅威防御を備えるクラウドネイティブ サービスとして、最新の脅威の状況に対応するように設計されています。民間企業、教育機関、政府機関における有害なコンテンツからの防御、アカウント乗っ取りの回避、脅威の特定、優先順位付け、対応を支援します。

Google は現代のコラボレーションを念頭に構築されたゼロトラストのセキュリティ モデルを通じて、あらゆる規模の企業の安全性を高めます。従来型の手法では、データセキュリティとプライバシーの要件を満たすために別のクラウドで多くの時間とコストをかける必要があります。一方、Workspace は単一のクラウドであり、最新の生産性機能とセキュリティ機能で常に最新の状態に保たれます。Google の多層防御インフラストラクチャは、セキュリティに関するトップクラスの専門家によって、数十年にわたる学習とセキュリティのベスト プラクティスを通じて開発されました。



脅威を防止

組織とそのデータを保護するために、ログインの保護対策と管理機能を実装して標的型攻撃を防ぎ、フィッシング、マルウェア、ソーシャル エンジニアリング詐欺によるアカウントの乗っ取りを防止します。



場所を問わず、より安全な働き方を実現

組み込みの管理機能とゼロトラスト アプローチにより、機密データへの最小権限アクセスが適切な条件下で適切なユーザーに許可されるため、従業員はどこからでも、どのデバイスでも安全に作業できます。



デジタル主権の確立とコンプライアンスの遵守

主権と管理の包括的な機能一式により、クラウド プロバイダによるデータへのアクセスを可視化し、コンプライアンスと規制の要件を満たします。



生成 AI 時代におけるデータのプライバシー保護

Gemini for Workspace では、お客様のプロンプトに対してより有用な回答を提供するためにのみお客様のコンテンツが使用されます。お客様の許可なく Gemini for Workspace およびその他の生成 AI モデルのトレーニングまたは改善のために使用されることはありません。

このセキュリティに対するアプローチは、現代の幅広いサイバー脅威からお客様を保護してきた非常に確かな実績によって裏付けられています。

0

Google Workspace における
過去 3 年間の共通脆弱性識
別子 (CVE) の数³

0

SolarWinds 事件の影響を受け
た Google システムの数⁴

0

高度な保護機能プログラムに登録さ
れているアカウントに対するフィッシン
グ攻撃が成功した事例の数⁵

Workspace をご利用のお客様には、技術と財務の両面でメリットがあります。このことは、保険会社の At-Bay が顧客から提出された保険金請求件数に基づいて実施した独自の分析によって証明されています。

- Workspace を利用する組織は、セキュリティ インシデントの発生件数が Microsoft 365 を利用する組織よりも **50%** 少ない⁶。
- Workspace を利用する組織は、メール関連のセキュリティ インシデントの発生件数が Microsoft Exchange を利用する組織よりも **62%** 少ない⁶。
- Workspace を使用することで、サイバー セキュリティ保険料を **50%** 節約できる可能性がある⁶。



セキュリティリスクを 下げながらコストを削減

Google は、Workspace に移行した企業はメリットとコスト削減をどのように実感できるかについて、[Forrester Total Economic Impact™](#)⁷の調査を委託しました。その結果、収益増加、従業員の効率性向上、リスク軽減、IT サポート サービスという、目に見える 4 つのメリットが確認されました。

Workspace によるセキュリティの強化により、組織がセキュリティ ツールにかかるコストが 3 年間で平均 **180 万ドル**節約されることが明らかになりました。

Google AI を活用してスパム、フィッシング、マルウェアを検出、防止

Workspace には AI を活用したセキュリティ機能のメリットがあるため、マルウェアやスパムを見落とす心配を最小限に抑えることができます。頻繁に確認される新しい脆弱性を修正するのに、費用のかかるアドオンは不要です。

Gmail の AI を活用した防御機能は、日々次のような成果をあげています。

- スパム、フィッシング、マルウェアの **99.9% 以上を、受信トレイに届かないようにブロック**
- **約 150 億通の迷惑メールをブロック**
- **1 億件超のフィッシング攻撃をブロック**

アカウントの乗っ取りを防いで組織を保護

Google はあらゆる場所、あらゆるデバイスでユーザーとデータを保護します。



ログインの保護対策と管理機能を実装

ログインの保護対策と管理機能により、標的型攻撃から防御し、アカウントの乗っ取りを防ぎます



パスワードレスのログインへ移行

パスワードよりも簡単かつ安全な認証方法である**パスキー**を実装します



標的型攻撃を受けるリスクが高いアカウントに、追加の安全保護対策を提供

管理者またはビジネス リーダーを Google の**高度な保護機能プログラム**に登録します

場所を問わず、より安全な働き方を実現

ゼロトラスト セキュリティ モデルは、分散型ワークに伴うセキュリティ リスクを軽減するために欠かせない存在になりました。Workspace は最初からこのモデルを念頭に置き、そのクラウド専用アーキテクチャと Google 独自の [BeyondCorp の実装](#) から学んだことを加味して構築されました。

従来の生産性向上ソリューションは、デスクトップ アプリ (通常はパッチの適用が必要)、エンドユーザーのデバイスに保存されているローカル ファイル (機密データが危機にさらされる可能性がある)、および脆弱な企業ネットワークや VPN に依存していることがよくあります。

そこで Workspace では、ブラウザおよびモバイルアプリで直接利用できるようにする、データをクラウドに保存する、ゼロトラスト制御を使用して適切な状況下で適切なユーザーだけがデータにアクセスできるようにするといった、異なるアプローチを採用しました。

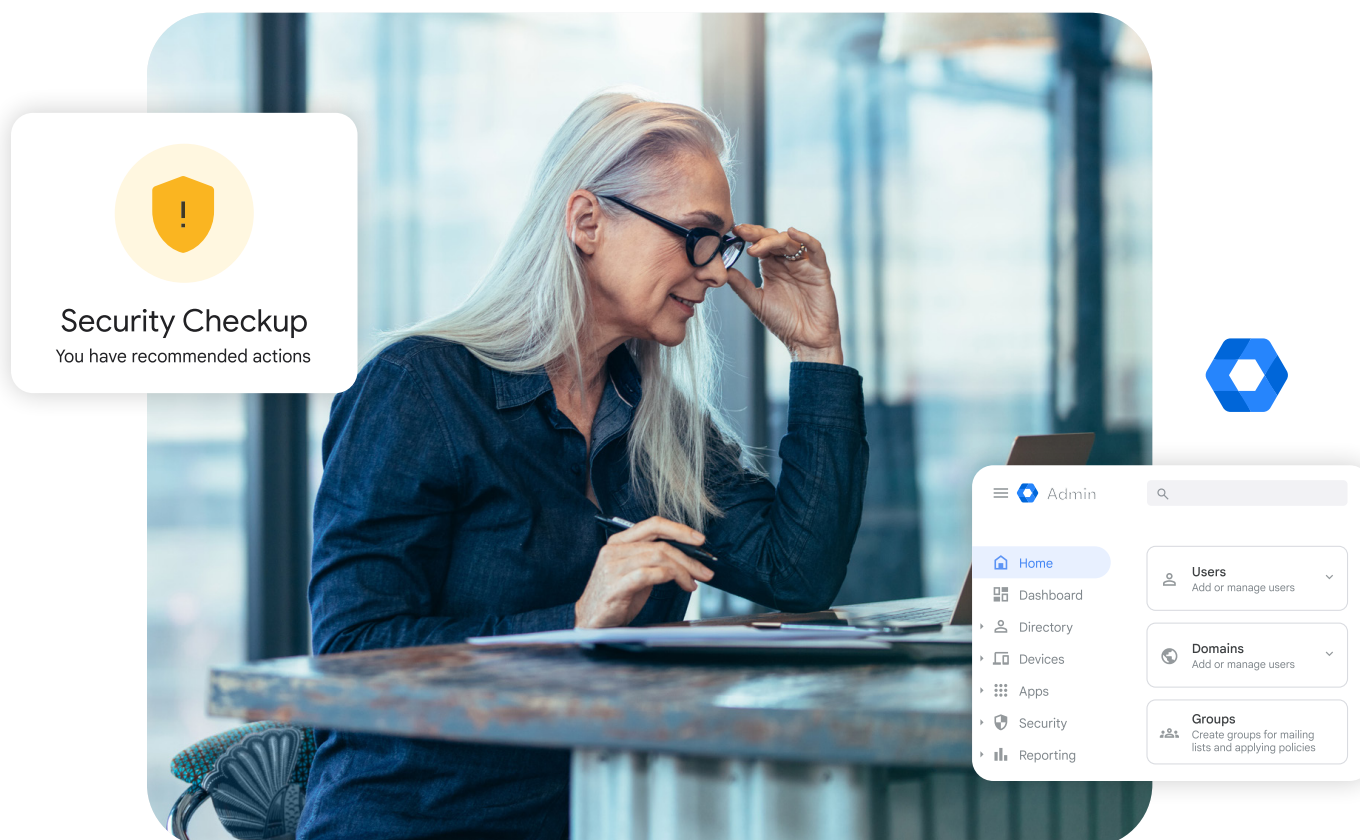
Workspace は、その最新のアーキテクチャとセキュリティ制御機能により、以下の取り組みをとおり、組織がゼロトラストの導入を加速し、[CISA の Zero Trust Maturity Model](#) などの業界フレームワークに適合できるようにしています。

- コンテキストに応じたアクセスの適用とゼロトラスト制御
- ユーザーが正しい行動を取るように誘導
- デバイスや場所をほぼ問わずに会社のデータを保護



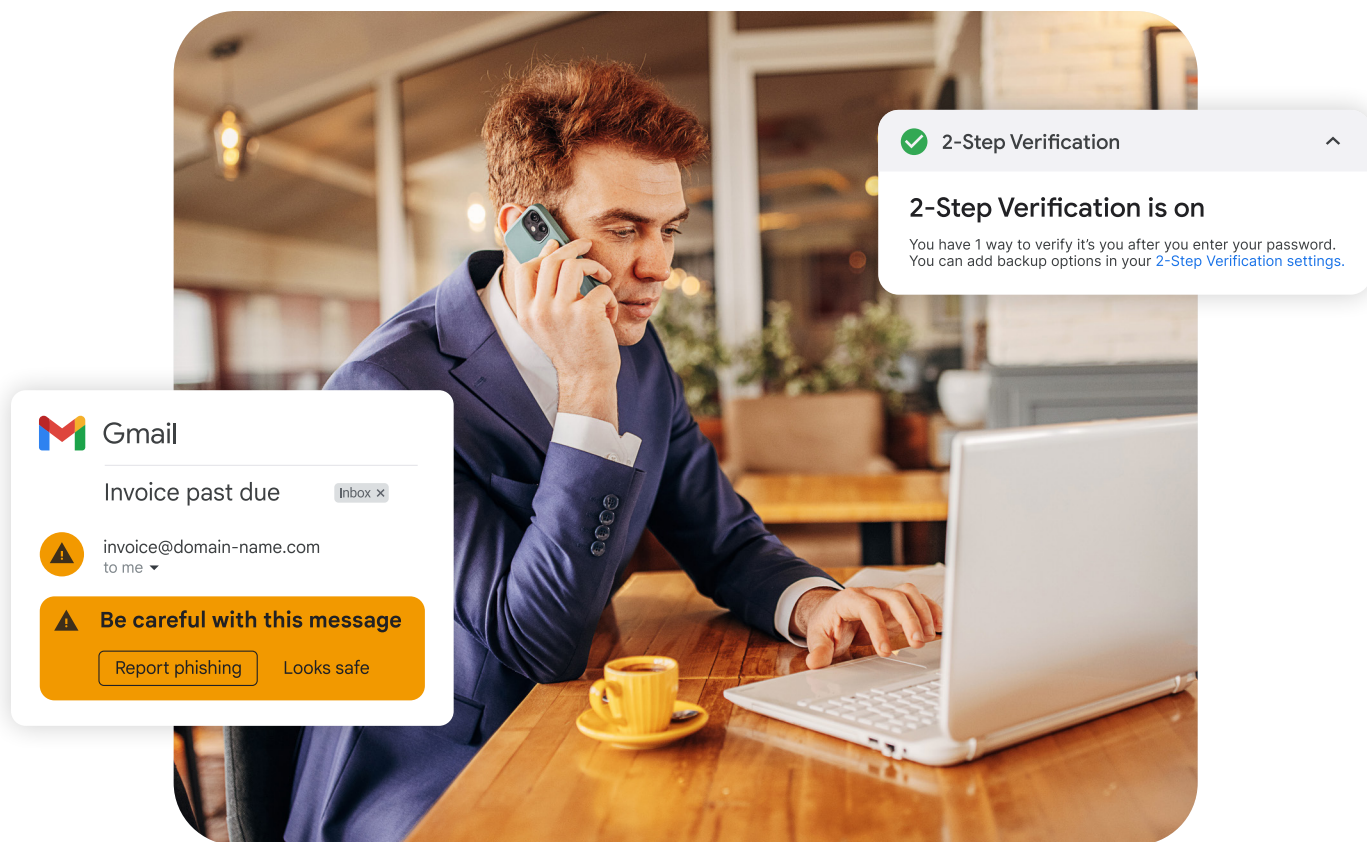
コンテキストに応じたアクセスの適用とゼロトラスト制御

他の生産性向上ツールおよびコラボレーション ツールのプロバイダは、社内ネットワークにアクセスできるユーザーはすべて正当なユーザーであると想定しています。一方、Workspace は、リクエストのコンテキストを継続的に検証して、機密情報への不正アクセスを防ぎます。管理者は、デバイスの場所やセキュリティステータスなどの属性に基づいて詳細なコンテキストアウェア アクセス ポリシーを作成して、Workspace アプリおよび API へのユーザー アクセスを制御できます。また、アクセス ポリシーをデプロイする前にモニターモードを使用してその影響を把握し、作業の中断を計画して最小限に抑えることも可能です。管理者は、Workspace アプリと API に対するデータアクセスと保護管理機能を、BeyondCorp Enterprise を使用して Chrome 経由でアクセスされるその他のアプリにも拡張して、防御を強化し、リスクを軽減できます。



ユーザーが正しい行動を取るように誘導

昨今、データ共有ポリシーを認識している従業員とそうでない従業員の間には大きな隔たりがあります。管理者は、組織に合ったデータ損失防止 (DLP) ポリシーを作成して、機密情報を検出し、組織内外での共有を制御できます。また、データ損失防止 (DLP) ポリシーとコンテキストアウェアアクセス ポリシーを組み合わせることでデータ損失に対する保護を強化し、エンドユーザーが機密性の高いコンテンツを共有する前に特定の基準を満たしていることを確認することも可能です。安全性をより一層強化するために、管理者は Google AI を活用してデータを継続的に分類し、データの適切な共有とデータ漏洩から保護を確実にすることができます。



デバイスや場所をほぼ問わずにデータを保護

Google Workspace はハイブリッド環境で安全なコラボレーションを実現できるように設計されているため、管理者は Android、ChromeOS、iOS、Windows など、ほぼすべての種類のデバイスで会社のデータを保護できます。これにより、従業員が所有するデバイス (BYOD)、企業から支給されたデバイス、第三者が管理するデバイスなどのさまざまなシナリオが可能になります。データはクラウドに存在するため、管理者は、デバイスからのデータアクセスの承認、ブロック、削除や、紛失または盗難にあったデバイスのデータの消去を、1 か所から最小限の労力で行うことができます。管理者は、統合エンドポイント管理およびモバイル上の脅威からの保護対策のために、専用のサードパーティ製デバイス管理ソリューションと統合することもできます。

≡  Admin

 Home

 Dashboard

▸  Security



コンプライアンスの遵守と デジタル主権の確立

世界中でデータの規制が厳しくなっています。[Gartner \(2022 年\)](#) は、2024 年末までに世界人口の 75% がプライバシーに関する最新の規則の対象となる個人データを所有すると推定しています。Workspace を使用するとデータを制御し、プライバシーを保護することができるため、データ主権とコンプライアンスを維持できます。

Google はお客様から、コンプライアンスを維持するために組織はデータに対して次の 3 つの目標を掲げている、と聞いています。

- 1 データへのローカル アクセスの確保
- 2 海外からのデータアクセスの防止
- 3 データの永続的なセキュリティとプライバシー

従来型のクラウド プロバイダは国内を所在地とするデータに重点を置っていますが、データは非常に多くの境界、ネットワーク、プロバイダを超えて存在するため、これだけでは上記の目標を達成するには不十分です。これらの目標を達成するには、デジタル主権とセキュリティを根本から組み込んだ総合的なアプローチが必要です。これこそが、データの所在地を問わずに企業のデジタル主権に関する取り組みをサポートする Workspace の真価であると Google は確信しています。

-  Google はお客様に柔軟なオプションをご提供します。お客様のデータは米国または EU で保存および処理できます。より高度な制御が必要な場合は、ローカル データストレージを使用して特定の国にデータを保存できます。
-  お客様のデータにアクセスしないことを契約により保証するとともに、Google および外国政府機関がお客様のデータにアクセスできないようにするための技術的機能（クライアントサイド暗号化など）も提供するクラウド プロバイダは、現在のところ Google だけです。
-  コンプライアンスを維持するには、損失と侵害行為を防ぐためのセキュリティ基盤を構築する必要があります。

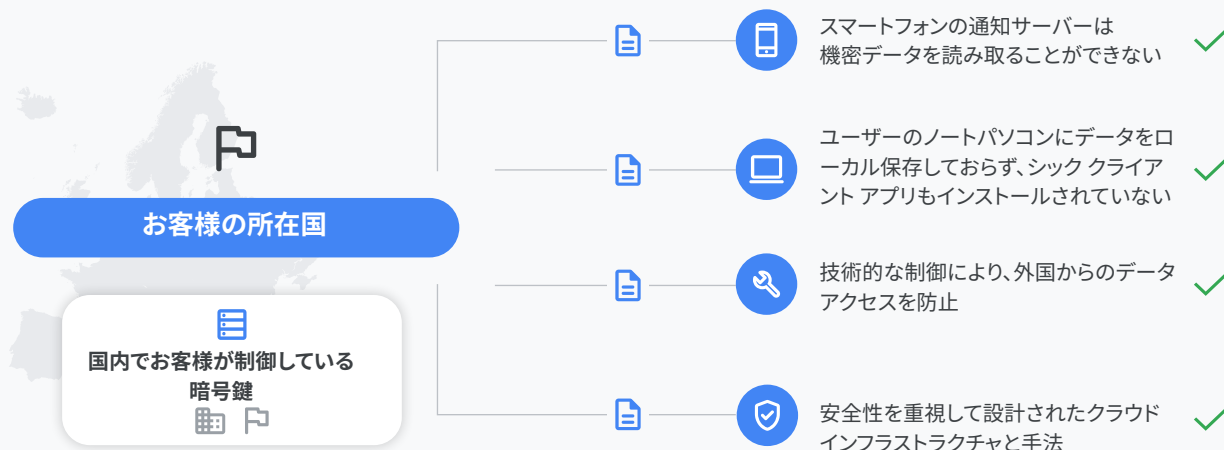
Workspace は主権とコンプライアンスに対するまったく新しいアプローチを提供し、その他の従来型プロバイダの構造的なセキュリティリスクを解決します。

 **ファイルのローカル保存に起因するデータ損失:** Workspace ではデータはクラウドに保存されます。つまり、ユーザーのデバイスには保存されないということです。データがクラウドに保存されることで、ユーザーからのリクエストごとにデータへのアクセスが確認され、データへのアクセスをすぐに取り消すことができます。また、エンドユーザーのデバイスで特別なエージェントを利用することなく、効果的な DLP、IRM、ゼロトラスト アクセス制御を適用することもできます。単純に聞こえるかもしれませんが、データがクラウドに保存されることにより、ファイルが何千台ものエンドユーザー デバイスに分かれて保存されている状態よりも、はるかに簡単にデータを管理、保護できます。

 **脆弱性に起因するデータ侵害:** Workspace では、パッチ適用または脆弱性対策が必要なシック クライアント アプリは使用されません。どの Workspace アプリにも Chrome などのブラウザからアクセスできます。この攻撃対象領域についても、心配する必要はありません。

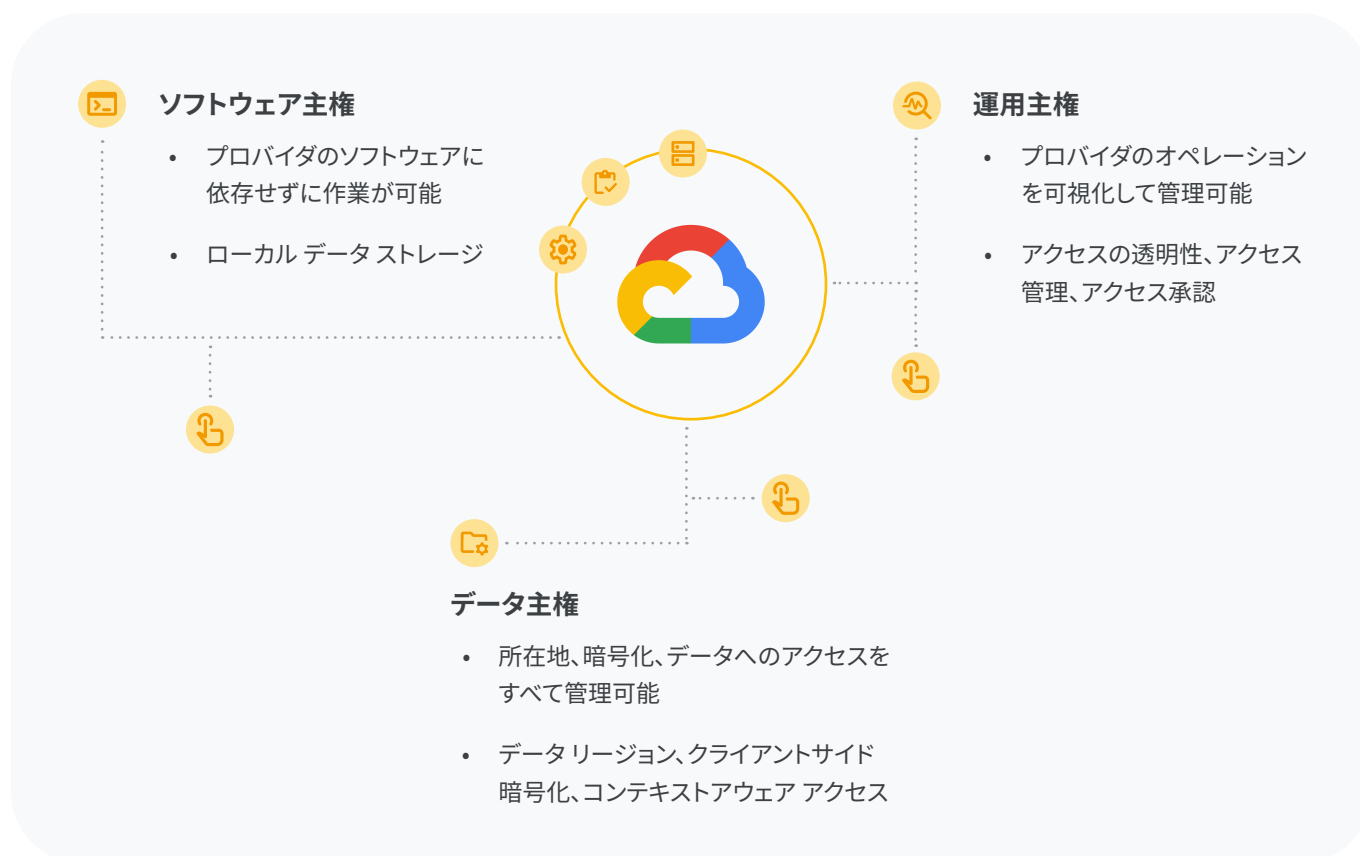
 **海外からのデータアクセス:** Workspace の Assured Controls とクライアントサイド暗号化により、データを完全に管理できます。クライアントサイド暗号化を使用することで、暗号鍵を Workspace の外部で任意の国に保存できるため、Google 社員および外国政府の法執行機関がデータを読み取れないようにできます。

 **脆弱性に起因するオンプレミスの侵害:** Google Workspace はオンプレミスのインフラストラクチャを必要としないため、オンプレミスのインフラストラクチャが攻撃にさらされる心配はありません。



世界中のお客様と政府機関にとって、コンプライアンスだけでなくデジタル主権も最優先のテーマです。Google は、新たな規制要件のニーズに応える、包括的な Workspace 向け主権管理を開発しました。Workspace におけるデータ主権の 3 つの柱は次のとおりです。

-  **ソフトウェア主権。**お客様は、クラウド プロバイダのソフトウェアに依存しなくてもすむように、国内にデータのコピーを保持することができます。
-  **データ主権。**お客様は、データの保存場所を選択し、データへのアクセス方法を完全に管理することができます。
-  **運用主権。**Google のサポート担当者がトラブルシューティングの目的にデータにアクセスする際に、お客様はいつ、どこから、どのような方法でのアクセスを許可するかを管理できます。



生成 AI 時代におけるデータのプライバシー保護

Google Cloud と Workspace は、ユーザーデータを保護しプライバシーを優先する方法についてまとめた、堅牢な[プライバシーに対するコミットメント](#)を長年にわたって共有してきました。生成 AI によってこうしたコミットメントが変わることはなく、むしろその重要性が再認識されています。生成 AI は、ユーザーが自らデータの選択と管理を行えるようにするための、Google の基本的なプライバシー保護の取り組みを変えるものではありません。それを明らかにするために、Workspace データの取り扱い方法に関する重要なポイントを以下に示します。

- ✓ **お客様のデータはお客様のものです。**お客様が Workspace サービスに保存するコンテンツ（メール、ドキュメントなど）は、あくまでお客様のものです。Google がお客様のデータを販売することは決してなく、お客様のコンテンツはお客様ご自身で削除やエクスポートが可能です。
- ✓ **お客様のデータは Workspace にとどまります。**Google がお客様の Workspace データを許可なく使用して、Workspace の外部にある Gemini、検索、Vertex、その他のシステムの動作基盤となっている生成 AI および大規模言語モデルのトレーニングまたは改善を行うことはありません。
- ✓ **お客様のプライバシーは保護されます。**スペル候補の受け入れまたは拒否、スパムの報告など、インテリジェントな Workspace 機能とのやり取りは匿名化または集約（あるいはその両方）され、スパムからの保護、スペルチェック、オートコンプリートなどの便利な Workspace 機能の改善または開発に使用される場合があります。これは、現在開発中の新機能にも適用されます（Workspace ユーザーが Gemini for Workspace 機能から最適な結果を得るのに役立つプロンプト候補の改善など）。これらの機能は、ユーザーが管理できるように、厳格な[プライバシー保護](#)とともに開発されています（法人のお客様向けのプライバシー、セキュリティ、コンプライアンスに関するその他のコミットメントの詳細については、以下をご覧ください）。
- ✓ **お客様のコンテンツが広告のターゲット設定に使用されることはありません。**Google が広告を目的として Workspace サービスでお客様のコンテンツを収集、スキャン、使用することはありません。

これらは Workspace のすべてのユーザーを対象とするプライバシーに対するコミットメントです。このことを言葉で宣言するだけでなく、こうした高い基準を継続的に満たすために、Google では、独立監査機関による国際基準とベスト プラクティスに照らし合わせた検証を受けています。

Gemini for Workspace で導入されている プライバシーとセキュリティの管理機能

Workspace をビジネスでご利用のお客様が [Gemini for Google Workspace Enterprise](#) を導入されると、それまでと同じ堅牢なデータ保護およびセキュリティ基準を満たしたあらゆる Workspace サービスをご利用いただけるのに加え、企業、教育機関、政府機関のお客様向けに次のような固有の保護対策が提供されます。

- ✓ **Gemini とのやり取りが組織外に開示されることはありません。**Gemini は、あらゆるプロンプトおよび生成物を Workspace のコンテンツと一緒に保存します。それらを組織外に共有することはありません。
- ✓ **既存の Workspace の保護が自動的に適用されます。**Gemini では他の Workspace サービスと同じエンタープライズグレードのセキュリティが提供され、データ リージョン ポリシーやデータ損失防止 (DLP) などの組織の既存の制御とデータの取り扱いの規定が自動的に適用されます。
- ✓ **お客様のコンテンツが他のお客様のために使用されることはありません。**お客様のコンテンツが許可なくお客様のドメイン外でモデルのトレーニングに使用されることはありません。



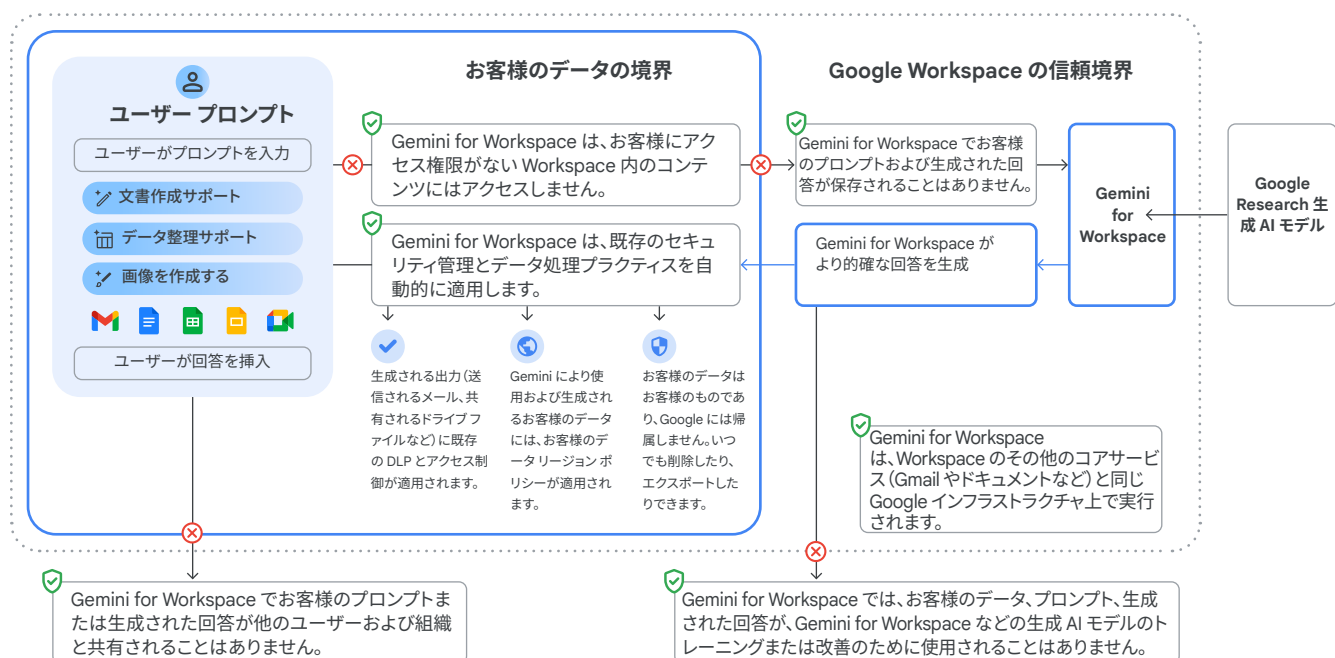
Gemini for Workspace が 信頼境界から逸脱しない仕組み

ユーザーからプロンプトが発行されると、Gemini for Workspace はユーザーにアクセスが許可されているドキュメントと情報のみを使用します。これは、プロンプトを根拠にし、より有用で状況に応じた結果を生成するためです。Gemini for Workspace では、お客様のデータ、プロンプト、生成された回答が、Gemini for Workspace などの生成 AI モデルのトレーニングまたは改善のために使用されることはありません。

Gemini for Workspace は、Workspace のその他のコアサービス (Gmail やドキュメントなど) と同じ Google インフラストラクチャ上で実行され、Workspace の既存のセキュリティ管理機能がすべて自動的に適用されます。これにより、お客様のデータとやり取りが組織外に流出するのを防ぎ、コンプライアンスとデータストレージの要件に対処できます。実際、Google のコンプライアンス チームはすでに規制当局と協力して、Workspace の認証を Gemini for Workspace にも拡大するよう取り組んでいます。

また、いかなる状況においても、Gemini for Workspace ではお客様のデータまたはプロンプトが組織外に流出することはありません。Google は、お客様が急速に進化する規制環境に適応し、常に最新の状況を把握できるよう支援する強力な技術ソリューションを提供することに尽力しています。

Gemini for Workspace Enterprise のデータのプライバシーとガバナンス



Workspace が既存の自社製およびサードパーティ製のセキュリティツールとシームレスに連携する仕組み

-  Workspace プラットフォームに組み込まれている主要なセキュリティ機能や信頼機能はもちろん、Google およびパートナーのセキュリティ サービスとも機能連携して、お客様の防御を強化し、リスクを軽減できるように支援します。
-  BeyondCorp Enterprise を使用すると、脅威対策とデータ保護を他の SaaS アプリケーションにまで拡張できます。Workspace の DLP とコンテキストアウェア アクセスを実行するのと同じポリシーエンジンが BeyondCorp Enterprise も実行します。
-  アプリケーションのセキュリティ以外のセキュリティ上の課題については、数多くの自社製ツールおよびサードパーティ製ツールとの機能連携に対応しています (Chronicle、CrowdStrike、Palo Alto Networks、VMware、Okta、JumpCloud、Thales など)。
-  Google Workspace を BeyondCorp Enterprise やその他のセキュリティ サービスと組み合わせることで、従業員のセキュリティをさらに強化するために必要なものがほぼすべて揃います。



Workspace のセキュリティと主権に関するお客様の声

「クラウド コラボレーションの機能を利用することで、大陸を越えてシームレスで安全な接続を行うことができ、同僚間の言語障壁を地球規模でなくすることができます。時間や場所を問わずに業務を遂行する能力が強化されました。特にネットワークの機能停止時や自然災害の発生時に、安全にコミュニケーションと連携を行う能力が増しました。」

- **Peter Guo 氏**、米海軍横須賀基地艦船修理廠および日本地区造修統括本部 (SRF-JRMC) CIO (最高情報責任者)

「Google Workspace により、わずか数か月で地理的なサイロ化を解消し、職場をより安全かつ効率的でモバイルに対応したデジタルファーストの文化に変革することができました。Google Workspace のおかげで、私たちは COVID-19 (新型コロナウイルス感染症) がもたらした課題を優位性を持って克服することができ、パンデミック中も 50 か国以上で安全で中断のないカスタマー サービスを提供し続けられました。」

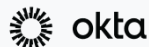
- **Gene Molloy 氏**、Iron Mountain、IT エンドユーザー テクノロジー担当バイス プレジデント

「私たちはかねてから、暗号化された通信がテクノロジープロバイダも含めた第三者にアクセスされないことを保証する機能を探してきました。Google は、機密データを完全に制御する機能の提供において、クライアントサイド暗号化によって独自の地位を築いているように見えます。クライアントサイド暗号化により、私たちは絶え間なく変化するデータ規制の世界で組織としてコンプライアンスを維持することができます。」

- **Shaun Bookham 氏**、PwC、英国オペレーションおよびテクノロジー担当ディレクター

「AI を活用して与信を変革するという私たちの使命には、強力なグローバル コラボレーションと強固なデータセキュリティが必要でした。成功を収めることができたのは、ひとえに Google Workspace のデータ損失防止 (DLP) ツールと生産性向上機能のおかげです。」

- **Rakesh Agrawal 氏**、Scienaptic、プロデュースおよびテクノロジー担当主任



働き方を改革して、安全に従業員の潜在能力をすべて引き出す

私たちの働き方はすでに大きく変化しています。これらの変化に、生成および保存される機密データの増加と、職場環境への生成 AI の普及率向上が重なって、セキュリティ上のリスクが高まっています。現在は世界中どこからでも簡単にアクセスできるように、こうしたデータの多くがクラウドに保存されます。そこからデータが社内外の関係者と共有され、それらの関係者がさらに再共有します。

これらはすべて従業員のコラボレーションと生産性向上にとって有効ですが、従来型のコラボレーション スイートではセキュリティリスクに対応できません。Workspace は徹底的にセキュリティを考慮して設計されています。

セキュリティ、プライバシー、コンプライアンスを重視した信頼できるコラボレーション スイート、[Workspace](#) をぜひお試しください。



¹ Cost of a Data Breach Report 2023, IBM, 2023 年

² Coalition - 「2023 Cyber Claims Report: Mid-year Update」, 2023 年 9 月

³ https://www.cvedetails.com/product-list/vendor_id-1224/Google.html

⁴ 「ソフトウェアのサプライ チェーン エコシステムを安全に再構築するための支援」、Google Cloud 公式ブログ、2021 年

⁵ Google 内部データ。Google の高度な保護機能プログラム

⁶ At-Bay - 「Ranking Email Security Solutions: A Data Analysis of Cyber Insurance Claims」2023 年 9 月

⁷ Forrester, The Total Economic Impact™ Of Google Workspace, 2023 年 12 月、Google の委託により Forrester Consulting が実施した調査