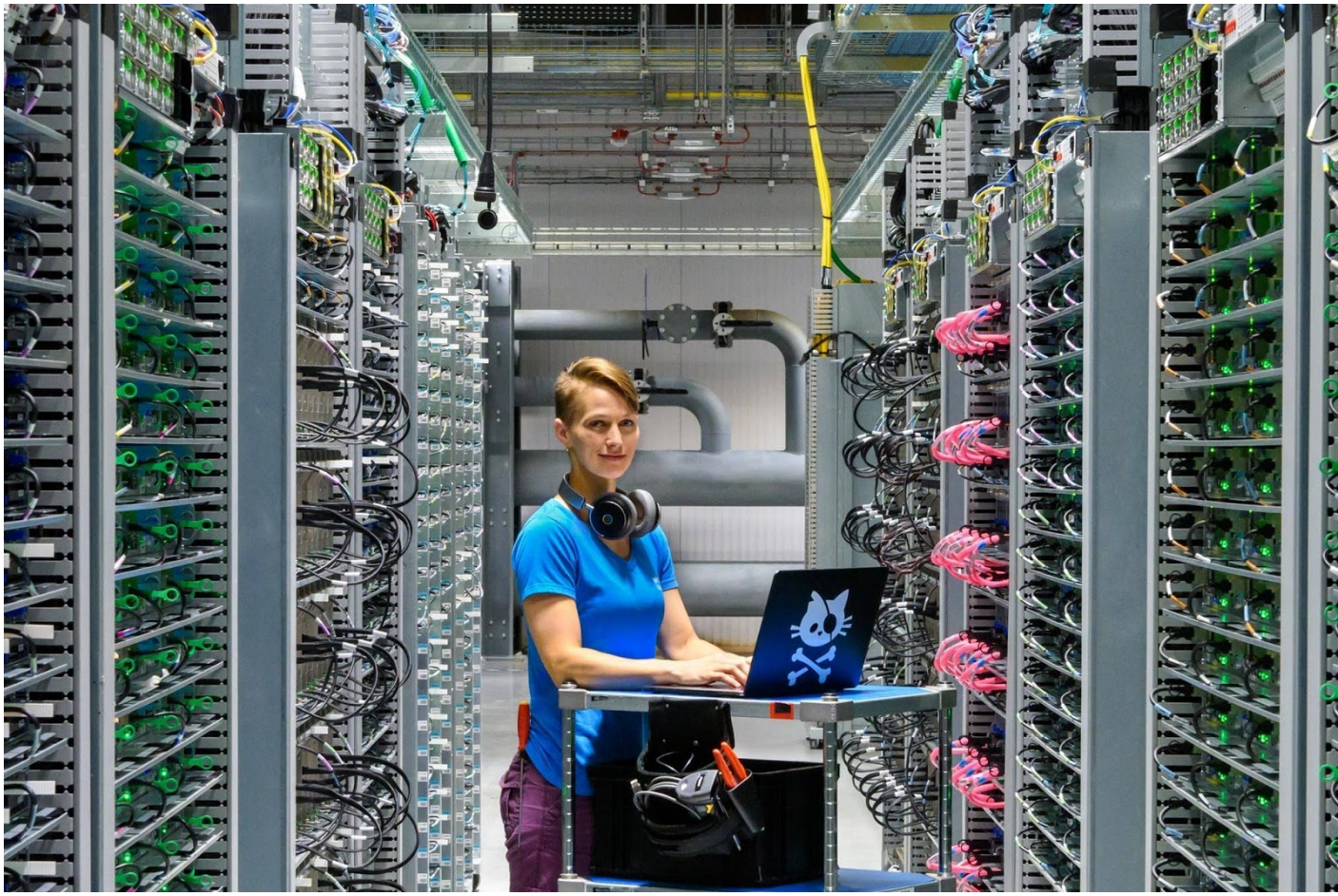
Google Cloud ホワイトペーパー
2020 年 10 月

Google Workspace セキュリティ ホワイトペーパー



Google Cloud

目次

はじめに

クラウド コンピューティングは、今日の企業のビジネス手法を変えました。組織は、インフラストラクチャ、運用、サービスの提供を管理するために主にパブリック クラウドに目を向けています。これは、プロバイダが人材とプロセスにより多くの投資を行うことで、安全性とコンプライアンスを満たすインフラストラクチャを提供できると認識しているからです。

Google は、クラウドのパイオニアとして、クラウドモデルのセキュリティが果たす意義を十分に理解しています。そのため、従来の多くのオンプレミス ソリューションよりも優れたセキュリティを提供するようにクラウド サービスを設計しました。Google は、セキュリティを優先して自社の業務を保護しています。すべてのお客様は同じ Google インフラストラクチャを活用していますから、それぞれの組織が Google のセキュリティによって保護されます。

Google の組織体制、研修の優先順位、雇用プロセスにおいても、セキュリティとデータ保護が重要視されています。Google のデータセンターの運用とテクノロジーはこの原則のもとに成り立っています。この原則はまた、脅威への対処方法を含め、日々の業務と災害計画の中核となっています。顧客データの取り扱い方においても、セキュリティとデータ保護は特に優先される要件です。さらに、Google のアカウント管理、コンプライアンス監査、お客様に提供する認定資格の基礎となっています。お客様のビジネスとデータに対する Google の取り組みは、Google Cloud Trust Principles に反映されています。お客様が Google Workspace と Google Cloud Platform を使用されるたびにお客様のプライバシーを保護する方法を確認しています。

このホワイトペーパーでは、Google のクラウドベースの生産性向上スイートである Google Workspace のセキュリティとコンプライアンスに対するアプローチについて説明します。何十万人もの社員を抱える大規模な銀行や小売業者から、急成長を遂げている新興企業まで、世界中の 500 万を超える組織に利用されている、Google Workspace と Google Workspace for Education には、こちらに掲載されているコラボレーションと生産性向上のためのツールが用意されています。Google Workspace と Google Workspace for Education は、チームのメンバーがどこにいても、どのデバイスを使用していても、新しい効率的な方法でチームが安全に共同作業できるように設計されています。たとえば、Gmail では毎週 3,000 億を超える添付ファイルをスキャンしてマルウェアを検出し、スパム、フィッシング、マルウェアの 99.9% 以上の侵入を防いでいます[1]。Google は、あらゆる種類のセキュリティ上の脅威からの保護、ユーザーと管理者向けの新しいセキュリティ ツールの革新、お客様への安全なクラウド サービスの提供に取り組んでいます。

注: Google Workspace は、今後数か月以内に非営利団体のお客様にご利用いただけるようになります。G Suite for Nonprofits は、引き続き Google for Nonprofits プログラムを通じて対象の組織に提供される予定です。特に明記されていない限り、このドキュメントの内容は Google Workspace と Google Workspace for Education を対象としています。

免責条項

このドキュメントの内容は 2020 年 10 月時点のもので、作成時点の状況を表しています。Google は継続的にお客様データの保護の強化を進めており、今後、Google Cloud のセキュリティ ポリシーやシステムは変更される可能性があります。

[1] 2020 年 4 月現在。

Google のセキュリティとプライバシーに重点を置いた文化

Google は、すべての従業員がセキュリティとプライバシーを重視する、包括的で活気あふれる社風を築いてきました。この文化の影響は、採用プロセス、社員の新人研修、継続的なトレーニング、意識向上のための全社的なイベントにも顕著に表れています。

社員の身元調査

Google は、誰かがスタッフに加わる前に、その人物の教育と雇用の経歴を確認し、内部および外部のリファレンス チェックを実施しています。地域の労働法または法規制で許可されている場合、役職に応じて、身元調査、犯罪歴調査、信用調査を実施し、移民ステータスを確認することもあります。

全社員向けのセキュリティ トレーニング

Google の全社員は、入社時研修中および在籍期間中を通じてセキュリティ研修を受けています。新入社員は入社時研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。

社員は、各自の役割に応じて、セキュリティの特定の側面に関する追加トレーニングに参加します。たとえば、情報セキュリティ チームは新しいエンジニアに安全なコーディング方法、プロダクト設計、脆弱性自動テスト ツールなどについて指導します。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。

安全な環境

Google のゼロトラスト アプローチでは、デバイス、その状態、デバイスに関連付けられているユーザー、その背景状況に関する情報に基づいて、重要なアクセス制御を適用しています。このアプローチでは、内部ネットワークと外部ネットワークの両方を本質的に信頼できないものと見なします。これにより、アプリケーション レイヤでアクセスレベルを動的に表明して適用するボーダレス コンプライアンスの概念が生まれます。こうすることで、Google のセキュリティ チームとコンプライアンス チームは、緊急時でも普段と変わらずに安全かつ効果的に対応できます。

COVID-19（新型コロナウイルス感染症）により、私たちの働き方だけでなく、働く場所も変わった今、業界のコンプライアンス要件を満たし続けるための新しいソリューションが必要になっています。ゼロトラストを活用することで、VPN や場所の要件に依存しない、テレワークのための安全でスケーラブルなソリューションを社員や外部の人材に提供できます。

内部セキュリティとプライバシー イベント

セキュリティとプライバシーは常に進化し続けている分野です。Google は、意識を高めるための重要な手段は社員のエンゲージメントであると認識しています。Google では、すべての社員が参加できる定期的な社内会議を開催して、セキュリティとデータ プライバシーの意識を高め、革新を推進しています。また、セキュリティとプライバシーに関するトピックに焦点を当てた定期的な「技術系プレゼンテーション」を開催しています。主な例として、「プライバシー週間」が挙げられます。この期間中、Google はグローバル オフィス全体でイベントを開催し、ソフトウェア開発やデータ処理からポリシー適用に至るまで、プライバシーのあらゆる側面に対する意識を高めています。

専任セキュリティ チーム

Google では、ソフトウェア エンジニアリングと運用部門の一部として、セキュリティおよびプライバシー専門家で構成されるフルタイムの専任チームを採用しています。このチームには、情報、アプリケーション、ネットワーク セキュリティに関する世界有数の専門家が含まれます。チームは、防衛システムの保守、セキュリティ レビュー プロセスの開発、セキュリティ インフラストラクチャの構築、企業のセキュリティ ポリシーの実装を担当し、商用ツールやカスタムツール、侵入テスト、品質保証（QA）対策、ソフトウェア セキュリティ レビューを使用して、セキュリティの脅威を積極的にスキャンします。

Google 内では、情報セキュリティ チームのメンバーが、さまざまな重要なサービスを提供しています。すべてのネットワーク、システム、サービスのセキュリティ計画のレビュー、Google のプロダクトおよびエンジニアリング チームへのプロジェクト固有のコンサルティング サービスの提供、Google のネットワーク上の疑わしいアクティビティのモニタリング、情報セキュリティの脅威への対処、定期的なセキュリティ評価と監査の実施、外部の専門家との定期的なセキュリティ評価の実施などを行います。さらに、Google は「プロジェクト ゼロ」として知られるフルタイムのチームを編成し、標的型攻撃を防ぐことを目的として、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。

これで終わりではありません。セキュリティ チームは、Google ソリューションを選択したユーザーだけでなく、より幅広いインターネット ユーザー コミュニティを保護するための調査やアウトリーチ活動にも参加しています。また、セキュリティ チームは、セキュリティ調査論文（誰でも入手可能）を公開し、オープンソース プロジェクトや学術会議の開催や参加を行っています。

プライバシー チーム

Google のプライバシー チームは、Google プロダクトのリリースに不可欠な要素です。プライバシー チームは、お客様の個人情報を処理するサービスが、設計どおり、かつ Google のデータ保護の取り組みに沿って機能するように、一連の自動モニタリング ツールを構築しました。また、プライバシー要件を遵守するために、設計文書とコード監査もレビューします。

このチームは部門の枠を超えて、ユーザーデータの収集における透明性、ユーザーと管理者への有意義なプライバシー構成オプションの提供など、強力なプライバシー基準を反映したプロダクトのリリースを支援しながら、Google のプラットフォームに保存されている情報に対して優れた管理を継続します。プロダクトのリリース後、Google のコンプライアンス プログラムとプライバシー プログラムは、適切なデータ使用量を検証するためにデータ トラフィックを監査する自動プロセスをモニタリングします。また、Google は、新しいテクノロジーのプライバシーに関するベスト プラクティスについてソート リーダーシップを提供する調査も実施しています。

内部監査とコンプライアンスのスペシャリスト

データ保護規則は、企業が自社でどのようにデータを取り扱っているか、誰がデータにアクセスできるか、どのようにセキュリティ インシデントを管理しているかを把握することに大きな重点を置いています。Google にはエンジニアとコンプライアンスの専門家からなる専任チームがあり、お客様のコンプライアンスとリスク管理に関する義務の遂行をサポートしています。Google は、お客様と協力して、お客様固有の規制ニーズを理解し、それに対応するアプローチを採用しています。新しい監査基準が作成されると、チームはそれを満たすために必要な制御、プロセス、システムを決定し、サードパーティによる独立した監査と評価を促進してサポートします。特定の状況下では、Google のセキュリティとコンプライアンス管理を検証するために、お客様が監査を実施できるようにします。

セキュリティ調査コミュニティとのコラボレーション

Google は長年、セキュリティ調査コミュニティと緊密な関係を築き、彼らによる Google Workspace やその他の Google プロダクトの脆弱性を特定する支援に深く感謝しています。脆弱性報奨金プログラムは、ユーザーの安全維持に役立つ外部からのすべての貢献を称えるために設定したものです。このプログラムでは、ユーザーデータの機密性や完全性に影響を及ぼしたり、顧客データを危険にさらしたりする設計や実装の問題について、研究者に報告を奨励しています。報酬は数万ドルに達する場合があります。

調査コミュニティとの連携により、2019 年には 650 万ドル以上の報酬を支払いました。2019 年の 1 年間でこれまでの総額の 2 倍の報酬になったのです。Google はこのような個人に公式に感謝の意を表し、Google サービスへの貢献者一覧を作成しました。

オペレーション セキュリティ

Google のセキュリティは、後から付け加えたり不定期な取り組みの対象になったりするものではなく、Google の業務の不可欠な部分です。

脆弱性管理

Google の脆弱性管理プロセスでは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などの組み合わせを使用して、セキュリティ上の脅威を積極的にスキャンしています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。担当チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。

また、Google はセキュリティ研究コミュニティのメンバーと頻繁にコミュニケーションを取り、Google のサービスやオープンソース ツールについて報告されている問題を追跡しています。セキュリティ問題の報告に関する詳細については、Google アプリケーション セキュリティをご覧ください。

マルウェアの防止

強力なマルウェア攻撃は、アカウントの侵害、データの盗難、場合によってはネットワークへの追加アクセスにつながる可能性があります。Google は、ネットワークとお客様に対するこのような脅威を非常に深刻に受け止め、マルウェアを防止、検出、根絶するためにさまざまな策を講じています。

マルウェア サイトやメールの添付ファイルは、ユーザーのパソコンに悪意のあるソフトウェアをインストールして、個人情報の盗難、ID の盗難、他のパソコンへの攻撃を行います。ユーザーがこのようなサイトにアクセスすると、パソコンを乗っ取るソフトウェアが知らないうちにダウンロードされます。Google のマルウェア対策では、まず感染を防止するために、手動および自動のスキャナを使用して、マルウェアまたはフィッシングの手段となる可能性のあるウェブサイトについて Google の検索インデックスを調査します。加えて、Google の重要な保護手段の一つに添付ファイル マルウェア スキャナがあり、有害なコンテンツをブロックするために毎週 3,000 億を超える添付ファイルを処理しています。Google がブロックする悪意のあるドキュメントの 63% は、日ごとに異なるため、この絶えず進化する脅威に先手を打つべく、Google では最近、ディープ ラーニングを活用した新世代のドキュメント スキャナを追加して検出機能を強化しました。

Google のセーフ ブラウジング テクノロジーにより、毎日 40 億台以上のデバイスが保護されています。セーフ ブラウジングでは、日々危険なサイトが新たに何千も発見されています。その多くは、侵害された正当なウェブサイトです。安全でないサイトを検出すると、Google 検索とウェブブラウザに警告が表示されます。

Google は、セーフ ブラウジング ソリューションに加えて、VirusTotal を運用しています。これは、ファイルや URL を分析して、ウイルス、ワーム、トロイの木馬など、ウイルス対策エンジンやウェブサイトのスキャナで検知された悪意のあるコンテンツの特定を可能にするオンライン サービスです。その使命は、無料のツールとサービスの開発を通じて、ウイルス対策とセキュリティ業界の改善を支援し、インターネットをより安全な場所にすることです。 Google では、Gmail、ドライブ、サーバー、ワークステーションで複数のウイルス対策エンジンを使用して、ウイルス対策署名で見逃される可能性のあるマルウェアを特定しています。

モニタリング

Google のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。内部トラフィックは、トラフィックのキャプチャと解析のためのオープンソース ツールと商用ツールの組み合わせを使用して、グローバル ネットワーク全体の多くのポイントで、ボットネット接続を示すトラフィックの存在などの疑わしい動作がないか検査されます。

Google は、Google テクノロジーを基盤とする独自の相関システムを使用してネットワーク分析をさらに補完し、システムログを調べて、顧客データへのアクセス試行などの異常な動作を特定します。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを、一般公開データ リポジトリに設定しています。また、受信したセキュリティ レポートの確認や、公開のメーリング リスト、ブログ投稿、Wiki のモニタリングを積極的に行っています。自動ネットワーク分析は、潜在的な未知の脅威を特定し、それを Google セキュリティ スタッフに通知します。このプロセスは、システムログの自動分析によって補完されます。

インシデント管理

インシデント対応は、Google のセキュリティとプライバシー プログラム全体の重要な側面です。Google は、データ インシデントを管理するための厳格な手順を実施しています。この手順では、お客様データの機密性保持、整合性、可用性に影響を与える可能性のあるインシデントのアクション、エスカレーション、リスク軽減、解決、通知を指定します。

Google のインシデント対応プログラムは、多くの専門部門からエキスパートを集結したインシデント対応担当者チームによって管理され、各インシデントから提示される課題に合わせて対応策を適切に調整します。

チームの対象分野の専門家による取り組みはさまざまで、たとえば、インシデント コマンダーはインシデントの性質を評価して、インシデント対応にあたります。これには、インシデントのトリアージ評価の実施、必要に応じた重大度の調整、事実のレビューによる調査が必要な主要分野の識別、適切な運用 / 技術リードによる必要なインシデント対応チームの動員、などがあります。解決プロセスの一環として、デジタル フォレンジック チームは進行中の攻撃を検出し、フォレンジック調査を行います。プロダクト エンジニアは、お客様への影響を抑え、影響を受けるプロダクトを修正するためのソリューションを提供します。法務チームは適切なセキュリティおよびプライバシー チームのメンバーと協力して、証拠収集に関する Google の戦略を実行しつつ、法執行機関や政府規制機関と連携して、法的問題や要件について助言します。サポート担当者は、お客様への通知を管理し、追加の情報や支援に関するお客様からの問い合わせと依頼に対応します。

データ インシデントの修復と解決に成功した後、インシデント対応チームはインシデントから得た教訓を評価します。インシデントによって重大な問題が提起された場合、インシデント コマンダーは事後分析を開始します。このプロセスでは、インシデント対応チームがインシデントの原因と Google の対応を確認し、改善すべき主要な領域を特定します。場合によっては、異なるプロダクト、エンジニアリング、運用チームとの話し合いやプロダクト強化作業が必要になることがあります。フォローアップ作業が必要な場合は、インシデント対応チームが作業完了までの行動計画を作成し、プロジェクト マネージャーを割り当てて長期的な作業を進めます。インシデントが終了するのは、修復作業が完了した時です。

セキュリティを中核とするテクノロジー

ハードウェア、ソフトウェア、ネットワーク、システム管理テクノロジーの革新者として、Google は「多層防御」の原則をもとに、従来のテクノロジーよりも安全で管理しやすい IT インフラストラクチャを構築しました。Google では、サーバー、独自のオペレーティング システム、地理的に分散したデータセンターをカスタム設計し、安全に動作するように着想、設計、構築されたテクノロジー プラットフォーム上で Google Workspace を安全に実行できるようにしました。

最先端のデータセンター

セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。

データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。

データセンターのフロアに近づくほど、セキュリティ対策が強くなります。実際、Google のデータセンターに足を踏み入れることができるのは、Google の 1% に満たない社員に限られています。特定の役割を持ち、事前に承認された社員は、セキュリティ バッジと生体認証を使用して、多要素アクセス制御を実装するセキュリティ通路を通るという方法でのみフロアにアクセスできます。

データセンターへの電力供給

Google のデータセンターは、24 時間体制で稼働しサービスを中断しないようにするため、冗長電源システムと環境管理を導入しています。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。インシデントが発生した場合、すべての重要なコンポーネントには主電源と同等のパワーを備えた代替電源が利用されます。ディーゼル エンジンのバックアップ発電機により、各データセンターは緊急時でも最大限の性能を発揮できる電力を得られます。火災検知と消火装置（熱、火災、煙探知器を含む）は、影響を受けるゾーン、セキュリティ操作コンソール、リモート モニタリング デスクで音声と視覚効果による警報をトリガーし、ハードウェアの損傷を防止します。

環境への影響

Google は、データセンターの環境への影響を最小限に抑えることに深い関心を持ち、最新の「グリーン」テクノロジーを活用して自社施設の設計と構築を行っています。たとえば、スマート温度制御を導入し、外気の使用や冷却水の再利用などの「フリークーリング」技術を利用して、不要なエネルギー損失を低減するために電力を分配する方法を再設計しています。また、状況を測定するために、総合的な効率測定を使用して各施設のパフォーマンスを計算しています。

Google は、環境、職場の安全、エネルギー管理で高い基準を設けている外部の認証を、データセンター全体で取得した最初の大手インターネット サービス企業であることを誇りに思っています。具体的には、非常にシンプルなコンセプトをベースに構築された ISO 14001、OHSAS 18001、ISO 50001 の認証を取得しています。有言実行、そして継続的な向上が大切なのです。

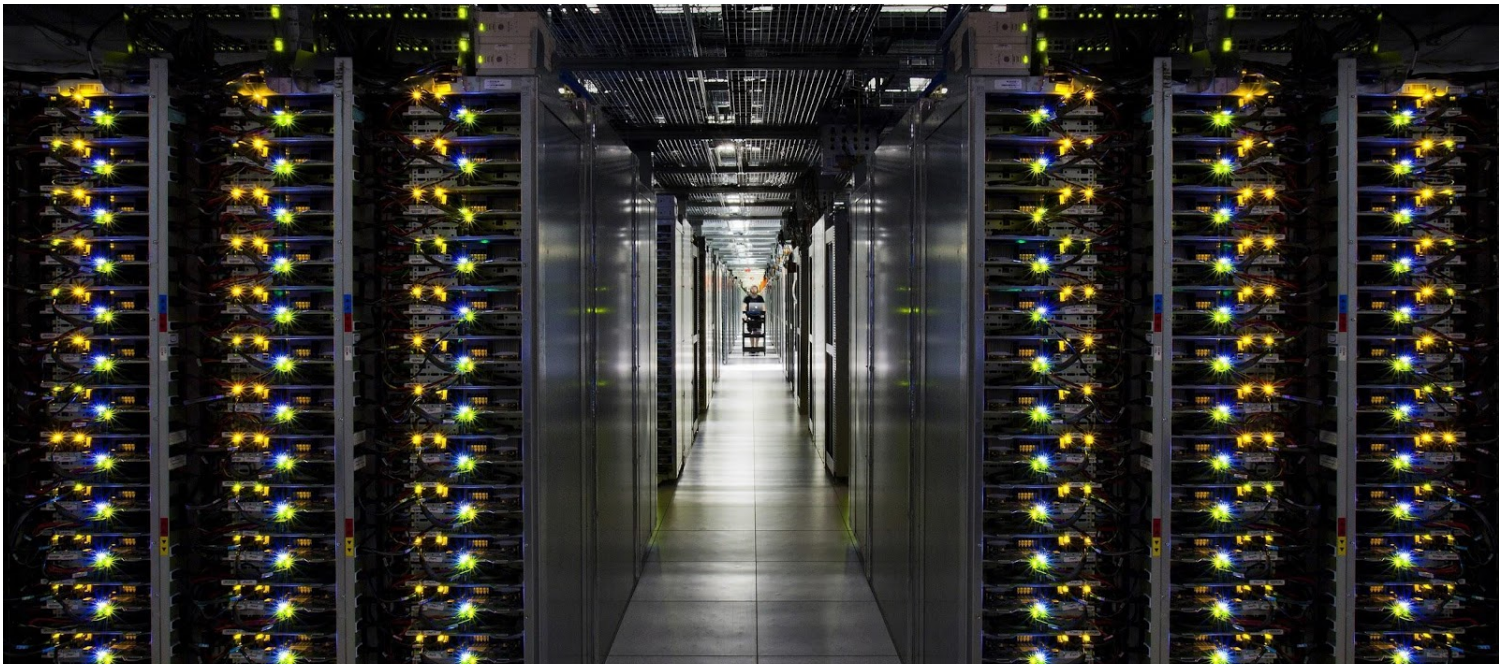
カスタム サーバー ハードウェアとソフトウェア

Google のデータセンターには、エネルギー効率に優れたカスタム専用サーバーとネットワーク機器があり、自社で設計と製造を行っています。また、Google の本番環境サーバーは、必要最低限のみを装備した強化版の Linux に基づいて設計されたオペレーティングシステム（OS）を実行しています。言い換えれば、Google のサーバーとその OS は、Google サービスの提供のみを目的として設計されています。つまり、多くの商用ハードウェアとは異なり、Google サーバーには、脆弱性を引き起こす可能性のあるビデオカード、チップセット、周辺機器コネクタなどの不要なコンポーネントが含まれていません。Google サーバーのリソースは動的に割り振られているため、拡張の柔軟性と迅速かつ効率的に適応する能力を実現し、お客様の需要に応じてリソースの追加または再割り振りを行います。この均質な環境は、バイナリの変更についてシステムを継続的にモニタリングする独自のソフトウェアによって維持されています。Google の標準イメージと異なる変更が見つかった場合、システムは自動的に公式の状態に戻ります。この自動化された自己修復メカニズムにより不安定なイベントをモニタリングして修正し、インシデントに関する通知を受信して、重大な問題になる前に潜在的なネットワーク侵害を遅らせることができます。

ハードウェアの追跡と廃棄

Google は、バーコードとアセットタグを使用して、取得とインストールから廃棄と破棄まで、データセンター内のすべての機器の場所とステータスを綿密に追跡しています。また、認可なしでデータセンターのフロアから機器が持ち出されないように、金属探知機と動画監視システムを実装しています。データセンターのライフサイクル中、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。

各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合には即座に対処されます。ハードドライブを破棄する際には、所定の権限を持つ担当者が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。



独自のセキュリティ上の利点を持つグローバル ネットワーク

Google の IP データ ネットワークは、Google 独自の光ファイバー、公共ファイバー、海底ケーブルで構成されているため、世界中で高可用性と低レイテンシのサービスを提供できます。

他のクラウド サービスやオンプレミス ソリューションの場合、顧客データは、パブリック インターネット上の「ホップ」と呼ばれるデバイス間をいくつか移動する必要があります。ホップ数は、お客様の ISP とソリューションのデータセンター間の距離によって異なります。ホップ数が増えるたびに、データが攻撃または傍受される新たな機会が生じます。Google のグローバル ネットワークは、世界中のほとんどの ISP にリンクされているため、パブリック インターネット上のホップ数を最小限に抑え、転送中のデータのセキュリティを向上させることができます。

多層防御とは、Google のネットワークを外部からの攻撃から保護するために複数のセキュリティ階層が設けられていることを意味します。まず、業界標準のファイアウォールとアクセス制御リスト（ACL）を使用してネットワークの分離を実施し、すべてのトラフィックをカスタム Google Front End（GFE）サーバー経由でルーティングして、悪意のあるリクエストや分散型サービス拒否攻撃（DDoS）を検出して阻止します。また、GFE サーバーは、内部的に制御されたサーバーリストとの通信のみが許可されます。これは、GFE サーバーが意図しないリソースにアクセスすることを防止する「デフォルト拒否」構成です。最後に、プログラミング エラーの原因分析のために、定期的にログが検査されます。また、ネットワーク デバイスへのアクセスは許可された担当者に制限されています。つまり、重要な点は、Google のセキュリティ要件を満たす承認済みのサービスとプロトコルのみが Google のネットワークを通過することを許可され、それ以外は自動的に破棄されるということです。

転送中のデータと保存データの暗号化

暗号化は Google Workspace のセキュリティ戦略の重要な要素であり、メール、チャット、ビデオ会議、ファイルなどのデータ保護に役立っています。まず、以下に説明するように特定のデータを「静止状態」で保存、すなわち、ディスク（ソリッド ステート ドライブを含む）またはバックアップ メディアに保存しながら、暗号化します。攻撃者や物理的なアクセス権を持つ人物がデータを保存しているストレージ機器を入手した場合でも、必要な暗号鍵がないため、データを読み取ることはできません。次に、インターネット上やデータセンター間で送受信される「転送中」の全ての顧客データを暗号化します。攻撃者がこのような送信を傍受した場合でも、取得できるのは暗号化されたデータのみです。保存データと転送中のデータを暗号化する方法について詳しく説明します。

Google は、メール ルーティングでの Transport Layer Security（TLS）の使用において業界をリードしてきました。これにより、Google と Google 以外のサーバーが暗号化された状態で通信できるようにしています。Google から TLS をサポートする Google 以外のサーバーにメールを送信すると、トラフィックが暗号化され、パッシブ盗聴を防止できます。Google では、TLS の普及が業界にとって非常に重要であると考えています。そのため、Email Encryption Transparency Report で TLS の進歩を報告しています。また、MTA-STS 標準を開発してサポートすることで、転送中のメールのセキュリティも向上しました。これにより、受信ドメインでメール転送時に機密性と整合性の保護が必要になります。また、Google Workspace ユーザーは、特定のドメインやメールアドレスが TLS で保護されている場合にのみ、そのドメインやメールアドレスにメールを送信できます。これは TLS コンプライアンス設定で管理できます。

暗号化の詳細については、Google Workspace 暗号化に関するホワイトペーパーをご覧ください。

低レイテンシの高可用性ソリューション

Google では、サーバー設計やデータの保存方法、ネットワーク接続やインターネット接続、さらにはソフトウェア サービス自体まで、プラットフォームのすべてのコンポーネントの冗長性が非常に高くなるように設計してい

ます。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。

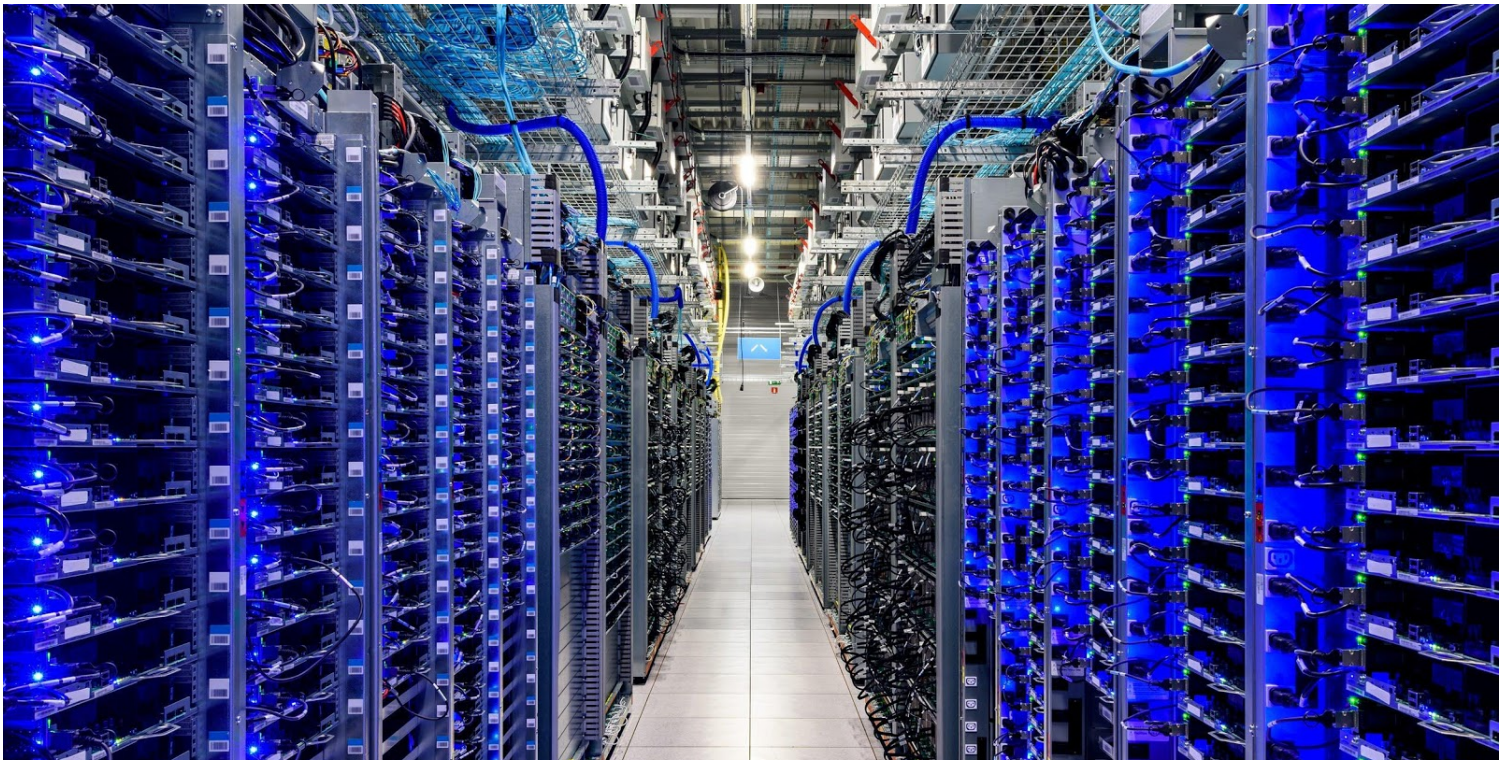
Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、ほとんどの場合、Google Workspace のお客様は中断することなく作業を続けることができます。また、グローバルに社員を抱えるお客様は、追加の構成や費用をかけずにドキュメントやビデオ会議などでコラボレーションでき、単一のグローバル ネットワークで共同作業することで、低レイテンシでパフォーマンスに優れたエクスペリエンスを共有できます。

冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Workspace では、目標復旧時点（RPO）の目標も、目標復旧時間（RTO）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Workspace プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。

これを効率的かつ安全に行うために、顧客データをランダムなファイル名を持つデジタルピースに分割します。分割されたピースのコンテンツもファイル名も、人間が読める形式で保存されることはありません。また、保存された顧客データは、ストレージの中で検査するだけでは特定の顧客やアプリケーションまで追跡できません。次に、各ピースが複数のディスク、複数のサーバー、複数のデータセンターにほぼリアルタイムで複製され、単一障害点を回避します。最悪の事態に備えるために、Google では、本社を含む個々のデータセンターが 30 日間利用できなくなることを想定した障害復旧演習を実施しています。

サービスの利用可能性

一部の Google のサービスは、現在または一時的に一部の法域において利用できない場合があります。Google の透明性レポートでは、Google プロダクトへのトラフィックの最近および現在の中断を紹介しています。Google のコードにより、世界中のトラフィック パターンを経時的に観察し、大幅な変化を検出できます。また、ジャーナリスト、活動家、その他の人々から問い合わせを受けたときにも、グラフを見て確認できます。Google は、オンライン情報の可用性を分析して把握できるよう、このデータを一般公開しています。



コンプライアンス要件のサポート

Google は、お客様のコンプライアンスとレポート作成のニーズを満たす安全なプロダクトとサービスの提供に取り組んでいます。ベスト プラクティスに関する広範な情報を共有し、コンプライアンス関連ドキュメントへの簡単なアクセスを提供します。Google Cloud はセキュリティ、サードパーティによる監査と認定、ドキュメント、法的取り組みで業界をリードしており、お客様のコンプライアンスをサポートします。Google のプロダクトは、定期的にセキュリティ、プライバシー、コンプライアンスの管理について個別に検証を受け、認証、コンプライアンスの証明書、世界規格に対する監査レポートを取得しています。サードパーティの監査担当者は、独立した検証プロセスの一環として、データセンター、インフラストラクチャ、運用など、Google のエンドツーエンドでのセキュリティ プラクティスを定期的に検証します。また、正式な認定や証明書が必要ない、または適用されない可能性のあるフレームワークや法律に照らして、リソース ドキュメントとマッピングを作成しました。Google のコンプライアンス リソース センターには、コンプライアンス関連のドキュメントとリソースの詳細が掲載されています。

Google は、対応できるコンプライアンスの範囲拡大に、常に取り組んでいます。業界をリードする標準と規制機関から入手可能なガイダンスを評価し、コンプライアンスの状況の変化に合わせて、セキュリティおよびプライバシー プログラムを調整しています。また、地域や業界ごとにプログラムを厳選し、お客様が Google のコンプライアンス リソースを活用して、十分な情報に基づいた意思決定を行えるように支援します。

Google Workspace の導入を検討されるお客様は、Google のコンプライアンス サービスを利用して、プロダクトスイートがセキュリティとコンプライアンスのニーズを満たしているかどうかを確認できます。

法規制に関するコンプライアンス

Google のお客様は、金融、政府機関、医療、教育など、規制の厳しい業界で事業を展開しています。Google Cloud は、お客様がさまざまな業界固有の要件を遵守できるようなプロダクトとサービスを提供しています。詳細については、こちらをご覧ください。

独立したサードパーティの認定と証明書

お客様や規制機関は、Google のセキュリティ、プライバシー、コンプライアンスの管理に対し、独立した検証を求めています。Google は、こうした声に応えて保証を提示するために、定期的に複数の独立したサードパーティの監査を受けています。Google が監査を受けている主要な国際標準には、次のようなものがあります。

- ISO/IEC 27001（情報セキュリティ管理）
- ISO/IEC 27017（クラウド セキュリティ）
- ISO/IEC 27018（クラウド プライバシー）
- ISO/IEC 27701（プライバシー）
- SOC 2 と SOC 3 レポート

また、FedRAMP（米国政府）、BSI C5（ドイツ）、MTCS（シンガポール）など、セクターや国別のフレームワークにも参加しています。また、正式な認証や証明書が必要ない、または適用されない可能性がある特定のフレームワークについて、リソース ドキュメントとマッピングも提供しています。

Google のコンプライアンス サービスの一覧については、コンプライアンス リソースセンターをご覧ください。

データの利用

Google の哲学

顧客データを所有しているのは Google Workspace のお客様であり、Google ではありません。Google Workspace を利用している組織がシステムに入力した顧客データはその組織のものであり、Google が広告のためにデータをスキャンすることはありません。Google ではお客様に詳細なデータ処理の修正条項を提示しています。この条項は、お客様のデータの保護に対する Google の取り組みを示すものです。さらに、お客様がデータを削除した場合、Google は 180 日以内にそのデータをシステムから削除します。Google は、お客様の管理者が Google のサービスの使用を中止される際、ご自身のデータを簡単に取得するためのツールを提供しています。Google により罰金や追加料金が課されることはありません。

Google Workspace への広告の非掲載

Google Workspace のコアサービスに広告が表示されることはありません。また、今後もこの点について変更する予定はありません。Google が、広告目的で Google Workspace コアサービスのデータを収集、スキャン、使用することはありません。お客様の管理者は、Google Workspace 管理コンソールからコアサービス以外のサービスへのアクセスを制限できます。Google は、迷惑メールのフィルタリング、ウイルス検出、スペルチェック、個人アカウント内のメールやファイルの検索機能といった有益なサービスを提供するため、顧客データのインデックスを作成します。

データのアクセスと制限

管理者権限

Google のシステムは、顧客データにアクセスできる社員の数を制限し、その社員の活動を積極的にモニタリングするように設計されています。Google の社員には、会社のリソースに対する既定のアクセス許可を制限したセットのみが付与されます。内部サポートツールへのアクセスは、アクセス制御リスト（ACL）を使用して制御されます。Google は、正式なプロセスに則って社員に Google リソースへのアクセス権を付与または無効にしており、退職した社員のアクセス権は自動的に削除されます。アクセス認可は、システムのすべての関連階層に適用されます。承認はワークフロー ツールで管理され、ログに記録されます。社員の承認設定は、Google Workspace プロダクトに関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。制御の有効性をチェックするために、アクセスは Google の専任セキュリティ チームによってモニタリングされています。セキュリティ チームは、アクセス パターンを積極的にモニタリングし、異常なイベントを調査します。

さらに、透明性とユーザーの信頼に対する Google の長期的な取り組みの一環として、アクセスの透明性を提供しています[2]。これは、お客様が特定の顧客データにアクセスするときに Google スタッフが行ったアクションのログを確認できるようにする機能です。アクセスの透明性と統合されているサービスの場合、Google はツールを使用して、アクセスに対して提示されたビジネス上の正当性が有効であることを検証し、その正当性をアクセスの透明性ログに記録します。

お客様の管理者向け

お客様は、Google Workspace 上のデータとサービスへのアクセスを制御して、組織の希望する構成に従ってデータを保護できます。ロールベースのアクセス制御により、ユーザーを管理者として指名し、そのユーザーに Google Workspace 管理コンソールで特定のタスクにアクセスして実行する権限を付与できます。ユーザーを、管理コンソールですべてのタスクを実行できる特権管理者に指定することができます。または、管理者が実行できるタスクを制限するロールを割り当てる方法もあります。たとえば、グループの作成、サービス設定の管理、ユーザーのパスワード リセットのみを許可できます。

法執行機関のデータ リクエスト

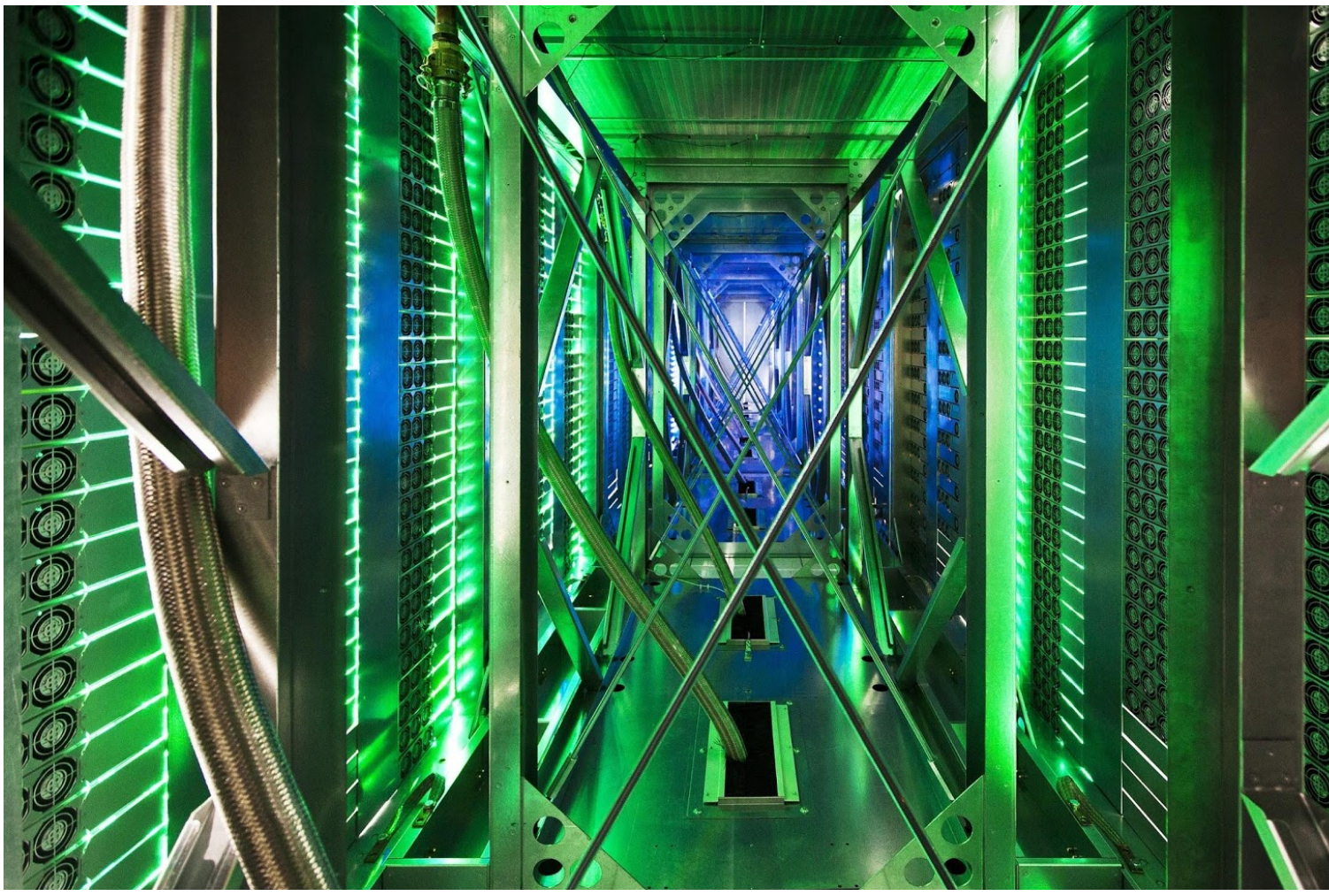
お客様はデータ所有者として、主に法執行機関のデータ リクエストに対応する責任があります。Google は、データ リクエストを直接お客様に対して行うよう政府機関に指示する方針をとっています。しかし、他のテクノロジー企業や通信企業と同様、Google は世界中の政府機関や裁判所から、お客様による Google のサービスの利用方法について直接リクエストを受ける場合があります。Google は、お客様のプライバシーを保護し、過剰なリクエストを制限するとともに、法的義務を遵守するための措置を講じます。お客様が Google に保存するデータのプライバシーとセキュリティを尊重することは、このような法的要求を遵守するにあたり、常に Google の優先事項となっています。

データ リクエストとそれに対する Google の対応に関する詳細情報は、透明性レポートに記載されています。詳細については、Google Workspace にデータを委ねるホワイトペーパーも合わせてご覧ください。

[2] アクセスの透明性は、Google Workspace Enterprise と Google Workspace for Education Plus でのみご利用いただけます。

サードパーティ サプライヤー

Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、Google は顧客サポートやテクニカル サポートなど、Google Workspace に関連するサービスを提供するためサードパーティ サプライヤーを利用することがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価したうえで、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。



ユーザーと管理者がセキュリティとコンプライアンスを改善できるようにする

お客様のデータの構造、テクノロジー、運用、アプローチにセキュリティを組み込む Google の堅牢なセキュリティ インフラストラクチャとシステムは、Google Workspace をご利用のすべてのお客様にとってデフォルトになっています。ユーザーはさらにこのレベルを超えて、ダッシュボードやアカウント セキュリティ ウィザードを使用して、個々のセキュリティ設定の強化とカスタマイズを行い、ビジネスニーズを満たすことができます。

また、Google Workspace の管理者は、組織の規模に関係なく、インフラストラクチャ、アプリケーション、システムの統合を管理コンソールを介して単一のダッシュボードで構成できるため、管理と構成を簡素化できます。DKIM（フィッシング対策機能）をオンプレミスのメールシステムに導入することを検討してください。従来、管理者はすべてのサーバーに個別にパッチを適用して構成する必要があり、構成ミスがサービス停止の原因になることがありました。しかし、管理コンソールを使用すると、数千、数十万のアカウントに対して数分で DKIM を構成でき、システム停止やメンテナンスの時間枠を気にする必要はありません。

これは一例にすぎません。管理者は、2 段階認証やシングル サインオンなどの認証機能や、セキュアな転送（TLS）の適用などのメール セキュリティ ポリシーなど、強力なツールを自由に使用でき、あらゆる組織でセキュリティとシステムの統合要件を満たすように構成できます。

アクセスと認証

2 段階認証とセキュリティ キー

お客様は、2 段階認証とセキュリティ キーを使用して、アカウントのセキュリティを強化できます[3]。これにより、社員のアクセス制御の構成ミスや、攻撃者によるアカウントの不正使用などのリスクを軽減できます[4]。エンタープライズ向けの高度な保護プログラムでは、登録ユーザーに対して、厳選された強力なアカウント セキュリティ ポリシーを適用できます。これには、セキュリティ キーの要求、信頼されていないアプリへのアクセスのブロック、メールの脅威に対する高度なスキャンなどが含まれます。

シングル サインオン（SAML 2.0）

Google Workspace では、ユーザーが同じサインイン ページと認証情報を使用して複数のサービスにアクセスできるシングル サインオン（SSO）サービスを提供しています。このサービスは、セキュアなウェブドメイン間でユーザー認証と認可データを交換できるようにする XML 標準の SAML 2.0 に基づいています。セキュリティを強化するために、SSO は RSA または DSA アルゴリズムで生成された公開鍵と証明書を受け入れます。お客様の組織は SSO サービスを使用して、Google Workspace のシングル サインオンを LDAP または他の SSO システムに統合できます。

OAuth 2.0 と OpenID Connect

Google Workspace は、認証と認可のためのオープン プロトコルである OAuth 2.0 と OpenID Connect をサポートしています。これにより、複数のクラウド ソリューションに対して 1 つのシングル サインオン サービス（SSO）を構成できます。ユーザーは認証情報を再入力したり、機密のパスワード情報を共有したりすることなく、Google Workspace からサードパーティ アプリケーションにログオンできます。また、その逆も可能です。

Information Rights Management（IRM）

ほとんどの組織は、**機密データの取り扱い**に関する内部ポリシーを定めています。Google は、Google Workspace 管理者が機密データを管理できるように、Google ドライブで **Information Rights Management** を提供しています。管理者とユーザーは、Google ドライブのアクセス許可を使用して、ファイルの再共有、ダウンロード、印刷、コピー、アクセス許可の変更を防止することで、機密性の高いコンテンツを保護できます。

メール配信の制限

デフォルトでは、ドメインに Gmail アカウントを持つユーザーは、任意のメールアドレス間でメールを送受信できます。場合によっては、ユーザーがメールを交換できるメールアドレスを管理者が制限することもできます。学校などでは、学生が教職員や他の学生とメールを交換できるようにし、学校外の人とは交換できないようにする必要があります。

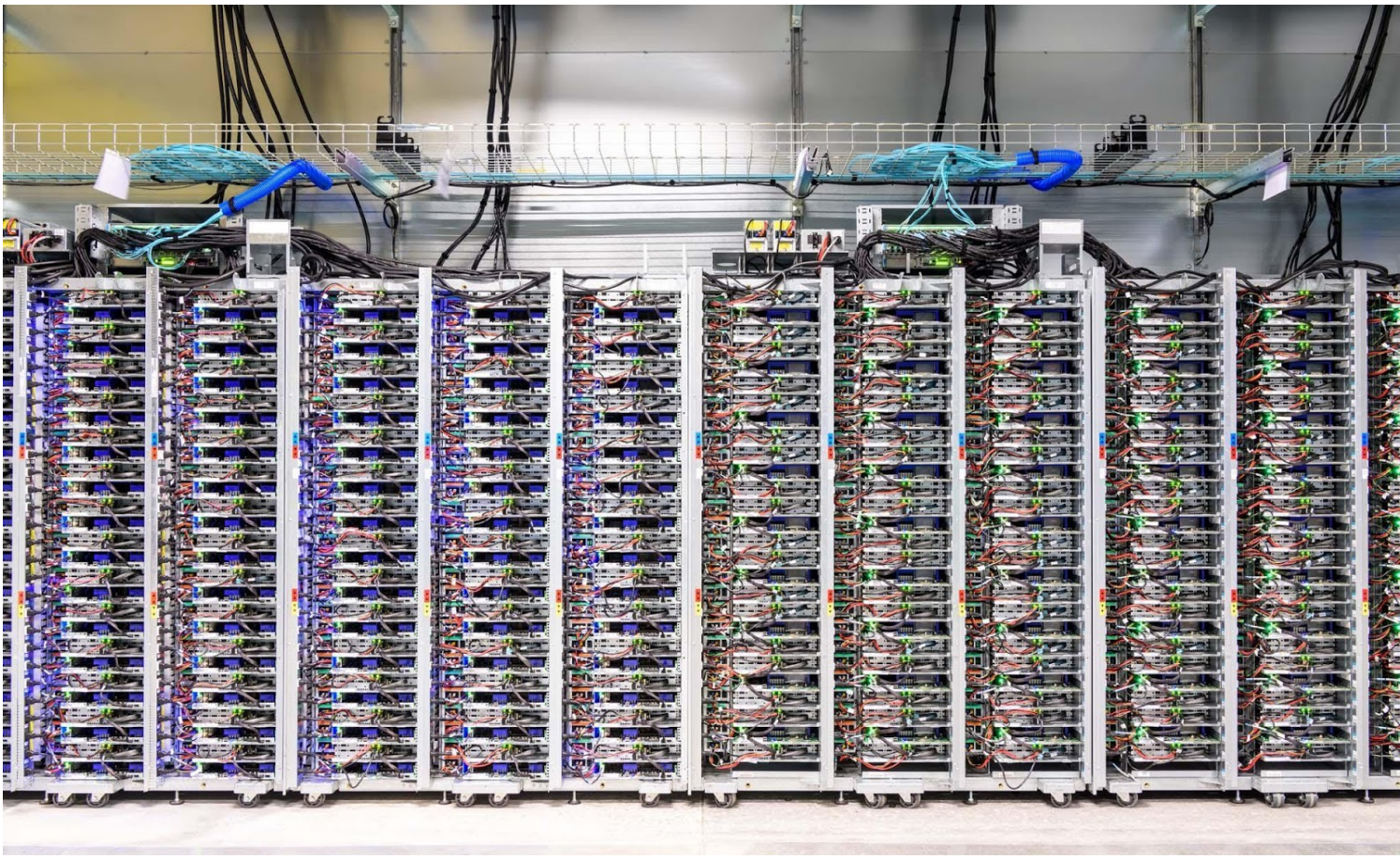
配信の制限設定を使用すると、管理者はユーザーがメール メッセージを送受信できるアドレスとドメインを指定できます。管理者が配信の制限設定を追加すると、ユーザーは許可されたパーティとのみ通信できます。リストにないドメインにメールを送信しようとすると、そのアドレスへのメールを禁止するポリシーと、メールが未送信であることを確認するメッセージが表示されます。同様に、ユーザーはリストに含まれるドメインから認証済みメッセージのみを受信します。リストにないドメインから送信されたメッセージ（またはリストに含まれるドメインからでも DKIM または SPF レコードを使用して検証できないメッセージ）は、ポリシーに関するメッセージを添えて送信者に返されます。

---

[3] 2 段階認証プロセスの導入の詳細については、サポートページをご覧ください。
[4] セキュリティ チェックリスト ページのセキュリティに関するベスト プラクティス ガイダンスをご覧ください。

ユーザー コンテキストに基づくアプリケーション アクセス

ユーザー アクセスを容易にすると同時に、データのセキュリティを保護するため、Google は、コンテキストアウェア アクセスを開発しました[5]。これにより、ユーザーの ID とリクエストのコンテキスト（デバイスのセキュリティ ステータスや IP アドレスなど）に基づいて、Google Workspace アプリをきめ細かく制御できます。Google が開発した BeyondCorp セキュリティ モデルに基づいて、ユーザーはリモート アクセス VPN ゲートウェイを使用せずに、ほぼすべてのデバイスを使ってどこからでもウェブ アプリケーションやインフラストラクチャ リソースにアクセスでき、管理者はユーザーのデバイスを制御できます。組織単位またはグループのすべてのメンバーに対して、2 段階認証などのアクセス ポリシーを設定することもできます。



[5] Cloud Identity との統合。コンテキストアウェア アクセス機能を使用して Google Workspace アプリへのアクセスを保護するには、Cloud Identity Premium または Google Workspace Enterprise ライセンスが必要です。

アセットの保護

スパム、フィッシング、マルウェアからのメールの保護

Gmail は、スパム、フィッシング詐欺、マルウェアから受信メールを保護します。Google の既存の機械学習モデルは、これを実現するうえで非常に効果的です。また、他の保護機能と組み合わせることで、Gmail の受信トレイに到達する脅威の 99.9% 以上をブロックできます。Google の主な保護機能の一つは、有害なコンテンツをブロックするために毎週 3,000 億以上の添付ファイルを処理するマルウェア スキャナです[6]。Google がブロックする悪意のあるドキュメントの 63% は、日ごとに異なります[7]。さらに、Gmail はセキュリティ サンドボックスと呼ばれる仮想環境で添付ファイルをスキャンまたは実行できます。脅威として識別された添付ファイルは、ユーザーの迷惑メールフォルダに配置、隔離できます。

Google は、フィッシングの早期検出により迷惑メール検出精度を向上させています。これは、厳格なフィッシング分析を実行し、ユーザーデータを侵害からさらに保護するために、メッセージを選択的に遅延させる（平均でメッセージの 0.05% 未満）専用の機械学習モデルです。

Google の検出モデルは、フィッシングや疑わしい URL を検索してフラグを立てる Google セーフ ブラウジングのテクノロジーと統合されています。この新しいモデルは、URL の評判や類似度分析など、さまざまな手法を組み合わせており、フィッシングやマルウェア リンクの URL のクリック時に警告を発することができます。新しいパターンが見つかると手動システムよりもはるかに迅速に適応できるこのモデルには、年々改良が重ねられています。

メールのなりすまし防止

迷惑メール送信者は、メール メッセージの「差出人」アドレスを信頼できる組織のドメインから送信されたように偽造することがあります。このメールのなりすましを防ぐため、Google は DMARC プログラムに参加しています。DMARC プログラムでは、ドメイン所有者が自身のドメインから未認証のメッセージが届いた場合の処理方法をメール プロバイダに伝えることができます。Google Workspace のお客様は、管理者用の設定画面で DMARC レコードを作成し、すべての送信メール ストリームに対して SPF レコードと DKIM キーを導入することで DMARC を実装できます。

データ損失を防ぐための社員への警告

社員がデータを保護するための適切な意思決定を行えるようになると、企業全体のセキュリティが向上します。Gmail では、ユーザーに意図しない外部への返信に関する警告を表示して、データの損失を防ぐことができます。会社のドメイン外のユーザーに返信しようとすると、そのメールの送信が意図したものかを確認するためのクイック警告が表示されます。また、Gmail のコンテキスト インテリジェンスにより、受信者が既存の連絡先か、ユーザーが定期的にやり取りしている相手かどうかを判断でき、必要な警告のみが表示されます。

ホスト型 S/MIME でセキュリティを強化

Google のホスト型 S/MIME ソリューションでは、S/MIME で暗号化されたメールを受信すると、そのメールが Google の暗号化を使用して保存されます。つまり、スパム、フィッシング、マルウェアに対する広範な保護、管理サービス（Vault の保持、監査、メール ルーティング ルールなど）のほか、メールのカテゴリ化、高度な検索、スマート リプライといった高価値エンドユーザー機能など、メールに対してすべての通常処理を行うことが

[6] 2020 年 2 月現在。
[7] 2020 年 2 月現在。

できます。大部分のメールについてはこれが最も安全なソリューションであり、Google の処理の安全性と機能性を損なうことなく、転送中の強力な認証と暗号化のメリットが得られます。

Gmail 情報保護モード

Gmail ユーザーは、Gmail の情報保護モードを使用して、機密情報を不正アクセスから保護できます。情報保護モードのメッセージの受信者には、添付ファイルを含めメッセージを転送、コピー、印刷、ダウンロードするオプションはありません。ユーザーは、メッセージの有効期限の設定、任意の時点でのメッセージ アクセスの取り消し、メッセージにアクセスするための SMS 認証コードのリクエストが可能です。

Gmail とドライブのデータ損失防止（DLP）

データ損失防止（DLP）[8] は、支払いカード番号、政府発行の個人識別番号、保護された健康情報などの機密情報や個人情報が組織外に漏洩するのを防ぐために設計された、より強固なセキュリティ機能です。DLP を使用すると、機密データが企業内でどのように流れているかを監査することや、警告やブロックのアクションを有効にして、ユーザーが**機密データを送信**できないようにすることができます。こうしたアクションを実行できるように DLP では、グローバル ID とリージョン ID、医療情報、認証情報の検出など、事前定義されたコンテンツ検出機能が提供されます。また、企業のニーズに合わせて独自のカスタム検出を定義することもできます。添付ファイルや画像ベースのドキュメントの場合、DLP は Google の光学式文字認識を使用して、検出範囲と品質を向上させます。Gmail DLP の詳細をご覧ください。DLP を使用して、ユーザーが Google ドライブまたは共有ドライブの機密性の高いコンテンツを組織外のユーザーと共有できないようにすることもできます。さらに、ドライブ ファイルの高度な DLP ルールを使った IRM 制御と分類を自動化できます。

Google Workspace のセキュリティ設定の構成

セキュリティとアラート管理

複数のセキュリティとプライバシー管理を導入している組織では、**一元的に脅威を防止、検出、修復できる場所が必要**です。Google Workspace セキュリティ センター[9] は、高度なセキュリティ情報と分析機能を提供し、ドメインに影響を与えるセキュリティの問題を可視化して制御します[10]。企業のデータとユーザーを保護するための、セキュリティ分析、行動につながる分析情報、Google が推奨するベスト プラクティスなどが統合されています。管理者は、セキュリティ ダッシュボードを使用して、さまざまなセキュリティ センター レポートの概要を確認できます。セキュリティ状況ページは管理コンソールの設定を可視化し、セキュリティ リスクの理解を深めて管理するのに役立ちます。さらに、セキュリティ調査ツールを使用すれば、ドメイン内のセキュリティとプライバシーの問題を特定し、優先順位を付けて対処できます。管理者は、このような問題をより迅速かつ効率的に検出して修正するアクティビティ ルールを作成することで、調査ツールのアクションを自動化できます。たとえば、ドライブ ドキュメントが社外で共有されている場合に、特定の管理者にメール通知を送信するようなルールを設定できます。

Google Workspace のアラート センターでは、Google Workspace のすべてのお客様に、ドメイン内のアクティビティに関するアラートと実用的なセキュリティ分析情報を提供し、フィッシング、マルウェア、不審なアカウン

---

[8] Google Workspace Enterprise と Google Workspace for Education のお客様のみご利用いただけます。
[9] Google Workspace Enterprise Edition、Google Workspace for Education Standard、Google Workspace for Education Plusに含まれています。
[10] セキュリティ センターにアクセスするには、Google Workspace Enterprise、Google Workspace for Education Standard、Google Workspace for Education Plus, Drive Enterprise、Cloud Identity Premium Edition のライセンスを持つ管理者である必要があります。Drive Enterprise または Cloud Identity Premium Edition では、セキュリティ ダッシュボードにセキュリティ センター レポートのサブセットが表示されます。

ト、不審なデバイス アクティビティなどの最新のセキュリティ脅威から組織を保護します。アラート センター API を使用して、既存のチケット発行プラットフォームまたは SIEM プラットフォームにアラートをエクスポートすることもできます。

ドライブ共有のための信頼できるドメイン

管理者は、組織内のユーザーによる Google ドライブのファイルやフォルダの共有方法を制御できます。たとえば、ユーザーが組織外のユーザーとファイルを共有できるかどうか、または共有が信頼できるドメインのみに制限されているかどうかを管理できます[11]。オプションのアラートを設定して、ファイルが社外で共有される前に機密情報でないことをユーザーに確認できます。

ビデオ会議の安全性

Google Meet は、Google がお客様の情報とプライバシーを保護するために使用しているのと同じ、設計段階からセキュリティが考慮されたインフラストラクチャ、組み込みの保護機能、グローバル ネットワークを活用しています。ウェブ会議と電話によるダイヤルインの両方のハイジャック対策を含め、一連の不正使用防止対策はデフォルトで有効になっており、会議を安全に実施できます。

Chrome、Firefox、Safari、新しい Edge をご利用の場合、プラグインまたはソフトウェアをインストールする必要はありません。Meet はブラウザで問題なく動作します。このため、Meet が攻撃の対象となる可能性が低減し、エンドユーザーのパソコンにセキュリティ パッチを頻繁に適用する必要がなくなります。モバイルでご利用の場合は、Apple App Store または Google Play ストアから Google Meet アプリをインストールしてください。

Google Meet では、ハードウェアとスマートフォンベースのセキュリティ キーと Google からのメッセージによる安全で便利な複数の 2 段階認証（2SV）オプションをサポートしています。Meet ユーザーは、Google の高度な保護プログラム（APP）にアカウントを登録できます。フィッシングおよびアカウントの乗っ取りに対して高度な保護を提供する APP は、リスクが最も高いアカウント向けに設計されており、このプログラムに参加済みのお客様は、繰り返しターゲットになることがあったとしても実際のフィッシング被害は未だ確認されていません。詳細については、このページをご覧ください。

[11] ホワイトリストに登録されたドメインのみへの共有の制限など、一部の機能は、Google Workspace Enterprise、Google Workspace for Education Plus、Drive Enterprise、Business、Nonprofits エディションでのみご利用いただけます。

エンドポイント管理

モバイル デバイスとデスクトップ デバイスの情報保護は、お客様にとって重要な懸念事項です。Google Workspace のお客様は、**エンドポイント管理**[12] を使用して、ユーザーの個人デバイスや組織の企業所有デバイス上の企業データを保護できます。管理対象としてデバイスを登録することで、ユーザーは Google Workspace サービスに安全にアクセスできます。組織は、デバイスの暗号化や画面ロック、パスワードの強制によってデバイスとデータを安全に保護するポリシーを設定できます。さらに、デバイスを紛失したり盗難にあったりした場合、企業アカウントをモバイル デバイスからリモートで消去し、ユーザーをデスクトップ デバイスからリモートでサインアウトできます。IT 管理者は、管理コンソールを使用して **Windows 10 デバイスの管理と構成を行う**こともできます。また、ユーザーは既存の Google Workspace アカウントの認証情報を使用して Windows 10 デバイスにログインし、シングル サインオン（SSO）でアプリやサービスにアクセスできます。レポートからポリシーのコンプライアンス状況をモニタリングし、ユーザーとデバイスに関する情報を取得できます。エンドポイント管理の詳細については、こちらをご覧ください。

レポート分析

Google Workspace 監査ログ

クラウドにデータを保存している企業は、**データアクセスとアカウント アクティビティの可視性**を求めています。Google Workspace 監査ログは、セキュリティ チームが Google Workspace で監査証跡を維持し、管理アクティビティ、データアクセス、システム イベントに関する詳細情報を表示するのに役立ちます。Google Workspace 管理者は、管理コンソールを使用してログにアクセスし、必要に応じてログをカスタマイズしてエクスポートできます。

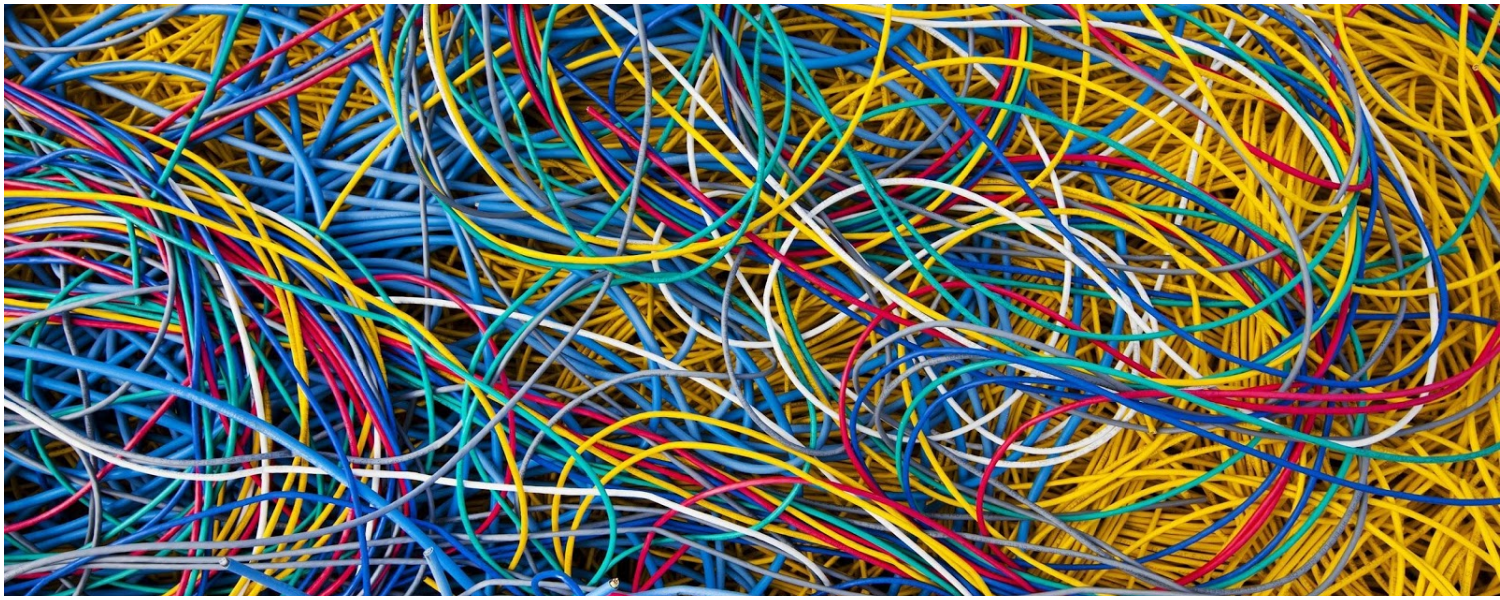
セキュリティ レポート

Google Workspace 管理者は、組織のデータが侵害される危険性について重要な情報を提供するセキュリティ レポートにアクセスできます。2 段階認証の未使用、外部アプリのインストール、ドキュメントの過剰な共有など、セキュリティ リスクの要因となるユーザーをすばやく検出できます。管理者は、セキュリティ上の脅威が疑われる場合にアラートを受信するように選択することもできます。

BigQuery を使用した分析情報

Google Workspace 管理者は、監査ログやその他の情報を BigQuery にエクスポートできます。大規模なデータ分析を目的とした Google のエンタープライズ データ ウェアハウス、BigQuery では、お客様は Google Workspace のログをパフォーマンスの良い高度なカスタムクエリによって分析できるほか、サードパーティ ツールを活用した詳細な分析を行えます。

[12] Google Workspace に標準装備。



データの復旧

最近削除したユーザーを復元する

管理者は、削除日から最大 20 日間まで、削除したユーザー アカウントを復元できます。20 日を過ぎるとユーザー アカウントは管理コンソールで完全に削除され、Google のテクニカル サポートにご連絡いただいても復元はできません。アカウントを削除できるのは、お客様の管理者のみです。

ユーザーのドライブまたは Gmail のデータを復元する

管理者は、Vault で設定された保持ポリシーに従って、データがユーザーのゴミ箱から削除されてから最大 25 日間まで、ユーザーのドライブまたは Gmail のデータを復元できます。25 日を過ぎると、テクニカル サポートにご連絡いただいてもデータを復元できません。Google は、お客様が削除したすべてのデータを、できるだけ速やかに（最長 180 日以内に）システムから削除します。

保持と電子情報開示

管理者は、Google Vault を有効にして、組織の保持と電子情報開示のニーズに合わせてデータを保持、検索、エクスポートできます。Vault は、Gmail メッセージ、Google ドライブ内のファイル、Google Meet の録画などのデータをサポートしています。

データ所在地

管理者は、データ リージョン ポリシーを使用して、対象データを特定の地理的ロケーション（米国またはヨーロッパ）に保存することを選択できます。データ リージョン ポリシーの適用対象となるのは、次の Google Workspace コアサービスのプライマリ保存データ（バックアップを含む）です。対象となるデータには、ドライブ ファイルのコンテンツ、Google Chat のメッセージと添付ファイル、Gmail のメールの件名とメッセージ、その他のコアサービスのデータが含まれます。

まとめ

顧客データの保護は Google のすべてのインフラストラクチャ、プロダクト、スタッフ業務で最も重要な考慮事項です。Google が実現できる保護の水準は、他のパブリック クラウド プロバイダや民間企業の IT チームがまず真似できない高さであると確信しています。

Google は、プライバシーとセキュリティの厳しい標準規格を満たすよう、業界のベスト プラクティスに基づいて Google Workspace を設計しました。Google は、データの所有、データの使用、セキュリティ、透明性、説明責任に関して、契約に基づく積極的な取り組みを行っています。お客様のデータやその処理はお客様が管理するものであることを約束します。たとえば、データが広告など Google Cloud サービス以外の目的で使用されることはありません。加えて、Google は、お客様がコンプライアンスや報告要件を満たすために必要となるツールも提供しています。

データの保護は Google Workspace の中核を成す要素です。そのため、セキュリティ、リソース、専門知識に対して、他社ではできない規模での投資も厭いません。Google の投資により、お客様は自社のビジネスとイノベーションに専念していただけます。Google の事業規模とセキュリティ調査コミュニティとの連携により、脆弱性への迅速な対応や、完全な防止が可能です。

このような理由から、世界中の 600 万を超える組織が、情報という最も貴重なアセットを Google に預けています。Google は Google Workspace への投資を続け、安全で透明性の高いサービスを提供していきます。