Google Cloud のセキュリティとコンプライアンスに関するホワイト ペーパー

Google のユーザーデータ保護の取り組みについて

Google Cloud

このホワイト ペーパーは、
次の G Suite サービスに適用されます

G Suite、*G Suite for Education*、*G Suite for Government*、
G Suite for Nonprofits、*Google Drive*、*and G Suite Business*

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に多くのメリットと利便性をもたらしています。社員はスマートフォンやタブレットを使ってどこからでも同時にドキュメントを共同編集でき、ビデオ通話や音声通話、インスタント メッセージ、メールで同僚と連絡を取り合うことができます。1 台のパソコンに拘束されることなく、場所や端末を問わずに仕事することが可能になりました。また企業としては、サーバーの維持や継続的なソフトウェア更新のためのコストや負担がかからないというメリットがあります。このような利点から、世界中の多数の組織がクラウドに情報を保存し、クラウドで仕事をするようになっています。

このクラウドの成長に伴い注目が集まるようになったのが、セキュリティと信頼性の問題です。これは、クラウド　サービスの運用が従来の社内導入型テクノロジーの運用とは大きく異なるためで、従来ならローカル　サーバー上にあったコンテンツが、グローバルなデータセンター ネットワーク内の Google サーバーで管理されるようになっています。以前は、インフラの運用方法や運用の責任者を社内ですべて把握できていましたが、クラウドに移行する場合は、サービスのインフラ、運用、配信の管理をクラウド　サプライヤーに依存することになります。ただしクラウド環境でも、企業の自社データについてはクラウドベースのツールやダッシュボードを使用して引き続きその企業で管理することが可能です。また、クラウドを使うことで、ユーザーはデスクトップ　パソコンだけでなく、個人のモバイル端末を使って仕事のファイルにアクセスできるようになりました。そこで重要なのが、クラウド　ソリューションのセキュリティ機能とコンプライアンスが、会社の要件を満たしているかを確認することです。そのためには、クラウド ソリューションでデータがどのように保護され、処理されるのかを理解する必要があります。このホワイト ペーパーで、セキュリティとコンプライアンスの観点から Google のテクノロジーについての理解を深めていただけましたら幸いです。

クラウドの先駆的企業として、Google　はクラウドモデルにおけるセキュリティの重要性を十分理解し、従来の社内導入型ソリューションよりも強固なセキュリティを持つクラウド サービスを設計しています。Google は自社の業務で取り扱うデータを保護するためにセキュリティに力を入れてきましたが、お客様へのサービスも同じインフラで提供していることから、これがそのままお客様のデータを保護することにもつながります。だからこそ Google はセキュリティを重視し、中でもデータの保護を最重要の設計基準としています。セキュリティを軸に社内の組織構造や研修の優先順位、雇用プロセスを構築しているほか、データセンターやそこで使われているテクノロジーも、セキュリティの観点から設計しています。脅威への対応策を含むセキュリティ対策は、Google の日々の業務や災害復旧計画の中心なのです。これはお客様のデータの取り扱いにおいても例外ではありません。強固なセキュリティを守れてこそ、アカウント管理、コンプライアンスの監査、Google がお客様に提供する証明書の品質が保たれるものと考えています。

このホワイト ペーパーでは、クラウドベースの生産性向上ツールである G Suite でのGoogle のセキュリティ、コンプライアンス対応について概要をご紹介します。G Suiteと G Suite for Education は、ユーザー数が数十万人を超える大規模な銀行や小売業者から、急速に成長している新興企業まで、世界中の 500 万を超える組織で使用されています。これらのサービスには、Gmail、カレンダー、グループ、ドライブ、ドキュメント、スプレッドシート、スライド、ハングアウト、サイト、トーク、コンタクト、Vault が含まれます。G Suite は、場所や使用端末を問わない、より効率的な新しい方法でのチーム作業を実現するように設計されています。

このホワイト ペーパーは、セキュリティとコンプライアンスという 2 つの主なセクションに分かれています。セキュリティのセクションでは、Google がユーザーのデータをどのように保護しているかに関連して、組織的、技術的なセキュリティ管理について詳しく説明します。次のコンプライアンスのセクションでは、ユーザーデータの処理方法と、組織が法規制の要件を満たす方法について説明します。

セキュリティは Google の最優先事項

Google では、明確で包括的なセキュリティの文化が全社員に行き渡っています。この文化の影響は、採用プロセス、新入社員トレーニング、入社後の継続的なトレーニング、そして認識を高めるための全社的なイベントに如実に現れています。

社員の身元調査

Google では、採用時に個人の学歴と職歴を確認するほか、社内や外部機関による身元照会を行います。また、地域の労働法や法的規制によって認められる範囲内で、犯罪歴のチェック、信用調査、入国審査の確認、セキュリティ チェックを行うこともあります。身元調査の内容は、応募先のポジションによって異なります。

全社員対象のセキュリティ トレーニング

Google のすべての社員には、オリエンテーションプロセスの一環として、またGoogle在職中にも継続的にセキュリティ トレーニングが課されます。新入社員は、オリエンテーションを通じて行動規約に同意します。行動規約は、お客様の情報を保護し、安全に保つという Google のコミットメントを明確に表明したものです。役職によっては、セキュリティ面に重点を置いた追加の研修が課される場合もあります。たとえば、情報セキュリティ チームは新しく採用されたエンジニアに対して、安全なコーディング方法、サービス設計、自動化された脆弱性テストツールといったトピックについて指導を行います。それ以外にもエンジニアは、セキュリティ関連トピックについての技術的なプレゼンテーションに参加するほか、新たな脅威や攻撃パターン、リスク軽減テクニックなどを取り上げたセキュリティ ニュースレターを受け取ります。

セキュリティとプライバシーに関する社内イベント

Google では、セキュリティについての認識を高め、セキュリティとデータのプライバシーに関するイノベーションを促進するために、全社員が参加できる社内会議を定期的に開催しています。セキュリティとプライバシーは常に進化している分野であり、社員に積極的に参加してもらうことが認識を高めるうえで重要だと Google は考えています。 1 つの例として、「Privacy Week」があります。この期間中は世界各国のオフィスで、ソフトウェア開発からデータの取り扱い、ポリシーの適用、プライバシーの原則まで、あらゆる側面からプライバシーについての認識を高めるイベントを開催します。また、定期的に開催する「Tech Talks」でも、セキュリティとプライバシーにかかわるテーマを頻繁に取り上げています。

Google には、ソフトウェア エンジニアリングと オペレーション担当部門に セキュリティとプライバシーを 専門とする 550 名以上の 常勤社員が在籍しており、 情報、アプリケーション、ネット ワークのセキュリティにかけて は世界でも有数のエキスパート が含まれています。

セキュリティ専任チーム

Google には、ソフトウェア エンジニアリングとオペレーション担当部門にセキュリティとプライバシーを専門とする 550 名以上の常勤社員が在籍しており、情報、アプリケーション、ネットワークのセキュリティにかけては世界でも有数のエキスパートが含まれています。チームの仕事は、会社の防御システムの維持、セキュリティ確認プロセスの開発、セキュリティ インフラの構築、Google のセキュリティポリシーの適用です。Google のセキュリティ専任チームは、他社製のツール、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 セキュリティ審査を通してセキュリティの脅威を徹底的に調査します。

Google 社内の情報セキュリティ チームのメンバーは、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を審査し、Google のサービスを担当するチームとエンジニアリング チームにプロジェクト単位でのコンサルティング サービスを提供します。また、Google ネットワークでの不審な挙動を監視して情報セキュリティ上の脅威を特定し、定期的にセキュリティの評価と監査を行います。さらに、外部の専門家と連携して定期的なセキュリティ評価も実施しています。Google は、Project Zero という常勤スタッフのチームを構成し、標的型の攻撃を防ぐことを目的としてソフトウェア ベンダーにバグを報告し、外部データベースに登録しています。

セキュリティ チームは、Google ソリューションを使用しているユーザーだけでなく、より広い範囲のインターネット ユーザー コミュニティを保護するために、調査や対外的な活動にも従事しています。このような調査で見つかった例として、POODLE SSL 3.0 の脆弱性や暗号サービス ソフトウェアの弱点があります。セキュリティ チームはセキュリティ調査報告書を発行し、一般に公開しています。また、オープンソース プロジェクトや学術的な会議を主催し、自らも参加しています。

プライバシー専任チーム

Google プライバシー チームは、サービス開発部門やセキュリティ部門とは独立して運営されていますが、すべての Google サービスのリリースに参加し、設計文書を審査したりコードレビューを実施したりして、プライバシー要件に沿っていることを確認しています。また、お客様データを扱うサービスが設計通りに Google のプライバシー ポリシーに沿って動作することを確認するために、一連の自動監視ツールを構築しています。このチームは、厳正なプライバシー基準を反映したサービスをリリースするために貢献しています。その基準とは、ユーザーデータを透明性のある方法で収集し、ユーザーと管理者にとって有効なプライバシー設定項目を提供するとともに、Google プラットフォームに保存された情報を適切に保護することです。サービスのリリース後、プライバシー チームは自動化されたプロセスを監視し、データ トラフィックを監査して、適切なデータ利用が行われているかどうかを確認します。さらに、実施する調査を通じて、新しい技術に適用するプライバシーのあり方について提案する役割を果たします。

内部監査とコンプライアンスの専門要員

Google　は専任の内部監査チームを設けており、このチームは世界中のセキュリティに関する法規制への準拠について審査します。新しい監査基準が作成されると、内部監査チームは、その基準を満たすためにどのような管理機能、プロセス、システムが必要かを判断します。また、第三者による独立した監査と評価を促進し、サポートします。

セキュリティ リサーチ コミュニティとの連携

Google は長きにわたりセキュリティ リサーチ コミュニティとの密接な関係を築いてきており、G Suite やその他の Google サービスの脆弱性を発見するうえで、この連携に大きな価値があると考えています。Google　の脆弱性報告の報奨制度は、お客様のデータを危険にさらす可能性がある設計と実装の問題の報告に協力をお願いする制度で、数万ドル単位の報奨金が用意されています。たとえば　Chrome では、不正なソフトウェアやフィッシングに注意していただくようユーザーに促し、セキュリティのバグ発見に対して報奨金を設けています。リサーチ　コミュニティとの連携によって、Google は Chrome のセキュリティ バグを 700 件以上修正し、総計 125　万ドルを超える報奨金を提供しました。脆弱性報告の報奨プログラム全体で提供した報奨金は、200 万ドルを超えます。Google はご協力いただいた方々に会社として謝意を表明し、Google のプロダクトやサービスへの貢献者としてお名前を掲載しています。

運用上のセキュリティ

セキュリティは、補足や一時的な取り組みではなく、Google の業務において重要な位置を占めています。

脆弱性の管理

Google　は、他社製のツールと専用の目的で作成された社内ツールの組み合わせ、自動または手動による侵入テスト、品質保証プロセス、ソフトウェアのセキュリティ審査、外部監査などを通じてセキュリティの脅威を徹底的に調査する、脆弱性の管理プロセスを運用しています。脆弱性管理チームは、脆弱性のトラッキングとフォローアップを担当します。修正が必要な脆弱性が特定されると、ログに記録され、重大度に応じて優先順位が設定されてから担当者に割り振られます。脆弱性管理チームは、このような問題をトラッキングし、修正が確認されるまで頻繁にフォローアップを行います。また、Google は、セキュリティ リサーチ コミュニティのメンバーと連携して、Google サービスとオープンソース ツールで報告された問題をトラッキングしています。セキュリティに関する問題の報告について詳しくは、Google アプリケーション セキュリティに関するページをご覧ください。

不正なソフトウェアによる被害の防止

不正なソフトウェアによる巧妙な攻撃によってアカウントが不正使用されたり、データが盗まれたり、ネットワークへの侵入が行われたりする可能性があります。Google は、ネットワークやユーザーへのこのような脅威を深刻に受け止め、さまざまな手段を講じて不正なソフトウェアの検出、被害の防止、根絶に努めています。また、Google Chrome、Mozilla Firefox、Apple Safari のユーザーが、個人情報の不正入手やコンピュータの乗っ取りを目的としたソフトウェアがインストールされる可能性のあるウェブサイトにアクセスしようとしたときに警告を表示して、毎日数億人のユーザーが自分の身を守れるようにしています。不正なソフトウェアを含むサイトやメール添付ファイルは、個人情報や ID の不正入手、他のコンピュータへの攻撃を目的として、悪意のあるソフトウェアをユーザーのコンピュータにインストールします。これらのサイトにユーザーがアクセスすると、ユーザーのコンピュータ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。不正なソフトウェアに対する Google の戦略は、感染を防ぐことから始まります。手動および自動のスキャナを使って、不正なソフトウェアやフィッシングの媒介となっている可能性のあるウェブサイトを Google の検索インデックスから削除します。およそ 10 億人のユーザーが Google のセーフ ブラウジングを日常的に使用しています。Google のセーフ ブラウジング テクノロジーは、安全でないウェブサイトを見つけるために 1 日あたり数十億個の URL を検査しています。毎日、数千個の安全でないウェブサイトが新たに見つかっており、その多くは正当なウェブサイトが不正使用されているケースです。安全でないサイトが見つかった場合、Google 検索とウェブブラウザに警告が表示されます。Google では、セーフ ブラウジング ソリューション以外にも、ファイルや URL の無料オンライン分析サービスである VirusTotal を提供しています。このサービスを使用すると、ウィルス対策エンジンとウェブサイト スキャナによって検出されたウィルス、ワーム、トロイの木馬やその他の不正なコンテンツを具体的に確認できます。VirusTotal の使命は、無料のツールやサービスの開発を通して、ウィルス対策およびセキュリティ業界の発展に寄与し、インターネットの安全性を高めることです。

Google は、ウィルス定義ファイルで検出できなかった不正なソフトウェアを検出するために、Gmail、ドライブ、サーバー、ワークステーション上で複数のウィルス対策エンジンを使用しています。

Google は、Google Chrome、Mozilla Firefox、Apple Safari のユーザーが、個人情報の不正入手やコンピュータの乗っ取りを目的としたソフトウェアがインストールされる可能性のあるウェブサイトにアクセスしようとしたときに、警告を表示して、毎日数億人のユーザーが自分の身を守れるようにしています。

監視

Google のセキュリティ監視プログラムは、内部ネットワーク トラフィックやシステム上での社員の操作から収集された情報、外部の脆弱性情報を重点的に監視しています。Google のグローバル ネットワークでは内部トラフィックを監視し、不審な挙動（ボットネット接続の可能性を示すトラフィックなど）をさまざまなポイントでチェックしています。この分析は、トラフィックをキャプチャ、解析するためのオープンソース ツールと商用ツールを組み合わせて実行されます。Google のテクノロジーに基づいて構築された独自の相関システムもこの分析をサポートしています。システムログを分析することもネットワーク分析を補完する役割を果たします。これにより、お客様のデータに対するアクセスの試みなどの不審な挙動を特定できます。Google のセキュリティ エンジニアは、検索アラートを公開データ リポジトリに設定し、会社のインフラに影響を及ぼす可能性のあるセキュリティ インシデントがないかを調べます。また、受け取ったセキュリティ レポートの確認や、公開メーリング リスト、ブログ投稿、Wiki ページの監視を徹底的に行います。正体不明の脅威がいつ発生する可能性があるのかを判断するには自動ネットワーク分析が役に立ちます。この分析により、Google セキュリティ スタッフへのエスカレーションが行われます。また、システムログの自動分析は、ネットワーク分析を補完する役割を果たします。

インシデントの管理

Google では、システムやデータの機密性、完全性、可用性に影響する可能性のあるセキュリティ イベントに対して、厳正なインシデント管理プロセスを確立しています。インシデントが発生すると、セキュリティ チームがそのインシデントをログに記録し、重大度に応じて優先順位を設定します。お客様に直接影響が及ぶ事例は、最優先で処理されます。このプロセスでは、アクション、通知、エスカレーション、緩和策、文書化の手順が指定されています。Google のセキュリティ インシデント管理プログラムは、インシデントの処理に関する NIST ガイダンス（NIST SP 800-61）に基づいて構築されています。主なスタッフは、問題の発生に備えて、調査や証拠の取り扱いに関するトレーニングを受けています。これには、サードパーティ製または自社製のツールの使用方法も含まれています。重要な項目（お客様の機密情報が格納されているシステムなど）に対してはインシデント レスポンス計画のテストが行われます。これらのテストでは、内部からの脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。Google セキュリティ チームは、セキュリティ インシデントを迅速に解決できるように、すべての Google 社員からの問い合わせに 24 時間 365 日対応します。インシデントにお客様のデータが関係する場合、Google または Google のパートナーからお客様に連絡し、サポートチームが調査作業をサポートします。

セキュリティを中核としたテクノロジー

G Suite は、安全に動作するように考慮、設計、構築されたテクノロジー プラットフォーム上で稼働します。Google はハードウェア、ソフトウェア、ネットワーク、システム管理のテクノロジーに革新をもたらす企業す。Google は自社サーバー、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独自に設計しており、さらに、「多層防御」の原則に基づいて、従来のテクノロジーよりも安全で管理の容易な IT インフラを構築しています。

最先端のデータセンター

データのセキュリティと保護を重視することは、Google の重要な設計基準の一つです。Google のデータセンターでは物理的なセキュリティとして、特注の電子アクセスカード、警報、車両侵入防止機構、敷地の境界フェンス、金属探知機、生体認証を含む多層セキュリティ モデルを採用しています。また、内部にはレーザーによる侵入検知システムが導入されています。Google のデータセンターは、侵入者を検知して追跡できる高解像度の屋内カメラと屋外カメラによって 24 時間 365 日監視されており、インシデントが発生した場合には、アクセス

ログ、アクティビティ記録、カメラの録画データを利用できます。また、厳正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を行っています。データセンター内部に近づくほど、より多くの安全保護対策が講じられており、内部にはセキュリティ通路からしかアクセスできません。セキュリティ通路には、セキュリティ　バッジや生体認証を使用した多元的なアクセス管理が行われています。特定の役割を持つ承認された社員のみが入ることができ、データセンターに足を踏み入れたことがある社員は実に 1% 未満です。

データセンターの電力供給

24 時間年中無休で稼働する中断のないサービスを保証するために、Google のデータセンターは冗長電源システムと環境制御装置を備えています。データセンターのすべての重要な機器には、同等の出力を持つ主電源と代替電源が用意されています。ディーゼル　エンジン式の補助発電装置は、緊急時に各データセンターを最大出力で稼働させるのに必要な電力を供給することができます。冷却システムはサーバーやその他のハードウェアの動作温度を一定に保ち、サービス停止のリスクを抑えます。火災検知および消火装置はハードウェアの損傷を防ぎます。熱や火災、煙を感知すると、影響が及ぶエリア、セキュリティ　オペレーション　コンソール、リモート監視デスクで警報音が鳴り、警報信号が発生します。

環境への影響

Google　は、データセンターの稼働による環境への影響を抑えるために、Google　独自の施設を設計し、建築しています。高度な温度制御装置を設置し、外気や再利用水を冷却に使用する「フリークーリング」技術を採用しているほか、配電設備の設計を見直して不要なエネルギー損失の削減を図っています。改善効果を確かめるために、包括的な効率性測定基準を用いて各施設のパフォーマンスを測定します。Google　は主要なインターネット　サービス企業として初めて、すべてのデータセンターで環境への配慮、職場の安全性、エネルギー管理の各基準について外部の認定を取得しました。具体的には、ISO 14001、OHSAS 18001、ISO 50001 を自主取得しました。これらの認定は、目標とその実行計画を宣言し、それを実行しているかというきわめてシンプルな基準に基づいて策定されています。

カスタム サーバー ハードウェアとソフトウェア

Google　のデータセンターは、エネルギー効率に優れた目的特化型のカスタム　サーバーとネットワーク機器 で構成されており、Google　はそれらを独自に設計、製造しています。多くの市販ハードウェアとは異なり、Google のサーバーには、脆弱性を招く可能性があるビデオカード、チップセット、周辺機器のコネクタなどの不要なコンポーネントは含まれていません。Google　の実稼働サーバーでは、余分な機能を取り除いて堅牢性が増した Linux をベースにカスタマイズされたオペレーティング システム（OS）が実行されています。Google のサーバーと OS は、Google のサービスを提供することだけを目的として設計されています。サーバーのリソースは動的に割り振られるため拡張性があり、お客様の需要に基づいてリソースの追加または再割り当てを行って、迅速かつ効率的に適応できます。この均質な環境は、システムを継続的に監視してバイナリの変更を検出する独自のソフトウェアによって管理されます。標準の Google イメージと異なる変更が検出されると、システムは自動的に正式な状態に戻されます。これらの自動化された自己修復メカニズムにより、Google　はシステムを不安定にするイベントを監視し、修正できます。また、インシデントについての通知を受け取り、ネットワークに対する攻撃の進行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、データセンター内のすべての機器の設置場所と状態を、機器の取得から設置、使用停止、廃棄に至るまで、バーコードと資産タグを使って細かく追跡します。許可なくデータセンターから機器が持ち出されることがないように、金属探知機と監視カメラが導入されています。コンポーネントがライフサイクルのいずれかの時点で性能テストに不合格となった場合、インベントリから削除されて使用停止となります。ハードディスクの使用を停止する場合、承認された社員が、ディスクのデータが消去されたことを確認します。データを消去するときは、ディスクにゼロを書き込んだ後、複数の手順からなる検証プロセスを実行してディスクにデータが残っていないことを確認します。なんらかの理由でディスクのデータを消去できない場合、ディスクは物理的に破壊できるときまで安全に保管されます。ディスクの物理的な破壊は複数段階からなるプロセスです。最初にディスクをクラッシャーで変形させ、次にシュレッダーで粉砕した後、安全な施設でリサイクルします。各データセンターは厳格な廃棄ポリシーを遵守し、逸脱があれば直ちに是正措置が取られます。

セキュリティ上の独自のメリットを持つグローバル ネットワーク

Google の IP データネットワークは、Google 独自の通信網、公衆通信網、海底ケーブルで構成され、可用性が高く待ち時間の少ないサービスの提供を実現しています。

他のクラウド サービスや社内導入型のソリューションでは、公共のインターネットでお客様のデータを装置から装置へ複数回転送する（「ホップ」と呼ばれる）必要があります。ホップの回数は、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、回数が増えれば、データが攻撃を受けたり傍受されたりする可能性が高くなります。Google のグローバル ネットワークは世界中の大部分の ISP にリンクされているため、公共のインターネットでのホップ数を制限することによって、転送中のデータのセキュリティを高めています。

多層防御とは、Googleのネットワークを外部攻撃から保護する複数層の防御体制のことです。Googleのセキュリティ要件を満たす承認されたサービスとプロトコルのみがGoogleのネットワークを通過でき、その他はすべて自動的に拒否されます。ネットワークの分離を適用するために業界標準のファイアウォールとアクセス制御リスト（ACL）が使用されています。すべてのトラフィックはカスタム GFE（Google フロントエンド）サーバー経由でルーティングされ、悪意のあるリクエストと分散サービス妨害（DDoS）攻撃の検出および停止が行われます。さらに、GFE サーバーは内部で制御されているリストにあるサーバーとのみ通信を許可されます。この「デフォルトで拒否」の設定は、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します。不正なコードやプログラミング エラーを発見するために、ログは定期的に調べられます。ネットワークに接続されている装置へのアクセスは、承認された担当者だけに制限されています。

Google の IP データ ネットワークは、Google 独自の通信網、公衆通信網、海底ケーブルで構成され、可用性が高く待ち時間の少ないサービスの提供を実現しています。

転送中や保管中のデータ、バックアップ メディア上のデータの暗号化

G Suite のお客様のデータは、ディスク上やバックアップ メディア上だけでなく、インターネットやデータセンター間での転送中も暗号化されています。お客様のデータ セキュリティに関する懸念に対処する暗号化ソリューションを提供することは、Google のコミットメントです。暗号化は、Google がセキュリティに取り組む上で重要な役割を果たし、メール、チャット、Google ドライブ ファイル、その他のデータの保護に役立ちます。転送中や保管中のデータ、バックアップ メディア上のデータを保護する方法と、暗号化鍵管理について詳しくは、G Suite における暗号化に関するホワイト ペーパーをご覧ください。

待ち時間が少なく可用性の高いソリューション

Google のプラットフォームのコンポーネントは、高度な冗長性を持つように設計されています。この冗長性は、サーバー設計、データ保存方法、ネットワークおよびインターネット接続、ソフトウェア サービス自体にも反映されています。この、あらゆるものに冗長性を備える対処には設計エラーの処理も含まれており、単一のサーバー、データセンター、またはネットワーク接続に依存しないソリューションを実現しています。Google のデータセンターは地理的に分散しているため、自然災害や停電などによる地域的なサービス中断が最小限に抑えられます。ハードウェア、ソフトウェア、またはネットワークに障害が発生した場合、データは自動的に 1 つの施設から別の施設に切り替えられるため、G Suite のユーザーはほとんどの場合、サービスが中断されることなく作業を継続できます。世界各地に社員を抱えるお客様は、改めて設定を行ったり費用をかけたりすることなく、ドキュメントやビデオ会議などでの共同作業を続けられます。グローバル チームは、高パフォーマンスで待ち時間の少ない環境を共有し、単一のグローバル ネットワークで作業できます。

また、自然災害や停電などの影響を最小限に抑えるため、データセンターを各地に分散させています。

また、高度な冗長性を備えた Google のインフラは、お客様をデータ損失から保護します。G Suite では、RPO（目標復旧時点）の目標はゼロで、RTO（目標復旧時間）の設計目標もゼロです。Google は、これらの目標をライブ複製または同期複製によって達成することを目指しています。G Suite サービス内でお客様が行った操作は同時に 2 つ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、データはお客様の操作が反映されている他方のデータセンターに転送されます。お客様のデータはランダムなファイル名を持つデジタルの小片（ピース）に分割されます。お客様のコンテンツまたはファイル名が、そのまま判読可能な形式で保存されることはありません。また、保存されたお客様のデータをストレージで調べても、特定のお客様またはアプリケーションにたどりつくことはありません。単一障害点を避けるために、各ピースはほぼリアルタイムで複数のディスク、複数のサーバー、複数のデータセンターに複製されます。さらに、最悪の事態に備えるために、災害復旧訓練を実施しています。この訓練では、個々のデータセンターと本社が 30 日間使用できなくなったと想定します。Google では、現実的なシナリオについて準備態勢ができているかどうかを定期的にテストするとともに、宇宙人やゾンビの襲来のような空想的な危機に対する態勢もテストします。

高度に冗長な設計により、Google はここ数年 Gmail で年間 99.984% の稼働時間を達成しており、**計画的なダウンタイムは一切ありません**でした。プラットフォームを修正またはアップグレードする必要があるときでも、ユーザーにダウンタイムやメンテナンス時間枠の影響が及ぶことはありません。

サービスの可用性

Googleの一部のサービスは、地域によって利用できないことがあります。多くの場合、これはネットワーク停止による一時的なものですが、政府による強制的な遮断に起因する永続的なものもあります。Google の透明性レポートには、Google のサービスに対する最近の継続的なトラフィックの遮断が示されています。このデータを提供する目的は、人々がオンライン情報を分析し、その利用可能性を理解できるようにするためです。

独立した第三者による認定

Google のお客様と規制機関は、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ついて、独立した検証がなされることを期待しています。これに応えるために、Google は定期的にいくつかの独立した第三者機関による監査を受け、データセンター、インフラ、オペレーションについての調査を行っています。定期的な監査では、ISO 27001、ISO 27017、ISO 27018、SOC 2、SOC 3 の監査規格へのコンプライアンスがチェックされます。また、米国連邦政府によるリスクおよび認証管理プログラム（FedRAMP）へのコンプライアンスもチェックされます。お客様が G Suite を検討する際、これらの認定は、Google のサービス パッケージがお客様のセキュリティ、コンプライアンス、データ処理のニーズを満たすことを確認するうえで役立ちます。

ISO 27001

ISO 27001は最も広く認識されて受け入れられている独立したセキュリティ規格の 1 つです。Google は、G Suite を実行するシステム、テクノロジー、プロセス、データセンターについて ISO 27001 を取得しています。Google の国際的な規格へのコンプライアンスは、オランダ国認証機関（国際認定フォーラム（IAF）のメンバー）によって認可された ISO 認証機関である Ernst & Young CertifyPoint によって認定されています。Google の ISO 27001 認定と認定範囲については、こちらのドキュメントでご確認いただけます。

ISO 27017

ISO 27017 は、クラウド サービスに特化した、ISO/IEC 27002 に基づく情報セキュリティ制御の実践に関する国際標準です。Google　の国際的な規格へのコンプライアンスは、オランダ国認証機関（国際認定フォーラム（IAF）のメンバー）によって認可された ISO 認証機関である Ernst & Young CertifyPoint によって認定されています。Google の ISO 27017 認定については、こちらでご確認いただけます。

ISO 27018

ISO 27018 は、パブリック クラウド サービスにおける個人識別情報（PII）の保護の実践に関する国際標準です。Google　の国際的な規格へのコンプライアンスは、オランダ国認証機関（国際認定フォーラム（IAF）のメンバー）によって認可された　ISO 認証機関である Ernst & Young CertifyPoint によって認定されています。Google の ISO 27018 認定については、こちらでご確認いただけます。

SOC 2 / 3

2014年、AICPA（米国公認会計士協会）のASEC（保証業務特別委員会）は、TSP（Trust　サービスの原則と規準）の改訂版を発表しました。SOC（サービス提供組織の内部統制）は、プライバシー以外の原則についての監査フレームワークであり、対象範囲にはセキュリティ、可用性、処理の完全性、機密性が含まれます。Google は SOC 2 と SOC 3 の両方の報告書を取得しています。Google の SOC 3　報告書は、こちらからダウンロードできます。非開示契約を締結する必要はありません。SOC　3　は、セキュリティ、可用性、処理の完全性、機密性の原則に対する Google のコンプライアンスを保証するものです。

FedRAMP

FedRAMP　は、米国連邦政府によるリスクおよび認証管理プログラムで、クラウドの製品やサービスのセキュリティ評価、認証、および継続的なモニタリングに関する標準的なアプローチを提供しています。このアプローチは、米国政府機関によるセキュリティ評価にかかる時間を短縮し、安全なクラウド　ソリューションへの移行を促進することを目的としています。Google は G Suite と App Engine に関して FedRAMP の ATO（運用権限）の承認を受けています。

データ利用

Google の哲学

G Suite ユーザーのデータの所有者はユーザー自身であり、Google ではありません。G Suite を利用する組織や個人が Google のシステムに保存するデータは、それぞれの組織や個人のものであり、Google がそのデータを広告の目的でスキャンしたり、第三者に販売したりすることはありません。Google は、お客様のデータの保護に対する Google のコミットメントを定めた、詳細なデータ処理の修正条項をお客様に提供しています。また、お客様がデータを削除した場合、Google は 180 日以内にシステムからデータを削除することを保証します。さらに、お客様の管理者が Google のサービスの使用を停止する場合、データを簡単に取り出すことができるツールを提供します。解約金や追加費用を課すことはありません。

G Suite での広告非表示

G Suite コアサービスに広告は表示されません。今後もこの方針を変更する予定はありません。G Suite コアサービスにおいて Google が広告の目的でデータを収集、スキャン、使用することはありません。お客様の管理者は、G Suite 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 はお客様のデータをインデックスに登録して、迷惑メールのフィルタリング、ウィルスの検出、スペルチェック、個人アカウントでのメールやファイルの検索機能などの有益なサービスを提供します。

データアクセスと制限

管理アクセス

データを非公開で安全に保つために、Google はお客様の G Suite データを、他のお客様やユーザーのデータから論理的に分離します（データが同じ物理サーバーに保存されている場合を含みます）。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割に基づいており、権限を最小限にし、知る必要がある人物にだけ知らせるという考え方に基づいて、アクセス権を定義済みの職責に対応付けています。Google 社員には、デフォルトでは、社員用メールや社内ポータルといった会社のリソースにアクセスするための制限されたアクセス権限のみが付与されます。追加アクセス権を要求する場合は、正式なプロセスに沿ってリクエストを行い、Google のセキュリティ ポリシーの規定に従って、データやシステムのオーナー、マネージャー、またはその他の上級管理職から承認を得る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査レコードが維持されます。このツールで承認設定の変更と承認プロセスの両方を

管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、G Suite サービス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。サポート サービスは、複数の方法による身元確認を経て承認された、お客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによって監視、監査されます。

お客様の管理者

お客様の組織内における G Suite の管理者の役割と権限はお客様によって設定、管理されます。これは、個々のチームメンバーが、すべての設定やデータへのアクセス権を取得することなく、特定のサービスの管理や、特定の管理機能を実行できることを意味します。統合された監査ログに管理操作の詳細な履歴が記録され、これはお客様がデータへの内部アクセスや自社ポリシーの遵守を監視する際に役立ちます。

法令によるデータ提供要請

法令によるデータ提供要請への対応は、主にデータ所有者であるお客様に行っていただくことになります。ただし、他のテクノロジー企業や通信企業と同じように、Google は世界各国の政府や裁判所から、あるユーザーが Google のサービスをどのように使用したかについて、直接データ提供要請を受けることがあります。Google は法的な義務を果たしながら、お客様のプライバシーを保護し、過剰な要請を制限するための手段を講じます。法令による要請に従う場合でも、お客様が保存したデータのプライバシーとセキュリティを守ることが Google の優先事項であることに変わりありません。このような要請を受けた場合、社内のチームが審査を行い、要請が法的要件と Google のポリシーを満たしていることを確認します。一般的に、Google が要請に従うためには、要請が書面でなされること、要請元機関の適切な権限を持つ役職者によって署名されていること、適切な法律のもとで発行されていることが必要です。要請の範囲が過剰に広いと判断される場合は、範囲を狭めることを試み、必要に応じて差し戻すこともよくあります。たとえば 2006 年、Google は主要な検索サービス提供企業として唯一、2 か月分のユーザー検索キーワードの提出を求める米国政府の要請を拒否しました。Google は召喚に異議を唱え、最終的に政府の要請は裁判所によって否決されました。場合によっては、1 つの Google アカウントに関連したすべての情報の提供を要請されることがあります。このケースでは、Google は要請した機関に”対して、特定のプロダクトやサービスに限定するよう求めます。Google は、ユーザーには政府から Google に要求されるユーザー情報の範囲を厳密に知る権利があると考えます。そのため Google は、企業として初めて、政府からのデータ提供要請に関するレポートを定期的に発行するようになりました。データ提供要請と Google の対応についての詳細情報は、Google の透明性レポートでご確認いただけます。Google は、法律または裁判所命令によって明示的に禁止されていない限り、お客様のデータに関する要請についてお客様に通知することをポリシーとしています。

Google は、ユーザーには政府から Google に要求されるユーザー情報の範囲を厳密に知る権利があると考えます。そのため Google は、企業として初めて、政府からのデータ提供要請に関するレポートを定期的に発行するようになりました。

サードパーティのサプライヤー

Googleでは、サービスを提供するためのデータ処理については実質的に自社で行っていますが、カスタマー サポートや技術サポートなどの G Suite 関連サービスの提供については、必要に応じてサードパーティのサプライヤーと契約しています。サードパーティのサプライヤーと契約する前に、Google はそのサプライヤーのセキュリティやプライバシーに関する活動を評価し、データへのアクセスや提供するサービスの範囲に対して適切なレベルのセキュリティとプライバシーを保てていることを確認します。Google がサードパーティのサプライヤーによって生じるリスクを評価した後、サプライヤーは、適切なセキュリティ、機密性、プライバシーの条件を定めた契約を結ぶことを求められます。

法規制への準拠

Google のお客様は、さまざまな法規制に準拠するための[コンプライアンス]のニーズを抱えています。お客様の企業が、金融、製薬、製造などの規制産業にまたがって運営されている場合もあります。

Google は契約により次の内容をお約束しています。

- 契約期間中、Google は ISO 27001、ISO 27018、SOC 2 / 3 の監査基準を遵守します。
- 規定されたセキュリティ標準。Google は、規定された特定のセキュリティ標準に従ってデータの処理、保管、保護の方法を定義します。
- データ プライバシー責任者へのアクセス。お客様は Google のデータ プライバシー責任者に対して質問やコメントを行うことができます。
- データのポータビリティ。管理者は、契約期間中いつでもお客様データを[標準形式]で書き出すことができます。Google はデータの書き出しに対して料金を請求しません。

データ処理の修正条項

Googleはデータ処理に対するコミットメントについてグローバルな対応を取ります。Googleも多くのお客様企業も、グローバルな環境で運営されています。G Suite は[データ処理の修正条項]と [EU モデル契約条項]を提供することで、司法管区固有の法律や規制への準拠を促進します。お客様の組織で Google のデータ処理の修正条項に同意する場合は、[ヘルプセンター]にある手順に沿ってください。

EU データ保護指令

第 29 条作業部会は、データの保護とプライバシーに関する独立したヨーロッパの諮問機関です。クラウド コンピューティング プロバイダと契約する際にヨーロッパのデータ プライバシー要件を満たすためのガイダンスを提供しています。Google は、第 29 条作業部会によるデータ保護の推奨条件のために開発された機能を提供し、契約により遵守する旨をお約束します。

EU のモデル契約条項

2010 年、欧州委員会は指令の要件に準拠する手段としてのモデル契約条項を承認しました。この決定により、特定の条項を契約に統合すれば、指令適用対象のプロバイダから EU または欧州経済領域の外部のプロバイダに個人データを転送することができるようになりました。Google はヨーロッパに広範な顧客基盤を持っているため、EU モデル契約条項を採用し、指令に準拠するための追加設定をお客様に行っていただけるようにしています。

米国 HIPAA（医療保険の相互運用性と説明責任に関する法律）

G Suite はお客様の米国 HIPAA（医療保険の相互運用性と説明責任に関する法律）への準拠をサポートします。HIPAA は、保護対象となる保険情報（PHI）の機密性とプライバシーを規定します。HIPAA の適用対象であり、G Suite を使用して PHI を扱うことを希望されるお客様は、Google との業務提携契約（BAA）を締結していただく必要があります。BAA の適用範囲は Gmail、Google カレンダー、Google ドライブ、Google サイト、Google Vault です。詳しくは Google の HIPAA 実装ガイドでご確認いただけます。

米国 FERPA（家庭教育の権利とプライバシーに関する法律）

3,000 万人を超える生徒が G Suite for Education を使用しています。G Suite for Education は FERPA（家庭教育の権利とプライバシーに関する法律）に準拠しており、準拠を保証する旨を契約にも明記しています。

米国 COPPA（児童オンライン プライバシー保護法、1998 年）

児童のオンライン データの安全を確保することは Google にとって重要です。Google では G Suite for Education を使用する学校に対し、COPPA の要求に従い Google のサービスを使用することに関して保護者の同意を得るよう契約で求めており、学校は、COPPA に準拠した形で Google のサービスを使用することができます。

セキュリティとコンプライアンスの向上を目的としたユーザーと管理者の権限の強化

Google のインフラ、テクノロジー、オペレーション、お客様データへのアプローチにはセキュリティ対策が施されており、この強固なセキュリティのインフラとシステムは、すべての G Suite ユーザーのデフォルトの環境になっています。しかし、ユーザーにはこの範囲にとどまらず、ダッシュボードやアカウント セキュリティ ウィザードを使って個人のセキュリティ設定を拡張、カスタマイズしてビジネス ニーズを満たすことができるように、積極的に権限が与えられます。また、G Suite では、管理者は組織の規模にかかわらず、管理コンソールのダッシュボードからインフラ、アプリケーション、システム統合のすべてを一元的に管理できるので、管理や設定の業務にかかる労力が軽減されます。たとえば、社内導入型のメールシステムにDKIM（フィッシング防止機能）を導入する場合、管理者はすべてのサーバーに対して個別に修正プログラムの適用と設定を行う必要があり、設定の間違いはサーバー停止の原因になります。G Suite の管理コンソールを使用すれば、数千単位、数十万単位のアカウントすべてに数分で簡単に DKIM を設定でき、しかも停止やメンテナンス期間は不要です。管理者は多数のツールを各自の判断で使用できます。たとえば、2 段階認証プロセスやシングル サインオンのような認証機能を使用したり、セキュア トランスポート（TLS）などのメール セキュリティ ポリシーを適用したりすることが可能です。これらのツールは組織のセキュリティやシステム統合の要件に合わせて設定できます。セキュリティとコンプライアンスのニーズに合わせて G Suite をカスタマイズするために役立つ主要な機能のいくつかを次に示します。

ユーザー認証と承認の機能

2 段階認証プロセス

2 段階認証プロセスを使用すると、ログイン時にユーザー名とパスワードに加えて確認コードの入力を要求することにより、G Suite アカウントの安全性が向上します。たとえば、ユーザーのパスワードが流出した場合でも、不正なアクセスが行われるリスクが大幅に軽減されます。確認コードはユーザーの Android、BlackBerry、iPhone などのモバイル端末に配信され、使用できるのは 1 回限りです。管理者はいつでも、自組織のドメインで 2 段階認証プロセスを有効に設定できます。

セキュリティ キー

セキュリティ キーを使用すると、2 段階認証プロセスの安全性をさらに高めることができます。Google は FIDO Alliance という標準化団体と連携してセキュリティ キーを開発しました。セキュリティ キーは Google アカウントへのアクセスに使用する物理キーです。セキュリティ キーではコードではなく暗号化された署名が送信されるので、ログイン情報がフィッシングされる危険性を回避できます。Google Cloud 管理者は、管理コンソールに新たに加わった設定を使用することで、セキュリティ キーを簡単に導入、監視、管理できます。追加のソフトウェアをインストールする必要はありません。IT 管理者は、使用状況の追跡情報やレポートを確認することで、従業員が最後にセキュリティ キーを使った場所や日時を把握できます。セキュリティ キーを紛失してしまった場合、管理者はそのキーへのアクセスを簡単に取り消して予備のコードを伝えることができるので、従業員は再度ログインして作業を続けることができます。

シングル サインオン（SAML 2.0）

G Suite はシングル サインオン（SSO）サービスに対応しています。このサービスを使用すると、ユーザーは同じログ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ます。シングル サインオンは SAML 2.0 の技術を使用しています。SAML 2.0 は、セキュリティで保護されたウェブドメインでのユーザー認証と承認のためのデータ交換を可能にする XML 標準です。高セキュリティな認証を行うため、SSO を利用するには、RSA または DSA のいずれかのアルゴリズムを使用して生成された公開キーと証明書を登録する必要があります。お客様の組織では、SSO サービスを使用して G Suite のシングル サインオンを自組織の LDAP またはその他の SSO システムに統合できます。

OAuth 2.0 と OpenID Connect

G Suite は、OAuth 2.0 と OpenID Connect をサポートしています。これは認証と承認のためのオープンなプロトコルで、このプロトコルを使うことで、お客様は複数のクラウド ソリューションにシングル サインオン サービス（SSO）を設定できます。ユーザーは、認証情報を再入力したり、機密性の高いパスワード情報を共有したりすることなく、G Suite からサードパーティのアプリケーションにログインできます。逆もまた同じです。

データ管理機能

IRM（Information Rights Management）

IRM（Information Rights Management）を使用することにより、共有の詳細メニューからのダウンロード、印刷、コピーを無効にできます。これは、ファイル共有の相手が特定の少人数のユーザーに限定されている場合に適しています。この設定は、Google ドキュメントで作成したドキュメント、スプレッドシート、プレゼンテーションなど、Google ドライブに保存されるすべてのファイルに対して適用できます。

また、G Suite では
管理者は組織の規模に
かかわらず、管理コンソールの
ダッシュボードを使って
インフラ、アプリケーション、
システム統合のすべてを
一元的に管理できます。

ドライブ監査ログ

ドライブ監査ログには、ドメインのユーザーがドライブ コンテンツを表示、作成、更新、削除、または共有するたびにログが記録されます。これには、Google ドキュメント、スプレッドシート、スライド、その他の G Suite で作成したコンテンツだけでなく、PDF や Word ファイルなど、他で作成してドライブにアップロードしたコンテンツも含まれます。

ドライブのコンテンツ コンプライアンスとアラート

G Suite の追加機能では、ドライブで特定の操作が行われた場合に管理者が確認したり、ドライブのカスタム アラートを設定したりすることができます。これにより、たとえば「機密」という語がタイトルに含まれているファイルが企業の外部と共有された場合に、それを検知できます。さらに、ダウンロード、印刷、プレビュー アラートなど、多数のイベントをドライブ監査で検知できるようになる予定です。

信頼できるドメインとのドライブ共有

G Suite と G Suite for Education の管理者はドメインのホワイトリストを作成できます。ホワイトリストを作成することで、エンドユーザーがやり取りできる相手を、リストに登録された信頼できるドメインのみに限定できます。この機能は、提携企業や支社の他、特定のドメインと信頼関係にある場合に最適で、ユーザーがこのようなドメインとのみ安全に情報を共有するよう設定できます。

メール セキュリティ機能

セキュアなトランスポート（TLS）の適用

G Suite 管理者は、特定のドメインまたはメールアドレスで送受信されるメールを TLS（Transport Layer Security）で暗号化することを要求できます。たとえば、外部の法律顧問宛てのすべてのメッセージをセキュリティで保護された接続経由で送信するよう設定できます。指定したドメインで TLS が使用できない場合、受信メールは拒否され、送信メールは送信されません。

フィッシングの防止

迷惑メールの送信者は、メール メッセージの「From」アドレスを偽装して、よく知られた組織のドメインから送信されたかのように見せかけることができます。フィッシングと呼ばれるこの行為は多くの場合、機密データを収集することが目的です。Google は、フィッシングを防止するために DMARC プログラムに参加しています。このプログラムでは、ドメインの所有者がメール プロバイダで、自ドメインからの未認証メッセージをどう処理するかを指定できます。G Suite のお客様は、管理設定で DMARC レコードを作成し、すべての送信メール ストリームに SPF レコードと DKIM キーを実装することによって、DMARC を導入できます。

Gmail のデータ損失防止（DLP）機能

Gmail のデータ損失防止（DLP）機能を使用すると、組織で送受信されるメール トラフィックのコンテンツにクレジット カードやマイナンバーなどが含まれているかどうかをチェックし、検出された場合のポリシーに基づく対応を設定して、メールの検疫、拒否、変更などの操作を行うことができます。定義済み検出項目を使用して DLP ポリシーを設定する場合、メールの件名、本文、添付ファイルが自動的にスキャンされます。定義済み検出項目にキーワードや正規表現を組み合わせて複合検出項目を作成することで、より高度なコンテンツ コンプライアンスのポリシーを構成できます。機密情報はテキスト ドキュメントだけでなく、スキャンしたコピーや画像にも含まれます。今回新しく OCR 機能が追加されたことで、よく使われる画像フォーマットの分析や、ポリシー評価のためのテキスト抽出を DLP ポリシーで行えるようになりました。管理者は、コンテンツ コンプライアンスや不快なコンテンツの両方のルールについて、組織部門（OU）レベルの OCR チェックを管理コンソールで有効にすることもできます。詳しくはDLP ホワイト ペーパーをご覧ください。

G Suite 管理者は、特定のドメインやメールアドレスで送受信されるメールを TLS（Transport Layer Security）で暗号化するよう指定できます。

メール コンテンツのコンプライアンス

管理者は、G Suite のメール メッセージで、事前定義した単語、フレーズ、テキスト パターンや数値パターンをスキャンするよう設定できます。一致するメールが指定された受信者に届く前にメールを拒否するか、変更を加えたうえで配信するようルールを作成できます。これまで、この設定を使用してクレジット カード情報、内部プロジェクト コード名、URL、電話番号、社員 ID 番号、マイナンバーなどの機密データや制限されたデータが監視されています。

不快なコンテンツ

不快なコンテンツ の設定では、管理者がカスタム ワードリストに基づいてメッセージに対して実行するアクションを指定できます。また、管理者は不快なコンテンツに関するポリシーを使用して、特定の単語（わいせつな単語など）を含むメッセージを拒否するか、変更したうえで配信するかを選択できます。これにより、たとえば、メッセージの内容が管理者の設定したルールに一致する場合に、他のユーザーに通知することができます。さらに管理者は、この設定によって、会社の機密情報を含む可能性がある送信メールを拒否することもできます。そのために、たとえば、「機密」という単語を検出する送信フィルタを設定できます。

メール配信の制限

デフォルトでは、お客様のドメインの Gmail アカウントを持つユーザーは、どのメールアドレスともメールをやり取りできます。ただし、場合によって管理者は、ユーザーがメールをやり取りできるメールアドレスを制限することができます。たとえば学校では、生徒がメールをやり取りする相手を教職員と他の生徒だけに制限し、校外のユーザーとのメールのやり取りを禁止できます。これには、配信制限の設定を使用して、管理者によって指定されたアドレスまたはドメインでのみメール メッセージを送受信できるようにします。管理者が配信制限の設定を追加すると、ユーザーは承認された相手としかメールをやり取りできなくなります。ユーザーが許可リストにないドメインにメールを送信しようとすると、そのアドレス宛てのメールを禁止するポリシーを示すメッセージが表示され、メールが送信されなかったことが通知されます。ユーザーは、リストにあるドメインからの認証されたメッセージだけを受け取ります。リストにないドメインから送信されたメッセージや、リストにあるドメインから送信されているけれども DKIM または SPF レコードを使っ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とともに送信者に返送されます。

電子情報開示の機能

電子情報開示の機能を使用すると、組織は訴訟やその他の法的問題に備えることができます。Google Vault は G Suite の電子情報開示ソリューションで、お客様はこれを使用して、ビジネス用 Gmail の保存、アーカイブ、検索、書き出しを行うことができます。管理者は、Google ドライブに保存したファイルの検索や書き出しを行うこともできます。

メール保持ポリシー

保持ルールを設定すると、ドメイン内の特定のメールについて、どのくらいの期間保存した後にユーザーのメールボックスから削除されて Google のすべてのシステムから消去されるようにするかを制御できます。G Suite では、ドメイン全体を対象にしたデフォルトの保持ルールを設定できます。より高度な実装が必要な場合、管理者は Google Vault を使用して、特定のコンテンツを保持するためのカスタム保持ルールを作成できます。この高度な設定により、管理者はメッセージを保持する日数を指定できるほか、保持期間を過ぎたらメッセージを完全に削除するかどうか、特定のラベルを付けてメッセージを保持するかどうか、ユーザー自身にメールの削除を管理させるかどうかを指定できます。

訴訟のための記録保持（リティゲーションホールド）

Google Vault を使用すると、管理者はユーザーに対して訴訟のための記録保持（リティゲーションホールド）を適用し、法的義務やその他の保存義務に従い、そのユーザーのすべてのメールとオフレコでないチャットを無期限で保存できます。ユーザー アカウントのすべてのコンテンツに対して適用することも、日付や単語に基づいて特定のコンテンツを対象にすることもできます。記録保持が適用されているメッセージをユーザーが削除した場合、メッセージはユーザーの画面に表示されなくなりますが、記録保持が解除されるまで Google サーバーからは削除されません。

検索と検出

Google Vault では、管理者が Gmail とドライブのアカウントの検索をユーザー アカウント、組織部門、日付、またはキーワードを基準にして実行できます。検索結果にはメール、オフレコでないチャット、Google の形式のファイル、Google の形式以外のファイル（PDF、DOCX、JPG など）が含まれます。

証拠の書き出し

Google Vault では、管理者は特定のメール、オフレコでないチャット、ファイルを標準形式で書き出し、一連の保護ガイドラインに従って、法的問題をサポートしながら、追加処理や審査を行うことができます。

サードパーティ メール プラットフォームのサポート

包括的なメール ストレージの設定により、自ドメインで送受信したすべてのメール（Gmail 以外のメールボックスで送受信したメールを含む）が、関連付けられたユーザーの Gmail メールボックスに保存されます。組織でメールを Gmail 以外のメールサーバーにルーティングする場合、この設定により、アーカイブや電子情報開示の目的で Gmail のメールボックスにメールを確実に保存できます。

エンドポイントのセキュリティ保護

モバイル端末管理（MDM）

G Suite のモバイル端末管理によって、社内用端末やサードパーティの管理ソリューションが不要になります。管理者は、組織内のモバイル端末にポリシーを適用したり、端末上のデータを暗号化したり、端末の紛失または盗難時にリモートでワイプやロックを実行したりすることができます。このような端末管理を設定しておけば、従業員が個人のスマートフォンやタブレットを使って仕事をする場合でも、仕事で使うデータのセキュリティを維持できます。G Suite のモバイル端末管理は、Android、iOS、Windows Phone のほか、Microsoft Exchange ActiveSync を使用している BlackBerry 10 のようなスマートフォンやタブレットで使用できます。

ポリシーベースの Chrome ブラウザ セキュリティ

G Suite のツールと機能はすべて、Google Chrome で最適にサポートされます。**管理者は Windows、OSX、Linux、iOS、Android にセキュリティと使用方法に関するポリシーを適用できます。**Chrome にはセーフ ブラウジング、サンドボックス、管理されたアップデートが標準セキュリティ機能として用意されており、ユーザーを悪意のあるサイトやウィルス、不正なソフトウェア、フィッシング攻撃から保護します。また、攻撃者が非公開データを不正に取得するために使用するクロスサイト スクリプトを防止する対策も施されています。組織全体に Chrome を導入する場合でも、要件に合わせたカスタマイズが可能です。管理者は、用意されている 280 以上のポリシーを利用して、社員が各種端末でどのように Chrome を使用するかを管理できます。たとえば、管理者は自動更新を有効にして最新のセキュリティ修正プログラムを入手したり、特定のアプリをブロックまたは許可したり、従来のブラウザのサポートを設定したりすることができます。

管理者は組織内のモバイル端末にポリシーを適用したり、端末上のデータを暗号化したり、端末の紛失または盗難時にリモートでワイプやロックを実行したりできます。

Chrome デバイスの管理

G Suite 管理コンソールでは、Chrome デバイス（Chromebooks、Chromebox、Chromebox for meetings など）にポリシーを適用できます。Chrome をオペレーティング システムとして実行するこれらのデバイスは、セキュリティ性に優れた、高速でコスト効果の高いコンピュータです。管理者は、組織の Chrome デバイスに関するセキュリティやその他の設定を 1 か所から簡単に管理できます。ユーザーが使用する Chrome の機能の設定、VPN や Wi-Fi ネットワークへのアクセスのセットアップ、アプリや拡張機能のプレインストール、特定のユーザーに対するログインの制限などを行うことができます。

管理者は、ユーザーのドライブデータまたは Gmail データを削除日から 25 日以内であれば復元できます。25 日を過ぎるとユーザーデータは完全に削除され、技術サポートに連絡しても復元することができません。

データ復旧

最近削除したユーザーの復元

管理者は、削除から 5 日以内であれば、削除したユーザー アカウントを復元できます。5 日を過ぎると、ユーザー アカウントは管理コンソールから完全に削除され、Google 技術サポートにお問い合わせいただいても復元できません。お客様の管理者だけがアカウントを削除できることにご注意ください。

ユーザーのドライブデータまたは Gmail データの復元

管理者はユーザーのドライブデータまたは Gmail データを削除日から 25 日以内であれば復元できます。25 日を過ぎると、ユーザーデータは完全に削除され、技術サポートにお問い合わせいただいても復元できません。お客様が削除したデータは、180 日以内に速やかに Google のシステムから削除されます。

セキュリティ レポート

G Suite 管理者はセキュリティ レポートにアクセスできます。セキュリティ レポートには、組織のデータ侵害の危険性に関する重要な情報が含まれます。ユーザーが 2 段階認証プロセスを意図的に回避したり、外部アプリをインストールしたり、ドキュメントをむやみに共有したりすることでセキュリティ上のリスクが生じている場合、管理者はそのユーザーを容易に特定できます。また、セキュリティの脅威になる可能性がある不審なログイン操作が行われた場合に、アラートを受け取るように設定することもできます。

まとめ

ユーザーデータの保護は、Googleのすべてのインフラ、アプリケーション、人材管理を考慮する上で最も重視すべきテーマであり、補完的あるいは一時的な取り組みではなく、業務の根幹をなすものです。Google　　は、他社の追随を許さない、高度な保護を実現できると自負しています。その根拠は、ユーザーデータの保護がGoogle のコアビジネスの一部になっており、2 段階認証やより高度な暗号方式など、セキュリティを革新するサービスを開発できる環境が整っていることです。また、セキュリティ、リソース、専門知識に対して、他社には真似できない規模の投資を行えることも強みです。業務規模を活かし、またセキュリティ リサーチ コミュニティと連携することで、脆弱性への予防措置や事後対策を講じています。さらに、Google のセキュリティとオペレーションの仕組みは、独立した第三者である監査機関の検証を受けています。

データ保護は単なるセキュリティの問題ではありません。Googleは、データ処理の修正条項を締結することで、データおよびデータの処理方法の管理権限がお客様ご自身にあることを契約によって明確に保証しています。また、G　Suite コアサービスのお客様のデータは、お客様との契約に示された目的にのみ使用し、広告には使用しないことも保証しています。

Fortune 500 企業の 64% を含む世界中の 500 万以上の組織に、最も価値の高い資産である「情報」の保管先として Google をお選びいただいている理由は、このような取り組みにあります。今後も皆様に安全かつ透明性の高いサービスをお届けできるよう、セキュリティやプラットフォーム向上のためのイノベーションへの投資を続けてまいります。

データ保護は単なるセキュリティの問題ではありません。Google は、データ処理の修正条項を締結することで、データおよびデータの処理方法の管理権限がお客様ご自身にあることを契約によって明確に保証しています。また、G Suite コアサービスのお客様のデータは、お客様との契約に示された目的にのみ使用し、広告には使用しないことも保証しています。