Google for Work 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

Google™ for Work

このホワイトペーパーは、次の Google Apps サービスに適用されます

Google Apps for Work、Education、Government、Nonprofit、Drive for Work、Google Apps Unlimited

目次

概要

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ます。社員は各自の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することができ、ビデオ通話、音声通話、インスタント メッセージ、メールを使って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す。その一方で、雇用主に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りません。そのため、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。

クラウドの成長に伴い、セキュリティと信頼性の問題に注目が集まるようになりました。それは、クラウド サービスの運用が従来の自社運用型テクノロジーの運用とは大きく異なるためです。今では、コンテンツはローカルサーバー上にあるのではなく、グローバルなデータセンター ネットワークの一部である Google サーバーで管理されています。以前は、インフラの運用方法と誰がその運用を行うかは完全に社内で管理できているとの認識がありましたが、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します。ユーザーはデスクトップ パソコンだけでなく、個人の携帯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。お客様は、クラウド ソリューションのセキュリティ コントロールとコンプライアンスが、自社の個別の要件を満たすかどうかを評価する必要があります。そのため、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の目的は、セキュリティとコンプライアンスに関する Google のテクノロジーを紹介することです。

クラウドのパイオニアとして、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ています。Google のクラウド サービスは、多数の従来の自社運用型ソリューションよりも強固なセキュリティを提供できるよう設計されています。セキュリティは Google の優先事項です。これは Google 自身のオペレーションを保護するためですが、お客様へのサービスも同じインフラで提供しているため、Google のセキュリティ保護策はお客様の組織にも直接メリットをもたらします。それが Google がセキュリティを重視する理由であり、データの保護は中でも最重要の設計基準となっています。セキュリティに対応するために Google の組織構造、研修の優先順位、雇用プロセスは変化します。また、Google のデータセンターとデータセンターに投入されるテクノロジーも進化します。Google の日々のオペレーションと災害復旧計画の中心は、脅威への対応策などのセキュリティ対策です。Google がお客様のデータを処理する方法においても、セキュリティが優先されます。セキュリティは、Google がお客様に提供するアカウント管理、コンプライアンスの監査、保証の要です。

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スイートである Google Apps に対して Google が行っているセキュリティとコンプライアンス対応について、概要をご紹介します。Google Apps for Work と Google Apps for Education は、ユーザー数が数千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。Google Apps は、メンバーがいる場所や使用する端末を問わない、新しい、より効率的な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た、組織と技術の管理機能の詳細を示します。次のコンプライアンスのセクションでは、ユーザーデータがどのように処理されるかを説明し、組織が法規制の要件を満たす方法に関する詳細を示します。

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、導入トレーニング、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反映されています。

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、地域の労働法または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セキュリティ トレーニングがあり、Google 在職中は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。エンジニアは、それ以外にも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し、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のイベント

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、専任の社員に従事させることが認識を高める重要な手段であると 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、データの取り扱いとポリシーの適用から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 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 500 名以上の常勤社員を配置しています。その中には、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 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 500 名以上の常勤社員を配置しています。その中には、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 ポリシーの実装です。Google のセキュリティ専任チームは、商用ツール、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固有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実行します。さらに、外部の専門家と連携した定期的なセキュリティの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バグを登録しています。

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 の脆弱性や暗号スイートの弱点があります。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への参加や主催を行っています。

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、設計文書を審査するほか、コードレビューを実行して、プライバシー要件に沿っていることを確認します。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、このチームは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ベスト プラクティスについて思想的リーダーシップを発揮します。

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。このチームは、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おり、Google Apps やその他の Google サービスの脆弱性を発見するうえで、このコミュニティと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、数万ドル単位の報奨金を用意して、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す。たとえば Chrome では、マルウェアやフィッシングについてユーザーに警告し、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 のセキュリティに関する 700 件以上のバグを修正し、125 万ドルを超える報奨金を支払いました。Google のさまざまな脆弱性報告の報奨プログラム全体で、支払った報奨金は 200 万ドルを超えています。Google はご協力いただいた方々に正式に謝意を表明し、Google のプロダクトやサービスへの貢献者として、それらの方々の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 は脆弱性の管理プロセスを適切に運用するために、商用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します。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、その脆弱性がログに記録され、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、修正されたことが検証されるまで頻繁にフォローアップを行います。また、Google では、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、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ます。セキュリティに関する問題の報告の詳細については、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。

マルウェアの防止

マルウェアによる巧妙な攻撃によってアカウントが不正に使用されたり、データの盗難や企業内ネットワークの更なるアクセスに繋がることがあります。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マルウェアの防止、検出、根絶に努めています。Google は、Google Chrome、Mozilla Firefox、Apple Safari のユーザーが、個人情報の窃盗や、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。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、マルウェアを含むサイトやメール添付ファイルから、悪意のあるソフトウェアがユーザーのコンピュータにインストールされます。ユーザーがこれらのサイトにアクセスすると、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。マルウェアに対する Google の戦略は、まず感染を防ぐことから始まります。手動および自動スキャナを使って、マル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、その多くは不正使用されている正当なウェブサイトです。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を表示します。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種類の不正なコンテンツを確認できます。VirusTotal の使命は、無料ツールとサービスの開発を通して、ウィルス対策とセキュリティ産業の品質向上に寄与し、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マル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 の窃盗や、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、システム上での社員の操作、外部の脆弱性情報から収集された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、通知手順、エスカレーション、緩和策、文書化の方法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専用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

Google Apps 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です。Google は特注の自社サーバー、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備えています。また、「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 インフラを構築しました。

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 1 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、データセンター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 日監視されています。インシデントが発生した場合、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、データセンターでは、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います。データセンター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ます。Google 社員のうち、データセンターに足を踏み入れたことがある社員は 1% 未満です。

データセンターの強化

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、同等の能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能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。火災検知と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、警報信号が表示されます。

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消費の削減を図っています。改善効果を測定するために、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 は主なインターネット サービス会社として初めて、すべてのデータセンターにおける環境への配慮、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 の認定の自主取得を行いました。簡単に言うと、これらの基準は有言実行と継続的な改善というきわめてシンプルな考え方に基づいて作成されています。

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、特定の目的で構築されたカスタム 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。多くの商用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を増したバージョンの 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に対する柔軟性があり、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ります。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、機器の取得と設置から使用停止、廃棄までバーコードと資産タグで細かく追跡します。許可なく機器がデータセンターから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。Google のハードディスクは FDE（フルディスク暗号化）やドライブロックのような技術を利用して保存済みのデータを保護します。ハードディスクの使用を停止する場合、承認された社員によって、ディスクのデータが消去されたことが確認されます。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が確認されます。何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ディスクを小片に粉砕した後、安全な施設でリサイクルされます。各データセンターは廃棄ポリシーを厳密に順守し、逸脱があればただちに対処が行われます。

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ます。これにより Google は、可用性が高く待ち時間の少ないサービスを世界中に提供することができます。

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ます。これにより Google は、可用性が高く待ち時間の少ないサービスを世界中に提供することができます。

他のクラウド サービスや自社運用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ます。ホップの回数が増えれば、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ます。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拒否（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「既定で拒否」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。ログは定期的に調べられ、不正なコードやプログラミング エラーがあれば明らかになります。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。

データ転送中のセキュリティ

データは、インターネットまたはネットワーク内を転送されるときが最も脆弱性が高まります。このため、Google では転送中のデータをセキュリティで保護することを優先しています。お客様の端末と Google の間で転送されるデータは、HTTPS/TLS（Transport Layer Security）で暗号化されます。実際、Google は、HTTPS/TLS を既定で有効にした最初の主要なクラウド プロバイダです。Google 以外のユーザーとメールを送受信するときは、チェーンのすべてのリンク（端末、ブラウザ、メールサービス プロバイダ）が強力で、暗号化が機能するように連携する必要があります。Google ではこの重要性を認識しているため、Google のセーフメール サイトで業界の TLS 採用について報告します。Google はまた、すべての RSA 証明書を 2048 ビットキーにアップグレードし、Google Apps とその他すべての Google サービスの転送時の暗号化をさらに強化しました。

PFS（Perfect Forward Secrecy）は、キーの不正使用や、暗号解読時の影響を最小限にとどめます。PFS は、耐久性のあるストレージに保管されて何年間も使用されるキーではなく、わずか数日だけ存続し、メモリだけに保持される短期間のキーを使用してネットワーク データを保護します。Google は、主要なウェブ企業として初めて PFS を既定で有効化しました。

Google は、自社のプライベート ネットワーク上のデータセンター間を移動するすべての Google Apps データを暗号化しています。

Google のデータセンターは地理的に分散しています。
各地で発生する自然災害や停電などの影響を最小限に抑えるためです。

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、Google のサーバー設計、データの保存方法、ネットワークとインターネット接続、ソフトウェア サービス自体に反映されています。この「あらゆるものの冗長性」には設計によるエラー処理が含まれており、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が構築されます。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の地域的なサービス中断の影響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、データは自動的かつ瞬時に 1 つの施設から別の施設に切り替えられるため、Google Apps 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、新たに設定し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共同作業が可能です。単一のグローバル ネットワークで作業するグローバルなチームは、高パフォーマンスで待ち時間の少ない環境を共有できます。

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。Google Apps 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。つまり、エラー発生時に瞬時にフェイルオーバーされる継続的なバックアップ プロセスが実行されています。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。次に、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。簡単に言うと、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、このようなサービス中断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も示されています。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、その可用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 はいくつかの独立した第三者による監査を定期的に受けています。それぞれの監査で、独立した監査機関がデータセンター、インフラ、オペレーションを調査します。定期的な監査は、ISO 27001、SOC 2、SOC 3 の監査規格へのコンプライアンスをチェックするために実施されます。Google Apps for Government については、米国政府が 2014 年に定めた FISMA（連邦情報セキュリティ近代化法）へのコンプライアンスも監査されます。お客様が Google Apps を検討する際、これらの認定は、Google のサービス スイート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、Google Apps 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）によって認証された 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、Google Trust Center 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z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。

FISMA

FISMA は、連邦政府機関の情報システムの情報セキュリティに関する米国連邦法です。この法律は、政府機関に対し、自組織のシステムと、Google などのサービス プロバイダによって運用されるシステムについて、NIST（アメリカ国立標準技術研究所）が規定する最小限のセキュリティ要件を満たすことを義務付けるものです。Google は、最も長期にわたってこれらの要件を満たしている実績を持つクラウド プロバイダの 1 つに数えられ、ATO（運用権限）を保持しています。FedRAMP（米国連邦政府のリスク・認証管理プログラム）は、FISMA の要件に加えてクラウド プロバイダが満たさなければならない、いくつかの要件を規定しています。FedRAMP プログラムの詳細とベンダーの対応状況については、fedramp.gov をご覧ください。

データ利用

Google の哲学

Google Apps 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。Google Apps 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することや、第三者に販売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、詳細なデータ処理修正条項をお客様に提供します。この条項では、Google が契約上の義務を果たす以外の目的

でデータを処理しないことを表明しています。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。

Google Apps での広告非表示

Google Apps 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。Google Apps 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、Google Apps 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、スパムのフィルタリング、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 Google Apps データを他のお客様やユーザー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ます。Google 社員には、社員のメールや Google 社員用の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、制限された既定の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い、データまたは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。このツールで認可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。社員の認可設定は、Google Apps 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

お客様の組織内で、Google Apps 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記録される管理操作の詳細な履歴は、お客様がデータへの内部アクセスや自社ポリシーの順守を監視する際に役立ちます。

法令によるデータ提供のリクエスト

法令によるデータ提供のリクエストへの対応は、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 が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、直接データのリクエスト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、過剰なリクエストを制限するための手段を講じます。法令によるリクエストに従う場合でも、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。このようなリクエストを受けた場合、社内のチームがリクエストを審査し、リクエストが法的要件と 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、リクエストに従うためには、リクエストが書面でなされること、リクエストした機関の承認された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。リクエスト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会社として唯一、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リクエストを拒否しました。Google は召喚に異議を唱え、最終的に政府のリクエスト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リクエストされることがあります。Google はリクエストした機関に対して、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、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ユーザーにはあると考えます。そのため Google は、企業として初めて、政府からのデータ提供のリクエスト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。データ提供のリクエストと 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ない限り、お客様のデータに関するリクエスト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、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ユーザーにはあると考えます。そのため Google は、企業として初めて、政府からのデータ提供のリクエスト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 は、サービスを提供するためのすべてのデータ処理操作を実質的に自ら直接実行しています。ただし Google は、カスタマー サポートや技術サポートなどの Google Apps 関連サービスを提供するために、サードパーティのサプライヤーと

契約する場合があります。サードパーティのサプライヤーと契約する前に、Google はサードパーティのセキュリティやプライバシーに関する活動を評価し、サプライヤーが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実現しているかどうかを確認します。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 と SOC 2/3 の監査基準を順守します。
- 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 プライバシー担当者へのアクセス。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 も多くのお客様も、グローバルな環境で運営されています。Google はすべてのお客様にデータ処理修正条項を通じて同等の高レベルの保護を提供します。データ処理修正条項に定められた Google のコミットメントは、管轄区域固有の法律や規制への準拠を促進することを目的としています。お客様の組織で Google のデータ処理修理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に関する推奨条件を順守するために開発された機能を提供し、契約により順守する旨をお約束します。

米国と EU 間、米国とスイス間のセーフハーバー フレームワーク

Google の法人顧客の半数以上が米国以外の国に拠点を置いており、その多くがヨーロッパで活動しています。それらの企業は欧州委員会のデータ保護指令への準拠を求められます。この指令は、EU 内での個人データの転送を規制するものです。米国と EU 間のセーフハーバー フレームワークは、ヨーロッパの企業が指令に則った方法で EU の外部に個人データを転送する方法を定めています。Googleは、自社の原則と、米国とスイス間のセーフハーバー フレームワークの原則を順守していることを保証します。

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ます。Google はヨーロッパに広範囲な顧客基盤を持っています。EU モデル契約条項を採用することにより、指令に準拠するための追加設定をお客様に提供します。

米国 HIPAA（医療保険の相互運用性と説明責任に関する法律）

Google Apps 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、Google Apps 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 Apps Vault です。

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 万を超える生徒が Google Apps for Education を使用しています。Google Apps 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 Google Apps for Education を使用する学校に対して契約で、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求めており、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、セキュリティが組み込まれています。Google 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 Google Apps ユーザーの既定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、積極的に権限を与えられます。また、Google Apps では、管理者は組織の規模に関係なく、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ます。このアプローチにより、管理と設定が簡略化されます。自社運用型のメールシステムに DKIM（フィッシング防止機能）を導入するとします。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。管理コンソールを使用すれば、数千または数十万のアカウントすべてに数分で DKIM を設定でき、しかも停止やメンテナンス期間が不要なので、安心して利用できます。管理者は各自の判断で多数のツールを使用できます。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の使用や、セキュア トランスポート（TLS）などのメール セキュリティ ポリシーの適用を行えます。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 Google Apps 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。

ユーザー認証と認可の機能

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ユーザーに要求することにより、Google Apps アカウントのセキュリティ レイヤを追加できます。これにより、ユーザーのパスワードが流出した場合に無許可の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、1 回限りの使用を目的としてユーザーの Android、BlackBerry、iPhone などの携帯端末に配信されます。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。

シングル サインオン（SAML 2.0）

Google Apps はお客様にシングル サインオン（SSO）サービスを提供します。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。これは SAML 2.0 に基づきます。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認可のためのデータ交換を可能にする XML 標準です。さらにセキュリティを強化するために、SSO 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受け取ります。お客様の組織では、SSO サービスを使用して Google Apps 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

Google Apps は、OAuth 2.0 と OpenID Connect をサポートしています。これは認証と認可のためのオープンなプロトコルです。これにより、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、Google Apps 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。

また、Google Apps では、管理者は組織の規模に関係なく、管理コンソールのダッシュボードから一元的にインフラ、アプリケーション、システム統合のすべてを管理できます。

メール管理機能

セキュアなトランスポート（TLS）の適用

Google Apps 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、お客様の組織では、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

スパム送信者は、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 プロバイダに、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。Google Apps 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。

Google Apps 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、Google Apps 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にするルールを作成できます。お客様は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、社会保障番号などの機密データや制限されたデータを監視しています。

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の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

既定では、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。配信制限の設定を使用して、管理者が指定したアドレスまたはドメインだけからメール 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、メール送信を確実に防ぐことができます。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が 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 Google Apps 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。

メール保存ポリシー

保存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。Google Apps では、ドメイン全体を対象にした既定の保存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存するためのカスタム保存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存する日数を指定できるほか、保存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存するかどうか、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に保存できます。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沿いながら、法的問題をサポートする方法で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

管理者は組織内の携帯端末にポリシーを適用し、端末上のデータの暗号化や、端末の紛失や盗難時にリモートでワイプやロックを実行できます。

携帯端末管理（MDM）

Google Apps の携帯端末管理によって、自社運用型端末または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。管理者は組織内の携帯端末にポリシーを適用し、端末上のデータの暗号化や、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できます。この管理方式により、社員が仕事に個人のスマートフォンやタブレットを使用する場合でも、ビジネスデータのセキュリティが保証されます。Google Apps の携帯端末の管理は、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

Google Apps 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、マルウェア、フィッシング攻撃から保護します。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手段も用意されています。Google Apps 管理者は、組織全体に Chrome for Work を導入して、ニーズに合わせてカスタマイズできます。管理者は、用意されている 280 以上のポリシーを利用して、社員が端末間でどのように 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。

Chrome 端末の管理

Google Apps 管理コンソールでは、Chrome 端末

（Chromebook、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端末は、セキュリティを強化した、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 端末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 WiFi 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。

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。ユーザーがドライブのファイルを削除するか、Gmail の受信トレイからメールを削除すると、そのアイテムはゴミ箱に移動します。ゴミ箱にあるアイテムは、管理者に依頼しなくても、ユーザーが自分で簡単に復元できます。ユーザーまたはシステムによってゴミ箱が空にされた時点で、アイテムは実際に削除されます。この場合、削除されたアイテムを復元できるのは管理者のみです。

セキュリティ レポート

Google Apps 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提供されています。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、ドキュメントを無闇に共有することでセキュリティ上のリスクになっている場合、管理者はそのユーザーを容易に特定できます。また、管理者は、セキュリティの脅威の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はできません。

まとめ

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 の契約による強いコミットメントにより、データとデータの処理方法についてはお客様が管理していくことを保証します。また、お客様のデータは Google Apps サービスの提供以外の目的（広告など）には使用されないことも保証しています。

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、要員管理において最優先される設計上の考慮事項です。ユーザーデータの保護は、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。Google は、他にほとんど類のないレベルの保護を実現できると確信しています。ユーザーデータの保護は Google のコアビジネスの一部になっているため、Google は 2 段階認証や、より強力な暗号方式など、セキュリティを革新するサービスを開発できます。Google は他社が追随できない規模でセキュリティ、リソース、専門知識に大がかりな投資を行うことができます。Google はそのオペレーションの規模と、セキュリティ リサーチ コミュニティとの連携によって、脆弱性に迅速に対処したり、脆弱性を未然に防止したりできます。Google のセキュリティとオペレーションの手順は、独立した第三者である監査人によって検証されています。

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 の契約による強いコミットメントにより、データとデータの処理方法についてはお客様が管理していくことを保証します。また、お客様のデータは Google Apps サービスの提供以外の目的（広告など）には使用されないことも保証しています。

これらは、Fortune 500 の企業の 64% を含む世界中の 500 万以上の組織から、最も価値の高い資産である情報の保管先として、Google が信頼されている理由の一部です。Google は、ユーザーが安全かつ透明性のある方法で Google のサービスのメリットを享受できるように、今後もプラットフォームへの投資を続けてまいります。