G Suiteのセキュリティと信頼

Google ではお客様のデータを保護することを最優先事項としています。

Google Cloud

目次

セキュリティ第一の姿で業界をリード

Google はクラウドから始まりクラウドで運営されてきました。だからこそ、クラウドでのビジネスの活性化にセキュリティが欠かせないことを十分に理解しています。Google の企業向けサービスは Googleと同じインフラストラクチャで運用されているため、Google が構築して日々利用している保護機能の利点をお客様の組織でもご活用いただけます。700 名を超えるセキュリティの専門家とイノベーションへの意欲、そしてこの堅牢でグローバルなインフラストラクチャにより、Google は常に時代を先取りしながら、各基準に準拠した安全で信頼性の高い環境をお客様に提供しています。

世界をリードするさまざまな組織からご信頼いただいています。

設計から考えられた安全性

最新鋭のクラウドセキュリティです。

良質なデータセンター セキュリティ

セキュリティとデータの保護は、Google データセンターの設計の中核となる要素です。Google では物理的なセキュリティ モデルとしてカスタムの電子アクセスカードを利用しているだけでなく、施設の外周をフェンスで囲ったうえで金属探知機を導入しています。生体認証やレーザーを利用した侵入検出機能など、最先端のツールも活用しており、攻撃者による物理的な侵害を「ミッション インポッシブル（不可能）」なシナリオにしています。
Google データセンターの内部をご覧ください。

パフォーマンスを考えたハードウェア設計

Google データセンターではカスタム設計のハードウェアを採用し、強化されたオペレーティング システムとファイル システムを搭載して運用しています。こうしたシステムのそれぞれがセキュリティとパフォーマンスの面で最適化されています。ハードウェア スタックを Google で管理しているため、脅威や脆弱性のリスクにも迅速に対応できます。

回復力を備えた、信頼性の高いネットワーク

Google のアプリケーションとネットワークのアーキテクチャは、信頼性と稼働時間を重視して設計されています。データは Google の各サーバー、各データセンターに分散されるので、マシンに障害が発生した場合のみならず、データセンター全体に障害が発生した場合でも引き続きデータにアクセスできます。 Google はデータセンターを世界各地に所有して運営しているので、サービスは 24 時間 365 日、継続してご利用いただけます。 Google がインフラストラクチャのセキュリティについて採用しているアプローチは統合的なものであり、ハードウェア インフラストラクチャをはじめ、サービスの導入、ユーザー ID、ストレージ、インターネット通信、運用上のセキュリティなど、複数の層にわたって協調して機能しています。詳しくは、インフラストラクチャ セキュリティ設計に関するホワイト ペーパーをご覧ください。

すべての段階で暗号化

非公開、グローバル、ソフトウェア定義の Google のネットワークは、他のクラウド サービス プロバイダをしのぐ柔軟性、制御性、セキュリティ機能を備えています。ネットワークは独自のファイバー ケーブル、公共ファイバー ケーブル、海底ケーブルを利用して複数のデータセンター間でつながれています。そのため、世界中の G Suite のお客様に対して均質で可用性が高くレイテンシの低いサービスを届けられます。これは、傍受されるおそれのある公共のインターネット空間にお客様のデータをさらす機会を限定することにもなります。 G Suite のお客様のデータはディスク上で暗号化されるだけでなく、バックアップ メディアへの保存時のほか、インターネット上やデータセンター間での移動時にも暗号化されます。暗号化は G Suite のセキュリティ戦略における重要な要素であり、お客様のメール、チャット、 Google ドライブ上のファイルなどのデータの保護に役立ちます。

G Suite の暗号化に関するホワイト ペーパーでは、保管中、送信中、バックアップ メディア上でのデータの保護方法と暗号化キーの管理に関する情報をご確認いただけます。

コミュニティへの貢献

Google の調査活動や支援活動では、Google のソリューションを選択したユーザーの皆様だけにとどまらず、インターネット ユーザーの幅広いコミュニティも対象とした保護の取り組みが行われています。Project Zero として知られるフルタイムのチームが、提供元が Google かどうかにかかわらず、広く普及したサービスを対象として、影響の大きな脆弱性 を検出することを目標に活動しています。Google ではこうした取り組みの透明性を確保し、第三者を介さずに直接ソフトウェア ベンダーにバグを報告するようにしています。

セキュリティ文化の推進

Google では全従業員が「セキュリティ第一」で考えることを求められます。Google にはセキュリティとプライバシーを専門とする従業員が数多く常勤しており、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関する分野で世界をリードする専門家も含まれています。Google では万全の保護体制を維持するため、ソフトウェア開発の全プロセスにセキュリティ機能を組み込んでいます。たとえば、セキュリティの専門家がアーキテクチャ案の分析やコードの確認を実施してセキュリティ上の脆弱性を明らかにすることで、新しいサービスや機能に対するさまざまな攻撃モデルについて理解を深めるようにしています。問題のある事象が確認された場合は、専門の G Suite インシデント管理チームがその対処にあたり、迅速な対応、分析、修復を通じてお客様への影響を最小限に抑えます。

最新鋭の
セキュリティの提供

Googleセキュリティを常に最優先事項としています。
たとえば、次のような厳しいセキュリティ対策を実施しています。

前方秘匿性

Google は、自社サーバーと他社サーバーの間を移動するコンテンツを暗号化する前方秘匿性という技術を、大手クラウド プロバイダとして初めて実現しました。前方秘匿性では接続に利用する秘密鍵が一時的なものであるため、攻撃者はもちろんサーバーの運用者ですら、過去に遡って HTTPS セッションを復号化することはできません。同業他社の多くが Google に倣って、この技術を採り入れたり、今後の採用に向けて取り組んだりしています。

メールを 100% 暗号化

すべての送信メールと受信メールは、Google データセンター間での移動時に 100% 暗号化されます。これにより、お使いの端末と Gmail サーバー間だけでなく、Google 内部でのメールの移動時にもメッセージが安全に保護されます。また、Google では TLS インジケーターを導入しており、お客様のメールが安全でない状態でプロバイダ間を移動した場合は、真っ先にユーザーに通知するようにしています

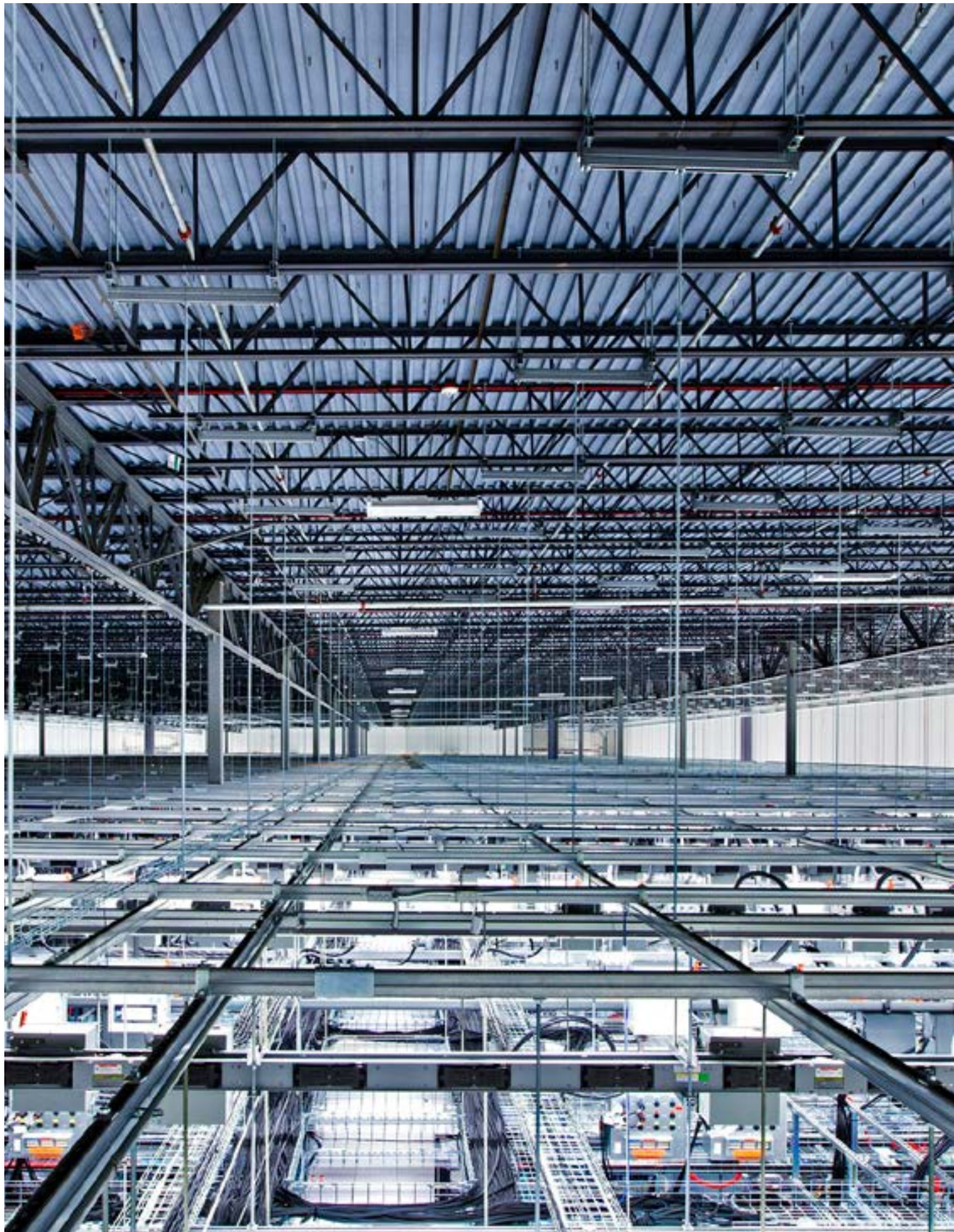
暗号化の強化

暗号解読技術の進歩からデータを守るために、Google は 2013 年、RSA 暗号化キーの長さを 2,048 ビットに倍増しました。さらに、数週間ごとにキーを変更する取り組みも開始しており、これが業界の水準を引き上げています。

サービス
セキュリティ
イノベーション

信頼できる
カスタマイズ可能な
データ保護の提供

G Suite では、企業のシステムやアプリケーションの設定を管理者が管理できます。認証、アセットの保護、運用上の管理をすべて 1 つのダッシュボードで行って、作業の合理化を図れます。組織のセキュリティ ニーズに最も合った G Suite のエディション をお選びいただけます。



アクセスと認証

- **厳格な認証機能**
  ログイン時に追加の本人確認をユーザーに求める 2 段階認証プロセスを採用しているため、未承認のアクセスが行われるリスクを大幅に減らせます。セキュリティ キーの使用を必須 にして物理キーを求めることで、ユーザー アカウントのセキュリティをさらに強化できます。キーからは暗号化された署名が送信され、所定のサイトでしか機能しないため、フィッシング対策として役立ちます。管理者は別途ソフトウェアをインストールする必要なく、G Suite の管理コンソールから規模に応じたセキュリティ キーの導入、監視、管理を簡単に行えます。

- **不審なログインの監視**
  Google では堅牢な機械学習の機能を不審なログインの検出に役立てています。不審なログインが検出されると管理者に通知が届くため、管理者はアカウントの保護に向けて対処できます

- **一元化された クラウド アクセス管理**
  シングル サインオン（SSO）がサポートされている G Suite では、他の企業向けクラウド アプリケーションへのアクセスを統合できます。 Google の Identity and Access Management（IAM）サービスを利用すれば、管理者はすべてのユーザーの認証情報やクラウド アプリケーションへのアクセスを 1 か所で管理できます。

- **高度なメール セキュリティ**
  G Suite では、管理者がカスタム ルールを設定することで、Secure/Multipurpose Internet Mail Extensions（S/MIME）を使ったメールの署名と暗号化を必須にすることができます。このようなルールを設定すれば、メール内で特定のコンテンツが検出された場合に S/MIME が自動的に実行されます。

アセットの保護

データ損失の防止

G Suite の管理者は、データ損失防止（DLP）ポリシーを設定して、Gmail やドライブ内の機密情報を保護できます。 定義済みコンテンツ検出項目 のライブラリが提供されているため、設定は簡単に行えます。DLP ポリシーを設定すると、たとえば Gmail では送信メールに含まれるすべての機密情報がチェックされ、データ漏えいを防ぐ措置（メールを隔離して精査する、ユーザーに情報の変更を求める、またはメールの送信をブロックしたうえで送信者に通知する）が自動的に実行されます。ドライブの DLP では、簡単に設定できるルールや画像に含まれているコンテンツの光学式文字認識（OCR）を利用できるため、管理者は簡単に機密性の高いコンテンツが含まれるファイルを監査したり、ユーザーが機密情報を外部と共有しないように警告するルールを設定したりできます。詳しくは、Google の DLP に関するホワイトペーパー をご覧ください。

スパムの検出

機械学習を利用することで、Gmail でのスパム検出の精度は 99.9% にまで達しています。機械学習は、必要なメールとしてシステムを通過する恐れのある迷惑メールやフィッシング メールのブロックにも役立っています。Gmail の受信トレイに届くメールのうち、迷惑メールは平均で 0.1% 未満となっており、メールが迷惑メールフォルダに誤って振り分けられる割合はさらに少ない 0.05% 未満となっています。

不正なソフトウェアの検出

不正なソフトウェアによる攻撃を防ぐため、Google ではユーザーが添付ファイルをダウンロードする前に、複数のエンジンで自動的にウィルス スキャンを行っています。Gmail では、メールを送信する前にも添付ファイルのウィルス チェックが行われます。こうしてスキャンを行うことで Gmail を利用するすべてのユーザーを保護し、ウィルスの拡散を防ぐことができます。添付ファイルのうち、.ade、.adp、.bat、.chm、.cmd、.com、.cpl、.exe、.hta、.ins、.isp、.jar、.js、.jse、.lib、.lnk、.mde、.msc、.msi、.msp、.mst、.nsh、.pif、.scr、.sct、.shb、.sys、.vb、.vbe、.vbs、.vxd、.wsc、.wsf、.wsh などの形式のものは、たとえ圧縮ファイルの一部として添付されていても、自動的にブロックされます。

フィッシングの防止

G Suite では機械学習を広く活用することで、ユーザーをフィッシング攻撃から保護しています。Google の学習モデルでは、過去にフィッシングと分類されたサイトと新しい未認識の URL との相似解析が実行され、新しいパターンが検出された場合にはどのような手動システムよりもすばやく適応しています。G Suite では、管理者がセキュリティ キーの使用を必須にすることで、フィッシング攻撃で漏えいした認証情報を使用できなくすることも可能です。

フィッシングを目的としたブランドの不正使用を防止

お客様のブランドがフィッシング攻撃の被害に遭わないよう、G Suite では DMARC 規格が採用されており、お客様のドメインから未承認のメールが送信された場合に、Gmail や使用されている他のメール プロバイダがそのメールをどのように処理するのかを、お客様ご自身で決定できます。ポリシーを定義することで、ユーザーや組織の評判を維持できます。

運用上の管理

統合された端末管理

G Suite と完全に統合されている[モバイル端末管理](#)（MDM）機能では、継続的にシステムを管理できるほか、不審な端末のアクティビティがあれば通知が送信されます。管理者はモバイル ポリシーの施行、端末上のデータの暗号化、紛失や盗難の際のモバイル端末のロック、リモートからの端末のワイプを実施できます。

サードパーティ製アプリケーションのアクセス制御

認証管理の一環として、管理者はサードパーティ製アプリケーションを把握、管理できます。認証や企業データへのアクセスには OAuth を利用します。OAuth でのアクセスは細分化されたレベルで無効にすることができ、検査済みのサードパーティ製アプリケーションをホワイトリストに登録することもできます。

Information Rights Management

管理者が機密データを継続的に管理できるように、Google では Google ドライブで IRM（Information Rights Management）をご利用いただけるようにしています。管理者やユーザーは、詳細な共有メニューからファイルのダウンロード、印刷、コピーを無効にできるほか、ファイルへのアクセスに有効期限を設定することも可能です。

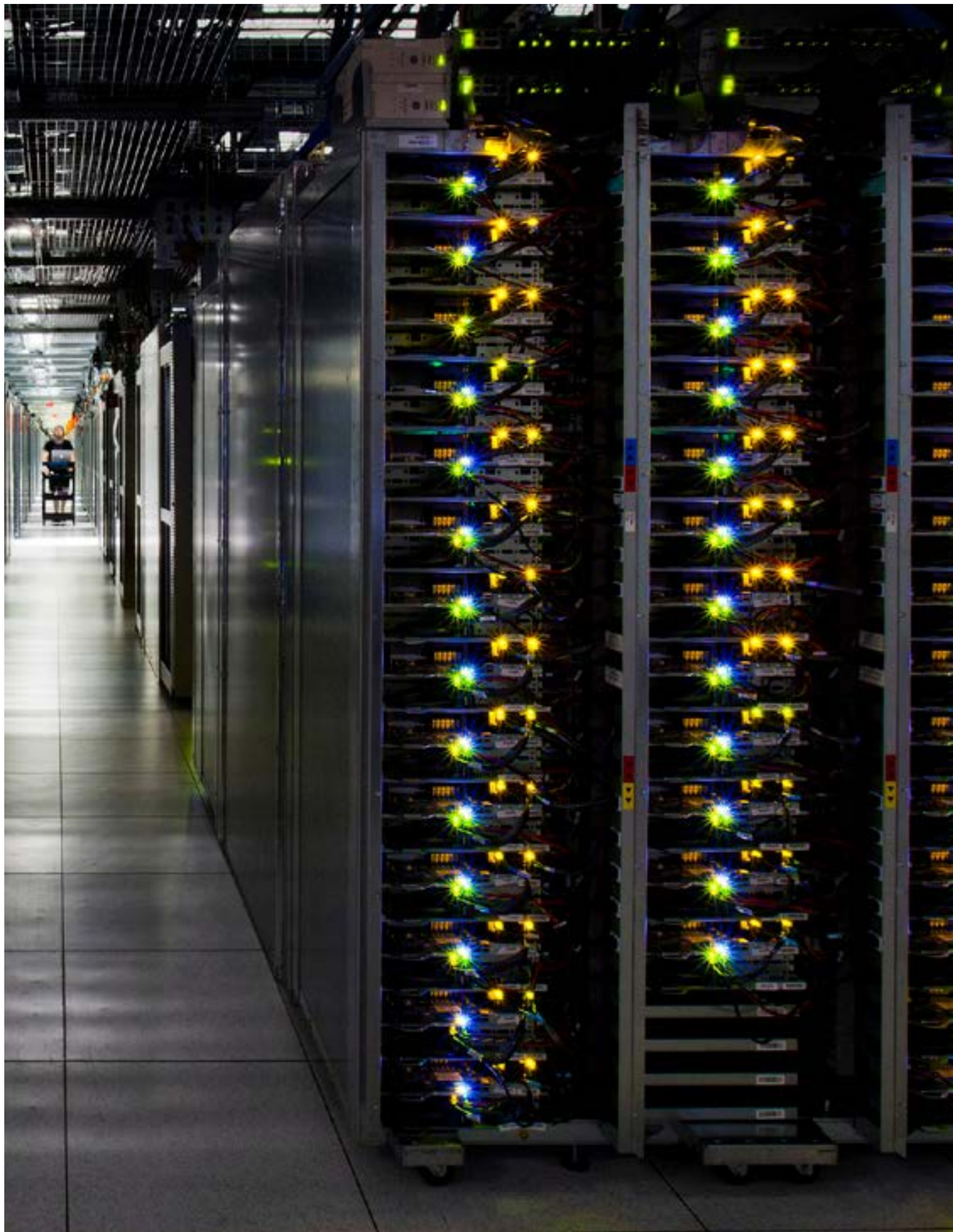
セキュリティ センター

G Suite の[セキュリティ センター](#)を利用すると、G Suite 向けのセキュリティ対策の導入状況を包括的に把握できます。Google が提供するセキュリティ分析、実用的なインサイト、おすすめの対策が 1 か所にまとめられており、組織のデータやユーザーを保護するにあたっての有益な情報を得ることができます。

コンプライアンス、電子情報開示、解析

最も厳しい
基準にも対応

G Suite は、業界のベスト プラクティスに基づき、厳格なプライバシー基準とセキュリティ基準に準拠するよう設計されています。Google はデータの所有、データの使用、セキュリティ、透明性、説明責任に関する契約上の義務を履行しているほか、お客様が報告に関する要件やコンプライアンスを満たすために必要となるツールも提供しています。



認証、監査、評価

Google のお客様や規制当局からは、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が独立した機関によって検証されることが求められています。これに対応するため、Google は複数の独立した第三者機関による監査を定期的に受けています。

ISO 27001

ISO 27001 は広く認識され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。G Suite の運用に必要なシステム、テクノロジー、プロセス、データセンターは、すべてこの ISO 27001 認証を取得しています。詳しくは、Google の ISO 27001 認証をご覧ください。

ISO 27017

ISO 27017 は、特にクラウド サービスを対象として、ISO/IEC 27002 に基づく情報セキュリティ管理の方法を規定した国際規格です。Googleの国際規格への準拠は、国際認定フォーラム（IAF）メンバーの DutchAccreditation Council により認証された ISO 認証機関である、Ernst& Young CertifyPoint によって認定されています。詳しくは、Google の ISO 27017 認証をご覧ください。

ISO 27018

G Suite が ISO/IEC 27018:2014 に準拠していることでおわかりいただけるように、Google ではプライバシーとデータの保護に関する国際的な基準に準拠することを自らの責務と捉えています。ISO 27018 のガイドラインには、お客様のデータを広告目的で使用しないこと、G Suite のサービス内にあるお客様のデータの所有者がお客様であること、データの削除と書き出しを行えるツールをお客様に提供すること、第三者から開示要請があった場合にお客様の情報を保護すること、お客様のデータの保管場所について透明性を確保すること、などが含まれています。Google の ISO 27018 認証 をご覧ください。

SOC 2、SOC 3

American Institute of Certified Public Accountants（AICPA: 米国公認会計士協会）のSOC（Service Organization Controls）2 と SOC 3 の各監査フレームワークは、セキュリティ、可用性、処理の整合性、機密性に関する Trust サービスの原則と基準に基づいています。Google では SOC 2 と SOC 3 のレポートを取得しています。 SOC 3 レポートはダウンロードしていただくことも可能です。

FedRAMP

G Suite のサービスは Federal Risk and Authorization Management Program（FedRAMP: 米国連邦政府によるリスクおよび認証管理プログラム）の要件に準拠しています。FedRAMP は米国政府が規定するクラウド セキュリティ規格です。G Suite は個人情報（PII）や管理対象非機密情報など、影響レベルが「中程度」のデータを米国連邦政府機関が管理する際に利用できるサービスとして承認されています。また、G Suite は 英国政府のセキュリティ原則 に従って、「公的な」情報（「公的な機密」情報を含む）を使用する際に適切であるとの評価も受けています。プロダクトやサービスに関するコンプライアンスについて詳しくは、FedRAMP の「Google Services」のページをご覧ください。

PCI DSS

Payment Card Industry Data Security Standard（PCI DSS）に準拠する必要があるG Suite のお客様については、データ損失防止（DLP）ポリシーを設定し、ペイメント カード情報を含むメールが G Suite から送信されないようすることができます。ドライブについては、監査が実施されるように Vault を設定したうえで、カード保有者に関するデータを一切保管しないようにすることも可能です。

FISC 安全対策基準

FISC（金融情報システムセンター）は、日本の金融情報システムに関する技術、利用、管理、脅威および防御に関連した研究を行う公益財団法人です。この組織が作成した主要なドキュメントの 1 つに、設備、運用、技術的インフラストラクチャに関する管理について解説されている「金融機関等コンピュータ システムの安全対策基準・解説書」があります。Google では、Google の管理環境が FISC ガイドラインにどのように準拠しているかについて、お客様に理解を深めていただけるようガイドを作成しました。Google のガイドで概説されている管理の多くは、第三者による監視対象となる ISO 27001、ISO 27017、ISO 27108 などのコンプライアンス プログラムの一部となっています。FISC による管理に対する Google の対応についてご覧ください。

法令遵守

HIPAA

G Suite は、保護対象医療情報（PHI）の保護、使用、開示を統制する U.S. Health Insurance Portability and Accountability Act（HIPAA: 米国の医療保険の相互運用性と説明責任に関する法律）をお客様が遵守できるよう支対応しています。HIPAA の対象となるお客様で、PHI の処理や保管に G Suite のご利用を希望される場合は、Google の 業務提携契約の修正条項 にご署名ください。詳しくは、G Suite の HIPAA コンプライアンス対応をご覧ください。

EU モデル契約条項

G Suite は、Google の データ処理の修正条項、データ処理再委託者の情報開示規定、EU モデル契約条項 に則って、第 29 条作業部会のデータ保護勧告に対応しているほか、EU モデル契約条項も継続的に遵守しています。また、プライバシー シールドも継続的に遵守してデータ可搬性を確保しているため、管理者は追加料金を課金されることなく、標準的な形式でデータを書き出すことができます。

一般データ保護規則

Google は、2018 年 5 月までに General Data Protection Regulation 2016/679（GDPR: 一般データ保護規則）に準拠できるよう取り組みを進めており、G Suite の データ処理の修正条項 を更新して GDPR の次回の改定内容を期日までに反映させる予定です。Google は長年にわたって、このデータ処理の修正事項とモデル契約条項を通じて厳格なポリシー、プロセス、管理を実施してきたほか、欧州データ保護当局と緊密に連携してその要件に準拠してきました。

米国家庭教育の権利とプライバシーに関する法 (FERPA)

G Suite for Education は数多くの学生の皆さまにご利用いただいています。G Suitefor Education のサービスは、家庭教育の権利とプライバシーに関する法律（FERPA: Family Educational Rights and Privacy Act）に準拠しています。FERPA への準拠については、Google の 利用規約に規定されています。

COPPA

オンラインで子どもたちを保護することは、Google にとって重要です。そこで、1998 年児童オンラインプライバシー保護法（COPPA: Children's Online Privacy Protection Act of 1998）の要件に基づき、G Suite for Education をご利用いただいている学校に対して、Google のサービスを利用する際に保護者の同意を得ることを契約で義務付けています。Google サービスは COPPA に準拠した形で利用することができます。

南アフリカの個人情報保護法 (POPI 法)

Google はサービス内のさまざまな機能や契約義務を通じて、お客様が南アフリカの 個人情報保護法（POPI 法）を遵守できるようにしています。POPI の適用対象となるお客様は、データ処理の修正条項に署名することで、ご自身のデータの保存方法、処理方法、保護方法を規定できます。

電子情報開示とアーカイブ

データの保持と電子情報開示

Google Vault では、組織のメールの保持、アーカイブ、検索、書き出しが可能で、電子情報開示やコンプライアンスの要件を満たせます。完全にウェブベースのサービスのため、追加のソフトウェアのインストールやメンテナンスは必要はありません。Vault では Gmail、Google ドライブ、Google グループのデータを検索したり、カスタムの保持ポリシーを設定したり、ユーザー アカウントや関連データを訴訟のための保持記録（リティゲーション ホールド）の対象にしたりできます。また、任意の時点でドライブにあるファイルを書き出すことも、関連する検索を管理することも可能です。

証拠の書き出し

Google Vault を利用すると、法的な基準やデータ管理に関する一連のガイドラインに沿う形で特定のメール、記録対象のチャットやファイルを標準的な形式で書き出して、追加処理や見直しを行うことができます。

コンテンツ コンプライアンス

G Suite's の監視ツールを利用すれば、管理者はメールをスキャンして、 英数字のパターン や 不適切なコンテンツ が含まれているメールを抽出できます。また、ルールを作成し、そのルールに一致するメールに対して「宛先に配信される前に拒否する」または「内容を変更して配信する」のいずれかの措置を適用できます。

レポート解析

簡単な管理

使いやすいインタラクティブなレポートを利用して、組織がさらされているセキュリティ上の問題をドメインレベルやユーザーレベルで評価できます。さまざまなアプリケーション プログラミング インターフェース(APIs) を使った拡張も行えるため、利用環境に適したカスタム セキュリティ ツールを構築することができます。ユーザーによるデータの共有状況、インストールされているサードパーティ製アプリ、2 段階認証プロセスなどの適切なセキュリティ対策の整備に関するインサイトを活用してセキュリティ体制を改善できます。

監査の追跡

G Suite 管理者は、 G Suite 内の ユーザーの操作を追跡 したり、カスタム通知を設定したりできます。この追跡機能は、管理コンソール、 Gmail、ドライブ、カレンダー、グループ、モバイル、サードパーティ製アプリケーションの承認設定を対象としています。たとえば、指定したファイルがダウンロードされたときや、「機密」という言葉が含まれるファイルが組織外部と共有されたときなどに、管理者に通知が届くように設定できます。

BigQuery によるインサイトの獲得

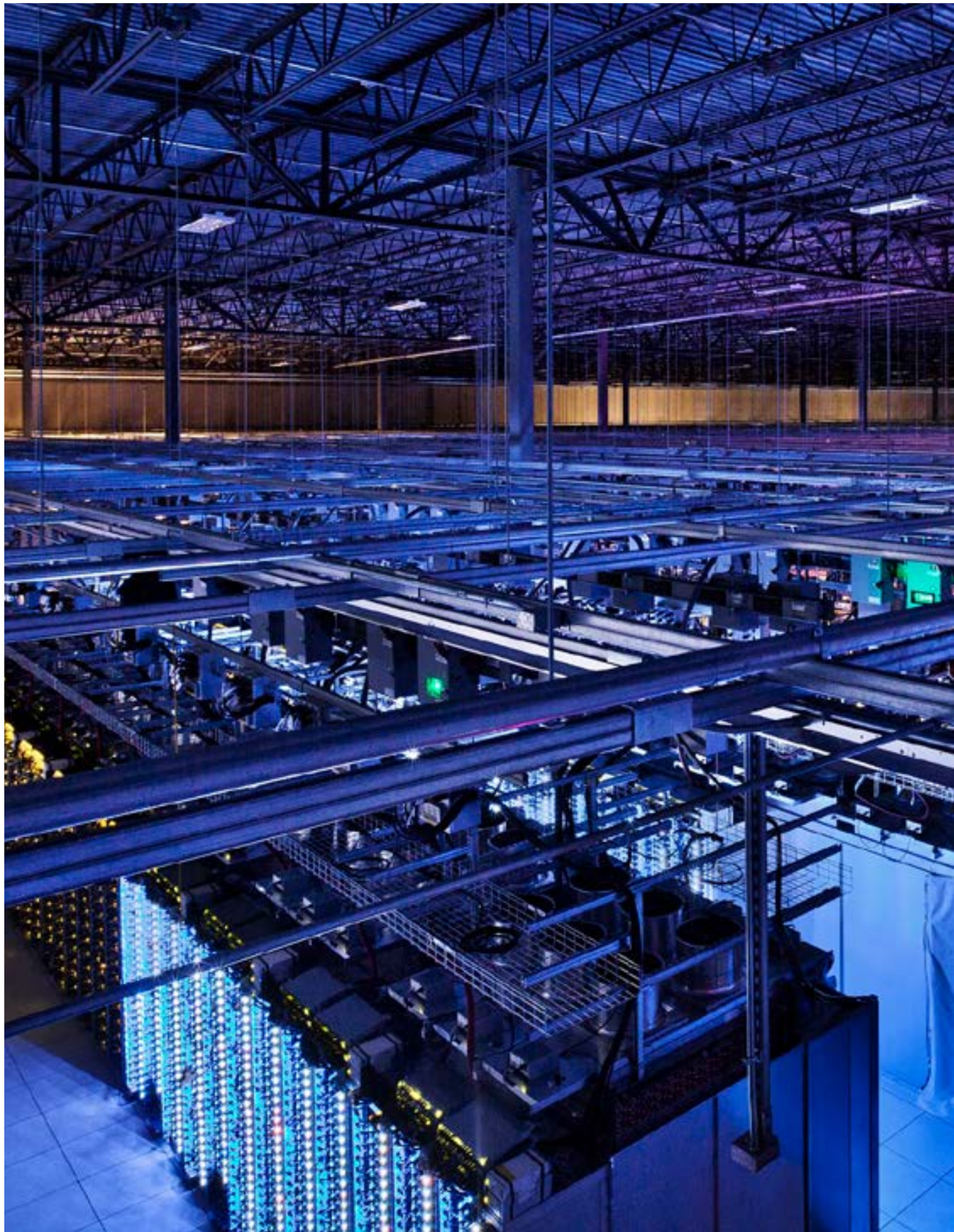
大規模なデータ解析に対応する Google の企業向けデータ ウェアハウス、BigQuery, を利用すると、洗練された高性能のカスタムクエリを使って Gmail ログを分析したり、サードパーティ製ツールを活用してさらに詳細な分析を行ったりできます。

透明性

パートナーシップには信頼性が必須

Google は透明性を重視しています。透明性を通じてお客様と信頼関係を築き、それを維持するために真摯に取り組んでいます。お客様のデータは Google ではなくお客様に帰属するものであり、Google がお客様のデータを第三者に販売することはありません。また、G Suite に広告が表示されることはなく、Google が広告を目的に G Suite のサービスからデータを収集したり、利用することも一切ありません。

お客様のデータを保護することに対する Google の責任については、Data Processing Amendment に詳しく記載されています。たとえば、データ処理の修正条項に基づき、Google は契約で指定された目的のためにお客様のデータを処理します。また、お客様が Google のサービスから削除したデータは、180 日以内に Google のシステムから完全に削除することを保証しています。さらに、お客様が Google のすべてのサービスの利用を停止される場合にデータを簡単に移行できるツールも提供しており、解約金や追加料金を課すことはありません。



広告の掲載は一切なし

Google が広告を目的に G Suite サービス内のユーザーデータを収集、スキャン、使用したり、G Suite に広告を表示したりすることはありません。お客様のデータは G Suite のサービスの提供のほか、システム サポート（迷惑メールの自動振り分け、ウィルス検出、スペルチェック、キャパシティ プランニング、トラフィック ルーティング、個人アカウント内でのメールやファイルの検索機能など）のために使用させていただきます。

データはお客様に帰属

企業、学校、政府機関がデータの保管に G Suite のサービスを利用しても、そのデータの所有権が Google に移行するわけではありません。企業の知的財産であれ、個人情報であれ、学校の宿題であれ、Google がお客様のデータを所有したり、第三者に売却したりすることはありません。

アプリへのアクセスは常に可能

G Suite は 99.9% のサービスレベル契約を提供しています。また、G Suite には計画的ダウンタイムやメンテナンスの時間枠もありません。他の多くのプロバイダとは異なり、Google では綿密な計画のもとに、サービスのアップグレード時やシステムのメンテナンス中でも常にアプリケーションを ご利用いただける ようにしています。

管理と監視が常に可能

Google では、システムや処理に関する情報（リアルタイムのパフォーマンスの概要、データの取り扱いに関する監査結果、データセンターの場所など）についてお客様に開示するよう努めています。お客様のデータは、所有者であるお客様が管理できるようになっており、いつでも削除したり、書き出したりしていただけます。また、Google では定期的に透明性レポートを公開し、政府やその他の機関がお客様のオンライン上のセキュリティやプライバシーにどのような影響を与える可能性があるのかについて詳細にお知らせしています。Google には、お客様の知る権利を尊重して、逐次情報を開示し、お客様の権利を保護してきた実績があります。

Google Cloud