Google Cloud の
セキュリティに対するアプローチ

Google Cloud

目次

常に一歩先へ。

日を追うごとに手法が巧妙化するサイバー攻撃。この脅威からグローバル　ネットワークを保護することは、現代の最重要課題の　1　つとなっています。Google では、米国、南米、ヨーロッパ、アジアにあるデータセンターで脅威に対する取り組みを日常的に実施し、公共部門と民間企業の数十億人のユーザーを守っています。

Google　のグローバル　ネットワークが保護するのは、Google　検索、YouTube、マップ、　Gmailなど、人気の高いサービスを含む7部門。各部門がそれぞれ10億人を超えるユーザーに利用されています。また、　Google の広告サービスを利用している広告会社やメディア企業のデータとオペレーションも保護の範囲に含まれます。Google　がここまで順調に成長し続けることができたのは、サービス、インフラストラクチャ、そしてユーザーのデータを安全に保護することを事業の核としてきたためです。脅威に対する進歩的な取り組みは、業界のベスト　プラクティスを実践することにとどまりません。Google　では高度なツールとストラテジーを独自に開発し、テクノロジー業界全体のセキュリティをリードしてきました。

システム間の通信を可能にするルールである、ネットワークコミュニケーションプロトコル。Google　では、このプロトコルを　1　秒間に数回の頻度で変更し、悪意のある侵入を防いでいます。Google Cloud 内のデータは、送受信中も保存されている状態でも暗号化されています。また、　Google　のネットワークはどんなトラフィック負荷も余裕をもって処理できる容量を備えています。そのため、ネットワークに過剰な負荷をかけてサービスを妨害しようとする分散型サービス拒否攻撃（DDoS）を受けたとしても、サービスの提供に影響を及ぼすことなく攻撃元を特定してトラフィックを停止できます。この他にも、さまざまなソリューション、ツール、プロセスを備えて、多層防御を行っています。

Google　のセキュリティに対する取り組みは、プラットフォームからインフラストラクチャ、ソフトウェアソリューション、独自設計の専用ハードウェアにいたるまで、すべてのサービスの基盤となるものです。データとアプリケーションはセキュリティとコンプライアンスの基準を満たしているため、Google　のお客様は安心してサービスをご利用いただけます。

この電子ペーパーでは、セキュリティとプライバシーに対する Google のアプローチを詳しくご紹介していきます。特に重要なデータとアプリケーションを Google に託せるかどうかを判断する際の参照資料としてご活用ください。

Google のセキュリティが 1 分間に処理するもの

1,000 万

Gmail ユーザーへの配信を阻止された迷惑メールの件数

694,000

有害ソフトウェアが含まれていないかどうかスキャンされた、インデックス登録済みウェブページの数

7,000

ブラウザの拡張機能で停止された偽装 URL、ファイル、コードの数

6,000

Chrome ユーザーに報告された望ましくないソフトウェア インスタンスの数

1,000

Chrome ユーザーに報告された不正なソフトウェアの疑いがあるソフトウェア インスタンスの数

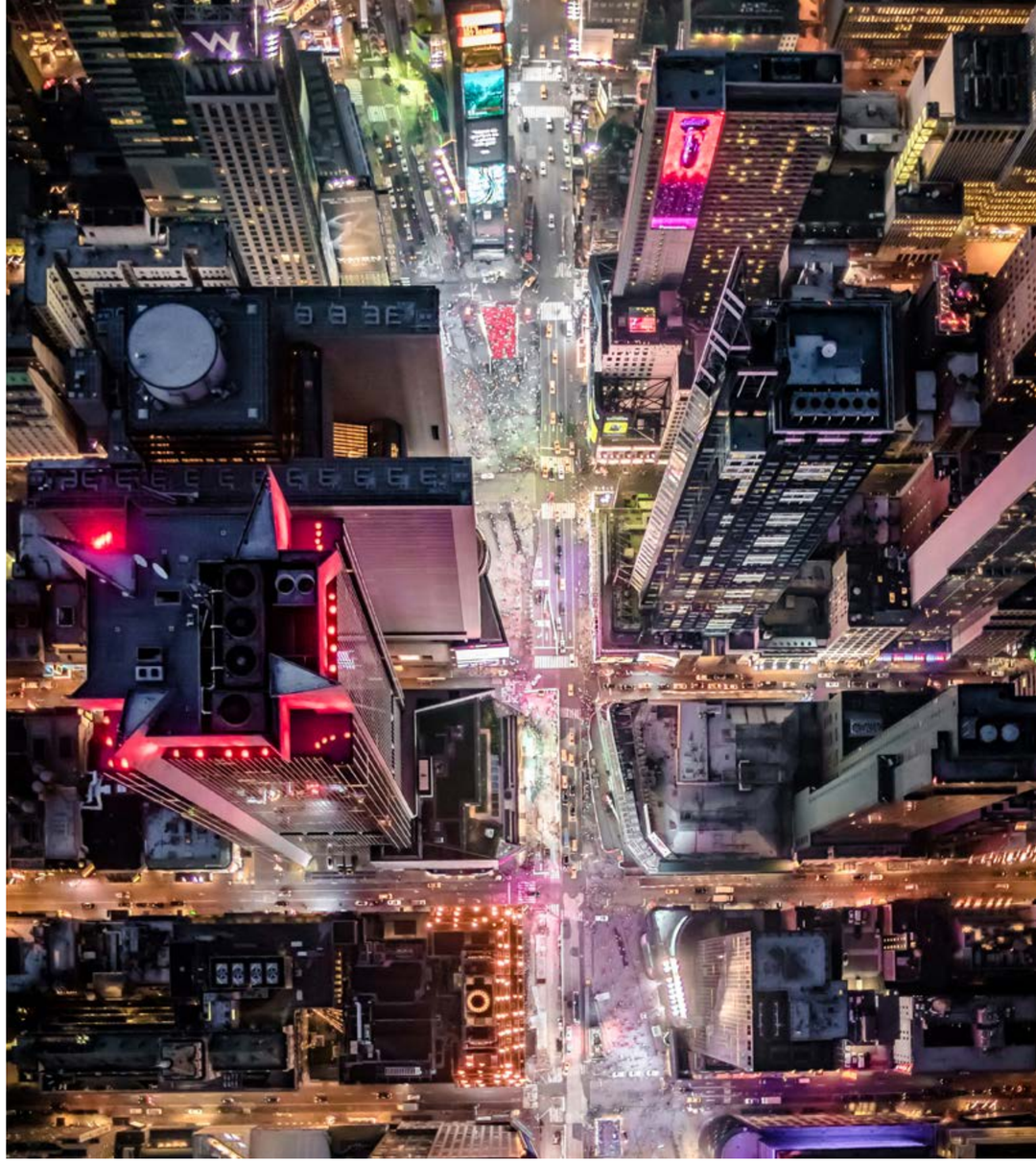
2

特定され、緩和されたフィッシング サイトの数（その他、特定および緩和された不正なソフトウェア サイトが 1 件）

リサーチ特集:
パブリック クラウドにおける セキュリティの未来

Google Cloud のセキュリティ チームの専門知識をビジネスに活用する McKinsey & Company。この企業が 100 の企業を対象に行った最近の調査では、回答者のほとんどが 3 年以内にパブリック クラウドの導入率を 2 倍に増やす予定であるという結果が出ています。これは、現在の 19% から 38% への増加となります。回答した組織の中には、将来的にワークロードの 90% がクラウドに移行すると予測するところもありました。

また、この調査結果では、ハイブリッド型のマルチクラウドならではの難しさも浮き彫りになっています。さまざまな構成とワークフローが混在する場合、単純にオンプレミスのセキュリティ コントロールをパブリック クラウドへと拡張するわけにはいかないのです。共有型のエンドツーエンドのセキュリティ モデルを導入するには、クラウド プロバイダと密接に連携することが求められます。



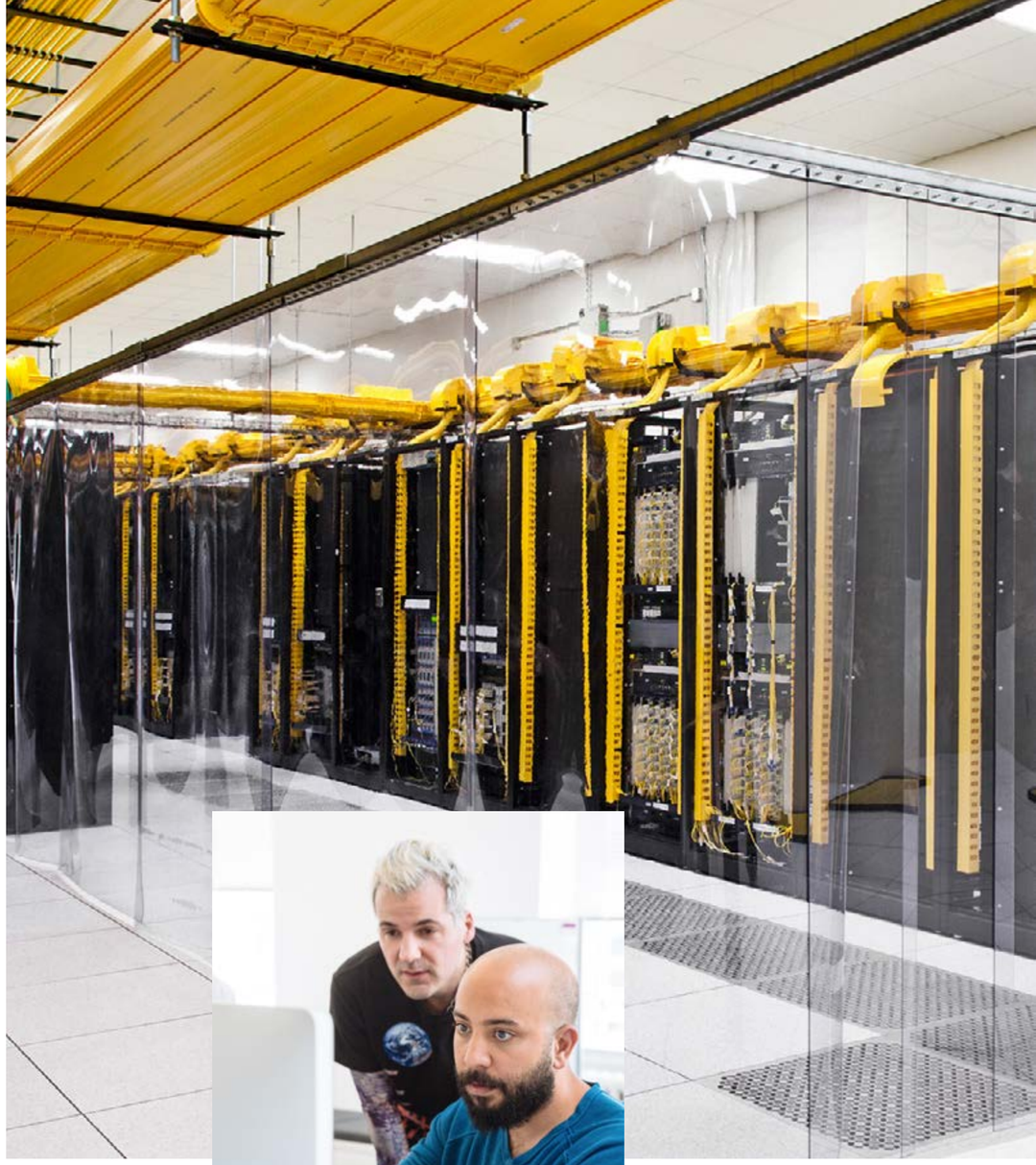
セキュリティの
基準を引き上げる

Google Cloud

セキュリティを重視する企業文化

Google では、850 人以上のセキュリティ プロフェッショナルがモニタリング、設計、研究に従事し、インターネットの専門家やユーザーのグローバル コミュニティと連携して取り組みを行っています。脆弱性の特定、ソフトウェアベンダーに対するバグの報告のほか、新しいセキュリティソリューションやアプローチの設計なども彼らの仕事です。

セキュリティは、Googleのソフトウェア開発プロセス全体に組み込まれています。その一例として、新しいサービスや機能に対してアーキテクチャやコードの分析を行い、脆弱性の発見や攻撃モデルの予測に役立てています。問題が発生した場合は、サービスへの影響が最小限で済むよう、専門のインシデント管理チームが迅速に対応、分析、修正にあたります。



脅威の防止と検出

Google Cloud をサイバー攻撃の脅威から効果的に保護するためには、警戒、イノベーション、敏捷性、そして高度な検出機能が必要です。Google がネットワークを安全な状態に保ち続けられる理由には、長年にわたって大量のインターネット トラフィックを処理してきた経験と、人工知能、大規模データセット、世界規模のインフラストラクチャへの投資が挙げられます。

企業のウェブマスターとアプリケーション開発者は、悪意のある攻撃があった場合に直接通知を受け取るだけでなく、ネットワークをモニタリングする診断ツールを活用できます。また、フィッシング攻撃に関する Google の研究から開発されたのがセキュリティ キーです。これは、簡単な操作で公開鍵暗号を使える小型のハードウェアデバイスで、強力な認証を実現します。セキュリティ キーは、Google Cloud Platform と G Suite を含む、Google Cloud サービス全体でユーザー アカウントを保護する役目を果たしています。

Google はこれまでにも、Google Chromebook などの端末を安全に保護するための対策に取り組んできました。企業のお客様は、この長年の経験が生かされたサービスをご利用いただけます。Google データセンターに採用されたのと同じセキュリティ原則の多くが使われており、高度な ID 管理、データ露出の最小化、端末の一元管理などの機能とプラクティスが、脅威に対する防御をさらにハイレベルなものにしています。

セキュリティ分野における世界的なパイオニア

Google　はこれまでに、セキュリティ、プライバシー、不正行為防止に関する論文を 300 編近く公開してきました。また、業界全体におけるソフトウェアセキュリティを向上させるため、多くのツールも配布しています。このようなツールの多くはオープンソースでリリースされ、他のオープンソースのソフトウェアアプリケーション同様、コミュニティとイノベーションの促進をサポートするものとなっています。その他にも、オープンソースへの20件を超えるソフトウェアプロジェクトの寄付、セキュリティプラクティスを向上させるための取り組み、オープンソースの Linux と Chrome の 100 以上のセキュリティ バグの修正などの取り組みを通じてセキュリティ分野に貢献しています。

前方秘匿性

Google は、前方秘匿性を初めて実現した大手クラウド プロバイダ。この機能は、暗号化された通信に対する強力な保護対策となり、秘密鍵やパスワードが不正利用される可能性を大きく減らしました。2011 年から、Gmail、Google ドキュメント、暗号化検索サービスに導入されています。

安全なリモート アクセスの手法を見直す

Googleの従業員にはアプリケーションへの安全なリモートアクセスが提供されていますが、大規模なプロジェクトが発生した際、その手法を見直す必要に迫られました。ここから生まれたのが BeyondCorp。Google の革新的なゼロトラスト セキュリティ モデルです。BeyondCorp では、人や端末がネットワークの内側にいるか外側にいるかではなく、IDや端末が信頼されているかどうかに基づいて計算を行い、個々のサービスへのアクセスを必要に応じて許可します。このモデルの登場により、従業員はどんな場所からでも Google のコアインフラストラクチャに安全にアクセスできるようになりました。従来から使用されてきた VPN はこれよりも安全性が低いため、Google では使用していません。

Google のゼロトラスト モデルは、ネットワークではなくユーザーに安全な認証が関連付けられているため、従業員は端末や場所を選ばずログインすることが可能になりました。つまり、どんな場所からでもシームレスに、そして安全に作業を進めることができ、より高いレベルの信頼性と生産性が期待できます。ユーザーがアクセスできるリソースを決めるポリシーは、管理者がコントロールを行います。

さらに強力な暗号化技術

暗号化技術の進歩に合わせて高まる脅威への保護対策として、Google は 2013 年に RSA 暗号鍵の長さを 2,048 ビットに延長。また、数週間ごとに鍵を変更するようになりました。

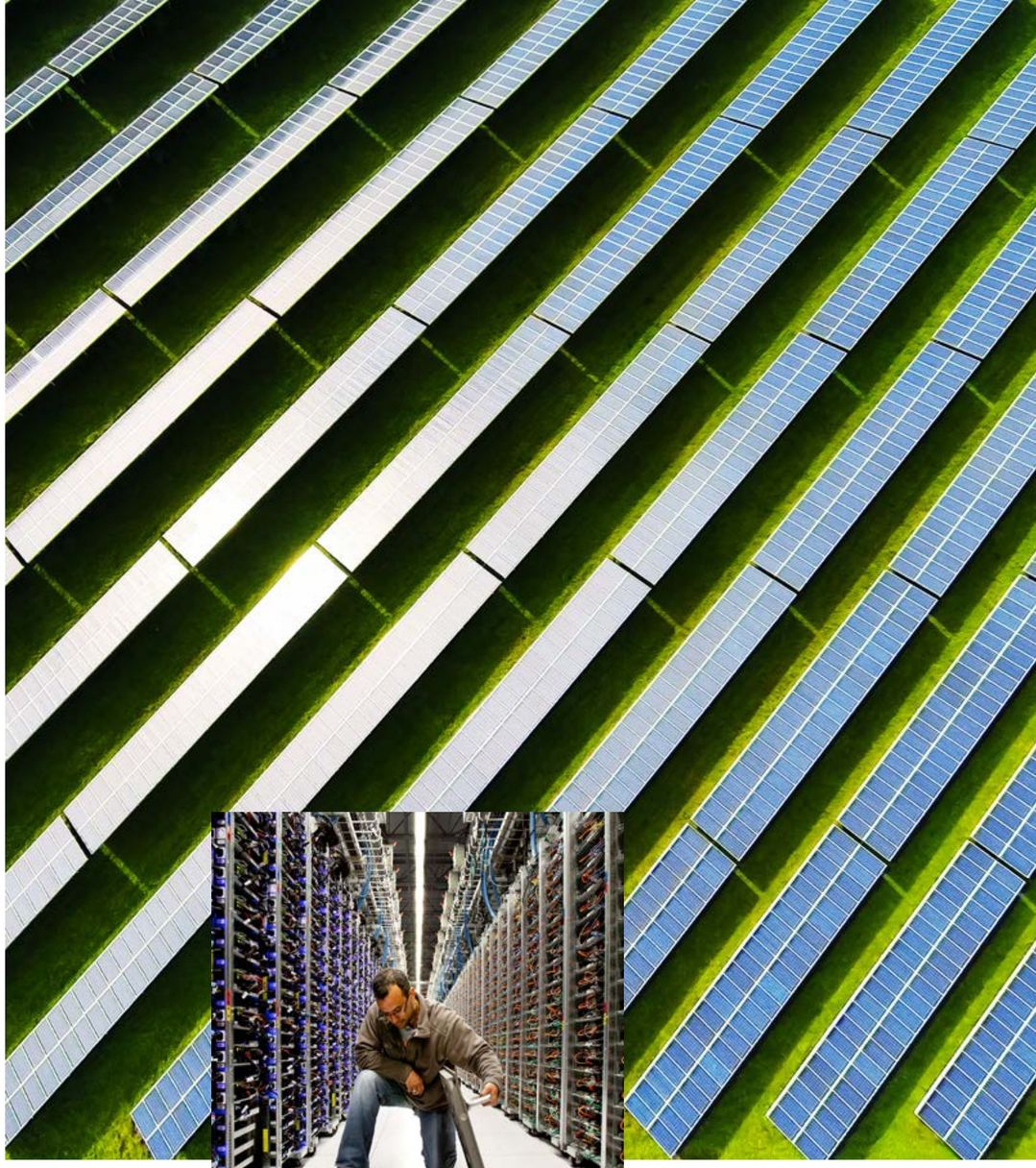
2017 年には、デジタル証明書を発行する独自のルート認証局として、Google Trust Services を開設。デジタル証明書は、信頼できるサード パーティーが公開鍵（通信で広く使用される X.509 暗号規格の一部）の所有権を認証するのと同じ意味を持ちます。

設計から考えられた
安全性

Google Cloud

設計から考えられた安全性

Google Cloud では、データセンターから端末にいたるデータのライフサイクル全体でセキュリティを管理しています。コラボレーションモデルのクラウドでは、お客様の企業独自のセキュリティ対策を追加できます。Google Cloudのセキュリティでは、さまざまな技術、アプローチ、規格、手法を活用し、アプリケーション、IT リソース、お客様のデータを保護しています。



多層的なアプローチ

Google Cloud Platform のインフラストラクチャ セキュリティは、ハードウェア、サービス、ユーザー識別、ストレージ、インターネット通信、オペレーションという複数の階層を持つ構造で設計されています。Googleではこれを多層防御と呼び、それぞれの層でアクセスと権限を厳しく管理しています。物理的なデータセンターのコンポーネントから、ハードウェアの供給元、ブートのセキュリティ、サービス間通信のセキュリティ、データのセキュリティ、インターネットのサービスへの保護アクセスにいたるまで、Google Cloud のセキュリティに対するアプローチは実効性が高く、現在も進化を続けています。また、こうした多層セキュリティに加え、Googleではオペレーション レベルでもセキュリティのための技術とプロセスを導入し、さらにセキュリティを高めています。

施設とハードウェアのセキュリティ

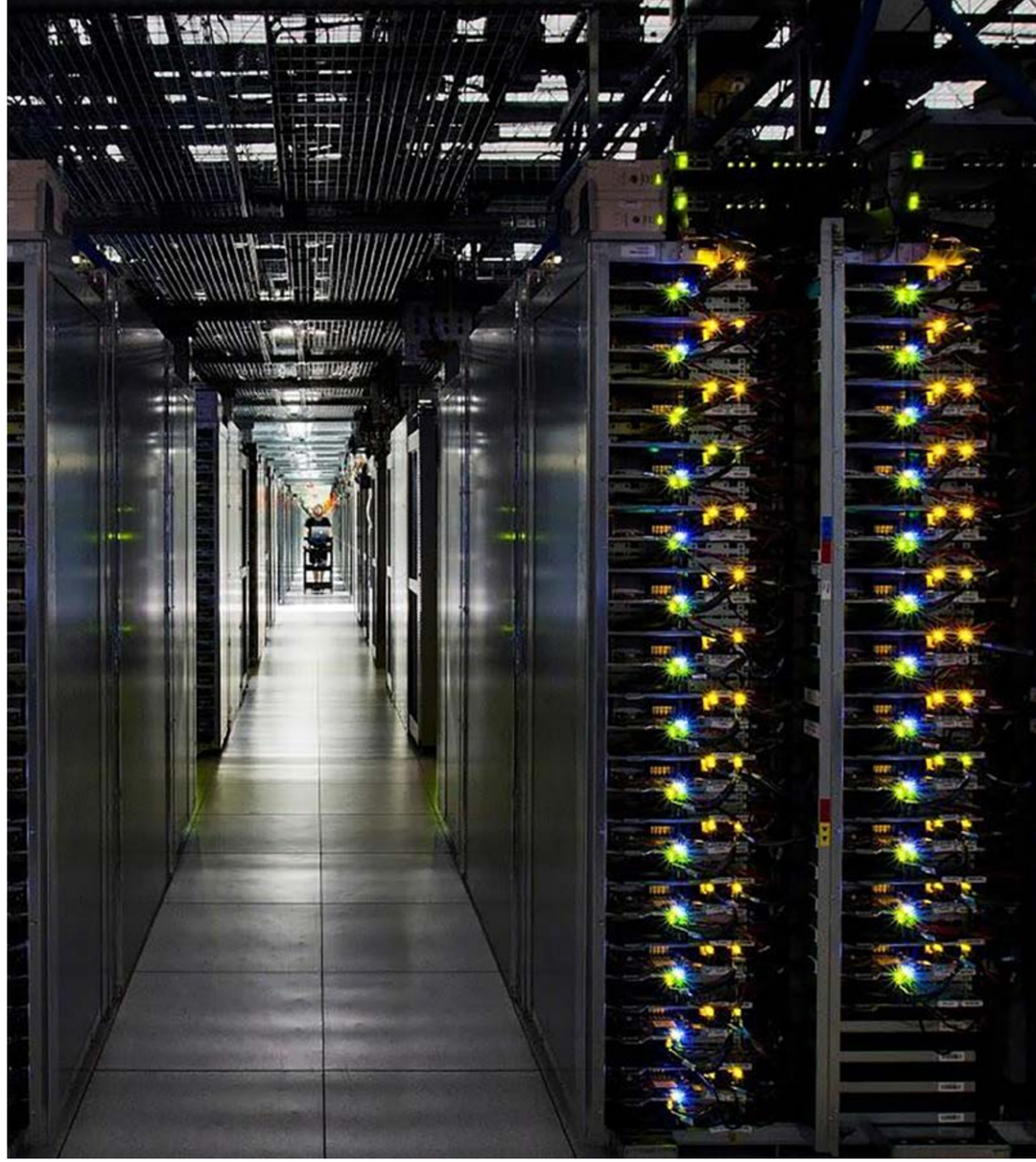
Googleのデータセンターにアクセスできるのは、特別な許可を得たごく少数の従業員に限られています。また、それぞれの階を安全に保つため、物理的にも複数のセキュリティ層を設けています。生体認証、金属探知器、カメラ、物理的な障壁、レーザーを使った侵入検知などの技術がその一例です。

データセンターにはローカルネットワークに接続された数千台のサーバーがあり、これが最初のセキュリティ層となります。サーバーボードとネットワーク機器は、Google の厳格なセキュリティ要件を満たすよう、独自に設計されたものを使用しています。他社の製品を使用する場合は、使用前にそのコンポーネントのセキュリティ プロパティの検証と確認を行います。Titan は Google 独自の設計によるチップの一つで、このハードウェアのセキュリティ チップをサーバーと周辺機器の両方にデプロイすることで、正規の Google 端末をハードウェア レベルで識別、認証できるようになっています。

ブートスタックと
マシン ID のセキュリティ

ブートに適切なソフトウェアスタックが使われるようにするため、Google　のサーバーマシンにはさまざまな技術が使われています。このような技術はすべて　Google　のエンジニアが設計、管理、増強を行っており、現在も進歩を続けています。自動システムによりサーバーでは常にセキュリティ　パッチを含む最新バージョンのソフトウェアが実行されます。また、ハードウェアとソフトウェアに関する問題の診断が行われ、対応が必要なマシンはサービスから削除されます。

それぞれのサーバーマシンには固有IDが割り当てられていて、ハードウェアのルート　オブ　トラスト（信頼の基点）とマシンがブートするソフトウェアに関連付けられるようになっています。つまり、マシンが　Google Cloud のネットワークと通信を行うたびに、その個別の ID が確認されています。



サービス ID、整合性、分離

Google Cloud では、コンピューティング、データ ストレージ、データ分析、機械学習のようなサービスに、暗号認証やアプリケーション レイヤでの認証などの高度な技術を使用しています。これはつまり、要求されたワークロードに対処するため数千台のマシンでサービスを実行していても、単一のクラスタ オーケストレーション サービスによって、最適な効率性と有用性を保った状態にコントロールされることを意味しています。

Google Cloud Platform では、IP スプーフィングを防止するため上りと下りのフィルタリングを使用していますが、内部ネットワークのセグメント化（インフラストラクチャの利用を特定のジョブを実行するために必要なネットワーク アセットだけに制限すること）やファイアウォールなどの特殊なセキュリティ アプライアンスなどは、主なセキュリティ メカニズムとして使用していません。ネットワーク内にいる全員を信頼するという前提に基づいた従来の境界セキュリティは、従業員が社内外のさまざまな場所から作業を行う企業では有効性が弱まっています。いつでも、どんな場所からでも作業できるよう、Google では別のアプローチを取っています。

各サービスにはサービス アカウント ID が関連付けられていて、暗号化された認証情報として提供されます。サーバーとクライアントは、この情報を使って ID を実証します。多くのソリューションを動かす基本的なソフトウェア プログラムである Google ソースコードは、一元化されたリポジトリに保存され、すべてのバージョンが監査可能な状態となっています。

サービス間アクセスの管理

Google Cloud プラットフォームの特定のサービスを使用するお客様には、それらのサービスのカスタマイズと管理をしていただけます。コンソールから、社内のサービスにアクセスできるサービスの指定と制限が行えます。たとえば、アプリケーション プログラミング インターフェース（API）を使って、アナリティクス バックエンド アプリケーションをエンタープライズ リソース プランニング（ERP）アプリに追加できます。また、API を使うことで、アカウント ID に基づいて特定のユーザーだけにサービスへのアクセス権を与えることもできます。

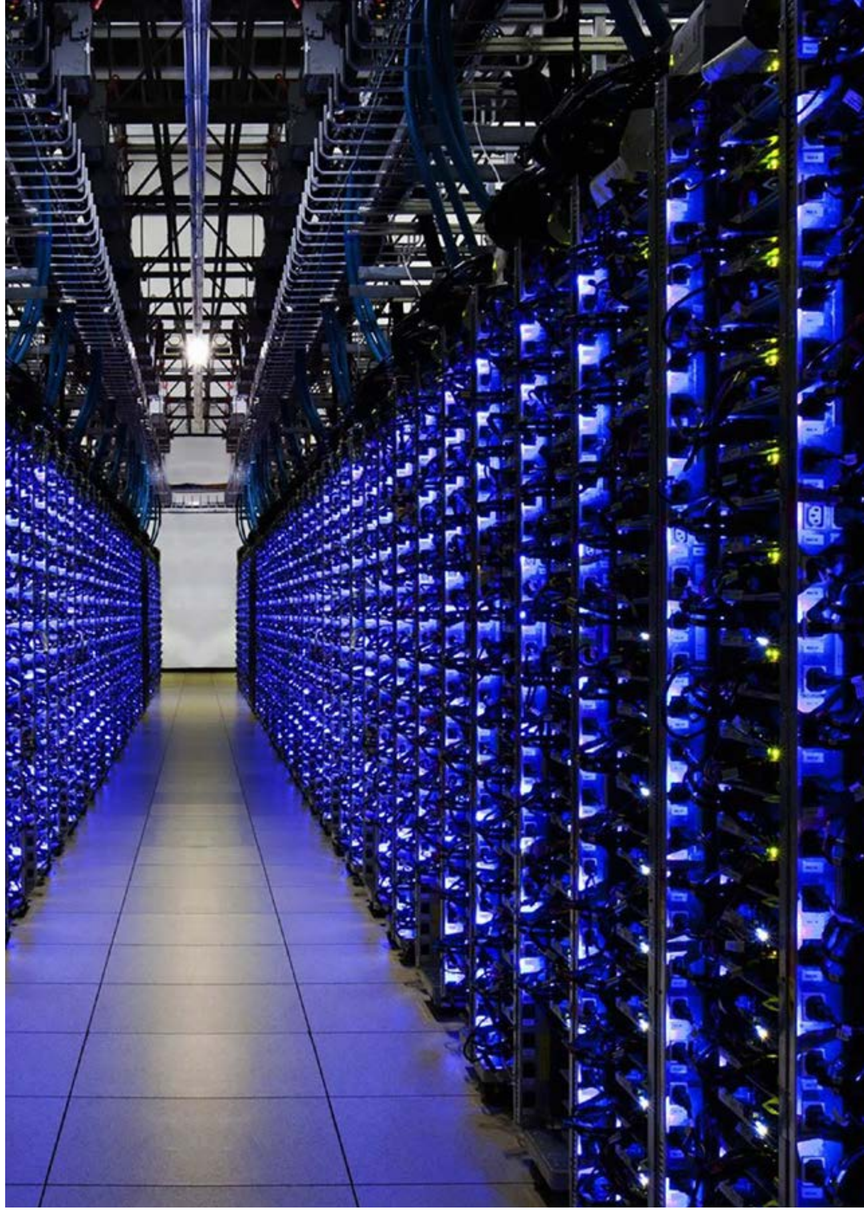
Google のエンジニアには個人 ID も発行されているので、サービスへのアクセスを個人レベルで許可することもできます。また、このインフラストラクチャでは、中央アクセス コントロール リスト（ACL）とグループ データベースからの読み込みも可能なので、別のセキュリティ対策を使用していてもユーザーとアクセス権限を検証できます。

ソフトウェアGoogleのコンテナで実行されています。これは、仮想マシンを立ち上げることなくオペレーティングシステム内からアプリケーションをデプロイできる効率の良い技術です。コンテナを利用することで、リソースの効率化だけでなく、システム単位の管理と高速なシステム監査が可能になります。構成変更やセキュリティ パッチはあらゆる場所で迅速にデプロイできるので、ダウンタイムを最小限に抑えられます。お客様には、このコンテナのオープンソース版である Kubernetes を提供しています。コンテナを利用すると、コンプライアンス監査に必要となるセキュリティ データ ログとセンシティブ データ ログに簡単にアクセスできます。以前なら数日を必要としたことが、ほんの数分間で完了します。

サービス間通信の暗号化

Google のインフラストラクチャでは、データセンター間の WAN でやり取りされるリモート プロシージャ コール（RPC）データの暗号プライバシーと整合性も提供しています。RPC は、別のネットワーク上のプログラム間でサービスをリクエストする通信を意味します。非公開の WAN リンクへの不正アクセスを試みる高度な知識を持った攻撃者から保護するため、すべてのインフラストラクチャ RPC トラフィックが自動的に暗号化されます。

暗号化とは、数学的な処理を施してデータの暗号化と復号化を行う技術です。Google では、暗号化を利用することで RPC データが秘匿された状態でネットワーク上を移動できるようにし、第三者に変更されることなく、信頼できるパートナー間でやり取りできるようにしています。このような暗号化機能は Google Cloud RPC のメカニズムに組み込まれているため、HTTP をはじめとするアプリケーション レイヤの他のプロトコルでも利用できます。これによりアプリケーション レイヤが分離され、ネットワーク パスのセキュリティに依存する必要がなくなります。たとえネットワークやネットワーク端末への不正侵入が発生しても、暗号化されたサービス間通信は安全な状態に保たれます。



エンドユーザー データのアクセス管理とアクセスの透明性

Google Cloud のインフラストラクチャでは、RPC の一部としてエンドユーザー権限チケットを発行する一元的なユーザー識別サービスを提供しています。このチケットは、サービスが特定のエンドユーザーの代わりにリクエストに応答していることを証明するものです。

エンドユーザーがログインする際には、まず一元的な識別サービスによる検証が行われ、次にユーザーのクライアント端末にユーザー認証情報（Cookie や OAuth トークンなど）が発行されます。その後、このクライアント端末から Google Cloud にリクエストをする場合、このユーザー認証情報の提示が必要となります。

2017 年、Google は SAP と提携し、共同データ管理者モデルを導入しました。このモデルでは SAP を Google Cloud にあるお客様のデータの管理者として設定し、定義済みの設定に基づく、コンプライアンスのための継続的なモニタリングが可能になっています。

データ ストレージのセキュリティ

Google のストレージサービスの多くは、一元化された鍵管理サービスの鍵を使って設定でき、物理ストレージに書き込む前にデータを暗号化できるようになっています。アプリケーションレイヤで暗号化を実行すると、インフラストラクチャは、ストレージの下位レベルでの潜在的な脅威（悪意のあるディスク ファームウェアなど）からインフラストラクチャ自体を分離することができます。また、ハードウェアによる暗号化などの別の保護レイヤも採用されています。

インターネット通信のセキュリティ

Google Cloud では、インターネットと Google Cloud のサービス間の通信が安全な状態に保たれています。インフラストラクチャをプライベート IP 空間に隔離することで外部のインターネット トラフィックと接するマシンを限定し、DDoS 攻撃の被害を軽減します。Google Cloud Armor（Cloud Load Balancer との併用で利用可能）などの機能では、攻撃元に近いネットワーク エッジで DDoS 攻撃から保護します。

Google Front End（GFE）サービスでは、すべての Transport Layer Security（TLS）接続が、必ず適切な証明書を使用し、ベスト プラクティスに従って終端されるようになっています。また、GFE では DDoS 攻撃に対する保護機能も提供しています。このしくみについて説明すると、まず、ロードバランサが中央の DDoS サービスに受信トラフィックに関する情報を報告します。DDoS 攻撃の発生が検出された場合、サービスはロードバランサにそのトラフィックをドロップさせるか上限を割り当てるよう設定できます。GFE レイヤからもアプリケーション レイヤの情報を含む DDoS の情報が報告されるので、GFE にも DDoS 攻撃が検出された場合にトラフィックをドロップさせるか上限を割り当てるよう設定できます。

Google の一元的な ID サービスは、ユーザーには Google のログインページとして表示され、ユーザー名とパスワードの入力を求めます。ここでは、過去に使われたのと同じ端末や同じ地域からログインしているかなど、さまざまなリスク要因が評価されます。そして、サービスからは Cookie や OAuth トークンなどの認証情報が発行されます。また、ログイン時には、ワンタイム パスワードやフィッシング対策用のセキュリティ キーなども使用されます。

オペレーション
セキュリティ

Googleのセキュリティチームは、年中無休でインシデントの選別、調査、対応にあたっています。セキュリティインシデントの検出とその対応を評価し、さらに向上させるため、日常的な取り組みを実施しています。Google Cloud では、開発者が特定の種類のセキュリティ バグを生み出さないようにするためのライブラリとフレームワークを提供しています。このバグには、ウェブアプリ内の XSS 脆弱性などが含まれます。また、ファザーなどのセキュリティ バグを検出するための自動ツール、静解析ツール、ウェブ セキュリティ スキャナも用意されています。さらに、手動によるセキュリティ審査も行われています。このような手動による取り組みを続けることは、一般的な組織では桁違いのコストと時間を要するものとして敬遠されています。

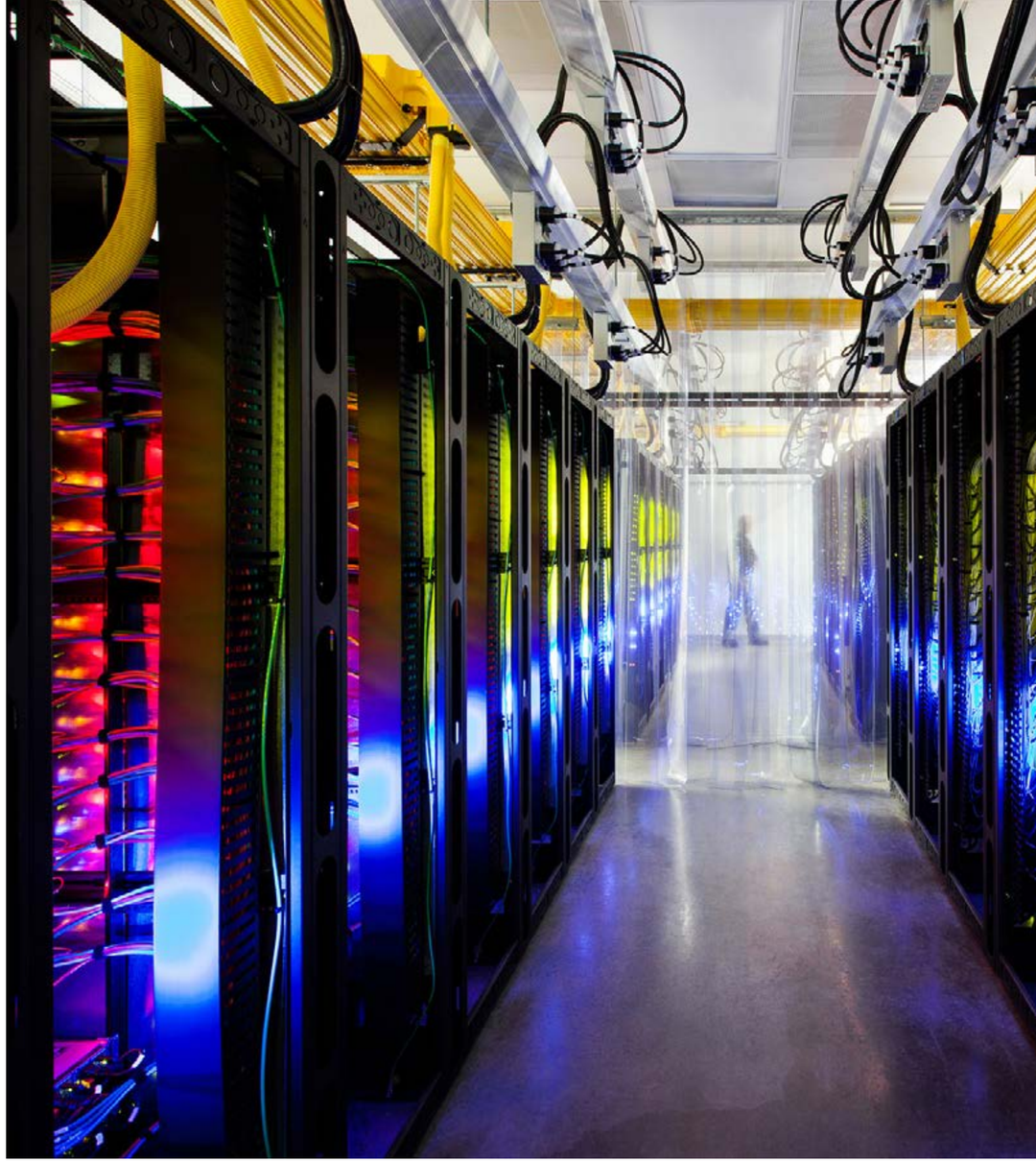
Googleでは従業員の端末と認証情報を保護するため、莫大な投資を行っています。このような投資には、物理的な設備、コンピュータ、データ、ネットワーク セキュリティ、アクセス管理、セキュリティ ロギングなどへの技術と厳格なポリシーの採用などが挙げられます。また、潜在的な情報漏洩や内部犯行者による不正行為を発見するためのモニタリングも行っています。アプリケーションレベルのアクセス管理設定では、社内アプリケーションへのアクセスを特定のユーザーに限定しています。管理者権限はごく一部の人にしか与えられず、その使用はモニタリングされています。また、個々の端末上のホストベースの信号、さまざまなモニタリングポイントからのネットワーク ベースの信号、インフラストラクチャ サービスからの信号を使った高度な侵入検知機能を採用しています。

コンプライアンスと信頼性

Google Cloud

セキュリティの
世界基準に対応する

Google は世界規模のネットワークとして、各拠点国で定められたネットワーク、データ、プライバシー、オペレーションのポリシーを採用しています。そのため、Google Cloud のお客様は、安心してポリシー、規制、ビジネス要件、コンプライアンスを満たしたサービスをご利用いただけます。Google が採用する業界基準には、国際標準化機構（ISO）、American Institute of Certified Public Accountants（AICPA: 米国公認会計士協会）の Service Organization Controls（SOC）2 および 3、Payment Card Industry Data Security Standard（PCI DSS: 支払いカード業界データ セキュリティ基準）、米国の National Institute of Standards and Technology（NIST: アメリカ国立標準技術研究所）の基準などがあります。



プライバシーとコンプライアンスの厳しい基準を満たす

Google Cloud は、欧州連合の一般データ保護規則（GDPR）に準拠するための取り組みを行っています。GDPR は個人データに対する個人の権利を向上させ、ヨーロッパ全体でデータ保護法を統一することを目指しています。また、Google Cloud では、オーストラリアの Australian Privacy Principles（APPs）および Australian Prudential Regulation Authority（APRA）の基準、日本の金融情報システムセンター（FISC）のガイドライン、シンガポールの Multi-Tier Cloud Security（MTCS）Singapore Standard（SS）584、スペインの Esquema Nacional de Seguridad（ENS）認定スキーム、英国の NCSC クラウド セキュリティ原則を遵守するための方法について説明したドキュメントを作成しています。

信頼性を第一に考えたアプローチ

Google Cloud Trust Principles では、お客様のデータのプライバシーを保護するための Google の取り組みについてまとめています。データは Google のものではなく、お客様のものです。データ分離、リージョンごとの設定、鍵暗号化、取り消しなどの要因を適用することで、データを Google Cloud にどのように保存するかを決められます。また、Google Cloud の利用を停止する場合、いつでもデータを移行できます。

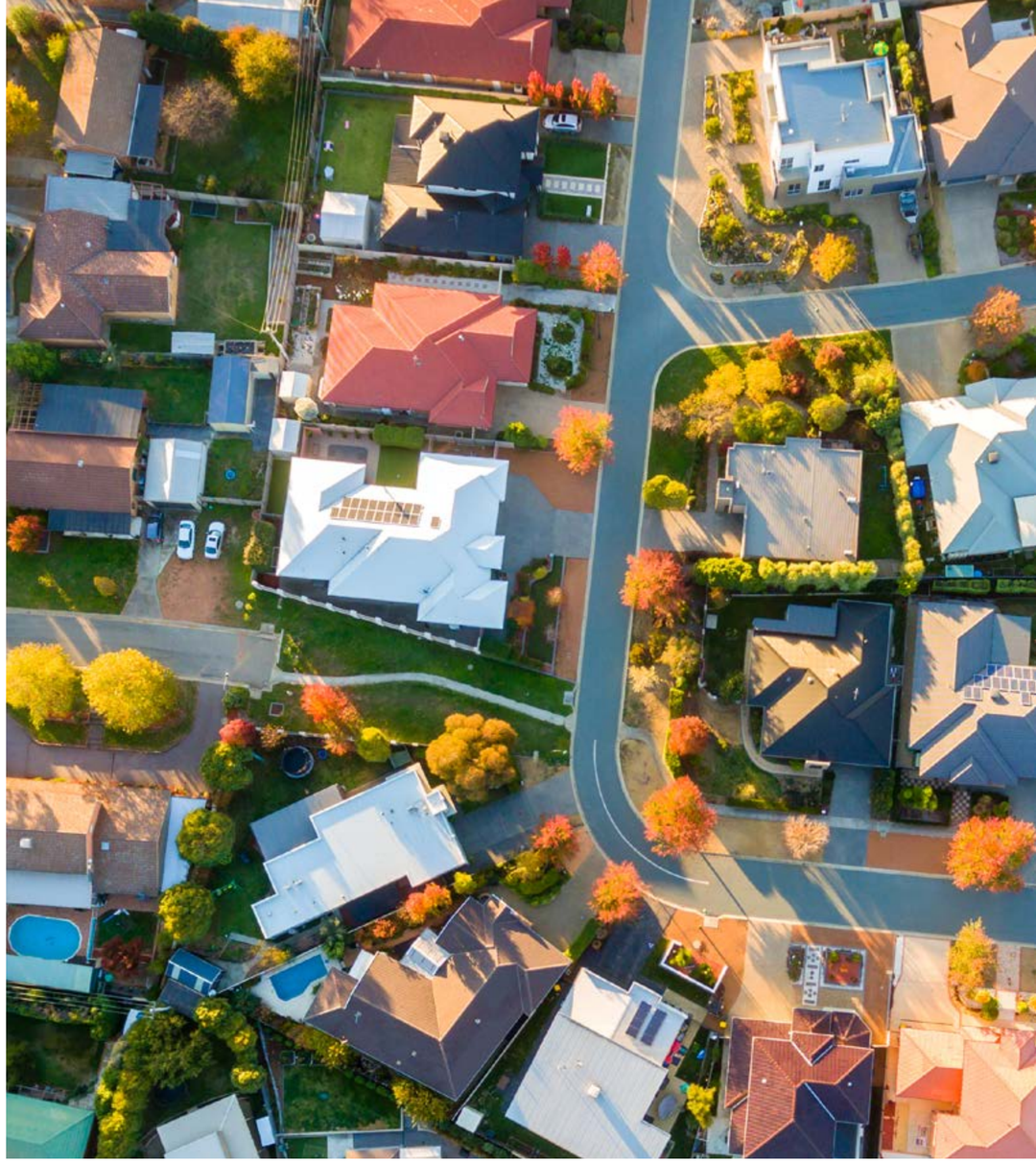
企業の保護性を
さらに高める

Google Cloud の大規模なオペレーションとセキュリティ リサーチ コミュニティとのコラボレーションにより、脆弱性の予防や迅速な対処が可能になりました。Google Cloud を利用するお客様は、各社独自のセキュリティ対策をコラボレーション パートナーシップ モデルで Google Cloud に拡張することで、セキュリティを高めるだけでなく、新しいサービスやビジネスモデルを提供して新たな収益源を得ることができます。

ロンドンを拠点とする金融テクノロジー企業の Ravelin は、機械学習と呼ばれる人工知能技術を使い、オンライン不正防止の分野におけるリーダー的存在になりました。Ravelin は Google Cloud のオープンソース技術への取り組みを活用し、企業のインフラストラクチャ全体を Google Cloud Platform に移行したのです。Google Cloud の強力なセキュリティと最先端の暗号化により、ISO/IEC 27001 と Payment Card Industry Data Security Standards（PCI DSS）に準拠しながら、クライアントのクレジット カード情報、ロケーション データ、個人情報をより安全に保存、分析できるようになっています。Ravelin の不正防止機械学習モデルでは 300 ミリ秒以内にトランザクションの処理を行い、2017 年までに 1 億ポンドを超える不正なトランザクションを停止させ、3 年間で 12 ペタバイト以上のデータを分析しています。

世界的に分散された ネットワーク

Google では、地域を問わず数百万人のユーザーがアクセスできるサービスを提供しています。Google Cloud は地理的に分散されたインフラストラクチャを使用してサービスを運用しており、そこで実行されるサービスの可用性と稼働時間は最大限に高められます。一般的に、データが単一のハードドライブ、サーバーラック、データセンター上に存在することはありません。データはいつでも利用可能な状態で安全に保管されているので、インドやオクラホマ州からでも、ニューヨークやドイツからと同じように簡単にアクセスできます。この信頼性、途切れることのない可用性、Google Cloud のセキュリティ、安全なデータ処理のためのベスト プラクティス、コンプライアンスのための取り組みが、世界中の企業の間で Google Cloud が人気を集め続ける理由です。



Conclusion

まとめ

Google Cloud

Google Cloud の 3 つの理念

お客様のビジネスを保護するため、人材、プロセス、技術を適切に調節できるコラボレーションプロセスを通じて、新しい脅威とセキュリティの課題に対処します。世界最大のコンピューティング　ネットワーク　インフラストラクチャに構築されたクラウドをビジネスに採用することで、Google Cloudの専門知識と経験、現在と未来の脅威に対処する敏捷性というメリットが手に入ります。GoogleCloud　のお客様が利用するインフラストラクチャは、機械学習、AI、IoT など、Google を持続、進歩させているインフラストラクチャと同じものです。

いつでもお客様がデータを管理できます。データの収集方法だけでなく、プロバイダ、従業員、顧客が利用するデータもお客様が設定できます。Google Cloud では、お客様にデータの透明性とアクセス管理機能を提供することに取り組んでおり、Google　の国際的なセキュリティとプライバシーの基準は、独立監査機関によって認証され、その正当性が認められています。また、Google Cloud　がお客様のデータを販売することは決してありません。

コンプライアンスを促進する世界的なセキュリティ基準に対応するための懸命な努力をしています。このコンプライアンスには、お客様の組織で求められる社内ポリシーや外部の規則も含まれます。また、データの取集方法、利用方法、アクセス方法も対象となります。Google　Cloudが提供する設定や機能は、今後も拡張を続けていきます。世界的なセキュリティ基準の一例には、SSAE16/ISAE3402 TypeII、ISO27001/27017/27018、FedRAMP、PCI DSS、HIPAA、CSASTAR、MTCSTier3、GDPR（ヨーロッパ）、NIST 800-171/800-53、FISC（日本）、MPAA、SOX、Australian Privacy Act およびAPPs、APRA　Standards、ENC（スペイン）などが挙げられます。

Google のセキュリティに対するアプローチのさらに
詳しい情報は、Google のウェブサイトをご覧ください。

Google Cloud