Google Cloud

Google インフラストラクチャのセキュリティ設計の概要

Google Cloud ホワイトペーパー

Google Cloud

目次

Google Cloud

CIO レベルの概要

- Google には、Google の情報処理ライフサイクル全域を通してセキュリティを確保するように設計されたグローバル規模の技術インフラストラクチャがあります。このインフラストラクチャによって、サービスのデプロイにおけるセキュリティ、データ ストレージのセキュリティ（とエンドユーザーのプライバシー保護）、サービス間の通信のセキュリティ、お客様とインターネット経由の通信の機密性とセキュリティ、管理者オペレーションの安全性が提供されています。

- 検索、Gmail、フォトなどの消費者向けサービスと、G Suite や Google Cloud Platform などの企業向けサービスの両方からなる Google のインターネット サービスは、このインフラストラクチャを使用して構築されています。

- インフラストラクチャのセキュリティは、進行型の階層構造で設計されています。まず、データセンターの物理的なセキュリティがあり、次にインフラストラクチャの基礎となるハードウェアとソフトウェアのセキュリティがあり、最後にオペレーションのセキュリティをサポートする技術的な制限やプロセスがあります。

- Google では、自社のインフラストラクチャと全社に分散した何百人ものセキュリティとプライバシー専門のエンジニア（中には業界の権威として認められている人もいます）に多大な投資を行っています。

はじめに

このドキュメントでは、Google の技術インフラストラクチャのセキュリティ設計についての概要を説明します。グローバルな規模を持つこのインフラストラクチャは、Google の情報処理ライフサイクル全域を通してセキュリティを確保するために設計されています。このインフラストラクチャによって、サービスのデプロイにおけるセキュリティ、データ ストレージのセキュリティ（とエンドユーザーのプライバシー保護）、サービス間の通信のセキュリティ、お客様とインターネット経由の通信の機密性とセキュリティ、管理者オペレーションの安全性が提供されています。

検索、Gmail、フォトなどの消費者向けサービスと、G Suite や Google Cloud Platform などの企業向けサービスの両方からなる Google のインターネット サービスは、このインフラストラクチャを使用して構築されています。

このインフラストラクチャのセキュリティについて、進行型の階層構造にそって説明していきます。まず、データセンターの物理的なセキュリティから始まって、インフラストラクチャの基礎となるハードウェアとソフトウェアのセキュリティに続き、最後に、オペレーションのセキュリティをサポートする技術的な制限やプロセスについて説明します。

Google インフラストラクチャ セキュリティ レイヤ

図 1.
Google インフラストラクチャ セキュリティ レイヤ:
一番下のハードウェア インフラストラクチャから一番上のオペレーションのセキュリティまでのさまざまなセキュリティのレイヤ。このドキュメントでは、それぞれのレイヤについて詳しく説明します。

下位インフラストラクチャの保護

このセクションでは、インフラストラクチャの一番下のレイヤをどのように保護しているかについて説明します。このレイヤには、物理施設から、データセンター内の専用ハードウェア、すべてのマシン上で動作している下位ソフトウェア スタックまでが含まれます。

物理施設のセキュリティ

Google では、複数の物理的セキュリティ保護レイヤからなるデータセンターを独自に設計して構築しています。これらのデータセンターへのアクセスは、ごく少数の Google 社員に制限されています。複数の物理セキュリティ レイヤを使用してデータセンターのフロアを保護しており、生体認証、金属検知、カメラ、車両障害物、レーザーを使った侵入検知システムなどの技術が利用されています。加えて、一部のサーバーをサードパーティ データセンターでホストしています。ここでも、データセンター オペレーターが提供するセキュリティ レイヤに加え、Google が管理する物理セキュリティ対策が設置されています。たとえば、これらのデータセンターには、独立した生体識別システム、カメラ、金属検知器を配備しています。

ハードウェアの設計と供給元

Google データセンターは、ローカル ネットワークに接続された数千台のサーバーマシンで構成されています。サーバーボードとネットワーク機器の両方を Google がカスタム設計しています。提携するベンダーは入念に調査し、コンポーネントを慎重に選定したうえで、ベンダーと連携してそれらのコンポーネントが提供するセキュリティ特性を監査および検証しています。また、現在サーバーと周辺機器の両方にデプロイされているハードウェア セキュリティ チップを含むカスタムチップも設計しています。これらのチップにより、正規の Google 端末をハードウェア レベルで確実に特定して認証することができます。

ブートスタックとマシン ID のセキュリティ

Google サーバーマシンでは、正しいソフトウェア スタックを起動するためにさまざまな技術を利用しています。BIOS、ブートローダー、カーネル、基本オペレーティング システム イメージなどの下位コンポーネントに対しては暗号署名を使用しています。これらの署名はブートまたは更新ごとに検証することができます。コンポーネントはすべて Google が管理、構築、強化しています。Google では、新しい世代のハードウェアを使用して継続的なセキュリティ強化に努めています。たとえば、サーバー設計の世代に応じて、ブートチェーンの信頼の根拠を、ロック可能なファームウェア チップ、Google が制作したセキュリティ コードを実行するマイクロコントローラ、上記の Google が設計したセキュリティ チップのいずれかに置くようにしています。

データセンター内の各サーバーマシンには、信頼のハードウェア根拠とマシンが起動時に使用したソフトウェアに関連付けることが可能な固有の ID が割り当てられています。この ID は、マシン上の下位管理サービスとの間でやり取りされる API 呼び出しの認証に使用されます。

Google では、サーバーが最新バージョンのソフトウェア スタック（セキュリティ パッチを含む）を実行することを保証し、ハードウェアとソフトウェアの問題を検出して診

Google データセンターは、ローカル ネットワークに接続された数千台のサーバーマシンで構成されています。サーバーボードとネットワーク機器の両方を Google がカスタム設計しています。

サービス間通信用のアプリケーション レイヤでは暗号認証および承認を使用しています。これにより、管理者とサービスが自然に認識できるような抽象化レベルと粒度で、強力なアクセス制御が提供されます。

断し、必要に応じてサービスからマシンを除外する自動システムを構築しました。

サービスのデプロイのセキュリティ

ここでは、基本のハードウェアとソフトウェアから、インフラストラクチャへのサービスのデプロイのセキュリティを確保するところまでを説明します。ここで言う「サービス」とは、デベロッパーが制作し、Gmail SMTP サーバー、BigTable ストレージ サーバー、YouTube 動画トランスコーダ、カスタム アプリケーションを実行する App Engine サンドボックスなどのインフラストラクチャ上で実行するアプリケーション バイナリのことです。必要な規模のワークロードを処理するために何千台ものマシンが同じサービスのコピーを実行する場合もあります。インフラストラクチャ上で動作するサービスは、Borg という名前のクラスタ オーケストレーション サービスによって管理されます。

後述するように、インフラストラクチャはその上で動作しているサービス間の信頼を前提としません。つまり、インフラストラクチャは、基本的に、マルチテナントとして設計されています。

サービス ID、整合性、分離

サービス間通信用のアプリケーション レイヤでは暗号認証および承認を使用しています。これにより、管理者とサービスが自然に認識できるような抽象化レベルと粒度で強力なアクセス制御が提供されます。

主要なセキュリティ メカニズムとして、内部ネットワークのセグメント化またはファイアウォール化に依存していない代わりに、追加のセキュリティ レイヤとして、IP スプーフィングを回避するための入口フィルタリングと出口フィルタリングをネットワーク内のさまざまなポイントで使用しています。このアプローチは、ネットワークのパフォーマンスと可用性の最大化にも役立ちます。

インフラストラクチャ上で動作する各サービスには、サービス アカウント ID が関連付けられます。サービスには、他のサービスとリモート プロシージャ コール（RPC）を送受信するときにその ID を証明するための暗号認証情報が付与されます。この ID は、クライアントが意図した正しいサーバーと通信していることを保証するためと、サーバーがメソッドとデータへのアクセスを特定のクライアントに制限するために使用されます。

Google のソースコードは中央レポジトリに保存されています。そこでは、最新バージョンのサービスと古いバージョンのサービスの両方を監査できます。加えて、インフラストラクチャは、サービスのバイナリをレビュー、チェックイン、テストが完了している特定のソースコードからビルドするように設定できます。このようなコードレビューには制作者以外に少なくとも 1 人のエンジニアの検査と承認が必要であり、さらに、どのシステムにおいてもコードを変更するにはそのシステムの所有者の承認が義務づけられています。これらの要件により、インサイダーや敵対者がソースコードに悪意のある変更を加えないよう制限され、サービスからそのソースまでの監査証跡も提供されます。

サービスを同じマシン上で動作している他のサービスから保護するためのさまざまな分離テクニックとサンドボックス化テクニックを使用しています。これらのテクニックには、正規の Linux ユーザーの分離、言語とカーネルベースのサンドボックス、ハードウェア仮想化が含まれます。通常は、よりリスクの高いワークロードに対してより多くのレイヤの分離を使用します。たとえば、ユーザーが指定したデータに対して複雑なファイル形式コンバータを実行する場合や、Google App Engine や Google Compute Engine などのプロダクトに対してユーザーが指定したコードを実行する場合です。追加のセキュリティ境界として、クラスタ オーケストレーション サービスや一部の鍵管理サービスなどの非常に機密性の高いサービスを専用のマシン上で排他的に実行できます。

サービス間アクセスの管理

サービスの所有者は、インフラストラクチャが提供するアクセス管理機能を使用して、通信可能な他のサービスを正確に指定することができます。たとえば、あるサービスが他のサービスの特定のホワイトリストに一部の API のみを提供する場合です。このサービスは、許可されたサービス アカウント ID のホワイトリストを使用して設定することができ、そのアクセス制限はその後にインフラストラクチャによって自動的に適用されます。

サービスの所有者は、インフラストラクチャが提供するアクセス管理機能を使用して、通信可能な他のサービスを正確に指定することができます。

サービスにアクセスする Google のエンジニアにも個別の ID が発行されるため、サービスにはそのアクセスの許可と拒否も同様に設定できます。この種の ID のすべて（マシン、サービス、社員）が、インフラストラクチャが維持するグローバルな名前空間内に存在します。後述するように、エンドユーザー ID は別に処理されます。

インフラストラクチャは、承認チェーン、ロギング、通知を含む、これらの内部 ID のための豊富な ID 管理ワークフロー システムを提供します。たとえば、これらの ID は、あるエンジニアが他のエンジニア（グループの管理者でもある）の承認が必要なグループに対する変更を申し込むことができる二者管理を可能にするシステムを介してアクセス制御グループに割り当てることができます。このシステムを使用すれば、セキュアなアクセス管理プロセスを、インフラストラクチャ上で動作する何千ものサービスに拡張することができます。

自動 API レベル アクセス制御メカニズムに加えて、インフラストラクチャは、中央の ACL とグループのデータベースから読み取る機能もサービスに与えるため、必要に応じて、カスタムのきめ細かいアクセス制御を実装することができます。

サービス間通信の暗号化

前のセクションで説明した RPC 認証および承認機能に加えて、インフラストラクチャは、ネットワーク上の RPC データの暗号プライバシーと整合性も提供します。これらのセキュリティ機能を HTTP などの他のアプリケーション レイヤ プロトコルでも利用できるように、これらをインフラストラクチャの RPC メカニズム内にカプセル化しています。つまり、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。ネットワークが不安定になったり、ネットワーク端末が侵害されたりしても、暗号化されたサービス間通信をセキュアなまま維持することができます。

サービスは、インフラストラクチャ RPC ごとに必要な暗号保護のレベルを設定することができます（たとえば、データセンター内部の低値データに対しては整合性レベルの保護を設定するだけです）。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ら保護するために、インフラストラクチャはデータセンター間を WAN 経由で移動するすべてのインフラストラクチャ RPC トラフィックを自動的に暗号化します。サービスから明示的に設定する必要はありません。Google では、このデフォルトの暗号化をデータセンター内のすべてのインフラストラクチャ RPC トラフィックに拡張可能にするハードウェア暗号アクセラレータのデプロイを開始しました。

エンドユーザー データのアクセス管理

標準的な Google サービスは、エンドユーザーのために何かをするように作られています。たとえば、エンドユーザーは、Gmail 上に自分のメールを保存しておくことができます。Gmail などのアプリケーションとエンドユーザーの相互作用は、インフラストラクチャ内の他のサービスにも及びます。そのため、たとえば、Gmail サービスは、エンドユーザーのアドレス帳にアクセスするために連絡先サービスから提供される API を呼び出すことができます。

Gmail サービス（または連絡先サービスが許可する他の特定のサービス）からの RPC リクエストのみが許可されるように連絡先サービスを設定できることは前のセクションで確認しました。

ただし、これは、広範囲に及ぶ権限の 1 つにすぎません。この権限の範囲内で、Gmail サービスはいつでも任意のユーザーの連絡先を要求することができます。

Gmail サービスは、特定のエンドユーザーの代わりに連絡先サービスに RPC リクエストを発行するため、インフラストラクチャは Gmail サービスに RPC の一部として「エンドユーザー権限チケット」を提示する機能を提供します。このチケットは、Gmail 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を処理していることを証明するものです。これにより、連絡先サービスは、チケット内で指定されたエンドユーザーに関するデータのみを返す安全保護対策を実装することができます。

インフラストラクチャは、これらの「エンドユーザー権限チケット」を発行する中央のユーザー アイデンティティ サービスを提供します。エンドユーザーのログインは、中央のアイデンティティ サービスで検証されます。その後で、このサービスが Cookie や OAuth トークンなどのユーザー認証情報をユーザーのクライアント端末に発行します。それ以降のクライアント端末から Google へのすべてのリクエストは、そのユーザー認証情報を提示する必要があります。

サービスがエンドユーザー認証情報を受け取ると、その認証情報を検証のために中央のアイデンティティ サービスに渡します。エンドユーザー認証情報が正しく検証されると、中央のアイデンティティ サービスがリクエストに関連した RPC に使用可能な有効期限の短い「エンドユーザー権限チケット」を返します。この例では、「エンドユーザー権限チケット」を取得するサービスが Gmail サービスであり、そこからチケットが連絡先サービスに渡されます。それ以降は、すべてのカスケード呼び出しに対して、呼び出し先への呼び出しサービスが RPC 呼び出しの一部として「エンドユーザー権限チケット」を継承できます。

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に、データセンター間を WAN 経由で移動する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るようになっています。

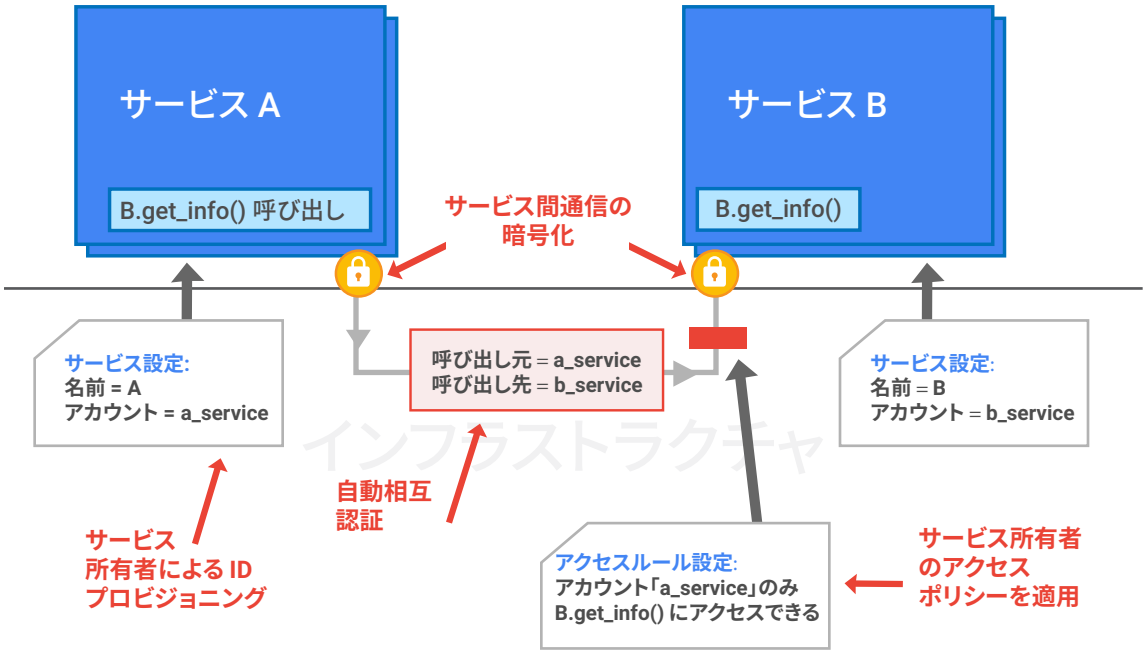

図 2.
サービス ID とアクセス管理: インフラストラクチャは、サービス ID、自動相互認証、暗号化されたサービス間通信、サービス所有者によって定義されたアクセス ポリシーの適用を可能にします。

データ ストレージのセキュリティ

ここまで、サービスのデプロイにおけるセキュリティについて説明してきました。ここからは、インフラストラクチャのセキュアなデータ ストレージの実装についての説明に移ります。

保存時の暗号化

Google のインフラストラクチャは、BigTable や Spanner などのさまざまなストレージ サービスと中央の鍵管理サービスを提供します。Google 上のほとんどのアプリケーションは、これらのストレージ サービスを介して間接的に物理ストレージにアクセスします。ストレージ サービスは、中央の鍵管理サービスから取得した鍵を使用して、物理ストレージに書き込まれる前のデータを暗号化するように設定できます。この鍵管理サービスは、自動鍵ローテーションをサポートし、豊富な監査ログを提供し、前述のエンドユーザー権限チケットと統合して、鍵を特定のエンドユーザーにリンクします。

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。つまり、インフラストラクチャは、追加の保護レイヤも実装しています。Google では、ハードドライブと SSD 内のハードウェア暗号化サポートを有効にし、すべてのドライブをそのライフサイクルを通して細かく追跡しています。廃棄予定の暗号化されたストレージ デバイスは物理的に管理下から外される前に、2 回の独立した検証を含む多段階プロセスを使用してクリーニングされます。このワイプ手順を通過していないデバイスは、オンプレミスで物理的に破壊（細断など）されます。

データの削除

Google におけるデータの削除は、ほとんどの場合、データを完全に削除するのではなく、特定のデータを「削除予定」としてマークすることから始まります。これにより、お客様が実施したのか、内部的なバグや処理エラーが原因なのかに関係なく、意図しない削除からの回復が可能になります。「削除予定」としてマークされたデータは、サービス固有のポリシーに従って削除されます。

エンドユーザーが自分のアカウント全体を削除した場合は、インフラストラクチャがアカウントが削除されたことをエンドユーザー データを処理するサービスに通知します。その後で、サービスは、削除されたエンドユーザー アカウントに関連付けられたデータを削除するようにスケジュールすることができます。この機能を使用すれば、サービスのデベロッパーは、エンドユーザー制御を簡単に実装することができます。

Google Front End では、すべての TLS 接続が正しい証明書を使用し、完全な前方秘匿性のサポートなどのベスト プラクティスに従って終端されることが保証されています。

インターネット通信のセキュリティ

ここまで、インフラストラクチャ上でサービスを保護する方法について説明してきました。このセクションでは、インターネットとこれらのサービス間の通信を保護する方法に関する説明に移ります。

前述したように、インフラストラクチャは、LAN や WAN を介して相互接続された物理マシンの大規模なセットで構成されており、サービス間通信のセキュリティは、ネットワークのセキュリティに依存していません。ただし、インフラストラクチャをインターネットから非公開の IP 空間に分離することにより、マシンのサブセットを直接外部のインターネット トラフィックに公開するだけで、サービス拒否（DoS）攻撃に対する防御などの追加の保護をより簡単に実装できます。

Google Front End サービス

サービスをインターネット上で利用可能にするには、それを Google Front End（GFE）と呼ばれるインフラストラクチャ サービスに登録する必要があります。GFE は、すべての TLS 接続が、正しい証明書を使用し、完全な前方秘匿性のサポートなどのベスト プラクティスに従って終端されることを保証します。加えて、GFE は、サービス拒否攻撃に対する防御（詳細は後述）を適用します。その後で、GFE が前述の RPC セキュリティ プロトコルを使用してサービスにリクエストを転送します。

実際には、外部に公開する内部サービスでは、GFE がスマートなリバース プロキシ フロントエンドとして使用されます。このフロントエンドは、パブリック DNS 名のパブリック IP ホスティング、サービス拒否（DoS）攻撃に対する防御、TLS 終端を提供します。GFE は、他のサービスと同様のインフラストラクチャ上で動作するため、着信リクエストの量に合わせてスケーリングできます。

サービス拒否（DoS）攻撃に対する防御

インフラストラクチャの規模が大きいために、Google では多くの DoS 攻撃を単純に吸収することができます。つまり、GFE の背後で動作しているサービスに対する DoS の影響のリスクを大幅に低減するマルチティアでマルチレイヤの DoS 防御が施されています。

インフラストラクチャの規模が大きいために、Google では多くの DoS 攻撃を単純に吸収することができます。つまり、GFE の背後で動作しているサービスに対する DoS 攻撃のリスクを大幅に低減する、マルチティアでマルチレイヤの DoS 防御が施されています。

Google のバックボーンは、データセンターのいずれかに外部接続を配信した後で、ハードウェアとソフトウェアの負荷分散の複数のレイヤを通過します。これらのロードバランサは、インフラストラクチャ上で動作している中央の DoS サービスへの受信トラフィックに関する情報を報告します。中央の DoS サービスは、DoS 攻撃が行われていることを検出すると、攻撃に関連付けられたトラフィックを破棄または抑制するようにロードバランサを設定することができます。

次のレイヤでは、GFE インスタンスが受信中のリクエストに関する情報も中央の DoS サービスに報告します。この情報には、ロードバランサが把握していないアプリケーション レイヤの情報が含まれます。その後で、中央の DoS サービスが、攻撃トラフィックを破棄または抑制するように GFE インスタンスを設定することもできます。

ユーザー認証

DoS に対する防御の次の防御レイヤは、中央のアイデンティティ サービスからもたらされます。このサービスは、通常、Google のログインページとしてエンドユーザーに提示されます。単純なユーザー名とパスワードを要求するのではなく、サービスは、ユーザーに対して、過去に同じ端末または同様の場所からログインしたことがあるかどうかなどのリスク要因に基づいて自動的に追加情報を要求します。ユーザーの認証後は、アイデンティティ サービスが、以降の呼び出しに使用可能な Cookie や OAuth トークンなどの認証情報を発行します。

ユーザーは、ログイン時に、OTP やフィッシング耐性のあるセキュリティ キーなどの 2 つ目の要素を採用することもできます。Google にとっても大きなメリットがあることを確認するために、FIDO Alliance で複数の端末ベンダーと協力して Universal 2nd Factor（U2F）オープン スタンダードを策定しました。現在、これらの端末は市場で入手可能であり、他の主要なウェブサービスも U2F のサポートを導入し始めています。

オペレーション セキュリティ

ここまで、インフラストラクチャに組み込まれているセキュリティ設計についてと、RPC 上でのアクセス制御といったセキュア オペレーションの仕組みの一部について説明してきました。

ここからは、インフラストラクチャの実際の運用におけるセキュリティの説明に移ります。Google では、セキュリティの万全なインフラストラクチャ ソフトウェアを作成し、社員のマシンと認証情報を保護し、内部と外部両方の攻撃者からのインフラストラクチャに対する脅威を防ぎます。

安全なソフトウェアの開発

前述した中央のソース管理機能と二者レビュー機能に加えて、デベロッパーが特定のクラスのセキュリティ バグを発生させないようにするためのライブラリも提供しています。たとえば、ウェブアプリの XSS 脆弱性を排除するライブラリとフレームワークが用意されています。また、ファザーなどのセキュリティ バグを自動的に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。

最終チェックとして、リスクが低い機能の迅速な選別から、最もリスクが高い機能の詳細設計および実装レビューまでにおよぶ手動セキュリティ レビューを使用しています。これらのレビューは、ウェブ セキュリティ、暗号化、オペレーティング システム セキュリティの各専門家を交えたチームによって実施されます。また、レビューは、新しいセキュリティ ライブラリ機能につながることもあれば、他の将来のプロダクトに適用可能な新しいファザーにつながることもあります。

加えて、インフラストラクチャやアプリケーションのバグを発見して報告した人に報奨金を出す脆弱性報奨金プログラムを運営しています。これまで、このプログラムで数百万ドルの報奨金が支払われています。

また、Google では、使用しているすべてのオープン ソース ソフトウェアのゼロデイ エクスプロイトなどのセキュリティ上の問題の発見と、それらの問題のアップストリームに全力で取り組んでいます。たとえば、OpenSSL Heartbleed バグは Google で発見されましたし、Linux KVM ハイパーバイザの CVE とセキュリティ バグの修正の最大の提出者でもあります。

Google では、インフラストラクチャやアプリケーションのバグを発見して報告した人に報奨金を出す脆弱性報奨プログラムを実施しています。

社員の端末と認証情報の安全の確保

Google では、社員の端末と認証情報を侵害から守る保護活動と、潜在的な情報漏洩や違法なインサイダー行為を発見するための監視活動に多くの投資を行っています。これは、インフラストラクチャが安全に運用されていることを保証するための投資の重要な部分です。

長年にわたって、巧妙なフィッシングが社員を標的とした手段でした。この脅威から保護するために、フィッシングされる可能性のある OTP 第 2 要素を、社員アカウントに対する U2F 互換セキュリティ キーの必須使用に置き換えました。

社員がインフラストラクチャの運用に使用するクライアント端末の監視に多大な投資を行っています。これらのクライアント端末のオペレーティング システム イメージがセキュリティ パッチを含む最新版であることを保証し、インストール可能なアプリケーションを管理しています。加えて、ユーザーがインストールしたアプリ、ダウンロード、ブラウザの拡張機能、ウェブから閲覧されたコンテンツの法人顧客に対する適合性をスキャンするためのシステムを導入しています。

アクセス権限を付与する主な基準は、社内の LAN 上に存在するかどうかではありません。代わりに、想定されるネットワークや地理的な場所で正しく管理された端末からアクセスしている特定のユーザーにのみ内部アプリケーションを公開できるようにするアプリケーション レベルのアクセス管理コントロールを使用しています（詳細については、BeyondCorp に関する追加情報をご覧ください）。

インサイダー リスクの低減

Google では、インフラストラクチャへの管理アクセス権が付与された社員の活動を強制的に制限し、積極的に監視しているほか、同じタスクを安全で管理された方法で自動的に実行する処理を提供することにより、特定のタスクに対する特権アクセスの必要性を排除する努力を続けています。たとえば、特定のアクションの実施に二

者の承認を必須とする処置や、機密情報を公開することなくデバッグすることが可能な制限付き API の導入などです。

エンドユーザー情報への Google 社員のアクセスは、下位インフラストラクチャ フックを介して記録することができます。Google のセキュリティ チームは、積極的に、アクセス パターンを監視し、異常なイベントを調査しています。

侵入検知

Google では、個々の端末上のホストベースの信号、インフラストラクチャ内の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統合する高度なデータ処理パイプラインを導入しています。これらのパイプライン上に構築されたルールとマシン インテリジェンスから、可能性のあるインシデントの警告が運用セキュリティ エンジニアにもたらされます。Google の調査およびインシデント対応チームは、これらの潜在的なインシデントを年中無休で選別、調査、対応しています。Google では、検出メカニズムと対応メカニズムの有効性を評価して改善するための Red Team 訓練を実施しています。

信号をモニタリングするパイプライン上に構築されたルールとマシン インテリジェンスから、可能性のあるインシデントの警告が運用セキュリティ エンジニアに通知されます。

Google Cloud Platform（GCP）の保護

このセクションでは、Google のパブリック クラウド インフラストラクチャである GCP が、基礎となるインフラストラクチャのセキュリティからメリットを得ている様子を説明します。Google Compute Engine サービスを例として取り上げ、インフラストラクチャ上に構築されたサービス固有のセキュリティ強化について詳しく説明します。

GCE を使用すれば、お客様は Google のインフラストラクチャ上で独自の仮想マシンを実行することができます。GCE 実装は、いくつかの論理コンポーネントで構成されます。注目すべき主なコンポーネントは管理制御プレーンと仮想マシン自体です。

管理制御プレーンは、外部 API サーフェスを公開し、仮想マシンの作成や移行などのタスクをオーケストレートします。このプレーンは、インフラストラクチャ上のさまざまなサービスとして動作するため、セキュアなブートチェーンなどの基本的な整合性機能を自動的に利用します。個々のサービスはそれぞれの内部サービス アカウントの下で実行されるため、すべてのサービスには、制御プレーンの残りの部分にリモート プロシージャ コール（RPC）を発行するときに必要になる権限のみを付与できます。前に述べたように、これらのすべてのサービスのコードが中央の Google ソースコード レポジトリに格納され、このコードと最終的にデプロイされるバイナリとの間の監査証跡が生成されます。

GCE 制御プレーンは、GFE を介してその API を公開するため、サービス拒否（DoS）攻撃の防御や一元管理された SSL/TLS のサポートなどのインフラストラクチャ セキュリティ機能を利用します。Google Cloud Load Balancer サービスは、GFE 上に構築された、さまざまな種類の DoS 攻撃を緩和できるオプションです。お客様はこの

オプションの使用を選択することで、GCE VM 上で動作するアプリケーションに対して同様の保護を手に入れることができます。

Compute Engine 制御プレーン API に対するエンドユーザー認証は、ハイジャック検出などのセキュリティ機能を提供する Google の集中型アイデンティティ サービスを介して実施されます。承認は、中央の Cloud IAM サービスを使用して実施されます。

GFE からその背後にある最初のサービスに流れるものとその他の制御プレーン サービス間を流れるものの両方の制御プレーンのネットワーク トラフィックは、自動的に、インフラストラクチャによって認証され、データセンター間を移動するたびに暗号化されます。加えて、インフラストラクチャは、データセンター内の制御プレーン トラフィックの一部を暗号化するようにも設定されています。

各仮想マシン（VM）は、関連する仮想マシン マネージャ（VMM）サービス インスタンスで動作します。インフラストラクチャは、これらのサービスに 2 つの ID を付与します。1 つの ID は、独自の呼び出し用の VMM サービス インスタンスによって使用され、もう 1 つの ID は、VMM がお客様の VM の代わりに発行する呼び出しに使用されます。これにより、VMM から着信した呼び出しに対する信頼をさらに分割することができます。

GCE 永続ディスクは、中央のインフラストラクチャ鍵管理システムによって保護された鍵を使用して保存中に暗号化されます。これにより、これらの鍵へのアクセスの自動ローテーションと中央監査が可能になります。

Google Compute Engine（GCE）制御プレーンでは、Google Front End（GFE）を介してその API を公開するため、サービス拒否（DoS）攻撃の防御や一元管理された SSL/TLS のサポートなどのインフラストラクチャ セキュリティ機能を利用します。

現在、お客様には、トラフィックを VM 間で送信する、インターネットにプレーンテキストで送信する、トラフィック用に選択した暗号化を実装する、の選択肢があります。Google では、お客様の VM 間トラフィックの WAN トラバーサル ホップ用の自動暗号化の展開を開始しました。前に述べたように、インフラストラクチャ内のすべての制御プレーン WAN トラフィックはすでに暗号化されています。将来的には、データセンター内の VM 間 LAN トラフィックも暗号化するために、前述のハードウェアで加速するネットワーク暗号化を利用する予定です。

VM に提供される分離は、オープンソース KVM スタックを使用したハードウェア仮想化に基づきます。コントロールとハードウェア エミュレーション スタックの一部をカーネル外部の非特権プロセスに移動することにより、KVM の特定の実装をさらに強化しました。また、ファジング、静解析、手動コードレビューなどのテクニックを使用して、KVM のコアを広範囲にテストしました。前に述べたように、KVM にアップストリームされた最近公開された脆弱性の大半が Google からの提出されたものです。

最後に、オペレーション セキュリティ制御は、データへのアクセスがポリシーに従っていることの確認の重要な部分です。Google Cloud Platform の一部として、Compute Engine のお客様のデータの使用法は、顧客データポリシーの GCP 使用法に従っています。つまり、Google が、お客様にサービスを提供するために必要な場合を除き、お客様のデータにアクセスしたり、使用したりすることはありません。

Google では、インフラストラクチャの保護に多額の投資をしており、Google の全域に数百人を数えるセキュリティおよびプライバシー専門のエンジニアを擁しています。中には、業界の権威として認知されている人材もいます。

まとめ

サービスをインターネット規模で安全に構築、デプロイ、運用するために Google インフラストラクチャがどのように設計されているかについて説明しました。この中には、Gmail などの消費者向けサービスと企業向けサービスの両方が含まれています。加えて、Google Cloud の各プロダクトもこの同じインフラストラクチャ上に構築されています。

Google では、インフラストラクチャの保護に多額の投資をしており、セキュリティとプライバシー専門の数百人ものエンジニアが Google 全域に配置されています。業界の権威として認識されているエンジニアも多数います。

これまで見てきたように、インフラストラクチャのセキュリティは、まずは物理コンポーネントとデータセンター、そしてハードウェアの供給元、次にブートのセキュリティ、サービス間通信のセキュリティ、保存データのセキュリティ、インターネットからサービスへの保護アクセス、そして最後に、オペレーションのセキュリティのために導入されている技術と人材によるプロセスというように、進行型の階層構造で設計されています。

追加情報

特定の分野の詳細については、以下の資料をご覧ください。

1. データセンターの物理的セキュリティ
   https://goo.gl/WYlKGG

2. クラスタの管理とオーケストレーションの設計
   http://research.google.com/pubs/pub43438.html

3. ストレージ暗号化機能と顧客対応 GCP 暗号化機能
   https://cloud.google.com/security/encryption-at-rest/

4. BigTable ストレージ サービス
   http://research.google.com/archive/bigtable.html

5. Spanner ストレージ サービス
   http://research.google.com/archive/spanner.html

6. ネットワーク負荷分散のアーキテクチャ
   http://research.google.com/pubs/pub44824.html

7. 企業セキュリティに対する BeyondCorp のアプローチ
   http://research.google.com/pubs/pub43231.html

8. セキュリティ キーと Universal 2nd Factor（U2F）標準を使用したフィッシング対策
   http://research.google.com/pubs/pub45409.html

9. Google 脆弱性報奨金プログラムの詳細
   https://bughunter.withgoogle.com/

10. GCP 上での HTTP とその他の負荷分散オファリングの詳細
    https://cloud.google.com/compute/docs/load-balancing/

11. GCP 上での DoS 防御のベスト プラクティスの詳細
    https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf

12. Google Cloud Platform の顧客データポリシーの使用
    https://cloud.google.com/terms/

13. G Suite（Gmail、ドライブなど）でのアプリケーション セキュリティとコンプライアンスの詳細
    https://goo.gl/3J20R2