セキュリティに関するホワイトペーパー: Google Apps コミュニケーション/コラボレーション サービス

Google

セキュリティに関するホワイトペーパー Google Apps コミュニケーション/コラボレーション サービス

目次

Google Apps の詳細については、次の URL をご覧ください。
www.google.com/a

はじめに

ここ数年、サードパーティがホストするサービスが増加しており、オンライン サービスのセキュリティに対する企業の関心が高まっています。さまざまな「クラウド コンピューティング」の概念と定義が出現したことで、データの所有権や保護だけでなく、クラウド コンピューティング テクノロジーの各種ベンダーがサービスを構築、実装する方法も注目されるようになり、セキュリティの専門家、エンドユーザー、企業の誰もがクラウド コンピューティング モデルのセキュリティの意味合いについて考えるようになっています。

Gmail、Google カレンダー、Google ドキュメントなどのウェブ アプリケーションで構成されている Google Apps では、使いやすいおなじみのサービスをビジネス向けに提供しています。コンピューティング環境の冗長性 とリソースの動的な割り当てを特徴とするこのサービスにより、ユーザーは インターネット対応デバイスからいつでもどこでも自分のデータにアクセスできます。「クラウド」と呼ばれているこのコンピューティング環境では、ユーザーが CPU、メモリ、ストレージ リソースを共有して利用できるようになると同時に、セキュリティの面での恩恵ももたらします。

Google では、Google 検索などの中核となるサービスと同様に、自社の業務をクラウドで推進することにより、信頼できるクラウド サービスの提供を行っています。クラウド内で、データを分離し処理するというセキュリティ制御手法は、Googleの中核となるテクノロジーと共に初期段階から開発されました。データの細分化、サーバー割り当て、データ保存、処理など、セキュリティは、各クラウド コンピューティング構成要素の重要なコンポーネントとなっています。

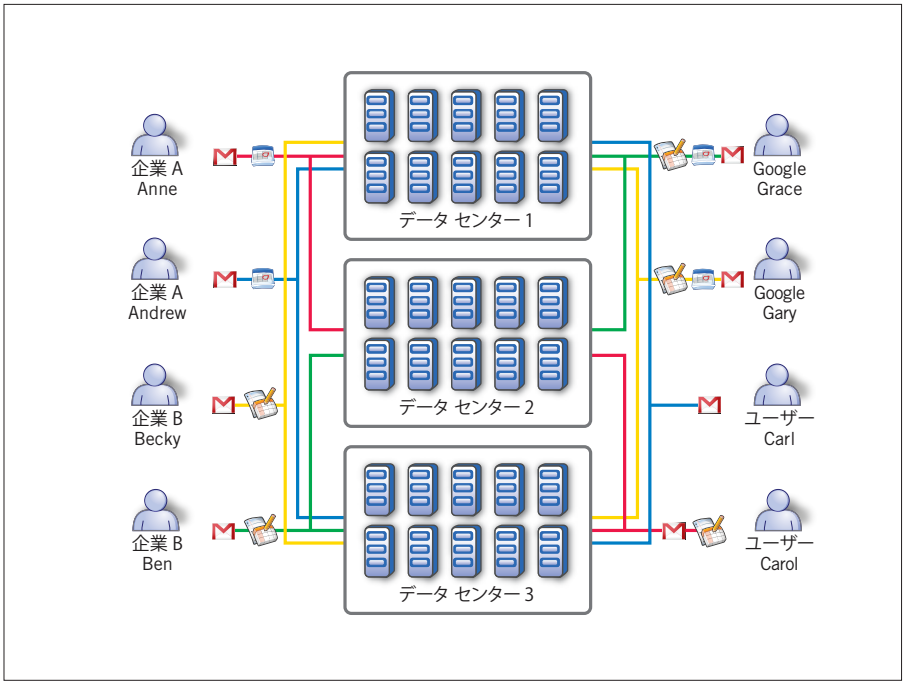

図 1: Google のマルチテナント分散環境

このホワイトペーパーでは、Google がどのようにして Google Apps サービスを提供するために、セキュリティが確保された安全なプラットフォームを構築しているのかについて説明します。たとえば、情報のセキュリティ、物理的なセキュリティ、運用上のセキュリティについて取り上げます。また、セキュリティが Google のクラウド コンピューティング システムにとって不可欠な構成要素であり、Google の設計、開発プロセスの重要な要素であることについても説明します。ここに記載されたポリシーは、このドキュメントが作成された時点の情報です。Google Apps には常に新しい機能やサービスが導入されるため、このドキュメントで説明している一部の機能については今後変更される可能性があります。

概要

Google のセキュリティについての考え方は、データ保存、アクセス、転送といった複数のレベルにおいてセキュリティを管理する多層化されたセキュリティ戦略に基づいています。この戦略は、次の 10 個の要素から成り立っています。

- Google のセキュリティ ポリシー
- 組織のセキュリティ
- 資産の分類と管理
- 個人のセキュリティ
- 物理的および環境的セキュリティ
- 運用上のセキュリティ
- アクセス制御
- システムの開発およびメンテナンス
- 障害復旧と事業継続
- 法令順守

Google のセキュリティ ポリシー

Google では自社のコンピュータ システムに保存されたすべての情報に対するセキュリティ確保を最優先としています。これについては、Google のウェブサイト（**http://investor.google.com/corporate/code-of-conduct.html**）に記載されている Google の行動指針（英語）をご覧ください。また、セキュリティについての Google の理念については、**http://www.google.com/intl/ja/corporate/security.html** をご覧ください。

Google のセキュリティは、物理面、アカウント、データ、企業サービス、ネットワークおよびコンピュータ システム、アプリケーション サービス、システム サービス、変更管理、インシデント レスポンス、データ センター セキュリティを対象とした、一連のセキュリティ ポリシーを基盤としています。これらのポリシーは、その有効性と正確性が継続的に確保されるように、定期的に見直されます。

Google のすべての従業員が従う必要があるセキュリティ ポリシーの他に、セキュリティに関するガイダンスもあります。このドキュメントでは、インターネットの安全な使用、遠隔地からの安全な操作、機密データの分類と取り扱いなど、情報の保護ポリシーの最も重要な側面について説明されています。また、特に関心の高い分野では補足ガイダンスが常に用意されます。このような分野には、携帯端末やピアツーピア ソフトウェアの安全な使用といった新しい分野のテクノロジーが当てはまります。これらの補足ガイダンスは、簡潔を旨とする Google のイデオロギーに基づいて記述されています。書面化されたポリシーが有効なのは、情報が理解され実践される場合のみだからです。

組織のセキュリティ

情報の保護

Google では、ソフトウェア エンジニアリング組織とオペレーション組織に情報セキュリティ チームを配置しています。このチームは、情報、アプリケーション、およびネットワークのセキュリティに精通した専門家を常勤スタッフとして迎えて編成されています。このチームは、防御システムの維持やセキュリティ レビュー プロセスの企画、独自にカスタマイズされたセキュリティ インフラの構築を担当しています。また、Google のセキュリティ ポリシーやセキュリティ基準を企画、文書化、実施するうえでも重要な役割を果たしています。

具体的には、情報セキュリティ スタッフは次の活動を行っています。

- 厳密で多面的なプロセスにより、Google 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確認します
- セキュリティ設計および実装レベルのレビューを実施します
- 所定のプロジェクトに関するセキュリティ上のリスクや、セキュリティ上の問題に対する解決策に関するコンサルティングを継続的に実施します

- Google ネットワーク上の不審なアクティビティを監視し、正式なインシデント レスポンスのプロセスに従って、情報の保護に対する脅威を迅速に認識して分析し、対応策を講じます
- セキュリティの評価や内部監査を定期的に実施することで、既存のポリシーを順守していることを確認します
- Google のセキュリティ ポリシー順守に関する従業員向けのトレーニングを立案して提供します。特にデータのセキュリティと セキュリティ確保のためのプログラミングの分野に重点を置いています。
- 外部のセキュリティの専門家と連携し、インフラとアプリケーションをセキュリティの面から定期的に評価します
- 脆弱性管理プログラムを実行し、ネットワーク上の問題のある領域を確認したり、修正が必要な既知の問題が決められたタイミングで修正されていることを確認したりします

情報セキュリティ チームは、Google 外部のセキュリティ コミュニティと協力して、次のような公開活動を行っています。

- 最新セキュリティの動向と問題に対応できるように、セキュリティ確保のための新しいプログラミング手法を公開します
- ソフトウェア ベンダーや保守業者と協力し、サードパーティのオープン ソース ソフトウェアやクローズド ソース ソフトウェアの脆弱性を特定し、修正します
- 世界的なプライバシー基準を策定します
- 情報セキュリティの問題に関する一般向けの教育資料を提供します（ブラウザ セキュリティ（**http://code.google.com/p/browsersec/wiki/Main**）（英語）など）
- オープン ソース プロジェクトへ参加したり、プロジェクトを組織したりします（完全自動化されたアクティブなウェブ アプリケーション セキュリティ検査ツールである Skipfish（**http://code.google.com/p/skipfish**）など）
- 主要な大学向けにトレーニング カリキュラムを作成します
- 学術的な会議を開催したり、また参加したりします

Google 従業員によるセキュリティやプライバシー関連の出版物のリストについては、**http://research.google.com/pubs/SecurityCryptographyandPrivacy.html**（英語）をご覧ください。

グローバル内部監査とグローバル コンプライアンス
Google には、常勤スタッフで編成された情報セキュリティ チームのほかに、世界的な法令順守に取り組む部門が複数あります。その中のグローバル コンプライアンス部門は法律や法令の順守を担当しています。また、グローバル内部監査部門は、SOX や Payment Card Industry（PCI）標準など、前述のコンプライアンス要件に従っているかどうかを調査、監査します。

物理的セキュリティ
Google には、Google のオフィスやデータ センター施設の物理的セキュリティを担当するグローバルなセキュリティ チームがあり、米国を本拠に活動しています。Google のセキュリティ責任者は高いスキルを有しており、ハイレベルなセキュリティ インフラを含む類似の環境を保護するためのトレーニングを受けています。

資産の分類と管理

情報へのアクセス
Google は、顧客情報のセキュリティを確保するために、広範囲に及ぶ情報管理と運用手法を備えています。

Google アプリケーションは、マルチテナント分散環境で実行されます。つまり、各顧客のデータは1 台または特定の複数コンピュータに保存されるのではなく、Google のすべての顧客の Google Apps データ（顧客データ、ビジネス データ、Google 自身のデータ）は共有インフラストラクチャ内に分散されます。このインフラストラクチャは、Google の数多くの同種のコンピュータで構成され、Google の複数データ センターにまたがって配置されています。

Google Apps では、多数のコンピュータにわたって大量のデータを保存できるように設計された分散ファイル システムが採用されています。そして、ファイル システム上に構築された大きな分散データベースに構造化されたデータが保存されます。データは分割されて複数のシステムにまたがって複製されるため、1 つのシステムがシステム全体の停止を引き起こしてしまうこと（単一障害点, Single Point of Failure)はありません。分割されたデータにはランダムにファイル名が付けられます。

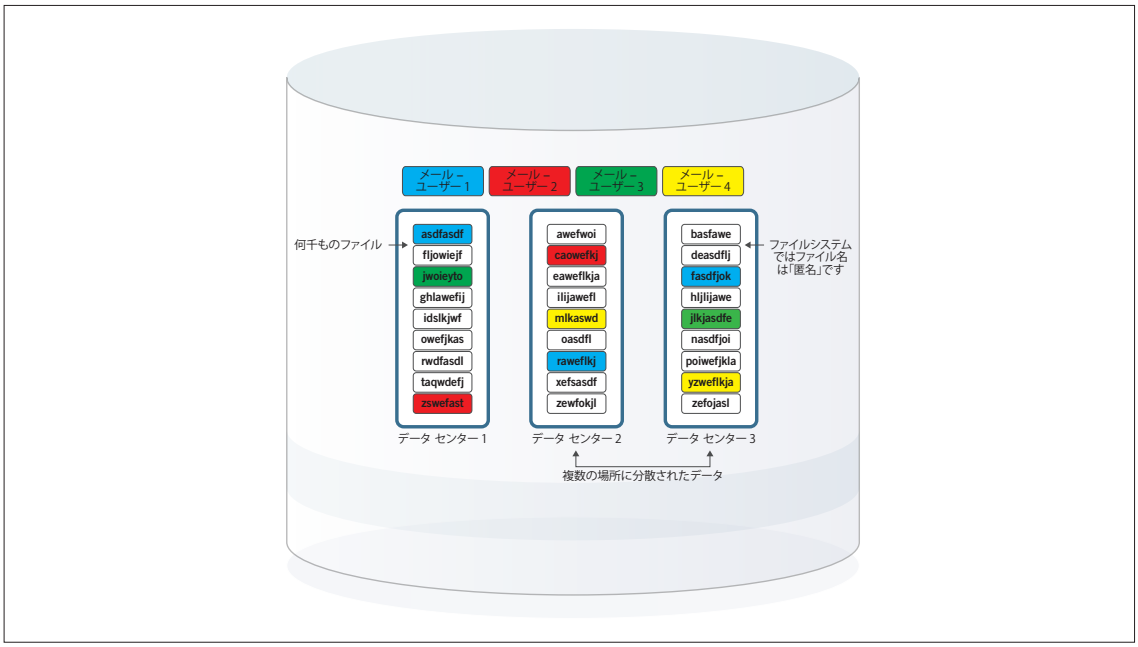

図 2: Google ファイル システム (GFS) アーキテクチャ

また、クリア テキストで保存されることはないので、人が解読することはできません。詳細については、http://labs.google.com/papers/gfs.html (英語) で抜粋をダウンロードしてください。

Google アプリケーションやストレージ スタックのレイヤでは、他のコンポーネントからのリクエストを認証/許可する必要があります。サービス間の認証はセキュリティ プロトコルに基づいており、このセキュリティ プロトコルは アプリケーション サービス間の認証チャネルを仲介する Google のシステムで実現されています。また、認証仲介時におけるインスタンス間の信頼性は、Google 内部の認証機関がGoogle の実運用ホストに対して発行した x509 証明書により確保されます。

たとえば、Gmail ウェブ フロントエンド サービスは、Gmail バックエンド サービスに対してリモート プロシージャ コールを行い、特定のユーザーの受信トレイのメッセージをリクエストします。リクエストを行ったサービスが、Gmail バックエンドへのアクセスが許可されているサービス ID で実行されている場合にのみ、Gmail バックエンドはそのリクエストを認証して処理します。次に、Gmail バックエンドは、Google 分散ファイル システムのファイルにアクセスするために認証を行います。そして、認証に成功した場合にのみ、ファイル アクセス制御リスト (ACL) に従ってアクセスが許可されます。

運用アプリケーションの管理エンジニアによる運用環境へのアクセスも、同じように制御されます。運用サービスへのエンジニアのアクセスの定義および制御には、グループとロール (役割) の一元管理システムが使用されます。その際、エンジニアに対して発行された個人の x509 証明書でエンジニアを認証する、上述のセキュリティ プロトコルの拡張機能が使用されます。

デバッグやメンテナンスを目的とした運用環境への管理アクセスは、ポリシーに従い、SSH (Secure Shell) 公開キー認証接続に基づいて行う必要があります。いずれの場合も、運用サービスやアカウントへのアクセスを許可するグループ メンバーシップが必要に応じて確保されます。

上述のセキュリティ制御は、一貫性のあるGoogle の運用プラットフォームを基盤としています。また、このプラットフォームは次の要素に基づいています。

- Google のデータ センター環境の物理的なセキュリティ確保
- Google の運用オペレーティング システム環境の完全性
- 運用ホストへのシステム管理者権限レベル (ルート) のアクセスは、必要に応じた制限付きアクセス。かつ、アクセスが監視されている従業員の特別なグループのみに付与

Google のこれらのセキュリティの管理の詳細については、このドキュメントの以降のセクションをご覧ください。

削除されたデータ

Google Apps ユーザーまたは Google Apps 管理者がメッセージ、アカウント、ユーザー、ドメインを削除し、これらのアイテムの削除を確認すると (たとえば、ゴミ箱を空にすると)、そのデータは削除さ

れ、ユーザーの Google Apps のインターフェースからアクセスできなくなります。

その後、そのデータは Google のアクティブ サーバーと複製サーバーから削除されます。そして、Google のアクティブ サーバーと複製サーバー上のそのデータへのポインタが削除されます。逆参照されているデータは、他の顧客データによって徐々に上書きされます。

メディアの廃棄
Google のシステムで使用されなくなったディスクに顧客情報が保存されている場合は、Google の施設外に運び出される前にデータ破壊処理が行われます。まず、ポリシーに従い、適切な権限を持つ従業員によって論理的にディスク内データが消去されます。このデータの消去プロセスでは、ゼロ（0x00）データをディスク全域に書き込み、その後、ディスク全域の読み取りを行いディスクが空であることを確認します。

そして、適切な権限を持つ別の従業員が 2 回目の検査を行い、ディスクが完全に消去されていることを確認します。この消去結果は、ディスクのシリアル番号によってログに記録され、追跡することができます。

最後に、消去されたディスクは再利用および再配布用に在庫に追加されます。ハードウェア障害が原因でディスクを消去できない場合、廃棄できるようになるまで安全に保管する必要があります。各施設では、ディスク消去ポリシーの順守に関して毎週監査が行われています。

個人のセキュリティ
Google の従業員は、守秘義務、ビジネス倫理、適切な使用、職業上の基準に関する会社のガイドラインに従って行動する必要があります。

Google では、採用時に個人の学歴や職歴を確認するほか、内部/外部による身元確認を行います。また、地域労働法または法的規制によって認められる範囲内で、犯罪経歴のチェック、信用調査、セキュリティ チェックを行うこともあります。身元確認の内容は、応募先のポジションによって異なります。

Google では、すべての従業員が採用時に秘密保持契約を締結する必要があります。また、Google の従業員ハンドブックを受領したことを確認し、そのポリシーに従うことに同意する必要があります。このハンドブックと新入社員向けオリエンテーションでは、特に顧客情報とデータの機密性とプライバシーについて重点的に説明されます。

従業員には、新入社員オリエンテーションの一環としてセキュリティ トレーニングが行われます。また、Google の各従業員は会社の行動指針を読んで理解し、それに関するトレーニングを受ける必要があります。この行動指針では、Google がすべての従業員に期待すること、すなわち法律を順守し、倫理的かつ誠実に、相互に尊重し合いながら、会社のユーザー、パートナー、そして競合企業にも敬意を払いつつビジネスを遂行することについて概説しています。Google の行動指針については、**http://investor.google.com/corporate/code-of-conduct.html**（英語）をご覧ください。

従業員の職種によっては、追加のセキュリティ トレーニングを受講したり、別のポリシーが適用されたりする場合があります。顧客データを取り扱う Google の従業員は、これらのポリシーに従って必要な要件を満たすことが求められます。顧客データに関連するトレーニングでは、データの適切な使用とビジネス プロセス、およびデータを不正使用した場合の影響について概説します。

Google のすべての従業員は、セキュリティおよびプライバシーに関する問題を特定の Google セキュリティ スタッフに報告する必要があります。Google には機密報告メカニズムが用意されており、従業員は目撃した倫理違反をすべて匿名で報告できます。

物理的および環境的セキュリティ

セキュリティ制御
各地に分散された Google のデータ センターでは、さまざまな物理的セキュリティ対策が導入されています。これらの施設で導入されているテクノロジーやセキュリティのメカニズムは、立地条件やその地域特有のリスクなど、地域の状況に応じて異なる場合があります。各 Google データ センターで採用されている物理的なセキュリティ制御は、既知のテクノロジーで構成され、一般に受け入れられている業界のベスト プラクティス（独自にカスタマイズされた電子カード アクセス制御システム、警報システム、屋内外の監視カメラ、警備員）に準拠しています。システムやシステム コンポーネントが設置、格納されているエリアへのアクセスは、一般のオフィスやロビーなどの共有スペースから切り離されています。これらのエリアそれぞれに監視カメラと警報システムが設置されており、不審な動きがないか集中監視されています。また、施設では警備員が自転車、電動二輪車、三輪式スクーターを使用して定期的にパトロールを行っています。

Google の施設では、動画解析機能を備えた高解像度カメラなどのシステムを使用して、侵入者を感

知して追跡します。行動記録や監視カメラの映像は後から必要に応じて確認できるように保管されます。必要に応じて、熱探知カメラ、侵入防止用のフェンス、生体認証などのセキュリティ制御が使用されることもあります。

データ センターのすべての施設にアクセスできるのは、許可された Google 従業員、承認されたビジター、およびデータ センターの運営を担当する許可された第三者に限られます。Google が保持するビジター アクセス ポリシーと一連の手順には、ビジターが特定の内部エリアにアクセスする場合、データ センター管理者の事前承認が必要であることを記述しています。また、このビジター ポリシーは、普段データ センターの施設にアクセスすることのできない Google 従業員にも適用されます。Google では、四半期ごとにデータ センターにアクセスできる権限を持つユーザーを監査し、適切な担当者のみが各フロアにアクセスできるようにしています。

このデータ センターへのアクセス制限は、役職ではなく職種に基づいて決定されます。このため、Google の最高幹部といえども Google のデータ センターにアクセスすることはできません。

環境制御
Google のコンピュータ クラスタは障害許容力と冗長性を考慮して設計されています。これにより単一障害点や一般的な設備故障や環境リスクの影響を最小限に抑えることができます。二重の回路、スイッチ、ネットワークなどの必要な装置を採用して冗長性を確保しています。データ センターの施設インフラは、堅牢性と耐障害性を備え、並列して維持できるように設計されています。

電力: Google の 24 時間 365 日の運用をサポートできるように、Google データ センターの電力系統は冗長性を備えています。データ センターのすべての重要なコンポーネントには、容量が等しい主電源と代替電源が用意されています。主電源に障害が発生（計画停電、停電、過電圧、低電圧など）した場合、補助発電装置が作動するまで無停電電源（UPS）により電力が供給されます。ディーゼル エンジン式の補助発電装置は、データ センターを一定期間フル稼働させるのに必要な電力を供給できます。

気候と温度: サーバーやその他のコンピュータ ハードウェアの動作温度を一定に保つには空気冷却が必要です。空気冷却により、過熱を防止し、動作停止のリスクを抑えることができます。コンピュータ ルームの空調装置は、通常の電気系統と緊急用の電気系統の両方から給電されています。

火災探知と消火: 自動火災探知と消火装置は、コンピュータのハードウェアへのダメージを防ぐのに役立ちます。火災探知システムでは、データ センターの天井や高床の下に設置された、熱、煙、および水を感知するセンサーを使用しています。火や煙を感知すると、影響するエリア、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。また、手動で操作する消火器もデータ センター全体に設置されています。データ センターの技術者は、消火器の使用方法を含め、火災防止と初期消火に関する訓練を受けています。

詳細情報
Google のデータ センターの詳細と動画ツアーについては、**http://www.google.com/corporate/green/datacenters/summit.html をご覧ください**。

運用上のセキュリティ

マルウェアの防止
マルウェア（不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェア）は、今日の IT 環境に重大なリスクをもたらします。マルウェアより攻撃を受けることで、アカウントの侵害やデータの盗難が発生し、ネットワークへの侵入が行われる可能性があります。Google は、ネットワークや顧客へのこうした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、根絶に努めます。

この戦略の第 1 段階は感染の防止です。手動および自動化されたスキャン システムを使用して、マルウェアやフィッシングに悪用され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探し出します。このプロセスの詳細については、**http://googlewebmastercentral.blogspot.com/2008/10/malware-we-dont-need-no-stinking.html**（英語）をご覧ください。このスキャン手順で作成されたブラックリストは、さまざまなウェブブラウザや Google ツールバーに組み込まれており、疑わしいウェブサイトや不正使用されている可能性のあるサイトからインターネット ユーザーを保護するのに役立ちます。一般に公開されているこれらのツールは、Google の従業員をも同様に保護する役割を担っています。

次に、Gmail、サーバー、ワークステーション上では、複数のウィルス対策エンジンが使用されています。これは、ウィルス対策においてシグニチャを見落とした可能性のある悪意のあるソフトウェアを見つけるのに役立ちます。サポート スタッフは、Google のネットワークに感染する可能性のある不正なソフトウェアを識別して根絶するためのトレーニングを受けています。異常な事例を発見した場

合は、インシデント レスポンス チームに報告されます。

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、システム上での従業員の操作、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。また、Google 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。これにより不審な挙動、たとえば元従業員のアカウントでの予期せぬアクティビティや顧客データへのアクセスの試みなどを特定できます。

Google セキュリティ エンジニアは、検索アラートを公開データ レポジトリに設定し、会社のシステム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、ウェブ上の掲示板の監視を積極的に行います。 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。

脆弱性の管理
Google では、脆弱性に対して適切なタイミングで確実に対処できるように、常勤スタッフによる専任チームを置いています。Google セキュリティ チームは、商用ツール、自動または手動による侵入操作、品質保証（QA）プロセス、ソフトウェアのセキュリティ レビュー、外部監査など通じて、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。

セキュリティ チームによって修正が必要な脆弱性が明確に特定されると、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、**http://www.google.com/intl/ja/corporate/security.html** をご覧ください。

インシデントの管理
Google には、システムやデータの機密性、整合性、可用性に影響する可能性のあるセキュリティ イベントのインシデント管理プロセスが用意されています。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、文書化の方法が記述されています。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。

主要なスタッフは、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も含まれています。重要なエリア（顧客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 従業員の問い合わせに 24 時間 365 日対応します。情報のセキュリティ インシデントが発生した場合、Google のセキュリティ スタッフ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。顧客に直接影響が及ぶ事例は、最優先として処理されます。個人またはチームが専任で問題の修正にあたり、必要に応じてサービスまたはその分野の専門家に協力を要請します。その問題が解決されるまで、他の業務に優先して対応を行います。

Google のセキュリティ エンジニアは、必要に応じて事後分析を実施し、単一の事例の根本原因、複数の事例にまたがる傾向を特定し、同様のインシデントが繰り返し発生しないように新しい戦略を策定します。

ネットワーク セキュリティ
Google では多重の防御システムにより、ネットワーク境界を外部の攻撃から保護します。会社のネットワークを行き来できるのは、Google のセキュリティ要件を満たす許可されたサービスとプロトコルのみで、許可されていないパケットは自動的に削除されます。

Google のネットワーク セキュリティ戦略は次の要素から構成されています:

- ネットワーク境界のサイズと構成要素の管理。業界標準のファイアウォールと ACL テクノロジーを使用してネットワーク分離を実施
- 変更管理、ピア レビュー、テストの自動化により、ネットワーク ファイアウォールと ACL ルールを組織的に管理
- ネットワーク デバイスへのアクセスを許可された関係者のみに制限
- すべてのトラフィックをカスタム フロントエンドサーバー経由でルーティング。これにより、不正なリクエストを検出して遮断
- 内部集約ポイントを作成し監視を強化
- プログラミング エラーの悪用（クロスサイト スクリプティングなど）が行われているかどうかをログでチェックし、問題が見つかった場合は最優先に設定したアラートを生成

オペレーティング システムのセキュリティ
社内で基礎部分から設計された Google の運用サーバーには、Google アプリケーションの実行に必要なコンポーネント（システムの管理やユーザー トラフィックに必要なサービスなど）のみが含まれるようにカスタマイズおよび簡素化された、Linux の強化版が採用されています。システムは、Google がハードウェアとソフトウェア スタック全体を完全に管理し、安全なアプリケーション環境を提供できるように設計されています。

Google の運用サーバーは、強化された標準のオペレーティング システム（OS）上に構築されており、セキュリティ修正は会社のインフラ全体に展開されます。この統一された環境は、継続的にシステムを監視してバイナリ変更がないかどうかを調べる独自のソフトウェアによって維持されます。標準の Google イメージとは異なる変更が見つかると、システムは自動的に正常な状態に戻されます。この自動化された自己回復メカニズムは、Google が安定性に影響を及ぼす問題を監視および修正し、インシデントに関する通知を受け取り、ネットワークに潜在するセキュリティ侵害を 緩和できるように設計されています。

また、強固な変更管理システムを使用して、すべてのシステムに影響する変更を登録、承認、トラッキングする集中管理メカニズムを導入することにより、許可されていない変更が標準の Google OS に加えられることによるリスクを最小限に抑えることができます。

アクセス制御

認証制御
Google では、従業員ごとに一意のユーザー ID を使用する必要があります。このアカウントを使用して、Google のネットワーク上の従業員のアクティビティ（従業員や顧客のデータへのアクセスなど）を特定します。この一意のアカウントは Google のすべてのシステムで使用されます。従業員には、雇用時に人事部によってユーザー ID が割り当てられます。また、以下で説明するデフォルトの権限セットが付与されます。退職するときは、ポリシーに従い、Google のネットワークへのアカウントのアクセスを人事システム内で無効にする必要があります。

認証でパスワードまたはパスフレーズが採用されている場合は（ワークステーションへのログインなど）、Google の強力なパスワード ポリシー（パスワードの有効期限、パスワードの再利用の制限、パスワードの長さなど）が適用されます。

Google では、証明書とワンタイム パスワード生成ツールなどの二要素認証メカニズムを広く採用しています。

許可制御
アクセス権とアクセス レベルは、従業員の職務権限と職責に基づいています。アクセス権限を定義された職責に結び付ける場合には、最小権限のみの割り当て、および情報を必要とする関係者のみへの割り当てという考え方が採用されています。

Google の従業員には、メール、Google の内部ポータル、人事情報などの会社のリソースにアクセスするための、限られたデフォルトの権限のみが付与されます。追加のアクセス権限が必要な場合は、正式なプロセスに沿ってリクエストします。このプロセスでは、Google のセキュリティ ポリシーに従い、データやシステムのオーナー、マネージャー、またはその他の管理者によるリクエストや承認が必要です。承認状況はワークフロー ツールを使用して管理されます。このツールには、すべての変更の監査記録が保持されます。このワークフロー ツールにより、許可設定の変更と承認プロセスの両方が管理され、承認ポリシーが一貫して適用されるようになります。

従業員の許可設定は、Google Apps サービスのデータやシステムを含む、すべてのリソースへのア

クセスを制御するのに使用されます。

アカウンティング

Google のポリシーでは、すべての Google の運用システムとすべてのデータに対する管理アクセスがログに記録されます。これらのログは、Google セキュリティ スタッフが、必要に応じて確認することができます。

システムの開発およびメンテナンス

Google のポリシーでは、プロジェクトのライフサイクル全体にわたって、Google が使用/提供するアプリケーション、システム、サービスのセキュリティに関する特性と影響を考慮します。

Google の「アプリケーション、システム、サービスのセキュリティ ポリシー」に従って、チームおよび個人は、開発中のアプリケーション、システム、サービスで、特定されたセキュリティ リスクと懸念事項に応じたセキュリティ対策を実装する必要があります。このポリシーでは、セキュリティ関連のガイダンスを提供し、リスク評価を行うためのセキュリティ チームを社内に設置することが定められています。

Google では、ユーザーに提供するソフトウェア サービスが高水準のセキュリティ条件を満たすよう、さまざまな手法を導入しています。このセクションでは、ソフトウェア セキュリティに対する Google の現在のアプローチについて概説します。このセクションの内容は、今後変更される場合があります。

セキュリティ コンサルティングとレビュー

アプリケーションやサービスの設計、開発、展開、運用に関して、Google セキュリティ チームでは主に次にカテゴリのコンサルティング サービスを Google のサービスおよびエンジニアリング チームに提供します。

- セキュリティ設計レビュー — プロジェクトのセキュリティ リスクと対応する軽減措置、およびその妥当性と有効性を設計レベルで評価します。
- 実装セキュリティ レビュー — 関連するセキュリティの脅威に対する堅牢性を確認するためにコード アーティファクトを実装レベルで評価します。
- セキュリティのコンサルティング — 指定されたプロジェクトに関連するセキュリティ リスク、およびセキュリティ上の懸念事項の解決策に関する継続的なコンサルティングです。多くの場合、プロジェクトのライフサイクルの初期段階において設計空間の調査という形で提供されます。

さまざまなセキュリティ上の懸念がサービス設計レベルで発生します。したがって、サービスの設計フェーズでは、こうした懸念事項を考慮し、これに対処しなければなりません。セキュリティ設計レビューの主な目的は、これが確実に行われていることを確認することです。また、セキュリティ設計レビューの目的には次のようなものがあります。

- プロジェクトに関連するセキュリティ リスクを、関連する脅威の調査に基づいて上位レベルでの評価を行う。
- 十分な情報に基づいてリスク管理に関する判断を下せるようにプロジェクトの意思決定者に対して情報を提供し、セキュリティに関する配慮をプロジェクトの目標に取り入れる。
- 計画されたセキュリティ制御（認証プロトコル、暗号化など）を選択し、正しく実装するためのガイダンスを提供する。
- 開発チームが、脆弱性、攻撃パターン、適切な軽減策の戦略に関して、十分なトレーニングを確実に受けられるようにする。

プロジェクトに革新的な機能やテクノロジーが導入される場合、こうした機能やテクノロジーに関連するセキュリティの脅威、攻撃パターン、テクノロジー固有の脆弱性を調査するのはセキュリティ チームの仕事です。

必要に応じてサードパーティのセキュリティ コンサルティング企業と提携し、Google セキュリティ チームのスキルを補完すると同時に、内部セキュリティ レビューに対する独立した第三者機関によるレビューを実施できるようにします。

Google のソフトウェア ライフサイクルにおけるセキュリティ

セキュリティは、Google の設計および開発プロセスの中核に位置します。Google のエンジニアリング組織では、サービス開発チームが特定のソフトウェア開発プロセスに従う必要はありません。チームはプロジェクトのニーズに応じたプロセスを選択して実装します。このように、Google で採用されているソフトウェア開発プロセスは、アジャイル ソフトウェア開発手法から従来の段階的なプロセスまでさまざまです。

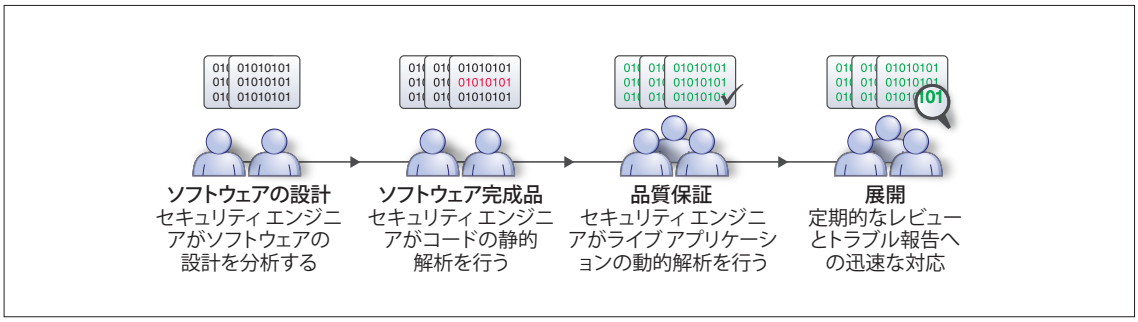

図 3: Google のシステム開発およびメンテナンス戦略

Google のセキュリティ レビュー プロセスは、選択されたフレームワーク内で機能するように調整されます。これが成功するかどうかは、Google の品質重視のエンジニアリング カルチャーや、エンジニアリング管理によって定義された、プロジェクト開発プロセスの次の要件によって決まります。

- 設計ドキュメントが専門家によって評価されている
- コーディング スタイルのガイドラインに従っている
- 専門家によるコード レビュー
- 多層化されたセキュリティ テスト

上に示した要件は Google のソフトウェア エンジニアリングの文化を形作っています。ここでは、ソフトウェアの品質、堅牢性、保全性が重要な目標に含まれます。これらの要件の主な目的は、すべての面で優れた品質のソフトウェア アーティファクトの作成を促進することにあります。また、Google セキュリティ チームの経験から、ソフトウェア設計における安全面での欠陥や欠点を減らすために、これらのプロセスがとても有効で幅広く適用可能であることが明らかになっています。

- 適切な詳細情報が記載された設計ドキュメントはセキュリティ設計レビュー プロセスには欠かせません。プロジェクトの初期段階では、通常、このドキュメントがセキュリティ評価の基礎となる唯一の使用可能なアーティファクトだからです。
- 実装レベルのセキュリティの脆弱性の多くは、基本的には低リスクの一般的な機能欠陥と何ら変わりがありません。実装レベルの脆弱性のほとんどは、開発者側の単純なミスに起因します。
- 開発者とコード レビューアが適切な脆弱性パターンとその回避策のトレーニングを受けている場合には、高品質なコード作成に重点を置いた専門家レビュー（ピアレビュー）をベースにした開発スタイルは、安全なコード ベースを実現するためにとても有効なものとなります。

Google セキュリティ チームのソフトウェア エンジニアは Google の他のエンジニアと協力して、再利用可能なコンポーネントの開発および確認を行います。このコンポーネントは、ソフトウェア プロジェクトが所定の脆弱性を回避できるように設計および実装されます。たとえば、SQL インジェクションの脆弱性に対して本質的に堅牢なデータベース アクセス レイヤや、クロスサイト スクリプティングの脆弱性に対する保護が組み込まれた HTML テンプレート フレームワーク（オープン ソースの **Google CTemplate** ライブラリの **自動エスケープ** メカニズムなど）が例として挙げられます。

セキュリティ教育

Google セキュリティ チームは、エンジニアリング担当者に対する安全なコーディング プラクティスのトレーニングの重要性を認識し、次に示すエンジニアリングの支援および教育プログラムを提供します。

- 新しいエンジニアに対するセキュリティ トレーニング。
- 安全な設計やコーディング プラクティスに関する豊富なドキュメントの作成とメンテナンス。
- 目的やコンテキストを重視したドキュメントやトレーニング資料の提供。たとえば、エンジニアが自動化された脆弱性テスト用ツールを使用した場合、ツールによって報告された特定または一連のバグに関するトレーニング資料や補足資料を参照できます。
- セキュリティ関連のトピックに関する技術的プレゼンテーション。
- セキュリティに関するニュースレター。Google のエンジニアが新たな脅威、攻撃パターン、緩和手法、セキュリティ関連のライブラリとインフラ、ベスト プラクティス、ガイドラインについて学習できるように、エンジニアリング チーム全体に配布されます。
- セキュリティ サミット。セキュリティ関連分野で働く Google のさまざまなチームのエンジニアが集まる Google 全体の会議で、Google のエンジニアリング全体に対してセキュリティに関する詳細な技術的プレゼンテーションを行います。

実装レベルのセキュリティ テストとレビュー

Google では、サービスにおける実装レベルのセキュリティ脆弱性の発生を抑えるために、さまざまなアプローチが採用されています。

- 実装レベルのセキュリティ レビュー: Google セキュリティ チームのメンバーが、通常、サービス開発の後半に実施します。実装レベルのセキュリティ レビューの目的は、関連するセキュリティの脅威に対するソフトウェア アーティファクトの堅牢性を評価することです。このレビューは、通常、セキュリティ設計レビューで特定された脅威と対応策の再評価、セキュリティに不可欠なコードに対する的を絞ったセキュリティ レビュー、コード品質をセキュリティの観点から評価するためのオプションのコード レビュー、的を絞ったセキュリティ テストで構成されています。
- 関連する所定の脆弱性の欠陥に対する自動テスト。このテストでは、社内開発ツールと市販のツールの両方を使用します。
- プロジェクト全体でのソフトウェア品質の評価やテストのために、ソフトウェア品質担当エンジニアが実行するセキュリティ テスト。

障害復旧と事業継続

ハードウェア障害、自然災害などによるサービス中断を最小限に抑えられるよう、Google では、すべてのデータ センターで障害復旧プログラムを実装しています。このプログラムには、次のような単一障害点のリスクを最小限に抑えるための複数のコンポーネントが用意されています。

- データ複製とバックアップ: 災害時の可用性を確保できるよう Google Apps のデータは同一データ センター内の複数のシステムに複製されます。また、別のデータ センターにも複製されます。
- Google では、1 つの地域で災害やその他の事故が発生しても継続してサービスを提供できるように、各地域にデータ センターを分散して稼働させています。データ センター間は高速回線で接続されており、フェイルオーバーが直ちに実行されます。データ センターの管理も分散され、場所に関係なく 24 時間システムを管理します。

データの冗長性、地理的に分散されたデータ センターのほかに、カリフォルニア州マウンテンビューの本社の事業継続計画もあります。この計画では、地震や公衆衛生危機などの大規模な災害に対応したものであり、人材とサービスが最大 30 日間利用できないことを想定しています。この計画は、ユーザーに対する Google のサービスを継続的に稼働できるようにすることを目的としています。障害復旧計画のテストは定期的に行っています。

法令順守

情報にアクセスするための法的手続き

Google では、標準的な法的手続きに従って、第三者からのユーザー情報の開示請求に対応します。第三者に情報が開示されるのは、捜査令状、裁判所命令、召喚状などの法律上の手続き、法定免除、ユーザーの同意がある場合のみです。情報開示の請求を受けた場合、Google の法務部門によりその請求が該当する法律に準拠しているかどうかが調べられます。請求が法的に有効である場合、Google のポリシーでは、情報開示を請求されている個人または組織にその旨を通知します。ただし、緊急時と法的に禁止されている場合を除きます。

プライバシー

Google では、厳正なプライバシー ポリシーに従って顧客データを保護しています。このポリシーの詳細については、**http://www.google.com/a/help/intl/ja/users/privacy.html** をご覧ください。また、Google Apps 内のすべてのアプリケーションにも記載されています。Google のプライバシー ポリシーや実践の詳細については、Google プライバシー センター（**http://www.google.com/privacy.html**）をご覧ください。

簡潔に申し上げるのであれば、Google では顧客データを所有しません。そして、今後もそうすべきと考えています。

Google は、顧客データに関して次の原則を順守します。

- Google では、**プライバシー ポリシー**に定める場合を除き、データを第三者と共有することはありません。
- 顧客が Google Apps と連携して外部のサービスを使用する場合や、Google サービスの利用を停止する場合、顧客は**データを持ち出す**ことができます。

ユーザーのコンテンツのスキャンまたはインデックス登録が行われるのは、顧客に高品質のサービスを提供するために必要な次の場合に限られます:

- メールやドキュメントなどのユーザー データの一部をスキャンして、顧客のドメイン内のユーザーが自分の Google Apps アカウントの情報を検索できるようにします。

- メールをスキャンして、Google が迷惑メールのフィルタリングやウィルスの検出を実行できるようにします。
- メールをスキャンして、Google が状況に応じてコンテンツへの関連性が高い広告を表示できるようにします。
- ユーザーが情報を公開することを選択した場合を除き、Google Apps データが google.com, google.co.jp の通常のインデックスに含まれることはありません。

スキャンとインデックス登録の手順は自動化されており、人が介入することはありません。また、Google は、Google Apps サービスの**利用規約**に違反するあらゆるコンテンツを削除することができます。

セーフハーバー
Google は、告知、選択、第三者への転送、セキュリティ、データの完全性、アクセスと実施に関する米国のセーフハーバー プライバシー ガイドラインを順守し、**米国商務省のセーフハーバー プログラム**に登録しています。

SAS 70
Google は、Google Apps コミュニケーション/コラボレーション サービスだけでなく、Google のセキュリティとコンプライアンス サービス（Postini）について、SAS 70 Type II 認定を取得しています。また、今後も同様の認定を取得するよう努めてまいります。SAS 70 監査は外部監査法人による独立した評価プロセスで、対象の企業が規定の規制を順守しているかどうか、またこれらの規制が効率的に機能しているかどうかを評価します。評価完了後、その会社の規制順守に関する詳細が記載されたレポートが監査法人によって作成されます。

セキュリティ機能のカスタマイズ

上記で説明した、セキュリティと顧客データのプライバシーを保護するために採用しているさまざまなセキュリティ制御の他に、Google Apps では、顧客のドメイン管理者が利用可能ないくつかの追加のセキュリティ オプションが用意されています。Google では、顧客が自分のドメインのセキュリティ制御を管理する際により多くの選択肢をご提供できるように常に取り組んでいます。

シングル サインオン（SSO）
Google Apps for Business、Google Apps for Education、Google Apps for Government、Google Apps for ISP をご利用の場合は、シングル サインオン（SSO）サービスをご利用いただけます。これらの Google Apps には SAML ベースの SSO API が用意されています。管理者は、この API を LDAP や他の SSO システムに統合できます。この機能を使用することで管理者は、証明書、ハードウェア トークン、生体認証などを、認証メカニズムとして利用することができます。

パスワードの長さと安全度
管理者は、自分のドメインのユーザーのパスワードの長さの要件を設定し、さらにパスワードが安全かどうかを表示できます。これにより、長さの要件は満たしていても、安全とは言えないパスワードを特定することができます。

パスワードの安全度の表示機能ではパスワードの安全性がリアルタイムで評価されるため、管理者が今後新たに出現する攻撃パターンに基づいて今後脆弱になる可能性のあるパスワードを識別できます。

管理者ベースのシングル サインアウト
管理者は、ユーザーのログイン Cookie をリセットすることで、ユーザーのアカウントへの不正アクセスを防止できます。これにより、対象となるユーザーはすべてのウェブブラウザ セッションから強制的にログアウトさせられるため、次回 Google Apps にアクセスするには、改めて認証を行う必要があります。

このユーザーログイン Cookie リセット機能と、既存のユーザー パスワード リセット機能を組み合わせて使用することで、デバイスの盗難や紛失が発生した場合でも、クラウド内のセキュリティを高く保つことができます。

セキュリティで保護されたブラウザ接続（HTTPS）
Google Apps for Business、Google Apps for Education、Google Apps for Government、Google Apps for ISP をご使用の場合、ドメイン管理者はドメイン内のすべてのユーザーに対して、Gmail、ドキュメン

ト、カレンダー、サイトなどのサービスで HTTPS（Hypertext Transfer Protocol Secure）を使用するように設定することができます。HTTPS 経由で送信された情報は、Google から送信して宛先コンピュータで受信するまでの間、暗号化されます。

ポリシーを適用した安全なメール転送（SMTP 用の TLS）
簡易メール転送プロトコル（SMTP）に対してTLS（Transfer Layer Security）を使用することで、管理者は、特定のドメイン間でメールを安全に送受信するためのポリシーを設定できます。たとえば、財務チームのメンバーから銀行に送信された外部メールすべてを TLS で保護し、TLS を使用できない場合は保留にするように指定できます。同様に、自分のドメインと、従業員が機密性の高いデータをやり取りする外部の弁護士、監査人、その他のパートナーとの間の接続で、必ず TLS を使用して安全性を確保するように要求できます。

アーカイブ検索
Google では、アーカイブ サービスが、業界固有のさまざまなニーズに対応するのに役立つことを認識しています。Google Message Discovery（Postini）を実装すると、顧客は一元的で検索可能な組織のメール レポジトリを作成できます。これにより、アーカイブ全体を検索して、メールを特定、エクスポートすることができます。このサービスは、顧客が定義した保存ポリシーに基づいて、すべてのメッセージを保存、インデックス登録できます。顧客は、関連するメッセージを特定したり、データを保存、検索、エクスポートして必要に応じて外部のベンダーと共有したりできます。

まとめ

Google では、コンピュータ システムに保存された情報の安全性とセキュリティ確保を最優先しています。Google の多層化されたセキュリティ戦略を構成する 10 個の構成要素は、それぞれが組織全体で承認され守られています。Google Apps では、データ保存、アクセス、転送のそれぞれのレベルでセキュリティを管理し制御することができます。Google を含め、何百万もの組織が Google Apps を利用してビジネスを行い、Google はその信頼に応えるための投資を日々欠かしません。Google はデータのプライバシー、機密性、整合性、可用性を重視しています。今後とも、Google Apps を安心してご利用いただければ幸いです。

Google

WP64-1005