Google Security & Compliance サービス

はじめに

電子通信のユビキタス化は諸刃の剣です。 組織の競争力において電子通信システムがますます重要な役割を果たす一方で、激増する迷惑メール、ウィルス、スパイウェアなどによる攻撃やその他の多くの脅威が組織にもたらされます。また、組織は法令順守の責任において数々の規制やポリシーに従う必要があります。

電子通信の保護についてはさまざまなアプローチが展開されてきましたが、そのほとんどは高価で導入や管理の複雑なポイント ソリューションをベースとしたものです。 これに対し、Google Security & Compliance サービスは、単一でオンデマンド型のプラットフォームによりマルチチャネル通信のセキュリティとコンプライアンスを確保します。 世界中の 4 万を超える企業や組織が電子通信の処理と監視に Google のサービスを採用し、重要な知的財産を外部の脅威から保護しています。

高度な技術と業界標準のポリシーに実践例を組み合わせた多層セキュリティ戦略により、Google のシステムと顧客の通信内容の可用性、整合性、機密性を確保しています。 このドキュメントでは、Google Security & Compliance サービスにおける多層セキュリティ戦略について、プライバシーとデータ統合、組織のセキュリティ、物理的セキュリティ、ネットワーク セキュリティ、アプリケーション セキュリティ、ホストのセキュリティ、運用上のセキュリティの 7 つのセクションに分けて説明します。

プライバシーとデータ統合

Google のサービスのセキュリティ ポリシーと手続きは、顧客の電子通信の機密情報とユーザーのプライバシーを保護するために設計されています。

Google Security & Compliance サービスでは、特許を取得したパススルー処理技術やさまざまな専門技術を使用して、メッセージ コンテンツをリアルタイムで評価します。 顧客の電子通信を手動で処理することはありません。 隔離されたメッセージを含め、コンテンツが正当または不正であろうと、Google のセキュリティとコンプライアンスに関するサービスでは電子通信をすべて自動で処理します。 このアプローチにより、グラム リーチ ブライリー法 (GLBA) や医療保険の相互運用性と説明責任に関する法律 (HIPAA) などの政府のプライバシー規制を順守する必要がある企業も、Google のサービスを使用して、非常に機密性の高いメールの処理を保護できます。

Google Security & Compliance サービスでは、次のようにユーザーのプライバシーを保護しています。

- Google からユーザーに個人の連絡先や属性情報を提供するよう要求することはありません。顧客はアプリケーションの設定を無効にすることで、いつでもサービスを停止することができます。

- Google が個人の名前、ユーザーのリスト、集計データを第三者に販売また公開することはありません。

- Google は顧客が要求するサービスを提供するためにのみ顧客のユーザーの設定情報を使用し、その他の目的で使用することはありません。

- コンテンツ、アドレス、カテゴリ、IP アドレスを含むユーザー固有のメール メッセージ情報の機密性はすべて厳しく保持されます。

Google は顧客との契約の次の条項によって、顧客のデータを常に保護する責任を有しています。

- Google Security & Compliance サービスには、顧客との契約における特定の守秘条項が含まれます。これらの条項は顧客の所在地によって異なりますが、顧客のデータの守秘義務に対する責任を明白に表明するものです。Google はすべての顧客のデータを顧客の財産とみなし、契約に明記されている以外の目的でデータを使用することはありません。また、Google Security & Compliance サービスに関連する顧客のデータを第三者と共有することはありません。

- Google Security & Compliance サービスの処理において、Google は契約上の責任だけでなく、顧客のデータの整合性を保つために運用上の責任も負います。 情報セキュリティ ポリシーの ISO (国際標準化機構) 17799 規格と GAPP 規格 (一般に認められたプライバシー原則) に基づき、認証監査とセキュリティ監査のプロセスの一環として、セキュリティ システムを客観的に測定します。 また、運用上の整合性とセキュリティのベスト プラクティスについて、AICPA Trust Service や SAS-70 Type II 規格による独立した検証を毎年実行しています。

- 機密性とデータ セキュリティの確保は、Google Security & Compliance サービスのアーキテクチャーに不可欠です。 顧客のデータの紛失や流出に対するリスクを減少するために設計されたシステム アーキテクチャーではリアルタイムの記憶領域処理が行われるため、顧客との契約に明記されたサービス レベル契約を満たすことができます。

組織のセキュリティ

セキュリティ戦略の基盤となる組織のセキュリティは、セキュリティ スタッフとセキュリティ ポリシーによって構築され、セキュリティ戦略の残りの 6 つの要素はこれらによって定義されます。

Google Security & Compliance サービスでは、経験豊富な情報セキュリティスタッフが次のことを行います。

- 組織の部署のセキュリティ ポリシーと標準規格を策定し、文書化、施行します。

- 厳正な多層プロセスを使用して、内部ネットワーク (顧客には提示されない) と運用ネットワークのシステム関連のセキュリティ計画をすべて精査します。

- 正規のインシデント レスポンス プロセスを実装し、情報セキュリティの偶発的事故や脅威をすばやく効果的に検出、分析、修正します。

- セキュリティ リスクの継続評価と内部監査によって、既定ポリシーの順守を監視します。

情報セキュリティ プログラムとそのポリシーは ISO 17799 規格に基づいています。これは、安全な企業インフラを構築するため広く採用されている国際規格です。 ISO 17799 には情報セキュリティの包括的な規制とベスト プラクティスが盛り込まれています。

Google Security & Compliance サービスは、運用上の整合性とセキュリティのベスト プラクティスについて、AICPA Trust Service や SAS 70 Type II 規格を使用した第三者による妥当性の検証を受けています。これは、Google が業務とセキュリティの取り組みを開示し、監査を受け、規格に従っていることを証明するものです。

物理的セキュリティ

物理的セキュリティにおいては、Google Security & Compliance サービスのデータ センターを最新かつ非常に安全な施設で保護しています。 各施設には警備員を 24 時間体制で配備し、外部と内部に監視カメラを設置し、施設内への出入りを制限しています。 また、施設の鍵付き設備は許可を受けた従業員以外アクセスできません。

数か所にあるプライマリ データ センターにはそれぞれセカンダリー データ センターまたは補助データ センターがあり、プライマリ データ センターに障害が発生した場合は重要な処理が自動的に引き継がれます。大惨事により複数のデータ センターに同時に影響が生じないよう、プライマリ データ センターと対応するセカンダリ データ センターを異なる地域で運用しています。すべてのデータ センター施設は、地震や洪水による損害や損失を防ぐため、床を高くし、耐震設備が施されています。 また、冷暖房空調設備 (HVAC)、温度調整、バックアップ電源や発電設備、消火設備などの環境管理によって、施設内のすべての装置とシステムは保護されています。

ネットワーク セキュリティ

すべての顧客のデータ処理とストレージ システムを含む運用ネットワークでは、最大限の安定性と稼働時間を確保しています。 各プライマリー システムはミラー サイトで複製され、すべてのメッセージ フロー処理が反映されます。 パフォーマンスやトラフィックのスループットを最大限にするため、システムの処理は内部で負荷が分散され、処理や通信業務をネットワーク リンクやリソースに分散します。 ハードウェアやソフトウェアの不測の障害による損害や損失を回避するため、システム内にサブシステムの冗長性を確保し、高度な障害耐久性を提供しています。

Google Security & Compliance サービスのシステムを管理するネットワーク オペレーション センターでは、スタッフが 24 時間体制で厳重に警備し、システムへのアクセスと状態を監視して、高い可用性とセキュリティを確保しています。

アプリケーション セキュリティ

Google Security & Compliance サービスでは、記憶領域のメッセージをリアルタイムで処理する特許技術により、中核を成すメール セキュリティ サービスにおいて最高レベルのセキュリティを提供しています。 これにより正当なメールをディスクに書き込む必要はなくなり、ディスクやサーバーに保存した場合に起こりうる不正アクセスや破棄、偶発的損失からメッセージを保護します。

メッセージ通信技術の重要な要素である Postini Threat Identification Network (PTIN)® では、リアルタイムのメッセージ処理だけでなく、不要なメッセージ トラフィックを送信している疑いのあるサーバーの起点 IP アドレスをリアルタイムでトラッキング、アップデートしています。

法令順守の要件を満たすためにメッセージをアーカイブする必要がある場合、保管されたデータは、厳格なセキュリティ ポリシーに従って運用環境とのトラフィックを適切に制限するセキュリティ機器により保護されます。図 2 に示すように、Google のセキュリティと法令順守のサービスのアーキテクチャには、保護された一般処理ゾーンと保護された非公開処理ゾーンの 2 つのセキュリティ ゾーンがあります。

保護された一般処理ゾーン

保護された一般処理ゾーンでは、メールと顧客のウェブ アクセスが処理されます。 パススルー処理中、正当なメールは顧客の送信先メール サーバーに直ちに配信され、ウィルスを含んでいたり迷惑メールのプロファイルに適合する疑いのあるメッセージはさらに検証されます。

疑わしいメールをブロックしたり、管理者やエンド ユーザーが確認するためウェブアクセスが可能なストレージ領域に隔離するよう設定することもできます。

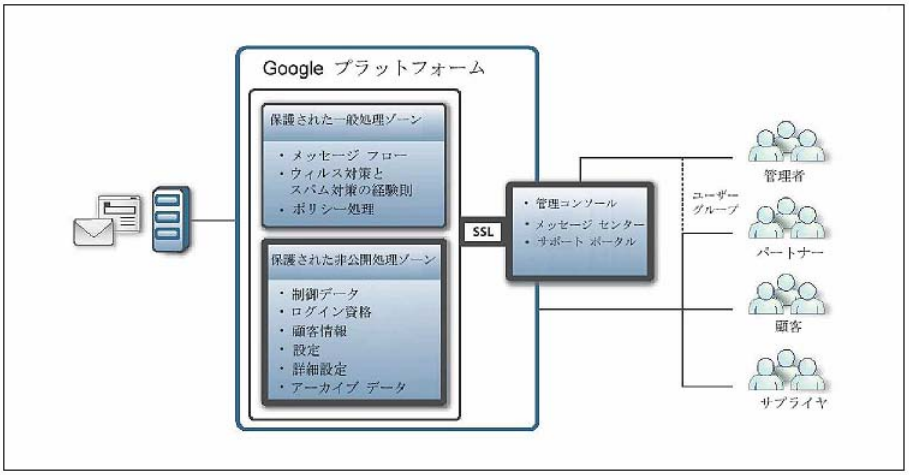

図 2: Google Security & Compliance サービスのアーキテクチャ

データ通信に使われる業界標準の公開キー暗号法である SSL (Secure Socket Layer) セッションを使用して、企業の管理者はウェブベースの管理コンソールに、エンドユーザーはメッセージ センターにアクセスできます。 Google 固有の認証メカニズムと業界標準の認証メカニズムを組み合わせることで、個人データへのアクセスは厳重に制御され、100% の整合性が確保されます。
管理者やエンドユーザーが管理コンソールへのログインに使用するパスワードはネットワーク転送時に暗号化されます。 また、すべてのパスワードは暗号化されてデータベースに保存されます。 機密性の高いメール通信を行う場合は、メッセージ層またはトランスポート層で暗号化送信を行う暗号化メール配信サービスをオプションで使用することができます。

保護された非公開処理ゾーン

保護された非公開処理ゾーンでは、アーカイブ サービスの一環としてメッセージが保存、保護され、有害な可能性のあるメッセージは隔離され、すべてのクライアントのプロファイルと設定情報が保護されます。

Google メッセージ フィルタリング (powered by Postini) または Google メッセージ セキュリティ (powered by Postini) を使用している場合、疑わしいメッセージは専用のデータベースに隔離されます。 不正アクセスからの保護を一層高めるため、隔離されたメッセージのヘッダーと本文は別々に保管されます。 また、隔離されたメールはすべてディスクに 4 回書き込まれます (うち 2 つは冗長サーバーで、どちらもミラー ストレージを使用します)。 この構造により、メッセージを紛失する可能性が排除されます。

Google メッセージ ディスカバリー (powered by Postini) によるメッセージ保管のほか、顧客の正当なメールは 3 つの状況においてディスクに書き込まれます。 そのうち 2 つは正当なメールが誤って隔離された場

合と、大容量の添付ファイルがメール配信の遅延を引き起こす場合ですが、その割合はごくわずかです。

3 つ目は障害復旧時のメールのスプーリングです。これはリクエストに基づくオプションの機能で、何らかの理由で顧客のメール サーバーを利用できない場合にメールをシステムに保管することができます。 顧客のメール サーバーへのメッセージ フローが復旧し、管理インターフェースから手動で配信をリクエストするか、サーバーの利用可能性を自動検出するようサービスを設定して自動的に配信をリクエストするまで、メッセージは保護されたデータベースに保管されます。

ホストのセキュリティ

Google Security & Compliance サービスでは、強化された専用のシステム ソフトウェアを使用して、運用アプリケーションを実行します。 システムを設計、アップグレードする際は、自動プロセスにより整合性を確保し、人的エラーや管理エラーのリスクを排除するとともに、インストール後の処理の整合性を検証します。 サードパーティ製のソフトウェアの導入に先立って、セキュリティ スタッフは次のことを行います。

- アプリケーションで目的の機能を提供でき、運用環境で安定性と信頼性の高い状態で動作できることを確認します。
- 予想されるアプリケーションの欠陥を綿密に検証し、セキュリティとパフォーマンスに与える潜在的な影響を測定します。
- サードパーティ製ソフトウェアのパッチとアップグレードは十分に検証してから承認し、運用サーバーに適用します。

Google ではシステムのセキュリティを監視するため、定期的にメール処理インフラの脆弱性評価を内外で行い、新たな攻撃ルートの有無を確認しています。 脆弱性評価には、修復スケジュールに対するシステム復旧を追跡する修復管理プロセスも含まれます。

運用上のセキュリティ

セキュリティとプライバシーの基準を順守するには、従業員が重要な役割を果たします。 これに対応するため、セキュリティのポリシーと手続きは人事政策と日常業務も対象としています。 雇用前にすべての内定者の身元調査を行い、採用時には全従業員がポリシーと手続きに関するセキュリティ トレーニングを受けます。 また、Google Security & Compliance サービスをサポート、管理、開発する従業員は、毎年行われる情報セキュリティ再認識トレーニングに参加することが義務付けられています。

採用後も、許可されたサポート スタッフ以外、データ センターや保護された設備、運用ネットワークにアクセスすることはできません。 管理者は暗号化された認証リモート接続を使用してシステム管理を行います。すべての運営スタッフは、システム管理のプロセスと手続きに関する訓練を十分に受けた後、システム管理機能を実行する権限が付与されます。

権限を付与されたサポート スタッフのみが運用データにアクセスでき、Google セキュリティ&コンプライアンス サービスに直接関連する問題のトラブルシューティング、インストールやアップグレードの実行、クライアントの移行処理、クライアント接続の検証、パフォーマンス動向の評価を行うことができます。 権限を付与されていないスタッフによる顧客データの操作は固く禁じられています。 ごくまれなケースとして、権限を付与されたサポート スタッフが顧客の電子メッセージ環境にアクセスすることがありますが、これは顧客

に関する問題を解決する目的でのみ行われます。 このようなアクセスや変更は顧客の承認を得たうえで行われます。

SAS 70 Type II 監査の一環として、特定の情報にアクセスする際のセキュリティとプライバシーの規格順守においてスタッフが与える影響を定期的に調査しています。 この監査では、雇用プロセスの詳細、各スタッフに付与されているアクセス権限、Google のセキュリティとプライバシーに関するポリシーの定期的な再検討とトレーニングなどが対象となります。

まとめ

Google Security & Compliance サービスをビジネス コミュニケーションに導入すると、多層セキュリティ戦略により、メッセージのプライバシーと整合性は安全に保護されます。 情報セキュリティのポリシーとベスト プラクティスを特許を取得した最新の処理技術と組み合わせたアプローチにより、企業や組織の機密性の高い知的財産を保護できます。

Google Message & Compliance サービスについて

既存のメール システムのセキュリティ、コンプライアンス、生産性を高めたい企業や組織では、Postini によるメッセージ セキュリティや法令順守のサービスをご利用になれます。 メッセージ セキュリティ サービスでは、迷惑メールやその他のメールによる脅威からシステムを保護します。 法令順守のサービスでは、メッセージ ポリシーとコンテンツ管理を実施し、開示サービスを使用してメッセージをアーカイブするほか、ウェブの閲覧を保護し、機密性のあるメールを暗号化します。 このサービスはインストールや管理の必要がないため、必要に応じて追加サービスを順次導入できます。