



# Google Apps のセキュリティと脆弱性対策に関する総合評価レポート

Google ホワイトペーパー 2007 年 2 月

# Google Apps のセキュリティ



---

詳細情報

---

[www.google.co.jp/a/](http://www.google.co.jp/a/)

---

どのようなシステムにおいても、ネットワーク ベースのアプリケーションをハッキングから保護することが重要となります。メールやコラボレーションのサービスでは、その重要性は決定的と言えるでしょう。Google では、Google Apps のデータを安全に機密保護するため、技術、人材、プロセスに数十億ドルもの投資を行っています。また、セキュリティの専門家からなる専任チームが、Google の厳格なセキュリティ基準とデータのプライバシー保護基準に従って、セキュリティを設計したり、システムやコード、完成したサービスの検証を行っています。Google Apps のホスティングと数十万のユーザー データの保護に使用されるインフラストラクチャは、何百万もの顧客データと数十億ドルにのぼる広告取引の管理にも使用されており、Google Apps のセキュリティと機密保護の高さを実証しています。

はじめに	3
組織的および運用上のセキュリティ	3
開発手法	4
運用上のセキュリティ	4
セキュリティ コミュニティと諮問機関	4
データのセキュリティ	4
物理的セキュリティ	4
論理的セキュリティ	5
情報へのアクセシビリティ	5
冗長性	6
脅威対策	6
スパムやウイルスからの保護	6
アプリケーションおよびネットワークへの攻撃	6
安全なアクセス	7
エンドユーザーの保護	7
管理機能	7
データの機密性	8
まとめ	8



## はじめに

世界中の情報を体系化するというミッションにともない、Google には数千万のユーザー データを安全に保持するという責任があります。Google はこの責任を非常に真剣に受け止め、多大な労力をかけてユーザーからの信用を獲得し、それに応えてきました。安全なサービスを提供することは Google のライフラインであり、この使命感が革新的なサービスの開発にもつながっています。

Google Apps は、過去にわたる安全で信頼性の高い数々のサービスの運用実績の恩恵を受けています。Google のツールやサービスは、業界最高水準のセキュリティ対策が講じられた高度な技術ソリューションで構成され、顧客やユーザーのデータを安全に保護しています。データやアプリケーションのセキュリティにとって最高の環境を構築するべく数十億ドルという膨大な金額を投じており、下記のようなセキュリティ対策に重点を置いています。

- 組織的および運用上のセキュリティ – 設計、導入、運用のすべての段階でセキュリティを確保するためのポリシーと手続きを策定
- データの機密性 – 保護されたサーバーやアプリケーションなど、安全な環境下で顧客データを管理
- 脅威対策 – 悪質な攻撃やハッキングからユーザーおよびユーザー情報を保護
- 安全なアクセス – 許可されたユーザーに限定したデータ アクセスとアクセスチャンネルの保護
- データの機密性 – 機密情報を安全に保持

本ドキュメントでは、物理的、論理的、運用面から多角的に考慮された Google のセキュリティ戦略について説明します。

## 組織的および運用上のセキュリティ

Google におけるセキュリティ戦略の基盤は人材とプロセスです。セキュリティ対策は人材、プロセス、技術の組み合わせにより構築され、これらを適切に連携させることで、安全で信頼できるコンピュータ環境を実現できます。セキュリティは単に事後検証するものではなく、サービス、アーキテクチャ、インフラストラクチャ、システムの設計段階からセキュリティを講じる必要があります。Google では、専任のセキュリティ チームが、包括的なセキュリティ ポリシーを策定、文書化、遂行しています。このセキュリティ チームは、情報、アプリケーション、ネットワーク セキュリティなどの各分野で世界トップの専門家により構成されています。

セキュリティ チームはさらに、ネットワーク境界線の防御、インフラの防御、アプリケーションの防御、脆弱性の検出と対策など、専門分野別に分かれています。経験豊かな情報セキュリティのエキスパート集団が、予防措置に最も注力しながらコードやシステムのセキュリティを設計段階から確保し、セキュリティの問題にも機敏に対応します。

## 開発手法

Google では、サービスの設計段階からセキュリティを重要視しており、エンジニア チームとプロダクト開発チームはさまざまなトレーニングを通じてセキュリティの基本を習得しています。開発はすべて、進行チェックポイントと完全な監査を含む、複数ステップのプランに従って進められます。

Google のアプリケーション セキュリティ チームは、設計の評価、コード監査、システムおよび機能テスト、リリース承認を含む、サービス開発の全工程に関与します。Google では、市場にある技術と独自の技術を活用して、あらゆるレベルでアプリケーションのセキュリティを確保しています。さらに、開発プロセスが顧客の安全をも確実に保護するものであるよう、責任をもって取り組んでいます。

## 運用上のセキュリティ

データの取り扱いやシステムの管理など、システム運用時のセキュリティ確保については、Google のセキュリティ運用チームが担当しています。ここでは、データセンターの運用を常時監査し、Google の物理的および論理的な資産に対する脅威を査定します。

また、セキュリティ運用チームでは、全社員が業務の遂行に必要な審査とトレーニングを受けているかどうかを、専門性とセキュリティの両面からチェックします。Google では所属や必要性に応じて、入社前に厳重な経歴審査を導入しています。セキュリティのプロセスと手続きの維持に関わるすべてのスタッフが、実践的なトレーニングを十分に積み、トレーニングを通じて常に新しい知識を習得する機会も整備されています。

## セキュリティ コミュニティと諮問機関

上記のプロセス以外にも、Google では積極的にセキュリティ コミュニティに関わって、世界中の有識者からの英知やアドバイスを享受しています。これにより、セキュリティの最新動向を把握し、新たに発生した脅威に迅速に対処できるほか、企業内外の専門知識を活用することができます。Google では、信頼できる公開情報を介して、このような大規模なセキュリティ コミュニティに積極的に関わっています。このプログラムの詳細と Google に協力いただいている主な専門家については、<http://www.google.co.jp/corporate/security.html> をご覧ください。

こうしてあらゆるレベルで対策を実施していても、未知の脆弱性がすべて排除されることはありません。このため、Google ではセキュリティの侵害や脆弱性に迅速に対応できる体制も整えています。Google のセキュリティ チームは、すべてのシステムについて考えうる脆弱性を監査し、既知の問題については直ちにエンジニア チームと連携して修正を行います。Google Apps Premier Edition でユーザーに影響するセキュリティ上の問題が発生した場合は、速やかにメールでお知らせします。

## データのセキュリティ

企業データとユーザー データのセキュリティを保護することは、Google のセキュリティ チームと運用チームの最も重要な任務です。Google のビジネスはユーザーの信頼の上に築かれたものであり、この信頼なくして Google のビジネスは存在しません。全社員がこれを真摯に受け止め、エンドユーザーに対する職責の重要性について教育を受けています。データの保護は常に Google のサービスの根底にあり、膨大なデータや広告取引の保護などに多額の費用を投じ万全な体制で臨んでいます。

Google の企業理念については、<http://investor.google.com/conduct.html> をご覧ください。

## 物理的セキュリティ

Google は世界各地に最大規模の分散型データセンター ネットワークを配備しており、これらのデータおよび知的財産の保護に最大の努力を払っています。世界各地に分散したデータセンターを完全に自社で所有、管理することで外部からのアクセスを排除しています。データセンターの拠点は、自然災害やその他の大惨事からの保護を考慮してリスク分散されています。データセンターとサーバーへのアクセスが許されているのは、Google のごく一部の社員だけであり、いかなるアクセスも厳重に管理・監査されます。セキュリティは現地と Google セキュリティ オペレーション センター本部の両方でコントロールされています。

これらの施設は、効率だけでなく、セキュリティと信頼性を最大限に高めることを目的として設計されています。さまざまなレベルで冗長性を持たせることで、最も過酷かつ極端な状況でも安定して運用し、サービスを提供できるように考慮されています。冗長性はセンター内のさまざまなレベルで確保され、発電機付きバックアップ機器による安定運用のほか、分散センター間でもバックアップシステムが配備されています。また、最先端の管理技術により、現地と遠隔地からセンターを監視し、システムを保護するための自動障害回避システムを導入しています。

## 論理的セキュリティ

ウェブベースのコンピュータ環境では、物理的なセキュリティと同様、データとアプリケーションの論理的なセキュリティが必要となります。アプリケーションの安全性、データの取り扱いにおける安全性と信頼性の確保、顧客データまたはユーザー データに対する不正外部アクセスの排除に並みならぬ対策を講じている Google では、さまざまな業界標準への準拠に加えて、独自の革新的な手法を採用し、特殊用途に特化したアプローチをとっています。

Google の多くの技術は、汎用コンピュータとは異なり、特殊機能を提供する目的で開発されています。たとえば、ウェブサーバー層は、特定のアプリケーション操作に必要な機能のみにアクセスできるように、Google で特別に設計、実装されています。これにより、市販のソフトウェアが影響を受けるようなさまざまな攻撃に対しても耐性があります。

また、Google では、セキュリティ確保のコア ライブラリに修正を行っています。Google のシステムは、汎用的なコンピュータ プラットフォームではなく、専用のアプリケーションシステムであるため、標準の Linux オペレーティング システムで提供されるサービスは、部分的または完全に使用できない場合があります。このような修正は、日常業務の遂行に必要なシステムの機能を強化し、セキュリティの侵害につながる不要なシステム要素を無効または除外することを目的としています。

さらに Google のサーバーは、さまざまなレベルのファイアウォールによって保護されています。攻撃の試みがないかトラフィックを適宜検査するとともに、ユーザー データを保護するためのあらゆる試みを行っています。

## 情報へのアクセシビリティ

メールなどのデータは、最適なパフォーマンスを得られるよう、従来のファイルシステムやデータベース様式ではなく、エンコード形式で保存されます。冗長性と臨機応変なアクセスを実現するため、複数の物理ボリュームと論理ボリュームにデータを分散することで改ざんも防ぐことができます。前述のとおり物理的な保護によって、Google のサーバー設備にアクセスすることは事実上不可能であり、稼働中のシステムに対するすべてのアクセスは暗号化されます (SSH、セキュア シェル)。エンドユーザーのデータにアクセスするには、データ構造および Google 独自のシステムに関する専門知識を必要とし、これは Google Apps において機密データのセキュリティを保護するセキュリティ レイヤーのひとつとなっています。

Google の分散型アーキテクチャは、従来型のシングル テナント アーキテクチャと比べ、より高水準のセキュリティと信頼性を実現する目的で構築されています。ユーザーデータは複数の匿名サーバー、クラスタ、データセンターに分散されるため、損失からデータを保護すると同時に高い機密性が確保されます。

ユーザー データは適切な権限を持っている場合のみアクセスでき、ユーザーが他のユーザーの正確なログイン情報を知らずに、そのデータにアクセスすることはできません。これは、メール、カレンダー、ドキュメントを数千万人のユーザーが日々利用しているほか、1 万人を超える Google の社員がメイン プラットフォームとして毎日の業務に使用していることから証明できます。

## 冗長性

Google が運用するアプリケーションとネットワークのアーキテクチャは、最大限の信頼性と可用性を保証できるように設計されています。Google のグリッドベースのコンピュータ プラットフォームは、ハードウェア障害の発生を想定して設計され、強固なソフトウェア障害回避機能によりサービスの中断を回避します。すべての Google システムは冗長に設計され、それぞれのサブシステムは物理サーバーや論理サーバーに依存することなく運用されます。

クラスタ化された Google のサーバー間でデータの複製が繰り返し行われるため、1 台のコンピュータに障害が発生した場合でも、別のシステムからデータにアクセスすることができます。また、ユーザー データはデータセンター間で複製されます。データセンター全体に障害や災害が発生した場合は、ただちにバックアップ先のデータセンターからユーザーにサービスが提供されます。

## 脅威対策

メール ウィルス、フィッシング攻撃、迷惑メールは、今日の企業のセキュリティにおいて最大の脅威となっています。受信メールの 2/3 以上は迷惑メールで、新しいメール ウィルスが日々発生し、インターネット上に配信されているという報告もあります。これらの脅威に対応し続けることは容易ではなく、スパム フィルタやウィルス対策の導入後も常に変化する脅威に注視し、システムを最新の状態に維持しなければなりません。また、ネットワーク ベースのアプリケーションは、データの改ざんやサービスの停止を目的とした不正攻撃の標的となります。Google のワールドクラスの脅威対策は、メッセージやファイルに含まれる悪質な攻撃からデータを厳重に保護します。

## スパムやウィルスからの保護

Google Apps は、業界最強水準のスパム フィルタとフィッシング フィルタを採用しています。Google では、迷惑メールとして識別されるメッセージのパターンを学習する高度なフィルタを開発し、数十億のメール メッセージの情報を継続的にフィルタに反映しています。これにより、迷惑メール、フィッシング、ウィルスをきわめて正確に識別し、ユーザーの受信トレイ、カレンダー、ドキュメントを保護しています。

Google のウェブベース インターフェースでは、ウィルス対策によって、ユーザーが知らないうちに企業の内部ネットワークを介してウィルス感染を拡大するリスクを回避しています。メッセージをローカル ドライブにダウンロードする従来のクライアントベースのメール アプリケーションとは異なり、サーバー上でウィルス チェックを行い、メッセージをスキャンして脅威が除去されるまでユーザーが添付ファイルを開けないようになっています。このように、メールのウィルスによってクライアント側のセキュリティの脆弱性が悪用されることはなく、ウィルスが含まれたドキュメントをうっかり開いてしまうこともなくなります。

## アプリケーションおよびネットワークへの攻撃

Google では、データのコンテンツから不正データやウィルスを排除するとともに、悪質な攻撃からの顧客保護に努めています。ハッカーは、ウェブベースのアプリケーションに忍び込んだり破壊する方法を常に探っています。日常的に発生しているネットワークを対象とした攻撃には、サービス拒否 (DoS)、IP 偽装、クロス サイト スクリプティング、パケット改ざんなどがあります。Google は、世界最大のウェブベース サービス提供企業として、

このような脅威からの保護に最大限尽力しています。市販および独自のさまざまな技術を利用して、ネットワークやアプリケーションを隔々までスキャンしています。また、Google のセキュリティ チームは外部機関と協力して、Google のシステムとアプリケーションのセキュリティ状態をテストし、増強しています。

## 安全なアクセス

データセンターで安全に保護されているデータも、ユーザーのコンピュータにダウンロードされると脆弱なものとなります。平均的なノート型パソコンには、1 万を超えるファイルと数千件のダウンロード済みメールが保存されていることが調査結果で示されています。社内のパソコンが 1 台でも悪意のあるユーザーの手に渡ると、ディスクをマウントするだけで企業の知的財産や機密情報にアクセスされる可能性があります。セキュリティで保護されたネットワーク上でデータを管理できる Google Apps なら、ユーザーがむやみに各自のパソコンにデータを保存することを抑え、前に述べたようなリスクを軽減できます。

## エンドユーザーの保護

Google Apps のデータは Google のサーバーで安全に保存されており、ユーザーがどこからでもアクセスできるというウェブベースならではの利便性があります。メールやスケジュール管理ツールをデスクトップパソコンやノート型パソコンに保存するとそのパソコンでしかデータにアクセスできませんが、Google Apps ならブラウザさえあればどこからでもメールやスケジュールをチェックできます。

他にも、Google ドキュメント など、充実したコラボレーション ツールを使用して情報を柔軟に管理することができます。Google ドキュメント にあるドキュメントもサーバーに保存されているので、ウェブ ブラウザひとつでいつでも閲覧・編集できます。また、各ユーザーのドキュメントへのアクセス権限や編集権限を細かく設定できるオプションもあります。これらの権限はドキュメントへのあらゆるアクセスに適用できるため、内部ドキュメントがメール添付を通じて企業外に流出されるという問題も回避できます。また、ドキュメント内の変更内容は詳細に記録されるため、誰がいつ何を変更したかを追跡することも可能です。

他にも、ネットワーク上での機密データの盗難を防ぎ、ユーザーが安全にデータにアクセスできるように回線のデータ移送を保護しています。Google Apps では管理コンソールもウェブベースです。多くのエンドユーザー向けアプリケーションと同じように、管理コンソールへのアクセスも Secure Socket Layer (SSL) で保護されます。Google Apps の多くのサービスは HTTPS アクセスに対応しており、メールやカレンダーなどの主要なサービスでは HTTPS アクセスのみを許可するように設定できます。この機能を利用すると、ユーザーのデータ アクセスと通信はすべて暗号化されます。

Google では、Cookie を使用してユーザーのコンピュータにパスワードや顧客データを保存することはありません。Cookie は、セッション情報の記録やユーザーの利便性向上の目的で使用されますが、機密情報の取得やユーザー アカウントへの不正侵入に使用されることは一切ありません。

## 管理機能

上述の企業データとユーザー データの保護機能の他にも、企業のセキュリティ、アクセス、監査、認証方法を Google Apps に統合するための管理機能を提供しています。SAML 2.0 に準拠した Google Apps のシングルサインオン API により、組織の既存の認証メカニズムを使用して Google Apps にアクセスできるようになります。たとえば、ログインに Active Directory 認証を使用するよう設定できますが、ウェブベースのツールにアクセスする際に、その認証情報が Google のサーバーを通じて送信されることはありません。これにより、パスワード強化や変更頻度のポリシーを継続して施行することも可能になります。

また、ユーザー管理のための管理コンソールと API も用意されており、管理者は問題のあるアカウントへのアクセスを直ちに遮断したり、要求に応じてアカウントを削除できます。この機能は、API を介してユーザーのプロビジョニングやプロビジョニング解除を行う内部プロセスと関連付けることもできます。

メールとインスタント メッセージは、メール ゲートウェイを経由してメール システムに配信されるよう設計されています。この構成では、メールはすべて貴社のシステムを介して送受信されるため、監視機能を取り入れたメール チェックやアーカイブなどが可能になります。

### データの機密性

Google では、企業とユーザーのプライバシー保護とアプリケーション データの機密保護に細心の注意を払っており、Google Apps で取り扱う情報のセキュリティについても徹底した体制を講じています。すべてのサービスに対して法的な拘束力を持つ Google のプライバシー ポリシーは、<http://www.google.co.jp/privacypolicy.html> でご確認ください。このポリシーおよび関連ポリシーに従い、Google Apps の各サービスにおいて Google 社員がユーザーの機密データにアクセスすることはありません。また、顧客やユーザーからの書面による明確な同意なく、損害を与えかねない形で Google がこのポリシーを改変することはありません。

### まとめ

Google Apps は、データセンター管理、ネットワーク アプリケーション セキュリティ、データ統合の最先端技術とベストプラクティスを結集した、安全性および信頼性の高いプラットフォームを提供します。技術とインフラに全面投資している Google が、貴社のデータ セキュリティ、機密性、整合性を堅牢に保護いたします。

Google Apps の詳細については <http://www.google.co.jp/enterprise/> をご覧ください。もしくは同ページ「お問い合わせ」よりお問い合わせください。