Acronis

ホワイトペーパー

G Suiteの6つの脅威とその対策

いつでも発生しうるデータ消失のリスク

G Suiteをビジネス業務で活用している企業では、重要なデータを保存しているG Suitへも高い稼働率が求められています。多くのIT専門家が、GoogleによりG Suiteに保存されたデータの完全な保護と長期間のデータ保存が実現されている誤解していますが。

現実には、G Suiteに保存されているメール、添付ファイル、カレンダーイベント、コンタクト、ファイルは単純な偶発的削除や巧妙なマルウェア攻撃などによる、深刻なデータ損失問題から保護されていません。

そのため、多くの組織にとってG Suiteに保存されたデータの保護をいかに強化するかが課題となっています。GoogleでG Suiteの標準では、ユーザー側の操作等で損失・破壊・損傷した場合、G Suiteとしてデータを復元するための機能は限定されていることを後から気づいても遅すぎるかも知れません。

> 本ホワイトペーパーでは、Googleのデータ保護機能で見逃しやすい制限事項を概説、これらの課題に対処する方法を考察、G Suite利用時に陥りやすいデータ損失問題への対策方法をご紹介します。

G SUITEを使用する際に直面する可能性があるデータセキュリティの脅威トップ6

Googleはこれまでデータセンターのハードウェア、ソフトウェア、ネットワーク、セキュリティ、オペレーションに多額の投資を行い、G Suiteにおいても高いパフォーマンス・アクセス・稼働時間を保証してきました。サービス提供者の第1の目標は、基本的なインフラの信頼性、つまり重大な自然災害（例えば、洪水、地震、台風など）があってもサービスの復旧・継続的な稼働が可能であること、そして損失・破損したG Suiteデータの短期的、限定的な復旧です。

つまり、自らのクラウドデータセンターの操作エラー、停止、ハードウェア障害、ネットワーク問題を迅速に検出して復旧でき、サービスレベル契約（SLA）で定めた稼働率を満たすことが基本です。しかし、こうした対策の中には、ユーザー企業の従業員による偶発的または不正なデータ削除、そしてランサムウェアやその他のマルウェア攻撃といったデータ整合性に対する外部からの攻撃のような、よくありがちなG Suiteのデータ損失リスクへの対策、データ保護にはつながりません。例えば、IT管理者がGmailのメールに対してあまり考慮せず短い保持期間を設定してしまい、メッセージがすぐ削除されてしまった場合、後日必要な際にGoogle側でも復元できないという事態が発生するリスクが考えられます。実際にこうしたトラブルは、頻繁に発生しています。

> G Suiteでは、ユーザーまたは管理者が削除した後、短期間なら大半のG Suiteデータを復元できます。デフォルトでは、Gmailメッセージと Driveファイルは25日間、ユーザープロフィールは20日間の設定になっています。(https://support.google.com/a/answer/6052340?hl=ja 詳細はこちらを参照ください。)長期休止中のプロジェクトや退職した従業員のファイルやEメールが再度必要になった場合に、長時間検索した後でようやく、Googleが復元可能なコピーを保持していなかったことが判明するという経験をすることもあるでしょう。

G SUITE管理者は6つの主要な分野でデータ脅威に対応する必要があります

1. 偶発的な削除の問題

データリスク: IT管理者、一般の従業員問わず、日常業務の中でG Suiteのユーザープロフィール、Gmailのメールと添付ファイル、カレンダーイベント、連絡先、Google Driveのファイルなどを削除することは比較的頻繁に発生します。こうしたデータ消失は偶発的なものであったり、意図的なものであったりしますが、いずれにしても後で後悔することも少なくありません。削除したばかりのメールが急に必要になることもしばしばです。

Googleで担保されないこと: こうした日常的なデータ消失は、見えないだけで社内では頻繁に繰り返されています。保存時間が経過したデータ消失の課題は、さらに深刻です。一定の期間を超えた古いデータは、物理的に削除され、二度と回復できなくなる可能性があります。一方。比較的新しいファイルやメールを削除した場合や、削除済みアイテムフォルダへ移動したファイルやメールは、ゴミ箱や回復可能なアイテムフォルダからリカバリできるため、問題ありません。

2. 悪意あるインサイダー

データリスク: 日常的な操作の中で発生する誤操作による削除とは別に、G Suiteのリソースは、不満を持つ従業員や犯罪者の従業員、請負業者、パートナーによる不正変更または意図的なデータ破壊のリスクも考えられます。IT管理者は、こうしたデータ消失のリスクからもデータを保護する必要があります。

Googleで担保されないこと: 原則、Googleから悪意あるインサイダーによるG Suiteデータの破壊や変更に対する保護は提供されません。つまり、こうしたリスクへの対策は利用者側が自己の責任範囲として考える必要があります。

3. サイバー脅威

データリスク: G Suiteでは、特定のファイル形式のものや指定のサイズ以下のファイルについてウイルスチェックを提供していますが、ユーザーデータを暗号化し、オンラインで身代金を要求するランサムウェアへの特別な保護機能は提供していません。

Googleで担保されないこと: Googleでは、ランサムウェアのようなマルウェア攻撃に対して特別な保護機能はなく、マルウェアによって暗号化されたり、変更されたりしたファイルを攻撃前の状態に復旧する際にも限定的な機能しか提供しません。

4. 離職する従業員

データリスク:離職する社員や解雇された従業員のG Suiteアカウントをデータの保存を行わずに削除してしまい重要なデータを消失するリスクがあります。

Googleで担保されないこと:最近削除されたG Suiteアカウント(20日以内)を除き、Googleは削除されたG Suiteのデータを復元できません。

5. 保持ポリシーのギャップ

データリスク:G Suiteデータの保持ポリシーの変更や不適切な優先順位によって、データの有効性が切れる前に物理的に削除される可能性があります。これは、定期的な見直しと保持ポリシーの更新によって部分的ではあるものの軽減することができます。

Googleで担保されないこと:G Suiteを利用する企業ユーザーは保持ポリシーを管理する責任を負いますが、理由を問わず、既存の保持ポリシーによって時間の経過とともに物理的削除が発生した場合、Googleは削除されたリソースを復元できません。

6. 法的/コンプライアンスの問題

データリスク:コンプライアンス要件(例えば、税務書類を指定された期間中保持する)や法的な問題は、上記で説明したような保護されていないデータの損失によって業務への支障が出る可能性があります。復元不能なG Suiteのデータ損失によって、企業が政府や業界固有の罰金、法的罰則(例えばe-ディスカバリーや証拠要件を満たさないことに起因する損害または敗訴)、または収益や株価の下落、顧客からの信頼喪失、企業ブランドの失墜などに直面する可能性があります。

Googleで担保されないこと: Googleが上記で説明したすべてのデータ損失リスクについて、さまざまなコンプライアンスや法的問題からG Suiteを使用する組織を保護することは、ほぼ不可能といって差し支えないでしょう。

結論

GoogleのG Suiteにデータを預けたままで安心ではなく、重要なデータを企業の要件に見合った形で保護できるデータ保護ソリューションを探す必要があることを認識しましょう。

ACRONIS BACKUPは、G SUITEに簡単かつ効率的に、そしてセキュアなクラウドバックアップを提供

操作が容易なクラウドツークラウドのG SUITEバックアップ

Acronis Backupは、Googleデータセンターからグローバルなアクロニスデータセンターにエージェントを介さずに直接バックアップすることによって、G Suiteのデータを保護します。Acronis Backupエージェントは、オンプレミスではなくセキュアなAcronis Cloud上で実行されるため、設定やメンテナンスをスムーズにし、簡略化します。

G SUITEの詳細な単位での復元

Acronis Backupでは、さまざまなG Suiteアイテムをすばやく容易に復元できる拡張機能を備えています。このような詳細単位の復元機能によって、バックアップから直接必要なファイルをダウンロードすること、複数バージョンの文書を（最新バージョンだけでなく）ダウンロードすること、データ要素を元の場所や新しい保存先に復元することが可能になります。

高度な検索機能

便利で簡単な検索機能によって、離職した従業員のメールや法的問題を解決するための古いドキュメントをすばやく探せるようになります。Gmailについて、お客様はメールボックスのメタデータ検索を評価でき（メールの件名、受信者、送信者、添付ファイル名、日付による検索）あるいはメール本文のデータを探すためにフルテキストの検索を使用できます。Drive、Contacts、Calendarについては、お客様はファイル名などのメタデータ別に検索できます

GOOGLE DRIVEデータ向けの独自なブロックチェーンベースのノータリゼーション

Acronis Backupを介してGoogle Drivesをバックアップする企業は、ブロックチェーン技術を使ってGoogle Driveのバックアップが改竄されていないことを確認するビルトインのAcronis Notaryサービスを利用できます。このようにGoogle Driveバックアップの整合性をテストできるというのは、法的文書、連絡先、メディアファイル、監視カメラの映像、医療記録、賃貸・リース契約、およびローン契約などで特に役に立ちます。

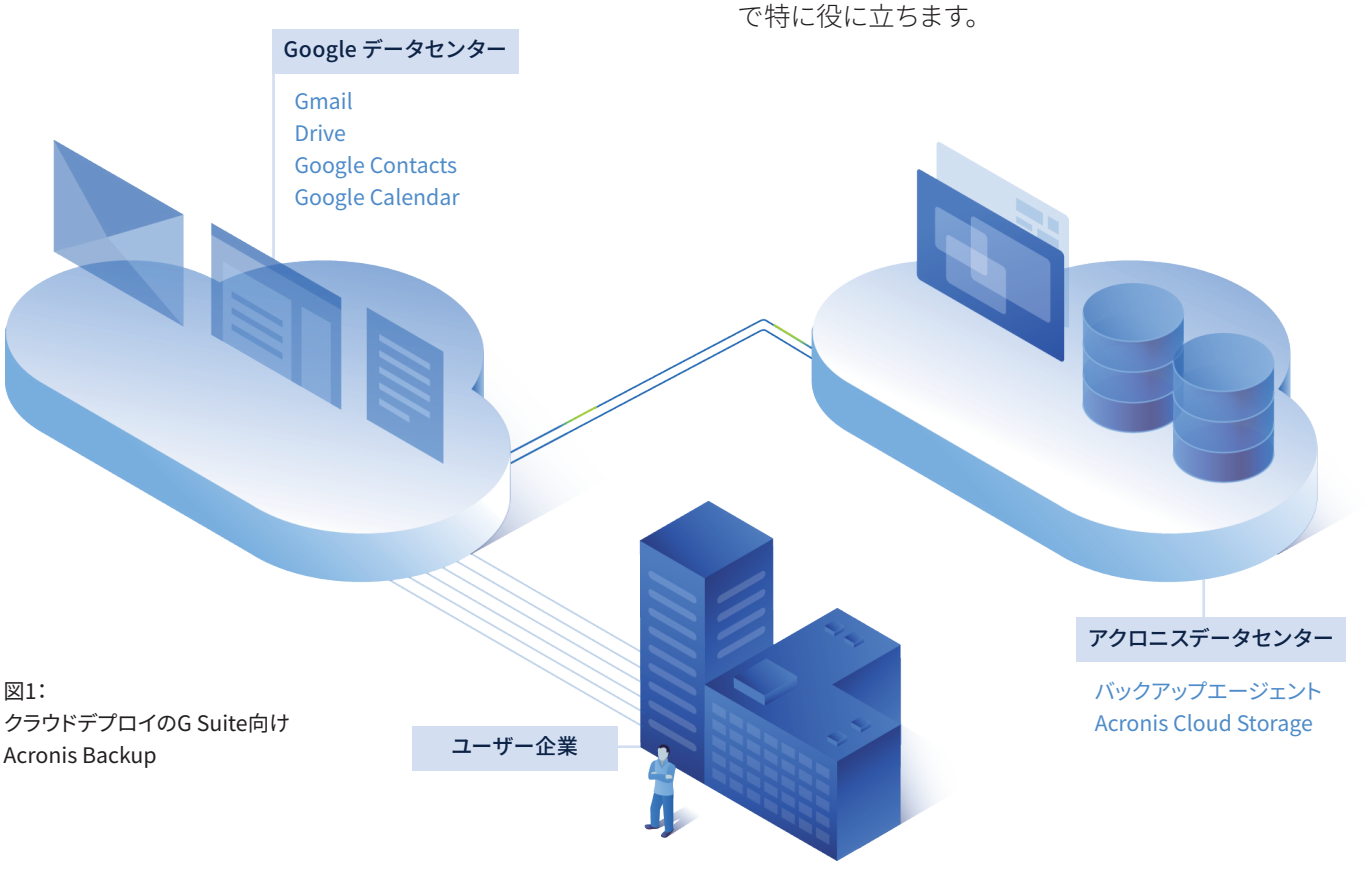

図1：
クラウドデプロイのG Suite向け
Acronis Backup

強化されたデータプライバシー

Acronis Backupは、TLS暗号化を備えたネットワークでのデータ転送、ハイグレードなディスクレベル暗号化を備えたデータセンターストレージ、AES-256を使用するアーカイブ単位の暗号化などによる強化されたマルチレベルのバックアップ暗号化を提供し、狡猾な犯罪者からデータを保護します。

G SUITEの新規ユーザーとチームドライブのオートディスカバリ

グループの初期バックアップ計画の設定が完了し、G Suiteの環境で有効化されると、新規G Suiteユーザーやチームドライブが追加されるたびにITスタッフが変更を行う必要はありません。Acronis Backupは追加されるたびに自動的に検出し、バックアップ計画を更新します。

GOOGLEの多要素認証サポート

AcronisはGoogleの多要素認証（MFA）をサポートし、トラステッドデバイスやフィンガープリントのような追加の認証手段を使用できるようにします。MFAがない場合、パスワードでの確認が必要です。

強力なレポート機能とステータス監視機能

アクロニスは高度なレポート機能とバックアップステータスの監視機能を提供して、ITスタッフの効率性と対応力を向上できるようにします。アクロニスの管理ポータルには、バックアップと復元に関する全統計情報、重要イベントのレポート、通知、アラートを含むコンパクトで分かりやすいウィジェットがあります。

セキュアなACRONIS CLOUD

アクロニスはG Suiteデータをグローバルネットワークである Acronis Cloudにバックアップします。このグローバルネットワークは、リスク評価に基づいたコントロールを含む包括的な情報セキュリティとコンプライアンスプログラムによって保護されたデータセンターネットワークから構成されます。

情報セキュリティポリシーとプロセスは、ISO 27001や国立標準技術研究所（NIST）といった広く承認されている国際セキュリティ標準に基づいており、ヨーロッパのEU一般データ保護規則（GDPR）、米国の医療保険の相互運用性と説明責任に関する法令（HIPAA）のような地域規制フレームワークの要件を考慮しています。Acronis Cloudが提供するデータ保護には以下のものが含まれます。

- **エンタープライズグレードのアクセスコントロール**独自ユーザーIDと強力なパスワード、セキュアな認証プロトコル（LDAP、Kerberos、SSH証明書、二要素認証およびWebアプリケーションファイアウォールの使用）に基づく
- **セキュリティを担保したクラウドバック**転送中、保管時のリアルタイム暗号化、HTTPS（TLS）を使用するセキュアなデータ転送、顧客データ向けのエンタープライズグレードのAES-256暗号化
- **高可用で冗長構造のデータセンター**UPSとディーゼル発電機、冗長構造のHVAC、ネットワークおよびUPS、VESDA、エアサンプリングとデュアルゾーンプレアクション（ドライパイプ）スプリンクラーシステム、温湿度監視によって保護

アクロニスはG SUITEの環境全体（その他のすべても含めて）を保護

Acronis Backupは、ワークロードのホスティングがオンプレミス、プライベートクラウド、パブリッククラウド、どの場合でも、**IT環境全体を保護できる単一のデータ保護ソリューション**です。

それには、物理、仮想、クラウドの環境、主要なオペレーティングシステム（OS）やハイパーバイザ、広く用いられているさまざまなアプリケーション、データベース、さらにデスクトップOS（macOS含む）、iOSやAndroidのようなモバイルOSといった**広範なプラットフォーム**やアプリケーションなどが含まれます。

ユーザーのIT環境全体を保護する単一のプラットフォームによって、互換性のないスタンドアロン型のオンプレミス専用やクラウド専用のバックアップソリューションをばらばらに導入・管理する必要がないため、ライセンス、トレーニング、運用にかかるコストも削減します。図2には**Acronis Backup**によって保護される20以上のプラットフォームが表示されています。

Acronis Backupのユーザーインターフェースは、IT部門の社員なら専門知識がなくても簡単に習得できるため、新しいデータプロテクションスタッフを迅速に立ち上げ、実装、保守、運用のコストを節約できます。

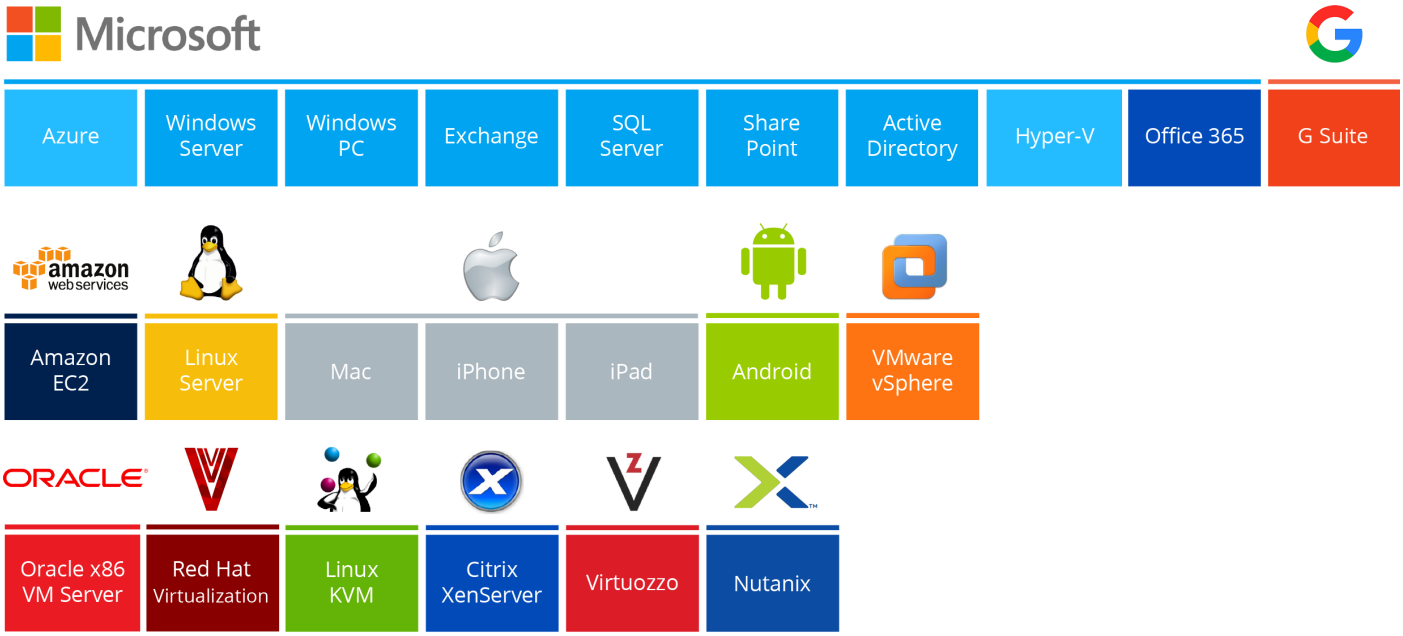

図 2.Acronis Backupが対応しているプラットフォーム

総括

G Suiteを使って業務を行う場合、あらゆる規模のビジネスに対応し、かつ信頼性が高く、使いやすいAcronis BackupでGoogleの限定的なデータ保護を補完する必要があります。

Acronis BackupのG Suiteデータ保護についてさらに知りたい方は、無償で30日間試用版をここから入手するか、アクロニスのリセラーをここから検索してお問い合わせください。