Tableau Online クラウドにおけるセキュリティ

tableau

目次

運用上のセキュリティ 4

システムメンテナンス 4

データのセキュリティとプライバシー 4

プライバシーシールド 4

バックアップと復旧 5

障害復旧 5

データガバナンス 5

ユーザーフィルターとデータソースフィルター 6

ユーザーのセキュリティ 7

アクセス権と認証 7

ロールとパーミッション 8

転送時 (ネットワーク) のセキュリティ 9

暗号化 9

アプリケーションのセキュリティ 9

マルチテナントアーキテクチャ 10

管理ダッシュボード 10

まとめ 10

はじめに

データのセキュリティとプライバシーは組織の成功の基盤となるものであるため Tableau はその保護を最優先にして取り組んでいます。このホワイトペーパーでは、Tableau Online 上にあるお客様のデータのセキュリティと可用性を確保するための Tableau の取り組みについて概要をご紹介します。

Tableau Online にパブリッシュされたデータは、エンタープライズレベルの次のようなセキュリティ機能で保護されています。

- 物理的なセキュリティ
- 運用上のセキュリティ
- データのセキュリティとプライバシー
- アカウントのセキュリティ
- 転送中のデータのセキュリティ
- アプリケーションのセキュリティ

このようなセキュリティ機能はすべて、可用性、パフォーマンス、キャパシティ、セキュリティが継続的に監視されているインフラを基盤にしています。その監視の結果は、お客様のデータの機密性、完全性、可用性を確保できるように、定期的な改善を促進するために利用されています。

Tableau は、さまざまな既知の脅威とゼロデイ攻撃に対して効果的な保護を行うよう設計された、多層セキュリティモデルを導入しました。Tableau のインシデント対応手順の一環として、セキュリティ侵害が発生した場合は、トラスト Web サイト (https://trust.tableausoftware.com) を通じて、または影響を受けるお客様に直接報告されます。インシデント報告には、範囲、重大度、解決策が記載されます。

Tableau は、お客様のデータが安全であると安心していただけるように、世界トップクラスのセキュアなホスティングサービスの維持に常に努めています。

運用上のセキュリティ

SOC 2 と ISAE 3402

Tableau は毎年、独立公認会計事務所の協力を得て、Tableau Online に対する統制目的と統制活動の詳細な監査を実施しています。Tableau Online サービスの統制手順は、米国保証業務基準第 16 号 (SSAE 16) および国際保証業務基準 (ISAE) 第 3402 号の条項に基づいて作成された、SOC 2 Type II 報告書で検証済みです。Tableau Online の SOC 2 Type II 報告書は、ご請求に応じて提供しています。

データセンター

Tableau Online サービスは、あらゆる重要なサービスに対して冗長性が組み込まれ、独立した監査が行われるエンタープライズクラスのデータセンターでホスティングされています。データセンターには、環境的な問題を検知し、機能停止を引き起こす前に対応するよう設計された、火災抑制システムなどの監視システムが設置されています。さらに、そのホスティングプロバイダーは、長時間の停電が発生した場合でも運用を維持できるようにするための契約を供給業者と結んでいます。

Tableau はご請求に応じて、秘密保持契約の締結後ただちに、Tableau のデータセンタープロバイダーに対する監査報告書を提供することが可能です。詳しくは、Tableau アカウント担当者にお問い合わせください。

システムメンテナンス

システムの安定性、セキュリティ、パフォーマンスを確保するために、Tableau Online インフラの維持に責任を負うチームが定期的にメンテナンスを実施しています。計画的なメンテナンスの日程は、最低でも 2 日前に Tableau トラストサイトで告知されます。また、サイト管理者には次回作業のお知らせメールを送信し、すべてのユーザーにも Tableau Online サイトへのログイン時に通知を表示します。

データのセキュリティとプライバシー

プライバシーシールド

欧州経済地域 (EEA) 居住者に関連する個人情報について、Tableau はプライバシーシールドフレームワーク (英語) の認定済みの積極的な参加組織 (英語) であり、連邦取引委員会の調査権限および執行権限に従います。

バックアップと復旧

バックアップは、重要なすべてのコンポーネントで作成されます。バックアップのメディアは暗号化され、セキュリティの保護された施設に常に保管されます。また、ディスクベースのバックアップは、セキュリティの保護されたデータセンター施設に保管されます。さらに、外部のバックアッププロバイダーのために作成されたバックアップは、暗号化のうえ輸送および保管されます。バックアップを入手できるのは承認されたシステム管理者のみです。

Tableau Online のバックアップポリシーに従い、毎日のバックアップは 31 日間保持されます。

これらのバックアップにより、Tableau は Tableau Online システム全体を復元することが可能です。現時点において、バックアップから単一の顧客サイトを復元することはできません。これはつまり、Tableau が、システム障害以外の事象により失われた、個々の顧客のワークブックもデータも復元できないということです。

障害復旧

Tableau は Tableau Online サービスのインスタンスごとに、地理的に異なる場所に、プライマリおよびバックアップのデータセンターを維持しています。プライマリデータセンターが利用できなくなった場合、システムは、サービス稼働トラフィック用に再構成される予定のバックアップサイトでステージングされます。その後、最新のバックアップからデータが復元されます。

Tableau Online は読み取り専用のアプリケーションであり、データは通常、お客様が管理するデータソースから提供されるため、バックアップから復元するのではなく直接ソースから情報を引き出すことにより、ビジュアライゼーションを再度パブリッシュできる可能性があります。これによって、復旧ポイント目標を大幅に短縮することができます。

データガバナンス

お客様のデータはお客様の所有物であり、Tableau Online 内に保存されている場合でも同様です。お客様のサイトに保存されているデータやワークブックにアクセスできるのは、お客様によって許可された個人のみであり、Tableau 従業員も他の顧客もお客様のデータにアクセスすることはできません。唯一の例外は、Tableau Online サービスを実行するシステムの管理を責務とする、少人数の信頼された Tableau 管理者です。このレベルのアクセスをユーザーに認可するためのプロセスは文書化されており、管理者レベルのすべてのアクセスは四半期ごとにレビューと承認を受けます。

お客様のデータの大半は、お客様が所有するデータソース内に安全に保存された状態であることを覚えておいてください。Tableau Online 内に保存されるのは、ワークブック、データ抽出、キャッシュされたデータのみです。

Tableau は、システムの利用状況、アカウントのステータス、パフォーマンスに関する指標にアクセスできるとともに、それらを監視する可能性があります。該当する指標には次のものが含まれます。

- アカウント別およびユーザー別のストレージ総使用量
- アカウント別およびユーザー別の帯域幅総使用量
- アカウント別およびユーザー別のワークブック総数とビュー総数
- ユーザー別のアクセス日時 (ログイン回数)
- アカウント別およびユーザー別のデータソース (SQL Server、Salesforce.com など) の数とタイプ
- アカウント別およびユーザー別のデータ更新日時
- サイトのパフォーマンス指標

データは次の 4 つの方法で Tableau Online に読み込まれます。

1. データが埋め込まれているワークブックのパブリッシュ
2. オンプレミスのソースから Tableau データ抽出へのデータの「プッシュ」。この方法では、リアルタイム接続ではなく必ずデータ抽出になるので、仮想プライベートネットワーク (VPN) や社内環境へのセキュアトンネルを作成する必要はありません。Tableau Online が直接アクセスできないデータソースについては、データ抽出をパブリッシュし、Tableau Online 同期クライアントを使って自動更新のスケジュールを設定することができます。
3. アプリケーションプログラミングインターフェイス (API) 経由での Web サービスへの接続Salesforce.com や Google アナリティクスなど、ほとんどのクラウドデータソースでは、定期的な更新のスケジュールを設定できるデータ抽出の生成に、API 接続を使います。
4. クラウドプラットフォームでホスティングされているデータへの直接接続。このようなデータソースでは、Tableau Online はリアルタイムのライブ接続または抽出ベースの接続を作成することができます。

ユーザーフィルターとデータソースフィルター

ワークブックとデータソースのセキュリティは、ユーザーフィルターおよびデータソースフィルターを追加して強化することができます。ユーザーフィルターは、パブリッシュされたビューで、特定のユーザーに見えるデータを制限できるようにする特殊なタイプのフィルターです。たとえば、売上レポートを地域担当マネージャーと共有する際に、西部担当のマネージャーには西部の売上だけを、東部担当のマネージャーには東部の売上だけを見せたいとします。その場合は、マネージャーごとに異なるビューを作成するのではなく、各マネージャーが特定の地域のデータだけを見られるようにするユーザーフィルターを定義することができます。

ユーザーフィルターは、個々のフィールドに対して定義します。そしてユーザーまたはグループに、そのフィールド内のメンバーのサブセットを見るパーミッションを与えます。上記の売上レポートの例では、地域フィールドでユーザーフィルターを定義し、各マネージャーには対応する地域を見るパーミッションを与えることになります。

データソースフィルターはユーザーフィルターと同様に動作しますが、パブリッシュされたデータソース全体にフィルターを適用できます。ワークブックやデータソースをパブリッシュし、ユーザーに見えるデータを制限する場合に便利です。データソースを Tableau Online にパブリッシュすると、データソースに加えて、関連するファイルまたは抽出がすべてサーバーに送信されます。データソースのパブリッシュでは、データソースのダウンロードや変更のアクセス権を定義できるほか、そのデータソースに対して Tableau Online 経由でクエリをリモートから実行できるユーザーとグループを選択することもできます。ユーザーがクエリ実行のパーミッションを持っており、ダウンロードのパーミッションは持っていない場合、計算フィールド、別名、グループ、セットなどがある高度なデータモデルを、クエリ実行専用として共有することができます。

さらに、このデータソースでクエリを実行するユーザーは、当初パブリッシュされたデータソースにあるデータソースフィルターを見ることも変更することも一切できませんが、これらのユーザーによるすべてのクエリに、データソースフィルターが適用されます。これは、制限があるデータサブセットへのアクセスを提供するのに適した方法です。

ユーザーのセキュリティ

アクセス権と認証

コンテンツとワークブックにアクセスできるのは、サイトに明示的に追加されたユーザーだけです。お客様が指定した管理者は、ユーザーの追加と削除、パーミッションの割り当てなど、アカウント管理のあらゆる役割に責任を負います。アカウント管理は、お客様が完全にコントロールできます。たとえばお客様のサイトに権限を失ったユーザーがいる場合は、単に削除すれば、Tableau Online 内に保存されているコンテンツにアクセスすることができなくなります。

Tableau Online で利用可能な認証方法は 2 つあり、そのいずれか、または両方を利用するように、柔軟にサイトを構成できます。

1. Tableau アカウント

Tableau アカウントは既定で使用され、Tableau が管理する ID ストア内でセキュリティ保護されています。この認証方法では、別の ID プロバイダーと統合しなくても、サイト管理者はすぐユーザーを構成することができます。アカウントは顧客別に管理され、Tableau Online でセキュアな認証を行えるようにします。また、アカウントは Tableau Web サイト、Tableau カスタマー/パートナーポータル、Tableau フォーラムなど、Tableau の他のサービスやリソースへのアクセスでも使用します。

ユーザー認証は、ユーザー名としてメールアドレスと、ユーザーが選んだパスワードを使って行われます。管理者がサイトにユーザーを追加すると、パスワードの設定方法を説明したメールがそのユーザーに送信されます。管理者はユーザーパスワードの設定は行わず、保存されたパスワードを取得することもできません。パスワードにはソルトが加えられ、強力なハッシュアルゴリズムを使ってハッシュ化されます。

アカウントは、サインインが 10 回失敗すると 10 分間ロックアウトされ、その後ロックアウトが発生するたびにロックアウト時間は 2 倍になります。また、ユーザーの同時セッション数は 4 つまでとし、8 時間後にタイムアウトになります。

パスワードは 8 文字以上の半角文字で、英文字と数字を使用する必要があります。

2. SAML

SAML により、管理者は自社の SAML 2.0 対応 ID プロバイダー (IdP) を使って、サイトでシングルサインオンを構成することができます。詳しくは、オンライン製品ガイドのサイト認証セクションをご覧ください。

注: 現在、SAML とシングルサインオンに関連する機能は、ご要望がある場合にのみご利用いただけます。これらの機能をご希望の場合は、Tableau サポートにお問い合わせください。

Tableau Online では、アイドル時間が 2 時間続くと、セッションは強制的にタイムアウトになります。

ロールとパーミッション

Tableau Online 内のアクセスは、サイトロールとパーミッションを組み合わせてコントロールします。Tableau Online に追加されたどのユーザーにも、サイトロールを割り当てなければなりません。サイトロールは管理者が割り当て、それにより Tableau Online へのコンテンツのパブリッシュ、操作、閲覧のみのうちどれを行えるかなど、ユーザーに許可するパーミッションのレベルが決定されます。サイトロールの詳細についてはこちらをご覧ください。一方、パーミッションはコンテンツ (プロジェクト、ワークブック、ビュー、データソース) に割り当てられ、個々のユーザーやグループに割り当てることもできます。パーミッションを指定する際、そのコンテンツを操作できるユーザーを指定するにはルールを使用します。

パーミッションを使用すると、作成、閲覧、変更、削除などを許可することができます。プロジェクトに割り当てられたパーミッションは、そのプロジェクトにパブリッシュされたすべてのワークブックとビューで、既定のアクセスレベルをコントロールします。また、パーミッションを管理しやすくするために、管理者は「財務ユーザー」のようなグループを作成することができます。

パーミッションのウィンドウ

オブジェクトのセキュリティ管理の目的で、20 以上のパラメーターでカスタマイズすることができます。詳しくは、オンラインドキュメントのパーミッションの管理セクションをご覧ください。

転送時 (ネットワーク) のセキュリティ

暗号化

クライアント (Tableau Desktop またはサポートされているブラウザ) と Tableau Online の間の通信はすべて、転送中のデータを保護する TLS を使って暗号化されます。

データソースへの接続は、そのデータソースの暗号化機能に応じて、暗号化される場合と暗号化されない場合があります。使用する予定のデータソースで利用可能な暗号化オプションを理解しておいてください。

さらに、Tableau 製品には、スプーフィング、ハイジャック、SQL インジェクション攻撃を防ぐのに役立つセキュリティ機能が数多く組み込まれています。Tableau はまた、製品の脆弱性テストを積極的に実施しており、定期的なアップデートで新たな脅威に対応しています。

サブスクリプションメールなどのメールを利用する機能は、標準で暗号化されない SMTP を使っていることに注意してください。

アプリケーションのセキュリティ

アプリケーションのセキュリティは、セキュリティ要件の定義、脅威のモデリング、コードレビュー、セキュリティテストなどの、セキュアな設計プラクティスを組み合わせて実現しています。開発プロセ

スの一環として自動および手作業の脆弱性テストが実施されており、メジャーリリースの前には、第三者のセキュリティ会社がアプリケーションの侵入テストを実施します。また Tableau は、第三者のセキュリティ専門家の協力を得て、セキュリティ上の懸念事項のテスト、発見、検証、対処に取り組んでいます。

さらに、Tableau Online も含めた Tableau のインターネット向けのリソースとサービスにおいて、継続的に脆弱性を詳しく調べる、第三者の脆弱性スキャンサービスも導入しています。発見があった場合はアラートが生成され、重大度と影響の評価のために優先順位が付けられます。必要になる可能性がある修正作業の優先度は、この評価に基づいて決定されます。

マルチテナントアーキテクチャ

Tableau Online はマルチテナントソリューションであり、顧客別の環境は提供していません。また、ユーザー、データ、メタデータをサイト別に論理分割することにより顧客を分離します。Tableau Online にアップロードまたはリンクされたすべてのデータは、プログラムによって、そのデータを所有する顧客に関連付けられます。これらのコントロールにより、顧客が他の顧客のデータにアクセスできないようになっています。

管理ダッシュボード

Tableau Online は、お客様のサイトの利用統計データを表示する、既定のダッシュボードのセットをパブリッシュします。表示される内容は、ユーザーのアクティビティ、表示回数、データソースの利用状況などです。管理者はこの既定のダッシュボードを利用して、サイトがどのように使われているかを把握することができます。

管理ダッシュボードの利用について、詳しくはオンライン製品ガイドの「管理ビュー」セクションをご覧ください。

まとめ

Tableau Online サービスは、業界のベストプラクティスに基づく、第三者のセキュリティ専門家によって検証された、堅牢なセキュリティモデルを基盤にして構築および運用されています。Tableau はお客様のデータの重要性を理解しており、それを保護する責任を非常に真剣に受け止めています。

Tableau について

Tableau は、インパクトを生み出すアクションにつながるインサイトを、お客様がデータから引き出せるように支援しています。どこにあるどのような形式のデータにでも、簡単にアクセスできます。隠れたビジネスチャンスを見つけ出すアドホック分析もすぐに行えます。ドラッグ & ドロップ操作で、高度なビジュアル分析を行えるインタラクティブなダッシュボードを作成できます。そして組織全体で共有すれば、チームメンバーが自分の視点からデータを分析できるようになります。グローバルな大企業から、中小企業やスタートアップまで、あらゆる場所で多くのお客様が Tableau の分析プラットフォームを使い、データを見て理解しています。

リソース

無料トライアル版をダウンロード

ビジネス分析をクラウドで行う理由

効果的なキャンペーンダッシュボードを作成するための 5 つのベストプラクティス

すべてのホワイトペーパーを見る