Tableau Server プラットフォーム セキュリティ

エンタープライズセキュリティの 4 つの原理の導入

tableau

目次

はじめに

Tableau は、ガバナンスにより大規模なセルフサービス分析を可能にするモダンなエンタープライズ分析プラットフォームです。セキュリティはデータとコンテンツのガバナンス戦略の最重要事項です。Tableau Server は総合機能と高い統合性で、エンタープライズセキュリティのあらゆる面に対応します。Tableau で組織は信頼できるデータソースを提供できるので、すべてのユーザーが適切なデータを使って正しい決断を素早く下せるようになります。クラウドにより単独の中央 EDW への期待が薄れ、データが急増し続ける中、様々なプラットフォームの間で一貫したセキュリティアクセスを管理することが企業にとって欠かせなくなります。

概要

エンタープライズアプリケーションセキュリティには大きく分けて 4 つのコンポーネントがあり、このホワイトペーパーは Tableau Server におけるこれらのコンポーネントについて詳細に説明します。

1. 認証

2. 許可

3. データのセキュリティ

4. ネットワーク – 送信時のセキュリティ

これらの 4 つのコンポーネントを適切に導入すると、すべてのエンタープライズセキュリティ要件を満たしつつ、幅広いユーザーベースが信頼できるデータにアクセスし、レポートやダッシュボードを作成し、共同分析を行えるようになります。ビジネスユーザーがセキュアなデータと分析プラットフォームに提供されたデータを信頼できるようになり、データが幅広く使用され、データからより多くの価値を引き出せるようになります。エンタープライズセキュリティ要件を満たしつつ、クライアントや契約者による同じ分析プラットフォームへの外部アクセスが可能になります。

Tableau Server は、金融サービス、政府、医療、および高等教育セクターのお客様による厳しいセキュリティ要件を満たしています。銀行や投資会社は機密の投資情報をクライアントに直接提供しています。大学では、Tableau Server を利用してパーソナライズされたレポートを学生や教職員に直接提供しています。Tableau Server は全軍隊支部、および州・連邦政府機関に導入されています。このドキュメントは、Tableau Server がどのようにエンタープライズ規模の総合セキュリティを確保するのかを説明します。

1 認証

Tableau Server は Active Directory、LDAP、Kerberos、OpenID Connect、SAML、信頼できるチケット、証明書を含む、業界標準の様々な認証をサポートしています。また、Tableau Server は、独自のユーザーアイデンティティサービスであるローカル認証もサポートしています。

ユーザーがサインインすると、Tableau Server が言語とロケール、パーソナライズされたスタートページ、個人の作成したコンテンツを含む、カスタマイズされたユーザーエクスペリエンスを提供します。Tableau Server は各セッションの間でユーザー情報を維持し、一貫してパーソナライズされたエクスペリエンスを実現します。Tableau はシステム上のすべてのユーザーに個々のアカウントを作成することで、これを実現しています。さらに、作成者とパブリッシャーは、サーバー全体のアイデンティティ情報を使用して、パブリッシュしたビューの参照元データに対する他のユーザーの許可レベルを管理することができます。

ユーザーアイデンティティ

前述の通り、Active Directory を使用するか、ローカル認証でサーバー内に保存することで、ユーザーアイデンティティの管理が可能です。これら 2 つのユーザー認証の管理方法の違いは次の通りです。

Active Directory

Active Directory をアイデンティティストアとして Tableau Server と統合した場合、Active Directory がすべてのユーザー名とパスワードを管理します。

ユーザーやグループが Active Directory によって一元管理されていても、Tableau Server は独自のリポジトリにユーザー名とグループのコピーを保管します。Tableau は Active Directory 認証が設定されている場合、パスワードを保管しません。ユーザーとグループは管理者によって手動で、または tabcmd コマンドラインユーティリティ か REST API を使用して自動的に Active Directory と同期させることができます。

ローカル認証

Tableau には、ローカル認証と呼ばれているユーザー管理と認証サービスも搭載されています。この方法は、Active Directory を使用しない場合や AD 外のクライアントに導入する場合に使用されます。ローカル認証を使用する場合、ユーザーとグループの管理、および認証プロセス全体が Tableau Server によって行われます。管理者はパスワードを Tableau Server に保管することができますが、パスワードとユーザー情報を OpenID や SAML などの外部サービスに委任することもできます。ユーザーリストは Tableau Server に簡単にインポートすることができ、ほとんどのユーザー管理機能が tabcmd または REST API で自動的に行えます。これにより、自動プロビジョニングプロセスの一部として Tableau ユーザーのプロビジョニングが簡単に行えます。

LDAP

Linux の Tableau Server では、Windows をサポートしている LDAP プロバイダーへの認証が近日サポートされるようになります。Active Directory サーバーで利用できるすべての認証とユーザー管理機能が、LDAP プロトコルと GSSAPI、簡易結合認証、または Kerberos による簡易結合認証のいずれかの認証メカニズムをサポートしているディレクトリサービスで利用できます。IT 部門と一緒にどの方法が適切かご検討ください。

シングルサインオンと外部認証サービスとの統合

Tableau Server は数種類のシングルサインオン (SSO) ソリューションおよび相互 SSL (クライアント証明書認証) をサポートしています。

相互 SSL は、すべてのデバイスで Tableau へのセキュアな自動サインインを実現します。相互 SSL により、有効な証明書のあるクライアント (Windows、Web ブラウザ、または tabcmd.exe の Tableau Desktop) が Tableau Server に接続した際、Tableau Server が有効なクライアント証明書の存在を確認し、自動的に証明書のユーザー名でユーザーをサインインします。

SSO を使用することにより、ユーザーが Tableau Server に手動でサインインする必要がなくなります。代わりに、他の外部認証サービスへの認証 (企業ネットワークへのサインインなど) に使用する認証資格情報を使用して、ログイン画面が表示されることなくシームレスに Tableau Server に認証することができます。SSO はユーザーのアイデンティティを外部で確認し、Tableau Server のアイデンティティストアに定義されているユーザーアイデンティティにマッピングします。

Tableau Server で外部認証サービスを利用した SSO を設定すると、外部認証サービスがすべての認証を行います。しかし Tableau Server は、アイデンティティストアに保存されたサイトロールに基づいて、Tableau リソースへのユーザーアクセスを管理します。詳細は、次の認証に関するセクションをご覧ください。

Tableau Server は次の外部認証サービスとの統合をサポートしています:

- **SAML:** SSO に SAML (セキュリティアサーションマークアップ言語) を使用するよう、Tableau Server を設定することができます。SAML により、外部のアイデンティティプロバイダー (IdP) はユーザーの認証資格情報を認証すると、Tableau Server にユーザーのアイデンティティに関する情報を提供するセキュリティアサーションを送信します。Active Directory やローカル認証の設定に関わらず、SAML を Tableau Server へのアクセスに使用することができます。また、サイトごとに異なる SAML IdP を使用するよう Tableau Server を設定することもできます。これはサイト別 SAML といいます。

- **Kerberos:** ご使用の環境で Kerberos が有効で、Tableau Server が Active Directory 認証を使用するよう設定されている場合、Windows アイデンティティに基づきユーザーにアクセスを提供することができます。Tableau Server がローカル認証を使用するよう設定されている場合、Kerberos は使用できません。

- **Windows 認証の統合:** Tableau Server に Active Directory 認証が設定されている場合、自動ログオンを有効にすることができます。自動ログオンは Microsoft SSPI を使用し、Windows のユーザー名とパスワードでユーザーをサインインします。ユーザーに認証画面は表示されず、シングルサインオン (SSO) や Kerberos のように利用できます。

- **OpenID:** OpenID Connect は、ユーザーが互換性のあるアイデンティティプロバイダーを通してサインインできる、標準の認証プロトコルです。アイデンティティプロバイダーにサインインした後、Tableau Server に自動的にサインインされます。Tableau Server で OpenID Connect を使用するには、ローカル認証を使用するようサーバーを設定する必要があります。Active Directory 認証はサポートされていません。

- **信頼できる認証:** 信頼できる認証 (別名信頼できるチケット) では、Tableau Server と 1 台もしくは複数の Web サーバーの間に信頼関係が設定されます。Tableau Server は、信頼できる Web サーバーからリクエストを受信すると、その Web サーバーが必要に応じてすでに認証を行ったものと見なします。Tableau Server は引き換え可能なトークンまたはチケットと共にリクエストを受信し、ユーザーのロールとパーミッションに基づきパーソナライズされたビューを表示します。

ゲストユーザーと匿名アクセス

注: このオプションはコアベースの Tableau Server ライセンスのみで利用できます。

Tableau Server は、ゲストアカウントによるビューへの匿名アクセスを許可するように設定できます。これは公開 Web などの大規模なユーザーコミュニティや、企業のイントラネットのようなユーザーアイデンティティが必要ないコミュニティにコンテンツを展開する際に便利です。ゲストライセンスにより、Tableau Server にアカウントがないユーザーが埋め込みビューを表示したり操作したりできるようになります。

匿名アクセスにより誤って機密データにアクセスされないよう、Tableau Server へのゲストアクセスは既定で無効になっています。このオプションを有効にすると、自動生成されたゲストユーザーにゲストライセンスが割り当てられます。ゲストユーザーは匿名、つまり誰であるかを認識できないのため、Tableau は誰にでも同じゲストユーザーアカウントを使用します。

匿名ユーザーは、Tableau Server にログインせずにビジュアライゼーションが埋め込まれた Web ページを読み込むことができますが、イントラネットまたはビューがホスティングされているページへのアクセスに認証資格情報を求めるよう設定することができます。匿名ユーザーはリポジトリを閲覧することができず、埋め込みビュー (「embed=true」パラメーターの設定されている URL) へのアクセスのみ可能です。つまり、匿名ユーザーがフラグの埋め込まれていないビューをリクエストした場合、Tableau Server は埋め込みビューのリクエストとして解釈します。そのため、メールで共有された URL や他の Web ページからリンクされた URL は、匿名ユーザー用に適切にプロセスされ、アクセスすることができます。匿名ユーザーには (パーミッションで定義された) ゲストアクセス可能なビューのみレンダリングされ、ゲストユーザーのアクセスが制限されているビューは「埋め込む」フラグの有無に関わらずレンダリングされない点にご注意ください。

コンテンツへのゲストユーザーパーミッションは、Tableau Server の他のすべてのユーザータイプに利用可能な役割全般、パーミッション、データセキュリティで管理できます。Tableau Server が埋め込みビューのリクエストを受信すると、まず初めにユーザーがログインしているか (つまりリクエストに有効期限の切れていないログオンのログインセッションクッキーが付いているか) を確認します。ユーザーがアクティブにログインしていない場合、ゲストユーザーオプションが有効であることを条件に、リクエストはゲストユーザーとしてプロセスされます。

Active Directory 認証の設定で自動ログインが有効になっていると、無効な認証資格情報の扱い方が曖昧なため、ゲストユーザーアクセスは機能しません。

ログアウト

認証においてよく見過ごされがちなのが、セッションの終了です。Tableau Server には、無操作の時間に基づく自動セッションタイムアウト機能があります。管理者は、タイムアウトまでの既定のアイドル時間を変更することができます。また、Tableau Server は絶対的セッションタイムアウトを設定することもできます。

Active Directory 認証を使用していて自動ログインが有効になっている場合、ユーザーは「サインアウト」の代わりに「ユーザーの切り替え」オプションが利用できます。これは、ログアウトすると自動的にまたログインされてしまうためです。他の認証方法では、セッションの終了時に「サインアウト」オプションで手動でログアウトすることができます。

ポータルに埋め込まれたビューのような統合環境では、ポータルのログアウトに加えて Tableau Server からも自動的に強制ログアウトするようにすると便利です。これは、クライアントからログアウト URL をコールすることで簡単に行えます。`https://<Tableau Server>/manual/auth/logout`。

2 許可

ユーザーが正しく認証されシステムへのアクセスが与えられたら、次は、どのコンテンツとサーバーのパーミッションを許可するかです。Tableau Server のサイトロールとパーミッションにより、管理者はユーザーのアクセスできるデータ、コンテンツ、オブジェクト、およびユーザーあるいはグループがそのコンテンツに対して行えるアクションを詳細に管理することができます。通常これらのアクションは機能と呼ばれ、閲覧や操作、コメントの追加、ワークブックの保存、データソースへの接続などがあります。

ユーザーをグループ分けして一斉により簡単にパーミッションを適用することもできます。Tableau Server は、各コンテンツ (プロジェクト、データソース、ワークブック、ワークブック内の個々のビュー) および特定のユーザーまたはグループに対してパーミッション (許可、拒否、または未指定/継承) を柔軟に設定することができます。コンテンツのパーミッションが特に設定されていない場合、Tableau は既定のパーミッションを適用します。これらの既定のパーミッションはコンテンツが作成された時点での既定の設定によって異なり、親コンテンツから継承されます。パーミッションは、ビューの中にどのデータが表示されるかを管理するものではありません。ユーザーがどのデータを閲覧できるかの管理方法は、後のデータアクセスセキュリティのセクションで説明します。

次の例では、オペレーショングループのメンバーに対し、サンプルビューのすべての機能が拒否に設定されています。一方、Joe Doe にはこのビューの全機能が許可されています。マーケティングチームのメンバーにはコンテンツの閲覧許可が与えられていますが、コンテンツの操作や編集の機能に関しては指定されていません。この場合、Tableau Server はワークブック、プロジェクトの順に、グループにこれらのパーミッションが与えられているかどうか確認します。パーミッションが与えられていない場合、拒否とみなされます。

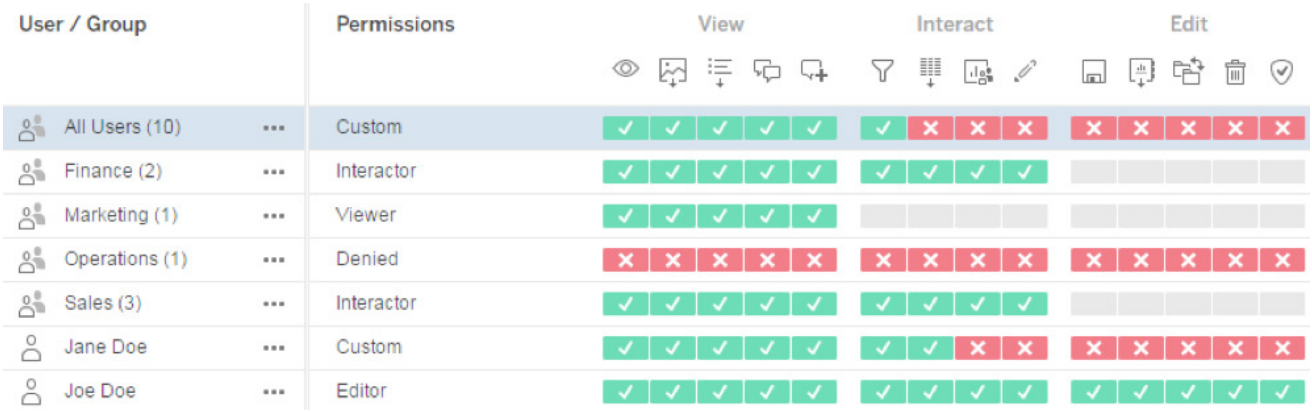

図 1: コンテンツに基づくグループとユーザーのカスタムパーミッションの設定

既定のパーミッションと継承

Tableau はテンプレートを使ってコンテンツの初期パーミッションを設定します。プロジェクトの初期パーミッションは、既定のプロジェクトからコピーされます。そのため、既定のプロジェクトのパーミッションを組織のセキュリティモデルに適したものに設定することが重要です。Tableau Server がオープンパーミッションモデルとも呼ばれている、知識と情報の共有が奨励されているセルフサービス環境に導入されている場合、既定のプロジェクトのパーミッションに「すべてのユーザー」グループを含め、インタラクターパーミッションロールのテンプレートに設定するのが適切です。ユーザーは既定でサーバーの閲覧とパブリッシュされたビューの操作ができ、カスタムパーミッションの定義されたワークブックへのアクセスのみが制限されます。データセキュリティとアクセス管理が必要なクローズドパーミッションモデルに Tableau Server が導入されている場合、既定のプロジェクトで「すべてのユーザー」グループにパーミッションをなしとします。これにより、既定でユーザーとグループには一切のパーミッションが与えられません。新たに作成されたプロジェクトのコンテンツをパブリッシュしたり利用するには、ユーザーとグループに明確なパーミッションを与える必要があります。

コンテンツパーミッションモデル

パブリッシュされたコンテンツにはデータソースやワークブック、ビューが含まれています。コンテンツパーミッションには閲覧、作成、編集、削除などの通常のコンテンツ管理アクションがあります。また、ユーザーがビューの中で行える操作も含まれています。パーミッションはユーザーがコンテンツを検索して Tableau Server UI を利用する際にも適用されます。

コンテンツパーミッションは階層を維持せず、アイテムが初めて作成された時点で初期パーミッションが親コンテンツからコピーされます。また、Tableau Server は親ワークブックのパーミッションからもビューの初期パーミッションをコピーします。親コンテンツのパーミッションへの変更は、コンテンツが手動で更新されパーミッションが再定義されない限り、子コンテンツに自動的に適用されません。コンテンツには親コンテンツと異なるパーミッションが設定されている場合があります。作成者はパーミッションを厳格に設定することも緩く設定することもできます。

ユーザーパーミッションモデル

コンテンツパーミッションモデルとは異なり、Tableau Server はユーザーとグループのパーミッションの継承モデルを提供します。ユーザーに特定のパーミッションが明確に設定されていない場合、ユーザーの属するグループの設定が継承されます。その場合、Tableau Server のパーミッションマネージャービューにはパーミッションが未指定と表示されるか、灰色のボックスが表示されます (図 1 と 2 を参照)。ユーザーやグループに継承でパーミッションが明確に与えられていない場合、その機能は利用できません。グループパーミッションへの変更は、個々のユーザー全員に自動的に適用されます。

パーミッションページでグループまたはユーザーを選択して、画面下のユーザーパーミッションのエリアを確認すると、ユーザーやグループの最終的なパーミッションを確認できることを知っておくと便利です。この方法で、グループの継承設定の適用後に各ユーザーに実際に与えられたパーミッションを確認することができます。また、特定の機能にマウスオーバーすると、機能の名前や最終的な設定、その設定がどのような経過で適用されたのかに関する情報も確認できます。

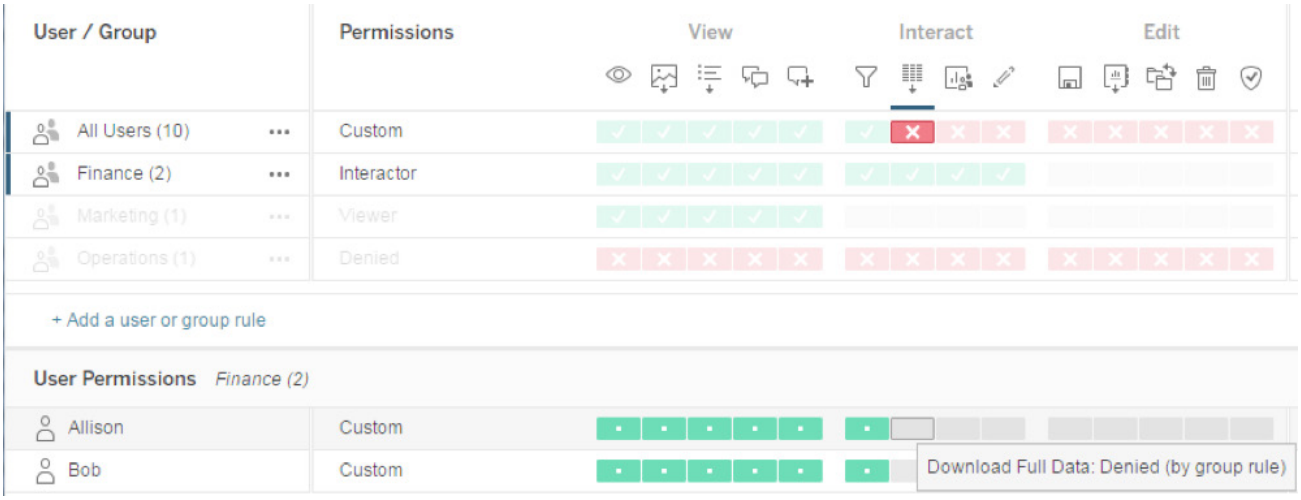

図 2: 各ユーザーの最終的なパーミッション

Tableau Server パーミッション

プロジェクト

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、ビュー、およびデータソースに対する既定のパーミッションは、プロジェクトが管理します。サイトとサーバーの管理者のみがプロジェクトの作成と変更、および作成されたプロジェクトのパーミッションの変更を行え、「プロジェクトリーダー」パーミッションのユーザーは作成したプロジェクト内のすべてのコンテンツとパーミッションを完全に管理できます。適切なパーミッションのあるユーザーは、コンテンツのどの部分に対しても既定のパーミッションを上書きすることができます。例えば、パブリッシャーはパブリッシュしたコンテンツへのアクセスパーミッションを完全に管理することができます。管理者が特定のプロジェクト内のパーミッションに関するより多くのコントロールを必要とする場合、そのプロジェクトのパーミッションを定義したり制限したりすることができます。プロジェクト内のパーミッションをロックした場合、そのプロジェクトにパブリッシュされたすべてのコンテンツに、管理者がそのプロジェクトに設定した規定のパーミッションが適用されます。

パーミッションテンプレート	説明
ビューアー	ユーザーまたはグループにプロジェクトのワークブックとビューの閲覧を許可します。
パブリッシャー	ユーザーまたはグループにサーバーへのワークブックとデータソースのパブリッシュを許可します。
プロジェクトリーダー	ユーザーまたはグループにプロジェクトのすべてのアイテムに対するパーミッションの設定を許可します。
なし	パーミッションルールのすべての機能を**未指定**に設定します。
拒否	パーミッションルールのすべての機能を**拒否**に設定します。
データソースコネクタ	ユーザーまたはグループにプロジェクトのデータソースへの接続を許可します。
データ ソース エディター	ユーザーまたはグループにプロジェクトのデータソースへの接続、編集、ダウンロード、削除、パーミッションの設定を許可します。また、データソースのパブリッシュも可能にします。パブリッシュされたデータソースの所有者は、接続情報と抽出の更新スケジュールを変更できます。このパーミッションは、アクセスしたビューがデータソースに接続する場合にそのビューを対象とします。

その場合、コンテンツ所有者はサーバー上でもワークブックのパブリッシュの際にも、パーミッションを変更することができません。パーミッションをロックするかコンテンツ所有者自身によるパーミッションの管理を許可するかは、管理者とプロジェクト自体の要件次第です。プロジェクトによってはパーミッションがロックされているものもあれば、オープンなものもあります。パーミッションは今後ニーズが変わると共に簡単に変更することができます。プロジェクトによってはパーミッションをロックしたほうが良いものもあれば、オープンにしておいたほうが良いものもあります。パーミッションは今後ニーズが変わると共に簡単に変更することができます。

ワークブックとビュー

機能と利用可能なパーミッションロールテンプレートは、ワークブックのパーミッションを設定するのかビューのパーミッションを設定するのかによって異なります。機能の定義は、パーミッションリファレンスをご覧ください。

パーミッションテンプレート	説明
ビューアー	ユーザーまたはグループにサーバーのワークブックとビューの閲覧を許可します。
インタラクター	ユーザーまたはグループにサーバーのワークブックとビューの閲覧、ワークブックのビューの編集、フィルターの適用、参照元データの閲覧、画像のエクスポート、データのエクスポートを許可します。他のすべてのパーミッションはユーザーまたはグループのプロジェクトパーミッションから継承されます。
エディター	ルールのすべての機能を**許可**に設定します。
なし	ルールのすべての機能を**未指定**に設定します。
拒否	ルールのすべての機能を**拒否**に設定します。
カスタム	選択された機能の組み合わせに対し管理者が定義したルールです。

データソース

データソースのパーミッションは、Tableau Desktop と Tableau Server の両方のユーザーにもう 1 層のセキュリティを提供します。

データソースの「接続」パーミッションのあるユーザーは、Tableau Server の Data Server コンポーネントから Tableau Desktop でデータソースにクエリを実行することができます。ユーザーは自分の認証資格情報を提供するか、元の作成者の保存済み認証資格情報が含まれている場合はそれを使用することもできます。これにより、Tableau Desktop ユーザーはデータウェアハウスや Tableau データ抽出に対してライブクエリを実行する際に、マシンにデータベースドライバーをインストールしたり、データをダウンロードしたりする必要がなく、個人のデータベース認証資格情報も必要ありません。データベースに直接接続することなく、Data Server がプロキシとして機能します。

パーミッションテンプレート	説明
コネクタ	ユーザーまたはグループにサーバーのデータソースへの接続を許可します。
エディター	ユーザーまたはグループにサーバーのデータソースへの接続、編集、ダウンロード、削除、パーミッションの設定を許可します。データソースのパブリッシュも可能で、パブリッシュされたデータソースの所有者である場合、接続情報と抽出の更新スケジュールを変更することもできます。(管理者またはプロジェクトリーダーがデータソースの所有者を変更した場合、最後の 2 つの機能は利用できなくなります。)
なし	パーミッションルールのすべての機能を**未指定**に設定します。
拒否	パーミッションルールのすべての機能を**拒否**に設定します。

また、Tableau Server にパブリッシュされたデータソースを使用しているビューは、ビューと参照元データソースの両方のパーミッション (データとビューの「表示」または「接続」パーミッション) を持っているユーザーしかアクセスできません。ただし、ビューのパブリッシャーにより認証資格情報がデータソースに埋め込まれている場合、ビューの閲覧パーミッションのあるユーザーもパブリッシャーの代理人としてデータソースにアクセスすることができます。Data Server に関する詳細は、Data Server ビデオをご覧ください。

接続について

Tableau Server は、パブリッシュの際にワークブックとデータソースの両方に自動的にデータ接続を確立します。そのため、管理者とデータソースの所有者は接続属性をビューとは別に管理することができます。これにより、それぞれのワークブックを個々に手動で編集する必要なく認証資格情報の更新や新しいデータベースサーバーへの移行が可能になります。さらに、複数ワークブックやデータソースが 1 つの接続を利用できるため、パフォーマンスが向上し重複データが少なくなります。また、キャッシュに保存されたデータがワークブック間で共有され、データベースサーバーへの負荷がさらに低減されます。

パーミッションと管理者

管理者にはサーバー管理者とサイト管理者の 2 つのタイプがあります。サーバー管理者はすべてのサーバーとサイトの機能、サーバーのすべてのコンテンツ、およびすべてのユーザーに完全にアクセスできます。また、サイトやユーザー、メンテナンス、設定、スケジュール、検索インデックスの管理を含め、サーバークラスタ全体を構成することもできます。サイト管理者はサイト内のユーザー、グループ、プロジェクト、ワークブック、データ接続の管理が行えます。サイト管理者は管理が委任されている場合、サイトへのユーザーの追加も行えます。

すべての管理者にはパブリッシュする特権が自動的に与えられます。また、管理者は自分と同じレベルの管理者を追加することもできます。

マルチテナント導入

管理者による組織内のコンテンツの整理やパーミッションの管理には一般的にグループとプロジェクトが使用されますが、単独の Tableau Server 上で複数の外部パーティー (テナント) をサポートするにはサイトが最も多く使用されています。実際に、Tableau のホスト型 SAAS である Tableau Online は、この方法で導入されています。各サイト内のコンテンツ (ワークブック、データソース、ユーザーなど) は、同じ Tableau Server インスタンスの他のすべてのコンテンツからサイロ化されています。言い換えれば、Tableau Server はサーバー管理者がサーバーにユーザーやコンテンツの異なる複数サイトを作成できるようにすることで、マルチテナントをサポートしています。すべてのサーバーコンテンツはサーバーごとにパブリッシュ、アクセス、管理、コントロールされています。つまり、データソースと接続はサイト間で共有することはできません。この機能により、Tableau Server はどのような状況でもクライアントが他のクライアントのデータを見ることがあってはならない金融、医療、教育、その他機関への導入のニーズを満たす強力なセキュリティを実現しています。

ただし、Tableau Server で管理者またはパブリッシャー権限のあるユーザーは、(新しいコンテンツのロールパーミッションを設定する役割があるため) Tableau Server の全ユーザーのリストを見ることができます。さらに、サーバー管理者は Tableau Server にパブリッシュされたすべてのコンテンツを見ることができますが、データへのアクセスはコンテンツのパーミッションとは別のため、Tableau Server の使用するすべてのデータにアクセスできるわけではありません。これに関しては次のセクションでさらに詳しく説明します。

Tableau Server のパーミッションに関する詳細は、Tableau Server: 全ユーザー向けインストールガイドをご覧ください。

3 データアクセスセキュリティ

データアクセスセキュリティはどの企業でも最重要事項ですが、連邦規制の適用される組織や Tableau Server を外部クライアントに導入している組織では特に重要になります。お客様が既存のデータセキュリティに足すことで現在欠けているシステムを補えるように、Tableau は幅広い機能を提供できなければなりません。目標は、ユーザーが Web にパブリッシュされたビューやモバイルデバイスからデータにアクセスしているのか、

それとも Tableau Desktop からアクセスしているのかに関わらず、データセキュリティを 1 か所で管理できるようにすることです。

データセキュリティには次の 3 つの主なアプローチがあります:

1. セキュリティをデータベースのみに導入 (データベース認証)
2. セキュリティを Tableau のみに導入
3. Tableau Server のユーザー情報とデータベースに共通のデータエレメントがあるハイブリッドアプローチを作成。

Tableau Server はこれら 3 つのアプローチをすべてサポートしていますが、多くのお客様にはそのシンプルさと柔軟性から、特に種類の異なる複数のデータソースを使用している場合、ハイブリッドアプローチが好まれています。

データベースセキュリティを利用する場合、データベースへの認証にどの手段を使うかがカギとなります。このレベルの認証は、上記の Tableau Server の認証とは別になります (つまり、ユーザーが Tableau Server にログインしてもデータベースにはログインしたことにはなりません)。そのため、Tableau Server ユーザーはデータベースレベルのセキュリティを適用するためにデータソースへのログイン用の認証資格情報も必要になります。データをさらに保護するため、Tableau はデータベースへの読み込みアクセスの認証資格情報のみを求め、ユーザーのアクセスを読み込み専用に限定することができます。これにより、パブリッシャーが誤って参照元データを変更してしまう事態を防ぐことができ、多くの場合クエリパフォーマンスの改善に繋がります。また、場合によっては一時表を作成するためのデータベースユーザーパーミッションを提供すると便利です。一時データは Tableau ではなくデータベースに保存されるため、これにはパフォーマンスとセキュリティの両方のメリットがあります。一時表を作成するために Tableau ユーザーに制限付きの書き込みアクセスを許可することと、Tableau Server により多くのデータをローカルで保存することの間にはトレードオフがあります。

ワークブックやデータソースにユーザーフィルターを設定することで、パブリッシュされたビューで Tableau Server のログインアカウントに基づきどのユーザーがどのデータを表示できるかをより詳細に管理することもできます。これらのテクニックを組み合わせることで、Tableau Server の幅広いユーザーにセキュアでパーソナライズされたデータと分析を提供できる 1 つのビューまたはダッシュボードをパブリッシュすることができます。

データベース認証

Tableau の高速データエンジンでデータを抽出した場合、データベースのセキュリティパーミッションはエンドユーザーに適用されません。抽出を自動的に更新または増分する際、Tableau Server は保存された単独の認証資格情報 (「実行ユーザー」としてまたはワークブックに埋め込まれた認証資格情報) でそれぞれのデータソースの抽出を生成します。その際そのユーザーのセキュリティ権限がデータベースに施行されます。

パブリッシュされたビューで Tableau Server へのライブデータ接続のあるものは、最新のデータを取得するたびにデータベースにクエリを実行する動的な性質があります。ユーザーがビューを開き、そのビューのデータソースが (Excel ワークブックやテキストファイルのようなものではなく) ログインの必要なデータ

ベースの場合、Tableau Server はデータベースに接続してデータを取得するためにデータベースのユーザー名とパスワードが必要になります。Tableau Server には、どのデータベースのユーザー名とパスワードをデータのアクセスに使用するかを指定するいくつかのオプションと設定があります。Tableau Server 自体にアクセスするための Tableau Server へのログインと、データソースへのアクセスに必要なデータベースへのログインをはっきりと区別することが重要です。次の表は、Tableau Server でビューを作成してパブリッシュするオプションをまとめたものです:

認証タイプ	Tableau Server の応答	Tableau Server がデータベースに搭載されたユーザーベースのデータセキュリティを利用するか
ユーザー名とパスワード入力画面	Tableau がビューアー全員に各自のデータベースの認証資格情報を入力するよう表示します。	利用します。各ユーザーアイデンティティはデータベースに記録されています。
埋め込みパスワード	作成者がビューのパブリッシュ時にデータベースの認証資格情報を指定します。ビューアーには認証視覚情報を入力する画面が表示されません。	利用しません。すべてのユーザーが作成者のデータベースの認証資格情報を使用します。
ビューアー/パブリッシャーの認証資格情報	Kerberos または SAML による SSO での認証にユーザーのドメインユーザー名とパスワードが使用されます。	利用します。各ユーザーアイデンティティはデータベースに記録されています。
Windows 統合セキュリティ (NT 認証)	Tableau Server の「実行ユーザー」	利用しません。すべてのユーザーが同じデータベースの認証資格情報を使用します。
Linux 統合セキュリティ (ad/kerberos 委任)	Tableau Server の「実行ユーザー」	利用します。各ユーザーアイデンティティはデータベースに記録されています。
カスタム		選択された機能の組み合わせに対し管理者が定義したルールです。

Windows 認証

Windows の Tableau Server は「実行ユーザー」の認証資格情報でデータベースに接続します。すべての Tableau Server ユーザーが、データベースへのアクセスにこのプロフィールの接続情報を使用します。この方法では、パブリッシャーの認証資格情報や Tableau Server にログインしているユーザーの認証資格情報は使用されません。このオプションは、データベースが Windows 統合セキュリティを利用している場合にのみ使用できます。これは SQL Server や SQL Server Analysis Services の導入で非常によく見られるケースです。インストール直後の既定の Tableau Server の「実行ユーザー」は、ネットワーク権限ユーザーです。ネットワーク権限アカウントはデータベースに接続する権限がありません。データソースへの NT 認証が可能なアカウントを使用するには、ドメイン名を含むユーザー名とパスワードを指定します。

Linux 認証

Linux の Tableau Server でも「実行ユーザー」認証資格情報が使用できますが、若干異なる形で行われます。Linux では、「実行ユーザー」として使用するユーザーのキータブファイルが必要になります。つまり、タスクごとに異なる「実行ユーザー」を確立する必要があります。たとえば、特定のデータベースに接続するには、データソースがデータソースの「実行プリンシパル」または「実行ユーザー」を使用している必要があります。データソースの「実行ユーザー」は単なるローカルユーザーではなくドメインユーザーである必要があります。

ユーザー名とパスワード (非埋め込み)

Tableau Server の各ユーザーには、データベース別のユーザー名とパスワードでデータベースにログインするよう表示されます。これは既にデータベースセキュリティが設定されている場合、Tableau Server でそのセキュリティを利用するのに有効なオプションです。Tableau Server の設定ページで「保存済み認証資格情報」オプションをオンにすると、Tableau Server のユーザーは 1 つのデータソースにつき認証資格情報を 1 度だけ入力すれば済むようになります。一度認証資格情報が入力されると、Tableau Server はユーザーのデータソースへの認証資格情報を保存し、次回そのユーザーが同じデータソースに接続する際に保存された認証資格情報を再利用します。これらの認証資格情報は通常 Tableau Server へのログインに使用されるものとは別になります。Tableau は常に Tableau Server リポジトリに保管されているすべてのパスワードを暗号化します。データベースパスワードは強力なキーで暗号化されています。導入環境ごとに tabadmin assetkeys コマンドで新しいアセットキーを生成する必要があります。

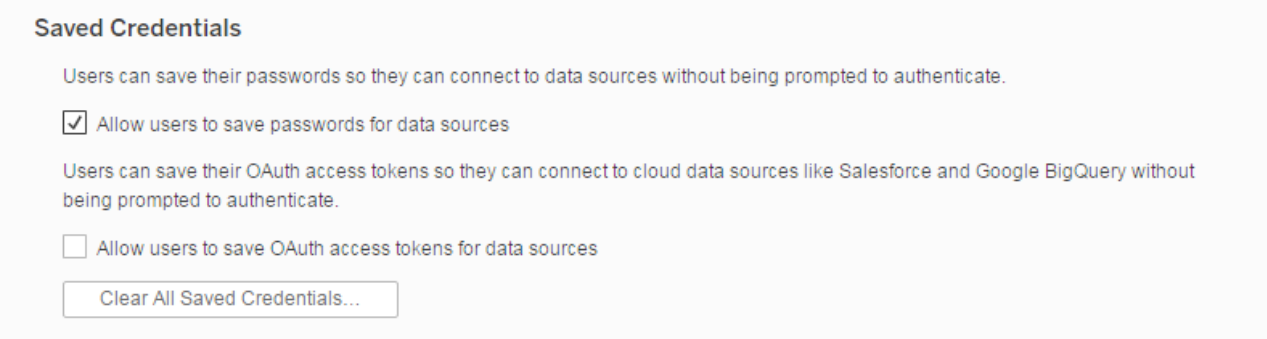

図 3: Tableau Server 設定ページの保存済み認証資格情報の設定

埋め込み認証資格情報 (Windows 認証との併用は不可)

埋め込みの認証資格情報が有効な場合、Tableau Server は各ワークブックの元の作成者のユーザー名とパスワードを保存します。パブリッシュの際に、作成者はデータベースの認証資格情報を入力、つまり作成者自身のユーザー名とパスワードを入力し、「認証資格情報の埋め込み」を選択します。これにより、すべての Tableau Server ユーザーがそのデータソースからのデータの取得にこの接続認証資格情報を使用するようになります。Tableau Server は前述した暗号化メカニズムで、リポジトリの埋め込みの認証資格情報の安全を確保します。この方法を選択する際は、パスワードが期限切れになりユーザーがデータにアクセスできなくなる場合がある点にご注意ください。

データベース別の他のオプション

偽装

Microsoft SQL Server のデータソースに対して、Tableau Server はクエリ実行時のユーザーの偽装をサポートしています。これにより、Tableau が既に Microsoft SQL Server に導入されているセキュリティを活用することができます。Tableau は「実行ユーザー」オプションか、埋め込みの認証資格情報でデータベースに接続します。しかし、すべてのクエリが別のユーザーによって接続されたかのように実行されます。Tableau の偽装機能は、Microsoft のデータベース偽装を使用したコンテキストの切り替えのベストプラクティスに従った SQL Server の偽装機能と併用できるようにデザインされています。

Kerberos 委任

Tableau Server は Kerberos 委任により、作成者ではなくワークブック閲覧者の Kerberos の認証資格情報を使用してクエリを実行することができます。これは次の状況で便利です:

- 誰がデータにアクセスしているのか知りたい場合 (閲覧者の名前がデータソースのアクセスログに記録されます)
- データソースの異なるセルに異なるユーザーがアクセスできる行レベルのセキュリティが設定されている場合。

この機能を利用するには、データベースが Kerberos 委任をサポートしている必要があります。Tableau Server には、ターゲットデータベースのサービスプリンシパル名 (SPN) への委任が許可されている「実行ユーザー」アカウントの制約付き委任が必要となります。Active Directory では委任が既定で有効になっていません。

行レベルのセキュリティと初期 SQL での偽装

データベースへの接続の際、ワークブックを開く際や抽出の更新、Tableau Server へのサインイン、Tableau Server へのパブリッシュの際に実行する初期 SQL コマンドを指定することができます。この初期 SQL はクエリを実行するリレーション (表) を定義するカスタム SQL 接続とは異なります。

このコマンドは次の用途に使用できます:

- セッション中に使用する一時表のセットアップ
- カスタムデータ環境のセットアップ

初期 SQL ステートメントでデータソースにパラメーターを渡すことができます。

これは次のような理由で便利です: **TableauServerUser** または **TableauServerUserFull** パラメーターで偽装を構成できます。データソースがサポートしている場合、行レベルのセキュリティ (Oracle VPD、SAP Sybase ASE など) をセットアップし、ユーザーに閲覧が許可されたデータのみが表示されるようにできます。

クエリバンディング

Tableau Server は Teradata のデータソースに対して、クエリバンドへのユーザー情報の挿入をサポートしています。これにより、データベースのルールまたはその他様々な Teradata のワークフロールールに基づきデータを制限することができます。また、クエリバンドを使うことでパフォーマンスを向上させることもできます。Tableau Server でクエリバンディングを行うには、適切な構成が必要です。

ユーザーフィルター

ユーザーフィルターは、Tableau Server の行レベルのセキュリティへのアプローチです。Tableau はログインしているユーザー名、グループメンバーシップ、その他属性に基づいて動的データフィルターを使用します。ビューを実行する際、Tableau Server はデータベースへのすべてのクエリに適切な WHERE 句を加えて、現在のユーザーがリクエストしているデータを適切に制限します。ユーザーフィルターはデータ抽出を含むすべてのデータソースに使用できます。

パブリッシュされたデータソースに計算フィールドを使用することで、ログインしているユーザーのユーザー名またはグループメンバーシップに基づき様々なディメンションやメジャーをコントロールすることができます。その場合、このフィールドはパブリッシュされる前にデータソースフィルターとして追加されます。ダウンロードを拒否することで、アドホック分析を目的にデータソースに接続しようとする Tableau Desktop と Tableau Server の両方のユーザーに対し、常にユーザーフィルターが適用されるようになります。

たとえば、注文表には顧客情報 (カスタマー ID)、営業担当者情報 (従業員 ID)、および注文の詳細が記録されています。1 つの計算フィールドをビューに追加することで、「username()=customerID OR username()=employeeID」のユーザーフィルターを適用することができます。これにより、Tableau Server にワークブックを 1 つパブリッシュするだけで、外部のお客様と内部の営業担当者に適切なデータをセキュアに提供することができます。それぞれの認証資格情報に基づき、お客様には自分の注文だけが表示され、営業担当者には自分の販売した注文だけが表示されます。

このアプローチのメリットは、新しいユーザーやデータがシステムに追加された際に、ビューに他のメンテナンスを行う必要がない点です。フィルタールールはビューに組み込まれていて、データベースはプロセスするためにこれらのルールに対するキーを動的に提供します。

どのユーザーにどのデータを提供するか自動的に判断するのに適切なコンテンツがデータベースにない場合、手動ユーザーフィルターを作成することができます。このタイプのユーザーフィルターは計算ユーザーフィルターと同様にプロセスされますが、新しいユーザーやデータエレメントに動的に適応しません。そのため、ビューへの追加メンテナンスが必要となります。

データソースフィルター

Tableau Server はデータソースへの直接のフィルター作成をサポートしています。これにより、データソースから返されるデータの量を減らすことができます。たとえば、データベースに過去 5 年から 10 年間のデータが記録されていて、ユーザーのアクセスを過去 3 年間のデータだけに制限したいとします。データソースフィルターを追加することで、簡単にその期間だけを表示させることができます。

既にデータソースフィルターが設定されているデータソースから抽出を作成した場合、これらのフィルターは自動的に抽出フィルターとして推奨され、抽出ダイアログに表示されます。これらの推奨フィルターは抽出フィルターリストに含める必要はなく、既存のデータソースフィルターから個別に削除することができます。

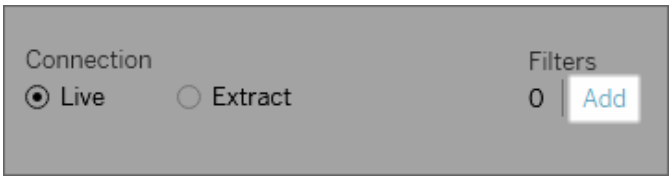

図 4: Tableau Desktop からの Tableau データソースへのフィルターの追加

データソースフィルターは、ワークブックやデータソースのパブリッシュ時に、ユーザーに表示されるデータを制限する場合に便利です。データソースを Tableau Server にパブリッシュすると、データソースと共に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時には、データソースのダウンロードや変更のアクセスパーミッションを定義できるほか、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で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、クエリ実行専用で共有することができます。

さらに、このパブリッシュされたデータソースにクエリを実行するユーザーは、参照元の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閲覧することも変更することも一切できず、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、特定のユーザーやグループのディメンションをフィルタリングしたり、固定の、または相対的な日付範囲に基づきデータソースフィルターを定義したりするなど、制限されたデータのサブセットの提供に有効な手段です。これはデータセキュリティに有効ですが、Tableau Server がユーザーに代わって最終的にクエリを実行するリモートデータベースのパフォーマンスを管理することもできます。区分の指定またはインデックスに大きく依存しているシステムの場合、データソースフィルターは Tableau からのクエリのパフォーマンスを大きく左右することができます。

抽出のセキュリティ

データの抽出が使用されている場合、ビューとワークブックに使用されているデータの保存とプロセスは Tableau Server が行います。データはエンコードされ圧縮されたバイナリ形式の Tableau データ抽出 (TDE) としてファイルシステムに保存されます。抽出の説明を記録したメタデータはプレインテキストで保存されます。

そのため、データは人間には読めませんが、データタイプやフィールド名などのデータの説明の一部を見分けることはできます。Tableau Server はこれらのファイルを保護するため、「実行ユーザー」とマシンのローカル管理者のみアクセスできる「Program Data」ディレクトリに保存します。抽出データファイル自体はディスク上で暗号化されていません。

Tableau が接続する他のデータベースと同様に、データエンジンの抽出は Tableau Server のユーザーインターフェイスから直接クエリを実行することができません。ユーザーはドラッグ & ドロップ分析を行うことはできますが、SQL、MDX、またはその他シンタックスによりデータエンジンデータベースを直接操作することはできません。これにより不正アクセス、SQL インジェクション、その他抽出への悪質な攻撃を防ぐことができます。

サードパーティーや OS のディスクレベルでの暗号化ソリューション (BitLocker など)、ファイルやディレクトリレベルの暗号化 (ファイルシステムの暗号化および EFS) と統合し、データ抽出ファイルのセキュリティをさらに強化することができます。しかし、これらのソリューションは基本的にディスク上のすべてのデータをターゲットにするため、Tableau Server のデータファイルだけが暗号化されるわけではありません。さらに、これらのソリューションを使用するとパフォーマンスに影響が及ぶ可能性があります。

リポジトリのセキュリティ

Tableau Server にはシステムに関する情報 (使用統計、ユーザー、グループ、パーミッションなど) とコンテンツ (ワークブック、ビュー、コメント、タグなど) を保存する内部リポジトリデータベースが搭載されています。このリポジトリには生データ、および Tableau のビューやワークブックで使用される抽出データは保存されません。

既定では、このリポジトリへの外部接続は許可されていません。そのため、リポジトリに保存された情報へのアクセスは既定では Tableau Server のコンポーネントのみに限られています。しかし、この情報に直接アクセスしたいお客様は、「tabadmin dbpass」コマンドでリポジトリを構成し、外部接続を許可することができます。外部接続は Tableau Server のコンテンツや構成の悪用や誤っての変更を防ぐため、データの読み取り専用のビューに限られています。また、Tableau Server の構成ユーティリティで SSL 接続のみを許可するようリポジトリを構成することもできます。

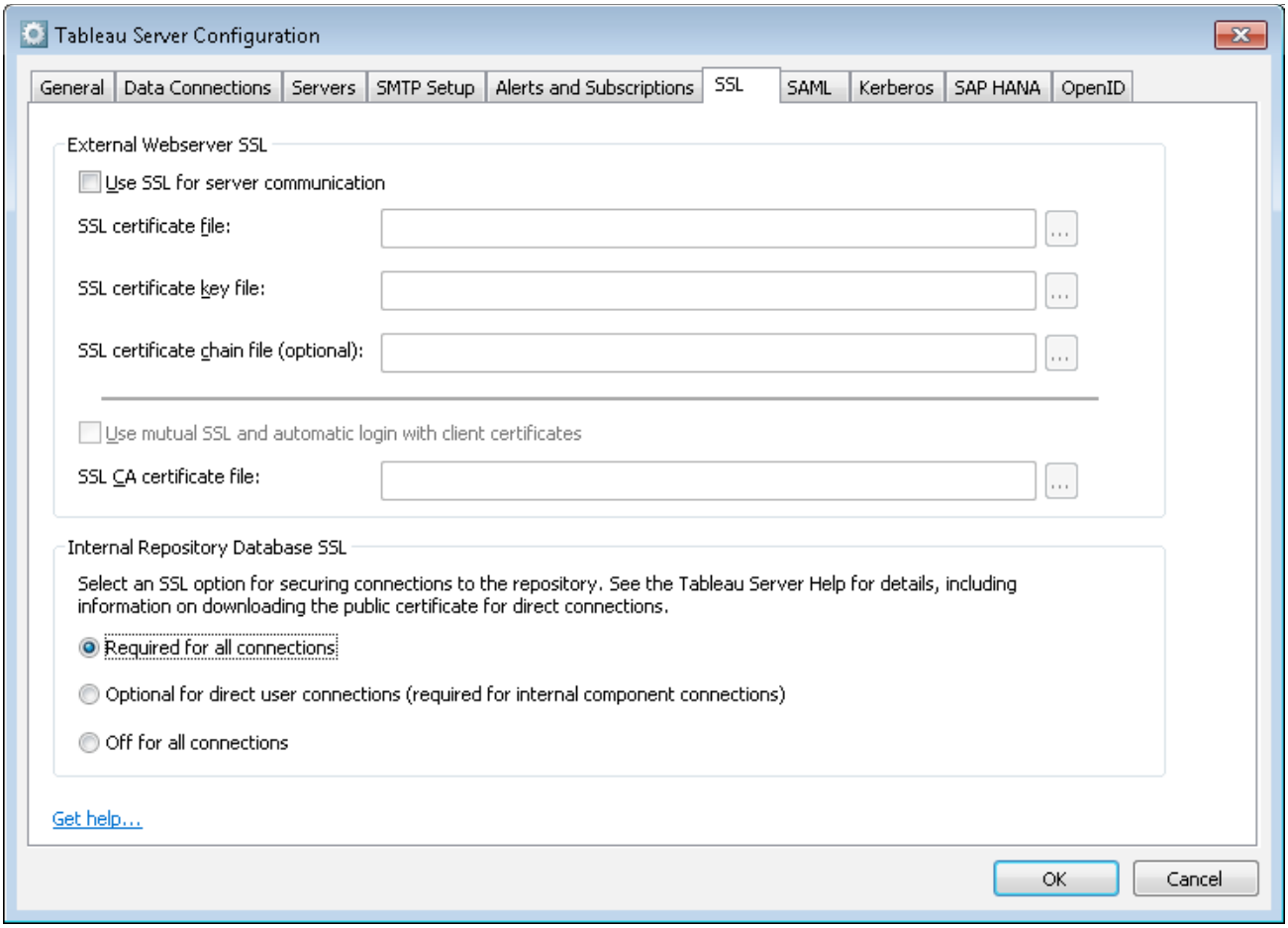

図 5: 内部リポジトリデータベースの SSL の構成

4 ネットワーク – 送信時のセキュリティ

管理者がネットワークセキュリティデバイスを使って、オンプレミスに導入された Tableau Server を信頼できないネットワークやインターネットからのアクセスから保護することがよくあります。しかし、このような場合でもネットワーク間で認証資格情報をセキュアに送信する必要があります。Tableau Server へのアクセスが制限されていない場合、機密データや認証資格情報の保護と Tableau Server の悪用防止に、送信時のセキュリティがさらに重要になります。Tableau Server には、どのような環境にも対応できるよう幅広い送信時のセキュリティ機能が搭載されています。

Tableau Server にはクライアントから Tableau Server、Tableau Server からデータベース、そして Tableau Server のコンポーネント間のコミュニケーションの 3 つの主なネットワークインターフェイスがあります。これらの各インターフェイスに関しては、以下に説明されています。Tableau はこれらの幅広いセキュリティ機能に加え、すべてのレイヤーとインターフェイスでパスワードの保管と送信に細心の注意を払っています。

クライアントから Tableau Server

この場合「クライアント」とは Web ブラウザ、Tableau Desktop、tabcmd、および REST API のことを指します。これらのコミュニケーションには既定で、ほとんどの内部導入環境に適切な標準の HTTP リクエストとレスポンスが使用されます。外部環境または機密性の高い環境では、Tableau Server をお客様の提供するセキュリティ証明書で HTTPS (SSL/TLS) に設定することができます。Tableau Server を HTTPS に設定すると、コンテンツとクライアント間のコミュニケーションがすべて暗号化され、HTTPS プロトコルが使用されます。セキュリティが重要なすべての環境で SSL/TLS を有効にすることをお勧めします。

Tableau Server を HTTPS に設定すると、ブラウザとサーバー上の HTTPS ライブラリが、共に使用する暗号化レベルのネゴシエーションを行います。Tableau はサーバー側の HTTPS ライブラリとして OpenSSL を使用しており、現時点で認められている規格を使うようにあらかじめ構成されています。また、SSL 経由で Tableau Server にアクセスするそれぞれの Web ブラウザは、ブラウザの標準 HTTPS 実装を使用します。この方法は埋め込みの場合でも利用でき、エンドユーザーにセキュリティ警告やポップアップ、例外が表示されないシームレスなエクスペリエンスを実現します。

Tableau Desktop は HTTP または HTTPS で Tableau Server とやり取りします。パスワードを確実にセキュアに送信するには、HTTPS を有効にする必要があります。

Tableau Server とデータベースのコミュニケーション

Tableau Server はデータベースに動的に接続し、結果のセットをプロセスし抽出を更新します。Tableau は可能な場合、ネイティブのドライバーを使用してデータベースに接続します。Tableau はネイティブドライバーが利用できない場合、一般的な ODBC アダプタを使用します。データベースへのすべてのコミュニケーションはこれらのドライバーを介して行われます。そのため、ネイティブドライバーはインストール時に非標準ポートの使用や転送の暗号化が構成され、Tableau はこれらの構成に透過的にアクセスできます。

Tableau Server のコンポーネント間のコミュニケーション

このセクションは Tableau Server が分散配置されている場合にのみ適用されます。Tableau Server コンポーネント間のコミュニケーションには信頼性と送信という 2 つの側面があります。Tableau クラスタ内の各サーバーノードは厳格な信頼性モデルを使用して、クラスタ内の他のノードから有効なリクエストを受信していることを確認します。信頼性は、IP アドレス、ポート、プロトコルのホワイトリストで確立されます。そのいずれかが無効であれば、リクエストは無視されます。同じクラスタに属するコンポーネント同士はすべて自由にやり取りできます。セキュアではないサーバーから Tableau Server をファイアウォールで保護することをお勧めします。

5 その他の検討事項

エクストラネットの外向きな性質から、Tableau Server には外部と接触のある環境でセキュリティを確保するための多くの機能が搭載されています。すべてのクライアントコミュニケーションを 1 つのポートで行うことがその一例です。さらに、組織のネットワークとインターネット間のコミュニケーションがプロキシサーバーを経由して行われるよう、フォワードプロキシとリバースプロキシの構成もサポートしています。

Tableau は、脆弱性を積極的にテストし、新たな脅威に素早く対処して毎月最新情報を提供する社内セキュリティチームを設立しました。最新情報は Tableau のセキュリティページで、セキュアな開発に関するホワイトペーパーをご覧ください。また、組織の Tableau Server 導入のセキュリティを強化するためのさらなるアドバイスを提供するセキュリティ強化チェックリストもぜひご覧ください。

まとめ

Tableau Server は、各環境のニーズに応える総合的なセキュリティ機能を提供します。Tableau は数え切れないほどのお客様のサイトで、一般向けの導入や、セキュアなネットワーク内への導入で成功を収めています。Tableau は最新の業界標準をベースラインとして用い、未来の脅威や問題に素早く対処しています。行レベルのセキュリティからセキュアな Web サイトまで、Tableau のプラットフォームにはお客様のセキュリティに関するありとあらゆるニーズに答える機能が組み込まれています。

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。どこに保存されているかに関わらず、あらゆる形式のデータに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、スタートアップ、中小企業まで、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

Tableau Server セキュリティ強化ガイド

Tableau Server 管理者ガイド

Tableau Server の高可用性: 規模に応じたミッションクリティカルな分析を実行する

Tableau Server のスケーラビリティ - サーバー管理者のための導入テクニカルガイド