

Technical Overview
January 2021

Qlik Sense[®] Enterprise SaaS

Contents

Qlik Sense の概要	2
Qlik Sense Enterprise SaaS の概要	3
アナリティクス向けの単一プラットフォーム	3
連想、インメモリアプリ	3
通知とアラート	5
テナント、ユーザーロール、エンタイトルメント	5
エンタープライズ データ容量	7
インフラストラクチャではなく、アナリティクスに重点を置く	8
オンプレミス データを SaaS に統合する	9
グローバル対応とローカライゼーション	11
信頼性	12
オープンで透明性が高い	12
グローバルな存在感	12
適応可能な高可用性インフラストラクチャ	12
サイト リライアビリティ エンジニアリング	13
セキュリティおよびガバナンス モデル	14
認証と認可	14
ガバナンス	15
標準ベースのセキュリティおよびコンプライアンス	17
コンプライアンスとプライバシー	17
Qlikのクラウドネイティブ プラットフォームと Kubernetes スタック	21
大規模で予測可能なパフォーマンス	22
Qlik Sense Enterprise SaaS の統合と拡張	23
統合のアプローチ	23
API ガバナンスポリシー	26
Qlik オープンソース	26
ツールとリソース	26
Qlik Sense Business から Qlik Sense Enterprise SaaS へのアップグレード	27
まとめ	28

Qlik Sense の概要

Qlik Sense は、第三世代のアナリティクス プラットフォームの基準となり、組織のすべての人がデータ主導の意思決定を行えるように支援しています。独自の連想エンジン上に構築されており、データからインサイトまでのライフサイクルにわたって様々なユーザーとユースケースをサポートします。セルフサービス型のアナリティクス、インタラクティブなダッシュボード、対話型アナリティクス、カスタムおよび組み込み型のアナリティクス、モバイルアナリティクス、レポート作成およびアラート機能など。AI 駆動のインサイトの提案、自動化、そして自然言語インタラクションによって、人の直観を拡張・強化します。さらに、Qlik Sense は、SaaS またはオンプレミスの展開の便利さを備え、比類なきパフォーマンスとガバナンスを提供します。

Qlik Sense は、Qlik が管理するクラウドベースのソリューションである、*Qlik Sense Enterprise SaaS* と *Qlik Sense Business*、および顧客が管理するソリューションである、*Qlik Sense Enterprise Client-Managed* によって構成されています。このドキュメントの焦点は、Qlik Sense Enterprise SaaS です。

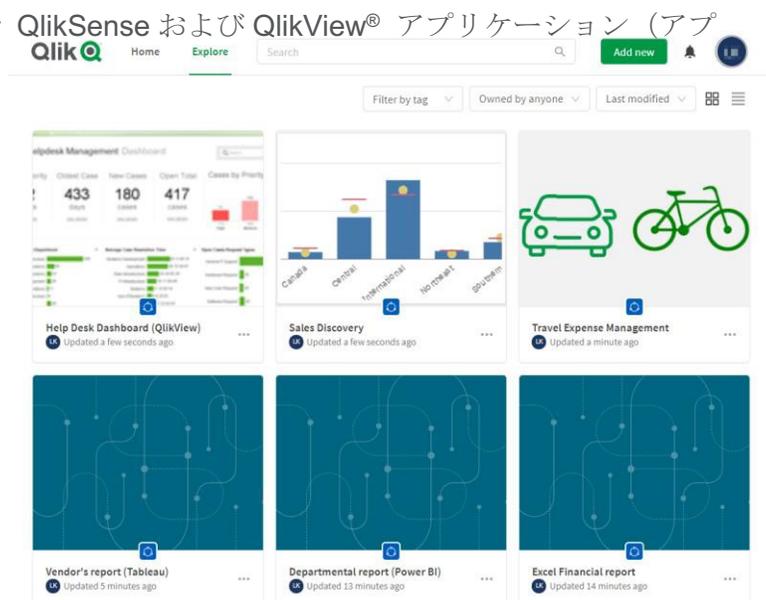
Qlik Sense Enterprise SaaS の概要

Qlik のクラウド ファースト戦略の一環として、独自のクラウドサービス Qlik Cloud Services (QCS) を開発し、製品ポートフォリオのクラウド版を管理して、ソフトウェア・アズ・ア・サービス (SaaS) として顧客に提供しています。Qlik Sense Enterprise SaaS は、プレミアム クラウド ソリューションで、企業が独自に導入・管理する複雑な作業を必要とせずに、世界クラスのアナリティクスをもたらします。

アナリティクス向けの単一プラットフォーム

Qlik Sense Enterprise SaaS の背後にあるマイクロサービスベースのアーキテクチャにより、顧客の Qlik Sense Enterprise SaaS テナントで QlikSense および QlikView® アプリケーション (アプリ) の両方をホストすることができます。

これにより、ユーザーは、Qlik アプリを開いて消費できる単一の場所を持つこととなります。Qlik アプリをホストすることに加え、Qlik Sense Enterprise SaaS はドキュメントなど他のタイプのレポートやアセットへのリンクを追加できるようになり、ユーザーが全てのアナリティクスやレポートのアセットを利用できる単一のポータルを提供します。



連想、インメモリアプリ

Qlik は、インメモリデータストレージ技術を連想エンジンと組み合わせることで、データの分析や操作を自由にかつ直観的に行えるようにします。第二世代では、実証済みの Qlik 連想エンジンによって、ユーザーは簡単にデータを探索し、同時に複数のデータソースからのデータに基づいてビジュアライゼーションを作成できます。これらのソースは、Excel®や Access®から、Oracle® や SQLServer などのデータベースや、Cloudera® や Redshift® などのビッグデータソースまで多岐にわたります。

Qlik Sense はコラム型インメモリストレージを使用します。ユニークな入力インメモリに一度だけ保存され、

データ要素間の関係は、ポインターとして表示されます。これにより、データの大幅な圧縮が可能となり、RAM 上のデータ量が増加し、ユーザーに対する応答時間がより迅速になります。

ビッグデータのシナリオの中には、データはソースに残すべきとありますが、これこそが、オンデマンドアプリケーション生成と呼ばれる内蔵テクノロジーを Qlik が用いている理由です。ユーザーの選択に基づいてデータソースのクエリを実行することができ、しかもユーザーに連想体験を提供します。Qlik の Dynamic Views 機能は、最大のデータソースを利用できるようにこの能力のさらなる向上を図っています。

ユーザー インターフェイス

Qlik Sense Enterprise SaaS 環境へは、ゼロフットプリントのウェブ ブラウザ インターフェイス (Qlik Sense ハブとして知られる) からアクセスできます。Qlik Sense ウェブ ブラウザ インターフェイスは、開発、ドラッグ&ドロップによるコンテンツ作成、利用のあらゆる側面を可能にします。Qlik Sense は応答性の高い設計手法を特長としており、ビジュアライゼーションの表示やサイズ調整を自動的に行って、ラップトップやデスクトップ、タブレット、あるいはスマートフォン上のブラウザであっても、デバイスに合わせて適切なレイアウトと情報を表示します。現在の標準である HTML5、CSS3、JavaScript®、およびウェブソケットとともに構築された Qlik Sense により、どのデバイスでもアプリを構築して利用できます。



ウェブベースのインターフェイスに加え、Qlik Sense は、Slack や MS Teams などの主なチャットプラットフォームと統合された対話型のアナリティクスやデータアラート機能をサポートし、ユーザーが登録するとデータへの主な変更の通知を受けられるようにします。

THE ASSOCIATIVE DIFFERENCE®

リレーショナルデータベースとクエリは、モダンアナリティクス向けではなく、トランザクション システム向けに 1980年代に設計されました。クエリベースのツールは、データを置き去りにして、ユーザーを制約された直線的な探索に制限した結果、盲点をもたらし、機会が失われます。

Qlik Sense は、独自の Qlik 連想エンジンで実行されるため、あらゆるスキルレベルのユーザーが制限なく自由にデータを探索できるようになります。Qlik 連想エンジンによって、データを置き去りにすることなく、ビッグデータであろうが、スモールデータであろうが、制限なくデータを組み合わせられます。これは、インタラクティブな選択と検索により前例のない探索の自由を提供し、即座に全てのアナリティクスを再計算して、ユーザーに緑 (選択値)、白色 (関連値)、グレー (除外値) で関連性を示します。コンテキストのビジュアライゼーションとともに、分析の関連値と除外値を保持することで、Qlik 連想エンジンは、クエリベースのツールでは見逃されてしまう隠れたインサイトをユーザーが発見できるようにします。

Qlik 連想エンジンは、多数のユーザーが利用する大容量のデータに対して、高度にスケーラブルで、動的な計算や関連付けを行うことを目的として構築されました。この独自の技術こそが、25年以上にわたる技術革新と投資による当社の最大の強みです。

通知とアラート

通知機能により、ユーザーは、**Qlik Sense Enterprise SaaS** システムベースのイベントを設定できます。これらのイベントには、アプリケーションのリロードのステータスのほか、スペース内のユーザーのステータスが含まれます。ユーザーは通知サブスクリプションを制御できるので、どのチャンネル（Eメールまたはウェブ）で受け取りたいかを管理することのほか、いつでもサブスクリプションを停止できます。

アラート機能により、ユーザーは、アプリケーションのデータに関連した顧客定義のビジネス条件に基づいてアラートを設定できます。アラートはアプリケーションのリロード時にユーザーにトリガーされ、アプリケーション内の軸とメジャーの組み合わせを使用するように設定できます。アラートは、ユーザーがアクセスを許可されたデータにのみ条件を適用し、設定されたチャンネル（ウェブまたはEメール）に配信することが可能です。**Qlik Sense Enterprise SaaS** の全てのユーザーが個人のアラートを作成できます。**Professional** ロールのユーザーは、他のユーザーを受信者としてアラートに追加できます。ただし、全ての受信者はアラートを受け取るためにアプリケーションへのアクセス権を持っている必要があります。**Qlik Sense Enterprise SaaS** により、ユーザーはアラート履歴を追跡できます。この情報は **AES-256** 暗号化によって保護されており、安全に **QCS** 内に保存されます。

通知とアラートは全て、以下の 2 つのチャンネルから送信するように設定できます。

Eメール。Eメールは、管理コンソールで定義された顧客提供の **SMTP** 設定を用いて送信され、顧客の **SMTP** サービスからのトランスポート レイヤー セキュリティ (**TLS**) セキュリティ設定を使用しています。同じ **SMTP** 設定は、**QCS** のEメール機能と統合された全ての機能で共有されます。

ウェブ。ウェブによる通知とアラートは、署名されたデジタル証明書を持つ **TLS 1.2 AES-256** を用いた安全な **HTTPS** 接続を経由して、**Qlik Sense** ウェブ クライアント ブラウザに送信されます。

テナント、ユーザーロール、エンタイトルメント

テナント

各顧客は、「テナント」と呼ばれる **Qlik Sense Enterprise SaaS** のインスタンスを作成します。**Qlik Sense Enterprise SaaS** の顧客はそれぞれ、独自のテナントを持っています。

ロール

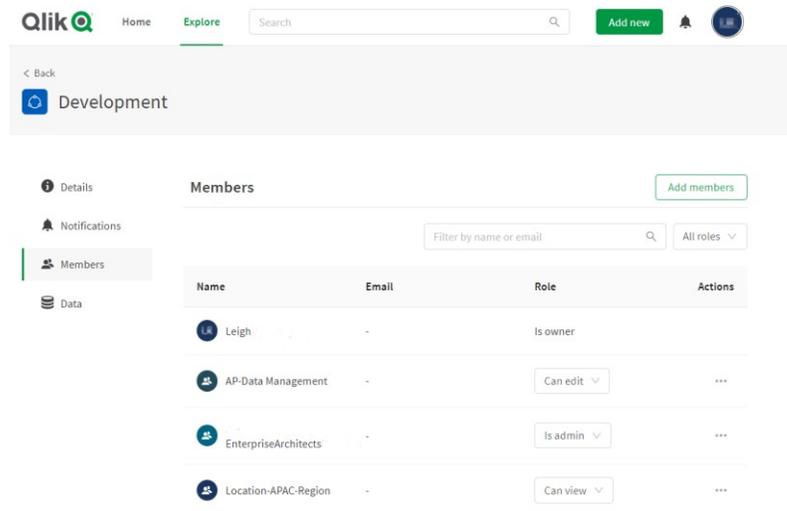
Qlik Sense Enterprise SaaS テナントでユーザーが所有できるロールは 3 つあります。ロールとエンタイトルメントの組み合わせにより、テナント内でのユーザーのアクセス権が決定されます。

- **ユーザー** – このロールは、テナントへのアクセス権を持つ全員に付与されます。これは、具体的に付与されるのではなく、暗黙的に付与されます。さらに、以下のライセンスタイプに分類されます。
 - **Professional - Professional** アクセス権は、**Qlik Sense Enterprise** 内の全機能にアクセスする必要があるユーザーのためのものです。ユーザー単位で課金されます。
 - **Analyzer - Analyzer** アクセス権は、他者が作成したコンテンツを消費するユーザーのためのものです。ユーザー単位で課金されます。
 - **Analyzer Capacity - Analyzer Capacity** アクセス権は、他者が作成したコンテンツを消費するユーザーのためのものです。ユーザーごとの料金ではなく、使用量に基づき課金されます。
- **Developer** – 開発者ロールにより、ユーザーは **API** キーを作成できます。**API** キーはテナントへのプログラムのアクセスや、**Qlik DataTransfer** などの特定の **Qlik** ツールのために使用されます。
- **テナント管理者** – テナント管理者のロールは、顧客のテナントのあらゆる管理面を管理するための管理コンソールへのフルアクセスを提供します。テナント管理者は常に **1** 名以上です。
- **サービス アカウント所有者** - テナント内のロールではありませんが、各テナントには、初期設定、マルチファクタ認証、および課金を管理するサービスアカウント所有者がいます。サービスアカウント所有者は最初のテナント管理者です。

スペース

スペースとは、アプリ、データファイル、データ接続へのアクセスを開発および管理するために使用される Qlik Sense ハブ内の作業エリアのことです。以下の 3 種類のスペースがあります。

- **個人スペース** - Qlik Sense ハブ内の各ユーザーのためのプライベートな作業エリアです。
- **共有スペース** - 共同でアプリを開発したり、スペース内の他のユーザーにそうしたアプリを共有するのに使用されるエリアです。ユーザーのグループは、プライベートの開発や独自のアプリの利用のために共有スペースを使用できます。
- **管理スペース** - アプリおよびアプリデータに対する厳格なアクセス制御によって、アプリへのアクセスに使用される Qlik Sense ハブの統制されたセクションです。



スペース内のデータファイルとデータ接続 – アプリと同様に、データファイルとデータ接続は、3 種類のスペースに保存して、再利用することもできます。

共有スペースおよび管理スペースへのアクセスについて、ユーザーまたはグループのいずれかに直接割り当てることができます。個別のユーザーにアクセス権を直接割り当てのではなく、グループを使用して、ID プロバイダー内のグループメンバーを管理することがベストプラクティスと見なされています。様々なレベルのアクセス権を割り当て可能なため、ユーザーは異なるスペースへの異なるアクセス許可を持つことができます。

エンタープライズ データ容量

テナント リソース

Qlik Sense Enterprise SaaS の各テナントは、フルに拡張可能なストレージ¹を提供し、標準の Qlik Sense Enterprise サブスクリプションで、各 Qlik Sense アプリは最大 5 ギガバイトのメモリを消費できます。

¹ 公正な利用規約に従う

Qlik Sense Enterprise SaaS は、システムリソースに求められる需要に合わせて拡張し、ユーザーがインフラストラクチャを設定する必要はありません。

拡張アプリと専用の容量

特定のユースケースでは、5 GB 以上のメモリを使用するアプリが必要とされる場合があります。Qlik は、5 GB～10 GBのメモリを使用するアプリケーションのために拡張アプリ オプションを提供します。さらに大きな容量を必要とするワークロードに対しては、Qlik は専用の容量のオプションを提供します。

また、Qlik Sense Enterprise SaaS は、AWS S3 や Azure ストレージなどのエンタープライズ ストレージ ソリューションとの統合をサポートし、独自のストレージ資産にアクセスできるようにします。詳細については、『[オンプレミス データを SaaS に統合する](#)』のセクションを参照してください。

インフラストラクチャではなく、アナリティクスに重点を置く

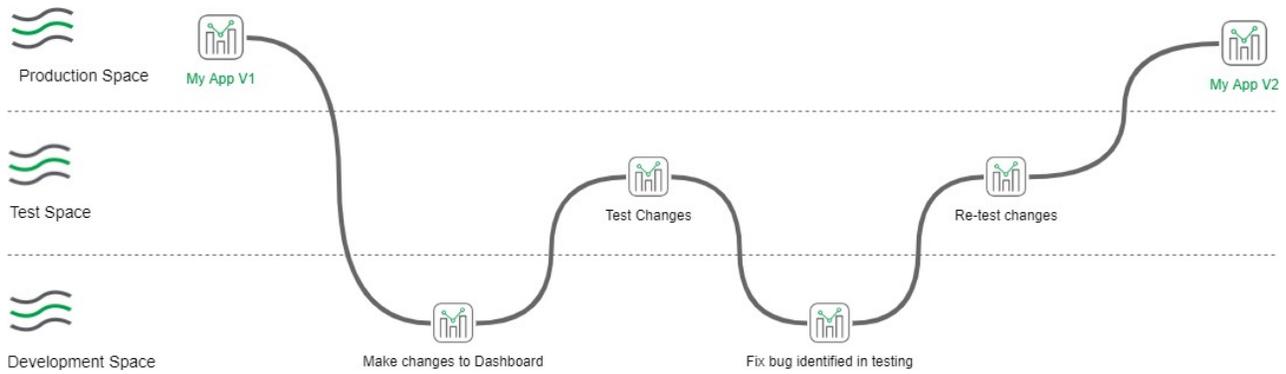
Qlik の目標の 1 つは、顧客がインフラストラクチャ管理に要しているコストや労力、およびデータからインサイトを得るために増大している時間を削減することです。オンプレミス展開を行う場合、顧客は、以下のようなビジネスの課題解決に直接関連しない複数のコストを考慮する必要があります。

- インフラストラクチャ資本と運用コスト
- オペレーティングシステム管理とソフトウェアライセンス
- インフラストラクチャ管理用スタッフの配置コスト

Qlik Sense Enterprise SaaS によって、顧客はアナリティクス環境の管理ではなく、ビジネスの課題解決に注力できます。その結果、アナリティクスの総所有コストと、アクションに繋がるアナリティクスに到達するまでの時間（Qlik が「インサイトまで数分」と呼んでいる）の両方を削減できます。

開発サーバーではなく、開発ライフサイクルを通してアプリを移動する

従来の BI 環境では、アプリは開発サーバーで開発されていました。開発が完了すると、テストサーバーに移動されたものです。テストで問題が見つかった場合、アプリケーションが本番環境に展開されるまでこのプロセスを何度も繰り返すことになり、多くのリソースと管理するためのインフラストラクチャを必要としていました。Qlik Sense Enterprise SaaS では、アプリは個別のスペースに保存されます。各スペースには独自のセキュリティ設定、データ接続、ファイルストレージがあります。顧客は、自社のソフトウェア開発のライフサイクルに合わせて必要とされる分だけ、開発、テスト、本番のスペースを作成できます。このアプローチによって、はるかに高い柔軟性、アジリティを獲得し、従来のオンプレミス設定よりもインフラストラクチャ費用を削減できます。



上記の例では、ユーザーは本番スペースでアプリを消費します。アプリへの変更が要求されると、開発スペースにコピーが作成され、アプリのテスターがレビューする準備ができるとテストスペースにそのコピーが公開されます。アプリが本番にリリースされるまで、複数のサイクルが発生する場合があります。

これらの流れをスムーズにするために、各スペースには独自のデータ接続とファイルストレージがあり、アプリが該当するライフサイクルのフェーズに適切なデータをロードできるようになります。

Qlik Cloud Services 更新時のダウンタイムをゼロにする展開

また、別の大きな労力として、オンプレミスのソフトウェアや多くの SaaS では、製品の実装、移行、アップグレードの際に顧客がテストや認証を行う必要があり、並行して SaaS 環境も構築しています。このような非常に時間がかかる作業を必要とする代わりに、Qlik では、Qlik Cloud Services インフラストラクチャに対してゼロダウンタイム展開のコンセプトを採用しています。

QlikのQlik Cloud Services向けゼロダウンタイム導入により、Qlik Cloud Servicesを顧客の使用に影響を与えずにアップグレード更新や修正を行うことができます。プラットフォーム上でのQlikの仕事は顧客に対して透明性を確保することです。Qlikのクラウドネイティブのアーキテクチャおよびゼロダウンタイム導入の仕組みに関する詳細については、[Qlik and Cloud Native](#)のセクションを参照してください。

オンプレミス データを SaaS に統合する

多くの組織が自社のシステムをクラウドへ移行している一方で、メインフレーム等オンプレミスに留まるシステムも常に存在することを、Qlik は理解しています。また、システムをパブリック SaaS 環境から直接アクセスできないプライベート環境へ移行することを選んでいる顧客も多くいます。そのため、Qlik は、オンプレミスデータソースを Qlik Sense Enterprise SaaS と統合する複数のソリューションを提供します。

Qlik DataTransfer™

Qlik DataTransfer は、Qlik Sense Enterprise SaaS に含まれている負荷の少ないユーティリティで、オンプレミスデータやローカルファイルを安全にクラウドへプッシュします。これは、Qlik Catalog™ などの完全なデータ統合ソリューションやQlik Sense Enterprise Client- Managed の完全な展開を必要とせず、オンプレミスデータに接続するファイアウォールを開きたくない顧客向けに設計されたものです。Qlik DataTransfer は、以下を提供します。

- ODBC や REST などの標準コネクタからソースデータを選ぶための接続作成・選択ダイアログ。
- 手動またはスケジュールでソースデータへの接続を実行できる「データセット」を作成し、それを Qlik Sense Enterprise SaaS に取り込み、オプションで同じ SaaS スペース内のアプリをスケジュールの一部としてリロードできる機能。
- サポートされるファイルタイプ（QVD、CSVなど）を選択したスペース内のデータファイルエリアへ移行し、オプションでトリガーされたら同じ SaaS スペース内のアプリのリロードも行う「フォルダーウォッチャー」。
- オンプレミスの事前構築された Qlik アプリをリロードし、SaaS テナントへ移行する機能。

データは、HTTPS を経由して安全に Qlik Sense Enterprise SaaS にアップロードされ、各スペースに付いているテナントストレージに暗号化して保存されます。

Qlik データ統合プラットフォーム

Qlikのデータ統合プラットフォームは、Qlik Catalog、Qlik Replicate®、データレイクやデータウェアハウス向けの Qlik Compose™などのコンポーネントとバンドルされたソリューションで、これらの製品は全て幅広いデータソースのエンドポイントから、S3 バケットなどのクラウドストレージロケーションにデータを公開する機能を提供しており、Qlik Sense Enterprise SaaS がアプリをロードするために使用することができます。Qlik Sense Enterprise SaaS で使用できるデータ統合製品には以下が含まれます。

- Qlik Replicate – ユニバーサルなデータレプリケーションとリアルタイムデータのインジェスチョン
- Qlik Catalog – アナリティクス対応データを容易に発見、準備、提供するための安全でエンタープライズ規模のデータカタログ。
- Qlik Compose – アジャイルなデータレイク作成とデータウェアハウスの自動化

Qlik のデータ統合プラットフォームに関する詳細については、次を参照してください。

<https://www.qlik.com/us/products/data-integration-products>

Qlik Sense Enterprise Client-Managed for Windows

Qlik Sense Enterprise on Windowsでは、Qlik Sense Enterprise SaaS とオンプレミスの Qlik Sense アプリを自動的に同期する機能を提供します。Qlik Sense Enterprise SaaS に配信するアプリをタグ付けするルールを使用できるため、配信する必要があるのはアプリのサブセットのみです。この機能により、顧客は、いくつかのアプリを Qlik Sense Enterprise SaaS に展開し、オンプレミスやプライベートクラウド上にその他のアプリを保持できます。

QlikView Publisher

QlikView は、QlikView Publisher を通じて QlikView アプリを Qlik Sense Enterprise SaaS に公開する機能を提供します。この機能により、QlikView の顧客は、インフラストラクチャのコストを大幅に削減しながら、同時にオンプレミスで QlikView アプリを引き続きリロードできます。

グローバル対応とローカライゼーション

Qlik Sense Enterprise SaaS は Unicode に対応した製品で、あらゆる言語で保存されたデータと互換性があります。ユーザーインターフェースおよびサポート文書は、英語、ドイツ語、スペイン語、フランス語、イタリア語、日本語、オランダ語、ポルトガル語（ブラジル）、ロシア語、スウェーデン語、中国語（簡体字）、ポーランド語、トルコ語、韓国語、中国語（繁体字）で利用可能です。

信頼性

オープンで透明性が高い

Qlik Sense Enterprise SaaS は、99.9% のアップタイム コミットメントを提供します。Qlik は、アップタイムとインシデントのデータを公開するため、顧客や見込み顧客は、Qlik Sense Enterprise SaaS を実行している Qlik Cloud Services プラットフォームの現在の状況や信頼性を把握できます。この情報は、以下で確認できます。

<https://status.qlikcloud.com/>.

顧客は、プラットフォームの全体的なアップタイムを確認するだけでなく、発生した特定の問題を調べて、その影響の詳細を確認することができます。

グローバルな存在感

世界の複数の地域をサポート

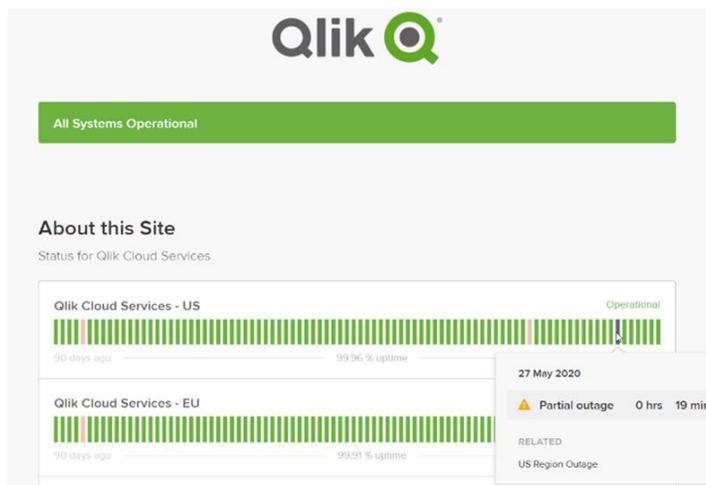
Qlik Sense Enterprise SaaS テナントが作成されると、顧客はテナントがベースを置く地域を選択します（米国、アイルランド、またはオーストラリア）。そのため、顧客は自社のビジネス要件に合う地域を選択できます。Qlik は顧客からのフィードバックを継続的にレビューし、需要に応じてより多くの地域が利用できるように検討します。

適応可能な高可用性インフラストラクチャ

Qlik Sense Enterprise SaaS プラットフォームは、世界有数のクラウド インフラストラクチャ ベンダーが提供する、成熟した高可用性と耐障害性を備えたインフラストラクチャ スタック上で実行され、複数の地域の複数のデータセンターに展開されています。さらに、このプラットフォームは、Kubernetes 上で実行されているマイクロサービスベースのアーキテクチャを用いて構築されており、スケーラビリティと耐障害性を中心にして一から設計されています。これにより、プラットフォームは、あらゆる変更やパッチに即座に対応し、プラットフォームの潜在的なダウンタイムを最小限に抑えることができます。

災害復旧 / バックアップとリカバリー

Qlik のサイト リライアビリティ エンジニアリング (SRE) のチームは、定期的に災害復旧テストを実施しています。これらのテストの一部として、チームは全く新しい Qlik Cloud Services のリージョンを構築しています。災害復旧テストは、新しいリージョンが立ち上がり、レプリケートされたデータ



が 100% 回復し、テナントが前回のバックアップ/レプリケーション期間から完全に利用可能になって初めて成功と見なされます。

顧客のテナント設定およびメタデータに関連した Qlik Cloud Services のデータやプラットフォームの情報は、セカンダリ リージョンへのレプリケーションが可能な形で保存されています。顧客のデータファイルは毎日バックアップされます。

サイト リライアビリティ エンジニアリング

Qlik の SRE チームは、Qlik Sense Enterprise SaaS インフラストラクチャの実行に責任を負いません。QlikSense Enterprise SaaS プラットフォームは主要なクラウドベンダー上で動作します。

スポットライト – Qlik のサイト リライアビリティ エンジニアリングのプロセス

Google のサービス リライアビリティの階層に基づき、Qlik の SRE チームは以下の領域に重点を置いています。

監視 - SRE チームは、本番環境に配信された全てのサービスが、そのパフォーマンス状況を Qlik に伝えることができるようにし、問題が発生した場合には、SRE チームがその問題を認識できるようにします。

インシデント対応 - SRE チームは問題に対する適切な対応計画を準備します。SRE チームが利用できる様々なオプションは、サービス別のプレイブックに記載されており、最適ではない方法で運用されているサービスに対処するための最良の方法を示しています。

事後分析と根本原因分析 - SRE チームは、本番環境でサービスが低下しているというアラートを受け取ると、根本的な問題をできるだけ速やかに解決する必要があります。事後分析とは、インシデント、そのインパクト、問題を最小化または解決するために行ったアクション、根本原因、インシデントの再発を防ぐためのフォローアップアクションを文書化した記録です。多くの場合、事後分析プロセスの成果の1つは、機能的な問題が再発しないように、継続的な配信パイプラインに自動化されたテストを追加することです。

容量計画 - SRE チームは、新サービスの継続的な設計に参加し、新機能/変更が既存サービスに与えるインパクトを共有します。以下が含まれます。

- サービスを拡張して、増加するトラフィックの負荷に対応する方法
- サービスを縮小して、容量の削減をシームレスに提供する方法
- インフラストラクチャの最適な規模とパフォーマンス特性の特定
- 自動スケーリングを必要とするサービスの特定

開発 - SRE チームは継続的にプラットフォームのパフォーマンスとスケーラビリティに関して技術革新を行っています。例えば、

- 測定ツールと監視ツールの継続的な機能強化
- 自動機能の継続的な改良と拡張 など

測定 - SRE チームは、環境のパフォーマンスを継続的に監視するために、内部指標（サービスレベルの指標やサービスレベルの目標など）を使用しています。

セキュリティおよびガバナンス モデル

認証と権限付与

ID およびアクセスの管理

ID プロバイダー (IDP) が、組織のために認証や認可の情報を管理する標準的な方法になっています。Qlik は、Open ID Connect プロトコル (OIDC) に対応することで、様々な ID プロバイダーとの統合をサポートします。

プロトコルベース - OpenID Connect (OIDC) は、シングルサインオンやインターネット上の ID 提供に対して事実上の業界標準となりました。OIDC はクラウド上で動作するように設計されており、ユーザー認証およびマシン認証の両方に対するソリューションを提供します。

証明書の管理 – Qlik で ID プロバイダーを使用する場合、Qlik は顧客のログイン名とパスワードを知りません。ログインプロセスは顧客の ID プロバイダーによって管理され、顧客はどの情報を Qlik Sense Enterprise SaaS に提供するかを決めます。この情報は、個人を特定しないショートネームやコードにできます。また、Qlik Sense Enterprise SaaS では、アクセス許可を制御するために ID プロバイダーグループを活用できます。

アクセスの制御 – 顧客の ID プロバイダーにおけるユーザーのアクセス権が削除または変更されると、ユーザーは自動的に Qlik Sense Enterprise SaaS にアクセスできないようになるか、該当する変更が自動的に適用されます。

OIDC の対応を通じて、Qlik Sense Enterprise SaaS は、Okta、Auth0、Azure AD、ADFS などの主要な ID プロバイダーの全てをサポートします。

Qlik アカウント

外部の利用可能な ID プロバイダーを持っていない顧客や、管理の必要がない製品内ソリューションを必要とする顧客のために、Qlik は、追加料金なしで、Qlik Sense Enterprise SaaS の一部として、利用可能なバンドルされた ID プロバイダーオプションとして Qlik アカウントを提供します。これにより、顧客は、Qlik アカウント登録用にメールでユーザーを招待し、そのアカウントを使用して Qlik Sense Enterprise SaaS にログインできるようになります。

Qlik アカウントは、顧客に対しては実装を簡素化しますが、Qlik Sense Enterprise SaaS 用に別々のユーザー名とパスワードが必要となります。顧客が希望する場合、Qlik アカウントから独自の ID プロバイダーへ変更することが可能です。

マルチファクタ認証

Qlik Sense Enterprise SaaS は、Qlik アカウントを用いて、または顧客の ID ソリューションから、テナント管理者のマルチファクタ認証をサポートします。また、Qlik のマルチファクタ認証は、Qlik アカウントや顧客の IDP を用いて、全てのユーザーに対して設定することもできます。

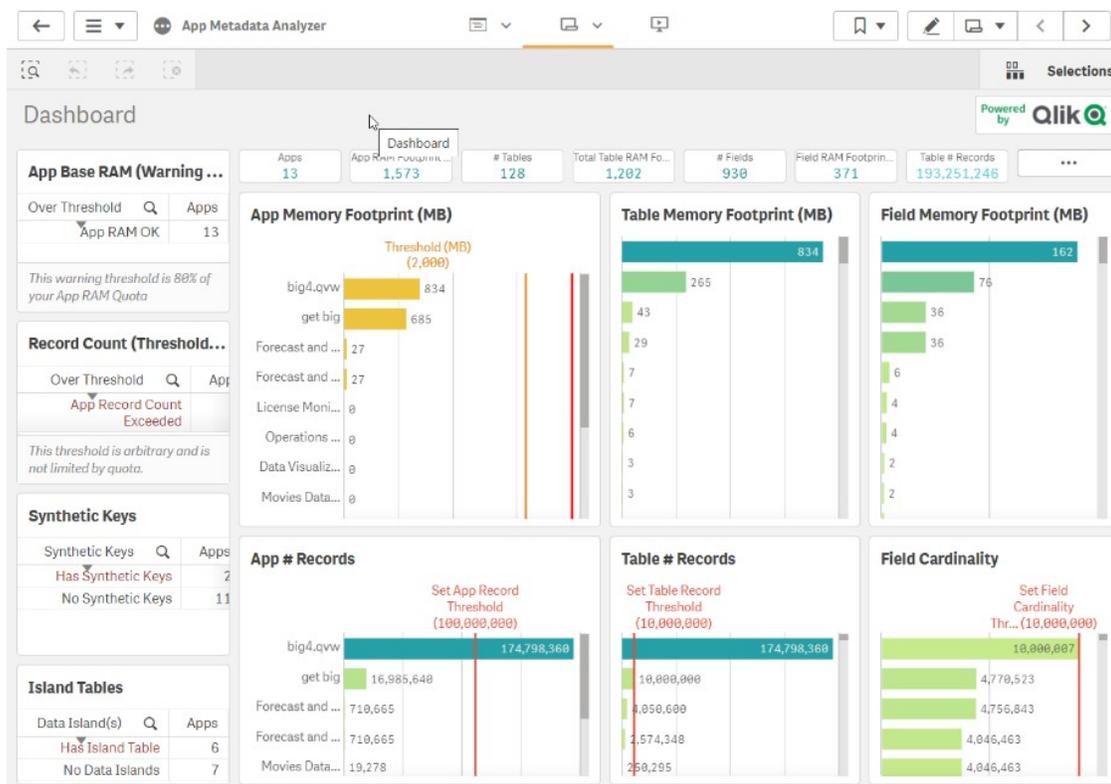
Section Access

Section Access は、アプリケーションのセキュリティを制御するために使用されます。データモデルを使用してデータレベルの認証を定義し、行および列のレベルでデータへのアクセスを制限できるようにします。詳細については、ヘルプ文書の [Section Access](#) を参照してください。

ガバナンス

テナントガバナンスを理解する

Qlik は、**App Analyzer for Qlik SaaS** を提供し、顧客の QlikSense Enterprise SaaS テナントにガバナンス情報をもたらします。このアプリでは、メモリの使用状況、カーディナリティ、データモデルなど、アプリのキーパフォーマンス特性を確認できます。



テナントのアクティビティを監視する

Qlik Sense Enterprise SaaS 管理コンソールには、Qlik Sense Enterprise SaaS テナントのガバナンスによって支援する複数のツールが含まれています。イベントビューワーでは、ユーザーやシステムがどのようなアクティビティを行ったかが表示され、ユーザーログイン、アプリの作成、アプリのエクスポート、アプリのリロード、アプリの削除などの主なアクティビティに対する監査証跡を提供します。Qlik Sense Enterprise SaaS テナント内では、アクティビティは API を介して顧客にも利用できるようになります。このアクティビティを顧客のセキュリティ情報やイベント管理ソリューションにダウンロードすることができます。

既存のガバナンス ソリューションへの統合

Qlik Sense Enterprise SaaS 管理コンソールを通じた監査証跡を文書化するだけでなく、Qlik Sense Enterprise SaaS は、テナントアクティビティを表示できる（修正や削除は不可）アプリケーション プログラマブル インターフェース（API）を提供します。顧客は、Qlik Sense Enterprise SaaS テナントの監査証跡を既存のガバナンスシステムに統合したり、API を介してQlik Sense Enterprise SaaS 内に新しい監査アプリケーションを構築することもできます。詳細については、ヘルプ文書の [Qlik Sense audit service](#) を参照してください。

Qlik Sense アプリケーションをアプリ評価サービスによって、統制・改良する

アプリ評価サービスによって、ユーザーはパフォーマンスの観点から、Qlik Sense Enterprise SaaS インスタンスを管理できます。このサービスは、アプリケーションサイズの増加やアプリケーションを開くのに要する時間の長さなど、Qlik Sense Enterprise SaaS アプリケーションの主要な指標をキャプチャします。さらに、考えられる変更の理由をフィードバックすることで、顧客がそうした問題に対処できるようになります。

The screenshot shows a 'Performance evaluation completed with warnings' dialog box. It contains a table of metrics and a list of warnings.

Evaluation details	
Results	Breakdown
Time to open	3.5 s
Peak size	453 MB
Data model size	314 MB
Total rows in app	85 rows
Public sheets in app	4 sheets
Public objects in app	35 objects

Warnings:

- Performance evaluation completed with warnings
- The calculation condition was unfulfilled
- This app utilizes section access, which means different users will see different results

Buttons: Help, Download log, Done

標準ベースのセキュリティおよびコンプライアンス

コンプライアンスとプライバシー

ワークロードを SaaS プラットフォームに移行する際、データが安全に保護されていること、サービスプロバイダーがセキュリティ管理のためにオープンで監査されたプロセスに従っていることを確認することが重要です。Qlik Sense Enterprise SaaS は、安全なプラットフォームとして一から構築されており、Qlik は外部のパーティーと協力して、適用される業界標準および/またはベストプラクティスの管理が確実に実施されるようにしています。

SOC 2 – Type 2

Qlik は、SOC 2 Type 2 に準拠しています。SOC 2 は AICPA トラストサービスの原則に基づいた独立系の会計事務所による厳正な審査であり、Qlik の内部統制の設計および運用の効果性の評価を提供します。

SOC 3

SOC 2 をベースに、Qlik は、SOC 3 アセスメントを完了しています。このアセスメントは一般的なユースレポートで、AICPA トラストサービスの原則に対する Qlik のコンプライアンス遵守を証明するものです。

ISO 27001

Qlik は ISO 27001 認証を取得し、情報セキュリティマネジメントシステム (ISMS) 実施の国際標準に合致しています。ISMS は、組織のリスク管理プロセスに関わる法務、物理的および技術的な管理を含む方針および手続きのフレームワークです。

Qlik の外部認証およびコンプライアンスに関する最新の情報については、[Trust ページ](#) にアクセスしてください。

データ主権

顧客のデータは、バックアップ/回復および災害復旧システム内のいかなるデータも含み、テナントを作成する際に顧客が登録する Qlik Sense Enterprise SaaS Services リージョン内で保持されます。リージョンからは何も移行されません。バックアップのコピーは同じリージョン内のセカンダリプロバイダーに保存されます。

データプライバシーと GDPR

Qlik は、包括的な社内プロセスを構築して、適用されるプライバシー (GDPR を含む) 要件を確実に遵守するようにします。Qlik の顧客およびパートナーのデータ保護に全力で取り組み、オー

オープンかつ透明性の高い方法でコミュニケーションを取っています。詳細については、[GDPRページ](#)にアクセスしてください。

データの分離、保管、移行

Qlik Sense Enterprise SaaS は、マルチテナントプラットフォームです。マルチテナントプラットフォームとして、各顧客のデータを他の顧客から分離することは極めて重要です。各テナントには、Qlik がその顧客のために管理する、一意に生成された暗号化キーのセットがあります。各テナントのキーは、Qlik がサービスを確保するために使用しているキーからサービスコミュニケーションまで分離されます。以下の暗号化は、Qlik Sense Enterprise SaaS プラットフォーム内で使用されません。

- 移行中 - TLS 1.2 暗号化
- 保存時 - AES-256 暗号化
- プラットフォーム内 – (顧客の指定 IDP による認証時に) 署名済みの JSON ウェブトークン (JWT) を使用して、整合性、信頼性、否認防止を確保する

テナントへのユーザーのアクセス権は、ID プロバイダーを通して顧客によって付与され、許可は顧客の管理ポータルを介して制御されます。

コンテンツの削除

「コンテンツ」とは、Qlik Sense Enterprise SaaS テナント内の顧客提供のデータや他の情報のことです。テナントに常駐するコンテンツの作成や削除は、顧客によって制御されます。顧客は、コンテンツをいつでも削除できます。バックアップは Qlik 社内のデータ保持方針に従って、一定期間が経過した後に削除されます。

顧客提供のデータは、Qlik Cloud Services によって使用されている Kubernetes ストレージソリューションの暗号化された QVD または QVF ファイルとして保存されます。顧客が Qlik Cloud Services のアプリを削除すると、このサービスが Kubernetes ストレージソリューションのファイルを削除します。QCS は Kubernetes ストレージソリューションのファイルシステムに依存し、ブロックストレージで削除を実行します。

Qlik は、バックアップのために Amazon AWS や Google を活用して、コンテンツが古くなって対応するファイルシステムから削除されるまでの 30 日間、コンテンツのコピーを保持します。QCS は Remote Sync や Amazon Simple Storage Service (S3) とともに Google Cloud Platform バックアップを活用して、コンテンツをバックアップ目的でコピーします。

Qlik Sense Enterprise SaaS プラットフォームセキュリティ

24 時間 365 日のセキュリティ監視

Qlik Cloud Services は、Qlik の SRE チームによって監視されています。全てのセキュリティログは一元的に SRE チームによって処理され、インシデントは全て Qlik のインシデント対応プログラムに従って対処されます。

セキュリティ ベストプラクティス

強力で安全な基盤を確保するために、Qlik はセキュリティの責任を業界トップのクラウドインフラストラクチャ ベンダーや評価の高いパートナーと共有します。これらのクラウド コンピューティング サービスは社内目的で Qlik に使用され、同様に自社のクラウド展開のために Qlik のクライアントにも使用されています。詳細な情報については、『コンプライアンスとプライバシー』のセクションを参照してください。

Qlik Cloud Services は、安全な物理的アクセス、冗長な（耐障害性）インフラストラクチャ、スケーラビリティのためにクラウド インフラストラクチャに依存しています。当社のクラウドパートナーのネットワーク設計と監視が、分散型サービス妨害 (DDoS)、中間者 (MITM)、IP なりすまし、ポート スキャンニング、パケット スニフィングなど、共通のネットワークセキュリティの問題を軽減します。

セキュリティに対する Qlik のアプローチはクラウドパートナーのセキュリティレイヤーに構築されています。Qlik は、侵入検知やプロセス監視などのネットワークおよびエンドポイントの監視管理を実施しています。ウェブレイヤーでは、Qlik はウェブ アプリケーション ファイアウォールを活用して、攻撃を検知して防ぎます。QCS へのアクセスはマルチファクタ認証およびロールベースのアクセス制御を利用しています。

Qlik はネットワークおよびエンドポイントの両レベルで、脆弱性の定期的なテストを行います。脆弱性の改善は、Qlik Cloud Services の継続的な展開手法に組み込まれています。

脆弱性管理へのアプローチ

Qlik のソフトウェア開発プロセスは、セキュア バイ デザインのアプローチをソフトウェア デリバリーに組み込んでいます。そのプロセスに大きく寄与しているのは、脆弱性管理に対する当社のアプローチです。Qlik は、以下を含む最新の脆弱性管理改善方針を維持しています。

- 業界標準の共通脆弱性評価システム (CVSS) に基づく脆弱性の深刻度評価を活用して、セキュリティ問題の深刻度を判断する。（1～10のスコアで、10が最も深刻である）
- 修復時間を含む、既知の脆弱性ととも、ソフトウェアの開発時およびリリース時に特定された脆弱性に関連した方針

- 修復時間を含む、Qlik Sense Enterprise SaaS 更新時に特定された脆弱性に関連した方針
- 脆弱性に対する顧客への通知方針
- サードパーティソフトウェアのセキュリティおよび改善の方針
- 脅威モデリング、動的および静的コードスキャン、侵入テスト、サードパーティソフトウェアのコンポーネントを対象とする、ツールとプロセス。

セキュア バイ デザイン – Qlik がセキュアなプラットフォームを構築する仕組み

Qlik は、Qlik Security Model を遵守することによって、ソフトウェア開発のライフサイクルに、セキュリティを組み込んでいます。Qlik Security Model は、Qlik Software Security Office によって開発されており、全てのソフトウェア開発がセキュリティに重点を置いて行われるようにする社内プロセスです。このモデルは、既存の有名でセキュアなソフトウェア開発プロセスからベストプラクティスを抽出し、Qlik のニーズに合わせて調整したものです。このモデルには、ソフトウェア開発のライフサイクル全体をカバーする5つのフェーズがあります。

分析と設計: プロセスのこのフェーズには、システムおよび機能レベルの脅威モデリングが含まれます。製品が設計されると、チームは各機能を検討し、この機能で起こり得る脅威を特定します。

各脅威を軽減するために、対応策が実施されます。

開発: Qlik は業界トップの静的コード分析ツールを利用して、新機能に特有のコードの問題やエンドツーエンドのコードの問題を特定します。展開後、静的コード分析ツールは定期的にレポートを実行します。自動化されたレポートは手動のセキュリティ テストプロセスで補完されます。手動の検証でセキュリティの問題が存在することを確認すると、展開に先立って対処されます。

アセンブル: セキュリティの観点からテストケースが作成され、開発プロセスで実行されます。テストには、システムレベル、機能レベル、ペネトレーションレベル、ファジングが含まれます。テストケースは、新製品リリースをエンドツーエンドで検討して、新製品内のセキュリティ問題を特定します。製品内の新機能を含むコードに対して具体的なテストを実施します。独立系のサードパーティセキュリティ企業が、ペネトレーションテストを通じて、製品を定期的に監査しています。

展開: Software Security Office は、脆弱性管理プロセスを通して展開フェーズに関わっています。外部のセキュリティ企業、顧客、パートナーと連携することにより、展開されるコードの脆弱性を特定し、チームは報告された脆弱性を評価して、適切なアクションを決定します。

進化: セキュリティモデルの一部であるアクティビティによる全ての結果は、Software Security Office によってレビューされます。改善すべき領域を特定し、それに従ってモデルを調整することを目標としています。

アーキテクチャ

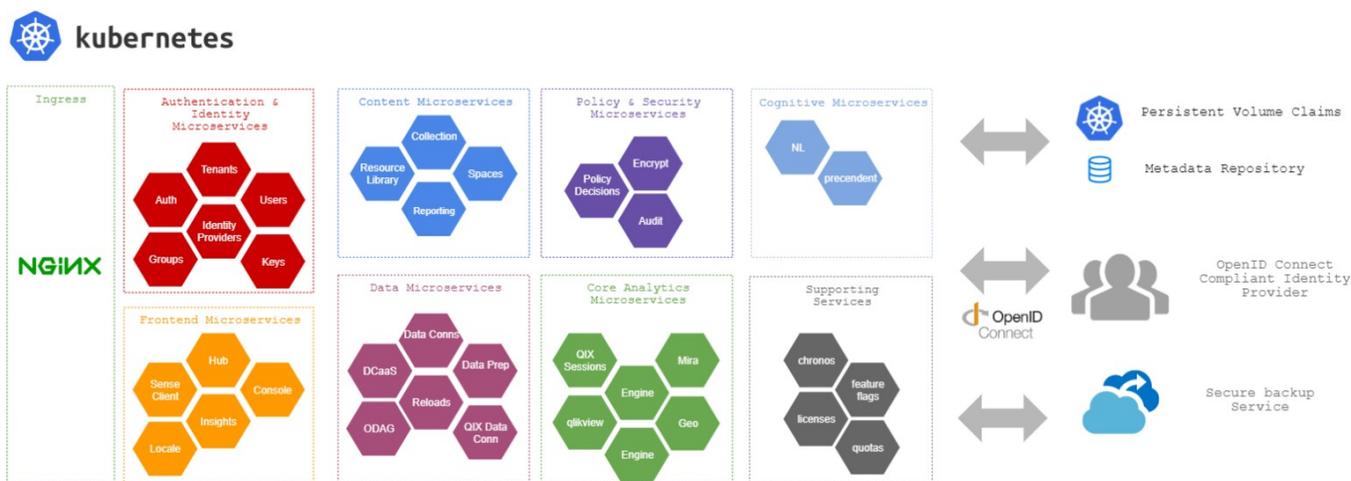
Qlikのクラウドネイティブ プラットフォームと Kubernetes スタック

高度にスケーラブルで、高可用性なクラウドプラットフォームとサービスを設計するために、Qlik は単に Windows 製品をシフトさせて、クラウドに移行するということではできませんでした。Qlik Cloud Services と Qlik Sense Enterprise SaaS はマイクロサービス アーキテクチャに基づいており、プラットフォームの様々なコンポーネントは、クラウドネイティブなソリューションを構築するために一から作り上げられています。Qlik のコンテナベースのマイクロサービス アーキテクチャによって、各コンポーネントは、従来のオンプレミスソリューションのようにサーバーを追加するのではなく、必要に応じて拡張できます。

このプラットフォームの主な特長は、ワークロードの増加に合わせて水平方向に拡張し、ワークロードの減少に合わせて縮小できることで、これは、プラットフォーム上のユーザー数にかかわらず、顧客に安定したパフォーマンスを提供するために Qlik Sense Enterprise SaaS で使用されています。リソースの監視と調整を自動化することによって、プラットフォームの全てのコンポーネントが、適切なリソースを適切なタイミングで利用できるようになります。

クラウドネイティブアプリのもう一つの重要な点は、ゼロ ダウンタイム展開の概念です。Qlik Sense Enterprise SaaS は、ゼロ ダウンタイム展開をサポートするために設計されています。Qlik は、プラットフォームの主要コンポーネントを停止することなく、アップグレードできます。

Qlik は、Docker と Kubernetes を活用して、プラットフォームのスケーリングの依存関係を管理します。Kubernetes 展開の参考図は、以下の通りです。



Qlik Sense Enterprise SaaS で使用されている主要な技術は、以下の通りです。

Kubernetes – Kubernetes は、コンテナの展開、スケーリング、管理を自動化します。詳細については、 <https://kubernetes.io/> を参照してください。

Docker – Docker は、Qlik マイクロサービスが動作するコンテナを提供します。コンテナは標準化されたソフトウェアの単位であり、開発者はコードを環境から分離でき、「自分のマシンで動作する」という頭痛の種を解決します。 <https://www.docker.com/why-docker> を参照してください。

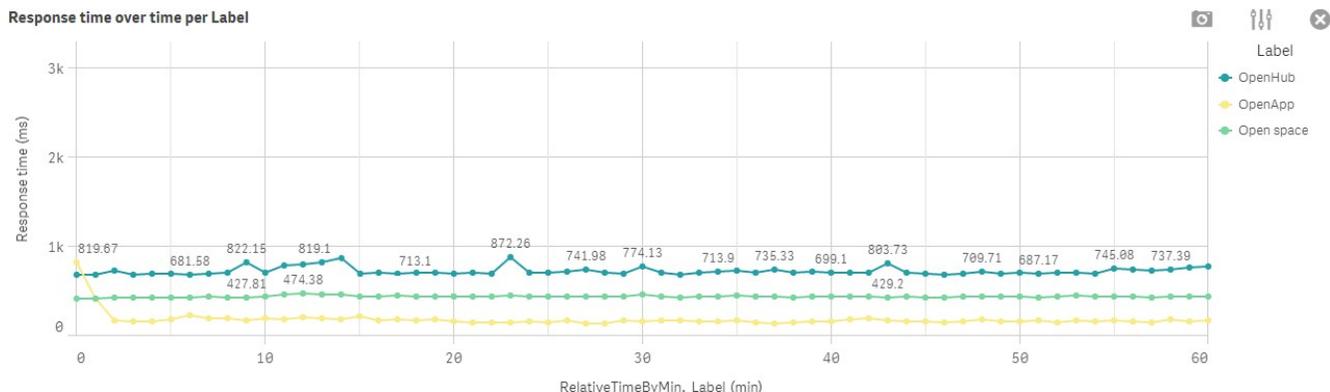
NGINX Ingress Controller – NGINX Ingress Controller はウェブ インターフェースと Qlik Sense Enterprise SaaS テナントの内部ロードバランシングを提供します。NGINX は、HTTP およびリバー ス プロキシ サーバー、ロードバランシング サーバー、ジェネリック TCP/UDP プロキシ サーバーです。 <https://www.nginx.com/products/nginx/kubernetes-ingress-controller/> を参照してください。

MongoDB – MongoDB は、クロスプラットフォームのドキュメント指向のデータベースです。Qlik Sense Enterprise SaaS 内のメタデータレポジトリとして使用されます。
<https://www.mongodb.com/>

大規模で予測可能なパフォーマンス

最高のエンドユーザーエクスペリエンスを実現するために、Qlik は継続して、個々のテナントのパフォーマンスおよびスケーラビリティの匿名化されたサンプルを採取します。複数の異なる構成をテストして、テナントが想定されるユースケースや負荷に必ず対処できるようにします。テストされたパラメータの一部は以下の通りです。

- ユーザー増加（つまり、時間単位でテナントにアクセスするユーザー数）
- ユーザータイプ - コンシューマーや作成者など
- 同時ユーザー数
- アプリの数とサイズ
- ドキュメント リロードの数、頻度、サイズ



この例では、1時間あたり10,000人のユーザーが、平均160万行のデータ量を持つ100種類のアプリ（利用可能な1600種類から）にアクセスするテストを行いました。上記のように、QlikSense Hubを開く、スペースを開く、個々のアプリを開くなどのレスポンスタイムは、全てのユーザーで1秒以下でした。

柔軟で拡張可能

Qlik Sense Enterprise SaaSは、顧客のニーズに合わせて柔軟に拡張できるように設計されています。ハイブリッド展開を考えている顧客が利用できる、複数の展開パターンがあります。これらの機能はQlik Sense Hubによって実現され、顧客は特定のデータをオンプレミスで保持するという法的要件に対応できます。

例えば、主にオンプレミスのデータソースを持つ顧客は、オンプレミスでQlikViewとQlik Senseのデータロード操作を行い、ユーザーのデータビジュアライゼーションの全てをQlik Sense Enterprise SaaSに移行するという選択が可能です。

また、ほとんどの業務をクラウドに移行しながらも、オンプレミス展開でバッチのレポート作成業務を行い、RやPython、その他サードパーティ製品などを用いた高度なアナリティクスソリューションと連携するという別のユースケースもあります。

Qlikは、顧客のビジネス要件に応じたSaaS展開についてアドバイスや支援を行うことができます。

Qlik Sense Enterprise SaaSの連携と拡張

統合のアプローチ

Qlik Sense Enterprise SaaSは、Qlikにホストされているアプリを顧客自身の環境と統合す

る、数多くのオプションをサポートしています。利用可能なオプションに関する詳細については、<https://qlik.dev/basics/authentication-options> を参照してください。

API キー

API キーは Qlik Sense Enterprise テナントのユーザーを示すトークンです。誰もが、API キーを使用してプログラマ的にプラットフォームとやり取りできます。トークンには、ユーザーのコンテキストが含まれ、ユーザーがテナント内に持っているアクセス制御の権限が尊重されます。API キーのユースケースとしては、`qlik-cli`（コマンドライン インターフェース）、スクリプトによるリクエスト、マシン ツー マシンのバックエンド ソリューションなどがあります。

インタラクティブ ログイン

ウェブアプリでユーザーを認証するには、複数の REST エンドポイントを使用して、ブラウザにアクティブな Qlik Sense SaaS セッションがあるかどうかを評価します。続いて、テナントのサインイン URL にリダイレクトします。

Qlik Sense オブジェクトやデータを組み込んでいるウェブアプリは、マッシュアップとしても知られていますが、テナントの設定でウェブ統合 ID を必要とします。ウェブ統合 ID は、組み込まれた Qlik Sense Enterprise SaaS コンテンツのクロス-オリジン リソース共有 (CORS) を処理するための Qlik Sense Enterprise SaaS のセキュリティ機能です。

さらに、コンテンツが組み込まれたウェブアプリでは、Qlik 連想エンジンと Qlik Sense Enterprise SaaS API を参照する URI とで供給されるクロスサイト リクエスト フォージェリ (CSRF) トークンを必要とします。

JSON ウェブ トークン (JWT)

JSON ウェブ トークンは、デジタル的に署名されたもので、一般的に「JWT」と言われています。JWT は、ソフトウェア アプリケーション間の情報を送信するための標準で、パブリック/プライベートのキーペアを用いて検証され、信頼された JSON オブジェクトの形をしています。JWT には、認証と情報交換という 2 つの主要なユースケースがあります。Qlik Sense Enterprise SaaS は、認証フェーズにおいて、外部の ID プロバイダーから JWT を読み込みます。Qlik Sense Enterprise SaaS は、セッション中に利用するために、認証後に内部 JWT を作成します。

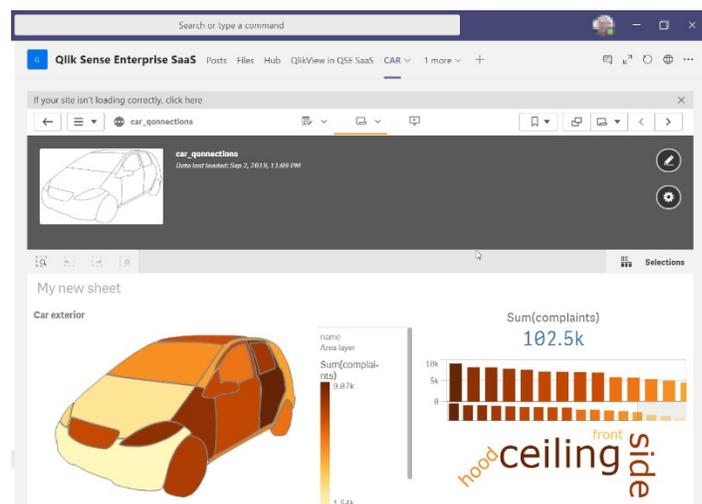
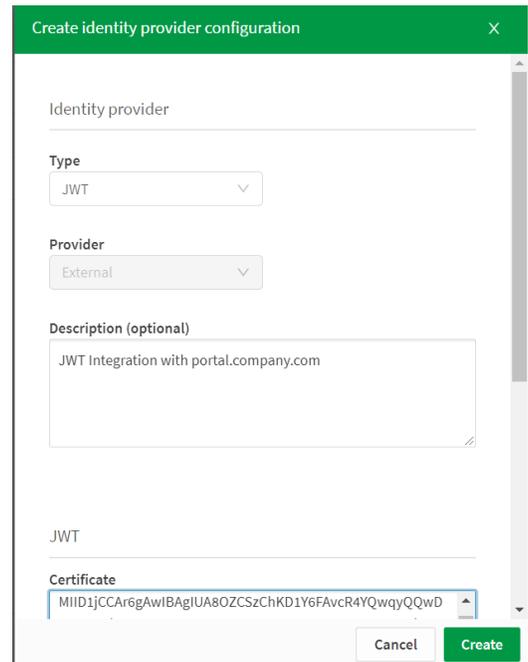
Qlik Sense Enterprise SaaS の外部JWT 認証オプションにより、Qlikテナントへのインタラクティブなサインインをパス通過させることによって、クライアントアプリケーションは直接カスタムJWT を送信できます。ユーザーはQlik Sense Enterprise SaaS にアクセスするために認証されます。

JWT 機能により、顧客のアプリケーションと Qlik Sense Enterprise SaaS 間のシームレスな連携を提供できます。

JWTを使って Qlik Sense Enterprise SaaS に接続するアプリケーションには、全ての統合と同様にウェブ統合 ID とクロスサイト リクエスト フォージェリの防止が必要です。

組み込み型

Qlik Sense Enterprise SaaS アプリは、他のウェブポータル内や、サードパーティ クライアントなどのツール内への組み込みをサポートします。詳細な作成方法については、ヘルプサイトにある [create mashups and web apps](#) を参照してください。また、Qlik は、顧客が Qlik アプリやビジュアライゼーションをマッシュアップやウェブアプリに組み込む際に使用できる、事前作成された例も提供しています。これらの例は、こちらの [GitHub](#) で利用できます。
<https://github.com/qlik-oss/web-integration-examples>



API ガバナンスポリシー

Qlik の API 戦略は、API ガバナンスポリシーに従って、Qlik の API ポートフォリオへの追加、変更、非推奨を伝えます。Qlik R&D は、API ガイドラインに従って、API の安定性を示し、仕様書への参照を標準化し（ReST API に対する OpenAPI 等）、API 非推奨を処理します。

API 戦略の主要な目的は、プラットフォームを拡張するのに Qlik API に依存している顧客やパートナーにオープンで透明性の高いガイダンスを提供することです。

Qlik R&D は、特許出願中の API ガバナンス フレームワークを開発しています。このフレームワークは、開発チームが行ったコミットから情報を収集し、API を発見・維持できるようにするものです。これにより、チームは継続的にプラットフォームを強化でき、社外の API 利用者が最高品質のコンポーネントにアクセスできるようになります。Qlik の API ガバナンスポリシーに関する詳細については、<https://qlik.dev/basics/api-governance> にアクセスしてください。

Qlik オープンソース

API のガバナンスに加え、Qlik R&D は、Qlik オープンソース (<https://github.com/qlik-oss>) を通じて Qlik Sense Enterprise SaaS の開発、テスト、統合を迅速化するライブラリを提供します。これらのファーストパーティ ライブラリの多くは、以下のようにプラットフォーム自体で使用されています。

- **Nebula.js** - JavaScript ライブラリ、ビジュアライゼーション、CLI のコレクション。開発者が Qlik 連想エンジン上にビジュアライゼーション構築・統合できるようにします。
- **Enigma.js** と **Enigma.go** - Qlik 連想エンジンを利用するための JavaScript および go lang ライブラリ。
- **Gopherciser** - Qlik Sense Enterprise SaaS 用の負荷試験ツール。

Qlik オープンソースの詳細については、<https://github.com/qlik-oss/open-source> を参照してください。

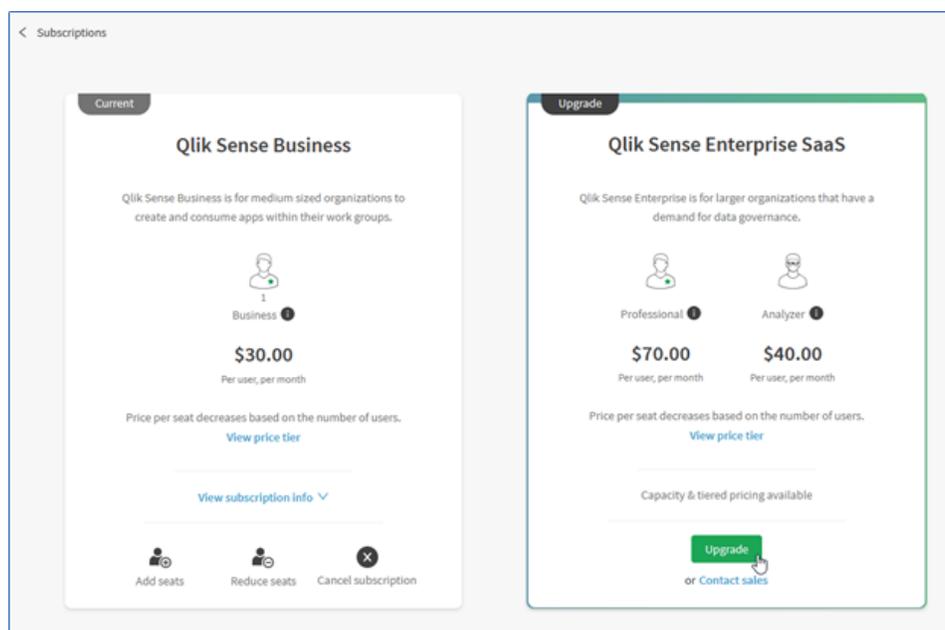
ツールとリソース

開発者向けポータル (<https://qlik.dev/>) – このポータルは、開発者が、Qlik Sense Enterprise SaaS を含む Qlik 製品を使って開発するために必要な情報（開発者向けドキュメント、API リファレンス、チュートリアルなど）を見つけるための一元化された場所です。

Qlik-cli - Qlik Sense Enterprise SaaS の管理アクティビティを自動化するコマンドライン インターフェースです。 <https://qlik.dev/libraries-and-tools/qlik-cli> から利用できます。

Qlik Sense Business から Qlik Sense Enterprise SaaS へのアップグレード

Qlik Sense Business の顧客が Qlik Sense Enterprise SaaS へアップグレードして、追加の機能やデータ容量を希望する場合、サブスクリプションをアップグレードできます。Qlik では、顧客が新規テナントを作成せずに、Qlik Sense Business トライアルや Qlik Sense Business サブスクリプションを Qlik Sense Enterprise SaaS サブスクリプションにアップグレードできるため、情報やデータが保持されます。



まとめ

Qlik Sense Enterprise SaaS は、顧客が安全に分析ワークロードをクラウドへ移行できるプラットフォームを提供するために作られたものです。Qlik Sense Enterprise SaaS は、クラウドネイティブ技術に基づいて構築されており、最新の企業のワークロードに合わせて自動的に拡張できるように設計されており、Qlik Sense、QlikView、その他 BI アプリを単一のハブに統合できるプラットフォームを顧客に提供します。

世界的な存在感を示し、セキュリティと可用性を重視した Qlik Sense Enterprise SaaS により、世界中の顧客に安全で安心なプラットフォームを提供しています。テナントのホスト先を選ぶことができるため、顧客は、自社の所在地の近くやビジネス要件を満たす地域にデータを置くことができます。

Qlik は、顧客がアナリティクスやビジュアライゼーションを自社のポータルやシステムに統合して組み込みたいと考えていることが多いと理解しています。そのため、Qlik では、顧客がより簡単に行えるように、統合アプローチやサポートされているオープンソースのライブラリやツールを提供し、さらに投資を続けています。包括的な API をはじめ、リソースやサンプルを提供する Qlik の開発者向けポータルによって、Qlik は、Qlik Sense Enterprise SaaS が顧客のソリューションの一部となるよう全力を尽くして支援します。

既存の Qlik Sense Enterprise Client-Managed の顧客に対しては、Qlik Sense Enterprise SaaS によって、SaaS への移行を促進できます。顧客は、アプリのリロードをオンプレミスで継続するか、一部のアプリを Qlik Sense Enterprise SaaS に移行するか、または Qlik データ統合ツールを使用してオンプレミスのデータソースにアクセスしながら、消費をクラウドに移行するかを選択できます。統合された ID プロバイダーと、柔軟な展開・サブスクリプションのオプションによって、管理が容易で、移行期のコストを最小限に抑えることができます。



Qlikについて

Qlikのビジョンは、誰もがデータとアナリティクスを使って意思決定を改善し、最も困難な問題を解決できる、データリテラシーの高い世界です。プライベートSaaS企業であるQlikは、データ、インサイトおよびアクションの間のギャップを解消するために、エンドツーエンドでリアルタイムなデータ統合およびアナリティクスのクラウドプラットフォームを提供しています。データをアクティブインテリジェンスに変換することで、企業はより適切な意思決定を行い、収益ならびに収益性を向上させ、顧客との関係を最適化することができます。Qlikは世界100カ国以上で事業を展開しており、世界中で5万人以上の顧客にサービスを提供しています。

クリックテック・ジャパン株式会社

〒106-6010

東京都港区六本木1-6-1

泉ガーデンタワー10階

qlik.com/jp

© 2021 QlikTech International AB. All rights reserved. All company and/or product names may be trade names, trademarks and/or registered trademarks of the respective owners with which they are associated.