GridDB Cloudのマルチテナント化技術

Technologies to Apply Multitenancy to GridDB Cloud Service

千葉　一輝 CHIBA Kazuki　　近藤　雄二 KONDO Yuji　　藤田　慎一 FUJITA Shinichi

IoT（Internet of Things）向けクラウドデータベース（DB）であるGridDB Cloudは，契約ユーザーごとにCPUやディスクなどのリソースを占有するシングルテナント形態であり，高コストでも高い安定性を求める用途に適している。しかし，低コストで手軽に使えるDBサービスの需要もあり，そのようなニーズを満たすために，複数ユーザーでリソースを共有するマルチテナント形態が必要だった。

東芝デジタルソリューションズ（株）は，セキュリティーを強化しながら低コストのマルチテナント形態を実現するために，アクセス分離とリソース制限の技術を開発した。2023年12月から，マルチテナント形態のGridDB Cloudを提供している。

Toshiba Digital Solutions Corporation offers GridDB Cloud, a cloud database managed service for the Internet of Things (IoT). This single-tenant service dedicates resources such as a central processing unit (CPU), disks, and other equipment to individual customers to achieve high stability while increasing costs. With growing demand for low-cost, easy-to-use cloud database managed services, there is greater need for a multitenant architecture in which resources are shared among multiple customers.

We have responded to this need by developing the following key technologies to apply multitenancy to GridDB Cloud: (1) access segregation technology to enhance the security of cloud services, and (2) resource limitation technology to optimize the operational efficiency of cloud services, and launched GridDB Cloud multitenant service in December 2023.

1. まえがき

東芝デジタルソリューションズ（株）は，従来提供してきたスケールアウト型DBであるGridDBを，DBaaS（Database as a Service）化したGridDB Cloudを開発し，2021年4月にマネージドサービスとして提供開始した。

GridDB Cloudは，オンプレミス版のGridDBの特長を継承しているため，高信頼で性能要求が高いシステムにも適用可能である。また，DBaaS化により，オンプレミスで課題であった初期導入期間の短縮と，サーバー運用・保守コストの低減を実現した。

今回，更なる低コスト化を目指して，マルチテナント形態でのサービス提供を可能にするために，セキュリティーを強化するアクセス分離と，契約ユーザーごとにリソースを制限する技術を開発した。

ここでは，GridDB Cloudのマルチテナント化の課題と，アクセス分離技術・リソース制限の技術について述べる。

2. GridDB Cloudの特長

GridDB Cloudは，特にIoTやビッグデータの分野で高いパフォーマンスと柔軟性を求めるアプリケーションに最適なDBソリューションである。その特長を以下にまとめる。

⑴　高可用性と高信頼性　　GridDB Cloudは高可用性を確保するための機能を備えている。データのレプリケーションや自動フェールオーバーにより，ノード（サーバー）に障害が発生しても自動検知し，代替ノードで処理を継続可能である。これにより，システムのダウンタイムを最小限に抑えられる。また，クラウドインフラの耐障害性を生かして，高い信頼性を提供する。

⑵　時系列データの最適化　　GridDBは時系列データの管理に特化した機能をサポートし，IoTデータやセンサーデータのような時刻付きデータの処理に優れている。効率的なデータ圧縮とインデックス作成により，高速なクエリー処理が可能である。

⑶　マネージドサービス　　GridDB Cloudは完全にマネージドされたサービスとして提供されており，ユーザーはインフラの管理やメンテナンスに煩わされることなく，DBの利用に集中できる。

⑷　高いセキュリティー　　データの暗号化や，アクセス制御，監査ログといったセキュリティー機能が充実しており，機密性の高いデータを安全に保護できる。

⑸　柔軟な料金プラン　　使用量に応じた柔軟な料金プランが提供されており，初期投資を抑えながら，ビジネスの成長に応じてプランを選択することで，スモールス

表1. シングルテナント形態とマルチテナント形態のメリット・デメリット
Advantages and disadvantages of single-tenancy and multitenancy

項　目	シングルテナント形態	マルチテナント形態
メリット	・リソースを占有できるため，ほかの契約ユーザーの利用状況が性能に影響しない。 ・システムのリソースを上限まで利用できる。 ・契約ユーザーデータが独立しているため，障害発生時の影響が特定の契約ユーザーに絞られる。	・リソースを共有するので1契約ユーザー当たりのコストが安い。 ・契約申し込み後，すぐに利用できる。
デメリット	・リソースのコストが高い。 ・契約ユーザー専用の環境を必要時に構築するため，利用できるようになるまでに時間が掛かる。	・ほかの契約ユーザーの利用状況が，性能に影響する。 ・システム上の有限のリソースを契約ユーザーで共有するため，リソースが限定される。 ・複数の契約ユーザーが同一環境を利用するため，障害発生時の影響が複数の契約ユーザーに及ぶ。

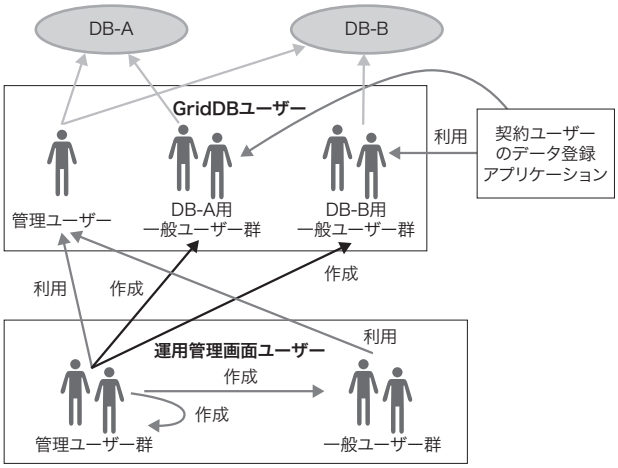

図1. シングルテナント形態におけるユーザー管理方法
シングルテナント形態では，運用管理画面ユーザーは，管理ユーザーか一般ユーザーかを問わず，どのDBにもアクセスできる。
Access control architecture of single-tenant GridDB Cloud service

タートからエンタープライズ規模まで対応可能である。必要時にノードを無停止で追加してシステム拡張するオプションプランもサポートしている。

3. マルチテナント化の課題

シングルテナント形態とマルチテナント形態の契約ユーザーは，GridDB Cloudのサービス提供の単位であるクラスター（複数のサーバーで構成）を，それぞれ次のように利用する。

シングルテナント形態：一人の契約ユーザーが占有

マルチテナント形態：複数の契約ユーザーで共有

二つの形態のメリット・デメリットを，**表1**に示す。マルチテナント形態では，一つのGridDBクラスターを複数の契約ユーザーが共有することで1契約ユーザー当たりのコストは安くなる。ただし，クラスターのCPUやディスクなどのリソースを共有するために，以下の二つの課題に対応する必要がある。

⑴　セキュリティー強化　　個々の契約者が互いの情報に不正アクセスできないように，セキュリティーを強化する必要がある。

⑵　運用適正化　　個々の契約者が過剰にリソースを消費することで，ほかの契約者のパフォーマンスに悪影響を与えることがないように，運用を適正化する対策が必要である。

そこで，セキュリティー強化のためにアクセス分離技術を，運用適正化のためにリソース制限技術を，開発した。

4. アクセス分離技術

まず，シングルテナント形態におけるユーザー管理方法を，**図1**に示す。この例では，GridDBの論理DBとしてDB-AとDB-Bの二つがあり，シングルテナント形態では，契約ユーザーは二つとも専有できる。

GridDB Cloudには大別して2種類のユーザーが存在する。

1種類目のユーザーは，DBへのアクセスを行うGridDBユーザーである。GridDBユーザーは，全てのDBへのアクセスが可能な管理ユーザーと，特定のDBだけにアクセス可能な一般ユーザーに細分化される。契約ユーザーのデータ登録アプリケーションは，一般ユーザーの権限でDBへアクセスする。

2種類目のユーザーは，運用管理画面ユーザーである。運用管理画面ユーザーは，GridDB Cloudに関する様々な操作を画面から行う。GridDBユーザーはGridDBのDBアクセスに焦点を当てており，画面ごとのアクセス制御を行うのが難しいため，運用管理画面ユーザーが別に必要になった。運用管理画面ユーザーは，アクセス制御やGridDBユーザーの作成などを行える管理ユーザーと，DBの操作を行う一般ユーザーに細分化される。いずれの運用管理画面ユーザーもGridDBにアクセスする操作に関しては，内部的にGridDBの管理ユーザーの権限で利用する。そのため，運用管理画面ユーザーは，管理ユーザーか一般ユーザーかを問わず，GridDBのどのDBにもアクセスできる。

次に，マルチテナント形態では，この仕様を変更し，運用管理画面ユーザーがほかの契約ユーザーの情報にアクセスできないようにする必要がある。

マルチテナント形態では1契約ユーザーに一つのGridDBの論理DBが割り当てられる。DB-AとDB-Bがある環境で，DB-Bを割り当てられた契約ユーザーによるユーザー管理

方法を，**図2**に示す。マルチテナント形態の運用管理画面ユーザーは，シングルテナント形態と異なり，内部的にはDB-Bだけにアクセスできる GridDBの一般ユーザーとして利用する。運用管理画面ユーザーとGridDBユーザーは，運用管理画面のサーバー側でひも付けて制御する。この仕組みにより，運用管理画面で表示されるデータは，DB-Bだけにアクセス可能なGridDBユーザーを通して取得されるため，ほかの契約ユーザーの情報には運用管理画面からアクセスできない。

また，GridDBの一般ユーザーの作成には，GridDBの管理ユーザー権限が必要である。そのため，この機能に限っては，運用管理画面ユーザーが内部的にGridDBの管理ユーザーの権限を利用する。この際，DB-A用の一般ユーザーが作成できるとアクセス分離ができなくなるため，DB-B用の一般ユーザー以外は作成できないよう，画面のサーバー側で制御する。

このように，マルチテナント形態で同じリソースを共有している契約ユーザー間のアクセス先を分離することで，セキュリティーを強化できる。

5. リソース制限技術

マルチテナント形態の利用例を，**図3**に示す。複数の契約ユーザーが同じクラスターを共有し，契約ユーザーとそのユーザーアプリケーションは，それぞれが契約したDBだけにアクセスできる。

ある契約ユーザーが共有リソースを大量に消費することで，ほかの契約ユーザーの性能が低下したり，データ登録ができなくなったりすることがないように，契約ユーザーごとにリソース使用量の上限を設定し，アクセス制御を行う二つの機能を開発した。

(1) リクエスト数制限機能　　契約ユーザーから送信するリクエスト数が単位時間内の上限値に到達したときに，アクセスを拒否する。

(2) ディスク使用量制限機能　　契約ユーザーのディスク使用量が上限値に到達したときに，データ登録不可にする。

5.1 リクエスト数制限機能

GridDB Cloudは，契約ユーザー向けのアクセス手段としてWebAPI（Web Application Programming Interface）を提供している。WebAPIによるアクセスのリクエスト数を制限するために，契約ユーザーから送信する単位時間内のリクエスト数が上限値に到達した場合にアクセスを拒否し，例えば一定時間リクエスト数が上限値を超えなかった場合にアクセスを許可するようにした。この機能は，WebAPIのリクエスト数の保存部と，単位時間当たりのリクエスト数が上限に到達したか否かを検知し，その結果に応じてアクセスを制御（拒否／許可）する監視プロセスで実現した（**図4**）。

リクエスト数制限機能により，特定の契約ユーザーが10分間などの期間で過剰な数のリクエストを送信した場合に，一定期間アクセスを拒否することで，GridDBサーバーの負荷を下げられる。これにより，特定の契約ユーザーが急に大量のアクセスを行っても全体の負荷が増えるおそれを低減し，安定稼働が可能になる。

5.2 ディスク使用量制限機能

契約ユーザーのディスク使用量が上限値に達した場合，DBを読み取り専用にしてデータ登録ができないようにする機能を開発した（**図5**）。この機能は，DBごとのディスク使用量の管理部に加えて，5.1節の監視プロセスを活用して

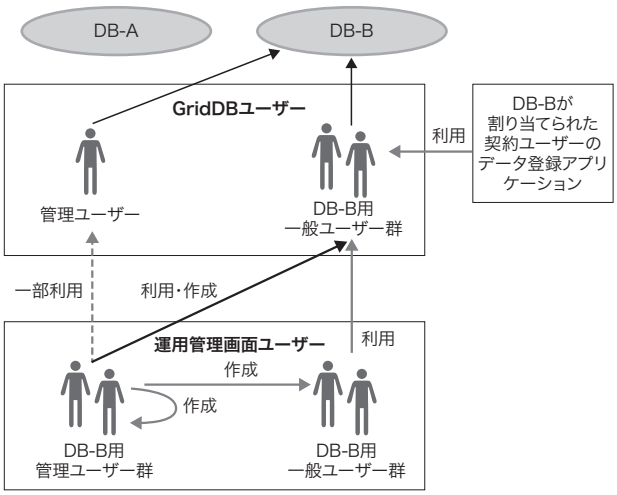

図2. マルチテナント形態におけるユーザー管理方法

マルチテナント形態では，運用管理画面ユーザーも，自分の契約したDBだけにアクセスできる。

Access control architecture of multitenant GridDB Cloud service

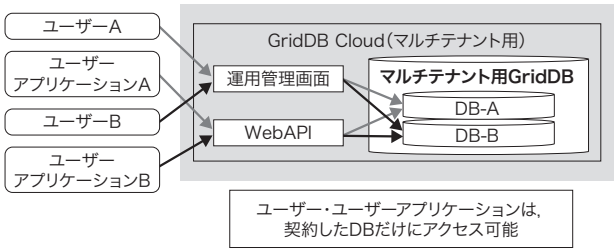

図3. マルチテナント形態の利用例

ある契約ユーザーが共有リソースを大量に消費することで，ほかの契約ユーザーの性能が低下したり，データ登録ができなくなったりすることがある。

Example of GridDB Cloud multitenant service usage

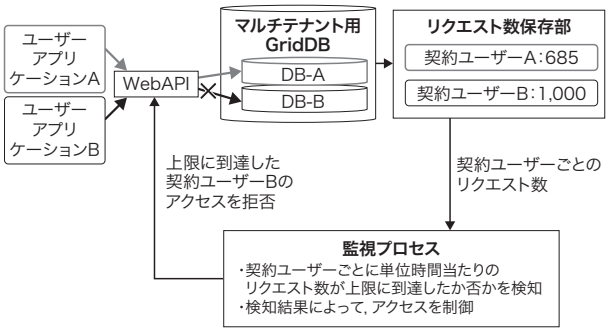

図4. リクエスト数制限機能の構成

WebAPIによるリクエスト数を監視し，上限に到達した場合にアクセスを拒否することで，リクエスト数を制限する。

Outline of access segregation function

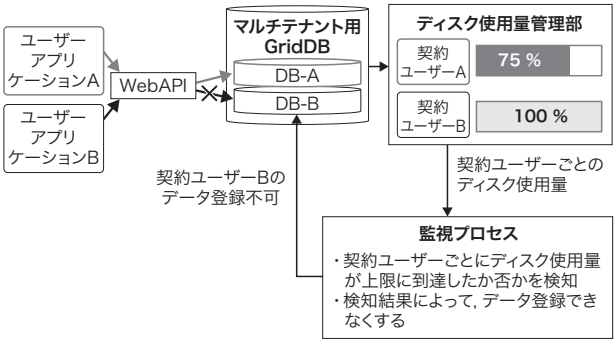

図5. ディスク使用量制限機能の構成

ディスク使用量を監視し，上限に到達した場合にDBを読み取り専用にすることで，ディスク使用量を制限する。

Outline of resource limitation to control disk usage

実現した。

ディスク使用量制限機能により，特定の契約ユーザーが大きな容量を使うことを防ぎ，適正な運用が可能になる。

リクエスト数制限機能とディスク使用量制限機能に使った監視プロセスは，汎用のアーキテクチャーであり，別の項目の監視が必要になった場合も，適用可能である。

6. あとがき

アクセス分離技術とリソース制限技術を開発したことにより，マルチテナント形態での，セキュリティー強化と運用の適正化が可能になった。GridDB Cloudのマルチテナント化により，低コストでサービス提供できるようになり，容易かつ短期間にDB環境を整えられる特長を生かして，小規模から大規模まで幅広いユーザーが利用しやすくなった。

今後は，マルチテナント形態でのアクセス方法として，ネイティブAPI（Java API・Python API）などへのサポート拡大を進めていく。

千葉　一輝　CHIBA Kazuki
東芝デジタルソリューションズ（株）
ソフトウェアシステム技術開発センター
ソフトウェア開発部
Toshiba Digital Solutions Corp.

近藤　雄二　KONDO Yuji
東芝デジタルソリューションズ（株）
ソフトウェアシステム技術開発センター
ソフトウェア開発部
Toshiba Digital Solutions Corp.

藤田　慎一　FUJITA Shinichi
東芝デジタルソリューションズ（株）
ソフトウェアシステム技術開発センター
ソフトウェア開発部
Toshiba Digital Solutions Corp.