QlikView

# QlikView
# Section Access 入門

改訂 1 - 2010 年 6 月 8 日

2010 年 4 月 17 日

# 本書について

本書は、QlikView リファレンス マニュアルの Section Access に関する情報を補足するものであり、Section Access を初めて使用するユーザー、デベロッパー トレーニングやリファレンス マニュアルと併せて本書を活用するユーザー、および過去に学んだことを復習するユーザーを対象としています。
本書の事例は QlikView Version 9 以降を対象に作成されています。

**本書は、シンクライアント（Plugin、Ajax）での Section Access の使用、および QlikView Publisher または QlikView Server を使用したリロードについては扱っていません。これらのテーマは、今後公開される手引書や、より高度な Section Access にて取り扱います。

## *警告*

- ドキュメントにSection Accessを実装する前に、アプリケーションをバックアップしてください。誤った構文は、ドキュメントへのアクセスを不能にし、データやスクリプトを復元することはできません。

- スクリプトにエラーがあった場合に、以前のバージョンのドキュメントに戻せるよう、ドキュメントの複製を複数保持することを推奨します。

# 目次

*Section Access 入門* ..... *1*
本書について ..... 2
警告 ..... 2
Section Access を使用する理由 ..... 4
Section Access の設定と有効化の方法 ..... 5
隠しスクリプト ..... 5
アクセス制御 ..... 6
Section Access のシステム項目 ..... 6
Section Access 向けにスクリプトで使用される項目 ..... 7
ACCESS ..... 7
USERID ..... 8
PASSWORD ..... 8
SERIAL ..... 8
NTNAME ..... 8
NTDOMAINSID ..... 8
NTSID ..... 9
OMIT ..... 9
REDUCTION ..... 9
Section Access のドキュメントレベルでの定義 ..... 10
「セクションアクセスによる初期データ削除」 ..... 10
「強制削除」 ..... 11
「バイナリロード禁止」 ..... 11
ドキュメントレベルでのセキュリティ設定 ..... 12
データの削除 ..... 12
シートの追加 ..... 13
ロードスクリプトの編集 ..... 13
リロード ..... 13
パーシャルリロード ..... 13
モジュールの編集 ..... 13
ドキュメントの保存（ユーザー） ..... 13
ドキュメントプロパティへのアクセス（ユーザー） ..... 13
シートの移動 ..... 14
エクスポートを許可する ..... 14
（エクスポート禁止時に）印刷を許可する ..... 14
タブプロパティへのアクセス ..... 14
マクロによるセキュリティの上書き ..... 14
すべてのシートとシートオブジェクトを表示 ..... 14
隠しロードスクリプトの進捗を表示 ..... 14
ユーザーにリロードを許可する ..... 14
セキュリティを管理者権限で上書きする ..... 14
さまざまなセキュリティ実装例 ..... 14
例 1： ..... 15
例 2： ..... 15
例 3： ..... 16
例 4： ..... 16
例 5： ..... 17
例 6： ..... 18
おわりに ..... 19

# Section Access を使用する理由

Section Access をドキュメントに実装すべき理由は 2 つあります。

- 無許可のアクセスからデータを保護するため。
- 権限のあるユーザーが閲覧できるデータの種類や、行える内容を制限するため。

QlikView は、情報を収集し、容易なデータ分析を可能にする最適な方法です。しかしながら、QVW ドキュメントは、他のコンピュータファイルと同様に、紛失したり盗まれたりする場合があります。Section Access を実装していない QVW ファイルは、QlikView をインストールしていれば誰でも開くことができるため、データは危険にさらされている可能性があります。Section Access を適切に実装したドキュメントは、そうした問題はありません。

また、権限のあるユーザーに、完全なデータセットを見せたくない場合もあります。Section Access は、データを削除し、権限のあるユーザーが閲覧できるデータ、閲覧できないデータを管理するのに非常に有効です。

Section Access には、さまざまな方法があります。ドキュメントによっては、単純にユーザー名とパスワードのみで十分です。あるいは、特定のユーザーに、ドメインで特定のマシンに特定のユーザーとしてログインし、特定のシリアル番号を使用してもらうことも可能です。

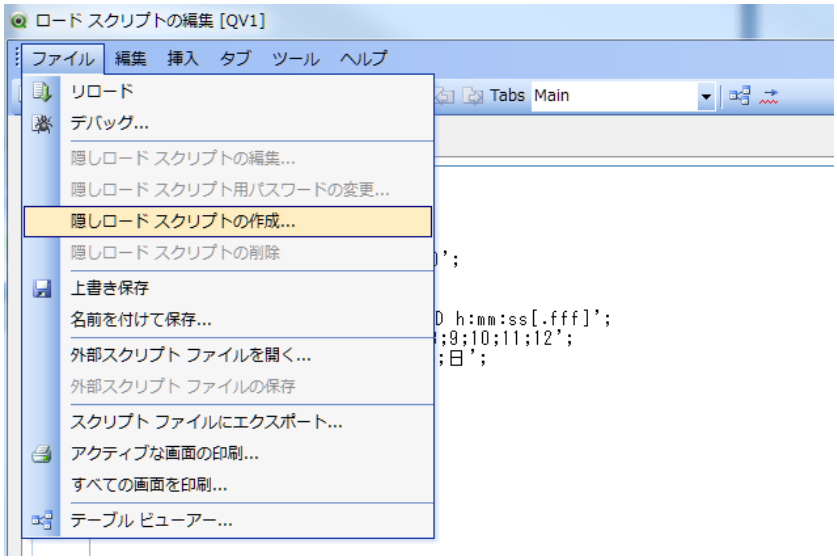
# Section Access の設定と有効化の方法

以下の 3 つのステップで、効果的な Section Access の設定が可能です。

スクリプト内での Section Access 定義の記述
ドキュメントレベルでの Section Access の有効化、およびユーザー許可の定義
ユーザーレベルのアクセス設定

## *隠しスクリプト*

Section Access は、隠しスクリプトでの実装を推奨します。




*「ファイル」→「隠しロードスクリプトの作成」*

ユーザー資格情報は、平文（インラインデータを使用している場合）で、または Section Access 定義の場所に表示されるため、ADMIN 権限を有するすべてのユーザー、およびスクリプトを表示する権限を与えられたユーザーは、スクリプトを表示することができます。隠しスクリプト内に Section Access を記述すれば、データのセキュリティはより確実なものになります。隠しスクリプトのパスワードは、紛失しても復元できないため、安全な場所に保管してください。ADMIN パスワードも同様です。ADMIN パスワードを紛失すると、ドキュメントへのアクセスは拒否され、パスワードを復元することもできません。

## *アクセス制御*

すべてのアクセス制御は、テキストファイル、データベース、または INLINE 句によって管理され、これは通常 QlikView でデータが処理される方法と同様です。
スクリプトにロードされるアクセスセクションは、SECTION ACCESS;ステートメントで宣言されます。
Section Access の定義は、「SECTION ACCESS;」 ステートメントと「SECTION APPLICATION;」 ステートメントの間に記述し、実際のデータがロードされる前に定義する必要があります。

## *Section Access のシステム項目*

アクセスレベルは、SECTION ACCESS 内にロードされる 1 つまたは複数のテーブル内のユーザーに割り当てられます。これらのテーブルには、さまざまなユーザー固有のシステム項目を含めることができます。
希望するセキュリティのレベルに応じて Section Access を構築するために、以下に一覧表示された複数の項目を組み合わせることができます。
標準項目とは別に、各ユーザーのデータ削除を管理するために、追加項目を定義できます。

**外部データソースからロードされたすべてのデータは、SECTION ACCESS ステートメントでは大文字でロードされる必要があります。これは、常に大文字として扱われるインラインデータには適用されません。

例：

```
SECTION ACCESS;
LOAD
        UPPER(Level) AS ACCESS,
        UPPER(DomainName) AS NTNAME,
        UPPER(PASSWORD) AS PASSWORD
FROM Access.XLSX;

SECTION APPLICATION;
```

## *Section Access 向けにスクリプトで使用される項目*


*「挿入」→「セクションアクセス」→「インラインロード」*

### ACCESS

対応するユーザーに与えられるアクセス権限を定義する項目であり、すべての Section Access の必須項目です。
Section Access には 、「ADMIN」と「USER」という 2 つのアクセスレベルがあります。ADMIN は、USER が QlikView ドキュメントで閲覧できる内容と、行える内容を管理します。ADMIN 特権を持つユーザーは、ドキュメント内のすべてを変更することができます。
（QlikView（サーバーから開く）、Plugin、または Ajax クライアントを使用してドキュメントを開いているユーザーは、ACCESS の定義にかかわらず、常に USER 権限です）。

## USERID

許可されるユーザーID を含む項目です。
QlikView がユーザーID の入力を要求し、この項目の値と比較します。
このユーザーID は、Windows のユーザーID と同一ではありません。
USERID は、大文字と小文字を区別しません。Section Access 定義のすべての項目は、大文字として扱われます。

## PASSWORD

この項目は、許可されるパスワードを含みます。
QlikView がパスワードの入力を要求し、この項目の値と比較します。
このパスワードは、Windows のパスワードと同一ではありません。
USERID は、大文字と小文字を区別しません。Section Access 定義のすべての項目は、大文字として扱われます。

## SERIAL

この項目は、QlikView のシリアル番号に対応する番号を含みます。
例：4900 2394 7113 7304
QlikView がユーザーのシリアル番号を確認し、その番号をこの項目の値と比較します。
SERIAL は以下から確認できます。「設定」→「ユーザープロパティ」→ 「ライセンス」タブ

## NTNAME

この項目は、Windows NT のドメインユーザー名またはグループ名に相当する文字列を含みます。
QlikView が OS からログイン情報を取得し、その情報をこの項目の値と比較します。
例：DOMAIN¥NTNAME

## NTDOMAINSID

この項目は、Windows NT ドメインの SID に対応する文字列を含みます。
例：S-1-5-21-125976590-467238106-1092489882
QlikView が OS からログイン情報を取得し、その情報をこの項目の値と比較します。
NTDOMAINSID はスクリプト、「挿入」→「ドメイン SID」から取得できます。

## NTSID

この項目は、Windows NT の SID を含みます。
例：S-1-5-21-125976590-467238106-1092489882-1378
QlikView が OS からログイン情報を取得し、その情報をこの項目の値と比較します。
NTSID は、「Getsid.exe」など、第三者機関の無料アプリケーションを使用して生成できます。

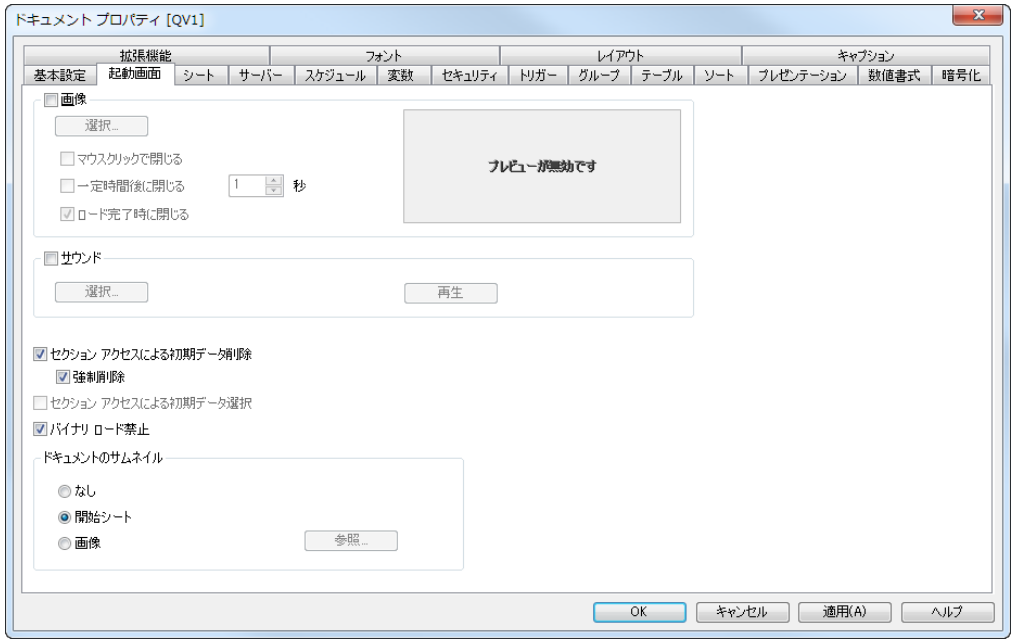
## OMIT

特定のユーザーに対して省略される項目です。

## REDUCTION

REDUCTION は、ユーザーごとのデータアクセスを制御するために追加される任意の項目名です。REDUCTION の値は、アプリケーション内の同一の名前の他の項目と一致させるために使用されます。一致がある場合、その項目のデータは削除され、ユーザーに表示されます。アプリケーションでこの項目が選択された場合と同様の結果となり、関連しない項目はすべて削除されます。

## *Section Access のドキュメントレベルでの定義*




*「設定」→「ドキュメントプロパティ」→「起動画面」*

### 「セクションアクセスによる初期データ削除」

チェックボックスを選択して、ドキュメントにおける Section Access を有効化します。

## 「強制削除」

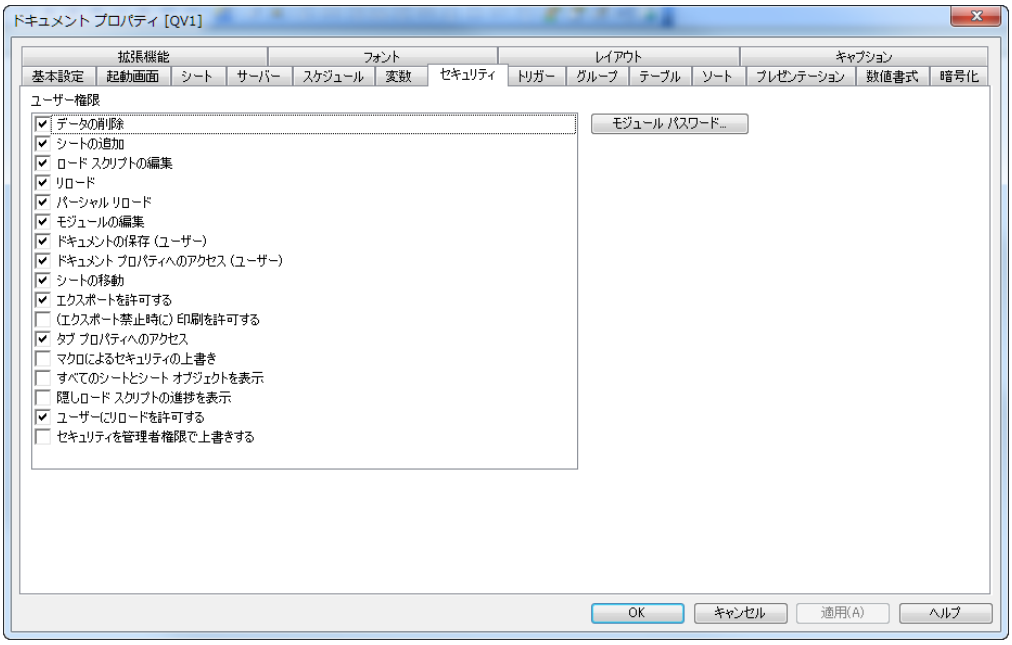
Section Access の REDUCTION の値が対応するセクション アプリケーション項目に一致しない場合、常にドキュメントへのアクセスは拒否されます。
このオプションが選択されておらず、データを削除するための一致がない場合、ドキュメントのすべてのデータが USER レベルで表示されます。ただし、ADMIN は REDUCTION 項目にかかわらず、常に全データを閲覧できます。QlikView ドキュメントへの望ましくないアクセスを防ぐためには、強制削除を使用することを推奨します。

## 「バイナリロード禁止」

このオプションが選択されている場合、別の QlikView ドキュメント内の Binary ステートメントを使用してドキュメントの QVW ファイルからデータをロードすることはできません。セキュリティ向上のために、このオプションを使用することを強く推奨します。

## *ドキュメントレベルでのセキュリティ設定*

セキュリティタブでは、USER 特権を持つユーザーが実行できるアクションを定義できます。
USER に特権を与えすぎると、セキュリティの実装が無用になる可能性があるため、このタブで適切な設定を行うことが極めて重要です。
ADMIN と USER に明確な違いを設けたい場合は、これらの設定を検討してください。
セキュリティタブは、Section Access の ADMIN からのみアクセスできることに留意してください。




*「設定」→「ドキュメントプロパティ」→「セキュリティ」*

## データの削除

このチェックボックスが選択されていない場合、ファイルメニューのデータの削除コマンドは非アクティブになります。

## シートの追加

このチェックボックスが選択されていない場合、レイアウトメニューのシートの追加コマンドは非アクティブになります。

## ロードスクリプトの編集

このチェックボックスが選択されていない場合、ファイルメニューおよびツールバーのロードスクリプトの編集コマンドは非アクティブになります。

## リロード

このチェックボックスが選択されていない場合、ファイルメニューおよびツールバーのリロードコマンドは非アクティブになります。
ユーザーにドキュメントのリロードを許可するのは、ドキュメントをリロードする際に常に完全なデータセットをリロードすることになるため、望ましくありません。

## パーシャルリロード

このチェックボックスが選択されていない場合、ファイルメニューのパーシャルリロードコマンドは非アクティブになります。ユーザーにドキュメントのリロードを許可するのは、ドキュメントをリロードする際に常に完全なデータセットをリロードすることなるため、望ましくありません。

## モジュールの編集

このチェックボックスが選択されていない場合、ファイルメニューのモジュールの編集コマンドは非アクティブになります。

## ドキュメントの保存（ユーザー）

このチェックボックスが選択されていない場合、USER 特権を持つユーザーに対して、ファイルメニューの保存コマンドが非アクティブになります。
ユーザーが保存を許可されている場合、削除されたデータセットが保存されることで、他のユーザーをドキュメントからロックアウトする可能性があります。

## ドキュメントプロパティへのアクセス（ユーザー）

このチェックボックスが選択されていない場合、USER 特権を持つユーザーに対して、設定メニューのドキュメントプロパティコマンドが非アクティブになります。
このオプションが選択されている場合でも、USER は起動画面タブ、およびセキュリティタブを閲覧できないことに留意してください。

### シートの移動

このチェックボックスが選択されていない場合、レイアウトメニューのシートを右へコマンドおよびシートを左へコマンドは非アクティブになります。

### エクスポートを許可する

このチェックボックスが選択されていない場合、エクスポート、印刷、クリップボードにコピーコマンドはすべて使用できません。

### （エクスポート禁止時に）印刷を許可する

上記のエクスポートを許可するチェックボックスが選択されていない場合でも、このチェックボックスが選択されていれば、すべての印刷コマンドは使用できます。

### タブプロパティへのアクセス

このチェックボックスが選択されていない場合、タブプロパティにはアクセスできません。

### マクロによるセキュリティの上書き

このチェックボックスが選択されている場合、オートメーション API（Application Program Interface）を使用したマクロとコマンドによって、すべてのセキュリティ設定を上書き可能です。

### すべてのシートとシートオブジェクトを表示

このチェックボックスが選択されている場合、シートおよびシートオブジェクトの条件付き表示はすべて却下されるため、すべてのシートとシートオブジェクトが表示されます。この機能は、Ctrl キー、Shift キー、S キーを同時に押して切り替え可能です。

### 隠しロードスクリプトの進捗を表示

このチェックボックスが選択されている場合、スクリプトを実行している間に、スクリプトの進行状況を表示するダイアログボックスが表示されます。

### ユーザーにリロードを許可する

このチェックボックスが選択されていない場合、上記のリロードチェックボックスが選択されていても、ドキュメントが USER モードで開かれているときにスクリプトをリロードすることはできません。

### セキュリティを管理者権限で上書きする

このチェックボックスが選択されている場合、ADMIN モードにおいて、ドキュメントとシートに対するすべてのセキュリティ設定が無視されます。

## さまざまなセキュリティ実装例

以下では、さまざまなセキュリティレベルにおける Section Access の一般的な実装例をいくつか示します。NTNAME、NTDOMAINSID、および NTSID を追加した場合、QlikView はアクセスを付与する前にこの情報を見つけて検証しなければいけないため、認証プロセスに時間がかかります。

Section Access においてよくある誤解は、Section Access での「*」（アスタリスク）の使用についてです。アスタリスクは、項目に対するすべての値ではなく、「記載されたすべての値」を意味します。この詳細については、スクリプトの例で説明します。

### *例１：*

```
Section Access;
LOAD * INLINE [
    ACCESS,     USERID,     PASSWORD
    ADMIN,      ADMIN,      ADMIN
    USER,       USER1,      U1
    USER,       USER2,      U2
    USER,       USER3,      U3
];
```

これは非常に基礎的な認証の形式です。
ドキュメントはどこからでも開くことができ、USERID と PASSWORD さえ知っていればアクセスできます。しかしながら、セキュリティの観点からは安全とは言えません。認証されたユーザーは、アプリケーション内のすべてのデータを閲覧できます。

### *例２：*

```
Section Access;
LOAD * INLINE [
    ACCESS,     NTNAME,             PASSWORD
    ADMIN,      DOMAIN¥ADMIN,       ADMIN
    USER,       DOMAIN¥USER1,       U1
    USER,       DOMAIN¥USER2,       U2
    USER,       DOMAIN¥USER3,       U3
];
```

これはより安全な例です。ユーザーは、Windows NT のアカウントでパスワードを用いてログインすることを要求されます。この方法の利点は、USERID が不要であることです。

### *例３：*

```
Section Access;
LOAD * INLINE [
    ACCESS,     NTNAME,             PASSWORD,     SERIAL
    ADMIN,      DOMAIN¥ADMIN,       ADMIN,
    USER,       DOMAIN¥USER1,       U1,           1234 5678 9012 3456
    USER,       DOMAIN¥USER2,       U2,           2345 6789 0123 4567
    USER,       DOMAIN¥USER3,       U3,           3456 7890 1234 5678
];
```

これはさらに安全な例です。ユーザーは、記載されたライセンス番号で登録されている QlikView からしかドキュメントを開くことができません。

### *例４：*

```
Section Access;
LOAD * INLINE [
    ACCESS,     NTNAME,             PASSWORD,     SERIAL,                 NTSID
    ADMIN,      DOMAIN¥ADMIN,           ADMIN,                  ,
          *
    USER,       DOMAIN¥USER1,           U1,               1234 5678 9012 3456, S-1-
5-21-2068569857-8585916410-466756119-12345

    USER,       DOMAIN¥USER2,           U2,               2345 6789 0123 4567, S-1-
5-21-2068569857-8585916410-466756119-23456

    USER,       DOMAIN¥USER3,           U3,               3456 7890 1234 5678, S-1-
5-21-2068569857-8585916410-466756119-34567
];
```

この例では、NTSID が追加されたことで、ドキュメントにアクセスするユーザーは、ドメインの特定のマシンにログインすることを要求されます。

***例 5：***

```
Section Access;
LOAD * INLINE [
    ACCESS,     USERID,     PASSWORD,    OMIT
    ADMIN,      ADMIN,      ADMIN,
    USER,       USER1,      U1,          SALES
    USER,       USER2,      U2,          WAREHOUSE
    USER,       USER3,      U3,          EMPLOYEES
    USER,       USER4,      U4,          SALES
    USER,       USER4,      U4,          WAREHOUSE
    USER,       USER5,      U5,          *
];

Section Application;
LOAD * INLINE [
    SALES,      WAREHOUSE,  EMPLOYEES,   ORDERS
    1,          2,          3,           4
];
```

この例では、OMIT が Section Access の一部として追加されました。
USER1 は SALES を閲覧できず、USER2 は WAREHOUSE を、USER3 は EMPLOYEES を閲覧できません。

USER4 には 2 度追加されました。このユーザーに対して、SALES と WAREHOUSE の 2 つの項目を OMIT したいためです。

USER5 には「*」が追加されました。これは、OMIT で記載されたすべての項目が使用できないことを意味しています。
USER5 は、SALES、WAREHOUSE、EMPLOYEES の項目を閲覧できません。

***例 6：***

```
Section Access;
LOAD * INLINE [
    ACCESS,     USERID,     PASSWORD,     REGION
    ADMIN,      ADMIN,      ADMIN,
    USER,       USER1,      U1,           AFRICA
    USER,       USER2,      U2,           AMERICA
    USER,       USER3,      U3,           ASIA
    USER,       USER4,      U4,           EUROPE
    USER,       USER5,      U4,           AMERICA
    USER,       USER5,      U5,           *

];

Section Application;
SALES:
LOAD * INLINE [
    REGION,     PROFIT
    AFRICA,     1000
    AMERICA,    2000
    ASIA,       3000
    EUROPE,     4000
    OCEANIA,    5000
];
```

この例では、REGION と呼ばれる REDUCTION 項目が追加されました。ユーザーを、各自の地域の販売収益に制限することが目的です。

USER1 は AFRICA の収益のみ閲覧でき、USER2 は AMERICA の、USER3 は ASIA 地域の収益のみ閲覧できます。

USER4 は、EUROPE と AMERICA の収益を閲覧できます。

USER5 は、OCEANIA を除く、REDUCTION 項目の REGION に記載されているすべての地域を閲覧できます。
USER5 の REDUCTION 項目 REGION は「*」ですが、この場合も星印は項目に対するすべての値ではなく、「すべての記載された値」を意味します。REGION に OCEANIA を記載したユーザーはいないため、USER5 は OCEANIA の値にアクセスすることはできません。

USER5 が OCEANIA も閲覧できるようにしたい場合、Section Access に以下の 1 行を追加する必要があります。

```
    USER,       USER5,      U5,           OCEANIA
```

# おわりに

Section Access は、データを保護し、アプリケーションへのアクセスを制限する優れた方法です。Section Access を実装しているすべての方に、以下を行うことを推奨します。

- Section Access を実装する前に、アプリケーションをバックアップする。
- 自身をロックアウトした際に以前の状態に戻れるよう、複数の複製を保持する。
- セキュリティ向上のために、隠しスクリプトに Section Access を実装する。
- 外部ソースから Section Access テーブルを読み取る場合は、安全性を確認する。
- 小規模で始め、簡潔にしておく。
- Section Access を管理しやすい状態にする。そうすることで、組織の成長に伴いユーザーを Section Access に追加したり削除したりする際に役立ちます。