IBM Information Management software

DB2 for LUW V9.5
セキュリティー・デザイン・ガイド
監査機能編・別冊

＜第1.0版　2008年4月＞

お断り：当資料は、DB2 Universal Database for Linux, UNIX and Windows V8.2, DB2 for Linux, UNIX and Windows V9.1, V9.5 をベースに作成されています。

監査機能編・別冊

- ClientInformationAPIと監査機能の組み合わせ
- AUDITパフォーマンス検証結果
- 監査レコードのフォーマット

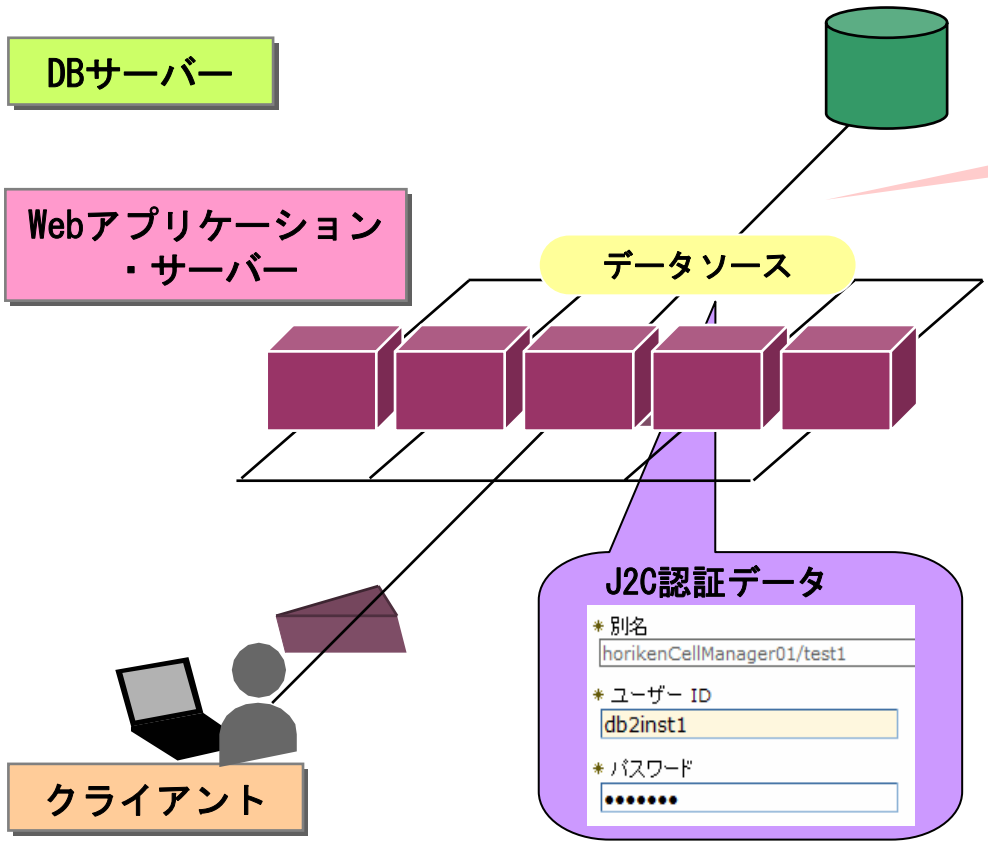
ClientInformationAPIと監査機能の組み合わせ

＜第1.0版　2008年4月＞

お断り：当資料は、DB2 Universal Database for Linux, UNIX and Windows V8.2, DB2 for Linux, UNIX and Windows V9.1, V9.5 をベースに作成されています。

3層Webシステム上における監査ログの課題

- Webアプリケーション・サーバー側では、ユーザー管理製品(IBM製品ではTivoli Access Manager)やフォーム認証等で認証したユーザー情報が記録されるが、DBサーバー側ではすべてデータソースに定義したユーザー情報が記録される



データソースに定義したユーザーでDBアクセス

システム内の取引過程を記録

監査ログ（DBサーバー）

db2inst1さん	ＸＸ検索処理しました
db2inst1さん	○○更新処理しました
db2inst1さん	△△検索処理しました

監査ログ（Webアプリケーション・サーバー）

Aさん	ＸＸ検索処理しました
Bさん	○○更新処理しました
Cさん	△△検索処理しました

Webアプリケーション・サーバーとDBサーバーの監査ログが一致しない

3層Webシステム上における監査ログの課題

解決策

- ClientInformationAPIをDB2監査機能と組み合わせて使用
  - Webアプリケーション側(WASV6以降)でClientInformationAPI を使用し、ユーザー情報をプロパティに設定する
  - 例:フォーム認証やユーザー管理製品で認証したユーザー情報を設定

DBサーバーの監査ログにも、ClientInformationAPIで設定したユーザー情報が記録される

- Webアプリケーション側での設定

```
import com.ibm.websphere.rsadapter.WSConnection;
(省略)
            con = (WSConnection) ds.getConnection();
            Properties props = new Properties();

            props.setProperty(WSConnection.CLIENT_ID, userid);
            props.setProperty(WSConnection.CLIENT_LOCATION, location);
            props.setProperty(WSConnection.CLIENT_ACCOUNTING_INFO, accounting);
            props.setProperty(WSConnection.CLIENT_APPLICATION_NAME, appname);
            props.setProperty(WSConnection.CLIENT_OTHER_INFO, other_info);
            props.setProperty(WSConnection.OTHER_CLIENT_TYPE, client_type);

            con.setClientInformation(props);
```

WSConnectionをimportする

クライアント情報を設定する

3層Webシステム上における監査ログの課題への解決策

DBサーバー側

- 監査ポリシーを設定し、監査ログを取得する

```
$ cat db2audit_ext.file
(省略)
timestamp=2008-02-26-15.05.10.030135;
category=EXECUTE;
audit event=STATEMENT;
(省略)
id=9.188.198.118.48254.08022606050;
application name=db2jcc_application;
client userid=user_Manager;
client workstation name= ;
client application name=select_appl ;
client accounting string=ise ;
package schema=db2inst1;
package name=SYSSN300;
package section=5;
local transaction id=0x00000000000022b7;
global transaction
(省略)
```

アプリケーションで指定したユーザー情報が表示される

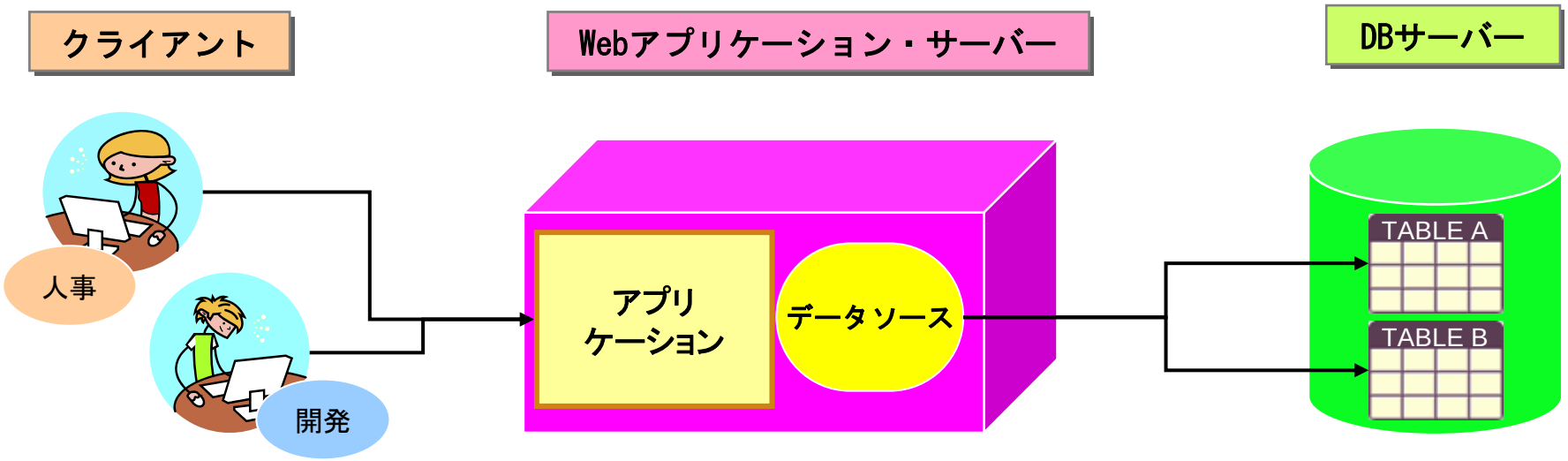
```
(省略)
  statement text=SELECT * FROM db2inst1.tableA
WHERE col1 between ? and ?;
  statement isolation level=RS;
  Compilation Environment Description
    isolation: RS
    query optimization: 5
    min dec div 3: NO
    degree: 1
(省略)
value index = 1
    type = BIGINT
    data = 48;
  value index = 2
    type = BIGINT
    data = 248;
(省略)
```

発行したSQL文が表示される

分離レベルが表示される

パラメーターマーカー値が表示される

ClientInformationAPI 使用時の監査ログ取得手順(1/8)



手順

1. APIによるユーザー情報の設定 (Webアプリケーション・サーバー側)
2. 監査ポリシーの設定 (DBサーバー側)
3. 監査開始 (DBサーバー側)
4. アプリケーション実行 (クライアント側)
5. 監査バッファのフラッシュと監査停止 (DBサーバー側)
6. 監査ログのアーカイブ (DBサーバー側)
7. 監査ログの確認 (DBサーバー側)

ClientInformationAPI 使用時の監査ログ取得手順(2/8)

1. APIによるユーザー情報の設定 (Webアプリケーション・サーバー側)

- ClientInformationAPIを使用して、ユーザー情報を設定する

```
import com.ibm.websphere.rsadapter.WSConnection;
(省略)

            con = (WSConnection) ds.getConnection();
            Properties props = new Properties();

            props.setProperty(WSConnection.CLIENT_ID, "user123");
            props.setProperty(WSConnection.CLIENT_LOCATION, "127.0.0.1");
            props.setProperty(WSConnection.CLIENT_ACCOUNTING_INFO, "accounting");
            props.setProperty(WSConnection.CLIENT_APPLICATION_NAME,  "select_appl");
            props.setProperty(WSConnection.CLIENT_OTHER_INFO, "cool stuff");
            con.setClientInformation(props);
```

WSConnectionをimportする

クライアント情報を入力する

参考情報:InfoCenter -「setClientInformation(Properties) API によるクライアント情報の設定」
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tdat_clientinfotask.html

参考情報:InfoCenter -「WLM_SET_CLIENT_INFO ストアードプロシージャ」
http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.sql.rtn.doc/doc/r0053116.html

ClientInformationAPI 使用時の監査ログ取得手順(3/8)

2. 監査ポリシーの作成 (DBサーバー側)

監査ポリシーを作成し、表に関連付ける

- SECADM権限があるユーザー (secadmin)を作成する

```
$ db2 "grant secadm on database to user secadmin"
DB20000I  The SQL command completed successfully.
```

インスタンスオーナーより、ユーザーsecadminに
SECADM権限をGRANT文で付与する

- ユーザーにSECADM権限が付与されたことを確認する

```
$ db2 "select * from syscat.dbauth"

GRANTOR
GRANTORTYPE GRANTEE
GRANTEETYPE BINDADDAUTH CONNECTAUTH CREATETABAUTH DBADMAUTH EXTERNALROUTINEAUTH IMPLSCHEMAAUTH
LOADAUTH NOFENCEAUTH QUIESCECONNECTAUTH LIBRARYADMAUTH SECURITYADMAUTH
(省略)
secadmin
U          SECADMIN
U          N          Y          N          N          N                    N                    N
N          N                     N                     Y
```

カタログ表を照会すると、ユーザーsecadminに
SECADM権限が付与されている

ClientInformationAPI 使用時の監査ログ取得手順(4/8)

2. 監査ポリシーの設定 (DBサーバー側)

- 監査ログパス、監査アーカイブログパスの変更(任意)
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit configure datapath /logs/audit/active archivepath /logs/audit/archives
AUD0000I  Operation succeeded.
```

監査ログ　/logs/audit/active,
監査アーカイブ・ログ　/logs/audit/archives　に出力

- 監査ポリシーをEXECUTEカテゴリーで作成する
  - SECADM権限のユーザー (secadmin)でコマンドを実行する

```
$ db2 "create audit policy pos_1 categories execute with data status both error type audit"
DB20000I  The SQL command completed successfully.
N                   N             N        N          N                   N              Y
```

監査ポリシー"pos_1"をexecuteカテゴリーで作成

- 作成した監査ポリシーを確認する
  - SECADM権限のユーザー (secadmin)で実行する

```
db2 "select * from SYSCAT.AUDITPOLICIES"
AUDITPOLICYNAME
AUDITPOLICYID CREATE_TIME                 ALTER_TIME                  AUDITSTATUS CONTEXTSTATUS
VALIDATESTATUS CHECKINGSTATUS SECMAINTSTATUS OBJMAINTSTATUS SYSADMINSTATUS EXECUTESTATUS
EXECUTEWITHDATA ERRORTYPE REMARKS
(省略)
POS_1
100 2008-02-26-14.51.22.329400 2008-02-26-14.51.22.329400 N           N              N
N              N              N              N              B              Y              A
```

ポリシー"POS_1"が表示される

ClientInformationAPI 使用時の監査ログ取得手順(5/8)

2. 監査ポリシーの設定 (DBサーバー側)

- 作成した監査ポリシーを監査対象の表に紐付ける
  - SECADM権限のユーザー (secadmin)で実行する

```
$ db2 "audit table db2inst1.tableA using policy pos_1"
DB20000I  The SQL command completed successfully.
```

tableA表に監査ポリシー"POS_1"を紐付ける

- 紐付けを確認する
  - SECADM権限のユーザー (secadmin)で実行する

```
$ db2 "select * from SYSCAT.AUDITUSE"
AUDITPOLICYNAME
AUDITPOLICYID OBJECTTYPE SUBOBJECTTYPE OBJECTSCHEMA
OBJECTNAME
(省略)
POS_1
100 T                          db2inst1
tableA
```

参考情報:InfoCenter -「CREATE AUDIT POLICY ステートメント」
http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.sql.ref.doc/doc/r0050607.html

ClientInformationAPI 使用時の監査ログ取得手順(6/8)

3. 監査開始 (DBサーバー側)

- 監査を開始する
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit start
AUD0000I  Operation succeeded.
```

4. アプリケーション実行 (クライアント側)

5. 監査バッファのフラッシュと監査停止 (DBサーバー側)

- 監査バッファをフラッシュする
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit flush
AUD0000I  Operation succeeded.
```

- 監査を停止する
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit stop
AUD0000I  Operation succeeded.
```

ClientInformationAPI 使用時の監査ログ取得手順(7/8)

6. 監査ログのアーカイブ (DBサーバー側)

- 監査ログをアーカイブする
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit archive database TEST

Node      AUD      Archived or Interim Log File
          Message
--------- -------- ----------------------------------------------------
        0 AUD0000I db2audit.db.TEST.log.0.20080226150728
AUD0000I  Operation succeeded.

$ ls -l /logs/audit/archives
合計 80
-rw-------    1 db2inst1 staff         14683 Feb 26 15:07 db2audit.db.TEST.log.0.20080226150728
```

「アーカイブログの出力先」に設定したパスにアーカイブされる

- 監査ログを抽出する
  - インスタンスユーザー (db2inst1)で実行する

```
$ db2audit extract file ./db2audit_ext.file from files db2audit.db.TEST.log.0.20080226150728
AUD0000I  Operation succeeded.

$ ls -l /logs/audit/archives
合計 80
-rw-rw-rw-    1 resi2008 staff         11526 Feb 26 15:11 db2audit_ext.file
-rw-------    1 resi2008 staff         14683 Feb 26 15:07 db2audit.db.TEST.log.0.20080226150728
```

指定したファイル名でファイルが作成される

ClientInformationAPI 使用時の監査ログ取得手順(8/8)

7. 監査ログの確認 (DBサーバー側)

```
$ cat /logs/audit/archives/db2audit_ext.file
(省略)
  timestamp=2008-02-26-15.05.10.030135;
  category=EXECUTE;
  audit event=STATEMENT;
  event correlator=77;
  event status=0;
  database=TEST;
  userid=db2inst1;
  authid=db2inst1;
  session authid=db2inst1;
  origin node=0;
  coordinator node=0;
  application id=9.188.198.118.48254.08022606050;
  application name=db2jcc_application;
 client userid=user123;
  client workstation name= ;
  client application name= ;
  client accounting string= ;
  package schema=db2inst1;
  package name=SYSSN300;
  package section=5;
  local transaction id=0x00000000000022b7;
  global transaction
  id=0x0000000000000000000000000000000000000000;
(省略)
```

アプリケーションで指定したユーザー情報が表示される

発行したSQL文が表示される

```
uow id=65;
  activity id=1;
  statement invocation id=0;
  statement nesting level=0;
  activity type=READ_DML;
  statement text=SELECT * FROM db2inst1.tableA
WHERE col1 between ? and ?;
  statement isolation level=RS;
  Compilation Environment Description
    isolation: RS
    query optimization: 5
    min dec div 3: NO
    degree: 1
    SQL rules: DB2
    refresh age: +00000000000000.000000
    resolution timestamp: 2008-02-26-15.05.09.000000
    federated asynchrony: 0
    maintained table type: SYSTEM;
  rows modified=0;
  rows returned=199;
  value index = 1
    type = BIGINT
    data = 48;
  value index = 2
    type = BIGINT
    data = 248;
(省略)
```

分離レベルが表示される

パラメーターマーカー値が表示される

WLM_SET_CLIENT_INFO ストアード・プロシージャー

```
>>-WLM_SET_CLIENT_INFO--(--client-userid--,--client_wrkstnname--, --client_applname--,
                          --client-acctstr--, --client-workload--)--<
```

- DB2サーバーでの現行接続に関連付けられたクライアント情報を設定可能
  - アプリケーションの言語に依存せず、クライアント情報を設定可能
  - 監査レコードにも表示される
  - 設定可能なクライアント情報
    - client_userid　　:クライアントのユーザーIDを指定する
    - client_wrkstnname　　:クライアントのワークステーション名を指定する
    - client_applname :クライアントのアプリケーション名を指定する
    - client_acctstr　:クライアントの計系情報ストリングを指定する
    - client_workload　:クライアントのワークロードの割り当てを指定する
  - 権限
    - WLM_SET_CLIENT_INFOプロシージャーに対するEXECUTE特権が必要

WLM_SET_CLIENT_INFO ストアード・プロシージャー 実行例

```
timestamp=2008-06-26-13.58.57.559318;
  category=EXECUTE;
  audit event=STATEMENT;
  event correlator=16;
  event status=0;
  database=TPCC;
  userid=db2inst5;
  authid=DB2INST5;
  session authid=DB2INST5;
  origin node=0;
  coordinator node=0;
  application id=9.188.198.119.38230.08062602423;
  application name=db2bp;
  client userid=db2admin;
  client workstation name=machine.makuhari.ibm.com;
  client application name=administrator;
  client accounting string=IMdepartment;
  package schema=DB2INST5;
  package name=SQLC2G13;
  package section=201;
  local transaction id=0x0000000000c3bdb0;
  global transaction id=0x00000000000000000000000000000000000000000000;
  uow id=4;
  activity id=1;
  statement invocation id=0;
  statement nesting level=0;
  activity type=READ_DML;
  statement text=select * from warehouse;
  statement isolation level=CS;
```

接続ユーザーは db2inst5

```
query optimization: 5
    min dec div 3: NO
    degree: 1
    SQL rules: DB2
    refresh age: +00000000000000.000000
    resolution timestamp: 2008-06-26-13.58.57.000000
    federated asynchrony: 0
    schema: DB2INST5
    maintained table type: SYSTEM;
  rows modified=0;
  rows returned=5;
```

以下のクライアント情報の設定が監査レコードに反映されている

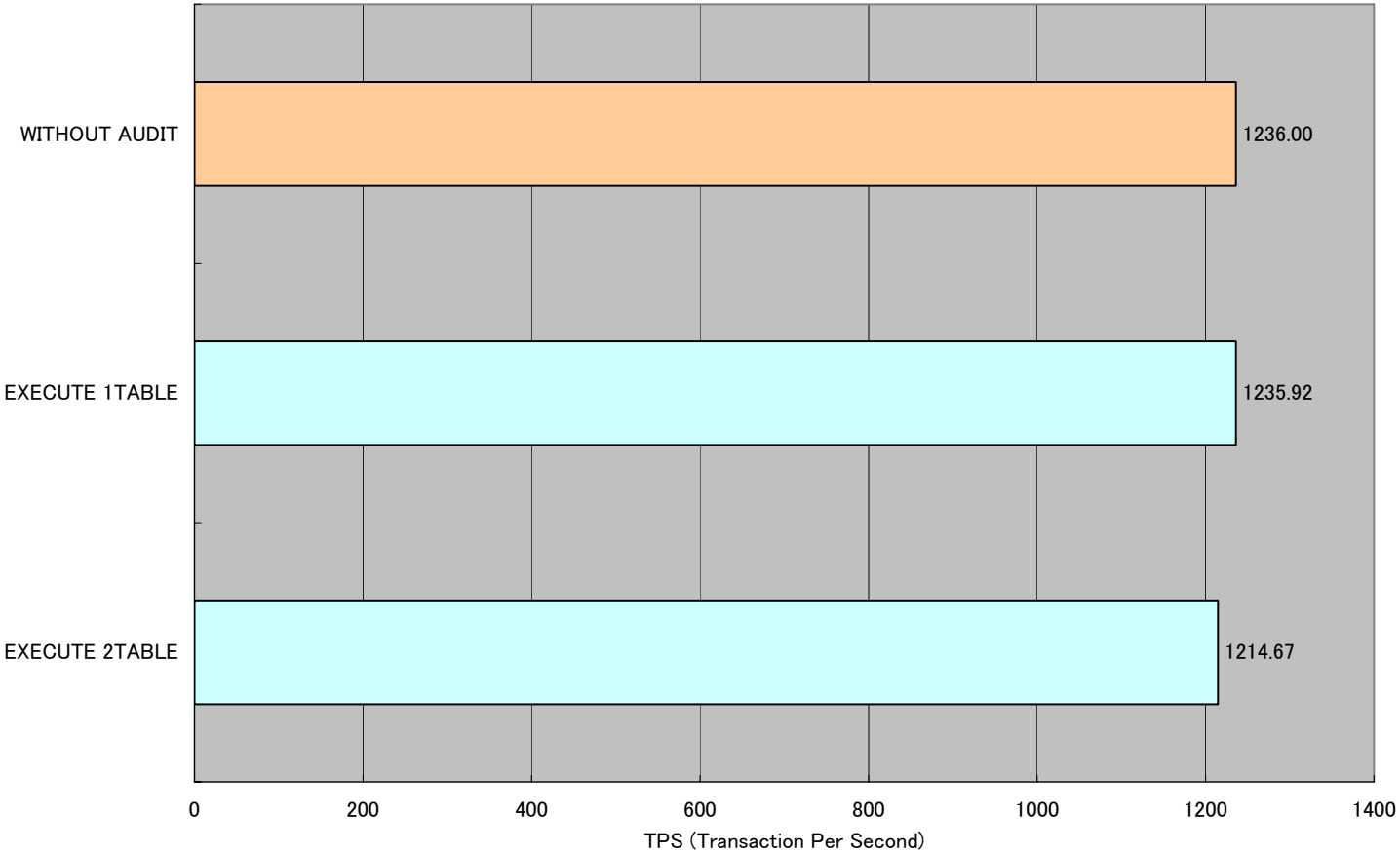
db2 "call sysproc.wlm_set_client_info ('db2admin', 'machine.makuhari.ibm.com', 'administrator', 'IMdepartment', NULL)“

AUDITパフォーマンス検証結果

＜第1.0版　2008年4月＞

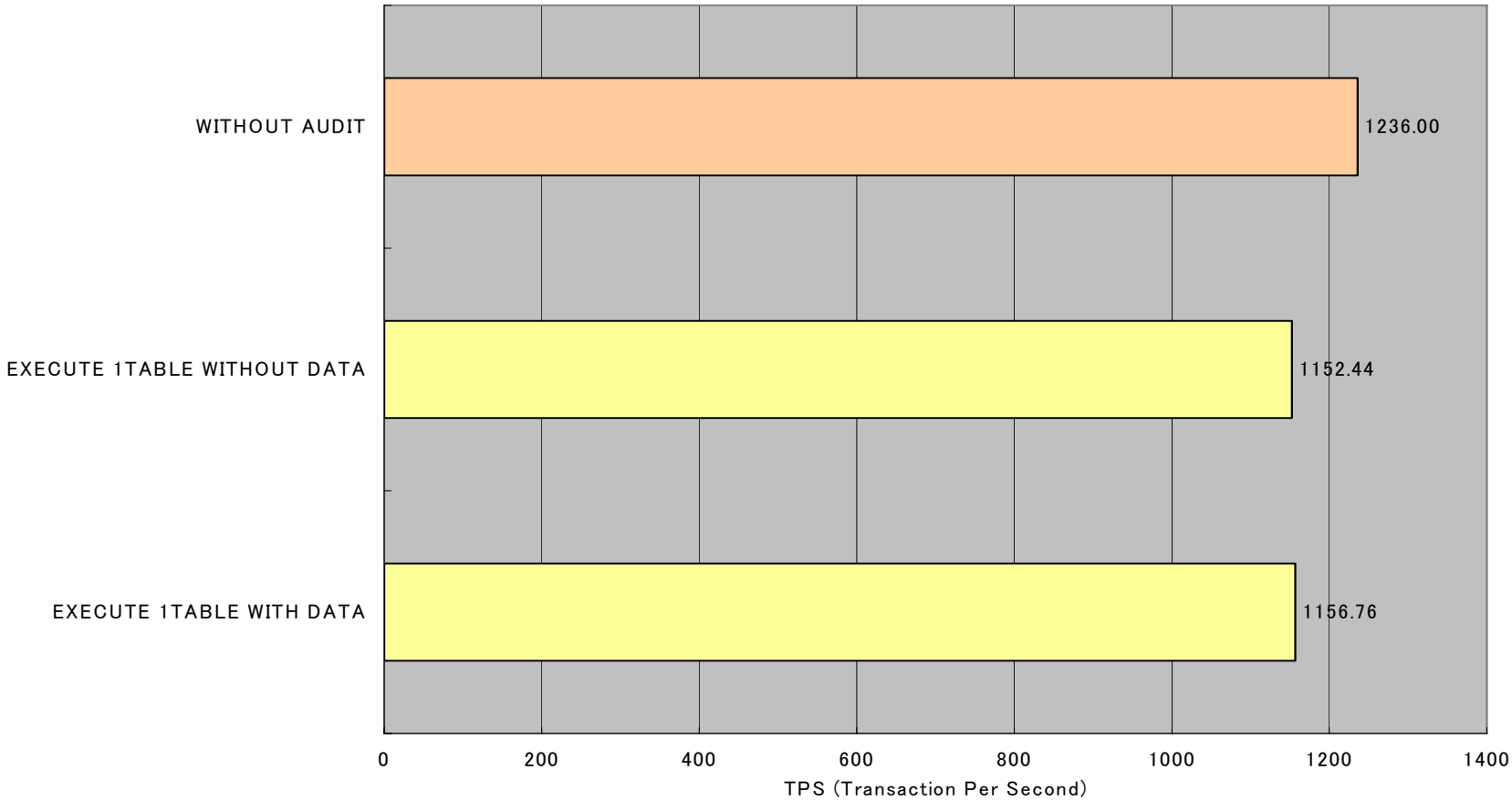
お断り：当資料は、DB2 Universal Database for Linux, UNIX and Windows V8.2, DB2 for Linux, UNIX and Windows V9.1, V9.5 をベースに作成されています。

監査対象の表数調整時のパフォーマンス



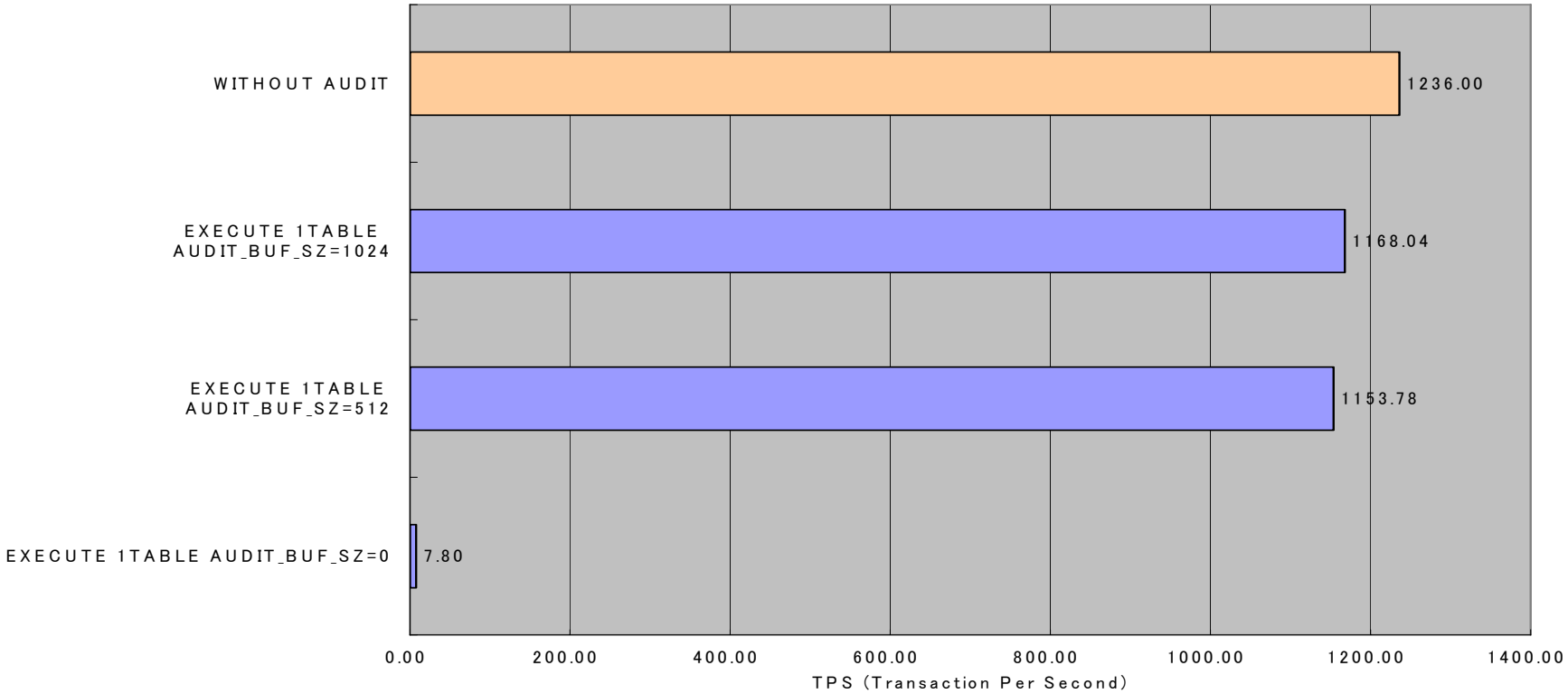
WITHOUT AUDIT	監査機能を使用しない場合
EXECUTE 1TABLE	EXECUTEカテゴリーで1表を監査した場合
EXECUTE 2TABLE	EXECUTEカテゴリーで2表を監査した場合

パラメーター・マーカー取得時・非取得のパフォーマンス



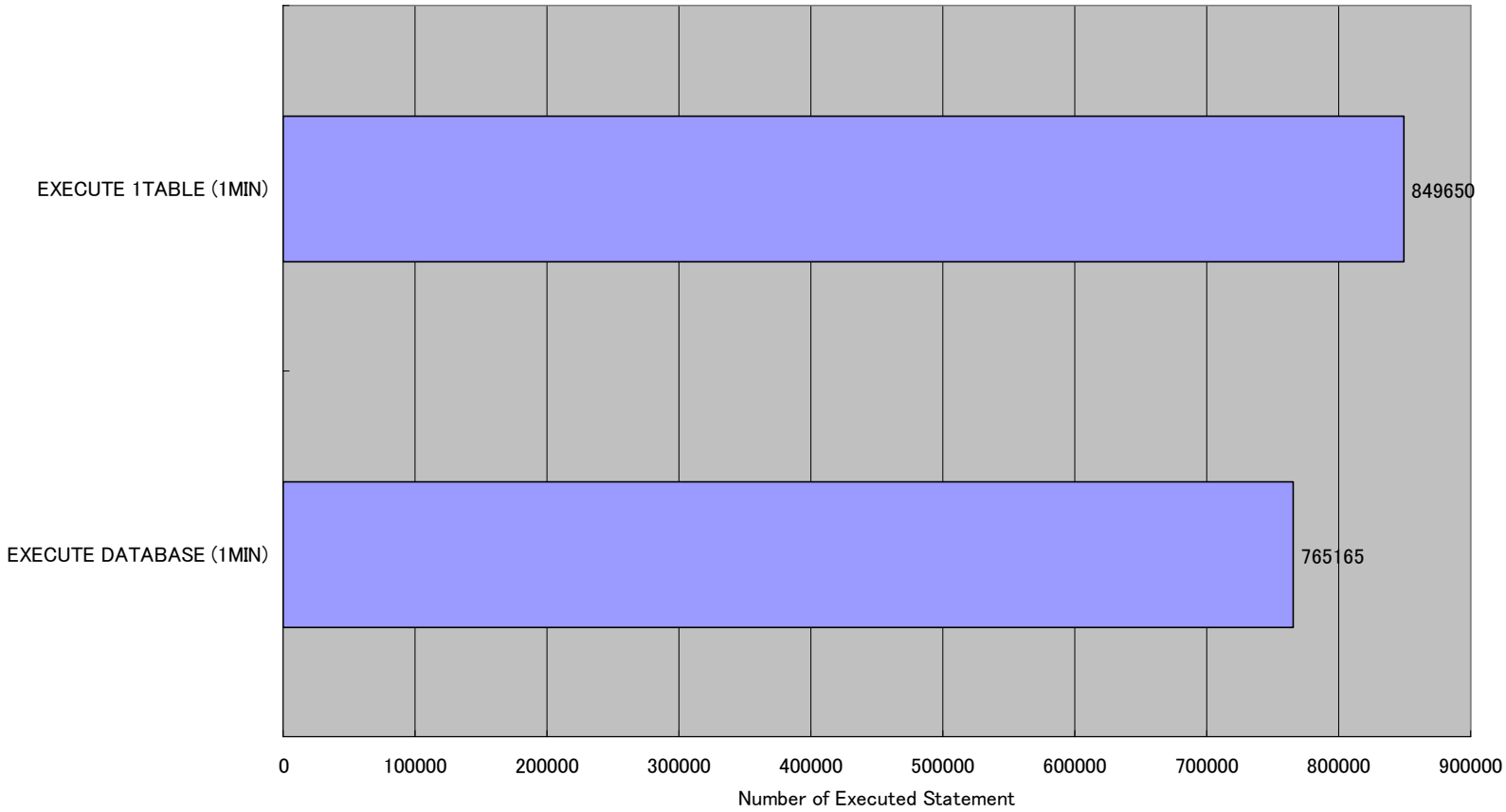
WITHOUT AUDIT	監査機能を使用しない場合
EXECUTE 1TABLE WITH DATA	EXECUTEカテゴリーで1表を監査し、パラメーター・マーカーを取得する場合
EXECUTE 1TABLE WITHOUT DATA	EXECUTEカテゴリーで1表を監査し、パラメーター・マーカーを取得しない場合

AUDIT_BUF_SZ調整時のパフォーマンス



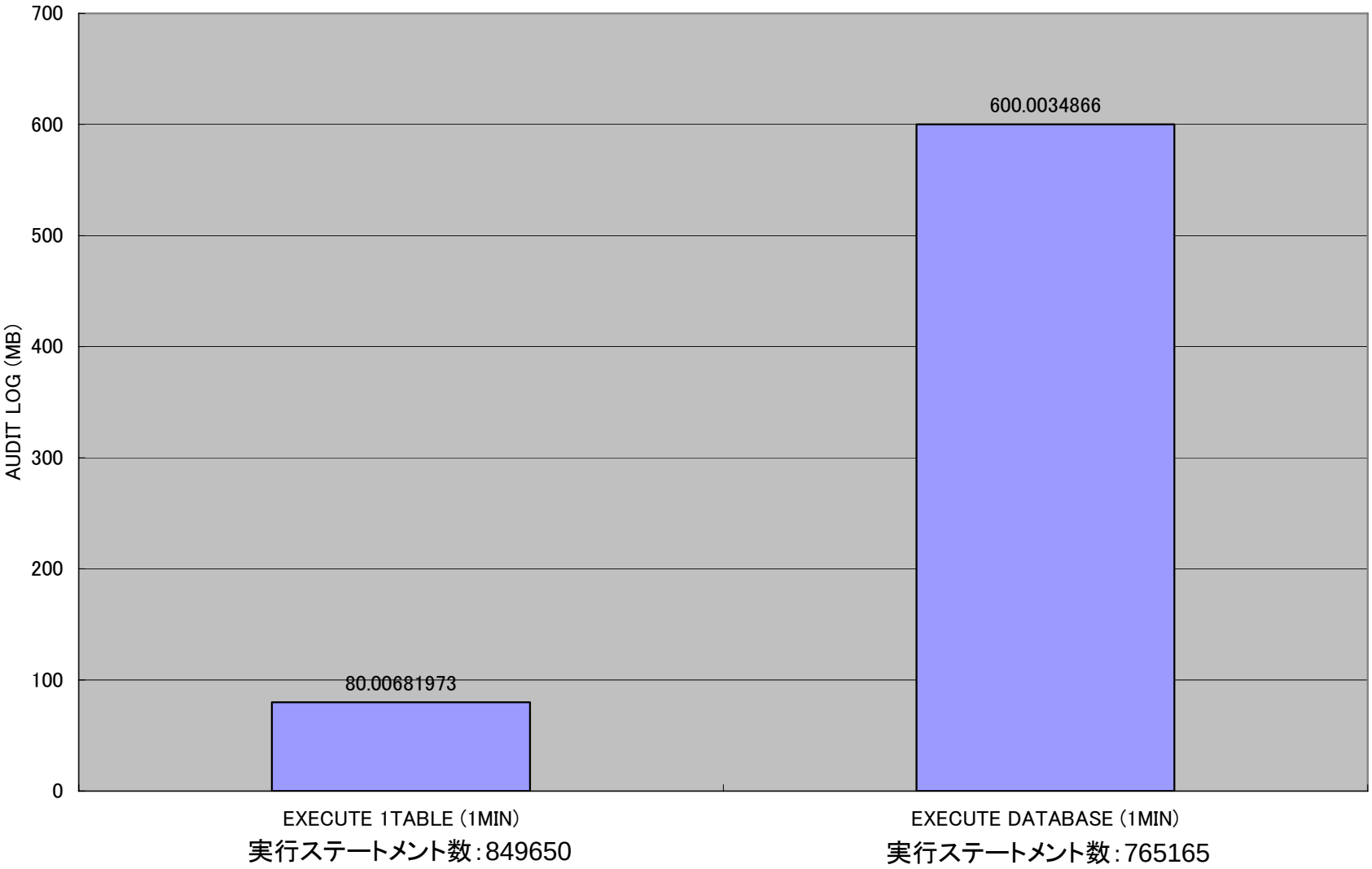
WITHOUT AUDIT	監査機能を使用しない場合
EXECUTE 1TABLE AUDIT_BUF_SZ=1024	AUDIT_BUF_SZ=1024に設定し、EXECUTEカテゴリーで1表を監査した場合
EXECUTE 1TABLE AUDIT_BUF_SZ=512	AUDIT_BUF_SZ=512に設定し、EXECUTEカテゴリーで1表を監査した場合
EXECUTE 1TABLE AUDIT_BUF_SZ=0	AUDIT_BUF_SZ=0に設定し、EXECUTEカテゴリーで1表を監査した場合

１表監査時とDB監査時の実行ステートメント数（１分間あたり）



EXECUTE 1TABLE (1MIN)	EXECUTEカテゴリーで１表を監査した場合 （1分間）
EXECUTE DATABASE (1MIN)	EXECUTEカテゴリーでDBを監査した場合 （1分間）

1表監査時とDB監査時の監査ログ量（1分間あたり）



実行ステートメント数：849650

実行ステートメント数：765165

監査レコードのフォーマット

＜第1.0版　2008年4月＞

お断り：当資料は、DB2 Universal Database for Linux, UNIX and Windows V8.2, DB2 for Linux, UNIX and Windows V9.1, V9.5 をベースに作成されています。

監査レコード・フォーマット

- 以下のページは各カテゴリで書かれるレコードのフォーマットです。
  - AUDIT
  - CHECKING
  - OBJMAINT
  - SECMAINT
  - SYSADMIN
  - VALIDATE
  - CONTEXT
  - EXECUTE

- 各レコードの以下のフィールドの値の一覧はInformation Centerの以下のページをご覧ください。
  - CHECKING, OBJMAINT, SECMAINTで操作対象となるオブジェクトの種類(OBJECT TYPEフィールドに記録される):「監査レコード・オブジェクト・タイプ 」
    http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.sec.doc/doc/r0011124.html
  - CHECKINGレコードの「AccessApprovalReason」フィールドの値:「有効な CHECKING アクセス承認理由のリスト」
    http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.sec.doc/doc/r0005641.html
  - CHECKINGレコードの「AccessAttempted」フィールドの値:「有効な CHECKING アクセス試行タイプのリスト」
    http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.sec.doc/doc/r0005643.html
  - SECMAINTレコードの「Privilege または Authority」フィールドの値:「有効な SECMAINT 特権または権限のリスト
    http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.admin.sec.doc/doc/r0005678.html

監査レコード – AUDIT

AUDIT カテゴリーのイベント

- ALTER_AUDIT_POLICY
- ARCHIVE
- AUDIT_REMOVE
- AUDIT_REPLACE
- AUDIT_USING
- CONFIGURE
- CREATE_AUDIT_POLICY
- DB2AUD
- DROP_AUDIT_POLICY
- EXTRACT
- FLUSH
- LIST_LOGS
- PRUNE (バージョン 9.5 以降では生成されません)
- START
- STOP
- UPDATE_ADMIN_CFG

監査レコード – AUDIT

名前	フォーマット	記述
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 AUDIT
Audit Event	VARCHAR(32)	可能な値のリストについては、監査イベントの AUDIT カテゴリーのセクションを参照してください。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR(255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。

監査レコード – AUDIT

名前	フォーマット	記述
Package Version	VARCHAR(64)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。
Policy Name	VARCHAR(128)	監査ポリシー名。
Policy Association Object Type	CHAR(1)	監査ポリシーを関連付けるオブジェクトのタイプ。可能な値は以下のとおりです。 N = ニックネーム S = MQT T = 表 (非型付き) i = 許可 ID g = 権限 x = トラステッド・コンテキスト ブランク = データベース

監査レコード – AUDIT

名前	フォーマット	記述
Policy Association Subobject Type	CHAR(1)	監査ポリシーを関連付けるサブオブジェクトのタイプ。オブジェクト・タイプが i (許可 ID) の場合、可能な値は以下のとおりです。 U = ユーザー G = グループ R = ロール
Policy Association Object Name	VARCHAR(128)	監査ポリシーを関連付けるオブジェクトの名前。
Policy Association Object Schema	VARCHAR(128)	監査ポリシーを関連付けるオブジェクトのスキーマ名。「Policy Association Object Type」で、スキーマが適用されないオブジェクトが識別されている場合は、NULL になります。
Audit Status	CHAR(1)	監査ポリシーの AUDIT 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Checking Status	CHAR(1)	監査ポリシーの CHECKING 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Context Status	CHAR(1)	監査ポリシーの CONTEXT 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Execute Status	CHAR(1)	監査ポリシーの EXECUTE 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Execute With Data	CHAR(1)	監査ポリシーの EXECUTE 区分の WITH DATA オプション。可能な値は以下のとおりです。 Y - WITH DATA N - WITHOUT DATA

監査レコード – AUDIT

名前	フォーマット	記述
Objmaint Status	CHAR(1)	監査ポリシーの OBJMAINT 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Secmaint Status	CHAR(1)	監査ポリシーの SECMAINT 区分の状況。可能な値については、「Audit Status」フィールドを参照してください。
Sysadmin Status	CHAR(1)	監査ポリシーの SYSADMIN 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Validate Status	CHAR(1)	監査ポリシーの VALIDATE 区分の状況。可能な値は以下のとおりです。 B- 両方 F- 失敗 N- なし S- 成功
Error Type	CHAR(8)	監査ポリシーのエラー・タイプ。可能な値は AUDIT および NORMAL です。
Data Path	VARCHAR(1024)	**db2audit configure** コマンドで指定されたアクティブ監査ログのパス。
Archive Path	VARCHAR(1024)	**db2audit configure** コマンドで指定されたアーカイブされた監査ログのパス。

監査レコード – CHECKING

- CHECKING カテゴリーのイベント
  - CHECKING_FUNCTION
  - CHECKING_MEMBERSHIP_IN_ROLES
  - CHECKING_OBJECT
  - CHECKING_TRANSFER

監査レコード - CHECKING

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 CHECKING
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。

監査レコード - CHECKING

名前	フォーマット	説明
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section Number	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。
Object Schema	VARCHAR(128)	監査イベントの生成対象となったオブジェクトのスキーマ。
Object Name	VARCHAR(128)	監査イベントの生成対象となったオブジェクトの名前。
Object Type	VARCHAR(32)	監査イベントの生成対象となったオブジェクトのタイプ。有効な値は、『監査レコード・オブジェクト・タイプ』というトピックに示されています。
Access Approval Reason	CHAR(18)	アクセスがこの監査イベントで承認された理由を示します。可能な値については、『有効な CHECKING アクセス承認理由のリスト』というトピックに示されています。
Access Attempted	CHAR(18)	試みられたアクセスのタイプを示します。可能な値については、『有効な CHECKING アクセス試行タイプのリスト』というトピックに示されています。
Package Version	VARCHAR (64)	監査イベントが発生した時点で使用されていたパッケージのバージョン。
Checked Authorization ID	VARCHAR(128)	許可 ID は監査イベント時の許可 ID と異なる場合にチェックされます。例えば、これは TRANSFER OWNERSHIP ステートメントのターゲット所有者などです。 監査イベントが SWITCH_USER である場合、このフィールドには、切り替え後の許可 ID が表示されます。

監査レコード – CHECKING

名前	フォーマット	説明
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。

監査レコード – OBJEMAINT

- OBJMAINT カテゴリーのイベント
  - ALTER_OBJECT (保護表を変更するときにのみ生成される)
  - CREATE_OBJECT
  - DROP_OBJECT
  - RENAME_OBJECT

監査レコード – OBJEMAINT

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 OBJMAINT
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。

監査レコード – OBJEMAINT

名前	フォーマット	説明
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR (256)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section Number	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。
Object Schema	VARCHAR(128)	監査イベントの生成対象となったオブジェクトのスキーマ。
Object Name	VARCHAR(128)	監査イベントの生成対象となったオブジェクトの名前。
Object Type	VARCHAR(32)	監査イベントの生成対象となったオブジェクトのタイプ。有効な値は、『監査レコード・オブジェクト・タイプ』というトピックに示されています。
Package Version	VARCHAR (64)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
Security Policy Name	VARCHAR(128)	オブジェクト・タイプが TABLE でその表がセキュリティー・ポリシーに関連している場合、そのセキュリティー・ポリシーの名前。
Alter Action	VARCHAR(32)	特定の変更操作 可能な値は以下のとおりです。 ADD_PROTECTED_COLUMN,ADD_COLUMN_PROTECTION,DROP_COLUMN_PROTECTION,ADD_ROW_PROTECTION ADD_SECURITY_POLICY,ADD_ELEMENT,ADD COMPONENT,USE GROUP AUTHORIZATIONS,IGNORE GROUP AUTHORIZATIONS USE ROLE AUTHORIZATIONS,IGNORE ROLE AUTHORIZATIONS, OVERRIDE NOT AUTHORIZED WRITE SECURITY LABEL.RESTRICT NOT AUTHORIZED WRITE SECURITY LABEL

監査レコード – OBJEMAINT

名前	フォーマット	説明
Protected Column Name	VARCHAR(128)	Alter Action が ADD_COLUMN_PROTECTION または DROP_COLUMN_PROTECTION の場合、これは影響される列の名前です。
Column Security Label	VARCHAR(128)	フィールド Column Name で指定された列を保護するセキュリティー・ラベル。
Security Label Column Name	VARCHAR(128)	行を保護するセキュリティー・ラベルを含む列の名前。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。

監査レコード – SECMAINT

SECMAINT カテゴリーのイベント

- ADD_DEFAULT_ROLE
- ADD_USER
- ALTER_DEFAULT_ROLE
- ALTER SECURITY POLICY
- ALTER_USER_ADD_ROLE
- ALTER_USER_AUTHENTICATION
- ALTER_USER_DROP_ROLE
- DROP_DEFAULT_ROLE
- DROP_USER
- GRANT
- IMPLICIT_GRANT
- IMPLICIT_REVOKE
- REVOKE
- SET_SESSION_USER
- TRANSFER_OWNERSHIP
- UPDATE_DBM_CFG

監査レコード – SECMAINT

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 SECMAINT
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。

監査レコード - SECMAINT

名前	フォーマット	説明
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section Number	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。
Object Schema	VARCHAR(128)	監査イベントの生成対象となったオブジェクトのスキーマ。 オブジェクト・タイプ・フィールドが ACCESS_RULE なら、このフィールドには規則に関連したセキュリティー・ポリシー名が含まれます。規則の名前はオブジェクト名のフィールドに格納されます。 オブジェクト・タイプ・フィールドが SECURITY_LABEL なら、このフィールドにはセキュリティー・ラベルがその一部であるセキュリティー・ポリシーの名前が含まれます。セキュリティー・ラベルの名前はオブジェクト名のフィールドに格納されます。
Object Name	VARCHAR(128)	監査イベントの生成対象となったオブジェクトの名前。 監査イベントが ADD_DEFAULT_ROLE、DROP_DEFAULT_ROLE、ALTER_DEFAULT_ROLE、ADD_USER, DROP_USER、ALTER_USER_ADD_ROLE、ALTER_USER_DROP_ROLE、または ALTER_USER_AUTHENTICATION のいずれかである場合に、ロール名を示します。 オブジェクト・タイプ・フィールドが ACCESS_RULE なら、このフィールドには規則の名前が含まれます。規則に関連するセキュリティー・ポリシーの名前はオブジェクト・スキーマのフィールドに格納されます。 オブジェクト・タイプ・フィールドが SECURITY_LABEL なら、このフィールドにはセキュリティー・ラベルの名前が含まれます。セキュリティー・ポリシーの一部である名前はオブジェクト・スキーマのフィールドに格納されます。
Object Type	VARCHAR(32)	監査イベントの生成対象となったオブジェクトのタイプ。有効な値は、『監査レコード・オブジェクト・タイプ』というトピックに示されています。 監査イベントが ADD_DEFAULT_ROLE、DROP_DEFAULT_ROLE、ALTER_DEFAULT_ROLE、ADD_USER、DROP_USER、ALTER_USER_ADD_ROLE、ALTER_USER_DROP_ROLE、および ALTER_USER_AUTHENTICATION のいずれかである場合、値は ROLE です。

監査レコード – SECMAINT

名前	フォーマット	説明
Grantor	VARCHAR(128)	特権や権限の付与または取り消しを行う ID。
Grantee	VARCHAR(128)	特権または権限が付与または取り消された被認可者の ID。 監査イベントが ADD_DEFAULT_ROLE、DROP_DEFAULT_ROLE、ALTER_DEFAULT_ROLE、ADD_USER, DROP_USER、ALTER_USER_ADD_ROLE、ALTER_USER_DROP_ROLE、または ALTER_USER_AUTHENTICATION のいずれかである場合に、トラステッド・コンテキスト・オブジェクトを示します。
Grantee Type	VARCHAR(32)	付与または取り消された被認可者のタイプ。可能な値は USER、GROUP、ROLE、AMBIGUOUS、または、監査イベントが ADD_DEFAULT_ROLE、DROP_DEFAULT_ROLE、ALTER_DEFAULT_ROLE、ADD_USER、DROP_USER、ALTER_USER_ADD_ROLE、ALTER_USER_DROP_ROLE、または ALTER_USER_AUTHENTICATION のいずれかである場合には TRUSTED_CONTEXT です。
Privilege または Authority	CHAR(18)	付与または取り消された特権または権限のタイプを示します。有効な値は、『有効な SECMAINT 特権または権限のリスト』というトピックに示されています。 監査イベントが ADD_DEFAULT_ROLE、DROP_DEFAULT_ROLE、ALTER_DEFAULT_ROLE、ADD_USER、DROP_USER、ALTER_USER_ADD_ROLE、ALTER_USER_DROP_ROLE、または ALTER_USER_AUTHENTICATION のいずれかである場合、値は ROLE MEMBERSHIP です。
Package Version	VARCHAR (64)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
アクセス・タイプ	VARCHAR(32)	セキュリティー・ラベルが付与されるアクセス・タイプ。 可能な値: READ、WRITE、ALL セキュリティー・ポリシーが変更されるアクセス・タイプ。可能な値: USE GROUP AUTHORIZATIONS IGNORE GROUP AUTHORIZATIONS USE ROLE AUTHORIZATIONS IGNORE ROLE AUTHORIZATIONS OVERRIDE NOT AUTHORIZED WRITE SECURITY LABEL RESTRICT NOT AUTHORIZED WRITE SECURITY LABEL

監査レコード – SECMAINT

名前	フォーマット	説明
Assumable Authid	VARCHAR(128)	付与される特権が SETSESSIONUSER 特権のとき、これは被認可者がセッション・ユーザーとして設定されることが可能な許可 ID です。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Grantor Type	VARCHAR(32)	付与者のタイプ。可能な値は、USER です。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context User	VARCHAR(128)	監査イベントが ADD_USER または DROP_USER であるときに、トラステッド・コンテキスト・ユーザーを識別する。
Trusted Context User Authentication	INTEGER	監査イベントが ADD_USER、DROP_USER、または ALTER_USER_AUTHENTICATION であるときに、トラステッド・コンテキスト・ユーザーの認証設定を示す。 1 : 認証が必要、0 : 認証は不要
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。

監査レコード – SYSADMIN

- SYSADMIN カテゴリーのイベント①
  - START_DB2
  - STOP_DB2
  - CREATE_DATABASE
  - ALTER_DATABASE
  - DROP_DATABASE
  - UPDATE_DBM_CFG
  - UPDATE_DB_CFG
  - CREATE_TABLESPACE
  - DROP_TABLESPACE
  - ALTER_TABLESPACE
  - RENAME_TABLESPACE
  - CREATE_NODEGROUP
  - DROP_NODEGROUP
  - ALTER_NODEGROUP
  - CREATE_BUFFERPOOL
  - DROP_BUFFERPOOL
  - ALTER_BUFFERPOOL
  - CREATE_EVENT_MONITOR
  - DROP_EVENT_MONITOR
  - ENABLE_MULTIPAGE
  - MIGRATE_DB_DIR
  - DB2TRC
  - DB2SET
  - ACTIVATE_DB
  - ADD_NODE
  - BACKUP_DB
  - CATALOG_NODE
  - CATALOG_DB
  - CATALOG_DCS_DB
  - CHANGE_DB_COMMENT
  - DEACTIVATE_DB
  - DROP_NODE_VERIFY
  - FORCE_APPLICATION
  - GET_SNAPSHOT
  - LIST_DRDA_INDOUBT_TRANSACTIONS
  - MIGRATE_DB
  - RESET_ADMIN_CFG
  - RESET_DB_CFG
  - RESET_DBM_CFG
  - RESET_MONITOR
  - RESTORE_DB

監査レコード – SYSADMIN

- SYSADMIN カテゴリーのイベント②
  - ROLLFORWARD_DB
  - SET_RUNTIME_DEGREE
  - SET_TABLESPACE_CONTAINERS
  - UNCATALOG_DB
  - UNCATALOG_DCS_DB
  - UNCATALOG_NODE
  - UPDATE_ADMIN_CFG
  - UPDATE_MON_SWITCHES
  - LOAD_TABLE
  - DB2AUDIT
  - SET_APPL_PRIORITY
  - CREATE_DB_AT_NODE
  - KILLDBM
  - MIGRATE_SYSTEM_DIRECTORY
  - DB2REMOT
  - DB2AUD
  - MERGE_DBM_CONFIG_FILE
  - UPDATE_CLI_CONFIGURATION
  - OPEN_TABLESPACE_QUERY
  - SINGLE_TABLESPACE_QUERY
  - CLOSE_TABLESPACE_QUERY
  - FETCH_TABLESPACE
  - OPEN_CONTAINER_QUERY
  - FETCH_CONTAINER_QUERY
  - CLOSE_CONTAINER_QUERY
  - GET_TABLESPACE_STATISTICS
  - DESCRIBE_DATABASE
  - ESTIMATE_SNAPSHOT_SIZE
  - READ_ASYNC_LOG_RECORD
  - PRUNE_RECOVERY_HISTORY
  - UPDATE_RECOVERY_HISTORY
  - QUIESCE_TABLESPACE
  - UNLOAD_TABLE
  - UPDATE_DATABASE_VERSION
  - CREATE_INSTANCE
  - DELETE_INSTANCE
  - SET_EVENT_MONITOR
  - GRANT_DBADM
  - REVOKE_DBADM
  - GRANT_DB_AUTHORITIES
  - REVOKE_DB_AUTHORITIES
  - REDISTRIBUTE_NODEGROUP

監査レコード – SYSADMIN

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 SYSADMIN
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。

監査レコード – SYSADMIN

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 SYSADMIN
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。

監査レコード – VALIDATE

- VALIDATE カテゴリーのイベント
  - AUTHENTICATE
  - CHECK_GROUP_MEMBERSHIP (バージョン 9.5 以降では生成されません)
  - GET_USERMAPPING_FROM_PLUGIN
  - GET_GROUPS (バージョン 9.5 以降では生成されません)
  - GET_USERID (バージョン 9.5 以降では生成されません)

監査レコード – VALIDATE

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 VALIDATE
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。 成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。
Execution ID	VARCHAR(1024)	監査イベントの時刻で使用していた実行 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。

監査レコード – VALIDATE

名前	フォーマット	説明
Authentication Type	VARCHAR(32)	監査イベントの時刻での認証タイプ。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section Number	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。
Package Version	VARCHAR (64)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
Plug-in Name	VARCHAR(32)	監査イベントが発生した時点で使用されていたプラグインの名前。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド・コンテキストを介して継承したロールの名前。

監査レコード – EXECUTE

EXECUTE カテゴリーのイベント

- COMMIT: COMMIT ステートメントの実行。
- CONNECT: データベース接続の確立。
- CONNECT RESET: データベース接続の終了。
- DATA: ステートメント用のホスト変数またはパラメーター・マーカーのデータ値。
  - このイベントは、ステートメントに含まれる各ホスト変数やパラメーター・マーカーごとに繰り返されます。DATA は、区切りファイルから監査ログを抽出するときにのみ表示されます。

- GLOBAL COMMIT: グローバル・トランザクション内での COMMIT の実行。
- GLOBAL ROLLBACK: グローバル・トランザクション内での ROLLBACK の実行。
- RELEASE SAVEPOINT: RELEASE SAVEPOINT ステートメントの実行。
- ROLLBACK: ROLLBACK ステートメントの実行。
- SAVEPOINT: SAVEPOINT ステートメントの実行。
- STATEMENT: SQL ステートメントの実行。
- SWITCH USER: トラステッド接続内でのユーザーの切り替え。

監査レコード – EXECUTE

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は EXECUTE です。
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Event Status	INTEGER	監査イベントの状況、次のような 1 つの SQLCODE で表されます。成功イベント > = 0 失敗イベント < 0
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。
Authorization ID	VARCHAR(128)	監査イベントの時刻でのステートメント許可 ID。
Session Authorization ID	VARCHAR(128)	監査イベントの時刻でのセッション許可 ID。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。
Client User ID	VARCHAR (255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Accounting String	VARCHAR (255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Client Workstation Name	VARCHAR (255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。

監査レコード – EXECUTE

名前	フォーマット	説明
Client Application Name	VARCHAR (255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION およびEXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。
Package Version	VARCHAR(164)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
UOW ID	BIGINT	アクティビティーが発生した作業単位の ID。この値は、作業単位ごとにアプリケーション ID 内で固有です。
Activity ID	BIGINT	作業単位内で固有のアクティビティー ID。
Statement Invocation ID	BIGINT	SQL ステートメントが実行されたルーチン呼び出しの ID。値は、アプリケーションで現行のネスティング・レベルがアクティブであったときに発生した、そのレベルでのルーチン呼び出しの数を示します。このエレメントを「Statement Nesting Level」と合わせて使用することにより、特定の SQL ステートメントの呼び出しを一意的に識別することができます。

監査レコード – EXECUTE

名前	フォーマット	説明
Statement Nesting Level	BIGINT	ステートメントが実行されていたときに有効であったネスティングまたは再帰のレベル。ネスティングの各レベルは、ストアード・プロシージャーやユーザー定義関数 (UDF) のネストされた、または再帰可能な呼び出しに対応しています。
Activity Type	VARCHAR(32)	アクティビティーのタイプ。 可能な値は以下のとおりです。 READ_DML,WRITE_DML,DDL,CALL,NONE
Statement Text	CLOB(8M)	適用できる場合には、SQL または XQuery ステートメントのテキストです。
Statement Isolation Level	CHAR(8)	ステートメントが実行されていたときに有効であった分離の値。 可能な値は以下のとおりです。 NONE (分離の指定なし) UR (非コミット読み取り) CS (カーソル固定) RS (読み取り固定) RR (反復可能読み取り)
Compilation Environment Description	BLOB(8K)	SQL ステートメントのコンパイル時に使用されたコンパイル環境。このエレメントは、COMPILATION_ENV 表関数または SET COMPILATION ENVIRONMENT SQL ステートメントに入力として渡すことができます。

監査レコード – EXECUTE

名前	フォーマット	説明
Rows Modified	INTEGER	以下の両方の結果として削除、挿入、または更新された行の総数。 削除操作成功後の制約の強制 アクティブにされたトリガーが起動した SQL ステートメントの処理 コンパウンド SQL が呼び出される場合は、すべてのサブステートメントの、これに該当する行の数の集計が含まれます。場合によっては、エラーが発生したときに、内部エラーを示す負の値がこのフィールドに表示されることがあります。この値は、SQLCA の sqlerrd(5) フィールドと等価です。
Rows Returned	BIGINT	ステートメントによって戻される行の総数。
Savepoint ID	BIGINT	ステートメントが実行されていたときにそのステートメントで有効であったセーブポイント ID。「Audit Event」が SAVEPOINT、RELEASE_SAVEPOINT、または ROLLBACK_SAVEPOINT である場合、「Savepoint ID」は、それぞれ設定、解放、またはロールバックされるセーブポイントになります。
Statement Value Index	INTEGER	SQL ステートメントで使用される入力パラメーター・マーカーまたはホスト変数の位置。
Statement Value Type	CHAR(16)	SQL ステートメントに関連付けられているデータ値のタイプのストリング表現。可能な値の例としては、INTEGER や CHAR が挙げられます。
Statement Value Data	CLOB(128K)	SQL ステートメントへのデータ値のストリング表現。LOB、LONG、XML、および構造化タイプのパラメーターは表示されません。日付、時刻、およびタイム・スタンプのフィールドは、ISO 形式で記録されます。

監査レコード – CONTEXT

- CONTEXT カテゴリーのイベント①
  - CONNECTCONNECT_RESET
  - ATTACH
  - DETACH
  - DARI_START
  - DARI_STOP
  - BACKUP_DB
  - RESTORE_DB
  - ROLLFORWARD_DB
  - OPEN_TABLESPACE_QUERY
  - FETCH_TABLESPACE
  - CLOSE_TABLESPACE_QUERY
  - OPEN_CONTAINER_QUERY
  - CLOSE_CONTAINER_QUERY
  - FETCH_CONTAINER_QUERY
  - SET_TABLESPACE_CONTAINERS
  - GET_TABLESPACE_STATISTIC
  - READ_ASYNC_LOG_RECORD
  - QUIESCE_TABLESPACE
  - LOAD_TABLE
  - UNLOAD_TABLE
  - UPDATE_RECOVERY_HISTORY
  - PRUNE_RECOVERY_HISTORY
  - SINGLE_TABLESPACE_QUERY
  - LOAD_MSG_FILE
  - UNQUIESCE_TABLESPACE
  - ENABLE_MULTIPAGE
  - DESCRIBE_DATABASE
  - DROP_DATABASE
  - CREATE_DATABASE
  - ADD_NODE
  - FORCE_APPLICATION

監査レコード – CONTEXT

CONTEXT カテゴリーのイベント②

- SET_APPL_PRIORITY
- RESET_DB_CFG
- GET_DB_CFG
- GET_DFLT_CFG
- UPDATE_DBM_CFG
- SET_MONITOR
- GET_SNAPSHOT
- ESTIMATE_SNAPSHOT_SIZE
- RESET_MONITOR
- OPEN_HISTORY_FILE
- CLOSE_HISTORY_FILE
- FETCH_HISTORY_FILE
- SET_RUNTIME_DEGREE
- UPDATE_AUDIT
- DBM_CFG_OPERATION
- DISCOVER
- OPEN_CURSOR
- CLOSE_CURSOR
- FETCH_CURSOR
- EXECUTE
- EXECUTE_IMMEDIATE
- PREPARE
- DESCRIBE
- BIND
- REBIND
- RUNSTATS
- REORG
- REDISTRIBUTE
- COMMIT
- ROLLBACK
- REQUEST_ROLLBACK
- IMPLICIT_REBIND
- EXTERNAL_CANCEL
- SWITCH_USER

監査レコード – CONTEXT

名前	フォーマット	説明
Timestamp	CHAR(26)	監査イベントの日付と時刻。
カテゴリー	CHAR(8)	監査イベントの区分。可能な値は以下のとおりです。 CONTEXT
Audit Event	VARCHAR(32)	特定の監査イベント。
Event Correlator	INTEGER	監査対象の操作の相関 ID。単一イベントにどの監査レコードが関連しているかを識別するために使用できます。
Database Name	CHAR(8)	どのイベントが生成されたかを示すデータベース名。インスタンス・レベルの監査イベントであった場合にはブランクとなります。
User ID	VARCHAR(1024)	監査イベントの時刻でのユーザー ID。 監査イベントが SWITCH_USER である場合、このフィールドには、切り替え後のユーザー ID が表示されます。
Authorization ID	VARCHAR(128)	監査イベントの時刻での許可 ID。 監査イベントが SWITCH_USER である場合、このフィールドには、切り替え後の許可 ID が表示されます。
Origin Node Number	SMALLINT	監査イベントが発生したノード番号。
Coordinator Node Number	SMALLINT	コーディネーター・ノードのノード番号。
Application ID	VARCHAR (255)	監査イベントが発生した時刻で使用していたアプリケーション ID。
Application Name	VARCHAR(1024)	監査イベントが発生した時刻で使用していたアプリケーション名。
Package Schema	VARCHAR(128)	監査イベントの時刻で使用していたパッケージのスキーマ。
Package Name	VARCHAR(128)	監査イベントが発生した時刻で使用していたパッケージ名。
Package Section Number	SMALLINT	監査イベントが発生した時刻で使用されていたパッケージのセクション番号。

監査レコード – CONTEXT

名前	フォーマット	説明
Statement Text	CLOB(8M)	適用できる場合には、SQL または XQuery ステートメントのテキストです。SQL または XQuery ステートメントのテキストが使用可能でない場合、NULL となります。
Package Version	VARCHAR (64)	監査イベントが発生した時刻で使用していたパッケージのバージョン。
Local Transaction ID	VARCHAR(10) FOR BIT DATA	監査イベントが発生した時刻で使用していたローカル・トランザクション ID。これは、トランザクション・ログの一部となる SQLU_TID 構造体です。
Global Transaction ID	VARCHAR(30) FOR BIT DATA	監査イベントが発生した時刻で使用していたグローバル・トランザクション ID。これは、トランザクション・ログの一部となる SQLP_GXID 構造体のデータ・フィールドです。
Client User ID	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT USERID 特殊レジスターの値。
Client Workstation Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_WRKSTNNAME 特殊レジスターの値。
Client Application Name	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_APPLNAME 特殊レジスターの値。
Client Accounting String	VARCHAR(255)	監査イベントが発生した時刻の CURRENT CLIENT_ACCTNG 特殊レジスターの値。
Trusted Context Name	VARCHAR(128)	トラステッド接続に関連付けられたトラステッド・コンテキストの名前。
Connection Trust Type	INTEGER	可能な値は以下のとおりです。 IMPLICIT_TRUSTED_CONNECTION EXPLICIT_TRUSTED_CONNECTION
Role Inherited	VARCHAR(128)	トラステッド接続を介して継承したロール。

特記事項

- この資料に含まれる情報は可能な限り正確を期しておりますが、IBMの正式なレビューを受けておらず、当資料に記載された内容に関してIBMは何ら保証するものではありません。この情報の使用、評価、実施は使用者の責任で使用者の環境に合わせて行ってください。
- 当資料の他社情報は一般公開されている資料を参照し、一般的な視点から論じたものであり、IBMは内容および実際の稼動を保証しません。
- この情報には、技術的に不適切な記述や誤植を含む場合があります。IBM は予告なしに、随時、この文書に記載されている内容に対して、改良または変更を行うことがあります。
- 当資料をコピー等で複製することは、IBMおよび執筆者の承諾なしではできません。
- 当資料に記載された製品名または会社名はそれぞれの各社の商標または登録商標です。