ES/1 NEO

MFシリーズ

MF-AUDIT
使用者の手引き

株式会社 アイ・アイ・エム

第24版　2024年2月

目次

MF-AUDIT プロセジャー覧

MF-AUDITプロセジャはセキュリティツールのログ情報を基に、システムや資源に対するアクセス状況を示すレポート群を作成・出力します。このアクセス状況には、「不正アクセス」「未定義ユーザ」「警告」「正常アクセス」が含まれす。

プロセジャで使用するパフォーマンス・データのレコードは、各プロセジャのマニュアルをご参照ください。

プロセジャ	実行 JCL	対象 OS					評価項目					機能
		MVS OS/390 z/OS	MSP MSP-EX	XSP	VOS3	ACOS-4	CPU	メモリ	入出力	業務	その他	
AUDITPRT	JCLAUDIT	SMF	SMF		SMS						●	セキュリティツールのログ情報を基にシステム資源のアクセス情報を報告します。
DSNCSV00	JCDSNCSV	SMF	SMF		SMS				●			データセットアクセス履歴情報を CSV ファイル形式で出力します。
AUDITMON	JCLADTM0	SMF	SMF		SMS						●	月間のセキュリティツールのログ情報を基にシステム資源のアクセス情報を報告します。
PNAVIADT	JCLPNADT JCADTCSV	SMF	SMF		SMS						●	Performance Navigator 用データ（セキュリティツールログ情報）の作成、またはセキュリティツールのログ情報を CSV ファイル形式で出力します。

使用データの意味は次の通りです。

MVS, OS/390, z/OS	（IBM システム）	SMF	SMF データ
MSP, MSP-EX	（富士通 MSP,MSP-EX システム）	SMF	SMF データ
VOS3	（日立システム）	SMS	SMS データ

第1章 AUDITPRT の使用方法

AUDITPRTプロセジャは、セキュリティツールのログ情報を基に、システムや資源に対するアクセス状況を示すレポート群を作成・出力します。

このアクセス状況には、

- 〇不正アクセス
- 〇未定義ユーザ
- 〇警告
- 〇正常アクセス

などが含まれます。

また、このプロセジャを実行するにはMF-AUDIT あるいはMF-SCOPE の契約が必要となります。

このプロセジャでは、下記に示すセキュリティツールのログ情報やジョブ情報を処理対象としています。

IBM	: RACF	SMFタイプ80	
		SMFタイプ20,	SMFタイプ30サブタイプ1と5
富士通	: RACF	SMFタイプ80	
		SMFタイプ20,	SMFタイプ30サブタイプ1と5
日　立	: TRUST E2	SMSタイプ118	

各システムでは、セキュリティツールのログ情報やジョブ情報を基にしたレポート機能を提供しています。この機能では、SMF/SMSデータセットに書き出されたログ情報を変換したレコードを入力としています。

このAUDITPRTプロセジャでは、SMF/SMSデータセットに書き出されたログ情報を入力としていますので注意してください。メーカツールにより変換されたデータは入力できません。

注意

このプロセジャは入力データ量、解析対象範囲、出力レポート数などにより大量の資源を使用する場合があります。

1.1　実行パラメータ

AUDITPRTプロセジャ用のサンプル・ジョブ制御文のDD名“PLATFORM”では、プロセジャの実行パラメータ指定部とプロセジャ本体が連結データセットとして定義されてます。実行パラメータでは、入力データの選択や出力レポート群の選択を行います。この実行パラメータには、セレクション・スイッチとコントロール・スイッチがあります。

```
//AUDITPRT JOB  (ACCT),MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,NOTIFY=USERID
//JOBLIB   DD  DSN=CPE.LOAD,DISP=SHR
//*JOBCAT   DD  DSN=USER.CAT,DISP=SHR
//*********************************************************************
//*    プロダクト名 : MF-SCOPE / AUDIT   プロセジャ名 : AUDITPRT      *
//*-------------------------------------------------------------------*
//*   JCLの以下のデータセット名を変更してください。                   *
//*    ES/1 NEO LIBRARY                                               *
//*            - CPE.LOAD    ( ロードモジュールライブラリ )           *
//*            - CPE.PARM    ( ソースライブラリ )                     *
//*    INPUT   - INPUT.DATA  ( 解析対象のSMF(SMS)データ )             *
//********************************************************* SINCE V3L26 ***
//SHELL   EXEC PGM=CPESHELL,REGION=4096K
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSUT1   DD  UNIT=SYSDA,SPACE=(TRK,(10,10))
//INPUT    DD  DISP=SHR,DSN=INPUT.DATA
//PLATFORM DD  *
*
*      セレクション・スイッチ  ／  コントロール・スイッチ
*
        DATESW   = 0              日付制御 ( 0:YYDDD 1:YYMMDD )
        SEL1     = 00000          解析開始日 ( YYDDD/YYMMDD )
        SEL2     = 0000           解析開始時刻 ( HHMM )
        SEL3     = 99999          解析終了日 ( YYDDD/YYMMDD )
        SEL4     = 2400           解析終了時刻 ( HHMM )
        OSTYPE   = 1              オペレーティングシステムの種別 (1:IBM 2:FUJI 3:HITC)
*
        SW10     = 1              処理レコード・サマリー・レポート
        SW20     = 1              ジョブ開始・終了：不正アクセス・レポート
        SW21     = 1              ジョブ開始・終了：未定義ユーザ・レポート
        SW22     = 1              ジョブ開始・終了：警告レポート
        SW30     = 1              リソース・アクセス・エラー・レポート
        SW40     = 1              リソース・アクセス状況サマリー・レポート
        SW50     = 1              コマンド処理レポート
        SW51     = 1              未定義ユーザのコマンド処理レポート
        SW60     = 1              特権ユーザ利用状況レポート
        SW70     = 1              ユーザ毎の最終アクセス・レポート
        SW80     = 1              特定ユーザのトレース・レポート
        SW80OPT  = 0              ジョブ開始／終了レコードを含める
* FOR SW30,SW50,SW60,SW80
        SELDSNSW = 0              データセット名の出力指示
*                                   1:出力
* FOR SW50
        SELCMDSW = 2              コマンド選択
*                                   0:正常 1:エラー 2:両方
* FOR SW60
        TRUSTOPT = 0              リソース・アクセス情報の処理選択（日立のみ）
*                                   0:失敗したアクセスのみ  1:全てのアクセス
* FOR SW70
        SELRSCSW = 1              レコード選択
        SELNMCHK = 1              ユーザ名をキーとする（IBMのみ）
* FOR SW80
        DIM TUID(100)
        TUID     = 2
        TUID(1)  = 'ユーザID'     トレースするユーザID
        TUID(2)  = 'ユーザID'     トレースするユーザID
* OTHER
        SYSID    = '    '         システム識別コード
        ERRORCDE = 8              エラー完了コード
        NOLIST
//         DD   DSN=CPE.PARM(AUDITPRT),DISP=SHR
```

Jcl 1.1　サンプル・ジョブ制御文（JCLAUDIT）

1.1.1. セレクション・スイッチ

セレクション・スイッチでは、評価対象とするべき時間帯や追跡するべきパフォーマンス・グループ番号などを指定します。

DATESW

日付形式

SEL1やSEL3のセレクション・スイッチで指定する解析対象日の形式を指定します。DATESWがオフ(“0”)の場合はジュリアン暦(cYYDDD), オン(“1”)の場合はグレゴリアン暦(cYYMMDD)であることを指示します。日付部の年を示すcYYは、c=0が1900年代、c=1が2000年代を意味します。これらの指定を簡略化する為に、日付部の年が50未満の場合には、2000年代として認識します。ジュリアン暦は0年から99年の1日から366日を指定します。この際、日付部のチェックを行っていない為、00000から99999までの指定が可能です。しかし、グレゴリアン暦の場合、月および日をチェックしている為、矛盾のある指定を行いますとプログラムは異常終了します。この点に留意して使用してください。

SEL1～SEL4

入力データ・レンジ

解析対象とするべきSMF/SMSレコードの日時の範囲を指定します。SEL1とSEL3で指定する日付は1900年代であっても2000年代であっても、下位2桁のみをYY部で指定することも可能です。この際、YY部が00～49の場合には2000～2049年、YY部が50～99の場合には1950～1999年の 指定として解析・評価を行います。

SEL1	開始日	(形式は YYMMDD)
SEL2	開始時刻	(形式は HHMM)
SEL3	終了日	(形式は YYMMDD)
SEL4	終了時刻	(形式は HHMM)

これらのスイッチの省略値は、次のようになっています。この際、最初に読み込んだレコードの日時から24時間を解析対象とします。

SEL1=00000
SEL2=0000
SEL3=99999
SEL4=2400

OSTYPE

オペレーティング・システムの種別

入力されるSMF/SMSレコード群が収集されたオペレーティング・システムの種別を指定してください。

OSTYPE=1 : IBMシステムのSMFレコード群
OSTYPE=2 : 富士通システムのSMFレコード群
OSTYPE=3 : 日立システムのSMSレコード群

1.1.2. コントロール・スイッチ

コントロール・スイッチでは、評価結果として出力する各種レポートの選択や入力データ群の選択などを指定します。

SW10

処理レコード・サマリー・レポート

入力されたSMF/SMSレコードの中で処理対象となったデータをサマリーしたレポートが作成されます。SW10が“1”に設定されていれば、このレポートが出力されます。

SW20
SW21
SW22

サマリー・レポート

解析したデータの中でジョブ開始・終了(TSO/TSSおよびSTC含む)時の状況を示すレポートを作成・出力します。このレポートには3種類があり、対応するスイッチが“1”に設定されていればレポートが出力されます。

SW30

リソース・アクセス・エラー・レポート

解析したデータの詳細なレポートを作成します。詳細レポートには3種類があり、条件にあったデータを基にレポートを作成し、対応するスイッチが‘1’に設定されていればレポートが出力されます。

SW40

リソース・アクセス状況サマリー・レポート

資源をアクセスした際の状況を示すレポートが作成されます。SW40が‘1’に設定されていれば、レポートが出力されます。

SW50
SW51 (注)
SELCMDSW

コマンド処理レポート

コマンド実行した際の状況を整理したレポートが作成されます。このコマンド処理レポートには、定義済ユーザと未定義ユーザに分類してレポートが作成・出力されます。 SW50が“1”に設定されていれば定義済ユーザのコマンド処理レポートが出力されます。SW50とSW51が共に“1”に設定されていれば未定義ユーザのコマンド処理レポートが出力されます。この際、定義済ユーザではコマンドの実行結果で選択することもできます。

SELCMDSW=0 ： 正常
SELCMDSW=1 ： エラー
SELCMDSW=2 ： 両方

(注)
日立システムでは
出力できません。

SW60
TRUSTOPT (注)

特権ユーザ利用状況レポート

特権ユーザが行なった操作を整理したレポートが作成されます。SW60が“1”に設定されていればレポートが出力されます。日立システムではTRUSTOPTスイッチが“1”に設定されていれば、全てのリソース・アクセス情報を報告します(大量のシステム資源を使用することがあります)。

TRUSTOPT=0 ： 失敗したリソース・アクセス情報のみ報告する
TRUSTOPT=1 ： 全てのリソース・アクセス情報を報告する

(注)
日立システム専用
です。

SW70
SELRSCSW
SELNMCHK

（注）
日立システムでは
動作しません。

ユーザ毎の最終アクセス・レポート

ユーザ毎にシステムをアクセスした最終日時を示すレポートが作成されます。SW70が“1”に設定されていればレポートが出力されます。セキュリティツールのログ収集方法によっては正常なアクセスのログが収集されないことがある為、SELRSCSWで解析対象ログの選択が可能となっています。

SELRSCSW=0 ： 開始・終了のみを対象
SELRSCSW=1 ： 全ての事象を対象
SELRSCSW=2 ： 全ての事象に加えてSMFタイプ20も対象(注)
SELRSCSW=3 ： 全ての事象に加えてSMFタイプ30サブタイプ1と5を対象(注)

IBMシステムの場合は、ユーザ名をレポート作成時のキーとすることができます。

SELNMCHK=0 ： ユーザ名はキーとしない
SELNMCHK=1 ： ユーザ名をキーとする（省略値）

【留意点】
RACF のログ設定でエラーのみを記録するように指定されている場合、ジョブ開始・終了レコードを解析対象とすると、報告される多くの項目が欠損値となることがあります。また、ジョブ開始・終了レコードを解析対象とする際には、RACF レコードとマージする時に大量の資源を使用することがありますので注意してください。タイプ20（SELRSCSW=2）では、仮想記憶域、タイプ30（SELRSCSW=3）ではプロセッサ時間が増加する可能性があります。いずれも入力されるレコード数に依存します。

SW80, TUID
SW80OPT

（注）
比較制御文字につ
いては、マニュアル
末尾にある「比較制
御文字について」を
ご参照ください。

特定ユーザのトレース・レポート

特定ユーザのアクセス状況を示すトレース・レポートが作成されます。SW80が“1”に設定されていればレポートが出力されます。この際、トレースするユーザIDはTUID配列変数で指定します。ユーザIDの定義を簡略化させる為に比較制御文字を利用した指定が可能です(注)

DIM TUID(m) 配列の定義
TUID(n)=’ユーザID’ トレースするユーザID

IBMと富士通システムの場合、ジョブ開始・終了レコードを解析対象ログとして含めることができます。これはSELRSCSWスイッチで指示します。SW80OPTではトレースレポートにジョブ開始・終了レコードを含める際に指定します。

SW80OPT=0 ジョブ開始・終了レコードは含めない（省略値）
SW80OPT=1 ジョブ開始・終了レコードを含める

SELDSNSW

データセット名出力指示

次のレポートでデータセット名の出力を制御します。SELDSNSWに“1”が設定されており、レポート出力指示がある際には、データセット名を出力します。

○リソース・アクセス・エラー・レポート （SW30）
○コマンド処理レポート （SW50、SW51）
○特権ユーザ利用状況レポート （SW60）
○特定ユーザのトレース・レポート （SW80）

リソースクラス名が「DATASET」の場合に、ボリューム通番とデータセット名（最大44バイト）を2行目に出力します。

SYSID

システム識別コード

入力として指定されたデータセットの中に、複数システムの稼働実績データが記録されている場合があります。このような場合、どのシステムの評価を行うべきかを指定する必要があります。SYSIDに評価対象とするべきシステムのシステム識別コードを指定してください。SYSIDがブランク（‘ ’）の場合、最初に読み込んだ稼働実績データのシステムが対象となります。

1.1.3. その他のプログラム・スイッチ

前述のセレクション・スイッチおよびコントロール・スイッチ以外に、サンプル・ジョブ制御文では次のスイッチを使用することができます。このスイッチは、プロダクト・テープで提供されるサンプル・ジョブ制御文には定義されておりません。

ERRORCDE

リターン・コード

解析対象のパフォーマンス・データがない場合、もしくはプロセジャが出力すべきデータがない場合、以下のメッセージを出力します。このときのリターン・コードを、ERRORCDEに任意の値を指定することで変更できます。
指定できる値は0～4095の範囲の整数で、省略値は8です。

・解析対象のパフォーマンス・データがない場合のメッセージ

```
NO PERFORMANCE DATA IS FOUND.
```

・プロセジャが出力すべきデータがない場合のメッセージ

```
THERE WAS NO OUTPUT DATA.
```

¥PROCNM

プロセジャ名

各レポートのヘッダー部にはプロセジャ名が表示されるようになっています。このプロセジャ名を表示したくない場合、「¥PROCNM=_NULL_」を指定することにより表示が「PAGE」に変わります。

◆省略値（指定なし）

```
(C) I I M  CORP.  1987-1997        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     6
PSW=SW10                                 ---- RACF PROCESS RECORDS REPORT ----                                  VER=09 LVL=99
```

◆指定あり（¥PROCNM=_NULL_）

```
(C) I I M  CORP.  1987-1997        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    PAGE         6
PSW=SW10                                 ---- RACF PROCESS RECORDS REPORT ----                                  VER=09 LVL=99
```

APARTD49 (注)

区切り文字（1文字）

IBMシステムでユーザ名に空白や記号の桁を含む際には、特殊処理が必要になります。省略値で実行した際に正しくユーザ名が出力されない場合にユーザ名の区切り文字を設定します。なお、設定する文字（1文字）は、ユーザ名に使用されていない文字を設定してください。省略値はAPARTD49='?'です。

（注）
IBM システム
専用です。

このページは余白です。

1.2　処理レコード・サマリー・レポート（SW10）

処理レコード・サマリー・レポートでは処理対象時間帯のセキュリティツール・ログ情報を事象毎に分類して出力します。これにより、ログ情報に記録されているデータの概要を知ることができます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     6
PSW=SW10                                  ---- RACF PROCESS RECORDS REPORT ----                                 VER=09 LVL=99

CODE COUNT   EVENT CODE MEANING   EVENT CODE QUALIFIER MEANING                                  DESCRIPTION
0109       1 JOBINIT/LOGON/LOGOFF UNDEFINED USERID                                           THE EVENT IS A VIOLATION
0200      69 RESOURCE ACCESS      SUCCESSFUL ACCESS                                         SUCCESSFUL
0500       8 DELETE RESOURCE      SUCCESSFUL SCRATCH                                        SUCCESSFUL
0700       1 DEFINE RESOURCE      SUCCESSFUL DEFINITION                                     SUCCESSFUL
0800       1 RACF COMMAND         ADDSD    : NO VIOLATIONS DETECTED                         SUCCESSFUL
1300       8 RACF COMMAND         ALTUSER  : NO VIOLATIONS DETECTED                         SUCCESSFUL
1700       1 RACF COMMAND         DELUSER  : NO VIOLATIONS DETECTED                         SUCCESSFUL
2400       1 RACF COMMAND         SETROPTS : NO VIOLATIONS DETECTED                         SUCCESSFUL
*TTL      90



SYSTEM = IIM0 (OS:MVS     ,RACF:7709) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1114
```

Rpt 1.2　処理レコード・サマリー・レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     6
PSW=SW10                                  ---- RACF PROCESS RECORDS REPORT ----                                 VER=09 LVL=99

CODE COUNT   EVENT CODE MEANING   EVENT CODE QUALIFIER MEANING                                  DESCRIPTION
0101      52 JOBINIT/LOGON        INVALID PASSWORD                                          THE EVENT IS A VIOLATION
0106      12 JOBINIT/LOGON        REVOKED USERID ATTEMPTING ACCESS                          THE EVENT IS A VIOLATION
0200    2078 RESOURCE ACCESS      SUCCESSFUL ACCESS                                         SUCCESSFUL
0201      15 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                                    THE EVENT IS A VIOLATION
0201       1 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                                    VIOLATION AND UNDEFINED USER
1800       4 RACF COMMAND         PASSWORD : SUCCESSFUL                                     SUCCESSFUL
*TTL    2162


SYSTEM = IIM1 (OS:MSP     ,RACF:0013) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1408
```

Rpt 1.2　処理レコード・サマリー・レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT     5
PSW=SW10                                  ---- TRUST PROCESS RECORDS REPORT ----                                VER=09 LVL=99

CODE COUNT   EVENT CODE MEANING   EVENT CODE QUALIFIER MEANING                                  DESCRIPTION
0000      90 RESOURCE ACCESS      SUCCESSFUL                                                SUCCESSFUL
0010       2 RESOURCE ACCESS      ACCESS ERROR DETECTED(REASON=08)                          THE EVENT IS A VIOLATION
0100       8 TRUST COMMAND        TRCHANGE : SUCCESSFUL                                     SUCCESSFUL
1400     149 TRUST COMMAND        DELETE   : SUCCESSFUL                                     SUCCESSFUL
1401     296 TRUST COMMAND        DELETE   : ERROR DETECTED                                 THE EVENT IS A VIOLATION
4000     908 JOB                  SUCCESSFUL INITIATION                                     SUCCESSFUL
4003      88 JOB                  INVALID USERID                                            VIOLATION AND UNDEFINED USER
4100     908 END_JOB              SUCCESSFUL                                                SUCCESSFUL
5000     323 LOGON                SUCCESSFUL INITIATION                                     SUCCESSFUL
5000       7 TRUST COMMAND        LOGON    : SUCCESSFUL                                     SUCCESSFUL
5001      10 LOGON                INVALID PASSWORD                                          THE EVENT IS A VIOLATION
5001       1 TRUST COMMAND        LOGON    : ERROR DETECTED                                 THE EVENT IS A VIOLATION
5003       3 LOGON                INVALID USERID                                            VIOLATION AND UNDEFINED USER
5100     321 LOGOFF               SUCCESSFUL                                                SUCCESSFUL
6000      14 STC                  SUCCESSFUL INITIATION                                     SUCCESSFUL
6100      11 END_STC              SUCCESSFUL                                                SUCCESSFUL
*TTL    3139

SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 FRI 1521
```

Rpt 1.2　処理レコード・サマリー・レポートの例（日立）

この処理レコード・サマリー・レポートの内容は次のようになっています。

CODE　　XXYY の 4 桁
　XX：　事象コード
　YY：　事象コード修飾子
　日立システムの TRUST の場合、事象コードと事象コード修飾子は次を意味します。
　　事象コード　　コマンドコード
　　事象コード修飾子　　エラー情報
　なお、擬似コマンド（JOB、LOGON、VERIFY）については、ユーザ検証時の事象と重複しますが分類して報告します。
COUNT　　件数
EVENT CODE MEANING
　　事象コードの説明
EVENT CODE QUALIFIER MEANING
　　事象コード修飾子の説明
DESCRIPTION　　結果

'VIOLATION AND UNDEFINED USER'
　　システムに未定義のユーザが不正アクセスを行った。
'THE EVENT IS A VIOLATION'
　　不正なアクセスを行った。
'USER IS NOT DEFINED TO RACF'
　　システムに未定義のユーザがアクセスした。
'THE EVENT IS A WARNING'
　　警告
'SUCCESSFUL'
　　正常に処理された。

事象コードや事象コード修飾子の詳細な説明については、下記のメーカ提供のマニュアルを参照してください。
IBMシステム　　：資源アクセス管理機能　監査担当者の手引き
　　Resource Access Control Facility　Auditor's Guide
富士通システム　　：OSIV/MSP RACFユーティリティ使用手引書
日立 システム　　：TRUST E2　セキュリティ監視の手引き

1.3　サマリー・レポート（SW20, SW21, SW22）

ジョブ開始･終了(TSO/TSSおよびSTC含む)時の状況を示すレポートには、次の3種類がありますが、出力される形式や項目はすべて同じです。

これらのレポートはヘッダー部で識別することができます。

サマリー・レポート名（出力指定スイッチ）	レ ポ ー ト 内 容
不正アクセス・サマリー（SW20）	システムや資源に対して不正アクセスを行ったユーザやその際の状況を示します。
未定義ユーザ・サマリー（SW20, SW21）	システムに未定義のユーザがアクセスした場合に作成・出力されます。
警告サマリー　　（SW20,　SW22）	ユーザがアクセスした際に警告が発せられた場合に作成・出力されます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2004        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    4
PSW=SW20                           ------ RACF JOB/LOGON/LOGOFF - VIOLATION SUMMARY REPORT ------              VER=09 LVL=99

                                                                                    *-TIME STAMP-*
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  *-USER NAME (ACEE)-* APPLNAME YY/MM/DD HH:MM *-- LOGGING REASON --*
0101 UID0062  GRP001                 TERM0340          .....                      98/11/10 14:12 RACINIT FAILURE
0101 UID0062  GRP001                 TERM0340 STCR00   ..... STCAPL0  98/11/10 14:22 RACINIT FAILURE
0101 UID0095  GRPM00                 TERM0302          .....                      98/11/10 17:03 RACINIT FAILURE
0101 UID0095  GRPM00                 TERM0304          .....                      98/11/10 19:58 RACINIT FAILURE
0101 UID1067  GRPDBM                 TERM0680          .....                      98/11/10 11:30 RACINIT FAILURE
0101 UID1295  GRPM00                 TERM0302          .....                      98/11/10 16:56 RACINIT FAILURE
0101 UID4312  GRPDBM                 TERM1920          .....                      98/11/10 11:39 RACINIT FAILURE
0101 UID9006  SYSOP                  TERM0270          .....                      98/11/10 03:33 RACINIT FAILURE
0101 UID9006  SYSOP                  TERM0270          .....                      98/11/10 03:33 RACINIT FAILURE
0101 UID9006  SYSOP                  TERM0270          .....                      98/11/10 03:33 RACINIT FAILURE
0101 : JOBINIT/LOGON/LOGOFF INVALID PASSWORD


SYSTEM = IIM0 (OS:MVS    ,RACF:1092) START = 98/11/10 TUE 0002 END = 98/11/10 TUE 2306   REPORTING DATE = 04/01/08 THU 1658
```

Rpt 1.3　不正アクセスサマリー・レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2004        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    4
PSW=SW20                           ------ RACF JOB/LOGON - VIOLATION SUMMARY REPORT ------                    VER=09 LVL=99

                                                    *-- JOB SUBMIT --*          *-TIME STAMP-*
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  USER-ID  GROUP-ID    APPLNAME YY/MM/DD HH:MM *-- LOGGING REASON --*
0101 FUIDTRC  *        NORMAL        TERM0100                                 98/11/11 17:03 RACINIT FAILURE
0101 UIDF109  *        NORMAL        TERM520B                                 98/11/11 11:31 RACINIT FAILURE
0101 UIDG001  *        NORMAL        TERM1727                                 98/11/11 18:57 RACINIT FAILURE
0101 UIDK058  *        NORMAL        TERMA180                                 98/11/11 11:48 RACINIT FAILURE
0101 : JOBINIT/LOGON         INVALID PASSWORD

0106 UIDN001  *        NORMAL        TERM0522                                 98/11/11 09:41 RACINIT FAILURE
0106 UID9249  *        NORMAL        TERMA103                                 98/11/11 19:51 RACINIT FAILURE
0106 : JOBINIT/LOGON         REVOKED USERID ATTEMPTING ACCESS
*** TOTAL VIOLATION COUNT =    31

SYSTEM = IIM1 (OS:MSP    ,RACF:0013) START = 98/11/10 TUE 2323 END = 98/11/11 WED 2335   REPORTING DATE = 04/01/08 THU 1655
```

Rpt 1.3　不正アクセスサマリー・レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2004        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT    4
PSW=SW20                           ------ TRUST JOB/LOGON/LOGOFF - VIOLATION SUMMARY REPORT ------            VER=09 LVL=99

                                                                RESOURCE          *-- START --* *-- STOP --* ACCESS COUNT
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  JOBCLASS /OBJECT    APPLNAME YY/MM/DD HH:MM YY/MM/DD HH:MM TOTAL  ERROR
5001 JOBTRC1  GRPL01                 TERMDM8  JOBTRC1  TSU                        98/11/09 12:15
5001 SYS2G18  SYS1                   TERMW10  SYS2G18  TSU                        98/11/09 12:16
5001 SYS2G27  SYS2                   TERM480  SYS2G27  TSU                        98/11/09 21:20
5001 TSU3020  GRPD03                 TERM060  TSU3020  TSU                        98/11/09 19:20
5001 : LOGON                 INVALID PASSWORD

5005 SYS2G12  SYS1                   TERM028  SYS2G12  TSU                        98/11/09 13:04
5005 TSU3048  GRPD03                 TERM014  TSU3048  TSU                        98/11/09 08:59
5005 : LOGON                 CURRENT PASSWORD HAS EXPIRED
*** TOTAL VIOLATION COUNT =    12

SYSTEM = IIM2 (OS:VOS3   TRUST:0003) START = 98/11/09 MON 0723 END = 98/11/10 TUE 0723   REPORTING DATE = 04/01/08 THU 1659
```

Rpt 1.3　不正アクセスサマリー・レポートの例（日立）

このサマリー・レポートの内容は次のようになっています。

CODE	事象コードと事象コード修飾子 全事象をこの値で分類し、CODE 毎にまとめて表示。また分類された各事象群の最終行では、その CODE 値が示す事象の意味を簡単に説明
USER-ID	ユーザ ID 未登録ユーザの場合はジョブ名
GROUP-ID	グループ ID 未登録ユーザの場合はステップ名
AUTHORITY	資源にアクセスしたユーザの権限や属性※
	 ※【解説】ユーザの権限・属性をご覧ください。
TERMINAL	端末名
JOBNAME	ジョブ名（バッチの場合にのみ有効）

■IBM システムの場合

USER NAME (ACEE)	ユーザ名
APPLNAME	業務プログラム名
TIME STAMP	事象発生日時
LOGGING REASON	レコード作成理由。各メッセージの内容は次の通り。
'SETROPTS AUDIT(CLASS) '	ー SETROPTS の AUDIT オペランド
'USER BEING AUDITED '	ー 利用者のログ
'SPECIAL USERS '	ー SPECIAL 属性
'AUDIT/RACHECK/FAILSOFT'	ー AUDIT オプション、RACHECK 出口ルーチンや FAILSOFT 処理
'RACINIT FAILURE '	ー 不正アクセス
'ALWAYS AUDITED '	ー コマンドログ
'VIOLATION & CMDVIOL ON'	ー コマンドエラー
'GLOBALAUDIT OPTION '	ー GLOBALAUTID オプション
'SECURITY LEVEL CONTROL'	ー 安全保護レベル
'VMEVENT '	ー 特定の VM 事象（データベースを VM システムと共用している場合のみ）
'LOGOPTIONS '	ー SETROPTS の LOGOPTIONS による特定クラスへのアクセス
'SECLABELAUDIT '	ー 安全保護ラベル
'COMPATMODE'	ー SETROPTS の COMATMODE
'APPLAUDIT '	ー SETROPTS の APPLAUDIT
'USER NOT DEFINED TO OE'	ー OMVS に未定義ユーザ
'INSUFFICIENT AUTH (OE)'	ー OMVS のアクセス権限が不足

■富士通システムの場合

JOB SUBMIT		
USER-ID	ジョブを投入したユーザ ID	
GROUP-ID	ジョブを投入したグループ ID	
APPLNAME	業務プログラム名	
TIME STAMP	事象発生日時	
LOGGING REASON	レコード作成理由。各メッセージの内容は次の通り。	
'SETROPTS AUDIT(CLASS)'	－	RACF コマンドまたは RACDEF 機能の使用
'USER BEING AUDITED'	－	利用者のログ
'SPECIAL USERS'	－	SPECIAL 属性
'RESOURCE ACCESS LOG'	－	資源アクセスログ
'RACINIT FAILURE'	－	不正アクセス
'RVARY/SETROPTS'	－	RVARY,SETROPTS,RREFRESH や MNGUPOTS コマンドが使用された
'VIOLATION & CMDVIOL ON'	－	コマンドエラー
'GLOBALAUDIT OPTION'	－	GLOBALAUDIT オプション
'SETROPTS GAUDIT'	－	グローバルチェック機能によるログ収集
'SETROPTS DAUDIT'	－	省略値保護機能によるログ収集
'SETROPTS OAUDIT'	－	資源保安要員の監査機能によるログ収集
'SETROPTS STAUDIT'	－	構造化グループ機能によるログ収集

■日立システムの場合

JOBCLASS	ジョブクラス
RESOURCE/OBJECT	リソース種別名
APPLNAME	常に空白
START	システム利用開始日時
STOP	システム利用終了日時
ACCESS COUNT	
TOTAL	リソースにアクセスした総回数
ERROR	アクセスエラー回数

【解説】ユーザの権限・属性

項目「AUTHORITY」は、「資源にアクセスしたユーザの権限や属性」を示します。次のレポートに出力されます。

－サマリー・レポート(SW20,SW21,SW22)
－リソース・アクセス・エラー・レポート(SW30)
－コマンド処理レポート(SW50,SW51)
－特権ユーザ利用状況レポート(SW60)
－ユーザ毎の最終アクセス・レポート(SW70,SELRSCSW)
－特定ユーザのトレース・レポート(SW80,TUID)

■IBM システムの場合

SPECIAL	SPECIAL 属性またはグループ SPECIAL 属性
OPERATIONS	OPERATIONS 属性またはグループ OPERATIONS 属性
AUDITOR	AUDITOR 属性またはグループ AUDITOR 属性
EXIT	出口ルーチンによりアクセスが許可
NORMAL	一般ユーザでアクセスが許可
FAILSOFT	ソフトウェア障害時
BYPASSED	ユーザ ID に BYPASS によりアクセス権限の検査を回避
TRUSTED	TRUSTED 属性でアクセスが許可
空白	上記以外

■富士通システムの場合

SPECIAL	最高管理者
OPERATIONS	資源保安要員
AUDITOR	監査役
EXIT	出口ルーチンによりアクセスが許可
GRPSPECIAL	グループデータセット最高管理者
GRPOPERATIONS	グループ資源保安要員
GRPAUDITOR	グループ監査役
RVARY	RVARY コマンド使用資格者
BLP	BLP 使用資格者
NL	NL 使用資格者
空白	アクセス制御の迂回や構造化グループ機能の資格チェックエラー
NORMAL	一般ユーザでアクセスが許可

■日立システムの場合

SYSMGR	センタ管理者 グループ ID が「SYS1」、ユーザ ID が「SYSUSER」の場合は無条件にセンタ管理者（SYSMGR）して取り扱います。
SCRTYMGR	セキュリティ管理者
AUDITOR	調査担当者
空白	一般ユーザ

1.4　リソース・アクセス・エラー・レポート（SW30）

リソース・アクセス・エラー・レポートでは、保護された資源をアクセスした際にエラーが発生した場合に作成・出力されます。入力のコントロールスイッチでSELDSNSW=1が設定されておりリソース種別名が「DATASET」の場合には、次の行にボリューム通番とデータセット名が表示されます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                          AUDITPRT     7
PSW=SW30                                 ------ RACF RESOURCE ACCESS ERROR REPORT ------                            VER=09 LVL=99

                                                                                  *-TIME STAMP-* RESOURCE
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  *-USER NAME (ACEE)-* YY/MM/DD HH:MM CLASS    INTENT  ALLOW
0201 TSO2     TSOGRP1  NORMAL                TSO3JOB  TSO2                 09/01/30 12:29 DATASET  CONTROL UPDATE
                                                                           ZOSVOL SYS1.MAN2
0201 TSO2     TSOGRP1  NORMAL                TSO2JOB  TSO2                 09/01/30 12:31 DATASET  CONTROL UPDATE
                                                                           ZOSVOL SYS1.MAN2
0201 TSO2     TSOGRP1  NORMAL                TSO2JOB  TSO2                 09/01/30 12:32 DATASET  CONTROL UPDATE
                                                                           ZOSVOL SYS1.MAN2
0201 TSO2     TSOGRP1  NORMAL                TSO2JOB  TSO2                 09/01/30 12:33 DATASET  CONTROL UPDATE
                                                                           ZOSVOL SYS1.MAN2
0201 TSO2     TSOGRP1  NORMAL                TSO2JOB  TSO2                 09/01/30 12:36 DATASET  CONTROL UPDATE
                                                                           ZOSVOL SYS1.MAN1
0201 : RESOURCE ACCESS      INSUFFICIENT AUTHORITY
*** TOTAL VIOLATION COUNT =     5

SYSTEM = IIM0 (OS:MVS    ,RACF:7709) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1114
```

Rpt 1.4　リソース・アクセス・エラー・レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                          AUDITPRT     9
PSW=SW30                                 ------ RACF RESOURCE ACCESS ERROR REPORT ------                            VER=09 LVL=99

                                                        *- ACCESS CHECK -* *-TIME STAMP-* RESOURCE
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  CHECK    TYPE      YY/MM/DD HH:MM CLASS    INTENT  ALLOW
0201 MSPU259  TSSGRP   NORMAL        TSSTRM00 MSPU259  GENERIC  UNIVACS   09/01/30 13:14 DATASET  UPDATE  READ
                                                                           LIB000 TSSGRP.LIB000.LIBRARY.FILE1
0201 MSPU259  TSSGRP   NORMAL        TSSTRM00 MSPU259  GENERIC  UNIVACS   09/01/30 13:14 DATASET  UPDATE  READ
                                                                           LIB000 TSSGRP.LIB000.LIBRARY.FILE1
0201 MSPU263  TSSGRP   NORMAL        TSSTRM00 MSPU263  GENERIC  UNIVACS   09/01/30 13:07 DATASET  UPDATE  READ
                                                                           LIB000 TSSGRP.LIB000.LIBRARY.FILE1
0201 MSPU263  TSSGRP   NORMAL        TSSTRM00 MSPU263  GENERIC  UNIVACS   09/01/30 13:12 DATASET  UPDATE  READ
                                                                           SYS001 CATALOG.MSPEDFM.VSYS001
0201 : RESOURCE ACCESS      INSUFFICIENT AUTHORITY


SYSTEM = IIM1 (OS:MSP    ,RACF:0013) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1408
```

Rpt 1.4　リソース・アクセス・エラー・レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                         AUDITPRT    12
PSW=SW30                                 ------ TRUST RESOURCE ACCESS ERROR REPORT ------                           VER=09 LVL=99

                                                                 STEP     *-TIME STAMP-* RESOURCE
CODE USER-ID  GROUP-ID AUTHORITY     TERMINAL JOBNAME  JOBCLASS NO       YY/MM/DD HH:MM /OBJECT  INTENT  ALLOW
0010 _BLANK_  _BLANK_                        JOBNAME1 S          21       09/01/30 23:02 DATASET  MASTER
                                                                          _UNKN_ TEMP.JCL.FILE.BACKUP1
0010 _BLANK_  _BLANK_                        JOBNAME1 S          23       09/01/30 23:26 DATASET  MASTER
                                                                          _UNKN_ TEMP.JCL.SEND.BACKUP1
0010 : RESOURCE ACCESS      ACCESS ERROR DETECTED(REASON=08)
*** TOTAL VIOLATION COUNT =     2



SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 FRI 1521
```

Rpt 1.4　リソース・アクセス・エラー・レポートの例（日立）

このリソース・アクセス・エラー・レポートの内容は次のようになっています。

CODE	事象コードと事象コード修飾子 全事象をこの値で分類し、CODE 毎にまとめて表示。 また分類された各事象群の最終行では、その CODE 値が示す事象の意味を簡単に説明。その際、未定義ユーザによるアクセスの場合は説明文の最後に'(UNDEFINED USER)'が表示される。
USER-ID	ユーザ ID
GROUP-ID	グループ ID
AUTHORITY	資源にアクセスしたユーザの権限や属性※1
TERMINAL	端末名
JOBNAME	ジョブ名

※1 「1.3 サマリー・レポート(SW20, SW21, SW22)」の【解説】ユーザの権限・属性をご覧ください。

■IBM システムの場合

USER NAME (ACEE)	ユーザ名
TIME STAMP	事象発生日時
RESOURCE CLASS	リソース種別名
INTENT	ユーザが要求したアクセス権※2
ALLOW	セキュリティツールが許可したアクセス権※2

■富士通システムの場合

ACCESS CHECK	
CHECK	アクセス権をチェックする際のユーザの権限や属性
GLOBAL	ー グローバルチェック機能
GENERIC	ー 総称名機能
DEFAULT	ー 省略値保護機能
DISCRETE	ー 個別名保護機能
UNIFYDS	ー 未登録データセットの一括保護機能
TYPE	アクセス権種別
USERACS	ー 利用者への特定アクセス権
GRPACS	ー グループへの特定アクセス権
PUSERACE	ー 利用者への特定パスアクセス権
PGRPACS	ー グループへの特定パスアクセス権
PPATHACS	ー 公衆パスアクセス権
UNIVACS	ー 公衆アクセス権
UNDEFTRM	ー 未登録端末の公衆アクセス権
GRPTUACS	ー 端末利用者限定属性
COACCACC	ー グループ公衆アクセス権
GLBLACS	ー グローバルアクセス権
GPATHACS	ー グローバルパスアクセス権
空白	ー 上記以外
TIME STAMP	事象発生日時
RESOURCE CLASS	リソース種別名
INTENT	ユーザが要求したアクセス権※2
ALLOW	セキュリティツールが許可したアクセス権※2

※2【解説】要求アクセス権と許可アクセス権をご覧ください。

■日立システムの場合

JOBCLASS	ジョブクラス
STEP	ジョブステップ番号
TIMESTAMP	事象発生日時
RESOUCE/OBJECT	リソース種別名（クラス名）
INTENT	ユーザが要求したアクセス権※2
ALLOW	常に空白

※2【解説】要求アクセス権と許可アクセス権をご覧ください。

【解説】要求アクセス権と許可アクセス権

項目「INTENT」と「ALLOW」はそれぞれ、「リソースをアクセスする際にユーザが要求したアクセス権」と「ユーザの要求に対してセキュリティツールが許可したアクセス権」を示します。次のレポートに出力されます。

－リソース・アクセス・エラー・レポート(SW30)
－リソース・アクセス状況サマリー・レポート(SW40)
－特権ユーザ利用状況レポート(SW60)
－特定ユーザのトレース・レポート(SW80,TUID)

■IBM、富士通システムの場合

INTENT		ユーザが要求したアクセス権
	ALTER	－ 改名削除権
	CONTROL	－ VSAM 制御権
	UPDATE	－ 書き込み権
	READ	－ 読み出し権
	EXECUTE	－ 実行権
	NONE	－ 上記以外
ALLOW		セキュリティツールが許可したアクセス権
	ALTER	－ 改名削除権
	CONTROL	－ VSAM 制御権
	UPDATE	－ 書き込み権
	READ	－ 読み出し権
	EXECUTE	－ 実行権
	NONE	－ アクセス禁止

■日立システムの場合

INTENT		ユーザが要求したアクセス権
	MASTER	－ MASTER 権限
	EXTEND	－ EXTEND 権限
	WRITE	－ WRITE 権限
	MEMBER	－ MEMBER 権限
	READ	－ READ 権限
	USE	－ USE 権限
	NONE	－ NONE 権限
	SPACEA	－ SPACEA 権限
ALLOW		常に空白

1.5　リソース・アクセス状況サマリー・レポート（SW40）

リソース･アクセス状況サマリー･レポートでは、ユーザが保護された資源をアクセスする際に使用したアクセス権許可されたアクセス権をサマリーしたレポートを作成･出力します。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2007        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     6
PSW=SW40                                  ---- RACF RESOURCE ACCESS SUMMARY REPORT ----                        VER=09 LVL=99

          RESOURCE TOTAL   ERROR   *------------- I N T E N T -------------* *------------- A L L O W -------------*
GROUP-ID  CLASS     COUNT   COUNT  ALTER   CONTROL UPDATE  READ    NONE    EXECUTE ALTER   CONTROL UPDATE  READ    NONE    EXECUTE
GRPAO     DATASET      12 .......     12 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPCD     DATASET      12 .......     12 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPCD     ACCTNUM       6 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPDA     ACCTNUM       3 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPDA     DATASET       2 .......      2 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPSHIN   ACCTNUM       1 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
  |         |         |
SYS1      DATASET      10 .......      2 .......       1       7 ....... ....... ....... ....... ....... ....... ....... .......
SYS1      ACCTNUM       7 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
--------- -------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- -------
*TOTAL*               1594 .......   1378 .......       1     215 ....... .......    1386 ....... .......     208 ....... .......

SYSTEM = IIMO (OS:MVS    ,RACF:7709) START = 98/11/10 TUE 0002 END = 98/11/10 TUE 2306   REPORTING DATE = 07/06/07 THU 1658
```

Rpt 1.5　リソース・アクセス状況サマリー・レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2007        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     6
PSW=SW40                                  ---- RACF RESOURCE ACCESS SUMMARY REPORT ----                        VER=09 LVL=99

          RESOURCE TOTAL   ERROR   *------------- I N T E N T -------------* *------------- A L L O W -------------*
GROUP-ID  CLASS     COUNT   COUNT  ALTER   CONTROL UPDATE  READ    EXECUTE NONE    ALTER   CONTROL UPDATE  READ    EXECUTE NONE
GRPAOO    DATASET       1 .......      1 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPA01    DATASET      34 .......     12 .......      11      11 ....... ....... ....... ....... ....... ....... ....... .......
GRPDBM    DATASET    1100 .......    318 .......     388     394 ....... ....... ....... ....... ....... ....... ....... .......
GRPLLL    DATASET      99 .......     31 .......      37      31 ....... ....... ....... ....... ....... ....... ....... .......
GRPSSS    DATASET      90 .......     30 .......      30      30 ....... ....... ....... ....... ....... ....... ....... .......
GRPTTT    DATASET     170 .......     55 .......      63      52 ....... ....... ....... ....... ....... ....... ....... .......
GRP200    DATASET       7 .......      2 .......       3       2 ....... ....... ....... ....... ....... ....... ....... .......
SYSGEN    DATASET     105 .......     30 .......      33      42 ....... ....... ....... ....... ....... ....... ....... .......
SYSOP     DATASET      96       1     18 .......      30      48 ....... ....... ....... ....... ....... ....... ....... .......
SYS1      DATASET      14 ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... ....... .......
--------- -------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- ------- -------
*TOTAL*               1716       1    497 .......     595     624 ....... ....... ....... ....... ....... ....... ....... .......

SYSTEM = IIM1 (OS:MSP    ,RACF:0013) START = 98/11/10 TUE 2323 END = 98/11/11 WED 2335   REPORTING DATE = 07/06/07 THU 1655
```

Rpt 1.5　リソース・アクセス状況サマリー・レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2007        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT     7
PSW=SW40                                  ---- TRUST RESOURCE ACCESS SUMMARY REPORT ----                       VER=09 LVL=99

          RESOURCE TOTAL   ERROR   *------------------- I N T E N T -------------------*
GROUP-ID  /OBJECT   COUNT   COUNT  MASTER  EXTEND  WRITE   MEMBER  READ    USE     NONE    SPACEA
_BLANK_   VOLUME        3       3 .......       .       3 ....... ....... ....... ....... .......
GRPDO2    TERMINAL     12 ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPDO3    TERMINAL    124 ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPDO8    TERMINAL      6 ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPL01    TERMINAL      2 ....... ....... ....... ....... ....... ....... ....... ....... .......
GRPMOO    VOLUME        4       4 .......       .       4 ....... ....... ....... ....... .......
SYS1      TERMINAL      7 ....... ....... ....... ....... ....... ....... ....... ....... .......
SYS2      TERMINAL     33 ....... ....... ....... ....... ....... ....... ....... ....... .......
USER      TERMINAL      1 ....... ....... ....... ....... ....... ....... ....... ....... .......
--------- -------- ------- ------- ------- ------- ------- ------- ------- ------- ------- -------
*TOTAL*               192       7 .......       7 ....... ....... ....... ....... .......

SYSTEM = IIM2 (OS:VOS3   TRUST:0003) START = 98/11/09 MON 0723 END = 98/11/10 TUE 0723   REPORTING DATE = 07/06/07 THU 1659
```

Rpt 1.5　リソース・アクセス状況サマリー・レポートの例（日立）

このリソース・アクセス状況サマリー・レポートの内容は次のようになっています。

GROUP-ID	グループ ID
RESOURCE CLASS	リソース種別名（クラス名）
TOTAL COUNT	総アクセス回数
ERROR COUNT	総アクセスエラー回数

■IBM、富士通システムの場合

INTENT	ユーザが要求したアクセス権※ ALTER, CONTROL, UPDATE, READ, NONE, EXECUTE の各権限で要求された回数
ALLOW	セキュリティツールが許可したアクセス権※ ALTER, CONTROL, UPDATE, READ, NONE, EXECUTE の各権限で許可された回数

■日立システムの場合

INTENT	ユーザが要求したアクセス権※ MASTER, EXTEND, WRITE, MEMBER, READ, USE,NONE, SPACEA の各権限で要求された回数

※「1.4 リソース・アクセス・エラー・レポート（SW30）」の【解説】要求アクセス権と許可アクセス権をご覧ください。

1.6　コマンド処理レポート（SW50、SW51）

コマンド処理レポートでは、ジョブ開始・終了およびリソースアクセス以外の状況を示します。このレポートを作成する際に、コマンドの実行結果を選択するスイッチ（SELCMDSW）が用意されています。このSELCMDSWスイッチは定義済ユーザ（SW50）にのみ有効です。入力のコントロールスイッチでSELDSNSW=1が設定されており、リソース種別名が「DATASET」の場合には次の行にボリューム通番とデータセット名が表示されます。

このレポートは、定義済ユーザ（SW50）と未定義ユーザ（SW50+SW51）(注)に分類して作成・出力されます。これらの出力項目はすべて同じでヘッダー部で識別できます。

（注）
日立システムでは出力できません。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                          AUDITPRT     8
PSW=SW50                                 ---- RACF COMMAND PROCESS SUMMARY REPORT ----                                VER=09 LVL=99

                                                          *-READER DATETIME-*          *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    COMMAND  RESULT  JOBNAME  YY/MM/DD HH:MM:SS.TH TERMINAL YY/MM/DD HH:MM CLASS    OWNER    CMD-PROC
SPUSR3   SPCGRP   SPECIAL      DELUSER  SUCCESS SPUSR3   09/01/30 13:30:42.39          09/01/30 13:30          TSUGRP
SPUSR4   SPCGRP   SPECIAL      DEFINE   SUCCESS SPUSR4   09/01/30 14:31:22.36 TS000009 09/01/30 14:41 DATASET  HOST
                                                                                _UNKN_ HOST.**
SPUSR4   SPCGRP   SPECIAL      ADDSD    SUCCESS SPUSR4   09/01/30 14:31:22.36 TS000009 09/01/30 14:41          HOST
SPUSR4   SPCGRP   SPECIAL      SETROPTS SUCCESS SPUSR4   09/01/30 14:31:22.36 TS000009 09/01/30 14:41
SPUSR4   SPCGRP   SPECIAL      ALTUSER  SUCCESS SPUSR4   09/01/30 14:31:22.36 TS000009 09/01/30 14:47          TSUGRP
SPUSR4   SPCGRP   SPECIAL      ALTUSER  SUCCESS SPUSR4   09/01/30 14:47:44.68 TS000009 09/01/30 14:51          TSUGRP
SPUSR4   SPCGRP   NORMAL       DELRES   SUCCESS SPUSR4   09/01/30 14:51:42.24 TS000009 09/01/30 14:52 DATASET  HOST
                                                                                HOST01 HOST.SPUSR4.TESTDATA
SPUSR4   SPCGRP   NORMAL       DELRES   SUCCESS SPUSR4   09/01/30 14:51:42.24 TS000009 09/01/30 14:52 DATASET  HOST
                                                                                HOST01 HOST.SPUSR4.TESTDAT2
SPUSR4   SPCGRP   SPECIAL      ALTUSER  SUCCESS SPUSR4   09/01/30 14:51:42.24 TS000009 09/01/30 14:52          TSUGRP

SYSTEM = IIM0 (OS:MVS     ,RACF:7709) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1114
```

Rpt 1.6　コマンド処理レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                          AUDITPRT    11
PSW=SW50                                 ---- RACF COMMAND PROCESS SUMMARY REPORT ----                                VER=09 LVL=99

                                                          *-READER DATETIME-*          *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    COMMAND  RESULT  JOBNAME  YY/MM/DD HH:MM:SS.TH TERMINAL YY/MM/DD HH:MM CLASS    OWNER    CMD-PROC
TSS2000  GROUP1   NORMAL       PASSWORD SUCCESS TSS2000  09/01/30 13:29:01.30 TTSS0010 09/01/30 13:29
TSS2100  GROUP2   NORMAL       PASSWORD SUCCESS TSS2100  09/01/30 10:51:14.76 TTSS0020 09/01/30 10:51
TSS5000  GROUP3   NORMAL       PASSWORD SUCCESS TSS5000  09/01/30 16:05:16.89 TTSS0030 09/01/30 16:05
TSS6000  GROUP4   NORMAL       PASSWORD SUCCESS TSS6000  09/01/30 15:34:02.61 TTSS0040 09/01/30 15:34


SYSTEM = IIM1 (OS:MSP     ,RACF:0013) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1408
```

Rpt 1.6　コマンド処理レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                         AUDITPRT    11
PSW=SW50                                 ---- TRUST COMMAND PROCESS SUMMARY REPORT ----                               VER=09 LVL=99

                                                                                    *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    COMMAND  RESULT  JOBNAME  STEP JOBCLASS TERMINAL YY/MM/DD HH:MM /OBJECT  OWNER    CMD-PROC
_SYSTEM_ _SYSTEM_              IPL      SUCCESS           0                       09/01/30 04:30 TRUST
GTSS01   GRP2                  LOGON    SUCCESS GTSS01    0 TSU      TTSS0001 09/01/30 11:33 PASSWORD
GTSS02   GRP2                  LOGON    SUCCESS GTSS02    0 TSU      TTSS0002 09/01/30 09:33 PASSWORD
GTSS03   GRP2                  LOGON    SUCCESS GTSS03    0 TSU      TTSS0003 09/01/30 10:24 PASSWORD
GTSS04   GRP2                  LOGON    SUCCESS GTSS04    0 TSU      TTSS0004 09/01/30 10:16 PASSWORD
GTSS05   GRP2                  LOGON    SUCCESS GTSS05    0 TSU      TTSS0005 09/01/30 17:44 PASSWORD
SYSUSER  SYS1     SYSMGR       CHANGE   SUCCESS BATCH41   1 2                     09/01/30 17:20 USER
SYSUSER  SYS1     SYSMGR       CHANGE   SUCCESS BATCH42   1 2                     09/01/30 17:25 USER


SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 FRI 1521
```

Rpt 1.6　コマンド処理レポートの例（日立）

このコマンド処理レポートの内容は次のようになっています。

USER-ID	ユーザ ID 未登録ユーザの場合はジョブ名
GROUP-ID	グループ ID 未登録ユーザの場合はステップ名
AUTHORITY	資源にアクセスしたユーザの権限や属性※
ERROR COUNT	総アクセスエラー回数

※「1.3 サマリー・レポート(SW20, SW21, SW22)」の【解説】ユーザの権限・属性をご覧ください。

COMMAND	コマンド名
RESULT	実行結果
SUCCESS	ー 正常
FAILURE	ー 失敗
WARNING	ー 警告（IBM のみ）
JOBNAME	ジョブ名（バッチの場合にのみ有効）

■IBM システムの場合

READER DATETIME	ジョブの入力日時
TERMINAL	端末名
TIME STAMP	コマンド実行日時
RESOURCE CLASS	リソース種別名
OWNER	資源の所有者名
CMD-PROC	コマンド実行後の状態
「NO BACKOUT」	ー コマンド処理中にエラーが発生し更新された（矛盾あり）
「NO UPDATE」	ー コマンド処理中にエラーが発生したが更新されていない

■富士通システムの場合

READER DATETIME	ジョブの入力日時
TERMINAL	端末名
TIME STAMP	コマンド実行日時
RESOURCE CLASS	リソース種別名
OWNER	資源の所有者名
CMD-PROC	コマンド実行後の状態
「NO BACKOUT」	ー コマンド処理中にエラーが発生し更新された（矛盾あり）
「NO UPDATE」	ー コマンド処理中にエラーが発生したが更新されていない

■日立システムの場合

STEP	ジョブステップ番号
JOBCLASS	ジョブクラス
TERMINAL	端末名
TIME STAMP	コマンド実行日時
RESOUCE/OBJECT	リソース種別名
OWNER	常に空白
CMD-PROC	常に空白

1.7　特権ユーザ利用状況レポート（SW60）

特権ユーザ利用状況レポートでは、特権ユーザの利用状況を示します。入力のコントロールスイッチでSELDSNSW=1が設定されておりリソース種別名が「DATASET」の場合には、次の行にボリューム通番とデータセット名が表示されます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     9
PSW=SW60                                 ---- RACF PRIVILEGED USER SUMMARY REPORT ----                          VER=09 LVL=99

                                                                    *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    JOBNAME  TERMINAL COMMAND  RESULT   YY/MM/DD HH:MM CLASS    INTENT   ALLOW
SPUSR3   SPCGRP   SPECIAL      SPUSR3X           DELUSER  SUCCESS  09/01/30 13:30
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 DEFINE   SUCCESS  09/01/30 14:41 DATASET
                                                                                  _UNKN_ HOST.**
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ADDSD    SUCCESS  09/01/30 14:41
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ALTUSER  SUCCESS  09/01/30 14:47
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ALTUSER  SUCCESS  09/01/30 14:51
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ALTUSER  SUCCESS  09/01/30 14:52
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ALTUSER  SUCCESS  09/01/30 15:02
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 ALTUSER  SUCCESS  09/01/30 15:05
SPUSR4   SPCGRP   SPECIAL      SPUSR4   TSO00009 SETROPTS SUCCESS  09/01/30 14:41


SYSTEM = IIM0 (OS:MVS     ,RACF:7709) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1114
```

Rpt 1.7　特権ユーザ利用状況レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    12
PSW=SW60                                 ---- RACF PRIVILEGED USER SUMMARY REPORT ----                          VER=09 LVL=99

                                                                    *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    JOBNAME  TERMINAL COMMAND  RESULT   YY/MM/DD HH:MM CLASS    INTENT   ALLOW
ACCESS2  SYSGRP   OPERATIONS   ACCESS2  LTRM1000 ACCESS   SUCCESS  09/01/30 13:34 DATASET  READ     NONE
                                                                                  TSS000 RACF.JCL
BATH131  TSSGRP   OPERATIONS   BATHJOBX          ACCESS   SUCCESS  09/01/30 09:27 DATASET  READ     NONE
                                                                                  LIBA00 BATCH33.WORK.FILE
BATH131  TSSGRP   OPERATIONS   BATHJOBX          ACCESS   SUCCESS  09/01/30 09:27 DATASET  READ     NONE
                                                                                  LIBA00 LIBRARY.BAT.DS1
BATH131  TSSGRP   OPERATIONS   BATHJOBX          ACCESS   SUCCESS  09/01/30 09:27 DATASET  READ     NONE
                                                                                  LIBA00 LIBRARY.BAT.DS2
BATH131  TSSGRP   OPERATIONS   BATHJOBX          ACCESS   SUCCESS  09/01/30 09:27 DATASET  READ     NONE
                                                                                  LIBA00 LIBRARY.BAT.DS3
BATH131  TSSGRP   OPERATIONS   BATHJOBX          ACCESS   SUCCESS  09/01/30 09:27 DATASET  READ     NONE
                                                                                  LIBA00 LIBRARY.BAT.DS4

SYSTEM = IIM1 (OS:MSP     ,RACF:0013) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1408
```

Rpt 1.7　特権ユーザ利用状況レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT    10
PSW=SW60                                 ---- TRUST PRIVILEGED USER SUMMARY REPORT ----                         VER=09 LVL=99

                                                                    *-TIME STAMP-* RESOURCE
USER-ID  GROUP-ID AUTHORITY    JOBNAME  TERMINAL COMMAND  RESULT   YY/MM/DD HH:MM /OBJECT  INTENT   ALLOW
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 LOGON    SUCCESS  09/01/30 05:53
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 DATASET  WRITE
                                                                                  VOSSYS SYS1.BRODCAST
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 VOLUME   SPACEA
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 VOLUME   SPACEA
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 DATASET  USE
                                                                                  CTLG01 SYS2.LINKLIB
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 DATASET  USE
                                                                                  CTLG01 SYS2.CMDLIB
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 DATASET  USE
                                                                                  CTLG01 SYS2.LINKLIB
VOSUSER  SYS1     SYSMGR       VOSUSER  PTSS0002 ACCESS   SUCCESS  09/01/30 05:53 DATASET  USE
                                                                                  CTLG01 SYS1.ASPEN.UOCLIB

SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 FRI 1521
```

Rpt 1.7　特権ユーザ利用状況レポートの例（日立）

この特権ユーザ利用状況レポートの内容は次のようになっています。

USER-ID	ユーザ ID
GROUP-ID	グループ ID
AUTHORITY	資源にアクセスしたユーザの権限や属性※1
JOBNAME	ジョブ名
TERMINAL	端末名
COMMAND	コマンド名
RESULT	実行結果
SUCEESS	ー 正常
FAILURE	ー 失敗
WARNING	ー 警告（IBM システムのみ）
TIME STAMP	実行日時
RESOURCE CLASS	リソース種別名
RESOURCE/OBJECT	リソース種別名
INTENT	ユーザが要求したアクセス権※2
ALLOW	セキュリティツールが許可したアクセス権※2

※1 「1.3 サマリー・レポート（SW20,SW21,SW22）」の【解説】ユーザの権限・属性をご覧ください。
※2 「1.4 リソース・アクセス・エラー・レポート（SW30）」の【解説】要求アクセス権と許可アクセス権をご覧ください。

1.8　ユーザ毎の最終アクセス・レポート（SW70,SELRSCSW,SELNMCHK）

ユーザ毎の最終アクセス･レポートでは、ユーザ毎のシステム利用状況をサマリーして示します。セキュリティツールのログ収集方法によっては正常なアクセスのログが収集されないことがある為、SELRSCSWスイッチで解析対象ログの選択が可能となっています。このレポートのユーザはグループID、ユーザIDと権限･属性の組み合わせが一意になるようにしています。また、IBM システムの場合、SELNMCHKスイッチでユーザ名を含めることもできます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2008        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    41
PSW=SW70                                 ---- RACF USER ACCESS SUMMARY REPORT ----                              VER=09 LVL=99

                              *-- START --* *-- STOP --* *---------- COUNT ----------*
GROUP-ID USER-ID  AUTHORITY   YY/MM/DD HH:MM YY/MM/DD HH:MM INIT   TERM   OTHER  ERROR  *-USER NAME (ACEE)-* *- COMMENTS -*
*        *        ............ 05/02/08 06:02 05/02/08 12:05      9      9 ...... ......
_BLANK_  UIDERRA               05/02/08 09:34 05/02/08 09:34 ...... ...... ......      1
GRPAO    JOBNO04  NORMAL       05/02/08 11:32 05/02/08 11:39 ...... ......     18 ...... ..................
GRPCD    AAAA041  NORMAL       05/02/08 13:19 05/02/08 18:11 ...... ......      5 ...... ..................
         AAAA041  ............ 05/02/08 18:27 05/02/08 18:27      1      1 ...... ......
  |        |        |            |     (中略)          |
_TOTAL_                                                  153    142    179      4

SYSTEM = IIM0 (OS:MVS    ,RACF:7709) START = 05/02/08 TUE 0002 END = 05/02/08 TUE 2359   REPORTING DATE = 08/01/31 THU 1658
```

Rpt 1.8　ユーザ毎の最終アクセス・レポートの例（IBM）

■富士通システムの場合

```
(C) I I M  CORP.  1987-2008        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT     9
PSW=SW70                                 ---- RACF USER ACCESS SUMMARY REPORT ----                              VER=09 LVL=99

                              *-- START --* *-- STOP --* *---------- COUNT ----------* *- COMMENTS -*
GROUP-ID USER-ID  AUTHORITY   YY/MM/DD HH:MM YY/MM/DD HH:MM INIT   TERM   OTHER  ERROR
*        FUIDTRC  NORMAL       05/02/08 17:03 05/02/08 17:03      1 ...... ......      1
         UIDF109  NORMAL       05/02/08 11:31 05/02/08 19:34      2 ...... ......      2
         UIDF367  NORMAL       05/02/08 11:45 05/02/08 11:45      1 ...... ......      1
GRPDBM   UIDK051  NORMAL       05/02/08 13:28 05/02/08 18:58 ...... ......     27 ......
         UIDR012  SPECIAL      05/02/08 11:31 05/02/08 11:31 ...... ......      1 ......
         UIDR012  NORMAL       05/02/08 12:53 05/02/08 17:18 ...... ......     12 ......
GRPSSS   UIDN002  NORMAL       05/02/08 10:16 05/02/08 15:36 ...... ......     90 ......
GRPTTT   UIDF048  NORMAL       05/02/08 11:23 05/02/08 12:00 ...... ......      7 ......
         UIDF361  NORMAL       05/02/08 11:43 05/02/08 16:58 ...... ......     30 ......
  |        |        |            |     (中略)          |
_TOTAL_                                                    4      0   4301      4

SYSTEM = IIM1 (OS:MSP    ,RACF:0014) START = 05/02/08 TUE 0002 END = 05/02/08 TUE 2359   REPORTING DATE = 08/01/31 THU 1655
```

Rpt 1.8　ユーザ毎の最終アクセス・レポートの例（富士通）

■日立システムの場合

```
(C) I I M  CORP.  1987-2007        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT    10
PSW=SW70                                 ---- TRUST USER ACCESS SUMMARY REPORT ----                             VER=09 LVL=99

                              *-- START --* *-- STOP --* *---------- COUNT ----------* *- ACCESS COUNT-* *- COMMENTS -*
GROUP-ID USER-ID  AUTHORITY   YY/MM/DD HH:MM YY/MM/DD HH:MM INIT   TERM   OTHER  ERROR  TOTAL   ERROR
_BLANK_  _BLANK_              05/02/08 18:04 05/02/08 22:41 ...... ......      3      3
         UIDE30               05/02/08 15:43 05/02/08 15:43      1 ...... ......      1                  UNDEFINED USER
         UIDV00               05/02/08 08:05 05/02/08 08:05      1 ...... ......      1                  UNDEFINED USER
_SYSTEM_ _SYSTEM_             05/02/08 07:23 05/02/08 07:23 ...... ......      1 ......
GRPD02   UIDD31               05/02/08 11:46 05/02/08 14:52      4      4      4 ......
         UIDD41               05/02/08 14:59 05/02/08 15:33      2      2      2 ......
         UIDD51               05/02/08 10:37 05/02/08 15:17      4      4      4 ......
GRPD03   UIDD15               05/02/08 17:29 05/02/08 17:38      1      1      1 ......
         UIDD16               05/02/08 10:21 05/02/08 11:50      4      4      4 ......
  |        |        |            |     (中略)          |
_TOTAL_                                                 1677   1576   1100     98    252      0

SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 05/02/08 TUE 0002 END = 05/02/08 TUE 2359   REPORTING DATE = 07/06/07 THU 1659
```

Rpt 1.8　ユーザ毎の最終アクセス・レポートの例（日立）

このユーザ毎の最終アクセス・レポートの内容は次のようになっています。

GROUP-ID　　グループ ID
USER-ID　　ユーザ ID
AUTHORITY　　資源にアクセスしたユーザの権限や属性※
IBM と富士通システムの場合、ジョブ開始・終了レコードを解析対象として選択（SELRSC SW）した際には、この欄は欠損値「.....」で表示されることがある。これは、ジョブ開始・終了レコードと RACF レコードがマージできなかったことを意味する。

※「1.3 サマリー・レポート(SW20,SW21,SW22)」の【解説】ユーザの権限・属性をご覧ください。

START　　最初のアクセス日時
STOP　　最終アクセス日時
COUNT
 INIT　　ジョブ数/LOGON 回数
 TERM　　終了した回数
 OTHER　　資源アクセスやコマンド実行回数
 ERROR　　アクセスエラー回数
COMMENTS　　ユーザ ID が未定義の場合に ‘UNDEFINED USER’ が表示される。

■IBM システムの場合
USER NAME (ACEE)　　ユーザ名

■日立システムの場合
ACCESS COUNT
 TOTAL　　リソース・アクセスの総回数
 ERROR　　リソース・アクセスエラー回数

【注意点】

このレポートに出力されるアクセス日時やCOUNT欄の回数はSELRSCSWスイッチの指定に従い次のように取得しています。

○アクセス日時

	START 欄	STOP 欄
SELRSCSW=0	開始事象	終了事象
SELRSCSW=1	全事象	全事象
SELRSCSW=2	全事象とタイプ 20	全事象とタイプ 20
SELRSCSW=3	全事象とタイプ 30-1	全事象とタイプ 30-1/5

○開始・終了回数

	INIT 欄	TERM 欄
SELRSCSW=0	開始事象	終了事象（IBM）
SELRSCSW=1	開始事象	終了事象（IBM）
SELRSCSW=2	タイプ 20	終了事象（IBM）
SELRSCSW=3	タイプ 30-1	タイプ 30-5

○事象発生回数

OTHER欄とERROR欄はセキュリティツールのログ情報から取得しているため、SELRSCSWスイッチの指定は関係ありません。

SELRSCSW=2/3を指定した場合には次のように動作します。
1)ジョブ開始・終了レコードにユーザ権限が記録されていないためユーザ権限や属性が明示されないことがあります。
2) INIT 欄にはジョブ開始時の RACF エラーはカウントされず、ERROR 欄に示されます。

1.9　特定ユーザのトレース・レポート（SW80,TUID,SW80OPT）

特定ユーザのトレース・レポートでは、指定された特定ユーザの利用状況をアクセスした際の状況を時系列に示します。入力のコントロールスイッチで SELDSNSW=1が設定されておりリソース種別名が「DATASET」の場合には、次の行にボリューム通番とデータセット名が表示されます。IBMと富士通システムの場合、ジョブ開始・終了レコードが解析対象として選択されている際（SELRSCSW）に、SW80OPT=1でそれらのレコードもレポートに表示することができます。

■IBMシステムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    15
PSW=SW80,TUID                            ------ RACF USER TRACE REPORT ( SPUSR4 ) ------                          VER=09 LVL=99

        *-TIME STAMP-*                                                          RESOURCE
EVENT   YY/MM/DD HH:MM RESULT  CODE GROUP-ID AUTHORITY    JOBNAME  TERMINAL CLASS    INTENT  ALLOW   *-USER NAME (ACEE)-*
ACCESS  09/01/30 21:51 SUCCESS 0200 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET  ALTER   ALTER   SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
ACCESS  09/01/30 21:51 SUCCESS 0200 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET  UPDATE  ALTER   SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
ACCESS  09/01/30 21:52 SUCCESS 0200 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET  UPDATE  ALTER   SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
ACCESS  09/01/30 21:52 SUCCESS 0200 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET  UPDATE  ALTER   SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
ACCESS  09/01/30 21:52 SUCCESS 0200 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET  ALTER   ALTER   SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
DELRES  09/01/30 21:52 SUCCESS 0500 SPCGRP   NORMAL       SPUSR4   TS000200 DATASET                  SPECIAL USER4
                                                                            HOST04 HOST.SPUSR4.TEST.DATA1
*** TOTAL COUNT : 101

SYSTEM = IIM0 (OS:MVS     ,RACF:7709) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1114
                                                                        Rpt 1.9　特定ユーザのトレース・レポートの例（IBM）
```

■富士通システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITPRT    16
PSW=SW80,TUID                            ------ RACF USER TRACE REPORT ( ACCESS2 ) ------                         VER=09 LVL=99

        *-TIME STAMP-*                                                          RESOURCE                *--ACCESS CHECK-*
EVENT   YY/MM/DD HH:MM RESULT  CODE GROUP-ID AUTHORITY    JOBNAME  TERMINAL CLASS    INTENT  ALLOW   CHECK    TYPE
ACCESS  09/01/30 09:28 SUCCESS 0200 SYSGRP   NORMAL       ACCESS2  LTRM2000 DATASET  READ    ALTER   DEFAULT
                                                                            TSS000 ACCESS2.RACF.JCL
ACCESS  09/01/30 09:29 SUCCESS 0200 SYSGRP   NORMAL       ACCESS2  LTRM2000 DATASET  UPDATE  ALTER   DEFAULT
                                                                            WORK02 ACCESS2.WORK.DS1
ACCESS  09/01/30 09:29 SUCCESS 0200 SYSGRP   NORMAL       ACCESS2  LTRM2000 DATASET  READ    ALTER   DEFAULT
                                                                            WORK02 ACCESS2.WORK.DS1
ACCESS  09/01/30 09:29 SUCCESS 0200 SYSGRP   NORMAL       ACCESS2  LTRM2000 DATASET  ALTER   ALTER   DEFAULT
                                                                            WORK02 ACCESS2.WORK.DS1
JOBINIT 09/01/30 13:17 FAILURE 0101 *        NORMAL                LTRM1000
JOBINIT 09/01/30 13:17 FAILURE 0101 *        NORMAL                LTRM1000
JOBINIT 09/01/30 13:17 FAILURE 0101 *        NORMAL                LTRM1000
ACCESS  09/01/30 13:34 SUCCESS 0200 SYSGRP   OPERATIONS   ACCESS2  LTRM1000 DATASET  READ    NONE    DEFAULT
                                                                            TSS000 RACF.JCL
*** TOTAL COUNT : 32

SYSTEM = IIM1 (OS:MSP     ,RACF:0013) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 MON 1408
                                                                        Rpt 1.9　特定ユーザのトレース・レポートの例（富士通）
```

■日立システムの場合

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                   AUDITPRT    14
PSW=SW80,TUID                            ------ TRUST USER TRACE REPORT ( UTRC20 ) ------                         VER=09 LVL=99

        *-TIME STAMP-*                                                          RESOURCE
EVENT   YY/MM/DD HH:MM RESULT  CODE GROUP-ID AUTHORITY    JOBNAME  TERMINAL /OBJECT  INTENT  ALLOW
ACCESS  09/01/30 09:45 SUCCESS 0000 GRP2                 UTRC20A           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
ACCESS  09/01/30 09:47 SUCCESS 0000 GRP2                 UTRC20A           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
ACCESS  09/01/30 10:10 SUCCESS 0000 GRP2                 UTRC20A           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
ACCESS  09/01/30 10:15 SUCCESS 0000 GRP2                 UTRC20A           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
ACCESS  09/01/30 10:16 SUCCESS 0000 GRP2                 UTRC20B           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
ACCESS  09/01/30 10:23 SUCCESS 0000 GRP2                 UTRC20A           DATASET  READ
                                                                            VOS400 ACCESS.DATASET.A1
*** TOTAL COUNT : 6

SYSTEM = IIM2 (OS:VOS3   TRUST:0004) START = 09/01/30 FRI 0002 END = 09/01/30 FRI 2359   REPORTING DATE = 09/02/02 FRI 1521
                                                                        Rpt 1.9　特定ユーザのトレース・レポートの例（日立）
```

この特定ユーザのトレース・レポートの内容は次のようになっています。

EVENT	事象
TIME STAMP	事象発生日時
RESULT	実行結果
SUCEESS	ー 正常
FAILURE	ー 失敗
WARNING	ー 警告（IBM システムのみ）
CODE	事象コードと事象コード修飾子
GROUP-ID	グループ ID
AUTHORITY	資源にアクセスしたユーザの権限や属性※1
JOBNAME	ジョブ名
TERMINAL	端末名
RESOURCE CLASS	資源名（クラス名）
かあるいは	
RESOURCE/OBJECT	資源名（オブジェクト名）
INTENT	ユーザが要求したアクセス権※2
ALLOW	セキュリティツールが許可したアクセス権※2

※1「1.3 サマリー・レポート(SW20,SW21,SW22)」の【解説】ユーザの権限・属性をご覧ください。
※2「1.4 リソース・アクセス・エラー・レポート(SW30)」の【解説】要求アクセス権と許可アクセス権をご覧ください。

■IBM システムの場合

USER NAME (ACEE)	ユーザ名

IBM と富士通システムでジョブ開始・終了レコードが解析対象の場合、下記の項目だけが有効です。

EVENT	
JOBSTART	ジョブ開始
JOBEND	ジョブ終了
TIMESTAMP	
RESULT	常に正常
GROUP-ID	
AUTHORITY	常に欠損値
JOBNAME	
TERMINAL	

■富士通システムの場合

ACCESS CHECK	
CHECK	アクセス権をチェックする際のユーザの権限や属性
GLOBAL	ー グローバルチェック機能
GENERIC	ー 総称名機能
DEFAULT	ー 省略値保護機能
DISCRETE	ー 個別名保護機能
UNIFYDS	ー 未登録データセットの一括保護機能
TYPE	アクセス権種別
USERACS	ー 利用者への特定アクセス権
GRPACS	ー グループへの特定アクセス権
PUSERACS	ー 利用者への特定パスアクセス権
PGRPACS	ー グループへの特定パスアクセス権
PPATHACS	ー 公衆パスアクセス権
UNIVACS	ー 公衆アクセス権
UNDEFTRM	ー 未登録端末の公衆アクセス権
GRPTUACS	ー 端末利用者限定属性
COACCACC	ー グループ公衆アクセス権
GLBLACS	ー グローバルアクセス権
GPATHACS	ー グローバルパスアクセス権
空白	ー 上記以外

第2章 DSNCSV00 の使用方法

DSNCSV00プロセジャはデータセットに対するアクセス履歴情報をCSV形式で出力します。出力されたCSVファイルをユーザプログラムや表計算プログラムで処理し、目的とするデータセットのアクセス状況を追跡することができます。これにより、データセットの使用状況を調査したり、ユーザのアクセス状況を監査することができます。CSVファイルに出力する内容はレコードタイプやユーザ／ジョブ名、およびボリューム名、データセット名で選択することが出来ます。

DSNCSV00プロセジャでは、次の解析が可能です。

■ODAMクローズレコード(日立のみ)
■INPUT,RDBACKデータセット活動
■OUTPUT,UPDAT,INOUT,OUTINデータセット活動
■スクラッチ・データセット状況
■非VSAMデータセットの名前変更状況
■VSAMボリューム・データセットの更新(IBM／富士通のみ)
■総合カタログ機能定義活動(IBMのみ)
■BCSレコード追加(富士通のみ)
■VSAMコンポーネントまたはクラスタのOPEN
■VSAMコンポーネントまたはクラスタのCLOSE
■総合カタログ機能の削除活動(IBMのみ)
■総合カタログ機能の更新活動(IBMのみ)
■BCSレコード削除(富士通のみ)
■BCSレコード更新(富士通のみ)
■VSAMスクラッチレコード(富士通／日立のみ)
■VSAMリネームレコード(富士通／日立のみ)
■ジョブ開始レコード
■TSS情報レコード(富士通のみ)
■TISP/BP課金情報レコード(富士通FTPクライアントのみ)
■TCP/IP統計レコード(IBMFTPサーバの取り出し)

このプロセジャでは次のパフォーマンス・データを使用します。

IBM	: 14、15、17、18、20、30－1、60、61、62、64、65、66、118－74
富士通	: 14、15、17、18、20、30－1、60、61、62、64、65、66、67、68、97、101
日立	: 13、14、15、17、18、20、62、64、67、68

このプロセジャは入力データ量、解析対象範囲、出力レコードなどにより大量の資源を使用します。
プロセジャ実行時には、追跡対象のジョブやボリューム等に絞り込みを行ってから実行してください。

2.1 実行パラメータ

DSNCSV00プロセジャ用サンプルジョブ制御文のDD文“PLATFORM”では、プロセジャの実行パラメータ指定部とプロセジャ本体が連結データセットとして定義されています。実行パラメータには、セレクション・スイッチとコントロール・スイッチがあります。

```
//DSNCSV00 JOB  (ACCT),MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,NOTIFY=USERID
//JOBLIB   DD  DSN=CPE.LOAD,DISP=SHR
//*JOBCAT   DD  DSN=USER.CAT,DISP=SHR
//*********************************************************************
//*  プロダクト名 : SAMPLE ( MF-ADVISOR )   プロセジャ名 : DSNCSV00   *
//*-------------------------------------------------------------------*
//*   JCLの以下のデータセット名を変更してください。                   *
//*    ES/1 NEO LIBRARY                                               *
//*           - CPE.LOAD    ( ロードモジュールライブラリ )            *
//*           - CPE.SAMP    ( サンプル・ライブラリ )                  *
//*    INPUT   - INPUT.DATA  ( 解析対象のSMF(SMS)データ )             *
//*    BASICUT1- OUTPUT.CSVFILE   ( CSVファイル )                     *
//*           - VOLSER           ( CSVファイル格納ボリューム)         *
//************************************************** SINCE V05L14 **
//SHELL    EXEC PGM=CPESHELL,REGION=4096K
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSUT1   DD  UNIT=SYSDA,SPACE=(TRK,(10,5))
//INPUT    DD  DISP=SHR,DSN=INPUT.DATA
//BASICUT1 DD  DSN=OUTPUT.CSVFILE,DISP=(NEW,CATLG,DELETE),
//             UNIT=SYSDA,SPACE=(CYL,(2,1),RLSE),VOL=SER=VOLSER
//PLATFORM DD  *
*
*       セレクション・スイッチ  ／  コントロール・スイッチ
*
        DATESW   = 0                    日付指定制御SW ( 0:YYDDD 1:YYMMDD )
        SEL1     = 00000                処理開始日( YYDDD/YYMMDD )
        SEL2     = 0000                 処理開始時刻( HHMM )
        SEL3     = 99999                処理終了日( YYDDD/YYMMDD )
        SEL4     = 2400                 処理終了時刻( HHMM )
*
        DTMAKER  = 1                    OS種別( 1:IBM 2:FJ 3:HT )
*
        SW013    = 1                    SMSタイプ13     ODAM  クローズレコード (日立のみ)
        SW014    = 1                    SMF/SMSタイプ14 INPUT,RDBACK データセット活動
        SW015    = 1                    SMF/SMSタイプ15 OUTPUT,UPDAT,INOUT,OUTIN データセット活動
        SW017    = 1                    SMF/SMSタイプ17 スクラッチ・データセット状況
        SW018    = 1                    SMF/SMSタイプ18 非VSAM データセットの名前変更状況
        SW020    = 1                    SMF/SMSタイプ20 ジョブ開始レコード
        SW0301   = 1                    SMFタイプ30サブタイプ1
                                                ジョブ開始レコード(IBM/富士通のみ)
        SW060    = 1                    SMFタイプ60     VSAMボリューム・データセットの更新(IBM/富士通のみ)
        SW061    = 1                    SMFタイプ61     総合カタログ機能定義活動またはBCSレコード追加
                                                                (IBM/富士通のみ)
        SW062    = 1                    SMF/SMSタイプ62 VSAMコンポーネントまたはクラスタのOPEN
        SW064    = 1                    SMF/SMSタイプ64 VSAMコンポーネントまたはクラスタのCLOSE
        SW065    = 1                    SMFタイプ65     総合カタログ機能の削除活動／BCSレコード削除
                                                            (IBM/富士通のみ)
        SW066    = 1                    SMFタイプ66     総合カタログ機能の更新活動／BCSレコード更新
                                                            (IBM/富士通のみ)
        SW067    = 1                    SMF/SMSタイプ67 VSAMスクラッチレコード(富士通/日立のみ)
        SW068    = 1                    SMF/SMSタイプ68 VSAMリネームレコード(富士通/日立のみ)
        SW097    = 1                    SMFタイプ97     TSS情報レコード(富士通のみ)
        SW101    = 1                    SMFタイプ101    TISP/BP課金情報レコード(富士通FTPクライアントのみ)
        SW118    = 1                    SMFタイプ118    FTPサーバの取り出し(IBMのみ)
*
        ECONCAT  = 1                    連結データセット情報出力抑止  (0:抑止しない 1:抑止する)
        ETEMPDS  = 1                    一時データセット情報出力抑止  (0:抑止しない 1:抑止する)
        EVTOCDS  = 1                    VTOCデータセット情報出力抑止  (0:抑止しない 1:抑止する)
        SELUNIT  = 0                    入出力装置タイプの選択
*                                         0:すべて出力
*                                         1:ディスク装置のみ
*                                         2:テープ装置のみ
*
        DIM SDSN(10),SDSN2(10),SDSN3(10)  変数配列の定義
*       SDSN (1)='DATASET_NAME1*'       検査対象データセット名(1)
*       SDSN2(1)=''
*       SDSN3(1)=''
*       SDSN (2)='DATASET_NAME2*'       検査対象データセット名(2)
*       SDSN2(2)=''
*       SDSN3(2)=''
        SDSN=0                          検査対象データセット数
*
        DIM EDSN(10),EDSN2(10),EDSN3(10)  変数配列の定義
*       EDSN (1)='DATASET_NAME1*'       検査対象外データセット名(1)
*       EDSN2(1)=''
*       EDSN3(1)=''
*       EDSN (2)='DATASET_NAME2*'       検査対象外データセット名(2)
*       EDSN2(2)=''
*       EDSN3(2)=''
        EDSN=0                          検査対象外データセット数
```

```
*
        DIM SJOB(10)                    変数配列の定義
        SJOB(1)='JOB01*'                検査対象ジョブ名(1)
        SJOB(2)='JOB02*'                検査対象ジョブ名(2)
        SJOB=0                          検査対象ジョブ数
*
        DIM EJOB(10)                    変数配列の定義
        EJOB(1)='TEST0*'                検査対象外ジョブ名(1)
        EJOB(2)='TEST1*'                検査対象外ジョブ名(2)
        EJOB=0                          検査対象外ジョブ数
*
        DIM SVOL(10)                    変数配列の定義
        SVOL(1)='VOL00*'                検査対象ボリューム名(1)
        SVOL(2)='VOL10*'                検査対象ボリューム名(2)
        SVOL=0                          検査対象ボリューム数
*
        DIM EVOL(10)                    変数配列の定義
        EVOL(1)='WORK*'                 検査対象外ボリューム名(1)
        EVOL(2)='TEMP*'                 検査対象外ボリューム名(2)
        EVOL=0                          検査対象外ボリューム数
*
        DIM SRACFU(10)                  変数配列の定義
        SRACFU(1)='RACF1*'              解析対象RACF ID名(1)
        SRACFU(2)='RACF2*'              解析対象RACF ID名(2)
        SRACFU=0                        解析対象RACF ID数
*
        DIM ERACFU(10)                  変数配列の定義
        ERACFU(1)='RACF1*'              解析対象外RACF ID名(1)
        ERACFU(2)='RACF2*'              解析対象外RACF ID名(2)
        ERACFU=0                        解析対象外RACF ID数
*
        DIM SRACFG(10)                  変数配列の定義
        SRACFG(1)='RACFG1*'             解析対象RACFグループ名(1)
        SRACFG(2)='RACFG2*'             解析対象RACFグループ名(2)
        SRACFG=0                        解析対象RACFグループ数
*
        DIM ERACFG(10)                  変数配列の定義
        ERACFG(1)='RACFG1*'             解析対象外RACFグループ名(1)
        ERACFG(2)='RACFG2*'             解析対象外RACFグループ名(2)
        ERACFG=0                        解析対象外RACFグループ数
*
        DIM SUSER(10)                   変数配列の定義
        SUSER(1)='USER01*'              解析対象ユーザID名(1)
        SUSER(2)='USER02*'              解析対象ユーザID名(2)
        SUSER=0                         解析対象ユーザID数
*
        DIM EUSER(10)                   変数配列の定義
        EUSER(1)='USER0X*'              解析対象外ユーザID名(1)
        EUSER(2)='USER0Y*'              解析対象外ユーザID名(2)
        EUSER=0                         解析対象外ユーザID数
*
        DIM SADR(10)                    変数配列の定義
        SADR(1)='10*'                   解析対象装置アドレス名(1)
        SADR(2)='00*'                   解析対象装置アドレス名(2)
        SADR=0                          解析対象装置アドレス数
*
        DIM EADR(10)                    変数配列の定義
        EADR(1)='1001'                  解析対象外装置アドレス名(1)
        EADR(2)='1002'                  解析対象外装置アドレス名(2)
        EADR=0                          解析対象外装置アドレス数
*
        DIM SPGM(10)                    変数配列の定義
        SPGM(1)='PGM01*'                解析対象プログラム名(1)
        SPGM(2)='PGM02*'                解析対象プログラム名(2)
        SPGM=0                          解析対象プログラム数
*
*       CHGUSRID='(UNKNON)'             ユーザーIDの文字列置換
*       SYSID = ' '                     評価対象システム識別コード
*       RECLIMIT=1000                   CSV出力件数の上限値
        FIXSW=0                         出力桁数固定設定
*
        NOLIST
//       DD DSN=CPE.SAMP(DSNCSV00),DISP=SHR
```

Jcl 2.1サンプル・ジョブ制御文（JCDSNCSV）

2.1.1. セレクション・スイッチ

セレクション・スイッチでは、解析対象とするべき時間帯を指定します。

DTMAKER

メーカの選択[必須]

入力するSMF/SMSレコード群が収集されたオペレーティング・システムの種別を指定してください。

DTMAKER=1　　IBMシステムのSMFレコード群
DTMAKER=2　　富士通システムのSMFレコード群
DTMAKER=3　　日立システムのSMSレコード群

DATESW

日付形式

SEL1(開始日)とSEL3(終了日)で解析対象日を指定する際、DATESWを“1”に設定すると、SEL1とSEL3の日付けをYYMMDD(グレゴリアン暦)で指定することができます。

SEL1～SEL4

入力データ・レンジ

解析対象とするべきSMF/SMSレコードの日時の範囲を指定します。

SEL1　開始日　(形式はYYDDDまたはYYMMDD)
SEL2　開始時刻　(形式はHHMM)
SEL3　終了日　(形式はYYDDDまたはYYMMDD)
SEL4　終了時刻　(形式はHHMM)

入力されたSMF/SMSレコード群の中から指定された時間帯のデータのみを抽出する為、SEL1とSEL2で指定された開始時刻以前のデータはすべて読み飛ばします。開始時刻以降でかつSEL3とSEL4で指定された終了時刻以前のデータが解析対象となります。但しADVISORのみご契約の場合は、最初に解析を開始した時刻以降、24時間分を処理しても終了時刻とならない場合、終了時刻の指定に拘わらずプロセジャは解析作業を終了します。

1.日付＝省略時
・MAGICライセンス無→最初のレコードから24時間
・MAGICライセンス有→最初のレコードから1ヶ月
※「最初のレコード」:対象レコードで最初に読込んだレコード。これを基準に各レコードの「レコード出力日時」を確認して処理範囲を選択。

[省略値]

```
SEL1=00000
SEL2=0000
SEL3=99999
SEL4=2400
DATESW=0
```

2.日付＝指定時
・MAGICライセンス無→範囲が24時間を越えている場合、SEL1+SEL2から24時間で抑止。
・MAGICライセンス有→設定された日時範囲を全て出力。

[設定例]

```
DATESW=1
SEL1=070801
SEL2=0900
SEL3=070802
SEL4=0900
```

2000年以降の指定について

SEL1とSEL3で指定する日付は1900年代であっても2000年代であっても、下位2桁のみをYY部で指定します。この為、YY部が00～49の場合には2000～2049年、YY部が50～99の場合には1950～1999年の指定として評価を行います。

注意点

1. 開始時刻(SEL2)と終了時刻(SEL4)のみの指定はできません。
2. DAY関数は年を跨ったデータを処理することができません。このような処理を行う場合は次のように記述してください。

【例】2009年1月1日に2008年12月31日0時から実行時までのデータを評価対象とする。

```
DATESW=0
SEL1=&YYDDD(&CENTURY(DAY)-1)
SEL2=0000
SEL3=DAY
SEL4=2400
```

2.1.2. コントロール・スイッチ

コントロール・スイッチでは、入力データ群の選択などを指定します。

パラメータ	内容	レコードタイプ（SWnnn）																	
		13	14	15	17	18	20	30.1	60	61	62	64	65	66	67	68	97	101	118
ECONCAT	連結 DS 情報の出力抑止	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
ETEMPDS	一時 DS 情報の出力抑止	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
EVTOCDS	VTOCDS 情報の出力抑止	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
SELUNIT	入出力装置タイプの選択	○	○	○	－	－	－	－	－	－	－	－	－	－	－	－	－	－	－
S/EDSN	出力、抑止 DS の選択	○	○	○	○	○	－	－	○	○	○	○	○	○	○	○	○	○	○
S/EJOB	出力、抑止 JOB の選択	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	－	－
S/EADR	出力、抑止装置アドレスの選択	○	○	○	－	－	－	－	－	－	－	○	－	－	－	－	－	－	－
S/EVOL	出力、抑止 VOL の選択	○	○	○	○	○	－	－	－	－	○	○	－	－	－	－	－	－	－
S/ERACFU	出力、抑止 RACF ユーザの選択	－	－	－	－	－	○	○	－	－	－	－	－	－	－	－	－	－	－
S/ERACFG	出力、抑止 RACF グループの選択	－	－	－	－	－	○	○	－	－	－	－	－	－	－	－	－	－	－
S/EUSER	出力、抑止ユーザ ID の選択	－	○※	○※	○※	○※	－	－	－	－	－	－	－	－	－	－	○	○	○
SPGM	出力プログラム名の選択		○※	○※															

※IBMのみ

SWnnn

SMF/SMSレコードの選択

解析対象とするSMF/SMSレコードを選択します。省略値は全て“0”です。

SW013=1	SMSタイプ13
SW014=1	SMF/SMSタイプ14
SW015=1	SMF/SMSタイプ15
SW017=1	SMF/SMSタイプ17
SW018=1	SMF/SMSタイプ18
SW020=1	SMF/SMSタイプ20
SW0301=1	SMFタイプ30サブタイプ1
SW060=1	SMFタイプ60
SW061=1	SMFタイプ61
SW062=1	SMF/SMSタイプ62
SW064=1	SMF/SMSタイプ64
SW065=1	SMFタイプ65
SW066=1	SMFタイプ66
SW067=1	SMF/SMSタイプ67
SW068=1	SMF/SMSタイプ68
SW097=1	SMFタイプ97（FIMPORTとFEXPORT）
SW101=1	SMFタイプ101（FTPクライアントのみ）
SW118=1	SMFタイプ118（FTPサーバの取り出し）

ECONCAT

連結データセット情報の出力抑止

SMF/SMSレコードタイプ14,15では、連結データセットの2つ目以降のデータセット名がSMF/SMSレコード自体に格納されません。この場合、出力されるCSV形式ファイルにおいても、データセット名が不明確な情報の為にファイル容量が大きくなる可能性があります。連結データセット情報が不必要な場合、ECONCATに“1”を指定すると連結データセット情報の出力を抑止します。

ECONCAT=0	連結データセット情報の出力を抑止しない（省略値）
ECONCAT=1	連結データセット情報の出力を抑止する

ETEMPDS

一時データセット情報の出力抑止

一時データセットの情報を管理する必要がない場合、ETEMPDSに“1”を指定すると一時データセット情報の出力を抑止します。

ETEMPDS=0	一時データセットのレコード出力を抑止しない（省略値）
ETEMPDS=1	一時データセットのレコード出力を抑止する

SMF/SMSレコードタイプ13、17では、一時データセットの判別ができません。データセットの除外にはEDSNスイッチを使用してください。

EVTOCDS

VTOCデータセット情報の出力抑止

VTOC領域をアクセスする際、プログラムは特殊なオープン処理を行います。この際、そのデータセット名は、判読不明な特殊文字列で構成されています。このようなデータセット名を検出すると、プロセジャでは自動的に次のようなデータセット名に置き換えます。

VOLUME_TABLE_OF_CONTENTS_(VTOC)

このようなデータセットの情報を管理する必要がない場合、EVTOCDSに“1”を指定するとVTOCデータセット情報の出力を抑止します。

EVTOCDS=0　　VTOCデータセットのレコード出力を抑止しない（省略値）
EVTOCDS=1　　VTOCデータセットのレコード出力を抑止する

SELUNIT

入出力装置タイプの選択

出力対象としたい入出力装置タイプを指定します。

SELUNIT=0　　すべての入出力装置タイプを出力する（省略値）
SELUNIT=1　　ディスク装置のみを出力する
SELUNIT=2　　テープ装置のみを出力する

SDSN(n)
SDSN2(n)
SDSN3(n)

出力対象データセットの選択

特定のデータセット情報のみを出力したい場合、SDSNにデータセット名を指定します。データセット名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)　データセット名が15文字より長い場合は、16字目以降をSDSN2(n)、SDSN3(n)に継続して指定します。

【例】以下の2つのデータセットを出力対象とする。

```
DSN1='IIM.USER001*'
DSN2='IIM.USER0001.IBM.SMFDATA.D070801.*'
DIM  SDSN(10),SDSN2(10),SDSN3(10)
SDSN(1)='IIM.USER001*'
* SDSN2(1)=''        ←コメント化
* SDSN3(1)=''        ←コメント化
SDSN(2)='IIM.USER0001.IB'
SDSN2(2)='M.SMFDATA.D0708'
SDSN3(2)='01.*'
SDSN=2
```

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

SDSN2(n)、SDSN3(n)を使用しない場合はコメント化して下さい。

SDSN2(n)、SDSN3(n)を使用しない場合はコメント化して下さい。
・TYPE14、15：連結データセット、一時データセット、VTOCデータセットは検索の対象外です。
・TYPE18：リネームは旧データセット名で検索を行います。

EDSN(n)
EDSN2(n)
EDSN3(n)

出力対象外データセットの選択

特定のデータセット情報のみを出力したくない場合、EDSNにデータセット名を指定します。データセット名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)　データセット名が15文字より長い場合は、16字目以降をEDSN2(n)、EDSN3(n)に継続して指定します。

【例】以下の2つのデータセットを出力対象とする。

```
DSN1='IIM.WORK*'
DSN2='IIM.USER00??.WORK*'
DIM  EDSN(10),EDSN2(10),EDSN3(10)
EDSN(1)='IIM.WORK*'
* EDSN2(1)=''        ←コメント化
* EDSN3(1)=''        ←コメント化
EDSN(2)='IIM.USER00??.WO'
EDSN2(2)='RK*'
* EDSN3(2)=''        ←コメント化
EDSN=2
```

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

SDSN2(n)、SDSN3(n)を使用しない場合はコメント化して下さい。

・TYPE14、15：連結データセット、一時データセット、VTOCデータセットは検索の対象外です。
・TYPE18：リネームは旧データセット名で検索を行います。

・SDSN/EDSNの両方を組み合わせて使用する場合、最初にSDSNのデータセットのみを抽出し、その後EDSNのデータセット名を除外します。
[例]'IIM'で始まるデータセットのみ抽出。ただし'IIM.WORK'で始まるデータセットは除外。
SDSN(1)='IIM*'
EDSN(1)='IIM.WORK*'
・SDSNとEDSNの指定内容が同じ、またはEDSNの方が指定範囲が広い場合、期待した抽出が出来ない場合がありますのでご注意下さい。
[例]'IIM.WORK'で始まるデータセットのみ抽出。ただし'IIM'で始まるデータセットは除外。
SDSN(1)='IIM.WORK*'
EDSN(1)='IIM*'
このような指定の場合EDSNが後に処理される為、'IIM'で始まるデータセットは全て除外。
なお、SVOL/EVOL、SJOB/EJOBも同様です。

SJOB

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象ジョブの選択

特定のジョブのアクセス情報のみを出力したい場合、SJOBにジョブ名を指定します。ジョブ名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SJOB(n)　　SJOBの最大配列数を指定してください。
SJOB(n)　　解析対象とするジョブ名を指定してください。

【例】JOB01xxxとJOB02xxxで始まるジョブを解析対象とする。

```
DIM SJOB(10)
SJOB(1)='JOB01*'
SJOB(2)='JOB02*'
SJOB=2
```

EJOB

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外ジョブの選択

特定のジョブのアクセス情報のみを出力したくない場合、EJOBにジョブ名を指定します。ジョブ名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM EJOB(n)　　EJOBの最大配列数を指定してください。
EJOB(n)　　解析対象外とするジョブ名を指定してください。

【例】TEST0xxxとTEST1xxxで始まるジョブを解析対象外とする。

```
DIM EJOB(10)
EJOB(1)='TEST0*'
EJOB(2)='TEST1*'
EJOB=2
```

SADR

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象装置アドレスの選択

特定の装置アドレスのアクセス情報のみを出力したい場合、SADRに装置アドレス名を指定します。装置アドレス名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SADR(n)　　SADRの最大配列数を指定してください。
SADR(n)　　解析対象とする装置アドレス名を指定してください。

【例】010xと020xで始まる装置アドレスを解析対象とする。

```
DIM SADR(10)
SADR(1)='010*'
SADR(2)='020*'
SADR=2
```

EADR

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外装置アドレスの選択

特定の装置アドレスのアクセス情報のみを出力したくない場合、EADRに装置アドレス名を指定します。装置アドレス名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM EADR(n)　EADRの最大配列数を指定してください。
EADR(n)　解析対象外とする装置アドレス名を指定してください。

【例】010xと020xで始まる装置アドレスを解析対象外とする。

```
DIM EADR(10)
EADR(1)='010*'
EADR(2)='020*'
EADR=2
```

SVOL

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象ボリュームの選択

特定ボリュームのアクセス情報のみを出力したい場合、SVOLにボリューム名を指定します。ボリューム名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SVOL(n)　SVOLの最大配列数を指定してください。
SVOL(n)　解析対象とするボリューム名を指定してください。

【例】VOL00xとVOL10xで始まるボリュームを解析対象とする。

```
DIM SVOL(10)
SVOL(1)='VOL00*'
SVOL(2)='VOL10*'
SVOL=2
```

EVOL

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外ボリュームの選択

特定ボリュームのアクセス情報のみを出力したくない場合、EVOLにボリューム名を指定します。ボリューム名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM EVOL(n)　EVOLの最大配列数を指定してください。
EVOL(n)　解析対象外とするボリューム名を指定してください。

【例】WORKxxとTEMPxxで始まるボリュームを解析対象外とする。

```
DIM EVOL(10)
EVOL(1)='WORK*'
EVOL(2)='TEMP*'
EVOL=2
```

SRACFU

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象RACFユーザの選択

ジョブ開始レコードにおいて、特定のRACFユーザのジョブ情報のみを出力したい場合、SRACFUにRACFユーザIDを指定します。RACFユーザIDの定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SRACFU(n)　SRACFUの最大配列数を指定してください。
SRACFU(n)　解析対象とするRACFユーザIDを指定してください。

【例】RACF1*とRACF2*で始まるRACFユーザを解析対象とする。

```
DIM SRACFU(10)
SRACFU(1)='RACF1*'
SRACFU(2)='RACF2*'
SRACFU=2
```

ERACFU

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外RACFユーザの選択

ジョブ開始レコードにおいて、特定のRACFユーザのジョブ情報を出力したくない場合、ERACFUにRACFユーザIDを指定します。RACFユーザIDの定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM ERACFU(n)	ERACFUの最大配列数を指定してください。
ERACFU(n)	解析対象外とするRACFユーザIDを指定してください。

【例】RACF1*とRACF2*で始まるRACFユーザを解析対象外とする。

```
DIM ERACFU(10)
ERACFU(1)='ERACF1*'
ERACFU(2)='ERACF2*'
ERACFU=2
```

SRACFG

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象RACFグループの選択

ジョブ開始レコードにおいて、特定のRACFグループのジョブ情報のみを出力したい場合、SRACFGにRACFグループ名を指定します。RACFグループ名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SRACFG(n)	SRACFGの最大配列数を指定してください。
SRACFG(n)	解析対象とするRACFグループ名を指定してください。

【例】RACFG1*とRACFG2*で始まるRACFグループを解析対象とする。

```
DIM SRACFG(10)
SRACFG(1)='RACFG1*'
SRACFG(2)='RACFG2*'
SRACFG=2
```

ERACFG

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外RACFグループの選択

ジョブ開始レコードにおいて、特定のRACFグループのジョブ情報を出力したくない場合、ERACFGにRACFグループ名を指定します。RACFグループ名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM ERACFG(n)	ERACFGの最大配列数を指定してください。
ERACFG(n)	解析対象外とするRACFグループ名を指定してください。

【例】RACFG1*とRACFG2*で始まるRACFグループを解析対象外とする。

```
DIM ERACFG(10)
ERACFG(1)='RACFG1*'
ERACFG(2)='RACFG2*'
ERACFG=2
```

SUSER

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象ユーザIDの選択

特定のユーザIDのアクセス情報のみを出力したい場合、SUSERにユーザIDを指定します。ユーザIDの定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SUSER(n)	SUSERの最大配列数を指定してください。
SUSER(n)	解析対象とするユーザID名を指定してください。

【例】USER01xxとUSER02xxで始まるユーザIDを解析対象とする。

```
DIM SUSER(10)
SUSER(1)='USER01*'
SUSER(2)='USER02*'
SUSER=2
```

EUSER

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象外ユーザIDの選択

特定のユーザIDのアクセス情報のみを出力したくない場合、EUSERにユーザIDを指定します。ユーザIDの定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM EUSER(n)　　EUSERの最大配列数を指定してください。
EUSER(n)　　解析対象外とするユーザID名を指定してください。

【例】USER0XxxとUSER0Yxxで始まるユーザIDを解析対象外とする。

```
DIM  EUSER(10)
EUSER(1)='USER0X*'
EUSER(2)='USER0Y*'
EUSER=2
```

SPGM

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

解析対象プログラム名の選択

特定のプログラム名のアクセス情報のみを出力したい場合、SPGMにプログラム名を指定します。
プログラム名の定義を簡略化する為に比較制御文字を利用した指定が可能です。(注)

DIM SPGM(n)　　SPGMの最大配列数を指定してください。
SPGM(n)　　解析対象とするプログラム名を指定してください。

【例】PGM01xxとPGM02xxで始まるプログラム名を解析対象とする。

```
DIM  SPGM(10)
SPGM (1)='PGM01*'
SPGM (2)='PGM02*'
SPGM=2
```

このパラメータは、IBM TYPE14, 15でのみ有効です。

CHGUSRID

ユーザーIDの文字列置換

ユーザーIDが"*"の場合、指定された文字列に置き換えます。SMF TYPE14,15,17,18で出力されるユーザーIDには"*"(アスタリスク)が設定される場合があります。ユーザーIDの選択パラメータ(S/EUSER)で使用する比較制御文字(*)と区別する際にご利用ください。省略値は"(UNKNON)"です。
S/EUSERパラメータでの選択・排他は、置き換え後の文字列で指定可能です。

SYSID

システム識別コード

指定されたシステム識別子のシステムのみを処理対象とします。省略値は全システムを出力します。

```
SYSID='cccc'
```

RECLIMIT

出力レコード件数の抑止

CSVファイルに出力するアクセス情報件数の上限値を指定します。指定された件数を超えると処理は中断されます。省略値は全件出力します。

```
RECLIMIT=nnnn
```

FIXSW

桁数固定形式での出力

出力項目の桁位置(桁数)を固定としたCSVファイル形式で出力します。項目と項目の間にはカンマ(,)が出力されます。またメーカやレコード毎に非出力となっている項目位置には、桁数分の空白とカンマが出力され、行の最後にもカンマが出力されます。

FIXSW=0　　桁数＝可変のCSV形式ファイルを出力する
FIXSW=1　　桁数＝固定のCSV形式ファイルを出力する

各桁位置は「2.2出力形式」をご参照ください。出力データセットはVB形式です。桁数固定で出力する場合、可変での出力よりファイルサイズが大きくなり、処理時間も長くなります。

2.1.3. その他の制御スイッチ

ERRORCDE

リターン・コード

解析対象のパフォーマンス・データがない場合、もしくはプロセジャが出力すべきデータがない場合、以下のメッセージを出力します。このときのリターン・コードを、ERRORCDEに任意の値を指定することで変更できます。
指定できる値は0～4095の範囲の整数で、省略値は8です。

・解析対象のパフォーマンス・データがない場合のメッセージ

```
NO PERFORMANCE DATA IS FOUND.
```

・プロセジャが出力すべきデータがない場合のメッセージ

```
THERE WAS NO OUTPUT DATA.
```

2.2　出力レコード形式

DSNCSV00が出力するデータセット・アクセス情報の一覧を示します。出力結果はユーザプログラムや表計算プログラムを使用して処理することが可能です。なお、一覧表の“桁位置”および最終行の項目“(非出力)”は、桁位置固定出力(FIXSW=1)を指定した場合に有効となります。

2.2.1.【タイプ 13 : ODAM クローズレコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号(固定「013.00」) ＊FIXSW=1 のとき	−	−	○
	2	−	数値	数値レコード番号(固定「13」) ＊FIXSW=0 のとき	−	−	○
2	4	8	文字	システム識別子	−	−	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	−	−	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	−	−	○
5	8	29	文字	ジョブ名または TSS ユーザ ID	−	−	○
6	6	38	文字	ボリューム通番	−	−	○
7	4	45	文字	装置アドレス	−	−	○
8	44	50	文字	データセット名	−	−	○
9	−	−	−	(非出力)	−	−	−
10	15	140	数値	EXCP 回数	−	−	○

2.2.2.【タイプ 14 : INPUT,RDBACK データセット活動】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号(固定「014.00」) ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号(固定「14」) ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名または TSS ユーザ ID	○	○	○
6	6	38	文字	ボリューム通番	○	○	○
7	4	45	文字	装置アドレス	○	○	○
8	44	50	文字	データセット名	○	○	○
9	−	−	−	(非出力)	−	−	−
10	15	140	数値	EXCP 回数	○	○	○
11-36	−	−	−	(非出力)	−	−	−
37	10	245	数値	トラック数	○	○	○
38	3	256	数値	エクステント数	○	○	○
39	8	260	文字	プログラム名	○	−	−
40-43	−	−	−	(非出力)	−	−	−
44	8	300	文字	ユーザーID	○	−	−
45-69	−	−	−	(非出力)	−	−	−
70	4	598	文字	暗号化タイプ 1(暗号化方式)	○	−	−
71	4	562	文字	暗号化タイプ 2(暗号鍵の種類)	○	−	−

2.2.3.【タイプ 15 : OUTPUT,UPDAT,INOUT,OUTIN データセット活動】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号(固定「015.00」) ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号(固定「15」) ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名または TSS ユーザ ID	○	○	○
6	6	38	文字	ボリューム通番	○	○	○
7	4	45	文字	装置アドレス	○	○	○
8	44	50	文字	データセット名	○	○	○
9	−	−	−	(非出力)	−	−	−
10	15	140	数値	EXCP 回数	○	○	○
11-36	−	−	−	(非出力)	−	−	−
37	10	245	数値	トラック数	○	○	○
38	3	256	数値	エクステント数	○	○	○
39	8	260	文字	プログラム名	○	−	−
40-43	−	−	−	(非出力)	−	−	−
44	8	300	文字	ユーザーID	○	−	−
45-69	−	−	−	(非出力)	−	−	−
70	4	598	文字	暗号化タイプ 1(暗号化方式)	○	−	−
71	4	562	文字	暗号化タイプ 2(暗号鍵の種類)	○	−	−

2.2.4. 【タイプ 17：スクラッチ・データセット状況】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「017.00」） ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号（固定「17」） ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名または TSO/TSS ユーザ ID	○	○	○
6	6	38	文字	ボリューム通番	○	○	○
7	−	−	−	（非出力）	−	−	−
8	44	50	文字	データセット名	○	○	○
9-43	−	−	−	（非出力）	−	−	−
44	8	300	文字	ユーザーID	○	−	−

該当データセットが複数のボリュームに跨っている場合、レコードをボリューム毎に複数出力します。

2.2.5. 【タイプ 18：非 VSAM データセットの名前変更状況】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「018.00」） ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号（固定「18」） ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名または TSO/TSS ユーザ ID	○	○	○
6	6	38	文字	ボリューム通番	○	○	○
7	−	−	−	（非出力）	−	−	−
8	44	50	文字	古いデータセット名	○	○	○
9	44	95	文字	新しいデータセット名	○	○	○
10-43	−	−	−	（非出力）	−	−	−
44	8	300	文字	ユーザーID	○	−	−

該当データセットが複数のボリュームに跨っている場合、レコードをボリューム毎に複数出力します。

2.2.6. 【タイプ 20：ジョブ開始】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「020.00」） ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号（固定「20」） ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名	○	○	○
6-39	−	−	−	（非出力）	−	−	−
40	8	269	文字	RACF グループ ID	○	○	−
41	8	278	文字	RACF ユーザ ID	○	○	−
42	8	287	文字	RACF 端末 ID	○	○	−

2.2.7. 【タイプ 30.1：ジョブ開始】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「030.01」） ＊FIXSW=1 のとき	○	○	−
	5(2.2)	−	数値	数値レコード番号（固定「30.01」） ＊FIXSW=0 のとき	○	○	−
2	4	8	文字	システム識別子	○	○	−
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	−
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	−
5	8	29	文字	ジョブ名または TSO/TSS ユーザ ID	○	○	−
6-39	−	−	−	（非出力）	○	○	−
40	8	269	文字	RACF グループ ID	○	○	−
41	8	278	文字	RACF ユーザ ID	○	○	−
42	8	287	文字	RACF 端末 ID	○	○	−
43	3	294	文字	ジョブクラス	○	○	−

2.2.8. 【タイプ 60：VSAM ボリューム・データセットの更新】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「060.00」） ＊FIXSW=1 のとき	○	○	－
	2	－	数値	数値レコード番号（固定「60」） ＊FIXSW=0 のとき	○	○	－
2	4	8	文字	システム識別子	○	○	－
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	－
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	－
5	8	29	文字	ジョブ名または TSO/TSS ユーザ ID	○	○	－
6-7	－	－	－	（非出力）	－	－	－
8	44	50	文字	データセット名	○	○	－
9-10	－	－	－	（非出力）	－	－	－
11	2	149	文字	更新内容 ・"UP" － 更新 ・"DE" － 削除 ・"IN" － 挿入	○	○	－
12-23	－	－	－	（非出力）	－	－	－
24	44	176	文字	VSAM ボリューム・データ・セット名（VVDS）	○	○	－
25	1	221	文字	項目タイプ ID(注)	○	○	－

2.2.9. 【タイプ 61：IBM：総合カタログ機能定義活動／富士通：BCS レコード追加】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「061.00」） ＊FIXSW=1 のとき	○	○	－
	2	－	数値	数値レコード番号（固定「61」） ＊FIXSW=0 のとき	○	○	－
2	4	8	文字	システム識別子	○	○	－
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	－
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	－
5	8	29	文字	ジョブ名	○	○	－
6-7	－	－	－	（非出力）	－	－	－
8	44	50	文字	データセット名	○	○	－
9-10	－	－	－	（非出力）	－	－	－
11	2	149	文字	更新内容 ・"UP" － 更新 ・"DE" － 削除 ・"IN" － 挿入	○	－	－
12-23	－	－	－	（非出力）	－	－	－
24	44	176	文字	VSAM ボリューム・データ・セット名（VVDS）	○	○	－
25	1	221	文字	項目タイプ ID(注)	○	○	－

（注）項目タイプIDについては、出力レコード形式の最後にある「項目タイプID」をご参照ください。

2.2.10. 【タイプ 62：VSAM コンポーネントまたはクラスタの OPEN】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「062.00」） ＊FIXSW=1 のとき	○	○	○
	2	－	数値	数値レコード番号（固定「62」） ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名	○	○	○
6	－	－	文字	データセットが存在するディスク装置のボリューム通番	○	○	○
7	－	－	－	（非出力）	－	－	－
8	44	50	文字	データセット名	○	○	○
9-11	－	－	－	（非出力）	－	－	－
項番 12～15：オープン状況（状況により'1'を設定）							
12	1	152	数値	コンポーネントまたはクラスターは、正常にオープンされた	○	○	○
13	1	154	数値	セキュリティー違反（＝不正なパスワード）	○	○	○
14	1	156	数値	レコードは、カタログまたはカタログ・リカバリー域(CRA) レコードである	○	－	－
				DD 文の DISP オペランドは SHR である	－	－	○
15	1	158	数値	レコードは、VSAM ボリュームデータセット(VVDS) またはデータセットとしてオープンあるいはクローズされている ICF カタログ用である	○	－	－
				ACB の MACRF オペランドに OUT を指定	－	－	○

2.2.11. 【タイプ 64：VSAM コンポーネントまたはクラスタの CLOSE】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「064.00」） ＊FIXSW=1 のとき	○	○	○
	2	−	数値	数値レコード番号（固定「64」） ＊FIXSW=0 のとき	○	○	○
2	4	8	文字	システム識別子	○	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	○
5	8	29	文字	ジョブ名	○	○	○
6	6	38	文字	データセットが存在するディスク装置のボリューム通番	○	○	○
7	4	45	文字	データセットが存在する装置のアドレス	○	○	○
8	44	50	文字	データセット名	○	○	○
9	−	−	−	（非出力）	−	−	−
10	44	140	数値	EXCP 回数	○	○	○
11−15	−	−	−	（非出力）	−	−	−
項番 16～22：状態標識(状態により'1' を設定)							
16	1	160	数値	コンポーネントがクローズされた	○	○	○
17	1	162	数値	ボリュームが切り替えられた	○	○	○
18	1	164	数値	使用可能なスペースがない	○	○	○
19	1	166	数値	レコードは、カタログまたはカタログ・リカバリー域(CRA) レコードである	○	−	−
20	1	168	数値	コンポーネントがクローズされた TYPE=T	○	−	−
21	1	170	数値	ABEND 処理時に書き込まれたレコード	○	−	−
22	1	172	数値	レコードは、VSAM ボリュームデータセット(VVDS) またはデータセットとして オープンあるいはクローズされている ICF カタログ用である	○	−	−
23−60	333	174ー 507	−	（非出力）	−	−	−
61	8	509	数値	レコードの削除によって減少したレコード数	○	○	○
62	8	518	数値	レコードの挿入によって増加したレコード数	○	○	○
63	8	527	数値	更新されたレコード数	○	○	○
64	8	536	数値	取り出されたレコード数	○	○	○

2.2.12. 【タイプ 65：IBM：総合カタログ機能の削除活動／富士通：BCS レコード削除】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「065.00」） ＊FIXSW=1 のとき	○	○	−
	2	−	数値	数値レコード番号（固定「65」） ＊FIXSW=0 のとき	○	○	−
2	4	8	文字	システム識別子	○	○	−
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	−
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	−
5	8	29	文字	ジョブ名	○	○	−
6−7	−	−	−	（非出力）	−	−	−
8	44	50	文字	項目名／エントリ名	○	○	−
9−10	−	−	−	（非出力）	−	−	−
11	2	149	文字	更新内容 ・"UP" − 更新 ・"DE" − 削除 ・"IN" − 挿入	○	−	−
12−22	−	−	−	（非出力）	−	−	−
23	1	174		処理コード ・"S" − スクラッチ ・"U" − アンカタログ	○	−	−
24	44	176	文字	カタログ名／BCS 名	○	○	−
25	1	221	文字	項目タイプ ID(注)	○	○	−

2.2.13. 【タイプ 66：IBM：総合カタログ機能の更新活動／富士通：BCS レコード更新】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「066.00」） ＊FIXSW=1 のとき	○	○	－
	2	－	数値	数値レコード番号（固定「66」） ＊FIXSW=0 のとき	○	○	－
2	4	8	文字	システム識別子	○	○	－
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	○	－
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	○	－
5	8	29	文字	ジョブ名	○	○	－
6-7	－	－	－	（非出力）	－	－	－
8	44	50	文字	項目名／エントリ名	○	○	－
9	44	95	文字	新項目名	○	○	－
10	－	－	－	（非出力）	－	－	－
11	2	149	文字	更新内容 ・"UP" － 更新 ・"DE" － 削除 ・"IN" － 挿入	○	－	－
12-22	－	－	－	（非出力）	－	－	－
23	1	174		処理コード ・"R" － カタログ項目がリネーム ・" " － その他	○	○	－
24	44	176	文字	カタログ名／BCS 名	○	○	－
25	1	221	文字	項目タイプ ID(注)	○	○	－

（注）項目タイプIDについては、出力レコード形式の最後にある「項目タイプID」をご参照ください。

2.2.14. 【タイプ 67：VSAM スクラッチレコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「067.00」） ＊FIXSW=1 のとき	－	○	○
	2	－	数値	数値レコード番号（固定「67」） ＊FIXSW=0 のとき	－	○	○
2	4	8	文字	システム識別子	－	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	－	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	－	○	○
5	8	29	文字	ジョブ名	－	○	○
6-7	－	－	－	（非出力）	－	－	－
8	44	50	文字	カタログレコード名（データセット名）	－	○	○
9-23	－	－	－	（非出力）	－	－	－
24	44	176	文字	VSAM カタログ名／クラスタ名	－	○	○
25	－	－	－	（非出力）	－	－	－
項番 26～29：DELETE 状態標識（'1' を設定）							
26	1	223	数値	データセットは VSAM カタログから削除された	－	○	○
27	1	225	数値	データセットのスペースは割り当て解除された（VSAM データセット以外）	－	○	○
28	1	227	数値	パスが削除された	－	○	○
29	1	229	数値	代替インデックスが削除された	－	○	○
項番 30～36：カタログレコードの形式（'1' を設定）							
30	1	231	数値	VSAM クラスタ	－	○	○
31	1	233	数値	VSAM データコンポーネント	－	○	○
32	1	235	数値	VSAM インデックスコンポーネント	－	○	○
33	1	237	数値	VSAM カタログ	－	○	○
34	1	239	数値	非 VSAM データセット	－	○	○
35	1	241	数値	世代データ群	－	○	○
36	1	243	数値	別名	－	○	○

2.2.15. 【タイプ 68：VSAM リネームレコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「068.00」） ＊FIXSW=1 のとき	－	○	○
	2	－	数値	数値レコード番号（固定「68」） ＊FIXSW=0 のとき	－	○	○
2	4	8	文字	システム識別子	－	○	○
3	8	13	YYYYMMDD	日付[レコード出力日付]	－	○	○
4	6	22	HHMMSS	時刻[レコード出力時刻]	－	○	○
5	8	29	文字	ジョブ名	－	○	○
6-7	－	－	－	（非出力）	－	－	－
8	44	50	文字	旧項目名	－	○	○
9	44	95	文字	新項目名	－	○	○
10-23	－	－	－	（非出力）	－	－	－
24	44	149	文字	VSAM カタログ名／クラスタ名	－	○	○

2.2.16. 【タイプ 97：TSS 情報レコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	数値レコード番号（固定「097.00」） ＊FIXSW=1 のとき	−	○	−
	5(2.2)	−	数値	数値レコード番号（固定「97」） ＊FIXSW=0 のとき xx = 01：FEXPORT xx = 02：FIMPORT	−	○	−
2	4	8	文字	システム識別子	−	○	−
3	8	13	YYYYMMDD	日付[レコード出力日付]	−	○	−
4	6	22	HHMMSS	時刻[レコード出力時刻]	−	○	−
5-7	−	−	−	（非出力）	−	−	−
8	44	50	文字	データセット名	−	○	−
9-43	−	−	−	（非出力）	−	−	−
44	8	300	文字	ユーザ ID	−	○	−
45	8	309	文字	端末識別名	−	○	−
46	8	318	文字	メンバ名	−	○	−
47	8	327	数値	レコード長（バイト）	−	○	−
48	−	−	−	（非出力）	−	−	−
49	8	345	数値	転送レコード数	−	○	−
50	12	354	数値	転送サイズ（バイト）	−	○	−
51	4	367	文字	レコード形式	−	○	−
52	4	372	文字	文字実行結果	−	○	−
53	8	377	YYYYMMDD	転送開始日付	−	○	−
54	6	386	HHMMSS	転送開始時刻	−	○	−
55	8	393	YYYYMMDD	転送終了日付	−	○	−
56	6	402	HHMMSS	転送終了時刻	−	○	−

2.2.17. 【タイプ 101：TISP/BP 課金情報レコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	レコード番号（固定「101.xx」） xx = 01：FTP クライアント	−	○	−
2	4	8	文字	システム識別子	−	○	−
3	8	13	YYYYMMDD	日付[レコード出力日付]	−	○	−
4	6	22	HHMMSS	時刻[レコード出力時刻]	−	○	−
5-7	−	−	−	（非出力）	−	−	−
8	44	50	文字	データセット名	−	○	−
9-43	−	−	−	（非出力）	−	−	−
44	8	300	文字	ユーザ ID	−	○	−
45	8	309	文字	端末識別名	−	○	−
46	8	318	文字	メンバ名	−	○	−
47	8	327	数値	レコード長（バイト）	−	○	−
48	8	336	数値	ブロック長（バイト）	−	○	−
49	−	−	−	（非出力）	−	−	−
50	12	354	数値	転送サイズ（バイト）	−	○	−
51	4	367	文字	レコード形式	−	○	−
52-53	−	−	−	（非出力）	−	−	−
54	6	386	HHMMSS	転送開始時刻	−	○	−
55	−	−	−	（非出力）	−	−	−
56	6	402	HHMMSS	転送終了時刻	−	○	−
57	64	409	文字	相手ホストシステム名	−	○	−
58	16	474	文字	相手ホストシステムでのユーザ ID	−	○	−
59	8	491	数値	送信マクロ発行回数	−	○	−
60	8	500	数値	受信マクロ発行回数	−	○	−

2.2.18. 【タイプ 118 : TCP/IP 統計レコード】

項番	バイト	桁位置	形式	内容	IBM	富士通	日立
1	6(3.2)	1	数値	レコード番号（固定「118.xx」） xx = 74: FTP サーバの取り出し	○	−	−
2	4	8	文字	システム識別子	○	−	−
3	8	13	YYYYMMDD	日付[レコード出力日付]	○	−	−
4	6	22	HHMMSS	時刻[レコード出力時刻]	○	−	−
5-7	−	−	−	（非出力）	−	−	−
8	44	50	文字	データセット名	○	−	−
9-43	−	−	−	（非出力）	−	−	−
44	8	300	文字	ユーザ ID	○	−	−
45	−	−	−	（非出力）	−	−	−
46	8	318	文字	メンバ名	○	−	−
47-49	−	−	−	（非出力）	−	−	−
50	12	354	数値	転送サイズ（バイト）	○	−	−
51	4	367	文字	レコード形式 ・"P" − PDS ・"S" − 順次 ・"H" − HFS	○	−	−
52	4	372	文字	実行結果	○	−	−
53	−	−	−	（非出力）	−	−	−
54	6	386	HHMMSS	転送開始時刻	○	−	−
55	−	−	−	（非出力）	−	−	−
56	6	402	HHMMSS	転送終了時刻	○	−	−
57-64	−	−	−	（非出力）	−	−	−
65	15	545	文字	ローカル IP アドレス	○	−	−
66	5	561	数値	ローカルポート番号	○	−	−
67	15	567	文字	リモート IP アドレス	○	−	−
68	5	583	数値	リモートポート番号	○	−	−
69	8	589	文字	TCP/IP ホスト名	○	−	−

※項目タイプID

【IBMタイプ60,61,65,66】

A	非 VSAM データ・セット
B	世代別データ・グループ(GDG)ベース
C	クラスター
D	データ・セット
E	VSAM 拡張レコード
F	フリー・スペース
G	代替索引
H	GDG ベースのアクティブな世代別データ・セット(GDS 項目)
I	索引
J	CDG 拡張レコード
K	VSAM ボリューム・レコード(VVR)
L	世代別データ・グループ(GDG)ベース
M	マスター・カタログ
N	非 VSAM レコード・ヘッダー
O	オブジェクト・アクセス方式(OAM)非 VSAM レコード
P	ページ・スペース
Q	VVR ヘッダー(2 次)
R	パス
T	真の名前レコード
U	ユーザ・カタログ
V	ボリューム
W	ライブラリー制御システム・ボリューム
X	別名レコード
Y	アップグレード
Z	VVR ヘッダー(1 次)
0	正常な非 VSAM レコード(X'00')
1	JES3 レコード(X'01')

【富士通 タイプ60】

D	データ部
I	インデックス部

【富士通タイプ 61,65,66】

A	非 VSAM データ・セット
B	世代別データ・グループ(GDG)ベース
C	クラスター
G	AIX
R	パス
U	ユーザ・カタログ
X	別名レコード

【ラベル一覧】

CSVファイルの先頭行に出力されるラベル名は以下の通りです。

項番	項目	長さ	桁位置	形式	ラベル 1 (FIXSW=0)	ラベル 2 (FIXSW=1)
1	レコード番号	6	1	F(3.2)	RECNUM	RECNUM
2	システム識別子	4	8	C	SYSID	SYS
3	日付	8	13	YYYYMMDD	DATE	YYYYMMDD
4	時刻	6	22	HHMMSS	TIME	HHMMSS
5	ジョブ名	8	29	C	JOBNAME	JOBNAME
6	ボリューム	6	38	C	VOLSER	VOLSER
7	装置アドレス	4	45	C	DEVADR	ADDR
8	データセット名	44	50	C	DSN1	DATASET1
9	データセット名 2	44	95	C	DSN2	DATASET2
10	EXCP 回数	8	140	I	EXCP	EXCP
11	更新内容	2	149	C	VVR INDICATES	VV
12	オープン状況	1	152	I	OPEN	O
13		1	154	I	SECURITY VIOLATION	S
14		1	156	I	CATALOG OR CRARE CORD	C
					DD DISP=SHR	D
15		1	158	I	VVDS OR ICF CATALOG	V
					ACB MACRF=OUT	A
16	状態標識	1	160	I	CLOSE	C
17		1	162	I	VOL SWITCHED	V
18		1	164	I	NO SPACE	N
19		1	166	I	CATALOG OR CRARE CORD	C
20		1	168	I	CLOSE TYPE=T	C
21		1	170	I	ABEND	A
22		1	172	I	VVDS OR ICF CATALOG	V
23	処理コード	1	174	C	FUNCTION CODE	F
24	VVDS/カタログ	44	176	C	CATALOG/VVDS	CATALOG/VVDS
25	項目タイプ ID	1	221	C	ENTRY TYPE ID	E
26	DELETE インジケータ	1	223	I	UNCATALOGED	U
27		1	225	I	SCRATCHED	S
28		1	227	I	PATH DELETED	P
29		1	229	I	ALTERNATE INDEX DELETED	D
30	状態標識	1	231	I	VSAM CLUSTER	C
31		1	233	I	VSAM DATA COMPONENT	D
32		1	235	I	VSAM INDEX COMPONENT	I
33		1	237	I	VSAM CATALOG	C
34		1	239	I	NON-VSAM DATA SET	N
35		1	241	I	GENERATION DATA GROUP	G
36		1	243	I	ALIAS	A
37	トラック数	10	245	I	TRACK	TRACK
38	エクステント数	3	256	I	EXTENT	EXT
39	プログラム名	8	260	C	PGM NAME	PGMNAME
40	RACF グループ ID	8	269	C	RACFGRP	RACFGRP
41	RACF ユーザ ID	8	278	C	RACFUSER	RACFUSER
42	RACF 端末 ID	8	287	C	RACFTERM	RACFTERM
43	ジョブクラス	3	296	C	JOBCLASS	CLS
44	ユーザ ID	8	300	C	USERID	USERID
45	端末識別名	8	309	C	TERMINAL	TERMINAL
46	メンバ名	8	318	C	MEMBER	MEMBER
47	レコード長	8	327	I	REC LEN	RECLEN
48	ブロック長	8	336	I	BLKSIZE	BLKSIZE
49	転送レコード数	8	345	I	XFERCNT	XFERCNT
50	転送サイズ(BYTE)	12	354	I	IBM:TRANS_BYTE FUJ:XFERSIZE	IBM:TRANS_BYTE FUJ:XFERSIZE
51	レコード形式	4	367	C	IBM:DS_TYPE FUJ:RECFM	IBM:DSTP FUJ:RCFM
52	実行結果	4	372	C	CC	CC
53	転送開始日付	8	377	YYYYMMDD	INITDATE	INITDATE
54	転送開始時刻	6	386	HHMMSS	INITTIME	INITTM
55	転送終了日付	8	393	YYYYMMDD	TERMDATE	TERMDATE
56	転送終了時刻	6	402	HHMMSS	TERMTIME	TERMTM
57	相手ホストシステム名	64	409	C	HOSTNAME	HOSTNAME
58	相手ホストシステムでのユーザ ID	16	474	C	REMOTE ID	REMOTEID
59	送信マクロ発行回数	8	491	I	SEND	SEND
60	受信マクロ発行回数	8	500	I	RECEIVE	RECEIVE

(続く)

項番	項目	長さ	桁位置	形式	ラベル 1 (FIXSW=0)	ラベル 2 (FIXSW=1)
61	レコードの削除によって減少したレコード数	8	509	I	REC_DELETE	REC_DELT
62	レコードの挿入によって増加したレコード数	8	518	I	REC_INSERT	REC_INST
63	更新されたレコード数	8	527	I	REC_UPDATE	REC_UPDT
64	入力されたレコード数	8	536	I	REC_RETRIEVE	REC_RETR
65	ローカル IP アドレス	15	545	C	LOCAL_IP	LOCAL_IP
66	ローカルポート番号	5	561	I	LOCAL_PORT	L_POT
67	リモート IP アドレス	15	567	C	REMOTE_IP	REMOTE_IP
68	リモートポート番号	5	583	I	REMOTE_PORT	R_POT
69	TCP/IP ホスト名	8	589	C	TCP_HOSTNAME	TCP_HOST

第3章 AUDITMON の使用方法

AUDITMONプロセジャは、セキュリティツールのログ情報を基に月次のレポートを作成・出力します。

また、このプロセジャを実行するにはMF-AUDITとMF-MAGIC、あるいはMF-SCOPEとMF-MAGICの契約が必要となります。

このプロセジャでは、下記に示すセキュリティツールのログ情報を処理対象としています。

IBM	:	RACF	SMF タイプ80
富士通	:	RACF	SMF タイプ80
日　立	:	TRUST E2	SMS タイプ118

各システムでは、セキュリティツールのログ情報やジョブ情報を基にしたレポート機能を提供しています。これらは、SMF/SMSデータセットに書き出されたログ情報を変換したレコードを入力として各種レポートを作成・出力します。
このAUDITMONプロセジャでは、SMF/SMSデータセットに書き出されたログ情報を入力としていますので注意してください。メーカツールにより変換されたデータは入力できません。

注意
このプロセジャでは、セキュリティツールのログ情報の量によっては大量のプロセッサ資源を使用することがあります。

3.1 実行パラメータ

AUDITMONプロセジャ用サンプルジョブ制御文のDD文“PLATFORM”では、プロセジャの実行パラメータ指定部とプロセジャ本体が連結データセットとして定義されています。実行パラメータでは、入力データの選択や出力レポート群の選択を行います。この実行パラメータには、セレクション・スイッチとコントロール・スイッチがあります。

富士通または日立システムの場合、DD文“CARDIN”をコメントアウトしてください。

```
//AUDITMON JOB (ACCT),MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,NOTIFY=USERID
//JOBLIB  DD DSN=CPE.LOAD,DISP=SHR
//*JOBCAT  DD DSN=USER.CAT,DISP=SHR
//*********************************************************************
//* プロダクト名 : MF-SCOPE / AUDIT プロセジャ名 : AUDITMON           *
//*-------------------------------------------------------------------*
//* JCLの以下のデータセット名を変更してください。                     *
//*  ES/1 NEO LIBRARY                                                 *
//*          - CPE.LOAD      ( ロードモジュールライブラリ )           *
//*          - CPE.PARM      ( ソースライブラリ          )           *
//*  INPUT   - INPUT.DATA    ( 解析対象のSMF(SMS)データ  )           *
//*************************************************** SINCE V5L02 ***
//SHELL   EXEC PGM=CPESHELL,REGION=4096K,TIME=1440
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//CARDIN   DD  DSN=CPE.PARM(@IBMRACF),DISP=SHR
//SYSUT1   DD  UNIT=SYSDA,SPACE=(TRK,(10,10))
//INPUT    DD  DISP=SHR,DSN=INPUT.DATA
//PLATFORM DD  *
*
* セレクション・スイッチ  ／  コントロール・スイッチ
*
         DATESW   = 0                    日付制御      ( 0:YYDDD 1:YYMMDD )
         SEL1     = 00000                解析開始日    ( YYDDD/YYMMDD )
         SEL2     = 0000                 解析開始時刻  ( HHMM )
         SEL3     = 99999                解析終了日    ( YYDDD/YYMMDD )
         SEL4     = 2400                 解析終了時刻  ( HHMM )
         OSTYPE   = 1                    オペレーティングシステムの種別 (1:IBM 2:FUJI 3:HITC)
*
         SW10     = 1                    処理レコード・サマリー・レポート
         SW20     = 1                    日毎のサマリー・レポート
         SW30     = 1                    ジョブグループ毎のサマリー・レポート
         SW40     = 1                    グループ毎のサマリー・レポート
         SW50     = 1                    ユーザ毎の不正アクセス・サマリー・レポート
* FOR SW20
         TIMEBASE = 00                   １日の開始時刻（ＨＨ）
* FOR SW30                               ジョブグループの定義
         DIM JOBGRP(100)                   配列の定義
         JOBGRP   = 3                      ジョブグループの数
         JOBGRP(1)= 'ABC*'                 ジョブ名によるジョブグループ１
         JOBGRP(2)= 'DEF*'                 ジョブ名によるジョブグループ２
         JOBGRP(3)= 'XYZ*'                 ジョブ名によるジョブグループ３
* FOR SW50
         SELNMCHK = 1                    ユーザ名をキーとする（ＩＢＭのみ）
* FOR SW50 - SELECT / EXCLUDE            事象コードによる選択・除外
         DIM SEVT(100),EEVT(100)           配列の定義
         SEVT     = 0                      選択する数
         SEVT(1)  = '0101'                 事象コードの選択１
         SEVT(2)  = '0102'                 事象コードの選択２
         EEVT     = 0                      除外する数
         EEVT(1)  = '0101'                 事象コードの除外１
         EEVT(2)  = '0102'                 事象コードの除外２
* FOR SW50 - SELECT / EXCLUDE            事象修飾子による選択・除外
         DIM SEVQ(100),EEVQ(100)           配列の定義
         SEVQ     = 0                      選択する数
         SEVQ(1)  = 'INSAUTH'              事象修飾子の選択１
         SEVQ(2)  = 'WARNING'              事象修飾子の選択２
         EEVQ     = 0                      除外する数
         EEVQ(1)  = 'INSAUTH'              事象修飾子の除外１
         EEVQ(2)  = 'WARNING'              事象修飾子の除外２
* FOR SW50 - THRESHOLD                   事象コードによる閾値設定
         DIM EVTNUM(100),EVTMAX(100)       配列の定義
         EVTNUM   = 0                      閾値を設定する事象コードの数
         EVTNUM(1)= '0101'                 事象コード１
         EVTMAX(1)= 2                      事象コード１の閾値
         EVTNUM(2)= '0102'                 事象コード２
         EVTMAX(2)= 1                      事象コード２の閾値
* FOR SW50 - THRESHOLD                   事象修飾子による閾値設定
         DIM EVQUAL(100),EVQMAX(100)       配列の定義
         EVQUAL   = 0                      閾値を設定する事象修飾子の数
         EVQUAL(1)= 'INSAUTH'              事象修飾子１
         EVQMAX(1)= 0                      事象修飾子１の閾値
         EVQUAL(2)= 'WARNING'              事象修飾子２
         EVQMAX(2)= 0                      事象修飾子２の閾値
```

```
* OTHER
        SYSID    = ' '                          システム識別コード
        ERRORCDE = 8                            エラー完了コード
        NOLIST
//        DD  DSN=CPE.PARM(AUDITMON),DISP=SHR
```

Jcl 3.1　サンプル・ジョブ制御文（JCLADTMO）

3.1.1. セレクション・スイッチ

セレクション・スイッチでは、解析対象とするべき時間帯を指定します。

DATESW

日付形式

SEL1(開始日)とSEL3(終了日)で解析対象日を指定する際、DATESWを“1”に設定すると、SEL1とSEL3の日付けをYYMMDD(グレゴリアン暦)で指定することができます。

SEL1～SEL4

入力データ・レンジ

解析対象とするべきSMF/SMSレコードの日時の範囲を指定します。

SEL1	開始日	(形式はYYMMDD)
SEL2	開始時刻	(形式はHHMM)
SEL3	終了日	(形式はYYMMDD)
SEL4	終了時刻	(形式はHHMM)

入力されたSMF/SMS レコード群の中から指定された時間帯に書き出されたレコードのみを抽出します。次のような指定の場合には、入力された先頭レコードの日時から1ヶ月分が対象になります。

```
DATESW  =0
SEL1    =00000
SEL2    =0000
SEL3    =99999
SEL4    =2400
```

2000年以降の指定について
SEL1とSEL3で指定する日付は1900年代であっても2000年代であっても、下位2桁のみをYY部で指定します。この為、YY部が00～49の場合には2000～2049年、YY部が50～99の場合には1950～1999年の指定として評価を行います。開始時刻(SEL2)と終了時刻(SEL4)のみの指定はできません。時間指定をする場合は必ず日付を指定してください。

TIMEBASE

日の開始時刻

1日の開始時刻をTIMEBASEで指定します。省略値は次のようになっています。

```
TIMEBASE=00
```

このスイッチで指定された値は日毎のレポートを作成・出力する際に利用されます。

OSTYPE

オペレーティング・システム識別

入力されるSMF/SMSレコード群が収集されたオペレーティング・システムの識別を指定してください。

OSTYPE=1: IBM システムの SMF レコード群
OSTYPE=2: 富士通システムの SMF レコード群
OSTYPE=3: 日立システムの SMS レコード群

3.1.2. コントロール・スイッチ

コントロール・スイッチでは、評価結果として出力する各種レポートの選択や入力データ群の選択などを指定します。

SW10

処理レコード・サマリー・レポート

入力されたセキュリティツールのログ情報の中で処理対象となったデータをサマリーしたレポートが作成されます。SW10が“1”に設定されていれば、このレポートが出力されます。

SW20

日毎のサマリー・レポート

セキュリティツール・ログに記録されている事象の発生回数を日毎にサマリーしたレポートが作成されます。SW20が“1”に設定されていれば、このレポートが出力されます。

SW30
JOBGRP

ジョブグループ毎のサマリー・レポート

このレポートはJOBGRPスイッチで指定された分類方法に従ってグループを決定します。そのグループ毎にセキュリティツールのログ情報をサマリーしたレポートが作成されます。SW30が “1”でJOBGRPが設定されていれば、このレポートが出力されます。ジョブ名による分類方法を定義する際には、定義を簡略化させる為に比較制御文字を利用した指定が可能です。(注)

(注)
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

```
DIM JOBGRP(m)          配列の定義
JOBGRP=3               グループ数を定義
JOBGRP(1)=’ABC ＊’     グループ 1 のジョブ名定義
JOBGRP(2)=’DEF ＊’     グループ 2 のジョブ名定義
JOBGRP(3)=’XYZ ＊’     グループ 3 のジョブ名定義
```

SW40

グループ毎のサマリー・レポート

セキュリティツールではユーザをグループ化することができます。このレポートでは、セキュリティツールで定義されているグループ毎に事象の発生回数をサマリーしたレポートが作成されます。SW40が“1”に設定されていれば、このレポートが出力されます。

SW50
SELNMCHK

ユーザ毎の不正アクセス・サマリー・レポート

セキュリティツールのログ情報には、正常なアクセス情報や不正アクセス情報が混在しています。このレポートでは、不正アクセスをユーザ単位にサマリーしたレポートが作成されます。 SW50が“1”に設定されていれば、このレポートが出力されます。IBMシステムの場合、ユーザを特定するときにユーザ名を含めることもできます。これは、SELNMCHKスイッチで指定します。

```
SELNMCHK=0      ： ユーザ名はキーとしない
SELNMCHK=1      ： ユーザ名はキーとする(省略値)
```

また、報告する事象の選択、除外や閾値の設定をすることもできます。これらの指定方法については、下記の「事象の選択・除外」と「閾値の設定」を参照してください。

SEVT, EEVT
SEVQ, EEVQ

事象の選択・除外

不正アクセス・サマリー・レポート(SW50)を作成・出力する際に、対象とする事象を選択・除外する時に定義します。事象の選択・除外の定義方法には事象コードと事象修飾子の2種類が用意されています。事象修飾子はIBMシステムのみが有効です。

【事象コードによる選択・除外】

```
DIM SEVT (100),EEVT(100)
SEVT            = 1
SEVT (1)        = '0101'

EEVT            = 1
EEVT (1)        = '0102'
```

【事象修飾子による選択・除外】

```
DIM SEVQ (100) , EEVQ(100)
SEVQ            = 1
SEVQ (1)        = 'INSAUTH'

EEVQ            = 1
EEVQ (1)        = 'WARNING'
```

選択・除外機能は、最初に選択機能、その後で除外機能の順番で処理します。

	(一致)	(不一致)
①選択機能	出力対象	対象外
②除外機能	対象外	事象の結果に従う

この為、選択と除外で同一事象を指定した際には対象外となります。また、選択された事象が正常の場合でもレポート対象となります。

EVTNUM
EVTMAX
EVQUAL
EVQMAX

閾値の設定

不正アクセス・サマリー・レポート(SW50)を作成・出力する際に、対象とする事象に閾値を設定する時に定義します。この閾値は、1つの事象で同一ユーザが発生させた回数に対する限界値になり、その閾値を超えた(≧閾値)ユーザの情報のみがレポートされます。事象修飾子はIBMシステムのみが有効です。

【事象コードによる閾値定義】

```
DIM EVTNUM(100),EVTMAX(100)
EVTNUM          = 1
EVTNUM (1)      = '0101'
EVTMAX (1)      = 2
```

【事象修飾子による閾値定義】IBMシステムのみ

```
DIM EVQUAL (100), EVQMAX (100)
EVQUAL          = 1
EVQUAL (1)      = 'INSAUTH'
EVQMAX (1)      = 3
```

SYSID　　システム識別コード

入力として指定されたデータセットの中に、複数システムの稼働実績データが記録されている場合があります。このような場合、どのシステムの評価を行うべきかを指定する必要があります。SYSIDに評価対象とするべきシステムのシステム識別コードを指定してください。SYSIDがブランク(‘ ’)の場合、最初に読み込んだ稼働実績データのシステムが対象となります。

3.1.3. その他のプログラム・スイッチ

前述のセレクション・スイッチおよびコントロール・スイッチ以外に、サンプル・ジョブ制御文では次のスイッチを使用することができます。このスイッチは、プロダクト・テープで提供されるサンプル・ジョブ制御文には定義されておりません。

ERRORCDE

リターン・コード

解析対象のパフォーマンス・データがない場合、もしくはプロセジャが出力すべきデータがない場合、以下のメッセージを出力します。このときのリターン・コードを、ERRORCDEに任意の値を指定することで変更できます。
指定できる値は0～4095の範囲の整数で、省略値は8です。

・解析対象のパフォーマンス・データがない場合のメッセージ

```
NO PERFORMANCE DATA IS FOUND.
```

・プロセジャが出力すべきデータがない場合のメッセージ

```
THERE WAS NO OUTPUT DATA.
```

¥PROCNM

プロセジャ名

各レポートのヘッダー部にはプロセジャ名が表示されるようになっています。このプロセジャ名を表示したくない場合、「¥PROCNM=_NULL_」を指定することにより表示が「PAGE」に変わります。

◆省略値(指定なし)

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                AUDITMON     9
PSW=SW10                                ---- RACF PROCESS RECORDS REPORT ----                                 VER=09 LVL=99
```

◆指定あり(¥PROCNM=_NULL_)

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                PAGE         9
PSW=SW10                                ---- RACF PROCESS RECORDS REPORT ----                                 VER=09 LVL=99
```

APARTD49 (注)

(注)
IBM システム
専用です。

区切り文字(1文字)

IBMシステムでユーザ名に空白や記号の桁を含む際には、特殊処理が必要になります。省略値で実行した際に正しくユーザ名が出力されない場合にユーザ名の区切り文字を設定します。なお、設定する文字(1文字)は、ユーザ名に使用されていない文字を設定してください。省略値はAPARTD49='?'です。

3.2　処理レコード・サマリー・レポート（SW10）

処理レコード・サマリー・レポートでは処理対象時間帯のセキュリティツール・ログ情報を事象毎に分類して出力します。これにより、ログ情報に記録されているデータの概要を知ることができます。

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON     6
PSW=SW10                                  ---- RACF PROCESS RECORDS REPORT ----                                  VER=09 LVL=99

CODE COUNT      EVENT CODE MEANING   EVENT CODE QUALIFIER MEANING                          DESCRIPTION
0101       203 JOBINIT/LOGON/LOGOFF INVALID PASSWORD                                  THE EVENT IS A VIOLATION
0106        24 JOBINIT/LOGON/LOGOFF REVOKED USERID ATTEMPTING ACCESS                  THE EVENT IS A VIOLATION
0200     14236 RESOURCE ACCESS      SUCCESSFUL ACCESS                                 SUCCESSFUL
0201        48 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                            THE EVENT IS A VIOLATION
0201         3 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                            VIOLATION AND UNDEFINED USER
1300         1 RACF COMMAND         ALTUSER  : NO VIOLATIONS DETECTED                 SUCCESSFUL
1800        15 RACF COMMAND         PASSWORD : NO VIOLATIONS DETECTED                 SUCCESSFUL
*TTL     14530


    ( TIMEBASE = 00 )
SYSTEM = IIMA (OS:MVS ,RACF :9999) START = 08/02/28 THU 2323 END = 08/03/09 SUN 1051     REPORTING DATE = 09/03/19 THU 1328
```

Rpt 3.2　処理レコード・サマリー・レポートの例

この処理レコード・サマリー・レポートの内容は次のようになっています。

CODE　　XXYY の 4 桁
　XX：事象コード
　YY：事象コード修飾子
　日立システムの TRUST の場合、事象コードと事象コード修飾子は次を意味します。
　　事象コード　　コマンドコード（16 進表示）
　　事象コード修飾子　　エラー情報（16 進表示）
　なお、擬似コマンド（JOB、LOGON、VERIFY）については、ユーザ検証時の事象と重複しますが分類して報告します。
COUNT　　件数
EVENT CODE MEANING
　事象コードの説明
EVENT CODE QUALIFIER MEANING
　事象コード修飾子の説明
DESCRIPTION　　結果
'VIOLATION AND UNDEFINED USER'
　システムに未定義のユーザが不正アクセスを行った。
'THE EVENT IS A VIOLATION'
　不正なアクセスを行った。
'USER IS NOT DEFINED TO RACF'
　システムに未定義のユーザがアクセスした。
'THE EVENT IS A WARNING'
　警告
'SUCCESSFUL'
　正常に処理された。

事象コードや事象コード修飾子の詳細な説明については、下記のメーカ提供のマニュアルを参照してください。
IBMシステム　：資源アクセス管理機能　監査担当者の手引き
　Resource Access Control Facility　Auditor's Guide
富士通システム　：OSIV/MSP RACFユーティリティ使用手引書
日立 システム　：TRUST E2　セキュリティ監視の手引き

3.3　日毎のサマリー・レポート（SW20）

セキュリティツール・ログに記録されている事象の発生回数を日毎にサマリーしたレポートを示します。これにより、日毎の不正アクセスの種類や件数を把握できます。事象が多く1ページに入らない場合は複数ページで出力されます。

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON     7
PSW=SW20                                    ---- RACF MONTHLY SUMMARY REPORT BY DAY ----                        VER=09 LVL=99

                0101   0106   0200   0201   0201   1300   1800                    *------- TOTAL COUNT -------*
YY/MM/DD(WEK) VIOL   VIOL   SUCC   VIOL   V+NU   SUCC   SUCC                    SUCCESS VIOLATE WARNING NOUSER
08/03/01(SAT)     23 ......   2130      1 ...... ......      1                       2131      24       0      0
08/03/02(SUN)     23      2   1328 ......      2 ......      2                       1330      27       0      2
08/03/03(MON)      2 ......    623 ...... ...... ...... ......                        623       2       0      0
08/03/04(TUE)      3 ......     70 ...... ...... ...... ......                         70       3       0      0
08/03/05(WED)     21 ......   1559      1 ...... ......      1                       1560      22       0      0
08/03/06(THU)     20      3   1544     16 ...... ......      3                       1547      39       0      0
08/03/07(FRI)     31      2   2928     13 ...... ...... ......                        2928      46       0      0
08/03/08(SAT)     52     12   2078     15      1 ......      4                       2082      80       0      1
08/03/09(SUN)      2 ......    240      1 ...... ......      1                        241       3       0      0
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
../../.. (...)
08/02/28(THU) ...... ......      3 ...... ...... ...... ......                          3       0       0      0
08/02/29(FRI)     26      5   1733      1 ......      1      3                       1737      32       0      0
../../.. (...)
../../.. (...)
_TOTAL_                                                                            14252     278       0      3

CODE COUNT      EVENT CODE MEANING   EVENT CODE QUALIFIER MEANING                  DESCRIPTION
0101       203 JOBINIT/LOGON/LOGOFF INVALID PASSWORD                              THE EVENT IS A VIOLATION
0106        24 JOBINIT/LOGON/LOGOFF REVOKED USERID ATTEMPTING ACCESS              THE EVENT IS A VIOLATION
0200     14236 RESOURCE ACCESS      SUCCESSFUL ACCESS                             SUCCESSFUL
0201        48 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                        THE EVENT IS A VIOLATION
0201         3 RESOURCE ACCESS      INSUFFICIENT AUTHORITY                        VIOLATION AND UNDEFINED USER
1300         1 RACF COMMAND         ALTUSER  : NO VIOLATIONS DETECTED             SUCCESSFUL
1800        15 RACF COMMAND         PASSWORD : NO VIOLATIONS DETECTED             SUCCESSFUL
*TTL     14530



   ( TIMEBASE = 00 )
SYSTEM = IIMA (OS:MVS ,RACF :9999) START = 08/02/28 THU 2323 END = 08/03/09 SUN 1051     REPORTING DATE = 09/03/19 THU 1328
```

Rpt 3.3　日毎のサマリー・レポートの例

この日毎のサマリー・レポートの内容は次のようになっています。

(1) 日毎の発生状況

YY/MM/DD(WEK)　日付（曜日）データが入力された日付は表示
XXYY　事象コードとその状態は 2 行で示されます。
STAT　状態は下記があります。
- SUCC ： 正常
- VOIL ： 不正
- NUSR ： 正常で未定義ユーザ
- V+NU ： 不正で未定義ユーザ
- WARN ： 警告
- W+NU ： 警告で未定義ユーザ

日立システムの場合、XXYY:Cと表示されることがあります。
これは、TRUSTコマンド(擬似コマンド含む)を意味します。

TOTAL COUNT　このページで報告されている事象の総数
SUCCESS　正常
VIORATE　不正
WARNING　警告
NOUSER　未定義ユーザ
未定義ユーザのアクセス数は他の正常、不正、警告と重なることがあります。

(2) 事象コードの詳細

形式及び内容は「処理レコード・サマリー・レポート（SW10)」に同じで、このページで報告された事象のみを対象とします。

CODE　XXYY の 4 桁
- XX：　事象コード
- YY：　事象コード修飾子

日立システムの TRUST の場合、事象コードと事象コード修飾子は次を意味します。
- 事象コード　コマンドコード（16 進表示）
- 事象コード修飾子　エラー情報（16 進表示）

なお、擬似コマンド（JOB、LOGON、VERIFY）については、ユーザ検証時の事象と重複しますが分類して報告します。

COUNT　件数
EVENT CODE MEANING
　事象コードの説明
EVENT CODE QUALIFIER MEANING
　事象コード修飾子の説明
DESCRIPTION　結果
- 'VIOLATION AND UNDEFINED USER'
  システムに未定義のユーザが不正アクセスを行った。
- 'THE EVENT IS A VIOLATION'
  不正なアクセスを行った。
- 'USER IS NOT DEFINED TO RACF'
  システムに未定義のユーザがアクセスした。
- 'THE EVENT IS A WARNING'
  警告
- 'SUCCESSFUL'
  正常に処理された。

事象コードや事象コード修飾子の詳細な説明については、下記のメーカ提供のマニュアルを参照してください。
- IBMシステム　：資源アクセス管理機能 監査担当者の手引き Resource Access Control Facility Auditor's Guide
- 富士通システム　：OSIV/MSP RACFユーティリティ使用手引書
- 日立 システム　：TRUST E2 セキュリティ監視の手引き

3.4　ジョブグループ毎のサマリー・レポート（SW30）

ジョブグループ毎のサマリー・レポートはセキュリティツールのログに記録されている事象の発生回数をJOBGRPスイッチで指定された分類方法に従ってジョブグループ単位に示します。

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON     8
PSW=SW30                                  ---- RACF MONTHLY SUMMARY REPORT BY JOBGROUP ----                     VER=09 LVL=99

                0101   0106   0200   0201   0201   1300   1800                *------- TOTAL COUNT -------*
JOBGROUP        VIOL   VIOL   SUCC   VIOL   V+NU   SUCC   SUCC          SUCCESS VIOLATE WARNING NOUSER
AAA*                                  425                                    425       0       0      0
BBB*                                   45      1                              45       1       0      0
CCC*                                   21                                     21       0       0      0
DDD*                                   10                                     10       0       0      0
EEE*                    1              3                     1                4       1       0      0
FFF*                                1129      4              4             1133       4       0      0
GGG*                                   15                                     15       0       0      0
HHH*                                   28                                     28       0       0      0
III*                                   51                                     51       0       0      0
JJJ*                                   52                                     52       0       0      0
KKK*                                   14                                     14       0       0      0
LLL*                                   64                     1               65       0       0      0
MMM*                                  158                                    158       0       0      0
NNN*                                  126      1                             126       1       0      0
OOO*                                 1367      8                            1367       8       0      0
PPP*                                  185                                    185       0       0      0
QQQ*                                  162                                    162       0       0      0
RRR*                                   77                                     77       0       0      0
SSS*                    1             9199     31      2              6       9205      34       0      2
TTT*                                   28                                     28       0       0      0
UUU*                                  419      1                             419       1       0      0
VVV*                                  608                             3      611       0       0      0
ZZ*                                    27                                     27       0       0      0
_OTHER_          203    22     23      2      1      1                       24     228       0      1

    ( TIMEBASE = 00 )
SYSTEM = IIMA (OS:MVS ,RACF :9999) START = 08/02/28 THU 2323 END = 08/03/09 SUN 1051      REPORTING DATE = 09/03/19 THU 1328
```

Rpt 3.4　ジョブグループ毎のサマリー・レポートの例

このジョブグループ毎のサマリー・レポートの内容は次のようになっています。

JOBGROUP	ジョブグループ名
XXYY	事象コードとその状態は 2 行で示されます。
STAT	状態は下記があります。
	SUCC ： 正常
	VOIL ： 不正
	NUSR ： 正常で未定義ユーザ
	V+NU ： 不正で未定義ユーザ
	WARN ： 警告
	W+NU ： 警告で未定義ユーザ

日立システムの場合、XXYY:C と表示されることがあります。
これは、TRUST コマンド(擬似コマンド含む)を意味します。

TOTAL COUNT	このページで報告されている事象の総数
SUCCESS	正常
VIORATE	不正
WARNING	警告
NOUSER	未定義ユーザ
	未定義ユーザのアクセス数は他の正常、不正、警告と重なることがあります。

3.5　グループ毎のサマリー・レポート（SW40）

セキュリティツールではユーザをグループ化することができます。このレポートでは、セキュリティツールで定義されているグループ毎に事象の発生回数をサマリーしたレポートが作成されます。SW40が“1”に設定されていれば、このレポートが出力されます。

```
(C) I I M  CORP.  1987-2009        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON     9
PSW=SW40                                  ------ RACF MONTHLY SUMMARY REPORT BY GROUPID ------                    VER=09 LVL=99

                0101   0106   0200   0201   0201   1300   1800                *-------- TOTAL COUNT --------*
GROUPID         VIOL   VIOL   SUCC   VIOL   V+NU   SUCC   SUCC          SUCCESS VIOLATE WARNING NOUSER
*                203     24 ..... ..... ..... ..... .....                     0     227       0      0
_BLANK_          ..... ..... ..... .....      2 ..... .....                     0       2       0      2
GIDA00           ..... ..... .....       3 ..... ..... .....                     3       0       0      0
GIDB00           ..... ..... .....    7694      1 .....      1      6         7701       1       0      0
GIDC00           ..... ..... .....       6 ..... ..... .....      2            8       0       0      0
GIDD00           ..... ..... .....     158 ..... ..... ..... .....           158       0       0      0
GIDE00           ..... ..... .....    2908 ..... ..... .....      3         2911       0       0      0
GIDF00           ..... ..... .....     532 ..... ..... ..... .....           532       0       0      0
GIDG00           ..... ..... .....       4 ..... ..... ..... .....             4       0       0      0
GIDH00           ..... ..... .....     898     29 ..... .....      4          902      29       0      0
GIDI00           ..... ..... .....      13 ..... ..... ..... .....            13       0       0      0
GIDJ00           ..... ..... .....      16 ..... ..... ..... .....            16       0       0      0
GIDK00           ..... ..... .....      96      1 ..... ..... .....           96       1       0      0
GIDL00           ..... ..... ..... ..... .....      1 ..... .....             0       1       0      1
GIDM00           ..... ..... ..... .....      1 ..... ..... .....             0       1       0      0
GIDN00           ..... ..... .....     425 ..... ..... ..... .....           425       0       0      0
GIDO00           ..... ..... .....    1201      8 ..... ..... .....         1201       8       0      0
GIDP00           ..... ..... .....     182 ..... ..... ..... .....           182       0       0      0
GIDQ00           ..... ..... .....     100      8 ..... ..... .....           100       8       0      0

    ( TIMEBASE = 00 )
SYSTEM = IIMA (OS:MVS ,RACF :9999) START = 08/02/28 THU 2323 END = 08/03/09 SUN 1051      REPORTING DATE = 09/03/19 THU 1328
```

Rpt 3.5　グループ毎のサマリー・レポートの例

このグループ毎のサマリー・レポートの内容は次のようになっています。

GROUPID	ジョブグループ名
XXYY	事象コードとその状態は 2 行で示されます。
STAT	状態は下記があります。 SUCC ： 正常 VOIL ： 不正 NUSR ： 正常で未定義ユーザ V+NU ： 不正で未定義ユーザ WARN ： 警告 W+NU ： 警告で未定義ユーザ

日立システムの場合、XXYY:C と表示されることがあります。
これは、TRUST コマンド(擬似コマンド含む)を意味します。

TOTAL COUNT	このページで報告されている事象の総数
SUCCESS	正常
VIORATE	不正
WARNING	警告
NOUSER	未定義ユーザ 未定義ユーザのアクセス数は他の正常、不正、警告と重なることがあります。

3.6　ユーザ毎の不正アクセス・サマリー・レポート（SW50）

セキュリティツールのログ情報には、正常なアクセス情報や不正アクセス情報が混在しています。このレポートでは、不正アクセスをユーザ単位にサマリーした状況を示します。IBMシステムの場合、ユーザを特定するときにユーザ名を含めることもできます。これは、SELNMCHKスイッチで指定します。また、報告する事象の選択、除外や閾値の設定をすることもできます。

■IBMシステム:ユーザ名を含む場合

```
(C) I I M  CORP.  1987-2010        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON    10
PSW=SW50                                 ---- RACF MONTHLY ERRORY REPORT ----                                    VER=09 LVL=99

GROUPID  USERID  :USER NAME FROM ACEE (COUNT) USERID  :USER NAME FROM ACEE (COUNT) USERID  :USER NAME FROM ACEE (COUNT)
EVENT CODE = 0101(INVPSWD ) JOBINIT/LOGON/LOGOFF INVALID PASSWORD
                            ( LIMIT =  0 , COUNT =     1 )
GR1      USER101 :USER_NAME_1         (    1)

EVENT CODE = 0109(UNDFUSER) JOBINIT/LOGON/LOGOFF UNDEFINED USERID
                            ( LIMIT =  0 , COUNT =     1 )
_BLANK_  USER102 :                    (    1)

EVENT CODE = 0125(PWDEXPR ) JOBINIT/LOGON/LOGOFF CURRENT PASSWORD HAS EXPIRED
                            ( LIMIT =  0 , COUNT =     1 )
GR2      USER103 :USER_NAME_3         (    2)

    ( TIMEBASE = 00 )
SYSTEM = IIMB (OS:MVS ,RACF :9999) START = 09/03/03 TUE 0635 END = 09/03/03 TUE 1203     REPORTING DATE = 10/04/15 THU 1120
```

■IBMシステム:ユーザ名を含まない場合

```
(C) I I M  CORP.  1987-2010        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON    10
PSW=SW50                                 ---- RACF MONTHLY ERRORY REPORT ----                                    VER=09 LVL=99

GROUPID  USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT)
EVENT CODE = 0201(INSAUTH ) RESOURCE ACCESS      INSUFFICIENT AUTHORITY
                            ( LIMIT =  0 , COUNT =     6 )
GRP1     USER001 (    1)
GRP2     USER002 (   22) USER003 (    5) USER004 (    1) USER005 (    1)
GRP3     USER006 (    1)

EVENT CODE = 0201(INSAUTH ) RESOURCE ACCESS      INSUFFICIENT AUTHORITY (UNDEFINED USER)
                            ( LIMIT =  0 , COUNT =     2 )
_BLANK_  USER014 (    2)
GRP7     USER015 (    1)

    ( TIMEBASE = 00 )
SYSTEM = IIMI (OS:MVS ,RACF :9999) START = 08/02/28 THU 2323 END = 08/03/09 SUN 1051     REPORTING DATE = 10/04/15 THU 1356
```

■富士通システムの場合

```
(C) I I M  CORP.  1987-2010        EXPERT SYSTEM / ONE       ***** RACF AUDIT REPORTS *****                    AUDITMON    13
PSW=SW50                                 ---- RACF MONTHLY ERRORY REPORT ----                                    VER=09 LVL=99

GROUPID  USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT)
EVENT CODE = 0201 RESOURCE ACCESS      INSUFFICIENT AUTHORITY
                 ( LIMIT =  0 , COUNT =    10 )
GRP1     USER001 (    3) USER002 (    1)
GRP2     USER003 (    1)
GRP3     USER004 (   12) USER005 (   10) USER006 (    4) USER007 (    1) USER008 (    1)
GRP4     USER009 (    2)
GRP5     USER010 (    1)

EVENT CODE = 1101 RACF COMMAND         ALTDSD   : INSUFFICIENT AUTHORITY
                 ( LIMIT =  0 , COUNT =     1 )
GRP6     USER011 (  150)

    ( TIMEBASE = 00 )
SYSTEM = MSP1 (OS:MSP ,RACF :9999) START = 09/03/02 MON 0000 END = 09/03/02 THU 2351     REPORTING DATE = 10/04/15 THU 1356
```

■日立システムの場合

```
(C) I I M  CORP.  1987-2010        EXPERT SYSTEM / ONE       ***** TRUST AUDIT REPORTS *****                    AUDITMON    11
PSW=SW50                                  ---- TRUST MONTHLY ERRORY REPORT ----                                  VER=09 LVL=99

GROUPID  USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT) USERID  (COUNT)
EVENT CODE = 5001 LOGON                INVALID PASSWORD
                ( LIMIT =  0 , COUNT =    15 )
GRP1     USER001 (    1)
GRP2     USER002 (    1) USER003 (    1) USER004 (    1) USER005 (    1) USER006 (    1) USER007 (    1) USER008 (    1)
         USER009 (    1) USER010 (    1) USER011 (    1) USER012 (    1) USER013 (    1) USER014 (    1)
GRP3     USER015 (    4)

EVENT CODE = 5003 LOGON                INVALID USERID
                ( LIMIT =  0 , COUNT =     6 )
_BLANK_  USER016 (    1) USER017 (    1) USER018 (    1) USER019 (    1) USER020 (    1) USER021 (    1)

    ( TIMEBASE = 00 )
SYSTEM = VOS3 (OS:VOS3,TRUST:9999) START = 09/03/02 MON 0430 END = 09/03/02 MON 2252     REPORTING DATE = 10/04/15 THU 1657
```

このユーザ毎の不正アクセス・サマリー・レポートの内容は次のようになっています。

(1) 事象の情報

EVENT CODE	事象コード（XXYY）
	事象コードや事象コード修飾子の説明
	事象コードの後の（事象修飾子）は IBM システムのみ表示
LIMIT	閾値
COUNT	ユーザの数

(2) 事象が発生したユーザ情報

GROUPID	グループ ID
USERID(COUNT)	ユーザ ID（このユーザでの発生回数）
USERID : USER NAME FROM ACEE (COUNT)	
	ユーザ ID:ユーザの名前（このユーザでの発生回数）

閾値が設定されている場合、閾値を越えたユーザがいない時には下記が出力されます。
'NO EXCEED LIMIT VALUE'

3.7　添付資料：事象修飾子（@IBMRACF メンバー）

このプロセジャを実行する際にはDD名CARDINで事象修飾子を定義したメンバーを指定します。このメンバーでは、各事象コードに対応する事象修飾子を定義しています。この定義を編集することで、事象修飾子をプロセジャの実行結果に反映することもできます。

【@IBMRACFメンバーの内容】

```
*XXYY EVENT QUALIFIER,EVENT CODE NAME,EVENT CODE,EVENT QUALIFIER NUMBER
*REFER TO Z/OS V1R10.0 SECURITY SERVER RACF MACROS AND INTERFACES
'0100' 'SUCCESSI' JOBINIT 01 00
'0101' 'INVPSWD ' JOBINIT 01 01
```

先頭の2行はコメントですが編集しないでください。3行目以降が定義部分になり、次の形式です。

' 事象コード' ' 事象修飾子' コメント

コメント部は事象コード名、事象コード、事象コード修飾子の順番です。

尚、事象修飾子については下記のメーカ提供マニュアルを参照してください。

「z/OS Security Server RACF マクロおよびインターフェース」

第4章 PNAVIADT の使用方法

PNAVIADTプロセジャは、セキュリティツールのログ情報を基に、システム資源に対するアクセス状況をCSV形式で出力します。

このアクセス状況には、

○不正アクセス

○未定義ユーザ

○警告

○正常アクセス

などが含まれます。

CSVファイルに出力する内容はユーザ／ジョブ名、およびボリューム名、データセット名などで選択することができます。

このプロセジャでは、下記に示すセキュリティツールのログ情報やジョブ情報を処理対象としています。

IBM	:	RACF	SMF タイプ80
富士通	:	RACF	SMF タイプ80
日　立	:	TRUST E2	SMS タイプ118、SMS タイプ 108

4.1 実行パラメータ

PNAVIADT提供されるサンプル・ジョブ制御文のは2つのジョブステップで構成されています。

1. CPEMACR0 ： 設定されたパラメータによりプロセジャの実行に必要なスイッチ群を生成します。

2. CPESHELL ： プロセジャを実行し、その結果をCSV形式のファイルに出力します。

富士通または日立システムの場合、DD文“CARDIN”をコメントアウトしてください。

```
//PNAVIADT JOB (ACCT),MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,NOTIFY=USERID
//JOBLIB   DD DSN=CPE.LOAD,DISP=SHR
//*JOBCAT  DD DSN=USER.CAT,DISP=SHR
//*********************************************************************
//* プロダクト名 : MF-SCOPE,AUDIT プロセジャ名 : PNAVIADT             *
//*-------------------------------------------------------------------*
//* JCLの以下の部分を変更してください。                               *
//* ES/1 NEO LIBRARY                                                  *
//*         - CPE.LOAD       ( ロードモジュールライブラリ )           *
//*         - CPE.PARM       ( ソースライブラリ           )           *
//*         - CPE.PCGM       ( マクロライブラリ           )           *
//* SHELL   - 環境にあわせてREGIONサイズを変更してください。          *
//* OSタイプを以下の中から選択してください。                          *
//*         - #OSTYPE        ( 実行環境OS                )           *
//*           (MVS,Z/OS,MSP,MSP-EX,VOS3)                              *
//* INPUT   - INPUT.DATA     ( 解析すべき稼働実績データ  )           *
//* BASICUT1- OUTPUT.CSVFILE ( CSV出力ファイル)                       *
//*         - VOLSER         ( CSVファイル格納ボリューム )           *
//******************************************************* SINCE V5L03 ***
//MACRO    EXEC PGM=CPEMACR0,REGION=4096K
//MACLIB   DD DSN=CPE.PCGM,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD DUMMY
//SYSUT1   DD UNIT=SYSDA,SPACE=(TRK,(10,10))
//PLATFORM DD DSN=&PLATFORM,UNIT=SYSDA,SPACE=(TRK,(1,1)),
//            DISP=(,PASS,DELETE)
//SYSIN    DD *
         ALIST ON
*   日付選択（必須）
         %PNSELDT  START=(00000,0000),
                   END=(99999,2400)
*   実行環境設定（必須）
*   CSV形式での出力指定
         %PNADTDEF OUTPUT=CSV,
                   OSTYPE
*                  OSTYPE=MVS,
*                  OSTYPE=Z/OS,
*                  OSTYPE=MSP,
*                  OSTYPE=MSP-EX,
*                  OSTYPE=VOS3,
*                  SYSTEM=,
*                  SUCC=YES,VIOL=YES,WARN=YES,NUSR=YES
*
*   資源の選択・排他
*        %PNADTSEL SJOB=,EJOB=,
*                  STRM=,ETRM=,
*                  SUID=,EUID=,
*                  SGID=,EGID=,
*                  SVOL=,EVOL=,
*        %PNADTSEL SDSN=(A1-15,A16-30,A31-44)
*        %PNADTSEL SDSN=(B1-15,B16-30,B31-44)
*        %PNADTSEL EDSN=(C1-15,C16-30,C31-44)
*        %PNADTSEL EDSN=(D1-15,D16-30,D31-44)
*
*   XNF/TCP情報の出力定義（日立のみ）
*        %PNADTTCP FTP=YES,CS560=YES,XAPI=YES,ZENGIN=YES
*
*   マクロ終了を告げる通知（必須）
         %PNEND
//*
//SHELL    EXEC PGM=CPESHELL,REGION=1024M,PARM=PARM,COND=(4,LT)
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD DUMMY
//SYSUT1   DD UNIT=SYSDA,SPACE=(TRK,(10,10))
//CPEPARM  DD *
   OVER16=SYMBOL
   OSTYPE=#OSTYPE
//INPUT    DD DISP=SHR,DSN=INPUT.DATA
//CARDIN   DD DSN=CPE.PARM(@IBMRACF),DISP=SHR
//BASICUT1 DD DSN=OUTPUT.CSVFILE,DISP=(NEW,CATLG,DELETE),
//            UNIT=SYSDA,SPACE=(CYL,(2,1),RLSE),VOL=SER=VOLSER
//PLATFORM DD DSN=&PLATFORM,DISP=(OLD,DELETE,DELETE)
//         DD DSN=CPE.PCGM(PNAVIADT),DISP=SHR
```

Jcl 4.1 サンプル・ジョブ制御文（JCADTCSV）

4.1.1. PNSELDT（日付選択（必須））

PNSELDTマクロでは、CPESHELLの入力データの範囲や、その際の日付形式を指定します。このマクロは他のすべてのマクロより先に定義しなければなりません。

名前	%命令	オペランド
[LABEL]	%PNSELDT	START=(yymmdd,hhmm) ,END=(yymmdd,hhmm) [,AMONTH=n] [,SDATE=n] [,EDATE=n] [,ATIME=(hhmm,hhmm)]

START＝（開始日付，開始時刻），END＝（終了日付，終了時刻）

対象とするパフォーマンス・データの日時を指定します。日付の形式は、ジュリアンデート（yyddd）、またはグレゴリアンデート（yymmdd）で指定します。このとき、STARTとENDパラメータの日付形式は、必ず一致するように指定する必要があります。

AMONTH＝n，ATIME＝（hhmm，hhmm）

毎月の定期的な作業として、前月分のデータ（1～末日）を解析対象としたい場合、「AMONTH」パラメータを使用します。

AMONTHで指定された数により、現在の月から最大12ヶ月の前月を指定することが可能です。なお、AMONTHパラメータを使用して解析対象日を指定した場合、時間帯の指定には「ATIME」パラメータを指定します。

【例】現在が1999年12月であり、前月(11月)のデータを指定。

AMONTH=1,ATIME=(0000,2400)

この指定はSUBSET＝NOおよびSUBSET＝SPECIALの時に有効です。

SDATE＝n，EDATE＝n，ATIME＝（hhmm，hhmm）

AMONTH同様、日時処理として前日分のデータを解析対象としたい場合に使用します。

SDATE/EDATEに、n日前のデータを処理対象とするかを指定します。

【例1】日時処理で前日のデータを対象とする場合

SDATE=1,EDATE=1,ATIME=(0000,2400)

【例2】前日の8時から今日の8時までを対象とする場合

SDATE=1,EDATE=0,ATIME=(0800,0759)

日付を跨ったデータを処理をする場合はCPEDBAMS（ES/1 NEO MF-MAGIC）のRANGE文で8時から7時59分のデータを抜き出す必要があります。

4.1.2. PNADTDEF（実行環境設定（必須））

PNAVIADTプロセジャを実行する上での実行環境を設定します。

名前	%命令	オペランド
[LABEL]	%PNADTDEF	[OSTYPE={MVS | Z/OS | MSP-EX | VOS3}] [,SYSTEM=sysid] [,OUTPUT={CSV | CSVID}] [,SUCC={YES | NO}] [,VIOL={YES | NO}] [,WARN={YES | NO}] [,NUSR={YES | NO}]

OSTYPE＝{MVS | Z/OS | MSP-EX | VOS3}

解析対象のオペレーティング・システムに合わせてこのパラメータを設定します。

SYSTEM＝sysid

ES/1共通レコード形式が持つシステム識別子を設定します。

OUTPUT＝{CSV | CSVID}

出力形式を指定します。

CSV　：レコード識別子なしのCSV形式で出力します。先頭行に各項目のラベル行が出力されます。
　　RACF/TRUST情報のみ出力の場合に選択可能です。

CSVID　：レコード識別子（SMF/SMSレコード番号）を付加したCSV形式で出力します。
　　先頭行に各項目のラベル行が出力されます。
　　複数の情報を出力する場合は、こちらを選択してください。

SUCC＝{YES | NO}
VIOL＝{YES | NO}
WARN＝{YES | NO}
NUSR＝{YES | NO}

セキュリティ（RACF/TRUST）レコードにおいて、事象の結果を選択して出力できます。

SUCC　：正常
VIOL　：不正アクセス
WARN　：警告
NUSR　：未定義ユーザ
　　※省略値はすべて“YES”（出力）です。

4.1.3. PNADTSEL（資源の選択・排他）

PNAVIADTプロセジャで出力される各要素毎に選択･排他による出力の絞込みを可能とします。

名前	%命令	オペランド
[LABEL]	%PNADTSEL	[SJOB={jobname | (jobname, jobname... jobname)}] [, EJOB={jobname | (jobname, jobname... jobname)}] [, STRM={tername | (tername, tername... tername)}] [, ETRM={tername | (tername, tername... tername)}] [, SUID={usrid | (usrid, usrid... usrid)}] [, EUID={usrid | (usrid, usrid... usrid)}] [, SGID={grpid | (grpid, grpid... grpid)}] [, EGID={grpid | (grpid, grpid... grpid)}] [, SVOL={volsee | (volser, volser... volser)}] [, EVOL={volsee | (volser, volser... volser)}] [, SDSN=(dsname1 | (dsname2, dsname3)] [, EDSN=(dsname1 | (dsname2, dsname3)]

```
SJOB={jobname | (jobname, jobname …jobname)}
EJOB={jobname | (jobname, jobname …jobname)}
```

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

セキュリティレコードにおいて、出力対象、または対象外とするジョブ名を指定します。ジョブ名の指定には比較制御文字を利用した指定が可能です。(注)

SJOB=jobname　：出力対象とするジョブ名
EJOB=jobname　：出力対象外とするジョブ名

```
STRM={tername | (tername, tername …tername)}
ETRM={tername | (tername, tername …tername)}
```

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

セキュリティレコードにおいて、出力対象、または対象外とする端末名を指定します。端末名の指定には比較制御文字を利用した指定が可能です。(注)

STRM=tername　：出力対象とする端末名
ETRM=tername　：出力対象外とする端末名

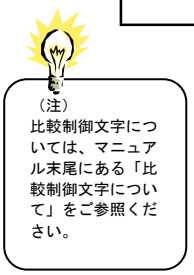
```
SUID={usrid | (usrid, usrid …usrid)}
EUID={usrid | (usrid, usrid …usrid)}
```

（注）
比較制御文字については、マニュアル末尾にある「比較制御文字について」をご参照ください。

セキュリティレコードにおいて、出力対象、または対象外とするユーザIDを指定します。ユーザIDの指定には比較制御文字を利用した指定が可能です。(注)

SUID=usrid　：出力対象とするユーザID
EUID=usrid　：出力対象外とするユーザID

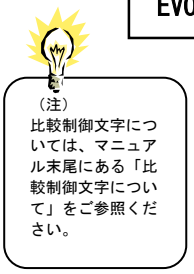
```
SGID={grpid | (grpid,grpid …grpid)}
EGID={grpid | (grpid,grpid …grpid)}
```



セキュリティレコードにおいて、出力対象、または対象外とするグループIDを指定します。グループIDの指定には比較制御文字を利用した指定が可能です。(注)

SGID=groupid　　：　出力対象とするグループID
EGID=troupid　　：　出力対象外とするグループID

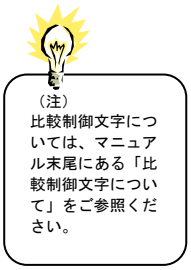
```
SVOL={volser | (volser,volser …volser)}
EVOL={volser | (volser,volser …volser)}
```



セキュリティレコードにおいて、出力対象、または対象外とするボリューム通番を指定します。ボリューム通番の指定には比較制御文字を利用した指定が可能です。(注)

SVOL=volser　　：　出力対象とするボリューム通番
EVOL=volser　　：　出力対象外とするボリューム通番

```
SDSN={dsname | (dsname,dsname …dsname)}
EDSN={dsname | (dsname,dsname …dsname)}
```



セキュリティレコードにおいて、出力対象、または対象外とするデータセット名を指定します。データセット名の指定には比較制御文字を利用した指定が可能です。(注)

SDSN=dsname　　：　出力対象とするデータセット名
EDSN=dsname　　：　出力対象外とするデータセット名

1つのSDSN/EDSNパラメータに1つのデータセット名を指定し、15文字ずつカンマ(,)で区切ります。
【例】以下の2つのデータセットを出力対象とする。
　　'IIM.USER001＊'
　　'IIM.USER0001.IBM.SMFDATA.D070801.＊'

[指定方法]
　%PNADTSEL　SDSN=IIM.USER001＊
　%PNADTSEL　SDSN=(IIM.USER0001.IB,M.SMFDATA.D0708,01＊)

4.1.4. PNADTTCP（日立 XNF/TCP 情報の出力定義）

日立XNF/TCP情報の出力項目を設定します。

名前	%命令	オペランド
[LABEL]	%PNADTTCP	[FTP={YES | NO}] [,CS560={YES | NO}] [,XAPI={YES | NO}] [,ZENGIN={YES | NO}]

```
FTP＝YES | NO
CS560＝YES | NO
XAPI＝YES | NO
ZENGIN＝YES | NO
```

CSVフラットファイルに出力するレコード種別を選択します。

FTP　　：FTP関連レコードを出力します。(省略時＝NO)
CS560　：C/S560関連レコードを出力します。(省略時＝NO)
XAPI　　：XAPI,OSAS/TCP関連レコードを出力します。(省略時＝NO)
ZENGIN ：OSAS/TCP(全銀協(TCP/IP)手順)関連レコードを出力します。(省略時＝NO)

当レコードを出力するには%PNADTDEF マクロで"OUTPUT=CSVID"を指定する必要があります。

4.1.5. その他の制御スイッチ

ERRORCDE

リターン・コード

解析対象のパフォーマンス・データがない場合、もしくはプロセジャが出力すべきデータがない場合、以下のメッセージを出力します。このときのリターン・コードを、ERRORCDEに任意の値を指定することで変更できます。
指定できる値は0～4095の範囲の整数で、省略値は8です。

・解析対象のパフォーマンス・データがない場合のメッセージ

```
NO PERFORMANCE DATA IS FOUND.
```

・プロセジャが出力すべきデータがない場合のメッセージ

```
THERE WAS NO OUTPUT DATA.
```

4.2 出力レコード形式

PNAVIADTが出力するCSVファイルの項目一覧を示します。出力結果はユーザプログラムや表計算プログラムを使用して処理することが可能です。

4.2.1. RACF | TRUST 情報

項番	バイト	形式	内容	IBM	富士通	日立
S1	3	数値	SMF/SMS レコード番号（OUTPUT=CSVID 指定時のみ）	○	○	○
S2	2	数値	SMS サブタイプ番号（OUTPUT=CSVID 指定時のみ）	－	－	○
1	4	文字	システム識別子	○	○	○
2	8	YY/MM/DD YYYY/MM/DD	事象発生日 ※OUTPUT=CSV → "YY/MM/DD" ※OUTPUT=CSVID → "YYYY/MM/DD"	○	○	○
3	5	HH:MM HH:MM:SS	事象発生時間 ※OUTPUT=CSV → "HH:MM" ※OUTPUT=CSVID → "HH:MM:SS"	○	○	○
4	8	文字	ユーザ ID	○	○	○
5	8	文字	グループ ID	○	○	○
6	8	文字	端末名	○	○	○
7	8	文字	ジョブ名	○	○	○
8	4	文字	結果 ・"SUCC" ： 正常 ・"VIOL" ： 不正アクセス ・"WARN" ： 警告	○	○	○
9	1	数値	未定義ユーザの識別 ・0： 定義済ユーザ ・1： 未定義ユーザ	○	○	○
10	20	文字	ユーザの名前	○	－	－
11	4	文字	事象コード	○	○	○
12	8	文字	事象名／コマンド名	○	○	○
13	8	文字	事象修飾子	○	－	－
14	1	文字	サブタイプ48（保護情報変更）識別（'C'）	－	－	○
15	16	文字	資源にアクセスしたユーザの権限や属性	○	○	○
16	8	文字	ユーザが要求したアクセス権	○	○	○
17	8	文字	セキュリティツールが許可したアクセス権	○	○	－
18	8	文字	アクセス権をチェックする際のユーザ権限や属性	－	○	－
19	8	文字	アクセス権種別	－	○	－
20	8	文字	リソース種別名	○	○	○
21	44	文字	データセット名／資源名	○	○	○
22	6	文字	ボリューム通番	○	○	○
23	44	文字	プロファイル名	○	○	－
24	10	YYYY/MM/DD	ジョブ入力日	○	○	－
25	44	HH:MM:SS	ジョブ入力時刻	○	○	－

※バイト＝最大バイト数

4.2.2. 日立 XNF/TCP 情報 (SMS108)

項番	バイト	形式	内容	FTP/SV		FTP/CL		CS560	XAPI		OSAS		全銀協	
				02	03	06	07	04	08	09	08	09	0D	0E
1	3	数値	SMS レコード番号(108)	○	○	○	○	○	○	○	○	○	○	○
2	2	数値	SMS サブタイプ番号	○	○	○	○	○	○	○	○	○	○	○
3	10	YYYY/MM/DD	コネクション確立日付	○	○	○	○	○	○	－	○	－	○	○
			ポートオープン日付	－	－	－	－	－	－	○	－	○	－	－
4	5	HH:MM:SS	コネクション確立時刻	○	○	○	○	○	○	－	○	－	○	○
			ポートオープン時刻	－	－	－	－	－	－	○	－	○	－	－
5	10	YYYY/MM/DD	コネクション解放日付	○	○	○	○	○	○	－	○	－	○	○
			ポートクローズ日付	－	－	－	－	－	－	○	－	○	－	－
6	5	HH:MM:SS	コネクション解放時刻	○	○	○	○	○	○	－	○	－	○	○
			ポートクローズ時刻	－	－	－	－	－	－	○	－	○	－	－
7	10	数値	送信バイト数(BYTE)	○	○	○	○	○	○	○	○	○	○	○
8	10	数値	受信バイト数(BYTE)	○	○	○	○	○	○	○	○	○	○	○
9	10	数値	送信セグメント数	○	○	○	○	○	○	－	○	－	○	○
			送信パケット数	－	－	－	－	－	－	○	－	○	－	－
10	10	数値	受信セグメント数	○	○	○	○	○	○	－	○	－	○	○
			受信パケット数	－	－	－	－	－	－	○	－	○	－	－
11	10	数値	再送回数	○	○	○	○	○	○	－	○	－	○	○
12	10	数値	受信セグメント破棄回数	○	○	○	○	○	○	－	○	－	○	○
13	10	数値	送信 ACK 数	○	○	○	○	○	○	－	○	－	○	○
14	10	数値	受信 ACK 数	○	○	○	○	○	○	－	○	－	○	○
15	10	数値	送信論理 ACK 数	－	－	－	－	－	－	－	－	－	○	○
16	10	数値	受信論理 ACK 数	－	－	－	－	－	－	－	－	－	○	○
17	8	文字	相手ホスト名	○	○	○	○	○	○	－	○	－	○	○
18	16	文字	相手 IP アドレス	○	○	○	○	○	○	－	○	－	○	○
19	16	文字	自 IP アドレス	○	○	○	○	○	○	－	○	－	○	○
20	5	数値	相手ポート番号	○	○	○	○	○	○	－	○	－	○	○
21	5	数値	自ポート番号	○	○	○	○	○	○	○	○	○	○	○
22	8	文字	接続アプリケーションプログラム名	○	－	－	－	－	－	－	－	－	－	－
	8	文字	XNF/TCP の本体用 UCE	－	○	－	－	－	－	－	－	－	－	－
	8	文字	端末 UCE 名	－	－	－	－	○	－	－	－	－	－	－
	8	文字	TSS のユーザ ID	－	－	○	－	－	－	－	－	－	－	－
	8	文字	ユーザ ID	－	－	－	○	－	－	－	－	－	－	－
	8	文字	XAPI ユーザプログラムから通知されるジョブ名	－	－	－	－	－	○	○	－	－	－	－
	8	文字	接続アプリケーション名(上位 AP の UCE 名)	－	－	－	－	－	－	－	○	○	－	－
	8	文字	接続アプリケーション名	－	－	－	－	－	－	－	－	－	○	○
23	8	文字	端末 UCE 名	○	－	－	－	－	－	－	－	－	－	－
	8	文字	XAPI の UCE 名	－	○	○	○	－	○	○	－	－	－	－
	8	文字	アプリケーションのセレクタ名	－	－	－	－	○	－	－	－	－	－	－
	14	文字	相手システムのアプリケーション対応 UCE 名	－	－	－	－	－	－	－	○	－	－	－
	8	文字	仮想相手システムの UCE 名	－	－	－	－	－	－	－	－	○	－	－
	8	文字	相手ホスト対応 UCE 名	－	－	－	－	－	－	－	－	－	○	○
24	8	文字	ユーザ ID	○	○	－	－	－	－	－	－	－	－	－
25	14	数値	センタ ID(上位 7Byte:相手センタ確認コード)	－	－	－	－	－	－	－	－	－	○	○
26	14	数値	センタ ID(下位 7Byte:相手センタ確認コード)	－	－	－	－	－	－	－	－	－	○	○

※バイト＝最大バイト数

比較制御文字について

ES/1 NEOでは、対象の絞り込み、またはグルーピングを行う場合などに以下の比較制御文字を使用することができます。

比較制御文字		IBM	富士通		日立	NEC
			MSP	XSP		
?	該当桁の比較を行わない	○	○	○	○	○
*	該当桁以降の比較を行わない	○	○	○	○	○
+	該当桁が数字（0～9）であるか比較を行う	○	○	○	○	－
/	該当桁が文字（A～Z）であるか比較を行う	○	○	○	○	－

【例1】先頭3桁が「ABC」で始まるものを対象とする
SELECT='ABC* '

【例2】先頭から4桁目が「D」のものを対象とする
SELECT='???D* '

【例3】先頭3桁が「ABC」で始まり、5桁目が「数字」のものを対象とする
SELECT='ABC?+*'

【例4】先頭3桁が「ABC」で始まり、5桁目が「文字」のものを対象とする
SELECT='ABC？/*'

ES/1 NEO MF シリーズ　プロセジャ共通仕様

ここでは、全プロセジャ共通の仕様について記述します。

◆規定桁数を超える値の表示

プロセジャが出力するレポート中、表示する値が規定の桁数を超える場合には自動的に表示を変更します。

○時間表示

HH:MM:SS　→　HHHHH:MM
HH:MM:SS.TH　→　HHHHH:MM:SS

【例】111時間22分33秒44の場合
HH:MM:SS形式　→　00111:22
HH:MM:SS.TH形式　→　00111:22:34

○数値表示

・K（キロ＝1000倍）
・M（メガ＝1000000倍）
・G（ギガ＝1000000000倍）

【例】表示桁数4桁の場合
123456　→　123K
12345678　→　12M