zSecure Alert
バージョン 2.3.0

ユーザー・リファレンス・マニュアル

SA88-7156-04

zSecure Alert
バージョン 2.3.0

ユーザー・リファレンス・マニュアル

SA88-7156-04

注記

本書および本書で紹介する製品をご使用になる前に、 181 ページの『特記事項』に記載されている情報をお読みください。

2017 年 **8** 月

本書は、IBM Security zSecure Alert (製品番号 5655-N21) のバージョン 2、リリース 3、モディフィケーション 0 に適用されます。また、改訂版などで特に断りのない限り、これ以降のすべてのリリースおよびモディフィケーションにも適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： SC27-5642-04
zSecure Alert
Version 2.3.0
User Reference Manual

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

本書について

本書では、セキュリティー・サーバー (RACF®) または CA-ACF2 で保護された z/OS® システムのリアルタイム・モニターである IBM® Security zSecure™ Alert の構成、使用、およびトラブルシューティングの方法を説明しています。

本書は次の読者向けに記述されています。

- IBM Security zSecure Alert の構成を担当するシステム・サポート担当者
- IBM Security zSecure Alert によって提供される追加のコマンド制御の実装を担当するセキュリティー管理者

本書の読者は、RACF および ACF2 の概念とコマンドも理解しておく必要があります。

IBM Security zSecure Alert のインストールについて詳しくは、「*IBM Security zSecure CARLa-Driven Components* インストールおよびデプロイメント・ガイド」を参照してください。

zSecure 資料

IBM Security zSecure Suite ライブラリーおよび IBM Security zSecure Manager for RACF z/VM ライブラリーの資料には、非ライセンス出版物とライセンス出版物が含まれています。このセクションでは、両方のライブラリーと、それらへのアクセス手順をリストします。

zSecure の非ライセンス出版物は、IBM zSecure Suite (z/OS) または IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から入手できます。IBM Knowledge Center は、IBM 製品資料のホームです。IBM Knowledge Center をカスタマイズし、独自の資料の集合を作成して、使用するテクノロジー、製品、およびバージョンを表示するように画面を設計できます。トピックにコメントを追加したり、Eメール、LinkedIn、Twitter で話題を共有したりすることで、IBM や同僚と対話することもできます。ライセンス出版物の入手手順については、viii ページの『ライセンス文書の入手』を参照してください。

表 *1.*

製品の **IBM Knowledge Center**	**URL**
IBM zSecure Suite (z/OS)	www.ibm.com/support/knowledgecenter/SS2RWS/welcome
IBM zSecure Manager for RACF z/VM	www.ibm.com/support/knowledgecenter/SSQQGJ/welcome

IBM Terminology Web サイトに、製品ライブラリーの用語が 1 カ所にまとめられています。

ライセンス文書の入手

プログラム・ディレクトリーを除き、IBM Security zSecure Suite 2.3.0 および IBM Security zSecure Manager for RACF z/VM 1.11.2 のすべてのライセンス出版物および非ライセンス出版物は、*IBM Security zSecure Documentation CD*、*LCD7-5373* に含まれています。zSecure *Documentation CD* のディスク・イメージ (`.iso`) ファイルを直接ダウンロードする方法は、この製品資料に記載されています。

Documentation CD の .iso ファイルまたは個々のライセンス出版物の PDF ファイルを入手するには、tivzos@us.ibm.com まで E メールをお送りください。IBM Security zSecure Suite 2.3.0 のライセンス出版物のアクセスを要求してください。会社の IBM お客様番号と、ご希望の連絡先情報を合わせて記入してください。ご注文を処理するための詳細が送信されます。

IBM zSecure Suite ライブラリー

IBM Security zSecure Suite ライブラリーには、非ライセンス出版物とライセンス出版物が含まれています。

非ライセンス出版物は、IBM zSecure Suite の IBM Knowledge Center から入手できます。非ライセンス出版物は、クライアントのみが入手できます。ライセンス出版物の入手ライセンス出版物を入手については、ライセンス出版物の入手を参照してください。ライセンス出版物には、L で始まる資料番号 (LCD7-5373 など) があります。

IBM Security zSecure Suite ライブラリーには、次の資料があります。

- 『このリリースについて』には、リリース固有の情報に加え、zSecure 固有ではない、より一般的な情報が含まれています。リリース固有の情報には、以下が含まれます。
  - 新機能: zSecure V2.3.0 の新機能および機能拡張をリストします。
  - リリース・ノート: 各製品リリースのリリース・ノートで、IBM Security zSecure 製品の重要なインストール情報、非互換性の警告、制限事項、および既知の問題を提供しています。
  - 資料: zSecure Suite および zSecure Manager for RACF z/VM のライブラリーをリストして、簡潔に説明します。また、資料にはライセンス出版物を入手するための手順が含まれています。
  - 関連資料: zSecure に関連する情報のタイトルおよびリンクのリストです。
  - 問題解決に対するサポート: 問題解決策が IBM の知識ベースで見つかる場合がよくあります。また、製品のフィックスが提供されている場合があります。IBM ソフトウェア・サポートに登録すると、IBM の週次 E メール通知サービスサービスを購読できます。IBM サポートでは、製品の問題点に関するサポートや、よくある質問への回答を提供するほか、問題解決の支援も行っています。
- *IBM Security zSecure CARLa-Driven Components* インストールおよびデプロイメント・ガイド, SA88-7162

  次の IBM Security zSecure コンポーネントのインストールと構成に関する情報を記載しています。

  - IBM Security zSecure Admin
  - IBM Security zSecure Audit for RACF/CA-ACF2/CA-Top Secret
  - IBM Security zSecure Alert for RACF and CA-ACF2
  - IBM Security zSecure Visual
  - IBM Security zSecure Adapters for SIEM for RACF/CA-ACF2/CA-Top Secret
- *IBM Security zSecure Admin and Audit for RACF* スタートアップ・ガイド, GI88-4318

  IBM Security zSecure Admin および IBM Security zSecure Audit の製品機能、およびユーザーが標準的なタスクや手順を実行する方法を紹介する、実地のガイドが記載されています。このマニュアルは、新規ユーザーが基本的な IBM Security zSecure Admin and Audit for RACF システム機能の実用的な知識を身につけるとともに、使用可能な他の製品機能を調べる方法を理解するのに役立つことを目的としています。
- *IBM Security zSecure Admin and Audit for RACF* ユーザー・リファレンス・マニュアル, LA88-7161

  IBM Security zSecure Admin および IBM Security zSecure Audit の製品機能について説明しています。ユーザーが ISPF パネルから管理機能および監査機能を実行する方法が記載されています。このマニュアルには、トラブルシューティング・リソース、および zSecure Collect for z/OS コンポーネントのインストール手順も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure Admin and Audit for RACF* 行コマンドおよび基本コマンドの要約, SC43-2894

  簡略な説明とともに、行コマンドおよび基本 (ISPF) コマンドをリストしています。
- *IBM Security zSecure Audit for ACF2 Getting Started*, GI13-2325

  zSecure Audit for CA-ACF2 の製品機能について説明し、ユーザーが標準的なタスクや手順 (ログオン ID、規則、グローバル・システム・オプションの分析など) を実行し、レポートを実行するための方法を記載しています。また、このマニュアルには、ACF2 用語に慣れていないユーザー向けに一般的な用語のリストも記載されています。
- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640

  メインフレーム・セキュリティーおよびモニタリングのために zSecure Audit for CA-ACF2 を使用する方法について説明しています。新しいユーザーのために、このガイドには、 CA-ACF2 の使用、および ISPF パネルからの機能のアクセスに関する概要と概念情報が記載されています。上級ユーザー向けに、このマニュアルには、詳細な参照情報、トラブルシューティングのヒント、zSecure Collect for z/OS の使用に関する情報、およびユーザー・インターフェースのセットアップに関する詳細情報が記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。
- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641

zSecure Audit for CA-Top Secret の製品機能について説明し、ユーザーが標準的なタスクや手順を実行する方法を記載しています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure CARLa* コマンド・リファレンス, LC43-2107

  CARLa Auditing and Reporting Language (CARLa) についての、一般ユーザーと上級ユーザーの両方の参照情報が記載されています。CARLa は、zSecure を使用してセキュリティーの管理レポートおよび監査レポートを作成するためのプログラミング言語です。「*CARLa* コマンド・リファレンス」には、データの選択および zSecure レポートの作成のための NEWLIST タイプおよびフィールドに関する詳細情報も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure Alert* ユーザー・リファレンス・マニュアル, SA88-7156

  セキュリティー・サーバー (RACF) または CA-ACF2 で保護された z/OS システムのリアルタイム・モニターである IBM Security zSecure Alert の構成、使用、およびトラブルシューティングの方法を説明しています。

- *IBM Security zSecure Command Verifier* ユーザー・ガイド, SA88-7158

  RACF コマンドが入力されたときに RACF ポリシーを実施することによって、RACF メインフレーム・セキュリティーを保護するために IBM Security zSecure Command Verifier をインストールし、使用する方法を説明しています。

- *IBM Security zSecure CICS Toolkit* ユーザー・ガイド, SA88-7159

  CICS® 環境から RACF 管理機能を提供するために、IBM Security zSecure CICS Toolkit をインストールし、使用する方法を説明しています。

- *IBM Security zSecure* メッセージ・ガイド, SA88-7160

  すべての IBM Security zSecure コンポーネントのメッセージ解説を記載しています。このガイドは、各製品または機能に関連したメッセージ・タイプを記述し、すべての IBM Security zSecure 製品メッセージとエラーを、メッセージ・タイプ別にソートされた重大度レベルと一緒にリストします。個々のメッセージに関する説明と追加のサポート情報も提供します。

- *IBM Security zSecure Visual* クライアント・マニュアル, SA88-7157

  Windows ベース GUI から RACF 管理用タスクを実行するために IBM Security zSecure Visual Client をセットアップし、使用する方法を説明しています。

- *IBM Security zSecure Documentation CD*, LCD7-5373

  IBM Security zSecure 資料を提供します。これには、ライセンス交付された製品資料とライセンス交付されていない製品資料が含まれています。「*Documentation CD*」はダウンロード可能な .iso ファイルとして使用できます。ライセンス出版物の入手を参照して、このファイルを取得してください。

プログラム・ディレクトリーはプロダクト・テープで提供されます。プログラム・ディレクトリーから最新のコピーをダウンロードすることもできます。

- プログラム・ディレクトリー*: IBM Security zSecure CARLa-Driven Components*, GI13-2277

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure CARLa-Driven Components (Admin、Audit、Visual、Alert、および IBM Security zSecure Adapters for SIEM) のインストールに関連した資料と手順に関する情報が記載されています。
- プログラム・ディレクトリー*: IBM Security zSecure CICS Toolkit*, GI13-2282

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure CICS Toolkit のインストールに関連した資料と手順に関する情報が記載されています。
- プログラム・ディレクトリー*: IBM Security zSecure Command Verifier*, GI13-2284

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure Command Verifier のインストールに関連した資料と手順に関する情報が記載されています。
- プログラム・ディレクトリー*: IBM Security zSecure Admin RACF-Offline*, GI13-2278

  このプログラム・ディレクトリーは、プログラムのインストールと保守を担当するシステム・プログラマーを対象としています。IBM Security zSecure Admin の IBM Security zSecure Admin RACF-Offline コンポーネントのインストールに関連した資料と手順に関する情報が記載されています。
- zSecure Administration、監査、およびコンプライアンスの各ソリューションのプログラム・ディレクトリー
  - 5655-N23: *Program Directory for IBM Security zSecure Administration*、GI13-2292
  - 5655-N24: *Program Directory for IBM Security zSecure Compliance and Auditing*、GI13-2294
  - 5655-N25: *Program Directory for IBM Security zSecure Compliance and Administration*、GI13-2296

IBM zSecure Manager for RACF z/VM ライブラリー

IBM Security zSecure Manager for RACF z/VM ライブラリーには、非ライセンス出版物とライセンス出版物が含まれています。

非ライセンス出版物は、IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から入手できます。ライセンス出版物には、L で始まる資料番号 (LCD7-5373 など) があります。

IBM Security zSecure Manager for RACF z/VM ライブラリーには、次の資料があります。

- *IBM Security zSecure Manager for RACF z/VM* リリース情報

製品リリースごとに、「リリース情報」のトピックで、 新機能と機能拡張、非互換性の警告、および資料の更新情報を提供します。最新バージョンのリリース情報は、zSecure for z/VM® 資料の Web サイト (IBM zSecure Manager for RACF z/VM の IBM Knowledge Center) から入手できます。

- *IBM Security zSecure Manager for RACF z/VM:* インストールおよびデプロイメント・ガイド*, SC27-4363*

  この製品のインストール、構成、およびデプロイについての情報を提供します。

- *IBM Security zSecure Manager for RACF z/VM* ユーザー・リファレンス・マニュアル、*LC27-4364*

  この製品のインターフェースおよび RACF 管理と監査機能の使用法について説明します。本書には、CARLa コマンド言語と SELECT/LIST フィールドの参照情報が記載されています。また、トラブルシューティング・リソース、および zSecure Collect コンポーネントの使用方法も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure CARLa* コマンド・リファレンス*,* LC43-2107

  CARLa Auditing and Reporting Language (CARLa) についての、一般ユーザーと上級ユーザーの両方の参照情報が記載されています。CARLa は、zSecure を使用してセキュリティーの管理レポートおよび監査レポートを作成するためのプログラミング言語です。「*zSecure CARLa* コマンド・リファレンス」には、データの選択および zSecure レポートの作成のための NEWLIST タイプおよびフィールドに関する詳細情報も記載されています。この資料は、ライセンス交付を受けたユーザーのみが入手できます。

- *IBM Security zSecure Documentation CD,* LCD7-5373

  IBM Security zSecure Manager for RACF z/VM 資料を提供します。これには、ライセンス交付された製品資料とライセンス交付されていない製品資料が含まれています。

- *Program Directory for IBM zSecure Manager for RACF z/VM, GI11-7865*

  この資料の情報を効率的に利用するには、プログラム・ディレクトリーから取得できる一定の前提知識が必要です。「*Program Directory for IBM zSecure Manager for RACF z/VM*」は、製品のインストール、構成、およびデプロイを担当するシステム・プログラマーを対象としています。ソフトウェアのインストールに関連した資料と手順に関する情報が記載されています。この「Program Directory」はプロダクト・テープで提供されます。 IBM zSecure Manager for RACF z/VM の IBM Knowledge Center から最新のコピーをダウンロードすることもできます。

関連資料

このセクションでは、zSecure に関連する情報のタイトルおよびリンクを記載します。

参照先	対象
IBM Knowledge Center: IBM Security zSecure	zSecure のすべての非ライセンス資料。 特定のリリースに固有の情報、システム要件、非互換性などについては、目的のバージョンを選択し、「このリリースについて」を選択します。『新機能』および『リリース・ノート』を参照してください。
IBM Knowledge Center: z/OS	z/OS に関する情報。表 2 に、zSecure で最も役立つ資料をいくつか示します。
z/OS Security Server Documentation	リソース・アクセス管理機能 (RACF)、および zSecure Admin and Audit を使用して報告されるイベントのタイプに関する詳細情報。 RACF コマンド、および各種キーワードの意味については、「*z/OS Security Server RACF* コマンド言語解説書」および「*z/OS Security Server RACF* セキュリティー管理者のガイド」を参照してください。RACF によって記録される各種イベントの情報については、「*z/OS Security Server RACF* 監査担当者のガイド」を参照してください。
CA-ACF2 の資料	ACF2、zSecure Audit for ACF2 を使用して報告されるイベントのタイプに関する情報。

表 *2. zSecure* で使用するのに最も役立つ *z/OS* の資料

資料タイトル	資料番号
z/OS Communications Server: IP 構成解説書	SC27-3651
z/OS Integrated Security Services エンタープライズ識別マッピング *(EIM)* ガイドおよび解説書	SA88-7076
z/OS MVS™ プログラミング*:* 高水準言語向け呼び出し可能サービス	SA88-7103
z/OS MVS システム・コマンド	SA88-5490
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804
z/OS Security Server RACF 監査担当者のガイド	SA88-5718
z/OS Security Server RACF コマンド言語解説書	SA88-6226
z/OS Security Server RACF マクロおよびインターフェース	SC43-2673
z/OS Security Server RACF メッセージおよびコード	SA88-5839
z/OS Security Server RACF セキュリティー管理者のガイド	SA88-5804
z/OS Security Server RACF システム・プログラマーのガイド	SA88-7029
z/Architecture® 解説書	SA88-8773

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。この製品では、支援技術を使用して、インターフェースを聞き取ったりナビゲートしたりできます。また、マウスの代わりにキーボードを使用して、グラフィカル・ユーザー・インターフェースのすべての機能を操作することもできます。

技術研修

技術研修の情報については、IBM Training and Skills の Web サイト (www.ibm.com/training) を参照してください。

zSecure の技術研修の情報については、zSecure 公開 Wiki の zSecure Training ページを参照してください。

サポート情報

IBM サポートでは、コード関連の問題や通常の短期インストールまたは使用方法に関する質問にお答えします。IBM ソフトウェア・サポート・サイトへは、www.ibm.com/software/support/probsub.html から直接アクセスできます。

適切なセキュリティーの実践に関する注意事項

IT システム・セキュリティーには、企業内外からの不正アクセスからの保護、検出、および対処によってシステムおよび情報を保護することが求められます。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

第 1 章 概要

IBM Security zSecure Alert は、セキュリティー・サーバー (RACF) または CA-ACF2 で保護された z/OS システムのリアルタイム・モニターです。zSecure Alert は、システムのセキュリティーに関連する重要イベントの発生時に、アラートを発行します。これは IBM Security zSecure Suite の一部であり、zSecure Audit 用に開発された機能に基づいて構築されます。この章では、zSecure Alert の機能について、基本 z/OS コンポーネントやその他の監査、自動化、およびモニター・ソフトウェアとの関係の観点から説明します。

z/OS システムの主たる監査ログは、システム管理機能 (SMF) ログです。このログには、データ機能記憶管理サブシステム (DFSMS) のイベントが記録されます。例えば、データ・セットのオープン、z/OS UNIX System Services、ネットワーク機能 (VTAM、TCP/IP)、RMF (パフォーマンス・データ)、JES2/JES3 (ジョブ・アクティビティー、TSO セッション、開始タスク・アクティビティー、SYSIN/SYSOUT/NJE 処理)、外部セキュリティー・マネージャー (RACF、ACF2、TSS)、およびその他のアプリケーションなどです。データは、さまざまな多くの目的のために、SMF ログのポストプロセッシングによって抽出することができます。リソースの使用に基づく会計・請求処理、パフォーマンス分析、キャパシティー管理、セキュリティーのモニターなど、さまざまな用途に使用可能な商用ソフトウェアがあります。zSecure Audit は、SMF ログをイベント監査レポートの基本情報として使用して、RACF システムまたは ACF2 システムの z/OS システム・セキュリティーを分析します。

従来型の SMF レコードのポストプロセッシングには、1 つの大きな欠点があります。それは、イベントからポストプロセッシングまでの経過時間が最大 1 日に及ぶ場合がよくあることです。この欠点は、会計管理やキャパシティー管理では受け入れられる場合がある一方、セキュリティーの問題が生じる場合もあります。実際の侵入試行が進行中の場合、ユーザーは直ちに対処する必要があります。zSecure Alert は、そのジョブを実行するように設計されています。ユーザーはアプリケーションまたはネットワークの一部を非活動化するか、証跡が消えないうちに、侵入者のロケーションと ID に関するデータを収集することができます。また、特定のイベントの SMF への記録をオフにするようグローバル・セキュリティー設定が変更された場合も、それを検知できます。

zSecure Alert はシステム内でアクティブになり、SMF データが SMF ログに書き込まれる前に、その SMF データを取り込みます。これは、問題のあるイベントを数秒から数分でユーザーに通知することができます。さらに、zSecure Alert は WTO を取り込むこともできるため、ユーザーは、例えば、SMF ログが満杯になる瞬間に通知を受けることができます。通知は、以下の形式での送信が可能です。

- E メールとして送信する
- E メール・ベースの中継を介して、ポケットベルや携帯電話へのテキスト・メッセージとして送信する
- 自動化操作パッケージをトリガーするために使用できる WTO として送信する

- IBM Tivoli NetView for z/OS やネットワーク・コンソールなどで取得できる SNMP トラップとして送信する
- QRadar Unix syslog レシーバーに対して
- HPE Security ArcSight Unix syslog レシーバーに対して

また、zSecure Alert は拡張モニター・アラートもサポートします。SMF および WTO イベントによってトリガーされるイベント・ベースのアラートとは異なり、拡張モニター・アラートは状況がベースになります。これらのアラートは、システム設定およびセキュリティー設定の状況の変更によってトリガーされます。このタイプのアラートは、現行システムおよびセキュリティー設定のスナップショットと、以前のシステムおよびセキュリティー設定のスナップショットとの比較が基礎になっています。スナップショットは、定期的なユーザー指定インターバルで取得されます。新しいスナップショットが取得されるたびに、データが比較されます。何か大きな変更があった場合は常に、アラートを生成できます。このアラート・タイプでは、システム内で発生した変更を、たとえそれらの変更が SMF または WTO イベントを生成しない場合でも、ユーザーに通知できます。

zSecure Alert は、次の 2 つのコンポーネントで構成されています。

- 実際の取り込み、相関、およびアラート生成を実行する長寿命のアドレス・スペース (開始タスク)。
- 報告するイベントとレポートのフォーマットを指定するために使用できる ISPF インターフェース。

zSecure Alert には、 59 ページの『第 3 章 事前定義アラート』で説明されている一連の事前定義アラートが付属しています。ユーザーは、独自のアラート条件を指定することもできます。CARLa Auditing and Reporting Language (CARLa) のすべての機能とイベントの選択としきい値の適用における高い柔軟性に関する情報については、ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」および「*IBM Security zSecure: CARLa* コマンド・リファレンス」を参照してください。通常、インストール済み環境固有のデータ (ユーザー・データやセキュリティー・データベースに保持されているインストール・データの部分など) とキー・ベースの検索を組み込むことにより、CARLa を使用してアラートをカスタマイズすることもできます。

次の図は、zSecure Alert アーキテクチャーを表しています。

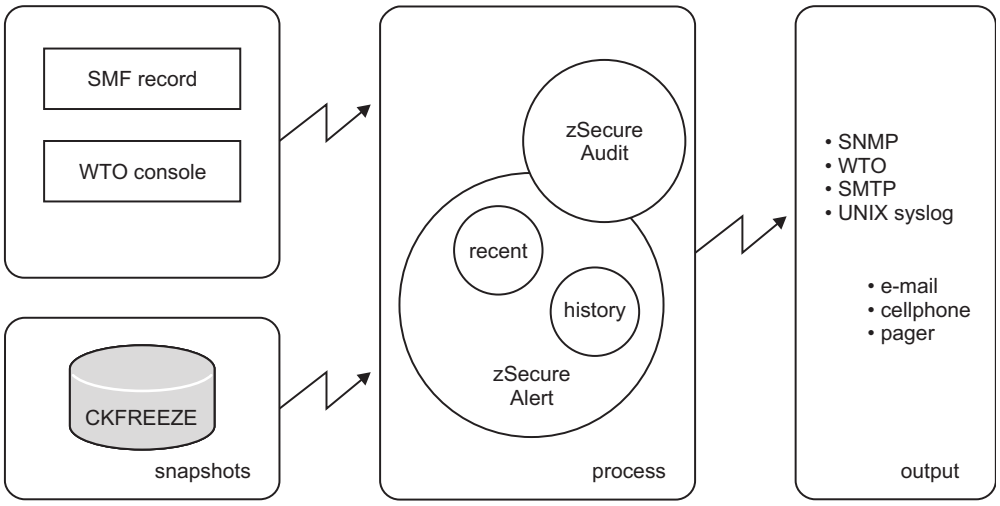

図 *1. zSecure Alert* アーキテクチャー

第 2 章 zSecure Alert 構成

この章では、zSecure Alert 構成プロセスについて説明します。ここでは、zSecure Alert を選択、構成、および活動化するさまざまなステップを詳しく説明します。

zSecure Alert 構成プロセスで使用される ISPF ユーザー・インターフェースには、独自の構成があります。この IBM Security zSecure 構成は、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」のポストインストール・タスクのセクションの説明に従って完了し、選択しておく必要があります。

zSecure Alert のアドレス・スペース操作については、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

概要

構成プロセスでは、お客様のインストール済み環境に固有の設定を指定する必要があります。アラート条件、結果のアラートを配信したい宛先、およびアラート・フォーマットを指定する必要があります。このすべての情報は、アラート構成に入っています。

本番環境に即時に影響を及ぼすことなく、構成を操作したい場合は、複数のアラート構成を作成できます。そうすることにより、複数の環境または異なる z/OS イメージに、さまざまな構成を簡単に設けることができます。それぞれの z/OS イメージ内で、一度にアクティブにできる構成は 1 つだけです。PlatinumPlex とも呼ばれる完全シスプレックス環境では、同じアラート構成をすべての z/OS イメージ上で使用できます。BronzePlex または GoldPlex とも呼ばれる部分的なシスプレックスの実装では、それぞれの z/OS イメージごとに異なるアラート構成を使用できます。アラート構成を完了した後、その構成を活動化することができます。

アラート構成には、2 つのタイプの情報が含まれています。

- 開始タスクに必要な一般的な設定 (データ・バッファーの数とサイズなど)。
- モニターしたいアラート条件と、結果のアラートを配信する方法の指定。

zSecure Alert では多数の事前定義アラート条件が用意されているため、これらのアラート条件はアラート・カテゴリーにグループ化されています。アラート条件はグループ化されているため、一度に複数のアラート条件を構成できます。以下のセクションでは、カテゴリー全体または個々のアラートのオプションを設定する方法について説明します。

アラート構成のほかに、*E* メール宛先 も作成できます。E メール宛先は、E メール・アドレスが入っているデータ・セットを参照します。E メール宛先は、データの解釈方法と、求める E メール・アドレスを見つける方法を指定します。アラート構成は、いくつかの作成済み E メール宛先を使用して、アラートを送信できる場所を指定します。

注: 携帯電話へのテキスト・メッセージも E メールで送信されます。このため、それらのメッセージにも E メール・アドレスが必要です。

図 2 は、zSecure Alert の構成の概要を示しています。zSecure Alert 構成データ・セットには、複数のアラート構成とゼロ個以上の E メール宛先定義が含まれています。それぞれの構成および宛先は、固有の名前を持っています。

注: アラート構成と E メール宛先の名前は、関係がなくてもかまいません。ただし、アラート構成と E メール宛先を容易に識別できるように、それらの用途が反映された短い簡略名を作成してください。

例の 図 2 では、アラート構成 ProdA にデフォルトの E メール宛先 TEST があります。いくつかのアラート・カテゴリーと個々のアラート条件には、指定変更する E メール宛先があります。それぞれの E メール宛先は、関連するデータ・セットのどの部分に、求める E メール・アドレスが含まれているかを定義します。E メール・アドレス・データ・セットは、zSecure Alert 構成データ・セットとは物理的に分離されています。

Alert Configuration data set

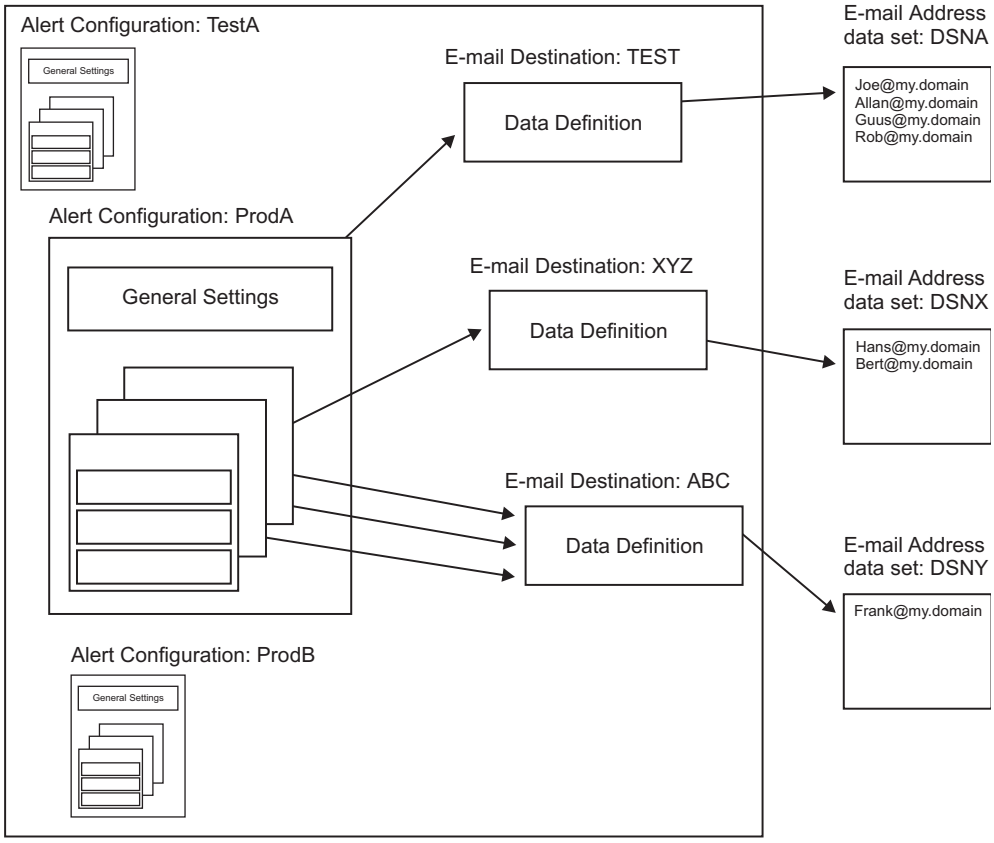

図 2. アラート構成データ・セット

アラートは、さまざまな宛先へ送信できます。zSecure Alert は、現時点で以下の宛先タイプをサポートしています。

- E メール
- テキスト・メッセージ

- WTO
- SNMP トラップ
- QRadar Unix syslog
- ArcSight CEF

アラート・フォーマットは、以下のように宛先タイプごとに指定されます。

- 製品に付属しているアラートには、共通の E メール・レイアウトがあります。このレイアウトについては、 64 ページの『標準 E メール・レイアウト』で説明しています。
- テキスト・メッセージ・フォーマットは、E メールからテキスト・メッセージへのゲートウェイで使用される E メール・フォーマットの短縮バージョンです。これは、携帯電話またはポケットベルに表示されます。
- WTO フォーマットについては、「*zSecure* メッセージ・ガイド」に説明があります。
- SNMP トラップ・フォーマットについては、 163 ページの『付録 A. SNMP 出力』に説明があります。
- QRadar Unix syslog レイアウトについては、 57 ページの『QRadar Unix syslog のレイアウト』を参照してください。
- HPE Security ArcSight CEF レイアウトについては、 57 ページの『ArcSight CEF のレイアウト』を参照してください。

提供される IBM アラートについて詳しくは、 59 ページの『第 3 章 事前定義アラート』を参照してください。独自のアラートを追加する場合は、必要に合わせて各種のフォーマットを調整できます。 39 ページの『インストール定義アラート』を参照してください。テキスト・メッセージングの構成について質問がある場合は、IBM ソフトウェア・サポートにお問い合わせください。

アラート活動化に関するガイドライン

zSecure Alert の構成における重要なステップの 1 つは、どのアラート条件をモニターするかと、アラートに特定の宛先が必要であるかどうかを決めることです。例えば、すべてのアラートを活動化すると、指定された受信者に E メールが大量に送信される可能性があります。最初に最も関心のあるアラート条件だけをモニターし、それらにどの程度のアテンションが必要かを調べることができます。

アラート条件の選択を支援するために、zSecure ではすべての事前定義アラートが分類されています。 59 ページの表 6を参照してください。

- クラス 1 には、ほとんどの場合、基本レベルまたは低レベルの警戒用にアクティブにされるアラート条件が含まれています。
- クラス 2 には、警戒レベルを中レベルに上げるために追加すべきと考えられる候補が含まれています。
- クラス 3 には、高レベルの警戒が必要な場合に活動化する必要があるアラート条件が含まれています。

この分類は、単なるグローバル・ガイドラインです。ある特定の警戒レベルに到達するようアラートを活動化するかどうかは、使用するセキュリティー・ポリシーと

ユーザーが防ぎたいアタックによって決まります。許可の悪用の可能性をモニターすることには、侵入試行の検出やサービス妨害アタックのアラートの受信とは別の要件があります。

例えば、アラート 1301 は、開始タスクが RACF システム上の STARTED クラスの包括的プロファイルからユーザー ID を取得したときにトリガーされます。アラート 2301 は、開始タスクが、ACF2 システム上の GSO OPTS 設定 DFTSTC によって指定されているデフォルトのログオン ID を使用した場合にトリガーされます。セキュリティー・ポリシーが、このアクションを禁止している場合もあり、その場合は、それをモニターできます。実際に、開始タスクの管理の手間を最小にするために、管理ポリシーを設定している場合もあります。その場合は、アラートを活動化すると混乱し、警戒レベルが悪化することになります。

拡張モニター・アラートを構成することもできます。拡張モニター・アラートは、システム内の変更の検出に基づいています。このアラートは、SMF または WTO イベント・レコードを伴わない変更のタイプに便利です。例えば、ある特定の z/OS 制御ブロックに対するストレージ内の更新は、適切な拡張モニター・アラートによって検出できます。そのような変更を SMF ベースまたは WTO ベースのアラートによって検出する必要はありません。拡張モニター・アラートは、単に何かが変更されたことだけを検出します。誰が変更したか、およびどのように変更されたかに関する詳細は、提供しません。

注**:** 拡張モニター・アラートを活動化する前に、zSecure Alert をインストールおよび構成するユーザーは、いくつかの構成タスクを実行する必要があります。構成タスクについて詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の zSecure Alert ポストインストール・タスクのセクションを参照してください。

実装フェーズのとき、特定のアラートを送信する代わりに、ファイルに書き込むことを検討してください。この手法により、生成されるアラート・メッセージの数が減り、受信者がすべてのメッセージを無視してしまう可能性が少なくなります。アラートのファイルへの書き込みについて詳しくは、 14 ページの『アラート構成: アラート構成の管理 (SE.A.A)』を参照してください。

構成のガイドラインとパフォーマンスへの影響

zSecure Alert 処理は、いくつかの部分から構成されています。開始時に指定したパラメーターは、zSecure Alert の全体的なパフォーマンスに影響し、それによって他のユーザーが受ける影響に関係します。各アラート構成の一般設定で指定されるパラメーターは、*intervals*、*buffer size*、および *number of buffers* です。

インターバル

関連するインターバルは、以下のとおりです。

- データ分析とアラートの生成を実行するための、レポート作成間隔
- 環境を再評価するための `stage 1` インターバル
- 「移動ウィンドウ」分析用の「平均」インターバル

デフォルトでは、データ分析は 60 秒ごとに行われます。リアルタイムのアラート・メッセージが必要でない場合、このインターバルを長くすることができます。より迅速な応答が必要な場合は、このインターバル時間を短くすることができます。

注: それぞれのレポート作成間隔ごとに、新しいバッファーが使用されます。『バッファー』で説明するバッファーの考慮事項は、これに関係しています。

stage-1 プリプロセッシング・サブタスクは、システム環境とユーザー属性に関する現行情報を取得します。このタスクは、デフォルトでは 1 時間ごとに実行されます。例えば、データ・セットやシステム制御ブロックなどに関する情報は、CKFREEZE データ・セット内に収集されます。このデータ・セットは、1 日に 1 回、指定された時刻にリフレッシュされます。ただし、オペレーター・コマンド MODIFY C2POLICE,COLLECT により、このタスクを zSecure Alert にディスパッチさせることもできます。

しきい値を持つ一部の「平均化」アラートでは、レポート作成間隔より長い時間枠を使用できます。これらのアラートの場合、例えばレポート作成間隔の 5 倍の時間にわたって、SMF レコードがヒストリー・バッファーに保持されます。この長期分析インターバルも、レポート作成の要件に応じて調整できます。

バッファー

zSecure Alert の構成に関するもう 1 つの重要な考慮事項は、メモリー内バッファーの使用状況です。zSecure Alert によって使用されるバッファー・スペースは、zSecure Alert 開始タスク・アドレス・スペースの専用領域内にある通常のページング可能ストレージです。これは、すべての面において、データ・セットを編集する TSO ユーザーの作業用ストレージに類似しています。バッファー・サイズを計算するガイドラインとして、以下のステップを実行できます。

注: 各ステップに付いている番号は単なる例示用です。システムの開始点としては使用しないでください。

1. SMF ダンプ・プログラムの出力を確認します。1 日に書き込まれた RACF SMF レコード数 (レコード・タイプ 80) または ACF2 SMF レコード数と、アカウンティング SMF レコード数 (レコード・タイプ 30) を合計します。

   例えば、ある小規模なシステムで、1 日に実行される平均的な MAN データ・セットの切り替えとダンプの回数が 5 回だとします。 IFASMFDP プログラムの出力には、RACF レコード数または ACF2 SMF レコード数について、50,000 32,000 69,000 49,000 および 27,000 が記録されているとします。この場合、平均的な 1 日に書き込まれた RACF レコードまたは ACF2 SMF レコードの合計数は 227,000 になります。SMF 30 レコードの数は、19000 15000 31000 23000 および 17000 でした。この場合、SMF 30 レコードの 1 日の合計数は 105,000 になります。
2. アラート・レポート作成間隔が 1 分 (デフォルト) であると仮定して、1 インターバル当たりのレコード数を計算します。

この例では、1 分当たり 227,000 / 1440 = 158 件の RACF レコードまたは ACF2 レコードと、105,000 / 1440 = 73 件の SMF-30 レコードが作成されます。

3. これらの SMF レコードの平均的なレコード長を知るため、SMF ダンプ・プログラムの出力を確認します。RACF レコードの場合は 250 - 300 バイト、ACF2 レコードの場合は 600 - 700 バイト、SMF-30 レコードの場合は 1000 - 1500 バイトになっているはずです。
4. 平均レコード数に平均レコード長を乗算すると、1 インターバル当たりの平均バッファー・サイズが分かります。

   この小規模システムの例では、結果は (158 * 274) + (73 * 1224) = 132,644 バイトになります。
5. 通常のシステム作業負荷の変動を考慮して、算出した平均値に 5 を掛け、最も近い切りのいい数値に切り上げると、*bufsize* パラメーターに最適の開始点が分かります。

   この例では、*bufsize* パラメーターの設定値には 700 KB が適切です。

最小バッファー・サイズが分かったら、次は必要なバッファーの数を知る必要があります。前述のように、最小バッファー数も長期のイベント分析に関連しています。例えば、ユーザーが 10 分間に 10 回を超える RACF ログオン違反を生成したときにアラートを生成したい場合、バッファーに保持するデータの量は 10 分以上を表している必要があります。1 つのバッファーには常に新しいイベントが書き込まれるため、平均化プロセスには使用できません。したがって、公式は次のようになります。

```
Numbufs > (AverageInterval / Interval) + 1
```

開始点として、この公式に基づくバッファー数の 2 倍の値を使用してください。したがって、「*Interval*」のデフォルト値 (60 秒) と「*AverageInterval*」のデフォルト値 (300 秒) を使用している場合は、最終的に 2*((300/60)+1) = 12 バッファーになります。

この手順で割り振られた追加のバッファーは、システム・アクティビティーが多い時間帯のオーバーフロー・バッファーとして使用することができます。通常、こうした時間帯が長く続くことはありません。上に示した計算例では、通常の量の 3 倍から 4 倍の SMF レコードを短時間 (1 分から 2 分) だけ取り込む必要がある場合を考慮しています。

上記の例では、「*Interval*」と「*AverageInterval*」にデフォルト値を使用することを想定しています。これらのパラメーターを決定するための主な基準は、レポート作成要件です。多くのインストール済み環境では、約 1 分のアラート応答時間が適切です。これは、E メールやその他のアラート配信方法の通常の応答時間においても適切な値です。「*AverageInterval*」の場合、5 分のインターバルを使用すれば、過度の誤ったアラームを回避するのに十分な長さです。また、アラートを必要とするほとんどの状態を検出するにも十分な時間です。

以下の値を、OPTION パラメーターと REPORT パラメーターの開始値として使用することができます。

Bufsize

RACF システムの場合は 1024 (=1 MB)、ACF2 システムの場合は 2028 (=2 MB)。

この値は、RACF レコードまたは ACF2 SMF レコードの平均の長さ、下記の指定されたインターバル、およびアクティビティーが多い時間帯の 1 秒当たり平均 40 件の RACF レコードまたは ACF2 SMF レコードに基づいています。

NumBufs

12

これは、長期のしきい値期間 (「*AverageInterval*」) と「*Interval*」期間に基づいています。また、6 個の追加オーバーフロー・バッファーも考慮しています。

Interval

60 秒

AverageInterval

300 秒

zSecure Alert の初期実行時に、DEBUG BUFFER 演算子または PARMLIB コマンドを使用して、メモリー内バッファーの使用状況をモニターします。その結果として、それぞれの「*Interval*」期間の終わりに、3 つのメッセージが生成されます。C2P0325 メッセージと C2P0326 メッセージは、SMF レコードと WTO メッセージで使用されたバッファー・スペースの量を示します。各インターバルの SMF レコードと WTO レコードのスペース量の合計が、ステップ 4 で算出したサイズに近い値になった場合、バッファー・スペースは適切な値になっているため、これ以上の変更は必要ありません。ステップ 5 では、予想される平均必要スペースの 5 倍のバッファー・サイズを指定しました。したがって、バッファーの約 20% 分だけ使用されることが予想されます。これにより、システム・アクティビティーの変動に備えて、十分なスペースが確保されます。

前の計算例で使用したものと同じ数値を使用すると、以下のメッセージが予想されます。

```
C2P0333I Buffer index is 09
C2P0325I Buffer stats: SMF(cnt,len) 00000214-00131928
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

これらのメッセージから、予想したレコード率がほぼ正しかったこと (予想した 231 レコードに対して 214 レコード)、およびレコードの平均サイズも大きさとして適切だったこと (予想した 132,644 に対して 131,928) を確認できます。

バッファー・デバッグ・メッセージを活動化すると、zSecure Alert は、オーバーフロー・バッファーが必要になるたびにメッセージも生成します。以下のメッセージ例を確認してください。

```
C2P0334I Extended buffer used
C2P0333I Buffer index is 02
C2P0325I Buffer stats: SMF(cnt,len) 00002728-01037650
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
C2P0333I Buffer index is 03
C2P0325I Buffer stats: SMF(cnt,len) 00000814-00307855
C2P0326I Buffer stats: WTO(cnt,len) 00000000-00000000
```

これらのメッセージは、通常のバッファー使用状況メッセージに追加して発行されます。メッセージで示されているバッファー「02」は、後続のバッファー (「03」) にオーバーフローしていたバッファーです。バッファー「03」は、それに続く通常の C2P0325 メッセージと C2P0326 メッセージで示されています。C2P0334 メッセージが 1 日に数回しか出力されない場合、バッファー・サイズは適切な値になっているため、これ以上の変更は必要ありません。通常の処理においては、C2P0334 メッセージが数回出力されることが予想されますが、これは、バッファーの不足や問題を示すものではありません。

上記に示したステップにより、過度なシステム・リソースを使用することなく、要件に合った最小バッファー・サイズとバッファー数を選択することができます。この方法では、必要に応じて増やすことができるように、小さなバッファーから開始します。代わりの方法として、多数の大きなバッファーから開始し、バッファーの統計メッセージをモニターすることもできます。テストを数回実行したら、バッファー・サイズの削減可能な量を判断することができます。

バッファーを割り振る場合は、zSecure Alert 開始タスク JCL で指定される仮想ストレージの量も考慮する必要があります。JCL 内の領域パラメーターは、*bufsize* と *numbufs* によって指定された合計バッファー・スペースより、少なくとも 64 MB 分だけ大きくする必要があります。

zSecure Alert の構成

このタスクについて

zSecure Alert 構成プロセスには、zSecure Admin and Audit メニューのオプション **SE.A** から実行するいくつかのステップがあります。このオプションを選択すると、次のパネルを表示できます。

```
 Menu  Options  Info  Commands  Setup         StartPanel
--------------------------------------------------------------------------------
                        zSecure Suite - Setup Alert
Option ===> ____________________________________________________________________

A    Alert           Select and customize alerts
E    E-mail          Configure e-mail address lists
P    PCI             Configure PCI data sets, userids, and groups
S    Sensitive       Configure sensitive resources, userids, and groups
```

図 *3. zSecure Suite: zSecure Alert* を構成するための「*Setup Alert*」パネル

zSecure Alert 構成アプリケーションは、以下のオプションを提供します。

- アラート条件と結果のアラートの宛先を構成するには、「アラート」を使用します。
- アラート構成内でハードコーディングされた E メール・アドレスを使用しないために、外部データ・セットから E メール・アドレスを取得する方法を定義するには、「**E** メール」を使用します。
- PCI PAN データ・セットおよび PCI AUTH データ・セット、およびこれらのデータ・セットにアクセスできる特権ユーザーおよびグループを定義するには、「**PCI**」 を使用します。

- 機密リソース、およびそれらのリソースにアクセスできる特権ユーザーおよびグループを定義するには、「機密」を使用します。

手順

zSecure Alert を構成するには、以下のステップを実行します。

1. オプション: オプション SE.A.E を使用して、ハードコーディングされた E メール・アドレスの指定を避けるために、アラート構成で使用する E メール宛先を少なくとも 1 つ定義します。注 1 を参照してください。
2. オプション: オプション SE.A.P を使用して、RACF アラート 1209、1210、1211、および ACF2 アラート 2209、2210、2211 用に、PCI PAN データ・セットと PCI AUTH データ・セット、およびこれらのデータ・セットへのアクセスが許可される特権ユーザーとグループを定義します。
3. オプション: オプション SE.A.S を使用して、RACF アラート 1204、1212、1213、および ACF2 アラート 2204、2212、2213 用に、機密リソース、およびこのリソースへのアクセスが許可される特権ユーザーとグループを定義します。
4. オプション SE.A.A を使用して、出荷された製品に含まれているデフォルトのアラート構成 (C2PDFL) をコピーします。注 2 を参照してください。
5. 一般設定を編集します。
6. アラート構成レベルでアラート宛先を指定します。
7. モニターしたいアラート条件を選択します。このプロセスの間、宛先をアラート・カテゴリー・レベルまたは個々のアラート・レベルで指定変更できます。
8. アラート構成を検査します。注 3 を参照してください。
9. アラート構成をリフレッシュまたは活動化します。注 3 を参照してください。

タスクの結果

注**:**

1. 1 のステップを完了した後、他のステップで E メール宛先を使用できます。しかし、本製品を初めて使用する場合は、ステップ 1 をスキップできます。その場合は E メール宛先を使用できませんが、それでも E メール・アドレスをアラート構成内でハードコーディングすることができます。この方法により、アラートのモニターと作成についての経験を積むことができます。zSecure Alert を実装するその後のステージで、構成プロセスを再度行うことができます。その時点で、必要な E メール宛先を追加し、それらを使用するようにアラート構成を変更できます。
2. ステップ 4 が含まれている理由は、デフォルトのアラート構成はユーザー独自の構成のテンプレートとして使用されることが想定されているためです。また、その理由から、必ずしもすべての調整がデフォルトの構成で使用されるわけではありません。アラート構成の作成に「コピー」コマンドを使用することの副次効果として、構成アプリケーションで、ユーザーに必要なすべての構成ステップが自動的に表示されます。したがって、ステップを追跡する必要はありませんが、必要なフィールドに入力する必要があります。

3. ステップ 8 (13 ページ) と 9 (13 ページ) は、どちらも、更新されたアラート構成を zSecure Alert アドレス・スペースで使用可能にするために必要です。場合によっては、これらのトランザクションを再実行する必要があります。それは、以下のような場合です。
   - より高いリリースの ISPF インターフェースを一時的に使用した後、フォールバックを実行する必要が生じた場合は、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」のバックアウトとアップグレードに関するセクションを参照してください。
   - IBM Security zSecure の特定のコンポーネントに対して保守が行われた場合もあります。その場合は、保守のインストーラーから通知を受ける必要があります。

以下のセクションでは、タスクの実行、保守を容易にするための E メール宛先のセットアップ、および独自のアラート定義の追加を行う方法について説明します。

アラート構成: アラート構成の管理 (SE.A.A)

このタスクについて

アラート構成を管理するには、オプション **SE.A.A (**アラート**)**を使用します。アラート構成は、モニターしたいアラート条件と、アラートの必要な送信先および送信方法を指定します。また、zSecure Alert 開始タスクに必要な一般的なパラメーターも含んでいます。 z/OS イメージ上で一度にアクティブにできるアラート構成は 1 つだけです。アラート条件、宛先、およびパラメーターを設定した後、アラート構成を検査する必要があります。検査プロセスは、構成に一貫性があり、使用できなくなるようなエラーが含まれていないことを確認します。検査が済んだアラート構成は、アクティブにすることができます。

注**:** アラート構成に加えた変更は、オプション **SE.A.A** を終了するまで永続的には保存されません。

オプション **SE.A.A (**アラート**)** を選択すると、次のパネルが表示されます。

```
   Menu  Options  Info  Commands  Setup
--------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert     Row 1 from 2
 Command ===> ____________________________________________          Scroll ===> CSR

Managing alert configurations
Line commands are available depending on the configuration stage: C(opy),
D(elete), I(nsert), E(dit), W(Who/Where), S(elect), V(erify), F(Refresh),
B(rowse)

------------------------------------------------------------------ Configuration steps ---
    Name      Description                                          Set Des Sel Ver Ref  Act
_   C2PDFL    zSecure Alert default alert configurati              Req Req Req Req Req  _
--------------------------------------------------------------------------------
_   PRODA1    Alert config for production image A1                 Req Req Req Req Req  _
--------------------------------------------------------------------------------
 ****************************** Bottom of data ********************************
```

図 *4.* 「*Setup Alert*」パネル*: zSecure Alert* の構成

このパネルは、既存のアラート構成の概要と、構成がどこまで進行したかを示します。「Configuration steps」には、ステップが完了している場合は「OK」が、アラート構成にその特定のステップが必要であれば「Req」が表示されます。「Act」列

には、そのシステム上で構成が現在アクティブであるかどうかが示される場合があります。ユーザーは、この表示画面ですべての構成ステップを実行する必要があります。このパネルには、以下のフィールドが表示されます。

Name アラート構成の名前。アラート構成名は、固有で、最大長が 6 文字でなければなりません。C2P の接頭部を持つアラート構成名は、IBM Security zSecure 用に予約されています。この名前の接頭部を持ついくつかの PDS/E メンバーは、「検査」(**V**) および「リフレッシュ」(**F**) 行コマンドによって作成されます。これらのステップで生成されるメンバーについて詳しくは、 29 ページの『アラート構成: アラート構成の検査』を参照してください。

Description
アラート構成の説明。

Configuration steps
このフィールド・グループは、構成を完了するために必要なステップと、それらのステップの順序を示しています。対応する行コマンドは、前のステップが完了した場合にのみ使用できます。初期には、ステップは「**Req**」として示されます。そのステップが正常に完了すると、表示は「**OK**」になります。以下のステップを実行します。

1. **Set:** zSecure Alert パラメーターを指定します。対応する行コマンドは **E**、つまり、一般的なアラート構成設定の編集です。
2. **Des:** このアラート構成で選択されたすべてのアラート条件について、デフォルトのアラート宛先を設定します。宛先は、E メール・アドレス、テキスト・メッセージ/携帯電話の受信者、SNMP アドレス、WTO メッセージ、QRadar Unix syslog 、および ArcSight CEF のいずれでもかまいません。対応する行コマンドは **W**、つまり、アラートを受信できる人またはアラートの送信先の指定です。
3. **Sel:** モニターしたいアラート条件を選択し、オプションとして、アラート宛先をアラート・カテゴリーまたは個々のアラート・レベルで指定します。独自のアラート条件を指定することもできます。対応する行コマンドは **S**、つまり、このアラート構成のアラートとその宛先の指定です。
4. **Ver:** 前記のすべてのステップを終了した後、アラート構成にエラーがないかどうか検査する必要があります。対応する行コマンドは **V**、つまり、アラート構成の検査です。
5. **Ref:** 検査が正常に完了した後、検査が済んだアラート構成を実動に配置するかどうかを決めることができます。「リフレッシュ」コマンドは、いくつかの PDS/E メンバーを既存の実動メンバーの上にコピーします。さらに、リフレッシュ・コマンドは、そのシステム内でアクティブであると思われる zSecure Alert アドレス・スペースに対しても発行されます。このコマンドにより、システムは構成メンバーを再度読み取ります。 対応する行コマンドは **F**、つまり、実動メンバーのリフレッシュです。

   注**:** 開始タスク JCL 内の PARMLIB DD ステートメントは、構成データ・セットとこのアラート構成をポイントしている必要があります。

6. **Act:** この列が「Yes」の場合、このアラート構成はこの z/OS イメージ上のアクティブ構成です。その逆は、必ずしも真ではありません。なぜなら、その情報を取り出すために必要な z/OS MODIFY コマンドを発行する十分な権限を、ユーザーが持っていない場合もあるからです (160 ページの『権限の問題』を参照)。アクティブな開始タスクの名前がアラート構成で指定された名前に一致しない場合、「**Act**」列はブランクになります。

アラート構成概要パネルは、すべてのアラート構成管理機能を備えています。次の表は、使用できる行コマンドを説明したものです。一部の行コマンドは、その前の構成ステップが完了した後でのみ使用できます。現在許可されている行コマンドを表示するには、スラッシュ (/) を入力します。

表 3. アラート構成管理の行コマンド

C	アラート構成をコピーします。このアクションにより、すべてのフィールドを備えた一般設定パネルを表示できます。これらのフィールドは、選択したアラート構成からコピーされます。ただし、「名前」フィールドは除き、それはアラート構成ごとに固有でなければなりません。
I	新しいアラート構成を挿入します。このアクションにより、すべてのフィールドがブランクになった一般設定パネルが表示されます。必要なすべてのフィールドに入力すると、新しいアラート構成が追加されます。
B	このアラート構成の一般設定をブラウズします。
E	このアラート構成の一般設定を編集します。対応する構成ステップは、「**Set**」です。
D	選択されたアラート構成を削除します。
W	アラート宛先をアラート構成レベルで設定します。宛先は、E メール・アドレス、テキスト・メッセージ/携帯電話の宛先、SNMP アドレス、WTO メッセージ、QRadar Unix syslog 、および ArcSight CEF のいずれでもかまいません。対応する構成ステップは、「**Des**」です。
S	モニターしたいアラート条件を選択し、オプションとして、アラート宛先をアラート・カテゴリーまたは個々のアラート・レベルで指定します。独自のアラート条件を作成することもできます。対応する構成ステップは、「**Sel**」です。
V	アラート構成にエラーがないかどうか検査します。対応する構成ステップは、「**Ver**」です。
F	実動メンバーをリフレッシュします。検査が済んだメンバーは、実動メンバーへコピーされます。このシステム上でアドレス・スペースがアクティブの場合は、その実動メンバーを再処理するためにコマンドが発行されます。これは、開始タスク JCL がこのアラート構成を使用する場合にのみ有効です。対応する構成ステップは、「**Ref**」です。

アラート構成: 一般設定の指定

一般設定パネルは、アラート構成概要パネルで **E** (編集)、**C** (コピー)、**I** (挿入) のいずれかの行コマンドを使用したときに表示されます。この 3 つのアクションの主な違いは、事前にパネルに表示される情報の量です。

- 「編集」する場合は、選択した構成に関するすべての現行情報が表示されます。
- 「コピー」する場合は、「名前」以外のすべての情報がコピー元の構成から取得されます。

- 「挿入」する場合は、デフォルト設定だけが入力されています。構成を有効なものにするには、追加情報を入力する必要があります。

次の画面は、「コピー」コマンドを使用してデフォルトのアラート構成 (C2PDFL) をコピーするときに表示されるパネル・イメージを示しています。

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert
Command ===> ____________________________________________________________

Name  . . . . . . . . . AHJB                    (also report member)
Description . . . . . . zSecure Alert default alert configuration

You may scroll forward/backward to view all parameters

SMTP node . . . . . . . ________
SMTP sysout . . . . . . B
SMTP writer . . . . . . SMTP
SMTP atsign . . . . . . @

Interval  . . . . . . . 60                      (in seconds)
Environment refresh . . 60                      (in minutes)
Average . . . . . . . . 300                     (in seconds)
Buffer size . . . . . . 10    MB                (in kilobytes/megabytes)
Number of buffers . . . 10

RACF database . . . . . BACKUP                  (PRIMARY or BACKUP)
Collect started task    C2PCOLL
CKFREEZE data set . . . CRMA.T.DATA.SP390.C2POLICE.CKFREEZE
CKFREEZE Collect time   0100                    (Time of day in hhmm)

Extended Monitoring . . y                       (Y/N)
Snapshot retention  . . 12                      (Number of hours, 1-99)
_  Suppress copy of UNIX syslog message in SYSPRRPT


Enter / to view/edit the global CARLa skeleton
_  Skeleton        C2PSGLOB
```

図 *5.* 「*Setup Alert*」パネル*:* デフォルトのアラート構成のコピー

このパネルで、関連情報を指定する必要があります。フィールドに入力したら、END キー (PF3) を使用して、これらの設定を保存することができます。 「コピー」または「挿入」行コマンドを使用してこのパネルを表示した場合は、END を押すと自動的に構成プロセスの次のステップに進みます。それ以外の場合は、アラート構成概要パネルに戻ることができます。

注**:** このパネルを使用する前に、 8 ページの『構成のガイドラインとパフォーマンスへの影響』を参照してください。

一般設定パネルには、以下のフィールドがあります。

Name アラート構成の名前。このフィールドは必須です。Nameを参照してください。

Description
アラート構成の説明。このフィールドは必須です。

SMTP node
E メールが最終処理のために経路指定される先の JES 宛先を指定します。この設定は、初期には SETUP OUTPUT から取得されます。(このオプションは、zSecure Admin and Audit インターフェースの一部です。) SETUP

OUTPUT で指定されなかった場合は、SMTPNODE の値を取得するために、REXX SMTPNOTE の検索が実行されます。 SMTP サーバーがご使用のローカル・システムで実行されている場合は、「LOCAL」を指定するか、このフィールドをブランクのままにします。それ以外の場合は、NJE NODE 名を指定するか、正しい設定についてシステム・プログラマーに問い合わせてください。

SMTP sysout
E メールの SMTP 出力処理に使用する JES 出力クラスを指定します。この設定は、初期には SETUP OUTPUT から取得されます。指定されなかった場合は、sysout クラス B のデフォルトが使用されます。このフィールドは必須です。正しい設定については、システム・プログラマーに問い合わせてください。

SMTP writer
E メールの SYSOUT データ・セットを選択する際に SMTP で使用する名前を指定します。外部書き出しプログラムの名前は、SMTP アドレス・スペースの名前と同じです。この設定は、初期には SETUP OUTPUT から取得されます。SETUP OUTPUT で指定されなかった場合は、SMTPJOB の値を取得するために、REXX SMTPNOTE の検索が実行されます。このフィールドは必須です。正しい設定については、システム・プログラマーに問い合わせてください。

SMTP atsign
SMTP がデフォルトのコード・ページ 1047 (16 進値 X'7C') で、Eメール・アドレスのドメインの始まりを示すために @ の代わりに使用する文字を指定します。このパラメーターは、SMTP サーバーまたは CSSMTP サーバーの ATSIGN オプションに一致していなければなりません。**SMTP atsign** を指定しない場合は、デフォルトの @ が使用されます。

Interval
レポート作成間隔を指定します。各インターバルごとに、zSecure Alert は収集した WTO および SMF レコードを分析し、アラート・メッセージを生成します。このインターバルは、メッセージを送信できる頻度も定義します。受信者は、サブスクライブしたすべてのアラートに関するメッセージを、そのアラートがインターバル中に 1 回以上トリガーされている場合に取得します。デフォルトは 60 秒です。

「**Interval**」は、REPORT オプション INTERVAL に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドのセクションで「**Interval**」フィールドの説明を参照してください。.

Environment refresh
zSecure Alert が環境依存の選択基準を生成する (つまり、RACF データベースおよび CKFREEZE ファイルを分析し、現在の RACF データベースの内容に基づいてアラート定義をリフレッシュする) 間隔を指定します。デフォルトは 60 分です。

Environment refresh は、REPORT オプションの STAGE1INTERVAL に対応しています。「*IBM Security zSecure CARLa-Driven Components:* イン

ストールおよびデプロイメント・ガイド」の REPORT コマンドのセクションで「**PreProcessInterval**」または「**Stage1Interval**」フィールドの説明を参照してください。.

Average

zSecure Alert が、移動ウィンドウ 分析のために、特定のイベントの発生の平均を求める際の対象期間を秒単位で指定します。デフォルトは 300、つまり 5 分です。「**Average**」、「**Interval**」、および「**Number of buffers**」の間の関係については、「**Number of buffers**」フィールドの説明を参照してください。

「**Average**」は、REPORT オプション AVERAGEINTERVAL に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドのセクションで「**AverageInterval**」フィールドの説明を参照してください。.

Buffer size

インターバル期間中に WTO レコードおよび SMF レコードを保管するために使用されるメモリー内の各バッファーのサイズを、キロバイト単位またはメガバイト単位で指定します。1 から 16384 キロバイトまたは 1 から 1024 メガバイトを指定できます。デフォルトは 1024 です。

あるインターバル中、1 つのバッファーでは小さすぎることが分かった場合、zSecure Alert は未使用のバッファーに切り替えようとします。空きバッファーがない場合は、最も古い情報が入っているバッファーに現行情報がオーバーレイされます。バッファーのサイズと数が不十分な場合は、データ損失エラー・メッセージがログに記録されます。

Buffer size は、OPTION BUFSIZE または BUFSIZEMB に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の OPTION コマンドのセクションで「**Bufsize**」フィールドおよび「**BufsizeMB**」フィールドの説明を参照してください。.

Number of buffers

割り振るバッファーの数を指定します。この数値は 2 から 32 までででなければなりません。 この数値は、Average / Interval + 1 個のバッファーを格納するのに十分な数でなければなりません。イベント着信率のピークを処理できるよう、最小値を超える余分なバッファーを割り振っておく必要があります。余分なバッファーは、バッファー・オーバーフローが起きた場合に使用できます。

「**Number of buffers**」は、OPTION NUMBUFS に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の OPTION コマンドのセクションで「**Numbufs**」フィールドの説明を参照してください。.

Security database

環境に依存する選択基準を生成するために、PRIMARY または BACKUP セキュリティー・データベースを使用するかどうかを指定します。ユーザーが最後にアクセスした時間など、特定の統計情報を使用する独自のアラートを作成する場合、PRIMARY データベースを使用しなければならないことがあります。それ以外の場合、BACKUP データベースを使用すると、他のシ

ステム・コンポーネントに対する影響が最小になり、事前に定義されたアラートで使用されるすべての情報が提供されます。

Collect started task
zSecure Alert アドレス・スペースによって「**CKFREEZE Collect time**」に開始された開始タスクの名前を指定します。この開始タスクは、プログラム CKFCOLL を呼び出して環境データを収集します。

「**Collect started task**」は、OPTION COLLECTSTCNAME に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の OPTION コマンドのセクションで「**CollectSTCName**」フィールドの説明を参照してください。.

CKFREEZE data set
環境データが入っている CKFREEZE データ・セットの名前を指定します。

注**:** zSecure Alert では、ユーザーがここで指定するデータ・セット名が「**Collect started task**」の JCL で指定されている名前と一致していなくてもかまいません。その場合、ユーザーがここで指定した名前は、単にアラート構成の「検査」処理のときにのみ使用されます。このデータ・セットは、「**Collect started task**」で指定されている場合、毎日「**CKFREEZE Collect time**」にリフレッシュされます。

CKFREEZE Collect time
「Collect started task」を開始する必要がある時刻を指定します。値 0000 は、zSecure Collect for z/OS 開始タスクを決して開始してはならないことを示すために使用します。

「**CKFREEZE Collect time**」は、OPTION COLLECTTIME に対応します。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の OPTION コマンドのセクションで「**CollectTime**」フィールドの説明を参照してください。.

Extended Monitoring
このフィールドは、拡張モニター・プロセスをアクティブにするかどうかを決定します。「YES」を指定した場合、拡張モニターは活動化されます。その結果、「**Environment refresh**」フィールドに指定された間隔でシステム・スナップショットが取得され、CKFREEZE データ・セットに書き込まれます。このオプションは、拡張モニター・アラートが選択されている場合にのみ有効です。拡張モニター・アラートが選択されていない場合は、検査プロセスで警告メッセージが発行されます。

Snapshot retention
拡張モニターのスナップショット・データ・セットの保存期間を指定します。指定した期間より古いスナップショット・データ・セットは、自動的に削除されます。この保存期間は、時間単位で指定します。この値は、1 から 99 の間の範囲 (1 と 99 を含む) でなければなりません。デフォルト値は 24 時間です。スナップショット・データ・セットを保存する主な理由は、生成されたアラートの詳細を分析できることにあります。

Suppress copy of UNIX syslog message in SYSPRRPT
選択すると、Unix syslog に送信されたメッセージが SYSPRRPT 出力にもコピーされません。これは、QRadar Unix syslog と ArcSight CEF の両方のメッセージに影響します。

Skeleton
このメンバーは、ALLOCATE、DEFTYPE、および DEFINE ステートメントなどのグローバルな CARLa ステートメントを含んでいます。独自のアラート条件を定義した場合は、このオプションが必要です。 39 ページの『インストール定義アラート』を参照してください。ただし、通常は、提供される C2PSGLOB メンバーを使用します。

アラート構成: アラート宛先の指定

アラート構成概要パネルまたはいずれかのアラート選択パネルで、**W** (人/場所) 行コマンドからアラート宛先パネルを選択できます。このパネルでは、アラートの送信先にしたい場所を指定できます。**W** 行コマンドを使用して、以下のアラート・タイプのそれぞれに対して、アラート宛先を指定できます。

- アラート構成
- アラート・カテゴリー
- 個々のアラート

このパネルは、アラート構成概要パネルで「コピー」または「挿入」機能を使用すれば、自動的に表示できます。このパネルは、END キー (PF3) を使用して一般設定を終了した場合に表示されます。

このパネルで複数の宛先タイプを選択することにより、アラート・メッセージを複数の宛先タイプに送信できます。 それぞれの宛先タイプは、独自の宛先を持つことができます。

すべての宛先タイプを選択した場合、表示されるパネルは次の画面のようになります。

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                      zSecure Suite - Setup - Alert
Command ===> ____________________________________________________________

You can scroll forward/backward to view all recipient types
Select the destination for alert configuration C2PDFL
/  E-mail
   _  Redirect e-mails to C2RSMTP DD

   Specify e-mail recipient(s)
   From . . . . . &jobname at &system <mbox@domain>_______________

   Mail to  . . . . . ____________________________________________________
   (You may specify : to receive a list of defined recipients :setname.fields)

   CC . . . . . ____________________________________________________
   BCC  . . . . . ____________________________________________________
   Reply to . . . . . ____________________________________________________
   Output format  . . 1  1. Normal (MIME/HTML)
                         2. Plain text (formatting may be lost)
       Font size  . . . . _  (number in range 1-7)

/  Text message to cell phone
   _  Redirect text messages to C2RSMTP DD

   Specify text message/cell phone recipient
   From . . . . . &jobname at &system <mbox@domain>_______________

   Phone@gateway  . . ____________________________________________________
   (You may specify : to receive a list of defined recipients :setname.fields)

   Reply to . . . . . ____________________________________________________

/  SNMP
   _  Redirect SNMP traps to C2RSNMP DD

   Specify SNMP receiver address(es)
   Destination (UDP)   ____________________________________________________

/  QRadar Unix syslog
  _  Redirect messages to C2RSYSLG DD

    Specify QRadar Unix syslog receiver address(es)
    Destination (UDP)  ____________________________________________________
    Destination (TCP)  ____________________________________________________

/  ArcSight CEF via syslog
  _  Redirect messages to C2RSYSLG DD

    Specify CEF receiver address(es)
    Destination (UDP)  ____________________________________________________
    Destination (TCP)  ____________________________________________________

/  WTO
   _  Redirect WTOs to C2RWTO DD

_  Reset all existing destination settings for this Alert Configuration
```

図 *6.* 「*Setup Alert*」パネル*:* 宛先タイプの指定

画面サイズが 24 x 80 の場合、すべてのフィールドを表示するにはスクロールダウンする必要があります。

このパネルの「**Mail to**」および「**Phone@gateway**」フィールドは、いくつかのフォーマットの E メール・アドレスを受け入れます。指定できる E メール・アドレスは、以下のとおりです。

- コンマ (,) で区切った 1 つ以上の auditor@mydomain.com 形式の E メール・アドレス。

- E メール・アドレスがデータ・セットに含まれており、そのデータ・セットにそれ以外のデータも行番号も含まれていない場合は、*//data_set_name* を使用できます。
- E メール宛先を定義済みである場合は、

  :destination-name.field-name を使用してそれを参照できます。

E メール宛先の名前、または使用したフィールド名が分からない場合は、単一のコロン (:) を使用して情報を要求できます。定義された E メール宛先、およびそれらの定義されたフィールドの選択リストが入ったパネルが表示されます。

以下のフィールドは、**Email** セクションに表示されます。

Email
アラートを E メールとして送信します。

Write emails to C2RSMTP DD
このフィールドと「**Email**」の両方にタグが付いている場合、生成された E メールは送信されず、C2RSMTP DD に書き込まれます。このオプションは、独自のアラート条件を定義するときに使用できます。生成されるアラートの数が不確かな場合は、このオプションにより、意図した受信者にアラートの E メールが殺到しないようにすることができます。

From
「送信元」の E メール・アドレス。このアドレスは、「From:」ヘッダーに追加されます。

変数 &jobname および &system、つまり SMF システム ID をフレーズの一部として使用できますが、引用符の中で使用することはできません。例えば、&jobname を &system<*mbox@domain*> で使用します。これらの変数には、大/小文字の区別があります。&SYSTEM、&system、および &System は許可されますが、それ以外の変数は許可されません。

Mail to
宛先の E メール・アドレスを入力します。E メール・アドレスの指定について詳しくは、このセクションで前に述べた「Mail to」および「電話」の指定に関する情報を参照してください。

CC E メールのコピーを受信する受信者の E メール・アドレスを、コンマで区切って入力します。

BCC E メールの隠しカーボン・コピーを受信する受信者の E メール・アドレスを、コンマで区切って入力します。これらのアドレスは、宛先リストには表示されません。

Reply to
E メールの「Reply-To」ヘッダーに設定されるアドレスまたはアドレスのリスト。

出力フォーマット
このオプションは、レポートのフォーマット設定に使用する方式を指定するために使用できます。サポートされるオプションは、次のとおりです。

Normal
制限付き HTML エンコードの MIME/HTML E メールを使用します。

Plain text
特殊なフォーマット設定は行いません。これは、MIME/HTML エンコードが行われないことを意味します。

Font size
これは、E メールに使用する HTML フォント・サイズを設定します。デフォルトは、1 です。 HTML フォント・サイズは、1 から 7 の範囲の数値です。これは、ブラウザーのデフォルト・フォントが 12 ポイントに設定されている場合、8、10、12、14、18、24、26 のポイント・サイズに対応します。ユーザーは、これを変更できます。

以下のフィールドは、テキスト・メッセージ・セクションに表示されます。

Text message to cell phone
アラートをテキスト・メッセージとして携帯電話またはポケットベルに送信します。

Write text messages to C2RSMTP DD
このフィールドと「**Text message to cell phone**」の両方にタグが付いている場合、生成されたテキスト・メッセージは送信されず、C2RSMTP DD に書き込まれます。このオプションは、独自のアラート条件を定義するときに使用できます。生成されるアラートの数が不確かな場合は、このオプションにより、意図した受信者にアラートが殺到しないようにすることができます。

From, Reply to
これらのフィールドは、E メール・セクションの「送信元」および「**Reply to**」と類似のフィールドです。

Phone@gateway
<phone number>@<gateway> としての電話またはテキスト・ページャーのアドレス。 「Mail to」のフィールド説明も参照してください。

以下のフィールドは、SNMP セクションに表示されます。

SNMP
アラートを SNMP トラップとして送信します。SNMP フィールドの宛先を指定する必要があります。

Write SNMP traps to C2RSNMP DD
このフィールドと「**SNMP**」の両方にタグが付いている場合、生成された SNMP トラップは送信されず、C2RSNMP DD に記号形式で書き込まれます。つまり、実際の ASCII トラップでなく、`sortlist` 出力が書き込まれます。このフィールドは、テスト用です。

Addresses
SNMP を選択した場合は、このフィールドを使用して SNMP トラップの送信先を指定する必要があります。宛先は、名前 (DNS によって検索された名前)、IP アドレス、またはコンマで区切ったリストでもかまいません。それぞれの宛先の直後に、コロンと 10 進形式のポート番号を続けることができます。

以下のフィールドは、QRadar Unix syslog セクションに表示されます。

QRadar Unix syslog
Log Event Extended Format (LEEF) で Unix syslog レシーバーにアラートを送信します (IBM QRadar SIEM など)。

Write messages to C2RSYSLG DD
このフィールドと「QRadar Unix syslog 」の両方を選択した場合、生成されたアラート・メッセージは QRadar Unix syslog 宛先へ送信されず、C2RSYSLG DD に書き込まれます。同じ DD が ArcSight CEF に使用されます。このフィールドは、テスト用です。これは、QRadar Unix syslog と ArcSight CEF の両方に影響します。

Destination
「QRadar Unix syslog 」を選択した場合は、このフィールドを使用してアラート・メッセージの送信先を指定する必要があります。zSecure Alert は、User Datagram Protocol (UDP) と伝送制御プロトコル (TCP) を介してメッセージの転送をサポートします。 UDP では、メッセージが失われる可能性があります。一方、TCP では、SYSLOG レシーバーが非常に低速である場合にすべてのアラートの処理が遅延する可能性があります。両方のオプションは同時に使用できます。宛先は、名前 (DNS によって検索された名前)、IP アドレス、またはコンマで区切ったリストでもかまいません。それぞれの宛先の直後に、コロンと 10 進形式のポート番号を続けることができます。

以下のフィールドは、ArcSight CEF セクションに表示されます。

ArcSight CEF
共通イベント・フォーマット (CEF) メッセージを使用して、アラートを HPE Security ArcSight CEF サーバーに送信します。

Write messages to C2RSYSLG DD
このフィールドと「ArcSight CEF」の両方を選択した場合、生成されたアラート・メッセージは ArcSight CEF 宛先へ送信されず、C2RSYSLG DD に書き込まれます。同じ DD が QRadar Unix syslog に使用されます。このフィールドは、テスト用です。これは、QRadar Unix syslog と ArcSight CEF の両方に影響します。

Destination
「ArcSight CEF」を選択した場合は、このフィールドを使用してアラート・メッセージの送信先を指定する必要があります。zSecure Alert は、User Datagram Protocol (UDP) と伝送制御プロトコル (TCP) を介してメッセージの転送をサポートします。 UDP では、メッセージが失われる可能性があります。一方、TCP では、SYSLOG レシーバーが非常に低速である場合にすべてのアラートの処理が遅延する可能性があります。両方のオプションは同時に使用できます。宛先は、名前 (DNS によって検索された名前)、IP アドレス、またはコンマで区切ったリストでもかまいません。それぞれの宛先の直後に、コロンと 10 進形式のポート番号を続けることができます。

以下のフィールドは、WTO セクションに表示されます。

WTO アラートの WTO を生成します。

Write WTOs to C2RWTO DD
このフィールドと「**WTO**」の両方にタグが付いている場合、生成された WTO はコンソールへ送信されず、C2RWTO DD に書き込まれます。このフィールドは、テスト用です。

「**Reset all existing destination settings for this Alert Configuration**」オプションは、個々のアラートのすべての宛先設定をリセットします。このオプションは、アラート構成レベルでのみ使用できます。

アラート構成: アラート・カテゴリーの選択

このパネルは、アラート構成で S (選択) 行コマンドを使用して選択できます。

このパネルは、アラート構成概要パネルで「コピー」または「挿入」を実行すると、自動的に表示されます。これは、END または PF3 によってアラート宛先パネルを完了した後に表示されます。

```
  Menu Options Info Commands Setup
                      zSecure Suite - Setup - Alert   Row 1 to 8 of 8
Command ===> _____________________________________________ Scroll ===> CSR

Select the alert category you want to work with
The following line commands are available: W(Who/Where), S(elect)
-------------------------------------------------------------------------------
    Id  Category                                  #alerts        #selected
S   1   User alerts                              19             1
_   7   Group alerts                             1              0
_   2   Data set alerts                          16             0
_   3   General resource alerts                  7              0
_   4   UNIX alerts                              11             0
_   5   RACF control alerts                      8              0
_   6   System alerts                            15             0
_   8   Application alerts                       5              1
    0   Other alerts                             1              0
****************************** Bottom of data ********************************
```

図 7. 「*Setup Alert*」パネル: アラート・カテゴリーの選択

このパネルには、使用可能なアラート・カテゴリーが表示されます。以下のフィールドが表示されます。

Id
レポート・カテゴリー ID。アラート ID の 2 桁目を使用してカテゴリーが判別されます。

カテゴリー
zSecure Alert レポート・カテゴリー。現在、以下のカテゴリーが定義されています。

- User alerts
- Group alerts (RACF システムの場合のみ)
- Data set alerts
- General resource alerts
- UNIX alerts
- RACF (または ACF2) control alerts
- System alerts
- Application alerts

- Other alerts

#alerts
このカテゴリーで定義されたアラートの数。

#selected
このカテゴリーで選択されたアラートの数。

W、つまり「人」または「場所」の行コマンドを使用して、このカテゴリーに含まれるすべてのアラートの宛先を指定できます。「**Reset all existing destination settings for this category**」を選択したときは、このカテゴリーのアラートに個々のアラート・レベルで設定された宛先は破棄されます。

S (選択) コマンドは、カテゴリー内のすべてのアラートを表示します。例えば、RACF システムでは、アラートの表示は次の画面のようになります。

```
  Menu         Options       Info    Commands     Setup
_______________________________________________________________________________
                         zSecure Suite - Setup - Alert       Row 1 to 19 of 19
Command ===> _____________________________________________ Scroll ===> CSR

User alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where),S(elect), U(nselect), B(rowse)
-------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSWUA CA EM
_   Logon by unknown user                          1101  No   gECSWUA    N
_   Logon with emergency userid                    1102  No   gECSWUA Y  N
_   Logon of a userid with UID(0) (Unix superuser) 1103  No   gECSWUA    N
_   Highly authorized user revoked for pwd violatio 1104 No   gECSWUA    N
_   System authority granted                       1105  No   gECSWUA    N
_   System authority removed                       1106  No   gECSWUA    N
_   Group authority granted                        1107  No   gECSWUA    N
_   Group authority removed                        1108  No   gECSWUA    N
_   SPECIAL authority used by non-SPECIAL user     1109  No   gECSWUA    N
_   non-OPERATIONS user accessed data set with OPER 1110 No   gECSWUA    N
_   Invalid password attempts exceed limit         1111  No   gECSWUA    N
_   Password history flushed                       1112  No   gECSWUA    N
_   Suspect password changes                       1113  No   gECSWUA    N
_   Connect authority>=CREATE set                  1114  No   gECSWUA    N
_   Too many violations                            1115  No   gECSWUA Y  N
_   Non-expiring password enabled                  1119  No   gECSWUA    N
_   Major administrative activity                  1120  No   gECSWUA Y  N
_   Protected status removed                       1121  No   gECSWUA    N
_   Logon with sensitive userid (from C2PACMON)    1122  No   gECSWUA Y  N
****************************** Bottom of data ********************************
```

図 *8.* 「*Setup Alert*」パネル*:* 選択されたカテゴリーのアラートの表示

ACF2 システムでは、アラートの表示は次の画面のようになります。

```
Menu        Options      Info    Commands     Setup
_____________________________________________________________________________
                        zSecure Audit for ACF2 - Setup - Al Row 1 to 13 of 13
Command ===> _____________________________________________ Scroll ===> CSR

User alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where),S(elect), U(nselect), B(rowse)
------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSWUA CA EM
_   Logon with emergency logonid                   2102  Yes  gE      Y  N
_   Highly authorized user revoked for pwd violatio 2104 No   gE      __ N
_   System authority granted                       2105  No   gE      __ N
_   System authority removed                       2106  No   gE      __ N
_   Invalid password attempts exceed limit         2111  No   gE      __ N
_   Password history flushed                       2112  No   gE      __ N
_   Suspect password changes                       2113  No   gE      __ N
_   Too many violations                            2115  No   gE      Y  N
_   non-SECURITY user accessed data set with SECURI 2116 No   gE      __ N
_   non-NON-CNCL user accessed data set with NON-CN 2117 No   gE      __ N
_   non-READALL user accessed data set with READALL 2118 No   gE      __ N
_   Non-expiring password enabled                  2119  Yes  gECSWU  __ N
_   Major administrative activity                  2120  Yes  gECSWU  Y  N
****************************** Bottom of data ********************************
```

図 *9. ACF2* システムの「*Setup Alert*」パネル*:* 選択されたカテゴリーのアラートの表示

以下のフィールドが表示されます。

Alert アラートの説明。

Id アラートの数値 ID。IBM のアラート ID は、1000 からの 1999 の範囲を使用します。4000 からの 4999 の範囲は、インストール定義アラート用に予約されています。この ID は、スケルトン・メンバー名、WTO 出力メッセージ番号、および SNMP トラップ番号を生成するために使用されます。

Sel このアラートが選択されているかどうかを示します。

gECSWUA

W 行コマンドで設定された、このアラートの宛先タイプ。表示される可能性のある値は以下のとおりです。

E: E メール、**C**: 携帯電話 (テキスト・メッセージ)、**S**: SNMP トラップ、**W**: WTO、**U**: QRadar Unix syslog 、**A**: ArcSight CEF

値の前に「**g**」が付く場合があり、これは、宛先がアラート構成で **W** 行コマンドによってグローバルに設定されていることを意味します。

C このアラートが、構成にインストール固有の名前などの項目が反映されることを許可するかどうかを示すフラグ。このアラートを選択すると、構成を実行できるよう、パネルが表示されます。 148 ページの『事前定義アラートの構成』を参照してください。

A このアラートがアクション・コマンドを生成するように構成されているかどうかを示すフラグ。

EM このアラートが、アラート構成一般設定パネルで拡張モニターの活動化を必要とする拡張モニター・アラートであるかどうかを示すフラグ。拡張モニター・アラートについて詳しくは、 1 ページの『第 1 章 概要』、および 7 ページの『アラート活動化に関するガイドライン』を参照してください。

以下の行コマンドを使用できます。

表 4. アラートのリスト表示で使用できる行コマンド

A	**CARLa** コードのプレビュー。このアクションは、ISPF BROWSE モードでこのアラートについて生成された CARLa を表示します。
B	アラート定義のブラウズ。このアクションは、アラート定義を表示します。
C	アラートのコピー。このアクションは、すべてのフィールドを備えたアラート定義パネルを表示します。これらのフィールドは、選択したアラートからコピーされます。ただし、フィールド ID は除き、それはアラートごとに固有でなければなりません。
D	選択されたアラートの削除。IBM Security zSecure で定義されたアラートを削除することはできません。
E	アラートの編集。アラート ID、レコード・タイプ、CARLa コード、およびアクション・コマンドなどのアラート特性を指定します。 148 ページの『アラート定義 -「Specify action」』を参照してください。
I	新しいアラートの挿入。このアクションは、すべてのフィールドがブランクであるアラート定義パネルを表示します。必要なすべてのフィールドに入力すると、新しいアラートが追加されます。
S	アラートの選択。アラート構成の検査およびリフレッシュの後、そのアラートは報告されます。
U	アラートの選択解除。アラート構成の検査およびリフレッシュの後、そのアラートは報告されなくなります。
W	アラートの送信先の人/場所。宛先は、E メール・アドレス、テキスト・メッセージ/携帯電話の受信者、SNMP アドレス、QRadar Unix syslog アドレス、および WTO フォーマットのいずれでもかまいません。あるアラートのすべての宛先を消去した場合は、そのアラート・カテゴリーの宛先が使用されます。アラート・カテゴリーの宛先も設定されていない場合、アラート構成の宛先が使用されます。

C (コピー) または **I** (挿入) 行コマンドを使用してアラートを追加する方法については、 39 ページの『インストール定義アラート』を参照してください。

アラート構成: アラート構成の検査

30 ページの図 10 に表示されているパネルは、アラート構成概要パネルで「**コピー**」または「**挿入**」を指定すれば自動的に表示できます。これは、アラート条件の選択を完了した後に表示されます。

```
  Menu   Options   Info   Commands   Setup   Startpanel
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert
Command ===> ____________________________________________________________


_  Use SETUP FILES input instead of zSecure Alert input data
The following selections are supported:
B Browse file           S Default action (for each file)
V View file

Enter a selection in front of a highlighted line below:

_  AHJBVS       Stage one member
_  AHJBVO       Environment dependent selection criteria
   AHJBV        zSecure Alert report member
   AHJBVE       zSecure Alert extended monitor member
   AHJBVP       zSecure Alert parameter member

Press Enter to start Alert set verification
```

図 *10.* 「*Setup Alert*」パネル*:* アラート構成の検査

検査関数は、Alert アドレス・スペースの処理をエミュレートします。このため、検査を実行するユーザー ID を制限モードにすることはできません。このユーザー ID は、Alert の構成で指定されているセキュリティー・データベースおよび CKFREEZE へのアクセス権限も必要です。または、アクセス権限を持っていない場合、このユーザー ID は UNLOAD を指定するか、自分がアクセス権限を持っている別のセキュリティー・データベース・ソースおよび CKFREEZE を指定する必要があります。図 10の「**Use SETUP FILES input instead of zSecure Alert input data**」を参照してください。このオプションを選択すると、セキュリティー・データベースとこのアラート・セット用に構成された CKFREEZE データ・セットではなく、SETUP FILES で選択された入力データ・セットが検査に使用されます。

注**:** このオプションは、検査機能にのみ適用されます。Alert のアドレス・スペースでは、構成されているセキュリティー・データベースおよび C2POLICE JCL メンバーに指定されている CKFREEZE データ・セットを常に使用します。

Enter を押すと、同じパネルに検査プロセスの結果が表示されます。ユーザーは、検査プロセスによって作成されたメンバーをブラウズまたは表示することができます。検査中にエラーが検出された場合は、エラーが含まれているファイルが赤で強調表示されます。正常に完了した「Alert Generation」検査プロセスの CARLa 出力を表示するには、SYSPRINT 基本コマンドを使用できます。検査プロセスの間、SMF および WTO レコードは提供されないので、実際のアラートは生成されません。

以下のメンバーが検査プロセスによって作成されます。

<configuration-name>VS
: 検査された zSecure Alert stage1 メンバー。このメンバーには、アラート分析のときに使用されたシステム依存 CARLa 選択ステートメントを生成するために使用された CARLa コマンドが含まれています。**F** 行コマンドを発行すると、このメンバーがメンバー **<configuration-name>S** にコピーされます。 stage1 メンバーの機能については、「*IBM Security zSecure*

CARLa-Driven Components: インストールおよびデプロイメント・ガイド」のアラート・アドレス・スペースに関するセクションを参照してください。.

<configuration-name>VO
このメンバーには、分析時に使用され、stage1 メンバーによって生成された環境依存の選択基準が含まれています。このメンバーは、ユーザー・インターフェースによってのみ使用されるため、zSecure Alert レポート・メンバーを検査できます。zSecure Alert 開始タスクは、この stage1 出力を C2P1OUT DD に書き込みます。

<configuration-name>V
検査された zSecure Alert レポート・メンバー。このメンバーには、収集したレコードの分析に使用された主な (基本) CARLa コマンドが含まれています。 **F** 行コマンドを発行すると、このメンバーがメンバー **<configuration-name>** にコピーされます。

<configuration-name>VE
拡張モニター・アラート用の検査された zSecure Alert レポート・メンバー。このメンバーには、最新の 2 つの CKFREEZE スナップショット・データ・セットを比較するために使用する CARLa コマンドが含まれています。F 行コマンドを発行すると、このメンバーがメンバー **<configuration-name>E** にコピーされます。

<configuration-name>VP
このメンバーには、zSecure Alert パラメーターが含まれます。**F** 行コマンドを発行すると、このメンバーがパラメーター・メンバー **<configuration-name>P** にコピーされます。このメンバーは、PARMLIB DD によって開始タスク JCL で割り振られます。

アラート構成: アラート構成のリフレッシュ

手順

1. アラート構成で **F** (リフレッシュ) 行コマンドを使用して、このパネルを選択します。

   このパネルは、検査処理の終了時にアラート構成概要パネルで「コピー」または「挿入」を実行すると、自動的に表示されます。

   「リフレッシュ」ステップで、構成データ・セット内の検査されたメンバーが実動メンバーにコピーされます。コピーが正常に完了した後、次の確認パネルが表示されます。

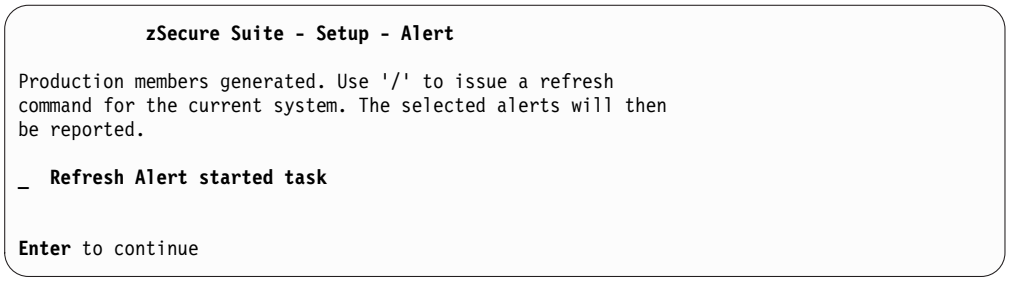

図 *11.* 「*Setup Alert*」パネル*:* アラート構成のリフレッシュ

2. このパネルで、開始タスクに対して REFRESH コマンドを発行する必要があることを指定します。

   開始タスクの JCL (PARMLIB DD ステートメント) が現行のアラート構成を使用するよう構成されている場合、REFRESH コマンドは開始タスクに、新規メンバーを再処理するよう指示します。
3. 「/」を使用して、MVS MODIFY C2POLICE,REFRESH コマンドを発行することができます。

   PF3 を押してリフレッシュ・パネルを終了すると、アラート構成パネルが再び表示されます。すべての構成ステップが正常に完了すると、状況の表示が「OK」になります。

E メール・アドレス・リスト (SE.A.E)

zSecure Alert では、E メール・アドレス・リストを使用して、複数の人にアラート・メッセージのメールを出すことができます。これは、各種のパネルで E メール・アドレスのコンマ区切りリストを直接指定して、行うことができます。 E メール・オプションには、代替の方法があります。E メール・オプションから、データ・セットと、各レコードから E メール・アドレスを抽出する方法を指定します。これをコンマ区切り E メール・アドレスのリストと区別するために、E メール宛先という用語を使用します。名前によって参照した E メール宛先は、アラートの「**Mail to**」フィールドで使用できます。詳しくは、「Mail to」フィールドの説明を参照してください。

注**:** アラート構成に加えた変更は、オプション **SE.A.E** を終了するまで永続的には保存されません。

zSecure Alert を初めて使用する場合は、この構成ステップをスキップできます。後でもっと柔軟な E メール・アドレスが必要になった場合は、このセクションに再びアクセスして、必要な E メール宛先を作成してください。

このオプションを初めて入力する場合は、次のパネルが表示されます。

注**:** 例として、ほとんどのフィールドは既に入力済みです。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert
Command ===> ____________________________________________________________

Enter zSecure Alert definition for e-mail destinations
Name  . . . . . . . . . SECADM
Description . . . . . . Security administrator e-mail addresses


Enter / to edit the e-mail destination data set
/  Data set name     'C2P.DATA.MAIL(SECADM)'

Field definitions
Field name        Start   Length||Word  Delimiter
secadmin userid   ______  ______  1     ;
e-mail address    ______  ______  2     ;
```

図 *12.* 「*Setup Alert*」パネル: *E* メール宛先の指定

このパネルには、以下のフィールドがあります。

Name この E メール宛先の短い記述名。このフィールドは必須で、固有でなければなりません。アラート構成のときに、この名前を使用して、この E メール宛先を参照できます。

説明 E メール宛先の説明。このフィールドは必須です。

Data set name

E メール・アドレスが含まれているデータ・セット。これは、順次データ・セットか区分データ・セットとすることができ、例えば 'C2P.DATA.MAIL(SECADM)' のように、メンバー名を括弧で囲みます。区分データ・セット、できれば PDS/E を使用してください。なぜなら、データ・セットは zSecure Alert アドレス・スペースによって (DISP=SHR で) 割り振られるからです。順次データ・セットでは、編集に排他的エンキューが必要になります。そのため、開始タスクによってそのデータ・セットが既に割り振られている場合は、それを取得できなくなります。また、PDS では、データ・セットを圧縮する必要がある場合に排他的エンキューが必要になります。

メンバーに対するすべての変更は、F C2POLICE,REFRESH ごとに、また環境リフレッシュ・インターバルごとに有効になります。デフォルトは 60 分です。

Field name

「**e-mail address**」などのフィールド名。

データ・セットが E メール・アドレスだけで構成されているにもかかわらず、行番号がある場合は、「**Start**」および「**Length**」フィールドを使用して E メール・アドレス・フィールドを定義します。例えば、FB 80 データ・セットの場合は、「開始」に 1、「長さ」に 72 を入力します。

データ・セットに E メール・アドレスのほかに他の情報が含まれている場合は、レコードのどの部分が使用したい E メール・アドレスであるかを識別するために、「Field Name」を指定する必要があります。

アラート構成のとき、***destination-name.field-name*** を指定することにより、このフィールドを参照できます。

Start フィールドの開始位置の数値を入力します。例えば、左端の文字から直接開

始するには、1 を入力します。このフィールドは、データ・セットから E メール・アドレスを抽出するために「長さ」フィールドと一緒に使用されます。

このフィールドを、フィールド「**Word**」および「**Delimiter**」と同時に使用することはできません。

Length

フィールドの長さ。このフィールドは、「開始」フィールドと一緒に使用されます。

このフィールドを、フィールド「**Word**」および「**Delimiter**」と同時に使用することはできません。

Word 必要な「語」のシーケンス番号。このフィールドは、データ・セットから E メール・アドレスを抽出するために「**Delimiter**」フィールドと一緒に使用されます。

このフィールドを、フィールド「**Start**」および「**Length**」と同時に使用することはできません。

Delimiter

語を互いに分離するために使用される文字。例としては、「;」またはスペースがあります。このフィールドは、「**Word**」フィールドと一緒に使用されます。

このフィールドを、フィールド「**Start**」および「**Length**」と同時に使用することはできません。

データ・セット名の前に / を入力することにより、E メール宛先セットを表示または編集できます。 33 ページの図 12で示したデータの場合、データ・セット・レイアウトは以下のようになります。

```
  File  Edit  Confirm  Menu  Utilities  Compilers  Test  Help
------------------------------------------------------------------------------
EDIT       C2P.DATA.MAIL(SECADM)                          Columns 00001 00072
Command ===> ____________________________________________ Scroll ===> CSR
****** ***************************** Top of Data ******************************
000001 C2PSA01;JohnBrown@company.com;
000002 C2PSA02;MarkTyler@company.com;
000003 C2PSA03;SteveJohnson@company.com;
000004 C2PSA04;KarenJones@company.com;
****** **************************** Bottom of Data ****************************
```

図 *13. E* メール宛先セットを表示または編集するためのパネル

E メール宛先が、END を押すことによって保存された場合は、次にパネルが表示されます。このパネルは使用できる E メール宛先の概要を示します。このパネルを使用して、宛先を管理することができます。次の例では、1 つの E メール宛先だけが定義されています。

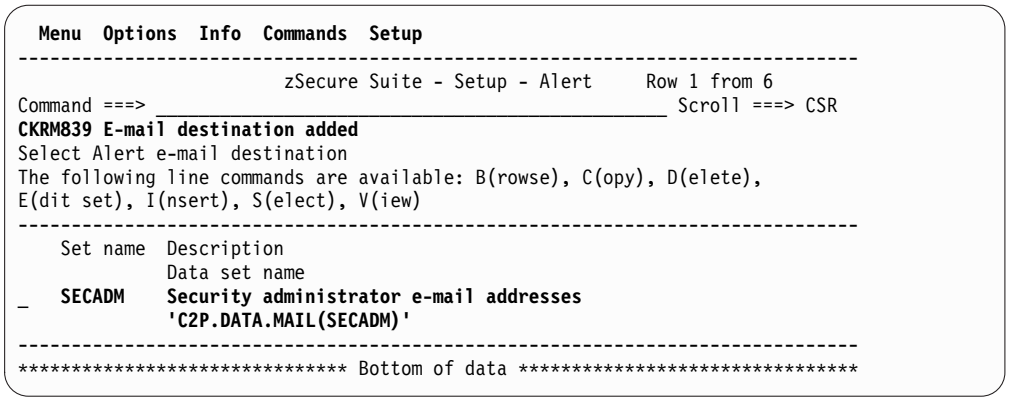

図 *14.* 「*Setup Alert*」パネル: *E* メール宛先更新の確認メッセージの保存

E メール宛先セット概要パネルでは、以下の行コマンドを使用できます。

表 *5. E* メール宛先セット概要パネルで使用可能な行コマンド

行コマンド	説明
/	使用可能な行コマンドを示したポップアップ・パネルを表示します。
C	E メール宛先をコピーします。このアクションは、 33 ページの図 12 に示すように、すべてのフィールドを備えた定義パネルを表示します。これらのフィールドは、E メール宛先ごとに固有でなければならない「**Name**」フィールドを除き、選択した E メール宛先からコピーされます。
D	E メール宛先を削除します。このアクションは、関連するデータ・セットには影響しません。
I	新しい E メール宛先を挿入します。このアクションは、すべてのフィールドがブランクである定義パネルを表示します。
S	この E メール宛先の一般設定を、変更のために選択します。
B	ISPF BROWSE サービスを使用して、データ・セットをブラウズします。
E	ISPF EDIT サービスを使用して、データ・セットを編集し、E メール・アドレスを変更できます。
V	ISPF VIEW サービスを使用して、データ・セットを表示します。

PCI PAN データ・セットと PCI AUTH データ・セット、ユーザー、およびグループの定義 (SE.A.P)

このオプションを使用して、Payment Card Industry の主要アカウント番号 (PCI PAN) のデータ・セットと機密認証データ (PCI AUTH) のデータ・セット、およびこれらのデータ・セットへのアクセスを許可された特権ユーザーとグループを定義します。

以下のパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Alert - PCI
Command ===> ____________________________________________________________

Select library for PCI members
1  1. Use Alert library 'C2POLICE.C2PCUST'
   2. Use Audit library 'AUDIT.CKACUST'

Enter / to edit member
_  PCI-DSS sensitive data sets
_  Privileged users and groups for PCI PAN data sets
_  Privileged users and groups for clear text PCI PAN data sets
_  Privileged users and groups for PCI AUTH data sets
```

図 *15.* 「*Alert - PCI*」パネル

C2PCUST データ・セットのみ使用可能な場合、メンバーはそのデータ・セットに保管されます。 C2PCUST と CKACUST の両方のライブラリーが使用可能な場合、使用するライブラリーは、オプション「**Select library for PCI members**」を使用して指定できます。

別のシステムのアラート構成が作成されていて、PCI データ・セットおよび特権ユーザー/グループが現行システムのものと同じ場合、選択した C2PCUST データ・セットまたは CKACUST データ・セットを共有できます。

各構成の PCI データ・セットまたは特権ユーザー/グループ、あるいはその両方が同じではない場合、以下の手順を実行します。

1. SCKRSAMP ジョブ CKAZCUST を使用して、新規 CKACUST ライブラリーを作成します。
2. パラメーター・メンバー (デフォルト C2R$PARM) で新しく作成された CKACUST を使用して、ユーザー・インターフェースを開始します。
3. オプション **SE.A.P** を使用して、メンバーを編集します。
4. **SE.A.A** を使用して、構成を完了します。

使用可能なオプションは次のとおりです。

PCI-DSS sensitive data sets
SIMULATE SENSITIVE ステートメントを含めることができるメンバー CLASSIFY の編集セッションを開始します。詳細については、『*IBM Security zSecure CARLa* コマンド・リファレンス』にて、SIMULATE コマンドの SENSITIVY=Site<*text*> を参照してください。このメンバーは、RACF のアラート 1209、1210、1211、および ACF2 のアラート 2209、2210、2211 で利用されます。

Privileged users and groups for PCI PAN data sets
メンバー PCIPAN の編集セッションを開始します。このメンバーを使用すると、アラートを生成してはならない特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1209 および ACF2 のアラート 2209 で利用されます。

Privileged users and groups for clear text PCI PAN data sets
メンバー PCIPANCL の編集セッションを開始します。このメンバーを使用す

ると、アラートを生成してはならない特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1210 および ACF2 のアラート 2210 で利用されます。

Privileged users and groups for PCI AUTH data sets
メンバー PCIAUTH の編集セッションを開始します。このメンバーを使用すると、アラートを生成してはならない特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1211 および ACF2 のアラート 2211 で利用されます。

機密リソース、ユーザー ID、およびグループ (SE.A.S)

機密リソース、およびそれらのリソースへのアクセスが許可される特権ユーザーおよびグループは、オプション SE.A.S を使用して定義します。

以下のパネルが表示されます。

```
 Menu         Options       Info     Commands     Setup
------------------------------------------------------------------------------
                        zSecure Suite - Alert - Sensitive
Command ===> ____________________________________________________________

Select library for sensitive resource members
1  1. Use Alert library 'C2POLICE.C2PCUST'
   2. Use Audit library 'AUDIT.CKACUST'

Enter / to edit member
_  Sensitive resources
_  UPDATE sensitive members in specific data sets
_  Privileged users and groups for site READ sensitive resources
_  Privileged users and groups for site UPDATE sensitive resources
_  Privileged users and groups for UPDATE on APF data sets
```

図 *16.* 「*Alert - Sensitive*」パネル

C2PCUST データ・セットのみ使用可能な場合、メンバーはそのデータ・セットに保管されます。 C2PCUST と CKACUST の両方のライブラリーが使用可能な場合、使用するライブラリーは、オプション「**Select library for sensitive resource members**」を使用して指定できます。

別のシステムのアラート構成が作成されていて、機密リソースおよび特権ユーザー/グループが現行システムのものと同じ場合、選択した C2PCUST データ・セットまたは CKACUST データ・セットを共有できます。

各構成の機密リソースまたは特権ユーザー/グループが同一ではない場合は、以下の手順に従ってください。

1. SCKRSAMP ジョブ CKAZCUST を使用して、CKACUST ライブラリーを作成します。
2. パラメーター・メンバー (デフォルト C2R$PARM) で新しく作成された CKACUST を使用して、ユーザー・インターフェースを開始します。
3. オプション **SE.A.S** を使用して、メンバーを編集します。
4. **SE.A.A** を使用して、構成を完了します。

使用可能なオプションは次のとおりです。

Sensitive resources
SIMULATE SENSITIVE ステートメントを含めることができるメンバー SENSRSRC の編集セッションを開始します。このメンバーは、RACF のアラート 1212 および 1213、および ACF2 のアラート 2211 および 2213 で使用されます。例えば、次のようにします。

```
SIMULATE CLASS=DATASET ACCESS=READ,
SENSITIVITY=Site-Dsn-R,
RESOURCE=FINANCE.ACCOUNT
```

SENSITIVITY には、以下のいずれかを使用します。

Site-Dsn-R
サイト READ 機密データ・セット用

Site-Dsn-U
サイト UPDATE 機密データ・セット用

UPDATE sensitive members in specific data sets
メンバー SENSMEMB の編集セッションを開始します。このメンバーを使用すると、アラートを生成する必要がある機密データ・セットおよびメンバーのリストを入力できます。このメンバーは、RACF のアラート 1214、および ACF2 のアラート 2214 で使用されます。データ・セット名は列 1 から44、メンバー名は列 46 から 53 で指定する必要があります。フィルター (RACF の場合は *、ACF2 の場合は - など) を使用できます。

Privileged users and groups for site READ sensitive resources
メンバー SENSREAD の編集セッションを開始します。このメンバーを使用すると、アラートを生成してはならない機密リソース、および特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1212、および ACF2 のアラート 2212 で使用されます。アラートは、zSecure によって既に機密性が割り当てられているリソース (APF ライブラリー、JES スプール・データ・セットなど) には生成されません。

ユーザーまたはグループは列 1 から 8、クラスは列 10 から 17、リソースは列 19 から 80 で指定する必要があります。例えば、次のようにします。

```
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----8
IBMUSER  DATASET  FINANCE.ACCOUNT
SYSADM   FACILITY USER.AUTH
```

すべてのクラスまたは特定のクラスのすべてのリソースに対して、1 つの特権ユーザーまたはグループを定義する場合、クラス名またはリソース名を * と指定できます。

Privileged users and groups for site UPDATE sensitive resources
メンバー SENSUPDT の編集セッションを開始します。このメンバーを使用すると、アラートを生成してはならない機密リソース、および特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1213 および 1214、および ACF2 のアラート 2213 および 2214 で使用されます。

ユーザー、グループ、およびリソースの定義方法については、「**Privileged users and groups for site READ sensitive resources**」を参照してください。

Privileged users and groups for UPDATE on APF data sets
メンバー SENSAPFU の編集セッションを開始します。このメンバーを使用す

ると、アラートを生成してはならない特権ユーザーおよびグループのリストを入力できます。このメンバーは、RACF のアラート 1204、および ACF2 のアラート 2204 で使用されます。

ユーザーまたはグループは列 1 から 8 で指定する必要があります。例えば、次のようにします。

```
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----8
IBMUSER
SYSADM
```

インストール定義アラート

既存のアラートをコピーして変更するか、アラートを最初から作成することにより、新しいアラートを作成できます。

アラートの指定は、大部分がスケルトン・メンバーのいくつかの CARLa コード・セクションで行われます。このスケルトン・メンバーは、「検査」操作のとき、zSecure Alert エンジンに渡す実際の CARLa を作成するために使用されます。一般に、それには高度な CARLa コーディングのスキルが必要です。この知識は、このセクション全体の前提となっています。詳しくは、「*IBM Security zSecure: CARLa* コマンド・リファレンス」を参照してください。

アラートを作成する場合は、以下の項目を決める必要があります。

- アラート ID。この 4 桁の番号は識別子として機能し、常に目立つ存在です。IBM 提供アラートには、アラート番号 1000-1999 (RACF)、2000-2999 (ACF2)、および 3000-3999 (TSS) が付いています。範囲 4000-4999 (RACF)、5000-5999 (ACF2)、および 6000-6999 (TSS) は、インストール定義アラート用に予約されています。この番号の 2 桁目は、アラートをアラート・カテゴリーに割り当てます。
- アラートをトリガーしたいイベント。
- アラート条件からの関連データを、アラートにどのようにフォーマット設定するか。
- アラートがカスタマイズ可能であるかどうか。

  例えば、アラートにデータ・セットまたはユーザー ID のリストが必要になる場合もあります。ユーザーは、このリストを、毎回スケルトンを編集することなく保守したいと考えます。アラートをカスタマイズ可能にしたい場合は、それをカスタマイズできるパネルが必要です。

  パネルの外観と、そのパネルがアラートをカスタマイズするために受け入れるパラメーターは、ユーザーが決めます。パネルを最初から作成するか、要件に適合する標準 zSecure パネルを使用するか、コピーするか、あるいはクローンを作成することができます。独自のパネルを必要とするユーザーは、それを独自のライブラリーに保管する必要があります。そのライブラリーを ISPF で使用できるようにするには、UPREFIX/WPREFIX zSecure 構成パラメーターを使用する必要があります。UPREFIX/WPREFIX パラメーターについては、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」を参照してください。

スケルトンに、アラートの CARLa を生成するために必要なパラメーターを提供するには、それらのパラメーターの名前を EXTVAR という名前の変数に割り当てる必要があります。つまり、以下のとおりです。

```
&extvar='c2peeus0,c2peeus1,c2peeus2,c2peeus3,c2peeus4'
```

既存のカスタマイズ・パネル C2PP3ZAG をユーザーの指定に使用したり、C2PP3ZBE を他のエンティティー (クラス、プログラム名など) に使用したりすることもできます。これらのパネルはアラート・テーブル C2PIDACx の拡張変数を IBM アラートに使用し、C2PIUACx をユーザー定義のアラートに使用して、カスタマイズ値のヘッダーとヘルプ・テキストを指定します。ISPF オプション 3.16 を使用して C2PCUST データ・セットの C2PIUAC*x* を編集し、これらの 2 つの拡張変数を指定できます。

アラートを送信するフォーマットは、宛先タイプごとに指定されます。以下の宛先タイプがあります。

- E メール
- テキスト・メッセージ
- WTO
- SNMP トラップ
- QRadar Unix syslog
- 共通イベント・フォーマット (CEF) の HPE Security ArcSight

E メール・フォーマットは、最も記述的なものです。製品に付属するアラートには共通のレイアウトがあります。このレイアウトについては、 64 ページの『標準 E メール・レイアウト』で説明しています。 E メールは、HTML フォーマットで送信されます。

IBM Security zSecure が提供するすべてのアラートのテキスト・メッセージ・フォーマットは、E メールからテキスト・メッセージへのゲートウェイで使用される E メール・フォーマットの短縮バージョンです。このゲートウェイでは、受信者 (例えば、携帯電話またはポケットベル) は、E メール・メッセージの「To」ヘッダー内で指定されます。テキスト・メッセージ自体は、ゲートウェイに応じて、件名または E メールの本体から取得できます。したがって、件名と送信される本体は、よく似ています。ただし、本体には少し詳しい情報が入っています。

WTO フォーマットは、自動化された運用ソフトウェアで使用できます。

SNMP トラップ・フォーマットは、ネットワーク・コンソールで使用できます。このフォーマットについて詳しくは、 163 ページの『付録 A. SNMP 出力』 を参照してください。

アラート ID とデータ・ソースの指定

手順

アラートを作成するには、以下のステップを実行します。

1. アラートを作成するには、オプション SE.A.A に進み、処理したいアラート構成を選択します。

2. アラート・カテゴリー・パネルで、「**System alerts**」など、いずれかのカテゴリーを選択します。

   新しいアラートが属するカテゴリーは、アラートの作成に使用したカテゴリーではなく、アラートの 2 桁目で決まります。

```
   Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                      zSecure Suite - Setup - Alert       Row 1 to 15 of 15
 Command ===> _____________________________________________ Scroll ===> CSR

System alerts
Select the alert you want to work with.
The following line commands are available: A(Preview), C(opy), D(elete),
E(dit), I(nsert), W(Who/Where),S(elect), U(nselect), B(rowse)
------------------------------------------------------------------------------
    Alert                                          Id    Sel  gECSWUA CA EM
    SMF data loss started                          1601  No   gECSWUA    N
    SMF logging resumed after failure              1602  No   gECSWUA    N
    SVC definition changed                         1603  No   gECSWUA    Y
    IBM Health Checker found low severity problem  1604  No   gECSWUA    N
    IBM Health Checker found medium severity proble 1605 No   gECSWUA    N
    IBM Health Checker found high severity problem 1606  No   gECSWUA    N
    SMF record flood detected                      1607  No   gECSWUA    N
    SMF record flood starts dropping records       1608  No   gECSWUA    N
    IP attacks blocked by filter no longer logged  1609  No   gECSWUA    Y
    IP attacks blocked by default filter no longer 1610  No   gECSWUA    Y
    IP SMF 119 subtype no longer written           1611  No   gECSWUA    Y
    IP filtering and IPsec tunnel support deactivat 1612 No   gECSWUA    Y
    IP ports below 1024 no longer reserved         1613  No   gECSWUA    Y
    IP interface security class changed            1614  No   gECSWUA    Y
    IP filter rules changed                        1615  No   gECSWUA    Y

 ****************************** Bottom of data ********************************
```

図 *17.* 「*Setup Alert*」パネル*:* カスタム・アラートのアラート *ID* とデータ・ソースの指定

3. **C** (コピー) または **I** (挿入) 行コマンドを発行することにより、アラートを作成できます。 「**コピー**」コマンドは、アラート ID 以外のすべてのフィールドをコピーします。

   次のパネルは、**I** 行コマンドを発行した後に表示されます。

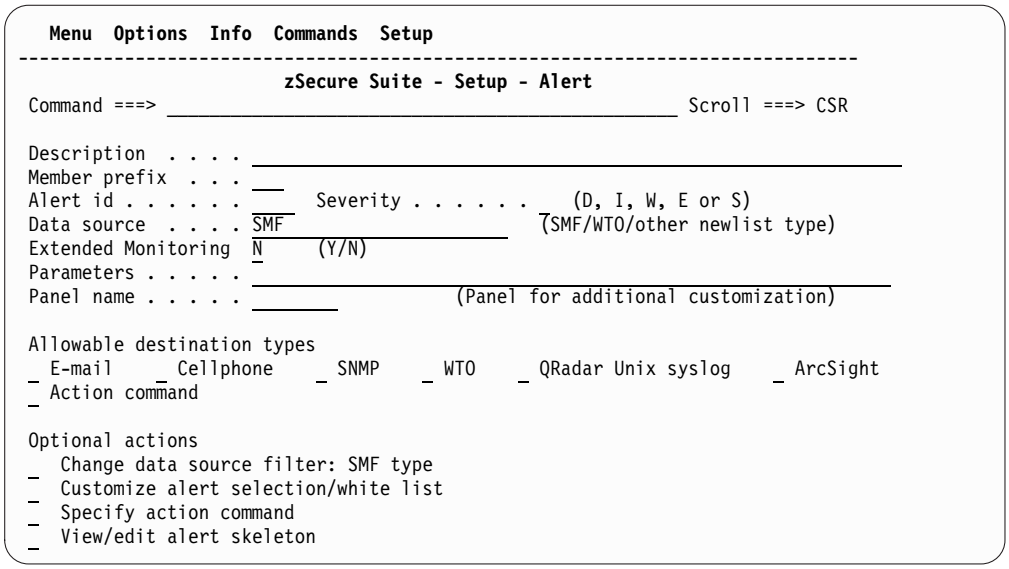

図 *18.* 「*Setup Alert*」パネル*:* アラートの追加

以下のフィールドが表示されます。

Description
アラートの説明。

Member prefix
3 文字からなる、スケルトン・メンバーの接頭部。生成されるスケルトン・メンバーの名前は、**<Member prefix>S<Alert id>** となります。3 文字の接頭部は、英字か「@」、「#」、「$」のいずれかで始まる必要があり、数字で始めることはできません。

接頭部 C2P は IBM Security zSecure 用に予約されています。

Alert id
アラートの数値 ID。IBM のアラート ID は、範囲 1000-1999 (RACF)、2000-2999 (ACF2)、および 3000-3999 (TSS) を使用します。範囲 4000-4999 (RACF)、5000-5999 (ACF2)、および 6000-6999 (TSS) は、インストール定義アラート用に予約されています。2 桁目は、アラート・カテゴリーを決定します。ID は、スケルトン・メンバーの名前を生成するために使用されます。

WTO を宛先タイプとして選択した場合、この値はメッセージ ID「**C2P<Alert id><Severity>**」の **<Alert id>** フィールドへの取り込みにも使用されます。

Severity
アラートの重大度。WTO を宛先タイプとして選択した場合、この値はメッセージ ID「**C2P<Alert id><Severity>**」の **<Severity>** フィールドへの取り込みにも使用されます。

次のリストは、有効な重大度を示しています。

D デバッグ。アクションは不要です。

I 情報。アクションは不要です。

W 注意。アクションが必要な場合もあります。

E エラー。アクションが必要です。

S 重大エラー。アクションが緊急に必要です。

宛先タイプが QRadar Unix syslog のアラートの場合、これらの重大度は次のリストに示すように変換されます。

重大度 優先順位

D 119

I 117

W 116

E 115

S 114

Data source
アラートの CARLa 新規リスト・タイプのデータ・ソース (例えば、`SMF` や `WTO` など)。

Extended Monitoring
このフィールドは、アラートが拡張モニター・アラートであるかどうかを指定します。現在と以前の CKFREEZE スナップショット・データ・セットを比較する拡張モニター・アラートの場合は、「**Y**」を指定します。イベント・ベースのアラートの場合は、「**N**」を指定します。必ず、「**Data Source**」フィールドには、拡張モニター設定に一致する正しい値を指定してください。イベント・ベースのアラートの場合、「**Data Source**」フィールドの値は SMF または WTO でなければなりません。拡張モニター・アラートの場合、「**Data Source**」フィールドには、サポートされている CKFREEZE ベースの NEWLIST タイプであれば、どのような値でも指定できます。拡張モニター・アラートについて詳しくは、7 ページの『アラート活動化に関するガイドライン』を参照してください。

Parameters
このフィールドは、生成された `NEWLIST` ステートメントに追加パラメーターを渡すためのものです。

Panel name
新しいアラートをカスタマイズ可能にしたい場合は、カスタマイズ用のパネルの名前をこのフィールドに指定します。指定するパネルは、要件に適合する標準 zSecure パネルとして、またはユーザー自身が作成したパネルとして既に存在し、アクセス可能であることが必要です。このパネルは、新しいアラートの作成時に、次のトランザクションとして表示されます。また、このアラートに対する将来の構成にも使用できます。

Allowable destination types
このアラートによってレポートを生成できる宛先タイプを選択します。アラートのスケルトンは、選択された宛先タイプごとにセクションを持っている必要があります。

Change data source filter
SMF ベースまたは WTO ベースのアラートの場合、これは、現在アラートに対して定義されている収集パラメーターを示します。SMF の場

合、タイプおよびオプションのサブタイプがリストされます。WTO の場合、メッセージ接頭語がリストされます。収集パラメーターを変更するには、チェック・ボックスに / を入力します。

アラート・スケルトンでは、そのアラートに関連する SMF レコードと WTO を選択する必要があることに注意してください。そのため、収集パラメーターが設定されていても、アラート・スケルトンには引き続き SELECT TYPE=*numbers* または SELECT MSGID=*wtoid* が含まれている必要があります。

Customize alert selection/whitelist
追加のカスタマイズのためにパネル名を指定した場合、このチェック・ボックスには、ユーザー、グループ、ジョブ名、またはクラスの選択または除外を指定するためのプロンプトを示すパネルが表示されます。

Specify action command
この行は、プロンプトの背後で「**active**」を表示することにより、アラートで現在アクション・コマンドが生成される場合に表示されます。

アラート条件がトリガーされたときのアクション・コマンドの実行をオンまたはオフに切り換える場合、およびコマンドを指定する場合は、このチェック・ボックスを選択します。 148 ページの『アラート定義 - 「Specify action」』を参照してください。

ISPF Skeleton
このアラートの ISPF スケルトンを編集するには、このフィールドにスラッシュ (/) を入力します。スケルトンには、アラート条件、アラート内容、およびアラート・レイアウトを指定する CARLa コードが含まれています。

「コピー」コマンドを使用してアラートを追加する場合、ソース・アラートのスケルトンがコピーされます。それ以外の場合は、モデル・スケルトンが使用されます。スケルトンが存在する場合、それは変更されません。

拡張モニター・アラートの場合、COMPAREOPT を他のすべてのセクションと共に ISPF スケルトンに追加する必要があります。

例えば、APF リストが SETPROG コマンドで更新された場合にトリガーされるアラートを定義するには、以下のようにします。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        zSecure Suite - Setup - Alert
 Command ===> ____________________________________________________________

 Description  . . . . APF List changed using SETPROG command_____________________
 Member prefix  . . . ABJ
 Alert id . . . . . . 4000  Severity . . . . W  (D, I, W, E or S)
 Data source  . . . . WTO
 Extended Monitoring  N     (Y/N)
 Parameters . . . . . _____________________________________________________
 Panel name . . . . . ________  (Panel for additional customization)

 Allowable destination types
/  E-mail   _  Cellphone   _  SNMP   _  WTO   _  QRadar Unix syslog   _  ArcSight

 Optional actions
 _  Change data source filter: SMF type
    Customize alert selection/white list
 _  Specify action command
 _  View/edite alert skeleton
```

図 *19.* 「*Setup Alert*」パネル*:* アラートの定義

4. Enter を押すと、アラートをトリガーするために使用される WTO メッセージ接頭語の入力を求めるプロンプトがパネルに表示されます。ここで、以下のように CSV410I を指定します。

```
  Menu         Options       Info    Commands     Setup
-------------------------------------------------------------------------------
                        Data source filters             Enter required field

Data source filters for alert 4000:

SMF records to be collected for this alert
Type Sub    Type Sub    Type Sub    Type Sub    Type Sub


WTO message ids and filters for this alert
Prefix    Prefix    Prefix    Prefix    Prefix
CSV410I   ________  ________  ________  ________
```

図 *20.* 「*Setup Alert*」パネル*: CSV410I* の指定

Type

データ・ソースが SMF の場合: このアラート用に収集する必要がある SMF レコード・タイプ。ACF2 レコードを収集する場合は、疑似タイプ ACF2 を指定できます。zSecure Alert プログラムは、ACF2 制御ブロックから正しいレコード・タイプを検索します。

Sub 収集する必要がある SMF レコード・サブタイプを指定します。このサブタイプは、SMF レコード・タイプ 30、80、92、および ACF2 レコードにのみ使用されます。 それ以外のすべての SMF レコード・タイプの場合、このサブタイプは無視されます。サブタイプは、以下のように解釈されます。

Rectype 30 サブタイプは、標準 SMF レコード・サブタイプです。

Rectype 80 サブタイプは RACF イベント・コードです。RACF イベント・コードの完全なリストについては、「RACF 監査担当者のガイド」を参照してください。

Rectype 92 サブタイプは、標準 SMF レコード・サブタイプです。現在、SMF レコード・タイプ 92 には 1 から 17 までのサブタイプだけが定義されていますが、zSecure Alert で受け入れられる範囲は 1 から 255 までです。

Rectype ACF2 サブタイプは ACF2 レコード・タイプです。ACF2 サブタイプの完全なリストについては、「*CARLa* コマンド・リファレンス」の『SELECT/LIST フィールド』の章を参照してください (NEWLIST TYPE=SMF の ACF2_SUBTYPE フィールドを参照)。

Prefix

データ・ソースが WTO の場合: どのメッセージ接頭部を収集する必要があるかを指定します。

Enter を押してデータ・ソース・フィルターを保存すると、アラートの指定パネルのチェック・ボックスが以下のように変更されます。

```
Change data source filter: WTO msg CSV410I
```

既存のアラートの CARLa スケルトン

既存のインストール定義アラートの CARLa スケルトンを編集できます。個々のアラートに対して E (編集) 行コマンドを使用した後に、「**ISPF skeleton**」オプションをチェックすることで、スケルトン・メンバーを編集できます。zSecure 提供のアラートで「**ISPF Skeleton**」オプションをチェックすると、ISPF VIEW パネルが表示されます。意図しない変更を防ぐには、B (ブラウズ) 行コマンドを使用します。

C (コピー) または I (挿入) 行コマンドを使用してアラートを追加する場合、同じパネルに到達します。その場合、通常では、まだスケルトン・メンバーが存在しません。必須パラメーターを指定すると処理が続行され、既存のスケルトン・メンバーがコピーされるか、モデル・スケルトンが作成されます。メンバーのコピーには名前付きフィルターが含まれることがあります。名前の競合を避けるためにこれらを変更してください。ローカル定義の名前はすべて末尾にアラート ID が付いていなければなりません。

このセクションの残りの部分では、モデル・スケルトン・メンバー C2PSMODL の内容について説明します。スケルトンは複数のセクションで構成され、各セクションには独自の固有ステートメントが含まれています。スケルトン内のこれらの各セクションには、以下のように識別用のコメント行でマークが付けられています。スケルトン内に出現する順に示します。

ID セクション

アラートのスケルトンの先頭には、アラート・メッセージに対して次の 3 つのテキスト値を設定します。

C2PXNAME

Unix SYSLOG メッセージと CEF メッセージで、イベントを分類するために使用されるイベント名を表します。引用符なしの短い固定値にする必要があります。

C2PXMSG

すべてのアラートに含めるアラート・メッセージ・テキストを指定しま

す。メッセージは、引用符で囲んだリテラルと CARLa フィールドで構成できます。最大長は、約 200 文字です。

C2PXDES
携帯電話メッセージと WTO メッセージ以外のすべてのアラート・フォーマットに含めるイベントの説明を指定します。メッセージは、引用符で囲んだリテラルと CARLa フィールドで構成できます。最大長は、約 450 文字です。

C2PXMSG と C2PXDES の構文については、49 ページの『ID セクション』を参照してください。

メッセージ・フォーマット・スケルトン C2PSFMSG は、これらのダイアログ変数を使用して、宛先に該当するフィールドを構築します。

スケルトン内の残りのセクションには、次のように識別用のコメント行でマークが付けられています。スケルトン内に出現する順に示します。各セクションは、セクションのコードをアクティブにするための条件を指定する)SEL コマンドで始まり、)ENDSEL コマンドで終わります。

)CM Pass one query
このセクションでは、stage1 メンバーの 2 パスの CARLa 照会を指定します。ご使用のアラート条件がセキュリティー環境に依存しており、フィールド・ルックアップを使用して容易に実装できない場合にこれを使用します。フィールド・ルックアップについては、「*zSecure CARLa* コマンド・リファレンス」のDEFINE コマンドに関するセクションで、『間接参照またはルックアップ』を参照してください。この照会は、環境リフレッシュの各サイクルの始めに実行されます。通常その出力は別の CARLa 照会であり、現在の環境値が取り込まれています。この出力は、レポート作成 CARLa の冒頭近くに含まれます。これにより、実際のセキュリティー環境に基づく事前選択を生成できます。ご使用のアラート条件でこの事前選択を参照することができます。パス 1 照会は環境リフレッシュの各サイクルの始めに実行されるため、この事前選択も現在の選択内容でリフレッシュされます。環境リフレッシュ・サイクルは通常、1 時間に 1 回です。**Environment refresh** パラメーターについては、16 ページの『アラート構成: 一般設定の指定』を参照してください。

CARLa ステートメントを)SEL 行と)ENDSEL 行の間に挿入します。

)CM Extended Monitoring COMPAREOPT
このセクションでは、アラートをトリガーする比較を定義するオプションの COMPAREOPT ステートメントを指定できます。名前の競合を避けるために、COMPAREOPT には、ALRT4001 のように末尾がアラート ID の名前が必要です。ダイアログ変数 &C2PENCMP には、COMPAREOPT コマンドの名前が設定されているため、このアラートのすべてのメッセージ・セクションから参照されます。これまでのリリースの zSecure Alert では、必須の COMPAREOPT ステートメントはメンバー C2PSGLOB に含まれ、対応する COMPAREOPT パラメーターはアラートの指定パネルに含まれていました。

CARLa ステートメントを)SEL 行と)ENDSEL 行の間に挿入します。拡張モニター・アラートで COMPAREOPT を使用しない場合は、このセクションから &C2PENCMP の割り当てと COMPAREOPT コマンド行を削除してください。

)CM Alert condition
アラートの選択基準を指定します。

)IM C2PSGNEW 行の後に CARLa ステートメントを挿入します。通常、このセクションには、オプションで先行する DEFINE コマンドを持つ SELECT コマンドが含まれています。

)CM EMAIL sortlist
E メール宛先に使用するレイアウト内のアラート・メッセージを指定します。

)CM Cellphone sortlist
テキスト・メッセージ内で使用するレイアウト内のアラート・メッセージを指定します。受信テキスト・メッセージが件名と E メールの本体のどちらから取得されるかは、使用している、E メールからテキスト・メッセージへのゲートウェイによって決まります。すべての IBM Security zSecure 提供アラートは、件名と本体の両方の中で、よく似たメッセージを送信します。

)CM SNMP sortlist
SNMP 宛先に使用するレイアウト内のアラート・メッセージを指定します。

)CM QRadar Unix syslog sortlist
Unix syslog 宛先に使用するレイアウト内のアラート・メッセージを指定します (例: IBM QRadar SIEM の zAlert DSM 用の Log Event Extended Format (LEEF) で指定)。

)CM ArcSight CEF
HPE Security ArcSight CEF 製品が使用する、共通イベント・フォーマット (CEF) に準拠するアラート・メッセージを指定します。

)CM WTO sortlist
コンソールに送るレイアウト内のアラート・メッセージを指定します。

)CM Action command
通常、これには、アクション・コマンドを指定できるように、次の 2 つの組み込みステートメントが含められます。

```
)IM C2PSACTX
)IM C2PSACTS
```

これら 2 つの)IM ステートメントを使用する場合、ISPF パネル・インターフェースで構成されている EXCLUDE ステートメントおよび COMMAND ステートメントが自動的に挿入されます。

148 ページの『アラート定義 -「Specify action」』を参照してください。

)CM Command
このコマンド・セクションの使用は非推奨になりました。既存のスケルトン・メンバー内には引き続き出現する可能性があります。

使用しないメッセージ・フォーマットを指定する必要はありません。ただし、そのフォーマットで使用されたアラートを認識できるよう、各セクションに少なくともアラート ID を保持しておくことができます。アラート ID の部分は、&c2pemem. スケルトン変数が現れる位置で認識できます。

実際の各 CARLa セクションは、)SEL と)ENDSEL のスケルトン・ディレクティブによって区切られていて、1 つ以上の)IM ディレクティブもあります。これらのディレクティブを変更してはなりません。

以下のマニュアルのセクションでは、それぞれの CARLa セクションについて詳しく説明します。スケルトンの変更が済んだら、PF3 を押してアラート・パネルに戻ります。アラートを追加した場合は、それが自動的に選択されます。PF3 をさらに 2 回押すと、アラート構成パネルに戻ることができ、そこで **V** (検査) コマンドを発行して、新しいアラートを検査できます。検査が正常に完了すると、**F** (リフレッシュ) コマンドを入力して、新しいアラートを活動化することができます。

ID セクション

zSecure Alert が生成するアラート・メッセージのレイアウトは、受信側とメッセージ・タイプに応じて異なります。Eメール・メッセージは、件名で始まり、通常、メール・ヘッダー行の情報を繰り返し、フィールドのリストに続きます。その他の場合 (SYSLOG アラートや CEF フォーマットのアラートなど)、アラート・メッセージはアラートの最終行、データ・フィールドの後にあります。

アラートのスケルトンを保守しやすくするために、zSecure Alert には、SORTLIST コマンドの一部 (人間が読むメッセージを部分的に含む) を構築するメッセージ・フォーマット・スケルトンC2PSFMSG が含まれています。これらの共通フィールドを指定するために使用できる次の 3 つのダイアログ変数があります。

C2PXNAME
: Unix SYSLOG メッセージと CEF メッセージで、イベントを分類するために使用されるイベント名を表します。引用符なしの短い固定値にする必要があります。

C2PXMSG
: すべてのアラートに含めるアラート・メッセージ・テキスト (引用符で囲んだリテラルと CARLa フィールドで構成されます) を指定します。最大長は、約 200 文字です。

C2PXDES
: 携帯電話メッセージと WTO メッセージ以外のすべてのアラートに含めるイベントの説明を指定します。最大長は、約 450 文字です。

```
)SETF C2PXNAME = &STR(Event_name)
)SETF C2PXMSG = &STR('Alert msg about' user(0))
)SETF C2PXDES = &STR('Alert description')
```

これらの割り当てでは、テキスト・ストリングを引用符で囲むために &STR(*text*) を使用します。割り当ての末尾に閉じ括弧を指定するのを忘れないでください。すべての ISPF スケルトン行にあてはまるとおり、位置 72 に ? を記述することで、値を以降の行に続けることができます。それ以外の場合、位置 72 は空のままにしてください。

C2PXMSG と C2PXDES は、CARLa リテラル、フィールド、および SORTLIST コマンドと SUMMARY コマンドで通常受け入れられる句読法を受け入れます。リテラルには、図示したとおり、単一引用符を使用する必要があります。出力修飾子にスペースを使用しないでください。代わりにコンマを使用してください。値内で継続文字としてコンマを追加する必要はありません。C2PSFMSG によって自動的に追加されます。

通常の CARLa 修飾子以外に、メッセージ・トークンとして次の疑似修飾子も使用できます。

T E メールと携帯電話のタイトルにのみトークンを含めます。

NOT E メールと携帯電話のタイトルからトークンを除外します。

V 携帯電話と WTO 宛先に対して生成された詳細メッセージにのみトークンを含めます。

NOV E メール、SNMP、QRadar Unix syslog 、および ArcSight CEF の各宛先に対して生成された非詳細メッセージにのみトークンを含めます。

WTO WTO 宛先に対して生成されたメッセージにのみトークンを含めます。

NOWTO
WTO 宛先に対して生成されたメッセージのトークンを除外します。

ACF2 ACF2 システムに対してのみトークンが生成されます。

RACF RACF システムに対してのみトークンが生成されます。

C2PXMSG 割り当て内の T 修飾子は、メッセージのヘッダー・セクションのフィールドを抑止するのみでなく、「Subject: 値」にそのフィールドが含まれている CARLa ステートメントに T 修飾子を渡します。

トークンには、フィールド、リテラル・ストリング、連結記号 (|)、または改行記号 (/) を使用できます。同じ括弧のセット内に疑似修飾子と CARLa 修飾子を混用できます。C2PSFMSG は、E メールと携帯電話のタイトルから一部の禁止修飾子 (0、HOR、WRAP、WORDWRAP、および WW) を自動的に削除します。これらの修飾子の例は、次のアラート 1105 にあります。

```
)SETF C2PXNAME = &STR(Grant_Privilege_System)
)SEL &C2PESECP = RACF
)SETF C2PXMSG = &STR('System authority'                                  ?
spec(0,V,NOT) |(V,NOT) oper(0,V,NOT) |(V,NOT)                            ?
audi(0,V,NOT) |(V,NOT) clau(0,V,NOT) |(V,NOT)                            ?
'granted to' racfcmd_user(0)                                             ?
'by'(V) user(0,V))
)SETF C2PXDES = &STR('System-level authority granted to user')
)ENDSEL
)SEL &C2PESECP = ACF2
)SETF C2PXMSG = &STR('System authority'                                  ?
secu(0,V,NOT) |(V,NOT) read(0,V,NOT) |(V,NOT) nonc(0,V,NOT) |(V,NOT)     ?
'granted to'  acf2_rulekey(8,T) acf2_rulekey(0,NOT)                      ?
'by'(V) user(0,V))
)SETF C2PXDES = &STR('System-level authority granted to user')
)ENDSEL
```

メッセージ・ヘッダーをさらにカスタマイズするために、メンバー C2PXFMSG を使用できます。このメンバーが C2PCUST 内に存在する場合、受信者ごとに構築されるメッセージ・ヘッダーの接頭部の後に、メッセージ・フォーマット・スケルト

ン (C2PSFMSG) から含められます。必要に応じて、)SETF ステートメントを C2PSFMSG から C2PXFMSG にコピーして調整できます。例えば、各 E メールの件名の先頭にシステム ID を含めるには、次のように C2PXFMSG を指定します。

```
)SEL &C2PERCTP = MAIL
)SETF C2PXSUB1 = &STR('Alert on'(t) system(t) | ':'(t))
)ENDSEL
```

注: C2PXSUB1 は、C2PSFMSG で使用される件名の先頭に対する変数であり、デフォルトで 'Alert:'(t) に設定されます。

フォーマットがデータ・ソースによって異なる場合は、&C2PENEWL の値内の NEWLIST タイプをさらに調べることができます。

環境依存の選択

アラート構成で環境依存の選択基準を使用したい場合は、「**)CM Pass one query**」セクションに入力する必要があります。

次の例は、IBM Security zSecure 提供アラート 1204 および 2204 のスケルトン・メンバー C2PS1204 からのものです。これは、NEWLIST TYPE=SENSDSN の DSN フィールドと APF フラグ・フィールドを使用して、現在 APF リストに含まれているデータ・セットを見つける stage1 照会を示しています。詳しくは、「*IBM Security zSecure: CARLa* コマンド・リファレンス」を参照してください。これらのデータ・セット名は、置換されて別の CARLa 照会に組み込まれます。そうでない場合、この照会は引用符に囲まれているため、このまま出力ファイルへコピーされ、レポート作成ステップの照会の開始点になります。

```
  )CM Pass one query
  )SEL &C2PEPASS = Y
  n type=system outlim=1 nopage
  sortlist,
    "n type=smf name=uapf1204 outlim=0" /,
  )SEL &C2PESECP = RACF
    " select event=access(allowed) intent>=update likelist=recent," /,
  )ENDSEL
  )SEL &C2PESECP = ACF2
    " select likelist=recent acf2_subtype=D," /,
    " acf2_access=(OUTPUT,UPDATE,INOUT,OUTIN,OUTINX)," /,
    " acf2_descriptor=LOGGING,
  )ENDSEL
    "        dsn=(,"
n type=sensdsn nopage
  select apf
  sortlist,
    "           " dsn(0) | ","
  n type=system outlim=1 nopage
  sortlist,
    "            )" /,
    " sortlist ''"
      [...]
  )ENDSEL
```

生成された照会には、生成された N (Newlist) ステートメント上の NAME キーワードによって、UAPF1204 の名前が付きます。これにより、アラート条件はこの名前を参照できます。NAME は、他のアラートで指定されたフィルターとの名前の競合を避けるために、アラート ID で終わります。

生成された照会は、事前選択専用であるため、出力を生成する必要がないことを意味する OUTLIM=0 を指定しています。事前選択は、以下のシチュエーションにおける SMF レコード用です。

- システムから取得された APF データ・セット用
- RACF システムの場合: EVENT=ACCESS(ALLOWED) INTENT>=UPDATE 用
- ACF2 システムの場合: ACF2_SUBTYPE=D ACF2_ACCESS= (OUTPUT|UPDATE|INOUT|OUTIN|OUTINX) 用

さらに、LIKELIST=RECENT 節は、選択を現行のレポート作成間隔中に書き込まれた SMF レコードだけに制限しています。次のセクションでは、選択に結合する SMF および WTO 入力データを指定するために、常時使用できる事前選択フィルターについて説明します。

拡張モニター COMPAREOPT

拡張モニター・アラートは、SMF や WTO 以外の NEWLIST タイプをレポートに使用します。これらは、COMPAREOPT を使用してシステム値の変更を識別したり、アラート条件を識別するために他の選択肢を含めたりできます。アラートが変更によってトリガーされる場合、COMPAREOPT ステートメントを使用してトリガーする変更内容を定義する必要があります。モデル・スケルトンには以下のセクションが含まれています。

```
)CM Extended Monitoring COMPAREOPT
)SEL &C2PEEMCO = Y
)SET C2PEEMCO  = N
)CM  Set C2PENCMP so COMPAREOPT name is included in newlist commands
)SET C2PENCMP = alrt&c2pemem
)CM  Insert COMPAREOPT here if needed for EM alert
 compareopt name=&c2pencmp,
            .....
)CM  Remove )SET and COMPAREOPT if this alert does not use COMPAREOPT
)ENDSEL
```

これまでのリリースの zSecure Alert では、必須の COMPAREOPT ステートメントはメンバー C2PSGLOB に含まれ、対応する COMPAREOPT パラメーターはアラートの指定パネルに含まれていました。次の COMPAREOPT の例は、アラート 1207 のグローバル・スケルトン・メンバー C2PSGLOB からのものです。

```
)CM Extended Monitoring CompareOpt
)SEL &C2PEEMCO = Y
)SET C2PEEMCO  = N
)SET C2PENCMP = alrt&c2pemem
 compareopt name=&c2pencmp,
     type=sensdsn,
     base=(complex=base),
     by=(dataset),
     compare=(volser,apf,apflist),
     show=add
)ENDSEL
```

ここで、

- この COMPAREOPT の例の *name* は alrt1207 に設定されており、名前の競合を避けるためにアラート ID が含まれています。名前は、&C2PENCMP に保存され、以降の NEWLIST コマンドに渡されます。
- type の値は、 42 ページの図 18 の「**Data source**」フィールドの値に一致します。

- by の値は、基本環境と現在の環境とで比較される項目を一意的に識別するフィールドを指定します。
- compare の値は、そのような項目のどの属性を比較対象とするかを指定します。
- show=add は、データ・セットが追加された場合にのみアラートがトリガーされることを示します。

拡張モニターを COMPAREOPT なしで使用する場合は、COMPAREOPT コマンドと、&C2PENCMP の割り当てを削除してください。

COMPAREOPT の指定について詳しくは、以下の資料を参照してください。

- ご使用の zSecure 製品の「*zSecure (Admin and) Audit* ユーザー・リファレンス・マニュアル」の『比較処理』セクション
- 「*zSecure CARLa* コマンド・リファレンス」の COMPAREOPT コマンドに関する情報

アラート条件

アラートを発行したい時期を示すには、「**)CM Alert condition**」セクションに入力する必要があります。次の例は、IBM Security zSecure 提供アラート 1204 および 2204 のスケルトン・メンバー C2PS1204 から取ったものです。この選択全体は、既に UAPF1204 という名前の事前選択で完了しています。この事前選択は、前のセクションで示したように、そのアラートの環境依存選択によって生成されたものです。

```
)CM Alert condition
)SEL &C2PEPASS = N
)IM C2PSGNEW
  select likelist=uapf1204
```

)IM ディレクティブによって組み込まれたスケルトン・メンバー C2PSGNEW は、選択基準用の CARLa NEWLIST ステートメントを生成します。)IM ステートメントの後に、DEFINE および SELECT ステートメントを入力できます。

LIKELIST キーワードは、先行する NEWLIST を参照し、これは、同じ値を持つ NAME キーワードを持っています。したがって、その NEWLIST からの有効な選択は、節として使用されます。この場合、それは唯一の節なので、まったく同じ選択が使用されます。アラート内で使用されるフィルターは、他のアラートとの名前の競合を避けるために、アラート ID で終わることができます。以下のグローバル事前選択フィルターと、アラート自体の中で定義されたフィルターのみを見てください。他のアラート内でのフィルターの参照が、整合するかしないかの保証はありません。

アラート条件は、どの SMF および WTO 入力を直接または間接的にモニターするかを示すために、常にグローバル事前選択フィルターに結合されている必要があります。この場合、UAPF1204 事前選択は既に RECENT 事前選択フィルターに結合されているため、この条件は間接的に満たされています。グローバル事前選択フィルターは、次のリストから選択できます。

likelist=recent
: 現行のレポート作成間隔中に書き込まれた最新の SMF レコードに結合します。

likelist=history
「平均化」インターバル中に書き込まれた「移動ウィンドウ」分析 SMF レコードに結合します。**recent** と **history** の間にオーバーラップはありません。

likelist=wtorec
現行のレポート作成間隔中に書き込まれた最新の WTO メッセージに結合します。

likelist=wtohis
「平均化」インターバル中に書き込まれた「移動ウィンドウ」分析 WTO メッセージに結合します。**wtorec** と **wtohis** の間にオーバーラップはありません。

このリストは、グローバル・スケルトン C2PSGLOB に適用されます。

注**:** 必要であれば、アラート構成に別のグローバル・スケルトンを使用できます。

これらの事前選択では、多くの場合、SMF レコードの TYPE および SUBTYPE、または WTO の MSGID に対する選択がさらに必要になります。例えば、SELECT likelist=wtorec MSGID(CSV410I) や SELECT likelist=recent type=42 です。

拡張モニター・アラートの場合、アラート条件には complex の選択のみが必要です。複合システム名 BASE および CURRENT は必須です。一部のアラートでは、追加の選択基準が必要な場合があります。例えば、アラート 1207 で COMPAREOPT を使用すると、SENSDSN newlist を使用することが指定されます。アラートの適用対象は APF データ・セットのみであるため、select ステートメントは追加の基準で拡張されます。以下のようになります。

```
select complex=(base,current) and (apf=yes or apflist=yes)
```

インストール定義アラートの場合、比較対象のフィールドを指定する COMPAREOPT ステートメントは、アラートのスケルトンの 52 ページの『拡張モニター COMPAREOPT』 セクションで定義されます。

永続的なダイアログ変数 &C2PENSEL は、それぞれのアラートのスケルトンが評価される前にクリアされます。これを使用して、スケルトンの一部を 1 回アクティブにし、以降の受け渡しではスキップできます。DEFINE コマンドを持つ C2PSSHAR スケルトンを 1 回のみ埋め込む必要があるアラート 1503 などで使用できます。

```
)SEL &C2PENSEL = &Z
)SET C2PENSEL = ShareIncluded
)IM C2PSSHAR
)ENDSEL
```

C2PCUST メンバー C2PXINIT に ISPF ダイアログ変数を設定することもできます。This member is imbedded one time at このメンバーは、コマンド生成ステージ (ステージ 1。レポート、および拡張モニター) の開始時に 1 回埋め込まれます。

アクションの指定

ISPF ユーザー・インターフェースでは、埋め込みパネルを使用してアクション・コマンドを柔軟に指定できます。これらのコマンドは、「**Action specification**」セクションで次の 2 つの組み込みステートメントを使用すると、自動的に処理されます。

```
)IM C2PSACTX
)IM C2PSACTS
```

ISPF パネルを使用してアクション・コマンドを入力する方法について詳しくは、148 ページの『アラート定義 -「Specify action」』を参照してください。

E メール・レイアウト

IBM Security zSecure 提供アラートには、 64 ページの『標準 E メール・レイアウト』に示すような共通レイアウトがあります。次の例は、アラート 1302 を示しています。

```
)CM EMAIL sortlist
)SEL &C2PERCTP = MAIL
 sortlist,
  recno(nd),
)IM C2PSFMSG
  / '   Alert id        &c2pemem;',
  / '   Date and time'(18) date(9) time(11),
  / '   Program'(18) resource,
  / '   Data set'(18) dataset,
  / '   User'(18) user(8) name,
  / '   Job name'(18) jobname,
  / '   System ID'(18) system,
  / '   Audit reason'(18) reason(0,explode,ww,hor),
  / /
)ENDSEL
```

注: メッセージ・フォーマット・スケルトン C2PSFMSG は、次のように C2PXMSG と C2PXDES の値を拡張します。

```
'Alert: Audited program'(t) resource(t,8) 'has been executed'(t),
'Alert: Audited program' resource(0) 'has been executed' /,
'A program with auditing specified has been executed' /,
```

タイトル修飾子 (t) は、E メールの件名を設定するために使用されます。フィールド recno(nd) は、SMF レコード番号によって、アラート E メールをオリジナルの順序に、番号を実際には表示せずに維持します。

典型的な拡張モニター・アラートは、変更されたオブジェクト (設定) を識別するキー・フィールドの一部を参照します。例えば、アラート 1207 には、以下のように、データ・セットおよび volser (ボリューム通し番号) に対する参照が含まれています。

```
)SEL &C2PERCTP = MAIL
 sortlist ,
)IM C2PSFMSG
  / ' Alert id &c2pemem.',
  / ' Date and time ' collect_datetime,
  / ' Data set ' dataset,
  / ' Volume ' volser,
  / ' APF ' APF,
```

```
  / ' APFLIST ' APFLIST,
  / ' System ID ' system
/ /
)ENDSEL
```

拡張モニター・アラートは、変更されたフィールドの一部を参照することもできます。これは、COMPARE_RESULT および COMPARE_CHANGES の変数を使用して行うこともできます。このような定義済み変数の使用例は、以下のようにアラート 1609 に見られます。

```
)SEL &C2PERCTP = MAIL
 sortlist ,
)IM C2PSFMSG
  / '   Alert id &c2pemem.',
  / '   Date and time             ' collect_datetime,
  / '   Changed field' comp_change(cmpchgc,hor,0),
  / '   Stack ' stack(0),
  / '   System ID ' system(0)
  / /
)ENDSEL
```

変数 *comp_change* の定義は、アラート・スケルトンの Extended Monitoring COMPAREOPT セクション内で行えます。変数の定義について詳しくは、「*zSecure CARLa* コマンド・リファレンス」の『比較結果用変数 (COMPAREOPT) の定義』を参照してください。

テキスト・メッセージ・レイアウト

「**)CM Cellphone sortlist**」セクションで、テキスト・メッセージの宛先用にアラート・メッセージのレイアウトを指定できます。受信テキスト・メッセージが件名と E メールの本体のどちらから取得されるかは、使用している、E メールからテキスト・メッセージへのゲートウェイによって決まります。すべての IBM Security zSecure 提供アラートは、件名と本体の両方の中で、よく似たメッセージを送信します。次の例は、アラート 1204 を示しています。

```
)CM Cellphone sortlist
)SEL &C2PERCTP = CELL
sortlist,
recno(nd),
)IM C2PSFMSG
)ENDSEL
```

)IM コマンドの後には CARLa フィールドがないことに注意してください。

SNMP レイアウト

「**)CM SNMP sortlist**」セクションで、SNMP 宛先用のアラート・メッセージのレイアウトを指定できます。このレイアウトでは、変数とその内容の組み合わせを指定します。 163 ページの『付録 A. SNMP 出力』 も参照してください。次の例は、アラート 1204 を示しています。

```
)CM SNMP sortlist
)SEL &C2PERCTP = SNMP
   [...]
sortlist,
 recno(nd),
 '&c2pemem.' /,
 'eventIntegral',
)IM C2PSFMSG
 'eventWhen' datetime(datetimezone,0) /,
 'onWhatDSNAME' dataset(0,hor) /,
```

```
 'onWhatGRANTED' intent /,
 'onWhatALLOWED' access /,
 'onWhatINTENT' intent /,
 'whoUSERID' userid(0) /,
 'whoNAME' name(0) /,
 'whatDESC' desc(0,explode) /,
 'whatJOBNAME' jobname(0) /,
 'whereSYSTEM' system(0)
)ENDSEL
```

QRadar Unix syslog のレイアウト

「**)CM QRadar Unix syslog sortlist**」セクションで、SYSLOG 宛先用のアラート・メッセージのレイアウトを指定できます。このメッセージ・フォーマットは、IBM QRadar SIEM 内の zAlert DSM 用に設計されていますが、他の SYSLOG レシーバーが処理できます。次の例は、アラート 1204 を示しています。

```
)CM QRadar Unix syslog sortlist
)SEL &C2PERCTP = SYSL
)SEL &C2PESECP = RACF
 sortlist,
  recno(nd) '<&C2PEPRIO.>' | datetime(cef_dt,15),
  system 'C2P&c2pemem.',
  '[C2P&C2PEMEM.',
  'onWhatDSNAME="' | dataset(0,firstonly) | '"',
  'onWhatGRANTED="' |  intent(0) | '"',
  'onWhatALLOWED="' | access(0) | '"',
  'onWhatINTENT="' |  intent(0) | '"',
  'whoUSERID="' | userid(0) | '"',
  'whoNAME="' | user:pgmrname(0) | '"',
  'whatACTION="&C2PXNAME"',
  'whatDESC="' | desc(0,explode) | '"',
  'whatJOBNAME="' | jobname(0) | '"',
  'whereSYSTEM="' | system(0) | '"]',
)IM C2PSFMSG
)ENDSEL
```

)IM コマンドの後には CARLa フィールドがないことに注意してください。

ArcSight CEF のレイアウト

「**)CM ArcSight CEF sortlist**」セクションで、共通イベント・フォーマット (CEF) 宛先用のアラート・メッセージのレイアウトを指定できます。次の例は、アラート 1604 を示しています。

```
)CM ArcSight CEF
)SEL &C2PERCTP = CEF
 sortlist,
  recno(nd) datetime(cef_dt,15),
  :run.system(4),
  'CEF:0|IBM|zSecure Alert|2.3.0|C2P&c2pemem.|' |,
  '&C2PXNAME.|&C2PECEFP.|' |,
  'dvchost=' | :run.system(0),
  'cs1=' | MsgTxt1(0),
         | MsgSep2 | MsgTxt2(0),
         | MsgSep3 | MsgTxt3(0),
         | MsgSep4 | MsgTxt4(0),
         | MsgSep5 | MsgTxt5(0),
         | MsgSep6 | MsgTxt6(0),
         | MsgSep7 | MsgTxt7(0),
         | MsgSep8 | MsgTxt8(0),
         | MsgSep9 | MsgTxt9(0),
  'cs1Label=ConsoleMsg',
  'outcome=Failure',
```

```
  'rt=' | datetime(cef_dtz,34),
  'msg=' |,
)IM C2PSFMSG
)ENDSEL
```

)IM コマンドの後には CARLa フィールドがないことに注意してください。

コマンド・セクション

RACF システムの場合、ISPF CARLa スケルトンの **)CM Command** セクションで、アラート条件が発生したときに発行するコマンドをオプションとして指定できます。このコマンド・セクションの使用は非推奨になりました。ISPF ユーザー・インターフェースでは、埋め込みパネルを使用してアクション・コマンドを柔軟に指定できます。これらは、「**Action specification**」セクションを使用すると、自動的に処理されます。

第 3 章 事前定義アラート

この章では、zSecure Alert に添付されているアラートについて説明します。「クラス」列の説明については、 7 ページの『アラート活動化に関するガイドライン』を参照してください。以下の表では、「重大度」列の意味について説明します。ID が 1000 から 1999 の範囲内にあるアラートは RACF アラートで、2000 から 2999 の範囲内にあるアラートは ACF2 アラートです。

表 6. 事前定義アラート

ID	説明	クラス	重大度
1001	ハートビート・イベント (その発信元が稼働中であることを示す)	3	0
1101	不明ユーザーによるログオン	2	3
1102	緊急時ユーザー ID を使用したログオン	1(*)	3
1103	UID(0) を持つユーザー ID (UNIX スーパーユーザー) のログオン	2	2
1104	パスワードによる高い許可レベルのユーザーの取り消し	2	3
1105	システム権限の認可	2	3
1106	システム権限の除去	3	2
1107	グループ権限の認可	2	2
1108	グループ権限の除去	3	2
1109	非 SPECIAL ユーザーによる SPECIAL 権限の使用	1	2
1110	非 OPERATIONS ユーザーによる OPERATIONS を使用したデータ・セットへのアクセス	1	3
1111	無効なパスワード試行の制限の超過	2	3
1112	パスワード・ヒストリーのフラッシュ	2	3
1113	疑わしいパスワード変更	3	2
1114	CREATE 以上の接続権限の設定	2	2
1115	違反が多すぎる	1	3
1119	無期限パスワードの有効化	2	2
1120	主要管理アクティビティー	2	2
1121	保護状況の削除	2	2
1122	機密性の高いユーザー ID を使用したログオン (発行元: C2PACMON)	1(*)	3
1201	データ・セットでの WARNING モード・アクセス	1	2
1202	DATASET プロファイルで設定された公開アクセス権限 >= UPDATE	2	3
1203	DATASET プロファイルで設定された公開アクセス権限 > NONE	3	2
1204	APF データ・セットでの更新	2	2
1205	SETPROG を使用した APF リストへのデータ・セットの追加	2	3

表 6. 事前定義アラート (続き)

ID	説明	クラス	重大度
1206	SETPROG を使用した APF リストからのデータ・セットの除去	2	2
1207	APF リストへのデータ・セットの追加の検出	2	3
1208	APF リストからのデータ・セットの除去の検出	2	2
1209	PCI PAN データへの不定期アクセス	2	2
1210	平文の PCI PAN データへの不定期アクセス	2	2
1211	PCI AUTH データへの不定期アクセス	2	2
1212	機密データ・セットに対するアクセス>=READ	2	2
1213	機密データ・セットに対するアクセス>=UPDATE	2	2
1214	UPDATE 機密メンバーに対するアクション	2	2
1215	DATASET プロファイルで設定された WARNING モード	1	3
1216	DATASET プロファイルで変更された LEVEL 値	3	2
1301	STC 用の包括的プロファイルの使用	3	2
1302	監査対象プログラムの実行	3	2
1303	一般リソースでの WARNING モード・アクセス	1	2
1304	一般リソース・プロファイルで設定された公開アクセス権限 > NONE	2	3
1305	一般リソース・プロファイルで設定された WARNING モード	1	3
1306	STC への「トラステッド」または「特権あり」の割り当て	2	3
1307	一般リソース・プロファイルで変更された LEVEL 値	3	2
1401	UNIX ファイル・アクセス違反	3	2
1402	ファイル・アクセスの変更時のグローバル書き込みの指定	2	3
1403	ファイル・アクセスの変更時のグローバル読み取りの指定	3	2
1404	拡張属性の変更 (1409 に置き換えられました)	2	2
1405	監査対象 UNIX プログラムの実行	3	2
1406	スーパーユーザー特権のある UNIX プログラムの実行	2	2
1407	ユーザーがスーパーユーザー特権のあるシェルを取得	2	2
1408	UNIX プログラムでのスーパーユーザー特権の設定	2	2
1409	拡張属性の変更	2	2
1410	UID(0) の割り当て	2	3
1411	BPX.SUPERUSER に対する許可の実行	2	3
1501	グローバル・セキュリティー対策の活動化	3(**)	2
1502	グローバル・セキュリティー対策の非活動化	1(*) (**)	4
1503	グローバル・セキュリティー対策またはオプションの変更	1	3
1504	RACF リソース・クラスの活動化	2	2

表 6. 事前定義アラート (続き)

ID	説明	クラス	重大度
1505	RACF リソース・クラスの非活動化	2	3
1506	グローバル・アクセス検査テーブルの変更	2	2
1507	動的クラス記述子テーブルの変更	2	2
1508	SETPROG EXIT による Command Verifier の非活動化	1(*)	3
1601	SMF データ損失の開始	1(*)	5
1602	障害の後の SMF ロギングの再開	3	2
1603	SVC 定義の変更	2	3
1604	IBM Health Checker による重大度が低レベルの問題の検出	3	2
1605	IBM Health Checker による重大度が中レベルの問題の検出	2	3
1606	IBM Health Checker による重大度が高レベルの問題の検出	1	4
1607	SMF レコードのフラッドの検出	1	4
1608	SMF レコードのフラッドによるレコードのドロップの開始	1	5
1609	フィルター規則によってブロックされたアタックがログに記録されなくなった	2	2
1610	デフォルト・フィルター規則によってブロックされたアタックがログに記録されなくなった	3	2
1611	特定の SMF 119 レコードが書き込まれなくなった - 監査証跡は不完全	1	3
1612	IPv4 または IPv6 フィルター処理サポートおよび IPSec トンネル・サポートの非活動化	1	4
1613	1024 未満の TCP または UDP ポートが予約されなくなった	1	4
1614	インターフェースのセキュリティー・クラスの変更	2	2
1615	IP フィルター規則の変更	2	2
1701	重要なグループへの接続	2	3
1801	zSecure Access Monitor が非アクティブ	2	3
1802	zSecure サーバー接続の逸失	2	3
1804	IBM Workload Scheduler ジョブが開始されていない	2	3
1805	IBM Workload Scheduler ジョブの遅延	2	3
1806	IBM Workload Scheduler ジョブの失敗	2	3
2001	ハートビート・イベント (その発信元が稼働中であることを示す)	3	0
2102	緊急時ユーザー ID を使用したログオン	1(*)	3
2104	パスワードによる高い許可レベルのユーザーの取り消し	2	3
2105	システム権限の認可	2	3
2106	システム権限の除去	3	2
2111	ユーザーに対する無効なパスワード試行の制限の超過	2	3

表 6. 事前定義アラート (続き)

ID	説明	クラス	重大度
2112	パスワード・ヒストリーのフラッシュ	2	3
2113	疑わしいパスワード変更	3	2
2115	違反が多すぎる	1	3
2116	非 SECURITY ログオン ID による SECURITY 権限の使用	1	2
2117	非 NON-CNCL ログオン ID による NON-CNCL 権限の使用	1	3
2118	非 READALL ログオン ID による READALL 権限の使用	1	3
2119	無期限パスワードの有効化	2	2
2120	主要管理アクティビティー	2	2
2201	データ・セットでの WARNING モード・アクセス	1	2
2204	APF データ・セットでの更新	2	2
2205	SETPROG を使用した APF リストへのデータ・セットの追加	2	3
2206	SETPROG を使用した APF リストからのデータ・セットの除去	2	2
2207	APF リストへのデータ・セットの追加の検出	2	3
2208	APF リストからのデータ・セットの除去の検出	2	2
2209	PCI PAN データへの不定期アクセス	2	2
2210	平文の PCI PAN データへの不定期アクセス	2	2
2211	PCI AUTH データへの不定期アクセス	2	2
2212	機密データ・セットに対するアクセス>=READ	2	2
2213	機密データ・セットに対するアクセス>=UPDATE	2	2
2214	UPDATE 機密メンバーに対するアクション	2	2
2301	STC 用のデフォルト STC ログオン ID の使用	3	2
2407	ユーザーがスーパーユーザー特権のあるシェルを取得	2	2
2409	拡張属性の変更	2	2
2501	グローバル・セキュリティー対策の追加	3	2
2502	グローバル・セキュリティー対策の削除	1 (*)	4
2503	グローバル・セキュリティー対策またはオプションの変更	1	3
2601	SMF データ損失の開始	1(*)	5
2602	障害の後の SMF ロギングの再開	3	2
2603	SVC 定義の変更	2	3
2604	IBM Health Checker による重大度が低レベルの問題の検出	3	2
2605	IBM Health Checker による重大度が中レベルの問題の検出	2	3
2606	IBM Health Checker による重大度が高レベルの問題の検出	1	4

表 6. 事前定義アラート (続き)

ID	説明	クラス	重大度
2607	SMF レコードのフラッドの検出	1	4
2608	SMF レコードのフラッドによるレコードのドロップの開始	1	5
2609	フィルター規則によってブロックされたアタックがログに記録されなくなった	2 (***)	2
2610	デフォルト・フィルター規則によってブロックされたアタックがログに記録されなくなった	3 (***)	2
2611	特定の SMF 119 レコードが書き込まれなくなった - 監査証跡は不完全	1 (***)	3
2612	IPv4 または IPv6 フィルター処理サポートおよび IPSec トンネル・サポートの非活動化	1 (***)	4
2613	1024 未満の TCP または UDP ポートが予約されなくなった	1 (***)	4
2614	インターフェースのセキュリティー・クラスの変更	2 (***)	2
2615	IP フィルター規則の変更	2 (***)	2
2802	zSecure サーバー接続の逸失	2	3
2804	IBM Workload Scheduler ジョブが開始されていない	2	3
2805	IBM Workload Scheduler ジョブの遅延	2	3
2806	IBM Workload Scheduler ジョブの失敗	2	3

(*) このアラートが発行された場合、迅速な応答が必要です。

(**) このアラートはアラート 1503 に含まれているため、両方のアラートで同じ受信側が設定されている場合、このアラートを活動化してもあまり意味がありません。

(***) このアラートのクラスおよび重大度は、対応する RACF アラートのクラスおよび重大度と同じです。

「重大度」列に、IBM Tivoli NetView でアラートに関連付けている重大度レベルをリストします。重大度レベルの範囲は、以下に示すように 0 から 5 です。

表 7. *NetView* での重大度レベル

重大度	**NetView** での意味
0	クリア
1	不確定
2	警告
3	マイナー・エラー
4	クリティカル
5	メジャー

アラートは、以下のさまざまなフォーマットで使用可能なアラート・メッセージによって伝達されます。

- E メール

- テキスト・メッセージ
- WTO
- SNMP トラップ
- QRadar Unix syslog
- 共通イベント・フォーマット (CEF) の HPE Security ArcSight

5 ページの『概要』を参照してください。

サンプルの E メールおよびテキスト・メッセージを、個々の事前定義アラートとともに、この章で示します。SNMP トラップ・フォーマットについては、163 ページの『付録 A. SNMP 出力』に説明があります。

この章の残りの部分では、E メール・フォーマットの一般レイアウトについて説明し、事前定義アラートを機能カテゴリーに分けて詳細に説明します。アラートを構成できる場合、そのアラートについてここで説明します。

アラートごとに、特定の SMF レコード・タイプをログに記録するか、特定の WTO メッセージを発行する必要があります。ほとんどの事前定義アラートで、SMF タイプ 80、RACF 処理が必要です。これらの SMF タイプをログに記録するものと想定しています。その他のすべての要件を、個々のアラートとともに示します。SMF ロギングは、サブシステムごとに制御されます。

標準 E メール・レイアウト

すべての E メール・アラート・メッセージの出力は似ています。以下に示す送信可能な E メールの例を参照してください。

```
From:    C2POLICE at DINO
Subject: Alert: Audited program ASMIDFA  has been executed

Alert: Audited program ASMIDFA has been executed
A program which auditing specified has been executed

   Alert id        1302
   Date and time   07Feb2003 13:44:43.20
   Program         ASMIDFA
   Data set        SHARED.LINKLIB
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
```

ここで、データ・セット SHARED.LINKLIB の ASMIDFA というプログラムの実行が開始されたことが分かります。プログラムを実行したユーザーは C##BDV2 で、ユーザー名は *Dionne Vont* です。プログラムは、システム DINO でジョブ C##BDV2 において実行されます。

E メールの送信側は、インターフェースを使用して構成できます。デフォルトは、*jobname* at *system name* です。E メールの件名ヘッダーおよび本文は、CARLa コードによって生成されます。E メール件名は、E メール本文の 1 行目と同じです。ただし、フォーマットが若干異なる場合があります。その行の下には、イベントについて記述する汎用ヘッダーがあります。

アラートのヘッダーの下には、詳細を示したセクションがあります。1 行目には、アラート ID が示されます。この番号は、SNMP、WTO、または SMS の出力を使

用して対応するアラートを検索したり、このドキュメンテーションで適切な項目を検索したりするのに使用できます。2 行目には、イベントが発生した日時が示されます。その後に、アラート固有のフィールドが続きます。最後に、ジョブ名、ジョブ ID、およびシステム名が入手可能であれば、それらがリストされます。

事前定義 RACF アラート

以下のトピックでは、zSecure Alert に付属する RACF アラートのカテゴリーについて説明します。

ユーザー・アラート

不明ユーザーによるログオン (1101)

このアラートは、以下の 2 つの場合にトリガーされます。

1. RACF にとって不明なユーザーが、TSO に正常にログオンした場合。このユーザーは、SYS1.UADS には定義されていますが、RACF には定義されていません。
2. このシステムに対して、別のシステムの NJE によってバッチ・ジョブが実行依頼された場合。受信側システムでは、ジョブを実行依頼したユーザーは、RACF に定義されていません。

このアラートを受信するには、SMF レコード・タイプ 30 サブタイプ 1 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Logon by unknown user

Alert: logon by unknown user
A user unknown to RACF logged on or submitted a batch job

   Alert id        1101
   Date and time   10Feb2003 06:53:16.60
   User            *
   Result          Success
   Job name + id   TSOB     JOB00042
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1101: Logon by unknown user *        job TSOB

Alert 1101: Logon by unknown user * job TSOB
```

生成された E メール・レポートには常に、ユーザーを表す「*」と、ログオンが成功したかどうかが示されます。

システムはユーザーとして「*」をログに記録するだけなので、不明なログオンのソースを検出するのが困難な場合があります。ただし、RACF に定義されていないユーザー ID が SYS1.UADS データ・セットに含まれていないことを確認できます。また、未定義ユーザーによるジョブ実行依頼を停止するために、SETROPTS JES(BATCHALLRACF) を設定できます。

緊急時ユーザー ID を使用したログオン (1102)

緊急用のユーザー ID が TSO ログオンまたはバッチ・ジョブの実行依頼に使用された場合、アラートが送信されます。

このアラートを受信するには、SMF レコード・タイプ 30 サブタイプ 1 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Emergency user IBMUSER  logged on

Alert: Emergency user IBMUSER logged on
Successful logon or job submit with a userid meant for emergencies

   Alert id        1102
   Date and time   03Feb2003 09:38:44.94
   User            IBMUSER  IBM DEFAULT USER
   Result          Success
   Job name + id   IBMUSER  TSU05900
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1102: emergency user IBMUSER  logged on

Alert 1102: emergency user IBMUSER logged on
```

生成された E メール・レポートには、システムへのログオンに使用されたユーザー ID と、ログオンが成功したかどうかが示されます。

サイトに合わせてアラートを構成できます。アラートを選択する際に、プロンプトがパネルに表示されます。使用するのは緊急時の場合のみとするユーザー ID を 10 個まで入力できます。 149 ページの『緊急時ユーザー構成 (アラート 1102 および 2102)』を参照してください。

UID(0) を持つユーザー ID (UNIX スーパーユーザー) のログオン (1103)

UNIX UID 0 のユーザー ID を使用して TSO または OMVS へのログオンが行われた場合、アラートが送信されます。スーパーユーザー特権を使用してログオンしてはならず、必要に応じて代わりに「su」を使用するというのが、UNIX での確固とした原則です。

このアラートを受信するには、SMF レコード・タイプ 30 サブタイプ 1 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Superuser C##BMR1  logon

Alert: Superuser C##BMR1 logon
A user with uid(0) has logged on

   Alert id        1103
   Date and time   03Feb2003 09:38:44.94
   User            C##BMR1  MARY ROBERTSON
```

```
   Logon to        TSO
   Result          Success
   Job name + id   C##BMR1  TSU05900
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1103: Superuser C##BMR1  logon to TSO

Alert 1103: Superuser C##BMR1 logon to TSO
```

生成された E メール・レポートには、システムへのログオンに使用されたユーザー ID、ログオンが行われたサブシステム (TSO または OMVS)、およびログオンの状況が示されます。

このアラートを受信した場合、このようなユーザーの OMVS セグメントで UID 0 定義を除去する必要があります。UNIXPRIV クラスのプロファイルおよび FACILITY クラスの BPX.SUPERUSER を使用して、ユーザーに選択的スーパーユーザー権限を付与します。

パスワードによる高い許可レベルのユーザーの取り消し (1104)

過度の無効なパスワード試行のために、システム・レベル権限 (SPECIAL、OPERATIONS、または AUDITOR) を持つユーザーが取り消された場合に、このアラートがトリガーされます。侵入者がユーザーのパスワードを推測しようとしたことが、このアラートの原因である可能性があります。

注: システム権限を持つすべてのユーザーが同時に取り消されないように注意する必要があります。SPECIAL 権限を持つ、取り消されていないユーザー ID を少なくとも 1 つ確実に復元するための何らかの手順を用意しておく必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Highly authorized user C##CX44  revoked for password violations

Alert: Highly authorized user C##CX44 revoked for password violations
System-level authorized user revoked due to excessive password attempts

   Alert id        1104
   Date and time   07Feb2003 14:58:27.13
   User            C##CX44  TEST USER
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1104: Highly authorized user C##CX44  revoked for password violations

Alert 1104: Highly authorized user C##CX44 revoked for password violations
```

レポートには、過度のパスワード違反のために取り消されたユーザー ID および付随するプログラマー名が示されます。

システム権限の認可 (1105)

ユーザーがシステム・レベル権限 (SPECIAL、OPERATIONS、AUDITOR、または CLAUTH) を取得した場合に、アラートが生成されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(USER) および SAUDIT を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: System authority granted to C##BMR2

Alert: System authority granted to C##BMR2
System-level authority granted to user

   Alert id        1105
   Date and time   29May2000 13:25:12.42
   Authority       SPECIAL
   Granted to      C##BMR2  MARY ROBERTSON
   Result          Success
   RACF command    ALTUSER C##BMR2 SPECIAL
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1105: System authority granted to C##BMR2  by C##BMR1

Alert 1105: System authority SPECIAL granted to C##BMR2 by C##BMR1
```

レポートには、認可されたシステム権限、権限を認可されたユーザー、完全な RACF コマンド、およびコマンドの結果が示されます。また、RACF コマンドを実行したユーザーも示されます。

システム権限の除去 (1106)

システム・レベル権限、すなわち、SPECIAL、OPERATIONS、AUDITOR、または CLAUTH がユーザーから除去された場合に、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(USER) および SAUDIT を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: System authority removed from C##BMR1

Alert: System authority removed from C##BMR2
System-level authority removed from user

   Alert id        1106
   Date and time   29May2000 13:25:16.15
   Authority       SPECIAL
   Removed from    C##BMR2  MARY ROBERTSON
   Result          Success
   RACF command    ALTUSER C##BMR2 NOSPECIAL
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1106: System authority removed from C##BMR2  by C##BMR1

Alert 1106: System authority SPECIAL removed from C##BMR2 by C##BMR1
```

レポートには、除去された権限、権限を除去されたユーザー、完全な RACF コマンド、およびコマンドの結果が示されます。また、RACF コマンドを実行したユーザーも示されます。

グループ権限の認可 (1107)

グループ・レベル権限、すなわち、SPECIAL、OPERATIONS、または AUDITOR がユーザーに認可された場合に、アラートが生成されます。

このアラートを受信するには、SETROPTS 設定 SAUDIT、AUDIT(USER)、または AUDIT(GROUP) を有効にする必要があります。

このアラートは、環境リフレッシュ時に RACF データベースに定義されているユーザー ID のグループ・レベル属性を使用します。コマンドによって、属性の値が環境リフレッシュ時に取得された値に設定されると、アラートは生成されません。複数の CONNECT コマンドが発行された場合、コマンドごとにアラートを受信する場合があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Group authority granted to C##ARO2  in C##C

Alert: Group authority granted to C##ARO2 in C##C
CONNECT  Group-level authority granted to user

   Alert id        1107
   Date and time   02Feb2003 09:47:23.29
   Authority       SPECIAL
   Granted to      C##ARO2  RICK OXSON
   Connected to    C##C
   Result          Success
   RACF command    CONNECT C##ARO2 AUTHORITY(USE) GROUP(C##C) NOADSP
                   NOAUDITOR NOGRPACC NOOPERATIONS OWNER(C##C) RESUME
                   SPECIAL UACC(NONE)
   User            C##BERT  ERWIN RETTICH
   Job name        CRRAC#17
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1107: Group authority granted to C##ARO2  in C##C

Alert 1107: Group authority SPECIAL granted to C##ARO2 in C##C
```

生成された E メール・レポートには、認可された権限、権限を認可されたユーザー、そのユーザーが所属するグループ、完全な RACF コマンド、コマンドの結果、およびコマンドを実行したユーザーが示されます。

注: 「RACF command」フィールドには、指定されたコマンド・キーワードおよびデフォルト・キーワードが示されるため、フィールドがかなり長くなることがあります。

グループ権限の除去 (1108)

グループ・レベル許可、すなわち、SPECIAL、OPERATIONS、または AUDITOR がユーザーから除去された場合、またはそのような許可を持つユーザーがグループから除去された場合に、アラートが生成されます。

このアラートを受信するには、SETROPTS 設定 SAUDIT、AUDIT(USER)、または AUDIT(GROUP) を有効にする必要があります。

このアラートは、環境リフレッシュ時に RACF データベースに定義されているユーザー ID のグループ・レベル属性を使用します。コマンドによって、属性の値が環境リフレッシュ時に取得された値に設定されると、アラートは生成されません。複数の CONNECT コマンドが発行された場合、コマンドごとにアラートを受信する場合があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Group authority removed for C##ARO2  in C##C

Alert: Group authority removed for C##ARO2 in C##C
Group-level authority removed from user

   Alert id        1108
   Date and time   02Feb2003 09:47:23.29
   Authority       OPERATIONS AUDITOR
   Removed from    C##ARO2  RICK OXSON
   Connected to    C##C
   Result          Success
   RACF command    CONNECT C##ARO2 AUTHORITY(USE) GROUP(C##C) NOADSP
                   NOAUDITOR NOGRPACC NOOPERATIONS OWNER(C##C) RESUME
                   SPECIAL UACC(NONE)
   User            C##BERT  ERWIN RETTICH
   Job name        CRRAC#17
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1108: Group authority removed for C##ARO2  in C##C

Alert 1108: Group authority OPERATIONS AUDITOR removed for C##ARO2 in C##C
```

レポートには、除去された権限 (または、接続が除去された場合は <CONNECT REMOVED>)、権限を除去されたユーザー、そのユーザーが所属するグループ、完全な RACF コマンド、コマンドの結果、およびコマンドを実行したユーザーが示されます。

注: 「RACF command」フィールドには、指定されたコマンド・キーワードおよびデフォルト・キーワードが示されるため、フィールドがかなり長くなることがあります。

非 SPECIAL ユーザーによる SPECIAL 権限の使用 (1109)

システムまたはグループの SPECIAL 許可を持たないユーザーが、グループまたはシステムの SPECIAL 許可を使用してコマンドを実行した場合に、このアラートが生成されます。これは、ユーザーが、グループまたはシステムの SPECIAL を必要とするコマンドを正常に実行する可能性があるが、SPECIAL 権限自体を持っていないことを意味します。この状態は、APF 許可ソフトウェアによって設定される可能性があります。

注: 原因となったプログラムを特定するための最初の試みとして、アラートが発行された時点までにジョブに関して記録された SMF レコードを分析する必要があります。

このアラートを受信するには、SETROPTS 設定 SAUDIT を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: non-SPECIAL user C##BDV1  issued SPECIAL command

Alert: non-SPECIAL user C##BDV1 issued SPECIAL command
SPECIAL authority used for RACF command by user without SPECIAL

   Alert id        1109
   Date and time   17Jan2003 03:00:16.89
   User            C##BDV1  DIONNE VONT
   RACF command    ADDSD 'SYS1.APF.NODATA.**' NOSET
   Result          Success
   Job name        C##BDV1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1109: non-SPECIAL user C##BDV1  issued SPECIAL command

Alert 1109: non-SPECIAL user C##BDV1 issued SPECIAL command ADDSD
'SYS1.APF.NODATA.**' NOSET
```

レポートには、ユーザー、ユーザーが実行した RACF コマンド、およびコマンドが成功したかどうかが示されます。

有効な許可なしにコマンドが発行された場合、SPECIAL 許可が設定された原因を調べ、それを除去する必要があります。

非 OPERATIONS ユーザーによる OPERATIONS を使用したデータ・セットへのアクセス (1110)

システムまたはグループの OPERATIONS を持たないユーザーが、グループまたはシステムの OPERATIONS 権限を使用してデータ・セットにアクセスした場合に、アラートが生成されます。これは、ユーザーが、ACL によって明示的に拒否されている場合を除き、ユーザーの範囲内のすべてのデータ・セットにアクセスできることを意味します。APF 許可プログラムが、RACF 制御ブロックにグループまたはシステムの OPERATIONS 権限を設定した場合に、この状態が生じる可能性があります。

注: 原因となったプログラムを特定するための最初の試みとして、アラートが発行された時点までにジョブに関して記録された SMF レコードを分析する必要があります。

このアラートを受信するには、SETROPTS 設定 OPERAUDIT を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: non-OPERATIONS user D##MUY   accessed data set with  OPERATIONS

Alert: non-OPERATIONS user D##MUY accessed data set with OPERATIONS
Successful data set access using OPERATIONS by user without OPERATIONS

   Alert id        1110
   Date and time   22Jan2003 10:26:16.81
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          ALTER
```

```
   User            D##MUY
   Result          Success
   Job name        D##MUY
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1110: non-OPERATIONS user D##MUY   accessed (ALTER  ) with
OPERATIONS data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 1110: non-OPERATIONS user D##MUY accessed (ALTER) with OPERATIONS
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

アラートには、アクセスされたデータ・セット、アクセス・レベル、アクセスしたユーザー、およびアクションの結果が示されます。

アクセスが有効なものでない場合、これらの OPERATIONS 許可が設定された理由を調べ、必要に応じて原因を除去する必要があります。

無効なパスワード試行の制限の超過 (1111)

特定の時間枠で 1 つの特定のユーザー ID に対して、無効なパスワードを指定して失敗したログオン試行が多すぎる場合に、アラートが送信されます。測定間隔は、REPORT オプション **Interval** および **AverageInterval** の合計です。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドに関する情報を参照してください。.

「多すぎる」とは、5 回以上と定義されます。別の制限を使用する場合、このアラートをインストール定義アラートにコピーする必要があります。新しいスケルトン・メンバーに以下のインスタンスが 7 つあります。

```
_cnt_historyInvPw1111(nd,<5), _cnt_totalInvPw1111(nd,>=5),
```

これらすべてを、5 の代わりに希望する制限を使用するように調整します。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Invalid password attempts exceed limit for C##BSG2

Alert: Invalid password attempts exceed limit for C##BSG2
Excessive number of password attempts by user

   Alert id        1111
   Date and time   03Mar2003 13:30:04.39 - 03Mar2003 13:39:23.78
   Attempts        6
   User            C##BSG2  SUSAN GAYNOR
   Result          Violation
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1111: Invalid password attempts exceed limit for C##BSG2

Alert 1111: Invalid password attempts exceed limit for C##BSG2
```

生成された E メール・レポートには、ログオン試行が行われた間隔、試行回数、システムへのログオン試行に使用されたユーザー ID、およびログオンの状況が示されます。このアラートでは、ログオンは常に違反です。

現在、ログオン試行のソース (端末) を表示することはできません。

パスワード・ヒストリーのフラッシュ (1112)

特定の時間枠で特定のユーザー ID に対するパスワードの変更回数が、パスワード・ヒストリーの SETROPTS 設定よりも多かった場合に、アラートが送信されます。これは、ユーザーがパスワード・ヒストリー全体をフラッシュし、前のパスワードを再使用できるようにしたことを意味します。測定間隔は、REPORT オプション **Interval** および **AverageInterval** の合計です。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドに関する情報を参照してください。

注**:** アラート 1112 と 1113 は関連しています。パスワード・ヒストリーのフラッシュ中にレポート作成間隔が終了した場合はアラート 1113 がトリガーされ、フラッシュが完了した場合はアラート 1112 が発生します。同じユーザーに対して複数のアラート 1113 を受信したが、アラート 1112 を受信しなかった場合も、ヒストリーのフラッシュ中と考えられます。ユーザーはフラッシュにもう少し時間を必要としていた可能性があります。

このアラートを受信するには、SETROPTS AUDIT(USER) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Password history flushed for C##BSG2

Alert: Password history flushed for C##BSG2
Repeated password changes flush password history

   Alert id        1112
   Date and time   05Mar2003 11:47:11.21 - 03Mar2003 11:47:12.04
   Pwd changes     33
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1112: Password history flushed for C##BSG2

Alert 1112: Password history flushed for C##BSG2
```

生成された E メール・レポートには、パスワード・ヒストリーのフラッシュが行われた間隔、パスワード変更回数、およびパスワード・ヒストリーをフラッシュしたユーザーのユーザー ID が示されます。

疑わしいパスワード変更 (1113)

特定の時間枠で特定のユーザー ID に対するパスワードの変更回数が多すぎるが、パスワード・ヒストリーが完全にフラッシュされる (その結果、アラート 1112 が発生する) ほど多くはない場合に、アラートが送信されます。「多すぎる」とは、5 回以上と定義されます。別の制限を使用する場合、このアラートをインストール定義アラートにコピーする必要があります。新しいスケルトン・メンバーに以下のインスタンスが 7 つあります。

```
_cnt_historyNoFlush1113(nd,<5),
_cnt_totalPwdCmd1113(nd,>=5) _cnt_totalNoFlush1113(nd),
```

これらすべてを、希望する制限を使用するように調整します。

このアラートを受信するには、SETROPTS AUDIT(USER) を有効にする必要があります。

詳細については、 73 ページの『パスワード・ヒストリーのフラッシュ (1112)』を参照してください。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Suspect password changes for C##BSG2

Alert: Suspect password changes for C##BSG2
Excessive number of password changes by user

   Alert id        1113
   Date and time   03Mar2003 15:17:12.32 - 03Mar2003 15:17:13.11
   Pwd changes     7
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1113: Suspect password changes for C##BSG2

Alert 1113: Suspect password changes for C##BSG2
```

生成された E メール・レポートには、パスワード変更が行われた間隔、パスワード変更回数、およびパスワードが何度も変更されたユーザー ID が示されます。

CREATE 以上の接続権限の設定 (1114)

接続に CREATE 以上の権限レベルが設定された場合に、アラートが送信されます。このようなレベルでは、分散管理者は、グループ・データ・セット・プロファイルを追加できます。レベルが CONNECT または JOIN の場合、ユーザーはさらに、既存のすべてのユーザーを当該のグループに接続できます。レベルが JOIN の場合、ユーザーは、サブグループを作成し、グループに対する接続権限を他のユーザーに付与することもできます。さらに、ユーザーが USER クラスでクラス権限 (CLAUTH) を持つ場合、グループに新規ユーザーを作成することもできます。

このアラートを受信するには、少なくとも SETROPTS 設定 AUDIT(USER) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Connect authority JOIN    set for C##BSG2  in C##B

Alert: Connect authority JOIN set for C##BSG2 in C##B
High authority specified when adding or altering a connect

Alert id        1114
Date and time   08May2003 10:11:09.51
Authority       JOIN
Granted to      C##BSG2 SUSAN GAYNOR
Connected to    C##B
Result          Success
RACF command    ALTUSER C##BSG2 AUTHORITY(JOIN) GROUP(C##B)
User            C##BERT  ERWIN RETTICH
Job name        CBERT#17
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1114: Connect authority JOIN    set for C##BSG2  in C##B

Alert 1114: Connect authority JOIN set for C##BSG2 in C##B
```

生成された E メール・レポートには、認可されたグループ権限、ユーザーとターゲット・グループ、完全な RACF コマンド、コマンドの結果、およびコマンドを実行したユーザーが示されます。

注: 「RACF command」フィールドには、指定されたコマンド・キーワードおよびデフォルト・キーワードが示されるため、フィールドがかなり長くなることがあります。

違反が多すぎる (1115)

zSecure Alert の REPORT オプション **AverageInterval** によって指定された間隔で特定のユーザー ID に関して、構成された数よりも多くの違反が記録された場合に、この修正アラートが生成されます。詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドに関する情報を参照してください。.

このアラートを生成するには、RACF アクセス違反を記録する必要があります。アクセス違反は、クラスの LOGOPTION 設定およびプロファイルの監査設定に応じて記録されます。

このアラートは、違反しているユーザー ID を自動的に取り消すように指定できるという点で、修正アラートです。また、zSecure Admin ライセンスにより、ALTUSER REVOKE コマンドの代わりに CKGRACF DISABLE コマンドを生成することを選択できます。

アラートのレポート・フォーマットは、zSecure Alert で修正アクションを実行することにしたかどうかによって異なります。

修正アクションがない場合のアラートの E メール・フォーマットは、以下のとおりです。

```
From:        C2POLICE at DINO
Subject:     Alert: 15 violations recorded for user C2RMUS01

Alert: 15 violations recorded for user C2RMUS01
Number of violation exceeds the configured 10

   Alert id        1115
   Date and time   09Mar2005 14:49:55.90 - 09Mar2005 14:54:57.89
   Violations      15
   User            C2RMUS01
   System ID       DINO

 Time  Intent  Allowed Class    Resource

 14:49 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000002.J
                                ESMSGLG
 14:49 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000003.J
                                ESJCL
 14:50 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000004.J
                                ESYSMSG
 14:50 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000101.?
 14:51 READ    NONE    JESSPOOL JES2DINO.DFHSM.DFHSM.STC05782.D0000104.?
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1115: 15 violations recorded for user C2RMUS01

Alert 1115: 15 violations recorded for user C2RMUS01
```

違反しているユーザー ID に対して ALU REVOKE コマンドを生成することにした場合、テキストは以下に変更されます。

```
User C2RMUS01 revoked after 15 violations
```

違反しているユーザー ID に対して CKGRACF DISABLE コマンドを生成することにした場合、テキストは以下に変更されます。

```
User C2RMUS01 disabled with schedule DIS#VIOL after 15 violations
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルでは、過度と見なされる違反の数を指定できます。また、除外するユーザー ID またはユーザー ID マスクを 10 個まで指定できます。 151 ページの『主要管理アクティビティー (1120 および 2120) 構成』を参照してください。

無期限パスワードの有効化 (1119)

PASSWORD NOINTERVAL コマンドを発行することにより、あるユーザー ID に対し無期限パスワードが設定された場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert:  User C##ASCH assigned non-expiring password for C##ABRJ

Alert: User C##ASCH assigned non-expiring password for C##ABRJ
User has been assigned a non-expiring password

 Alert id        1119
 Date and time   03Feb2013 10:12:05.30
 User            C##ABRJ JOHN BROWN
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         PASSWORD C##ABRJ NOINTERVAL
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1119: User C##ASCH assigned non-expiring password for C##ABRJ

Alert 1119: User C##ASCH assigned non-expiring password for C##ABRJ
```

アラートには、コマンド発行者、および無期限パスワードが設定されたユーザー ID が示されます。

主要管理アクティビティー (1120)

zSecure Alert の REPORT オプション **AverageInterval** によって指定された間隔で、特定のユーザー ID に関して、構成された数よりも多くの RACF コマンドが記録された場合、アラートが送信されます。

zSecure Alert の REPORT オプション **AverageInterval** について詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」で、REPORT コマンドに関する情報を参照してください。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: 126 commands recorded for user CDADMIN

Alert: 126 commands recorded for user CDADMIN
Number of commands exceeds the configured 100

 Alert id        1120
 Date and time   03Feb2013 10:12:05.30
 Commands        126
 User            CDADMIN   BATCH ADMIN JOB
 System ID       DINO

   Time  Event    Event description

   14:30 ALTUSER  Altuser command (Success:No violations detected)
   14:30 ALTUSER  Altuser command (Success:No violations detected)

   ..... .......  ........................................
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1120: 126 commands recorded for user CDADMIN

Alert 1120: 126 commands recorded for user CDADMIN
```

アラートには、ユーザー ID、発行されたコマンドの数、およびイベントのリストが示されます。

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルでは、過度と見なされる違反の数を指定できます。また、除外するユーザー ID またはユーザー ID マスクを 10 個まで指定できます。 151 ページの『主要管理アクティビティー (1120 および 2120) 構成』を参照してください。

保護状況の削除 (1121)

ALTUSER コマンドを使用してユーザー ID にパスワードまたはフレーズを割り当てることによりユーザー ID の保護状況が削除された場合は、アラートが送信されます。これまでに使用されなかったユーザー ID はこのアラートから除外されます。これまでに使用されなかったユーザー ID を正確に除外するには、SETROPTS INITSTATS がアクティブでなければなりません。

このアラートは、環境リフレッシュ時に RACF データベースに定義されているユーザー ID の保護状況を使用します。複数の ALTUSER コマンドが発行された場合、コマンドごとにアラートを受信する場合があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert:  User C##ASCH removed protected status from COLLSTC

Alert: User C##ASCH removed protected status from COLLSTC
Protected status removed
```

```
Alert id        1121
Date and time   03Feb2013 10:12:05.30
Removed from    COLLSTC COLLECT TASK
Result          Success
User            C##ASCH SIRAM CHRISTIAN
Job name        C##ASCHL
System ID       DINO
Command         ALTUSER COLLSTC PASSWORD(<password>)
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1121: User C##ASCH removed protected status from COLLSTC

Alert 1121: User C##ASCH removed protected status from COLLSTC
```

アラートには、コマンド発行者、および保護状況が削除されたユーザー ID が示されます。

機密性の高いユーザー ID を使用したログオン (発行元: C2PACMON) (1122)

機密性の高いユーザー ID を使用してログオンすると、Alert 1122 が発行されます。このアラートを使用するには、ADMINRACF または同等の資格がユーザーにあり、イベント転送用にアクセス・モニターが構成されている必要があります。

機密性の高いユーザー ID が使用されると、アラートが送信されます。このアラートは、zSecure Admin アクセス・モニターによって転送される ACCESS レコードに基づきます。このアラートを使用するには、zSecure ADMINRACF または同等の資格がユーザーにある必要があります。このような資格がない場合、または使用不可になっている場合、アラート指定は通知なしで無視されます。zSecure Admin アクセス・モニターは、実行されていて、VERIFY イベントを zSecure Alert 開始タスクに転送するように構成されている必要があります。アクセス・モニターがイベント転送用に構成されていない場合、RACF VERIFY イベントに対する ACCESS レコードを zSecure Alert が使用できず、Alert 1122 は実行されません。アクセス・モニターのイベント転送について詳しくは、「zSecure インストールおよびデプロイメント・ガイドの『zSecure Admin アクセス・モニターのセットアップ』章にある EventsToAlert キーワードと、『構成コマンド』セクションにある OPTION コマンドを参照してください。

ほとんどのジョブの開始には、複数の RACF VERIFY イベントが関与するため、同様のイベントはすべて、インターバルごとに単一のアラートに結合されます。単一のジョブの開始に対するイベントが、複数のインターバルで発生した場合は、複数のアラートが発行される場合があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: Sensitive user IBMUSER logged on
The user is on a watch list

   Alert id              1122
   First date and time   18Nov2016 03:50:29
         Last date and time    18Nov2016 03:50:29
         User ID               IBMUSER  IBM DEFAULT USERID
         Job name + id         IBMUSER
   Return code             0
   Application
   Port of entry         TERMINAL:SC0TCP02
         System ID             BCSC
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1122: Sensitive user IBMUSER logged on
Alert 1122: Sensitive user IBMUSER logged on
```

生成された E メール・レポートには、システムへのログオンに使用されたユーザー ID が表示されます。環境に合わせてアラートを構成できます。アラートを選択するときに、プロンプトのパネルが表示され、機密性の高いユーザー ID を 10 個まで入力できます。この構成プロセスは、緊急時ユーザー ID のプロセスと同一です。149 ページの『緊急時ユーザー構成 (アラート 1102 および 2102)』を参照してください。

データ・セット・アラート

このセクションでは、データ・セット・アクセスおよびデータ・セット・プロファイル変更に関する事前定義アラートについて説明します。

データ・セットでの WARNING モード・アクセス (1201)

データ・セットがアクセスされ、警告モードのためアクセス権限が認可されました。 92 ページの『一般リソースでの WARNING モード・アクセス (1303)』 も参照してください。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode READ    on data set CDS.SCDSSAMP

Alert: WARNING mode READ on data set CDS.SCDSSAMP
Data set access granted due to warning mode

   Alert id        1201
   Date and time   21Jan2003 09:11:11.01
   Data set        CDS.SCDSSAMP
   Granted access  READ
   Normal access   NONE
   Profile         CDS.SCDS*
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1201: WARNING mode READ    by C##BMR1 on data set
CDS.SCDSSAMP

Alert 1201: WARNING mode READ by C##BMR1 on data set CDS.SCDSSAMP
```

レポートには、データ・セット、このデータ・セットへのアクセス権限を要求したユーザー、アクセス権限が照合されたプロファイル、認可されたアクセス権限、およびプロファイルが WARNING モードでなかった場合に認可されていたと考えられる通常のアクセス権限が示されます。

WARNING モードのプロファイルは、このモード以外ではプロファイルが許可しないようなアクセス権限も含めて、リソースへのすべてのアクセス権限を認可できます。WARNING モードは通常、アクセス制御を実施する前に、プロファイルのアクセス設定の効果を分析するために使用されます。このモードは、実動に関する問題を克服するための一時的な手段として機能します。このアラートを受信した場合、アクセス権限を認可する必要があるかどうかを確認しなければなりません。確認し

たら、それに応じてプロファイルのアクセス設定を変更します。このアクセス権限が生じてはいけないことになっている場合、必要に応じて是正措置を取ります。

DATASET プロファイルで設定された公開アクセス権限 >= UPDATE (1202)

UPDATE 以上の UACC がデータ・セット・プロファイルで指定された場合、または ID(*) で UPDATE 以上のアクセス権限が許可された場合に、アラートが生成されます。指定されたアクセス権限が READ に等しいときでもアラートを受信する場合は、アラート 1203 を使用できます。

このアラートを受信するには、SETROPTS 設定 AUDIT(DATASET) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: Public access >= UPDATE set: CRMB##1.**
High UACC specified when adding or altering a data set profile

   Alert id        1202
   Date and time   19Jul2017 19:43:30.07
   Profile         CRMB##1.**
   Public access   UPDATE
   Method          UACC
   Result          Success
   RACF command    ALTDSD 'CRMB##1.**' GENERIC UACC(UPDATE)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

または

```
Alert: Public access >= UPDATE set: CRMB##1.**
High ID(*) access specified when adding or altering a data set profile

   Alert id        1202
   Date and time   19Jul2017 19:43:30.07
   Profile         CRMB##1.**
   Public access   UPDATE
   Method          ID(*) access
   Result          Success
   RACF command    PERMIT 'CRMB##1.**' ACCESS(UPDATE) CLASS(DATASET) GENERIC ID(*)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
subject: Alert 1202: Public access >= UPDATE set by CRMB##1 : CRMB##1.**

Alert 1202: Public access >= UPDATE set: CRMB##1.** ID(*) access set to UPDATE by
CRMB##1
```

または

```
Alert 1202: Public access >= UPDATE set: CRMB##1.** UACC set to UPDATE by
CRMB##1
```

アラートには、変更されたプロファイル、完全な RACF コマンド、コマンドの結果、コマンドを実行したユーザー、および付与された公開アクセス権限レベルが示されます。

DATASET プロファイルで設定された公開アクセス権限 > NONE (1203)

NONE よりも高い UACC がデータ・セット・プロファイルで指定された場合、または ID(*) で NONE よりも高いアクセス権限が許可された場合に、アラートが生成されます。指定されたアクセス権限が READ より高いときにのみアラートを受信する場合は、アラート 1202 を使用できます。

このアラートを受信するには、SETROPTS 設定 AUDIT(DATASET) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: Public access > NONE set: CRMB##1.**
High ID(*) access specified when adding or altering a data set profile

   Alert id        1203
   Date and time   19Jul2017 19:24:16.93
   Profile         CRMB##1.**
   Public access   UPDATE
   Method          ID(*) access
   Result          Success
   RACF command    PERMIT 'CRMB##1.**' ACCESS(UPDATE) CLASS(DATASET) GENERIC ID(*)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

または

```
Alert: Public access > NONE set: CRMB##1.**
High UACC specified when adding or altering a data set profile

   Alert id        1203
   Date and time   19Jul2017 19:24:16.94
   Profile         CRMB##1.**
   Public access   UPDATE
   Method          UACC
   Result          Success
   RACF command    ALTDSD 'CRMBRT1.**' GENERIC UACC(UPDATE)
   User            CRMBRT1  RENE VAN TIL
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1203: Public access > NONE set by CRMB##1 : CRMB##1.**

Alert 1203: Public access > NONE set: CRMB##1.** ID(*) access set to UPDATE by
CRMB##1
```

または

```
Subject: Alert 1203: Public access > NONE set by CRMB##1 : CRMB##1.**

Alert 1203: Public access > NONE set: CRMB##1.** ID(*) access set to UPDATE by
CRMB##1
```

アラートには、変更されたプロファイル、完全な RACF コマンド、コマンドの結果、コマンドを実行したユーザー、および付与された公開アクセス権限レベルが示されます。

APF データ・セットでの更新 (1204)

APF 許可データ・セットが更新された場合に、アラートが送信されます。

このアラートを生成するには、RACF の正常な更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(update)) または GLOBALAUDIT(success(update)) が指定されている場合に該当します。必要なコマンドは、zSecure Audit VERIFY SENSITIVE ステートメントを使用して作成できます。

アラートを生成してはならない特権ユーザーおよびグループは、SE.A.S オプション「**Privileged users and groups for UPDATE on APF data sets**」で指定できます。

注:

- 環境データが含まれた CKFREEZE データ・セットは、リフレッシュすることが推奨されます。SETPROG コマンドなどによって APF リストが更新されている場合、MODIFY C2POLICE,COLLECT コマンドを発行して、APF 許可データ・セットの現在のリストを取得します。
- このアラートでは、ボリューム名は考慮されません。現在の APF リストで発生する、名前を持つすべてのデータ・セットの更新についてトリガーされる可能性があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Update by C##ASCH  on APF data set C##A.D.C##NEW.APF.LOAD

Alert: Update by C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
APF data set successfully updated

   Alert id        1204
   Date and time   03Feb2003 10:12:05.30
   Data set        C##A.D.C##NEW.APF.LOAD
   Access          ALTER
   User            C##ASCH  SIRAM CHRISTIAN
   Result          Success
   Job name        C##ASCHL
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1204: Update by user C##ASCH  on APF data set
C##A.D.C##NEW.APF.LOAD

Alert 1204: Update by user C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
```

アラートには、更新されたデータ・セット、使用されたアクセス・レベル、およびデータ・セットにアクセスしたユーザーが示されます。

SETPROG を使用した APF リストへのデータ・セットの追加 (1205)

SET PROG コマンドまたは SETPROG コマンドを使用して、データ・セットが APF リストに動的に追加された場合に、アラートが生成されます。

このアラートを生成するには、WTO メッセージ CSV410I が入手可能で、処理のために選択される必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set added to APF list using SETPROG: SYSPROG.APF.LOAD

Alert: Data set added to APF list using SETPROG:SYSPROG.APF.LOAD
A data set is dynamically added to the APF list

   Alert id        1205
   Date and time   21Feb2003 11:44:36.71
   Data set        SYSPROG.APF.LOAD
   Volume          <SMS MANAGED>
   Console ID      R##SLIN
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1205: Data set added to APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD

Alert 1205: Data set added to APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

アラートには、APF リストに追加されたデータ・セットおよびデータ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。SET PROG コマンドまたは SETPROG コマンドが SDSF から入力された場合は、ユーザーがそのコマンドを入力したコンソールの名前も示されます。コンソール名は、デフォルトではユーザー ID になります。

SETPROG を使用した APF リストからのデータ・セットの除去 (1206)

SET PROG コマンドまたは SETPROG コマンドを使用して、データ・セットが APF リストから動的に除去された場合に、アラートが生成されます。

このアラートを生成するには、WTO メッセージ CSV410I が入手可能で、処理のために選択される必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set removed from APF list using SETPROG: SYSPROG.APF.LOAD

Alert: Data set removed from APF list using SETPROG: SYSPROG.APF.LOAD
A data set is dynamically removed from the APF list

Alert id        1206
Date and time   21Feb2003 11:44:36.71
Data set        SYSPROG.APF.LOAD
Volume          <SMS MANAGED>
Console ID      R##SLIN
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1206: Data set removed from APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD

Alert 1206: APF Data set removed from APF list using SETPROG from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

アラートには、APF リストから除去されたデータ・セットが示されます。また、データ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。SET PROG コマンドまたは SETPROG コマンドが SDSF から入力された場合は、ユーザーがそのコマンドを入力したコンソールの名前も示されます。コンソール名は、デフォルトではユーザー ID になります。

APF リストへのデータ・セットの追加の検出 (1207)

データ・セットが何らかの方法で APF リストに追加された場合に、このアラートが生成されます。

このアラートには、SET PROG コマンドまたは SETPROG コマンドの使用や、他の製品の使用などがあります。このアラートを生成するには、拡張モニターがアクティブである必要があります。このアラートは、2 つのシステム・スナップショットの比較に基づいています。データ・セットを追加するために使用されたユーザー ID またはジョブ名についての情報も、追加を実行するために使用されたプロセスについての情報も提供しません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD
An addition of a data set to the APF list has been detected

       Alert id              1207
       Date and time         18Nov2016 03:50:29
       Data set              SYSPROG.APF.LOAD
       Volume                <SMS MANAGED>
       APF                   No
       APFLIST               Yes
       System ID             DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1207: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert 1207: Data set addition to APF list detected: SYSPROG.APF.LOAD
```

アラートには、APF リストに追加されたデータ・セットが示されます。また、データ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいています。データ・セットを追加するために使用されたユーザー ID またはジョブ名についての情報も、追加を実行するために使用されたプロセスについての情報も提供しません。

APF リストからのデータ・セットの除去の検出 (1208)

データ・セットが何らかの方法で APF リストから除去された場合に、このアラートが生成されます。

このアラートを生成するには、拡張モニターがアクティブである必要があります。このアラートは、2 つのシステム・スナップショットの比較に基づいています。データ・セットを除去するために使用されたユーザー ID、ジョブ名についての情報、および除去を実行するために使用されたプロセスについてのいずれの情報も提供されません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD

Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD
A removal of a data set from the APF list has been detected

       Alert id              1208
       Date and time         18Nov2016 03:50:29
       Data set              SYSPROG.APF.LOAD
       Volume                <SMS MANAGED>
       APF                   Yes
       APFLIST               No
       System ID             DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1208: Data set removal from APF list detected: SYSPROG.APF.LOAD

Alert 1208: Data set removal from APF list detected: SYSPROG.APF.LOAD
```

アラートには、APF リストから除去されたデータ・セットが示されます。また、データ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいています。データ・セットを除去するために使用されたユーザー ID、ジョブ名についての情報、および除去を実行するために使用されたプロセスについてのいずれの情報も提供されません。

PCI PAN データへの不定期アクセス (1209)

PCI PAN (クレジット・カード主要アカウント番号) データ・セットへの不定期の READ 以上のアクセスが成功した場合、アラートが送信されます。

このアラートを生成するには、RACF の正常な読み取りアクセスおよび更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(read)) または GLOBALAUDIT(success(read)) が指定されている場合に該当します。

オプション SE.A.P を使用すると、PCI PAN データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1209: READ access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN

Alert 1209: READ access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN
Non-regular access

 Alert id        1209
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-PAN
```

```
 Access          READ
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1209: READ access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN

Alert 1209: READ access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (READ など)、およびデータ・セットにアクセスしたユーザーが示されます。

平文の PCI PAN データへの不定期アクセス (1210)

平文の PCI PAN (クレジット・カード主要アカウント番号) データへの不定期の READ 以上のアクセスが成功した場合、アラートが送信されます。

このアラートを生成するには、RACF の正常な読み取りアクセスおよび更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(read)) または GLOBALAUDIT(success(read)) が指定されている場合に該当します。

オプション SE.A.P を使用すると、平文の PCI PAN データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1210: READ access by C##ASCH on PCI-PAN-clr data set
C##A.D.C##NEW.PAN

Alert 1210: READ access by C##ASCH on PCI-PAN-clr data set C##A.D.C##NEW.PAN
Non-regular access

 Alert id        1210
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-PAN-clr
 Access          READ
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1210: READ access by C##ASCH on PCI-PAN-clr data set
C##A.D.C##NEW.PAN

Alert 1210: READ access by C##ASCH on PCI-PAN-clr data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (READ など)、およびデータ・セットにアクセスしたユーザーが示されます。

PCI AUTH データへの不定期アクセス (1211)

PCI AUTH (クレジット・カード機密認証データ) データ・セットへの不定期の READ 以上のアクセスが成功した場合、アラートが送信されます。

このアラートを生成するには、RACF の正常な読み取りアクセスおよび更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(read)) または GLOBALAUDIT(success(read)) が指定されている場合に該当します。

オプション SE.A.P を使用すると、PCI AUTH データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1211: READ access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN

Alert 1210: READ access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN
Non-regular access

 Alert id        1211
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-AUTH
 Access          READ
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1211: READ access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN

Alert 1211: READ access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (READ など)、およびデータ・セットにアクセスしたユーザーが示されます。

サイト機密データ・セットに対するアクセス>=READ (1212)

サイト機密データ・セットに対する不定期の READ 以上のアクセスが成功した場合、アラートが送信されます。

このアラートを生成するには、RACF の正常な読み取りアクセスおよび更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(read)) または GLOBALAUDIT(success(read)) が指定されている場合に該当します。プロファイルの監査設定を変更する場合、障害の監査も目的に従って設定されるようにしてください。

オプション SE.A.S を使用すると、サイト機密データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。アラートは、zSecure によって既に機密性が割り当てられているリソース (APF ライブラリー、JES スプール・データ・セットなど) には生成されません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1212: READ access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB

Alert 1212: READ access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB
Non-regular access
```

```
 Alert id        1212
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.MACLIB
 Sensitivity     Site-Dsn-R
 Access          READ
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1212: READ access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB

Alert 1212: READ access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (READ など)、およびデータ・セットにアクセスしたユーザーが示されます。

サイト機密データ・セットに対するアクセス>=UPDATE (1213)

サイト機密データ・セットに対する不定期の UPDATE 以上のアクセスが成功した場合、アラートが送信されます。

このアラートを生成するには、RACF の正常な読み取りアクセスおよび更新アクセスを記録する必要があります。これは、関連したプロファイルに対して AUDIT(success(update)) または GLOBALAUDIT(success(update)) が指定されている場合に該当します。プロファイルの監査設定を変更する場合、障害の監査も目的に従って設定されるようにしてください。

オプション SE.A.S を使用すると、機密データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。アラートは、zSecure によって既に機密性が割り当てられているリソース (APF ライブラリー、JES スプール・データ・セットなど) には生成されません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1213: UPDATE access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB

Alert 1213: UPDATE access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB
Non-regular access

 Alert id        1213
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.MACLIB
 Sensitivity     Site-Dsn-U
 Access          UPDATE
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1213: UPDATE access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB

Alert 1213: UPDATE access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (UPDATE など)、およびデータ・セットにアクセスしたユーザーが示されます。

UPDATE 機密メンバーに対するアクション (1214)

UPDATE 機密メンバーに対するアクションが成功した場合、アラートが送信されます。すなわち、INITIALIZE、DELETE、ADD、REPLACE、または RENAME のうち、いずれかのアクションがメンバーに対して行われた場合です。

SE.A.S. オプション「**UPDATE sensitive members in specific data sets**」を使用すると、当該メンバー、およびそれらのメンバーが属しているデータ・セットを指定できます。SE.A.S オプション 「**Privileged users and groups for site UPDATE sensitive resources**」を使用すると、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 1214: Action by C##ASCH on UPDATE sensitive member IEASYS81

Alert 1214:  Action by C##ASCH on UPDATE sensitive member IEASYS81
Action on UPDATE sensitive member

 Alert id        1214
 Date and time   03Feb2013 10:12:05.30
 Data set        USER.PARMLIB
 Action          REPLACE
 Member          IEASYS81
 Alias
 Old Member
 User            C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1214: REPLACE action by C##ASCH on UPDATE sensitive member IEASYS81

Alert 1214: REPLACE action by C##ASCH on UPDATE sensitive member IEASYS81 in data
set USER.PARMLIB
```

アラートには、更新されたデータ・セットおよびメンバー、およびそのメンバーに対して実行されたアクションが示されます。

DATASET プロファイルで設定された WARNING モード (1215)

DATASET プロファイルが警告モードに設定され、すべてのユーザーに対してアクセスが許可される場合に、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: WARNING mode set: CRMB##2.*.**
WARNING mode on DATASET profile allows all access, incl. UPDATE and DELETE

   Alert id        1215
   Date and time   19Jul2017 20:57:10.17
```

```
   Profile         CRMB##2.*.**
   Result          Success
   RACF command    ALTDSD 'CRMB##2.*.**' WARNING
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1215: WARNING mode set by CRMB##1 : CRMB##2.*.**

Alert 1215: WARNING mode set: CRMB##2.*.** by CRMB##1
```

アラートには、変更されたプロファイル、完全な RACF コマンド、コマンドの結果、およびコマンドを実行したユーザーが示されます。

DATASET プロファイルで変更された LEVEL 値 (1216)

新しい DATASET プロファイルで 0 以外の LEVEL 値が設定された場合、または既存の DATASET プロファイルで LEVEL 値が変更された場合、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: LEVEL value set: CRMB##1.**
LEVEL can contain a security control

   Alert id        1216
   Date and time   19Jul2017 20:17:37.59
   Profile         CRMB##1.**
   Level              66
   Result          Success
   RACF command    ALTDSD 'CRMB##1.**' GENERIC LEVEL(66)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1216: LEVEL value set by CRMB##1 : CRMB##1.**

Alert 1216: LEVEL value set: CRMB##1.** by CRMB##1
```

アラートには、更新された DATASET プロファイル、コマンドを実行したユーザー、および指定された LEVEL が示されます。

一般リソース・アラート

以下のアラートは、一般リソースの使用および変更について報告します。

STC 用の包括的プロファイルの使用 (1301)

開始タスクが STARTED クラスの包括的プロファイルと照合された場合に、アラートが送信されます。

このアラートを受信するには、包括的プロファイルで、RALTER STARTED コマンドを使用して TRACE(YES) を設定する必要があります。これにより、WTO メッセージ IRR812I が出力されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: STARTED/*.*  used for STC IEFBR1A .IEFBR1B

Alert: STARTED/*.*  used for STC IEFBR1A.IEFBR1B
A started task is checked against a catchall profile

   Alert id        1301
   Date and time   11Feb2003 18:14:48.78
   Profile         *.*
   Started task    IEFBR1A
   Started jobname IEFBR1B
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1301: STARTED/*.*  used for STC IEFBR1A .IEFBR1B

Alert 1301: STARTED/*.*  used for STC IEFBR1A .IEFBR1B
```

レポートには、突き合わせを行った包括的プロファイルと、開始タスクのメンバーおよびジョブ名が示されます。このレポートには、開始タスクを開始したユーザーは示されません。

STARTED クラスで member.jobname を定義した場合、このアラートの原因を除去できます。この開始タスクについては、包括的プロファイルは検査されなくなります。

監査対象プログラムの実行 (1302)

監査対象プログラムの実行が開始された場合のアラート。

監査対象プログラムは、READ の成功に対して少なくともユーザーまたは監査員の監査が設定された、PROGRAM クラスのプロファイルによって保護されます。

このアラートを受信するには、十分な監査を有効にした状態で、PROGRAM クラスの関連プロファイルが指定されている必要があります。このような監査は、RDEFINE または RALTER コマンドで AUDIT(SUCCESS(READ)) または GLOBALAUDIT(SUCCESS(READ)) キーワードを使用するなどして設定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Audited program ASMIDFA  has been executed

Alert: Audited program ASMIDFA has been executed
A program with auditing specified has been executed

   Alert id        1302
   Date and time   07Feb2003 13:44:43.20
   Program         ASMIDFA
   Data set        SHARED.LINKLIB
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
   Audit reason    <reason>
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1302: Audited program ASMIDFA  has been executed by C##BDV2  in
job C##BDV2

Alert 1302: Audited program ASMIDFA from data set SHARED.LINKLIB has been executed
by C##BDV2 in job C##BDV2
```

レポートには、実行が開始されたプログラム、プログラムが常駐するデータ・セット、プログラムを実行したユーザー、および監査の理由が示されます。

一般リソースでの WARNING モード・アクセス (1303)

一般リソース・クラスのプロファイルでアクセス権限が検査され、警告モードのためアクセス権限が認可されました。

データ・セットに対する同様のアラートが、 79 ページの『データ・セットでの WARNING モード・アクセス (1201)』にあります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode access to FACILITY IRR.LISTUSER

Alert: WARNING mode READ on FACILITY IRR.LISTUSER
Resource access granted due to warning mode

   Alert id        1303
   Date and time   07Feb2003 14:15:09.60
   Class           FACILITY
   Resource        IRR.LISTUSER
   Granted access  READ
   Normal access   NONE
   Profile         IRR.LISTUSER
   User            C##BDV2  DIONNE VONT
   Job name        C##BDV2
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1303: WARNING mode READ    by C##BDV2  on
FACILITY IRR.LISTUSER

Alert 1303: WARNING mode READ by C##BDV2 on FACILITY IRR.LISTUSER
```

レポートには、アクセスされたリソースのクラスと名前、このリソースへのアクセス権限を要求したユーザー、およびアクセス権限が照合されたプロファイルが示されます。また、認可されたアクセス権限と、プロファイルが WARNING モードでなかった場合に認可されていたと考えられる通常のアクセス権限が示されます。

WARNING モードのプロファイルは、このモード以外ではプロファイルが許可しないようなアクセス権限も含めて、リソースへのすべてのアクセス権限を認可します。WARNING モードは通常、アクセス制御を実施する前に、プロファイルのアクセス設定の効果を分析するために使用されます。このモードは、実動に関する問題を克服するための一時的な手段としても使用されます。このアラートを受信した場合、アクセス権限を許可する必要があるかどうかを確認しなければなりません。許可が必要な場合、それに応じてプロファイルのアクセス設定を変更します。このアクセス権限が生じてはいけないことになっている場合、必要に応じて是正措置を取ります。

一般リソース・プロファイルで設定された公開アクセス権限 > NONE (1304)

NONE よりも高い UACC が一般リソース・プロファイルで指定された場合、または ID(*) で NONE よりも高いアクセス権限が許可された場合に、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: Public access > NONE set: FACILITY DITTO.DISK.**
High UACC specified when adding or altering a FACILITY profile

   Alert id        1304
   Date and time   19Jul2017 20:34:45.47
   Class           FACILITY
   Profile         DITTO.DISK.**
   Public access   ALTER
   Method          UACC
   Result          Success
   RACF command    RALTER FACILITY (DITTO.DISK.**) UACC(ALTER)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

または

```
Alert: Public access > NONE set: FACILITY DITTO.DISK.**
High ID(*) access specified when adding or altering a FACILITY profile

   Alert id        1304
   Date and time   19Jul2017 20:34:45.48
   Class           FACILITY
   Profile         DITTO.DISK.**
   Public access   UPDATE
   Method          ID(*) access
   Result          Success
   RACF command    PERMIT DITTO.DISK.** ACCESS(UPDATE) CLASS(FACILITY) ID(*)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1304: Public access > NONE set by CRMB##1 : FACILITY DITTO.DISK.**

Alert 1304: Public access > NONE set: FACILITY DITTO.DISK.** UACC set to ALTER by
CRMB##1
```

または

```
Alert 1304: Public access > NONE set: FACILITY DITTO.DISK.** ID(*) access set to
UPDATE by CRMB##1
```

アラートには、更新された一般リソース・プロファイル、公開アクセス権限、およびコマンドを実行したユーザーが示されます。

一般リソース・プロファイルで設定された WARNING モード (1305)

一般リソース・プロファイルが警告モードに設定され、すべてのユーザーに対してアクセスが許可される場合に、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: WARNING mode set: OPERCMDS MVS.DUMP
WARNING mode on OPERCMDS profile allows all access.

   Alert id        1305
   Date and time   19Jul2017 21:06:44.01
   Class           OPERCMDS
   Profile         MVS.DUMP
   Result          Success
   RACF command    RALTER OPERCMDS (MVS.DUMP) WARNING
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1305: WARNING mode set by CRMB##1 : OPERCMDS MVS.DUMP

Alert 1305: WARNING mode set: OPERCMDS MVS.DUMP by CRMB##1
```

アラートには、変更されたプロファイル、完全な RACF コマンド、コマンドの結果、およびコマンドを実行したユーザーが示されます。

STC への「トラステッド」または「特権あり」の割り当て (1306)

STARTED クラスのプロファイルに対する RDEFINE または RALTER コマンドの使用により、TRUSTED 属性または PRIVILEGED 属性が開始タスク (STC) に割り当てられた場合、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(STARTED) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: User C##ASCH has allowed any access for STC GRS.*

Alert: User C##ASCH has allowed any access for STC GRS.*
Started Task is now allowed to access any resource

 Alert id        1306
 Date and time   03Feb2013 10:12:05.30
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         ralter STARTED GRS.* STDATA(trusted(YES))
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1306: User C##ASCH has allowed any access for STC GRS.*

Alert 1306: User C##ASCH has allowed any access for STC GRS.*
```

アラートには、開始プロファイルおよびコマンド発行者が示されます。

一般リソース・プロファイルで変更された LEVEL 値 (1307)

新しい一般リソース・プロファイルで 0 以外の LEVEL 値が設定された場合、または既存のプロファイルで LEVEL 値が変更された場合、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
Alert: LEVEL value set: FACILITY R##E.TEST
LEVEL can contain a security control

   Alert id        1307
   Date and time   19Jul2017 21:13:29.74
   Class           FACILITY
   Profile         R##E.TEST
   Level             67
   Result          Success
   RACF command    RALTER FACILITY (R##E.TEST) LEVEL(67)
   User            CRMB##1  RON V
   Job name        CRMB##1
   System ID       8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1307: LEVEL value set by CRMB##1 : FACILITY R##E.TEST

Alert 1307: LEVEL value set: FACILITY R##E.TEST by CRMB##1
```

アラートには、更新された一般リソース・プロファイル、コマンドを実行したユーザー、および指定された LEVEL が示されます。

UNIX アラート

以下のアラートは、UNIX ファイル、ディレクトリー、またはプログラムに関するイベントが発生した場合にトリガーされます。

UNIX ファイル・アクセス違反 (1401)

UNIX ファイルまたはディレクトリーでアクセス違反が発生した場合に、アラートが送信されます。

このアラートを生成するには、SETROPTS 設定 LOGOPTIONS(FAILURES (DIRACC DIRSRCH FSOBJ)) を設定する必要があります。あるいは、関連するファイルに、**chaudit** コマンドによってアクセス障害の監査を指定する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: UNIX access violation on ./actuator/bin/db2asc

Alert: UNIX access violation on ./actuator/bin/db2asc
Non-authorized UNIX file or directory access

   Alert id        1401
   Date and time   28May2000 01:10:06.67
   Path            ./actuator/bin/db2asc
   Access type     FACCESS
   Intended access --w-
   Granted access   r-x
   User            C##BOON  OTTO ONSLEY
   Job name        C##BOON
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1401: UNIX access violation (--w-) by C##BOON
on ./actuator/bin/db2asc

Alert 1401: UNIX access violation (--w-) by C##BOON on ./actuator/bin/db2asc
```

レポートには、ファイルまたはディレクトリーのパス、アクセス・タイプ、すなわち、FACCESS、DIRACCESS、または DIRSRCH、目的のアクセス権限と認可されたアクセス権限、およびファイルまたはディレクトリーにアクセスしようとしたユーザーが示されます。パラメーター UNIX=YES を指定して作成された CKFREEZE ファイルを使用する場合、レポートに示される UNIX パスは絶対パスです。

ファイル・アクセス権限の変更時のグローバル書き込みの指定 (1402)

UNIX ファイルまたはディレクトリーの権限の「その他」のグループ で書き込み権限が指定された場合に、このアラートが生成されます。

このアラートを受信するには、SETROPTS 設定 LOGOPTIONS(ALWAYS(FSSEC)) を有効にする必要があります。パラメーター UNIX=YES および AUTOMOUNT=YES を指定して作成された CKFREEZE ファイルがない場合は、その他のファイル以外の UNIX オブジェクトでもこのアラートを受信することがあります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global write specified on www/log/access.log

Alert: Global write specified on www/log/access.log
Global write specified when altering file access

   Alert id        1402
   Date and time   09Feb2003 08:07:01.66
   Path            www/log/access.log
   Old permissions rw-r--r--
   New permissions rw-rw-rw-
   Result          Success
   User            C##BER2  ERWIN RETTICH
   Job name        C##BER2
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1402: Global write specified by C##BER2  on www/log/access.log

Alert 1402: Global write specified by C##BER2 on www/log/access.log
```

アラートには、ファイルまたはディレクトリーのパスおよび古い権限と新しい権限が示されます。また、**chmod** コマンドの結果および権限モードを変更したユーザーが示されます。パラメーター UNIX=YES を指定して作成された CKFREEZE ファイルを使用する場合、レポートに示される UNIX パスは絶対パスです。

ファイル・アクセス権限の変更時のグローバル読み取りの指定 (1403)

UNIX ファイルの許可の「その他」グループで読み取り権限が指定された場合に、このアラートが送信されます。

このアラートを受信するには、SETROPTS 設定 LOGOPTIONS(ALWAYS(FSSEC)) を有効にする必要があります。パラメーター UNIX=YES および AUTOMOUNT=YES を指定して作成された CKFREEZE ファイルがない場合は、その他のファイル以外の UNIX オブジェクトでもこのアラートを受信することがあります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global read specified on www/log/access.log

Alert: Global read specified on www/log/access.log
Global read specified when altering file access

   Alert id        1403
   Date and time   09Feb2003 08:05:22.61
   Path            www/log/access.log
   Old permissions rw-------
   New permissions rw-r--r--
   Result          Success
   User            C##BER2  ERWIN RETTICH
   Job name        C##BER2
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1403: Global read specified by C##BER2  on www/log/access.log

Alert 1403: Global read specified by C##BER2 on www/log/access.log
```

アラートには、ファイルのパス、古い権限と新しい権限、**chmod** コマンドの結果、および権限モードを変更したユーザーが示されます。パラメーター UNIX=YES を指定して作成された CKFREEZE ファイルを使用する場合、レポートに示される UNIX パスは絶対パスです。

拡張属性の変更 (1404)

拡張属性 (すなわち、APF、プログラム制御、または BPX shareas) が UNIX ファイルまたはプログラムで設定または除去された場合に、アラートが生成されます。

このアラートは、z/OS 1.11 以降でのみ使用可能なアラート 1409 に置き換えられました。アラート 1409 は、アラート 1404 に比べて、構成がより簡単で、使用するリソースがかなり少なくなっています。

アラート 1404 を受信するには、少なくとも SETROPTS 設定 LOGOPTIONS(DEFAULT(FSOBJ)) を有効にする必要があります。そうすると、z/OS UNIX の **chaudit** コマンドを使用して、監査対象プログラムに対して正常な書き込みの監査を活動化することができます。正常な監査を活動化していない場合、送信されるアラートのテキストは不完全であり、必須の部分 (アラート番号やファイル識別など) が欠落しています。個々のファイルに対して正常な監査の設定が必要となるのを避けるために、LOGOPTIONS(ALL(FSOBJ)) の設定を検討する場合があります。ただし、この設定を行うと、作成される SMF レコードの数が大幅に増えます。タイプ 1404 のアラートを受信する場合、FACILITY クラスで BPX.SAFFASTPATH プロファイルを定義することもできません。

E メールで送信されるアラートでは、変更された実際の拡張属性を組み込もうとします。これを正常に組み込むには、BPX.FILEATTR.APF および BPX.FILEATTR.PROGCTL に一致する、FACILITY プロファイルの READ ロギングも必要です。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Extended attribute changed: APF

Alert: Extended attribute changed: APF
```

```
APF or program control bit changed on UNIX file or directory

   Alert id        1404
   Date and time   05Feb2003 13:17:52.49
   Path            audfrbg
   User            C##BERT  ERWIN RETTICH
   Job name        C##BERT
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1404: APF or program control bit changed by C##BERT  on
UNIX file or directory audfrbg

Alert 1404: APF or program control bit changed by C##BERT on UNIX file
or directory audfrbg
```

アラートには、設定または除去された拡張属性が示されます。また、ファイルまたはディレクトリーのパスおよび属性を変更したユーザーが示されます。パラメーター UNIX=YES と、オプションで AUTOMOUNT=YES を指定して作成された CKFREEZE ファイルを使用する場合、レポートのパスは絶対パスです。

監査対象 UNIX プログラムの実行 (1405)

正常な実行の監査 (ユーザーまたは監査員) が有効な z/OS UNIX プログラムの実行が開始された場合に、アラートが送信されます。

このアラートは、SETUID ビットが有効で所有者としてスーパーユーザーが設定されたプログラムは、対象としていません。詳細については、 99 ページの『スーパーユーザー特権のある UNIX プログラムの実行 (1406)』を参照してください。

このアラートを受信するには、監査対象プログラムが HFS ファイル・システム内に存在している必要があります。少なくとも SETROPTS 設定 LOGOPTIONS(DEFAULT(FSOBJ)) を有効にする必要があり、また、FACILITY クラスで BPX.SAFFASTPATH プロファイルを定義してはなりません。さらに、パラメーター UNIX=YES と、オプションで AUTOMOUNT=YES を指定して作成された CKFREEZE ファイルを使用する必要があります。アラートは、CKFREEZE ファイルに情報があるプログラムに対してのみ送信されます。

z/OS UNIX の **chaudit** コマンドを使用して、監査対象プログラムに対して正常な実行の監査ビットを設定することができます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: UNIX program executed: chprot

Alert: UNIX program executed: chprot
A UNIX program with execution auditing specified has been executed.

   Alert id        1405
   Date and time   11Mar2003 11:05:11.49
   Path            /usr/bin/chprot
   User            C##BSG2  SUSAN GAYNOR
   Job name        C##BSG2
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1405: UNIX program executed by C##BSG2 : /usr/bin/chprot

Alert 1405: UNIX program executed by C##BSG2: /usr/bin/chprot
```

アラートには、プログラムのパスおよびプログラムの実行を開始したユーザーが示されます。

スーパーユーザー特権のある UNIX プログラムの実行 (1406)

SETUID が有効で、UID 0 に所有されている UNIX プログラムの実行が開始された場合に、アラートが送信されます。

プログラムでは、正常な実行の監査 (ユーザーまたは監査員) を有効にする必要があります。ユーザーの権限とは無関係に、これらのプログラムはスーパーユーザー特権を使用して実行され、UNIX サブシステム上のすべてのファイルまたはディレクトリーの読み取りと書き込みができます。

このアラートを受信するには、監査対象プログラムが HFS ファイル・システム内に存在している必要があります。少なくとも SETROPTS 設定 LOGOPTIONS(DEFAULT(FSOBJ)) を有効にする必要があり、また、FACILITY クラスで BPX.SAFFASTPATH プロファイルを定義してはなりません。さらに、パラメーター UNIX=YES と、オプションで AUTOMOUNT=YES を指定して作成された CKFREEZE ファイルを使用する必要があります。アラートは、CKFREEZE ファイルに情報があるプログラムに対してのみ送信されます。

このアラートは、アラート 1405 に付随します。アラート 1405 は、これらの特殊特権のない監査対象 UNIX プログラムの実行が開始された場合にメッセージを送信します。 98 ページの『監査対象 UNIX プログラムの実行 (1405)』を参照してください。付随する CARLa を使用して、スーパーユーザー特権を使用して実行されるすべてのプログラムで、監査員の実行の監査を設定する UNIX コマンドを生成できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged UNIX program executed: rdefcha

Alert: Superuser privileged UNIX program executed: rdefcha
An audited UNIX program started execution with superuser privileges

Alert id        1406
Date and time   13May2003 21:59:05.12
Path            /usr/local/bin/rdefcha
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1406: Superuser privileged UNIX program executed by C##BSG1: rdefcha

Alert 1406: Superuser privileged UNIX program executed by C##BSG1: rdefcha
```

アラートには、SETUID 特権が設定されたプログラムのパスおよびプログラムの実行を開始したユーザーが示されます。

ユーザーによるスーパーユーザー特権のあるシェルの取得 (1407)

ユーザーが、UNIX の <cmdname>su</cmdname> コマンドを使用してスーパーユーザー特権のあるシェルを取得した場合に、アラートが生成されます。

このアラートを受信するには、正常な READ ロギングを BPX.SUPERUSER FACILITY プロファイルに指定する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged shell obtained by user C##BSG1

Alert: Superuser privileged shell obtained by user C##BSG1
A user used su to obtain a shell with superuser privileges

Alert id        1407
Date and time   14May2003 14:15:21.98
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1407: Superuser privileged shell obtained by user C##BSG1

Alert 1407: Superuser privileged shell obtained by user C##BSG1
```

レポートには、**su** を使用してスーパーユーザー特権のあるシェルを取得したユーザーが示されます。このユーザーは、UNIX サブシステム上のすべてのファイルまたはディレクトリーの読み取りと書き込みができます。

UNIX プログラムでのスーパーユーザー特権の設定 (1408)

UNIX スーパーユーザーによって所有されるプログラムで SETUID ビットが設定された場合に、このアラートが生成されます。

このような特権のあるプログラムは、スーパーユーザー権限を使用して実行されるので、すべての UNIX ファイルまたはデータ・セットにアクセスできます。

注: 所有者を SETUID が有効なプログラムの UID 0 に変更すると、SETUID ビットがリセットされるので、これは機密漏れにはなりません。

このアラートを受信するには、SETROPTS 設定 LOGOPTIONS(ALWAYS(FSSEC)) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileges set on UNIX program collogs

Alert: Superuser privileges set on UNIX program collogs
The setuid bit is specified on a UNIX program owned by a superuser

Alert id        1408
Date and time   28Mar2003 11:49:33.66
Path            /usr/local/bin/collogs
User            C##BER2  ERWIN RETTICH
Job name        C##BER2
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1408: Superuser privileges set on UNIX program collogs

Alert 1408: Superuser privileges set on UNIX program collogs
```

アラートには、プログラムのパスおよびプログラムがスーパーユーザー特権を使用して実行されるように権限を変更したユーザーが示されます。パラメーター UNIX=YES を指定して作成された CKFREEZE ファイルを使用する場合、レポートに示される UNIX パスは絶対パスです。

拡張属性の変更 (1409)

このアラートが活動化されている場合、UNIX ファイルまたはプログラムの拡張属性設定 (APF、プログラム制御、または _BPX_SHAREAS) で変更が検出されると通知メッセージが生成されます。このアラートを受信するには、z/OS システムのレベルは少なくとも 1.11 である必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Extended attribute changed for db2asc

Alert: Extended attribute changed for db2asc
Extended attributes indicate z/OS special handling

   Alert id         1409
   Date and time    19Jul2017 19:43:30.07
   Path             ./actuator/bin/db2asc
   Previous value   APF authorized;
   New value
   User             C##BER2 ERWIN RETTICH
   Job name         C##BER2
   System id        DINO
```

E メール通知では、**Previous value** および **New value** には、共有ライブラリー、APF 許可、およびプログラム制御の値を組み合わせたものが含まれる場合があります。

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1409: Extended attribute changed (APS-> APS) by C##BER2 for db2asc.

Alert 1409: Extended attribute changed (APS-> APS) by C##BER2 for db2asc
```

UNIX ファイル (db2asc) の拡張属性が変更されました。旧拡張属性と新規拡張属性は、括弧に入れて表示されます。ストリング APS は拡張属性 (APF 許可、プログラム制御、および共有ライブラリー) を表します。コマンドは C##BER2 によって発行されました。

UID(0) の割り当て (1410)

ALTUSER コマンドまたは ADDUSER OMVS(UID(0)) コマンドを使用して UID(0) が割り当てられた場合、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(USER) を有効にする必要があります。SPECIAL 属性のあるユーザーによってコマンドが実行される場合、アラートの受信には SETROPTS 設定 SAUDIT でも十分です。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: User C##ASCH assigned UID(0) for C##ACS1

Alert: User C##ASCH assigned UID(0) for C##ACS1
Root privilege granted to C##ACS1

 Alert id        1410
 Date and time   03Feb2013 10:12:05.30
 User            C##ACS1 ARTHUR SMITH
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         ALTUSER C##ACS1 OMVS(UID(0))
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1410: C##ASCH assigned UID(0) for C##ACS1

Alert 1410: C##ASCH assigned UID(0) for C##ACS1
```

アラートには、コマンド発行者、および UID(0) が割り当てられたユーザー ID が示されます。

BPX.SUPERUSER に対する許可の実行 (1411)

FACILITY クラスのプロファイル BPX.SUPERUSER に対して許可が実行された場合、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(FACILITY) を有効にする必要があります。SPECIAL 属性のあるユーザーによってコマンドが実行される場合、アラートの受信には SETROPTS 設定 SAUDIT でも十分です。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: User C##ASCH issued permit on BPX.SUPERUSER for C##ACS1

Alert: User C##ASCH issued permit on BPX.SUPERUSER for C##ACS1
Permit issued for BPX.SUPERUSER

 Alert id        1411
 Date and time   03Feb2013 10:12:05.30
 User            C##ACS1 ARTHUR SMITH
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         PERMIT BPX.SUPERUSER  ID(C##ACS1) ACCESS(READ) CLASS(FACILITY)
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1411: User C##ASCH issued permit on BPX.SUPERUSER for C##ACS1

Alert 1411: User C##ASCH issued permit on BPX.SUPERUSER for C##ACS1
```

アラートには、コマンド発行者、および許可が割り当てられたユーザー ID が示されます。

RACF 制御アラート

以下のアラートは、RACF SETROPTS 設定の変更について報告します。

グローバル・セキュリティー対策の活動化 (1501)

RACF SETROPTS コマンドでシステムのセキュリティーを厳しくした場合に、アラートが送信されます。

注: このアラートをトリガーする条件は、アラート 1503 をトリガーする条件のサブセットです。両方のアラートを選択する唯一の理由は、これらのアラートを異なる受信者に送信するということです。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure activated by C##BNA2

Alert: Global security countermeasure activated by C##BNA2
SETROPTS command tightened system security

   Alert id        1501
   Date and time   23Jan2003 12:13:34.58
   RACF command    SETROPTS
                   LOGOPTIONS(NEVER(FACILITY),FAILURES(DATASET))
   User            C##BNA2  NICK AFTERSOCK
   Result          Success
   Job name        C##BNA2
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1501: Global security countermeasure activated by C##BNA2

Alert 1501: Global security countermeasure activated by C##BNA2: SETROPTS
LOGOPTIONS(NEVER(FACILITY),FAILURES(DATASET)) PASSWORD(NOHISTORY)
```

アラートには、実行された RACF コマンド、コマンドを実行したユーザー、およびコマンドの戻り状況が示されます。

グローバル・セキュリティー対策の非活動化 (1502)

RACF SETROPTS コマンドでシステムのセキュリティーを低下させた場合に、アラートが生成されます。

対策が非活動化されることが zSecure Alert で確実に認識されると、このアラートは、携帯電話のメッセージを介してより時宜にかなった通知を保証します。

注: このアラートをトリガーする条件は、アラート 1503 をトリガーする条件のサブセットです。両方のアラートを選択する唯一の理由は、これらのアラートを異なる受信者に送信するということです。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure deactivated by C##BNAT

Alert: Global security countermeasure deactivated by C##BNAT
SETROPTS command loosened system security

   Alert id        1502
   Date and time   23Jan2003 11:51:56.01
   RACF command    SETROPTS NOSAUDIT
```

```
   User            C##BNAT  NICK AFTERSOCK
   Result          Success
   Job name        C##BNAT
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1502: Global security countermeasure deactivated by C##BNAT

Alert 1502: Global security countermeasure deactivated by C##BNAT: SETROPTS ADSP
NOSAUDIT <Ignored>
```

アラートには、実行された RACF コマンド、コマンドを実行したユーザー、およびコマンドの戻り状況が示されます。

グローバル・セキュリティー対策またはオプションの変更 (1503)

RACF SETROPTS コマンドでシステムのセキュリティーを変更した場合に、アラートが生成されます。

このアラートには、実行された RACF コマンド、コマンドを実行したユーザー、およびコマンドの戻り状況が示されます。

注: アラート 1501 および 1502 をトリガーする条件は、アラート 1503 をトリガーする条件のサブセットです。アラート 1501 または 1502 をアラート 1503 と組み合わせて選択する唯一の理由は、これらのアラートを異なる受信者に送信するということです。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Global security countermeasure changed by C##BNAT

Alert: Global security countermeasure changed by C##BNAT
SETROPTS command changed system security

   Alert id        1503
   Date and time   23Jan2003 11:51:56.01
   RACF command    SETROPTS NOSAUDIT
   User            C##BNAT  NICK AFTERSOCK
   Result          Success
   Job name        C##BNAT
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1503: Global security countermeasure changed by C##BNAT

Alert 1503: Global security countermeasure changed by C##BNAT: SETROPTS ADSP
NOSAUDIT <Ignored>
```

RACF リソース・クラスの活動化 (1504)

RACF リソース・クラスが活動化されていることが検出された場合に、このアラートが生成されます。

このアラートには、活動化されたリソース・クラスが示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、変更がどのように実施されたかについての情報を提供しません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at IDFX
Subject: Alert: RACF resource class has been activated: DASDVOL

Alert: RACF resource class has been activated: DASDVOL
A change in the status of a RACF resource class has been detected

       Alert id              1504
       Date and time         19Jul2017 19:43:30.07
       CLASS                 DASDVOL
       Status                Active
       Complex               IDFX
       System ID             IDFX
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1504: RACF resource class has been activated: DASDVOL

Alert 1504: RACF resource class has been activated: DASDVOL
```

RACF リソース・クラスの非活動化 (1505)

RACF リソース・クラスが非活動化されていることが検出された場合に、このアラートが生成されます。

このアラートには、非活動化されたリソース・クラスが示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、変更がどのように実施されたかについての情報を提供しません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at IDFX
Subject: Alert: RACF resource class has been deactivated: DASDVOL

Alert: RACF resource class has been deactivated: DASDVOL
A change in the status of a RACF resource class has been detected

       Alert id              1504
       Date and time         19Jul2017 19:43:30.07
       CLASS                 DASDVOL
       Status                Inactive
       Complex               IDFX
       System ID             IDFX
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1505: RACF resource class has been deactivated: DASDVOL

Alert 1505: RACF resource class has been deactivated: DASDVOL
```

グローバル・アクセス検査テーブルの変更 (1506)

グローバル・アクセス検査テーブルが、GLOBAL クラスの RDEFINE、RALTER、または RDELETE コマンドを使用して変更された場合、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(GLOBAL) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: User C##ASCH issued command to change the GAC table for class
DATASET

Alert: User C##ASCH issued command to change the GAC table for class DATASET
```

```
RACF command issued to change the Global Access Checking (GAC) table

 Alert id        1506
 Date and time   03Feb2013 10:12:05.30
 Class           GLOBAL
 Profile         DATASET
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         RALTER GLOBAL DATASET ADDMEM('SYS1.BRODCAST'/UPDATE)
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1506: User C##ASCH issued command to change the GAC table for
class DATASET

Alert 1506: User C##ASCH issued command to change the GAC table for class DATASET
```

アラートには、追加、削除、または変更されたグローバル・アクセス検査テーブル、およびコマンド発行者が示されます。

動的クラス記述子テーブルの変更 (1507)

動的クラス記述子テーブル (CDT) が、CDT クラスの RDEFINE、RALTER、または RDELETE コマンドを使用して変更された場合、アラートが送信されます。

このアラートを受信するには、SETROPTS 設定 AUDIT(CDT) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: User C##ASCH issued command to change the dynamic CDT for class
MYCLASS

Alert: User C##ASCH issued command to change the dynamic CDT for class MYCLASS
RACF command issued to change the dynamic CDT

 Alert id        1507
 Date and time   03Feb2013 10:12:05.30
 Class           CDT
 Profile         MYCLASS
 Result          Success
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
 Command         RALTER CDT MYCLASS CDTINFO(DEFAULTRC(8))
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1507: User C##ASCH issued command to change the dynamic CDT for
class MYCLASS

Alert 1507: User C##ASCH issued command to change the dynamic CDT for class
MYCLASS
```

アラートには、追加、削除、または変更された動的クラス記述子テーブル項目、およびコマンド発行者が示されます。

SETPROG EXIT による Command Verifier の非活動化 (1508)

zSecure Command Verifier が、SETPROG EXIT,DELETE,EXITNAME=IRREVX01,MODNAME=C4RMAIN オペレーター・コマンド、または SET PROG=*xx* オペレーター・コマンドの結果として非活動化された場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Command Verifier deactivated

Alert: Command Verifier deactivated
System messages report the SETPROG EXIT command has been issued

 Alert id        1508
 Date and time   03Feb2013 10:12:05.30
 WTO message     CSV420I MODULE C4RMAIN HAS BEEN DELETED FROM EXIT
                  IRREVX01

 Console ID      CR@SRT1
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1508: Command Verifier deactivated at CR@SRT1 : CSV420I MODULE
C4RMAIN HAS BEEN DELETED FROM EXIT IRREVX01

Alert 1508: Command Verifier deactivated at: CR@SRT1 : CSV420I MODULE C4RMAIN HAS
BEEN DELETED FROM EXIT IRREVX01
```

アラートには、SETPROG コマンドの応答、およびこのコマンドの実行元のコンソール ID が示されます。

システム・アラート

以下のアラートは、一般システム・イベントをモニターするためのものです。

SMF データ損失の開始 (1601)

SMF データ損失が開始されたことを WTO が報告した場合に、このアラートが生成されます。これは、メッセージ IEE351I、IEE979W、 および IEE989I で報告されます。

注: 緊急の機密漏れが生じたら通知されるように、アラート 1602 を活動化することを選択できます。

このアラートを受信するには、WTO メッセージ IEE351I、IEE979W、および IEE989I を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: SMF data loss started

Alert: SMF data loss started
System messages report that SMF data loss has started

   Alert id        1601
   Date and time   10Feb2003 16:36:27.07
   WTO message     IEE979W SMF DATA LOST - NO BUFFER SPACE
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1601: SMF data loss started. WTO msgid: IEE979W

Alert 1601: SMF data loss started. WTO msgid: IEE979W
```

生成された E メールには、発行された WTO メッセージのみが示されます。

障害の後の SMF ロギングの再開 (1602)

バッファーがいっぱいになったため SMF データが失われたが、システムがロギングを再開した場合に、このアラートが生成されます。

注: アラート 1601 によって示される緊急の機密漏れが生じたら通知されるように、このアラートを活動化することを選択できます。

このアラートを受信するには、SMF レコード・タイプ 7 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF logging resumed after failure

Alert: SMF logging resumed after failure
SMF data is lost, but the system has resumed logging

   Alert id        1602
   Start of loss   10Feb2003 17:35:58.97
   Date and time   10Feb2003 17:36:27.12
   #records lost   4121
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1602: SMF logging resumed after failure.  4121 records lost.

Alert 1602: SMF logging resumed after failure. 4121 records lost.
```

生成された E メールには、データが失われた期間の開始時刻 (Start of loss) および終了時刻 (Resume time) が示されます。また、失われた SMF レコードの数が示されます。

SVC 定義の変更 (1603)

SVC テーブルまたは SVC ESR テーブルの SVC の定義で変更が検出されると、このアラートが生成されます。

このアラートには、変更された SVC の SVC および ESR 番号が示されます。SVC コードの現行アドレスが、現行 APF 状況と一緒に示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、変更がどのように実施されたかについての情報を提供しません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at IDFX
Subject: Alert: SVC Definition changed: SVC/ESR 220

Alert: SVC Definition changed: SVC/ESR 220
A change in the definition of an SVC has been detected
```

```
 Alert id    1603
 SVC/ESR number  220/
 Address     00147080
 APF      Yes
 System ID    IDEX
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1603: SVC Definition changed: SVC/ESR 220/
Alert 1603: SVC Definition changed: SVC/ESR 220/ at address 00147080 APF
```

IBM Health Checker による重大度が低レベルの問題の検出 (1604)

重大度が低レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0001I で報告されます。このアラートを受信するには、WTO メッセージ HZS0001I を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found low severity problem

Alert: IBM Health Checker found low severity problem
Check found a problem that should be investigated

  Alert id       1604
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):


                 ISGH0305E Global Resource Serialization synchronous
                 RESERVE processing
                 is not active.
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1604: IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
Alert 1604:  IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
```

IBM Health Checker による重大度が中レベルの問題の検出 (1605)

重大度が中レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0002E で報告されます。このアラートを受信するには、WTO メッセージ HZS0002E を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found medium severity problem

Alert: IBM Health Checker found medium severity problem
Check found a problem that should be investigated

  Alert id       1605
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
```

```
                ILRH0107E Page data set slot usage threshold met or
                exceeded
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1605: IBM Health Checker medium severity: HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
Alert 1605:  IBM Health Checker medium severity: HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
```

IBM Health Checker による重大度が高レベルの問題の検出 (1606)

重大度が高レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0003E で報告されます。このアラートを受信するには、WTO メッセージ HZS0003E を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found high severity problem

Alert: IBM Health Checker found high severity problem
Check found a problem that should be investigated

  Alert id       1606
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):

                 IXCH0242E One or more couple data sets have a single
                 point of failure.
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1606: IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
Alert 1606:  IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
```

SMF レコードのフラッドの検出 (1607)

SMF レコードのフラッドが検出されたことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ IFA780A で報告されます。このアラートを受信するには、WTO メッセージ IFA780A を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood detected

Alert: SMF record flood detected
System messages report SMF record flood detected
   Alert id        1607
   Date and time   03May2010 17:50:05.46
   WTO message     IFA780A SMF RECORD FLOOD MSG FILTER FOR TYPE 40
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1607: SMF record flood detected. WTO msgid:IFA780A SMF
RECORD FLOOD MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
```

```
Alert 1607:  SMF record flood detected. WTO msgid:IFA780A SMF RECORD FLOOD
MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
```

SMF レコードのフラッドによるレコードのドロップの開始 (1608)

SMF レコードのフラッドによりレコードのドロップが開始されたことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ IFA782A で報告されます。このアラートを受信するには、WTO メッセージ IFA782A を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood starts dropping records

Alert: SMF record flood starts dropping records
System messages report SMF record flood starts dropping records
   Alert id        1608
   Date and time   03May2010 17:00:00.33
   WTO message     IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1608: SMF record flood starts dropping records. WTO
msgid:IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
Alert 1608: SMF record flood starts dropping records. WTO msgid:IFA782A SMF
RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
```

フィルター規則によってブロックされたアタックがログに記録されなくなった – 監査証跡は不完全 (1609)

パケット・フィルター処理のロギングが有効でなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by filter rules are no longer logged

Alert: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1609
   Changed field IPSEC_LOGENABLE(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1609: Attacks blocked by filter rules are no longer logged - audit
trail incomplete in TCP/IP stack TCPIP

Alert 1609: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、パケット・フィルター処理のロギングが有効でないことを IP_STACK フィールド IPSEC_LOGENABLE が表していることが示されます。

アラートには、変更されたフィールドの名前 (IPSEC_LOGENABLE)、フィールドの古い値 (Yes)、フィールドの新しい値 (No)、およびセキュリティーの指示 (-) が示されます。

デフォルト・フィルター規則によってブロックされたアタックがログに記録されなくなった – 監査証跡は不完全 (1610)

暗黙的なデフォルト規則によって拒否されたパケットのロギングが有効でなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by default filter rules are no longer logged

Alert: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1610
   Changed field IPSEC_LOGIMPLICIT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP

Alert 1610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、暗黙的なデフォルト規則によって拒否されたパケットのロギングが有効でないことを IP_STACK フィールド IPSEC_LOGIMPLICIT が表していることが示されます。

SMF 119 サブタイプが書き込まれなくなった - 監査証跡は不完全 (1611)

以下のいずれかのアクションが行われたときに SMF 119 レコードが書き込まれなくなった場合に、このアラートが生成されます。

- ユーザーが FTP クライアント・コマンドを開始した (FTPCLIENT)。
- LINK の使用率に関連する統計が使用可能になった (IFSTAT)。
- トンネルが追加、除去、活動化、または非活動化された (IPSECURITY)。
- 予約された PORT の使用率に関連する統計が使用可能になった (PORTSTAT)。
- TCP 接続が確立された (TCPINIT)。
- TCP/IP スタックが活動化または終了された (TCPIPSTACK)。
- TCP/IP 統計が使用可能になった (TCPIPSTAT)。
- TCP 接続が終了された (TCPTERM)。
- TSO Telnet クライアント・コードが接続を開始または終了した (TN3270CLIENT)。
- UDP ソケットがクローズされた (UDPTERM)。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: SMF 119 FTPCLIENT is no longer written by stack name

Alert: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      1611
   Changed field SMF119_FTPCLIENT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1611: SMF 119 FTPCLIENT is no longer written - audit trail incomplete
in TCP/IP stack TCPIP

Alert 1611: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、関連付けられた SMF 119 サブタイプに対応する IP_STACK フラグ・フィールドが、指定されたサブタイプのレコードが書き込まれないことを表していることが示されます。

IP フィルター処理サポートおよび IPSec トンネル・サポートの非活動化 (1612)

IPv4 または IPv6 IP フィルター処理サポートおよび IPSec トンネル・サポートが活動化されなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: IPv4 IP filtering support and IPsec tunnel support deactivated

Alert: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP
   Alert id      1612
   Changed field IPCONFIG_IPSECURITY(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1612: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP

Alert 1612: IPv4 IP filtering support and IPsec tunnel
support deactivated in TCP/IP stack TCPIP
```

生成された E メールには、IPv4 IP フィルター処理および IPSec トンネル・サポートが活動化されていないことを IP_STACK フィールド IPCONFIG_IPSECURITY が表していること、または IPv6 IP フィルター処理および IPSec トンネル・サポートが活動化されていないことを IP_STACK フィールド IPCONFIG6_IPSECURITY が表していることが示されます。

1024 未満のポートが予約されなくなった (1613)

ユーザーに対して TCP ポートまたは UDP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: UDP ports below 1024 are not reserved anymore by stack name

Alert: UDP ports below 1024 are not reserved anymore in
TCP/IP stack TCPIP
   Alert id      1613
   Changed field UDP_RESTRICTLOWPORTS(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1613: UDP ports below 1024 are not reserved anymore in TCP/IP stack
TCPIP

Alert 1613: UDP ports below 1024 are not reserved anymore in TCP/IP stack TCPIP
```

生成された E メールには、ユーザーに対して TCP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されないことを IP_STACK フィールド TCP_RESTRICTLOWPORTS が表していること、またはユーザーに対して UDP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されないことを IP_STACK フィールド UDP_RESTRICTLOWPORTS が表していることが示されます。

インターフェースのセキュリティー・クラスの変更 (1614)

このインターフェースの IP フィルター処理で使用されるセキュリティー・クラスが変更された場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Security class changed for interface interface

Alert: Interface EELINK security class has changed in
TCP/IP stack TCPIP
   Alert id       1614
   Changed field  SECCLASS(255->238)
   Interface      EELINK
   Security class 238
   Stack          TCPIP
   System ID      DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1614: Interface EELINK           security class has changed in TCP/IP
stack TCPIP

Alert 1614: Interface EELINK security class has changed in TCP/IP stack TCPIP
```

生成された E メールには、IPv4 または IPv6 インターフェース名およびこのインターフェースの IP フィルター処理で使用されるセキュリティー・クラスが示されます。

IP フィルター規則の変更 (1615)

IP フィルター規則が変更、追加、または削除された場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: IP filter rules changed in TCP/IP stack TCPIP

Alert: IP filter rules changed in TCP/IP stack TCPIP
   Alert id                      1615
   Kind of change                CHG-
   Changed fields                LOG(Yes->No)-
   Source IP
   Source prefix length          0
   Source port                   0
   Destination IP
   Destination prefix length     0
   Destination port              0
   Protocol
   Type                          64
   Code                          0
   Packet filter logging enabled No
   Routing                       LOCAL
   Security class                0
   Stack                         TCPIP
   System ID                     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1615: IP filter rules changed in TCP/IP stack TCPIP

Alert:1615: IP filter rules changed in TCP/IP stack TCPIP
```

生成された E メールには、変更、追加、または削除された IP フィルター規則のいくつかの構成要素が示されます。示されるのはアウトバウンド規則のソース IP アドレス、ソース・サブネット・アドレスの接頭部の長さ、アウトバウンド規則のソース・ポート (TCP または UDP トラフィックの場合)、アウトバウンド規則の宛先 IP アドレス、宛先サブネット・アドレスの接頭部の長さ、アウトバウンド規則の宛先ポート (生成されたインバウンド規則のソース・ポートに対応)、規則が適用されるトラフィックのタイプ、ICMP 値 (ICMP トラフィックの場合)、デフォルト・フィルター規則でパケット・フィルターのロギングが有効かどうかの指示、規則が適用されるパケット・ルーティングのタイプ、および規則のセキュリティー・クラスです。

グループ・アラート

重要なグループへの接続 (1701)

ユーザー ID が重要なグループに接続された場合に、このアラートが生成されます。

このアラートを受信するには、SETROPTS 設定 SAUDIT、AUDIT(USER)、または AUDIT(GROUP) を有効にする必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:           C2POLICE at DINO
Subject:        Alert: C2RMUS02 issued connect to important group SYS1 for C2RMUS01

Alert: C2RMUS02 issued connect to important group SYS1 for C2RMUS01
User connected to an important group
   Alert id        1701
   Date and time   09Mar2005 14:49:55.90
   User            C2RMUS01
   Group           SYS1
   Result          Success
```

```
Issued by       C2RMUS02
Job name        C2RMUS0
System ID       DINO
Command         CONNECT C2RMUS01 GROUP(SYS1)
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1701:  C2RMUS02 issued connect to important group SYS1 for C2RMUS01

Alert 1701:  C2RMUS02 issued connect to important group SYS1 for C2RMUS01
```

生成された E メール・レポートには、どのユーザー ID がどの重要なグループに接続されたかが示されます。

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルでは、過度と見なされる違反の数を指定できます。また、除外するユーザー ID またはユーザー ID マスクを 10 個まで指定できます。 151 ページの『主要管理アクティビティー (1120 および 2120) 構成』を参照してください。

アプリケーション・アラート

zSecure Access Monitor が非アクティブ (1801)

zSecure Access Monitor が非アクティブであり、Access Monitor データが収集されない場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: zSecure Access Monitor not active

Alert: zSecure Access Monitor not active
System messages report the zSecure Access Monitor is no longer active

 Alert id        1801
 Date and time   03Feb2013 10:12:05.30
 WTO message     C2P0100A zSecure Access Monitor not active
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1801: zSecure Access Monitor not active

Alert 1801: zSecure Access Monitor not active
```

アラートには、zSecure Access Monitor がアクティブではなくなったことを示す WTO メッセージが表示されます。

zSecure サーバー接続の逸失 (1802)

パートナー zSecure サーバーへの最後の TCP 接続が失われた場合、アラートが送信されます。接続は、新しい割り振り要求が受信されるまでは失われたままになります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: zSecure Server connection lost

Alert: zSecure Server connection lost
```

```
System messages report the zSecure Server lost a connection

 Alert id       1802
 Date and time  03Feb2013 10:12:05.30
 WTO message    CKN165I 00 zSecure Server PROD1/S1 lost last connection to PROD2/S2
 System ID      DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1802: zSecure Server connection lost

Alert 1802: zSecure Server connection lost
```

アラートには、接続されなくなった zSecure サーバーを示す WTO メッセージが表示されます。

IBM Workload Scheduler ジョブが開始されていない (1804)

IBM Workload Scheduler ジョブが開始されなかった場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB39 has not started in application MYAPP39

Alert: Job JOB39 has not started in application MYAPP39
System messages report that a IWS Job has not started

   Alert id        1804
   Jobname         JOB39
   JES job id      JOB00584
   Application     MYAPP39
   Date and time   04May2014 22:47:34.54
   WTO message     EQQE039I LONG TIME ON INPUT QUEUE FOR JOB JOB39(JOB00
                   (010), APPL = MYAPP39, WORK STATION = CPUA,
                   IA=1404010034
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1804: Job JOB39    has not started in application MYAPP39

Alert 1804: Job JOB39 has not started in application MYAPP39
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

IBM Workload Scheduler ジョブの遅延 (1805)

IBM Workload Scheduler ジョブが遅延した場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB37 is late starting for application MYAPP37

Alert: Job JOB37 is late starting for application MYAPP37
System messages report that a IWS Job is late starting

   Alert id        1805
   Jobname         JOB37
   JES job id      1234
```

```
   Application     MYAPP37
   Date and time   14May2014 13:06:01.65
   WTO message     EQQE037I JOB RENEJOB1(1234),OPERATION (OPERNUM) IN APPLICATION MYAPP37 IS
                   LATE, WORK STATION = WSID, IA = ARRTIME
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1805: Job JOB37    is late starting for application MYAPP37

Alert 1805: Job JOB37    is late starting for application MYAPP37
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

IBM Workload Scheduler ジョブの失敗 (1806)

IBM Workload Scheduler ジョブが失敗した場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB36 ended in error in application MYAPP36

Alert: Job JOB36 ended in error in application MYAPP36
System messages report that a IWS Job ended in error

   Alert id        1806
   Jobname         JOB36
   JES job id      JOB32463
   Application     MYAPP39
   Date and time   14May2014 13:05:55.62
   WTO message     EQQE036I JOB JOB36   (JOB06424), OPERATION(0010),
       OPERATION TEXT(                          ), ENDED IN ERROR S806.
                   PRTY=5, APPL = MYAPP36         , WORK STATION = CPUA, IA= 1405150001,
                   NO E2E RC
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 1806: Job JOB36    ended in error application MYAPP36

Alert 1806: Job JOB36    ended in error application MYAPP36
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

事前定義 ACF2 アラート

ここでは、zSecure Alert に付属する ACF2 アラートのカテゴリーについて説明します。

ユーザー・アラート

以下のアラートは、特定のユーザーに関係するイベントのモニターと、ユーザーに対する変更の監査に使用されます。

緊急時ログオン ID を使用したログオン (2102)

緊急時用のログオン ID が TSO ログオンまたはバッチ・ジョブ実行依頼に使用された場合に、アラートが送信されます。

このアラートを受信するには、SMF レコード・タイプ 30 サブタイプ 1 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Emergency user IBMUSER  logged on

Alert: Emergency user IBMUSER logged on
Successful logon or job submit with a logonid meant for emergencies

   Alert id        2102
   Date and time   03Feb2006 09:38:44.94
   User            IBMUSER  IBM DEFAULT USER
   Job name + id   IBMUSER  TSU05900
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2102: emergency user IBMUSER  logged on

Alert 2102: emergency user IBMUSER logged on
```

生成された E メール・レポートには、システムへのログオンに使用されたログオン ID と、ログオンが成功したかどうかが示されます。

このアラートでは、サイトに合わせてパネルを構成できます。アラートを選択する際に、プロンプトがパネルに表示されます。使用するのは緊急時の場合のみとするログオン ID を 10 個まで入力できます。 149 ページの『緊急時ユーザー構成 (アラート 1102 および 2102)』を参照してください。

パスワードによる高い許可レベルのユーザーの取り消し (2104)

過度の無効なパスワード試行のために、システム・レベル権限 (SECURITY、NON-CNCL、または READALL) を持つユーザーが取り消された場合に、このアラートがトリガーされます。

侵入者がパスワードを推測しようとしたことが、このアラートの原因である可能性があります。

注: システム権限を持つすべてのユーザーが同時に取り消されないように注意する必要があります。SECURITY 権限を持つ、取り消されていないログオン ID を少なくとも 1 つ確実に復元するための何らかの手順を用意しておく必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Highly authorized user C##CX44  revoked for password violations

Alert: Highly authorized user C##CX44 revoked for password violations
System-level authorized user revoked due to excessive password attempts

   Alert id        2104
   Date and time   07Feb2006 14:58:27.13
   User            C##CX44  TEST USER
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2104: Highly authorized user C##CX44  revoked for password violations

Alert 2104: Highly authorized user C##CX44 revoked for password violations
```

レポートには、過度のパスワード違反のために取り消されたログオン ID および付随するプログラマー名が示されます。

システム権限の認可 (2105)

ユーザーがシステム・レベル権限 (SECURITY、NON-CNCL、または READALL) を取得した場合に、アラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: System authority granted to C##BMR2

Alert: System authority granted to C##BMR2
System-level authority granted to user

   Alert id        2105
   Date and time   29May2006 13:25:12.42
   Authority       SECURITY
   Granted to      C##BMR2  MARY ROBERTSON
   Logonid         C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2105: System authority granted to C##BMR2  by C##BMR1

Alert 2105: System authority SECURITY granted to C##BMR2 by C##BMR1
```

レポートには、認可されたシステム権限、権限を認可されたユーザー、および ACF2 コマンドを実行したユーザーが示されます。

システム権限の除去 (2106)

システム・レベル権限 (SECURITY、NON-CNCL、または READALL) がユーザーから除去された場合に、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: System authority removed from C##BMR1

Alert: System authority removed from C##BMR2
System-level authority removed from user

   Alert id        2106
   Date and time   29May2006 13:25:16.15
   Authority       SECURITY
   Removed from    C##BMR2  MARY ROBERTSON
   Logonid         C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2106: System authority removed from C##BMR2  by C##BMR1

Alert 2106: System authority SECURITY removed from C##BMR2 by C##BMR1
```

レポートには、除去された権限、権限を除去されたユーザー、および ACF2 コマンドを実行したユーザーが示されます。

無効なパスワード試行の制限の超過 (2111)

特定の時間枠で 1 つの特定のログオン ID に対して、無効なパスワードを指定して失敗したログオン試行が多すぎる場合に、このアラートが送信されます。測定間隔は、REPORT オプション **Interval** および **AverageInterval** の合計です。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドに関する情報を参照してください。.

「多すぎる」とは、5 回以上の試行と定義されます。別の制限を使用する場合、このアラートをインストール定義アラートにコピーする必要があります。新しいスケルトン・メンバーに以下のインスタンスが 7 つあります。

```
_cnt_historyInvPw1111(nd,<5), _cnt_totalInvPw1111(nd,>=5),
```

これらすべてを、5 の代わりに希望する制限を使用するように調整する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Invalid password attempts exceed limit for C##BSG2

Alert: Invalid password attempts exceed limit for C##BSG2
Excessive number of password attempts by user

   Alert id        2111
   Date and time   03Mar2006 13:30:04.39 - 03Mar2003 13:39:23.78
   Attempts        6
   User            C##BSG2  SUSAN GAYNOR
   Result          Violation
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2111: Invalid password attempts exceed limit for C##BSG2

Alert 2111: Invalid password attempts exceed limit for C##BSG2.
```

このアラートは、パスフレーズ違反の場合も生成されます。このアラートでは、パスワードとパスフレーズの違反を組み合わせた数が考慮されます。

生成された E メール・レポートには、ログオン試行が行われた間隔および試行回数が示されます。また、システムへのログオン試行に使用されたログオン ID およびログオンの状況が示されます。このアラートでは、ログオンは常に違反です。

パスワード・ヒストリーのフラッシュ (2112)

特定の時間枠で特定のログオン ID に対するパスワードの変更回数が、パスワード・ヒストリーの GSO 設定よりも多かった場合に、このアラートが送信されます。これは、ユーザーがパスワード・ヒストリー全体をフラッシュし、前のパスワードを再使用できるようにしたことを意味します。測定間隔は、REPORT オプション **Interval** および **AverageInterval** の合計です。「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」の REPORT コマンドに関する情報を参照してください。.

注: アラート 2112 と 2113 は関連しています。パスワード・ヒストリーのフラッシュ中にレポート作成間隔が終了した場合はアラート 2113 がトリガーされ、フラッシュが完了した場合はアラート 2112 が発生します。同じユーザーに対して複数のアラート 2113 を受信したが、アラート 2112 を受信しなかった場合、ヒストリーがフラッシュ済みかフラッシュ中と考えられますが、ユーザーはフラッシュにもう少し時間を必要としていた可能性があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Password history flushed for C##BSG2

Alert: Password history flushed for C##BSG2
Repeated PASSWORD commands flush password history

   Alert id        2112
   Date and time   05Mar2006 11:47:11.21 - 03Mar2006 11:47:12.04
   Pwd changes     33
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2112: Password history flushed for C##BSG2

Alert 2112: Password history flushed for C##BSG2
```

生成された E メール・レポートには、パスワード・ヒストリーのフラッシュが行われた間隔、パスワード変更回数、およびユーザーのパスワード・ヒストリーをフラッシュしたユーザーのログオン ID が示されます。

疑わしいパスワード変更 (2113)

特定の時間枠で特定のログオン ID に対するパスワードの変更回数が、5 回以上であった場合に、アラートが送信されます。

このパスワード変更は、パスワード・ヒストリーが完全にフラッシュされる (その結果、アラート 2112 が発生する) ほど多くはありません。別の制限を使用する場合、このアラートをインストール定義アラートにコピーする必要があります。新しいスケルトン・メンバーに、以下のインスタンスが 4 つあります。

```
#history(nd,<5) #total(nd,>=5),
```

これらはすべて、5 の代わりに目的とする制限を使用するよう調整してください。

詳細については、 121 ページの『パスワード・ヒストリーのフラッシュ (2112)』を参照してください。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Suspect password changes for C##BSG2

Alert: Suspect password changes for C##BSG2
Excessive number of PASSWORD commands by user

   Alert id        2113
   Date and time   03Mar2006 15:17:12.32 - 03Mar2006 15:17:13.11
   Pwd changes     7
   User            C##BSG2  SUSAN GAYNOR
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2113: Suspect password changes for C##BSG2

Alert 2113: Suspect password changes for C##BSG2
```

生成された E メール・レポートには、パスワード変更が行われた間隔、パスワード変更回数、およびパスワードが何度も変更されたログオン ID が示されます。

非 SECURITY ログオン ID による SECURITY 権限の使用 (2116)

SECURITY を持たないユーザーが、SECURITY 権限を使用してデータ・セットにアクセスした場合に、アラートが生成されます。

このアラートは、SECURITY 権限を持たないユーザーがすべてのデータ・セットにアクセスでき、また SECURITY を必要とするコマンドを正常に実行する可能性があることを意味します。この状態は、APF 許可ソフトウェアによって設定される可能性があります。

注: 原因となったプログラムを特定するための最初の試みとして、アラートが発行された時点までにジョブに関して記録された SMF レコードを分析する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: non-SECURITY user C##BDV1 accessed data set with SECURITY

Alert: non-SECURITY user C##BDV1 accessed data set with SECURITY
Successful data set access using SECURITY by user without SECURITY

   Alert id        2116
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          UPDATE
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2116: non-SECURITY user C##BDV1  accessed (UPDATE  ) with
SECURITY data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2116: non-SECURITY user C##BDV1 accessed (UPDATE  ) with SECURITY
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

非 NON-CNCL ログオン ID による NON-CNCL 権限の使用 (2117)

NON-CNCL を持たないユーザーが、NON-CNCL 権限を使用してデータ・セットにアクセスした場合に、アラートが生成されます。

このアラートは、ユーザーがすべてのデータ・セットにアクセスできることを意味します。この状態は、APF 許可ソフトウェアによって設定される可能性があります。

注: 原因となったプログラムを特定するための最初の試みとして、アラートが発行された時点までにジョブに関して記録された SMF レコードを分析する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: non-NON-CNCL user C##BDV1 accessed data set with NON-CNCL

Alert: non-NON-CNCL user C##BDV1 accessed data set with NON-CNCL
Successful data set access using NON-CNCL by user without NON-CNCL

   Alert id        2117
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          UPDATE
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2117: non-NON-CNCL user C##BDV1  accessed (UPDATE  ) with
NON-CNCL data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2117: non-NON-CNCL user C##BDV1 accessed (UPDATE  ) with NON-CNCL
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

非 READALL ログオン ID による READALL 権限の使用 (2118)

READALL を持たないユーザーが、READALL 権限を使用してデータ・セットにアクセスした場合に、アラートが生成されます。

このアラートは、ユーザーがすべてのデータ・セットを読み取れることを意味します。この状態は、APF 許可ソフトウェアによって設定される可能性があります。

注: 原因となったプログラムを特定するための最初の試みとして、アラートが発行された時点までにジョブに関して記録された SMF レコードを分析する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: non-READALL user C##BDV1 accessed data set with READALL

Alert: non-READALL user C##BDV1 accessed data set with READALL
Successful data set access using READALL by user without READALL

   Alert id        2118
   Date and time   17Jan2003 03:00:16.89
   Data set        D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
   Access          READ
   User            C##BDV1  DIONNE VONT
   Result          LOGGING
   Job name        C##BDV1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2118: non-READALL user C##BDV1  accessed (READ  ) with
READALL data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00

Alert 2118: non-READALL user C##BDV1 accessed (READ  ) with READALL
data set D##BEV.GBS001.D##Y.DC107SCK.BV0GBS00
```

無期限パスワードの有効化 (2119)

LIDZMAX 属性を割り当てることにより、あるログオン ID に対し無期限パスワードが有効化された場合、アラートが送信されます。無期限パスワードは、ログオン ID に MAXDAYS(0) が設定された場合に有効になります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert:  User C##ASCH enabled non-expiring password for C##ABRJ

Alert: User C##ASCH enabled non-expiring password for C##ABRJ
Non-expiring password has been enabled by assigning LIDZMAX

 Alert id        2119
 Date and time   03Feb2013 10:12:05.30
 User            C##ABRJ JOHN BROWN
 Issued by       C##ASCH SIRAM CHRISTIAN
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2119: User C##ASCH enabled non-expiring password for C##ABRJ

Alert 2119: User C##ASCH enabled non-expiring password for C##ABRJ
```

アラートには、コマンド発行者、および LIDZMAX 属性が設定されたログオン ID が示されます。

主要管理アクティビティー (2120)

zSecure Alert の REPORT オプション **AverageInterval** によって指定された間隔で、特定のユーザーに関して、構成された数よりも多くの ACF2 コマンドが記録された場合、アラートが送信されます。

zSecure Alert の REPORT オプション **AverageInterval** について詳しくは、「*IBM Security zSecure CARLa-Driven Components:* インストールおよびデプロイメント・ガイド」で、REPORT コマンドに関する情報を参照してください。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: 126 commands recorded for user CDADMIN

Alert: 126 commands recorded for user CDADMIN
Number of commands exceeds the configured 100

 Alert id        2120
 Date and time   03Feb2013 10:12:05.30
 User            CDADMIN   BATCH ADMIN JOB
 System ID       DINO

       Time  Event            Event type

       10:40 ChgLogonid       REPLACE
       10:40 ChgLogonid       REPLACE

       .... ..........       ........................................
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2120: 126 commands recorded for user CDADMIN

Alert 2120: 126 commands recorded for user CDADMIN
```

アラートには、ユーザー、発行されたコマンドの数、およびイベントのリストが示されます。

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルでは、過度と見なされる違反の数を指定できます。除外するユーザー ID またはユーザー ID マスクを 10 個まで指定できます。 151 ページの『主要管理アクティビティー (1120 および 2120) 構成』を参照してください。

データ・セット・アラート

このセクションでは、データ・セット・アクセスに関する事前定義アラートについて説明します。

データ・セットでの WARNING モード・アクセス (2201)

データ・セットがアクセスされ、警告モードのためアクセス権限が認可されました。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: WARNING mode READ    on data set CDS.SCDSSAMP

Alert: WARNING mode READ on data set CDS.SCDSSAMP
Data set access granted due to warning mode

   Alert id        2201
   Date and time   21Jan2006 09:11:11.01
   Data set        CDS.SCDSSAMP
   Granted access  READ
   Rule            CDS.-
   User            C##BMR1  MARY ROBERTSON
   Job name        C##BMR1
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2201: WARNING mode READ    by C##BMR1 on data set
CDS.SCDSSAMP

Alert 2201: WARNING mode READ by C##BMR1 on data set CDS.SCDSSAMP
```

レポートには、データ・セット、このデータ・セットへのアクセス権限を要求したユーザー、アクセス権限が照合された規則、および認可されたアクセス権限が示されます。

WARNING モードの規則は、このモード以外では規則が許可しないようなアクセス権限も含めて、リソースへのすべてのアクセス権限を認可します。WARNING モードは通常、アクセス制御を実施する前に、規則のアクセス設定の効果を分析するために使用されます。このモードは、実動に関する問題を克服するための一時的な手段として使用されます。このアラートを受信した場合、アクセス権限を許可できる

どうかを確認しなければなりません。許可できる場合、それに応じて規則のアクセス設定を変更します。このアクセス権限が生じてはいけないことになっている場合、必要に応じて是正措置を取ります。

APF データ・セットでの更新 (2204)

APF 許可データ・セットが更新された場合に、アラートが送信されます。

アラートを生成してはならない特権ユーザーおよびグループは、SE.A.S オプション「**Privileged users and groups for UPDATE on APF data sets**」で指定できます。

注: 環境データが含まれた CKFREEZE データ・セットは、リフレッシュすることが推奨されます。SETPROG コマンドまたは SET PROG コマンドを使用して APF リストを更新してから、MODIFY C2POLICE,COLLECT コマンドを使用します。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Update by C##ASCH  on APF data set C##A.D.C##NEW.APF.LOAD

Alert: Update by C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
APF data set successfully updated

   Alert id        2204
   Date and time   03Feb2003 10:12:05.30
   Data set        C##A.D.C##NEW.APF.LOAD
   Access          UPDATE
   User            C##ASCH
   Result          LOGGING
   Job name        C##ASCHL
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2204: Update by user C##ASCH  on APF data set
C##A.D.C##NEW.APF.LOAD

Alert 2204: Update by user C##ASCH on APF data set C##A.D.C##NEW.APF.LOAD
```

アラートには、更新されたデータ・セット、使用されたアクセス・レベル、およびデータ・セットにアクセスしたユーザーが示されます。

APF リストへのデータ・セットの追加 (2205)

SET PROG コマンドまたは SETPROG コマンドを使用して、データ・セットが APF リストに動的に追加された場合に、アラートが生成されます。

このアラートを生成するには、WTO メッセージ CSV410I が入手可能で、処理のために選択される必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set added to APF list: SYSPROG.APF.LOAD

Alert: Data set added to APF list: SYSPROG.APF.LOAD
A data set is dynamically added to the APF list

   Alert id        2205
   Date and time   21Feb2003 11:44:36.71
```

```
Data set        SYSPROG.APF.LOAD
Volume          <SMS MANAGED>
Console ID      R##SLIN
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2205: Data set added to APF list from console R##SLIN:
SYSPROG.APF.LOAD

Alert 2205: Data set added to APF list from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

アラートには、APF リストに追加されたデータ・セットおよびデータ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。SET PROG コマンドまたは SETPROG コマンドが SDSF から入力された場合は、ユーザーがそのコマンドを入力したコンソールの名前も示されます。コンソール名は、デフォルトではユーザーのログオン ID になります。

APF リストからのデータ・セットの除去 (2206)

SET PROG コマンドまたは SETPROG コマンドを使用して、データ・セットが APF リストから動的に除去された場合に、アラートが生成されます。

このアラートを生成するには、WTO メッセージ CSV410I が入手可能で、処理のために選択される必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set removed from APF list: SYSPROG.APF.LOAD

Alert: Data set removed from APF list: SYSPROG.APF.LOAD
A data set is dynamically removed from the APF list

Alert id        2206
Date and time   21Feb2003 11:44:36.71
Data set        SYSPROG.APF.LOAD
Volume          <SMS MANAGED>
Console ID      R##SLIN
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2206: Data set removed from APF list from console R##SLIN:
SYSPROG.APF.LOAD

Alert 2206: APF Data set removed from APF list from console R##SLIN:
SYSPROG.APF.LOAD on volume <SMS MANAGED>
```

アラートには、APF リストから除去されたデータ・セットおよびデータ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。SET PROG コマンドまたは SETPROG コマンドが SDSF から入力された場合は、ユーザーがそのコマンドを入力したコンソールの名前も示されます。コンソール名は、デフォルトではユーザーのログオン ID になります。

APF リストへのデータ・セットの追加の検出 (2207)

データ・セットが何らかの方法で APF リストに追加された場合に、このアラートが生成されます。

このアラートには、SET PROG コマンドまたは SETPROG コマンドの使用や、他の製品の使用などがあります。このアラートを生成するには、拡張モニターがアクティブである必要があります。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、データ・セットを追加するために使用されたユーザー ID、ジョブ名についての情報も、追加を実行するために使用されたプロセスについての情報もありません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert: Data set addition to APF list detected: SYSPROG.APF.LOAD
An addition of a data set to the APF list has been detected

       Alert id              2207
       Date and time         18Nov2016 03:50:29
       Data set              SYSPROG.APF.LOAD
       Volume                <SMS MANAGED>
       APF                   No
       APFLIST               Yes
       System ID             DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2207: Data set addition to APF list detected: SYSPROG.APF.LOAD

Alert 2207: Data set addition to APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

アラートには、APF リストに追加されたデータ・セットおよびデータ・セットが常駐するボリュームが示されます。データ・セットが SMS に管理される場合、ボリューム・フィールドには <SMS MANAGED> が示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、データ・セットを追加するために使用されたユーザー ID、ジョブ名についての情報も、追加を実行するために使用されたプロセスについての情報も提供しません。

APF リストからのデータ・セットの除去の検出 (2208)

データ・セットが何らかの方法で APF リストから除去された場合に、このアラートが生成されます。

このアラートには、SET PROG コマンドまたは SETPROG コマンドの使用や、他の製品の使用などがあります。このアラートを生成するには、拡張モニターがアクティブである必要があります。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、データ・セットを除去するために使用されたユーザー ID またはジョブ名についての情報も、除去を実行するために使用されたプロセスについての情報も提供しません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD
```

```
Alert: Data set removal from APF list detected: SYSPROG.APF.LOAD
A removal of a data set from the APF list has been detected.

       Alert id              2208
       Date and time         18Nov2016 03:50:29
       Data set              SYSPROG.APF.LOAD
       Volume                <SMS MANAGED>
       APF                   Yes
       APFLIST               No
       System ID             DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2208: Data set removal from APF list detected: SYSPROG.APF.LOAD
Alert 2208: Data set removal from APF list detected: SYSPROG.APF.LOAD
on volume <SMS MANAGED>
```

アラートには、APF リストから除去されたデータ・セットおよびデータ・セットが常駐するボリューム (または、データ・セットが SMS によって管理される場合は <SMS MANAGED>) が示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいているため、データ・セットを除去するために使用されたユーザー ID またはジョブ名についての情報も、除去を実行するために使用されたプロセスについての情報も提供しません。

PCI PAN データへの不定期アクセス (2209)

PCI PAN (クレジット・カード主要アカウント番号) データ・セットへの不定期の INPUT 以上のアクセスが成功した場合、アラートが送信されます。

オプション SE.A.P を使用すると、PCI PAN データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2209: INPUT access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN

Alert 2209: INPUT access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN
Non-regular acces

 Alert id        2209
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-PAN
 Access          INPUT
 User            C##ASCH SIRAM CHRISTIAN
 Result          LOGGING
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2209: INPUT access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN

Alert 2209: INPUT access by C##ASCH on PCI-PAN data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (INPUT など)、およびデータ・セットにアクセスしたユーザーが示されます。

平文の PCI PAN データへの不定期アクセス (2210)

平文の PCI PAN (クレジット・カード主要アカウント番号) データへの不定期の INPUT 以上のアクセスが成功した場合、アラートが送信されます。

オプション SE.A.P を使用すると、平文の PCI PAN データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2210: INPUT access by C##ASCH on PCI-PAN-clr data set
C##A.D.C##NEW.PAN

Alert 2210: INPUT access by C##ASCH on PCI-PAN-clr data set C##A.D.C##NEW.PAN
Non-regular access

 Alert id        2210
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-PAN-clr
 Access          INPUT
 User            C##ASCH SIRAM CHRISTIAN
 Result          LOGGING
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2210: INPUT access by C##ASCH on PCI-PAN-clr data set
C##A.D.C##NEW.PAN

Alert 2210: INPUT access by C##ASCH on PCI-PAN-clr data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (INPUT など)、およびデータ・セットにアクセスしたユーザーが示されます。

PCI AUTH データへの不定期アクセス (2211)

PCI AUTH (クレジット・カード機密認証データ) データ・セットへの不定期の INPUT 以上のアクセスが成功した場合、アラートが送信されます。

オプション SE.A.P を使用すると、PCI AUTH データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2211: INPUT access by C##ASCH on PCI-AUTH data set
C##A.D.C##NEW.PAN

Alert 2210: INPUT access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN
Non-regular access

 Alert id        2211
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.APF.LOAD
 Sensitivity     PCI-AUTH
 Access          INPUT
```

```
 User            C##ASCH SIRAM CHRISTIAN
 Result          LOGGING
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2211: INPUT access by C##ASCH on PCI-AUTH data set
C##A.D.C##NEW.PAN

Alert 2211: INPUT access by C##ASCH on PCI-AUTH data set C##A.D.C##NEW.PAN
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (INPUT など)、およびデータ・セットにアクセスしたユーザーが示されます。

サイト機密データ・セットに対するアクセス>=READ (2212)

サイト機密データ・セットに対する不定期の READ 以上のアクセスが成功した場合、アラートが送信されます。ACF2 の場合、これはアクセス INPUT、READBACK、OUTPUT、UPDATE、INOUT、OUTIN、または OUTINX になります。

オプション SE.A.S を使用すると、機密データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。アラートは、zSecure によって既に機密性が割り当てられているリソース (APF ライブラリー、JES スプール・データ・セットなど) には生成されません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2212: INPUT access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB

Alert 2212: INPUT access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB
Non-regular access

 Alert id        2212
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.MACLIB
 Sensitivity     Site-Dsn-R
 Access          INPUT
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2212: INPUT access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB

Alert 2212: INPUT access by C##ASCH on site sensitive READ data set
C##A.D.C##NEW.MACLIB
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (INPUT など)、およびデータ・セットにアクセスしたユーザーが示されます。

サイト機密データ・セットに対するアクセス>=UPDATE (2213)

サイト機密データ・セットに対する不定期の UPDATE 以上のアクセスが成功した場合、アラートが送信されます。ACF2 の場合、これはアクセス OUTPUT、UPDATE、INOUT、OUTIN、または OUTINX になります。

オプション SE.A.S を使用すると、機密データ・セットを指定できるほか、アラートを生成してはならない特権ユーザーおよびグループを指定できます。アラートは、zSecure によって既に機密性が割り当てられているリソース (APF ライブラリー、JES スプール・データ・セットなど) には生成されません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2213: OUTPUT access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB

Alert 2213: OUTPUT access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB
Non-regular access

 Alert id        2213
 Date and time   03Feb2013 10:12:05.30
 Data set        C##A.D.C##NEW.MACLIB
 Sensitivity     Site-Dsn-U
 Access          OUTPUT
 User            C##ASCH SIRAM CHRISTIAN
 Result          Success
 Job name        C##ASCHL
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject:  Alert 2213: OUTPUT access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB

Alert 2213: OUTPUT access by C##ASCH on site sensitive UPDATE data set
C##A.D.C##NEW.MACLIB
```

アラートには、アクセスされたデータ・セット、使用されたアクセス・レベル (OUTPUT など)、およびデータ・セットにアクセスしたユーザーが示されます。

UPDATE 機密メンバーに対するアクション (2214)

機密メンバーに対する UPDATE 以上のアクセスが成功した場合、アラートが送信されます。すなわち、INITIALIZE、DELETE、ADD、REPLACE、または RENAME のうち、いずれかのアクションがメンバーに対して行われた場合です。

SE.A.S. オプション「**UPDATE sensitive members in specific data sets**」を使用すると、当該メンバー、およびそれらのメンバーが属しているデータ・セットを指定できます。SE.A.S オプション 「**Privileged users and groups for site UPDATE sensitive resources**」を使用すると、アラートを生成してはならない特権ユーザーおよびグループを指定できます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert 2214: Action by C##ASCH on UPDATE sensitive member IEASYS81

Alert 2214:  Action by C##ASCH on UPDATE sensitive member IEASYS81
Action on UPDATE sensitive member
```

```
Alert id        2214
Date and time   03Feb2013 10:12:05.30
Data set        USER.PARMLIB
Action          REPLACE
Member          IEASYS81
Alias
Old Member
User            C##ASCH SIRAM CHRISTIAN
Job name        C##ASCHL
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2214: REPLACE action by C##ASCH on UPDATE sensitive member IEASYS81

Alert 2214: REPLACE action by C##ASCH on UPDATE sensitive member IEASYS81 in data
set USER.PARMLIB
```

アラートには、更新されたデータ・セットおよびメンバー、およびそのメンバーに対して実行されたアクションが示されます。

一般リソース・アラート

以下のアラートは、一般リソースの使用について報告します。

STC 用のデフォルト STC ログオン ID の使用 (2301)

開始タスクがデフォルト STC ログオン ID を使用すると、アラートが送信されます。

このアラートを生成するには、WTO メッセージ ACF9CCCD が入手可能で、処理のために選択される必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: STC default LID ACFSTCID used for STC IEFBR14A

Alert: STC default LID ACFSTCID used for STC IEFBR14A
A started task uses the STC default logonid

   Alert id        2301
   Date and time   11Feb2003 18:14:48.78
   Logonid         ACFSTCID
   Started task    IEFBR14A
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2301: STC default LID ACFSTCID used for STC IEFBR14A

Alert 2301: STC default LID ACFSTCID used for STC IEFBR14A
```

レポートには、使用された ACF2 デフォルト・ログオン ID と、開始タスクのメンバー名が示されます。このレポートには、開始タスクを開始したユーザーは示されません。

この開始タスクに GSO STC レコードを定義した場合、このアラートの原因を除去できます。これにより、この開始タスクについて、デフォルト・ログオン ID は検査されなくなります。

UNIX アラート

以下のアラートは、UNIX スーパーユーザー特権が取得された場合にトリガーされます。

ユーザーによるスーパーユーザー特権のあるシェルの取得 (2407)

ユーザーが、UNIX の su コマンドを使用してスーパーユーザー特権のあるシェルを取得した場合に、アラートが生成されます。

このアラートを受信するには、正常な READ ロギングを BPX.SUPERUSER FACILITY 規則項目に指定する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Superuser privileged shell obtained by user C##BSG1

Alert: Superuser privileged shell obtained by user C##BSG1
A user used su to obtain a shell with superuser privileges

Alert id        2407
Date and time   14May2003 14:15:21.98
User            C##BSG1  SUSAN GAYNOR
Job name        C##BSG1
System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2407: Superuser privileged shell obtained by user C##BSG1

Alert 2407: Superuser privileged shell obtained by user C##BSG1
```

レポートには、**su** を使用してスーパーユーザー特権のあるシェルを取得したユーザーが示されます。このユーザーは、UNIX サブシステム上のすべてのファイルまたはディレクトリーの読み取りと書き込みができます。

拡張属性の変更 (2409)

このアラートが活動化されている場合、UNIX ファイルまたはプログラムの拡張属性設定 (APF、プログラム制御、または _BPX_SHAREAS) で変更が検出されると通知メッセージが生成されます。このアラートを受信するには、z/OS システムのレベルは少なくとも 1.11 である必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Extended attribute changed for db2asc

Alert: Extended attribute changed for db2asc
Extended attributes indicate z/OS special handling

   Alert id         2409
   Date and time    19Jul2017 19:43:30.07
   Path             ./actuator/bin/db2asc
   Previous value   APF authorized;
   New value
   User             C##BER2 ERWIN RETTICH
   Job name         C##BER2
   System id        DINO
```

E メール通知では、**Previous value** および **New value** には、共有ライブラリー、APF 許可、およびプログラム制御の値を組み合わせたものが含まれる場合があります。

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2409: Extended attribute changed (APS-> APS) by <userid> for db2asc.

Alert 2409: Extended attribute changed (APS-> APS) by C##BER2 for db2asc
```

UNIX ファイル db2asc の拡張属性が変更されました。旧拡張属性と新規拡張属性は、括弧に入れて表示されます。ストリング APS は拡張属性 (APF 許可、プログラム制御、および共有ライブラリー) を表します。コマンドは C##BER2 によって発行されました。

ACF2 制御アラート

以下のアラートは、ACF2 GSO 設定の変更について報告します。

グローバル・セキュリティー対策の追加 (2501)

ACF2 GSO 設定が追加された場合に、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure added by C##BNA2

Alert: Global security countermeasure added by C##BNA2
ACF2 command used to add GSO setting

   Alert id        2501
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/value     WRNDAYS/5
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2501: Global security countermeasure added by C##BNA2

Alert 2501: Global security countermeasure added by C##BNA2: C-GSO-CRM     PSWD
```

アラートには、GSO 規則キー、GSO フィールドとその値、およびコマンドを実行したユーザーが示されます。

SNMP では、1 つの GSO 規則キー、GSO フィールド、および値のみが変数 whatParm によって送信されます。

グローバル・セキュリティー対策の削除 (2502)

ACF2 GSO 設定が削除された場合に、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure deleted by C##BNA2

Alert: Global security countermeasure deleted by C##BNA2
ACF2 command used to delete GSO setting
```

```
   Alert id        2502
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/value     WRNDAYS/5
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2502: Global security countermeasure deleted by C##BNA2

Alert 2502: Global security countermeasure deleted by C##BNA2: C-GSO-CRM     PSWD
```

アラートには、GSO 規則キー、GSO フィールドとその値、およびコマンドを実行したユーザーが示されます。

SNMP では、1 つの GSO 規則キー、GSO フィールド、および値のみが変数 whatParm によって送信されます。

グローバル・セキュリティー対策の変更 (2503)

ACF2 GSO 設定が変更された場合に、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Global security countermeasure changed by C##BNA2

Alert: Global security countermeasure changed by C##BNA2
ACF2 command used to change GSO setting

   Alert id        2503
   Date and time   23Jan2003 12:13:34.58
   Rule key        C-GSO-CRM     PSWD
   Field/Old/New   WRNDAYS/5/10
   User            C##BNA2  NICK AFTERSOCK
   Job name        C##BNA2
   System id       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2503: Global security countermeasure changed by C##BNA2

Alert 2503: Global security countermeasure changed by C##BNA2: C-GSO-CRM     PSWD
```

アラートには、GSO 規則キー、GSO フィールドおよびその古い値と新しい値、およびコマンドを実行したユーザーが示されます。

SNMP では、1 つの GSO 規則キー、GSO フィールド、および値のみが変数 whatParm によって送信されます。

システム・アラート

以下のアラートは、一般システム・イベントをモニターするためのものです。

SMF データ損失の開始 (2601)

SMF データ損失が開始されたことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ IEE351I、IEE979W、および IEE989I で報告されます。

注: 緊急の機密漏れが生じたら通知されるように、アラート 2602 を活動化することを選択できます。

このアラートを受信するには、WTO メッセージ IEE351I、IEE979W、および IEE989I を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: SMF data loss started

Alert: SMF data loss started
System messages report that SMF data loss has started

   Alert id        2601
   Date and time   10Feb2003 16:36:27.07
   WTO message     IEE979W SMF DATA LOST - NO BUFFER SPACE
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2601: SMF data loss started. WTO msgid: IEE979W

Alert 2601: SMF data loss started. WTO msgid: IEE979W
```

生成された E メールには、発行された WTO メッセージのみが示されます。

障害の後の SMF ロギングの再開 (2602)

バッファーがいっぱいになったため SMF データが失われたが、システムがロギングを再開した場合に、このアラートが生成されます。

注: アラート 2601 によって示される緊急の機密漏れが生じたら通知されるように、このアラートを活動化することを選択できます。

このアラートを受信するには、SMF レコード・タイプ 7 をログに記録する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF logging resumed after failure

Alert: SMF logging resumed after failure
SMF data is lost, but the system has resumed logging

   Alert id        2602
   Start of loss   10Feb2003 17:35:58.97
   Date and time   10Feb2003 17:36:27.12
   #records lost   4121
   System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2602: SMF logging resumed after failure.  4121 records lost.

Alert 2602: SMF logging resumed after failure. 4121 records lost.
```

生成された E メールには、データが失われた期間の開始時刻 (Start of loss) および終了時刻 (Resume time) が示されます。また、失われた SMF レコードの数が示されます。

SVC 定義の変更 (2603)

SVC テーブルまたは SVC ESR テーブルの SVC の定義で変更が検出されると、このアラートが生成されます。

このアラートには、変更された SVC の SVC および ESR 番号が示されます。SVC コードの現行アドレスが、現行 APF 状況と一緒に示されます。このアラートは、2 つのシステム・スナップショットの比較に基づいて生成されるため、変更がどのように実施されたかについての情報はありません。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at IDFX
Subject: Alert: SVC Definition changed: SVC/ESR 220/

Alert: SVC Definition changed: SVC/ESR 220/
A change in the definition of an SVC has been detected

   Alert id        2603
   SVC/ESR number  220/
   Address         00147080
   APF             Yes
   System ID       IDFX
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2603: SVC Definition changed: SVC/ESR 220/
Alert 2603: SVC Definition changed: SVC/ESR 220/ at address 00147080 APF
```

IBM Health Checker による重大度が低レベルの問題の検出 (2604)

重大度が低レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0001I で報告されます。

このアラートを受信するには、WTO メッセージ HZS0001I を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found low severity problem

Alert: IBM Health Checker found low severity problem
Check found a problem that should be investigated

  Alert id       2604
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):


                 ISGH0305E Global Resource Serialization synchronous
                 RESERVE processing
                 is not active.
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2604: IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
Alert 2604:  IBM Health Checker low severity: HZS0001I CHECK(IBMGRS,GRS_SYNCHRES):
```

IBM Health Checker による重大度が中レベルの問題の検出 (2605)

重大度が中レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0002E で報告されます。

このアラートを受信するには、WTO メッセージ HZS0002E を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found medium severity problem

Alert: IBM Health Checker found medium severity problem
Check found a problem that should be investigated

  Alert id       2605
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0002E CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):


                 ILRH0107E Page data set slot usage threshold met or
                 exceeded
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2605: IBM Health Checker medium severity: HZS0002E
CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
Alert 2605: IBM Health Checker medium severity: HZS0002E
CHECK(IBMASM,ASM_LOCAL_SLOT_USAGE):
```

IBM Health Checker による重大度が高レベルの問題の検出 (2606)

重大度が高レベルの問題を IBM Health Checker が検出したことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ HZS0003E で報告されます。

このアラートを受信するには、WTO メッセージ HZS0003E を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: IBM Health Checker found high severity problem

Alert: IBM Health Checker found high severity problem
Check found a problem that should be investigated

  Alert id       2606
  Date and time  10Feb2010 16:36:27.07
  System ID      DINO
  WTO message    HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):

                 IXCH0242E One or more couple data sets have a single
                 point of failure.
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2606: IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
Alert 2606:  IBM Health Checker high severity: HZS0003E CHECK(IBMXCF,XCF_CDS_SPOF):
```

SMF レコードのフラッドの検出 (2607)

SMF レコードのフラッドが検出されたことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ IFA780A で報告されます。

このアラートを受信するには、WTO メッセージ IFA780A を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood detected

Alert: SMF record flood detected
System messages report SMF record flood detected
   Alert id        2607
   Date and time   03May2010 17:50:05.46
   WTO message     IFA780A SMF RECORD FLOOD MSG FILTER FOR TYPE 40
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2607: SMF record flood detected. WTO msgid:IFA780A SMF
RECORD FLOOD MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
Alert 2607:  SMF record flood detected. WTO msgid:IFA780A SMF RECORD FLOOD
MSG FILTER FOR TYPE 40 EXCEEDED AT TIME=
```

SMF レコードのフラッドによるレコードのドロップの開始 (2608)

SMF レコードのフラッドによりレコードのドロップが開始されたことを WTO が報告した場合に、このアラートが生成されます。

このアラートは、メッセージ IFA782A で報告されます。

このアラートを受信するには、WTO メッセージ IFA782A を受信する必要があります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: SMF record flood starts dropping records

Alert: SMF record flood starts dropping records
System messages report SMF record flood starts dropping records
   Alert id        2608
   Date and time   03May2010 17:00:00.33
   WTO message     IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74
                   EXCEEDED AT TIME=
   System ID       NMPIPL87
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2608: SMF record flood starts dropping records. WTO
msgid:IFA782A SMF RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
Alert 2608: SMF record flood starts dropping records. WTO msgid:IFA782A SMF
RECORD FLOOD DROP FILTER FOR TYPE 74 EXCEEDED AT TIME=
```

フィルター規則によってブロックされたアタックがログに記録されなくなった – 監査証跡は不完全 (2609)

パケット・フィルター処理のロギングが有効でなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by filter rules are no longer logged

Alert: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      2609
   Changed field IPSEC_LOGENABLE(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2609: Attacks blocked by filter rules are no longer logged - audit
trail incomplete in TCP/IP stack TCPIP

Alert 2609: Attacks blocked by filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、パケット・フィルター処理のロギングが有効でないことを IP_STACK フィールド IPSEC_LOGENABLE が表していることが示されます。アラートには、変更されたフィールドの名前 (IPSEC_LOGENABLE)、フィールドの古い値 (Yes)、新しい値 (No)、およびセキュリティーの指示 (-) が示されます。

デフォルト・フィルター規則によってブロックされたアタックがログに記録されなくなった – 監査証跡は不完全 (2610)

暗黙的なデフォルト規則によって拒否されたパケットのロギングが有効でなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Attacks blocked by default filter rules are no longer logged

Alert: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      2610
   Changed field IPSEC_LOGIMPLICIT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP

Alert 2610: Attacks blocked by default filter rules are no longer logged -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、暗黙的なデフォルト規則によって拒否されたパケットのロギングが有効でないことを IP_STACK フィールド IPSEC_LOGIMPLICIT が表していることが示されます。

SMF 119 サブタイプが書き込まれなくなった - 監査証跡は不完全 (2611)

以下のいずれかのアクションが行われたときに SMF 119 レコードが書き込まれなくなった場合に、このアラートが生成されます。

- ユーザーが FTP クライアント・コマンドを呼び出した (FTPCLIENT)。
- LINK の使用率に関連する統計が使用可能になった (IFSTAT)。
- トンネルが追加、除去、活動化、または非活動化された (IPSECURITY)。
- 予約された PORT の使用率に関連する統計が使用可能になった (PORTSTAT)。
- TCP 接続が確立された (TCPINIT)。
- TCP/IP スタックが活動化または終了された (TCPIPSTACK)。
- TCP/IP 統計が使用可能になった (TCPIPSTAT)。
- TCP 接続が終了された (TCPTERM)。
- TSO Telnet クライアント・コードが接続を開始または終了した (TN3270CLIENT)。
- UDP ソケットがクローズされた (UDPTERM)。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: SMF 119 FTPCLIENT is no longer written by stack name

Alert: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
   Alert id      2611
   Changed field SMF119_FTPCLIENT(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2611: SMF 119 FTPCLIENT is no longer written - audit trail incomplete
in TCP/IP stack TCPIP

Alert 2611: SMF 119 FTPCLIENT is no longer written -
audit trail incomplete in TCP/IP stack TCPIP
```

生成された E メールには、関連付けられた SMF 119 サブタイプに対応する IP_STACK フラグ・フィールドが、指定されたサブタイプのレコードが書き込まれないことを表していることが示されます。

IP フィルター処理サポートおよび IPSec トンネル・サポートの非活動化 (2612)

IPv4 または IPv6 IP フィルター処理サポートおよび IPSec トンネル・サポートが活動化されなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: IPv4 IP filtering support and IPsec tunnel support deactivated

Alert: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP
   Alert id      2612
   Changed field IPCONFIG_IPSECURITY(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2612: IPv4 IP filtering support and IPsec tunnel support deactivated
in TCP/IP stack TCPIP

Alert 2612: IPv4 IP filtering support and IPsec tunnel
support deactivated in TCP/IP stack TCPIP
```

生成された E メールには、IPv4 IP フィルター処理および IPSec トンネル・サポートが活動化されていないことを IP_STACK フィールド IPCONFIG_IPSECURITY が表していること、または IPv6 IP フィルター処理および IPSec トンネル・サポートが活動化されていないことを IP_STACK フィールド IPCONFIG6_IPSECURITY が表していることが示されます。

1024 未満のポートが予約されなくなった (2613)

ユーザーに対して TCP ポートまたは UDP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されなくなった場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: UDP ports below 1024 are not reserved anymore by stack name

Alert: UDP ports below 1024 are not reserved anymore in
TCP/IP stack TCPIP
   Alert id      2613
   Changed field UDP_RESTRICTLOWPORTS(Yes->No)-
   Stack         TCPIP
   System ID     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2613: UDP ports below 1024 are not reserved anymore in TCP/IP stack
TCPIP

Alert 2613: UDP ports below 1024 are not reserved anymore in TCP/IP stack TCPIP
```

生成された E メールには、ユーザーに対して TCP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されないことを IP_STACK フィールド TCP_RESTRICTLOWPORTS が表していること、またはユーザーに対して UDP ポート 1 から 1023 が PORT ステートメントおよび PORTRANGE ステートメントによって予約されないことを IP_STACK フィールド UDP_RESTRICTLOWPORTS が表していることが示されます。

インターフェースのセキュリティー・クラスの変更 (2614)

このインターフェースの IP フィルター処理で使用されるセキュリティー・クラスが変更された場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: Security class changed for interface interface

Alert: Interface EELINK security class has changed in
TCP/IP stack TCPIP
   Alert id       2614
   Changed field  SECCLASS(255->238)
   Interface      EELINK
   Security class 238
   Stack          TCPIP
   System ID      DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2614: Interface EELINK           security class has changed in TCP/IP
stack TCPIP

Alert 2614: Interface EELINK security class has changed in TCP/IP stack TCPIP
```

生成された E メールには、IPv4 または IPv6 インターフェース名およびこのインターフェースの IP フィルター処理で使用されるセキュリティー・クラスが示されます。

IP フィルター規則の変更 (2615)

IP フィルター規則が変更、追加、または削除された場合に、このアラートが生成されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From:    C2POLICE at DINO
Subject: Alert: IP filter rules changed in TCP/IP stack TCPIP

Alert: IP filter rules changed in TCP/IP stack TCPIP
   Alert id                      2615
   Kind of change                CHG-
   Changed fields                LOG(Yes->No)-
   Source IP
   Source prefix length          0
   Source port                   0
   Destination IP
   Destination prefix length     0
   Destination port              0
   Protocol
   Type                          64
   Code                          0
   Packet filter logging enabled No
   Routing                       LOCAL
   Security class                0
   Stack                         TCPIP
   System ID                     DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2615: IP filter rules changed in TCP/IP stack TCPIP

Alert:2615: IP filter rules changed in TCP/IP stack TCPIP
```

生成された E メールには、変更、追加、または削除された IP フィルター規則のいくつかの構成要素が示されます。示されるのはアウトバウンド規則のソース IP アドレス、ソース・サブネット・アドレスの接頭部の長さ、アウトバウンド規則のソース・ポート (TCP または UDP トラフィックの場合)、アウトバウンド規則の宛先

IP アドレス、宛先サブネット・アドレスの接頭部の長さ、アウトバウンド規則の宛先ポート (生成されたインバウンド規則のソース・ポートに対応)、規則が適用されるトラフィックのタイプ、ICMP 値 (ICMP トラフィックの場合)、デフォルト・フィルター規則でパケット・フィルターのロギングが有効かどうかの指示、規則が適用されるパケット・ルーティングのタイプ、および規則のセキュリティー・クラスです。

アプリケーション・アラート

zSecure サーバー接続の逸失 (2802)

パートナー zSecure サーバーへの最後の TCP 接続が失われた場合、アラートが送信されます。接続は、新しい割り振り要求が受信されるまでは失われたままになります。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: zSecure Server connection lost

Alert: zSecure Server connection lost
System messages report the zSecure Server lost a connection

 Alert id        2802
 Date and time   03Feb2013 10:12:05.30
 WTO message     CKN165I 00 zSecure Server PROD1/S1 lost last connection to PROD2/S2
 System ID       DINO
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2802: zSecure Server connection lost

Alert 2802: zSecure Server connection lost
```

アラートには、接続されなくなった zSecure サーバーを示す WTO メッセージが表示されます。

IBM Workload Scheduler ジョブが開始されていない (2804)

IBM Workload Scheduler ジョブが開始されなかった場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB39 has not started in application MYAPP39

Alert: Job JOB39 has not started in application MYAPP39
System messages report that a IWS Job has not started

   Alert id        2804
   Jobname         JOB39
   JES job id      JOB00584
   Application     MYAPP39
   Date and time   04May2014 22:47:34.54
   WTO message     EQQE039I LONG TIME ON INPUT QUEUE FOR JOB JOB39(JOB00
                   (010), APPL = MYAPP39, WORK STATION = CPUA,
                   IA=1404010034
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2804: Job JOB39    has not started in application MYAPP39

Alert 2804: Job JOB39 has not started in application MYAPP39
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

IBM Workload Scheduler ジョブの遅延 (2805)

IBM Workload Scheduler ジョブが遅延した場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB37 is late starting for application MYAPP37

Alert: Job JOB37 is late starting for application MYAPP37
System messages report that a IWS Job is late starting

   Alert id        2805
   Jobname         JOB37
   JES job id      1234
   Application     MYAPP37
   Date and time   14May2014 13:06:01.65
   WTO message     EQQE037I JOB RENEJOB1(1234),OPERATION (OPERNUM) IN APPLICATION MYAPP37 IS
                   LATE, WORK STATION = WSID, IA = ARRTIME
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2805: Job JOB37    is late starting for application MYAPP37

Alert 2805: Job JOB37    is late starting for application MYAPP37
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

IBM Workload Scheduler ジョブの失敗 (2806)

IBM Workload Scheduler ジョブが失敗した場合、アラートが送信されます。

アラートの E メール・フォーマットは、以下のとおりです。

```
From: C2POLICE at DINO
Subject: Alert: Job JOB36 ended in error in application MYAPP36

Alert: Job JOB36 ended in error in application MYAPP36
System messages report that a IWS Job ended in error

   Alert id        2806
   Jobname         JOB36
   JES job id      JOB32463
   Application     MYAPP39
   Date and time   14May2014 13:05:55.62
   WTO message     EQQE036I JOB JOB36   (JOB06424), OPERATION(0010),
       OPERATION TEXT(                        ), ENDED IN ERROR S806.
                   PRTY=5, APPL = MYAPP36         , WORK STATION = CPUA, IA= 1405150001,
                   NO E2E RC
   System ID       TVT8018
```

アラートのテキスト・メッセージ・フォーマットは、以下のとおりです。

```
Subject: Alert 2806: Job JOB36    ended in error application MYAPP36

Alert 2806: Job JOB36    ended in error application MYAPP36
```

このアラートは、組織に合わせてカスタマイズできます。アラートを選択する際に、プロンプトがパネルに表示されます。このパネルで、このアラートを生成する必要がある IWS アプリケーションを指定できます。

事前定義アラートの構成

このセクションでは、事前定義アラートのいくつかをインストール固有の名前で構成する方法について説明します。

アラート定義 -「Specify action」

アラート定義パネルで「**Specify action**」を選択すると、以下のパネルが表示されます。

```
 Menu         Options       Info    Commands     Setup
_______________________________________________________________________________
                          zSecure Suite - Setup - Alert
Command ===> _____________________________________________________________

Specify action
_  TSO-RACF command
   _  Write TSO-RACF command to C2RCMD DD

   Specify command (Press Help key in this field for help)
   _____________________________________________________________________

Enter up to 5 EXCLUDE condition sets (use EGN masks)
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
X _____________________________________________________________________
```

図 *21.* 「*Setup Alert*」パネル: 「*Specify action*」

以下のフィールドが表示されます。

TSO-RACF command
このアラートに対して TSO-RACF コマンドを生成するには、このフィールドを選択します。

Write TSO-RACF command to C2RCMD DD
このフィールドと「**TSO-RACF command**」の両方にタグが付いている場合、生成されたコマンドは送信されず、C2RCMD DD に書き込まれます。

Specify command
このアラートに対して発行するコマンドを入力します。固定コマンド・ストリング部分を単一引用符 (') で囲みます。例えば、次のようにします。

```
'ALU' USER(0) 'REVOKE'
```

「Enter up to 5 EXCLUDE condition sets (use EGN masks)/(use ACF2 masks)」。これらのフィールドには、コマンドを生成すべきでない除外条件セットを 5 個まで入力できます。例えば、次のようにします。

```
USER=(IBMUSER,SYS*)
```

緊急時ユーザー構成 (アラート 1102 および 2102)

アラート 1102 または 2102 は、緊急時ユーザーによるログオンを意味します。このアラートを選択すると、以下のパネルが表示されます。このパネルで、緊急時ユーザーを 10 人まで入力できます。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
              zSecure - Setup - Alert
Command ===> ____________________________________________________________
Enter emergency users
User 1  . . . . . . . IBMUSER
User 2  . . . . . . . . ________. . . ________
User 3  . . . . . . . . ________. . . ________
User 4  . . . . . . . . ________. . . ________
User 5  . . . . . . . . ________. . . ________
User 6  . . . . . . . . ________. . . ________
User 7  . . . . . . . . ________. . . ________
User 8  . . . . . . . . ________. . . ________
User 9  . . . . . . . . ________. . . ________
User 10 . . . . . . . . ________. . . ________
```

図 22. 「*Setup Alert*」パネル: 緊急時ユーザーの構成 (アラート *1102* および *2102*) パネル

注: zSecure Alert では、少なくとも 1 人の緊急時ユーザーを入力することが想定されています。入力を行わない場合、デフォルトとして IBMUSER が使用されます。

過度の違反に対する取り消し (1115 および 2115) の構成

アラート 1115 および 2115 は、アラートの送信を行うだけでなく、違反が多すぎることを意味します。これらのアラートでは、問題のあるユーザーを取り消すことができます。

RACF アラート 1115 の場合、要求された修正アクションを実行できるようにするために、開始タスクを実行しているユーザーは、以下のタスクに対する十分な権限が必要です。

- RACF 取り消し、RACF システム全体にわたる SPECIAL、またはグループ SPECIAL など。RACF の資料を参照してください。
- CKGRACF DISABLE コマンド権限。管理対象のユーザーは、開始タスク・ユーザーの CKGRACF 範囲内になければなりません。「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を参照してください。

アラート 1115 を選択すると、以下のパネルが表示されます (2115 の場合も同様のパネルが表示されます)。

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                          zSecure - Setup - Alert
Command ===> ____________________________________________________________

Configure alert 1115: Too many violations

Number of violations    10

_  Issue RACF ALTUSER REVOKE command
_  Disable user with CKGRACF revoke schedule  ________

Exclude the following users from revocation
User 1  . . . . . . . ________
User 2  . . . . . . . ________. . . ________
User 3  . . . . . . . ________. . . ________
User 4  . . . . . . . ________. . . ________
User 5  . . . . . . . ________. . . ________
User 6  . . . . . . . ________. . . ________
User 7  . . . . . . . ________. . . ________
User 8  . . . . . . . ________. . . ________
User 9  . . . . . . . ________. . . ________
User 10 . . . . . . . ________. . . ________
```

図 *23.* 「*Setup Alert*」パネル*:* 過度の違反に対する取り消しの構成

以下のフィールドが表示されます。

Number of violations
アラート構成の一般設定パネルでフィールド「Average」によって指定されたヒストリー間隔において、許容される違反の最小数。有効な値は、1 から 999 の範囲の数値です。指定しない場合、デフォルト値 10 が使用されます。

RACF システムの場合、指定された違反数を超えると、開始タスクは、違反しているユーザーを取り消すために RACF コマンドまたは CKGRACF コマンドを発行する場合があります。

Issue RACF ALTUSER REVOKE command
このフィールドは RACF システムの場合のみ使用できます。このフィールドが選択されている場合、指定された違反数を超えると、RACF ALTUSER REVOKE コマンドが発行されます。

Disable user with CKGRACF revoke schedule
このフィールドは RACF システムの場合のみ使用できます。このフィールドが選択されている場合、指定された違反数を超えると、CKGRACF USER DISABLE コマンドが発行されます。

このフィールドは、zSecure Admin ライセンスが検出されている場合にのみ選択可能です。このオプションを選択した場合、取り消しスケジュールの名前の指定も行う必要があります。

このオプションは、「Issue RACF ALTUSER REVOKE command」と同時に指定することはできません。

User 1 から **User 10**
これらのフィールドでは、取り消しから除外する必要があるユーザー ID またはログオン ID を指定できます。

フィルターを使用して、複数のユーザー ID またはログオン ID を選択できます。フィルターには、% (すなわち、任意の 1 文字に相当) を含めることができ、* (すなわち、ゼロ個またはそれ以上の文字に相当) を末尾に置くことができます。

主要管理アクティビティー (1120 および 2120) 構成

アラート 1120 または 2120 は、主要管理アクティビティーに対して発行されます。

アラート 1120 または 2120 のいずれかを選択すると、以下のパネルが表示されます。過度と見なされるコマンドの数、およびアラートを生成してはならない最大 10 人のユーザーを入力できます。

このアラートを選択すると、以下のパネルが表示されます。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure - Setup - Alert
Command ===> ____________________________________________________________

Configure alert 1120: Major administrative activity

Number of commands  . . 100

Do not generate alert for the following users (filter allowed)
User 1  . . . . . . . . ________
User 2  . . . . . . . . ________. . . . ________
User 3  . . . . . . . . ________. . . . ________
User 4  . . . . . . . . ________. . . . ________
User 5  . . . . . . . . ________. . . . ________
User 6  . . . . . . . . ________. . . . ________
User 7  . . . . . . . . ________. . . . ________
User 8  . . . . . . . . ________. . . . ________
User 9  . . . . . . . . ________. . . . ________
User 10 . . . . . . . . ________. . . . ________
```

図 *24.* 「*Setup Alert*」パネル*:* 主要管理アクティビティーの構成 *(*アラート *1120* および *2120)*

注**:** zSecure Alert では、コマンドの数の値を入力することが想定されています。入力を行わない場合、デフォルトとして 100 が使用されます。

NONE よりも高い公開アクセス権限構成 (1304)

このパネルで、NONE よりも高いアクセス違反をアラートする必要があるクラス名を指定します。クラス値を指定しないでアラートを選択した場合、すべてのクラスに対してメッセージが生成されます。

```
 Menu  Options  Info  Commands  Setup         StartPanel
------------------------------------------------------------------------------
                        zSecure Suite - Setup Alert
Command ===> ____________________________________________________________________

Enter CLASS names to be monitored. Leave empty to monitor all classes.
1 . . . . . . . . . . . ________
2 . . . . . . . . . . . ________
3 . . . . . . . . . . . ________
4 . . . . . . . . . . . ________
5 . . . . . . . . . . . ________
6 . . . . . . . . . . . ________
7 . . . . . . . . . . . ________
8 . . . . . . . . . . . ________
9 . . . . . . . . . . . ________
10  . . . . . . . . . . ________
```

図 *25.* アラート *1304* の構成

重要なグループ (1701) の構成

重要なグループへの接続を意味するアラート 1701 を選択すると、以下のパネルが表示されます。

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                          zSecure - Setup - Alert
Command ===> ____________________________________________________________________
Specify important group(s)
Group  . . . . . . . SYS1      ________  ________  ________  ________  ________
                     ________  ________  ________  ________  ________  ________
                     ________  ________  ________  ________  ________  ________
                     ________  ________  ________  ________  ________  ________
```

図 *26.* 「*Setup Alert*」パネル*:* 重要なグループの構成 *(*アラート *1701)*

このパネルでは、重要なグループを 20 個まで入力できます。

複数のグループを選択する場合は、フィルター・パターンを使用することができます。フィルター・パターンには、パーセント記号 % (すなわち、1 文字に相当) を含めることができ、アスタリスク * (すなわち、ゼロ個またはそれ以上の文字に相当) を末尾に置くことができます。

IBM Workload Scheduler (1804、1805、1806、2804、2805、2806)

RACF アラート 1804、1805、1806、および ACF2 アラート 2804、2805、2806 については、アラートが選択されると、「Setup Alert」パネルが表示されます。

```
  Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                          zSecure - Setup - Alert
Command ===> ____________________________________________________________________

Enter application names
Application name 1  . . _________________
Application name 2  . . _________________
Application name 3  . . _________________
Application name 4  . . _________________
Application name 5  . . _________________
Application name 6  . . _________________
Application name 7  . . _________________
Application name 8  . . _________________
Application name 9  . . _________________
Application name 10 . . _________________
```

図 *27.* 「*Setup Alert*」パネル*: IBM Workload Scheduler* の構成 *(*アラート *1804*、*1805*、*1806*、*2804*、*2805*、*2806)*

最大 10 個の IWS アプリケーションを指定できます。

第 4 章 定期的な概要

定期的な概要を受信者のための覚え書として送信でき、これは、正しい設定か変更された設定かの確認に役立てることもできます。

この目的で、ジョブ C2PJRECI およびプロシージャー C2PCRECI が提供されています。ジョブ・スケジューリング・ソフトウェアで使用するデータ・セットにジョブ C2PJRECI をコピーし、必要に応じて調整する必要があります。特に、パラメーター ACONF をアラート構成が反映されるように調整し、パラメーター CONFIG を zSecure Alert 対応 zSecure 構成が反映されるように調整する必要があります。

zSecure 提供のジョブをカスタマイズする一般的な手順については、「*IBM Security zSecure Admin and Audit for RACF:* ユーザー・リファレンス・マニュアル」を参照してください。

第 5 章 問題判別ガイド

次の情報を使用して、zSecure Alert の問題を識別およびトラブルシューティングします。

一般的な概要に、問題が、zSecure Alert メインプログラムである C2POLICE の標準機能を提供するために使用される CKFCOLL プログラムまたは CKRCARLA プログラムで発生しているかどうかを判別する方法が説明されています。一般的な zSecure Alert 異常終了コードの解説と、ライセンス問題の診断方法が記載されています。また、zSecure Alert がアラートを生成しない状況について、いくつかのトラブルシューティングのヒントも示します。

問題診断に関する情報

次のガイドラインを使用して、zSecure Alert および zSecure Audit の問題を識別およびトラブルシューティングします。

ISPF インターフェースで問題が発生した場合は、5 ページの『第 2 章 zSecure Alert 構成』、またはご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」を参照してください。

zSecure Collect からの CKF*nnn* メッセージと、C2PCOLL 開始タスク (プログラム CKFCOLL) での異常終了に関する情報は、ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」に記載されています。

それ以外の問題の場合、最初のステップは、zSecure Alert 開始タスクの出力を見ることです。問題が発生する場所が、C2POLICE メインプログラムと、前処理ステップおよび実際のレポート作成ステップで使用される CKRCARLA プログラムのいずれであるかを判別する必要があります。zSecure Alert 開始タスクの出力は、一部がスプールに書き込まれ、一部が開始タスク C2POLICE の JCL で指定されたデータ・セットに書き込まれます。

CKR*nnnn* メッセージは、CKRCARLA プログラムによって発行されます。これらについての説明は、「*IBM Security zSecure:* メッセージ・ガイド」に記載されています。

C2P*nnnn* メッセージは、CKRCARLA プログラムによって発行されます。これらについての説明は、「*IBM Security zSecure:* メッセージ・ガイド」に記載されています。0 から 999 の範囲のメッセージ番号は、zSecure Alert 開始タスクを指しています。

CKRCARLA 問題診断

発生している問題が、CKRCARLA 処理内の問題であると判別された場合、次のステップは、その問題が前処理 (ステージ 1 処理とも呼ばれます) の一部として発生したか、アラート生成 (レポート作成フェーズとも呼ばれます) の一部として発生したかの判別になります。CKRCARLA を使用するたびに、SYSPRINT 出力が生成されます。最新の前処理実行の出力は、zSecure Alert JCL 内で SYSPRST1 DD 名に

割り振られたデータ・セットに入っています。同様に、最新の完了したレポート作成実行の出力は、SYSPRRPT にあります。zSecure Alert 開始タスクの JCL を調べて、これらのデータ・セットの名前を入手してください。これらのデータ・セットは、以降のレポート作成間隔 (デフォルトでは 1 時間ごと) のために zSecure Alert が CKRCARLA を呼び出すと再利用されるため、すぐにコピーを作成することを検討してください。zSecure Alert がまだ実行中の場合、これらのデータ・セットは既に再利用されている可能性があります。データ・セットの定義によっては、現在の CKRCARLA インスタンスによって最初の部分が上書きされている場合があります。コンテンツの信頼性を高めるには、まず zSecure Alert 開始タスクを停止する必要があります。zSecure Alert 開始タスクがまだ実行中の間にデータ・セットのコンテンツを検査する場合は、データ・セットの定義で同時共有アクセスが許可されていることを確認する必要があります。

完全な SYSPRINT に加えて、ゼロ以外の戻りコードで終了した CKRCARLA 呼び出しの出力のうちの選択した出力が、C2PDEBUG DD 名に割り振られたデータ・セットに追加されます。

SYSPRINT ファイル内の情報の検査時に、CKRCARLA に対して提供された入力ステートメントが予期したとおりであることを確認し、CKR*nnnn* メッセージを調べてください。この情報は常に、問題報告書の診断のために非常に重要です。

- レポート作成実行の SYSPRINT に、解決されなかった LIKELIST キーワード参照に関連するエラーが含まれている場合、それは、`stage 1` 実行での問題を指しています。
- CKR メッセージが構文エラーを示している場合、最も考えられる原因はスケルトン・メンバー内のエラーです。

詳しくは、ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」を参照してください。

zSecure Alert の問題診断

zSecure Alert が異常終了した場合は、『一般的な問題および異常終了』を参照してください。バッファー・サイズの問題を指している C2P メッセージを受け取った場合は、 5 ページの『第 2 章 zSecure Alert 構成』を参照してください。

それ以外の問題の場合は、IBM ソフトウェア・サポートに連絡して、以下の情報を提供してください。

- 問題が発生した環境についての説明
- C2POLICE メッセージ・ログ、または関連する SYSLOG の部分
- 使用した JCL と、入力コマンドのリスト

一般的な問題および異常終了

次のガイドラインを使用して、zSecure Alert の異常終了に対してトラブルシューティングおよび対応します。

このセクションでは、C2POLICEプログラム で発生する異常終了について説明します。異常終了が CKFCOLL プログラムまたは CKRCARLA プログラムで発生する場合、ご使用の zSecure 製品の「ユーザー・リファレンス・マニュアル」を参照してください。

以下のリストでは、zSecure Alert で発生する最も一般的なシステム異常終了コードをリストし、考えられる原因と修復に関する推奨事項を示します。お客様は最初に、異常終了と理由コードの正確な意味が記載されている、オペレーティング・システムの適切なメッセージ・マニュアルを確認する必要もあります。

001 ブロック・サイズの問題。ジョブ・ログでメッセージを調べて、DD 名を判別してください。この DD 名に連結を使用した場合は、最大のブロック・サイズが最初にあることを確認します。あるいは、最大ブロック・サイズを最初の DD ステートメントの DCB=BLKSIZE= パラメーターで指定します。

047 ロード・モジュールが、非 APF 許可ライブラリーから開始されています。C2POLICE STEPLIB が APF 許可ライブラリーであることを確認してください。

322 CPU 時間制限を超えました。ジョブ・ログをチェックして、異なる異常終了コードを示す異常終了メッセージが前に出ていないかどうかを調べてください。前に異常終了が発生していた場合は、この異常終了を解決します。

722 出力行数が多すぎます。

80A 878
GETMAIN エラー。EXEC ステートメントの REGION パラメーターを増やしてみてください。サイトの最大値に達した場合は、システム・プログラマーに連絡してください。

913 データ・セットの 1 つへのアクセスが拒否されました。ジョブ・ログで ICH408I または ACF99913 メッセージを検討し、どのデータ・セットであるかを判別してください。

D37 B37
出力データ・セットのいずれかが小さすぎたか、またはデータ・セットを拡張するためのスペースがボリューム上に残っていませんでした。ジョブ・ログでメッセージを調べて、DD 名を判別してください。

EC6 異常終了 EC6 は、UNIX サービスの実行中に異常終了が発生したことを意味します。何についての異常終了であるかを知るには、理由コードが必要です (例えば、CPU 時間の使用限度に到達 - この場合の理由コードは FD1D)。

IBM Security zSecure による問題で支援を得るには、一般に、少なくとも SYSMDUMP、使用した JCL、および入力コマンドのリストを提供する必要があります。

権限の問題

zSecure Alert の管理者は C2POLICE 開始タスクに対して z/OS オペレーター・コマンドを発行し、現在のパラメーター・メンバーの名前および C2PCUST のデータ・セット名を取得します。これは、MODIFY C2POLICE,DISPLAY を介して達成されます。必要な情報を得るために出力が構文解析されます。

REFRESH (F) 行コマンドについて、MODIFY C2POLICE,REFRESH が発行されます。

zSecure Alert は、管理者に TSOAUTH CONSOLE に対する (READ) 権限があるかどうかを検査します。許可されている場合、オペレーター・コマンドは CONSOLE を介して発行されます。許可されていない場合、zSecure Alert は、SDSF がインストールされているかどうか、および ISFSLASH インターフェースが使用可能かどうかを検証します。これが真である場合、オペレーター・コマンドは ISFSLASH を介して発行されます。実際にコマンドを実行するには、管理者には、MVS.MODIFY.STC.C2POLICE.C2POLICE を保護する OPERCMDS プロファイルに対する許可が付与されている必要があります。この許可が欠落している場合、権限の障害が発生します。

管理者による MODIFY コマンドの試行を阻止するには、TSOAUTH CONSOLE および SDSF ISFCMD.ODSP.ULOG.** へのアクセスを NONE にする必要があります。

ライセンス問題

zSecure Alert を使用するには、いずれかの zSecure Alert フィーチャーがインストールされていること、それを実行するシステム上で z/OS PARMLIB メンバー IFAPRDxx が無効になっていないことが必要です。それらのフィーチャーは外部セキュリティー・モニターを示しており、製品コード ALERTRACF および ALERTACF2 によって表されます。

zSecure Alert エンジン (C2POLICE) にライセンス問題がある場合は、C2PDEBUG ファイルを調べます。表示される情報が、予期していたものに対応するかどうかを検査してください。

予期したアラートが発生しない

予期したアラートが発生しない場合は、以下のような構成上の問題がないかどうかを確認してください。

- zSecure Alert が、アラートをファイルに送信するように構成されている (つまり、オプション SE.A.A のアクション R)。
- アラートが、アクティブ構成に含まれていない。アクティブ構成の名前は、オペレーター・コマンド MODIFY C2POLICE,DISPLAY で分かります。C2P メッセージ 127、128、および 135 を探すことができます。どの アラート構成を使用するかを動的に変更できない ことを思い起こしてください。「リフレッシュ」アクションは、異なるメンバーを活動化しません。メンバーの内容は、前回の stage 1 実行から変更されている可能性があります。変更した場合は、以下の点を考慮する必要があります。
  - アラート構成を「検査」したか
  - 構成をオンラインにするために「リフレッシュ」アクションを実行したか

– リフレッシュは成功したか

これは、zSecure Alert 開始タスク C2POLICE の JESMSGLG ファイルか、SYSLOG で検査できます。

- アラートはアクティブ構成に含まれているが、選択されていない。
- アラートに必要な SMF ロギングが活動化されていない。SMFPRM*xx* で、必要な SMF レコード・タイプが書き込まれるように指定しているかどうかを確認してください。事前定義アラートの要件については、 59 ページの『第 3 章 事前定義アラート』 の説明を参照してください。現行 SMF オプションは、オペレーター・コマンド DISPLAY SMF,O で分かります。 インストール定義アラートの場合は、正しいフィルター基準を指定しているかどうかを確認する必要があります。また、C2PCUST データ・セット・メンバー <set name>VP に、対応するフィルター基準が含まれているかどうかも確認する必要があります。
- アラートに必要な WTO が見つからない。WTO が MPFLSTxx、または、MPF に関連するいずれかの出口によってインターセプトされているかどうかを確認する必要があります。その出口は、IEAVMXIT でも、PARMLIB(MPFLSTxx) の USEREXIT パラメーターで指定した出口ルーチンでもかまいません。詳しくは、「MVS 初期設定およびチューニング解説書」を参照してください。

レポート作成実行からの SYSPRINT 出力 (157 ページの『CKRCARLA 問題診断』を参照) で、アラートが発行されたかどうかが分かります。WTO の場合は、CKR1239 が発行されます。SNMP トラップの場合は、CKR1227 が発行されます。このメッセージを検出した場合は、受信側を調べてください。E メールまたはテキスト・メッセージの場合は、CKR1225 が発行されます。このメッセージを検出した場合は、E メールまたはテキスト・メッセージが、まだ zSecure Alert 開始タスク C2POLICE の C2REMAIL ファイル内のスプール上に存在するかどうかを確認します。存在する場合は、オプション「SE.7」で SMTP 設定を確認し、システム・プログラマーに正しいパラメーターを問い合わせてください。それらの設定が正しければ、SMTP の問題が考えられます。E メールまたはテキスト・メッセージがスプール上に存在しない場合、それらは SMTP によって送信されています。SMTP ログを調べて、診断を進めてください。

SYSPRINT から、アラートが発行されなかったことが分かった場合は、メッセージ CKR1240 (Could not resolve to any SNMP receivers (どの SNMP 受信側へも解決できなかった)) の有無を確認します。重大度がゼロでない WTO のすべてのメッセージを調べてください。

アラートが何も送信されておらず、理由が分からない場合は、SMF ログか、WTO の SYSLOG を確認します。探しているイベントがログに記録されているかどうかを調べてください。「移動ウィンドウ」アラートの場合は、時間枠内でしきい値を超えていないかどうかを確認します。

このいずれのアクションも役立たない場合は、IBM ソフトウェア・サポートに連絡してください。その際に、環境と問題についての説明、レポート作成サブタスクからの SYSPRINT、および該当すると思われる場合は `Stage-1` サブタスクからの SYSPRINT、使用した JCL を手元に用意してください。また、それ以前の診断ステップで検出した予期しない結果があれば、それもお知らせください。

付録 A. SNMP 出力

独自の SNMP トラップを定義できます。SNMP トラップを定義するには、LIST/SORTLIST-output に特殊な形式が必要です。 zSecure Alert は、NEWLIST SNMP を使用して、LIST/SORTLIST 出力を自動的に処理することができます。出力の特殊な形式は、以下のようにする必要があります。

specific-trap ['**-c** *community*'] ['**-g** *global-trap*'.] ['**-e** *enterprise*'] /,
variable_1 <*variable_1* に割り当てられる内容> /,
variable_2 <*variable_2* に割り当てられる内容> /,
...
variable_n <*variable_n* に割り当てられる内容>

このテンプレートに準拠する CARLa 出力は、一連の割り当てステートメントです。それは、SNMP トラップの生成時に NEWLIST SNMP によって処理されます。これらの割り当ては、以下の事前定義変数を使用でき、管理情報ベース SCKRCARL(C2PMIB) ではユーザー定義変数を示す整数も使用できます。400000 から 699999 の範囲は、ユーザー定義変数用に予約されています。 4 桁の SNMP トラップ番号の後に、独自に選択した 2 桁の数字を使用する必要があります。SNMP 生成コードは以下のようになることがあります。

```
'eventIntegral'  'short description of the specific trap at hand' /,
'eventWhen' datetime(datetimezone,0) /,
```

必須出力を生成する CARLa の例を以下に示します。

```
)CM SNMP sortlist
)SEL &C2PERCTP = SNMP
  sortlist,
   recno(nd),
   '&c2pemem.' /,
   'eventIntegral',
    'Alert: APF list changed by SETPROG APF command' '-',
    'System messages report that SETPROG APF command is issued' /,
   'eventWhen' datetime(datetimezone,0) /,
   '&c2pemem.00' MsgTxt1(0,hor) /,
   'whereSYSTEM' system(0)
)ENDSEL
```

上記の例の変数は、'eventIntegral'、'eventWhen'、'&c2pemem.00'、および 'whereSYSTEM' です。'eventIntegral'、'eventWhen'、および 'whereSYSTEM' は事前定義変数で、'&c2pemem.00' はインストール定義変数です。

変数の内容には改行を含めてはなりません。繰り返しグループのフォーマット修飾子 firstonly または hor を強制的に付けることが必要な場合があります。

recno(nd) の後の行にある、*specific-trap* フィールドと呼ばれる '&c2pemem.' と / の間には、オプション -c *community*、-g *global-trap*、および -e *enterprise* を挿入できます。 *community* のデフォルト値は public で、*global-trap* はデフォルトで 6 になります。これは、エンタープライズ特定トラップであることを示します。*enterprise* はデフォルトで 1.3.6.1.4.1.9399.1.2 になります。これは enterprises.consul.software.zAlert であることを示します。 specific-

trap、community、global-trap、および enterprise パラメーターについて詳しくは、RFC 1215 などの SNMP 資料を参照してください。

SNMP 出力には以下のような事前定義変数が出現する可能性があります。

表 *8. SNMP* 出力に出現する可能性のある事前定義変数

変数	説明
eventIntegral	人間が判読できるアラートのタイトル。大半は E メール・レポートのタイトルと同じです。
eventWhen	日時。
fromWhereCONSOLE	ユーザーがコマンドを入力したコンソール。
fromWhereTERMINAL	端末 ID。
onWhatACCESS	RACF により許可されたアクセス権限。
onWhatALLOWED	WARNING モードにより認可されたアクセス権限を除き、セキュリティー規則によって許可されたアクセス・レベル。onWhatGRANTED を参照してください。
onWhatAUTHORITY	認可または除去されるシステム・レベル権限。
onWhatCLASS	一般プロファイルが置かれているクラス。
onWhatDSNAME	アラートに対応して、アクセス試行が行われた時点で更新されるか、プログラムの起点であるデータ・セット。
onWhatGRANTED	認可されたアクセス・レベル。WARNING モードにより認可されたアクセス権限が含まれます。onWhatALLOWED を参照してください。
onWhatGROUP-AUTHORITY	認可または除去されるグループ・レベル権限。
onWhatINTENT	要求されたアクセス・レベル。
onWhatNEW-PERMISSIONS	**chmod** コマンドの後の UNIX ファイルまたはディレクトリーの許可。
onWhatOLD-PERMISSIONS	**chmod** コマンドの前の UNIX ファイルまたはディレクトリーの許可。
onWhatPATH1	要求されたパス名 (拡張長再配置セクション 263 に対応)。
onWhatPROFILE	アクセス権限チェックに使用される一般リソースまたはデータ・セット・プロファイル。
onWhatRACFCMD-AUTH	RACF コマンドで使用される接続権限。
onWhatRACFCMD-GROUP	RACF コマンドで使用されるグループ。
onWhatRACFCMD-NAME	RACF コマンドで使用されるユーザーのプログラマー名。
onWhatRACFCMD-USER	RACF コマンドまたは ACF2 コマンドで使用されるユーザーのユーザー ID。

表 8. SNMP 出力に出現する可能性のある事前定義変数 (続き)

変数	説明
onWhatRESOURCE	RACF または ACF2 がアクセス権限チェックを行うリソース。このリソースは一般リソースでもかまいません。RACF の命名規則テーブルを使用したデータ・セット名から作成されるリソースにすることもできます。SMF 記述クラス PROGRAM の場合は、実行されるプログラムの名前になります。
onWhatUNIX-ACCESS-ALLOWED	許可された UNIX アクセス権限。
onWhatUNIX-ACCESS-INTENT	意図された UNIX アクセス権限。
onWhatUNIX-PATHNAME	ファイルまたはディレクトリーの絶対パスまたは相対パス。使用される CKFREEZE ファイルが UNIX=YES (および AUTOMOUNT=YES) で作成されたもので、ファイルまたはディレクトリーが含まれている場合は、絶対パス名になります。
onWhatVOLUME	データ・セットが置かれているボリューム、またはデータ・セットが SMS で管理されている場合は <SMS MANAGED>。
onWhatWORKTYPE	ログオンのタイプにより、「TSO」または「OMVS」のいずれか。
whatATTEMPTS	実施された試行の数。
whatCOMPCODE	ジョブまたはステップの完了コード。
whatCOMPSTAT	ジョブまたはステップの完了状況。
whatCOUNT-SMF-LOST	バッファーがフルになったために失われた SMF レコードの数。
whatDESC	イベントの状況に応じて、このフィールドは、「Success」、「Undefined user」、「Violation」、または「Warning」のいずれかになります。
whatEVENT	人間が判読できるイベント ID。
whatEVENTDESC	イベントの名前、結果の標識 (「Success」、「Warning」、「Failure」、または「Undefined」)、およびイベント修飾子の短い説明 (例: Invalid password) が含まれます。
whatEVENTQUAL	数値イベント修飾子。
whatJOBID	イベントが作動させたか、イベントによって作成されるジョブのジョブ ID。
whatJOBNAME	イベントが作動させたか、(ログオンなどの) イベントによって作成されるジョブのジョブ名。
whatJOBTAG	システム ID、ジョブ名、リーダー日付、およびリーダー時刻。
whatLOGSTR	SAF ログ・ストリング。
whatPARM	ACF2 GSO フィールド、古い値、および新規値

表 8. SNMP 出力に出現する可能性のある事前定義変数 (続き)

変数	説明
whatPROGRAM	プログラム名。
whatPWDCHANGES	最終測定間隔で行われたパスワード変更の数
whatRACFCMD	アラートを作動させた RACF コマンド。 (権限が不十分なために) 無視されるキーワードには <IGNORED> のラベルが付きます。
whatRECORDDESC	レコードを要約する記述ストリング。
whatRULE	ACF2 規則
whatSTC	開始タスク・プロシージャーの名前。
whatSTEPNAME	ステップ名。
whatSUBTYPE	SMF レコード・サブタイプ。
whatTYPE	SMF 数値レコード・タイプ。
whatUACC	プロファイル上の UACC セット。
whatVIOLATIONS	違反の数。
whatWTO-MESSAGE	WTO の出力の先頭行。この行は WTO メッセージ ID で始まります。
whenSMF-FAILURE	バッファーがフルのために、SMF データが失われた期間の開始日時。終了日時は eventWhen フィールドで確認できます。
whenStart	開始日および開始時刻。
whereSYSTEM	システム名。
whereSYSTYPE	オペレーティング・システムのタイプ。
whoNAME	whoUSERID でのユーザーのプログラマー名。
whoUSERID	SMF レコードまたは WTO レコードが書き込まれる原因となったユーザーのユーザー ID。

付録 B. NetView 構成

この付録の情報は以下の目的で使用されます。

- zSecure Alert 用に AIX および Windows 上で NetView を構成する
- ユーザー定義アラートを管理情報ベースに追加する
- AIX システムおよび Windows システム用に addtrap コマンドを作成する

AIX および Windows 用の NetView の構成

このタスクについて

このセクションでは、(ユーザー定義の) zSecure Alert トラップを適切に表示するための NetView の構成方法について説明します。このタスクには、SNMP トラップ構成ファイルに特定のトラップ・アスペクトをインポートするためのシェル・スクリプトの実行が含まれます。

このセクションでは、`zSecure-Alert-addtraps.sh` は、IBM 提供の AIX 用トラップ構成シェル・スクリプトの省略形として使用されます。これと同様に、`user-addtraps.sh` は、ユーザー定義のトラップ構成スクリプトの省略形として使用されます。これらのファイルの Windows バージョンは、`zSecure-Alert-addtraps.bat` および `user-addtraps.bat` と呼ばれます。`user-addtraps.sh` の作成方法については、174 ページの『AIX 用の addtrap コマンド』を参照してください。

IBM Knowledge Center で、ご使用のバージョンの IBM Security zSecure Suite 用の「サンプル」ページから、IBM 提供のファイルをダウンロードできます。「サンプル」ページは、「*IBM Security zSecure Documentation CD*」にも含まれています。Documentation CD の .iso ファイルのダウンロード方法については、ライセンス文書の入手を参照してください。

AIX 用の NetView の構成

このタスクについて

AIX 上で zSecure Alert 用に NetView を構成するには、(場合によるとユーザー拡張の) zSecure Alert MIB を NetView にロードする必要があります。次に、次の手順を実行します。ほとんどのステップには、スーパーユーザー特権が必要です。ユーザー定義のトラップがない場合は、`user-addtraps.sh` に関連するステップを無視できます。

AIX 5.2 では、NetView 構成の実行に Tivoli NetView バージョン 7.1.5 を使用していました。 NetView バージョン 7.1.5 以上を使用する必要があります。

手順

1. 最新バージョンの `zSecure-Alert-addtraps.sh` ファイルが含まれるディレクトリーを見つけます。

2. 最新バージョンの user-addtraps.sh ファイルが含まれるディレクトリーを見つけます。
3. zSecure-Alert-addtraps.sh ファイルが含まれるフォルダーから sh zSecure-Alert-addtraps.sh を実行します。 これにより、IBM 提供の zSecure Alert 定義を NetView トラップ構成ファイル (/usr/OV/conf/C/trapd.conf) に配置します。このステップを以前に実行している場合は、IBM 提供の古い zSecure Alert 定義が新しい定義に置き換えられます。
4. user-addtraps.sh ファイルが含まれるフォルダーから sh user-addtraps.sh を実行します。 これにより、ユーザー定義の zSecure Alert 定義を NetView トラップ構成ファイル (/usr/OV/conf/C/trapd.conf) に配置します。このステップを以前に実行している場合は、古いユーザー定義が新しい定義に置き換えられます。
5. snmptrap コマンドを使用して、サンプル・トラップを送信できます。ここで、*IP.NBR.COMP* はご使用のコンピューターの IP 番号です。

```
/usr/OV/bin/snmptrap -p 162 IP.NBR.COMP ¥
.1.3.6.1.4.1.9399.1.2 "" 6 1601 "" ¥
.1.3.6.1.4.1.9399.1.2.1 OctetString "Variable eventIntegral sample" ¥
.1.3.6.1.4.1.9399.1.2.2 OctetString "Variable eventWhen sample" ¥
.1.3.6.1.4.1.9399.1.2.31 OctetString "Variable whatWTO-MESSAGE sample" ¥
.1.3.6.1.4.1.9399.1.2.6 OctetString "Variable whereSYSTEM sample"
```

6. トラップが正しく処理されたかどうか確認できます。

Windows 用の NetView の構成

このタスクについて

Windows 上で zSecure Alert 用に NetView を構成するには、(場合によるとユーザー拡張の) zSecure Alert MIB を NetView にロードする必要があります。次に以下のステップを実行します。ユーザー定義のトラップがない場合は、user-addtraps.bat に関連するステップを無視できます。

Microsoft Windows 2000 (Service Pack 4) では、上記のステップの実行に NetView バージョン 7.1.5 を使用していました。

手順

1. 最新バージョンの zSecure-Alert-addtraps.bat ファイルが含まれるディレクトリーを見つけます。
2. 最新バージョンの user-addtraps.bat ファイルが含まれるディレクトリーを見つけます。
3. zSecure-Alert-addtraps.bat ファイルが含まれるフォルダーから zSecure-Alert-addtraps.bat を実行します。 これにより、zSecure Alert 定義が正しい場所に配置されます。このステップを以前に実行している場合は、古い zSecure Alert 定義が新しい定義に置き換えられます。
4. user-addtraps.bat ファイルが含まれるフォルダーから user-addtraps.bat を実行します。 これにより、ユーザー定義の zSecure Alert 定義が正しい場所に配置されます。このステップを以前に実行している場合は、古いユーザー定義が新しい定義に置き換えられます。

ユーザー定義アラートの MIB への追加

このセクションでは、ユーザー定義アラート (トラップとも呼ばれます) を使用した管理情報ベース (MIB) の拡張機能について説明します。 MIB は、AIX または Windows で実行されている NetView を使用してインポートできます。これについては、 167 ページの『AIX および Windows 用の NetView の構成』で説明しています。

zSecure Alert は、拡張予定の元の MIB ファイルを提供します。その名前は *zSecure-Alert-v210.mib* のようになっています。

トラップのメイン・コンポーネントは変数です。zSecure Alert MIB で定義される変数のみを使用してトラップを定義できますが、追加の変数を定義して使用することもできます。 『変数』では、MIB に変数を定義する方法を示します。これらの変数はトラップで使用されます。その定義については 171 ページの『トラップ』で説明しています。『ユーザー定義アラートの MIB への追加』には複数の MIB ファイルを組み合わせる方法が示されています。これは、zSecure Alert 提供だがユーザー拡張の MIB があり、新規の zSecure Alert MIB を受け取る場合に必要です。

変数

トラップの一部である変数を zSecure Alert 提供 MIB で既に定義されている変数から選択できます。ただし、新規変数を定義してそれらを MIB に追加し、トラップで使用することもできます。変数定義の完全構文については RFC 1212 (`www.faqs.org/rfcs`) を参照してください。以下は、簡単な変数定義構文と変数定義の例です。

```
name OBJECT-TYPE          | user-whatATTEMPTS OBJECT-TYPE
   SYNTAX syntax          |     SYNTAX DisplayString (SIZE (0..1023))
   ACCESS access          |     ACCESS read-only
   STATUS status          |     STATUS mandatory
   DESCRIPTION            |     DESCRIPTION
          description     |            "Number of password attempts"
   ::= { Alert number }   |     ::= { Alert 400047 }
```

変数には以下のコンポーネントがあります。

name *name* は小文字で始まっていなければなりません。小文字、大文字、数字、およびダッシュ (-) のみ使用できます。以下が変数名の例です。

```
user-whatATTEMPTS
```

zSecure Alert によって既に定義されている変数名は、アラート・アスペクトの簡略説明です。変数名に複数の語が含まれていると、`justLikeThis` のように、最初の語以外の語はそれぞれ大文字で始まります。これらの規則も使用できます。今後 zSecure Alert 提供のあらゆる変数名との競合を防ぐため、サンプル変数 `user-whatATTEMPTS` のように、個々のユーザー定義変数名の前に `user` または `user-` を付けることができます。

zSecure Alert 提供の変数名の大半には、`who`、`what`、`onWhat`、`when`、`where`、`whereTo`、または `fromWhere` が含まれ、アスペクト・ドメインを示します。また、変数と CARLa (つまり、CARLa Auditing and Reporting Language) フィールド間に直接の対応がある場合、その変数名は大文字で書かれたフィールド名で終了します。

syntax

syntax には複数の形式がありますが、通常は以下のようになります。

```
DisplayString (SIZE (0..1023))
```

この形式を使用すると、変数には 1023 文字まで使用できます。

access *access* には複数の形式がありますが、通常は以下のようになります。

```
read-only
```

status *status* には複数の形式がありますが、通常は以下のようになります。

```
mandatory
```

description

description は以下のような引用符付きストリングです。

```
"this description"
```

number

number は以下のような正整数です。

```
432100
```

変数名と数値は、拡張する MIB 内で固有である必要があります。 MIB は OBJECT-TYPE ステートメントを使用して複数の変数を定義します。個々のステートメントは以下で始まり、

name OBJECT-TYPE

以下で終了します。

::= { Alert *number* }

新規変数は、MIB 内のどの OBJECT-TYPE キーワードの前でもまだ使用されていない名前を取得する必要があります。この新規変数は、MIB 内の ::= { Alert *number* } でまだ使用されていない数値を取得する必要があります。 4 桁のトラップ番号の後に、独自に選択した 2 桁の数字を使用する必要があります。 171 ページの『トラップ』に示すように、ユーザー定義のトラップ番号は 4000 から 6999 までの範囲の数値でなければなりません。そのため、ユーザー定義変数の数値は、ユーザー定義変数用に予約された範囲である 400000 から 699999 までででなければなりません。この範囲外の変数番号は、IBM 用に予約されています。

注**:** これらの予約は、1.3.6.1.4.1.9399.1.2 とコード化されるエンタープライズ・ツリー iso.org.dod.internet.private.enterprises.consul.software.zAlert に属します。

変数定義のコンポーネントが決まったら、既存の変数定義の直後にそれを挿入することにより、MIB に定義を追加します。定義は MIB の中で、::= { Alert *n* } で終了します。

ユーザーが使いやすいように、変数定義をソートして、変数番号が小さい順に出現するようにします。ソートによって予約済みの変数番号を簡単に確認することができます。順序のソートは必須ではありません。

変数について詳しくは、www.faqs.org/rfcs にある RFC 1212 を参照してください。

トラップ

トラップ定義の完全構文については RFC 1215 (www.faqs.org/rfcs) を参照してください。簡単なトラップ定義構文とサンプルのトラップ定義は、以下の例のようになります。

```
name TRAP-TYPE          | smfDataLost TRAP-TYPE
   ENTERPRISE Alert     |     ENTERPRISE Alert
   VARIABLES {          |     VARIABLES {
                v1,     |                   eventIntegral,
                v2,     |                   eventWhen,
                ...     |                   whatWTO-MESSAGE,
                vm      |                   whereSYSTEM
              }         |                 }
   DESCRIPTION          |     DESCRIPTION
         description    |             "SMF data is lost"
   ::= number           |     ::= 1601
```

トラップ定義構文にあるように、トラップ定義には複数のコンポーネントがあります。

name トラップの名前は小文字で始まっていなければなりません。小文字、大文字、数字、およびダッシュ (-) のみ使用できます。以下がトラップ名の例です。

```
smfDataLost
```

変数のリスト

トラップの一部として送信される変数 v_1、v_2、. . .、v_m。トラップの VARIABLES セクションにリストされている個々の変数は、OBJECT-TYPE として定義されている必要があります。変数定義については、 169 ページの『変数』で説明されています。

注: MIB 構文規則により、ゼロ変数のトラップは VARIABLES { ... } セクションを持つことができません。

description

zSecure Alert によって既に定義されているトラップ名は、アラートの簡略説明です。トラップ名に複数の語が含まれていると、justLikeThis のように、最初の語以外の語はそれぞれ大文字で始まります。これらのトラップ命名規則も使用できます。description は以下のような引用符付きストリングです。

```
"this description"
```

number

number は以下のような正整数です。

```
1601
```

トラップ名と数値は、拡張する MIB 内でまだ使用されていない必要があります。

ユーザー定義トラップは、zSecure Alert 提供のトラップ定義をコピーするだけで作成されます。変数名を保持して、name、description、および number を固有値で上書きします。以下の zSecure Alert 提供トラップを開始点とみなします。

```
smfDataLost TRAP-TYPE
    ENTERPRISE Alert
    VARIABLES {
                eventIntegral,
                eventWhen,
```

```
                whatWTO-MESSAGE,
                whereSYSTEM
              }
   DESCRIPTION
         "System messages report that SMF data is lost (5)"
   ::= 1601
```

トラップ定義のイタリック体の部分は、以下の定義の取得のために変更できます。

```
mirrorGroupConnected TRAP-TYPE
    ENTERPRISE Alert
    VARIABLES {
                eventIntegral,
                eventWhen,
                user-whatMirrorGroup
              }
    DESCRIPTION
          "Connect to mirror group defined"
    ::= 4001
```

上記の例では、zSecure Alert 提供の 2 つの変数は保存され、他の変数はユーザー定義変数 `user-whatMirrorGroup` で置き換えられています。個々のユーザー定義変数は、OBJECT-TYPE として定義されている必要があります。 169 ページの『変数』を参照してください。

トラップ名とトラップ番号は、zSecure Alert 定義かつユーザー拡張の MIB 全体で固有でなければなりません。新規トラップは、MIB 内のどの TRAP-TYPE キーワードの前でもまだ使用されていない名前を取得する必要があります。この新規トラップは、MIB 内のどの TRAP-TYPE ... ::= の後でもまだ使用されていない名前を取得する必要があります。

番号は、ユーザー定義トラップ用に予約された範囲である 4000 から 6999 までででなければなりません。この範囲外のトラップ番号は、IBM 用に予約されています。(これらの予約は、1.3.6.1.4.1.9399.1.2 とコード化されるエンタープライズ・ツリー iso.org.dod.internet.private.enterprises.consul.software.zAlert に属します。) トラップ番号は ISPF zSecure Alert インターフェースでのアラート番号と同じでなければなりません。4000 から 4999 までの範囲は RACF アラート用です。5000 から 5999 までの範囲は ACF2 アラート用です。 6000 から 6999 までの範囲は ACF2 アラート用です。

新規トラップは、::= *n* で終了する一部のトラップの後にその定義を挿入することにより、MIB に追加できます。ここで *n* は MIB に既に出現しているトラップ番号です。

トラップ定義をソートして、その番号が小さい順に出現するようにします。ソートによって予約済みのトラップ番号を簡単に確認することができます。順序のソートは必須ではありません。

トラップについて詳しくは、`www.faqs.org/rfcs` にある RFC 1215 を参照してください。

MIB ファイルのマージ

いくつかのトラップと変数を MIB に追加して、IBM から交換用またはアップグレード用の MIB を入手した場合は、 4000 から 6999 の範囲にあるお客様が定義したトラップと、400000 から 699999 の範囲にある変数を、古い MIB から新しい

MIB にコピーする必要があります。これにより、古い MIB ファイルをアンロードし、新しい MIB ファイルをロードする際に、お客様が定義したトラップと変数が確実に引き続き認識されます。

Tivoli Enterprise Console クラスを使用したユーザー定義の BAROC ファイル

このセクションではユーザー定義の BAROC ファイルの作成について説明します。

ユーザー定義の BAROC ファイルは、Tivoli Enterprise Console の構成に記述されているように、Tivoli Enterprise Console によってインポートできます。

zSecure Alert BAROC ファイル (zSecure-Alert.baroc) はクラスおよび変数を使用して拡張できますが、そうではなく別個の BAROC ファイルを作成する必要があります。ファイル user-Alert.baroc をここで呼び出すこともできますが、別の固有名を指定する必要があります。ユーザーは zSecure Alert 提供の BAROC ファイルとユーザー定義の BAROC ファイルを別個のエンティティーとして保持する必要があります。

以下のサンプルの user-Alert.baroc ファイルの定義を開始点としてみなす必要があります。ここで、v_1、v_2、...、v_m はすべてのユーザー定義変数のリストです。それぞれの # 文字は、その行の最後にまで及ぶコメントを開始します。USER_DEFINED_ALERT が出現している場所は、MY_COMPANY_ALERT などのより適切なフレーズに置き換えることができます。ユーザー定義の user-Alert.baroc ファイルは、複数の zSecure Alert BAROC クラスを提供する zSecure-Alert.baroc ファイルに依存することに注意することが重要です。

```
TEC CLASS: USER_DEFINED_ALERT ISA ZSECURE_ALERT
     DEFINES {
                v1: STRING; # e.g. user-whatATTEMPTS: STRING;
                v2: STRING; # e.g. user-whatMirrorGroup: STRING;
                ...
                vm: STRING; # e.g. user-whoManager: STRING;
     };
END

TEC CLASS: USER_DEFINED_ALERT_HARMLESS ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = HARMLESS;
     };
END

TEC CLASS: USER_DEFINED_ALERT_UNKNOWN ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = UNKNOWN;
     };
END

TEC CLASS: USER_DEFINED_ALERT_WARNING ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = WARNING;
     };
END

TEC CLASS: USER_DEFINED_ALERT_MINOR ISA USER_DEFINED_ALERT
     DEFINES {
                severity: default = MINOR; };
END
```

```
TEC CLASS: USER_DEFINED_ALERT_CRITICAL ISA USER_DEFINED_ALERT
     DEFINES {
               severity: default = CRITICAL;
     };
END

TEC CLASS: USER_DEFINED_ALERT_FATAL ISA USER_DEFINED_ALERT
     DEFINES {
               severity: default = FATAL;
     };
END
```

AIX 用の addtrap コマンド

このセクションではユーザー定義の addtrap コマンドによるシェル・スクリプトの作成について説明します。

このシェル・スクリプトは、 167 ページの『AIX および Windows 用の NetView の構成』で説明されているように、NetView を実行している AIX コンピューターで実行することを意図したものです。 Windows コンピューター用のユーザー定義の addtrap コマンドを含むスクリプトの作成については、 176 ページの『Windows 用の addtrap コマンド』で説明します。

個々の addtrap コマンドは、zSecure Alert 提供かつユーザー拡張の MIB に存在する単一のユーザー定義トラップに対応します。これについては、 169 ページの『ユーザー定義アラートの MIB への追加』で説明しています。addtrap コマンドのリストは、zSecure Alert 提供スクリプトとは別のスクリプトに置かれる必要があります。そのため、addtrap コマンドのリストは、IBM によって新規のバージョンのスクリプトが提供される際に誤って失われることはありません。作成されるスクリプトは本文中で user-addtraps.sh と呼ばれますが、別の固有の名前を指定する必要があります。

MIB 内のトラップ番号 (::= 演算子の直後に出現します) は、n_1、n_2、...、および n_m であると想定します。これらの番号はそれぞれ、ユーザー定義トラップ用に予約された 4000 から 6999 までの範囲に含まれている必要があります。 1601 のような範囲外のトラップ番号は、IBM 用に予約されています。

MIB 内の TRAP-TYPE キーワードの直前に出現する対応するユーザー定義トラップ名は、$name_1$、$name_2$、...、および $name_m$ であると想定します。

最初に、重大度 s_i を個々のユーザー定義トラップ i に割り当てます。重大度は以下のコードのいずれかになります。

0 無害/クリア

1 不確定または不明

2 警告

3 マイナー

4 クリティカル

5 メジャーまたは致命的

次に、トラップの簡単な説明 d_i を作成します。トラップの MIB 記述を使用してもかまいません。最終的には、$v_{i,1}$、$v_{i,2}$、...、$v_{i,j}$ のように、MIB に出現する順序でトラップの変数名のリストを作成します。

次に、それぞれの名前 $name_i$、対応するトラップ番号 n_i、重大度 s_i、クラス名 c_i、説明 d_i、および変数 $v_{i,1}$、$v_{i,2}$、...、$v_{i,j}$ について、以下の行を user-addtraps.sh に追加します。

```
addtrap -l name_i -s n_i -S s_i -g 6 -n Alert ¥
        -i 1.3.6.1.4.1.9399.1.2 -o A ¥
        -c "Status Events" -e c_i ¥
        -D d_i ¥
        -E 'v_i,1' -V '$V1' ¥
        -E 'v_i,2' -V '$V2' ¥
        ...
        -E 'v_i,j' -V '$Vj' ¥
        -t 0 -f - -F '$S $1'
```

171 ページの『トラップ』に示されるサンプルのユーザー定義 mirrorGroupConnected トラップから派生した addtrap コマンドの例を示します。トラップの重大度は 3 (-S 3) です。

```
addtrap -l mirrorGroupConnected -s 4001 -S 3 -g 6 -n Alert ¥
        -i 1.3.6.1.4.1.9399.1.2 -o A ¥
        -c "Status Events" -e USER_DEFINED_ALERT_MINOR ¥
        -D "Connect to mirror group defined" ¥
        -E 'eventIntegral' -V '$V1' ¥
        -E 'eventWhen' -V '$V2' ¥
        -E 'user-whatMirrorGroup' -V '$V3' ¥
        -t 0 -f - -F '$S $1'
```

他のサンプルの addtrap コマンドについては、zSecure-Alert-addtraps.sh スクリプトを参照してください。

注:

1. addtrap コマンドとそのオプションには大文字と小文字の区別があります。
2. コマンドの個々のバックスラッシュは、コマンドが次の行へ続くことを示します。
3. zSecure Alert 提供 MIB 内の変数名とは異なり、このスクリプトの変数名はそれぞれアンダースコアー (_) で始まります。アンダースコアーにより、変数がトラップ表示にグループ化されます。 user-addtraps.sh 内の変数名の前にもアンダースコアーを配置できます。

user-addtraps.sh スクリプトを既に用意していて、多数の新規トラップを MIB ファイルに追加済みである場合は、新規のユーザー定義トラップに対応する行を追加することにより、user-addtraps.sh を拡張する必要があります。これと同様に、MIB からトラップを削除した後に、user-addtraps.sh から対応する addtrap 行を削除する必要もあります。最終的に、重大度などのトラップの一部のアスペクトを変更する際には、対応する addtrap 行を変更できます。

user-addtraps.sh を作成または変更したら、このスクリプトを実行して、NetView に新規トラップまたは変更したトラップを通知する必要があります。

Windows 用の addtrap コマンド

このセクションでは、MIB 内のユーザー定義トラップに対応する addtrap コマンドを使用したファイルの作成と使用について説明しています。このファイルは、NetView を実行している Windows コンピューターで実行されることを意図しています。 167 ページの『AIX および Windows 用の NetView の構成』を参照してください。AIX コンピューター用のユーザー定義の addtrap コマンドを含むスクリプトの作成については、 174 ページの『AIX 用の addtrap コマンド』で説明します。

zSecure Alert 提供ファイル zSecure-Alert-addtraps.bat 以外のファイル user-addtraps.bat を addtrap コマンドで作成する必要があります。この方法では、ユーザー定義の addtrap コマンドは、IBM によって新規のバージョンの zSecure-Alert-addtraps.bat が提供される際に失われることはありません。作成されるファイルは本文中で user-addtraps.bat と呼ばれますが、より具体的な別の名前を指定してもかまいません。

zSecure Alert 提供かつユーザー拡張の MIB (例えば、zSecure-Alert-v210.mib) 内で、::= 演算子の直後に出現するユーザー定義トラップ番号は、n_1、n_2、...、および n_m であると想定します。これらの番号はそれぞれ、ユーザー定義トラップ用に予約された 4000 から 6999 までの範囲に含まれている必要があります。この範囲外のトラップ番号は、IBM 用に予約されています。

最初に重大度を個々のユーザー定義トラップに割り当てます。重大度は 0 (無害またはクリア)、1 (不確定または不明)、2 (警告)、3 (マイナー)、4 (クリティカル)、または 5 (メジャーまたは致命的) のいずれかになります。重大度 s_1、s_2、...、および s_m が、トラップ番号 n_1、n_2、...、および n_m に対応するトラップに割り当てられていると想定します。

MIB 内の (TRAP-TYPE キーワードの直前に出現する) 対応するユーザー定義トラップ名は、$name_1$、$name_2$、...、および $name_m$ であると想定します。

次に、それぞれの名前 $name_i$、対応するトラップ番号 n_i、および対応する重大度 s_i について、以下の行を user-addtraps.bat に追加します。

```
addtrap -l nameᵢ -s nᵢ -S sᵢ -g 6 -n Alert
    -i 1.3.6.1.4.1.9399.1.2 -o A
        -c "Status Events" -t 0 -f - -F "$S $1¥n$# args: $*"
```

171 ページの『トラップ』に示されるサンプルのユーザー定義 mirrorGroupConnected トラップから派生した addtrap コマンドの例を示します。トラップの重大度は 3 (マイナー) です。

```
addtrap -l mirrorGroupConnected -s 4001 -S 3 -g 6 -n Alert
    -i 1.3.6.1.4.1.9399.1.2 -o A
        -c "Status Events" -t 0 -f - -F "$S $1¥n$# args: $*"
```

他のサンプルの addtrap コマンドについては、zSecure-Alert-addtraps.bat スクリプトを参照してください。 addtrap コマンドとそのオプションには大文字と小文字の区別があります。

MIB のロード後に、user-addtraps.bat を実行して、ユーザー定義トラップの特定のアスペクト (重大度など) を NetView に通知する必要があります。

user-addtraps.bat と呼ばれるファイルとユーザー定義の多数の新規トラップが既にある場合、新規のユーザー定義トラップに対応する行で user-addtraps.bat ファイルを拡張できます。 MIB からユーザー定義トラップを削除した場合は、user-addtraps.bat ファイルから対応する addtrap 行も削除する必要があります。最終的に、ユーザー定義トラップの一部のアスペクトを変更する際には、対応する addtrap 行を変更できます。

user-addtraps.bat を変更したら、このファイルを再実行して、新規または変更したユーザー定義トラップのアスペクトを NetView に通知する必要があります。

注: NetView でユーザー定義トラップのアスペクトを変更した場合、user-addtraps.bat ファイルを再実行して、これらのアスペクトを user-addtraps.bat ファイル提供の値に戻すことができます。特定のトラップのアスペクト (名前が $name_i$ のアスペクトなど) を変更したくない場合は、user-addtraps.bat ファイルを再実行する前に、このファイルから addtrap -l $name_i$ ... 行を削除する必要があります。

付録 C. QRadar SIEM の SYSLOG フォーマット

IBM Security QRadar SIEM に送信されるユーザー定義の syslog アラート (第 2 章、『zSecure Alert 構成』->『インストール定義アラート』を参照) に **whoUSERID** タグが含まれる必要があります。 QRadar では、ユーザー名フィールドを設定するためにこのタグを選択します。

QRadar SIEM が、whoUSERID 以外のタグで検索、表示、および報告できるようにするために、QRadar SIEM カスタム・イベントおよびフロー・プロパティーを作成することができます。このトピックの説明は、「*IBM Security QRadar SIEM* ユーザーズ・ガイド」の『カスタム・イベント・プロパティーとカスタム・フロー・プロパティー』の章と、QRadar SIEM に組み込まれた製品ヘルプ・システムにあります。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は AXELOS Limited の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は AXELOS Limited の登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc. の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

［カ行］

［サ行］

［タ行］

［ハ行］

［マ行］

［ヤ行］

［ラ行］

［数字］

A

B

C

D

E

F

G

I

L

M

N

O

P

Q

R

S

U

V

W

Z

Printed in Japan

SA88-7156-04

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21