

Security zSecure Alert
バージョン 2.1.0

**ユーザー・リファレンス・
マニュアル**

IBM

Security zSecure Alert
バージョン 2.1.0

**ユーザー・リファレンス・
マニュアル**

IBM

お願い

本書および本書で紹介する製品をご使用になる前に、143 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。

本書は、IBM Security zSecure Alert (製品番号 5655-N21) のバージョン 2、リリース 1、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： SC27-5642-00
Security zSecure Alert
Version 2.1.0
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

第1刷 2013.11

© Copyright IBM Corporation 2002, 2013.

目次

本書について	vii
本書の対象読者	vii
本書の内容	vii
資料および用語集へのアクセス	viii
関連資料	xi
アクセシビリティ	xii
技術研修	xii
サポート情報	xii
適切なセキュリティの実践に関する注意事項	xii
第 1 章 概要	1
第 2 章 zSecure Alert 構成	5
概要	5
アラート活動化に関するガイドライン	7
構成のガイドラインとパフォーマンスへの影響	8
インターバル	8
バッファ	9
zSecure Alert の構成	12
アラート構成: アラート構成の管理 (SE.A.A)	13
アラート構成: 一般設定の指定	16
アラート構成: アラート宛先の指定	20
アラート構成: アラート・カテゴリーの選択	24
アラート構成: アラート構成の検査	27
アラート構成: アラート構成のリフレッシュ	29
E メール・アドレス・リスト (SE.A.E)	30
インストール定義アラート	33
アラート ID とデータ・ソースの指定	34
既存のアラートの CARLa スケルトン	38
環境依存の選択	40
アラート条件	41
E メール・レイアウト	42
テキスト・メッセージ・レイアウト	43
SNMP レイアウト	43
UNIX syslog レイアウト	43
コマンド・セクション	44
第 3 章 事前定義アラート	45
標準 E メール・レイアウト	49
事前定義 RACF アラート	50
ユーザー・アラート	50
不明ユーザーによるログオン (1101)	50
緊急時ユーザー ID を使用したログオン (1102)	50
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)	51
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)	52
システム権限の認可 (1105)	52
システム権限の除去 (1106)	53
グループ権限の認可 (1107)	53

グループ権限の除去 (1108)	54
非 SPECIAL ユーザーによる SPECIAL 権限の使用 (1109)	55
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)	56
無効なパスワード試行の制限の超過 (1111)	57
パスワード・ヒストリーのフラッシュ (1112)	57
疑わしいパスワード変更 (1113)	58
CREATE 以上の接続権限の設定 (1114)	59
違反が多すぎる (1115)	60
データ・セット・アラート	61
データ・セットでの WARNING モード・アクセス (1201)	61
DATASET プロファイルでの UACC>=UPDATE (1202)	62
DATASET プロファイルでの UACC>NONE (1203)	62
APF データ・セットでの更新 (1204)	63
SETPROG を使用した APF リストへのデータ・セットの追加 (1205)	64
SETPROG を使用した APF リストからのデータ・セットの除去 (1206)	64
APF リストへのデータ・セットの追加の検出 (1207)	65
APF リストからのデータ・セットの除去の検出 (1208)	65
General resource alerts	66
STC 用の包括的プロファイルの使用 (1301)	66
監査対象プログラムの実行 (1302)	67
一般リソースでの WARNING モード・アクセス (1303)	67
UNIX アラート	68
UNIX ファイル・アクセス違反 (1401)	68
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)	69
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)	70
拡張属性の変更 (1404)	70
監査対象 UNIX プログラムの実行 (1405)	71
スーパーユーザー特権のある UNIX プログラムの実行 (1406)	72
ユーザーによるスーパーユーザー特権のあるシエルの取得 (1407)	73
UNIX プログラムでのスーパーユーザー特権の設定 (1408)	73
拡張属性の変更 (1409)	74
RACF 制御アラート	75
グローバル・セキュリティ対策の活動化 (1501)	75

グローバル・セキュリティ対策の非活動化 (1502)	75	データ・セットでの WARNING モード・アクセス (2201)	93
グローバル・セキュリティ対策またはオプションの変更 (1503)	76	APF データ・セットでの更新 (2204)	94
RACF リソース・クラスの活動化 (1504)	76	APF リストへのデータ・セットの追加 (2205)	94
RACF リソース・クラスの非活動化 (1505)	77	APF リストからのデータ・セットの除去 (2206)	95
システム・アラート	77	APF リストへのデータ・セットの追加の検出 (2207)	95
SMF データ損失の開始 (1601)	77	APF リストからのデータ・セットの除去の検出 (2208)	96
障害の後の SMF ロギングの再開 (1602)	78	General resource alerts	97
SVC 定義の変更 (1603)	78	STC 用のデフォルト STC ログオン ID の使用 (2301)	97
IBM Health Checker による重大度が低レベルの問題の検出 (1604)	79	UNIX アラート	97
IBM Health Checker による重大度が中レベルの問題の検出 (1605)	79	ユーザーによるスーパーユーザー特権のあるシエルの取得 (2407)	98
IBM Health Checker による重大度が高レベルの問題の検出 (1606)	80	拡張属性の変更 (2409)	98
SMF レコードのフラッドの検出 (1607)	80	ACF2 制御アラート	99
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)	81	グローバル・セキュリティ対策の追加 (2501)	99
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)	81	グローバル・セキュリティ対策の削除 (2502)	99
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)	82	グローバル・セキュリティ対策の変更 (2503)	100
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)	82	システム・アラート	100
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)	83	SMF データ損失の開始 (2601)	100
1024 未満のポートが予約されなくなった (1613)	84	障害の後の SMF ロギングの再開 (2602)	101
インターフェースのセキュリティ・クラスの変更 (1614)	84	SVC 定義の変更 (2603)	101
IP フィルター規則の変更 (1615)	85	IBM Health Checker による重大度が低レベルの問題の検出 (2604)	102
グループ・アラート	85	IBM Health Checker による重大度が中レベルの問題の検出 (2605)	102
重要なグループへの接続 (1701)	85	IBM Health Checker による重大度が高レベルの問題の検出 (2606)	103
事前定義 ACF2 アラート	86	SMF レコードのフラッドの検出 (2607)	103
ユーザー・アラート	86	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)	104
緊急時ログオン ID を使用したログオン (2102)	86	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)	105
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)	87	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)	105
システム権限の認可 (2105)	87	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)	106
システム権限の除去 (2106)	88	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)	106
無効なパスワード試行の制限の超過 (2111)	88	1024 未満のポートが予約されなくなった (2613)	107
パスワード・ヒストリーのフラッシュ (2112)	89	インターフェースのセキュリティ・クラスの変更 (2614)	107
疑わしいパスワード変更 (2113)	90	IP フィルター規則の変更 (2615)	108
違反が多すぎる (2115)	91	事前定義アラートの構成	109
非 SECURITY ログオン ID による SECURITY 権限の使用 (2116)	91	アラート定義 - 「Specify action」	109
非 NON-CNCL ログオン ID による NON-CNCL 権限の使用 (2117)	92	緊急時ユーザー構成 (アラート 1102 および 2102)	110
非 READALL ログオン ID による READALL 権限の使用 (2118)	92	過度の違反に対する取り消し (1115) の構成	110
データ・セット・アラート	93	重要なグループ (1701) の構成	112

違反数および除外するログオン ID (2115) の構成	112	AIX および Windows 上での NetView の構成	129
第 4 章 定期的な概要	115	ユーザー定義アラートの MIB への追加	130
第 5 章 問題判別ガイド	117	変数	131
問題診断に関する情報	117	トラップ	132
zSecure Audit の問題診断	117	MIB ファイルのマージ	134
zSecure Alert の問題診断	118	Tivoli Enterprise Console クラスを使用したユーザー定義の BAROC ファイル	134
一般的な問題および異常終了	118	AIX 用の addtrap コマンド	136
ライセンス問題	119	Windows 用の addtrap コマンド	138
予期したアラートが発生しない	119	付録 C. QRadar SIEM の SYSLOG フォーマット	141
付録 A. SNMP 出力	123	特記事項	143
付録 B. Tivoli Enterprise Console および NetView の構成	127	商標	145
Tivoli Enterprise Console の構成	127	索引	147

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。

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。

本書の対象読者

本書は以下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 RACF 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 の概念とコマンドを理解しておく必要があります。

本書の内容

本書には以下の情報が含まれています。

- 1 ページの『第 1 章 概要』では、IBM Security zSecure Alert の概要と機能、使用した場合の利点について説明します。
- 5 ページの『第 2 章 zSecure Alert 構成』では、さまざまなアラート・メッセージ・フォーマットについて説明します。これらのフォーマットには、E メール、ポケットベルまたは携帯電話のテキスト・メッセージ、自動化操作の WTO、ネットワーク・コンソールの SNMP トラップ、および UNIX syslog などがあります。この章では、対象の事前定義アラートを構成および選択する方法、また独自の追加を行う方法についても説明します。
- 45 ページの『第 3 章 事前定義アラート』では、事前定義アラートについて説明します。
- 115 ページの『第 4 章 定期的な概要』では、定期的な概要を送信するために実行が必要な内容について説明します。
- 117 ページの『第 5 章 問題判別ガイド』では、IBM Security zSecure Alert の問題を診断して修正する方法について説明します。
- 123 ページの『付録 A. SNMP 出力』では、SNMP 出力のフォーマットについて説明します。
- 127 ページの『付録 B. Tivoli Enterprise Console および NetView の構成』では、IBM Security zSecure Alert トラップとユーザー定義の IBM Security zSecure Alert トラップを正しく表示するために IBM Tivoli Enterprise Console[®] を構成する方法と、IBM Security zSecure Alert 用に AIX[®] 上に IBM NetView[®] を構成する方法について説明します。

資料および用語集へのアクセス

このセクションでは、以下について述べます。

- 『IBM Security zSecure ライブラリー』 の資料のリスト。
- xi ページの『オンライン資料』 へのリンク。
- xi ページの『IBM Terminology Web サイト』 へのリンク。

IBM Security zSecure ライブラリー

以下の資料が IBM Security zSecure ライブラリーでオンラインで入手可能です。

- *IBM Security zSecure* 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、IBM Security zSecure 製品の新機能と機能拡張、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、http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.htm から入手できます。

- *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/ACF2
- IBM Security zSecure Visual for RACF
- IBM Tivoli® Compliance Insight Manager Enabler for z/OS
- *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 パネルから機能を実行する方法、RACF の管理と監査のユーザー資料を、CARLa コマンド言語と SELECT/LIST フィールド用の、一般ユーザーと上級ユーザーの両方の参照資料とともに記載しています。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 Audit for ACF2 Getting Started*, GI13-2325

IBM Security zSecure Audit for ACF2 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・セキュリティおよびモニタリングのために IBM Security zSecure Audit for ACF2 を使用する方法について説明しています。新規ユーザーの場合、このガイドには、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。上級ユーザーの場合、このマニュアルには、メッセージと戻りコードのリスト、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を含む、詳細な参照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*

IBM Security zSecure Audit for Top Secret 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。

- *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・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・セキュリティを保護するために IBM Security zSecure Command Verifier をインストールし、使用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 クイック・リファレンス, SA88-7163*

このブックレットは、IBM Security zSecure Suite コンポーネント (Admin、Audit、Alert、Collect、および Command Verifier) のコマンドとパラメーターを要約しています。廃止されたコマンドは省略されます。

- *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。この「*IBM Security zSecure: Documentation CD*」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。

- *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 Tivoli Compliance Insight Manager Enabler for z/OS) 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・ディレクトリーはプロダクト・テープで提供されます。また、IBM Security zSecure 資料 Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) 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 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・ディレクトリーはプロダクト・テープで提供されます。また、IBM Security zSecure 資料 Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) 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 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・ディレクトリーはプロダクト・テープで提供されます。また、IBM Security zSecure 資料 Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) 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 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。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。また、IBM Security zSecure 資料 Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) から最新のコピーをダウンロードすることもできます。

オンライン資料

IBM では、製品のリリース時および資料の更新時に、以下の場所に製品資料を掲載しています。

IBM Security zSecure ライブラリー

製品資料サイト(http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) には、ライブラリーのウェルカム・ページおよびナビゲーションが表示されます。

IBM Security Systems Documentation Central

『IBM Security Systems Documentation Central』には、すべての IBM Security Systems 製品ライブラリーのアルファベット順のリストと、各製品の特定バージョンのオンライン資料へのリンクが掲載されています。

IBM Publications Center

The IBM Publications Center サイト (<http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss>) には、必要なすべての IBM 資料を見つけるのに役立つカスタマイズ検索機能が用意されています。

IBM Terminology Web サイト

IBM Terminology Web サイトは、製品ライブラリーの用語を 1 つのロケーションに統合したものです。Terminology Web サイトには、<http://www.ibm.com/software/globalization/terminology> からアクセスできます。

関連資料

RACF、および IBM Security zSecure Alert を介して報告されるイベントのタイプに関する詳細情報は、複数の IBM マニュアルで見つけることができます。非互換性について詳しくは、IBM Security zSecure の資料 Web サイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/welcome.html) にある『リリース情報』に含まれる非互換性に関するセクション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、「RACF 監査担当者のガイド」に記載されています。

表 1. RACF 管理、監査、プログラミング、およびコマンドについての詳細情報

マニュアル	資料番号
z/OS V1 Security Server RACF コマンド言語解説書	SA88-8617
z/OS V1 Security Server RACF セキュリティー管理者のガイド	SA88-8613
z/OS V1 Security Server RACF 監査担当者のガイド	SA88-8614
z/OS V1 Security Server RACF システム・プログラマーのガイド	SA88-8611
z/OS MVS™ システム・コマンド	SA88-8593

アクセシビリティ

アクセシビリティ機能は、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进行操作することもできます。

技術研修

以下は英語のみの対応となります。技術研修の情報については、以下の IBM Education Web サイト (<http://www.ibm.com/software/tivoli/education>) 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・サポートのサイトには、<http://www.ibm.com/software/support/probsub.html> で直接アクセスできます。

適切なセキュリティの実践に関する注意事項

IT システムのセキュリティでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。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、システム、製品、またはサービスが、悪意のある行為または不正な行為から影響を受けないこと、またはこれらの行為がお客様の企業に影響を与えないことを保証しません。

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 上に構築されます。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 Security Operations Manager 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

- UNIX syslog へ送信する

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。

RACF システムでは、zSecure Alert は追加の RACF 出口 (ICHPWX01) を動的にインストールして活動化し、ユーザー・パスワードの変更に関する SMF レコードを作成することができます。それらの SMF レコードは、RACF PASSWORD コマンドで作成されるレコードによく似ていますが、SMFUID フィールドの特殊な値によって認識することができます。これらの出口の活動化は、zSecure 構成の C2XEXITS パラメーターを使用して制御できます。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*」の構成情報に関する説明を参照してください。

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、45 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、「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」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。

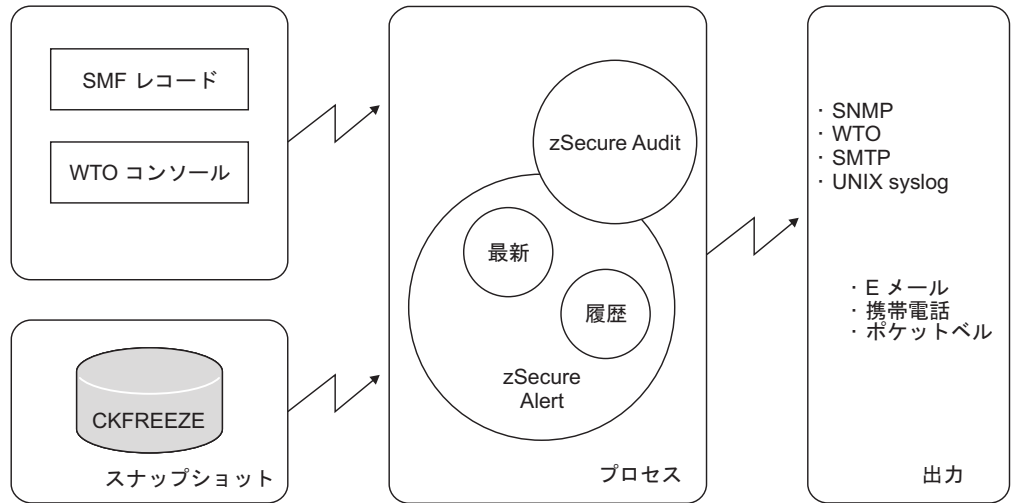


図1. zSecure Alert アーキテクチャー

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。

アラート構成データ・セット

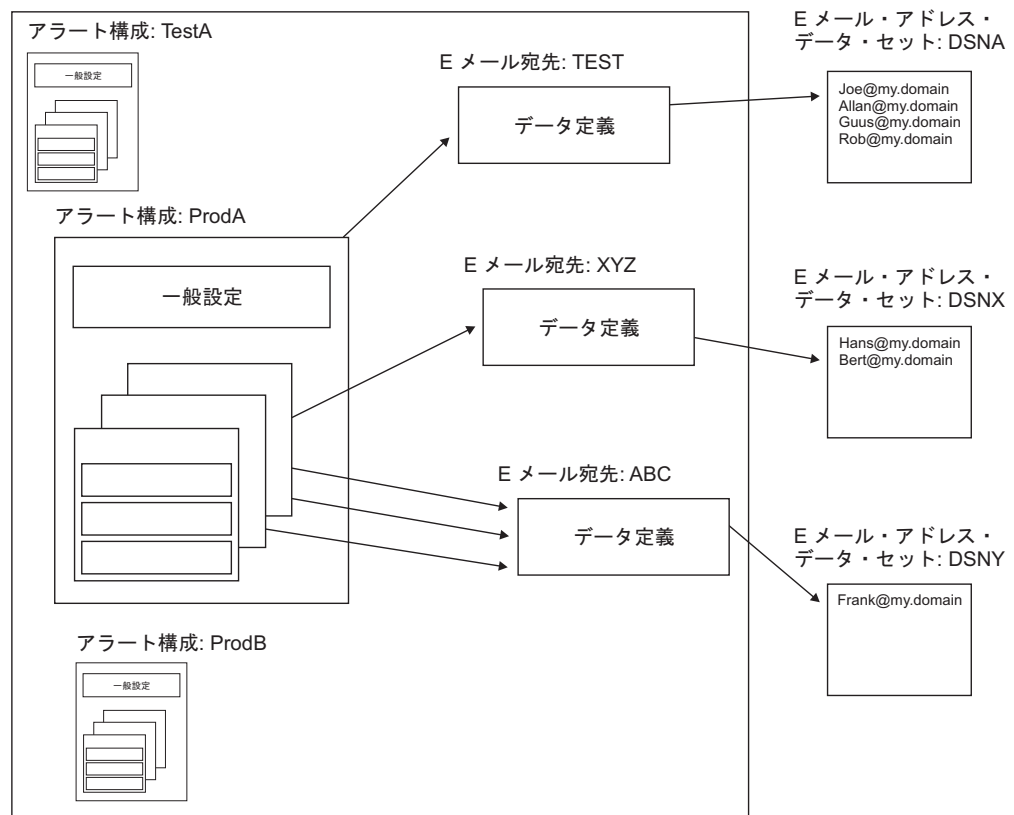


図2. アラート構成データ・セット

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
- UNIX syslog

アラート・フォーマットは、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、49 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。UNIX syslog レイアウトについては、43 ページの『UNIX syslog レイアウト』を参照してください。SNMP トラップ・フォーマットについては、123 ページの『付録 A. SNMP 出力』に説明があります。提供される IBM アラートについて詳しくは、45 ページの『第 3 章 事前定義アラート』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。

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。33 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。45 ページの表 5 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、単に何かの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、13 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。9 ページの『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せん。

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、アカウント 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が。
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れます。

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・サイズが分かったら、次は必要なバッファの数を知る必要があります。前述のように、最小バッファ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。

$$\text{Numbufs} > (\text{AverageInterval} / \text{Interval}) + 1$$

開始点として、この公式に基づくバッファ数の 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 $2 * ((300/60)+1) = 12$ バッファになります。

この手順で割り振られた追加のバッファは、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・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・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・サイズを指定しました。したがって、バッファの約 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一数値を使用すると、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・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「02」は、後続のバッファ (「03」) にオーバーフローしていたバッファです。バッファ「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・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・サイズとバッファ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から開始し、バッファの

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・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・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
```

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。

手順

zSecure Alert を構成するには、以下のステップを実行します。

- オプションとして、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。これは、オプション SE.A.E を使って実現できます。注 1 を参照してください。
- 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。このステップと以下の各ステップは、オプション SE.A.A を使って実現できます。注 2 を参照してください。
- 一般設定を編集します。
- アラート構成レベルでアラート宛先を指定します。
- 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。
- アラート構成を検査します。注 3 を参照してください。
- 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 (12 ページ) 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 (12 ページ) 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。
- ステップ 2 (12 ページ) 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。
- ステップ 6 (12 ページ) と 7 (12 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ある場合は、「*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を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は、27 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/携帯電話の受信先、SNMP アドレス、WTO メッセージ、UNIX syslog 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。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 2. 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。
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、UNIX syslog 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。

表 2. アラート構成管理の行コマンド (続き)

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。
B	このアラート構成の一般設定をブラウズします。

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 Admin+Audit for RACF - 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

Interval . . . . . 60                (in seconds)
Environment refresh . . 60            (in minutes)
Average . . . . . 300                (in seconds)
Buffer size . . . . . 1024           (in kilobytes)
Number of buffers . . . 10

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

Extended Monitoring . . . y            (Y/N)
Snapshot retention . . . 12           (Number of hours, 1-99)

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、このフィールドを空白のままにしてもかまいません。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、システム・プログラマーに正しい設定を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。

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。

「**インターバル**」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、WTO および SMF レコードを保管するために使用するメモリー内バッファ 1 個のサイズを、キロバイト単位で指定します。この数値は、1 から 16384 まででなければなりません。デフォルトは 1024、つまり 1 MB です。あるインターバル中、1 つのバッファでは小さすぎるのが分かった場合、zSecure Alert は未使用のバッファに切り替えようとします。空きバッファがない場合は、最も古い情報が入っているバッファに現行情報がオーバーレイされます。バッファ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 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**」フィールドの説明を参照してください。

Number of buffers

割り振るバッファの数を指定します。この数値は 2 から 32 ま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を割り振っておく必要があります。余分なバッファは、バッファ・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。

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。33 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 ==>> _____

Select the alert destination
/  E-mail
  _  Write e-mails to C2RSMTMP 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
  _  Write text messages to C2RSMTMP 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
  _  Write SNMP traps to C2RSNMP DD

Specify SNMP receiver address(es) (multiple addresses in parentheses,
separated by a comma)
Address . . . . . _____

/  UNIX syslog
  _  Write messages to C2RSYSLG DD

Specify UNIX SYSLOG address(es) (multiple addresses in parentheses,
separated by a comma)
Address(es) . . . _____

/  WTO
  _  Write 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 を使用できません。

- E メール宛先を定義済みである場合は、それを `:destination-name.field-name` から参照できます。

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 C2RSMTTP 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、C2RSMTTP 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জァーのアドレス。「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、UNIX syslog セクションに表示されます。

UNIX syslog

アラートを UNIX syslog に送信します。

Write messages to C2RSYSLG DD

このフィールドと「UNIXsyslog」の両方を選択した場合、生成されたアラ-

ト・メッセージは UNIX syslog へ送信されず、C2RSYSLG DD に書き込まれます。このフィールドは、テスト用です。

Addresses

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。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(select)
-----
  Id  Category                #alerts  #selected
S  1  User alerts                15        0
-  7  Group alerts                1        0
-  2  Data set alerts            6        0
-  3  General resource alerts    3        0
-  4  UNIX alerts                8        8
-  5  RACF control alerts       3        0
-  6  System alerts              2        0
-  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
- 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。その場合、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 Audit for RACF - Setup - Al Row 1 to 13 of 15
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  gECSWU  CA  EM
- Logon by unknown user                   1101 No  g    U    _  N
- Logon with emergency userid              1102 No  g    U    Y  N
- Logon of a userid with UID(0) (Unix superuser) 1103 No  g    U    _  N
- Highly authorized user revoked for pwd violatio 1104 No  g    U    _  N
- System authority granted                 1105 No  g    U    _  N
- System authority removed                 1106 No  g    U    _  N
- Group authority granted                  1107 No  g    U    _  N
- Group authority removed                  1108 No  g    U    _  N
- SPECIAL authority used by non-SPECIAL user 1109 No  g    U    _  N
- non-OPERATIONS user accessed data set with OPER 1110 No  g    U    _  N
- Invalid password attempts exceed limit     1111 No  g    U    _  N
- Password history flushed                 1112 No  g    U    _  N
- Suspect password changes                 1113 No  g    U    _  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 Suite - Setup - Alert                               Row 1 to 11 of 11
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  gECSWU  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
***** 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。

gECSWU

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:** UNIX syslog

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。109 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 3. 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。
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、および CARLa コードなどのアラート特性を指定します。
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。
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、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。
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。
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。また、アクション・コマンドを指定することもできます。 109 ページの『アラート定義 - 「Specify action」』を参照してください。

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、33 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

28 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 Admin+Audit for RACF - 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

オプション「Use SETUP FILES input instead of zSecure Alert input data」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。アラート・アドレス・スペースは、常にセキュリティー・データベースと CKFREEZE データ・セットを構成されたとおりに使用します。

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ため、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。

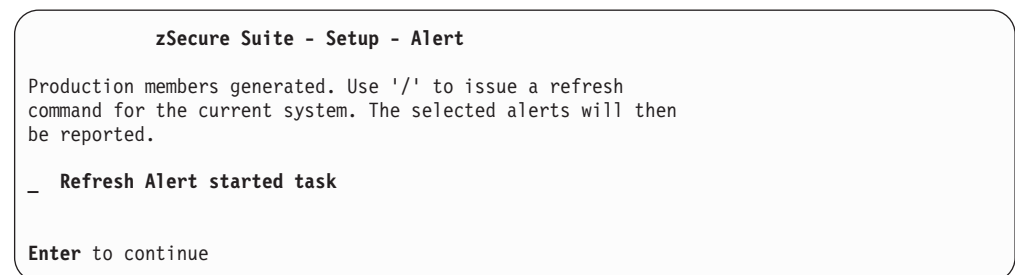


図 11. 「Setup Alert」パネル: アラート構成のリフレッシュ

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、それを取付できなくなります。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・アドレスのほかには他の情報が含まれている場合は、レコードのどの部分を使用したい 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。30 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。

```

Menu Options Info Commands Setup
-----
zSecure Suite - Setup - Alert      Row 1 from 6
Command ==> _____ Scroll ==> CSR
CKRM839 E-mail destination added
Select Alert e-mail destination
The following line commands are available: B(rowse), C(opy), D(elete),
E(dit set), I(nsert), S(elect), V(iew)
-----
Set name  Description
         Data set name
-  SECADM  Security administrator e-mail addresses
         'C2P.DATA.MAIL(SECADM)'
-----
***** ***** Bottom of data *****

```

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 4. 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、30 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。

表 4. 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 (続き)

行コマンド	説明
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。

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 Admin and Audit for RACF: User Reference Manual*」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'
```

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
- UNIX syslog

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、49 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、IBM Tivoli Compliance Insight Manager または Tivoli Security Information and Event Manager、またはネットワーク・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、123 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・パネルで、「**System alerts**」など、いずれかのカテゴリを選択します。

新しいアラートが属するカテゴリは、アラートの作成に使用したカテゴリではなく、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 1 of 1
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  gECSW  C  EM
I  SMF data loss started                   1601 Yes  gE W    N
-  SMF logging resumed after failure       1602 Yes  gE W    N
-  SVC definition changed                   1603 No   gE W    Y
***** Bottom of data *****

```

図 15. 「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。

```

Menu      Options      Info      Commands      Setup
-----
                                zSecure Admin+Audit for RACF - Setup - Alert
Command ==> _____

Description . . _____
Member prefix _____
Alert id. . . . _____ Severity. . . . _ (I, W, E or S)
Data source . . SMF _____
Parameters . . . _____
Panel name . . . _____ (Panel for additional customization)

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

Specify WTO filters for this alert
Prefix     Prefix     Prefix     Prefix     Prefix

Allowable destination types _____ E-mail _____ Cellphone _____ SNMP _____ WTO
_____ UNIX syslog _____ Action _____
Specify action . . . . . N (Y/N)
Extended Monitoring alert . . (Y/N)
View/edit the alert skeleton _____ ISPF Skeleton

```

図 16. 「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。

重大度 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。

- 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 UNIX 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

- 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)。

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。拡張モニター・アラートの場合は、このフィールドに、必須の COMPAREOPT=<compareopt-name> を入力する必要があります。

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。

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、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 ACF2 ACF2 サブタイプの完全なリストについては、「IBM Security zSecure Audit for ACF2: User Reference Manual」を参照してください。

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。

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。

Specify action

このアラートのアクションを指定するには、「Y」を選択します。109 ページの『アラート定義 - 「Specify action」』を参照してください。

Extended Monitoring alert

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。

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、この「ISPF Skeleton」では、選択基準、アラート内容、およびアラート・レイアウトだけが指定されます。ユーザーは、既に存在するデフォルトの CompareOpt ステートメントによく似た必須の CompareOpt ステートメントを、グローバル CARLa スケルトンの下部に追加する必要があります。必須の CompareOpt ステートメントの名前は、このリストで前に述べた「Parameters」フィールドに指定します。

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 Admin+Audit for RACF - Setup - Alert
Command ==> _____
Description . . . APF List changed using SETPROG command
Member prefix AHJ
Alert id . . . . 4000 Severity . . . . W (I, W, E or S)
Data source . . . WTO
Parameters . . . _____
Panel name . . . _____ (Panel for additional customization)

Specify SMF records to be collected for this alert
Type Sub     Type Sub     Type Sub     Type Sub     Type Sub
-----
Specify WTO filters for this alert
Prefix       Prefix       Prefix       Prefix       Prefix
CSV410I
Allowable destination types / E-mail Cellphone _ SNMP _ WTO
                        _ UNIX syslog
Extended Monitoring alert . . (Y/N)
View/edit the alert skeleton / ISPF Skeleton

```

図 17. 「Setup Alert」パネル: アラートの定義

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する **E** (編集) 行コマンドで表示されるパネルで、「ISPF skeleton」オプションにタグを付けてください。IBM Security zSecure 提供アラートに対してこのアクションを実行すると、代わりに ISPF VIEW セッションが実行されます。**B** (ブラウズ) 行コマンドでも同じパネルが表示されます。

C (コピー) または **I** (挿入) 行コマンドでアラートを追加した場合は、表示されるパネルで、このオプションにタグを付けることができます。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。「コピー」の場合は、コピーされたアラートのスケルトン・メンバーからコピーが行われます。コピーされたメンバーでローカル事前選択フィルターが定義されている場合は、名前の競合を避けるため

に、コピー内のそれらの名前を変更する必要があります。これらの名前は、アラート ID 内で終了するものと想定されます。「挿入」の場合は、「空」のスケルトン・メンバーが表示されます。

このセクションの残りの部分では、「空」のスケルトンメンバーに基づいて説明します。いずれの場合でも、CARLa コードを持つ 7 つのセクションが表示されます。最初の 2 つのセクションは、アラート条件を指定します。その次の 4 つのセクションは、さまざまな宛先タイプのアラート・メッセージ・フォーマットを指定します。最後のセクションは、アラート条件が立ち上げられたときに発行できるコマンドを指定します。

スケルトン内の各 CARLa セクションには、以下のような識別用のコメント行が付いています。

)CM Pass one query

ここでは、stage1 メンバーの 2 パスの CARLa 照会を指定できます。アラート条件が環境に依存する場合は、それを使用します。この照会の stage1 ステップでは、その出力がレポート作成ステップの接頭部として使用されます。この出力は、現在の環境の値が取り込まれる 1 パスの CARLa 照会です。これを使用すると、実際の環境に基づいて、事前選択を生成できます。この事前選択は、アラート条件で参照できます。事前選択は、環境のリフレッシュを実行するたびに調整されます。通常、それは 1 時間に 1 回です。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。

)CM Alert condition

アラートをトリガーしたいアラート条件を指定します。拡張モニター・アラートの場合、complex の選択のみが必要です。例えば、select complex=(base, current) です。どのレコードがアラートをトリガーするかを決めるフィールドは、グローバル CARLa スケルトンで定義された CompareOpt ステートメントの中で指定されます。

)CM Action command

ここでは、アクション・コマンドを指定できるよう、以下のステートメントの組み込みを指定できます。

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

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

)CM EMAIL sortlist

ここでは、E メール宛先に使用するレイアウト内のアラート・メッセージを指定できます。

)CM Cellphone sortlist

ここでは、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。

)CM SNMP sortlist

ここでは、SNMP 宛先に使用するレイアウト内のアラート・メッセージを指定できます。

)CM UNIX syslog sortlist

ここでは、SYSLOG 宛先に使用するレイアウト内のアラート・メッセージを指定できます。

)CM WTO sortlist

ここでは、コンソールに送るレイアウト内のアラート・メッセージを指定できます。

)CM Command

ここでは、条件が発生したときに発行するコマンドを追加できます。

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ます。stage1 セクションにも)IM ディレクティブがあります。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。

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、stage1 照会を示しており、現在どのデータ・セットが APF リストに含まれているか、つまり、NEWLIST TYPE=SENSDSN の DSN フィールドと APF フラグ・フィールドをシステムに問い合わせます。詳しくは、「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」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)," /,
    )ENDSEL
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。この事前選択は、RACF システムに対する event=access(allowed) intent=>update の SMF レコード用です。または、ACF2 システムに対する acf2_subtype=D ACF2_ACCESS=OUTPUT 用、およびそのシステムから取得された APF データ・セット用です。

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。

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、選択基準用に 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、UAPP1204 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) などです。

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。例えば、select complex=(base, current) です。ただし、特定のレコードだけが含まれるよう、システム設定およびセキュリティー設定の相違点の検索を制限するには、追加の選択基準が必要になる場合があります。例えば、アラート 1207 では NEWLIST TYPE=SENSDSN が使用されます。しかし、この選択は、比較操作を APF データ・セットだけに制限します。45 ページの表 5 の ID 1207 を参照してください。比較するフィールドを指定する CompareOpt ステートメントは、グローバル CARLa スケルトンで定義されます。

E メール・レイアウト

IBM Security zSecure 提供アラートには、49 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),
  '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' /,
  / ' 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,
//
)ENDSEL

```

注: 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。

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),
  'Alert &c2pemem;: Update by'(t) user(t) 'on APF data set'(t),
  dataset(t),
  'Alert &c2pemem;: Update by' user(0) 'on APF data set',
  dataset(0)
)ENDSEL

```

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。123 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',
  'Alert: Update on APF data set' dataset(0,hor) '- ',
  'APF data set successfully updated' /,
  '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

```

UNIX syslog レイアウト

「)CM 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。次の例は、アラート 1204 を示しています。

```

)CM UNIX syslog sortlist
)SEL &C2PERCTP = SYSL
)SEL &C2PESECP = RACF
sortlist,

```

```

recno(nd) '<&C2PEPRI0.>' | date(month,3) date(monthday,0) time(8),
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) | ""',
'whatDESC="" | desc(0,explode) | ""',
'whatJOBNAME="" | jobname(0) | ""',
'whereSYSTEM="" | system(0) | ""]',
'Alert: Update on APF data set' dataset(0,hor) '--',
'APF data set successfully updated'
)ENDSEL

```

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。次の例では、選択されたアラートの適用先であるユーザーは、RACF によって取り消されます。

```

)CM Command
)SEL &C2PERCTP = CMD
"alu" userid(0) "revoke"
)ENDSEL

```

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 5. 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	3
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
1201	データ・セットでの WARNING モード・アクセス	1	2
1202	DATASET プロファイルでの UACC>=UPDATE の設定	2	3
1203	DATASET プロファイルでの UACC>NONE の設定	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
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
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

表 5. 事前定義アラート (続き)

ID	説明	クラス	重大度
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
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
1505	RACF リソース・クラスの非活動化	2	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

表 5. 事前定義アラート (続き)

ID	説明	クラス	重大度
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
2112	パスワード・履歴のフラッシュ	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
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
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
2607	SMF レコードのフラッドの検出	1	4

表 5. 事前定義アラート (続き)

ID	説明	クラス	重大度
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

(*) 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、Tivoli Enterprise Console および 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 6. Tivoli Enterprise Console および NetView での重大度レベル

重大度	Tivoli Enterprise Console での意味	NetView での意味
0	無害	クリア
1	不明	不確定
2	警告	警告
3	マイナー	マイナー・エラー
4	クリティカル	クリティカル
5	致命的	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

- UNIX syslog

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、123 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わかります。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、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を示されます。

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を示されます。

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。110 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。

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##AR02 in C##C

Alert: Group authority granted to C##AR02 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##AR02 RICK OXSON
Connected to C##C
Result       Success
RACF command CONNECT C##AR02 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##AR02 in C##C

Alert 1107: Group authority SPECIAL granted to C##AR02 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。

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##AR02 in C##C

Alert: Group authority removed for C##AR02 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##AR02 RICK OXSON
Connected to  C##C
Result       Success
RACF command CONNECT C##AR02 AUTHORITY(USE) GROUP(C##C) NOADSP
             NOAUDITOR NOGRPACC NOOPERATIONS OWNER(C##C) RESUME
```

```
User          SPECIAL UACC(NONE)
Job name      C##BERT  ERWIN RETTICH
System ID     CRRAC#17
              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##AR02 in C##C

Alert 1108: Group authority OPERATIONS AUDITOR removed for C##AR02 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を示されます。

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 4 つあります。

```
#history(nd,<5), #total(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:

1. 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。

- アラート 1112 と 1113 は両方とも、IBM Security zSecure の新規パスワード出口を活動化するかどうかに左右されます。「*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*」を参照してください。デフォルトでは、この出口はインストールされ、活動化されます。新規パスワード出口が活動化された場合、JOB カードによって行われたパスワード変更またはログオン時に行われたパスワード変更により、SMF レコードは、PASSWORD コマンドに対して生成された SMF レコードとまったく同じになります。これらのパスワード変更は、アラート 1112 および 1113 で数えられています。IBM Security zSecure の新規パスワード出口を活動化しない場合、JOB カードによって行われたパスワード変更もログオン時に行われたパスワード変更も検出されません。

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 commands 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いが、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 4 つあります。

```
#history(nd,<5), #total(nd,>=5),
```

これらすべてを、希望する制限を使用するように調整してください。

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、57 ページの『パスワード・履歴のフラッシュ (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 commands 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 ESMSG LG
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

このアラートでは、サイトに合わせてカスタマイズを行えます。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。パネルでは、過度と見なされる違反の数と、修正アクションを生成するかどうかを指定できます。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。110 ページの『過度の違反に対する取り消し (1115) の構成』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。67 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う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 プロファイルでの UACC>=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に、アラートが生成されます。指定された UACC が READ に等しいときでもアラートを受信する場合は、次のアラートを使用できます。『DATASET プロファイルでの UACC>NONE (1203)』を参照してください。

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。

```
From: C2POLICE at DINO
Subject: Alert: UACC>=UPDATE set: C##QAP2.ONZI.**
```

```
Alert: UACC>=UPDATE set: C##QAP2.ONZI.**
High UACC specified when adding or altering a data set profile
```

```
Alert id      1202
Date and time 04Feb2003 01:12:18.45
Profile       C##QAP2.ONZI.**
UACC          UPDATE
Result        Success
RACF command  ALTDSO 'C##QAP2.ONZI.**' UACC(UPDATE)
User          C##QAP2 ALEXANDER POUVIER
Job name      C##QAP2
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 1202: UACC>=UPDATE set by C##QAP2 : C##QAP2.ONZI.**
```

```
Alert 1202: UACC>=UPDATE set: C##QAP2.ONZI.** UACC set to UPDATE by C##QAP2
```

レポートには、変更されたプロファイル、指定された UACC、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 プロファイルでの UACC>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に、アラートが生成されます。指定された UACC が READ より高いときのみアラートを受信する場合は、前のアラートを使用できます。『DATASET プロファイルでの UACC>=UPDATE (1202)』を参照してください。

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。

From: C2POLICE at DINO
Subject: Alert: UACC>NONE set: C##QAP2.ONZI.**

Alert: UACC>NONE set: C##QAP2.ONZI.**
High UACC specified when adding or altering a data set profile

Alert id	1203
Date and time	04Feb2003 01:12:18.45
Profile	C##QAP2.ONZI.**
UACC	UPDATE
Result	Success
RACF command	ALTDSO 'C##QAP2.ONZI.**' UACC(UPDATE)
User	C##QAP2 ALEXANDER POUVIER
Job name	C##QAP2
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 1203: UACC>NONE set by C##QAP2 : C##QAP2.ONZI.**

Alert 1203: UACC>NONE set: C##QAP2.ONZI.** UACC set to UPDATE by C##QAP2

レポートには、変更されたプロファイル、指定された UACC、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。

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 の VERIFY SENSITIVE コマンドによって作成できます。

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: 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
Data set SYSPROG.APF.LOAD
Volume <SMS MANAGED>
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
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 addition to 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
Data set SYSPROG.APF.LOAD
Volume <SMS MANAGED>
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
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。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。

General resource alerts

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、少なくとも AUDIT(SUCCESS(READ)) または GLOBALAUDIT(SUCCESS(READ)) をプロファイルに指定する必要があります。PROGRAM クラスで、これらのプロファイルについて報告されることが必要です。

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: 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、61 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。

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<i>「その他」のグループ</i>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 ログインも必要です。

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、72 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す。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表示されます。

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す。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。71 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: rdefcha

Alert 1406: Superuser privileged UNIX program executed: 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 <Unix-filename>

Alert Extended attribute changed for <Unix-filename>

Alert id 1409
Previous value <old value>
New value <new value>
Date and time Date(9) Time(11)
Path Unix pathname
User User(8)Name
Job name JobName
System id System

E メール通知では、*old 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 <userid> for <unix file name>.

Alert 1409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>

The extended attributes of a UNIX file *unix file name* changed. The old and new extended attributes are shown between the parentheses. The string APS stands for the extended attributes: APF Authorized, Program controlled, and Shared Library. The command was issued by *userid*.

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合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 activated: DASDVOL

Alert: RACF resource class activated: DASDVOL
A change in the status of a RACF resource class has been detected

Alert id 1504
CLASS DASDVOL
Status Active
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 activated: DASDVOL
Alert 1504: RACF resource class 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 deactivated: DASDVOL

Alert: RACF resource class deactivated: DASDVOL
A change in the status of a RACF resource class has been detected

Alert id 1505
CLASS DASDVOL
Status Inactive
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 deactivated: DASDVOL
Alert 1505: RACF resource class deactivated: DASDVOL

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 レコードの数も示されます。

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 による重大度高レベルの問題の検出 (1606)

重大度高レベルの問題を 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・サポートの非活性化 (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・サポートが活性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・サポートが活性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・サポートが活性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 SECCCLASS(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。

このアラートでは、サイトに合わせてグループを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るので、重要なグループを 20 個まで指定します。ユーザー ID の接続に使用されたコマンドと、そのコマンドの発行者も示されます。112 ページの『重要なグループ (1701) の構成』を参照してください。

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を示されます。

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。110 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 4 つあります。

```
#history(nd,<5), #total(nd,>=5),
```

「5」以外の制限を使用する場合は、これら 4 つのインスタンスをすべて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てください。

詳細については、89 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。

違反が多すぎる (2115)

REPORT オプションによって指定された間隔で、特定のログオン 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、このアラートが生成されます。

「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: 15 violations recorded for user C2RMUS01
```

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

```
Alert id      2115
Date and time 09Mar2006 14:49:55.90 - 09Mar2006 14:54:57.89
Violations   15
User         C2RMUS01
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 2115: 15 violations recorded for user C2RMUS01
```

```
Alert 2115: 15 violations recorded for user C2RMUS01
```

このアラートでは、サイトに合わせてカスタマイズを行えます。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るので、過度と見なされる違反の数を指定します。また、除外するログオン ID (またはログオン ID マスク) を 10 個まで指定できます。112 ページの『違反数および除外するログオン ID (2115) の構成』を参照してください。

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

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か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う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

タイプ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
Data set     SYSPROG.APF.LOAD
Volume       <SMS MANAGED>
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
Data set     SYSPROG.APF.LOAD
Volume       <SMS MANAGED>
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。

General resource alerts

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せん。

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 ログインを 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 <Unix-filename>
```

```
Alert Extended attribute changed for <Unix-filename>
```

```
Alert id      2409
Previous value <old value>
New value     <new value>
Date and time Date(9) Time(11)
Path          Unix pathname
User          User(8)Name
Job name      JobName
System id     System
```

E メール通知では、*old 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 <unix file name>.
```

```
Alert 2409: Extended attribute changed (APS-> APS) by <userid> for <unix file name>
```


The extended attributes of a UNIX file *unix file name* changed. The old and new extended attributes are shown between the parentheses. The string APS stands for the extended attributes: APF Authorized, Program controlled, and Shared Library. The command was issued by *userid*.

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 SECCCLASS(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

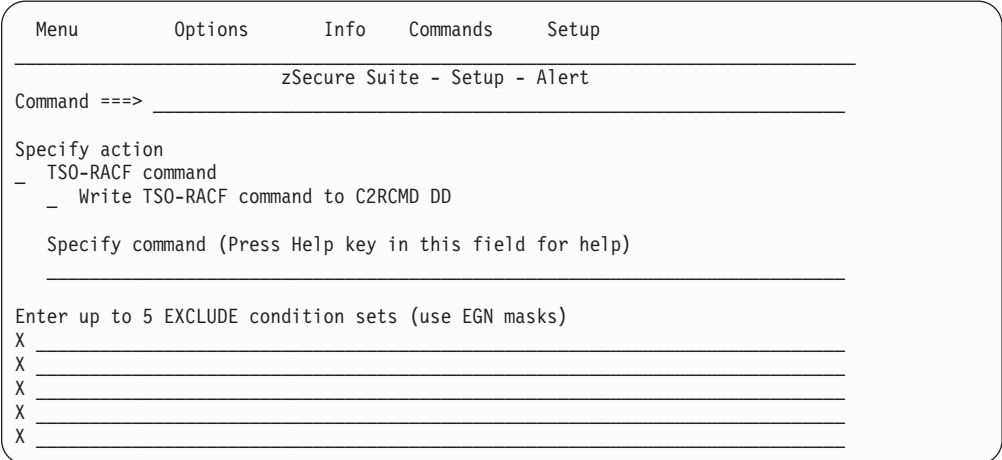
フィルター規則でパケット・フィルターのロギングが有効かどうかの指示、規則が適用されるパケット・ルーティングのタイプ、および規則のセキュリティー・クラスです。

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 18. 「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 19. 「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) の構成

アラート 1115 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。このアラートでは、問題のユーザーを取り消すことができます。

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: User Reference Manual*」を参照してください。

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。

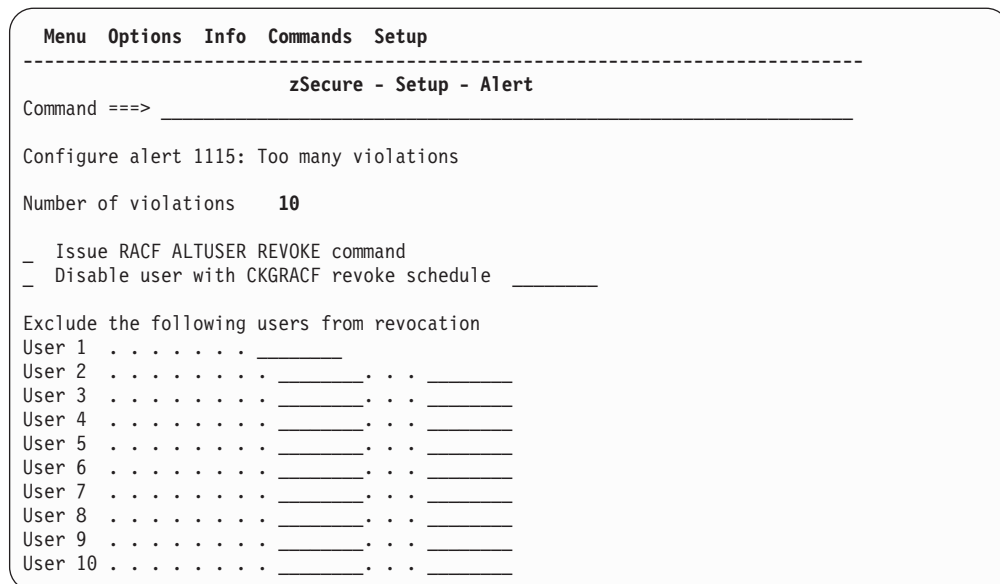


図 20. 「Setup Alert」パネル: 過度の違反に対する取り消しの構成 (アラート 1115)

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。

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。

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。

Issue RACF ALTUSER REVOKE command

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 を指定できます。

複数のユーザー ID を選択する場合は、フィルターを使用することができます。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。

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 21. 「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) を含むことができ、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。

違反数および除外するログオン ID (2115) の構成

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 1115: Too many violations
Number of violations 10

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 22. 「Setup Alert」パネル: 違反数および除外するログオン ID の構成 (アラート 2115)

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。

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を指定できます。

複数のユーザーを選択する場合は、フィルターを使用することができます。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。

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 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: User Reference Manual*」を参照してください。

第 5 章 問題判別ガイド

この情報を使用して、zSecure Alert の問題を識別してトラブルシューティングします。

一般的な概要では、zSecure Collect および zSecure Alert の問題と zSecure Alert の問題を区別する方法と、それらの問題の解決方法について説明します。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

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「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」を参照してください。

zSecure Collect からの CKFnnn 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、「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」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 zSecure Alert と zSecure Audit のどちらで起きているかを判断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。

CKRnnnn メッセージは、zSecure Audit 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。

C2Pnnnn メッセージは、zSecure Alert 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。

zSecure Alert 開始タスクが異常終了した場合は、zSecure Alert に問題があります。プログラム C2POLICE の要約ダンプを受け取った場合は、zSecure Alert に問題があります。プログラム CKRCARLA の要約ダンプを受け取った場合は、zSecure Audit に問題があります。

zSecure Audit の問題診断

zSecure Audit に問題がある場合、次のステップは、問題が stage 1 準備サブタスクにあるのか、それともレポート作成サブタスクにあるのかを確かめることです。zSecure Audit を実行すると、SYSPRINT 出力が生成されます。最新の stage 1 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、最新のレポート作成実行の出力は、SYSPRRPT から分かります。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、zSecure Alert が zSecure

Audit を再び呼び出すと再利用されるため、直ちにコピーを作成してください。zSecure Alert がまだ実行されている場合、それらは既に再利用されています。それでも、それらのデータ・セットには、現在の実行でなく、前に完了した実行が反映されている可能性があります。また、ゼロ以外の戻りコードで終了したすべての zSecure Audit 呼び出しからの SYSPRINT 出力は、C2PDEBUG ファイルに追加されます。

SYSPRINT には、zSecure Audit に送信された入力コマンドと、指標となる CKRnnnn メッセージが必ず含まれています。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、「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」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。バッファオーバー・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

このセクションでは、zSecure Alert で発生する異常終了について説明します。zSecure Collect または zSecure Audit で発生する異常終了については、「*IBM Security zSecure Admin and Audit for RACF: User Reference Manual*」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があります。

- 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。
- 80A878**
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。

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・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。SMFPRMxx 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、45 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を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 (117 ページの『zSecure Audit の問題診断』を参照) で、アラートが発行されたかが分かります。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 7. 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 7. 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
whatPROGRAM	プログラム名。

表 7. 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
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. Tivoli Enterprise Console および NetView の構成

この付録の情報は以下の目的で使用されます。

- Tivoli Enterprise Console を構成する
- 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
- Tivoli Enterprise Console クラスを使用してユーザー定義の BAROC ファイルを作成する
- 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

Tivoli Enterprise Console の構成

このタスクについて

このセクションでは、zSecure Alert トラップおよびユーザー定義の zSecure Alert トラップを正しく表示するために Tivoli Enterprise Console を構成する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・スクリプトを実行すること、および Tivoli Enterprise Console 構成ファイル BAROC (Basic Representation of Object in C) を Tivoli ルール・ベースにインポートすることが含まれます。詳細な説明については、publib.boulder.ibm.com/tividd/td/EnterpriseConsole3.9.html にある IBM 提供の Tivoli Enterprise Console の資料を参照してください。必要なステップの一部は強調表示されています。AIX 5.2 では、Tivoli Enterprise Console バージョン 3.9 を使用していました。

ルール・ベースが作成済みでアクティブになっていることを前提としています。このルール・ベースは本文中で `crm_rb` と呼ばれます。また、NetView Server Daemon (`nvserverd`) が実行中であること、および NetView トラップ構成ファイル (`/usr/0V/conf/tecint.conf`) で NetView Server Daemon がイベントを Tivoli Enterprise Console に転送する必要があることが示されていることも前提となります。以前の Tivoli Enterprise Console セットアップには `nvserverd` アダプターが含まれていない可能性があります。本文で記述されるスクリプトに加えて、OID 構成ファイルおよび CDS 構成ファイルが必要な場合があります。このようなセットアップについては、ここでは説明しません。

本文中の `zSecure-Alert-addtraps.sh` は、IBM 提供の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。さらに、`zSecure-Alert.baroc` は IBM 提供の BAROC ファイルの省略形であり、`user-Alert.baroc` はユーザー定義の BAROC ファイルの省略形です。`user-Alert.baroc` の作成については 134 ページの『Tivoli Enterprise Console クラスを使用したユーザー定義の BAROC ファイル』で説明さ

れ、`user-addtraps.sh` の作成については 136 ページの『AIX 用の `addtrap` コマンド』で説明されます。IBM が提供するファイルの最新バージョンは、オンラインで利用できる zSecure インフォメーション・センター (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc_2.1/samples.html) からダウンロードできます。また、最新の「*IBM Security zSecure: Documentation CD*」からもダウンロード可能です。ファイルは、目次パネルの **zSecure** 項目の「Sample (Tivoli Enterprise Console and NetView Configuration, XSLT)」からアクセスすることができます。

以下のステップのコマンドの大半にはスーパーユーザー特権が必要です。さらに、ご使用の `$PATH` に `wrb` コマンドと `addtrap` コマンドを入れる必要もあります。これはドットとスペースから始まる以下のコマンドを実行することで行われます。

```
. /etc/Tivoli/setup_env.sh
```

以下のコマンドは、IBM 提供のトラップとユーザー定義のトラップの両方に関連します。ユーザー定義のトラップがない場合は、`user-addtraps.sh` および `user-Alert.baroc` に関連するすべてのステップを無視できます。

手順

1. Tivoli Enterprise Console が稼働中であればそれを停止します。
2. 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。

このファイルと他の構成ファイルは、オンラインで利用できる IBM Security zSecure インフォメーション・センターからローカル・ディレクトリーにダウンロードできます。最新の「*IBM Security zSecure: Documentation CD*」からもダウンロード可能です。

3. 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探します。
4. `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/0V/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。
5. `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/0V/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。
6. 既存のユーザー定義の Tivoli Enterprise Console クラスを除去します。このステップは、以前に `user-Alert.baroc` をインポートしたことがある場合にのみ実行する必要があります。次のステップを実行する前に、これらのクラスを除去しておく必要があります。

```
wrb -delrbclass user-Alert.baroc crm_rb
```

7. 既存の zSecure Alert Tivoli Enterprise Console クラスを除去します。このステップは、以前に `zSecure-Alert.baroc` をインポートしたことがある場合にのみ実行する必要があります。

```
wrb -delrbclass zSecure-Alert.baroc crm_rb
```

8. netview.baroc がインポートされているかどうか確認します。次のステップを実行するにはこのファイルがインポートされている必要があります。Tivoli Enterprise Console Server を使用して netview.baroc がインポートされているかどうか確認できます。「Tivoli Enterprise Console Server Desktop for Administrator」ウィンドウで「Event Server」アイコンをダブルクリックします。「Event Server Rule Bases」ウィンドウで crm_rb アイコンを右クリックし、次に「**Import**」を選択します。インポートされるクラスは、「Import Into Rule Bases」ウィンドウの「**Position to insert imported class file**」テキストの下にリストされます。netview.baroc ファイルがここにリストされていなければなりません。リストされていない場合は、ファイルをインポートする必要があります。

9. zSecure Alert BAROC ファイル zSecure-Alert.baroc を Tivoli にインポートします。

```
wrb -imprbclass zSecure-Alert.baroc crm_rb
```

10. ユーザー定義の BAROC ファイル user-Alert.baroc を Tivoli にインポートします。前のステップが実行されている場合にのみ、インポートが正常に行われます。

```
wrb -imprbclass user-Alert.baroc crm_rb
```

11. crm_rb ルール・ベースをコンパイルしてロードします。

```
wrb -comprules crm_rb wrb -loadrb crm_rb
```

12. 以下のコマンドを実行して、Tivoli Enterprise Console イベント・サーバーを停止して再始動します。

```
wstopesvr  
wstartesvr
```

13. Tivoli Enterprise Console を開始します。Tivoli Enterprise Console サーバーが再び実行中になったかどうか確認するには、wstatesvr コマンドを実行します。

14. 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。10.10.3.52 をご使用のコンピューターの IP 番号に置き換えてください。

```
/usr/OV/bin/snmptrap -p 162 10.10.3.52 ¥  
.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"
```

15. トラップが正しく処理されたかどうか確認できます。wtdump1 コマンドを実行して、コマンド出力の最後の数行を確認します。Tivoli Enterprise Console を使用して確認することもできます。

AIX および Windows 上での 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 sh zSecure-Alert-addtraps.sh コマンドと sh user-addtraps.sh コマンドを実行します。これらのコマンドについては 127 ページの『Tivoli Enterprise Console の構成』

で説明しています。これにより、一部の 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。これらのコマンドを以前に実行している場合は、既存の zSecure Alert トラップ定義が新しい定義に置き換えられます。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。

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。

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探します。このようなディレクトリーとしては、最新の「*IBM Security zSecure: Documentation CD*」に含まれている samples があります。
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探します。
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。

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。

Windows 上の NetView で、イベントを Tivoli Enterprise Console に転送する場合は、追加の構成が必要です。zSecure Alert イベントを追加するには、tecad_nv6k.cds ファイルおよび tecad_nv6k.oid ファイルにイベント用の項目を追加する必要があります。次にコンフィギュレーターを再実行するか、項目を組み込むように CONF ファイルを編集します。NetView for Windows 用の CDS ファイル、OID ファイル、および CONF ファイルの編集方法について詳しくは、「*IBM Tivoli Enterprise Console アダプター・ガイド*」を参照してください。

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、129 ページの『AIX および Windows 上での 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。131 ページの『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 132 ページの『トラップ』で説明しています。130 ページの『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。

<pre>name OBJECT-TYPE SYNTAX <i>syntax</i> ACCESS <i>access</i> STATUS <i>status</i> DESCRIPTION <i>description</i> ::= { Alert <i>number</i> }</pre>	<pre><i>user-what</i>ATTEMPTS OBJECT-TYPE SYNTAX <i>DisplayString</i> (SIZE (0..1023)) ACCESS <i>read-only</i> STATUS <i>mandatory</i> DESCRIPTION "Number of password attempts" ::= { Alert 400047 }</pre>
---	---

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
```

説明 *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。『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。

<pre>name TRAP-TYPE ENTERPRISE Alert VARIABLES { v₁, v₂, ... v_m } DESCRIPTION <i>description</i> ::= <i>number</i></pre>	<pre>smfDataLost TRAP-TYPE ENTERPRISE Alert VARIABLES { eventIntegral, eventWhen, whatWTO-MESSAGE, whereSYSTEM } DESCRIPTION "SMF data is lost" ::= 1601</pre>
---	--

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, \dots, 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、131 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。

説明] 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。131 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、127 ページの『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、別の固有な名前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、127 ページの『Tivoli Enterprise Console の構成』で記述されているように、Tivoli Enterprise Console または 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、138 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、130 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

重大度 s_1 、 s_2 、...、および s_m をユーザー定義トラップに割り当てると想定します。個々の重大度 s_i は、クラス名 cn_i に対応しています。

表 8. クラス名に割り当てられる重大度レベル

重大度	説明	クラス名
0	無害/クリア	USER_DEFINED_ALERT_HARMLESS
1	不確定/不明	USER_DEFINED_ALERT_UNKNOWN
2	警告	USER_DEFINED_ALERT_WARNING
3	マイナー	USER_DEFINED_ALERT_MINOR
4	クリティカル	USER_DEFINED_ALERT_CRITICAL

表 8. クラス名に割り当てられる重大度レベル (続き)

重大度	説明	クラス名
5	メジャー/致命的	USER_DEFINED_ALERT_FATAL

重大度とクラス名の間に対応は、BAROC ファイルに指定され、その作成については 134 ページの『Tivoli Enterprise Console クラスを使用したユーザー定義の BAROC ファイル』に記述されています。

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 namei -s ni -S si -g 6 -n Alert ¥
-i 1.3.6.1.4.1.9399.1.2 -o A ¥
-c "Status Events" -e ci ¥
-D di ¥
-E 'vi,1' -V '$V1' ¥
-E 'vi,2' -V '$V2' ¥
...
-E 'vi,j' -V '$Vj' ¥
-t 0 -f - -F '$S $1'
```

132 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、`USER_DEFINED_ALERT_MINOR` クラスに対応します。

```
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 (`_`) で始まります。アンダースコアにより、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、Tivoli Enterprise Console 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。Tivoli Enterprise Console のユーザー・インターフェース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.sh` ファイルを再実行して、これらのアスペクトを `user-addtraps.sh` 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 `namei` のアスペクトなど) を変更したくない場合は、`user-addtraps.sh` ファイルを再実行する前に、このファイルから `addtrap -l namei ...` 行を削除する必要があります。 `addtrap` コマンドを削除せずに、現在のトラップ・アスペクトを反映するように調整する方がさらに良いでしょう。

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。これについては、129 ページの『AIX および Windows 上での NetView の構成』で説明しています。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、136 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、`name1`、`name2`、...、および `namem` であると想定します。

次に、それぞれの名前 `namei`、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: $*"
```

132 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・プロパティとカスタム・フロー・プロパティ』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を提供し、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。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認できません。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をお願いします。

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ます、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](http://www.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 は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency 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、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 は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

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]

アクセシビリティ xii

値, パラメーターの 9

宛先, アラートの 5

アドレス・リスト, E メール の 30

アラート 1

ある特定のログオン ID に対する無効なパスワード試行の制限の超過 88

一般リソースでの WARNING モード・アクセス 67

違反が多すぎる 60, 91

インストール定義 33

インターバル 8

インターフェースのセキュリティークラスの変更 84, 107

疑わしいパスワード変更 58, 90

拡張属性の変更 70, 74, 98

活動化のガイドライン 7

監査証跡は不完全 (1609) 81

監査証跡は不完全 (1610) 82

監査証跡は不完全 (1611) 82

監査証跡は不完全 (2609) 105

監査証跡は不完全 (2610) 105

監査証跡は不完全 (2611) 106

監査対象 UNIX プログラムの実行 71

監査対象プログラムの実行 67

緊急時ユーザー ID を使用したログオン 50

緊急時ログオン ID を使用したログオン 86

グループ権限の除去 54

グループ権限の認可 53

グローバル・セキュリティ対策の活動化 75

グローバル・セキュリティ対策の削除 99

グローバル・セキュリティ対策の追加 99

グローバル・セキュリティ対策の非活動化 75

グローバル・セキュリティ対策の変更 100

グローバル・セキュリティ対策またはオプションの変更 76

アラート (続き)

構成プロセス 5

作成 33

システム権限の除去 88

システム権限の認可 87

システム・レベル権限の除去 53

システム・レベル権限の認可 52

事前定義 45

指定, 宛先の 5

重要なグループへの接続 85

障害の後の SMF ログイングの再開 78

障害の後の SMF ログイングの再開 (2602) 101

条件クラス 7

スーパーユーザー特権のある UNIX プログラムの実行 72

タイプ 5

追加, ユーザー定義の MIB への 130

データ・セットでの WARNING モード・アクセス 93

データ・セットでの WARNING モード・アクセス・アラート 61

データ・ソース 34

定義, 発行条件の 41

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 82, 105

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 52, 87

パスワード・ヒストリーのフラッシュ 57, 89

バッファー 9

非 NON-CNCL ログオン ID による NON-CNCL 権限の使用 92

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 56

非 READALL ログオン ID による READALL 権限の使用 92

非 SECURITY ログオン ID による SECURITY 権限の使用 91

非 SPECIAL ユーザーによる SPECIAL 権限の使用 55

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 69

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 70

フィルター規則によってブロックされたアタック (1609) 81

アラート (続き)

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かった 105

不明ユーザーによるログオン 50

無効なパスワード試行の制限の超過 57

問題判別 119

ユーザー ID のログオン 51

ユーザーがスーパーユーザー特権のあるシェルを取得 73, 98

レイアウト, E メール 49

1024 未満のポートが予約されなくなった 84, 107

APF データ・セットでの更新 63, 94

APF リストからのデータ・セットの除去 95

APF リストからのデータ・セットの除去の検出 96

APF リストからのデータ・セットの除去の検出 (1208) 65

APF リストへのデータ・セットの追加 94

APF リストへのデータ・セットの追加の検出 95

APF リストへのデータ・セットの追加の検出 (1207) 65

CREATE 以上の接続権限の設定 59

DATASET プロファイルでの UACC>NONE 62

DATASET プロファイルでの UACC>=UPDATE 62

IBM Health Checker による重大度が高レベルの問題の検出 80, 103

IBM Health Checker による重大度が中レベルの問題の検出 79, 102

IBM Health Checker による重大度が低レベルの問題の検出 79, 102

IP フィルター規則の変更 85, 108

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 83, 106

RACF リソース・クラスの活動化 76

RACF リソース・クラスの非活動化 77

SETPROG を使用した APF リストからのデータ・セットの除去 64

SETPROG を使用した APF リストへのデータ・セットの追加 64

SMF 119 サブタイプが書き込まれなくなった 82, 106

アラート (続き)

- SMF データ損失の開始 77
- SMF データ損失の開始 (2601) 100
- 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) 81
- 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) 104
- SMF レコードのフラッドの検出 (1607) 80
- SMF レコードのフラッドの検出 (2607) 103
- STC 用のデフォルト STC ログオン ID の使用 97
- STC 用の包括的プロファイルの使用 66
- SVC 定義の変更 78, 101
- UNIX ファイル・アクセス違反 68
- UNIX プログラムでのスーパーユーザー特権の設定 73
- アラート ID 34
- アラート宛先 20
 - 行コマンド 20
- アラート構成
 - 宛先 20
 - 一般設定 16
 - 管理、構成の 13
 - 既存の宛先設定のリセット 20
 - 検査 27
 - 構成名 13
 - 説明 13
 - 選択、アラート・カテゴリの 24
 - パラメーター 8
 - リフレッシュ 29
- アラート構成の管理 13
- アラート構成のステップ 13
- アラート構成のリフレッシュ 29
- アラート定義パネル 109
- アラート・カテゴリ 24
- アラート・フォーマット
 - テキスト・メッセージ 33
 - E メール 33
 - SNMP 33
 - WTO 33
- ある特定のログオン ID に対する無効なパスワード試行の制限の超過アラート 88
- 異常終了、問題判別 118
- 一般リソースでの WARNING モード・アクセス・アラート 67
- 一般リソース・アラート
 - ACF2 97
 - RACF 66
- 移動ウィンドウ
 - 構成 9
 - バッファ 9
 - ユーザー・インターフェース 16

- 違反が多すぎるアラート 60, 91
- インストール固有の名前 109
- インストール定義アラート 40
 - コマンド・セクション 44
 - 事前選択フィルター 41
 - ステージ 1 メンバー 38
 - 追加、カスタムの 33
 - テキスト・メッセージ・レイアウト 43
 - E メール・レイアウト 42
 - ISPF Skeleton 34, 38
 - LIKELIST 41
 - SMF フィルター 34
 - SNMP レイアウト 43
 - UNIX syslog レイアウト 43
 - WTO フィルター 34
- インターバル、アラートの 8
- インターフェースのセキュリティー・クラスの変更アラート 84, 107
- 疑わしいパスワード変更アラート 58, 90
- オンライン
 - 資料 viii
 - 用語 viii

[力行]

- 拡張属性の変更アラート 70, 74, 98
- 数、バッファの
 - 構成 9
 - バッファ 9
- カテゴリ、アラートの 24
- 環境依存の選択基準 40
- 監査証跡は不完全 (1609) アラート 81
- 監査証跡は不完全 (1610) アラート 82
- 監査証跡は不完全 (1611) 82
- 監査証跡は不完全 (2609) アラート 105
- 監査証跡は不完全 (2610) アラート 105
- 監査証跡は不完全 (2611) アラート 106
- 監査対象 UNIX プログラムの実行アラート 71
- 監査対象プログラムの実行アラート 67
- 緊急時ユーザー ID を使用したログオン・アラート 50
- 緊急時ユーザー構成 110
- 緊急時ログオン ID を使用したログオン・アラート 86
- クラス、アラート条件の 7
- グループ権限の除去アラート 54
- グループ権限の認可アラート 53
- グループ・アラート 85
- グローバル・スケルトン 41
- グローバル・セキュリティー対策の活動化アラート 75
- グローバル・セキュリティー対策の削除アラート 99

- グローバル・セキュリティー対策の追加アラート 99
- グローバル・セキュリティー対策の非活動化アラート 75
- グローバル・セキュリティー対策の変更アラート 100
- 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アラート 76
- 研修 xii
- 構成
 - アラート 1102 110
 - アラート 1701 112
 - アラート 2102 110
 - アラート 2115 112
 - 違反数および除外するログオン ID アラート 112
 - ガイドライン 8
 - 緊急時ユーザー 110
- 構成、アラートの 5
- 構成過度の違反に対する取り消しアラートアラート 1115 110
- 構成データ・セット 5
- コマンド、アラート定義における 44

[サ行]

- 作成、アラートの 33
- システム権限の除去アラート 88
- システム権限の認可アラート 87
- システム・アラート
 - 一般 77
 - ACF2 100
- システム・レベル権限の除去アラート 53
- システム・レベル権限の認可アラート 52
- 事前定義アラート
 - 一般リソース ACF2 97
 - 一般リソース RACF 66
 - インストール固有の名前 109
 - グループ 85
 - システム 77
 - 重大度レベル 45
 - データ・セット・アクセス 61
 - データ・セット・プロファイル 61
 - フォーマット 49
 - リスト 45
 - ACF2 86
 - ACF2 システム 100
 - ACF2 制御 99
 - ACF2 データ・セット 93
 - ACF2 ユーザー 86
 - RACF 50
 - RACF 制御 75
 - RACF ユーザー 50
 - UNIX ACF2 97
 - UNIX RACF 68
- 重要なグループ 112

重要なグループへの接続アラート 85
障害の後の SMF ロギングの再開 (2602)
アラート 101
障害の後の SMF ロギングの再開アラ
ート 78
条件クラス、アラートの 7
資料
 アクセス、オンライン viii
 本製品用のリスト viii
スーパーユーザー特権のある UNIX プロ
 グラムの実行アラート 72
ステージ 1 メンバー
 インストール定義アラート 38
 検査 28
制御アラート
 ACF2 99
選択基準 40

[タ行]

追加、アラートの 33
通知方法 1
データ・セットでの WARNING モード・
 アクセス・アラート 61, 93
データ・セット・アラート
 ACF2 93
 RACF 61
定期的な概要 115
テキスト・メッセージ
 アラート・フォーマット 33
 送信元アドレス 20
 ユーザー・インターフェース 20
 レイアウト 43
 Recipient 20
 Replyto アドレス 20
デフォルト・フィルター規則によってプロ
 ックされたアタックがログに記録されな
 くなったアラート 82, 105
トラップ
 定義の構文 132
 変数 131
トラブルシューティング xii

[ハ行]

パスワードによる高い許可レベルのユーザ
 ーの取り消しアラート 52, 87
パスワード・ヒストリーのフラッシュ・ア
 ラート 57, 89
発行、アラートの 41
バッファー
 使用、モニター 9
バッファー、アラートの 9
バッファー数
 ユーザー・インターフェース 16

バッファー・サイズ 9
 計算 9
 構成 9
パネル
 アラート 20
 Setup Alert 12, 24, 27, 30
パラメーター
 値 9
 OPTION 9
 REPORT 9
非 NON-CNCL ログオン ID による
 NON-CNCL 権限の使用アラート 92
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・アラート 56
非 READALL ログオン ID による
 READALL 権限の使用アラート 92
非 SECURITY ログオン ID による
 SECURITY 権限の使用アラート 91
非 SPECIAL ユーザーによる SPECIAL
 権限の使用アラート 55
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アラート 69
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アラート 70
フィルター規則によってブロックされたア
 タック (1609) アラート 81
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アラ
 ート 105
不明ユーザーによるログオン・アラート
 50

[マ行]

無効なパスワード試行の制限の超過アラ
 ート 57
メモリー内バッファーの使用 9
メンバー、検査による 27
モニター、一般システム・イベントの
 100
モニター、ユーザー・イベントの
 ACF2 ユーザー 86
 RACF ユーザー 50
問題診断、zSecure Alert の 118
問題診断、zSecure Audit の 117
問題診断に関する情報 117
問題判別 xii
 ガイダンス 117
 診断に関する情報の検索 117
 ライセンス 119

[ヤ行]

ユーザー ID のログオン・アラート 51

ユーザー定義アラート
 追加、MIB への 130
ユーザーによるスーパーユーザー特権のあ
 るシェルの取得アラート 73, 98
ユーザー・アラート
 ACF2 86
 RACF 50
用語 viii

[ラ行]

ライセンス問題診断 119
リフレッシュ
 ユーザー・インターフェース 29
レポート作成間隔
 構成 8
 バッファー 9
 ユーザー・インターフェース 16
レポート作成の実行、問題判別 117

[数字]

1024 未満のポートが予約されなくなった
 アラート 84, 107

A

ACF2 事前定義アラート 86
ACF2 データ・セット・アラート 93
ACF2 ユーザー・アラート 86
Alert パネル 20
APF データ・セットでの更新アラート
 63, 94
APF リストからのデータ・セットの除去
 アラート 95
APF リストからのデータ・セットの除去
 の検出 (1208) アラート 65
APF リストからのデータ・セットの除去
 の検出アラート 96
APF リストへのデータ・セットの追加ア
 ラート 94
APF リストへのデータ・セットの追加の
 検出 (1207) アラート 65
APF リストへのデータ・セットの追加の
 検出アラート 95
AVERAGEINTERVAL
 構成 9
 バッファー 9
 ユーザー・インターフェース 16

B

BAROC ファイル 134
BCC 20

Buffer size
ユーザー・インターフェース 16
BUFSIZE 9
構成 9
ユーザー・インターフェース 16

C

C2RSYSLG DD 20
CC 20
CKFREEZE
収集時刻 16
ユーザー・インターフェース 16
Collect name
ユーザー・インターフェース 16
Collect time
ユーザー・インターフェース 16
COLLECTSTCNAME
ユーザー・インターフェース 16
COLLECTTIME
ユーザー・インターフェース 16
CREATE 以上の接続権限の設定アラート
59

D

DATASET プロファイルでの
UACC>NONE アラート 62
DATASET プロファイルでの
UACC>=UPDATE アラート 62
DEBUG BUFFER 9

E

E メール
アドレス・リスト 30
アラート・フォーマット 33, 49
受信側アドレス 20
出力フォーマット 20
送信元アドレス 20
ユーザー・インターフェース 20
レイアウト 42
BCC アドレス 20
C2RSMTP DD 20
CC アドレス 20
Font size 20
Replyto アドレス 20
Environment refresh
構成 8
問題判別 117
ユーザー・インターフェース 16

F

FROM 20

150 ユーザー・リファレンス・マニュアル

G

GSO 設定の変更 99

I

IBM
ソフトウェア・サポート xii
Support Assistant xii
IBM Health Checker による重大度が高レ
ベルの問題の検出アラート 80, 103
IBM Health Checker による重大度が中レ
ベルの問題の検出アラート 79, 102
IBM Health Checker による重大度が低レ
ベルの問題の検出アラート 79, 102
INTERVAL
構成 8
バッファ 9
ユーザー・インターフェース 16
IP フィルター規則の変更アラート 85,
108
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アラート
83, 106
ISPF Skeleton
インストール定義アラート 34

L

LIKELIST
事前選択フィルター 41
問題判別 117

M

MAILFONTSIZE 20
MAILTO 20
MIB ファイルのマージ 134

N

NetView
構成 129
NUMBUFS
構成 9
バッファ 9
ユーザー・インターフェース 16

O

OPTION パラメーター 9

Q

QRadar SIEM
SYSLOG フォーマット 141

R

RACF
事前定義アラート 50
制御アラート 75
データ・セット・アラート 61
ユーザー・アラート 50
RACF リソース・クラスの活動化アラ
ート 76
RACF リソース・クラスの非活動化アラ
ート 77
REFRESH コマンド 29
REPLYTO 20
REPORT パラメーター 9

S

sddtrap コマンド
AIX 136
Windows 138
SETPROG を使用した APF リストからの
データ・セットの除去アラート 64
SETPROG を使用した APF リストへのデ
ータ・セットの追加アラート 64
Setup Alert パネル 12, 24, 27, 30
Skeleton
グローバル 16
SMF 119 サブタイプが書き込まれなくな
ったアラート 82, 106
SMF データ損失の開始 (2601) アラート
100
SMF データ損失の開始アラート 77
SMF フィルター
インストール定義アラート 34
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) アラート 81
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) アラート 104
SMF レコードのフラッドの検出 (1607)
アラート 80
SMF レコードのフラッドの検出 (2607)
アラート 103
SMF_x
ユーザー・インターフェース 34
SMTPTOFILE 20
SNMP
アラート・フォーマット 33
受信側アドレス 20
出力 123
トラップ 123
ユーザー・インターフェース 20

SNMP (続き)
レイアウト 43
C2RSNMP DD 20
SNMPTO 20
SNMPTOFILE 20
STAGE1INTERVAL
構成 8
ユーザー・インターフェース 16
STC 用のデフォルト STC ログオン ID
の使用アラート 97
STC 用の包括的プロファイルの使用アラ
ート 66
SVC 定義の変更アラート 78, 101
SYSLOG フォーマット
QRadar SIEM 141

T

Tivoli Enterprise Console
構成 127

U

UNIX syslog
アドレス 20
ユーザー・インターフェース 20
レイアウト 43
C2RSYSLG DD 20
UNIX アラート
ACF2 97
RACF 68
UNIX ファイル・アクセス違反アラート
68
UNIX プログラムでのスーパーユーザー特
権の設定アラート 73

V

Verify
ユーザー・インターフェース 27

W

WTO
アラート・フォーマット 33
ユーザー・インターフェース 20
C2RWTO DD 20
WTO フィルター
インストール定義アラート 34
WTOTOFILE 20
WTOx
ユーザー・インターフェース 34

Z

zSecure Alert
構成 12, 13, 16, 20



Printed in Japan

SA88-7156-00



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