



IBM Software Group

System z 内部統制強化セミナー ～ 監査対応とSecurity Server～

2008年 5月23日, 6月13日

日本アイ・ビー・エム株式会社

ソフトウェア事業

System z ソフトウェア・テクニカルセールス

鈴木優子

 Tivoli software



目次

- System z のセキュリティーと監査
 - ▶ Security Server に関する監査の質問項目と対応例
- 監査対応に役立つツール
 - ▶ Tivoli zSecure スイート
- 事例のご紹介
- アクセスログとzSecure Audit
- (ご参考) 監査のポイントとレポートの例
- (ご参考) Tivoli zSecure 1.9.1 最新リリース情報



System z のセキュリティーと監査

- 監査人はこんなことを言っています

システムの安全性確保のために**アクセス管理などの内部統制**が必要です。

財務報告に関連するシステムやソフトウェアで、**適切なアクセス管理等の方針**を定め実施していますか？



監査人

セキュリティーポリシーやアクセスコントロールは全ての統制の基本です！



System z のセキュリティーと監査

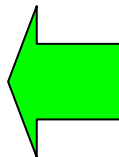
～Security Serverに関する監査の質問項目例

設定全般

特権ID関連

ユーザー管理関連

監査ログ関連



-Security Server 設定を把握・管理していますか。

-ID管理は適切になされていますか。

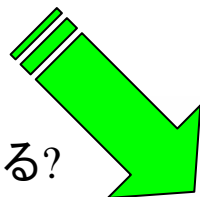
-“誰が”,”いつ”システムにアクセスし”何に対して何をしたか”の履歴を取得・把握されていますか。違反のチェックはされていますか。



監査人

設定は勿論把握している?

監査ログ- 特に誰がいつ何を
したか等 - はレポートが
簡単に出せるよね?



IT担当者, セキュリティ担当者

他の対応も大変なのに
そんな簡単に出せないよ。
Security Serverの設定把
握・変更は難しい!!
いったどうしたら??



System z のセキュリティーと監査

～Security Serverに関する監査の質問項目具体例

設定全般

- RACFコマンドの実行は適切なセキュリティ管理者にのみ実行できるよう設定され適切に管理、監視(ログ)されていますか。
- 重要なシステム設定データへのアクセスは限られた特権ユーザーに絞られ、管理されていますか。
- RACFのPROTECTALLが設定されていますか。
- RVARVコマンドのパスワードがデフォルトでなくきちんと設定されていますか。
- RACFリソースクラスが適切に管理され、必要に応じて活動状態になっていますか。

特権ID関連

- デフォルトの特権ユーザーであるIBMUSERが使用できない設定となっていますか。
- 管理者権限が職務分掌として管理されていますか

ユーザー管理関連

- ユーザーIDは適切に管理されていますか。不要IDを定期的に見直し、削除等適切に対処していますか。また一定期間以上不使用のIDが使用不能となる設定になっていますか。
- パスワード・ルールが決められ、一定期間でパスワード変更する運用となっていますか。

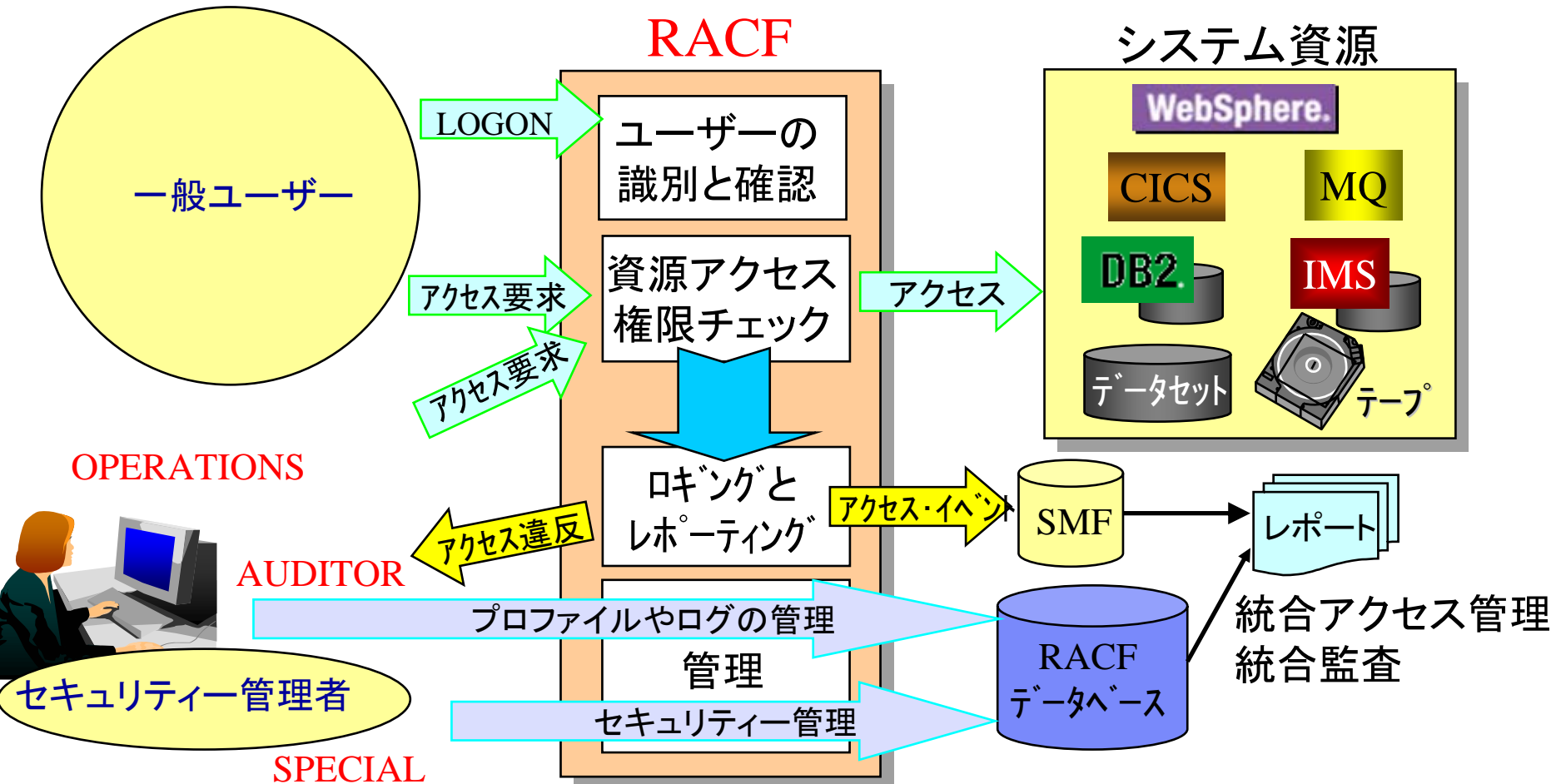
監査ログ関連

- 監査ログの分析や違反レポートは適切に作成・チェックされていますか。

監査人



System z のセキュリティーと監査 ～Security Server(RACF)の役割



RACFがz/OS環境での統合セキュリティー管理を提供

Security Serverに関する監査の質問項目=>対応例(1)

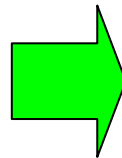
RACF標準機能による対応

設定全般

特権ID関連

ユーザー管理関連

監査ログ関連



RACF標準機能による課題点

- RACFを熟知していないと設定そのものやレポート出力内容の理解が難
- レポート内容・フォーマットが限定される(DSMON使用にはAuditor権限必須)
- 場合によりプログラミングが必要
- RACFスキルをつけるには時間と経験が必要

- DSMON
(AUDITOR 属性でのみ実行可能なユーティリティ)
 - ▶ システムの設定状況確認
 - ▶ クリティカルな資源の保護状況
 - ▶ 特権ユーザー/PPT/...
- IRRICE (DFSORT/ICETOOL) ...(<=RACFRW)
 - ▶ システムの設定状況確認
 - ▶ 最近のセキュリティ違反表示
 - ▶ RACF関連事象の時系列表示
- SETROPTS LIST コマンド
 - ▶ システムの設定状況確認
 - ▶ その他のRACFコマンド
 - ▶ LISTxxxx/RLIST, SEARCH, ...
- 各種ユーティリティ
 - ▶ IRRUT100, IRRRID00, ...

Security Serverに関する監査の質問項目=>対応例(2)

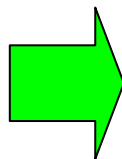
RACF標準機能の課題対応策

設定全般

特権ID関連

ユーザー管理関連

監査ログ関連



■ ツールの使用

- ▶ Tivoli zSecure Admin
 - RACF管理を容易に
- ▶ Tivoli zSecure Audit
 - 柔軟で容易なレポート作成

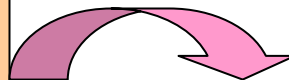
■ 利点

- ▶ 熟練者でなくともすぐに使用可能
- ▶ 必要に応じて柔軟にレポート作成・変更
- ▶ RACFのみでなくミドルウェアを含めた多角的な証跡・監査レポートの作成
- ▶ ツール使用によるレポート信頼性

RACF標準機能による課題点

- RACFを熟知していないと設定そのものやレポート出力内容の理解が難
- レポート内容・フォーマットが限定される(DSMON使用にはAuditor権限必須)
- 場合によりプログラミングが必要
- RACFスキルをつけるには時間と経験が必要

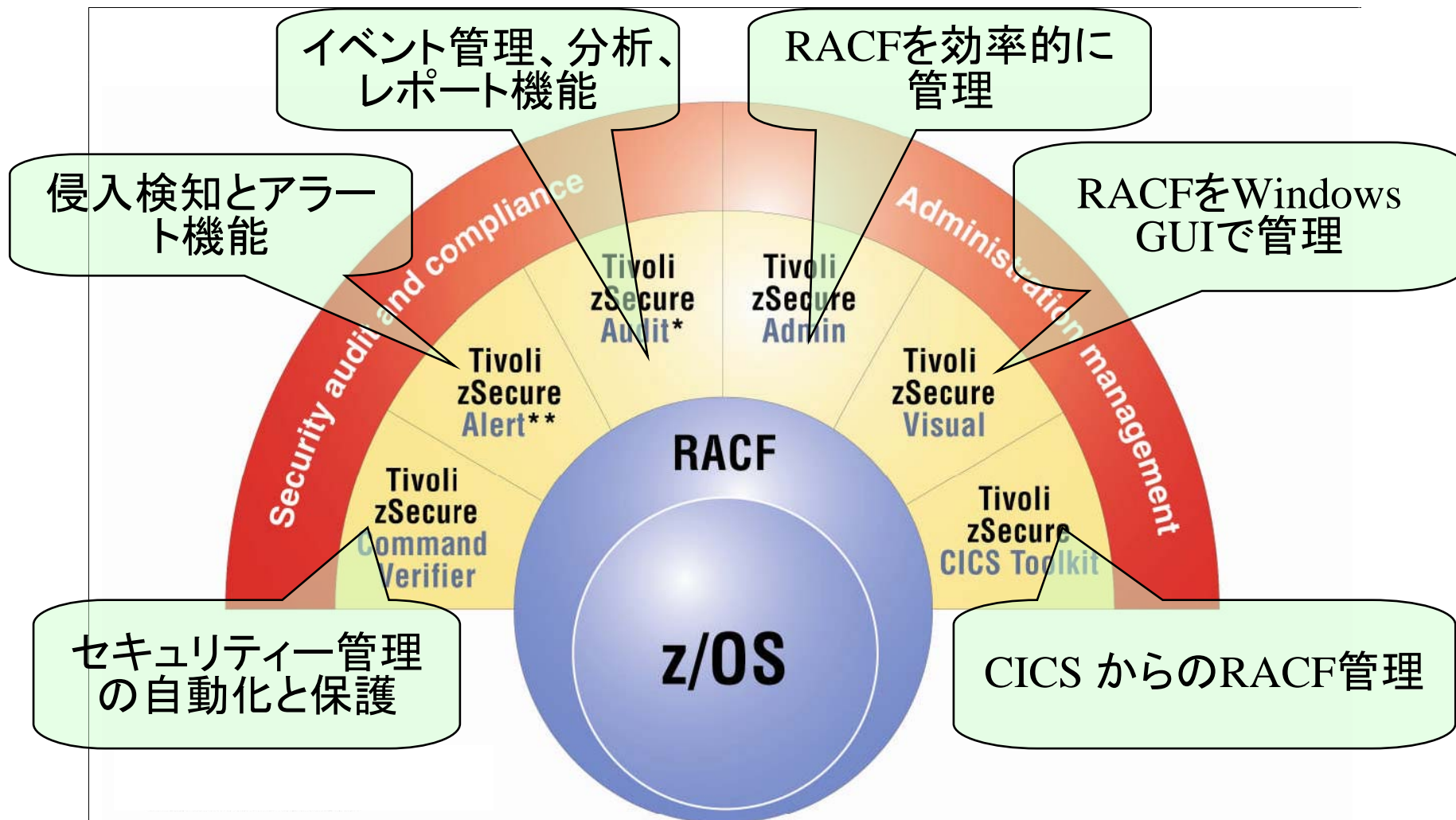
加えて



内部統制プロジェクトでは
IT担当者の仕事の負荷が間違いなく高くなる!!



Tivoli zSecure スイート



詳細は 2007年7月 System z 内部統制セミナー資料(以下リンク先)を参照

<http://www-06.ibm.com/jp/servers/eserver/zseries/seminar/jsox/document200707.html>

Tivoli zSecure の特長

- 自動監査、リスク特定機能
 - ▶ RACFのみでなくz/OSシステム・パラメータの設定にまでおよぶ**詳細なリスク分析やレポート**が可能
- 柔軟で簡易なレポート・インターフェース
 - ▶ **標準レポートのみでなく**、簡易なインターフェースおよび簡易なCARLaというレポート言語を使用し、**自在にレポート・フォーマットおよび抽出項目をカスタマイズ可能**
⇒ **今後J-SOX対応に必須の機能**
- 豊富なSMFレコード・タイプをサポート
 - ▶ **約40種類ものSMFレコード・タイプをサポート**
 - ▶ 特に**DB2, TCPIP, USS(Unix System Service)関連の詳細レコード**も処理しレポートが可能
- オープン系との統合証跡管理(将来へ向けて)
 - ▶ 注:2008年5月現在、オープン系のログ証跡管理ツールであるTCIM(Tivoli Compliance Insight Manager)は日本語OS上のサポート未対応です。
- 日本語サポートの強化
 - ▶ **操作パネルをはじめとして順次日本語サポートを拡大予定**



事例のご紹介

- zSecure採用の決め手となったのは
 - ▶ J-SOX対応で必要な人がやるべきことを正常に実施している事実を証明したい
 - 証明するためのレポートをすばやく出力できることが必要
 - レポートを柔軟にカスタマイズできることが必要
 - 今現在および過去に遡って柔軟に監査証跡を確認できることが必要
 - ▶ J-SOXのみでなく個人情報保護法等の対応として
 - 素早く漏れなく監査証跡の確認ができる環境を作ることで情報漏洩リスクをなくすることができる
 - ▶ 監査人に指摘された事項に短期間で対応できそうだと実感した
 - デモンストレーションを見て簡単にできそうだと実感した
 - RACFの設定変更を要求されてもすぐに対応できる
 - ▶ Security Server(RACF)の管理が容易
 - コマンド自動生成は非常に便利
 - RACFのオペレーションは難しい
 - ▶ いろいろな視点でのレポート生成が必要
 - この人がいつ何をしたと言う検索のみではなく以下のようなレポートが欲しい
 - このファイルにはいつ誰がアクセスした
 - このジョブはいつ誰が実行した

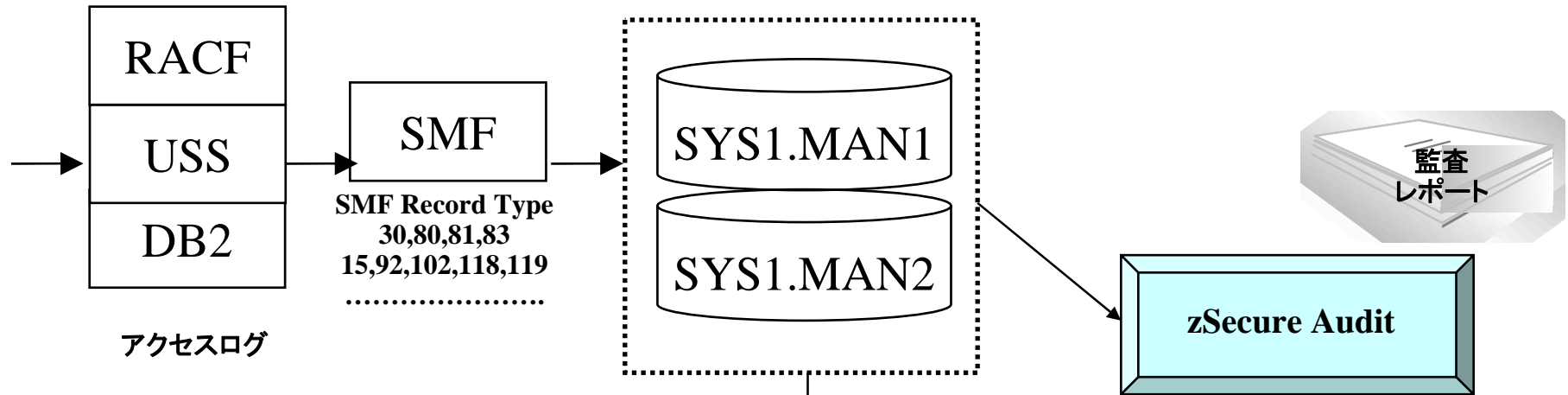


事例のご紹介

- 採用されたzSecure 製品
 - ▶ Tivoli zSecure Admin/Audit の組み合わせ
 - 最も一般的な使用法
 - Admin を使用してRACF設定変更を安全・確実に実施
 - 日々の運用を効率的に実施
 - Audit を使用して監査対応と状況分析
 - 監査証跡レポートの出力
 - RACF設定, OS設定 共にセキュリティ上の脆弱性分析を実施
 - 定義の整合性分析と定義見直し
 - 日々の運用を効率的に実施
 - ▶ Tivoli zSecure Admin/Audit/Alert の組み合わせ
 - もう一歩進んだリアルタイム通知
 - Alert を使用して重要な操作が行われたことや違反を通知
 - 違反レポートを毎日確認する非効率作業をやめてAlertに変更
 - ▶ Tivoli zSecure Admin/Audit および DB2 Log Analysis Tool の組み合わせ
 - DB2をお持ちのお客様に理想的な採用方法
 - ミドルウェアも含めたRACFの設定確認・変更はAdminを使用
 - RACFおよびミドルウェアについてはAudit を使用して多角的な監査証跡レポート
 - DB2関連はLog Analysis Toolを主体として使用
 - 主要な表のみにトレースをかけ、zSecure Audit で確実に証跡管理



アクセスログとzSecure Audit

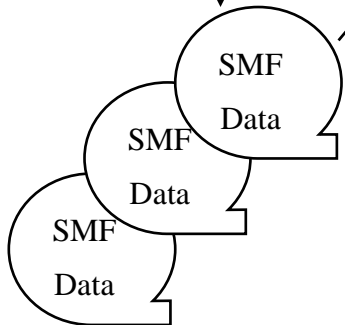


アクセスログ

SMF Record Type
30,80,81,83
15,92,102,118,119
.....

Unload 処理

- SMF レコード・タイプ**
- 14: データセットWRITE
 - 15: データセットREAD
 - 92: Unix System Service
 - 102: DB2監査レコード
 - 118: TCPIP, TELNET, FTP
 - 119: TCP UDP, IP



Tivoli zSecure Audit では
RACF以外にTCPIPやFTP,USS等
のレコード処理が可能
またRACF DBやシステム設定内
容(CKFREEZE)を抽出、分析可能

(ご参考) J-SOXで必要と考えられている監査のポイントとレポートの例

- セキュリティーのための制御が実施されている
 - ▶ ユーザーID管理状況のレポート(設定情報、使用状況)
 - ▶ 特権ユーザー状況のレポート
 - ▶ ユーザー認証管理(パスワード)状況のレポート
 - ▶ システム資源のアクセス保護状況のレポート

- 適切なユーザーが適切なアクティビティを実施している
 - ▶ RACFアクティビティの全記録レポート
 - ▶ 不要ユーザーIDのレポート
 - ▶ ユーザー認証の違反レポート
 - ▶ システム資源のアクセス状況レポート
 - ▶ システム資源のアクセス違反レポート
 - ▶ 特権ユーザー・アクティビティ・レポート



特権ユーザー状況のレポート

zSecure Admin+Audit for RACF ユーザー概要 - complex SYS1
special OR operations OR auditor の全ユーザー

7Mar2008 21:04

page 1

User	Name	DfltGrp	Owner	RIRF	SOAg	LCX	Int	LastCon	Connect	groups	Pri	InstData
ABPUSER	DB2 THREAD EXPERT	OMVSGRP	TANAKA	I	SU	X		27Nov06	OMVSGRP			
AKANE	HAYASHI#2	OMVSGRP	SYS1	I	SOA	X	32	25Jul07	DB2TST01	OMVSGRP		
CONSL01	テスト	OMVSGRP	OMVSGRP		SO			7Mar08	AOP ASM ASU BPA CBC CDS			
									CEE CIM CMX CPAC CSC CSF			
									DIT DVG EGN EOX EOY EPH			
									EQAW EUV EUVF FFST FMN			
									GDDM GIM GLD GSK HCM IBMZ			
									ICA ICQ IDI ILM IMO IMW			
									ING IOA IOE ISF ISP MSOPS			
									NETVIEW NPM OMVSGRP OS390			
									OS390GRP PAGE REXX SMPE			
									SYSCTLG SYS1 TCPIVP TPNS			
									VSAMDSET ZOS4MCAT			
									ZOS4MCAT ZOS5			

特権ユーザー一覧とその属性をレポート・管理します。

S: Special => RACF特権コマンドを実行(セキュリティ設定変更)

O: Operations => 全RACF保護資源へアクセス

A: Auditor => 監査関連コマンドやSpecialユーザー使用のプロファイル
情報にアクセス

ICA ICQ IDI ILM IMO IMW

.....

特権ユーザー・アクティビティ・レポート

zSecure Admin+Audit for RACF ユーザー・イベント 23Jul07 21:16 to 5Mar08 17:20

page 1

特権ユーザー・アクティビティ 詳細

Date	Time	User	Sys	Description
23Jul2007	21:16	SUZUKI	SYS1	RACF SETROPTS success for SUZUKI
Jobname + id: SUZUKI TSU05144				
RACF command: SETROPTS REFRESH WHEN(PROGRAM)				
Name : SUZUKI Instdata :				
24Jul2007	23:50	CONSL03	SYS1	RACF RDEFINE success for CONSL03: RDEFINE SURROGAT IBMUSER.**
Jobname + id: CONSL03 TSU05315				
RACF command: RDEFINE SURROGAT (IBMUSER.** LEVEL(0)				
Name : TEST03 Instdata :				
24Jul2007	23:50	CONSL03	SYS1	RACF RALTER success for CONSL03: RALTER SURROGAT IBMUSER.**
Jobname + id: CONSL03 TSU05315				
RACF command: RALTER SURROGAT (IBMUSER.** (READ))				
Name : TEST03 Instdata :				

特権ユーザーが、いつ・どのような特権コマンドを実行したか、詳細をレポートしています。

特権ユーザーが権限の範囲で必要なアクティビティを実施している証明となります。

また、万が一の場合に特権を使用したミスや故意の操作状況を解明できます。

05Mar2008	17:20	CONSL03	SYS1	RACF ALTUSER YUKO RESUME
Jobname + id: CONSL03 TSU03278				
RACF command: ALTUSER YUKO RESUME				
Name : TEST03 Instdata :→				

一定期間以上未使用のアカウント概要

zSecure RACF USER オーバービュー - complex SYS1
2007年以降未使用のユーザー

7Mar2008 20:21

page 1

User	Name	DfltGrp	Owner	RIRP	SOAgC	LCX	Int	LastCon	Connect	groups	Pri	InstData
irrcerta	CERTAUTH	Anchor	irrcerta	R		CX						
irrmulti	Criteria	Anchor	irrmulti	R		X						
irrsitec	SITE	Anchor	irrsitec	R		X						
ABPUSER	DB2 THREAD EXPERT	OMVSGRP	TANAKA	I	SO	X		27Nov06	OMVSGRP			
AESTCMDS	NPMIP	OMVSGRP	OMVSGRP	I		X	35	23Jun04	OMVSGRP	OS390 OS390GRP		
AESTCPIP	NPMIP	OMVSGRP	OMVSGRP	I		X	35	23Jun04	OMVSGRP	OS390 OS390GRP		
AESTNETS	NPMIP	OMVSGRP	OMVSGRP	I		X	35	23Jun04	OMVSGRP	OS390 OS390GRP		
AOFARCAT	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTBASE	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON01	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON02	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON03	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON04	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON05	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON06	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON07	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON08	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON09	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON10	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON11	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON12	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON13	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTCON14	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTGSS	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTHB	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTHUB	NETVIEW MSM	NETVIEW	NETVIEW			X	35		NETVIEW			
AUTHW001		NETVIEW	NETVIEW			X	35		NETVIEW			
AUTHW002		NETVIEW	NETVIEW			X	35		NETVIEW			
AUT101	NETVIEW V3R1MO	NETVIEW	NETVIEW			X	35		NETVIEW			

未使用IDにより不要なIDを割り出します。

未使用IDの棚卸により未使用IDの不正使用等の危険性を取り除きます。

ユーザー認証の違反レポート

RACFユーザー・イベント 4Mar08 17:14 to 7Mar08 20:08
 ログオン成功・失敗の全ユーザー・アクティビティ詳細

page 1

ユーザー	システム	日付	開始時間	終了時間	Date	Time	Sys	Description
CONSL01	SYS1	07Mar2008	19:42:35.46	19:42:35.46		7 Mar 2008	19:42	SYS1 Start of job CONSL01 (TSU03466) for user CONSL01
CONSL03	SYS1	05Mar2008	17:14:50.67	17:33:01.49		5 Mar 2008	17:14	SYS1 Start of job CONSL03 (TSU03278) for user CONSL03
CONSL03	SYS1	07Mar2008	18:59:12.28	18:59:12.28		5 Mar 2008	17:33	SYS1 End of job CONSL03 (TSU03278) for user CONSL03 code RCO
HAYASHI	SYS1	04Mar2008	18:02:38.42	23:26:23.92		7 Mar 2008	18:59	SYS1 Start of job CONSL03 (TSU03462) for user CONSL03
						4 Mar 2008	18:02	SYS1 End of job HAYASHI (TSU03113) for user HAYASHI code S222
						4 Mar 2008	22:07	SYS1 Start of job HAYASHI (TSU03171) for user HAYASHI
						4 Mar 2008	22:10	SYS1 Start of job DB2@DIAG (JOB03172) for user HAYASHI
						4 Mar 2008	22:10	SYS1 End of job DB2@DIAG (JOB03172) for user HAYASHI code RCO
						4 Mar 2008	22:31	SYS1 Start of job MHI@ORG (JOB03176) for user HAYASHI
						4 Mar 2008	22:31	SYS1 End of job MHI@ORG (JOB03176) for user HAYASHI code RCO
						4 Mar 2008	22:32	SYS1 Start of job MHI@BAK (JOB03177) for user HAYASHI

ユーザーのアクティビティをレポートします。

ログオン、ログオフのシステムへのアクセス記録とジョブの実行やファイル・アクセス状況をレポートします。

各ユーザーが必要な作業を実施していることを証明すると共に万が一の場合に違反状況を追求できます。

4 Mar 2008 22:43 SYS1 End of job BAT@ORG (JOB03186) for user HAYASHI code RCO
 4 Mar 2008 22:44 SYS1 Start of job BAT@ORG (JOB03187) for user HAYASHI
 4 Mar 2008 22:44 SYS1 End of job BAT@ORG (JOB03187) for user HAYASHI code RCO

脆弱パスワードを持つユーザー一覧

脆弱パスワード・ユーザー一覧 7 Mar 2008 20:32

page 1

Profile Name	CreateDate	LastUseDate	LastPwdChg	Rev	PwTry	InstData
ABPUSER DB2 THREAD EXPERT	1 Dec 2005	27 Nov 2006			0	
AUTXCF2	19 Aug 2003					
BOH2 BOH2	15 Nov 2005					
CANCEL	26 May 2004					
CNMCSSIR	1 Dec 1998	19 Nov 2002			0	
CONSL01 テスト	18 Apr 2007	7 Mar 2008	18 Apr 2007		0	
CONSL02 TEST02	18 Apr 2007	30 Jan 2008	28 Nov 2007		0	
CONSL03 TEST03	18 Apr 2007	7 Mar 2008	28 Nov 2007		0	
CONSL04 TEST04	18 Apr 2007	28 Nov 2007	28 Nov 2007		0	
CONSL05 TEST05	18 Apr 2007	28 Nov 2007	28 Nov 2007		0	
CONSL06 TEST06	18 Apr 2007	28 Nov 2007	28 Nov 2007		0	
CONSL07 TEST07	18 Apr 2007	28 Nov 2007	28 Nov 2007		0	
DBUSER USER_DBUSER		26 Jul 2006	26 Jul 2006		0	
DB2ADMIN DB2CONNECT USER					0	
DFS					0	
GEST01						
IBMU						
IHSA						
IMSU						
IMSU						
INET						
INOK						
LOGO						
NETO						
PMUS						
SIMU						
SMFCL						
SMFDUMP						
TSOWAS1 WAS TSO	3 Jun 2005	3 Jun 2005			0	
TS014	22 Sep 2006	22 Sep 2006			0	
WSADMIN WAS ADMINISTRATOR	1 Jul 2005	1 Jul 2005	1 Jul 2005		0	
WSAMPLE WORKSHOP SAMPLE	13 Apr 1999	13 Apr 1999	13 Apr 1999		0	
WSGUEST WAS DEFAULT USER	1 Jul 2005					

パスワードとユーザーIDが同じ、等の脆弱設定ユーザーを一覧します。

システム上のセキュリティ設定で脆弱パスワード登録を許可しない方法もありますが、このように一覧レポートとして出力することで、早期に対処が可能となります。

パスワード期限のないユーザー一覧

ユーザーの概要 - complex SYS1 7Mar2008 21:01

page 1

パスワード期限のない全ユーザー

User	Name	DfltGrp	Owner	RIRP	SOAgC	LCX	Int	LastCon	Connect	groups	Pri	InstData
irrcerta	CERTAUTH Anchor		irrcerta	R		CX						
irrmulti	Criteria Anchor		irrmulti	R		X						
irrsitec	SITE Anchor		irrsitec	R		X						
ABPUSER	DB2 THREAD EXPERT	OMVSGRP	TANAKA	I	SO	X		27Nov06	OMVSGRP			
CONSL01	テスト	OMVSGRP	OMVSGRP		SO			7Mar08	AOP ASM ASU BPA CBC CDS CEE GIM CMX CPAC CSC CSF DIT DVG ECN EOX EOY EPH EQAW EUV EUVF FFST FMN GDDM GIM GLD GSK HCM IBMZ ICA ICQ IDI ILM IMO IMW ING IOA IOE ISE LSP MSOPS			

通常は30日毎など定期的にパスワード変更がされるようなシステム設定が推奨されています。

緊急時使用のためのユーザーやログオン・ユーザーでないプログラムが使用するユーザーに対してパスワード期限を設定しないケースがありますが、パスワード・クラックの可能性は期限のあるユーザーに比して非常に大きくなります。このためリストされたユーザーに対する設定の必要性確認・監視が非常に重要な監査ポイントとなります。

全資源へのアクセス状況概要

Consul zSecure data set events 20Apr07 08:00 to 20Apr07 21:25 page 1
 SMF records for all data sets

Dataset	User	Jobname	Job id	Sys	Date	Start	End Date	Time	Sys	Description
@FTPV2.TSO210.LOAD						0:31:33	16:37:43			
	KAIHO	KAIHO	TSU05987	SYS1	20Apr2007	10:31:33	10:31:33			
						20 Apr 2007 10:31	SYS1 KAIHO			Input activity for concatenation starting with @FTPV2.TSO210.LOAD
	KAIHO	KAIHO	TSU06036	SYS1	20Apr2007	16:04:44	16:04:44			
						20 Apr 2007 16:04	SYS1 KAIHO			Input activity for concatenation starting with @FTPV2.TSO210.LOAD
	KAIHO	KAIHO	TSU06040	SYS1	20Apr2007	16:15:52	16:15:52			
						20 Apr 2007 16:15	SYS1 KAIHO			Input activity for concatenation starting with @FTPV2.TSO210.LOAD
	KAIHO	KAIHO	TSU06060	SYS1	20Apr2007	16:37:43	16:37:43			
						20 Apr 2007 16:37	SYS1 KAIHO			Input activity for concatenation starting with @FTPV2.TSO210.LOAD
CATRP.CAT0641.ISPPLIB						13:49:33	17:58:57			
	NAKAMUR	NAKAMUR	TSU06016	SYS1	20Apr2007	13:49:33	17:58:57			
						20 Apr 2007 13:49	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.ISPPLIB
						20 Apr 2007 13:49	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.ISPPLIB
						20 Apr 2007 13:49	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.ISPPLIB
CATRP.CAT0641.LOAD						13:48:08	17:58:57			
	NAKAMUR	CATBKUP	JOB06016	SYS1	20Apr2007	14:58:13	14:58:13			
						20 Apr 2007 14:58	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.LOAD
						20 Apr 2007 14:58	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.LOAD
	NAKAMUR	CATBKUP	JOB06019	SYS1	20Apr2007	15:11:25	15:11:25			
						20 Apr 2007 15:11	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.LOAD
						20 Apr 2007 15:11	SYS1 NAKAMUR			Input activity for non-VSAM data set CATRP.CAT0641.LOAD

ユーザーのアクティビティをレポートします。

各ユーザーが許された範囲の必要な作業を実施していることを証明すると共に万が一の場合に違反状況を追求できます。

全資源へのアクセス状況概要

SMF RECORD LISTING 20Apr07 08:00 to 22Apr07 18:12

page 1

Consul zAudit user defined SMF report

Jobname	User	Count	Date	Time	Typ	SubTp	User	Jobname	Description
FAUDITDE	NAKAMUR	5							
			20 Apr 2007	14:07 20			NAKAMUR	FAUDITDE	Start of job FAUDITDE for user NAKAMUR
			20 Apr 2007	14:07 30	1		NAKAMUR	FAUDITDE	Start of job FAUDITDE (JOB06011) for user NAKAMUR
			20 Apr 2007	14:17 14			NAKAMUR	FAUDITDE	NAKAMUR Input activity for non-VSAM data set FASTAUD.MFA0901.LOAD
			20 Apr 2007	14:17 30	4		NAKAMUR	FAUDITDE	Totals for step STEP00 of job FAUDITDE for user NAKAMUR code S222
			20 Apr 2007	14:17 30	5		NAKAMUR	FAUDITDE	End of job FAUDITDE (JOB06011) for user NAKAMUR code S222
FAUDITMC	NAKAMUR	14							
			20 Apr 2007	14:05 20			NAKAMUR	FAUDITMC	Start of job FAUDITMC for user NAKAMUR
			20 Apr 2007	14:05 30	1		NAKAMUR	FAUDITMC	Start of job FAUDITMC (JOB06009) for user NAKAMUR
			20 Apr 2007	14:05 14			NAKAMUR	FAUDITMC	NAKAMUR Input activity for non-VSAM data set FASTAUD.MFA0901.LOAD
			20 Apr 2007	14:05 30			NAKAMUR	FAUDITMC	NAKAMUR Input activity for non-VSAM data set FASTAUD.MFA0901.PARMLIB
			20 Apr 2007	14:05 30			NAKAMUR	FAUDITMC	Totals for step STEP00 of job FAUDITMC for user NAKAMUR code RC0
			20 Apr 2007	14:05 30	4		NAKAMUR	FAUDITMC	Totals for step STEP01 of job FAUDITMC for user NAKAMUR code RC0
			20 Apr 2007	14:18 15			NAKAMUR	FAUDITMC	NAKAMUR Output activity for non-VSAM data set FASTAUD.MFA0901.FAUDIT.UCAT1
			20 Apr 2007	14:18 14			NAKAMUR	FAUDITMC	NAKAMUR Input activity for non-VSAM data set FASTAUD.MFA0901.LOAD
			20 Apr 2007	14:18 14			NAKAMUR	FAUDITMC	NAKAMUR Input activity for non-VSAM data set SYS07110.T140529.RA000.FAUDITMC.MCAT1.H01
			20 Apr 2007	14:18 30	4		NAKAMUR	FAUDITMC	Totals for step STEP02 of job FAUDITMC for user NAKAMUR code S222-0F
			20 Apr 2007	14:18 30	5		NAKAMUR	FAUDITMC	End of job FAUDITMC (JOB06009) for user NAKAMUR code S222
IBMUSER		1							
			20 Apr 2007	13:43 26			IBMUSER	JES2	purge of job IBMUSER (TSU05717)
WS82DST		696							
			20 Apr 2007	08:55 41	1		WS82DST	DIV	ACCESS
			20 Apr 2007	08:55 41	2		WS82DST	DIV	UNACCESS
			20 Apr 2007	08:55 41	1		WS82DST	DIV	ACCESS

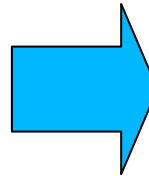
各ジョブ名毎に、どのユーザーがいつ、そのジョブを使用してどのファイルにアクセスしたかをレポートしています。

(ご参考)Tivoli zSecure 1.9.1 最新リリース情報

- Tivoli zSecure リリース変遷
 - ▶ Tivoli zSecure スイート V1.8.1 - 2007.7 発表、使用可能
 - ▶ Tivoli zSecure スイート V1.9.0 - 2007.12 発表、使用可能
 - Tivoli zSecure スイートV1.9.1 - 2008.3 使用可能
- Tivoli zSecure V1.9.1 拡張機能
 - ▶ IBM Tivoli zSecure Admin 製品の一機能としてRACF Offline 機能を追加
- RACF Offline 機能とは

お客様の要望

- 本番適用前にあらかじめRACFコマンドをテストしたい
- さまざまなシナリオをクイックにテストしたい
- RACF定義の構成変更およびクリーンアップが意図通りに実施できるかの確認をしたい
- RACF管理者のためのテスト環境を提供して欲しい

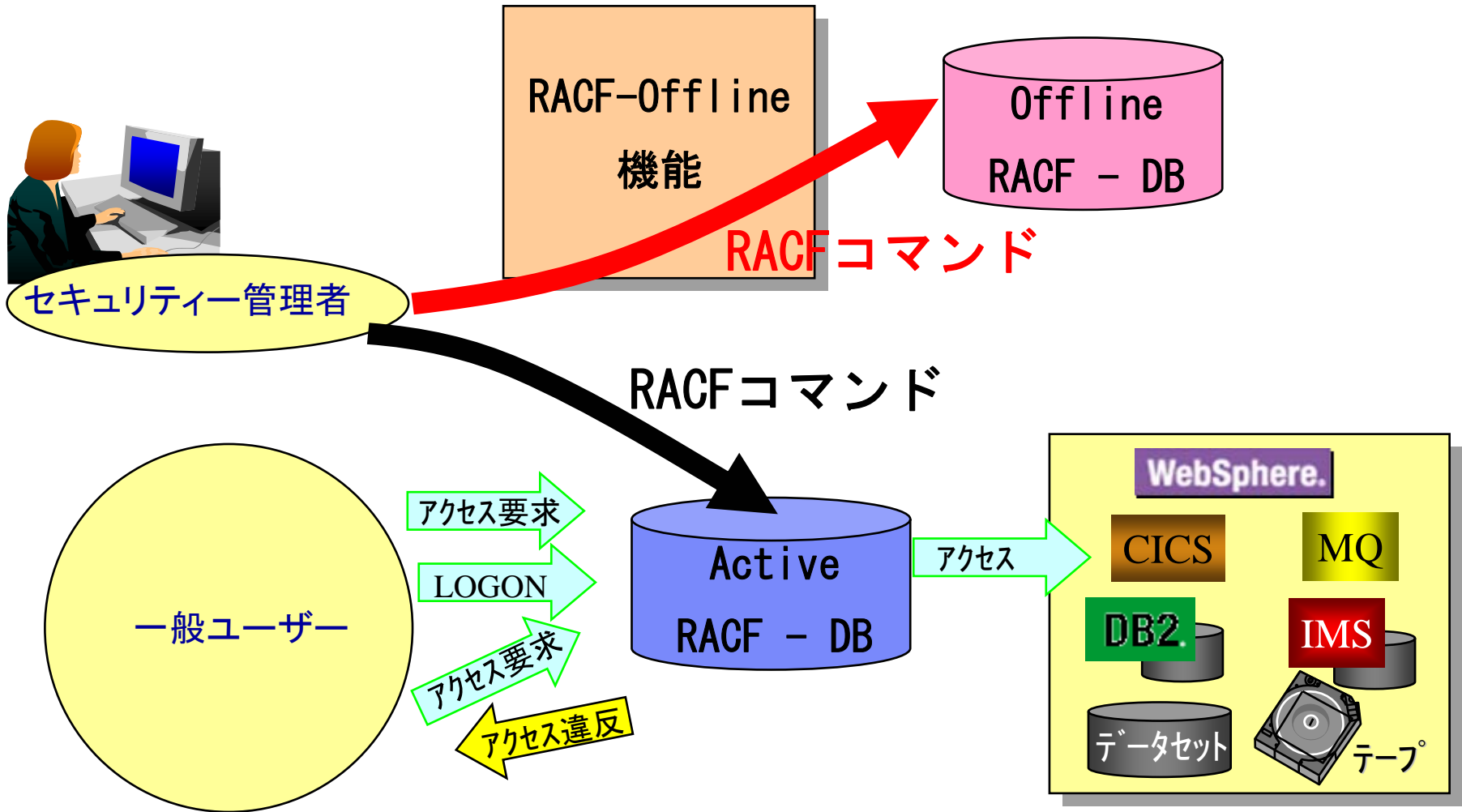


RACF Offline による実現機能

- 非活動のRACF環境に対するRACFコマンド実行
- 活動/非活動環境間の容易な切り替え
- 複数RACF環境に対する同様のシナリオテスト再生機能を提供



RACF Offline 環境



RACF Offline 使用法の例

■ RACFデータベースのマージ

- ▶ マージ・ルールのデザイン
- ▶ zSecure Admin Merge機能によりコマンドを生成
- ▶ RACF-Offline経由でコマンドを実行
- ▶ 結果のプロファイル进行分析
- ▶ マージ・ルールの見直し、修正

■ プロファイル再構成

- ▶ 存在するプロファイル进行分析
- ▶ プロファイルの追加/削除のコマンド組み立て
- ▶ RACF-Offline経由でコマンドを実行
- ▶ zSecure Adminをとおして結果プロファイル进行分析
- ▶ コマンドの見直し、修正



ありがとうございました。

