Tivoli software

IBM

- IBM Tivoli Security Management for z/OS でより堅牢に -
z/OS RACF 環境におけるセキュリティー / コンプライアンス管理

メインフレーム・セキュリティーを管理する
一方で管理にかかる時間、労力、コストを削減

監査およびコンプライアンスの
取り組みのシームレスな統合を
活用

メインフレーム・セキュリティー
を強化する一方で複雑さを軽減

Axel Buecker
Michael Cairns

Redpaper

ibm.com/redbooks

International Technical Support Organization

- IBM Tivoli Security Management for z/OS でより堅牢に -

z/OS RACF 環境におけるセキュリティー / コンプライアンス管理

SG88-4059-00

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、v 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。

第 1 刷 2011.3

本書は、IBM Tivoli Security Management for z/OS V1.11 オファリング (製品番号 5698-B43) に適用されます。

目次

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。
〒242-8502 神奈川県大和市下鶴間1623 番14 号日本アイ・ビー・エム株式会社
法務・知的財産知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が 禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾 :

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. 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。

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

CICS®	Redbooks®	Tivoli®
DB2®	Redpaper™	z/OS®
IBM®	Redbooks (logo)  ®	
RACF®	System z®	

以下の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

Microsoft、Windows 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。

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。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

前書き

どの組織にも、保護が必要な、中核となる一連の基幹業務データがあります。セキュリティーが失効したりセキュリティーに障害が発生したりすると、単に混乱を招くだけではなく、壊滅的な事態を引き起こすおそれがあり、その結果は企業全体に影響します。特権ユーザーの不注意なミスだけでも、意図しない構成エラーや不注意なセキュリティー・コマンドによって多額の損害をもたらすことがあります。悪意のあるユーザーがアクセス権限を持つと、さらに大きな損害を招くことがあります。このため、セキュリティー管理は企業の機密データを適切に保護する上で大きな課題に直面します。さらに、IT スタッフは、ますます増える要求に時間を取られながらも、詳細な監査および管理文書の提出を要求されます。

セキュリティーおよびコンプライアンスのプロセスを自動化し、簡素化することにより、これらの課題に対処し、効果的で持続可能なユーザー管理ソリューションおよび監査ソリューションを確立することができます。これには、セキュリティー・データベースのクリーンアップ、構成および設定の反復可能な監査、および変更とイベントの能動的モニタリングが含まれます。IBM Tivoli Security Management for z/OS V1.11 は、これらのソリューションを提供して、自動化された監査および管理を通じてメインフレーム・システムのセキュリティー強化を支援します。

この IBM Redpaper 文書では、Tivoli Security Management for z/OS によって、z/OS、RACF、および DB2 から得たメインフレーム・セキュリティーの情報を企業の監査とコンプライアンスのソリューションに送る仕組みを説明するとともに、z/OS、RACF、および DB2 から得たメインフレーム・データを他のオペレーティング・システム、アプリケーション、およびデータベースのデータと結合して、包括的なログ・データを取得し、先進的なログ分析を通じてそのデータを解釈し、その結果を企業全体の監査およびコンプライアンスに関するレポート作成のために効率的かつ合理的に伝達する方法を説明します。

本書の執筆に携わったチームについて

本書は、International Technical Support Organization Austin Center に世界各地から参加しているスペシャリストのチームによって作成されました。

Axel Buecker は、International Technical Support Organization Austin Center の認定コンサルティング・ソフトウェア IT スペシャリストです。ソフトウェア・セキュリティー・アーキテクチャーおよびネットワーク・コンピューティング・テクノロジーの分野について、幅広く執筆し、世界中の IBM クラスで教えています。Axel Buecker はドイツのブレーメン大学でコンピューター・サイエンスの学位を取得しています。ワークステーション、システム管理、ネットワーク・コンピューティング、および e- ビジネス・ソリューション関連のさまざまな分野において、23 年の経験があります。2000 年 3 月に ITSO に加わる前は、ソフトウェア・セキュリティー・アーキテクチャーのシニア IT スペシャリストとしてドイツ IBM に勤務していました。

Michael Cairns は、IBM Tivoli ANZ のテクニカル・セールス・スペシャリストです。1986 年以降、オーストラリア、ニュージーランド、および英国で、IBM メインフレームを導入している大小さまざまな企業に勤務してきました。2007 年、メインフレーム・セキュリティー管理製品 zSecure Suite の獲得をきっかけに IBM に加わりました。z/OS セキュリティーを専門とし、特に RACF Security Server と関連製品に精通しています。これまでに、アプリケーション開発、システム・プログラミング、キャパシティーおよびパフォーマンス管理、セキュリティー・アーキテクチャーなどに携わってきました。現在は、アジア太平洋地域でメインフレーム・セキュリティーの教育と指導を行っているほか、IBM Systems

Magazine のテクニカル・エディターとして、z/OS の管理とセキュリティーに関する記事を定期的に執筆しています。

このプロジェクトにご協力いただいた以下の方々に感謝します。

Alison Chandler
International Technical Support Organization Poughkeepsie Center

Glinda Cummings、Rob Weiss
IBM

執筆にご協力ください

スキルを生かしてキャリアを伸ばし、それと同時に執筆に協力できる機会がここにあります。ITSO の実習プログラムに参加しませんか。ご自分の専門分野に関する資料の作成を手伝いながら、最先端のテクノロジーを実地に体験することができます。技術担当者や関係者との人脈を開拓しながら、製品をお客様にとってより使いやすいものにして、お客様の満足度を向上させるために協力してください。実習期間は 2 週間から 6 週間で、直接参加することも、ご自宅からリモート実習生として参加することもできます。

実習プログラムについて詳しくは、次の URL で実習に関する索引を参照して、オンラインで申し込んでください。

ibm.com/redbooks/residencies.html

ご意見をお寄せください

以下は英語のみの対応となります。皆様の貴重なご意見をお寄せください。

IBM では、本書ができる限り皆様のお役に立つものになるように努力しています。本書または他の Redbooks についてのご意見を以下のいずれかの方法でお寄せください。

- 以下の URL からオンラインの「**お問い合わせ (Contact us)**」レビュー・フォームを使用する。

  ibm.com/redbooks

- 以下の宛先にインターネット・メモで送信する。

  redbook@us.ibm.com

- 以下の住所に郵送する。

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

IBM Redbooks 関連情報

- Facebook で探す。

  http://www.facebook.com/IBMRedbooks

- Twitter でフォローする。

  http://twitter.com/ibmredbooks

- LinkedIn で探す。
  http://www.linkedin.com/groups?home=&gid=2130806
- IBM Redbooks の週刊ニュースレターで新しい Redbooks 資料、実習、ワークショップを調べる。
  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- RSS フィードで最近の Redbooks 資料に関する最新情報を入手する。
  http://www.redbooks.ibm.com/rss.html

1

IBM Tivoli Security Management for z/OS

この章では、IBM Tivoli Security Management for z/OS ソリューションについて概説し、この製品に含まれている個々のコンポーネントを簡単に紹介します。その次に、このソリューションで実現できる具体的なメリットおよび ROI に関する報告をいくつか取り上げます。

15 ページの『第 2 章 お客様シナリオ』では、このオファリングを構成する個々の技術的ソリューションの結合性を示すために、3 つのお客様シナリオを使用します。

1.1 ソリューションの概要

IBM Tivoli Security Management for z/OS V1.11 は、ブラウザー・ベースの監査インターフェース、自動化された XML でのレポート作成とアラート生成、および直観的なユーザー・インターフェースを使用して、メインフレームの新たな側面を提示します。この製品により、組織は、難しさを増す z/OS ベースの IT セキュリティーの課題にさらに効率よく対処して、より多くのリソースを現実のセキュリティー向上プロジェクトに投入できるようになります。同時にこの製品は、z/OS 管理者がシステムの IT セキュリティー・プロファイルを改善するための作業プランも提供します。

IBM System z を使用する組織では、通常、IT セキュリティーが全体的に重視され、IT 部門の総費用から多額の予算が割り当てられます。ところが、メインフレームはこのセキュリティー予算であまりにも軽視されています。つまり、*声を上げないとなかなか予算が付きません*。分散システムは、そのセキュリティーのぜい弱性が毎日、毎週、毎月のように明らかとなるため、常に IT セキュリティー予算の最大部分を占める傾向にあります。また、メインフレームは*設計上セキュアである*という一般認識があり、それはある程度事実です。確かに、最新の System z ハードウェアを組み合わせた z/OS 環境は、世界で最も「セキュリティーが確保された」商用コンピューティング・システムと言えます。ところが、多くの商用インストール済み環境では、重大な機密漏れが、多くの場合は認識も軽減もされずに存在していることがわかっています。Tivoli Security Management for z/OS ソリューション・バンドルの存在理由は、ここにあります。経験の浅いメインフレーム管理者でも、このソリューションを使用することで、全世界にいるピア・グループ・リーダーのスキルや知識を活用し、System z 環境を最小限の手間、時間投資、およびリスクで適切に保護できるようになります。

最新のブラウザー・インターフェースの下にある Tivoli Security Management for z/OS の原動力は、20 年以上にわたってメインフレーム・セキュリティー構成のベスト・プラクティスを蓄積したデータベースおよびこれと併用するカスタムの照会エンジン (*CARLa* プログラミング言語) です。この照会エンジンは、z/OS 環境であらゆる種類のセキュリティー関連データを処理するために特別に設計されたものです。z/OS セキュリティーの管理者、監査員、マネージャー、またはその他関係者によるこれらのツールの使用効果は、全世界にいる z/OS セキュリティーのエキスパートの知識によって高められ、組織の全体的なセキュリティー体制およびリスク管理コンプライアンスの要件に役立ちます。

IBM Tivoli Security Management for z/OS V1.11 には以下の機能があります。

- セキュリティー要件およびセキュリティー・ポリシーへのコンプライアンスを促進
- 監査およびコンプライアンス管理への取り組みに対する企業全体の視点とのシームレスな統合を活用
- 機密漏れの検出と防止、およびリスクの最小化を支援するために、インシデントのモニターおよび監査を実施
- 日常的な管理用タスクを自動化して、コストと複雑さを軽減するとともに、生産性と効率の向上を図る
- 仮想サーバーを含めた、集中サーバー管理の保全性を包含
- RACF でプロアクティブにポリシー・コンプライアンスを実施し、不適合なセキュリティー・コマンドが実行されないようにして、RACF データベースの汚染を低減
- RACF コマンド・アクセス権限の選択的な配布、処理前に行う RACF セキュリティー・コマンド検査、および監査証跡によるセキュリティー・コマンド情報の検索を可能にすることにより、特権コマンドの乱用およびエラーの防止を支援

Tivoli Security Management for z/OS ソリューション・バンドルで提供されているソフトウェアの組み合わせは、連携して包括的な z/OS セキュリティーを実現する統合スイートで

す。以下の各セクションでは、このスイートのコンポーネントで対応される、z/OS セキュリティーおよび管理に関する一般的なトピックについて説明します。

1.1.1 監査およびセキュリティー・アクティビティーのレポート作成

z/OS セキュリティーで従来使用されているレポート作成ツールは、使いづらく、解釈も容易ではありません。Tivoli Security Management for z/OS は、RACF 管理および監査レポート作成のための直観的な ISPF[1] ベースのインターフェースを提供するとともに、監査とコンプライアンスのレポート作成および準リアルタイムのセキュリティー・イベント・アラート生成のための Web ブラウザー・ベースのインターフェースを提供します。真にリアルタイムのセキュリティー・イベント・アラートを生成する必要がある場合は、IBM Tivoli zSecure Suite の追加のコンポーネントで対応できます。

Tivoli Security Management for z/OS ソリューション・バンドルの ISPF ベースのコンポーネントには、数百種類の監査レポートと、一般的な RACF タスクを実行するために必要な多数の管理ツールが用意されています。さらにこれらのツールでは、通常はシステム・プログラマーの領域であるためにほとんどのセキュリティー管理者は意識することがない z/OS 構成データが、詳細に可視化されます。z/OS 構成のエラーは、z/OS セキュリティーの侵害につながる最も一般的な*バック・ドア*であるため、この情報に容易にアクセスできることは重要です。

これらのツールでは、実証された業界のベスト・プラクティスと現在の構成を比較することができ、経験の浅い管理者に RACF および z/OS の構成を改善するためのロードマップを提供します。この比較は変更トラッキング機能としても使用できます。これにより、容認された*セキュリティー・ベースライン*を現在のセキュリティー設定と比較し、セキュリティー関連の変更が見逃されたり、組織の変更制御機能を迂回できたりすることがないようにします。

1.1.2 セキュリティー・イベントのアラート生成

現在、ほとんどの組織が IBM 製の重要な分散プラットフォームで侵入防御ソフトウェア (IPS) を実行していますが、z/OS で同じ基準が採用されている例はほとんどありません。

それはなぜでしょうか。

ほとんどの場合、組織は、z/OS とそのサブシステム用に IPS またはその他のセキュリティー・イベント駆動型のレポート作成機能が提供されていることを知らないと答えています。Tivoli Security Management for z/OS ソリューション・バンドルでは、IBM Tivoli Security Information and Event Manager というツールでこれらの機能を提供しています。

このツールでは、さまざまなシステム・リソースへのアクセスを監査できるほか、機密リソースの使用または高い権限を持つスタッフによるアクセスに対してアラートを生成し、業界の規制やその他のガイドラインとアクセス・パターンを比較することができます。Tivoli Security Information and Event Manager で生成されるレポートは Web ブラウザー・ベースであり、PDF、Microsoft Excel などの複数の共通フォーマットにエクスポートできます。何よりも Tivoli Security Information and Event Manager のレポートは、z/OS プラットフォームの専門知識がなくても実行して解釈することができます。

Tivoli Security Information and Event Manager は、300 種類を超える IT プラットフォーム、データベース、およびアプリケーションで生成された監査ログからレポートを作成できる汎用監査ツールです。Tivoli Security Information and Event Manager は、カスタム・アプリケーション・ログの処理にも対応できます。

---

[1] *ISPF* (Interactive System Productivity Facility) は、従来のメインフレーム・システム・インターフェースです。

Tivoli Security Information and Event Manager の包括的な説明については、IBM Redbooks 資料「*IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*」(SG24-7530) を参照してください。

1.1.3 きめ細かいコマンド制御

実質的にすべてのシステム管理者がプラットフォームの種類に関係なく共有する経験があります。これは、ユーモアを込めて *Oh-No! Moment* (しまった、と思う瞬間) と呼ばれています。「Oh-No! Moment」の定義は、機密性が高いシステム・コマンドに対して *Enter* キーを押した瞬間にプロセスの重要なステップを飛ばしたことに気付き、稼働中のシステムに修復不能な被害を与えた可能性があることがわかったときの胃が痛むような気分です。

経験を積んだ IT 管理者は、誰もが過去の仕事で「Oh-No! Moment」を経験しています。これは、IT システムでの変化の速さと、このような機密性の高い環境で作業することの重圧が招いた結果であり、避けることはほとんど不可能です。Tivoli Security Management for z/OS には、誤って入力された RACF およびセキュリティーに関連する変更を原因とする機能停止や損害、あるいはこのような変更に伴うリスクを軽減し、場合によっては解消できるようにする機能があります。

IBM Tivoli zSecure Command Verifier は、機密性の高い RACF コマンドへのアクセスを追加で分離できるようにする RACF の拡張機能です。適切にデプロイされた Tivoli zSecure Command Verifier は、システムの可用性や機能性を脅かす最も一般的な RACF コマンド・エラーの防止に役立ちます。さらにこの製品では、サイトで定義されたカスタムの命名規則およびその他の基本的な RACF 構成基準を施行することによって、RACF プロセスを標準化できます。

時として、稼働中のシステムで RACF 制御を操作することは、弾の入った銃を携行するのと同じように、必要時には非常に役立ちますが、潜在的にかなり危険です。Tivoli zSecure Command Verifier は、ユーザーが自らに損害をもたらすことを防ぎ、同時に組織の重要なインフラストラクチャーが潜在的に損害を受けることを防ぎます。

1.1.4 効率的なセキュリティー管理

RACF ユーザー ID の管理 (RACF ユーザー ID の作成や削除など) に関して業界で報告された一般的統計によると、比較的単純であるはずのタスクに 30 分から 1 時間以上の時間がかかっています。

なぜそんなに時間がかかるのでしょうか。

RACF でユーザー ID を作成するには、複数のステップが必要です。これらのステップは正しい順序で実行する必要があり、多くの場合、潜在的な新規ユーザーのアクセス要件を事前に調査することが求められます。新規のユーザーが、すべてのアクセスが正しく定義されるまで、追加支援やユーザー ID 定義の変更を複数回要求することは珍しくありません。これは、システム・セキュリティー管理者側にスキルが不足しているためではなく、大規模な z/OS ベースの環境ですべての設定を正しく行うことが技術的に複雑であるためです。

z/OS RACF のセキュリティー管理者は、ユーザー ID の準備以外にも多くのタスクを実行しなければなりません。そのタスクの多くは、この例で示すものに比べてはるかに複雑であり、重要なシステム・リソースおよびサブシステムの保護が必要となることもあります。これらのタスクは、当然ながら 1 回で正しく実行する必要があります。そうしないと深刻な機密漏れがシステムで発生しかねません。

IBM Tivoli zSecure Admin for RACF を使用すると、多くのインストール済み環境で実証されたように、大半の RACF 管理アクティビティーの時間のかかる部分を大幅に削減できます。例えば、以前は 実行に 1 時間もかかっていた複雑なジョブが、以前の業務慣例と比較

すると、ほとんど 5 分未満で完了するようになったお客様もいます。システムで実行する RACF 関連作業がごく少量であっても、節約された時間はすぐに積み上げられます。

ただし、効率的なセキュリティー管理とは、単に共通の反復タスクにかかる時間が削減されることではありません。より困難で潜在的に危険なタスク、例えば古い定義をリスクなく安全にクリーンアップする作業などにかかる時間が増えることでもあります。Tivoli zSecure Admin の使い方を学んだ管理者は、何年も要求リストの受信箱にたまっていた多数のタスク、つまり z/OS セキュリティー体制を現実に強化するタスクに集中する時間を確保できるようになり、時間が経過しても何も改善できずにただ現状を維持することはなくなります。

1.1.5 セキュリティーおよび監査のベースラインの確立

Tivoli Security Management for z/OS ソリューション・バンドルに固有の特徴の 1 つは、ご使用のシステムを z/OS セキュリティーに関する業界のベスト・プラクティスと比較できる点です。この機能は、IBM Tivoli zSecure Audit で提供されています。多くの組織が、ほとんどの場合メインフレームの経験がない監査員から、z/OS システムが明確なベスト・プラクティス基準を満たしていることを証明する文書を要求されています。Tivoli zSecure Audit では、20 年以上にわたってセキュリティーの構成ミスや潜在的なぜい弱性を蓄積したデータベースを利用して、この機能を実現します。分析する実際のシステムは、米国国防総省が認めた IT セキュリティー評価基準の一部である B1、C1、および C2 と比較できるほか、20 年にわたって開発され、かつ IBM が多くのお客様のデプロイメントで確かめた一般に容認されている商用 (軍事用ではない) のベスト・プラクティスに基づく準 *zSecure 基準* とも比較することができます。

これにより、システムが堅牢に保護されているかを確認し、そうでなければ、望ましいセキュリティー・レベルを実現するためにどのような変更が必要かを把握することができます。さらに、Tivoli zSecure Audit のレポートを定期的に使用して、ご使用のシステムを自社で認めたベスト・プラクティス基準と比較し、通常のシステム変更およびシステム保守によって経時的に逸脱が生じていないかを確認できます。

1.1.6 冗長なセキュリティー定義の自動クリーンアップ

Tivoli Security Management for z/OS は、すべての RACF 定義の使用状況を分析する自動ツールを提供し、(指定された期間に使用されていなかったことで) 冗長と判断された定義を除去するために必要な RACF コマンドを生成するためのレポートを配信します。お客様からは、ユーザー・アクティビティーとシステム・アクティビティーのビジネス・サイクル全体を分析した後に、データベース内の定義の最大 50% が除去されたという報告を受けています。

セキュリティー・データベース内の使用されていない定義が攻撃の手段となっていることは、IT セキュリティーで一般に認識されています。特に該当するのはユーザー ID 定義ですが、他の RACF リソースおよびグループの場合も同様です。z/OS RACF 環境では、アプリケーションを破棄した後、データを再構築した後、または他の命名規則を変更した後に、使用されていないリソースのクリーンアップが行われることはまずありません。これは、z/OS 環境の重要な特徴であるシステム全体の安定性と可用性が変化することによる固有のリスクがあるためです。しかし、IBM Tivoli zSecure Admin のアクセス・モニター機能とクリーンアップ機能によって、システムが潜在的なリスクとして抱えている残存した定義項目を、有害な副作用を心配することなく安全に取り除くことができるようになりました。

1.1.7 機密特権および機密権限の分離

z/OS RACF 環境のシステム管理者には、UNIX の *root* ユーザーと同様に、*システム全体の鍵* が与えられます。適切な監査ツールが提供されていても、システムのダウンや損傷が発生する事態や、競争上有利なビジネス・データやその他の機密ビジネス・データが公開さ

れたり競合他社の手に渡ったりする事態が発生すると、それらのツールはほとんど役に立たなくなります。

簡単に言うと、問題はシステム管理者を*信頼*するかどうかではなく、各個人にどの程度の信頼レベルを割り当てるかということです。z/OS システム上の全データへのアクセスを 1 人のユーザーに許可することは、決してよい方法ではありません。IT セキュリティー原則 101 *最小特権の原則*では、システム管理者であっても、日常業務の遂行に必要なアクセス権限と特権のみを付与するように推奨しています。この原則に従わないと、内部の不正行為またはそれ以上に深刻な事態を招きます。

残念なことに、既存のインストール済み環境の多くはこの原則に従っていません。RACF 管理特権が、実際に必要な範囲よりもはるかに広いユーザー・コミュニティーに割り当てられており、それによる既存の IT システムへのリスクは多くの場合、過小評価されています。Tivoli Security Management for z/OS のコンポーネントである Tivoli zSecure Command Verifier では、機密性の高い RACF コマンドの使用を異なる管理者セットの間で分けることができます。さらに、管理者を異なる機能グループに分けて、必要なワークフローおよび第 2、第 3 のレベルの権限を割り当てることで、機密性の高いデータのセキュリティーが一個人によって侵害されるのを未然に防止できます。

この分離アプローチは、セキュリティー特権を必要以上に広範囲のユーザーに割り当てることの固有のリスクの軽減策と考えることができます。一度割り当てた特権を実際に取り消すことは、多くは政治的な理由から、かなり困難です。ユーザーからは苦情が上がり、経営陣も巻き込むことになります。さらに IT セキュリティー管理者は、何か*問題*が起きる前に、自らのアクションを正当化する必要に迫られます。Tivoli zSecure Command Verifier では、これらのスタッフの特権を維持しながら、スタッフが意図的あるいは偶発的にデータに損害を与えたり別の方法でアクセスしたりする可能性を大幅に軽減できます。さらに、このユーザー・コミュニティーによる特権使用のモニタリングと監査を設定して、その特権を*ジョブの実行に最低限必要な*ものへと徐々に縮小することができます。これは、一般的なセキュリティー上の問題に対する安全かつ政治的に受け入れられるアプローチです。

1.1.8 トラステッド・ユーザーの特定

Tivoli Security Management for z/OS では、一般に*トラステッド・ユーザー*と呼ばれるユーザーを固有の視点で捉えています。つまり、トラステッド・ユーザーを、あらゆる手段を通じて z/OS 環境の運用に損害やその他の破壊をもたらすおそれのある人員と定義しています。トラステッド・ユーザー・レポートは、*分離*や*最小特権*といった課題への対応が十分であることを確認するために不可欠です。誰がトラステッド・ユーザーであるかを把握しない限り、信頼の範囲を必要最小限まで縮小するという課題に取り組むことはできません。

Tivoli zSecure Audit で信頼分析レポートを実行すると、重大度の高い順に、信頼しているユーザーおよびそのユーザーがアクセスできる RACF リソース (実質的な信頼状況を示す) が表示されます。さらに、監査関連の結果には、検出されたすべての信頼状況がわかりやすく記述されるので、非技術系の監査員でも各信頼ベクトルに伴うリスクを適切に評価することができます。

Tivoli zSecure Audit の信頼分析は、さまざまな視点から行われます (例えば、*社内のトラステッド・ユーザーは誰か*、あるいは*トラステッド・ユーザーによってセキュリティーを侵害される可能性があるリソースは何か*など)。本質的に同じ問題に関してこの 2 つの代表的な質問を与えることで、最小人数のスタッフで影響を最小限に抑えながら最大限のセキュリティーを確保できるポイントが相対的に明らかとなります。この機能により、信頼の問題に対して自動的な 80/20 規則のアプローチを取ることができます。つまり、システム上のリソース定義またはユーザー ID の 20% を変更するだけで、80% の改善を容易に実現できます。この 20% の内容を見極めるのは常に困難な作業でした。今後は、この作

業を Tivoli zSecure Audit に任せて、z/OS 環境を最小限の影響と労力で実際に保護するという重要な作業に取り組むことができます。

外部資料 : IBM Tivoli Security Management for z/OS V1.11 製品スイートについて詳しくは、以下の資料を参照してください。

Tivoli zSecure Suite Version 1.11 インフォメーション・センター

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/welcome.html

Tivoli zSecure Suite の詳細情報は以下のサイトでも入手できます。

http://www.ibm.com/software/tivoli/products/zsecure/

Tivoli Security Information and Event Manager V2.0 インフォメーション・センター

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tsiem.doc/welcome.html

Tivoli Security Information and Event Manager の詳細情報は以下のサイトでも入手できます。

http://www.ibm.com/software/tivoli/products/security-info-event-mgr/index.html

1.2 IBM Tivoli Security Management for z/OS のコンポーネント

Tivoli Security Management for z/OS V1.11 は、セキュリティー管理機能を提供し、RACF と密接に統合して、メインフレーム上でのコンプライアンス管理、セキュリティー管理、ユーザー管理、およびセキュリティー・モニタリングを可能にします。Tivoli Security Management for z/OS V1.11 は、以下の製品で構成されています。

- IBM Tivoli zSecure Admin
- IBM Tivoli zSecure Audit
- IBM Tivoli zSecure Command Verifier
- IBM Tivoli Security Information and Event Manager
- IBM Tivoli Compliance Insight Manager Enabler for z/OS のコンポーネント :
  - IBM Tivoli Compliance Insight Manager Enabler for z/OS - RACF
  - IBM Tivoli Compliance Insight Manager Enabler for z/OS - DB2
  - IBM Tivoli Compliance Insight Manager Enabler for z/OS - CICSÆ

以下のセクションでは、これらの製品について概説します。

1.2.1 IBM Tivoli zSecure Admin

Tivoli zSecure Admin は、z/OS に対する従来の (ISPF ベースの) ユーザー・インターフェースにおける RACF の新たな側面です。この製品は、RACF の*ユーザー ID*、*グループ*、*データ・セット*、および*一般リソース*を、さまざまなメインメニュー項目から検索、ソート、スクロール (上下左右) が可能な表形式で表示できるようになっているため、RACF 管理者はその経験の長さにかかわらず直観的かつ簡単に使用できます。

各メインメニュー項目からは、ほぼ同じ画面が表示されます。画面には、オプションのフィルター、選択基準、およびさらに詳細なリソース固有の項目が表示され、管理者が作業に必

要なプロファイルや定義に簡単にドリルダウンして、特定のタスクを実行できるようになっています。特定のリソース (ユーザー ID、グループ、データ・セット、または一般リソース) を選択すると、そのリソースのすべての関連情報を含んだスクロール可能な画面が表示されます。この画面では、各種フィールドの平易な説明のほか、リソース属性の意味および用途を説明する包括的なコンテキスト依存のヘルプ画面を表示することができます。Tivoli zSecure Audit が併せてインストールされている場合は、特定のリソースに対する具体的な監査結果も表示され、ユーザー・インターフェースからその結果に*ジャンプ*して、その結果が妥当である理由に関する詳細情報を Tivoli zSecure Audit から入手することができます。

一般的な RACF 管理用タスク (ユーザーの削除または定義、すべてのユーザー・アクセス権に関するレポート、SMF からのユーザー・アクティビティーに関するレポートなど) では、*基本コマンド*および*行コマンド*を使用することができます。すべてのレポートは、インラインの ISPF 表示またはバッチ・レポートとして生成するか、関係者に電子メールで即時に送信することができます。

前述したように、Tivoli zSecure Admin を使用して管理者の効率が向上することにより、エンド・ユーザーの業務成果が上がるだけでなく、管理者業務のセキュリティー成果も向上します。管理者はもはや手順を追うだけの作業員ではなく、z/OS を必要なセキュリティーで保護するために、より高いレベルで RACF 管理機能を実行する権限を与えられるようになりました。

1.2.2 IBM Tivoli zSecure Audit

z/OS セキュリティーの審査を受けるために、組織はどのくらいの頻度で外部のコンサルタントや監査員に多額の費用を支払っているのでしょうか。そして管理者はその審査の結果にどの程度満足しているのでしょうか。z/OS および RACF のセキュリティー実装の完全な技術的審査を実行できる有資格者も確かに存在しますが、人数がかなり少ないため、費用は高額です。z/OS 対応の監査プログラムを宣伝している代理店の多くは、インターネットや過去の (したがって最新でない) 資料から得た時代遅れのかなり単純な監査ガイドラインに従っています。*形式的な*監査で経営陣は z/OS セキュリティーに満足してしまいがちですが、技術スタッフは監査と自社のシステム構成の両方に重大な不備があることに気付いています。場合によっては、このような監査の後に、審査では見つからなかったセキュリティー・ホールが悪用されて、機密データがアクセスされ、システムのセキュリティーが侵害されることもあります。

Tivoli zSecure Audit は、自動化された*コンピューター内の監査員*として、20 年以上にわたる豊富な技術的監査の経験を組織に取り込み、いつでも必要なときに専門家の意見を仰ぐことができるようにして、このような問題に対応します。

Tivoli zSecure Audit をデプロイした組織は、*監査の準備ができた状態*になります。つまり、現在の監査状況に関する資料、改善のための推奨事項、および標準の定期監査レポートを、簡単かつエンド・ユーザーにわかりやすい方法で作成することができます。実際に、適切にデプロイされた Tivoli zSecure Audit は、監査員の仕事を年に一度ではなく毎日こなします。Tivoli zSecure Audit のユーザーは、定期的な監査を日次またはリアルタイムのセキュリティー・モニタリングに移行して、監査のベスト・プラクティスをグローバルに変化させています。

1.2.3 IBM Tivoli zSecure Command Verifier

前述したように、Tivoli zSecure Command Verifier は、ユーザーが不適切な RACF コマンドによって誤ってシステムに損害を与えることを防ぎます。また、RACF コマンド特権をきめ細かく分離できるようにするほか、Tivoli zSecure Admin とともにマルチレベルの許可プロセスを実装して、少なくとも一定レベルの同僚または経営陣の審査が行われるまではどのユーザーも機密コマンドを実行できないようにすることができます。これらの機能は、シス

テムの弾力性を強化するとともに、ユーザーが RACF 特権を制御された安全な方法で委任して受容可能なリスクを取ることができるようにします。

さらに Tivoli zSecure Command Verifier は、RACF 定義にいつ誰が変更を加えたかを把握できるようにする、コマンド監査証跡 (CAT) 機能と呼ばれる高度な監査証跡を提供します。法令遵守の目的で、RACF 管理者または監査員が、特定のコマンドがいつ誰によって実行されたかを特定するように要求されることがよくあります。この行為がどの程度前に行われたかによって、簡単な質問への答えを見つけるために SMF 監査証跡を何週間も検索することになる可能性があります。コマンド監査証跡が有効である場合、管理者が問題のプロファイルを調べると、Tivoli zSecure Command Verifier にそのプロファイルに対して行われた過去 64 件の変更がコマンドの実行者とともに表示されます。これにより、管理者は疑わしいコマンドに関して特定の SMF 日付範囲に直ちに狙いを付け、同じ時期に行われた可能性があるその他の関連アクティビティーを報告できるので、このような法令遵守に関する質問に素早く回答することができます。

Tivoli zSecure Command Verifier のもう 1 つの主要な機能は、RACF リソースの命名に関して組織で文書化されているガイドラインに従うために、命名規則と基準を施行できることです。これにより、データベースで間違った定義が作成されるのを防止できます。また、内部の慣行を文書化された基準に合わせることができるので、全体的なポリシー・コンプライアンス目標の実現に役立ちます。

1.2.4 IBM Tivoli Security Information and Event Manager

Tivoli Security Information and Event Manager は、クロスプラットフォームのログ管理と分析、監査、およびレポート作成を行うツールです。このツールでは、ポリシー違反を特定するために、セキュリティー・ポリシーに関して収集されたログ・データでレポートが生成されます。

Tivoli Security Information and Event Manager は、システム・ログ・レコードからわかった実際のエンド・ユーザーの行動を、Tivoli Security Information and Event Manager 管理コンソールで設定可能な望ましい行動と比較します。Tivoli Security Information and Event Manager は、ユーザーによる組織データへのアクセスと対話をモニターし、許容できる利用に関する定義を逸脱した場合にアラートを生成することができます。

Tivoli Security Information and Event Manager は、ユーザー・ベースおよびデータ・セットの分類に関して正規化されたメタデータを生成することで、この機能を実現します。このメタデータを収集して正規化する方法は、組織ごとに個別に定義できます。さらに、定義済みのユーザー・モデルおよびデータ分類モデルを利用することができます。これらのモデルは、多くの国で普及し、一部の業種では法的要件となりつつある複数の業界規制の枠組みから派生したものです。Tivoli Security Information and Event Manager では、サーベンス・オクスリー法 (SOX)、Health Insurance Portability and Accountability Act (HIPAA)、Payment Card Industry Data Security Standard (PCI DSS) などの法的規制に関するコンプライアンス・レポートの作成を、反復可能で調整可能なアクティビティーにすることができます。

Tivoli Security Information and Event Manager は、監査プロセスでループを閉じます。実際のユーザー行動 (ログ) を分析し、ポリシーからの逸脱を特定することで得た情報を基に、ポリシーを改善するか、あるいはセキュリティー実装をポリシーに合わせて修正し、望ましいユーザー行動からのさらなる逸脱を防ぐことができます。

これを実現するために、非技術系の監査員にも理解しやすい Web ブラウザー・ベースのレポート作成インターフェースが使用され、一般に要求される一連の標準監査レポートが提供されます。Tivoli Security Information and Event Manager は、z/OS SMF ベースの情報を処理できる一方で、300 種類を超えるアプリケーション、プラットフォーム、およびデータベースのログ情報を収集して管理することもできます。これらの異種データ・ソースを 1 つのレポート作成フレームワークに統合できることにより、ようやく組織は、何年にもわたっ

て生成し保管してきたあの厄介なシステム・ログから真の利益を得られるようになりました。

IBM Tivoli Compliance Insight Manager Enabler for z/OS

Tivoli Security Management for z/OS ソリューション・バンドルには、RACF、DB2、および CICS のデータを処理するために特別に構築された Tivoli Security Information and Event Manager のコンポーネントが含まれています。Tivoli Security Information and Event Manager は RACF、DB2、および CICS に対応しているため、Tivoli Security Information and Event Manager のメタデータや構成にはほとんど手間をかけることなく、ごく短い設定時間で有益なレポートを得ることができます。つまり、このツールは、システム上のどのユーザーが機密データに対する高いレベルの特権またはアクセス権限を持っているかを認識します。Tivoli Security Information and Event Manager では、ユーザーとデータの両方の基本的な分類が即座に実行されるので、デプロイメントへの投資に対してすぐに利益を得ることができます。

名前の混在 : このたび IBM Tivoli Security Information and Event Manager v2 が IBM Tivoli Compliance Insight Manager 製品の後継となりました。以前のバージョン用の既存のアドオンの一部には、Tivoli Compliance Insight Manager の名前がまだ使われています (例えば、このツールの場合は IBM Tivoli Compliance Insight Manager Enabler for z/OS)。ただし、これらは Tivoli Security Information and Event Manager と問題なく連動します。

1.3 具体的な利点と ROI

前述の各セクションでは、Tivoli Security Management for z/OS を利用することの直接的な利点をいくつか説明しました。それらの利点を以下に挙げておきます。

- 監査の準備ができた状態にするための時間および関連コストを削減します。
- 標準的なセキュリティー・アクティビティーの時間を短縮し、コンプライアンスを高めます。
- アラート生成とベースライン・セキュリティーの改善を組み合わせることで、セキュリティー・リスクを軽減します。
- 変更制御のトラッキングを強化して、変更に伴う可用性リスクを軽減します。
- 基本的な監査レポートを実行する際の、高度な専門知識を持つ (コストの高い) スタッフへの依存度を下げます。
- 誤った RACF コマンドを原因とする意図しない機能停止のリスクを軽減します。
- 高度なスキルを持つスタッフの労力を他にシフトできるようにすることで、セキュリティー体制を改善します。
- 国際的に承認されたセキュリティー・ベースラインの基準をシステムが満たしていることを確認することで、リスク管理を強化します。
- 冗長なセキュリティー定義を自動的に除去することで、機密漏れのリスクを軽減します。
- 高いレベルの特権を適切に分離することで、セキュリティー・リスクを軽減します。
- ユーザーが必要なアクセスを安全かつタイムリーに行えるようにすることで、セキュリティー・プロセスに対するユーザーの満足度を高めます。
- 定期的に行う詳細な技術的監査のために専門家を雇う必要性を減らします。
- セキュリティーの変更をタイムリーにレポートし、さらに最初に不要な変更が行われないようにするための機能を高めます。

- ログの収集と分析を集中化し、その効率的なアプローチによって付随的な利益を実現します。

これらの節減を ROI の観点から数量化することは、いまだに困難かつ間違いが起きやすいプロセスです。同じデータに常に複数の見方が存在するため、かなり異なる結論が出ることになります。このジレンマに対応するために、IBM は、IT コミュニティー全体を対象にベンダーに依存しないサービスとして明確に定義された投資収益率 (ROI) 分析を生成する独立系企業 Alinean Inc. と提携しています。

以下の各セクションでは、ビジネス・ドライバーおよび IT 運用に対する ROI の影響を確認します。ここでは、Alinean Inc. 提供のレポートからデータを引用しています。このレポートは、IT セキュリティーに関する代表的な業界標準のベスト・プラクティスを使用して実現できる、最小限の予想コスト削減値を示したものです。前に列挙した記載項目は、すべて IBM Tivoli Security Management for z/OS ソリューション・バンドルを採用することで実現でき、その多くはここで示すレポートの抜粋の中で明確に数量化されています。

パートナーについて : Alinean Inc. (http://www.alinean.com/) は、オンデマンドの販売ツールおよび関連サービスの主要プロバイダーです。IBM は Alinean と提携して、ビジネス価値と投資収益率に的を絞って IBM ソリューションを財務的に正当化するための支援を行う IBM Business Value Analyst を開発しました。Business Value Analyst は、Extreme Leverage および Tivoli Knowledge Center の「IBM Business Partners」を通じて Tivoli 販売チームに提供されているツールです。

1.3.1 ビジネス・ドライバーへの影響

このセクションでは、ビジネス・ドライバーへの影響を確認します。

- 内部関係者の脅威 / データ窃盗

  内部関係者の脅威の 80% は、特権ユーザーまたは技術系ユーザーによって引き起こされます。Tivoli Security Information and Event Manager では、ユーザー行動の証拠として監査証跡ログを収集し、参照できるようにすることで、ネットワークを*監視カメラ*のように見張ります。内部関係者が監視されていることを知ると、データ窃盗の可能性が減少するほか、ミスの把握、回避、修正がより的確に行えるようになります。

  また、Tivoli zSecure Audit が提供する構成およびぜい弱性のチェック機能、ベスト・プラクティスとの比較機能、および修復機能によって、システムは外部および内部の攻撃とミスの影響を受けにくくなります。侵入やミスが発生した場合は、Tivoli zSecure Audit を使用して、その状態を切り分けて原因を把握し、迅速に修正することができます。さらに、Tivoli zSecure Audit は、技術系の内部関係者が使用するぜい弱なデフォルト設定を無効にして、特権ユーザーが違反を起こさないようにします。

  この観点で、Tivoli Command Verifier はメインフレームの構成および設定がコンプライアンスに準拠するように支援して、内部 / 外部の違反、および自ら招く損害が発生する可能性を減らすことができます。

  Tivoli zSecure Admin を使用することで、RACF 管理はより公正になり、エラーが起こりにくくなります。また、社内のセキュリティーと規制のポリシーにさらに準拠するようになることは言うまでもありません。これにより、ぜい弱性が軽減され、内部違反や多大な損害をもたらすミスの可能性が減少します。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 10% から 15% のコスト削減を実現できます。

- ユーザー・アクセスでの節減

  経験の浅い管理者やさまざまな場所で管理を行う管理者にとって、RACF の習得は容易ではありません。Tivoli zSecure Admin は、簡易性を高めた管理者用 RACF インター

フェースを提供し、管理者がタスクを実行する際の時間と労力を節減できるようにします。

Alinean の Business Value Analyst ツールによると、これによって組織は約 5% から 10% のコスト削減を実現できます。

1.3.2 IT 運用への影響

このセクションでは、IT 運用への影響を確認します。

- ポリシー管理

  Tivoli Security Information and Event Manager では、ログ管理での収集を実際的な規則 (誰が、何を、いつ、どこで、どこから、どこに対して実行できるか) に体系化できます。これによって、*許容できる利用ポリシーと変更管理ポリシー*を自動的にモニターし、施行できるようになります。

  System z 側では、Tivoli zSecure Audit を使用してポリシーの手動チェックを自動化されたプロセスへと進化させることができます。その出力は、Tivoli Security Information and Event Manager 内に統合された形で使用できます。

  Tivoli Command Verifier を使用すると、RACF ポリシーを*インライン*で自動的に施行できます。これにより、コマンドを実行する*前に*、コマンドが監査ポリシーと規制ポリシーを満たしていることが検査されます。

  Tivoli zSecure Admin のユーザー・フレンドリーな RACF 管理用インターフェースでは、識別ポリシーとアクセス・ポリシーを施行できます。ユーザーのライフサイクル全体を、より低コストで、より簡単に、かつ社内ポリシーに従って管理することができます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 10% から 15% のコスト削減を実現できます。

- コンプライアンスの管理とレポート

  Tivoli Security Information and Event Manager は、セキュリティー・ログ・データの全般的な収集、保管、取り出し、および調査を可能にしてログ管理を自動化し、ログをコンプライアンス・レポートと調査レポート用に自動的にフォーマットして処理することができます。SOX、HIPAA、ISO、GLBA などの特定の規制に対応したモジュールでレポート作成が自動化され、さらに時間を節減できます。

  監査員向けの多数の組み込みレポート、および Tivoli zSecure Audit の CARLa レポート作成言語を、お客様のニーズに合わせて利用できます。

  Tivoli zSecure Command Verifier では、コマンドを実行する*前に*コマンドが監査ポリシーおよび規制ポリシーを満たしていることを検査して、RACF データベースをクリーンでコンプライアンスに準拠した状態に維持できます。このため、監査にも簡単に合格できます。

  Tivoli zSecure Admin での RACF に対する自動化されたポリシー・コンプライアンス・セキュリティー管理によって、コンプライアンスを確保できます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 15% から 25% のコスト削減を実現できます。

- ログ管理

  Tivoli Security Information and Event Manager は、セキュリティー・ログ・データの全般的な収集、保管、取り出し、および調査を可能にしてログ管理を自動化し、ログをコンプライアンス・レポートと調査レポート用に自動的にフォーマットして処理します。

  また、メインフレームで Tivoli zSecure Audit を使用してログ管理を自動化し、Tivoli Security Information and Event Manager などの企業ログ管理ソリューションにログを供給することもできます。

Alinean の Business Value Analyst ツールによると、これによって組織は約 20% から 40% のコスト削減を実現できます。

- 法令遵守

  Tivoli Security Information and Event Manager のユビキタスなログ収集、法令遵守、および管理機能により、あらゆるサーバー、アプリケーション、データベース、またはデバイスにわたってユーザー行動のログの保管、取り出し、および調査を行うことができます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 15% のコスト削減を実現できます。

- セキュリティー・ツールのカスタマイズ、管理、および保守

  Tivoli zSecure Audit の詳細な監査機能を使用することで、RACF 監査用のカスタム・ツールは不要となります。

  コマンドを実行する*前に*、コマンドが社内の監査ポリシーおよび規制ポリシーを満たしていることを検査するソリューションとして Tivoli zSecure Command Verifier を活用することで、企業内ツールを作成する手間を省くことができます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 30% のコスト削減を実現できます。

- 監査および監査前の準備にかかる内部と外部の平均時間

  監査の準備には多額のコストがかかります。Tivoli Security Information and Event Manager および Tivoli zSecure Audit は、ログ・ファイルの収集、コンプライアンス・レポートの生成、規制や基準を満たしている証拠の明示、監査の調査の有効化などに関連する側面を自動化できるようにします。

  Tivoli zSecure Audit は、メインフレーム上での RACF、ACF2、TopSecret、z/OS、DB2、および UNIX のセキュリティー・コンプライアンスを継続的に分析することで、監査の自動化と合理化を実現します。多数のレポートや分析をすぐに利用でき、監査員が来たときに使用できます。

  これにより、監査の前後および監査中の時間と労力を大幅に節減できます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 10% から 15% のコスト削減を実現できます。

- 監査にかかる内部と外部の平均時間

  現場にいる監査員から大量のデータやレポートを要求される可能性があります。セキュリティー監査の場合は、Tivoli Security Information and Event Manager でコンプライアンスに対するログ情報の収集とレポート作成を自動化できます。これにより、必要なコンサルタントの数が減り、監査の時間が短縮されます。

  Tivoli zSecure Audit は、メインフレーム上での RACF、ACF2、TopSecret、z/OS、DB2、および UNIX のセキュリティー・コンプライアンスを継続的に分析することで、監査の準備の自動化と合理化を実現します。多数のレポートや分析をすぐに利用でき、監査員が来たときに使用できます。これにより、監査の前後および監査中の時間と労力を大幅に節減できます。

  Alinean の Business Value Analyst ツールによると、これによって組織は約 10% から 15% のコスト削減を実現できます。

Tivoli zSecure 製品への投資で回収されるコストを経営陣に対して正当化するために ROI 分析を作成する予定がある場合は、この製品と同等の機能を提供するために現在かかっているコストを基準として、分析で得た数値を使用できます。ここから、現在実行している IT セキュリティー・プロセス全体にわたって節減額を計算でき、z/OS および RACF セキュリティー・インフラストラクチャーへの投資を合理的に正当化できる可能性が高くなります。

1.4 まとめ

この章では、IBM Tivoli Security Management for z/OS が組織に対して監査およびコンプライアンス管理レポートを提供する仕組みを説明しました。また、z/OS、RACF、CICS、および DB2 から得たセキュリティー情報に影響するセキュリティーの変更を監査することで、脅威の情報集約、分析、およびモニターを行う方法を説明しました。結果として、IBM Tivoli Security Management for z/OS では、包括的なログ・データを収集し、先進的なログ分析によってそのデータを解釈し、タイムリーな追跡調査のために効率的かつ合理的な方法でその結果を伝達することができます。

IBM Tivoli Security Management for z/OS V1.11 は、管理にかかる時間、労力、コンプライアンスのオーバーヘッド、およびコストを削減する一方で、メインフレーム・セキュリティーの管理を支援します。この製品は、RACF データベースのクリーンアップ機能を使用して、使われなくなった権限の問題に対応し、例外に関するレポートを作成する際にリソース使用の監査を行います。また、ポリシー・コンプライアンスを徹底し、自動化されたアクセス・モニタリングを行ってデータベースが汚染されないようにします。

次の章では、3 つのビジネス・シナリオを取り上げて、これらの機能を説明します。

2

お客様シナリオ

この章では、Security Management for z/OS 製品の各種コンポーネントをデプロイするための 3 つの一般的なシナリオについて説明します。各シナリオでは、すべての製品が使用されているわけではありません。これは、1 つのコンポーネントの単純なデプロイメントで実現できる直接的なメリットを説明し、後からスイートの別のコンポーネントをデプロイしてこのメリットを拡張できることを示すことを目的としています。

各お客様シナリオの背景にある主な動機は、特定のビジネス目標です。各組織が直面している課題の概要を以下に示します。

- z/OS セキュリティー環境が適切に管理され保護されていることを、内部と外部の監査員に納得させる。
- 特権を持つ内部関係者による悪用から重要な RACF リソースを保護する。
- 監査への即応性およびポリシー・ベースでのセキュリティー・アクセス権の管理を実証する。

これらは、多くの組織が直面している一般的なビジネス上の課題です。ここからは、これらの懸案事項に効果的に対応すると同時に、コスト削減、セキュリティー改善、および業界のベスト・プラクティス基準への適合を実現するために、Tivoli Security Management for z/OS オファリングの各種コンポーネントのデプロイを成功させるにはどうすればよいかを説明していきます。

2.1 z/OS セキュリティー環境が適切に管理され保護されていることを内部と外部の監査員に納得させる

最初のシナリオでは、ある政府機関を取り上げます。この機関は定期的に監査を受けており、監査部門は z/OS に特化した監査でのスキルを最近ようやく拡大したところです。課題はますます難しくなり、監査で要求される深度および技術的詳細も増えています。そこでこの機関は、厳しさを増す監査に合格しやすくなるように、z/OS セキュリティー管理の慣行を一掃して最新化することにしました。

この要件に取り組むため、この機関では、以下の 3 フェーズ・アプローチによって、リスクを最小化しながら、プロジェクトの早期に ROI をできるだけ向上させることを決定しました。

フェーズ 1 Tivoli zSecure Admin および Tivoli zSecure Audit をデプロイする。

フェーズ 2 Tivoli zSecure Audit から推奨されたベースラインの改善点を実装する。

フェーズ 3 宣言されているセキュリティー・ポリシーおよびベスト・プラクティス基準への継続的なコンプライアンスを確実にするために、ベースライン・トラッキングを確立する。

2.1.1 フェーズ 1 - Tivoli zSecure Admin および Tivoli zSecure Audit をデプロイする

Tivoli zSecure Audit は、この政府機関に対し、現在のセキュリティー状況の詳細説明とその状況を改善するための推奨事項を記載したレポートを提供します。Tivoli zSecure Admin は、zSecure Audit から推奨された改善点を効果的かつ迅速に実装するために必要な管理ツールを提供します。

どちらの製品も、システム修正変更プログラム / 拡張機能 (SMPE: System Modification Program Enhanced) から標準の z/OS インストール・プロセスを使用してインストールされます。

初歩的なトレーニングを受けることで、RACF 管理の効率面ですぐにメリットを実現できます。これにより RACF 管理スタッフは、自分の時間をベースライン・セキュリティーの推奨された改善点に費やすことができます。

この実装では、関連性のある 3 つのカテゴリーのセキュリティー関連データの日次、週次、および月次アーカイブが、スケジュールされたバッチ・ジョブを通じて自動生成されます。

1. バッチ・レポートまたはその他の定期レポートを効率的に処理するために最適化された、アンロード形式の RACF データベース (zSecure UNLOAD ファイル)。
2. PARMLIB およびその他のシステム構成データから得られる、関連したシステム・セキュリティー設定のスナップショット (CKFREEZE ファイル)。
3. 日次、週次、および月次の各アーカイブ・データ・セットの対応する SMF データのコピー。

上記のデータ・ソースの 1 と 2 は、z/OS および RACF に関連するセキュリティー構成を詳細に調査できるようにするために、限定的に zSecure Audit で生成されます。3 番目のデータ・ソースは、通常 z/OS プラットフォームの既存のツールと自動化を使用して生成されます。ほとんどのデプロイメントで、この SMF 監査証跡のアーカイブを保持することが要望されますが、システム上のアクティビティーの完全な法令遵守分析を行うための十分な情報がこのアーカイブに含まれていることは、そのための構成を特に行っていない限り、ほとんどありません (この例を 23 ページの『重要なインフラストラクチャー・リソースの監査設

定を正しく行って、機密構成データの変更に関連する SMF 監査証跡が生成されるようにする』に示しています。

これらのアーカイブ・データ・ソースには付加的な機能があります。例えば、システム・セキュリティー・ベースラインに関して、過去のある時点と現時点を比較することができます。これによって、管理に対するセキュリティーの改善の進捗を実証し、セキュリティー改善プロジェクトの成果を示す測定基準を得ることができます。過去と現在の定義の比較には、zSecure Audit の機能が使用されます。

インストール済み環境は、災害復旧などの運用上の理由から別々のデータ・センターに設置された 2 台の物理的な System z マシン上に散在する、複数の z/OS ロジカル・パーティション (LPAR) で構成されます。zSecure Audit と zSecure Admin の両ソリューションはすべての LPAR にインストールされます。これには、新しい z/OS リリースをインストールしてテストするシステム・プログラミング・テスト LPAR (よく *サンドボックス* と呼ばれます) も含まれます。

インストール済み環境には、LPAR 全体で共有される専用の DASD があります。RACF データベースが LPAR 間で異なっていると、これがぜい弱性をもたらす可能性があります。複数の LPAR からデータがアクセス可能である場合、zSecure Audit では、このようないくぶん一般的な構成上の問題を考慮に入れて、両面またはあらゆる側面から分析を行います。このデプロイメント・アーキテクチャーを図 2-1 に示します。

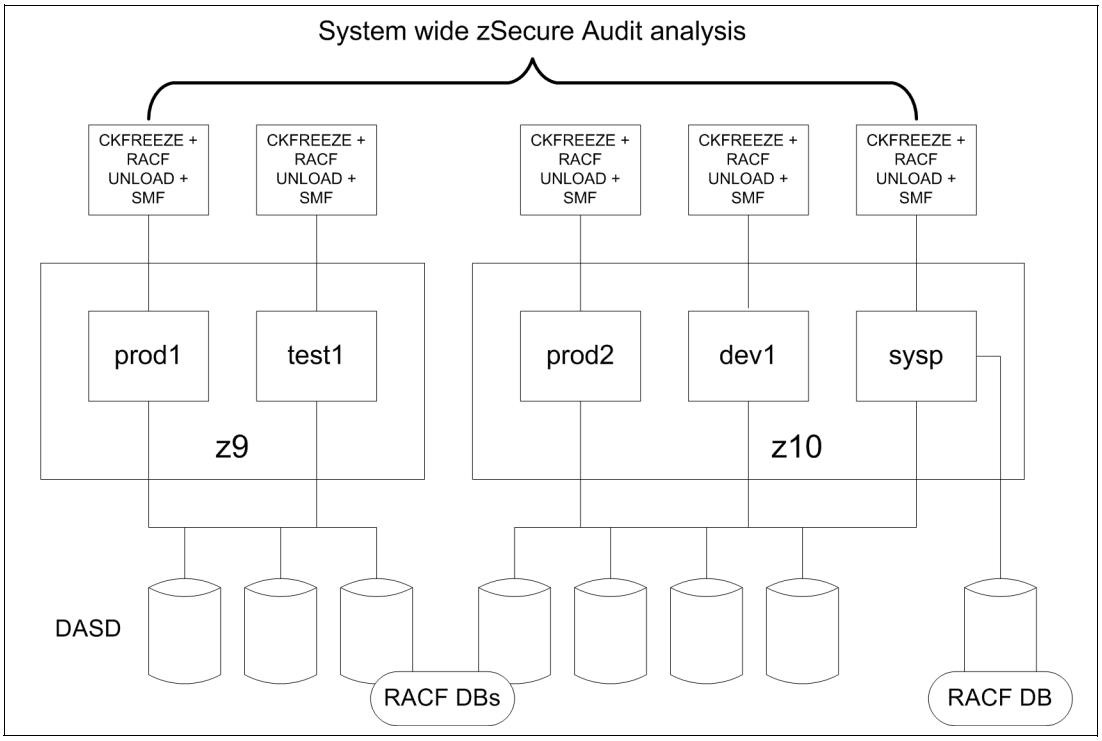


図 2-1　デプロイメント・アーキテクチャー

セキュリティー管理者は、システム・プログラマーおよび運用スタッフと協力して、スケジュールされた一連のセキュリティー・アクティビティーおよびベースライン比較のレポートを実装します。一般にこれらのレポートでは、一連の日次データ収集ジョブで生成されたデータ、つまり一致する日の CKFREEZE ファイル、RACF UNLOAD ファイル、および SMF データが使用されます。

これにより、18 ページの図 2-2 に示すバッチ・データ・フローが発生します。データが生成され、保存され、レポートに使用され、履歴として使用するためにアーカイブされることがわかります。

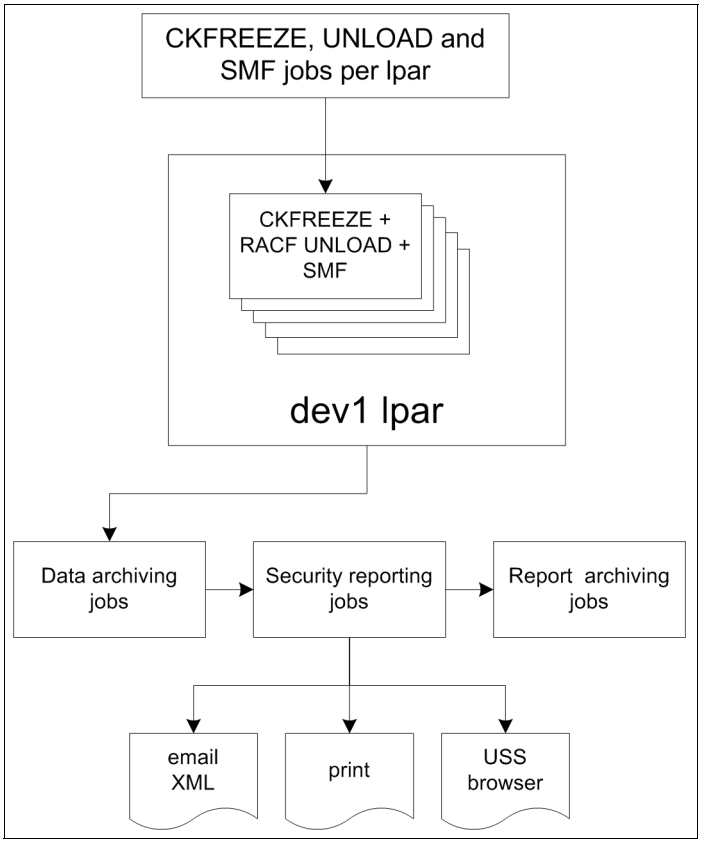


図 2-2　バッチ・データとレポート作成フロー

この政府機関では、複数の CARLa ベースのカスタム・レポートを実装して、XML 形式のファイルが添付された自動電子メール・レポートを生成することにしました。これらのレポートは、従来のメインフレームのユーザー・インターフェースではなく、わかりやすいデスクトップ・ベースのテクノロジーからアクセスできるため、非技術系ユーザー向きです。

実装されるカスタム・レポートは以下のとおりです。

1. 電子メールで担当マネージャーに配信される、日次ユーザー・アクセス違反。
2. チーム・リーダーとその他の担当マネージャーに配信される、四半期別アクセス再検査レポート。
3. データを所有するマネージャーに配信される、機密データに対する高レベルのアクセスに関する日次電子メール・レポート。
4. セキュリティー管理者に電子メールで配信される、RACF 設定の追加または変更。
5. システム・プログラマーに電子メールで配信される、z/OS システム設定の追加または変更。
6. セキュリティー担当者に電子メールで配信される、実行された RACF コマンドのサマリー。
7. セキュリティー担当者に電子メールで配信される、高レベルの特権を使用したリソースへのアクセス。

zSecure 運用の収集ステージで収集されたすべてのデータは、将来参照できるようにアーカイブされ、明白かつ包括的な履歴監査証跡となります。すべての LPAR から収集されたデータは、特定の非実動 LPAR に保管されます。この LPAR ですべてのレポートが生成されるため、実動システムには管理上のこの作業負荷がかかりません。

すべてのレポートは同じようにアーカイブされ、UNIX システム・サービス・ファイル・システムを介してホストされます。また、組み込みの z/OS Web サーバーから利用可能となるため、ユーザーと監査員は標準的な Web ブラウザーを使用して履歴レポートを参照できます。zSecure では、これらのレポートを自動的に UNIX システム・サービス・ファイル・システムにエクスポートできます。保存されたレポートを循環させてアーカイブするための、小さな z/OS UNIX システム・サービス・シェル・スクリプトを作成することをお勧めします。

この時点で、この政府機関は、IBM Tivoli Security Management for z/OS のデプロイメントを成功したプロジェクトと見なしています。既に監査員は、標準化されて簡単にアクセスできるレポートのメリットを経験し、管理者は日常業務での効率改善を実現しつつあります。次は、監査に合格しやすくなるように、システムのベースライン・セキュリティーの改善を開始します。

2.1.2 フェーズ 2 - zSecure Audit から推奨されたベースラインの改善点を実装する

zSecure Audit を実装していれば、ISPF インターフェースから標準の付属レポートを通じて、優先順位が付けられたシステム監査の懸案事項のリストを簡単に生成できます。図 2-3 は、このようなベースライン・レポートの標準的な出力を示しています。

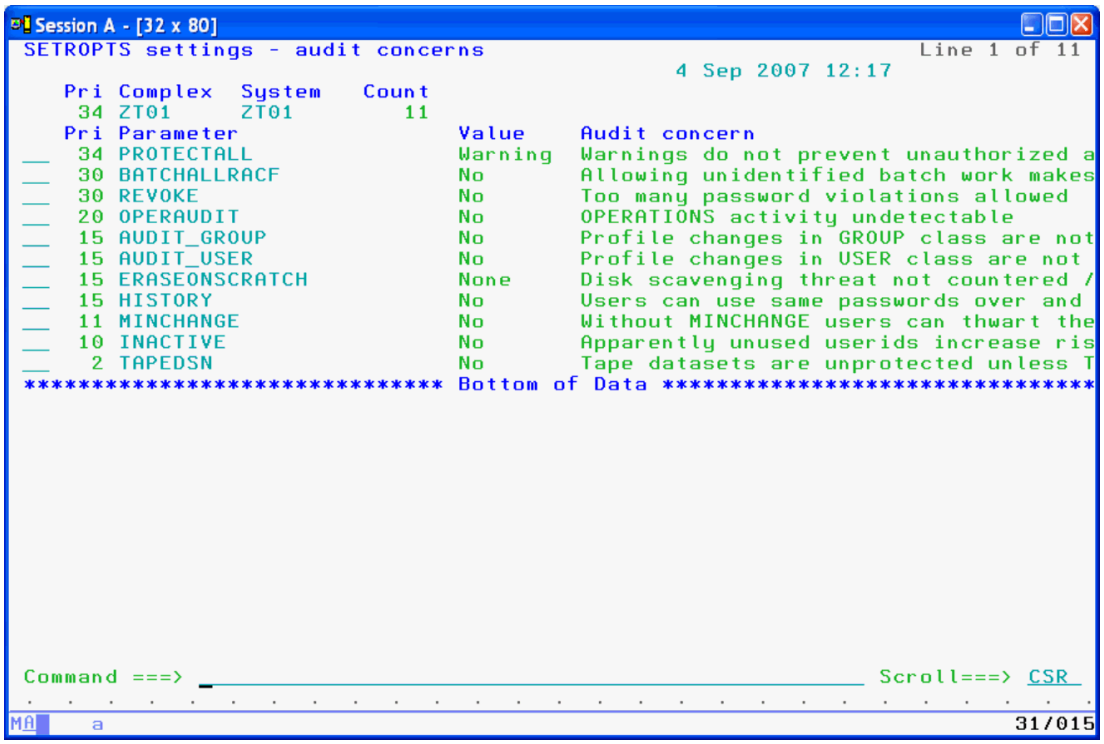


図 2-3 zSecure Audit ベースライン・レポート

これらのレポートは、セキュリティー管理 (つまり非実動) LPAR から実行され、1 回ですべての LPAR の RACF データベースおよび CKFREEZE システム・スナップショットを処理します。これにより、システム間の分離に関係なく、システム全体のビューがこの政府機関

に示されます。複数の LPAR が存在する環境では、全体的なセキュリティーとセキュリティー変更の影響を確実に把握するために、このビューが不可欠となります。

この政府機関の z/OS 環境では、一部の LPAR のベースライン制御が他の LPAR に比べて非常に弱いことがレポートからわかりました。特に、システム・プログラマーが使用する環境のセキュリティ制御は、実動 LPAR と比べてかなり甘くなっています。テスト環境ではこの状況が予想されますが、この場合は、DASD が共有されているために、システム・プログラミング LPAR からアクセスされた場合に、実動システムに属する特定の重要なリソースがぜい弱になることが zSecure Audit で強調されました。これは、システム・プログラミング LPAR が使用する別の RACF データベースで、いくつかの重要な制御が非アクティブ化されているためです。そこで次の作業として、これらのテスト用 LPAR の適正な使用をできるだけ阻害せずに、これらの制御を再びアクティブ化します。

複数の制御を再アクティブ化するか、その他のアクセス・パスを除去または削減する必要があります。これには以下の制御が含まれます。

- RACF SETROPTS NOPROTECTALL の使用
- データにアクセスするためのユーザー属性 OPERATIONS の幅広い使用
- UNIX システム・サービス・スーパーユーザー (UID 0) 特権の幅広い使用
- 重要なインフラストラクチャー・リソースの監査設定が誤っているために、機密構成データの変更に関する SMF 監査証跡が作成されない

NOPROTECTALL の使用の排除

NOPROTECTALL をシステム設定として使用すると、データが RACF で保護されないままシステムに存在することになり、事実上システムのすべてのユーザーが利用できる状態になります。実動システムではこの状況がほとんど見られないものの、発生することは確かであり、この慣行が短時間でも定着してしまうと、状況を解消することは難しくなります。

ここで生じる疑問は、*RACF で保護されていないシステムにどのデータが存在しているか*ということです。都合のいいことには、zSecure Audit には、適合する RACF プロファイルがないデータ、およびその逆に当該 LPAR で利用可能な DASD 上に適合するデータがない RACF プロファイル (存在する場合) の両方を表示する簡単なレポート機能があります。

次に解決が必要な疑問は、*これまで保護されていなかったすべてのデータが保護されたタイミングがわかるか*、*また NOPROTECTALL SETROPTS パラメーターを非アクティブ化できるか*ということです。この場合も、zSecure Audit が提供する、非正規の手段によるデータへのすべてのアクセスに関するレポートが役立ちます。

回答が必要な最後の疑問は、*これまで保護されていなかったデータに対してユーザーが正しいレベルのアクセス権を付与されていることがどのようにしてわかるか*ということです。この場合も zSecure が役立ちます。

このためこの政府機関は、この機密漏れを徐々に削減して最終的に解消するために、ある程度反復的な複数ステップのプロセスを開発することになりました。

1. zSecure Audit のレポートを実行して、保護されていない DASD データ・セットを識別します。
2. これらのデータ・セットに対してプロファイルを定義し、プロファイル自体を WARN モードに設定してアクセスを拒否しないようにします (この作業には zSecure Admin を使用)。
3. 保護されていないデータ・セットがなくなるまで、ステップ 1 と 2 を繰り返します。

4. モニターの対象を、保護されていないデータから WARN モードのデータ・セット・プロファイルに移行します。zSecure Audit には、そのための組み込みレポートがあります。
5. zSecure Audit の日次 WARN モード・アクセス・レポートを確認します。場合によっては、ユーザーに特定レベルのアクセス権が必要であることが明らかとなります。
6. WARN モードのデータ・セット・プロファイルへの最も一般的なアクセスを確認できるだけの SMF レコードを取得した後は、CARLa サマリー・レポートを使用して、モニター期間中にデータにアクセスしたユーザー、および各ユーザーが実際に使用した最も高いレベルのアクセス権を確認します。これは、ユーザーの正当な要件であることを確信した上で適切なレベルのアクセス権を付与するために必要なデータとなります。
7. zSecure Admin を使用して、プロファイルから WARN モード・フラグを除去し、レポートを続行します。ただし今度は、アクセス違反の行為に関するレポートを作成します。これも zSecure Audit 付属の標準レポートです。
8. zSecure アクセス違反レポートを、結果的に生成される可能性があるユーザーのアクセス権要求とともに使用して、これまで保護されていなかったデータ・セット・プロファイルのアクセス・リストを微調整します。

このプロセスをひととおり実行し、WARN モードでのアクセスおよび保護されていないデータへのアクセスに関する日次レポートを確認することで、このタイプのアクセスの件数をすぐに減らすことができます。ある時点で、望ましくないアクセスがほとんどなくなるので、PROTECTALL をアクティブ化し、最終的にこの機密漏れの状態を終わりにすることができます。この政府機関が取り組んでいるシステムでの安心感のレベルおよびセキュリティー・エラーの影響によっては、WARN モードの PROTECTALL で一定期間システムを稼働させてから、最終目的である FAIL モードでの PROTECTALL のアクティブ化を行う場合もあります。

この機関は、各ステップで zSecure Admin を使用して、必要な RACF コマンドを生成するか、または単純な上書き可能フィールドを使用して RACF SETROPTS 設定を変更できます。これにより、構文エラーを発生させることもなく、また資料を検索してコマンドが正しいことを確認することもなく、正しいコマンドを実行できます。

データにアクセスするためのユーザー属性 OPERATIONS の使用の排除

OPERATIONS 属性はいまだに広く使用され、実動システムでも多く見られます。この属性は、長年にわたって z/OS 環境での運用作業の要件として段階的に廃止されてきました。現在は、データ機能データ・セット・サービス (DFDSS) のユーザーに提供される機能制御を使用して、データへの汎用アクセス権を付与する方法が望ましく、また推奨されています。OPERATIONS が段階的に廃止された理由は、職務 (通常はストレージ管理者の職務) を実行するために一般に必要なアクセス権を超えるアクセス権をこの属性が含んでいるためです。OPERATIONS では、データを移動および管理するためのアクセス権が付与されるだけでなく、ユーザーがデータを読み取って変更することも許可されます。これは明らかに、標準的なストレージ管理者の役割には含まれません。このため、OPERATIONS は IT セキュリティーの原則である*最小特権*に違反します。

OPERATIONS に代わる手段は、RACF FACILITY クラス内で定義され、DFDSS データ管理ツール・スイート内でプログラムによって参照される一連の RACF プロファイルです。通常は先頭が STGADMIN (ストレージ管理) となるように定義されるこれらの RACF プロファイルへのアクセス権では、ストレージ管理者に対して、データの管理が許可されますが、ほとんどの環境でデータの読み取りまたは変更は許可されません。

DFDSS 機能プロファイルを使用するために、ストレージ管理者はストレージ管理バッチ・ジョブで特別な *admin* キーワードをコーディングする必要があります。そこで、この古くて冗長で危険な OPERATIONS 属性を除去するために、この政府機関は、セキュリティー改

善プロジェクトが原因で予期しない結果が生じるリスクを最小化する、複数ステップのレポート作成および分析プロセスを実装します。

これを実現するために、この政府機関は以下の作業を実行します。

1. zSecure Admin を使用して、FACLILITY クラスに STGADMIN 機能をカバーするプロファイルを定義し、ストレージ管理者に必要なレベルのアクセス権を付与します。
2. ADMIN キーワードが組み込まれるように、ストレージ管理者のすべてのジョブを更新します。
3. OPERATIONS 属性が使用されていたアクティビティーに対して、zSecure Audit 付属のレポートを実行します。場合によっては、ユーザーに特定レベルのアクセス権が必要であることが明らかとなるので、必要に応じて、その権限を付与します。
4. OPERATIONS の使用に関する詳細データを一定期間収集した後に、CARLa サマリー・レポートを実行して、ユーザーごとの最も高く重複しないレベルのアクセス権を表示します。この情報を適切に検証した後に、正しいと判別されたアクセス権を付与します。
5. レポートにこのタイプのアクセスが一切またはほとんど表示されなくなるまで、ステップ 3 と 4 を繰り返します。

この時点で、すべてのユーザーから OPERATIONS 属性を除去し、日常のシステム管理に新しいストレージ管理者機能プロファイルを使用できるようになります。zSecure Admin と zSecure AdminAudit を併用すれば、この種のマイグレーションは当初予想されるほど難しくありません。適切なツールが揃っている状況で、これらの古くて危険なセキュリティー慣行を z/OS 環境で継続することはもはや許されません。

UNIX システム・サービス・スーパーユーザー (UID 0) 特権の使用の削減

前のセクションで説明した OPERATIONS 属性と同様に、UNIX UID 0 は制御されることなくアクセス権を付与しますが、適切に管理された IT セキュリティー・インフラストラクチャーでは通常それは許容されません。多くの場合、システム・プログラマーには UNIX UID 0 およびホーム・ディレクトリー「/」または root が割り当てられ、UNIX システム・サービス環境内でアクセスに関するそれ以外の制御は行われません。ベテランの UNIX 管理者または Linux 管理者は、このアプローチに驚くはずです。従来のベテランの z/OS システム管理者を弁護すると、IBM が z/OS UNIX システム・サービスの取り扱いを開始した時点で、彼らには一般に認められている UNIX のセキュリティー基準の経験がほとんど、またはまったくありませんでした。しかし、状況は変わりました。UINX セキュリティーを意識する z/OS 管理者が増え、z/OS UNIX システム・サービスを他の UNIX インストール済み環境と同じか、またはより優れた基準に合わせて実行することが重要であるという認識が、z/OS の世界で急速に広まりつつあります。

再度、このシナリオの政府機関は、z/OS 環境での UID 0 の幅広い使用を削減するために従う手順のチェックリストを作成しました。

1. UID 0 が現在割り当てられているすべてのユーザーを識別します。zSecure Audit にはそのための組み込みレポートがあります。
2. これらのユーザーに割り当てられているホーム・ディレクトリーをレポートします。同じ zSecure Audit レポートにこのデータも表示されます。
3. これらのユーザーに固有のホーム・ディレクトリーを作成して割り当てます。zSecure Admin では、作成されたホーム・ディレクトリーを、ISHELL ユーティリティーまたはネイティブの UNIX コマンドを使用して割り当てることができます。
4. UID 0 が割り当てられていたスタッフに、固有の UID を割り当てます。これは、zSecure Admin インターフェースで簡単に行えます。
5. スーパーユーザーのサービスにアクセスすることがスタッフの正当な要件として文書化されている場合は、zSecure Admin を使用して、FACILITY クラスの BPX.SUPERUSER

プロファイルへのアクセス権をそのスタッフに付与します。これでスタッフは、制御および監査の下で、UNIX の **su** コマンドを使用してスーパーユーザーの特権を得ることができます。

6. プライベート・ユーザー・データを以前のホーム・ディレクトリーからユーザー固有の新しいホーム・ディレクトリーに移動し、新しいユーザー固有の UID が反映されるようにこのデータに対して所有権の適切な変更を行います。これは UNIX の **chown** コマンドを使用して行います。

関係するステップはそれほど複雑ではありませんが、ターゲットのユーザー ID *ごと* に実行する必要があります。この条件を備えたユーザーが多数存在する場合は、これらの変更をスクリプト化し、UID の割り当ておよび新しい構造へのユーザーとそのデータの移動をある程度自動化することが可能です。この作業は zSecure の範囲外であり、ある程度の基本的な UNIX プログラミング・スキルを必要とするため、この資料では取り上げません。

重要なインフラストラクチャー・リソースの監査設定を正しく行って、機密構成データの変更に関連する SMF 監査証跡が生成されるようにする

一般に組織では、全部ではなくてもほとんどの RACF リソース・プロファイル定義に対して、デフォルトの RACF SMF ロギングである*違反のみ*の生成を許可しています。このロギングでも、あるレベルの監査証跡は作成されますが、完全な監査ロギングには追加のデータが必要であり、法令遵守調査の可能性がある場合も同様です。データがログに記録されていないと、照会が行われた場合に誰が何を行ったかを判別できません。

この政府機関では、標準の zSecure Audit システム検査レポートを使用することで、全部ではありませんが、ほとんどの機密システム・リソースに対して不十分な監査が行われていたことがわかりました。つまり、正当なアクセス権を持つユーザー (システム・プログラマーやその他の高い特権を持つユーザーなど) がそのアクセス権を使用してシステム定義データ・セットを破壊した場合でも、SMF 監査証跡にはこの行動の有効な記録が存在しないことになります。

zSecure Audit 検査レポートには、この状態を修正するために推奨される RACF コマンド・リストが示されます。zSecure Audit では、CKFREEZE システム・スナップショット・データベースを通じて判別された機密データ・セットごとに、そのレベルの重要度のデータに割り当てる必要がある正しい監査属性、消去属性、および汎用アクセス属性が推奨されます。セキュリティー管理者は、推奨されたコマンドを確認し、ローカルの命名規則や基準に合わせてそれらのコマンドを変更し、結果として得られた一連のプロファイルを実装する必要があります。

これで 2 番目の実装フェーズは終了です。zSecure Audit および zSecure Admin を使用して環境のレポート作成および制御を行うシステムが完成しました。また、監査上の検出事項をいくつか除去し、全体的なビジネス・リスクを低減して、システムの全体的なセキュリティー体制を大幅に改善しました。フェーズ 3 では、状況を確実に維持するためのプロセスを確立します。

2.1.3 フェーズ 3 - ベースライン・トラッキング

最後のフェーズでは、宣言されているセキュリティー・ポリシーおよびベスト・プラクティス基準への継続的なコンプライアンスを確実にするために、ベースライン・トラッキングを確立します。

トラステッド・コンピューティング・ベースの確立

*セキュリティー・ベースライン*の変更をモニターする際には、まず無理なく実現できるベスト・プラクティスにできるだけ近いベースラインを作成します。これまでのフェーズで

この政府機関が行った作業が、この段階で役立ちます。ここでシステムのスナップショットを作成し、それが許容されるベースラインであることを宣言します。このスナップショットを、*トラステッド・コンピューティング・ベース* (TCB) と呼びます。

zSecure Audit では、「*変更トラッキング*」という基本メニュー・オプションでこの機能を提供しています。この機能では、保存された TCB のコピーが、現在のシステムでの設定と比較されます。容認された TCB との違いが報告された場合は、以下の 3 種類のアクションのいずれかを選択します。

1. 変更を受け入れて TCB に反映する。

   これは、ユーザーがこの変更を認識しており、この変更が既存の容認された TCB に取り込まれることが望ましい改善であることを示します。

2. 変更を拒否する。

   これは、変更が制御の下で行われておらず、TCB に取り込むべきではないことを示します。この変更は、システムで取り消されるか、または現在の TCB に取り込んで後から容認することを決定するまで、日次分析に表示され続けます。

3. 変更を延期する。

   変更の延期は、変更を TCB に取り込むことが望ましいかどうかが不明である場合に選択します。この変更については、適切なアクション (容認または拒否) を決定する前に、システム・プログラマー、管理者、および監査員との協議が必要になる場合があります。

この組み込みの zSecure Audit 機能を使用すると、機能的な方法で、セキュリティーおよびオペレーティング・システム構成に関してシステムを望ましい状態に保つことができます。

アクセス・モニターおよび自動化されたクリーンアップ機能の使用

この政府機関は、TCB ベースラインを確立したときに、zSecure Admin 付属のアクセス・モニター・ユーティリティーおよびクリーンアップ・ユーティリティーのデプロイも行っています。これらの機能は、1 年間にわたってバックグラウンドで受動的に実行されてから、次のステップに進みます。この間に、システム上で*誰が何を行ったか*、およびそのアクションを実行する際に使用された RACF アクセス権またはそれ以外の特権は何かを判別するために特別に高度に最適化されたフォーマットでデータが収集されます。

このデータがビジネス・サイクル全体にわたって収集された後に (この政府機関は丸 1 年分の処理が必要と判断)、クリーンアップ機能が使用されて、報告されたすべてのアクセスが、RACF データベースで定義されているすべてのアクセス権と比較されます。RACF データベースで定義されているアクセスと実際に観測されたアクセスの間に違いがある場合は、1 年間参照されなかった RACF 定義のリストが管理者に示されます。管理者は、システムにマイナスの影響がないことを十分に確信した上で、これらの冗長な RACF 定義の削除を開始できます。

2.1.4 シナリオ 1 のまとめ

これでこの政府機関は、Tivoli Security Management for z/OS の初期段階での用途を確立しました。オファリング全体に含まれている製品を追加でデプロイするにつれて、この機関のセキュリティーおよび結果としての ROI がさらに向上する可能性が十分にあります。ただし、この時点で既にこの機関は、監査の即応性を実証できる点と、業務を遂行する場である RACF と z/OS の構成と環境を高度にセキュアな状態に保つことが管理上の重点であることを実証できる点で満足しています。

さらに、アクセス・モニター機能とクリーンアップ機能をデプロイしたことによって、次の年の同じ時期には、RACF 定義に関して継続的な改善の正しいプロセスが確立されたことを監査員に実証できるでしょう。確実な TCB とクリーンなセキュリティー・データベースの相乗効果で、この機関は RACF セキュリティーに関して世界で最も成功したインフラスト

ラクチャーの 1 つに数えられています。このシステムに関する監査レポートの内容は、次第に肯定的になることが予想されます。

2.2 特権を持つ内部関係者による悪用から重要な RACF リソースを保護する

2 番目のお客様シナリオでは、金融セクターのある企業を取り上げます。この企業は、RACF 環境でセキュリティー特権が適切に分離されていることを実証するという緊急の内部監査要件を抱えています。監査上の一番の懸案事項は、すべてのセキュリティー管理者がシステムの最高レベルの RACF 特権である SPECIAL 権限を使用していることでした。ここ数年の監査レビューで、この最高レベルの RACF 管理者権限がなくても管理者は職務を遂行できるはずであると監査員から何度か指摘されています。

Tivoli Security Management for z/OS オファリングを購入したこの企業は、この最重要懸案事項に対応するために、まず zSecure Command Verifier コンポーネントをデプロイすることにしました。その後の段階で、z/OS プラットフォーム用のより優れた総合監査ソリューションを実装するために、zSecure Audit および Tivoli Security Information and Event Manager を実装する予定です。このソリューションに内部監査部門自体がアクセスすることで、セキュリティー・チームおよびシステム・プログラミング・チームをレポートの準備から解放して本来の業務に従事できるようにします。

この作業にも、段階的なアプローチを使用する必要があります。ここでは、以下の 2 フェーズ・アプローチが使用されます。

フェーズ 1 より優れた RACF リソースの所有および分類の構造を確立する。

フェーズ 2 zSecure Command Verifier 製品でこの構造を使用して各種の管理役割を分離する。

以下のステップは、この 2 つのフェーズにまたがって (ほとんどの場合並行して) 実行されます。

1. 管理者の各種ターゲット役割を確立します。
2. リソース所有構造を確立します。
3. 施行するリソースおよびプロファイルの命名規則を確立します。
4. zSecure Command Verifier がこの新しい構造を利用する際に使用する RACF ルールを確立します。
5. zSecure Command Verifier をアクティブ化し、新しいプロセスをテストします。
6. 必要に応じて改良します。

2.2.1 フェーズ 1 - 新しい構造、役割、およびワークフローの設計

この最初のフェーズでは、リサーチ・プロジェクトのように、現在設定されている役割および実際に使用されているセキュリティー管理の慣行を特定し、それらをより適切に分離する方法を設計します。

まず、現時点でチームの最上級者から最下級者までのすべてのセキュリティー管理者が、最高レベルの RACF 特権を使用していることを確認します。これらのスタッフの多くは、日常業務でこのレベルの特権を行使する必要がないことが明らかであるため、第一原則である *最小特権* に既に違反しています。

最初の作業として、さまざまな管理者が担当している日常業務を正確に把握し、それぞれの業務に必要な最小限の特権を特定します。管理者は以下に示すいくつかの別個のカテゴリーに分類されることがわかりました。

1. 基本的なユーザー・プロビジョニングとパスワード管理を行う管理者。
2. RACF 機能リソース定義を操作する管理者 (主にこれらのリソースのアクセス・リストを管理する)。
3. RACF グループ構造を操作し、必要に応じて新規リソースの定義や新規クラスのアクティブ化を行う管理者。RACF SETROPTS コマンドによる全体的なシステム設定への不定期な変更を実行するように求められることもあります。
4. 特殊なケースとして、上記のすべての役割を実行できる最上級管理者および総合チーム・リーダー。

これらは、作業リストの第一のポイントを満たす妥当なターゲット役割セットと思われます。次に、zSecure Command Verifier を使用して、RACF 構造内でこれらの役割を定義し、制御する必要があります。

次の 2 つのステップは、リソース所有構造の確立と、施行するリソースとプロファイルの命名規則の確立ですが、これらは互いに密接に結び付いています。管理者カテゴリーのリストで最初に挙げた、基本的なユーザー・プロビジョニングとパスワード管理を行う管理者は、容易に分離することができます。

この最初の管理者グループに対する単純なアプローチでは、すべてのユーザー ID の所有者として RACF グループを定義します。より緻密なアプローチでは、組織図に対応し、すべての STAFF ユーザー ID を所有するサブグループを含んでいる RACF グループ・ツリーの一部分の所有者として RACF グループを定義します。RACF グループ・ツリーのこの部分には、IT インフラストラクチャーに関連するユーザー ID が含まれていないことが必要です。これには、バッチ処理用、開始タスク用、システムまたはアプリケーションのユーザー ID 定義用などのユーザー ID があります。実質的には、人事が認識している実際のスタッフのみを管理するために、RACF 内に*分離された領域*を作成していることになります。

ここで zSecure Command Verifier を使用して、図 2-4 に示すように、グループ・ツリーのこのセクションに含まれないユーザーに対して*ユーザー管理者* が RACF コマンドを適用できないようにすることができます。最初の分離の見本は既にあります。

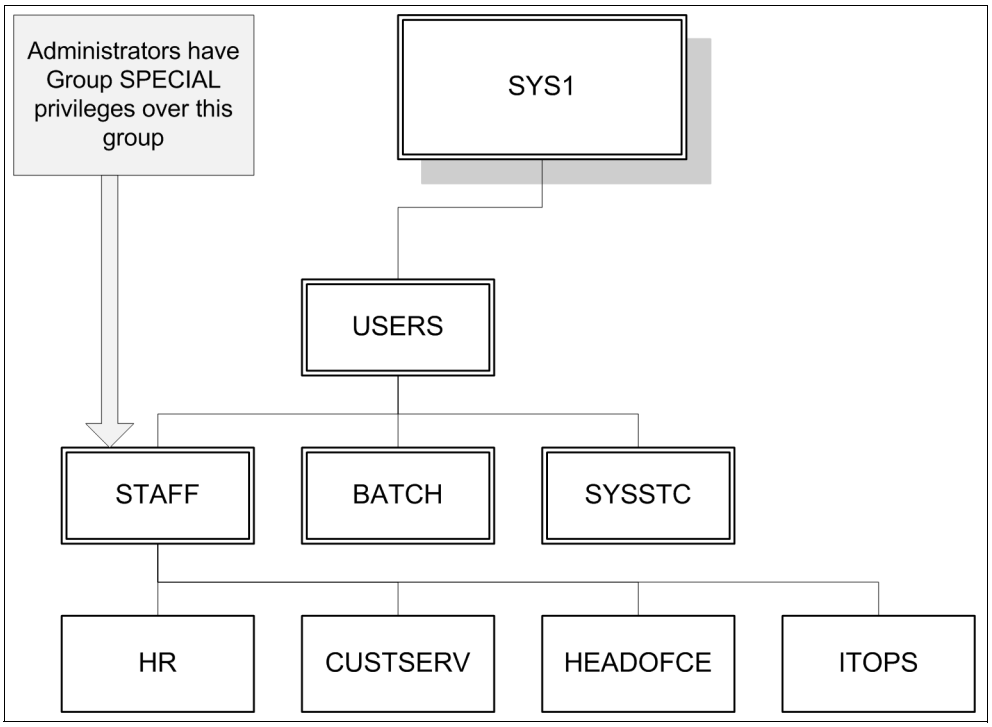


図 2-4 RACF グループ・ツリーの STAFF セクション

次に、リソース・アクセス・リスト全般を管理する 2 番目の主要管理者グループの管理構造を定義する必要があります。ここでも、リソース所有という RACF の概念を使用します。RACF に新しいグループを定義し、このグループが管理することになるすべての機能プロファイルの *RACF 所有者* として指定します。ここで zSecure Command Verifier を使用して、これらの管理者の実行するコマンドが、この新しいグループが直接所有していないリソースに適用されないように制限することができます。この管理者グループを実質的にユーザー管理機能から切り離し、機能プロファイル (FACILITY、OPERCMDS、SDSF など) だけを操作できるように制限しました。これで分離が現実になり始めました。

別の zSecure Command Verifier 組み込み機能を使用して、どの管理者も、容認された命名規則から外れる RACF プロファイル、ユーザー ID、またはグループを定義できないようにします。これは、RACF プロファイル自体の定義を通じて行います。つまり、RACF 管理者が実行できることを RACF 自体が制御または制限するようにします。これらの zSecure Command Verifier RACF プロファイルは、他のユーザーが他の RACF コマンドに関して実行できることと実行できないことを制御するために zSecure Command Verifier で参照されることから、*制御プロファイル* と呼ばれています。

ここにこのプロセスの真の秘訣があります。zSecure Command Verifier で参照される実際の RACF プロファイルを使用することで、RACF 管理者のアクションを制御しています。しかし、管理者がいずれかの制御プロファイルを変更して、分離を必要とした機能へのアクセスを自分自身に許可するとどうなるでしょうか。

リソース管理領域でのこの懸案事項とリスクに適切に対処するには、追加の分離が必要です。図 2-5 に示すように、zSecure Command Verifier 制御プロファイルを所有する専用のグループを作成します。再び zSecure Command Verifier を使用して、制御プロファイルに対して RACF コマンドを実行できるユーザーを限定します。この権限は、1、2 名の比較的下級のリソース管理者またはユーザー管理者に付与します。このスタッフは通常の職務に加えてシステムを制御することになるため、慎重に人選を行ってください。RACF 定義を通常の基準から外す必要があり、そのために zSecure Command Verifier 制御プロファイルを無効にする必要がある場合は、このスタッフが「もう 1 つの目」となって、その RACF 定義の

変更に関与する必要があります。つまり監視者の監視者です。このスタッフは、IT セキュリティーで高い責任を負うための教育を受けていること、およびこの責任を負うために必要なスキルと心構えを備えていることが理想的です。

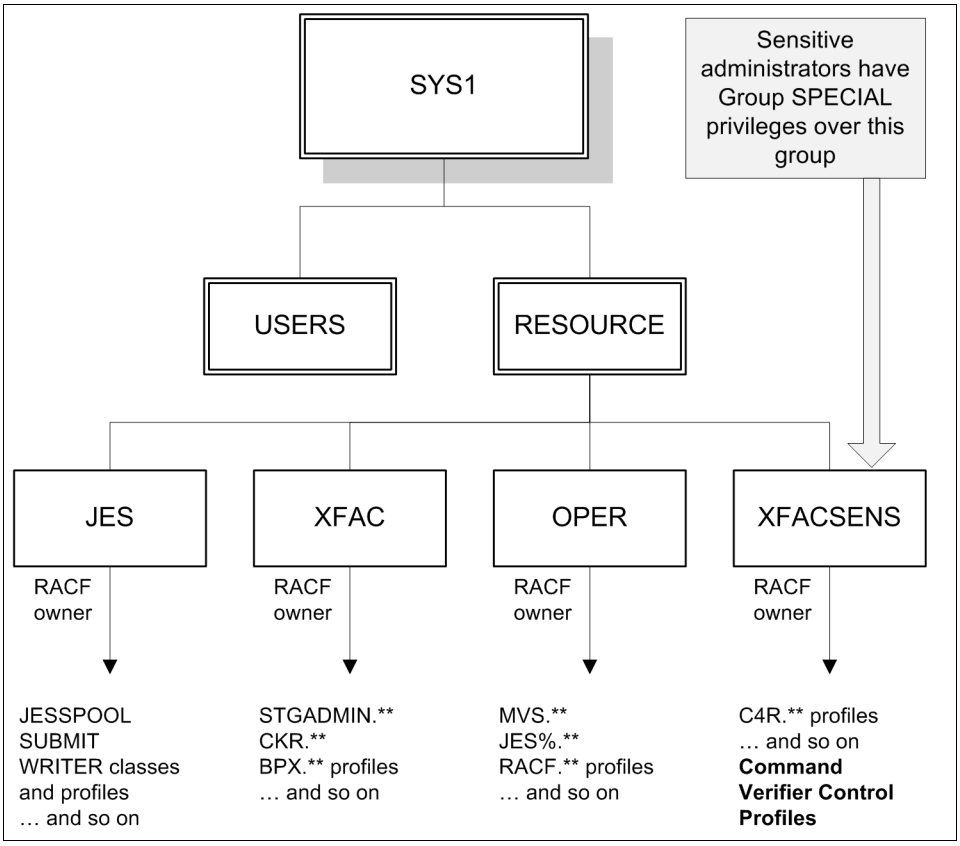


図 2-5 RACF グループ・ツリーのリソース所有セクション

このソリューションの長所は、監視者に高いレベルの RACF 特権が不要である点です。つまり、単純な SPECIAL グループ権限 (直接的なリソース所有権) があれば、zSecure Command Verifier 制御プロファイルを管理するのに十分です。監視者が制御プロファイルを使用して自らにより高いレベルのアクセス権を付与しようとしても、監視者固有の RACF アクセス権は、監視者だけで実質的な損害を与えられるほど高くはありません。監視者にできるのは、最上級の管理者グループ (26 ページの項目 3 と 4 に挙げた管理者) に制御の回避を許可することだけです (このようなアクションが適切な管理上の承認を得ている場合)。監視者だけで不適切な行為を行うことはできません。これで真の分離が実現しました。今後は、少なくとも 1 人の上級管理者と 1 人の下級管理者が事前に結託しないと、サイトで容認された RACF 基準およびその他の確立された分離を覆すことはできなくなります。

同じように、zSecure Command Verifier のこの分離機能を使用して、異なるセキュリティー・プロトコルを設定することができます。例外的な状況で zSecure Command Verifier の制御を回避する場合に、上級管理者と下級管理者を 1 人ずつ要求する代わりに、2 人の上級管理者、あるいは上級管理者と IT の変更に関する実行委員会のメンバーを 1 人ずつ要求することもできます。

2.2.2 フェーズ 2 - 分離機能の実装とテスト

実装中に、zSecure Admin を使用して、RACF データベース構造の新しく定義されたセクションを所有する新しい RACF グループが作成されます。次の作業では、ユーザーまたは

リソースが所有する既存のグループをすべて新しい構造グループの下に移しますが、これもzSecure Admin を使用すれば軽微な作業です。

このような*軽微な作業*で、zSecure Admin の真の能力とメリットを実現できます。リソースが所有するすべてのグループを識別し、構造上の新しい所有ポイントに移動する作業は、従来のツールを使用すると数週間かかりますが、zSecure Admin を使用すると数分で終わります。RACF 用 zSecure Admin を導入した環境で、組織図に対応しなくなった、あるいはビジネスの IT セキュリティー・ニーズに合わなくなった古い RACF グループ・ツリー構造を使い続ける理由はありません。

zSecure Command Verifier 制御プロファイルの確立も、制御プロファイル自体に対する追加の分離と同様に、zSecure Admin を使用して実装されます。

zSecure Admin によって可能となるもう 1 つの機能は、機密性の高い zSecure Command Verifier 制御プロファイルに対して、*マルチレベルの許可*がないとそのプロファイルを変更できないように*マークを付ける*機能です。これは、Tivoli Security for z/OS オファリングが提供する高度な分離機能のもう 1 つの例です。

zSecure Command Verifier 制御プロファイル、および RACF リソースの分離を実装したら、ほぼすべての管理者の System SPECIAL 特権を除去し、代わりに RACF の Group SPECIAL 特権を割り当てて、最終的な実装をテストできます。

この実装では、上級チーム・リーダーに完全な User SPECIAL 特権を残しました。この措置は不要であった可能性もありますが、新しい分離体制によって生じる悪影響を緩和するための賢明な対応と判断されました。

2.2.3 シナリオ 2 のまとめ

中規模から大規模のチームに分かれた z/OS RACF セキュリティー管理者の中で RACF コマンドの権限を分離するという課題には、RACF の SPECIAL グループ権限の固有機能である程度対応できます。zSecure Command Verifier と zSecure Admin を併用することで、この固有機能を新たなレベルへと引き上げることができます。つまり、RACF で制御された安全な方法で、管理者を分類し、管理者のアクションを特定の RACF プロファイルまたはプロファイル・タイプに制限できます。

以前から、多くの組織が SPECIAL グループ権限の使用を避けています。これは、正しい管理が難しい上に、制御が設計どおりに機能していることを確認するのが困難であるためです。zSecure Admin と Command Verifier は、特定の管理者が操作できるプロファイルを識別して複数のレベルに細分化することで、このような問題を回避します。これは、RACF グループ範囲という固有の概念に比べてはるかに柔軟なアプローチであり、組織が RACF グループ・ツリーの厳密な管理を強いられることはなくなります。zSecure は、必要な制御を提供しながら、きわめて柔軟に制御の使用を選択できるようにします。

2.3 監査への即応性およびポリシー・ベースでのセキュリティー・アクセス権の管理を実証する

最後のお客様シナリオでは、ある製造販売会社を取り上げます。この会社は、顧客データを悪用から保護するよう法的に要求される一方で、他社と競合するプログラムや販売プログラムでデータを使用する必要があります。ここでは基本的に 2 つの課題があります。1 つは*この機密データに関して自分が権限を与えたユーザーは誰か*、もう 1 つは*権限を与えたユーザーだけがそのデータを使用していることを示すにはどうすればよいか*ということです。これらの課題に対処するために、この会社ではセキュリティー情報およびイベ

ント管理 (SIEM: Security Information and Event Management) 重視のアプローチを社内のすべてのプラットフォームに適用することを選択しました。

必要な監査関連データとセキュリティー関連データをすべて集中管理するために、複数のプラットフォームにわたって SIEM に対応する単一の統合ソリューションが求められます。すべてのプラットフォームにわたって監査ログとセキュリティー情報を管理するために選ばれたのは、IBM Tivoli Security Information and Event Manager オファリングでした。この会社は、購入した Tivoli Security Information and Event Manager を、手頃な価格の IBM Tivoli Security Management for z/OS オファリングで拡張することを選択しました。

このシナリオでは、Security Management for z/OS オファリングの Tivoli Security Information and Event Manager コンポーネントの実装に焦点を当てます。このデプロイメントは、Tivoli Security Information and Event Manager によって閉じたループの監査が可能になることを実証します。ここでは、IT セキュリティー管理機能に組み込む必要がある継続的な改善サイクルの一環として、実際のユーザー・アクティビティー・ログの分析が使用されます。この製造販売会社では、セキュリティー改善プログラムの後半の段階で、Security Management for z/OS オファリングから追加の機能 (zSecure Admin、Audit、Command Verifier 制御など) を導入する予定です。

Tivoli Security Information and Event Manager のデプロイには、これまでと同様に段階的なアプローチを使用します。フェーズ 1 では、ユーザー・コミュニティーに対して現在定義されている役割と責任を分析し、z/OS 環境で管理されているデータの基本的な分類を行います。フェーズ 2 では、Tivoli Security Information and Event Manager ソフトウェアのインストールと構成を考察し、フェーズ 3 では Tivoli Security Information and Event Manager が提供するレポートと分析の種類、およびこれを使用して基礎となる z/OS セキュリティー構成を改善する方法を説明します。

フェーズ 1　情報の検出

フェーズ 2　インストールと構成

フェーズ 3　RACF を使用した閉じたループの監査

2.3.1 フェーズ 1 - 情報の検出

Tivoli Security Information and Event Manager のインストールを成功させる秘訣は、実際にソフトウェアをインストールする前に、分析および計画の段階で時間をかけることです。このステップを徹底的に実行すれば、Tivoli Security Information and Event Manager の実際のデプロイメントがそれだけ簡単かつ効果的になります。ビジネス・メリットの実現性は、この計画プロセスをどの程度徹底的に行ったかに比例します。

この会社の事例では、監査ログ分析のターゲット・システムが RACF であることが幸いしています。RACF では、アクセス要件を共有するユーザーの集合として、グループという概念を採用しています。Tivoli Security Information and Event Manager では、これらのユーザー・グループを、ユーザーを分類する基本的な方法として使用できます。この場合、RACF に定義されているユーザー・グループが、実際に共通のアクセス要件にマップされていることが前提となります。マップされていない場合は、zSecure Admin を使用してこの RACF 構成の問題を是正することができます。RACF でユーザー・グループが明確に定義されておらず、かつグループを変更したくない場合は、Tivoli Security Information and Event Manager メタデータを代わりに使用して、RACF システム上のさまざまなユーザー・カテゴリーを適切に定義することも可能です。

ユーザー分類テンプレート

このシナリオでは、RACF グループが既に明確に定義され、管理されているため、これらのグループを使用してユーザー・コミュニティーをさまざまなタイプに分類できます。分析か

ら、この z/OS システム上のユーザーは以下の主要なカテゴリーに分類されることがわかりました。

1. 財務
2. 管理者
3. 部門責任者
4. 販売
5. IT サポート・スタッフ
6. 人事
7. マーケティング
8. ユーザー (管理者以外の全ユーザー)
9. その他 (システム、アプリケーション、開始タスク、またはその他の IT システムに関連する機能別ユーザー ID (スタッフ以外が使用) を含む)

データ分類テンプレート

Tivoli Security Information and Event Manager で使用できる基本的なユーザー分類を作成しました。次に、システムで管理されるデータを同様に分類します。この場合も、z/OS と RACF が採用されていることが幸いしています。z/OS 環境で使用される一般に強力な命名規則によって、このデータの識別と分類がはるかに容易になるためです。システム上のデータを、以下の主要なタイプに分類しました。

1. 財務データ
2. 人事データ
3. システム・データ
4. 顧客データ
5. システム・テスト・データ
6. その他の分類不能なデータ

このレベルに詳細化することで、比較的単純であるが機能的なフレームワークの中で、Tivoli Security Information and Event Manager ソリューションをデプロイできます。最初に単純なフレームワークを定義し、このフレームワークに対する基本的なレポートを取得した後に、ユーザーとデータをさらに細かく分類していく中で、フレームワークを改良することが可能です。

2.3.2 フェーズ 2 - インストールと構成

Tivoli Security Information and Event Manager は、WindowsÆ サーバーにインストールされ、監査対象の z/OS LPAR にインストールされている Tivoli Security Information and Event Manager エージェントを使用して z/OS 環境に接続されます。z/OS 用のエージェントは、標準の z/OS SMPE プロセスを使用してインストールされます。SMF データは、z/OS UNIX システム・サービス・コンポーネントに対するリモート・プロシージャー・コール (RPC) を使用して、z/OS システムから定期的に (Tivoli Security Information and Event Manager の Windows 管理コンソールで定義される) 収集されます。その後に z/OS UNIX システム・サービスが CARLa 処理エンジン (従来の z/OS 実行可能ライブラリーにインストール済み) を呼び出して、Tivoli Security Information and Event Manager サーバー上の集中型ログ管理リポジトリーに SMF のデータを暗号化および圧縮して伝送できるように準備します。

Tivoli Security Information and Event Manager が正常にインストールされ、SMF データが z/OS LPAR から正しく受信されたら、z/OS ユーザー向けの許容されるデータ使用ポリシーを定義できます。この作業は、コンプライアンス・ダッシュボードと呼ばれる Tivoli Security Information and Event Manager サーバーとのブラウザー・インターフェースを使用して行います。コンプライアンス・ダッシュボードでは、一連のポリシーを作成してアーカイブし、収集されたデータをマップする際に使用されるポリシーを選択できます。複数のポリシーを定義して、実現されるコンプライアンス・レベルを 複数のポリシーの間で比較

するのが有効な手法です。Tivoli Security Information and Event Manager は、ポリシーに対してソース・データをマップした後で初めてそのレポートを適用するため、過去または現在のいずれかのソース・データを使用して、過去のポリシーからレポートを生成することができます。このアプローチにより、ポリシーが時間とともに改善されていること、およびポリシーへのコンプライアンスのレベルが上がっていることを実証できます。

ユーザーおよびデータの分類を実行することで、ポリシーに複数のルールを実装する必要があることが即座にわかります。

- 財務と人事のユーザー (前出のリストのユーザー・タイプ 1 と 6) は、財務と人事の実動データにアクセスできます。
- アプリケーションとタスクに関連するユーザー (タイプ 9) は、全データにアクセスできます。
- エンド・ユーザー (タイプ 8) は、人事、財務、顧客の各実動データにのみアクセスできます。
- 販売ユーザー (タイプ 4) は、その役割に関連する実動データ (顧客) にのみアクセスできます。
- システム管理者 (タイプ 2) は、システム、テスト、およびその他のデータにのみアクセスできます。
- IT サポート・スタッフ (タイプ 5) は、システム、テスト、およびその他のデータにのみアクセスできます。
- マーケティング・エンド・ユーザー (タイプ 7) は、財務、顧客、その他の各実動データにのみアクセスできます。
- 部門責任者 (タイプ 3) は、実動データにアクセスできません (経営幹部は管理レポートを通じてデータにアクセスします。これらのユーザーは、z/OS データに直接アクセスする必要がありません)。

許容される使用ポリシーを定義するために、表 2-1 に示すマトリックスを作成します。このマトリックスにより、ユーザー分類とデータ分類の関係をより的確に把握した上で、誰にどのデータへのアクセスを許可すべきかを定義できます。

表 2-1 ユーザー分類とデータ分類のマトリックス

	財務	人事	システム	顧客	システム・テスト	その他
財務	OK	OK	OK	x	x	OK
管理者	x	x	OK	OK	OK	OK
責任者	x	x	x	x	x	OK
販売	x	x	x	OK	x	OK
IT スタッフ	x	x	OK	x	OK	OK
人事	x	OK	x	x	x	OK
マーケティング	OK	x	x	OK	x	OK
エンド・ユーザー	OK	OK	x	OK	x	OK
その他	x	x	x	x	OK	x

この表のすべての関係を網羅するには多数のポリシー・ルールが必要になるように思われますが、Tivoli Security Information and Event Manager の設計では、許容されるアクセス行

動をポリシーに指定するだけで済みます。ポリシーで明確に規定されていない、データへのユーザー・アクセスは、違反と見なされて報告されます。マトリックスの各「OK」ボックスに対してルールを定義する必要があります。つまり、この段階でポリシー・ルールの総数は 24 個になります。これらのポリシーを、Tivoli Security Information and Event Manager で Policy Explorer を使用して z/OS 監査ポリシーに対して定義できます。

収集された SMF データに対して次に Tivoli Security Information and Event Manager のマッピングを実行すると、コンプライアンス・ダッシュボードに臨時の結果が表示されます。図 2-6 に示すように、この結果には、各タイプのユーザーおよびデータをマップする際に入力したメタデータを使用して、組織が緊急に調査する必要がある領域が示されます。

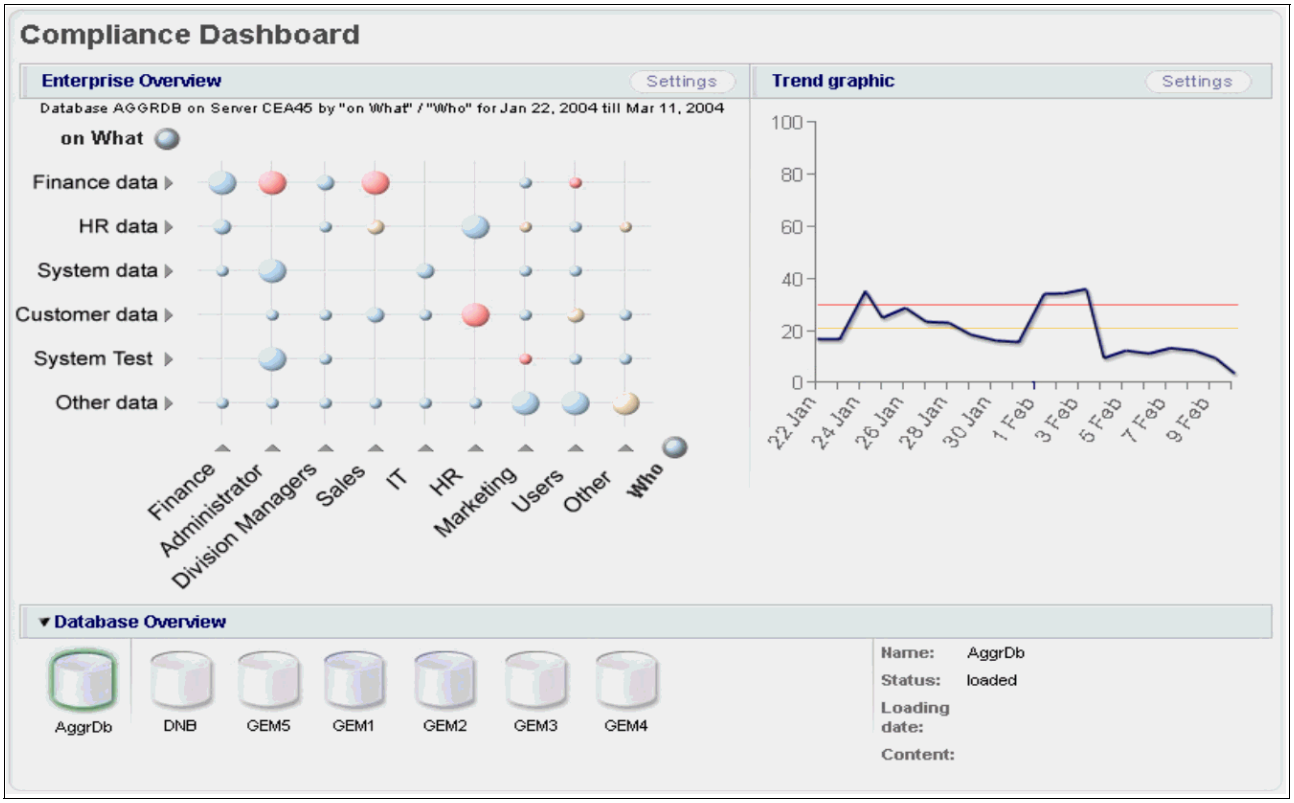
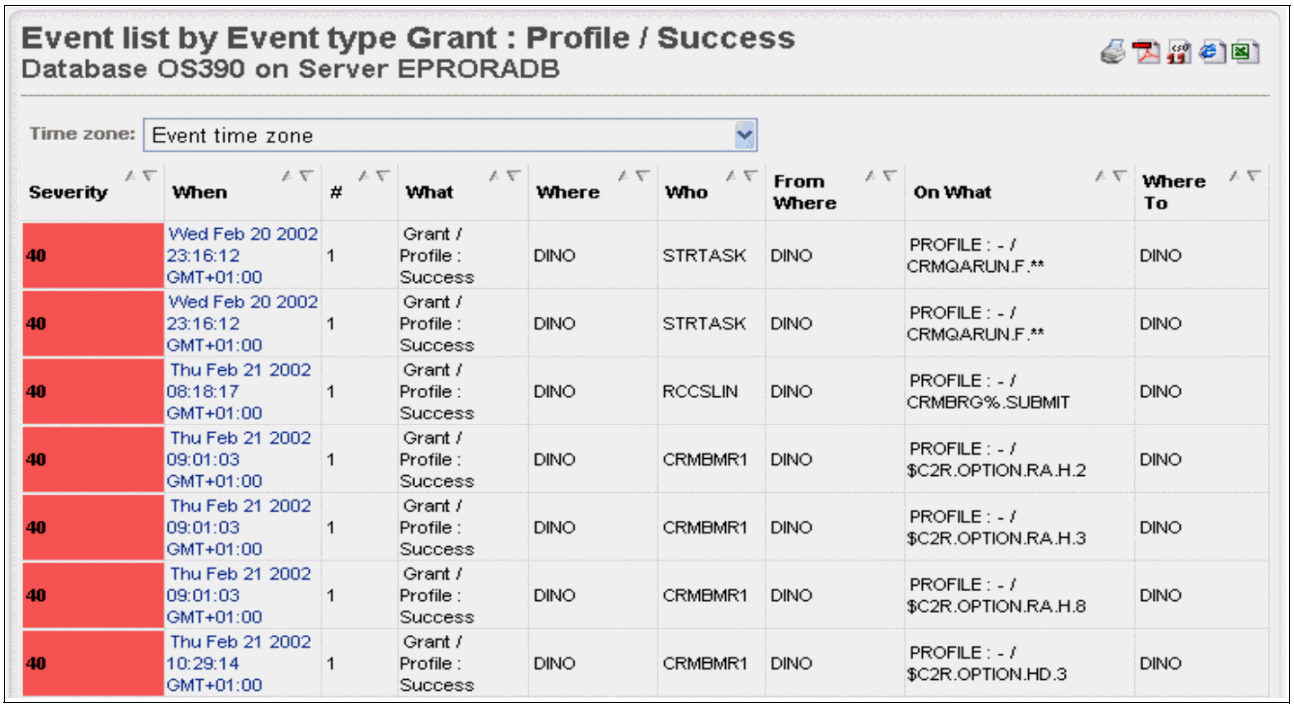


図2-6　コンプライアンス・ダッシュボードの「エンタープライズの概要」

Tivoli Security Information and Event Manager では、あるタイプのユーザーによる、あるタイプのデータへのアクセスがポリシーで許可されていない場合に、そのアクセスが強調表示されます。図 2-6 に示すレポートでは、以下の問題領域が即座にわかります。

- 管理者が財務データにアクセスした。
- 販売役割のユーザーが財務データにアクセスした。
- 人事ユーザーが顧客関連データにアクセスした。

次のステップでは、これらの例外に悪意がないかを調査する必要があります。このデータへのアクセスに悪意がなかった場合は、ポリシーを改良する必要があります。この調査では、Tivoli Security Information and Event Manager を使用して、ポリシー違反および関係する RACF プロファイルを示しているログ・レコード内の、詳細な SMF 情報のレベルまでドリルダウンできます。この情報を使用して、このコンプライアンスに反したデータの使用を許可した RACF データベースの状態を修正することができます。イベント・リストの例を 34 ページの図 2-7 に示します。



Event list by Event type Grant : Profile / Success
Database OS390 on Server EPRORADB

Time zone: Event time zone

Severity	When	#	What	Where	Who	From Where	On What	Where To
40	Wed Feb 20 2002 23:16:12 GMT+01:00	1	Grant / Profile : Success	DINO	STRTASK	DINO	PROFILE : - / CRMQARUN.F.**	DINO
40	Wed Feb 20 2002 23:16:12 GMT+01:00	1	Grant / Profile : Success	DINO	STRTASK	DINO	PROFILE : - / CRMQARUN.F.**	DINO
40	Thu Feb 21 2002 08:18:17 GMT+01:00	1	Grant / Profile : Success	DINO	RCCSLIN	DINO	PROFILE : - / CRMBRG%.SUBMIT	DINO
40	Thu Feb 21 2002 09:01:03 GMT+01:00	1	Grant / Profile : Success	DINO	CRMBMR1	DINO	PROFILE : - / $C2R.OPTION.RA.H.2	DINO
40	Thu Feb 21 2002 09:01:03 GMT+01:00	1	Grant / Profile : Success	DINO	CRMBMR1	DINO	PROFILE : - / $C2R.OPTION.RA.H.3	DINO
40	Thu Feb 21 2002 09:01:03 GMT+01:00	1	Grant / Profile : Success	DINO	CRMBMR1	DINO	PROFILE : - / $C2R.OPTION.RA.H.8	DINO
40	Thu Feb 21 2002 10:29:14 GMT+01:00	1	Grant / Profile : Success	DINO	CRMBMR1	DINO	PROFILE : - / $C2R.OPTION.HD.3	DINO

図2-7　詳細なイベント・リスト

2.3.3 フェーズ 3 - RACF を使用した閉じたループの監査

Tivoli Security Information and Event Manager が効果的にデプロイされ、z/OS アクティビティーの監査レポートを生成するようになったので、これらのレポートを確認し、ポリシーからの逸脱が強調表示されている場合は調査します。その後に RACF に戻り、そのユーザーのポリシー違反を可能にしたアクセス許可をすべて除去します。

この段階では、収集されたログ・データを使用して、セキュリティー・システム自体のセキュリティーの管理と改善を進めます。これによって、すべてのセキュリティー管理者が長年抱えていた*セキュリティー・データベース内で付与されているアクセス権はユーザーの職務に本当に適しているのか*という疑問は解消されます。Tivoli Security Information and Event Manager では、この疑問を解消するために、宣言されているポリシーに対する実際のユーザー・アクティビティーからのフィードバックを提供して、セキュリティー定義の改善を支援します。

また、Tivoli Security Information and Event Manager は、収集されたログ・データを使用するレポート・エンジンを備え、非技術系スタッフがブラウザー・ベースのユーザー・インターフェースから簡単にアクセスできるようになっています。このため監査員は、以前から必要としていた詳細な照会を、専門の技術系スタッフの支援を受けることなく独自に実行できます。この状況は、監査員から質問された時点で技術系スタッフが自らのアクティビティーについてレポートを作成する場合に比べてはるかに理想的です。35 ページの図 2-8 では、ISO 17799 関連レポートが、非技術系監査員が簡単に選択できるブラウザー・ベースのリストで示されています。

図2-8　簡単にアクセスできるISO 17799 レポートのリスト

2.3.4 シナリオ 3 のまとめ

Tivoli Security Information and Event Manager では、さまざまなプラットフォームからのログの収集と保管を自動化することができます。ここでは、特殊なケースとして z/OS プラットフォームを監査するためにのみこの製品を使用していますが、さらに幅広いエンタープライズ・デプロイメントへといつでも拡張できます。

Tivoli Security Information and Event Manager で効果的な監査レポートを出力するために実装されたステップは以下のとおりです。

1. z/OS 用の Tivoli Security Information and Event Manager エージェントで自動ログ収集を使用して z/OS から SMF データを収集します。
2. Tivoli Security Information and Event Manager ポリシーを定義します。
3. このポリシーに対して、初期の分析で明らかとなったユーザーとデータの分類を定義します。
4. 定義したユーザー分類による定義したデータ分類の許容された使用方法に基づいて、新規ポリシー内でポリシー・ルールを作成します。
5. このポリシーに対して必要なアテンション・ルールを作成し、必要に応じてアラートを関連付けます。
6. 収集されたデータをロードします。Tivoli Security Information and Event Manager によって、このデータにポリシー内のルールがマップされ、許容された使用ポリシーからの逸脱が直ちに強調表示されます。

Tivoli Security Information and Event Manager のデプロイメントと構成について詳しくは、37 ページの『関連資料』を参照してください。

2.4 まとめ

この章では、Tivoli Security Management for z/OS ソリューション・バンドルの各種コンポーネントをそれぞれに使用する 3 例のまったく異なるお客様シナリオを考察しました。各シナリオでは、それぞれ異なるビジネス上および技術上の要件に焦点を当てながら、各顧客がこの一連の統合製品をさらに活用することを選択した場合に、他のシナリオで紹介したすべての機能を自由に利用できることに触れました。

簡単にまとめると、各顧客が以下の懸案事項にどのように対処したかを説明しました。

- z/OS セキュリティー環境が適切に管理され保護されていることを、内部と外部の監査員に納得させる。
- zSecure Admin と zSecure Audit を使用してベースラインの改善点、およびベースラインの変化の自動トラッキングを実装して、重要な RACF リソースが特権を持つ内部関係者によって悪用されないように保護する。
- zSecure Command Verifier と zSecure Admin を併用して管理チーム内の分離を実装して、労力とリスクを緩和する。
- 拡張と改良が可能な z/OS 用のシンプルな監査プロファイルである Tivoli Security Information and Event Manager をデプロイすることで、監査の即応性およびポリシー・ベースでのセキュリティー・アクセス権の管理を実証し、その一方で監査員に直接の ROI を示し、セキュリティー実装の継続的な改善へのフィードバックを提供する。

IBM Tivoli Security Management for z/OS v1.11 ソリューション・バンドルは、z/OS RACF ベースのシステムを保護する際に直面していた従来の問題に対する最新の包括的なアプローチを提供します。

関連資料

このセクションにリストされている資料は、本書で扱われているトピックに関する詳細を学習するのに特に適していると思われる資料です。

IBM Redbooks

これらの資料の注文については、37 ページの『Redbooks の入手方法』を参照してください。なお、ここに参照されている資料の中には、ソフトコピーでしか提供されていないものもあります。

- *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager* (SG24-7530)
- *z/OS Mainframe Security and Audit Management using IBM Tivoli zSecure* (SG24-7633)
- *Enterprise Security Architecture Using IBM Tivoli Security Solutions* (SG24-6014)

オンライン資料

IBM Tivoli Security Management for z/OS V1.11 製品スイートについて詳しくは、次の資料を参照してください。

- Tivoli zSecure Suite Version 1.11 インフォメーション・センター

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.zsecure.doc/welcome.html
- Tivoli zSecure Suite の詳細情報は、以下のサイトでも入手できます。

  http://www.ibm.com/software/tivoli/products/zsecure/
- Tivoli Security Information and Event Manager V2.0 インフォメーション・センター

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tsiem.doc/welcome.html
- Tivoli Security Information and Event Manager の詳細情報は、以下のサイトでも入手できます。

  http://www.ibm.com/software/tivoli/products/security-info-event-mgr/index.html

Redbooks の入手方法

以下は英語のみの対応となります。以下の Web サイトでは、Redbooks、Redpapers、技術情報、ドラフト文書、およびその他の追加資料の検索、閲覧、またはダウンロードができるほか、ハードコピー版の Redbooks を注文できます。

ibm.com/redbooks

IBM からの支援

IBM サポート & ダウンロード

ibm.com/support

IBM グローバル・サービス

ibm.com/services

- IBM Tivoli Security Management for z/OS でより堅牢に -
z/OS RACF 環境におけるセキュリティー / コンプライアンス管理

Redpaper™

メインフレーム・セキュリティーを管理する一方で管理にかかる時間、労力、コストを削減

監査およびコンプライアンスの取り組みのシームレスな統合を活用

メインフレーム・セキュリティーを強化する一方で複雑さを軽減

どの組織にも、保護が必要な、中核となる一連の基幹業務データがあります。セキュリティーが失効したりセキュリティーに障害が発生したりすると、単に混乱を招くだけではなく、壊滅的な事態を引き起こすおそれがあり、その結果は企業全体に影響します。特権ユーザーの不注意なミスだけでも、意図しない構成エラーや不注意なセキュリティー・コマンドによって多額の損害をもたらすことがあります。悪意のあるユーザーがアクセス権限を持つと、さらに大きな損害を招くことがあります。このため、セキュリティー管理は企業の機密データを適切に保護する上で大きな課題に直面します。さらに、IT スタッフは、ますます増える要求に時間を取られながらも、詳細な監査および管理文書の提出を要求されます。

セキュリティーおよびコンプライアンスのプロセスを自動化し、簡素化することにより、これらの課題に対処し、効果的で持続可能なユーザー管理ソリューションおよび監査ソリューションを確立することができます。これには、セキュリティー・データベースのクリーンアップ、構成および設定の反復可能な監査、および変更とイベントの能動的モニタリングが含まれます。IBM Tivoli Security Management for z/OS V1.11 は、これらのソリューションを提供して、自動化された監査および管理を通じてメインフレーム・システムのセキュリティー強化を支援します。

この IBM Redpaper 文書では、Tivoli Security Management for z/OS によって、z/OS、RACF、および DB2 から得たメインフレーム・セキュリティーの情報を企業の監査とコンプライアンスのソリューションに送る仕組みを説明するとともに、z/OS、RACF、および DB2 から得たメインフレーム・データを他のオペレーティング・システム、アプリケーション、およびデータベースのデータと結合して、包括的なログ・データを取得し、先進的なログ分析を通じてそのデータを解釈し、その結果を企業全体の監査およびコンプライアンスに関するレポート作成のために効率的かつ合理的に伝達する方法を説明します。

SG88-4059-00

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

経験に基づく技術情報の構築

IBM Redbooks は、IBM International Technical Support Organization により開発されています。世界中の IBM の専門家、お客様、およびパートナーが、現実的なシナリオに基づいたタイムリーな技術情報を作成しています。具体的な推奨事項が提供されているため、ご使用の環境でより効率よく IT ソリューションを実装することができます。

詳しくは次にアクセスしてください。
ibm.com/redbooks