NPO法人日本システム監査人協会　近畿支部
第154回　定例研究会

ツールが無くてもここまでできる
SAP ERP内部統制監査

2015年9月18日

三洋電機株式会社
品質・業務推進センター　IT統制推進部
（現パナソニックインフォメーションシステムズ（株）グループIT統制支援室）

於：大阪大学　中之島センター　講義室702

S-ITCPD

1. 三洋電機㈱でのシステム監査の歴史
2. SAP監査のグローバル傾向
3. 職務分掌の評価（職務の分離と実行権限の付与）
4. SAP標準機能を活用した監査手法
5. 内部統制レベルアップへの取り組み
6. 参考文献

0.メンバー紹介

- 浦上豊蔵
  システム監査技術者, 公認システム監査人（CSA), 第1種情報処理技術者, MBA（ボストン大学）
  組込システムの開発を経て, 社内情報システムの企画・開発および業務プロセス(SCM)改革を責任者として推進，その後システム監査に従事。監査室　IT上席担当部長，三洋インフォメーションシステムズ(株)監査室長，サンヨーノースアメリカ　IT担当VP，パナソニックグループ海外システム監査統括担当を歴任, 2015年三洋電機退職
  所属：システム監査学会, NPO日本システム監査人協会, NPOシステム監査普及機構, ISACA監査基準研究会
  共著：IT内部監査人(2010)
- 梅谷正樹
  システム監査技術者, 情報セキュリティスペシャリスト, データベーススペシャリスト, ネットワークスペシャリスト, プロジェクトマネージャ, ソフトウェア開発技術者, ISMS審査員補, BATIC(コントローラーレベル)
  三洋電機，パナソニックグループにおいて，IT統制の推進・監査リーダーを担当
  SAP，Oracle EBSの監査技法開発，CAAT技法開発などを牽引
- 下田あずさ
  システム監査技術者, 公認システム監査人（CSA), Oracle Master Silver, ISMS審査員補
  アパレルメーカー等での生産管理システムの導入, 情報システム会社での外販システムの開発や，外資系会社のオフショア開発・システム運用，内部統制対応の業務受託等を経て, 三洋電機勤務。内部統制監査, 英語研修コンテンツ作成と研修講師, パナソニックIT統制監査受託業務を担当。SAP・Oracle EBS等のERPシステム監査技法や，不正監査技法開発等の業務に従事。
  所属：NPO日本システム監査人協会, ISACA監査基準研究会　　共著：IT内部監査人(2010)
- 木ノ原真由美
  PMP, 第1種情報処理技術者, ISMS審査員補, ITIL Foundation
  本社情報システム部門および情報子会社でSEとしてグループ内情報システム(営業システム，生販在システム)の企画・開発・運用
  UNISYS, IBMホスト, オープン系のシステム構築, PMに従事。その後, システム監査および内部統制監査教育を担当。SAP教育用サーバーを英子会社に設置し，SAPの実践的監査手法をメンバーと共に研究し監査に適用。 共著：IT内部監査人(2010)
- 中川昭仁
  公認情報システム監査人（CISA），　ISMS審査員補
  三洋電機で情報関連商品の商品企画、販売企画、マーケティングを長年担当。業務改革の一環で、SFAシステム、営業管理システムを開発。その後、三洋電機営業系システムの責任者，サービス系システムの責任者など歴任
  三洋電機㈱IT統制責任者(現職)として、SAP，Oracle EBSの監査技法開発，CAAT技法開発など推進

1．三洋電機㈱でのシステム監査の歴史

1-1.三洋電機㈱でのシステム監査の歴史

1987頃 ～ 1990頃

＜黎明期＞

- 三洋電機監査室でシステム監査担当を１名配置
- 本社情報システム部門を対象にシステム監査基準に基づく監査

- システム監査担当の退職に伴い中断

1999 ～ 2005

＜IT業務監査＞

- 監査体制強化策としてシステム監査チームを担当２名で発足
- 三洋電機㈱及び国内子会社を対象に，ＩＴ業務監査，情報セキュリティ監査，ソフトウェアライセンス監査

2006 ～ 2010

＜内部統制（J-SOX）監査＞

- システム監査チームの増強　担当７名
- 事業所情報システム部門間のクロス監査体制を構築
- 三洋電機㈱及び国内外子会社の内部統制（J-SOX）の指導と監査

2011 ～ 現在

＜内部統制（US-SOX）※1 監査・情報セキュリティ監査＞

- パナソニック子会社化に伴い，監査体制の準拠と統制評価の統一
- システム監査チームを，本社情報システム部門へ移籍
- 三洋電機㈱及び国内外子会社の内部統制（US-SOX）の指導と監査

※1 2013年3月パナソニックUS上場廃止に伴い，以降はJ-SOX

■ 海外標準システム
2000年問題の対応を機に，海外子会社にSAP　R/3を展開
国内外　26拠点/165拠点で導入
→　J-SOX内部監査対象としてSAPは重要システム

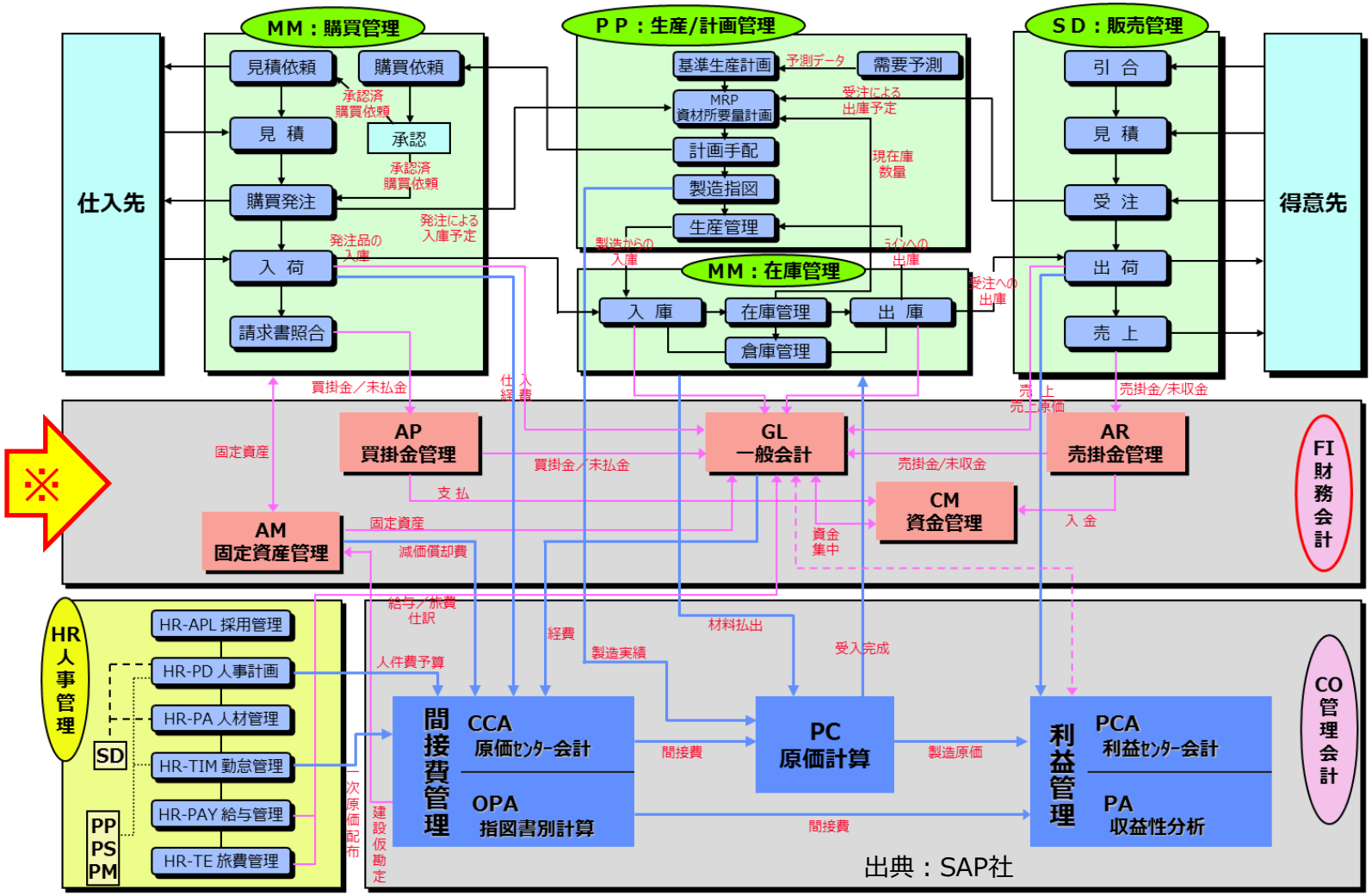
■ 外部監査における監査の傾向
国内：　自動化統制の動作検証 (公認会計士協会　IT委員会研究報告第31号 Q15)
海外：　職務分掌(SoD)に応じたアクセス権の妥当性

■ 内部統制評価の厳格化
職務分掌：　IT部門 / 業務部門
→ 業務部門間 (経理 / 販売 / 購買 / 物流)
→ 業務担当間（伝票入力 / 承認)

■ 課題
2007年以前に導入されたSAPシステムは，内部統制対応が十分に考慮されていない

内部統制に関わるSAPシステムの詳細知識が必須
SAP監査技法を開発と内部統制の高位平準化

1-3.[前提知識]SAPシステムの特徴

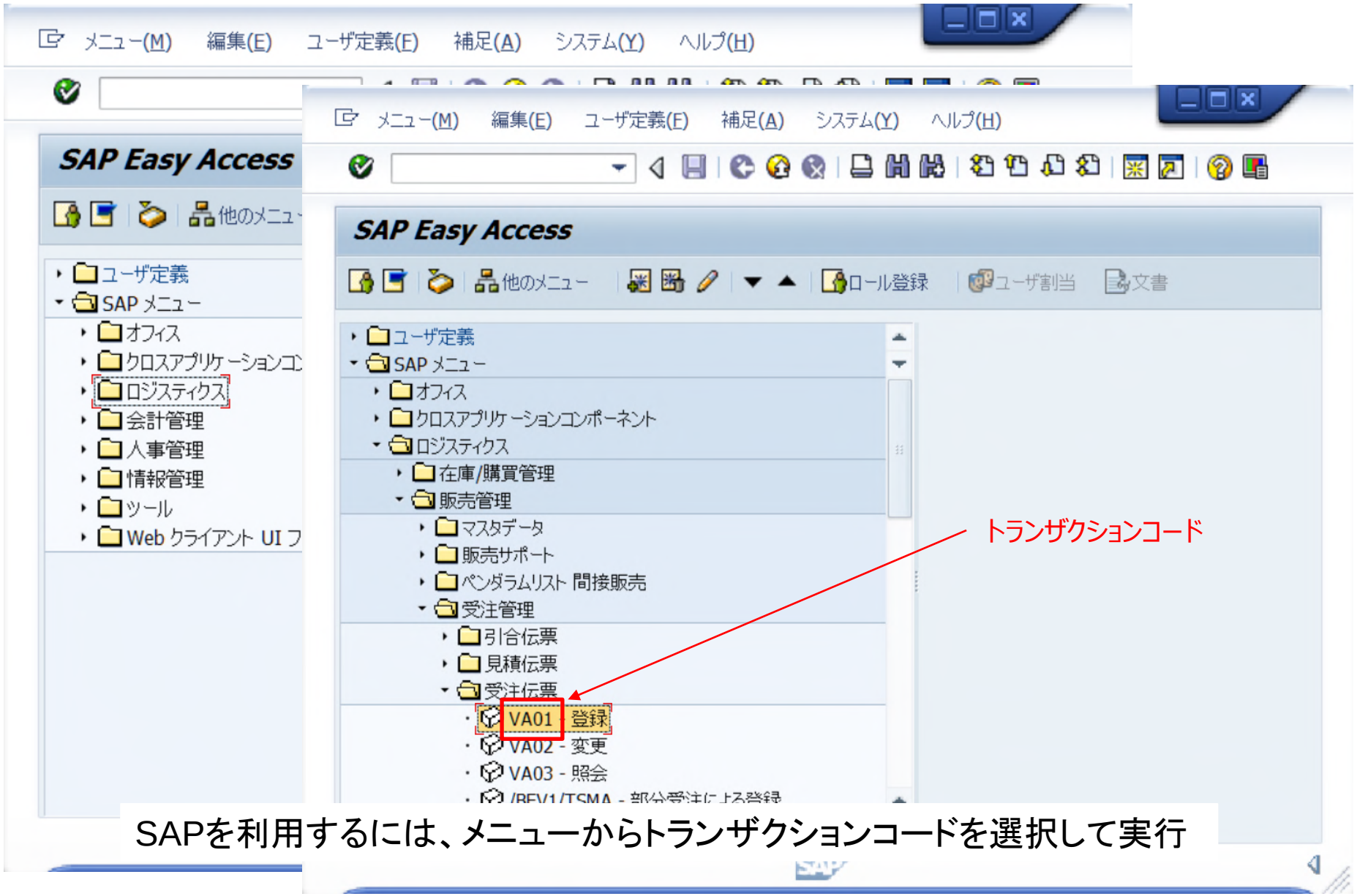


会社運営に必要な業務機能が網羅されており、すべての業務データが会計システムに連携しているという特徴がある。※

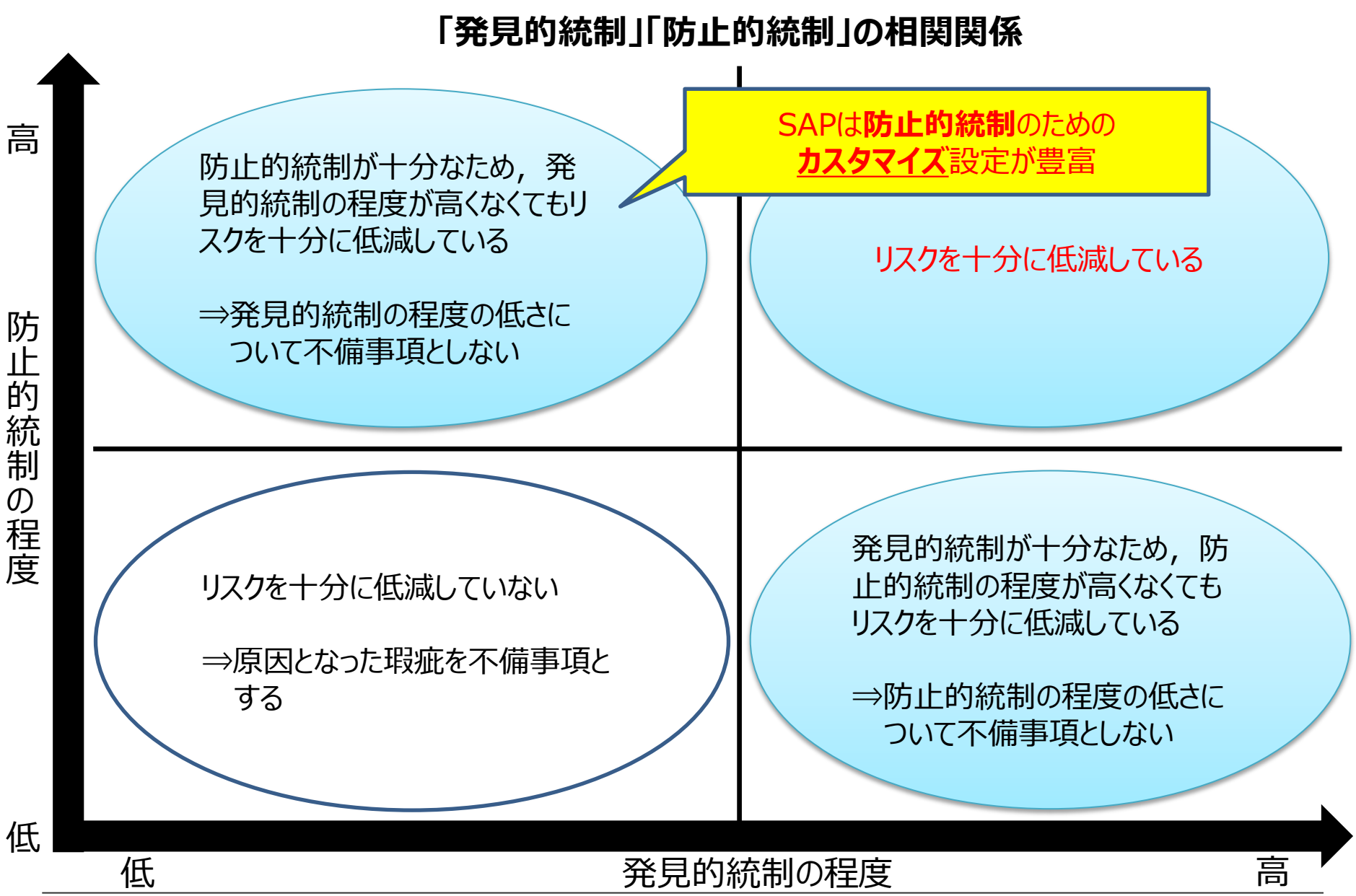
SAPシステム内では、関連する業務データはリアルタイムに更新される。

- 最新版はSAP ECC 6.0。 2025年までのサポートが保証されている。
- SAP 4.6C, 4.7, 5.0 はすでにサポートが終了しているが、不具合が発生しにくいため，継続利用されている場合がある。
- 社内では複数のバージョンが混在してるが、基本的に機能が継承されているため、一度習得した監査手続きを継続的に適用できる

2000/5	• SAP R/3 4.6C	
2002/7	• SAP R/3 ENTERPRISE 4.7X110	
2002/9	• SAP R/3 ENTERPRISE 4.7X200	
2004/6	• SAP ECC 5.0	2013年3月まで
2005/10	• SAP ECC 6.0	2025年まで SAP Business Suite 7を含む



SAPを利用するには、メニューからトランザクションコードを選択して実行


「発見的統制」「防止的統制」の相関関係
高
防止的統制の程度
低
防止的統制が十分なため，発見的統制の程度が高くなくてもリスクを十分に低減している
⇒発見的統制の程度の低さについて不備事項としない
SAPは防止的統制のためのカスタマイズ設定が豊富
リスクを十分に低減している
リスクを十分に低減していない
⇒原因となった瑕疵を不備事項とする
発見的統制が十分なため，防止的統制の程度が高くなくてもリスクを十分に低減している
⇒防止的統制の程度の低さについて不備事項としない
低
発見的統制の程度
高

2. SAP監査のグローバル傾向

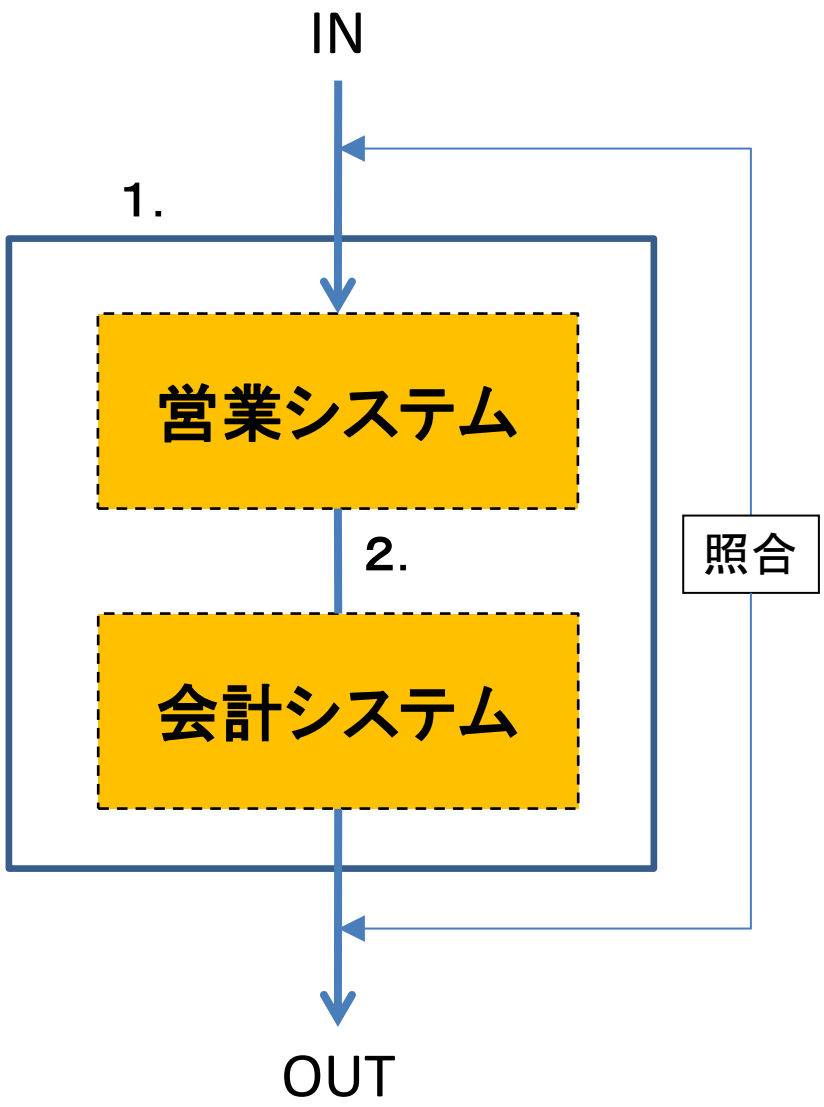
■公認会計士協会　ＩＴ委員会研究報告第31号　　平成18年3月17日
IT委員会報告第3号「財務諸表監査における情報技術（IT）を利用した情報システムに関する重要な虚偽表示リスクの評価および評価したリスクに対応する監査人の手続きについて」 Q&A　から抜粋し要約

Q15：ERPシステムが利用されている際のリスク評価手続き及びリスク対応手続きにおける留意点はどのようなものでしょうか。

ERPであっても処理の正確性、網羅性の確認が求められる

1.　業務処理統制の観点
- ①　ユーザマニュアルがあってもシステム使用の説明が明確でない場合がある
- ②　組込まれた内部統制機能を利用せずに業務が行われる場合がある
- ③　リアルタイム会計システムに連携する他の業務システム（機能）への入力業務
- ④　従来の業務手続きの踏襲とERPシステムの機能の不一致への対応

2.　全般統制の観点
- ①　業務パラメータ設定の妥当性のテスト，承認，事後検証等の管理手続き
- ②　機能の追加開発に関する手続き



1. ERPシステムに組み込まれた機能を，その設計時の想定したデザイン通りに利用するような統制があるかを評価

2. 業務の取引データがリアルタイムで会計データに反映されることを原則とするため，会計システムと連携する業務システムのデータインプットの正当性，網羅性，正確性などの確保の検証の実施状況を評価

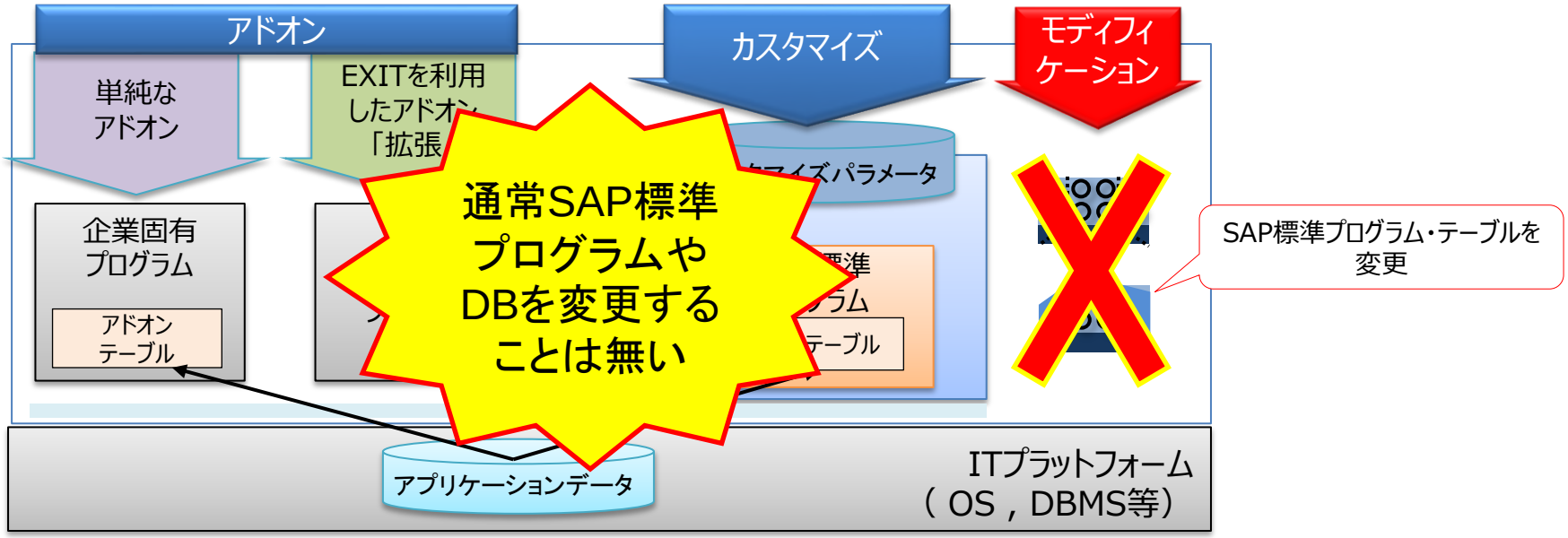
→IN-OUTの照合で処理の正確性、データの網羅性等を検証する

3. プログラム変更の検証も同じ手続きで行う
（変更が無いことの確認も含む）

出典：日本公認会計士協会　ＩＴ委員会研究報告第31号
「ＩＴ委員会報告第３号「財務諸表監査における情報技術（ＩＴ）を利用した情報システムに関する重要な虚偽表示リスクの評価及び評価したリスクに対応する監査人の手続について」Ｑ＆Ａ　から抜粋し要約

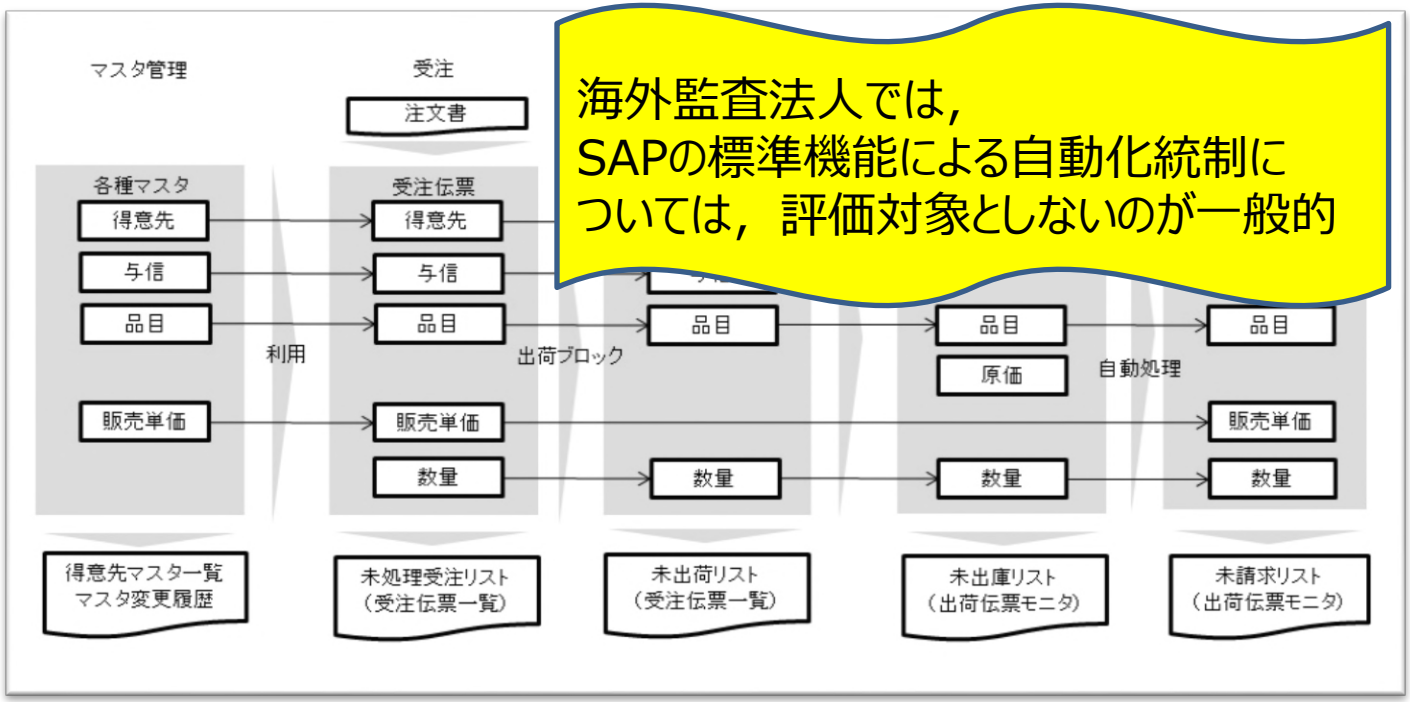
2-7.SAPのカスタマイズ・アドオンとモディフィケーション

カスタマイズ	•開発者が専用画面でカスタマイズパラメータを設定変更することによりシステムの動作を変更すること •実際のプログラミング（ソース記述）は伴わない •リリースアップ時に自動的に移行される
拡張	•ＳＡＰ標準プログラムにあらかじめ組み込まれた「Exit」に企業固有のプログラムを追加 •拡張はアドオンの一種であるが，リリースアップの影響を受けにくい
アドオン	•ＳＡＰ標準のプログラムを変更しないで，外付けで追加すること •新たにプログラムやテーブルを追加すること（アドオン・テーブル） •バージョンアップ時に動作検証が必要となる
モディフィケーション (原則実施しない)	•ＳＡＰ標準のプログラム，テーブルを変更すること •モディフィケーションを実施するとＳＡＰ社のサポートが受けられなくなり、バージョンアップ時の動作保証がなくなる



2-8.SAPの自動化統制の評価

モディフィケーションしない場合、
SAPの自動化処理の妥当性は，伝票フローで確認することができ、
処理の正確性、網羅性はSAPの標準機能として保証される



伝票フローの画面

各伝票明細を見るときは
アイコンをクリック

受注伝票
出荷伝票
出荷指示票
出庫伝票
請求伝票
売上伝票（会計）

特権ユーザおよび
ユーザアクセス権に関
する指摘が多数を占
めている

SAP監査では職務分掌とそのアクセス権の評価が重要

これまでの監査不備事例

- 職務分掌の逸脱

  初期導入時/組織再編時に職務を十分に考慮せず，必要の無い権限を付与

- 高権限の限定付与の未実施

  高権限の過剰な付与や，高権限操作者に対するモニタリングの未実施

これらは主に外部監査不備
外部監査では，SAPシステムから直接証跡データを取り出し検証している
現状では外部監査が内部監査より先行しており詳細な確認を行っている

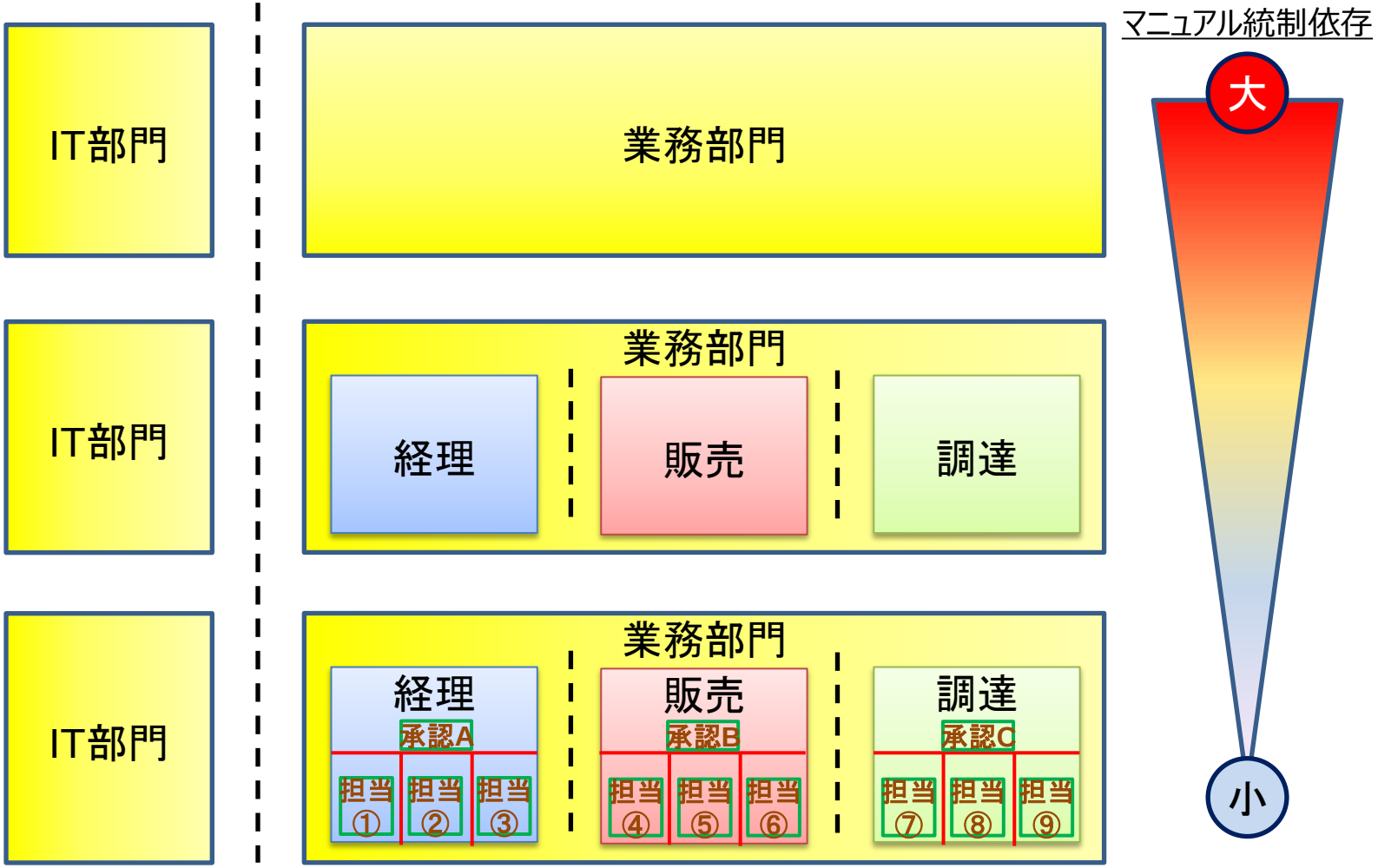
内部監査でもSAPの専門知識を備え，外部監査のレベルに追随していく必要がある
また，内部監査人自らSAPにログインして検証を行うことが有効である

３．職務分掌の評価

（職務分掌に応じた権限の割り当て）

3-1.職務分掌評価の厳格化

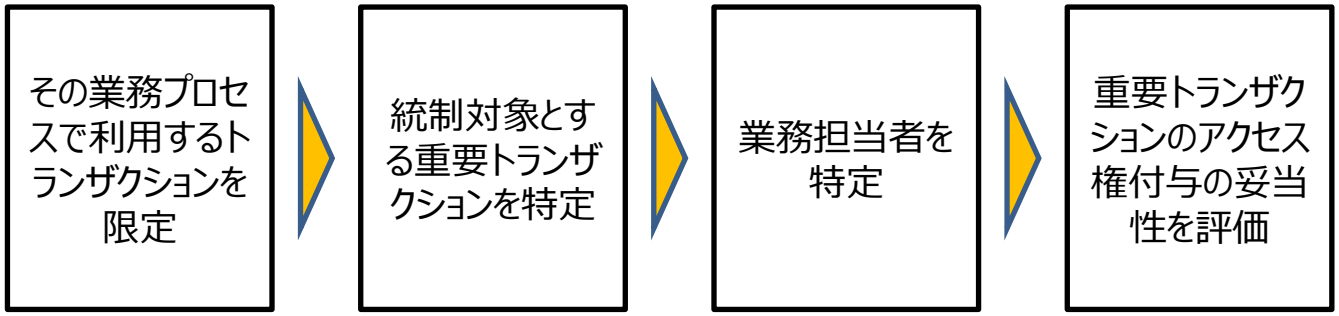
当初は、業務機能優先で内部統制対応が十分に考慮されていなかった
業務部門の役割を明確にすることからスタートしたが、現在では担当者レベルまで
職責に応じた権限の確認が求められている



3-2.職務分掌に関わる重要トランザクションの特定

- SOX監査当初は，ユーザに過剰なトランザクション権限を付与しているSAPシステムが大多数
- SAPには6万個以上のトランザクションがあり，すべてのトランザクションに対して職責に関わる統制を網羅的に把握するのは困難
- そのため、統制に関わる重要トランザクションを特定し、権限付与の妥当性の評価から実施
  - マスターデータ（取引先・品目・勘定科目）の登録・更新
  - 伝票（受注・出荷・発注・検収・請求・会計等）の登録・更新
  - 与信限度額の変更
  - ユーザID情報の登録・変更

➢ ○○プロセスの評価手続き



- 最近の傾向として，**不正防止の観点**が重要視されている

SOX監査　不備なし

- 手続きの準拠性を評価
- サンプリング評価
- 監査対象拠点の限定

不正発覚

- 規程・基準・手続きの脆弱性
- サンプリング評価の限界

不正リスクを考慮した監査の要求

衝突する特定トランザクションの付与を禁止し、不正の機会を抑止

➢ ○○プロセスの評価手続き

その業務プロセスで利用するトランザクションを限定 → 統制対象とする重要トランザクションを特定 → 業務担当者を特定 → 重要トランザクションのアクセス権付与の妥当性を評価 → 不正シナリオに基づき，権限の衝突の有無とモニタリングの妥当性評価

3-4.不正防止を考慮した職務分掌(SOD)ルール

一般的な不正リスクシナリオから始めて，その不正を防止するという観点でSODルールを考え、その上でSAPで実現可能なコントロールを明確化する
いかに過剰なコントロールとならないようにするかがポイントとなる

不正リスクシナリオ	SODルール	SAPでのコントロール
・得意先マスタの更新 ・受注処理 上記の権限を同一ユーザに付与することにより、架空の得意先を作成し，架空の受注・出荷処理が実施でき、商品が架空の得意先住所に発送され横領等の不正行為が発生する可能性がある。	得意先マスタ管理と受注処理の権限分離	得意先マスタ管理（変更・登録）と受注処理（受注伝票登録・変更）の両方を持つロールをなくし、また複数ロールを通して同一ユーザにそれらを割り当てないようにする。 デモ
・受注登録 ・与信ブロック解除 上記の権限を同一ユーザに付与することにより、回収可能性の低い得意先との取引を継続でき、滞留債権が発生する。	受注処理と与信ブロック解除処理の権限分離	受注処理（変更・登録）と与信ブロック解除処理の両方を持つロールをなくし、また複数ロールを通して同一ユーザにそれらを割り当てないようにする。
・債権計上 ・入金・入金消込 上記の権限を同一ユーザに付与することにより架空の債権計上及び架空入金が実施でき，現金・預金の横領等の不正行為が発生する可能性がある。	債権計上処理と入金・入金消込処理の権限分離	債権計上に繋がる処理及び計上処理と入金・入金消込処理の両方を持つロールをなくし、また複数ロールを通して同一ユーザにそれらを割り当てないようにする。
…		

【参考】SAP GRC Solutions

SAP GRC SAP Governance , Risk , and Compliance Solutions ➔ 企業のガバナンス，リスク，コンプライアンスを管理するコンポーネント

GRC高度化要求

- 不正リスク
- プライバシー保護
- セキュリティ管理
- 事業継続計画（BCP）

特徴的な課題

- GRCプロセス細分化
- 既存ITテクノロジ非統合

SAP GRC Solutions

- 統合GRCプロセスを展開
- すべてのアプリケーション（SAP/非SAP）を統合

GRC高度化の実現

リアルタイムでの**プロセス可視化**により，**予防的なビジネス戦略**と**意思決定**の実行を実現

SAP GRC Solutions

SAP Access Control（AC）：アクセス管理

SAP Process Control （PC）：統制自動化

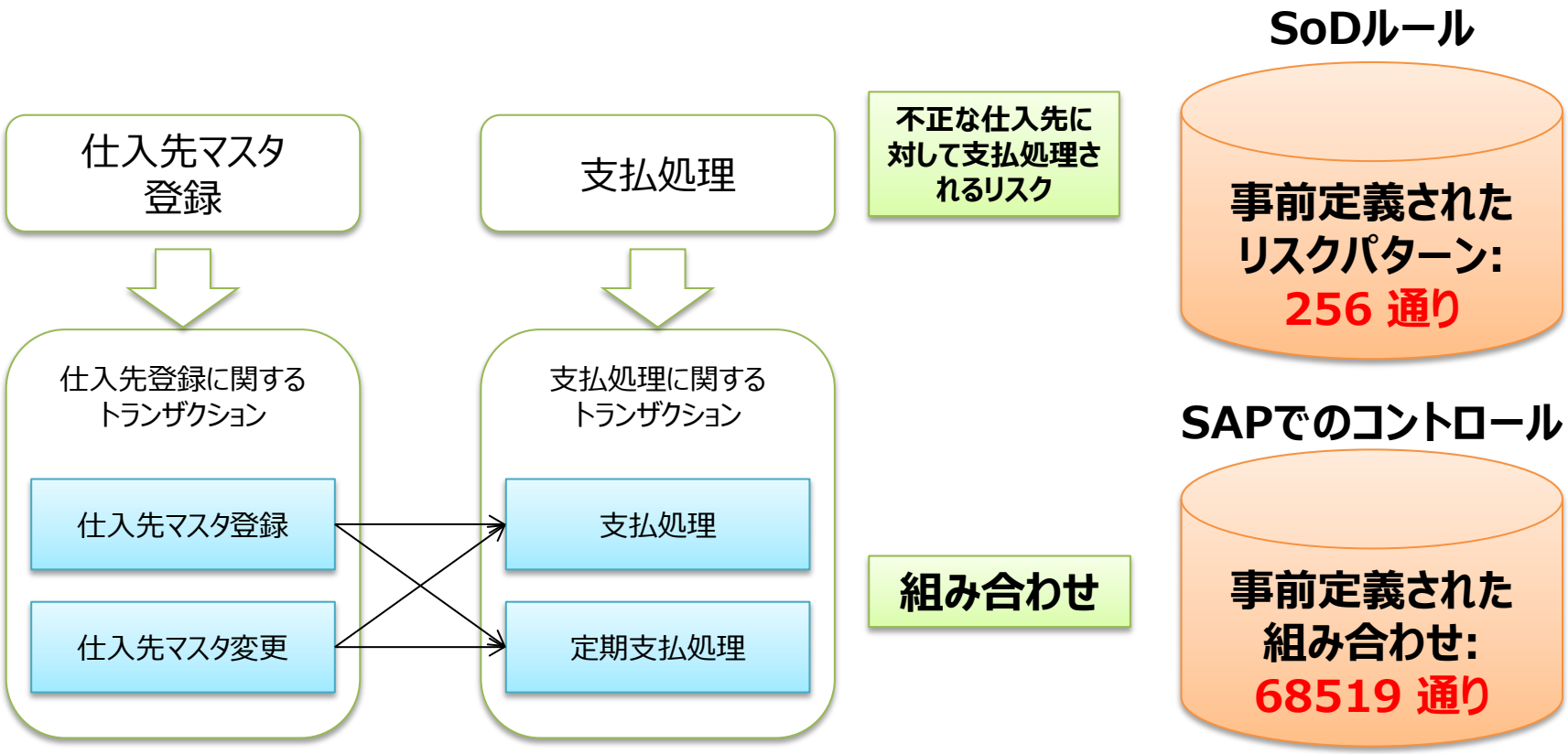
SAP Global Trade Control （GTS）：輸出入管理

SAP Risk Management（RM） ：リスク管理

SAP GRC Solution	機能･特徴	ポイント
SAP RM リスク管理	• 『リスク特定 → リスク分析 → リスク対応 → リスクモニタリング』循環モデルのベストプラクティスを提供する • リスク指標（KRI）を利用しマネジメントにレポーティングとアラート通知を行う • 全ての活動はダッシュボードとレポーティング機能でモニタリング可能である	多様なコーポ―レートリスク全般を把握し管理する統合的アプローチを提供 ⇒ 企業価値毀損の最小化
SAP AC アクセス管理	• 4つのモジュール（ARA，BRM，EAM，ARM）から構成され，アプリケーション横断的に効果的な**職務分掌（SoD）リスクを低減**可能なソリューションを提供する • 全社レベルでアクセスと認証を管理することにより，**的確なSoD管理を実現**する	継続可能な権限管理効率化とコンプライアンス強化 ⇒全ての関係者のSoD管理連携
SAP PC 統制自動化	• 自動的かつ合理的な統制機能を業務プロセスに組み込む • 内部統制モデル（自動化統制，手作業統制，統制評価，承認ワークフロー）の管理業務を一元化する • モニタリングとして，自動テスト，マニュアルテスト，セルフアセスメントを実行する • 統制環境を整備し，コンプライアンス実現に最も効率的かつ効果的なコントロールを明らかにする	内部統制モデル，内部統制に対するコンプライアンスのモニタリング ⇒ 手作業統制からの脱却
SAP GTS 輸出入管理	• 審査，エンバーゴ（出入港制限）チェック，輸出入ライセンス管理を自動化する • 還付管理の自動化による輸出補助金の処理を効率化する • 貿易協定などの特恵貿易協定活用の情報提供や，信用状管理強化による財務リスクを低減する	全社環境で標準化された貿易コンプライアンスプロセスを実現 ⇒ルール，コンプライアンスの一元管理

出典：監査法人　不正監査研修資料より

- **トランザクションコードの衝突をチェックする**
  - ✓ リスクパターン(不正リスクシナリオ) 256 通り
  - ✓ トランザクションコードの衝突パターン(SAPでのコントロール) 68,519 通り



職務権限設定の妥当性を分析し、リスクのある権限の組み合わせをレポート

出典：SAP社GRCソリューション説明資料より

【参考】SAP GRC AC の利用により期待される効果

✓ SAP GRC ACを利用した場合のメリット

- SAP社が用意した**SoDルールセットにより，一定水準を満たした**形でクイックかつ網羅的に**権限のコンフリクトチェック**ができる
- 権限払出や回収に係るプロセスを一元管理できる
- Fire Fighterによる緊急時の特権管理が適切に行える
- 海外子会社への容易な展開が行える

✓ SAP GRCを利用する場合の留意点

- すでに適切なJob Matrixが準備され，払出管理プロセス等が定義されている場合には，**高い価格**に見合うものであるかどうかの検討が必要

【補足情報】

※SAP GRCにおける 権限管理の仕組み
⇒ 複数の似たT-CodeをFunction Codeというものにまとめ，F-Codeの組合せごとにリスクをレーティングし，Mitigationを定義する
⇒ この定義をRulesetと呼び会社コード単位で管理する

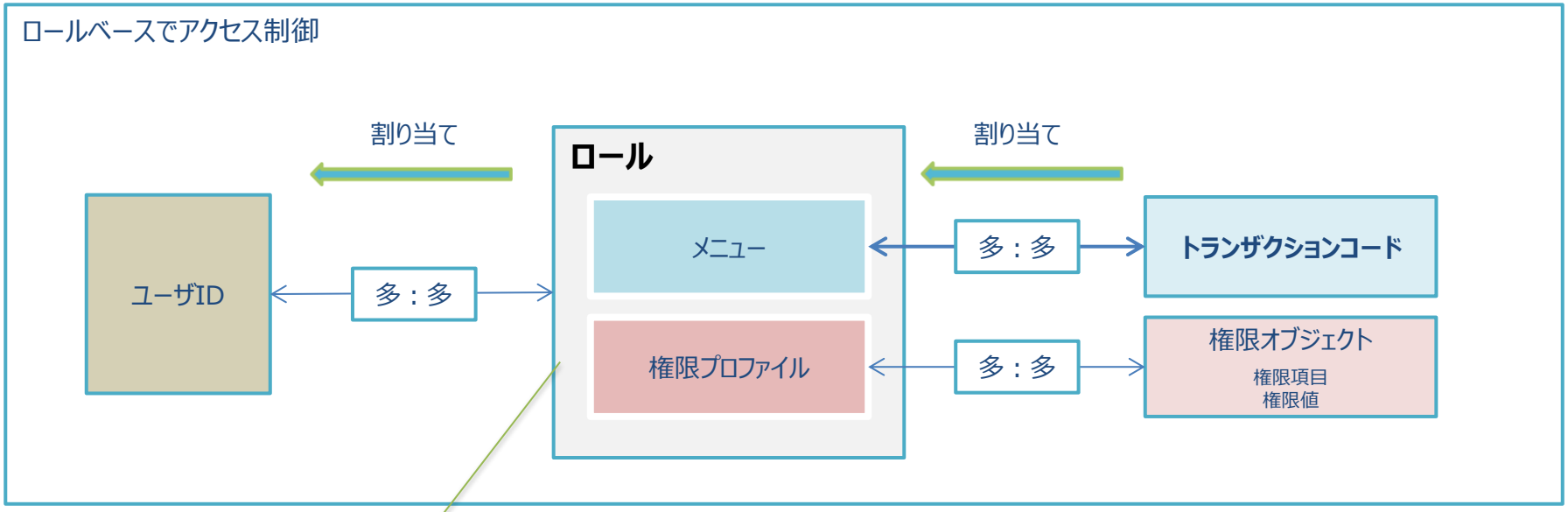
※ SAP GRCの特権管理の方針
⇒ 一般的には上記をExcelで細かく定義した上で，SAP上に実装する

（注） 当該参照情報は一般的な概要レベルの情報を整理したものであり，正確な情報はソリューション提供元のSAP社にお問い合わせください。

出典：監査法人 不正監査研修資料より S-ITCPD

3-5.[前提知識]アクセス制御の仕組み

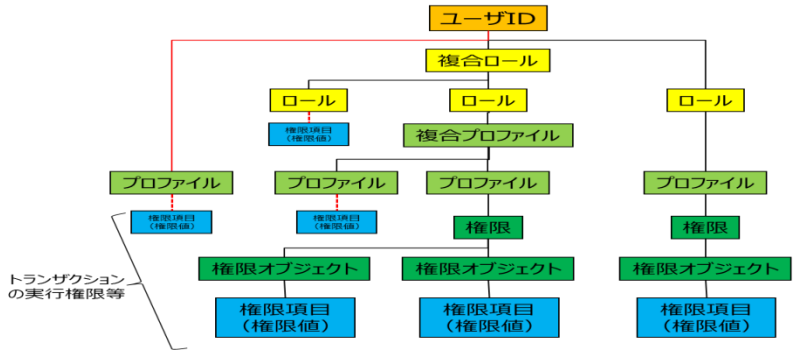
「ロール」をユーザに付与することでアクセス制御を実施



ロールは主に「メニュー」と「権限プロファイル」から構成

- メニューは，トランザクションコードを割り当てたもので，ユーザがログインしたときにツリー形式で表示される
- 権限プロファイルは権限オブジェクトを割り当てたもので，ロールの権限を決定する

＜参考＞ SAP社のアクセス権付与の説明



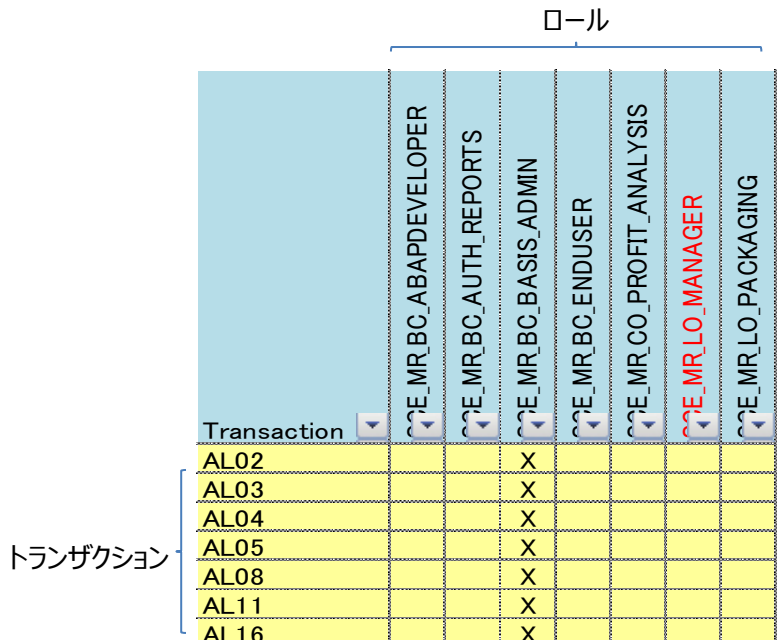
出典：SAP社研修資料をもとに作成

3-5.[前提知識]アクセス権の管理 - アクセス権マトリクス

職責毎にロールを作成し、職務実行に必要なトランザクションを定義　（①ロール・トランザクション表）
実際のユーザに与えられた職務に応じたロールを定義　（②ユーザID・ロール表）

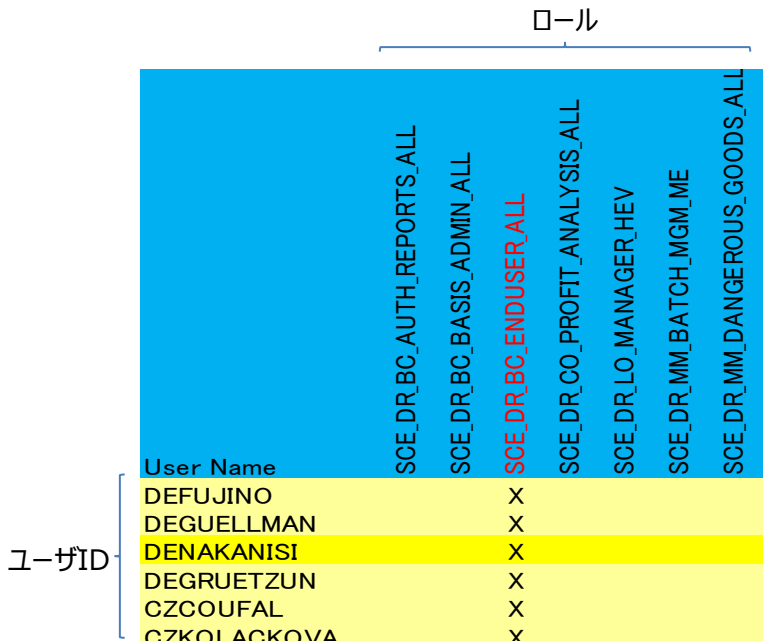
①②はSAP上では　AGR_TCODES およびAGR_USERSテーブルに保存されている

①，②をロールで結合することにより、ユーザID－トランザクションの関係が判る



① ロール・トランザクションコード

AGR_TCODES



② ユーザID・ロール

AGR_USERS

デモンストレーション

3-6.ロールのSODチェック

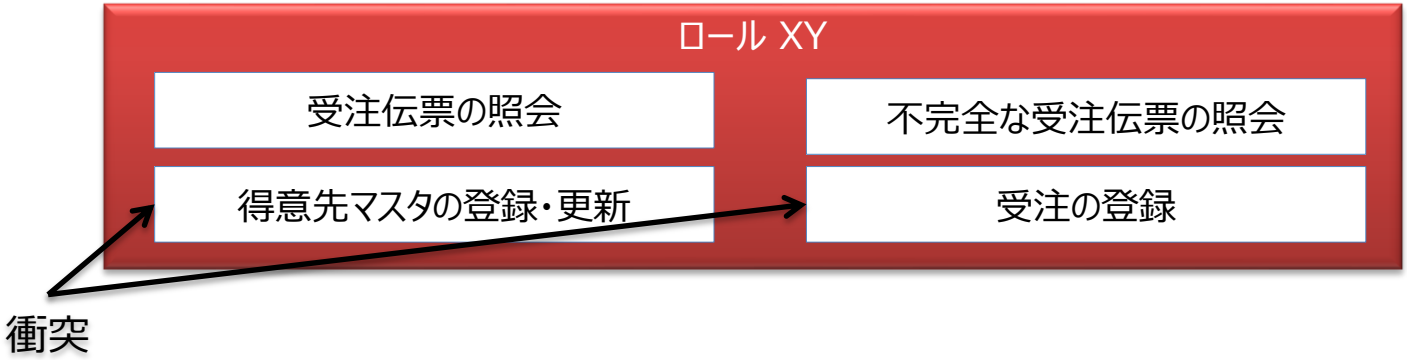
ロール－トランザクション表から、衝突するトランザクションのパターンを持つロールを抽出する

3-7.ユーザのSODチェック

ユーザ－トランザクション表を作成し、衝突するトランザクションのパターンを持つユーザを抽出する

3-6.ロールのSODチェック (1/5)

SOD(職務の分離)の観点から，一人のユーザに同時に付与すべきではないトランザクションコードがある。
しかし，ロールに広い業務範囲のトランザクションコードが付与されていると、職務範囲を超えた業務の実行ができ、SODは実現できない。この状態をトランザクションコードの衝突（コンフリクト）と呼ぶ。
そこで，ロール毎にトランザクションコードの衝突が無い事を調べることが重要である。



リスク

一人のユーザが得意先マスタファイルの登録・更新と受注の登録ができる場合，架空の得意先を登録してその得意先に対して受注を登録することが可能となり，現預金の横領といった不正が起こりえる。また売上が過大評価されうる。

統制

次のアクセス権を分離し，同一ユーザに付与しないことが推奨される。

- 得意先マスタの登録・更新
- 受注の登録

SODの観点でロールをチェックする手続き

1. SODルールの定義
2. SODを満たさないトランザクションコードのパターンの洗い出し
3. ロール・トランザクションコードテーブルのダウンロード
4. ロールにトランザクションコードの衝突が無いかのチェック

3-6.ロールのSODチェック (3/5)

1. SODルールの定義

例). ルール1: 次の**トランザクションの分離**

(1) **得意先マスタ管理（変更･登録）**

(2) 受注処理（受注伝票登録･変更）

2. SODを満たさないトランザクションコードのパターンの洗い出し

(1) 得意先マスタ管理（変更･登録）　　(トランザクションコード 15個)

FD01 / FD02 / FD02CORE / FD05 / FD06 / VD01 / VD02 / VD05 / VD06 / XD01 / XD02 / XD05 / XD06 / XD07 / XD99

(2)受注処理（受注伝票登録･変更）　　(トランザクションコード 3個)

V-01 / VA01 / VA02

注). Tcode：トランザクションコード

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
Rule1	･･･	･･･
Rule1	XD99	V-02

15X3 = 45 パターン

1と2を繰り返し，SODを満たさない多くのパターンを作成する

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
･･･	･･･	･･･
Rule XXX	Tcode U	Tcode M

? パターン

SAP GRC
60,000 パターン

3-6.ロールのSODチェック (4/5)

3. ロール – トランザクションコードテーブルのダウンロード

SE16を実行し，"AGR_TCODES"からロール－トランザクションコードをダウンロードし，MSアクセスに取り込む

ロール – トランザクションコードテーブル

Role	Tcode
CFM_INSURANCE_COMPANIES	F-04
T_COMP_PCC	F-06
SAP_QM_IT_CALIB_PLANNING	QS23
SAP_QM_IT_CALIB_PROCUREMENT	MBST
…	

4. ロールにトランザクションコードの衝突が無いかのチェック

下に示す構造のクエリを作成/実行し、“SOD トランザクションコードの衝突パターン”に合致したトランザクションの組合せを検出

ロール – トランザクションコードテーブル

ロール	Tcode
CFM_INSURANCE_COMPANIES	F-04
CFM_INSURANCE_COMPANIES	F-06
SAP_QM_IT_CALIB_PLANNING	QS23
SAP_QM_IT_CALIB_PROCUREMENT	MBST
…	

結合

結合

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
…	…	…
Rule XXX	Tcode U	Tcode M

結合

ロール – トランザクションコードテーブル

Role	Tcode
CFM_INSURANCE_COMPANIES	F-04
SAP_QM_IT_CALIB_PLANNING	F-06
SAP_QM_IT_CALIB_PLANNING	QS23
SAP_QM_IT_CALIB_PROCUREMENT	MBST
…	

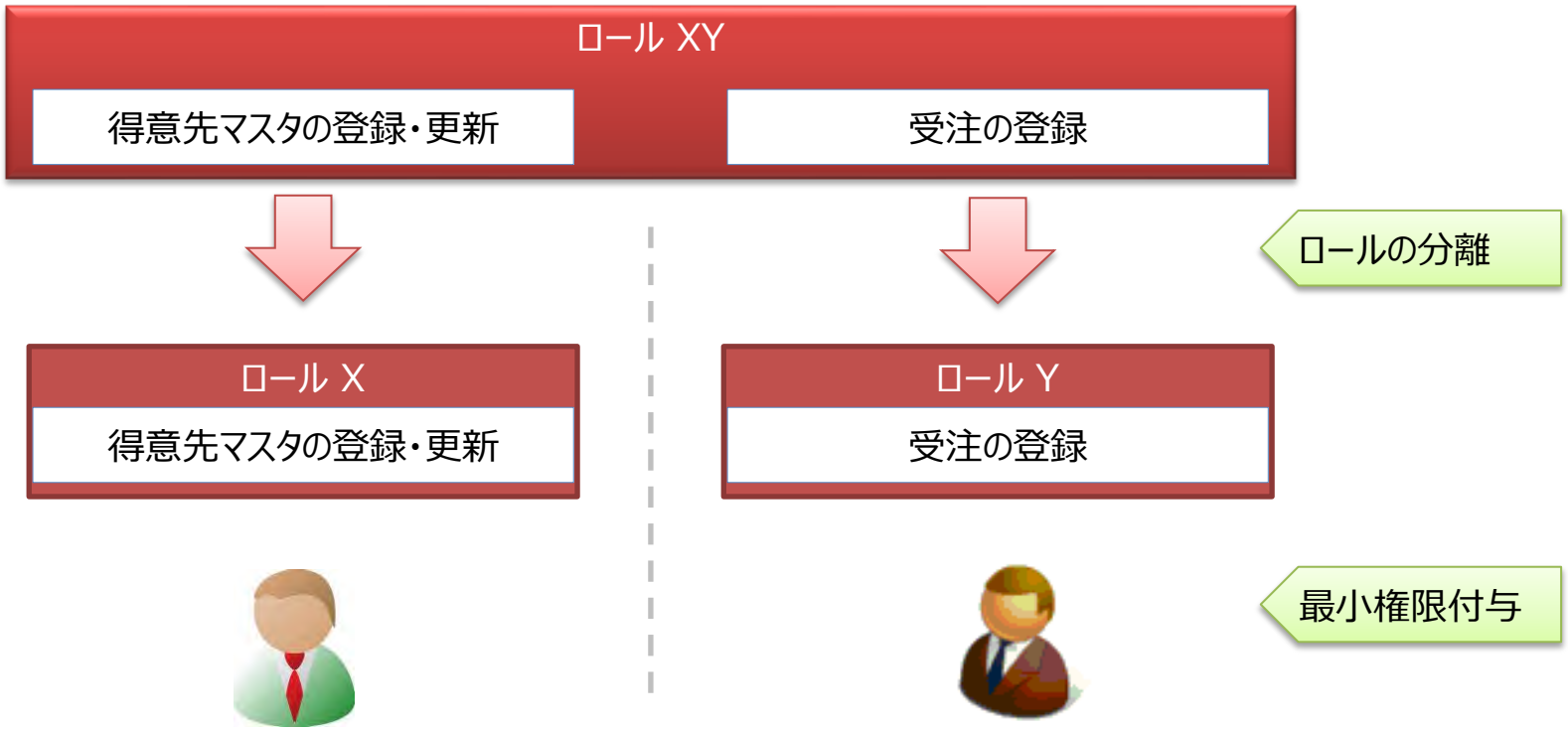
出力

衝突トランザクションコードを含むロールを抽出する

検出されたSOD衝突パターン

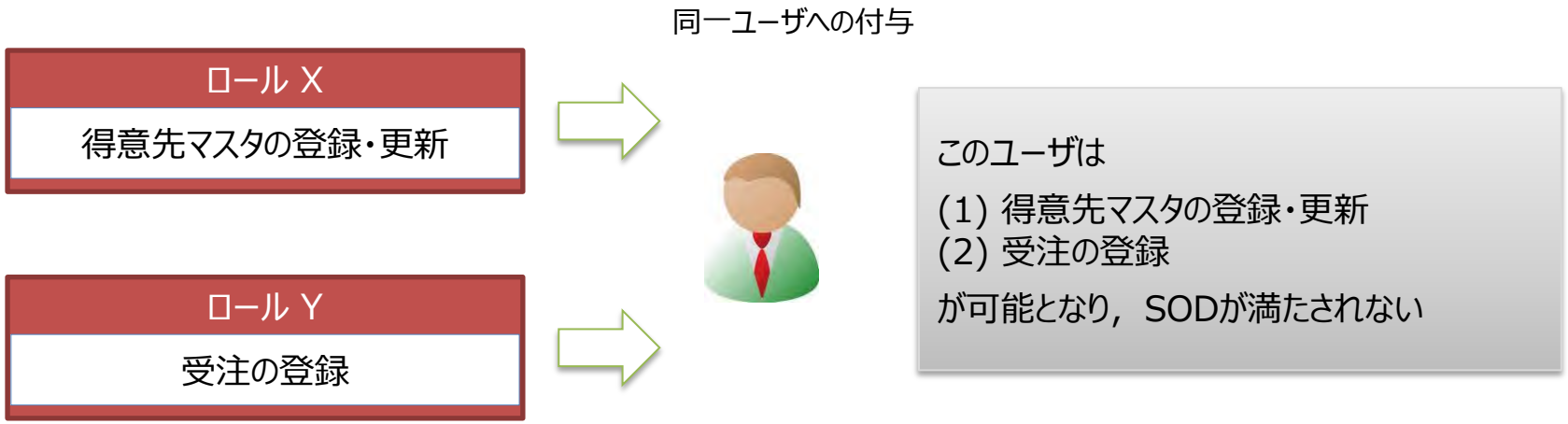
ルール	ロール	Tcode1	Tcode2
Rule3	Role A	VKM5	VA02
Rule3	Role A	VKM3	VA02
…		…	…
Rule XXX	Role K	Tcode U	Tcode M

衝突トランザクションコードを含むロールがあった場合，そのロールを分離する。
そして，各ユーザにSODの観点から最小権限を付与する。
もしロールが分離できない場合，補完的な統制を適用する。



3-7.ユーザのSODチェック (1/5)

例えロールが衝突トランザクションコードを含まなかったとしても，複数のロールが不適切に付与された場合，ユーザは衝突トランザクションコードを持つ恐れがある。



SODの観点でユーザをチェックする手続き

1. SODルールの定義
2. SODを満たさないトランザクションコードのパターンの洗い出し
3. ユーザ－トランザクションコードテーブルの作成
4. ユーザが衝突トランザクションコードを持つかのチェック

3-7.ユーザのSODチェック (3/5)

1. SODルールの定義

例). ルール1: 次の**トランザクションの分離**

(1) 得意先マスタ管理（変更･登録）
(2) 受注処理（受注伝票登録･変更）

2. SODを満たさないトランザクションコードのパターンの洗い出し

(1) 得意先マスタ管理（変更･登録）　(トランザクションコード 15個)
FD01 / FD02 / FD02CORE / FD05 / FD06 / VD01 / VD02 / VD05 / VD06 / XD01 / XD02 / XD05 / XD06 / XD07 / XD99

(2) 受注処理（受注伝票登録･変更）　(トランザクションコード 3個)
V-01 / VA01 / VA02

注). Tcode：トランザクションコード

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
Rule1	･･･	･･･
Rule1	XD99	V-02

15X3 = 45 パターン

1と2を繰り返し，SODを満たさない多くのパターンを作成する

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
･･･	･･･	･･･
Rule XXX	Tcode U	Tcode M

? パターン

SAP GRC
60,000 パターン

3-7.ユーザのSODチェック (4/5)

3. ユーザ・トランザクションコードテーブルの作成

ロール・トランザクションコードテーブル(AGR_Tcode)と
ロール・ユーザテーブル(AGR_USERS)から,
ユーザ・トランザクションコードテーブルを作成し，MSアクセスに取り込む。

ユーザ－トランザクションコードテーブル

ユーザ	Tcode
AU_UME	VKM5
AU_UME	VA02
AU_SHIMO	VKM5
AU_SHIMO	VA01
…	

4. ユーザが衝突トランザクションコードを持つかのチェック

下に示すテーブルの結合とクエリの作成/実行を行い、“SOD トランザクションコードの衝突パターン”に合致したトランザクションの組合せを検出

ユーザ－トランザクションコードテーブル

ユーザ	Tcode
AU_UME	VKM5
AU_UME	VA02
AU_SHIMO	VKM5
AU_SHIMO	VA01
…	

結合

SOD トランザクションコードの衝突パターン

ルール	Tcode1	Tcode2
Rule1	FD01	V-01
Rule1	FD02	V-01
…	…	…
Rule XXX	Tcode U	Tcode M

結合

ユーザ－トランザクションコードテーブル

ユーザ	Tcode
AU_UME	VKM5
AU_UME	VA02
AU_SHIMO	VKM5
AU_SHIMO	VA01
…	

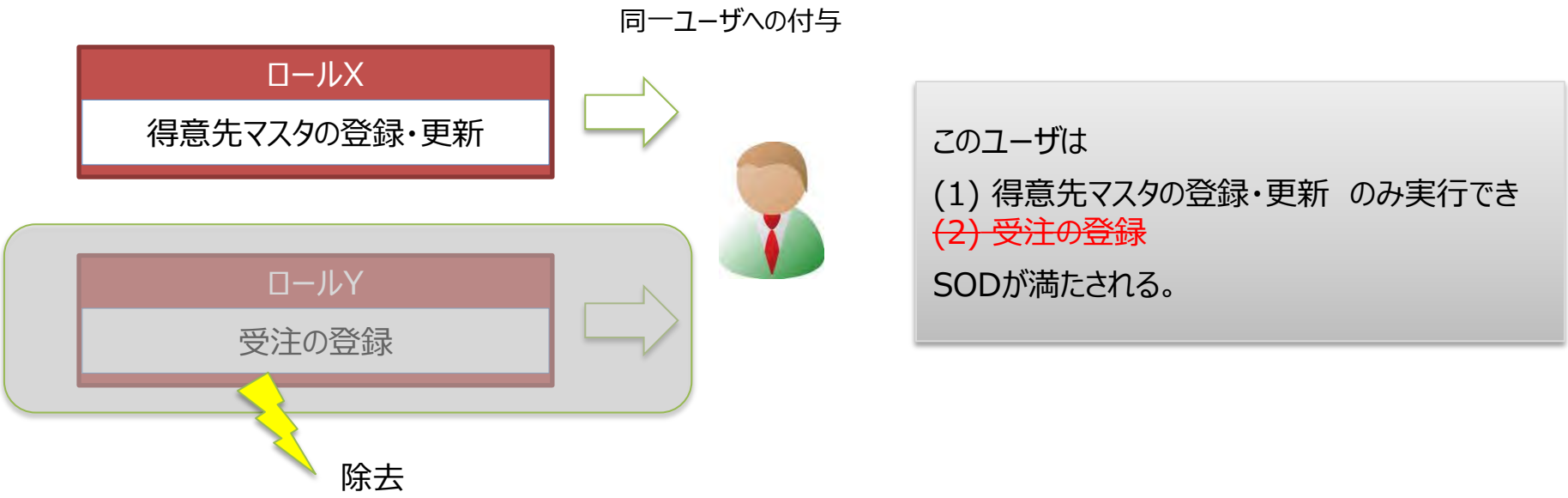
出力

衝突トランザクションコードを含むユーザを抽出する

検出されたSOD衝突パターン

ルール	ユーザ	Tcode1	Tcode2
Rule3	AU_UME	VKM5	VA02
Rule3	AU_UME	VKM3	VA02
…		…	…
Rule XXX	AU_X	Tcode U	Tcode M

衝突トランザクションコードを持つユーザが検出された場合，過剰なロールを取り除く。
SODの観点から各ユーザには最小権限を付与する。
ロールが取り除かれない場合，マニュアルによる補完的な統制を適用する。



4. SAP標準機能を活用した監査手法

4-1.SAPにおける高権限IDの管理

高権限ID

特権ユーザ
（スーパーユーザという場合もある）

ＳＡＰシステムに予め登録されているユーザＩＤであり、強力な権限を付与されているだけでなく、初期パスワードが公開されているため、リスクが高い
①ＳＡＰ＊（サップアスター）： 全権が割り当てられていて、ハード・コーディングされている。
②ＤＤＩＣ（ディーディック）： 全権が割り当てられていて、インストール時などで使用
③ＳＡＰＣＰＩＣ（サップシーピック）： システム間、プログラム間の通信ユーザ
④ＥＡＲＬＹＷＡＴＣＨ（アーリーウォッチ）： （本稼動開始前の）SAP社の診断サービス用ユーザ

強力な権限プロファイルを付与されたユーザID

ＳＡＰシステムでは特権ユーザと同等の権限を持つ強力な権限プロファイルを提供しています。
この強力な権限を付与されたユーザが高権限IDとなる
①SAP_ALL：SAPシステムに存在するすべての権限を割り当てるプロファイル
（SAP*と同様の権限）
②SAP_NEW： リリースアップの際、既存機能に対して新規の権限チェックや権限チェックの内容変更がある場合に、ユーザがいままでどおりに作業を続行できるように追加された新しい権限をもつ。（ＤＤＩＣと同様の権限）

重要なトランザクションが実行できるユーザID

A.システムパラメータの設定等ができるトランザクション
- RZ10，RZ11…プロファイル保存，プロファイルパラメータ更新
- SPRO … … … システムパラメータ設定
- SE16，SM30…データ直接修正
- SE06，SCC4 … 本番環境の変更管理設定
- SA38，SE38…プログラム実行権限
- SM35，SM37 … ジョブ実行権限

B.ユーザIDの登録・修正・削除ができるトランザクション
- SU01 … … … ユーザ管理
- SU02 … … … 権限プロファイル管理
- SU10 … … … ユーザ管理での一括更新
- SU03 … … … 権限オブジェクト管理
- SU12 … … … ユーザマスタの一括更新
- PFCG … … … ロール管理

4-2.SAPにおける高権限IDの確認手続き (1/5)

具体的な確認手続き

特権ユーザ

①オールマイティ（SAP*等）

I. オールマイティな権限プロファイルを持つビルトインの高権限ID（SAP*，DDIC，EARLYWATCH)は使用しないことが望ましく，そのために次のA～Dのいずれかが満たされているかを確認する。
(下記①-Ⅰ-Dはハードコーディングされ たID(SAP*）のみ該当)

A) IDがロックされているか，または有効期限が切れているか　**①-Ⅰ-A**

B) SAP_ALL, SAP_NEWが剥奪されているか　①-Ⅰ-B

C) 初期パスワードが変更され，以後の使用がないか　①-Ⅰ-C

D) ログインできない設定を施しているか　①-Ⅰ-D

強力な権限プロファイルを付与されたユーザID

II.オールマイティな権限プロファイル(SAP_NEW, SAP_ALL)を持つIDが限定されているかを確認する。

E) SAP_NEW, SAP_ALLを持つIDの限定　**①-Ⅱ-E**

重要なトランザクションが実行できるユーザID

②アプリ用の重要なパラメータ等設定ID

III.アプリ用の重要なパラメータ等の設定に係るトランザクションコードの実行が可能なIDが限定されているか確認する。

F) アプリ用の重要なパラメータ等の設定に係るトランザクションコード実行可能IDの限定　**②-Ⅲ-F**

③IDの登録・修正・削除が可能なID

IV. IDの登録・修正・削除に係るトランザクションコードの実行が可能なIDが限定されているか確認する。

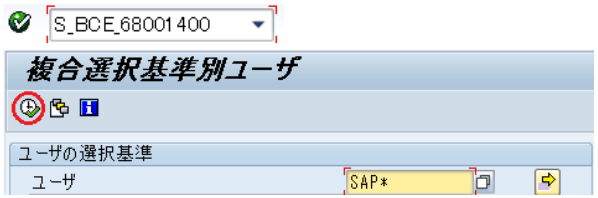
G) IDの登録・修正・削除が可能なIDに係るトランザクションコードの限定　**③-Ⅳ-G**

4-2.SAPにおける高権限IDの確認手続き (2/5)

①-Ⅰ-A） 特権ユーザIDがロックされているか，または有効期限が切れているか

トランザクションコード：S_BCE_68001400
ユーザ：SAP*，等
実行icon クリック (F8)

上記と同様の手続きで下記IDを検証する
DDIC，EARLYWATCH



S_BCE_68001400のメニューパス
SAPメニュー > ツール > システム管理 > ユーザ管理 > 情報システム > ユーザ > 複合選択基準別ユーザ > S_BCE_68001400-複合選択基準別ユーザ

S_BCE_68001400の用途
複数条件に合致するユーザを抽出

監査ポイント

複合選択基準別ユーザ画面が出力されるので，SAP*の状況を確認する。
ロック済の列に鍵マークがあれば，ロックされていることになり，使用ができない状態であるのでOKとなる。
また有効終了日が昨年度以前の過去の日付であれば，今期の使用はないのでOKとなる。
OKであれば，残りの①-Ⅰ-B，C，Dの確認は不要となる。

下図ではSAP*はロックされておらず，有効終了日も空なので，使用可能な状態となっているのでNG。
残りの①-Ⅰ-B，C，Dを確認する。

なお，ロックされた日付はログで確認可能である。(ITG034-01【高権限操作者の操作内容の確認（アプリ側）】 参照)
有効終了日には最終ログイン日より以前の日付は指定できない。つまり不正目的で有効終了日を操作して，最終ログインの事実を隠すことはようになっている。

【参考】ロック／有効期限の設定

4-2.SAPにおける高権限IDの確認手続き (3/5)

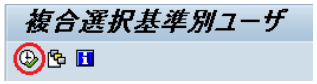
①-Ⅱ-E）
SAP_NEW, SAP_ALLを持つIDの限定

トランザクションコード：S_BCE_68001400
プロファイル複数選択icon クリック
指定値：SAP_ALL ， SAP_NEW
実行icon クリック (F8)

S_BCE_68001400のメニューパス
SAPメニュー > ツール > システム管理 > ユーザ管理 > 情報システム > ユーザ > 複合選択基準別ユーザ > S_BCE_68001400-複合選択基準別ユーザ

S_BCE_68001400の用途
複数条件に合致するユーザを抽出

実行icon クリック (F8)



監査ポイント

出力されたID一覧と管理上の高権限管理ファイルを照合し，高権限プロファイルを持つ不要な/未承認のIDがないかを検証する。
IDがロックされていたり，有効期限が切れている場合はOKとする。

なお，ロックされた日付はログで確認可能である。(ITG034-01【高権限操作者の操作内容の確認（アプリ側）】 参照)
有効終了日には最終ログイン日より以前の日付は指定できない。つまり不正目的で有効終了日を操作して，最終ログインの事実を隠すことはようになっている。

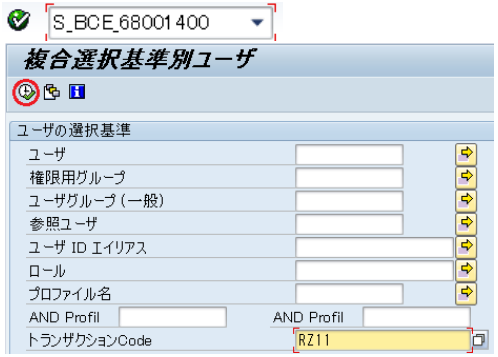
【参考】ロック／有効期限の設定

ユーザ名	氏名（省略なし）	User Group	Account No	ロック済	ユーザロックの理由	有効開始日付	有効終了日
OLZOG	OLZOG	SUPER					
P25099400	Ruth Cabrera	ESSUSER		🔒	USR	01.01.2000	31.12.9999
PERRON	Tracy PERRON	GFO					

4-2.SAPにおける高権限IDの確認手続き (4/5)

②-Ⅲ-Ｆ）
アプリ用の重要なパラメータ等の設定に係るトランザクションコード実行可能IDの限定

トランザクションコード：S_BCE_68001400
トランザクションcode：RZ11，他
実行icon クリック (F8)



S_BCE_68001400のメニューパス
SAPメニュー > ツール > システム管理 > ユーザ管理 > 情報システム > ユーザ > 複合選択基準別ユーザ > S_BCE_68001400-複合選択基準別ユーザ

S_BCE_68001400の用途
複数条件に合致するユーザを抽出

下記のトランザクションコードについて同様の確認を行う

トランザクション：RZ10， RZ11	プロファイル保存，プロファイルパラメータ更新
トランザクション：SPRO	システムパラメータ設定
トランザクション：SE16，SM30	データ直接修正
トランザクション：SA38，SE38	プログラム実行権限
トランザクション：SE06，SCC4	本番環境の変更管理設定
トランザクション：SM35，SM37	ジョブ実行権限

監査ポイント

出力されたID一覧と管理上の高権限管理ファイルを照合し，不要な/未承認のIDがないかを検証する。

高権限管理ファイル ⟷ 照合

ユーザ名	氏名（省略なし）	User Group	アカウント ID	ロック済	理由	有効開始日	有効終了日	ユーザタイプ	参照ユーザ	ポリ
100026	Reference user b2c	TEMPLATE			USR			A Dialog	RCF_CAND_INT	
100197	James Matlock	ESSUSER			USR			A Dialog		
100198	Michael Ryan	ESSUSER			USR			A Dialog		
100209	Timmy Tabasco	ESSUSER			USR			A Dialog		
100226	Matthew Black	ESSUSER			USR			A Dialog		
100227	George Metzger	ESSUSER			USR			S サービス	RCF_CAND_INT	
123456	RF User 123456	TEMPLATE			USR			S サービス		

4-2.SAPにおける高権限IDの確認手続き (5/5)

③ -Ⅳ-G）

ユーザの登録・修正・削除が可能なトランザクションコードに係る実行可能IDの限定

トランザクションコード：S_BCE_68001400

トランザクションcode：SU01

実行icon クリック (F8)

S_BCE_68001400のメニューパス
SAPメニュー > ツール > システム管理 > ユーザ管理 > 情報システム > ユーザ > 複合選択基準別ユーザ > S_BCE_68001400-複合選択基準別ユーザ

S_BCE_68001400の用途
複数条件に合致するユーザを抽出

下記のトランザクションコードについて同様の確認を行う

トランザクション：SU01　ユーザ管理
トランザクション：SU10　ユーザ管理での一括更新
トランザクション：SU12　ユーザマスタの一括更新
トランザクション：SU02　権限プロファイル管理
トランザクション：SU03　権限オブジェクト管理
トランザクション：PFCG　ロール管理

監査ポイント

出力されたID一覧と管理上の高権限管理ファイルを照合し，不要な/未承認のIDがないかを検証する。

高権限管理ファイル ⟷ 照合

ユーザ名	氏名（省略なし）	User Group	アカウント ID	ロック済	理由	有効開始日	有効終了日	ユーザタイプ	参照ユーザ
100026	Reference user b2c	TEMPLATE			USR			A Dialog	RCF_CAND_INT
100197	James Matlock	ESSUSER			USR			A Dialog	
100198	Michael Ryan	ESSUSER			USR			A Dialog	
100209	Timmy Tabasco	ESSUSER			USR			A Dialog	
100226	Matthew Black	ESSUSER			USR			A Dialog	
100227	George Metzger	ESSUSER			USR			S サービス	RCF_CAND_INT
123456	RF User 123456	TEMPLATE			USR			S サービス	

4-3.不要ユーザ(退職者等)の抽出

最終ログイン日付を確認することにより、不要ユーザを確認

最終パスワード変更日の確認

検索条件を指定して、「６ヶ月以上ログインしていない」、「3か月以上パスワード変更していない」等のユーザのみ抽出できる。

SA38
RSUSR200

ユーザ名

有効期間、
ロック状態

最終ログオン日

最終PW変更日

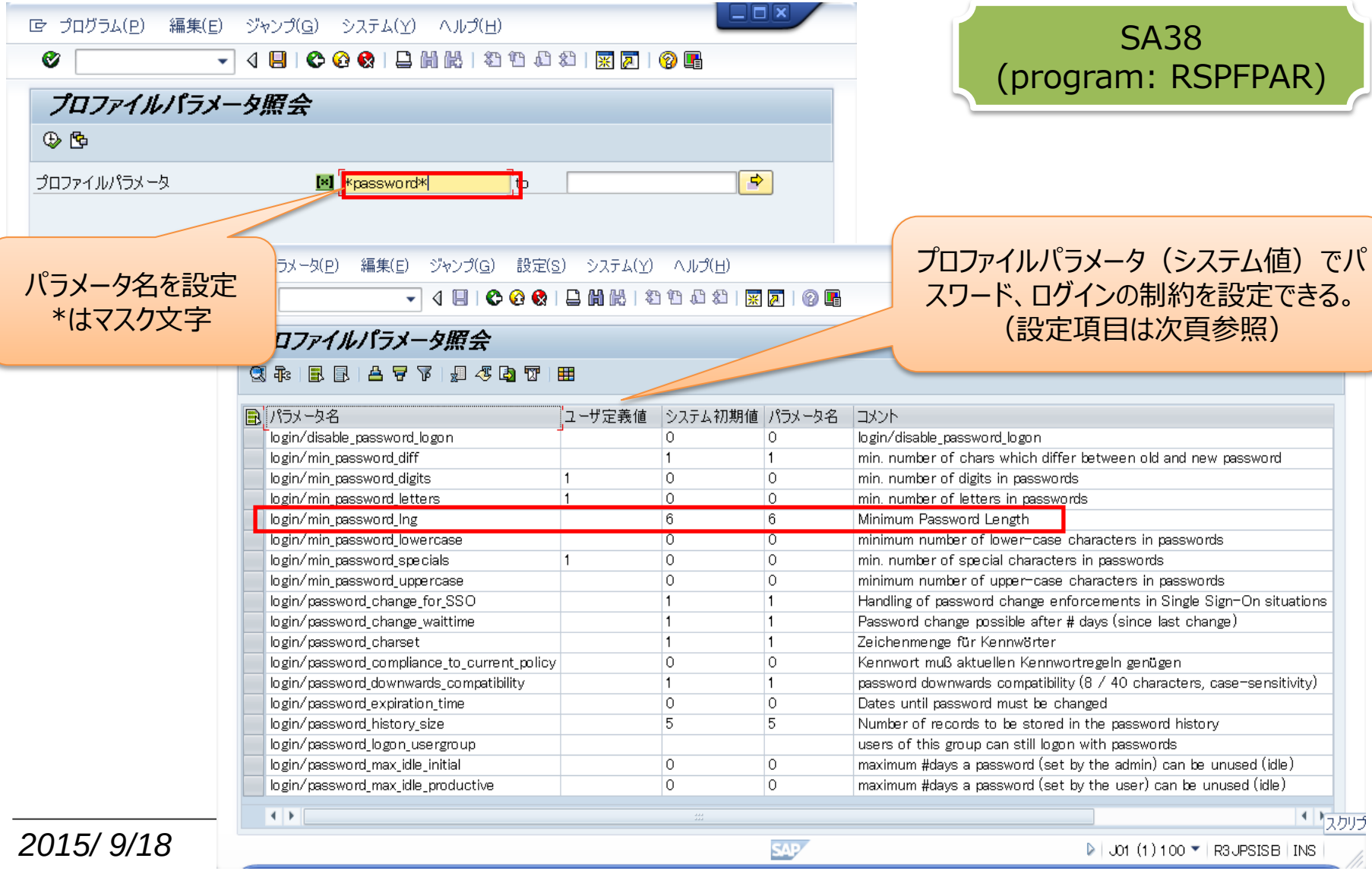
ユーザ	グループ	タイプ	登録者	登録日付	有効開始日	有効期限	ログオン	ログオン	パスワード	パスワード変更	ロック	ロック理由
ASHIE		A Dialog	J01 ADM	2011/01/25			2014/03/18	11:44:48	✔	2013/08/07		
AU_HIRAOKA		A Dialog	TESTUSR01	2013/10/17			2014/03/18	12:32:53	✔	2013/11/29		
AU_KINOHARA		A Dialog	TESTUSR01	2013/10/17			2014/03/18	17:17:48	✔	2014/03/18		
AU_MORI		A Dialog	TESTUSR01	2013/10/17		2015/12/31	2014/02/19	16:13:39	✔	2013/10/22		
AU_NAKAGAWA		A Dialog	TESTUSR01	2013/10/17		2015/12/31	不使用		✖	2013/10/22		
AU_URAKAMI		A Dialog	TESTUSR01	2013/10/15			2014/02/26	10:43:35	✔	2014/02/13		
AU_WHITE		A Dialog	TESTUSR01	2013/10/17		2015/12/31	2013/11/18	15:25:31	✔	2013/10/21		
CHUMA		A Dialog	ASHIE	2014/02/21			2014/03/13	16:45:11	✔	2014/02/28		
GR##-ADM		A Dialog	AU_MORI	2014/01/31			不使用		✖	2014/01/31		
GR01-ADM		A Dialog	AU_MORI	2014/02/07			不使用		✖	2014/02/07		
HARANO		A Dialog	J01 ADM	2011/01/25			2013/06/27	09:54:26	✔	2013/06/26	🖶	不正なログオ
J01 ADM		A Dialog	SAP*	2011/01/18			2013/04/23	11:54:23	✔	2011/01/18		
KAI		A Dialog	J01 ADM	2011/01/25			2013/08/22	12:40:36	✔	2013/08/22		
KAMIYAMA		A Dialog	J01 ADM	2011/01/25			2013/08/22	12:29:42	✔	2013/07/25		
KAWANISHI		A Dialog	NISHIKIORI	2013/06/04			2013/07/12	17:17:38	✔	2013/06/04		
KEISUKE		A Dialog	ASHIE	2013/01/16			2013/01/16	21:26:03	✔	2013/01/16		
KISHIMOTO		A Dialog	TOKUTOMI	2013/06/26			2014/03/04	11:52:31	✔	2013/06/26		
MASAKI		A Dialog	TOKUTOMI	2013/01/30			2013/04/24	16:39:11	✔	2013/04/15		
MIURA		A Dialog	J01 ADM	2011/01/24			2014/03/14	10:37:54	✔	2011/01/24		
NISHIKIORI		A Dialog	ASHIE	2012/12/04			2013/12/20	09:18:21	✔	2013/02/07		
NISHIMURA		A Dialog	ASHIE	2013/03/29			2013/08/19	09:46:29	✔	2013/03/29		
NISHIYAMA		A Dialog	ASHIE	2014/02/21			2014/03/07	19:03:08	✔	2014/02/21		
OYA		A Dialog	J01 ADM	2011/01/25			不使用		✖	2011/01/25		
SHIMODAIRA		A Dialog	J01 ADM	2011/01/25			不使用		✖	2011/01/25		
SHIRONO		A Dialog	J01 ADM	2011/01/25			不使用		✖	2011/01/25		
TESTUSR00		A Dialog	TESTUSR01	2013/10/07			2013/11/29	14:04:29	✔	2013/11/29		
TESTUSR01		A Dialog	MIURA	2013/10/07			2013/10/18	18:09:42	✔	2013/10/07		
TESTUSR02		A Dialog	TESTUSR01	2013/10/07			不使用		✖	2013/10/07		
TOKUTOMI		A Dialog	J01 ADM	2011/01/25			2013/12/06	10:25:01	✔	2013/06/25		
YOKOYAMA		A Dialog	J01 ADM	2011/01/25			2011/08/04	14:39:52	✔	2011/06/15		

プロファイルパラメータによるセキュリティ設定

SA38
(program: RSPFPAR)

パラメータ名を設定
*はマスク文字

プロファイルパラメータ（システム値）でパスワード、ログインの制約を設定できる。
（設定項目は次頁参照）



パラメータ名	ユーザ定義値	システム初期値	パラメータ名	コメント
login/disable_password_logon		0	0	login/disable_password_logon
login/min_password_diff		1	1	min. number of chars which differ between old and new password
login/min_password_digits	1	0	0	min. number of digits in passwords
login/min_password_letters	1	0	0	min. number of letters in passwords
login/min_password_lng		6	6	Minimum Password Length
login/min_password_lowercase		0	0	minimum number of lower-case characters in passwords
login/min_password_specials	1	0	0	min. number of special characters in passwords
login/min_password_uppercase		0	0	minimum number of upper-case characters in passwords
login/password_change_for_SSO		1	1	Handling of password change enforcements in Single Sign-On situations
login/password_change_waittime		1	1	Password change possible after # days (since last change)
login/password_charset		1	1	Zeichenmenge für Kennwörter
login/password_compliance_to_current_policy		0	0	Kennwort muß aktuellen Kennwortregeln genügen
login/password_downwards_compatibility		1	1	password downwards compatibility (8 / 40 characters, case-sensitivity)
login/password_expiration_time		0	0	Dates until password must be changed
login/password_history_size		5	5	Number of records to be stored in the password history
login/password_logon_usergroup				users of this group can still logon with passwords
login/password_max_idle_initial		0	0	maximum #days a password (set by the admin) can be unused (idle)
login/password_max_idle_productive		0	0	maximum #days a password (set by the user) can be unused (idle)

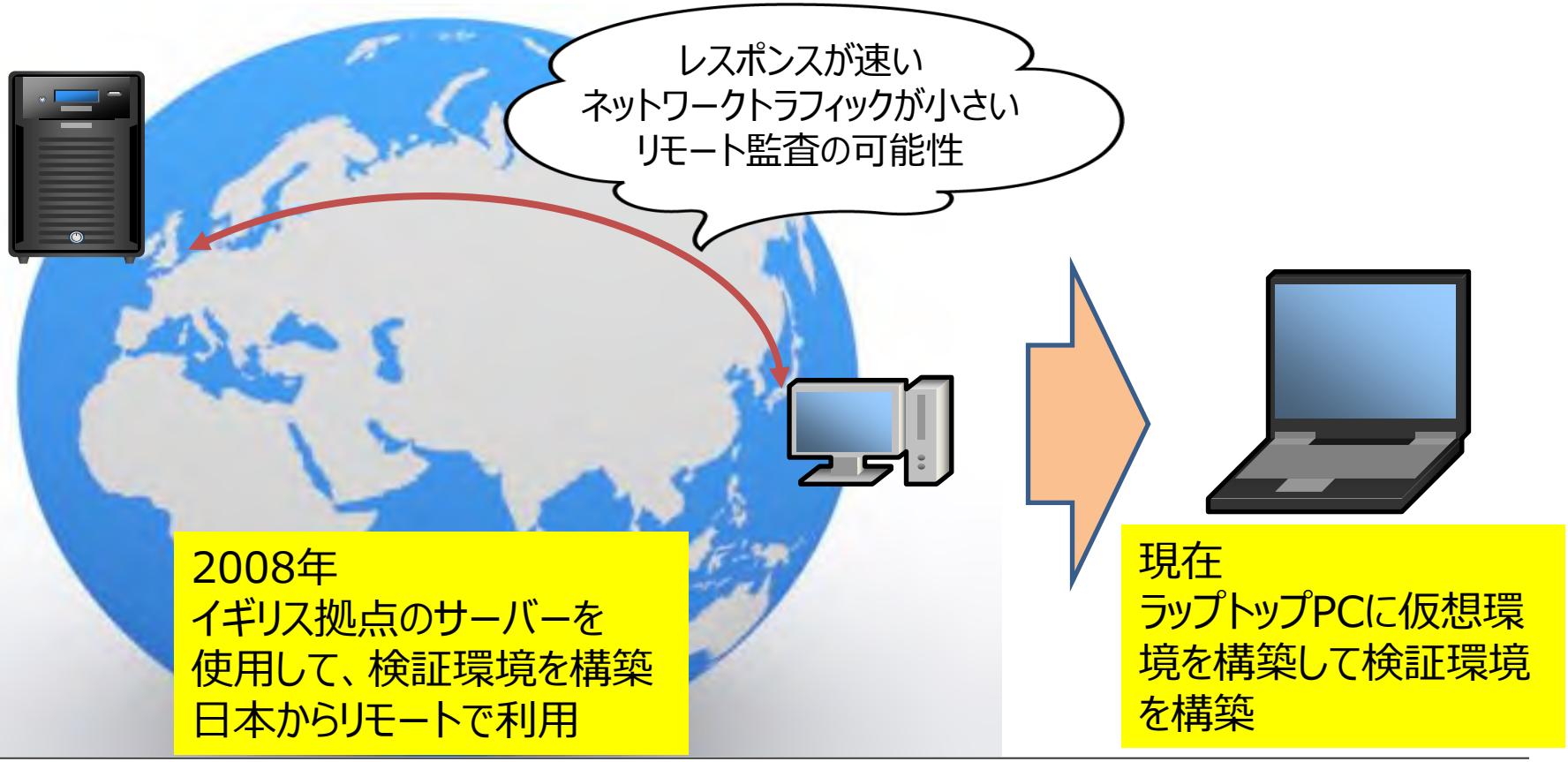
プロファイルパラメータの例

パラメータID	役割	チェック事項
login/fails_to_session_end	1 ユザID で一定回数連続してログオンに失敗した場合、セッションを終了させる。デフォルト＝３、値の範囲＝１～９９	３回程度に設定されている事（推奨）。
login/failed_user_auto_unlock	不正ログオンによってロックされたユーザのロック解除を制御する。このパラメータを 1 に設定すると (デフォルト)、不正ログオンのためにロックされたユーザのロックが２４：００に自動解除される。値 を 0 にすると、ロックの自動解除は行われなくなる。	不正ログオンによってロックされたユーザのロック自動解除が行われないように設定されている事（推奨）。
rdisp/gui_auto_logout	ユーザが一定時間操作を行っていない場合、強制ログオフするまでの時間を指定する。デフォルト＝ 0 （自動ログオフしない）、値の範囲＝制限なし。	スクリーンセイバーにより画面ロックが設定されている場合等、必要度は低い。
login/min_password_lng	ログオンパスワードの最低の長さ指定	原則として６文字以上
login/min_password_digits 等	パスワードに含まれる「数字」、「文字」、「特殊文字」、「大文字」、「小文字」の最小数このパラメータによりパスワードに含まれていなければならない最少桁数が設定される。このパラメータは新規パスワードの割当およびパスワードの変更/リセットの両方に対して有効である。有効な入力、書式、範囲 ： 0 – 8	パスワードに数字、大文字、小文字、特殊文字がそれぞれ最低１文字含まれるように設定されていることを確認する（推奨）。
login/password_expiration_time	0 より大きい値を指定した場合、その値の日数を超過すると、ログオンパスワードを変更しなければならなくなる。	３０日程度に設定されていることを確認する（推奨）。
login/password_history_size	パスワード履歴のサイズを定義する (エントリ数)。システムでは、ユーザが以前に使用したパ スワードを再使用できない。（ユーザが自分で設定したパスワードは、パスワード履歴に格納されるが、ユーザ管理者によって設定されたパスワードは、パスワード履歴に保存されない)	３以上を推奨
Login/no_automatic_user_sapstar	SAPのプログラム中にハードコーディングされたID(SAP*）はパスワードを変更できません。ハードコーディングされたID(SAP*）を無効にするには、①SAP*をユーザマスターに登録するか、②このパラメータを”0”にすることで無効化できます。	①または②を必ず実施すること

５．内部統制レベルアップへの取り組み

IDES（Internet Demonstration and Evaluation System）

IDESとは仮想企業のデータが予め格納された評価、検証用途向けのシステム
モデル企業は複数の海外子会社をもつ国際的なグループによって構成されている。
SAP システムで実行可能なさまざまなビジネスシナリオに対応するアプリケーション
データが予め用意されている。



課題：伝票フローを確認するために、本番環境での検証が不可欠
標準で準備されている監査人用ロールでは対応できない

- ■ 監査人にユーザが業務で使用するトランザクションの利用権限を本番環境上で付与することは、誤って業務データを変更、削除するリスクがあり適切でない
- □ SAPのトランザクションの実行をトレースするため、実行結果を保存できない権限を作成し、監査人に付与することで対応できる

SAP_ALL_DISPLAY

SAPの古いバージョン（4.7以前）では標準で装備されていたが、
以降のバージョンでは装備されない。

SAPの古いバージョンのSAP_ALL_DISPLAYの定義情報を抽出し
新しい環境にインポートすることで利用可能　（IDES環境で検証）

副次的な利用として、ユーザサポート担当者にSAP_ALL_DISPLAYを付与し、
業務データに影響を与えずに操作指導を行える様にすることが可能になる

研修・マニュアル

1. SAP概要

- 1-1. ERPとしてのSAP
- 1-2. SAPの歴史
- 1-3. SAPモジュールの構成
- 1-4. SAPのカスタマイジングとアドオン
- 1-5. SAPのメニューとトランザクションコード

2. SAPのITGC

- 2-1. 本番環境の保護と移送
- 2-2. アクセス制御の仕組み
- 2-3. 高権限ID/高権限プロファイル
- 2-4. 各マスタファイルへのアクセス制御
- 2-5. ログ管理
- 2-6. 不備事例

3. SAPのITAC

- 3-1. 組織構造
- 3-2. 販売プロセス
- 3-3. 購買プロセス
- 3-4. 在庫管理プロセス
- 3-5. 売上原価の求め方
- 3-6. 生産管理プロセス

■ SAP内部統制に関するキーコントロールに対して、自己点検結果をY/Nで回答する自己点検CS入力支援ツール

○ 統制要求を具体的にSAP上でどのように実装しているかを質問しているため、抽象的な統制要求に比べより明確な統制実装の状況を評価できる

○ キーコントロールに対する認識を被監査部門と監査人の間で一致させることができる

#	Key Points	回答	補足、回答がY以外の場合の理由、代替の統制、等
1	SAP*を使用できる者は最小限に限定されている。	Y	
2	SAP_ALLを付与されているIDは最小限に限定されている。	Y	
3	DDICを使用できる者は最小限に限定されている。	Y	
4	SAPCPICを使用できる者は最小限に限定されている。	Y	
5	EARLYWATCHはロックされている。	Y	
6	SAP_NEWを付与されているIDは最小限に限定されている。	Y	

項目番号	確認内容
ITGC01	開発案件のテスト実施の際の本番環境の保護
ITGC02	障害対応結果の適切性確認
ITGC03	プログラムの本番登録手続と登録権限者の限定
ITGC04	プログラム本番登録の事前承認
ITGC05	役割と職責に応じたアクセス権限
ITGC06	アクセス権限を行使する個人の特定
ITGC07	パスワード管理ルール
ITGC08	高権限操作者の操作内容の確認

販売	監査項目内容
1	得意先マスタのアクセス制限
2	販売価格マスタのアクセス制限
3	EDIで受信する受注データの登録処理
4	受注入力のアクセス制限
5	受注入力(殊に販売単価)
6	出荷指示データ作成処理
7	各社(各部門)が採用する売上計上基準への準拠

販売

購買	監査項目内容
1	仕入先マスタのアクセス制限
2	仕入先銀行口座設定機能のアクセス制限
3	仕入単価マスタのアクセス制限
4	所要量計算処理
5	所要量計算による発注データ作成処理
6	所要計画発注データの転送処理
7	仕入入力

購買

会計	監査項目内容
1	仕訳伝票および証憑に管理番号の付加機能
2	仕訳データによる仕訳日記帳作成機能
3	仕訳日記帳の合計金額の貸借の一致
4	会計システムへのデータ転送
5	会計システムのアクセス制限(システムに依る)
6	会計システムの仕訳処理機能に対するアクセス制限
7	外貨のレート換算処理

会計

販売	監査項目内容	確認内容	使用Tr-Code
1	得意先マスタのアクセス制限	アクセス権限について、下記Tr-Codeが実行可能なユーザを抽出する。 **FD01** :「得意先登録:第一画面」 **FD02** :「得意先変更:第一画面」 **FD05** :「得意先ブロック/解除:第一画面」 **FD06** :「得意先削除フラグ:第一画面」 **VD01** :「得意先登録:第一画面」 **VD02** :「得意先変更:第一画面」 **VD05** :「得意先ブロック/解除:第一画面」 **VD06** :「得意先削除フラグ:第一画面」 **XD01** :「得意先登録:第一画面」 **XD02** :「得意先変更:第一画面」 **XD05** :「得意先ブロック/解除:第一画面」 **XD06** :「得意先削除フラグ:第一画面」 **XD07** :「勘定グループ変更」 **XD99** :「一括更新」	
2	販売価格マスタのアクセス制限	アクセス権限について、下記Tr-Codeが実行可能なユーザを抽出する。 **VK11** :「条件レコード登録」 **VK12** :「条件レコード変更」 ・【確認1】販売価格マスターへのアクセス権が設定されたユーザを抽出するまでの、帳票の起動方法、抽出条件の入力方法、抽出結果の見方を紹介する。	**SUIM** : ユーザ>複合選択基準別ユーザ>複合選択基準別ユーザ **SA38** :「ABAP:プログラム実行」 **S_BCE_68001400** :「複合選択基準別ユーザ」
3	EDIで受信する受注データの登録処理	・【確認1】EDIを受信できる設定がされていることを確認する。 ・【確認2】IDoc一覧よりEDIによる受信状況が適切にモニタリングされていることを確	**WE20** :「パートナプロファイル」 **WE05** :「IDoc 一覧」

◇不正監査SAP版研修
不正防止の設定確認方法や事後的に不正を発見するための手法を習得し，不正監査の実施を目指す

■全10回の研修受講(知識研修，データ分析演習) ： 3ヶ月間
■不正リスクシナリオ/データ分析シナリオの作成

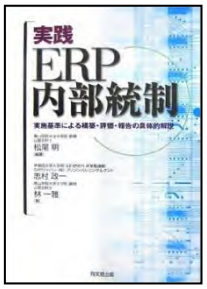
SAP不正監査の実施により，国内外で広く使用されているSAPに係る不正リスクを軽減し，健全な経営に寄与する

Day 1 前提知識①
Day 2 前提知識②
Day 3 前提知識MM編(購買)
Day 4 前提知識MM編(在庫)
Day 5 前提知識SD編(販売管理)
Day 6 前提知識NW・権限管理編
Day 7 データ分析演習①（FI：会計）
Day 8 データ分析演習②（MM：購買在庫Ⅰ）
Day 9 データ分析演習③（MM：購買/在庫②）
Day10データ分析演習④（SD：販売）

1. 「SAP ERP IT全般統制チェックリスト　概要解説書」
2009年12月　システム監査学会　会計システム専門監査人部会
http://www.sysaudit.gr.jp/senmon/jssa-cmaas-b_saperp_itgi_ChecList(gaisetsu).pdf

2. 「セキュリティ，監査，コントロールの特徴　SAP R/3 第2版
テクニカル/リスク・マネジメントリファレンス・ガイド」
2008年1月　ISACA　絶版

3. 「実践ERP内部統制」
2007年4月　松尾明[編著]，同文舘出版



4. 「IT内部監査人」
2010年12月　ISACA監査基準研究会，生産性出版

■ お問い合わせ先

三洋電機株式会社

品質・業務推進センター　IT統制推進部

中川 昭仁

Mail：nakagawa.aki@jp.panasonic.com

ご清聴ありがとうございました

S-ITCPD