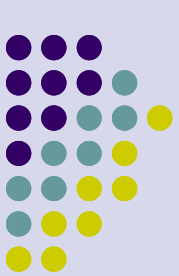
SAPシステム　権限管理

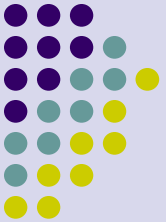


株式会社　スカイテック

はじめに

- 本書では、SAPシステムに共通する権限の管理とその環境について管理および設定方法の概要を記します。

トレーニングの概要



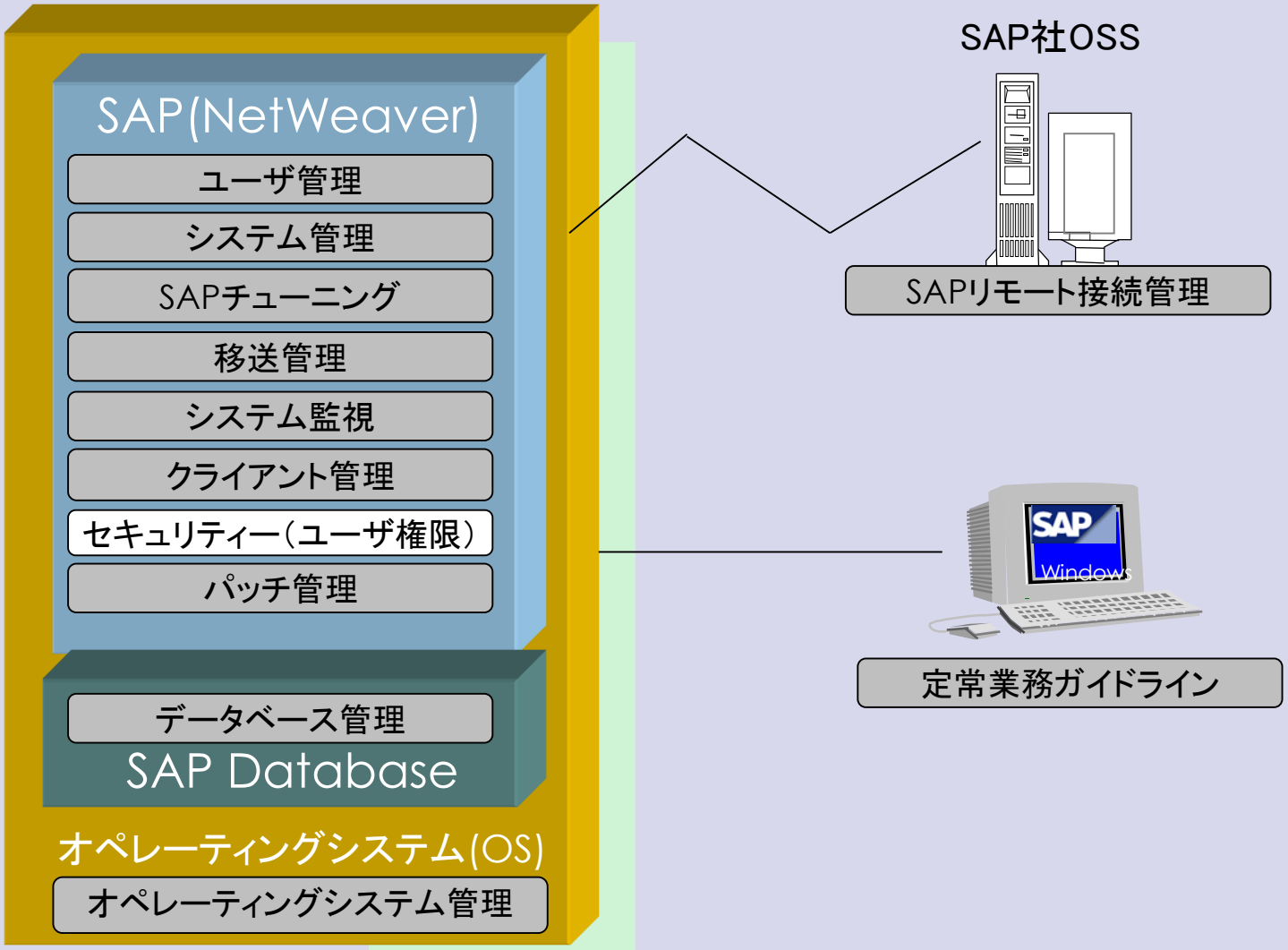
1. 権限管理の位置付け
2. SAPシステムの構造
3. クライアント
4. システムランドスケープ
5. SAPシステムのセキュリティ　概要
6. SAPシステムでの権限設計
7. 権限の設定
8. 権限テスト環境
9. 権限設定　モデル運用フロー
10. ユーザ比較

目的

- SAPシステムの「権限」について、クライアント構造との関係を知ることができます。
- SAPシステムの「権限管理」の概要と設計、ならびに設定の基礎を知ることができます。

1. 権限管理の位置付け

SAPの運用におけるBASIS運用スキルのうち、権限管理の位置付けを示します。



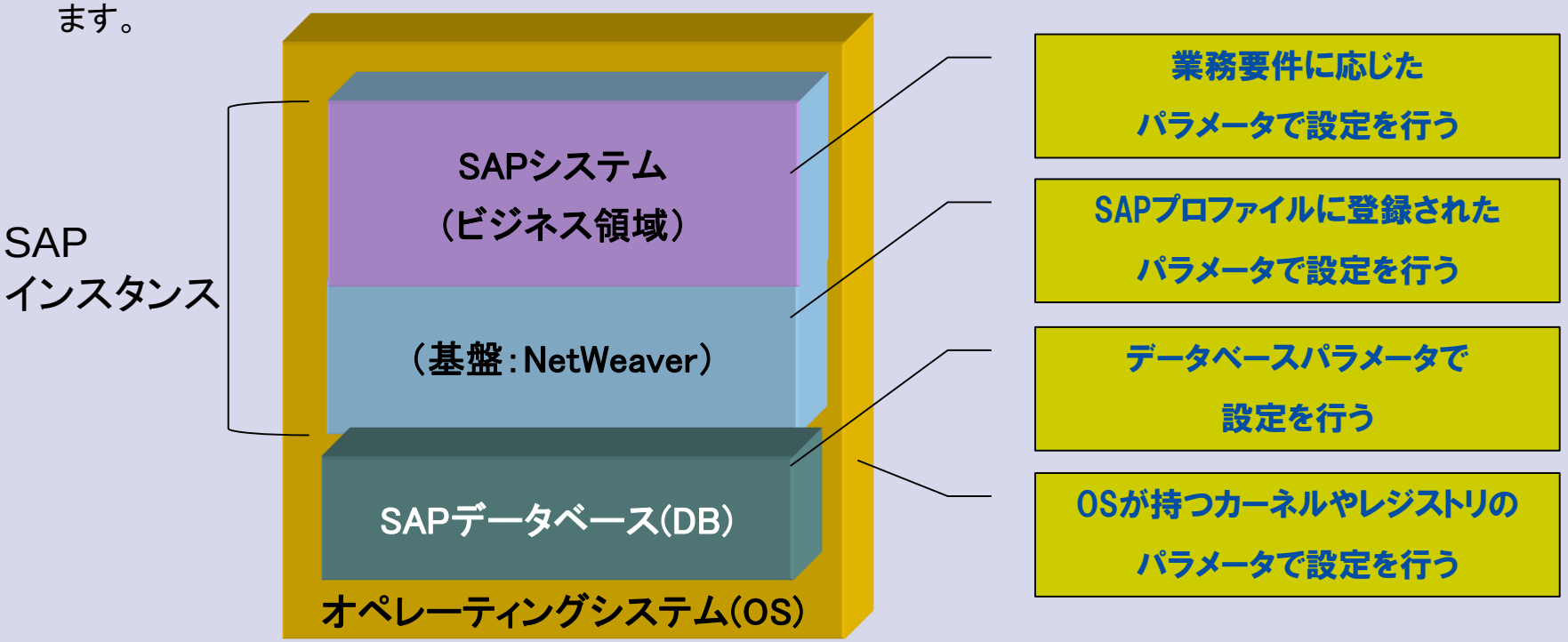
2．SAPシステムの構造

・SAPシステムは、オペレーティングシステム(OS)、データベース(DB)、SAPシステム（ビジネス領域と基盤領域）の3つの要素から成り立っています。

・SAPシステムは1つ以上のSAPインスタンスから構成されています。

・SAP システムの設定を変更する場合、OSであればカーネルパラメータ（UNIX/Linux）/レジストリ（Windows）が、データベースであればデータベースパラメータが、SAPシステムに対しては基盤領域ではSAPプロファイル（パラメータ）を、ビジネス領域では業務要件に応じたパラメータをそれぞれ変更します。

・ビジネス領域では、インスタンスの要件に適合するように、個別構成パラメータをカスタマイズすることができます。

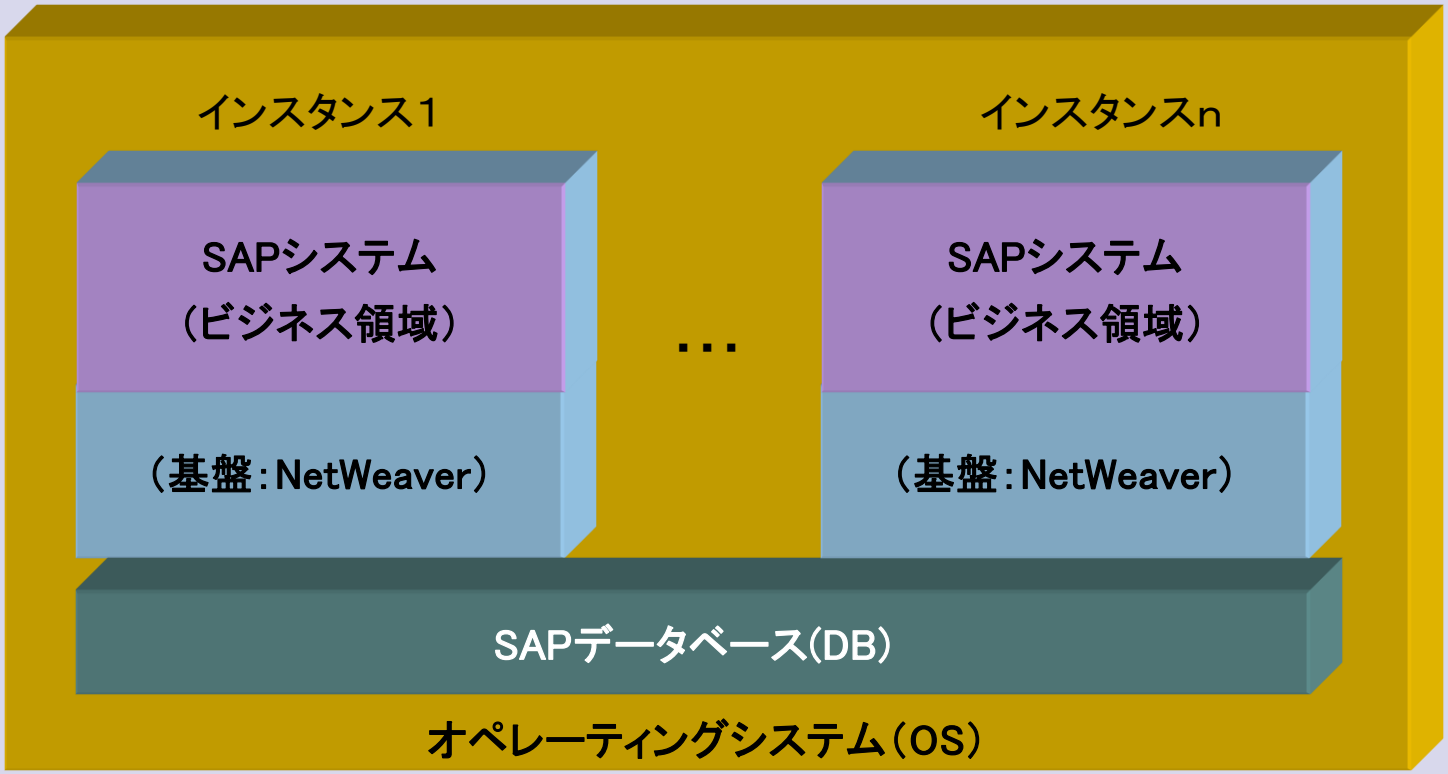


2．SAPシステムの構造

・SAPシステムは1つ以上のSAPインスタンスから構成されています。

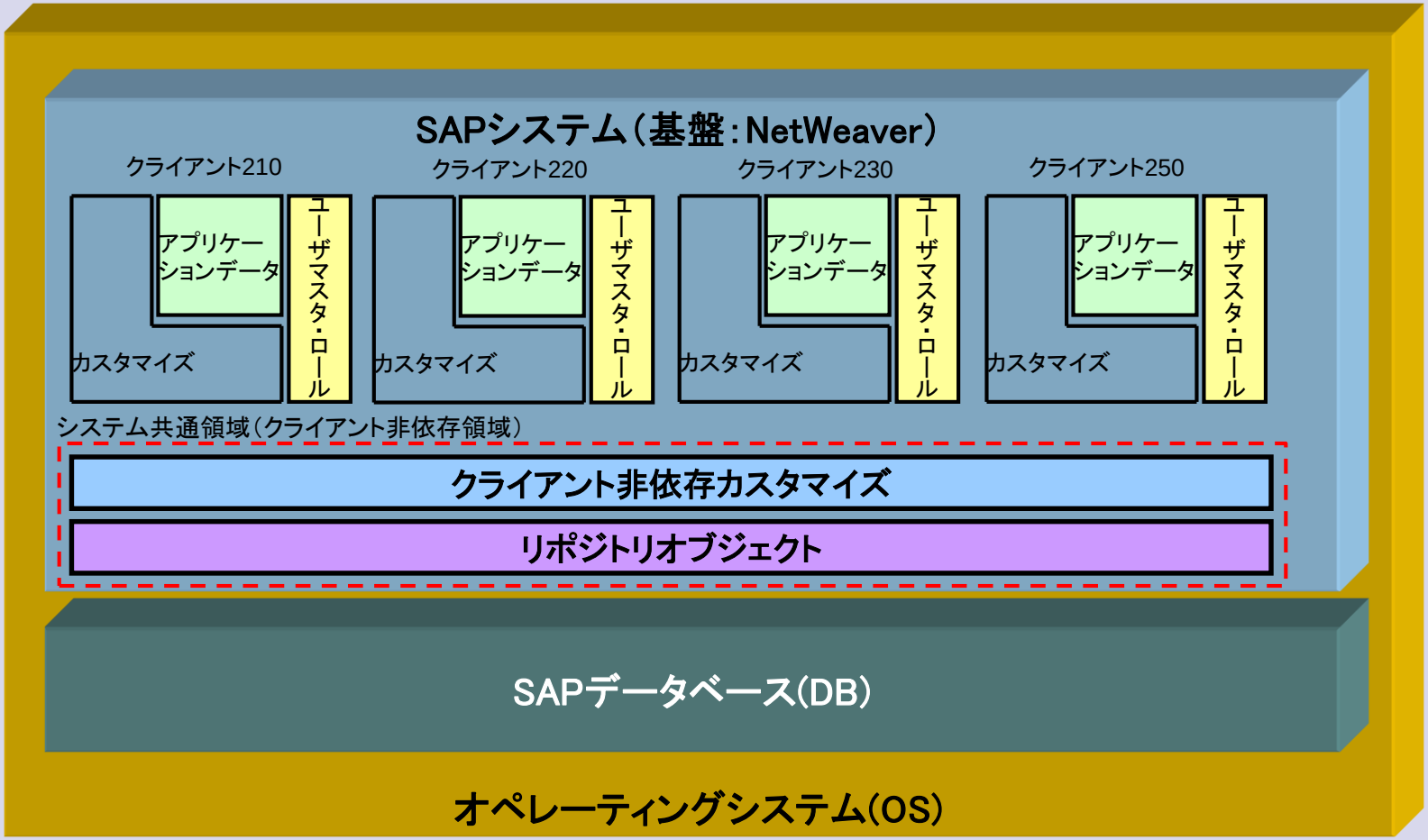
・個々のSAPインスタンスがデータベースを使用する場合、データの混用が行わないようシステムIDで区切られています。

・SAP社ではSAPシステムの構成については、原則として1サーバ1インスタンスと規定しています。



2．SAPシステムの構造

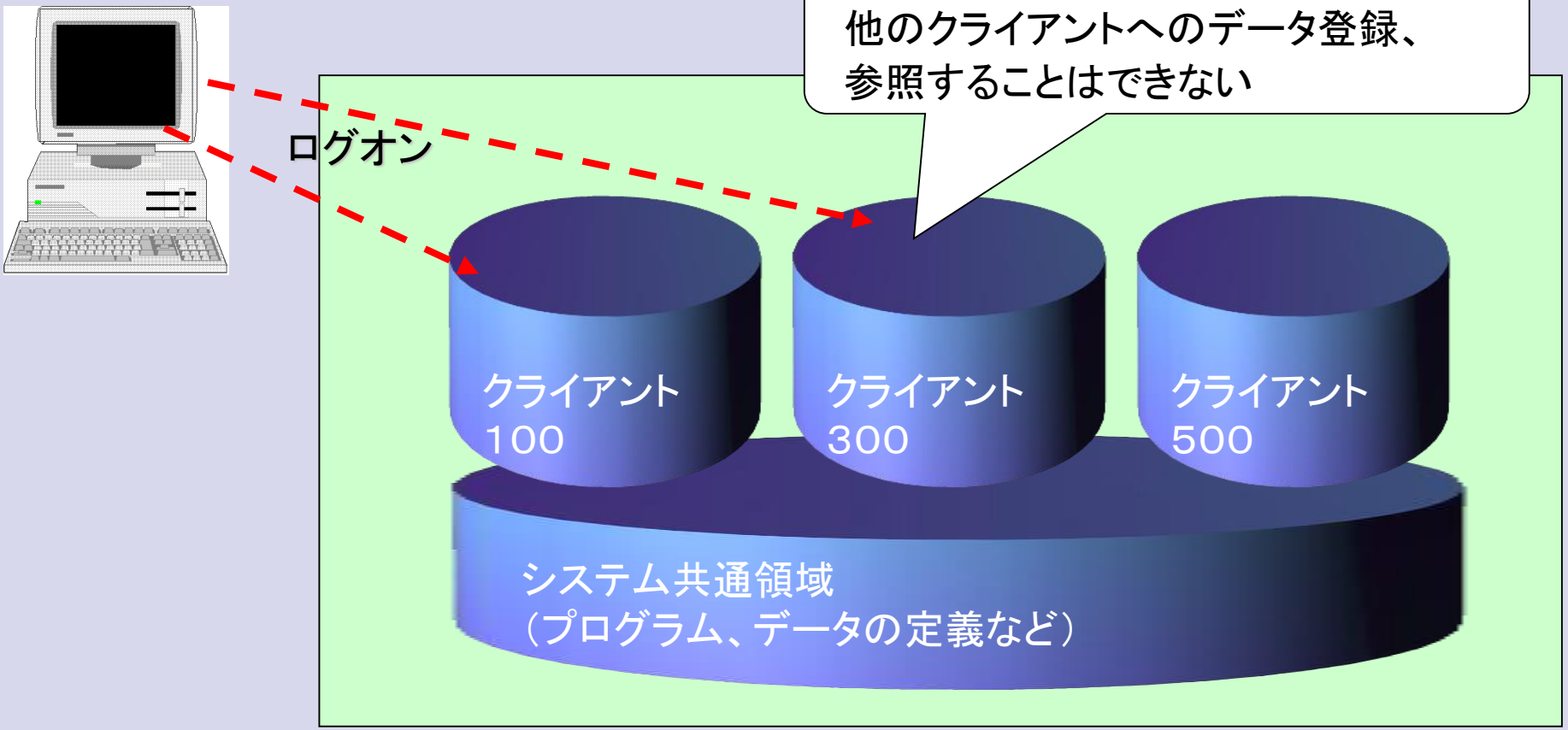
- 前ページの図からSAPインスタンスを取り出し詳細化すると、下図のようになります。



３．クライアント

- SAPシステム（インスタンス）の「クライアント」とは、**「業務、組織、及びデータ面で独立したSAPシステム内の１単位」**になります。

- 各クライアントは固有のビジネスデータ環境と、それを支える固有のマスタデータ、トランザクションデータ、固有のユーザデータを持っています。



３．クライアント

【前ページの説明】

・SAPのシステムは図に示すようなクライアントシステムです。
　クライアントのコンセプトとして、1つのシステムで互いに独立した複数の企業の業務を行うことができます。

・各ユーザセッションでアクセスできるのは、ログオン時に選択したクライアントのデータのみです。

・クライアントとは、SAPシステム内で独立した構成単位のことです。
　各クライアントには独立したデータ構造、つまり、独自のマスタデータおよびトランザクションデータ、ユーザマスタレコードと権限ロール、勘定コード表、また固有のカスタマイジングパラメータがあります。

3．クライアント

- SAPシステム初期インストール時点でのクライアントについて

SAPシステムの初期インストールが終了した時点では、以下の３クライアントが設定されています。

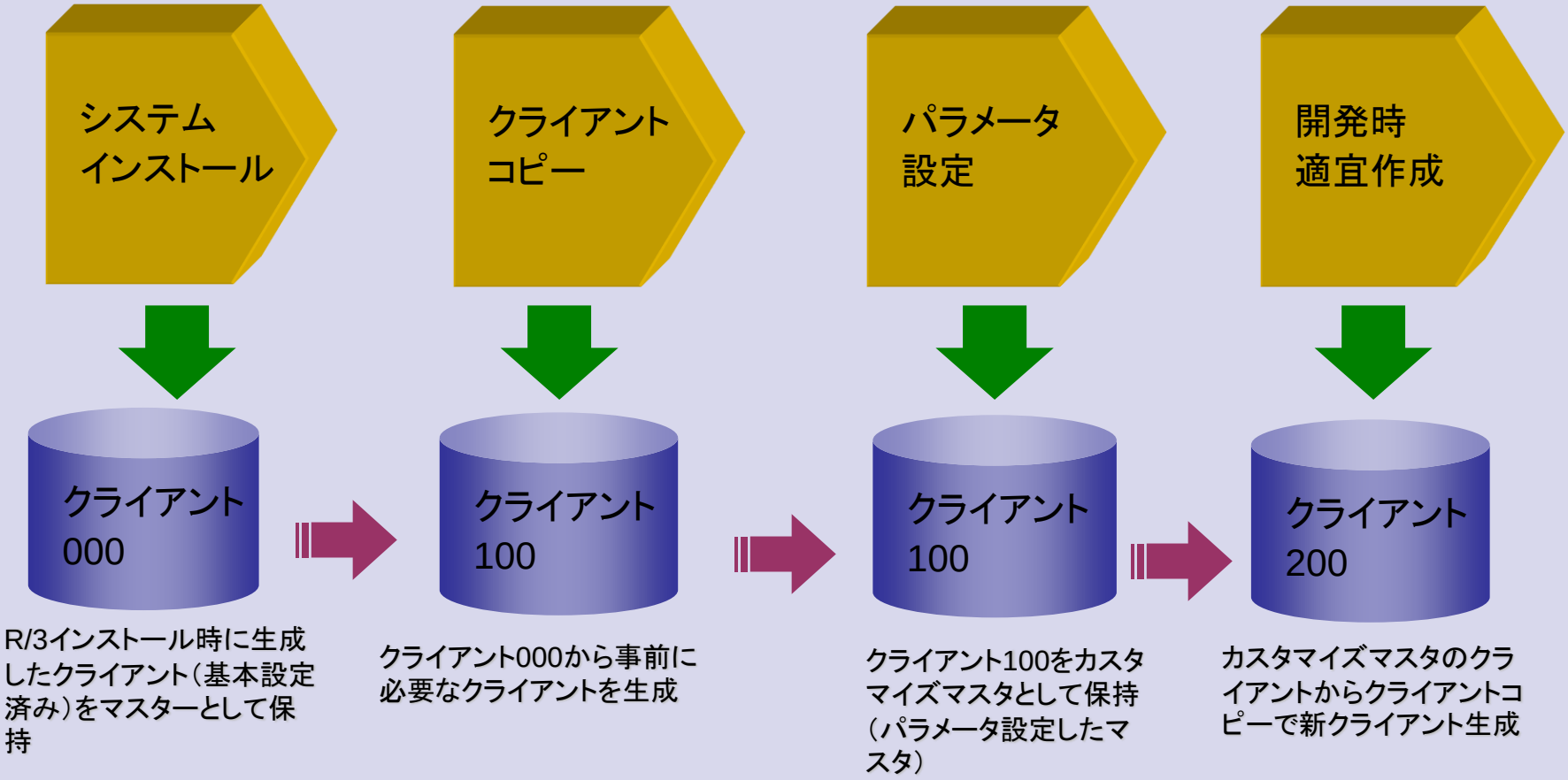
クライアント	000、001		066
特殊ユーザ	SAP*	DDIC	EarlyWatch
初期パスワード	06071992	19920706	support

（注意）これらの特殊ユーザは誰もが知っているユーザなので　無権限のアクセスから保護する必要があります。

3．クライアント

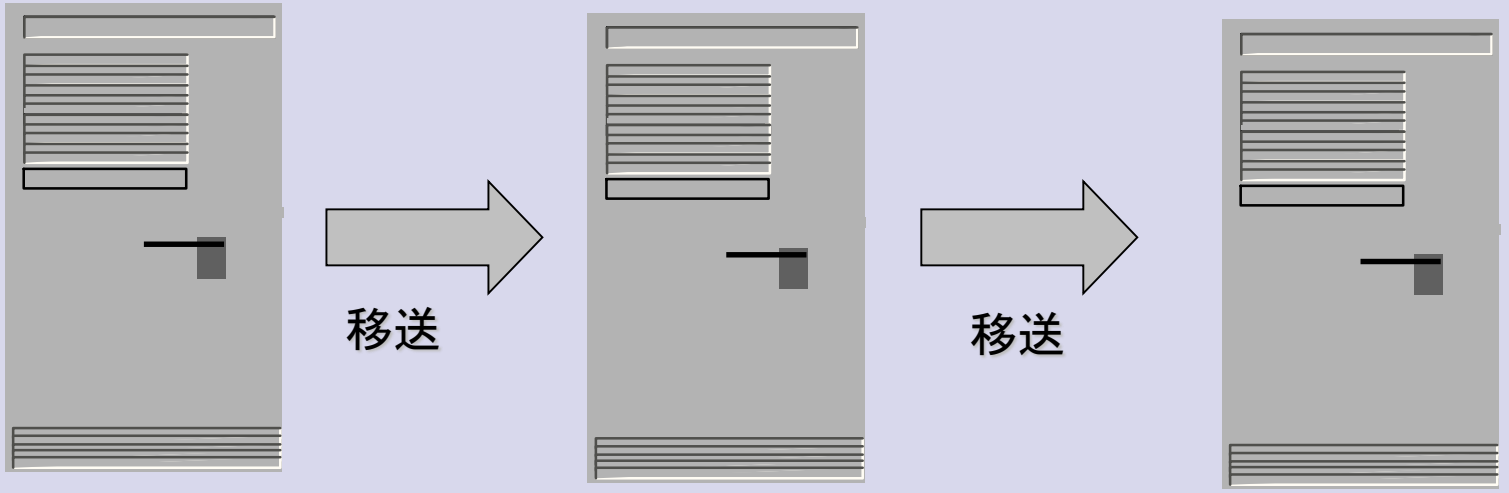
クライアント（一般的な開発機構成例）

通常、クライアントを下記の通り、複数作成することが一般的に行われています。



4．システムランドスケープ

SAP社では3システムランドスケープを推奨しております。



開発機
カスタマイズ用システム

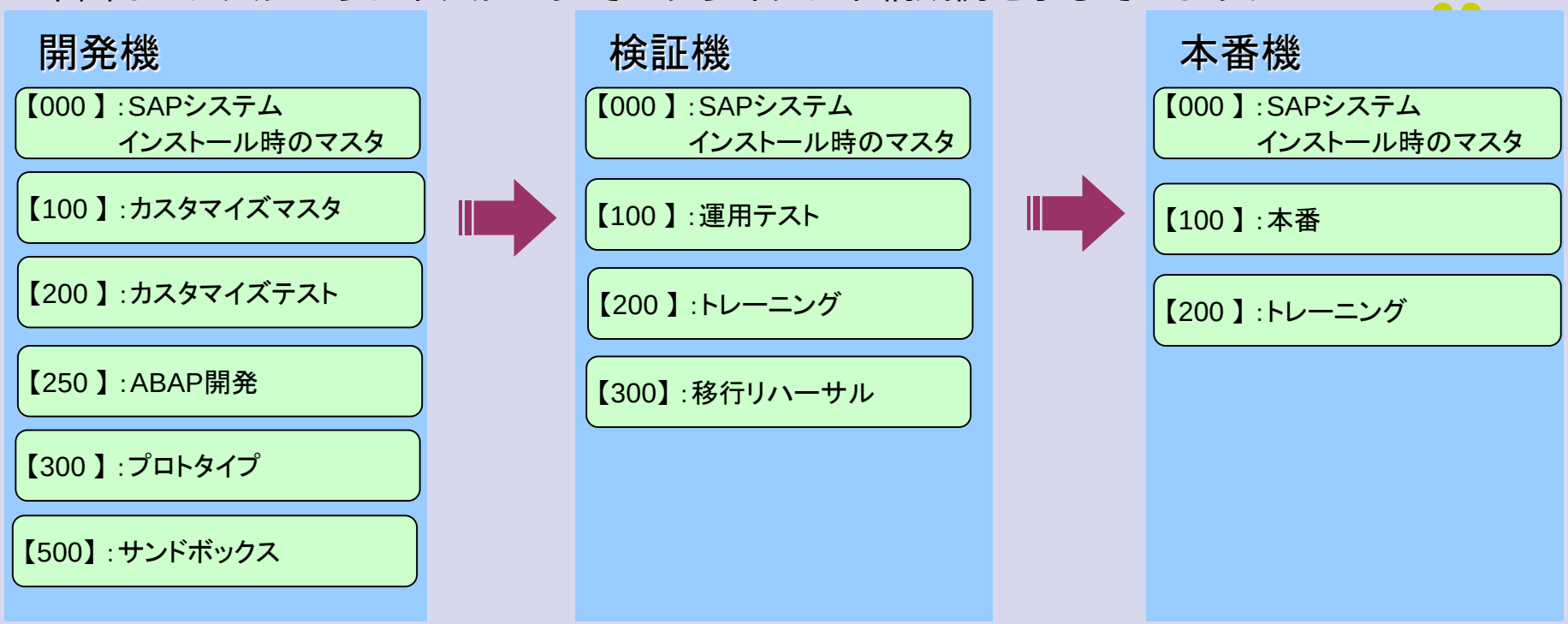
テスト機
ユーザテスト用システム

本番機
本稼動用システム

※1システム＝1インスタンス

4．システムランドスケープ

下図は３システムランドスケープでのクライアント構成例を示しています。



・カスタマイズマスタ:
パラメータ設定のマスタとして補完
・カスタマイズテスト:
パラメータ設定をテストするクライアント
・ABAP開発:ABAPプログラム開発、
テスト用クライアント
・プロトタイプ1,2:プロトタイプ評価用
・サンドボックス:単体テスト環境

・運用テスト:お客様運用テスト用
クライアント
・トレーニング:トレーニング用
クライアント
・移行リハーサル:本番機への移行
リハーサル実施用
クライアント

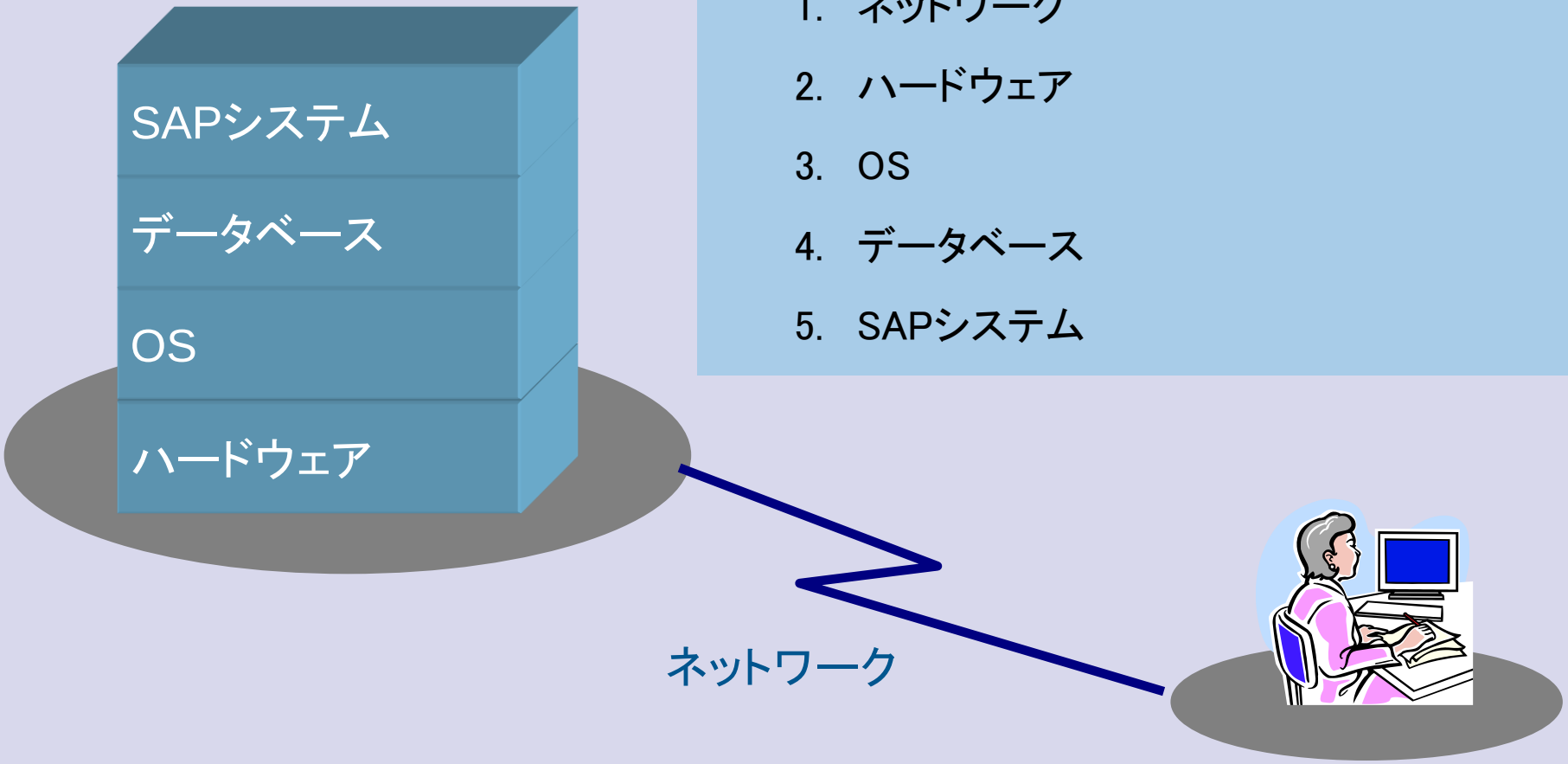
・本番:本番用クライアント
・トレーニング:トレーニング用
クライアント

5．SAPシステムのセキュリティ　概要

5.1　SAPシステムで考慮すべき「セキュリティ」のポイント

SAPシステムでセキュリティを考えるポイントは・・・

1. ネットワーク
2. ハードウェア
3. OS
4. データベース
5. SAPシステム



5．SAPシステムのセキュリティ　概要

5.1　SAPシステムで考慮すべき「セキュリティ」のポイント　解説

セキュリティに関して、コンサルタントが受け持つ領域での役割分担を下表に記します。

No.	セキュリティレベル	具体例	SAP業務領域	SAP Basis領域	インフラ領域
1	ネットワークレベル	ネットワークセグメント分離、ファイアーウオール等	×	一部●	●
2	ハードウェアレベル	マシンルームに入る人を制限、ラックに鍵をする等	×	×	●
3	OSレベル	OSユーザ、ファイルアクセス権限、アンチウイルス等	×	一部●	●
4	データベースレベル	DBユーザ、SAPシステムを介さないデータベースアクセス　*1	一部●	一部●	一部●
4	SAPシステムレベル	SAPユーザ、適切な権限の付与 *2	一部● *2	一部● *2	×

*1：インタフェースアプリケーションなど。
*2：権限ロール設計に関してはSAP各業務領域が、設定に関してはBASIS領域のコンサルタントが主対応。

5．SAPシステムのセキュリティ 概要

5.2 ネットワークでの「セキュリティ」補足 ネットワークセグメント

◆おさらい – IPアドレス/ネットワークアドレスとは

ネットワークセグメントについて説明する前に、IPアドレスやネットワークアドレスの意味を理解する必要があります。
IPアドレスとは簡単に言うと、ネットワーク通信する上での住所です。

端末は他の端末と通信をやり取りしたいとき、自分の住所と相手の住所を記載した上でデータを送ります。
相手の端末まで届くと送り手の住所が分かるので、返信が必要な場合は同じように自分の住所と相手の住所を記載し、 データを送ります。

今やIPはインターネットでも利用されている、世界標準の通信方法です。インターネット通信をする端末は、基本的に IPアドレスが割り振られています。

IPアドレスは32bitで構成され、8bitずつ10進数に変換し、.(ドット)で区切られて表現されます。

IPアドレスはネットワーク部とホスト部に分けることができ、ネットワーク部を表現したアドレスを特に **ネットワークアドレス**と呼びます。
例えば、192.168.1.254というアドレスがあるとき、ネットワーク部を 先頭から24bitとしたとき、ネットワークアドレスは192.168.1.0となります。（次ページの表参照）

5．SAPシステムのセキュリティ　概要

5.2　ネットワークでの「セキュリティ」補足　ネットワークセグメント

表：IPアドレス/ネットワークアドレス

IP アドレス：192.168.1.254　　↓先頭24bitがネットワーク部

	第1オクテット	第2オクテット	第3オクテット	第4オクテット
2進数	11000000	10101000	00000001	11111110
10進数	192	168	1	254

末尾8bitがホスト部↑

ネットワークアドレス：192.168.1.0

	第1オクテット	第2オクテット	第3オクテット	第4オクテット
2進数	11000000	10101000	00000001	00000000
10進数	192	168	1	0

◆ネットワークセグメントとは

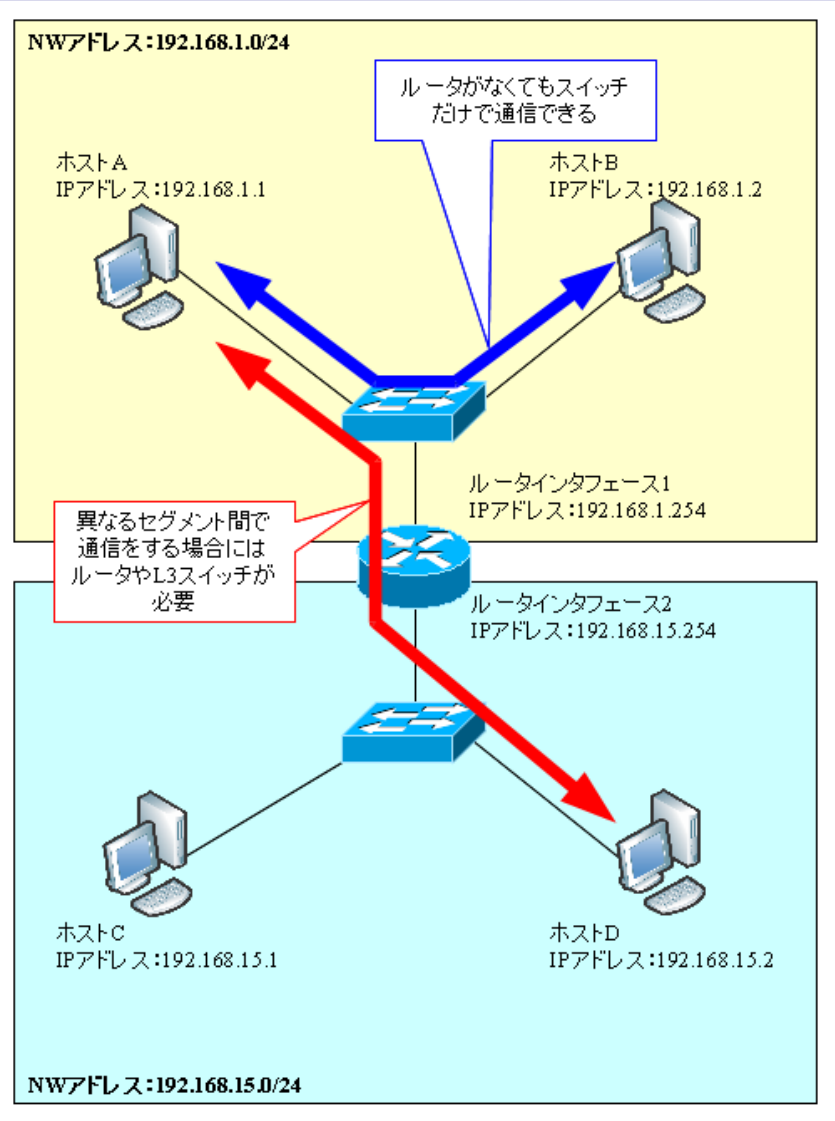
ネットワークアドレスを別名でネットワークセグメント、もしくは単にセグメントと呼ぶこともあります。

同じネットワークセグメント内のホスト同士はハブやL2スイッチだけで通信ができ、異なるネットワークセグメントのホスト同士は、ルータやL3スイッチにより通信ができるようになります。

5．SAPシステムのセキュリティ 概要

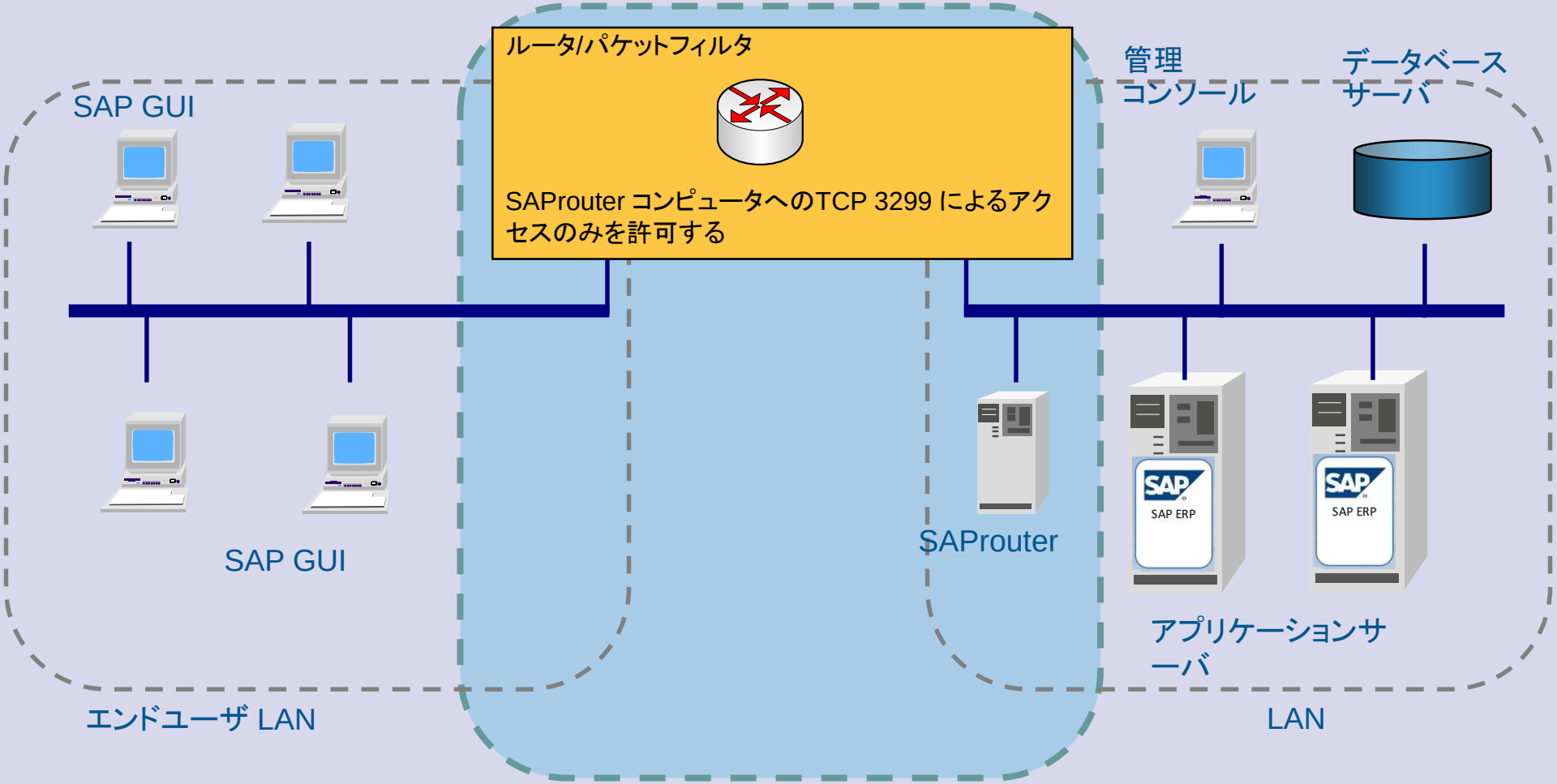
5.2 ネットワークでの「セキュリティ」補足 ネットワークセグメント

図：ネットワークセグメント



5．SAPシステムのセキュリティ　概要

5.2　ネットワークでの「セキュリティ」



※ 上記構成は一例です。

5．SAPシステムのセキュリティ　概要

5.2　ネットワークでの「セキュリティ」

SAPシステムに関連するポートは以下のとおりです。

接続の種類	サービス名	接続の向き	例 <nn> = 01
SAPgui – SAPシステム (直接接続)	sapdp<nn>	→ (外 → 内)	3201
SAPgui – SAPシステム (グループログオン)	sapms<sid>	→ (外 → 内)	3600
外部RFCクライアント – SAPシステム	sapgw<nn>	→ (外 → 内)	3301
RFCサーバ – SAPシステム	sapgw<nn>	← (内 → 外)	3301
SAPシステム– SAPlpd (プリンタ)	printer	←→ (双方向)	515
外部のすべてのシステム – SAProuter	sapdp99	→ (外 → 内)	3299

・「接続の向き」はSAPシステムのあるネットワークセグメントから見て判断します。
　　* 外→内：データセンタ外から、SAPシステムのあるネットワーク（セグメント）へ
　　* 内→外：SAPシステムのあるネットワーク（セグメント）から、データセンタ外へ

5．SAPシステムのセキュリティ　概要

5.2　ネットワークでの「セキュリティ」　解説

・「接続の向き」はSAPシステムを載せたサーバのあるネットワークセグメントからみて判断します。
　　外→内：データセンタ外から、SAPシステムを載せたサーバのあるネットワーク（セグメント）へ
　　内→外： SAPシステムを載せたサーバがあるネットワーク（セグメント）から、データセンタ外へ

・SNC (Secure Network Communications) を使用する場合は、以下のポートが必要です。
　　sapdp<nn>s (47<nn>)
　　sapgw<nn>s (48<nn>).
　　.
・ポート定義はservicesファイル
　　UNIX/Linux：/etc/services
　　Wndows：C:¥Windows¥system32¥drivers¥etc¥services
に定義されています。

※SAPしステムインストール時点で自動で定義組み込み。**マニュアルでの変更は不可。**

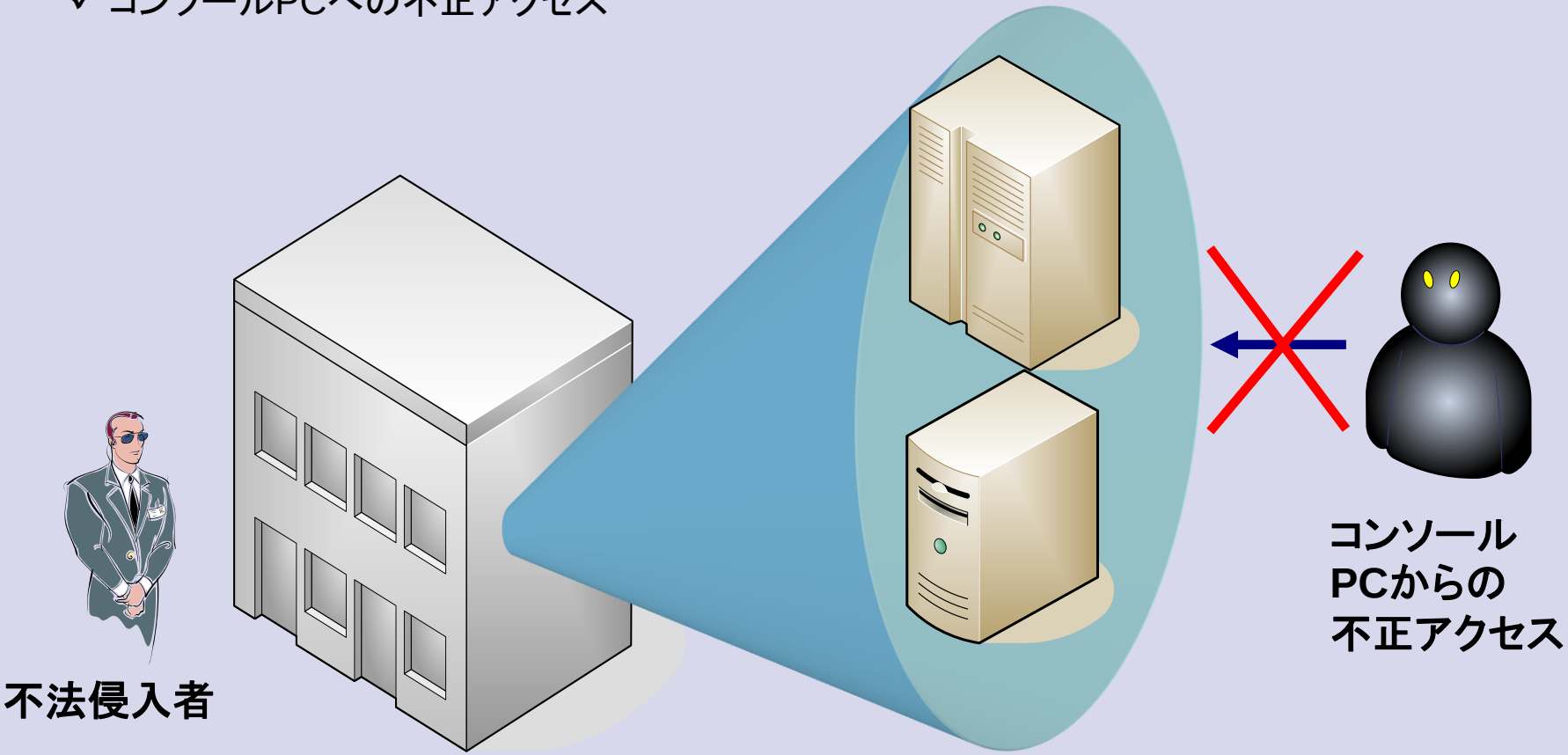
5．SAPシステムのセキュリティ　概要

5.3　ハードウェアでの「セキュリティ」

✓SAPシステムが設置されている データセンタへの侵入

✓ SAPシステムが設置されているマシンルームへの侵入

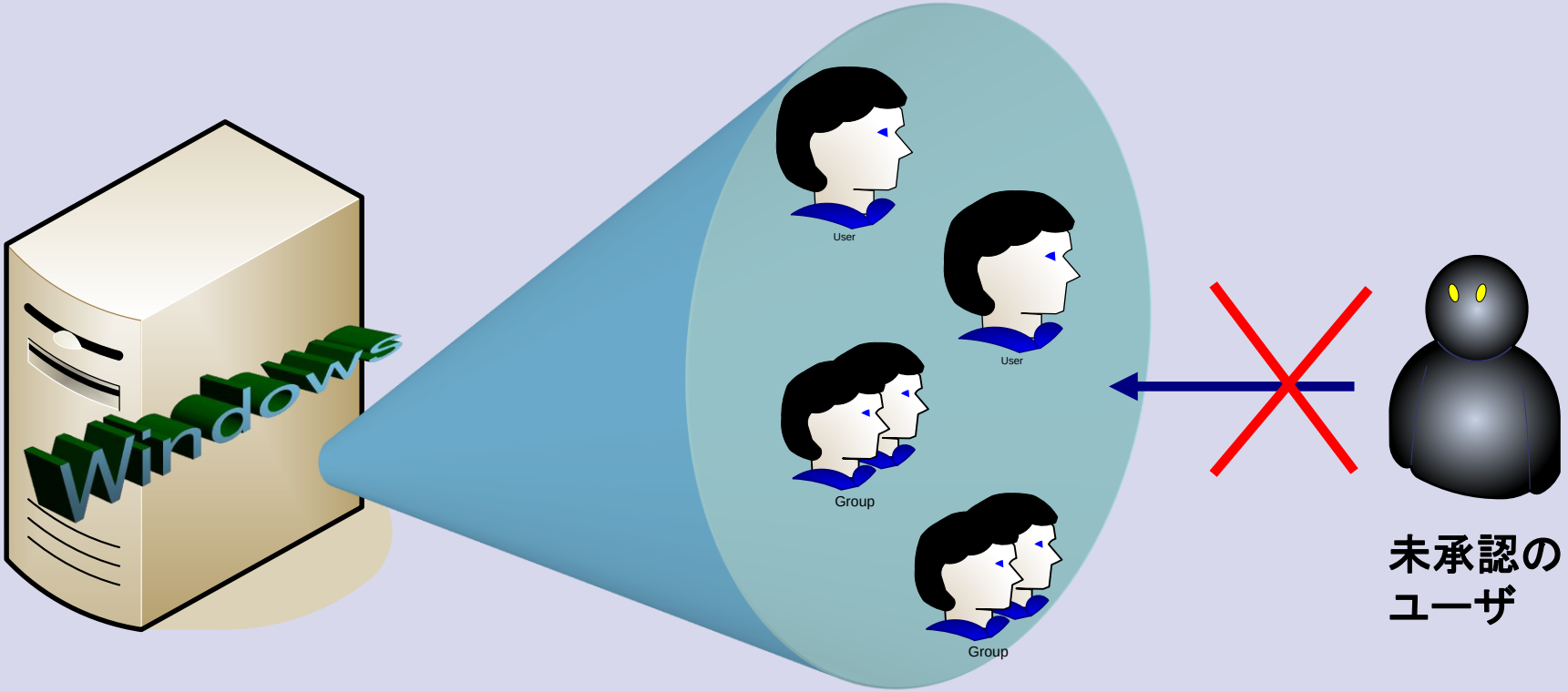
✓ コンソールPCへの不正アクセス



5．SAPシステムのセキュリティ　概要

5.4　OS（オペレーティングシステム）での「セキュリティ」

- ✓ 不要なアカウント･グループ
- ✓ 未承認のユーザによるログオン

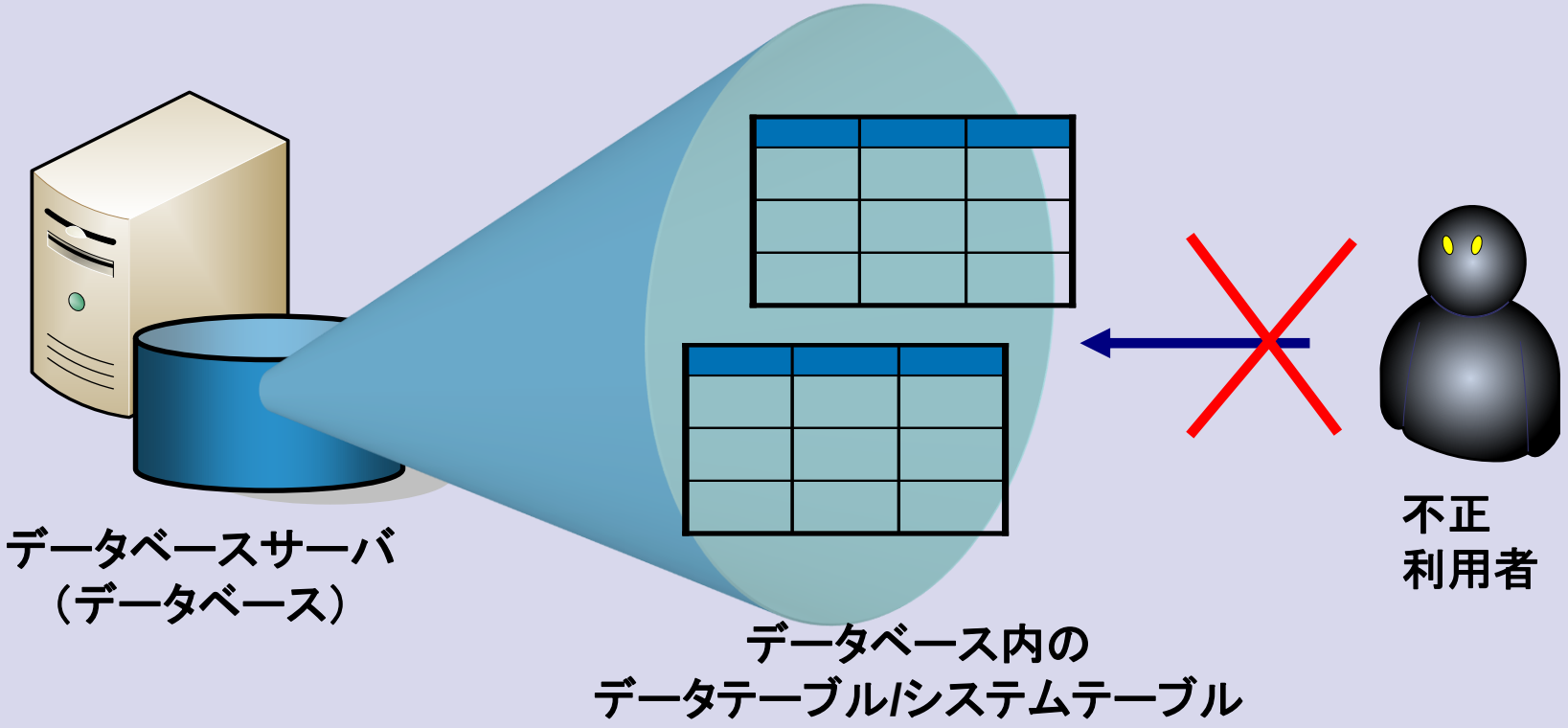


5．SAPシステムのセキュリティ　概要

5.5　データベースでの「セキュリティ」

✓デフォルトアカウントのパスワード

✓ SAP提供ツール、または認定済みツール以外でのデータベースアクセス

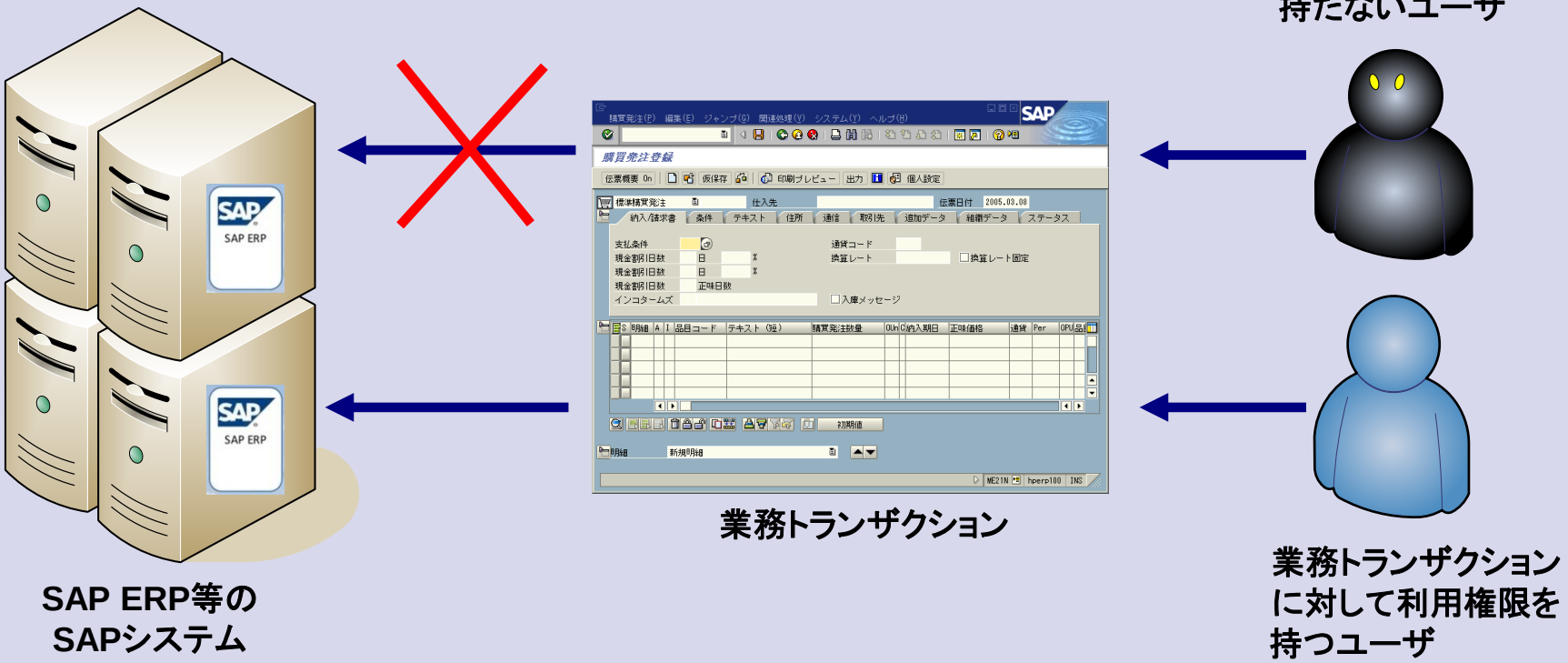


5．SAPシステムのセキュリティ　概要

5.6　SAPシステムでの「セキュリティ」

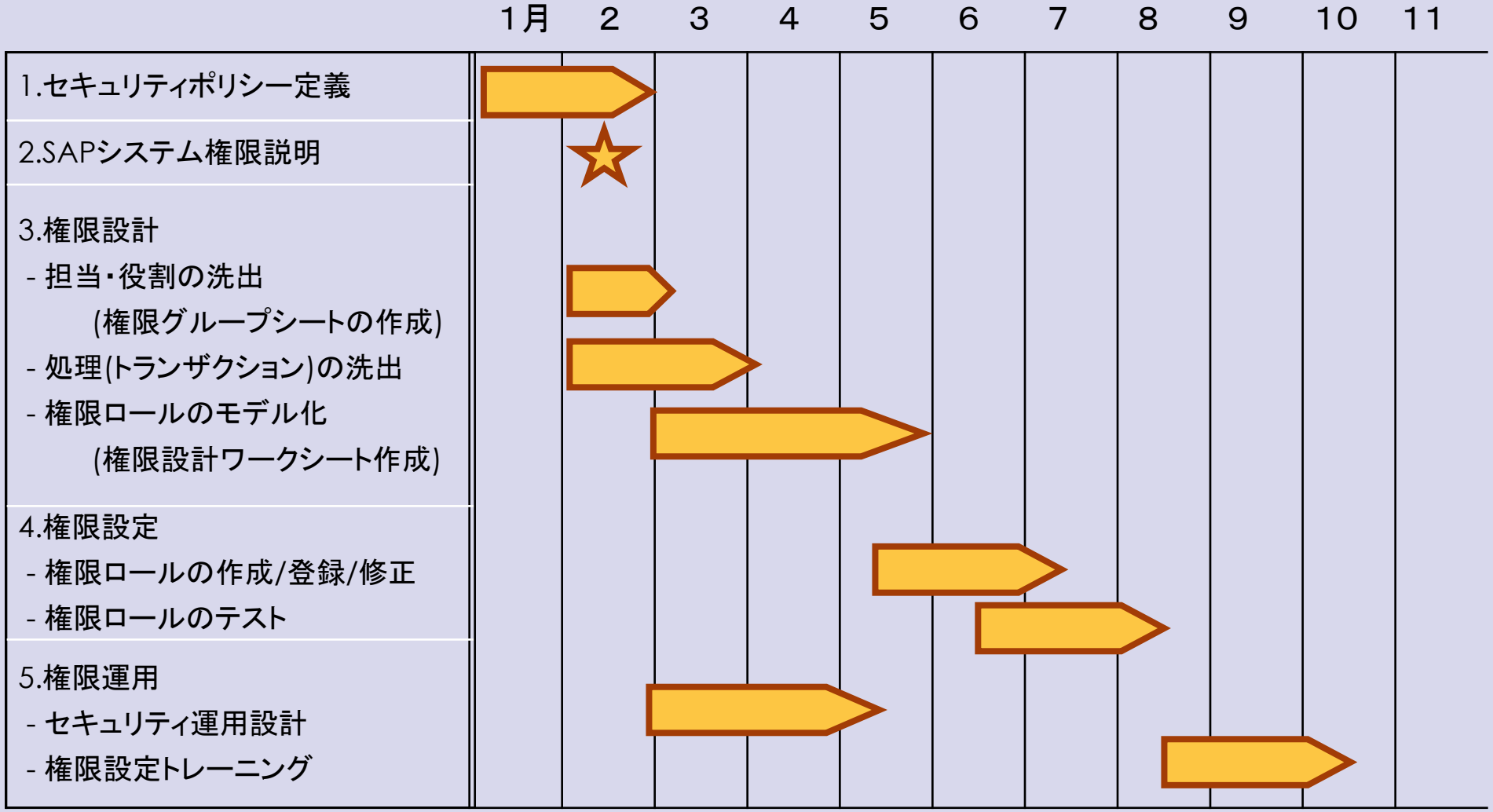
- ✓ 不要なSAPユーザIDや複数の利用者で共用しているSAPユーザID
- ✓ トランザクション毎の実行権限の制御

⇒**SAPユーザID毎に適切な権限を付与する。**



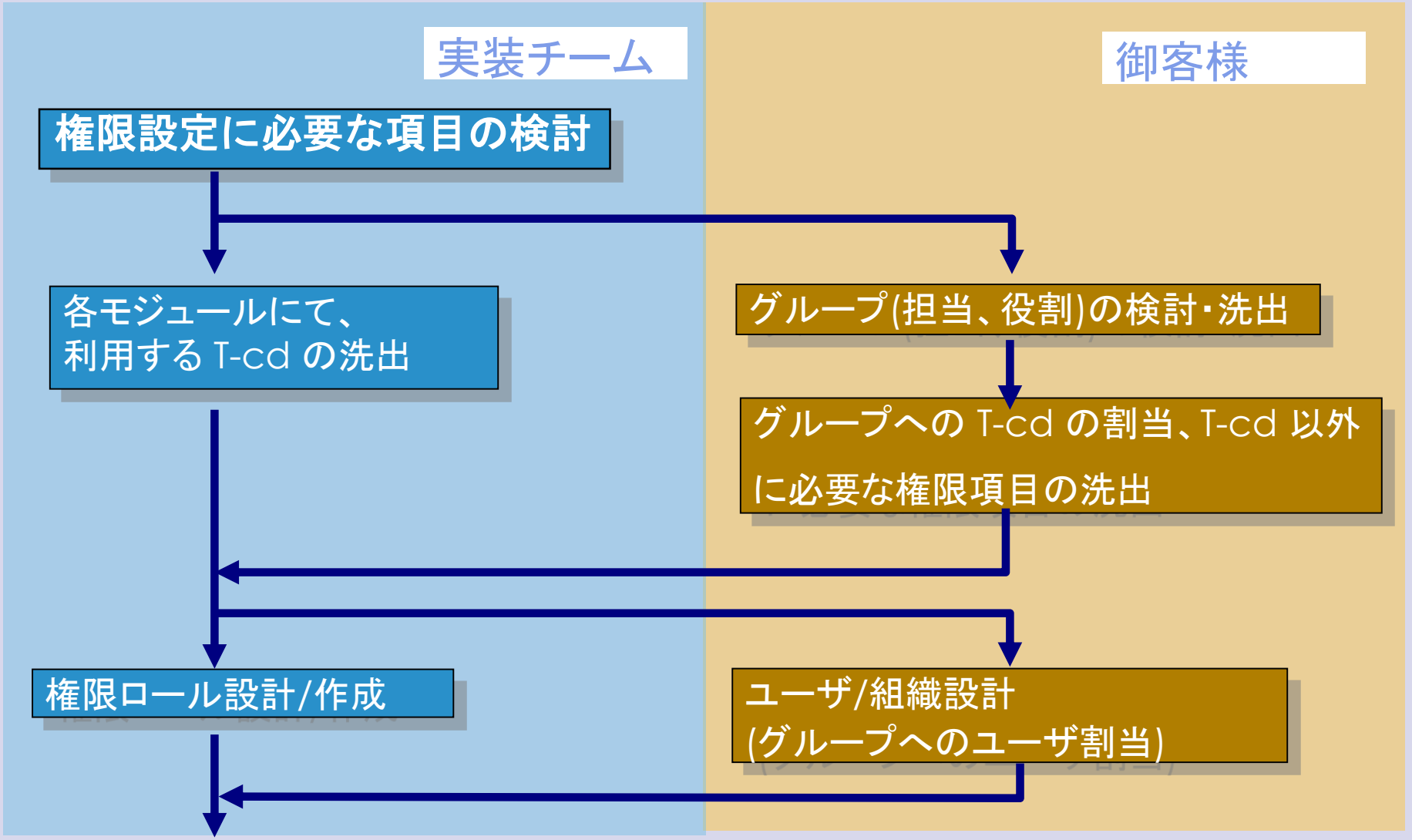
6. SAPシステムでの権限設計

6.1　権限導入スケジュールの例



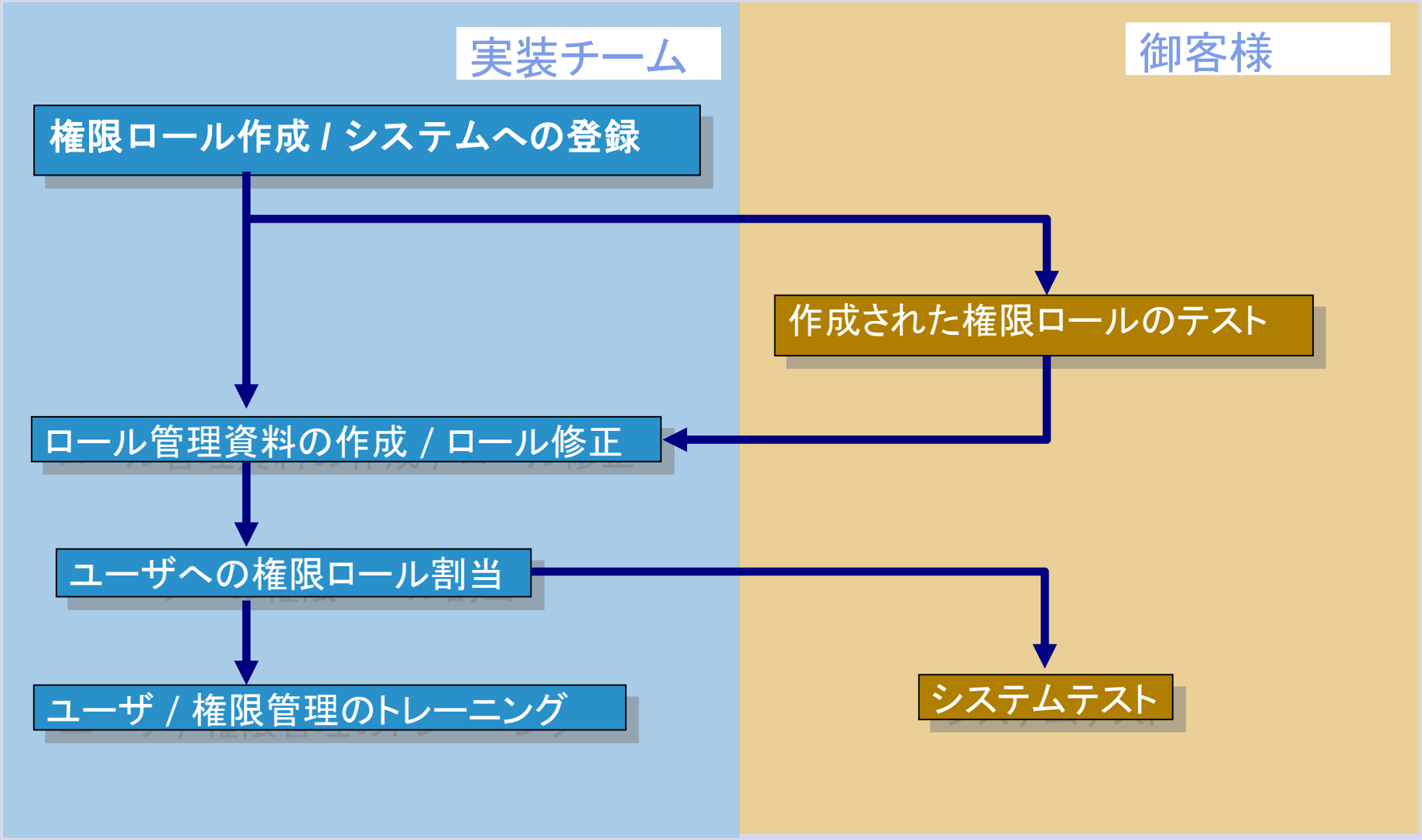
6. SAPシステムでの権限設計

6.2　権限設計フロー (1/2)



6. SAPシステムでの権限設計

6.2　権限設計フロー (2/2)



6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>SAP 権限コンセプトにより、SAP システム内のトランザクション、プログラム、サービスが、不正なアクセスから保護されます。権限コンセプトにもとづき、管理者は SAP システムでユーザがシステムにログオンし、自身を認証した後に実行できるアクションを決定する権限をユーザに割り当てます。

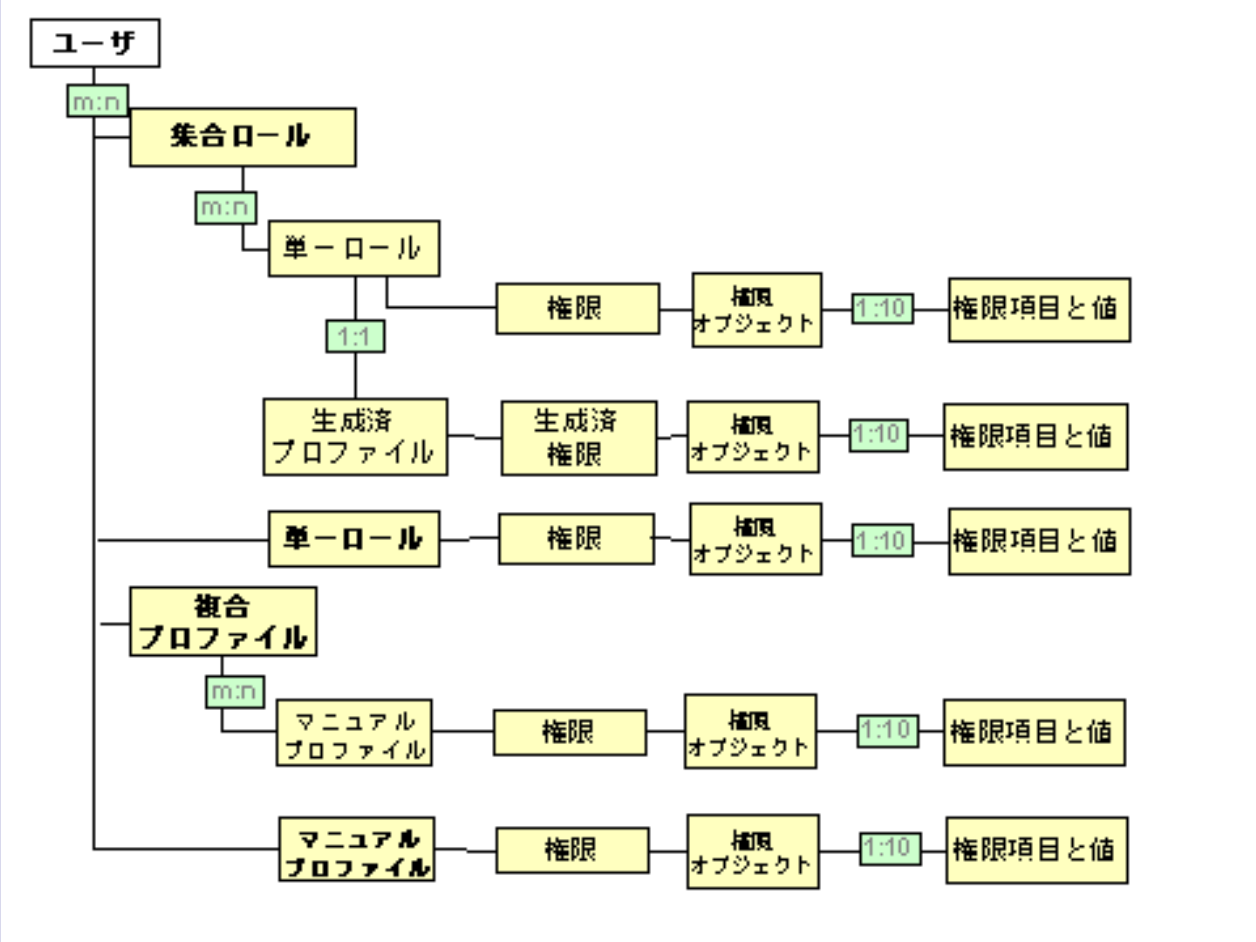
>ビジネスオブジェクトやトランザクションは権限オブジェクトによって保護されているため、ビジネスオブジェクトへのアクセス、または SAP トランザクションの実行を行うユーザには、対応する権限が必要です。権限は、一般権限オブジェクトのインスタンスを表し、従業員のアクティビティおよび責任に応じて定義されています。権限は、ロールに関連付けられた権限プロファイルに結合されます。ユーザ管理者は次に、ユーザがタスクのために適切なトランザクションを使用できるように、ユーザマスタレコードを使用して対応するロールを割り当てます。

>次ページの図では、権限コンポーネントとそれらの関係を表しています。

6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>下図では、権限コンポーネントと、それらの関係を表示しています。



6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>前ページの図の用語説明（1／4）

用語	備考
ユーザマスタレコード	ユーザマスタレコードにより、ユーザは SAP システムにログオンすることができ、ロールに指定された権限プロファイルの制限内で SAP システムの機能とオブジェクトにアクセスすることができます。ユーザマスタレコードには、対応するユーザに関する権限を含むすべての情報が含まれます。 変更は、ユーザが次回システムにログオンするまで有効になりません。変更中にログオンしていたユーザは、現セッションではその影響を受けません。
単一ロール	単一ロールは、プロファイルジェネレータを使用して登録され、これによって権限プロファイルの自動生成が可能になります。ロールには、ユーザの権限データとログオンメニューが含まれます。
集合ロール	集合ロールには、任意の数の単一ロールが含まれます。
生成済権限プロファイル	生成済権限プロファイルは、ロール更新でロールデータから生成されます。
マニュアル権限プロファイル	権限プロファイルを使用している場合は、保守作業を最小限にするため、常に、ユーザマスタレコードに単一の権限を入力せず、権限プロファイルに結合された権限を入力してください。権限への変更は、ユーザマスタレコードにプロファイルが含まれるすべてのユーザが、次回システムにログオンする際に有効となります。すでにログオンしているユーザは、この変更の影響をすぐには受けません。

6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>前ページの図の用語説明（2／4）

用語	備考
マニュアル権限プロファイル	権限プロファイルを使用している場合は、保守作業を最小限にするため、常に、ユーザマスタレコードに単一の権限を入力せず、権限プロファイルに結合された権限を入力してください。権限への変更は、ユーザマスタレコードにプロファイルが含まれるすべてのユーザが、次回システムにログオンする際に有効となります。すでにログオンしているユーザは、この変更の影響をすぐには受けません。 ⇒プロファイルの割当は、マニュアルではなく、プロファイルジェネレータで自動生成することを強くお奨めします。
複合プロファイル	複合プロファイルには、任意の数の権限プロファイルが含まれます。
権限	権限オブジェクトの定義、すなわち、権限オブジェクトの各権限項目の許容値を組合せたものです。 権限により、権限オブジェクト項目値のセットにもとづいて、SAPシステムで特定のアクティビティを実行することができます。 権限を使用することで、権限オブジェクトの項目に対して任意の数の指定値または値範囲を項目に対して指定することができます。また、すべての値を許可したり、空の項目を許容値として許可したりすることもできます。

6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>前ページの図の用語説明（3／4）

用語	備考
権限	権限を変更すると、その権限を含む権限プロファイルを持つすべてのユーザが影響を受けます。 システム管理者は、次の 2 つの方法で権限を変更することができます。 ● ロール更新で、SAP デフォルトを拡張および変更することができます。 ● マニュアルで権限を変更することができます。 これらの変更は、権限が有効化されるとすぐに関連するユーザに対して有効になります。 機能をプログラミングするプログラマは、権限をチェックするかどうかを決定し、チェックする場合は場所と方法を決定します。プログラムによって、ユーザは特定のアクティビティに対して適切な権限を持つかどうかが確認されます。これは、プログラムで指定された項目値と、ユーザマスタレコードの権限の値とを比較することによって行われます。 プロファイルジェネレータの権限行の色は黄色になります。

6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

>前ページの図の用語説明（4／4）

用語	備考
権限オブジェクト	権限オブジェクトは、AND で結合された項目を 10 個までグループ化します。 権限オブジェクトにより、権限の複雑なテストを複数の条件に対して行うことができます。ユーザがシステム内で実行するアクションは、権限にもとづいて許可されます。権限チェックを正常に実行するためには、権限オブジェクトの全項目値をユーザマスタで適切に更新する必要があります。 権限オブジェクトは、クラスに分類されます。オブジェクトクラスは権限オブジェクトの論理的な組合せで、たとえばアプリケーション (財務会計、人事管理など) に対応します。プロファイルジェネレータの権限オブジェクトクラスの行の色はオレンジ色になります。 権限値の更新に関する情報については、権限オブジェクトをダブルクリックしてください。 プロファイルジェネレータの権限オブジェクトの行の色は緑色になります。
権限項目	権限項目には、ユーザが定義した値が含まれます。権限項目は ABAP ディクショナリで保存されたデータエレメントに接続されています。

6. SAPシステムでの権限設計

6.3　SAP権限　コンセプト

・オブジェクト (権限、プロファイル、ユーザマスタレコード、ロールなど) は、クライアントごとに割り当てられます。 これらのオブジェクトのあるクライアントから別のクライアントへの反映は移送により行います。

・ユーザ独自のトランザクションやプログラムを開発する場合は、開発に関する権限を自身で追加する必要があります 。

権限方針を正常に導入するには、信頼できる権限プランが必要です。プランを作成するには、最初に SAP のどのユーザがどのタスクを実行できるかを決定する必要があります。次に、SAP システムでこれらのタスクに必要な権限を各ユーザに割り当てる必要があります。

堅実で信頼性のある権限プランによる作業は恒常的なプロセスです。権限プランが常にユーザの要件に一致するように、定期的にプランを改訂することをお奨めします。ロール、プロファイル、権限の登録と割当のための標準ロールと手順を定義してください。

6. SAPシステムでの権限設計

6.4　権限設計方針 (1/2)

- **SAPシステムにおける権限の設定は複雑なので、「企業」の役割をあまり細かく分割しないようにします。**

  ⇒例えば、「会計担当・販売担当・調達担当のそれぞれに対してスーパーユーザと一般ユーザを設定する」などに留めます。

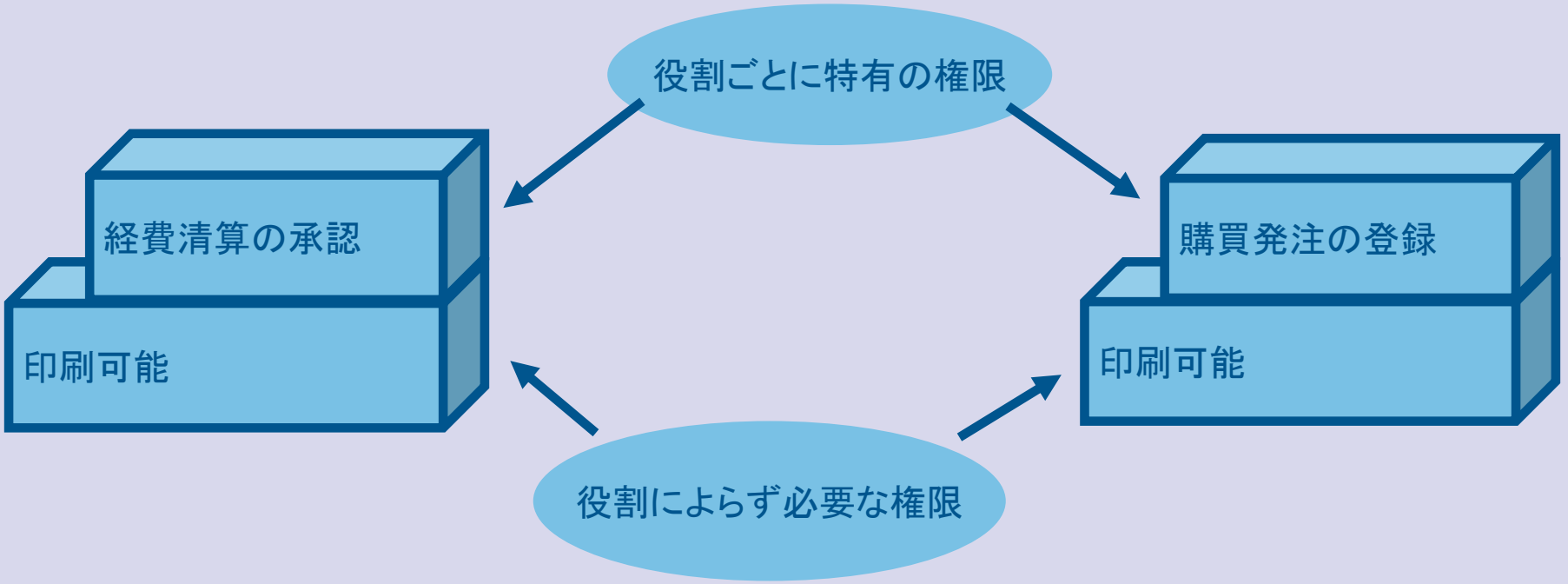
スーパーユーザだから、
他部門データにもアクセス可能

一般ユーザだから、
自部門データにだけアクセス可能

6. SAPシステムでの権限設計

6.4　権限設計方針（2/2）

- **企業における役割に固有の処理と、すべての役割に共通の処理とを整理します。**
  - 例えば、「経費清算の承認は会計担当のみ、購買発注の登録は調達担当のみだが、SAPシステムからの印刷は両方の役割で実行できる。」など。



7. 権限の設定

7.1 SAPシステムでの権限チェックのメカニズム

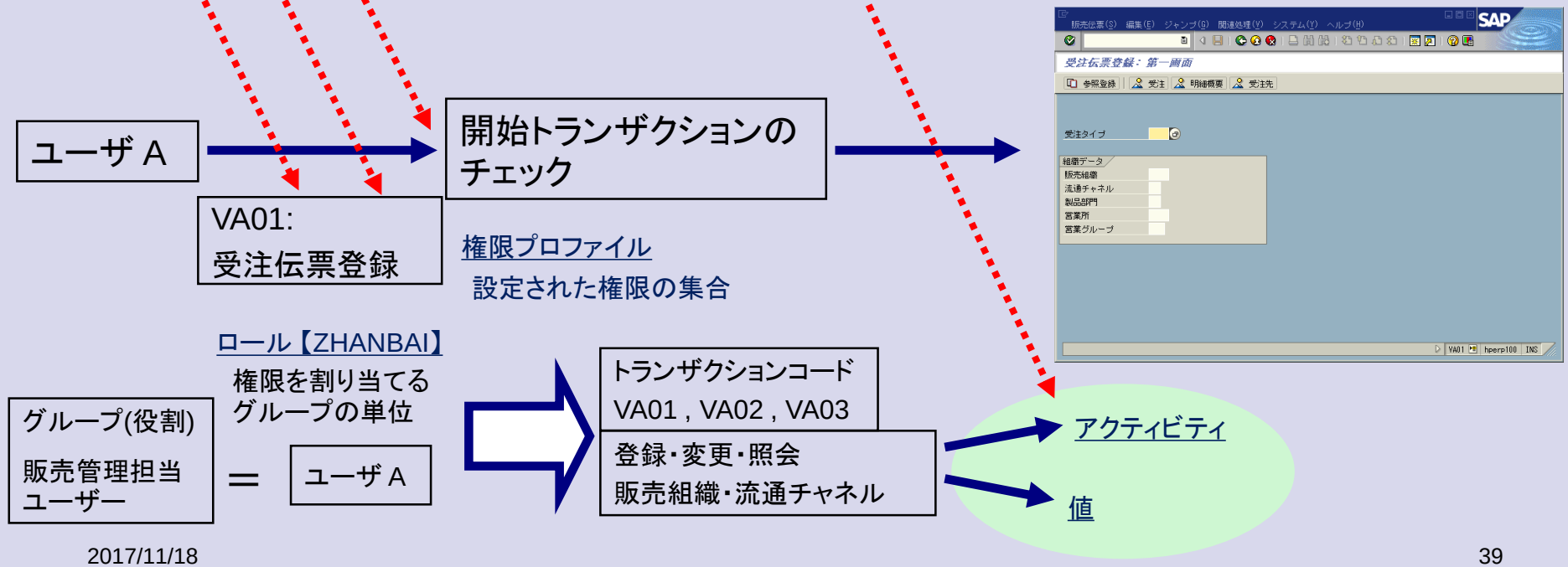
SAPシステム上でトランザクションが開始される際には、以下のようにSAPシステム側で権限をチェックします。

① トランザクションコードは有効であるか？　(テーブル：TSTC のチェック)

② トランザクションがシステム管理者によってロックされているか？　(テーブル：TSTC のチェック)

③ ユーザはトランザクションを開始する権限を持っているか？　(権限オブジェクト：S_TCODE)

④ ユーザは割り当てられた権限オブジェクトの権限を持っているか？

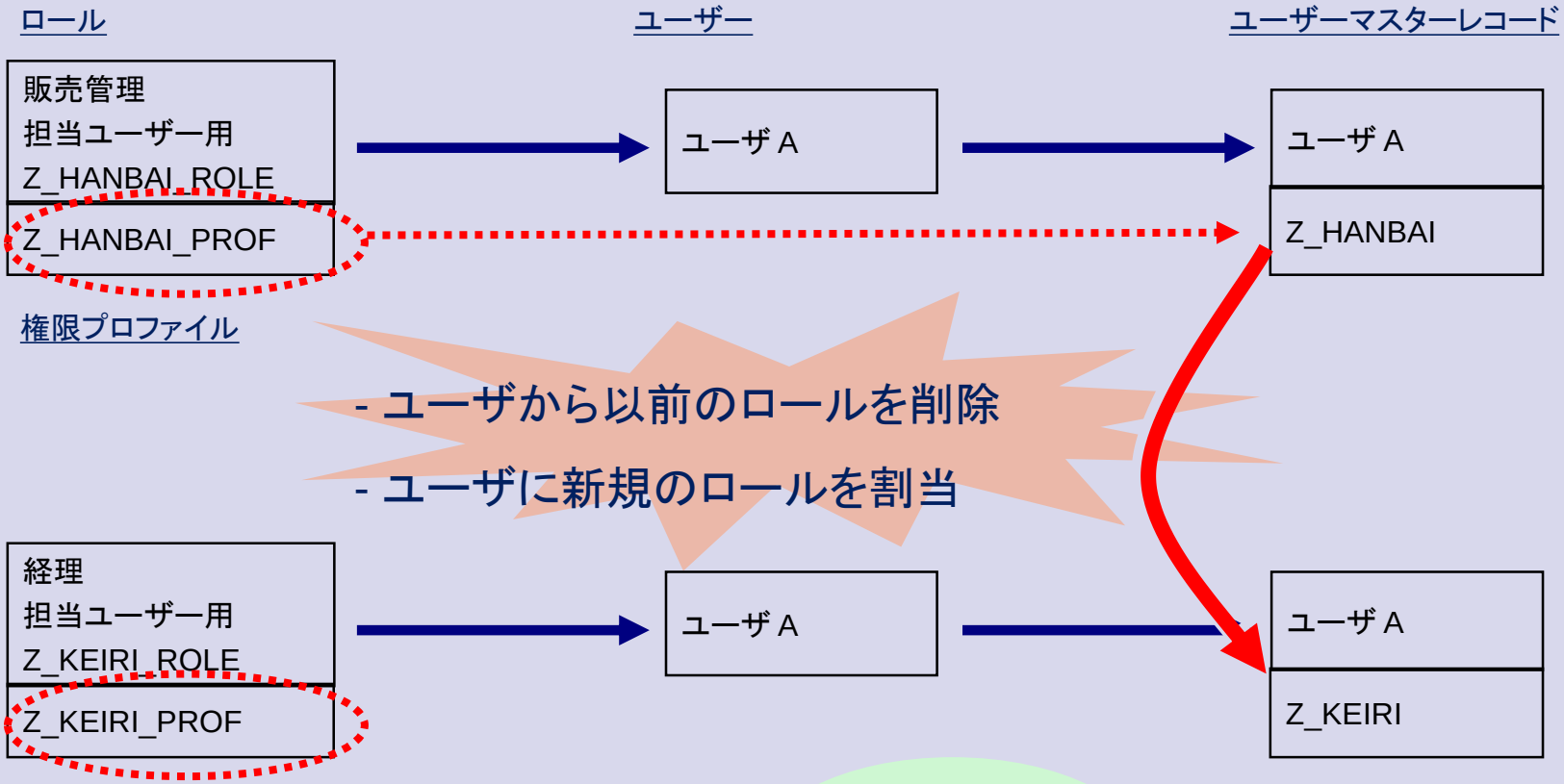


7. 権限の設定

7.2 SAPシステムの権限コンセプト

ロールと権限プロファイル、ユーザマスターレコードの関係

例えば販売担当から経理担当に役割が変わるといった場合でも、ユーザに割り当てるロールを変更するだけで対応が可能です。



7. 権限の設定

7.3 プロファイルジェネレータ (1/2)

権限プロファイルを
マニュアルで作成する場合・・・

全SAPシステムの権限コンポーネントを詳細に理解する必要があります。

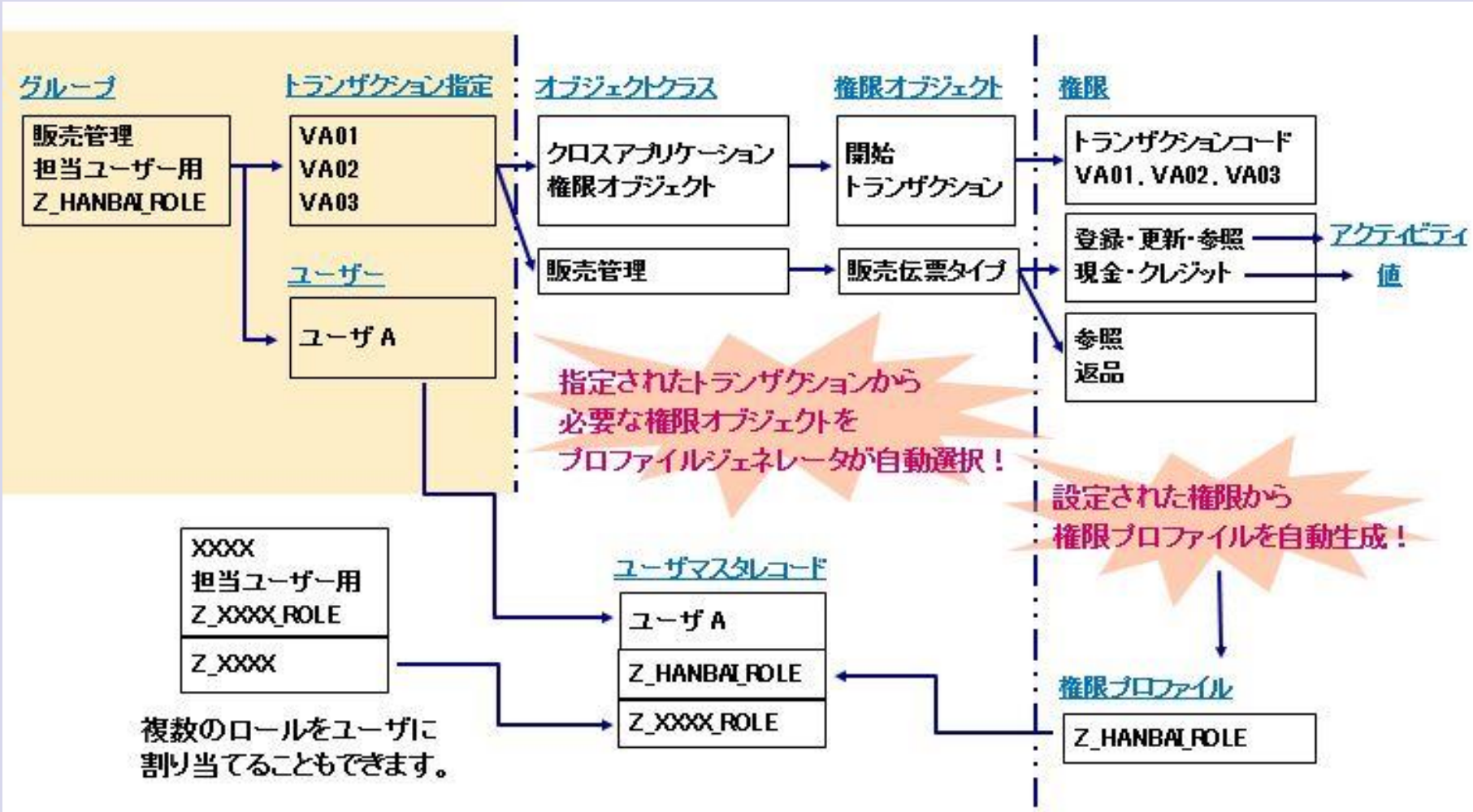
非常に困難です。

プロファイルジェネレータ

- 全SAPシステムの権限コンポーネントを詳細に理解する必要はありません！
- 必要なトランザクションやレポートを選択し、アクティビティを指定すれば、プロファイルを自動で生成できます！

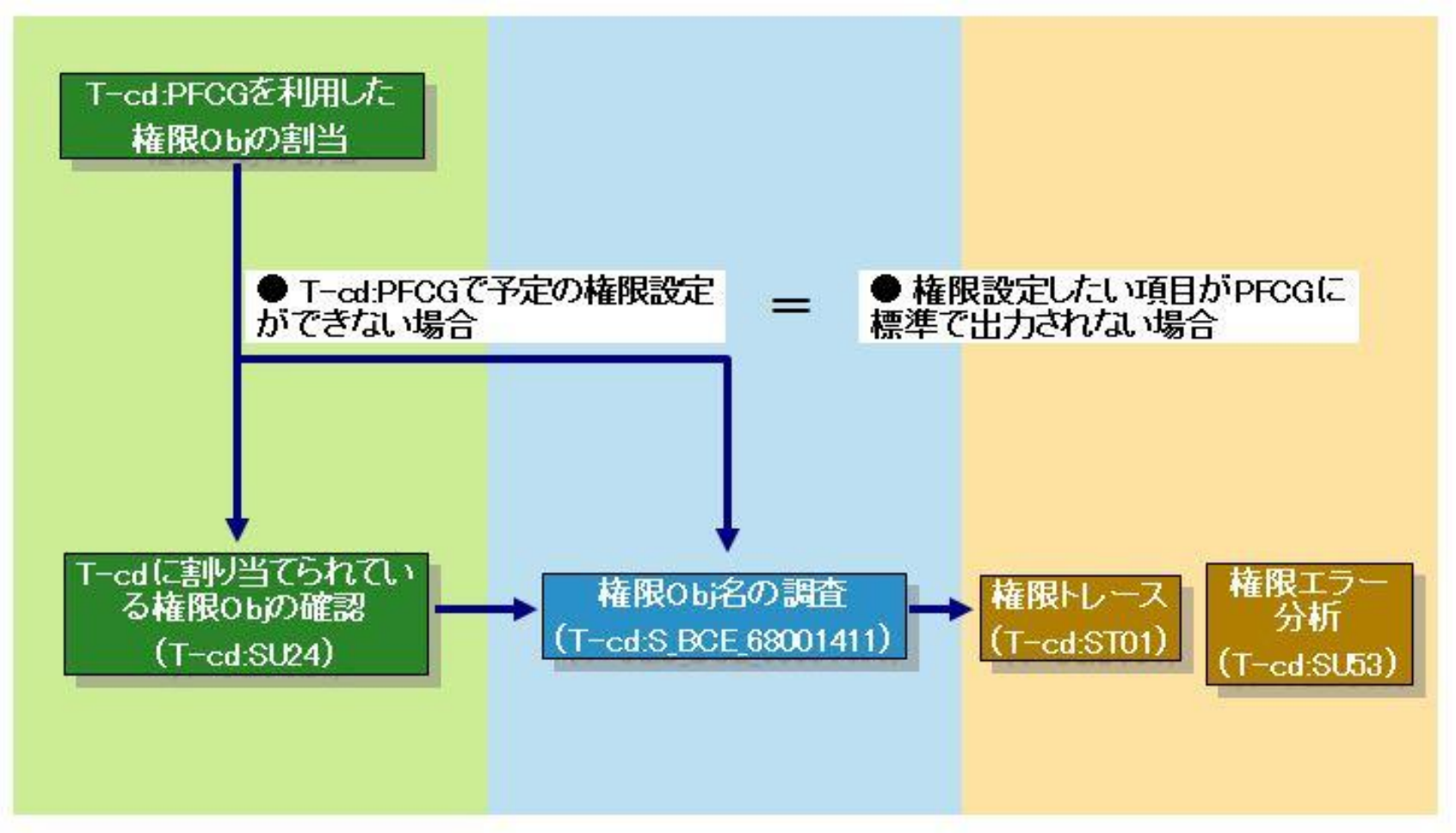
7. 権限の設定

7.3 プロファイルジェネレータ (2/2)



7. 権限の設定

7.4 権限設定フロー

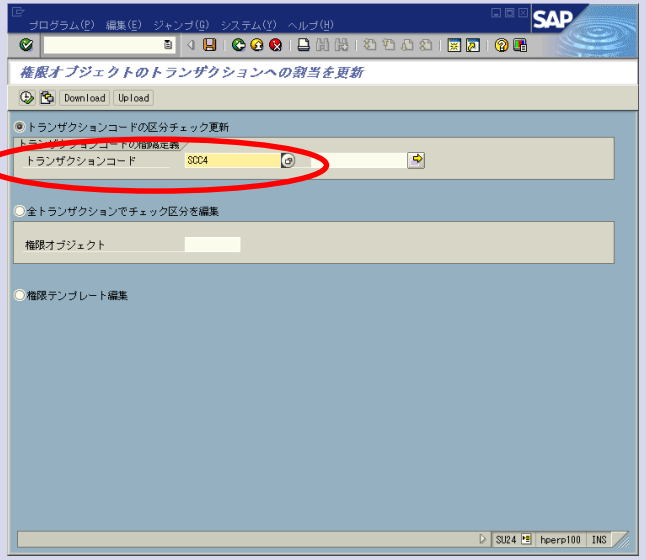


7. 権限の設定

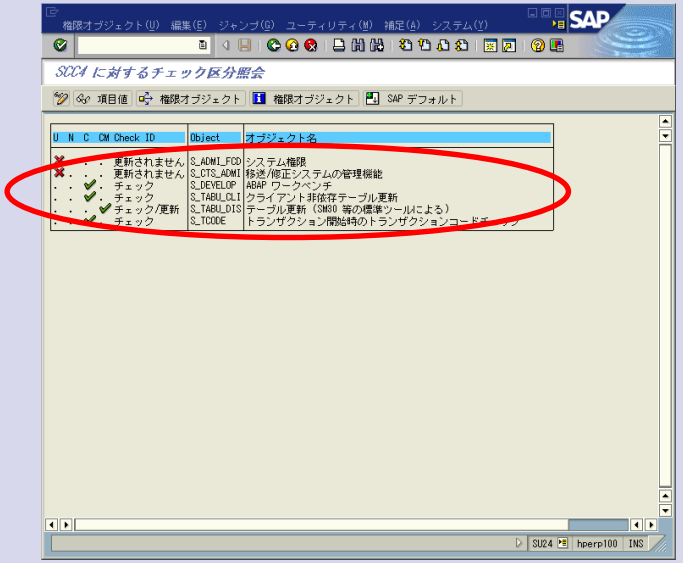
7.5 権限設定関連ツール (1/4)

■ **T-cd : SU24　(参照のみ)**

(1) T-cd に割り当てられている権限オブジェクトの照会



(2) 「チェック/更新」と記載されている項目が権限チェック対象

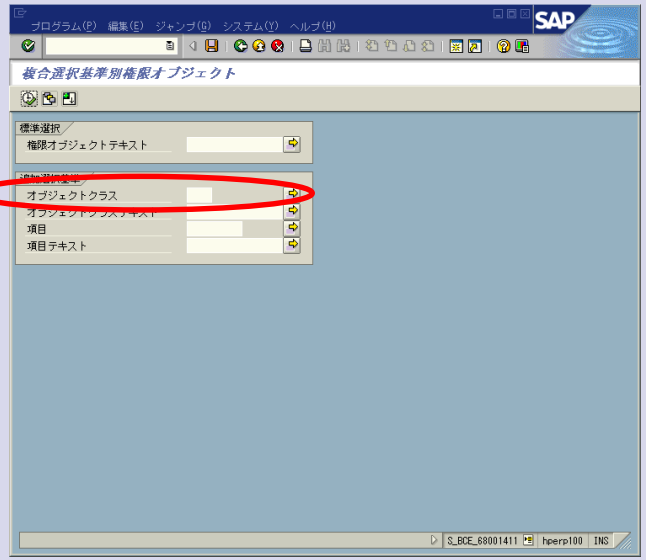


7. 権限の設定

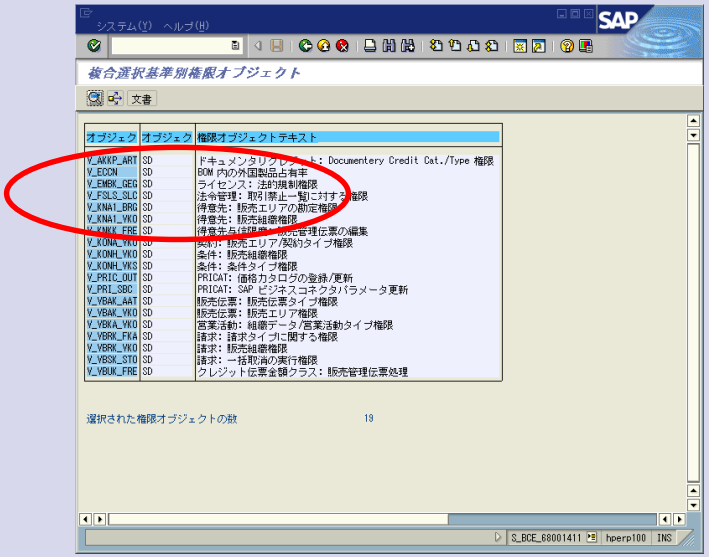
7.5 権限設定関連ツール (2/4)

■ T-cd : S_BCE_68001411

(1) オブジェクトクラス(例：SD)で利用できる権限オブジェクトを照会



(2) SDで利用できる権限オブジェクトの一覧を表示

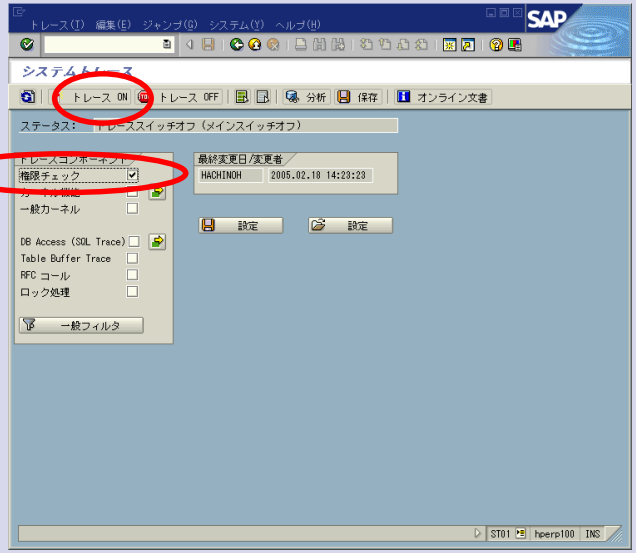


7. 権限の設定

7.5 権限設定関連ツール (3/4)

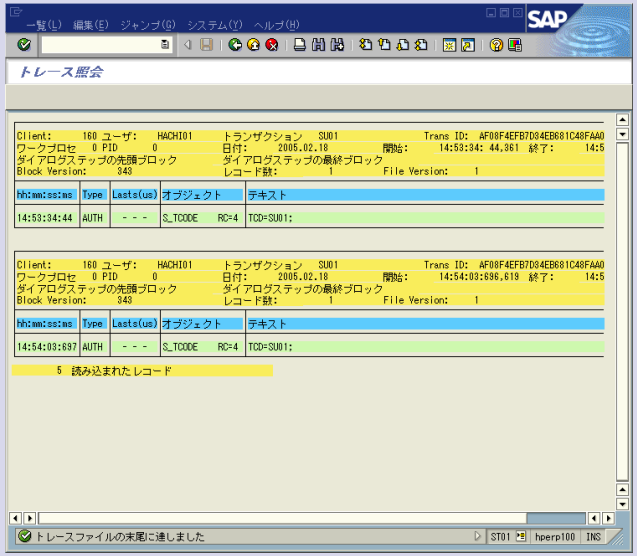
■ T-cd : ST01

(1) 「権限チェック」にチェックを入れ、「トレースON」を押す。



(2) テストユーザで、トランザクションを実行

(3) トレース結果を参照、チェックされた権限項目、結果などがわかる。

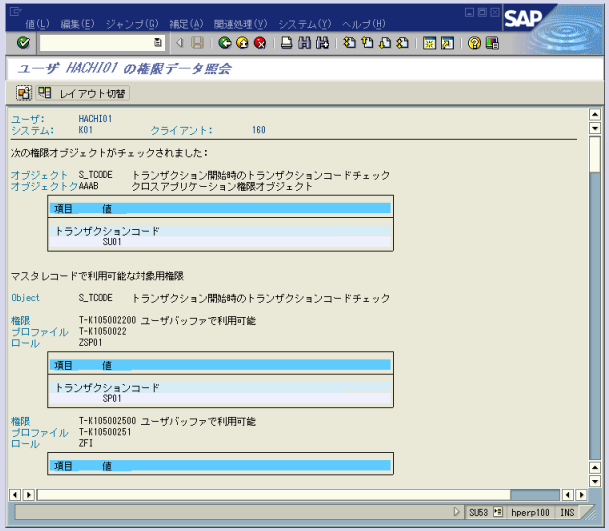


7. 権限の設定

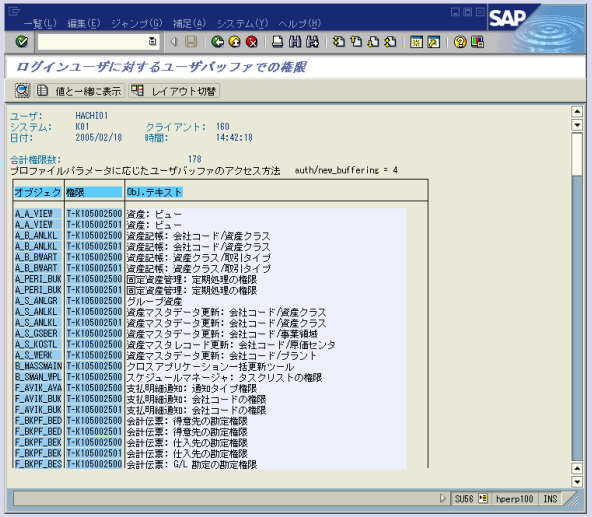
7.5 権限設定関連ツール (4/4)

■ T-cd : SU53　もしくは [メニュー]→[ユーティリティ]→[権限チェック表示]

#1　設定した権限の下でトランザクションを実行し、エラーが発生した直後にT-cd : SU53を実行することで、エラーが生じた権限オブジェクトを確認できる。



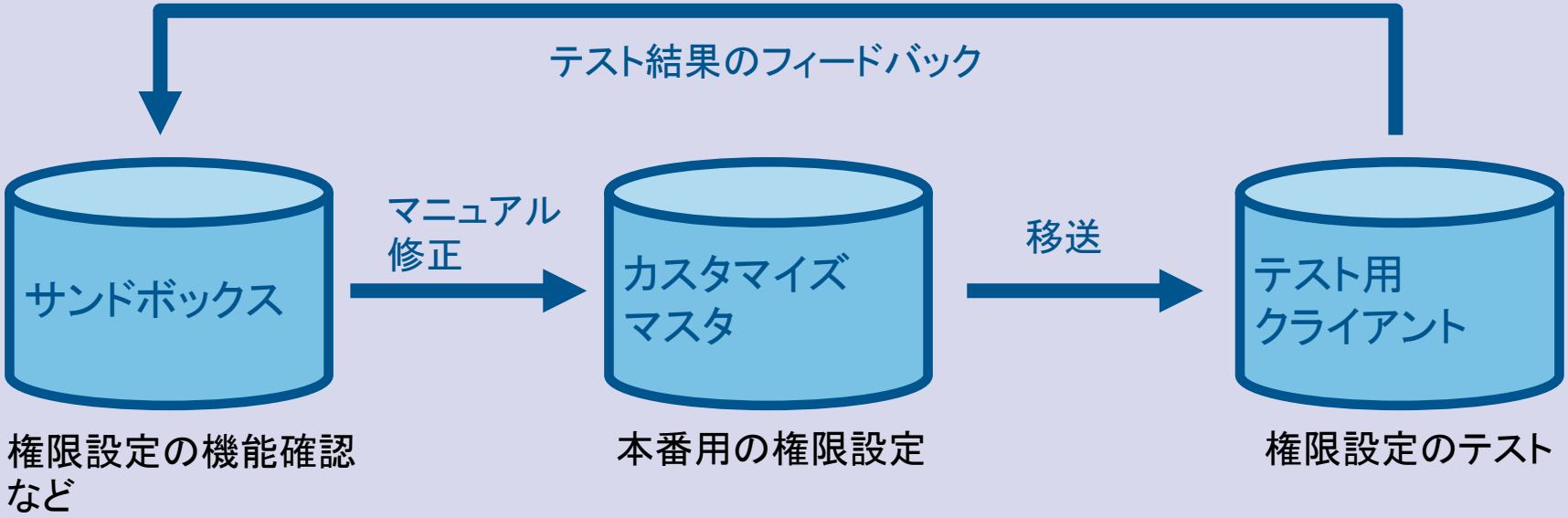
#2　T-cd : SU56 を使用すると、現在のユーザに割り当てられている権限オブジェクトが表示される。



※※ SU53 , SU56 を実行できるように、テストユーザにあらかじめ権限を割り当てておく必要がある。

8. 権限テスト環境

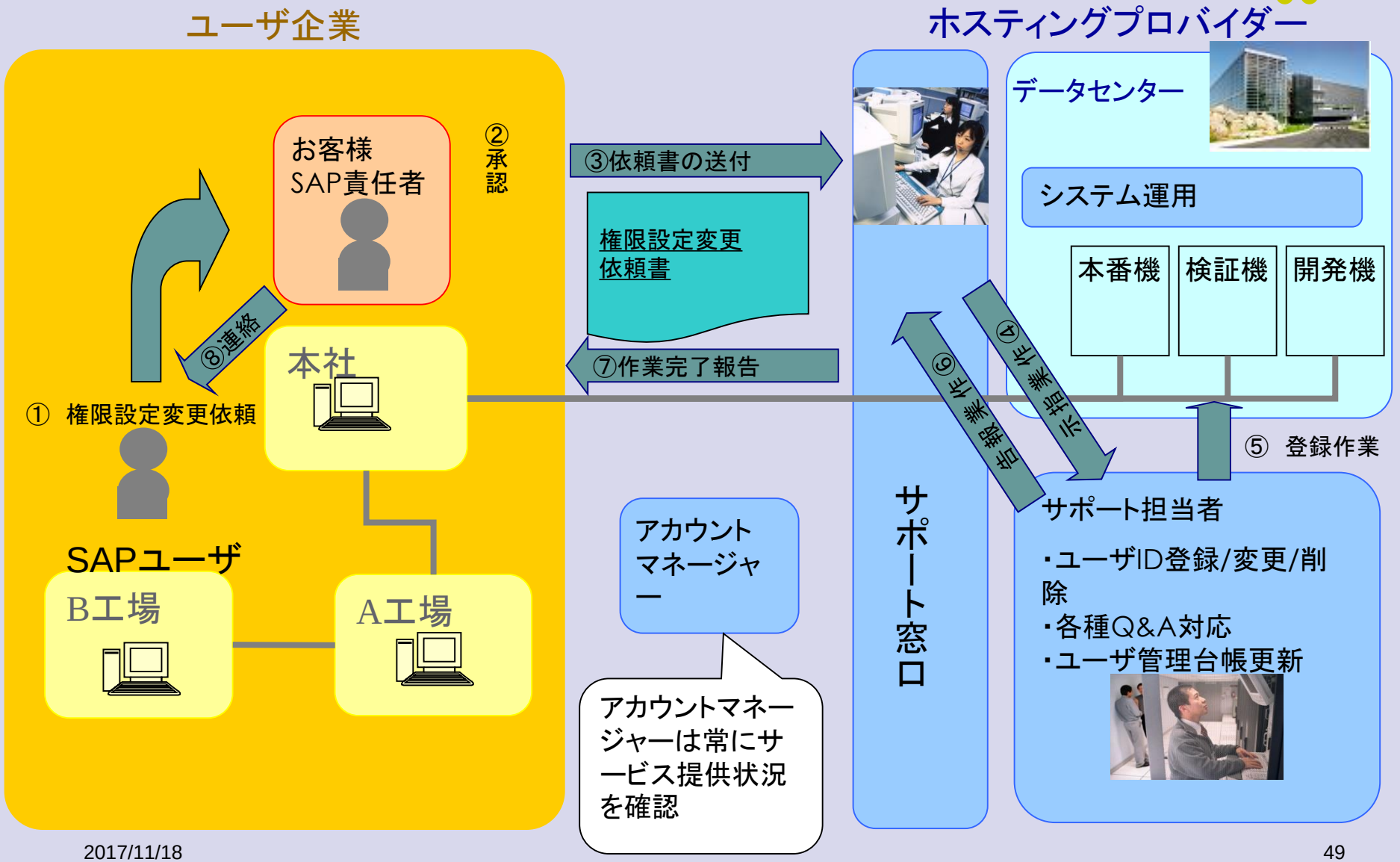
権限設定テスト環境概要



【注意】
権限設定は移送しただけでは有効になりません。
権限設定を移送した後、そのクライアント上のユーザに割り当てなければなりません。

9. 権限設定　モデル運用フロー

ホスティングプロバイダーでのモデル運用フロー図



10. ユーザマスタレコード比較

10.1 ユーザマスタレコードの機能

ユーザマスタレコードにより利用者は SAP システムにログオンすることができ、ロールに指定された権限プロファイルの制限内で SAP システムの機能とオブジェクトにアクセスすることができます。

ユーザマスタレコードには、対応するユーザに関する権限を含むすべての情報が含まれます。

ユーザ属性や権限ロールの変更は、利用者が次回システムにログオンするまで有効になりません。

これらの変更中にログオンしていた利用者は、ログオフしない限りその影響を受けません。

このため、ユーザ属性や権限ロールの変更を即有効とするためには、**ユーザマスタレコード比較**を行う必要があります。

10.2 比較方法

ユーザマスタレコード比較には、次の 3 つのタイプの比較があります。

（1）プロファイル比較

時間依存ロール割当のプロファイルが更新されます。

ユーザマスタレコード内に、権限プロファイルの期限やそのエントリを設定することはできません。

（2）集合ロールエリア

集合ロールに定義されたロール割当が更新されます。すなわち、追加または削除されます。

（3）HR 比較

HR-ORG モデルの間接ロール割当から直接ロール割当が生成されます。

この他、クリーンアップオプションによって、無効な生成済プロファイルや無効なロール割当を削除することもできます。

10. ユーザマスタレコード比較

10.3 手順

（１）トランザクション PFUD によるマニュアルでの比較

・次のいずれかのアクションを選択、実行します。

① **プロファイル比較**

・プロファイルの生成またはインポート後、すぐにプロファイル比較を開始します。

時間依存ロール割当を使用している場合は、この比較をバックグラウンドジョブとして毎日スケジュールすることをお奨めします。

これにより、権限プロファイルがユーザマスタレコードと比較されます。

すなわち、最新ではなくなったプロファイルはユーザマスタレコードから削除され、最新のプロファイルがユーザマスタレコードに入力されます。

② **集合ロール比較**:

・集合ロール定義を変更した (すなわち、集合ロールの単一ロールを追加または削除した) 場合、または変更をインポートする場合に集合ロール比較を開始します。単一ロール割当がユーザの集合ロール割当と比較されます。単一ロールを集合ロールに追加すると、単一ロールが集合ロールに割り当てられたユーザに割り当てられます。反対に、ユーザの単一ロール割当が削除されるとその単一ロールは集合ロールから削除されます。

③ **HR 比較**

・ 間接ロール割当に影響するローカルの HR-ORG モデルを変更するか、または変更をシステムに移送する場合にHR 比較を開始します。

HR-ORG が有効な場合にのみ、すなわち、テーブルPRGN_CUST のスイッチ HR_ORG_ACTIVE が **YES** に設定されている場合にのみ、この処理タイプを選択することができます。

10. ユーザマスタレコード比較

10.3 手順

④　**クリーンアップ**:

・プロファイルの生成またはインポートを行う際にクリーンアップを実行します。
存在しなくなった生成済プロファイルが削除されます。
　ロールとプロファイルを頻繁に移送する場合は、これによって可能性のある不整合を迅速に解決することができるため、定期的なクリーンアップが特に重要です。

（２）完全比較のジョブのスケジュールまたはチェック

・ジョブの実行時間を指定することで、レポート PFCG_TIME_DEPENDENCY を開始することができます。一覧にはすでにスケジュールされたバックグラウンドジョブのステータスが表示されます。

①　レポート **PFCG_TIME_DEPENDENCY** を毎日始業前に、全体の比較としてスケジュールします。
　このレポートがエラーなしに実行される場合はユーザマスタレコードの権限プロファイルは毎朝最新のものになります。

②　このアクションを選択すると先に記した処理タイプでの選択に関係なく4 つのタイプ　－　プロファイル比較、集合ロール比較、HR 比較、クリーンアップ　－のプロセスが必ず含まれます。
　特定の比較の処理タイプだけをバックグラウンドプログラムとして実行(実行時動作の改善のためなど)することもできます。

参考:SAP_ALL と SAP_NEW の違い

・ユーザに割り当てる権限プロファイルでよく登場してくる SAP_ALL と SAP_NEW ですが、この2つの違いが分かりますか。
　プロジェクトでは、開発メンバーにはとりあえず SAP_ALL と SAP_NEW の両方の権限プロファイルを割り当てているケースが多いのではないかと思います。
（ちなみに、SAP_ALL と SAP_NEW の両方を割り当てる必要はありません）

　プロジェクトによっては開発メンバーに全権限を付与せずに個別ロールを作成して、必要以上に権限を付与しないようにしているところもあります。

・**SAP_ALL** はその名の通り、SAP ABAPシステムの全トランザクション、全機能を実行できる権限を持っています。**SAP_NEW の権限も含んでいます**。
・**SAP_NEW** は以前のリリースから存在しているトランザクション（プログラム）の中で、アップグレード時に追加された権限チェックの権限を持っています。

・例えば、R/3 4.6C の時は SU01 でユーザ登録をするために必要な権限は A と B だったのに、ERP 6.0 では、権限 A, B, C が必要になったとします。
　SAP_ALL の権限プロファイルが割り当てられているユーザであれば、問題なくユーザ登録を実行できますが、権限A,B のみを含むロールしか割り当てられていないユーザはERP 6.0 にアップグレードした途端にユーザ登録できなくなってしまうのです。

　上記例のように、**既存プログラム内に追加された権限チェックを満たすための権限プロファイル**がSAP_NEWです。ちなみに、新しいリリースで追加された機能、トランザクション（プログラム）の権限は SAP_NEWには含まれていませんのでご注意を。あくまで既存プログラム内の追加権限チェックに対する権限を持っているのです。

Copyright 2017 Skytech co. ,ltd. All rights reserved