

SAP ERP IT 全般統制チェックリスト 概要解説書

システム監査学会
会計システム専門監査人部会

2008 年度研究結果

2009 年 12 月

目次

1	「SAP ERP IT 全般統制監査 チェックリスト」について	1
1.1	「SAP ERP IT 全般統制監査 チェックリスト」作成の背景	1
1.2	「SAP ERP IT 全般統制監査 チェックリスト」の策定目的及び全体像	1
1.3	本解説書について	1
1.4	研究グループについて	2
2	IT 全般統制視点から見た SAP ERP の特徴 と 主要統制機能	3
2.1	SAP ERP 全般統制を支援する「Web アプリケーションサーバ」	3
2.2	SAP ERP の内部統制機能	4
2.3	SAP ERP の統制および監査の考え方	4
2.4	システムランドスケープ	5
2.4.1	「3 システムランドスケープ」の構成	5
2.4.2	「クライアント」：アプリケーション関連データの管理単位	6
2.4.3	変更属性の設定	7
2.5	クリティカルトランザクションのロック	8
2.6	アクセスコントロール機能	8
2.6.1	識別、認証、許可	8
2.6.2	特権ユーザ	9
2.7	開発／保守コントロール機能	10
2.8	セキュリティ監査ログ機能	11
2.9	監査情報システム (AIS)	13
2.10	プロファイルパラメータ	14
3	チェックリストの特徴と形式	19
3.1	チェックリストの形式	19
3.2	チェックリストの特徴	19
4	SAP ERP IT 全般統制監査の方法	21
4.1	本運用環境の監査手順	22
4.2	開発／保守の監査手順	23
4.3	アクセスコントロールの監査手順	27
4.4	運用の監査手順	31
5	用語集	34
6	チェックリスト	60
6.1	本運用環境	60
6.2	開発環境	60
6.3	アクセスコントロール	60
6.4	運用統制	60

1. 「SAP ERP IT 全般統制監査 チェックリスト」について

1.1 「SAP ERP IT 全般統制監査 チェックリスト」作成の背景

会計システム専門監査人 B グループでは、2007 年度から、ERP における統制機能を監査人として利用する立場からの研究として、SAP ERP システムに実装されている全般統制機能について研究を行って来ている。(SAP ERP 以外の ERP パッケージについては、今後の対象として考えている)。

2007 年度には、別添資料の様に、SAP ERP の全般統制機能と経済産業省発行の「システム管理基準 追補版 (財務報告に係る IT 統制ガイダンス) 平成 19 年 3 月 30 日」を比較検討し、システム管理基準追補版に示されている IT 全般統制と SAP ERP の統制機能の対比表を作成した。この対比表(名称としては「システム管理基準追補版と SAP ERP の対比」)により、SAP ERP 統制機能でカバーされている IT 統制項目について概観する事が可能になり、監査人による被監査企業の統制整備の確認の為の参考材料として使用できると考えられる。

その後、上記比較表は、それを元に監査人が SAP ERP での IT 統制監査を検討する際の参考にはなり得るが、現実にはそのものを使用しての監査はそれだけでは難しいという判断から、2008 年度では、その次の段階として監査人が実際に利用できる監査ツールとして、SAP ERP (ECC 6.0) システムに特化した「SAP ERP IT 全般統制監査 チェックリスト」を作成する事になった。作業の結果として、本解説書で解説する成果物が完成した。

1.2 「SAP ERP IT 全般統制監査 チェックリスト」の策定目的及び全体像

「SAP ERP IT 全般統制監査 チェックリスト」の策定の目的としては、上記の背景を基に、監査人が、SAP ERP システムの ITGC 監査を行う際に標準監査ツールとして使用し、整備状況及び運用状況の確認を容易に判断出来る様にする事である。

これは、SAP ERP で実装されている統制機能を前提に考えた場合、統制項目の抽出は多くの場合標準的な考え方に基づいた策定が可能であり、また備えられている監査ツールの利用を前提にした監査を行う事により、迅速かつ正確な監査を行うことが可能となると考えられる事から標準的なチェックリストが策定可能であるという議論の結果に基づいている。

この様なチェックリストは、汎用性を持たせる為に、個々の被監査企業の事情に応じて、ある程度の柔軟性も必要である。本チェックリストでは、基本的な必須統制項目と、被監査企業におけるリスク解析により、優先度として必須項目より低く考えられるものとを分類を行っている。従って、監査人が取捨選択してチェックを行うことが可能となっている。

「SAP ERP IT 全般統制監査 チェックリスト」を利用する場合の注意点としては、本チェックリストが求められている IT 全般統制項目全てをカバーしている分では無いという事を理解頂きたい。それは、ERP 上に組み込まれた統制機能により、全ての統制が行えるわけではないという点からも明白である。従って、このチェックリストにおいてカバーされていない部分に関しては、上記で示した 2007 年度成果物である「システム管理基準追補版と SAP ERP の対比」などを参考に、別途監査人が被監査企業の統制に関して個別に対応する事を想定している。

1.3 本解説書について

本解説書の内容の記述レベルは、前提として、IT、アプリケーションシステム、監査論などに見識

を所有している監査人を対象とし、また、SAP ERP に特化した内容である為、ある程度 SAP ERP の統制機能について知識を有している事が必要となっている。しかしながら、SAP ERP に関しての全体にわたっての深い見識が必要という事までは想定していない。

本解説書の目的およびスコープとしては、SAP ERP システムの ITGC 監査を行う際の参考ツールとして、「SAP ERP IT 全般統制監査 チェックリスト」が監査人により容易に活用できる様に内容及び利用方法の解説をすることである。従って、上記の策定目的・全体像において示した様に、チェックリストでカバーされている統制項目の範囲が解説の対象範囲、スコープとなっている。

1.4 研究グループについて

システム監査学会 会計システム専門監査人部会において、「SAP ERP IT 全般統制監査 チェックリスト」及び本解説書の作成に携わったメンバーは次の通りである。(順不同)

植野 俊雄	ISU 代表
切山 裕明	本田技研工業 (株)
日下部 公	NEC ネクサソリューションズ (株) コンサルティング部
黒田 康博	黒田 ITC 事務所 代表
後藤 知久	合同会社兵法マネジメント塾 代表社員
志村 政一	アビームコンサルティング (株) ディレクター
平塚 康哲	(株) ヒラツカコンサルティング エグゼクティブ・コンサルタント

及び、アドバイザーとして

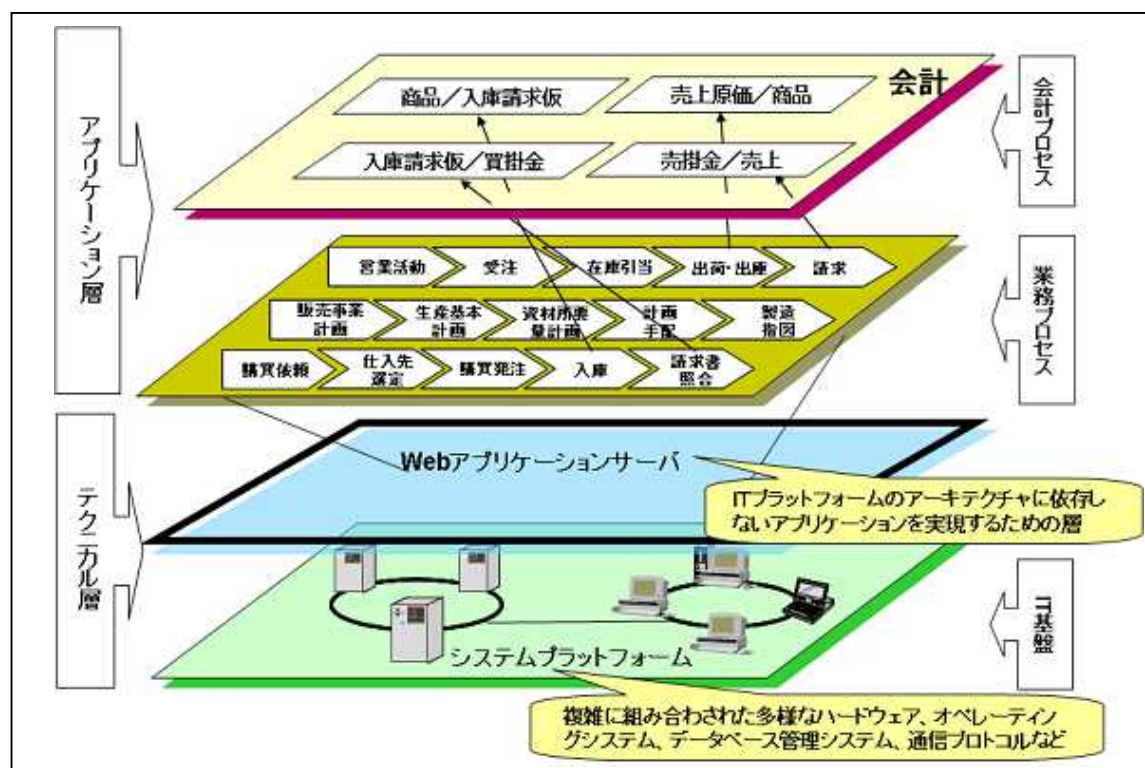
清水 恵子	新日本監査法人 IT ソリューション室長
-------	----------------------

2. IT 全般統制視点から見た SAP ERP の特徴 と 主要統制機能

2.1 SAP ERP 全般統制を支援する「Web アプリケーションサーバ」

SAP ERP システムは 「Web アプリケーションサーバ」(古いリリースでは「ベースス」と呼ばれる SAP 固有のミドルウェア) 上で動作している。(図表 2.1-1)

図表 2.1-1 SAP ERP の構造



「Web アプリケーションサーバ」の役割は、テクノロジーの変化に迅速に対応可能にすることである。SAP ERP が様々な OS や DBMS 上で動作できるように「Web アプリケーションサーバ」がオペレーティングシステム（以後、OS と記載）やデータベース管理システム（以後、DBMS と記載）の差異を吸収する。これにより SAP ERP 導入企業は、採用する OS や DBMS を様々な条件を勘案し、独自の判断で選択することができる。OS を例にとると、SAP ERP は Windows、UNIX、リナックスなどに対応している。

各 OS や DBMS はそれぞれ固有の API (Application Program Interface)、アクセスコントロール機能、開発支援機能、運用支援機能を実装しており、夫々に独自性がある。しかし、これは SAP 社、および ERP ユーザ双方にとって不都合である。SAP 社にとっては、SAP ERP を複数の OS や DBMS の固有インタフェースに合わせて ERP を開発／保守し続けるのは非現実的である。また、ユーザにとっても使用している OS や DBMS が異なると、操作性が異なってしまうのは不都合である。

そこで、SAP 社はアプリケーション層と IT プラットフォーム層 (OS、DBMS 層) の間に、OS/DBMS 等の差異を吸収する「SAP 独自のミドルウェア層」を置き、これを「Web アプリケーションサーバ」と呼んでいる。長い間「ベースス」という名称で呼ばれていたが、サービスオリエンテッド基盤への移

行に伴い大幅な機能拡張が行われ、同時に名称も変更された。

内部統制の観点からは、Web アプリケーションサーバに組み込まれている、高度な統制機能および監査支援機能を理解する必要がある。

2.2 SAP ERP の内部統制機能

SAP ERP の動作基盤となっている「Web アプリケーションサーバ」は次のような統制機能および監査支援機能を提供している。

① 全般統制機能

- 3 システムランドスケープ（「ISO27001 A10.1.4 開発施設、試験施設及び運用施設の分離」を実現するために実装された機能）
- 移送および移送承認機能
- クリティカルトランザクションのロック機能（開発環境では有用な機能だが運用環境で実行されてはならない機能）を本稼動システム上でロックする機能（＝使えなくする）
- アクセスコントロール機能
- 開発／保守コントロール機能
- 運用支援機能
- 監査証跡記録機能
-

② 業務処理統制機能

- コンピュータファイルマッチング機能
- スリーウェイマッチング機能
- アクセスコントロール機能
- 会計期間のオープンクローズ
- 監査証跡ロギング機能
-

③ 監査支援機能

- 監査情報システム（Audit Information System）
- システム監査ログ機能

2.3 SAP ERP の統制および監査の考え方

図表 2.3-1 は、SAP システムに備えられた統制機能および監査機能を活かした SAP ERP システムの統制概念図表である。

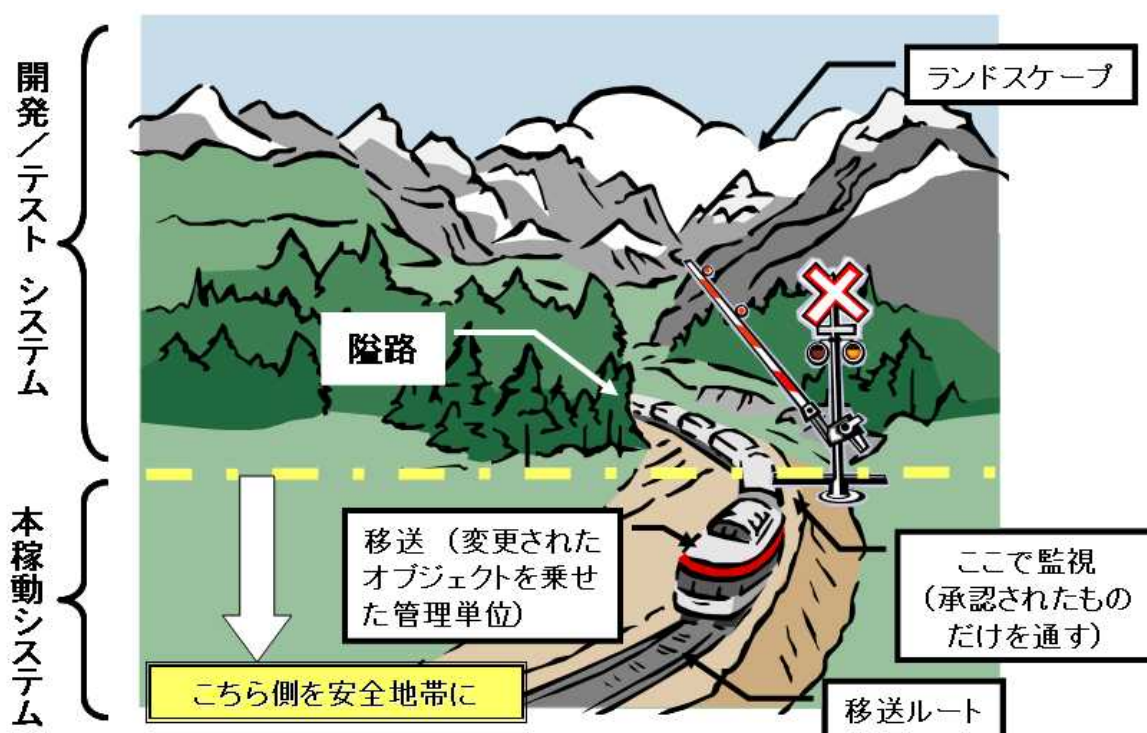
意図するところは、先に述べた SAP システムの統制機能を使い 「できる限り自動的な統制を実現し、残るリスクだけを監査機能を使ってモニタリングする」と言う考え方である。これは、孫子の兵法「隘路の計」の適用と言うことができる。これを簡単に説明すると次のようになる。

- ① 「移送」以外の方法で本稼動システムのプログラムおよびカスタマイズパラメータを変更できないようにコントロールする。これは、後述する 3 システムランドスケープと移送承認機能を適切に設定することによって実現する。
- ② クリティカルトランザクションの実行を本稼動システム上で禁止（ロック）する。
- ③ SAP ERP 上で OS コマンドを実行できる機能（外部 OS コマンド）の利用をコントロールする。
- ④ セキュリティポリシーに沿って、プロファイルパラメータ（後述）を設定する。

- ⑤ 上記①～④の対策ではカバーできない脅威（特権者による悪意ある行為）、および、①～④のコントロールそのものに対する脅威（例えば、特権者がクリティカルトランザクションのロックを解除する）をモニタリングする。モニタリングは、セキュリティ監査ログ や AIS (Audit Information System) を使って行うことができる。

このような方針に基づいて統制を行わないと、ERP システムを導入しているにもかかわらず、手組みシステムと同様に、一般的に考え得る全てのリスクへの対応を考える必要が生じてしまう。同様に、監査においても一般的に考え得る全てのリスクを監査することが必要となる。たとえば、「全てのテーブルに対する、全ての変更ログを残しておく」と言う方針を立ててしまうことである。これは、SAP ERP が持つ統制機能を適切に設定したならば起き得ないリスクの発生までを想定しているためである。仮に、全てのテーブルの全ての変更ログを残したとしても、記録されるログのボリュームが膨大となり、それらをモニタリングし続けることは事実上不可能である。また、一つ一つのテーブル変更ログから、アプリケーション上の意味を読み解くのは困難でもある。

図表 2.3-1 SAP ERP の統制機能と監査支援機能を活かす



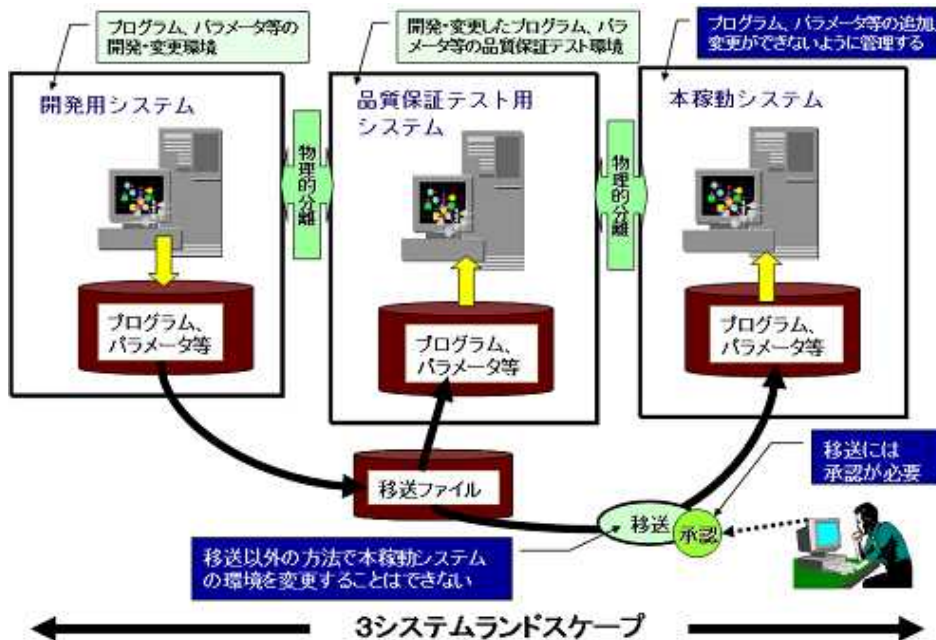
2.4 システムランドスケープ

2.4.1 「3 システムランドスケープ」 の構成

SAP ERP システムにおいては、開発、テスト、運用を行うシステムを物理的に分離（ハードウェアを分離すると言う意味）することが原則となっている。開発、テスト、運用を行うシステムを分離する考えは、もともと「ISO27001 A10.1.4 開発施設、試験施設及び運用施設の分離」で定義されており、SAP システム固有の考え方ではない。この考え方を実装したものが ERP システムの「ランドスケープ」という概念である。

図表 2.4.1-1 に示すように SAP システムでは、「開発」「テスト」「運用」システムを分離した環境を「3 システムランドスケープ」と呼ぶ。

図表 2.4.1-1 3 システムランドスケープ



2.4.2 「クライアント」： アプリケーション関連データの管理単位

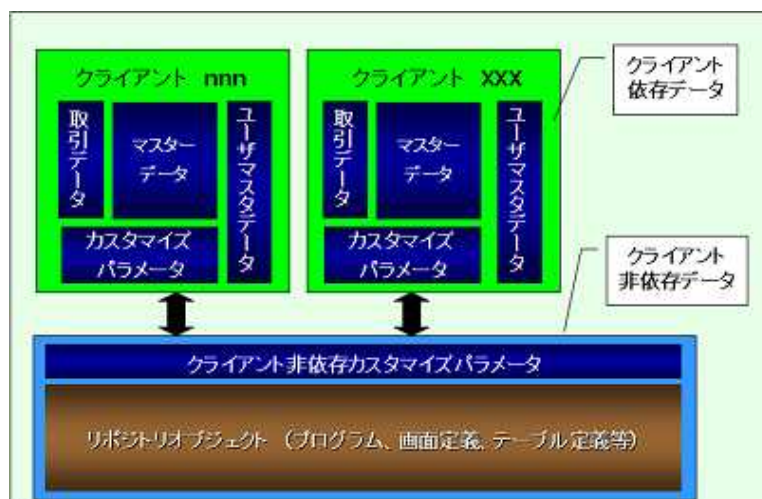
SAP ERP システムには「クライアント」と呼ぶアプリケーションデータの管理単位が存在する。(図表 2.4.2-1 参照)

マスターデータ、トランザクションデータ（取引データ）、カスタマイズパラメータ、ユーザ ID／パスワードなど（これらは「ユーザマスタ」に記録される）は、クライアント単位に固有データを持つことができる。クライアント毎に管理されるデータを「クライアント依存データ」と呼ぶ。

一方、プログラム／画面定義などを「リポジトリオブジェクト」と呼び、これらはシステム単位（開発システム、品質保証システム、本稼動システム）に管理される。このように、システム毎、すなわちどのクライアントにも属さない形で管理されるデータを「クライアント非依存データ」あるいは「システム依存データ」と呼ぶ。

言い方を換えると、クライアント依存データを変更しても、影響を受けるのは該当クライアント内だけであるが、クライアント非依存データを変更すると、全てのクライアントが影響を受ける。監査の実施にあたりこの点を留意しておかなければならない。

図表 2.4.2-1 クライアント依存データと非依存データ



2.4.3 変更属性の設定

SAP ERP システムには、権限管理機能とは別に、プログラムやカスタマイズパラメータの開発／保守を完全に禁止する機能がある。この機能を利用し、本稼動システムおよび品質保証テストシステムは、プログラムやカスタマイズパラメータの変更を全面禁止するように設定することができる。このように設定しておけば、万一全権者（スーパーユーザ）が不正に、あるいは間違っってプログラム等を変更することを防ぐことができる。

開発／保守の禁止／許可は、図表 2.4.3-2 に示す画面で設置する。

この設定はクライアント単位に行うことができ、「禁止」（画面上では「変更なし」）に設定されたクライアント上では、たとえユーザが開発／保守権限を持っていたとしても、開発／保守作業を行うことはできない。

このように、3 システムランドスケープ（クライアント管理を含め）を適切に設定すると、たとえ全権を持っていたとしても開発システム以外でプログラムやカスタマイズパラメータの開発／保守を実施できないように統制することが可能である。

更に、上記環境が変更された場合、「だれが」「いつ」「どのように変更したか」を自動的にロギングするように設定できる。 監査人は、今現在の変更属性の設定を確認するだけでなく、変更ログをチェックし、監査対象期間中の設定変更もチェックすべきである。

（補足） ログを取るためには、後述のプロファイルパラメータで、ログを自動的に記録するように設定する必要がある。

図表 2.4.3-2 クライアント毎に開発／保守作業の可否を定義する画面

ランドスケープのセキュリティを高めるため、適切な属性を設定を行う必要があります

クライアント 800 IDES-ALE Central FI Syst

市区町村 Frankfurt - Deutschland 最終変更者: 日付: 20...

編理システム T90CLNT090

標準通貨 EUR

クライアントロール P 本稼動

クライアント依存オブジェクトの変更と移送

- ☐ 自動記録のない変更
- ☐ 変更の自動記録
- ☒ 変更禁止
- ☐ 自動記録なしの変更、移送が不許可

クライアント非依存オブジェクト変更

3 リポジトリとクライアント非依存 Customizing Obj への変更なし

保護: クライアントコピープログラムと比較ツール

L 保護レベル 2: 上書き不可、外部利用不可

CATT と eCATT の制限

eCATT と CATT - 不可

制限

- ☐ クライアントコピーのためのロック済
- ☐ SAP upgrade に対する保護

クライアント非依存カスタマイジングオブジェクトの変更なし

2 リポジトリオブジェクトの変更なし

3 リポジトリとクライアント非依存 Customizing Obj への変更なし

リポジトリとクライアント非依存カスタマイジングへの変更許可

保護レベル 2: 上書き不可、外部利用不可

X 保護レベル 1: 上書き不可

保護レベル 0: 制限なし

E eCATT を許可し、FUN/ABAP と CATT を許可しない

F eCATT を許可し、FUN/ABAP と CATT を認証済 RFC でのみ許可

T eCATT と CATT を認証済 RFC に対してだけ許可

X eCATT と CATT を許可

eCATT と CATT を許可しない

2.5 クリティカルトランザクションのロック

開発／保守／テスト段階では非常に有用なトランザクション、例えばプログラムの開発／変更／デバッグに係わるトランザクションや、アプリケーションプログラムを介さずテーブル内容を直接追加／変更するトランザクション機能などをロックすることができる。

本稼動システム上でこれらのトランザクション（クリティカルトランザクションと呼ぶ）をロックしておくことにより、本稼動システムの安全性を高めることができる。

また、トランザクションのロック／ロック解除操作を、後述の「セキュリティ監査ログ」によってモニタリングすることが可能である。

2.6 アクセスコントロール機能

2.6.1 識別、認証、許可

SAP ERP のアクセスコントロール機能は、図表 2.6-1 に示すように、次の 3 ステップで実行される。

- ・ 識別 (Identification) : 本人確認
- ・ 認証 (Authentication) : 特定の機能（トランザクション コード）に対する実行権限の確認
- ・ 許可 (Authorization) : 特定のデータに対するアクセス権限の確認

図表 2.6.1-1 を見ながら、アクセスコントロールの手順を説明する。

（識別ステップ）

- ① ログオンユーザが自分に割り当てられている「ユーザ ID」「パスワード」を入力する。
- ② システムは、「ユーザ ID」「パスワード」が「ユーザマスタ」に登録されている内容と突合せを行なう。

- ③ 「ユーザID」「パスワード」が一致する場合、SAP ERP のメニュー画面をユーザ端末に表示する。(SAP ERP ではこの画面を SAP Easy Access と呼んでいる)

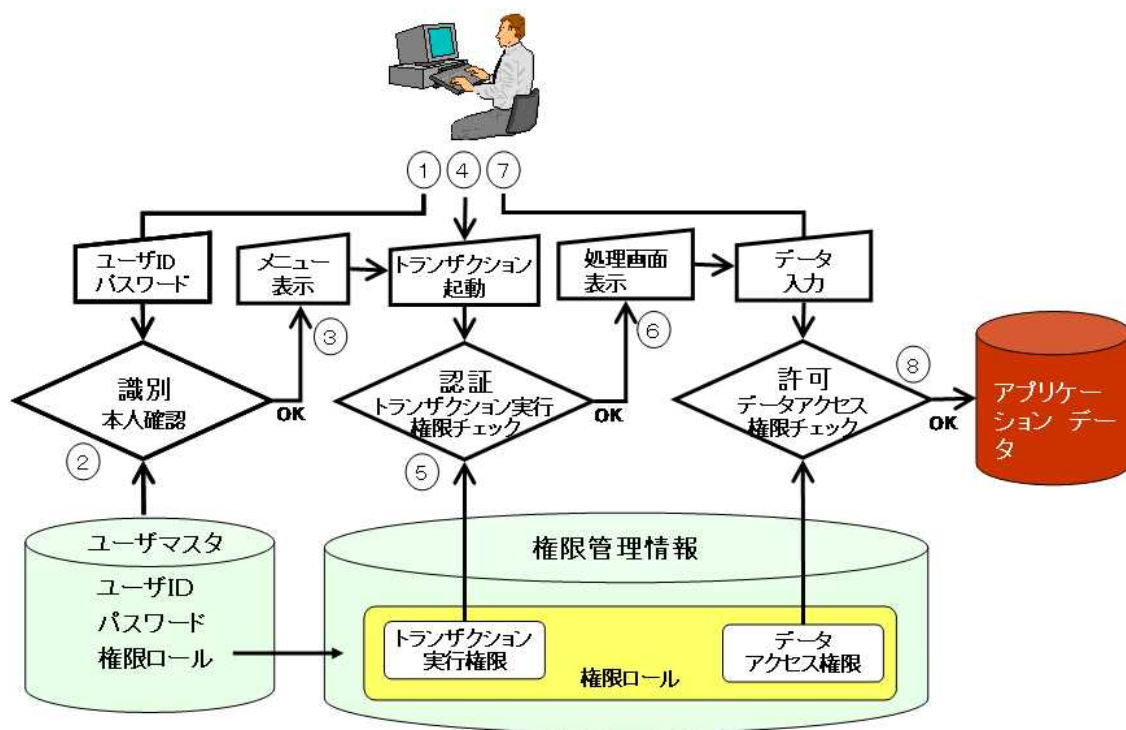
(認可ステップ)

- ④ ユーザは、表示されたメニュー画面から実行したい機能（トランザクション コード）を選択する。
- ⑤ システムは、選択された機能（トランザクション コード）に対する実行権限がユーザに割り当てられているか確認する。
- ⑥ 実行権限が割り当てられていれば、システムは指定された機能（トランザクション コード）を実行する。その結果、ユーザ端末に処理画面が表示される。

(許可ステップ)

- ⑦ ユーザは⑥によって表示された画面にデータ（何時、どこで、誰が、何を、幾つ、幾らでなどの情報）を入力する。
- ⑧ システムは、入力されたデータ（例えば、得意先、仕入先、品目など）に対するアクセス権限（登録権限、変更権限、参照権限）がユーザに割り当てられているか確認する。
- ⑨ ①～⑧が完了すると、ユーザがアプリケーションデータを処理可能になる。

図表 2. 6. 1-1 SAP ERP のアクセスコントロール手順



2.6.2 特権ユーザ

SAP ERP には、システムのインストールや管理のために用いる特権ユーザ（全権を割り当てられているユーザ ID）が存在する。特に注意を払う必要があるユーザ ID に“SAP*”と“DDIC”がある。これらのユーザ ID は、システムインストール時に自動登録され、その初期パスワードが広く知られている。

➤ SAP*

- ・ SAP*は特権ユーザであり、全権が割り当てられている。従って、パスワードの管理を厳重に行う必要がある。
- ・ 特権ユーザ ID “SAP*” は、ユーザマスタに登録されている。SAP*（初期パスワード 06071992）と登録されていない“SAP*”の2種類が存在する点に注意が必要である。
- ・ ユーザマスタに登録されていない（＝ユーザマスタにユーザ登録する前から存在する）SAP*のパスワードは‘PASS’に定められており、これは広く知られている。更に、重要な点はこのパスワードを変更できない点である。何故なら、この“SAP*”がユーザマスタに登録されていないからである。（SAP 技術者はこの SAP* を「ハードコーディングされているユーザ ID」という言い方をすることが多い）
- ・ この“SAP*”が存在する理由は、ランドスケープのところで説明した「クライアント」の登録直後（＝ユーザ ID が一つも登録されていない状況）、そのクライアントにログオンできるユーザが最低一つ必要だからである。
- ・ この“SAP*”はユーザマスタに“SAP*”が登録された時点で自動的に使用できなくなる。すなわち、“SAP*”のパスワードは‘PASS’ではなくなり、ユーザマスタに登録した“SAP*”のパスワードになる。
- ・ ユーザマスタに登録されている。“SAP*”の初期パスワード（＝06071992）も広く知られている
- ・ 特に注意しなければならないのは、何らかの理由でユーザマスタから“SAP*”を削除すると、ユーザマスタに登録されていない SAP*が復活し、パスワードが‘PASS’に戻ってしまうことである。
- ・ ユーザマスタに登録されていない“SAP*”を定常的に無効化するには、プロファイルパラメータの設定が必要である。ユーザマスタに登録されていない“SAP*”を定常的に無効化するためのプロファイルパラメータ ID は“`login/no_automatic_user_sapstar`”である。

➤ DDIC

- ・ DDICはインストールやアップグレード作業等で、ディクショナリ情報を登録／変更するために用意されている。ユーザ ID である。
- ・ “SAP*”同様 DDIC には全権が割り当てられているので、パスワードの管理を厳重に行う必要がある。

2.7 開発／保守コントロール機能

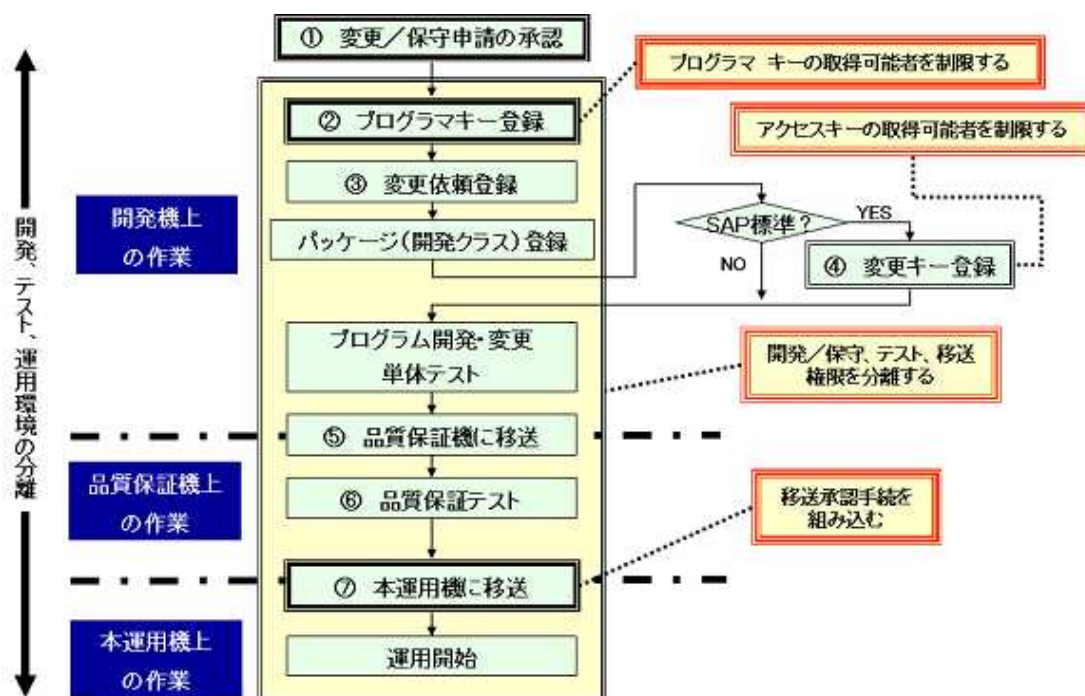
SAP ERP の開発／保守コントロール機能は、3 システムランドスケープを前提に構築されている。すなわち、

- ① 開発システムでのみ、開発／保守、単体／結合テストが実施できるように設定する
- ② 品質保証システムでは、本稼働のシミュレーションとして「統合テスト」／「ユーザ受入テスト」を行う。
- ③ ユーザ受入テストが終了し、ユーザ承認を得た後、「移送」とよぶ処理を介して本稼働システムに開発・変更内容を反映する
- ④ SAP ERP の統制機能である「移送の承認プロセス」を組み込んでおくと、権限者による「承認処理」を実行しないと、「移送」操作を行うことができないようにコントロールすることができる。

図表 2.7-1 を見ながら、SAP ERP の開発／保守コントロールを説明する。

- ① 開発／保守申請を審査し、承認する。申請の承認手続きは、SAP ERP の外で行われる。（「承認」手続を SAP ワークフローを使って行うこともできる）
- ② 開発／保守作業を実施するには、開発権限の他に「プログラマキー（開発者キー）」が必要である。プログラマキー（開発者キー）の取得権限を特定の者に制限することにより、プログラム開発／変更に対する強力な統制を実現できる
- ③ 「変更依頼」は開発／保守した複数のオブジェクトを束ねる役割を果たす。移送を行うには必ず「変更依頼」を登録しなければならないので、変更依頼の登録権限の管理は開発／保守統制に重要な役割を果たす。
- ④ 開発者はアクセスキーがないと、開発権限があっても SAP 標準のプログラムやテーブル定義等の変更ができない。アクセスキーの取得権限を特定の者に制限することにより、モディフィケーション（＝SAP 標準プログラムやテーブル定義等の変更）に対する強力な統制を働かすことができる
- ⑤ 品質保証システムへ移送を行う
- ⑥ 品質保証テスト（＝統合テスト／ユーザ受入テスト）を行う
- ⑦ 本稼動システムへ移送を行う。前述したように、移送操作を行うにあたり権限者による承認がないと移送ができないように指定することができる。

図表 2.7-1 開発／保守プロセスと統制機能



2.8 セキュリティ監査ログ機能

セキュリティ監査ログ機能を有効化するとユーザ管理、権限管理に関する操作等をログに残すこ

とができる。ログに残すことが可能な情報を 表 2.8-1 に示す。

セキュリティ監査ログ機能は、SAP ERP をインストールしただけでは使えない。有効化作業を実行することによって使えるようになる。

また、フィルタを設定することにより収集／照会するログの種類を選択することができる。図表 2.8-2 参照。

図表 2.8-1 セキュリティ監査ログ機能概要

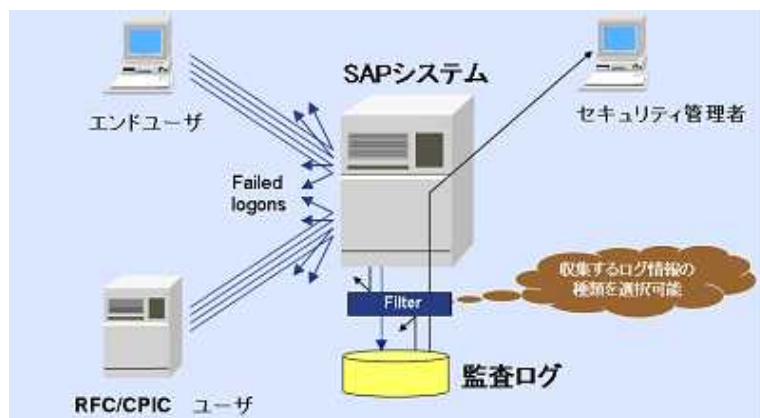


表 2.8-2 セキュリティ監査ログの種類

・ ユーザのログオフ
・ 正常にログオン
・ ログオンに失敗
・ ユーザ &B がクライアント &A でパスワードチェックに失敗した後でロック
・ ユーザ &B がクライアント &A で不正パスワード入力後のロックを解除
・ RFC/CPIC ログオンに成功
・ RFC/CPIC ログオンに失敗
・ RFC コール &C (汎用グループ = &A) が正常に実行した
・ RFC コール &C (汎用グループ = &A) に失敗した
・ トランザクション &A が開始された
・ トランザクション &A がロックされた
・ トランザクション &A がロック解除された
・ トランザクション &A の開始に失敗
・ レポート &A が開始された
・ レポート &A の開始に失敗した (理由 = &B)
・ クライアント &A のユーザ &B のパスワードが変更された
・ ユーザ &A が削除された
・ ユーザ &A がロックされた
・ ユーザ &A がロック解除された
・ ユーザ &A の権限が変更された
・ ユーザマスタレコード &A が変更された
・ 権限/権限プロファイル &B が登録された
・ 権限/権限プロファイル &B が削除された
・ 権限/権限プロファイル &B が変更された
・ ユーザ &A が登録された
・ 権限/権限プロファイル &B が有効化された
・ &A バイトがファイル &C にダウンロードされた
・ クライアント &A のユーザ &B がパスワードチェックで不合格

監査人は、システム監査ログをチェックし、不正なアクセスの兆候や可能性を評価することができる。

2.9 監査情報システム (AIS)

監査情報システム (AIS : Audit Information System) を使うと、SAP ERP が収集／保持している様々な情報を分析し、監査 (内部統制監査、会計監査、税務監査、システム監査など) に役立つ多様なレポートを作成することができる。

監査情報システムは大手監査法人の協力を得て SAP 社が開発したツールであり、監査人の目から見て必要な情報を網羅している。

監査情報システムの実体は、監査に必要なレポートのセットである。リース 4.6 以降はレポートをセットにする方法として、権限管理のロールが備えるメニュー機能を使っている。図表 2.9-1 に監査情報システムのメニュー例を示す。

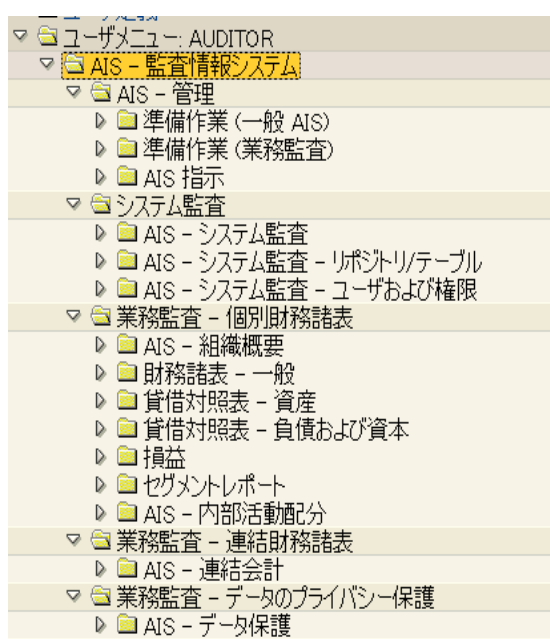
SAP ERP の監査人は効果的かつ効率的な監査を行うために、監査情報システムの利用方法を習得する必要がある。

第3章で示すチェックリストには、実査を行う方法として AIS に含まれるレポートの ID (=プログラム名) が示されている。ものがある。

なお、監査情報システムを使って全般統制監査を行うには、次の権限（ロール）を事前に付与してもらう必要がある。

- SAP_AUDITOR_SA_BC
- SAP_AUDITOR_SA_BC_CCM_USR
- SAP_AUDITOR_SA_BC_CUS_TOL

図表 2.9-1 監査情報システムのメニュー例



2.10 プロファイルパラメータ

SAP ERP のセキュリティ機能は、プロファイルパラメータの値によってコントロールされる。例えばパスワードの最低長や有効期間などをはじめとして、セキュリティにかかわる様々なチェック、制限等がプロファイルパラメータの値に基づいて実施される。

従って、監査人は、プロファイルパラメータ値の妥当性を確認する必要がある。

図表2.10-1 全般統制監査を行うに当たりチェックが必要なパラメータを示す。

図表2.10-1 チェックが必要なパラメータ

パラメータ ID	役割	チェック事項
login/disable_multi_gui_login	多重ログオンを無効化する。 このパラメータを 1 にセットすると、R/3 システムへの多重ログオン(同一のクライアントに同一のユーザ名でログオンすること) はシステムによって禁止される。 システムが多重ログオンを検出した際に、“現在のセッションを強制終了する” もしくは “このログオンを強制終了する” というオプションを持つ。	無効に設定されている。

パラメータ ID	役割	チェック事項
	イアログボックスが表示される。 このパラメータは SAPGUI ログオンでだけ機能する。	
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。
login/fails_to_session_end	1 ユーザ 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。
login/fails_to_user_lock	何回ログオンを失敗するとユーザ ID をロックするか指定する。	6回程度に設定されている事。
login/min_password_diff	ユーザが自身のパスワードを変更する場合、新規パスワードにおいて、旧パスワードと異なっていなければならない文字の数を指定する。 このパラメータは、新規ユーザの登録時、またはパスワードのリセット時(=> 初期パスワード)には影響を及ぼさない。	最短パスワード長の半分程度の長さが設定されている事。
login/min_password_digits	パスワードに含まれる「数字」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 小桁数 (0-9) 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 効である。有効な入力、書式、範囲 : 0 - 8	(解説) 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事。ことを確認する。 このパラメータの値が、1文字以上に設定されている事。ことを確認する。
login/min_password_letters	パスワードに含まれる「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文字の最小数が設定される。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	同上
login/min_password_specials	パスワードに含まれる「特殊文字」の最小数 このパラメータによりパスワードに含まなければならない 特殊文字の最小数が設定される。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効である。特殊文字 = (! " \$ % & ' () = ? ` * + ~ # - _ . : ; [ \ ] ^ _ ` { } ~ "), 有効な入力、書式、範囲 : 0 - 8	同上
login/min_password_uppercase (リリース依存)	パスワードに含まれる大文字数の最小値 このパラメータにより、パスワードに含まれる大文字数の最小値が規定される。 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またはリセットに影響を及ぼす。 プロファイル login/password_downwards_compatibility に 5 という値が設定されている。場合、このパラメータは評価されないません 単位 : 大文字 (A - Z) の数	同上
login/min_password_lowercase (リリース依存)	パスワードに含まれる小文字数の最小値 このパラメータによりパスワードに含まれる小文字の数の最小値が規定される。 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またはリセットに影響を及ぼす。 プロファイル login/password_downwards_compatibility に 値“5”が設定されている。場合、このパラメータは無効になる。 単位 : 小文字 (a - z) の数	同上
login/min_password_length	ログオンパスワードの最低の長さ指定	6以上に設定されている事。こと
login/multi_login_users	多重ログオンが許可されたユーザのリスト このリストには、システムへの多重ログオンが許可された R/3 ユーザの ID (クライアント未指定) を含む。 このプロファイルパラメータは、ダイアログユーザのみに適用される。	ユーザIDが登録されていないことを確認する
login/no_automatic_user_sapstar	コーディングレベルで存在する特殊ユーザ“SAP*”を無効化する	無効化されている事。ことを確認する
login/password_comp	ユーザパスワードをパスワードルールに照らしてチェックするかどうかを	登録済ユーザIDのパスワードを、

パラメータ ID	役割	チェック事項
liance_to_current_policy	指定 値 0: チェックなし 値 1: パスワード変更が必要かどうかをチェック タイプが“SERVICE” および“SYSTEM”であるユーザは原則的にパスワード変更要件から除外されるためこのパラメータの影響を受けない。 変更されたパスワード規則は過去のパスワードには該当しない。 パスワード規則はパスワード変更が行われる際にのみ評価される。 NetWeaver 7.0 以降では、特定のユーザに対しパスワードを早期に変更するよう明確に指示することができる。これには、パスワードが現在のパスワード規則に準拠していないユーザが該当する。(ノート 862989)	新しく設定したパスワードルールに照らしてチェックを行い、ルールに合わない場合、パスワードの変更を要求するように設定されている事。ことを確認する。(値=1)
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。	1ヶ月程度に設定されている事。ことを確認する。
login/password_max_idle_initial (リリース依存)	未使用初期パスワードの有効期間 ユーザ管理者が新しいユーザIDを登録した場合、または、既存のユーザIDのパスワードを変更した場合、ユーザは次のログオン時にそのパスワード(初期パスワード)を変更しなければならない(ユーザ自身のみが自分のパスワードを知っていることを保証するため)。 パスワードをリセット した後、初期パスワードを使用してログオンするまでの期間の最大値を設定する。この期間が経過すると、メッセージ“The initial password has expired; request a new one”が表示されてログオンは拒否される。	1ヶ月程度に設定されている事。ことを確認する。
login/password_max_idle_productive (リリース依存)	未使用の実パスワードの有効期間 ユーザが自分自身のパスワードを変更すると“実”パスワードが登録される。このユーザが自分のパスワードを変更できるのは、早くとも login/password_change_waittime によって指定した日数を過ぎた後に限られます。 パラメータ login/password_expiration_time により、何日経過した後でシステムがユーザに対してパスワードの変更を要求するかを指定する。 このパラメータを使用して、変更したパスワードの有効期間を設定することができる。。新パスワードでログオンしないまま、この期間を経過するとそのパスワードは無効になる。メッセージ“Password was not used for a long period and therefore deactivated”が表示され、ログオンが拒否される。	1ヶ月程度に設定されている事。ことを確認する。
login/password_max_new_valid (リリース依存)	新規登録ユーザ用パスワードの使用期限 ユーザ管理者は、新規ユーザの登録時に初期パスワードを 割り当てる。このプロファイルパラメータを使用して、ユーザID を登録した時点から、ユーザが最初に ログオンする時点までの最長期間を設定する。この期間を過ぎると、“初期パスワードが期限切れになりました”という メッセージが表示され、ログオンが拒否される。 値 0: 初期パスワードは無期限の期間に対して有効 値 1: 初期パスワードは同一日についてのみ有効 それ以外: 指定日数を過ぎると、ユーザは初期パスワードでログオンできなくなる。	1ヶ月程度に設定されている事。ことを確認する。
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事。場合必要度は低い。

<Web AS ABAP 7.00 または NetWeaver 2004s 以降の変更点>

◆ パスワード:

大文字と小文字の区別、最大長の 8 桁から 40桁への増加

新規パスワードでは、大文字と小文字が区別される。さらに、パスワードに 40 桁まで含めることが可能になる(これまでは、最大長は 8 桁)。新しくインストールされたシステムでは、このルールは即時にすべてのユーザに適用される。下位リリースから Web AS ABAP 7.00 または NetWeaver 2004s にアップグレードされたシステムでは、すべてのユーザは引き続き従来のパスワードを使用してログオンする

ことができる。ユーザマスタレコードに、そのユーザが新規のパスワードを使用しているのか、または古いタイプのパスワードを使用しているかの情報が格納される。システムがパスワードをチェックする際に、この情報が分析される。ユーザが古いタイプのパスワードを使用している場合は、パスワードの最初の 8 桁が大文字に変換され、残りの 32 桁はスペースとなる。このような処理が行われない場合、大文字への変換なしでパスワード全体が分析される。ユニコードシステムでは、パスワードにユニコード文字を使用することができる。

関連する（新規）プロファイルパラメータ

- login/min_password_lowercase
- login/min_password_uppercase
- login/password_downwards_compatibility

◆ パスワード履歴: 必要に応じたサイズ定義（従来の制限は 5 エントリまで）

パスワード変更時にユーザが割り当てたパスワードは、パスワード履歴に格納される（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）。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しないようにする。これまで、パスワード履歴は 5 エントリまでに制限されていました。今後は、プロファイルパラメータ（login/password_history_size）を使用して、パスワード履歴のサイズを定義することができる（最大 100 エントリ）。

◆ パスワード変更のロック期間の選択（従来の期間は 1 日間）

パスワード履歴が無視されないようにするため、ユーザはロック期間を経過した後でのみパスワードの再変更を行うことができる（例外: システムによってパスワードの変更が求められる場合）。プロファイルパラメータ login/password_change_waittime（最大値: 1000 日間）を使用して、ロック期間を選択することができる。

◆ （改善）より厳しいパスワードルールによるパスワード変更

現在のパスワードがパスワードルールに沿っていないユーザに対してのみ、（あらかじめ）パスワードの変更が要求されるように設定することができる。これには、以下のプロファイルパラメータを設定する。

login/password_compliance_to_current_policy = 1

◆ 使用されていないユーザのパスワード有効期間の制限

初期パスワード（ユーザ管理者によって割り当てられ、ユーザが次の機会に変更しなければならないパスワード）を含め、使われなくなったユーザIDのパスワードをそのまま放置することはセキュリティ上のリスクが伴う。初期パスワードを含め、休止状態のユーザのパスワードの有効期間を制限できるようになった。

タイプ SERVICE および SYSTEM の（技術）ユーザは、このルールから除外される。

関連する（新規）プロファイルパラメータ

- login/password_max_idle_initial
- login/password_max_idle_productive

■ 変更点

◆ ログオン:

不適切なエラーメッセージの回避

不適切なログオンデータを使用してログオンしようと する場合、原則として、今後は**一般的なエラーメッセージ** “正しいユーザ名とパスワードでもう一度ログオンしてください” のみが出来される。失敗したログオンに関する詳細な理由（例：ユーザアカウントのロック、ユーザアカウントの有効期限切れなど）は、有効なログオンデータが入力されてから提供される。システムがログオンデータをチェックすることができない、または追加チェックが許可されていないなどのエラーシナリオは、このルールから除外される。

- “パスワードを持っていません: パスワードを使用してログオンできません”
- “パスワードによるログオンはできません - 失敗回数が多すぎます”

◆ セキュリティに関連する一部のプロファイルパラメータのデフォルト値が変更されました。

- login/failed_user_auto_unlock : 0 (1 から変更)
失敗したログオンのロックは、無制限の期間で有効となる。
- login/fails_to_user_lock : 5 (12 から変更)
失敗したログオンに対するロックは、パスワードログオンが 5 回失敗した後で設定される。
- login/no_automatic_user_sapstar : 1 (0 から変更)
スーパーユーザは、明示的に有効化される必要がある。
- login/min_password_lng : 6 (3 から変更)
パスワードは、6 桁以上でなければならない。
- login/ticket_expiration_time : 8 (60 から変更)
ログオンチケットは、8 時間のみの有効。

◆ プロファイルパラメータ login/password_max_new_valid および login/password_max_reset_valid は、プロファイルパラメータ login/password_max_idle_initial によって置き換えられた。つまり、初期パスワードの有効期間の制限に関して、ユーザ管理者による最初の設定および後続設定が区別されなくなる。

3 チェックリストの特徴と形式

3.1 チェックリストの形式

図表 3.1-1 にチェックリストの形式を示す

図表 3.1-1 チェックリストの形式

No	分類	区分	ランク	チェック内容	関係するリスク、確認方法、統制・緩和方法等	監査手順、確認方法	評価
1.	文書化・運用・監視	重要度	区分 ・文書化 ・運用 ・監視	ユーザー管理に関する管理規程・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ ☐ ユーザーIDの登録・変更・削除申請書は定義され、使用されていますか はい ☐ いいえ ☐ 管理手順を説明してください （ユーザーIDの登録・変更・削除申請書の提出する権限の承認を行なうのは誰（部署、役割）ですか） ユーザーIDの登録・変更作業を行うのは誰ですか （誰によって承認（モニタリング）は誰（部署、役割）ですか） トレーニング等を通じ、関係者にはIPアドレスにおけるユーザーIDの管理手順を周知徹底していますか はい ☐ いいえ ☐ 承認されていますか （承認してください）		【整備状況評価】 1. 一般ユーザーIDに対する登録・廃止・削除のルールを定めた規程等が存在し承認されていることを確認する。 【運用状況評価】 1. 一般ユーザーIDの登録・変更・削除のログを抽出し、それに従って一般ユーザーIDの登録・変更・削除の申請書を出す。	
2.			分類 項目名称	フォームはありますか？ はい ☐ いいえ ☐ はいの場合、提出されたフォームを承認するのは誰ですか？ （承認してください） フォームには次のような項目が含まれていますか？ ☐ ユーザタイプ	（解説） ユーザタイプには、「ダイアログ」、「システム」、「送信」。		

3.2 チェックリストの特徴

本チェックリストにおいて、特徴的な点としては、以下の様なものがある。

(1) 分類・区分分け

分類項目毎に、チェック内容をいくつかの区分に分けてチェック出来る様な形式を採った。

チェック項目としては、基本的にはこの区分が単位となるが、項目が多い場合、さらに分けている場合もある。これは、ひとつの区分でも、下記で示す異なるランクを定義する必要がある場合などに対応している。

図表 3.2-1 は、アクセスコントロールに関するチェックリスト例である（表の一部を示している）。

「区分」欄に次の様な分類を示している。

- ・ 文書化、教育
- ・ 命名規則
- ・ RFC 宛先（ユーザ）
- ・ 運用

（以下省略）

(2) ランク・優先度付け

チェックリスト項目に優先度（ランク）を示した。

A : 必須

B : A ランク項目のチェック結果に依存して実施

C : 参考項目

A ランクは、「ないと設計評価ができないもの。SOX対象業務の稼動環境、業務システムに対し直接的な改ざん、破壊につながるもの」であり、監査上必須であると考えられる。

B 及び C ランクは、監査の状況に応じて行われるものとなる。

(3) 成熟度の評価

本チェックリストでは、チェック結果を OK/NG だけで判断するのではなく、成熟度レベルで判断できるように考慮した。これは、被監査企業において、今後の内部統制体制等を見直す時の判断材料となる事を想定している。

図表 3.2-2 チェックリスト例

No	分類	区分	ラ ン ク	チェック内容	関係するリスク、確認方法、統制・緩和方法等	監査手順、確認方法	評 価
1.	ユー ザ 管 理	文書化・ 教育	A	ユーザ管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ ☐ ユーザIDの登録・変更・削除申請書は定式化され、使用されていますか はい ☐ いいえ ☐ 管理手順を説明してください ユーザIDの登録・変更・削除申請書を提出する権限があるのは誰(部署、役職)ですか 「 」 申請書の承認を行なうのは誰(部署、役職)ですか 「 」 システム上に、ユーザIDの登録・変更作業を行うのは誰(部署、役職)ですか 「 」 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役職)ですか 「 」 トレーニング等を通し、関係者にSAP ERPにおけるユーザIDの管理手順を周知徹底していますか はい ☐ いいえ ☐ それは、どのように実施していますか、説明してください。 「 」		【整備状況評価】 1. 一般ユーザIDに対する登録・修正・削除のルールを定めた規程等が存在し承認されていることを確認する。 【運用状況評価】 1. 一般ユーザIDの登録・変更・削除のログを抽出し、それに紐づく一般ユーザIDの登録・変更・削除の申請書を抽出する。	
2.			A	ユーザID登録/変更フォームはありますか? はい ☐ いいえ ☐ はいの場合、提出されたフォームを承認するのは誰ですか 「 」 フォームには次のような項目が含まれていますか: ☐ ユーザタイプ	・ ユーザIDの登録/変更フォームを規定します このフォームには、少なくともユーザ名、所在地、電話番号、有効日付(一時ユーザの場合)、およびこのユーザがSAPシステムで実行する権限ロールを記入します このフォームの提出には管理職の承認を必要とします。 (解説) ユーザタイプには、「ダイヤログ」、「システム」、「通信」。		

4 SAP ERP IT 全般統制監査の方法

ここでは、チェックリストを使いどのように監査（場合によっては、内部統制設計／評価）手順のモデルを示す。

チェックリストは、次の4種がある。

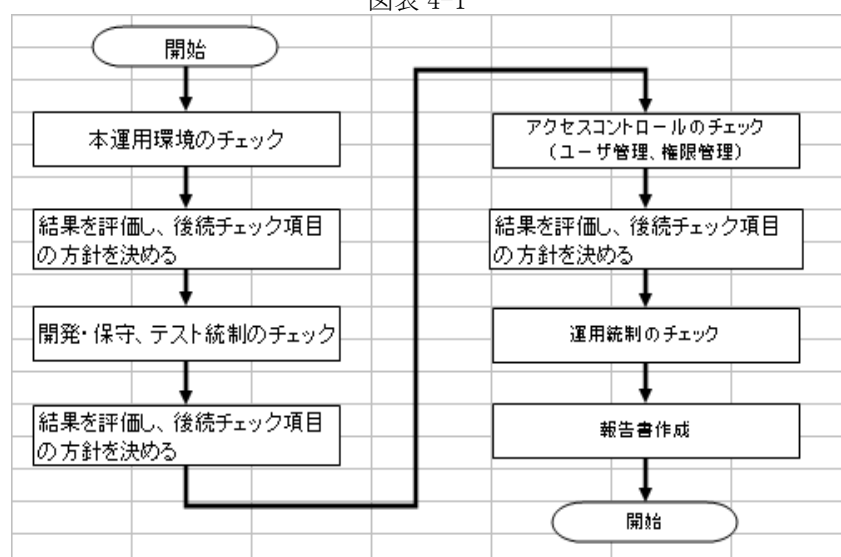
- ・ 本運用環境チェックリスト
- ・ アクセスコントロールチェックリスト
- ・ 開発／保守・テストチェックリスト
- ・ 運用統制チェックリスト

上記チェックリストの標準的な適用順序は次のようになる。

監査対象の特性、監査目的などに応じ、順序の変更、あるいは一部の実行も可能である。

図表 4-1

1. 「本運用環境チェックリスト」を使い、本運用環境の統制状況をチェックする。
2. ①の結果を評価し、これ以後のチェック方針を決める。
3. 「開発／保守、テスト統制チェックリスト」を使い、開発／保守、テストに関する統制状況をチェックする。
4. ③の結果を評価し、これ以後のチェック方針を決める。
5. 「アクセスコントロール チェックリスト」を使い、ユーザ管理、権限管理の統制の状況をチェックする。
6. ⑤の結果を評価し、これ以後のチェック方針を決める。

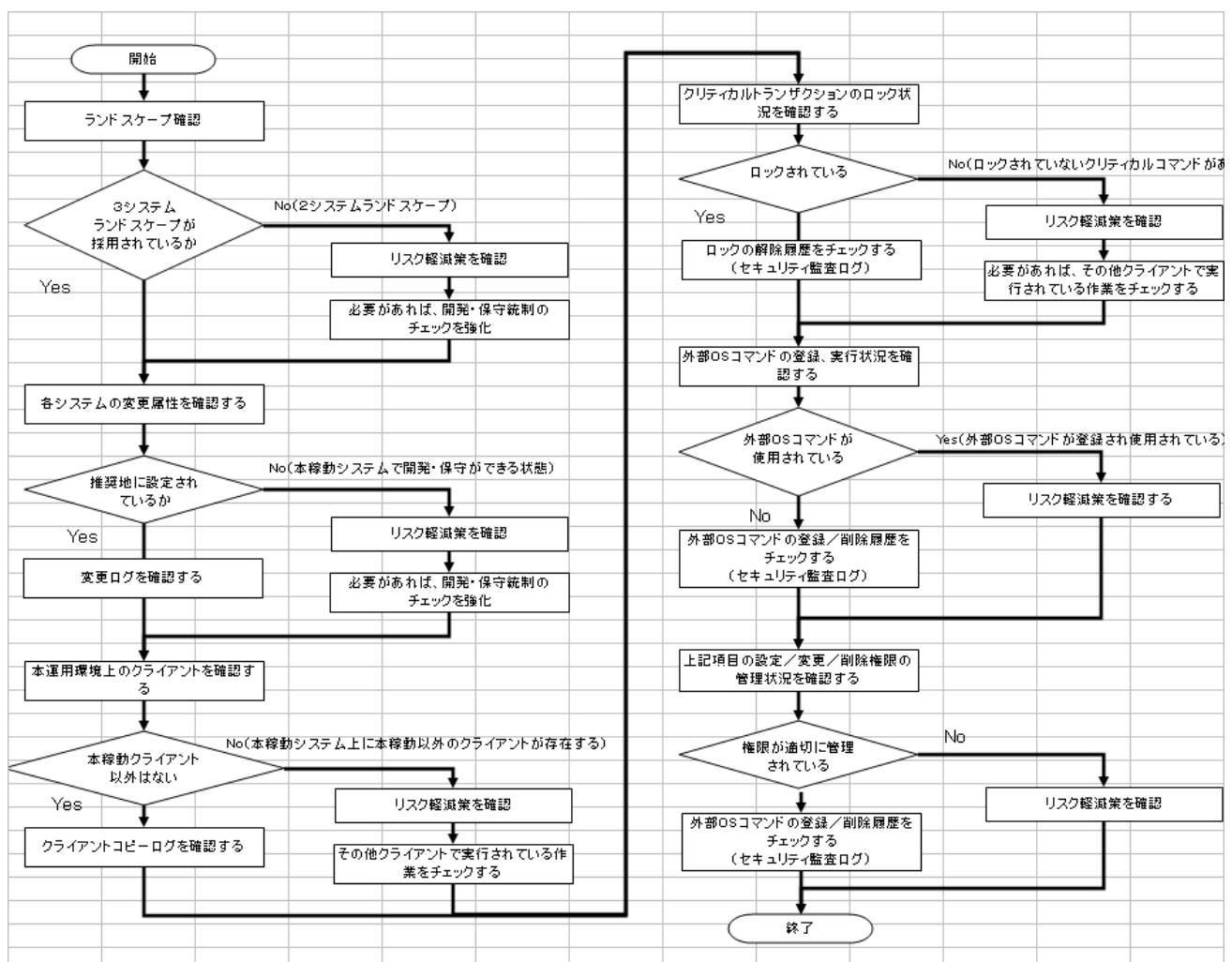


4.1 本運用環境の監査手順

本運用環境が、Web アプリケーションサーバ機能を有効に使い、安全に設定されている。か監査確認する。監査のポイントは下記の通り。

- 3 システムランドスケープ構成となっていること
- 開発用クライアント（開発システム）、テスト用クライアント（品質保証システム）、本稼動クライアント（本稼動システム）の変更属性が適切に設定されていること
- 開発システム環境では有用なコマンドであるが、本運用環境ではリスクが大きいコマンド（クリティカルコマンドと呼ぶ）がロックされていること
- クリティカルコマンド（トランザクションコード）がロックされていること
- 上記の登録／変更権限が適切に割り当てられていること
- 上記内容が文書化され、教育されていること

図表 4.1-1



4.2 開発／保守の監査手順

「開発／保守チェックリスト」は、監査人が、企業が財務報告に関連して SAP システムのカスタマイズ・アドオンやモディフィケーションを実施する場合において承認及び導入前のテスト等が適切に行われているかをチェックする際に使用することができる。

「開発／保守チェックリスト」は、全 31 のチェック項目からなり、その構成（分類）は次の通り。

No. 1～ 4 開発・保守に関する現状把握

No. 5～ 9 カスタマイズ・アドオン

No.10～13 モディフィケーション

No.14～17 テスト

No.18～21 移送

No.22～24 緊急対応

No.25～28 アップグレード

No.29～31 開発・保守権限の分離

監査人は、監査の基準として「システム管理基準 追補版」や「COBIT for SOX」を用いる場合においても、「開発／保守チェックリスト」の対応するチェック項目を参照することにより、SAP システムの特性を踏まえて開発・保守の統制状況を監査することができる。「システム管理基準 追補版」と「開発／保守チェックリスト」との対応例を次に示す。

図表 4.2-1 「システム管理基準 追補版」と「開発／保守チェックリスト」との対応例

経済産業省 システム管理基準 追補版		開発／保守チェックリスト		
項番	統制目標の例	No.	分類	チェック内容
3－（１）－③ 一ホ	プログラムの変更は、変更 管理手順に基づき、保守の 責任者の承認を得ること	6	カスタマイズ・ア ドオンプロセスの 監査	実施する全てのカスタマイ ズ・開発・保守は承認され たものですか
		11	モディフィケーシ ョン	実施する全てのモディフィ ケーションは適切な承認者 による承認を得ていますか

「開発／保守チェックリスト」を用いた監査の標準的な手順は、次の通り（フロー参照）。

【開発・保守に関する現状把握】

最初に「開発・保守に関する現状把握」のチェック項目により、監査対象システムの開発・保守の実施状況を確認する。

また、開発・保守の体制についても実名で確認しておく。

監査対象システム上にアドオンオブジェクト（トランザクション、プログラム）やモディフィケーションオブジェクトが存在しない場合、または存在しても監査対象期間中にそのアドオンやモディフィケーションの作業が実施されていない場合には、チェック項目の内、整備状況の評価項目である「文書化・教育」の区分に属する項目だけをチェックすればよく、運用状況の評価項目である「運用」や「モニタリング」の区分に属する項目についてはチェックを省略できる。

【整備状況評価】

整備状況評価では、区分が「文書化・教育」のチェック項目について、規程類等の閲覧や関係者への質問等の方法により確認する。その際、承認手続きに使用する申請フォーム等の様式も合わせて確認する。

また、規程類と実際の運用との整合性を確認するため、実際のサンプルを1件閲覧して評価する。

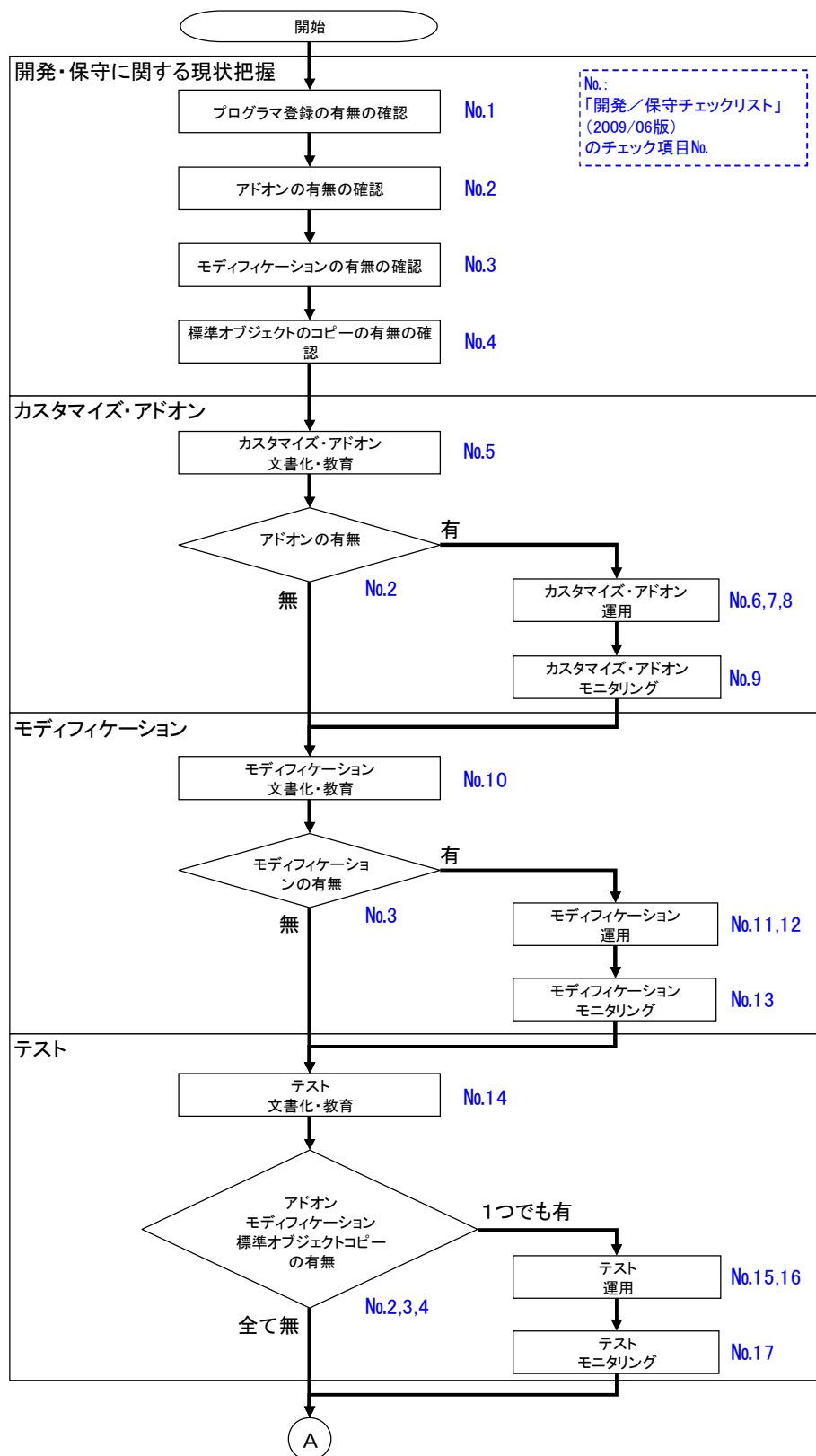
【運用状況評価】

運用状況評価では、区分が「運用」及び「モニタリング」のチェック項目について、評価対象期間中のコントロール発生状況（母数）に応じてサンプリングを行い、証憑を閲覧して評価する。

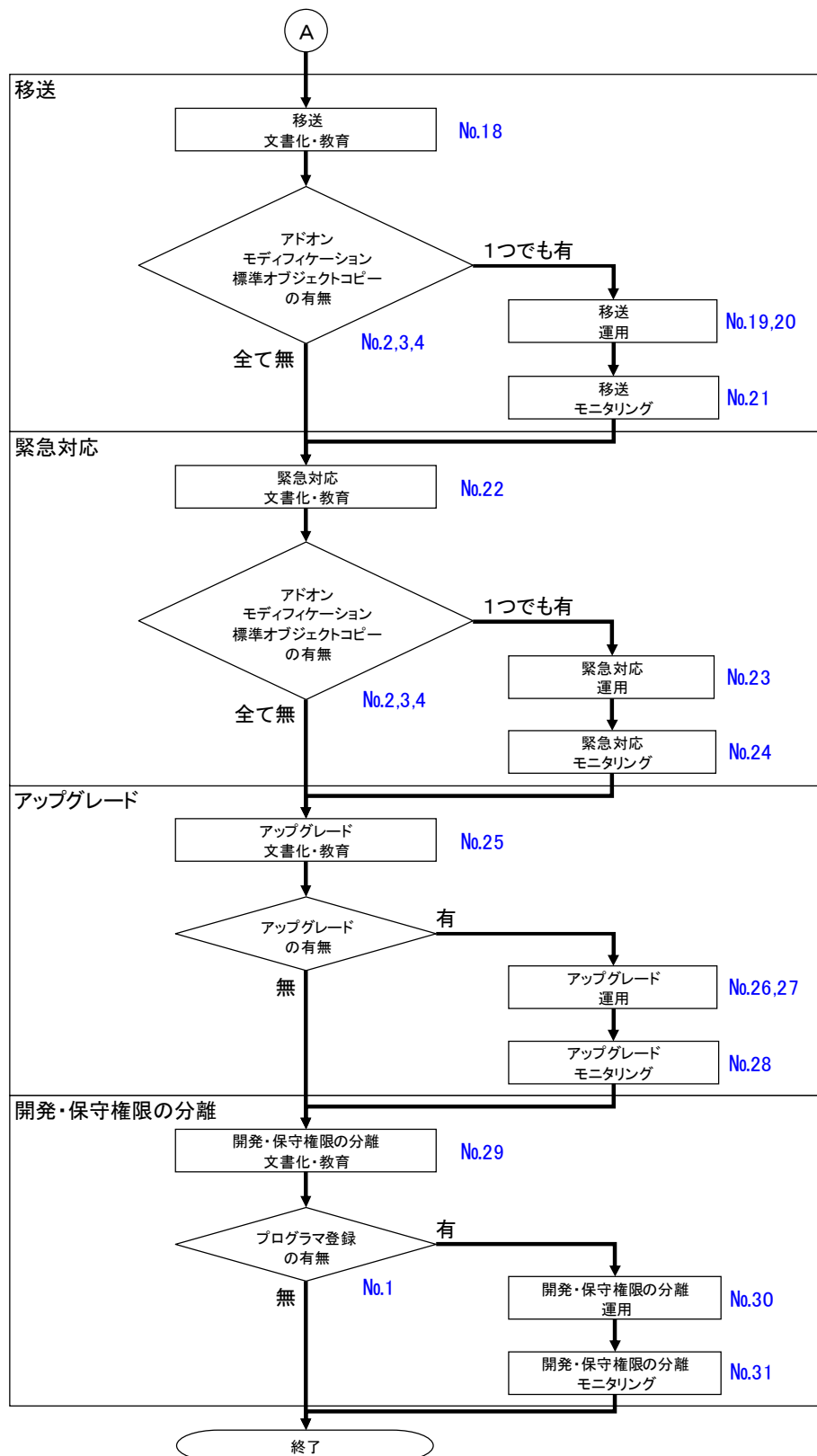
なお、開発・保守の作業者として登録されているプログラマのシステム上の権限については、アクセスコントロールの監査において、権限設定の適切性を評価する。

開発／保守の監査手順（フロー）

図表 4. 2-2



図表 4. 2-3



4.3 アクセスコントロールの監査手順

【整備状況評価】

アクセスコントロールの概要を関係者への質問、規程類等の閲覧により把握し、システムの実装状況との整合性をシステムからの出力情報により確認する。

1. ユーザ ID 管理体制の確認する
 - ・ OS、データベース、アプリケーションの特権、アプリケーションのユーザ ID のそれぞれについて管理ルールを確認する。
 - ・ ユーザ ID の登録者と権限の登録者、権限のユーザ ID への割当者等の分離状況を確認する。
 - ・ ユーザ ID のロック解除の手続きを確認する。
 - ・ 初期パスワードの本人への連絡方法を確認する。
2. スーパーユーザの概念を確認する。
 - ・ OS、データベース、アプリケーションについて、どういう権限を付与されているユーザをスーパーユーザとして管理しているかを確認する。
3. パスワードポリシーを確認する
 - ・ パスワード桁数
 - ・ 定期的なパスワードの変更ルール
4. ユーザ ID 管理台帳の整備状況を確認する。
 - ・ ユーザ ID と権限の一覧を入手する。
 - ・ プロファイルパラメタの更新権限付与者の確認
 - ・ 本番環境への移送権限付与者の確認
 - ・ アプリケーションのスーパーユーザ付与者確認
5. ログの取得状況を確認する。
 - ・ 運用状況を評価するための母集団を決定するため監査ログの取得状況を確認する。監査ログ等を母集団としてサンプルを抽出するのが理想であるが、監査ログ等が取得されていない場合は、何を母集団とすべきか検討する必要がある。

【運用状況評価】

ユーザ ID やそれに紐づく権限の登録、変更、削除等の運用状況を確認する。

監査ログが取得されている場合は、監査ログよりサンプルを抽出する。監査ログが取得されていない場合は、管理台帳等を母集団とすることになるが、その場合は母集団の網羅性、正確性に留意する必要がある。

監査する際に「システム管理基準 追補版」を基準として参照する場合には「アクセスコントロー

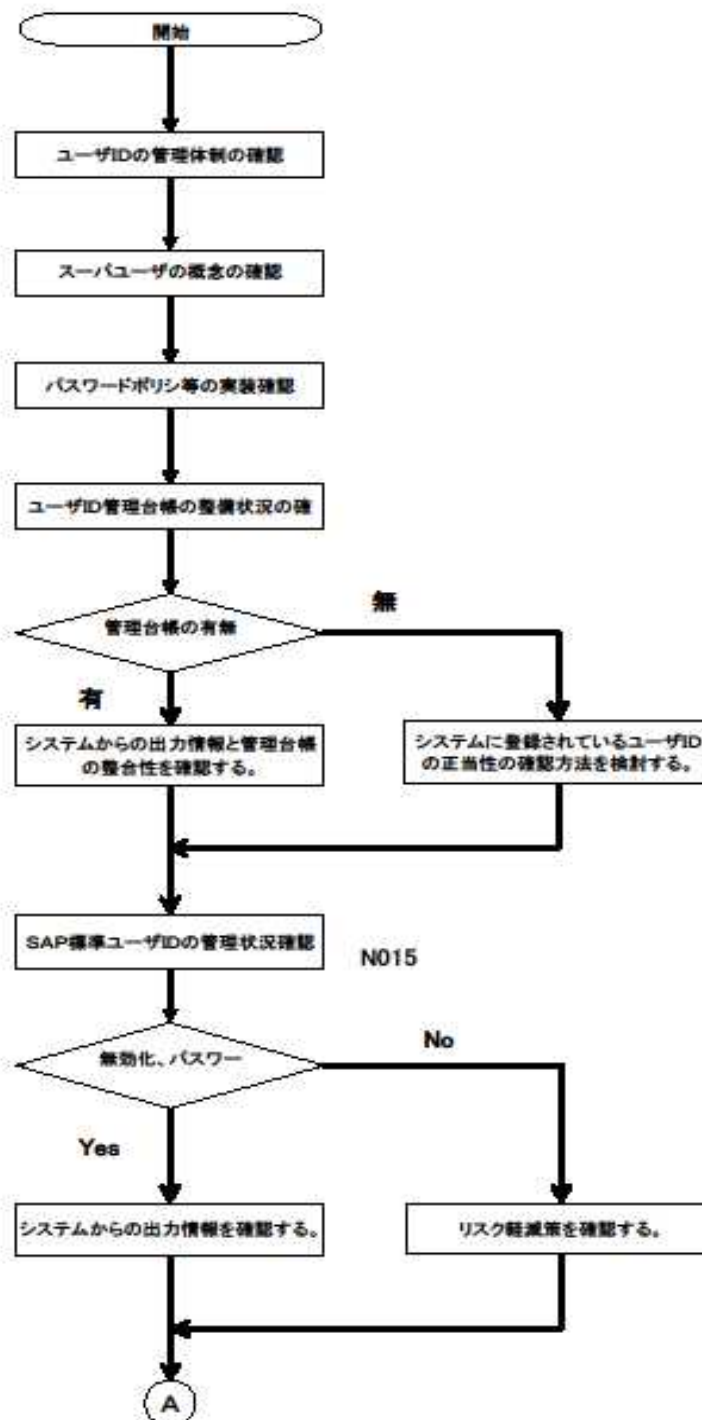
ル チェックリスト」との対応関係に留意する。

「アクセスコントロール チェックリスト」と「システム管理基準 追補版」の統制項目は必ずしも1:1では対応しておらず1:NまたはN:1の関係にあることに留意する。

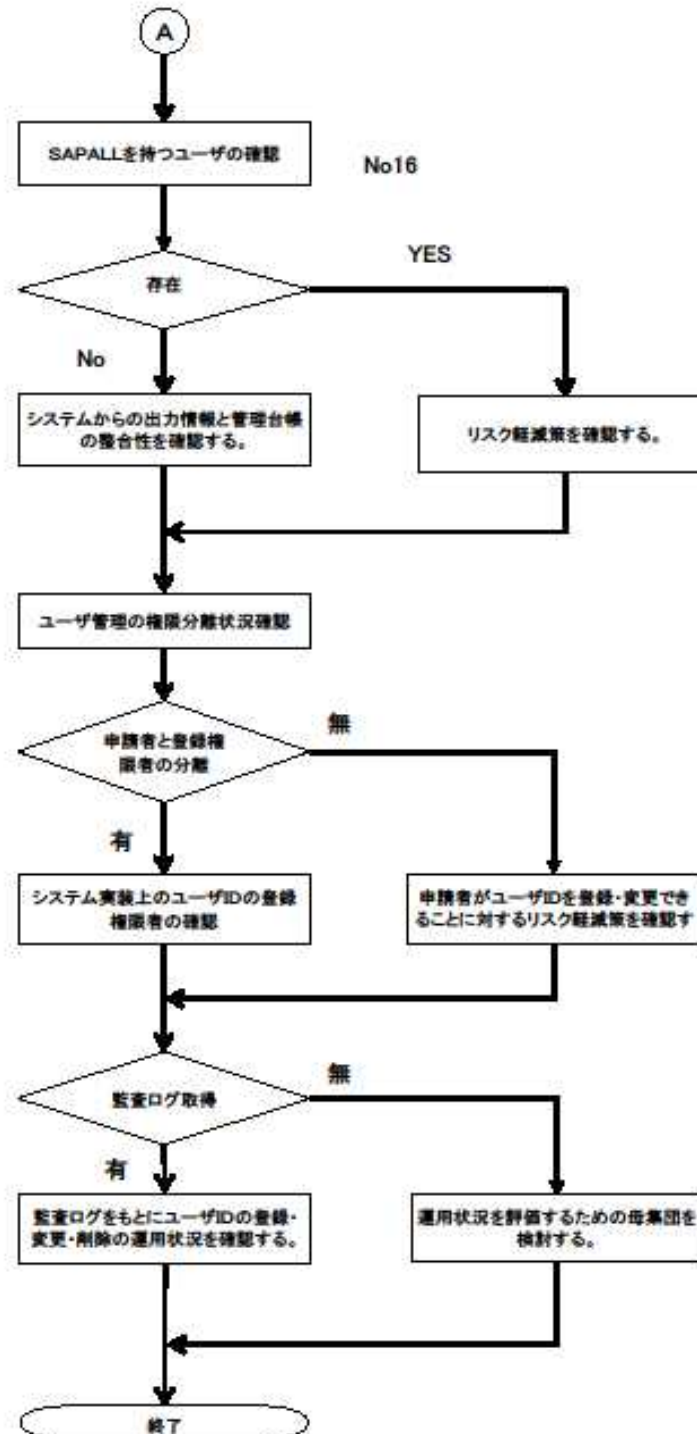
図表 4.3-1 「システム管理基準 追補版」と「アクセスコントロール チェックリスト」との対応例

経済産業省 システム管理基準 追補版		アクセスコントロール チェックリスト		
項番	統制目標の例	No.	分類	チェック内容
3-(3)-② 一口	担当者の登録及び登録削除のための手順が定められ、承認されていること。	1	ユーザ管理	ユーザ管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか
		2		ユーザ ID 登録/変更フォームはありますか?
		6		退社した従業員や、担当プロジェクトが終了したコンサルタントのユーザIDを削除する手順はありますか?
		13	特権ユーザの管理	特権ユーザ管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか
		17	権限管理	権限管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか
		21	緊急対応	緊急時における、パスワードの変更、ユーザロックの解除、権限の追加などの管理規定・手順等は文書化され、関係者に周知徹底されていますか

図表 4.3-2



図表 4.3-3



4.4 運用の監査手順

「運用チェックリスト」は監査人が SAP システムの運用関連作業（システムの起動／停止、緊急時対応、バックグジョブの実施等）の評価を実施する際に使用することができる。また運用の統制設計を行う際の参考資料としても利用できる。

この運用チェックリスト」は次の 8 つのチェック項目からなり、その構成（分類）は次の通り。

- No. 1 運用管理体制全般
- No. 2 システム起動／停止
- No. 3 緊急時対応
- No. 4 会計データに係るバックグラウンドジョブ
- No. 5 プロファイルパラメータ
- No. 5 SAP システムから通知されるエラー／警告
- No. 7 外部 OS コマンド
- No. 8 バックアップ／リストア

監査人は、監査の基準として「システム管理基準 追補版」や「COBIT for SOX」を用いる場合においても、「運用チェックリスト」の対応するチェック項目を参照することにより、SAP システムの特性を踏まえて運用の統制状況を監査することができる。「システム管理基準 追補版」と「運用チェックリスト」との対応例を次に示す。

図表 4. 4-1 「システム管理基準 追補版」と「運用チェックリスト」との対応例

経済産業省 システム管理基準 追補版		運用チェックリスト		
項番	統制目標の例	No.	分類	チェック内容
3-(2)-①-へ	情報システムで発生した問題を識別するために、システム運用の作業ログ・障害の内容ログ及び原因ログを記録し、保管すること。 取得されたログは、内容が改ざんされないように保管することが望ましい	6	SAPシステムから通知されるエラーや警告への対応 (SAP システムはアップリケーションの実行に影響を与えるエラーや問題点を監視しています。エラーや問題を認識するとログを作成し記録します 定期的にこのログを監視し、適切な対応を行う必要があります)	責任者にヒアリングを行う。必要に応じ、SAP システムのログを参照し、裏づけをとる。 ・ SAP システムから通知される エラーをトランザクション RZ20 または SM21 でチェックする ・ 失敗した更新 の有無をトランザクション SM13 でチェック ・ ABAP プログラム実行時エラー の有無をトランザクション ST22 でチェック

「運用チェックリスト」を用いた監査の標準的な手順は次の通り（フロー参照）。

【運用に関する文書の整備状況を把握】

まず運用手順書（運用マニュアル等）をチェックし（項目 No1）、概要システムの運用状況全体を評価する

【整備状況評価】

整備状況評価では項目 No2～8 の項毎に、区分が「文書化・教育」のチェック項目について、規程類等の閲覧や関係者への質問等の方法により確認する。その際、承認手続きに使用する申請フォーム等の様式も合わせて確認する。

また、規程類と実際の運用との整合性を確認するため、実際のサンプルを 1 件閲覧して評価する。

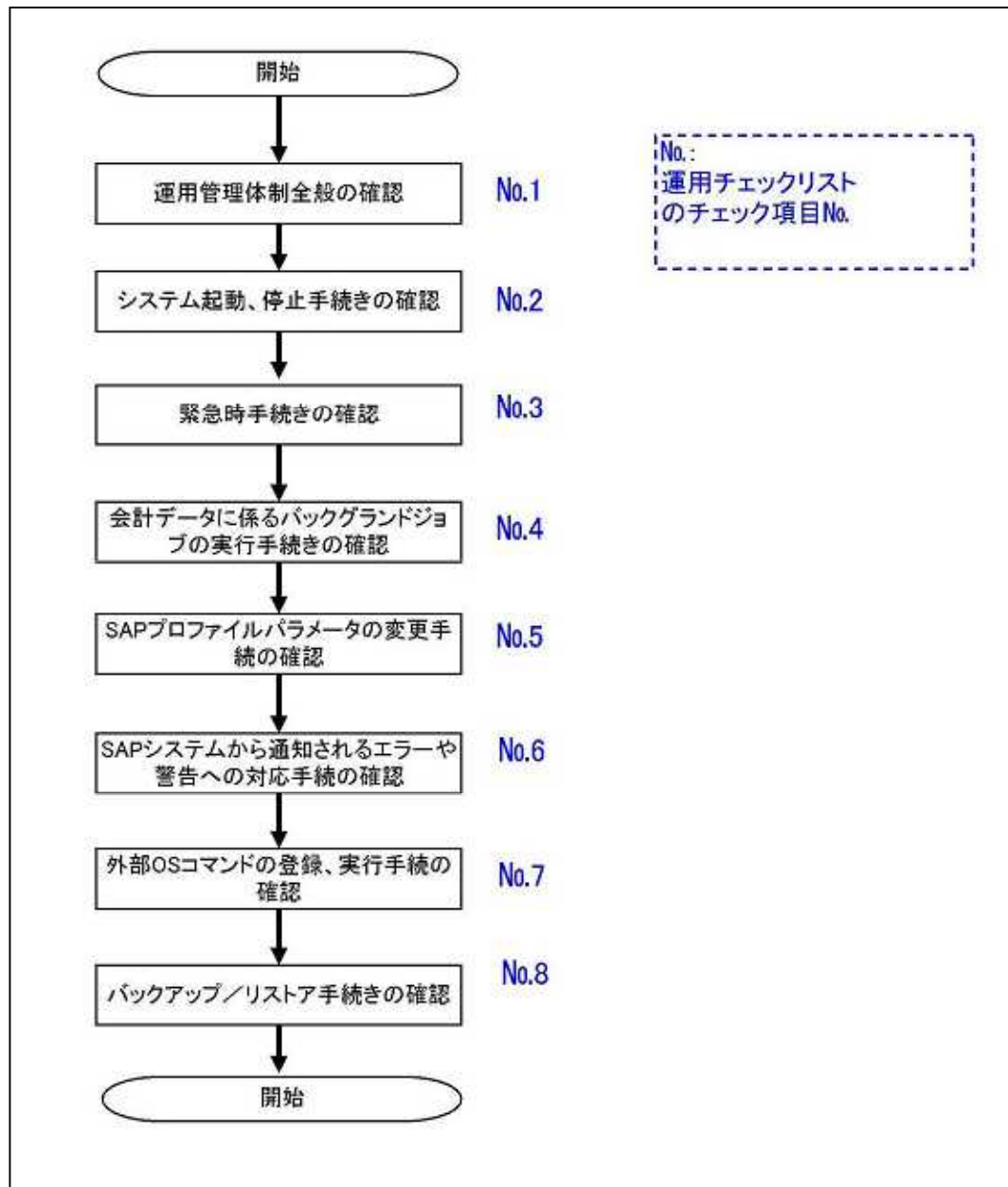
【運用状況評価】

運用状況評価では、区分が「運用」及び「モニタリング」のチェック項目について、評価対象期間中のコントロール発生状況（母数）に応じてサンプリングを行い、証憑を閲覧して評価する。

なお、「運用の作業者の権限」および「情報セキュリティインシデント」に関する評価はアクセスコントロールの監査チェックリストで扱っているので、必要に応じて参照のこと。

運用の監査手順（フロー）

図表 4. 4-2



5 用語集

SAP ERP 監査用語集

図表 5-1

用語	説明
ABAP	Advanced Business Application Programming Language SAP 社が開発したアプリケーション開発用プログラミング言語。 ABAP 言語の特長は次のとおり。 ・インタプリタ型言語に属するが、処理速度の向上をはかるため、中間言語を自動的にコンパイルする。言わば、インタプリタ型言語とコンパイル言語の「良い所取り」をしたようなアプリケーション開発用言語である ・COBOL に似た体系を持ち、短期に習得でき、生産性が非常に高い言語である ・マウスによる画面指定やファンクション キーによるイベントを簡単に処理できる(イベント指向) ・ABAP ワークベンチを使って、生産性および品質の高いアドオン開発を行うことが可能 ・従来型のコーディングも、オブジェクト指向のコーディングも可能 (補足) トランザクション実行中に、(そのトランザクションで使用している)ABAP プログラムを参照することができる。 SAP メニュー : システム>ステータス>プログラム名をダブルクリック → ABAP ワークベンチ Advanced Business Application Programming. The SAP programming language.
ABAP-OO	ABAP Object-Oriented オブジェクト指向プログラミングに対応した ABAP。 Component of the ABAP programming language that allows object-oriented programming on the basis of classes and interfaces.
ABAP エディタ	ABAP Editor ABAP プログラムのコーディング、テスト、変更のためのツール(エディタ) The ABAP Editor enables you to create, test and change ABAP programs, function modules, screen flow logic and logical databases. The ABAP Editor provides functions to support program development, as well as normal text operations such as insert, find, and replace. You can use the ABAP Editor in the following modes: ▪ Editor control mode ▪ PC mode with line numbering ▪ PC mode without line numbering ▪ Command mode
ABAP クエリ	→ SAP Query A tool that allows users who have no knowledge of the ABAP programming language to define and execute their own reports. To determine the structure of reports in SAP Query, you just have to enter texts, and select fields and options. If necessary, you can edit lists using Drag&Drop and the functions in the available toolbars. → アドホッククエリ
ABAP ディクショナリ	ABAP dictionary SAPシステムのメタデータ管理簿。プログラム、画面、テーブル、データエレメントなど「SAP システムリポジトリオブジェクト」の情報(メタデータという)を管理するツール/収納庫である。例を挙げると、プログラムのメタデータには、開発者、開発日時、サイズ、使用するテーブルなどが該当する。プログラムの開発時や実行時には、ABAP インタプリタは、ABAP ディクショナリに記録されているメタデータを必ず参照する。このとき、データテーブルなどのプログラムの関連項目に変更がないかチェックが働く。関連項目に変更があると、プログラムは自動的に再コンパイルされ整合性が確保される。 A directory containing data. An ABAP dictionary contains the following information: ▪ Description of all application data for an enterprise ▪ Relationships between the application data Use of the application data in programs and screen templates ▪ The descriptive data for the ABAP Dictionary is also known as meta data since it represents data about data.

ABAP プログラム	ABAP program ABAP プログラミング言語で記述されているプログラム。ABAP プログラミングは、2つの種類に分類できる。1つは対話型でデータベースの更新を行う「ダイアログプログラム」。このタイプのプログラムは、トランザクションコードを割当て、トランザクションとして呼出す。トランザクション登録は、SE93で行う。第2はデータベースから情報を読み出してレポートを生成する「レポートプログラム」これはデータベースの更新は行わないのが基本。SAP 標準レポートプログラムの ID は一般的に文字 'R' から始まり、2文字目がコンポーネントを表している。例: RFBILL00 は財務会計 (FI) のレポートプログラム。BS/PL を出力する。このタイプのプログラムを「レポート」と呼ぶ。「レポート」は直接呼出すことも、トランザクションを割当て、トランザクションとして呼出すこともできる。
ABAP ワークベンチ	ABAP workbench ABAP ワークベンチは、一般に言う CASE (Computer Aided Software Engineering) 環境の、SAP 版である。アドオン開発の上流工程から下流工程までの開発作業を首尾一貫して支援し、アドオンプログラムの生産性および品質の向上に寄与する。 SAP システムには開発担当者が使用する開発ツールの一式が組み込まれている。 尚、「ワークベンチ」とは「作業台」を意味することばである。 Integrated graphical development environment in the SAP System. The ABAP Workbench allows you to develop, modify, test, and manage client/server applications written in ABAP. The ABAP Workbench tools enable you to: • Write ABAP code • Create user interfaces • Check applications for errors • Create and access database information • Create Internet services
ACID 属性	Atomicity, Consistency, Isolation および Durability の頭文字をとった略語 トランザクション処理における基本概念を表す言葉。 • Atomicity: 原子性 = トランザクションの状態が確定すること • Consistency: 一貫性 = データの整合性が保たれていること • Isolation: 独立性 = 各トランザクションの変更が他のトランザクションデータに影響を与えないこと • Durability: 耐久性 = 一度確定したトランザクションは、その後に障害が起きても影響を受けないこと。
ALOG	このログファイルには、移送ディレクトリで実行される全移送ステップの個々のリターンコードが記録される。デフォルトのファイル名が ALOG であることから、通常 ALOG と呼ばれる。 ファイル ALOG は、移送ディレクトリのサブディレクトリ log に格納され、ファイル名は、移送プロファイルで定義することができる(移送ディレクトリのサブディレクトリ bin 内のファイル)。 デフォルト値は ALOG\$(year)\$(week)。2文字ずつ現在の年と現在の週を示す。 → SLOG
APPC	Advanced Program to Program Communication Protocol developed by IBM as part of its Systems Network Architecture (SNA). The protocol is designed to be enable application programs running on different computers to communicate with each other and exchange data.
BAPI	Business Application Programming Interface SAP ビジネスオブジェクト(例: 受注伝票、得意先、品目など)を操作するために定義されたアプリケーション・プログラム・インタフェース。CORBA、DCOM と互換性をもつ。 SAP ビジネスオブジェクトに操作(登録、変更、削除など)を行う時は、BAPI を利用することが推奨されている。 BAPI で ビジネスオブジェクトを操作するには、要素を指定する。 • ビジネスオブジェクト ID (例: 受注伝票・得意先など) • メソッド (例: 登録・変更・削除など) • 属性 (例: 伝票番号・得意先コードなど) を指定する → API A standardized programming interface that facilitates external access to business processes and data in the SAP System. You define Business Application Programming Interfaces (BAPIs) in the Business Object Repository (BOR) as methods of SAP business objects or SAP interface types. BAPIs offer an object-oriented view of business components in the SAP System. They are

	implemented and stored as RFC-enabled function modules in the Function Builder of the ABAP Workbench.
BAPI ActiveX	ActiveX control that enables external applications to access business functions in the SAP System by calling BAPIs through OLE Automation. OLE-enabled client programs access proxy objects, which are instances of SAP business objects managed by the BAPI ActiveX control. These proxy objects correspond to real SAP business objects stored in SAP's Business Object Repository (BOR). The actual details of the process are invisible to the client program, because the data structures exported from the SAP System through the BAPI ActiveX control are encapsulated in objects.
BAPI ブラウザ	The BAPI Browser displays all the business objects, for which BAPIs have been implemented. トランザクションコード: BAPI
BC	Basis Component (ベースコンポーネント) リリース 46D 以降無効 SAP システムは、「アプリケーション層」「ベース層」および「プラットフォーム層」から構成されている。 「ベース層」は、「アプリケーション層」と「プラットフォーム層」の間に位置するので、「ミドルウェア」と呼ばれる事がある。 「アプリケーション層」は、FI、CO、SD、MM、PP などのアプリケーション機能を提供するレイヤを指す。 「プラットフォーム層」は、SAP システムが移動するために必要な環境を提供するレイヤで、オペレーティングシステムやデータベース管理システムなどから構成される。 「ベース層」の役割を分類すると、次の三つになる。 ① SAP 共通インタフェースの提供。すなわち移植性の保証 ② 開発環境の提供 ③ 運用管理支援機能の提供 注意: 「基本コンポーネント」と訳してはいけない。
BC	Business Connector: ビジネスコネクタ A middleware application based on the B2B integration server from webMethods. The SAP Business Connector enables both bi-directional synchronous communication and asynchronous communication between SAP applications and SAP and non-SAP applications. The SAP Business Connector makes all SAP functions that are available via BAPIs or IDocs accessible to business partners over the Internet as an XML-based service. The SAP Business Connector uses the Internet as a communication platform and XML or HTML as the data format. It integrates non-SAP products by using an open, non-proprietary technology.
BDC	Batch Data Communication バッチインプットで使用するデータセットを BDC と呼ぶ。 バッチインプットは、SAP システムの画面入力をエミュレーションする機能である。すなわち、人間の代わりにバッチインプットが画面入力を行う。画面入力エミュレーションを可能にするため、レガシシステムデータを変換し、BDC データ形式のファイルを作成しなければならない。 BDC データは、移行対象データが、 ・どのトランザクションの ・どのプログラムの ・どの画面の ・どの項目に該当するか、 示す情報である。「バッチインプット」機能は、BDC データの内容に従って、トランザクションを呼び出す。次に、人間が画面入力をするのとおなじように、画面上にデータを設定する。データにエラーが無ければ、トランザクションを実行する。 補足: レガシシステム マイグレーション ワークベンチ (LSMW) を使って、旧システムのデータを BDC データに変換するプログラムを開発することができる。 → LSMW
CCMS	Computing Center Management System 「コンピュータセンタ管理システム」。SAP システムの稼動状況の監視、起動と停止、バックグラウンド・ジョブのスケジュール、システムプロファイルの管理、動的負荷分散など、SAP システムの運用管理に必要な幅広い機能を提供する。 CCMS provides integrated tools for the monitoring and administration of SAP system landscapes. It covers the following task areas: ・ System monitoring over the whole landscape ・ Determining and displaying statistical data ・ System management (e. g. starting and stopping of SAP systems, ・ configuration, printing, background processing, resource management, database administration)

	メニューは、ツール＞CCMS
CCSV	Customizing Cross System Viewer(カスタマイジング・クロスシステム・ビューア) 二つのシステム間のカスタマイジング内容を比較するツール。リリース 4.6 以降で提供されている機能。
CMS	Contents Management Service ユーザの要求に応じて Web ページを柔軟に生成する動的な Web サイトの構築や保守を効率化するコンテンツ管理プログラム
CPI-C	Common Programming Interface-Communication システム間およびプログラム間での同期通信の基礎となるプログラミングインタフェース。IBM メインフレーム時代からのプロトコル Standardized interface for system-wide communication between programs. (Common Programming Interface-Communication). The protocol can be divided into four areas: • Session setup • Session control • Communication • End of session
CTO	Change and Transport Organizer(移送/修正オーガナイザ) 死語。 46C 以降、移送ワークベンチに統合されている。 A set of tools in the SAP System for managing development projects in the ABAP Workbench and in Customizing, and for preparing and managing transports between SAP Systems.
CTS	Change & Transport System (BC-CTS): 移送/修正システム A set of tools in the SAP System for managing and transporting ABAP Workbench and Customizing changes made in systems in the SAP System landscape and distributed between these systems. 「Correction & Transport System」は死語。 SAP 標準用語では「Change & Transport System」が正しい用語。
CUA	Central User Administration: 集中ユーザ管理 SAP を複数のサーバで運用(分散環境)する際のユーザー管理を支援するソリューション。ユーザ登録、マスタデータ変更、権限変更を(ALE を使って)一括集中管理する機能を提供する。(例) SAP、APO、CRM などといった複数の SAP 製品を統合して利用する場合など。 具体的な実現機能に次のようなものがある。 ・一つのセントラルシステム(CUA サーバ)から集中ユーザ管理ランドスケープユーザでのクライアントのユーザを管理する(移送のランドスケープとは別物) <注> 通常 CUA サーバは、最もユーザ数が多いコンポーネント、例えば、SAP(Enterprise)上におかれる) ・セントラルシステムとローカルシステムの間でのユーザ情報の不整合をチェック ・ユーザマスタデータ、ロールや権限の割当情報(割当のみ)、ユーザロック情報を配信する The maintenance of users in a central system. A system group includes several SAP systems with several clients. The same users are often created and the same roles assigned in each client. Central User Administration is designed to perform these tasks in a central system and distribute the data to the systems in the system group.
DDIC	「ディーディック」と読む。SAP*とならび、SAP のスーパーユーザの一つ。ユーザ DDIC は、インストール、ソフトウェアロジスティクス、および ABAP ディクショナリに関する特権を持ったユーザである。SAP システムのインストールの際、ユーザマスタレコードはクライアント 000 および 001 で登録される。 DDIC ユーザを誤用から保護するため、クライアント 000 と 001 で DDIC の初期パスワード "19920706" を変更して置く必要があるが、ユーザ DDIC はシステムでの特定のインストール作業や設定作業に必要なので、削除してはならない。 → SAP*
DFD	Data Flow Diagram(データフローダイアグラム) 企業組織における業務の流れを記述するための表記法の一つ。
DIA	Dialog work process 対話型ワークプロセス。SAP GUI から依頼される対話型処理依頼を実行する。
Dynpro	Dynamic Program 「対話型プログラム」のこと。Dynpro は次の3つの構成要素からなる。 ・ユーザとの間で情報の受け渡しを行うための対話画面(画面の識別 ID を Dynpro 番号と呼ぶ), ・対話画面を表示する前に呼び出され実行されるプログラムモジュールである PBO(Process Before Output)。PBO では、一般にデータ項目の初期化や画面に表示するデフォルト値の設定などを行う。 ・画面から入力されたデータの処理を行うプログラムモジュールである PAI (Process After Input)。

	PAI は、ユーザの入力が終わった後に呼び出される。
Exit 機能	モディフィケーションを行うことなしに SAP 標準機能を拡張するための機能。Exit 機能は、予め定められたタイミングでユーザのアドオンプログラムを呼び出す仕掛けである。EXIT を使用することを機能「拡張」と呼ぶ。 注意：リリース 4.6A 以降の新規用語は“ビジネスアドイン” カスタマ Exit には4つのタイプがある。いずれの Exit も、アドオンプログラムを標準プログラムに組み込むための留め金の役割を果たす。 (1)メニュー Exit 標準 SAP アプリケーションのプルダウンメニューに明細を追加するための EXIT。このメニュー明細を使用すれば、独自の画面をコールしたり、アドオンアプリケーションをトリガすることなどを行うことができる。 (2)Dynpro Exit SAP アプリケーションの画面に項目を追加するための EXIT。SAP は、標準 SAP 画面内に特別な従属画面領域を配置し、標準 Dynpro の制御ロジックからユーザの従属画面をコールすることによって、Dynpro Exit を登録する。 (3)汎用モジュール Exit SAP アプリケーションに機能を追加するための EXIT。 予め、標準 SAP プログラム内にユーザが追加した機能(汎用モジュール)をコールする命令 ”CALL CUSTOMER-FUNCTION ‘ 001 ’ ” が定義されている。 (4)キーワード Exit ABAP デictionary内に定義されている「データエレメント」に、文書を追加するための EXIT。この文書はユーザが「？」ボタンまたは F1 を押したとに表示される「項目ヘルプ」 トランザクション:CMOD Program interface at which additional methods can be inserted without modifying the original object. Java component comparable to Business Add-Ins, User Exits, Customer Function Calls.
LSMW	Legacy System Migration Workbench レガシイ(旧)システムのデータを、SAP システムに移植するためのプログラム開発を支援する環境。詳細は、LSMW 日本語環境資料(SAP ネット)参照。 An SAP system tool that supports one-time and periodic data transfers from external systems to SAP systems. The Legacy System Migration Workbench facilitates the conversion of data to the necessary format. Technologies supported include Batch Input, Call Transaction, Direct Input, BAPIs, and EDI. The Legacy System Migration Workbench is only available as an add-on. Additional data transfer tool: Data Transfer Workbench (DX-WB).
PAI	Process After Input オペレータが Dynpro 画面に入力を終えた後(=エンターキー押下時)に実行する Dynpro プロセス。
PID	Parameter ID 該当 PID に任意の値を割り当てることにより、特定の画面項目にデフォルト値をセットすることができる。 例えば、得意先コード、仕入先コード、販売組織など。 特定の項目の PID を知るには、①その項目にカーソルを設定し、②ヘルプアイコンまたは、F1 キーを押し、③技術情報を表示する。
QA システム	品質保証システム。SAP システムランドスケープを構成するシステムの一つで、本番稼働前の総合テストを実施するためのシステム。
RFC	Remote Function Call(リモートファンクションコール) CPI-C をベースにした SAP インタフェースプロトコル。 これにより、システム間通信プロセスのプログラミングを簡略化することができる。RFC を使用して、事前定義された機能をリモートシステムや同一システム内部で呼び出して実行することができる。 →RPC ファンクション ID、RFC 宛先、引数(Export,Inport)を指定して、リモートホスト上のプログラムを実行し、処理結果を受け取ることができる。 Call of a function module that runs in a different system (destination) from the calling program. Connections are possible between different SAP systems and between an SAP system and a non-SAP system. In non-SAP systems, instead of function modules, special programmed functions are called, whose interface simulates a function module. We distinguish between synchronous, asynchronous, and transactional function calls. The called system is accessed via the RFC interface. → tRFC

RFC 宛先	Remote Function Call(リモートファンクションコール)宛先 RFC で指定した機能を実行するリモートホスト(一般的には SAP システム)を定義したもの。リモートファンクションコールを実行する時に RFC 宛先指定する。 RFC の定義を行うトランザクション: SM59(RFC 宛先)
SAINT	SAP Add-On Installation Tool SAP アドオンインストールツール Tool that allows you to install and upgrade add-ons directly from the SAP System
SAP GUI	SAP Graphical User Interface SAP システムの利用者が、(グラフィカルなユーザインタフェースを介して)SAP システムと情報交換するために私用するプログラムを指す。SAP GUI はクライアント機(一般にパソコン)上で動作する。SAP GUI を使用することにより、SAP 使用者は簡単なマウス操作で、複雑な機能を実行したり、処理結果をグラフ変換することが可能になる。SAP GUI は次の三種類が提供されている。 ①Windows 版 ②JAVA 版 ③HTML 版 SAP system software component on the presentation server. Represents the SAP-specific GUI of the ABAP-based application server applications and supports additional functions on the presentation server, such as GUI controls or OLE automation.
SAP GUI	SAP GUI SAP system software component on the presentation server. Represents the SAP-specific GUI of the ABAP-based application server applications and supports additional functions on the presentation server, such as GUI controls or OLE automation.
SAP LUW	SAP Logical Unit Work(論理ユニットワーク) 論理的なひとかたまり(一連)の処理単位。SAP では、一つのトランザクション処理を、対話処理を実行する LUW とデータベースの更新を行う LUW に分割して処理する。 LUW は、SAP ベースシステム非同期更新処理を実現するための基本概念である。 SAP LUW : Logically connected unit of dialog steps whose database changes are executed within a single database LUW. SAP LUWs are realized using bundling techniques in which update function modules or subroutines are registered in different work processes and executed by a single work process. A SAP LUW is ended using the Open SQL statement COMMIT WORK. Changes within a SAP LUW can be undone using the Open SQL statement ROLLBACK WORK.
SAP Web ディス パッチャ	SAP Web dispatcher (Internet Communication Manager (BC-CST-IC)) The SAP solution for load balancing of Web requests. If more than one instance of the SAP Web Application Server is being used at any one time, the SAP Web dispatcher accepts requests from the browser and forwards these to the application server that currently has the most capacity. The choice of application server is based on information from the SAP Message Server. Administration is thus made much easier, as there is only one point of entry (IP address, HTTP port, and so on) to the SAP system.
SAP*	「サップアスター」と読む(SAP*を”エスエーピーアスタ”とは読まず”サップアスター”と読むのが慣例): SAP システムのスーパーユーザ ID (=全ての機能を実行可能なユーザ ID) SAP*は SAP システムのスーパーユーザであり、強力な権限を持つが、初期パスワードは公開されている。 SAP* には次の 2 種類が存在する。 ① ユーザマスタ上に、レコードが存在しない(ハードコーディングされた)SAP*。パスワードは”PASS”。②で説明する、SAP*が登録された時点で、この SAP*は無効化されるが、削除されると、再び有効化される。従って、このタイプの SAP*は、プロファイルパラメータを設定して無効化しておく必要がある。 ② ユーザマスタ上に、レコードが存在する SAP*。このタイプの SAP*のパスワード”06071992”を直ちに、特定のものだけが知る文字列に変更する必要がある。 SAP*は他のユーザ ID と同様、クライアント依存であるので各クライアントことに対応が必要である。 →DDIC
SAPconnect	SAP システムと他社の非 SAP 通信システムとの標準通信インタフェース。 FAX、電子メール(SMTP)、X.400、ポケットベル(SMS)などをサポートする。 The RFC interface for integrating external communications with the SAP System. SAPconnect enables third-party vendors to connect their communication servers to the SAP System. The following communication methods are supported: ・Fax

	•Internet (SMTP) •X.400 •Paging (SMS) •R/3 to R/3 •Printer
SAPExchange コネクタ	MS Exchange Server と SAP システムをリンクさせるコンポーネント。
SAP クエリ	SAP システムが提供するレポート生成ツールの一つ。SAP クエリを利用すると、ABAP をコーディングせずにエンドユーザ自身が必要なレポートを作成できる。 具体的には、レポート出力したい項目を選択し、ソートキーや集計キーを指定するだけでレポートを作成することができる。 三種類のレポート形式(基本一覧、統計一覧、およびランク一覧)を選択することができる。 「ABAP クエリ」ともよぶ。 A tool that allows users who have no knowledge of the ABAP programming language to define and execute their own reports. To determine the structure of reports in SAP Query, you just have to enter texts, and select fields and options. If necessary, you can edit lists using Drag&Drop and the functions in the available toolbars. →アドホッククエリ
SAP スクリプト	SAPscript レポートの書式(=フォームオーバーレイ)を定義するためのスクリプト。 SAP が提供する書式の多くは SAP スクリプトで記述されている。SAP スクリプトを使って書式を定義する利点は、プリンタに依存しない定義が可能なことである。最近では、SSP として提供されている書式定義ツールを利用して、導入企業固有の書式をアドオンするケースが多い。 A tool for text management and form printing. SAPscript consists of the following components: •An editor for entering and editing text •Styles and forms for designing the print layout •A composer, which is the central module for output formatting •A programming interface for integrating SAPscript components in your own application programs and programming the output using forms •Various database tables for storing texts, styles and forms
SAP ソフトウェア変更登録 (SSCR)	SAP Software Change Registration SAP システムにリポジトリオブジェクトを登録・変更するには、プログラマ(作業責任者)を SAP に登録しなければならない。さらに、SAP 標準リポジトリオブジェクトを変更する場合、該当オブジェクトの変更キーを SAP から取得しなければならない。この登録作業および、登録システムを SSCR と呼ぶ。SSCR はネットワーク経由で行う。 Procedure that registers modifications to SAP Repository objects and thus provides an overview. SAP Software Change Registration does not register SAP matchcodes and tuning measures (such as the creation of database indexes and buffers).
SLO	System Landscape Optimization
SLOG	このログファイルには、R/3 システムで実行される全インポートの情報が記述される。デフォルトのファイル名が SLOG であることから、通常 SLOG と呼ばれる。 ファイル SLOG は、移送ディレクトリのサブディレクトリ log に格納されます。ファイル名は、移送プロファイルで定義できる(移送ディレクトリのサブディレクトリ bin 内のファイル)。 デフォルト値は SLOG\$(year)\$(week).\$(system) で、2 桁ずつ現在の年と現在の週を示す。 → ALOG
SPP	service parts planning サービスパーツ計画
SQL	Structured Query Language リレーショナルデータベースシステム用の構造化問い合わせ言語。 SQLを使用することで、テーブル(表)の定義やデータ操作、関係演算など、リレーショナルデータベースに関するほとんどの操作を機械可読なテキストとして記述できる。SQL は一般的な言語だが、実際は各データベースシステム固有の機能などが追加されているため、各データベースメーカー毎に SQL が拡張されている。よって、データベースの製品毎に SQL も異なる仕様を持っているのが現状である。
TMS	Transport Management System(移送管理システム) 移送を支援する管理システム

	→移送
TMS 品質保証機能	TMS 品質保証とは、開発成果物を後続システムにデリバリする前に品質保証システムで承認を必須とし、本稼働システムの品質と可用性を向上させる機能。承認手順が有効化されたシステムは、QA システムと呼ばれる。承認手順を有効化すると、QA システムで移送依頼ごとに QA 承認ステップがすべて処理され、各依頼が承認された場合にだけ、成果物がデリバリシステムに転送される。却下された依頼は、QA システムのデリバリシステムにインポートされない。
TPPARAM	TP global Parameter file
UDDI レジストリ	UDDI レジストリとは、ネットワーク上に存在する Web サービスの情報を検索するためのディレクトリ・サービス。
UME	SAP User Management Engine Java-based user management component that features centralized user management, Single Sign-On, and secure access to distributed applications
VB	Verbuchen(独)=Update(英)=更新(日本語)
WAS	Web Application Server →Web AS “WAS”は、無効同義語
WBO	Work Bench Organizer:ワークベンチオーガナイザ Tool for managing central and decentralized development projects in the ABAP Workbench. The Workbench Organizer is part of the Change and Transport Organizer (CTO). →CTO
Web AS	Web Application Server 従来、ベースと呼ばれる部分を拡張したもので、NetWeaver アプリケーション開発、実行基盤（プラットフォーム）である。WAS は、ABAP 資産を継承すると共に、HTTP、XML などのインターネット上の資源を統合することを可能にする。 WAS is The SAP NetWeaver application platform. SAP Web Application Server supports native Internet technology such as HyperText Transfer Protocol (HTTP), eXtensible Markup Language (XML), as well as the Java and ABAP programming languages. SAP Web Application Server facilitates the development of Web applications with server-side scripting technologies, provides a scalable and reliable Web application infrastructure that delivers Web services at high performance, ensures that an e-business solution is always online, and supports Web access via a Web browser and a range of mobile devices.
WIF	Work Flow Information System(ワークフロー情報システム)
WP	Work Process(ワークプロセス) →ワークプロセス
アーカイブオブジェクト	Archive Object アーカイブの処理単位となる論理オブジェクトで、具体的には、受注・発注伝票、会計伝票、仕入先・得意先・品目マスターデータなどである。アーカイブが正常に完了すると、専用に生成された削除プログラムを使って論理オブジェクトを削除することができる。
アーカイブリンク	Archive Link アーカイブリンクは、SAP アプリケーションと外部コンポーネントとの間の通信インタフェースで、BC コンポーネントに組み込まれている。アーカイブリンクが備えるインタフェースは、次の三項目から構成される。 ①ユーザインタフェース ②SAP アプリケーションとのインタフェース ③外部コンポーネントとのインタフェース(アーカイブシステム、ビューアシステム、スキャンシステムなどとの連携を支援する)
アドイン	Add in :アドイン A location in a program defined by the developer where software recipient layers such as industries, partners and customers can insert additional code without modifying the original object. Business Add-Ins enable you to distinguish between enhancements that can have no more than one implementation and those that can be actively used by any number of customers at the same time. You can also define Business Add-Ins that depend on a filter value. You can create Business Add-Ins at every level of a multi-level system infrastructure. You edit Business Add-Ins in the BAdI Builder.
アドオン	add on SAP 標準オブジェクト(プログラム、テーブル定義など)を変更すること無く、プログラムやテーブルあるいはテーブル項目を追加すること。 注意:命名規則を守ること。多くの場合、アドオンしたオブジェクトの名前は“Y”または“Z”で始める

	規則になっている。→モディフィケーション
移送	Transport SAP オブジェクト(ABAP プログラム、テーブル定義、カスタマイジングパラメータのセットなど)を他の SAP システムに移すこと。(厳密には、これを「システム間移送」と呼ぶ。) また、あるクライアント上の「カスタマイジングパラメータのセット(変更依頼で管理される)」を同じ SAP システム上の他のクライアントに移すこと。(厳密には、これを「コピー」と呼ぶ。この場合「システム間移送」と区別するため「クライアント間移送」と呼ぶとよい。) →変更依頼 The transfer of SAP System components from one system to another. The components to be transported are specified in the object list of a transport request. Each transport consists of an export process and an import process: The export process reads objects from the source system and stores them in a data file at operating system level. The import process reads objects from the data file and writes them to the database of the target system. The SAP System maintains a transport log of all actions during export and import.
移送/修正オーガナイザ	Change and Transport Organizer (CTO) ABAP 開発作業、カスタマイジング作業および移送を管理するツールの総称を指す。 カスタマイジングオーガナイザ(トランザクション=SE10)、ワークベンチオーガナイザ(トランザクション=SE09)、移送オーガナイザ(トランザクション=SE01)から構成される。46C からは、これらのツールは移送オーガナイザ(SE01)に統合されている。 A set of tools in the SAP System for managing development projects in the ABAP Workbench and in Customizing, and for preparing and managing transports between SAP Systems.
移送/修正システム	→CTS
移送依頼	Transport Request リリースされエクスポートされた変更依頼を移送依頼と呼ぶ。 移送依頼には、開発・変更プロジェクトの成果物が記録されている。移送依頼は、移送ディレクトリ上に OS ファイル形式で置かれ、一つの SAP システムから別のシステムへプログラムやカスタマイジングパラメータを移すのに使用される。 Document for copying corrections between different system types. A transport request records released corrections. When the request is released, the transport is performed. For example, you can transport corrections from an integration system to a consolidation system.
移送オーガナイザ	Transport organizer リリース 46C からの用語 A tool for managing centralized and decentralized ABAP Workbench development projects and Customizing projects. (トランザクション=SE01) 次の機能を提供する ・個別照会: 依頼番号またはタスク番号の直接入力 ・コピーの移送および再編成の照会/編集 - コピーの移送 - パッケージの変更を伴わない再編成 - パッケージの自動変更を伴う再編成 - 全パッケージの再編成 (移送レイヤが自動で変更される) ・オブジェクト一覧の照会/編集 ・クライアント移送の照会 ・デリバリー移送の照会/編集 トランザクションコード: SE01 →カスタマイジングオーガナイザ
移送可能変更依頼	transportable change request リポジトリオブジェクトおよびクライアント非依存オブジェクトを管理するための「変更依頼」。 Change request that is transported to the target system defined by the system settings after release. →カスタマイジング依頼、ローカル変更依頼
移送グループ	transport group 移送ディレクトリを共有する SAP システムのグループ。 All SAP Systems connected by transport routes. A system group can include several transport groups or transport domains. While the transport

	domain is an administrative unit, and the transport group a technical unit, the system group is a logical unit.
移送ディレクトリ	Transport Directory SAP システム間で移送する全データを一時的に置くための OS ディスク領域。 移送ディレクトリのパスは、UNIX では、デフォルトパス: /usr/sap/trans。Windows NT では、デフォルトパス: %\$\$(SAPTRANSHOST)%sapmnt%trans であり、ドメイン名サーバ上の移送ホストをエイリアス SAPTRANSHOST で定義する必要がある。 移送ディレクトリ下のサブディレクトリは以下のとおり。 ・ bin: tp と TMS の設定ファイル (tp: TP_<DOMAINNAME>.PFL、TMS: DOMAIN.CFG) ・ data: エクスポートされたデータ ・ olddata: アーカイブまたは削除される旧エクスポートデータ ・ log: 移送ログ、トレースファイル、統計 ・ actlog: 全タスクと全依頼のアクションログ ・ buffer: 各システムの移送バッファ。インポートする移送を指定する。 ・ cofiles: 移送タイプ、オブジェクトクラス、必要なインポートステップ、後処理用 Exit コードに関する情報が格納されたコマンドファイルまたは変更依頼情報ファイル ・ sapnames: 各 SAP ユーザの移送依頼についての情報 ・ EPS: 先行修正とサポートパッケージのダウンロードディレクトリ ・ tmp: 一時データとログファイル A directory that manages all data to be transported between SAP systems.
移送ドメイン	transport domain 移送ドメインは、移送を一元管理するすべての SAP システムで構成される。移送ドメインを構成する SAP システムの中から 1 つの SAP システムを選び「移送ドメインコントローラ」として指定する。 All SAP Systems that are managed jointly by the Transport Management System. All systems in a transport domain have the same settings as the Change and Transport System. →移送ドメインコントローラ
移送ドメインコントローラ	transport domain controller 移送ドメインコントローラは、移送ルートや RFC 接続の設定など、移送ドメイン全体に関する設定を管理する。ドメインコントローラには以下の条件を満たす SAP システムを選択する必要がある ・ 高い可用性 ・ 高いセキュリティレベル ・ 高い保守レベル (補足) 通常は、本移動システムまたは品質保証システムをドメインコントローラとして設定する。ドメインコントローラのシステム負荷は小さく、負荷が増えるのは TMS 設定変更時のわずかな時間だけである。 デフォルトの移送ドメイン名は DOMAIN_<SID> (<SID> はドメインコントローラのシステム ID)。 ドメインコントローラとしての役割をもつ SAP システムが移動していないと、TMS 設定を変更することはできない。このため SAP では、必要に応じてドメインコントローラの機能を代行できるバックアップドメインコントローラを設定することを推奨する SAP System in which the transport route configuration is maintained centrally for all systems in the same transport domain.
移送ルート	Transport Route ランドスケープを構成する SAP システム(「開発システム」「品質保証システム」「本運用システム」)間の移送順序を指定したもの。移送ルートは、変更依頼のコンソリデーションシステムが終わった変更依頼のデリバリシステムとなる SAP システムを定義する。移送ルートは、コンソリデーションルートまたはデリバリルートのいずれかのタイプである。 標準的な 3 システムランドスケープの移送ルートは以下のとおり。 ① コンソリデーションルートは、開発システムと品質保証システムを接続する。自動的に作成される移送レイヤの名称は、Z<SID> (<SID> は開発システムのシステム ID) ② デリバリルートは、品質保証システムと本移動システムの間に作成される。 ③ 開発システムでは、コンソリデーションルートに対応する(標準)移送レイヤとリンクしているパッケージのオブジェクトに変更を加えた場合、その変更は変更依頼に記録され、品質保証システムを経て本移動システムに移送される。 SAP が提供するオブジェクト(=標準オブジェクトと呼ぶ)への変更は、変更依頼に「仮修正」属性のタスクとして記録される。この場合、移送レイヤとして“SAP”を使用することを除いて、他のオブジェクトの場合と同じ方法で移送することができる。 →コンソリデーションルート、デリバリルート
移送レイヤ	Transport Layer

	移送レイヤは、SAP リポジトリオブジェクトの開発/変更を実施する SAP システムおよび、該当オブジェクトの移送先システム（品質保証システムや本運用システムなど）を定義する。開発インテグレーションシステムインテグレーションシステム」と呼び、移送先システムをコンソリデーションシステム」と呼ぶ。 リポジトリオブジェクトは特定の「パッケージ」に属し、「パッケージ」に「移送レイヤ」が割り当てらる。従って、あるパッケージに属する全ての SAP リポジトリオブジェクトは、同一のインテグレーションシステム上で開発され、同一のコンソリデーションシステムに移送される。 A means of determining the integration and consolidation system for objects to be transported. A transport layer is assigned to each development class and thus to all objects in that class. The transport layer determines: In which SAP System developments or changes to Repository objects are made Whether objects are transported to other systems within the group when development work has been completed →パッケージ、移送ルート
一括移送	mass transport Transport where all requests queued for import are imported into the target system collectively.
一般出荷(GA リリース)	unrestricted shipment phase SAP システムのリリース（＝新リリースの提供）方針の一つ。すべての企業で、特定のリリースが利用可能になるフェーズ。 これに対し、ファーストカスタマシップメント(FCS)段階は、CA(Controlled Availability)すなわち限定出荷とも呼ばれ、特定の企業のみで利用可能なフェーズを表す。 Second delivery phase for a new software release. During this phase, all customers can obtain the new release. →ファーストカスタマシップメント(FCS)
インスタンス	Instance SAP インスタンスは SAP システムの開始と停止の単位。インスタンスの識別名称は、そのインスタンスが扱うサービスを示す文字と、コンピュータごとに固有のインスタンス番号で構成される。サービスには D、V、E、B、M、G、および S があり、それぞれダイアログ、更新、エンキュー、バックグラウンド、メッセージ、ゲートウェイ、スプールの各サービスを意味する。インスタンス番号の例： DVEBMGS00 用語「インスタンス」は、用語「アプリケーションサーバ」と区別せずに使用されていることも多い。多くの場合、「アプリケーションサーバ」と区別せずに使っても問題ないが、厳密には誤り。正しくは、「SAP システムの動作単位であり、起動と停止の単位となる、メモリやワークプロセスなどのリソースのグループ」でもある。 各インスタンスは「インスタンス プロファイル パラメータ」の値に従って起動・実行される。インスタンス プロファイル パラメータには、バッファサイズ、ワークプロセスの種類と数などが設定されている。一つの SAP システムは、一つまたは複数のインスタンス（一般には1つ）で構成されており、端末からの処理要求は、インスタンスによって処理される。 補足：“instance”は「例、実例、事実」などの意味をもつ言葉。オブジェクト指向プログラミングでは、あるクラスの定義をテンプレートにして、実際に作られたオブジェクトをインスタンス（実例）と呼ぶ。インスタンスはあくまで一つの例であるため、同じクラスに属する複数のインスタンスはそれぞれ異なった値（データ）を持ち得る。 An administrative unit that groups components of an SAP system that provide one or more services. These services are started and stopped at the same time. All components belonging to an instance are provided with parameters using a common instance profile. A central SAP System consists of a single instance that includes all the necessary SAP services. （補足1）上記インスタンスの他、SAP システムには ITS インスタンスをはじめ、様々なインスタンスが存在することに注意 （補足2）SAP システムのインスタンスと ORACL データベースでいうインスタンスとは意味が違ふことにも注意。
インスタンスプロファイル	instance profile Profile that contains application server-specific configuration parameters to complete the set values of the default profile. → プロファイルパラメータ、デフォルトプロファイル
インスタンスパラメータ	Instance parameter → インスタンスプロファイル
インターネットトランザクションサー	Internet Transaction Server →ITS

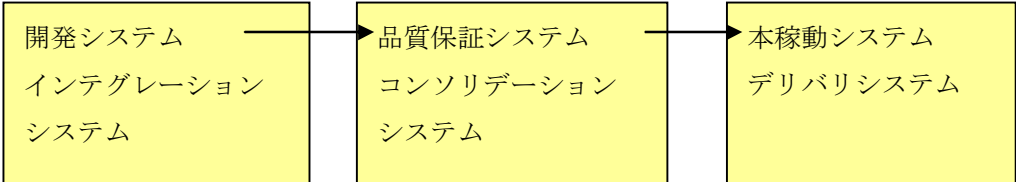
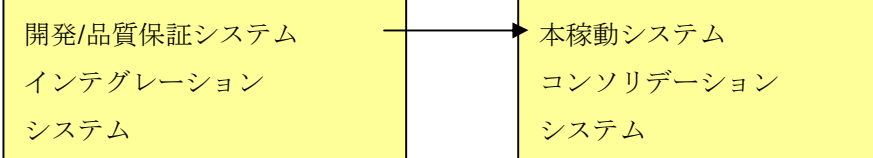
バ(ITS)	
インテグレーションシステム	integration system : インテグレーションシステム A system in the SAP System group where objects are usually developed and then transported to the consolidation system. Each Repository object is assigned to an integration system by its package (formerly development class) and transport layer. The integration system should consist only of separate test or development systems where SAP application programs are not being used in a production environment.
Web アプリケーションサーバ	Web Application Server →Web AS
エンキュー	enqueue 「ロック」と同義語。 SAP エンキューは、複数のユーザが同時に、同一オブジェクトを変更することがないように制御するための機能。いわゆる、排他制御機能を提供する。 SAP エンキューは、ABAP プログラムの中でエンキュー汎用モジュールによって明示的に設定され、デキュー汎用モジュールによって明示的に解除される。SAP エンキューは SAP トランザクション内の複数のステップにまたがって適用することが可能。SAP トランザクションが異常終了すると、残っていた SAP エンキューはベースシステムによって自動的に解除される。
オブジェクト指向プログラミング	Object Oriented Programing オブジェクト指向に基づいたプログラムの作成手法。 →ABAP O-O (ABAP Object-Oriented)
開発クラス(最新用語は「パッケージ」)	development class →パッケージ Enterprise リリースから用語「開発クラス」は「パッケージ」と表現するようになった。 特定のアプリケーション機能(例えば、売掛管理機能、買掛管理機能など)を構成する全リポジトリオブジェクト(プログラム、テーブル定義、画面定義、メニューなど)をグループ化して管理・移送するための仕掛である。 (注意: ロジスティックで使用する「クラス」とは全く別物) 移送が必要なリポジトリオブジェクトを登録する際は、必ず開発クラスに割り当てなければならない。開発クラスには、移送レイヤが割り当てられる。開発クラス単位でリポジトリオブジェクトの移送を行うことができる。すなわち、特定の機能を構成する全リポジトリオブジェクトをまとめて移送することが可能。 一度登録した開発クラスは、一般に永久に存続する。一方「変更依頼」は、アプリケーションの開発・変更プロジェクトの開始と共に作られ、リリースをおこなうことによって消滅する(=リリースステータスに変わる) → 変更依頼、移送レイヤ
開発システム	development system システムランドスケープ内で、アドオンとカスタマイジング作業を実施するシステム
開発者キー	developer key リポジトリオブジェクト(プログラム、トランザクション、テーブルなど)の変更を行うときに必要となる、ユーザ ID 毎のキー。リポジトリオブジェクトに対する登録・変更権限が割り当てられていても、開発者キーが割当られないと、リポジトリオブジェクトの変更はできないようにコントロールされている。 設定された開発者キーは、テーブル”DEVACCESS”に記録される。
外部セッション	external session SAP GUI によって管理される個々の画面をセッションと呼ぶ。 メインフレームの TSS(タイムシェアリングシステム)のセッションとは意味が異なるので注意。 論理的には、最大 6 個のセッションを同時に利用することができ、セッション毎に、固有のトランザクションを実行できる。 An instance of an SAP window within the SAP GUI on the application server. When you log on to the SAP System, the system opens an external session. You can then open up to five more sessions, which all behave like separate logons to the SAP System. The number of the current external session is displayed in the status bar.
拡張	Customer Enhancements カスタマ Exit を利用して SAP 標準プログラムにユーザ固有の機能を追加すること。 「拡張」は、SAP リポジトリオブジェクトを変更しないので「モディフィケーション」ではない。ABAP ワークベンチを使用して、「拡張」を実行することができる。拡張機能はリリースアップをおこなっても、原則、影響を受けない。 (注意) 広義には、「拡張」も「アドオン」といえるが、SAP では用語「アドオン」と「拡張」を区別して使用する。「アドオン」と「拡張」の違いは「カスタマ Exit を使用しているかどうか」にある。すなわち、カスタマ Exit を使ってアドオンをおこなうことを「拡張」という

	An adjustment to the standard SAP system, requested by the customer. SAP designs empty modification modules at particular points in the standard system where customer enhancements are anticipated. These modules, known as exits, can be filled with customer-specific logic. → 仮修正、Exit 機能、ビジネスアドイン
拡張移送制御	extended transport control 特定のクライアントを指定して移送を行う機能。拡張移送制御を有効化すると、対象グループ(注)または移送対象システムの「特定のクライアント」を移送対象に指定することができる。拡張移送制御を有効化しない場合、移送管理者が対象となるクライアントをインポート時に指定する必要がある。 クライアント依存の移送対象(オブジェクト)は、<SID>.<client>の形式で作成する。(例: WAJ.610) A function of the Transport Management System (TMS) that allows you to define client-specific transport routes and target groups. (注) 移送対象グループを使用して、クライアント依存の移送ルートを設定することができる。対象グループの名称は、先頭と末尾が“/”でなければならない。(例: /TQASGR/)
仮想 SAP システム	→ 仮想システム
仮想システム	virtual SAP System 計画したすべての SAP システムを同時にセットアップすることは、通常少ない。ほとんどの場合、システムランドスケープは段階的にセットアップされる。計画中の SAP システムを(移送ドメインの中の)「仮想 SAP システム」として設定することにより、システムランドスケープの移送ルートを TMS でモデル化することができる。 SAP System configured as a placeholder for an SAP System that has not yet been configured. You can define transport routes for virtual systems, and create and display the import queue.
仮修正	repair SAP リポジトリオブジェクトを、そのオブジェクトを開発したシステム(=マスタシステムと呼ぶ)以外で変更・修正した場合、その修正を「仮修正」と呼ぶ。すなわち、そのオブジェクトを開発したシステム(マスタシステム)以外でリポジトリオブジェクトを修正する行為は、すべてコピー版に対する修正であり、「あくまで、仮の修正」ということになる。 従って、SAP 導入企業のシステム上で、SAP 標準オブジェクトの変更を行う行為、すなわちモディフィケーションはすべて仮修正となる。 同様に SAP 導入企業のシステムランドスケープ内においても、アドオンしたプログラムを「開発システム」以外で変更・修正する作業は「仮修正」となる。 Repository objects that are changed in a system other than their original system are entered in repairs. Objects can be transferred from their original system by transports.
機能リリース	functionality release 最新用語は「CA リリース」。改善されたビジネスプロセスや新しいテクノロジーを SAP システムに導入するための SAP リリース。 機能リリースは、新機能をテストしたいと希望するカスタマの依頼に応じて出荷される。機能リリースは、本稼動システムで使用しないのが原則。 → GA リリース、修正リリース
クライアント	client 「クライアント」は「弁護依頼人、広告主」(広辞苑)や、「クライアント/サーバ」といった使い方があるので、誤解を招きやすい SAP 用語の一つである。 「クライアント」は、一つの ASP システムの中に設定された複数の「仮想的な一つのシステム」。 たとえば、一つの SAP システム内に、「パラメータ設定用クライアント」「テストクライアント」「トレーニング用クライアント」「サンド BOX クライアント」などを設定し、効率よく導入作業を進めることができる。論理的には、最大 1000 個のクライアントを設定することが可能。ただし、クライアントを増やすとその分だけ、データベース容量が増大する。 ・クライアントは下記メカニズムとして実装されている。 ①多くの、アプリケーション関連テーブルの第一キー項目は、クライアント番号である。(クライアント番号を第一キーに持つテーブルを、クライアント依存テーブルと呼ぶ)。ユーザがデータ(伝票情報やマスタ情報など)を登録すると、自動的に、ログオン時に指定したクライアント番号が第一キーの値としてレコードが記録される。 ②SAP プログラムからクライアント依存テーブルをアクセスすると、自動的に、アクセスキーにログオン中のクライアント番号が付与される。 ③従って、ユーザがアクセスできるデータは、ログオンしたクライアントに属するデータに限られる事になる。 ・クライアントとデータやユーザ登録の関係を整理すると

	①ABAP プログラム、リポジトリ定義(テーブルやデータ項目の定義など)および、一部のカスタマイジング パラメータはクライアント毎に管理されていないので「クライアント」を完全に独立した、個別の SAP システムとして扱うことはできない。クライアント毎に管理されていないデータを「クライアント非依存」または「システム依存データ」と呼ぶ。 ②クライアントごとにユーザ登録が必要である。 ③他のクライアントに移るためには、該当クライアントにログオンし直す必要がある。 ・一般的に、3 システムランドスケープを構成する各 SAP システムに、次のようなクライアントが設定される。 ①開発システム上: カスタマイジング用、アドオン用、単体/結合テスト用、サンド BOX(実験用)クライアントなど。 ②品質保証システム上: 統合テスト用、ユーザトレーニング用クライアントなど。 ③運用システム: 本稼動用クライアント(まれに「プレ本稼動用」クライアント)。 注意: 文脈によっては、「顧客」あるいは「クライアント/サーバ」の「クライアント」の意味で使われることがあるので注意 In commercial, organizational and technical terms, selfcontained units in an SAP system with separate master records and its own set of tables. 3 digit number E.g. 000, 001 and 066 One or more clients per SID.
クライアント/サーバシステム	Client/ Server System クライアント/サーバシステムは、「クライアント」及び「サーバ」と呼ばれる役割を持つ複数のコンピュータシステムから構成されるシステムである。 クライアントとは、処理を依頼する側を指し、サーバとは、クライアントからの処理依頼を実行する側を指す。 SAP システムは、3 階層のクライアント/サーバ方式を採用している。3 階層のクライアント/サーバ方式とは、情報システムを、3 つの層、すなわち、 ①「グラフィカルユーザインタフェースの提供」を行う「プレゼンテーションサーバ」層 ②「アプリケーションロジックの実行」を担当する「アプリケーションサーバ」層 ③「データベースの管理」を担当する「データベースサーバ」層から構成されるシステムである。 それぞれの層を、個別のサーバで処理できるので、柔軟かつ、コストパフォーマンスのよい、拡張の高い、システム構築を可能にしている。 3 階層のクライアント/サーバ方式では、クライアント上では、アプリケーション処理(演算など)を一切行わないのが原則である。クライアントとサーバそれぞれが役割分担することで、コンピュータ処理の負荷分散を図ることができる。
クライアント移送	client transport 「クライアントの内容を別の SAP システムのクライアントにコピーするための機能。 まずクライアントエクスポートを実行し、続いてクライアントインポートを実行する機能。 → クライアントコピー
クライアント依存移送ルート	client-dependency transport request 移送先として単に SAP システムを指定するだけでなく、SAP システムとクライアントの組合せを指定して移送するためのコンソリデーションルートまたはデリバリルート。 クライアント依存移送ルートは、リリース 4.5(拡張移送制御)から利用できる。
クライアント依存データ	client-dependency data クライアント毎に管理されるデータ、すなわち、クライアント固有データのこと。 アプリケーションデータ、カスタマイジングパラメータの多くは、クライアント依存データである(例: マスタデータ、トランザクションデータ)。 Specific only to one client. Settings in “Client Dependent” tables relate only to the client, which was accessed during the log on process. Such tables contain the client number in the table’s key. (MANDT field)
クライアントコピー	client copy SAP システムのクライアントデータの一部、または全体を、別のクライアントにコピー(=移送)すること。同一システム内の他クライアントにコピーすることも、他のシステムのクライアントにコピーすることもできる。 コピーパラメータ(プロファイル)により、どのような情報をコピーするか選択することができる A function for copying a client. This applies in particular to copying the entire Customizing context (environment) of a source client to a target client, either within one SAP system or to a different SAP system. The system settings determine what is to be copied.
クライアント非依存	client-independent, cross-client 「システム共通」「クライアント間共通」と同義。 例えば、ABAP プログラムやテーブルの定義は、システムで一意に管理されるデータ、すなわちクラ

	クライアント非依存である。
クライアント非依存カスタマイジングパラメータ	client-independent customize parameter クライアント毎に異なる情報を設定できないカスタマイジングパラメータ。大多数のカスタマイジングパラメータは「クライアント非依存」である。 従って、このタイプのパラメータの変更および移送には十分に注意を払う必要がある。各パラメータがクライアント依存かクライアント非依存かは、IMG に明示されている。
権限管理機能	authorization maintenance function SAPシステム内部のアクセスコントロール機能。SAPシステムは独自の権限管理機能を提供する。汎用機オペレーティングシステムや Windows などでは、ファイル単位にユーザのアクセス権限を管理することが多いが、SAP では権限オブジェクト単位（具体的にはマスタやトランザクションデータ、プリンタ、画面に表示された情報 など）ごとにアクセス権限を管理する。 SAP の権限定義は、次の三つの要素から構成される。 ① 権限オブジェクト：品目、会計伝票、得意先などアクセス権限を管理する対象。 ② アクティビティ：権限オブジェクトに対して許可される操作（権限オブジェクトの登録・変更・削除）。 ③ 権限値：①②で「どのようなオブジェクトに」「どのような操作（登録・変更・削除など）ができるか」が決まるが、権限値の指定により、範囲を更に絞り込むことが可能（例：操作可能な、品目コードの範囲、得意先の範囲、ビューの種類など）。 権限の管理単位（＝ロール）の定義を支援するため、プロファイルジェネレータが提供されている。
権限コンセプト	authorization concept メインフレームシステムや Windows などでは、ファイル単位にアクセス制御を行っている。これに対し、SAP は、ロール（職務分掌）毎に、メニューベースで、権限範囲を定義・管理するようになっている。 補足：メニューは、どのようなオブジェクトに対し、どのようなアクションを実行できるかが定義されている。 例：「会計伝票（＝オブジェクト）を転記する（＝アクション）」、「受注伝票（＝オブジェクト）を照会する（＝アクション）」など従って、権限管理のポイントは、まず企業におけるロール（職務分掌）を明確化することである。次に各ロールに必要な（＝許可される）メニューを明らかにすることである。これが決定されると、後は、プロファイルジェネレータを利用して、ロールと権限プロファイルを生成することができる。 The structure and functions associated with authorization assignment and checking in SAP systems. You use authorizations to protect the system from unauthorized or unwanted access.
権限プロファイル	authorization profile 権限プロファイルには権限のセットが登録されている。プロファイルがユーザマスタレコードに割り当てられると、ユーザにはこのプロファイルで定義されたすべての権限が与えられる。HR の組織構造に権限プロファイルを割り当てると、人事異動による権限の付替え作業を減らすことができる。権限プロファイルは、プロファイルジェネレータによって生成できる。 Authorization profiles give users access to the SAP System. They contain authorizations, which are identified using the name of an authorization object and the name of an authorization. If a profile is specified in a user master record, the user is assigned all of the authorizations defined in this profile.
言語移送	language transport Transport that imports translated texts into a target system
更新ビュー	maintenance view テーブル内のデータを更新できるビュー。 SAPシステムではトランザクション SM31 を使って、更新ビューによるデータ更新を行うことができる。また、IMG は更新ビューを多用してカスタマイジングパラメータの登録、更新を行っている。 View type in ABAP Dictionary. You can use a maintenance view to maintain data that is distributed over several tables at the same time. → ビュー → IMG
コードページ	code page 言語コードと「文字」をマッピングしたテーブル。 SAPLOGON のプロパティで使用するコードページを設定する必要がある。因みに日本語は 8000 番のコードページで定義されている。
コピーの移送	Transport of copies 移送オーガナイザ (SE01) の機能で、オブジェクトリストにあるオブジェクトやサブオブジェクトを別の

	SAP システム へ移送する移送機能。ワークベンチやカスタマイジング依頼とは異なり、コピーの移送は、自動 で別のシステムに配信されない。 Transports of copies allow you to transport (sub-)objects in an object list into any other SAP System you want. In contrast to Workbench or Customizing requests there is no automatic delivery into other systems for transport of copies.
コミット	commit データベースに対するデータ操作を確定するための命令。 通常、データベースへのデータ操作は、LUW(論理ユニットワーク)の単位で処理され、すべてのデータ操作命令が正常に終了すると、LUW 全体を確定するためにコミットを実行する。
コンソリデーションシステム	consolidation system 開発システムからの変更依頼のエクスポート先として指定されたシステムのことで、コンソリデーションルート上定義する。コンソリデーションシステムは、3 システムランドスケープでは品質保証システム、2 システムランドスケープでは本稼動システムを指す。 A system in the SAP system group that receives transports of tested, stable developments from the integration system. The consolidation system can be a quality assurance system where final testing takes place or, in the case of minor developments, a production system. 補足: consolidate は、「会社、土地などを合併する。…を統合して[…に]する」、「強化する」などを意味する単語。
コンソリデーションルート	consolidation route SAP システムのリポジトリオブジェクトを開発システムから品質保証システムへ移送するルート。コンソリデーションルートは、移送対象オブジェクトが属する「パッケージ」に割り当てられている「移送レイヤ」によって決まる。→デリバリルート <pre> graph LR A[開発システム インテグレーション] --> B[品質保証システム コンソリデーションシ] B --> C[本稼動システム デリバリシステム] </pre> コンソリデーションルート デリバリルート The regular transport path of a Repository object from the integration system to the consolidation system. The consolidation route is specified for each Repository object in the package (development class) and transport layer. → インテグレーション システム → コンソリデーションシステム → デリバリシステム
サーバ	server この言葉は、「ハードウェアビュー」(＝ハードウェア視点から見た場合)と「ソフトウェアビュー」(ソフトウェア視点から見た場合)とで意味するところが異なる。 ハードウェアビュー ハードウェア特性から「サーバ」マシンと、「クライアント」マシンが区別される。 ソフトウェアビュー 処理を依頼する側を「クライアント」、クライアントの依頼を処理する側を「サーバ」と呼ぶ。 → クライアント/サーバシステム
サンドボックスクライアント	sand box client プレイグラウンドクライアントと同義語。 → プレイグラウンドクライアント
システムランドスケープ	

	system landscape SAP では、SAP システムを効率的かつ安全に「導入～運用、リリースアップ」を行うため、開発システム、品質保証システム、本稼動システムから構成される 3 システムランドスケープを推奨している。  <pre> graph LR A[開発システム インテグレーション システム] --> B[品質保証システム コンソリデーション システム] B --> C[本稼動システム デリバリシステム] </pre> 3 システムランドスケープ  <pre> graph LR A[開発/品質保証システム インテグレーション システム] --> B[本稼動システム コンソリデーション システム] </pre> 2 システムランドスケープ システムランドスケープは、カスタマイジング環境と開発環境の整合性を維持するために変更依頼を共有する、すべての SAP システムで構成される。システムランドスケープは、通常は「移送ドメイン」に対応つけられる。システムランドスケープ内のすべての SAP システムを同じ移送ドメインに入れることにより、すべての変更依頼の設定の整合性が保たれ、依頼の移送が容易になる。
集中ユーザ管理	Central User Administration → CUA The maintenance of users in a central system. A system group includes several SAP systems with several clients. The same users are often created and the same roles assigned in each client. Central User Administration is designed to perform these tasks in a central system and distribute the data to the systems in the system group.
スキーマ	schema データベースはスキーマ(概念スキーマとも言う)、副スキーマ、記憶スキーマの 3 層で定義される。スキーマ(概念スキーマ)は、リレーショナルデータベース、階層型データベースなどの、データベース名、レコード型(網型データベース)またはテーブル構造(リレーショナルデータベース)、各レコードの名前や属性、キー項目など、データベースの構造全体に関する定義を含む。
セッション	session → 外部セッション → 内部セッション
セントラルインスタンス	central instance ①SAP システムを構成するインスタンス群の内、中心的な役割を果たすインスタンス。セントラルインスタンスは同一サーバマシン上でメッセージサーバ(メッセージサーバも一つのインスタンス)が動作している。一般的にエンキューワークプロセスも稼動する。 ②アプリケーションサーバとデータベースサーバが同じサーバマシン上で動作している場合(=1 サーバマシン構成の SAP システム)、このシステム全体を「セントラルインスタンス」と言う場合もある。 The application services for the SAP System, including the enqueue and message services, that are located on a single host machine. Typically, the central instance has multiple work processes for the dialog, update and background services. The machine on which it runs is called the central host.
セントラルホスト	central Host セントラルインスタンスを実行するサーバマシンをセントラルホストと呼ぶ。
操作モード	operation mode SAP インスタンスにおける「ワークプロセスの組合せ」を定義したもの。複数の操作モードを定義し、これをスケジュール表に基づいて自動的に切り替える機能が提供されている(=CCMS 機能)。この機能を使って、対話型処理中心の昼間の操作モードに対してバッチ JOB 中心の夜間の操作モードというように、ワークプロセスの利用度に応じて操作モードを切り替えて運用できる。
ソリューションマネージャ	solution manager SAP ソリューションマネージャは、SAP ソリューションの導入および運用支援環境

	SAP ソリューションマネージャは、以下の構成要素を含む。 ・ソリューションスコープ: システムランドスケープやコア・ビジネスプロセスの定義。システムランドスケープ全体を1つのプラットフォーム上に統合して管理することができる。 ・オペレーションポータル: 各 SAP のサービスやベストプラクティスへのアクセス ・モニタリング(監視): 周期的なサービスレベル管理レポートやシステムコンポーネント及びビジネスプロセスのオンラインソリューション監視 ・サポートポータル: SAP ノートアシスタントや SAP サポートサービスへのダイレクト接続による素早い問題解析や解決の為に高度なメッセージ処理の支援 また、別の見方をすると SAP ソリューションマネージャは、システムランドスケープ全体の管理を、1つのプラットフォーム上に統合する機能である。
ダイアログプログラム	dialog program 「対話型プログラム」を意味する(「ダイアログプログラム」に対し「レポートプログラム」がある)。「ダイアログプログラム」が対話形式でデータベースの更新を行うのに対し、レポートプログラムは、データベース情報の更新を行ってはならないことになっている(これは、ルールとしての規定なので、レポートプログラムから UPDATE 命令を発行すると、データベースの変更が実行されてしまう)。 ダイアログプログラムは一つ以上の画面を持ち、ユーザとの対話を行いながら処理を進めるプログラム。一般的なトランザクションプログラムはこの形式のプログラムである。ダイアログプログラムは Dynpro から構成される。 A dialog program consists of an ABAP program of the type "module pool", screens, and a transaction code for calling the program. There is also a graphical user interface that offers a number of functions. You can start a dialog program with a transaction code. However, the transaction code is often incorporated into an area menu.
対話型プログラム	dialog program ダイアログプログラムと同義語。 → ダイアログプログラム
ディスパッチャ	dispatcher ディスパッチャはアプリケーションサーバ上で動作しているプロセス。ユーザ端末から処理依頼を受け付け、利用可能なワークプロセスを探し、依頼を振り分ける。 実際のデータ処理は、ワークプロセスにおいて行われる。ワークプロセスでの処理結果は、再びディスパッチャを介して、ユーザ端末に返される。 Central process on an application server. In addition to other tasks, the SAP dispatcher is responsible for the following principle tasks: ・Initialization, reading profile parameters, starting work processes and logging on to the message server ・Evenly distributing the transaction load across work processes ・Connecting to the GUI layer ・Organizing communication processes
データアーカイブ	data archive SAP データベースからリアルタイムにアクセスする必要がないデータを削除し、アーカイブ装置(光ディスクなど)に保存すること。
データ転送ワークベンチ	Data Transfer Workbench <CA-GTF (General Application Functions)> A central SAP tool for organizing and performing data transfer to the SAP System. The Data Transfer Workbench supports various business objects such as customers and master data. Technologies supported include Batch Input, Call Transaction, Direct Input, and BAPIs. An additional tool for data transfer is the Legacy System Migration Workbench (LSMW). <SAP B1> Migration tool that can be used to migrate master and transaction data from legacy systems into SAP Business One. The Data Transfer Workbench offers pre-defined data file templates to simplify the data preparation process.
データモデル	data model SAP システムのデータ構造を表現したモデル図。 データモデル図の "A、H、R" (カテゴリ) の意味は次のとおり H: 階層 1つのソースエンティティタイプに対して1つのターゲットエンティティタイプが決定される。ソースエンティティタイプが存在しない場合には、ターゲットエンティティタイプは存在しない。ソースエンティティタイプのキーは、ターゲットエンティティタイプの標準キーの一部になる。 A: 集合

	複数のソースエンティティタイプに対して1つのターゲットエンティティタイプが決定される。ソースエンティティタイプが存在しない場合 には、ターゲットエンティティタイプは存在しない。ソースエンティティタイプのキーは、ターゲットエンティティタイプの標準キーの一部になる。 R: 参照 ターゲットエンティティタイプはソースエンティティタイプを参照している。つまり、ソースエンティティタイプに対してターゲットエンティティタイプを決定することはできない。ソースエンティティタイプのキー属性は、非キーの属性としてターゲットエンティティタイプに含まれている。2つのエンティティ間の関係は変更することができる。
デフォルトプロファイル	default profile A profile that contains values that apply to all application servers. There is always one active default profile that is defined, like all profiles, in the SAP R/3 global profile directory. The default profile is also known as the system profile. 有効同義語: system profile
デリバリシステム	delivery system システムランドスケープを構成する SAP システムタイプの一つ。デリバリシステムは、コンソリデーションシステムにリンクされる。このリンクにより、デリバリシステムはコンソリデーションシステムにインポートされる変更依頼のコピーを常に受け取ることが可能になる。標準的な SAP システムランドスケープでは、デリバリシステムは本稼動システムである。
デリバリシステム	delivery system: デリバリシステム A function where there is development in distributed systems. A delivery system must be linked to a consolidation system. By means of this link, the delivery system continually receives copies of transports performed in the consolidation system. Delivery systems are usually production systems.
デリバリルート	delivery route リポジトリオブジェクトと、カスタマイジングパラメータを移送するための、コンソリデーションルートに続く、移送ルート。コンソリデーションシステム上で品質保証テストが完了すると、デリバリルートに従って(一般的には本稼動システムへ)移送が行われる。→ コンソリデーションルート
透過テーブル	transparent table SAP リポジトリ上の定義と DBMS 上のテーブルが 1:1 に対応するテーブルを透過テーブルと呼ぶ。一方、SAP にはリポジトリ上の定義と DBMS 上のテーブルが 1:1 に対応しないテーブルがある。1:1 に対応しないテーブルには、プール型テーブルとクラスター型テーブルがある。
トランザクションコード	transaction code トランザクション処理機能を識別するためのコード 例:「受注の登録=VA01」「会計伝票登録=FB50」「リポジトリオブジェクト一覧表示=SE15」など。 トランザクションコードおよびその内容説明は、テーブル TSTCT に記録されている。 トランザクションコードの定義は、非常にシンプルである。すなわち、SAP ユーザがトランザクションコードを呼び出した時に、最初に起動されるプログラムが紐付けられているだけである。(トランザクション定義: SE93) → トランザクション処理
トランザクション処理	transaction processing 単語「トランザクション」は「(ビジネス)取引あるいは取引伝票」とも訳される。従って「トランザクション処理」とは「取引伝票を(コンピュータ上で)処理する」と言う意味になる。 たとえば、「受注伝票の入力/照会/変更」「発注伝票の入力/照会/変更」などが、それぞれトランザクション処理である。また、「バッチ JOB の登録」「ログオンユーザの一覧表示」などのベース機能も、(SAP システムにおいては)トランザクション処理の一つである。 → トランザクションコード (広辞苑より)①取引、処理 ②<電算>マスタファイルの内容に影響を及ぼすような行為(登録、変更など)・データ
トランザクションバリエーション	transaction variant A alternative of a transaction in the SAP System. You can create different variants for the same transaction. This enables you to simplify transaction flows by: • Preassigning values to fields • Suppressing and changing the readiness for input of fields • Suppressing whole screens A transaction variant consists of a number of screen variants.
内部セッション	internal session Instance of an ABAP program within an external session. External procedure calls allow you to load several ABAP programs in an internal session. Program calls open their own internal sessions.

ネーミングコンベンション	naming convention 「命名規則」。アドオンを行う場合、アドオンオブジェクトのネーミングコンベンション(=命名規約)が決められており、SAP 導入企業は、この規約を遵守しなければならない。 大多数のオブジェクトの名称は一文字めが'Y'または'Z'からはじまる規約になっている。但し、例外があるので注意すること。詳細は、オンラインドキュメントを参照。 → 名称範囲
バックアップドメインコントローラ	backup transport domain controller バックアップ用のドメインコントローラ。必要に応じてドメインコントローラの機能を代行することができる。 → 移送ドメインコントローラ
バックグラウンド処理	background processing メインフレームで言う、バッチ処理に該当する。 バックグラウンド処理は、ユーザ(オペレータ)との対話なしに処理が実行される。対話処理とバックグラウンド処理の実行優先度は同じである。対話処理は「対話ワークプロセス」で実行され、バックグラウンド処理は「バックグラウンド・ワークプロセス」で実行される。「対話ワークプロセス数」および「バックグラウンド・ワークプロセス数」の初期値はインスタンス プロファイル パラメータで規定する。時間帯ごとに「対話ワークプロセス数」および「バックグラウンド・ワークプロセス数」を自動的に変更することが可能。 バックグラウンド処理は、実行タイミングをスケジュールすることが可能。 Processing that does not take place on the screen. Background processing enables you to process data in the background while executing other functions in parallel on the screen. Although background processes are not visible to the user (there is no dialog), they have the same priority as online processes. バックグラウンド JOB スケジューリングモニタ RZ01 バックグラウンド JOB の登録:トランザクション SM36 バックグラウンド JOB の照会・変更:トランザクション SM37 ワークプロセスの監視:トランザクション SM50
パッケージ	Package 旧用語「開発クラス」改め「パッケージ」と呼ぶようになった 特定のアプリケーション機能(例えば、売掛管理機能、買掛管理機能など)を構成する全リポジトリオブジェクト(プログラム、テーブル定義、画面定義、メニューなど)をグループ化して管理・移送するための仕掛である。 (注意:ロジスティックで使用する「クラス」とは全く別物) 移送が必要なリポジトリオブジェクトを登録する際は、必ずパッケージに割り当てなければならない。パッケージには、移送レイヤが割り当てられる。パッケージ単位でリポジトリオブジェクトの移送を行うことができる。すなわち、特定の機能を構成する全リポジトリオブジェクトをまとめて移送することが可能。 一度登録したパッケージは、一般に永久に存続する。一方「変更依頼」は、アプリケーションの開発・変更プロジェクトの開始と共に作られ、リリースをおこなうことによって消滅する(=リリースステータスに変わる) → 変更依頼、移送レイヤ A container for semantically related development objects. A package consists of subpackages and development objects (programs, tables, screens, function modules and classes), that are developed and transported together. Packages are characterized according attributes including nesting, interfaces, visibility, and use access. You can create and manage packages with the Package Builder. Packages replace the previously used development classes. → パッケージ
パッチ	patch パッチとは、SAP システム内のエラー修正や、法改正などに伴って必要となるバグフィックスや機能調整・追加を行うためのファイル(内容は、移送ファイル、プログラムコード、など)。 各パッチは、特定のリリースに対してのみ有効である(ただし、すべてのデータベースとオペレーティングシステムに対して有効)。潜在的な問題の顕在化を回避するため、パッチが提供されたら、できる限り速やかに適用する必要がある。パッチを適用することを「パッチをあてる」という。 → パッチタイプ SPAM(SAP Patch Manager)により、指定した順序でパッチを適用することができる。 → SAPM 補足:patch は「継ぎ布、継ぎはぎ」の意。
バッチインプット	batch input

	他のシステム(多くの場合、レガシシステムを指す)のデータを SAP に取り込むための機能。次のような方法があり、ニーズに合わせて、使い分ける。 ①画面のエミュレーション機能(狭義には、この方法をバッチインプットと呼ぶ) レガシデータを BDC 形式に変換し、バッチまたは、一件ずつ(Call Transaction) 処理することができる。バッチ処理の場合、「全件、画面表示」、「エラーデータのみ表示」、「非表示」の三つの処理形式を選択することが可能。→BDC ②BAPI インタフェースを利用する方法 ③ダイレクトインプット(汎用モジュールを利用する方法)。但し、この場合、該当データに対する汎用モジュールが、SAP から提供されている場合に限る。 ④IDoc インタフェースを利用する方法 注意 1: SQL コーディングによる SAP DB の直接更新は厳禁。これを行うと、データベースの不整合をきたす危険性が非常に高くなる。 注意 2: 狭義には、上記の「画面のエミュレーション機能」だけをバッチインプットと呼ぶ。 → BDC A data transfer technology that enables the transfer of large volumes of data to an SAP System using the online transaction. A batch input session is created for this purpose which you can then process using the Batch Input Monitor. Additional transfer technologies: Call transaction, direct input, EDI and BAPIs.
バッチ処理	Batch Processing バックグラウンド処理と同義語。対話(ダイアログ)処理の反語。 あらかじめ一連の処理を登録しておき自動的に実行させる処理方式のこと。一連の処理単位をバッチという。 バッチ処理の目的は、コンピュータ資源を有効利用し高い処理効率を得ることである。そのため人間が操作しなくても済むよう、複数のプログラムを連続実行できるように JCL(Job Control Language)を用いて定義する。 運用方法にはオペレータが登録・処理し、利用者に結果を返すクローズド・バッチと、利用者自身が登録・処理をするオープン・バッチがある。日次・月次の売り上げデータや受注データの集計など、大量データを集めて繰り返し行う処理に有効である。 バッチ処理では、プログラムの実行順序を指定するスケジューリング機能や処理中障害が発生した場合のリラン(再起動)機能が必要となる。 SAP システムのベース機能の一部としてこれらの機能を備えている。 トランザクションコード: SM36、SM37 → バックグラウンド処理
パッチタイプ	patch type パッチには、以下のタイプがある。 PAT: SPAM 更新用パッチ。このタイプのパッチには、SAP パッチマネージャのアップデート、改良、拡張が含まれる。 FFD: FCS 最終デルタパッチ(FFDP)を示す。FFDP により、FCS システムがパッチを適用する前の最終状態に戻る。 COP: 一般コンポーネントパッチを示す。これは一つのコンポーネント(SAP_BASIS、SAP_HR、SAP_APPL など)に対して有効で、そのコンポーネントにおけるリポジトリとディクショナリのエラー修正のみが含まれる。SAP_HR に対するパッチには、修正以外に法改正による調整も含まれる。 BWP: SAP ビジネスウェアハウスパッチ(BWP)を示す。SAP ビジネスウェアハウスパッチは、SAP ビジネスインフォメーションウェアハウス(SAP_BW)に対するコンポーネントパッチで、このコンポーネントの修正のみが含まれる。 AOP: アドオンパッチを示す。これは、特定のリリースの追加機能に対して常に適用される。 CRT: コンフリクト解消移送(CRT)を示す。CRT は IS-IS や IS-OIL などアドオン専用で使用される。このパッチにより、一般コンポーネントパッチとアドオンの間に発生するコンフリクトを解消することができる。 HOT: ホットパッケージを示す。このパッチには、リポジトリとディクショナリオブジェクト内の一連のエラー修正が含まれる。 SAP から個別に提供された修正が、定期的にホットパッケージに集められ、SAPNet-SAP フロントエンドによって通知される。 → パッチ、サポートパッケージ、ホットパッケージ
汎用モジュール	function module 「西暦から和暦への変換」「通貨の換算」「文字列の操作」など SAP 内で共通に使われる機能を提供するプログラム。 多岐に渡る汎用モジュールを汎用モジュールライブラリとして管理している。SAP アプリケーションコンポーネントは汎用モジュールを利用して開発効率の向上、品質の向上を図っている。SAP 導入

	企業固有の汎用モジュールをライブラリ登録することも可能。汎用モジュールを ABAP プログラムに組み込むと、該当汎用モジュールに受け渡すパラメータのコードが自動生成される。これにより、プログラムの品質向上と生産性の向上に効果がある。 An external subroutine written in ABAP. Developed in the Function Builder, they are managed in a central function library, and can therefore be called from any ABAP program. This helps to avoid redundant code and makes the programming process more effective. In contrast to FORM routines, function modules have the same standard interface.
引数	Argument 「ひきすう」と読む。関数やサブルーチン、マクロ命令などに受け渡す定数や変数などの総称。引数には仮引数と実引数がある。仮引数は手続きやサブルーチンの定義で使われ、それぞれが呼び出されるときに実引数で置き換えられる。引数には変数の値そのものを渡す「値呼び出し」(Call by Value)と、変数のアドレスを渡す「参照呼び出し」(Call by Reference)がある。
ビジネスコネクタ	business connector SAP メッセージ標準である IDoc と XML/HTML との形式変換を行うサブシステム。全ての SAP コンポーネントで利用可能(リリース 3.1 以降)。ビジネスコネクタによって、SAP コンポーネントと Web アプリケーションやレガシシステムとのシームレスな統合が可能となる。 A middleware application based on the B2B integration server from webMethods. The SAP Business Connector enables both bi-directional synchronous communication and asynchronous communication between SAP applications and SAP and non-SAP applications. The SAP Business Connector makes all SAP functions that are available via BAPIs or IDocs accessible to business partners over the Internet as an XML-based service. The SAP Business Connector uses the Internet as a communication platform and XML or HTML as the data format. It integrates non-SAP products by using an open, non-proprietary technology.
ビジネスコンフィグレーションセット	→ BC セット
非同期更新	asynchronous update 「トランザクション処理に必要なデータの受け付け(=取引データの入力)」と「実際のデータ更新処理」の同期をとらないメカニズムを「非同期更新」と呼ぶ。 SAP では、非同期更新メカニズムを使ってアプリケーションデータの更新(=トランザクション処理)が実行される。 非同期更新メカニズムの目的は、レスポンスタイムの短縮である。非同期更新を行うトランザクションの場合、データ入力を終わると、(更新処理の完了を待つことなしに)、すぐに次のトランザクション入力を開始することができる。これは、非同期更新では、「トランザクション処理に必要なデータの受理」と「実際の更新処理」が切り離されているからである。 注意: 非同期更新型のプログラムを作成する場合、データ入力時のチェックを厳重に行い、データ更新時にエラーが発生しないようにしなければならない。万一、データ更新時にエラーが発見されると、更新要求はエラーログに記録される。エラー原因を解析後、エラーログを削除することも、エラーログを使って更新を再実行することも可能。 トランザクション: SM13
ビュー(表)	view ABAP ディクショナリに実在する複数のテーブルを結合 (Join)、射影 (Projection)、選択 (Selection) 操作によって作り出した、Read Only な「仮想テーブル」 結合 (Join) 機能により、複数のテーブルをあたかも一つのテーブルのように扱うことができる 射影 (Projection) 機能により、結合したテーブルの任意の項目だけを操作できるようにすることができる。これにより、機密データをプログラムで操作できなくする(隠してしまう)ことができる 選択 (Selection) 機能により、指定した範囲のデータだけを選択することができる。例えば、年収 1000 万円を超える従業員だけを含む「仮想テーブル」を定義することができる Virtual table that contains no data but is an application-specific view of one or more tables in the ABAP Dictionary. When you create a table, you assign a key to it. However, the fields in the key may be inadequate for solving some problems, so you can generate a view from several tables or parts of tables. → 更新ビュー
品質保証システム	quality assurance system 3 システムランドスケープを構成するシステムの一つで、総合テストを実施するためのシステム。 → システムランドスケープ System into which tested, stable development versions and the parameters of the Customizing objects are transport from the development or test system at defined events.

	This is the basis for performing the final test in this system.
ファイアウォール	fire wall インターネットと LAN との間に置くことでデータ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを守る仕組み、または機能的役割のこと。 防火壁 (Firewall) にちなんでネーミングされた。 → SAP ルータ
プレイグラウンドクライアント	playground client サンドボックスクライアントとも呼ぶ。一般にシステムランドスケープの「開発システム」上に設定されるクライアントで、主に実験用に利用する。例えば、「クリティカルなパラメータ(一度設定してしまうと、変更することが難しいパラメータ)を設定する前にまず、プレイグラウンドクライアント上で設定結果の確認を行う」などの使い方がある。
プロファイルジェネレータ	Profile generator 職務分掌(ロールと言う)単位にメニューを指定することにより、(権限)プロファイルおよびロールを自動生成するツール。
プロファイルパラメータ	profile parameter SAP システムのミドルウェア(ベーススまたはウェブアプリケーションサーバ)の機能をカスタマイズするためのパラメータ。例えば、バッファのサイズ、セキュリティ設定レベルなど多岐にわたる。 SAP インスタンス毎のプロファイルパラメータを「インスタンスプロファイルと呼ぶ」 → インスタンスプロファイル、デフォルトプロファイル
ベーススコンポーネント	Basis component SAP システムは、「アプリケーション層」「ベースス層 (Enterprise リリース以降 "Web AS " と呼ぶ)」および「プラットフォーム層」から構成されている。「アプリケーション層」は、FI, CO, SD, MM, PP などのアプリケーション機能を提供するレイヤである。「ベースス層」は、「アプリケーション層」と「プラットフォーム層」の間に位置する「ミドルウェア」である。「プラットフォーム層」は、SAP システムが稼動するために必要な環境を提供するレイヤで、オペレーティングシステムやデータベース管理システムなどから構成される。「ベースス層」を設けたことが SAP 製品の特徴で、これにより①移植性を保証する SAP 共通インタフェースの提供、②開発環境の提供、③運用管理支援機能の提供を実現している。なお、ベースス層を実装したコンポーネントは、現在では「SAP Web アプリケーションサーバ」である。
変更依頼	change request ABAP プログラム、テーブル定義など、いわゆるリポジトリオブジェクトと、カスタマイジングパラメータの登録・変更を記録・管理および移送を行うための「変更の履歴を管理する管理簿」のこと。 個々の変更依頼は管理番号を持つ(自動採番される)。 変更依頼の登録/変更/参照はトランザクション SPRO ADMIN、もしくは、SE10 で行う。 リポジトリオブジェクト(ここでは、所謂リポジトリオブジェクトとクライアント非依存カスタマイジングパラメータを含む)に対する変更依頼を「移送可能変更依頼」と呼び、カスタマイジングパラメータに対する変更依頼を「カスタマイジング依頼」と呼んで区別している。 変更依頼を「リリース」すると、変更依頼は「移送依頼」となり、移送ファイルが自動作成される。 →カスタマイジング依頼、移送可能変更依頼、ローカル変更依頼 注意:「変更を依頼する」という意味ではない。誤解の多い SAP 用語の一つ。
変更管理	change management ABAP プログラム、テーブル定義など、いわゆるリポジトリオブジェクトと、カスタマイジングパラメータに対する登録・変更の管理を指す。 ある SAP システムで作成した成果物を、一つ以上の SAP システムに整合性を保ちながら適切な時期に配信する手続きを指す。 ASAP でいう「変更管理」と区別する必要がある。→ASAP 変更管理
変更キー	changeover key リポジトリオブジェクト(プログラム、トランザクション、テーブルなど)の変更を行うときに必要となるキー。リポジトリオブジェクトごとにキーが必要になる。 変更キーは、ライセンス番号、リポジトリ識別 ID、オブジェクトタイプごとに一意に決定される。 設定された変更キーは、テーブル "ADIRACCESS" に記録される。
本稼動システム	go live system 企業の実際のビジネスプロセスを処理する SAP システム。
名称範囲	name range → ネーミングコンベンション、命名規則
命名規則	naming convention SAP アドオンを行う場合、アドオンオブジェクトのネーミングコンベンションが決まっており、これを遵守しなければならない。ほとんどのオブジェクト名は一文字「Y」または「Z」からはじめる規約になっているが、一部例外があるので注意が必要。

モディファイ	modify 「モディフィケーション」と同義語。→モディフィケーション 原義は「部分修正する」の意
モディフィケーション	modification SAP が提供する標準プログラムやテーブルなどを導入企業の責任において変更することをモディフィケーションと呼ぶ。 モディフィケーションを行う事は、「SAP システムに時限爆弾を埋め込むのに等しい」との認識をもつ必要がある。埋め込んだ時限爆弾は、リリースアップのときに爆発する。すなわち、リリースアップを行う度に、導入企業の責任において、全モディフィケーション箇所が新リリースに適合しているかテストしなければならない。もし、適合しない場所があれば、モディフィケーションをやり直さなければならない。この作業には膨大な時間と人と金が必要である。
モディフィケーションアシスタント	modification assistant モディフィケーションの管理機能。 モディフィケーションの内容を明確に文書化し、オブジェクトの元の状態を保存し、変更内容を管理する機能。 モディフィケーション内容が新リリースに適合するかどうかの確認は、導入企業の責任において検証する必要がある。 Tool for supporting adjustment of the SAP standard. The Modification Assistant ensures that the upgrade is simplified. You can go to a special modification mode if you access the ABAP Workbench editors when modifying objects of the SAP standard. The original object is protected in this mode and can be changed only with additional actions. The Modification Assistant logs changes, providing a fast and detailed overview of the modifications and reducing the load during upgrade.
ユーザマスタ	user master SAP ユーザの ①ログオンと権限に関する情報、 ②デフォルト情報 などが記録されるマスタ。 SAP では、「ユーザの登録」とは「ユーザマスタレコード」を登録することである。 「ユーザマスタレコード」を持つユーザだけが、SAP システムにログオンし、トランザクションを実行することができる。 ユーザマスタは、クライアント依存情報なので、ログオンしたいクライアント毎にユーザマスタレコードを登録しなければならない。
リポジトリ	repository →SAP リポジトリ
リポジトリオブジェクト	repository object リポジトリ上で管理されるオブジェクトの意味。具体的には、ABAP プログラム、Dynpro、テーブル定義、項目定義などがある
リモートファンクションコール	Remote function call →RFC
レポートまたはレポートプログラム	report SAP における用語「レポート(プログラム)」は、データベースのデータを読み出し、分析結果を表示するプログラムまたは、その結果を出力したものを指す。レポートプログラムでは、データベースに対するアクセスは、読み出しだけに限定し、データの追加・変更を行わないことがルールである。 ABAP program that implements the reporting – that is, it reads data and displays it. It is usually an executable program and the program starts with the REPORT statement, in which event blocks are implemented for the reporting events and which displays the data in a list.
ローカルオブジェクト	local object ローカルオブジェクトは、そのオブジェクトが作成された SAP システムだけで使用するオブジェクトであり、移送処理の対象とすることはできない(すなわち、他のシステムに移すことができない)。たとえば、テスト用のプログラムなど、該当システム上での使い捨て「プログラム」などである。 Development object created for private use. Local objects belong to the development class \$TMP. They are not transported to other systems. You can access the local objects of other users as well as your own.
ローカル変更依頼	local change request 他の SAP システムに移送できない変更依頼。 ローカル変更依頼を移送することはできないが、この変更依頼に記録されたプログラムやテーブルは、他のユーザが変更できないようにロックされる。すなわち、排他制御を目的として使われる変更依頼である。

ロール	role 一般に言う「職務分掌」「職責」「ジョブディスクリプション」などを指す言葉。 例えば、システム管理者、給与管理担当者、人事部出納係などのロールがある。 SAP はロール単位に権限管理を行う。 →プロフィールジェネレータ、権限プロフィール The collection of activities that a person performs to participate in one or more business scenarios in an organization. Access to the transactions, reports, Web-based applications, and other objects contained in roles is through user menus. mySAP.com Workplace provides the user access using a Web browser to a role-based portal for completing his or her tasks.
ロールバック	rollback データベースに対するデータ操作を取り消すための命令。 通常、データベースへのデータ操作は、LUW(論理ユニットワーク。複数のデータベース操作を含む)の単位で処理される。その中で、一つでもデータベースへの命令が実行できなければ、LUW 全体を取り消す必要があり、このような場合にロールバックを実行する。 SAP の操作面から見ると、トランザクションを中止または終了ボタンをクリックしたときロールバックが実行される。一方、保存ボタンを押すと、コミットが実行される。 →コミット
ロック	lock →エンキュー
ロックオブジェクト	lock object SAP システムの排他制御の単位 SAP では、ロックオブジェクト単位に排他制御を行えるので、プログラム開発者は個別のテーブルを意識せずに、排他制御を行うことが可能である。 ロックオブジェクトの登録は、トランザクション SE11。ロック中のオブジェクトを参照するには、トランザクション SM13 Object type in the ABAP Dictionary. When you activate a lock object, you generate function modules that set and release locks. You can use these function modules in ABAP programs.
ロックテーブル	lock table 登録あるいは更新中のロックオブジェクトを記録するためのテーブルで、排他制御のために使われる。 このテーブルに記録されているロックオブジェクトは、「排他制御機能」によって、他のユーザが同時に更新することができないようにコントロールされる。→エンキュー A table stored in the main memory of the enqueue server which contains entries for the current locks in the system. Each lock includes the owner of the lock, the lock mode, and the name and the fields of the locked table. →エンキュー
論理データベース	Logical database: 論理データベース ABAP Runtime Environment (BC-ABA) Special ABAP program that provides other ABAP programs with data from the nodes of a hierarchical tree structure. Is either linked in the program attributes of an executable program or called using the function module LDB_PROCESS. A logical database has a structure with nodes, a database program written in ABAP, and its own standard selection screen . Logical databases are maintained in the Logical Database Builder.
論理ユニットワーク	Logical Unit of Work Period of time between two consistent states on the database. → SAP LUW
ワークプロセス	work process 端末からの処理依頼、あるいはバックグラウンド・ジョブのスケジューラからの依頼を受け、プログラムを実行する仕掛(プロセス)。ディスパッチャの配下で動作する。 ワークプロセスには次のようなタイプがある。 ・ダイアログ管理(DIA) ・変更文書の更新(UPD) ・バックグラウンド処理(BGD) ・スプール処理(SPO) ・ロック管理(ENQ)

	システム管理者は、システムのパフォーマンスとユーザニーズを勘案して、ワークプロセスの数とタイプを適切に管理しなければならない。 稼働させるワークプロセスの数は、プロファイルパラメータ(インスタンスパラメータ)で定義する。 A process that as a component of an application server executes an ABAP application. To process SAP requests from several front ends, an SAP application server has a dispatcher, which collects the requests and forwards them to work processes for execution. There are the following types of work process: • Dialog: For executing dialog programs • Update, Upd2: For asynchronous database updates • Background (batch): For executing background jobs • Enqueue: For executing lock operations • Spool: For print formatting Work processes can be assigned to dedicated application servers. In the service overview (SM51), you can see which work process types are provided by the individual servers. Each work process is logged onto the database system as a user for the entire runtime of the SAP system. Each work process is assigned for the duration of a dialog step to an ABAP program.
ワークベンチオーガナイザ	work bench organizer (WBO) Invalid as of Release: 46C ABAP ワークベンチ上で開発された成果物を管理するためのツール群。 ワークベンチオーガナイザは、移送/修正オーガナイザ(CTO)の構成要素。46C 以降死語。 補足: 一般的な「CASEツール」における、「構成管理機能・バージョン管理機能」に相当するSAPの開発系ツール環境 Tool for managing central and decentralized development projects in the ABAP Workbench. The Workbench Organizer is part of the Change and Transport Organizer (CTO).

6 チェックリスト

以下のチェックリストを別添として示す。

6.1 本運用環境

6.2 開発環境

6.3 アクセスコントロール

6.4 運用統制

本運用環境 チェックリスト

(補足)

項目 1、2 は、事前にクライアントから文書提出を求め確認しておく。

実施基準が例示する「全社的な内部統制」の要求

財務報告に係る全社的な内部統制に関する評価項目の例(実施基準 P89)

I Tへの対応

- ・ 経営者は、I Tに関する適切な戦略、計画等を定めているか。
- ・ 経営者は、内部統制を整備する際に、I T環境を適切に理解し、これを踏まえた方針を明確に示しているか。
- ・ 経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びI Tを用いた統制の利用領域について、適切に判断しているか。
- ・ I Tを用いて統制活動を整備する際には、I Tを利用することにより生じる新たなリスクが考慮されているか。
- ・ 経営者は、I Tに係る全般統制及びI Tに係る業務処理統制についての方針及び手続を適切に定めているか。

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
1.	全社 的統 制	戦略、 計画等	A	経営者は戦略、計画、方針等を定めているか。		事前に質問表を渡し、回答してもら う。不明点をヒアリングする。	
				経営者は信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか。		同上	
				ERPシステムを利用することにより生じる新たなリスクが考慮されているか		同上	
				経営者は、ERPシステムに係る全般統制及びERPシステムに係る業務処理統制についての方針及び手続を適切に定めているか。		同上	
2.	ランド スケー プ/ク ライ アント 管 理	文書化・ 教育	A	ランドスケープ/クライアント(本稼動、品質保証、開発システムを物理的分離)の管理規定・手順等は文書化され、周知徹底されていますか はい ☐ いいえ ☐ 管理手順を説明してください クライアントの登録・変更・削除申請書を提出する権限があるのは誰(部署、役割)ですか : 申請書の承認を行なうのは誰(部署、役割)ですか : クライアントの登録・変更作業を行うのは誰(部署、役割)ですか : 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役割)ですか : トレーニング等を通し、関連者にランドスケープ/クライアントに関する知識と管理手順を周知徹底していますか はい ☐ いいえ ☐ クライアントの登録・変更・削除申請書はありますか はい ☐ いいえ ☐ 申請書には次のような項目がある。か ☐ 申請日	- クライアント管理が厳格に行なわれていないとクライアントデータ(アプリケーションのマスタデータ/取引(伝票)データ、ユーザマスタなど)の破壊、統制機能の低下が起こる。 - その前提として、文書化および教育等を通し周知徹底が必要である。	事前にランドスケープに関わる文書入手する。次の点を確認し、現場でヒアリング/確認する項目を決定する - 文書の形式(必要項目の有無) - 文書の内容(記述の有無と記述内容の妥当性) 提出を求める文書の - 文書体系 - システムランドスケープ/クライアント(本稼動、品質保証、開発システムを物理的分離)の管理手順 - クライアントの登録・変更・削除申請書	ランドスケープ/クライアント管理の評価 レベル 0. 1. 2. 3. 4. 5

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				☐ 申請部署 ☐ 承認者 および サイン／印 ☐ 実施時期 ☐ クライアントの有効期間 ☐ 対象システム(本稼動／品質保証／開発の別、システム ID、) ☐ 登録・変更の目的、クライアントの役割 ☐ クライアントの属性 ☐ コピー元クライアント、選択プロファイル ☐ 必要なディスク容量 ☐ 作業完了(作業担当者、日時) ☐ 増加したディスク容量、残存ディスク容量 ☐ 作業完了確認(確認担当者サイン／印、日時)			
3.			A	ランドスケープを構成する全てのクライアントの管理簿はありますか。 はい ☐ いいえ ☐ 各システムにどのようなクライアントを設定してある。か (クライアント 000、001、066 は除く) DEV(開発) : (クライアント番号、名称、利用目的、管理者(部署)を説明してください) 品質保証(QA)テスト : (クライアント番号、名称、利用目的、管理者(部署)を説明してください) PRD(本稼働) : (クライアント番号、名称、利用目的、管理者(部署)を説明してください)	管理されていないクライアントから、本稼働クライアントへの不正アクセスが行なわれる可能性がある。	事前にランドスケープ/クライアント管理簿を取り寄せ、記述されているランドスケープ/クライアントの妥当性を確認する。 (チェックのポイント) 3システムランドスケープが採用されていること - 本稼働システム上に 000、001、066 を除くクライアントが存在しないこと	
4.		実装の確認	A	3システムランドスケープを採用していますか。 はい ☐ いいえ ☐ 本稼働システムへの移送は、責任者による承認が無いとできないように設定されていますか。	2システムランドスケープ/クライアントの場合、ユーザ受入テストを「本稼働のシミュレーション」の位置付けで実行することはできない。 3システムランドスケープ/クライアントへの早急な移行を考えてください	トランザクション STMS を使い 移送ルートの定義をチェックし、3システムランドスケープであることを確認する。	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				はい ☐ いいえ ☐		・品質保証システムから本稼働システムへ移送する場合、管理者による承認がないと実行できないように設定されている(スタンプのアイコンが表示されている)。	
5.			A	本稼働システム上に本稼働以外のクライアントが存在しますか？(クライアント 000、001、066 は除く) はい ☐ いいえ ☐ 「はい」の場合、どのような目的で、どのようなクライアントを設定してある。か。 ：	・本稼働システム上に 000、001、066 以外のクライアントを置いてはいけない理由は以下のとおり。 ・本稼働クライアント以外のクライアントが存在する場合、それらのクライアントから、本運用クライアントのデータがアクセスされる危険性がある。 ・本稼働以外のクライアントのユーザが、間違っって本稼働クライアントにログオンする危険性がある。 ・クライアントの作成/削除によってテーブル領域が断片化(フラグメンテーション)が起こり、アクセス効率に影響を与える可能性がある。 ・他のクライアントの処理が本運用クライアントのパフォーマンスに影響を与える可能性がある。	本稼働システム上で、トランザクション SCC4 を使って、クライアントの設定状況を確認し、次のクライアント以外のクライアントが存在しないことを確認する。 ・本稼働クライアント ・000、 ・001、 ・066 上記以外のクライアントが存在する場合、それらのクライアントの用途、セキュリティの確保対策を確認する。 (リスクの緩和策) 本稼働以外のクライアントが存在(クライアント 000、001、066 は除く)し、妥当性がある場合、リスクの緩和策として、それらのクライアントに登録されている一般ユーザを、通常時はロックしておき、申請に基づいてロックを解除する運用を行う。	
6.			A	各クライアントの変更属性はどのように設定されていますか 本稼働(PRD)用クライアントの属性 ロール (推奨値「本稼働」) ☐ カスタマイジング ☐ デモ ☐ トレーニング/教育 ☐ 本稼働 ☐ SAP 参照 ☐ テスト	・クライアント属性を適切に設定しておかないと SAP システムが持つ統制機能が低下する。 ・品質保証(QA)システムおよび本稼働システムのクライアントでは、変更を許可しないように設定する。 ・本稼働用クライアントのロールは必ず「本稼働」に設定する。また、本稼働用クライアントでは保護レベルを最高度に設定(推奨値)する。 ・クライアントのロールを「本稼働」に設定しておく、運用時に変更が必要な一部のカスタマイズテーブル(換算レートや税額など)の変更が可能になる。	・トランザクション SCC4 を使い、各クライアントの属性を表示し、属性が推奨値になっているか確認する。 ・推奨値と異なっている場合、次の点を質し、妥当性を評価する。 ➢ 推奨値にしない理由 ➢ 推奨値にしないことによるリスクへの対応	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
			B	クライアント依存オブジェクトの変更と移送（推奨値「変更禁止」） ☐ 自動記録の無い変更 ☐ 変更の自動記録 ☐ 変更禁止 自動記録なしの変更、移送が不許可 クライアント非依存オブジェクトの変更（推奨値「リポトリとクライアント非依存カスタマイジング オブジェクトの変更なし」） ☐ クライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポトリオブジェクトの変更なし ☐ リポトリとクライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポトリとクライアント非依存カスタマイジング オブジェクトの変更許可 保護：クライアントコピープログラムと比較ツール（推奨値「保護レベル2：上書き不可、外部利用不可」） ☐ 保護レベル1：上書き不可 ☐ 保護レベル2：上書き不可、外部利用不可 ☐ 保護レベル0：制限なし CATTとeCATT 解指時の制限（推奨値「eCATTとCATT－不可」） ☐ eCATT－許可、FUN／ABAPとCATT－不可 ☐ eCATT－許可、FUN／ABAPとCATT－‘認証済RFC’のみに対し許可 ☐ eCATTとCATT－‘認証済RFC’のみに対し許可 ☐ eCATTとCATT－許可 ☐ eCATTとCATT－不可 品質保証(QA)テスト用クライアントの属性 ロール（推奨値「テスト」） ☐ カスタマイジング ☐ デモ			

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
			B	☐ トレーニング／教育 ☐ 本稼動 ☐ SAP 参照 ☐ テスト クライアント依存オブジェクトの変更と移送 (推奨値「変更禁止」) ☐ 自動記録の無い変更 ☐ 変更の自動記録 ☐ 変更禁止 自動記録なしの変更、移送が不許可 クライアント非依存オブジェクトの変更 (推奨値「リポジットとクライアント非依存カスタマイジング オブジェクトの変更なし」) ☐ クライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポジットオブジェクトの変更なし ☐ リポジットとクライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポジットとクライアント非依存カスタマイジング オブジェクトの変更許可 保護:クライアントコピープログラムと比較ツール (推奨値「保護レベル2:上書き不可、外部利用不可」) ☐ 保護レベル1:上書き不可 ☐ 保護レベル2:上書き不可、外部利用不可 ☐ 保護レベル0:制限なし CATT と eCATT 解指時の制限 (推奨値「eCATT と CATT—許可」) ☐ eCATT—許可、FUN／ABAP と CATT—不可 ☐ eCATT—許可、FUN／ABAP と CATT—‘認証済 RFC’ のみに対し許可 ☐ eCATT と CATT—‘認証済 RFC’ のみに対し許可			

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				☐ eCATT と CATT－許可 ☐ eCATT と CATT－不可 開発(DEV)用クライアントの属性 ロール (推奨値「カスタマイジング」) ☐ カスタマイジング ☐ デモ ☐ トレーニング／教育 ☐ 本稼動 ☐ SAP 参照 ☐ テスト クライアント依存オブジェクトの変更と移送 (推奨値「変更の自動記録」) ☐ 自動記録の無い変更 ☐ 変更の自動記録 ☐ 変更禁止 自動記録なしの変更、移送が不許可 クライアント非依存オブジェクトの変更 (推奨値「リポジトリとクライアント非依存カスタマイジング オブジェクトの変更許可」) ☐ クライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポジトリオブジェクトの変更なし ☐ リポジトリとクライアント非依存カスタマイジング オブジェクトの変更なし ☐ リポジトリとクライアント非依存カスタマイジング オブジェクトの変更許可 保護:クライアントコピープログラムと比較ツール (推奨値「eCATT と CATT－不可」) ☐ 保護レベル1: 上書き不可	- 開発クライアントの属性を「変更の自動記録」に設定することは、非常に重要な設定である。このように設定することによって、カスタマイズ内容はすべて「変更依頼」に記録されるので、人為ミスによる移送漏れを防ぐことができる。 - プレイグラウンド クライアント(実験用クライアント)が存在する場合、クライアント非依存オブジェクトの「変更の自動記録」がオフであることを確認する。(理由: 変更記録をとっても使い道がなく、ゴミを記録することになる。) - カスタマイジングクライアントは、クライアントコピーで上書きされないように保護する。		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				☐ 保護レベル2: 上書き不可、外部利用不可 ☐ 保護レベル0: 制限なし CATT と eCATT 解指時の制限 (推奨値「eCATT と CATT—不可」) ☐ eCATT—許可、FUN/ABAP と CATT—不可 ☐ eCATT—許可、FUN/ABAP と CATT—‘認証済 RFC’ ☐ のみに対し許可 ☐ eCATT と CATT—‘認証済 RFC’ のみに対し許可 ☐ eCATT と CATT—許可 ☐ eCATT と CATT—不可	- カスタマイジング用クライアントでは、テスト作業を行うべきでない。従って、テスト支援トランザクションである eCATT と CATT を利用できないようにする。「eCATT と CATT—不可」 - 一方、単体・結合テスト用クライアントは「eCATT と CATT—許可」とする		
			A	本稼動クライアントの変更属性の変更をモニタリングしていますか? はい ☐ いいえ ☐	- 不正な変更等が実行されていないことを確認するため、変更ログを定期的にチェックする。 - 属性の変更依頼通りに、変更が実施されることが確認する。	トランザクション SCC4 を妥当な周期で実行し、変更ログをモニタリングしていることを確認する。	
7.		権限管理	A	<クライアントの登録・削除 権限> クライアントの登録・削除権限を持つのは誰(部署、役割)ですか? : <システム and/or クライアント属性の変更 権限> システム and/or クライアントの変更オプションを変更する権限を持つのは誰ですか(部署、役割)ですか? :		- クライアントの登録・削除に関連する下記トランザクションの実行権限を持つユーザー一覧を作成し、各ユーザの妥当性をチェックする ➤ SM30、 ➤ SCC1～SCC9 (クライアントコピー関連トランザクション) - 適切な周期で、トランザクション SCC3 を使用して移送ログのモニタリング、and/or SCC4 を使用して、クライアントの増減をモニタリングモニタリングしていることを確認する。	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				手続きは文書化され、周知徹底していますか はい ☐ いいえ ☐ 変更をモニタリングしていますか はい ☐ いいえ ☐ モニタリングの方法とタイミングを教えてください :			
8.		運用	B	複数の本稼働クライアントを使用する予定はありますか? はい ☐ いいえ ☐ そのクライアントについて説明してください。 : 手続きは文書化され、周知徹底していますか はい ☐ いいえ ☐ クライアントの登録・削除をモニタリングしていますか? はい ☐ いいえ ☐	1つのSAP本稼働システムで複数の本稼働クライアントを設定できますが、そのような環境では - クライアント非依存データに変更を加えるたびに、他のクライアントへの影響をテストする必要がある。 - クライアント非依存データに変更を加えた場合の移送管理におけるリスクが高まります。本稼働クライアントを1つの統合するようにします。		
9.			B	トレーニング用クライアントは開発システムや本稼働システムと分離されていますか はい ☐ いいえ ☐ 移送パスにトレーニングシステムは含まれていますか? はい ☐ いいえ ☐	- トレーニングクライアントと開発クライアントが同一システム上に存在すると、本稼働と同じ環境でのトレーニングはできません - トレーニングクライアントと本稼働クライアントが同一システム上に存在すると、トレーニングの実施が本稼働システムのパフォーマンス等に影響します。 - トレーニングクライアントは、品質保証機に置くようにします		
				トレーニング用クライアントへの移送手続き、手順は文書化され、周知徹底されていますか はい ☐ いいえ ☐	移送パスにトレーニングシステムが含まれていないと、本稼働システムと同じ環境でのテストができなくなる。		
				トレーニング用クライアントへの移送がモニタリングされていますか はい ☐ いいえ ☐			
10.			B	本稼働クライアントをコピーして開発クライアントまたは品質保証クライアントをリフレッシュする計画はありますか。あるいは過去に実施していますか? 開発クライアント	- 本稼働システムをコピーしてQAシステムをリフレッシュする場合がありますが、本稼働システムには機密データが格納されています。 - QAシステムでは、大きな権限を持つ開発者が作業していることを考慮すると、機密データをコピーした		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				目的は何ですか(何でしたか) ： はい ☐ いいえ ☐ 品質保証クライアント 目的は何ですか(何でしたか) ： はい ☐ いいえ ☐ 両方 目的は何ですか(何でしたか) ： はい ☐ いいえ ☐ コピー後、機密データをマスクするための特別な手順を実施しますか? はい ☐ いいえ ☐ その方法を説明してください ：	ままにしておくと、データ漏洩のリスクが高まります。 - したがって、コピーの後に機密データをクレンジングするための作業が必要となります。 - 本稼働システムをコピーすると、品質保証クライアントで行なう CATT/eCATT (Computer Aided Test Tool) で使用するアプリケーションデータにも影響がでる可能性も考慮する必要があります。 - 本稼働システムをコピーとして開発システムをリフレッシュすると、リポジトリオブジェクトの変更履歴とバージョン履歴がすべて消失してしまいます。 - その結果、アップグレード時に必要となる情報が失われてしまい、アップグレード時に多大な時間が必要となる。		
				これらの作業に関する手続・手順は文書化され、周知徹底されていますか はい ☐ いいえ ☐			
				これらの作業はモニタリングされていますか はい ☐ いいえ ☐			
11.	リモート接続	RFC接続	B	テストシステム、品質保証システムおよび他の本稼働システムから本稼働クライアントをターゲットにする RFC 宛先を登録していますか はい ☐ いいえ ☐ RFC 宛先を登録・変更できる権限を持つのは誰(責任部門、責任者)ですか ：	- レポート RSUSR002 (複合選択基準別ユーザ) を実行して、RFC 宛先の登録トランザクション SM59 の実行権限を持つユーザを確認する。 - セキュリティ監査ログの RFC によるログイン情報をモニタリングする (SM20)		ランドスケープ/クライアント管理の評価 レベル 0. 1. 2. 3. 4. 5
				RFC 宛先の登録・変更手順および規定書は文書化され、周知徹底されていますか ：			

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				RFC 宛先の登録・変更作業をモニタリングしていますか はい ☐ いいえ ☐	・		
12.	外部 OS コマンド	文書化 ／教育 モニタリング	A	外部 OS コマンド機能を利用していますか はい ☐ いいえ ☐ どのようなコマンドを登録していますか ： それらのコマンドを誰が使いますか どのような外部 OS コマンドが登録されていますか ： 外部 OS コマンドを登録できる権限を持つのは誰（責任部門、責任者）ですか ：	危険な OS コマンドが登録され、実行されると、OS レベルで不正にログオンされたのと同じリスクが発生する。	- 外部 OS コマンド更新 トランザクション SM69 を使用して登録されている OS コマンドを確認し、クリティカルなコマンド (DELETE など) がないか確認する - 外部 OS コマンド更新 トランザクション SM69 および、外部 OS コマンドを実行 トランザクション SM49 の実行権限を持つユーザを確認する。 トランザクション SM69、トランザクション SM49 の実行権限を持つユーザー一覧を作成し、各自の妥当性をチェックする	外部 OS コマンド管理の評価 レベル 0. 1. 2. 3. 4. 5
				外部 OS コマンドの登録・利用手順は文書化され、周知徹底されていますか ：			
				外部 OS コマンドの登録・変更をモニタリングしていますか はい ☐ いいえ ☐			
13.	クリティカルコマンド	文書化 ／教育	A	本稼動クライアントではクリティカルトランザクションをロックしていますか はい ☐ いいえ ☐ どのようなトランザクションをロックしていますか ：	- クリティカルトランザクションのロック：トランザクション SM01 - 本稼動クライアントでは、例えば次のようなトランザクション（一例）がロックされているか確認する - テーブルやビューの内容を直接照会/変更する機能を持つトランザクションの例 - SE11：ABAP ディクショナリ - SE15：オブジェクトナビゲータ (ABAP ワークベンチ) - SE16：データブラウザ - SE17：一般テーブル照会 - SE38：プログラム開発		クリティカルコマンド管理の評価 レベル 0. 1. 2. 3. 4. 5 （アクセスコントロールにおけるクリティカルコマンドに対するコントロールと併せて評価する）

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
					◇ SE8X : オブジェクトナビゲータ (ABAP ワークベンチ) ◇ SM30 : テーブルビュー管理 ◇ SM31 : テーブルビュー管理 ・ 運用環境の変更機能を持つトランザクション ◇ SPRO : カスタマイズパラメータの登録、更新 ◇ SE06 : システム環境設定 ◇ SU01 : トランザクションロックd ◇ RZ10 : プロファイルパラメータの更新 ・ 特殊な機能を提供するトランザクション ◇ SM49 : 外部コマンド実行 ◇ SM69 : 外部コマンド登録 ・ レポートプログラムを実行する機能を持つトランザクション ◇ SA38 : レポートプログラムを起動 ・ AIS (Audit Information System) を使ってロック済みトランザクションを評価します ・ S_ALR_87101283 - ロック済みトランザクション ・ クリティカルトランザクションのロック／ロック解除をシステム監査ログ機能を使ってモニタリングするようにします ・ システム監査ログフィルタ登録 : トランザクション SM19 ・ システム監査ログ照会 : トランザクション SM20		
				クリティカルコマンドの登録・利用手順は文書化され、周知徹底されていますか :	・		
				外部 OS コマンドの登録・変更をモニタリングしていますか はい ☐ いいえ ☐	・		

開発／保守チェックリスト

実施基準に記載されている「システムの開発・保守」に係わる監査人の留意事項

システムの開発・保守

監査人は、企業が財務報告に関連して、新たにシステム、ソフトウェアを開発、調達又は変更する場合、承認及び導入前の試験が適切に行われているかチェックする。
その際、監査人は、例えば、以下の点に留意する。

1. システム、ソフトウェアの開発、調達又は変更について、事前に経営者又は適切な管理者に所定の承認を得ていること
2. 開発目的に適合した適切な開発手法がシステム、ソフトウェアの開発、調達又は変更に際して、適用されていること
3. 新たなシステム、ソフトウェアの導入に当たり十分な試験が行われ、その結果が当該システム、ソフトウェアを利用する部門の適切な管理者及びIT部門の適切な管理者により承認されていること
4. 新たなシステム、ソフトウェアの開発、調達又は変更について、その過程が適切に記録及び保存されるとともに、変更の場合には、変更前のシステム、ソフトウェアに関する内部統制の整備状況に係る記録が更新されていること
5. 新たなシステム、ソフトウェアにデータを保管又は移行する場合に、誤謬、不正等を防止する対策が取られていること
6. 新たなシステム、ソフトウェアを利用するに当たって、利用者たる従業員が適切な計画に基づき、教育研修を受けていること

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
1	開発・保守に関する現状把握	リポジトリオブジェクトを開発・保守できる可能性のあるユーザーの確認	A	各システムに何人のプログラマが登録されていますか 開発システム： 品質保証システム： 本稼動システム： 本稼動システムにプログラマが登録されている場合、その存在を合理的に説明できますか	(解説1) SAP システムでは、プログラムやテーブル等(リポジトリオブジェクト)の追加・変更を厳しくコントロールするため、リポジトリオブジェクトを追加・変更できる条件として、次の2点を必須にしている。 ① そのユーザIDが開発・保守権限を保有 ② そのユーザIDに対するプログラマキーを取得し、該当システムに登録されている プログラマキーは、SAP サービスポータルにログインし、該当ユーザIDに対するプログラマキーを取得する。従って、プログラマキーの取得権限(=SAP サービスポータルにログインし、プログラマキーを取得する手続の実行権限)を厳重に管しなければならない。 (解説2) 開発システム以外(=品質保証テスト機、本稼動機)にプログラマが登録されている場合、特に本稼動システムに登録されている場合、リスク管理体制の不備が疑われる	- 監査対象システム上に、プログラムやテーブル等(リポジトリオブジェクト)の追加・変更が可能なユーザIDが登録されていないか確認し、監査の方針を決める。 (確認手順)登録されているプログラマ数をチェックする：ランドスケープを構成する各システム上で、トランザクション SE17 > テーブル名 DEVACCESS > 項目: Char20に X > 実行 - 登録されているプログラムをサンプリングして「プログラム登録申請書」などと突合し、該当プログラムの正当性、完全性、正確性、維持継続性をチェックする。 - 開発システム以外にプログラマ登録がされている場合、その理由を確認し、開発権限の管理と合わせて評価する。	
2	開発・保守されたリポジトリオブジェクトの確認	開発・保守されたリポジトリオブジェクトの確認	A	本稼動システムにはアドオン(追加開発)したリポジトリオブジェクトは幾つありますか トランザクション： ・ アドオントランザクションには権限オブジェクトが割当てられていますか はい ☐ いいえ ☐ プログラム： アドオンプログラムには権限チェックが組み込まれていますか はい ☐ いいえ ☐	大量のアドオンはリスクを高める。アドオンを必要最小限に抑える規定と、それが遵守される手順・体制が確立されていなければならない。	- 監査対象期間中に、監査対象システム上で、幾つのプログラムやテーブル等(リポジトリオブジェクト)が追加・変更(アドオン)されたか確認し、監査方針を決める。 (確認手順)トランザクション SE15 > オブジェクトの種類を選択 > 全選択 > オブジェクト名 Z*、Y* > 変更日付 From To を指定 > 実行 - 上記で確認したアドオンオブジェクトをサンプリングし、「機能拡張申請書」、「開発仕様書」、「テスト仕様書」、「テスト結果」などと突合し、該当オブジェクトの正当性、網羅性、	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				プログラム登録時に権限グループを割り当てていますか はい ☐ いいえ ☐ テーブル : アドオンテーブルは権限グループに割当てられていますか はい ☐ いいえ ☐ それらのアドオンオブジェクトの存在を合理的に説明できますか はい ☐ いいえ ☐		正確性をチェックする。 - アドオンされたトランザクションの定義に権限オブジェクトが設定されているかサンプリングテストする : (手順) トランザクション SE93 > 入力可能値でアドオントランザクション(Z*, Y*)を検索して実行 > 権限オブジェクト項目の値を確認 - アドオンプログラムに権限チェックが組み込まれていることをチェックする (手順)トランザクション S_ALR_87101287(統計プログラム分析) > レポート/汎用モジュール/Transactコードに対象オブジェクトの IDを指定 > ABAP 言語コマンド に“AUTHORITY-CHECK”を指定 > 実行 - アドオンプログラムがどの権限グループに属しているか(いないか)チェックする (手順) トランザクション SA38 > プログラム RSCSAUTH > 実行 > チェックしたいプログラムを指定して実行 - アドオンテーブルが権限グループに割当てられていることをチェックする (手順)トランザクション SE17 > テーブル名 TDDAT > エンタ > 項目:テーブル名に Z*, 項目:権限の出力に X > 実行	
3		モディ ファイ ケーション されたり ポジトリ オブ ジェクト の確認	A	本稼動システムにはモディフィケーションされたりポジトリオブジェクトは幾つありますか プログラム :	(解説)モディフィケーションは、SAP 標準プログラムを変更することを言う。モディフィケーションは、SAP システムの機能的な不適合性、セキュリティの弱体化を招く可能性があり、極力避けるべき行為である。 モディフィケーションを行う場合は、厳重なコントロール下で実施しなければならない。	監査対象システム上で、監査対象期間中に、幾つのプログラムやテーブル等(リポジトリオブジェクト)がモディフィケーションされたかチェックする。 (手順) モディフィケーションプログラム: トランザクション SE15	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				テーブル ： それらのアドオンオブジェクトの存在を合理的に説明できますか はい ☐ いいえ ☐		> プログラムライブラリ > プログラム > 全選択 > プログラム名 not Z*,Y* > 変更日付 From To を指定 > 実行 (手順) モディフィケーションテーブル: トランザクション SE15 > ABAPディクショナリ > データベーステーブル > 全選択 > テーブル名 not Z*,Y* > 変更日付 From To を指定 > 実行 モディフィケーションされたリポジトリオブジェクトをサンプリングし、機能拡張申請書、開発仕様書、テスト仕様書、テスト結果などと突合し、正当性、網羅性、正確性をチェックする	
4		標準オブジェクトをコピーして作成したオブジェクトの確認	A	SAP標準プログラムをコピーし、それを変更して利用しているプログラムはありますか はい ☐ いいえ ☐ そのプログラム本数は ： どのようなリスクを認識していますか ： それらのリスクをどのようにヘッジしていますか ：	(解説)「形式としての」モディフィケーションを避けるため、SAP 標準プログラムを導入企業固有名称(プログラム ID)にコピーした後、当該プログラムを変更する行為である。 これを実行した場合、もし、コピー元のプログラムに問題が発生し、SAPから修正パッチが提供されても、コピー先プログラムは名称変更が行われ、かつ、コードが変更されているため、修正パッチを適用することは困難になる。	- 監査対象システム上で、監査対象期間中に、幾つのSAP標準プログラムがコピーされ、変更されたかチェックする。 (手順) この行為を体系的に検出できる方法がSAPシステムに備わっていない。あまりにも危険な行為であり、本来このようなことが行われることを想定していないためと考えられる。 - この事例が有ることが分かった場合、リスクをどのようにヘッジしているかヒアリングし、評価する。	
5	カスタマイズ・アドオンプロセスの監査	文書化・教育	A	カスタマイズ・開発・保守に関する規程・手順が文書化されていますか はい ☐ いいえ ☐ それらの文書は教育等を通し、周知徹底されていますか はい ☐ いいえ ☐	- カスタマイズ・開発・保守申請を承認するための正式な手続が規定されており、それらが関係者に周知徹底されており、遵守されていないと認められない - 開発・保守申請フォームの承認とは、経営者が申請書に記載された機能拡張／変更を確認し、承認した	開発プロセスに関する規定・手順が定義され、文書化され、遵守されていることを、事前に関連書類を入手してチェックする。 <事前に提出を求める文書の例>	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				開発・保守申請フォームを定義し、使用していますか？ はい ☐ いいえ ☐ 「はい」の場合、開発・保守申請フォームには次のような項目が含まれていますか ☐ 申請部門、依頼者 ☐ 申請管理番号 ☐ 開発・保守が必要となった理由、原因、背景 ☐ 開発・保守するアプリケーション機能 ☐ 該当プログラム等の異常終了を含む緊急事態への対応／復旧機能 ☐ エンドユーザトレーニングの必要性和範囲 ☐ 会計データへの影響の有無 ☐ 想定される他機能への影響 ☐ 開発・保守対象コンポーネントとオブジェクト ☐ 開発・保守作業者名またはカスタマイズ設定者名 ☐ 単体テストの結果 ☐ ユーザ受入テスト(QA のテスト)の検収基準 ☐ ユーザ受入テスト(QA のテスト)の結果 ☐ 本稼働へのインポートを承認するためのユーザ部門の責任者の検収 ☐ 本稼働へのインポートを承認するための開発部門の責任者の検収 ☐ 本稼働へのインポートを承認するための運用部門の責任者の検収 ☐ インポートを実行したユーザ名とその日付 ☐ インポートリターンコード (台帳を兼ねる場合) ☐ 登録した 変更依頼 ID ☐ 移送依頼 ID	ことを証明することである。 - 開発・保守申請フォームの管理番号と SAP“変更依頼”、開発・保守内容、テスト内容、“移送依頼”ID 等を紐付けで管理し、申請書承認から本稼働システムへの移送完了(＝カットオーバー)までの監査証跡を一貫して追跡できるようにしなければならない。 - 開発・保守が必要となった原因が、インシデント／問題に起因する場合、問題管理番号とも紐付けて管理されていなければならない。	- 文書体系、管理体制 - カスタマイズ、開発・保守に関する規程・手順書 - 開発・保守申請フォーム - 開発・保守管理台帳：開発・保守申請が提出されていから、カットオーバーされるまでの経過(申請／承認 → 開発・保守 → テスト／承認 → 承認／本稼働システムへの移送)をトレースできるようになっているもの) - 上記のチェックを行い、現地でチェックする内容を決定する <チェック内容の例> - 規定・手順が教育等を通し、周知徹底され、遵守されていることの確認。	
6		運用	A	カスタマイズ・開発・保守申請を作成・提出することができるのは誰ですか。 ：		実施された、全てのカスタマイズ・開発・保守が申請され承認されていることをチェックする。 (手順) 移送ログ、開発・保守ログ	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				実施する、全てのカスタマイズ・開発・保守は承認されていますか はい ☐ いいえ ☐ カスタマイズ・開発・保守申請を承認することができるのは誰(部署、職責)ですか。 : 開発・保守申請の承認プロセスについて説明してください。 :		などをサンプリングし、開発・保守申請書等と突合し、承認印(サイン)をチェックする ● 承認者の妥当性をチェックする(手順) 組織図等と突合し、承認者の妥当性をチェックする	
7			B	カスタマイズ・開発・保守作業が開発・保守作業に関する規程・手順(方法論)に基づいて、おこなわれていますか はい ☐ いいえ ☐			
8			B	開発者(プログラマキー)登録の規程・手順は文書化されていますか はい ☐ いいえ ☐ 開発者キーを取得する権限を持つのはだれですか :	(解説) SAP システムでリポジトリオブジェクト(プログラム、画面デザイン、テーブル定義など)を変更するためには、開発権限と共に開発者キー(プログラマキー)の登録が必須。 ● SAP サービスポータルから開発者キーの取得できる者を限定するため、ユーザ ID とパスワードの管理を厳重に行います	● 開発者(プログラマキー)登録行為の正当性、網羅性、正確性をチェックする。	
9		モニタリング	B	カスタマイズ・開発・保守申請が提出されてから完了するまでのプロセスを監視していますか はい ☐ いいえ ☐ 監視プロセスを説明してください : 開発・保守申請フォームやその他監査証拠を管理するデータベースシステムはありますか? はい ☐ いいえ ☐ 使用しているフォームが紙書式の場合は、作業完了後そのフォームをどのように管理していますか? :		● カスタマイズ・開発・保守申請が承認されてからカットオーバーされるまでの証拠をトレースできるようになっていることをチェックする。 ● 申請書をサンプリングし、監査証拠をトレースする ● 開発・保守申請フォームやその他監査証拠が確実に管理されているかチェックする	
10	モディフィケーション	文書化・教育	A	モディフィケーションに関する規程・手順が文書化されていますか はい ☐ いいえ ☐ それらの文書は教育等を通し、周知徹底されていますか	(解説) ● モディフィケーションとは SAP 標準リポジトリオブジェクト(プログラム、画面、テーブル定義など)を変更することを言います。 ● SAP システムでは、モディフィケーションは許可しない	● モディフィケーションの承認は、代案をすべて検討し、SAP 拡張機能を使用できる可能性がないことを確認してから行うようにします。	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				はい ☐ いいえ ☐ モディフィケーションの申請フォームを定義し、使用していますか？ はい ☐ いいえ ☐ 「はい」の場合、モディフィケーションの申請フォームには、通常の開発・保守申請書の項目以外に次のような項目が含まれていますか ☐ モディフィケーション以外に代替案が無いことの説明 ☐ このモディフィケーションによって発生するリスク	方針を設定することが推奨されています。 - モディフィケーションを許す場合、管理が不十分だと現行システムに影響を与えるだけでなく、サービスパッケージ(障害の修正、法律改正等への対応、機能拡張などを行うためのパッチのセット)の適用、アップグレード作業に影響を与えるだけでなく、SAPシステムが本来備えている統制機能の低下／破壊に繋がることもある。 - SAP モディフィケーションを実行すると、アップグレード時や サービスパッケージ等の適用時に予期せぬ障害が発生する可能性がある。 - モディフィケーションの申請は「全社統制」の視点からも詳細に吟味し、拡張 機能 (ユーザ Exit またはカスタマ Exit) が利用可能か、そのモディフィケーションは全体最適の視点で本当に必要であるかなどについて確認する必要がある。 - サービスポータル から オブジェクトの 変更キーを取得する権限は、少数の人間に限定して付与するようにします。これにより、未承認のモディフィケーションの実施を制限することができます。 - モディフィケーションブラウザ(トランザクション SE95)を使ってモディフィケーションをモニタリングします。	- コーディング中のコメント文書が標準化され、カスタマイズ部分のコーディングがカプセル化されるようにルール化されていることを確認します。 - モディフィケーションは文書で依頼され、管理職によって承認されます。	
11		運用	B	モディフィケーション キー(SCCRキー)を取得する権限を持つのはだれですか ： モディフィケーション キーをどのようにして、開発者に知らせますか ：		- 各モディフィケーションをレビューし、ルールが順守されていることをチェックする。 - モディフィケーションを実施する場合は、モディフィケーションアシスタント(リリース 4.6 以降)が使われていることをチェックする。	
12		運用	A	実施する全てのモディフィケーションは適切な責任者による承認を得ていますか。 ： 承認を行う責任者(部署)は誰ですか ：		全てのモディフィケーション オブジェクトが、適切な責任者による承認を得て実施されたものであることをチェックする。	
13		モニタリング	B	モディフィケーションのレビュープロセスはありますか？ はい ☐ いいえ ☐		全てのモディフィケーションに対し、レビューを行っているかチェックす	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				そのレビュープロセスには何が含まれますか？ ：		る。	
14	テスト	文書化・教育	A	テスト規程・手順は文書化されていますか。 はい ☐ いいえ ☐ どのようなテストの分類がされていますか ☐ 単体(ユニット)テスト ☐ 結合テスト ☐ ユーザ受入テスト ☐ パフォーマンステスト その他 ： それらの文書は教育等を通し、周知徹底されていますか はい ☐ いいえ ☐ テストケースを定義するフォームはありますか？ はい ☐ いいえ ☐ テストケース フォームには、次の項目が含まれていますか ☐ テストの狙い、目的 ☐ テストケース作成者 ☐ テスト実施日 ☐ 入力データ ☐ 予測結果 ☐ 実際の結果 ☐ 検収者	- テスト中に発見された問題は、問題管理データベースに記録する。 - 各テスト単位に 完了基準を定義する必要があります。 - 開発システムにおけるテスト(単体、結合テスト)と品質保証システムにおけるテスト(統合テスト、ユーザ受入テスト)を 同じスタッフが行わないことが重要です。 - 開発・保守に関するテスト文書は、該当する変更依頼と関連付ける必要があります。 - エラーの修正なども、最初の変更依頼または修正依頼と関連付ける必要があります。 - 統合テストは、問題がなくなった時に完了します。しかしながら、全ての問題がなくなることはほとんどありません。そこで、統合テストの完了を判断する基準を設定しておく必要があります。そうしないと、完了について様々な解釈が行われ、延々と統合テストが続行されることとなります。	- テストに関する規定、手順が定義され、文書化されていることをチェックする。 - それらの規定が教育等を通して周知徹底されているかチェックする	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				テストケースを実行するのは誰ですか。 ： テスト中に発見された問題の管理手順は文書化されていますか。 はい ☐ いいえ ☐ 本稼動システムへのインポート依頼を承認するのは誰ですか。 ：			
15		運用	A	開発・保守、アップグレードを行なった場合、必ずユーザ受入テストを計画し実行していますか。 はい ☐ いいえ ☐ 「いいえ」の場合、どのようなときにユーザ受入テストを省略しますか ： ユーザ受入テストのテストケースを設定するのは誰ですか。 ： ユーザ受入テストの完了基準を定義していますか。 はい ☐ いいえ ☐ ユーザ受入テストの完了は適切な責任者によって承認されていますか はい ☐ いいえ ☐ ユーザ受入テストの検収責任者は誰ですか。 利用する部門 ： 開発・保守部門（IT部門） ： 運用部門（IT部門） ：	- 適切なユーザ受入テストは開発・保守プロセスのキーコントロールです - 開発・保守を申請したエンドユーザ（部門）が品質保証システムでのテストを担当する必要があります。	- 全てのカスタマイズ・登録・保守申請に対しエンドユーザ受入テストが実施され、適切な責任者によって承認されていることをチェックする。 - 実施基準では、 「新たなシステム、ソフトウェアの導入に当たり十分な試験が行われ、その結果が当該システム、ソフトウェアを利用する部門の適切な管理者及びIT部門の適切な管理者により承認されていること」	
16			B	テストケースには内部統制に関するテストが含まれてい	テストケースに内部統制に関するテストが含まれてい	テストケースに内部統制にかかわる	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				内部統制に関連し、どのようなテストを実行しますか。 ： テスト中に発見された問題点の管理をどのように行っていますか ：	ない限り、内部統制に関する確認が行われることはない。	項目が含まれていることをチェックする。	
17		モニタリング	B	テストが規定・手順に沿って実施されていることをモニタリングしていますか はい ☐ いいえ ☐ 何を、どのようにモニタリングしていますか ：		テストが規定・手順に沿って実施されていることをチェックする	
18	移送	文書化・教育	A	移送に関する規程・手順が文書化されていますか はい ☐ いいえ ☐ それらは教育等を通し、関係者に周知徹底されていますか はい ☐ いいえ ☐		- 移送に関する規定、手順が定義され、文書化されていることをチェックする。 - それらの規定が教育等を通して周知徹底されているかチェックする	
19		運用	A	本稼動システムへの移送は、ユーザ部門、およびシステム部門(開発部門、運用部門)の適切な責任者が全て承認したときにだけ実施していますか はい ☐ いいえ ☐ 本稼動の移送をコントロールするために、SAP 移送管理システム(STMS)の承認機能を利用していますか はい ☐ いいえ ☐ 利用していない場合、その理由を説明してください ：	(解説)実施基準では、次のように記述している。 「新たなシステム、ソフトウェアの導入に当たり十分な試験が行われ、その結果が当該システム、ソフトウェアを利用する部門の適切な管理者及びIT部門の適切な管理者により承認されていること」 すなわち、① 利用部門の適切な管理者、② IT 部門の適切な管理者 による承認を求めている。 ・	本稼動システムへの移送は、ユーザ部門、およびシステム部門(開発部門、運用部門)の適切な責任者が全て承認したときに実施していることをチェックする。 - 責任者による承認がないと本稼動システムへ移送ができないように設定されているかチェックする。 (手順) 移送承認の設定 : トランザクション STMS > 移送ルート > 品質保証システムの承認ボタンをクリック(承認ボタンが表示されていない場合、承認機能が設定されていない) - インポートのリターンコードが 0 よりも大きい場合は、責任者(または開発者)に通知されるようになってい	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
						ることをチェックする。 インポート後は、インポートの実行者名、インポートの日付と時刻、およびインポートリターンコードを開発・保守申請フォームに記入し、トレーサビリティが確保されていることをチェックする。	
20			C	“tp”コマンドを直接使用していますか。 はい ☐ いいえ ☐ “tp”コマンドは使用せず、移送管理システムを使用していますか？ はい ☐ いいえ ☐ チームメンバは SAP の移送管理システムを理解していますか？ はい ☐ いいえ ☐	(解説)古いリリースでは、オペレーティングシステムレベルで提供されている“tp”コマンドを使って移送を行っていた。様々なリスクを無くすため、新しいリリースでは、移送管理システムを使って移送を行うように改良されている。	- カスタマイズ、開発・保守結果を“tp”コマンドを使って移送していないことをチェックする。 “tp”コマンドを使って移送を行うケースがある場合、その理由と、リスクをどのようにヘッジしているか確認し、評価する。	
21		モニタリング	B	移送に関する規程・手順に基づいて、移送作業がおこなわれていることを監視していますか はい ☐ いいえ ☐ 監視プロセスを説明してください ： 移送をインポートした後、リターンコードをチェックしていますか？ はい ☐ いいえ ☐ 移送完了通知を誰に、どのように行っていますか？ 誰に ： 方法 ：	- 移送に誤りがあると、カットオーバー後、大きな問題が起きる。 - リターンコードをチェックする責任者を設け、移送の所有者に確実に通知する必要がある。	移送の実績を確認し、承認済みカスタマイズ、変更・保守申請と突合する (手順) 移送ログ照会(Aログ)：トランザクション S_ALR_87101261 移送ログ照会(Sログ)：トランザクション S_ALR_87101262	
22	緊急対応	文書化・教育	A	本稼動システムで緊急事態が発生した場合の、修正／テスト／インポート等の規定、手順は定義され、文書化されていますか		本稼動中に緊急事態が発生した場合の、修正／テスト／インポート等の規定、手順が定義され、文書化さ	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
				はい ☐ いいえ ☐ それらの規定は教育等を通して周知徹底されていますか はい ☐ いいえ ☐ 緊急事態が発生した場合の手順を説明してください :		れていることをチェックする。 それらの規定が教育等を通して周知徹底されているかチェックする	
23		運用	A	緊急時の対応は規程・手順に基づいて作業がおこなわれていますか はい ☐ いいえ ☐			
24		モニタリング	B	緊急時の対応が規程・手順に基づいて実施されていることを監視していますか はい ☐ いいえ ☐ 監視プロセスを説明してください :			
25	アップグレード	文書化・教育	B (注) 監査対象期間中にアップグレードが実	アップグレードに関する規程・手順は文書化されていますか はい ☐ いいえ ☐ 承認手続きを説明してください : 責任者(部署、責任者)はだれですか : アップグレードはどのように計画および開始されますか? :	ASAP(SAP 方法論)が提示するアップグレード手順を企業固有環境に合わせてカスタマイズして、アップグレード作業を行う	アップグレードを行なった後は、すべてのモディフィケーションをテストし、新リリースでも正確に動作することを確認します。	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
			施された場合 A ランク				
26		運用	B	どのような順序でシステムをアップグレードしますか？ ： どのシステムをつかってアップグレード結果をテストしますか？ ：	- 大規模なアップグレードプロジェクトでは、アップグレードテストシステムを導入することを検討します。 - 移送パスに合わせてシステムランドスケープをアップグレードします。		
27			B	アップグレード後のユーザトレーニングを計画していますか？ はい ☐ いいえ ☐	影響を受けるエンドユーザ全員を対象に、新機能または変更された手順に関するトレーニングを計画します。		
28		モニタリング	B	アップグレード規程・手順に基づいて実施されていることを監視していますか はい ☐ いいえ ☐ 監視プロセスを説明してください ：			
29	開発・保守権限の分離	文書化・教育	A	開発・保守権限の分離に関する規程・手順は文書化されていますか はい ☐ いいえ ☐ それらの文書は教育等を通し、周知徹底されていますか はい ☐ いいえ ☐ 開発・保守プロセスに係わる権限をどのように分離していますか ：	(解説) 開発・保守プロセスにおいては、次の権限が分離されていることが望ましい - 開発・保守を実施することに対する承認権限 「変更依頼」登録権限(ERP 権限) - 開発・保守実行権限(ERP 権限) - 変更依頼リリース権限(ERP 権限) - 移送承認権限(ERP 権限) - 移送実施権限(ERP 権限) このうち、「承認権限」、「開発・保守実施権限(ERP 権限)」、「移送権限(ERP 権限)」は分離されていなければならない。	- 開発・保守権限の分離に関する規程・手順が文書化されているかチェックする - それらの文書が教育等を通し、周知徹底されているかチェックする	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
30		運用	B	開発・保守権限分離(SoD)規定・手順に基づいて、権限の付与、変更を行っていますか はい ☐ いいえ ☐		開発・保守権限の分離に関する規程・手順に基づいて、開発・保守関連の権限付与が行われていることを証跡に基づいてチェックする。 <実査1: アドオンと移送の権限分離テスト> トランザクション SA38 > プログラム RSUSR002 実行 > 値による検索 権限オブジェクト1 S_TCODE SE10(変更依頼登録) AND 権限オブジェクト2 S_TCODE SE38(アドオン) AND 権限オブジェクト3 S_TCODE STMS(移送) <実査2: カスタマイズと移送の権限分離テスト> トランザクション SA38 > プログラム RSUSR002 実行 > 値による検索 権限オブジェクト1 S_TCODE SE10(変更依頼登録) AND 権限オブジェクト2 S_TCODE SPRO(カスタマイズ) AND 権限オブジェクト3 S_TCODE STMS(移送)	
31		モニタリング	B	開発・保守権限分離(SoD)規定に反する権限を持つユーザIDが登録されていないかモニタリングしていますか はい ☐ いいえ ☐ 「はい」の場合、どのようなタイミングでモニタリングしていますか : 監視プロセスを説明してください :		- プログラムの登録・保守の権限分離: 変更依頼の登録・リリース(トランザクション:SE10)、プログラムの開発・変更(トランザクション:SE38)、移送(トランザクション:STMS)の実行権限を併せ持つユーザがないことをチェックする。 - カスタマイズの権限分離: 変更依頼の登録・リリース(トランザクション:SE10)、カスタマイズ(トランザクション:SPRO)、移送(トランザクション:STMS)の実行権限(手順)レポートプログラム RSUSR002 を使用して、上記トランザクション(セット)の実行権限を	

項番	分類	区分	ランク	チェック内容	関係するリスク、統制・緩和方法等	監査手順、確認方法	評価
						持つユーザIDの有無を調べる	

アクセスコントロール チェックリスト

実施基準に記載されている「システムの安全性の確保」に係わる監査人の留意事項

システムの安全性の確保

監査人は、企業がデータ、システム、ソフトウェア等の不正使用、改竄、破壊等を防止するために、財務報告に係る内部統制に関連するシステム、ソフトウェア等について、適切なアクセス管理等の方針を定めているか確認する

参考 COBIT DS5 システムセキュリティの保証

レベル		内容
レベル0	不在	組織がITセキュリティの必要性を認識していない。セキュリティを確保するための実行責任と説明責任が割り当てられていない。ITセキュリティ管理を支援する対策が実施されていない。ITセキュリティに関する報告とITセキュリティ違反発生時にとるべき対応プロセスが存在しない。システムのセキュリティ管理プロセスと呼べるようなものがまったく存在しない。
レベル1	初期/その場対応	I組織がITセキュリティの必要性を認識している。セキュリティの必要性に関する意識は、主として個人に依存している。ITセキュリティへの取り組みは事後対応という形である。ITセキュリティの成果測定は行われていない。責任の所在が明確ではなく、ITセキュリティ違反が発見された場合、責任のなすり合いが起こる。ITセキュリティ違反への対応は予測できない。
レベル2	再現性はあるが直感的	ITセキュリティの実行責任と説明責任はITセキュリティに関する調整を担う担当者に課せられているが、この担当者には限られた管理権限しか与えられていない。セキュリティの必要性に関する意識は断片的で限定的である。セキュリティ関係の情報はシステムによって生成されているが、分析は行われていない。サードパーティが提供するサービスが、セキュリティに関する組織特有のニーズに対応していない可能性がある。セキュリティポリシーを策定中であるが、スキルとツールが不十分である。ITセキュリティの報告体制は、不完全で、誤解を招きやすく、適切ではない。セキュリティ研修が提供されているが、受講するかどうかは主に個人の自発性に委ねられている。ITセキュリティは主にIT部門の責任および分野であると見なされており、ビジネス部門側にITセキュリティが自己の責任分野であるとの意識がない。
レベル3	定められたプロセスがある	セキュリティに対する意識があり、マネジメント層もその向上を推進している。ITセキュリティ手続が定義され、ITセキュリティポリシーとの整合が図られている。ITセキュリティに関する責任が割り当てられ、理解されているものの、一貫した実行はなされていない。リスク分析に基づいたITセキュリティ計画とセキュリティソリューションがある。セキュリティに関する報告には、明確なビジネス的視点が含まれていない。セキュリティのテスト(侵入テストなど)は場当たり的に行われている。IT部門とビジネス部門の両方を対象にしたセキュリティ研修が提供されているが、計画と運営は非公式に行われているにすぎない。
レベル4	管理され、測定可能である	ITセキュリティの責任が明確に割り当てられ、管理、実行されている。ITセキュリティのリスクと影響に関する分析が、一貫して行われている。セキュリティポリシーと手続が、具体的なセキュリティ基準に従って実施されている。セキュリティ意識の向上に向けた取り組みには、全員の参加が義務付けられている。ユーザの識別や、認証、認可が標準化されている。セキュリティの監査や管理の責任を負うスタッフメンバーには、セキュリティ資格の取得が求められている。セキュリティテストは、正式な標準プロセスに従って実施され、それがセキュリティレベルの向上につながっている。ITセキュリティプロセスと組織全体のセキュリティ機能との調整が図られている。ITセキュリティに関する報告と、ビジネス目標との関連付けが行われている。ITセキュリティに関する研修が、ビジネス部門とIT部門の双方において行われている。ITセキュリティに関する研修が業務上の要請や文書化されたセキュリティリスク分析結果に対応する形で計画、管理されている。セキュリティ管理に対する目標と指標が定義されているが、測定までは行われていない。
レベル5	最適化	ITセキュリティはビジネス部門とIT管理部門の共同責任であり、企業のセキュリティに関するビジネス目標に組み込まれている。ITセキュリティ要件が明確に定義され最適化されており、承認されたセキュリティ計画に盛り込まれている。ユーザと顧客は、セキュリティ要件の定義に対してますます大きな説明責任を負い、設計段階からセキュリティ機能がアプリケーションに組み込まれている。セキュリティインシデントへの対応は、自動化ツールを利用した正式なインシデント対応手続に基づいて、迅速に行われている。定期的なセキュリティ評価が行われ、導入したセキュリティ計画の有効性が評価されている。脅威と脆弱性に関する情報が体系的に収集・分析されている。リスクを軽減するための適切なコントロールが直ちに伝達され、実施されている。セキュリティテスト、インシデントの根本的原因の分析、およびリスクを積極的に発見することで、継続的にプロセスを改善している。組織全体でセキュリティプロセスと技術の統合が図られている。セキュリティ管理の指標が測定および収集され、周知されている。マネジメント層はこれらの測定結果を用いて、セキュリティ計画を継続的に改善している。

A：ないと設計評価ができないもの。S O X対象業務の稼働環境、業務システムに対し直接的な改ざん、破壊につながるもの

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
1.	ユーザ管理	文書化・教育	A	ユーザ管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ ユーザIDの登録・変更・削除申請書式は定義され、使用されていますか はい ☐ いいえ 管理手順を説明してください ユーザIDの登録・変更・削除申請書を提出する権限があるのは誰(部署、役割)ですか : 申請書の承認を行なうのは誰(部署、役割)ですか : システム上に、ユーザIDの登録・変更作業を行うのは誰(部署、役割)ですか : 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役割)ですか : トレーニング等を通し、関連者にSAP ERPにおけるユーザIDの管理手順を周知徹底していますか はい ☐ いいえ ☐ それは、どのように実施していますか。説明してください。 :		【整備状況評価】 1. 一般ユーザIDに対する登録・修正・削除のルールを定めた規程等が存在し承認されていることを確認する。 【運用状況評価】 1. 一般ユーザIDの登録・変更・削除のログを抽出し、それに紐づく一般ユーザIDの登録・変更・削除の申請書を抽出する。	
2.			A	ユーザID登録/変更フォームはありますか? はい ☐ いいえ ☐ はいの場合、提出されたフォームを承認するのは誰ですか? : フォームには次のような項目が含まれていますか: ☐ ユーザタイプ ☐ 権限ロール ☐ 権限プロフィール	- ユーザIDの登録/変更フォームを規定します - このフォームには、少なくともユーザ名、所在地、電話番号、有効日付(一時ユーザの場合)、およびこのユーザがSAPシステムで実行する権限ロールを記入します - このフォームの提出には管理職の承認を必要とします。 (解説) ユーザタイプには、「ダイアログ」、「システム」、「通信」、		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				☐ 有効期限 ☐ 権限チェック用ユーザグループ ☐ ユーザグループ ☐ 個人情報 ☐ 通信 ☐ 開始メニュー ☐ 言語 ☐ デフォルト情報 ☐ パラメータ ☐ その他の項目 ユーザ ID を登録および変更する責任者は誰ですか？ : ユーザのロック解除とパスワードのリセットを行う責任者は誰ですか？ : ユーザのロック解除またはパスワードのリセットでは、文書による依頼を必要としますか？ はい ☐ いいえ ☐ 「いいえ」の場合、理由を説明してください :	「サービス」、「参照」がある。各タイプの役割はは、次の通り。 ダイアログ 'A' タイプ:ダイアログユーザは、すべてのタイプのログオンで1人が使用します。ダイアログログオン時には、失効パスワードと初期パスワードがチェックされ、パスワードの変更オプションが提供されます。多重ログオンはチェックされ、必要に応じてログに記録されます。 システム 'B' 内部的なシステム処理 (-> バックグラウンド処理) またはシステム関連の処理 (-> ALE、ワークフロー、TMS、CUA など) を行うには、システムユーザのタイプを使用します。ダイアログログオン (SAP GUI 使用) はできません。このタイプのユーザは、パスワード有効期間の一般設定からは除外されます。ユーザ管理者だけが、SU01 (ジャンプ-> パスワード変更) を使用してパスワードを変更することができます。 通信 'C' タイプ:通信のユーザは、システム間のダイアログを使用しない通信 (-> RFC または CPIC) 用に使用します。ダイアログログオン (SAP GUI 使用) はできません。パスワードの有効期間の一般設定は、このタイプのユーザに適用されます。このタイプのユーザは、ユーザ自身のパスワードを変更することができます (ダイアログユーザと同様)。パスワード変更のダイアログが、呼出元 (RFC/CPIC クライアント) によって提供されなければなりません。RFC 汎用モジュール USR_USER_CHANGE_PASSWORD RFC または RFC API 機能 RfcOpenEx() を使用してパスワードを変更することができます。 サービス 'S' タイプ サービスのユーザは、より大きいグループのユーザが匿名で利用可能なダイアログユーザです。通常、このタイプのユーザには、非常に限定された権限しか与えられません。たとえば、サービスユーザは ITS サービスや公開 Web サービスを使用した匿名システムアクセスに使用されます。ある個人が認証されると、サービスユーザを使用して匿名で開始されたセッションは、ダイアログユーザを使った個人セッションとして続行することができます (SUSR INTERNET USERSWITCH を参		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
					照)。ログオン時、システムは失効パスワードと初期パスワードのチェックを行いません。パスワードはユーザ管理者だけが変更できます。多重ログオンが許可されます。 参照 'L' サービスユーザと同様、参照ユーザも一般ユーザであり、特定の人間には割り当てられません。参照ユーザではログオンできません。参照ユーザは、追加権限を割り当てるためだけに使用されます。参照ユーザは、インターネットユーザに同一の権限を与えることを目的として導入されています。ロールタブでは、参照ユーザを指定してダイアログユーザに追加権限を割り当てることができます。通常、参照ユーザの割当はアプリケーションが制御します。参照ユーザの名称は変数を使って割り当てることができます。この変数の先頭は "\$" でなければなりません。参照ユーザへの変数の割当は、トランザクション SU_REFUSERVARIABLE を使用して行います。この割当は、CUA ランドスケープの全システムに適用されます。割り当てられた参照ユーザがいずれかの CUA 子システムに存在しなかった場合、割当は無視されます。		
3.		命名規則	A	ユーザID および ユーザグループIDの命名規則は文書化されていますか はい ☐ いいえ ☐ 命名規則を説明してください。 ユーザグループ: : ユーザID: :	・ ユーザID やユーザグループID の命名規則が定められ、その規則に従って、登録が行われていなければならない ・	【整備状況評価】 1. ユーザIDやグループIDの命名規則が規程等に定められていることを確認する。 2. 台帳管理しているグループIDとシステムから出力したグループIDの一覧表の整合性を確認する。 3. 台帳管理しているユーザID一覧（権限を含む）とシステムから出力したユーザID一覧（権限を含む）との整合性を確認する。	
4.		RFC宛先（ユーザ）	B	本稼動クライアントにログオン可能なRFC宛先のリスクを認識していますか はい ☐ いいえ ☐ 本稼動クライアントにログオン可能なRFC宛先が周辺システムに登録されないために、どのようなコントロールをしていますか :	・ 本稼動システムにログオンできる RFC 宛先が他のシステム／クライアントに登録されていると、その RFC 宛先を使って、本稼動システムに不正にログオンされてしまう危険性が高くなります。 ・ 本稼動システムにログオンできる RFC 宛先の登録が不可避なばあい、其の宛先を不正に使用できないようにコントロールする必要があります。		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				本稼働クライアントにログインできるRFC宛先が登録されないことをどのようにしてチェックしていますか ：			
5.		運用	B	ユーザに初期パスワードをどのように伝えていますか？ ： 初期パスワードの安全性はどのように確保しますか？ ：	- パスワードは電話で伝えないで、安全な方法でつたえるようにします。電話でユーザの身元を常に確認できるとは限りません。 - 他人の初期パスワードを使用してシステムにログインするのを不可能にします。初期パスワードはそのまま長期間放置できないようにプロファイルパラメータを設定します。 - 初期パスワードの有効期限をプロファイルパラメータで設定します。		
6.		ユーザIDの整理	A	退社した従業員や、担当プロジェクトが終了したコンサルタントのユーザIDを削除する手順はありますか？ はい ☐ いいえ ☐ 手順を説明してください ：	- 退社した従業員や、担当プロジェクトが終了したコンサルタントのユーザIDを削除する手順を定義する必要があります。 - たとえば、人事部門は、退社した全 SAP ユーザの週間レポートを SAP 管理者に通知するようにします。 - 長期間ログインしていないユーザを定期的に確認し、理由を調査します。 - 登録されているすべての一時ユーザの有効期限を設定し、一時ユーザが契約終了後も有効なまま残る可能性を減らします。	NO1の【運用状況評価】の手続きで確認。	
7.		パスワードセキュリティ	B	見破られ易いパスワードの使用を禁止していますか はい ☐ いいえ ☐	- ありふれたパスワードや推測しやすいパスワードは使用させないようにします。これらのパスワードを テーブル USR40 に登録しエンドユーザが使用できないようにします。 テーブル USR40 に登録するパスワードの例として、会社名やプロジェクト名などが考えられます。		
8.		ユーザメニュー	B	エンドユーザには「ユーザメニュー」だけを表示するように制限していますか はい ☐ いいえ ☐	テーブル USERS_SSM に、ユーザIDを登録し「ユーザメニュー項目」にだけチェック(✓)を付けます - セキュリティ監査ログを使って、「権限のないトランザクションの実行」をモニタリングする場合、この処置は重要です。		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価																												
11.			A	ユーザ管理に関連する下記プロファイルパラメータは適切に設定してありますか。 (注意: パラメータはリリースによって異なるものがあるので注意。 本チェックリストの最終 2 ページの記述を確認の事) プロファイルパラメータの一覧作成 : トランザクション SA38 > プログラム RSPFPAR または RSPARAM を 起動し 第一画面の“☐ プロファイルパラメータ照会” に✓を付けて実行 <table><thead><tr><th>パラメータ ID</th><th>役割</th><th>チェック事項</th><th>ランク</th></tr></thead><tbody><tr><td>login/disable_multi_gui_login</td><td>多重ログオンを無効化します。 このパラメータを 1 にセットすると、R/3 システムへの多重ログオン(同一のクライアントに同一のユーザ名でログオンすること) はシステムによって禁止されます。 システムが多重ログオンを検出した際に、“現在のセッションを強制終了する” もしくは “このログオンを強制終了する” というオプションを持つダイアログボックスが表示されます。 このパラメータは SAPGUI ログオンでだけ機能します。</td><td>無効に設定されている</td><td></td></tr><tr><td>login/failed_user_auto_unlock</td><td>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します。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に自動解除されます。 値を 0 にすると、ロックの自動解除は行われなくなります</td><td>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</td><td>A</td></tr><tr><td>login/fails_to_session_end</td><td>1 ユーザ 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ます。 デフォルト=3、値の範囲=1~99</td><td>3回程度に設定されている</td><td>A</td></tr><tr><td>login/fails_to_user_lock</td><td>何回ログオンを失敗するとユーザ ID をロックするか指定します</td><td>6回程度に設定されている</td><td>A</td></tr><tr><td>login/min_password_diff</td><td>ユーザが自身のパスワードを変更する場合、新規パスワードにおいて、旧パスワードと異ならないなければならない文字の数を指定します。 このパラメータは、新規ユーザの登録時、またはパスワードのリセット時(==> 初期パスワード)には影響を及ぼしません</td><td>最短パスワード長の半分程度の長さが設定されている</td><td>A</td></tr><tr><td>login/min_password_digits</td><td>パスワードに含まれる「数字」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 小桁数 (0-9) が設定されます このパラメータは新規パスワードの割当 よびパスワードの変更/リセットの両方に対して 効です。 有効</td><td>(解説) 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。</td><td>A</td></tr></tbody></table>	パラメータ ID	役割	チェック事項	ランク	login/disable_multi_gui_login	多重ログオンを無効化します。 このパラメータを 1 にセットすると、R/3 システムへの多重ログオン(同一のクライアントに同一のユーザ名でログオンすること) はシステムによって禁止されます。 システムが多重ログオンを検出した際に、“現在のセッションを強制終了する” もしくは “このログオンを強制終了する” というオプションを持つダイアログボックスが表示されます。 このパラメータは SAPGUI ログオンでだけ機能します。	無効に設定されている		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します。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に自動解除されます。 値を 0 にすると、ロックの自動解除は行われなくなります	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	A	login/fails_to_session_end	1 ユーザ 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ます。 デフォルト=3、値の範囲=1~99	3回程度に設定されている	A	login/fails_to_user_lock	何回ログオンを失敗するとユーザ ID をロックするか指定します	6回程度に設定されている	A	login/min_password_diff	ユーザが自身のパスワードを変更する場合、新規パスワードにおいて、旧パスワードと異ならないなければならない文字の数を指定します。 このパラメータは、新規ユーザの登録時、またはパスワードのリセット時(==> 初期パスワード)には影響を及ぼしません	最短パスワード長の半分程度の長さが設定されている	A	login/min_password_digits	パスワードに含まれる「数字」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 小桁数 (0-9) が設定されます このパラメータは新規パスワードの割当 よびパスワードの変更/リセットの両方に対して 効です。 有効	(解説) 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。	A		【整備状況評価】 各パラメータ設定内容を確認する。	
パラメータ ID	役割	チェック事項	ランク																																
login/disable_multi_gui_login	多重ログオンを無効化します。 このパラメータを 1 にセットすると、R/3 システムへの多重ログオン(同一のクライアントに同一のユーザ名でログオンすること) はシステムによって禁止されます。 システムが多重ログオンを検出した際に、“現在のセッションを強制終了する” もしくは “このログオンを強制終了する” というオプションを持つダイアログボックスが表示されます。 このパラメータは SAPGUI ログオンでだけ機能します。	無効に設定されている																																	
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します。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に自動解除されます。 値を 0 にすると、ロックの自動解除は行われなくなります	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	A																																
login/fails_to_session_end	1 ユーザ 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ます。 デフォルト=3、値の範囲=1~99	3回程度に設定されている	A																																
login/fails_to_user_lock	何回ログオンを失敗するとユーザ ID をロックするか指定します	6回程度に設定されている	A																																
login/min_password_diff	ユーザが自身のパスワードを変更する場合、新規パスワードにおいて、旧パスワードと異ならないなければならない文字の数を指定します。 このパラメータは、新規ユーザの登録時、またはパスワードのリセット時(==> 初期パスワード)には影響を及ぼしません	最短パスワード長の半分程度の長さが設定されている	A																																
login/min_password_digits	パスワードに含まれる「数字」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 小桁数 (0-9) が設定されます このパラメータは新規パスワードの割当 よびパスワードの変更/リセットの両方に対して 効です。 有効	(解説) 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。	A																																

項番	分類	区分	ランク	チェック内容		関係するリスク・統制・緩和方法等		監査手順・確認方法	評価
					な入力、書式、範囲：0-8	このパラメータの値が、1文字以上に設定されていることを確認する			
				login/min_password_letters	パスワードに含まれる「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文字の最小数が設定されます。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す。 有効な入力、書式、範囲：0-8	同上	A		
				login/min_password_specials	パスワードに含まれる「特殊文字」の最小数 このパラメータによりパスワードに含まなければならない特殊文字の最小数が設定されます。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す。特殊文字=(!¥"@%&/()=?`^*~#_.,:;[]{}¥%<> "), 有効な入力、書式、範囲：0-8	同上	A		
				login/min_password_uppercase (リリース依存)	パスワードに含まれる大文字数の最小値 このパラメータにより、パスワードに含まれる大文字数の最小値が規定されます。 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またはリセットに影響を及ぼします プロファイ login/password_downwards_compatibility に5という値が設定されている場合、このパラメータは評価されません 単位：大文字 (A-Z) の数	同上	A		
				login/min_password_lower_case (リリース依存)	パスワードに含まれる小文字数の最小値 このパラメータによりパスワードに含まれる小文字の数の最小値が規定されます。 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またはリセットに影響を及ぼします。 プロファイ login/password_downwards_compatibility に値“5”が設定されている場合、このパラメータは無効になります。 単位：小文字 (a-z) の数	同上	A		
				login/min_password_length	ログオンパスワードの最低の長さ指定	6以上に設定されていること	A		
				login/multi_login_user	多重ログオンが許可されたユーザのリスト	ユーザIDが登録されてい			

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				s このリストには、システムへの多重ログオンが許可された R/3 ユーザの ID (クライアント未指定) を含みます。 このプロファイルパラメータは、ダイアログユーザのみに適用されます	いことを確認する		
				login/no_automatic_user_sapstar コーディングレベルで存在する特殊ユーザ“SAP*”を無効化する	無効化されていることを確認する	A	
				login/password_compliance_to_current_policy ユーザパスワードをパスワードルールに照らしてチェックするかどうかを指定 値 0: チェックなし 値 1: パスワード変更が必要かどうかをチェック タイプが“SERVICE” および“SYSTEM”であるユーザは原則的にパスワード変更要件から除外されるためこのパラメータの影響を受けません。 変更されたパスワード規則は過去のパスワードには該当しません。パスワード規則はパスワード変更が行われる際にのみ評価されます。 NetWeaver 7.0 以降では、特定のユーザに対しパスワードを早期に変更するよう明確に指示することができます。これには、パスワードが現在のパスワード規則に準拠していないユーザが該当します (ノート 862989)	登録済ユーザIDのパスワードを、新しく設定したパスワードルールに照らしてチェックを行い、ルールに合わない場合、パスワードの変更を要求するように設定されていることを確認する。(値=1)		
				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ります	1ヶ月程度に設定されていることを確認する。		
				login/password_max_jd_initial (リリース依存) 未使用初期パスワードの有効期間 ユーザ管理者が新しいユーザIDを登録した場合、または、既存のユーザIDのパスワードを変更した場合、ユーザは次のログオン時にそのパスワード(初期パスワード)を変更しなければなりません (ユーザ自身のみが自分のパスワードを知っていることを保証するため)。 パスワードをリセットした後、初期パスワードを使用してログオンするまでの期間の最大値を設定します。この期間が経過すると、メッセージ “The initial password has expired; request a new one” が表示されてログオンは拒否されます	1ヶ月程度に設定されていることを確認する。		
				login/password_max_jd_productive (リリース依存) 未使用の実パスワードの有効期間 ユーザが自分自身のパスワードを変更すると“実”パスワードが登録されます。このユーザが自分の	1ヶ月程度に設定されていることを確認する。		

項番	分類	区分	ランク	チェック内容		関係するリスク・統制・緩和方法等			監査手順・確認方法	評価
					パスワードを変更できるのは、早くとも login/password_change_waittime によって指定した日数を過ぎた後に限られます。 パラメータ login/password_expiration_time により、何日経過した後でシステムがユーザに対してパスワードの変更を要求するかを指定します。 このパラメータを使用して、変更したパスワードの有効期間を設定することができます。新パスワードでログオンしないまま、この期間を経過するとそのパスワードは無効になります。メッセージ “Password was not used for a long period and therefore deactivated” が表示され、ログオンが拒否されます。					
				login/password_max_new_valid（リリース依存）	新規登録ユーザ用パスワードの使用期限 ユーザ管理者は、新規ユーザの登録時に初期パスワードを 割り当てます。 このプロファイルパラメータを使用して、ユーザ ID を登録した時点から、ユーザが最初に ログオンする時点までの最長期間を設定します。この期間を過ぎると、“初期パスワードが期限切れになりました” という メッセージが表示され、ログオンが拒否されます。 値 0: 初期パスワードは無期限の期間に対して有効 値 1: 初期パスワードは同一日についてののみ有効 それ以外: 指定日数を過ぎると、ユーザは初期パスワードでログオンできなくなります。	1ヶ月程度に設定されていることを確認する。				
				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します。 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必要度は低い				
12.		モニタリング	A	セキュリティ監査ログを取り、次のような項目を監視していますか ☐ ユーザのログオフ ☐ 正常にログオンしました (タイプ=&A) ☐ ログオンに失敗しました (理由 = &B、タイプ = &A) ☐ 多重ログオンに失敗しました (理由 = &B、タイプ = &A) ☐ ユーザ &B がクライアント &A でパスワードチェックに失敗した後でロックされました ☐ ユーザ &B がクライアント &A で無効パスワード入力によ		赤字で記載されたものは ランク A ・ 頻繁にログオンに失敗しているログが有る場合、不正なログオ、ンが試みられている可能性があります。 ・ 入社・退社情報と、ユーザIDの登録・変更ログを付き合わせ、妥当性をチェックする必要があります			【整備状況評価】 1. 規程等にセキュリティ監査ログのモニタリングルールが定められていることを確認する。 【運用状況評価】 2. セキュリティ監査ログのモニタリング記録を確認する。	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				るロックを解除されました ☐ RFC/CPIC ログオンに成功しました (Type = &A) ☐ RFC/CPIC ログオンに失敗しました (理由 = &B、タイプ = &A) ☐ クライアント &A のユーザ &B のパスワードが変更されました ☐ ユーザ &A が削除されました ☐ ユーザ &A がロックされました ☐ ユーザ &A がロック解除されました ☐ ユーザ &A の権限が変更されました ☐ ユーザマスタレコード &A が変更されました			
13.	特権ユーザの管理	文書化・教育	A	特権ユーザ管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ 管理手順を説明してください 特権ユーザ ID の登録・変更・削除申請書を提出する権限があるのは誰(部署、役割)ですか ： 申請書の承認を行なうのは誰(部署、役割)ですか ： システム上に、特権ユーザ ID の登録・変更作業を行うのは誰(部署、役割)ですか ： 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役割)ですか ： トレーニング等を通し、関連者に特権ユーザIDの管理手順を周知徹底していますか はい ☐ いいえ ☐ それは、どのように実施していますか。説明してください。 ：	(解説) 特権ユーザ(＝高度な権限を持つユーザ)は、様々な手段でシステムおよびアプリケーションデータを改竄できるので、管理を厳重に行う必要がある	【整備状況評価】 1. 規程等に特権ユーザの管理ルールが定められていることを確認する。 【運用状況評価】 1. セキュリティ監査ログより「特権ユーザの登録・削除を抽出し、それに紐づく特権ユーザの登録・変更・削除の申請書を抽出する。	
14.		SAP	A	SAP 標準特権ユーザのパスワードはすべてのクライアントで変	(解説)	<チェック方法>	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
		標準特権ユーザ		更されていますか？ ➤ DDIC (すべてのクライアント): はい ☐ いいえ ☐ ➤ SAP* (すべてのクライアント): はい ☐ いいえ ☐ ➤ EARLYWATCH (066): はい ☐ いいえ ☐	SAP システムの導入等のクリティカルな作業を実施するために、予めシステムに登録されているユーザを標準ユーザと呼んでいる。このユーザは、その役割上を全権を持っている。 ・	プログラム RSUSR003を起動し、第一画面の“ロプロファイルパラメータの紹介”のチェックをはずし、実行ボタンを押す。 処理結果として、クライアント毎に標準特権ユーザのパスワード変更状況一覧が表示される。	
15.			A	ハードコーディングされた SAP* を無効に設定していますか？ はい ☐ いいえ ☐	・	<チェック方法> プロファイルパラメータ ogin/no_automatic_user_sapstar = 1 (ハードコーディングされた SAP* を無効にする) セキュリティの向上を図るため、このパラメータが“1”に設定されていることをチェックする。	
16.		SAP_ALLを持つユーザ	A	システム内に 権限プロファイル SAP_ALL を持つユーザは存在しますか？ はい ☐ いいえ ☐ 権限プロファイル SAP_ALLを持つユーザの数: : 今後どのように“SAP_ALL”権限を持つユーザの整理方針を説明してください :	(解説) 権限プロファイル “SAP_ALL” をユーザに割り当てると、そのユーザは全権を行使することができる。従って、特殊な役割を果たすユーザ以外に、この権限プロファイルを与えてはならない。	・ SAP_ALL 権限を持つ一般ユーザがシステムに登録されていないことをチェックする。 ・ システム管理者は、必要に応じて自分自身に SAP_ALL を与える権限を持つ必要がある場合があるが、不要になった時点で、直ちに除去するようにしているかチェックする。 <チェック方法> ・ 権限プロファイル SAP_ALL を持つユーザの検索 : トランザクション S_BCE_68001395 - プロファイル別ユーザ > プロファイル名に “SAP_ALL” を指定して実行(または、: トランザクション SUIM > ユーザ情報システム > ユーザ > 複合選択基準ユーザ > プロファイル別 > プロファイル名に “SAP_ALL” を指定して実行)	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
17.	権限管理	文書化・教育	A	権限管理に関する管理規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ (権限)ロール、プロフィール、オブジェクト、値の登録・変更・削除申請書フォートはありますか はい ☐ いいえ 管理手順を説明してください (権限)ロール、プロフィール、オブジェクト、値の登録・変更・削除申請書を提出する権限があるのは誰(部署、役割)ですか ： 申請書の承認を行なうのは誰(部署、役割)ですか ： システム上に、権限の登録・変更作業を行うのは誰(部署、役割)ですか ： 権限をユーザに割り当てることができるのは誰ですか ： 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役割)ですか ： 管理規定・手順等をトレーニング等を通し、関係者に周知徹底していますか はい ☐ いいえ ☐ トレーニング等は、どのように実施していますか。説明してください。 ：		【整備状況評価】 1. SAP上の権限一覧とそれを誰に割り当てるかのルールを定めたドキュメントが存在し、承認されていることを確認する。 2. 規程等に権限の登録・変更・削除のルールが定められていることを確認する。	
18.		権限定義の開発・移送	A	開発システム上で ロールを登録／変更し、品質保守システムで品質確認テストを行ない、本稼動システムに移送するようにしていますか？ はい ☐ いいえ ☐ システム上でロールを登録・変更・削除するのは誰(部門)ですか？	他のリポジトリオブジェクト同様、3システムランドスケープを使って開発・テストを実施します。これにより、権限の詳細なテストが可能です。		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				: 登録・変更したロールのテストを実施し、承認するのは誰(部門)ですか : 権限の移送を承認するのは誰(部門)ですか :	- ユーザ受入テストは本稼働システムで使用する権限を使用して実行するようにします。 - 権限を慎重にテストしないと本稼働に移行後、問題が発生する可能性が高くなります。		
19.		モニタリング	A	権限の登録、変更、削除が適切に行われていることをモニタリングしていますか はい ☐ いいえ ☐ どのようにモニタリングしていますか : セキュリティ監査ログを取り、次のような項目を監視していますか ☐ 権限/権限プロファイル &B が登録されました ☐ 権限/権限プロファイル &B が削除されました ☐ 権限/権限プロファイル &B が変更されました ☐ ユーザ &A が登録されました ☐ 権限/権限プロファイル &B が有効化されました		【運用状況評価】 1. 権限の登録・変更・削除のログを抽出しそれに紐づく申請書を抽出する。	
20.	緊急対処	ユーザID	A	緊急時における、パスワードの変更、ユーザロックの解除、権限の追加などの管理規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ ☐ 緊急対応を申請する書式は定義され、常に使用されていますか はい ☐ いいえ ☐ 緊急対応手順を説明してください 緊急対応申請書を提出する権限があるのは誰(部署、役割)ですか : 申請書の承認を行なうのは誰(部署、役割)ですか :		【整備状況評価】 1. 規程等に緊急時におけるパスワードの変更、ユーザロックの解除、権限の追加等のルールが定められていることを確認する。 【運用状況評価】 1. 障害報告等の台帳より案件を抽出しパスワードの変更、ユーザロックの解除、権限の追加等がルール通り行われていることを確認する。	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
				システム上で緊急対応を行うのは誰（部署、役割）ですか ： 作業結果を申請書に基づいて確認（モニタリング）するのは誰（部署、役割）ですか ： トレーニング等を通し、緊急時の対応手順、管理手順等は定義されていますか はい ☐ いいえ ☐ それは、どのように実施していますか。説明してください。 ：			
21.	緊急対処		A	夜間緊急時など、やむを得ず本稼働システム上で権限の登録・変更を行うことはありますか？ はい ☐ いいえ ☐ 「はい」の場合、どのようにしてリスクを低減していますか ：	・ 本稼働システムで行う権限の登録・変更は、すべて「権限の登録・変更依頼書」を使って申請し、責任者による承認を受けたあと実行しなければなりません。 ・ 本稼働システム上で権限を直接変更した場合、同様の変更を品質保証システムおよび開発システム上で実施しないと、各システムの同期がとれなくなります。 ・ 文書が常に最新の状態を保つように権限の変更履歴をすべて記録します。		
22.	緊急対処	監視	A	緊急対処結果をモニタリングしていますか はい ☐ いいえ ☐ 「はい」の場合、			
23.	SoD	アクセスコントロールのSOD	A	権限管理に係わる次の3つ権限を分離していますか？ ・ ユーザを登録する権限 ・ 権限を登録・変更する権限 ・ ユーザに権限を割り当てる権限 はい ☐ いいえ ☐ 「いいえ」の場合、次の2つの権限を分離していますか ・ ユーザを登録する権限 ・ ユーザに権限を割り当てる権限 はい ☐ いいえ ☐ 上記で、「いいえ」と答えた場合、リスクをどのように軽減していますか？ ：	（解説） 権限ロールを登録する権限とそれをユーザIDに割当てる権限を持つユーザは、全権限を持っているのと同じであり、リスクが大きい		

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
24.	OS／DBMSのアクセスコントロール	文書化・教育	B	OSおよびDBMS ユーザの管理に関する規定・手順等は文書化され、関係者に周知徹底されていますか はい ☐ いいえ OSおよびDBMS ユーザ／権限の登録・変更・削除申請書式は定義され、使用されていますか はい ☐ いいえ 管理手順を説明してください 申請書を提出する権限があるのは誰(部署、役割)ですか : 申請書の承認を行なうのは誰(部署、役割)ですか : システム上で登録・変更・削除作業を行うのは誰(部署、役割)ですか : 作業結果を申請書に基づいて確認(モニタリング)するのは誰(部署、役割)ですか : トレーニング等を通し、関連者に管理手順を周知徹底していますか はい ☐ いいえ ☐ それは、どのように実施していますか。説明してください。 :	・	(注) 今回、SAPシステムの監査リストの作成を中心としているのでランク“B”としたが、IT全般統制の中では“A” 【整備状況評価】 1. 規程等にOS、データベースへアクセスするためのユーザIDの登録・変更・削除のルールが定められていることを確認する。 【運用状況評価】 OS、データベースの登録・変更・削除のログを抽出し、それに紐づく申請書等が存在していることを確認する。	
25.		運用	B	オペレーティングシステムにログオンできるユーザの一覧はあります はい ☐ いいえ ☐ それらのユーザが異動または退社した場合、直ちに削除または、パスワードを変更する手順はありますか はい ☐ いいえ ☐ その管理手順を説明ください。 :	・ オペレーティングシステムレベルへのアクセスが可能なユーザは、システムおよびデータベースにアクセスする大きな権限を持ちます。これらのユーザの一覧を作成・管理し、該当ユーザが退社／異動した時には、迅速に削除またはパスワードを変更する手順を文書化し、運営を行ないます。 ・ 可能な限り、SAP 標準ユーザ以外のユーザはオペレーティングシステムレベルで定義しないでください。どうしても必要な場合、これらのユーザの権限は限られたものにし、データベースアクセスは絶対に許可しないようにします。	(注) 今回、SAPシステムの監査リストの作成を中心としているのでランク“B”としたが、IT全般統制の中では“A” 【整備状況評価】 1. OSにログオンできるユーザIDの一覧が整備され承認されていることを確認する。 2. 台帳管理されているOSにログオンできるユーザIDの一覧とシステムから出力したユーザIDの一覧が整合していることを確認する。	

項番	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順・確認方法	評価
					- オペレーティングシステムのユーザパスワードを定期的に変更する必要があります。 - 不正なログイン試行の有無について、オペレーティングシステムのログを定期的に確認してください。		
26.		運用	B	データベースにログオンできるユーザの一覧はありますか？ はい ☐ いいえ ☐ それらのユーザが異動または退社した場合、直ちに削除または、パスワードを変更する手順はありますか はい ☐ いいえ ☐ その管理手順を説明ください。 ：	- 通常、SAP システムと同時にインストールした DBMS は SAP システムの運用目的以外で使用することは許されていません。 - 従って、SAP システムの運用に関するユーザ以外は、正当な理由が無い限り登録しないようにします - DBMS ユーザは、SAP システムが備える権限チェックを受けずに機密データにアクセスできません。 - DBMS ユーザ ID の一覧を作成し、その中のユーザの 1 人が異動または退社した場合、直ちに削除または、パスワードを変更する手順を確立する必要があります。	【整備状況評価】 1. データベースにログオンできるユーザIDの一覧が整備され承認されていることを確認する。 2. 台帳管理されているデータベースにログオンできるユーザIDの一覧とシステムから出力したユーザIDの一覧が整合していることを確認する。	
27.		モニタリング	B	不正なログイン試行の有無について、オペレーティングシステムのログを使って、定期的に確認していますか？ はい ☐ いいえ ☐		（注）今回、SAP システムの監査リストの作成を中心としているのでランク“B”としたが、IT 全般統制の中では“ A ” 【運用状況評価】 1. OSにログインしたログを抽出し、それに紐づく作業申請書等が存在することを確認する。 2. データベースにログインしたログを抽出しそれに紐づく作業申請書等が存在することを確認する。	

＜＜Web AS ABAP 7.00 または NetWeaver 2004s 以降の 改善点および変更点＞＞

■ 改善点

◆ パスワード:

大文字と小文字の区別、最大長の 8 桁から 40 桁への増加

新規パスワードでは、大文字と小文字が区別されます。さらに、パスワードに 40 桁まで含めることが可能になります（これまでは、最大長は 8 桁でした）。新しくインストールされたシステムでは、このルールは即時にすべてのユーザに適用されます。下位リリースから Web AS ABAP 7.00 または NetWeaver 2004s にアップグレードされたシステムでは、すべてのユーザは引き続き従来のパスワードを使用してログオンすることができます。ユーザマスタレコードに、そのユーザが新規のパスワードを使用しているのか、または古いタイプのパスワードを使用しているかの情報が格納されます。システムがパスワードをチェックする際に、この情報が分析されます。ユーザが古いタイプのパスワードを使用している場合は、パスワードの最初の 8 桁が大文字に変換され、残りの 32 桁はスペースとなります。このような処理が行われない場合、大文字への変換なしでパスワード全体が分析されます。ユニコードシステムでは、パスワードにユニコード文字を使用することができます。

関連する（新規）プロファイルパラメータ

- login/min_password_lowercase
- login/min_password_uppercase
- login/password_downwards_compatibility

◆ パスワード履歴: 必要に応じたサイズ定義（従来の制限は 5 エントリまで）

パスワード変更時にユーザが割り当てたパスワードは、パスワード履歴に格納されます（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ません）。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しないようにします。これまで、パスワード履歴は 5 エントリまでに制限されていました。今後は、プロファイルパラメータ (login/password_history_size) を使用して、パスワード履歴のサイズを定義することができます（最大 100 エントリ）。

◆ パスワード変更のロック期間の選択（従来の期間は 1 日間）

パスワード履歴が無視されないようにするため、ユーザはロック期間を経過した後でのみパスワードの再変更を行うことができます（例外: システムによってパスワードの変更が求められる場合）。プロファイルパラメータ login/password_change_waittime（最大値: 1000 日間）を使用して、ロック期間を選択することができます。

◆ （改善）より厳しいパスワードルールによるパスワード変更

現在のパスワードが現在の（厳しい）パスワードルールに沿っていないユーザに対してのみ、（あらかじめ）パスワードの変更が要求されるように設定することができます。これには、以下のプロファイルパラメータを設定します。

login/password_compliance_to_current_policy = 1

◆ 使用されていないパスワードの有効期間の制限

権限のあるユーザによって使用されていないパスワードには、セキュリティ上のリスクが伴います。このため、そのようなパスワードの有効期間を制限できるようになりました。ここでは、初期パスワード（つまり、ユーザ管理者によって割り当てられ、ユーザが次の機会に変更しなければならないパスワード）および初期値ではないパスワード（つまり、ユーザによって設定されたパスワード）が区別されます。

タイプ SERVICE および SYSTEM の（技術）ユーザは、このルールから除外されます。

関連する(新規)プロファイルパラメータ

- login/password_max_idle_initial
- login/password_max_idle_productive

■ 変更点

◆ ログオン:

不適切なエラーメッセージの回避

不適切なログオンデータを使用してログオンしようとする場合、原則として、今後は**一般的なエラーメッセージ**“正しいユーザ名とパスワードでもう一度ログオンしてください”のみが出力されます。失敗したログオンに関する詳細な理由(例: ユーザアカウントのロック、ユーザアカウントの有効期限切れなど)は、有効なログオンデータが入力されてから提供されます。システムがログオンデータをチェックすることができない、または追加チェックが許可されていないなどのエラーシナリオは、このルールから除外されます。

- “パスワードを持っていません: パスワードを使用してログオンできません”
- “パスワードによるログオンはできません - 失敗回数が多すぎます”

◆ セキュリティに関連する一部のプロファイルパラメータのデフォルト値が変更されました。

- login/failed_user_auto_unlock : 0 (1 から変更)
失敗したログオンのロックは、無制限の期間で有効となります。
- login/fails_to_user_lock : 5 (12 から変更)
失敗したログオンに対するロックは、パスワードログオンが 5 回失敗した後で設定されます。
- login/no_automatic_user_sapstar : 1 (0 から変更)
スーパーユーザは、明示的に有効化される必要があります。
- login/min_password_lng : 6 (3 から変更)
パスワードは、6 桁以上でなければなりません。
- login/ticket_expiration_time : 8 (60 から変更)
ログオンチケットは、8 時間のみの有効です。

◆ プロファイルパラメータ login/password_max_new_valid および login/password_max_reset_valid は、プロファイルパラメータ login/password_max_idle_initial によって置き換えられました。つまり、初期パスワードの有効期間の制限に関して、ユーザ管理者による最初の設定および後続設定が区別されなくなります。

運用チェックリスト

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
1.	運用管理体制全般	文書化・教育	A	運用マニュアルは文書化され承認されていますか はい ☐ いいえ ☐ 運用マニュアルに基づいたチェックリストはありますか はい ☐ いいえ ☐ それらの内容は教育等によって、関係者に周知徹底されていますか はい ☐ いいえ ☐ 運用マニュアルの管理責任者は誰（責任部門、責任者）ですか ： 運用手順マニュアルには以下の内容が記載されていますか。 - 改定履歴（年月日、改定内容、改定者、承認者など） はい ☐ いいえ ☐ - ポリシー はい ☐ いいえ ☐ - 運用体制 はい ☐ いいえ ☐ - システム ランドスケープ はい ☐ いいえ ☐ - ハードウェア構成 はい ☐ いいえ ☐ - ソフトウェア構成 はい ☐ いいえ ☐ - デスクトップ OS はい ☐ いいえ ☐ - LAN 環境 はい ☐ いいえ ☐ - サービスレベル契約 はい ☐ いいえ ☐ - システムの起動停止 はい ☐ いいえ ☐ - バックアップ／リストア はい ☐ いいえ ☐ - 緊急対応 はい ☐ いいえ ☐ - データベース管理 はい ☐ いいえ ☐ - システム管理 はい ☐ いいえ ☐	- 運用マニュアルを整備し、責任者による承認を得ます - 時期やイベントに対応した複数のチェックリストが必要です。 - たとえば、次のようなチェックリストを作成し、実施するようにします。 「1 日」毎のチェックリスト 「1 週間」毎のチェックリスト - システム起動後のチェックリスト - システム停止前のチェックリスト	関連文書を確認する	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				はい ☐ いいえ ☐ ・ システムセキュリティ ・ バックグラウンドジョブ処理 ・ 印刷 ・ プロファイルパラメータの設定／変更 ・ SAP システムから通知されるエラー／警告への対応 ・ 外部 OS コマンドの管理 ・ モニタリング ・ 変更管理 ・ デスクトップ管理 ・ ネットワーク管理 はい ☐ いいえ ☐			
		運用	A	運用管理は定められた手順に従って実行されていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
		モニタリング	A	規定・手順に沿って運用されていることをモニタリングしていますか はい ☐ いいえ ☐ システム運用責任者とモニタリング責任者は分離されていますか。 はい ☐ いいえ ☐ モニタリングを行うスタッフの知識および受講済トレーニングの内容とレベルについて説明してください。 :		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
運用詳細							
2.	通常のシステム起動／停止	文書化・教育	A	システムの起動停止に関する手順は文書化され承認されていますか はい ☐ いいえ ☐	・ システムの正常な運用を保障するため ➢ SAP システム起動時のチェック ➢ SAP システム停止前のチェック が重要です	・ 責任者にヒアリングを行う	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				SAP システム起動直後／停止直前に行うべきチェック項目のリストはありますか はい ☐ いいえ ☐ それらを教育等によって、関係者に周知徹底していますか はい ☐ いいえ ☐			
		運用	A	システムの起動／停止は定められた手順に従って実行されていますか はい ☐ いいえ ☐ システムのシャットダウン／起動は自動化されていますか。 はい ☐ いいえ ☐ システムのシャットダウンによるバックグラウンドジョブの強制終了を避けるための手段を説明してください。 :		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
		モニタリング	A	システムの起動／停止が手順に従って実施されていることをモニタリングしていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
3.	緊急時対応	文書化・教育	A	緊急時の対応手順が文書化され承認されていますか はい ☐ いいえ ☐ 緊急時の内部および外部への正式なエスカレーション手順(意志決定者、連絡先など)は定義されていますか。 はい ☐ いいえ ☐ 本稼働システムを緊急に変更しなければならない場合の手続きは文書化されていますか はい ☐ いいえ ☐ それらの手順等を教育等によって、関係者に周知徹底していますか はい ☐ いいえ ☐	・ 緊急時のエスカレーション手順と責任者(1次、2次)を定め、文書化しなければなりません ・ 緊急事態への対応責任者を任命し、24 時間連絡がとれるようにします。 ・ 本稼働システムの変更手順を明確に定義し、本稼働システムに加えたすべての変更を、開発システムと品質保証(QA)システム(必要な場合)にも反映されるように手順を定義します。	・ 関連文書を確認する	
		運用	A	緊急時の対応は定められた手順に従って実行されていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
		モニタリング	A	緊急対応が手順に沿って実施されていることをモニタリングしていますか		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				はい ☐ いいえ ☐ 最近発生した緊急システム停止／起動について説明してください ：		る	
4.	会計データに係るバックグラウンドジョブ	文書化・教育	A	会計データに係るバックグラウンドジョブの実行手順が文書化され承認されていますか はい ☐ いいえ ☐ 規定、実行手順は関係者に周知されていますか はい ☐ いいえ ☐ 規定、手順には次のような項目が含まれていますか ・ ジョブ名 ・ 処理内容の説明 ・ オーナ(責任者) ・ 異常終了時の連絡先 ・ 処理周期またはトリガー ・ 予想処理時間 ・ 入力データの発生元システム(ハード、ソフト) ・ 入力データの発生元システムの正当性、完全性／網羅性、正確性の担保のために取られている手段 ・ 入力データの発生元システムの責任者 ・ 入力データの種類 ・ 処理されるデータのおおよその件数と金額 ・ エラーデータの再入力手順 ・ 異常終了時の再実行手順が定義されていますか。 ・ 処理の正当性、完全性／網羅性、正確性の担保のために取られている手段 はい ☐ いいえ ☐			

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和等方法等	監査手順、確認方法	評価
5.	SAPプロファイルパラメータ	運用	A	会計データに係るバックグラウンドジョブは定められた手順に従って実行されていますか はい ☐ いいえ ☐ バックグラウンドジョブの登録権限を持つユーザを上げてください : バックグラウンドジョブの登録権限を持つユーザを上げてください : バックグラウンドジョブの登録権限を持つユーザを上げてください :	・ 一般ユーザにバックグラウンドジョブの登録、実行権限を与えないようにすると統制しやすくなります	・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる ・ バックグラウンドジョブの登録 : トランザクション SM36 ・ バックグラウンドジョブのモニタリング : トランザクション SM37 、RZ01 ・ J-SOX との関係において重要なジョブとは、会計データを登録、変更するすべてのジョブです。重要なジョブをモニタリング、エラー対処手順を文書化しておく必要があります。 ・ バッチインプットログのモニタリング : トランザクション SM35 (バッチインプットログ)。バッチインプットセッションを実行した後、必ずこのトランザクションを実行し、エラーデータをチェックしなければなりません。 ・ バッチインプット処理でエラーになったデータを修正した後、エラーデータの再処理を行います。 ・	
		モニタリング	A	会計データに係るバックグラウンドジョブが規定・手順文書に沿って実施されていることをモニタリングしていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
		文書化・教育	A	SAP プロファイルパラメータの変更手続が文書化され承認されていますか はい ☐ いいえ ☐ それらの手順等を教育等によって、関係者に周知徹底させていますか はい ☐ いいえ ☐ パラメータ変更の責任者は誰(責任部門、責任者)ですか。		・ 関連文書を確認する	
		運用	A	プロファイパラメータの設定／変更定められた手順に従って実行されていますか はい ☐ いいえ ☐ プロファイパラメータの設定／変更権限を持っているの	・ 不正あるいは不正確なプロファイルパラメータの変更はシステムに重大なダメージを与えます ・ すべての変更を企業の変更管理データベース	・ 責任者にヒアリングを行う ・ 必要に応じて ➢ ログを参照し、裏づけをとる ➢ トランザクション RZ10 の実行権限を持つユーザの妥当性を確	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				誰(責任部門、責任者)ですか はい ☐ いいえ ☐	スマートな管理ワークブックに文書化して記録します。	認する ➤ プロファイルパラメータの変更記録照会 : トランザクション TU02	
		モニタリング	A	プロファイル パラメータの変更が規定・手順文書に沿って実施されていることをモニタリングしていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じ	
6.	SAPシステムから通知されるエラーや警告への対応	文書化・教育	A	SAPシステムから通知されるエラーや警告に対する解決手順が文書化され承認されていますか : それらの規定／手順等を教育等によって、関係者に周知徹底されていますか はい ☐ いいえ ☐	・ SAPシステムはアプリケーションの実行に影響を与えるエラーや問題点を監視しています。エラーや問題を認識するとログを作成し記録します ・ 定常的にこのログを監視し、適切な対応を行う必要があります	・ 関連文書を確認する	
		運用	A	SAPシステムから通知されるエラーや警告に対する解決が定められた手順に従って実行されていますか はい ☐ いいえ ☐ 次のような項目をチェックしていますか ☐ SAPシステムから通知される エラー ☐ 失敗した更新 ☐ ABAP プログラムの実行時エラー(ショートダンプの有無)		・ 責任者にヒアリングを行う ・ 必要に応じ ➤ ログを参照し、裏づけをとる ➤ SAPシステムから通知される エラーをトランザクション RZ20 または SM21 でチェック (補足) トランザクション RZ20 and/or SM21 を使って SAPシステムが発行するエラーおよび警告情報のほとんどを監視できます。赤(エラー)、黄(警告)、緑(正常)の信号アイコンで情報が区分表示されます ➤ 失敗した更新の有無をトランザクション SM13 でチェック ➤ ABAP プログラム実行時エラーの有無をトランザクション ST22 でチェック ・ エラーや警告の記録がある場合、対応が適切に行われている確認する	
		モニタリング	A	システムから通知されるエラーや警告の解決が手順に従って実施されていることをモニタリングしていますか モニタリング結果をどこに記録しますか。 :		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				エラーや警告の根本原因を追跡していますか。 はい ☐ いいえ ☐ その責任者はだれですか :			
7.	外部OSコマンド	文書化・教育	A	外部 OS コマンドの登録、実行に関する手順が文書化され承認されていますか はい ☐ いいえ ☐ それらの規定／手順等を教育等によって、関係者に周知徹底させていますか はい ☐ いいえ ☐	(補足) 「外部 OS コマンド」とは SAP ERP の実行基盤であるオペレーティングシステム (UNIX や Windows 等) が備えているコマンドを意味します。SAP ERP 上で予め OS コマンドを登録しておく、OS にログオンすることなしに、OS コマンドを実行することができます	・ 関連文書を確認する ・ 外部 OS コマンドの登録/変更 : トランザクション SM69 ・ 外部 OS コマンドを実行 : トランザクション SM49	
		運用	A	外部OSコマンドの登録／実行は定められた手順に従って実行されていますか はい ☐ いいえ ☐ どのような外部 OS コマンドが登録されていますか : 外部 OS コマンドを登録できる権限を持つのは誰(責任部門、責任者)ですか :		・ 責任者にヒアリングを行う ・ 必要に応じて ➢ ログを参照し、裏づけをとる ➢ トランザクション SM69、SM49 の実行権限を持つユーザの妥当性を確認する ➢ トランザクション SM69 を使用し、登録されている外部 OS コマンドを確認し、利用目的をヒアリングする	
		モニタリング	A	手順に従って実施されていることをモニタリングしていますか	・	・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	
8.	バックアップ／リストア	文書化・教育	A	バックアップ／リストア手順が文書化され承認されていますか はい ☐ いいえ ☐ 教育等により、バックアップ／リストア手順は関係者に周知されていますか はい ☐ いいえ ☐	(補足) SAP ERP 固有のバックアップ／リストア機能を使わず、市販のツールを利用している企業も多い。	・ 関連文書を確認する ・ どのようなバックアップ／リストア ツールを利用しているか確認する ・ バックアップスケジュール (DBA 計画可カレンダー) : トランザクション DB13 ・ バックアップ／リストア履歴照会 : トランザクション DB12	
		運用	A	バックアップ／リストアは定められた手順に従って実行されていますか はい ☐ いいえ ☐ 定期的なリストア訓練を実施していますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	

N0	分類	区分	ランク	チェック内容	関係するリスク・統制・緩和方法等	監査手順、確認方法	評価
				前回実行したのは何時ですか ：			
		モニタリング	A	手順に従って実施されていることをモニタリングしていますか はい ☐ いいえ ☐		・ 責任者にヒアリングを行う ・ 必要に応じてログを参照し、裏づけをとる	