システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
2-(1)-①	経営者が財務報告に関連したIT への対応について戦略・計画を定めること	IT への対応が組織として計画的に実施されないことにより、財務報告の信頼性を阻害する。				※ERPに限定されない ・財務諸表に影響のあるIT投資や計画に対して経営陣が承認を与えている（経営会議、投資に関して議決する委員会等）
2-(1)-②	IT に関する方針や計画決定のための全社的な組織が設けられ、有効に運営されていること	IT に関連する組織の不備により、財務報告に関連するIT への対応が適切に実施されない。				※ERPに限定されない ・IT投資、計画に対して経営陣が承認を与え、企画から運用までのプロセスが管理されている （経営会議、投資に関して議決する委員会等）
2-(1)-③	IT に関する業務の役割分担、責任及び権限が明確になっていること	IT に関する業務の管理・実施責任が不明確なことにより、不正やミスが見逃されたり、情報の信頼性が確保されない。				※ERPに限定されない ・IT部門とその他の部門の業務に関する職務の組織的な分離が明確に規定され、運用されている
2-(1)-④	IT に関連する業務に携わるIT 部門及びユーザ部門の人材の採用・育成及び教育訓練が適切に行われていること	IT に関連する業務に携わる適切な人材が確保されないことより、業務が適切に実施されない。				・導入したERPの導入、運用に関して熟知した要員が確保され、信頼性、安全性、機密性を維持した業務システムの運用ができている
2-(1)-⑤	情報セキュリティの基本方針を定めていること⇒（システム管理基	明確な情報セキュリティへの方針がないと、適切な情報セキュリティが保証されない。				※ERPに限定されない ・情報セキュリティに関する規程が策定、運用されている
2-(2)-①	IT に関連するリスク評価の方針が定められており、運用されていること	IT リスク評価が実施されないことにより、重要なリスクを見落とす（対策が講じられない）。				※ERPに限定されない ・定期的にリスク評価を行うことで、企業のリスクの所在を認識し、適宜、必要な対策を実施している
2-(2)-②	統制活動へのIT の利用によって、新たに生じるリスクを考慮していること	統制活動へのIT の利用によって、新たなリスクが生じる。				・情報基盤への投資、システム開発の着手は、関連するユーザー部門や経営層の承認を得て着手され、本番段階の利用において当初の目的を達成したかどうか確認し、結果を経営陣に報告している
2-(3)-①	IT全般統制及びIT業務処理統制に関する方針及び手続を適切に定めていること	IT に関する統制活動が適切に行われないことにより、財務報告の信頼性が確保されない。				・IT部門は業務システムを利用するユーザー部門と組織的に分離されており、IT部内においても技術部門、システム開発、保守部門が分離されている
2-(3)-②	統制活動にITを利用する場合に備えた方針及び手続があること	統制活動にIT を利用する場合には、その方針及び手続を適切に定めていないことによりIT の適切な利用がなされない。				・システムの開発や保守は、企画段階から運用移行までのプロセスが策定され、投資の決定、本番運用開始などの重要な局面では、IT部門とユーザー部門の責任者が評価を行い、実施の可否を判断している
2-(4)-①	IT に関する業務の状況についての情報を識別・把握・処理し、その情報を企業内及び企業外の関係者に伝達する仕組が整備され、適切に運用されていること。	IT に関する重要な問題点（システム障害、変更点、対応状況等）が、企業内（経営者、IT 部門、ユーザ部門及び関係部 門）、業務委託先、提携先、取引先等の関係者に適切に伝えられないため、IT に関するリスクの対応に支障が生じる。				・情報システムに関係するトラブルは、情報基盤と業務システムの双方で問題管理の手続が策定され、問題の認識から分析、暫定措置の実施、恒久措置の実施までのプロセスが定められている本番環境への適用に当たってはユーザー部門が確認し、本番移行を判断している

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(1)-①-イ	情報システムの開発方針・手続、開発手法（開発標準）が存在し、責任者が承認していること	IT の開発の際に意図的な不正なプログラムが埋め込まれたり、処理に誤りが顕在化する。	調達／導入のための標準化された方針や手続きが制定されないと、不正なプログラムの埋め込みや処理誤りが発生する恐れがある	・開発申請、開発実行、エンドユーザ受入テスト、インポートに関する方針、手続きが制定されている ・ソリューションマネージャにより文書管理を行う	・調達／導入のための標準化された方針・手続きが制定され、承認手続きが明確化されている	・関係者に対する方針、手続きの周知徹底および遵守意識の向上に向けた教育を行う ・責任者を交えたレビューにより開発過程における方針、手続きの遵守状況についてのモニタリングを行う
3-(1)-①-ロ	開発手法は、財務情報の完全性、正確性、正当性を考慮していること	IT の開発プロセスにおいて、意図的な不正や、処理に誤りの起きる可能性がある。	アドオン、モディフィケーションに対する開発標準が整備されないと、意図的な不正や処理誤りが発生する恐れがある	・カスタマイジング、アドオン、モディフィケーションの定義を明確にし、拡張以外のアドオン、およびモディフィケーションについて、リスクが高いことを表明している ・EXITインタフェースを提供し、アドオンが必要な場合の他への影響等のリスクを低減する	・モディフィケーションを原則禁止するとともに、アドオン時の開発標準を明確化する ・機能のサービス化を進めて、アドオンやモディフィケーションの必要性を低減する	・アドオンを行う場合の開発標準を明確化する ・アドオン機能についての仕様書レビュー等により、不正や処理誤りに対する統制機能が組み込まれていることを確認する
3-(1)-①-ハ	情報システムは、誤り防止、不正防止、可用性、他のシステムとの整合性を考慮して設計されていること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-①-ニ	財務情報に係る情報システムの調達は、全社的なIT 方針に沿って計画されていること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-①-ホ	統制が有効に整備・運用されていることを検証するために十分で適切なテストが実施されること	誤りや不正防止機能が確実に動作しないと、誤りが起きる可能性がある。	十分で適切なテストが実施されないと、誤りが発生する恐れがある	・CATTを提供し、テストの自動化を支援している ・ソリューションマネージャを提供し、テストシナリオ、テスト結果等の保存、管理を支援している	・標準的なテスト体系を規定し、それに基づいたテスト支援ツールの提供を行う	・必要十分なテストシナリオを策定し、責任者の承認を得る ・ユーザ部門によるテストへの参画、テスト結果の承認を行う
3-(1)-②-イ	IT 基盤（ネットワーク機器やソフトウェアを含むサーバ、コンピュータ等のインフラシステム）が、財務情報に係る情報機器の信頼性を達成するものであること	IT 基盤のインタフェースが信用できないと、扱うデータを信頼できない。	IT基盤のインタフェースの信用度が低いと、扱うデータの信頼性が低下する恐れがある	・外部データ入力に対してパッチインプット及びBAPIインタフェースを提供し、データの信頼性を確保している	・外部に対する標準的なインタフェースが提供されている	・導入時のテストや稼働後の変更管理を徹底する ・テストにはユーザ部門も参画し、データの正当性、正確性、完全性等についての総合的な検証を行う
		IT 基盤の設定が不適切な場合、システムが正しく動作しない。	IT基盤が適切に設定・維持されないと、システムが正しく動作しない恐れがある	・SAPミドルウェアの設定はプロファイルパラメータで可能であるが、DB、OS等のIT基盤自体の設定に対する統制機能はない	統制範囲外	・設定時のテストや稼働後の変更管理を徹底する ・テストにはユーザ部門も参画し、機能面、性能面等についての総合的な検証を行う ・IT基盤に関連するベンダに対し、設定時の十分な技術支援を要請する
3-(1)-③-イ	変更管理ルールと手順を定め、業務責任者及び開発及び保守の責任者が承認すること	プログラムが改ざんされたり、承認なく変更される。	変更するための標準化された規定・手順が文書化されないと、プログラム改ざんの恐れがある	・変更申請、変更実行、エンドユーザ受入テスト、インポートに関する手順、規定が文書化され、承認手続きが明確化されている ・ソリューションマネージャを提供し、文書管理を支援している	・変更するための標準化された規定・手順が文書化され、承認手続きが明確化されている	・関係者に対する規定、手順の周知徹底および遵守意識の向上に向けた教育を行う ・責任者を交えたレビューにより変更過程における規定、手順の遵守状況についてのモニタリングを行う ・アクセスログのチェック等により、未承認の変更が行われてないことを定期的に確認する
3-(1)-③-ロ	変更管理要求が生じた場合、他システムの影響を考慮すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ハ	緊急の変更要求は文書化され、変更管理手続にしたがっていること。	緊急時にプログラムが改ざんされたり、承認なく変更される。	緊急時の対応手続きが存在しないと、プログラム改ざんの恐れがある	・3システムランドスケープ上で品質保証テスト用システムに対する「仮修正」の手続きを規定している	・開発環境と本番環境を分離し、緊急時であっても本番環境への直接アクセスは原則禁止する	・緊急時の対応手続きを規定し、関係者に周知徹底する ・責任者が対応前の承認を行うとともに、アクセスログのチェック等により実施した内容の妥当性を確認する ・本番環境にアクセスできる特権ID等の数を必要最小限に抑える

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(1)-③-ニ	システム設計書、プログラム設計書等は、保守計画に基づいて変更し、業務責任者、担当者及び保守の責任者が承認すること	本番環境に変更結果を移行する際にプログラムが改ざんされる。	本番環境への変更結果の移行に対する承認が行われないと、プログラム改ざんの恐れがある	・移送管理システムの承認機能を設定し利用することで本番環境への移行に対する承認を行い、かつtpコマンドでの直接移送を抑制している	・開発環境と本番環境を分離し、本番環境へのプログラム移行は責任者の承認がないと実施できない機能を実装する	・職務を分離し、移行は開発担当者ではなく運用担当者が行う ・移行前に、運用責任者とシステムオーナの承認を受ける ・アクセスログのチェック等により、未承認の移行が行われてないことを定期的に確認する
3-(1)-③-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	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ヘ	プログラム設計書に基づいてプログラミングしていることを検証すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ト	プログラムのテストの実施は、テスト計画に基づいて行うこと	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-チ	プログラムのテストには業務担当者等が参画すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-リ	プログラムのテスト結果は、担当者、運用及び保守の責任者が承認すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ヌ	プログラムの本番への移行は、運用担当者が実施すること。	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ル	プログラムのテスト結果、本番への移行結果を記録及び保管すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ヲ	機能の追加等の変更は必須の項目に限ること。	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ワ	最新の承認されたパッチが導入されていることを確認すること。	追補版に記載なし （本表の次版で追加検討）				

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(1)-③-カ	テストを実施して、結果を保管すること。	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-ヨ	本番への移行は運用担当者のみが実施すること。	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-タ	変更の結果は、業務担当者及び開発責任者が承認すること、変更によって、IT 基盤の運用や保守に大きな変更が生じた場合には運用責任者や保守責任者が承認すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-③-レ	起案から完了までの状況を文書管理し、進捗を把握すること	追補版に記載なし （本表の次版で追加検討）				
3-(1)-④-イ	アプリケーション・システムのソフトウェア及びIT基盤のテストのために、テストの方針と手続が定められていること	IT 基盤の情報転送機能がテストされないと、財務情報が正確にシステム間で受け渡されているか確認できない。	適切な（ユーザ受入）テストが計画されていない IT基盤とSAP側のインターフェースが適切に管理されておらず、SAP側の処理結果に誤りが発生したり、改竄が起きる		・IT基盤上における情報転送機能のテストをアプリケーションとは切り離して別途、確実に行なう ・OS，DBMSの設定に関係する部分がどのように関係しているか確認する	・品質保証（テスト管理部門）の管理体制をしっかりとさせる
3-(1)-④-ロ	テスト計画は、開発及びテストの責任者が承認すること	IT 基盤のテストが事前に計画されていないとテスト項目に漏れが起きる。	テスト規定・手順を文書化していない		・テスト項目のレビューを行い、網羅性のチェックを行う ・OS，DBMSの設定に関係する部分がどのように関係しているか確認する	・品質保証（テスト管理部門）の管理体制をしっかりとさせる
3-(1)-④-ハ	テストは、本番環境と隔離された環境で行うこと	追補版に記載なし （本表の次版で追加検討）				
3-(1)-④-ニ	テストに当たっては、要求事項を網羅し、実際の運用を想定したテストケースを設定し、テストデータを作成すること	財務情報データを旧システムから新システムに移行する際に、テストが行われないと、移行したデータが正確かどうか分からない。	適切な（ユーザ受入）テストが計画されていない SAPへの移行にあたって作業手順が計画、承認されておらず、旧システムからのコンバージョンの誤りが発生したり、SAP側での動作が正しいのか、わからなくなってしまう		・テスト項目について内部・外部の専門家の意見を取り入れる ・本番移行段階でユーザー側が機能の確認と本番移行データのコンバージョン結果を確認している本番移行はその確認（UAT）が完了した後、ユーザー部門、システム部門双方の部門長承認後に行なわれる	・品質保証（テスト管理部門）の管理体制をしっかりとさせる
3-(1)-④-ホ	テストに当たっては、想定される環境での負荷を考慮して実施すること。また、ピーク負荷が情報システムの耐性に大きな影響がある場合には、ピーク負荷のテストを実施すること	IT 基盤やアプリケーション・システムは、負荷が大きいときに正しく動作しない。	適切な（ユーザ受入）テストが計画されていない SAPの利用に必要な能力レベルのIT基盤が用意されず、可用性に問題が起きる		・テスト項目について内部・外部の専門家の意見を取り入れる ・ERPに関する負荷と情報基盤の負荷の状態がモニタリングされ、適宜リソースの増強のための判断ができるようになっているリソースの増強に関する投資は投資に関する委員会の判断後に増強される	・品質保証（テスト管理部門）の管理体制をしっかりとさせる
3-(1)-④-ヘ	テストには、開発当事者以外の者（運用担当者や保守担当者等）が参画すること	受入テストをシステムを開発した担当者が実施すると、誤りや不正が見逃される可能性が残る。	適切な受け入れテストが出来ていない 受け入れテストの実施が、開発担当者によって行われている		・テスト実行者の分離を確実に行う本番移行は開発、保守に従事するもの以外の要員や部門で行なわれる ・本番移行前のUATは必ずユーザー部門が行なうことになっており、その結果確認がとれたものが本番移行の対象となる ・外部要員によるプログラムの修正や変更は、社内要員によって結果の確認が行なわれ、開発要員は品質保証、本番環境へのアクセス、移行ができない	・品質保証（テスト管理部門）の管理体制をしっかりとさせる

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(1)-④-ト	テストで発生した問題点について、問題毎の対応策とリスクが明確になっていること。その記録が保存されていること	テスト結果の記録が残されていないと、機能が正しく開発されているかの証拠がない。	テスト結果の記録がなく、テスト結果の真偽が確かめられない テスト中に発見された問題が、問題管理データベースに記録されていないまた、各ビジネスプロセスのテストごとに完了基準を定義されていない	・問題管理データベースによる管理	・テスト計画が事前に作成され、そのテスト計画に沿って行なわれたテスト結果は記録され、システム開発の責任者が確認しているテスト結果は本番移行後も一定期間保管されている ・全てのテスト項目に対する全ての記録の存在、内容の確かさをチェックする	・品質保証(テスト管理部門)の管理体制をしっかりとさせる
3-(1)-⑤-イ	企業の開発及び保守に係る手続は、環境変化に合わせて、適宜見直し、変更されること	外部環境が変化したときに、開発やプログラムの変更管理、アクセス管理、運用にかかわる方針と手続が変更されないと、リスクが大きくなる。	※SAP側のポリシ設定に該当する機能に対して必要な設定内容を示す		・会社、あるいはIT，部門の組織変更のたびに、IT部門の職務と対応する権限が見直され、作業に必要な特権の管理も移管される ・特権の利用手続は規定され、その権限が必要な作業にすべては管理、保管されている	・会社、あるいはIT，部門の組織変更のたびに、IT部門の職務と対応する権限が見直され、作業に必要な特権の管理も移管される ・特権の利用手続は規定され、その権限が必要な作業にすべては管理、保管されている
3-(2)-①-イ	運用ルールを定め、順守すること	運用時の誤操作によって誤った処理が行 われる。	・規程・手順書や運用体制が整備されていないと、誤ったオペレーションが行われたり、その発見が遅れる ・システム運用責任者とモニタリング責任者を分離しないと不正な操作等を発見できない		・ジョブスケジュールに基づく自動運転機能	・運用チェックリスト
3-(2)-①-ロ	運用ルールに基づいた運用計画を策定し、承認すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-①-ハ	運用ルールには、例外処理のオペレーションが含まれること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-①-ニ	規模、処理日時、システム特性、業務処理の優先度を考慮したジョブスケジュールにしたがって運用すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-①-ホ	情報システムはアクセス記録を含む運用状況を監視することが望ましく、また、情報セキュリティインシデントを記録し、一定期間保管すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-①-ヘ	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	運用時の不正な操作等を発見できない。	・問題管理の手順や体制を整備していない場合は、問題の発見や不正な操作等の発見が遅れる	・SAP警告モニタ	・オペレーションログ等の取得機能 ・モニタリングする事象や閾値等の設定機能 ・アラーム機能	・運用体制の整備
		情報システムが処理するデータの信頼性が保証されない。		・すべてのアクションが適切に実行され、活等に漏れがないことを確認できるように、モニタリング結果を記録する必要があります。	・オペレーションログ等のアクセス制御	・OS標準のアクセス機能の利用
3-(2)-①-ト	情報システムの利用に先立ち、担当者向けの支援プログラムや教育プログラムが準備され、教育研修が実施されていること	財務情報に係る情報システムの担当者が、リスクと適切な操作方法等について教育を受けていないと、誤操作によるシステムの誤りや不正の防止につながる。	・エンドユーザマニュアルが業務上必要なもの以外にも公開されている場合は、システムの不正利用のリスクが増大する		・操作権限毎のオンラインマニュアル	・マニュアルの配布管理

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(2)-②-イ	管理ルールと手順を定め、運用責任者が承認すること	ソフトウェア、ハードウェア、アプリケーション・システム等が無断で設置・廃棄されることにより、誤処理やシステム停止が起こる。				・サーバやクライアント等の設置や廃棄の手続きを定める。 ・クライアントやサーバのプログラムやパラメタの変更手順を定める。 ・構成管理台帳を整備する。 ・構成管理台帳を元に定期的にたな卸しを実施する。
3-(2)-②-ロ	許可された以外のソフトウェア、ハードウェアは使用禁止にすること	許可されないソフトウェアの使用によってデータの改変やシステムの停止が起こる。	不正に、不正確にプロファイルパラメータの変更がなされる	・開発者キーの取得を特定の責任者だけが行えるように統制できる ・開発環境、テスト環境、本番環境を物理的に分離し運用するアーキテクチャを具備している ・任意の機能を実行禁止にできる	・本番プログラム管理機能とモニタリング機能	・ソフトウェア変更の手順書が整備され、運用されている適切に整備・運用状況がモニタリングされ、是正されている
3-(2)-②-ハ	導入や調達したソフトウェア、ハードウェア及びネットワークの記録が適切に管理簿に反映されていること。	変更が正しくシステム管理情報に反映されないために、システムの不整合が起きるリスクがある。	不正に、不正確にプロファイルパラメータの変更がなされる	・開発者キーの取得を特定の責任者だけが行えるように統制できる ・開発環境、テスト環境、本番環境を物理的に分離し運用するアーキテクチャを具備している ・任意の機能を実行禁止にできる	・アクセス管理によるシステム変更統制機能	・システム変更の手順書が整備され、運用されている適切に整備・運用状況がモニタリングされ、是正されている
		管理期限の経過したハードウェア等の継続使用により、処理に誤りが起こるリスクがある。	SLAが適切に管理運用されず、あるいはCCMS警告モニタなどが有効に機能せず、誤利用により処理に誤りが発生する	・CCMS警告モニタ機能	・アラーム機能	・契約書、SLAのモニタリング
3-(2)-②-ニ	調達先とのサポート体制を維持すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-②-ホ	緊急時を含む障害対策があること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-②-ヘ	設定について適切であることを確かめるためのテストと評価を実施すること。	追補版に記載なし （本表の次版で追加検討）				
3-(2)-②-ト	想定されるリスクを明らかにして、対応すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-③-イ	データ管理ルールと手順を定め、責任者が承認すること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-③-ロ	データの送受、交換、複製及び廃棄は、データ管理ルールに基づいて、誤り防止、不正防止、機密保護の対策を行うこと	処理結果の配布や保存について手続が定められていないと財務情報を紛失したり、伝達できなくなる。	SAP DB上で保存期間が正しく設定されず、必要な財務情報を紛失する	・データアーカイブ機能、運用モニタリング機能、SAP警告機能などを具備している	・アクセスログ、プロセス実行ログ、オペレーションログ機能、モニタリング機能、アラーム機能	・運用管理手順書が整備され運用されている適切なモニタリングが実施され是正されている

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(2)-③-ハ	情報システムの内部のデータが不正アクセス又は改ざんから論理的、物理的に保護されること	データの保管や移送の際には、改ざん、不正複写等の可能性がある。	責任者のアクセス権管理が適切に実施されず、改ざん、不正複写が実施される	・本番稼動環境への移送を責任者よる承認なしに実施できないようにロックできる	・本番データ移行管理機能とモニタリング機能	・本番移行手順書が整備され運用されていおる適切にモニタリングされ是正されている
3-(2)-③-ニ	障害や故障等によるデータ消失等に備え、財務情報や販売管理に関するデータは、バックアップすること	追補版に記載なし （本表の次版で追加検討）				
3-(2)-③-ホ	バックアップ媒体からの復旧をテストすること	文書やデータについては、保管が正しくなされず、重要な情報を紛失したり、無駄なデータが長期保管される。	バックアップのスケジュール機能を利用するパラメータが正しくセットされないため、障害時などに正しく文書やデータを復元できないまた、不用な文書、データが長期間保管される	・バックアップのスケジュール機能が標準装備されている完全・差分・トランザクションコードログ・バックアップ、データベース整合性チェックなど	・バックアップのスケジュール機能とモニタリング機能	・バックアップ/リカバリ手順書が整備され・運用されている適切なタイミングでモニタリングされ是正されている
		バックアップされていないと、データを消失した場合に、復元ができない。	バックアップのスケジュール機能を利用するパラメータが正しくセットされないため、障害時などに正しくデータを復元できない	・バックアップのスケジュール機能が標準装備されている完全・差分・トランザクションコードログ・バックアップ、データベース整合性チェックなど	・バックアップのスケジュール機能とモニタリング機能	・バックアップ/リカバリ手順書が整備され・運用されている適切なタイミングでモニタリングされ是正されている
3-(3)-①-イ	情報セキュリティ基本方針に基づいて組織の情報セキュリティのフレームワークを構築していること	情報セキュリティの基本指針とフレームワークがなければ、情報システムにおけるアクセス管理が適切に実施されない。	情報セキュリティの基本指針とフレームワークがなければ、プロファイルパラメータの値をを適切に設定することができず適切な品質のアクセス管理ができない	・プロファイルパラメータの値を調整することによりセキュリティポリシーに合わせた品質でパスワード管理を行うことが可能	・企業ポリシーに合わせてパスワード管理レベルを柔軟に実装できる機能	・情報セキュリティの基本指針とフレームワークを明確にし自社のアクセス管理方針を規程する
3-(3)-②-イ	業務上及びセキュリティの要求事項に基づいて、職務権限に対応したアクセス範囲、アクセス権限のレベルを決めていること	職務権限が決められていないと不正アクセスが起きてデータが改ざんされる危険性がある	本番環境の権限設定のテストが不十分 同一ユーザが持ってはならない権限の組合せを定義せず、また権限設定の棚卸しをしていない	・品質保守システムでテストを行い本稼動システムへ移送することができる ・AISによりチェックすることが可能	・職務分掌に応じたアクセス権限設定機能 ・重複保有を禁止する権限の組合せを登録することにより全ユーザを一括チェックする機能	・職務分掌に応じた権限付与の承認と設定 ・定期的なユーザIDの棚卸しの際に重複保有禁止の権限をチェックする
		施設へのアクセスに制限がなければ、関係者でない人物によって重要な財務情報にアクセスされたり、改ざんされたりする。				・入退館管理対策として、基本的な方針と手続を策定し必要な対策を行なう（例　入退館申請、入退館記録、電子ロック）
3-(3)-②-ロ	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	担当者のアカウントの発行、停止等の管理がなされていないと不正使用されて、データへの改ざんや漏えいが起きる。	・ユーザIDが使い回しされる ・退職や異動者のユーザIDが放置される ・パスワードが盗まれ、あるいは破られ、不正ログオンされる ・特権ユーザが悪用される	・識別機能をユーザ管理機能として実装 － 多重ログオンを禁止する － パスワードに関わるプロファイルパラメータを適切に設定し、パスワードの品質を高める － 人事異動とユーザIDを連動させる － 特権ユーザID等の厳重管理	・業務・役職に応じた詳細な権限設定機能 ・権限の妥当性の自動チェック・分析機能	・ユーザ管理の組織体制を構築 ・ユーザID/ﾊﾟｽﾜｰﾄﾞ管理規程の整備と周知徹底 ・システム監査ログを定期的にチェックする ・人事異動データに基づき登録ユーザ数の増減をチェックする
3-(3)-②-ハ	担当者の役割又は職務に変更があったり、担当者が離職した場合には、直ちにアクセス権が解除されていること	適切なアクセス制御機能がなく、データへの改ざんや不正な参照が起きる。	権限管理が厳重に行われていない ・アドオンプログラムに許可手続きが組み込まれていない ・権限チェックの縮小／無効化機能が使用されている	・SAP権限チェック機構による自動チェック	・オペレーティングシステム、データベース管理システム、ネットワークなどの権限管理を厳重に行なう	・開発規程に許可手続きに関する規程を定める ・開発プロセスのモニタリング ・AISレポートによる権限管理のモニタリング
3-(3)-②-ニ	担当者IDは、適宜点検されて、長期間利用されていない担当者ID等が削除され、この記録が保管されること	追補版に記載なし （本表の次版で追加検討）				

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(3)-②-ホ	特権IDの付与にあたっては、担当者や利用期間を限定し、そのIDに対応する業務にのみ利用していること	特権ユーザは情報システムの変更や担当者の追加・削除等ができるため、統制されないと改ざん等の不正が発生する。	ロールを登録する担当者とロールを割り当てる担当者が分離されていない SAP　ALL権限	・権限管理	・特権ユーザの検索機能 ・一人で同時に保持できる重複権限のうち禁止される権限設定のチェック機能	・権限設定権限と他の特権の重複保有の禁止や特権ユーザの定期的な棚卸しなどを実施する
3-(3)-②-ヘ	パスワードの割当ては、アクセス手順にしたがって付与されること	追補版に記載なし （本表の次版で追加検討）				
3-(3)-②-ト	担当者のネットワークへの接続は、事前に定められたルールによって制限すること	インターネットを利用する場合は不正侵入対策が実施されている。	ネットワークのアクセス権限管理が厳重に行われていない	・SAP権限チェック機構による自動チェック	・ ネットワークのアクセス権限管理を厳重に行なう	・セキュリティ監査ログや監査情報システムによる日常的モニタリングの実施する
3-(3)-②-チ	担当者のネットワークへのアクセス権は、アクセス制御方針にしたがって、維持し更新すること	追補版に記載なし （本表の次版で追加検討）				
3-(3)-②-リ	認可されている担当者本人の認証を行う機能があること	適切な認証がないと、データへの改ざんや不正な参照が起きる。	不完全な権限分離、過剰な権限の付与などにより、データ及びプログラムの改竄、破壊、漏洩等が行なわれ、財務報告の信頼性が損なわれる	・ユーザ ID登録、権限ロール登録、権限ロール割当ての各権限を分離する ・3システムランドスケープを採用する ・移送のコントロールを採用する ・権限のないトランザクションコードをメニューに表示しない	・権限のあるユーザーのみが承認された業務処理を行えるような統制機能 － 職務分離の統制機能 － 重要トランザクションもしくはマスターデータに関するアクセス制限付与 － トランザクションの実行権限やユーザー別メニューによるアクセス管理	・管理組織体制の整備 ・権限管理規程の整備と周知徹底 ・セキュリティ監査ログや監査情報システムによる日常的モニタリングの実施する
3-(3)-②-ヌ	システムへの認証の成功及び失敗が記録され、保管されること	追補版に記載なし （本表の次版で追加検討）				
3-(3)-②-ル	特定の業務用ソフトウェアの禁止及び接続に関するアクセス制御が実施されること	追補版に記載なし （本表の次版で追加検討）				
3-(3)-③-イ	情報セキュリティインシデントの影響度に応じた報告体制及び対応手順を明確にすること	情報セキュリティインシデントへの対応が適切に行われないと、被害が拡大する。		・不正ログオンのロック機能	・不正ログオン、異常な操作の検出と警告機能 ・ログオンのロック機能、DBのロック機能、ログ解析機能	・インシデント発生時の緊急対応体制を明確にし対応手順をあらかじめ策定しておく
3-(3)-③-ロ	情報セキュリティインシデントの内容を記録し、情報システムの運用の責任者に報告すること	承認されていない行為をモニタできず不正な行為が行われて、インシデントが発生する。	承認されていない行為をモニタできず不正な行為が行われて、インシデントが発生する	・セキュリティ監査ログ	・セキュリティ監査ログ ・ログ分析機能 ・警告機能	・不正の予防的統制として、本番環境へは限られた者だけがアクセス可能とし、特権保有者はできる限り少人数とする 開発者と運用者の分離
3-(3)-③-ハ	情報セキュリティインシデントの原因を究明し、再発防止の措置を講じること	ログ取得されず、インシデントの原因究明ができない。	ログ取得されず、インシデントの原因究明ができない	・セキュリティ監査ログ	・ログ採取機能	・ログ採取が不可能な場合、最低限、特権IDによるログインと操作内容、ジョブ実行、本番環境の変更などについての記録と責任者によるチェックと承認

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
3-(4)-①-イ	（財務報告に直接係る）情報システムの開発・運用等を委託するとき、その委託計画が承認されていること	委託先とのサービスレベルの契約がセキュリティ統制について触れていないと、サービスレベルが維持できなくなり、適切に財務情報が作成されなくなる。				・委託先との契約に関して情報セキュリティに関する教育や遵守事項が盛り込まれ、達成できない時の罰則が規程されている
3-(4)-①-ロ	委託業務の目的、範囲、予算、体制等が明確になっていること	追補版に記載なし （本表の次版で追加検討）				
3-(4)-①-ハ	情報システムの開発・運用等を委託するとき、組織の委託先選定方針にしたがって業者選定していること	委託先選定や委託先の管理方針が不明確であると、サービスレベルが維持できなくなり、委託した財務情報が適切に得られなくなる。				・委託先選定のための条件が定められており、その内容が契約書に盛り込まれている
3-(4)-①-ニ	候補業者の業務提供能力の評価と財務上の適格性を判断していること。	委託先選定基準が不明確で、不適格な業者を選定すると、サービス品質が低かったり、納期が守れなかったりして、財務情報の信頼性を保証できなくなる。				・委託先選定のための条件が定められており、その内容が契約書に盛り込まれている
3-(4)-①-ホ	契約書には、委託業務に関する主要なリスクに対する統制方法を明記していること	追補版に記載なし （本表の次版で追加検討）				
3-(4)-①-ヘ	業務内容及び責任分担を明確にすること	追補版に記載なし （本表の次版で追加検討）				
3-(4)-①-ト	委託業務の実施状況を把握し、適宜、確認すること	委託先とのサービスレベルの内容を見直さないと、サービス品質が低下していても分からない。				・定期的にSLAの遵守状況について確認、見直しが行なわれている
3-(4)-①-チ	成果物の検収は、委託契約に基づいて行うこと	追補版に記載なし （本表の次版で追加検討）				
3-(4)-①-リ	財務情報に係る信頼性について、サービスレベルをモニタリングして（例えば、委託業務の結果サンプリング等で検証して）、問題があれば、業務責任者に報告すること	サービスレベルをモニタしないと、処理される財務情報の完全性、正確性、正当性が保たれない。				・システムのリソースの利用状況はモニタリングされ、定められた閾値に近づくと実施するプロセスが規程されている
3-(4)-②-イ	財務報告・財務情報に係る情報システムの開発・運用を委託する場合、サービスレベルを定義し、そのレベルに維持する。そのために、委託先とサービスレベル契約（SLA）を結ぶことが望ましい。	サービスレベルが定義されていないと、安定したサービスを継続して利用できず、財務情報の信頼性が損なわれる。				・システムのリソースの利用状況はモニタリングされ、定められた閾値に近づくと実施するプロセスが規程されている

システム管理基準追補版の統制目標		システム管理基準追補版のリスクの例	SAP ERPにおけるリスクの例示	SAP ERPの統制機能	一般的にERPに求められる統制機能	代替機能または人的統制
		サービスレベルが維持されていることを管理しないと、サービスレベルが低下しても気づかない。				・システムのリソースの利用状況はモニタリングされ、定められた閾値に近づくと実施するプロセスが規程されている

凡例： 該当する記述不可