

1-2-4 解答例

IT全般統制RCM

会社名	A社
決算期	平成〇〇年3月
事業拠点	本社及び倉庫
対象システム	販売管理、在庫管理、会計
関連する勘定科目	売上高、売掛金、棚卸資産

整備状況		
文書	プロセス	システム実装

作成者・作成日	◇◇◇◇ 2006/6/23
質問への回答者（実施部署）	*****（情報システム部）

高：統制活動の結果のリスクが大きい場合（重要な欠陥など）
 中：結果のリスクが無視できない場合（不備がある）
 低：結果のリスクが小さい

リスク	統制目標		No.	現在の統制の状況	整備運用	予防発見	手作業自動化			頻度	統制評価手続	評価並びに検出事項 (検出事項がある場合、その影響)	調書番号	評価結果			
	留意事項																
報処発ウに財 に理エ係務 信結調ア情 頼果達ガわ をのさ適ソ 置財れ正の け務不に信 な情開頼性	開発・調達	ITを開発する際に意図的な不正プログラムが埋め込まれることを防止し、処理に誤りが発生しないようにする		開発に関する明文の規定が存在せず、したがって、標準的な開発のプロセスも存在しない。ITを開発するための標準化された方針および手続が存在していない。	整備	予防	手作業	×	×	NA	年	ITの開発は標準化された手順、文書で実施されていることを、情報システム担当者へのヒヤリングと、規定の査閲により確かめた。		不正や誤りの組み込まれない、品質の高い開発が実施されるための統制がない。不備に該当するので、改善を行うべきである。 (検出事項)開発に関する明文の規定は存在しない。 (影響) 自社開発されたアプリケーションについて、処理に誤りなどが存在する可能性があるため、業務処理統制の評価を十分行う必要がある。	記載省略	中	
	以下省略																
が務実変 失処施更 わ理さ管 れ統れ理 る制なが のい適 信と切 頼業に	変更管理	プログラムが改ざんされたり、承認なく変更されない		アプリケーション・プログラムの変更管理につき、規定があり、それに基づいた仕組みと手続が確立されている。	整備	予防	手作業	○	○	NA	月週	情報システム担当者へのヒヤリングと、規定および定型帳票の査閲により、変更管理手続の規定、および、それに従ったプロセスがあることを確かめた。		OK。規定とプロセスは存在する。 (留意点) プログラム変更については、規定により情報システム部長の承認が必要とされているが、実際には業務の忙しさとオープン系の導入により、一部混乱が生じて、変更の記録と管理が不十分な点がある、とヒヤリングした。こうした点について、運用の評価において検証を行うこと。	記載省略	低	
	以下省略																
を務告処の運 確処等入と用 保理力に での日集、財 なき信常計、登 頼業録、務備 ない性業報、報あ	運用管理	運用時の誤操作によって誤った処理が行われない		夜間バッチ処理の運用につき、正確性、完全性、正当性を満足する規定が存在し、それに基づくジョブ管理ツールが実装され、担当者の手続が確立されている。	整備	発見	併用	○	○	○	毎日	情報システム担当者へのヒヤリングと、規定およびジョブ管理ツールの説明書の査閲、及び、ウォークスルーにより、ツールの実装と夜間バッチ処理の異常の有無の確認方法を確かめた。		OK。夜間バッチの異常終了の有無を確認し、必要な対応を実施する仕組みが確立している。 (留意点) 在庫管理システムにつき、異常終了が頻発しているとのことなので、業務処理統制で、十分、評価を実施する必要がある。	記載省略	低	
	以下省略																
務力デ 処、一 理登タ の録、理 信頼処に 性理不 備、備 を確集 保計、あ でき報 なき告 ない等、財 務日情 の業入	データ管理	正当な権限、手続きによらないで、データの入力、訂正が実施されない		データ管理に関する規定、および、それに沿ったプロセスは存在するが、異常終了の際のデータ訂正について、運用担当者によるデータの直接の訂正が認められており、適切な職務分離がなされていない。	整備	予防	手作業	×	×	NA	毎日	情報システム担当者へのヒヤリングと、規定等の査閲により、データ管理の規定と手続きを確かめた。		正当な権限・手続きによらないデータの訂正が行われ、データの信頼性が失われる可能性があるため、不備に該当し、改善の必要がある。 (検出事項)規定において、運用担当者によるデータの直接訂正が認められている。 (影響) 関連する業務処理統制において、十分な評価を行う必要がある。	記載省略	中	
	以下省略																
が報ア あのク る改セ ざん管 理削不 削除等 備がな るさる と、財 務性	アクセス管理	データの改ざんや不正な参照、漏洩が起きないように、すべての担当者に適切な認証及びアクセス制御機能が存在する		イントラネット上のPCの使用については、個人IDとパスワードが必要であり、その管理は人事情報と連動して十分に行われている。ただし、パスワード設定のルールに関する規定は無い。	整備	予防	自動化	×	○	○	毎日	情報システム担当者へのヒヤリングと規定、説明書などの査閲により、イントラネットのID、パスワードの規定と手続きを確かめた。		パスワード設定のルールがないため、パスワードの強度について保証できない不備があり、改善を行うべきである。 (検出事項)パスワードの強度に関する規定がない。 (影響) 対象となる勘定科目に係るアプリケーションは、イントラネットと異なるアクセス管理を、アプリケーションごとに実施しているため、影響は小さいと考えられる。 (留意点)各アプリケーションごとの業務処理統制におけるアクセス管理の評価により、イントラネットの不備を補完できるかどうかを検討すること。	記載省略	中	
	以下省略																
が報ア あのク る改セ ざん管 理削不 削除等 備がな るさる と、財 務性	ネットワーク	ネットワークへの外部からの不正侵入により、データへの改ざんや不正な参照、漏洩が起きないようにする		ネットワークへの外部からの不正侵入を防止するための規定及びプロセスが存在する。	整備	予防	自動化	○	○	○	毎日	情報システム担当者へのヒヤリングと規定等の査閲により、ネットワークのセキュリティに関する規定を確かめた。		OK 規定に基づき、本社と倉庫を結ぶイントラネットはIP-VPNを使用している。	記載省略	低	
	以下省略																

整備状況については、問題なく実施されている場合に○、不備などがある場合に×、該当しない場合にNAを記載している。