



AIMConsulting

これから始める【IT統制評価】

Account
Information & Intelligence
Management
Consulting

エイアイエムコンサルティング株式会社
コンサルティングサービス事業部
ビジネスコンサルティンググループ

Agenda

■ IT統制の概要

- IT統制と評価範囲について
- IT統制の評価項目について

■ IT統制の評価ポイント

- IT全社統制の評価ポイント
- IT全般統制の評価ポイント～システム開発～
- IT全般統制の評価ポイント～システム変更～
- IT全般統制の評価ポイント～システム運用～
- IT全般統制の評価ポイント～アクセス管理～
- IT全般統制の評価ポイント～外部委託管理～
- IT業務処理統制の評価ポイント

■ IT統制評価を進めるにあたり

- IT統制評価の効果的な進め方～IT統制を巡る役割～

IT統制の概要

IT統制と評価範囲について

◆ IT統制の種類と評価範囲

IT 統制	1	IT全社統制	会社全体のITに係る方針・計画・ルール・手続
	2	IT全般統制	システムが有効に機能するために必要なルール・手続
	3	IT業務処理統制	システムのプログラムに組み込まれた個別機能による統制

評価範囲

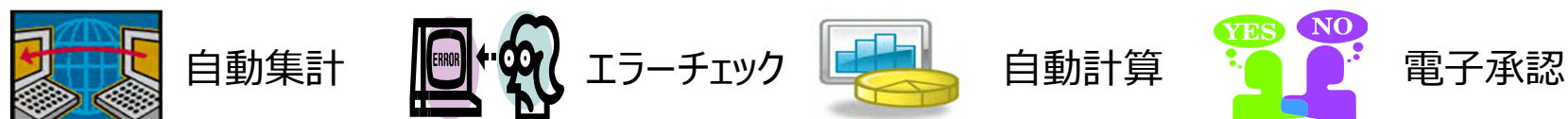
1 IT全社統制： 重要性が僅少な拠点を除く全拠点（全社統制と同様）



2 IT全般統制： 重要な勘定科目に係るシステム



3 IT業務処理統制： プログラムに組み込まれた個別機能



IT統制の評価項目について

◆ IT全社統制・IT全般統制・IT業務処理統制評価の項目

1 IT全社統制評価

会社全体のITに係る方針やルールが定められているかを評価

統制環境



IT戦略・方針

リスク評価と対応



ITリスク検討・対応

統制活動



IT統制・プロセス対応

情報と伝達



業務状況の伝達

モニタリング



モニタリングの仕組み

2 IT全般統制評価

システムが有効に機能するためのルール・手続が構築、運用されているかを評価

システム開発



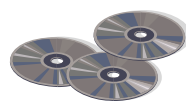
企画・開発・導入

システム変更



仕様変更・移行

システム運用



データ保管・管理

アクセス管理



安全性管理

外部委託管理

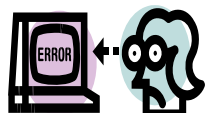


委託先管理・評価

3 IT業務処理統制評価

システム内の個別機能が正確に処理されているかを評価

入力チェック



自動チェックの適切性

マスタチェック



マスタとの一致性

データ自動転送



データ転送の整合性

データ自動計算



計算結果の整合性

ワークフロー



適切な承認権限

IT統制の評価ポイント

IT全社統制の評価ポイント

◆ IT全社統制の評価ポイント



ITに係る全社的なルールや管理体制が整備・運用されているか、会社単位で評価を行う。また、ITに係るリスクの評価が行われ、定期的にコントロールのモニタリングが行われていることを評価する。

■ リスク・コントロールと評価ポイント

基本的要素	リスク	コントロール例	評価ポイント
統制環境	経営方針と合致しないITが構築され、データの正確性が確保できない	ITの構築に関する事業計画書を策定し、承認する	<ul style="list-style-type: none"> ➤ IT構築計画の検討 ➤ 決裁者による承認
リスク評価	リスクの発見が遅れることにより、システムの安全性を損なう	1年に1回、ITリスクの有無や重要性に関する評価を行っている	<ul style="list-style-type: none"> ➤ リスク評価の記録 ➤ リスク対応の検討
統制活動	ITの利用ルールが周知されていないことにより、誤った処理が行われる	開発、運用、セキュリティ等、ITに係る規程を周知している	<ul style="list-style-type: none"> ➤ IT利用に関する規程類 ➤ 規程類の承認・周知
情報と伝達	ITに係る問題への対応が遅れ、問題発生による損害が拡大する	ITに係る問題が発生した際の連絡フローを構築している	<ul style="list-style-type: none"> ➤ 問題発生時の対応体制 ➤ 連絡に関する仕組みの有無
モニタリング	ITの利用に係る不正や誤謬の発見が遅れる可能性がある	部門長が業務モニタリングを実施し、問題点は報告する	<ul style="list-style-type: none"> ➤ モニタリング体制の設置 ➤ モニタリング結果の記録

IT全般統制の評価ポイント～システム開発～

◆ IT全般統制『システム開発』の評価ポイント



システム開発における各フェーズ（企画選定・要件定義・設計・開発・テスト・導入）の作業結果を記録し、その作業結果を関係者（特にユーザ部門）が承認しているかを評価する。

■ リスク・コントロールと評価ポイント

※システムリプレイスが行われた時のみ評価が必要になる。

開発フェーズ	リスク	コントロール例	評価ポイント
企画選定	ニーズに合ったシステムが構築できず、業務に影響を及ぼす	選定結果を稟議書に添付・回覧し、決裁者が承認する	<ul style="list-style-type: none"> ➤ 選定結果の記録 ➤ 選定結果の承認
要件定義	ユーザ部門が意図したシステムが開発されず、適切に利用できない	作成した要件定義書を回覧し、ユーザ部門が承認する	<ul style="list-style-type: none"> ➤ 要件定義書の作成 ➤ ユーザ部門による承認
設計	要件通りのシステムが構築できず、安全性を保証できない	システム設計書を作成し、情報システム部長が承認する	<ul style="list-style-type: none"> ➤ 設計書の作成 ➤ 情報システム部長の承認
開発	適切に開発が行われないことにより、誤ったデータが作成される	開発完了を報告し、情報システム部長が承認する	<ul style="list-style-type: none"> ➤ 開発完了の記録 ➤ 情報システム部長の承認
テスト	要件を満たしているか確認できず、数値の正確性を確保できない	要件定義に則り、テストを実施し、ユーザ部門が承認する	<ul style="list-style-type: none"> ➤ テストの実施記録 ➤ ユーザ部門による承認
導入	適切な移行が行われないことにより、データの網羅性を担保できない	本番環境への移行完了を報告し、ユーザ部門が承認する	<ul style="list-style-type: none"> ➤ 本番環境への登録確認 ➤ ユーザ部門による承認

IT全般統制の評価ポイント～システム変更～

◆ IT全般統制『システム変更』の評価ポイント



システム変更における各フェーズ（変更依頼・変更実施・テスト・移行・移行確認）の作業結果を記録し、その作業結果を関係者（特にユーザ部門）が承認しているかを評価する。

■ リスク・コントロールと評価ポイント

※評価年度内でシステム変更が発生した場合のみ評価を行う。

変更フェーズ	リスク	コントロール例	評価ポイント
変更依頼	不正につながるシステム変更が行われ、データの信頼性が失われる	変更申請書で依頼し、ユーザ部門長が承認する	<ul style="list-style-type: none"> ➤ 変更依頼の記録 ➤ ユーザ部門による承認
変更実施	ユーザ部門が意図したシステムに変更されず、数値に影響を及ぼす	変更申請書に作業記録を残し、情報システム部長が承認する	<ul style="list-style-type: none"> ➤ 変更実施の記録 ➤ 情報システム部長の承認
テスト	要件の充足や適否が確認できず、数値の正確性を確保できない	変更申請書にテスト記録を残し、ユーザ部門長が承認する	<ul style="list-style-type: none"> ➤ テスト実施の記録 ➤ ユーザ部門による承認
移行	不適切なプログラムが移行され、不正処理が行われる	変更申請書に移行記録を残し、システム部長が承認する	<ul style="list-style-type: none"> ➤ 移行完了の記録 ➤ システム部門による承認
移行確認	ユーザが意図したシステム変更が行われず、システムを利用できない	変更申請書に確認結果を残し、ユーザ部門長が承認する	<ul style="list-style-type: none"> ➤ 本番環境への登録確認 ➤ ユーザ部門による承認

IT全般統制の評価ポイント～システム運用～

◆ IT全般統制『システム運用』の評価ポイント



安定的にシステムを利用するための仕組みがあり、正しく運用されているかを評価する。障害の発生に備え、定期的にデータを保存して迅速に復旧できる仕組みが整備され、運用されているかを評価する。

■ リスク・コントロールと評価ポイント

運用業務	リスク	コントロール例	評価ポイント
ジョブ設定	ジョブが実行されず、正確なデータ処理が行われない	ジョブ設定申請書を作成し、部門長の承認を受ける	<ul style="list-style-type: none"> ➤ ジョブ設定の承認 ➤ 設定権限者の制限
バックアップ	適切に実施されないと、障害発生時に、データが消失する	定期的にバックアップを実施し、実施記録を保存・承認している	<ul style="list-style-type: none"> ➤ 定期的な実施 ➤ バックアップ実施の承認
データ管理	リカバリー手順が不明確であると、データを復旧できない	バックアップデータの復旧手順を定め、定期的にテストを行う	<ul style="list-style-type: none"> ➤ リカバリー手順の明文化 ➤ リカバリーテストの実施
障害管理	障害が起きた際に迅速に対応できず、大きな損害を被る	原因・対応を障害報告書に記録し、部門長の承認を受ける	<ul style="list-style-type: none"> ➤ 原因・対応の分析 ➤ 障害記録の承認
ログ管理	問題発生時、原因究明ができず、問題解決ができない	不正処理が行われた場合、警告が出る仕組みとなっている	<ul style="list-style-type: none"> ➤ 監視の定期実施 ➤ 不正分析の可否

IT全般統制の評価ポイント～アクセス管理～

◆ IT全般統制『アクセス管理』の評価ポイント



不正アクセスによるデータの改ざん・破壊のリスクに対する各管理対象ID（アプリケーション・ネットワーク・データベース・データセンター等）の発行・棚卸・モニタリングといったコントロールを評価する。

※特に特権ID（マスター等の作成、変更、削除が可能な特別なID）の管理には留意が必要である。

■ リスク・コントロールと評価ポイント

管理対象	リスク	コントロール例	評価ポイント
アプリケーション	不正アクセスにより、データの改ざんや破壊が行われる	申請書で依頼し、承認する。半期に1回アカウントを棚卸する	<ul style="list-style-type: none"> ➤ 職権と合致した権限 ➤ 定期的な棚卸の実施
ネットワーク	外部からの不正侵入により、システムへの攻撃を受ける危険性がある	利用者を制限しており、利用する際は承認後、作業を行う	<ul style="list-style-type: none"> ➤ 外部接続に関する承認 ➤ ネットワークのログ監視
データベース	不正アクセスにより、データの改ざんや破壊が行われる	修正申請書の承認後、作業を実施し、結果を記録する	<ul style="list-style-type: none"> ➤ 権限の制限、承認 ➤ 作業履歴の管理
データセンター	不正アクセスにより、データの改ざんや破壊が行われる	入退館記録を残し、申請の有無を定期的に確認する	<ul style="list-style-type: none"> ➤ 入館申請、物理的制限 ➤ 入退館のログ管理
パスワード	なりすましによるデータの改ざんや不正な参照が起きる	文字制限および、半年に1回自動で変更を促す仕組みがある	<ul style="list-style-type: none"> ➤ 桁数や文字の制限 ➤ 定期的な変更の設定

IT全般統制の評価ポイント～外部委託管理～

◆ IT全般統制『外部委託管理』の評価ポイント



開発や運用等、IT業務を外部に委託する際、適切なプロセスを経て委託先（ITベンダー）を選定し、委託元（企業側）が委託先（ITベンダー）の作業状況を定期的に確認しているかを評価する。

■ リスク・コントロールと評価ポイント

※SLA：サービスの提供者とその利用者間で結ばれるサービス水準に関する合意書

実施業務		リスク	コントロール例	評価ポイント
選定	計画の承認	委託元の担当者と委託先との癒着による不正が行われる	外部委託に係る計画書を作成し、決裁者が承認する	<ul style="list-style-type: none"> ➤ 依頼内容の明文化 ➤ 決裁者による承認
	委託先調査	開発・運用が適切に行われず、数値の正確性に影響を及ぼす	各業者の提案内容について、比較資料を作成し、承認する	<ul style="list-style-type: none"> ➤ 選定根拠の有無 ➤ 関係者による承認
	選定・契約	問題が発生した場合の責任が不明確となり、対応が遅れる	契約書の社内承認を経て、委託先と契約書を締結する	<ul style="list-style-type: none"> ➤ 委託契約書の承認 ➤ SLAの締結
品質確認	状況報告	委託先への牽制が働かず、不正・誤謬が発生する可能性がある	委託先から報告書を受領し、情報システム部長が承認する	<ul style="list-style-type: none"> ➤ 報告書を受領 ➤ 委託管理者による承認
	検査実施	委託先のサービス品質が低下し、数値の正確性に影響を及ぼす	問題点等があれば改善指示を行い、対応結果を確認する	<ul style="list-style-type: none"> ➤ SLA維持 ➤ 改善指示結果の承認

IT業務処理統制の評価ポイント

◆ IT業務処理統制における評価ポイント



業務に組み込まれたIT統制の状況について、実際のプログラム機能上のコントロール手段（エラーチェック、マスタチェック、自動計算等）をテスト環境で再現して評価する。

※プログラムの変更が無く、かつ前年度の評価が有効であれば、毎年評価を行う必要はない。

■ リスク・コントロールと評価ポイント

統制内容	リスク	コントロール例	評価ポイント
エラー チェック	システムへの入力ミスにより、誤った金額が計上される	上限を超えた金額を入力した場合、エラーメッセージが出る	<ul style="list-style-type: none"> エラーメッセージの出力（不一致金額を入力し再現）
マスタ チェック	架空の取引先との間での不正取引が行われる	登録されていない取引先は、起票できないようになっている	<ul style="list-style-type: none"> エラーメッセージの出力（架空の取引先を登録し再現）
データ 自動転送	システムへの転記ミスにより、誤った金額が計上される	基幹システムのデータは、会計システムに自動で反映される	<ul style="list-style-type: none"> 転送前後の数値一致（転送前後の値を照合確認）
データ 自動計算	担当者の計算ミスにより、誤った金額が計上される	処理画面上で計算が実行され、自動で金額が算出される	<ul style="list-style-type: none"> 計算前後の数値一致（1件再計算を行って確認）
担当者別の 権限制御	職務権限以上の操作が可能であることにより、不正処理が行われる	担当者と承認者で利用できる機能を制限している	<ul style="list-style-type: none"> 担当者別の設定確認（利用機能の違いを確認）

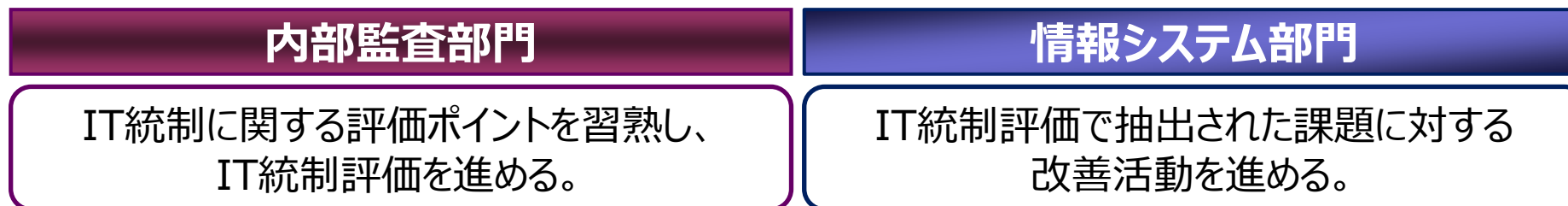
IT統制評価を進めるにあたり

IT統制評価の効果的な進め方～IT統制を巡る役割～

◆ IT統制を巡る内部監査部門と情報システム部門の役割



◆ IT統制評価の効果的な進め方



IT統制の評価は…

内部監査部門が評価を実施し、情報システム部門は改善活動（IT統制の構築・運用）を進める。



AIMConsulting

これから始める情報システム監査

Account
Information & Intelligence
Management
Consulting

エイアイエムコンサルティング株式会社
コンサルティングサービス事業部
ビジネスコンサルティンググループ

Agenda

■ 情報システム監査の進め方

- 情報システム監査における監査テーマ
- 情報システムにおける内部監査部門に求められる役割
- 情報システム監査の全体プロセス

■ 情報システム監査における確認ポイント

- これから始める情報システム監査のポイント：IT戦略とIT予算
- これから始める情報システム監査のポイント：情報システム部門の体制
- これから始める情報システム監査のポイント：情報システム関連規程
- これから始める情報システム監査のポイント：障害・復旧
- これから始める情報システム監査のポイント：論理的アクセスコントロール
- これから始める情報システム監査のポイント：物理的アクセスコントロール

■ 内部監査部門が行う情報システム監査上の留意点

情報システム監査の進め方

情報システム監査における監査テーマ

◆ 情報システム監査における監査テーマの検討

情報システムに関する監査テーマは多岐にわたる。上場企業であれば、**J-SOX（IT統制の構築・評価）**、**ISMS**や**Pマーク**の認証に必要な監査もあるため、**各監査との棲み分けを行い、重複を避けて監査を実施**することが望ましい。

◆ 主な監査テーマと各要素の関係性 ※J-SOXやISMS、Pマーク等でカバーできていないテーマを中心に情報システム監査を行う。

	情報システム関連の 主な監査テーマ	財務報告に直接かかわるシステム中心	情報セキュリティ中心	個人情報関係中心
		J-SOX 内部統制報告制度	ISMS 情報セキュリティマネジメントシステム	Pマーク 個人情報保護マネジメントシステム
基礎	IT戦略とIT予算	△（全システムではなく対象システムのみ）	ISMSでは対象外	Pマークでは対象外
	情報システム部門の体制	△（全システムではなく対象システムのみ）	△（情報セキュリティのみ対象）	△（個人情報管理のみ対象）
	情報システム関連規程	△（全システムではなく対象システムのみ）	△（情報セキュリティのみ対象）	△（個人情報管理のみ対象）
個別	情報システムの障害・復旧	△（全システムではなく対象システムのみ）	○	Pマークでは 対象外
	論理的アクセスコントロール	△（全システムではなく対象システムのみ）	○	
	物理的アクセスコントロール	△（全システムではなく対象システムのみ）	○	
	個人情報保護	J-SOXでは 対象外	ISMSでは対象外	○
	セキュリティポリシー		○	Pマークでは 対象外
	サイバー攻撃		○	
	システムの開発・変更	△（全システムではなく対象システムのみ）	ISMSでは 対象外	
	システムの運用	△（全システムではなく対象システムのみ）	ISMSでは 対象外	Pマークでは 対象外
	委託先管理	△（全システムではなく対象システムのみ）		

※対象外としている項目でも一部対象になっている場合があります。

★ 監査テーマは、情報システム監査の実施状況によっても異なる★

これから監査を始める場合は、**情報システム管理の土台となる基礎（方針・規程や体制）から監査**を行い、情報セキュリティの観点から、**自社の状況を踏まえて個別にテーマ（障害・復旧やアクセスコントロール等）を選択**して監査を行う。

情報システムにおける内部監査部門に求められる役割

◆ 内部監査部門に求められる役割

情報システム監査が行われていない場合、システム関係の『**規程**』や『**体制**』が整備されていないことが多い。**これから情報システム監査を行うのであれば、情報システム管理における『**規程**』や『**体制**』から監査することが求められる。**

◆ これから情報システム監査を行う場合の監査テーマ

情報システムは会社の戦略と合致しているか

【確認事項】会社の経営戦略や中期経営計画と現システムと今後のシステム計画が考慮されているか確認する。

【達成目標】会社として情報システムへの投資計画が経営戦略や中期経営計画が一致している。



情報システム部門の役割が定められているか

【確認事項】業務分掌規程等に情報システムに関する担当部門と役割が明記されているか確認する。

【達成目標】会社として情報システム部門の担当者はどのようなことを行うか明文化し、位置づけを定める。



情報システム内のルールが策定されているか

【確認事項】情報システム部門に関係する規程・マニュアル・作業手順書等が作成されているか確認する。

【達成目標】情報システム部門の業務が適正に設計され、属人化されていない。



情報システムに関する体制に問題がないか

【確認事項】会社規模・システム数・システムの難易度等を勘案し、担当者のレベル・人数等を確認する。

【達成目標】会社として情報システム部門の担当者のレベル・人数等が適正である。



★ システムリスク低減に向けた監査の実施 ★

監査では、システムリスクを低減するための対策が整備され、運用されているかを客観的に評価（チェック）し、改善を促すことが求められる。システムリスク低減の**根幹である『**規程**』と『**体制**』から、整備・運用されているかを監査するべきである。**

情報システム監査の全体プロセス

◆ 情報システム監査の全体像

通常の内部監査プロセスと同様、PDCAサイクルに従って行が、情報システム監査の特徴に留意して監査を遂行する。

◆ 情報システム監査プロセス







情報システム監査における確認ポイント

これから始める情報システム監査のポイント：IT戦略とIT予算

◆「IT戦略とIT予算」の監査ポイント

会社全体のIT戦略やIT予算が明確でない場合、戦略に合致したIT投資が行われず、事業計画に遅れが生じるリスクがある。内部監査部門は、**IT戦略やIT予算の判断基準や手続が定められ、適切に運用されているかを監査**する。

◆「IT戦略とIT予算」の監査方法（例）

	検証内容	監査手続	確認ポイント
	IT予算が1年ごとに作成され、取締役会等で承認されているか。	取締役会議事録等を確認し、IT予算が承認されていることを確認する。	<ul style="list-style-type: none"> IT予算資料の有無 意思決定機関による承認
	情報システム投資の「費用対効果」判定基準が文書化されているか。	情報システム管理規程等に「費用対効果」の判定基準が規定されているかを確認する。	<ul style="list-style-type: none"> IT投資判断基準の文書化 IT投資決定プロセスの有無
	定められた判定基準に従って、投資の可否が決定されているか。	システム投資の稟議書や申請書等を入手し、判定基準が反映されているかを確認する。	<ul style="list-style-type: none"> IT投資に関する記録の有無 IT投資判定基準の遵守
	意思決定者に適時かつ適切にITに関する情報が伝達されているか。	議事録や資料等を入手し、ITに関する情報の伝達がなされているかを確認する。	<ul style="list-style-type: none"> IT管理者への経営戦略の伝達 定期的な報告体制の有無

★経営戦略とIT予算の整合性！★





情報システム部門や特定の部門の意見だけを反映する形でIT予算が編成されてしまうと、全社的に最適なIT投資と乖離する可能性がある。**内部監査部門は、IT投資に関する判断基準が明確にされており、遵守されているかを確認**する。

これから始める情報システム監査のポイント：情報システム部門の体制

◆「情報システム部門の体制」の監査ポイント

情報システム部門は、システムを安定稼働させるため、IT技術の進歩に追随し、体制整備やスキルの強化を行うべきである。内部監査部門は、**ITに関するスキルの強化、リスクや問題点等の情報共有が行われているかを監査**する。

◆「情報システム部門の体制」の監査方法（例）

	検証内容	監査手続	確認ポイント
	情報システム部員の資格やスキルが適宜、把握され文書化されているか。	情報システム部員に求める資格やスキルの一覧が作成されているかを確認する。	<ul style="list-style-type: none"> 資格やスキルに係る資料の有無 資格やスキルの取得管理
	情報システム部門長は部門の目標や方針を明文化し、共有しているか。	部門目標、方針が明文化されているか、また、共有方法についても確認する。	<ul style="list-style-type: none"> 部門目標の有無 部門目標の共有状況
	開発部門・運用部門が定期的にリスク・問題点等を共有しているか。	議事録等入手し、定期的にリスクや問題点の共有が行われているかを確認する。	<ul style="list-style-type: none"> 定期的な会議の実施 リスクや問題点の把握
	他部門に対して研修等を行い、ITリテラシーの向上に努めているか。	研修計画や研修資料入手し、IT利用に関する研修を実施していることを確認する。	<ul style="list-style-type: none"> 定期的な研修の実施 研修の参加状況

★情報システムの安定稼働に向けたスキルの強化！★





情報システム部門は、ITに係るスキルを習得するとともに、利用部門に対してもITの利用ルール等を周知徹底させることが求められる。**内部監査部門は、ITスキルの向上に努め、ルールを周知しているか、情報システム部門の活動状況を確認**する。

これから始める情報システム監査のポイント：情報システム関連規程

◆「情報システム関連規程」の監査ポイント

情報システム部門は、情報システムを管理するにあたり、各業務（システム開発・変更・運用・情報セキュリティ・委託先管理等）のルールを整備し運用する必要がある。内部監査部門は、**各規程の整備状況および運用状況を監査**する。

◆「情報システム関連規程」の監査方法（例）

	検証内容	監査手続	確認ポイント
	情報システムの開発/変更の基準等が明文化されているか。	情報システムの開発/変更の方針・基準が取締役会等で承認されているか確認する。	<ul style="list-style-type: none"> 開発/変更の基準に関する承認 開発/変更プロセスの明文化
	運用設計に基づいて、管理規則および運用手順は作成されているか。	情報システムの運用ルールを定めた規程・細則・マニュアル等があるか確認する。	<ul style="list-style-type: none"> 運用ルールの承認 運用計画の有無
	情報セキュリティに対する基本方針・実施手順が整備されているか。	情報セキュリティの基本方針・実施手順が体系的に明文化されているか確認する。	<ul style="list-style-type: none"> 管理基準、実施手順の有無 基本方針・実施手順の周知
	委託業者を選定する際の選定基準が文書化され、周知されているか。	委託先の選定基準やサービス品質の評価ルール等が明文化されているかを確認する。	<ul style="list-style-type: none"> 選定基準や手続の明文化 委託先評価の実施

★情報システムに係るルールの整備・運用！★





情報システムの管理ルールが明文化されておらず、情報システム部門の業務がブラックボックスになっているケースもある。**内部監査部門は、ルールが整備・運用されているかを確認し、改善指導を行うことにより、情報システムの管理精度を高める。**

これから始める情報システム監査のポイント：障害・復旧

◆「障害・復旧」の監査ポイント

情報システム部門の役割として、障害が発生した場合においてもシステムを復旧させ、業務に影響を与えないようにすることが求められる。内部監査部門は、**早期復旧の手順や体制が整備され、運用できているかを監査**する。

◆「障害・復旧」の監査方法（例）

	検証内容	監査手続	確認ポイント
	障害発生時の復旧手順、体制が明確になっているか。	規程、マニュアル等を確認し、障害発生時のフローが文書化されていることを確認する。	<ul style="list-style-type: none"> ・障害発生時の対応手順の有無 ・対応手順の改定状況
	情報システムの障害発生時の緊急窓口が全社員に周知されているか。	障害発生時の緊急窓口の周知文や周知方法を確認する。	<ul style="list-style-type: none"> ・全社への周知状況 ・障害発生時の連絡先の有無
	障害発生時の実施要領に従い、定期的に訓練が行われているか。	障害発生対応フローを訓練した履歴やシミュレーションした記録を確認する。	<ul style="list-style-type: none"> ・定期的な訓練の実施 ・訓練実施記録の有無
	障害発生時の真因が追及され、再発防止の対策が講じられているか。	障害対応の記録に、真因まで言及され再発防止策が検討・実施されているか確認する。	<ul style="list-style-type: none"> ・真因の把握状況 ・再発防止策の進捗記録

★障害発生時の真因追求が大事！★





障害対応の仕組みがあっても、障害発生時の真因まで特定して対策が講じられていないケースが見受けられる。障害は再発する可能性があるため、**内部監査部門は、障害発生時の真因を把握し、適切に再発防止策が講じられてるかを監査**する。

これから始める情報システム監査のポイント：論理的アクセスコントロール

◆「論理的アクセスコントロール」の監査ポイント

不正アクセスによる情報漏えいやデータの改ざん等を防ぐため、論理的アクセスコントロールは重要なテーマである。内部監査部門は、アクセス制限等の予防的統制やモニタリング等の発見的統制が行われているかを監査する。

◆「論理的アクセスコントロール」の監査方法（例）

	検証内容	監査手続	確認ポイント
	対象範囲と許可する利用者を適切に特定し、強度を変えているか。	アクセス権に関する台帳等を入手し、適切に利用範囲を定めているかを確認する。	<ul style="list-style-type: none"> アクセス権を定義した資料の有無 職務権限に応じたアクセス付与
	特権IDの利用が必要最低限になるようなルールになっているか。	特権IDの付与ルールが規定され、リスクが最小になるようなルールになっているか確認する。	<ul style="list-style-type: none"> 特権ID付与ルールの有無 特権ID付与対象者の定義
	定期的にユーザアカウントの棚卸を実施し、不要なIDが残っていないか。	アカウント棚卸の実施記録を入手し、定期的に棚卸が行われていることを確認する。	<ul style="list-style-type: none"> 定期的なアカウント棚卸の実施 不要IDの削除（退職者等）
	不正処理が行われていないかを定期的に確認しているか。	ログの収集状況を把握し、定期的なログのモニタリングが行われているかを確認する。	<ul style="list-style-type: none"> モニタリング記録の有無 営業時間外の利用理由の特定

★予防的統制・発見的統制の統制状況を確認！★

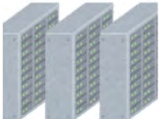



内部関係者による情報システムに係る不正行為（情報漏えいやデータの改ざん）が増えている。内部監査部門は、職務権限に応じてアカウントを付与しているか、定期的にシステムの利用状況のモニタリングが行われているかを監査する。

これから始める情報システム監査のポイント：物理的アクセスコントロール

◆「物理的アクセスコントロール」の監査ポイント

情報システム部門としては、設備に対する統制・入退館に対する統制・IT機器（パソコン・スマートフォン等）に対する管理を行う必要がある。内部監査部門は、ヒアリングや視察も交えて、物理的アクセスコントロールの監査を行う。

◆「物理的アクセスコントロール」の監査方法（例）

	検証内容	監査手続	確認ポイント
	データセンター等で地震等の被害を最小限にする対策が取られているか。	データセンターの仕様書等を入手し、物理的なトラブルの対策を確認する。	<ul style="list-style-type: none"> ・物理的対策の明文化 ・ラック等、災害対策の実施状況
	データセンター等で入退館記録の取得、監視カメラの設置がされているか。	入退出記録の取得状況および、監視カメラ等の設置状況を確認する。	<ul style="list-style-type: none"> ・入退館記録の有無 ・監視する仕組みの有無
	パソコンの盗難防止対策や不正使用の対策が取られているか。	ヒアリングや実査により、パソコンの盗難対策ルールや対策の実施状況を確認する。	<ul style="list-style-type: none"> ・施錠可能な場所への保管 ・外部記憶媒体への保存禁止
	不正処理が行われていないかを定期的に確認しているか。	携帯端末の紛失・盗難発生時における情報漏えい対策が取られているかを確認する。	<ul style="list-style-type: none"> ・パスワードロックの設定 ・遠隔操作によるデータ消去

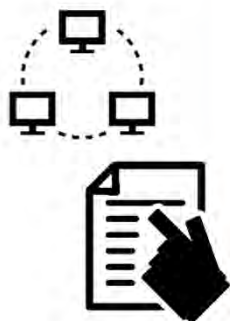
★人的なリスクも含め、監査を実施！★

IT機器の紛失・盗難等、人的な要因により、情報セキュリティが損なわれるリスクがある。内部監査部門は、情報システム部門の管理体制や管理ルールだけでなく、外部ベンダーやユーザー部門の利用状況も対象に含めて監査を行う。

内部監査部門が行う 情報システム監査上の留意点

内部監査部門が行う情報システム監査上の留意点

◆ 情報システム監査における実務上の留意点

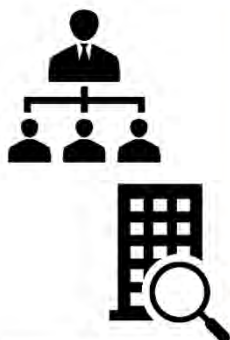


他の監査との
棲み分け

! J-SOX（内部統制評価）、ISMSやPマーク等の監査との棲み分けを行い、重複をしないように監査を行う。

監査の実施状況・上場/非上場・認証等により、監査テーマは変わる。

上場会社ではIT統制の評価が強制されており、ISMSやPマークの認証に伴う監査が行われている企業も多い。**自社のシステム監査状況を踏まえて、内部監査部門が対応すべき監査テーマ（基礎・個別テーマ）を選択して実施することが望ましい。**

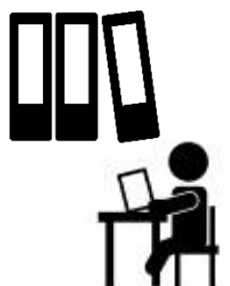


基礎テーマから
監査を実施

! これから内部監査部門が情報システム監査を行う場合は、**基礎テーマであるルールや体制から監査を行う。**

情報システムに関するルールや体制が整備できていないことも多い。

現在は多くの情報システムが利用されているが、システム管理ルールが規定されていない、情報システム部門の役割が曖昧になっているといった会社も少なくない。通常の監査と同様、**内部監査部門がルールや体制が整っているかを監査すべきである。**



情報システムに
係る知識

! **最低限のIT知識は必要になることから、基本的な情報システムの知識を習得して監査を行う。**

内部監査部門も基本的な情報システムの知識は習得すべきである。

プログラム言語やインフラの設計等、詳細なIT知識は不要であるが、**基本的なシステムの管理方法やシステムリスク、監査方法は理解**すべきである。経済産業省の「システム管理基準」「システム監査基準」等を活用し、基本的な知識を習得する。

AIMC

AIM Consulting

エイアイエムコンサルティング株式会社

<https://www.aimc.co.jp>

不明点等につきましては、下記よりお問合せください。

<http://www.aimc.co.jp/inquiry/>