# GAITメソドロジー

## GAIT

### The **G**uide to the **A**ssessment of **IT** Risk

### ITリスク評価のためのガイド

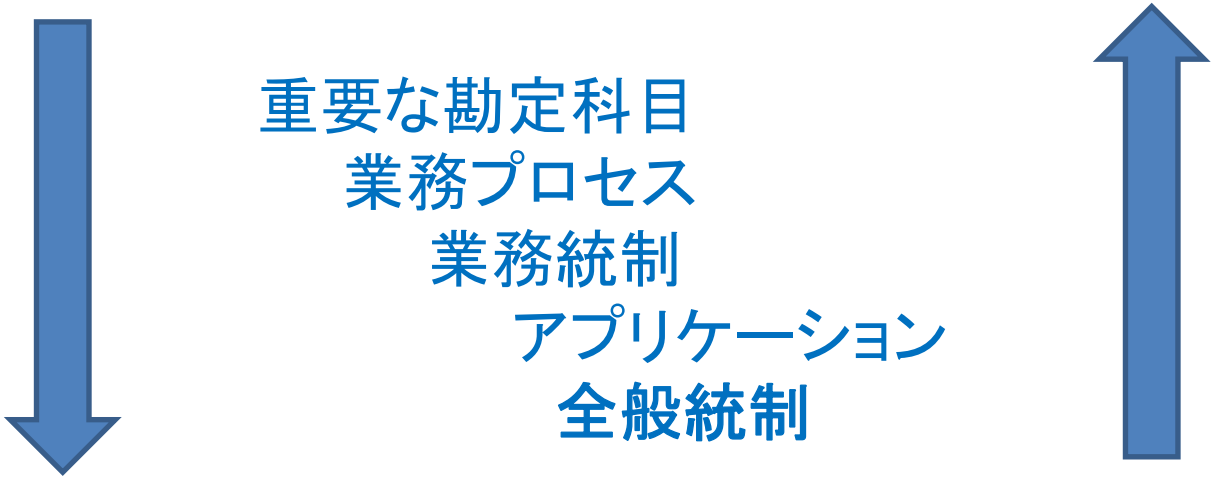
財務諸表上のリスク、業務プロセスのキー・コントロール、自動化されたコントロールとその他の重要なIT機能、IT全般統制のキー・コントロールについてそれぞれの関連を解説する一連の指針

GAITメソドロジー（トップダウン型リスクベース・アプローチによるIT全般統制のスコーピング）から発展しシリーズへ

# GAITメソドロジー

## ■ GAITメソドロジーによるスコーピング

財務諸表および開示について重要な虚偽記載リスクおよび不正のリスク




重要な虚偽記載または不正のリスクに応じてスコーピング

# GAITメソドロジー

## ■ ITリスク評価とスコーピング

**ステップ1：**
**理解の検証**

- 重要な勘定科目
  - 業務プロセス
    - 業務統制
      - アプリケーション
      - ITプロセス内の統制
        - 変更管理、オペレーション、セキュリティ
          - ・アプリケーション
          - ・データベース
          - ・オペレーションシステム
          - ・ネットワーク

**ステップ2：**
**リスク評価**

**ステップ3：　このITプロセス内の不備が、業務処理統制と財務諸表の重要な虚偽記載に影響するか？**

# GAITメソドロジー

## ■ 4つの原則

IT全般統制プロセスにおけるリスク等の識別のアプローチ:

- ✓ トップダウン、リスクベース

識別すべきIT全般統制プロセスのリスクが影響を与えるもの:

- ✓ 財務的に重要なアプリケーションに関連する重要なIT機能およびデータ

識別すべきIT全般統制プロセスのリスクが存在する場所:

- ✓ プロセス中の様々なITレイヤー(アプリケーションプログラムのコード、DB、OSおよびネットワーク)

IT統制プロセスにおけるリスクの軽減:

- ✓ 個別の統制ではなく、IT統制目標の達成による

# GAITメソドロジー

## 4つの原則： 原則1
（IT全般統制プロセスにおけるリスク等の識別のアプローチ）

### トップダウン、リスクベース

*ＩＴ全般統制プロセス（例えば、変更管理、導入・展開、アクセスのセキュリティ、運用等）におけるリスクおよび関連する統制の識別には、業務プロセスにおける重要な勘定科目、これら勘定科目に関するリスクとキー・コントロールを識別するために用いられるトップダウン型リスクベースのアプローチをとる*（AS2/AS5のアプローチを継承する）

＜フェーズ全体に適用＞

# GAITメソドロジー

## 4つの原則： 原則2
## （識別すべきIT全般統制プロセスのリスクが影響するもの）

### 財務的に重要なアプリケーションに関連する重要なIT機能およびデータ

*識別されるべきIT全般統制のフロセスにおけるリスクは、①財務的に重要なアプリケーションに関連するIT機能および②財務的に重要なアプリケーションに関連するデータ、に影響を与えるものである*

＜フェーズ2に適用＞

# GAITメソドロジー

## 4つの原則： 原則3
## （識別すべきIT全般統制プロセスのリスクが存在する場所）

*原則1に基づき、リスクベース・アプローチによる評価を行う*

**プロセス中の様々なITレイヤー（アプリケーションプログラムのコード、データベース、オペレーティングシステムおよびネットワーク）**

*識別すべきT全般統制プロセスのリスクは、IT全般統制各種プロセス中の様々なITレイヤー（アプリケーションプログラムのコード、データベース、オペレーティングシステムおよびネットワーク）に存在する*

＜フェーズ3に適用＞

# GAITメソドロジー

## 4つの原則： 原則4
## （IT統制プロセスにおけるリスクの軽減）

### 個別の統制ではなくIT統制目標の達成による

*IT全般統制プロセスにおけるリスクは、**IT統制目標**を達成することによって軽減されるものであり、**個別の統制によって軽減されるものではない***

＜フェーズ4に適用＞

# GAITメソドロジー

## ■ GAITを適用する際の5つのフェーズ

### フェーズ1

重要なIT機能を識別する（必要に応じ確認する）

### フェーズ2

IT全般統制をテストすべき（重要な）アプリケーションを識別する

### フェーズ3

IT全般統制プロセスのリスクとそれに関連する統制目標を識別する

### フェーズ4

統制目標に合致し、テストすべき、IT全般統制のキー・コントロールを識別する

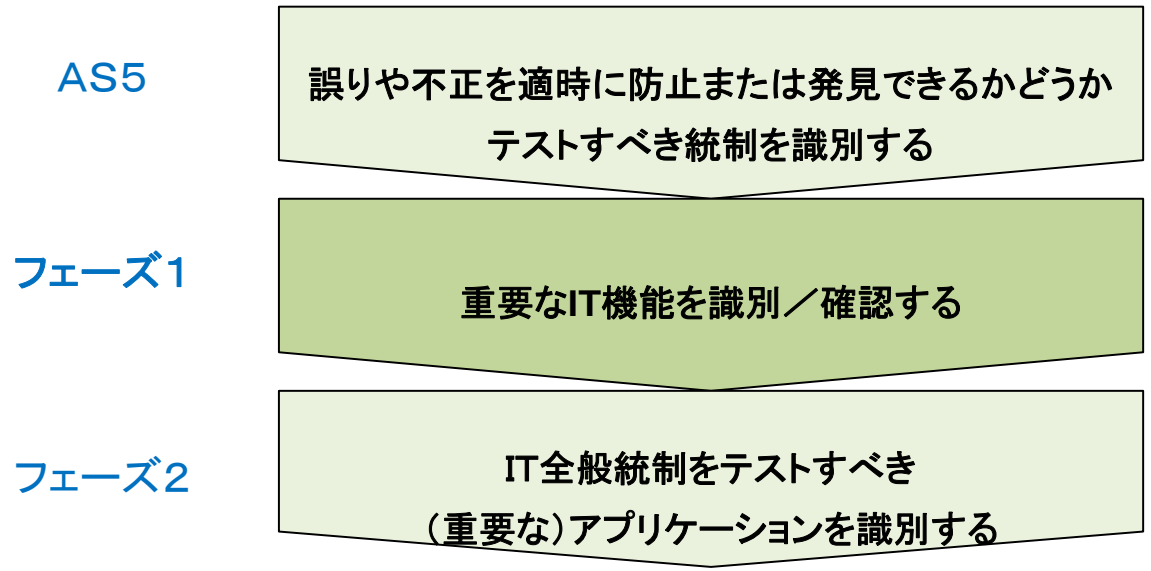
### フェーズ5

適切な人物によるレビューを実施する

# GAITメソドロジー

## フェーズ1： 重要なIT機能を識別する（必要に応じ確認する）

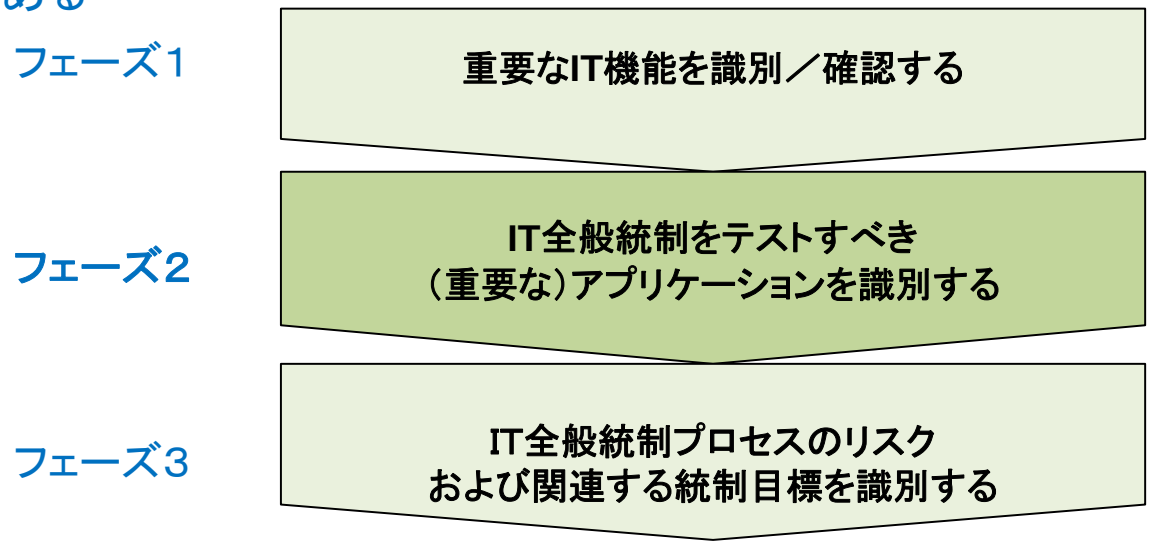
- 原則1に基づき、業務プロセスをトップダウンにより評価することにより、手作業によるキー・コントロールまたは自動化されたキー・コントロールを識別する
- GAITは、GAIT評価の基礎である重要なIT機能のリストを確定し、すべての重要なIT機能が識別されていることを保証することにより、トップダウンのプロセスを継続する。



# GAITメソドロジー

## フェーズ2： IT全般統制をテストすべき（重要な）アプリケーションを識別する

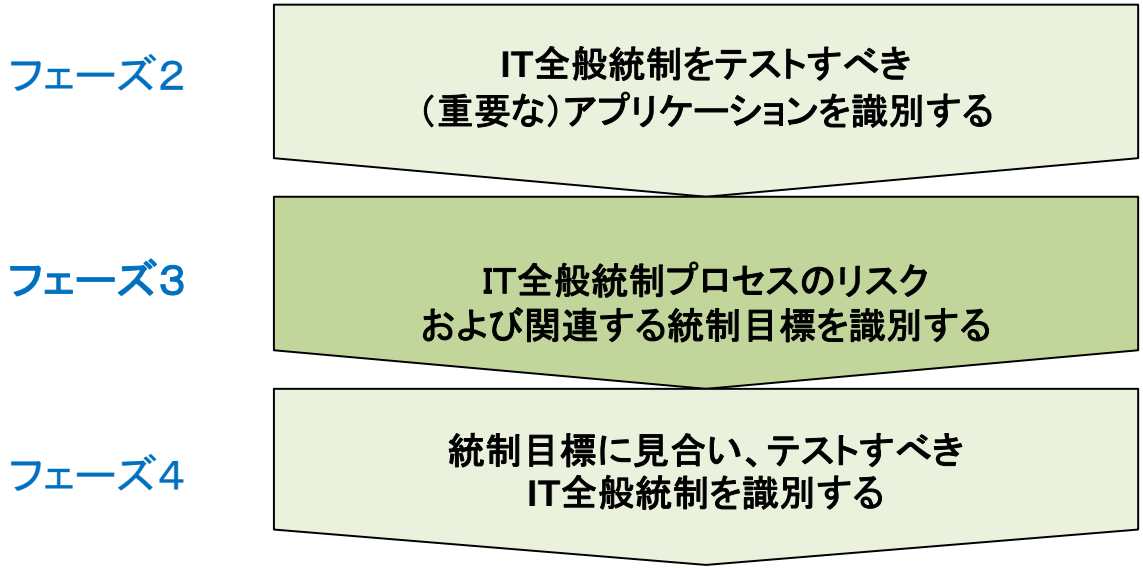
- 重要なIT機能の確認後、IT全般統制をテストすべき、財務的に重要なアプリケーションを確認する
- 財務的に重要なアプリケーションとは、原則2に基づき、重要なIT機能またはデータを含むためにIT全般統制プロセスのリスクが存在する可能性のあるアプリケーションである



# GAITメソドロジー

## フェーズ3： IT全般統制プロセスのリスクおよび関連する統制目標を識別する

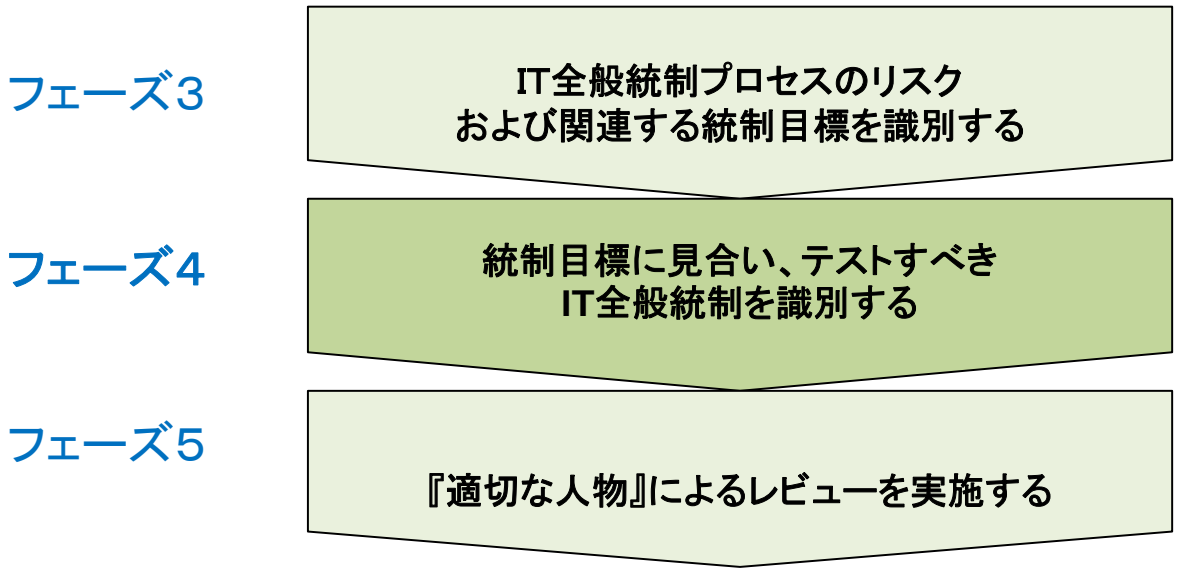
- 原則1に基づき、リスクベース・アプローチによる評価を行うため、重要なアプリケーションのそれぞれについてさらに情報を入手する
- 重要なアプリケーションのそれぞれについて、原則3に基づき、各レイヤーの各IT全般統制プロセスについてリスクを評価する



# GAITメソドロジー

## フェーズ4： 統制目標に見合い、テストすべき、IT全般統制のキー・コントロールを識別する

■ フェーズ3 IT全般統制のリスクおよび関連するIT統制目標の識別後、原則4に基づき、IT統制目標に対応するIT全般統制プロセスのキー・コントロールを具体的に決定する



# GAITメソドロジー

## フェーズ5： 適切な人物によるレビューを実施する

■ レビューに当っては、

① 独立した適切な人物の眼において、リスクおよびキー・コントロールが、財務諸表に対するリスクについて合理的な見方を示していることを確認する

② 404条スコーピング（評価範囲の決定）におけるリスク許容度を前提として、リスクの選択が合理的であることを保証する