

# 組織の成功に不可欠な 変更・パッチ管理のコントロール



## GTAG 2 ( I T 監査の国際的ガイダンス 2 )

# 本ガイドの内容

- IT変更・パッチ管理が健全なIT環境の基本である理由
- IT変更・パッチ管理のコントロールがITリスクとコストの管理を助ける方法
- 効果的な方法、非効果的な方法
- 変更のソースおよびビジネス目的への想定される影響

# このガイドの内容

- 有効な変更管理（ベストプラクティス）と無効な変更管理（危険信号）の比較
- IT変更にともなうリスクを軽減するために優先すべき5ステップ
- 評価ツールの提供および内部監査人のなすべきこと

まとめ： 本GTAGはIT変更管理のプロセスとリスクについての実用的な知識を提供

## IT変更管理の理解

- ビジネスの要件は高水準のIT稼動時間(可用性)を必要とするが、サーベンスオクスレー法などの法的要求は情報の機密性とインテグリティを必要とする
- 安定し管理されたIT本番環境であるためには、変更が予測可能で反復可能な方法で実施される必要がある
- 変更を行うIT担当者は、定義され、監視され、確実に実施される統制のゆきとどいたプロセスに準拠する必要がある
- 防止的コントロール(職責分離)と発見的コントロール(監督)を組み合わせる必要がある

# 変更管理の成熟度

効率性

組織が変更をコントロール:

変更が組織をコントロール:

## 1 - 反応型

- 50%以上の時間が計画されていない作業に費やされる
- 無秩序環境; その場しのぎ策がほとんど
- MTTR(平均修復時間)は非常に長い; 貧弱なサービスレベル
- 問題ごとに担当者を投入することのみで評価される

## 2 - 自己管理システム

- 30-50%時間が計画されていない作業に費やされる
- いくつかのテクノロジーが配備
- 正しいビジョンはあるがアカウントビリティ(説明責任)に欠ける
- 管理者あたりのサーバー率が低過ぎる
- ITコストが高過ぎる
- “適切な”担当者への会話でプロセスが覆る

## 3 - 閉ループプロセス

- 15-35%の時間が予定されていない作業に費やされる
- チケット制/ワークフローシステムがいくらか実施されている
- 変更が文書化され承認されている
- 変更の成功率は高い
- サービスレベルは良好かつ世界レベルである
- 管理者あたりのサーバー率は良好だがベストではない
- ITコストは改善中
- セキュリティインシデントは減少

## 4 - 継続的改善

- 5%以下の時間が計画されていない作業に費やされる
- 変更成功率は非常に高い
- サービスレベルは世界レベル
- ITオペレーションコストが管理されている
- ITのキャパシティがITコストにおける限界収益点の上昇で迅速に測定される
- 変更のレビューおよび学習プロセスが機能している
- 費用効率のよい方法でキャパシティの増加が可能

反応型

自己管理システム

閉ループ変更管理

継続的改善

# なぜ変更管理を監査するのか？

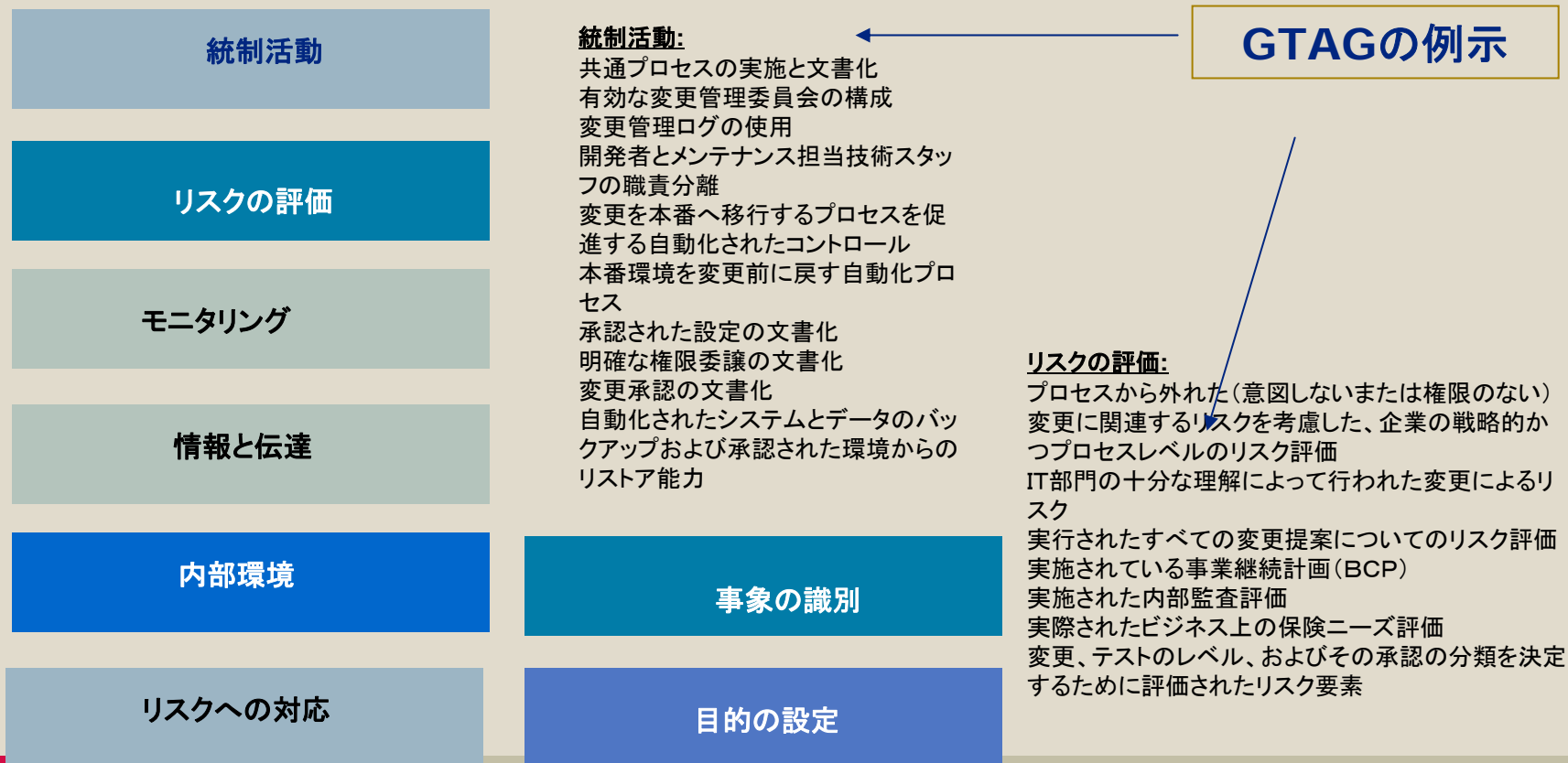
- ITコントロールに関する法的要求事項の増大
  - 監査委員会と経営者からの関心の増大
  - ITコントロールへのアシュアランスを提供する内部監査人の責任
- 技術はあらゆる場所に存在
  - 組織の情報処理の80%は電子的形態
  - 事業上のすべての決断は、結果的に少なくともひとつのIT変更をとともなう。変更がコントロールされない場合、組織全体に影響が及ぶ可能性がある
  - アナリストによると、機能障害の80%は変更が原因
- つまり、CAE(内部監査部門長)はITの変更管理の責任をIT監査人に転嫁できない

## 良好な変更・パッチ管理プロセスの利点

- より多くの時間を、事業の目的および目標を推進するための新規開発に費やせる
- 新しい可能性を実現するため、(その場しのぎに)“火を消す”のではなく、ITスタッフ資源を再配分できる
- 計画されていないIT作業へ費やす時間が少なくなる
- IT停止時間の減少
- 重要なパッチを最小の中断でインストール可能

# 変更・パッチ管理プロセスの評価

## 変更・パッチ管理のCOSO ERMモデル





# 役割と責任

- 取締役会 / ガバナンス機関
  - 監査委員会 – 変更管理などの重要プロセスのモニタリングによってITリスクをマネージする組織の能力を検討
- 経営管理者 – 変更管理プロセスの定義、承認、実施および実行
  - 開発者、オペレーター、テスト担当者、承認者、その他によってさまざまな役割
- 監査人
  - 内部監査人 – 経営管理者へアシュアランスを提供
  - 外部監査人 – 財務諸表を作成しサーベンスオクスレー法へ準拠するため、統制への依拠を判定する独立的評価