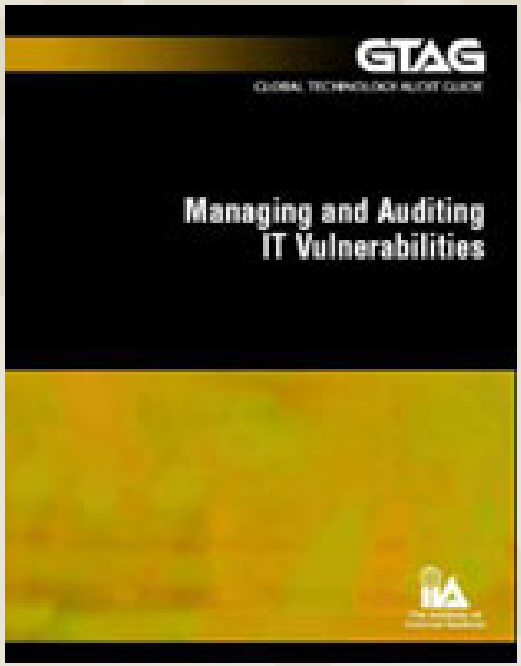
IT 脆弱性の
マネジメントと監査

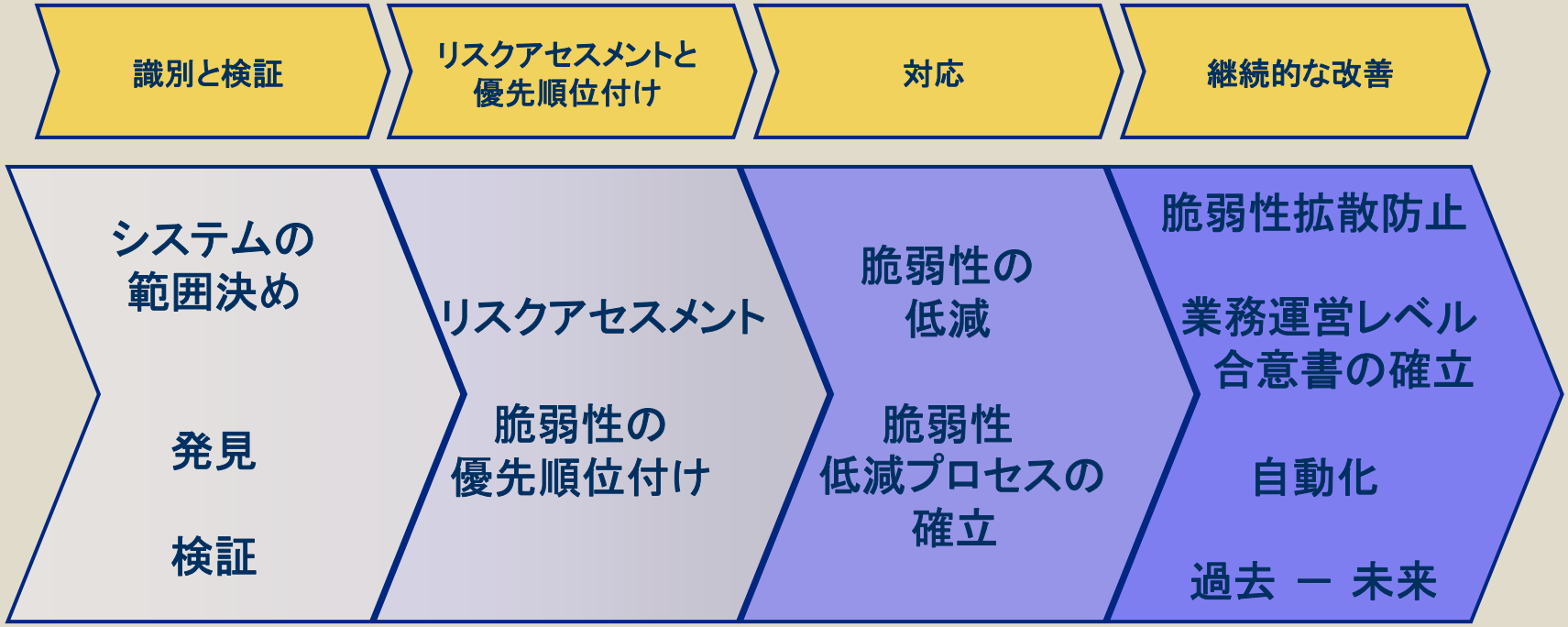


GTAG 6
（IT監査の国際的ガイダンス 6）

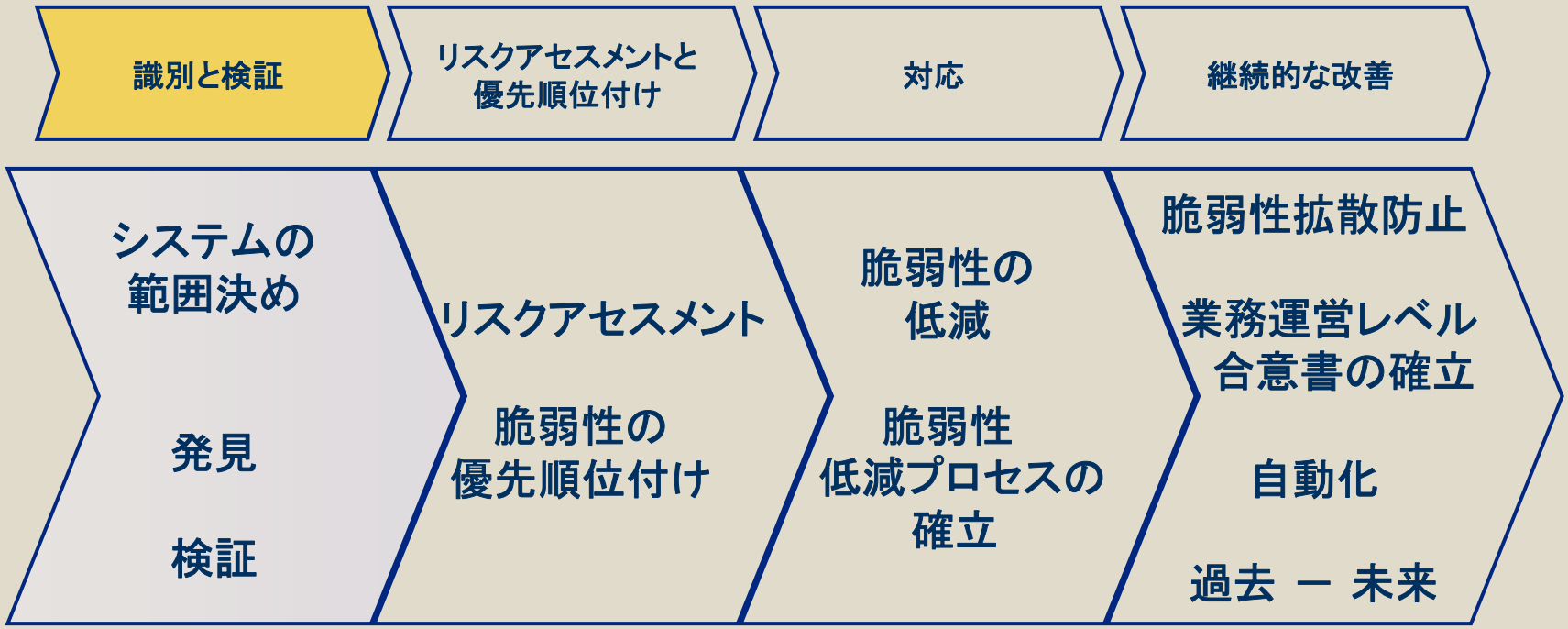
目次

- 脆弱性マネジメント・ライフサイクルの定義
- 脆弱性マネジメントの監査範囲
- 組織の成熟度
- 付録
  - 主要なメトリクス
  - リスク・マネジメント

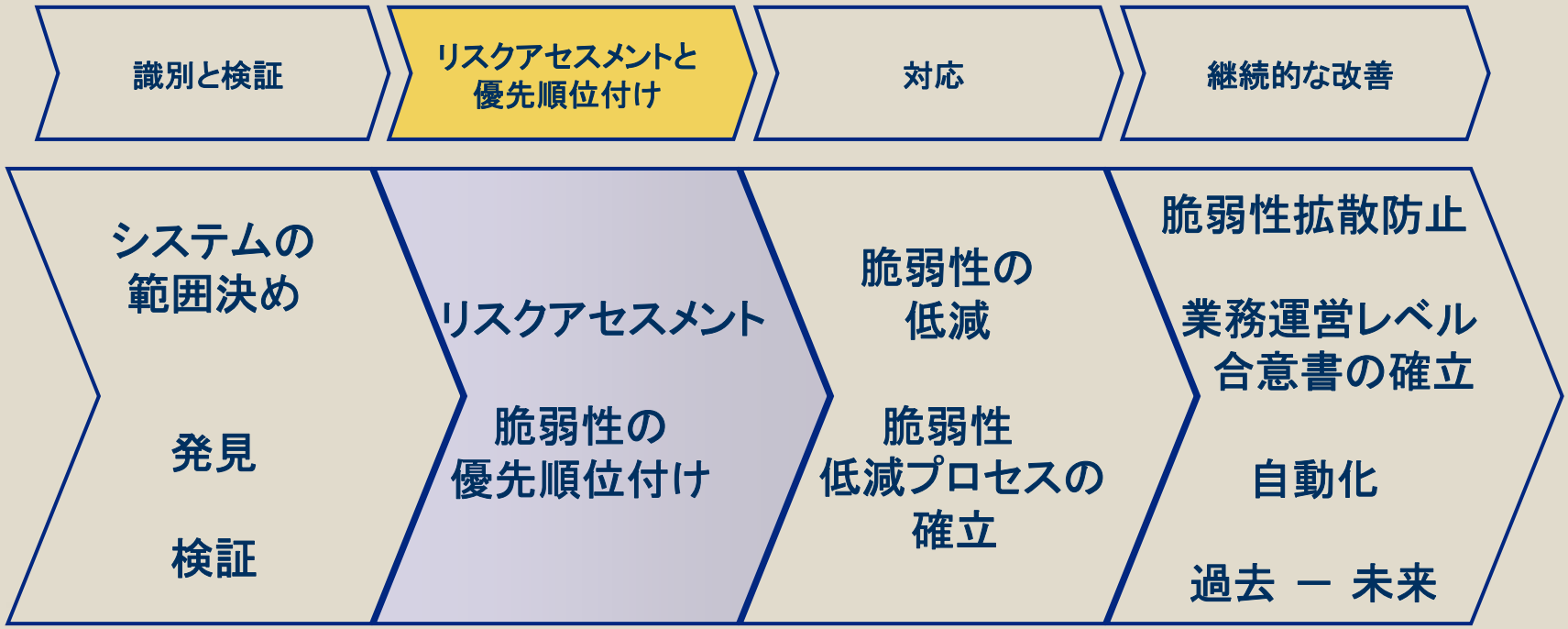
脆弱性マネジメントのライフサイクル



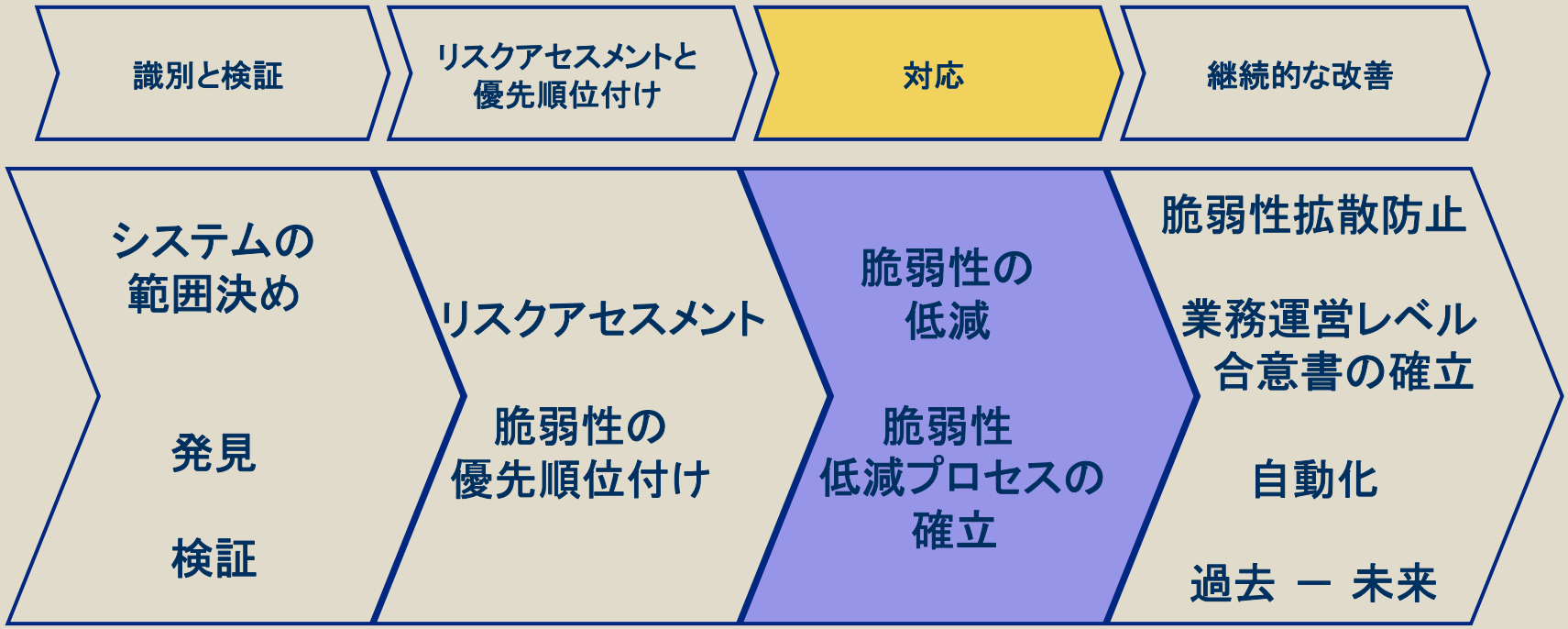
脆弱性マネジメントのライフサイクル



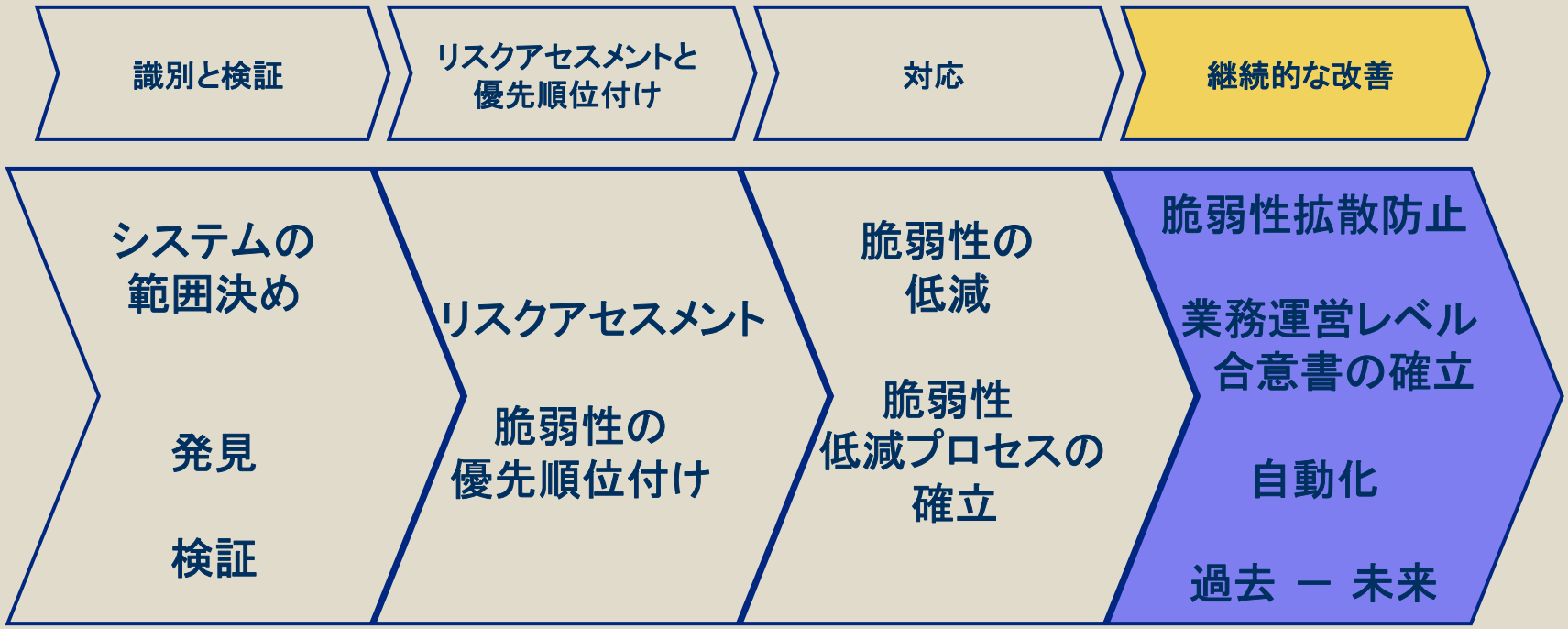
脆弱性マネジメントのライフサイクル



脆弱性マネジメントのライフサイクル



脆弱性マネジメントのライフサイクル



監査範囲

識別と検証 資産の目録 脆弱性の検知 発見事項の検証	**対応** モニタリング インシデント管理 変更管理 パッチテスト
リスクアセスメントと優先順位付け リスクアセスメント 脆弱性の優先順位	**保守と改善** 構成管理 オペレーションレベルの合意 方針と要求事項

組織の成熟度

識別と検証

未熟な組織

- IT資産を調査及び管理している割合が低い、あるいは管理していることが測定できない。
- ネットワーク構成図が不完全あるいは部分的
- 調査結果の検証不能
- 是正措置が限定的あるいは皆無
- 資産管理システムがない。
- 設定の不整合が多い。

成熟した組織

- 有効な資産管理
- 調査され、管理された重要な資産の割合を知っている。
- 調査を検証して間違った結果を識別する。

組織の成熟度

リスクアセスメントと優先順位付け

未熟な組織

- 重要なIT資産とそうでないものの区別や優先順位付けが行えない。
- 非常に数多くの修復すべき脆弱性がある。

成熟した組織

- 日常的なITリスクアセスメント
- 対応費用が見積もられている。
- 前回のパッチと変更メトリクスを活用して、高リスクなパッチを見つける。

組織の成熟度

対応

未熟な組織

- パッチ管理が自動化されていない。
- パッチテスト不足
- IT組織が処理できる以上の業務量がある。
- 構成管理がない、あるいは脆弱性管理を集成していない。
- 計画されていない業務

成熟した組織

- システム設定が標準化されている。
- 組織としての取決めがある。
- パッチテストを含めパッチ適用が、自動化されている。
- 対応が追跡され、検証されている。

組織の成熟度

継続的な改善

未熟な組織

- ごく限られた自動化されたプロセス
- OLAs（オペレーションレベルの合意）がない。
- 反動的である
- 混乱が発生して、セキュリティインシデントが検知される。
- パッチや変更の成功率が記録がない。

成熟した組織

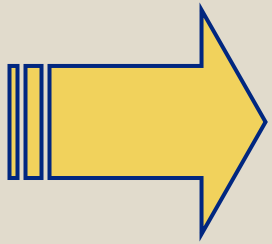
- 安全な構造のために構成管理に経営資源を投入している。
- 調査する頻度と範囲を増やしている。
- 生産に先立って装置が分析されている。
- 標準的なIT設定がある。
- パッチ適用によるリスクが識別されている。

主要なメトリクス

- 総システム数に対する、モニターまたは調査された割合.
- 異常な脆弱性の数
- 管理されているシステムの割合
- 検証されている脆弱性の割合
- 対応完了までの平均時間
- オペレーションレベルの合意 (OLA)件数
- 計画されていない業務に要した時間
- セキュリティインシデントの数
- セキュリティインシデントの影響度

リスクマネジメント

- 資産評価
- 脅威分析
- 脆弱性分析
- リスク測定
- リスク判定



脆弱性管理

類似した目標