1.マネジメント監査サービス

- 1.0監査方針確認
  - 1.01監査目的・監査スコープ確認
    - 1.011サイバーリスク認識の確認
  - 1.02監査基準選定
  - 1.03監査実施計画策定
- 1.1サイバーセキュリティマネジメント監査
  - 1.11ポリシー・管理体制評価
  - 1.12セキュリティリスクアセスメント評価
    - 1.121情報資産評価
    - 1.122脆弱性・脅威・リスク評価
  - 1.13リスク対策規程整備状況評価
  - 1.14リスク対策規程運用状況評価
  - 1.15自己点検・改善状況評価
- 1.2サイバーセキュリティ対策運用評価
  - 1.21日常インシデント管理体制評価
    - 1.211モニタリング・監視体制評価
    - 1.212ログ管理体制評価
  - 1.22緊急時対応体制評価
  - 1.23外部委託管理評価
  - 1.24クラウドセキュリティ運用評価
  - 1.25BCP対策評価
  - 1.26SNS利用体制評価
  - 1.27セキュリティ教育評価

監査要件確認 P.3参照

リスク認識確認 P.4参照

マネジメント監査としては、従来よりシステム監査や情報セキュリティ監査が実施されていますが、昨今のサイバセキュリティ・リスク環境を鑑み、サイバーセキュリティに特化した監査も行われています。

本サイバーセキュリティ監査では、それぞれの組織のサイバーセキュリティ発生構造や対策実施状況に合わせて、自律的にかつ継続的に、サイバーセキュリティ対策が有効に実施されることを支援します。すなわち、PDCA管理による対策の改善が継続して実施されている状態を目指します。

サイバーセキュリティ監査を効率的・効果的に実施し、実効を上げるためには、セイバーセキュリティ・リスクアセスメントを的確に実施することが前提になります。セイバーセキュリティ・リスクは組織のシステム利活用方法、システム運用環境、セキュリティ対策状況、に合わせて実施することになります。

サイバーセキュリティ監査は、第三者による助言型で行われます。リスクアセスメントの下に、サイバーセキュリティ対応態勢、リスク対策、等も考慮に入れて、段階的に改善することを目指します。

また、重要性・緊急性・リスク強度から、監査テーマを適宜設定してタイムリーに実施することも有効と言えます。

付1.1　サイバーセキュリティ・マネジメント監査要件の確認

❶マネジメント監査目的 と位置づけの確認

・ビジネスリスク認識
・監査・診断・コンサルの目的適合性と効率性・経済性

サイバーセキュリティ・マネジメント監査目的等
・目的の確認
□情報資産ライサイクル視点の完全性、機密性、可用性確保
□対策の有効性と残存リスク評価
□特定テーマに係わる運用状況
□サイバーセキュリティリスク管理状況
□情報資産価値評価
□情報環境資産の脆弱性評価
□脆弱性に対する脅威の評価
□リスクの影響度・発生可能性評価
□リスク対策の有効性評価
□残存リスク評価
□委託管理‥選定基準・定期評価基準
□個人情報保護等安全管理措置
□特定個人情報安全管理措置
□クラウド運用の脆弱性診断
□Webアプリの脆弱性診断
□プラットフォームの脆弱性診断
・位置づけ
□内部監査の一環として監査
□内部統制の〃
□コンプライアンス監査の〃

❷マネジメント 監査対象の確認

□対象システムの要件確認
　システム機能要件／非機能要件
　システムの稼働環境
　システムの運用環境
□システムの対象フェーズ確認
　企画・設計
　開発・テスト・導入
　運用・保守
　ユーザ利活用

❸マネジメント監査手続 と手順の確認

・監査体制と被監査部門の負荷‥期間・工数
・費用対効果

❸-1マネジメント監査手続

目的設定
　□内部目的‥助言型
　□外部目的‥保証型
監査基準
　□システム監査/管理基準
　□情報セキュリティ〃
　□法制度実施ガイドライン
　□監督官庁ガイドライン
　□PCI DSS
監査方法
　□面談‥チェックリスト
　□アンケート、自己診断
　□運用記録閲覧、文書レビュー
　□記録のサンプリング評価
　□脆弱性侵入テスト
　□各種HP自己診断‥IPA推奨基準
監査結果評価
　□検出事項
　□指摘事項
　□改善助言

❸-2マネジメント監査手順

1.経営計画による位置づけ確認
　中期経営計画　/年度経営計画
　情報化中期計画　/年度計画反映

　中期セキュリティ監査計画
　基本セキュリティ監査計画
　個別セキュリティ監査計画

2.監査実施計画の策定
　監査テーマと対象範囲
　監査スケジュール
　監査手順の明確化

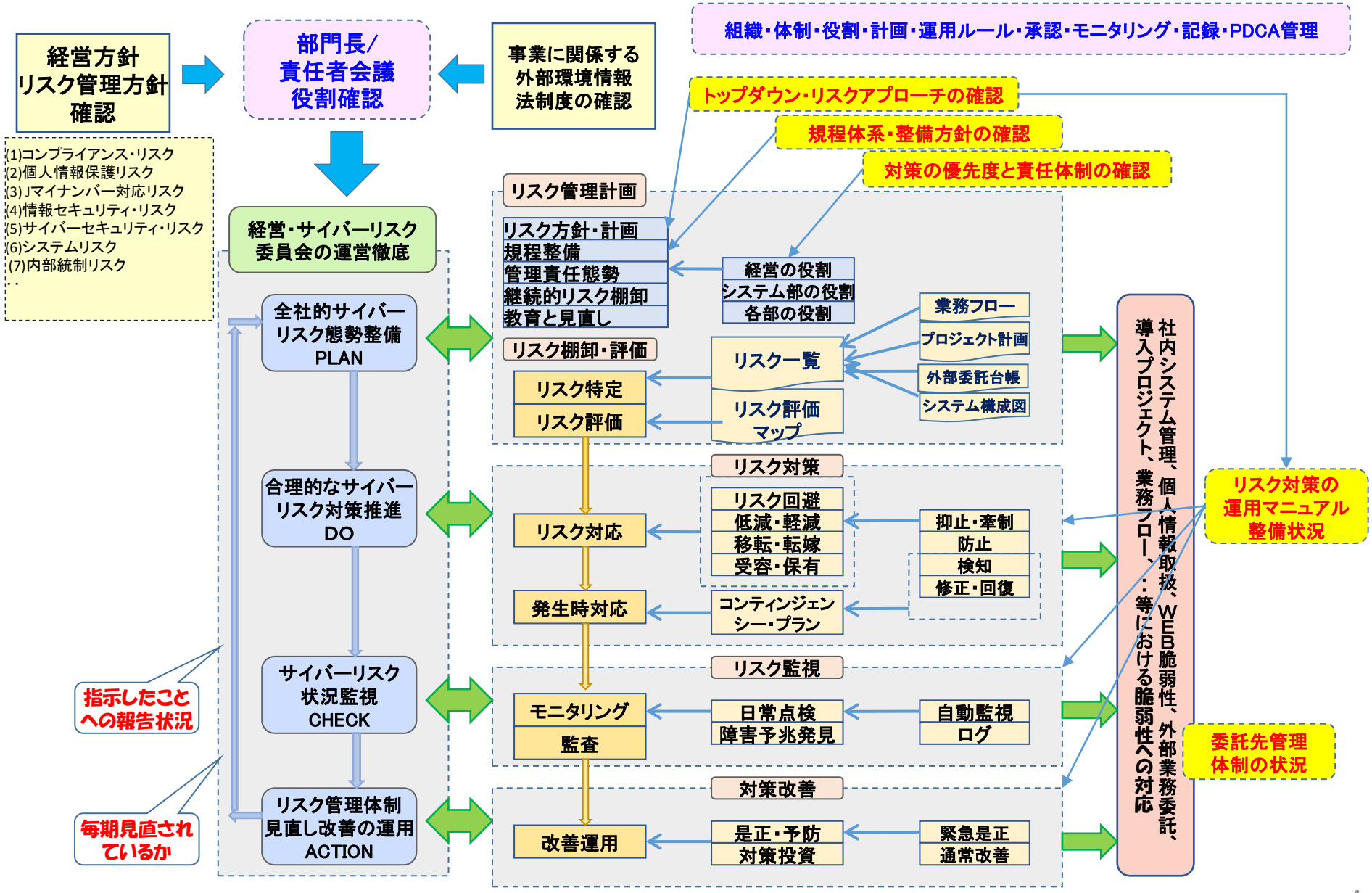
3.予備調査
　システム運用概況把握
4.本調査

5.分析・評価・結論
6.監査結果の報告
7.フォローアップの実施

❹ マネジメント監査の有効性確保の前提

監査実施の前提等
　□守秘契約締結
　□監査効率化のための協力体制
　　・監査責任者および監査窓口と業務分担の決定
　　・被監査部門責任者および担当者への周知
　　・他の監査・検査との連携および調整
　□被監査部門の協力依頼
　　・ヒアリング時間の確保、アンケート提出依頼
　　‥監査証跡提供依頼
　　　承認記録、議事録、運用記録等の閲覧

付1.2　サイバーセキュリティ・リスク管理態勢の評価



付1.3　サイバーセキュリティ・リスク認識確認例