ISO/IEC 27001（ISMS）
構築支援

ヒアリング診断用

20XX年X月
NPO東京ITC

ＩＳＭＳの構築についてのヒアリング

- ISMS構築の準備（現状確認）
- ISMS構築の準備（社内業務の仕組み調査）
- ISMS構築の基本的な考え方
- ISMS構築のための組織と役割
- ISMS構築のスケジュール
- ISMS構築の手順

ＩＳＭＳ構築の準備（現状確認）

1.経営トップによるISMS構築の宣言

2.構築プロジェクトの目標設定

適用範囲概略、期間、運営方針、責任と権限、成果物

3.構築プロジェクトの編成

4.業種、企業規模、拠点配置の現状把握とセキュリティニーズ

業界ガイドライン調査

5.ITの活用状況、情報システム・インフラの運用状況の現状把握

6.情報セキュリティ対策の現状把握

7.予算措置の検討、審査機関の検討

ＩＳＭＳ構築の準備（社内業務の仕組み調査）

1. □社内組織図と社内委員会制度の概要
2. □業務分掌、職務規定、権限規定、稟議規定、意思決定プロセス

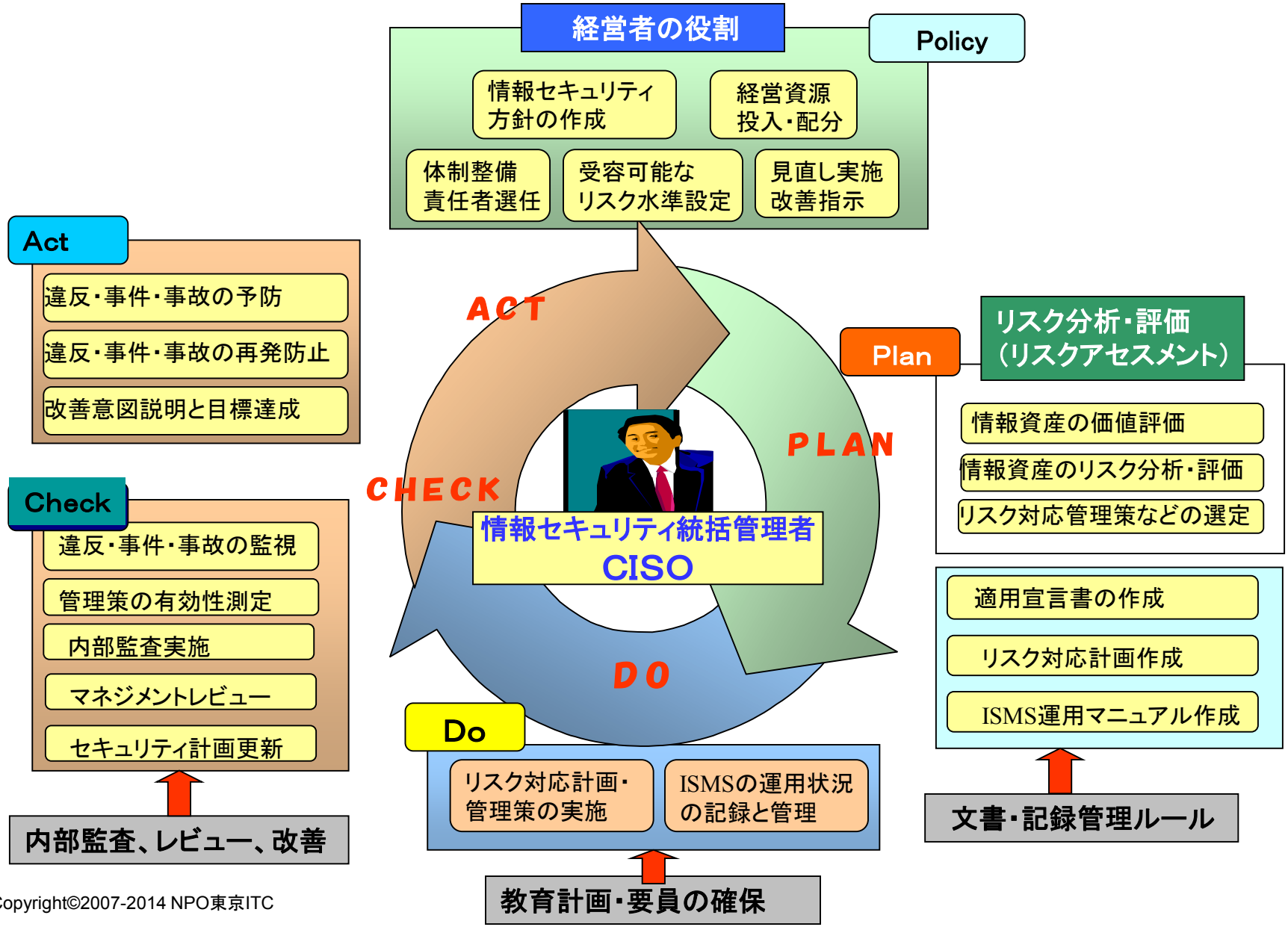
3. □業務記述書、業務マニュアル、業務フロー図
4. □就業規則、誓約書、入退出管理規則

5. □委託先契約書、守秘契約書、覚書、委託先選定基準
6. □委託元との契約書、守秘契約書、覚書

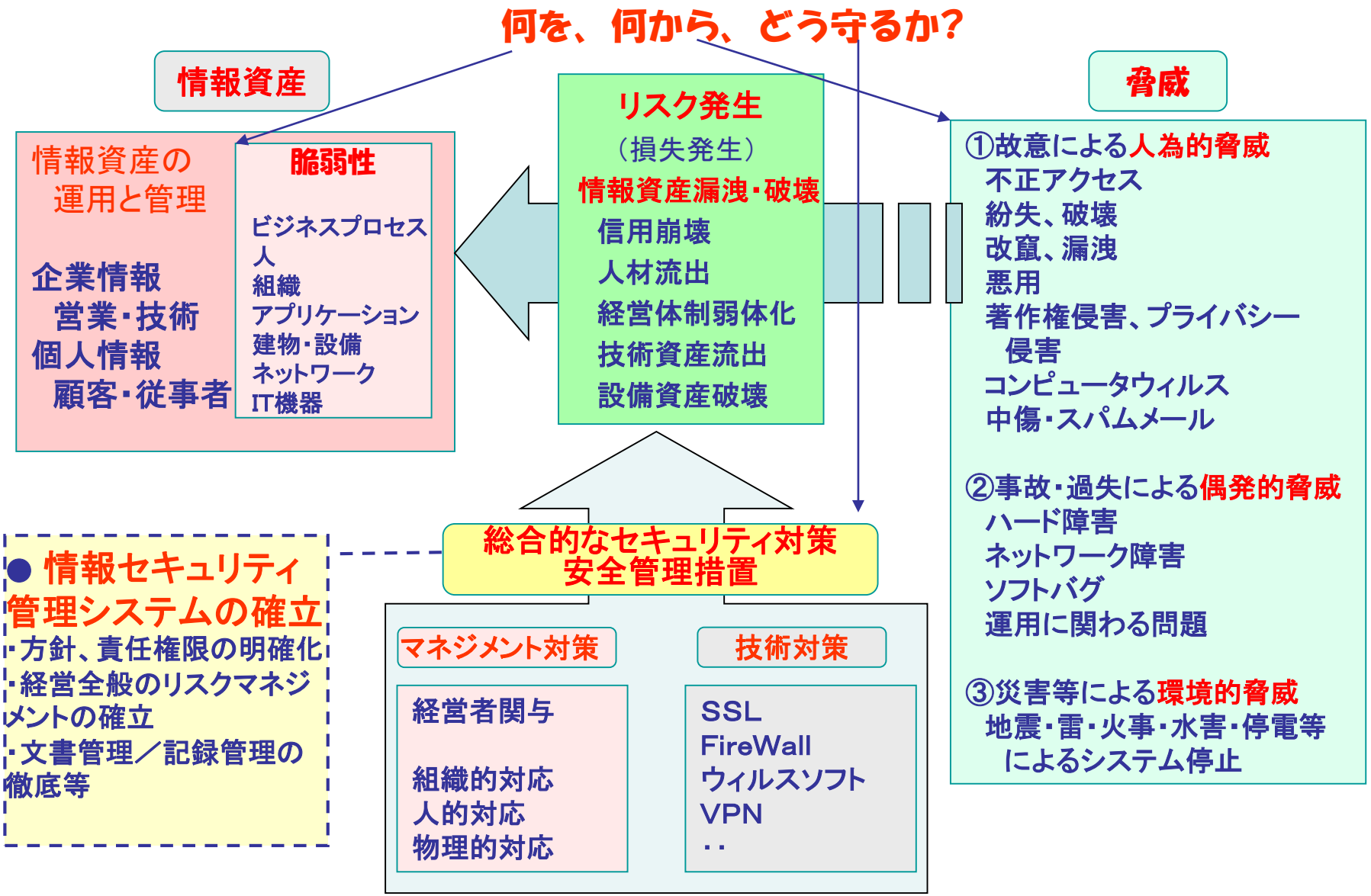
7. □IT戦略・IT方針・IT計画、情報セキュリティポリシー（別途）
8. □IT部門規定、IT開発規定・IT利用規定・IT運用規定
9. □全社システム体系図、ネットワーク図、導入システム・機器・ソフト台帳

10. □ユーザマニュアル、操作マニュアル
11. □システム概要説明書、システム仕様書、プログラム仕様書、運用マニュアル
12. □システム運用記録、各種申請書、伺い承認記録帳票
13. □システム各種変更記録（申請、承認）
14. □その他システム関係書類(業務委託契約書、SLA、仕様書等)

ＩＳＭＳが求めていること

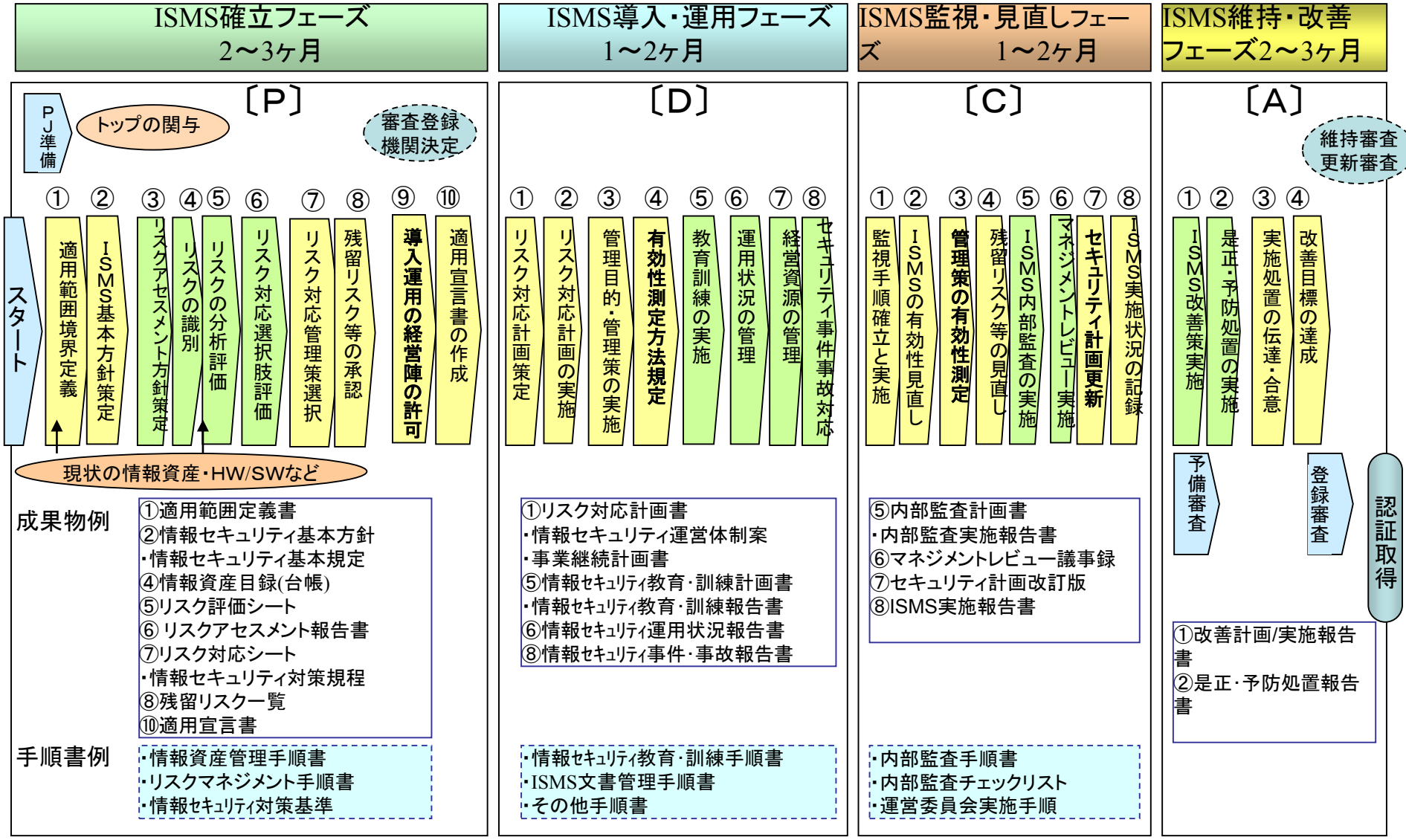


情報セキュリティ・リスクへの体系的対応

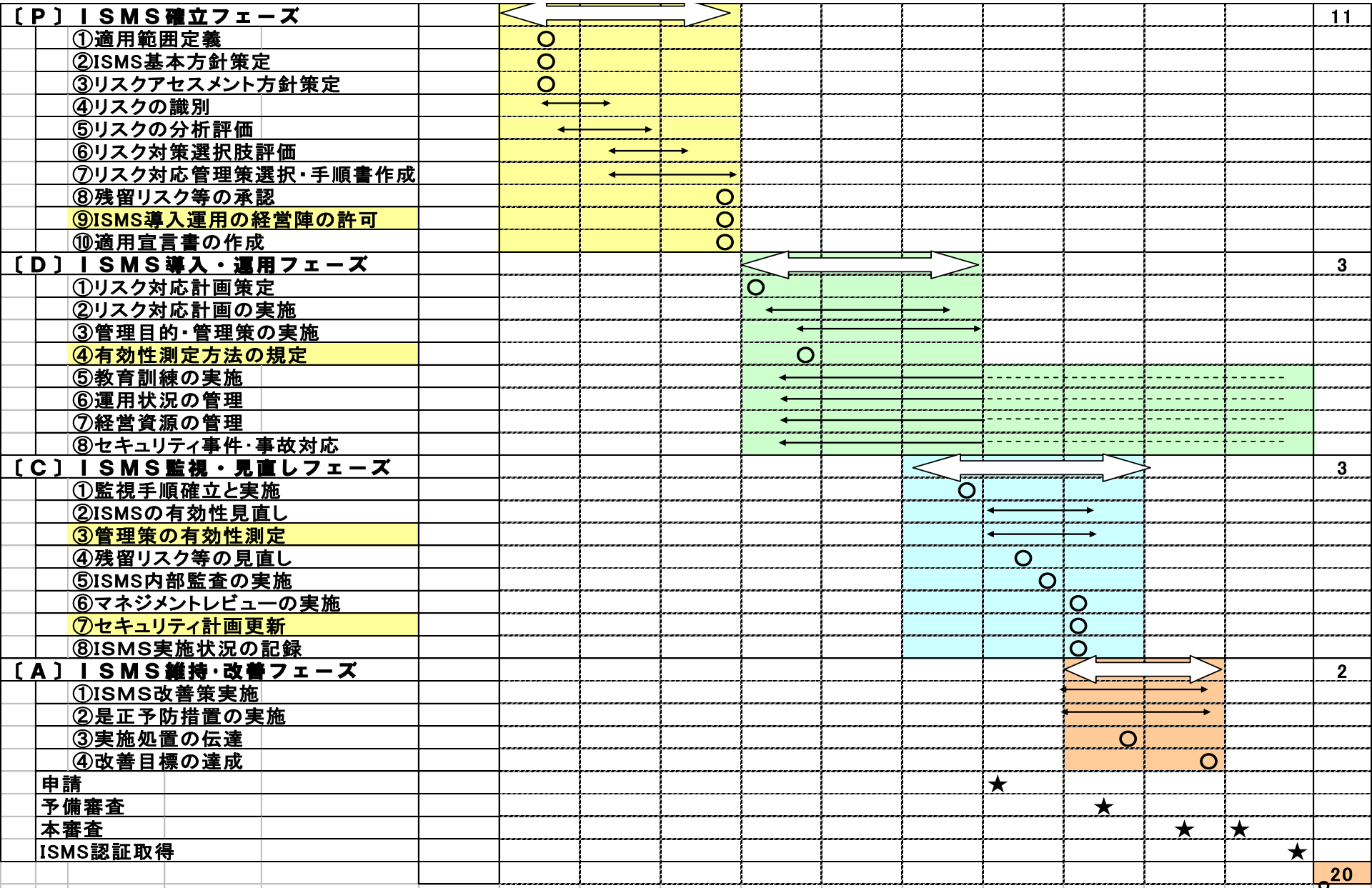


ＩＳＭＳの標準構築プロセス

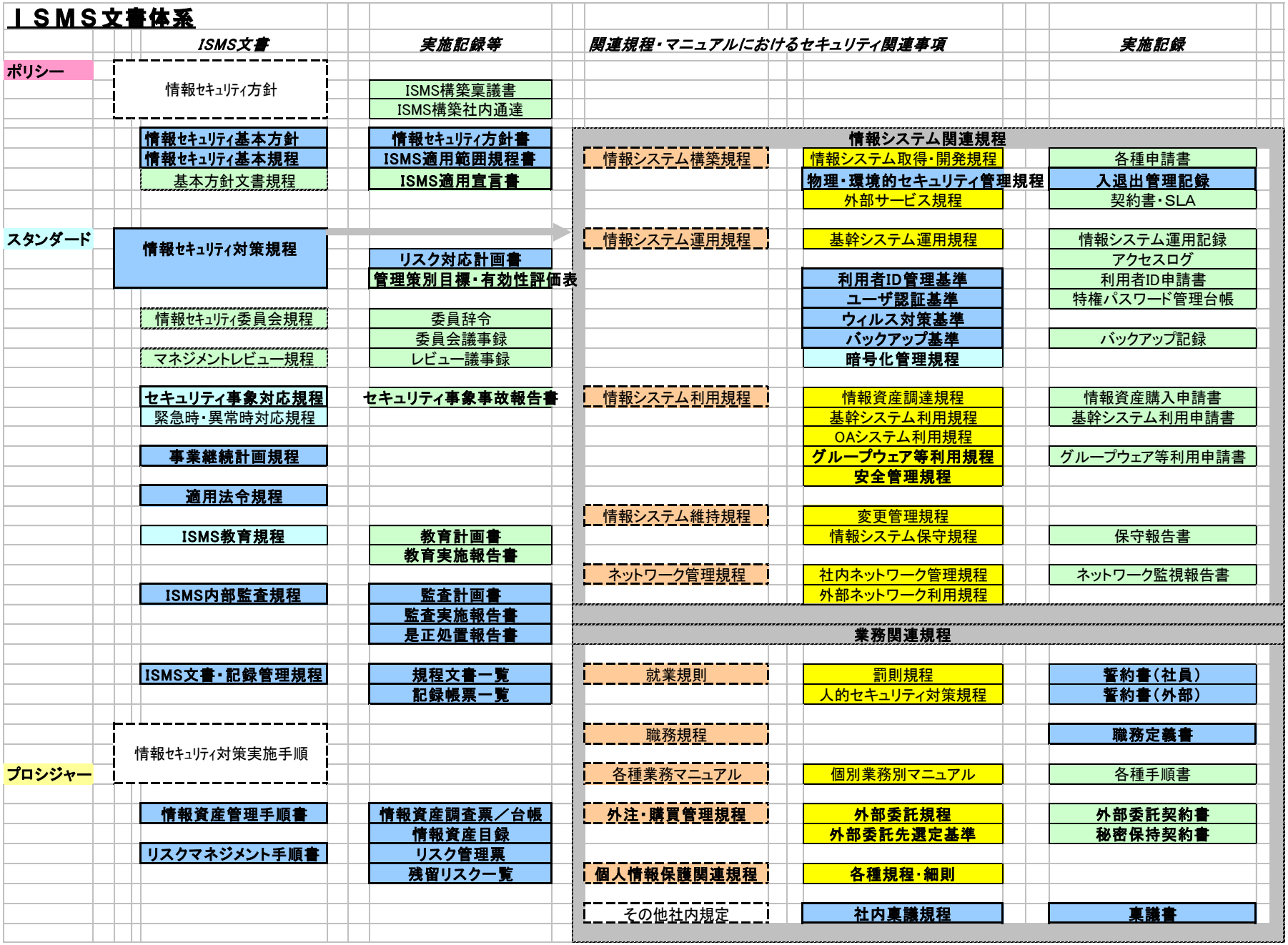
ISO27001ベース(改1)



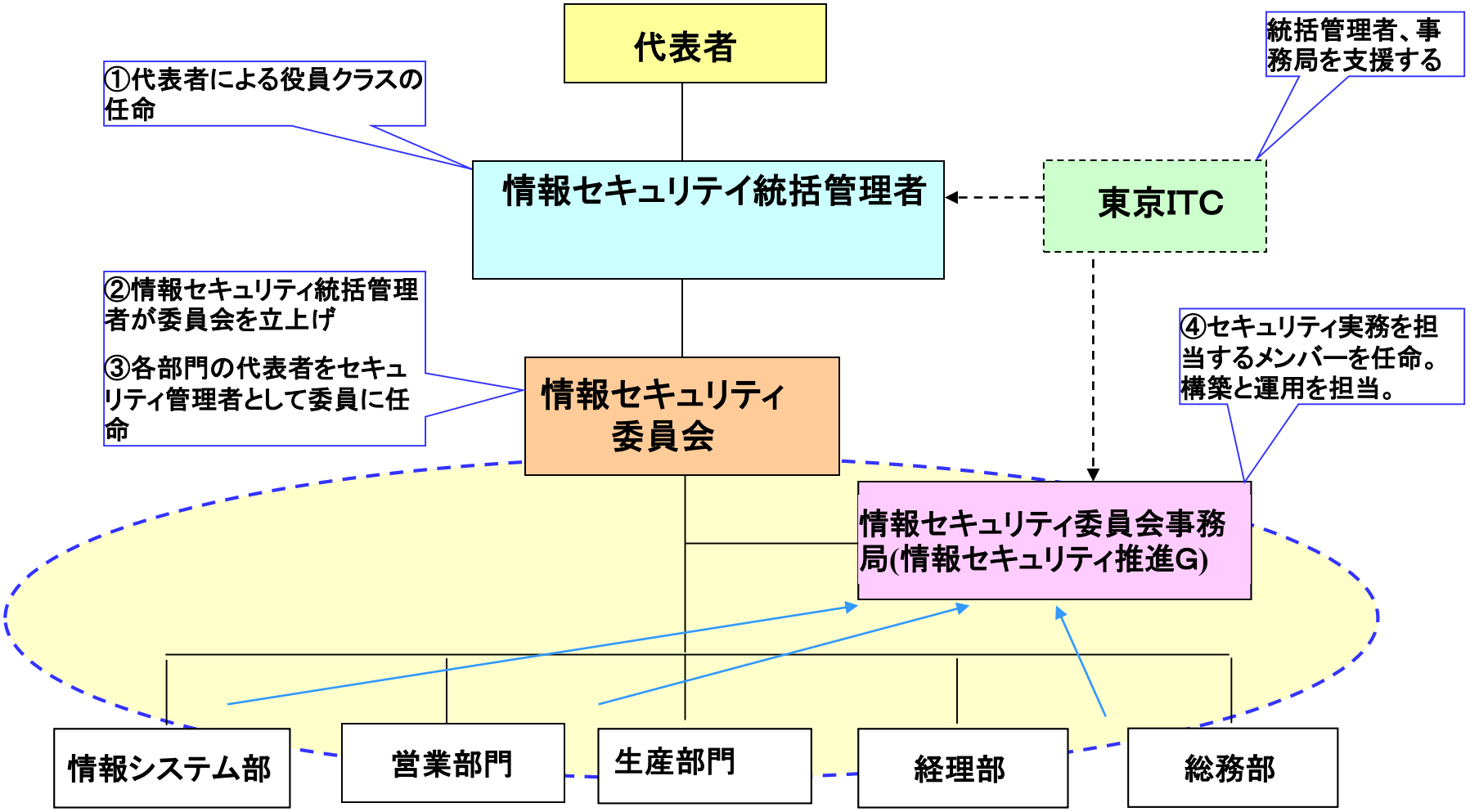
ＩＳＭＳ導入作業スケジュール例



ＩＳＭＳ文書体系



ＩＳＭＳ構築の推進体制（例）



付 ISMS認証基準ver.2からISO27001への変更ポイント

項目	ISO27001における要求事項	影響
適用宣言書の見直し 4.2.1.j)2)	「現在実施されている管理目的と管理策」を明らかにすること	・適用宣言書の選択管理策に実施状況を追記 ・未実施の理由と予定の追記
リスクマネジメントの見直し 4.2.1.c)2)	「リスクアセスメント」の方法は比較可能で再現可能であること	・リスクマネジメント手順の明文化 ・手順書の版管理 ・作業結果との紐付け
管理策の有効性評価 4.2.2.d 4.2.3.c 4.2.3.d)5) 4.3.1.g) 7.2.f) 7.3.e)	管理策を実施するだけでなく、「管理策の有効性の評価とその監視・測定」が加わった	・管理策の有効性についての 評価基準 評価方法 管理目標 監視・測定方法の設定運用 ・有効性評価を容易にする管理策のグルーピング

項目	ISO27001における要求事項	影響
セキュリティ事象の監視 4.2.3.a)4) A14.1.2	セキュリティ事故・事件の「予兆としてのセキュリティ事象」を検出し、予防すること	・予防措置体制の確立 セキュリティ事象の定義 当該事象の監視方法明確化 当該事象の判定基準値設定 当該事象の監視、記録
第三者が提供するサービスの管理手順見直し A10.2	外注委託先の管理の強化要請により、「アウトソーシング等のサービスレベル、監視、レビュー、変更管理の手順を明確化」すること	・提供サービスについて サービスのセキュリティ管理策 サービスの定義、SLA明確化 監視・監査 変更管理
全般	上記の変更に伴う整合性 追加記録体制の確立	・規定の見直し ・追加記録帳票の準備