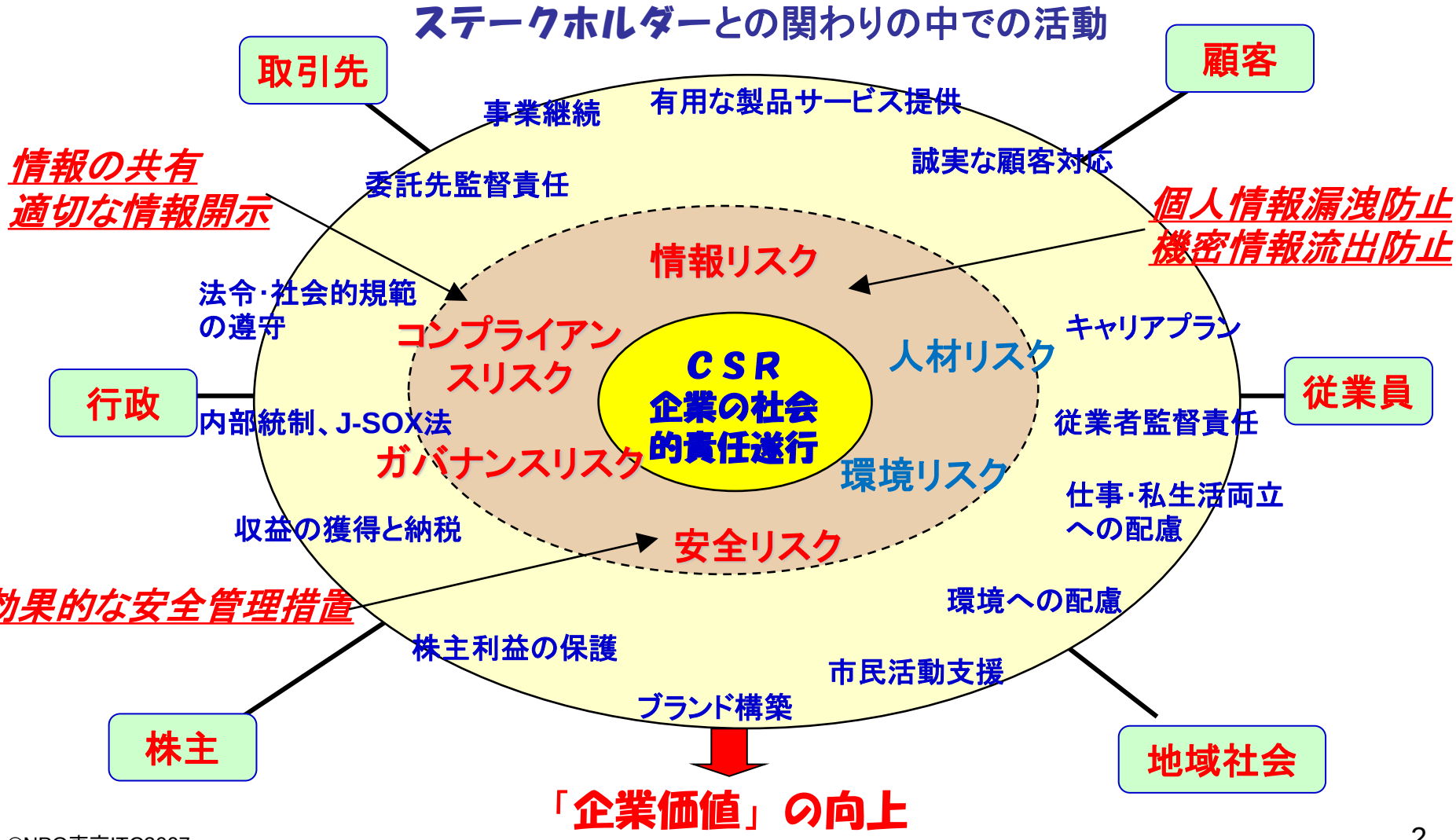
株式会社　○○　御中

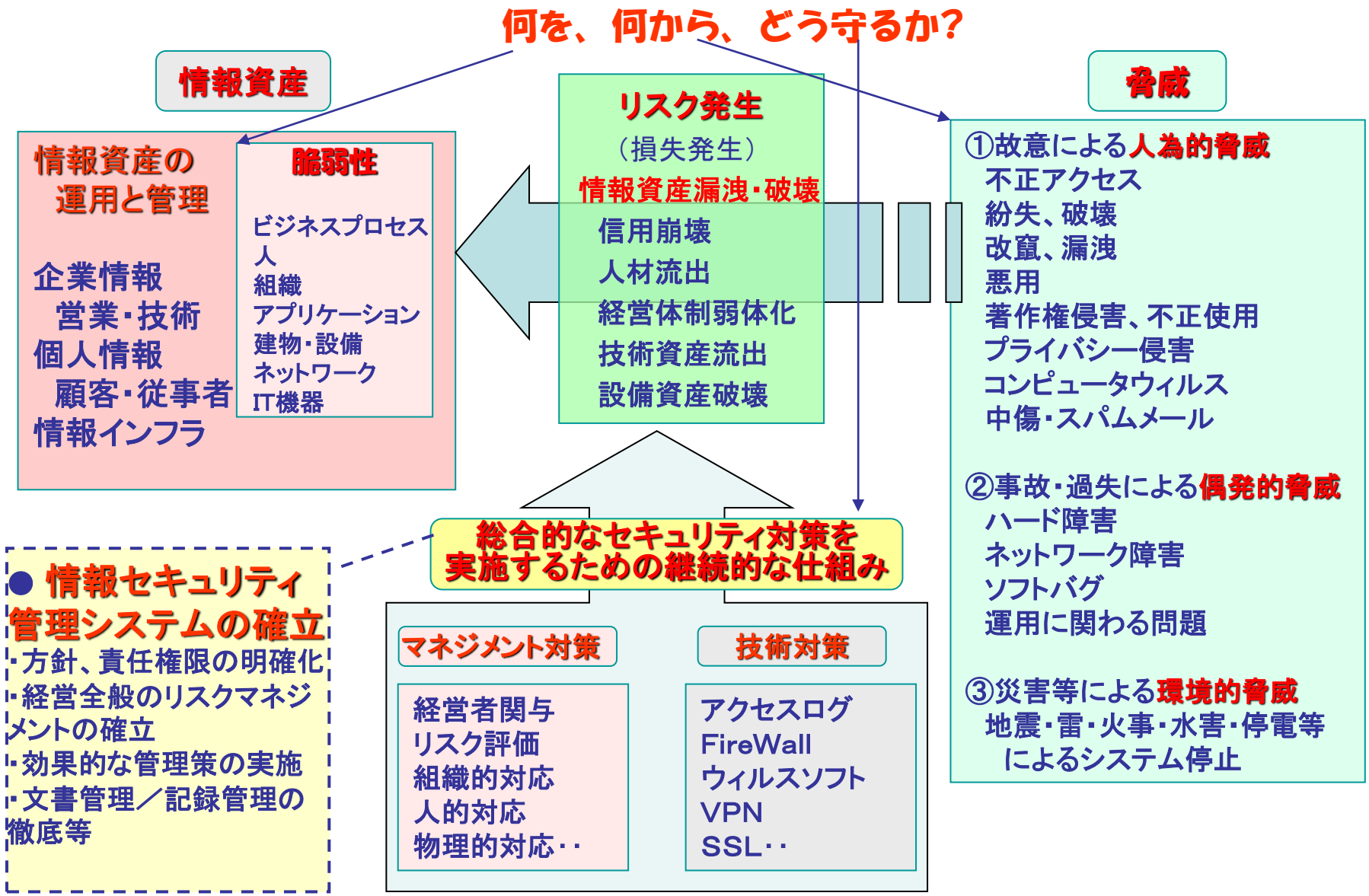
ISMS認証取得支援コンサルティング のご提案

特定非営利活動法人 東京ITコーディネータ

企業の社会的な責任の遂行とリスク対応
（ CSR:Coporate Social Responsibility ）



情報セキュリティ・リスクへの体系的対応



ISMSが求めていること

経営者の役割

Policy

- 情報セキュリティ方針の作成
- 経営資源投入・配分
- 体制整備 責任者選任
- 受容可能なリスク水準設定
- 見直し実施 改善指示

Act

- 違反・事件・事故の予防
- 違反・事件・事故の再発防止
- 改善意図説明と目標達成

情報セキュリティ統括管理者
CISO

Plan

リスク分析・評価（リスクアセスメント）

- 情報資産の価値評価
- 情報資産のリスク分析・評価
- リスク対応管理策などの選定

- 適用宣言書の作成
- リスク対応計画作成
- ISMS運用マニュアル作成

文書・記録管理ルール

Check

- 違反・事件・事故の監視
- 管理策の有効性測定
- 内部監査実施
- マネジメントレビュー
- セキュリティ計画更新

内部監査、レビュー等

Do

- リスク対応計画・管理策の実施
- ISMSの運用状況の記録と管理

教育計画・要員の確保

「プライバシーマーク制度」と「ISMS適合性評価制度」との関係

■情報処理サービス業システム安全対策事業所認定制度を引き継ぐ
■JISX5080情報セキュリティマネジメント実践のための規範の反映
□一般社団法人情報マネジメントシステム認定センターが運営

プライバシーマーク制度

■第三者による「個人情報保護措置」の認証制度
⇒JIS Q 15001適合性

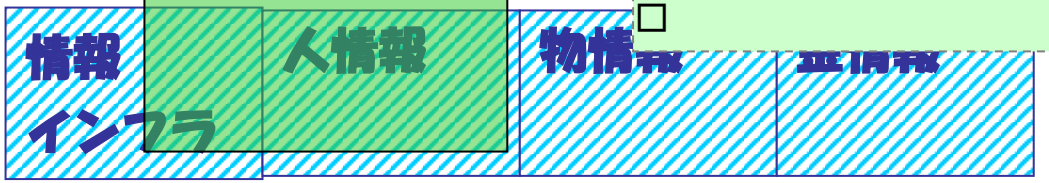
□財団法人日本情報処理開発協会（現、一般財団法人日本情報経済社会推進協会）が運用

■自主的に認定を受けた団体のみを拘束する規範でBtoCが多い

■コンプライアンスが中心で、セキュリティレベルは具体的には規程していない
□

プライバシーマーク

ISMS



情報セキュリティマネジメントシステム

ISMS
旧日本情報処理開発協会

■第三者による情報セキュリティ・マネジメントシステムの認証制度
⇒「ISMS適合性評価制度」

■自主的に認定を受けた団体のみを拘束する規範で、BtoBが多い

■リスクマネジメントが主眼

その他の制度
□BS7799
□TRUSTe
□BBBOnline
□個人情報保護マーク（（財）日本データ通信協会 ）

「ISMS適合性評価制度」とは何か

1. ISMSの目的

ISMS適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントとしての第三者適合性評価制度であり、本制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものです。

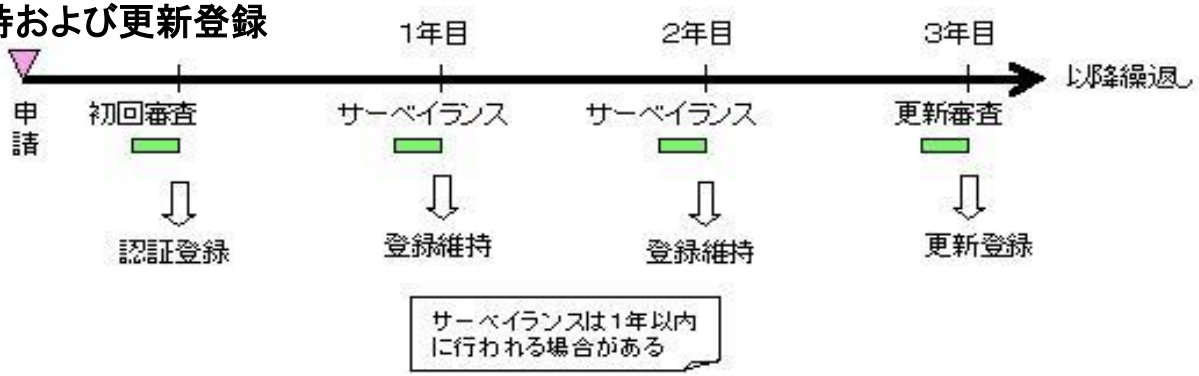
2. ISMSの認証基準

従来のISMSの認証基準（Ver. 2）は、英国規格BS 7799-2:2002に基づき作成したもので、本基準で使用する用語、表現については、JIS X 5080:2002（国際規格ISO/IEC 17799:2000）との互換性を確保していました。2005年のISO/IEC27001の発行に伴い、これに対応して国内規格のJIS Q 27001が発行され、ISMS認証基準（Ver. 2）は、2006年5月20日より「JIS Q 27001:2006」へ移行しました。

3. ISMSの適用範囲

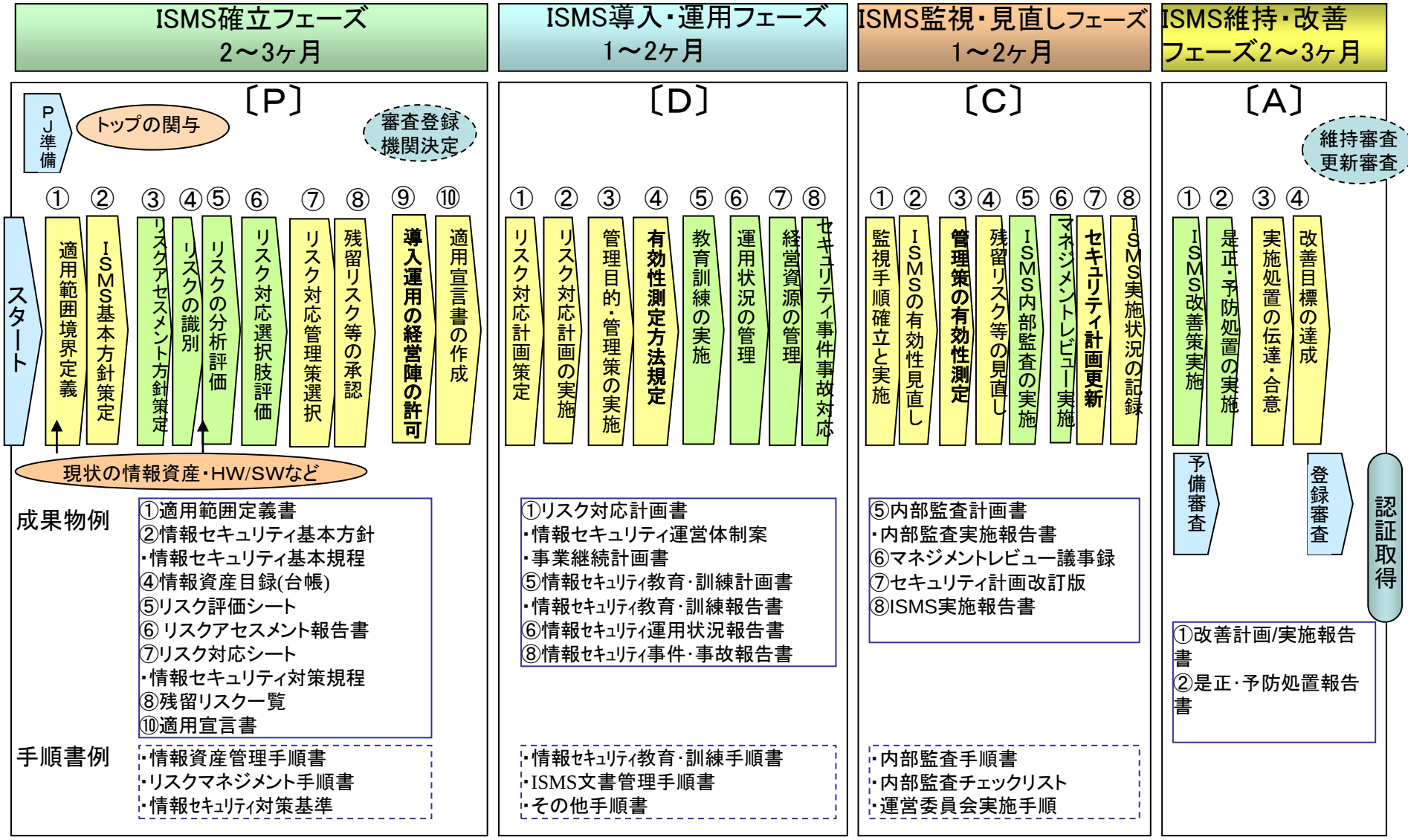
ISMSの適用範囲は、企業情報を大量にマネジメントする企業内の部署を限定して導入を図ることが可能です。このため、ISMSはPマークに比べ大企業や事業所の多い企業に向いています。

4. 登録と維持および更新登録

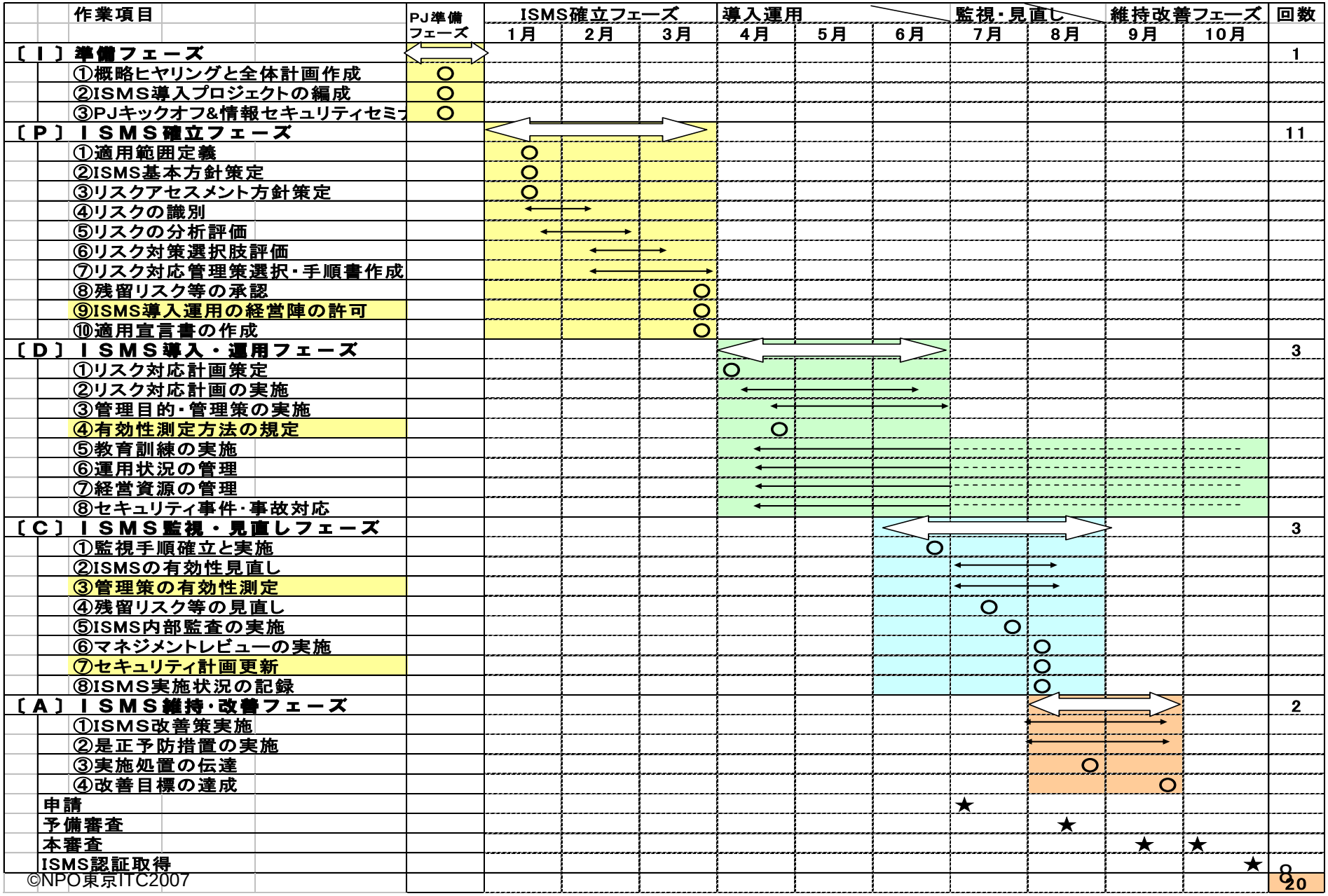


ISMSの標準構築プロセス

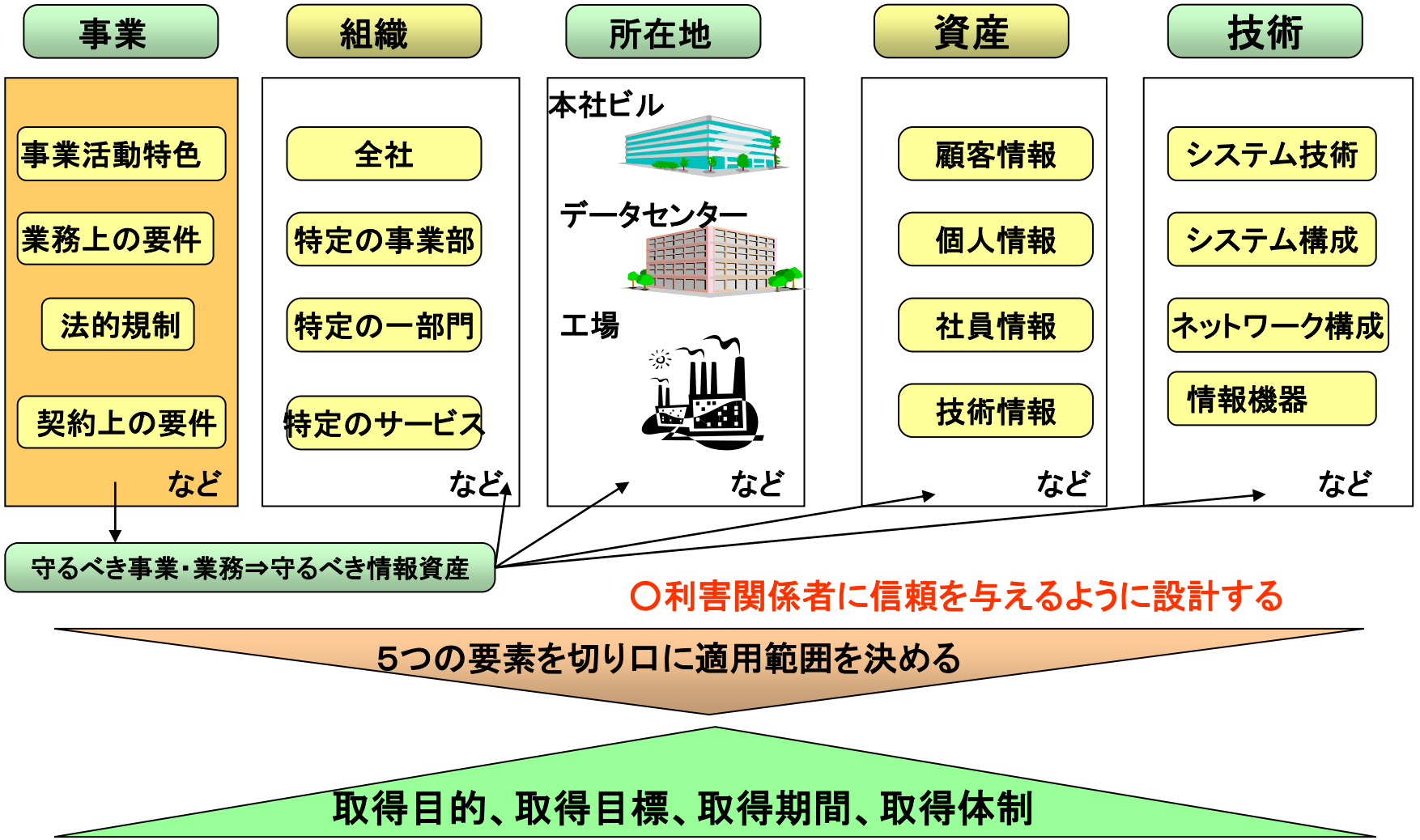
ISO27001ベース(改1)



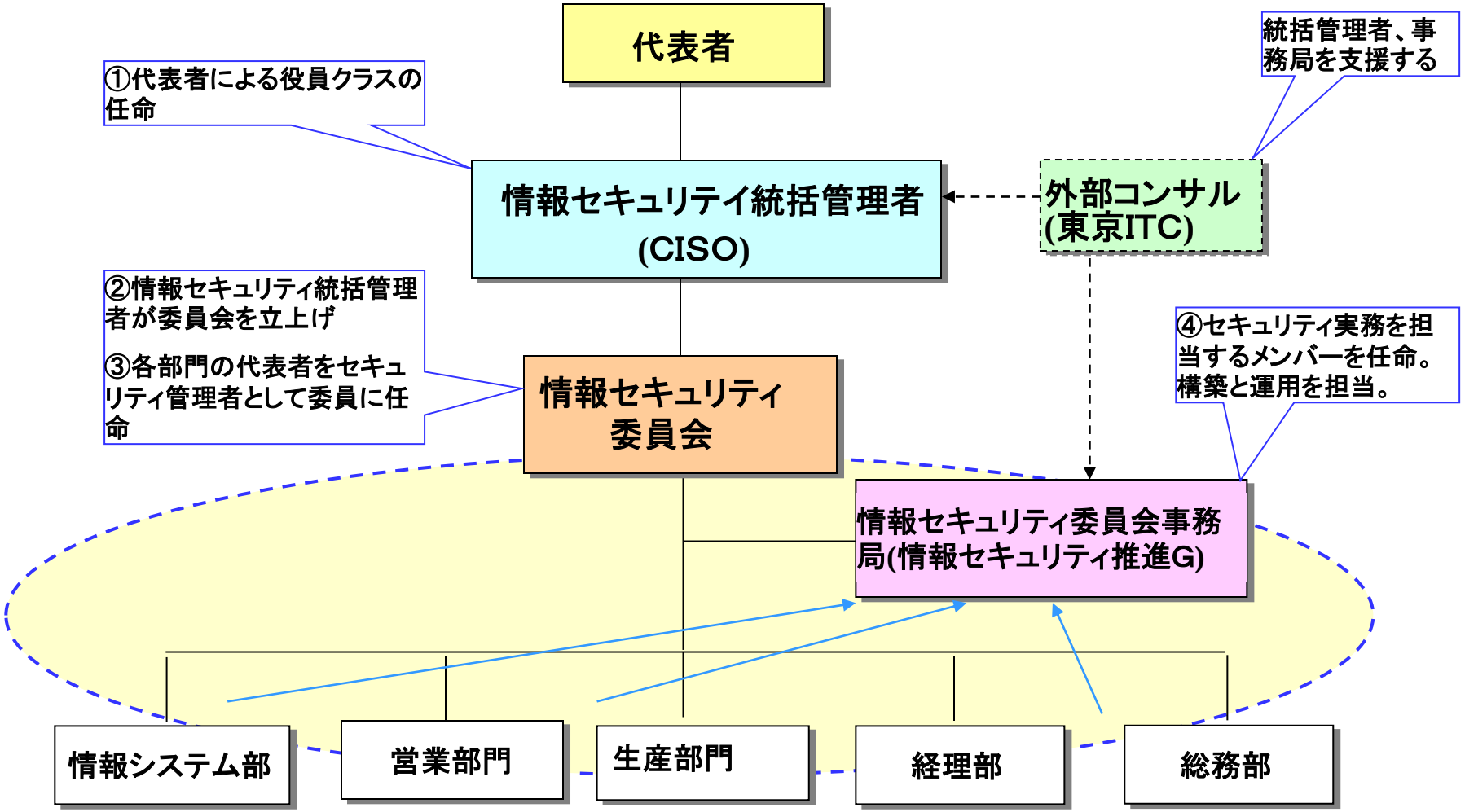
作業スケジュール例



適用範囲の決定の考え方

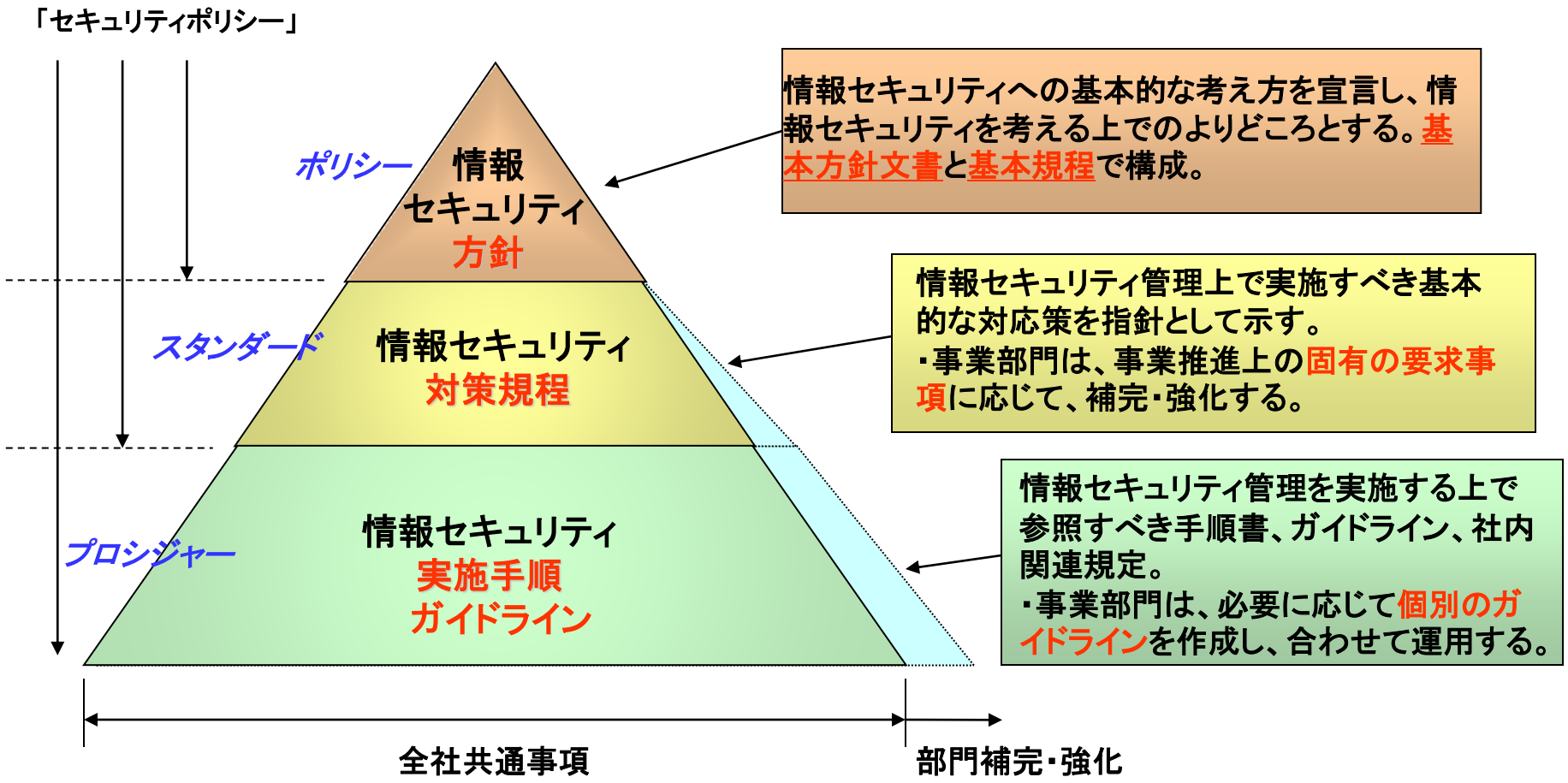


情報セキュリティ管理システム構築の推進体制（例）



情報セキュリティ文書体系

・「情報セキュリティ」とは情報の機密性、完全性、可用性を保つことであり、このセキュリティに対する考え方(ポリシー)を明文化し、全社員で共有する



情報セキュリティへの基本的な考え方を宣言し、情報セキュリティを考える上でのよりどころとする。基本方針文書と基本規程で構成。

情報セキュリティ管理上で実施すべき基本的な対応策を指針として示す。
・事業部門は、事業推進上の固有の要求事項に応じて、補完・強化する。

情報セキュリティ管理を実施する上で参照すべき手順書、ガイドライン、社内関連規定。
・事業部門は、必要に応じて個別のガイドラインを作成し、合わせて運用する。

ＩＳＭＳ文書体系

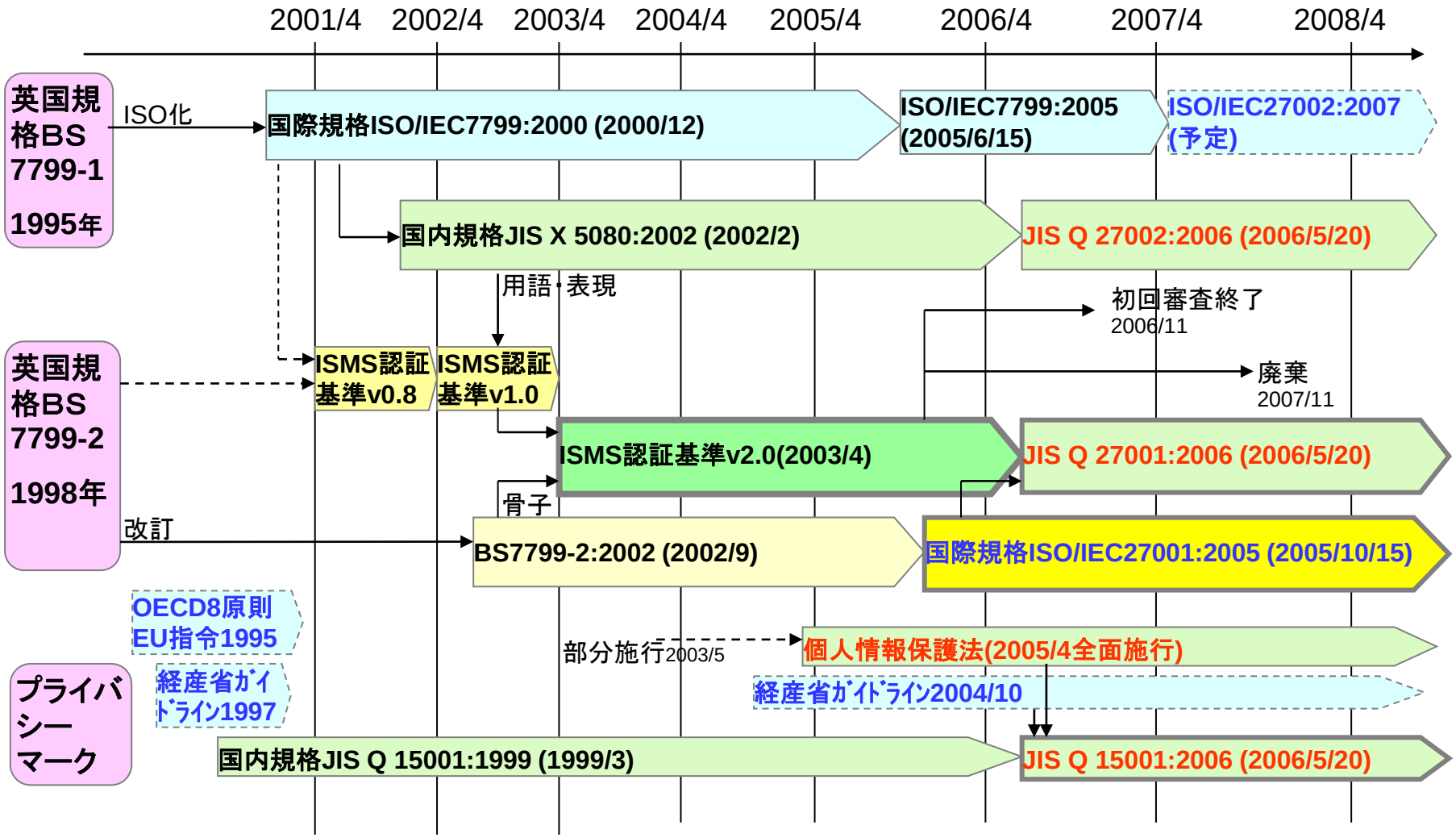
ＰマークとＩＳＭＳとの比較（１）

	プライバシーマーク	ISMS
目的・狙い	・「個人情報」の取扱について適切に扱っている事業者を認定する。 ・個人の権利・利益を守る。	・企業の情報資産全般のセキュリティマネジメントシステムの確立と運用・維持できていることを認定する。 ・情報資産をリスクから守る。
適用対象	・自ら保有する「個人情報」 ⇒個人情報をある程度保有する業種・事業者向け ・認定申請に当たっては事業者単位の取り組みが前提となっている	・ソフト、ハードを含む「情報資産全般」 ⇒業種に関係なく適用 ・組織の必要性に合わせて、部門・場所等の適用範囲を合理的に決定して申請できる
審査適用規格	JIS Q 15001　個人情報保護マネジメントシステム－要求事項	ISO/IEC27001：2005 ／ JIS Q 27001
認証取得状況	・1998年スタート ・2020.4現在・・16,459事業者	・2002年スタート ・2020.4現在・・6130事業者
認証取得方法	・事業者単位(全社単位)に取得	・適用範囲を限定し逐次範囲拡大可能
維持更新	・2年に1回更新	・毎年サーベランスがある ・3年に1回更新

ＰマークとＩＳＭＳとの比較（２）

	プライバシーマーク	ISMS
申請費用	申請費用は中規模企業の場合600千円、更新料は450千円（2年毎）	従業員数、拠点数、機関によるので見積り要例：1拠点10名で申請時1290千円、毎年263千円。3拠点60名で申請時1720千円、毎年437千円、更新時787千円（3年毎）。
管理の対象範囲	・個人情報保護は、個人情報の安全管理策を実施するだけでなく、個人情報の本人の権利に対応することも含まれる。 ・情報取得時には事前に利用目的等を伝えた上で本人の同意をとることが必要であり、取得後も本人からの修正・削除などの要望に応じる必要がある。	・基本的に、組織の事業活動全般及びリスク全般を考慮し、事業上の要求事項、法的又は規制要求事項に対するリスクアセスメントによりセキュリティ対策（管理策）を実施する。
マネジメントシステム構築	・個人情報の安全管理策を構築することに加えて、情報主体の権利に対する要求への管理策が必要となる。また、個人が対象となるために、苦情処理窓口を準備して対応するなど消費者保護の側面を考慮する必要がある。	・組織の事業継続や、運用コストも配慮した総合的な観点でセキュリティ対策の取組みがされているかが重要なポイントとなる。
特色	・日本固有の制度 ・個人情報が多い企業で有効 ・管理策を決定する手順は明確でない ・B2Cビジネスに有効	・ISOに準拠したグローバルスタンダード ・情報の安全を守る管理策を決定する手順が明確 ・主としてB2Bビジネスに有効

情報セキュリティの規格変革期



NPO法人「東京ITC」が提案する取得支援作業