

プライバシーマーク認証取得 についてのご提案

～ JISをベースにした個人情報保護体制の構築 ～

特定非営利活動法人 東京ITコーディネータ

個人情報セキュリティ・リスクの構造

何を、何から、どう守るか？

個人情報

- ・顧客情報
- ・取引先担当者/責任者のデータベース
- ・メールアドレス帳
- ・従業員・家族・関係者のデータベース
- ・採用・リクルート関係

- ・苦情・相談・問い合わせの個人情報
- ・アンケート回答

脆弱性

ビジネスプロセス
人
組織
アプリケーション
建物・設備
ネットワーク
IT機器

個人情報
事故事件

脅威

- ①故意による**意図的脅威**
不正アクセス
紛失、破壊
改竄、漏洩
悪用
著作権侵害、プライバシー侵害
コンピュータウイルス
中傷・スパムメール
- ②事故・過失による**偶発的脅威**
ハード障害
ネットワーク障害
ソフトバグ
運用に関わる問題
- ③災害等による**環境的脅威**
地震・雷・火事・水害・停電等によるシステム停止

総合的なセキュリティ対策 安全管理措置

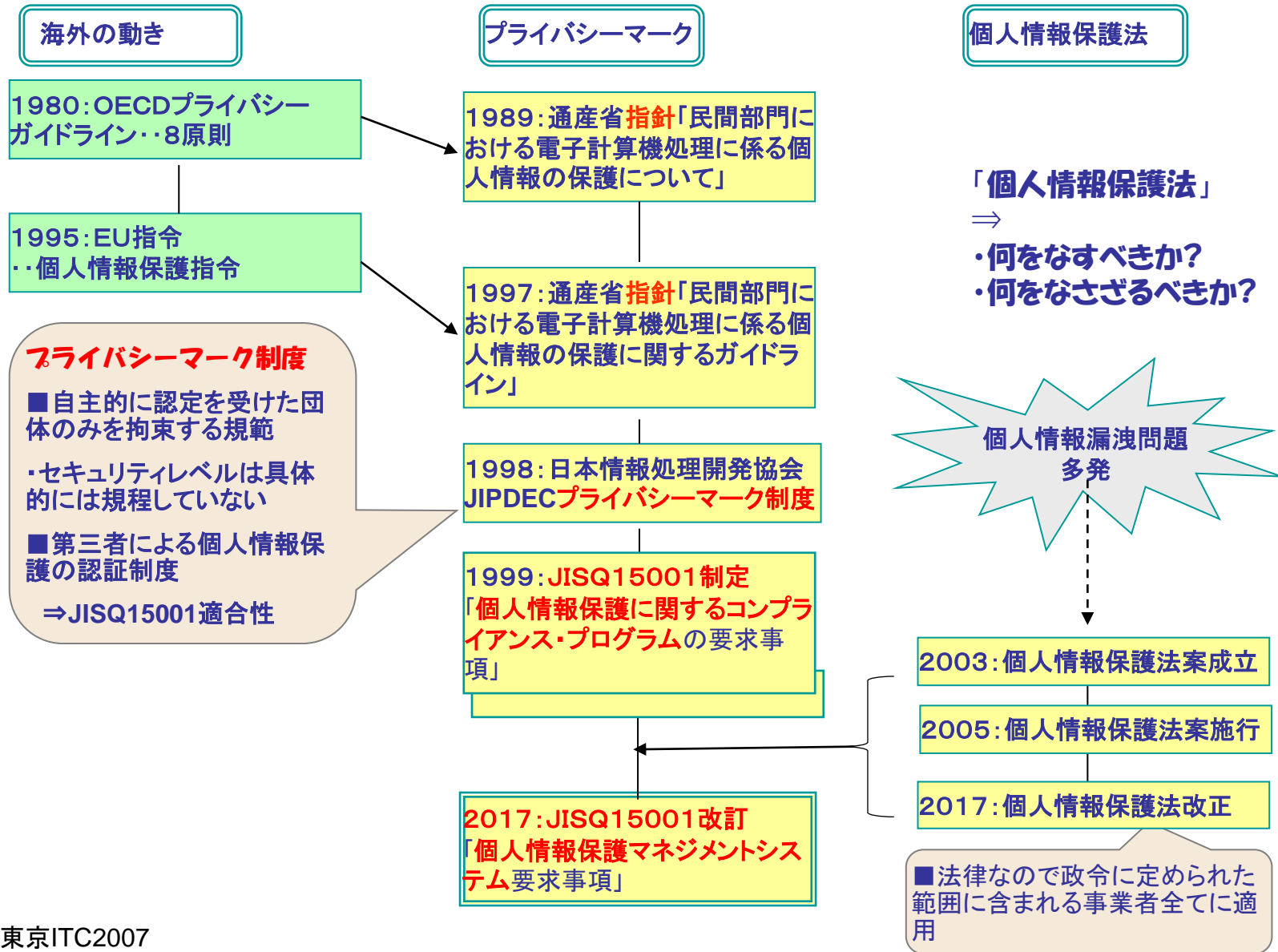
マネジメント対策

- 経営者関与
- 組織的対策
- 人的対策
- 物理的対策

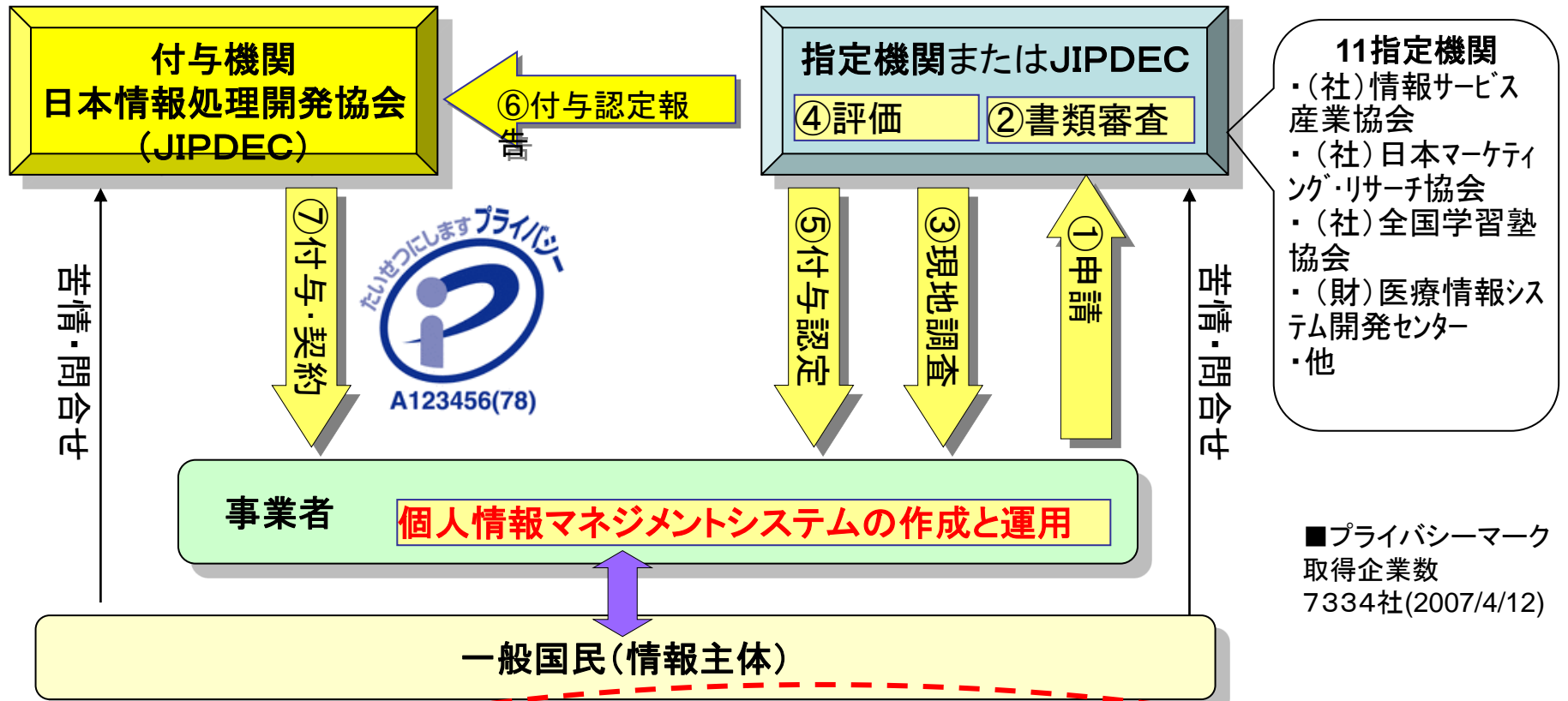
IT技術対策

FireWall
ウイルスチェック
アクセス・ログ
VPN
SSL・・

個人情報保護法とプライバシーマーク



プライバシーマーク制度の手続きの概要



認定費用	小規模企業	中規模企業	大規模企業
申請料	52,382	52,382	52,382
審査料	209,524	471,429	995,238
付与登録料	52,382	104,762	209,524
計	314,288	628,573	1,257,144

中規模	製造業等	卸売業	小売業	サービス業
資本金	3億円以下	1億円以下	5000万円以下	5000万円以下
従業員	300人以下	100人以下	50人以下	100人以下
小規模	20人以下		5人以下	

保有している個人情報の現状調査

貴社にどんな個人情報がありますか？

企業取引タイプによる個人情報の分類

文書、電子データ、写真、映像、音声

(BtoB) — 取引先情報 — (法人販売先、購入先情報のうち)
代表者情報、担当者情報、名刺

(BtoC) — 顧客情報
会員情報 — 顧客個人情報、家族情報、取引履歴
購買情報、資産情報、信用情報、
苦情情報、アンケート情報

(BtoE) — 従業員情報
役員、OB — 役職員個人情報、家族情報、家情調
書、人事査定情報、健康診断情報、
昇進試験情報、履歴書、経歴書

(その他) — 個人情報
関係者情報 — 社外委員情報、アンケート情報、問合
せ・相談情報、応募情報、その他

個人情報漏洩が起こりにくい仕組み作り

2004年6月に経済産業省が「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を公表。法を執行する場合の基準。

個人情報保護マネジメントシステム(PMS)の構築 (コンプライアンス・プログラム:CP)

安全管理措置の確立

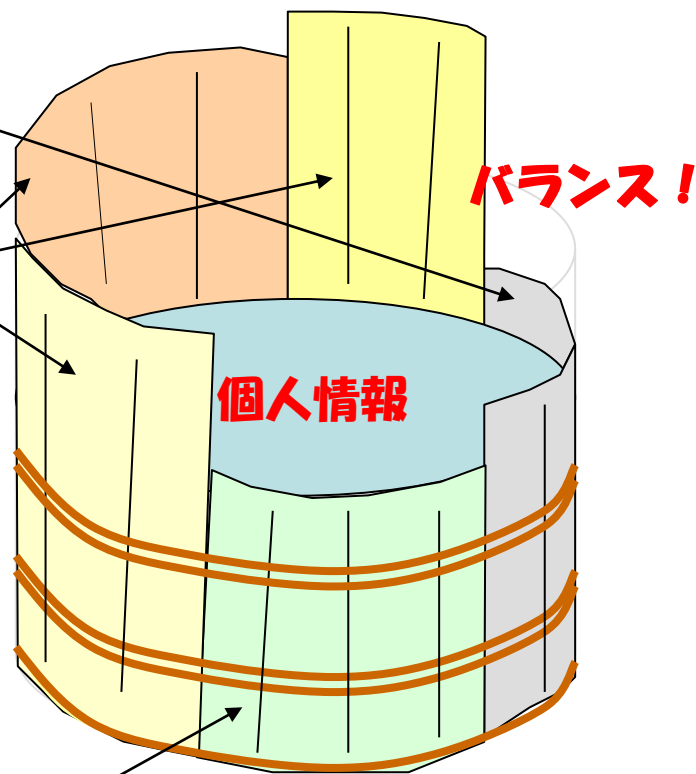
組織的 安全管理措置

人的 安全管理措置

物理的 安全管理措置

技術的 安全管理措置

- JISQ15001:2006
- 個人情報保護法
- 業界ガイドライン



経営トップのセキュリティポリシー

個人情報保護マネジメントシステム(PMS)とは

- ・「個人情報保護 措置」
- ・「個人情報保護 実践 順守計画」とも言う

PLAN

PMS体制の確立

- ・個人情報保護方針の作成
- ・個人情報の特定
- ・コンプライアンス・プログラム作成

組織体制

役割・権限・責任

方針・規程・細則

実施管理・監査

教育

ACT

常に最良のPMS状態の維持

- ・代表者による仕組の見直し

「個人情報保護マネジメントシステム」(PMS) は個人情報保護に関する実施体制、規程類、実施管理の仕組を含むマネジメントシステムを構築すること

DO

PMSの適切な運用

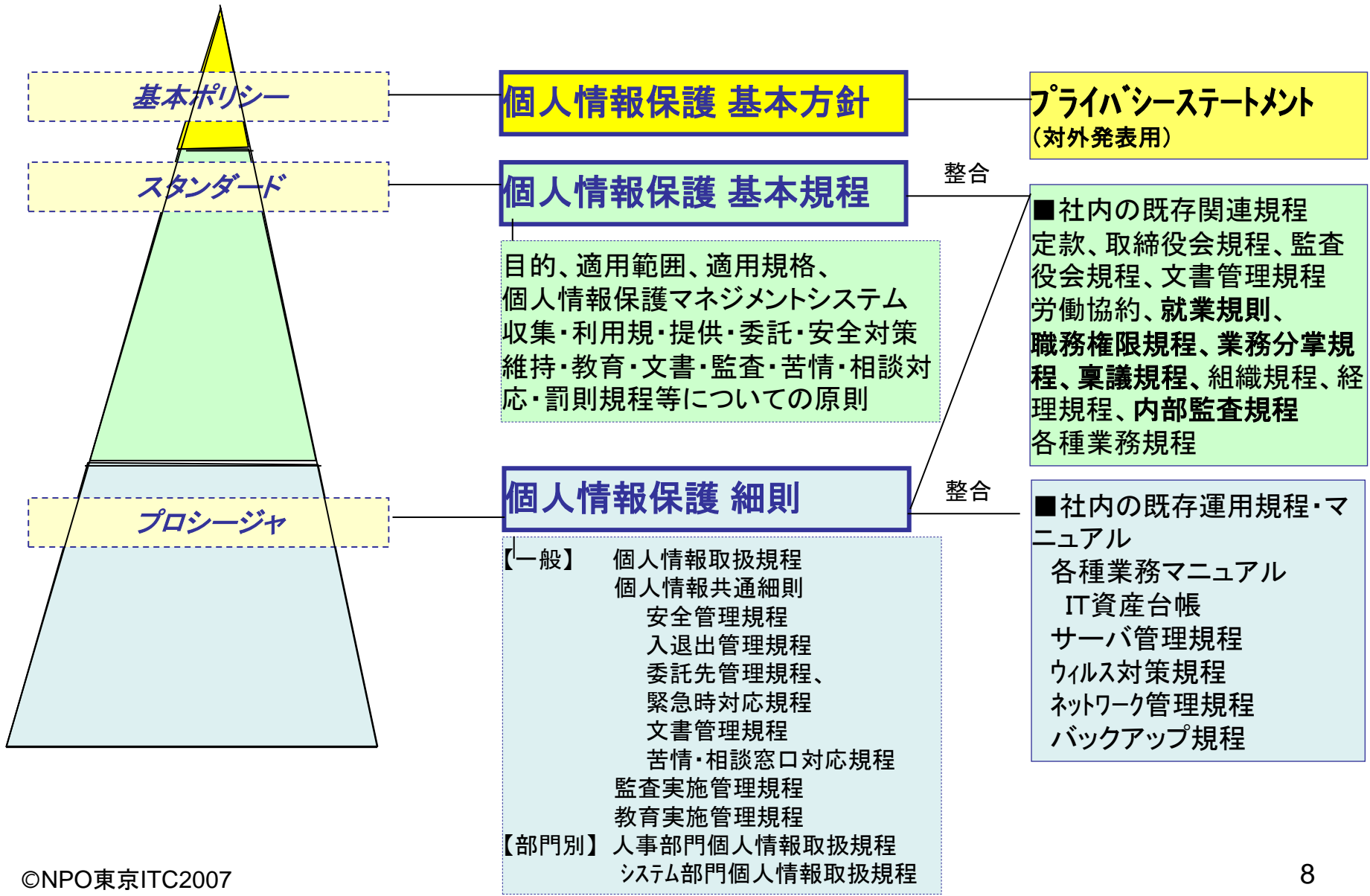
- ・適切な個人情報の収集・利用・提供
- ・適切な管理、権利の保護
- ・社員教育、苦情対応、文書管理

CHECK

PMSの定期的な確認

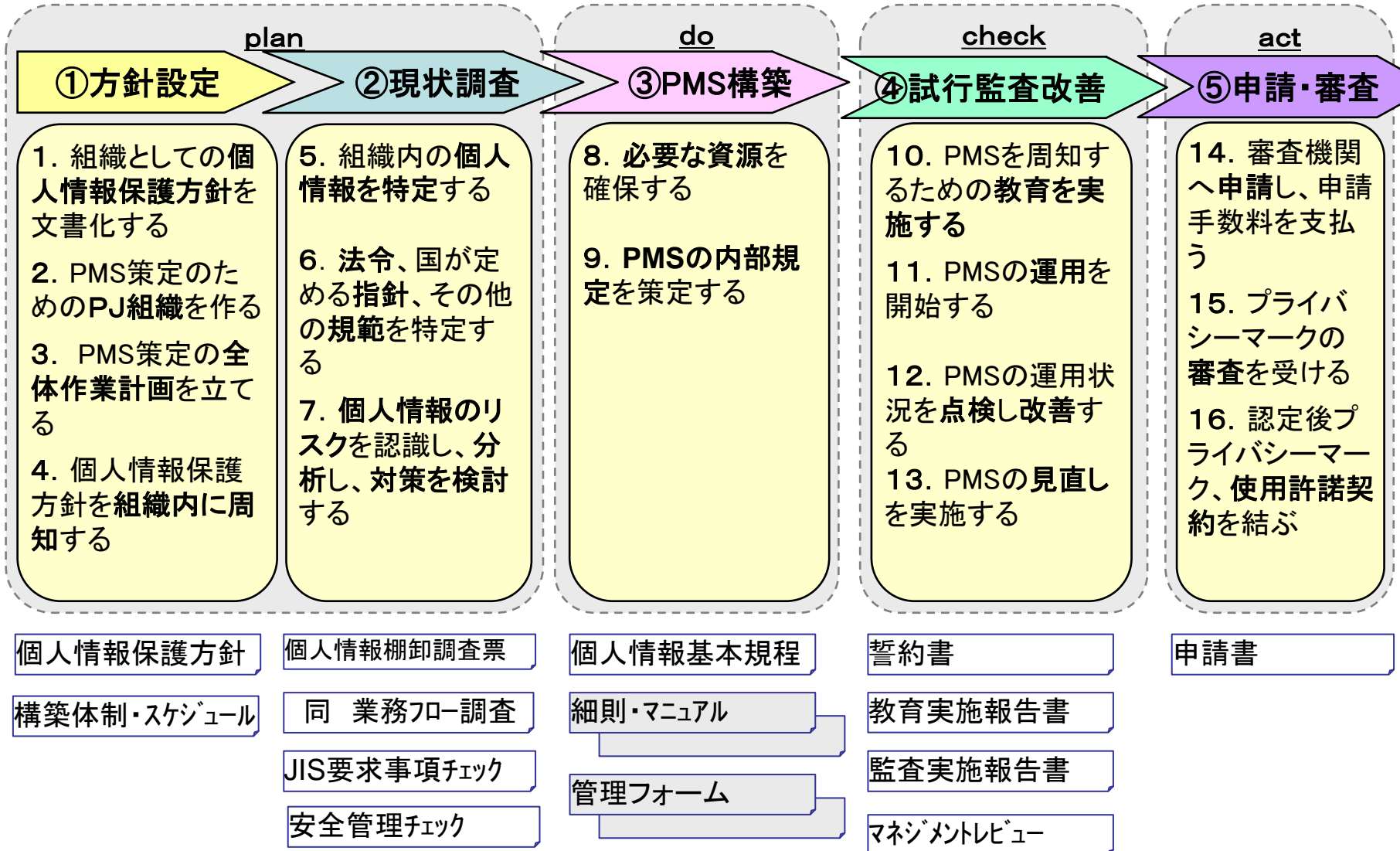
- ・内部監査の実施
- ・監査報告書作成

個人情報保護マネジメントシステムに関する規程の整備



プライバシーマーク取得までの作業概要

～ 5フェーズ・16ステップ アプローチ～

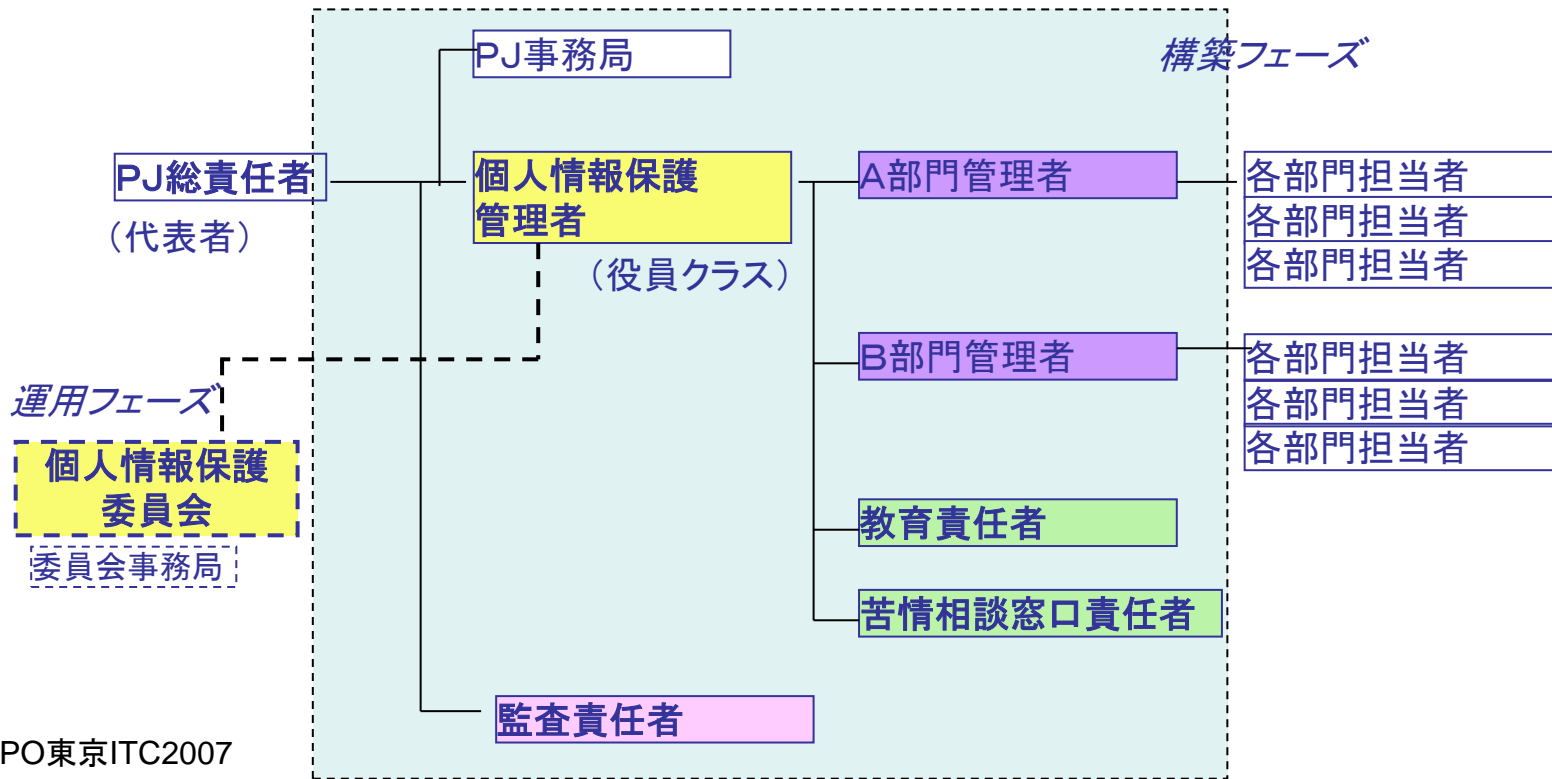


個人情報保護マネジメントシステム構築・推進組織

□立上げ時のプロジェクト組織と本番運用組織の想定

- ①PJによる機動的な運営の場合
- ②委員会方式で運営の場合
- ③共通・教育、監査担当の早期任命

□組織の明確化・役割・権限・責任の明確化(明文化)



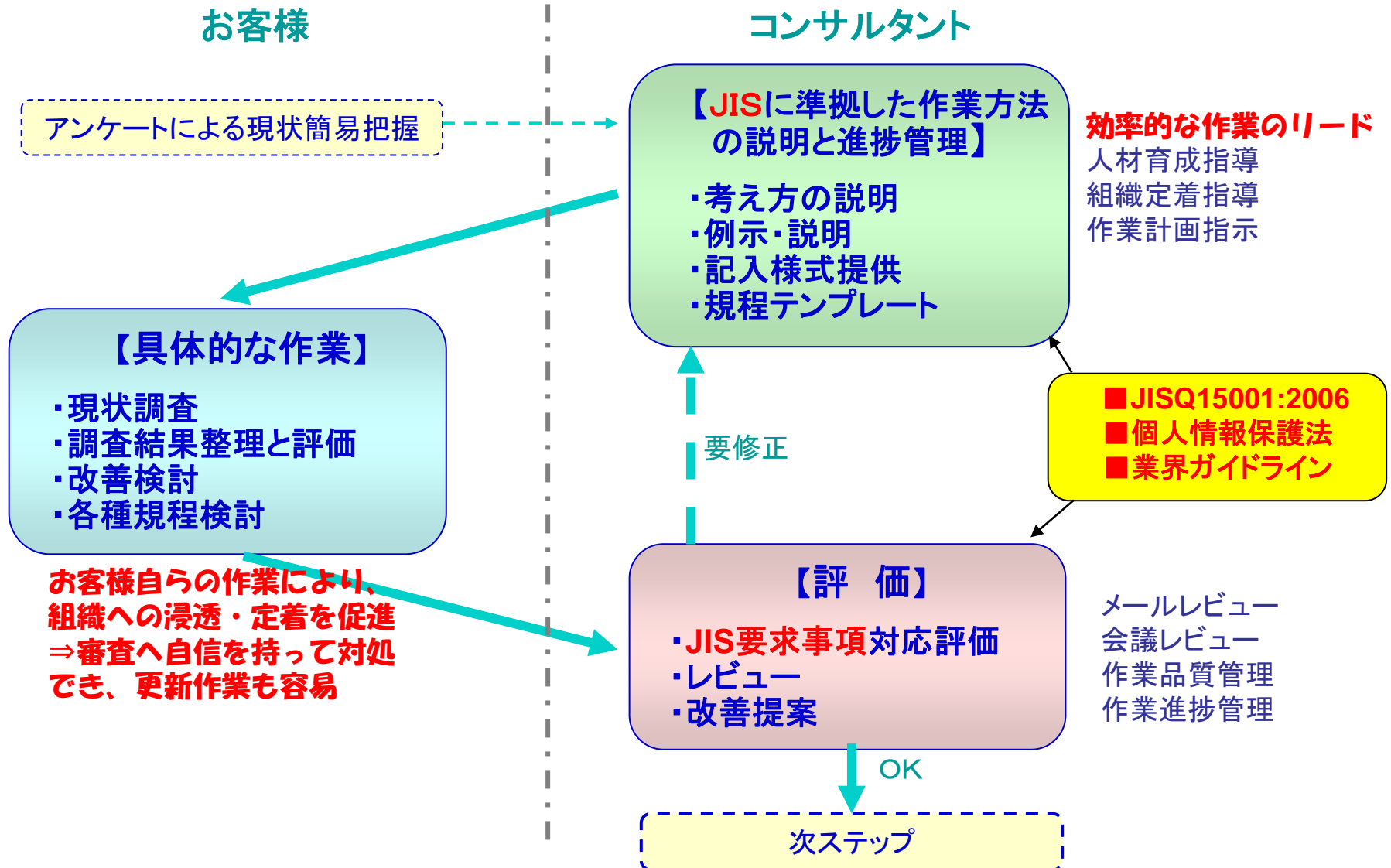
プライバシーマーク取得のための主要作業イメージ(1)

ステップ	フェーズ	作業項目	成果物例	貴方の作業	弊社の主な支援	日程例
1.	方針設定	○組織としての個人情報保護方針を文書化する	個人情報保護方針	<input type="checkbox"/> 方針の明確化 <input type="checkbox"/> 代表者主導実施	・方針ヒヤリング ・テンプレート提供	1 日目
2.		○PMS(個人情報保護マネジメントシステム)策定のためのPJ組織を作る	PJ体制表	<input type="checkbox"/> PJ組織化とPJメンバー人選	・検討支援 ・テンプレート提供	1
3.		○PMS策定の全体作業計画を立てる	作業計画スケジュール表	<input type="checkbox"/> 全体計画検討 <input type="checkbox"/> 関係者協力依頼	・作業スケジュール案提示	1
4.		○PJキックオフ ○個人情報保護方針を組織内に周知する	教育実施報告書	<input type="checkbox"/> 教育対象拡大 <input type="checkbox"/> 意義の理解	*キックオフ会における全体教育の支援	2
5.	現状調査	○組織内の個人情報を特定する ・個人情報棚卸、JIS要求事項と比較	個人情報調査票 個人情報管理台帳	<input type="checkbox"/> 調査・ヒヤリング <input type="checkbox"/> リスク評価検討	・調査方法の指導 ・テンプレート提供	2～ 4
6		○法令、国が定める指針、その他の規範を特定する	関連法規一覧	<input type="checkbox"/> 業界ガイドライン調査 <input type="checkbox"/> 事業関連法令調査	・サンプル提供	3～ 5
7		○個人情報リスクを認識し、分析し、対策を検討する	業務フローリスク分析 安全対策計画	<input type="checkbox"/> リスク分析	・現状調査シート提供 ・纏めかた説明	3～ 5
8	PMS構築	○必要な資源を確保する。	個人情報保護体制図 安全対策投資予算	<input type="checkbox"/> 経営資源投入計画検討	・安全対策レビュー	4 5
9		○PMSの内部規程を策定する	基本規程 その他各種規程	<input type="checkbox"/> 規程体系検討 <input type="checkbox"/> 各種規程の作成	・テンプレート提供 ・成果物レビュー	6～ 9

プライバシーマーク取得のための主要作業イメージ(2)

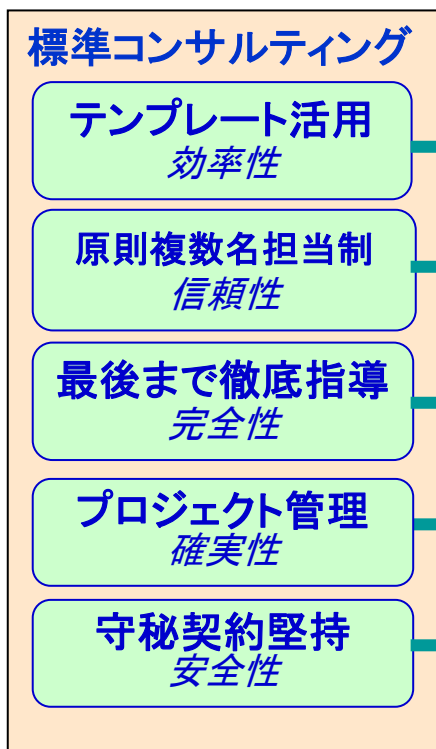
ステップ	フェーズ	作業項目	成果物例	貴方の作業	弊社の主な支援	日程例
10.	試行・監査・改善	OPMSを周知するための教育を実施する	教育計画 教育実施報告書	<input type="checkbox"/> 社内教育の実施 <input type="checkbox"/> 機能別教育	・教育?監査計画 (教育オプション)	9
11.		OPMSの運用を開始する	実施記録	<input type="checkbox"/> 実施計画作成	・実施計画レビュー	
12		OPMSの運用状況を点検し改善する 是正処置・予防措置検討	監査計画 監査実施報告書	<input type="checkbox"/> 内部監査の実施 <input type="checkbox"/> 改善処置	・監査方法の指導 ・監査チェックリスト	9 9
13		OPMSの見直しを実施する	PMS文書の改定	<input type="checkbox"/> PMSの見直し <input type="checkbox"/> PMS改善と文書反映 <input type="checkbox"/> 改定内容徹底	・改善案レビュー	10
14	申請・審査	○審査機関へ申請し、申請手数料を支払う	申請書	<input type="checkbox"/> 申請諸作成と申請 <input type="checkbox"/> 申請手数料支払	・申請書作成支援 ・文書審査後対応	10
15		○プライバシーマークの審査を受ける		<input type="checkbox"/> リハーサル <input type="checkbox"/> 受審 <input type="checkbox"/> 審査結果対応	・リハーサル ・現地審査後対応	10
16		○認定後プライバシーマーク、使用許諾契約を結ぶ	認定書 Pマーク添付	<input type="checkbox"/> 使用許諾契約締結 <input type="checkbox"/> Pマーク使用料支払	-	-
★	スパイラルアップ	PMSの継続的な運用 ⇒2年単位更新	顧客の信頼 経営基盤強化	<input type="checkbox"/> 運用と教育 <input type="checkbox"/> 監査と改善	(オプション)	-

個人情報保護マネジメントシステム構築作業方法



NPO東京ITCから提案させていただく取得支援作業

お客様の「顧客満足度向上マネジメント」を支援
(コンプライアンス経営の確立)



現場へのスムーズな導入
リスク最小化提案

導入企業における人材育成
組織定着

個別支援作業／アフターフォロー
調査・ヒヤリング・教育・監査

追加コンサルティング
(オプション)

研修・実務支援
(オプション)

PMS標準支援サービスの進め方

□中堅企業向け支援サービスの期間・回数の設定

- ・目標: 6~10ヶ月間に「10回」支援させていただきます。

(拠点数、事業種類・規模、管理体制により変動します)

□支援の進め方(役割分担)

- ・**貴社:** 貴社の**個人情報保護マネジメントシステムの確立のためのプロジェクトを編成し、トップダウンで実務作業を推進していただきます。**
- ・**弊社:** そのために必要な**進め方を助言し、基本的な規定のサンプルやテンプレートの提供**を行います。尚、現場の教育、調査等の実務作業は別途と致します。

□上記以外の取り扱い

- ・上記の**期間・回数**を越えた場合の指導や、**実務支援**については別途**オプション契約**とさせていただきます。
- ・ご質問は**メール**でもお受けいたします。
- ・効率的な会議進捗のために、事前に**次回資料**を電子メールで送信させていただく場合がございます。
- ・会議席上には**プロジェクター**をご準備願います。

□相互の**秘密保持契約**を締結させていただきます。