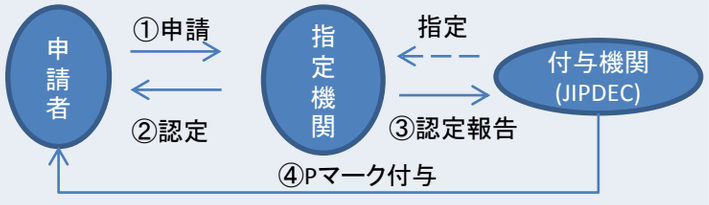
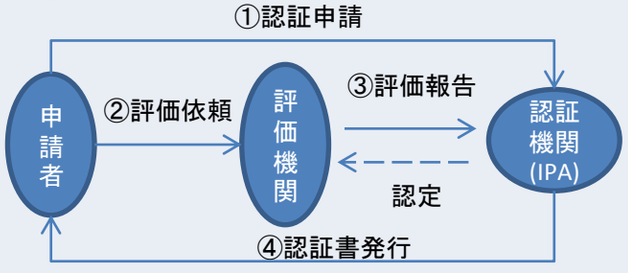
情報保護評価に関連する認定制度

参考資料6

項目	プライバシーマーク制度	ISMS適合性評価制度	ITセキュリティ評価及び認証制度
定義	個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度	組織の情報セキュリティ管理に関する仕組みを、第三者（認証機関）が評価し、認証する制度	IT関連製品（例　デジタル複合機、ミドルウェア、ネットワーク機器）のセキュリティ機能の適切性・確実性を、第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度
認証基準	JIS Q 15001：2006	JIS Q 27001：2006（ISO/IEC 27001：2005）	JIS X 5070（CC (ISO/IEC 15408)）
経緯	1998年4月、運用開始 1999年3月、JIS Q 15001:1999制定に伴い、認証基準をそれまでの通商産業省ガイドラインから上記に変更 2006年5月、JIS Q 15001:2006公表に伴い、認証基準を上記に変更	2002年4月、運用開始 2003年4月、認証基準をv2.0（BS7799-2準拠）に改訂 2007年11月、認証基準v2.0をJIS Q 27001:2006に移行完了	2001年 4月、創設 2003年10月31日、国際的な相互承認の協定であるCCRA（Common Criteria Recognition Arrangement）に加盟 2004年 4月、同制度の認証業務が、独立行政法人製品評価技術基盤機構(NITE)より独立行政法人情報処理推進機構（IPA）に移管。
取得の流れ	1.申請者は、指定機関（JIPDECが指定したもの）に申請を行う（ただし、一部の事業者はJIPDECが申請を受理し、審査・認定を行う）。 2.指定機関は、申請書の受理後、文書審査と現地審査を行う。 3.指定機関は、審査結果に基づきプライバシーマーク付与の可否を決定し、申請者と付与機関に通知する。 4.付与機関（JIPDEC）は、プライバシーマーク使用許諾証を申請者に交付し、ホームページで公表する。 5.認定の有効期間は2年間。それ以降は更新手続が必要となる。 	1.申請者は、認証機関（JIPDECが認定したもの）を選択し、その認証機関に対して認定申請する。 2.認証機関は、まず、書面等をベースにISMSの構築状況を審査して、審査の焦点を絞る（第一段階審査）。次に、絞った焦点を中心に、現場ヒアリング等を通じてISMSの運用・実施状況を審査する（第二段階審査）。 3. 審査の結果、認証されると、認証機関は認証登録を行い、その結果をJIPDECに対し報告し、JIPDECはこれを公開する。 4.認証登録されたら、通常1年毎に審査を行い（サーベイランス審査）、3年毎に再認証審査が行われる。 	1.申請者は、評価機関（認証機関が認定したもの）を選択し、製品の評価依頼をするとともに、認証機関（IPA）に認証申請を提出する。 2.評価機関は、製品に係る様々なセキュリティの側面をセキュリティ評価基準に基づいて評価する（開発資料や流通過程、ガイダンスなど）。 3.評価機関は、評価が完了すると認証機関に対し、評価結果を記載した評価報告を提出する。 4.認証機関は、評価報告を確認した後、セキュリティ評価基準を達成していれば、認証保証レベル（EAL）に応じて、その製品に対する認証書を発行する。 ※セキュリティ機能の変更がなければ、製品のバージョンアップ後も保証が継続する。 
取得数	12,182社（2001/8/15時点） ※認定は法人単位	3,830機関（2011/7/1時点） ※認定は申請者が適用範囲として示した組織単位となる	290（2011/6/29時点） ※認定申請の単位が複数製品に共通の機能の場合もあることから、製品数とは一致しない。
評価内容	法人において、PMS（個人情報保護マネジメントシステム）確立から維持及び改善までのPDCAサイクルが有効に機能しているか（認証基準の要求事項を満たしているか）評価する。	組織において、ISMS（情報セキュリティマネジメントシステム）確立から維持及び改善までのPDCAサイクル（別紙参照）が有効に機能しているか（認証基準の要求事項を満たしているか）評価する。	セキュリティ機能の適切性・確実性が、要件定義・設計・開発・テスト・設置・運用のライフサイクル全体を通して保証されているか（認証基準の要求事項を満たしているか）を評価する。どの工程まで評価するか、どこまで詳細に評価するかによって、EALが異なる。

JIS Q 27001:2006におけるPDCAサイクル

別紙

<Plan>ISMSの確立　※下図参照

・リスク対応計画の作成・実施等
・教育、訓練、意識向上等

<Do>ISMSの導入及び運用

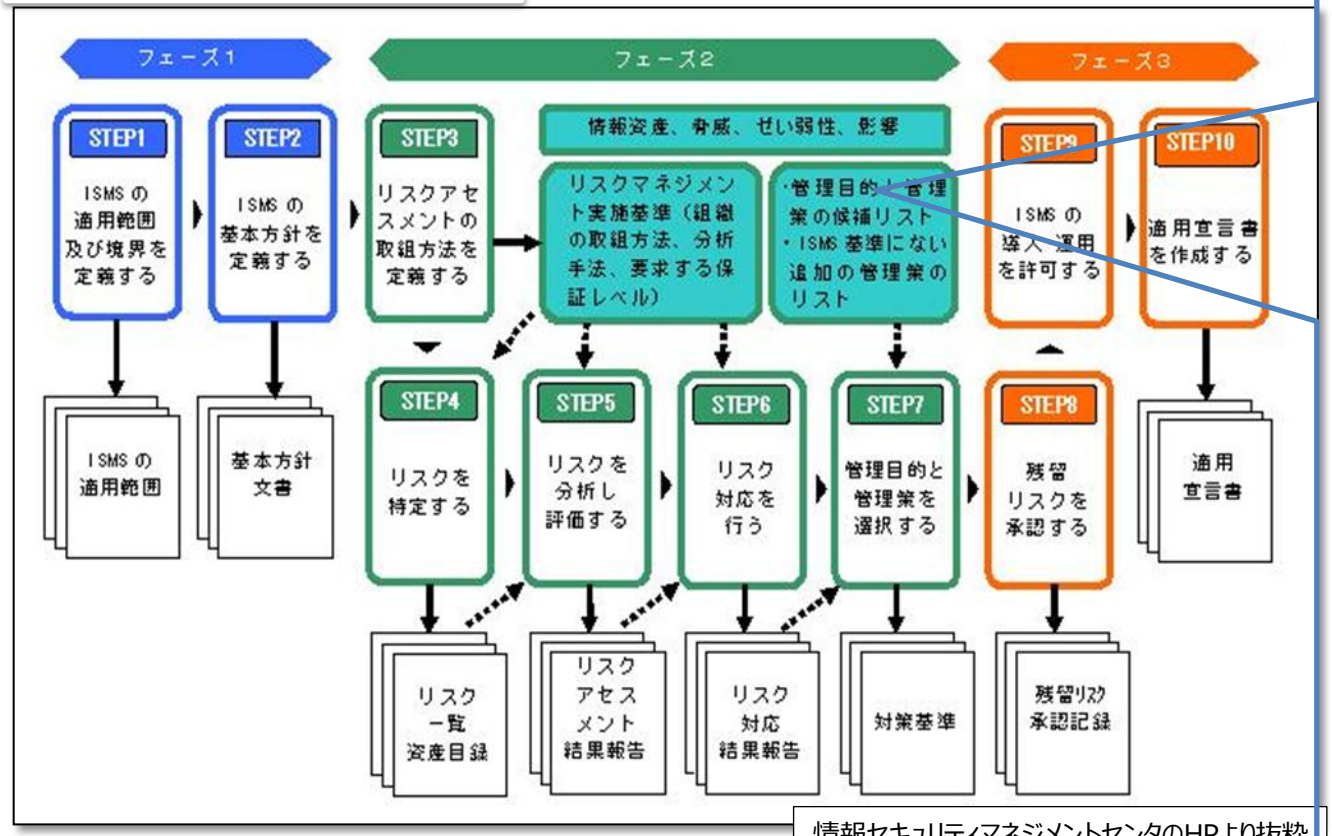
・ISMS内部監査の実施
・ISMSのマネジメントレビュー等

<Check>ISMSの監視及びレビュー

・是正処置、予防措置の実施等

<Action>ISMSの維持及び改善

ISMSの確立

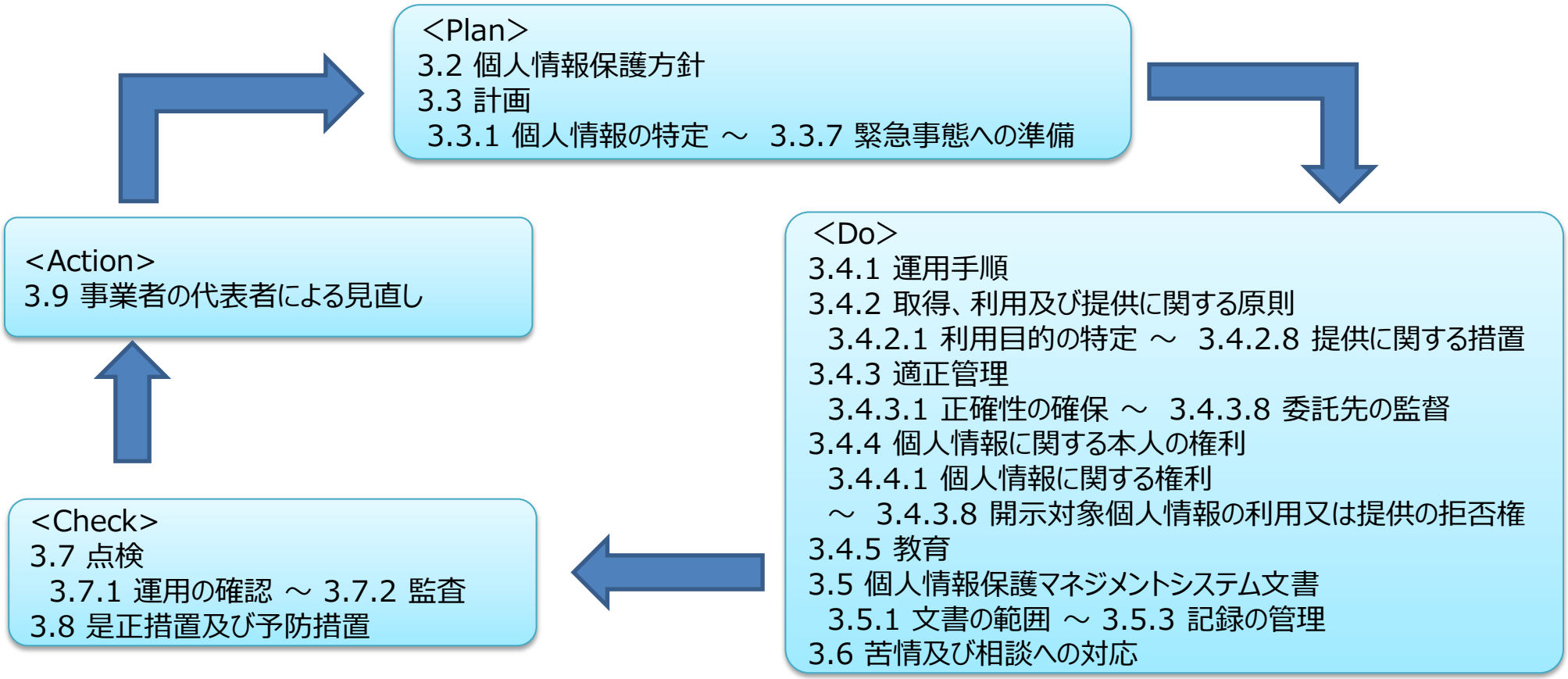


情報セキュリティマネジメントセンタのHPより抜粋

選択肢となる管理策は、「付属書A」が規定している。
【付属書Aの記載事項】 ※ISO/IEC27001:2005から引用

1．セキュリティ基本方針
・経営陣の方向性、セキュリティ管理の原則など
2．情報セキュリティのための組織
・従業員との秘密保持契約の内容など
3．資産の管理
・資産目録の作成、管理責任者の設置など
4．人的資源のセキュリティ
・雇用条件、教育・訓練計画、雇用終了後の措置など
5．物理的及び環境的セキュリティ
・施設の入退室管理や装置の設置基準など
6．通信及び運用管理
・操作手順の整備、変更管理、ウイルス対策、バックアップ、媒体の取り扱い、システム監視、ログの取得など
7．アクセス制御、
・ネットワーク・OS・ミドルウェア・業務アプリケーションのアクセス制御など
8．情報システムの取得、開発及び保守
・業務アプリケーションの正確性確保、暗号による秘匿、ソフトウェアなどの脆弱性管理など
9．情報セキュリティインシデントの管理
・脆弱性発見時の報告、事故発生時の手順など
10．事業継続管理
・事業継続計画の策定・維持・評価など
11．順守
・法令要求事項、方針、情報セキュリティ監査など

JIS Q 15001:2005 におけるPDCAサイクル



個人情報保護マネジメントシステム（PMS）構築の具体的な進め方

STEP1　個人情報保護方針を定め文書化する。
STEP2　PMS策定のための組織を作る。
STEP3　PMS策定の作業計画を立てる。
STEP4　個人情報保護方針を組織内に周知する。
STEP5　個人情報を特定する。
STEP6　法令、国が定める指針その他の規範を特定する。
STEP7　個人情報のリスクを認識し、分析し対策を検討する。
STEP8　必要な資源を確保する。
STEP9　PMSの内部規定を策定する。
STEP10　PMSを周知するための教育を実施する。
STEP11　PMSの運用を開始する。
STEP12　PMSの運用状況を点検し改善する。
STEP13　PMSの見直しを実施する。