

プライバシーマーク®制度について



2011年9月7日

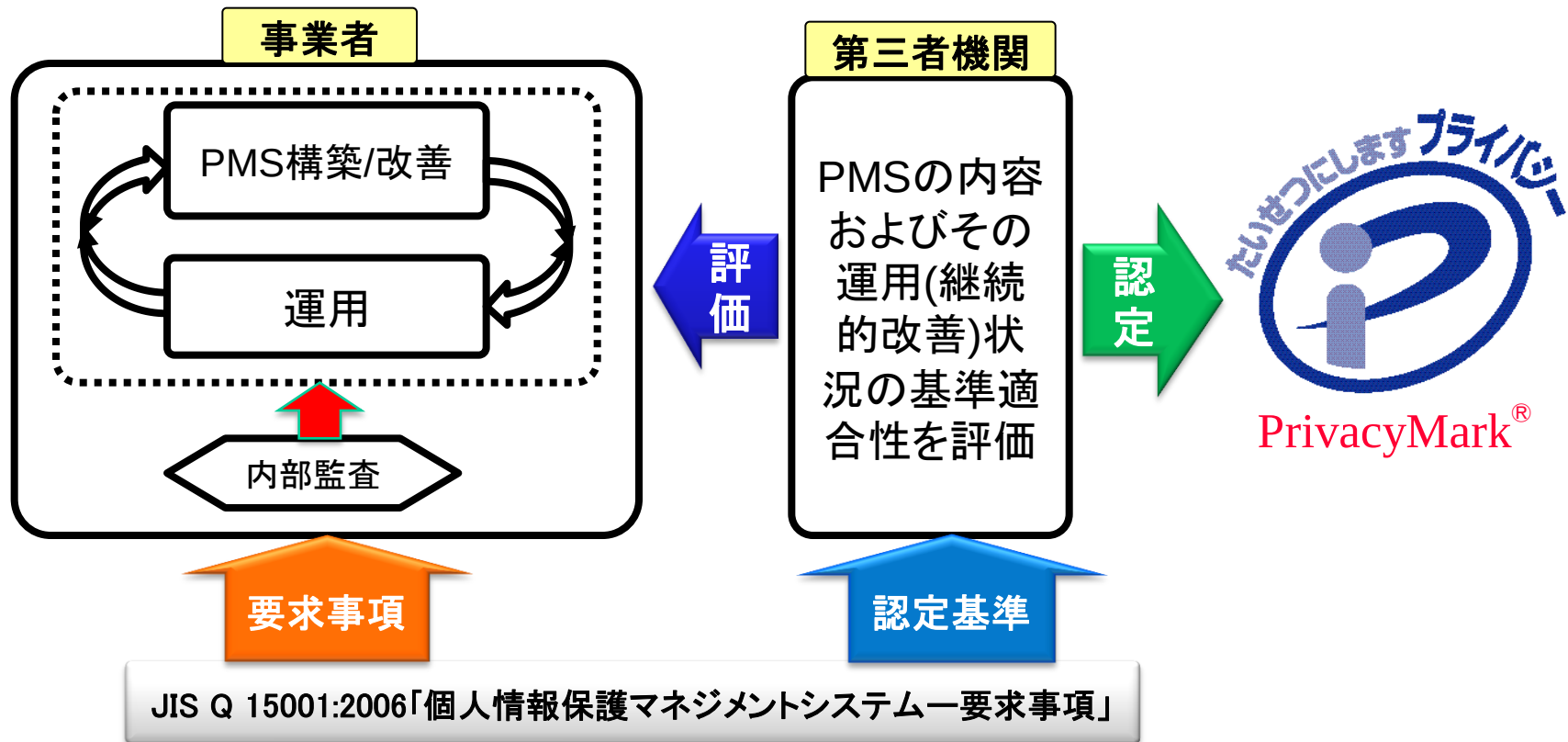
JIPDEC

一般財団法人 日本情報経済社会推進協会

プライバシーマーク®制度とは

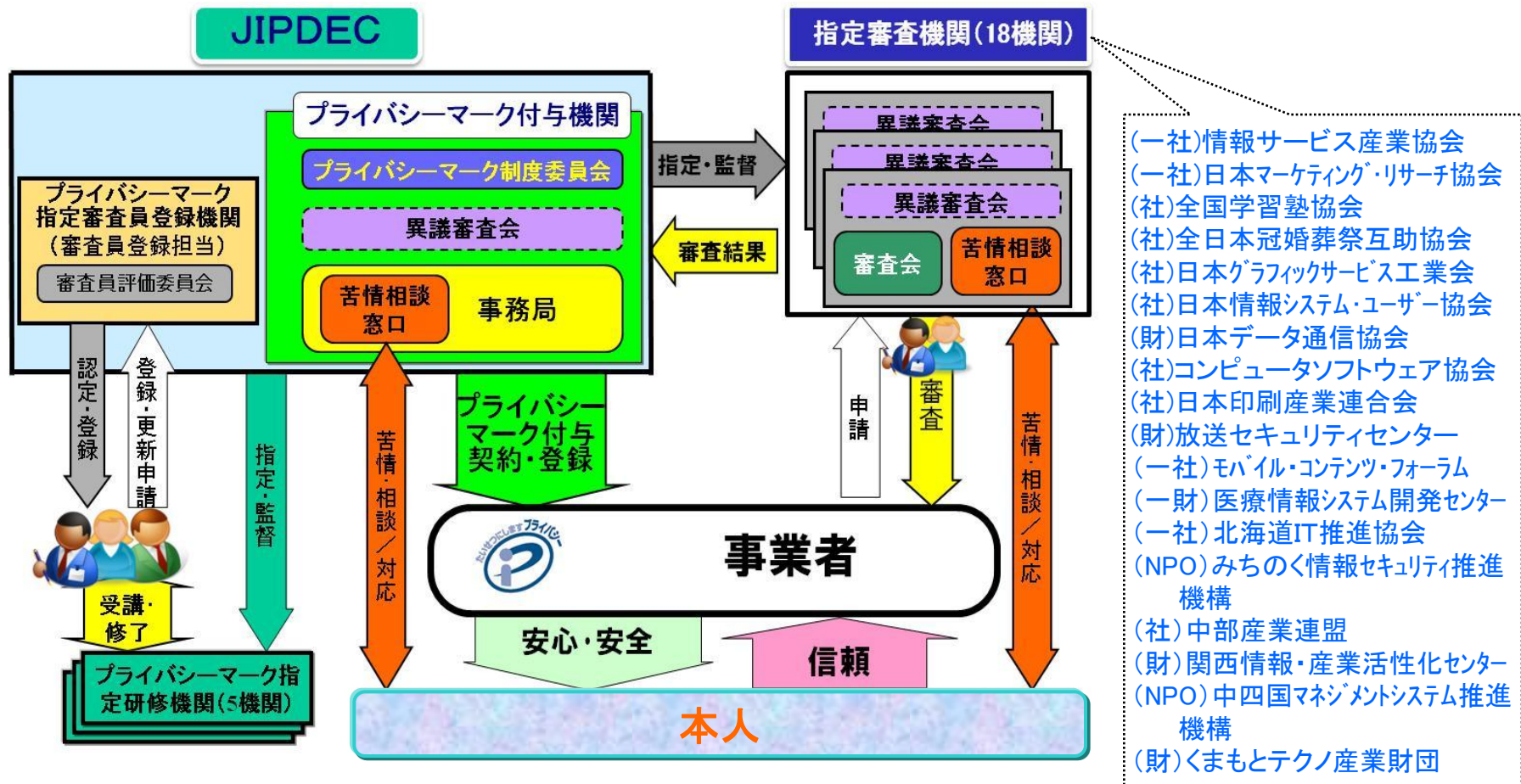
- 事業者の個人情報を取扱う仕組み～個人情報保護マネジメントシステム（PMS）～がJIS Q 15001:2006に適合し、その運用が適正であることを評価して“プライバシーマーク®”の使用を認める制度
- 1998（平成10）年4月スタート
- 法人が認定の単位

* JIS Q 15001:2006「個人情報保護マネジメントシステム—要求事項」



プライバシーマーク®制度とは

プライバシーマーク制度運用体制



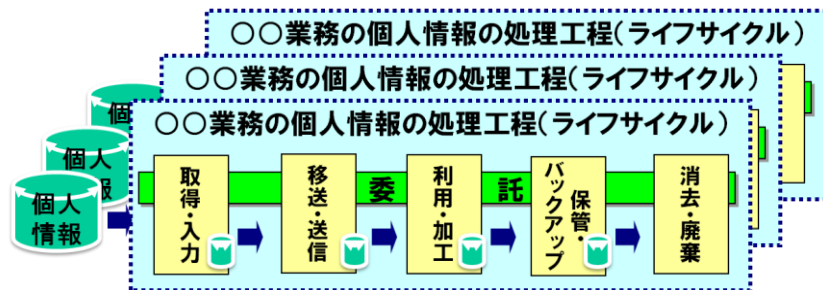
プライバシーマーク®制度におけるPMS構築

事業者

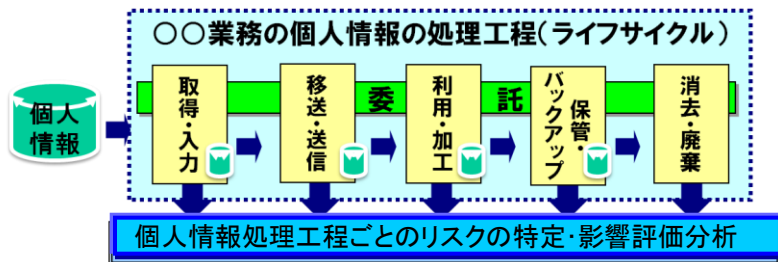
PMS(個人情報保護マネジメントシステム)

個人情報の取扱いに関するリスクを適正に管理するために、Plan、Do、Check、Act要素を含んだ管理の仕組み

1. 個人情報を業務と結び付けて特定(洗い出す)

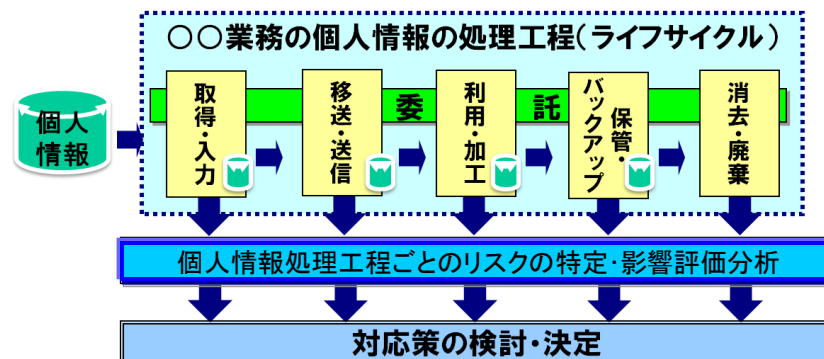


2. 業務上の取扱いにおいて発生可能性のあるリスクの特定・影響評価分析



リスク: 同意のない取得／提供、目的外利用、権利への不対応、不正な取得、毀損、漏えい、紛失(滅失)、破壊 等

3. リスク顕在化を防止する対応策を検討し選択・決定



4. 決定した対応策を実装、ルール(規定)化



プライバシーマーク®制度の事業者による内部監査

事業者の
PMS
構築
作業

個人情報取扱上のリスクの特定とそのリスクが顕在化した場合の影響分析により、そのリスク顕在化を予防する仕組み作り

→自らによる個人情報保護の観点から影響評価を踏まえた仕組み作り

PMS
運用
段階
の
監
査

1. 適合性監査 と運用監査

- ① 当該事業者の(我が社の)PMSがJIS Q 15001に適合しているかを評価する
- ② 各業務部門が、個人情報の取扱いをPMSの定めたルール(規定)通りに行っているか評価する

2. 監査で使用する チェック リスト

- ① リスク分析結果を反映したチェックリストを作成し、その結果が反映されたPMSになっているか評価する
- ② 経済的な理由等で、リスク対策を打てなかった部分に関する日常点検の実施状況の評価する

3. 監査体制の 確立

- ① 他の業務に関わりなく監査の権限を与えることで、可能な限り客観性を確保する
- ② 監査の資質を踏まえた体制確保が難しい(内部監査の信頼性)

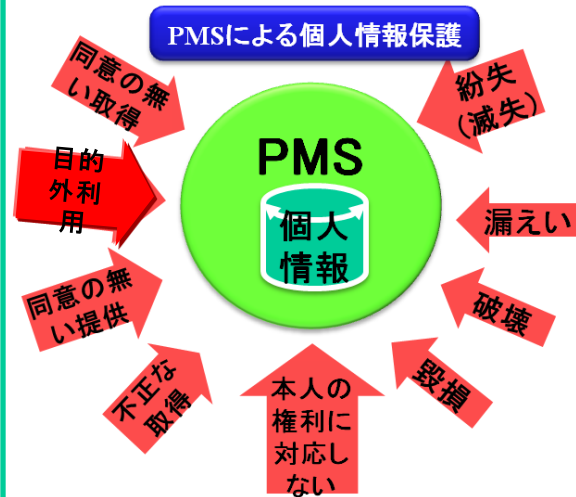
PMSが環境変化等による新たなリスクによる影響に対応できているかを評価し、その結果をPMSの改善に結び付ける活動

プライバシーマーク®制度の審査

事業者

PMS

個人情報の取扱いに関するリスクを適正に管理するために、Plan、Do、Check、Act要素を含んだ管理の仕組みを構築し運用している状況



審査機関(第三者機関)による評価

1. 事業者における個人情報取扱いに係る個人情報保護上の影響評価

- ① 当該事業者における全ての業務と、その業務で取り扱う個人情報が漏れなく認識(特定)されていることを評価する
- ② 業務毎に、業務手順(工程)における個人情報の取扱いに関するリスクが漏れなく洗い出されていることを評価する
- ③ リスクが顕在化した場合の本人及び当該事業者への影響の大きさ等が分析されていることを評価する

2. 影響をヘッジする(最小限に抑える)仕組みの評価

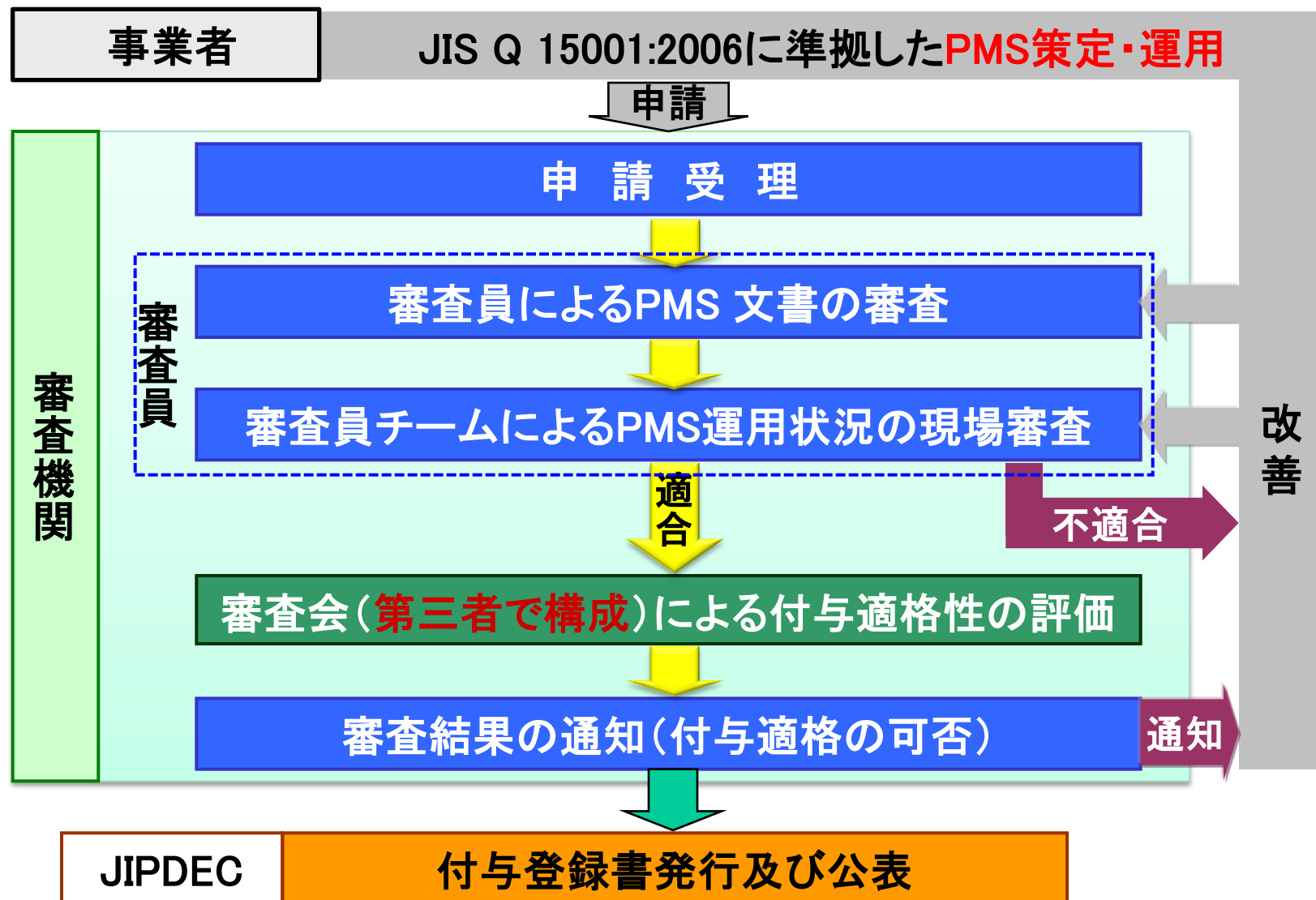
- ① リスクの顕在化を防止する対策が検討され合理的な対策を選択・決定していることを評価する

3. 当該組織が定めたPMS通りに運用されているかの評価

- ① 日常の運用および不具合が発見されたときにPMSの通りに適切に対応できているかを評価する
- ② 内部監査などの実施結果を踏まえて見直しが行われているかを評価する

Pマークによる認定審査 → 事業者自らによる個人情報保護影響評価の適切性評価

プライバシーマーク®制度の認定までの流れ



プライバシーマーク®制度の基準(JISQ15001)

参考: JIS Q 15001:2006の要求事項の構成

項番	内容	項番	内容
PLAN(計画)		3.4.3	適正管理
3.1	一般要求事項	3.4.4	個人情報に関する本人の権利
3.2	個人情報保護方針	3.4.5	教育
3.3	計画	3.5	個人情報保護マネジメントシステム文書
3.3.1	個人情報の特定	3.5.1	文書の範囲
3.3.2	法令、国が定める指針その他の規範	3.5.2	文書管理
3.3.3	リスクなどの認識、分析及び対策	3.5.3	記録の管理
3.3.4	資源、役割、責任及び権限	3.6	苦情及び相談への対応
3.3.5	内部規程	CHECK(点検)	
3.3.6	計画書	3.7	点検
3.3.7	緊急事態への準備	3.7.1	運用の確認
DO(実施)		3.7.2	監査
3.4	実施及び運用	3.8	是正処置及び予防処置
3.4.1	運用手順	ACT(見直し)	
3.4.2	取得、利用及び提供に関する原則	3.9	事業者の代表者による見直し



一般財団法人日本情報経済社会推進協会 プライバシーマーク推進センター

〒105-0011 東京都港区芝公園3-5-8 機械振興会館内

TEL: 03-3432-9387

FAX: 03-3432-9419

<http://privacymark.jp/>

**JIPDEC**

