改定3版

プライバシーマーク取得支援サービス

有限会社オフィスネットワーク

１．主な情報セキュリティ事故

■近年の主な情報セキュリティ事故

■サントリー　　：顧客情報７５,０００人分流出
■北海道警　　：巡査の私物パソコンから捜査情報流出
■社会保険事務所：未納者カード３７２人分紛失
■京都府警　　：捜査書類流出、十数人がネット上に
■東武鉄道　　：１３万人の顧客情報漏えいか
■ NTT系アッカ・ネット：最大１４０万人分流出か
■奈良県の病院　：盗難パソコンに7,５００人分個人情報
■シティバンク　：海外で１２万口座分の顧客情報を紛失
■金沢医科大　　：電子カルテ・パスワード漏えい
■三井住友カード：業務委託先におけるサーバーへの不正侵入
■ジャパネットたかた：数十万人分流出か
■ヤフーＢＢ　　：４６０万人分の個人情報流出
■三洋信販　　：３２万人分？流出の可能性も
■セゾン情報システムズ：採用応募者名など漏えい
■神戸電鉄　　：メールアドレス１９０人分を誤配信
■長野赤十字血液センター：献血者の氏名など流出
■りそな銀行　　：９８万件の個人情報を紛失
■国税庁　　：ＨＰから他人の確定申告書が印刷
■国土地理院　　：ＨＰから個人情報流出
■群馬県国際課　：２００人分メルアド流出、職員による操作ミス
■ヤフーＢＢ　　：顧客情報２４２件流出
■ＪＣＢなど3社：6,９２３人分記録のＦＤ紛失
■海上自衛隊　　：情報セキュリティ関連資料、業者に

2．個人情報の保護について

■個人情報とは

「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。
死者に関する情報でも、生存する遺族個人に関する場合は、その生存する個人に関する情報としてとらえることになる。
＊法人及び団体は個人情報とはなりませんが、代表者等の個人名等は個人情報とみなされます（契約書etc）

e-mailも個人に識別できれば個人情報とみなされます。

■個人情報保護法

高度情報通信社会の進展にともない個人情報の利用が著しく拡大していることに鑑みて次の2点をポイントとして制定された。

1．個人情報の適正な取り扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務を明らかにする。

2．個人情報を取り扱う事業者の遵守すべき義務を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護する。

3．個人情報保護法による個人情報取扱事業者の義務

■個人情報法による個人情報取扱事業者の義務

OECD8原則	個人情報取扱事業者の義務
①目的明確化の原則 収集目的を明確にし、データ利用は収集目的に合致すべき	■利用目的をできる限り特定しなければならない（第15条） ■利用目的の達成に必要な範囲を超えて取り扱ってはならない（第16条） ■本人の同意を得ずに第三者に提供してはならない（第23条）
②利用制限の原則 データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない。	
③収集制限の原則 適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき	■偽りその他不正の手段により取得してはならない（第17条）
④データ内容の原則 利用目的に沿ったもので、かつ正確、完全、最新であるべき	■正確かつ最新の内容に保つよう努めなければならない（第19条）
⑤安全保護の原則 合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護すべき	■安全管理のために必要な措置を講じなければならない（第20条） ■従業者・委託先に対して必要な監督を行わなければならない（第21,22条）
⑥公開の原則 データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき。	■取得したときは利用目的を通知又は公表しなければならない（第18条） ■利用目的等を本人の知り得る状態に置かなければならない（第24条） ■本人の求めに応じて保有個人データを開示しなければならない（第25条） ■本人の求めに応じて訂正等を行わなければならない（第26条） ■本人の求めに応じて利用停止等を行わなければならない（第27条）
⑦個人参加の原則 自己に関するデータの所在及び内容を確認させ、又は意義申立を保証するべき。	
⑧責任の原則 管理者は諸原則の実施の責任を有する。	■苦情の適切かつ迅速な処理に努めなければならない（第31条）

＊OECD：「Organization for Economic Cooperation and Development：経済協力開発機構」の略で、
本部はフランスのパリに置かれています。（現在加盟国はEUを中心とした世界30ヵ国）

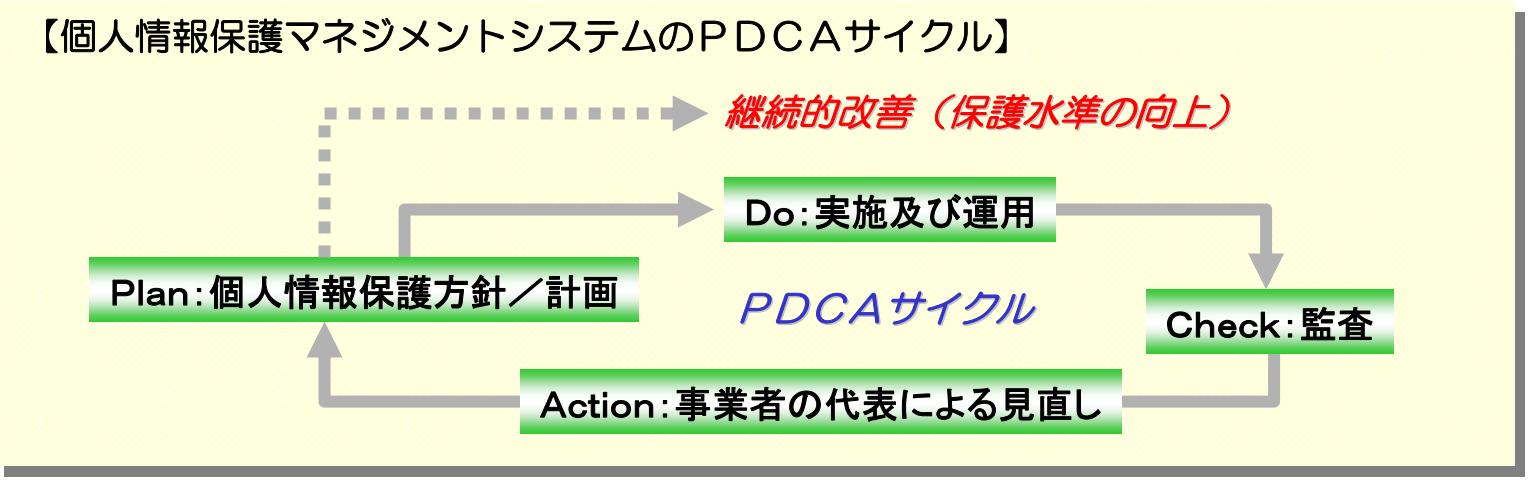
4．プライバシーマーク制度について

■プライバシーマーク制度とは

個人情報保護ＪＩＳ（JIS　Q 15001:2006）に適合した個人情報保護マネジメントシステムを整備し、個人情報の取り扱いを適切に行っている事業者を、第三者機関であるJIPDEC（及びその指定機関）が評価・認定し、その証としてプライバシーマークと称するロゴの使用を承諾する制度。

■個人情報保護マネジメントシステムとは

「自らの事業の用に供している」個人情報について個人情報保護に関する方針・計画策定から、
実施・運用、監査、見直しといった一連の規則と計画を作成し、記録に残すことを継続的に行っていくもの。



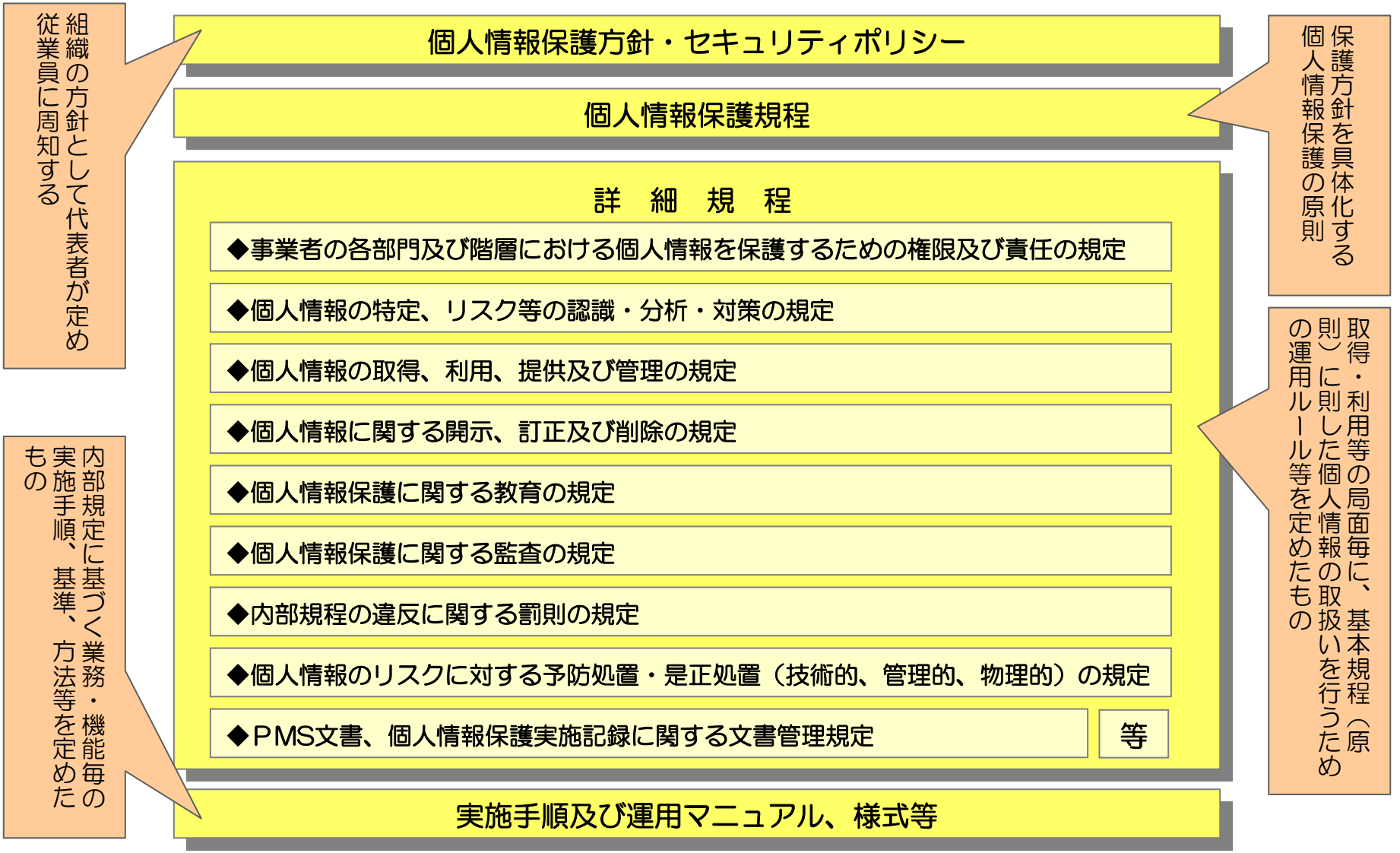
5．JIS　Q　15001規格の構成

■JIS Q 15001：2006規格の構成

1. 適用範囲
2. 用語及び定義
3. 要求事項
3.1 一般要求事項
3.2 個人情報保護方針
3.3 計画　**Plan**
3.3.1 個人情報の特定
3.3.2 法令、国が定める指針その他の規範
3.3.3 リスクなどの認識、分析及び対策
3.3.4 資源、役割、責任及び権限
3.3.5 内部規定
3.3.6 計画書
3.3.7 緊急事態への準備
3.4 実施及び運用　**Do**
3.4.1 運用手順
3.4.2 取得、利用及び提供に関する原則
3.4.2.1 利用目的の特定
3.4.2.2 適正な取得
3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限
3.4.2.4 本人から直接書面によって取得する場合の措置
3.4.2.5 個人情報を3.4.2.4以外の方法によって取得した場合の措置
3.4.2.6 利用に関する措置
3.4.2.7 本人にアクセスする場合の措置
3.4.2.8 提供に関する措置
3.4.3 適正管理
3.4.3.1 正確性の確保
3.4.3.2 安全管理措置
3.4.3.3 従業者の監督
3.4.3.4 委託先の監督
3.4.4 個人情報に関する本人の権利
3.4.4.1 個人情報に関する権利
3.4.4.2 開示等の求めに応じる手続
3.4.4.3 開示対象個人情報に関する事項の周知など
3.4.4.4 開示対象個人情報の利用目的の通知
3.4.4.5 開示対象個人情報の開示
3.4.4.6 開示対象個人情報の訂正、追加又は削除
3.4.4.7 開示対象個人情報の利用又は提供の拒否権
3.4.5 教育
3.5 個人情報保護マネジメント文書
3.5.1 文書の範囲
3.5.2 文書管理
3.5.3 記録の管理
3.6 苦情及び相談への対応
3.7 点検　**Check**
3.7.1 運用の確認
3.7.2 監査
3.8 是正処置及び予防処置
3.9 事業者の代表者による見直し　**Action**

6．個人情報保護マネジメントシステムの策定

■個人情報保護マネジメントシステムの策定



7．プライバシーマーク取得のメリット

■プライバシーマーク取得のメリット

1．顧客への信頼性向上　　*ＪＩＳ規格において第三者が審査・認証していることがポイント！*

個人情報を保護する取り組みを行っている企業として顧客や取引先より信頼され安心感を与える。

2．社員の教育・訓練

教育・訓練はプライバシーマーク取得の大きな要求事項の一つであり、個人情報保護に関する業務の関連するすべての人々にしかるべき教育・訓練の実施を要求しているため社員の意識改革になります。→人が一番のセキュリティーホール

3．自社のＰＲ

プライバシーマークを広告宣伝に使うことにより、個人情報を適切に取り扱っている企業としてアピールすることができる。

4．他社との差別化

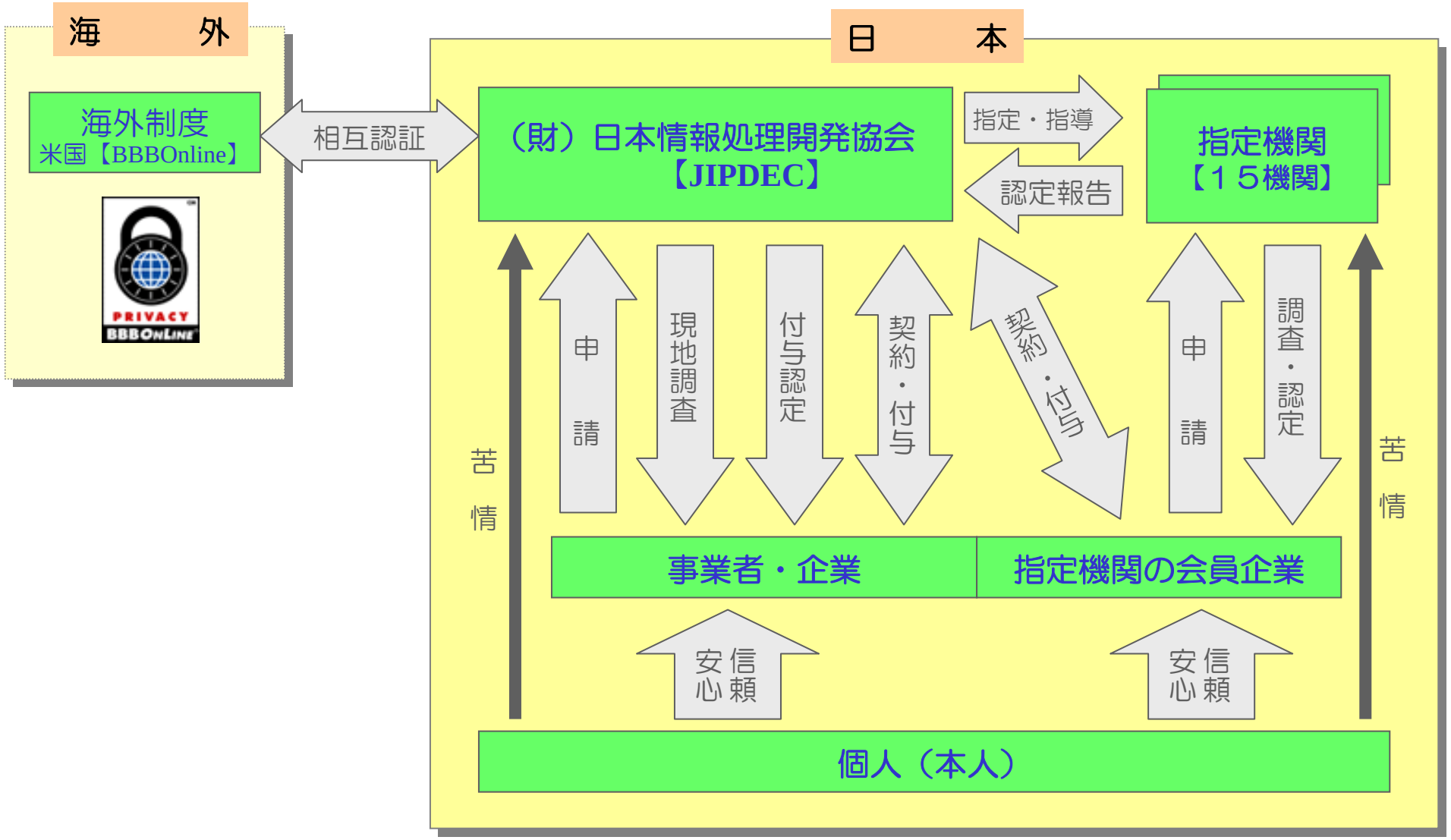
個人情報を保護する仕組みをつくることによって、個人情報を適切に管理している企業として顧客や取引先からの信用度がアップして競合他社との差別化をはかることができる

5．既存のＩＳＯマネジメントシステムと併用できる

既存の品質マネジメントシステム（ISO9001）、及び環境マネジメントシステム（ISO14001）、情報セキュリティマネジメントシステム（ISMS）等との併用ができます。

８．プライバシーマーク認定制度の仕組み

■プライバシーマーク認定制度の仕組み



9．プライバシーマーク取得審査料金について

■料金表

種　別	小規模事業者	中規模事業者	大規模事業者
申請手数料	50,000円	50,000円	50,000円
現地調査料	200,000円	450,000円	950,000円
マーク使用料	50,000円	100,000円	200,000円
合　計	300,000円	600,000円	1,200,000円

あくまでも審査料金です。
コンサルティング料金は
別途お見積りなります。

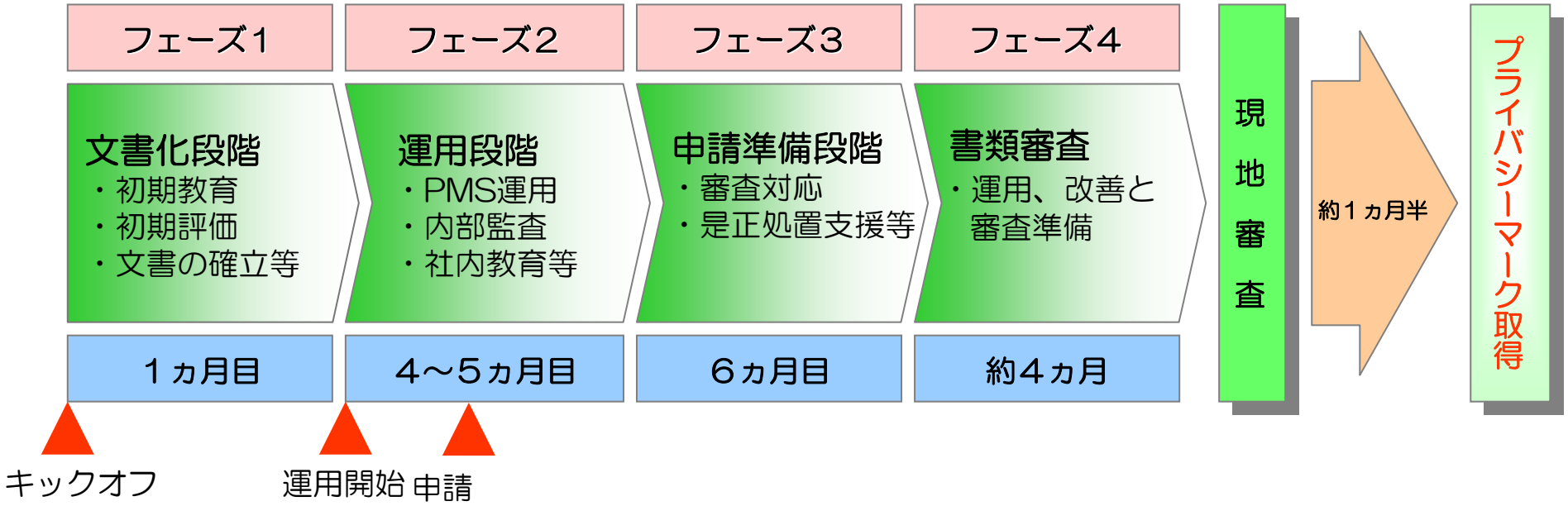
＊更新審査は別料金です。

■事業規模分類

		卸売業	小売業	サービス業	製造業／その他
小規模事業者	従業員	5人以下			20人以下
中規模事業者	資本金	1億円以下	5,000万円以下	5,000万円以下	3億円以下
	従業員	6～100人以下	6～50人以下	6～100人以下	21～300人以下
大規模事業者	―	中規模事業者を超える規模			

１０．プライバシーマーク取得までのスケジュール

■コンサルティング概略スケジュール



■プライバシーマーク取得後の審査について

プライバシーマーク取得後 ⇨ 更新審査：２年毎

１１.プライバシーマーク認証取得コンサルスケジュール（ゆったりコース）

■プライバシーマークコンサルスケジュール
（工程ごとのおおまかな実施回数を示す。６時間／回　程度　）

工　　程	1ヶ月目	2ヶ月目	3ヶ月目	4ヶ月目	5ヶ月目	6ヶ月目	7ヶ月目	8ヶ月目	9ヶ月目	10ヶ月目
組織・体制の確立	１回									
基本方針の策定		２回								
リスク分析			２回							
コンプライアンスプログラムの策定				４回						
教育・啓蒙 導入・運用	１回					２回　＋　内部監査員教育　１回				
監　査									１回	

１２.プライバシーマーク認証取得コンサルスケジュール（最短コース）

■プライバシーマークコンサルスケジュール
（工程ごとのおおまかな実施回数を示す。６時間／回　程度　）

工　　程	1ヶ月目	2ヶ月目	3ヶ月目	4ヶ月目	5ヶ月目	6ヶ月目	7ヶ月目	8ヶ月目	9ヶ月目	10ヶ月目
組織・体制の確立	１回									
基本方針の策定	２回									
リスク分析	２回									
個人情報保護マネジメントシステムの策定	４回									
教育・啓蒙 導入・運用	１回		２回　＋　内部監査員教育　１回							
監　査				１回						

＊最短期間で取得する場合は、文書作成を最優先して対応します。

１３．コンサルティング概略内容

■コンサルティング概略内容

ステップ	お 客 様	コンサルティング内容
組織・体制の確立	■PMS策定のための組織を作る ■PMS策定のための作業計画をたてる	■推進体制の指導 ■作業計画作成指導
基本方針作成	■個人情報保護方針（必要に応じてセキュリティポリシー）を定め文書化する ■方針の組織内への周知	■個人情報保護方針、セキュリティポリシーの作成指導
システム構築	■PMSの構成を検討する ■PMSの基本となる規定を策定する ■PMSの詳細規程を策定する ■PMSを文書化する ■PMSに準じた体制の整備を行う ■PMSを周知するための研修を実施する	■PMS文書体系の検討の仕方について指導 ■組織・体制の整備について指導 ■基本規程の作成指導 ■詳細手順の作成指導
現状調査･分析	■個人情報の特定 ■業務フローの作成 ■リスク分析 ■物理的状況調査 ■ギャップ分析	■個人情報の特定の指導 ■業務フローの作成の指導 ■リスク分析の指導 ■物理的状況調査の指導 ■ギャップ分析の指導
社内教育	■PMSを周知するための研修を実施する	■情報セキュリティ教育の実施
内部監査	■PMSの運用状況を監査する ■PMSの改善を実施する	■内部監査実施指導
模擬監査	■受審に備えての模擬審査実施	■模擬審査による指導

１４．プライバシーマーク認定取消しについて

■プライバシーマーク認定取消しについて

消費者からのクレーム等・・・

（財）日本情報処理開発協会又は指定機関

①報告書の提出を求める
②実態調査の実施
③改善勧告
④改善の要請

従わない場合、認定の取消し！

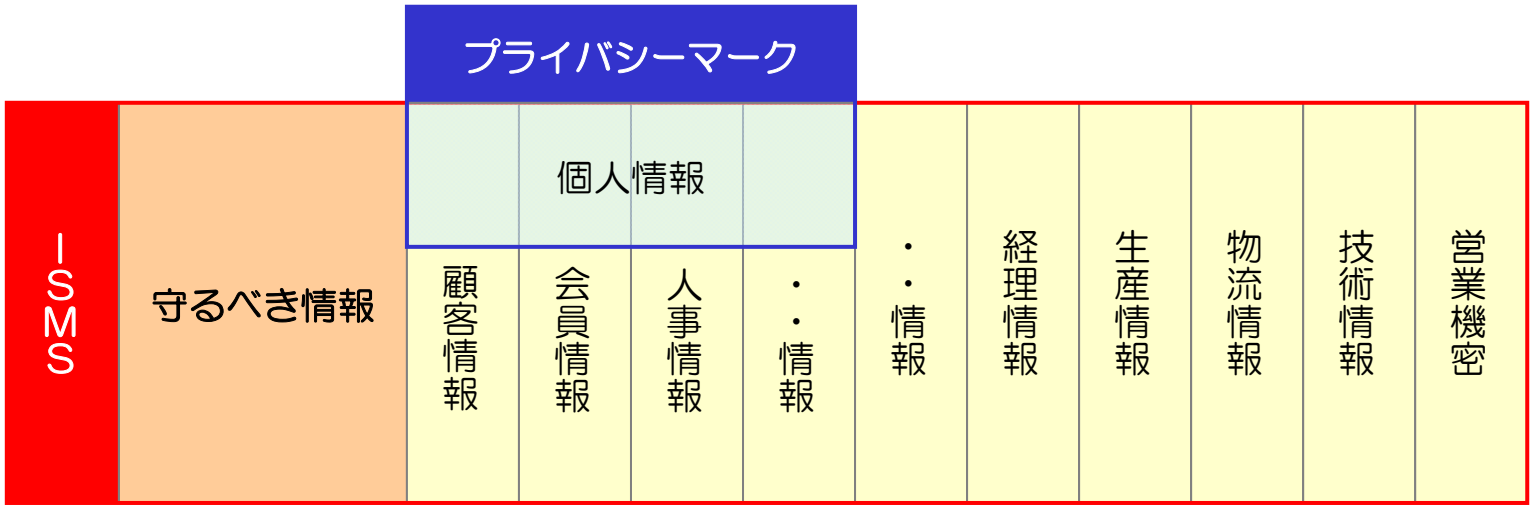
事業者・企業

１５．プライバシーマークの認定制度

■プライバシーマークの第三者機関の認定制度

プライバシーマーク制度 JIS　Q　15001	■企業が保有する個人情報のみの保護 ■ＢｔｏＣが中心 ■コンプライアンス（法令順守）が主目的 →個人情報保護法
ＩSMS適合性評価制度	■情報全体のセキュリティに関わるマネジメントシステム ■ＢｔｏＢが中心 ■企業のリスクマネジメントが主目的

■プライバシーマークとＩSMSの適用範囲の違い



１６．ＩＳＭＳ制度とプライバシーマーク制度の違い

■ＩＳＭＳ制度とプライバシーマーク制度の比較表

項　目	ＩSMS制度	プライバシーマーク制度
規　格	国際規格（ISO27001）に準拠	国内規格（JIS Q 15001）に準拠
適用範囲	組織に応じて適用範囲を決定	全社的な取り組みが基本
保護の対象	組織が保護すべき情報資産を識別し、セキュリティ対策を実施する	組織が取扱う個人情報を特定し、個人情報の保護対策を実施
管理範囲	基本的に、組織の情報資産に対してセキュリティ対策（管理策）を実施	個人情報の保護は、安全管理策を実施するだけでなく、管理する個人情報について情報主体の権利に対応することも含まれている。 情報収集時には事前に利用目的を伝えた上で本人の同意をとる必要があり、収集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。
規格と作成文書	JIS-Q-27001(2006)に従い、組織内のリスク評価に基づいて情報セキュリティマネジメントシステム文書を作成	JIS Q 15001個人情報保護に関する個人情報保護マネジメントシステムの要求事項に従って、事業者が個人情報保護マネジメントシステムを作成。
マネジメント構築のポイント	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	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。
取得にかかる期間	約１０ヵ月	約１０ヵ月
更新期間	維持審査：毎年　更新審査：３年毎	２年間
審査費用	事業規模によりかなり差がある	３００,０００円～１２００,０００円

＊共通点は、組織内のセキュリティ保護のインフラ整備や構成員への教育、（内部）監査、経営者レビューなどがあり、
常にＰＤＣＡのマネジメントサイクルを回せれば、組織にとって有効な活動となります。

１７．プライバシーマーク取得への誤った期待

プライバシーマーク認定をされて、個人情報が完璧に守られる訳ではありません。
個人情報を適切に保護する準備・体制が整ったに過ぎません。
御社で作成した個人情報保護マネジメントシステムを継続的に実行し改善して
いくことが重要です。

個人情報保護マネジメントシステム
を継続的に実行・改善

顧客・取引先の信頼向上

１８．おわりに

■弊社では、プライバシーマーク認定はマネジメントシステムであり、同時に企業経営ツールとしてとらえ、コストパフォーマンスによる身の丈にあったコンサルティングを行っております。

■御社にて構築されたマネジメントシステムが経営ツールとして御社の成長にお役立ちできるよう継続的に種々アドバイスさせていただきたいと考えております。

■弊社のコンサルティングサービスの提案の場を提供いただきお礼申し上げます。ぜひ弊社に御社のコンサルティングサービスをさせていただきたくよろしくお願いいたします。