認証を持っていない会員様への御提案

ISO27001認証
情報セキュリティマネジメントシステム

日本情報セキュリティ推進協会（JISSA）

IOS27001（ISMS）とは？
個別の技術対策のほかに、マネジメントとして組織自らのリスクアセスメントを行い、必要なセキュリティレベルを決定し、プランをもち、資源を分配し、システムを運用する、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システムに対する第三者適合性評価制度です。
企業が扱う個人情報や企業情報は、犯罪や事故などで漏えいした場合、社位的な責任が追及されるとともに、企業の存続にも重大な影響を及ぼす可能性があります。
現代の情報社会において、情報セキュリティマネジメントシステムを構築し、適切に維持していくことが求められています。

日本情報セキュリティ推進協会（JISSA）によるISO27001認証

日本情報振興協同組合（JIA）では、会員及びユーザーの情報セキュリティレベルを向上させるため、日本情報セキュリティ推進協会（JISSA）によるISO27001の団体認証を実施します。
通常、ISOを認証取得する場合、入会費用、運用費用に多大なコストがかかります。
しかし、JISSAの団体認証では、そのコストを最小限に抑え、ISOを取得し維持いたします。

ISO入会費用：50，000円（100名以上の事業所複数の場合は別途相談）
ISO維持費用：12，000円/月額
ISO研修費用：25，000円/人【助成金活用可】（税別）
※助成金活用の場合は一定の要件がございます。

※月1回（4h）×6回の情報セキュリティ研修に参加していただきます。
※毎年1名以上の受講が必要になります。（30名単位で1名追加）

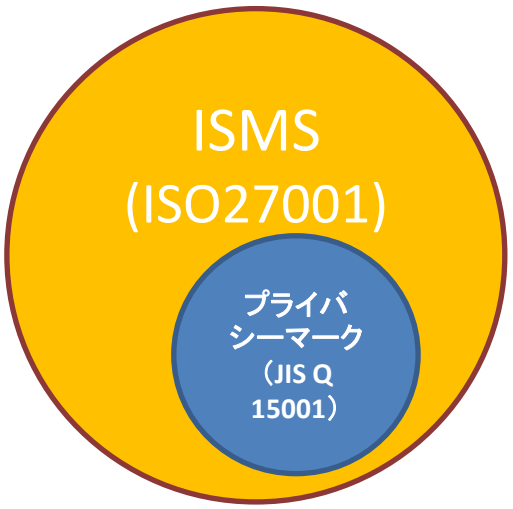
お問い合わせ
JISSA管理センター　株式会社日本マネジメントシステム
〒231-0002　神奈川県横浜市中区海岸通3-9
TEL：045-319-6031　　FAX：045-319-6032
E-mail：info@j-ms.biz

貴社にはPマークよりもISMSが必要ではありませんか？
個人情報保護（プライバシーマーク）と情報セキュリティマネジメント（ISMS）の違い

	Pマーク	ISMS
認定基準	JIS Q 15001（国内のみの基準）	ISO/IEC27001（国際的な基準）
認証単位	全社での取得が原則。	工場・支店や部門単位でも取得が可能。
対象情報	個人情報（顧客、社員情報を含む）のみ。	認証範囲の個人情報を含む重要な情報全て。
ペナルティ	認定の停止、社名を2年間公開。	認証の停止、公開はなし。
審査員	JIPDEC職員（一部例外あり）。	認証機関の審査員。
アプローチ	個人情報の収集（取得）から保管、利用、提供、委託や返却、輸送、破棄などの業務フロー的なアプローチ。	まず適用範囲を定め、その範囲の重要情報を洗い出す、リスクマネジメントのアプローチ。
構築手順	“合理的な安全対策”を要求しているが、審査員のバラツキがあり不明確で、要求がエスカレーション（コスト増加）することがある。	体系的なISO/IEC27001管理策。 もちろん、管理策には個人情報保護の管理も含まれる。 管理策は自社の判断で追加しても良い。
構築費用	会社単位での取得が原則のため会社規模が大きくなれば費用負担が大きい。	適用範囲を絞り込み安価に構築が可能。
審査費用	事業規模の大小に関わらず、30万、60万、120万の3段階であるため、審査費用は安価。	事業規模に応じて審査工数が適用されるため、50名を超えたあたりから割高感がある。
運用費用	2年間に1回の訪問審査。しかし、審査でも指摘は事業上の重要性に関わらず一律に管理策を構築する必要があり、整備するためのコストが必要。	年に1回の訪問審査。また、3年毎に更新審査があるため、毎年継続的に費用が発生する。指摘事項への対応は事業上の重要性に見合った指摘であり、経営コストの悪影響は少ない。
望ましい受審事業者	自社で直接取得する顧客等の個人情報が多い場合。（B to C）	自社で直接取得する個人情報が従業員情報ぐらいであり外部からの情報処理等で預かる個人情報。（B to B）

ISMSとプライバシーマーク図解

ISMSは国際規格（ISO27001）をベースとしているのに対し、プライバシーマークは、個人情報保護法、及びJISQ15001をベースとしています。
プライバシーマークは、個人情報に限定されるのに対し、ISMSは会社が保有する情報全てについての保護とリスク対応を範囲としていますので、下の様な図となります。
※ISMSの認証にプライバシーマークが付いてくると言う意味ではありません。



プライバシーマーク、ISMS費用比較表

新規取得費用比較表（例）

組織規模	プライバシーマーク（サービス業）	ISMS（通常認証）	ISMS（団体認証）
5名未満	308,573	700,000	**150,000**
6名～20名	617,144	700,000	**194,000**
21名～50名	617,144	700,000	**194,000**
51名～100名	617,144	1,000,000	**194,000**
101名～200名	1,234,286	1,500,000	**338,000**

※ISMSは認証機関により個別見積りとなりますので、値引き等がある場合があります。
※ISMSは認証機関により個別見積りとなりますので、一般的な概算費用を記載しております。

維持費用比較表（例）

組織規模	プライバシーマーク（サービス業）	ISMS（通常認証）	ISMS（団体認証）
5名未満	113,143	200,000	**144,000**
6名～20名	231,429	250,000	**144,000**
21名～50名	231,429	250,000	**144,000**
51名～100名	231,429	400,000	**144,000**
101名～200名	462,857	600,000	**288,000**

※プライバシーマークは2年毎の審査となりますので審査費用を2分の1にし1年間の審査費用として記載しております。
※ISMSは認証機関により個別見積りとなりますので、一般的な概算費用を記載しております。
※団体認証には、内部監査等の内部工数が含まれております。
※プライバシーマークは、上記費用かける事業所数が審査費用となります。