ISO27001（ISMS）　ご説明資料
（ISO27001：2013年版）
（JISQ：27001：2014年版）

※ISO27001：情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑに関する国際標準
※ISO：国際標準化機構（International Organization for Standardization ）
　　が策定した国際的な標準（約束ごと）
※ISMS（Information Security Management System：情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ）

株式会社エスケイワード
コンサルティング事業部

POINT 1

ISO27001とは

■ 「重要な情報」を安全に管理するための仕組み
・漏えい、不正アクセス、紛失、利用停止などが、ない
・ＩＳＭＳ（情報セキュリティマネジメントシステム）

◆ 中立的な立場の第三者機関が評価･認証
・審査登録機関（２６機関：2017年11月現在）
・ISO27001（又は、JIS Q 27001）
（2013年10月 ISO27001：2013版 改訂） （2014年 3月 JIS Q 27001 ：2014版 改定）

◆ 認証された企業は、認証ロゴを、使用
・名刺、会社案内、ホームページに掲載
・安全に管理できていることを対外的にアピールする

POINT 2

ISO27001 取得企業数

■ 5，５８２社（2018年6月）（4,435社（2014年1月）参考）
■ 東京都での取得企業は、2，940社 （２018年6月時点）
■ 愛知県での取得企業は、203社 （２018年6月時点）
（Pマークは、15,726社 東京都 8,387社 愛知県 672社 ）

検討 1

PマークとISO27001の違い（参考）

比較項目	Pマーク	ISO27001 （ ISMS）
対象となる情報	「個人情報」	重要な「情報」すべて
取得の単位	全社単位	任意 （部門毎、業務毎も可能）
審査の基準	JIS Q 15001	ISO27001 （又はJIS Q27001）
審査費用（初回）	30、60、120万円	70万円～200万円
更新頻度	2年に一度更新	3年に一度更新審査 1年に一度の部分審査
マーク		

・ISO　27001は、 **「機密性」「完全性」「可用性」**の維持・改善し、重要な情報資産を安全に活用するMS（マネジメントシステム）です。
プライバシーマークは個人情報保護のMSです。（主に**機密性**を重視）

・ ISO　27001とプライバシーマークの共通項目は個人情報の保護の観点のみです。

・ ISO　27001は、受審組織が審査機関を選べますが、プライバシーマークは指定の審査機関となります。

検討 2

ISO27001　認証に伴う、適用範囲　組織体制を決める

プライバシーマークは、全社で認証となりますが、ISO27001の場合は、部門毎の認証も可能です。※ただし、マークの使用は、該当部門のみ
具体的には、本社と、他の支社が分かれているとします。
本社は認証して、他支社は適用範囲外にする。または、本社のシステム部のみ適用範囲とするという事も可能です。
これを決めていただくことにより、審査機関やコンサルタントへの見積依頼が可能となります。
その際に、組織体制を決めていただくことにより、スムーズに構築が進めれるでしょう。対象となる業務、部門の関係者を全て含めることがポイントです。

検討 3

ISO27001　審査機関　選定

地域指定等ある、プライバシーマークの審査機関と違い、国内にあるISO27001の審査対応が可能な　6審査機関より審査機関を選定していただきます。
費用や、審査方法も　審査機関に応じて、相違があります。

検討 4

ISO27001（ISMS）とプライバシーマークの差分

- **情報セキュリティ　基本方針**

プライバシーマークでは、個人情報保護方針にあたる最上位の基本方針となります。

- **情報資産管理台帳**

適用範囲内の情報資産全てを記載した台帳です。
プライバシーマークでは、個人情報一覧表（個人情報管理台帳）にあたります。

- **適用宣言書**

ISO27001　付属書Aにある114の詳細管理策に対して、適用もしくは適用除外を記載します。
（※JISQ：27001：2005年版は133の詳細管理策）

- **リスク管理表**

リスクを特定し、そのリスクの大きさを特定します。（プライバシーマークも一部流用可能です。）

- **事業継続計画規程（BCP）**

災害時やシステム障害時等に速やかに事業を継続出来る為の規程を策定します。

- **セキュリティ　ルールブック（抜粋　簡易版）**

新しいルールを社員様用に判りやすく解説する為のマニュアルです。

POINT

現在の規程、（ISMS等の）を活かして、プライバシーマークを効率よく取得する事が可能です。
エスケイワード では、**運 用 実 績** のあるコンサルタントが、プライバシーマーク構築も考慮してい　ISO27001/ISMSのルール作成のお手伝いを致します。

ISO27001 構築は以下の6ステップで実施いたします。

STEP 1 方針・体制構築/現状分析　（推進チーム構築　業務ヒアリング）

STEP 2 改善策検討　（情報資産洗い出し支援）

STEP 3 文書構築　（マニュアル　作成支援）

STEP 4 教育　（全社員向け実施）/　内部監査　（全部門）

STEP 5 マネジメント・レビュー会議　（経営層による見直し）

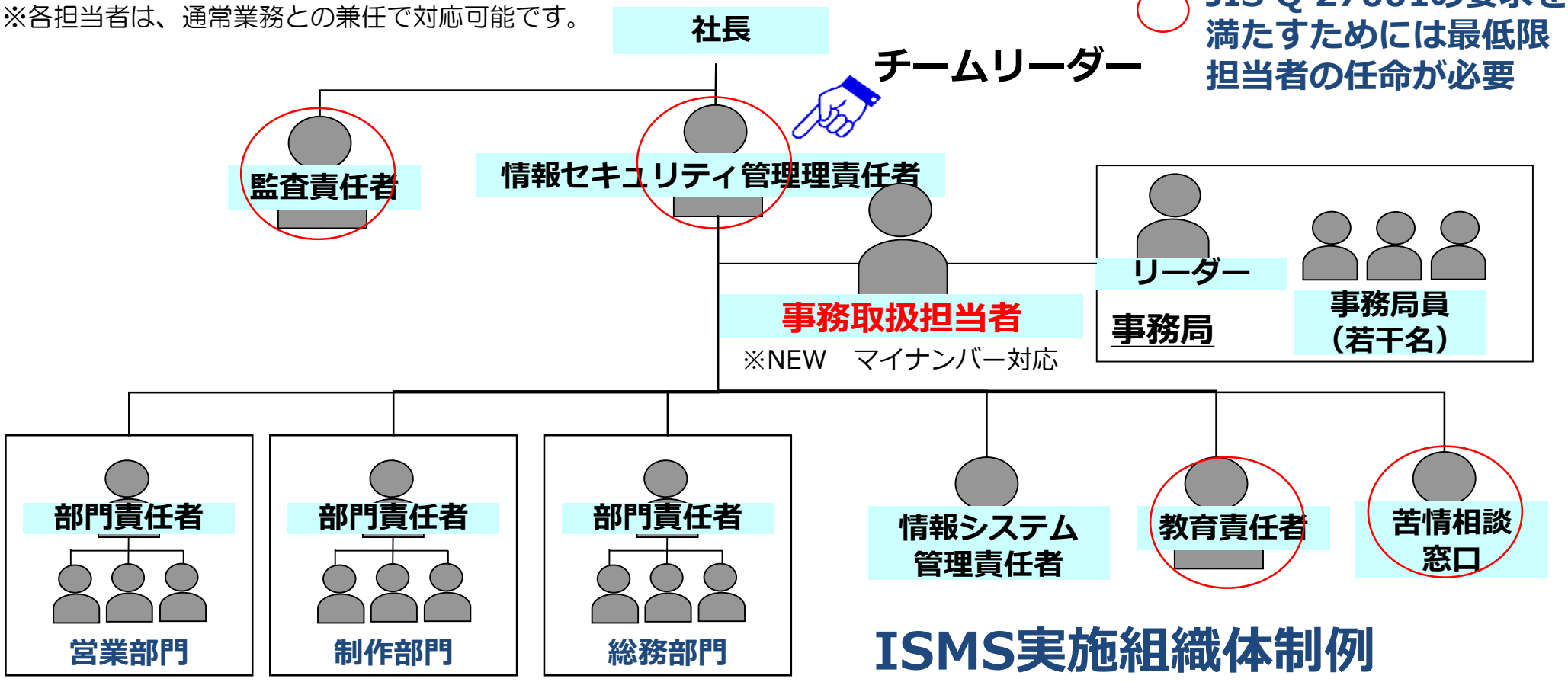
STEP 6 ISO27001申請　/　現地審査レクチャー

STEP 1

方針・体制構築/現状分析　（推進チーム構築　業務ヒアリング）

※各担当者は、通常業務との兼任で対応可能です。

○ JIS Q 27001の要求を満たすためには最低限担当者の任命が必要



ISMS実施組織体制例

POINT

よくある課題として、キックオフまで、時間がかかるケースがありますが、初回ご訪問時までにお客様にて準備していただくことはたったの３つです。①開催日の決定　②キックオフミーティング・業務ヒアリングの為、関係者様への周知③会場の準備　スムーズにキックオフを迎えるよう、資料等も全て準備いたします。

STEP 2

改善策検討　（情報資産洗い出し支援）

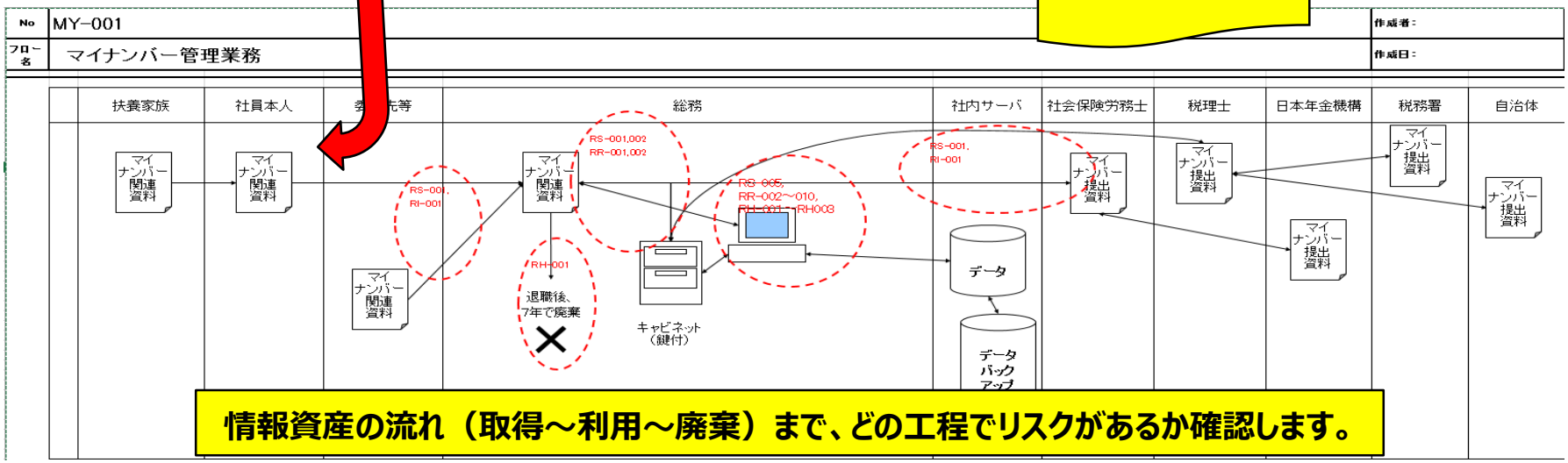
フロー図名	業務名	利用目的	本人へのアクセス※1	機微な個人情報の取扱い	件数	個人情報（データ・書類、種別）	媒体	取得区分※2 直接書面	取得区分※2 それ以外	開示対象※1	第三者提供※1	委託※1	保管場所	保管（利用）期間
													端末	業務終了後、消去ま
FJ-001		Pマーク管理業務のため	○	×	○○件	採用応募者の個人情報の取り扱いについて	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						社員情報の取り扱いについて	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						誓約書	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						サーバ管理者用誓約書	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						入退室管理シート	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						来客管理シート	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
						テスト	紙	●		○	×	×	総務部キャビネット（鍵付）	2年
							紙	●		○	×	×	総務部キャビネット（鍵付）	2年
MY-001	マイナンバー情報管理	マイナンバー情報管理業務のため	○	×	○○件	社員等のマイナンバー（社員と扶養家族の氏名、個人番号）	紙	●	●	○	○	○	総務部キャビネット（鍵付）	退職後7年
						社員等のマイナンバーデータ（社員と扶養家族の氏名、個人番号）	データ	●	●	○	○	○	サーバ	退職後7年
						取引先等のマイナンバー（氏名、個人番号）	紙	●		○	○	×	総務部キャビネット（鍵付）	取引終了後7年
						取引先等のマイナンバーデータ（氏名、個人番号）	データ	●		○	○	×	サーバ	取引終了後7年

情報資産一覧表

情報資産を洗い出し、内容と、件数を記載します。

自社に何件情報があるか把握する為の表です。

データフロー図



情報資産の流れ（取得～利用～廃棄）まで、どの工程でリスクがあるか確認します。

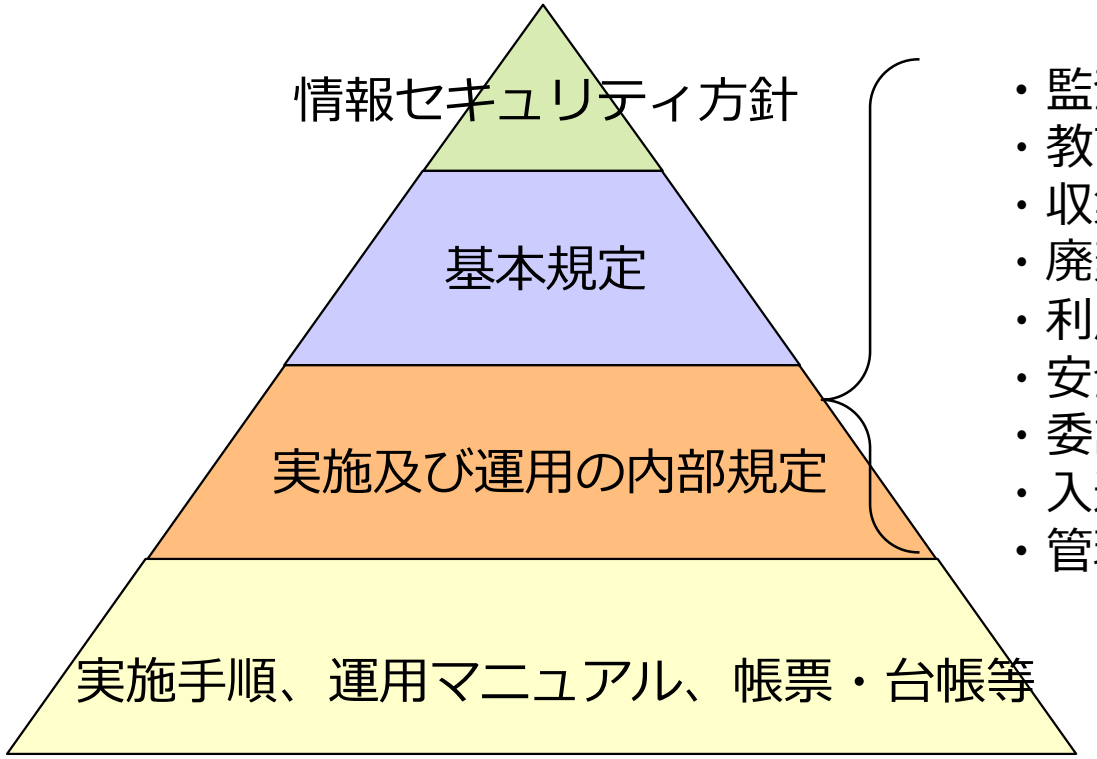
POINT

ルール作りが、全てにおいて、がんじらめな運用に変えてしまったら、通常業務がまわらなくなってしまいます。エスケイワード のコンサルタントは、相反する、安全なルールと確実に運用出来るルールのバランスを取った具体的な実例を基にコンサルティングが可能です。

STEP 3

文書構築　（マニュアル　作成支援）

情報資産の取り扱いルールなど、文書を作成いたします。



- 監査規定
- 教育規定
- 収集の規定
- 廃棄基準
- 利用 / 提供の規定
- 安全管理基準
- 委託先選定基準
- 入退室管理規定
- 管理者・担当者の指名

POINT

よくある課題として、『規程、様式が多くなって管理が大変になった。ルールが形骸化されている。』という声をお聞きします。
エスケイワード がご提供する、規程類は自社でも実施している為、簡素化でスリムで運用しやすい規程と様式となっています。

STEP 4

教育　（全社員向け実施）　/　内部監査　（全部門）

ISO27001で、新たに作成したルールを全社員にコンサルタントが　教育を実施いたします。

ISO27001のルールが
正しく運用出来ているかを
コンサルタントが初回は　立ち合いのもと実施いたします。

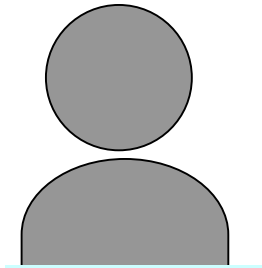
POINT

エスケイワード のコンサルタントは、情報セキュリティセミナーを適宜開催し、情報発信を続けています。IT全般に詳しく、運用実績があるコンサルタントを次ページにてご紹介いたします。 IT系の会社でシステムに関する豊富な経験を積んできたコンサルタントの為、オーバースペックな提案は致しません。

STEP 5

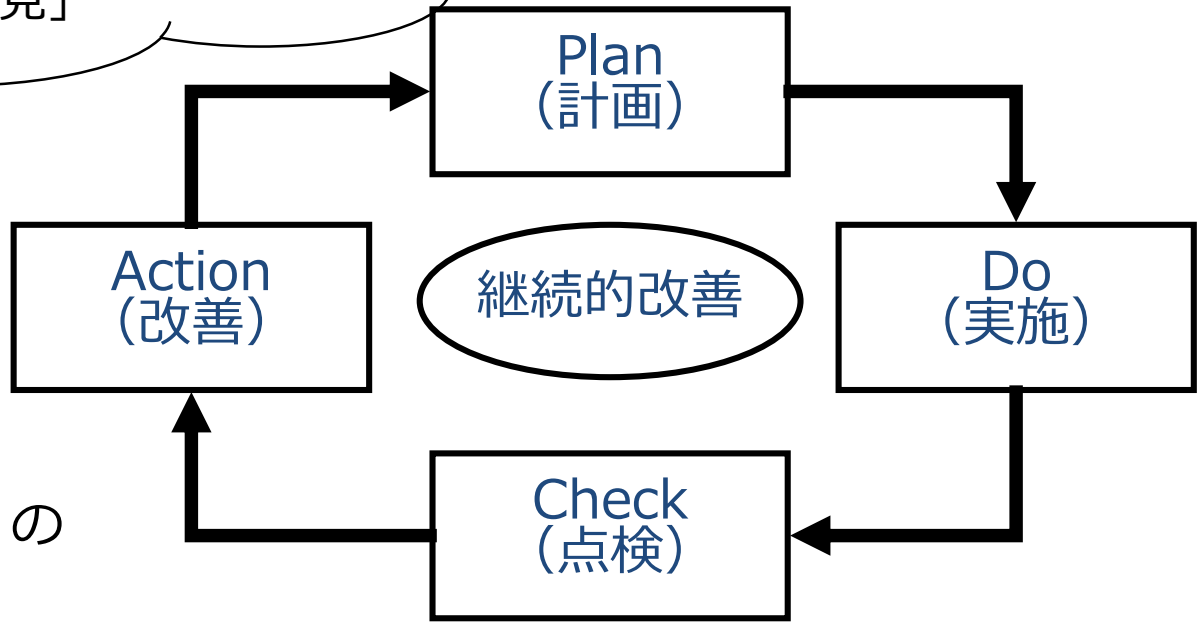
マネジメント・レビュー会議　（経営層による見直し）

「情報保護に関する活動状況」
「情報保護に影響のある社内、
社外の環境変化」
「外部からのクレームや意見」



社長

活動（システム・仕組み）の
見直し（改善）の指示



POINT

今回のISO改定に伴い、経営層の方の関与が重要となりました。エスケイワード では、マネジメントレビューにて、（経営層による見直し）経営に、どうISO27001（情報セキュリティマネジメントシステム）を活かすかの、コンサルティングを行います。

STEP 6

ISO27001申請　/　現地審査レクチャー

審査機関に提出する　規程、書類一式の
作成のサポートをいたします。

当日審査がスムーズに進むように、審査前に
審査対応レクチャー（模擬審査）を実施します。

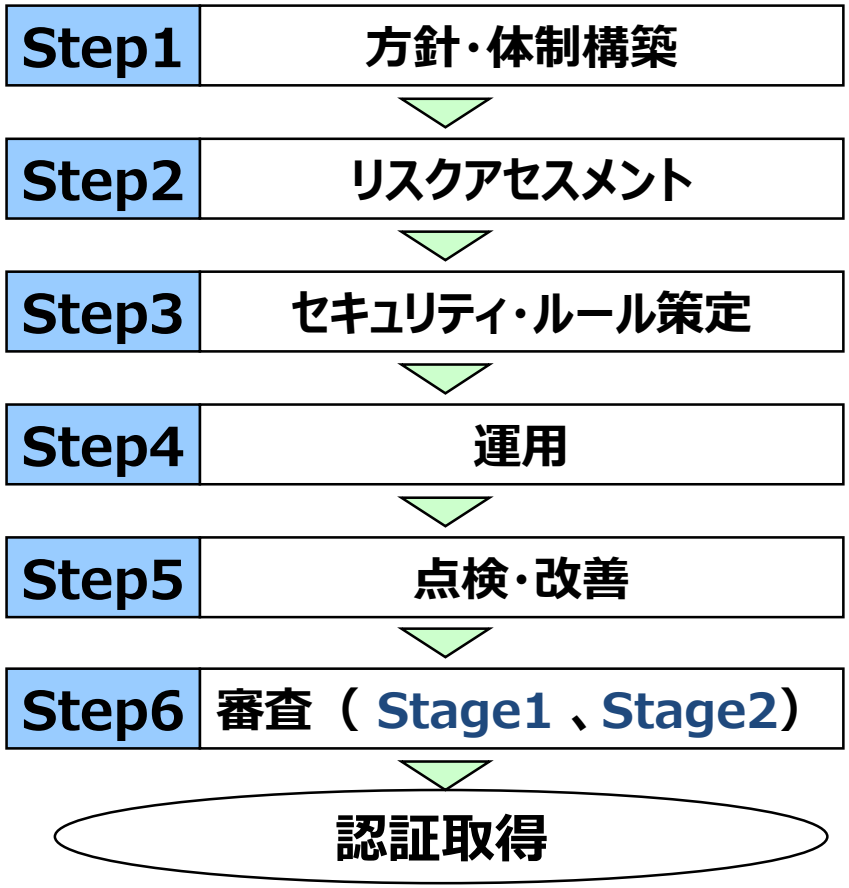
また、審査後のフォローも実施いたします。

POINT

審査機関へ　規程（マニュアル）の提出が、大変ですが、提出前に、訪問し、規定類の提出前に、総点検致します。
また、１次審査　（文書）２次審査　を含めた、初回認証取得まで、フォローを実施致します。

1 取得スケジュール（例）

構築まで、約３ヶ月～ 8ヶ月必要



標準構築期間
平均8ヶ月＋審査期間

※ISMSとプライバシーマークの２つのルールによって、二重 管理にならないように、既存の規程をそのまま流用して、構築を早める事が可能です。

審査（Stage1）：文書審査（構築状況を審査）
審査（Stage2）：実地審査（実施状況を審査）

POINT

構築まで、お客様の予定に応じて、スケジュール案をご提示いたします。
また、認証取得後も、運用実績のあるコンサルタントが、取得後にしっかりと運用ができるように、考慮してサポートを致します。

4 コンサル支援内容

①移行対応メンバーの任命と社内周知
②現行規程類の提示と説明
③業務内容のご説明
④現行の課題、問題点のご提示
⑤事業計画のご提示
⑥当社が作成した規程類等の確認、修正
⑦ISMS周知対象メンバーへの研修
⑧内部監査実施
⑨MR実施
⑩外部審査対応

5 貴社へのご依頼事項

①現在のセキュリティ関連のドキュメント類ご提示
②業務ヒアリングの為の資料ご提示
③新規格対応マニュアル等作成
④周知資料の作成
⑤部門長向け周知と研修
⑥内部監査員 研修
⑦外部審査指摘事項対応
⑧次年度ISMS活動テーマご検討

1 安心のISO27001認定業者　～安心のバックアップ体制～ まずは、お気軽に　お問い合わせください。

当社は、マネジメントシステム評価センターの厳正なる審査により
国際認証規格「ISO27001 (ISMS)情報セキュリティ」の
取扱業者に認定されております。
同認証は下記の要件を満たした業者で、エスケイワードも含まれております。（2018年8月時点）
また、最新規格のISO27001：2013/JISQ27001：2014年版
の移行審査を終えはいち早く審査を終了いたしました。

2 ISO27001／ISMS情報セキュリティマネジメントシステムとは？

ISO27001 /ISMSとは、個別の技術対策の他に、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め、プランを持ち、資源配分を行い、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に対する第三者適合性評価制度です。
※2018年8月時点で　国内で、5,606 組織が認定されています。

株式会社エスケイワード　コンサルティング事業部
サービス・メニュー

①ISMS/ISO27001 ・ プライバシーマーク認定取得支援サービス
②IT-BCP（事業継続計画）診断 ・ 構築支援サービス
③プライバシー保護 ・ 情報セキュリティ体制　「1日診断サービス」
④「スポット」コンサルティングサービス （更新支援、IT診断等）
⑤内部監査・教育研修サービス （定期教育、定期診断）
⑥ 各種セミナー ・ 情報セキュリティ勉強会（開催/講師）

本社　〒461-0001　愛知県名古屋市東区泉一丁目21番27号
泉ファーストスクエア９階
TEL.052-953-7161（代表）　FAX 052-953-7163
東京オフィス　〒100-0013　東京都千代田区霞が関3-7-1 霞が関東急ビル303
TEL. 03-6811-2305

http://www.sk-con.jp/
担当　土本　（ツチモト）　tsuchimoto@sky-inet.ne.jp