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）

ISO27001（ISMS）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：2015年3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

ISMS/ISO27001　認証取得企業の動向

■　全業種のおける認定事業者は、

4,604社（2015年３月）（4,435社（2014年1月）参考）

※参考　ISO9001　約50,190社、　ISO14001　約26,106社
（２０１２年12月時点）

■　東京都での取得企業は、２,４５１社　（２015年3月時点）

■　愛知県での取得企業は、１７９社　（２015年3月時点）

（Pマークは、13,945社
東京都　7,275社
愛知県　577社 ）

情報セキュリティとは

- 重要だと考える「情報資産」
- 「機密性」「完全性」「可用性」の維持・改善

ISMSでは
機密性、
完全性、
加用性、
をトータル
的に
判断する

機密性＝漏えいを防ぐこと

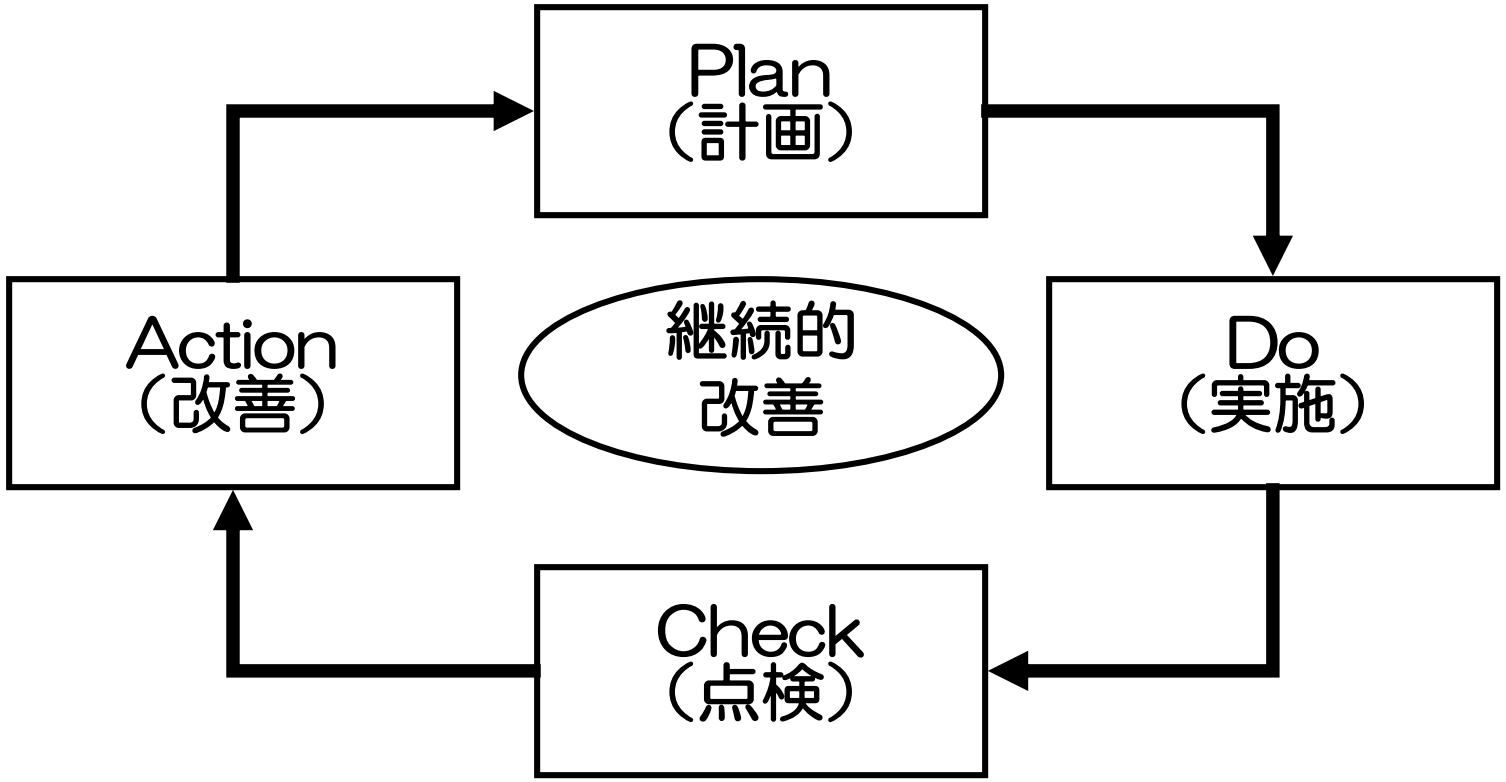
プライバシー
マークで
重視される
POINT

完全性＝改ざんや破壊を防ぐこと

可用性＝必要なときに利用できること

情報セキュリティマネジメントシステムとは

PDCAサイクルを回すことで、情報セキュリティ対策の継続的な改善を図るための仕組み。



認証までの流れ･期間

認証取得まで、約１０ヶ月必要

標準構築期間
平均10ヶ月

※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）

SKword

認証までの流れ･期間

Step 1	方針・体制構築
	ISOの認証取得の範囲を決めると共に、活動メンバーと役割分担を決め認証取得のための推進体制を作ります。また、「情報セキュリティ基本方針」を作成し、全社員向けに取得活動の開始宣言を行うことで、正式に取得活動をスタートさせます。
Step 2	リスクアセスメント
	認証取得範囲に存在する重要な情報資産を洗い出し、その取り扱い状況から漏えい・紛失などの脅威の有無と発生の際の影響を分析します。また分析結果を踏まえ必要な対策を検討します。
Step 3	セキュリティ・ルール策定
	検討結果を踏まえ自社で実施すべき対策を、セキュリティ・ルールとして策定し文書化します。

認証までの流れ･期間

Step 4	運用
	文書化したセキュリティ・ルールを、関係する従業員に教育し、新しいルールに基づいた業務遂行を開始します。 その後、1ヶ月程度試行運用します。
Step 5	点検・改善
	試行運用の状況について内部監査及びマネジメント・レビューを行い、発見された不具合を改善します。
Step 6	審査（ Stage1 、 Stage2）
	審査スケジュールを確定し、審査（Stage1、Stage2）に望みます。それぞれの審査での指摘に対する是正計画を報告し、 審査（Stage2）での指摘に対する是正計画が認められれば晴れて認証取得となります。

ISO　27001　とプライバシーマークの違い

- 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。
- **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。

プライバシーマークに無く、ISMSに必要な規程、マニュアル

■ 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、個人情報管理台帳にあたります。

■ 適用宣言書

ISO27001　付属書Aにある115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（プライバシーマーク用を一部流用可能）

リスクを特定し、そのリスクの大きさを特定します。

■ 事業継続計画規程

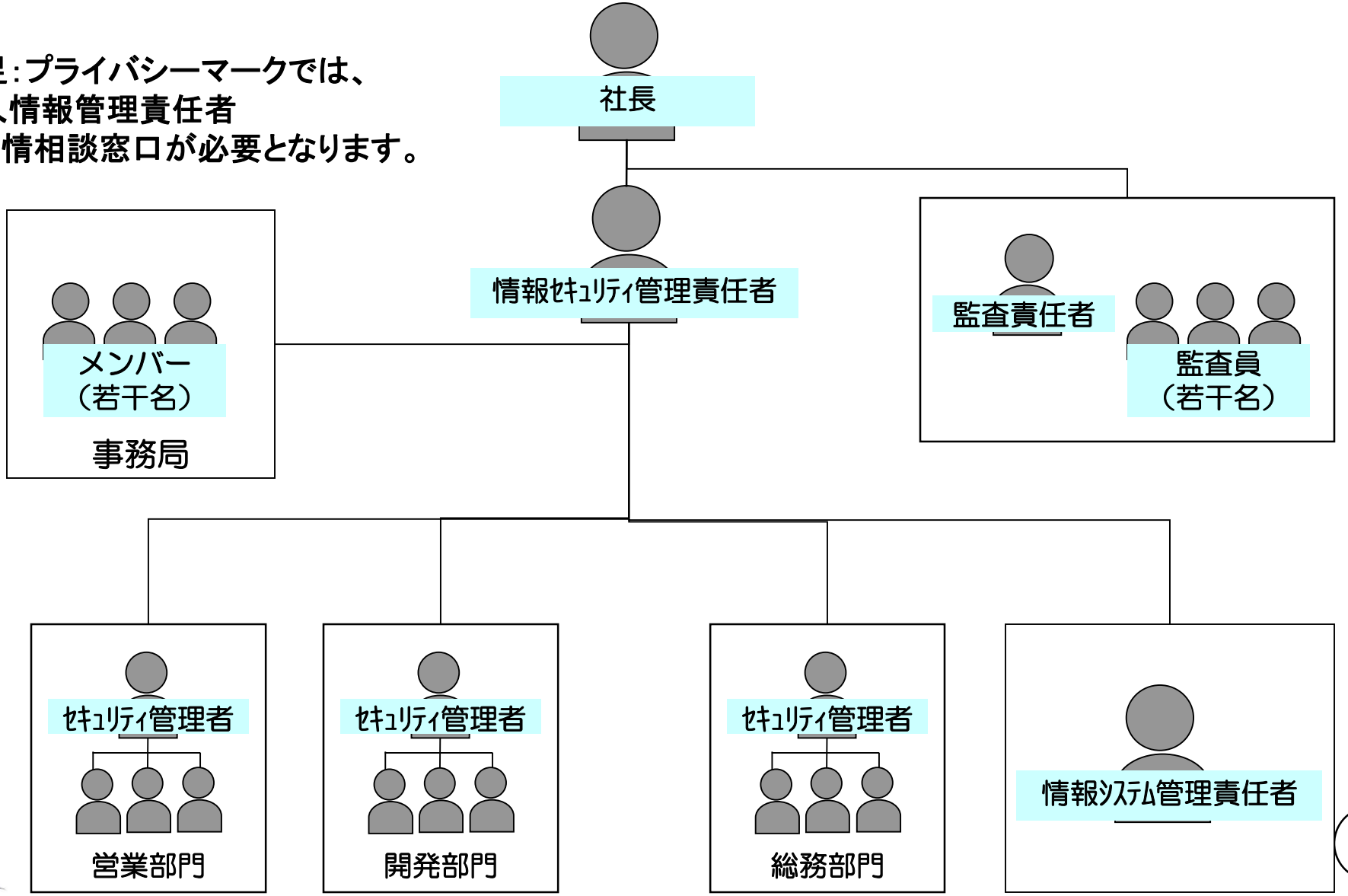
災害時やシステム障害時等に速やかに事業を継続出来る為の規程を策定します。

■ 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。

取得推進組織(例)

補足:プライバシーマークでは、
個人情報管理責任者
と苦情相談窓口が必要となります。



認証取得に必要な費用は

審査登録機関審査料	：５０～２００万円（※１）
登録料	：１５～２０万円
コンサルティング費用（※２）	：１５０～２５０万円
新規設備投資等	：α万円～
合計	：２１５万円～

※１：拠点数、従業員数及び審査登録機関により異なります。
※２：価格は、企業規模及びコンサルティング会社により異なります。
※３：その他：その他、認証取得後には、毎年：定期審査料が、３年毎に更新審査費用が必要となります

取得にあたって、まず必要なことは

■ 適用範囲（認証取得の対象範囲）の決定

- 対象となる業務、部門（事業所、支店）などを決定します。
- 対象は、原則自由に設定できます。

※ただし、マークの使用は、該当部門のみ

■ 取得推進体制の構築

- 取得推進に当たるメンバーを決定します。
- 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。

ISO27001を取得した場合のメリットは？（社外）

- 情報セキュリティ全般に対する取組みをアピールしやすい、納得してもらいやすい
- 営業面での他社との差別化を図りやすい
- 新規の取引先の開拓につながった
- しっかりした会社との企業イメージの向上につながった
- クライアント企業から情報セキュリティに関する相談を受けるようになった
- 新聞、雑誌等に取り上げられることによる広報効果
  etc

当社ｺﾝｻﾙﾃｨﾝｸﾞ・ｻｰﾋﾞｽの特徴

■2013年版　改定版　対応　プログラムがあります。

2013年改定版の対応も可能です。弊社自身が、ISO27001に移行作業を実施しています。今ある規程をそのまま活用して、 無理なく取得出来る支援カリキュラムがあります。

■　シンプルな仕組みづくり。余分な文書、様式は作りません。

ISO取得で陥りやすい罠のひとつに、手続きや文書の過多があげられます。私どもは、業務への影響を最小限に考えたシンプルな仕組みづくりを提案します。また、文書および様式は運用実績に基づくすっきりした体系の雛型をご用意。フルサポートコースでは文書作成の代行も行い、文書作成に多くの時間を割くこともありません。

当社ｺﾝｻﾙﾃｨﾝｸﾞ・ｻｰﾋﾞｽの特徴

■ コンサルタントが親身のご指導をいたします。

貴社をご担当するコンサルタントは、ISO27001審査員の資格のある専任コンサルタントです。ありがちな一律な指導ではなく、柔軟な対応で貴社に適した体制を構築します。もちろん、認証取得に至るまで親身のご支援をいたします。

■ 情報セキュリティ技術にも強い。

人的資源に限りのある中小企業では、技術的なセキュリティ対策に弱点を抱える企業も少なくありません。当社では、セキュリティ技術（ネットワーク、サーバー構築等）の専門スタッフがこうしたご相談にお応えし、コストを考慮した最適なご提案もさせていただいています。

ISO　27001：2013版　対応計画

ISO 27001	2013.10	2014.4	2014.8	2014.9	2014.10	2015.8	2015.9	2015.10	
2005版								2005版廃止	
2013版		△ JIS版							
2014年までの以降審査例				△ **移行審査**	審査会				
2015年までの以降審査例			△審査	審査会		△ **移行審査**	審査会		

移行に関しては、規格発行から2年以内に移行を完了する必要があります。（現時点のJIPDECからの指示です）規格が発行されたのが、2013年10月1日ですので、2015年9月30日までに認証決定会議をする必要があります。よって審査は2015年8月31日には終了することが要求される予定です。

ISO27001：2013　改訂支援計画
～フルサポート・コース～

　既にＩＳＯ27001は取得しているが、移行に関する支援のコンサルを依頼したい！また、「とにかく工数をかけずに取得したい」というニーズにお応えするためのコースです。業務多忙で、レクチャー後の課題の消化に時間を割けるか不安がある、少しでも短期間で取得したいといった企業に最適です。 工数の掛かる規程（書類）作成や、業務フロー図の作成、教育実施をコンサルタントが肩代わりすることで、効率的に改訂を目指します。

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		

（株）エスケイワード
コンサルティング事業部のご紹介

□　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情報セキュリティ勉強会、各種セミナー（開催/講師）

HEAD OFFICE 〒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）

TOKYO OFFICE 〒106-0047 東京都港区南麻布2-10-13 OJ HOUSE 202
TEL. 03-6267-7066

http://www.sk-con.jp/

担当　土本　（ツチモト）

SKword