ISMS団体認証のご提案

日本情報セキュリティ推進協会（ＪＩＳＳＡ）
株式会社日本マネジメントシステム
〒231-0002 横浜市中区海岸通3-9 横浜ビル６F
TEL 045-319-6031 FAX 045-319-6032

アジェンダ

1.ご提案の概要
2.日本情報セキュリティ推進協会について
3.日本マネジメントシステムについて
4.ISO規格について
5.ISMSについて
6.ISMS団体認証について
7.Q&A

ご提案の概要

パソコン、スマートフォン、タブレットなど情報機器のなしでは、仕事が進まない現代社会において情報セキュリティは企業にとって必須の課題と言えます。
サイバーテロ、標的型攻撃など、ニュースや話題となる事象だけでなく、情報セキュリティにおいては、自社の仕組みの構築が重要な要素のひとつといえます。

もちろん、様々なセキュリティ製品を導入し、ネットワークや端末を保護してゆくことは必要なことですが、俯瞰的に何がどの程度重要で、情報セキュリティの観点から、どの情報に対し、どの程度のセキュリティ対策を実施するか？という全体的な戦略がなくては、有効な情報セキュリティ対策になりえません。

高額な製品を購入し、セキュリティ対策を行っている企業を良く見ますが、それはウィルス感染や標的型攻撃などの事象に対した対策であり、俯瞰的な戦略なくして製品を購入することは、もぐらたたき状態と言えます。

まずは、自社がどの様な情報を保有しており、その情報が「機密性」「完全性」「可用性」の観点からどの程度重要で、どの程度のセキュリティ対策を講ずるべきかを検証することが重要です。

そのひとつの指標として、ISMS認証取得を目指されてはいかがでしょうか？

ご提案の概要

情報セキュリティの重要性も理解しているし、ISMSもできることなら取得したい、、、
しかし、ヒト・モノ・金など社内のリソースが潤沢でなく、難しいとお考えの企業様も多いと思います。

その様な、企業様の悩みにお応えするべく、ISMS団体認証の制度は設計されました。
そして、2016年1月27日、
資本関係を持たない任意の組織としては、日本で初めて
JISSA（日本情報セキュリティ推進協会）32社が同時に認証取得いたしました。

現在は、およそ100社がISMS団体認証により、ISMSの認証受け情報セキュリティ対策を行っています。

5

協会概要

団体名	日本情報セキュリティ推進協会
公式ＨＰ	https://www.jissa.info/
所在地	〒062-0933 北海道札幌市豊平区平岸3条8丁目6-1 信和リッチ405
お問合せ先	JISSA情報セキュリティ管理センター（横浜） 〒231-0002 神奈川県横浜市中区海岸通3-9 横濱ビル6F 株式会社日本マネジメントシステム

7

事業概要

情報セキュリティ関連事業：
情報セキュリティコンサルティング、情報セキュリティ対策実装

IT関連事業：
ITシステム企画開発、ITコンサルティング

ISO関連事業：
ISO認証取得コンサルティング、ISO事務局代行、ISO関連セミナー開催

情報セキュリティ関連事業

サイバーセキュリティアセスメント及び対策、ISMS認証コンサルティング、CSIRT構築コンサルティング、セキュリティ監視、脆弱性診断／ペネトレーションテスト、フォレンジック、セキュリティ製品導入等をご支援いたします。

研修事業

情報セキュリティ関連を中心に研修コースを開催しております。
また、ISOに関する研修コース（ISO27001入門コース、IRCA認定ISMSファンデーションコース、IRCA認定ISMS内部監査員トレーニングコース等）、技術研修コース（JAVA、PHP等）もご用意させていただいております。

ＩＴ関連事業

ITシステム導入をコンサルティングからシステム企画、開発（カスタマイズ）、オペレーションの最適化までをワンストップで行います。

ＩＳＯ関連事業

ISO27001（ISMS）、ISO2000（ITSMS）、ISO9001（QMS）、ISO14001（EMS）等のISO認証取得、維持のご支援いたします。

会社概要

会　社　名	株式会社日本マネジメントシステム
代表取締役	橋口　謙
設　　立	2010年9月17日
資　本　金	10,000,000円
所　在　地	〒231-0002 神奈川県横浜市中区海岸通3-9　横浜ビル6F

情報セキュリティアセスメント

ISO27001,27002,COBIT,NIST,PCIDSS等の規格、ガイドラインなどをベースに情報セキュリティ対策状況を分析し、対策ロードマップを作成いたします。

セキュリティ製品導入

多くの企業がセキュリティ製品導入を俯瞰的且つ計画的に行うことが出来ていません。また、折角導入した製品を十分に活用しきれていない企業も多く見受けられます。
弊社はセキュリティのプロとして全体的なセキュリティの最適化を前提に製品導入をご支援いたします。

CSIRT構築支援

CSIRTガイドラインとして、NIST SP800-61「コンピュータセキュリティインシデント対応ガイド」ベースに「文書整備」「インシデント対応チームの構成」「インシデント対応の準備」「予防」「検知と分析」「封じ込め・根絶・復旧・事後活動」6分野を中心に構築いたします。

セキュリティ対策要員派遣

セキュリティ対策には専門的知識をもった人材が必要です。私どもでは、情報セキュリティ対策に必要な様々なスキルを持った人材を派遣することが可能です。

ISMS認証取得支援

私どもは、ISO27001（ISMS）認証をセキュリティ対策の結果のひとつと考えています。サイバーセキュリティを含む様々な対策のひとつの形として、ISO27001（ISMS）の認証取得ということがあるべき姿との考えに基づきご支援しております。

脆弱性診断 ペネトレーションテスト

システムを構成するサーバやファイヤー　ウォール等のネットワーク機器に対して、OSやア　プリケーションに潜むセキュリティホールが存在しないかどうかをネットワーク経由にて診断し、対応策を提示します。ＷＥＢアプリケーションについても擬似攻撃により脆弱性を診断いたします。

標的型メール攻撃訓練

実際に標的型攻撃の現場で対策を行っていた攻撃手法を熟知したエンジニアから擬似的な（無害な）標的型攻撃の侵入を実施させていただき、侵入を軽減させるためのご支援をさせていただきます。

情報セキュリティ研修

IRCA認定ISMSトレーニングコースをはじめとして、様々な情報セキュリティ研修をご用意しております。
詳細は、別資料をご参照ください。

セキュリティエンジニア入門コース（2日間）
一般ユーザ/非IT部門担当者/未経験技術者

セキュリティエンジニアスキルアップコース（3日間）
中級エンジニア向け

セキュリティエンジニア上級コース（3日間）
上級エンジニア向け

事故事例から学ぶ情報セキュリティ（eラーニング）

カスタマイズコース
ご要望に応じた内容での教育を行います

技術者育成コース
JAVA、PHP、ネットワーク、サーバ等

ISMS入門コース（１日間）
ISO27001認証取得について学ぶエントリーコース

IRCA認定
ISMSファンデーションコース（eラーニング）

IRCA認定
ISMS内部監査員トレーニングコース（eラーニング＋１日間）

ISMS主任審査員・審査員トレーニングコース（eラーニング＋3日間）

SOC/CSIRT 入門コース（1日間）
CSIRTについて学ぶエントリーコース

SOC/CSIRT トレーニングコース（3日間）
CSIRT構築～運用を実施するための担当者向け

ISO規格とは

ISO規格：国際規格
ISOが開発した国際的な規格。(基準、記号など様々なものを標準化)
加盟国は、ISO規格を採用する必要がある。

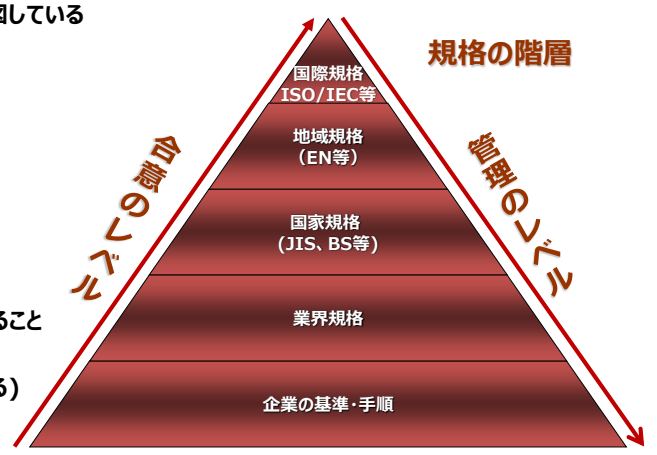
Bsiジャパン資料より

13

ISO規格(国際規格)の位置づけ

より多くの組織が活用できることを意図している

限定された対象が具体的に活用できること
を意図している
(より具体的な現実内容を示している)

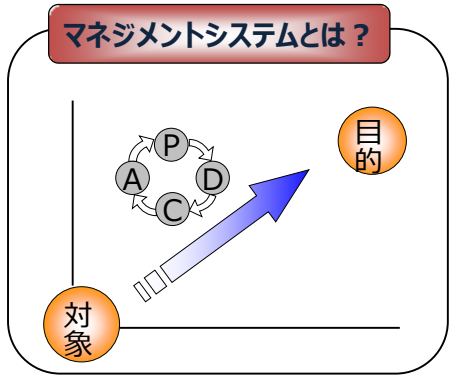


Bsiジャパン資料より

14

ISOマネジメントシステム規格とは

ISOが開発したマネジメントシステム(管理の仕組み)に関する規格



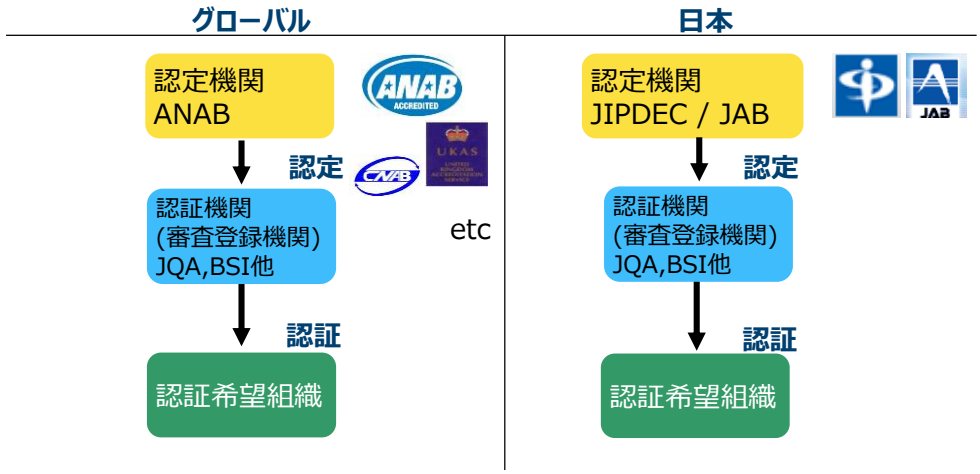
組織の諸活動を目的に導くための仕組み

例：
品質マネジメントシステム
環境マネジメントシステム
情報セキュリティマネジメントシステム

Bsiジャパン資料より

15

ISOの認定・認証制度



16

世界の主な認定機関

SCC (Canada)
ANAB (USA)
EMA (Mexico)
INMETRO (Brazil)
RvA* (Netherlands)
UKAS* (UK)
KAB (Korea)
HKCAS (Hong Kong)
JAB (Japan)
ENAC (Spain)
SAC (Singapore)
TAF (Taiwan)
CNAB (China)
NABCB (India)
JAS-ANZ (Australia)
IATF – Automotive
itSMF
IT Service Management
JIPDEC (Japan)
ISMS & ITSMS
SAI
Social Accountability
TGA / VDA (Germany)
Automotive

17

認証とは

日本では、1991年の品質分野におけるISO9001の認証が第一号です。当時、国際的に活動していたNACCB（UK／後のUKAS）、RAB （USA／後のANAB）、RVC（オランダ）、JAS-ANZ（オセアニア）が認定機関としてありましたが、日本にはまだ認定機関が存在しませんでした。

ここ数年の国際的な認証の動向は、先進国内の内需の減少と新興国（特殊な政治介入が有る中国は除く）の外資系の認証の増加であり、新興国での国際的な知名度を有する認証の優位性が鮮明に表れています。

日本国内の認証は閉鎖的ですが、認証の価値は、如何に多くの方から認められているかによって決まります。

業界団体認証は、アジア、オセアニアに強いJAS-ANZの認定を有する認証機関を今回パートナーとして選びました。

勿論、海外事業所を持つ組織を視野に入れての事です。

ISO認証の流れ

◆取得範囲を決定する
取得範囲の定め方により、ISO構築の期間、マニュアルの内容などが異なる。構築をスタートさせた後、取得範囲を変更することのないよう、最初に明確にしておくこと。

◆キックオフ宣言
全従業員に対し、経営者は「ISOを取得する」ことを宣言する。
※ISOでは、ひとりひとりの「責任」と「権限」を重視するが、中でも経営者は、最も大きな責任と権限を持つことが求められる。キックオフ宣言は、経営者自身及び全従業員に、その意識を持たせるための大切な儀式である。

◆ISO構築の中心となる担当者を決める
品質管理責任者、事務局、部署メンバーを選定する。
※品質管理責任者は、取締役もしくは同程度の役職より任命されるのが一般的。
※実際にISOシステムを構築し、マニュアルを作る作業は、事務局が中心となる。

◆ISOの知識を身につける
社内の勉強会、研修等を開催し、ISO規格の解釈について学ぶ。

◆業務の見直し
現状の業務手順（製品の流れ、作業手順）について各部署にヒアリングを行い、業務の流れを整理する。

◆社内文書の確認
社内の規定類・文書のフォームや管理方法を確認する。

◆管理側面を明確に
前ステップの結果を踏まえ、管理すべき側面を明確にする。
※業務のすべてを管理するのではなく、『管理すべきポイント』を決めていく。
◆ISO9001では：プロセスアプローチ分析を行う。
◆ISO14001では：環境影響評価を行う。
◆ISO22000では：ハザード評価を行う。管理手段（オペレーションPRPかCCPか）を決定。
◆OHSAS18001では：リスク評価を行う

◆目標管理
管理すべき項目の中から、達成すべきテーマを選び、誰が、何を、いつ、どのように行う、といった具体的な内容を決定する。

◆マニュアル案を完成
手順書や帳票類の見直しおよび作成を行い、マネジメントシステムを構築し、マニュアルを完成させる。

◆各手順、対策を決める
・不適合製品の管理を決める
・是正処置の対象と処置手順を決める
・回収の手順を決める（ISO22000）

◆マニュアルを運用
マニュアルができたら、それを運用する。数ヶ月「試運転」してみて、そのマニュアルが使いやすいものであるかを確認する。

◆内部監査員教育
自社内で『内部監査員』を選び、育成を行う。

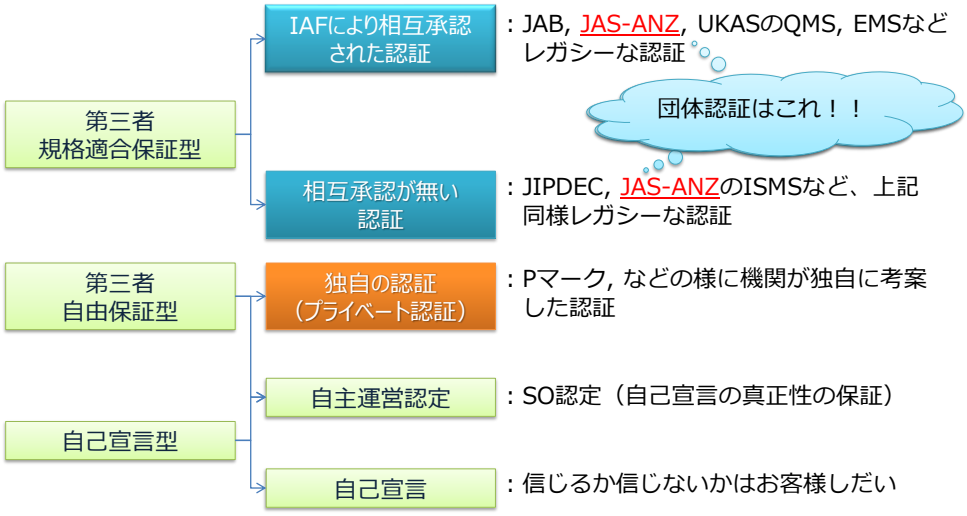
◆教育訓練
ISOマニュアルで規定した内容を遵守できるよう、社員に対して教育を行っていく。
※一人一人が、「自分がすべきこと」を自覚できるような教育を行うことが大切。

◆マネジメントレビューを行う
改善の必要性と機会を考慮しながら、常に管理手段を確認し、効率的・効果的な改善を行っていく。

◆マネジメントシステムを更新する
更新したら効果を確認し、効果がある場合は文書を改定し根付かせるようにする。

認証とは

認証又はそれに相当する証明の体系とその特徴を記します。



ISO/IEC 27001（ISMS）とは？

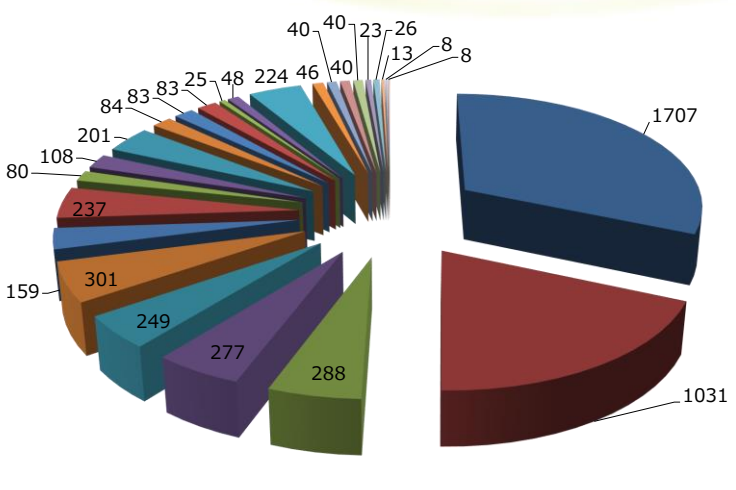
近年、IT化の進展に伴い、不正アクセスやコンピュータウイルスによる被害、及び内部不正者や外注業者による情報漏えい事件など、情報資産を脅かす要因が著しく増加しており、これらの脅威に対して適切にリスクアセスメントを実施して、企業における総合的な情報セキュリティを確保するためには、ISMSの構築・運用が必須事項となっています。

ISMSとは、個別の問題毎の技術対策の他に、組織のマネジメントとして、リスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することです。
ISMSが、達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性をバランス良く維持・改善し、**リスクを適切に管理**しているという信頼を利害関係者に与えることにあります。
そのためには、ISMSを、組織のプロセス及びマネジメント構造全体の一部とし、かつ、その中に組み込むことが重要です。

ISMSの認証とは、上記ISMSをISO/IEC27001の国際規格に基づき構築し、認証機関の審査を受け適合性が証明されることを言います。

主なISO27001認証件数（JIPDEC公開資料より）

総件数 5496件



- BSI-J
- JQA
- JICOA
- JUSE-ISO Center
- JACO
- SGS
- BVサーティフイケーション
- ＡＳＲ
- ＤＮＶ
- ＪＭＡＱＡ
- ＭＳＡ
- ＩＣＭＳ
- ＪＳＡ
- ＰＪＲＪ
- ＴＵＶ　ＲＪ
- DQS JAPAN
- ＩＳＡ
- ＵＬ　ＤＱＳ
- ＬＲＱＡ　ＪＡＰＡＮ
- ＪＡＴＥ
- ＢＬ－ＱＥ
- ＢＳＫ
- Ｊ－ＶＡＣ
- ＮＫＫＫＱＡ
- ＪＣＱＡ
- ＪＥＴ

23

どのようにするとISMSの認証取得ができるか？

- ISO/IEC27001規格要求事項すべて網羅し、準拠した組織の仕組みを整備し、実施する。

JIS

情報技術－セキュリティ技術－
情報セキュリティマネジメントシステ
要求事項

JIS Q 27001：2014
（ISO/IEC 27001：2013）
（JSA）

平成 26 年 3 月 20 日 改正
日本工業標準調査会 審議
（日本規格協会 発行）

目 次

ページ

24

ISMSの構築のポイント- 構築ステップ

1. 適用範囲の決定
2. ISMS基本方針の策定
3. リスクアセスメントの実施、適用宣言書の作成
4. ISMSの文書化
5. フレームワークの確立(PDCA)
6. セキュリティ対応計画の策定・実施
7. 導入教育
8. 内部監査制度の確立
9. マネジメントレビュー・是正処置の仕組み確立
10. 審査（ＳＴ１、ＳＴ２）

25

ＩＳＭＳ団体認証とは

1. ＩＳＭＳ団体認証とは、業界団体として会員企業の情報セキュリティの状況を定期的に監査、監視する仕組みがISO/IEC27001(ISMS)に適合していることを認証したものです。
2. ＩＳＭＳ団体認証の認証プロセスは、例えば大企業グループ（大規模な組織）の認証と同じと考えてください。傘下の企業を同種組織として認証範囲に含むことも多く有り、考え方は良く似ています。
3. 業界団体が、情報セキュリティついて一つの組織としてマネジメントプロセスを共有していること。同業種団体ならではの共通の情報セキュリティに関する課題とリスク／機会に関する統制が必要です。
   ※弊社日本マネジメントシステムがご支援いたします。
4. ＩＳＭＳ団体認証は正式な国際的に通用するJAS-ANZが認定した通常の認証プロセスです。適合性の認証に対する社会的信頼性は、JABやJIPDECと同格です。
5. ＩＳＭＳ団体認証は、通常各個別の会社で負担する認証維持費用（審査費用、設備・ソリューション費用、情報セキュリティ対策にかかわる人件費）を基本的な仕組みとして業界団体が提供し、その費用を会員企業で負担する形式であるため、一会員あたりの費用負担が大幅に安価です。

27

ＩＳＭＳ団体認証のメリット･デメリット（会員企業）

メリット

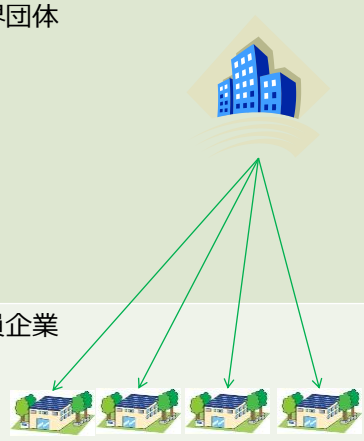
1. 大手取引や行政の入札などの情報セキュリティに関する取引条件クリア(実績あり)
2. 取引先や顧客等における安心感
3. セキュリティに関するリスク低減（基本的な対策は団体として支援）
   1. リスク管理一元化（監視やハイスペックなエンドポイント製品の共同導入なども可）
   2. 基本的な情報セキュリティ対策サポート
   3. インシデント対応のノウハウ
4. 保険適用端末については、セキュリティ保険を適用（オプション：別費用）

デメリット

1. ISMS認証のための業務負荷（個別認証よりは少ない）
2. 団体加入に関する会費等

28

ＩＳＭＳ団体認証のタスクと役割

	タスク
業界団体 	1. ISMSの仕組み構築 ・情報セキュリティ基本方針制定 ・共通の規定制定 2. 規定、記録の雛形提供 3. 内部監査指導（教育、実施） 4. 情報セキュリティ教育の提供 5. 情報セキュリティ監視（オプション：別費用） 6. セキュリティ事故対応支援 7. 情報セキュリティ保険の提供（オプション：別費用）
会員企業	1. 窓口設定 2. 内部監査実施 3. 定期審査の受審 4. 所定の報告事項報告 5. 会費の支払い

※業界団体のタスクは、すべて弊社日本マネジメントシステムが請け負います。

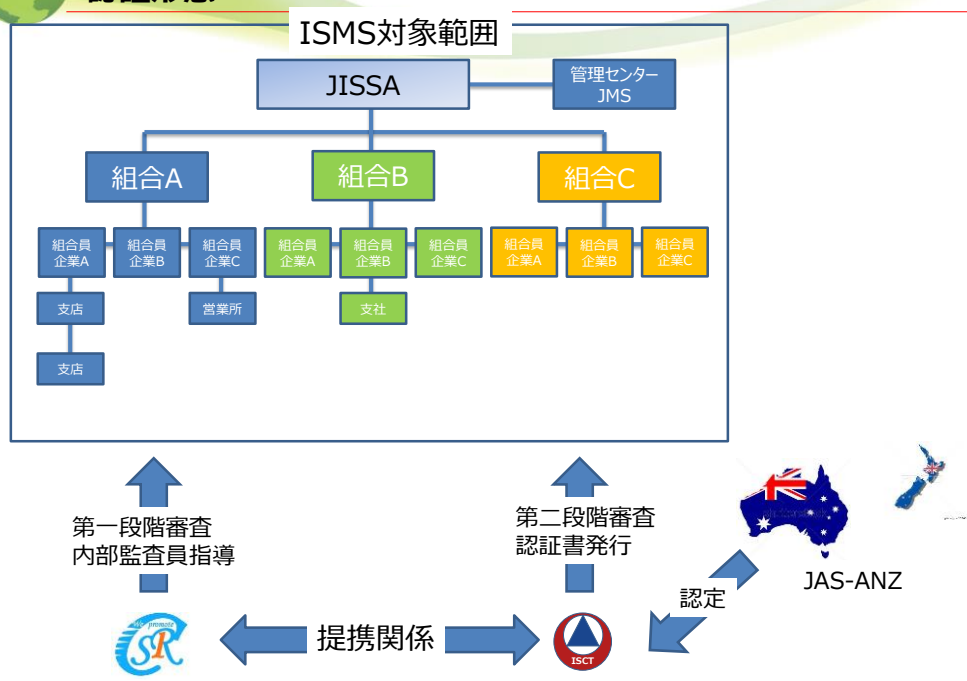
29

単独認証との比較

比較項目	ISO27001単独認証	ISO27001団体認証
規格	ISO27001（ISMS）	ISO27001（ISMS）
認証登録範囲	各社任意で決定	団体（JISSA）にて指定
認証機関／認定機関	各社で選択可能	ISC（東京）／JAS-ANZ（オーストラリア）
審査	1年に1回	サンプリングによる審査（3年1回程度）
ISMSマニュアル 適用宣言書	各社にて作成	団体にて作成したものを使用
内部監査	各社にて実施	各社にて実施
事務局	各社にて対応	団体にて一括
教育	各社にて対応	団体にて実施
セキュリティ事故対応	各社にて対応	各社対応後、再発防止対応は団体にて行う
認証維持審査費用	継続　300,000円～ 再認証　500,000円～	会費に含まれる

30

認証形態



31

日本情報セキュリティ推進協会団体認証の登場組織と役割

日本情報セキュリティ推進協会

ISO27001認証取得の母体

一般社団法人日本シーエスアール登録機構

ISO27001団体認証フレームのシンクタンク

ISC東京での提携関係により審査の一部を担当

ISC東京株式会社

認証機関（審査登録機関）

JAS－ANZ

ISC東京のISO27001審査を認定している組織

株式会社日本マネジメントシステム

日本情報セキュリティ推進協会のISO27001に関するサポート組織

（管理センター、研修実施など）

32

認証登録証イメージ

認証書見本

認証登録証
ISO 27001:2013

日本情報セキュリティ推進協会
〒231-0002 神奈川県横浜市中区海岸通3-9

当社は、貴社の情報セキュリティマネジメントシステムを審査した結果、
下記の認証範囲において上記規格要求事項に適合していることを証します。

認証範囲：日本情報セキュリティ推進協会及び会員各社における下記IT商品
及びITサービスの提供（会員各社の認証範囲は付属書に明記）
1. システムインテグレーション
2. ICTソリューション
3. デザイン制作
4. ソフトウエア・ハードウエアの販売
5. 技術者派遣

適用宣言書：2015年11月24日付　第1版
初回登録日：2016年1月27日

Tateki Sakaguchi
Managing Director
ISC Tokyo Co., Ltd.

登録番号：ISMS/0393
最新登録日：2016年1月27日
有効期間：2019年1月26日

登録証明付属書
ISO 27001:2013

日本情報セキュリティ推進協会
〒231-0002 神奈川県横浜市中区海岸通3-9

株式会社 **********
〒 *****　**********

当社は、貴社の情報セキュリティマネジメントシステムを審査した結果、
下記の認証範囲において上記規格要求事項に適合していることを証します。

認証範囲：ソフトウエア 開発及び販売、ICT導入コンサルティング、
技術者派遣

適用宣言書：2015年11月24日付　第1版
初回登録日：2016年1月27日

Tateki Sakaguchi
Managing Director
ISC Tokyo Co., Ltd.

登録番号：ISMS/0393
最新登録日：2016年1月27日
有効期間：2019年1月26日

33

認証書授与式の模様

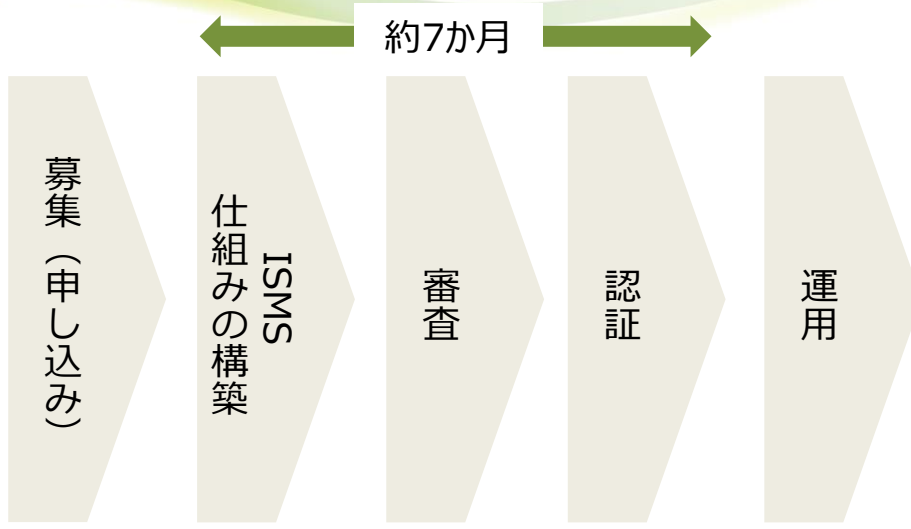
34

費用

初期費用	本社	60,000円
	支店、営業所等	30,000円
ISMS維持費用	本社	15,000円/月
	支店、営業所等	7,500円/月
ISMS講習費用	認証取得前　１回／月×6	25,000円/人
	認証取得後　６回／年	25,000円/人

35

団体認証取り組みのプロセス



お申込みＷＥＢページ

https://www.jissa.info/jissa-日本情報セキュリティ推進協会入会申込/

36

Q & A

Q
入会すれば必ず認証が付与されますか？
A
ISO27001規格を網羅できれば（管理センターがからの依頼事項全てをクリアしていただければ）、認証が付与されます。
全てをクリアできない場合、または組織的に全ての取り組みが困難な場合、ISMSの部分認証を付与致します。

Q
部分認証は取引先からの基準等に対し有効ですか？
A
有効です。ただし、取引先から特別に情報セキュリティに対する取り組み依頼がある場合、それを取り入れる必要があります。

Q
なぜ費用が安いのですか？
A
審査がサンプリングによる審査となること、構築費用を長期且つ会員全体で割合で負担することから費用が低減されます。

Q＆A

Q
通常の認証と団体認証は何が違いますか？
A
団体の方針に基づいたISMS構築及び運用となりますが、通常の認証と大きな差異はありません。

Q
ISOの認定マークは付与されますか？
A
付与されます。ただし部分認証の場合はこの限りではありません。

Q
入札資格等で、認証は有効ですか？
A
有効です。ただし、取引先から特別なセキュリティ管理や個別での認証を求められている場合は管理センターにご相談ください。有効か否かの確認をさせていただきます。

39

Q＆A

Q
運用について専任が必要ですか？
A
専任は必要ありませんが、内部監査及び管理センターとの連絡窓口となる担当者を決めていただきます。内部監査員及び担当者は他業務との兼任で構いません。

Q
審査は毎年行われますか？
A
原則としてサンプリングによる審査となりますので、2年または3年に1回の審査になります。
審査については、事前に日程、当日のタイムテーブル等の連絡があります。

Q
認定証には名前が入りますか？
A
認定証の名前はJISSAになりますが、付属書にお客様の社名が入ります。

40

Q＆A

Q
今回のISO取得でPマークの扱いはどの様になりますか？
A
Pマークの維持継続については各社にてご判断をお願い致します。
ISMSは個人情報保護も含む情報セキュリティの仕組みですので、取引先からの要求がPマークに限定されていないということでしたら、Pマークを継続しない選択もございます。

Q
講習はどのような形で行われますか？
A
管理センター（日本マネジメントシステム）を本部としてWEB会議形式で行います。

41

Japan Management System

www.j-ms.biz