情報セキュリティマネジメントシステム（ISMS）認証事業者実態調査
自由コメント（2013.03）

１ ISMS はリスクに対して，自由度の高い認証だと思います。 短的には，「トップがリスクを容認していれば OK」と言ったもので，認証企業が他社からみて，本当にセキュリティ事故が低いのか判断できない。 取得する企業も，特に決められたツール，運用を守らなくても認証されると思ってしまいます。 社員は対するセキュリティ意識の向上には役立っているが，実効性のあるものにするには，多くの費用が必要になり，導入の障壁が高いと感じます。 全体的には自由度が高く，解釈に悩む指針が多く，「認証のための作業」が大きな負担です。 ガイドラインの充実と他社の具体的な取り組みをもっと情報発信して欲しいです

２ 社員個人々々の意識を高めているには，どうしたら良いか難しいです。（ルールを守るだけでなく，自分である程度 リスクを判断できるようになって欲しい）

３ ISMS を取得した後，ルールが形骸化している。 教育をしても一部社員の意識が薄く，なかなか浸透しない。 先任者がいないため改善事項が進まない

４ 特に業務として負担となっていることは少ない。 当社は ISMS を含め３規格の認証を取得しているが，審査費用が高く感じる

５ 認証取得からまだ間もないため，これからいろいろと出てくるかも知れませんが，現時点では特にありません

６ 情報セキュリティ責任者（ISMS 事務局兼務）と内部監査員が各１名ずつなので，負担が大きいし，何かあった時に困る。 業務分担と新しい人材に対しての教育が今後の課題である

７ 取得前のコンサルでは小規模の会社でも回せると説明されましたが，実際には人手が少ないため，なかなか厳しいです。 通常業務との兼務は負担もあるため，なかなか他の人を割り当てることも会社として出来ずにいます。 取得時に取り組んでいないと認証規定を理解することが難しい文面になっております。 そのため，後任をさがす作業が難航しがちではないかと思われます

８ 各種（３大 ISO)以外にも，特約条項等の監査があり，その対応（準備）することが重複することもあり，無駄な作業が多くなってきていると感じています。 今後は，一本化することなどで，無駄な時間を改善できるように検討したいと考えています

９ 審査員の経験によって判断基準が異なる点が困る → 気にするポイントも異なるし，対処方法も指導も異なる

１０ JIDEC が発行する認証書の認証代が高い。 他の ISO も同様

１１ 管理においてあいまいな項番があるように見つけるので改善して欲しいと思っています

１２ 初期に構築したシステムがとても運用コストがかかり（人的），ほかの人がかかわり難くなっている。 そこから再構築をするための最適化された手順，手法がない。 結果，手つかずから社内への波及もままならず，形だけの ISMS になっている。 また，その要因には社内の過度なセキュリティに対する「守らないといけない」，「危ないことはしてはいけない」という改善していく仕組みへの不理解が根強い

１３ ①システム文書を簡略化して，よりわかりやすくすることが課題 ②ISMS 認証の効果的な PR が課題 ③ISMS の維持，運用が通りいっぺんになっていないか心配です

１４ ISMS 上の BCP は範囲が狭く，当社の BCP とあっていない部分が多い

１５ ISMS 認証の維持運用と情報システムのセキュリティレベルがあいまいと思える。 例えば，メールシステムのセキュリティレベルを上げるための方策と ISMS 管理策が具体的に合致しない

１６ 実運用に合わせたルール作りが難しい

１７ ISMS の他にＰマークも維持・運用しているが，２つの規格を維持するのは費用・体制面

で難しいと感じている。 この２つの規格が１つになれば，維持する側としては望ましい。セキュリティに関しては漏えいしない事は企業としての責任だと考えるが，日本の社会自体があまりにも過敏に反応していると思われる。 マスコミ等の報道の仕方にも問題がある。 いたずらに不安を煽るような報道は謹んでもらいたい。 政府も漏えいした情報を悪用する個人･企業については，厳しい罰則を設けるべきだと考える。

１８ 昨年，審査機関を変更した。 理由は 審査員の質のバラツキと審査費用の見直し。 それまでは，審査毎に審査員が変わり，指摘に一貫性がなく困惑していた。 現状は 審査員を固定して，審査の質が大きく向上した。 これによりマネジメントシステムの有効性が更に高まったと感じている

１９ やたらとリスク分析や対策がらみの資料が多い。 この部分が実態と乖離しており，審査のためだけに作っているものが多い。 トラブル分析を進めると，能力不足や教育訓練不足に行き当たることが多い。 ISMS の教育ではこの分野の有効な手段を持たない

２０ 外部審査について，サンプリング審査なので仕方ない面もあると思うが，審査員によって指摘されたり，されなかったりするケースがある。 サーベランスと更新では，工数に約２倍の開きがあり，これが経費に直接跳ね返ってくるので，厳しいところがある。 審査時のコンサルはできないことになっているが，折角の機会なので，維持・運用のやり方等に，もう少し踏み込んだアドバイスをして頂きたい。(同業他社との意見交換を行うなかで，審査機関により，かなりの違いがあると感じている)

２１ 軽微なセキュリティ事故（入館証の紛失，携帯電話の紛失）がなくならない

２２ アルバイトを含め 10 名程度の会社ですが，管理部門と生産部門の境を戸で閉めたり，携帯電話等の社内持ち込み禁止等は不便に感じているはず。 情報管理の色々な規制は社員を信頼していないとの前提に立たざるを得ず，社員の会社への不信感，忠誠心の欠如になるのではないかと危惧する。 小企業の場合は，会社と社員は一心同体であるとの信念で社員を信頼して 規制しない方がよいのではとも思う

２３ 取得時に作りすぎてしまった記録や文書をやっと最近減らし始めた。 どれもこれも書類として残さないといけないと思わせる指南書(コンサル含む)が多いような気がする。 一度つくると，「これを減らすと次回の審査に影響があるのではないか」と心配になってしまいなかなか減らせないのが困る。 取得後１０年近くになり，簡素化を目指している

２４ 担当者の入れ替わりや，兼務といったこともあり，全体的に情報セキュリティ理解度が低いことが今の問題と感じる。 規則化，マニュアル化をしっかりすれば，社員は守ってくれるため，業務上の負担とならないような運用手順を整備していきたい （現状，申請書の種類が多かったり，承認すべき上司が多かったりするため，社員からは面倒との声が多い)。何がセキュリティ事故で，何がそうでないか（例えば，パスワード失念等）判断が難しい（特に，一般社員にとって）

２５ 審査員に関する質問・回答において，当社の審査員は毎年変更がありますので，最高のメンバーを念頭においた（１回，自己主張のみで当方の話を聞き入れてくれない為，次回から別の人をお願いしたこともあった)。 審査機関や審査員によって，レベルや理解度，費用等，大きな隔たりがあり，また，何の審査を行っているのかわからない時がある。審査に望むことは コンサルがダメなことはわかっているのだが，今後 この規格を活用する上でのヒントが欲しい （直近の審査の際，非常に良いヒントを頂き，現在運用を大幅に見直し中)。 当社はこの規格をうまく活用しようと考えているが，認証だけ欲しいと思っている会社と同じような審査に疑問。 信頼性を上げて欲しい

２６ リスクアセスメント（特に リスク評価）における効果的なツールがないか考えている

２７ 2014 年１月より，次世代システムへの移行を予定している。 それに伴い ISMS 定期審査を 2013 年 9 月に実施することとし，今後、審査を 2014 年 9 月に実施する予定。 また、2014 年度より他地域の情報センターを ISMS 範囲に組み入れ，拡大審査を予定している。

２８　中小企業においては，維持・運用するのに相当な負担がかかるが，入札条件になっていることも多いので認証取得は避けられない

２９　社員のセキュリティレベルがなかなか高まらないという悩みはあるが，時間をかける（教育を繰り返す）しかないかと考えている。

３０　ISMS と JIS Q 15001 の二認証を取得しているが，情報セキュリティと個人情報保護に関するマネジメントの運用手法や考え方が重なる所があり，この２つの規格の組み合わせ審査を受けている。 合理的な審査であり，非常に経済的である。 この他，QMS と EMS に関しては複合審査を実施しており，マネジメントシステムを統合的にし、合理化を目指している。　経営計画の段階で，リスク管理ツールとして各種マネジメントシステムの要素を無理なく無駄なく生かす方法を常に模索している。　Ｐマークも取得しているが，審査機関のマネジメントに対する観点の違いが感じられる。　Ｐマーク取得は同じJISQ15001としての入札条件はないように思える。　１つの規格で２種類の認証を取得し，維持費が倍かかっている。　JISQ15001 規格としての認証が入札条件となれば，Ｐマークは継続を断念する方向にある。 したがって，ISMS の維持・運用のみならず，取得している全マネジメントシステムを規格にのっとった形で，効率良く融合させることを課題に日々運営している

３１　完全にセキュリティチェックを行うと，人手とコストが非常にかかる。　どこまでおこなえばリスクが防げるか疑問に思う。　教育を徹底し，モラルに頼るしかない。　良い方法を教えて欲しい

３２　ISMS，Ｐマークの認証取得により，社員及び社内でのモラルの向上は評価できると考えている。　しかし，公共団体への入札条件として，ISMS，Ｐマーク両方とも取得になっていること，本当に必要か？　差別化とはいえ，金取り主義ではと感じる

３３　ISMS 取得により，業務量が増加し，費用対効果の観点からも社員の理解を得るのが難しい。　本来業務に溶け込むような仕組み，システムがあると良いと思う

３４　やたら記録を求められ閉口しています。 当社は古紙回収業で，ＰＣはあるが LAN はない事業所

３５　現状の課題と取組状況について： ISMS の取組み及びセキュリティ目標については，全社的な取り組みとして，社内ホームページや定期的な社用ニーズ等により，運用の徹底及び意識向上を図っているが，情報セキュリティについての意識レベルが十分とは言えない状況が散見され，特に情報管理責任者（管理者）等の意識が希薄である。　このような状況の中，今回の更新審査結果において，「改善の機会」や「グッドポイント」等の意見を頂いたことから，現在も改善に取り組んでいる中で，事務局が中心となり，情報管理責任者の意識向上を図ることとしている。　具体的には情報セキュリティマネジメント委員会において，改善等スケジュールを検討し，情報管理者，実務者等連携の上，情報セキュリティインシデント　０件に向けて，取組み，更なる理解レベルの向上を図ることとする。　並行して，全社員研修も継続実施する

３６　本格的な事業継続計画への取組み

３７　セキュリティ対策の有効性の評価が何を指標にすれば良いのか分からない　（事故は起こさないのが常識であり，ウイルスによる被害も極々軽微なものでしかない)。　リスク分析の手法は詳細リスク分析法でなければ認証不可であることに疑問を感じる。　合議制でも良いのではないか。　要求事項が多すぎ，規格の書き方も難解（ＱＭＳ，ＥＭＳも同様)。　このアンケートで寄せられた意見・要望は規格や審査の見直しに反映されるのか？

３８　クラウドやモバイルへの対応が課題

３９　情報資産から，CIA 分析，リスク値の算定からリスクマネジメント，及び運用までといったプロセスの多さは兼務業務でやっている職員としては，とてもハードなことであるが，一方で，このツールを活かした手法で情報管理を整理運用していくことは，将来的にはと

ても強みになるものと期待し，努力し，高い目標に近づけなければと事務局は考えている。職員全体のスキルが上がり，広がることで負担感なるものも分散化され，有用なしくみに育っていくのではとの期待感もある。　常に前進しつづける仕組み作りに，今ついた所と思っている

４０　情報セキュリティの向上よりも，認証が目的となっている感が現場、事務局ともにある。このため，やらされているという意識が強くなっている

４１　当社はコンピュータシステム開発を主要な業務としており，社員の情報セキュリティに関する認知度は比較的高く，事故の発生はこれまでもなく，人的要因が絡んだ情報セキュリティインシデントはほとんど発生していない。　しかし，ISMS は必ずしも定着している訳ではない。　顧客契約のほとんどが請負契約で，大手顧客に ISMS やＰマークが普及している現状では，請負契約でも多くの場合，顧客環境での業務が要求される。 顧客環境での業務遂行では，顧客ルールの順守が，当社の ISMS、Ｐマークのルールとなっており，このような環境での社員は顧客ルールが当たり前になり，自社のルールを顧みない傾向がある。 この傾向は情報セキュリティルールだけでなく，事務処理等のルールにも当てはまる。 これは，社内的にはマルチスタンダードに他ならない。　一方，社内で実施する請負案件では，顧客が個別に順守を要求してくる。所謂ガイドラインの影響を多分に受けている。　これらのガイドラインの要求事項は一般に，弊社の想定リスクより高いリスクを想定しており，予防処置の要求も高い。　これら要求事項に対する対応として，弊社では ISMS，Ｐマークのルールそのものを改定するのではなく，社内のガイドラインの改定とそれに伴う設備，運用の変更で対処している。　大手各社のガイドラインの要求事項をできる限り取り入れている（できないものは顧客と交渉）ため，ISMS 運用は企業規模からみて，非常に厳しいものになっている。　しかし，運用コスト面からみて，全ての要求事項に対応するため，運用を切り替えて行くことは難しく，それが内部監査の指摘事項となっている。　ISMS の維持費用を妥当な金額に抑えているが，決して十分ではない。　マルチスタンダート（客先勤務社員）とダブルスタンダード（社内ルール）の問題を運用上，どのように解決するかが，大きな課題

４２　ISMS 審査・受審時に毎回思うこと　「不適合にならない！」　あえて，不適合にする必要はないが，このあたりが ISMS が形骸化している要因になっていると推察される。 弊社は比較的（相対的に）真面目に取り組んでいると思う。　継続することの重要性，意義を年々ひしひしと感じている。

４３　ISMS の求める要求を満足させるためには，対象範囲をせばめれば，せばめるほど，構築は容易と思う（特定の対象組織に絞る）。　逆に言うと，ISMS の適用範囲の拡大は，その対象候補先の対策が未完成または，残留リスクにしないといけない部分が増えることがわかっているので，拡大に二の足を踏んでしまうことはわかる。　適用宣言書を組織別に作って認証取得できるような仕組みにするとかにしないと，ISMS を採用する組織は増えないと思う。　例えば，100% 満足する所と，50% 満足する組織でも，共同で取れるというイメージ。　当社の場合であれば，情報を管理するっコールセンター（データセンター）だけならば，ISMS 認証は可能だが，物を扱う倉庫などは，インフラなどのコスト面で障害が高く，中小企業にとっては，ISMS 取得より，企業存続の方が重要

４４　サーベランスにおける文書，記録の作成が課題である。　認証当初は，社員に ISMS の活動を意識付けるため，専用の記録を作成していたが，社内規定とのダブルスタンダートを避けるため，業務フローに落とし込み，社内で使用している記録を ISMS 記録としたが，逆に ISMS の取組みという意識が薄れたように感じられる。　特に，新・転入者には，見えにくいようで，事務局として規格，アネックスと業務フローの連携について，力を入れている

４５　当社は，事業部単位での ISMS 取得を実施してるが，今後は全社・全体として ISMS の取得が必要になると考えられる （現状は，大きなインシデントは発生していないが・・・）

４６　教育の不足もあり，社内における ISMS の理解度（知識・必要性）は低い。　経営者も取得後，維持の必要性を示しておらず，一部の管理職が社員を管理するツールとして ISMS が利用されている。　経営者が人のつながりを重視する事でもあり，杓子定規なＩＳＯは当社にそぐわないと思っている。　維持も社外への不信感につながることを恐れてであり，もはや 形骸化している

４７　従業員のセキュリティ意識の継続や維持が難しい。　内部監査の形骸化の恐れ，内部監査員のレベルの均一化が難しい

４８　定型的なリスク評価では，回数を重ねるに従い，抽出できるリスクがなくなってくる。 効果的な方法がないか？　教育コストが予想以上に高い。　内部監査員のレベル維持の方法

４９　規格の要求事項が事業者の業種により不足している所があり（当社は追加の管理策を設けて補完），認証取得企業の全てが理にかなった運用ができているように思えない部分がある。　コンプライアンスを含め，業種ごとの事業内容にあった審査を経たうえで，認証すべきではないかと思う所がある

５０　経営者，従業員への教育が大変

５１　電子メールの送信間違い，添付ファイルの間違いなどの人のエラーが減らない

５２　同業他社が認証取得をやめたら，弊社もやめたい。　理由は以下の通り。　* 費用対効果が説明できない　* 全社として ISMS は取得していないが，情報運用管理部門が 全社情報セキュリティ対策を十分に行っている

５３　マネジメントシステムに対する社員の意識向上策

５４　社内の情報統括室内に ISMS 事務局を設置しており，疑問や課題等は共有・相談する体制になっている。　なお，今回の回答は，現場の一担当者の位置づけで回答している

５５　ISMS と PMS の社内体制は別に組織している。　社員が守るべき規定やマニュアルも別であるが，重複ルールが多数あり，一方，独自のルールも存在している中で，社員からの報告や一連の処置でどちらのルールに従って運用するかで戸惑いが発生している。　特に，報告で体制の違いから連絡ルートも異なっている。　ISMS，PMS の体制と規定等の見直し改善が必要と考えている。　経費面，運用面より，ISMS と QMS との複合審査を計画している。　PMS も含めたいが，JIPDEC であるため，断念するが，運用面で効率化を図りたい

５６　ISO 認証および ISMS を大いに活用できている

５７　ISMS 取得により，社員のシステムに対する意識が高まった。　内部監査の実施に関しては，やや有名無実気味。　自己監査を重視してもいいのではないか

５８　(1) ISMS 認証の維持・運用が長期（８年目）になると，毎年レベルアップを図るのが難しくなってくる。　(2) 人員の入れ替わりが多くなると，所属員のレベルが保てなくなったり，事務局サイドのスキルの維持（力量）が難しくなってくる。　(3) 技術的な進歩が速いため，対策が追い付かないケースも発生してくる。　(4) マネジメントシステム自体が初期の頃からすると適用対象者の状況がより，パーソナル化している為，マネジメントシステムとしては適用しにくい状況が発生しているようにも思う。　* パーソナル化については，スマートホン等の普及に伴い，個人と会社の区別がしづらくなってきている。　(5) ISMS 認証の取得が目的化してしまう傾向になり，より実質的な情報資産の保護には結びつきにくくなってしまう。　(6) (1)～(5)以上に大切なのは，経営層による情報セキュリティに対する認識・資源・人材の投資である

５９　事務局としては，ISMS を社内に広げていきたいと思っているが，各担当者は業務に多忙なため，教育をはじめとする時間がなかなか取れない

６０　62　セキュリティに関する「慣れ」をどう防ぐかが課題。　常に高い意識を保ち続けるこ

とが必要

６１ 現在は自社の規模レベルに応じた規程を策定し，運用している。　会社に規模拡大に応じて規程を順次，見直していく必要があると思っている

６２ 業務とは別の資料をかなりの量 作成する必要があり，業務部門への依頼が申し訳ない。内部監査の実施も結構負担になっている。　規程書のボリュームが大きすぎ，メンテナンスが大変である。　新しい技術の規程さくせいがなかなか進まない

６３ 世の中における ISMS の認知度が低いのではないかと感じている

６４ 特にコンシューマビジネスを展開しているお客様では，「Ｐマーク認証」を求められる場合が多い。　結果，ISMS 認証とＰマーク認証を併存することとなる。　内容的にはかぶっている部分が多いので，企業の立場としては，コスト的にデメリット。　各認証機関が「差分認証」制度を立ち上げたりしているようだが，世間に認知が進んでおらず，今の段階では利用できない

６５ 社員は社外における業務（ＳＥ）が多いので社内運用上の煩雑さを感じることが少ないと思われるが，今後，社内作業が増えた場合を考えるとマニュアルの見易さ，理解のし易さ，実業務との乖離がでないか等懸念している。　兼任だが，運用責任者は１名であり，事業規模や企業体力の面で，これ以上要員を増やすことは困難であり，ノウハウの蓄積も一人に集中している為，今後の ISMS 運用維持においても課題を残している。　認証取得当初に考えていた程，受注条件として ISMS 認証企業であるか否かが有利／不利に影響していない。　努力して認証取得した企業のモチベーションが下がらない様な仕組みが欲しい

６６ ISO と JIS は少し異なるのは・・・　27002 の管理策の取り扱い（要求事項なのか，リスクの受容を判断した上で，選択不要ではダメなのか？）が難しい。　中小企業でセキュリティ推進責任者を専任はムリ。　中小企業でセキュリティ責任者を担当して有効に機能させる人財は他にも重要なポストを担当する可能性が高い

６７ メンテナンスの時間が取れないため，時代の流れに追いついていけない所もある（クラウド対応など）

６８ 何事も始めは大変なことは分かっているが，未だに恩恵をうけていない

６９ 監査で，Good point を獲得できるノウハウや成功事例を他社の事例でも知りたい。　単に維持するだけでなく，ポジティブに改善できるような運用の仕組みにする為に，アドバイスをたくさん頂戴したいと思います

７０ 運用ルールの更新頻度とレビュー，承認の場であるマネジメントレビューの実施頻度があわない。　結果，未完了案件が累積していく。　ISMS 事務局メンバーが全員通常業務と兼務しているため，直接打ち合わせるマネジメントレビューをなかなか実施できない

７１ 要求事項や管理策が，コンサル，外部監査員，専門書によって違う場合があり，対策に迷うことがある

７２ 情報セキュリティ対策はこれで十分という線はなく，どこまでやるのか，どこまで費用をけけるのか，そのバランスが難しい。　最も影響が大きいと思われるのは，従業員の質であることを痛感している。　従って，基本教育（主に モラル）を最も重視している

７３ ISMS の維持・運用により，社内の情報セキュリティのレベルが一定以上に保たれていると実感している。　これからも維持運用のレベルを上げて，事件・事故を防ぐつもり

７４ とにかく大変である。　しかしながら，やり続けることによる効果がみえてきている。　課題：　認証取得後３年経過するが，なかなか自然体の運用になれない

７５ 現在の ISMS 認証は，全社になっていないため、ISMS を水平展開したいと考えている。そのため，非認証センターでも入退館管理を行っている。　全部門・全センターの内部監査では，情報セキュリティに関する項目を加えて実施している。　情報セキュリティテス

トは，全従業員（含役員）を対象に実施しており，新入社員（含中途採用）研修に組み入れて実施している。　情報セキュリティ基本方針は全社に掲示し，セキュリティ意識向上に役立てている。　主要センターは ISO9001 認証を受けており，ISMS の水平展開は認証拡大時を想定して行っている。　大企業，特に外資系の情報セキュリティ要求は高いが，弊社の業界では、ISMS 認証取得が少ないため，差別化になり，受注に役立っており，会社のステータスになるとの評価も受けている。　サーベランス，更新審査の費用負担が大きいが，一定の費用対効果があると社内では評価されている。　運用は順調だが，「有効性測定」は負担に感じている。　重すぎず，意味のある有効性評価，測定を試行錯誤している所である

７６　認証維持・運用のためには，全従業員の情報セキュリティ意識の醸成とその維持・増進が鍵と考える。　設定したルールが形骸化しないように常に注意しているが，何か良い方法があれば，教示願いたい

７７　旧通産省の「安対」から活動し，運用は安定している。　ISMS 認証取得当初に担当後，別部門に異動，昨春，９年ぶりに出戻ってきたが，当初の運用に比べると，運用が煩雑になった印象がある。　安定しているが故に，内部監査チームの指摘や外部コンサルの提言が，ゼロという訳にいかないのか，毎年無理やり出されており、事務局がその対応に振り回されている感がある。　当社はＰマークも昨年新たに取得したが，ISMS との整合性等も悩みの種である。　前回調査で「専門化している故に人事異動が難しい」との記述があったが，私のように戻されるケースもあるのではないか

７８　ISMS 認証後，３年がたち，更新審査が終わったばかりである。　とにかく，難しい規格であり，私自身が審査員資格を取得するまでになった（理解するためにどうすればよいかと進んでいった結果である）。　日常業務の中で，維持運用を行っていくには，更なる工夫が必要であると感じている。　スタッフへの理解も３年かけて少しずつ進んでいるように思う。　早く「文化」としての ISMS になっていくように進めていきたいと思っている

７９　①リスクアセスメントの際，数値目標というか，レベルの基準を作ることが難しかった。②計画に合わせて予算を考えるのが，良いと思っている。　③証書の発行に費用がいるのはなぜ？　④ISMS を導入していることで，「ダメですよ」と言いやすくなった

８０　すべての費用が高い

８１　ISMS やＰマークの認識が会社全体に深く浸透していないし，情報の漏えいや紛失の怖さを知らない。　もっと頻度をあげて社員教育をしたいが，教材，ツールが見つからない。毎月できる教材（１年で終結するようなもの）を探している。　うっかりや手抜きや知識不足から起こるものであり，レベルは高くなく，注意喚起を第一の目的にするような教材があれば助かる

８２　限定された範囲での認証であったのに審査のたびに拡大していく。　本来求めていたものを違う形になってしまうよう注意したい

８３　Ｐマークと合わせて運用を行っているが，審査機関が別であるため，更新の工数が非常に多く，効率が悪い。　統合審査制度を実現して欲しい

８４　個人情報保護マネジメントシステムと情報セキュリティマネジメントシステム認証の統合ができないか？

８５　手間はかかるが，PDCA の運用は会社としてメリットが大きい

８６　①審査員によって，指摘する観点が異なるため，毎年の審査対応で疑問を感じている。　②ISMS の構築時は，コンサルを導入していたが，予算枠が取れない為，取得後以降はコンサルなしで維持を行っているが，審査時に指摘を受けてもコンサルに相談できず，また，審査員もコンサルをすることは不可能なため，対応に困っている。　③各ポジションのスキルアップ（特に内部監査）のために，社内でどのように研修を行っていくか課題となっている

８７ ①ISO 側の規格や見解変更にキャッチアップする具体的方法が未確立であることが課題。②ISMS 審査員により審査ポイントの着目点が異なることがあるため，準備時の心理的負担がある。 ③発注する側の ISMS に対する評価がもっと上がって欲しい

８８ 私物の携帯電話（スマートフォン等，ＰＤＡ端末を含む）の業務利用とそれらの端末にデータが保存可能であり，これらを防ぐための有効な対策を講じるには費用の増加が必然となってしまう。 データ保管は個人の認識に大きく依存されてしまうのが現状であり，これをどうルールづけてコントロールしていくか，社員の情報取扱いに関する教育の強化，モラルの向上，コンプライアンス順守等整理すべき課題がある

８９ ①リスクアセスメントの分析を自社に合ったものへ改良していく（初めに コンサルからもらった内容では，自社に合わないものが多いため)。 ②QMS との共通化。 ③各種管理台帳の統廃合

９０ 今後，このようなアンケートはウェブ回答方式で実施いただけると迅速に回答することが可能になる。 一考を

９１ 一事業部として ISMS 運用しているが，全社としては ISMS ではなく，情報セキュリティ活動，個人情報保護活動として，事業部メンバーを含む全社体制で活動しており，事業部の ISMS と重複しているので，うまく一体化できないかを考えている。 妙案が欲しい所。但し，全体の情報セキュリティ体制メンバーと ISMS 推進委員は同じ社員をアサインしている

９２ 審査費用が高い（インシデントや指摘事項の推移状況を考慮した審査方法があっても良いのではないかと思われる)。

９３ 有効性測定方法や評価基準の見直し等には多大な工数を必要とし，また，それなりのスキルを必要とする。 小さな組織で事務局も全員が兼務の状況では ISMS 活動を効率化したいが，そのための見直しになかなか踏み切れない。 結局，小手先の対応となってしまい，毎年 同じ様な悩みが続くことになってしまう

９４ 経営環境(特に IT)の急速な変化に対応すべく ISMS の更新を実施しようとしているが，経営資源の制約などを考えると必ずしも最適な対処ができず苦労している

９５ PMS，ISMS を運用しているが，個人情報，情報資産での守備範囲であり，リスクアセスメントの相違は理解できる。 しかし，安全管理措置については，同等のものですので，統合的な規格，要求事項のもとで，運用できれば効率的であると考える。 審査機関の違いによる統合可能性を改善して欲しい

９６ マニュアルと実業務の乖離をどう解決するかに多大な労力が必要

９７ 一事業部での運用にとどまり，会社全体として 取組みが行われていない。 その為，情報セキュリティ部門や監査部門が積極的に ISMS 関わっていない

９８ 100 管理策要求事項の内容より，具体的な説明があれば尚良い。 一通り，該当する見本的事項を当てはめているが

９９ リスクアセスメント手順については，試行錯誤を繰り返している。 GMITS をベースにした市販ツールを使っていたが，ツール内にある脅威や管理策の範囲でしか分析ができないため，数年使い続けると現実的な対策案がでてこなくなった。 現在は，非形式アプローチをベースにした独自の手順で分析・評価をしている。 ただ，非形式アプローチは不慣れな者には，継承が難しいことから，簡易ツールの作成に取り組んでいる

１００ 事務局（推進側）と社員など（ISMS 管理を実施する者）の間の情報セキュリティに関する意識の乖離が問題

１０１ ISO 適合のための ISMS 活動となっている状況。 有効性のある活動への移行を目指しているが，進んでいないのが現状

１０２　リスクアセスメント手法の確立　（実態にあった改善）

１０３　有効なリスクアセスメント手法が見つからない　（無駄に感じる）。　法的要求事項の見直しが ISMS と違って難しい