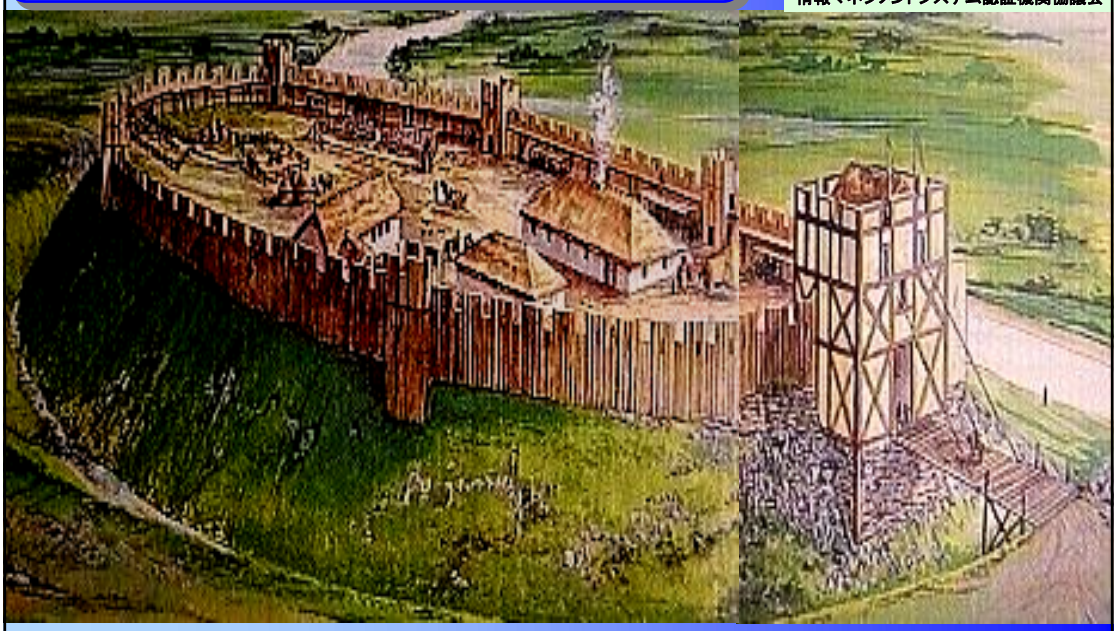
付加価値のある審査
（ パネルディスカッション ）

2009年3月03日
ISMSセミナー 2009
情報マネジメントシステム認証機関協議会



情報セキュリティ大学院大学 & 横浜市CIO補佐監

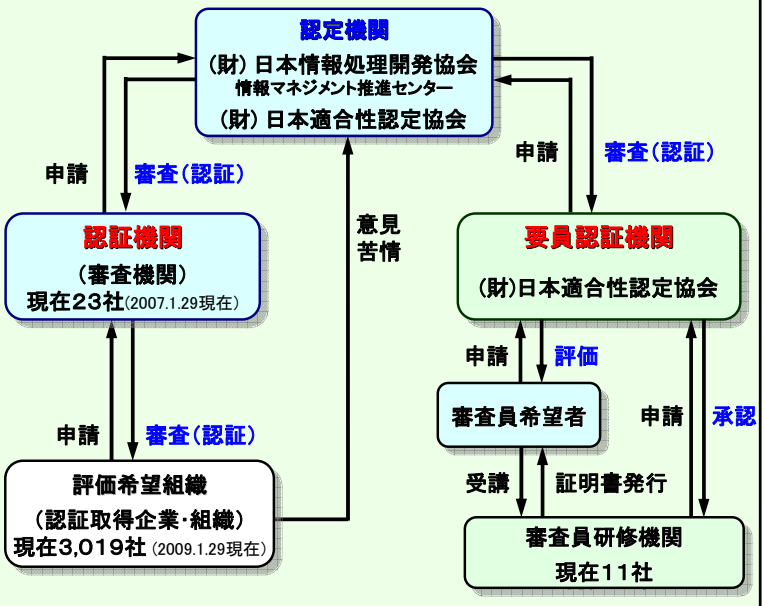
内田　勝也（uchidak@gol.com）

ISMS認証制度運用体制

認証機関（審査機関）一覧

1. （財）日本品質保証機構
2. 日本検査キューエイ（株）
3. BSIマネジメントシステムジャパン（株）
4. （財）日本科学技術連盟
5. （財）日本規格協会
6. （株）日本情報セキュリティ認証機構
7. デット ノルスケ ベリタス エーエス DNVインダストリージャパン
8. 国際マネジメントシステム認証機構（株）
9. （社）日本能率協会
10. ベリージョンソン レジストラー（株）
11. （財）電気通信端末機器審査協会
12. （株）トーマツ審査評価機構
13. テュフ・ラインランド・ジャパン（株）
14. （株）マネジメントシステム評価センター
15. （株）ジェイーヴァック
16. ビューローベリタスジャパン（株）
17. （財）防衛調達基盤整備協会
18. ロイド レジスター クオリティ アシュアランス リミテッド
19. SGSジャパン（株）
20. （財）ベターリビング
21. 日本海事検定キューエイ（株）
22. （株）グローバルテクノ
23. エイエスアール（株）

財団法人：　６社　社団法人：　１社
株式会社：１４社　外国企業：　２社



耐震偽装裁判結果（下級審だが）

耐震計算偽装：愛知・半田のホテル耐震偽装　愛知県に賠償命令

- 耐震計算偽装：愛知・半田のホテル耐震偽装　愛知県に賠償命令　確認審査、注意怠る
- 3者 計5,704万円 ⇒ 名地裁判決
- 姉歯秀次・元一級建築士による耐震強度偽装事件にからみ解体に追い込まれた愛知県半田市のビジネスホテル「センターワンホテル半田」が、建築確認審査をした県とホテル開業を指導したコンサルタント会社、総研の所長を相手取り、約5億1500万円の損害賠償訴訟の判決が24日、名古屋地裁であった。戸田久裁判長は「建築主事は確認審査における職務上の注意義務を怠った」と県の過失を認定、県を含む3者に約5704万円の支払いを命じた。耐震強度不足を見抜けなかった行政の責任を問う訴訟の判決は初めてで、同種の訴訟にも影響を与えそうだ
- 訴訟では、県が建築確認審査で負う注意義務の範囲が争点となった。県側は、問題発覚後の06年の建築基準法改正前に定められていた審査項目以外については「審査義務を負っていない」と主張したが、判決は「一般的に通用する技術的基準に反するような構造設計がされている場合、その真意を設計者に質問すべきだ」と判断した
- その上で、ホテルが各フロアの耐震壁の設計を2枚壁とすべきところを1枚壁として、耐震強度が基準の42%しかなかったことを確認審査で指摘しなかった点について「容易に発見できるもので、調査確認しないまま法規定に適合したと判断したのは注意義務に違反する」と認定。「耐震壁の評価は設計者に委ねられている工学的判断で、確認審査の対象ではない」とした県側の主張を退けた

リスク・監査の考え方がなければならないことを示した

制度等の崩壊は、現在抱えている直接的な問題が契機になるのではなく、
マスコミ等で取り上げられた問題を契機に制度全体への不信感で起こる？

毎日新聞　2009年2月25日　中部朝刊　http://mainichi.jp/chubu/news/20090225ddq001040002000c.html

ISMSの有効性の向上と認証審査

認証取得、5つ課題（2007年の調査）

1. **経営者の課題**：経営者が情報セキュリティ、ISMS推進などへの関心がない、または低い。 このため、推進事務局の努力が報われていない。経営者がISMSに関心を示さないケースは、営業上の目的などで形式的にISMSを取得する事業所等がある
2. **ISMSへの誤解**：管理策への誤解が多い。管理策で必要ないものは適用除外したり、または追加の管理策で更に高度なセキュリティレベルを構築してもよいことを理解していない。 ISMS導入前にレベルの低いコンサルタントの利用や認証取得を優先したのではないかと思われる面もある
3. **コンサルタントの問題**：認証取得のためにISMSへの支援を求めたコンサルタントがISMSを理解していないため、審査時に指摘事項の山となることもある
4. **審査機関・審査員の課題**：審査機関にも問題がある可能性もあるが、審査員がISMSの基本を理解していないために起こっている
5. **ISMS独自の課題**：2006年にISMSがJIS Q 27000シリーズに移行したが、移行期間が短かったため、移行審査への対応で、本来業務に支障を来した。ISMSからJIS Q 27000シリーズに移行する期間か1年と限られたため、ISMS認証を取得した事業所がJIS Q 27000シリーズへの移行作業を行う必要があった。ISMS認証を取得したばかりの事業所にとっては、審査を続けざまに受けるごとになり負担が高まった。移行期間が短いことと移行に関する情報不足がこの問題に拍車を掛けた

（財）ニューメディア開発協会「ISMS認証取得及びその継続における課題を探るためのアンケート」
http://lab.iisec.ac.jp/~uchida_lab/enq/isms/result.html
情報セキュリティ認証制度、実態調査で見えてきた課題
http://it.nikkei.co.jp/business/netjihyo/index.aspx?ichiran=True&n=MMITs20000280620007&Page=1

ISMSの有効性の向上と認証審査

認証取得、5つ課題（2007年の調査）
4．審査機関・審査員の課題

4．**審査機関・審査員の課題**： 審査機関にも問題がある可能性もあるが、審査員がISMSを理解していないケースも結構見うけられる

- 審査員、審査機関で判断が異なる
- コンサル、審査機関の選定が重要
- 審査機関によって審査の難易度や質的レベル差が大きい
- 審査員は現場を知らなすぎる人が多い。規格の杓子定規的な理論ばかり先行して、付加価値のある審査を望めない
- 審査員とコンサルとの判断の相違があり、適用宣言書の作成に苦労
- 審査員の質、現場、経営者の立場での視点の欠如、技術を知らない
- 有効性の測定の解釈が曖昧で、審査員の主観がかなり影響している

- 審査機関の審査方針が大きく影響している？
- 審査員の継続的な教育・訓練が必要では？
- 情報セキュリティ、情報システムを知らなくても、審査はできるのか？
- 監査概念のない審査員が結構いる（チェックリスト形式の審査。 リスク・環境変化を考えていない）？

- 相互審査ができなければ、第三者による審査評価が必要では？
- 審査員教育の充実
- 他マネジメントシステム審査員の受入教育・訓練の再考

認証取得、5つ課題（2007年の調査）
4．審査機関・審査員の問題

4．審査機関・審査員の課題

- 非常に優秀な審査員で、指摘事項に対する対策まで考えてくれた

- 審査機関がこの様な対応を推奨していないだろうか？
  - もし、指摘事項に対する対応策を推奨した場合、次回の審査時にその内容が指摘事項にならないだけの保証を与えられるのか？
  - 前回、審査員の指導により、構築した仕組みを指摘されるのは、おかしいと言われる可能性もある。 そこまで言われなくても、審査員・審査機関の不信感にならないか？
  - ISMS審査（監査）の考え方では、この様な問題を避けるために、マネジメントシステムの審査をしても、指導（コンサル）はすべきではないと考える

以下のような声もあったが・・・
- ISMSの要求レベルは、顧客などのステークホルダーの要求を満たしていない。 更に高いレベルの対応が必要
- 顧客先で顧客の指示に従ってシステム開発を行っている場合のISMS適用形態がわからない
- J－SOXには、ITIL（ISO/IEC 20000）での適用が大切

一部の審査員、コンサル、ユーザが監査やリスクを理解できないことがISMSの課題の１つでは？

ISMS認証取得組織調査より

有効性の向上
- 有効性の評価に対するISOの要求が漫然としている
- 定期審査時に審査員に対して、「管理策の有効性の測定」について質問をするが、的を得た回答を頂けない。JIPDECのガイドラインを参考に、算定式をつくってはみたが、有効性の判定を下す際に、妥当な判定かどうか、疑問である
- 有効性の評価（測定）について、早急に明確な基準（指針）を示して欲しい
- リスク分析手法、及び管理策の有効性評価が確立されていないことを感じ、現状では表面的にならざるを得ない面がある

審査員について
- 審査員の質に大いなる疑問を抱いている。 基準に対する個々の解釈の相違（決して小さくない）が歴然と存在しており、何よりも、その人間性（尊大な態度等）も問題です。全ての面において、必要なレベルに達していないと感じています
- マネジメントシステムでありながら、審査の場がセキュリティ脆弱性のチェックになっているように見えることがある。 マネジメントシステム＝経営のしくみ、として、情報セキュリティとしての目標管理的な進め方が今一つ腑に落ちない。 統合マネジメントでもやや異質の扱いになっている
- 審査員によって、指摘・提案のレベル差が相当にある

ISMSの有効性の向上と認証審査　ISMS認証取得組織調査より

企業・組織側の課題

- 目的が外部審査を問題なく実施されることに重点を置くため、審査前の作業が増加（記録のねつ造等）。 本来の目的を見失う傾向がある
- どこまでやればいいのか？
- 詳細管理策に対する適合宣言書について、本当に必要か違和感を感じる
- 全社への展開の必要性を感じているが、営業部門と製造部門では守るべき資産の違いがあり、統一ルールが適用し難い
- 基準の全社的な合意がとりにくい
- ISMSの内容に関する理解について、社内の格差が大きい
- ISO27001の要求事項、各種ガイドライン等の記述・内容が、現在のITインフラの観点からみて古い（過去のインフラ技術を基準とした）。 もっと、短サイクルでの内容の見直しが必要と思われる。
- 「管理目的及び管理策」にすべて対応するのは難しく、費用がかかる。内容に分かり難い点がある
- 適用範囲外の社員の教育、監査について、頻度や軽重の判断、やり方（どこまでやるか）が難しい
- 情報セキュリティについての社員意識をどう変革できるかがキーであるが
- 事務局主導でなく、自発的な取組が出来ることを目指しているが、難しい（業績の良くない部署は本業優先になる）
- 役職別の教育を行ない、それぞれの理解度を高めたいが、実施手法がわからない
- 受講者のスキルアップの評価測定が十分にできていない

ISMSの有効性の向上と認証審査　ISMS認証取得組織調査より

企業・組織側の課題

- ISMS認証制度とプライバシーマーク制度の不整合による問題点
  1. ISMSの認証を受けている大部分の事業者は、P-Markの認証を受けているものと思う。弊社も同様である。 認証審査の周期の違いは、統合審査の道を閉じている
  2. ポリシーや文書（規程や手順書）についても、認証基準を意識したものとして、基本規程が一部ダブルスタンダードにせざるを得ない
  3. 認証基準の改訂に対応し易い、ポリシーや文書は認証基準毎の独立性が高いものであるが、複数の認証を取得している事業者としては、統一したポリシーや文書を規程した方が、周知徹底が画れると云う相矛盾する課題を克服する必要がある

情報技術システムのための セキュリティ評価基準ガイド

NIST Special Publication 800-55

A.7 物理的な保護と環境的な保護

重要項目	7.1 物理的なダメージやアクセスのリスクに対して十分な物理的セキュリティコントロールが実装されていますか?
詳細質問	7.1.3 保管庫からのテープや他の記録メディアの貸し出しや返却は承認され、記録されていますか?
評価尺度	テープの貸し出しや返却の記録をとっている情報システムライブラリの割合
目的	テープや他の記録メディアに保存された蓄積データに対して、組織が実施する制御レベルを特定し、認定ユーザに対するアクセスを制限する
実施証拠	1. 機関内にはメディア保管庫がいくつあるか? _____ 2. 貸出しや返却が行われた記録メディアのうち、記録から理由のわかるものはいくつあるか? ___ 3. アクセスコントロールリスト上で承認された職員が借り出した記録メディアはいくつあるか? ___ 4. メディアの貸し出しと返却を記録している保管庫はいくつあるか? ___
頻度	半年ごと、年1 回
計算式	貸し出しや返却のイベントを記録している保管庫の数(質問4)／メディア保管庫の数(質問1)
データソース	メディア保管庫のログ、システム保管庫、ISSO
指標	このメトリクスの目標は100%である。割合が低い場合、データ格納メディアの管理が行われていないことが原因となり、セキュリティ事件によるデータ流出の危険性があることを意味する。

解説: 使われているデータ格納メディアの数を明確にし(質問2)、適切な職員だけがメディアにアクセスでき、かつ、メディアの場所を記録していることを確認する(質問3)ことで、テープやメディアの貸し出しプロセスのコントロールが有効に働くようになる。

カーク・パトリックの研修効果測定モデル

研修効果測定レベル

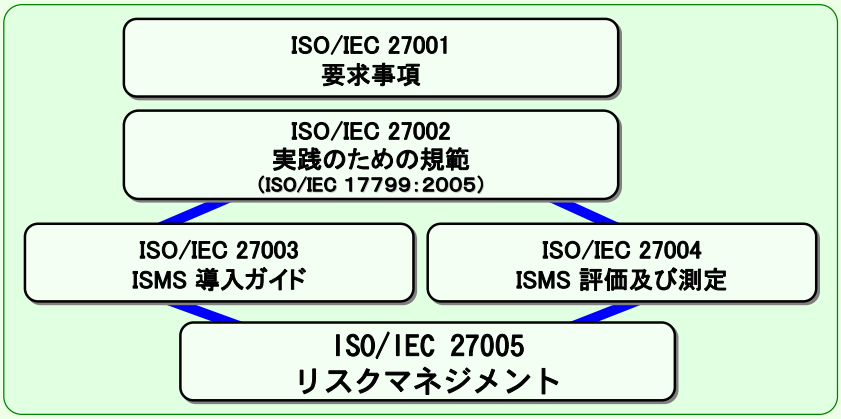
- レベル1：反応（Reaction） 研修に参加した人材の反応、すなわち、研修を気に入ったかどうかで効果を評価する。 アンケート調査が一般的。 研修内容があなたの要望に合致していたか？ 内容はわかりやすかったですか？ 講師の指導は良かったか？
- レベル2：学習（Learning） 参加者が何を学習したのかを評価。 試験の実施が有効。学習効果を測るには効果的。 参加者が学習内容を振り返ることができる点でも有効
- レベル3：行動（Behavior） 参加者が研修で学んだ知識・スキルなどを仕事や行動の変化として反映させたかを評価する。 行動変化をアンケートやインタビュー形式で周囲の人達に確認する
- レベル4： 結果（Results） 研修前後で売上、生産コスト、離職率などの数字の変化を評価する。但し、研修結果なのかの判定は容易でないため、上司等のインタビューで測定精度を高める等が必要になる
- レベル5： ROI（投資対効果） 研修の効果測定は、その効果を収益に換算し、収益を教育研修への投資額と比較する（ジャック・フィリップス：Dr. Jack J. Phillipsが提唱）

CMMI（Capability Maturity Model Integration）

能力成熟度モデル統合（CMMI）

1. **初期状態**（混沌とした、いきあたりばったりで、一部の英雄的なメンバー依存の状態） 成熟したプロセスを導入する際の、出発点のレベル
2. **管理された状態**（反復できる状態、プロジェクト管理・プロセスの規則の存在） 反復してプロセスを実行できるレベル
3. **定義された状態**（制度化された状態） プロセスが標準ビジネスプロセスとして明示的に定義され関係者の承認を受けているレベル
4. **定量的に管理された状態**（計測できる状態） プロセス管理が実施され、さまざまなタスク領域を定量的に計測しているレベル
5. **最適化している状態**（プロセスを改善する状態） 継続的に自らのプロセスを最適化し改善しているレベル

ISO/IEC 27000シリーズ全体像



ISO/IEC 27001	Information technology -- Security techniques -- Information security management systems - Requirements
ISO/IEC 27002	Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 27003	Information technology - Security techniques - Information security management system implementation guidance
ISO/IEC 27004	Information technology - Security techniques - Information security management measurements
ISO/IEC 27005	Information technology - Security techniques - Information Security Risk Management
ISO/IEC 27006	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Information technology -- Security techniques -- Guidelines for Information security management systems auditing
ISO/IEC 27011	Information technology -- Security techniques -- Information security management guidelines for telecommunications
ISO/IEC 27031	Information technology -- Security techniques -- Specification for ICT Readiness for Business Continuity
ISO/IEC 27032	Information technology -- Security techniques -- Guidelines for cybersecurity

http://www.iso27001security.com/index.html