Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

ISMS 認証事業所調査からみた セキュリティマネジメントの課題

内田勝也[†]　　星智恵[††]

東日本大震災や最近のサイバー攻撃で,情報セキュリティへの関心が高まったが,局所的,技術的な対応だけに関心が集まっている．しかし，本来，組織の情報セキュリティ対策は，利用者も含め，全体的･包括的に考える必要がある．

情報セキュリティマネジメントシステム適合性評価制度が 2002 年 4 月より本格運用され，多くの組織が取得している．しかし，他の認証制度と同様，認証取得効果の疑問や制度の誤解，取得が目的化している組織が少なからず存在する．

制度自体が優れており，審査を行う審査員やその審査等の運用が適切で，受審組織の推進が適切であれば，有効に機能する．

本稿は，ISMS 認証取得事業所調査等を通して，制度，運用，推進の各段階での課題を明確にし，その対応を考え，更に，どの様な経営課題があるかを考察した．

Information security management issues from ISMS certified organization survey

Katsuya Uchida[†]　and Tomoe Hoshi[††]

By the Great East Japan Earthquake and increase of a cyber attack, the information security became highly concerned. And the spotlight on local and technical area of the information security has been put. However, essentially, the organization needs to think in the systematic and comprehensive security.

The certified ISMS systems have been started from Apr. 2002. And many Japanese organizations have acquired them. The organizations have misunderstood the certification systems. And the certification acquisition has become the purpose of many organizations.

If the system in itself is good, and the procedures of the auditing by auditors/Lead auditors are appropriate, the staff in the certification organizations also do the proper actions, the certification systems perform effectively.

In this paper, from the survey of ISMS certificated organizations, we indicate the issues of three phases, that is, the certification systems, the auditing by auditors and the implements and improvements by the organization staff. And we review the issues of management.

1. はじめに

8 ヶ月のパイロット期間を経て，2002 年 4 月より本格運用が始まった情報セキュリティマネジメントシステム適合性評価制度（以下，ISMS 認証制度という）は，2006 年 5 月から，ISO/IEC 27001/27002 の日本語版の JISQ27001/27002 を適用することになった．2010 年末に，(財)情報処理開発協会[1]（以下,「JIPDEC」とする）への登録が 3,744 件[2]，（公益財団法人）日本適合性認定協会への登録が 778 件[3]あり，合計 4,522 事業所[4]が認証取得している．

世界における ISMS 認証取得事業所数の半分以上を日本が占めている[5]が，ISMS 実態調査結果では，取得後，業務負荷が増大，末端まで ISMS が浸透していない，更に，認証維持のため,二重帳簿的な対応をしている,実業務と乖離している等の回答もある．認証制度の課題は，他の認証制度，ISO9001(品質マネジメントシステム)でも指摘[6]されている．

また，審査員の指摘が必ずしも認証取得事業所に対して適切でない，審査員毎に異なる指摘がある．更に，審査費用が高いとの不満もある．

2011 年 1 月に実施した調査では，認証取得の古い順に 2,000 社[7]を選択し，アンケートを送付した． なお，前 2 回の調査[8]は，ISMS 認証取得事業所全てにアンケートを送付し，回答を求めた．

2. ISMS 実態調査について

2.1. 調査概要

JIPDEC の ISMS 適合性評価制度で,「ISMS 認証取得組織」の公開事業所から，認証取得が古い 2,000 事業所に郵送による調査を行った(所在地非公開事業所は除いた)．

質問は以下のグループに分けられる．

(1) 事業所，記入者の基礎情報(7 問)：組織規模(資本金，従業員数)，業種，記入者の所属部門，役職，ISMS 運用での役割，経験年数

(2) ISMS 認証取得関連(11 問)： ISMS 取得年月，対象従業員数，他の認証取得年月，ISMS 認証取得目的，発案者，運用責任者，取得範囲変更の有無，ISMS 認

† 横浜市（非常勤）City of Yokohama (Assistant to CIO)
†† ビジネスアシュアランス(株)　Business Assurance Co., Ltd.

1 現在は,「一般財団法人日本情報経済社会推進協会」と名称を変更している．英語略称「JIPDEC」は変更ないため，以降，JIPDEC と記述する

2 2012 年 1 月 6 日現在の登録数，3,975 事業所

3 2012 年 1 月 1 日現在の登録数，17 事業所

4 ISMS 認証制度は，場所，特性等で企業・団体は，本社，事業部，データセンター等で認証取得できるため,「事業所」数とした

5 2011 年 11 月現在,全世界で 7,536 事業所の内,日本は 3,939 事業所で,全体の約 52%を占める.(International Register of ISMS Certificates なお，国内の登録件数とは異なる）http://www.iso27001certificates.com/

6 日経コンストラクション「ISO を入札要件から外す」日経 BP 社 2004 年 6 月 11 日号 QMS の課題，特に官庁等の入札要件の問題点を韓国での事例等を含めて解説している

7 2008 年 10 月までに ISMS 認証を取得した事業所で，ISMS 取得後，2 年以上経過
2011 年 1 月に実施，2,000 事業所に送付，有効回答：426 事業所（回収率 21.3%）

8 第 1 回：2007 年 2 月に実施，1,422 事業所に送付，有効回答：264 事業所（回収率 18.6%）
第 2 回：2008 年 12 月～2009 年 1 月に実施，2,096 事業所に送付，有効回答：352 事業所（回収率 16.8%）

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

証取得効果，想定外の影響，

(3) ISMS 認証運用関連(9 問)： 運用上の負担，ISMS の効果増進の取組み，ISMS と実務の乖離の有無，維持費用，ISO27002 の取組み方，経営者のマネジメントレビューへの関与，現在の事務局人数，当初要員残留率，事務局員教育等

(4) コンサルタント(12 問)： コンサルタント利用の有無，コンサルタントの理解度，費用の妥当性，コンサルタントの選定重視項目等

(5) ISMS 審査員(7 問)： 審査員の各種理解度，指摘事項の妥当性，審査員に対する重視項目等

(6) ISMS 認証の重要運用項目関連(6 問)： 内部監査の実施頻度，体制，指摘事項の改善の有無とその対応，マネジメントレビューの実施頻度，実施形態

(7) 教育･社内ルール(8 問)： 社員，情報セキュリティ管理者，経営層等の教育方法，社員への教育頻度，教育担当部門と各担当部門の情報セキュリティレベル，教育以外の啓発方法，教育(集合，e-ラーニング)の評価方法

(8) その他(5 問)： 実施情報漏えい対策，可搬型ＰＣ・記録媒体の持出ルールの有無，社内持込ルール，コンピュータウイルスの感染の有無と感染原因

回答事業所の中から，インタビューを行い，郵送アンケート調査を補った．(表２)

表１ ISMS 調査概要

	今回 (2011 年 1 月)	前回 (2009 年 1 月)	初回(2007 年 1 月)
対象事業所数	2,000（古い順）	2,092（全対象）	1,422（全対象）
有効回答数	426（22.1%）	352（16.8%）	264（18.6%）
調査期間	2011 年 1 月 01 日 ～2 月 14 日	2009 年 1 月 01 日 ～2 月 27 日	2007 年 2 月 01 日 ～3 月 09 日
回答形式	• 原則無記名(組織名，住所，記入者名，メールアドレス任意記入) • 今回：企業名 256 (60.6%)，記入者 231 (54.2%)，メール 198 (46.5%) • 全記入 195(45.8%)（記名で，コンサル/審査員の課題を記述あり）		
質問内容	事業所の基礎情報，ISMS 認証取得作業，認証の運用，コンサル，審査員，教育･啓発活動等の調査		
	①事業所，記入者基礎情報 (7 問) ②ISMS 認証取得関連 (11 問) ③ISMS 認証運用関連 (9 問) ④コンサルタント (12 問) ⑤ISMS 審査員 (7/5 問) ⑥ISMS 認証の重要運用項目 (6 問) ⑦教育・社内ルール (8/10 問) ⑧その他 (5 問)		①事業所基礎情報(6 問) ②認証取得作業(10 問) ③認証運用(13 問) ④教育･啓発活動(6 問)
インタビュー	6 事業所	2 事業所	2 事業所

2.2. 主な調査結果とその考察

主な調査結果は以下の通り．

(1) 事業所の基本情報

- 「1,000 万円以上 5 億円未満」企業が 78.6%を占めた．資本金「5 億円以上」は 19.0%あり，大規模組織でも積極的に ISMS 認証を取得している．
- 従業員 300 人未満が 65.7%，従業員規模では小規模組織が多い．
- 情報通信業 (40.5%)，製造業(11.8%)，複合サービス業 (10.6%) が上位業種．

(2) 認証取得対象事業所の基本情報

- 認証取得範囲の従業員数は，100 人未満 (54.6%)，100～300 人未満 (29.9%) が全体の 84.5%を占め，認証取得の大半が 300 人未満の事業所である．
- 認証取得後 平均 4.1 年経過． 複数の企業での認証取得もある (表２)

表２ 認証対象従業員数と組織の従業員数比較

従業員⇒ / 認証対象者	100人未満	300人未満	500人未満	1,000人未満	1,500人未満	5,000人未満	10,000人未満	10,000人以上	Total
100人未満	148	46	9	12	5	7	2	1	230
300人未満	3	75	12	9	3	18	2	1	126
500人未満	0	1	18	4	2	2	0	0	27
1,000人未満	0	0	0	13	3	3	0	0	19
1,500人未満	0	0	0	1	7	3	0	0	11
5,000人未満	0	0	0	0	0	4	1	2	7
10,000人未満	0	0	0	0	0	0	0	1	1
10,000人以上	0	0	0	0	0	0	0	0	0
Total	151	125	39	39	20	37	5	5	

(3) 認証取得目的

- 「営業活動に有利」(75.2%)，「情報セキュリティ対策向上」(66.2%)，「業務改善」(44.7%)の順．
- 認証取得は，会長・社長(52.0%)，他取締役(20.8%)，管理職(17.0%)の発案だが，運用責任は，他取締役(36.3%)，管理職(30.7%)，会長・社長(20.2%)の順になっている．

表３ 事務局人数と構成

	合計	専任のみ	兼務のみ	その他	専任+兼務	専任・兼務・他
1人	83	12	45	0	0	26
2人	87	6	69	0	12	
3人	86	7	73	0	6	
4～6人	89	9	76	1	3	
7～9人	29	0	28	0	1	
10人以上	48	0	22	0	26	

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

表３ 認証取得の主な目的（N=423）

(3) 認証取得の効果･影響

- 効果として「社員のセキュリティ意識の浸透と実践」(87.1%),「情報資産の明確化と整理」(80.3%),「事故発生時の体制･計画の整備」(61.5%),「情報流出や漏洩の防止・軽減」(61.3%)をあげている.
- 影響では,「業務量の増加」(39.9%),「業務上の制約の増加」(33.1%),「対策コストの増加」(31.9%),「組織･人が必要」(25.8%),「手続きの煩雑化」(25.8%)の順で,全体の半数以上, 50.7%が業務量の増加や手続きの煩雑化･効率低下と回答し,更に, その 58.6% が「監査目的のための資料作成」を回答. また, 33.1%が業務上の制約増加, 79.4%が機器の取扱(持出･持込)の制約, 55.3%が資料作成ルール,上長承認の増加と回答.

(4) 運用上の負担と重点的取組み

- 運用上の負担は,「リスクアセスメントの見直し」(50.0%),「ポリシー(含規定類等)改訂や記録等更新作業」(44.8%),「情報資産台帳の見直し」(43.1%),「内部監査対応」(37.4%)の順.
- 重点的取組は,「一般社員の認識･理解の強化」(67.5%),「有効性評価手法の改善」(31.5%),「内部監査者のスキル強化」(31.5%),「教育研修の改善」(30.5%)の順.
- 実業務と ISMS の乖離は,「乖離はない」(38.2%),「どちらとも言えない」(35.3%),「乖離はある」(26.5%)で,「乖離はある」は, 前回調査(12%弱)の２倍以上あった.

(5) 推進体制

- 事務局人数は,「3 人」(22.7%),「2 人」(21.1%),「4 人」(13.7%)の順. 兼務のみ(74.2%)で, 兼務：3 名(17.3%), 2 名(16.4%), 1 名(10.7%)となっている.
- 初回認証取得時の事務局員が,「全員残っている」(21.1%),「50～70%未満」(21.1%),「誰もいない」(19.6%)の順.
- 新規事務局員の ISMS 関連スキル教育は,「社内講習」(55.4%),「OJT」(220 件, 53.0%),「外部講習」(39.3%).

(6) コンサルタント

- コンサルタント利用は, 認証取得前では, 利用(71.2%), 一部利用(7.7%)だが, 取得後は, 利用(13.2%), 一部利用(17.7%)となり, 前後で逆転している.
- コンサルタントを理解度, コミュニケーション, 能力等の分野で, 10 段階評価[9]を行った（表４）. 10 段階評価で 8.00 以上を期待したが, 8 項目のうち, 5 項目が 6 点台であった.

表４ コンサルタント評価

ISMS の理解度	**7.78**
情報セキュリティの理解度	**7.79**
業務の理解度	**6.62**
コミュニケーション	**6.95**
実効性のある提案	**6.54**
確立したコンサル手法	**6.67**
一貫性のあるコンサルテーション	**6.97**
ISMS 認証取得に役立った	**7.72**

表５ 審査員評価

ISMS の理解度	**8.65**
セキュリティ技術の理解度	**8.31**
業務の理解度	**6.98**
コミュニケーション	**7.66**
実効性のある指摘	**7.39**
効果や課題を確認する能力	**7.58**

(7) 審査員

- 審査員の評価は, 8 を越える項目もあるが, 総じて厳しい評価であった（表５）.

(8) 内部監査, マネジメントレビュー

- 内部監査は, 審査にあわせ「年 1 回」(77.1%), 「半年に 1 回」(20.3%)が続く. また, 内部監査は,「社内常設」(51.4%),「社内非常設」(44.6%)と続く.
- 指摘事項の改善は,「行われている」(85.2%),「一部のみ」(14.5%),「未実施」(0.2%)と続く.
- 未実施理由は,「現場の改善余力なし」(31.8%),「現場が非協力的」(12.9%),「マネジメントの支援が不十分」(16.5%),「事務局に改善余力なし」(17.6%)とある.
- マネジメントレビューは, 内部監査の傾向とほぼ同じで,「年 1 回」(70.7%),「半年に 1 回」(20.3%)となっている.

(9) 教育について

9 国内の評価では, 3, 5 段階の奇数段階評価を行うが, 真ん中を選択される事が多い. また, 偶数段階評価だと, メモリのない真ん中にマークをする回答もある. 海外等の評価を参考に 10 段階評価にした[1].

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

- 社員の教育方法は,「集合研修」(82.0%),「冊子の配布」(42.6%),「ＯＪＴ」(33.1%),「E-ラーニング」(30.3%)と続く．なお，3 事業所が教育を行っていないと回答している．
- 社員への教育頻度は,「3 ヶ月に 1 回」(43.1%),「月 1〜2 回」(26.0%)と頻繁に教育を実施している．
- 有効性測定方法は,「テストの実施」(集合教育：57.3%，e-learning：82.7%)が最も多い．但し，集合教育では,「アンケートの実施」(18.9%),「出欠確認」(17.0%)が比較的高い割合を示している．
- 啓発活動は,「ポスター掲示」(71.4%),「会議での連絡・通知」(69.0%),「ウェブ啓発活動」(23.8%)と続く．

(10) 社内ルールについて

社内ルール（個別のセキュリティポリシー）やコンピュータウイルスに関する質問をした．

- 情報漏えい対策は,「ログインパスワード認証」(95.3%),「パスワードの定期的変更」(87.2%),「ファイルの暗号化」(67.1%),「外部媒体接続制限」(56.6%)の順．
- 可搬媒体(①ノート PC，②外部記録媒体)の社外持出ルールは,「ルールあり(要許可)」(①82.1%，②84.3%),「持出禁止」(①12.6%，②9.4%)の順．
- 社内持込／利用制限機器は,「ノート PC」(89.4%),「外部記憶媒体」(85.7%)の順だが,「携帯電話」(21.6%)も増えてきた．
- ウイルス感染の有無と感染原因は,「感染なし」(66.4%),「感染あり」(32.5%)で，一般のセキュリティ調査から比較すると感染割合が低い．
- 感染原因は,「ウェブ閲覧によるドライブバイダウンロード」(5.18%),「パターン更新漏れ」(19.7%),「ゼロディウイルス」(15.3%)と続く．但し，厳密に言えば,「ウェブ閲覧」では，トロイの木馬やスパイウェアではないかと思われる．

(11) 自由回答欄について

ISMS 認証維持・運用上で感じている事項や疑問，課題等について自由に記入を求めた．所属組織名，記入者名，メールアドレス等は無記名も可としたが，30.8%に何らかの記述(除「特になし」等)があった．

- 制度面では，有効性は高いが，規格書がわかり難い(不適切な日本語訳あり)．
- 運用面では，①P マークとの統合審査，②審査員の指摘が毎回異なる，レベルが低い，③審査料に見合う審査でない，④費用対効果から，認証返上した．
- マネジメントシステムの推進では，①推進担当者が少なく，兼務等で，作業負荷が大きい，②教育が不徹底で，情報セキュリティ意識向上・定着化しない，③インシデントが減らない，④新情報機器の管理手順等の確立が後手に回る，⑤情報資産のリスク評価等の作業のマンネリ化／不十分，⑥セキュリティ対策と業務効率のバランスが難しい，⑦推進担当者の専門性が高く，人事異動が難しい．

2.3. インタビューについて

アンケート回答組織から 6 事業所を選定し，インタビューを行いアンケート回答の補足を行った．

(1) 推進担当と経営者の理解

- 兼務で推進しており，経営者の理解が推進に影響している．内部監査の実施，審査の立会等，担当者の専門性が高くなり，人事異動が難しい．
- コンサルタントの選定の拠り所は，業界関係者の紹介やセミナー等の講師が多いが客観的な情報がなく，課題もある．
- 審査員，審査機関にも課題があるとの回答もある．

2.4. その他

詳細な調査報告書は，以下に掲載してある．

http://www.uchidak.com/isms/ [2]

3. 調査からみる ISMS の課題

今回の調査は，取得年の古い順に 2,000 事業所を対象にし，426 事業所から回答を得たが，初回認証取得後，平均 4.5 年経過しており，多くの事業所(81.4%)は更新審査(更新審査は 3 年毎，サーベイランスは毎年行う．)を経験している．

本調査の対象となる制度は,「ISMS 適合性評価制度」(以下,「本制度」という)と言われるが，JISQ 27001[3]を基準に運用している．この基準は，ISO/IEC の基準を日本語に翻訳した．

ISO/IEC にて決められた基準の翻訳文書などに関する「制度」，審査機関･審査員が認証取得事業所に対して行う審査等の「運用」，認証取得事業所が情報セキュリティマネジメントシステムを確立し，維持推進を行う「推進」の３つに分けて，考察を行った．

3.1. 制度面の課題

基準書の日本語が分かり難く，適切な日本語になっていないとの指摘ある．分かりやすい基準書は ISMS 推進にとっても重要であり，おかしな部分については，ウェブ等で公開する等の対応も必要と思われる．

- 過去の資料等との整合性を保つためには，同じ英単語を同じ日本語に訳す必要もあるが，その言葉の使われている内容で，同じ単語に同じ訳語を使うことが適切でないこともある．
  例： agreements：「合意」とあるが，通常は「契約書」である(A.10.2)．
- 英語表現をそのまま日本語に翻訳しており，日本語として適切と思えない．
  例： It shall be ensured that：基準書は,「〜することを確実にしなければな

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

らない」とあるが，日本語では「確実に～しなければならない」である．

- 2006 年の JISQ 27001 への移行時，期間が短く，移行審査対応のため，本来業務に支障がでた．移行期間が 1 年で，旧認証取得事業所は JISQ27001 への移行が必要であり，審査を連続的に受ける負担が発生した．

3.2. 運用面の課題

運用面では，コンサルタントや審査機関・審査員，認証取得事業所が関係する課題も多い．

(1) リスクやリスクアセスメント，リスクマネジメントの誤解や無理解

- 全体的には，リスクに対する考えが低い感じを受ける．リスクはゼロにならなし，変化する．また，リスクはマイナスもプラスの概念もある．
- 情報資産のリスク評価･リスク管理が重要だが，時間の経過，環境変化でリスクが変わることが理解できず，重要資産の識別が漏れてしまうことがある．

(2) JISQ27001 附属書Ａ「管理目的及び管理策」の誤解や無理解

- 管理目的や管理策は取捨可能であるが，全ての管理目的･管理策を適用しなければならないと考えている(4.2.1 g)．
  管理策を「チェックリスト」と誤解し，全ての項目を「丸バツ」で判断すれば良いと誤解している．
- 情報資産は全て明確な識別が必要だが，重要資産目録は作成･維持する必要がある(A.7.1)．情報資産を重要度に従って ABC に分類する「ABC 分析」の考えを適用できる．

(3) コンサルタント，審査員の課題

- コンサルタントや審査員の業務理解度が低い． 特に一部の審査員に当該業界経験が少ないと思われる．
- 「審査をやり，認証を与えてやる」と言った態度を示す審査員が一部にいる．
- 審査員の ISMS やセキュリティ技術の理解度は高い評価(8 以上)を得ているが，アンケート等からは厳しい記述も見られる．
- 審査員毎に見解が異なり，その理由が明確でないこともあり，一部の審査員の態度や指摘内容からセキュリティ知識の欠如が見られる．
- 審査員には，「継続的専門能力開発（CPD)」との名称で資格修得後に教育を行っているが，コンサルタントは特にないため，コンサルタントの利用での判断に迷うとの指摘もある．任意で「継続的専門能力開発（CPD)」を行い，協議会等のウェブに公表する仕組みを構築することも検討に値する．

(4) その他(入札条件について)

- ISMS 認証取得が目的化している．この問題は，ISO9000(品質マネジメント)では，2004 年頃から官庁･自治体等の入札条件から外す動きがでてきた[4]．認証取得組織の資質が入札条件を満たさない，認証未取得企業でも十分な資質があるという矛盾からきた．ISMS でも同じ問題が発生している．私企業が取引先企業に要求するのは自由だが，官庁･自治体等の対応は ISO9000 と同様に入札条件から外すべきであろう．

表６ 某審査員から指摘された内容

社外持出 PC で： (1)ハードディスクを暗号化し，(2)PC 起動時に ①BIOS，②ハードディスク暗号化ソフト，③Windows の 3 段階のパスワードが必要で，(3)メーラー起動時もパスワードが必要だったが，審査員は電子メールはサーバに格納すべきと指摘（観察事項）し，反論に対し，「これは常識です．どこの会社でもやっている」と述べた．

3.3. 推進面の課題

(1) 管理目的･管理策への誤解

- 管理目的･管理策の誤解は推進を担う事務局担当者(以下,「ISMS 推進者」という)にも多い．
  - 管理策を「チェックリスト」と考え，各項目の可否を確認し，判断する
  - 管理項目の取捨選択，内容の変更(内容の高度化)ができないとの誤解
  - 管理項目が最新技術等に対応していないとの誤解

(2) ISMS 対応と業務処理の乖離

- 業務と乖離ありの回答が 26%以上あり，どちらとも言えないも 35%を越えている．
- ISMS 更新審査やサーベイランスが毎年あるが，それが近づくと，ISMS 向けの資料作成を ISMS 推進者が作成し，維持･更新をはかるという本末転倒のことまで一部で行われている．
- 禁止ポリシーを作成することが推進者の責任と考えている．
  例：ノート PC 等の持出禁止ポリシーの作成．
- ISMS の効果を高めるために，一般社員の認識･理解の向上に 67%以上が努めている．大部分が集合教育(82&：複数回答)を中心に据えているが，17% が出欠だけという現状もある．

(3) 教育･訓練について

- 教育もその効果を考え，参加者の興味を引く[10]工夫も必要で，教育の効果測定も大切になる(付録２ カークパトリックの４段階評価[5])．
- 少人数で推進している事業所では，ISMS 推進者の育成ができず，担当者が定年退職時期になっている事も多い．ISMS 推進者が全く育っていないという課題も

10 1953 年に心理学者 E.C.チェリー (E.C.Cherry)が提唱した「カクテルパーティ効果」というものがある．カクテルパーティ会場等で，様々な会話が行われていても，興味のある会話はきちんと聞き取ることができる人間の特性． 逆に考えれば，興味を持たないことは記憶にも残らないと考えられる

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

顕在化している.

(4) その他

- インシデントが減らない要因には，いくつか考えられる.
  - インシデントの詳細が報告されず，概要で集計される．コンピュータウイルス感染の有無で，感染があった事業所(約 33%)で「ウェブ感染」(約 52%：複数回答)のみ半数以上となっているが，「ウイルス感染」のみの報告では十分な対応ができないと考えられる.
  - 原因追及は「個人責任を追求する」との考えがあり，原因を除去できない.
  - 経営者の「予断」が，インシデントの本質を曲げる[6].

4. セキュリティマネジメント体制確立への提言

ISMS 認証を取得した企業において，セキュリティマネジメント体制を確立するためにはどの様なことが必要かを ISMS 調査等から考察を行なう.

(1) 経営者／経営層の課題

- 最低限，情報セキュリティや ISMS への関心を持つ．ISMS はマネジメント体制を確立することで，情報セキュリティ技術の詳細を知る必要はない.
  例１：数年の間に，二人の社長から「ISMS 認証取得をしないのか？」と聞かれた複数の課長は ISMS 認証取得のため，調査･研究を行い，効率的な ISMS 体制が構築できた.
  例２：OS の脆弱性を狙ったワームが世界中に広がったニュースを見た社長は担当役員に，担当役員は担当課長に自社サーバの脆弱性を確認した.
- ISMS は，個人情報保護が中心と考えている経営者が多いが，情報資産[11]全般が対象で，個人情報だけでなく，企業機密の多くが情報資産と考えられ，それらを保護する事は企業経営からも重要との認識が必要である.
- ISMS 推進に対する透明度を高めることが大切．推進担当から，二重帳簿的な対応をしていると言った仕組みを解消すべき.

(2) ISMS 推進者の課題

- ISMS 認証制度は，マネジメントシステムである認識を持ち，リスクや監査の考えを適用する.
- 現場の従業員を巻き込む仕組みを考え，単に「禁止」することを優先しない.
- 経営層に分かる言葉で説明し，ISMS や情報セキュリティに関心を抱かせる努力を行う.

(3) 審査機関の課題

- 認証取得事業所調査･情報収集を行い，審査等の課題を解消する.
- 認証取得事業所トップに，ISMS 体制の重要性[12]を聞いてみる.

5. まとめと今後の課題

本稿では，ISMS 認証取得事業所調査を中心に考察を行った．ISMS 制度の要求を十分満たしているとの回答もあるが，時間の経過や環境の変化でリスクが変動することを考えると終わりはないと言える.

また，ISMS 推進がマンネリ化しているとの回答もあるが，「成熟度モデル」を ISMS 推進に取り入れ，ISMS の維持・推進を行うことも有効であると考えられる．情報セキュリティやマネジメントシステムの「現場力」を養成できれば，組織としての効率化･高度化を達成できると考える.

ただ，残念ながら，認証制度自身にも多くの課題があるが，制度面からの課題は比較的小さく，ISMS 推進事業所を中心に，審査機関等の協力があれば，十分，情報セキュリティマネジメントシステムの確立は可能である.

今後，ISMS 関連調査や認証取得認定の最終段階(認証機関審査判定委員会)等を通して，ISMS 認証の維持･推進での課題(「問題事例」,「成功事例」)を深めて行きたい．また，ISMS 認証取得事業所や審査機関での教育･訓練について考察を行いたい.

謝辞 本調査実施にあたり，一般財団法人ニューメディア開発協会の資金を利用させて頂きました．お礼申し上げます.

参考文献

[1] フレッド・ライクヘルド：顧客ロイヤルティを知る「究極の質問」,ランダムハウス講談社(2006)
[2] ISMS 認証事業所調査 http://www.uchidak.com/isms/
[3] 日本工業標準調査会: JISQ27001:2006 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ム－要求事項,日本規格協会(2006)
[4] 日経コンストラクション：ISO を入札要件から外す,日経 BP 社(2004.6.11)
[5] (独)雇用･能力開発機構：公共能力開発施設の行う訓練効果測定(2005)
[6] M.A.ロベルト： なぜ危機に気づけなかったのか，英治出版(2010)

11 情報資産には，情報(デジタル，アナログ)，情報処理機器，周辺設備，人間を含まれる.

12 経営者に「大規模な情報漏えいやシステム停止が発生を考えたことがあるか？」と聞いてみるのも1つの方法であろう.

Vol.2012-DPS-150 No.26
Vol.2012-CSEC-56 No.26
2012/2/29

付録

付録１ 管理目的及び管理策

A.5 セキュリティ基本方針	**A.11 アクセス制御**
A.5.1 情報セキュリティ基本方針	A.11.1 アクセス制御に対する業務上の要求事項
A.6 情報セキュリティのための組織	A.11.2 利用者アクセスの管理
A.6.1 内部組織	A.11.3 利用者の責任
A.6.2 外部組織	A.11.4 ネットワークのアクセス制御
A.7 資産の管理	A.11.5 オペレーティングシステムのアクセス制御
A.7.1 資産に対する責任	A.11.6 業務用ソフトウェア及び情報のアクセス制御
A.7.2 情報の分類	A.11.7 モバイルコンピューティング及びテレワーキング
A.8 人的資源のセキュリティ	**A.12 情報システムの取得，開発及び保守**
A.8.1 雇用前	A.12.1 情報システムのセキュリティ要求事項
A.8.2 雇用期間中	A.12.2 業務用ソフトウェアでの正確な処理
A.8.3 雇用の終了又は変更	A.12.3 暗号による管理策
A.9 物理的及び環境的セキュリティ	A.12.4 システムファイルのセキュリティ
A.9.1 セキュリティを保つべき領域	A.12.5 開発及びサポートプロセスにおけるセキュリティ
A.9.2 装置のセキュリティ	A.12.6 技術的ぜい弱性管理
A.10 通信及び運用管理	**A.13 情報セキュリティインシデントの管理**
A.10.1 運用の手順及び責任	A.13.1 情報セキュリティの事象及び弱点の報告
A.10.2 第三者が提供するサービスの管理	A.13.2 情報セキュリティインシデントの管理及びその改善
A.10.3 システムの計画作成及び受入れ	**A.14 事業継続管理**
A.10.4 悪意のあるコード及びモバイルコードからの保護	A.14.1 事業継続管理における情報セキュリティの側面
A.10.5 バックアップ	**A.15 順守**
A.10.6 ネットワークセキュリティ管理	A.15.1 法的要求事項の順守
A.10.7 媒体の取扱い	A.15.2 セキュリティ方針及び標準の順守，並びに技術的順守
A.10.8 情報の交換	A.15.3 情報システムの監査に対する考慮事項
A.10.9 電子商取引サービス	
A.10.10 監視	

付録２ カークパトリックの４段階評価

レベル	説　明
1.研修満足度	受講直後のアンケート調査等による受講者の研修に対する満足度の評価 ある基準と比較して望ましい研修が行なわれたかを評価
2.学習到達度	筆記試験やレポート等による受講者の学習到達度の評価 研修受講の結果，受講者という個人に与えた効果（学習到達）を測定
3.行動変容度	受講者自身へのインタビューや他者評価による行動変容の評価 研修受講の結果，受講者という個人に与えた効果（行動変容）を測定
4.成果達成度	研修受講による受講者や職場の業績向上度合いの評価 受講者個人の行動がもたらした組織への影響
5.投資収益率	効果測定は，効果を収益に換算し，収益を教育研修への投資額との比較ではじめて有意義になる（ジャック・フィリップスの提案） 収益貢献度（レベル 5A） = その成果を収益金額に換算 顧客満足度（レベル 5B） = 顧客の満足に与えた成果を見たもの