Vol.2010-CSEC-50 No.42
2010/7/2

Pマーク審査から見た中堅企業の情報セキュリティ・ガバナンス

板倉征男[†]　松田治男[††]　鈴子 学[†]

P（プライバシー）マークの審査を通してみた最近の中堅企業の情報セキュリティ・マネジメントや情報漏えい対策の傾向，特に経営者の情報セキュリティに対する考え方の傾向を述べる．不況下で一般に情報セキュリティに対しては従来のようなマンパワーは掛けられないが，ローコストながら全社で取り組んで成果をあげつつある中堅企業も見られ学ぶべき事も多い．
キーワード：ローコスト情報セキュリティ対策，持続可能な PDCA サイクル，不況下の情報
セキュリティ・ガバナンス

Information Security Governance for Medium enterprise through P mark certification

Yukio Itakura[†]　Haruo Matsuda[††]　Manabu Suzuko[†]

In this paper, we suggest the tendency of the recent medium enterprise information security management and the information leakage measure through the certification of the P mark, specifically, the tendency of the way of thinking about the information securities of the executive.
Under the depression, the general enterprise can not spend operation like the past on the information securities.

１．はじめに

中小企業の情報セキュリティ対策は，大企業に比べて遅れているとされている．確かに中小企業においては，専門家やスタッフの人材が不足しており，組織全体の取組みが十分出来ていない事など，大企業に比べてハンディは大きい．

IPA の報告によれば，自社診断シートの合格目標である 70 点をクリアー出来る中小企業は，全体の 3 割にとどまっている[1].

一方，プライバシーマーク(以下 P マークと略す)の取得企業は 2010 年 5 月現在で 1 万 1000 社を超え，その中で中小企業が 1900 社を超えている．2)　事業上，P マークは企業にとって，必要な認証資格となっており，取得に要する費用も ISMS に比べれば経済的であるため，中小から大企業未満の，いわゆる中堅企業でも幅広く普及し続けている．そこでこれら中堅企業の情報セキュリティの最近の動向を把握するために P マークの審査状況を参考にメスを入れてみる事とする．

２．Pマークの審査

2.1 Pマークの審査のフロー

P マークは企業等における個人情報保護の認識，総合的なマネジメント体制の確立，及びその維持を目的に審査を行い，基準をクリアーできた申請者に認証を付与する仕組みである[2].
審査フローの概要は図-1 に示す様に進められる．

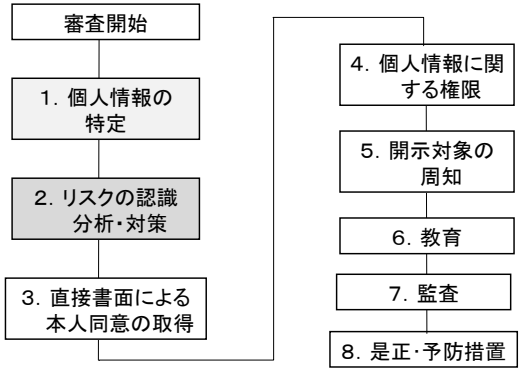

図-1 P マーク審査のフロー

(1)　個人情報の特定

組織によって特有な個人情報の把握が行われ，重要度の認識や取捨選択のポリシーなどいわゆる個人情報の特定作業の実施状況を審査する．

この段階では管理すべき個人情報の漏れがないかが問われる．漏れが指摘される

[†] 情報セキュリティ大学院大学
Institute of Information Security
[††] 日本データ通信協会
Japan Data Communications Association

例としては, 入退場記録, PMS(プライバシーマークシステム)の運用記録, 教育記録, バックアップ記録，音声記録，個人情報取得の同意書などがある．

(2) リスクの認識・分析・対策

個人情報の特定の後，ライフサイクルに基づく分析，リスクの認識・分析・対策及びその規定の存在，残存リスクの認識などが問われる．これらの対策ができているのは全体の 2-3 割に過ぎないと言われている．

(3) 直接書面による本人同意の取得

個人情報を収集する時，直接本人から書面で同意書をとっているかが問われる．なお次の 8 項目は利用目標の公表だけでよい．a.事業者の氏名・名称，b.個人情報保護者，c.利用目的，d.第 3 者への提供，e.委任，f.問い合わせ窓口

(4) 個人情報に関する情報

保有個人データは開示権限や訂正権限の明確な管理が問われる．開示対象の個人情報には，認識の間違いが多い．

2.2 審査過程と指摘事項

この様にして P マークの審査が進められるが，各段階で審査内容が不十分でクリアーできない場合は，審査員指摘事項となり，修正・改善などの手直しが求められる．これには軽微なものと重大なものがある．後に指摘事項の質と量を，受診者の評価の参考とするために前者を△，後者を×として記録を残している．

図-2 は上記の項目順に審査が進む時，審査員指摘が，どの項目でどの程度の数になるかを，グラフにしたものである．横軸の下記の A.B.C・・・は審査の項目のうち，指摘が特に多いものを示している[3].

A.個人情報の特定
B.直接書面による承諾
C.リスクの認識・分析及び対策
D.委託先の監督
E.監査
F.是正措置・予防措置

縦軸の棒グラフは，各々の審査項目で審査員が示した指摘事項の総数を示している．2 つの棒グラフのうち，左側は重大な指摘(×)，右側は軽微な指摘(△)である．サンプルはいずれも新規審査で，サンプルの全数が 106 社であるから，ここに取り上げた審査項目については，いかに多くの指摘を受けているかがわかる．

これらの審査項目にうち A(個人情報の特定)，B（直接書面による承諾）と C（リスクの認識・分析及び対策）は関連する指摘事項と考えてよい．個人情報が特定できないと，直接書面による承諾が行われない．その結果，リスクの認識・分析及び対策もできていないという事になる．大半の申請者はこの三箇所で躓いている．

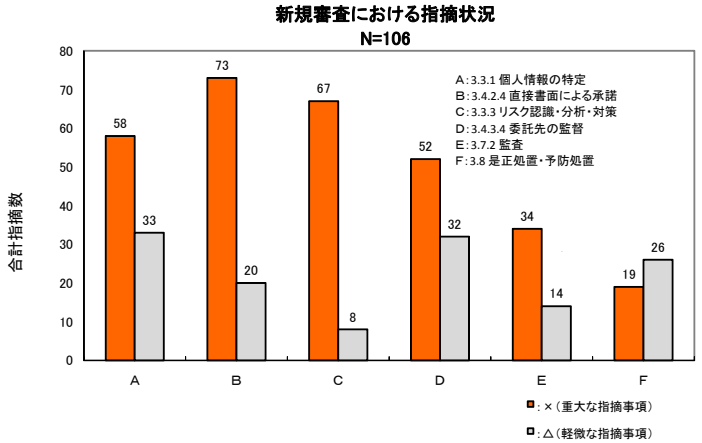

図-2　新規審査時の指摘事項

2.3 指摘事項の内容

(1) 個人情報の特定が出来ていない

事業者は自らの業務フローの中で，どのような個人情報をどう扱うか，方針を決める事が最も重要である．経営者が本気で考えなくては，個人情報は特定出来ないが，P マークの取得だけを求める事業者は，概してあいまいにしているケースが多い．

(2) リスク分析が出来ていない

リスクに対する要求レベルも不明確である事業者が多い．個人情報の特定が出来ていないと次の段階でリスクの把握が出来ない．残存リスクもつかめない．

(3) PDCA サイクルのマネジメントに取り組んでいない

更新審査までの間は PDCA サイクルのマネジメントに取り組んでいない事業者が多い．

2 年間に 1 度の更新審査が終わると，2 年間のお休みになる事業者もある．更新審査が迫ると慌てて準備して受診する事になるが，毎年義務付けられている見直しを実施していない事業者は，本来更新に際してチェックアウトされてもおかしくない．

(4) 委託先の管理が出来ていない

委託先での個人情報の漏えいが問題であるが，管理されていないケースが多い．

Vol.2010-CSEC-50 No.42
2010/7/2

その他，審査側の問題として，審査判断基準のばらつきがあり，定期的なチェックに対する要求基準が不明確である．また事業者のモラル，特に，消費者保護法に抵触する受診者の排除ができない，などの指摘がある．

図-3 は更新審査時の指摘事項の状況である．更新審査において，本来，指摘数は新規審査より格段に少ない事が自然であるが，実際には上記の A,B,C 項目などについて，新規審査と同様に指摘を受けている．この点については次章で取り上げ，追求する．

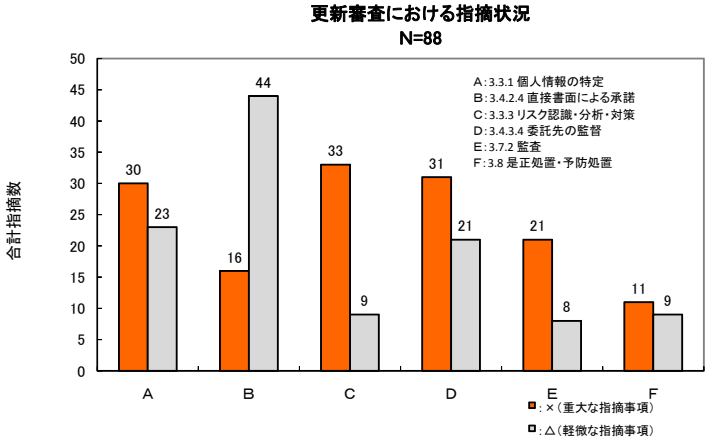

図-3　更新審査時の指摘事項

2.4　企業側の体制の問題

以上の審査状況から，P マークを取得している企業の情報セキュリティ・マネジメントの水準は必ずしも高くない事が想定される，ちなみに現在関係している審査組織のリーダクラスの審査員アンケートによって，企業の取組み姿勢を評価してもらった．図-4 はこれらの P マーク取得済みの企業群を A：組織全体で取組み PDCA を良好に回している，B：取組みは不十分である，C：目的や主旨の理解がほとんど出来ておらず取組みに問題がある，と振り分けて評価してもらったところ A＝28%，B＝60%，C＝12%という結果となった．つまり A クラスを除けば，およそ 7 割強は PDCA を十分回していないか，全く回していないという状況である事が分かった．

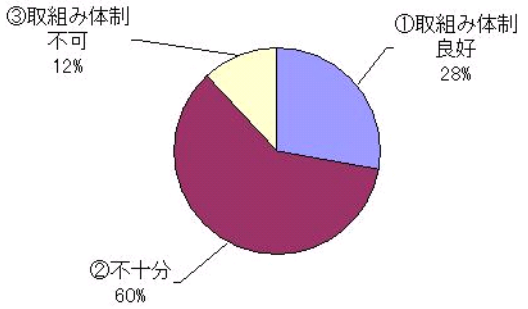

図-4　取得企業の体制概要　N＝100

3.　PDCA サイクルの状況確認

3.1　問題構造図と PDCA サイクル回転状況

組織の情報漏えい対策の問題点を構造的に把握するツールとして考えたのが，問題構造図である．この図は縦横 3×4 のマトリクスで表した問題の整理棚であり，縦軸は経営層－管理層－実務層という組織のハイアラーキを，また，横軸は各々の層が自らの責任で，毎日取り組んでいる仕事の PDCA プロセスチェーンを示している．

図-5 はこの問題構造図を使って，一般的な組織の情報セキュリティ対策の実状を示したものである[4]

一般的に組織の情報セキュリティ対策とは Plan の欄の経営層から方針が出され，それが管理層に下りて実行計画が作られ，さらに実務層すなわち現場に下ろされて，施策が実施される．その後，現場からの報告で結果の反省が行われ，実務層と管理層の間のやり取りで修正され，継続的に推進される．管理層で手に負えないところは，経営層に問題が上げられて必要なアクションがとられる，というプロセスを立体的に見る事が出来るであろう．

問題がある時は，階層間で情報の伝達と理解がスムーズにできていないからである．それを解明するためにも，この整理棚は活用出来る．すなわち問題がある状態を，階層別に何が問題になっているかという観点で，悪さ加減を縦横に整理し，問題解決のための対策を打てる様にする．問題点と課題を全組織で「見える化」すると考えればよい．

Vol.2010-CSEC-50 No.42
2010/7/2

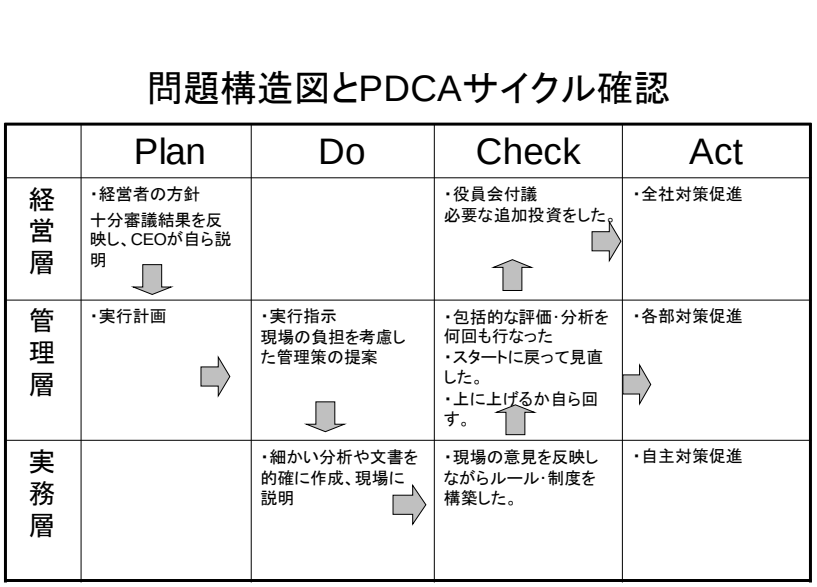

図-5　問題構造図を用いた情報セキュリティの PDCA

図-6 は情報セキュリティ対策の取組み体制が不可と指摘される典型的な例である．経営層の理解と方針が不明確なまま走り出すと，管理層の甘い実行計画で現場に指示を出し，実務層は被害者意識で形だけの情報セキュリティ対策をするだけ，となるパターンである．問題構造図で×をつけたところで問題が発生している事が分かるが，それだけでなく，前後も関係している．したがって，その動的な関係にメスを入れていけば問題解決のヒントを得る事が出来る．

図-7 は情報セキュリティ対策の取組みが理想的にできている組織を示す．この企業はトップが方針を示し，管理層に指示した後，管理層のスタッフは実務層以下の取組み意識を高め，全員参加型の取組みに勤めている．各整理棚の位置に，太字で記述した詳細な取組みの数々が，全社の取組みを推進する要素となっている．特に，管理層から実務層の Check から Act の区間で，これらの太字で書かれた細かい施策が，現場を取込んで効果的に PDCA を回している事につながっている．

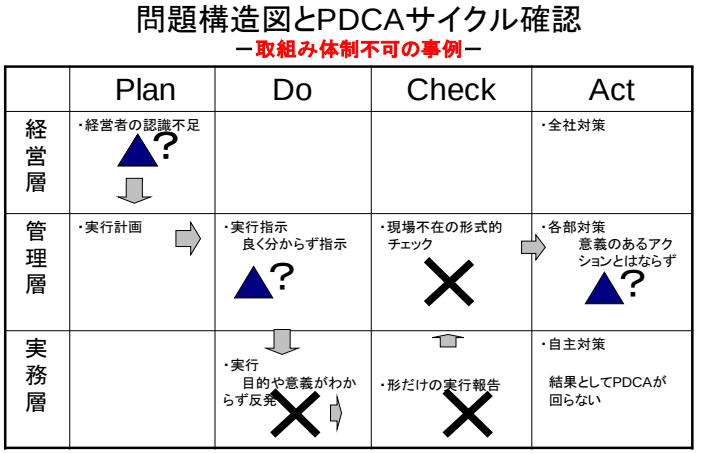

図-6　取組み不十分な体制の例

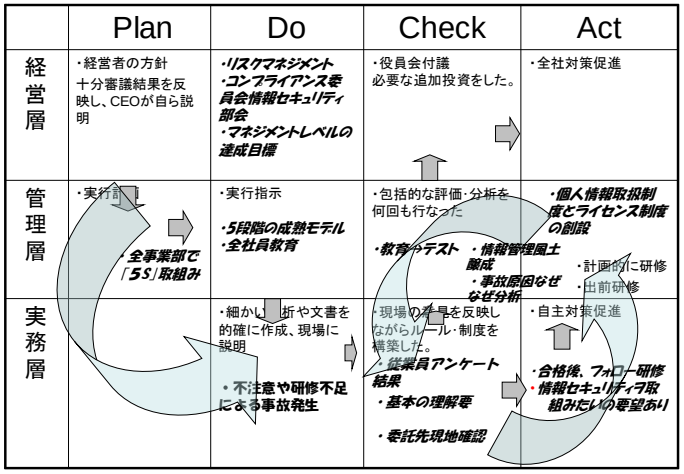

図-7　全社的取組み体制良好な事例

4. 更新審査の役割りの再認識

4.1 更新審査の意義と活用

中堅企業においては，個々の情報セキュリティ対策を評価する前に，企業全体として PDCA サイクルがきちんと回っているか，把握する事が重要である．大企業では事業が多角化するし，組織も大きくなるので，必ずしも全社で一元的に施策を講ずる事が最適とは言えないであろうが，中堅企業では，各部で個別に投資の多寡を論じている余裕は無いと考えられるため，まず全体で，コストをかけずに，PDCA を継続的に回しているか，という点を最優先で見ておかねばならない．

PDCA の回っている状態をどのようなアルゴリズムで確認するかは，前章の様に，問題構造図を描いて情報セキュリティ対策の体系的問題を探る事が説得力のある方法である．しかし情報の収集と結果の分析に多くの手間がかかる．そこでもっと簡単に PDCA の回転状況を探る方法を考察する．

ここで，図-3 の結果を振り返ると，更新審査は 2 年おきという比較的短い周期で受診する事になるが，審査員の指摘事項が新規審査と同じ項目について，高い割合で指摘されていた．図-4 の審査員の評価の対象は，およそ半数が更新審査である事を勘案すると，更新審査における企業の実態は，新規の時と同様に，7 割方不十分であり，PDCA サイクルも良好に回っていないと推定する事が出来る．

視点を変えると，更新審査の状況をみれば，その企業の情報セキュリティ対策の状況が評価でき，打つべき基本的な戦略が提言出来るという事である．

このような発想で更新審査の実態をもう一度精査するため，2010 年 5 月に，過去 1 年分の更新審査受診した 88 社を取り上げた．

サンプルとした 88 社は,いずれも電気通信事業者及び電気通信に関する事業者である．売上高は年商 20-50 億円が一番多く，従業員の数は 11-30 名が一番多い．

4.2 更新審査で分かる企業の情報セキュリティ体制の実態

(1) 更新審査時の指摘事項の数と審査に要する期間の関係

図-8 より，更新審査において，企業の平素の取組みが良好であると，審査員の指摘事項の数が絶対的に少なく，その結果，更新審査に掛かる期間，すなわち審査完了までの期間が短い．このような企業は，概ね 1 ヶ月で更新審査をクリアーする．
一方，取組みが不十分であると，審査員の指摘を何回も受ける事になり，2 ヶ月以上，長い場合で数ヶ月掛かる例もある．

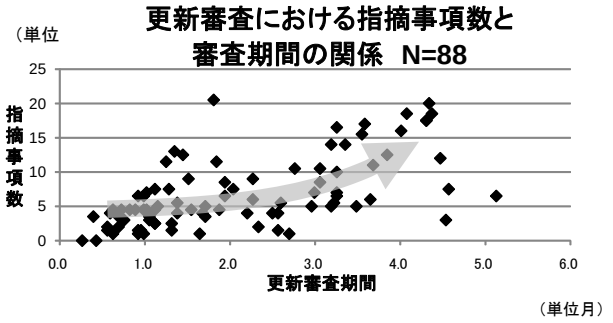

図-8　指摘事項数と審査期間の関係(更新審査)

(2) 企業側の取組み体制と更新審査に要する期間の関係

次に，更新審査を受診する企業の情報セキュリティ対策の取組み体制と，更新審査に要する期間を分析した結果を図-9 に示す．

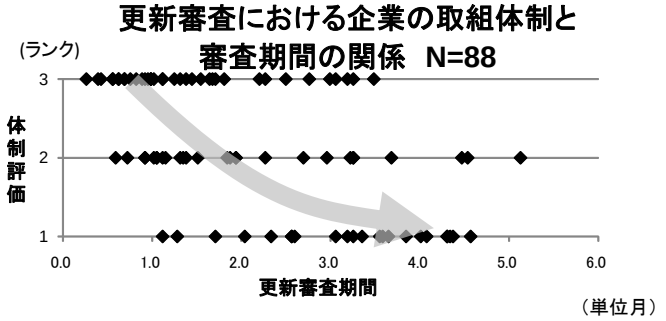

図-9 企業の取組体制と審査期間の関係(更新審査)

この表の縦軸は企業の取組み体制を 3 ランクに分けてプロットしたものであり，ランク 3 は経営層・管理層・実務層の 2 つ以上の層にキーマンとなる人物がいる，ランク 2 はいずれか 1 つの層にキーマンとなる人物がいる，ランク 1 はその層にもキーマンとなる人物がいない．ここでキーマンとは，企業側の情報セキュリティ対策を担当する人物の中で，P マークについて，基礎及び応用知識を持ち，他の社員を指導して，

審査をクリアー出来る人材を言い,審査に当たった複数の審査員が総合的に評価した．なお，中堅企業であるからキーマンは必ずしも専任でなくてもよく，例え兼任でも，その人が十分研鑽を重ね，更新審査の目的を十分理解し，信念を持って社内を指導できればよい．リーダの力を持つキーマンがいない企業は，予想通り，指摘の数が多くなる傾向があり，PDCA が良好に回っていない事を物語っている．

5. おわりに

以上，世間一般に低調だと言われる，中堅企業の情報セキュリティの取組みについて，P マークの認証取得，特に，更新審査の実態を通じて分析した．

全体で 3 割弱の，良好な成果を上げていると言われる企業の経営陣の中には，P マークの更新審査を一つのきっかけとして，組織内の情報セキュリティの対処策を推進し，全組織員の力を引き出して，PDCA サイクルを良好に回している例もあった．P マークでは個人情報の保護に力点を置いているが，これらの例から，認証取得審査は，個人情報の保護だけに留まらず，全組織の情報の総合的な安全管理を一気に進めるための，一つのきっかけになり得ると考える．

残るスペースでは，力任せの情報セキュリティ施策で壁にぶつかっている大企業が学ぶべき中堅企業のノウハウを紹介する[5][6].

先進中堅企業のローコスト PDCA 促進事例

(1) トップのビジョンの見える化と具体的方針の現場への提示

・情報セキュリティ委員会には CEO（社長）も出席する．社員からトップへのフィードバックは，CISO もメンバーである役員会で，毎回討議し打開策を講じる．

・顧客から情報セキュリティに関する要求があった場合，トップがそのセクションの委員と打ち合わせ，フォローしている．

・持ち株会社傘下のグループ会社で実施状況を点数評価し，グループ会社間の順位を公表する．

・P マークの取得後，キックオフを兼ねて社長表彰を行い，盛り上げている．

・マネージャクラスの輪番制を実施し，自身で考えるきっかけとしている．

(2) 持続的な会議の開催による現場との一体化

・セキュリティ部門で毎月 1 回，ミーティングを実施している．

・各部門のセキュリティリーダが参加する会議体を設け，現場の実施状況や実施に伴う提言や要望事項を発表し，問題解決に向けた意見交換を行っている．

・毎月開催する会議体で，他社の事故等の事例を共有する．また，社内への対策指示をここで行う．会議の結果は詳細な議事録を添付し全社に回覧する．出欠もチェックされる．

(3) 教育研修の工夫

・E ラーニングにより規則，規定類の改定の周知，ヒヤリ・ハットの周知，理解度の確認を行う．

・ハンドブックを全社員に配布し，平素の心掛けを指導している．

(4) 監査を通しての施策の徹底

・監査を通じて「リスク対応手順書」等の周知徹底を図る．監査員に対しては情報セキュリティ推進部門が後ろ盾となっている．

(5) セキュリティを日々の日課とするセルフチェック文化

・「自覚し自ら回す」という自社の情報セキュリティ対策の基本として，チェックシートを利用したセルフチェックを実施し，PDCA を回している．

・社内小集団の各ラインの小集団グループで「なぜなぜ分析」や「ヒヤリ・ハット体験の原因究明」などのグループ討議活動を実施した．また各グループで自分達が考えたり検討したりしている事を発表しあって全社的な意識の高揚に努めている．

・第一線から気さくに出る課題が重要と考え，そのような課題を委員会で取り上げて話をする．A4 で 4，5 枚のレポートを提案者が取りまとめ，委員会に発表してもらう．

参考文献

1) IPA セキュリティセンター：中小企業の情報セキュリティ対策の実施状況調査, http://www.ipa.go.jp/security/fy21/reports/sme-report/documents/sme-report(All).pdf pp.12-15(2009.10)
2) JIPDEC：プライバシーマーク制度, http://privacymark.jp/
3) 板倉征男,松田治男：プライバシーマーク付与審査から見た中堅 ICT 事業者の個人情報保護・情報セキュリティの現状と課題，日本データ通信,No.172(2010)
4) 板倉征男：情報セキュリティ課題への問題構造化技法の適用,経営情報学会(2008.4)
5) 猪野泰弘, 松田治男, 板倉 征男：情報漏えい対策における持続可能な PDCA サイクルを推進する方法, 暗号と情報セキュリティシンポジウム(SCIS)2010, (2010)
6) 吉岡宏明・菅沢博：当社の個人情報漏えい対策, 事例に学ぶ情報漏えい対策, 情報セキュリティ大学院大学セミナー(2010.6.24)